Safeguard for Privileged Passwords 7.0 LTS

管理者ガイド

Rev 1.2

2023/3/13

ジュピターテクノロジー

この文書の原本は、「One Identity Safeguard for Privileged Passwords 7.0.2 LTS - Administration Guide」です。この文書についてご不明な点やお気づきの点がございましたら、ジュピターテクノロジー株式会社までお問い合わせください。

このガイドの表記規則

警告：警告アイコンは、人身事故や物的損害を引き起こす可能性があり、業界標準の安全対策が推奨されることを表しています。このアイコンは、多くの場合、ハードウェアに関連する電気的な危険と関連しています。

注意：注意アイコンは、指示に従わない場合、ハードウェアの損傷やデータの損失が発生する可能性があることを示します。

変更履歴

版	発行日	変更内容
第 1.0 版	2022/11/24	新規作成（7.0 対応）
第 1.1 版	2022/12/12	7.0.1 対応
第 1.2 版	2023/03/13	7.0.2 対応

目次

1　はじめに

この文書は、Safeguard for Privileged Passwords（以降、「SPP」と表記します）の管理者ガイドです。想定される対象読者は、SPP を初めてインストールして構成する IT 管理者、UNIX 管理者、セキュリティ管理者、システム監査人、その他 IT プロフェッショナルの方々です。

> **メモ：**「Unix」という用語は、SPP の文書では、商標システムである Unix に酷似したオペレーティングシステムを示すために非公式に使用されています。

1.1　Safeguard for Privileged Passwords とは

Safeguard for Privileged Passwords アプライアンス（SPP アプライアンス）は、特権管理ソフトウェア Safeguard for Privileged Passwords（SPP）用に特化して構築されており、プリインストールされているためすぐに使用することができます。アプライアンスは、ハードウェア、オペレーティングシステム、ソフトウェアの各レベルでシステムの安全性を確保するために、強化されています。アプライアンスは、特権管理ソフトウェアを攻撃から保護すると同時に、導入と継続的な管理を簡素化し、価値を生み出すまでの時間を短縮します。

SPP 仮想アプライアンス、クラウドアプリケーションも利用できます。仮想環境を構築する際には、CPU、メモリの空き容量、I/O サブシステム、ネットワークインフラなど構成要素を慎重に検討し、仮想レイヤーに必要なリソースを確保できるようにしてください。詳細については、「One Identity 製品のサポートポリシー」を参照してください。

Safeguard 特権管理ソフトウェアスイート

Safeguard 特権管理ソフトウェアは、特権ユーザーアカウントとアクティビティを制御、監視、管理し、悪意のあるアクティビティの可能性を特定して資格リスクを検出し、改ざん防止の証拠を提供するために使用されます。Safeguard 製品は、インシデント調査、フォレンジック、コンプライアンスの取り組みにも役立ちます。

Safeguard 製品独自の強みは次の通りです：

- すべての特権アクセス管理のニーズに対応するワンストップソリューション
- 導入と統合が簡単
- 比類のない記録の深さ
- 資格とアクティビティの包括的なリスク分析
- 特権アカウントの徹底的なガバナンス

このスイートには、次のモジュールが含まれます：

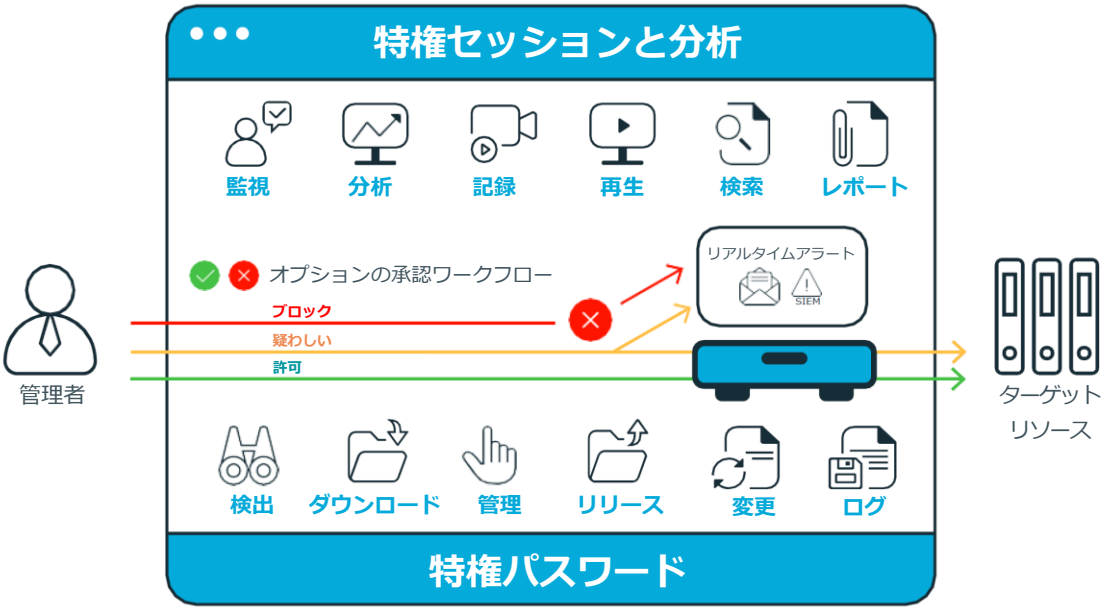
- **Safeguard for Privileged Passwords（SPP）**
  ロールベースのアクセス管理と自動化されたワークフローにより、特権資格情報の付与プロセスを自動化、制御、保護します。堅牢なアプライアンス上に展開される SPP は、ソリューション自体への安全なアクセスに関する懸念を払拭し、お客様のシステムや IT 戦略との統合を迅速に行うことができます。さらに、ユーザーを重視した設計のため短時間で習得でき、どこからでもほぼすべてのデバイスを使用してパスワードを管理することができます。企業のセキュリティを確保し、特権を持つユーザーに新たなレベルの自由と機能性を提供します。

- **Safeguard for Privileged Sessions（SPS）**
  One Identity の特権アクセス管理ポートフォリオの一部です。大企業のニーズに対応した特権セッション管理ソリューションで、業界最高水準のアクセスコントロールに加え、特権アカウントの悪用防止、コンプライアンスの推進、フォレンジック調査の迅速化を実現するセッション監視・記録を提供します。

  SPS は、クライアントやサーバーから完全に独立しているため、既存のネットワークにシームレスに統合でき、迅速に展開できるエンタープライズアプライアンスです。ユーザープロファイリングに必要なアクティビティデータを取得し、フォレンジック調査のためにユーザーセッションの完全なドリルダウンを可能にします。

- **Safeguard for Privileged Analytics（SPA）**
  Safeguard for Privileged Sessions（SPS）のデータを統合し、特権ユーザーの行動分析のベースとして使用します。SPA は、機械学習アルゴリズムを用いて行動の特徴を精査し、個々の特権ユーザーごとにユーザー行動プロファイルを生成します。SPA は、実際のユーザーの行動とユーザープロファイルをリアルタイムで比較し、プロファイルは機械学習により継続的に調整されます。SPA は、異常を検出し、リスクに基づいてランク付けを行うため、優先順位を付けて適切な対応を行い、最終的にデータ侵害を防ぐことができます。

図 1：特権セッションと特権パスワード



1.1.1 エンティティの概要

SPP は、コンピューター、サーバー、ネットワークデバイス、ディレクトリ、アプリケーションなどの資産を安全に保護するための、パスワード、キー（鍵）、シークレットの保管庫です。

SPP エンティティの概要と関係は、次の通りです。

資産、パーティション、プロファイル

資産には、SPP が管理するコンピューター、サーバー、ネットワークデバイス、ディレクトリ、アプリケーションなどが含まれます。資産には、ユーザーアカウントとサービスアカウントが関連付けられます。資産とアカウントは（例えば、Active Directory から）インポートすることができます。資産は、資産グループに属している場合もあれば、そうでない場合もあります。

パーティションは、アカウントのパスワード、SSH キー（確認と変更を含む）に対する委任管理のためのコンテナです。パーティションは、SoD（Separation of Duties＝職務分掌）を実現するために、資産をさまざまな所有者に分離するためにも有効です。パーティションでは、複数の資産管理者を設定でき、それぞれが独自のワークスペースで管理対象システムのパスワードガイドラインを定義することができます。一般的には、地理的な場所、所有者、機能、オペレーティングシステムによって資産をパーティション化します。たとえば、Unix 資産をパーティションにグループ化し、Unix 管理者にその管理を委任することができます。すべてのパーティションには、パーティション所有者が必要です。

１つの資産は、一度に 1 つのパーティションにのみに割り当てることができます。資産をパーティションに割り当てると、その資産に関連付けられているすべてのアカウントが自動的にそのパーティションに再割り当てされます。その後、その資産に追加した新しいアカウントは、自動的にそのパーティションに割り当てられます。

プロファイルには、パーティションに割り当てられた資産と資産のアカウントを管理するスケジュールとルールが含まれています。たとえば、プロファイルは、資産またはアカウントでパスワードチェックを必要とする頻度を定義します。

パーティションには、必要に応じて、それぞれが異なる資産に割り当てられた複数のプロファイルを含めることができます。アカウントは、1 つのプロファイルのみによって管理されます。アカウントにプロファイルが明示的に割り当てられていない場合、そのアカウントは親資産に割り当てられたアカウントによって管理されます。その資産にプロファイルが割り当てられていない場合、パーティションのデフォルトプロファイルが割り当てられます。パスワードの変更時にサービスを更新または再起動する場合、資産に割り当てられたプロファイルは、依存するアカウントサービスの変更に使用されます。

新しいパーティションを作成すると、SPP はデフォルトのスケジュールとルールを使用して、対応するデフォルトのプロファイルを作成します。複数のプロファイルを作成して、パーティションに割り当てられたアカウントを管理できます。資産とアカウントの両方がプロファイルのスコープに割り当てられます。

例えば、12 個のアカウントを持つ資産があり、60 日ごとにパスワードを確認して変更するようにプロファイルを構成したとします。そのうちの 1 つのアカウントで 7 日ごとにパスワードを管理したい場合は、別のプロファイルを作成し、その新しいプロファイルに個々のアカウントを追加できます。これで、SPP は 7 日ごとに変更されるこのアカウントを除き、この資産のすべてのパスワードを 60 日ごとに確認し、変更します。

以下の例では、パーティション A に 3 つのプロファイル（プロファイル A、B、C）とデフォルトのプロファイルがあります。プロファイル A は 30 日ごとにパスワードをチェックします。プロファイル B は 3 か月ごとにパスワードをチェックし、プロファイル C は最もセキュリティレベルが高く、7 日ごとにパスワードをチェックします。「資産：サーバー」には、資産に関連する異なるアカウントを管理する 2 つのパーティションプロファイルがあることに注意してください。プロファイル A、B、C はすべて、表示されているアカウントと資産に明示的に割り当てられています。「資産：クラウドサービス」には、明示的に割り当てられたプロファイルがないため、資産のアカウント管理にはデフォルトが使用されます。

図 2 ：パスワード制御

詳細：資産と資産グループ

- 資産とは、コンピューター、サーバー、ネットワークデバイス、ディレクトリ、アプリケーションです。
- 1 つの資産に複数のアカウントでログインすることができますが、1 つのアカウントは 1 つの資産にしか関連付けることができません。
- プロファイルに資産を選択すると、すべてのアカウントが含まれます。
- 資産は 1 つのパーティションにのみ割り当てる必要があります。通常、資産にはプロファイルがありますが、必須ではありません。
- 同じデバイスまたはアプリケーションに対して複数の資産を作成し、資産ごとに異なるアカウントを管理できます。たとえば、ディレクトリ資産はフォレストのサブセットを管理できます。
- 資産グループは、資格のアクセスリクエストポリシーのスコープに追加できる資産のセットです。

詳細：パーティションとプロファイル

- パーティションは、プロファイルによって管理される資産（および資産に関連するアカウント）のグループで、資産管理を委任するために使用されます。１つの資産が同時に所属できるのは、１つのパーティションのみです。その資産に関連付けられているすべてのアカウントは、自動的にパーティションに追加されます。
- プロファイルとは、パーティションの資産と資産のアカウントを管理するスケジュールとルールのことです。デフォルトのプロファイルを設定し割り当てることも、プロファイルを資産やアカウントに手動で割り当てることもできます。
- パーティションが作成されると、そのパーティション用にデフォルトプロファイルが作成されます。このプロファイルは、パーティションに追加されたすべての資産とアカウントに暗黙的に関連付けられます。後で、別のプロファイルを資産とアカウントに手動で割り当てることができます（これは、明示的な関連付けと呼ばれます）。明示的な関連付け（手動割り当て）は、暗黙的な関連付け（自動割り当て）より優先されます。

アカウント、アカウントグループ、資格、資格アクセスリクエストポリシー

資産には、ユーザーアカウントや Windows サービスのアカウントのような、関連するアカウントがあります。アカウントは、１つの資産にのみ関連付けることができます。

資格は、ユーザー、ユーザーグループ、またはその両方へのアクセスを許可します。資格には、１つ以上のアクセスリクエストポリシーが含まれ、ヘルプデスクサポートや Unix 管理者のような職務に関連することがあります。

資格アクセスリクエストポリシーは、ポリシーによって管理されるものを定義し、「ポリシーのスコープ」として参照されます。アクセスリクエストには、パスワードタイプとセッションタイプがあります。

- パスワードリクエストまたは SSH キーのアクセスリクエストポリシーを定義するためにスコープ内の有効なプロパティはアカウントとアカウントグループです。
- セッションリクエストのアクセスリクエストポリシーを定義するためにスコープ内の有効なプロパティは、アカウント、アカウントグループ、資産、資産グループです。アクセスリクエストポリシーで資産または資産グループのみが定義されている場合、**［資産ベースのセッションアクセス］**オプションは**［なし］**以外である必要があります。

資格アクセスリクエストポリシーには、次のものが含まれる場合があります：

- アクセスタイプ：
    - 資格情報アクセスタイプは、パスワードと SSH キーを含みます。
    - セッションアクセスタイプは、Secure SHell（SSH）、Remote Desktop Protocol（RDP）、Telnet プロトコルを含みます。
- スコープ：
  必要に応じて、アカウント、アカウントグループ、資産、資産グループ
- 要求者設定：
  リクエストの理由、コメント、（該当する場合）チケット番号、アクセス期間を含む
- 承認者とレビュー担当者の設定：
  必要に応じて、承認者とレビュー担当者、通知を含む
- アクセス設定：
  アクセスタイプ（パスワード、SSH キー、SSH セッション、以前に設定した RDP セッション）に応じた設定
- セッション設定：
  SPS を使用している場合、セッションを記録するために使用
- 時間制限：
  アクセスできる日数と時間帯を設定
- 緊急設定：
  連絡先（この情報を指定することを選択した場合）

以下の例では、各アカウントまたはアカウントグループは、1 つの資産にのみ割り当てられています。「資産：サーバー」は、「アカウント D」と複数のアカウントで構成される「アカウントグループ A」に関連付けられています。「アカウントグループ A」には、「資格：アクセスリクエストポリシーA」が割り当てられているため、このグループは月曜日から金曜日の午前 8 時から午後 5 時まで、承認不要でパスワードをチェックアウトすることができます。「アカウント D」に関連付けられている「資格：アクセスリクエストポリシーB」は、同じ時間帯のパスワードのチェックアウトを許可していますが、チェックアウトには承認が必要です。「資格：アクセスリクエストポリシーC」は、システムメンテナンス時間を考慮して、午前 12 時 59 分から午後 11 時 1 分までパスワードのチェックアウトを許可しています。

図３：資格とアカウント

詳細：アカウントとアカウントグループ

- アカウントは１つの資産にのみ関連付けることができます。
- アカウントグループは、資格アクセスリクエストポリシーのスコープに追加することができるアカウントのセットです。アカウントグループは複数の資産にまたがることができます。
- ディレクトリアカウントは、ディレクトリである資産に関連付けられます。
- ディレクトリアカウントとディレクトリ資産の両方を、特定の目的のためにパーティションの境界を越えて表示または「共有」することができます。ディレクトリ資産は、AssetDiscovery ジョブで共有できます。ディレクトリアカウントは、Windows サービスやタスクのサービスアカウントまたは依存アカウントとして使用できます。

詳細：資格とアクセスリクエストポリシー

- 資格とは、リソースを制限するアクセスリクエストポリシーのセットであり、通常はジョブロールによって制限されます。
- 資格は、ユーザーまたはユーザーグループのメンバーが、資格アクセスリクエストポリシーのセットの範囲内のアカウントにアクセスすることを承認するために使用されます。1 つの資格は、0、1、または複数のアクセスリクエストポリシーを持つことができます。ユーザーとユーザーグループは、資格に追加することができます。
- アクセスリクエストポリシーは、アクセスの種類の詳細と条件を含みます。例えば、アクセスの種類には、パスワードかセッションか（RDP セッション、SSH クライアント、その他のプロトコル）、時間制限、個人の説明責任（チェックイン後に変更）、その他の設定が含まれます。条件としては、承認者の数、時間帯、チケットシステム、理由コードなどが含まれます。アクセスリクエストポリシーは、1 つの資格にのみ関連付けることができます。
- アクセスリクエストポリシーは、リソースにスコープされます。スコープがアカウントに対して直接行われ、資産が暗黙的に関連づけられることがあります。または、スコープが資産に対して行われ、アクセスリクエストポリシーがアカウントを識別する場合もあります。

ユーザーとユーザーグループ

ユーザーは個人です。ユーザーには、資産、パーティション、アカウント、資格アクセスリクエストポリシーを管理するための管理者アクセス許可権限が割り当てられる場合があります。ユーザーには、権限許可管理者によって複数のアクセス許可セットが割り当てられる場合があります。管理権限の割り当てにおいては、職務分掌（SoD）の原則に従うことがベストプラクティスです。たとえば、資産管理者、セキュリティポリシー管理者、ユーザー管理者、監査人は、異なるユーザーに割り当てるべきです。

一般ユーザーは管理アクセス許可権限を持ちません。一般ユーザーは、アクセスのリクエスト、アクセスリクエストの承認、完了したアクセスリクエストのレビューを行うことができます。

ユーザーには、二要素認証を設定することができます。

詳細：ユーザーとユーザーグループ

- ユーザーとは、SPP にログインできる人のことです。ユーザーは、ローカルの ID プロバイダと関連付けることも、Microsoft Active Directory などの外部 ID ストアのディレ

クトリユーザーとすることもできます。ユーザーは、ユーザーグループ、パーティション、資格、およびリンクアカウントに関連付けることができます。

- ユーザーグループは、資格に追加できるユーザーのセットであり、一般的にロールに基づきます。ユーザーグループのアクセスは、資格のアクセスリクエストポリシーによって管理されます。ローカルユーザーグループとディレクトリユーザーグループの両方を SPP に追加することができます。
- ユーザーには、資産やセキュリティなどに関する管理アクセス許可権限を割り当てることができます。一般ユーザーは、管理アクセス許可権限を持たず、アクセスリクエストの承認など、他の職務を実行します。

検出

管理されていない資産とアカウントを検出し、必要に応じてそれらを管理下に置くことができます。検出ジョブは、資産とアカウントを検出するために構成することができます。

アクセスリクエストワークフロー

大まかに言えば、エンドユーザーまたはカスタム統合アプリケーションは、次のアクセスリクエストを送信できます：

- SPP によって管理される資格情報（パスワードまたは SSH キー）
- SPS が追加された SPP によって管理されている資産へのセッション（RDP、SSH、Telnet など）

アクセスリクエストはすぐに許可される場合もあれば、最初に承認プロセスを経由する必要がある場合もあります。

承認されると、資格情報またはセッションをチェックアウトして使用できます。セッションの場合、すべての接続は SPS を介してプロキシされ、記録されます。

資格情報またはセッションを使用した後、チェックインすることで、そのユーザーの使用が終了したことを示すことができます。アクセスリクエストポリシーは、再度チェックアウトする前にリクエストのレビューが必要とするように設定することができます。資格情報タイプのリクエストの場合、アクセスリクエストポリシーは資格情報を変更するように設定することもできます。

1.1.2 アプライアンスの仕様

SPP アプライアンスは、特権管理ソフトウェア SPP 用に特化されて構築されています。ハードウェア、オペレーティングシステム、およびソフトウェアの各レベルでシステムの安全性を確保するために強化されています。

次の表は、SPP 4000 アプライアンスの仕様と電力要件です：

表：4000 アプライアンスの特長と仕様

4000 アプライアンス	特長/仕様
プロセッサ	Intel Xeon 4310T 2.3 GHz
プロセッサ数	1
コア数/プロセッサ	10 コア (20 スレッド)
L2/L3 キャッシュ	15 MB キャッシュ
チップセット	Intel C621A Chipset
DIMMs	ECC DDR4-2667
RAM	64 GB
内部 HD コントローラ	LSI MegaRAID SAS 9361-4i Single
ディスク	4 x Seagate Exos 7E10 2TB SAS 512e
可用性	TPM 2.0, EEC Memory, Redundant PSU
I/O スロット	2x PCIe 4.0 x16 FHHL 1x PCIe 4.0 x16 HHHL
RAID	RAID10
NIC/LOM	Broadcom P210TP - 2 x 10G BASE-T Broadcom P210P - 2 x 10G SFP+
パワーサプライ	Redundant, 500W/600W, Auto Ranging (100v~240V), RoHS and REACH compliant
ファン	6 Supermicro FAN-0141L
シャーシ	1 U ラック
サイズ（HxWxD）	43 x 437.0 x 650.0 (mm) 1.7 x 17.2 x 25.6 (in)
重量	最大： 37 lbs（16.78 Kg）

次の表は、SPP 3000 アプライアンスの仕様と電力要件です：

表：3000 アプライアンスの特長と仕様

3000 アプライアンス	特長/仕様
プロセッサ	Intel Xeon E3-1275v6 3.8 GHz
プロセッサ数	1
コア数/プロセッサ	4 コア（8 スレッド）
L2/L3 キャッシュ	8MB L3 キャッシュ
チップセット	Intel C236 Chipset
DIMMs	Unbuffered ECC UDIMM DDR4 2400MHz
RAM	32 GB
内部 HD コントローラ	LSI MegaRAID SAS 9361-4i Single
ディスク	4 x Seagate 7E2000 2TB SAS 512E
可用性	TPM 2.0, EEC Memory, Redundant PSU
I/O スロット	x16 PCIe 3.0, x8 PCIe 3.0
RAID	RAID10
NIC/LOM	4 port - dual GbE LAN with Intel i210-AT
パワーサプライ	Redundant, 700W, Auto Ranging (100v~240V), ACPI compatible
ファン	1 Supermicro SNK-P0046P and 2 Micron 16GB 2666MHz 2R ECC Unb Z01B Dual Label
シャーシ	1 U ラック
サイズ（HxWxD）	43 x 437.0 x 597.0 (mm)
重量	最大：16.78 Kg

表：4000 および 3000 アプライアンスの電源

入力電圧	100-240 Vac
周波数	50-60Hz
消費電力	170.9（Watts）
BTU	583

SPP は、仮想アプライアンスやクラウドからも利用可能です。

詳細については、以下を参照してください。

- 仮想アプライアンスと Web 管理コンソールの使用
- クラウドデプロイの考慮事項

2　システム要件とバージョン

SPP を使用すると、管理対象アカウントおよびシステムのアクセスリクエスト、承認、レビューを管理することができます。

- Web クライアントは、エンドユーザー用のビューと管理者用のビューで構成されています。完全な機能を備えたクライアントは、認証されたユーザーのロール（役割）に基づいて、SPP のすべての機能を公開します。
- Web 管理コンソールは、仮想アプライアンスに接続するたびに表示され、初めての構成に使用されます。仮想環境をセットアップするときは、CPU、メモリの可用性、I/O サブシステム、ネットワークインフラストラクチャなどの構成を慎重に検討して、仮想レイヤーに必要なリソースが利用可能であることを確認してください。

システムが、これらのクライアントのハードウェアおよびソフトウェアの最小要件を満たしていることを確認してください。

SPS アプライアンスが SPP に関連付けられている場合、セッションの記録は SPS を介して処理されます。関連付けは、SPS から行います。関連付け手順と問題解決の詳細については、「Safeguard for Privileged Sessions（SPS）管理者ガイド」を参照してください。

帯域幅

オーバーヘッドを含む接続は、サイト間帯域が 10 メガビット/秒より速く、片方向遅延（one-way delay）が 500 ミリ秒未満であることが推奨されます。トラフィックシェーピングを使用する場合は、シェーピングプロファイルのポート 655 UDP に十分な帯域幅と優先度を許可する必要があります。これらの数値はガイドラインとして提供されているもので、その他の要因によってネットワークのチューニングが必要になる場合があります。これらの要因には、ジッター、パケットロス、応答時間、使用量、ネットワークの飽和などが含まれますが、これらに限定されるものではありません。さらにご質問がある場合は、ネットワーク管理チームにお問い合わせください。

2.1 Web クライアントのシステム要件

表：Web 要件

コンポーネント	要件
Web ブラウザー	デスクトップブラウザー： • Apple Safari 16.0 for desktop 以降 • Google Chrome 108 以降 • Microsoft Edge 108 以降 • Mozilla Firefox 108 以降 モバイルデバイスブラウザー： • Apple Safari Mobile 14.7 以降 • Google Chrome on Android 180 以降

2.2 Web 管理コンソールのシステム要件

表：Web kiosk 要件

コンポーネント	要件
Web 管理コンソール	デスクトップブラウザー： • Apple Safari 16.0 for desktop 以降 • Google Chrome 108 以降 • Microsoft Edge 108 以降 • Mozilla Firefox 108 以降

プラットフォームとバージョンは次の通りです：

- Microsoft Windows ライセンスで VM をライセンスする必要があります。MAK または KMS のいずれかの方法を使用することをお勧めします。ライセンスに関する具体的な質問は、弊社までお問い合わせください。
- サポート対象のハイパーバイザー：
    - Microsoft Hyper-V (VHDX) version 8 以降
    - VMware vSphere with vSphere Hypervisor (ESXi) version 6.5 以降
    - VMware Worksation version 13 以降

- 最小リソース：
  4 CPU、10GB RAM、500GB ディスク。仮想アプライアンスのデフォルトのデプロイでは、適切なリソースが提供されません。これらの最小リソースが満たされていることを確認してください。

2.3 サポート対象のプラットフォーム

SPP は、カスタムプラットフォームを含むさまざまなプラットフォームをサポートします。

SPP でテスト済みプラットフォーム

以下の表は、SPP の動作確認済みのプラットフォームとバージョンの一覧です。SPP には、追加の資産を追加することができます。資産を追加する際に特定のプラットフォームが表示されない場合は、**［資産］**ダイアログの**［管理］**タブで**［Other］**、**［Other Managed］**、**［Other Directory］**、**［Linux］**を使用してください。詳細については、「管理タブ（資産の追加）」を参照してください。

SPS にリンクされた SPP：セッションプラットフォーム

> ⚠ **注意： SPS を SPP に関連付ける場合、SPS と SPP のバージョンが完全に一致することを確認し、アップグレード中もバージョンを同期させておく必要があります。たとえば、SPS バージョン 6.6 には、SPP バージョン 6.6 のみを関連付けることができ、SPS をバージョン 6.7 にアップグレードする場合は、SPP も 6.7 にアップグレードする必要があります。**
>
> **Long Term Supported（LTS）と機能リリースを混在させないように注意してください。たとえば、SPS バージョン 6.0.1 を SPP バージョン 6.1 に関連付けないでください。**

SPP が SPS アプライアンスとリンクされている場合、次のプロトコルのいずれかを使用するプラットフォームがサポートされます。

- SPP 2.8 以前：RDP、SSH
- SPP 2.9 以降：RDP、SSH、Telnet

プラットフォームによっては、複数のプロトコルをサポートする場合があります。たとえば、Linux（または Linux のバリエーション）プラットフォームは、SSH プロトコルと Telnet プロトコルの両方をサポートします。

表：サポート対象のプラットフォーム：管理可能な資産

プラットフォーム名	テスト済みバージョン	SPP サポート	SPS アクセスサポート
ACF2 - Mainframe	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	○	○
ACF2 – Mainframe LDAP	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	○	-
Active Directory	Active Directory	○	-
AIX	AIX 7.1 AIX 7.2 AIX 7.3	○	○
Amazon Linux	Amazon Linux 2 Amazon Linux 2022 Amazon Linux Other	○	○
Amazon Web Services	Amazon Web Services 1	○	-
CentOS Linux	CentOS Linux 7 CentOS Linux 8	○	○
Check Point GAiA (SSH)	Check Point GAiA (SSH) R76 Check Point GAiA (SSH) R77 Check Point GAiA (SSH) R80.30	○	○
Cisco ASA	Cisco ASA 7.X Cisco ASA 8.X Cisco ASA 9.X	○	○
Cisco IOS (510)	Cisco IOS 12.X Cisco IOS 15.X Cisco IOS 16.X	○	○
Cisco ISE	Cisco ISE 2.7 Cisco ISE 3	○	-
Cisco ISE CLI	Cisco ISE CLI 2.7 Cisco ISE CLI 3	○	○
Cisco NX-OS	Cisco NX-OS 9.3(7) Cisco NX-OS 9.3(7a)	○	○
Debian GNU/Linux	Debian GNU/Linux 9 Debian GNU/Linux 10 Debian GNU/Linux 11	○	○
Dell iDRAC	Dell iDRAC 7 Dell iDRAC 8 Dell iDRAC 9	○	○
eDirectory LDAP	eDirectory LDAP 9.0	○	-
ESXi	ESXi 7.0 ESXi 8.0	○	-

プラットフォーム名	テスト済みバージョン	SPP サポート	SPS アクセスサポート
F5 Big-IP	F5 Big-IP 12.1.2 F5 Big-IP 13.0 F5 Big-IP 14.0 F5 Big-IP 15.0	○	○
Fedora	Fedora 36 Fedora 37	○	○
Fortinet FortiOS	Fortinet FortiOS 5.2 Fortinet FortiOS 5.6 Fortinet FortiOS 6.0 Fortinet FortiOS 6.2 Fortinet FortiOS 7.0	○	○
FreeBSD	FreeBSD 12 FreeBSD 13	○	○
HP iLO	HP iLO 2 HP iLO 3 HP iLO 4 HP iLO 5	○	○
HP iLO MP	HP iLO MP 2 HP iLO MP 3	○	○
HP-UX	HP-UX 11iv3 (B.11.31)	○	○
IBM i	IBM i 7.3 IBM i 7.4	○	○
Junos – Juniper Networks	Junos - Juniper Networks 19 Junos - Juniper Networks 20 Junos - Juniper Networks 21 Junos - Juniper Networks 22	○	○
LDAP	OpenLDAP 2.4	○	-
Linux		○	○
macOS	macOS 11 macOS 12 macOS 13	○	○
MongoDB	MongoDB 4.2 MongoDB 4.4 MongoDB 5.0 MongoDB 6.0	○	-
MySQL	MySQL 5.7 MySQL 8.0	○	-
Oracle	Oracle 19c Oracle 21c	○	-
Oracle Linux(OL)	Oracle Linux (OL) 7 Oracle Linux (OL) 8 Oracle Linux (OL) 9	○	○

プラットフォーム名	テスト済みバージョン	SPP サポート	SPS アクセスサポート
Other		-	-
Other Directory		○	-
Other Linux		○	-
Other Managed		○	-
PAN-OS	PAN-OS 9.1 PAN-OS 10.1 PAN-OS 10.2	○	○
PostgreSQL	PostgreSQL 11 PostgreSQL 12 PostgreSQL 13 PostgreSQL 14 PostgreSQL 15	○	-
RACF - Mainframe	RACF - Mainframe z/OS V2.1 Security Server zSeries RACF - Mainframe z/OS V2.2 Security Server zSeries RACF - Mainframe z/OS V2.3 Security Server zSeries	○	○
RACF - RACF - Mainframe LDAP	RACF - Mainframe LDAP z/OS V2.1 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.2 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.3 Security Server zSeries	○	-
Red Hat Enterprise Linux (RHEL)	Red Hat Enterprise Linux (RHEL) 7 Red Hat Enterprise Linux (RHEL) 8 Red Hat Enterprise Linux (RHEL) 9	○	○
Red Hat Directory Server	Red Hat Directory Server 11	○	-
SAP HANA	SAP HANA SAP HANA 2	○	-
SAP Netweaver Application Server	SAP Netweaver Application Server 7.3 SAP Netweaver Application Server 7.4 SAP Netweaver Application Server 7.5	○	-
Solaris	Solaris 10 Solaris 11.3 Solaris 11.4	○	○
SonicOS	SonicOS 6.5 SonicOS 7 SonicOSX 7	○	-
SonicWALL SMA or CMS	SonicWALL SMA or CMS 11.3.0	○	-

プラットフォーム名	テスト済みバージョン	SPP サポート	SPS アクセスサポート
SQL Server	SQL Server 2012 SQL Server 2014 SQL Server 2016 SQL Server 2017 SQL Server 2019 SQL Server 2022	○	-
SUSE Linux Enterprise Server (SLES)	SUSE Linux Enterprise Server (SLES) 12 SUSE Linux Enterprise Server (SLES) 15	○	○
Sybase (Adaptive Server Enterprise)	Sybase (Adaptive Server Enterprise) 15.7 Sybase (Adaptive Server Enterprise) 16 Sybase (Adaptive Server Enterprise) 17	○	-
Top Secret - Mainframe	Top Secret - Mainframe r14 zSeries Top Secret - Mainframe r15 zSeries Top Secret - Mainframe r16 zSeries	○	-
Top Secret – Mainframe LDAP	Top Secret - Mainframe LDAP r14 Top Secret - Mainframe LDAP r15 Top Secret - Mainframe LDAP r16	○	○
Ubuntu	Ubuntu 18.04 Ubuntu 22.04 LTS Ubuntu 22.10	○	○
Windows Desktop Windows Desktop (SSH) Windows Desktop (WinRM) Windows Server Windows Server (SSH) Windows Server (WinRM)	Windows (SSH) 10 Windows (SSH) 11 Windows (SSH) Server 2012 Windows (SSH) Server 2012 R2 Windows (SSH) Server 2016 Windows (SSH) Server 2019 Windows (SSH) Server 2022 Windows 10 Windows 11 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022	○	○

表：サポート対象のプラットフォーム：検索可能なディレクトリ

プラットフォーム名	プラットフォームバージョン
Microsoft Active Directory	Windows 2008+ DFL/FFL
LDAP	2.4

すべてのサポート対象プラットフォームについて、最新の更新を適用していることが前提です。サポート対象プラットフォームでパッチが適用されていないバージョンについては、ケースバイケースで調査および支援しますが、プラットフォームのアップグレードや SPP のカスタムプラットフォーム機能の利用が必要になる場合があります。

カスタムプラットフォーム

次のサンプルプラットフォームスクリプトが利用可能です：

- Custom HTTP
- Linux SSH
- Telnet
- TN3270 transports

詳細については、「カスタムプラットフォーム」および「カスタムプラットフォームスクリプトの作成」を参照してください。

サンプルのカスタムプラットフォームスクリプトとコマンドの詳細は、GitHub の Safeguard Custom Platform Homewiki から入手できます。

- コマンドラインリファレンス: https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Command-Reference
- カスタムプラットフォームスクリプトの記述: https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Writing-A-Custom-Platform-Script
- サンプルプラットフォームスクリプト: https://github.com/OneIdentity/SafeguardCustomPlatform/tree/master/SampleScripts

> **注意：サンプルスクリプトは情報提供のためにのみ提供されます。本番環境で使用する前に、更新、エラーチェック、テストが必要です。SPP は、値が文字列、ブーリアン、整数、パスワード（API スクリプトでは secret と呼ばれます）を含むプロパティの型と一致するかどうかをチェックします。SPP は、カスタムプラットフォームに入力された値の有効性やシステムへの影響をチェックすることはできません。**

2.4 ライセンス

ハードウェアアプライアンス

SPP ハードウェアアプライアンスには、パスワード管理モジュールが組み込まれていますが、機能を利用可能にするためには、有効なライセンスをインストールする必要があります。

モジュールをインストールすると、SPP はライセンス状態であると表示され、動作可能な状態になりますが、モジュールのライセンスがインストールされていない場合は、機能が制限されます。つまり、パスワード管理モジュールのライセンスがインストールされていない場合、アクセスリクエストを構成することはできても、パスワードのリリースをリクエストすることはできません。

バーチャルアプライアンス Microsoft Windows ライセンス

仮想アプライアンスに Microsoft Windows ライセンスを付与する必要があります。MAK または KMS のいずれかの方法を使用することをお勧めします。ライセンスに関する具体的なご質問は、お問い合わせください。仮想アプライアンスは、オペレーティングシステムが適切にライセンスされていない場合、機能しません。

ライセンスの設定と更新

初回ログイン時のライセンス情報登録

アプライアンス管理者として初めてログインすると、ライセンスを追加するよう要求されます。ライセンスが追加されると、成功ダイアログが表示されます。

仮想アプライアンスでは、ライセンスは初期セットアップの一部として追加されます。詳細については、「仮想アプライアンスのセットアップ」を参照してください。

> **重要：**ライセンスの追加に成功すると、Software Transaction Agreement（ソフトウェア取引契約）が表示されます。内容を確認し、SPP の利用を開始する場合は承諾してください。

ライセンス期限切れのリマインド設定

SPP の使用に支障が出ないように、アプライアンス管理者は SMTP サーバーを構成し、「ライセンスが失効しました（License Expired）」および「ライセンスがまもなく失効します（License Expiring Soon）」イベントタイプのメールテンプレートを定義する必要があります。これにより、有効期限が近づいていることが確実に通知されるようになります。詳細については、「メール通知の有効化」を参照してください。

「appliance is unlicensed（アプライアンスがライセンスされていない）」という通知を受けた場合、ユーザーはアプライアンス管理者に連絡するように指示されます。

アプライアンス管理者は、「license expiring（ライセンス期限切れ）」通知を受け取った場合、新しいライセンスを適用してください。

ライセンスファイルの更新

ライセンスの更新は、ハードウェアではなく仮想マシンを使用する場合のみ可能です。

ライセンスのアクティベート

ライセンスページに移動します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ライセンス］**の順に選択します。
    - 新しいライセンスファイルをアップロードするには、**［新しいライセンスファイルのアップロード］**をクリックし、**［参照］**でライセンスファイルを選択し

ます。Software Transaction Agreement（ソフトウェア取引契約）を確認し、承諾します。

- ライセンスファイルを削除するには、ライセンスを選択し、 **［選択したライセンスの削除］**をクリックします。

2.5 長期サポート（LTS）とフィーチャーリリース

リリースでは、次のバージョン表記を使用しています：

- 長期サポート（LTS）リリース：
  1 桁目がリリースを示し、2 桁目は 0 です（例：6.0 LTS）。
- メンテナンス LTS リリース：
  3 桁目の数字の後に LTS が付きます（例：6.0.6 LTS）。
- フィーチャーリリース：
  フィーチャーリリースのバージョン番号は 2 桁（例：6.6）です。

リリースを受け取るために、長期サポート（LTS）リリースまたはフィーチャーリリースの２つのパスを選択することができます。詳細については、次の表を参照してください。

表：長期サポート（LTS）とフィーチャーリリースの比較

	長期サポート（LTS）リリース	フィーチャーリリース
一般リリース	• **範囲**： 新機能、問題修正、セキュリティ更新を含む • **バージョン管理**： 1 桁目は LTS、 2 桁目は 0 （例：6.0 LTS、7.0 LTS など）	• **範囲**： 最新の機能、問題修正、OS のセキュリティパッチなどの他の更新を含む • **バージョン管理**： 1 桁目は LTS、2 桁目はフィーチャーリースの識別番号 （例：6.6、6.7 など）
メンテナンスリリース	• **範囲**： 重要な問題解決を含む • **バージョン管理**： ３桁目はメンテナンス LTS リリース（例：6.0.6 LTS）	• **範囲**： 非常に重大な解決済みの問題が含まれています。 • **バージョン管理**： ３桁目はメンテナンスフィーチャーリリース（例：6.6.1）

詳細情報については「Product Life Cycle」を参照してください。

> **注意：最新のフィーチャーリリースからダウングレードした場合、たとえ LTS リリースであったとしても、SPP のサポートは無効になります。**

One Identity 社は、使用するリリースパス（長期サポートパスまたはフィーチャーリリースパス）の最新リビジョンを、常にインストールすることを強くお勧めします。

LTS バージョンとフィーチャーリリースバージョン間の移行

LTS バージョン（たとえば、6.0.7 LTS）から同じフィーチャーバージョン（6.7）に移行してから、それ以降のフィーチャーバージョンにパッチを適用することができます。その後、パッチの最小バージョン（通常は 3 世代前）からパッチを適用することができます。LTS バージョンからフィーチャーバージョンに移行する場合、次の LTS リリースまでしかフィーチャーリリースを適用できないことを通知する次のような警告が表示されます。

Warning: You are patching to a Feature Release from an LTS Release. If you apply this update, you will not be able to upgrade to a non-Feature Release until the next LTS major release version is available. See the Administration Guide for details.

フィーチャーリリースから LTS リリースに移行することはできません。たとえば、6.7 から 6.0.7 LTS に移行することはできません。次の LTS リリースバージョンが公開されるまで、新しいフィーチャーリリースごとにアップグレードを続ける必要があります。この例では、7.0 LTS が使用可能になるまで待つことになります。

パッチ

メジャーバージョンからのパッチ適用のみ可能です。たとえば、バージョン 6.6 を使用していて、7.7 のパッチを適用したい場合は、7.0 LTS にパッチを適用してから 7.7 を適用する必要があります。

SPP の LTS メジャーバージョンは、同じ LTS メジャーバージョンの SPS とのみ動作します。最高のエクスペリエンスを得るには、サポートされる最新バージョンを使用することをお勧めします。

3 API の使用と PowerShell ツール

SPP には、使いやすいチュートリアルを備えた堅牢な API があります。Safeguard PowerShell を使用して、機能を自動化することができます。

API の使用
Safeguard PowerShell の使用

3.1 API の使用

SPP は、API ファーストの設計で構築されており、他のアプリケーションやシステムとの相互作用を可能にする REST アーキテクチャに基づく最新の API を使用しています。すべての機能は API を介して公開され、実行するアクションやアプリケーションがどの言語で書かれているかに関係なく、迅速かつ簡単に統合することができます。SPP API を介してのみ実行可能なものもいくつかあります。

> ⚠ **注意：** SPP 6.8 から、ASP.NET SignalR を使用してイベントを監視するカスタムソリューションを構築したユーザーは、ASP.NET Core SignalR へのアップグレードにより、ソリューションに変更を加える必要があります。この変更と 2 つのバージョン間のアップグレード方法の詳細については、Microsoft のドキュメントを参照してください。

> **メモ：** GitHub でホストされているオープンソースプロジェクト (SafeguardDotNet, SafeguardJava, safeguard-bash) の SPP 6.8 バージョンが ASP.NET Core SignalR サポートに更新され、SPP 6.8 の新しい SignalR 変更で動作するようになりました。

API チュートリアル

SPP API チュートリアルは、GitHub の次の場所で公開されています：
https://github.com/oneidentity/safeguard-api-tutorial

3.1.1 SPP API アクセス

SPP には、次の API カテゴリがあります：

- **Core：**
  ほとんどの製品機能はここにあります。クラスタ全体のすべての操作：アクセスリクエストワークフロー、資産管理、ポリシー管理など
  https://<Appliance IP>/service/core/swagger/
- **Appliance：**
  IP アドレスの設定、メンテナンス、バックアップ、サポートバンドル、アプライアンス管理などの RAppliance 固有の操作
  https://<Appliance IP>/service/appliance/swagger/
- **Notification**：
  匿名の認証されていない操作。このサービスは、アプライアンスが完全にオンラインでない場合でも利用できます。
  https://<Appliance IP>/service/notification/swagger/
- **Event**：
  リアルタイムイベント用に SignalR に接続するための専用エンドポイント
  https://<Appliance IP>/event/signalr
- **a2a**：
  アプリケーション統合固有の操作。パスワードと SSH キーの取得、ユーザーに代わってアクセスリクエストを行うなど
  https://<Appliance IP>/service/a2a/swagger

API のほとんどのリソースにアクセスするには、Bearer トークンを使用する必要があります。Swagger Web UI（上記 URL で参照）を使用する場合は、各ページの上部にある**［Authorize（認証）］**ボタンをクリックし、Web UI を使用してログインしてください。Swagger Web UI は、Bearer トークンを各 API リクエストに自動的に追加します。ただし、手動で API リクエストを行う場合や、独自のアプリケーション/スクリプトを作成する場合は、次の 2 つの手順を実行して Bearer トークンを取得します。

1. 最初に、OAuth 2.0 **リソース所有者のパスワード（または SSH キー）クレデンシャル**または**クライアントクレデンシャル**の付与タイプを使用して認証する必要があります。リソース所有者パスワードクレデンシャルの例は次のとおりです。

```
POST https://<ApplianceIP>/RSTS/oauth2/token
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json
        {
                "grant_type": "password",
                "username": "<Username>",
                "password": "<Password>",
                "scope": "rsts:sts:primaryproviderid:local"
        }
```

- grant_type は必須であり、password に設定する必要があります。
- username は必須であり、ログインするユーザーアカウントを設定します。
- password は必須あり、username に関連付けられたパスワードを設定します。
- scope は必要であり、使用可能な ID プロバイダのスコープ ID の 1 つを設定します。例に示されている値、rsts:sts:primaryproviderid:local は、すべての SPP アプライアンスで使用可能なデフォルト値です。SPP で直接作成したユーザーアカウント（つまり、Active Directory または LDAP アカウントではない）は、ほとんどの場合、このスコープ値を持ちます。

  > **メモ：** ID プロバイダのリストは動的であり、関連するスコープ ID は、次の要求を行うことによってのみ取得できます:
  >
  > https://<ApplianceIP>/service/core/v3/AuthenticationProviders
  >
  > そして、RstsProviderScope プロパティに対して返された JSON を解析します。

  クライアント証明書を使用して認証する場合は、OAuth 2.0 **Client Credentials** 付与タイプを使用する必要があります。この場合、証明書は SSL 接続のハンドシェイクの一部として含まれ、Authorization HTTP ヘッダーは無視されます。scope を rsts:sts:primaryproviderid:certificate またはクライアント証明書認証をサポートするその他の ID プロバイダに設定します。

```
POST https://<ApplianceIP>/RSTS/oauth2/token
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json
        {
            "grant_type": "client_credentials",
            "scope": "rsts:sts:primaryproviderid:certificate"
        }
```

2. 認証に成功すると、API にアクセスするためにユーザートークンと交換する必要がある access_token がレスポンスに含まれます。

```
POST https://<ApplianceIP>/service/core/v3/Token/LoginResponse
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json
        {
            "StsAccessToken": "<access_token from previous response>"
        }
```

これで、今後すべての API リクエストに使用する認証トークンができました。トークンは、Bearer トークンとして HTTP Authorization ヘッダーに含まれます。

Authorization: Bearer <UserToken value>

例：

```
GET https://<ApplianceIP>/service/core/v3/Users/-2
Host: <ApplianceIP>
Accept: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni...
```

メモ：トークンは、トークンが発行された時点で、SPP で構成されている**［トークンの有効期間］**の設定に従って期限切れになります。

3.1.2 API クエリパラメーターを用いた応答のカスタマイズ

次の API クエリパラメーターを使用して、API から返される応答をカスタマイズすることができます。

次の出力パラメーターで、含まれるプロパティ名と並べ替えに使用されるプロパティ名を定義できます。

表：API クエリフィルタリング：アウトプット

アウトプット	例	説明/メモ
fields	GET /Users?fields=FirstName,LastName	出力に含まれるプロパティ名のリスト
orderby	Get /AssetAccounts?orderby=-AssetName,Name	出力の並べ替えに使用されるプロパティ名のリスト。降順を暗示

次のページングパラメータでは、項目数、開始ページ、ページあたりの項目数を含めることができます。

表：API クエリフィルタリング：ページング

ページング	例	説明/メモ
count	GET /Assets?count=true	条件に一致する項目の総数を表す整数値で返すかどうかを True または False で指定します。
page & limit	GET /DirectoryAccounts?page=3&limit=100	page は、どのページのデータ（0 から始まる）を返すかを定義します。limit は、ページデータのサイズを定義します。

次の演算子を使用して、結果をフィルタリングできます。

表：API クエリフィルタリング：filter パラメーター

演算子	例	説明/メモ
eq	GET /AssetAccounts?filter=Name eq 'George'	equal to（等しい）
ne	GET /Users?filter=LastName ne 'Bailey'	not equal to（等しくない）
gt	GET /Assets?filter=Id gt 10	greater than（より大きい）

演算子	例	説明/メモ
ge	GET /Assets?filter=Id ge 10	greater than or equal to（以上）
lt	GET /Assets?filter=Id lt 10	less than（未満）
le	GET /Assets?filter=Id le 10	less than or equal to（以下）
and	GET /UserGroups?filter=(Id eq 1) and (Name eq 'Angels')	両方のオペランドが true を返します
or	GET /UserGroups?filter=(Id eq 1) or (Name eq 'Bedford')	少なくとも 1 つのオペランドが true を返します
not	GET /UserGroups?filter=(Id eq 1) and not (Name eq 'Potters')	結果から「not」値を除外して検索を絞り込みます
contains	GET /Users?filter=Description contains 'greedy'	単語またはフレーズが含まれています
q	GET /Users?q=bob	q は、テキストプロパティを横断的に検索するために使用できます。
in	GET /Users?filter=UserName in ['bob', 'sally', 'frank']	事前定義されたセットのプロパティ値

filter パラメーターを使用する場合、括弧（）を使用して論理式をグループ化できます。

例：
GET/Users?filter=(FirstName eq 'Sam' and LastName eq 'Smith') and not Disabled

filter パラメーターを使用する場合は、バックスラッシュ文字（\）を使用して、文字列内の引用符をエスケープします。例：Get/Users?filter=UserName contains '\''

3.2 Safeguard PowerShell の使用

PowerShell は、タスクベースのコマンドラインシェルとスクリプト言語で、オペレーティングシステムとプロセスを管理するタスクを自動化するために使用されます。SPP Powershell モジュールとスクリプトリソースは、GitHub の次の場所にあります：[OneIdentity/safeguard-ps]

インストレーション

SPP Powershell モジュールは、PowerShell ギャラリーに公開されており、組み込みの Import-Module コマンドレットを使用して簡単にインストールすることができます。最新の機能を取得するには、Update-Module コマンドレットを使用します。

デフォルトでは、Powershell モジュールはすべてのユーザーにインストールされます。すべてのユーザーにインストールするには、管理者として Powershell を実行する必要があります。

> Install-Module safeguard-ps

または、管理者の許可を必要としない -Scope パラメーターを使用してモジュールをインストールすることもできます:

> Install-Module safeguard-ps -Scope CurrentUser

4 仮想アプライアンスと Web 管理コンソールの使用

始める前に：プラットフォームとリソース

仮想環境をセットアップするときは、CPU、メモリの可用性、I/O サブシステム、ネットワークインフラストラクチャなどの構成面を慎重に検討して、仮想レイヤーに必要なリソースを確保できるようにしてください。環境の仮想化に関する詳細は、One Identity の製品サポートポリシーを参照してください。

仮想アプライアンスには、Microsoft Windows のライセンスが必要です。ライセンスに関してご質問がある場合は、お問い合わせください。

プラットフォームとバージョンは次のとおりです。

- Microsoft Windows ライセンスで VM をライセンスする必要があります。MAK または KMS のいずれかの方法を使用することをお勧めします。
- サポート対象のハイパーバイザー：
    - Microsoft Hyper-V (VHDX) version 8 以降
    - VMware vSphere Hypervisor (ESXi) version 6.5 以降
    - VMware Worksation version 13 以降
- 最小リソース：4 CPU、10GB RAM、500GB ディスク。仮想アプライアンスのデフォルトのデプロイでは、適切なリソースが提供されません。これらの最小リソースが満たされていることを確認してください。

利用可能なウィザード

アプライアンスのラッキングと初期構成を担当するアプライアンス管理者は、仮想アプライアンスを作成し、Safeguard Web 管理コンソールを起動して、次のウィザードのいずれかを選択します。

- **初期セットアップ**：
  名前、OS ライセンス、ネットワークなど、仮想アプライアンスの初期設定を行うために使用します。詳細については、「仮想アプライアンスのセットアップ」を参照してください。

- **セットアップ**：
  初期セットアップ後、SPP の更新やネットワークの変更は、Web 管理コンソールから**［セットアップ］**をクリックして行うことができます。
- **サポートキオスク**：
  サポートキオスクは、SPP の問題を診断し解決するために使用されます。キオスクにアクセスできるすべてのユーザーは、アプライアンスの再起動またはシャットダウン、サポートバンドル作成など、リスクの低いサポート操作を実行できます。管理者パスワードをリセットするには、ユーザーは One Identity サポートからチャレンジレスポンストークンを取得する必要があります。詳細については、「サポートキオスク」を参照してください。

セキュリティ

> **注意：強化されたアプライアンスがない場合にセキュリティを最大限に高めるには、Safeguard 仮想ディスク、Web 管理コンソール、MGMT インターフェイスへのアクセスをできるだけ少数のユーザーに制限することです。管理 Web キオスクは、サポートバンドルの取得やアプライアンスの再起動など、認証なしの機能へのアクセスが可能です。**

セキュリティに関する推奨事項は次のとおりです。

- X0 はパブリック API をホストしており、仮想マシンの設定ではネットワークアダプター1 になっています。これを内部ネットワークに接続します。
- MGMT は Web 管理コンソールをホストし、仮想マシンの設定ではネットワークアダプター2 になっています。このインターフェイスの IP アドレスは常に 192.168.1.105 です。これを管理者のみがアクセスできる制限付きのプライベートなネットワークに接続するか、ネットワークから切断して、アプライアンスの再起動やシャットダウンなどの認証されていないアクションを制限します。Web 管理コンソールは、VMware コンソールからも利用できます。

セットアップが完了したら、**［サポートキオスク］**>**［アプライアンス情報］**>**［ネットワーク（X0）］と［管理（MGMT）］**にある MAC アドレス情報を参照して、どの NIC が MGMT と X0 であるかを確認できます。詳細については、「サポートキオスク」を参照してください。

バックアップ：仮想アプライアンスとハードウェアアプライアンス

Safeguard ハードウェアアプライアンスのセキュリティポスチャ（セキュリティ体制）を保護するため、Safeguard ハードウェアアプライアンスを Safeguard 仮想アプライアンスとクラスタ化することはできません。ハードウェアアプライアンスから取得したバックアップを仮想アプライアンスで復元することはできず、仮想アプライアンスから取得したバックアップをハードウェアアプライアンスで復元することはできません。

詳細については、「仮想アプライアンスのバックアップと復元」を参照してください。

アップロードとダウンロード

192.168.1.105 で Web 管理コンソールが稼働しています。仮想ディスプレイを介して仮想アプライアンスに接続すると、Web 管理コンソールが自動的に表示されますが、この方法で接続すると、アップロードおよびダウンロード機能は無効になります。

仮想マシンインフラストラクチャのネットワークを構成して、デスクトップから https://192.168.1.105 にプロキシできるようにすることもできます。この方法で接続すると、Web 管理コンソールからのアップロードとダウンロードが可能になります。

> ⚠ **注意：クローン作成とスナップショットはサポートされていませんので、使用しないでください。クローンを作成する代わりに、新しい VM をデプロイして初期セットアップを実行してください。スナップショットの代わりに、仮想アプライアンスのバックアップを取得してください。SPP のバックアップと復元機能のみがサポートされています（「仮想アプライアンスのバックアップと復元」）。**

VM の移行

VMware VMotion は、ある物理サーバーから別の物理サーバーへの仮想マシンのライブマイグレーションに使用することができます。

4.1 仮想アプライアンスのセットアップ

アプライアンス管理者は、初期セットアップウィザードを使用して、仮想アプライアンスに一意の ID を付与し、基盤となるオペレーティングシステムのライセンスを取得し、ネットワークを構成します。初期セットアップウィザードは、仮想アプライアンスが最初にデプロイされた後に 1 回だけ実行する必要がありますが、将来再度実行することもできます。将来実行しても、アプライアンス ID は変更されません。

セットアップが完了すると、アプライアンス管理者はアプライアンス名、ライセンス、およびネットワーク情報を変更できますが、アプライアンス ID（ApplianceID）を変更することはできません。アプライアンスは、一意の ID を持つ必要があります。

アプライアンス管理者が仮想アプライアンスを初期セットアップする手順は、次のとおりです：

手順 1：十分なリソースを用意する

仮想アプライアンスのデフォルトのデプロイでは、適切なリソースが提供されません。最低限必要なリソースは、次の通りです： 4 CPU、10 GB RAM、500GB ディスク。十分なディスク容量がない場合パッチは失敗します。ディスク容量を拡張してからパッチを再アップロードする必要があります。

手順 2：仮想マシン（VM）をデプロイする

仮想マシン（VM）を仮想インフラストラクチャにデプロイします。仮想アプライアンスは **InitialSetupRequired** 状態です。

Hyper-V zip ファイルのインポートとセットアップ手順

Hyper-V を使用する場合、仮想アプライアンスをセットアップするには、Safeguard Hyper-V zip ファイルが必要になります。次の手順で、ファイルを展開してインポートします。

1. Safeguard-hyperv-prod ... zip ファイルを展開します。
2. **［操作］＞［仮想マシンのインポート］**を選択します。
3. **［次へ］**をクリックします。
4. **［フォルダーの検索］**で**［参照...］**ボタンをクリックし、インポートする仮想マシンを含むフォルダーを指定します。
5. **［次へ］**をクリックします。
6. **［仮想マシンの選択］**で Safeguard-hyperv-prod... を選択します。
7. **［次へ］**をクリックします。
8. **［インポートの種類の選択］**で**［仮想マシンをコピーする(新しい一意な ID を作成する)］**を選択します。
9. **［次へ］**をクリックします。
10. **［移動先の選択］**で**［仮想マシンの構成フォルダー］**、**［チェックポイントストア］**、**［スマートページングフォルダー］**の場所を指定します。
11. **［次へ］**をクリックします。
12. **［保存するフォルダーを選択します］**でインポートした仮想ハードディスクのこの仮想マシンでの保存場所を指定します。

13. **［次へ］**をクリックします。

14. **［要約］**ページの内容を確認し、**［完了］**をクリックします。

15. **［設定...］＞［ハードウェアの追加］**で、Safeguard の MGMT および X0 ネットワークアダプターに接続します。

16. Safeguard-hyperv-prod... を右クリックして**［接続...］**をクリックして構成を完了し、起動します。

手順 3：初回アクセス

次のいずれかの方法でアクセスを開始します。

- 仮想ディスプレイ経由：
  仮想マシンの仮想ディスプレイに接続します。このアクセス方法では、パッチを適用する機会は提供されません。仮想ディスプレイからは、アップロードとダウンロードはできません。手順 4 へ進みます。Hyper-V を使用している場合、ディスプレイの拡張セッションモードが無効になっていることを確認します。詳細については、Hyper-V のドキュメントを参照してください。
- ブラウザー経由：
  ワークステーションから仮想アプライアンスの https://192.168.1.105 をアクセス可能なアドレスにプロキシするように仮想インフラのネットワークを構成し、そのアドレスにブラウザーを開きます。この方法については、仮想インフラストラクチャ（例：VMWare）のドキュメントを参照してください。このアクセス方法では、パッチを適用する機会が提供されます。アップロードとダウンロードは、ブラウザーから行うことができます。手順 4 へ進みます。

  > **重要：** OVA をインポートした後、VM の電源を入れる前に、VM に USB コントローラがないことを確認してください。USB コントローラがある場合は、それを取り外してください。

手順 4：初期設定の完了

［初期セットアップの開始］をクリックします。この作業が完了すると、アプライアンスはオンライン状態で再開します。

手順 5：SPP のログインと設定

1. パッチを適用する場合は、リソースを確認し、必要に応じてディスク容量を拡張してください。最小リソースは、4CPU、10GB RAM、500GB ディスクです。

2. ログインするには、**Bootstrap Administrator** の次のデフォルトの資格情報を入力し、**［Log in］**をクリックします。
    - User Name: admin
    - Password: Admin123

3. https://192.168.1.105 経由で接続されたブラウザーを使用している場合、**［初期セットアップ］**ペインは、現在の SPP バージョンを識別し、パッチを適用する機会を提供します。**［パッチのアップロード］**をクリックしてパッチを現在の SPP バージョンにアップロードするか、**［スキップ］**をクリックします。（これは、Safeguard Virtual Kiosk 仮想ディスプレイを使用している場合は使用できません。）

4. Web 管理コンソールの **［初期セットアップ］**ペインで、次のように入力します。

    a. **アプライアンス名**：　仮想アプライアンスの名前を入力します。

    b. **Host DNS Suffix：**　ホストの DNS サフィックスを入力します。

    c. **Windows ライセンス**：　次のオプションのいずれかを選択します。
        - **KMS サーバーの使用：**
          このフィールドを空白のままにすると、SPP は DNS を使用して KMS サーバーを自動的に検索します。KMS サーバーを見つけるには、DNS サフィックスでドメイン名を定義しておく必要があります。KMS が DNS に登録されていない場合は、KMS サーバーのネットワーク IP アドレスを入力します。
        - **製品キーの使用**：
          選択した場合、組織の Microsoft アクティベーションキーを追加するために必要な検証のために、アプライアンスをインターネットに接続する必要があります。

    d. **NTP**：ネットワークタイムプロトコル（NTP）の構成を完了します。
        - **［NTP の有効化］**を選択して、プロトコルを有効にします。
        - **［プライマリ NTP サーバー］**の IP アドレスと、オプションで**［セカンダリ NTP サーバー］**の IP アドレスを指定します。

e. **ネットワーク (X0)：**X0（パブリック）インターフェイスの場合、IPv4 および/または IPv6 情報と **DNS サーバー**の情報を入力します。ディレクトリまたはネットワークスキャンは IPv4 でサポートされます（IPv6 はサポートされません）。

5. **［保存］**をクリックします。仮想アプライアンスは、SPP、ネットワークアダプター、およびオペレーティングシステムのライセンスを構成するときに進行状況情報を表示します。

6. 「メンテナンスは完了しています」というメッセージが表示されたら、**［続行］**をクリックします。

手順 6： Web クライアントの使用

ブラウザーから X0（パブリック）インターフェイスの仮想アプライアンス IP アドレスに移動できます。

手順 7：Bootstrap Administrator のパスワードの変更

セキュリティ上の理由から、Bootstrap Administrator ユーザーのパスワードを変更してください。詳細については、「ローカルユーザーのパスワード設定」を参照してください。

手順 8：クラスタ後、信頼できるサーバー、CORS、リダイレクト設定の変更

ベストプラクティスとして、SPP のクラスタを作成した後（または単一の仮想マシンを使用するだけの場合）、信頼できるサーバー、CORS、リダイレクト設定を空の文字列または値のリストに変更し、許可したいアプリケーションを統合してください。詳細については、「信頼できるサーバー、CORS、リダイレクト」を参照してください。

仮想アプライアンス設定の閲覧と変更

仮想アプライアンスの設定を閲覧または変更できます。

- Web 管理コンソールで **［ホーム］**をクリックすると、仮想アプライアンスの名前、ライセンス、ネットワーク情報が表示されます。
- 最初のセットアップ後、**［セットアップ］**をクリックして、Web 管理コンソールから SPP の更新とネットワークの変更を行うことができます。

4.2　仮想アプライアンスのバックアップと復元

次の情報を使用して、SPP 仮想アプライアンスをバックアップおよび復元します。仮想アプライアンスの場合、工場出荷時リセットオプションはありません。仮想アプライアンスを工場出荷時リセットするには、アプライアンスを再デプロイしてください。

仮想アプライアンスのバックアップ

ハードウェアアプライアンスのセキュリティを確保するため、ハードウェアアプライアンスから取得したバックアップを仮想アプライアンスに復元することはできません。仮想アプライアンスから取得したバックアップをハードウェアアプライアンスに復元することもできません。

詳細については、「バックアップと復元」をしてください。

仮想アプライアンスのリカバリー

SPP 仮想アプライアンスは、次のリカバリー手順を使用してリセットされます。

オンプレ仮想アプライアンス（例：Hyper-V、VMware）

1. 仮想アプライアンスを再デプロイし、**［初期セットアップ］**を実行します。詳細については、「仮想アプライアンスのセットアップ」を参照してください。
2. バックアップを復元します。詳細については、「バックアップと復元」を参照してください。

クラウド仮想アプライアンス（例：AWS、Azure）

1. 以下の手順をにて再デプロイします。
    - AWS：詳細については、「AWS デプロイ」を参照してください。
    - Azure：詳細については、「Azure デプロイ」を参照してください。

4.3　サポートキオスク

接続が失われた、または障害が発生した Hyper-V または VMware 仮想アプライアンスをトリアージするアプライアンス管理者は、仮想アプライアンスが隔離されている場合でもサポートキオ

スクを使用することができます。詳細については、「アプライアンスが隔離された場合の対処法は？」を参照してください。

ターミナル設定は、90 x 45 以上にすることをお勧めします。これより小さい設定にすると、次のようなエラーが発生することがあります。Screen dimension to small.（画面寸法が小さすぎます）。

Windows キオスクを使用する場合、コピー＆ペーストはできません。Hyper-V では、キーボードからのテキスト入力を自動化することができ、ESX では、API コール PutUsbScanCodes()を使用してキー入力をエミュレートすることができる場合があります。

1. Web 管理コンソールで、**［サポートキオスク］**をクリックします。

2. 次のアクティビティのいずれかを選択します。

   - **アプリケーション情報**
     これは読み取り専用です。ネットワーク情報を変更するには、セットアップを再実行します。

   - **電源オプション**
     仮想アプライアンスを再起動またはシャットダウンできます。

     a. 仮想アプライアンスを再起動またはシャットダウンする理由を入力します。

     b. **［再起動］**または**［シャットダウン］**をクリックします。

   - **管理者パスワードがリセットされました**
     Bootstrap Administrator は、アプライアンスを初めて稼働させるための組み込みアカウントです。デフォルトの資格情報（admin/Admin123）は、SPP の構成後にを変更する必要があります。パスワードを紛失した場合は、以下のチャレンジレスポンスプロセスを使用してデフォルトにリセットできます。

     チャレンジレスポンスプロセス

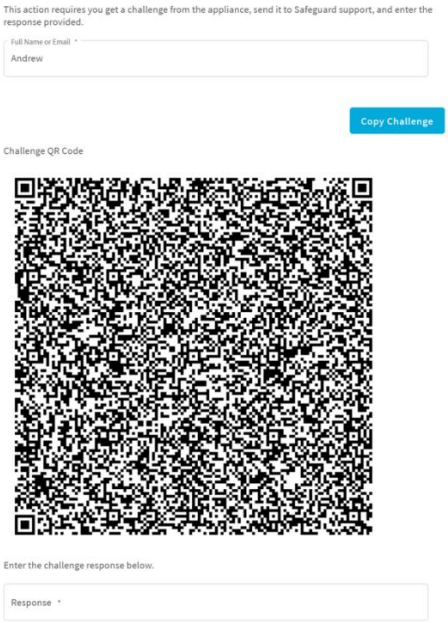
     a. **［フルネームまたはメール］**に、チャレンジの質問を受信するための名前またはメールを入力します。

     b. **［チャレンジの取得］**をクリックします。

     c. チャレンジレスポンスを取得するには、次のいずれかを実行します（次の図を参照）。

        - **［チャレンジをコピー］**をクリックします。チャレンジがクリップボードにコピーされます。そのチャレンジを Safeguard サポートに送信します。サポートは 48 時間有効なチャレンジレスポンスを返送します。画面を更新しないでください。

- QR コードをスクリーンショットし、サポートに送信します。サポートは、48 時間有効なチャレンジレスポンスを返送します。チャレンジレスポンス操作中は、ページを移動したり、更新したりしないでください。これを行うと、チャレンジレスポンスが無効となり、処理を再開する必要があります。
- 携帯電話の QR コードリーダーを使用して、チャレンジレスポンスを取得します。



d. レスポンスが受理されたら、**[パスワードのリセット]** をクリックします。操作が完了すると、**admin** アカウントのパスワードはデフォルトの **Admin123** に戻ります。

- **Support Bundle**（サポートバンドル）
サポートバンドルには、問題を分析および診断するために One Identity サポートに送信されるシステムおよび設定情報が含まれています。サポートバンドルをダウンロードするか、既に設定した Windows 共有場所に保存することができます。サポートバンドルを生成するには：

a. オペレーティングシステムのイベントを含める場合は、**[イベントログを含める]** を選択します。サポートから要求がない限り、サポートバンドルの生成にかなり時間がかかるため、これをオフのままにしておくことをお勧めします。

b. 次のいずれかの方法を使用して、サポートバンドルを作成します。

- ディスプレイではなくブラウザーを介して接続している場合は、**[ダウンロード]** をクリックし、ダウンロード先に移動して、**[OK]** をクリックします。

- バンドルを共有にコピーする場合は：

  i. **［UNC パス］**、**［ユーザー名］**、および**［パスワード］**を入力します。

  ii. 必要に応じて、**［イベントログを含める］**を選択します。

  iii. **［共有にコピー］**をクリックします。
  プログレスバーが表示されます。

- **診断パッケージ**

アプライアンス管理者は、信頼できる安全なアプライアンス診断パッケージを実行することで、構成、同期、クラスタリングに関する問題や、その他の内部課題の解決を支援することができます。アプライアンス診断パッケージは、シリアルキオスク（リカバリーキオスク）ではなく、Web サポートキオスクから利用できます。アプライアンス診断パッケージは、アプライアンスが隔離された状態でも使用できます。外部の脅威から保護するために、Safeguard は不正なアプライアンス診断パッケージを拒否します。アプライアンス診断パッケージのマニフェストファイルには、SPP の最小バージョン、アプライアンス ID、有効期限のタイムスタンプ UTC などの基準が記載されています。新しい製品コードとデータベースの変更は、アプライアンス診断パッケージに含まれません。

a. 初めてロードする場合は、**［アップロード］**をクリックし、拡張子が.sgd のファイルを選択して、**［開く］**をクリックします。

   - アップロード条件が満たされていない場合、アプライアンス診断パッケージはアップロードされず、次のようなメッセージが表示されます：The minimum Safeguard version needed to run this diagnostic package is <version>.（この診断パッケージを実行するために必要な Safeguard の最小バージョンは<version>です。）

   - アップロードが成功すると、診断パッケージ情報が**［Staged］**というステータスで表示されます。**［実行］**を選択し、ステータスが**［完了］**に変わるまで待ちます。

b. アップロードすると、次のことができます：

   - **［ログのダウンロード］**を選択して、ログファイルを保存します。監査ログエントリは、実行中および実行後にアクティビティセンターから利用でき、アプライアンス履歴の一部となります。

- 有効期限が過ぎていない場合は、**［実行］**を選択して、アプライアンス診断パッケージを再度実行することができます。
- **［削除］**を選択すると、アプライアンス診断パッケージと関連するログファイルが削除され、実行中のアプライアンス診断パッケージが停止されます。別のアプライアンス診断パッケージをアップロードする前に、アプライアンスごとに 1 つのアプライアンス診断パッケージしか存在できないため、現在のパッケージを削除する必要があります。

5　クラウドデプロイの考慮事項

SPP はクラウドから実行することができます。

始める前に：プラットフォームとリソース

仮想環境をセットアップするときは、CPU、メモリの可用性、I/O サブシステム、ネットワークインフラストラクチャなどの構成面を慎重に検討し、仮想レイヤーに必要なリソースが利用可能であることを確認してください。環境の仮想化に関する詳細については、One Identity の製品サポートポリシーを参照してください。

クラウドデプロイでテストされたプラットフォームは次のとおりです：

- AWS 仮想マシン（VM）：詳細については、「AWS デプロイ」を参照してください。
- Azure 仮想マシン（VM）：詳細については、「Azure デプロイ」を参照してください。

これらのデプロイの場合、テストで使用される最小リソースは、4CPU、10GB RAM、60GB ディスクです。適切なマシンと構成テンプレートを選択します。たとえば、Azure Marketplace で**［Create］**（作成）をクリックすると、既定のプロファイルが表示されます。**［Change size］**（サイズの変更）をクリックして、別のテンプレートを選択することができます。

クラウドデプロイのための Web 管理キオスクへのアクセス制限

Web 管理キオスクは、AWS と Azure のポート 9337 で実行され、アプライアンス管理者による診断とトラブルシューティングを目的としています。

> ⚠ **注意：管理 Web キオスクは、クラウドプラットフォーム（AWS および Azure を含む）の HTTPS ポート 9337 を経由して利用できます。管理 Web キオスクでは、サポートバンドルの取得やアプライアンスの再起動など、認証なしで機能にアクセスできます。AWS では、明示的に許可されていない限り、すべてのポートが拒否されます。ポート 9337 へのアクセスを拒否するには、そのポートをファイアウォールルールから除外する必要があります。ポートを使用する場合、ファイアウォールルールは対象となるユーザーへのアクセスを許可する必要があります。**

Azure: port 9337 のブロック手順

次の手順で、Azure のポート 9337 へのアクセスをブロックします。

1. SPP を実行している仮想マシンに移動します。

2. 左側のナビゲーションメニューで、**[Networking]**（ネットワーク）を選択します。

3. **[Add inbound port rule]**（受信ポートルールの追加）をクリックします。

4. インバウンドセキュリティルール（inbound security rule）を次のように構成します。

   Source: Any
   Source port ranges: *
   Destination: Any
   Destination port ranges: 9337
   Protocol: Any
   Action: Deny
   Priority: 100 (use the lowest priority for this rule)
   Name: DenyPort9337

5. **[Add]**（追加）をクリックします。

AWS: port 9337 のブロック手順

次の手順で、AWS のポート 9337 へのアクセスをブロックします。

1. EC2 ダッシュボードから、SPP を実行している EC2 インスタンスに移動します。

2. インスタンスを選択します。

3. **[Description]**（説明）タブで、**[Security groups]**（セキュリティグループ）フィールドを見つけて、セキュリティグループの名前をクリックします。

4. **[Inbound]**（インバウンド）タブを選択します。

5. **[Edit]**（編集）をクリックします。

6. 既存のルールをすべて削除し、次のルールを追加します。

   - Type: Custom UDP Rule
     Protocol: UDP
     Port Range: 655
     Source: Anywhere
     Description: Cluster VPN
   - Type: HTTPS
     Protocol: TCP
     Port range: 443
     Source: Anywhere
     Description: Web API
   - Type: Custom TCP Rule
     Protocol: TCP
     Port Range: 8649
     Source: Anywhere
     Description: SPS Cluster

7. **[Save]**（保存）をクリックします。

5.1 AWS デプロイ

> **重要：**デプロイの前に、「クラウドデプロイの考慮事項」を確認してください。

SPP は、Amazon Web Services（AWS）を使用してクラウド上で実行することができます。

AWS から SPP の Amazon Machine Image（AMI）をデプロイするには、SPP の AWS マーケットプレイスリスト（こちら）にアクセスし、「デプロイ手順」に従います。

ディスクサイズに関する考慮事項

> ⚠ **注意：ディスクサイズを変更する前に、VM をシャットダウンしてください（停止して割り当て解除）。**

SPP は、最小限の OS ディスクサイズでデプロイされます。推定使用量と予算に応じて、OS ディスクのサイズを増やす必要があります。ハードウェア上の SPP には、1TB のディスクが付属しています。予想される資産数、アカウント数、1 日のユーザー数に応じて、これより多くても少なくても構いません。500GB が最小、2TB が最大です。

ディスクサイズは、Amazon Elastic Compute Cloud（Amazon EC2）を介して処理できます。詳細については、「Amazon EC2 の開始方法」を参照してください。VM を起動すると、SPP は自動的に OS ディスクボリュームのサイズを変更して、利用可能なスペースを使用します。

AWS のセキュリティに関する考慮事項

AWS で SPP を実行する場合、ハードウェアアプライアンスには適用されないセキュリティ上の考慮事項があります。

- SPP にパブリック IP アドレスを設定しない。
- AWS キーボールトを使用してディスクを暗号化する。
- AWS 内のアクセスを SPP 仮想マシンに限定する。
  AWS の SPP は、ハードウェアアプライアンスと同じように不正な管理者から保護することはできません。

静的 IP アドレスが必要

AWS で SPP の VM を静的 IP アドレスで構成します。AWS では、VM のデプロイ後に IP アドレスが変更されないようにする必要があります。IP アドレスを変更する必要がある場合は、バックアップを取り、再度デプロイして、バックアップを復元してください。IP アドレスの構成で既存

の仮想 NIC をピックアップするように、VM のデプロイをスクリプト化することができます。詳細については、Amazon Virtual Private Cloud（VPC）ドキュメントを参照してください。

デプロイメント手順

AWS は、AWS KMS を使用してデプロイ中に自動的にオペレーティングシステムのライセンスを取得します。

大規模なデプロイメントでは、より大きなサイジングの選択が保証されます。SPP のハードウェアアプライアンスは、32GB RAM と 4 プロセッサ、少なくとも 1TB のディスクスペースを備えています。

AWS マーケットプレイスの手順

1. SPP の AWS マーケットプレイスリスト（こちら）にアクセスします。
2. **［One Identity Safeguard for Privileged Passwords］**ページで、**［Continue to Subscribe］**をクリックします。
3. リソース作成画面に進み、インスタンスを構成します。ディスクサイズ、AWS セキュリティ、静的 IP アドレスに加え、One Identity は **m4.2xlarge** インスタンスタイプを選択することを推奨しています。
4. インスタンスの構成が完了したら、インスタンスの起動を選択します。

   > **メモ：**インスタンスの起動プロセスは完了までに時間がかかる場合があります。

5. インスタンスの起動が完了したら、静的 IP アドレスを使用して Web クライアントにログインします。デフォルトのユーザー名（admin）とパスワード（<instance id>）を使用する必要があります。admin のパスワードはすぐに変更してください。詳細については、「ローカルユーザーのパスワード設定」を参照してください。

   > **メモ：**パスワードはデプロイメントごとに一意であり、初期パスワードは常にデプロイメントのインスタンス ID になります。

クラウド仮想アプライアンスの設定の表示または変更

仮想アプライアンスの設定を表示または変更することができます。

診断とトラブルシューティングのために、ポート 9337 の SPP Web 管理キオスクを使用することができます。

また、AWS 経由でシステムログを確認することもできます。

1. AWS からシステムログを表示するには、**［Actions］> ［Instance Settings］> ［Get SystemLog］**の順に選択します。

2. https://<your IP>:9337 からログインします。

新しいバージョンにパッチを適用するには、API を使用します。

5.2 Azure デプロイ

> **重要：**デプロイの前に、「クラウドデプロイの考慮事項」を確認してください。

SPP は、Azure を使用してクラウド上で実行することができます。SPP のバージョンは Azure Marketplace で入手でき、Azure 仮想マシン（VM）が必要です。VM のセットアップ詳細については、「Azure での仮想マシン」を参照してください。

Azure を使用する場合、SPP は HTTPS X0 で使用できます。Azure のデプロイでは、MGMT サービスは使用されません。リカバリ（シリアル）キオスクは、アプライアンス情報の表示、管理者パスワードのリセット、電源の再起動またはシャットダウン、およびサポートバンドルの生成に使用します。詳細については、「リカバリキオスク（シリアルキオスク）」を参照してください。

ディスクサイズに関する考慮事項

SPP は、最小限の OS ディスクサイズでデプロイされます。推定使用量と予算に応じて、OS ディスクのサイズを増やす必要があります。ハードウェア上の SPP には、1TB のディスクが付属しています。想定する資産数、アカウント数、1 日あたりのユーザー数に応じて、これより多くても少なくでも構いません。500GB が最小、2TB が最大です。

1. SPP をデプロイします。

2. ログインできることを確認します。

3. VM をシャットダウンします（停止して割り当てを解除します）。

4. ディスクサイズを増やすための Microsoft のガイダンス「Windows 仮想マシンに接続されている仮想ハード ディスクを拡張する方法」に従ってください。

VM を起動すると、SPP は OS ディスクボリュームのサイズを自動的に変更して、使用可能なスペースを使用します。

Azure のセキュリティに関する考慮事項

Azure で SPP を実行する場合、ハードウェアアプライアンスには適用されないセキュリティ上の考慮事項があります：

- SPP にパブリック IP アドレスを設定しない。
- Azure キーボールトを使用してディスクを暗号化する。
- Azure 内のアクセスを SPP 仮想マシンに制限する。
  Azure の SPP は、ハードウェアアプライアンスと同じように不正な管理者から保護することはできません。

静的 IP アドレスが必要

Azure で SPP の VM を静的 IP アドレスで構成します。Azure では、VM のデプロイ後に IP アドレスを変更してはいけません。IP アドレスを変更する必要がある場合は、バックアップを取り、再度デプロイして、バックアップを復元してください。VM デプロイをスクリプト化することで、既存の仮想 NIC を IP アドレス構成で取得することができます。詳細については、Microsoft の Virtual Network のドキュメントを参照してください。

デプロイメント手順

SPP は、Azure Marketplace からデプロイされます。Azure は、Azure KMS を使用して、デプロイ中にオペレーティングシステムのライセンスを自動的に取得します。

Azure ベースイメージには、Microsoft のガイダンス「Azure にアップロードする Windows VHD または VHDX を準備する」に従って Azure にデプロイするために必要な構成が含まれています。

1. Azure ポータルにログインします。
2. **［Azure services］**で、**［Create a resource］**をクリックします。
3. “One Identity Safeguard for Privileged Passwords” を検索し、タイルをクリックします。
4. One Identity Safeguard for Privileged Passwords 画面で、**［Create］**をクリックします。
5. リソース作成画面を進めます。考慮事項は次のとおりです：
   - 小規模なデプロイの場合は、少なくとも VM サイズ Standard D2s v3 を選択することをお勧めします。大規模なデプロイの場合は、より大きなサイズを選択する必要があります。Safeguard ハードウェアアプライアンスには、32GB RAM と 4 プロセッサ、少なくとも 1TB のディスクスペースがあります。

- イメージの作成時に管理者ユーザー名とパスワードを設定する必要がありますが、SPP は初期設定時にこのアカウントを無効にします。
- public inbound ports を**［None］**に設定します。
- Windows ライセンスオプションを選択します。
- ブート診断とシリアルキオスクを必ず有効にしてください。Azure シリアルコンソールは、Safeguard Recovery Kiosk へのアクセスを提供するために使用されます。

6. VM の構成が完了したら、**［Create］**をクリックします。Azure が SPP 仮想マシンをデプロイします。

7. 仮想マシンのデプロイが完了すると、SPP は最初の使用のために自動的に初期化を開始します。これは、VM のサイズにもよりますが、通常 5～30 分ほどかかります。初期化中、SPP はファイアウォールを有効にし、VM へのリモートアクセスを無効にします。初期化の進行状況は、Azure シリアルコンソールから監視することができます。初期化中は、VM にログインしたり、VM の電源を切ったり再起動したりしないでください。

8. 初期化が完了すると、Azure シリアルコンソール画面に Safeguard Recovery（Serial）Kiosk が表示されます。

9. デフォルトのユーザー名とパスワード（admin/Admin123）を使用して、Web 経由でアプライアンスにログインします。admin のパスワードはすぐに変更する必要があります。詳細については、「ローカルユーザーのパスワード設定」を参照してください。

10. クラスタリング後、信頼できるサーバー、CORS、リダイレクトの設定を変更します。ベストプラクティスとして、SPP のクラスタを作成した後（または単一の仮想マシンを使用しているだけの場合）、信頼できるサーバー、CORS、リダイレクトの設定を空文字列または値のリストに変更して、許可したいアプリケーションを統合します。詳細については、「信頼できるサーバー、CORS、リダイレクト」を参照してください。

クラウド仮想アプライアンスの設定の表示または変更

仮想アプライアンスの設定を表示または変更することができます。

管理者は、リカバリキオスク（シリアルキオスク）を使用して次のことを実行します：

- アプライアンス情報の取得
- 管理者パスワードのリセット
- 仮想アプライアンスの再起動またはシャットダウン
- サポートバンドルの生成

- 検疫を解決（詳細については、「アプライアンスが隔離された場合の対処法は？」を参照してください。）

詳細については、「リカバリキオスク（シリアルキオスク）」を参照してください。

新しいバージョンにパッチを適用するには、API を使用します。

5.3 仮想アプライアンスのバックアップと復元

次の情報を使用して、SPP の仮想アプライアンスをバックアップおよびリカバリーします。仮想アプライアンスの場合、工場出荷時リセットオプションはありません。仮想アプライアンスを工場出荷時にリセットするには、アプライアンスを再デプロイしてください。

仮想アプライアンスのバックアップ

ハードウェアアプライアンスのセキュリティを確保するため、ハードウェアアプライアンスから取得したバックアップを仮想アプライアンスで復元することはできず、仮想アプライアンスから取得したバックアップをハードウェアアプライアンスで復元することはできません。

詳細については、「バックアップと復元」を参照してください。

仮想アプライアンスの復元

SPP 仮想アプライアンスは、次の復元手順でリセットします。

オンプレミスの仮想アプライアンス（例：Hyper-V、VMware）の場合

1. 仮想アプライアンスを再デプロイし、**初期セットアップ**を実行します。
   詳細については、「仮想アプライアンスのセットアップ」を参照してください。

2. バックアップを復元します。
   詳細については、「バックアップと復元」を参照してください。

クラウド仮想アプライアンス（例：AWS、Azure）の場合

1. 以下の手順をにて再デプロイします。
   - AWS：詳細については、「AWS デプロイ」を参照してください。
   - Azure：詳細については、「Azure デプロイ」を参照してください。

6 SPP の初期設定

SPP が特権アカウントのパスワードと特権セッションを管理する前に、ユーザー、アカウント、資産など、アクセスリクエストポリシーを作成するために必要なすべてのオブジェクトを最初に追加する必要があります。これらの手順に従うことで、管理者の階層が設定され、企業がロールベースのアクセス制御に従うことが保証されます。詳細については、「管理者のアクセス許可」を参照してください。

このセクションのセットアップ手順は、「Safeguard for Privileged Passwords アプライアンスセットアップガイド」のアプライアンスの初期インストールおよび構成手順が完了していることを前提としています。

SPP が Windows システムのローカルアカウントパスワードをリセットする前に、ローカルセキュリティポリシーを変更してユーザーアカウント制御を無効にしておく必要があります。すべての管理者を管理者承認モードで実行します。詳細については、「パスワードまたは SSH キーの変更に失敗する」を参照してください。

6.1 手順 1: 権限許可者の作成

1. Bootstrap Administrator アカウントでログインします。
2. 他の管理者に権限を与えることができるユーザーである権限許可者を作成します。ユーザーが他のユーザーに権限を付与し自身の権限を変更できるように、ユーザーに権限を付与します。詳細については、「ユーザーの追加」を参照してください。
3. Bootstrap Administrator アカウントをログアウトします。
4. 権限許可者としてログインします。

5. Bootstrap Administrator を無効にします。

6.2 手順 2: 権限許可者で管理者を作成

ユーザー管理者権限を追加します。1 人のユーザーは複数の権限を持つことができます。SPP の管理権限一覧は、「管理者のアクセス許可」を参照してください。

1. 権限許可管理者アカウントでログインしていることを確認します。
2. 次の管理者権限のユーザーを追加します。
    a. ユーザー管理者
    b. HelpDesk 管理者
    c. アプライアンス管理者
    d. 操作管理者
    e. 監査人
    f. 資産管理者
    g. セキュリティポリシー管理者

6.3 手順 3: アプライアンス管理者でアプライアンスを構成

1. アプライアンス管理者アカウントでログインします。
2. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク］**に移動して、以下を設定します。
    a. IP アドレス
    b. ネットマスク
    c. デフォルトゲートウェイ
    d. DNS サーバー
    e. DNS サフィックス

    詳細については、「ネットワーク」を参照してください。
3. アクセスリクエストとパスワードおよび SSH キー管理機能が有効になっていることを確認します（**[アプライアンス管理］＞［サービスの有効化または無効化]**）。詳細については、「サービスの有効化または無効化」を参照してください。

4. （オプション）**［アプライアンス管理］>［サービスの有効化または無効化］**で、**［アプリケーション – アプリケーションが有効になりました］**を有効または無効にし、Safeguardfor Privileged Sessions（SPS）とのデータ共有を監査します。詳細については、「サービスの有効化または無効化」を参照してください。

5. 適用する外部統合設定を構成します（**［設定］>［外部統合］**）。

    a. メール：
    メール通知に使用する SMTP サーバーを構成します。SPP は、ほとんどのイベントに対してデフォルトのメールテンプレートを提供しますが、カスタマイズすることができます。詳しくは「メール」を参照してください。

    b. ID と認証：
    Active Directory や LDAP サーバーなどのディレクトリサービスを、SPP ユーザーの ID および認証プロバイダとして使用するよう構成します。SPP を、SAML 2.0 を使用して外部フェデレーションサービスと統合し、ユーザーを認証する証明書利用者として構成します。プライマリまたはセカンダリ認証プロバイダとして使用する RADIUS サーバーを作成します。

    c. SNMP：
    特定のイベントが発生したときに SNMP トラップを SNMP コンソールに送信する SNMP サブスクリプションを構成します。詳しくは「SNMP」を参照してください。

    d. Starling：
    他の Starling サービスを利用するために SPP を Starling に参加させます。詳しくは「Starling」を参照してください。

    e. Syslog：
    イベント通知を送信する syslog サーバーを設定します。詳しくは「Syslog」を参照してください。

    f. チケットシステム：
    外部チケット追跡システムを追加するか、外部チケットシステムに関連付けられていないチケットを追跡します。詳しくは「チケットシステム」を参照してください。

6.4 手順 4: ユーザー管理者でユーザーを追加

1. ユーザー管理者アカウントでログインします。

2. SPP にログインできるユーザーを追加します。

3. 1 人以上のユーザーに Help Desk 管理者権限を付与します。

6.5 手順 5: 資産管理者で管理対象システムを追加

1. 資産管理者アカウントでログインします。
2. パーティションを追加し、任意でパーティションの所有権を他のユーザーに委任します。
3. （任意）次のパスワードプロファイルを設定します（または、パーティションが追加されたときに定義されたデフォルトのルールと設定を編集します）。
    - アカウントパスワードルール
    - パスワードの変更
    - パスワードの確認
    - パスワードの同期グループ
4. （任意）次の SSH キープロファイルを設定します。
    - SSH キー設定の変更
    - SSH キー設定のチェック
    - SSH キーの検出設定
    - SSH キー同期グループ設定
5. （任意）パスワードプロファイルを作成するか、作成されたデフォルトプロファイルを編集します。
6. （任意）適切なパーティションとプロファイルに資産を追加します。
7. アカウントを追加して、資産へのアクセスを制御します。

> **メモ：**資産とアカウントの検出ジョブを作成して資産とアカウントを検出し、任意で SPP に自動的に追加します。詳細については、「検出」を参照してください。

6.6 手順 6: セキュリティポリシー管理者でアクセスリクエストポリシーを追加

1. セキュリティポリシー管理者アカウントでログインします。
2. 理由を設定します。
3. ユーザーグループを追加します。
4. ローカルユーザーまたはディレクトリユーザーをローカルユーザーグループに追加します。
5. アカウントグループを追加します。
6. アカウントグループにアカウントを追加します。
7. 資格を追加します。
8. 資格にユーザーまたはユーザーグループを追加します。
9. アクセスリクエストポリシーを作成します。

7　Web クライアントの使用

Web クライアントは、レスポンシブユーザーインターフェイスデザインを使用しており、デスクトップからタブレットや携帯電話まで、ユーザーのデバイスに適応します。ブラウザセッション中は、1 つのユーザーセッションのみが持続されます。最初の認証後に開いたタブは、既存のユーザーセッションを使用します。

Web クライアントアプリケーションへのログイン

以下の手順は、SPP アプライアンスが構成済みでありライセンスが適用済みであることを前提としています。ライセンスが登録されていない旨の通知を受けた場合は、アプライアンス管理者に連絡してください。

1. Web ブラウザーを起動し、SPP の URL を IP アドレスで入力します（例：https://11.1.111.11)。
2. ログイン通知が表示されたら、**[OK]** をクリックして、記載されている通知と制限を受諾します。
3. ユーザーログイン画面で、認証情報を入力し、**[ログイン]** をクリックします。

アバター写真の更新

Web クライアントで写真を変更するには、右上の **「ユーザー名」** のドロップダウンを展開し、**[自分の設定]** を選択します。**[自分の設定]** ページで **[私のアカウント]** を選択し、ユーザー名の丸いアイコンをクリックします。画像ファイル（64KiB 以下）を選択し、**[開く]** をクリックします。

左側のナビゲーションメニューの使用

> **メモ：** ナビゲーションメニューの展開と折り畳みの切り替えは、☰ボタンを使用します。

左側のナビゲーションメニューからトップレベルの見出しの 1 つをクリックすると、そのセクションが展開され、関連するサブページが表示されます。たとえば、**[ユーザー管理]** をクリックすると、ナビゲーションメニューが展開され、ユーザーの管理に関するアクセス権限のあるすべてのページが表示されます。

左側のメニューは、左側のナビゲーションメニューの下部にある ボタンを使って縮小することができます。

7.1 自分の設定

［自分の設定］では、Web クライアントを使用するためのさまざまな制御を設定することができます。表示される設定は、ユーザーの役割と権限に基づいています。

［自分の設定］へのアクセス

右上のユーザー名の横にある をクリックして**［私の設定］**を選択すると、**［私の設定］**画面が表示されます。ユーザーの役割と権限に応じたタブが利用できます。

［全般］タブの使用

- **言語**ドロップダウン：
  このドロップダウンを使用して、サイトの言語を変更します。デフォルトでは、**「ブラウザ言語（自動検出）」**に設定されています。
- **Safeguard について**：
  アプライアンスのバージョンが表示されます。

［私のアカウント］タブの使用

- **連絡先情報：**
  ［メール］、［勤務先電話］、［携帯電話］を変更するには、**［編集］**をクリックします。変更を保存する場合は **［保存］**をクリック、以前の設定に戻す場合は **［キャンセル］**をクリックします。
- **場所：**
  ドロップダウンボックスでタイムゾーンを選択します。タイムゾーンの変更は、お客様の組織のセキュリティ手順により禁止されている場合があります。利用可能な場合は、以下を選択します。
  - **ローカルコンピュータ時間で時刻を表示**：
    これはデフォルトです。ローカルコンピュータに設定されているタイムゾーンです。
  - **自分の設定済みタイムゾーンで時刻を表示**：
    このページで設定されているタイムゾーンです。

- **メール通知の管理**：
  ［メール通知の管理］では、メール通知を受信するイベントの種類が表示されます。通知を受信するイベントの種類を定義することができます。デフォルトでは、すべてのイベントが選択されています。イベントが SPP に組み込まれている場合は、**「ビルトイン」**に ✔ が表示されます。複数のイベントがある場合、イベントの**名前**、**説明**、**カテゴリ**を一覧表示する**サブスクリプション**ダイアログを表示するイベントリンクが表示されます。
  - メール通知を受信したくないイベントのチェックボックスをオフにします。
  - すべてのチェックボックスを設定するには、ヘッダーの左側のチェックボックスを選択またはクリアします。

  > **メモ：**パーティションに委任所有者が割り当てられていない場合、パーティションに関連するメール通知は資産管理者に送信されます。ただし、パーティション内の資産とアカウントを管理する委任所有者が指定されている場合、パーティションに関連するメール通知は、資産管理者ではなく、委任所有者に送信されます。

- **FIDO2 キーの管理**（**FIDO2** 二要素認証の実行が必要な場合に利用できます）：
  FIDO2 機能が有効な場合、少なくとも 1 つの FIDO2 キーが登録されている必要があります。キーが追加されると、プレースホルダー名は無名キーとなります。意味のある名前を入力するか、後で名前を編集することができます。鍵の紛失や破損に備えて、すべてのユーザーが複数の鍵を登録することをお勧めします。既存のキーについては、それぞれの既存のキーが登録され、最後に使用された名前と日付が表示されます。
  - 名前を変更するには、新しい名前を入力し、**［保存］**をクリックします。
  - キーを削除するには、キーの横にある **［削除］**をクリックします。キーは 1 つ登録したままにしておく必要があります。物理セキュリティキーを紛失した場合、必ず関連するキーを SPP から削除してください。
  - キーを追加するには、**［新しい FIDO2 キーを登録する］**をクリックします。
    a. 新しいキーを挿入または接続するよう求められます。
    b. 確認のため、主要な認証情報を再入力するよう促されます。
    c. 登録されている新しい FIDO2 キーをタップするか、アクティベートします。
    d. **FIDO2 キーの管理**ページに戻り、新しく登録したキーに名前を付けて、**［保存］**をクリックします。

- **パスワード変更**：
  パスワードの要件が表示されます。指示に従い、**［現在のパスワード］**と**［新しいパス**

ワード］を入力します（入力されたパスワードの表示/非表示を切り替えるには、［**表示**］または［**非表示**］をクリックします）。［**保存**］をクリックします。

7.1.1 パスワードの変更

パスワードを変更することができます。

パスワードの変更手順

1. 右上隅のユーザー名の横にある ▼をクリックします。
2. ［**自分の設定**］を選択します。
3. ［**私のアカウント**］を選択します。
4. ［**パスワードの変更**］をクリックします。パスワードの要件が表示されます。
5. ［**現在のパスワード**］と［**新しいパスワード**］を入力します。（入力されたパスワードの表示/非表示を切り替えるには、［**表示**］または［**非表示**］をクリックします）。
6. ［**保存**］をクリックして新しいパスワードを保存します。

7.1.2 FIDO2 キー

FIDO2 機能が有効な場合、少なくとも 1 つの FIDO2 キーが登録されている必要があります。キーが追加されると、プレースホルダー名は無名キーとなります。意味のある名前を入力するか、後で名前を編集することができます。鍵の紛失や破損に備えて、すべてのユーザーが複数の鍵を登録することをお勧めします。

1. 右上隅のユーザー名の横にある ▼をクリックします。
2. ［**自分の設定**］を選択します。
3. ［**私のアカウント**］を選択します。
4. ［**FIDO2 キーの管理**］を選択します。キーが存在する場合は、既存のキーの名前と登録時と前回の使用日が表示されます。
5. 操作を行います：

- 名前を変更するには、新しい名前を入力し、**［保存］**をクリックします。
- キーを削除するには、キーの横にある **［削除］**をクリックします。キーは 1 つ登録したままにしておく必要があります。物理セキュリティキーを紛失した場合、必ず関連するキーを SPP から削除してください。
- キーを追加するには、**［新しい FIDO2 キーを登録する］**をクリックします。
    a. 新しいキーを挿入または接続するよう求められます。
    b. 確認のため、主要な認証情報を再入力するよう促されます。
    c. 登録されている新しい FIDO2 キーをタップするか、アクティベートします。
    d. **FIDO2 キーの管理**ページに戻り、新しく登録したキーに名前を付けて、**［保存］**をクリックします。

7.2 アプリケーションスイッチャー

アプリケーションスイッチャーは、SPP に関連する One Identity 製品間を移動することができます。ツールバーからアクセスできます。

アプリケーションスイッチャーの使用手順

1. 右上のユーザー名の横にある ボタンをクリックすると、アクセス可能な One Identity 製品が表示されます。Safeguard for Privileged Sessions などの一部の製品は、アプリケーションスイッチャーで利用前にリンクされていることが必要です。
2. 表示された製品のいずれかをクリックすると、新しいタブでその製品が表示されます。

7.3 ログアウト

Web クライアントから常に安全にログアウトします。ログイベントは、ユーザーのログアウト方法に基づいて「UserLoggedOut」または「InactiveUserLoggedOut」が作成されます。

ログアウト手順

1. 右上のユーザー名の横の をクリックします。
2. **［ログアウト］**をクリックして、SPP Web クライアントを安全に終了します。

7.4　検索ボックス

検索ボックスを使用して、表示されるデータをフィルタリングすることができます。検索ボックスにテキスト文字列を入力すると、入力されたテキストを含む文字列属性を持つアイテムが結果に含まれます。この基本的な検索機能は、多くの詳細ペインと選択ダイアログでも使用でき、関連するペインまたはダイアログに表示されるデータをフィルタリングできます。

オブジェクトリストでオブジェクトを検索する場合、特定の属性に基づいて結果をフィルタリングすることができる属性検索機能も利用できます。つまり、指定された属性にテキストが含まれていれば、検索語が一致します。属性検索を実行するには、🔍アイコンをクリックして検索する属性を選択します。

検索機能を使用するためのルール

- 検索文字列は、大文字と小文字を区別しません。例外として、承認とレビューの検索は大文字と小文字が区別されます。
- 検索バーの検索アイコンをクリックすると、グリッドで利用可能な検索属性（列）のドロップダウンが表示されます。これは、入力された検索文字列と組み合わせて使用することができます。

  検索属性の中には、サブサーチを展開するための矢印が表示されているものもあります。これらのサブサーチには、あらかじめ定義された検索文字列があります。
- デフォルトでは、結果はアルファベット順に表示されます。
- ワイルドカードは使用できません。
- 引用符を使用、または引用符の省略を試してみてください。製品を使用するにつれて、頻繁に使用する検索フィールドの検索要件に慣れてきます。SPP は、一般的な検索（例えば、引用符を省略する）またはリテラル検索（例えば、引用符を含む）を実行することができます。シナリオ例は次のとおりです：
  - **［アプライアンス管理］＞［検索］**ではリテラル検索が実行されるため、検索文字列は完全一致である必要があります。引用符や下線を追加しないでください。例えば、**［設定］**ペインでパスワードルール と入力すると、**［Safeguard アクセス］＞［パスワードルール］**が返されます。“**password rules**” または ”**password_rules**”を入力すると、**“一致が見つかりません”**というメッセージが返されます。
  - **［ユーザー］**ペインの検索ボックスで、検索名にスペースがある場合は、属性検索で引用符を使用できます。例えば、検索ボックスのユーザー名に次のように入力すると、「ab_misc2」は次のようになります。“AB_misc2”

- 複数の検索文字列が含まれている場合、オブジェクトが結果リストに含まれるためには、すべての検索条件が満たされる必要があります。Web クライアントでは、同じ検索に相反する属性が入力された場合（たとえば、true と false の両方）、それらの属性のいずれかに適合する限り、結果は拡大してすべてのマッチが表示されます。
- 文字列検索と属性検索を組み合わせる場合、検索ボックスに入力される順序が重要です。属性検索はどのような順番でもかまいませんが、文字列検索は属性検索の後に入力する必要があります。
- Web クライアントで日付と時刻を使って検索するには、YYYY-MM-DDThh:mm:ss の形式を使用します。例えば、2021 年 12 月 1 日に期限が切れる資格を検索する場合、ExpirationDate:2021-12-01 を使用します。検索に最小値と最大値を含めるには、...を使用して 2 つの値を区切ります。例えば、2021 年 12 月 1 日から 2021 年 12 月 3 日の間に期限が切れる資格を検索する場合、ExpirationDate:2021-12-01..2021-12-03 を使用します。

オブジェクトまたはオブジェクト詳細の検索手順

1. **検索**ボックスにテキスト文字列を入力します。入力すると、文字列属性に入力した文字列が含まれるアイテムがリストに表示されます。

   例：

   - 検索ボックスに **T** と入力すると、“T” を含む項目が検索されます。
   - **sse** と入力すると、文字列 “sse” を含むすべての項目（”Asset”など）がリストアップされます。

   > **注意：**コンソールの下部にあるステータスバーには、返された項目の数が表示されます。

2. 検索条件をクリアするには、⊗ボタンをクリックします。
   検索条件をクリアすると、オブジェクトの元のリストが表示されます。

7.4.1 属性による検索

検索に使用できる属性は、検索対象のオブジェクトのタイプによって異なります。検索ドロップダウンメニューには、選択可能な属性が一覧表示されます。

検索可能な API 属性

ドロップダウンメニューには、検索できる属性の数が制限されています。しかし、API に表示される任意の属性の英語名を使用して属性検索を実行できます。ネストされた属性は、ピリオド（.）を使用して連鎖させることができます。すべての属性のリストを表示するには、API ドキュメントを参照してください。API の詳細については、「API の使用」を参照してください。

検索文字列の入力手順

1. アイコンをクリックして、検索する属性を選択します。
   選択した属性が検索ボックスに追加されます。例えば、**[姓]** を選択すると、**[姓:]** が検索ボックスに追加されます。

2. 検索ボックスに、属性ラベルのコロンの後にテキスト文字列を入力します。
   複数の属性を指定することもできます。この手順を繰り返して、検索ボックスに別の属性を追加してください。異なる属性を区切るために、カンマやコロンなどの区切り記号を追加しないでください。複数の属性が含まれる場合、オブジェクトが結果リストに含まれるためには、すべての検索条件を満たす必要があります。Web クライアントでは、同じ検索に相反する属性が入力された場合（たとえば、true と false の両方）、それらの属性のいずれかに適合する限り、結果は拡大してすべてのマッチが表示されます。

   入力すると、選択した属性に入力されたテキストが含まれるアイテムがリストに表示されます。

   > **メモ：** コンソールの下部にあるステータスバーには、返されたアイテムの数が表示されます。

3. 検索条件をクリアするには、ボタンをクリックします。
   検索条件をクリアすると、オブジェクトの元のリストが表示されます。

7.5 データのエクスポート

Web クライアントでは、表の上に **[エクスポート]** ボタンが表示されている場合、その表に表示されているデータを JSON ファイルまたは CSV ファイルとしてエクスポートできることができます。

データのエクスポート手順

1. エクスポートする情報が表示されているページに移動します。たとえば、SPP にログインできるユーザーを確認するためにユーザー情報をエクスポートする場合は、**[ユーザー]** ページに移動します。

2. （任意）表示されたデータにフィルターまたは検索条件を適用します。

3. **[エクスポート]** ボタンをクリックします。

4. エクスポートダイアログで、CSV または JSON を選択します。選択した内容によって、利用できる情報が異なる場合があります。例えば、データが情報の配列の場合、CSV には配列内の項目数のみがレポートされ、JSON には完全なリストがレポートされます。CSV ではグループ内のアカウント数が表示されますが、JSON ではグループ内のすべてのアカウントの情報が表示されます。

5. **[フィールド]** をクリックすると、**[フィールドをエクスポート]** ダイアログが開き、レポートに含めるフィールドを選択することができます。**[フィールドをエクスポート]** ダイアログには、このページから最後にデータをエクスポートした際に選択された内容があらかじめ入力されています。

6. **[OK]** をクリックして、選択内容を保存します。

7. **[ソート基準]** をクリックすると、**[ソート順をエクスポート]** ダイアログが開き、前回選択したフィールドのソート順を選択することができます。これにより、必要性に応じてエクスポートされたデータを整理することができます。

    - **[ソート順の追加]**：データを並べ替えるためのフィールドを追加します。
    - **[すべてのソート順の消去]**：選択したすべてのフィールドをクリアします。
    - **[ソート順を変更するには上または下にドラッグします]**：ソート順を変更することができます。複数のソート順がある場合、このアイコンをカーソルでクリックしたまま、選択したソート順をリストの好きな場所にドラッグします。
    - **[並べ替え順]**：このドロップダウンを使って、データの並べ替えを行うフィールドを選択します。**[ソート順の追加]** ボタンを使用すると、ドロップダウンを追加することができます。**[並べ替え順]** フィールドには、このページから最後にデータをエクスポートした際に選択された内容があらかじめ入力されています。
    - または **[ソート方向の変更]**：このボタンをクリックすると、そのフィールドのソート方向が変更されます。例えば、**[ソート方向の変更]** ドロ

ップダウンで **FirstName** を選択した場合、エクスポートされたデータは **FirstName** を基準にしたアルファベット順に並びます。

- ー **［削除］**：関連する［並べ替え順］の選択が解除されます。

8. **［OK］**をクリックすると、選択内容が保存されます。
9. **［結果を制限］**チェックボックスを選択すると、**［含める結果の数］**フィールドが表示され、エクスポートされるファイルに含まれる結果の数を制限するために使用されます。このフィールドには、このページから最後にデータをエクスポートした際に選択された結果があらかじめ入力されています。
10. **［エクスポート］**をクリックします。

7.6 ホーム

［ホーム］をクリックすると、ホームページに移動します。**ホーム**ページは、ユーザーの権利とアクセス許可に応じて調整されます。アクセスリクエストを要求、承認、またはレビューを行う権限を持っている場合、**ホーム**ページには、すぐに注意を払う必要があるアクセスリクエストタスクが表示されます。

ダッシュボードには、ロールに基づいて、**私のリクエスト**、**承認**、**レビュー**、各キューのタスク数、各タスクのステータス（例：**利用可能**、**拒否**、**取り消し**、**保留中**）、およびそのタスクの期限が表示されます。

また、**アプライアンスのリソース**や**クラスタのステータス**など、その他のウィジェットも利用できる場合があります。

ホームページでは、自分のロール（役割）に応じたタスクの他、次の操作が可能です：

- ページに表示される情報をカスタマイズする。**［設定］**をクリックします。
- アプライアンス管理者からの**［その日のメッセージ］**を読む。詳細については、「その日のメッセージ」を参照してください。

7.6.1 要求者のホーム画面

［新しいリクエスト］ボタンをクリックすると、**［新しいアクセスリクエスト］**ダイアログが表示され、アクセスを許可されている資産とアカウントが一覧表示されます。このダイアログから、リクエストする資産、アカウント、アクセスの種類、リクエストに関する追加の詳細を指定します。

詳細については、以下を参照してください：

- パスワードリリースをリクエストする
- SSH キーリリースをリクエストする
- セッションアクセスをリクエストする

［私のリクエスト］をクリックすると、処理待ちのリクエストが表示されます。

詳細については、以下を参照してください。

- パスワードリリースリクエストに対応する
- SSH キーリリースリクエストに対応する
- セッションリクエストに対応する

お気に入りペインには、お気に入りとしてマークしたリクエストのリストが表示され、素早くアクセスをリクエストすることができます。

7.6.2 承認者のホーム画面

承認者は、自分の**ホーム**ページに表示されているアクセスリクエストに対して、承認または拒否を行うことができます。**［承認］**をクリックすると、承認待ちのリクエストが表示されます。承認者の場合、自分が要求者に指定されていない限り、お気に入りは表示されません。

詳細については、以下のトピックを参照してください：

- パスワードリリースリクエストを承認する
- SSH キーリリースリクエストを承認する
- セッションリクエストを承認する

7.6.3 レビュー承認者のホーム画面

レビュー承認者の仕事は、自分のホームページに表示されている完了したアクセスリクエストを確認することです。**［レビュー］**をクリックすると、レビューが必要な完了したリクエストが表示されます。レビュー承認者として、要求者としても指定されていない限り、お気に入りが表示されることはありません。

詳細については、以下のトピックを参照してください：

- 完了したパスワードリリースリクエストをレビューする

- 完了した SSH キーリリースリクエストをレビューする
- セッションリクエストをレビューする

7.6.4 私のリクエスト

要求者の場合は、**［私のリクエスト］**をクリックしてリクエストを行うか、リクエストに関する情報を表示します。

［アカウントリクエストの可用性を表示］を有効にすると、特権アカウントが使用可能かどうかを識別することができます。リクエストによって使用中の場合、アカウントには 警告バッジが表示されます。複数のユーザーからのアカウントリクエストが重複しないようにするため、アカウントの状態は変更されるとすぐに更新されます。バッジにカーソルを合わせると、<X>個のアカウントのうち<X>個が使用可能であることが表示されます。アカウントの使用状況を表示するには、追加の API クエリが必要であり、パフォーマンスに影響を与える可能性があります。このトグルは、管理者ではなくユーザーが設定します。グローバルなトグルはありません。

> **メモ：**要求を管理するポリシーで**［同時アクセスを許可］**が有効になっている場合、**［アカウント要求の空き状況を表示］**で使用中と表示されていても、要求はまだ使用可能であることがあります。

［私のリクエスト］ページには、表示される情報を構成するために使用できる追加の設定があります。 ボタンをクリックすると、以下のオプションがあるパネルが表示されます。

- **私のリクエストのお気に入り**：このオプションをオンにすると、設定したお気に入りのリクエストを表示するウィジェットが表示されます。
- **アカウントリクエストの可用性を表示（パフォーマンスが低下する場合があります）**：このオプションをオンにすると、アカウントリクエストの可用性が表示されます。リクエストの数によっては、パフォーマンスに影響を与える可能性があります。
- **［セッション起動］ボタンを表示**：このオプションをオンにすると、**私のリクエスト**ページに**［セッション起動］**ボタンが追加されます。このボタンを使って、登録された URL スキームでセッションを開くことができます。
- **［Web セッション起動］ボタンを表示**：このオプションを選択すると、私のリクエストページに Web セッション起動ボタンが追加されます。このボタンを使用すると、One Identity Starling 経由で Safeguard Remote Access セッションを開くことができます。
- **ページサイズ**：関連するタイル（**25**、**50**、**100**）を使用して、**私のリクエスト**ページに表示されるリクエストの数を選択します。

リクエスト手順

必要な資産とアカウントのリクエストを作成するには、資格が承認されたユーザーである必要があります。

1. **［私のリクエスト］**をクリックして、**私のリクエスト**ページに移動します。
2. ワークフローの手順に従います。詳細については、「パスワードリリースのリクエスト」を参照してください。

お気に入りの作成手順

使用頻度の高いリクエストをお気に入りとして作成することができます。詳しくは、「お気に入り」を参照してください。

リクエストの閲覧と管理

私のリクエストページで、リクエストを閲覧することができます。次の方法で表示を制御します：

- チェックイン可能なすべてのリクエストをチェックインする場合は **［すべてをチェックイン］**、すべてのリクエストを削除する場合は **［すべて削除］**、保留中のすべてのリクエストをキャンセルして削除する場合は **［保留中のすべてのリクエストをキャンセル］**をクリックします。
- アカウント名、資産名、次回期限、次回失効、最新、ステータスでソートする場合は、**［ソート］**を選択します。
- 昇順でソートする場合は **［昇順］**、降順でソートする場合は **［降順］**をクリックします。
- ステータスによりフィルタする場合は、**［フィルタ］**をクリックします。
    - **利用可能**：表示またはコピーする準備ができている承認済みリクエスト
    - **承認が保留中**：承認待ちリクエスト
    - **承認済み**：承認されたが、チェックアウト時間に達していないリクエスト、または SPP の一時停止機能を使用しているときに復元された保留中のアカウントの場合
    - **取り消し済み**：承認者によって取り消された承認済みリクエスト（承認者は、リクエストが利用可能になった後、リクエストを取り消すことができます。）
    - **失効**：**チェックアウト期間**が経過したリクエスト
    - **拒否**：承認者によって拒否されたリクエスト

- 🔍**［検索］**をクリックして、検索可能な要素のリストを表示します。または、検索文字を入力します。詳細については、「検索ボックス」を参照してください。
- 拒否または取り消しされたリクエストに承認者がコメントをつけている場合、リクエストに関連する 💬 ボタンをクリックしてコメントを表示することができます。

Web セッションの起動

SPP の Web クライアントからブラウザベースのセッションを起動するには、2 つのオプションがあります。

- **セッションの起動**：このオプションでは、ブラウザで登録された URL スキームを使用してセッションを開くことができます。
- **Web セッションの起動**：このボタンを使用すると、One Identity Starling 経由で Safeguard Remote Access セッションを開くことができます。

Web セッションの起動ボタンを使用して Safeguard Remote Access セッションを起動するには、いくつかの追加要件を満たしている必要があります。

- SPP は Starling に参加する必要があります。
- Safeguard Remote Access および Safeguard for Privileged Sessions には、追加の構成要件がある場合があります。詳細については、Safeguard Remote Access および Safeguard for Privileged Sessions のドキュメントを参照してください。

7.6.5 個人用パスワードボールト

個人用パスワードボールトは、ビジネスユーザーがパスワードを保管・管理するためのセキュリティとクレデンシャル保護を拡張します。ユーザーは、**個人用パスワードボールト**アクセス許可を付与されている必要があります。

ユーザーメリットは以下の通りです：

- 最大 100 個の個人用パスワードを保存し、オプションで有効期限を設定し、パスワードを共有することができます。
- 最後にパスワードを変更した日を確認することができます。
- 個人用パスワードの変更履歴を持ちます。これは、ユーザーがボールトでパスワードを変更しても、ターゲットアカウントでは変更しない場合や、バックアップから作業する必要がある場合に便利です。

- パスワードは、ユーザーが他の 1 人のユーザーと共有することができます。たとえば、ユーザーが不在の場合、同僚にパスワードへのアクセス権を与えることができます。また、パスワードを共有したユーザーは、共有の解除が可能です。

個人用パスワードボールトでは、ビジネスユーザーのパスワードは IT チームとセキュリティチームの管理下に置かれ、様々な方法でパスワードを保管することができます。個人用パスワードボールトは、セキュリティポリシー管理者とユーザー管理者にとって、以下のようなメリットがあります。

- ユーザーが個人用パスワードを保管するために、組織として承認され管理されたツールを使用することができます。
- 個人パスワードは安全で暗号化されます。個人パスワードは、管理されたアカウントのパスワードとは別に保管されます。
- 個人用パスワードボールトは、パスワードの取得と変更を監査するため、管理者はユーザーがいつボールトから情報を取得したかを知ることができます。
- 管理者は、誰かが会社を辞めるときにパスワードを回復することができます。管理者は、認証プロバイダをローカルに変更し、ユーザーのパスワードを設定した後、ログインして個人用パスワードボールトを表示する必要があります。
- 削除されたユーザーの個人用パスワードボールトを復元する方法はありません。

システムユーザー（Bootstrap admin）は、個人アカウントを作成できません。

> **重要**: 個人用パスワードボールトのアクセス許可は、他のアクセス許可と同様に、ユーザー上で明示的に設定するか、ディレクトリグループから継承することができます。個人用パスワードボールトのアクセス許可を持つユーザーが 1 つ以上の個人用パスワードを保存し、その後、明示的にまたは彼らがそれを継承したすべてのディレクトリグループから削除されたことによって、アクセス許可を取り消した場合、ユーザーは個人用パスワードボールト機能にアクセスすることができなくなります。しかし、データボールト内のユーザーデータは維持されます。任意の時点でユーザーが再び個人用パスワードボールトのアクセス許可を付与された場合、彼らは既存のすべてのデータへアクセスすることができます。

詳しくは、「アクセス許可タブ（ユーザー追加）」を参照してください。

個人用パスワードボールトページのツールバーの機能は次のとおりです。

表：個人用パスワードボールト：ツールバー

オプション	説明
＋ 新しいエントリ	個人用パスワードボールトにエントリを追加します。

オプション	説明
エントリの削除	選択した 1 つまたは複数のエントリを個人用パスワードボールトから削除します。エントリを削除すると、その資格情報にはアクセスできなくなります
エントリの編集	選択したエントリを変更します。
情報	選択したエントリに関する以下の情報を表示します。 • **名前**：アクセスするアプリケーションまたはアカウントに割り当てられた意味のある名前 • **アカウント名**：ログオン認証のためのユーザー名。**［アカウント名のコピー］**をクリックすると、名前がクリップボードにコピーされます。 • パスワード：秘密情報。**表示**、**非表示**、**パスワードのコピー**を行えます。 • **失効**：パスワードが無効になる日付 • **メモ**：ユーザーとパスワードを共有する人のための情報（二次的な秘密やその他の指示など）。 • **共有先**：パスワードを共有するユーザー名と、共有の有効期限。共有の有効期限を変更するには、**［編集］**をクリックして日付を変更し、**［保存］**をクリックします。
資格情報の共有	1 つまたは複数のエントリを選択し、資格情報を共有するユーザーと共有を停止する日付を選択します。表示するには、この機能を有効にしておく必要があります。詳しくは、「アクセス許可タブ（ユーザーの追加）」を参照してください。
共有の終了	1 つまたは複数のエントリを選択し、**［共有の停止］**をクリックします。 パスワードが他の所有者によって共有されている場合、ユーザーは共有を削除することはできませんが、自分自身を共有から外すことは可能です。

オプション	説明
履歴	パスワードの履歴は、デフォルトで 30 日分表示されます。パスワード履歴を表示する日付範囲を設定するには、カレンダーで **［開始］**と**［宛先］**（正しくは終了）の値を選択します。また、**［日付範囲］**をクリックして期間を選択することもできます。変更日付でパスワードの **［表示］**、**［非表示］**、**［パスワードのコピー］**を行うことができます。
アカウント名のコピー	選択したエントリのアカウント名をコピーします。
パスワードのコピー	選択したエントリのパスワードをコピーします。
URL を開く	パスワードの追加、編集時に入力された URL の Web アドレスを開くことができます。
表示する列の選択	表示する列を選択できます。
検索	をクリックすると、検索可能な要素のリストが表示されます。または、検索文字を入力します。詳しくは、「検索ボックス」を参照してください。

様々なアプリケーションやシステムの入力内容が表に表示されます。

表：個人用パスワードボールト

オプション	説明
名前	アクセスするアプリケーションやアカウントに付けられた意味のある名前。例：Company Twitter
アカウント名	ログオン認証に使用されるユーザー名
失効	パスワードの有効期限、またはパスワードに有効期限がない場合は空白（値なし）
共有	次の値をすべて表示するか、フィルタをクリックして表示する値をいくつか選択します。 • **非共有**：パスワードが他のユーザーと共有されていない • **共有**：他のユーザーとパスワードを共有している • **私と共有**：他のユーザーが自分とパスワードを共有している

オプション	説明
共有先	パスワードが共有されているユーザー名（およびドメイン名（該当する場合））、パスワードが共有されていない場合は空白 ユーザー名の上にカーソルを置くと、確認用のメールアドレスが表示されます。
所有者	パスワードの所有者
共有の有効期限	共有が終了し、共有相手のユーザーがパスワードを利用できなくなる日

パスワードの追加手順

1. **個人用パスワードボールト**ページで、＋**［新しいエントリ］**をクリックします。
2. 以下の値を入力します。
    a. **名前**：アクセスするアプリケーションまたはアカウントの意味のある名前（例：Company Twitter）を入力します。
    b. **アカウント名**：認証のためにログオンする際に使用するユーザー名を入力します。
    c. **パスワード**：パスワードを入力するか、パスワードを自動生成することができます。

    パスワードの追加は任意です。例えば、アプリケーションやシステムに関する情報を**メモ**に保存し、実際のパスワードは保存しないようにすることができます。**メモ**の制限文字数は 2000 文字です。

    - パスワードを入力した場合、**［表示］**または**［非表示］**をクリックして、エントリを表示するかしないかを選択することができます。また、**［パスワードのコピー］**をクリックすると、パスワードをクリップボードにコピーすることができます。
    - パスワードを自動的に生成するには、**［パスワードの生成］**をクリックします。パスワードが自動生成されます。パスワードのルールを変更することができます。

        i. **長さ**：スライダーを使用するか値を入力して、必要な長さを再設定します。

        ii. **番号**（正しくは**「数字」**）：パスワードに数字を使用するかどうかのオン・オフを切り替えます。パスワードは設定に従って再生成されます。

iii. **記号**：パスワードに記号を使用するかどうかのオン・オフを切り替えます。パスワードは設定に従って再生成されます。

iv. **［再生成］**をクリックして、新しいパスワードを生成します。

v. **［OK］**をクリックすると、生成されたパスワードが保存されます。

vi. 新しいエントリパネルに戻り、**［パスワードのコピー］**をクリックすると、パスワードをクリップボードにコピーすることができます。

d. **失効**：アクセスを保護するために、有効期限を設定することをお勧めします。日付を入力するか、カレンダーをクリックして日付を選択することができます。

e. **URL**：アプリケーションまたはシステムの Web アドレスを入力します（例：Amazon.com など）。**［URL を開く］**をクリックすると、リンクをテストすることができます。**［URL のコピー］**をクリックすると、URL をコピーすることができます。

f. **メモ**： 自分やパスワードを共有する相手に役立つフリーフォームのメモを入力します。または、認証やキーなど、アプリケーションやシステムに関する情報にも使用できます。上限は、2,000 文字です。

3. **［保存］**をクリックします。

他のユーザーとのパスワード共有手順

1. **個人用パスワードボールト**ページの表で、共有する 1 つまたは複数のエントリを選択します。

2. **［資格情報の共有］**をクリックします。

3. **［資格情報の共有］**ダイアログで、**個人パスワードボールト**アクセス許可を持つユーザーが利用可能です。管理者はアクセス許可を追加することができます。詳細については、「アクセス許可タブ（ユーザーの追加）」を参照してください。

   ユーザーを 1 人選択します。ユーザーを検索するには、**［検索］**テキストボックスに値を入力するか、アイコンをクリックしてから、ドメイン、表示名、メールアドレスで検索するように選択します。値の最初の文字を入力すると、一致するものが表示され、ユーザーが選択されます。

   ［OK］をクリックします。

4. 共有の終了日を 1 日～1 年の間で設定します。**［共有の終了］**で、日付を入力するか、カレンダーをクリックして日付を選択するか、**［共有の有効期限］**をクリックして 1 週間または 1 ヶ月の間隔を選択します。終了日になると、ユーザーはパスワードを利用できなくなります。

5. **［共有］**をクリックします。

［共有期限］の日付を後で変更する簡単な方法として、エントリを選択して **［情報］**をクリックする方法があります。**［共有の有効期限］**フィールドをクリックして、日付を変更します。

他のユーザーとのパスワード共有の停止手順

1. パスワードを共有している場合、**個人用パスワードボールト**ページの表の**［共有］**列は**「共有」**と表示されます。

2. 共有を停止するエントリのチェックボックスを 1 つ以上選択します。

3. **［共有の終了］**をクリックします。**［共有の終了］**ダイアログが警告として表示されます。

4. **［共有の終了］**をクリックします。

7.6.6 承認

ページの左側にある **［承認］**をクリックして承認を管理します。**承認**ページでは、次のことが可能です：

- リクエストを選択すると、ページの右側に詳細が表示されます。
- 1 つ以上のリクエストの承認：リクエストを選択し、**［承認］**をクリックして、選択したすべてのリクエストを承認します。必要に応じて、コメントを入力します。
- 1 つ以上のリクエストの拒否：リクエストを選択し、**［拒否］**をクリックして、選択したすべてのリクエストを拒否します。必要に応じて、コメントを入力します。
- 表示する列の変更：**［表示する列の選択］**をクリックします。
    - アクション：このリクエストのみ承認/ このリクエストのみ拒否 が表示されます。
    - **要求者/ステータス**：承認者名とステータス（例: 1 件の承認が保留中）が表示されます。

- **資産/資産タイプ**：資産名と資産タイプ（例： パスワード、SSH キー、RDP、SSH、Telnet）が表示されます
- **アカウント**：管理対象のアカウント名が表示されます。
- **チケット番号**：必要に応じてチケット番号が表示されます。
- **リクエスト期間**：利用可能な期間（例：2021 年 3 月 20 日 9:56 2 時間）が表示されます。

- 検索：詳細については、「検索ボックス」を参照してください。

詳細については、「パスワードリリースリクエストの承認」を参照してください。

7.6.7 レビュー

レビューを管理するには、ページの左側にある **［レビュー］**を選択します。**レビュー**ページでは、次のことが可能です：

- リクエストを選択すると、ページの右側に詳細が表示されます。
- 1 つ以上のリクエストをレビュー済みとしてマーク：リクエストを選択し、以下を行います。
  - コメントが不要な場合は、**［選択したすべてのリクエストをレビュー済みとしてマーク］**をクリックします。
  - コメントが必要な場合は、**［選択したリクエストの 1 件以上でコメントが必要です］**をクリックします。コメントを追加し、**［レビュー済みとしてマーク］**をクリックします。
- 表示する列の変更：**［表示する列の選択］**をクリックしてから、表示する列を選択します。
  - **アクション**：**［このリクエストでは、レビューコメントが必要です］**または**［選択したリクエストのみをレビュー済みとしてマーク］**をクリックします。
  - **要求者：**要求者の名前を表示されます。
  - **アクセスタイプ**：アクセスタイプが表示されます（例: パスワード、SSH キー、RDP、RDP アプリケーション、SSH、Telnet）。
  - **アカウント**：管理済みアカウント名が表示されます。
  - **チケット番号**：必要に応じてチケット番号が表示されます。

- **リクエスト期間**：利用可能な期間が表示されます（例：2021 年 3 月 20 日 9:56 2 時間）

- **検索**：詳細については、「検索ボックス」を参照してください。

7.6.8 お気に入り

ホームページまたは **私のリクエスト**ページには、「**お気に入り**」が表示されます。頻繁に行うリクエストをお気に入りに登録しておけば、お気に入りをクリックするだけで、すばやくリクエストを行うことができます。

お気に入りに登録する資産やアカウントに対して、リクエストを作成する権限が必要です。お気に入りタイルを変更するには、アイコン、または アイコンをクリックします。

［アカウントリストの可用性を表示］を有効にすると、特権アカウントが使用可能かどうかを識別することができます。リクエストによって使用中の場合、アカウントには 警告バッジが表示されます。複数のユーザーからのアカウントリクエストが重ならないようにするため、アカウントの状態は変更後すぐに更新されます。バッジにカーソルを合わせると、<X>個のアカウントのうち<X>個が使用可能であることが表示されます。アカウントの使用状況を表示するには、追加の API クエリが必要であり、パフォーマンスに影響を与える可能性があります。このトグルは、管理者ではなくユーザーが設定します。グローバルなトグルはありません。

> **注意:** リクエストを管理するポリシーで**［複数ユーザーの同時アクセスを許可］**が有効になっている場合、**［アカウントのリクエストの可用性を表示］**で使用中と表示されていても、リクエストは使用可能である可能性があります。

お気に入りの追加手順

1. **［新しいお気に入り］**をクリックします。
2. **新しいお気に入り**ページで、アクセスする資産を選択します。次の方法で、必要な資産をすばやく見つけることができます：
   - **［検索］**をクリックして、**資産**、**ネットワークアドレス**、**プラットフォーム**を検索します。詳細については、「検索ボックス」を参照してください。
   - **資産**を選択すると、**選択した資産**の数が左下に表示されます。
   - 右下で、表示される**［ページあたりの項目数］**を選択します。矢印をクリックしてページ間を移動します。
3. **［次へ］**をクリックします。

4. **［お気に入りの詳細］**で、お気に入りの名前を入力します。

5. **ホーム** および **私のリクエスト**ページでお気に入りを表示するときに使用する色を選択します。

6. **［お気に入りの保存］**をクリックします。

   このアクセスリクエストは、**「お気に入り」**に追加されます。一度作成されたお気に入りは、**ホーム**ページまたは **私のリクエスト**ページのお気に入りから選択することで、使用したり変更したりすることができます。

   > **メモ：**お気に入りには固有のリンクが設定されます。このため、リンクをブックマーク/コピーしておけば、後で Web クライアントを操作することなく、そのリンクからアクセスすることができます。

8　特権アクセスリクエスト

SPP は、時間制限、複数の承認者、レビュー担当者、緊急アクセス、ポリシーの有効期限をサポートするワークフローエンジンを提供します。また、理由コードを入力し、チケットシステムと直接統合する機能も含まれています。

リクエストをワークフロープロセスで進行させるために、承認されたユーザーは割り当てられたタスクを実行します。これらのタスクは、ユーザーの **ホーム**ページから実行されます。

SPP ユーザーとして、**ホーム**ページには、すぐに注意が必要なアクセスリクエストタスクへのクイックビューを提供します。さらに、管理者は、注意が必要な保留中のタスクがある場合にユーザーに送信するアラートを設定することができます。詳細については、「アラートの構成」を参照してください。

ホームページに表示されるアクセスリクエストタスクは、資格のアクセスリクエストポリシーによって割り当てられた権限とアクセス許可によって異なります。たとえば、次のようになります：

- 要求者には、新しいアクセスリクエストの送信に関連するタスクと、リクエストが承認された後に実行されるアクション（たとえば、パスワードの表示、パスワードのコピー、セッションの起動、完了したリクエストのチェックインなど）が表示されます。

  また、要求者は、お気に入りのリクエストを定義することもでき、お気に入りのリクエストは、後で使用するために **ホーム**ページに表示されます。
- 承認者には、アクセスリクエストの承認（または拒否）および取り消しに関連するタスクが表示されます。
- レビュー担当者は、完了した（チェックインされた）アクセスリクエストのレビューに関連するタスクが表示されます（セッションの記録が有効な場合は、セッションの再生も含まれます）。

以下の 3 つのワークフローを利用できます：

- パスワードリリースリクエストワークフロー
- SSH キーリリースリクエストワークフロー
- セッションリクエストワークフロー

8.1　アラートの構成

すべてのユーザーは、次のメール通知を購読することができます。ただし、ユーザーは、要求者（ユーザー）、承認者、レビュー担当者としてポリシーに含まれていない場合は、メール通知を受信しません。

- アクセスリクエストの承認
- アクセスリクエストの拒否
- アクセスリクエストの有効期限切れ
- 承認保留中のアクセスリクエスト
- アクセスリクエストの取り消し
- パスワードの変更
- SSH キーの変更
- レビューが必要

8.1.1　　メール通知

ユーザーがメール通知を受信するには、SPP を適切に構成する必要があります。

- ローカルユーザーの場合、**[自分の設定]**でメールアドレスを正しく設定する必要があります。詳細については、「自分の設定」を参照してください。
- ディレクトリユーザーの場合、ユーザーが存在するディレクトリにメールを正しく設定します。
- セキュリティポリシー管理者は、保留中のアクセスワークフローイベント（つまり、保留中の承認と保留中のレビュー）を通知するように、アクセスリクエストポリシーを設定する必要があります。詳細については、「アクセスリクエストポリシーの作成」を参照してください。
- アプライアンス管理者は、SMTP サーバーを構成する必要があります。詳細については、「メール通知の有効化」を参照してください。

デフォルトで生成されるロール（役割）ベースのメール通知

SPP は、調査またはアクションが必要な操作について警告するメール通知を送信するように構成できます。管理者権限によって、デフォルトで受信するメール通知が決まります。

表：管理者権限に基づくメール通知

管理者権限	イベント/警告
アプライアンス管理者、操作管理者	Appliance Healthy Appliance Restarted Appliance Sick Appliance Task Failed Archive Task Failed Cluster Failover Started Cluster Replica Enrollment Completed Cluster Replica Removal Started Cluster Reset Started Disk Usage Warning Factory Reset Appliance License Expired License Expiring Soon NTP Error Detected Operational Mode Appliance Raid Error Detected Reboot Appliance Shutdown Appliance
パーティション所有者（存在しない場合は、資産管理者に送信されます。） **メモ：**資産管理者がパーティション所有者と一緒に通知を受け取りたい場合は、明示的な所有者として設定するか、イベントのメールサブスクリプションを作成できます。 API /service/core/v3/EventSubscribers エンドポイントを使用して、特定の資産またはアカウントのイベントを含む、イベントのイベントサブスクライバーを作成できます。	Account Discovery Failed Dependent Asset Update Failed Password Change Failed Password Check Failed Password Check Mismatch Password Reset Needed Restore Account Failed Service Discovery Failed SSH Check Mismatch SSH Host Key Mismatch SSH Key Change Failed SSH Key Check Failed SSH Key Discovery Failed SSH Key Install Failed SSH Key Reset Needed SSH Key Was Reset Suspend Account Failed Test Connection Failed
セキュリティポリシー管理者	Policy Expiration Warning Policy Expired Entitlement Expiration Warning Entitlement Expired

メモ：SPP 管理者は、次の API を使用して、これらの組み込みのメール通知をオフにすることができます。

POST /service/core/v3/Me/Subscribers/{id}/Disable

さらに、SPP 管理者は、次の API を使用して、管理者権限に基づいて追加のイベントをサブスクライブできます。

POST /service/core/v3/EventSubscribers

8.2　パスワードリリースリクエストワークフロー

SPP は、アカウントパスワードを必要になるまで保存し、許可された人だけにリリース（公開）することで、管理アカウントを安全に制御します。その後、SPP は、構成可能なパラメーターに基づいてアカウントのパスワードを自動的に更新します。

通常、パスワードリリースリクエストは次のようなワークフローで行われます：

1. **リクエスト**：
   資格の承認済みユーザーとして指定されたユーザーは、その資格のポリシーの範囲内で任意のアカウントのパスワードをリクエストすることができます。

2. **承認**：
   セキュリティポリシー管理者がどのようにポリシーを構成するかによって、パスワードリリースリクエストは、1 人以上の SPP ユーザーによる承認を必要とするか、自動承認されるかのいずれかになります。このプロセスは、アカウントパスワードのセキュリティを確保し、説明責任を果たし、システムアカウントに対する二重の制御を提供します。

3. **レビュー**：
   セキュリティポリシー管理者は、オプションとしてポリシーの範囲内のアカウントに対して完了したパスワードリリースリクエストのレビューを要求するようにアクセスリクエストポリシーを設定することができます。

8.2.1　パスワードリリースのリクエスト

資格の許可ユーザーとして指定されている場合は、資格のポリシーの範囲内で任意のアカウントのパスワードをリクエストすることができます。

SPP を構成して、パスワードリリースリクエストが保留中、拒否、または取り消された場合など、保留中のパスワードリリースワークフローイベントを通知することができます。詳細については、「アラートの構成」を参照してください。

パスワードリリース手順

1. **［ホーム］**をクリックし、**［新しいリクエスト］**をクリックするか、**私のリクエスト**ページで **＋［新しいリクエスト］**をクリックします。

> **メモ：**以前にお気に入りとして保存したアクセスリクエストは、**［お気に入り］**ペインから送信することもできます。

2. **［新しいアクセスリクエスト］**ページで、アクセスリクエストに含まれるアカウントと選択したアカウントごとにアクセスタイプを選択します。資産情報に基づいてアカウントを検索することができます。選択可能な資産は、資格のアクセスリクエストポリシーで定義されているスコープに基づきます。

   > **メモ：** ボタンを使用すると、表示する列を選択することができます。

   - **資産**：管理対象システムの表示名
   - **アカウント**：使用可能なアカウントが**［アカウント］**列に表示されます。**［アカウントリクエストの可用性を表示］**が有効の場合、特権アカウントが利用可能かどうかを識別することができます。リクエストで使用中の場合、アカウントに **警告**マークが表示されます。複数のユーザーからのアカウント申請が重ならないように、アカウントのステータスは変更後すぐに更新されます。マークにカーソルを合わせると、「<X>アカウントのうち<X>個が使用中」と表示されます。アカウントの使用状況を表示するには、追加の API クエリが必要であるため、パフォーマンスに影響を与える可能性があります。このオプションは、管理者ではなくユーザーが設定します。グローバルなオプションはありません。

     > **注意:** リクエストを管理するポリシーで**［複数ユーザーの同時アクセスを許可］**が有効になっている場合、**［アカウントリクエストの可用性を表示］**で使用中と表示されていても、リクエストはまだ使用可能である可能性があります。

   - **アクセスタイプ**：アクセスリクエストのタイプが**［アクセスタイプ］**列に表示されます。タイプがハイパーリンクの場合、複数のアクセスリクエストタイプを使用できます。ハイパーリンクを選択し、アクセスタイプを選択します。タイプがドロップダウンの場合、複数のアクセスリクエストタイプが利用可能です。ドロップダウンを開き、アクセスタイプ（例：パスワード、RDP、SSH、SSH キー、Telnet）を選択します。
   - **アカウントの説明：**該当する場合、アカウントの説明が表示されます。
   - **資産の説明：**該当する場合、資産の説明が表示されます。

   グリッド内のエントリに関連付けられたチェックボックスをクリアすることで、リストからアカウントを削除することができます。

3. **［リクエストの詳細］**で、選択したすべての資産とアカウントに適用される次の設定を構成します。

a. **緊急アクセス**：ポリシーで緊急アクセスが有効になっている場合、このオプションを選択すると、このパスワードへの緊急アクセスが直ちに行われます。緊急アクセスを使用する場合、リクエストの承認は必要ありません。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

b. **いつですか**：以下のいずれかのオプションを選択します：

   i. **今すぐ**：選択すると、リクエストが即時作成されます。

   ii. **後で**：選択すると、ユーザーの現地時間でのリクエストの日時を入力するフィールドが表示されます。

c. **期間は？**：ポリシーに基づいて、次のいずれかを実行します：

   - **チェックアウト期間**を表示します。
   - ポリシーで**［要求者に期間の変更を許可］**オプションが有効になっている場合、パスワードを使用する日、時間、および分を設定することができます。これは、アクセスリクエストポリシーで設定された**チェックアウト期間**より優先されます。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

d. **チケット番号**：ポリシーでチケット番号が必要な場合、チケット番号を入力します。複数のアカウントがリクエストに含まれ、1 つ以上のアカウントがチケット番号を必要とする場合、チケット番号はこのアクセスリクエストに関連付けられているすべてのリクエストに適用されます。詳細については、「チケットシステム」を参照してください。

e. **理由**：ポリシーで理由が必要な場合は、理由を入力します。複数のアカウントがリクエストに含まれ、1 つ以上のアカウントが理由を必要とする場合、理由はこのアクセスリクエストに関連付けられているすべてのリクエストに適用されます。詳細については、「理由」を参照してください。

   選択した理由に対して定義された説明を表示するには、**［説明］**の下矢印を選択します。

f. **コメント**：必要に応じて、このリクエストに関する情報を入力します。リクエストに複数のアカウントが指定されている場合、選択したアカウントのいずれかがコメントを必要とする場合、コメントを入力する必要があります。このコメントは、このアクセスリクエストに関連付けられているすべてのリクエストに適用されます。入力できる文字数の上限は、1000 文字です。

4. アクセスリクエストをお気に入りとして保存するには、**［このリクエストをお気に入りとして保存します］**をチェックし、お気に入りの名前を入力します。

このリクエストは、**[お気に入り]** に追加されます。お気に入りは **ホーム**ページと **私のリクエスト**ページに表示されます。

5. 必要な情報を入力したら、**[リクエストの送信]** をクリックします。

   送信されたアクセスリクエストが失敗した場合は、追加情報が表示され、問題への対処方法が示されます。問題を解決してから、リクエストを再送信してください。

リクエストが承認されると、パスワードを使用できます。詳細については、「パスワードリリースリクエストに対するアクションの実行」を参照してください。

パスワードリリースリクエストに対するアクションの実行

パスワードリリースリクエストに対して実行できるアクションは、リクエストの状態と使用しているクライアントインターフェイスによって異なります。

パスワードリリースリクエストでのアクション手順

1. Web クライアントから、**[私のリクエスト]** をクリックします。表示されるリクエストを制御するには、次のいずれかの方法を使用します。
   - をクリックし、利用可能なすべてのリクエストをチェックインするには **[利用可能なすべてをチェックイン]**、すべてのリクエストを削除するには **[すべて消去]**、すべての保留中のリクエストをキャンセルして削除するには **[保留中のすべての承認を削除]** を選択します。
   - **[ソート]** をクリックし、[アカウント名]、[資産名]、[次回期限]、[次回失効]、[最新]、[ステータス] のいずれかを選択してソートします。
   - **[昇順]** または **[降順]** をクリックすると、昇順または降順でソートされます。
   - **[フィルタ]** をクリックすると、ステータスでフィルタリングします。
     - **利用可能**：表示またはコピーする準備ができている承認済みリクエスト
     - **承認が保留中**：承認が保留中のリクエスト
     - **承認済み**：承認されたが、チェックアウト期間に達していないリクエスト。または、SPP の一時停止機能を使用したときに復元された保留中のアカウントの場合

- **取り消し済み**：承認されたリクエストが承認者によって取り消されたもの。承認者は、リクエストが利用可能になった後に、リクエストを取り消すことができます。
- **失効**：チェックアウト期間が経過したリクエスト
- **拒否**：承認者によって拒否されたリクエスト

- **［検索］**をクリックすると、検索可能な要素のリストが表示されます。または、検索文字を入力します。詳細については、「検索ボックス」を参照してください。
- 拒否または取り消しされたリクエストに承認者がコメントをつけている場合、リクエストに関連する ボタンをクリックしてコメントを表示することができます。

2. パスワードリリースリクエストに対して、次のアクションのいずれかを実行できます：
   - **［利用可能］**なリクエスト：ユーザーインターフェイスに基づいてリクエストを選択します。
     - 名前、アカウント、残り時間が表示されます。
     - ブラウザーで許可されている場合は、**［コピー］**をクリックして、パスワードをチェックアウトします。これにより、パスワードがクリップボードに保存され、すぐに使用できるようになります。または、**［表示］**をクリックすると、パスワードがチェックアウトされ、パスワードが表示されます。パスワードは 20 秒間画面に表示されます。Web クライアントは、パスワードを 10,000 文字まで表示し、残りを切り捨てますが、API では 1MB 以下の任意の設定パスワードペイロードを許可します。チェックアウト中にパスワードが変更され、現在のリクエストがまだ有効な場合は、コピーまたは再表示のいずれかを選択して、新しいパスワードを取得してください。
     - **［非表示］**を選択すると、情報が表示されなくなります。
     - 作業が完了したら、**［リクエストのチェックイン］**をクリックして、パスワードのチェックアウトプロセスを完了します。
   - **［承認済み］**リクエスト：**［リクエストのキャンセル］**を選択すると、リクエストが削除されます。リクエストされた時間に達すると、パスワードリリースリクエストは**［承認済み］**から**［利用可能］**に変更されます。このリクエストはキャンセルするか、期間が終了するまで利用できます。
   - **［保留中］**のリクエスト：**［リクエストのキャンセル］**を選択すると、リクエストが削除されます。

- **［取り消し済み］**リクエスト：**［再送信］**を選択すると、パスワードの再リクエストができます。
- **［期限切れ］**のリクエスト：**［リクエストの削除］**を選択すると、リストからリクエストが削除されます。
- **［拒否］**されたリクエスト：**［再送信］**を選択すると、パスワードを再度リクエストします。
  リストからリクエストを削除するには、**［リクエストの削除］**を選択します。

8.2.2 パスワードリリースリクエストの承認

セキュリティポリシー管理者がポリシーをどのように構成したかに応じて、パスワードリリースリクエストは、1 人以上の SPP ユーザーによる承認を必要とするか、自動承認されるかのどちらかになります。このプロセスにより、アカウントパスワードのセキュリティが確保され、説明責任が果たされ、システムアカウントの二重管理が可能になります。

要求者がリクエストを閲覧してからチェックインするまでの間に、リクエストを取り消すことができます。

資格のある承認者は、パスワードリリースリクエストがすでに承認または自動承認された後でも、その要求を拒否することができます。一度拒否されると、要求者はそのパスワードにアクセスできなくなりますが、再度そのパスワードをリクエストする別の機会が与えられます。要求者は、リクエストが拒否されたことを通知するメールを受け取ります。

SPP は、承認が必要なパスワードリリースリクエストを通知するように構成することができます。詳細については、「アラートの構成」を参照してください。

パスワードリリースリクエストの承認または拒否手順

ページの左側にある**［承認］**をクリックして承認を管理します。**承認**ページでは、次のことができます:

- 詳細の表示：リクエストを選択すると、ページの右側に詳細が表示されます。
- 1 つ以上のリクエストを承認：リクエストを選択し、**［選択されたすべてのリクエストを承認］**をクリックして、選択したすべてのリクエストを承認します。必要に応じて、コメントを入力します。
- 1 つ以上のリクエストを拒否：リクエストを選択し、**［選択されたすべてのリクエストを拒否］**をクリックして、選択したすべてのリクエストを拒否します。必要に応じて、コメントを入力します。

- **表示する列を変更**：をクリックして表示させたい列を選択します。以下の列を選択できます：
    - アクション：**［このリクエストのみ承認］**と**［このリクエストのみ拒否］**が表示されます。
    - **要求者/ステータス**：ユーザー名とステータス（例：1 件の承認が保留中）が表示されます。
    - **資産/資産タイプ**：資産名とアクセスタイプ（例：パスワード、SSH キー、RDP、SSH、Telnet）が表示されます。
    - **アカウント：**管理アカウントの名前が表示されます。
    - **チケット番号**：必要に応じてチケット番号が表示されます。
    - **リクエスト期間**：利用可能な日時（例：2021 年 3 月 20 日 9:56 2 時間）が表示されます。
- **検索**：詳細については、「検索ボックス」を参照してください。

8.2.3 完了したパスワードリリースリクエストのレビュー

セキュリティポリシー管理者は、アクセスリクエストポリシーを構成して、ポリシーの範囲内のアカウントに対して完了したパスワードリリースリクエストのレビューを要求することができます。

SPP を構成して、レビューが必要なパスワードリリースリクエストを通知することができます。詳細については、「アラートの構成」を参照してください。

完了したパスワードリリースリクエストのレビュー手順

ページの左側にある**［レビュー］**を選択します。レビューページでは、次のことができます：

- リクエストを選択すると、ページの右側に詳細が表示されます。
- 1 つ以上のリクエストをレビュー済みとしてマーク：リクエストを選択し、以下を行います。
    - コメントが不要な場合：**［選択したすべてのリクエストをレビュー済みとしてマーク］**をクリックします。
    - コメントが必要な場合：**［選択したリクエストの 1 件以上でレビューコメントが必要です］**が表示されます。コメントを追加し、**［レビュー済みとしてマーク］**をクリックします。

- **表示する列の変更**： をクリックし、表示する列を選択します。
    - アクション：**［このリクエストでは、レビューコメントが必要です］**と**［このリクエストのみレビュー済みとしてマーク］**が表示されます。
    - **要求者**：要求者のユーザー名が表示されます。
    - **アクセスタイプ**：アクセスタイプ（例：パスワード、SSH キー、RDP、SSH、Telnet）が表示されます。
    - **アカウント：**管理アカウントの名前が表示されます。
    - **チケット番号：**必須の場合チケット番号が表示されます。
    - **リクエスト期間/リクエストされた期間：**利用可能な日時（例：2021 年 3 月 20 日 9:56 2 時間）が表示されます。
- **検索**：詳細については、「検索ボックス」を参照してください。

8.3 SSH キーリリースリクエストワークフロー

SPP は、SSH キーを必要な時まで保管し、許可された人にのみリリースすることで、管理対象アカウントの安全な制御を提供します。SPP は、設定可能なパラメーターに基づいて、自動的にアカウントの SSH キーを更新します。

通常、SSH キーのリリースリクエストは次のようなワークフローで行われます。

1. **リクエスト**：資格で権限を与えられたユーザーとして指定されたユーザーは、その資格のポリシーの範囲内で任意のアカウントの SSH キーをリクエストすることができます。
2. **承認**：ポリシー構成により、自動、またはシステムアカウントに対するより密接な制御を提供する 1 人以上のユーザーの同意を必要とすることができます。
3. **レビュー**：セキュリティポリシー管理者は、任意でアクセスリクエストポリシーを構成して、ポリシーの範囲内のアカウントに対して完了した SSH キーリリースリクエストのレビューを要求することができます。

8.3.1 SSH キーリリースのリクエスト

資格で権限を与えらえたユーザーとして指定されている場合、資格のポリシーの範囲内の任意のアカウントの SSH キーをリクエストすることができます。

SSH キーリリースリクエストが保留中、拒否、取り消された場合など、保留中の SSH キーリリースワークフローイベントを通知するように SPP を構成することができます。詳細については、「アラートの構成」を参照してください。

SSH キーのリリースリクエスト手順

1. **［ホーム］**をクリックして**［新しいリクエスト］**をクリックするか、**［私のリクエスト］**を開いて**［新しいリクエスト］**をクリックします。

   > **メモ：**以前にお気に入りとして保存した場合は、お気に入りペインからアクセスリクエストを送信することもできます。

2. **新しいアクセスリクエスト**ページで、アクセスリクエストに含めるアカウントと、選択した各アカウントに要求するアクセスの種類を選択します。アカウントは、資産情報に基づいて検索することができます。選択可能な資産は、資格のアクセスリクエストポリシーで定義されたスコープに基づいています。

3. ボタンを使用して、表示する列を選択します。

   - **資産**: 管理対象システムの表示名
   - **アカウント**：利用可能なアカウントが表示されます。資産に利用可能な複数のアカウントがある場合、**［アカウントの選択］**またはアカウント名がハイパーリンクとして表示されます。ハイパーリンクをクリックすると、利用可能なアカウントのリストが表示され、アクセスリクエストに含めるアカウントを選択できます。
   - **アクセスタイプ**：アクセスリクエストの種類が表示されます。ドロップダウンの場合、ドロップダウンをクリックすると、複数のアクセスリクエストタイプが利用できます。ドロップダウンをクリックして、アクセスタイプ（この場合は、**SSH キー**）を選択します。
   - **アカウントの説明**：（該当する場合）アカウントの説明
   - **資産の説明**：（該当する場合）資産の説明

   表のエントリに関連するチェックボックスをオフにすると、リストから資産またはアカウントを削除することができます。

4. **［次へ］**をクリックします。

5. **リクエストの詳細**で、選択したすべての資産とアカウントに適用される以下の設定を行います。

   a. **緊急アクセス**：ポリシーで緊急アクセスを有効にしている場合、このオプションを選択すると、この SSH キーに緊急にアクセスできます。**緊急アクセス**

を使用する場合、リクエストの承認は必要ありません。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

b. **いつですか？**:次のオプションのいずれかを選択します。

   i. **今すぐ**：選択すると、リクエストが直ちに作成されます。

   ii. **後で**：選択すると、ユーザーのローカルタイムでリクエストの特定の日時を入力するフィールドが表示されます。

c. **期間は？**：ポリシーに基づいて、次のいずれかを実行します。

   - チェックアウト期間を表示します。
   - ポリシーで**［要求者に期間の変更を許可する］**オプションが有効になっている場合、パスワードを使用する日時を設定することができます。これは、アクセスリクエストポリシーで設定されたチェックアウト期間より優先されます。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

d. **チケット番号**：チケット番号が必要な場合、チケット番号を入力します。複数のアカウントがリクエストに含まれ、1 つ以上のアカウントがチケット番号を必要とする場合、チケット番号はこのアクセスリクエストに関連するすべてのリクエストに適用されます。詳しくは、「チケットシステム」を参照してください。

e. **理由**：理由が必要な場合、理由を入力します。複数のアカウントがリクエストに含まれ、1 つ以上のアカウントが理由を必要とする場合。理由は、このアクセスリクエストに関連付けられているすべてのリクエストに適用されます。詳細については、「理由」を参照してください。

   選択した**理由**に対して定義された説明を表示するには、**［説明］**の下矢印を選択します。

f. **コメント**：必要な場合、このリクエストに関する情報を入力します。リクエストに複数のアカウントが指定されている場合、選択したアカウントのいずれかがコメントを必要とする場合、コメントを入力する必要があります。このコメントは、このアクセスリクエストに関連するすべてのリクエストに適用されます。入力できる文字数の上限は、1000 文字です。

6. アクセスリクエストをお気に入りとして保存するには、**［このリクエストをお気に入りとして保存します］**チェックボックスを選択し、名前を入力します。

   このアクセスリクエストが**［お気に入り］**に追加されます。お気に入りは **［ホーム］**ページと **［私のリクエスト］**ページに表示されます。

7. 必要な情報を入力したら、**［リクエストの送信］**をクリックします。

   送信したアクセスリクエストが失敗した場合、追加情報が表示され、問題への対処方法が表示されます。問題が解決されると、リクエストを再送信することができます。

リクエストが承認されると、SSH キーを使用できるようになります。詳細については、「SSH キーリリースリクエストに対するアクション」を参照してください。

SSH キーリリースリクエストに対するアクション

SSH キーリリースリクエストに対して実行できるアクションは、リクエストのステータスに依存します。

SSH キーリリースリクエストに対してのアクション実行手順

1. **［私のリクエスト］**をクリックします。次のいずれかの方法を使用して、表示されているリクエストを制御します。
   - をクリックし、利用可能なすべてのリクエストをチェックインするには**［利用可能なすべてチェックイン］**、すべてのリクエストを削除するには**［すべてクリア］**、保留中のすべてのリクエストをキャンセルして削除するには**［リクエストされたすべての保留中のリクエストをキャンセル］**を選択します。
   - **［ソート基準］**をクリックし、［アカウント名］、［資産名］、［次回期限］、［最新］、［ステータス］のいずれかを選択します。
   - **［昇順］**または**［降順］**をクリックすると、昇順または降順に並べ替えられます。
   - **［フィルタ］**をクリックすると、ステータスでフィルターをかけることができます。
     - **利用可能**：承認されたリクエストで、表示またはコピーする準備ができています。
     - **承認が保留中：**承認を待っているリクエスト
     - **承認済み**：承認はされたが、チェックアウト時刻が来ていないリクエスト。または、SPP のサスペンド機能を使用したときに復元された保留中のアカウント

- **取り消し済み**：承認されたリクエストが承認者によって撤回されたもの。承認者は、リクエストが利用可能になった後に、リクエストを取り消すことができます。
- **失効**：チェックアウト期間が経過したリクエスト
- **拒否**：承認者によって拒否されたリクエスト

- **［検索］**をクリックすると、検索可能な要素のリストが表示されます。または、検索文字を入力します。詳しくは、「検索ボックス」を参照してください。
- 拒否または取り消しが承認者によってコメントされている場合、リクエストに関連する ボタンをクリックしてコメントを表示することができます。

2. SSH キーリリースリクエストに対して、次のいずれかのアクションを実行できます。
   - 利用可能なリクエスト：リクエストの選択を行います。
     a. 名前、アカウント、残り時間が表示されます。追加情報を見るにはタイルをクリックするか、**［SSH キーの取得］**ボタンを使用します。
     b. 必要に応じて形式（OpenSSH、SSH2、PuTTY）を選択します。選択した形式は、次回のアクセスリクエストのデフォルトとして事前選択されます。
     c. SSH キーをチェックアウトするには、**［SSH キーのチェックアウト］**をクリックします。これで SSH キーがクリップボードに保存され、すぐに使用できるようになります。
     d. **［SSH セッションの開始］**をクリックすると、セッションが開始されます。
     e. **秘密キー**：**［保存］**または **［コピー］**をクリックすることができます。
     f. **パスフレーズ**：アクセスリクエストポリシーの作成時に**［パスフレーズによる SSH キーの保護］**をオンにした場合、**［表示］**または **［コピー］**をクリックすることができます。
     g. 選択した形式に応じて、次のような情報が表示されます。
        - **SHA-1 フィンガープリント**
        - **MD5 フィンガープリント**
        - **公開キー**：**［保存］**または **［コピー］**をクリックできます。

SSH キーをチェックアウトしている間に SSH キーが変更され、現在のリクエストがまだ有効である場合、以下を選択して新しい SSH キーを入手することができます：(利用可能な場合) **[保存]**、**[コピー]**、**[表示]** のいずれかを選択します。

h. 作業が完了したら、**[リクエストのチェックイン]** をクリックして、SSH キーのチェックアウト処理を完了します。

- **承認済み**リクエスト：リクエストを削除するには、**[リクエストのキャンセル]** を選択します。

  SSH キーリリースリクエストは、リクエストされた時間に達すると、承認済みから**利用可能**に変わります。リクエストを取り消すか、期間終了になるまで利用可能な状態になります。

- **保留中**のリクエスト：リクエストを取り消すには、**[リクエストのキャンセル]** を選択します。

- **取り消された**リクエスト：**[再送信]** を選択すると、SSH キーを再度リクエストできます。**[リクエストの削除]** を選択すると、リストからリクエストが削除されます。

- **失効した**リクエスト：**[リクエストの削除]** を選択して、リストからリクエストを削除します。

- **拒否された**リクエスト：**[再送信]** を選択すると、SSH キーを再度リクエストできます。**[リクエストの削除]** を選択すると、リストからリクエストが削除されます。

8.3.2 SSH キーリリースリクエストの承認

SSH キーリリースリクエストが 1 人以上の SPP ユーザーの承認を必要とするか、自動承認されるかは、セキュリティポリシー管理者がどのようにポリシーを構成したかにより変わります。

要求者は、リクエストを表示してからチェックインするまでの間に、リクエストを取り消すことができます。

承認者は、すでに承認または自動承認された後に、SSH キーリリースリクエストを拒否することができます。拒否されると、要求者はその SSH キーにアクセスできなくなりますが、その SSH キーを再度リクエストすることができます。要求者は、リクエストが拒否されたことを通知するメールを受け取ります。

SPP は、自分が承認しなければならない SSH キーリリースリクエストを通知するように設定することができます。詳細については、「アラートの構成」を参照してください。

SSH キーリリースリクエストの承認または拒否手順

ページの左側にある **［承認］** をクリックして、承認を管理します。**［承認］** ページでは、次のことが可能です：

- リクエストを選択すると、ページの右側に詳細が表示されます。
- 1 つまたは複数のリクエストを承認：リクエストを選択し、**［選択されたすべてのリクエストを承認］** をクリックすると、選択されたすべてのリクエストが承認されます。任意で、コメントを入力します。
- 1 つまたは複数のリクエストを拒否：リクエストを選択し、**［選択されたすべてのリクエストを拒否］** をクリックすると、選択されたすべてのリクエストを拒否することができます。任意で、コメントを入力します。
- 表示する列を変更する：をクリックし、表示する列を選択します。以下のような列を選択できます。
    - **アクション**：**［このリクエストのみ承認］** と **［このリクエストのみ拒否］** が表示されます。
    - **要求者/ステータス**：ユーザー名と承認ステータス（例：1 件の承認が保留中）が表示されます。
    - **資産/資産タイプ**：資産の名前とアクセスの種類（例：パスワード、SSH キー、RDP、SSH、Telnet）が表示されます。
    - **アカウント**：管理アカウント名を表示します。
    - **チケット番号**：必要な場合は、チケット番号が表示されます。
    - **リクエスト期間：**利用可能期限が表示されます。（例：2022 年 3 月 20 日 9:56 2 時間）。
- 検索：詳しくは、「検索ボックス」を参照してください。

8.3.3 完了した SSH キーリリースリクエストのレビュー

セキュリティポリシー管理者は、アクセスリクエストポリシーを設定して、ポリシーのスコープ内のアカウントの完了した SSH キーリリースリクエストのレビューを要求することができます。

レビューが必要な SSH キーリリースリクエストを通知するように設定することができます。詳細については、「アラートの構成」を参照してください。

完了した SSH キーリリースリクエストのレビュー手順

レビューを管理するには、ページの左側にある **［レビュー］**を選択します。レビューページでは、次のことが可能です：

- リクエストを選択すると、ページの右側にワークフローを含む詳細が表示されます。
- 1 つまたは複数のリクエストをレビュー済みとしてマークします：リクエストを選択し、次の操作を行います：
    - コメントが不要な場合は、**［選択したすべてのリクエストをレビュー済みとしてマーク］**をクリックします。
    - コメントが必要な場合は、**［選択したリクエストの 1 件以上でレビューコメントが必要です］**が表示されます。コメントを追加し、**［レビュー済みとしてマーク］**をクリックします。
- 表示する列を変更する。をクリックし、表示する列を選択します。
    - **アクション**：**［このリクエストでは、レビューコメントが必要です］**と**［このリクエストのみレビュー済みとしてマーク］**が表示されます。
    - **要求者**：要求者のユーザー名が表示されます。
    - **アクセスタイプ**：アクセスタイプ（例：パスワード、SSH キー、RDP、RDP アプリケーション、SSH、Telnet）が表示されます。
    - **アカウント：**管理アカウントの名前が表示されます。
    - **チケット番号：**必須の場合チケット番号が表示されます。
    - **リクエスト期間/リクエストされた期間：**利用可能な日時（例：2021 年 3 月 20 日 9:56 2 時間）が表示されます。
- **検索**：詳細については、「検索ボックス」を参照してください。

8.4　セッションリクエストワークフロー

権限を付与されたユーザーは、接続の承認、アクティブな接続の表示、特定のリソースへのアクセス制限、接続が事前に設定された制限時間を超えた場合のアラート、接続の終了を行うことができます。

通常、セッションリクエストは以下のワークフローで行われます。

1. **リクエスト**：資格の承認済みユーザーとして指定されたユーザーは、その資格のポリシーの範囲内で任意の資産へのセッションをリクエストすることができます。

2. **承認**：セキュリティポリシー管理者がポリシーをどのように構成したかによって、セッションリクエストは 1 人以上の SPP ユーザーによる承認を必要とするか、自動承認されるかのどちらかになります。

3. **レビュー**：セキュリティポリシー管理者は、オプションでアクセスリクエストポリシーを構成して、ポリシーの範囲内の資産に対する完了したリクエストのレビューを要求することができます。また、ポリシーでセッションの記録が有効になっている場合、レビュー担当者はレビュープロセスの一環として、ワークフロートランザクションを監査し、デスクトッププレーヤーを起動して、セッションを再生することができます。

8.4.1 セッションと記録について

SPP は、すべてのセッションをターゲットリソースにプロキシします。ユーザーはリソースに直接アクセスできないため、ユーザーのシステム上のウイルス、マルウェア、その他の危険なアイテムから企業を保護することができます。Safeguard は、Unix/Linux、Windows、ネットワークデバイス、ファイアウォール、ルーターなどをプロキシして記録することができます。

> **メモ：** SSH セッションのリクエストには PuTTY を、RDP セッションのリクエストには MSTSC を使用して SSH クライアントを起動します。PuTTY または MSTSC を使用したセットアップ方法については、SCALUS を参照してください。

重要な注意事項

- セッションリクエストはデフォルトで有効になっています。権限を付与されたユーザーがセッションをリクエストできない場合は、Web クライアントの **[セッションリクエスト]**（**[アプライアンス管理]** > **[サービスの有効化または無効化]**）をオンにしてください。

  > **メモ：** サービス設定を管理するには、アプライアンス管理者の権限が必要です。

- すべてのセッションアクティビティ（送信されたすべてのパケット、マウスの動き、クリック、キーストロークなど、画面上で行われたすべてのアクション）が記録され、再生できるようになります。
- 特権セッション中に SPP が 10 分間アクティビティがないことを検出した場合、そのセッションはクローズされます。

8.4.2 セッションアクセスのリクエスト

資格の許可ユーザーとして指定されている場合、資格のポリシーの範囲内で、任意のアカウントまたは資産への特定の期間（またはセッション）のアクセスをリクエストすることができます。

SPP を構成して、セッションリクエストが保留中、拒否、または取り消されたときなど、保留中のアクセスリクエストワークフローイベントを通知することができます。詳細については、「アラートの構成」を参照してください。

セッションアクセスのリクエスト手順

1. **［ホーム］**または**［私のリクエスト］**をクリックし、**［新しいリクエスト］**をクリックします。

   > **メモ：**以前にお気に入りとして保存した場合は、**［お気に入り］**ペインからアクセスリクエストを送信することもできます。

2. **新しいアクセスリクエスト**ページで、アクセスリクエストに含めるアカウントと選択したアカウントをリクエストするためのアクセスタイプを選択します。選択可能な資産は、資格のアクセスリクエストポリシーで定義されているスコープに基づいています。

   アクセスリクエストの作成時に SPS_Initiated 接続ポリシーが選択されている場合、そのリクエストに関連付けられている資産は表示されません。SPS_Initiated に割り当てられたセッション関連のアクセスポリシーは除外されます。資産に対するアクセスリクエストを作成するには、SPS_Initiated 以外の接続ポリシーを選択する必要があります。

   > **メモ：** ボタンを使用して表示する列を選択します。

   - **資産**：管理対象システムの表示名
   - **アカウント**：使用可能なアカウントが**［アカウント］**列に表示されます。資産に利用可能な複数のアカウントがある場合、**［アカウントの選択］**またはアカウント名のいずれかが**［アカウント］**列にハイパーリンクとして表示されます。**［アカウント］**列のハイパーリンクをクリックすると、使用可能なアカウントのリストが表示され、アクセスリクエストに含めるアカウントを選択できます。
     ［アカウントリクエストの可用性を表示］を有効にすると、特権アカウントが使用可能かどうかを識別することができます。リクエストによって使用中の場合、アカウントには 警告バッジが表示されます。複数のユーザーからのアカウントリクエストが重複しないようにするため、アカウントの状態は変更されるとすぐに更新されます。バッジにカーソルを合わせると、<X>個のアカウントのうち<X>個が使用可能であることが表示されます。アカウントの使用

状況を表示するには、追加の API クエリが必要であり、パフォーマンスに影響を与える可能性があります。このトグルは、管理者ではなくユーザーが設定します。グローバルなトグルはありません。

> **メモ：**リクエストを管理するポリシーで**［同時アクセスを許可］**が有効になっている場合、［アカウントリクエストの空き状況を表示］で使用中と表示されていても、要求はまだ使用可能であることがあります。

- **アクセスタイプ**：アクセスリクエストのタイプが**［アクセスタイプ］**列に表示されます。複数のアクセスリクエストタイプが利用可能な場合、この値はハイパーリンクとして表示され、選択すると、アクセスタイプを選択するための追加のダイアログが表示されます。
- **アカウントの説明：**（該当する場合）アカウントの説明
- **資産の説明：**（該当する場合）資産の説明

表内のエントリに対応するチェックボックスをクリアすることでリストから資産またはアカウントを削除することができます。

3. **［次へ］**をクリックします。
4. **［リクエストの詳細］**で、次の設定を構成します。この設定は、すべての資産およびアカウントに適用されます。
    a. **緊急アクセス**：ポリシーで緊急アクセスが有効になっている場合は、このオプションを選択すると、このパスワードへの緊急アクセスが直ちに行われます。**緊急アクセス**を使用する場合、リクエストの承認は必要ありません。詳細については、「アクセスリクエストポリシーの作成」を参照してください。
    b. **いつですか**：以下のいずれかのオプションを選択します：
        i. **今すぐ**：選択すると、リクエストが即時作成されます。
        ii. **後で**：選択すると、ユーザーの現地時間でのリクエストの日時を入力するフィールドが表示されます。
    c. **期間は？**：ポリシーに基づいて、次のいずれかを実行します：
        - **チェックアウト期間**を表示します。
        - ポリシーで**［要求者に期間の変更を許可］**オプションが有効になっている場合、パスワードを使用する日、時間、および分を設定することができます。これは、アクセスリクエストポリシーで設定された**チェックアウト期間**より優先されます。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

d. **チケット番号**：ポリシーでチケット番号が必要な場合、チケット番号を入力します。複数のアカウントがリクエストに含まれ、1 つ以上のアカウントがチケット番号を必要とする場合、チケット番号はこのアクセスリクエストに関連付けられているすべてのリクエストに適用されます。詳細については、「チケットシステム」を参照してください。

e. **理由**：ポリシーで理由が必要な場合は、理由を入力します。複数のアカウントがリクエストに含まれ、1 つ以上のアカウントが理由を必要とする場合、理由はこのアクセスリクエストに関連付けられているすべてのリクエストに適用されます。詳細については、「理由」を参照してください。

選択した理由に対して定義された説明を表示するには、**[説明]**の下矢印を選択します。

f. **コメント**：必要に応じて、このリクエストに関する情報を入力します。リクエストに複数のアカウントが指定されている場合、選択したアカウントのいずれかがコメントを必要とする場合、コメントを入力する必要があります。このコメントは、このアクセスリクエストに関連付けられているすべてのリクエストに適用されます。入力できる文字数の上限は、255 文字です。

5. アクセスリクエストをお気に入りとして保存するには、**[このリクエストをお気に入りとして保存します]**をチェックし、お気に入りの名前を入力します。

   このリクエストは、**[お気に入り]**に追加されます。お気に入りは **ホーム**ページと **私のリクエスト**ページに表示されます。

6. 必要な情報を入力したら、**[リクエストの送信]**をクリックします。

   送信されたアクセスリクエストが失敗した場合は、追加情報が表示され、問題への対処方法が示されます。問題を解決してから、リクエストを再送信してください。

リクエストが承認されると、パスワードを使用できます。詳細については、「パスワードリリースリクエストに対するアクションの実行」を参照してください。

セッションが起動しない場合

まれに、アクセスリクエストが起動可能なセッションリクエストにならない場合、次のような通知が表示されます。

- Please try again. The linked sessions module state is currently down or may be in a locked state.

  このメッセージは、次のいずれかを意味する場合があります。

  - SPP は SPS に接続できませんでした。リクエストを SPS クラスタ内の別の管理対象ホストにリダイレクトできるように、再試行してください。

- SPS の構成がロックされています。この状態は通常、新しいアクセスリクエストの作成またはセッションの開始と同時に、SPS 管理者が SPS アプライアンスに対して構成変更を行っているため、再試行してください。

- Missing the session connection policy.

  または

  The selected Access Request Policy cannot be used to initiate a session from SPP. The highest priority policy must be associated with a valid SPS connection policy.

  接続ポリシーの構成を確認してください。クライアントで、有効な接続ポリシー（**[セキュリティポリシー管理]** > **[資格]** > **（編集）** > **[アクセスリクエストポリシー]**）を追加します。ポリシーを保存して、アクセスリクエストを再作成します。

セッションリクエストに対するアクションの実行

特権セッションへのアクセスリクエストを許可されたユーザーが実行できるアクションは、リクエストのステータスと使用しているクライアントインターフェイスによって異なります。

セッションリクエストに対するアクションの実行手順

1. Web クライアントから、**[私のリクエスト]** をクリックします。
2. 検索して必要なものを見つけます。詳細については、「検索ボックス」を参照してください。
3. ステータスでフィルタリングするには、**[フィルタ]** をクリックします。
   - **すべて**：すべてのステータスのリクエスト
   - **利用可能**：承認されたリクエストのうち準備ができたもの（つまり、起動可能なセッション）
   - **承認が保留中**：承認が保留中のリクエスト
   - **承認済み**：承認されたが、チェックアウト期間に達していないリクエスト
   - **取り消し済み**：承認されたリクエストが承認者によって取り消されたもの
     - 承認者は、リクエストが利用可能になった後でもリクエストを取り消すことができます。
     - セキュリティポリシー管理者権限を持つユーザーがライブセッションを取り消した場合、アクティブなセッションはクローズされます。
   - **失効**：チェックアウト期間が経過したリクエスト

- **拒否**：承認者によって拒否されたリクエスト

4. リクエストの種類によっては、タイルをクリックすると追加情報が表示される場合があります。

5. ステータスに応じて、セッションリクエストに対して次のアクションを実行できます：
    - **利用可能なリクエスト**：チェックアウト中にパスワードまたは SSH キーが変更され、現在のリクエストがまだ有効である場合、管理者が有効にしていれば、**［コピー］**またはもう一度 **［表示］**のいずれかを選択して新しいパスワードを取得します。
        - SSH および RDP アカウントの場合：
            - **［RDP セッションの開始/SSH セッションの開始］**をクリックして、SSH クライアントまたは RDP 接続を起動します。詳細については、「SSH クライアントの起動」または「RDP セッションの起動」を参照してください。
            - セッションが終了したら、**［チェックイン］**をクリックしてチェックアウトプロセスを完了します。
            - さらに、セッションの起動に必要な資格情報を含むダイアログを表示したり、情報をコピーしたりするには、以下のボタンを使用することができます：
                - **［コピー］**をクリックすると、資格情報がチェックアウトされコピーされます。
                - **［表示］**をクリックすると、資格情報がチェックアウトされ、表示されます。
        - telnet または TN3270/TN5250 アカウントの場合、必要なフィールドは使用中のターミナルサービスアプリケーションに基づきます。
            - インバンド接続文字列（telnet など）を使用するターミナルサービスアプリケーションの場合、**［コピー］**をクリックしてホスト名接続文字列をコピーし、パスワードまたは SSH キーをチェックアウトします。次に、その情報をログイン画面に貼り付けます。
            - ターミナルサービスアプリケーションがログインのためにさらに多くの情報を必要とする場合（たとえば、Telnet 経由の TN3270/TN5250）：

- **［表示］**をクリックして、Vault アドレス（SPP アドレス）、ワンタイムトークン、ユーザー名、資産、セッションモジュール（SPS アドレス）を含む値を表示します。
- いずれかの値のそばにある **［コピー］**をクリックすると、１つの値がコピーされます。または、すべての値の右側にある **［コピー］**をクリックすると、ターミナルサービスアプリケーションで必要な場合、接続文字列全体がコピーされます。
- 必要な情報をターミナルサービスアプリケーションに貼り付けます。

◦ **［リクエストのチェックイン］**をクリックして、パスワードのチェックアウトプロセスを完了します。これにより、セッションリクエストがレビュー担当者に公開されます。

◦ **［非表示］**をクリックすると、情報が表示されなくなります。

◦ **［承認済み］**：**［リクエストのキャンセル］**を選択すると、リクエストが削除されます。セッションリクエストはリクエストされた時間に達すると、**［承認済み］**から**［利用可能］**に変わります。セッションリクエストは、ユーザーがリクエストをキャンセルするか、期間が終了するまで利用できます。

◦ **［保留中］**：**［リクエストのキャンセル］**をクリックすると、リクエストが削除されます。

◦ **［取り消し済み］**：

◦ **［再送信］**をクリックすると、パスワードまたは SSH キーが再度リクエストされます。

◦ **［リクエストの削除］**をクリックすると、リストからリクエストが削除されます。

◦ **［失効］**：**［リクエストの削除］**をクリックすると、リストからリクエストが削除されます。

◦ **［拒否］**：

◦ **［再送信］**をクリックすると、パスワードまたは SSH キーが再度リクエストされます。

◦ **［リクエストの削除］**をクリックすると、リストからリクエスターが削除されます。

8.4.3 セッションリクエストの承認

セキュリティポリシー管理者がポリシーをどのように構成したかによって、セッションリクエストは、1 人以上の SPP ユーザーの承認を必要とするか、自動承認されるかのいずれかになります。

SPP は、あなたの承認を必要とするアクセスリクエストを通知するように設定することができます。詳細については、「アラートの構成」を参照してください。

セッションリクエストの承認または拒否手順

ページの左側にある **［承認］**をクリックして承認を管理します。**［承認］**ページでは、次のことができます。

- リクエストを選択すると、ページの右側に詳細が表示されます。
- 1 つ以上のリクエストを承認：リクエストを選択し、**［選択されたすべてのリクエストを承認］**をクリックして、選択したすべてのリクエストを承認します。必要に応じて、コメントを入力します。
- 1 つ以上のリクエストを拒否：リクエストを選択し、**［選択されたすべてのリクエストを拒否］**をクリックして、選択したすべてのリクエストを拒否します。必要に応じて、コメントを入力します。
- **表示する列を変更**：をクリックして表示させたい列を選択します。以下の列を選択できます：
    - **アクション**：**［このリクエストのみ承認］**と**［このリクエストのみ拒否］**が表示されます。
    - **要求者/ステータス**：ユーザー名とステータス（例：1 件の承認が保留中）が表示されます。
    - **資産/資産タイプ**：資産名とアクセスタイプ（例：パスワード、SSH キー、RDP、SSH、Telnet）が表示されます。
    - **アカウント：**管理アカウントの名前が表示されます。
    - **チケット番号**：必要に応じてチケット番号が表示されます。
    - **リクエスト期間**：利用可能な日時（例：2021 年 3 月 20 日 9:56 2 時間）が表示されます。
- **検索**：詳細については、「検索ボックス」を参照してください。

8.4.4 SSH クライアントの起動

SSH セッションリクエストが使用可能になると、要求者は SSH クライアントを起動してセッションを開始することができます。

SSH クライアントを起動してセッションを開始し、その後セッションを閉じる手順

1. ポリシーで**［ユーザー指定］**オプションが選択されている場合、ユーザーの資格情報を入力するように求められます。リクエストされた資格情報を入力したら、**［適用］**をクリックします。これにより、SSH クライアントの起動に必要な情報（ホスト名、接続文字列など）が取得されます。

2. 資産名に関連するある ▶ **［SSH セッション開始］**ボタンをクリックします。Web クライアントでは、アプリケーションが登録されていれば、セッションが起動します（SSH プロトコルの場合は、ssh://）。

   > **メモ：** ▶ **［SSH セッションの開始］**オプションは、ユーザーの設定で有効化されている場合のみ利用できます。

3. SSH クライアントで、ターゲットホスト上のコマンドまたはプログラムを実行します。開いているセッションで 10 分程度操作がない場合、セッションはクローズされます。ただし、リクエストが**［利用可能］**ステータスであれば、再びセッションを起動してタスクを再開することができます。

4. 作業が完了したら、ターゲットホストからログアウトし、✔ **［チェックイン］**を選択して、セッションリクエストの処理を完了します。

8.4.5 RDP セッションの起動

RDP セッションリクエストが使用可能になると、要求者はリモートデスクトップ接続を起動してセッションを開始できます。

リモートデスクトップ接続の起動手順

1. ポリシーで**［ユーザー指定］**オプションが選択されている場合、ユーザーの資格情報を入力するように求められます。リクエストされた資格情報を入力したら、**［適用］**をクリックします。これにより、リモートデスクトップセッションの起動に必要な情報（たとえば、ユーザー名接続文字列）が取得されます。

2. Web クライアントで：

   > **メモ：** ▶**［SSH セッションの開始］**オプションは、ユーザーの設定で有効化されている場合のみ利用できます。

   - アプリケーションが登録されている場合（RDP セッションの場合は rdp://）、資産名の▶**［RDP セッションの開始］**ボタンをクリックしてから、**［接続］**をクリックします。アプリケーション登録の詳細については、KB 313918 を参照してください。パスワードの入力が必要ですが、sg をお勧めします。パスワードが空白の場合、セッションは失敗します。
   - アプリケーションを登録していない場合は、▶**［RDP セッションの開始］**ボタンを使用する代わりに、RDP 起動ファイルをダウンロードします。パスワードの入力が必要で、sg をお勧めします。パスワードが空白の場合、セッションに失敗します。

RDP セッションを開始し、そのセッションを閉じる手順

1. リモートデスクトップセッションで、ターゲットホスト上のでコマンドまたはプログラムを実行します。開いているセッションに 10 分程度操作がない場合、セッションは閉じられます。ただし、リクエストが**［利用可能］**ステータスであれば、再びセッションを起動してタスクを再開することができます。

2. 作業が完了したら、ターゲットホストからログアウトし、✔**［チェックイン］**を選択してセッションリクエストプロセスを完了します。

8.4.6 リモートデスクトップアプリケーションセッションの設定と起動

リモートデスクトップアプリケーションセッションリクエストを起動するには、いくつかの追加設定が必要です。

リモートデスクトップアプリケーションの設定と起動手順

1. 6.12 から利用できる SPS の RemoteApp ランチャーをインストールし、設定します。詳細については、『One Identity Safeguard for Privileged Sessions 管理ガイド』を参照してください。

2. Microsoft の説明に従って **OISGRemoteAppLauncher** アプリケーションを公開します。SPP/SPS を使用して起動するすべてのリモートアプリケーションは、OISGRemoteAppLauncher で起動するように構成する必要があり、目的のリモートアプリケーションを参照するコマンドラインを含める必要があります。リモートアプリケーションのプログラム名とエイリアスは、アクセスリクエストポリシーを設定する際に必要になるため、メモしておいてください。

3. **［資産管理］＞［資産］**で、以下の資産が必要です（詳細については、「資産の追加」を参照してください）。

    a. **Windows Server** 資産：この資産は、Windows アプリケーションサーバーと接続するために使用されます。

    b. **Other/Other Managed** 資産：（いずれかのプラットフォームタイプ）のこの資産は、リモートアプリケーションと接続するために使用されます。以下の設定が必要です：

        - **ネットワークアドレス**：なし
        - **認証タイプ**：なし
        - **［アカウント］**タブに追加されたリモートアプリケーションのアカウント

4. **［セキュリティポリシー管理］＞［資格］**で、Remote Desktop Application のアクセスリクエストポリシーを含む権限が必要です。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

5. SPS 内で、次の属性を含むチャネルポリシーを修正または作成する必要があります。このチャネルポリシーは、RDP 接続ポリシーから参照する必要があります。詳細については、『One Identity Safeguard for Privileged Sessions 管理ガイド』を参照してください。

    a. **RDP Control** > **Connections** で **applications** に **Channel policy** を設定します。

    b. **RDP Control** > **Channel Policies** で以下を作成します：

        i. **Dynamic virtual channel**：構成済み設定なし

        ii. **Custom**：**Permitted channels** に以下を追加します：
            - **rail**
            - **rail_ri**
            - **rail_wi**

リモートデスクトップアプリケーションセッションリクエストが利用可能になると、要求者はリモートデスクトップ接続を起動してセッションを開始することができます。

リモートデスクトップアプリケーション接続の開始手順

Web クライアントで 資産に関連付けられた ▶ **［RDP セッションの開始］**ボタンをクリックします。

> **メモ**：▶ **［RDP セッションの開始］**オプションは、ユーザー設定によって有効になっている場合、およびセッションクライアントアプリケーション起動 Uri システム（詳細については、「SCALUS」を参照）がインストールされている場合のみ使用できます。

> **メモ**：ランチャーがリモートデスクトップアプリケーションセッションをロードする際に、黒いウィンドウが画面に表示されることがあります。

8.4.7 セッションリクエストのレビュー

セキュリティポリシー管理者は、ポリシーの範囲内の資産またはアカウントに対して完了したセッションリクエストのレビューを要求するようにアクセスリクエストポリシーを構成することができます。

> **メモ：**SPP を構成して、レビューが必要なアクセスリクエストを通知することができます。詳細については、「アラートの構成」を参照してください。

Desktop Player ユーザーガイド

Safeguard Desktop Playerユーザーガイドが必要な場合は、「Safeguard Desktop Player ユーザーガイド」を参照してください。

完了したセッションリクエストのレビュー手順

レビューを管理するには、ページの左側にある **［レビュー］**を選択します。レビューページでは、次のことができます。

- リクエストを選択すると、ページの右側にワークフローを含む詳細が表示されます。
- 1 つまたは複数のリクエストをレビュー済みとしてマークします：リクエストを選択し、次の操作を行います：

- コメントが不要な場合は、**［選択したすべてのリクエストをレビュー済みとしてマーク］**をクリックします。
- コメントが必要な場合は、**［選択したリクエストの 1 件以上でレビューコメントが必要です］**が表示されます。コメントを追加し、**［レビュー済みとしてマーク］**をクリックします。

- 表示する列を変更する：をクリックし、表示する列を選択します。
  - **アクション**：**［このリクエストでは、レビューコメントが必要です］**と**［このリクエストのみレビュー済みとしてマーク］**が表示されます。
  - **要求者**：要求者のユーザー名が表示されます。
  - **アクセスタイプ**：アクセスタイプ（例：パスワード、SSH キー、RDP、RDP アプリケーション、SSH、Telnet）が表示されます。
  - **アカウント：**管理アカウントの名前が表示されます。
  - **チケット番号：**必須の場合チケット番号が表示されます。
  - **リクエスト期間/リクエストされた期間：**利用可能な日時（例：2021 年 3 月 20 日 9:56 2 時間）が表示されます。
- **検索**：詳細については、「検索ボックス」を参照してください。

9　アプライアンス管理

Web クライアントで、左側のナビゲーションペインで**［アプライアンス管理］**セクションを展開します。アプライアンス管理者、運用管理者、ブートストラップ管理者が利用できます（監査者は読み取り専用アクセス）。

9.1　アプライアンス

アプライアンス設定を使用して、アプライアンスの一般情報の表示、診断ツールの実行、SPP ハードウェアアプライアンスのリセットまたは更新を行います。

SPP は、仮想アプライアンスを使用するように設定することができます。詳細については、「仮想アプライアンスと Web 管理コンソールの使用」を参照してください。

［アプライアンス管理］＞［アプライアンス］に移動します。

SPP では、アプライアンスを導入して使用する際に遭遇する可能性のある多くの一般的な問題を解決するために、次の情報を提供しています。

表：アプライアンス設定

設定	説明
アプライアンスの診断	設定の問題、同期の問題、クラスタリングの問題、その他の内部問題の解決に役立つ、信頼できる安全な診断パッケージを実行することができます。
アプライアンス情報	アプライアンスに関する一般的な情報、パフォーマンス使用率、メモリ使用量を表示します。**アプライアンス名**と**ホスト DNS サフィックス**を編集することができます。
デバッグ	Syslog サーバーへのデバッグロギングを有効化/無効化することができます。
ライセンス	SPP ライセンスを追加/更新することができます。
ネットワーク診断	アプライアンスの診断テストを実行することができます。

設定	説明
ネットワーク	プライマリネットワークインターフェイス、および該当する場合はセッションネットワークインターフェイスを表示および設定することができます。
オペレーティングシステムのライセンス	仮想マシンでのみ利用できます。ハードウェアでは利用できません。仮想アプライアンスのオペレーティングシステムを設定することができます。
パッチの更新	パッチ更新ファイルをアップロードしてインストールすることができます。
電源	Web クライアントでアプライアンスをシャットダウンまたは再起動することができます。
SSH アルゴリズム	アカウントパスワードおよび SSH キーを管理するため SSH アルゴリズムを構成することができます。
Support Bundle	アプライアンスの問題を分析および診断するために One Identity Support に送信するシステムおよび構成情報を含むサポートバンドルが作成されます。
時間	Network Time Protocol（NTP）を有効にし、プライマリおよびセカンダリ NTP サーバーを設定することができます。クラスタのレプリカは、常にプライマリアプライアンスを NTP サーバーとして参照します。 プライマリの時間は手動で設定することができますが、クラスタではできません。 ⚠ **注意：手動で時刻を設定する場合は、注意が必要です。時間の変更は、重大なデータ損失の原因となることがあります。**
ファクトリーリセット	ハードウェアでのみ利用できます。仮想マシンでは利用できません。 アプライアンスを工場出荷時の状態に戻すために、工場出荷時のリセットを実行することができます。

設定	説明
ライトアウト管理 (BMC)	ハードウェアでのみ利用できます。仮想マシンでは利用できません。 ベースボード管理コントローラ（BMC）を使用して SPP の電源状態とシリアルコンソールをリモートで管理できるライトアウト管理を有効/無効にすることができます。

アプライアンスのオプションに加え、以下のトラブルシューティングツールがあります。

表：その他のトラブルシューティングツール

ツール	説明
アクティビティセンター	特定のイベントまたはユーザーアクティビティの詳細を表示します。詳細については、「アクティビティセンター」を参照してください。
LCD ステータスメッセージ	アプライアンスの起動時またはシャットダウン時に、アプライアンスのステータスを表示するためのアプライアンス上の LCD 画面です。詳細については、「LCD ステータスメッセージ」を参照してください。
リカバリキオスク（シリアル・キオスク）	アプライアンスの基本情報の表示、リモートでのアプライアンスの再起動、アプライアンスのシャットダウン、Bootstrap Administrator のパスワードの初期値へのリセット、工場出荷時の復元、Windows 共有へのサポートバンドルの生成と送信のためにアプライアンスに直接接続した端末またはノートパソコンです。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。

9.1.1 アプライアンスの診断

アプライアンス管理者は、信頼できる安全なアプライアンスの診断パッケージを実行して、構成、同期、およびクラスタリングに関する問題や、その他の内部課題の解決を支援することができます。アプライアンスの診断パッケージは、シリアルキオスク（リカバリキオスク）ではなく、Web サポートキオスクから利用できます。アプライアンスの診断パッケージは、アプライアンスが隔離された状態でも使用できます。外部の脅威から保護するために、SPP は不正なアプライアンスの診断パッケージを拒否します。アプライアンスの診断パッケージのマニフェストファイルには、SPP の最小バージョン、アプライアンス ID、有効期限のタイムスタンプ UTC など

の基準が記載されています。新しい製品コードとデータベースの変更は、アプライアンスの診断パッケージには含まれません。

［アプライアンス管理］＞［アプライアンス］＞［アプライアンスの診断］に移動します。

1. アプライアンスの状態が表示されます（例：**オンライン**）。状態を更新するには、**［更新］**をクリックします。

2. アプライアンスの診断パッケージがロードされていない場合、**［診断のアップロード］**をクリックし、拡張子が.sgd のアプライアンス診断パッケージファイルを選択し、**［開く］**をクリックします。
    - アップロード基準が満たされていない場合、アプライアンス診断パッケージはアップロードされず、次のようなメッセージが表示されます。「この診断パッケージを実行するために必要な Safeguard の最小バージョンは<version>です。」
    - アップロードが成功すると、診断パッケージ情報に**「ステージング」**のステータスが表示されます。
        - **［実行］**を選択し、**［ステータス］**が**［完了］**または**［エラー］**に変更されるまで待ちます。
        - **［削除］**を選択すると、アプライアンス診断パッケージと関連するログファイルが削除されます。

3. アップロードが完了すると、以下のアクティビティを実行できます。
    - **有効期限**が過ぎていない場合、**［実行］**を選択してアプライアンスの診断パッケージを再度実行することができます。
    - **［削除］**を選択すると、アプライアンス診断パッケージと関連するログファイルが削除され、実行中のアプライアンス診断パッケージが停止されます。アプライアンスごとにアプライアンス診断パッケージは 1 つしかないため、別のアプライアンス診断パッケージをアップロードする前に、現在の診断パッケージを削除する必要があります。
    - **［ログのダウンロード］**を選択して、ログファイルを保存します。監査ログエントリーは、実行中および実行後にアクティビティセンターから利用でき、アプライアンス履歴の一部となります。ログは、診断パッケージが削除されるまで、実行中および実行後にも利用可能です。

9.1.2 アプライアンス情報

アプライアンスのステータスを監視するのは、運用管理者またはアプライアンス管理者の責任です。

アプライアンス情報への移動：

- Web クライアントで、**［アプライアンス管理］＞［アプライアンス］＞［アプライアンス情報］**をクリックします。

更新：

- **［アプライアンス管理］＞［アプライアンス］＞［アプライアンス情報］**をクリックします。**［更新間隔］**で更新間隔（秒）を選択します。値が変更されると直ちに更新され、選択された値に基づいて次の更新がスケジュールされます。

以下の情報が表示されます。

表：アプライアンスプロパティ

プロパティ	説明
アプライアンス名	アプライアンスの名前。 アプライアンス管理者は名前を変更することができます。 **［編集］**をクリックし、**［アプライアンス名］**に新しい名前を入力して**［Save］**をクリックします。
ホスト DNS サフィックス	ホスト DNS サフィックス名。 アプライアンス管理者は名前を変更することができます。 **［編集］**をクリックし、**［ホスト DNS サフィックス］**に新しい DNS サフィックスを入力して**［Save］**をクリックします。
ホスト	アプライアンスネットワークサーバーの IP アドレス
アプライアンスのバージョン	SPP アプライアンスのバージョン
稼働時間	アプライアンスが稼働している時間（時間と分）
前回の起動日付	アプライアンスが最後に回起動された日付

全般タブ情報

ディスクには、ディスクの使用量と空き容量がグラフで表示されます。ディスク使用量が 80% を超えると、ログに反映されます（DiskUsageWarningEvent）。

表：全般タブ

プロパティ	説明
メーカー	システム製造元
モデル	システムのモデル
BIOS の説明	システムの BIOS 説明
BIOS のシリアル番号	システムの BIOS シリアル番号
シリアル番号	通信用ネットワークインターフェイスに割り当てられたメディアアクセスコントロールアドレス（MAC アドレス）
出荷日	アプライアンスの出荷日
プロセッサ	プロセッサ情報
仮想メモリ	仮想メモリ割り当て
物理メモリ	物理メモリ割り当て
TLS 1.2 のみ	以前のバージョンの Transport Layer Security (TLS)プロトコルを無効にし TLS v1.2 のみを使用するにはこのトグルをクリックします。 **メモ：**TLS 1.2 のみを有効にした後はアプライアンスを再起動する必要があります。 有効 無効

パフォーマンスタブ

表：パフォーマンスタブ

プロパティ	説明
合計 CPU および **コア_n**	CPU 情報とアプライアンスのパフォーマンス使用率が表示されます。
メモリ	アプライアンスのメモリ使用量、現在使用中および空き容量が表示されます。
ディスク領域	使用されているディスク容量と空き容量が表示されます。

アプライアンスのシャットダウン

Web クライアントまたはアプライアンス本体からアプライアンスをシャットダウンすることができます。

> ⚠ **注意: アプライアンスを再起動すると、現在のユーザーに対するサービスが停止します。**

アプライアンスのシャットダウン手順

Web クライアントで、左側の**［アプライアンス管理］＞［アプライアンス］＞［電源］**からアプライアンスをシャットダウンすることができます。詳しくは、「電源」を参照してください。

アプライアンス：アプライアンスからのシャットダウン手順

アプライアンスの前面パネルにある赤い×ボタンを使用します。赤い×ボタンを押したまま、POWER OFF と表示されるまで 4 秒待ちます。

> ⚠ **注意: SPP アプライアンスが起動したら、赤い×ボタンを 13 秒以上押し続けないでください。これにより、アプライアンスの電源がオフになり、故障の原因となることがあります。**

アプライアンスの再起動

Web クライアントまたはアプライアンス本体からアプライアンスを再起動することができます。

アプライアンスの再起動手順

Web クライアントで、左側の**［アプライアンス管理］＞［アプライアンス］＞［電源］**からアプライアンスを再起動することができます。詳しくは、「電源」を参照してください。

アプライアンス：アプライアンスからの再起動手順

アプライアンスの電源をオフにした後、物理的にアクセスする必要があります。アプライアンスの前面パネルにある緑色のチェックマークボタンを 1 秒以上押して、アプライアンスに電源を入れます。

> ⚠ **注意: SPP アプライアンスが起動したら、緑色のチェックマークボタンを 4 秒以上押し続けないでください。このボタンを 4 秒以上押し続けると、アプライアンスの電源がコールドリセットされ、破損する可能性があります。**

アプライアンス名およびホスト DNS サフィックスの設定

SPP は、アプライアンスに自動的に名前を割り当てますが、**アプライアンス情報**ページから名前を変更することができます。また、Web クライアントでは、SPP の初期セットアップ時に設定したホスト DNS サフィックスを編集することができます。

アプライアンス名とホスト DNS サフィックスの編集手順

1. **［アプライアンス管理］＞［アプライアンス］＞［アプライアンス情報］**ページに移動します。
2. **［アプライアンス名］**と**［ホスト DNS サフィックス］**の右側にある **［編集］**をクリックして、両方のフィールドを編集できるようにします。
3. **［アプライアンス名］**または**［ホスト DNS サフィックス］**に必要な変更を行います。
4. **［Save］**をクリックします。

9.1.3 デバッグ

SPP の内部サービスごとに、ログのレベルおよびデバッグログを保存する外部 syslog サーバーを指定できます。これにより、リアルタイムでデバッグを行うことができます。

デバッグログの記録はアプライアンス固有です。syslog サーバーに送信されるデータには、Support Bundle のデバッグデータを含めることができますが、これに限定されるものではありません。クラスタ全体の TLS 監査イベントは、syslog サーバーに記録できます（「Syslog イベント」を参照してください）。

デバッグログはデフォルトではオフになっていますが、オンまたはオフにすることができます。デバッグログはかなりの量になる可能性があるため、特定のシナリオやテストのデバッグ用にオンにし、日常的な運用ではオフにするのがよいでしょう。

API を使用した TLS ログ接続メッセージの使用

API を使用すると、外部サーバーとの TLS 接続を閉じたときに、デバッグログに TLS ログ接続メッセージを生成するかどうかを制御できます。ログレベルが設定されている場合（下記参照）、このイベントは syslog サーバーにも送信されます。

TLS 接続情報をログに記録するには、
https://<ネットワークアドレス>/service/appliance/v3/Service/Debug エンドポイントにある

NetworkDebugEnabled プロパティを true に設定します。詳しくは、「API の使用」を参照してください。

デバッグログを Syslog サーバーに送信するように設定する手順

1. 構成済みの syslog サーバーが必要です。Syslog サーバーが構成されていない場合、「追加のデバッグログオプションを設定するには、最初に Syslog サーバーを設定する必要があります。」というメッセージが表示されます。**［Syslog サーバーの設定］**をクリックしてください。詳細については、「Syslog サーバーの構成と検証」を参照してください。

2. Syslog サーバーが構成されている場合は、**［アプライアンス］＞［デバッグ］**を開きます。

3. デバッグログを送信したい **Syslog Server** を選択します。デフォルトは**［Syslog にログしない］**です。

4. **［機能］**で、使用する Syslog ファシリティを選択します。**Kernel**、**User**、**Mail**、**Daemons**、**Authorization**、**Syslog** です。

5. ログレベルを設定します。

    - すべてのログレベルを設定するには、**［すべてを設定］**をクリックし、いずれかのレベルで**［すべてを設定］**を選択します。これは、ほとんどのサービスに必要な最も一般的なログレベルを設定するのに便利です。
    - 個々のサービス名のログレベルを設定するには、そのサービスの横にある ▼ を選択して、そのサービスのログレベルを変更します。

    すべてのレベルの設定または個々のサービス名のレベルのいずれかを選択すると、ログには選択したログレベルだけでなく、選択したレベルより下にリストされているものも含まれます。その情報は、すぐにサーバーに送信されます。たとえば、以下のようになります：

    - デバッグ（デバッグ、情報、警告、エラーを含む）
    - 情報（情報、警告、エラーを含む）
    - 警告（警告、エラーを含む）
    - エラー（エラーのみ）
    - なし（無効）ログは送信されません。

6. グリッドには、デバッグログをサポートする各**サービス名（enum 名）**と現在の**ログレベル**が表示されます。

    - 最新の情報を表示するには、**［更新］**をクリックします。

- 特定のサービスを探すには、🔍**［検索］**をクリックします。

9.1.4 ライセンス設定

> ⚠ **注意: SPP 7.0 にアップグレードするすべてのお客様には、新しいライセンスが必要です。詳しくは、サポートにお問い合わせください。**

SPP のライセンス管理は、アプライアンス管理者の責任で行ってください。

ハードウェアアプライアンス

SPP ハードウェアアプライアンスには、機能を有効にするために有効なライセンスが必要な特権パスワード管理モジュールが同梱されています。

有効なライセンスをインストールする必要があります。モジュールをインストールすると、SPP のライセンス状態が**「ライセンス済み」**と表示され、動作可能な状態になります。モジュールのライセンスがインストールされていない場合は、機能が制限されます。パスワード管理モジュールのライセンスがインストールされていない場合、アクセスリクエストを設定することはできても、パスワードリリースをリクエストすることはできません。

仮想アプライアンスの Microsoft Windows ライセンス

仮想アプライアンスは、Microsoft Windows ライセンスを登録する必要があります。MAK または KMS 方式のいずれかを使用することをお勧めします。ライセンスに関する具体的なご質問は、営業担当者にお尋ねください。オペレーティングシステムが適切にライセンスされていない限り、仮想アプライアンスは機能しません。

初回ログイン時にライセンス情報を入力する手順

アプライアンス管理者として初めてログインすると、ライセンスの追加を促すメッセージが表示されます。

仮想アプライアンスでは、ライセンスは初期セットアップの一部として追加します。詳細については、「仮想アプライアンスのセットアップ」を参照してください。

> **重要：**ライセンスの追加に成功すると、ソフトウェア取引契約が表示されます。SPP を使用するためには、これを読み、同意する必要があります。

ライセンス期限切れのリマインダーの構成手順

SPP の使用に支障が出ないように、アプライアンス管理者は SMTP サーバーを構成し、**「ライセンスが失効しました」**および**「ライセンスが間もなく失効します」**イベントタイプのメールテンプレートを定義する必要があります。これにより、失効日が近づいていることが確実に通知されるようになります。詳細については、「メール通知の有効化」を参照してください。

「アプライアンスはライセンスされていません」という通知を受けた場合、ユーザーはアプライアンス管理者に連絡するように指示されます。

アプライアンス管理者は、「ライセンスが失効しました」という通知を受け取った場合、新しいライセンスを適用してください。

ライセンスファイルの更新手順

ライセンスの更新は、ハードウェア経由ではなく、仮想マシンを使用してのみ可能です。

ライセンス関連作業の実行手順

1. **［アプライアンス管理］＞［アプライアンス］＞［ライセンス］**に移動します。
    - 新しいライセンスファイルをアップロードするには、＋**［新しいライセンスファイルのアップロード］**をクリックし、ライセンスファイルを選択します。このプロセスでは**［ソフトウェア取引契約］**が表示されます。内容を確認し、承諾する必要があります。
    - ライセンスファイルを削除するには、ライセンスを選択し、🗑**［選択したライセンスを削除］**をクリックします。

9.1.5 工場出荷時リセット

アプライアンス管理者は、工場出荷時リセット機能を使用して、SPP アプライアンスをリセットして重大な問題から回復したり、アプライアンスのデータと構成設定を消去したりすることができます。

工場出荷時リセットは、仮想アプライアンスのオプションではありません。アプライアンスを再展開する必要があります。

> ⚠ **注意: この操作により、すべてのデータと監査履歴が削除され、工場出荷時の状態に戻ります。物理アプライアンスに対して工場出荷時リセットを実行する場合はご注意ください。工場出荷時リセットの実行は、BMC/IPMI インターフェイスまたは IP アドレスをリセットしません。ただし、BMC/IPMI インターフェイスは、リセット完了後に再度有効**

にする必要があります（詳細については、「ライトアウト管理（BMC）」を参照してください）。アプライアンスは、工場出荷時と同様に再度設定を行う必要があります。詳細については、「SPP の初期設定」を参照してください。

工場出荷時のリセットを実行すると、デフォルトの SSL 証明書とデフォルトの SSH ホストキーが変更される場合があります。

アプライアンスは、現在のロングタームサポート（LTS）バージョンにリセットされます。たとえば、アプライアンスがバージョン 6.6（機能リリース）または 6.0.6 LTS （メンテナンスロングタームサポートリリース）を実行している場合、工場リセットすると、アプライアンスは 6.0 LTS にリセットされ、希望のバージョンにパッチアップする必要があります。詳細については、「長期サポート（LTS）とフィーチャーリリース」を参照してください。

クラスタ化されたアプライアンスの工場出荷時リセット

クラスタ化されたハードウェアアプライアンスで工場出荷時リセットを実行しても、アプライアンスはクラスタから自動的に削除されません。推奨されるベストプラクティスは、アプライアンスで工場出荷時リセットを実行する前に、クラスタからアプライアンスを解除することです。解除して工場出荷時リセットを行った後、アプライアンスを再度構成する必要があります。詳細については、「SPP の初期設定」を参照してください。

Web クライアントから工場出荷時リセットを実行する手順

1. （仮想マシンではなく）ハードウェアの工場出荷時リセットのページ（**[アプライアンス管理]** > **[アプライアンス]** > **[工場出荷時リセット]**）に移動します。
2. **[工場出荷時リセット]** をクリックします。
3. 工場出荷時リセットの確認ダイアログで、**「工場リセット」**と入力し、**[工場リセット]** をクリックします。

   アプライアンスはメンテナンスモードになり、アプライアンスを元に戻します。アプライアンスがクラスタにあった場合、ファクトリーリセットアプライアンスの結合を解除する必要がある場合があります。工場出荷時リセットのアプライアンスを再度構成する必要があります。詳細については、「SPP の初期設定」を参照してください。アプライアンスにログインすると、SPP ライセンスを追加するよう促されます。

リカバリキオスクまたはサポートキオスクから工場出荷時リセットを実行することもできます。詳細については、「工場出荷時リセット」を参照してください。

9.1.6 ライトアウト管理（BMC）

ライトアウト管理（Lights Out Management）機能は、ベースボード管理コントローラ（BMC）を使用して、SPP の電源状態およびシリアルコンソールをリモートで管理することができます。LAN インターフェイスが構成されている場合、これによってアプライアンス管理者は、リモートでアプライアンスの電源を入れたり、リカバリキオスクと対話したりすることができます。

アプライアンス管理者は、ライトアウト管理機能を有効化し、構成することができます。Lights Out Management を有効にすると、アプライアンス管理者はベースボード管理コンソール（BMC）のパスワードを設定または変更し、ネットワーク情報を修正することができます。SPP を無効にすると、パスワードが直ちにランダムな値にリセットされ、ネットワーク設定もデフォルト値にリセットされます。

ライトアウト管理は、（仮想マシンではなく）ハードウェアでのみ利用可能です。

- 仮想アプライアンス Support Kiosk、Lights Out Managment (BMC)を使用します。詳しくは、「サポートキオスク」を参照してください。

LAN インターフェイス

この機能を使用するには、LAN インターフェイスが有効であり、設定されていることが必要です。SPP の BMC は、この機能を提供するために次の LAN インターフェイスをサポートしています：

- SSH
- IPMI v2
- Web
- シリアルオーバーLAN

LAN インターフェイスは、信頼できる環境でのみ有効にすることが強く推奨されます。

Lights Out Management の有効化

静的 IP アドレスを割り当て、ネットワークケーブルをアプライアンス背面の IPMI イーサネットポートに接続する必要があります。これは、標準の X0 ネットワークインターフェイスに追加されます。

1. **Lights Out Management (BMC)**に移動します。
2. この機能を有効または無効にするには、**［Lights Out Management の有効化］**トグルをクリックします。トグルオンまたはトグルオフを設定します。

3. 有効化したら、BMC に関する以下の情報を入力します：

    a. **IP アドレス**：ホストマシンの IPv4 アドレス

    b. **ネットマスク**： IPv4 アドレスのネットワークマスク

    c. **デフォルトゲートウェイ**： IPv4 アドレスのデフォルトゲートウェイ

4. **［Set BMC Admin Password］**を使用して、ホストマシンのパスワードを設定します。最大パスワード長は、20 文字です。

    > **メモ：**この機能が以前に有効になっていた場合、代わりに**［Update BMC Admin Password］**ボタンが表示されます。任意で、**［Update BMC Admin Password］**ボタンをクリックすると、ホストマシンのパスワードがリセットされます。

5. **［OK］**をクリックして、ホストマシン上の設定を保存します。

BMC へのアクセス

SPP で Lights Out Management を有効にすると、以下の方法で BMC にアクセスすることができます。

- SSH で IPMI ポートに接続し、SPP の電源状態およびシリアルコンソールをリモートで管理します。
- Web ブラウザー

SSH 接続

SPP Kiosk コンソールには、Putty、Linux コマンドライン、またはお好みの SSH クライアントを使用してアクセスすることができます。

1. IPMI インターフェイスに割り当てられた IP に接続し、Admin ユーザーでログインします（デフォルトの認証情報は ADMIN/admin です）。

2. プロンプトで、/system1/sol1 を実行します。遅延が発生することがあります。接続が確立されるまでお待ちください。次のようなメッセージが表示されたら、続行するように指示されます：

    ->start / system1soll
    press <Enter>, <Esc>, and then <T> to terminate session
    (press the keys in sequence, one after the other)

3. 下図のメニューで、矢印キーを使用して移動します。右矢印を押すとメニューオプションが選択され、左矢印を押すとメニューリストに戻り、上または下を押すと別のメニューオプションが選択されます。

Appliance Information >
Power Options >
Admin Password Reset >
Factory Reset >
Support Bundle >

4. 画面がフリーズしたり、情報が歪んで表示されたりした場合は、**CTRL+R** または **CTRL+D** を押して画面を更新することができます。

5. Kiosk を終了するには、**Enter** キーを押したあと、**ESC** キーを押し、**SHIFT+T** キーを押します。プロンプトで、**exit** と入力します。

アプライアンスが隔離されている場合、Kiosk メニューから「Quarantine Bundle」を生成し、そのファイルをネットワーク共有にコピーしてください。バンドルが取得された後、キオスクで再起動を実行し、アプライアンスが自力で回復するかどうかを確認します。隔離されたままの場合、工場出荷時のリセットが必要になる可能性があります。詳細については、「工場出荷時リセット」を参照してください。

Web ブラウザインターフェイス

SSH によるログインが困難な場合は、Web アクセスも可能です。

1. Web ブラウザで、IPMI インターフェイスの IP アドレスに移動します（https://10.10.10.10）にアクセスし、BMC 管理者アカウントでログインします。デフォルトは ADMIN/admin です。

2. **［Maintenance］＞［Unit Reset］＞［Select Reset］**と移動して、SSH 接続の修復を試みることができます。60 秒後に SSH 接続を再試行します。

3. **［Remote Control］＞［Select Launch SOL］**を選択して、Web 経由で Kiosk にログインします（この方法の場合、Java が必要です。Kiosk は JNLP ウィンドウで起動します）。

4. カーソルキーとリターンを使って移動します。ページアップは、バックスペースを使用します。Java ビューアーを使用する場合、コピー＆ペーストはできません。

再起動

BMC Web ブラウザインターフェイスからの再起動は、ハードウェアレベルの再起動に限られます。

Web ブラウザインターフェイスを使用して再起動する必要がある場合：

1. BMC Web ブラウザインターフェイスにログインします。

2. Serial over Lan エミュレーターを開き、Kiosk インターフェイスを開きます。

3. メニューから reboot を選択します。

Lights Out Management/BMC/IPMI インターフェイスを使用して Kiosk にリモートでアクセスする方法については、KB 263835 を参照してください。

9.1.7 ネットワーク診断

SPP では、アプライアンス管理者と運用管理者がこれらの診断テストを利用できます。

> **メモ：**これらの診断テストを実行すると、アプライアンス上で実行されます。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**に移動します。

2. 実行するテストの種類を選択し、手順を完了します。

    - ARP：Address Resolution Protocol (ARP)を使用して、インターフェイス、インターネットアドレス、物理アドレス、タイプ（動的または静的）を検出します。
    - Netstat： netstat を使用して、アクティブな接続プロトコル、ローカルアドレス、外部アドレス、状態を表示します。
    - NSLookup：ドメイン名または IP アドレスを取得します。
    - Ping：ネットワークの接続性と応答時間を確認するために使用します。
    - ルートの表示：ルーティングテーブル情報を取得します。
    - Telnet：インターネットのような TCP/IP ネットワーク上でリモートコンピューターにアクセスします。
    - スループット：クラスタ内の他のアプライアンスへのスループットをテストします。
    - ルートの追跡：ルーター情報を取得するため。トレースルートは、ある IP アドレスから別の IP アドレスにパケットが通過する経路を決定します。

ARP

Address Resolution Protocol (ARP)を使用して、インターフェイス、インターネットアドレス、物理アドレス、タイプ（動的または静的）を検出します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**を選択します。

2. **［ARP］**をクリックします。

3. **［ARP テーブルの表示］**をクリックして、テストを実行します。テスト結果は**［出力］**ウィンドウに表示されます。インターフェイス、インターネットアドレス、物理アドレス、タイプが含まれる場合があります。

Netstat

アクティブな接続プロトコル、ローカルアドレス、外部アドレス、および状態を表示するには、netstat を使用します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**を選択します。

2. **［Netstat］**をクリックします。

3. **［接続の表示］**をクリックして、テストを実行します。テスト結果は**［出力］**ウィンドウに表示され、アクティブな接続、プロトコル、ローカルアドレス、外部アドレス、状態が含まれる場合があります。

NSLookup

SPP アプライアンスに関連して、指定したホストのドメインネームサーバーまたは IP アドレスを取得するには、NS Lookup クエリを使用します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**に移動します。

2. **［NSLookup］**をクリックします。

3. リモートホストの **IP アドレス** または **ホスト名**を入力します。

4. **［レコードタイプ］**で、照会する DNS レコードの種類を選択します。

5. **［表示する設定を増やす］**を選択し、**［クエリオプション］**でクエリの種類を選択します。

6. **［ルックアップ］**をクリックして、テストを実行します。テスト結果は**［出力］**ウィンドウに表示されます。

Ping

Ping テストを使用して、SPP アプライアンスと指定したホスト間のネットワーク接続と応答時間を確認します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**に移動します。
2. **［Ping］**をクリックします。
3. リモートホストの **IP** または**ホスト名**を入力します。
4. 任意で**［表示する設定を増やす］**をクリックし、以下の追加設定を行います：
    - **IP アドレスをホスト名に解決します**
    - **サイズ**：バッファーサイズ：1～65500 の範囲
    - **有効時間**：1～255 までの値を入力します。
    - **ホップ数のルートを記録します（IPv4 のみ）**：1～9 の値を入力します。
    - **各応答を待つタイムアウトの時間（ミリ秒）**：1～4000 の値を入力します。
    - **送信するエコーリクエストの数**。1～65527 の値を入力します。
    - **パケット内の「don't fragment」フラグを設定します（IPv4 のみ）**
    - **サービスのタイプ：**1～255 の値を入力
    - **ホップ数のタイムスタンプ（IPv4 のみ）**：1～4 を入力します。
    - **内部アドレスをソースとして使用します**
5. **［Ping］**をクリックしてテストを実行します。テスト結果は**［出力］**ウィンドウに表示されます。

ルートの表示

接続性の問題をさらに調査するためにルーティングテーブルを取得するには、**［ルートの表示］**を使用します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**を選択します。
2. **［ルートの表示］**を選択します。
3. テスト結果は**［出力］**ウィンドウに表示されます。

Telnet

SPP アプライアンスと指定したホスト間の TCP/IP 接続をテストするには、Telnet を使用します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**を選択します。
2. **［Telnet］**を選択します。
3. **［IP またはホスト名］**に入力します。
4. **［ポート］**にポート番号を入力します。デフォルトは 23 ですが、 0 から 65535 までの値を入力することができます。
5. **［接続］**をクリックしてテストを実行します。テスト結果は**［出力］**ウィンドウに表示されます。

スループット

クラスタ内の他のアプライアンスへのスループットをテストします。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**を選択します。
2. **［スループット］**を選択します。
3. **［ターゲットアプライアンス］**でリストからターゲットのクラスタアプライアンスを選択します。
4. **［転送する MB］**にテストのための転送サイズを選択（1 から 1000MB）します。
5. **［スループットのテスト］**をクリックしてテストを実行します。テスト結果は**［出力］**ウィンドウに表示されます。

ルートの追跡（Trace Route）

ある IP アドレスから別の IP アドレスへ移動する経路情報を取得するために使用します。

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク診断］**を選択します。
2. **［ルートの追跡］**を選択します。

3. **［IP またはホスト名］**にリモートのホスト IP アドレスまたはホスト名を入力します。
4. 任意で、**［表示する設定を増やす］**をクリックして次を設定します：
    - **IP アドレスをホスト名に解決します**
    - **ターゲットを検索するときの最大ホップ数**
    - **各応答を待つタイムアウトの時間（ミリ秒）**
5. **［ルートの追跡］**をクリックしてテストを実行します。テスト結果は**［出力］**ウィンドウに表示されます。

9.1.8 ネットワーク

［ネットワーク］で、プライマリネットワークインターフェイス、および該当する場合は Web トラフィックを中継するプロキシサーバー、およびセッションネットワークインターフェイスを表示し、構成します。

ネットワークインターフェイス（X1）は、Web クライアントで X1 に関連付けられた仮想ネットワークアダプターを追加するために使用することができます。

ネットワークインターフェイスが正しく構成されていることを確認するのは、アプライアンス管理者の責任です。

> ⚠ **注意：AWS または Azure の場合、ネットワーク設定のユーザーインターフェイスは読み取り専用です。ネットワーク設定は、AWS または Azure の管理者によって構成されます。クラスタ化されたアプライアンスの内部ネットワークアドレスを変更すると、クラスタが壊れ、アプライアンスの未接続/再接続が必要になります。**

ネットワーク構成設定の変更手順

1. **［アプライアンス管理］＞［アプライアンス］＞［ネットワーク］**をクリックします。
2. **［MGMT］**のネットワーク設定を行います。詳しくは、「IP アドレスの変更」を参照してください。
    - **MAC アドレス**：（読み取り専用）Media Access Control Address（MAC アドレス）、通信用ネットワークインターフェイスに割り当てられた一意の識別子
    - **IPv4 アドレス**：ネットワークインターフェイスの IPv4 アドレス
    - **IPv4 サブネットマスク**：ネットワークインターフェイスの IPv4 サブネットマスク

- **IPv4 ゲートウェイ**：IPv4 デフォルトゲートウェイ
- **DNS サーバー**：プライマリ DNS サーバーの IP アドレス
- **DNS サフィックス**：DNS サーバーの IP アドレス。DNS サーバーのネットワークサフィックスです。

  > **注**：**[アプライアンス] > [ネットワーク]** ページの **[グローバル DNS サフィックス]** フィー ルドを使用することもできます。

- **IP6 アドレス**：ネットワークインターフェイスの IPv6 アドレス
- **IPv6 プレフィックスの長さ**：IPv6 サブネットプレフィックス長。範囲検証される IPv6 サブネットプレフィックスの長さ。IPv6 アドレスが存在する場合、有効な値は 1～127 です。
- **IPv6 ゲートウェイ**：IPv6 デフォルトゲートウェイ

3. **[ネットワーク X0]** のネットワーク設定を行います。最大 31 の VLAN に仮想ネットワークアダプターを追加してください。
   - **MAC アドレス**：（読み取り専用）Media Access Control Address（MAC アドレス）、通信用ネットワークインターフェイスに割り当てられた一意の識別子
   - **IPv4 アドレス**：ネットワークインターフェイスの IPv4 アドレス
   - **IPv4 サブネットマスク**：ネットワークインターフェイスの IPv4 サブネットマスク
   - **IPv4 ゲートウェイ**：IPv4 デフォルトゲートウェイ
   - **DNS サーバー**：プライマリ DNS サーバーの IP アドレス
   - **DNS サフィックス**：DNS サーバーの IP アドレス。DNS サーバーのネットワークサフィックスです。

     > **注**：**[アプライアンス] > [ネットワーク]** ページの **[グローバル DNS サフィックス]** フィールドを使用することもできます。

   - **IP6 アドレス**：ネットワークインターフェイスの IPv6 アドレス
   - **IPv6 プレフィックスの長さ**：IPv6 サブネットプレフィックス長。範囲検証される IPv6 サブネットプレフィックスの長さ。IPv6 アドレスが存在する場合、有効な値は 1～127 です。
   - **IPv6 ゲートウェイ**：IPv6 デフォルトゲートウェイ
   - **VLAN ID :** ネットワークの VLAN ID。これは、管理者によって追加されたネットワークインターフェイスにのみ適用されます。このフィールドを変更すると、アダプタの名前も更新されます。

4. **［プロキシサーバー］**で、以下のネットワーク設定を行います。
    - **プロキシ URI**：プロキシサーバーの IP アドレスまたは DNS 名
    - **ポート：**プロキシサーバーが HTTP リクエストをリッスンするために使用するポート番号。値は 1～65535 の整数です。プロキシ URI と**［ポート］**フィールドで異なるポートが指定されている場合、**［ポート］**フィールドが優先されます。
    - **ユーザー名：**プロキシサーバーへの接続に使用するユーザー名。ユーザー名とパスワードは、プロキシサーバーで指定が必要な場合のみ必要です。
    - **パスワード：**プロキシサーバーに接続するために必要なパスワード。ユーザー名とパスワードは、プロキシサーバーで指定する必要がある場合のみ必要です。

5. **［静的ルートの表示］**をクリックし、以下の内容で変更します。完了したら、**［保存］**をクリックします。**［保存］**をクリックすると、「これらの値を変更すると、すべてのユーザーがアプライアンスへの接続を失う可能性があります。」というメッセージが表示されます。これは、一般的なネットワーク設定の保存エラーであり、静的ルートに固有のものではありません。
    - 必要に応じて、以下のツールバーボタンを使用します。
        - ルートを追加するには、＋をクリックして情報を入力します。
        - ルートの情報を変更するには、ルートを選択し、**［静的ルートの編集］**をクリックして、情報を変更します。
        - 経路を削除するには、経路を選択し、**［静的ルートの削除］**をクリックします。ルートは即座に削除されます。
        - 保存されていない変更を破棄し、データベースから最後に取得した情報に戻すには、ルートを選択し、**［保存されていない静的ルートの編集内容をすべて元に戻す］**をクリックします。
    - 次の情報を追加または変更できます。
        - **IP バージョン**：IPv4 または IPv6 を選択します。
        - **プレフィックス**：IPv4 または IPv6 を選択します。IPv4 または IPv6 の IP アドレスです。
        - **プレフィックス長**：IP サブネットプレフィックスの長さです。
        - **次のホップ**：ルーティングパスで次に近い、または最適なルーターの IP アドレスです。
        - **メトリック**：ルートの使用に関連するコストを特定する値。

IP アドレスの変更

SPP クラスタ内の他のアプライアンスに新しいサブネットが表示されている限り、SPP アプライアンスの IP アドレスを変更することができます。

以下の手順はテスト環境で使用し、その後本番環境に導入することをお勧めします。IP アドレスが変更されるまでの時間を十分にとってください。クラスタに変更が適応されるまで、操作の完了に数分かかります。

1. SPP 2.4 以降を使用していることを確認します。
2. X0 IP アドレスを変更する前に、バックアップを作成します。
3. IP アドレスを変更する予定のアプライアンスで、サポートバンドルを生成します。まずレプリカから始めます。
4. X0 IP アドレスの変更後、クラスタリングが機能していることを確認します。レプリカにログオンして、プライマリのデータを変更し、それがレプリカに表示されることを確認することをお勧めします。
5. 他のレプリカについても、ステップ 3、4、および 5 を繰り返します。
6. レプリカの変更が完了したら、プライマリに進みます。

SPS の IP アドレスの変更

> ⚠ **注意：SPP と SPS をリンクした後、SPS クラスタマスタ（中央管理ロール）または SPP プライマリアプライアンスのいずれかの IP アドレスが変更された場合、SPP/SPS のリンクをやり直す必要があります。以下の情報を参照してください。**

1. SPS クラスタの役割、設定、および IP アドレスの更新について理解するために、SPS ドキュメントの次の情報を使用してください。
    - クラスタの役割：ノードへロールを割り当てます。
    - ネットワークの設定：IP アドレスを含む、SPS ネットワークインターフェイスとネーミングを設定します。
    - クラスタの構築：クラスタの中央管理ノードを割り当て（元に戻すことはできません）、その後他のノードを参加させます。
    - クラスタ内のノードにロールを割り当て：クラスタ内のノードに中央管理ロールを含むロールを割り当てます。

- クラスタ内のノードの IP アドレスの更新：SPS Managed Nodes の IP アドレスを更新します。
- High Availability One Identity Safeguard for Privileged Sessions （SPS）クラスタの管理：プライマリノードが機能しなくなった場合にノードを処理するように、SPS を設定します。

2. IP アドレスが変更された場合は、クラスタを再リンクする必要があります。詳細については、Safeguard for Privileged Sessions 管理者ガイドを参照してください。

3. SPS の IP アドレスが正常に変更されたら、SPP の設定でセッション接続を削除し、SPS クラスタマスタを SPP のプライマリに再リンクする必要があります。詳細については、「SPP と SPS のリンクガイダンス」を参照してください。

9.1.9 オペレーティングシステムのライセンス

仮想マシンのみ利用できます。ハードウェアアプライアンスでは表示されません。

オペレーティングシステムの設定は、アプライアンス管理者の責任で行ってください。AWS および Azure のデプロイメントでは、オペレーティングシステムのライセンスは自動です。

仮想アプライアンスのオペレーティングシステムを表示および構成するには、**［オペレーティングシステムのライセンス］**ペインを使用します。

1. **［アプライアンス管理］＞［アプライアンス］＞［オペレーティングシステムのライセンス］**に移動します。

2. **［更新］**をクリックして設定を更新します。

3. Windows が KMS でライセンスされているか、プロダクトキーでライセンスされているかが表示されます。**［詳細の表示］**をクリックすると、追加情報が表示されます。

9.1.10 SSH アルゴリズム

アプライアンス管理者は、必要に応じて SSH アルゴリズムを設定し、任意の SSH サーバーへの接続時に使用するアルゴリズムを制限するオプションがあります。この設定は、SPP が SSH を使用して資産に接続する場合、または SSH を使用してアーカイブサーバーに接続する場合のいずれであっても、任意の SSH サーバーに接続するたびに適用されます。

SSH クライアントがサーバーに接続するとき、接続の各側は、相手側に接続パラメーターとして使用するアルゴリズムの 4 つのリストを提供します。これらは以下の通りです。

- 公開キー：SSH サーバーが SSH クライアントに自分自身を認証するために受け入れられる公開鍵のアルゴリズム
- Cipher：接続を暗号化するための暗号
- Kex：接続ごとの鍵を生成するための鍵交換方式
- MAC：トラフィックの改変を検出するために使用されるメッセージ認証コード

デフォルトでは、SPP は、SSH を使用してアーカイブサーバーまたは資産に接続する場合、サポートされているすべてのアルゴリズムを提供します。アルゴリズムの種類ごとに、サポートされているアルゴリズムのサブセットを提供するように Safeguard を設定することができます。デフォルト（すべてのアルゴリズムをサポート）に戻すには、入力したすべてのアルゴリズム情報を削除してから、変更を保存します。

接続を成功させるには、各パラメーターで相互にサポートされる選択肢が少なくとも 1 つ必要です。SPP は、資産またはアーカイブサーバーへの SSH 接続を開始しても、相互に受け入れ可能なアルゴリズムをネゴシエートできない場合があります。エラーが報告され、ネゴシエートできなかったアルゴリズムタイプの特定が試みられます。一部の SSH サーバーは、アルゴリズムの種類を特定するのに十分な情報を提供しません。

SSH アルゴリズムを確認方法

1. **［アプライアンス管理］＞［アプライアンス］＞［SSH アルゴリズム］**に移動します。
2. **［更新］**をクリックして更新します。
3. テキストボックスに必要なアルゴリズムをカンマ区切りで入力します。サポートされているすべてのアルゴリズムを許可するには、テキストボックスを空白にします。
    - **公開キー**
    - **暗号化（Cipher）**
    - **キー（Kex）**
    - **Mac**
4. **［保存］**をクリックします。

公開鍵アルゴリズムの優先順位の調整

デフォルトでは、ホストキーにサポートされ、ID 鍵に使用できる公開鍵アルゴリズムのリストは、この優先順位で SSHD サーバーとネゴシエートされます。

1. Ssh-ed25519,
2. ecdsa-sha2-nistp256,
3. ecdsa-sha2-nistp384,
4. ecdsa-sha2-nistp521,
5. ssh-rsa,
6. rsa-sha2-256,
7. rsa-sha2-512,
8. ssh-dss

SshAlgorithms API を使用して PublicKey 一覧を構成することにより、優先順位を変更したり、利用可能なアルゴリズムをこの一覧のサブセットに制限したりすることができます。

9.1.11 パッチの更新

実行中のアプライアンスのソフトウェアまたは構成を変更するために更新ファイルをインストールし、SPP を更新またはアップグレードすることは、アプライアンス管理者の責任で行う必要があります。利用可能な SPP リリースとバージョンパッチについては、「ソフトウェアのダウンロード」ページを参照してください。

更新に失敗した場合、監査ログに反映されます（PatchUploadFailed）。

クラスタ環境

クラスタ内のすべてのアプライアンスが同じバージョンになるようにパッチを適用します。詳細については、「クラスタメンバーへのパッチ適用」を参照してください。

更新ファイルのインストール手順

> **重要**: パッチ更新を開始したら、ページを離脱したり更新したりしないでください。ブラウザーがパッチアップデートの記録を失い、処理を再開しなければならなくなります。

1. 更新ファイルをインストールする前に、システムをバックアップしてください。詳細については、「バックアップと復元」を参照してください。
2. **［アプライアンス管理］＞［アプライアンス］＞［パッチの更新］**を選択します。現在のアプライアンスバージョン、オペレーティングシステムのレベル、アプライアンスがオンラインかオフラインか、アプライアンスがプライマリかどうかが表示されます。
3. **［ファイルのアップロード］**をクリックして、更新ファイルを選択します。ファイルをアップロードしただけでは、ファイルはインストールされません。次の手順を完了する

必要があります。パッチの検証が失敗すると、エラー警告が表示されます。エラーまたは警告のカウントのいずれかをクリックすると、現在記録されているエラーまたは警告が表示されます。

4. ファイルが正常にアップロードされたら、次のいずれかをクリックします。
    - **［今すぐインストール］**をクリックすると、更新ファイルがインストールされます。警告を含む確認ダイアログに応答します。インストールプロセスが開始され、アプライアンスはメンテナンスモードに入ります。
      更新ファイルを一度インストールすると、アンインストールすることはできません。このボタンは、パッチがすべてのクラスタメンバーに配布されるまで無効化されます。これが単一アプライアンスクラスターの場合、配布は必要ありません。
    - エラーが発生した場合は、**［クラスタへ配布］**を無効にします。**［クラスタへ配布］**をクリックすると、すべてのクラスタメンバーへのパッチの配布が開始されます。**［キャンセル］**をクリックすると、配布が停止します。各メンバーがパッチを受信すると、クラスタの更新状況ブロックが更新されます。
    - パッチを適用する前の状態のチェックを開始するには、**［エラーのチェック］**をクリックします。パッチが配布されていない場合、または検証中にエラーが報告された場合、これはローカルアプライアンス上でのみチェックを実行します。パッチが配布されている場合は、すべてのクラスタメンバーでチェックが実行されます。各クラスタメンバーから同じ警告が返されることがあります。
    - パッチがアップロードされると、**［削除］**が有効になります。パッチをすべてのクラスタメンバーから削除（ステージ解除）するには、**［削除］**をクリックします。

［更新］ペインには、アップグレードの進行状況と、アプライアンスがいつ正常にアップグレードされたかが表示されます。

9.1.12 電源

アプライアンス管理者または運用管理者は、Web クライアントから、またはアプライアンス自体から直接、アプライアンスの電源をオフにしたり再起動したりすることができます。

注意 アプライアンスを再起動すると、現在のユーザーに対してサービス停止が発生します。

> ⚠ **警告：アプライアンスを再起動すると、現在のユーザーに対してサービス停止が発生します。**

アプライアンスのシャットダウン手順

1. **［アプライアンス管理］＞［アプライアンス］＞［電源］**を選択します。
2. **［理由］**に SPP をシャットダウンする理由を入力し、**［シャットダウン］**をクリックします。
3. 確認画面の入力ボックスに**［シャットダウン］**と入力し、**［シャットダウン］**をクリックします。
4. SPP アプライアンスの液晶画面に、LCD service terminating と表示されます。

アプライアンスの再起動手順

1. **［アプライアンス管理］＞［アプライアンス］＞［電源］**を選択します。
2. **［理由］**に SPP を再起動する理由を入力し、**［再起動］**をクリックします。
3. 確認画面の入力ボックスに**［再起動］**と入力し、**［再起動］**をクリックします。
4. SPP アプライアンスの液晶画面に、起動中のアプライアンスのランレベルステータスが表示されます。詳細については、「LCD ステータスメッセージ」を参照してください。

アプライアンス

アプライアンス自体からアプライアンスをシャットダウンまたは再起動することができます。

アプライアンス：アプライアンスからのシャットダウン手順

アプライアンスの前面パネルにある赤い×ボタンを使用します。赤い×ボタンを押したまま、POWER OFF と表示されるまで 4 秒待ちます。

> ⚠ **注意: SPP アプライアンスが起動したら、赤い×ボタンを 13 秒以上押し続けないでください。これにより、アプライアンスの電源がオフになり、故障の原因となることがあります。**

アプライアンス：アプライアンスからの再起動手順

アプライアンスの電源をオフにした後、物理的にアクセスする必要があります。アプライアンスの前面パネルにある緑色のチェックマークボタンを 1 秒以上押して、アプライアンスに電源を入れます。

⚠ **注意: SPP アプライアンスが起動したら、緑色のチェックマークボタンを 4 秒以上押し続けないでください。このボタンを 4 秒以上押し続けると、アプライアンスの電源がコールドリセットされ、破損する可能性があります。**

9.1.13 Support Bundle

問題を分析し診断するために、One Identity サポートは、アプライアンス管理者または運用管理者に、システムと構成情報を含むサポートバンドルの送信を依頼することがあります。

別の方法として、Recovery Kiosk を使用してサポートバンドルを生成し、Windows 共有に送信することができます。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。

仮想アプライアンスのサポートバンドルは、Web 管理コンソールから生成されます。詳細については、「サポートキオスク」を参照してください。

> **重要：**ユーザーは、バンドルが完了するまでそのページに留まる必要があります。ページを更新したりページから移動したりした場合、バックエンドのバンドル処理は完了するまで実行されますが、保留中の Web リクエストはキャンセルされ、バンドルは取得できなくなります。

サポートバンドルの作成手順

1. **［アプライアンス管理］＞［アプライアンス］＞［Support Bundle］**に移動します。
2. オペレーティングシステムイベントを含める場合は、**［イベントログを含める］**を選択します。サポートから要求がない限り、サポートバンドルの生成に時間がかかるため、このチェックは外しておくことをお勧めします。
3. **［含まれるログファイルの制限］**を選択し、データを収集する日数を指定します。
4. **［新しい Support Bundle を生成］**をクリックします。
5. Support Bundle の.zip ファイルを保存する場所を選択し、**［保存］**をクリックします。
6. サポートバンドルを One Identity サポートに送信します。

9.1.14 時間

アプライアンス時間を管理するのは、アプライアンス管理者の責任です。

時刻は、現在のアプライアンスの時刻を表示し、ネットワークタイムプロトコル（NTP）を有効にし、プライマリおよびセカンダリ NTP サーバーを設定することができます。また、有効にすると、NTP クライアントのステータスを表示することができます。ベストプラクティスとして、時間に関連する可能性のある問題を排除するために、NTP サーバーを設定します。

推奨されませんが、プライマリ（クラスタではない）でアプライアンスの時間を手動で設定することもできます。

> ⚠ **注意：アプライアンスの時間を変更すると、アプライアンスで実行中のプロセスに予期せぬ結果をもたらす可能性があります。たとえば、パスワード確認と変更プロファイルが中断され、監査ログのタイムスタンプが誤解を招く可能性があります。アプライアンスが機能しなくなるため、システム時刻を Safeguard 内部証明書の有効期間の前または後に設定しないでください。**

クラスタ環境

NTP 設定の変更は、クラスタ内のプライマリアプライアンスで行われます。レプリカアプライアンスがクラスタに登録されると、プライマリアプライアンスの VPN IP アドレスをプライマリ NTP サーバーとして指し示し、レプリカアプライアンスで NTP クライアントサービスが有効化されます。レプリカを新しいプライマリに昇格させるフェイルオーバー操作を行う場合、プライマリ NTP サーバーは「古い」プライマリアプライアンスから保存、適用されます。

警告

ローカルタイムとアプライアンスタイムが 5 分以内でない場合、以下の警告が表示されます。One Identity 社は、時間に関連する可能性のある問題を排除するために、NTP サーバーを設定することを推奨します。

- ログオン時：
  警告： Safeguard に関連する時刻とローカル時刻が 5 分以上ずれています。Safeguard の管理者に連絡し、この問題を修正してから使用してください。
- **［アプライアンス管理］＞［アプライアンス］＞［時間］**ページ：
  アプライアンス時刻とローカル時刻が 5 分以上ずれています。NTP サーバーを設定することをお勧めします。

ネットワークタイムプロトコル（NTP）を有効にして、プライマリおよびセカンダリ NTP サーバーを設定する手順

1. **［アプライアンス管理］＞［アプライアンス］＞［時間］**に移動します。
2. **［NTP の有効化］**チェックボックスを選択し、以下の情報を入力します：

- **［プライマリ NTP サーバー］**：プライマリ NTP サーバーの IP アドレスまたは DNS 名を入力します。
- **［セカンダリ NTP サーバー］:**（任意）セカンダリ NTP サーバーの IP アドレスまたは DNS 名を入力します。

3. **［保存］**をクリックして、選択内容を保存します。

   NTP が有効な場合、**［詳細の表示］**をクリックすると NTP クライアントの状態について以下の情報が表示されます。

   - 前回の同期時間
   - リープインジケータ
   - ポール間隔
   - 精度
   - 参照 ID
   - ルート遅延
   - ルート分散
   - ソース
   - 階層
   - 前回の同期エラー
   - 前回同期が成功してから経過した時間

NTP が設定されていて時間を変更する必要がある場合は、API に移動し、Set-SafeguardTime を使用してください。API の使用に関する情報は、「API の使用」を参照してください。

（クラスタではない）プライマリでアプライアンス時刻を手動で設定する手順

（クラスタではないプライマリ）アプライアンス時刻を手動で設定するには、以下の手順に従います。

> ⚠ **注意: 時間を手動で設定する場合は、慎重に行う必要があります。時間の変更により、重大なデータ損失が発生する可能性があります。**

1. **［アプライアンス管理］＞［アプライアンス］＞［時間］**へ移動します。
2. **［NTP の有効化］**チェックボックスをオフにします。
3. **［保存］**をクリックします。
4. **［編集］**をクリックします。

5. 正確な時間を設定するために、以下の手順を素早く行います。

    a. **［システム時刻の設定］**ダイアログで、**［クライアント時刻の使用］**をクリックしてローカル時刻を使用するか、日付と時刻を選択します。

    b. **［OK］**をクリックします。

    「Safeguard 時刻が大きく変わると重大なデータ消失の原因となることがあります。」というメッセージが表示されます。

    c. **「時刻の設定」**と入力し、**［OK］**をクリックします。

9.1.15 タイムゾーン

SPP は、セットアップを実行する人の所在地に基づいてデフォルトのタイムゾーンを設定します。タイムゾーンは UTC +または - 時:分で表され、時間指定アクセスに使用されます（たとえば、午前 9 時から午後 5 時までのアクセスなど）。Bootstrap Administrator は、セットアップ時に希望するタイムゾーンを設定することをお勧めします。権限許可者管理者は、タイムゾーンを変更することもできます。

タイムゾーンの設定手順

1. **［ユーザー管理］＞［設定］＞［タイムゾーン］**に移動します。
2. ユーザー管理者は、希望するタイムゾーンを検索して選択することができます。
3. ユーザー管理者は、**［ユーザーは、自分のタイムゾーンを変更できます］**を変更することができます。
    - ユーザーにタイムゾーンの変更を許可する設定を有効にする（デフォルト）。
    - この設定を無効にすると、ユーザーがタイムゾーンを変更することを禁止することができます。

9.2 バックアップと保持

SPP のバックアップとアーカイブサーバーを管理するには、［バックアップと保持］設定を使用します。

SPP のバックアップと保持の設定を構成するのは、アプライアンス管理者の責任です。

［バックアップと保持］に移動します。

表：バックアップと保持設定

設定	説明
アーカイブサーバー	バックアップファイルやセッション記録を保存するためのアーカイブサーバーを追加管理します。
監査ログメンテナンス	アーカイブおよびパージする監査ログを定義し、監査ログアーカイブタスクを実行するためのスケジュールを設定します。
バックアップと復元	バックアップの開始またはスケジュール、バックアップファイルのアップロードまたはダウンロード、バックアップファイルが保存されるアーカイブサーバーの指定が行えます。
バックアップ保持	バックアップ保持を有効（または無効）にし、SPP がアプライアンスに保存するバックアップファイルの最大数を設定します。
VM 互換バックアップを許可する	SPP のハードウェアアプライアンスのバックアップをダウンロードし、SPP の仮想マシンにアップロードしてリストアすることを許可する設定です。

9.2.1 バックアップについて

SPP は、以下をバックアップします：

- 以下を除くすべての設定：
    - アプライアンス IP アドレス
    - Network Time Protocol（NTP）の設定
    - Domain Name System（DNS）構成
- 監査ログ
- SPP オブジェクトに関するすべての情報:
    - アカウント
    - アカウントグループ
    - 資産
    - 資産グループ
    - 資格
    - パーティション

- ユーザー
- ユーザーグループ

SPP は、アプライアンス外のストレージにダウンロードできるようにする前に、データを暗号化し署名します。アプライアンスにアップロードされた後のバックアップを復号化できるのは、本物の SPP アプライアンスのみです。仮想アプライアンスからダウンロードしたバックアップは、仮想アプライアンスにのみアップロードおよびリストアすることができます。ハードウェアアプライアンスからダウンロードされたバックアップは、ハードウェアアプライアンスにのみアップロードおよびリストアすることができます。ハードウェアバックアップは、ハードウェアアプライアンスが VM 互換性バックアップの認可を受けている場合、仮想互換としてダウンロードできます。VM 互換バックアップは、仮想アプライアンスにアップロードおよびリストアすることができます。

9.2.2 アーカイブサーバー

アーカイブサーバーは、バックアップファイルとセッション記録を保存する外部の物理サーバーです。アーカイブサーバーを構成および管理するには、**［バックアップと保持］**の設定ビューの**［アーカイブサーバー］**ページを使用します。

自動バックアップのスケジュールを設定し、スケジュールバックアップ中または手動でバックアップを実行する際に、自動的にアーカイブするアーカイブサーバーを指定することができます。

詳細については、「バックアップ設定」を参照してください。

詳細については、「バックアップのアーカイブ」を参照してください。

アーカイブサーバーの閲覧と管理手順

1. **［アプライアンス管理］**>**［バックアップと保持］**>**［アーカイブサーバー］**に移動します。
2. **［アーカイブサーバー］**ページには、以前に設定したアーカイブサーバーに関する以下の情報が表示されます：
    - **名前**：アーカイブサーバーの名前
    - **アーカイブ方法**：使用されている転送プロトコルの種類
    - **ネットワークアドレス**：ネットワーク上でサーバーに接続するために使用されるネットワークの DNS 名または IP アドレス
    - **ストレージパス**：アーカイブサーバーにバックアップファイルを保存するファイルパス。

- **認証タイプ**：パスワード、ディレクトリアカウント、または SSH キーなど、アーカイブサーバーへのアクセスに使用される認証のタイプ
- **SSH ホストキーのフィンガープリント**：SPP が資産への認証に使用する SSH キーのフィンガープリント
- **説明**： アーカイブサーバーに関する情報

3. これらのツールバーボタンを使用して操作を実行します。
   - **追加**：アーカイブサーバーを追加します。詳細については、「アーカイブサーバーの追加」を参照してください。
   - **削除**：削除します。選択したアーカイブサーバー構成を削除します。
   - **編集**：選択したアーカイブサーバーの構成を変更します。
   - **更新**：アーカイブサーバー構成のリストを更新します。

アーカイブサーバーの追加

アーカイブサーバーは、バックアップファイルをアーカイブするために選択したり、アプライアンスに割り当ててそのセッション記録を保存したりすることができます。

アーカイブサーバーの設定手順

1. **［アプライアンス管理］＞［バックアップと保持］＞［アーカイブサーバー］**に移動します。
2. **［追加］**をクリックします。
3. **［名前］**にアーカイブサーバーの表示名を入力します。制限：100 文字。
4. ［**説明**］にアーカイブサーバーの情報を入力します。制限：255 文字。
5. **［アーカイブ方法］**で転送プロトコルタイプを選択します：
   - **CIFS**：Common Internet File System
   - **SCP**：Secure Copy Protocol
   - **SFTP**：Secure File Transfer Program
6. **［ネットワークアドレス］**でネットワーク上のサーバーへの接続に使用する DNS 名または IP アドレスを使用します。制限：255 文字。

7. SCP または SFTP の場合、管理対象システムにログインするために使用する SSH ポートを入力します。CIFS を使用する場合はありません。

8. **［ストレージパス］**にアーカイブサーバー上でバックアップファイルを保存したいファイルパスを入力します。

9. **［認証タイプ］**で、アーカイブサーバーにアクセスするために使用する認証タイプを選択します。
    - **パスワード**（デフォルト）
    - **ディレクトリアカウント**
    - **SSH キー**（アーカイブ方法で SCP または SFTP が選択されている場合）

10. **［認証タイプ］**が**［ディレクトリアカウント］**の場合、
    a. **［アカウント名］**の**［参照］**をクリックしてアーカイブサーバーへのアクセスに使用するサービスアカウントを選択します。
    b. **［アーカイブ方法］**が **SCP** または **SFTP** の場合、アーカイブサーバーを作成するときに SSH ホストキーを自動的に受け入れるように**［SSH ホストキーの自動承認］**を選択することができます。

11. **［認証タイプ］**が**［パスワード］**の場合、
    a. **［アカウント名］**については以下のいずれかを行うことができます：
        - アプライアンス管理者として、資産管理者権限を持っているか、委任されたパーティション所有者である場合、**［参照］**をクリックして、アーカイブサーバーへのアクセスに使用するサービスアカウントを選択することができます。**ネットワークアドレス**が入力されている場合、その**ネットワークアドレス**の管理されたアカウント、または関連する**ネットワークアドレス**がないアカウントが表示されます。
          選択したアカウントは、**［リセット］**ボタンで解除することができます。
        - 管理されたアカウントを参照する代わりに、**［アカウント名］**を入力することもできます。
    b. **［パスワード］**にサービスアカウントのパスワードを入力します。
    c. **［アーカイブ方法］**で **SCP** または **SFTP** が選択されている場合、**［SSH ホストキーの自動承認］**を選択することができます。アーカイブサーバーが作成されると、SPP は自動的に SSH ホストキーを受け入れます。

12. **［アーカイブ方法］**で **SCP** または **SFTP** が選択されていて、**［認証タイプ］**として **SSH キー**を選択した場合は以下の手順を行います。

    a. **［アカウント名］**で以下のいずれかを行います：

        - アプライアンス管理者として、資産管理者権限を持っているか、委任されたパーティション所有者である場合、**［参照］**をクリックして、アーカイブサーバーへのアクセスに使用するサービスアカウントを選択することができます。**ネットワークアドレス**が入力されている場合、その**ネットワークアドレス**の管理されたアカウント、または関連する**ネットワークアドレス**がないアカウントが表示されます。
          選択したアカウントは、**［リセット］**ボタンで解除することができます。
        - 管理されたアカウントを参照する代わりに、**［アカウント名］**を入力することもできます。

    b. **［SSH キーの生成および展開］**で以下のいずれかの設定を行います：

        - **［新しい SSH キーを自動的に生成して展開します］**：**［パスワード］**を入力します。任意で**［SSH ホストキーの自動承認］**を選択すると、SPP がアーカイブサーバーを作成する際に SSH ホストキーを自動的に受け入れるようになります。
        - **［新しい SSH キーを自動的に生成して自分で展開します］**：任意で**［SSH ホストキーの自動承認］**を選択すると、SPP がアーカイブサーバーを作成する際に SSH ホストキーを自動的に受け入れるようになります。
        - **［SSH キーをインポートして自分で展開します］**：**［参照］**して SSH キーファイルを選択します。

          > **注**：SPP は、現在、authorized key のオプションを管理していません。インポートされた鍵に、資産上の authorized key ファイルで構成されたオプションがある場合、SPP によって鍵がローテートされたときに、これらのオプションは保持されません。

            i. **［参照］**をクリックします。**SSH キーのインポート**ダイアログで**［参照］**をクリックし、秘密鍵ファイルを選択します。

            ii. 必要な場合は、**［パスワード］**を入力します。秘密鍵が暗号化されている場合、パスワードが必要です。

iii. **［インポート］**をクリックします。

iv. 任意で、**［SSH ホストキーの自動承認］**を選択すると、SPP がアーカイブサーバーを作成する際に SSH ホストキーを自動的に受け入れるようになります。

13. **［接続のテスト］**をクリックし、アプライアンスがアーカイブサーバーと通信できることを確認します。
    - 接続のテスト
    - アーカイブサーバーの接続のテストが失敗する

14. **［OK］**をクリックします。

アーカイブサーバーの設定が完了したら、バックアップファイルとセッション記録の両方についてターゲットアーカイブを指定する必要があります。バックアップファイルについては、「バックアップのアーカイブ」を参照してください。

9.2.3 監査ログメンテナンス

アプライアンス管理者は、SPP が週次メンテナンス、監査ログパージ、指定アーカイブサーバーへの監査ログアーカイブを実行するように構成することができます。監査ログをアーカイブすることで、重要かつ関連性の高いデータをオンラインかつ最新の状態に保ちながら、不要になった監査ログを削除またはアーカイブすることができます。

監査ログを消去すると、バックアップの量が少なくなり、新しいクラスタメンバーを登録するときにストリームする監査ログデータが少なくなるという利点があります。Safeguard アプライアンスには、6 か月分以上の監査ログを保存しないことをお勧めします。

デフォルトの監査ログメンテナンス設定は、土曜日の午前 12 時にのみデータと監査ログを同期するようになっています。

> ⚠ **注意：監査ログのメンテナンスでは、クラスタがロックされます。アプライアンス上の監査ログデータ量、アーカイブ/パージされるデータ量、クラスタ内の同期ノード間のネットワークに応じて操作に数時間かかることがあります。**

監査ログメンテナンス設定の確認

1. プライマリアプライアンスに接続した状態で、**［アプライアンス管理］＞［バックアップと保持］＞［監査ログメンテナンス］**に移動します。

2. 構成済みの場合、以下が表示されます：

- **アーカイブ**：操作で必要な場合、アーカイブサーバー
- **アクション**：監査ログメンテナンスで定義されたアクション
- **スケジュール**：毎週 Saturday の 00:00（UTC）のようなスケジュール
- **次にスケジュールされているメンテナンス**：スケジュールされたメンテナンスが次に行される時間
- **前回成功したアーカイブ/消去**：最後にアーカイブまたは消去が成功したローカル時間
- **前回失敗したアーカイブ/消去**：最後にアーカイブまたは消去に失敗したときのローカル時間
- **前回の監査ログ同期**：最後に監査ログを同期させたローカル時間
- **前回のデータ同期**：最後のデータ同期のローカル時間

監査ログメンテナンスの設定とスケジュール

監査ログメンテナンスを定義してスケジュールするには、以下を構成します。クラスタの場合は、プライマリアプライアンスを構成します。各アクションの処理には、ある程度の時間がかかります。処理中はクラスタがロックされ、他のクラスタ操作を実行できなくなります。アクティビティセンターで進行状況を確認することができます。

1. プライマリアプライアンスに接続した状態で、**［アプライアンス管理］＞［バックアップと保持］＞［監査ログメンテナンス］**に移動します。
2. ⚙**［設定］**をクリックして、**［監査ログメンテナンス］**を構成します。
3. **監査ログメンテナンス**ダイアログで、アクションを選択します：
    - **データと監査ログのみの同期**（デフォルトアクション）：データと監査ログが同期されます。同期に失敗したデータは、翌日の設定された開始時間に再度同期が実行されます。監査ログはアーカイブされず、アプライアンスから消去されません。
    - **次の日数以上経過した監査ログをアーカイブして削除した後に同期**：指定された日数より古い監査ログは、プライマリによって指定されたアーカイブサーバーにアーカイブされます。次に、これらの監査ログは各ノードから削除されるため、各ノードの短時間のメンテナンスが必要です。消去された監査ログは復元できません。デフォルトは 365 日です。最小値は 30 日で、最大値はありません。監査ログを消去すると、バックアップの量が少なくなり、新しいクラスタメンバーを登録するときにストリームする監査ログデータが少なくなるとい

う利点があります。Safeguard アプライアンスに保存する監査ログは、6 か月分以下にすることをお勧めします。このオプションは、アーカイブサーバーを構成している場合のみ使用できます。詳細については、「アーカイブサーバーの追加」を参照してください。

a. **日数**を入力します。指定した日数より古い監査ログはアーカイブされ、アプライアンスから消去されます。デフォルトは 365 日です。最小値は 30 日で、最大値はありません。より高い保持値を使用した場合、クラスタの登録に時間がかかることがあります。データも同期されます。

b. **［アーカイブサーバーに送信］**で、構成済みのアーカイブサーバーを選択します。監査ログは、スケジュールされた監査ログメンテナンスの間、または**［今すぐ実行］**が選択されたときに、指定されたアーカイブサーバーにアーカイブされます。

- **次の日数以上経過した監査ログを削除した後に同期**：指定した日数より古い監査ログは、アプライアンスから消去されます。消去された監査ログは復元できません。デフォルトは 365 日です。最小値は 30 日で、最大値はありません。監査ログを消去する利点には、バックアップの縮小と、新しいクラスタメンバーを登録するときにストリームする監査ログデータの縮小があります。Safeguard アプライアンスには、6 か月分以上の監査ログを保存しないことをお勧めします。

4. 監査ログメンテナンスを実行するスケジュールを設定します：

a. **［曜日］**を選択します。デフォルトは土曜日です。

b. をクリックして、**［開始時間］**を選択します。デフォルトは 00:00 です。

c. タイムゾーンを選択します。デフォルトは協定世界時（UTC）です。

5. **［OK］**をクリックします。

監査ログメンテナンスの進行状況の監視

監査ログメンテナンスは、入力された構成設定とスケジュールを自動的に実行します。また、手動で監査ログメンテナンスを実行することもできます。アクションに基づき、アクティビティセンターで結果を確認します。任意の時点で操作をキャンセルする必要がある場合は、「監査ログメンテナンスのキャンセル」手順に従います。

- **データと監査ログのみの同期**（アーカイブと削除は実行しない）
    - 処理と正常終了：監査ログメンテナンスの同期には、データと監査ログの同期コンポーネントがあります。これらは、クラスタでのみ動作します。操作の開始時に、「データの一貫性を確保する」ためにクラスタがロックされます。これは**［監査ログメンテナンス］**の概要と、**［設定］＞［クラスタ管理］**の両方で確認することができます。
      データ同期の開始は、SynchronizingDataStarted イベントで記録されます。完了すると、SynchronizingDataCompleted イベントで、すべてのデータが正常に同期されたのか、一部だけが完了したのかが報告されます。次に、監査ログの同期開始が SynchronizingAuditLogStartedEvent で記録されます。完了すると、SynchonizingAuditLogCompletedEvent によって、すべての監査ログが正常に同期されたのか、一部だけが完了したのかが報告されます。

      すべてのアプライアンスに一貫したデータと監査ログがあることを保証するために、毎週すべてのデータを正常に同期する必要があります。
    - 失敗した部分：完全なイベントがすべての同期が成功しなかったことを示す場合、同期は翌日の設定された開始時間にトリガーされ、失敗した部分を再試行します。
- **次の日数以上経過した監査ログをアーカイブして削除した後に同期**
    - 処理中：監査ログのアーカイブでは、消去日以降のすべての監査ログが選択され、アーカイブされます。操作の開始時に、クラスタは監査ログをアーカイブおよび/または消去するためにロックされます。監査ログメンテナンスは、アーカイブが成功した場合にのみパージが続行されます。各アプライアンスでは、消去操作によって消去するデータがあるかどうかが判断されます。データがある場合、レプリカは一度に 1 つずつメンテナンスに入り、データを消去します。各アプライアンスがメンテナンスに入る時間は 5 分未満であるべきです。完了すると、プライマリはメンテナンス中に消去されます。クラスタロックは解除されます。監査ログのメンテナンスは、上記の箇条書きで説明した同期操作に進みます。
    - 成功：アーカイブがアーカイブサーバーに正常に送信されると、ArchiveTaskSucceeded イベントが生成されます。パージが必要で成功した場合、AuditLogPurged イベントが生成されます。クラスタロックが解除され、SchedulerJobSucceeded イベントがアーカイブ/消去操作の終了を示します。監査ログのメンテナンスは、上記で説明したように、同期するために継続されます。
    - 失敗：プライマリアプライアンスが監査ログをアーカイブできない場合、ArchiveTaskSucceeded イベントは発生せず、その後のパージは行われません。データはすべてのアプライアンスに残ります。アーカイブ/消去操作は、

ジョブ ID = core.AuditLogMaintenance を含む SchedulerJobFailed イベントで完了します。イベントには、失敗の理由が表示されます。監査ログのメンテナンスは、上記で説明したように、同期するために継続されます。

- **次の日数以上経過した監査ログを削除した後に同期**
    - 処理中：監査ログの消去は、クラスタ内の各アプライアンスから削除する消去日以降のすべての監査ログを列挙します。データを回復することはできません。操作の開始時に、クラスタは監査ログをアーカイブおよび/または消去するためにロックされます。各アプライアンスでは、消去操作によって消去するデータがあるかどうかが判断されます。データがある場合、レプリカは一度に 1 つずつメンテナンスに入り、データを消去します。各アプライアンスがメンテナンスに入る時間は 5 分未満であるべきです。完了すると、プライマリはメンテナンス中に消去されます。クラスタロックは解除されます。監査ログのメンテナンスは、上記の箇条書きで説明した同期操作に進みます。
    - 成功：消去が必要で成功した場合、AuditLogPurged イベントが発生します。クラスタロックは解放され、SchedulerJobSucceeded イベントはアーカイブ/消去操作の終了を示します。監査ログのメンテナンスは、上記で説明したように同期を取りながら継続されます。
    - 失敗：プライマリアプライアンスが監査ログを削除できない場合、操作は、ジョブ ID = core.AuditLogMaintenance を含む SchedulerJobFailed イベントで完了します。イベントには、失敗の理由が表示されます。監査ログのメンテナンスは、上記で説明したように同期化するために継続されます。

監査ログメンテナンスの手動実行

手動で監査ログメンテナンスを実行することができます。監査ログメンテナンスの設定に基づき、上記と同様の動作が実行されます。各操作は処理に時間がかかります。処理中はクラスタがロックされ、他のクラスタ操作を実行することはできません。アクティビティセンターで進行状況を確認できます。

1. プライマリアプライアンスに接続した状態で、**［アプライアンス管理］＞［バックアップと保持］＞［監査ログメンテナンス］**に進みます。
2. **［設定］**をクリックし、監査ログメンテナンスの構成が正しいことを確認します。
3. **［今すぐ実行］**をクリックして、構成通りに監査ログメンテナンスを実行します。確認ダイアログボックスが表示されます。どのように進めるかは、選択したアクションによって異なります。

- アクションが**「データと監査ログのみの同期**（アーカイブと削除は行わない）**」**場合、**［同期］**ダイアログボックスが表示されます。
    - テキストボックスに**「同期」**と入力し、**［今すぐ実行］**をクリックします。アクティビティセンターで進捗状況を監視するには、「監査ログメンテナンスの進捗状況の監視」を参照してください。
- アクションが、**「次の日数以上経過した監査ログをアーカイブして削除した後に同期」**の場合、アーカイブダイアログボックスにアーカイブサーバーの名前が表示されます。
    - テキストボックスに**「アーカイブ」**と入力し、**［今すぐ実行］**をクリックします。アクティビティセンターで進捗状況を監視するには、「監査ログメンテナンスの進行状況の監視」を参照してください。
- アクションが**「次の日数以上経過した監査ログを削除した後に同期」**の場合、保持ポリシー（入力した日数）に従って監査ログが消去されることを示す**「消去」**ダイアログが表示されます。消去された監査ログは復元できません。
    - テキストボックスに**「消去」**と入力し、**［今すぐ実行］**をクリックします。アクティビティセンターで進捗状況を監視するには「監査ログメンテナンスの進行状況の監視」を参照してください。

監査ログメンテナンスのキャンセル

監査ログメンテナンスの実行中は、クラスタがロックされ、**［キャンセル］**ボタンが利用可能になります。**［キャンセル］**をクリックすると、**［クラスタのロック解除］**確認ダイアログが表示されます。**［クラスタのロック解除］**と入力し、**［クラスタのロック解除］**をクリックします。クラスタロックはすぐに解除されますが、操作が完了したことを確認するために、次のようにアクティビティセンターを監視する必要があります。詳細については、「監査ログメンテナンスの進行状況の監視」を参照してください。

- **データと監査ログのみの同期：**キャンセルすると、ロックはすぐに解除されますが、作業の完了についてはアクティビティセンターを監視する必要があります。アクティビティセンターで、SynchronizingDataCompletedEvent、SynchronizingAuditLogsCompletedEvent の順に表示されてから他のクラスタリング操作を進め、クラスタのすべてのノードがすべての監査データを保持していることを確認します。キャンセルされると、クラスタは翌日の監査ログ管理開始時間に監査ログの同期を完了しようとします。

- **次の日数以上経過した監査ログをアーカイブして削除した後に同期**：キャンセルすると、ロックはすぐに解除されますが、作業の完了については、アクティビティセンターを監視する必要があります。監査ログのアーカイブおよび/または消去のためにクラスタがロックされている間にキャンセルすることを選択した場合、アーカイブ/パージが完了したことを示すジョブ ID = core.AuditLogMaintenance を含む SchedulerJobSucceeded または SchedulerJobFailed イベントについてアクティビティセンターを監視してください。監査ログメンテナンスは関係なく同期を続けます。また、データの一貫性を確保するために、クラスタがロックされていることを確認したら、キャンセルする必要があります。アクティビティセンターで、操作の完了を示す SynchronizingAuditLogCompleted イベントを監視します。これで、クラスタリング操作を続けても安全です。
- **次の日数以上経過した監査ログを削除した後に同期**：キャンセルするとロックはすぐに解除されますが、作業が完了するかどうかアクティビティセンターを監視する必要があります。監査ログのアーカイブおよび/または消去のためにクラスタがロックされている間にキャンセルすることを選択した場合、アーカイブ/消去が完了したことを示すジョブ ID = core.AuditLogMaintenance を含む SchedulerJobSucceeded または SchedulerJobFailed イベントについてアクティビティセンターを監視してください。監査ログメンテナンスは関係なく同期を続けます。また、データの一貫性を確保するために、クラスタがロックされていることを確認したら、キャンセルする必要があります。アクティビティセンターで、操作の完了を示す SynchronizingAuditLogCompleted イベントを監視します。これで、クラスタリング操作を続行しても大丈夫になりました。

クラスタ管理から監査ログメンテナンスをキャンセルする手順

次の手順でクラスタのロックを解除することにより、クラスタ管理から監査ログメンテナンスをキャンセルすることもできます。詳細については、「ロックされたクラスタのロック解除」を参照してください。

1. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**に移動します。
2. **［クラスタ管理］**で、「監査ログのアーカイブおよび/または消去」と「開始時間」のバナーが表示されます。このメッセージは、処理中はクラスタがロックされ、他のクラスタ操作を実行できないことを思い出させるものです。操作が完了すると、クラスタは自動的にロックが解除されます。
3. 警告バナーの右上隅にある 🔒 ロックアイコンをクリックします。
4. **［クラスタのロック解除］**確認ダイアログで、**「クラスタのロック解除」**と入力し、**［OK］**をクリックします。

これにより、クラスタ内のすべてのアプライアンスにかけられたクラスタロックが解除され、操作が終了します。

> **重要**: ロックされたクラスタのロックを解除する際には、注意が必要です。クラスタ内の 1 つ以上のアプライアンスがオフラインで、現在のオペレーションを終了しないことが確実な場合にのみ使用する必要があります。クラスタのロックを強制的に解除すると、アプライアンスが不安定になり、工場出荷時のリセットが必要になり、クラスタの再構築が必要になる場合があります。進行中の操作に確信が持てない場合は、クラスタのロックを解除しないでください。

9.2.4 バックアップと復元

SPP のバックアップを管理するのは、アプライアンス管理者の責任です。

ベストプラクティスは、バックアップをアプライアンスの外部にあるアーカイブサーバーに保存し、壊滅的なディスクまたはハードウェア障害が発生した場合でも、バックアップイメージを復元できるようにすることです。アプライアンスには最小限のバックアップファイルのみを保存します。Safeguard Backup Files (.sgb)をダウンロードまたはアーカイブした後、**［削除］**を使用してそれらを削除します。アプライアンスに保持するバックアップファイルの最大数は、**［バックアップと保持］**で設定できます。

バックアップを最大限に保護するために、アプライアンス管理者はクラスタ全体の GPG 公開鍵またはパスワード暗号化を構成することができます。どちらを選んでも、クラスタ内の各アプライアンスから生成された後続のバックアップはすべて保護されます。GPG による保護は、ダウンロードまたはアーカイブされたときに適用されます。パスワードによる保護は、生成時に適用されます。詳細については、以下を参照してください：

- バックアップの保護設定
- バックアップのアップロード
- バックアップの復元

［アプライアンス管理］＞［バックアップと保持］＞［バックアップと復元］に移動します。

［バックアップと復元］ページには、現在データベース内にあるバックアップの以下の情報が表示されます。

表：バックアップと復元：プロパティ

プロパティ	説明
日付	バックアップの日付
進行状況	バックアップの状態：実行中または完了
ファイルサイズ	バックアップファイルのサイズ（MB）
アプライアンス名	アプライアンスの名前
アプライアンスのバージョン	SPP アプライアンスのバージョン
保護タイプ	保護タイプを表示するアイコン • （デフォルト）標準保護：パスワードや GPG キーは必要ありません。 • GPG 公開キー保護：リストアするバックアップをアップロードする際に秘密鍵が必要です。 • パスワード保護：バックアップを復元する際にパスワードが必要です。
ユーザー	バックアップを作成したユーザーの名前
前回のアーカイブ日	選択したバックアップが実行された日付
アーカイブサーバー名	バックアップがアーカイブされたサーバーの名前
ファイル名	Safeguard バックアップファイル名（.sgb ファイル）

SPP のバックアップを管理するには、以下のツールバーボタンを使用します。

表：バックアップと復元：ツールバー

オプション	説明
＋ 今すぐ実行	アプライアンスに現在あるデータのバックアップコピーを作成します。詳細については、「今すぐ実行」を参照してください。
削除	選択したバックアップファイルを**［バックアップ］**ページおよび SPP データベースから削除します。バックアップは即座に削除されます。
ダウンロード	選択したバックアップファイルをアプライアンス上の場所に保存します。詳細については、「バックアップのダウンロード」を参照してください。

オプション	説明
VM 互換のダウンロード	このオプションを使用して VM 互換バックアップをダウンロードし、SPP の仮想マシンにアップロードして復元することができます。VM 互換バックアップをダウンロードするには、パスワードまたは GPG 公開鍵保護設定で作成されている必要があります。ハードウェアアプライアンスの VM 互換バックアップをダウンロードするオプションを有効にするには、「VM 互換のバックアップの認可」を参照してください。 **重要：**ハードウェアから VM 互換としてダウンロードされたバックアップをハードウェアにアップロードすることはできません。
アップロード	ファイルの場所からバックアップファイルを取得し、**[バックアップ]** ページのリストに追加します。詳細については、「バックアップのアップロード」を参照してください。
復元	現在のデータを上書きし、SPP を選択したバックアップに復元します。詳細については、「バックアップの復元」を参照してください。
アーカイブ	バックアップファイルを外部のアーカイブサーバーに保存します。詳細については、「バックアップのアーカイブ」を参照してください。
設定	• **バックアップ設定**：自動バックアップのスケジュールを設定します。詳細については、「バックアップ設定」を参照してください。 • **バックアップ保護設定：**アプライアンスまたはクラスタ全体の保護のためにプライマリアプライアンスでバックアップ暗号化を設定します。詳細については、「バックアップの保護設定」を参照してください。
更新	**[バックアップ]** ページのバックアップファイルのリストを更新します。

今すぐ実行

［今すぐ実行］をクリックすると、手動でトリガーして新しいバックアップを作成することができます。アプライアンスまたはプライマリアプライアンスでパスワードまたは GNU Privacy Guard (GPG) 暗号化がクラスタ全体の暗号化のために設定されている場合、それらの暗号化設定は**［今すぐ実行］**を選択したときに強制されます。

［アーカイブサーバーに送信］を選択した場合、バックアップはアーカイブサーバーに送信されます。詳細については、「バックアップ設定」を参照してください。

新しいバックアップの作成手順

1. **［アプライアンス管理］＞［バックアップと保持］＞［バックアップと復元］**に移動します。
2. ＋**［今すぐ実行］**をクリックします。「バックアップファイルを追加しています」進捗バーが表示されます。
3. クラスタ全体のバックアップ暗号化のためにアプライアンスまたはプライマリアプライアンスでパスワード暗号化が必要な場合、パスワードを入力するよう求められます。暗号化が設定されている場合、必要に応じてバックアップを後で復元するために、パスワードまたはプライベート GPG キーが利用可能であることを確認します。詳細については、「バックアップと復元」、「バックアップの保護設定」を参照してください。
4. Safeguard バックアップファイル（.sgb）が作成されたことを確認します。

> ⚠ **注意：ローカルログイン制御設定で設定された［パスワードの最大有効期間］よりも古いバックアップを復元すると、（Bootstrap 管理者を含む）すべてのユーザーアカウントがロックアウトされ、すべてのユーザーアカウントのパスワードをリセットしなければならなくなります。この状況を回避するには、バックアップを実行する前に［パスワードの最大有効期間］をゼロにリセットし、復元後にリセットしてください。**

> **ヒント**: ベストプラクティスは、バックアップは**［パスワードの最大有効期間］**設定よりも頻繁に実行することです。

> ⚠ **注意：SPP は、バックアップ中に処理中のアクセスリクエストワークフローイベントを復元することはできません。**

> ⚠ **注意：ハードウェアセキュリティモジュールを統合して作成したバックアップを復元する場合、バックアップ作成時に使用した暗号化キーがまだ存在し、SPP アプライアンスか**

> **らアクセス可能であることが必要です。そうでない場合、アプライアンスはバックアップのデータを暗号化するために使用されたハードウェアセキュリティモジュールの設定を確認することができません。復元を続行することはできますが、SPP アプライアンスはその過程で隔離される可能性が高いので、これは推奨されません。**

バックアップのダウンロード

SPP では、選択したバックアップファイルをコンピューター上の任意の場所に保存することができます。SPP は選択したバックアップファイルをコピーしますが、バックアップと復元ページに表示されるリストからバックアップを削除することはありません。アプライアンスからバックアップがダウンロードされると、Appliance Backup Downloaded イベントが生成され、監査ログに送信されます。このイベントには、バックアップが VM 互換としてダウンロードされたかどうかが記録されます。リスト表示からファイルを削除するには、ファイルを選択し、🗑 **［削除］**をクリックします。

バックアップファイルのダウンロード

1. **［アプライアンス管理］＞［バックアップと保持］＞［バックアップと復元］**に移動します。
2. バックアップファイルを選択します：
    - **ダウンロード**：このオプションを使用して、選択したバックアップファイルをアプライアンス上の場所に保存します。
    - **VM 互換のダウンロード**：このオプションを使用して、VM 互換バックアップをダウンロードし、Safeguard 仮想マシンにアップロードして復元することができます。VM 互換バックアップをダウンロードするには、パスワードまたは GPG 公開鍵保護設定で作成されている必要があります。これは、VM 互換のバックアップの認可をリクエストし、承認されたハードウェアアプライアンスでのみ利用可能です。

      > **重要**：VM 互換としてハードウェアからダウンロードされたバックアップをハードウェアにアップロードすることはできません。
3. .sgb ファイルは、ブラウザーの設定で定義されているブラウザーのダウンロードフォルダーにダウンロードされます。このファイルは、日付を含む次のような名前になります: 946d66a4fecb4359a8b01fab75519d80_Safeguard_Backup_20200617-165625.sgb

    > **注**：通常のダウンロードと VM 互換ダウンロードでは、ダウンロードされるバックアップのファイル名に違いはありません。

バックアップのアップロード

SPP ファイルの場所から Safeguard バックアップファイル（.sgb）を取得し、SPP アプライアンスバックアップと復元ページのリストに追加することができます。詳細については、「バックアップの復元」を参照してください。

バックアップがアプライアンスに正常にアップロードされると、アプライアンスバックアップアップロードイベントが生成され、監査ログに保存されます。アプライアンスへのバックアップのアップロードが失敗すると、「Appliance Backup Upload Failed」イベントが生成され、監査ログに保存されます。

仮想マシンから生成およびダウンロードされたバックアップは、仮想マシンにのみアップロードできます。ハードウェアアプライアンスで生成およびダウンロードされたバックアップは、ハードウェアアプライアンスにのみアップロードできます。ハードウェアアプライアンスで VM 互換として生成およびダウンロードされたバックアップは、仮想マシンにのみアップロードできます。

バックアップファイルのアップロード手順

> **重要：** バックアップのアップロードを開始したら、ページを閉じたり更新したりしないでください。これらを行うと、ブラウザーがアップロードの記録を失い、プロセスを再開する必要があります。

1. バックアップの暗号化に GPG 公開鍵が使用された場合、SPP にアップロードする前に、秘密鍵の所有者が Safeguard バックアップファイル（.sgb）を復号化する必要があります。詳細については、「バックアップの保護設定」を参照してください。
2. Safeguard バックアップファイル（.sgb）をアップロードするには、**［アプライアンス管理］＞［バックアップと保持］＞［バックアップと復元］**に移動します。
3. ↥ **［アップロード］**をクリックします。
4. **［参照］**してバックアップファイルを選択し、**［開く］**をクリックします。バックアップファイルのアップロードの進捗バーが表示されます。完了すると、ファイルがアップロードされ、復元できるようになります。詳細については、「バックアップの復元」を参照してください。

バックアップの復元

SPP では、選択したバックアップのデータでアプライアンス上のデータを復元できます。SPP は、アプライアンス IP アドレス、NTP 設定、DNS 設定は復元しません。

復元後に設定が正しいかどうかを確認するには、次のページに移動します：
［アプライアンス管理］＞［アプライアンス］＞［アプライアンス情報］

クラスタ化されたアプライアンスのリストアには、特別な考慮事項があります。詳細については、「クラスタ化されたアプライアンスを復元するためのバックアップの使用」を参照してください。

> ⚠ **注意：「ローカルログイン制御」設定で設定されたパスワード最大有効期間よりも古いバックアップを復元すると、すべてのユーザーアカウント（Bootstrap Administrator を含む）が無効になり、すべてのユーザーアカウントのパスワードまたは SSH キーをリセットする必要があります。Bootstrap Administrator のパスワードがロックアウトされている場合、リカバリキオスクからリセットできます。詳細については、「admin パスワードのリセット」を参照してください。**

> ⚠ **注意：ハードウェアセキュリティモジュールを統合して作成したバックアップを復元する場合、バックアップ作成時に使用した暗号化キーがまだ存在し、SPP アプライアンスからアクセス可能であることが必要です。そうでない場合、アプライアンスはバックアップのデータを暗号化するために使用されたハードウェアセキュリティモジュールの設定を確認することができません。復元を続行することはできますが、SPP アプライアンスはその過程で隔離される可能性が高いので、これは推奨されません。**

バックアップを復元する際のバージョンの考慮事項

アプライアンス管理者は、SPP バージョン 6.0.0.12276 までのバックアップを復元することができます。データのみがリストアされ、実行中のバージョンは変更されません。

アプライアンスで実行中のバージョンより新しいバージョンからバックアップを復元することはできません。復元は失敗し、次のようなメッセージが表示されます。Restore failed because backup version [version] is newer than one currently running [version]（バックアップ バージョン［バージョン］は現在実行中のものよりも新しいので、復元に失敗しました）。

バックアップバージョンと実行中のバージョンは、Safeguard がリストアを開始、完了、または失敗したときに生成されるアクティビティセンターのログに表示されます。

SPP アプライアンスをバックアップから復元する手順

1. **［アプライアンス管理］＞［バックアップと保持］＞［バックアップと復元］**に移動します。

2. バックアップを選択します。バックアップファイルが一覧にない場合は、.sgb バックアップファイルを **アップロード**することができます。詳細については、「バックアップのアップロード」を参照してください。

3. **［復元］**をクリックします。

   問題のある状態が検出されると、**［バックアップの復元に関する警告］**が表示され、**［復元の警告、X の警告］**メッセージに詳細が表示されます。**［キャンセル］**をクリックして復元プロセスを停止して警告に対処するか、**［続行］**をクリックして次の警告（ある場合）に進むか、プロセスを完了します。

4. バックアップがパスワードで保護されている場合は、**［保護されたバックアップのパスワード］**ダイアログが表示されます。**［バックアップパスワードを入力］**テキストボックスにパスワードを入力します。入力したパスワードが正しくない場合は、**［OK］**ボタンが無効となり、処理を進めることができません。詳細については、「バックアップの保護設定」を参照してください。

5. **［復元］**ダイアログが表示されたら、ボックスに**「復元」**と入力し、**［復元］**をクリックします。SPP は、必要に応じてアプライアンスを自動的に再起動します。

6. バックアップからの復元後、以下が正しく設定されていることを確認します。

   - 自動バックアップスケジュールでアーカイブサーバーを確認します。必要に応じて、正しいアーカイブサーバーを設定します。詳細については、「バックアップのアーカイブ」を参照してください。
   - セッションアーカイブの設定でアーカイブサーバーを確認します。必要に応じて、正しいアーカイブサーバーを設定します。埋め込みセッションモジュールを使用していて、アーカイブサーバーを設定している場合、アーカイブサーバーはアーカイブされたセッションを再生するように設定されている必要があります。
   - バックアップを別のアプライアンスに復元した場合、管理されたネットワークに割り当てられたアプライアンスがなくなります。パスワードと SSH キーの管理および検出タスクは失敗します。詳細については、「管理対象ネットワーク」を参照してください。

7. アプライアンスが完全に動作するようになると、クライアントを再起動するように要求されます。バックアップの作成以降に SPP オブジェクトに対して行われたすべての変更は失われます。

> ⚠ **注意：復元後、要求者、承認者、レビュー担当者は、バックアップの時点で処理中だったアクセスリクエストワークフローイベントにアクセスできなくなります。アクティビティセンターには、これらのワークフローイベントが未完成として表示されます。**

バックアップのアーカイブ

SPP では、バックアップファイルを外部のアーカイブサーバーに保存することができます。

バックアップファイルのアーカイブ手順

1. **［管理ツール］＞［設定］＞［バックアップと保持］＞［Safeguard バックアップと復元］**の順に移動します。
2. アーカイブするバックアップを選択します。
3. **［アーカイブ］**をクリックし、**［アーカイブバックアップ］**を選択します。
4. アーカイブサーバー選択ダイアログで、**［アーカイブサーバー］**を選択します。

   > **メモ**：アーカイブサーバー選択ダイアログからアーカイブサーバーを追加するには、ツールバーの「アーカイブサーバーの追加」ボタンをクリックします。

SPP は、バックアップファイルをアーカイブサーバーにコピーします。

バックアップ設定

自動バックアップのスケジュールを設定することができます。

バックアップをスケジュールして、その間隔（分、時間、日、週、または月）のバックアップがすでに実行されている場合、次の分、時間、日、週、または月が来るまでは別のバックアップは実行されません。たとえば、今日すでにバックアップが発生しており、バックアップスケジュールを毎日バックアップするように設定した場合、SPP は明日までバックアップを実行しません。バックアップスケジュールウィンドウの終了時刻は、開始時刻より後でなければなりません。

バックアップスケジュールの設定手順

1. **［アプライアンス管理］＞［バックアップと保持］＞［バックアップと保持］**に移動します。
2. ⚙**［設定］**をクリックします。
3. **［バックアップ設定］**ダイアログで、バックアップのスケジュールを指定します。
    - 以下を設定します：

      開始時刻と終了時刻を指定せず実行間隔を指定するには、次のコントロールから選択します。開始時刻と終了時刻を指定する場合は、このセクションの**［時間ウィンドウを使用］**選択に移動します。

        - **なし**：設定されたスケジュールに従ってジョブは実行されません。それでも手動でジョブを実行することは可能です。
        - **分**：指定した分単位の頻度でジョブが実行されます。たとえば、間隔を **30 分**に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないことをお勧めします。
        - **時間**：指定した分単位の設定ごとに実行されます。たとえば、午前 9 時で午前 9 時 15 分から 2 時間おきに、15 分経過した時点でジョブを実行したい場合、**［バックアップ間隔 2/時間/正時 @分 15］**を設定します。
        - **日数**：入力された日数と時間の頻度で実行されます。たとえば、午前 0 時前に隔日でジョブを実行する場合は、**［バックアップ間隔 2/日数/開始：23:59］**と設定します。
        - **週**：指定した時刻と曜日に、週単位の頻度で実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［バックアップ間隔 2/週/開始 05:00/次の日に繰り返し 月曜、水曜、金曜］**を設定します。
        - **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［バックアップ間隔： 2/月/開始 01:00］、［その月の曜日 /First/Saturday］**を設定します。
    - **開始**時刻と**終了**時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。＋**［追加］**または －**［削除］**をクリックすると、複数の時間制限を制御することができます。各タイムウィンドウは、1 分以上の間隔をあけ、重ならないようにする必要があります。

たとえば、毎日 22 時から 2 時まで 10 分おきにジョブを実行する場合、次の値を入力します：

［バックアップ間隔 10/分］、［時間ウィンドウを使用］を選択します。

- **開始： 22:00 / 終了 23:59**
- **開始： 0:00 / 終了 02:00**

  開始 22:00 / 終了 02:00 と入力すると、終了時刻が開始時刻より後でなければならないため、エラーになります。

  日数、**週**、**月**を選択した場合、入力した時間枠の中でジョブを何回繰り返すかを選択することができます。

  1 日おきに 10 時 30 分に 4 時から 20 時の間に 2 回実行するジョブの場合、次の値を入力します：

  ［バックアップ間隔 2/日数］、［時間ウィンドウを使用］を選択して**［開始 4:00 / 終了 20:00 / 繰返し 2］**に設定してください。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行が終了すると、そのタスクは次の即時インターバルに再スケジュールされます。

4. **［アーカイブサーバーに送信］**では、スケジュールバックアップ中または手動バックアップ実行時にアプライアンスから外部にバックアップファイルを保存するために、構成済みのアーカイブサーバーを選択します。詳細については、「アーカイブサーバーの追加」を参照してください。
5. **［バックアップ保護］**設定を選択することができます。詳細については、「バックアップの保護設定」を参照してください。
6. **［OK］**をクリックして変更を保存し、ページを閉じます。

バックアップの保護設定

最大限の保護を実現するために、アプライアンスまたはプライマリアプライアンスでバックアップの暗号化を設定し、クラスタ全体の保護を実現します。Safeguard バックアップファイル（.sgb）は、次のいずれかの方法で暗号化することができます：

- 標準（デフォルト）：パスワードまたは GPG キーは必要ありません。
- パスワード: 任意のパスワード値を入力できます。バックアップを復元するには、このパスワードが必要です。

> ⚠ **注意： パスワードは必ず安全な保管庫に保存してください。バックアップを復元するために必要なパスワードを復元する方法はありません。**

- GNU Privacy Guard（GPG）公開鍵（RSA のみ）：公開鍵とメタデータを含む .txt ファイルをアップロードするか、公開鍵とメタデータをコピーして SPP に貼り付けることができます。GPG 公開キーで作成されたバックアップファイルは、ダウンロードまたはアーカイブされるときに暗号化されます。ファイルをアップロードして復元する前に、秘密鍵の所有者だけがバックアップファイルを復号化することができます。秘密鍵の所有者がバックアップを復号化すると、バックアップはアプライアンス保護のみが選択されたときに生成されたバックアップと同じになります。

> ⚠ **注意： GPG 秘密鍵は必ず安全な保管庫に保存してください。秘密鍵がないと、GPG で保護されたファイルの暗号化を解除する方法がありません。**

一度設定すると、今後手動または自動で作成されるバックアップは保護されます。

SPP は、無効なバックアップのアップロードの試行をすべて検出します。バックアップが GNU Privacy Guard（GPG）で暗号化されている場合、次のようなメッセージが表示されます。「アップロードされたファイルは、本物の Safeguard バックアップイメージとして検証できませんでした。アプライアンスからブロックされました。」失敗したバックアップロードに対して、無効な署名を含むエラー理由とともに、監査イベントが作成されます。

詳細については、以下を参照してください。

- バックアップのアップロード
- バックアップの復元

バックアップ保護の設定手順

1. GPG キー保護を使用する場合、公開鍵ファイルを生成し、アップロードまたはコピー＆ペーストする .txt ファイルを作成します。
2. **［アプライアンス管理］＞［バックアップと復元］**に移動し、**［設定］**をクリックします。
3. **［バックアップ設定］**ダイアログから、アプライアンスのバックアップ保護の種類を選択します。プライマリアプライアンスの設定は、クラスタにレプリケートされます。設定は、各クラスタノードで読み取り専用になります。
   - **アプライアンス保護のみ**：これはデフォルトであり、バックアップのパスワードまたは GPG キーによる保護は含まれません。バックアップは、Safeguard の純正バックアップとしてのみ暗号化されます。

- **パスワード保護の追加**：選択した場合、**［バックアップパスワード］**テキストボックスにパスワードを入力します。パスワードがすでに存在する場合は、静的な数のドットが表示されます。既存のパスワードの代わりに新しいパスワードを入力し、そのパスワードを確認することができます。入力したパスワードは、パスワードを設定した時点から変更するまでのバックアップに使用されます。パスワード情報は、必ず安全な保管庫に保管してください。
- **GPG キー保護の追加**：選択した場合、次のいずれかを実行します：
  - **［参照］**をクリックして、先ほど作成した .txt ファイルから公開鍵ファイルをアップロードします。
  - 先ほど作成した公開鍵の情報をテキストボックスに貼り付けます。

  このダイアログに戻ると、公開鍵ファイルを識別するための名前、フィンガープリント、詳細が表示されます。

  送信した GPG 公開鍵は、保護が設定されてから変更されるまでに生成されたバックアップに使用されます。GPG が設定されている間にバックアップが生成されると、生成後にアプライアンスで変更された設定に関係なく、常に GPG 公開キー暗号化でダウンロードまたはアーカイブされます。GPG 公開鍵暗号化は、バックアップのメタデータと一緒に残ります。さらに、バックアップを別のアプライアンスにアップロードする場合、バックアップを再度ダウンロードすると、最初に提供されたものと同じ GPG 公開キーで暗号化されます。

4. **［OK］**をクリックします。

バックアップ保持

アプライアンスに保存するバックアップファイルの最大数を設定するのは、アプライアンス管理者の責任です。

アプライアンスのバックアップ保持設定の構成手順

1. **［アプライアンス管理］＞［バックアップと保持］＞［バックアップ保持］**に移動します。
2. アプライアンスに保存するバックアップファイルの最大数を入力します。アプライアンスに保存するバックアップファイルの数には、0～40 を入力できます。**［保存］**をクリックします。

最大数のバックアップファイルが保存されると、次回のバックアップ実行時に、最も古い日付のバックアップファイルが削除されます。

9.2.5 VM 互換のバックアップの認可

SPP Web クライアントでは、ハードウェアアプライアンス上でバックアップを生成し、Safeguard 仮想マシン上にアップロードしてリストアすることができます。

> **重要:** ハードウェアアプライアンスから仮想マシンへの移行には潜在的なセキュリティリスクがあるため、この機能を有効にする前に、リクエストを行うアプライアンス管理者は、このプロセスの一部として One Identity サポートに連絡する必要があります。この承認は、［Authorize VM Compatible Backups］ページの上部にある［Not Authorized/Authorized］インジケータによって表示されます。

> **重要:** 以前にハードウェアから VM 互換としてダウンロードしたバックアップを、ハードウェアアプライアンスにアップロードすることはできません。そのようなバックアップは、Safeguard 仮想マシンにのみアップロードできます。

> **重要:** この機能は、クラスタ内のレプリカでは使用できません。

仮想マシンで使用するハードウェアアプライアンスのバックアップ生成許可

1. **［アプライアンス管理］＞［バックアップと保持］＞［VM 互換バックアップの承認］**を開きます。
2. **［チャレンジリクエストユーザー識別子］**フィールドに、バックアップの生成の許可を要求するユーザーの名前を入力します。
3. **［リクエストの生成］**をクリックします。

   > **重要:** 一度にアクティブにできるチャレンジリクエストは 1 つだけです。保留中のチャレンジリクエストがすでにアクティブになっている場合、新しいリクエストを生成する前に、既存のチャレンジリクエストを無効にするチェックボックスを選択することで、アクティブなリクエストを取り消すことができます。

4. **チャレンジリクエスト**テキストボックスが表示されます。このテキストボックスには、VM 互換バックアップ認証リクエストが有効であることを確認するために One Identity が必要とする情報が含まれています。以下のオプションのいずれかを使用して、情報をコピーします。

- **リクエストのコピー**：チャレンジリクエストをクリップボードにコピーします。
- **リクエストのダウンロード**：チャレンジリクエストをテキストファイルにダウンロードします。

5. ハードウェアアプライアンスからの VM 互換バックアップのダウンロードを承認するリクエストについては、One Identity Support にお問い合わせください。リクエストされたら、コピーまたはダウンロードしたチャレンジリクエストを One Identity Support に送信します。

6. One Identity Support がリクエストを確認すると、チャレンジレスポンスが返送されます。このテキストは、**チャレンジレスポンス**テキストボックスにコピー/ペーストするか、アップロード（**[参照]**ボタンを使用）する必要があります。

7. **［レスポンスの検証］**をクリックすると、リクエストが承認されたことが確認されます。

   確認されると、[Authorize VM Compatible Backups] ページの上部に [Authorized] インジケータが表示されます。ハードウェアアプライアンスの**［バックアップと復元］**ページのボタンから**［VM 互換のダウンロード］**オプションが利用できるようになります。VM 互換バックアップをダウンロードするには、パスワードまたは GPG 公開鍵保護設定で作成されている必要があります。

   この機能を無効にするには、**［認証の削除］**ボタンを使用します。再度有効にするには、One Identity Support に新しいチャレンジリクエストを送信する必要があります。

9.3 証明書

証明書設定を使用して、SPP を保護するために使用される証明書を管理します。このページのペインには、置き換え可能なデフォルトの証明書、または SPP に追加されたユーザー提供の証明書が表示されます。

SPP で使用される証明書を管理するのは、アプライアンス管理者の責任です。

［アプライアンス管理］＞［証明書］を選択します。

表：証明書設定

設定	説明
監査ログ署名証明書	アーカイブサーバーに保存された監査ログを検証するために使用される監査ログ署名証明書を管理する場所です。監査ログがエクスポートされるとき、ログが正当であり、エクスポート後に改ざんされていないことを確認するために、この証明書でログに署名されます。
証明書署名リクエスト	SPP で発行された証明書署名要求 (CSR) を表示および管理します。SPP で作成される可能性のある CSR は以下の通りです：監査ログ署名証明書、SMTP クライアント証明書、SSL 証明書、Syslog クライアント証明書
ハードウェアセキュリティモジュール証明書	クライアントおよびサーバーのハードウェアセキュリティモジュール証明書を管理します。これらの証明書は、ハードウェアセキュリティモジュールデバイスに接続するために使用されます。
SMTP クライアント証明書	SMTP クライアント証明書を管理します。
SSL/TLS 証明書	証明書のインストールや、公開 SSL/TLS 証明書を登録するための CSR の作成など、SSL/TLS 証明書を管理します。この証明書は、すべての HTTP トラフィックを保護するために使用されます。
Syslog クライアント証明書	SPP と Syslog サーバー間のトラフィックを保護するために使用される Syslog クライアント証明書を管理します。
信頼できる CA 証明書	SPP によって信頼される証明書を追加および管理し、さまざまな用途で証明書の信頼の連鎖を検証するために使用します。たとえば、信頼できる証明書は、お客様の会社のルート認証局(CA)証明書または中間証明書である場合があります。

9.3.1 証明書（CSR）について

SPP で証明書署名要求（CSR）を作成することができます。秘密鍵は SPP アプライアンスで安全に保管され、公開されることはありません。公開鍵と詳細は、エンコードされたテキストファイルになっています。以下はその手順です：

1. SPP から CSR を作成します。詳しくは以下を参照してください：
    - 監査ログ証明書署名リクエストの作成
    - SMTP 証明書署名リクエストの作成
    - SSL/TLS 証明書署名リクエスト（CSR）の作成
    - Syslog クライアント証明書署名リクエストの作成
2. エンコードされたテキストファイルを認証局（CA）に提出し、CA を信頼する他のエンティティから信頼される適切な X509 証明書を作成します。
3. CA によって生成された証明書を、秘密鍵に関連付けられた SPP にインストールします。次を参照してください。
    - 監査ログ署名証明書のインストール
    - SMTP 証明書のインストール
    - SSL/TLS 証明書のインストール
    - Syslog クライアント証明書のインストール
4. 必要に応じて、SPP の信頼された証明書に CA 証明書を追加します。詳細については、「信頼できる CA 証明書」を参照してください。

SPP の証明書インフラストラクチャは、次のように構成されています。

交換可能な証明書

SPP には、以下のデフォルト証明書が同梱されていますが、信頼されていないため交換してください。

- 監査ログ署名証明書
- SMTP 証明書
- SSL/TLS 証明書
- Syslog クライアント証明書

ユーザー提供の証明書

使用するセキュリティ証明書を指定することができます。証明書を交換または追加する場合は、以下の点に留意してください：

- SPP は、あらゆる種類の証明書を登録するための Certificate Signing Requests (CSR) をサポートしています。CSR は、PKCS (Public-Key Cryptography Standard) #10 形式を使用します。
- インポートする場合、SPP は関連するネットワークリソースにアクセスし、署名済み CSR で指定された CRL エンドポイントを検証する必要があります。
- 秘密鍵付きの証明書をアップロードする場合、SPP は PKCS #12 標準に従った .pfx （または .p12）ファイルをサポートします。
- CSR で生成された証明書をインストールする場合、SPP は DER エンコードファイル（.cer、.crt、.der）と PEM エンコード ファイル（.pem）をサポートします。
- SSL/TLS 証明書については、SPP では、CSR をアップロードまたは使用して、複数の証明書を登録し、異なるアプライアンスに適用することができます。
- SPP は SSL/TLS 証明書ストアを提供し、アップロードまたは登録された証明書を任意のアプライアンスに割り当てることができます。
- サーバーの署名権限証明書を SPP の信頼された証明書ストアに追加する必要があるかどうかを検討します。たとえば、SSL/TLS サーバー証明書検証を使用する資産を追加する前に、署名機関証明書を信頼された証明書ストアに追加する必要があります。または、秘密鍵付きの Syslog 証明書をアップロードした場合、その証明書のルート CA を信頼済み証明書のリストにアップロードすることもできます。詳細については、「信頼できる CA 証明書」を参照してください

9.3.2 監査ログ署名証明書

証明書設定ページの**［監査ログ署名証明書］**ペインには、アーカイブサーバーに保存された監査ログファイルに署名するために使用される証明書についての詳細が表示されます。

監査ログ署名証明書は、監査ログが特定の SPP クラスタによって作成され、そこから来たものであることを証明します。

監査ログ署名証明書の定義

監査ログ署名証明書は 1 つだけ定義でき、同じクラスタ内のすべての SPP アプライアンスで使用されます。デフォルトの監査ログ署名証明書が提供されますが、独自の証明書をロードすることをお勧めします。証明書をアップロードしない場合、デフォルトが使用されます。詳しくは、「監査ログ署名証明書のインストール」を参照してください。

証明書署名要求（CSR）の生成

監査ログ署名証明書を定義したら、証明書署名要求（CSR）の作成を使用して、証明書署名要求（CSR）を生成することをお勧めします。詳細については、「監査ログ証明書署名リクエストの作成」を参照してください。

共通の署名形式が使用されます。各監査ログアーカイブは、SHA256 ハッシュアルゴリズムを使用してハッシュ化されます。ハッシュ値は、監査ログ署名証明書の秘密鍵で、PSS 署名パディングを使用した RSA 署名を使用して署名されます。署名ファイルは、アーカイブファイルと同じファイル名で作成されますが、拡張子は.sig となります。

署名証明書の使用方法

この署名証明書は、エクスポートされた監査ログ履歴が SPP クラスタから発信されたものであることを確認したい管理者が使用します。

この証明書の公開鍵は、署名された監査ログを検証するために利用できる必要があり、証明書チェーンの場合は、証明書の発行元を検証します。

> **重要**: Safeguard-ps PowerShell コマンドレットの 6.6 バージョンから、Test-SafeguardAuditLogArchive という新しいコマンドレットが追加されました。このコマンドレットは、アーカイブされた ZIP ファイル内のすべての監査ログファイルを 1 つのコマンドで検証し、各ファイルの結果を表示します。このコマンドレットを実行するとき、ZIP ファイル内の個々のログファイルの署名を検証します。OneIdentity/safeguard-ps を参照してください。

OpenSSL を使用したい場合、または PowerShell コマンドレットが行うことの詳細については、次の説明も参照してください。

1. 監査ログのパブリック証明書を取得します。以下を参照してください：
    - 独自の PKI を使用している場合、公開証明書が利用可能である必要があります。
    - 次の SPP API から Base64 形式のパブリック証明書を取得します。

      GET /AuditLog/Retention/SigningCertificate
2. パブリック証明書を API から取得した場合、Base64 データを cert.pem に保存します。
3. OpenSSL を使用して、pem ファイルを公開鍵ファイルに変換します。
    - openssl x509 -pubkey -in cert.pem -noout > cert.pub
4. OpenSSL を使用して、監査ログファイルが署名され、その内容が有効であることを確認します。

- openssl dgst -sha256 -sigopt rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -signature <signature-file>.sig -verify cert.pub <audit-log-file>

監査ログ署名証明書の管理

［アプライアンス管理］＞［証明書］＞［監査ログ署名証明書］に移動します。監査ログ署名証明書を管理するために、以下のプロパティとコントロールが利用可能です。

表：監査ログ証明書：プロパティ

プロパティ/コントロール	説明
更新	**［更新］**をクリックすると、**「監査ログ署名証明書」**ペインに表示される証明書が更新されます。
件名	証明書が要求されたときに割り当てられたサブジェクト（ユーザー、プログラム、コンピューター、サービス、その他のエンティティなど）の名前
サムプリント	証明書を識別するための一意のハッシュ値
証明書の追加	**［証明書の追加］**をクリックし、次のオプションのいずれかを選択して、デフォルトの証明書を新しい証明書に置き換えます。 • **CSR から生成された証明書のインストール** • **秘密キーを含む証明書のインストール** • **証明書署名リクエスト（CSR）の作成**
デフォルトを使用	**［デフォルトを使用する］**をクリックすると、証明書がデフォルトに戻されます。

監査ログ証明書署名リクエストの作成

SPP で提供されるデフォルトのセッション証明書を使用しない場合、CSR（Certificate Signing Request）を使用して証明書を登録し、デフォルトの証明書を置き換えることができます。後でデフォルトの証明書に戻すことができます。

監査ログ署名証明書 CSR 作成手順

1. **［アプライアンス管理］＞［証明書］＞［監査ログ署名証明書］**に移動します。

2. 置き換える証明書の**［証明書の追加］**ボタンをクリックし、**［証明書署名リクエスト（CSR）の作成］**を選択します。

3. **［署名リクエストの作成］**ダイアログで、以下の情報を入力します。

    a. **サブジェクト（識別名）**：証明書を発行する個人またはエンティティの識別名を、cn=Common name,ou=organizational unit,o=organization のような適切な書式で入力してください。
    例：cn=sam doe,ou=marketing,o=mycompany
    最大文字数は 500 文字です。

        - **［識別名の作成者を使用］**をクリックすると、**［完全修飾ドメイン名］、［部門］、［組織］、［都市/地域］、［州/国/地域］、［国］**に基づいて識別名を作成することができます。

    b. **サブジェクトの別名（DNS）**：任意で、この証明書によって保護されるサーバーのデータソース（DNS）名を入力します。例えば、SPP クラスタ内のすべてのアプライアンスの DNS 名になる可能性があります。DNS 名が変更された場合は、新しい証明書を生成する必要があります。

    c. **サブジェクトの別名（IP アドレス）：**任意で、この証明書によって保護されるサーバーの IP アドレスを入力します。例えば、SPP クラスタ内のすべてのアプライアンスの IP アドレスになる可能性があります。IP アドレスが変更された場合は、新しい証明書を生成する必要があります。

    d. **キーサイズ**：秘密鍵ペアのビット長を選択します。ビット長によって、証明書のセキュリティレベルが決まります。ビット長が大きいほど、セキュリティが強固であることを意味します。

        - 1024
        - 2048（デフォルト）
        - 4096

4. **［OK］**をクリックします。「次の証明書リクエストを保存して、証明機関（CA）に送信してください。」のようなメッセージが表示されます。

5. **［保存］**をクリックし、証明書署名リクエスト（CSR）をファイルに保存します。保存しない場合、別の証明書署名リクエスト（CSR）を生成する必要があります。

6. **監査ログ署名証明書**ペインで**［更新］**をクリックし、追加された証明書のリストを更新します。

監査ログ署名証明書のインストール

SPP に付属するデフォルトの証明書を使用しないことをお勧めします。代わりに、秘密鍵を持つ別の証明書に置き換えます。

デフォルトの証明書を独自の証明書に置き換えるには、その証明書が次のものである必要があります。

- サーバー認証（1.3.6.1.5.5.7.3.1）OID 値を持つ拡張キー使用法（Enhanced Key Usage）を使用します。
- サーバー認証（2.5.29.37.3）OID 値を持つ Digital Signature キー使用法

CSR は以下の形式でインストールすることができます。

- 以下を含む CSR から生成された証明書をインストールします。
    - DER エンコードファイル（.cer、.crt、.der）
    - PEM エンコードされたファイル（.pem）
- 以下を含む秘密鍵付き証明書のインストール
    - PKCS#12（.p12 または.pfx）
    - 個人情報交換ファイル（.pfx）

監査ログ署名証明書のインストール手順

1. **［アプライアンス管理］＞［証明書］＞［監査ログ署名証明書］**に移動します。
2. 交換するセッション証明書の**［証明書の追加］**ボタンをクリックします。適切なオプションを選択します：
    - **CSR から生成された証明書のインストール**
    - **秘密キーを含む証明書のインストール**
3. **［参照］**して、証明書ファイルを選択し、**［OK］**をクリックします。
4. 秘密鍵付きの証明書をインストールする場合は、ダイアログボックスが表示されます。証明書をインポートするために、大文字と小文字を区別するパスフレーズを入力しま

す。証明書に秘密鍵のパスフレーズがない場合は、フィールドを空のままにして、**［OK］**をクリックします。

5. インストールされると、この新しい証明書は、**「監査ログ署名証明書」**ペインに表示されているデフォルトの証明書と置き換わります。

監査ログ署名証明書のアップロードに失敗した場合、監査ログに AuditLogSigningCertificateUploadFailed と記録されます。

デフォルト証明書の使用手順

SPP に付属しているデフォルトのセッション証明書を使用することができます。

1. **［アプライアンス管理］＞［証明書］＞［監査ログ署名証明書］**に移動します。
2. 監査ログ署名証明書をデフォルトに置き換えるには、**［デフォルトを使用］**ボタンをクリックします。
3. 警告ダイアログで「**デフォルト**」と入力し、デフォルトの証明書に戻すことを確認します。
4. **［デフォルト］**をクリックして確定します。

9.3.3 証明書署名リクエスト

証明書の中には、認証局（CA）が証明書リクエストを処理する前に、デジタル署名を必要とするものがあります。次のような場合、SPP で証明書署名リクエストを作成する必要がある場合があります。

- 監査ログ署名証明書
- SMTP 証明書
- SSL/TLS 証明書
- Syslog クライアント証明書

証明書署名リクエストペインには、証明書署名リクエスト（CSR）を通じて登録された証明書に関する詳細が表示されます。このペインでは、CSR を削除することもできます。

［アプライアンス管理］＞［証明書］＞［証明書署名リクエスト］の順に移動します。CSR を介して登録された証明書は、このペインに表示され、以下の詳細が表示されます。

表：証明書署名リクエスト：プロパティ

プロパティ	説明
件名	証明書の発行対象となる個人またはエンティティの識別名
証明書タイプ	要求された証明書のタイプ • 監査ログ署名証明書 • SSL 証明書
キーサイズ	秘密鍵ペアのビット長
サムプリント	証明書を識別するための一意のハッシュ値
有効期限	CSR の有効期限がある場合、その期限
代替 DNS 名	証明書がリクエストされたときに指定された追加または代替のホスト名（サイトまたはコモンネームなど）。詳細については、「監査ログ証明書署名リクエストの作成」を参照してください。
代替 IP アドレス	証明書がリクエストされたときに指定された追加または代替のホスト名（IP アドレスやコモンネームなど）。詳細は、「監査ログ証明書署名リクエストの作成」を参照してください。

以下のツールバーボタンを使用して、証明書署名リクエストを管理します。

表：証明書署名リクエスト：ツールバー

オプション	説明
署名リクエストの削除	選択した CSR を SPP から削除します。
更新	CSR のリストを更新します。

9.3.4 ハードウェアセキュリティモジュール証明書

SPP を使用すると、アプライアンス管理者は、Thales Network Luna デバイスに接続するための秘密鍵付きハードウェアセキュリティモジュールクライアント証明書とハードウェアセキュリティモジュールサーバー証明書の両方をアップロードすることができます。

ハードウェアセキュリティモジュールクライアント証明書

［アプライアンス管理］＞［証明書］＞［ハードウェアセキュリティモジュールクライアント証明書］に移動します。

ハードウェアセキュリティモジュールクライアント証明書の以下の情報を表示するには、証明書を選択します。

表：クライアント証明書：プロパティ

プロパティ	説明
件名	証明書がリクエストされたときに割り当てられた件名（ユーザー、プログラム、コンピューター、サービス、その他のエンティティなど）の名前
アプライアンス	証明書が割り当てられたアプライアンスの名前がリストアップされます。
件名	証明書を発行した認証局（CA）名
サムプリント	証明書を識別するための一意のハッシュ値
次まで無効	証明書を使用する前に満たす必要のある開始日時
有効期限	証明書の有効期限が切れ、使用できなくなる日時

ハードウェアセキュリティモジュールのクライアント証明書を管理するには、これらのツールバーボタンを使用します。

表：クライアント証明書：ツールバー

アクション	説明
＋ 証明書の追加	ハードウェアセキュリティモジュールのクライアント証明書をアップロードします。詳しくは、「ハードウェアセキュリティモジュールのクライアント証明書インストール」を参照してください。
選択項目の削除	選択した証明書を SPP から削除します。
アプライアンスへの証明書の割り当て	選択した証明書を 1 つまたは複数のアプライアンスに割り当てます。詳細については、「ハードウェアセキュリティモジュールクライアント証明書の割り当て」を参照してください。

アクション	説明
アプライアンスからの証明書割り当て解除	選択した証明書を 1 つまたは複数のアプライアンスから割り当て解除します。
更新	利用可能なハードウェアセキュリティモジュールクライアント証明書のリストを更新します。

ハードウェアセキュリティモジュールサーバー証明書

［アプライアンス管理］＞［証明書］＞［ハードウェアセキュリティモジュール証明書］に移動します。

表：サーバー証明書：プロパティ

プロパティ	説明
件名	証明書がリクエストされたときに割り当てられた件名（ユーザー、プログラム、コンピューター、サービス、その他のエンティティなど）の名前
発行元	証明書を発行した認証局(CA)の名前
証明書タイプ	Unknown と表示されます
サムプリント	証明書を識別するための一意のハッシュ値
次まで無効	証明書を使用する前に満たす必要のある開始日時
有効期限	証明書の有効期限が切れ、使用できなくなる日時

ハードウェアセキュリティモジュールのサーバー証明書を管理するには、これらのツールバーボタンを使用します。

表：サーバー証明書：ツールバー

アクション	説明
＋ 証明書のアップロード	ハードウェアセキュリティモジュールのクライアント証明書をアップロードします。詳しくは、「ハードウェアセキュリティモジュールクライアント証明書のインストール」を参照してください。
選択項目の削除	選択した証明書を SPP から削除します。

アクション	説明
更新	証明書のリストを更新します。

ハードウェアセキュリティモジュールクライアント証明書のインストール

ハードウェアセキュリティモジュールクライアント証明書のインストール手順

1. **［アプライアンス管理］＞［証明書］＞［ハードウェアセキュリティモジュール証明書］＞［クライアント証明書］**に進みます。
2. ＋**［証明書の追加］**をクリックします。
3. **［クライアントの公開キー］**で**［ファイルのアップロード］**をクリックします。
4. クライアント証明書の公開鍵ファイルを選択し、**［開く］**をクリックします。
5. **［クライアントの秘密キー］**で**［ファイルのアップロード］**をクリックします。
6. クライアント証明書の秘密キーのファイルを選択し、**［開く］**をクリックします。
7. **［クライアント証明書の追加］**ダイアログで**［OK］**をクリックします。証明書がアップロードされたら、その証明書を 1 つまたは複数のアプライアンスに割り当てる必要があります。詳細については、「ハードウェアセキュリティモジュールクライアント証明書の割り当て」を参照してください。

ハードウェアセキュリティモジュールクライアント証明書の割り当て

SPP では、事前にアップロードしたハードウェアセキュリティモジュールのクライアント証明書をクラスタ環境内の任意のアプライアンスに割り当てることができます。

アプライアンスへのクライアント証明書の割り当て手順

1. **［アプライアンス管理］＞［証明書］＞［ハードウェアセキュリティモジュール証明書］＞［クライアント証明書］**に移動します。

2. 証明書を選択し、**［アプライアンスへの証明書の割り当て］**をクリックします。
3. **［アプライアンスへの証明書の割り当て］**ダイアログで、1 つまたは複数のアプライアンスを選択します。
4. **［OK］**をクリックします。

ハードウェアセキュリティモジュールサーバー証明書のアップロード

SPP では、ハードウェアセキュリティモジュールサーバー証明書をアップロードすることができます。

ハードウェアセキュリティモジュールサーバー証明書のアップロード手順

1. **［アプライアンス管理］＞［証明書］＞［ハードウェアセキュリティモジュール証明書］＞［サーバー証明書］**に移動します。
2. **［証明書のアップロード］**をクリックします。
3. サーバー証明書を選択し**［開く］**をクリックします。

9.3.5 SMTP 証明書

初期状態では、使用されるデフォルトの自己署名付き SMTP クライアント証明書がリストされ、アプライアンスに割り当てられています。このデフォルトの証明書は信頼できる証明書ではないので、交換する必要があります。

考慮すべきこと：

- リモート証明書は、有効な CN および/または DNS SAN を持つ必要があり、以下の場合は CRL を発行する必要があります：
    - SMTP で TLS (STARTTLS または SMTPS) が使用されている。
    - **［アプライアンス管理］＞［外部統合］＞［メール］**で［**SMTP サーバー証明書の検証］**が選択されている。
- SPP は、デフォルトモードと TLS 1.2 モードの両方で SMTP TLS 用の暗号スイートをサポートしています。詳細については、「暗号のサポート」を参照してください。

- SMTP ユーザー認証に管理されたドメインアカウントが使用されている場合、リモート SMTP サーバーは user@domain 形式のユーザー名を受け入れる必要があります。

［アプライアンス管理］＞［証明書］＞［SMTP クライアント証明書］へ移動します。

SMTP クライアント証明書ペインには、データベースに保存されている SMTP クライアント証明書に関する以下の情報が表示されます。

表：SMTP クライアント証明書：プロパティ

プロパティ	説明
更新	利用可能な（SPP にアップロードされた）SMTP クライアント証明書のリストを更新します。
件名	証明書がリクエストされたときに割り当てられた件名（ユーザー、プログラム、コンピューター、サービス、その他のエンティティなど）の名前
サムプリント	証明書を識別するための一意のハッシュ値
証明書の追加	**［証明書の追加］**をクリックし、以下のオプションを選択します： • **CSR から生成された証明書のインストール** • **秘密キーを含む証明書のインストール** • **証明書署名リクエスト(CSR)の作成**
デフォルトの使用	デフォルトの SMTP クライアント証明書に戻す場合にクリックします。

SMTP 証明書署名リクエストの作成

ハードウェアセキュリティモジュールのサーバー証明書を管理するには、これらのツールバーボタンを使用します。

SMTP 証明書用 CSR の作成手順

1. **［アプライアンス管理］＞［証明書］＞［SMTP クライアント証明書］**に移動します。
2. 置き換える証明書の**［証明書の追加］**ボタンをクリックし、**［証明書署名リクエスト（CSR）の作成］**を選択します。

3. **［署名リクエストの作成］**ダイアログで、以下の情報を入力します。

    a. **サブジェクト（識別名）**：証明書を発行する個人またはエンティティの識別名を、cn=Common name,ou=organizational unit,o=organization のような適切な書式で入力してください。
    例：cn=sam doe,ou=marketing,o=mycompany
    最大文字数は 500 文字です。

        - **［識別名の作成者を使用］**をクリックすると、**［完全修飾ドメイン名］、［部門］、［組織］、［都市/地域］、［州/国/地域］、［国］**に基づいて識別名を作成することができます。

    b. **キーサイズ**：秘密鍵ペアのビット長を選択します。ビット長によって、証明書のセキュリティレベルが決まります。ビット長が大きいほど、セキュリティが強固であることを意味します。

        - 1024
        - 2048（デフォルト）
        - 4096

4. **［OK］**をクリックして保存します。証明書が SMTP クライアント証明書ペインに表示されます。

SMTP 証明書のインストール

SPP に付属するデフォルトの SMTP クライアント証明書を使用しないことをお勧めします。

デフォルトの SMTP クライアント証明書を独自の証明書に置き換えるには、その証明書が次のものである必要があります。

- サーバー認証（1.3.6.1.5.5.7.3.1）OID 値を持つ拡張キー使用（Enhanced Key Usage）
- サーバー認証（2.5.29.37.3）OID 値を持つ Digital Signature キー使用

CSR は以下の形式でインストールすることができます。

- 以下を含む CSR から生成された証明書をインストールします：
    - DER エンコードファイル（.cer、.crt、.der）
    - PEM エンコードされたファイル（.pem）
- 以下を含む秘密鍵付き証明書のインストール：
    - PKCS#12（.p12 または.pfx）
    - 個人情報交換ファイル（.pfx）

SMTP 署名証明書のインストール手順

1. **［アプライアンス管理］＞［証明書］＞［SMTP クライアント証明書］**に移動します。SMTP クライアント証明書ペインにデータベースに保存されている SMTP 証明書の情報が表示されます。

2. 交換する SMTP 証明書の**［証明書の追加］**ボタンをクリックします。適切なオプションを選択します：
    - **CSR から生成された証明書のインストール**
    - **秘密キーを含む証明書のインストール**

3. **［参照］**して、証明書ファイルを選択し、**［OK］**をクリックします。

4. インストールされると、この新しい証明書は、**「監査ログ署名証明書」**ペインに表示されているデフォルトの証明書と置き換わります。

デフォルト証明書の使用手順

1. **［アプライアンス管理］＞［証明書］＞［SMTP クライアント証明書］**に移動します。

2. SMTP 証明書をデフォルトに置き換えるには、**［デフォルトを使用］**ボタンをクリックします。

3. 警告ダイアログで「**デフォルト**」と入力し、デフォルトの証明書に戻すことを確認します。

4. **［デフォルト］**をクリックして確定します。

9.3.6 SSL/TLS 証明書

SPP では、アプライアンス管理者がプライベートキー付きの SSL 証明書をアップロードしたり、CSR を使用して SSL 証明書を登録したりできます。

初期状態では、HTTPS に使用されるデフォルトの自己署名入り SSL 証明書がリストされ、アプライアンスに割り当てられています。このデフォルトの証明書は信頼できる証明書ではないので、交換する必要があります。

［アプライアンス管理］＞［証明書］＞［SSL/TLS 証明書］に移動します。**［SSL/TLS 証明書］**ペインには、データベースに保存されている SSL 証明書に関する以下の情報が表示されます。

表：SSL/TLS 証明書：プロパティ

プロパティ	説明
件名	証明書がリクエストされたときに割り当てられたサブジェクト（ユーザー、プログラム、コンピューター、サービス、その他のエンティティなど）の名前
アプライアンス	証明書が割り当てられているアプライアンス名前一覧
発行者	証明書を発行した認証局（CA）の名前
サムプリント	証明書を識別するための一意のハッシュ値
代替 DNS 名	証明書が要求されたときに指定された追加または代替のホスト名（サイト、コモンネームなど）。詳しくは「SSL/TLS 証明書署名リクエスト（CSR）の作成」を参照してください。
代替 IP アドレス	証明書が要求されたときに指定された追加または代替のホスト名（IP アドレス、コモンネームなど）。詳しくは「SSL/TLS 証明書のインストール」を参照してください。デフォルトの自己署名 SSL 証明書の場合、アプライアンスの名前と IP アドレス
次まで無効	証明書を使用する前に満たす必要のある開始日時
有効期限	証明書の有効期限が切れ、使用できなくなる日時

以下のツールバーボタンを使用して、SSL 証明書を管理します。

表：SSL/TLS 証明書：ツールバー

オプション	説明
＋ 証明書の追加＞証明書のアップロード	SSL 証明書をアップロードします。詳細については、「SSL/TLS 証明書のインストール」を参照してください。
＋ 証明書の追加＞証明書署名リクエスト（CSR）の作成	証明書を登録するための CSR を作成します。詳細については、「SSL/TLS 証明書署名リクエスト（CSR）の作成」を参照してください。
選択項目の削除	選択した証明書を SPP から削除します。

オプション	説明
アプライアンスへの証明書の割り当て	選択した証明書を 1 つまたは複数のアプライアンスに割り当てます。詳細については、「アプライアンスへの SSL/TLS 証明書の割り当て」を参照してください。
アプライアンスからの証明書の割り当て解除	選択した証明書を 1 つまたは複数のアプライアンスから割り当て解除します。
更新	利用可能な SSL 証明書（SPP にアップロードされたもの）のリストを更新します。

SSL/TLS 証明書署名リクエスト（CSR）の作成

CSR を作成する場合、リクエストされた証明書を使用するユーザーまたはエンティティを一意に識別します。SPP では、CSR を使用して SSL 証明書をアップロードまたは登録することができます。アップロードまたは登録された SSL 証明書は SSL 証明書ストアに追加され、1 つまたは複数の SPP アプライアンスに割り当てることができるようになります。

SSL 用 CSR 作成手順

1. **［アプライアンス管理］＞［証明書］＞［SSL/TLS 証明書］**に移動します。
2. ＋**［証明書の追加］**ボタンをクリックし、**［証明書署名リクエスト（CSR）の作成］**を選択します。
3. **［署名リクエストの作成］**ダイアログで、以下の情報を入力します。
    a. **サブジェクト（識別名）**：証明書を発行する個人またはエンティティの識別名を、cn=Common name,ou=organizational unit,o=organization のような適切な書式で入力してください。
    例：cn=sam doe,ou=marketing,o=mycompany
    最大文字数は 500 文字です。
        - **［識別名の作成者を使用］**をクリックすると、**［完全修飾ドメイン名］、［部門］、［組織］、［都市/地域］、［州/国/地域］、［国］**に基づいて識別名を作成することができます。
    b. **サブジェクトの別名（DNS）**：任意で、この証明書によって保護されるサーバーのデータソース（DNS）名を入力します。例えば、SPP クラスタ内のす

べてのアプライアンスの DNS 名になる可能性があります。DNS 名が変更された場合は、新しい証明書を生成する必要があります。

c. **サブジェクトの別名（IP アドレス）：**任意で、この証明書によって保護されるサーバーの IP アドレスを入力します。例えば、SPP クラスタ内のすべてのアプライアンスの IP アドレスになる可能性があります。IP アドレスが変更された場合は、新しい証明書を生成する必要があります。

d. **キーサイズ**：秘密鍵ペアのビット長を選択します。ビット長によって、証明書のセキュリティレベルが決まります。ビット長が大きいほど、セキュリティが強固であることを意味します。

- 1024
- 2048（デフォルト）
- 4096

4. **［OK］**をクリックします。「次の証明書リクエストを保存して、証明機関（CA）に送信してください。」のようなメッセージが表示されます。

5. **［保存］**をクリックし、証明書署名リクエスト（CSR）をファイルに保存します。保存しない場合、別の証明書署名リクエスト（CSR）を生成する必要があります。

6. **署名証明書**ペインで**［更新］**をクリックし、追加された証明書のリストを更新します。

SSL/TLS 証明書のインストール

SSL 証明書をインストール手順：

1. **［アプライアンス管理］＞［証明書］＞［SSL/TLS 証明書］**を開きます。

2. ＋**［証明書の追加］**をクリックし、**［証明書のアップロード］**を選択します。

3. **［参照］**し、証明書ファイルを選択して**［開く］**をクリックします。

4. ダイアログボックスで、証明書をインポートするための大文字と小文字を区別するパスフレーズを入力します。証明書に秘密鍵のパスフレーズがない場合は、フィールドを空のままにして、**［OK］**をクリックします。

5. 証明書がアップロードされたら、その証明書を 1 つまたは複数のアプライアンスに割り当てます。詳細については、「アプライアンスへの SSL/TLS 証明書の割り当て」を参照してください。

⚠ **注意: プライベート SSL キーへの不適切なアクセスは、アプライアンスとの間のトラフィックを危険にさらす可能性があります。最も安全な構成にするには、証明書署名リクエスト（CSR）を作成し、通常の署名機関によって署名してもらいます。**

その後、署名されたリクエストを SPP SSL Webserver Certificate として使用します。この方法では、SPP が使用するプライベート SSL キーに管理者がアクセスすることはできず、トラフィックは安全に保たれます。

アプライアンスへの SSL/TLS 証明書の割り当て

SPP は、クラスタが所有する SSL 証明書ストアをサポートします。これにより、以前にアップロードした、または CSR を介して登録した SSL 証明書を、クラスタ化された環境内の任意のアプライアンスに割り当てることができます。

アプライアンスへの証明書の割り当て手順

1. **［アプライアンス管理］＞［証明書］＞［SSL/TLS 証明書］**に移動します。
2. グリッドから証明書を選択し、ツールバーの **「アプライアンスへの証明書の割り当て」**ボタンをクリックします。
3. **［アプライアンス］**ダイアログで、1 つまたは複数のアプライアンスを選択し、**［OK］**をクリックして選択内容を保存します。

証明書の割り当て解除も、同じ手順て行います。

9.3.7 Syslog クライアント証明書

アプライアンス管理者は、SPP が匿名クライアントを受け入れない Syslog サーバーに認証されたメッセージを送信できるように、Syslog クライアント証明書をアップロードすることができます。詳細については、「Syslog」を参照してください。

定義可能な Syslog クライアント証明書は 1 つだけで、同じクラスタ内のすべての SPP アプライアンスで使用されます。

デフォルトの Syslog クライアント証明書を使用するのではなく、**［証明書署名リクエスト（CSR）の作成］**を使用して証明書署名リクエスト（CSR）を生成することをお勧めします。詳細については、「Syslog クライアント証明書署名リクエストの作成」を参照してください。

署名証明書リクエスト（CSR）の管理

Syslog クライアント証明書を定義、生成、管理するには、**［アプライアンス管理］＞［証明書］＞「Syslog クライアント証明書」**に移動します。

以下のプロパティとコントロールは、シスログクライアント証明書を管理するために利用できます。

表：Syslog クライアント証明書：プロパティ

プロパティ	説明
更新	使用されているクライアント証明書の最新情報を取得します。
件名	証明書がリクエストされたときに割り当てられた件名の名前
サムプリント	証明書を識別するための一意のハッシュ値
有効期限	証明書の有効期限
証明書の追加	**［証明書の追加］**をクリックし、以下のオプションを選択します： • **CSR から生成された証明書のインストール** • **秘密キーを含む証明書のインストール** • **証明書署名リクエスト(CSR)の作成**
デフォルトの使用	**［デフォルトを使用］**をクリックすると、証明書がデフォルトにリセットされます。 デフォルトでは、データは転送中に暗号化されますが、クライアント/サーバーの認証は行われません。

Syslog クライアント証明書署名リクエストの作成

証明書署名リクエスト（CSR）は、デジタル署名された証明書を取得するために、認証局（CA）に提出されます。CSR を作成する場合、リクエストされた証明書を使用するユーザーまたはエンティティを一意に識別します。SPP では、CSR を使用して Syslog クライアント証明書をアップロードまたは登録することができます。アップロードまたは登録されると、Syslog クライアント証明書は Syslog クライアント証明書ストアに追加され、1 つまたは複数の SPP アプライアンスに割り当てることができるようになります。

Syslog 用 CSR の作成手順

1. **［アプライアンス管理］＞［証明書］＞［Syslog クライアント証明書］**に移動します。
2. **［証明書の追加］**をクリックし、**［証明書署名リクエスト（CSR）の作成］**を選択します。
3. **［署名リクエストの作成］**ダイアログで、以下の情報を入力します。
    a. **サブジェクト（識別名）**：証明書を発行する個人またはエンティティの識別名を、cn=Common name,ou=organizational unit,o=organization のような適切な書式で入力してください。
    例：cn=sam doe,ou=marketing,o=mycompany
    最大文字数は 500 文字です。
        - **［識別名の作成者を使用］**をクリックすると、**［完全修飾ドメイン名］、［部門］、［組織］、［都市/地域］、［州/国/地域］、［国］**に基づいて識別名を作成することができます。

    b. **キーサイズ**：秘密鍵ペアのビット長を選択します。ビット長によって、証明書のセキュリティレベルが決まります。ビット長が大きいほど、セキュリティが強固であることを意味します。
        - 1024
        - 2048（デフォルト）
        - 4096
4. **［OK］**をクリックして保存します。

Syslog クライアント証明書のインストール

Syslog クライアント証明書のインストール手順

1. **［アプライアンス管理］＞［証明書］＞［Syslog クライアント証明書］**に移動します。
2. **［証明書の追加］**をクリックし適切なオプションを選択します：
    - **秘密鍵付きの証明書のインストール**：証明書と秘密鍵を含む PFX ファイルをアップロードします。
    - **CSR から生成した証明書のインストール**：CSR を生成して、信頼できる CA に署名してもらいます。
3. **［参照］**して、証明書ファイルを選択し、インストールを完了します。

4. **秘密キーパスフレーズを入力で**
    - 証明書をインポートするためのパスフレーズを入力し、**[OK]**をクリックします。 をクリックすると、パスフレーズが表示されます。
    - パスフレーズがない場合は、フィールドを空白にして、**[OK]**をクリックします。

5. アップロードした鍵の**件名**、**サムプリント**、**有効期限**が表示されます。必要に応じて、**[デフォルトを使用]**を選択して確認ダイアログに応答すると、デフォルトに戻すことができます。

6. プライベートキー付きの証明書をアップロードした場合、その証明書のルート CA を信頼済み証明書のリストにアップロードすることができます。詳細については、「信頼できる CA 証明書」を参照してください。

9.3.8 信頼できる CA 証明書

SPP アプライアンスに信頼できるルート証明書を追加または削除するのは、アプライアンス管理者の責任です。サーバー証明書を検証する場合は、**[信頼できる証明書]**のサーバー証明書の信頼チェーンから証明書が必要です。

例：

- 秘密キー付きの Syslog クライアント証明書をアップロードした場合、その証明書のルート CA を信頼済み証明書のリストにアップロードする必要がある場合があります。詳細については、「Syslog クライアント証明書」を参照してください。
- SSL/TLS 証明書は、機関のチェーンを解決するために信頼される必要があります。SSL/TSL 証明書では、SPP が SSL 証明書の検証オプションを有効にした資産に接続すると、資産が提示する証明書の署名権限が、信頼できる証明書ストアにある証明書と比較されます。詳細については、「ディレクトリアカウント」を参照してください。

以下に移動します。

[アプライアンス管理] > [証明書] > [信頼できる CA 証明書]に移動します。

証明書を選択して、信頼済み証明書ストアに追加されたユーザー提供の証明書にについて、以下の情報が表示されます：

表：信頼できる CA 証明書：プロパティ

プロパティ	説明
件名	証明書が要求されたときに割り当てられた件名（ユーザー、プログラム、コンピューター、サービス、その他のエンティティなど）の名前
発行者	証明書を発行した認証局（CA）の名前
証明書タイプ	Trusted 信頼できる
サムプリント	証明書を識別するための一意のハッシュ値
次まで無効	証明書を使用する前に満たさなければならない「開始」日時
有効期限	証明書の有効期限が切れて使用できなくなる日付と時刻

ツールバーオプションは以下の通りです：

表：信頼できる CA 証明書：ツールバー

オプション	説明
新しい信頼できる CA 証明書のアップロード	信頼できる証明書を追加します。
信頼できる CA 証明書の削除	選択した証明書を削除します。
更新	証明書のリストを更新します。

信頼できる証明書の追加

SSL サーバー証明書の検証を使用する資産を追加する前に、証明書のルート CA と中間 CA を SPP の信頼できる証明書ストアに追加してください。

Syslog サーバーの証明書が同じ CA によって署名されている場合、追加する必要がある場合があります。

証明書のアップロードに失敗すると、監査ログに TrustedCertificateUploadFailed または ServerCertificateUploadFailed と表示されます。

信頼できる証明書の追加手順

1. **［アプライアンス管理］＞［証明書］＞［信頼できる CA 証明書］**に移動します。
2. 詳細ツールバーから ＋ **［新しい信頼できる CA 証明書のアップロード］**をクリックします。
3. **［参照］**をクリックし、証明書ファイルを選択して**［開く］**を選択します。
4. ダイアログボックスで、大文字と小文字を区別するパスフレーズを入力して、証明書をインポートします。証明書に秘密鍵のパスフレーズがない場合は、フィールドを空のままにして、**［OK］**をクリックします。

信頼できる証明書の削除

アプライアンスから証明書を削除する手順

1. **［アプライアンス管理］＞［証明書］＞［信頼できる CA 証明書］**に移動します。
2. 証明書を選択します。
3. 詳細ツールバーの 🗑 **［信頼できる CA 証明書の削除］**をクリックします。

> **重要**: SPP では、組み込みの認証局を削除することはできません。

9.4　クラスタ

クラスタ環境の作成、クラスタとそのメンバーの状態の監視、および高可用性と負荷分散を目的とした管理対象ネットワークの定義には、クラスタ設定を使用します。

クラスタの作成、クラスタの状態の監視、および管理対象ネットワークの定義は、アプライアンス管理者または運用管理者の責任で行います。

SPP クラスタを作成する前に、「ディザスタリカバリとクラスタ」の章をよく読んで理解してください。

- プライマリアプライアンスとレプリカアプライアンス
- コンセンサス
- SPP でサポートされているクラスタ

- ポート
- アプライアンスがクラスタとのコンセンサスを失った場合（接続性や可用性が失われた場合など）、自動または手動でアクセスリクエスト、承認、解放を可能にするオフラインワークフロー：「オフラインワークフローモードの手動制御」
- クラスタへの登録：レプリカをクラスタに登録する
- コンセンサスを失ったクラスタの回復：詳細については、「コンセンサスが失われたクラスタのリセット」を参照してください。

［アプライアンス管理］＞［クラスタ］に移動します。

表：クラスタ設定

設定	説明
クラスタ管理	クラスタの作成と管理、およびクラスタとそのメンバーの健全性の監視を行う場所です。
管理対象ネットワーク	クラスタ環境のタスク負荷を分散させるための管理対象ネットワークを定義する場所です。
オフラインワークフロー	アプライアンスのコンセンサス（クォーラム）が失われた場合に自動的に起動するオフラインワークフローモードを設定し、オプションでオンラインワークフローを自動的に再開することができます。また、ここでは、手動で**［オフラインワークフローの有効化］**と**［オンライン操作の再開］**を行うこともできます。詳細については、「オフラインワークフローモードとは」を参照してください。
セッションアプライアンス	セッションの記録と監査のために SPS クラスタが SPP にリンクしている場合に、リンク接続を表示、編集、および削除する場所です。詳細については、「SPP と SPS のリンクガイダンス」を参照してください。

9.4.1 クラスタ管理

クラスタ管理では、クラスタの作成と診断ができます。

Web クライアントからクラスタ管理を使用する場合、クラスタの他のメンバーに対して操作を実行すると、Cross-Origin Resource Sharing (CORS) HTTP リクエストが発生します。このため、

Web ブラウザーで使用されている特定のホスト名を許可するように［信頼できるサーバー、CORS、リダイレクト］設定を変更する必要がある場合があります。

［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］に移動します。

クラスタ管理の表

- ヘルスインジケータ：クラスタ管理グリッドの最初の列には、ヘルスインジケータが表示されます。クラスタメンバーは、クラスタ内の他のアプライアンスに定期的に照会して、その健全性情報を取得します。クラスタメンバーの情報および健全性情報はメモリにキャッシュされ、最新の結果が表示されます。

  ノード上のヘルスインジケータは、クラスタメンバーが以下の状態のいずれかにあることを示します。

  エラー：クラスタの機能に影響を与える明確な問題があることを示しています。

  警告：クラスタに潜在的な問題があることを示しています。

  ロック：クラスタがロックされていることを示しています。

  ✔（緑）：健全な状態であることを示しています。

- **名前**：アプライアンスの名前
- **ネットワークアドレス**：アプライアンス構成インターフェイスの IPv4 アドレス（または IPv6 アドレス）。アプライアンス IP アドレスを変更することができます。詳細については、「アプライアンスの構成設定を変更できますか？」を参照してください。
- **プライマリ**：アプライアンスがプライマリである場合、**「はい」**と表示されます。
- **アプライアンスの状態**：アプライアンスの状態が表示されます。利用可能な状態のリストについては、「アプライアンスの状態」を参照してください。

アプライアンスを選択すると、そのアプライアンスの詳細が右側に表示されます。名前、ネットワークアドレス、プライマリ、状態に加えて以下の追加情報が表示されます：

- **ディスク領域：**使用済みディスク容量と空きディスク容量
- **バージョン**：アプライアンスのバージョン番号
- **前回正常性チェック**：選択したアプライアンスの情報が最後に取得された日時
- **稼働時間**：アプライアンスが稼働している時間（日、時間、分）
- レプリカが選択されている場合、以下の追加情報がプライマリ用に表示されます：
  - **ネットワークアドレス**：クラスタのプライマリアプライアンスのネットワーク DNS 名または IP アドレス

- **MAC アドレス**：メディアアクセス制御アドレス（MAC アドレス）、通信用のネットワークインターフェイスに割り当てられた一意の識別子
- **リンクプレゼント**：通信リンクが開いているかどうかを示す「はい」または「いいえ」のいずれかが表示されます。
- **リンクレイテンシ**：プライマリがレプリカと通信するのにかかる時間（ミリ秒単位）。ネットワークのレイテンシは、データのパケットがある指定されたポイントから別のポイントに到達するまでにかかる時間を表すものです。レイテンシは限りなくゼロに近い状態が理想です。

- エラーと警告が報告されます：
  - **エラー**：エラーはレポートされます。たとえば、アプライアンスがプライマリから切断された場合（クォーラムがない）場合、次のようなエラーメッセージが表示されることがあります。「リクエストワークフロー：クラスタ構成データベースの健全性を判断できませんでした。」
  - **警告**：警告がレポートされます。たとえば、アプライアンスがプライマリから切断された場合（クォーラムなし）場合、次のような警告メッセージが表示されることがあります。「ポリシーデータ：ポリシーデータのレプリケーションに問題があります。詳細：ポリシーデータベーススレーブ IO が実行されていません。Safeguard プライマリはこのアプライアンスからアクセスできない可能性があります。」

ツールバーアクション

- ＋ **[レプリカの追加]**：アプライアンスをレプリカとしてプライマリアプライアンスに参加させます。詳細については、「レプリカのクラスタへの登録」を参照してください。
- アプライアンスの詳細とクラスタの健全性ペインツールバーボタン：
  - **参加解除**：**[参加解除]**をクリックして、レプリカをクラスタから削除します。詳細については、「クラスタからのレプリカの参加解除」を参照してください。
  - **フェイルオーバー**: **[フェイルオーバー]**をクリックすると、レプリカをプライマリアプライアンスに昇格させることができます。詳細については、「レプリカを新しいプライマリに昇格させることによるフェイルオーバー」を参照してください。
  - ✳ **アクティブ化**：✳ **[アクティブ化]**をクリックして、読み取り専用のアプライアンスをアクティベートし、データの追加、変更、削除ができるようにし

ます。詳細については、「読み取り専用アプライアンスの有効化」を参照してください。

> **注意：** **読み取り専用モードのアプライアンスをアクティブ化すると、読み取り専用状態から解除され、管理アカウントのパスワードおよび SSH キーのチェックと変更が可能になります。他の SPP アプライアンスがこれらのアカウントをアクティブに監視していないことを確認してください。**

- **［診断］**：**［診断］**をクリックすると、診断ペインが開き、以下を実行できます。
  - アプライアンス診断の表示：詳細については、「アプライアンスの診断」を参照してください。
  - アプライアンスの情報の表示：詳細については、「アプライアンス情報」を参照してください。
  - アプライアンスに対して診断テストの実行：詳細については、「ネットワーク診断」を参照してください。
  - ネットワーク設定の表示と編集：詳細については、「ネットワーク」を参照してください。
  - 工場出荷時リセットの実行：詳細については、「工場出荷時リセット」を参照してください。
  - OS ライセンスの確認（仮想マシンのみ）：詳細については、「オペレーティングシステムのライセンス」を参照してください。
  - パッチの更新：詳細については、「パッチの更新」を参照してください。
  - アプライアンスのシャットダウンまたは再起動：詳細については、「電源」を参照してください。
  - サポートバンドルの生成：詳細については、「Support Bundle」を参照してください。
  - 時間設定の表示と編集：詳細については、「時間」を参照してください。
- **正常性の確認**：選択したアプライアンスの現在の状態をキャプチャして表示します。
- **再起動**：**［再起動］**をクリックすると、選択したアプライアンスが再起動されます。**「理由」**を入力し、**［再起動］**をクリックします。

- **クラスタのリセット**：コンセンサスが失われたクラスタを回復します。詳細については、「コンセンサスが失われたクラスタのリセット」を参照してください。

  > **注意**: クラスタのリセットは最後の手段にしてください。クラスタをリセットするのではなく、バックアップから復元することをお勧めします。

- **更新**： クラスタ内のアプライアンスのリストを更新します。
- **オフラインワークフローの有効化**：このボタンは、アプライアンスのコンセンサスが失われ、選択したアプライアンスにログインしており、アプライアンスをまだオフラインワークフローモードにしていない場合に使用できます。アプライアンスの状態は、［Isolated］または［Lost Quorum］になります。**［オフラインワークフローの有効化］**をクリックすると、選択したアプライアンスをオフラインワークフローモードに手動で配置します。アプライアンスはクラスタの残りの部分から分離して実行されます。詳細については、「オフラインワークフローモードの手動制御」を参照してください。
- **オンライン操作の再開**：このボタンは、アプライアンスのコンセンサスが失われ、選択したアプライアンスにログインしており、アプライアンスがオフラインワークフローモードである場合に利用可能です。アプライアンスの状態は、［Isolated］または［Lost Quorum］になります。**［オンライン操作の再開］**をクリックすると、手動でアプライアンスをクラスタに再統合し、監査ログをマージします。詳細については、「オンライン操作の手動再開」を参照してください。

ロックされたクラスタのロック解除

一貫性と安定性を維持するために、一度に実行できるクラスタ操作は 1 つだけです。これを確実にするために、SPP は、登録、参加解除、フェイルオーバー、パッチ、リセット、セッションモジュール参加、IP 更新、監査ログメンテナンスなどのクラスタ操作の実行中に、クラスタをロックします。クラスタがロックされている間は、操作が完了するまでクラスタ構成への変更は許可されません。

ロック通知は、次のように表示されます。

［アプライアンスの状態］に赤いロックアイコン（）が表示されます。

SPP の参加解除、フェイルオーバー、クラスタリセット、復元、パッチ、IP アドレスの更新のために、クラスタロックを絶対に解除しないでください。その他、以下について考慮してください：

- SPP への参加（登録）に時間がかかっている場合、監査データのストリーミングステップ中にそれをキャンセルすることができます。

- パッチの配布に時間がかかっている場合は、配布をキャンセルしてレプリカに直接パッチをアップロードすることができます。
- 監査ログの同期処理に時間がかかっている場合、またはクラスタ内のアプライアンスのダウンにより同期処理が完了しないと思われる場合は、その処理をキャンセルできます。この操作をキャンセルするには、「監査ログメンテナンス」ページの「監査ログメンテナンスのキャンセル」で詳しく説明されているように、監視が必要です。
- 監査ログアーカイブまたは消去操作に長い時間がかかっている場合、またはクラスタ内のアプライアンスのダウンにより完了しないと思われる理由がある場合、この操作をキャンセルすることができます。この操作をキャンセルするには、「監査ログメンテナンス」ページの「監査ログメンテナンスのキャンセル」の詳細に従って監視する必要があります。

ロックされたクラスタのロック解除手順

1. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**に移動します。
2. 警告バナーの右上隅にある 🔒 ロックアイコンをクリックします。
3. クラスタのロック解除確認ダイアログで**［クラスタのロック解除］**を入力し、**［OK］**をクリックします。これにより、クラスタ内のすべてのアプライアンスにかけられたクラスタロックが解除され、操作が終了します。

> 重要: ロックされたクラスタのロックを解除する際には、注意が必要です。クラスタ内の 1 つ以上のアプライアンスがオフラインで、現在のオペレーションを終了しないことが確実な場合にのみ使用する必要があります。クラスタのロックを強制的に解除すると、アプライアンスが不安定になり、工場出荷時のリセットが必要になり、クラスタの再構築が必要になる場合があります。進行中の操作に確信が持てない場合は、クラスタのロックを解除しないでください。

9.4.2 管理対象ネットワーク

管理ネットワークは、クラスタ環境において特定の SPP または SPS アプライアンスがサービスするネットワークセグメントの名前付きリストです。管理ネットワークは、パスワードや SSH キーの変更、アカウント検出、セッション記録、資産検出などのタスクをスケジューリングして、タスクの負荷を分散するために使用されます。管理対象ネットワークを使用すると、次のことが可能になります。

- 負荷を分散し、クラスタトラフィックを最小限にする。

- 実際のタスクを実行するために、ターゲット資産に最も近いアプライアンスを使用するように指定する。

SPP クラスタには、すべてのクラスタメンバーで構成されるデフォルトの管理対象ネットワークがあります。他の管理対象ネットワークを定義することもできます。

> ⚠ **注意：リンクされた SPS クラスタに属する管理対象ホストの役割が変更された場合、または管理対象ホストがクラスタに追加または削除された場合、SPP は各中央管理ノードに照会して変更を検出し、SPS クラスタトポロジとの同期を維持しようと試みます。中央管理ノードがダウンしている場合、SPP は管理者に次のようなメッセージで無効なポリシーがある可能性を警告します：「セッション接続ポリシーが見つかりませんでした。」また、壊れたアクセスリクエストポリシーに「Invalid」（[セキュリティポリシー管] > [資格] > [アクセスリクエストポリシー]）タブでフラグを付けます。ネットワークの規模やその他の要因に基づき、この作業には 1～10 分かかり、この間、利用できない管理対象ホストが［管理対象ネットワーク］ページに表示され続けることがあります。この間、利用できない管理対象ホストは、［管理対象ネットワーク］ページに表示され続けます。作成されたリクエストは無効となり、セッションを開始することができなくなります。**

タスクの委任

SPP のクラスタは、プラットフォームのタスク負荷に基づいて、プラットフォーム管理タスク（パスワードおよび SSH キーの確認やパスワードおよび SSH キーの変更など）をアプライアンスに委任します。プライマリアプライアンスは委任を行い、使用中のプラットフォームタスクスレッド数を許可されたプラットフォームタスクスレッドの最大数で割って算出される内部フィットネススコアを使用してクラスタメンバーの適合性を評価します。

許可されるプラットフォームタスクスレッドの最大数は、アプライアンス/設定 API を使用して、MaxPlatformTaskThreads の値を調整することができます。この値を調整することで、タスクの分散を調整することができます。

> **重要**：MaxPlatformTaskThreads を調整すると、アクセスリクエストの処理に使用できる SPP のリソースに影響を与え、ユーザーエクスペリエンスに影響を与える可能性があります。この値を変更する必要がある場合は、プロフェッショナルサービスを利用するのがベストプラクティスです。

許可されたプラットフォームタスクスレッドの最大数を増やすと、フィットネススコアが低下し、そのアプライアンスに渡されるタスクの数が増えます。

フィットネススコアはキャッシュされ、スケジューラがビジーでないときに 8 分間隔で再計算されます。スケジューラがタスクを実行しているときは、より頻繁にフィットネススコアが計算され、スケジューラが動的に調整できるようになります。

SPS アプライアンスの選択は、主に管理対象ネットワークルールに依存します。ただし、管理対象ネットワークルールがない場合、または管理対象ネットワークルールの結果、複数の SPS アプライアンスが選択された場合は、フィットネススコアがタイブレーカーとして使用されます。フィットネススコアは、使用可能なディスクの割合から SPS アプライアンスの全体的なロードアベレージを引いた値に基づいて計算されます。(ロードアベレージは、サーバーで使用されている全体的なリソース容量を数値で示す Linux の指標です。) フィットネススコアが高いほど、対応するアプライアンスが選択される可能性が高くなります。

優先順位

[セキュリティポリシー管理] > [資格] > [アクセスリクエストポリシー] タブでの選択が **[アプライアンス管理] > [クラスタ] > [管理対象ネットワーク]** ページでの選択に優先されます。**[管理対象ネットワーク]** ルールに異なる SPS クラスタのノードが含まれている場合、SPP は **[アクセスリクエストポリシー]** タブの **[セッション設定]** ページで割り当てられた同じクラスタのノードのみを選択します。

> **重要**：管理対象ネットワークがサブネットで構成されているが、アプライアンスに割り当てられていない（アプライアンスが空白）場合、検出、パスワード、SSH キーの確認と変更は機能しません。管理対象ネットワークに割り当てられたアプライアンスが存在しない場合、次のようなメッセージが表示されます。「ネットワーク '<NameOfEmptyNetwork>' にプラットフォームタスクリクエストを実行するために利用できるアプライアンスがありません。この問題を解決するには、パスワード、SSH キー、および/またはセッションを管理するアプライアンスを少なくとも 1 つ割り当てるか、管理対象ネットワークエントリを削除します。」

管理対象ネットワークに移動します。

[アプライアンス管理] > [クラスタ] > [管理対象ネットワーク] に移動します。

[管理対象ネットワーク] ページには、以前に定義された管理対象ネットワークに関する以下の情報が表示されます。初期状態では、このページにはデフォルト管理対象ネットワークのプロパティが含まれており、このネットワークにはすべてのネットワークが暗黙的に含まれ、クラスタのすべてのアプライアンスによって提供されています。

表：管理対象ネットワーク：プロパティ

プロパティ	説明
名前	SPP に追加されたときに管理対象ネットワークに割り当てられた名前
サブネット	管理対象ネットワークに含まれるサブネットのリスト。**[管理対象ネットワーク]** グリッドのエントリをダブルクリッ

プロパティ	説明
	クすると、選択した管理対象ネットワークに関連するサブネットの詳細が表示されます。 SPS に参加している場合は、以下が適用されます。 • **パスワード管理**： SPP アプライアンス ID（ノードの MAC アドレスの後に IP アドレスが続く） • **セッション管理**: 該当する場合、SPS アプライアンスのホスト名に続いて SPS ノードの IP アドレス
パスワード管理者	指定されたサブネットを管理するために割り当てられたアプライアンスのホスト名と IP アドレス、MAC アドレス
セッション管理者	クラスタノードのホスト名と IP アドレス
説明	管理対象ネットワークを定義する際に入力した説明テキスト

以下のツールバーボタンを使用して、管理対象ネットワークの定義とメンテナンスします。

表：管理対象ネットワーク：ツールバー

オプション	説明
追加	管理対象ネットワークを追加します。詳細については「管理対象ネットワークの追加」を参照してください。
削除	選択した管理対象ネットワークを SPP から削除します。デフォルト管理対象ネットワークは削除できません。
更新	管理対象ネットワークリストを更新します。
編集	選択された管理対象ネットワーク構成を更新します。デフォルトの管理対象ネットワークは編集できません。
ネットワークの解決	管理対象ネットワークリストで IP アドレスを見つけます。詳細については「IP アドレスの解決」を参照してください。

管理対象ネットワークの追加

クラスタ環境でのタスク負荷を分散させるために使用できる管理対象ネットワークを追加するには、**［管理対象ネットワーク］**ページを使用します。管理対象ネットワークの定義と維持は、アプライアンス管理者の責任です。

管理対象ネットワークの追加手順

1. **［アプライアンス管理］＞［クラスタ］＞［管理対象ネットワーク］**に選択します。
2. ＋**［追加］**をクリックします。
3. **［管理対象ネットワーク］**ダイアログで、以下の情報を入力します。
    a. **名前**：管理対象ネットワークの表示名を入力します。これは、リンクされた SPS セッション接続の認証に使用される SPS アプライアンスの名前である可能性があります。制限：50 文字。
    b. **説明**：（オプション）管理対象ネットワークに関する情報を入力します。制限：255 文字
    c. **サブネット**：＋**［追加］**をクリックして、管理するサブネット（ホストのグループ）を指定します。

    各サブネットは CIDR 記法（例：0.0.0.0/0）を用いて入力します。

    > **メモ：**サブネットは、1 つの管理対象ネットワークにのみ追加できます。同じサブネットを別の管理対象ネットワークに追加しようとすると、エラーが表示されます。IP アドレスがすでに管理ネットワークに関連付けられているかどうかわからない場合は、**［ネットワークの解決］**検索ボックスを使用します。詳細については、「IP アドレスの解決」を参照してください。

    d. **パスワード管理者**： 指定したサブネットを管理するために使用するアプライアンスを選択します。

    > **メモ：**最初に管理対象ネットワークを定義する際に、アプライアンスを指定する必要はありません。✎**［編集］**ボタンを使用して、後で管理アプライアンスを指定することができます。

    e. **セッション管理者**：該当する場合、管理対象ネットワークに関連付ける SPS アプライアンスを選択します。

4. **［OK］**をクリックして選択内容を保存し、管理対象ネットワークを追加します。

管理対象ネットワークの削除

管理対象ネットワークの削除手順

1. **［アプライアンス管理］＞［クラスタ］＞［管理対象ネットワーク］**に移動します。
2. 削除する管理対象ネットワークを選択し、**［削除］**をクリックします。
3. 確認ダイアログで、**［はい］**をクリックします。

IP アドレスの解決

アプライアンス管理者は、**［管理対象ネットワーク］**ページを使用して、管理対象ネットワークのサブネットのリスト内で IP アドレスを検索することができます。

管理対象ネットワーク内で IP アドレスを検索する手順

1. **［アプライアンス管理］＞［クラスタ］＞［管理対象ネットワーク］**に移動します。
2. **［ネットワークの解決］**検索ボックスで、IP アドレスを入力し、**［Enter］**を押します。

   IP アドレスに最も近いサブネットを含む管理ネットワークがハイライト表示されます。IP アドレスに一致するサブネットがない場合は、デフォルトの管理ネットワークがハイライト表示されます。

9.4.3 オフラインワークフロー（自動）

潜在的なダウンタイムを減らすために、アプライアンス管理者はオフラインワークフローモードを自動的に実行するように設定することができます。オフラインワークフローモードでは、コンセンサス（クォーラム）を失ったアプライアンスがクラスタから分離して動作し、キャッシュされたポリシーデータを使用してアクセスリクエストを処理することができます。

停止が短時間の停止でないことを保証するために、アプライアンスがオフラインワークフローモードに自動的に切り替わるまでのデフォルトの時間は 15 分です。この時間のしきい値は、5 分以上に変更することができます。

自動オフラインワークフローモードが有効な場合、オンラインワークフローの自動再開を有効にして、コンセンサスが復元されるとアプライアンスが自動的にオンライン操作を再開できるようにすることができます。コンセンサスが回復してから自動的にオンラインワークフローを再開するまでの待ち時間は、デフォルトで 15 分です。時間のしきい値は、5 分以上に変更することができます。

オフラインワークフローモードが自動的に実行されるように構成されている場合、アプライアンス管理者は、必要に応じて自動設定を無効にして、アプライアンスを手動でオフラインワークフローモードにしたり、アプライアンスを手動でオンラインワークフローに回復させたりすることができます。

ユーザーは、アプライアンスの状態を明確に伝えるステータスメッセージと、パスワードおよび SSH キーをリクエストする機能を表示します。

オフラインワークフローモードの一般的な情報については、「オフラインワークフローモードとは」を参照してください。

［アプライアンス管理］＞［クラスタ］＞［オフラインワークフロー］に移動します。**［オフラインワークフロー］**ページには、次の情報が表示されます。

表：オフラインワークフロー プロパティ

プロパティ	説明
自動オフラインフローの有効化	アプライアンスが接続を失い、コンセンサスを確立できない場合に、アプライアンスを自動的にオフラインワークフローモードに配置します。
自動オフラインワークフローのしきい値	コンセンサスが失われた後、アプライアンスが自動的にオフラインワークフローモードに切り替わるまでの分数を指定します。デフォルトは 15 分で、5 分以上で変更することができます。設定されたしきい値は、再起動後は保持されません。
オフラインワークフローの自動再開	**［自動オフラインフローの有効化］**が選択されている場合、**［オンラインワークフローの自動再開］**を選択することで、コンセンサスが復元されたらアプライアンスが自動的にオンライン操作を再開するようにすることができます。
オフラインワークフローの自動再開のしきい値	コンセンサスが復元された後、アプライアンスが自動的にオンラインワークフローに切り替わるまでの分数を指定します。デフォルトは 15 分で、5 分以上に変更することも可能です。

以下のツールバーボタンを使用して、管理されたネットワークを定義し、維持します。

表：オフラインワークフロー：ツールバー

オプション	説明
更新	ページに表示される情報が更新されます。
オフラインワークフローの有効化	オフラインワークフローモードをトリガーします。
オンライン操作の再開	オフラインワークフローモードからオンライン操作へアプライアンスを移行します。

自動オフラインワークフローの有効化

［オフラインワークフロー］ページでは、オフラインワークフローモードを制御するための自動設定を行うことができます。自動設定を手動で上書きすることができます。詳細については、「自動オフラインワークフローを手動でオーバーライドする」を参照してください。

オフラインワークフローモードを制御するための自動設定の構成手順

1. **［アプライアンス管理］**>**［クラスタ］**>**［オフラインワークフロー］**に移動します。
2. **［オフラインワークフロー］**ダイアログで**［自動オフラインフローの有効化］**を選択し、アプライアンスが接続を失い、入力した指定分数（次のステップを参照）クラスタとのコンセンサスを確立できない場合、アプライアンスが自動的にオフラインワークフローモードになるように設定します。
3. コンセンサスが失われた後、アプライアンスが自動的にオフラインワークフローモードに切り替わるまでの「分」数を指定します。自動オフラインワークフローしきい値のデフォルトは 15 分で、5 分以上に変更することができます。
4. 最初のチェックボックスを選択して自動オフラインワークフローモードを有効にした場合、**［オンラインワークフローの自動再開］**を選択して、コンセンサスが回復するとアプライアンスが自動的にオンライン操作を再開できるようにすることができます。
5. コンセンサスが復元された後、アプライアンスが自動的にオンラインワークフローに切り替わるまでの「分」数を指定します。**［オンラインワークフローの自動再開しきい値］**のデフォルトは 15 分で、5 分以上に変更することも可能です。
6. **［保存］**をクリックします。

自動オフラインワークフローを手動でオーバーライドする

［オフラインワークフロー］ページを使用で、オフラインワークフローを手動で有効にしたり、オンライン操作を再開したりします。これらの操作の詳細については、「オフラインワークフローモードの手動制御」を参照してください。

オンライン操作を再開する前に、オンライン操作を再開するための考慮事項を参照してください。

オフラインワークフローの手動有効化手順

このオプションは、アプライアンスがクラスタとのコンセンサスを失った場合にのみ利用可能です。

1. **［アプライアンス管理］**>**［クラスタ］**>**［オフラインワークフロー］**に移動します。
2. **［オフラインワークフローの有効化］**をクリックして、オフラインワークフローモードを手動でトリガーします。
3. ダイアログボックスで、**［オフラインワークフローの有効化］**と入力し、**［Enter］**を押します。アプライアンスはオフラインワークフローモードになり、メンテナンスに入ります。
4. **［クラスタ管理］**ウィンドウでリクエストを確認し、ヘルスチェックを表示することができます。詳細については、「クラスタ管理」を参照してください。

オンライン操作の手動再開手順

このオプションは、アプライアンスがオフラインワークフローモードである場合にのみ利用できます。

1. **［アプライアンス管理］**>**［クラスタ］**>**［オフラインワークフロー］**に移動します。
2. オフラインワークフローモードからオンライン操作に戻すためにアプライアンスを手動でトリガーするには、**［オンライン操作の再開］**をクリックします。
3. ダイアログボックスで、**［オンライン操作の再開］**と入力し、**［Enter］**を押します。
4. メンテナンスが完了したら、再起動をクリックします。アプライアンスがメンテナンスモードに戻されます。
5. クラスタ管理ウィンドウで要求を確認し、健全性チェックを表示することができます。詳細については、「クラスタ管理」を参照してください。

9.4.4 SPS リンクのあるセッションアプライアンス

資産管理者は、セッションの記録と監査のために、SPS クラスタを 1 台以上のアプライアンスからなる SPP クラスタにリンクさせることができます。実際のリンクは、SPP プライマリと SPS クラスタマスタの間で行う必要があります。つまり、SPS クラスタは SPP クラスタの各ノードを認識します。またその逆も同じです。

リンクされると、すべてのセッションはアクセスリクエストによって SPP アプライアンスによって開始され、SPS アプライアンスによって管理され、セッションはセッションアプライアンスを介して記録されます。

> ⚠ **注意：SPS を SPP にリンクする場合、SPS と SPP のバージョンが完全に一致していること、アップグレードの際はバージョンを同期させることが必要です。たとえば、SPS バージョン 6.6 は SPP バージョン 6.6 のみとリンクすることができ、SPS をバージョン 6.7 にアップグレードする場合は、SPP も 6.7 にアップグレードする必要があります。**
>
> **Long Term Supported（LTS）と機能リリースを混在させないように注意してください。たとえば、SPS バージョン 6.0.1 を SPP バージョン 6.1 にリンクしないでください。**

> **メモ：**単一ノードの SPS クラスタで、中央管理ノードが検索マスタでもある場合、SPP はセッションを開始できません。クラスタ内に、セッションを記録できる SPS アプライアンスが少なくとも 1 つ存在する必要があります。Safeguard for Privileged Sessions 管理者ガイドの「クラスタ管理」を参照してください。

SPP のリンクガイダンス

リンクを開始する前に、リンクについてのガイダンスと注意事項を確認てください。詳細については、「SPP と SPS セッションアプライアンスのリンクガイダンス」を参照してください。

SPS ノードに割り当てられた役割に注意を払います。SPP からのセッション再生が失われないようにするために、次のような注意があります。

> ⚠ **注意：SPS ノードの役割を、Search Local の役割から Search Minion の役割に切り替えないでください。切り替えた場合、Search Local の役割で記録したセッションの再生は SPP アプライアンスから再生されず、SPS Web ユーザーインターフェイス経由でのみ再生される可能性があります。Search Minion の役割のノードで行われた記録は、Search Master ノードにプッシュされ、SPP にダウンロードできるようになります。SPS のノードとロールの詳細については、『Safeguard for Privileged Sessions 管理者ガイド』を参照してください。**

初回リンク後の標準的な操作手順

初回リンク後に別の SPS クラスタを追加する場合は、以下の標準的な操作手順に従います。

1. リンク接続を追加します。このトピックで後述するリンク接続の表示、削除、または編集を参照してください。
2. 資格アクセスリクエストポリシー（クラスタマスタの IP アドレスである SPS 接続ポリシー）上のセッション設定を確認します。詳細については、「アクセスリクエストポリシーの作成」を参照してください。
3. 管理対象ネットワークを割り当てます。詳細については、「管理対象ネットワーク」を参照してください。
4. **［セッションアクセス有効化］**トグルをオンにします。

SPS 中央管理ノードがダウンしている場合

SPP は、SPS 中央管理ノードが停止している場合でも、管理対象ホスト上でセッションを起動し続けます。ただし、中央管理ノードが停止している間は、SPP は既存のポリシーを検証できず、SPS クラスタトポロジを検証することもできません。「Safeguard for Privileged Sessions 管理者ガイド」の「Managing a High Availability One Identity Safeguard for Privileged Sessions (SPS) cluster」を参照してください。

接続の削除: ソフト削除とハード削除

目的に応じて、ソフト削除またはハード削除を実行できます。

接続のソフト削除

セッション接続が削除されると、接続情報はソフト削除され、同じ SPS アプライアンスの再リンクで同じ値を再利用できるようになります。ソフト削除して再リンク時に同じ接続値を再利用するこの方法では、以前のセッション接続を参照していたすべてのアクセスリクエストポリシーが破損されるのを避けることができます。

接続のハード削除

セッション接続を永久に削除するために、ハード削除を実行することができます。これは通常、再リンクを希望しないか、以前のセッション接続値を保持することで SPS アプライアンスのリンクまたは再リンクを妨げている場合にのみ実行されます。

ハード削除は、PowerShell または Swagger を使用して、以下の手順で API から実行することができます。

PowerShell を使用したハード削除

Safeguard PowerShell の最新版には、ハード削除を実行するための 2 つのコマンドレットが含まれています。

split-safeguardSessionCluster -SessionMaster <name or ID of session master>

Remove-SafeguardSessionSplitCluster -SessionMaster <name or ID of session master>を実行します。

Swagger を使用したハード削除

1. ブラウザーで、https://<your-ip-address>/service/core/swagger に移動します。
2. **［Authorize］**ボタンを使ってサービスに認証します。
3. Cluster->GET /v3/cluster/SessionModules に移動し、**［Try it out!］**をクリックします。
4. 不要なセッション接続がリスト上に存在するかどうかを確認します。
    a. 不要なセッション接続がリストに存在する場合：
        i. セッション接続の ID をメモします。
        ii. Cluster DELETE /v3/cluster/SessionModules に移動します。
        iii. ID を入力します。
        iv. **［Try it out!］**をクリックします。
        v. 手順 3 へ進みます。
    b. 不要なセッション接続がリストに存在しない場合：
        i. includeDisconnected パラメーターを true に設定します。
        ii. **［Try it out!］**をクリックします。
        iii. 不要なセッション接続がリストに存在する場合は、手順 4a に進み、エントリを 2 回目も削除します（ハード削除になります）。
5. これでプロセスは完了し、セッション接続は永久に削除されます。

リンク接続の表示、削除、編集

参加が完了したら、**［アプライアンス管理］＞［クラスタ］＞［セッションアプライアンス］**に移動して、リンク接続を表示、削除、または編集します。**［セッションアプライアンス］**ペインには、次のようなセッションの詳細が表示されます。

表：セッションアプライアンス：プロパティ

プロパティ	説明
ホスト名	SPS アプライアンスホストクラスターマスターのホスト名
管理対象ホスト	管理対象ホスト名と IP アドレスで識別される SPS クラスタ内の他のノード。⚠ **［警告］**アイコンにカーソルを合わせると、管理対象ホストが**［利用不可］**または**［不明］**であるかどうかが表示されます。
ネットワークアドレス	セッション接続のネットワーク DNS 名または IP アドレス
接続ユーザー	SPP のユーザー名。ユーザー名にはスペースを含めないでください。
サムプリント	証明書を識別するための一意のハッシュ値
説明	（オプション）SPS セッション接続に関する説明テキスト（例：20 on cluster - 172 primary node）

［ホスト名］の行をクリックすると、**［セッションモジュール接続］**ダイアログが表示されます。

表：セッションモジュール接続：プロパティ

プロパティ	説明
ノード ID	リンクされた SPS セッション接続の認証に使用される SPP アプライアンスの名前
ホスト名	SPS アプライアンスのホストクラスタマスターのホスト名
接続ユーザー名	SPP のユーザー名。ユーザー名にはスペースを含めないでください。
説明	（任意）SPS セッション接続に関する説明テキスト（例：20 on cluster - 172 primary node）
ネットワークアドレス	セッション接続のネットワーク DNS 名または IP アドレス

プロパティ	説明
ホスト名の使用（IP アドレスではない）	チェックした場合、セッションの起動に使用される接続文字列は、IP アドレスではなく、SPS アプライアンスのホスト名を使用します。

以下のツールバーボタンを使用して、セッションを管理します。

表：セッション管理：ツールバー

オプション	説明
削除	選択したリンクされた SPS セッション接続を削除します。ソフト削除とハード削除の詳細については、前述の「接続の削除：ソフト削除とハード削除」を参照してください。
編集	セッションモジュール接続ダイアログで、選択したリンクされた SPS セッション接続の**［説明］**または**［ネットワークアドレス］**を変更します。
更新	リンクされた SPS セッション接続のリストを更新します。

9.5　サービスの有効化または無効化

SPP では、アクセスリクエストおよびパスワードと SSH キーの管理サービスを有効または無効にすることができます。これらの設定は、パスワードまたは SSH キーのリリースリクエスト、アカウントのパスワードまたは SSH キーの手動検証、およびリセットタスク、ならびにパーティションにおける自動プロファイル確認と変更タスクを制御します。また、検出タスク、ディレクトリ同期、監査ログストリームサービスを有効または無効にすることもできます。

デフォルトでは、監査ログストリームサービス以外のサービスは有効になっています。

デフォルトでは、サービスアカウント、および検出ジョブの一部で検出されたアカウントと資産に対して、サービスが無効になっています。サービスアカウントはこれらのスケジュールを遵守するように変更することができ、検出されたアカウントは管理時にアクティブにすることができます。

これらの設定を管理するのは、アプライアンス管理者の責任です。

［アプライアンス管理］＞［サービスの有効化または無効化］に移動すると、以下の設定が表示されます。

- アプライアンス管理者は**［すべての有効なサービスを無効化］**をクリックして、すべてのサービスを無効にすることができます（少なくとも 1 つのサービスが現在有効になっている場合に限ります）。サービスを無効にする前に、確認ダイアログが表示されます。
- 設定を変更するにはトグルをクリックします：トグルオントグルオフ
- ページ上の情報を更新するには、  **［更新］**をクリックします。

表：サービスの有効化または無効化：プロパティ

設定	説明
すべての有効なサービスを無効化	アプライアンス管理者は、（少なくとも 1 つのサービスが有効である場合）すべてのサービスを無効にすることができます。サービスを無効にする前に、確認ダイアログが表示されます。各サービスを個別に再有効化する必要があります。
リクエスト	
セッションリクエスト	セッションリクエストはデフォルトで有効になっており、許可されたユーザーがセッションへのアクセスリクエストを作成できることを示します。1 回のアクセスリクエストには、1,000 セッションの制限があります。**［セッションリクエスト］**をクリックすると、このサービスが無効になり、セッションのリクエストができなくなります。 **メモ：**セッションリクエストを無効にすると、新しいセッションアクセスリクエストを開始することができなくなります。対象の資産/アカウントを制御するアクセスリクエストポリシーによっては、セッションリクエスト機能が使用できないことを通知するメッセージが表示されます。 また、現在のセッションアクセスリクエストを開始することはできません。セッションリクエストが使用できないことを通知するメッセージが表示されます。例えば、次のようなメッセージが表示されることがあります。「この機能は一時的に無効になっています。詳細については、アプライアンス管理者に問い合わせてください。」

設定	説明
パスワードのリクエスト	パスワードリクエストはデフォルトで有効になっており、許可されたユーザーがパスワードリリースリクエストを行うことができることを示しています。 **［パスワードのリクエスト］**のトグルをクリックして、このサービスを無効にすると、パスワードがリクエストできなくなります。 **メモ：**パスワードのリクエストサービスを無効にすると、このサービスが再び有効になるまで、開いているリクエストはすべて保留になります。
SSH キーリクエスト	SSH キーのリクエストはデフォルトで有効になっており、認証されたユーザーが SSH キーのリリースリクエストを行うことができることを示しています。 **［SSH キーリクエスト］**をクリックすると、このサービスが無効になり、SSH キーのリクエストができなくなります。 メモ：パスワードリクエストサービスを無効にすると、このサービスが再び有効になるまで、開いているリクエストは保留されます。
パスワード管理	
パスワードのチェック管理	パスワード確認の管理はデフォルトで有効になっており、プロファイルがスケジュールされている場合、SPP が自動的にパスワード確認タスクを実行し、アカウントのパスワードを手動で確認することができることを示します。 **［パスワードのチェック確認］**トグルをクリックすると、パスワード管理サービスが無効になります。 **メモ:** SPP は、デフォルトで自動パスワード管理サービスを有効にします。通常は、組織全体のメンテナンス期間のみ無効にします。 パスワード管理サービスを無効にすると、SPP は現在実行中のすべてのタスクの完了を許可しますが、新しいタスクの開始は許可しません。

設定	説明
パスワードの変更管理	パスワードの変更管理はデフォルトで有効になっており、SPP がプロファイルをスケジュールした場合にパスワード変更タスクを自動的に実行し、アカウントのパスワードを手動でリセットできることを示します。 **［パスワードの変更管理］**トグルをクリックすると、パスワードリセットサービスが無効になります。 **メモ:** SPP は、デフォルトで自動パスワード管理サービスを有効にします。通常は、組織全体のメンテナンス期間中のみ無効にします。 パスワード管理サービスを無効にすると、SPP は現在実行中のすべてのタスクの完了を許可しますが、新しいタスクの開始は許可しません。
SSH キーの管理	
SSH キーのチェック	SSH キーの確認はデフォルトで有効になっており、パーティションに割り当てられた資産と資産のアカウントを管理するプロファイルごとに SSH キーの確認が管理されていることを示します。 **［SSH キーのチェック］**トグルをクリックすると、サービスが無効になります。
SSH キーの変更	SSH キーの変更はデフォルトで有効になっており、パーティションに割り当てられた資産と資産のアカウントを管理するプロファイルごとに SSH キーの変更が管理されることを示します。 **［SSH キーの変更］**トグルをクリックすると、変更サービスを無効になります。
検出	
資産検出	資産検出はデフォルトで有効になっており、利用可能な資産検出ジョブが Active Directory などのディレクトリ資産を検索するか、ネットワーク IP 範囲をスキャンすることによって資産を見つけることを示しています。詳細については、「検出」を参照してください。

設定	説明
アカウント検出	アカウント検出はデフォルトで有効になっており、利用可能なアカウント検出ジョブは、Active Directory などのディレクトリ資産を検索するか、アカウント検出ジョブに関連付けられた Windows および Unix 資産のローカルアカウントデータベース (/etc/passwd) をスキャンしてアカウントを検出することが示されています。詳細については、「検出」を参照してください。
サービス検出	サービス検出はデフォルトで有効になっており、利用可能なサービス検出ジョブが Safeguard が管理するアカウントとして実行される Windows サービスを検出することを示します。詳細については、「検出」を参照してください。
SSH キーの検出	SSH キーの検出はデフォルトで有効になっています。このトグルをオンにすると、管理対象アカウントの SSH キーが検出されます。詳細については、「SSH キーの検出」を参照してください。
ディレクトリ	
ディレクトリの同期	ディレクトリの同期はデフォルトで有効になっており、ディレクトリ資産への追加や削除が同期されることを示しています。同期を行う「分」数を設定することができます。詳しくは、「管理タブ（資産の追加）」を参照してください。

設定	説明
監査	
監査ログストリームサービス	SPP のデータを SPS に送信し、Safeguard 特権管理ソフトウェアスイートを監査するには、このトグルを使用します。この機能はデフォルトで無効になっています。 SPP データを受け入れるには、SPS アプライアンス管理者が監査ログの同期をオンにする必要があります。詳細については、『Safeguard for Privileged Sessions 管理ガイド』を参照してください。 この機能を使用するには SPP と SPS がリンクされている必要があります。詳しくは、「SPP と SPS セッションアプライアンスリンクガイダンス」を参照してください。 SPP と SPS の同期は継続されますが、多少の遅延があるため、SPS が任意の時点ですべての監査データを持つことは保証されません。 **メモ**：この設定は、**［セキュリティポリシー管理］＞［設定］**でも利用可能です。詳細については、「セキュリティポリシー設定」を参照してください。

9.6 外部統合

アプライアンス管理者は、以下を行うことができます：

- アプライアンスがさまざまな外部システムにイベント通知を送信するように構成する。
- 外部チケットシステムとの統合、または一般的なチケット番号の追跡。
- 外部認証サービスプロバイダとセカンダリ認証サービスプロバイダの両方を構成する。

外部統合へのアクセス：

［アプライアンス管理］＞［外部統合］へ移動します。

表：外部統合設定

設定	説明
メール	特定のイベントが発生したときに SPP が自動的にメール通知を送信するように設定する場所です。
メールテンプレート	SPP のメールテンプレートを設定します。
ハードウェアセキュリティモジュール	SPP が外部のハードウェアセキュリティモジュールデバイスを利用して暗号化するためのハードウェアセキュリティモジュール統合を設定する場所です。
SNMP	特定のイベントが発生したときに SNMP コンソールに SNMP トラップを送信するように設定します。
Starling	Starling サービスを利用するために、SPP を Starling に参加させる場所です。
Syslog	SPP がイベントに関する詳細を含むイベント通知を Syslog サーバーに送信するよう設定する場所です。
Syslog イベント	既存の Syslog サーバーを使用して、サブスクライバーを作成し、イベントを割り当てます。
チケットシステム	SPP を外部のチケットシステムと統合する、または外部のチケットシステムと統合せずに一般的なチケットを追跡するように設定する場合です。
信頼できるサーバー、CORS、リダイレクト	ログインリダイレクトと CORS（Cross Origin Resource Sharing）リクエストを、指定した IP アドレス、ホスト名（DNS ワイルドカードを含む）、および CIDR 表記ネットワークのリストに制限することができる場所です。

9.6.1 メール

特定のイベントが発生したときにメール通知を自動的に送信するように SPP を設定するのは、アプライアンス管理者の責任です。

［メール］ペインを使用して、メール通知に使用される SMTP サーバーを構成し、メール通知の内容を定義するメールテンプレートを編集します。

開始前に

SMTP サーバーを構成する前に、必要に応じて以下を実行してください。

- DNS サーバーを構成し、ユーザーのメールアドレスを正しく設定します。
- メール認証にトランスポート層を使用する場合は、**［証明書の追加］＞［証明書署名リクエスト（CSR）の作成］**オプションを使用して、SPP で証明書署名リクエスト（CSR）を作成することをお勧めします。詳細については、「監査ログ証明書署名リクエストの作成」を参照してください。

  CSR は、以下の形式でインストールできます。

  - 以下を含む CSR から生成された証明書をインストールします：
    - DER エンコードファイル（.cer、.crt、.der）
    - PEM エンコードされたファイル（.pem）
  - 秘密鍵を含む証明書のインストール
    - PKCS#12 （.p12 または.pfx）
    - 個人情報交換ファイル（.pfx）

SMTP サーバーの設定手順

1. **［アプリケーション管理］＞［外部統合］＞［メール］**に移動します。
2. メール通知を構成するには、すべてのメールについて、以下のグローバル設定を入力します：
   - **SMTP サーバーのアドレス**：メールサーバーの IP アドレスまたは DNS 名を入力します。未指定の場合、メールクライアントは無効となります。
     IPv6 アドレスを入力する場合は、[b86f:b86f:b86f:1:b86f:b86f:b86f]のように角括弧付きで記入してください。
     Mail eXchanger record（MX レコード）を使用する場合は、メールサーバーのドメイン名を指定する必要があります。
   - **SMTP ポート**： SMTP のデフォルトポートが設定されていますが、必要に応じて変更する必要があります。デフォルトの SMTP ポートは 25 ですが、SSL/TLS を使用している場合のデフォルトはポート 465 です。範囲は 1～65535 です。
   - **TLS（トランスポート層セキュリティ）**：以下のいずれかを選択します：
     - **STARTTLS が必要**： STARTTLS コマンドをサポートする SMTP サーバーに接続し、接続をテキストベースから TLS に昇格させることができます。

- **SMTPS が必要**：ターゲット SMTP サーバーへの接続で直ちに TLS が使用されます。
- **なし**：メールに適用されるトランスポートレイヤーセキュリティはありません。

「STARTTLS が必要」または**「SMTPS が必要」**を選択した場合、次のいずれか、または両方を選択できます：

- **SMTP サーバー証明書の検証**：選択しない場合、リモート SMTP サーバーの SSL 証明書は検証されません。
- **クライアント証明書の使用**：リモート SMTP サーバーへの TLS 接続時にクライアント証明書を提示する場合は、このチェックボックスを選択します。

- **ユーザー認証**：SMTP サーバーへのアクセスを認証したい場合に選択します。
  - **アカウント**：**［ディレクトリアカウント］**または**［資産アカウント］**をクリックして、認証に使用するアカウントを選択します。
  - **パスワード**：認証に使用する**［アカウント名］**と**［アカウントパスワード］**を入力します。
  - **なし**：ユーザーは認証されません。
- **テストメールの宛先**：アプライアンスから送信されるすべてのメールの送信元アドレスとして使用するメールアドレスを入力します。これは、**SMTP サーバーアドレス**を指定した場合に必要です。上限は 512 文字です。

設定の検証手順

メール設定をテストします。テスト時には、テスト以外のメールは扱われません。

1. **［テストメールの宛先］**に、テストメールの送信先メールアドレスを入力します。
2. **［指定されたタイムアウトの使用］**にテストメールの配信開始からメール送信に成功するか、エラー通知が返ってくるまでのタイムアウトを入力します。各 IP アドレスのテストが行われ、1 つでも失敗した場合は、全処理に対してエラーが返されます。1 つの IP チェックにつき、最大 255 秒です。エラーログは 2 日間保存されます。テスト中、**［送信者のメール］**アドレスが有効であっても**［宛先アドレス］**が無効であると、配信されません。
3. **［テストメールの送信］**をクリックします。設定を使用してメールが送信されます。エラーまたはタイムアウトが発生した場合、ユーザーインターフェイスにメッセージが表示されます。

4. メールが配信されたことを確認してください。ユーザーインターフェイスにメッセージが表示されなかったが、メールが配信されなかった場合、SMTPSVC1 フォルダのサポートバンドルのログファイルを確認します。2 日分のログが保持されています。詳しくは、「Support Bundle」を参照してください。

メール通知の有効化

ユーザーがメール通知を受信できるようにするには、いくつかの項目を適切に設定する必要があります。

メール通知の有効化手順

1. ユーザーはメールアドレスを正しく設定する必要があります。
    a. ローカルユーザーの場合：
        i. 権限許可者管理者またはユーザー管理者が、ユーザーの連絡先で設定します。詳細については、「ユーザーの追加」を参照してください。

        または

        ii. ユーザーは、**[私のアカウント]** 設定で設定します。

    b. ディレクトリユーザーは、Active Directory または LDAP ドメインでメールを設定する必要があります。
2. アプライアンス管理者は、SMTP サーバーを構成する必要があります。詳細については、「メール」を参照してください。

> **ヒント**：
> https://<アプライアンス IP>/service/core/swagger/ui/index#/EventSubscribers
> を使用して、任意のメールイベントタイプに対するメール購読を設定することができます。詳細については、「API の使用」を参照してください。

9.6.2 Email Events（メールイベント）

Email Events ページは、特定の SPP イベントに関するメールを受信する購読者を追加および管理するために使用されます。

Email Events へのアクセス：

［アプライアンス管理］＞［外部統合］＞［Email Events］に移動します。

Email Events ペインには、定義された購読者について次のように表示されます。

表：Email Events：プロパティ

プロパティ	説明
Subscriber	メールイベントの受信者の名前
説明	メールイベントの説明
Shared	すべてのアプライアンス管理者が**［Email Events］**ページでメールイベントサブスクリプションの情報を見ることができる場合、チェックマークが表示されます。
イベント数	メール送信されたイベントの数

メールイベントのサブスクライバーを管理するには、次のツールバーボタンを使用します。

表：Email Events：ツールバー

オプション	説明
追加	新しいメールイベントの登録者を追加します。詳しくは、「メールイベントの追加」を参照してください。
削除	選択したメールイベントを SPP から削除します。
編集	メールイベントを変更します。
コピー	選択したメールイベントのクローンを作成します。
Show System Owned **Hide System Owned**	これらのボタンを使用して、システム所有のメールイベントを一覧から表示または非表示にします。
更新	E メールイベントのリストを更新します。
テストイベントの送信	テストメッセージを送信します。

メールイベントの追加

イベントの追加は、アプライアンス管理者の責任です。

メールイベントの追加手順

1. **［アプライアンス管理］＞［外部統合］＞［Email Events］**に移動します。
2. ＋ **［追加］**をクリックし、**［Email Events Subscription］**ダイアログを開きます。
3. **［Email Events Subscription］**ダイアログで、以下を入力します：
    a. **Email Address**：受信者のメールアドレスを入力するか、**［参照］**ボタンを使用します。
    b. **説明**：イベントの説明を入力します。
    c. **Subscribe to All Events**：このチェックボックスを選択すると、今後追加される可能性のある新しいイベントも含め、すべてのイベントに登録されます。未選択の場合は、特定のイベントを選択します。

    イベントを作成するユーザーが、設定されたすべてのイベントを受信するのに十分な権限を持っていることを確認してください。設定されているすべてのイベントを受信するのに十分な権限を持たないユーザーがイベントを設定した場合、一部のイベントが受信されないことがあります。このような場合は、メールイベントを削除し、十分な権限を持つユーザーで再作成してください。
    d. **すべてのイベントにサブスクライブ：** 選択されていない場合は、**［参照］**をクリックし、受信するイベントのチェックボックスを選択します。**［OK］**をクリックします。
4. **［OK］**をクリックします。

9.6.3 メールテンプレート

SPP は、Cluster Primary Quorum Fails や Access Request Denied など、ほとんどのイベントに対してデフォルトのメールテンプレートを提供しています。各イベントタイプは、テンプレートを使用するメール通知をトリガーします。

メールテンプレートへのアクセス

［アプライアンス管理］＞［外部統合］＞［メールテンプレート］に移動します。

メールテンプレートを管理するには、以下のツールバーボタンを使用します。

表：メールテンプレート：ツールバー

オプション	説明
リセット	選択したテンプレートをデフォルトにリセットします。
編集	選択したメールテンプレートを編集します。
更新	メールテンプレートリストを更新します。
検索	特定のテンプレートを検索します。一致する文字列を入力して検索します。詳しくは、「検索ボックス」を参照してください。

マクロのプロパティ

各イベントタイプは、そのイベントのタイプに適したテンプレート内の特定のマクロをサポートしています。テンプレートの編集時に**［イベントプロパティマクロの挿入］**をクリックすると、二重波括弧で囲まれたキーワードを使用して、件名行または本文のテキストに挿入するプロパティを選択することができます。例えば、メールの件名に以下のイベントプロパティを選択することができます。

「アクセスポリシーが作成されました {{EventDescription}} {{PolicyId}}」

SPP は、イベントタイプでサポートされていないマクロを無視します。サポートされていないマクロは、メールプレビューで空白表示されます。また、以下のような警告メッセージが表示されることがあります。「BodyTemplate プロパティのフォーマットが無効です。」

メールテンプレートの編集手順

メールテンプレートはイベント種類以外の情報を変更することができます。後で元のテンプレートに戻す場合は、テンプレートを選択し、**［リセット］**をクリックします。テンプレートを変更するには、次の手順を実行します。

1. **［アプライアンス管理］**＞**［外部統合］**＞**［メールテンプレート］**に移動します。
2. **メールテンプレート**表で修正するテンプレートを選択して をクリックします：
    a. **イベント**：詳細については、「メール通知の有効化」を参照してください。
    b. **件名**：メールメッセージの件名行を編集します。

    ［イベントプロパティマクロの挿入］をクリックすると、件名行に定義済みのテキストが挿入されます。例えば、以下のような件名を作成することができます：

{{Requester}}のリクエストに対して承認が必要です。

SPP は、二重波括弧内のマクロで定義されたデータを生成します。制限: 1024 文字

c. **返信先**：この通知について返信する人のメールアドレスを 512 入力します。制限：512 文字

d. **本文**：メッセージの本文を入力します。

入力中に＋**［イベントプロパティマクロの挿入］**をクリックすると、本文に定義済みのテキストが挿入されます。例えば、メールテンプレートに以下のような本文を作成することができます。

{Requestester}}は{{AssetName}}上の{{AccountName}}のパスワードをリクエストしました。

ここで、SPP は、二重波括弧内のマクロで定義されたデータを生成します。

制限: 16384 文字

e. **メールのプレビュー**: このリンクを選択すると、メールのプレビューダイアログが表示され、メールメッセージがどのように表示されるかを確認することができます。

f. **［OK］**をクリックします。更新されたテンプレートがメールテンプレートページに追加されます。

3. デフォルトに戻したい場合は、メールテンプレートを選択して**［リセット］**を選択します。

9.6.4 ハードウェアセキュリティモジュール

SPP を外部のハードウェアセキュリティモジュールと統合して暗号化するように構成するのは、アプライアンス管理者の責任です。

ハードウェアセキュリティモジュールペインを使用して、ハードウェアセキュリティモジュール統合を構成してください。以下のハードウェアセキュリティモジュールがサポートされています。

- Thales Luna 7.X
- Thales Luna 6.X
- Thales データ保護オンデマンド

ハードウェアセキュリティモジュールへのアクセス

［アプライアンス管理］＞［外部統合］＞［ハードウェアセキュリティモジュール］に移動します。

開始前に

ハードウェアセキュリティモジュールの統合を構成する前に、Thales Luna 環境が完全にインストールされ構成されている必要があります。これには以下が含まれますが、これに限定されるものではありません。

- Crypto Officer のパスワードの設定
- ハードウェアセキュリティモジュールのサーバー証明書の生成（ネットワーク Luna のみ）
- SPP クラスタアプライアンスごとにハードウェアセキュリティモジュールのクライアント証明書を生成（ネットワーク Luna のみ）
- パーティションの初期化
- SPP が利用する高可用性グループの作成

SPP は、統合を構成するために以下の情報を必要とします：

- Crypto Officer パスワード
- サーバー証明書（複数可）（ネットワーク Luna のみ）
- クライアント証明書（複数可）（ネットワーク Luna のみ）
- パーティションラベル（高可用性グループラベルでも可）
- crystoki.ini ファイル

ネットワーク Luna デバイスを含む統合を構成する場合、まず、お使いの環境に合わせたハードウェアセキュリティモジュールクライアント証明書とサーバー証明書をインストールし、割り当てます。詳しくは、「ハードウェアセキュリティモジュールクライアント証明書のインストール」、「ハードウェアセキュリティモジュールクライアント証明書の割り当て」、「ハードウェアセキュリティモジュールサーバー証明書のアップロード」を参照してください。

> **重要：**ネットワーク Luna デバイスへの接続は、ネットワークトラストリンク（NTLs）接続を介してのみサポートされています。SPP と統合する場合、Secure Trusted Channel（STC）接続はサポートされません。

注意: **ハードウェアセキュリティモジュールの統合のベストプラクティスは、スタンドアロンの SPP アプライアンスでのみ有効または無効にすることです。SPP アプライアンス内に保存されている暗号化データは、これらの操作中に再暗号化されます。クラスタ環境で有効化または無効化する場合、クラスタは破壊され、プライマリ SPP アプライアンスはスタンドアロンアプライアンスに設定され、メンテナンスタスクの完了後にすべてのレプリカをクラスタに再接続する必要があります。この間、データの破損を避けるため、パスワードの確認や変更など、暗号化されたデータを使用する操作がレプリカアプライアンスで実行されないようにします。**

注意: **SPP は、ハードウェアセキュリティモジュールパーティションに保存された暗号化キーの予約済みラベルを使用します。これらのラベルは、初めて統合を行うときにパーティションに存在することはできません。**

予約されたキーのラベル名：SafeguardMasterKey1

注意: **ネットワーク Luna デバイスを含む統合を構成する場合、プライマリ SPP アプライアンスに、将来のすべてのクラスタメンバー用にすべてのクライアント証明書とサーバー証明書がインストールされていることを確認します。さらに、クラスタに参加する前に、必要なクライアント証明書をレプリカにインストールし、割り当てます。**

ハードウェアセキュリティモジュールの統合設定

1. **［アプライアンス管理］**＞**［外部統合］**＞**［ハードウェアセキュリティモジュール］**に移動します。
2. **［外部 HSM の使用］**チェックボックスを選択します。
3. **［パーティションラベル］**フィールドに、SPP がハードウェアセキュリティモジュールデバイスで使用するパーティションラベルを入力します。
4. SPP がハードウェアセキュリティモジュールデバイスに接続するために使用する暗号化責任者のパスワードを入力します。
5. **［ファイルのアップロード］**をクリックし、crystoki.ini 構成ファイルを参照します。
6. 選択したら、**［開く］**をクリックします。
7. **［保存］**をクリックします。

   メモ: 提供された構成に基づいて統合を進める際に SPP の機能にエラーが発生した場合、ユーザーインターフェイスに詳細情報を示すメッセージが表示されます。

ハードウェアセキュリティモジュール統合の構成が完了すると、次の情報とオプションが利用できるようになります。

表：ハードウェアセキュリティモジュール：プロパティ

設定	説明
健全性ステータス	前回のハードウェアセキュリティモジュールの検証結果が表示されます。
更新	ハードウェアセキュリティモジュールの検証を実行します。これは、SPP アプライアンスを HardwareSecurityModuleError 状態から移行させるために使用することができます。
前回のアクセス成功日	前回ハードウェアセキュリティモジュールの状態が健全になった日付と時刻
詳細の表示	ハードウェアセキュリティモジュールの統合に使用されている現在の crystoki.ini の内容が表示されます。

ハードウェアセキュリティモジュール統合の無効化

1. **［アプライアンス管理］＞［外部統合］＞［ハードウェアセキュリティモジュール］**に移動します。
2. **［外部 HSM のを用］**チェックボックスの選択を解除します。
3. **［保存］**をクリックします。

9.6.5 SNMP

SNMP（Simple Network Management Protocol）は、IP ネットワーク上のデバイスを管理するためのインターネット標準のプロトコルです。SPP では、特定のイベントが発生したときに SNMP トラップを SNMP コンソールに送信するための SNMP サブスクリプションを設定することができます。

SNMP へのアクセス：

［アプライアンス管理］＞［外部統合］＞［SNMP］に移動します。

SNMP ペインには、定義された SNMP サブスクライバーについて、次のように表示されます。

表：SNMP:プロパティ

プロパティ	説明
ネットワークアドレス	プライマリ SNMP ネットワークサーバーの IP アドレスまたは FQDN
ポート	SNMP トラップ用の UDP ポート番号
バージョン	使用する SNMP のバージョン
説明	SNMP サブスクライバーの説明
コミュニティ	SNMP サブスクライバーによって使用されている SNMP コミュニティ文字列
イベント数	SNMP コンソールに送信するために選択したイベントの数

SNMP サブスクリプションを下のツールバーボタンを使用して管理します。

表：SNMP：ツールバー

オプション	説明
追加	新しい SNMP サブスクリプションを追加します。詳細については、「SNMP」を参照してください。
削除	選択した SNMP サブスクリプションを削除します。
編集	選択した SNMP サブスクリプションを変更します。
SNMP テンプレートのコピー	選択した SNMP サブスクリプションのクローンを作成します。
更新	SNMP サブスクリプションのリストを更新します。

SNMP サブスクリプションの設定

特定のイベントが発生したときに SNMP コンソールに SNMP トラップを送信するよう SPP を設定することは、アプライアンス管理者の責任です。

SNMP 設定を検証するために、テストを作成することができます。詳細については、「SNMP 設定の検証」を参照してください。

アプライアンスから SPP の MIB モジュール定義をダウンロードするには、Web ブラウザーに次の URL を入力します（認証なし）。

https://<アプライアンス IP アドレス>/docs/mib/SAFEGUARD-MIB.mib

SNMP サブスクリプションの構成手順

1. **［アプライアンス管理］＞［外部統合］＞［SNMP］**に移動します。
2. ＋**［追加］**をクリックし、**SNMP** ダイアログを開きます。
3. 以下の情報を入力します：
    - **ネットワークアドレス**：プライマリ SNMP ネットワークサーバーの IP アドレスまたは FQDN を入力します。制限：255 文字
    - **UDP ポート**：SNMP トラップ用の UDP ポート番号を入力します。デフォルト：162
    - **説明**：SNMP サブスクリプションの説明を入力します。制限：255 文字
    - **すべてのイベントにサブスクライブ**：すべてのイベントを購読する場合は、このチェックボックスを選択します。
    - **イベント**：**［すべてのイベントにサブスクライブ］**が選択されていない場合に使用できます。**［参照］**をクリックして、1 つまたは複数の SNMP イベントの種類を選択します。このリストから個々のイベントを削除するには、**［消去］**アイコンを使用し、リストからすべてのイベントを削除するには、**［消去］**ボタンを選択します。SNMP ペインには、イベントの名前ではなく、選択したイベントの数が表示されます。
    - **バージョン：** SNMP のバージョンを選択します。デフォルトはバージョン 2 です。選択したバージョンに応じて、以下のフィールドが表示されます。
        - バージョン 1 とバージョン 2：
            - **［コミュニティ］**：SNMP コミュニティ文字列を入力します（例：public）。SNMP コミュニティ文字列は、ルーターなどのデバイスの統計情報へのアクセスを許可するユーザーID、パスワードのようなものです。PRTG Network Monitor は、すべての SNMP リクエストと一緒にコミュニティ文字列を送信します。コミュニティ文字列が正しい場合、デバイスは要求された情報を応答します。コミュニティ文字列が正しくない場合、デバイスは単に要求を破棄し、応答しませ ん。

4. **［OK］**をクリックします。

SNMP 設定の検証

SNMP 表の下にある**［テストイベントの送信］**を使用し、テストイベントを送信して SNMP の設定を検証します。

設定の検証手順

1. **［アプライアンス管理］＞［外部統合］＞［SNMP］**に移動します。
2. SNMP サブスクリプションを設定する際に、**SNMP** ダイアログで、テストイベントをイベントサブスクリプションに追加します。詳細については、「SNMP サブスクリプションの設定」を参照してください。
3. SNMP 設定ペインで以下を行います：
    a. 表中の SNMP 設定を選択します。
    b. **［テストイベントの送信］**をクリックします。SPP は、SNMP コンソールにテストイベント通知を送信します。

9.6.6 Starling

SPP は、クラウドプラットフォームの One Identity Starling と連携することができます。One Identity Starling に参加することで、SPP のお客様は、複数の Starling サービスのコンパニオン機能を利用することができるようになります。また、SPP が Starling に参加すると、Starling の ID および認証プロバイダが自動的に Safeguard に追加されます。ただし、管理者が Starling のディレクトリ設定ページを介して Microsoft Azure Active Directory テナントを Starling 組織に追加するまで、ユーザーやグループは利用できません。詳細については、以下のセクションを参照してください。

- Starling 参加
- Starling 参加後
- Starling の参加解除

Starling 参加

Starling サービスに関連する SPP 機能を使用するためには、SPP を Starling に参加させる必要があります。SPP を Starling に参加させることは、アプライアンス管理者の責任です。

Starling Cloud プラットフォームおよびサービスに関するその他の情報およびドキュメントについては、「One Identity ドキュメント」を参照してください。

前提条件

現在サポートされているプラットフォームについては、Starling リリースノートを参照してください。

Starling のサービスからコンパニオン機能を利用するためには、まず以下の設定を行います：

- Starling 組織を登録する。：Starling の詳細については、「One Identity Starling User Guide」を参照してください。

  > **重要**：すべての Starling サービスが、米国と欧州連合の両方のデータセンターの組織で利用できるわけではありません。Starling サービスのドキュメントを確認し、データセンターの制約があるかどうかを確認してください。

- あなたの会社がインターネットにアクセスするためにプロキシの使用を必要とする場合、使用する Web プロキシを設定する必要があります。SPP が統合サービスへのアウトバウンド Web リクエストに使用する Web プロキシの設定については、「ネットワーク」を参照してください。

- クラウドアシスタント機能を使用するには、Starling クラウドアシスタント機能に参加し、使用するチャネル（複数可）を設定する必要があります。

SPP を Starling に参加させる

> **メモ：**SPP を Starling に参加させるには、Starling 組織の組織管理者である必要があります。

1. **［アプライアンス管理］＞［設定］＞［外部統合］＞［Starling］**に移動します。このページには、Starling に関する情報を提供するリンクも含まれています：
   - **詳細は、オンラインを参照してください**： Starling アカウントを新規に作成できる Starling ログイン ページが表示されます。
   - **参加できませんか？**： Starling のサポートページが表示され、Starling への参加の要件と手順に関する情報が表示されます。

2. **［Starling に参加］**をクリックし、表示される指示に従って手続きを行ってください。

   以下の追加情報が必要な場合があります。

   - Starling との既存のセッションがない場合、認証を求めるプロンプトが表示されます。
   - Starling アカウントが複数の組織に属している場合、SPP をどの組織に参加させるか選択するよう促されます。

3. 参加が正常に完了すると、SPP クライアントに戻り、Starling の設定ペインに Joined to Starling と表示されるようになります。利用可能になった機能については、「Starling 参加後」を参照してください。Starling から参加解除する方法については、「Starling の参加解除」を参照してください。

   > **重要**：クラウドアシスタント機能を使用するには、Starling に参加した後、**［外部統合］＞［Starling］**ペインで**［クラウドアシスタントに送信者として登録］**トグルを有効にする必要があります。

Starling 参加後

SPP を Starling に参加させると、以下の SPP 機能が有効になります。

Starling Connect を利用した機能

- Starling Connect に登録されたコネクタ

  この機能は、お客様の Starling コネクタと SPP を統合するものです。これにより、コネクタに保存されたアカウントは、パスワードをローテートさせて追加のセキュリティを提供することができるパーティションの使用を通じて、SPP によって検出および制御されるようになります。詳細については、「登録済みコネクタ」を参照してください。

Starling Cloud Assistant を使用した機能

- Cloud Assistant

  Cloud Assistant 機能は、アクセスリクエストのワークフローを Starling Cloud Assistant と統合し、アクセスリクエストが送信されると、承認者は設定されたチャネルを通じて通知を受けることができます。承認者は、SPP Web アプリケーションにアクセスすることなく、チャネルを通じてアクセスリクエストを承認（または拒否）することができます。

Cloud Assistant 機能は、SPP を Starling に参加させると有効になります。詳細については、「Starling」を参照してください。有効にした後、アクセスリクエストを承認するために Cloud Assistant を使用する権限を持つユーザーを定義するのは、セキュリティポリシー管理者の責任です。

> **重要**：Cloud Assistant 機能を使用するには、Starling に参加した後、**［アプライアンス管理］＞［外部統合］＞［Starling］**ペインで**［Cloud Assistant に送信者として登録］**トグルを有効にする必要があります。

ID プロバイダとしての Starling

SPP が Starling に参加すると、Starling の ID および認証プロバイダが自動的に Safeguard に追加されます。これは、Starling 下にある Realm(s)のセクションで示されます。しかし、管理者が Starling の Directories settings ページを通じて Microsoft Azure Active Directory テナントを Starling 組織に追加するまでは、利用できるユーザーやグループは存在しません。

ID プロバイダとして Starling を使用する手順

1. SPP を Starling に参加させます。詳細については、「Starling 参加」を参照してください。

2. Starling 組織で Microsoft Azure Active Directory テナントを有効にします（Starling に複数の Microsoft Azure Active Directory テナントを追加できますが、Safeguard で使用する際には 1 つのテナントとして利用・扱われます）。これは、Starling の Directories 設定ページで行います。詳細については、『Starling ユーザーガイド』を参照してください。

3. Safeguard のユーザーが Starling に対して認証を行うには、Starling のアプリケーション設定ページで Relying Party Trust アプリケーションを作成する必要があります。詳細については、『Starling ユーザーガイド』を参照してください。

   Starling でアプリケーションを作成するには、「ID と認証」から Safeguard Federation Metadata をダウンロードする必要があります。

   > **メモ**: Add OpenID Connect Application は SPP と一緒にを使用することはできません。

4. 新しい Starling 認証プロバイダと関連付けるために、Realm(s)セクションに 1 つ以上の値を入力する必要があります。これにより、Safeguard にログインしているユーザーは、External Federation を選択し、認証に Starling を使用できるようになります。

5. Require User to Always Authenticate チェックボックスを選択すると、ユーザーはすでにログインしているかどうかにかかわらず、常に外部プロバイダで認証情報を入力する必要があります。

Starling から Safeguard への新しいユーザーとグループの追加は、他のディレクトリベースの ID プロバイダ（Active Directory や LDAP など）と同じプロセスに従い、ユーザー情報は定期的に Starling から同期されます。

> **重要**：Starling を利用可能な ID プロバイダとして表示するために、クライアントを再起動する必要がある場合があります。

Starling の参加解除

Starling から SPP の参加を解除するのは、アプライアンス管理者の責任です。

Starling Cloud プラットフォームおよびサービスに関する追加情報および文書については、「One Identity ドキュメント」を参照してください。

Starling から SPP の参加を解除する手順

1. **［アプライアンス管理］＞［外部統合］＞［Starling］**を選択します。
2. **［Starling への参加を解除する］**をクリックします。

   SPP は Starling に参加しなくなるため、SPP では Cloud Assistant、Starling ID プロバイダ、および統合コネクターも無効化されます。Starling Organization Admin アカウントは、いつでも SPP を Starling に再参加させることができます。

   > **重要**: ID と認証に Starling プロバイダを使用する Safeguard ユーザーまたはグループがまだ存在する状態で Starling から再参加しようとすると、エラーが表示されます。Starling からアンインストールする前に、まず手動でユーザーまたはグループを削除する必要があります。

9.6.7 Syslog

SPP では、SPP イベントメッセージのログに使用する 1 つまたは複数の Syslog サーバーを定義することができます。アプライアンス管理者は、異なるタイプのメッセージを異なる Syslog サーバーに送信するように指定することができます。クライアント認証証明書の有無にかかわらず、TLS 暗号化を使用するように Syslog サーバーへの接続を構成することができます。詳細については、「Syslog クライアント証明書」を参照してください。

Syslog サーバーの定義と管理へのアクセス：

［アプライアンス管理］＞［外部統合］＞［Syslog］に選択します。

[Syslog]ペインには、定義された各 Syslog サーバーについて以下が表示されます。

表：Syslog サーバー：プロパティ

プロパティ	説明
名前	Syslog サーバーの名前
ネットワークアドレス	Syslog サーバーの IP アドレスまたは FQDN
ポート	Syslog サーバーのポート番号
プロトコル	ネットワークプロトコルと Syslog ヘッダータイプ
TCP フレーム	TCP プロトコルで Syslog を使用する場合、接続はストリームベースなので、クライアントとサーバーの両方が同じデリミタを使用してデータを処理するように設定される必要があります。詳細については、「RFC 6587 の 3.4.1 項と 3.4.2 項」を参照してください。デフォルトでは、RFC 6587 推奨のオクテットカウンティングを使用します。ただし、一部の Syslog サーバーは、オクテットカウンティングに対応していません。その場合は、この設定を使用して、SPP が Syslog サーバーでサポートされている区切り記号を使用するように構成します。
TLS 暗号化の使用	✔の場合、TCP 上のプレーンテキストではなく、Syslog サーバーとの暗号化された通信を提供します。
クライアント証明書の使用	✔の場合、Syslog サーバーはクライアントに認証を要求します
サーバー証明書の使用	✔の場合、SPP が Syslog サーバーTLS 証明書の信頼性を確認できる場合にのみ、Syslog サーバー証明書メッセージが送信されます。

Syslog サーバー設定は下のツールバーボタンを使用して管理します。

表：Syslog サーバー：ツールバー

オプション	説明
＋ 追加	新しい Syslog サーバー設定を追加します。詳細については「Syslog サーバーの構成と検証」を参照してください。
削除	選択した Syslog サーバー設定を SPP から削除します。

オプション	説明
	使用中の Syslog サーバーを削除しようとすると、次のようなメッセージが表示されます。「<syslog server>は削除されます。」「**はい**」または「**いいえ**」を選択します。 以下のようなメッセージが表示されることがあります。「このシスログサーバーには依存関係があります。このオブジェクトは ServiceDebug によって参照されています。このサーバーを強制的に削除しますか？**［強制削除］**または**［キャンセル］**を選択します。**［強制削除］**を選択すると、依存する設定（イベントサブスクライバーやデバッグロギングなど）も削除されます。
編集	選択した Syslog サーバー設定を編集します。
Syslog テンプレートのコピー	選択した Syslog サーバー設定を複製します。
更新	Syslog サーバー設定のリストを更新します。

Syslog サーバーの構成と検証

イベントメッセージを Syslog サーバーに記録するよう SPP を設定するのは、アプライアンス管理者の責任です。以下の手順では、構成を説明します。

その他の考慮事項：

- イベントメッセージをログに記録するには、SPP を設定して、アラートを送信する必要があります。詳細については、「アラートの構成」を参照してください。
- Syslog クライアント証明書が使用されます。詳細については、「Syslog クライアント証明書」を参照してください。

Syslog サーバーの構成手順

1. **［アプライアンス管理］＞［外部統合］＞［Syslog］**に移動します。
2. ＋**［追加］**をクリックして、**［Syslog サーバー］**ダイアログを表示します。
3. **Syslog** ダイアログで、以下を入力します：
    a. **名前**：Syslog サーバーの名前を入力します。

b. **ネットワークアドレス**：Syslog サーバーの IP アドレスまたは FQDN を入力します。制限：255 文字

c. **ポート**：Syslog サーバーのポート番号を入力します。
デフォルト：514。範囲：1～32767 の間

d. **プロトコル**：ネットワークプロトコルと Syslog ヘッダーの種類を選択します。

- UDP（RFC 3164）：RFC 3164 で指定されている Syslog ヘッダー形式を使用して、UDP でメッセージを送信します。
- UDP (RFC 5424)：RFC 5424 で指定されている Syslog ヘッダー形式を使用して UDP でメッセージを送信します。
- TCP (RFC 5424)：RFC 5424 で指定されている Syslog ヘッダー形式を使用して、TCP 上でメッセージを送信します。TCP は TLS オプションのために必要です。

e. **TCP（RCF 5424）**プロトコルを選択した場合、TCP フレームを設定し、SPP が TLS (Transport Layer Security) を使用するように設定するための追加選択を行うことができます。これは、TCP 上のプレーンテキストではなく、Syslog サーバーとの暗号化通信を提供します。

- **TCP フレーム**を選択します。デフォルトでは、**[オクテットカウント]**が選択されます。可能なオプションは以下の通りです：
  - **オクテットカウント**：デフォルトおよび推奨のフレームです。詳細については、https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.1 を参照してください。オクテットカウントでは、区切り文字として使用される可能性のある文字がメッセージに含まれる可能性はありません。
  - **LF**：改行文字（LF 0x0A）を Syslog メッセージ間のデリミタとして使用します。詳細については、https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2 を参照してください。RFC では、このフレームを使用する際の問題点を記述しているため、推奨されないことに注意してください。しかし、Syslog サーバーの中には、オクテットカウントをサポートせず、これらの非透過的なフレームオプションを使用しなければならないものがあります。SPP は、この文字がメッセージ自体に現れた場合、この文字をエスケープアウトすることを試みません。その場合、断片化された、潜在的に不正なメッセージ/データを受信することになります。

- **CR**：キャリッジリターン文字（CR 0x0D）を Syslog メッセージ間のデリミターとして使用します。詳細については、https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2 を参照してください。この RFC では、このフレームを使用する際の問題点を説明しているため、推奨されないことに注意してください。しかし、Syslog サーバーの中には、オクテットカウントをサポートせず、これらの非透過的なフレームオプションを使用するものがあります。SPP は、この文字がメッセージ自体に現れた場合、この文字をエスケープアウトすることを試みません。その場合、断片化された、潜在的に不正なメッセージ/データを受信することになります。
- **CRLF**：キャリッジリターン文字とラインフィード文字の両方（CRLF 0x0D0A）を、Syslog メッセージ間の区切り文字として使用します。詳細については、https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2 を参照してください。RFC は、このフレームを使用する際の問題点を記述しているので、推奨されないことに注意してください。しかし、syslog サーバーの中には、オクテットカウントをサポートせず、これらの非透過的なフレームオプションを使用しなければならないものがあります。SPP は、この文字がメッセージ自体に現れた場合、この文字をエスケープアウトすることを試みません。その場合、断片化された、潜在的に不正なメッセージ/データを受信することになります。
- **NUL**：NUL 文字（0x00）を Syslog メッセージ間のデリミタとして使用します。詳しくは、https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2 を参照してください。RFC では、このフレームを使用する際の問題点を説明しているため、推奨されないことに注意してください。しかし、Syslog サーバーの中には、オクテットカウントをサポートせず、これらの非透過的なフレームオプションを使用するものがあります。SPP は、この文字がメッセージ自体に現れた場合、この文字をエスケープアウトすることを試みません。その場合、断片化された、潜在的に不正なメッセージ/データを受信することになります。

◦ **[TLS 暗号化の使用]** を選択します。

- **Syslog サーバー証明書の検証**：選択した場合、SPP が Syslog サーバーTLS 証明書の信頼性を確認できた場合のみ、Syslog サーバー証明書メッセージが送信されます。SPP が Syslog サーバーの TLS 証明書を信頼できるルートに解決できない場合、メッセージは送信されません。
- **クライアント証明書の使用**：Syslog サーバーがクライアントの認証を必要とする場合、このオプションを選択します。また、Syslog クライアント証明書を適切に設定する必要があります。詳細については、「Syslog クライアント証明書署名リクエストの作成」を参照してください。

4. **［OK］**をクリックして選択を保存し、Syslog サーバーの設定を追加します。
5. Syslog サーバーを検証することができます。次のセクションを参照してください。

Syslog サーバー設定の検証手順

1. **［アプライアンス管理］＞［外部統合］＞［Syslog イベント］**に移動します。
2. **［テストイベントの送信］**をクリックします。詳しくは「Syslog イベント」を参照してください。

9.6.8 Syslog イベント

Syslog サーバー（クラスタ全体）に送信する監査イベントログを設定することができます。監査イベントには、接続、クローズ、障害が含まれます。失敗には、理由、イニシエータ、ターゲットが含まれます。たとえば、証明書検証の失敗には、イニシエータとターゲットが含まれます。

Syslog サーバーへのデバッグログは利用可能で、アプライアンスに依存します。「デバッグ」を参照してください。

監査イベントログを Syslog サーバーに送信する設定手順

1. 構成済みの Syslog サーバーが必要です。Syslog サーバーが構成されていない場合、次のようなメッセージが表示されます。「追加のデバッグログオプションを設定するには、Syslog サーバーを設定する必要があります。」**［Syslog サーバーの設定］**をクリックします。詳細については、「Syslog サーバーの構成と検証」を参照してください。
2. **［アプライアンス管理］＞［外部統合］＞［Syslog イベント］**を選択します。

3. **［Syslog イベント］**ペインに以下が表示されます。

表：Syslog イベント：プロパティ

プロパティ	説明
Syslog サーバー	Syslog サーバーの名前
機能	Syslog メッセージの作成に使用されるプログラムの種類（例：User または Mail）
ログの形式	CEF または JSON
説明	Syslog イベントの説明
イベント数	Syslog サーバーに記録されるイベントの数

Syslog イベント設定は下のツールバーボタンを使用して管理します。

表：Syslog イベント：ツールバー

オプション	説明
追加	新しい Syslog イベント設定を追加します。
削除	選択した Syslog イベント設定を削除します。
編集	選択した syslog イベント設定を変更します。
Syslog テンプレートのコピー	選択した Syslog イベント設定を複製します。
更新	Syslog イベントのリストを更新します。
テストイベントの送信	指定した Syslog イベントを送信します。

Syslog イベントサブスクライバーの追加

イベントサブスクライバーを追加するのは、アプライアンス管理者の責任です。

イベントサブスクライバーの追加手順

1. **［アプライアンス管理］＞［外部統合］＞［Syslog イベント］**を選択します。
2. **＋［追加］**をクリックして、**［Syslog イベント］**ダイアログを表示します。

3. **［Syslog イベント］**ダイアログで、以下を入力します：

    i. **Syslog サーバー**:イベントの送信先となるサーバーを選択します。

    ii. **説明**：Syslog イベントの説明を入力します。

    iii. **すべてのイベントにサブスクライブ：**このチェックボックスを選択すると、今後追加される可能性のある新しいイベントも含め、すべてのイベントを購読します。未選択の場合は、特定のイベントを選択します。

    Syslog イベントエントリを作成するユーザーが、設定したすべてのイベントを受信するのに十分な権限を持っていることを確認してください。設定されているすべてのイベントを受信するのに十分な権限を持たないユーザーが Syslog イベントエントリを設定した場合、一部のイベントが受信されないことがあります。この場合、Syslog イベントエントリを削除して、十分な権限を持つユーザーで再作成してください。

    iv. **［すべてのイベントにサブスクライブ］**が選択されていない場合は、**［参照］**をクリックし、受信するイベントのチェックボックスを選択します。**［OK］**をクリックします。

    v. **機能**（Facility）：送信する Syslog 機能を選択します（例：User または Mail）。

    vi. **ログの形式**：Common Event Format (CEF) または Javascript Object Notation (JSON) のいずれかを選択します。

    vii. **属性のプレフィックス**：JSON を選択した場合、JSON 属性の前に付加される属性のプレフィックスを入力します。

4. **［OK］**をクリックします。

9.6.9 チケットシステム

外部のチケットシステムで構成されていないチケットを使用したり、外部のチケットシステム（ServiceNow や Remedy など）と統合したりすることができます。

チケットは、アクティビティセンターの**［チケット番号］**列で確認できます。

外部チケットシステムと統合していない場合

セキュリティポリシー管理者は、要求者がパスワードまたはセッションアクセスのリクエストでチケット番号を参照することを要求できますが、チケットは外部のチケットシステムに対して検

証されません。オプションとして、汎用チケットシステムの正規表現に対して検証される場合があります。チケット番号はリクエストの承認を決定する際に使用されます。

チケットシステムへのアクセス

［アプライアンス管理］＞［外部統合］＞［チケットシステム］へ移動します。

チケットツールバー

SPP と統合するために定義されたチケットシステムを管理するには、これらのツールバーボタンを使用します。

- **［追加］:** 新しいチケットシステムを追加します。
- **［削除］:** 選択したチケットシステムを SPP から削除します。
- **［編集］**:選択したチケットシステムの設定を変更します。
- **［更新］**: チケットシステムのリストを更新します。

セットアップとワークフロー

セットアップとワークフローの詳細については、使用するチケットに基づき、以下を参照してください。

- ServiceNow チケットシステム統合
- Remedy チケットシステム統合
- チケットシステムとの統合なし

ServiceNow チケットシステム統合

ServiceNow は、クラウドベースの課題追跡システムです。SPP は、ServiceNow と以下のチケットタイプを交換することができます。

- INC（インシデント）チケット
- CHG（変更）チケット
- RITM（リクエスト）チケット
- PRB（問題）チケット

ServiceNow 固有のデータ項目は、お客様の設定によりオプションとなる場合があります。

ServiceNow を使用するには、ServiceNow に必要なルート CA 証明書が SPP にインストールされている必要があります。詳細については、「信頼できる CA 証明書」を参照してください。信頼できる証明書を追加するには、「信頼できる証明書の追加」を参照してください。

チケットは、アクティビティセンターの「チケット番号」列で確認することができます。

統合設定

1. **［アプライアンス管理］＞［外部統合］＞［チケットシステム］**に移動します。
2. ＋ **［追加］**をクリックし、**［ServiceNow］**チケットシステムを追加します。
3. インストールに基づき、認証情報を入力します。
    - **名前**： チケットシステムの名前を入力します
    - **URL**：チケットシステムの Web サイトのアドレスを入力します。
    - **ユーザー名**：SPP がチケットシステムにアクセスするために使用するアカウントを入力します。
    - **パスワード**：ユーザーアカウントのパスワードを入力します。
    - **クライアント ID**： ServiceNow クライアント ID を入力します。
    - **クライアントシークレット**：ServiceNow のシークレットキーを入力します。
4. **［接続のテスト］**をクリックして、ServiceNow への接続をテストします。

チケットワークフロー

1. セキュリティポリシー管理者は、アクセスリクエストの作成時に要求者にチケット番号の提供を要求するアクセスリクエストポリシーを作成します。
2. 要求者はリクエストを作成する際に、既存の ServiceNow チケット番号を**［新規アクセスリクエスト］**ダイアログの**［リクエスト詳細］**タブ、**［チケット番号］**フィールドに入力する必要があります。参照してください。
    - パスワードリリースのリクエスト
    - SSH キーリリースのリクエスト
    - セッションアクセスのリクエスト
3. SPP は、設定されているすべてのチケットシステムに照会し、そのチケット番号が存在し、オープンな状態であるかどうかを確認します。ServiceNow の場合、Safeguard は ServiceNow API から返された識別されたチケットのアクティブプロパティを確認し、そ

のインシデントに対してアクティブプロパティが偽でなければ、チケット番号を有効であるとみなします。

a. チケットがアクティブでない場合、リクエストは拒否されます。

b. チケットがアクティブの場合、アクセスワークフローは続行されます。

Remedy チケットシステム統合

Remedy と統合するように設定されたチケットを使用することができます。

チケットは、アクティビティセンターの「チケット#」列で確認することができます。

Safeguard は、Remedy API から返されたインシデントの Status プロパティをチェックします。Status が クローズ または キャンセルでない場合、チケットは有効であるとみなされます。

Remedy 固有のデータ項目は、お客様の設定に基づきオプションとなる場合があります。

統合設定

1. **［アプライアンス管理］＞［外部統合］＞［チケットシステム］**に移動します。
2. ＋ **［追加］**をクリックし、**［Remedy］**チケットシステムを追加します。
3. インストールに基づき、認証情報を入力します。
    - **名前**： チケットシステムの名前を入力します
    - **URL**：チケットシステムの Web サイトのアドレスを入力します。
    - **ユーザー名**：SPP がチケットシステムにアクセスするために使用するアカウントを入力します。
    - **パスワード**：ユーザーアカウントのパスワードを入力します。
    - **認証文字列**： Remedy AR（アクションリクエスト）システムサーバーのクライアント ID を入力します。
4. **［接続のテスト］**をクリックして、Remedy への接続をテストします。

チケットワークフロー

1. セキュリティポリシー管理者は、アクセスリクエストの作成時に要求者にチケット番号の提供を要求するアクセスリクエストポリシーを作成します。
2. 要求者はリクエストを作成する際に、既存の ServiceNow チケット番号を**［新規アクセスリクエスト］**ダイアログの**［リクエスト詳細］**タブ、**［チケット番号］**フィールドに入力する必要があります。参照してください。
    - パスワードリリースのリクエスト
    - SSH キーリリースのリクエスト
    - セッションアクセスのリクエスト
3. SPP は、設定されているすべてのチケットシステムに照会し、そのチケット番号が存在し、オープンな状態であるかどうかを確認します。

チケットシステムとの統合なし

外部のチケットシステムと統合していないチケットを使用して、チケットを追跡することができます。

チケットは、アクティビティセンターの「チケット番号」列で確認できます。

セキュリティポリシー管理者は、要求者がパスワード、SSH キー、またはセッションアクセスリクエストでチケット番号を参照することを要求できます。チケットは外部のチケットシステムに対して検証されませんが、オプションとして、一般的なチケットシステムの正規表現に対して検証される可能性があります。チケット番号はリクエストの承認を決定する際に使用されます。

統合設定

1. **［アプライアンス管理］＞［外部統合］＞［チケットシステム］**に移動します。
2. ＋ **［追加］**をクリックし、**［その他］**チケットシステムを追加します。
3. インストールに基づき、認証情報を入力します。
    - **名前**： チケットの追跡で使用する名前を入力します。
    - **正規表現**：完全一致を確認するための正規表現パターンを入力します。詳細については、「正規表現」を参照してください。
4. **［検証］**をクリックして、正規表現の入力を検証します。

チケットワークフロー

1. セキュリティポリシー管理者は、アクセスリクエストの作成時に要求者にチケット番号の提供を要求するアクセスリクエストポリシーを作成します。

2. 要求者はリクエストを作成する際に、既存の ServiceNow チケット番号を**［新規アクセスリクエスト］**ダイアログの**［リクエスト詳細］**タブ、**［チケット番号］**フィールドに入力する必要があります。参照してください。

    - パスワードリリースのリクエスト
    - SSH キーリリースのリクエスト
    - セッションアクセスのリクエスト

3. SPP は、設定されているすべてのチケットシステムに照会し、そのチケット番号が存在し、オープンな状態であるかどうかを確認します。

9.6.10 信頼できるサーバー、CORS、リダイレクト

ログインリダイレクトと Cross Origin Resource Sharing（CORS）要求を、指定した IP アドレス、ホスト名（DNS ワイルドカードを含む）、および CIDR 表記ネットワークのリストに制限することができます。デフォルトでは、1 つのアスタリスク（*）は、制限がないことを意味します。これにより、複数の SPP アプライアンスを簡単に結合して、クラスタを形成することができます。さらに、SPS アプライアンスにリンクすることもできるようになります。ただし、ベストプラクティスは、クラスタを構成した後にこの値を変更または削除することです。外部からの CORS リクエストや不明なサーバーへのログインリダイレクトを防ぐために、空の文字列に設定することをお勧めします。または、Safeguard API と統合している既知のサーバーのリストに設定します。

1 つ以上の値は、スペース、カンマ、または改行で区切ることができます。スキーム、ポート、パスは含めないでください。設定の最大長は、セパレータを含めて 512 文字です。値の例とその他の詳細は、次の表で確認できます。

表：値の詳細

許可されるホスト	例
IPv4 DNS の逆引きは行いません。 スキームやポートの値は考慮されません。	10.5.33.37 192.168.0.2

許可されるホスト	例
IPv6 DNS の逆引きは行いません。 スキームやポートの値は考慮されません。	2001:0db8:85a3:0000:0000:8a2e:0370:7334 2001:0db8:85a3:0:0:8a2e:0370:7334 2001:db8::1:0:0:1 2001:db8::2:1 2001:db8::1
DNS/ホスト名 大文字小文字を区別しない一致。スキームやポートの値は考慮されません。国際化ドメイン名（IDN）を使用する場合は、Punycode の相当値も手動で含める必要があります。	spp.contoso.corp primary.spp.contoso.corp widget.contoso.corp widget
DNS ワイルドカード SSL 証明書と同様に、ワイルドカードへの 1 レベルのみ許可されます。スキームやポートの値は考慮されません。国際化ドメイン名(IDN)を使用する場合は、Punycode の相当語も手動で含める必要があります。	*.spp.contoso.corp *.contoso.corp
CIDR ノーテーション 検証される DNS またはホスト名の値は、解決された IP アドレスが指定された CIDR ネットワークのいずれかに含まれるかどうかを確認するために DNS ルックアップが実行されます。スキームやポートの値は考慮されません。	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 76.240.155.0/24 fd12:3456:789a:1::/64 fd00::/8
すべて許可 アスタリスク 1 つで、他の値は許可されません。	*
なしを許可 すべての値を削除し、空の文字列として残します。	すべての値を削除し、空の文字列として残します。

以下について考慮してください

- SPP クラスタに新しいノードを追加する場合、このリストでノードのホスト名または IP アドレスを指定するか、すべてを許可する場合はアスタリスクを 1 つ入力する必要があります。

- SPS を SPP にリンクする場合、SPS アプライアンスのホスト名または IP アドレスをこのリストで指定するか、アスタリスク 1 つを入力してすべてを許可する必要があります。
- ベストプラクティスとして、クラスタリング後（または単一のアプライアンス/VM のみを使用する場合）、設定値を空の文字列または許可する統合アプリケーションのリストに変更します。

信頼できるサーバー、CORS、リダイレクトの設定手順

1. **［アプライアンス管理］＞［外部統合］＞［信頼できるサーバー、CORS、リダイレクト］**に移動します。
2. **［更新］**をクリックすると、表示されている情報が更新されます。
3. **［許可されるホスト］**に、IP アドレス、ホスト名（DNS ワイルドカードを含む）、および CIDR 表記のネットワークのリストを入力します。前述のとおり、デフォルトはアスタリスク（*）1 つで、これは制限がないことを意味します。
4. **［保存］**をクリックします。

9.7　リアルタイムレポート

SPP では、クラスタ、アプライアンスのスケジュール、スケジュールされたプラットフォームタスク、およびアプライアンスリソースに関するリアルタイムの情報を表示することができます。

［アプライアンス管理］＞［リアルタイムアラート］に移動します。

表：リアルタイムレポートページ

ページ	説明
クラスタ情報	
概要	構成されているアプライアンスを一覧表示します。
<アプライアンス名>	各アプライアンスの情報を表示する個別のタブ
セッションアプライアンス	セッションの記録と監査のために、SPS クラスタが SPP にリンクされている場合のリンク接続が表示されます。
アプライアンスのスケジュール	

ページ	説明
監査ログ	監査ログのスケジュールに関する情報が表示されます。
バックアップ	現在ログインしているアプライアンスのバックアップスケジュールに関する情報を表示します。
プロファイルのスケジュール	各プロファイルと検出タイプのスケジュールに関する情報が表示されます。
スケジュールされたプラットフォームタスク	
アプライアンス	各アプライアンスのスケジュールされたタスクに関する情報が表示されます。
タスク数	左ペインには、個々のタスクが表示されます。タスクのチェックボックスを選択すると、カレンダー（右ペインに表示）が更新され、選択したタスクが表示されます。 右ペインには、タスクのインタラクティブなカレンダービューが表示されます。カレンダー上のタスクをクリックすると、そのタスクに関する追加情報が表示されます。カレンダーを操作するには、以下のオプションを使用します： • : 今日の日付に移動します。カレンダー上の他の日付を探すには、ナビゲーションオプション（、、、、、）を使用します。タスクが関連付けられている日付間をジャンプするには、ナビゲーションオプション（、、、）を使用します。 • ：月別表示に切り替わります。 • ：週単位での表示に切り替えます。 • ：日次表示に切り替えます。

アプライアンスのリソース

このページには、現在ログインしているアプライアンスで使用されているリソースのグラフが表示されます。グラフをマウスオーバーすると、表示されているパーセンテージの追加情報が表示されます。

9.8 Safeguard アクセス

SPP では、SPP へのアクセスに関連する設定を行うことができます。

アクセス設定への移動方法

［アプライアンス管理］＞［Safeguard アクセス］に移動します。

表：SPP アクセス設定

ページ	説明
メッセージング	ログイン通知と本日のメッセージを設定します。
ローカルログイン制御	ユーザーログイン制御設定を行う場所です。
ローカルパスワードルール	ユーザーパスワードの複雑性のルールを設定します。
ID と認証	SPP にログインする際に使用する ID プロバイダと認証プロバイダを設定する場所です。

9.8.1 メッセージング

SPP では、以下の通知を設定することができます。

メッセージングへの移動方法：

［アプライアンス管理］＞［Safeguard アクセス］＞［メッセージング］に移動します。

表：メッセージング設定

設定	説明
ログイン通知	ユーザーが SPP にアクセスする前に確認する必要があるログインバナーを有効にする場所です。このメッセージテキストは匿名で閲覧することができます。
その日のメッセージ	ホームページに表示される「その日のメッセージ」を設定します。これは、認証されたユーザーがログインした後にのみ表示されます。

ログイン通知

ユーザーが SPP にログインしたときに表示されるログイン通知を設定するのは、アプライアンス管理者の責任です。この機能は通常、使用制限、法的合意、ユーザーがシステムにアクセスすることで同意するその他の適切な情報を説明するために使用されます。メッセージテキストは匿名で見ることができることに注意してください。したがって、未認証のユーザーに読まれたくない機密情報は記載しないようにしてください。認証されたユーザーのみが利用できるメッセージについては、「その日のメッセージ」を参照してください。

ログイン通知を設定手順

1. **［アプライアンス管理］＞［Safeguard アクセス］＞［メッセージング］**に移動します。
2. **［ログイン通知］**に入力します。
3. **［保存］**をクリックします。

その日のメッセージ

ホーム画面に表示される今日のメッセージを設定するのは、主にアプライアンス管理者の責任ですが、管理者権限を持つユーザーであれば誰でも今日のメッセージを設定することができます。このメッセージは、認証されたユーザーがログインした後にのみ表示されます。

その日のメッセージの設定手順

> **注**：RSS を選択した場合、フィードは HTTPS である必要があります。RSS サーバーは、CORS ポリシーを有効にする必要があります。

1. **［アプライアンス管理］＞［Safeguard アクセス］＞［メッセージング］**に移動します。
2. **［その日のメッセージ］**で、**「RSS」**または**「件名行」**のいずれかのオプションを選択します。
3. **RSS** オプションを選択した場合は、Web アドレスを入力します。
4. **件名行**オプションを選択した場合は、次の情報を入力します。
    - **件名：** 短い説明を入力します。

- **メッセージ：**最大 255 文字のテキストを入力します。

5. **［保存］**をクリックします。

9.8.2 ローカルログイン制御

アカウントをロックアウトする前に、サインインの失敗回数などのユーザーログイン制御を最初に設定するのは、アプライアンス管理者の責任です。

ログイン制御を設定手順

1. **［アプライアンス管理］＞［Safeguard アクセス］＞［ローカルログイン制御］**に移動します。

2. 次の情報を提供します。一部の設定は、**［ロックアウトウィンドウ］**など、ローカルユーザーのみに適用されます。その他の設定は、**［トークンの有効期間］**など、すべてのユーザータイプに適用されます。

オプション	説明
トークンの有効期間	ユーザーが SPP にログインしたままにしていられる時間（分）を設定します。 範囲：10 分～28,800 分（20 日） デフォルト: 1,440 分（1 日）
Web クライアントの非アクティブタイムアウト	ユーザーがサーバーに最後にリクエストしてから、自動的にログアウトされるまでの最大時間を設定します。デフォルトは 15 分です。この値に合わせて**［トークンの有効期間］**を長くした場合、最小値は 5 分、最大値は 2,880 分（2 日間）となります。**［トークンの有効期間］**を長くしない場合、トークンは**［Web クライアントの非アクティブタイムアウト］**前に失効します。 タイムアウトになると、メッセージが表示され、ユーザーは続行するかログアウトすることができます。応答がない場合、ユーザーは自動的にログアウトされます。デフォルトは 15 分です。

オプション	説明
ロックアウト期間	ロックアウトされたアカウントがロックされたままになる時間を設定します。 範囲は 1～9,999。9,999 を設定した場合は、管理者が手動でアカウントのロックを解除する必要があります。 デフォルトは 15 分です。
ロックアウトしきい値	ユーザーアカウントをロックするために必要な**［ロックアウトウィンドウ］**内での連続したサインイン失敗の回数を設定します。 **［ロックアウトウィンドウ］**内で、アカウントのロックアウトしきい値の設定で指定された最大回数、ユーザーが不正なパスワードを提出した場合、SPP は**［ロックアウト期間］**が経過するまでアカウントをロックします。 範囲は、0～100 回のサインイン失敗。0（ゼロ）は、ログイン失敗によってユーザーのアカウントがロックされることがないことを示します。 デフォルトは、連続 5 回失敗です。**［ロックアウトしきい値］**を十分に高く設定することで、許可されたユーザーがパスワードの入力ミスでユーザーアカウントからロックアウトされることがなくなります。
ロックアウトウィンドウ	SPP がサインインの失敗回数を増加させる期間（分）を設定します。 範囲：0 ～ 15 分。値 0 は、ログオン試行失敗の追跡に時間制限を設けないことを意味します。 デフォルト：10 分
次の期間が経過したら非アクティブ化	非アクティブなユーザーアカウントを自動的に無効にするまでの日数を設定します。 ユーザーがこの日数だけ SPP にログオンしなかった場合、SPP はそのユーザーアカウントを無効にします。 **メモ:** 無効になったアカウントを再度有効にする場合、認証者管理者はユーザーのパスワードもリセットする必要があります。 範囲：14 ～ 365 日。デフォルト: 365 日
パスワードの最小有効期間	ユーザーがパスワードを変更する前に待機しなければならない日数を設定します。

オプション	説明
	範囲：0 ～ 14 日。デフォルト： 0 日
パスワードの最大有効期間	ユーザーが現在のパスワードを変更しなければならないまでに使用できる日数を設定します。 範囲：0 ～ 180 日。値 0 は、パスワードに有効期限がないことを意味します。デフォルト：42 日
パスワード有効期間リマインダー	パスワードの最大有効期間に達し、SPP がパスワードの有効期限が迫っていることをユーザーに通知し始めるまでの期間（日数）を設定します。
パスワード履歴	SPP がユーザーアカウント用に保存している古いパスワードの数を入力します。保存されたパスワードは再利用できず、先入れ先出し方式で交換されます。 **メモ:** 管理者は、パスワード履歴の設定による制限はありません。 範囲を指定します。0 ～ 24 個の古いパスワード。値 0 は、パスワード履歴の制限を無効にし、ユーザーが常に古いパスワードを再利用できるようにします。 デフォルト： 5 つ
ロックされたアカウントをユーザーに通知	このチェックボックスを選択すると、SPP がアカウントをロックしたときに、ユーザーがログインしようとしたときに通知します。オフにすると、SPP はユーザーにアクセスが拒否されたことを通知します。 **メモ：** セキュリティ上の理由から、One Identity では、ログインと認証の問題のトラブルシューティングを行う場合を除き、このオプションをクリアしたままにすることを推奨します。 ロックされたアカウントを持つユーザーは、ロックアウト期間が経過するか、管理者がアカウントのロックを解除するまで、SPP にサインインすることができません。詳細については、「ユーザーのアカウントのロック解除」を参照してください。 デフォルト：オフ

オプション	説明
非アクティブ化されたアカウントをユーザーに通知	このオプションを選択すると、SPP がアカウントを無効にしたときに、ユーザーがログインしようとすると通知されます。クリアすると、SPP はユーザーにアクセスが拒否されたことを通知します。 **メモ:** セキュリティ上の理由から、One Identity では、ログインや認証に関する問題のトラブルシューティングを行う場合を除き、このオプションをクリアしたままにしておくことを推奨しています。 無効化されたユーザーは、管理者がアカウントを再度有効にするまで、SPP にサインインすることができません。詳細については、「ユーザーの有効化または無効化」を参照してください。 デフォルト: オフ
不正なパスワードをユーザーに通知	パスワードが不正な場合にユーザーに通知する場合は、このチェックボックスを選択します。 デフォルト：オフ
失効したパスワードをユーザーに通知	パスワードが期限切れになったときにユーザーに通知する場合は、このチェックボックスを選択します。 デフォルト：オフ
無効なトークンをユーザーに通知	トークンが無効な場合にユーザーに通知する場合は、このチェックボックスを選択します。 デフォルト：オフ
セキュアなトークンサービスログインタイムアウトの有効化	このチェックボックスを選択すると、セッションベースの Cookie の有効期限を 15 分に設定できます。 セッションベースのクッキーは、ログイン時に使用されます。通常、セッションベースの Cookie は有効期限がなく、ブラウザー/ユーザーエージェントが閉じると削除されます。この設定を有効にすると、セッションベースの Cookie は、サーバーによって強制的に 15 分の有効期限を持つようになります。これにより、セキュリティが強化され、一部のリプレイ攻撃を防ぐことができます。エンドユーザーは、多要素認証を含め、この時間内にログインプロセスを完了させる必要があります。

9.8.3 ローカルパスワードルール

パスワードルールは、以下のように SPP へのユーザー認証に必要な複雑さの要件を定義し、ユーザーが作成できるパスワードの種類を管理するルールを作成することができます。

- 許容されるパスワードの長さを 3 ～ 225 文字の範囲で設定する。
- 最初の文字の種類と最後の文字の種類を設定する。
- 大文字、小文字、数字、印刷可能な ASCII 記号を許可し、それぞれの最小数も設定する。
- 除外する大文字、小文字、数字、記号を指定する。
- 連続した文字、数字、記号の繰り返しが可能かどうかを確認し、可能な場合は繰り返しの最大回数を設定する。

メモ: これらのルールはローカルユーザーにのみ適用されます。Microsoft Active Directory などの外部プロバイダから SPP にアクセスするユーザーには適用されません。パスワードルールは、パスワードの設定ダイアログに表示されます。詳細については、「ローカルユーザーのパスワード設定」を参照してください。

ユーザーパスワード要件の変更

ユーザーパスワードルールを設定するのは、アプライアンス管理者の責任です。

ユーザーパスワードルールの設定手順

1. **［アプライアンス管理］＞［Safegaurd アクセス］＞［ローカルパスワードルール］**に移動します。
2. **［ルール概要］**に表示される現在のパスワード要件を確認します。
3. パスワードルールの要件を次のように設定します。
    - **パスワード長**
      パスワードの許容長さを 3 ～ 255 文字の範囲で設定します。デフォルトは 8 文字から 64 文字です。最大長は、次の手順で必要な最小文字数の合計と同じかそれ以上でなければなりません。たとえば、パスワードに大文字 2 文字、小文字 2 文字、数字 2 文字が必要な場合、パスワードの長さの最小値は 6 でなければなりません。なお、発音区分文字は 1 文字とする。

- **最初の文字のタイプ**
  以下のいずれかを選択します。
  - **すべて**：アルファベット、数字、または記号
  - **英数字**：アルファベットまたは数字
  - **アルファベット**： アルファベットのみ
- **最後の文字のタイプ**
  以下のいずれかを選択します。
  - **すべて**：アルファベット、数字、記号
  - **英数字**：アルファベットまたは数字
  - アルファベット：アルファベットのみ
- **繰り返し文字**
  以下のいずれかを選択します。
  - **繰り返される文字を許可**
    任意の文字、数字、記号を、連続を含め、任意の順序で繰り返すことができます。
  - **連続する繰り返し文字はありません**
    文字、数字、記号をそれ自身の後に繰り返すことはできません。大文字、小文字、数字、記号、またはそれらの組み合わせによって、後に連続して繰り返される文字の数を制限することができます。
  - **繰り返し文字はありません**
    すべての文字、数字、記号は、パスワードの中で一度だけ使用することができます。
- **大文字を許可**
  大文字を許可するかどうかを選択します。
  - **最低文字数の大文字が必要です**
    最低限必要な大文字の数を数字で入力します。大文字を許可するが必要としない場合は、この値を 0 に設定します。
  - **連続する繰り返し大文字を制限**
    先に繰り返しを許可した場合、チェックボックスを選択して、連続して繰り返される大文字の数を制限します。**[許可される最大文字数]**の値を 1 以上入力する必要があります。
  - **これらの大文字を除外してください**
    パスワードから除外したい大文字を入力します。このフィールドでは、大文字と小文字が区別されます。

- **小文字を許可**
  小文字を許可するかどうかを選択します。
  - **最低文字数の小文字が必要です**
    小文字を最低限必要とする数を入力します。小文字を許可するが必要としない場合は、この値を 0 に設定します。
  - **連続する繰り返し小文字を制限**
    繰り返し文字を許可した場合、チェックボックスを選択すると、連続して繰り返される小文字の数が制限されます。[許可される最大文字数] に 1 以上の値を入力する必要があります。
  - **[これらの小文字を除外してください]** パスワードから除外したい小文字を入力します。このフィールドでは、大文字と小文字が区別されます。
- **連続する繰り返し小文字を制限**
  小文字と大文字を組み合わせた繰り返しの数を設定するには、**[許可される最大文字数]** を入力します。
  たとえば、**[許可される最大文字数]** に「2」に設定すると、パスワードの中で隣り合うアルファベットは 2 つまでとなります。この例では、Ab1Cd2EF は有効ですが、AbC1d2EF はアルファベットが 3 つ並んでいるため、無効となります。
- **数字（0-9）を許可**
  パスワードに数字を使用することを許可するかどうかを選択します。
  - **最低文字数の数字が必要です**
    パスワードに必要な数字の量を示す数字を入力します。数字を許可するが要求しない場合は、この値を 0 に設定します。
  - **連続する繰り返し数字を制限**
    連続して繰り返される数字の数を制限する場合は、チェックボックスをオンにします。**[許可される最大文字数]** に 1 以上の値を入力する必要があります。
  - **これらの数値文字を除外してください**
    パスワードから除外したい数字を入力します。このフィールドでは、大文字と小文字が区別されます。
- **記号（@ # $ % &など）を許可**
  印刷可能な ASCII 文字を許可する場合は、このチェックボックスをオンにします。これらの文字には、次のようなものがよく含まれます。~ ` ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

- **最低文字数の記号が必要です**
  必要な最小限の記号の数を示す数字を入力します。記号の使用を許可するが、記号を必要としない場合は、この値を 0 に設定します。
- **連続する繰り返し記号を制限**
  チェックボックスを選択すると、連続して繰り返される記号の数が制限されます。**［許可される最大文字数］**に 1 以上の値入力する必要があります。
- 以下を設定します。
  - **有効な記号**
    有効な特殊文字を入力する場合は、このオプションを選択します。**［記号リスト］**テキストボックスに、有効な記号を入力します。
  - **無効な記号**
    このオプションを選択すると、入力が禁止された特殊文字を入力できます。**［記号リスト］**テキストボックスに禁止されている記号を入力します。

4. **［ルールのテスト］**をクリックして、設定したルールを確認します。
5. ルールが完成したら、**［ルールの適用］**をクリックします。

9.8.4 ID と認証

SPP では、既存のディレクトリサービスと統合するために、さまざまなタイプの ID および認証プロバイダを作成することができます。これにより、ユーザーと Safeguard へのログイン方法を効果的に管理することができます。Active Directory、OpenLDAP 2.4、任意の SAML 2.0 連携サービス、または Radius 用のプロバイダを作成することができます。

［アプライアンス管理］＞［Safeguard アクセス］＞［ID と認証］の順に選択します。**［ID と認証］**ペインには、定義されている ID プロバイダと認証プロバイダについて以下の詳細が表示されます。

表：ID と認証：プロパティ

プロパティ	説明
名前	ID または認証プロバイダに割り当てられた名前。名前は、ID または認証プロバイダを作成した管理者によって割り当

プロパティ	説明
	てられます。プロバイダの種類によっては、Active Directory、外部フェデレーション、および任意の 2FA プロバイダを除いて、ログインページのドロップダウンリストに名前が表示される場合があります。
タイプ	ID と認証プロバイダの種類は次のとおりです。有効な一次認証と二次認証の組み合わせがあります。詳細については、「認証プロバイダの組み合わせ」を参照してください。 • Active Directory • LDAP • 外部フェデレーション • Radius（セカンダリ認証プロバイダとして使用） • Radius as Primary（プライマリ認証プロバイダとして使用） • FIDO2 • OneLogin MFA
説明	管理用に使用する任意の説明情報を入力します。

ID および認証プロバイダ設定を管理するには、次のツールバーボタンを使用します。

表：ID と認証：ツールバー

プロパティ	説明
追加	ID または認証プロバイダ構成を追加します。詳細については、「ID と認証プロバイダの追加」を参照してください。
削除	選択した ID または認証プロバイダを削除します。プロバイダは、関連するユーザーが存在しない場合に削除できます。
編集	選択した ID または認証プロバイダを変更します。
今すぐ同期	ディレクトリユーザー（ID プロバイダ）およびディレクトリユーザーグループのディレクトリ追加（インクリメンタル）同期処理を実行します。削除を除くすべての変更が同期されます。タスクウィンドウにタスクの進行状況と結果が表示されます。**［詳細］**をクリックすると詳細情報が表示され、**［停止］**をクリックするとタスクがキャンセルされます。

プロパティ	説明
	ディレクトリの削除と追加（フル）の同期処理は、API（IdentityProviders/Synchronize）から実行する必要があります。
Safeguard フェデレーションメタデータのダウンロード	SPP の Federation Metadata XML ファイルのコピーをダウンロードします。このファイルは、STS サーバーで対応する信頼関係を作成するために必要です。フェデレーションメタデータ XML ファイルには通常、デジタル署名が含まれており、空白を含め、いかなる方法でも変更することはできません。メタデータに問題があるというエラーが表示された場合は、ファイルが編集されていないことを確認してください。
更新	ID および認証プロバイダのリストを更新します。

認証プロバイダの組み合わせ

認証プロバイダの中には、一次認証にのみ使用できるものと、二次認証にのみ対応できるものがあります。許可される認証プロバイダの組み合わせの詳細については、次の表を参照してください。

SPP にログインするときに二要素認証を使用するようにユーザーアカウントを設定するのは、権限許可管理者またはユーザー管理者の責任です。詳細については、「セカンダリ認証ログインの要求」を参照してください。

ID プロバイダとしてローカルを使用する

表：許可されるローカル ID プロバイダの組み合わせ

一次認証	二次認証
ローカル： 指定したログイン名とパスワードまたは SSH キーが認証に使用されます。	なし OneLogin MFA Radius Active Directory LDAP FIDO2

一次認証	二次認証
証明書： 指定された証明書サムプリントが認証に使用されます。	なし OneLogin MFA Radius Active Directory LDAP FIDO2
外部フェデレーション： 指定されたメールアドレスまたは名前クレームが認証に使用されます。	なし OneLogin MFA Radius Active Directory LDAP FIDO2
Radius： 指定されたログイン名が認証に使用されます。 **メモ：**Radius サーバーは、企業の既存の ID および認証ソリューションと統合するように構成され、独自の二要素認証の手段を提供することができます。	なし OneLogin MFA Active Directory LDAP FIDO2

ID プロバイダとして Active Directory を使用する

表：使用可能な Active Directory の ID プロバイダの組み合わせ

一次認証	二次認証
Active Directory： samAccountName または X509 証明書が認証に使用されます。 **メモ：**ユーザーは、自分のアカウントが存在するドメインに対して認証を行う必要があります。	なし OneLogin MFA Radius LDAP FIDO2
外部フェデレーション： 指定されたメールアドレスまたは名前クレームが認証に使用されます。	なし OneLogin MFA Radius Active Directory LDAP FIDO2

一次認証	二次認証
Radius： 指定されたログイン名が認証に使用されます。 **メモ：**Radius サーバーは、企業の既存の ID および認証ソリューションと統合するように構成され、独自の二要素認証の手段を提供することができます。	なし OneLogin MFA Active Directory LDAP FIDO2

ID プロバイダとして LDAP を使用する

表：許可された LDAP ID プロバイダ組み合わせ

一次認証	二次認証
LDAP: 指定されたユーザー名を認証に使用します。	なし OneLogin MFA Radius Active Directory FIDO2
外部フェデレーション： 指定されたメールアドレスまたは名前クレームが認証に使用されます。	なし OneLogin MFA Radius Active Directory LDAP FIDO2
Radius : 指定されたログイン名が認証に使用されます。 **メモ：**Radius サーバーは、企業の既存の ID および認証ソリューションと統合するように構成され、独自の二要素認証の手段を提供することができます。	なし OneLogin MFA Active Directory LDAP FIDO2

ID プロバイダとして Starling を使用する

表：許可された Starling ID プロバイダ組み合わせ

一次認証	二次認証
Starling	なし

ID と認証プロバイダの追加

ID および認証プロバイダとして使用するディレクトリを Safeguard に追加するのは、アプライアンス管理者の責任です。

Active Directory フォレストに複数のドメインがある場合、ID および認証に使用するドメインとログオン画面に表示するドメインを選択します。認証に使用する外部フェデレーションまたは Radius プロバイダを作成するのは、アプライアンス管理者の責任です。

ID および認証プロバイダの追加

1. **［アプライアンス管理］＞［Safeguard アクセス］＞［ID と認証］**に移動します。
2. ＋**［追加］**をクリックします。
3. プロバイダをクリックします。
    - Active Directory：「Active Directory と LDAP の設定」を参照してください。
    - LDAP：「Active Directory と LDAP の設定」を参照してください。
    - 外部フェデレーション：「外部フェデレーション設定」を参照してください。
    - Radius：「RADIUS 設定」を参照してください。
    - FIDO2：「FIDO2 設定」を参照してください。
    - OneLogin MFA：「OneLogin MFA 設定」を参照してください。

Active Directory と LDAP の設定

［全般］タブで、必要なサービスアカウント情報を追加します。次の表は、プロパティの一覧と、該当する場合は Active Directory または LDAP のプロパティを指定したものです。

表：Active Directory と LDAP：全般タブプロパティ

プロパティ	説明
製品	製品名
フォレストルートドメイン名	フォルストルートドメイン名
名前	一意の名前

プロパティ	説明
サービスアカウントのドメイン名（Active Directory の場合）	example.com のような完全修飾された Active Directory ドメイン名を入力します。 server.example.com のようなドメインコントローラーのホスト名、10.10.10.10 のようなドメインコントローラーの IP アドレス、EXAMPLE のような NETBIOS ドメイン名は入力しないでください。 サービスアカウントドメイン名は、サービスアカウントが存在するドメインの名前です。SPP は、DNS-SRV を使用してドメイン名を実際のドメインコントローラーに解決します。
ネットワークアドレス（LDAP）	SPP がネットワークを介して管理対象システムに接続するために使用する、ネットワーク DNS 名または LDAP サーバーの IP アドレスを入力します。
サービスアカウント名（Active Directory 用）	SPP が管理タスクに使用するアカウントを入力します。アカウント名がすでに ID プロバイダにリンクされているアカウント名と一致する場合、プロバイダが自動的に割り当てられます。 パスワードをリリースできるようにする場合は、**「アクセスリクエスト」**をクリックし、詳細ツールバーから**［パスワードリクエストの有効化］**を選択します。セッションアクセスを有効にするには、**「セッションリクエストの有効化」**を選択します。 SPP で管理したいすべてのドメインとアカウントを読取り権限を持つアカウントを追加します。 SPP はフォレストを意識しています。指定したサービスアカウントを使用して、SPP は自動的にフォレスト内のすべてのドメインを検索し、フォレスト全体を表すディレクトリオブジェクトを作成します。ディレクトリオブジェクトは、指定したアカウントに関係なく、フォレストルートドメインと同じ名前になります。 詳細については、「サービスアカウントについて」を参照してください。

プロパティ	説明
サービスアカウントの識別名（LDAP）	SPP が管理タスクに使用する完全修飾識別名 (FQDN) を入力します。例：cn=dev-sa,ou=people,dc=example,dc=com
サービスアカウントのパスワード	SPP がこのディレクトリに認証するために使用するパスワードを入力します。
説明	この外部 ID プロバイダに関する情報を入力します。
接続	**［接続］**をクリックして、資格情報を確認します。Active Directory プロバイダを追加する場合、フォレスト内のすべてのドメインが表示されます。ID と認証に使用できるドメインを選択します。
ID と認証に使用可能なドメイン（Active Directory の場合）	ディレクトリのユーザーグループからインポートされた新規作成されたすべての Safeguard ユーザーのプライマリ認証プロバイダは、そのユーザーのディレクトリドメインを使用するように設定されています。複数のドメインを持つ Active Directory フォレストの場合、ドメインは**「ID と認証に利用可能なドメイン」**としてマークされている必要があります。フォレストルートドメインを消去すると、ディレクトリユーザーとグループを管理する際に望ましくない結果が生じます。詳細については、「ディレクトリユーザーグループの追加」を参照してください。
詳細	以下の同期化設定を表示するために開きます。
ポート（LDAP）	LDAP ディレクトリとの通信に使用するポート 389 を入力します。
SSL 暗号化の使用	LDAP サーバーに接続する際に SSL を使用するかどうかを選択します。有効な SSL 証明書があり、SSL の発行者証明書が SPP によって信頼されている必要があります。詳細については、「信頼できる CA 証明書」を参照してください。
ドメインコントローラー	Active Directory の場合、SPP が DNS および CLDAP の ping からドメインコントローラーを自動的に見つける代わりに、ドメインコントローラーを指定することができます。

プロパティ	説明
追加同期間隔	SPP がディレクトリの追加を同期する頻度（分）を入力または選択します。これにより、SPP にマップされたグループメンバーシップおよびユーザーアカウント属性を含むディレクトリオブジェクトに加えられた追加または修正が SPP に反映されます。 デフォルト: 15 分。範囲： 1 から 2147483647 の間
削除同期間隔	SPP がディレクトリの削除を同期する頻度（分）を入力または選択します。これにより、SPP にマッピングされたグループメンバーシップおよびユーザーアカウント属性を含むディレクトリオブジェクトに対して行われた削除が SPP に更新されます。 既定値: 15 分。範囲 1 から 2147483647 の間

属性タブ

［属性］タブで、SPP の属性をディレクトリスキーマの属性に同期させます。**［属性］**タブには、ユーザーのファーストネームなど、SPP のプロパティにマップされるデフォルトのディレクトリ属性が表示されます。

サポートされている有効なスキーママッピングは複数あり、必要に応じてその設定を変更することができます。たとえば、LDAP ダイアログの**［属性］**タブでは、ディレクトリの構成に応じて、ユーザー名を cn <表示名>または uid <ユーザー名>として表示することができます。

SPP のプロパティを異なるディレクトリ属性にマッピングする手順

1. ユーザー、コンピューター、グループカテゴリに対して、必要に応じて 1 つ以上のオブジェクトクラスを参照し、選択します。

   メモ: デフォルトのオブジェクトクラスを使用または削除することができます。

2. デフォルトのプロパティを使用しない場合は、プロパティボックスへの入力を開始します。SPP のオートコンプリート機能により、選択すべき属性のリストがすぐに表示されます。SPP では、ユーザー、グループ、コンピューターで選択したオブジェクトクラスで有効な属性のみを選択することができます。

3. すべての属性を設定したら、**［適用］**をクリックします。

次の表は、デフォルトのディレクトリ属性の一覧です。

表：Active Directory と LDAP：属性タブ（デフォルト）

SPP 属性	ディレクトリ属性
ユーザー	
ObjectClass	ユーザーオブジェクトクラスの有効な属性を定義するクラス定義を参照して選択します。 デフォルト：Active Directory の場合 user、LDAP の場合 inetOrgPerson
ユーザー名	Active Directory の場合 sAMAccountName、 LDAP の場合 cn
パスワード	LDAP の場合 userPassword
名	givenName
姓	sn
勤務先電話	telephoneNumber
携帯番号	mobile
メール	mail
説明	description
外部フェデレーション	外部フェデレーション認証リクエストの SAML レスポンスからメールアドレスリクエストまたは名前リクエストの値を一致させるために使用されるディレクトリ属性です。通常、これはユーザーのメールアドレス、または外部のセキュアトークンサービス（STS）で使用される他の一意の識別子を含む属性になります。 Active Directory と OpenLDAP 2.4 の両方について、これはデフォルトで "mail" 属性となります。 これは、外部フェデレーションプロバイダを一次認証として使用するように構成されたディレクトリユーザーグループのメンバーを処理する場合にのみ使用されます。 詳細については、「ディレクトリユーザーグループの追加」を参照してください。
Radius 認証	一次認証または二次認証に設定された外部 Radius サーバーのユーザー名と一致させるために使用されるディレクトリ属性です。

SPP 属性	ディレクトリ属性
	Active Directory の場合は、デフォルトで samAccountName 属性を使用します。LDAP 2.4 の場合は、デフォルトで cn 属性が使用されます。 **メモ：**これは、Radius を一次または二次認証プロバイダとして使用するように設定されたディレクトリユーザーグループのメンバーを処理する場合にのみ使用されます。 詳細については、「ディレクトリユーザーグループの追加」を参照してください。
管理対象オブジェクト	既存の管理対象アカウントをディレクトリユーザーグループのユーザーにリンクアカウントとして自動的に関連付ける際に使用されるディレクトリ属性です。 デフォルト： • Active Directory の場合、このデフォルトは managedObjects です。ただし、Active Directory のどこに情報が保存されているかによって、directReports 属性を使用する場合もあります。 • LDAP 2.4 の場合、デフォルトは seeAlso 属性です。 属性を選択する際には、その属性はユーザー自身に存在し、他のディレクトリユーザーオブジェクトの識別名値を 1 つ以上含んでいる必要があります。たとえば、LDAP 2.4 の owner 属性はリレーションシップの方向が正しくないので使用したくありません。代わりに、デフォルトの seeAlso 属性のような owner 属性を指定します。 詳細は、「ディレクトリユーザーグループの追加」を参照ください。
グループ	
ObjectClass	グループオブジェクトクラスの有効な属性を定義するクラス定義を参照して選択します。 デフォルト：Active Directory の場合は group、LDAP の場合は groupOfNames

SPP 属性	ディレクトリ属性
名前	Active Directory の場合は sAMAccountName、LDAP の場合は cn
メンバー	member
説明	description

外部フェデレーション設定

SPP は SAML 2.0 Web Browser SSO Profile をサポートしており、Microsoft の AD FS など、さまざまな STS サーバーやサービスとのフェデレーション認証を設定することが可能です。フェデレーションメタデータの交換を通じて、2 つのシステム間に信頼関係を構築することができます。次に、SPP のユーザーアカウントを作成し、連携アカウントと関連付けます。エンドユーザーがログインすると、外部 STS にリダイレクトされ、資格情報を入力し、STS で必要とされる二要素認証を実行します。認証に成功すると、SPP にリダイレクトされ、ログインされます。

> **メモ:** 外部 STS からリダイレクトされた後に再度認証を行うよう、関連する SPP のユーザーアカウントに追加の二要素認証を割り当てることができます。

外部フェデレーションを使用するには、まず STS のフェデレーションメタデータ XML をダウンロードし、ファイルに保存しておく必要があります。例えば、Microsoft の AD FS の場合、フェデレーションメタデータ XML は以下からダウンロードすることができます。

https://<adfs server>/FederationMetadata/2007-06/FederationMetadata.xml

外部フェデレーションの追加手順

1. **［外部フェデレーション］**ダイアログで、以下の情報を入力します。
    a. **名前**： 外部フェデレーションサービスプロバイダに割り当てられた一意の名前。この名前は管理目的でのみ使用され、エンドユーザーには表示されません。
    b. **説明**：任意のテキストを入力します。このテキストはここだけに表示され、管理目的に使用されます。
    c. **領域**：この STS を認証に使用するユーザーのメールアドレスに一致する一意のレルム値（通常は contoso.com などの DNS サフィックス）を入力します。値は、スペース、カンマ、セミコロンで区切ることができます。ホー

ム領域検出を実行する際には、大文字と小文字を区別しない比較が行われます。ワイルドカートは使用できません。上限は 255 文字です。

d. **フェデレーションメタデータファイル**：**[参照]**をクリックして、STS フェデレーションメタデータ xml ファイルを選択します。

e. **Require User to Always Authenticate**：チェックボックスを選択すると、ユーザーはすでにログインしているかどうかにかかわらず、外部プロバイダで常に資格情報の入力が必要になります。

2. **Safeguard フェデレーションメタデータのダウンロード**をクリックします。このファイルは、STS サーバーに対応する信頼関係を作成するために必要です。フェデレーションメタデータ XML ファイルは通常、デジタル署名を含んでおり、空白を含め、いかなる方法でも変更することはできません。メタデータに問題があるというエラーが表示された場合は、ファイルが編集されていないことを確認してください。「STS 証明書利用者信頼（Relying Party Trust）の作成方法は？」を参照してください。

RADIUS 設定

プライマリ認証プロバイダまたはセカンダリ認証プロバイダとして使用するための Radius サーバーを作成し、設定します。Radius サーバーをプライマリ認証とセカンダリ認証の両方に使用するには、2 つの認証プロバイダを作成する必要があります。Radius をプライマリプロバイダまたはセカンダリプロバイダとして作成する手順は次のとおりです。

1. **RADIUS** ダイアログで、次の情報を入力します。

   a. **名前**：一意の表示名。一次認証用の Radius プロバイダを作成すると、この名前の値がログインページのドロップダウンリストに表示されます。

   b. **説明：**任意のテキストを入力します。このテキストはここだけに表示され、管理目的に使用されます。

   c. **タイプ**：**[プライマリ認証として]**または**[セカンダリ認証として]**を選択します。

   d. **サーバーアドレス**：ネットワーク DNS 名、またはネットワーク経由でサーバーに接続するために使用する IP アドレスを入力します。

   e. **セカンダリーサーバーアドレス**：（任意）追加または冗長サーバーのネットワーク DNS 名または IP アドレスを入力します。

f. **共有シークレット**：サーバーのシークレットキーを入力します。👁をクリックすると、サーバーの秘密鍵が表示されます。

g. **ポート**：Radius サーバーが認証要求をリッスンするために使用するポート番号を入力します。デフォルトはポート 1812 です。

h. **タイムアウト**。Radius 認証要求がタイムアウトするまでの待ち時間を指定します。デフォルトは 20 秒です。

i. **チャレンジ／レスポンスの事前認証：**選択した場合、ユーザー認証を試みる前に、ユーザー名のみを含む Access-Request コールが Radius サーバーに送信されます。これは、Radius サーバーにユーザーの ID を通知し、チャレンジ/レスポンスサイクルを開始することで認証プロセスを開始できるようにするためのものです。これは、ユーザーの状態データのシードを作成するために必要な場合があります。さらに、Radius サーバーの応答には、そのユーザーに固有の表示すべきログインメッセージが含まれる場合があります。

   Radius サーバーが Access-Challenge で応答するように設定されていない場合、ログインに失敗し、ユーザーは処理を続行できなくなります。この設定は、Radius を二次認証プロバイダとして使用する場合にのみ適用されます。一次認証プロバイダでこの設定を有効にしても、効果はありません。

j. **ユーザー入力を常にマスク**：この設定を選択すると、ユーザーがワンタイムパスワードや Radius サーバーが要求するその他のチャレンジを入力するテキストボックスは、常にパスワード形式のテキストボックスになり、ユーザーの入力はマスクされてクリアテキストではなく、一連のドットとして表示されます。これは、チャレンジがワンタイムパスワードであるだけでなく、ユーザーの PIN を含む場合にも望まれるかもしれません。これにより、通行人が個人情報を見ることを防ぐことができます。ただし、この設定を有効にすると、Radius サーバーの Access-Challenge レスポンスの Prompt 属性が上書きされ、ユーザーの入力は常にマスクされることに注意してください。

k. **説明**：任意のテキストを入力します。このテキストはここでしか表示されません。管理目的に使用されます。

2. **［OK］**をクリックします。

メモ：SPP が Radius サーバーに対してユーザー認証を試みる場合、常に NAS-Identifier Radius 属性にアプライアンス ID が設定された値が含まれます。これをオンまたはオフにしたり、カスタム値を指定したりする設定はありません。

FIDO2 設定

セカンダリ認証プロバイダとして使用するために、FIDO2 を作成し、設定します。

1. **FIDO2** ダイアログで、以下の設定を行います。

    a. **名前**：プロバイダに割り当てられる一意の名前。この名前は管理目的でのみ使用され、エンドユーザーには表示されません。

    b. **ドメインサフィックス**： これは、アプライアンスを識別する DNS 名である必要があります。通常、これは Safeguard にアクセスするために使用される DNS 名になります。IP アドレスは使用できません。値は、登録または認証式が実行される WebAuthn Relying Party を識別するドメイン文字列です。

    public key credential（公開鍵クレデンシャル）は、登録されたのと同じエンティティ（この値で識別）との認証にのみ使用できます。ただし、この値は、登録時にユーザーのブラウザーに表示されるものの、登録可能なドメインサフィックスにすることができます。たとえば、https://www.contoso.com または https://node1.contoso.com にあるサーバーに対して登録するために contoso.com と入力することができます。後で、同じ認証者セキュリティキーを使用して、どちらの場所でも認証することができます。

    c. **説明：**任意のテキストを入力します。このテキストはここでしか表示されず、管理目的に使用されます。

2. **［OK］**をクリックします。

OneLogin MFA 設定

セカンダリ認証プロバイダとして OneLogin MFA を作成および構成します。

> **重要**: OneLogin 認証プロバイダとして構成する前に、まず OneLogin.com でサブスクリプションを購入し、SPP で使用される API クレデンシャルを作成する必要があります。OneLogin の詳細については、「OneLogin ドキュメント」を参照してください。

メモ: OneLogin 管理サイトは、必要な認証要素、セキュリティポリシー、ユーザーを構成するために使用します。ＳＰＰは現在、以下の二次認証方式をサポートしています：

- OneLogin Protect
- Authenticator
- SMS
- Email

1. OneLogin MFA ダイアログで、以下の設定を行います。

    a. **名前**：プロバイダに割り当てられた固有の名前。この名前は管理目的のみで、エンドユーザーには表示されません（最大 50 文字）。

    b. **説明**：任意のテキストを入力します。このテキストはここでのみ表示され、管理目的に使用されます（最大 255 文字）。

    c. **DNS Host Name**：サブスクリプションの完全な OneLogin DNS ホスト名を入力します。例：<subdomain>.onelogin.com

    d. **Client ID**：OneLogin で作成した API クライアント ID を入力します。SPP では、OneLogin で作成した API クレデンシャルに **Manage All** 権限が使用されていることが必要です。詳細については、「Working with API Credentials」を参照してください。

    e. **クライアントシークレット**：OneLogin で作成した API クライアントシークレットを入力します。特権パスワードの保護には、OneLogin で作成された API クレデンシャルに **Manage All** 権限が使用されていることが必要です。詳細については、「Working with API Credentials」を参照してください。

2. **［OK］**をクリックします。

メモ： OneLogin MFA を認証プロバイダとして構成した後、個々のユーザーを SPP に追加する場合、そのユーザーに対して構成したメールアドレスが OneLogin にあるものと同一であることを確認する必要があります。初期設定後、必要に応じて OneLogin のユーザー情報を更新しても、SPP との接続に影響を与えることはありません。

9.9　アプライアンス管理設定

アプライアンス管理には、プラットフォームタスクの最大再試行回数を管理するための設定ページがあります。

［アプライアンス管理］＞［設定］で以下を設定できます。

表：プラットフォームタスク設定

設定	説明
最大プラットフォームタスク再試行数	プラットフォームの最大再試行回数を設定します。

10 資産管理

Web クライアントで、左側のナビゲーションペインにある**［資産管理］**セクションを展開します。

10.1 Account Automation（アカウントの自動化）

ホームページのペインとしても利用できる**［資産管理］＞［Account Automation］**ページでは、資産管理者が異なるタイプのタスクに失敗または成功したアカウントに関する情報を見ることができます。このページでは、自動タスクと手動タスクの両方の結果が含まれます。ビューでタスクの 1 つをクリックすると、追加情報が表示されます。

アカウントの自動化 種類

デフォルトでは、以下のアカウント自動化タスクの情報が表示されます。⚙ボタンをクリックすると、表示されるタスクがカスタマイズされます。

- **パスワードの確認失敗**：パスワードの確認タスクが失敗したアカウントの一覧が表示されます。
- **パスワードの変更失敗**：パスワードの変更に失敗したアカウントの一覧が表示されます。
- **SSH キーのチェック失敗**：SSH キーの確認に失敗したアカウントの一覧が表示されます。
- **SSH キーの変更失敗**： SSH キーの変更タスクが失敗したアカウントの一覧が表示されます。
- **SSH キーの検出失敗**：SSH キーの検出タスクが失敗したアカウントの一覧が表示されます。
- **SSH Key Revoke Failures**（SSH キーの失効失敗）：SSH キーの取り消しタスクが失敗したアカウントの一覧が表示されます。
- **Suspend Account Failures**（アカウントの一時停止失敗）：一時停止タスクが失敗したアカウントの一覧が表示されます。
- **Restore Account Failures**（アカウントの復元失敗）：復元タスクが失敗したアカウントのリストが表示されます。

- **Password Check Successes**（パスワード確認の成功）：過去 24 時間にパスワード確認が成功したアカウントの一覧が表示されます。
- **Password Change Successes**（パスワードの変更に成功）：過去 24 時間にパスワード変更タスクが成功したアカウントの一覧が表示されます。
- **SSH Key Check Successes**（SSH キー確認の成功）:過去 24 時間に SSH キーの確認タスクが成功したアカウントの一覧が表示されます。
- **SSH Key Change Successes**（SSH キー変更の成功）：過去 24 時間に SSH キーの変更タスクが成功したアカウントの一覧が表示されます。
- **SSH Key Discovery Successes**（SSH キー検出の成功）：過去 24 時間に SSH キーの検出タスクが成功したアカウントの一覧が表示されます。
- **SSH Key Revoke Successes**（SSH キーの失効成功）：過去 24 時間に SSH キーの取り消しタスクが成功したアカウントの一覧が表示されます。

アカウントの自動化：ツールバー

タスクを選択して追加情報を表示した後、詳細グリッドの上部にあるツールバーを使用して、次のタスクを実行します。

- **詳細の表示：**表からタスクを選択した後、このボタンをクリックすると、タスクの追加情報が表示されます。
- **Re-Run Task（タスクの再実行）**：失敗したタスクにのみ有効で、選択したタスクを再実行する場合に選択します。
- **エクスポート**：現在表示されている Account Automation（アカウントの自動化）グリッドの.csv または.json ファイルを作成し、任意の場所に保存する場合に選択します。詳細については、「データのエクスポート」を参照してください。
- **更新**：表に表示されているデータを更新する場合に選択します。
- **列**：グリッドに表示可能な列のリストを表示する場合に選択します。グリッドに含めるデータのチェックボックスを選択し、グリッドから除外するデータのチェックボックスをオフにします。

10.2 アカウント

SPP のアカウントは、SPP が資産へのアクセスを制御するために使用する一意の識別子です。管理された（ディレクトリアカウントとサービスアカウントを含む）アカウントとアカウントグル

ープは、資産に関連付けることができます。各アカウントには関連する資産があり、資産を削除すると、SPP はそれに関連するすべてのアカウントを永久に削除します。

監査人と資産管理者は、**アカウント**にアクセスする権限を持っています。

Unix 資産では、アカウントは etc/passwd に保存されますが、プラットフォームごとにこのコンセプトの実装が異なります。

サービスアカウントは、**サービスアカウント**アイコンで指定されます。詳細については、「サービスアカウントについて」を参照してください。

アカウントへのアクセス

［資産管理］＞［アカウント］に移動します。必要に応じて、パーティションのドロップダウンを使用して、アカウントの親パーティションを選択できます。アカウントを選択し、クリックすると、追加情報とオプションが表示されます。

アカウントをダブルクリックすると、以下の情報が表示されます：

- **プロパティ**：選択したアカウントに関する一般的な情報が表示されます。
- **所有者**：アカウントの所有者に関する情報が表示されます。
- **依存資産**（ディレクトリ資産）：選択されたディレクトリアカウントに依存する資産が表示されます。このタブは、ディレクトリ資産に対してのみ表示され、選択したディレクトリアカウントに依存関係がある資産が表示されます。
- **確認と変更の記録**：選択したアカウントのパスワードと SSH キーの検証およびリセットの履歴が表示されます。
- **SSH キーが検出されました**：アカウントで検出された SSH キーが表示されます。
- **履歴**：選択したアカウントに影響を与えた各操作の詳細が表示されます。

SPP でアカウント検出を構成する方法については、「アカウント検出ジョブワークフロー」を参照してください。

アカウントを管理するには、次のツールバーボタンを使用します。

- **新しいアカウント**：SPP にアカウントを追加します。詳細については、「アカウントの追加」を参照してください。
- **削除：**選択したアカウントを削除します。詳細については、「アカウントの削除」を参照してください。
- **詳細の表示**：アカウントを選択し、このボタンをクリックすると、そのアカウントの追加情報およびオプションが表示されます。
- **アカウントセキュリティ**：メニューオプションは以下の通りです。

- **パスワードの確認**、**パスワードの変更**、**パスワードの設定**。詳細については、「アカウントパスワードの確認、変更、設定」を参照してください。
- **SSH キーのチェック**、**SSH キーの変更**、**SSH キーを表示または設定**。詳細については、「SSH キーの確認、変更、設定」を参照してください。
- **SSH キーのアーカイブ**：詳細は、「SSH キーアーカイブの表示」を参照してください。

- **アクセスリクエスト**：選択したアカウントに対して、アクセスリクエストサービスを有効または無効にすることができます。メニューオプションは次のとおりです。
  - パスワードリクエストの有効化
  - パスワードリクエストの無効化
  - セッションリクエストの有効化
  - セッションリクエストの無効化
  - SSH キーリクエストの有効化
  - SSH キーのリクエストの無効化

- **SSH キーの検出**：SSH キー検出ジョブを実行します。
- **無効化済みの表示**：管理されておらず無効化されていて関連する資産がないアカウントが表示されます。
  - **無効化** をクリックすると、選択したアカウントを SPP で管理しないようにします。
  - **有効化**をクリックすると、選択したアカウントが管理され、デフォルトプロファイルのスコープに割り当てられます。
- **無効化済みの非表示**：管理されておらず無効化されていて関連する資産がないアカウントが非表示にされます。
  - **無効化** をクリックすると、選択したアカウントを SPP で管理しないようにします。
  - **有効化** をクリックすると、選択したアカウントが管理され、デフォルトプロファイルのスコープに割り当てられます。
- **エクスポート**：このボタンを使用して、リストされたデータを JSON ファイルまたは CSV ファイルのいずれかにエクスポートします。詳細については、「データのエクスポート」を参照してください。
- **更新**：アカウントの一覧を更新します。
- **検索**：文字列、または選択した属性から、条件を入力して検索することができます。選択した属性で検索するには、**［検索］**をクリックし、検索する属性を選択します。詳しくは、「検索ボックス」をご覧ください。

10.2.1 プロパティ

プロパティタブには、選択したアカウントに関する情報が表示されます。

プロパティへのアクセス

［資産管理］＞［アカウント］＞（詳細の表示）**＞［プロパティ］**を開きます。

アカウントの情報が表示されます。以下の情報は、すべてのアカウントに適用されるわけではありません。

プロパティタブの上部には、2 つのボタンがあります：

- **アカウントセキュリティ**：メニュー オプションは次のとおりです。
    - パスワードの確認、パスワードの変更、パスワードの設定、SSH キーのチェック、SSH キーの変更、SSH キーの表示または設定。詳細については、「アカウントパスワードの確認、変更、設定」および「SSH キーの確認、変更、設定」を参照してください。
    - パスワードのアーカイブ
    - SSH キーのアーカイブ
- **SSH キーの検出**：このオプションを使用して、選択した SSH キーの検出ジョブを実行します。
- **有効化/無効化**：次のいずれかを選択します。
    - **有効化** を選択すると、SPP は無効な資産を管理します。アカウント検出ジョブは、過去に有効または無効とマークされているかどうかに関係なく、検出ルールの基準に一致するすべてのアカウントを見つけます。

      選択した資産を SPP が管理しないようにするには、**無効化** を選択します。資産を無効にすると、SPP はその資産を無効にし、関連するアカウントをすべて削除します。後で資産を管理することを選択した場合、SPP は関連するすべてのアカウントを再び有効にします。

以下のフィールドは、資産の種類（たとえば、Windows、Linux、LDAP、Active Directory）に基づいて、**［プロパティ］**タブのセカンダリタブに表示されます。セカンダリタブの 1 つで **［編集］**ボタンをクリックすると、アカウントを編集することができます。

表：アカウントのプロパティタブ：一般的なプロパティ

プロパティ	説明
名前	選択されたアカウントの名前

プロパティ	説明
説明	選択されたアカウントの説明
資産	このアカウントに関連付けられた管理対象システムの表示名。アカウントは 1 つの資産にのみ関連付けられます。

表：アカウントプロパティ：管理プロパティ

プロパティ	説明
アクセスリクエスト	このアカウントで有効になっているアクセスリクエストの種類を示します。
パスワードプロファイル	パーティションに割り当てられたアカウントに適用されるパスワードプロファイルの名前。 パスワードプロファイルが資産またはパーティションから継承されている場合、パスワードプロファイルの名前の横に「(継承済み)」と表示されます。 パスワードプロファイルが明示的に設定されている場合、✕ボタンが表示され、明示的に設定されたパスワードプロファイルをクリアして、代わりに継承されたパスワードプロファイルを使用することができます。
SSH キープロファイル	SSH キープロファイルの名前。 SSH キープロファイルが資産またはパーティションから継承されている場合、SSH キープロファイルの名前の横に「(継承済み)」と表示されます。 SSH キープロファイルが明示的に設定されている場合、明示的に設定された SSH キープロファイルをクリアするための✕ボタンが表示されます。クリアされたプロファイルの変更が適用されると、割り当てられた継承されたプロファイルが表示されます。パーティションに指定された既定のSSHキープロファイルがない場合、その資産には SSH キープロファイルが割り当てられなくなります。資産に明示的に設定された SSH キープロファイルがない場合、その資産上のアカウントに SSH キープロファイルが割り当てられなくなります。パーティションに既定の SSH キープロファイルを指定すると、そのパーティション内のすべての資産とアカウントに SSH キープロファイルが継承されるようになります。

タグ：選択したアカウントに割り当てられたタグ

［タグ］ペインに表示される情報には、タグ付けルールによって追加された動的タグと、手動で追加された静的タグの両方が含まれます。タグの割り当てを表示するだけでなく、資産管理者は、静的に割り当てられたタグを追加および削除することができます。

削除： 選択したアカウントを削除するには、このボタンをクリックします。

10.2.2 所有者タブ

所有者タブには、アカウント（および関連する資産）に関連付けられた**［所有者］**に関する情報が表示されます。タグを介して割り当てられた所有者の変更については、「資産または資産アカウントのタグの変更」を参照してください。

所有者にアクセスする手順

［資産管理］＞［アカウント］＞（詳細表示）**＞［所有者］**に移動します。

所有者タブには「アカウント所有者」、「資産所有者」、「パーティション所有者」の 3 つのビューがあります。

表：アカウント：所有者タブプロパティ

プロパティ	説明
アカウント所有者	
タイプ	所有者のタイプ
名前	所有者の名前
プロバイダ	認証プロバイダの名前
直接	この列は、オブジェクトの所有権がタグではなく、直接割り当てられたことを示します。
タグを使用	この列は、オブジェクトの所有権が、タグを使用して割り当てられたことを示します。
資産所有者	
タイプ	所有者のタイプ
名前	所有者の名前

プロパティ	説明
プロバイダ	認証プロバイダの名前
直接	この列は、オブジェクトの所有権がタグではなく、直接割り当てられたことを示します。
タグを使用	この列は、オブジェクトの所有権が、タグを使用して割り当てられたことを示します。
パーティション所有者	
タイプ	ユーザーまたはグループのタイプ
名前	ユーザーまたはグループの名前
プロバイダ	認証プロバイダの名前

詳細ツールバーの以下のボタンを使用して選択したアカウントが所有するオブジェクトを管理します。

表：アカウント：所有者ツールバー

プロパティ	説明
＋ 追加	選択したアカウントに、1 人または複数のユーザーまたはユーザーグループを追加します。詳しくは、「アカウントへのユーザーまたはユーザーグループの追加」を参照してください。
ー 削除	選択したオブジェクトを、選択したアカウントのマネージャーから削除します。アカウントに直接割り当てられたオブジェクトのみを削除することができます（タグを使用して割り当てられたオブジェクトとは異なります）。
エクスポート	このボタンを使って、リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートします。詳細については、「データのエクスポート」を参照してください。
更新	所有者／管理者のリストを更新します。
検索	このリストの中から特定のオブジェクトを見つけるには、一致するものを検索するために使用する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

10.2.3 依存資産

依存資産タブは、ディレクトリアカウントに対してのみ表示され、選択したディレクトリアカウントに依存する資産が表示されます。詳細については、「アカウントの依存関係を追加」を参照してください。

依存資産へのアクセス

［資産管理］＞［アカウント］＞（詳細の表示）＞［依存資産］に移動します。

表：アカウント： 依存資産タブのプロパティ

プロパティ	説明
名前	選択されたアカウントの名前
ネットワークアドレス	管理対象システムのネットワーク DNS 名または IP アドレス
プラットフォーム	選択した管理対象システムのプラットフォーム
資産パーティション	Windows 資産に割り当てられたパーティション

詳細ツールバーのボタンを使用して、依存する資産を管理します。

表：アカウント： アクセスリクエストポリシータブプロパティ

オプション	説明
更新	選択したアカウントに割り当てられている依存資産のリストを更新します。
検索	このリストから特定の依存資産の場所を見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.2.4 確認と変更の記録タブ

確認と変更の記録タブには、選択したアカウントのパスワードと SSH キーの検証およびリセットの履歴が表示されます。

デフォルトでは、表示される確認と変更ログのエントリは、過去 24 時間分です。Web クライアントでは、**［日付範囲］**ドロップダウンを使用して表示する時間枠を選択し、**［エクスポ**

ート】を使用して表示されたデータを JSON または CSV ファイルとしてエクスポートします（詳細については、「データのエクスポート」を参照してください）。別の時間間隔を選択しても表示が更新されない場合は、**［更新］**をクリックします。

確認と変更ログへのアクセス

［資産管理］>**［アカウント］**>（詳細の表示）>**［確認と変更の記録］**に移動します。

表：アカウント：確認と変更の記録タブのプロパティ

プロパティ	説明
ユーザー	イベントを発生させたユーザーの表示名
状態	トランザクションのステータス • 失敗 • 成功 • キュー
理由	パスワードと SSH キーの検証およびリセット操作に関連するシステムメッセージ
タイプ	トランザクションのタイプ： • パスワードの確認 • パスワードの変更 • SSH キーの確認 • SSH キーの変更 **メモ：確認と変更の記録**は、アプライアンスが実行するイベントのみを表示します。つまり、確認と変更トランザクションのみを表示します。つまり、チェックと変更のトランザクションのみが表示されます。次を参照してください： • アカウントパスワードの確認、変更、設定 • SSH キーの確認、変更、設定
日付/時間	トランザクションの日付です。トランザクションのタイムスタンプは、ユーザーのローカルタイムに基づきます。
期間	トランザクションが完了するまでにかかった時間です。

10.2.5 SSH キーが検出されました

SSH キーが検出されましたタブには、アカウントで検出された SSH キーが表示されます。

SSH キーが検出されましたタブへのアクセス

［資産管理］＞［アカウント］＞（詳細の表示）**＞［SSH キーが検出されました］**に移動します。

表：アカウント：SSH キーが検出されましたタブのプロパティ

プロパティ	説明
フィンガープリント	認証に使用される SSH キーのフィンガープリント
アカウントステータス	Safeguard アカウントのステータス
SSH キーが管理されています	この列には、現在アカウントで使用されている SSH キーにチェックマークが付きます。
コメント	フリーフォームのコメント
キータイプ	RSA や DSA などの SSH キーの ID タイプ。詳しくは、「SSH キープロファイル」を参照してください。
キー長	サポートされている RSA または DSA のキー長
資産名	アカウントに関連付けられた資産の名前
アカウント	SSH キーが検出されたアカウントの名前
日付/時間が検出されました	SSH キーが検出された日付/時間

詳細ツールバーで次のボタンを使用します。

表：アカウント：SSH キーが検出されましたタブプロパティ

オプション	説明
▶ **SSH キーの検出**	選択した SSH キー検出ジョブを実行します。進行状況と完了を表示するタスクポップアップが表示されます。 このボタンは、プロファイル（スケジュールを持つもの）を含む設定が完了したときに有効になります。詳しくは、

オプション	説明
	「SSH キープロファイルタブ」タブ（パーティション）を参照してください。
取り消し	管理されていない SSH キーのアクセスを取り消すには、このボタンを使用します。
更新	選択したアカウントに割り当てられている依存資産のリストを更新します。
検索	このリストから特定の依存資産の場所を見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.2.6 履歴タブ

履歴タブでは、選択したアカウントに影響を与えた各操作の詳細を表示したり、エクスポートしたりすることができます。

履歴へのアクセス

［資産管理］>**［アカウント］**> （詳細の表示）>**［履歴］**に移動します。

履歴タブの上部には、次の情報が表示されます。

- **日付範囲**：既定では、履歴の詳細は過去 24 時間について表示されます。ドロップダウンから、時間間隔の一つを選択すると、その時間枠の履歴の詳細が表示されます。
- **エクスポート**：このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
- **更新**：表示されているリストを更新します。
- **検索**：詳細は、「検索ボックス」を参照してください。

表：アカウント：履歴タブのプロパティ

プロパティ	説明
日付/時間	イベントの日付と時刻

プロパティ	説明
ユーザー	イベントをトリガーしたユーザーの表示名
ソース IP	イベントをトリガーした管理システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択したアカウントの名前
イベント	選択したアカウントに対して行われた操作の種類。 • 作成 • 削除 • 更新 • メンバーシップの登録 • メンバーシップの削除 **メモ：**メンバーシップ操作は、選択したアカウントがアカウントグループのメンバーシップに追加された、または削除されたなど、関連または親オブジェクトとの関係の変更を示します。
関連オブジェクト	関連オブジェクトの名前
関連オブジェクトタイプ	関連オブジェクトのタイプ
親	選択されたアカウントが子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

10.2.7 アカウントの管理

アカウントページのコントロールとタブページを使用して、SPP アカウントを管理するための以下のタスクを実行します。

- アカウントの追加
- クラウドプラットフォームアカウントの追加
- アカウントへのタグの手動追加
- アカウントの削除
- アカウントへのユーザーまたはユーザーグループの追加
- アカウントパスワードの確認、変更、設定

- パスワードアーカイブの表示
- SSH キーの確認、変更、設定
- SSH キーアーカイブの表示

アカウントの追加

SPP に資産とアカウントを追加するのは、資産管理者の責任です。1 つの資産に複数のアカウントを持つことはできますが、1 つのアカウントは 1 つの資産にしか関連付けることができません。

新しいアカウントは、**アカウント**リストに表示されます。

> **メモ:** SPP では、自動的に実行されるアカウント検出ジョブを設定することができます。詳細については、アカウント検出ジョブのワークフローを参照してください。

アカウントの追加手順

1. **［資産管理］＞［アカウント］**に移動します。
2. ツールバーの ＋ **［新しいアカウント］**をクリックします。
3. **［新しいアカウントの資産を選択］**ダイアログで、このアカウントに関連付ける資産を選択し、**［資産の選択］**をクリックします。
4. **［新しいアカウント］**ダイアログで、以下の情報を入力します。
    - **全般**タブ
        - **名前**
            - **ローカルアカウント**：このアカウントのログインユーザー名を入力します。制限：100 文字
            - **ディレクトリアカウント**：アカウントを検索するために参照します。
        - **説明**：（任意）この管理アカウントに関する情報を入力します。制限：255 文字
    - **管理**タブ
        - **パスワードリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してパスワードリリースリクエストが有効であることを示しています。このオプショ

ンをオフにすると、誰かがこのアカウントのパスワードをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは許可されたユーザーである資格の範囲内で、任意のアカウントのパスワードをリクエストできます。

- **セッションリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してセッションアクセスリクエストが有効であることを示します。このオプションをオフにすると、誰かがこのアカウントを使用してセッションアクセスをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは、許可されたユーザーである資格の範囲内で、任意のアカウントに対してアクセスリクエストを行うことができます。
- **SSH キーリクエストの有効化：**このチェックボックスはデフォルトで選択されており、このアカウントに対して SSH キーのリリースリクエストが有効であることを示します。このオプションをオフにすると、誰かがこのアカウントの SSH キーをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは自分が承認されたユーザーである権限の範囲内で、任意のアカウントの SSH キーをリクエストすることができます。
- **パスワードプロファイル**および **SSH キープロファイル：**このアカウントを管理するためのプロファイルを**［参照］**して選択します。

  デフォルトでは、アカウントはその関連付けられた資産のプロファイルを継承しますが、このパーティションに対して別のプロファイルを割り当てることができます。詳細については、「パスワードプロファイルと SSH キープロファイルに資産またはアカウントを割り当て」を参照してください。
- **すべてのパーティションで使用可能**（グローバルアクセス）（一部の種類のディレクトリアカウントでのみ使用可能）：選択すると、どのパーティションでもこのアカウントを使用することができ、パスワードは他の管理者に渡されます。例えば、このアカウントは、他の資産の依存アカウントやサービスアカウントとして使用することができます。潜在的には、このアカウントでサービスを実行している資産があり、サービスアカウントが変更されたときに、それらの資産を更新することができるかもしれません。選択しない場合、パーティション所有者や他のパーティションは、そのアカウントの存在を知ることはありません。アーカイブサーバーはパーティションに拘束されませんが、アーカイブサーバーの

ディレクトリアカウントを設定するには、このオプションが選択されている必要があります。

5. **［OK］**をクリックします。

クラウドプラットフォームアカウントの追加

SPP は、Amazon Web Services (AWS)などのクラウドプラットフォームアカウントを管理することができます。

クラウドプラットフォームアカウントを SPP に追加する前に、まずアカウントを関連付ける資産を追加する必要があります。詳細については、「Amazon Web Services プラットフォームの準備」を参照してください。

クラウドプラットフォームアカウントの追加手順

1. **［資産管理］＞［資産］**に移動します。
2. **［資産］**で、ツールバーの ＋ **［新しい資産］**をクリックします。
3. **［全般］**タブ：
    a. **名前**：すべてのクラウドプラットフォームアカウントを管理するために使用できる「クラウドアカウントサーバー」など、意味のある資産名を入力します。
    b. （任意）**説明**：資産の説明を入力します。
4. **パーティション**タブ
    a. **プラットフォーム**：**Amazon Web Services** など、適切な製品を選択します。
    b. **バージョン**：**Amazon Web Services** の場合、バージョンを選択します。
    c. **アーキテクチャ：**製品のシステムアーキテクチャを入力します。
    d. **ネットワークアドレス**：**Amazon Web Services** の場合、AWS IAM ユーザーのビューにある AWS アカウント ID またはエイリアスを入力します。
    e. **認証タイプ：**以下のいずれかを選択します：
        i. **アクセスキー**を使用して資産に認証するためのアクセスキー。以下の情報を入力します：

- **サービスアカウント名**：設定した IAM サービスアカウントを入力します。
- **アクセスキーID**：IAM サービスアカウント用に作成したアクセスキーID を入力します。
- **シークレットキー**：IAM サービスアカウント用に作成したシークレットキーを入力します。

ii. 資産を認証せず、手動で管理する場合は**［なし］**を選択します。

5. **［OK］**をクリックして保存します。

クラウドプラットフォームの資産を追加すると、アカウントを関連付けることができます。

クラウドプラットフォームにアカウントを追加する手順

1. **［資産］**で、クラウドプラットフォーム資産を選択し、**［アカウント］**タブに切り替えます。
2. 詳細ツールバーの ＋ **［新しいアカウント］**をクリックします。
3. **［全般］**タブの**［名前］**フィールドに、クラウドプラットフォームアカウントのユーザー名、メールアドレス、または電話番号を入力します。
4. （任意）**［説明］**を入力します。
5. **［管理］**タブで**［パスワードリクエストの有効化］**オプションがオンになっていることを確認します。
6. **［参照］**してこのアカウントを管理するプロファイルを選択します。
7. **［アカウントの追加］**をクリックします。
8. **［OK］**をクリックして保存します。

これで、クラウドプラットフォームアカウントのパスワードを手動で確認、変更、または設定できます。SPP は、アカウントを管理するプロファイルの確認と変更の設定に従って、パスワードを自動的に管理することができます。

クラウドプラットフォームアカウントをチェックアウトする手順

1. クラウドプラットフォームのアカウントグループを追加し、アカウントをグループに追加します。
2. クラウドプラットフォームアカウントの資格を追加します。

3. ユーザーを資格に追加します。
4. パスワードリリースポリシーを資格に追加します。
5. クラウドプラットフォームのアカウントグループをポリシーのスコープに追加します。

アカウントへのタグの手動追加

資産管理者は、アカウントに静的タグを手動で追加および削除することができます。ルールによって定義され、稲妻のアイコンが表示される動的なタグを手動で削除することはできません。動的タグを削除する場合は、動的タグに関連付けられたルールを変更する必要があります。詳細については、「資産または資産アカウントのタグの変更」を参照してください。

アカウントへのタグの手動追加手順

1. **［資産管理］＞［アカウント］**に移動します。
2. アカウントを選択し、**［詳細の表示］**をクリックします。
3. **［タグ］**タブで、**［編集］**をクリックします。既存のタグが表示されます。
4. **［編集］**をクリックします。
5. 次のいずれかの方法を使用して、アカウントにタグを割り当てます：
    - 以前に作成したタグを割り当てる場合：
        a. **［タグの追加］**をクリックします。
        b. アカウントに追加するタグを選択します。
        c. **［タグの選択］**をクリックして、選択を保存します。
    - 新しいタグを作成する場合：
        a. **［タグの追加］**をクリックします。
        b. **［タグの選択］**ダイアログで**［新しいタグ］**をクリックします。
        c. タグに必要な情報を入力し、**［OK］**をクリックします。
        d. 新しいタグの追加を終えたら、**［タグの選択］**ダイアログでアカウントに追加するタグを選択します。
        e. **［タグの選択］**をクリックし、選択内容を保存します。
6. **［OK］**をクリックします。

アカウントの削除

アカウントを削除する場合、SPP はそのアカウントを関連する資産から削除するのではなく、単に SPP から削除します。

サービスアカウントを削除すると、SPP は資産の認証タイプを**［なし］**に変更します。この資産に関連付けられたすべてのアカウントの自動パスワードおよび SSH キー管理が無効になります。すべての資産には、それに関連するアカウントのパスワードまたは SSH キーを確認および変更するために、サービスアカウントを持つ必要があります。詳細については、「サービスアカウントについて」を参照してください。

アカウントの削除手順

1. **［資産管理］＞［アカウント］**に移動します。
2. 削除するアカウントを選択します。
3. **［削除］**をクリックします。
4. リクエストを確認します。

アカウントへのユーザーまたはユーザーグループの追加

アカウントにユーザーを追加する場合、そのアカウントの所有権を持つユーザーまたはユーザーグループを指定することになります。

アカウントにユーザーおよびユーザーグループを追加するのは、資産管理者（または委任されたパーティション所有者）の責任です。セキュリティポリシー管理者は、グループを追加する権限のみを持ち、ユーザーを追加する権限は持ちません。詳細については、「管理者のアクセス許可」を参照してください。

アカウントにユーザーを追加する手順

1. **［資産管理］＞［アカウント］**に移動します。
2. **［アカウント］**で、オブジェクトリストからアカウントを選択し、**［詳細の表示］**をクリックします。
3. **［所有者］**タブを開きます。

4. アカウント所有者、資産所有者、および/またはパーティション所有者タブで、＋**［追加］**をクリックします。

5. **［ユーザー/ユーザーグループ］**ダイアログのリストから、1 人以上のユーザーまたはユーザーグループを選択します。

6. **［所有者の選択］**をクリックして、選択内容を保存します。

アカウントパスワードの確認、変更、設定

資産管理者は、**［アカウントセキュリティ］**メニューから、アカウントパスワードを手動で確認、変更、設定することができます。

アカウントのパスワードの手動確認、変更、設定手順

1. **［資産管理］＞［アカウント］**へ移動します。

2. **［アカウント］**で、オブジェクトリストからアカウントを選択します。

3. ツールバーから**［アカウントセキュリティ］**を選択します。
   以下のオプションのいずれかを選択します。
   - **パスワードの確認**：アカウントのパスワードが SPP データベースと同期していることを検証します。パスワードの確認に失敗した場合は、パスワードを変更します。
   - **パスワードの変更**：アカウントパスワードをリセットし、SPP データベースと同期させます。
   - **パスワードの設定**：SPP データベースのアカウントパスワードを設定します。設定オプションは、資産上のアカウントパスワードを変更しません。次のオプションがあります：
     - **手動パスワード**：SPP データベースにアカウントパスワードを手動で設定します。
       a. **パスワードの設定**ダイアログで、パスワードを入力し、確認します。**［パスワードの設定］**をクリックして、SPP データベースを更新します。
       b. 物理デバイスのアカウントパスワードを設定して、SPP データベースと同期します。

- パスワードの生成：SPP に、アカウントのプロファイルに設定されているパスワードルールに準拠した、新しいランダムなパスワードを生成させます。

    a. **パスワードの設定**ダイアログで、**［パスワードの生成］**をクリックします。

    b. **［パスワードのコピー］**をクリックし、コピーバッファに格納します。

    c. 古いパスワードを使用してデバイスにログインし、コピーバッファのパスワードに変更します。

    d. **［パスワードの設定］**をクリックして、SPP データベースのパスワードを変更します。

パスワードアーカイブの表示

資産管理者は、特定の日付のアカウントの以前のパスワードにアクセスすることができます。

［パスワードのアーカイブ］ダイアログには、指定された日付に基づいて、選択された資産の以前に割り当てられたパスワードのみが表示されます。このダイアログには、資産の現在のパスワードは表示されません。パスワードアーカイブが削除されることはありません。

アカウントのパスワード検証とリセット履歴は、**［確認と変更の記録］**タブで確認できます。

アカウントの以前のパスワードにアクセスする手順

1. **［資産管理］＞［アカウント］**に移動します。
2. **［アカウント］**を選択し、**［パスワードのアーカイブ］**を選択します。
3. **［パスワードのアーカイブ］**ダイアログで、日付を選択します。今日の日付（または前の日付）を選択してもエントリが返されない場合、これは資産がまだ現在のパスワードを使用していることを示します。
4. **［表示］**列で、をクリックすると、その日時に資産に割り当てられていたパスワードが表示されます。
5. 詳細ダイアログで、**［コピー］**をクリックすると、パスワードがコピーバッファにコピーされます。

SSH キーの確認、変更、設定

資産管理者は、**［アカウントセキュリティ］**メニューから SSH キーを手動で確認、変更、設定することができます。

SSH キーの手動確認、変更、設定手順

1. **［資産管理］＞［アカウント］**へ移動します。
2. 一覧からからアカウントを選択します。
3. ツールバーから **［アカウントセキュリティ］**をクリックします。
4. 以下のいずれかオプションを選択します。
    - **SSH キーのチェック**：アカウントの SSH キーが SPP データベースと同期していることを確認します。SSH キーの検証に失敗した場合は、SSH キーを変更することができます。
    - **SSH キーの変更**： SSH キーをリセットし、SPP データベースと同期させることができます。サービスアカウントの場合、この選択を使用して、SSH キーを変更するために **SSH キーの生成**を使用しないでください。
    - **SSH キーの設定**：SSH キーを SPP データベースに設定します。**［SSH キーの設定］**オプションは、資産上のアカウントの SSH キーを変更しません。**SSH キーの設定**には、次のオプションがあります。
        - **SSH キーの生成**：新しい SSH キーを生成して、それをアカウントに割り当てます。SSH キーは、アカウントのプロファイルに設定されている SSH キーのルールに準拠しています。

          > ⚠ **注意：**資産への接続が失われるため、サービスアカウントに新しい SSH キーを生成しないでください。代わりに、**［アカウントセキュリティ］＞［SSH キーの変更］**を使用てください。

          ［SSH キーの生成］を選択すると、キーが生成され、SPP データベースに保存されます。以下のフィールドが表示されます。

            - **アカウント**：アカウント名
            - **フィンガープリント**：認証に使用される SSH キーのフィンガープリント
            - **キーのコメント**：SSH キーに関する情報

- **キータイプ**：RSA や DSA などの SSH 認証鍵のタイプ。詳しくは、「SSH キープロファイル」を参照してください。
- キー長：SSH 認証キーの長さ。詳細については、「SSH キープロファイル」を参照してください。
- **公開キー**：生成されたキー。**［コピー］**をクリックして、コピーバッファに入れます。その後、古い SSH キーを使用してデバイスにログインし、コピーバッファ内の SSH キーに変更することができます。

◦ **SSH キーのインポート**：SPP 以外に生成した SSH キーの秘密鍵ファイルをインポートして、アカウントに割り当てます。**［参照］**をクリックしてキーファイルをインポートし、**［パスワード］**を入力してから**［OK］**をクリックします。

資産上のアカウントにすでに手動で設定されている SSH キーをインポートする場合、キーをインポートする前に、まずキーが正しく設定されていることを確認することをお勧めします。たとえば、SSH クライアントプログラムを実行して、秘密キーが資産へのログインに使用できることを確認できます：

ssh -i <privatekeyfile> -l <accountname> <assetIp>

authorized key の設定方法の詳細については、ターゲットプラットフォームの OpenSSH サーバーのドキュメントを参照してください。

> **メモ**: SPP は、現在、authorized key のオプションを管理していません。インポートされた鍵に、資産上の authorized key ファイルで構成されたオプションがある場合、SPP によって鍵がローテートされたときに、これらのオプションは保持されません。

◦ **SSH キーの自動転送**：まだ設定されていない場合、アカウントの現在の SSH キーを資産上のアカウント用の正しいファイルにインストールします。

SSH キーアーカイブの表示

資産管理者は、特定の日付のアカウントの以前の SSH キーにアクセスすることができます。

SSH キーのアーカイブダイアログには、指定された日付に基づいて選択された資産に以前割り当てられた SSH キーのみが表示されます。このダイアログでは、資産に対する現在の SSH キーは表示されません。SSH キーのアーカイブが削除されることはありません。

アカウントの SSH キーの検証およびリセットの履歴は、**［変更と履歴の記録］**タブに表示されます。

アカウントの以前の SSH キーへのアクセス手順

1. **［資産管理］＞［アカウント］**を開きます。
2. アカウント名を選択し、**［SSH キーのアーカイブ］**をクリックします。
3. **［SSH キーのアーカイブ］**ダイアログで、日付を選択します。今日の日付（または以前の日付）を選択してもエントリが返されない場合、これは資産がまだ現在の SSH キーを使用していることを示します。
4. **［表示］**列で、をクリックすると、その日時に資産に割り当てられていた SSH キーが表示されます。
5. **詳細**ダイアログで、**［コピー］**をクリックして SSH キーをコピーバッファにコピーするか、**［終了］**をクリックしてダイアログを閉じます。

10.3 資産

SPP の資産とは、SPP が管理するコンピューター、サーバー、ネットワークデバイス、アプリケーションのことです。

SPP に資産とアカウントを追加するのは資産管理者（または委任されたパーティション所有者）の責任です。監査人は、資産にアクセスする権限を持っています。アカウント所有者は、自分のアカウントに関連する資産の［プロパティ］タブと［アカウント］タブに対する読み取り権限を持っています。

SPP に資産を追加する前に、資産が適切に構成されていることを確認する必要があります。詳細については、「管理のためのシステム準備」を参照してください。

各資産は、［アカウント］タブ（資産）で識別される関連アカウント（ユーザー、グループ、サービス）を持つことができます。資産が削除されると、関連するアカウントも削除されます。

すべての資産にはプロファイルが必要です。詳細については、「資産にプロファイルを割り当て」を参照してください。新しい資産には、特に指定がない限り、デフォルトのプロファイルが自動的に適用されます。

資産は、一度に 1 つのパーティションにしか配置できません。詳しくは「資産をパーティションに割り当て」を参照してください。資産をパーティションに追加すると、その資産に関連するすべてのアカウントが自動的にそのパーティションに追加されます。

ドメインコントローラー（DC）資産の使用

ドメインコントローラー（DC）資産でタスクとサービスを管理することができます。従属アカウントは DC 資産で管理されます。DC 資産は、依存するパスワードの更新のみをサポートします。ドメインコントローラーのアカウントパスワードは、ディレクトリ資産で管理されます。

1. DC 資産を Windows サーバープラットフォームとして作成し、接続サービスアカウントにディレクトリ認証を使用します。詳細については、「資産の追加」を参照してください。

2. 管理したいタスク/サービスのサービスアカウントが、ディレクトリ資産に定義されていることを確認します。詳細は、「資産にアカウントを追加」を参照してください。

3. DC 資産に、サービスアカウントのアカウント依存関係を追加します。詳細については、「アカウントの依存関係を追加」を参照してください。

Check Point GAiA の使用

パスワードおよび SSH キーは、Check Point GAiA プラットフォーム（R76～R80.30）で管理できます。

SPP では、ユーザーアカウントの管理に加えて、Check Point の **expert** コマンドのパスワードも管理することができます。**expert** パスワードは、SPP では特権アカウントとしてマークされている以外は、通常のユーザーアカウントと同様に表示されます。つまり、サービスアカウントとして使用することはできず、このアカウント用の SSH キーを生成したりインストールしたりすることもできません。

Check Point 用のサービスアカウントを選択するための最小要件は次のとおりです：

- Check Point 用のサービスアカウントは、CLI アクセスが有効であり、以下の RBA 機能が有効である必要があります。
    - read-write ユーザー（読み書き可能なユーザー）
    - read-only グループ（読み取り専用グループ）
- expert パスワードを管理するには、サービスアカウントで以下の RBA 機能が有効になっている必要があります。
    - read-write expert-password-hash（読み書き可能な expert-password-hash）
    - read-write expert（読み書き可能な expert）

SSH キーを管理するために、サービスアカウントにはログインシェルとして Unix シェルが設定されている必要があります。UID が 0 でない場合は、権限を昇格するために sudo 権限が必要となります。

資産を追加する際には、製品として Check Point GAiA (SSH) を選択し、特権アカウントには **expert** が表示されます。

資産ビュー

資産へのアクセス

［資産管理］＞［資産］に移動します。必要に応じて、パーティションのドロップダウンを使用して、資産の親パーティションを選択できます。資産を選択し、✎をクリックすると、追加の情報とオプションを表示します。

資産ビューには、選択したシステムに関する以下の情報が表示されます。すべての資産ですべての選択項目が利用できるわけではありません。

- **プロパティ**タブ：選択した資産の一般設定、管理設定、接続設定が表示されます。
- **所有者**タブ：資産の所有者であるユーザーおよびユーザーグループに関する情報が表示されます（このタブから割り当てられたもの、またはこの資産に関連付けられたタグから派生した所有権のいずれか）。このタブには、この資産の有効な所有者でもあるパーティション所有者は表示されません。
- **アカウント**タブ：この資産に関連付けられたアカウントが表示されます。
- **アカウントの依存関係**タブ：Windows のみ。選択した Windows サーバーがサービスやタスクを実行するために依存するディレクトリアカウントが表示されます。
- **検出されたサービス**タブ：選択した資産に関連する検出されたサービスの詳細が表示されます。
- **SSH キーが検出されました**タブ：資産で検出された SSH キーが表示されます。
- **履歴**タブ：選択した資産に影響を与えた各操作の詳細が表示されます。

ツールバー

次のツールバーボタンを使用して、資産を管理します。

- ＋**［新しい資産］**：SPP に資産を追加します。詳細については、「資産の追加」を参照してください。

- **［削除］**：選択した資産を削除します。資産を削除すると、資産に関連付けられているすべての SPP アカウントも完全に削除されます。詳細については、「資産の削除」を参照してください。
- **［詳細の表示］**：資産を選択してこのボタンをクリックすると、資産の追加情報およびオプションが表示されます。
- **［アクセスリクエスト］**：選択した資産のアクセスリクエストサービスを有効または無効にできます。メニューオプションには、**［セッションリクエストの有効化］**と**［セッションリクエストの無効化］**があります。
- **［SSH ホストキー］**：以下のメニューオプションがあります：
    - **［SSH ホストキーの検出］**：このオプションは、Unix ベースの資産や Linux ベースの資産など、SSH ホストキーを交換する資産にのみ適用されます。選択した資産の最新の SSH ホストキーを取得します。**［SSH ホストキーの検出］**ダイアログには、SSH ホストキーがいつ最新になったかも表示されます。SSH ホストキーが資産で検出されない場合、システムの確認、パスワードの確認、パスワードの変更など特定のタスクが資産に関連付けられたアカウントで利用できなくなります。
    - **［SSH ホストキーの取得］**：このオプションは Cisco NX-OS 資産にのみ適用され、プラットフォームから最新の SSH ホストキーを取得するために使用されます。また、**［SSH キーの取得］**ダイアログには、SSH ホストキーがいつ最新になったかが表示されます。SSH ホストキーが資産から取得されない場合、セッションは利用できなくなります。
    - **［SSH ホストキーの設定］**：このオプションは、SPP が（Other Directory 資産など）資産を自動的に検出できない場合、ホストキーを資産に手動で追加することができるようにします。
    - **［SSH ホストキーのダウンロード］**：選択した資産に SSH キーを追加します。詳細については、「公開 SSH キーのダウンロード」を参照してください。
- **［接続のテスト］**：SPP が現在のサービスアカウントの資格情報を使用して資産にログインできることを確認するために選択します。詳細については、「資産の接続性の確認」を参照してください。
- **［今すぐ同期］**：資産とアカウントによるディレクトリ追加（増分）同期処理を実行します。同期はプロバイダごとに資産ごとにキューに入れられ、その資産に対して一度に 1 つのディレクトリ同期が実行されます。異なる資産で複数の同期を並行して実行することができます。削除は同期されないので、これはディレクトリ同期の高速タイプです。タスクウィンドウには、タスクの進行状況と結果が表示されます。**［詳細］**をクリックしてさらに情報を確認したり、**［停止］**をクリックしてタスクをキャンセルしたりすることができます。API（Assets/Synchronize）を使用して、すべて

の削除、追加、および変更を含む削除（完全）同期を実行することができます。この同期には時間がかかります（おそらく数時間）。特に、ディレクトリの設定に基づいて初めて実行する場合は、時間がかかります。

- ▶ **［アカウントの検出］**：関連するアカウント検出ジョブを実行します。詳細については、「アカウント検出」を参照してください。
- **［有効化-無効化］**：次のいずれかを選択します：
  - **［有効化］**を選択すると、SPP が無効な資産を管理します。アカウント検出ジョブは、過去に有効または無効としてマークされているかどうかに関係なく、検出ルールの基準に一致するすべてのアカウントを検出します。
  - **［無効化］**を選択すると、SPP は選択した資産を管理しません。資産を無効にすると、SPP はその資産を無効にし、関連するすべてのアカウントを削除します。後で資産を管理することを選択した場合、SPP は関連するすべてのアカウントを再び有効にします。
- **［無効化済みの表示］**：管理されておらず、無効化されており、関連付けられたアカウントがない資産を表示します。資産管理は、資産を右クリックして**［有効化］-［無効化］**を選択することで制御できます。
- **［無効化済みの非表示］**：管理されておらず、無効化されており、関連付けられたアカウントがない資産を非表示にします。資産管理は、資産を右クリックして**［有効化］-［無効化］**を選択することで制御できます。
- **［エクスポート］**：このボタンを使用して、一覧に表示されたデータを JSON または CSV ファイルとしてエクスポートします。詳細については、「データのエクスポート」を参照してください。
- **［更新］**：資産のリストを更新します。

10.3.1 プロパティタブ

プロパティタブには選択した資産に関する情報が一覧表示されます。

プロパティへのアクセス

［資産管理］＞**［資産］**＞（詳細の表示）＞**［プロパティ］**に移動します。

表：プロパティタブ：全般プロパティ

プロパティ	説明
名前	資産の名前

説明	資産を識別するための説明テキスト
パーティション	選択した資産が存在するパーティションの名前

表：プロパティタブ：接続プロパティ

プロパティ	説明
プラットフォーム	選択した管理対象システムのプラットフォーム
バージョン	該当する場合は、システムのバージョン
アーキテクチャ	該当する場合は、オペレーティングシステムのアーキテクチャ
ネットワークアドレス	該当する場合は、管理対象システムのネットワーク DNS 名または IP アドレス
認証タイプ	コンソールが管理されたシステムに接続する方法。詳細については「カスタムプロパティ」を参照してください。
Telnet セッションポート	TN3270 または TN5250 に接続する場合、接続用のポート
フォレストの管理（ディレクトリ）	**真**の場合、フォレスト全体が管理されます。
フォレストルートドメイン名（ディレクトリ）	資産のフォレストルートドメイン（[**全般**] タブの [**名前**])。複数のディレクトリ資産を同じドメインで管理できるように、1 つのドメインは複数のディレクトリ資産に対して特定できます。
ドメイン	該当する場合、管理対象ドメイン
セッションリクエストの有効化	資産に対してセッションアクセスリクエストが有効になっている場合は、チェックボックスをオンにします。
ポート	接続に使用するポート。デフォルトは 22
RDP セッションポート	該当する場合、RDP セッションアクセスリクエストに使用されるターゲットサーバー上のアクセスポート
SSH セッションポート	該当する場合、SSH セッションアクセスリクエストに使用されるターゲットサーバー上のアクセスポート
Telnet セッションポート	TN3270 または TN5250 に接続する場合は、接続用のポート

プロパティ	説明
SSH ホストキーのフィンガープリント	資産への認証に使用される管理システムの公開ホストキーのフィンガープリント。SSH ホストキーが必要な資産にキーがない場合、パスワードの確認は失敗します。詳細については、「接続障害」を参照してください。
［数］分ごとに追加を同期	該当する場合、SPP がオブジェクトへの追加または変更を同期する頻度。最後の同期、最後に失敗した同期、最後に成功した同期の日時が表示されます。間隔はディレクトリごとに異なります。
［数］分ごとに削除を同期	該当する場合、SPP がオブジェクトの削除を同期する頻度。最後の同期、最後に失敗した同期、最後に成功した同期の日時が表示されます。間隔はディレクトリごとに異なります。

表：プロパティ：管理プロパティ

プロパティ	説明
パスワードプロファイル	資産のアカウントを管理するプロファイルの名前。 パスワードプロファイルがパーティションから継承されている場合は、パスワードプロファイルの名前の横に（継承）というテキストが表示されます。パスワードプロファイルを明示的に設定すると、✕ボタンが表示され、明示的に設定したパスワードプロファイルをクリアして、代わりにパーティションから継承したパスワードプロファイルを使用することができます。 **注**：すべての資産には、プロファイルが適用される必要があります。新しい資産は、特に指定がない限り、自動的にデフォルトのプロファイルに支配されます

プロパティ	説明
SSH キープロファイル	資産のアカウントを管理するプロファイルの名前。 SSH キープロファイルがパーティションから継承されている場合、SSH キープロファイルの名前の横に（継承）というテキストが表示されます。 SSH キープロファイルが明示的に設定されている場合、明示的に設定された SSH キープロファイルをクリアするための ✕ ボタンが表示されます。クリアされたプロファイルの変更が適用されると、割り当てられた継承されたプロファイルが表示されます。パーティションに指定されたデフォルトの SSH キープロファイルがない場合、その資産には SSH キープロファイルが割り当てられなくなります。資産に明示的に設定された SSH キープロファイルがない場合、その資産上のアカウントには SSH キープロファイルが割り当てられなくなります。パーティションにデフォルトの SSH キープロファイルを指定すると、そのパーティション内のすべての資産とアカウントに SSH キープロファイルが継承されるようになります。 **メモ**：すべての資産には、プロファイルが適用される必要があります。新しい資産は、特に指定がない限り、すべて自動的にデフォルトのプロファイルに支配されます。
管理対象ネットワーク	ワークロードバランシングに割り当てられる管理ネットワーク。詳しくは、「管理対象ネットワーク」を参照してください。
すべてのパーティションで検出に使用可能	**真**の場合、この資産はパーティションを越えて資産検出ジョブの読み取りアクセスが可能です。
セッションリクエストの有効化	**真**の場合、この資産に対してセッションアクセスリクエストが有効になります。

表：プロパティタブ：アカウント検出プロパティ

プロパティ	説明
アカウント検出	アカウント検出の識別子
説明	スケジュールの説明

プロパティ	説明
スケジュール	アカウント検出のスケジュール
前回成功したアカウント検出	最後に成功したアカウント検出の日付と時間
前回失敗したアカウント検出	最後に失敗したアカウント検出の日付と時間
次のアカウント検出	次回のアカウント検出の日時
前回成功したサービス検出	最後に成功したサービス検出の日付と時間
前回失敗したサービス検出	最後に失敗したサービス検出の日付と時間
次回のサービス検出	次回のサービス検出の日時

タグ：選択した資産に割り当てられたタグ。**［タグ］**タブに表示される情報には、タグ付けルールによって資産に割り当てられた動的タグと、手動で追加された静的タグの両方が表示されます。タグの割り当てを表示するだけでなく、資産管理者はこのタブを使用して、静的に割り当てられたタグを追加および削除することができます。

削除：選択した資産を削除するには、このボタンをクリックします。

10.3.2 アカウントタブ

資産の**［アカウント］**タブには、この資産に関連するアカウントが表示されます。

選択した資産にアカウントを関連付けるには、詳細ツールバーの＋**［新しいアカウント］**をクリックします。

アカウントへのアクセス

［資産管理］＞**［資産］**＞（詳細の表示）＞**［アカウント］**に移動します。

表：資産：アカウントタブプロパティ

プロパティ	説明
名前	選択した資産に関連するアカウント名。 1 つのアカウントは 1 つの資産にしか関連付けられませんが、複数のアカウントで資産にログインすることができます。
ドメイン名	アカウントのドメイン名で、アカウントの一意性を判断するのに役立ちます。
パスワードプロファイル	アカウントを管理するプロファイルの名前
SSH キープロファイル	SSH キープロファイルの名前
サービスアカウント	アカウントがサービスアカウントである場合、✔チェックマークが表示されます。
パスワードリクエスト	アカウントでパスワードリリースリクエストが有効である場合、✔チェックマークが表示されます。 詳細ツールバーの **［アクセスリクエスト］** をクリックすると、選択したアカウントに対するユーザーのアクセスリクエスト機能を有効または無効にすることができます。
セッションリクエスト	アカウントでセッションアクセスリクエストが有効である場合、✔チェックマークが表示されます。 詳細ツールバーの **［アクセスリクエスト］** をクリックすると、選択したアカウントに対するユーザーのアクセスリクエストが有効または無効になります。
SSH キーリクエスト	アカウントで SSH キーリリースリクエストが有効である場合、✔チェックマークが表示されます。 詳細ツールバーの **［アクセスリクエスト］** をクリックすると、選択したアカウントへのユーザーのアクセスリクエストを有効または無効にすることができます。
無効	資産が管理されていないこと、無効であること、関連するアカウントがない場合、✔チェックマークが表示されます。
パスワード	アカウントにパスワードが設定されている場合、✔チェックマークが表示されます。詳細については、「アカウントパスワードの確認、変更、設定」を参照してください。

プロパティ	説明
SSH キー	アカウントに SSH キーが設定されている場合、✔チェックマークが表示されます。詳細については、「SSH キーの確認、変更、設定」を参照してください。
説明	アカウント追加時に入力した説明文
タグ	アカウントに関連付けられたタグ

詳細ツールバーの以下のボタンを使用して、資産アカウントを管理します。

表：資産：アカウントタブツールバー

オプション	説明
＋ 新しいアカウント	選択した資産にアカウントを追加します。詳細については、「資産にアカウントを追加」を参照してください。
削除	選択したアカウントを資産から削除します。
詳細の表示	選択したアカウントを編集します。
アカウントセキュリティ	以下のメニューオプションがあります： • **パスワードの確認、パスワードの変更、パスワードの設定**：詳細については、「アカウントパスワードの確認、変更、または設定」を参照してください。 • **SSH キーのチェック、SSH キーの変更、SSH キーの設定：**詳細については、「SSH キーの確認、変更、設定」を参照してください。
▶ SSH キーの検出	アカウントに関連付けられた SSH キーの検出ジョブを実行します。詳細は、「SSH キーの検出」を参照してください。

オプション	説明
アクセスリクエスト	選択したアカウントに対してアクセスリクエストサービスを有効または無効にするオプションを選択します。値は、資産のプラットフォームがパスワードリクエスト、SSH キーリクエスト、セッションリクエストのいずれかをサポートしていることを示すかどうかから得られます。必要に応じて、パスワードリクエスト、セッションリクエスト、SSH キーリクエストを有効または無効にすることができます。 サービスアカウントは、資産の作成時に作成され、デフォルトでは、セッションまたはパスワードアクセスは有効になっていません。 検出されたアカウントは、アカウントを検出する際に使用されるアカウント検出テンプレートによって制御されます。これらは、アカウント検出ジョブのルールテンプレートのプロパティです。詳細については、「アカウント検出ルールの追加」を参照してください。
有効化 – 無効化	■ **［有効化］**を選択すると、SPP が無効な資産を管理します。アカウント検出ジョブは、過去に有効または無効とマークされているかどうかに関係なく、検出ルールの基準に一致するすべてのアカウントを検出します。 ⊘ **［無効化］**を選択すると、SPP が管理しないようになります。資産を無効にすると、SPP はその資産を無効にし、関連するアカウントをすべて削除します。後で資産を管理することを選択した場合、SPP は関連するすべてのアカウントを再び有効にします。
エクスポート	このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
更新	資産アカウントのリストを更新します。
検索	このリストから特定の資産アカウントまたはアカウントのセットを見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.3.3 アカウントの依存関係タブ

アカウントの依存関係タブには、選択した Windows サーバーがサービスとタスクを実行するために依存しているディレクトリアカウントが表示されます。**アカウントの依存関係**タブは、Windows プラットフォームで、1 つ以上のディレクトリが SPP に追加されている場合のみ適用できます。

詳細ツールバーから ＋ **［アカウントの追加］**をクリックして、選択した資産にアカウントの依存関係を関連付けます。詳細については、「アカウントの依存関係を追加」を参照してください。

アカウントの依存関係へのアクセス

［資産管理］ > **［資産］** > （詳細の表示） > **［アカウントの依存関係］**に移動します。

表：資産：アカウントの依存関係タブプロパティ

プロパティ	説明
名前	ディレクトリアカウントの名前
ディレクトリ	アカウントが存在するディレクトリ
ドメイン名	ディレクトリのフォレストルートドメイン名
識別名	ディレクトリアカウントの識別名
説明	アカウントの依存関係の説明

ツールバーには次のオプションがあります：

表：資産：アカウントの依存関係ツールバー

オプション	説明
＋ **アカウントの追加**	アカウントの依存関係を選択した資産に追加します。
ー **削除**	アカウントの依存関係を資産から削除します。
更新	アカウントの依存関係の一覧を更新します。
検索	このリストから特定のアカウント依存関係を見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.3.4 所有者タブ

所有者タブには、アカウント（および関連する資産）に関連付けられた所有者の情報が表示されます。タグを介して割り当てられた所有者の変更については、「資産または資産アカウントのタグの変更」を参照してください。

所有者へのアクセス

［資産管理］>**［資産］**>  （詳細の表示）>**［所有者］**に移動します。

所有者タブには、**資産所有者**タブと**パーティション所有者**タブの 2 つのビューがあります。

表：資産: 所有者タブのプロパティ

プロパティ	説明
資産所有者	
タイプ	所有者のタイプ
名前	所有者の名前
プロバイダ	認証プロバイダの名前
直接	オブジェクトの所有権が、タグの使用ではなく、直接割り当てられたことを示します。
タグを使用	オブジェクトの所有権がタグを使用して割り当てられたことを示します。
パーティション所有者	
タイプ	ユーザーまたはグループのタイプ
名前	ユーザーまたはグループの名前
プロバイダ	認証プロバイダの名前

詳細ツールバーの以下のボタンを使用して、選択した資産が所有するオブジェクトを管理します。

表：資産: 所有者ツールバー

オプション	説明
＋ 追加	選択した資産に 1 人または複数のユーザーまたはユーザーグループを追加します。詳細については、「資産にユーザーまたはユーザーグループを追加」を参照してください。
ー 削除	選択したオブジェクトを、選択した資産のマネージャーから削除します。削除できるのは、（タグを使用して割り当てられたオブジェクトではなく）資産に直接割り当てられたオブジェクトのみです。
エクスポート	リストされたデータを JSON または CSV ファイルとしてエクスポートします。詳細については、「データのエクスポート」を参照してください。
更新	所有者/管理者のリストを更新します。
検索	このリストから特定のオブジェクトを見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.3.5 SSH キーが検出されました

SSH キーが検出されましたタブには、この資産のすべてのアカウントの検出された SSH キーが表示されます。

SSH キーが検出されましたへのアクセス

［資産管理］＞［資産］＞（詳細表示）**＞［検出された SSH キー］**に移動します。

表：資産：SSH キーが検出されましたタブプロパティ

プロパティ	説明
フィンガープリント	認証に使用される SSH キーのフィンガープリント
アカウントステータス	Safeguard アカウントのステータス
SSH キーが管理されています	現在アカウントで使用されている SSH キーにチェックマークが付きます。
コメント	フリーフォームのコメント

プロパティ	説明
キータイプ	RSA や DSA などの SSH キーの ID タイプ。詳しくは、「SSH キープロファイル」を参照してください。
キー長	サポートされている RSA または DSA の鍵の長さ
資産名	アカウントに関連付けられた資産の名前
アカウント	SSH キーが検出されたアカウントの名前
日付/時間が検出されました	SSH キーが検出された日付と時間

詳細ツールバーには以下のボタンがあります。

オプション	説明
取り消し	管理されていない SSH キーのアクセスを取り消します。
更新	選択したアカウントに割り当てられた依存資産のリストを更新します。
検索	このリストから特定の依存資産を見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.3.6 検出されたサービスタブ

検出されたサービスタブには、選択した資産に固有の情報が表示され、Windows 資産にのみ適用されます。

検出されたサービスへのアクセス

［資産管理］>**［資産］**>（詳細の表示）>**［検出されたサービス］**に移動します。

これらのボタンを使用して、検出されたサービスを管理します。

表：検出されたサービス：ツールバー

オプション	説明
サービスの検出	選択したサービス検出ジョブを実行します。
更新	サービス検出ジョブのリストを更新します。

オプション	説明
🔍 **検索**	この資産を見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

検出されたサービスについて以下の情報が表示されます。

表：検出されたサービスタブプロパティ

プロパティ	説明
アカウント	資産上の検出されたサービスまたはタスクに関連する、検出されたアカウントに対応する Safeguard のアカウント。これは、ローカルアカウントまたは Active Directory のアカウントにすることができます。
ドメイン名	アカウントが Active Directory アカウントの場合、そのアカウントのドメイン名
システム名	アカウントが関連付けられている資産
アカウントステータス	Safeguard アカウントのステータス
依存アカウント	アカウントが資産のアカウント依存として関連付けられている場合、✔チェックが表示されます。アカウントが資産のアカウント依存として関連付けられていない場合、値は空白になります。
サービスタイプ	検出されたサービスの種類（**サービス**または**タスク**）
サービス名	検出されたサービスまたはタスクの名前
サービスが有効化されました	資産上のサービスまたはタスクが有効かどうかを✔チェックマークで表示します。チェックマークがない場合、そのサービスまたはタスクは無効です。
検出されたアカウント	設定されている検出されたサービスのアカウント名
日付/時間が検出されました	サービスまたはタスクが発見された日付と時刻

10.3.7　履歴タブ

履歴タブでは、選択した資産に影響を与えた各操作の詳細を表示したり、エクスポートしたりすることができます。

履歴へのアクセス

［資産管理］＞**［資産］**＞ （詳細表示）＞**［履歴］**に移動します。

履歴タブの上部には、次の情報が表示されます：

- **日付範囲**：デフォルトでは、履歴の詳細は過去 24 時間について表示されます。ドロップダウンから、時間間隔の 1 つを選択すると、その時間枠の履歴の詳細が表示されます。
- **エクスポート**：このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
- **更新**：表示されているリストを更新します。
- **検索**：詳細については、「検索ボックス」を参照してください。

表：資産履歴タブのプロパティ

プロパティ	説明
日付/時間	イベントの日付と時刻
ユーザー	イベントを発生させたユーザーの表示名
ソース IP	イベントをトリガーした管理システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択した資産の名前
イベント	選択した資産に対して行われた操作の種類： • 作成 • 削除 • 更新 • メンバーシップの追加 • メンバーシップの削除 **メモ：**メンバーシップの操作は、選択した資産にアカウントの依存関係が追加または削除されたなど、関連オブ

プロパティ	説明
	ジェクトまたは親オブジェクトとの関係が変更されたことを示します。
関連オブジェクト	関連オブジェクトの名前
関連オブジェクトのタイプ	関連オブジェクトのタイプ
親	選択した資産が子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

10.3.8 資産の管理

SPP の資産を管理するために、**資産**ページのコントロールとタブページを使用して、次のタスクを実行します。

- 資産の追加
- 資産の接続性の確認
- 資産をパーティションに割り当て
- 資産にプロファイルを割り当て
- 資産にタグを手動で追加
- 資産にアカウントを追加
- アカウントの依存関係を追加
- 資産にユーザーまたはユーザーグループを追加
- 資産の削除
- 公開 SSH キーのダウンロード

資産の追加

SPP に資産とアカウントを追加するのは、資産管理者の責任です。

SPP では、自動的に実行される資産検出ジョブを設定することができます。詳細については、「資産検出ジョブのワークフロー」を参照してください。

SPP にシステムを追加する前に、システムが適切に構成されていることを確認してください。詳細については、「管理のためのシステム準備」を参照してください。

> **メモ：** MS SQL 資産を SPP に追加するには、特別な考慮事項があります。詳細については、KB 261806 を参照してください。

資産の追加手順

1. **［資産管理］**>**［資産］**に移動します。
2. ツールバーから ＋ **［新しい資産］**をクリックします。
3. **新しい資産**ダイアログで、各タブに情報を入力します：

タブ	説明
全般タブ（資産の追加）	資産に関する一般的な情報を追加する場所
接続タブ（資産の追加）	ネットワークアドレス、オペレーティングシステム、およびバージョン情報を追加する場所
管理タブ（資産の追加）	パーティションおよびプロファイル情報を追加し、セッションリクエストを有効化する場所
アカウント検出タブ（資産の追加）	アカウント検出ジョブを追加する場所

全般タブ（資産の追加）

全般タブでは、資産に関する一般情報を指定します。

表：資産：全般プロパティ

プロパティ	説明
名前	（必須）資産の一意の表示名を入力します。 上限：100 文字
説明	（任意）この管理対象システムに関する情報を入力します。 上限：255 文字
パーティション	この資産のパーティションを参照して選択します。特定のパーティションをデフォルトとして設定することができます。

接続タブ（資産の追加）

接続タブで、プラットフォーム、**認証タイプ**を選択し、アカウントの資格情報を指定します。資産にカスタムプラットフォームがある場合は、**カスタムプロパティ**要素が表示されます。詳細については、「カスタムプラットフォーム」を参照してください。ディレクトリ資産を作成すると、作成されたアカウントは［検出されたアカウント］プロパティグリッドに［検出されたアカウント］として表示されます。詳細については、「検出されたアカウント」を参照してください。

資産の設定は次のとおりです。

表：資産：接続プロパティ

プロパティ	説明
プラットフォーム	この資産のオペレーティングシステムまたはディレクトリサービスを選択します。 カスタムプラットフォームを選択することもできます。詳細については、「カスタムプラットフォーム」を参照してください。 **一般的なオペレーティングシステムの選択：** SPP では、汎用のオペレーティングシステムとして、**Other**、**Other Managed**、**Other Directory**、**Linux** を選択することができます。これにより、特定のプラットフォームを指定せずに SPP に資産を追加することができます。 • **Other**：その他のオペレーティングシステムを持つ資産は管理できません。その他のオペレーティン

プロパティ	説明
	グシステムを持つ資産に関連付けられているアカウントのパスワードを手動で変更することはできます。SPP は資産に接続できないため、パスワードまたは SSH キーの自動チェックと変更、接続のテスト、または接続を必要とするその他のアクティビティは行われません。 • **Other Managed**：SPP はパスワードを保存し、プロファイル構成に従って自動的にチェックおよび変更することができます。アクティブな接続やサービスアカウントはありません。パスワードは内部でローテーションされ、ローテーションが完了すると、イベント通知が送信されます。別のコンポーネントや自動化の一部で、パスワードを変更したり、設定ファイルでパスワードを使用したりすることができます。例えば、リスナーは、SPP Application to Application（A2A）サービス経由で変更イベントを受け取り、必要に応じてアクションを実行することができます。 • **Other Directory**：資産とアカウントレベルでのディレクトリプロパティの追加をサポートしています。これにより、アクセス構成設定を使用して、リンクされたアカウントまたはディレクトリアカウントを介して、それらに格納されたアカウントをセッションポリシーで使用することができます。Other Directory は実際にはディレクトリに接続されていないため、Other Directory が代表する実際のディレクトリに属するアカウントや資産を検出することはできません。そのため、すべてのアカウント、資産、認証情報は、SPP に手動で入力する必要があります。 ⚠ **注記：Other Directory は実際にはディレクトリに接続されていないため、Other Directory の資産とアカウントが Other Directory が表す実際のディレクトリと同期していることを確認するのはお客様の責任となります。**

プロパティ	説明
	たとえば、SPP でパスワードを変更しても、そのパスワードは実際のディレクトリには設定されません。このため、SPP のアカウントと実際のディレクトリのアカウントとの同期がとれなくなります。手動で修正するまでは、そのパスワードを使用することはできません。 **重要**: Other Directory は、ディレクトリとドメインの間に 1 対 1 の関係を必要とします。システム単位のライセンスの場合、お客様の資産を完全にサポートするために多くのライセンスが必要となる場合があります。 • **Linux**： SPP は、ベストエフォートベースで「Linux」を使用して資産を管理します。 **Other** プラットフォームの詳細：**Other** プラットフォームタイプは、別のプラットフォームタイプへ変更することができます。逆に、任意のプラットフォームタイプを **Other** に変更することができますが、現在のプラットフォームタイプに固有のプロパティ値は失われます。たとえば、**Linux** オペレーティングシステムを、AIX、HP-UX、Solaris などの任意のタイプの Linux に変更することができます。その後、必要に応じて、特定のプラットフォームタイプを **Other** に戻すことができます。
バージョン	（任意）該当する場合は、オペレーティングシステムのバージョンを選択します。Linux または Macintosh OS X システムを追加する場合、SPP では Other バージョンを選択することができます。カスタムプラットフォームでは、バージョンを選択することはできません。 SPP は、ドメインコントローラー上のアカウントのパスワードを管理しません。ドメインコントローラー上のアカウントは、ドメインコントローラーをホストするディレクトリ資産

プロパティ	説明
	で管理します。詳細については、「資産にアカウントを追加」を参照してください。
アーキテクチャ	（任意）製品のシステムアーキテクチャ。カスタムプラットフォームでは、アーキテクチャを設定することはできません。
ネットワークアドレス	該当する場合は、ネットワーク DNS 名またはネットワークを介して管理対象システムに接続するために使用する IP アドレスを入力します。 Amazon Web Services 資産の場合は、Amazon AWS アカウント ID またはエイリアスを入力します。
認証タイプ	資産に使用する認証方式を選択します。
ドメイン名（ディレクトリ）	資産のドメイン（**[全般]** タブの **[名前]**）。複数のディレクトリ資産を同じドメインで管理できるように、1 つのドメインは複数のディレクトリ資産に対して特定することができます。
NetBIOS 名	資産の NetBIOS 名
ドメインの一意の ID	ドメイン固有 ID（Other Directory のみ）
名前付けコンテキスト	資産のネーミングコンテキスト
フォレストの管理（一部のタイプのディレクトリアカウントでのみ使用可能）	フォレスト全体を管理する場合に選択します。 1 つのドメインだけを管理する場合は選択しないでください。
ドメインコントローラー（ディレクトリアカウントの種類によっては使用できません）	この値は、ディレクトリ（Active Directory など）に対して設定されます。Windows ドメインコントローラー上のタスクとサービスを管理するには、ドメインコントローラーの Windows 資産を追加する必要があります。 Active Directory の場合、SPP が DNS および CLDAP の ping からドメインコントローラーを自動的に見つける代わりに、ドメインコントローラーを指定することができます。
RDP セッションポート	該当する場合、RDP セッションリクエストに使用するターゲットサーバーのアクセスポートを指定します。 デフォルトポート 3389

プロパティ	説明
SSH セッションポート	該当する場合、SSH セッションリクエストに使用するターゲットサーバー上のアクセスポートを指定します。 デフォルトポート 22
Telnet セッションポート	TN3270 または TN5250 に接続する場合、接続用のポートを指定します。デフォルトでは、Telnet サーバーは通常ポート 23 でリッスンします。
追加同期間隔（ディレクトリ）	追加同期（増分同期）は、削除を除くすべての変更を同期させます。これは、より高速な同期タイプです。 ディレクトリ資産の場合、追加を同期する頻度(分)を入力または選択します。これにより、SPP にマッピングされたグループメンバーシップやユーザーアカウント属性など、オブジェクトに加えられた追加や変更が SPP に反映されます。 デフォルトは 15 分で、範囲は 1 ～ 2147483647 分です。 ディレクトリ同期はデフォルトで有効になっており、無効にすることもできます。詳細については、「サービスの有効化または無効化」を参照してください。
削除同期間隔（ディレクトリ）	削除同期（完全同期）は、すべての変更と削除を同期します。この同期は、ディレクトリの設定に基づき、特に初回実行時に時間がかかります（おそらく数時間）。 ディレクトリ資産の場合、SPP に削除を同期させる頻度を入力または選択します(単位は分)。 これにより、SPP にマッピングされたグループメンバーシップおよびユーザーアカウント属性を含むオブジェクトに対して行われた追加、変更、および削除が SPP に更新されます。 デフォルトは 15 分で、範囲は 1 ～ 1440 分です。 ディレクトリ同期はデフォルトで有効になっており、無効にすることもできます。詳細については、「サービスの有効化または無効化」を参照してください。 削除（完全）同期は、API Assets/Synchronize および IdentityProviders/Synchronize を使用して、オンデマンドで実行できます。

表：接続タブ：資産認証タイプ

認証タイプ	説明
SSH キー	SSH 認証キーを使用して資産を認証します。
ディレクトリアカウント	Microsoft Active Directory などの外部 ID ストアのディレクトリアカウントを使用して資産を認証します。 **メモ：**この認証タイプを使用するには、最初にディレクトリ資産を追加し、ドメインユーザーアカウントを追加する必要があります。詳細については、「アカウント」を参照してください。
Starling Connect	Starling Connect で構成されたコネクタを使用して資産に認証を行います。 **メモ：**この認証タイプを使用するには、最初に Starling Connect コネクタを登録する必要があります。詳細については、「登録済みコネクタ」を参照してください。
ローカルシステムアカウント	SQL Server 資産の場合、SQL データベースをホストしているサーバー上の Windows ユーザーアカウントであるローカルシステムアカウントを使用して資産を認証します。
パスワード（ローカルサービスアカウント）	ローカルサービスアカウントとパスワードを使用して資産を認証します。
アカウントパスワード	関数アカウントの資格情報がカスタムスクリプトにない場合（Amazon Web Services など）。詳細については、「クラウドプラットフォームアカウントの追加」を参照してください。
アクセスキー	Amazon Web Services 資産の場合、アクセスキーを使用して資産を認証します。詳細については、「クラウドプラットフォームアカウントの追加」を参照してください。
カスタム	カスタムパラメータまたはカスタマープラットフォームスクリプトのパラメーターが使用されるため、認証情報は取得されません。資産に関連付けられているアカウントは保存されません。詳細については、「カスタムプラットフォーム」を参照してください。
なし	認証情報は取得されず、確認/変更機能は無効となります。資産に関連付けられたアカウントは保存されません。

認証タイプ	説明
	SPP は、サービスアカウントの資格情報の種類として**［なし］**を選択した場合でも、検出された資産の SSH ホストキーを検出します。
接続のテスト	指定したサービスアカウントの資格情報を使用して、SPP が資産にログインできることを確認します。
タイムアウト	接続コマンドのタイムアウトの両方を待つ時間（秒）を入力します。

クライアント ID：SAP 資産の場合、クライアント ID を入力します。

カスタムプロパティ

接続タブの**［プラットフォーム］**フィールドがカスタムプラットフォームを識別した場合、カスタムプラットフォームスクリプトのカスタムプロパティに基づいてダイアログを完成させます。SPP は、値が文字列、ブーリアン、整数、パスワード（API スクリプトでは secret と呼ばれる）を含むプロパティのタイプと一致するかどうかをチェックします。SPP は、カスタムプラットフォームに入力された値の有効性やシステムへの影響をチェックできません。詳細については、「カスタムプラットフォームスクリプトの作成」を参照してください。

サービスアカウントについて

SPP は、資産に接続し、その資産上のアカウントとパスワードを安全に管理するために、サービスアカウントを使用します。そのため、サービスアカウントには、他のアカウントのパスワードを編集するための十分な権限が必要です。

資産を追加すると、SPP はそのサービスアカウントを「アカウント」のリストに追加します。デフォルトでは、SPP は、その資産を管理するプロファイルの確認および変更スケジュールに従って、サービスアカウントのパスワードと SSH キーを自動的に管理します。「パスワードプロファイルの追加」と「SSH キープロファイルの作成」を参照してください。

サービスアカウントを追加すると、SPP は自動的にそのアカウントをアクセスリクエストから無効化します。パスワードまたは SSH キーをリリースできるようにするには、**［アクセスリクエスト］**をクリックして、**［パスワードリクエストの有効化］［パスワードリクエストの有効化］［SSH キーリクエストの有効化の有効化］**を選択します。セッションアクセスを有効にする場合は、**［セッションリクエストを有効にする］**を選択します。

> **ヒント：** ベストプラクティスとして、SPP でサービスアカウントのパスワードまたは SSH キーを管理したくない場合は、そのアカウントをパスワードまたは SSH キーを変更しないように設定したプロファイルに追加してください。

サービスアカウントを削除すると、SPP は資産の認証タイプを**「なし」**に変更し、この資産に関連するすべてのアカウントの自動パスワードまたは SSH キーの管理を無効にします。ユーザーはパスワードまたは SSH キーをチェックアウトし続けることができますが、アカウントを管理するポリシーでリリース後にパスワードまたは SSH キーを変更する必要がある場合、パスワードまたは SSH キーはパスワードリセット保留状態で動かなくなる可能性があります。詳細については、「パスワードまたは SSH キーのリセットが保留されている」を参照してください。

接続のテスト

SPP で障害が発生する最も一般的な原因は、アプライアンスと管理システム間の接続性の問題、またはサービスアカウントの問題のいずれかです。問題が発生した場合、まず、サービスアカウントを使用して、SPP とは無関係の別のシステムから管理対象システムにアクセスできることを確認します。接続の問題のトラブルシューティングの詳細については、「接続のテストが失敗する」および「接続障害」を参照してください。

接続のテストについて

資産を追加する際、**[接続のテスト]** は SPP が提供したサービスアカウントの資格情報を使用して資産にログインできることを確認します。

SSH ホストキーを必要とする資産を追加する場合、**[接続のテスト]** はまずキーを検出し、承諾のためにそれを表示します。ユーザーが承諾すると、**[接続のテスト]** はユーザーが設定したサービスアカウント資格情報を使用して資産にログインできることを確認します。

新しい資産を保存すると、SPP はサービスアカウントの認証情報を保存します。SPP は、これらの資格情報を使用して資産に接続し、その資産上のアカウントとパスワードを安全に管理します。詳細については、「サービスアカウントについて」を参照してください。

既存の資産の接続を確認する場合は、Web クライアントで **[接続のテスト]** ボタンを使用します。詳細については、「資産の接続性の確認」を参照してください。

[ドメイン コントローラの指定] に値を入力した場合、SPP がリスト内でドメインコントローラーを見つけられないと、テスト接続は失敗し、エラーが返されます。

SSH キー

接続タブでは、SSH 認証キーを使用して管理対象システムを認証するように SPP を設定することができます。SSH キーをローテートするには、資産のプロファイル変更スケジュールで**［SSH キーの管理］**オプションを選択する必要があります。詳細については、「SSH キー変更設定の追加」を参照してください。

> **メモ：** このオプションは、すべてのオペレーティングシステムで使用できるわけではありません。しかし、SPP 資産が SSH ホストキーを必要とし、それを持っていない場合、「SSH キーのチェック」、「SSH キーの変更」、「接続のテスト」は失敗します。詳細については、「接続障害」を参照してください。

表示される情報は、SSH キーを自動的に生成するか、SSH キーをインポートして手動で配備するかを選択した場合に異なります。

表：SSH キー認証タイププロパティ

プロパティ	説明
新しい SSH キーを自動的に生成して展開します	以下のオプションのいずれかを選択します： • 新しい SSH キーを自動的に生成して展開します。 　◦ **［パスワード］**フィールドに、SSH キーのパスワードを入力します。 • 新しい SSH キーを自動的に生成して自分で展開します。 • SSH キーをインポートして自分で展開します。 **メモ：** SPP は、現在、authorized key のオプションを管理していません。インポートされた鍵に、資産上の authorized key ファイルで構成されたオプションがある場合、SPP によって鍵がローテートされたときに、これらのオプションは保持されません。 1. **［参照］**をクリックします。**［SSH キーのインポート］**ダイアログで**［参照］**をクリックし、秘密キーファイルを選択します。 2. 必要な場合は、**パスワード**を入力します。秘密キーが暗号化されている場合、パスワードが必要です。 3. **［インポート］**をクリックします。

プロパティ	説明
キーのコメント	（任意）SSH キーの説明を入力します。最大 255 文字
アカウント名	SPP が管理タスクに使用するサービスアカウント名を入力します。これは、SPP が資産に SSH 認証キーをインストールするために使用するアカウントです。詳細については、「サービスアカウントについて」を参照してください。
権限昇格コマンド	必要であれば、特権昇格コマンド（sudo など）を入力します。これは、システム上で特権的なアクセスを必要とするコマンドや、Unix ベースのシステムでアカウントを管理するコマンド、つまり、SSH キーの確認と変更、アカウントの検出のための接頭辞として使用されます。 sudo コマンドには以下が続きます： • AuthorizedKeyCommand ユーザーの公開鍵を検索するプログラムを指定します。 • cat • chmod • chown • chuser • cp • dscacheutil • dscl • echo • egrep • find • grep • host • ls • mkdir • modprpw (hpux only) • mv • psswd • pwdadm • rm • sed • sshd • ssh-keygen • tee • test • touch • usermod 資産を追加する際、このコマンドで**［接続のテスト］**を行います。詳細については、「接続のテスト」を参照してください。

プロパティ	説明
	特権昇格コマンドは、非対話的に、つまりパスワードの入力を求めずに実行する必要があります。詳細については、「Unix ベースシステムの準備」を参照してください。 上限は 255 文字です。
SSH ホストキーの自動承認	このオプションを選択すると、SPP の資産を作成する際に、SSH ホストキーを自動的に受け入れます。 このオプションを選択すると、SPP は検出された SSH ホストキーのサムプリントを表示します。SSH ホストキーが必要な管理対象システムにキーがない場合、SSH キーのチェックは失敗します。詳細については、「接続障害」を参照してください。
接続のテスト	このボタンをクリックすると、SPP が提供したサービスアカウント資格情報を使用してこの資産にログインできることを確認できます。詳細については、「接続のテスト」を参照してください。
ポート	管理対象システムにログインするために SSH で使用するポート番号を入力します。必須
接続のタイムアウト	接続タイムアウトとコマンドタイムアウトの両方の待ち時間を入力します（秒）。デフォルト：20 秒
（カスタムプラットフォームオペレーション 例：システムプロパティの確認）	カスタムプラットフォームスクリプトにカスタムパラメータがある場合、ここにカスタムパラメータを入力します。システムパラメータの一覧はこちらです。リストにないパラメーターは、カスタムパラメータとなります。

ディレクトリアカウント

> **メモ：**部のタイプのディレクトリ アカウントでのみ利用可能です。

接続タブでは、Microsoft Active Directory などの外部 ID ストアからのアカウントを使用して管理対象システムに認証するように SPP を設定できます。この認証タイプを使用するには、まず SPP にディレクトリ資産を追加し、ドメインユーザーアカウントを追加する必要があります。管理アカウントユーザーは、Protected Users AD Security グループのメンバーにはなれません。詳細については、「アカウント」を参照してください。

表：ディレクトリアカウント認証タイププロパティ

プロパティ	説明
サービスアカウント名	**［アカウント名］**をクリックします。管理タスクに使用するサービスアカウント名を選択します。選択可能なアカウントは、事前に SPP に追加したディレクトリにリンクされているドメインユーザーアカウントです。
サービスアカウントパスワード	必要な場合は、認証に使用するパスワードを入力します。
権限昇格コマンド	必要であれば、特権昇格コマンド（sudo など）を入力します。これは、システム上で特権的なアクセスを必要とするコマンドや、Unix ベースのシステムでアカウントを管理するコマンド、つまり、SSH キーの確認と変更、アカウントの検出のための接頭辞として使用されます。 sudo コマンドには以下が続きます： • AuthorizedKeyCommand ユーザーの公開鍵を検索するプログラムを指定します。 • cat • chmod • chown • chuser • cp • dscacheutil • dscl • echo • egrep • find • grep • host • ls • mkdir • modprpw (hpux only) • mv • psswd • pwdadm • rm • sed • sshd • ssh-keygen • tee • test • touch • usermod

プロパティ	説明
	資産を追加する際、このコマンドで**［接続のテスト］**を行います。詳細については、「接続のテスト」を参照してください。 特権昇格コマンドは、非対話的に、つまりパスワードの入力を求めずに実行する必要があります。詳細については、「Unix ベースシステムの準備」を参照してください。 上限は 255 文字です。
接続のテスト	このボタンをクリックすると、SPP が提供したサービスアカウント資格情報を使用してこの資産にログインできることを確認できます。詳細については、「接続のテスト」を参照してください。
サービスアカウントパスワードプロファイル	**［参照］**をクリックしてプロファイルを追加するか、**［削除］**をクリックして割り当てられたプロファイルを削除します。利用可能なプロファイルは、［全般］タブ（資産検出）で選択したパーティションに基づきます。プロファイルを後で更新するには、サービスアカウントに移動してプロファイルを更新します。詳細については、「プロパティ(アカウント)」を参照してください。
サービスアカウント接続に名前付きパイプを使用	資産に接続する際に名前付きパイプを使用することを選択します。資産に接続するときに TCP/IP を使用する場合は、このチェックボックスをオフにします。
SSL 暗号化の使用	デフォルトで選択されているこのオプションは、Safeguard がこの資産との通信を暗号化するために使用します。 Active Directory で SSL をサポートするには、Active Directory フォレストで使用されている SSL 証明書をアップロードする必要があります。SSL バインドはポート 636 にする必要があります。Active Directory 内のこのプロセスについては、「サード パーティ証明機関を使用して SSL 経由で LDAP を有効にする」を参照してください。 暗号化を強制するように構成されている MicrosoftSQL Server でこのオプションを選択しない場合、テスト接続は信頼されていない暗号化を使用し、有効な資格情報で成功します。Safeguard データベースサーバーが SSL を使用する方法

プロパティ	説明
	の詳細については、「SPP データベースサーバーでどのように SSL を使用しますか？」を参照してください。
SSL 証明書の検証	このオプションを使用して、資産での SSL 証明書の検証を有効または無効にします。有効にすると、SPP が資産に接続するたびに、資産が提示する証明書の署名権限を 信頼できる CA 証明書ストアにある証明書と比較します。SPP が資産を管理するには、信頼が確立されている必要があります。SPP が SSL 証明書を検証するには、資産の署名機関証明書を信頼できる CA 証明書ストアに追加する必要があります。**［SSL 証明書の検証］**オプションは、資産との信頼関係を確立しない場合にのみクリアしてください。
特権レベルパスワード	必要に応じて、Cisco 構成へのアクセスを許可するための system enable パスワードを入力します。
SSH ホストキーの自動承認	SPP が SSH ホストキーを自動的に受け入れるようにするには、このオプションを選択します。SSH ホストキーが必要な資産に SSH ホストキーがない場合、パスワードの確認は失敗します。詳細については、「接続障害」を参照してください。
インスタンス	この資産に SQL Server の複数のインスタンスを構成している場合、インスタンス名を指定します。ホスト上に SQL Server のデフォルト（無名）インスタンスを構成している場合は、IP アドレスとポート番号を指定する必要があります。
ポート	資産にログインするためのポート番号を入力します。このオプションは、すべてのオペレーティングシステムで使用できるわけではありません。
接続のタイムアウト	ディレクトリ接続のタイムアウト時間を入力します。デフォルト：20 秒

Starling Connect

接続タブでは、SPP を設定して、Starling Connect に登録されているコネクタを認証することができます。この認証タイプを使用するには、まず Starling Connect のコネクタを登録する必要があります。詳細については、「登録済みコネクタ」を参照してください。

表：Starling Connect 認証タイプのプロパティ

プロパティ	説明
接続のテスト	このボタンをクリックすると、SPP が提供したサービスアカウント資格情報を使用してこの資産にログインできることを確認できます。詳細については、「接続のテスト」を参照してください。
接続のタイムアウト	接続のタイムアウト時間を入力します。デフォルト：20 秒

ローカルシステムアカウント

接続タブでは、SPP を設定して、ローカルシステムアカウントとパスワードを使って管理対象 SQL Server を認証することができます。ローカルシステムアカウントは、SQL データベースをホストしているサーバー上の Windows ユーザーアカウントです。

> **メモ:** この認証タイプを使用するには、SPP に Windows 資産と SQL Server 資産の両方を追加する必要があります。

表：ローカルシステムアカウント認証タイプのプロパティ

プロパティ	説明
接続のテスト	このボタンをクリックすると、SPP が提供したローカルシステムアカウントの資格情報を使用してこの資産にログインできることを確認できます。詳細については、「接続のテスト」を参照してください。
SSL 暗号化の使用	このオプションを選択すると、Safeguard がこの資産との通信を暗号化できるようになります。強制的に暗号化するように構成されている Microsoft SQL Server でこのオプションを選択しない場合、**［接続のテスト］**は信頼されていない暗号化を使用し、有効な資格情報を使用して成功します。 Safeguard データベースサーバーが SSL を使用する方法の詳細については、「SPP データベースサーバーでどのように SSL を使用しますか？」を参照してください。
SSL 証明書の検証	このオプションを使用して、資産での SSL 証明書の検証を有効または無効にします。有効にすると、SPP が資産に接続するたびに、資産が提示する証明書の署名権限を 信頼できる

プロパティ	説明
	CA 証明書ストアにある証明書と比較します。SPP が資産を管理するには、信頼が確立されている必要があります。SPP が SSL 証明書を検証するには、資産の署名機関証明書を信頼できる CA 証明書ストアに追加する必要があります。**[SSL 証明書の検証]**オプションは、資産との信頼関係を確立しない場合にのみクリアしてください。
インスタンス/サービス名	この資産に SQL Server の複数のインスタンスを構成している場合、インスタンス名を指定します。ホスト上に SQL Server のデフォルト（無名）インスタンスを構成している場合は、IP アドレスとポート番号を指定する必要があります。 Oracle プラットフォームの場合、Oracle でターゲットシステムを識別するために TNSNAMES 命名方法を使用します。Oracle 環境の構成に応じて、インスタンス（Oracle では SID とも呼ばれる）および/またはサービス名（ServiceName）を使用して、ターゲットデータベースを識別することができます。
ポート	資産にログインするためのポート番号を入力します。
接続のタイムアウト	接続タイムアウトとコマンドタイムアウトの両方の待ち時間を入力します（秒単位）。デフォルト：20 秒

パスワード（ローカルサービスアカウント）

接続タブでは、ローカルのサービスアカウントとパスワードを使用して管理対象システムを認証するように SPP を設定することができます。

> **メモ：** 一部のオプションは、すべてのオペレーティングシステムで使用できるわけではありません。

表：パスワード認証タイプのプロパティ

プロパティ	説明
識別名	LDAP プラットフォームの場合、サービスアカウントの完全修飾識別名（FQDN）を入力します。 例：cn=dev-sa,ou=people,dc=example,dc=com

プロパティ	説明
サービスアカウント識別名	**［参照］**して SPP が管理タスクに使用するサービスアカウントを選択します。資産を追加すると、SPP は自動的にサービスアカウントをアカウントに追加します。詳細については、「サービスアカウントについて」を参照してください。 識別名を使用する LDAP プラットフォームを除き、必須です。
パスワード	この資産への認証に使用するサービスアカウントのパスワードを入力します。 制限：255 文字
権限昇格コマンド	必要であれば、特権昇格コマンド（sudo など）を入力します。これは、システム上で特権的なアクセスを必要とするコマンドや、Unix ベースのシステムでアカウントを管理するコマンド、つまり、SSH キーの確認と変更、アカウントの検出のための接頭辞として使用されます。 sudo コマンドには以下が続きます： • AuthorizedKeyCommand ユーザーの公開鍵を検索するプログラムを指定します。 • cat • chmod • chown • chuser • cp • dscacheutil • dscl • echo • egrep • find • grep • host • ls • mkdir • modprpw (hpux only) • mv • psswd • pwdadm • rm • sed • sshd • ssh-keygen • tee • test • touch • usermod

プロパティ	説明
	資産を追加する際、このコマンドで**［接続のテスト］**を行います。詳細については、「接続のテスト」を参照してください。 特権昇格コマンドは、非対話的に、つまりパスワードの入力を求めずに実行する必要があります。詳細については、「Unix ベースシステムの準備」を参照してください。 上限は 255 文字です。
特権レベルパスワード	必要に応じて、Cisco 構成へのアクセスを許可するための enable パスワードを入力します。
SSH ホストキーの自動承認	このチェックボックスはデフォルトで選択されており、SPP が SSH ホストキーを自動的に受け入れることを示します。このオプションは、すべてのプラットフォームで使用できるわけではありません。 SSH ホストキーが検出されると、SSH ホストキーのフィンガープリントが表示されます。 SSH ホストキーを必要とする資産に SSH ホストキーがない場合、パスワードの確認は失敗します。詳細については、「接続障害」を参照してください。
接続のテスト	このボタンをクリックすると、SPP が提供したサービスアカウント資格情報を使用してこの資産にログインできることを確認できます。詳細については、「接続のテスト」を参照してください。
サービスアカウントパスワードプロファイル	**［参照］**をクリックしてプロファイルを追加するか、**［削除］**をクリックして割り当てられたプロファイルを削除します。利用可能なプロファイルは、全般タブ（資産検出）で選択したパーティションに基づきます。プロファイルを後で更新するには、サービスアカウントに移動してプロファイルを更新します。詳細については、「プロパティ（アカウント）」を参照してください。
サービスアカウントの SSH キープロファイル	**［参照］**をクリックしてプロファイルを追加するか、**［削除］**をクリックして割り当てられたプロファイルを削除します。利用可能なプロファイルは、全般タブ（資産検出）で選択したパーティションに基づきます。プロファイルを後で更

プロパティ	説明
	新するには、サービスアカウントに移動してプロファイルを更新します。詳細については、「プロパティ（アカウント）」を参照してください。
SSL 暗号化の使用	このオプションは、Safeguard がこの資産との通信を暗号化するために使用します。 暗号化を強制するように構成されている MicrosoftSQL Server でこのオプションを選択しない場合、テスト接続は信頼されていない暗号化を使用し、有効な資格情報で成功します。Safeguard データベースサーバーが SSL を使用する方法の詳細については、「SPP データベースサーバーでどのように SSL を使用しますか？」を参照してください。
SSL 証明書の検証	このオプションを使用して、資産での SSL 証明書の検証を有効または無効にします。有効にすると、SPP が資産に接続するたびに、資産が提示する証明書の署名権限を 信頼できる CA 証明書ストアにある証明書と比較します。SPP が資産を管理するには、信頼が確立されている必要があります。SPP が SSL 証明書を検証するには、資産の署名機関証明書を信頼できる CA 証明書ストアに追加する必要があります。**[SSL 証明書の検証]** オプションは、資産との信頼関係を確立しない場合にのみクリアしてください。
権限として（As Privilege）	選択した Oracle サービスアカウントで接続する際に使用する Oracle 権限レベルを指定します（必要な場合）。Oracle SYS アカウントは、SYSDBA または SYSOPER の特権レベルを必要とします。詳細については、Oracle ドキュメント「About Administrative Accounts and Privileges」および「SYSDBA and SYSOPER System Privileges」を参照してください。
インスタンス/サービス名	SQL Server プラットフォームの場合、この資産に SQL Server の複数のインスタンスを構成している場合は、インスタンス名を指定します。ホスト上に SQL Server のデフォルト（無名）インスタンスを構成している場合は、IP アドレスとポート番号を指定する必要があります。 Oracle プラットフォームの場合、TNSNAMES 命名法を使用して、Oracle でターゲットシステムを識別します。Oracle 環境の構成に応じて、インスタンス（Oracle では SID とも呼ば

プロパティ	説明
	れる）および/またはサービス名（ServiceName）を使用して、ターゲットデータベースを識別することができます。
ワークステーション ID	構成されたワークステーション ID を指定します（該当する場合）。このオプションは IBM i システム用です。
ポート	資産が接続をリッスンするポート番号を入力します。 デフォルト：ポート 22、SQL サーバーの場合はポート 1433、SonicWALL SMA または CMS アプライアンスの場合はポート 8443。
接続のタイムアウト	接続タイムアウトとコマンドタイムアウトの両方を待つ時間（秒）を入力します。デフォルト：20 秒

アクセスキー

接続タブでは、アクセスキーを使用して管理対象システムを認証するように SPP を設定できます。

表：アクセスキー認証タイプのプロパティ

プロパティ	説明
サービスアカウント名	SPP が管理タスクに使用するアカウントを入力します。詳細については、「サービスアカウントについて」を参照してください。
アクセスキーID	秘密キーに関連付けられた一意の識別子を入力します。アクセスキーID と秘密キーは、プログラムによる AWS リクエストに暗号的に署名するために一緒に使用されます。 上限：英数字 32 文字
シークレットキー	プログラムによる Amazon Web Services (AWS)リクエストに暗号署名するために使用するシークレットアクセスキーを入力します。 上限：40 文字（英数字）、「+」「/」も使用可能です。
接続のテスト	このボタンをクリックすると、SPP が提供したサービスアカウント資格情報を使用してこの資産にログインできることを

	確認できます。詳細については、「接続のテスト」を参照してください。
ポート	資産にログインするためのポート番号を入力します。
接続のタイムアウト	接続タイムアウト時間（秒）を入力します。 デフォルト：20 秒

なし

接続タブの資産の**［認証タイプ］**が**「なし」**に設定されている場合、SPP は資産に関連するアカウントを管理せず、資産関連の資格情報を保存しません。

資産に関連するアカウントのパスワードを確認および変更するためには、すべての資産にサービスアカウントが必要です。

SPP がアーカイブサーバーを作成するときに SSH ホストキーを自動的に受け入れるようにするには、**［SSH ホストキーの自動承認］**を選択します。詳細については、「アーカイブサーバーの追加」を参照してください。

管理タブ

［資産管理］＞［資産］＞［管理］タブを使用して、資産が割り当てられているパーティションとプロファイルを追加します。資産は、一度に 1 つのパーティションにのみ存在できます。資産をパーティションに追加すると、その資産に関連するすべてのアカウントが自動的にそのパーティションに追加されます。すべての資産は、プロファイルによって管理される必要があります。新しい資産は、特に指定がない限り、自動的にデフォルトのプロファイルで管理されます。

資産に関する設定を以下に示します。

表：資産：管理タブのプロパティ

プロパティ	説明
	この資産のアカウントを管理するためのパスワードプロファイルを**［参照］**をクリックして選択します。
パスワードプロファイル	すべての資産をプロファイルに割り当てる必要があります。新しい資産はすべて、別のプロファイルを指定しない限り、デフォルトのプロファイルに割り当てられます。特定のプロファイルをデフォルトとして設定することができます。詳細

プロパティ	説明
	については、「デフォルトプロファイルの設定」を参照してください。 **［選択の消去］**をクリックすると、プロファイルが現在のデフォルトに設定されます。 **［選択の消去］**ボタンは、資産がプロファイルに明示的に割り当てられている場合にのみ有効になります。資産がプロファイルに暗黙的に割り当てられているだけの場合、**［選択の消去］**ボタンはアクティブになりません。資産をプロファイルに明示的に割り当てない場合、その資産は常に現在のデフォルトのプロファイルに割り当てられます。
SSH キープロファイル	この資産のアカウントを管理するための SSH キーのプロファイルを**［参照］**して選択します。 すべての資産をプロファイルに割り当てる必要があります。別のプロファイルを指定しない限り、すべての新しい資産はデフォルトのプロファイルに割り当てられます。特定のプロファイルをデフォルトとして設定することができます。詳細については、「デフォルトプロファイルの設定」を参照してください。 **［選択の消去］**をクリックすると、プロファイルが現在のデフォルトに設定されます。 **［選択の消去］**ボタンは、資産がプロファイルに明示的に割り当てられている場合にのみ有効になります。資産がプロファイルに暗黙的に割り当てられているだけの場合、**［選択の消去］**ボタンはアクティブになりません。資産をプロファイルに明示的に割り当てない場合、その資産は常に現在のデフォルトのプロファイルに割り当てられます。
セッションリクエストの有効化	該当する場合、このチェックボックスはデフォルトで選択されており、承認されたユーザーがこの資産のセッションアクセスをリクエストできることを示します。 この資産のセッションリクエストを許可しない場合は、このチェックボックスをオフにします。資産がセッションに対して無効になっており、その資産のアカウントがセッションに対して有効になっている場合、その資産はセッションを許可していないため、セッションを利用できません。

プロパティ	説明
すべてのパーティションで検出利用	LDAP、Red Hat Directory Server、eDirectory LDAP 資産で使用できます。このチェックボックスを選択すると、資産をすべてのパーティションで検出できるようになります。
ハッシュパスワードを使用した管理	LDAP、Red Hat Directory Server、eDirectory LDAP 資産で使用できます。このチェックボックスを選択すると、パスワード変更操作の実行時に Safeguard によってパスワードの暗号化が実行されることを示します。
管理対象ネットワーク	作業負荷分散のために割り当てられている管理ネットワーク。詳細については、「管理対象ネットワーク」を参照してください。

属性タブ

> **メモ：属性**タブは、新しい資産を正常に追加した後にのみ表示され、資産を編集することでアクセスできます。

Web クライアントでは、属性タブはディレクトリ資産（Active Directory および LDAP を含む）に属性を追加するために使用されます。詳細については、「ID と認証プロバイダの追加」を参照してください。

> **重要:** 一部の Active Directory 属性は固定されており、変更することはできません。

表：Active Directory と LDAP：属性タブ

SPP 属性	ディレクトリ属性
ユーザー	
オブジェクトクラス	デフォルト：Active Directory の場合は user、LDAP の場合は inetOrgPerson **［参照］**をクリックして、ユーザーオブジェクトクラスの有効な属性を定義するクラス定義を選択します。
ユーザー名	Active Directory の場合は sAMAccountName、LDAP の場合は cn
パスワード	LDAP の userPassword

SPP 属性	ディレクトリ属性
説明	description
MemberOf	デフォルトでは空白ですが、この属性には、ユーザーがメンバーであるディレクトリグループのリストを含むディレクトリスキーマ属性を設定することができます。
代替ログイン名	userPrincipalName **メモ：**デフォルトでは、ディレクトリの代替ログイン名属性は userPrincipalName に設定されていますが、 UPN タイプのアカウント名を含む別のディレクトリ属性を使用することもできます。 この属性は、API の UseAltLoginName 設定（デフォルトでは無効）と併用することで、アカウント名として代替ログイン名を使用することができます。API は PUT https://<host>/service/core/v3/AccessPolicies/{id} で、{id} は UseAltLoginName を true に設定する accessPolicy の id である。UseAltLoginName は、資産データオブジェクトのブール型フィールドです。
グループ	
オブジェクトクラス	デフォルト：Active Directory の場合は group、LDAP の場合は groupOfNames **［参照］**をクリックして、コンピューターオブジェクトクラスの有効な属性を定義するクラス定義を選択します。
名前	Active Directory の場合は sAMAccountName、LDAP の場合は cn
メンバー	member
コンピューター	
オブジェクトクラス	デフォルト：Active Directory の場合は computer、LDAP の場合は ipHost **［参照］**をクリックして、コンピューターオブジェクトクラスの有効な属性を定義するクラス定義を選択します。
名前	cn

SPP 属性	ディレクトリ属性
ネットワークアドレス	Active Directory の場合は dNSHostName、LDAP の場合は ipHostNumber
オペレーティングシステム	ActiveDirectory の operatingSystem
オペレーティングシステムのバージョン	ActiveDirectory の operatingSystemVersion
説明	description

資産の接続性の確認

資産を追加した後、**［接続のテスト］**オプションを使用して、SPP がその資産にログインできることを確認することができます。

> **メモ：**資産の**接続**タブから**［接続のテスト］**を実行する場合（最初に資産を追加するときなど）、サービスアカウントの資格情報を入力する必要があります。資産を SPP に追加すると、これらの資格情報が保存されます。
>
> **［接続のテスト］**オプションでは、保存された資格情報を使用してその資産にログインできることを確認するため、サービスアカウントの資格情報を入力する必要はありません。

資産の接続確認手順

1. **［資産管理］** > **［資産］**を開きます。
2. 資産を選択します。
3. **［接続のテスト］**ボタンを選択します。

   SPP は、タスクペインに結果を表示します。

資産をパーティションに割り当て

資産をパーティションに割り当てるには、**資産**ビューを使用します。資産は、一度に 1 つのパーティションにしか配置できません。資産をパーティションに追加すると、その資産に関連付けられているすべてのアカウントも自動的にそのパーティションに追加されます。

パーティションから資産を削除することはできません。ただし、他のパーティションのスコープまたは資産の**プロパティ**タブから、その資産を他のパーティションに追加することはできます。

資産をパーティションに割り当てる手順

1. **［資産管理］**>**［資産］**に移動します。
2. 資産を選択し、**［詳細の表示］**をクリックします。
3. **［パーティション］**フィールドの**［参照］**をクリックします。
4. パーティションを選択し、**［パーティションの選択］**をクリックします。
5. **［OK］**をクリックして変更を保存します。

資産にプロファイルを割り当て

資産ビューを使用して、プロファイルを資産に割り当てます。

資産にプロファイルを割り当てる手順

1. **［資産管理］**>**［資産］**へ移動します。
2. 資産を選択して**［詳細の表示］**をクリックします。
3. 管理の**［編集］**をクリックします。
4. **［パスワードプロファイル］**フィールドの**［参照］**ボタンをクリックしてプロファイルを選択し、**［パスワードプロファイルの選択］**をクリックします。選択した資産のパーティションにあるプロファイルのみを選択することができます。
5. **［OK］**をクリックして変更を保存します。

資産にタグを手動で追加

資産管理者は、**資産**ビューで資産を選択したときに**全般**タブの下部にある**［タグ］**ペインを使用して、資産に静的タグを手動で追加および削除することができます。

ルールによって定義され、稲妻のアイコンが表示されている動的なタグを手動で削除することはできません。動的タグを削除するには、そのタグに関連付けられたルールを変更する必要があります。詳細については、「資産または資産アカウントのタグの変更」を参照してください。

資産にタグを手動で追加する手順

1. **［資産管理］＞［資産］**に移動します。
2. 資産を選択して **［詳細の表示］**をクリックします。
3. **［タグ］**の **［編集］**をクリックします。
4. 以下のいずれかの方法で資産にタグを割り当てます：。
    - 以前に作成されたタグを割り当てる場合：
        a. **［タグの追加］**をクリックします。
        b. **［タグの選択］**ダイアログで、資産に追加するタグを選択します。
        c. **［タグの選択］**をクリックして、選択内容を保存します。
    - 新しいタグを作成する場合：
        a. **［タグの追加］**をクリックします。
        b. **［タグの選択］**ダイアログで、**［新しいタグ］**をクリックします。
        c. タグに必要な情報を入力し、**［OK］**をクリックします。
        d. 新しいタグの追加が完了したら、資産に追加するタグを選択します。
        e. **［タグの選択］**をクリックし、選択内容を保存します。
5. **［OK］**をクリックします。

資産にアカウントを追加

資産にアカウントを追加するには、資産ビューの**アカウント**タブを使用します。

ドメインコントローラー（DC）資産でタスクとサービスを管理することができます。詳細については「ドメインコントローラー（DC）資産の使用」を参照してください。

資産にアカウントを追加する手順

1. **［資産管理］＞［資産］**に移動します。

2. 資産を選択し、**［詳細の表示］**タブを開きます。
3. **［アカウント］**タブを開きます。
4. 詳細ツールバーから**［新しいアカウント］**をクリックします。
5. **［全般］**タブで、次の情報を入力します。
    - **名前**：
        - ローカルアカウント：このアカウントのログインユーザー名を入力します。制限：100 文字。
        - ディレクトリアカウント：**［参照］**してアカウントを見つけます。
    - **説明**:（任意）この管理アカウントに関する情報を入力します。制限：255 文字。
6. **［管理］**タブで、次の情報を入力します。
    - **パスワードリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してパスワードリリースリクエストが有効であることを示しています。このオプションをオフにすると、誰かがこのアカウントのパスワードをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは、自分が承認されたユーザーである資格の範囲内で、任意のアカウントのパスワードをリクエストできます。
    - **セッションリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してセッションアクセスリクエストが有効であることを示しています。このオプションをオフにすると、誰かがこのアカウントを使用してセッションアクセスをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは、自分が認証ユーザーである資格の範囲内で任意のアカウントに対してアクセスリクエストを行うことができます。
    - **パスワードプロファイル：**このアカウントを管理するプロファイルを選択します。デフォルトでは、アカウントは関連する資産のプロファイルを継承しますが、このパーティションのために別のプロファイルを割り当てることができます。詳細については、「パスワードプロファイルと SSH キープロファイルに資産またはアカウントを割り当て」を参照してください。
    - （ディレクトリアカウントのみ）**すべてのパーティションで使用可能**：選択した場合、どのパーティションでもこのアカウントを使用でき、パスワードは他の管理者に渡されます。たとえば、このアカウントは、他の資産の依存アカウントやサービスアカウントとして使用することができます。潜在的には、このアカウントとしてサービスを実行している資産があり、サービスアカウントが変更されたときに、それらの資産を更新することができるかもしれません。選

択しない場合、パーティションの所有者や他のパーティションは、そのアカウントの存在を知ることはありません。アーカイブサーバーはパーティションにバインドされませんが、アーカイブサーバーがディレクトリアカウントで構成されている場合は、このオプションを選択する必要があります。

7. **［OK］**をクリックして資産へのアカウント追加を保存します。

ディレクトリ資産

ディレクトリ資産にディレクトリユーザーアカウントを追加すると、SPP は設定したプロファイルのスケジュールに従ってユーザーパスワードを自動的に変更します。これにより、ディレクトリユーザーが SPP にログインできなくなる可能性があります。ディレクトリユーザーを SPP のユーザーとして設定する方法については、「ユーザーの追加」を参照してください。

Active Directory の場合、ディレクトリ管理タスク（例えば、ディレクトリアカウント、ディレクトリユーザーアカウント、ディレクトリユーザーグループの追加）のために、環境内のすべての Windows グローバルカタログサーバーと SPP アプライアンスが通信するには、ファイアウォールで標準グローバルカタログポート 3268（LDAP）が開いている必要があります。LDAP は、暗号化されていない接続にポート 389 を使用します。詳細については、Microsoft のパブリケーションである「How the Global Catalog Works」を参照してください。

ディレクトリアカウントをディレクトリ資産に追加する手順

1. **［資産管理］**>**［資産］**を開きます。
2. ディレクトリ資産を選択し、**［詳細の表示］**タブを開きます。
3. **［アカウント］**タブを開きます。
4. 詳細ツールバーの **［新しいアカウント］**をクリックします。
5. **［新しいアカウント］**ダイアログで、**［アカウントの選択］**をクリックします。
6. **［アカウントの検索オプション］**ダイアログで以下を行います：
    a. **次で開始（Active Directory ANR 検索）**：このフィールドを使用して、完全または部分的なアカウント名を入力します。
    b. **検索場所：［参照］**ボタンを使用して、ディレクトリ内のコンテナを「検索場所」として選択します。
    c. **サブコンテナのオブジェクトを含める：**チェックボックスはデフォルトで選択されており、子オブジェクトが検索に含まれることを示します。このチェ

ックボックスをオフにすると、子オブジェクトが検索対象から除外されます。

d. **［アカウントの検索］**をクリックしてアカウントを検索します。

7. 検索結果は、**［アカウントの選択］**グリッドに表示されます。SPP に追加するアカウントを選択します。

8. 選択したアカウントを保存するには、**［アカウントの選択］**をクリックします。

9. **［OK］**をクリックして、ディレクトリアカウントをディレクトリ資産に保存します。

アカウントの依存関係を追加

1 つ以上の Windows サーバーは、ホストされているサービスやタスクを実行するために、ディレクトリアカウント（Active Directory アカウントなど）を使用することができます。資産管理者は、ディレクトリアカウントと Windows サーバー間の依存関係を構成できます。SPP は、依存システムの更新を実行し、依存するアカウントを使用するすべてのシステムで、依存するアカウントのパスワードを維持します。例えば、SPP がディレクトリアカウントのパスワードを変更すると、このアカウントを使用するサービスまたはタスクが中断されないように、Windows サーバーのすべての依存アカウントの資格情報を更新します。ナレッジベース記事 KB article 312212 も参照してください。

ドメインコントローラー（DC）資産上のタスクとサービスを管理することができます。詳細については、「ドメインコントローラー（DC）資産の使用」を参照してください。

資産へのアカウントの依存関係の設定

1. ディレクトリアカウント：

   a. アカウントの依存関係を設定する前に、ディレクトリアカウントを追加する必要があります。詳細については、「アカウントの追加」を参照してください。

   b. ディレクトリアカウントから、**［すべてのパーティションで使用可能］**オプションを選択して、ドメインパーティション以外でも使用できるようにします。詳細については、「アカウントの追加」を参照してください。

2. 資産：ターゲットのディレクトリアカウントを資産の依存アカウントとして追加する必要があります。資産が Windows Server プラットフォームである場合、サービスアカウントは、ドメインアカウント（ドメイン情報を検索するため）またはローカルアカウントにすることができます。資産が Windows SSH プラットフォームである場合、依存するア

カウントを更新するために、サービスアカウントはドメインアカウントである必要があります。

> **重要：**Windows SSH 資産の場合、ローカルアカウントは、ドメインアカウントとして実行されているサービスを検出するために必要なアクセス権を持っていません。そのため、ローカルアカウントが使用されている場合、SPP はローカルアカウントとして実行されているサービスのみを検出し、ドメインアカウントの依存性は更新されません。

次の手順を実行します：

a. **［資産管理］>［資産］**に移動します。

b. 資産（Windows サーバーなど）を選択し、**［アカウントの依存関係］**タブを選択します。

c. 詳細ツールバーから ＋ **［アカウントの追加］**をクリックし、1 つ以上のディレクトリアカウントを選択します。SPP では、ディレクトリアカウントのみを選択できます。

3. プロファイル：

a. ターゲットディレクトリアカウントは、依存資産と同じパーティションプロファイルである必要があります。

b. 資産で必要な更新を実行するには、**パスワードの変更**タブで依存資産のプロファイルを設定する必要があります。例えば、**［パスワード変更時にサービスを更新する］**チェックボックスを選択する、などです。詳細については、「パスワードプロファイルの作成」を参照してください。

資産にユーザーまたはユーザーグループを追加

資産にユーザーを追加すると、その資産の所有権を持つユーザーまたはユーザーグループを指定することになります。

資産にユーザーまたはユーザー グループを追加するのは、資産管理者（または委任されたパーティション所有者）の責任です。セキュリティポリシー管理者には、グループを追加する権限のみを持ち、ユーザーを追加する権限は持ちません。詳細については、「管理者のアクセス許可」を参照してください。

資産にユーザーを追加する手順

1. **［資産管理］>［資産］**に移動します。

2. 一覧から資産を選択し、**［詳細の表示］**をクリックします。
3. **所有者**タブを選択します。
4. **［追加］**をクリックします。
5. **ユーザー/ユーザーグループ**ダイアログのリストから、1 人以上のユーザーまたはユーザーグループを選択します。
6. **［所有者の選択］**をクリックして、選択内容を保存します。

資産の削除

資産管理者は、アクティブなアクセスリクエストがある場合でも資産を削除することができます。

> **重要：** 資産を削除すると、その資産に関連するすべての SPP アカウントも永久に削除されます。

資産の削除手順

1. **［資産管理］＞［資産］**へ移動します。
2. 削除する資産を選択します。
3. **［削除］**をクリックします。
4. リクエストを確認します。

アカウント検出タブ（資産の追加）

アカウントの検出タブは、Active Directory 資産が作成された後でのみ使用できます。

アカウントの検出タブのデフォルトは**［アカウント検出は実行しないでください］**です。

アカウント検出へのアクセス

［資産管理］＞［資産］＞（詳細の表示）**＞［アカウント検出］**

次の表で説明する設定は、**アカウント検出**タブから**［追加］**または**［編集］**オプションを使用することで利用できます。

表：アカウント検出タブプロパティ

プロパティ	説明
説明	アカウント検出ジョブの説明を選択すると、設定の詳細が表示されます。 ジョブを追加する場合は ＋ **[追加]**、ジョブを編集する場合は ✎ **[編集]** をクリックします。ドロップダウンをクリックして、**[アカウント検出は実行しないでください]** を選択することもできます。
パーティション	検出された資産またはアカウントを管理するパーティション
検出タイプ	プラットフォームのタイプ（Windows、Unix、ディレクトリなど）
ディレクトリ	アカウント検出のためのディレクトリ
スケジュール	ジョブのスケジュールを制御するには、**[スケジュール]** をクリックします。 **[実行間隔]** を選択すると、入力した実行の詳細に従ってジョブが実行されます（**[実行間隔]** をクリアすると、スケジュールの詳細が失われます）。 • 実行間隔を選択します： ◦ **なし**：設定されたスケジュールに従ってジョブが実行されることはありません。手動でジョブを実行することは可能です。 ◦ **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。 ◦ **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、[**実行間隔 = 2/時間/正時@分 = 15**] と設定します。

プロパティ	説明
	◦ **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。 ◦ **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。 ◦ **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2/月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。 • 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。**＋［追加］**または **-［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、**［時間ウィンドウを使用］**を選択します。 ◦ 開始 22：00：00、終了 23：59：00 ◦ 開始 00：00：00、終了 2：00：00 開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。 **［日数］**、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

プロパティ	説明
	隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。 日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。 スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行が終了すると、そのタスクは次の即時インターバルに再スケジュールされます。
ルール	ルールグリッドは、＋**［追加］**、**［削除］**、**［編集］**、**［コピー］**をクリックして更新することができます。 選択したアカウント検出設定ルールの詳細には、資産のタイプに基づいて次のものが含まれます： • **名前**：検出ジョブの名前 • **ルールタイプ**：何を基準に検索するか。たとえば、検索がアカウントプロパティに基づいている場合、ルールは名前ベースまたはプロパティ制約ベースである可能性があります。詳細については、「アカウント検出ルールの追加」を参照してください。 • **検索場所のフィルタ**：ディレクトリが検索される場合、検索されたディレクトリ内のコンテナです。 • **自動管理**：検出されたアカウントが SPP に自動的に追加される場合は、チェックマークが表示されます。 • **デフォルトパスワードの設定**：ルールによってデフォルトのパスワードが自動的に設定される場合は、チェックマークが表示されます。 • **デフォルトの SSH キーの設定：**ルールによってデフォルトの SSH キーが自動的に設定される場合は、チェックマークが表示されます。 • **パスワードプロファイル**：割り当てられたパスワードプロファイル

プロパティ	説明
	• **同期グループへの割り当て**：ルールがアカウントをパスワード同期グループに自動的に関連付けた場合、チェックマークが表示されます。 • **パスワード同期グループ：**割り当てられたパスワード同期グループの名前 • **SSH キープロファイル：**割り当てられた SSH キープロファイルの名前 • **SSH キー同期グループ：**割り当てられた SSH キー同期グループの名前 • **パスワードリクエストの有効化**：パスワードリリースが可能な場合、チェックマークが表示されます。 • **セッションリクエストの有効化**：セッションアクセスが有効な場合、チェックマークが表示されます。 • **SSH キーリクエストの有効化：**SSH キーリクエストが有効な場合、チェックマークが表示されます。

公開 SSH キーのダウンロード

資産を追加して、(**[資産]**ダイアログの**[接続]**ページで**[SSH ホストキーの自動承認]**設定) SSH キーの自動生成を選択すると、SPP は SSH キーをダウンロードして、資産に手動でインストールできるようにします。

パブリック SSH キーのダウンロード手順

1. **[資産管理]** > **[資産]**に移動します。
2. SSH キー認証タイプの資産を選択します。
3. **[SSH ホストキー]**ドロップダウンを展開し、**[SSH ホストキーのダウンロード]**を選択します。SSH キーは、ブラウザーのファイル ダウンロード設定に従ってダウンロードされます。

10.4 パーティション

パーティションは、委任管理のために資産を分離するために使用できる資産用の名前付きコンテナです。SPP にパーティションを追加するのは、資産管理者の責任です。パーティションを使用すると、複数の資産マネージャーを設定し、それぞれが独自のワークスペースで管理対象システムのパスワードガイドラインを定義することができます。一般的には、地理的な場所、所有者、機能、オペレーティングシステムによって資産をパーティション化します。例えば、SPP を使用すると、Unix 資産をパーティションでグループ化し、Unix 管理者に管理を委任することができます。すべてのパーティションには、パーティション所有者を設定する必要があります。詳細については、「パーティションの追加」を参照してください。

すべての資産、および資産に関連するアカウントをパーティションに割り当てる必要があります。デフォルトでは、SPP はすべての資産とその関連アカウントをデフォルトのパーティションに割り当てますが、別のパーティションをデフォルトに設定することも可能です。

パーティションへのアクセス

［資産管理］＞［パーティション］に移動します。

パーティションをクリックすると、追加の情報とオプションが表示されます：

- **プロパティ**タブ：選択したパーティションに関する一般的な情報が表示されます。
- **資産**タブ：選択したパーティションに割り当てられている資産が表示されます。
- **アカウント**タブ：選択したパーティションに割り当てられているアカウントが表示されます。
- **所有者**タブ：パーティションの所有者の情報が表示されます。
- **パスワードプロファイル**タブ：このパーティションに関連付けられたプロファイルが表示されます。パーティションを追加すると、そのパーティションにデフォルトの資産プロファイルが作成されます。デフォルトのプロファイルは、編集は可能ですが、削除はできません。
- **SSH キープロファイル**タブ：このパーティションに関連する SSH キープロファイルが表示されます。
- **履歴**タブ：選択したパーティションに影響を与えた各操作の詳細が表示されます。

ツールバーボタンを使用して、パーティションを管理します。

- **＋［新しいパーティション］**： SPP にパーティションを追加します。詳細については、「パーティションの追加」を参照してください。

- **[削除]**：選択したパーティションを削除します。詳細については、「パーティションの削除」を参照してください。
- **[詳細を表示]**：パーティションを選択し、このボタンをクリックすると、パーティションの追加情報およびオプションが表示されます。
- **[デフォルトとして設定]**：パーティションをデフォルトとして設定します。追加した新しい資産はすべて、デフォルトパーティションに自動的に割り当てられます。詳細については、「デフォルトパーティションの設定」を参照してください。
- **[エクスポート]**：このボタンを使用して、リストされたデータを JSON または CSV ファイルとしてエクスポートします。詳細については、「データのエクスポート」を参照してください。
- **[更新]**：パーティションのリストを更新します。
- **[検索]**：文字列または選択した属性で、条件を入力して検索できます。選択した属性で検索するには、**[検索]** をクリックして、検索する属性を選択します。詳細については、「検索ボックス」を参照してください。

10.4.1 プロファイルとは

プロファイルには、パーティションに割り当てられた資産や資産のアカウントに適用されるスケジュールやルールが含まれています。例えば、パーティションプロファイルは、資産やアカウントでパスワードチェックが必要な頻度を定義します。

パーティションは、必要に応じて複数のパーティションプロファイルを持つことができ、それぞれが異なる資産に割り当てられます。アカウントは、1 つのプロファイルによってのみ管理されます。アカウントにプロファイルが明示的に割り当てられていない場合、そのアカウントは、親資産に割り当てられたプロファイルが適用されます。その資産にプロファイルが割り当てられていない場合、パーティションのデフォルトプロファイルが割り当てられます。パスワード変更時にサービスを更新または再起動すると、資産に割り当てられたプロファイルが依存するアカウントサービスの変更に使用されます。

新しいパーティションを作成すると、SPP は、デフォルトのスケジュールとルールで対応するデフォルトのプロファイルを作成します。パーティションに割り当てられたアカウントを管理するために、複数のプロファイルを作成することができます。資産とアカウントの両方がプロファイルのスコープに割り当てられます。

たとえば、12 個のアカウントを持つ資産があり、60 日ごとにパスワードをチェックして変更するようにパーティションプロファイルを構成したとします。そのうちの 1 つのアカウントのパスワードを 7 日ごとに管理したい場合は、別のプロファイルを作成し、その新しいプロファイルに個々のアカウントを追加すればよいです。これで、SPP は、このアカウント以外のこの資産上の

すべてのパスワードを 60 日ごとにチェックして変更し、このアカウントのパスワードを 7 日ごとに変更するようになります。

暗黙の関連付けと明示的な関連付け

プロファイルへの暗黙的な割り当てと明示的な割り当ての違いを理解することが重要です。

暗黙の関連付け

SPP は、暗黙的な割り当てを行います。たとえば、SPP に資産を追加すると、自動的に資産がデフォルトパーティションに追加され、デフォルトプロファイルのスコープに割り当てられます。これは、暗黙の関連付けと呼ばれます。資産は、パーティションのデフォルトプロファイルを暗黙的に継承します。同様に、アカウントもその親資産のプロファイルを継承します。つまり、資産にアカウントを追加すると、SPP はそのアカウントをその資産のプロファイルに暗黙のうちに追加します。

その後、資産を別のプロファイルに再割り当てすると、SPP は、資産に関連するすべてのアカウントを新しいプロファイルに自動的に再割り当てします。

明示的な関連付け

SPP では、資産またはアカウントを特定のプロファイルに明示的に追加することができます。資産をプロファイルに明示的に割り当てると、パーティションからの暗黙の継承が上書きされ、資産のプロファイルがパーティションによって決定されなくなります。同様に、アカウントをプロファイルに明示的に割り当てると、SPP は資産からの暗黙の継承を上書きし、そのアカウントのプロファイルはその資産によって決定されなくなります。

これで、資産を別のプロファイルに再割り当てしても、SPP は、古いプロファイルに明示的に割り当てられた資産の関連アカウントを再割り当てすることはありません。

デフォルトプロファイルにリセット

別のプロファイルをデフォルトとして設定した場合、SPP はすべての資産とその関連アカウントをその新しいデフォルトに暗黙的に再割り当てしますが、プロファイルに明示的に割り当てた資産やアカウントは再割り当てされません。暗黙の継承が解除されると、パーティションのデフォ

ルトのプロファイルを変更しても、プロファイルのスコープには影響しません。詳細については、「デフォルトプロファイルの設定」を参照してください。

10.4.2 プロパティタブ

プロパティタブには、選択したパーティションに関する情報が一覧表示されます。

プロパティへのアクセス：

［資産管理］>**［パーティション］**>（詳細の表示）>**［全般］**タブを選択します。

表：パーティションプロパティ：プロパティタブ

プロパティ	説明
名前	パーティション名
説明	選択したパーティションに関する情報

削除：このボタンをクリックすると、選択したパーティションが削除されます。

10.4.3 資産タブ

資産タブには、選択したパーティションに割り当てられている資産が表示されます。

選択したパーティションに 1 つまたは複数の資産を追加するには、詳細ツールバーの **［資産の追加］**をクリックします。

資産へのアクセス

［資産管理］>**［パーティション］**>（詳細の表示）>**［資産］**タブに移動します。

表：パーティション：資産タブのプロパティ

プロパティ	説明
名前	資産名
パスワードプロファイル	資産を管理するプロファイルの名前
SSH キープロファイル	SSH キープロファイルの名前

プロパティ	説明
アカウント検出ジョブ	ルール条件を満たすこの資産のアカウントを検出するために割り当てられたアカウント検出ジョブ。パーティション内の各資産には、個別に固有のアカウント検出ジョブを設定することができます。
資産検出ジョブ	Active Directory などのディレクトリ資産を検索するか、パーティション内のルール条件を満たすネットワーク IP 範囲をスキャンして、資産を発見するために割り当てられた資産発見ジョブ。パーティションの境界を越えて、資産検出ジョブが読み取りアクセスできるようにすることができます。詳細については、「管理タブ（資産の追加）」を参照してください。
プラットフォーム	選択した資産のプラットフォーム
セッションリクエスト	この列のチェックは、その資産に対してセッションアクセスリクエストが有効であることを示します。
無効	この列のチェックは、その資産が無効であることを示します。
製品ライセンス	該当する場合（例えば、Windows 資産の場合）、System または Desktop などのライセンスモデルが表示されます。
接続タイプ	パスワード、SSH キー、ディレクトリアカウント、ローカルシステムアカウントなど、資産の接続認証タイプ。詳細は、「接続タブ（資産の追加）」を参照してください。
説明	資産を追加したときに入力した説明情報

選択したパーティションに割り当てられた資産を管理するには、詳細ツールバーのボタンを使用します。

表：パーティション：資産タブツールバー

オプション	説明
資産の追加	選択したパーティションに 1 つまたは複数の資産を追加します。
削除	選択した資産をパーティションから削除します。
詳細の表示	選択した資産を編集します。
アクセスリクエスト	選択した資産のセッションリクエストを許可するには、**［セッションリクエストの有効化］**を選択します。選択した資産のセッショ

オプション	説明
	ンリクエストを許可しない場合は、**［セッションリクエストの無効化］**を選択します。
SSH ホストキー	このオプションでは、SPP が資産を自動的に検出できない場合 (Other Directory 資産など)、資産にホストキーを手動で追加することができます。
接続のテスト	SPP が現在のサービスアカウントの資格情報を使用して資産にログインできることを確認するために選択します。詳細については、「資産の接続性の確認」を参照してください。
今すぐ同期	資産とアカウントによるディレクトリ追加（増分）同期処理を実行します。同期はプロバイダごとに資産ごとにキューに入れられ、その資産に対して一度に 1 つのディレクトリ同期が実行されます。異なる資産で複数の同期を並行して実行することができます。削除は同期されないので、これはディレクトリ同期の高速タイプです。タスクウィンドウには、タスクの進行状況と結果が表示されます。**［詳細］**をクリックすると、さらに情報を確認したり**［停止］**をクリックしてタスクをキャンセルしたりすることができます。API（Assets/Synchronize）を使用して、すべての削除、追加、および変更を含む削除（完全）同期を実行することができます。この同期には時間（おそらく数時間）がかかります。特に、ディレクトリの設定に基づいて初めて実行される場合は、時間がかかります。
アカウント検出	アカウント検出ジョブを実行します。
有効化- 無効化	以下のいずれかを選択します： ［**有効化**］を選択すると、SPP が無効なパーティションを管理するようになります。 **［無効化］**を選択すると、SPP がパーティションを管理しないようになります。
無効化済みの表示	管理されておらず無効化されており、関連するアカウントがない資産を表示します。資産管理は、資産を選択して**［有効化/無効化］**をクリックすることで制御できます。
無効化済みの非表示	管理されておらず無効化されており、関連するアカウントがない資産を非表示にします。資産管理は、資産を選択して**［有効化/無効化］**をクリックすることで制御できます。

オプション	説明
エクスポート	このボタンを使用して、リストされたデータを JSON または CSV ファイルとしてエクスポートします。詳しくは、「データのエクスポート」を参照してください。
更新	選択したパーティションに関連する資産の最新リストを取得し、表示します。
検索	このリストから特定の資産を見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.4.4 アカウントタブ

アカウントタブには、選択したパーティションに割り当てられているアカウントが表示されます。

> **メモ**：デフォルトでは、資産に関連するすべてのアカウントは、同じプロファイルに割り当てられていますが、再割り当てすることができます。詳細については、「パスワードプロファイルの作成」を参照してください。

アカウントへのアクセス

［資産管理］ > **［パーティション］** > （詳細の表示） > **［アカウント］**

表：パーティション：アカウントタブプロパティ

プロパティ	説明
名前	アカウント名
ドメイン名	アカウントが Active Directory アカウントの場合、そのアカウントのドメイン名。一意性を判断するために使用されます。
親	アカウントが存在する資産が属するパーティション
パスワードプロファイル	このアカウントを管理するプロファイルの名前
SSH キープロファイル	パーティションに割り当てられたアカウントを管理する SSH キープロファイルの名前

プロパティ	説明
サービスアカウント	この列のチェックは、アカウントがサービスアカウントであることを示します。
パスワードリクエスト	この列のチェックは、アカウントに対してパスワードリリースリクエストが有効であることを示します。
セッションリクエスト	この列のチェックは、このアカウントでセッションアクセスリクエストが有効であることを示します。
SSH キーリクエスト	この列のチェックは、そのアカウントで SSH キーのリリースリクエストが有効であることを示します。
無効	この列のチェックは、アカウントが無効であることを示します。
パスワード	この列のチェックは、アカウントにパスワードが設定されていることを示します。詳細は、「アカウントパスワードの確認、変更、設定」を参照してください。
SSH キー	この列のチェックは、そのアカウントに SSH キーが設定されていることを示します。詳細は、「SSH キーの確認、変更、設定」を参照してください。
説明	アカウントが追加されたときに入力された説明の情報
タグ	アカウントに関連付けられたタグ

詳細ツールバーのボタンを使用して、選択したパーティションに割り当てられているアカウントを管理します。

表：パーティション：アカウントタブツールバー

オプション	説明
＋ 新しいアカウント	選択した資産にアカウントを追加します。詳細については、「パーティションへアカウントを追加」を参照してください。
削除	選択したアカウントを資産から削除します。
詳細の表示	選択したアカウントの追加情報を表示します。
アカウントセキュリティ	以下のメニューオプションがあります：

オプション	説明
	• **パスワードの確認、パスワードの変更、パスワードの設定**：詳細については、「アカウントパスワードの確認、変更、または設定」を参照してください。 • **SSH キーのチェック、SSH キーの変更、SSH キーの設定：**詳細については、「SSH キーの確認、変更、設定」を参照してください。 • **パスワードのアーカイブ** • **SSH キーのアーカイブ**
アクセスリクエスト	選択したアカウントに対してアクセスリクエストサービスを有効または無効にするオプションを選択します。値は、資産のプラットフォームがパスワードリクエスト、SSH キーリクエスト、セッションリクエストのいずれかをサポートしていることを示すかどうかから得られます。必要に応じて、パスワードリクエスト、セッションリクエスト、SSH キーリクエストを有効または無効にすることができます。 サービスアカウントは、資産の作成時に作成され、デフォルトでは、セッションまたはパスワードアクセスは有効になっていません。 検出されたアカウントは、アカウントを検出する際に使用されるアカウント検出テンプレートによって制御されます。これらは、アカウント検出ジョブのルールテンプレートのプロパティです。詳細については、「アカウント検出ルールの追加」を参照してください。
SSH キーの検出	アカウントに関連付けられた SSH キーの検出ジョブを実行します。
有効化 – 無効化	**［有効化］**を選択すると、SPP が無効な資産を管理します。 **［無効化］**を選択すると、SPP が管理しないようになります。
エクスポート	このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。

オプション	説明
更新	資産アカウントのリストを更新します。
検索	このリストから特定の資産アカウントまたはアカウントのセットを見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.4.5 所有者タブ

所有者タブには、パーティションに関連づけられている管理オブジェクトに関する情報が表示されます。

所有者へのアクセス

［資産管理］＞［パーティション］＞（詳細表示）**＞［所有者］**に移動します。

表：パーティション：所有者タブプロパティ

プロパティ	説明
タイプ	オブジェクトのタイプ
名前	ユーザーまたはユーザーグループの名前
プロバイダ	認証プロバイダの名前

詳細ツールバー上の次のボタンを使用して選択したパーティションの所有者を管理します：

表：パーティション：所有者ツールバー

プロパティ	説明
追加	選択したパーティションに、1 人または複数のユーザーまたはユーザーグループを追加します。詳しくは、「パーティションへのユーザーまたはユーザーグループの追加」を参照してください。
削除	選択したオブジェクトを、選択したパーティションのマネージャーから削除します。

プロパティ	説明
エクスポート	このボタンを使って、リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートします。詳細については、「データのエクスポート」を参照してください。
更新	リストを更新します。
検索	このリストの中から特定のオブジェクトを見つけるには、一致するものを検索するために使用する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

資産管理者と監査人は、特定のオブジェクトの所有権（有効な所有権を含む）に関するより詳細な情報を示すレポートを作成することもできます。詳細については、「所有権レポート」を参照してください。

10.4.6 パスワードプロファイルタブ

パスワードプロファイルタブには、このパーティションに関連するパスワードプロファイルが一覧表示されます。詳しくは「プロファイルとは」を参照してください。パスワードプロファイルを作成してから、パスワードプロファイルに資産とアカウントを追加することができます。詳細については、「パスワードプロファイルと SSH キープロファイルに資産またはアカウントを割り当て」を参照してください。

詳細ツールバーの**［新しいプロファイル］**をクリックして、選択したパーティションにパスワードプロファイルを追加します。詳細については、「パスワードプロファイルの作成」を参照してください。

パスワードプロファイルへのアクセス

［資産管理］>**［パーティション］**> （詳細の表示）>**［プロファイル］**タブに移動します。

表：パーティション：パスワードプロファイルタブ

プロパティ	説明
デフォルト	デフォルトのプロファイルの場合、が表示されます。詳細については、「デフォルトプロファイルの設定」を参照してください。
名前	パスワードプロファイルの名前

プロパティ	説明
パスワードの確認	アカウントのパスワードを確認するために使用されるパスワードの確認設定。詳細については、「パスワードの確認」を参照してください。
パスワードの変更	アカウントのパスワードを確認するために使用されるパスワードの変更設定。詳細については、「パスワードの変更」を参照してください。
パスワードルール	パスワードの自動変更中に SPP によって作成される新しいパスワードの構築を管理するアカウントパスワードルール。詳細については、「アカウントパスワードルール」を参照してください。
説明	選択したプロファイルに関する情報

次の詳細ツールバー上のボタンを使用してパーティションのパスワードプロファイルを管理します：

表：パーティション：パスワードプロファイルタブツールバー

オプション	説明
新しいプロファイル	選択したパーティションにパスワードプロファイルを追加します。詳細については、「パスワードプロファイルの作成」を参照してください。
削除	選択したパーティションのプロファイルを削除します。 パスワードプロファイルを削除すると、SPP はすべての資産とアカウントをデフォルトのプロファイルに再割り当てします。
詳細の表示	選択したパスワードプロファイルの詳細を表示します。
デフォルトとして設定	選択したパスワードプロファイルをデフォルトパスワードプロファイルに設定します。詳細については、「デフォルトプロファイルの設定」を参照してください。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	パスワードプロファイルのリストを更新します。

オプション	説明
検索	このリストで特定のパスワードプロファイルまたはパスワードプロファイルのセットを検索するには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.4.7 SSH キープロファイルタブ

各管理対象アカウントは、1 つの SSH ID キーを持つことができます。SSH キーは、A2A（アカウントレベルのスコープ）のためにリクエストおよび構成され、セッションに使用することができます。

SSH キープロファイルタブには、選択したパーティションに関連する SSH キープロファイルが一覧表示されます。詳細については、「プロファイルとは」を参照してください。

SSH キープロファイルへのアクセス

［資産管理］>**［パーティション］**> （詳細を表示）>**［SSH キープロファイル］**に移動します。

表：パーティション：SSH キープロファイルタブのプロパティ

プロパティ	説明
デフォルト	デフォルトのプロファイルの場合、が表示されます。詳細については、「デフォルトプロファイルの設定」を参照してください。
名前	SSH キーでプロファイルの名前
SSH キーのチェック	SSH キーを確認するために使用される SSH キーの確認設定。詳細については、「SSH キー設定のチェック」を参照してください。
SSH キーの変更	SSH キーを確認するために使用される SSH キーの変更設定。詳細については、「SSH キー設定の変更」を参照してください。
SSH キーの検出	SSH キーを検出するために使用する SSH キー検出ジョブ。詳しくは「SSH キーの検出設定」を参照してください。
説明	選択した SSH キープロファイルに関する情報

次の詳細ツールバーボタンを使用してパーティションプロファイルを管理します。

表：パーティション：SSH キープロファイル

オプション	説明
新しいプロファイル	選択したパーティションに SSH キープロファイルを追加します。詳細については、「SSH キープロファイルの作成」を参照してください。
削除	選択した SSH キープロファイルを削除します。 SSH キープロファイルを削除すると、SPP はすべての資産とアカウントをデフォルトのプロファイルに再割り当てします。デフォルトのプロファイルが設定されていない場合、SPP はプロファイルに関連付けられている資産とアカウントを削除します。
詳細の表示	選択した SSH キープロファイルの詳細を表示します。
デフォルトとして設定	（任意）選択した SSH キープロファイルをデフォルトプロファイルに設定します。一度デフォルトプロファイルを選択すると、常にデフォルトプロファイルが存在することになります（どのプロファイルをデフォルトにするかはいつでも変更可能ですが、デフォルトプロファイルは常にパーティションに必要です）。デフォルトプロファイルを選択することを止める唯一の方法は、パーティションから全ての SSH プロファイルを削除することです。詳しくは、「デフォルトプロファイルの設定」を参照してください。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	SSH キープロファイルのリストを更新します。
検索	このリストで特定の SSH プロファイルまたはプロファイルのセットを検索するには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

10.4.8 履歴タブ

履歴タブでは、選択したパーティションに影響を与えた各操作の詳細を表示したり、エクスポートしたりすることができます。

履歴タブへのアクセス

［資産管理］ > **［資産］** > （詳細の表示） > **［履歴］**

履歴タブの上部には、次の情報が表示されます：

- **日付範囲**：デフォルトでは、履歴の詳細は過去 24 時間について表示されます。ドロップダウンから、時間間隔の 1 つを選択すると、その時間枠の履歴の詳細が表示されます。
- **エクスポート**：このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
- **更新**：表示されているリストを更新します。
- **検索**：詳細については、「検索ボックス」を参照してください。

表：パーティション：履歴タブプロパティ

プロパティ	説明
日付/時間	イベントの日付と時刻
ユーザー	イベントを発生させたユーザーの表示名
ソース IP	イベントをトリガーした管理システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択したパーティションの名前
イベント	選択した資産に対して行われた操作の種類： • 作成 • 削除 • 更新 • メンバーシップの追加 • メンバーシップの削除 **メモ：**メンバーシップの操作は、選択した資産にアカウントの依存関係が追加または削除されたなど、関連オブ

プロパティ	説明
	ジェクトまたは親オブジェクトとの関係が変更されたことを示します。
関連オブジェクト	関連オブジェクトの名前
関連オブジェクトのタイプ	関連オブジェクトのタイプ
親	選択した資産が子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

10.4.9 パーティションの管理

パーティションページのコントロールとタブページで、パーティションを管理するためのタスクを実行します。

- パーティションの追加
- パーティションに資産を追加
- パーティションへアカウントを追加
- パーティションから資産を削除
- パーティションへのユーザーまたはユーザーグループの追加
- パスワードプロファイルの作成
- SSH キープロファイルの作成
- デフォルトパーティションの設定
- デフォルトプロファイルの設定
- パスワードプロファイルと SSH キープロファイルに資産またはアカウントを割り当て
- パーティションの削除

パーティションの追加

SPP にパーティションを追加するのは、資産管理者の責任です。新しいパーティションを作成すると、SPP は、デフォルトのスケジュールとルールを持つ対応するデフォルトのプロファイルを作成します。詳細については、「デフォルトプロファイルの設定」を参照してください。

パーティションの追加手順

1. **［資産管理］＞［パーティション］**に移動します。
2. ツールバーの ＋ **［新しいパーティション］**をクリックします。
3. **新しいパーティション**ダイアログで、次の情報を入力します：
    a. **名前：**パーティションに一意の名前を入力します。制限：50 文字
    b. **説明：**（任意）このパーティションに関する情報を入力します。制限：255 文字
4. **［OK］**をクリックして、パーティションを保存します。

新しいパーティションを作成すると、SPP は、デフォルトのスケジュールとルールを持つ対応するデフォルトプロファイルを作成します。次のことができます：

- 作成したパーティションのプロファイルを変更する。
- デフォルトプロファイルを変更する。詳細については、「デフォルトプロファイルの設定」を参照してください。

パーティションに資産を追加

パーティションビューの**資産**タブを使用して、1 つまたは複数の資産をパーティションに追加します。パーティションに資産を割り当てると、その資産に関連するすべてのアカウントもそのパーティションに割り当てられます。

資産は一度に 1 つのパーティションにしか割り当てられません。資産をパーティションに割り当てると、その資産に関連するすべてのアカウントが自動的にそのパーティションに再割り当てされます。その後、その資産のために追加した新しいアカウントは、自動的にそのパーティションに割り当てられます。

資産を別のパーティションに再割り当てするには、別のパーティションのスコープまたは資産の全般プロパティから行います。詳細については、「資産をパーティションに割り当て」を参照してください。

資産をパーティションに関連付けると、その資産に関連付けられたすべてのアカウントも、そのパーティションのスコープに追加されます。詳細については、「プロファイルとは」を参照してください。

パーティションに資産を追加する手順

1. **［資産管理］＞［パーティション］**へ移動します。

2. オブジェクトリストからパーティションを選択し、**［詳細の表示］**を選択します。
3. **資産**タブを選択します。
4. 詳細ツールバーの **［資産の追加］**をクリックします。
5. **［パーティションに追加する資産を選択してください］**ダイアログで、1 つまたは複数の資産を選択します。
6. **［資産の選択］**をクリックします。

探している資産が表示されず、資産管理者である場合、選択ダイアログで **［新しい資産］**をクリックして作成することができます。詳細については、「資産の追加」を参照してください。

パーティションへアカウントを追加

パーティションビューの**アカウント**タブを使用してパーティションにアカウントを追加できます。

ドメインコントローラー（DC）資産でタスクとサービスを管理できます。詳しくは「ドメインコントローラー（DC）資産の使用」を参照してください。

パーティションへのアカウントの追加手順

1. **［資産管理］＞［パーティション］**に移動します。
2. パーティションを選択し、**［詳細の表示］**をクリックします。
3. **［アカウント］**タブを開きます。
4. 詳細ツールバーから **［新しいアカウント］**をクリックします。
5. **［新しいアカウントの資産を選択］**ダイアログで、このアカウントに関連付ける資産を選択し、**［資産の選択］**をクリックします。
6. **［新しいアカウント］**ダイアログで、以下の情報を入力します。
    - **［全般］**タブ：
        - **名前**：
            - ローカルアカウント：このアカウントのログインユーザー名を入力します。制限：100 文字。

- ディレクトリアカウント：［参照］してアカウントを検索します。

- **説明**：（任意）この管理アカウントに関する情報を入力します。制限：255 文字。
- **［管理］**タブ：
  - **パスワードリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してパスワードリリースリクエストが有効であることを示します。このオプションをオフにすると、誰かがこのアカウントのパスワードをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは自分が承認されたユーザーである権限の範囲内で、すべてのアカウントのパスワードをリクエストできます。
  - **セッションリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してセッションアクセスリクエストが有効であることを示します。このオプションをオフにすると、誰かがこのアカウントを使用してセッションアクセスをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは自分が認証されたユーザーである権限の範囲内で、任意のアカウントに対してアクセスリクエストを行うことができます。
  - **すべてのパーティションで使用可能**（一部のタイプのディレクトリアカウントでのみ使用可能）：選択すると、どのパーティションでもこのアカウントを使用することができ、パスワードは他の管理者に渡されます。例えば、このアカウントは、他の資産の依存アカウントやサービスアカウントとして使用することができます。潜在的には、このアカウントとしてサービスを実行している資産があり、サービスアカウントが変更されたときに、それらの資産を更新することができるかもしれません。選択しない場合、パーティション所有者や他のパーティションは、そのアカウントの存在を知ることはありません。アーカイブサーバーはパーティションに拘束されませんが、アーカイブサーバーのディレクトリアカウントを設定するには、このオプションが選択されている必要があります。

7. **［OK］**をクリックします。

パーティションから資産を削除

パーティションから資産を削除することはできません。

資産を別のパーティションに再割り当てするには、別のパーティションのスコープまたは資産の**［全般］**プロパティから行います。詳細については、「資産をパーティションに割り当て」を参照してください。

資産をパーティションに関連付けると、その資産に関連付けられたすべてのアカウントも、そのパーティションのスコープに追加されます。詳細については、「プロファイルとは」を参照してください。

パーティションへのユーザーまたはユーザーグループの追加

パーティションにユーザーを追加する場合、パーティションの所有権を持つユーザーまたはユーザーグループを指定することになります。

パーティションにユーザーとユーザーグループを追加するのは、資産管理者の責任です。セキュリティポリシー管理者には、グループを追加する権限のみがあり、ユーザーを追加する権限はありません。詳細については、「管理者のアクセス許可」を参照してください。

パーティションにユーザーを追加する手順

1. **［資産管理］＞［パーティション］**を開きます。
2. リストからパーティションを選択し、**［詳細の表示］**をクリックします。
3. **［所有者］**タブを開きます。
4. **［追加］**をクリックします。
5. **［ユーザー/ユーザーグループ］**ダイアログのリストから、1 人以上のユーザーまたはユーザーグループを選択します。
6. **［所有者の選択］**をクリックし、選択内容を保存します。

パスワードプロファイルの作成

パーティションにパスワードプロファイルを追加するのは、資産管理者またはパーティションの委任管理者の責任です。

パーティションにプロファイルを追加する手順

1. **［資産管理］＞［パーティション］**に移動します。
2. リストからパーティションを選択し、**［詳細の表示］**をクリックします。
3. **パスワードプロファイル**タブを選択します。
4. 詳細ツールバーから **［新しいプロファイル］**をクリックします。
5. **［全般］**タブで、次の情報を入力します。
    a. **名前**： プロファイルの一意の名前を入力します。制限：50 文字
    b. **説明**：このプロファイルに関する情報を入力します。このプロファイルに関する情報を入力します。文字数制限：255 文字
6. **［パスワードの確認］**タブで、ドロップダウンメニューから以前に定義したパスワード確認設定を選択するか、［追加］をクリックして新しいチェックパスワード設定を追加します。これらは、アカウントパスワードの確認に使用されるルールです。詳細については、詳細については、「パスワードの確認設定の追加」を参照してください。
7. **［パスワードの変更］**タブで、ドロップダウンメニューから以前に定義したパスワード変更設定を選択するか、［追加］をクリックして新しいパスワード変更設定を追加します。アカウントのパスワードをリセットするために使用されるルールです。詳細については、「パスワード変更設定の追加」を参照してください。
8. **［アカウントパスワードルール］**タブで、以前に定義したアカウントパスワードルールを選択するか、［追加］をクリックして新しいアカウントパスワードルールを追加します。アカウントパスワードルールは、パスワードの自動変更中に SPP によって作成される新しいパスワードの構築を管理する複雑さのルールです。詳細については、「アカウントパスワードのルールの追加」を参照してください。
9. **［OK］**をクリックして、選択内容を保存し、プロファイルを作成します。

新しいプロファイルを作成する場合、**［パスワード同期グループ］**タブは表示されません。このタブは、プロファイルの編集時に表示されます。**［パスワード同期グループ］**タブを使用して、プロファイルの変更スケジュールで管理されるパスワード同期グループを追加または更新することができます。詳細については、「パスワード同期グループ」を参照してください。

SSH キープロファイルの作成

パーティションに SSH キープロファイルを追加するのは、資産管理者またはパーティションの委任された管理者の責任です。

パーティションに SSH キープロファイルを追加する手順

1. **［資産管理］＞［パーティション］**に移動します。
2. リストからパーティションを選択し、**［詳細の表示］**をクリックします。
3. **［SSH キープロファイル］**タブを開きます。
4. 詳細ツールバーから ＋ **［新しいプロファイル］**をクリックします。
5. **［全般］**タブで、以下の情報を入力します：
    - **名前**：プロファイルの一意の名前を入力します。制限：50 文字
    - **説明**：このプロファイルに関する情報を入力します。文字数制限：255 文字
6. **［SSH キーのチェック］**タブで、ドロップダウンメニューから以前に定義した SSH キーの確認設定を選択します。これらは、SPP がアカウントの SSH キーを確認するために使用するルールです。詳細については、「SSH キーの確認、変更、設定」を参照してください。
7. **［SSH キーの変更］**タブで、ドロップダウンメニューから以前に定義した SSH キーの変更設定を選択します。これらは、アカウントの SSH キーをリセットするために使用されるルールです。詳細については、「SSH キー変更設定の追加」を参照してください。
8. **［SSH キーの検出］**タブで、以前に定義した SSH キー設定の検出を選択します。これらは、SSH キーを検出するために使用されるルールです。詳細については、「SSH キー検出の追加」を参照してください。
9. **［OK］**をクリックして、選択内容を保存し、プロファイルを作成します。

新しいパーティション SSH キープロファイルを作成する場合、**［SSH キー同期グループ］**タブは表示されません。このタブは、パーティション SSH キープロファイルを編集しているときに表示されます。**［SSH キー同期グループ］**タブを使用して、プロファイル変更スケジュールで管理される SSH キー同期グループを追加または更新することができます。詳細については、「SSH キー同期グループの設定」を参照してください。

デフォルトパーティションの設定

各資産管理者は、固有のデフォルトパーティションとプロファイルを設定し、管理者が追加するすべての新しい資産がデフォルトパーティションとデフォルトプロファイルに自動的に割り当てられるようにすることができます。詳細については、「デフォルトプロファイルの設定」を参照してください。

デフォルトパーティションの設定手順

1. **［資産管理］＞［パーティション］**に移動します。
2. パーティションを選択し、ツールバーから **［デフォルトとして設定］**をクリックします。

デフォルトプロファイルの設定

新しいパーティションを作成すると、SPP は、デフォルトのスケジュールとルールを持つ対応するデフォルトのプロファイルを作成します。資産管理者は、固有のデフォルトパーティションとプロファイルを設定できます。一度デフォルトのプロファイルを設定すると、追加したすべての新しい資産とアカウントは、自動的にそのプロファイルに割り当てられます。

SPP は、デフォルトのスケジュールを「決して」パスワードまたは SSH キーを検証またはリセットしないように設定します。

資産をパーティションに関連付けると、その資産に関連付けられたすべてのアカウントも、そのパーティションのスコープに追加されます。詳細については、「プロファイルとは」を参照してください。

別のプロファイルをデフォルトとして設定する手順

1. **［資産管理］＞［パーティション］**に移動します。
2. パーティションを選択し、**［詳細の表示］**をクリックします。
3. **［パスワードプロファイル］**または**［SSH キープロファイル］**タブを選択します。
4. 現在のデフォルトでないプロファイルを選択し、詳細ツールバーまたはコンテキストメニューから **［デフォルトとして設定］**をクリックします（デフォルトのプロファイルを選択すると、**［デフォルトとして設定］**アイコンはグレー表示されます）。

パスワードプロファイルと SSH キープロファイルに資産またはアカウントを割り当て

パスワードプロファイル、SSH キープロファイル、またはその両方に、資産またはアカウントを割り当てることができます。資産とアカウントは、プロファイルに割り当てるパーティションの範囲内にある必要があります。

SPP を設定して、自動的な資産検出またはアカウント検出のジョブを実行することもできます。詳細については、「検出」を参照してください。

> **注意: アカウントをプロファイルに関連付けるのは、SPP に管理させたいものだけにしてください。**

プロファイルに資産またはアカウントを追加する手順

1. **［資産管理］＞［パーティション］**に移動します。
2. リストからパーティションを選択し、**［詳細の表示］**をクリックします。
3. **［パスワードプロファイル］**または**［SSH キープロファイル］**タブを開きます。
4. プロファイルを選択し、**［編集］**をクリックします。
5. 選択したプロファイルに資産を追加するには、**［資産］**タブに切り替えます。
6. 追加する資産（複数可）を選択します。
7. 選択したプロファイルにアカウントを追加するには、**［アカウント］**タブに切り替えます。
8. 追加するアカウントを選択します。
9. プロファイルの編集が終了したら、プロファイルダイアログの外側をクリックして保存し、終了します。

パーティションの削除

パーティションを削除する場合、すべての資産とアカウントを転送するために、別のパーティションを指定する必要があります。削除するパーティションのプロファイルと関連するプロファイル設定、検出ジョブ、履歴データは、プロファイルと一緒に削除されます。

パーティションの削除

1. **［資産管理］＞［パーティション］**に移動します。
2. 削除するパーティションを選択します。
3. **［削除］**をクリックします。
4. ダイアログで、資産とアカウントを再割り当てするパーティションを選択します。
5. **［パーティションの選択］**をクリックして、資産とアカウントを再割り当てし、選択したパーティションを削除します。

10.5 検出

SPP の検出ジョブは、ネットワーク環境内の資産、アカウント、SSH キー、サービスを検出することができます。これにより、ネットワーク環境における特権アカウントの初期展開と継続的な保守を簡素化することができます。

ジョブの詳細は以下のとおりです：

- 資産検出ジョブは、Active Directory などのディレクトリ資産を検索したり、ネットワーク IP 範囲をスキャンしたりして、資産を見つけます。どの資産を検索するかは、ルールで制御します。資産検出ジョブは、定期的に実行するようにスケジュールすることができます。検出ジョブは、接続の詳細など、新しく作成された資産のデフォルト設定を設定するテンプレートを使って構成することができます。検出ジョブによって作成された資産は SPP によって管理されているとみなされますが、ネットワーク資産には何の影響も与えません。有効な接続情報を持つ資産は、アカウント検出に使用できます。

  資産の検出方法として**ディレクトリ**を使用する場合、共有されているディレクトリ資産を任意のパーティションに検出することができます。ディレクトリ資産を共有するには、その資産のすべてのパーティションで **［検出可能］**を選択します。「管理タブ（資産の追加）」を参照してください。
- **アカウント検出**：アカウント検出ジョブは、Active Directory などのディレクトリ資産を検索するか、アカウント検出ジョブに関連付けられた Windows および Unix 資産(/etc/passwd)のローカルアカウントデータベースをスキャンして、アカウントを検出します。検出されるアカウントはルールで制御されます。アカウント検出ジョブは、定期的に実行されるようにスケジュールすることができます。検出ジョブは、新しく作成されたアカウントにデフォルト設定を設定するように構成することができます。アカウント検出によって検出されたアカウントは、管理または無効化を決定するま

で、管理も無効化もされません。アカウントが SPP によって管理される場合、これは、検出ジョブに関連付けられたプロファイル設定に従ってパスワードを管理できることを意味します。SPP は、構成された資格とポリシーに従って、アカウントをパスワードおよび/またはセッションリクエストで利用できるようにすることができます。

検出ジョブの範囲内のアカウントには、以前に SPP パーティションに（手動で）追加されたアカウントが含まれる場合があります。詳細については、「アカウントの追加」を参照してください。

- **サービス検出**：サービス検出ジョブは、SPP が管理するアカウントとして実行される Windows サービスを検出します。SPP がサービスアカウントのパスワードを管理している場合、パスワードが変更されたときに SPP は Windows サービス設定をパスワードに合わせて更新し、サービスを自動的に再起動することができます。
- **SSH キー検出：**SSH キー検出ジョブは、ユーザーディレクトリを検索し、管理されたアカウントで許可された SSH キーを検出します。

Web クライアントには、デフォルトで検出されたすべてのアイテムの情報が表示されます。また、**［パーティション］**ドロップダウンを使用して、情報を表示する特定のパーティションを選択することもできます。

［検出された項目］セクションには、次のタイルが表示されます：

- **アカウント**：検出されたアカウントの数が表示されます。タイルをクリックすると詳細が表示されます。
- **サービス**：検出されたサービスの数が表示されます。タイルをクリックすると詳細が表示されます。サービスアカウントの検出ジョブは、**［資産管理］＞［資産］＞** （詳細の表示）**＞［検出されたサービス］**から起動できます。詳細については、「検出されたサービスタブ(資産)」を参照してください。
- **SSH キー**：検出された SSH キーの数が表示されます。タイルをクリックすると詳細が表示されます。

［検出ジョブ］セクションは、以下のタブに分かれています。

- **資産**タブ：このタブには、ディレクトリまたはネットワークに対して実行可能な資産検出ジョブが表示され、潜在的な管理表示のための資産を検出します。
- **アカウント**タブ：このタブには、管理画面の候補となるアカウントを検出するために、範囲内の資産に対して実行可能なアカウント検出ジョブが表示されます。
- **SSH キー**タブ：このタブには、管理対象アカウントに対して実行可能な SSH キー検出ジョブが表示され、潜在的な管理ディスプレイ用の SSH キーを検出します。

10.5.1 資産検出

SPP に追加したディレクトリまたはネットワーク（IP 範囲）に対して、1 つまたは複数の資産検出ジョブをスケジュールして自動的に実行することができます。検出ジョブの範囲内の資産には、以前に SPP パーティションに（手動で）追加した資産が含まれる場合があります。詳細については、「資産の追加」を参照してください。

資産の検出方法として**［ディレクトリ］**を使用する場合、共有されているディレクトリ資産は任意のパーティションに検出することができます。ディレクトリ資産を共有するには、その資産のすべてのパーティションで**［検出可能］**を選択します。「管理タブ（資産の追加）」を参照してください。

資産検出ジョブが実行されると、検出された資産が**［資産］**に追加されます。ネットワークスキャンまたはディレクトリによる資産検出でオペレーティングシステムが検出されない場合、**Linux** オペレーティングシステムが適用されます。これは後で変更することができます。

詳細については、「資産検出ジョブのワークフロー」を参照してください。

プロパティとツールバー

［資産管理］＞［検出］を開きます。

次のツールバーボタンを使用して、検出ジョブの設定を管理します。

表：資産検出：ツールバー

オプション	説明
＋ 新しい資産検出ジョブ	資産検出ジョブを追加します。詳細については、「資産検出ジョブの追加」を参照してください。
削除	選択した資産検出ジョブを削除します。
詳細の表示	選択した資産検出ジョブを修正します。また、行をダブルクリックして編集ダイアログを開くこともできます。
▶ 今すぐ実行	選択した資産検出ジョブを実行します。進行状況と完了を示すタスクポップアップが表示されます。
エクスポート	このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
更新	実行された資産検出ジョブのリストを更新します。

オプション	説明
🔍 検索	一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

資産検出ジョブがグリッドに表示されます。

表：資産検出：資産検出ジョブグリッド

列名	説明
名前	検出ジョブの名前
作成者	ジョブの作成者
検出タイプ	ジョブの種類（例：Windows、Unix、ディレクトリ）
ディレクトリ	検出ジョブが実行されるディレクトリ
パーティション	検出された資産や、資産を管理するパーティション
スケジュール	資産検出ジョブの実行タイミング
前回の実行日	選択した資産検出ジョブが実行された日
次の実行日	資産検出ジョブが次に実行される予定日
前回の実行成功日	選択した資産検出ジョブが正常に実行された直近の日付
前回の実行失敗日	選択した資産検出ジョブが失敗した直近の日付

資産検出ジョブのワークフロー

資産検出ジョブの設定、スケジュール、テスト、および実行が可能です。ジョブの実行後、資産を管理するかどうかを選択することができます。また、実行された資産検出ジョブに関する情報を表示することもできます。

資産検出ジョブワークフロー

1. 資産検出ジョブを作成します。詳細については、「資産検出ジョブの追加」を参照してください。

2. 資産検出ジョブを保存した後、▶ **［今すぐ実行］**を選択してテストすることができます。詳細については、「資産検出」を参照してください。

3. 資産検出ジョブの実行後、資産検出ジョブを選択して **［詳細の表示］**をクリックします。詳細については、「資産検出の結果」を参照してください。

4. 資産の管理を制御するには、**［資産管理］＞［資産］**を開き、資産を選択して以下のいずれかのオプションを選択します。

オプション	説明
▣ 有効化	SPP に無効化された資産を管理させる場合は、▣ **［有効化］**を選択します。このオプションは、無効化された資産に対してのみ有効です。
⊘ 無効化	SPP に選択した資産を管理させないようにするには、⊘ **［無効化］**を選択します。資産を無効にすると、SPP はその資産を無効にし、関連するすべてのアカウントを削除します。後で資産を管理することを選択した場合、SPP は関連するすべてのアカウントを再度有効にします。

5. **［資産管理］＞［資産］**上で、以下のボタンを使用し、無効としてマークした資産を表示または非表示にすることができます。

ボタン	説明
無効化済みの表示	無効化された資産を表示します。
無効化済みの非表示	無効化された資産を表示しません。

6. アクティビティセンターで、実行された検出ジョブの情報を検索します。SPP は、資産検出アクティビティカテゴリにある **資産検出アクティビティ**を一覧表示します。

資産検出ジョブの追加

新しい資産検出ジョブを追加することができます。

1. **［資産管理］＞［検出］**に移動します。

2. **［資産］**タブを選択します。

3. ＋ **［新しい資産検出ジョブ］**をクリックして、新しい資産検出ジョブを作成します。

4. **［新しい資産検出ジョブ］**ダイアログで、以下のタブに検出ジョブの情報を入力します。

タブ	説明
全般タブ	ここでは、検出ジョブに関する一般情報を追加し、SPP が検出した資産を追加したいパーティションを特定します。また、検出方法（**ディレクトリ**または**ネットワークスキャン**）を指定します。
情報タブ	ここでは、ディレクトリを選択し、検索場所を設定します。
資産検出ルールタブ	検索制約と条件を定義し、タグを追加し、検出された資産を管理するプロファイルを選択する場所です。
スケジュールタブ	検出ジョブのスケジュールを設定します。

検出ジョブを保存した後、**資産検出**ツールバーを使用してジョブを修正または実行することができます。詳細については、「資産検出」を参照してください。

全般タブ

［資産管理］＞［検出］＞［資産］（資産検出ジョブの追加または編集）に移動します。

資産検出ダイアログの**［全般］**タブで、資産検出ジョブに関する一般情報を入力し、SPP が検出した資産を追加するパーティションを特定します。

表：検出：全般プロパティ

プロパティ	説明
名前	資産検出ジョブの名前を入力します。 制限： 50 文字
説明	資産検出ジョブに関する情報を入力します。 制限： 255 文字
パーティション	検出された資産を管理するパーティションを選択するには、**［参照］**を使用します。また、**［パーティション］**ダイアログ（**［参照］**ボタンからアクセス可能）から ＋ **［新しいパーティション］**をクリックして、新しいパーティションを追加することもできます。

プロパティ	説明
	重要：この検出ジョブを保存した後、パーティションを変更することはできません。

情報タブ

［資産管理］＞**［検出］**＞**［資産］**＞（資産検出ジョブの追加または編集）に移動します。

情報タブで、検出ジョブのディレクトリまたはネットワーク情報を定義します。

表：検出タイプ

プロパティ	説明
検出タイプ	検出タイプを選択します： • **Directory** • **Network** **Directory** を選択した場合、共有されているディレクトリ資産を任意のパーティションに検出することができます。ディレクトリには、Active Directory または LDAP が含まれます。「サポート対象のプラットフォーム」の「検索可能なディレクトリ」を参照してください。 ディレクトリ資産を共有するには、**［すべてのパーティションで検出に使用可能］**を選択します（［管理］タブ（資産の追加）を参照）。チェックボックスが選択されていない場合、資産は共有されず、資産はディレクトリ資産が割り当てられているパーティションにのみ検出されます。

表：検出：ディレクトリスキャンの情報プロパティ

プロパティ	説明
Directory	資産検出ジョブを実行するディレクトリを選択します。

表：検出：ネットワークスキャンの情報プロパティ

プロパティ	説明
OS 検出の有効化	このチェックボックスはデフォルトで選択されており、使用されているオペレーティングシステムを検出するために OS フィンガープリン

プロパティ	説明
	トを使用することを意味します。OS のフィンガープリントを使用しない場合は、このチェックボックスをオフにします。
開始 IP アドレス	開始 IPv4 アドレスを入力します。この IPv4 アドレスと**［終了 IP アドレス］**フィールドに入力した IPv4 アドレスの間のすべての IPv4 アドレスが検出対象に含まれます。 **メモ：**IPv6 スキャンはサポートされていません。
終了 IP アドレス	IPv4 アドレスを入力します。この IPv4 アドレスと**［開始 IP アドレス］**フィールドに入力された IPv4 アドレスの間のすべての IPv4 アドレスは、検出に含まれます。 **メモ：**IPv6 スキャンはサポートされていません。
IP アドレスの除外	SPP では、指定した IPv4 範囲内の IP アドレスをスキャンから除外することができます。 ＋ **［追加］**をクリックすると、スキャンから IP アドレスを除外できます。 － **［削除］**をクリックすると、対応する除外された IPv4 アドレスが削除され、その IP アドレスがスキャンに含まれます。

資産検出ルールタブ

［資産管理］＞［検出］＞［資産］＞（資産検出ジョブの追加または編集）へ移動します。

資産検出ルールタブで検出された資産を管理します。

検出の詳細

- SPP は一度資産を作成すると、別のジョブによって資産が再検出された場合、資産を再作成または変更しようとはしません。
- 検出時に見つかった SSH ホストキーは、自動的に受け入れられます。
- 1 つの資産検出ジョブに対して複数のルールを設定することができます。SPP が資産検出ジョブを実行するとき、複数のルールで資産を検出した場合、資産を検出した最初のルールの接続とプロファイルの設定を適用します。

新しい資産検出ルールの追加手順

1. **［資産検出ルール］**タブで **［編集］**をクリックします。
2. **［追加］**をクリックします。
3. **［新しい資産検出ルール］**ダイアログで、**［名前］**を 50 文字以内で入力します。
4. 各ルールには、少なくとも 1 つの条件、接続、プロファイルを指定する必要があります：
    a. **［条件］**で**［追加］**をクリックして、1 つまたは複数の**グループ、制約、LDAP フィルタ**（LDAP または Active Directory の場合）、**すべて検索**を追加します。詳しくは、「条件の追加（資産検出）」を参照してください。
    b. **［接続テンプレート］**は必須であり、デフォルトは**「検出されたプラットフォームを使用」**（資格情報は関連付けられていない）です。これを変更するには、チェックボックスのチェックをクリアします。
    c. **［管理］**タブでは、検出された資産を管理するためのプロファイルを管理することができます。
        - **パスワードプロファイル**：
            - デフォルトは、［パスワードプロファイル］タブ（パーティション）で設定されたパーティションのデフォルトパスワードプロファイル、またはパーティションレベルで設定されたデフォルトパーティションになります。
            - **［全般］**タブで選択されたパーティションに基づきます。
            - 新しいパスワードプロファイルの作成を許可します（＋**［新しいプロファイル］**を使用）。
        - **SSH キープロファイル**を選択して、SSH キープロファイルを選択または作成することができます。
        - **アカウント検出ジョブ**を選択または作成するために、アカウント検出ジョブを選択できます。
        - **管理対象ネットワーク**では、ワークロードバランシングに割り当てられた管理ネットワークを選択することができます。
    d. **［タグ］**タブを使用して、ルールベースのタグを追加します。タグをルールに追加するには、＋**［タグの追加］**をクリックし、タグを入力します。
5. **［適用］**をクリックして、資産検出ルールを保存します。

条件の追加

資産検出ルールは複数の条件を持つことができ、各条件には 1 つ以上の制約を付けることができます。SPP が検出ジョブを実行すると、すべての検索条件を満たすすべての資産が検出されます。

［管理管理］>**［検出］**>**［資産］**>（資産検出ジョブの追加または編集）>**［資産検出］**ダイアログ>**［資産検出ルール］**ダイアログ>**条件の追加**タブ>（条件の追加）に移動します。

［すべて検索］条件の追加手順

1. **［条件］**ダイアログの**［検索条件］**で、**［すべて検索］**を選択します。
2. ディレクトリの資産検出ジョブを設定している場合、**［検索場所のフィルタ］**を参照して、資産を検索するディレクトリ内のコンテナを選択します。サブコンテナからオブジェクトを含めるには、**［サブコンテナからオブジェクトを含める］**を選択し、子オブジェクトを検出対象から除外するにはチェックボックスをオフにします。
3. **［プレビュー］**をクリックして、設定した条件をテストし、入力した条件に基づいて SPP が指定したディレクトリまたはネットワークで検出する資産のリストを表示します。
4. **［OK］**をクリックします。

［LDAP フィルタ］条件の追加手順（LDAP または Active Directory）

検索ベースは、（オプションが選択されている場合はサブコンテナを含む）指定されたディレクトリの定義されたブランチに検索を制限します。この条件は、ディレクトリ検出ジョブ（LDAP または Active Directory ディレクトリ）でのみ利用可能です。

1. **［条件］**ダイアログで
    a. **検索条件：［LDAP フィルタ］**を選択し、使用する検索条件を入力します。
    b. **検索場所のフィルタ：**資産を検索するディレクトリ内のコンテナを**［参照］**して選択します。

    > **ヒント：**資産検出ジョブのディレクトリルートを選択しないでください。

    c. **［サブコンテナのオブジェクトを含める］**オプションで、このチェックボックスを選択すると、サブコンテナ内の資産を検索することができます。

2. **［プレビュー］**をクリックし、設定した条件をテストします。

3. **［OK］**をクリックして、選択した条件を保存します。

ディレクトリ条件でのグループ追加

この条件は、**ディレクトリ**検出ジョブにのみ使用できます。

1. **［条件］**ダイアログで：

    a. **検索条件**：**［グループ］**を選択します。

    b. ＋**［追加］**をクリックして、**［グループ］**ダイアログを起動します。

    c. **次で開始**：グループ名の一部または全部を入力し、**［グループの検索］**をクリックします。一度に入力できる文字列は 1 つだけです（グループ名の全部または一部）。

    d. **検索場所**：ディレクトリ内で検索するコンテナを**［参照］**して選択します。

    e. **［サブコンテナのオブジェクトを含める］**：子オブジェクトを含めるには、このチェックボックスを選択します。

    f. **追加するグループを選択：**検索結果がこのグリッドに表示されます。検出ジョブに追加するグループを 1 つまたは複数選択します。

2. **［プレビュー］**をクリックすると、設定した条件をテストし、入力した条件に基づいて SPP が指定したディレクトリまたはネットワークで検出する資産のリストが表示されます。

3. **［OK］**をクリックすると、選択した内容が保存されます。

制約条件の追加手順

1. **［条件］**ダイアログの**［検索条件］**で、**［制約］**を選択します。

2. 検索場所のフィルタを変更するには、**［参照］**をクリックし、検索範囲となる検索場所を選択します。ネットワークスキャン資産検出ジョブは、検索拠点の設定に対応していません。

3. 制約（検索条件）を適用するには：

    a. プロパティを選択します：

        - **名前**
        - **説明**
        - **ネットワークアドレス**

- **オペレーティングシステム**
- **オペレーティングシステムのバージョン**

> **メモ：**ネットワークスキャンの場合、ネットワークが検出した情報（**名前**と**オペレーティングシステム**）に対してのみ制約を適用することができます。

b. オペレーターを選択します。

- **等しい**
- **等しくない**
- **次で開始**
- **次で終了**
- **次を含む**

c. テキストボックスに、最大 255 文字までの値を入力します。検索では、大文字と小文字が区別され、ワイルドカードは使用できません。

4. **［プレビュー］**をクリックすると、設定した条件をテストし、入力した条件に基づいて SPP が指定したディレクトリまたはネットワークで見つける資産のリストが表示されます。
5. 制約を追加または削除することができます：
   a. ＋**［追加］**をクリックすると、検索条件に制約が追加されます。
   b. －**［削除］**をクリックすると、対応する制約が検索条件から削除されます。
6. **［OK］**をクリックし、選択した内容が保存します。

接続テンプレートの編集（資産検出）

SPP が検出された資産に接続し、通信する方法を変更することができます。デフォルトの**［接続テンプレート］**は**「なし」**なので、資産は手動で認証されます。

［資産管理］＞［検出］＞［資産］＞（資産検出ジョブの追加または編集）**＞［新しい資産検出ジョブダイアログ］＞［資産検出ルール］タブ＞**（資産検出ルールの追加）**＞［新しい資産検出ルールダイアログ］＞［接続テンプレート］**に移動します。

検出の詳細

- SPP は一度資産を作成すると、別のジョブによって資産が再検出された場合、資産を再作成または変更しようとはしません。
- 検出時に見つかった SSH ホストキーは、自動的に受け入れられます。

- 1 つの資産検出ジョブに対して複数のルールを設定することができます。SPP が資産検出ジョブを実行するとき、複数のルールで資産を発見した場合、資産を検出した最初のルールの接続とプロファイルの設定を適用します。

接続テンプレート情報の編集手順

1. **［新しい資産検出ルール］**ダイアログに移動し、**［接続テンプレート］**タブを選択します。

2. **［接続テンプレート］**タブでは、**［検出されたプラットフォームを使用］**がデフォルトで選択されています。このオプションの選択を解除すると、［プラットフォーム］フィールドを使用して別のプラットフォームを選択することができるようになり、選択した製品に基づいて追加の情報を入力する必要が生じる場合があります。

3. **［認証タイプ］**を選択し、選択したものに必要の情報を入力します。
    - **SSH キー**：SSH 認証キーを使用して資産に認証するには、**［SSH キーの生成および展開］**を選択します。
        - **新しい SSH キーを自動的に生成して展開します**：新しい SSH 認証キーを生成して展開する場合は、このオプションを選択します。
        - **新しい SSH キーを自動的に生成して自分で展開します**：このオプションを選択すると、SSH 認証キーが生成され、この公開キーがサービスアカウントの管理システム上の認証キーファイルに手動で追加されます。詳細については、「公開 SSH キーのダウンロード」を参照してください。SSH 認証キーは SPP が資産を作成したとに利用可能になります。このオプションを選択しない場合、SPP は、SSH 認証キーを自動的にインストールします。このオプションを選択した場合、SPP はキーを作成し、作成中の SPP 資産と関連付けますが、管理対象システムにインストールしてくれるわけではありません。
        - **SSH キーをインポートして自分で展開します**：このオプションを選択し、**［参照］**で SSH 認証キーをインポートし、**［パスワード］**を入力します。秘密キーは、サービスアカウントに関連付けられます。

            > **メモ:** SPP は、現在 authorized key のオプションを管理していません。インポートされた鍵に、資産上の authorized key ファイルで構成されたオプションがある場合、SPP によって鍵がローテートされたときに、これらのオプションは保持されません。

- SSH キーを生成するか、インポートするかによって、次のように表示されます。
  - **SSH キー**：（インポート）［参照］をクリックして、インポートする SSH キーを選択します。**［SSH キーのインポート］**ダイアログで、秘密キーファイルを参照し、**［パスワード］**を入力します。
  - **キーのコメント**：（生成）意味のあるコメントを入力します。空白のままだと、コメントのデフォルトは「Generated by Safeguard」になります。
  - **サービスアカウント名**： サービスアカウントの名前を入力します。
  - **パスワード**：（自動生成）パスワードを入力します。
  - **サービスアカウントパスワードプロファイル**：編集または削除できます。利用可能なプロファイルは、全般タブ（資産検出）で選択したパーティションに基づきます。
  - **サービスアカウント SSH キープロファイル**：編集または削除できます。利用可能なプロファイルは、全般タブ（資産検出）で選択したパーティションに基づきます。
- **ディレクトリアカウント**：Microsoft Active Directory などの外部 ID ストアからサービスアカウントを使用して資産に認証を行うには、サービスアカウントを選択します。
  - **アカウント名**： **［参照］**をクリックして、ディレクトリアカウントを選択します。
  - **サービスアカウントパスワードプロファイル**：編集または削除することができます。利用可能なプロファイルは、**［全般］**タブ（資産検出）で選択したパーティションに基づきます。
- **パスワード**：ローカルのサービスアカウントとパスワードを使用して資産に認証する場合
  - **［アカウント名］**と**［パスワード］**を入力します。
  - **［サービスアカウントパスワードプロファイル］**は、編集または削除することができます。利用可能なプロファイルは、全般タブ（資産検出）で選択したパーティションに基づきます。
- **なし**：資産に関連するアカウントは管理されず、資産に関連する資格情報は保存されません。

4. 選択された**認証タイプ**に応じて、以下の情報が必要になる場合があります。

   - **権限昇格コマンド**：
     必要な場合は、特権昇格コマンド（sudo など）を入力します。これは、システム上で特権的なアクセスを必要とするコマンドや、Unix ベースのシステムでアカウントを管理するコマンド、つまり SSH キーの確認と変更、アカウントの検出のための接頭辞として使用されます。

     sudo コマンドに以下が続きます：

     - AuthorizedKeyCommand

     ユーザーの公開鍵を検索するプログラムを指定します。

     - cat
     - chmod
     - chown
     - chuser
     - cp
     - dscacheutil
     - dscl
     - echo
     - egrep
     - find
     - grep
     - host
     - ls
     - mkdir
     - modprpw (hpux only)
     - mv
     - psswd
     - pwdadm
     - rm
     - sed
     - sshd
     - ssh-keygen
     - tee
     - test
     - touch
     - usermod

   資産を追加する際に、このコマンドを使用して**［接続のテスト］**を実行します。詳細については、「接続のテスト」を参照してください。

   特権昇格コマンドは、非対話的に、つまり、パスワードの入力を要求せずに実行する必要があります。詳細については、「Unix ベースシステムの準備」を参照してください。

   パスワードは 255 文字までに制限されています。

   - **ポート**：接続に使用するポート番号を入力します。
   - **セッションリクエストの有効化**：このチェックボックスはデフォルトで選択されており、許可されたユーザーが検出された資産のセッションアクセスをリク

エストできることを示します。資産へのセッションリクエストを許可しない場合は、このチェックボックスをオフにします。

- **RDP ポート**：RDP セッションリクエストに使用されるターゲットサーバーのアクセスポートを指定します。
- **SSH セッションポート**：SSH セッションリクエストに使用されるターゲットサーバーのアクセスポートを指定します。

- **接続のタイムアウト：**接続タイムアウトとコマンドタイムアウトの両方の待ち時間を入力します（秒）。
- **特権レベルパスワード**：設定へのアクセスを許可する system enable パスワードを入力します。
- **Client ID**：アプリケーションのクライアント ID を入力します（例：ServiceNow や SAP の場合）。
- **SSL 暗号化の使用**：SPP がこの資産との通信を暗号化することを有効にするには、このオプションを選択します。強制的に暗号化するように構成されている Microsoft SQL Server でこのオプションを選択しない場合、**［接続のテスト］**は信頼されていない暗号化を使用し、有効な資格情報で成功します。SPP データベースサーバーがどのように SSL を使用するかの詳細については、「SPP データベースサーバーでどのように SSL を使用しますか？」を参照してください。
- **SSL 証明書の検証**：このオプションを使用して、資産で SSL 証明書の検証を有効または無効にします。有効にすると、SPP が資産に接続するたびに、資産が提示する証明書の署名権限を信頼できる CA 証明書ストアにある証明書と比較します。SPP が資産を管理するためには、信頼が確立されている必要があります。SPP が SSL 証明書を検証するには、資産の署名機関証明書を信頼できる CA 証明書ストアに追加する必要があります。SPP の信頼できる CA 証明書ストアにある資産の証明書で信頼を確立したくない場合のみ、**［SSL 証明書の検証］**オプションをオフにしてください。本番環境においてこのオプションを無効にすることは推奨しません。
- **ワークステーション ID**： 該当する場合、構成されたワークステーション ID を指定します。このオプションは、IBM i システム用です。
- **インスタンス/サービス名**： SQL Server プラットフォームの場合、この資産に SQL Server の複数のインスタンスを構成している場合は、インスタンス名を指定します。ホスト上に SQL Server のデフォルト（無名）インスタンスを構成している場合は、IP アドレスとポート番号を指定する必要があります。
  Oracle プラットフォームの場合、TNSNAMES 命名法を使用して、Oracle でターゲットシステムを識別します。Oracle 環境の構成に応じて、インスタンス

（Oracle では SID とも呼ばれる）および/またはサービス名（ServiceName）を使用して、ターゲットデータベースを識別することができます。

5. **［OK］**をクリックします。

6. **［ホストの認証の確認］**を求められた場合は、**［はい］**をクリックしてホストの SSH キーを受け入れます。

資産プロファイルの追加（資産検出）

資産検出の際、SPP は検出した資産を自動的に追加し、**ルール**タブで設定した資産プロファイルの設定に従って管理を開始します。

検出の詳細

- SPP は一度資産を作成すると、別のジョブによって資産が再検出された場合、再作成や資産を変更しません。
- 検出時に見つかった SSH ホストキーは、自動的に受け入れられます。
- １つの資産検出ジョブに対して、複数のルールを設定することができます。SPP が資産検出ジョブを実行するとき、複数のルールで資産を発見した場合、資産を検出した最初のルールの接続とプロファイルの設定を適用します。

［資産管理］＞**［検出］**＞**［資産］**＞（資産検出ジョブの追加または編集）＞**［新しい資産検出ジョブ］**ダイアログ＞**［資産検出ルール］**タブ＞（資産検出ルールの追加）＞**［新しい資産検出ルール］**ダイアログ＞**［管理］タブ**に移動します。

資産プロファイル情報の編集手順

1. **［新しい資産検出ルール］**ダイアログの**［管理］**タブの**［パスワードプロファイル］**の横にある **［参照］**をクリックします。

2. 検出された資産を管理するためのプロファイルを選択します。

   > **メモ：［全般］タブ（資産検出）**で選択したパーティションに関連するプロファイルのみを選択することができます。

3. **［パスワードプロファイルの選択］**をクリックして、選択を保存します。

4. **［新しい資産検出ルール］**ダイアログで、**［SSH キープロファイル］**の横にある**［参照］**をクリックします。

5. 検出された資産を管理する SSH キープロファイルを選択します。

> **メモ**：**［全般］**タブ（資産検出）で選択したパーティションに関連するプロファイルのみを選択することができます。

6. **［SSH キープロファイルの選択］**をクリックして、選択を保存します。
7. **［新しい資産検出ルール］**ダイアログで**［資産検出ジョブ］**の隣にある**［参照］**をクリックします。
8. 検出された資産のアカウント検出ジョブを選択します。選択は自動で保存されます。
9. 選択したら、**［アカウント検出ジョブの選択］**ダイアログを終了します。
10. **［新しい資産検出ルール］**ダイアログで、**［管理ネットワーク］**ドロップダウンを使用して使用するネットワークを選択します。

スケジュールタブ

［資産管理］＞［検出］＞［資産］＞（資産検出ジョブの追加または編集）

スケジュールタブで、資産検出ジョブを実行するタイミングを設定します。

［実行間隔］を選択すると、入力した実行の詳細に従ってジョブが実行されます。（**［実行間隔］**をクリアすると、スケジュールの詳細が失われます）。

- 実行間隔を選択します：
    - **なし**：設定されたスケジュールに従ってジョブが実行されることはありません。手動でジョブを実行することは可能です。
    - **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
    - **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、**［実行間隔 = 2/時間/正時@分 = 15］**と設定します。
    - **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
    - **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。

- **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2/月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

- 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。**＋［追加］**または **-［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、［**時間ウィンドウを使用］**を選択します。

  - 開始 22：00：00、終了 23：59：00
  - 開始 00：00：00、終了 2：00：00

  開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

  ［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

  隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

  日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行が終了すると、そのタスクは次の即時インターバルに再スケジュールされます。

資産検出ジョブの削除

資産検出ジョブを削除することができます。

1. **［資産管理］＞［検出］**を開きます。
2. **［資産］**タブで削除する資産検出ジョブを選択します。
3. **［削除］**をクリックします。
4. **［OK］**をクリックします。

10.5.2 資産検出の結果

1 つまたは複数の資産検出ジョブを実行した結果を表示することができます。

1. **［資産管理］＞［検出］＞［資産］＞**（資産検出ジョブを追加または編集する）に移動します。
2. **［資産検出結果］**タブで：
    - 完了したジョブの時間枠を、過去 24 時間、過去 7 日間、過去 30 日間、過去 60 日間、過去 90 日間で選択するか、**［カスタム］**をクリックして、カスタム時間枠を作成します。
    - **［更新］**をクリックすると、結果が更新されます。
3. **［検索］**をクリックし、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。
4. 列をクリックすると、各ジョブに表示される列情報を並べ替えることができます。
    - **日付/時間：**資産検出ジョブが正常に実行された直近の日付と時間
    - **ユーザー**：ジョブを実行したユーザー、またはジョブが自動スケジュールで実行されている場合は、自動化システム
    - **イベント：**資産検出に成功しました、資産検出に失敗しました、資産検出が開始されましたのいずれか
    - **パーティション：**検出された資産を管理するパーティション
    - **アプライアンス：**APP アプライアンスの名前
    - **ディレクトリ：**該当する場合、資産検出ジョブが実行されたディレクトリの名前
    - **資産数**：検出ジョブで見つかった資産の数

10.5.3 アカウント検出

アカウント検出ジョブには、SPP が資産に対してアカウント検出を実行するために使用するルールが含まれています。アカウント検出ジョブを追加すると、検出されたアカウントを自動的に管理するかどうか、サービスを検出するかどうか、および依存するシステムを自動的に構成するかどうかを特定できます。

検出ジョブの範囲内のアカウントには、以前に SPP パーティションに（手動で）追加されたアカウントが含まれる場合があります。詳細については、「アカウントの追加」を参照してください。

アカウント検出ジョブを構成およびスケジュールするには、次のいずれかを実行します：

- アカウント検出ジョブを作成または編集し、**［発生回数］**ボタンを使用してアカウント検出ジョブに資産を関連付けることができます。

  > **重要:** **［発生回数］**をクリックして、アカウント検出ジョブに関連付ける必要があります。資産をアカウント検出ジョブに関連付けない場合、アカウントは検出されません。

- 資産を作成または編集し、その過程でアカウント検出ジョブを割り当てまたは作成することができます。詳細については、「資産の追加」を参照してください。

サポートされるプラットフォーム

SPP は、次のプラットフォームでのアカウント検出をサポートしています：

- AIX
- HP-UX
- Linux/Unix（ベース）
- MAC OS X
- Solaris
- Windows（サービスおよびタスク）

プロパティとツールバー

［資産管理］＞［検出］＞［アカウント］に移動します。

次のツールバーボタンを使用して、アカウント検出ジョブを管理します。

表：アカウント検出：ツールバー

オプション	説明
＋ 新しいアカウント検出ジョブ	アカウント検出ジョブを追加します。詳細については、「アカウント検出ジョブの追加」を参照してください。
削除	選択したアカウント検出ジョブを削除します。
詳細の表示	選択したアカウント検出ジョブを編集します。行をダブルクリックすると編集ダイアログが開きます。

オプション	説明
アカウントの検出	選択したアカウント検索ジョブのアカウントを検索します。**［資産］**ダイアログで資産を選択します。**［タスク］**ポップアップが表示され、進行と完了がわかります。
サービスの検出	選択したアカウント検出ジョブ上のサービスを検出します。**［資産］**ダイアログで資産を選択します。**［タスク］**ポップアップが表示され、進捗と完了がわかります。
発生回数	アカウント検出ジョブに関連付けられた資産を追加、削除、更新します。 **重要**：アカウントを検索するためには、資産をアカウント検出ジョブに関連付ける必要があります。
エクスポート	このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
更新	アカウント検出ジョブのリストを更新します。
検索	一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

アカウント検出ジョブがグリッドに表示されます。

表：アカウント検出：アカウント検出ジョブグリッド

列名	説明
名前	検出ジョブの名前
作成者	ジョブの作成者
検出タイプ	実行された検出のタイプ（Windows、Unix、ディレクトリ）
ディレクトリ	検出ジョブが実行されるディレクトリ
パーティション	検出された資産や、アカウントを管理するパーティション
スケジュール	検出ジョブの実行タイミング
サービスの検出	ジョブがサービスアカウントを検出する場合は、チェックマークが表示されます。

列名	説明
自動設定	サービス検出ジョブで検出されたアカウントが、資産の依存アカウントとして自動的に構成される場合、チェックマークが表示されます。
資産	アカウント検出ジョブに割り当てられた資産の総数。アカウント検出ジョブにアカウントが割り当てられていないため、データが検出されない場合は、⚠警告が表示されます。
説明	検出ジョブの説明

アカウント検出ジョブワークフロー

SPP のアカウント検出ジョブは、プロファイルの範囲内にある資産のアカウントを検出します。詳細については、「プロファイルとは」を参照してください。アカウント検出ジョブには、サービス検出を含めることができます。

アカウント検出ジョブは、設定、スケジュール、テスト、実行が可能です。ジョブの実行後、アカウントが自動的に管理されるように識別されていない場合、そのアカウントを管理するかどうかを選択することができます。

1. アカウント検出ジョブを作成して資産を関連付けるか、資産を作成してアカウント検出ジョブを関連付けます。
    - アカウント検出ジョブを作成してから資産を追加する。詳細については、「アカウント検出ジョブの追加」を参照してください。
    - 資産を作成してからアカウント検出ジョブを関連付ける。詳細については、「資産の追加」を参照してください。
2. アカウント検出ジョブは、自動的に実行されるようにスケジュールすることができます。また、以下のいずれかの方法で、これらのジョブを手動で起動することができます。
    - **［資産管理］**>**［検出］**>**［アカウント］**>  **［アカウントの検出］**または  **［サービスの検出］**をクリックします。
    - **［資産管理］**>**［資産］**>  （詳細の表示）>  **［アカウントの検出］**をクリックします。
3. アカウント検出ジョブの実行後、**［検出］**>**［検出された項目］**>**［アカウント］**から、管理対象アカウントをマークできます。

- 選択したアカウントを SPP で管理しないようにするには、⊘ **[無効化]** をクリックします。
- 選択したアカウントを管理し、デフォルトプロファイルのスコープに割り当てるには、■ **[有効化]** をクリックします。

> **メモ**: 検出ジョブは、状態に関係なく検出ルールの基準に一致するすべてのアカウントを発見し、検出されたアカウントのうち現在存在しないもののみをレポートします。アカウントの検出では、既存のアカウントは更新されません。

実行された検出ジョブの情報については、アクティビティセンターを検索してください。SPP は、**[アカウント検出アクティビティ]** カテゴリにあるアカウント検出イベントを一覧表示します。

アカウント検出ジョブの追加

SPP がどのようにアカウント検出を実行するかを管理するルールを設定するのは、資産管理者またはパーティションの委任管理者の責任です。詳細については、「アカウント検出ジョブワークフロー」を参照してください。

アカウント検出ジョブの追加手順

1. **[資産管理]** > **[検出]** > **[アカウント]** に移動します。
2. ＋ **[新しいアカウント検出ジョブ]** をクリックして、**[新しいアカウント検出ジョブ]** ダイアログを開きます。
3. **[全般]** タブで以下の情報を入力します：
   - **名前：** アカウント検出ジョブの名前を入力します。
   - **説明**：アカウント検出ジョブの説明テキストを入力します。
   - **パーティション**：**[参照]** してパーティションを選択します。また、**[パーティションの選択]** ダイアログ（**[参照]** ボタンからアクセス可能）から **[新しいパーティション]** をクリックして、新しいパーティションを追加することもできます。

     > **重要**：検出ジョブの保存後は、パーティションを変更することはできません。
4. **[情報]** タブで、以下の情報を入力します：

- **検出タイプ：**プラットフォームを選択します。検出タイプは、**［全般］**タブで選択したパーティションに関連する資産に対して有効であることを確認します。
- **サービスの検出**：（Windows アカウントのみ、デフォルトでは非選択）このチェックボックスを選択すると、検出ジョブの実行時にサービスが検出されます。

  ［サービスの検出］を選択すると、**［自動的に依存システムを設定］**チェックボックスも使用できます。このチェックボックスを選択すると、サービス検出ジョブで検出されたディレクトリアカウントは、サービスまたはタスクが検出された資産の依存アカウントとして自動的に構成されます。依存関係が見つかると、［アカウント依存］タブ（資産）から手動で削除することのみが可能です。

5. **［アカウント検出ルール］**タブは、アカウント検出ジョブが作成された後にのみ利用できます。詳細については、「アカウント検出ルールの追加」を参照してください。

6. **［スケジュール］**タブ以下の情報を入力します：
   - 実行間隔を選択します：
     - **なし**：設定されたスケジュールに従ってジョブが実行されることはありません。手動でジョブを実行することは可能です。
     - **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
     - **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、**［実行間隔 = 2/時間/正時@分 = 15］**と設定します。
     - **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
     - **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
     - **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間**

隔 = 2/月/開始 = 1:00:00/その月の曜日/First/Saturday］と設定します。

- 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。＋**［追加］**または **-［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、［**時間ウィンドウを使用］**を選択します。
  - 開始 22：00：00、終了 23：59：00
  - 開始 00：00：00、終了 2：00：00

  開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

  ［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

  隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

  日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

  スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行が終了すると、そのタスクは次の即時インターバルに再スケジュールされます。

7. **［OK］**をクリックします。

> **メモ**：新しいアカウント検出ジョブを保存すると、**［アカウント検出ルール］**タブが利用可能になり、ルールを追加、削除、編集、コピーすることができます。詳細については、「アカウント検出ルールの追加」を参照してください。

8. 以下のいずれかの方法を使用して、アカウント検出ルールを適用する資産を選択します。
   - 資産に移動し、アカウント検出ルールを設定します。詳細については、「アカウント検出タブ（資産の追加）」を参照してください。
   - **［アカウント検出］**ジョブグリッドの**［資産数］**列のリンクをクリックして、資産を選択します。詳細については、「アカウント検出」を参照してください。

アカウント検出ルールの追加

［アカウント検出ルール］ダイアログを使用して、ディレクトリアカウントを検出するために使用する検索条件を定義します。

Active Directory からアカウントに動的にタグ付けすることができます。さらに、Active Directory のグループのメンバーシップ、またはアカウントが Active Directory の組織単位（OU）にある場合に基づいて、動的なアカウントグループを追加することができます。

> **メモ：**Unix の場合、すべての検索語句が完全一致で返されます。ADM のユーザー名検索では、ADM のみが返され、AADMM や 1ADM2 は返されません。ADM を含むすべての名前を検索するには、検索語に「**.***」を含める必要があります（**.*ADM.***）。
>
> Windows とディレクトリの場合、検索語は結果に含まれます。ADM のユーザー名検索では、ADM、AADMM、および 1ADM2 が返されます。
>
> **すべての検索語は、大文字と小文字が区別されます。**（大文字と小文字を区別しない）Windows プラットフォームでは、大文字と小文字に関係なく adm で始まるすべてのアカウントを検索するには、**[Aa][Dd][Mm].*** と入力する必要があります。

アカウント検出ルールの追加手順

1. **［資産管理］**＞**［検出］**＞**［アカウント］**に移動します。
2. 既存のアカウント検出ジョブを選択し、**［詳細の表示］**をクリックします。
3. **［アカウント検出ルール］**タブで **［編集］**をクリックします。
4. **［追加］**をクリックして**［新しいアカウント検出ルール］**ダイアログを開きます。
5. **［名前］**にアカウント検出ルールの名前を入力します。上限 50 文字
6. **［条件］**から検索タイプを選択します。

   前の**［アカウント検出］**ダイアログの**［検出タイプ］**が Windows または Unix の場合、**［制約］**または**［すべて検索］**で検索することができます。**［検出タイプ］**がディレクトリの場合は、**［名前］**、**［グループ］**、**［LDAP フィルタ］**を利用できます。

   - **名前：**アカウント名で検索する場合はこのオプションを選択します。
     - 通常の検索（ディレクトリではない）の場合、**［次を含む］**に検索する文字を入力します。
     - ディレクトリを検索する場合：

- ディレクトリを検索する場合：**[次で開始]**または**[次を含む]**を選択し、フォレスト内のサブセットを検索するために使用する文字を入力します。

  検索に Active Directory を使用する場合、Ambiguous Name Resolution（ANR）検索を使用することができます。アカウント名を完全または部分的に入力します。一度に入力できる文字列は 1 つ（完全なアカウント名または部分的なアカウント名）だけです。例えば、「t」と入力すると、「t」で始まるすべてのアカウント名が返されます。Timothy、Tom、Ted など。しかし、「Tim, Tom, Ted」と入力すると、結果は何も表示されません。

- **[参照]**をクリックして、ディレクトリ内で検索するコンテナを選択します。**[検索場所のフィルタ]**に場所が表示されます。
- **[サブコンテナのオブジェクトを含める]**を選択して、サブコンテナを検索対象に含めます。
- **[プレビュー]**をクリックし、**[アカウント]**ダイアログで**[名前]**と**[ドメイン名]**を含む検索結果を確認します。

◦ **グループ**：このオプションを選択すると、グループ名で検索することができます。

  ◦ ＋**[追加]**をクリックすると、**[グループ]**ダイアログが表示されます。

  ◦ **[次で開始]**または**[次を含む]**：グループ名の一部または全部を入力し、**[検索]**をクリックします。一度に入力できる文字列は 1 つ（グループ名の全部または一部）だけです。

  ◦ **[検索場所]**：**[参照]**をクリックし、ディレクトリ内で検索するコンテナを選択します。

  ◦ **[サブコンテナのオブジェクトを含める]**：子オブジェクトを含めるには、このチェックボックスを選択します。

  ◦ **[追加するグループを選択]**：検索結果は、このグリッドに表示されます。検出ジョブに追加するグループを 1 つまたは複数選択します。

  ◦ **[プレビュー]**をクリックし、**[アカウント]**ダイアログで**[名前]**と**[ドメイン名]**を含む検索結果を確認します。

- **制約**： このオプションを選択すると、アカウントのプロパティに基づいてアカウントが検索されます。利用可能な Unix のプロパティは、GID、UID、名前、グループです。利用可能な Windows およびディレクトリのプロパティは、RID、GID、UID、名前、グループです。すべて 255 文字の数字に制限されています。

  > **重要**：**[制約]** の選択によっては、結果が遅くなることがあります。特に **[グループ]** の使用は推奨されません。

  - 選択：

    - **RID（範囲）：** RID プロパティは、Windows と Microsoft Active Directory にのみ適用されます。1 つまたは複数の Relative Identifier 番号を入力します。複数の ID または ID の範囲を入力するには、リストの各要素を別々に入力する必要があります。例えば、**1000** と入力した後にスペースを入れ、次に、**5000-7000** と入力します。
    - **GID（範囲）**：1 つまたは複数の Group Identifier 番号を入力します。複数の ID または ID の範囲を入力するには、リストの各要素を別々に入力する必要があります。たとえば、**8** と入力した後にスペースを入れ、次に、**10-12** と入力します。
    - **UID（範囲）**：1 つまたは複数の User Identifier 番号を入力します。複数の ID または ID の範囲を入力するには、リストの各要素を別々に入力する必要があります。たとえば、**1** と入力した後にスペースを入れ、次に **5-7** と入力します。
    - **名前（正規表現）：名前（正規表現）**の使用は、結果が遅くなる可能性があるため、お勧めしません。アカウント名で検索する場合は、**名前**（前述）を使用することをお勧めします。OpenLDAP 資産の場合は、部分文字列のマッチングのみが可能です（たとえば、abc* のような検索語句）。マッチングは大文字小文字を区別しません。使用するには、1 つの正規表現パターンを入力します。詳細は、「正規表現」を参照してください。
    - **グループ（正規表現）**：グループ（正規表現）の使用は、検索結果が遅くなる可能性があるため、お勧めしません。グループ名で検索するには、**グループ**（前述）を使用することをお勧めします。OpenLDAP 資産では、部分文字列のマッチングのみが利用可能です（たとえば、abc* のよう

な検索語句)。マッチングは大文字小文字を区別しません。使用するには、1 つの正規表現パターンを入力します。詳細については、「正規表現」を参照してください。

- ディレクトリを検索する場合：
  - **［参照］**をクリックして、ディレクトリ内で検索するコンテナを選択します。その場所は**［検索場所の選択］**に表示されます。
  - サブコンテナを検索対象に含めるには、**［サブコンテナのオブジェクトを含める］**を選択します。
  - **［プレビュー］**をクリックし、**［アカウント］**ダイアログで、**［名前］**と**［ドメイン名］**を含む検索結果を確認します。

7. **検出済みアカウントの自動管理**：検出されたアカウントを自動的に SPP に追加する場合に選択します。選択すると、**［デフォルトパスワードの設定］**を選択して、パスワードを入力することができます。

8. **パスワード同期グループ：［参照］**をクリックして関連するすべてのアカウントで検証とリセットを制御するパスワード同期グループを選択します。また**［追加］**を使用して新しい同期グループを追加することもできます。「パスワード同期グループ」を参照してください。

9. **パスワードプロファイル：**プロファイルが同期グループに自動的に割り当てられなかった場合（前の手順）、**［参照］**をクリックしてプロファイルを選択し、検出されたアカウントの構成設定を特定します。また、新しいプロファイルを使用して、新しいパスワードプロファイルを追加することもできます。詳細については、「パスワードプロファイル」タブ（パーティション）を参照してください。

10. **デフォルトパスワードの設定：**選択した場合、入力したパスワードは、資産で初めてパスワードが変更されるまで、検出された資産のプレースホルダーとなります。**［デフォルトパスワードの設定］**が選択されていない場合、資産で初めてパスワードが変更されるまで、パスワードは保存されません。パスワードが変更される前にアカウントが要求された場合、エラーが発生することがあります。

    デフォルトのパスワードは、SPP で設定されていますが、資産上では設定されていません。

    > **メモ：** パスワードを設定するアカウント検出ルールが構成され、パスワードを自動的に変更するパスワード プロファイル (パスワード プロファイルに割り当てるオプショ

> ンで選択) も構成されている場合、パスワード変更スケジュールが優先され、アカウントは検出時にパスワードが変更されます。

11. **SSH キー同期グループ**：**[参照]** をクリックして、SSH キー同期グループを選択します。詳細については、「SSH キー同期グループの設定」を参照してください。

12. **SSH キープロファイル**：同期グループにプロファイルが自動的に割り当てられなかった場合、詳しくは、「SSH キープロファイルタブ（パーティション）」を参照してください。

13. **デフォルトの SSH キーの設定**：デフォルトの SSH キーを設定する場合に選択します。**[SSH キーのインポート]** ダイアログでは、SPP 以外で生成された SSH キーの秘密鍵ファイルをインポートして、アカウントに割り当てることができます。**[参照]** をクリックして鍵ファイルをインポートし、**[パスワード]** を入力して **[OK]** をクリックします。

    資産上のアカウントにすでに手動で設定されている SSH キーをインポートする場合、鍵をインポートする前に、まず鍵が正しく設定されていることを確認することをお勧めします。たとえば、SSH クライアントプログラムを実行して、秘密鍵が資産へのログインに使用できることを確認できます：ssh -i <privatekeyfile> -l <accountname> <assetIp> authorized key の設定方法の詳細については、ターゲットプラットフォームの OpenSSH サーバーのドキュメントを参照してください。

    > **メモ：** SPP は、現在、authorized key のオプションを管理していません。インポートされた鍵に、資産上の authorized key ファイルで構成されたオプションがある場合、SPP によって鍵がローテートされたときに、これらのオプションは保持されません。

14. **パスワードリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してパスワードリリースリクエストが有効であることを示しています。このオプションをオフにすると、誰かがこのアカウントのパスワードをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは自分が認証されたユーザーである資格の範囲内で、すべてのアカウントのパスワードをリクエストすることができます。

15. **セッションリクエストの有効化**：このチェックボックスはデフォルトで選択されており、このアカウントに対してセッションアクセスリクエストが有効になっていることを示します。このオプションをオフにすると、誰かがこのアカウントを使用してセッションアクセスをリクエストするのを防ぐことができます。デフォルトでは、ユーザーは自分が認証ユーザーである資格の範囲内で、どのアカウントに対してもアクセスリクエストを行うことができます。

16. **SSH キーリクエストの有効化：**（ディレクトリアカウントのみ）**すべてのパーティションで使用可能**：選択した場合、どのパーティションでもこのアカウントを使用でき、パス

ワードは他の管理者に渡されます。たとえば、このアカウントは、他の資産の依存アカウントやサービスアカウントとして使用することができます。潜在的には、このアカウントとしてサービスを実行している資産があり、サービスアカウントが変更されたときに、それらの資産を更新することができるかもしれません。選択しない場合、パーティション所有者や他のパーティションは、そのアカウントの存在を知ることはありません。アーカイブサーバーはパーティションに拘束されませんが、アーカイブサーバーがディレクトリアカウントで構成されている場合は、このオプションを選択する必要があります。

17. **タグ：**タグを選択または新しいタグを追加することができます。
18. **［適用］**をクリックします。
19. **［OK］**をクリックして、アカウント検出ジョブを保存します。

アカウント検出ジョブの削除

資産検出ジョブを削除することができます。

アカウント検出ジョブの削除手順

1. **［資産管理］＞［検出］＞［アカウント］**に移動します。
2. アカウント検出ジョブを選択します。
3. **［削除］**をクリックして、選択した資産検出ジョブを削除します。
4. **［はい］**をクリックします。

10.5.4 アカウント検出結果

1 つまたは複数のアカウント検出ジョブを実行した結果を表示することができます。検出の結果を表示するには、「検出されたアカウント」を参照してください。

1. **［資産管理］＞［検出］＞［アカウント］**（アカウント検出ジョブの追加または編集）に移動します。
2. **［アカウント検出結果］**グリッドで：

- 表示する完了したジョブの時間枠を選択します（過去 24 時間、過去 7 日間、過去 30 日間、過去 60 日間、過去 90 日間を選択可能）。または、**［カスタム］**をクリックして、カスタム時間枠を作成します。
- **［更新］**をクリックして、結果を更新します。

3. 各ジョブについて、以下の情報表示を確認します：
   - **日付/時間**：アカウント検出ジョブが正常に実行された直近の日付と時間
   - **ユーザー**：ジョブを実行したユーザー、またはジョブが自動スケジュールで実行されている場合は Automated System。
   - **イベント**：アカウント検出成功、アカウント検出失敗、アカウント検出開始のいずれか
   - **資産:** アカウント検索ジョブに関連付けられた資産
   - **パーティション**：検出されたアカウントが管理されるパーティション
   - **プロファイル**：検出されたアカウントを管理するパーティションプロファイル
   - **アプライアンス**：SPP アプライアンスの名前
   - **アカウント数**：検出ジョブで検出されたアカウントの数

10.5.5 検出されたアカウント

パーティションで実行されたことのあるすべてのアカウント検出ジョブの結果（言い換えると、これまでに検出されたすべてのアカウント）が表示され、アカウントを有効または無効にすることができます。

作成されたアカウントは、**［検出されたアカウント］**のプロパティグリッドに管理アカウントとして表示されます（下記参照）。詳細については、以下を参照してください。

検出されたアカウントへのアクセス

［資産管理］＞［検出］＞［検出された項目］＞［アカウント］に移動します。

これらのツールバーボタンを使用して、検出されたアカウントを管理します。

表：検出：検出されたアカウントツールバー

オプション	説明
管理	**［管理］**を選択すると、選択した 1 つまたは複数のアカウントのステータスが管理に変更されます。SPP によって管理されている

オプション	説明
	アカウントは、資産のアカウントおよびアクセスリクエストポリシーのリストに追加されます。検出ジョブは、アカウントを管理済みとマークするか、このボタンを使用して選択し管理済みとマークすることができます。
無視	**［無視］**を選択すると、**［ステータス］**を**［無視］**に設定し、SPP が選択したアカウントを管理しないようにします。アカウントのステータスが **［なし］**である場合、結果としてステータスは**［無視］**になります。 アカウントのステータスが**［管理］**の場合は、**［アカウント］**ページでステータスを変更する必要があります。
無視済みの表示	ステータスが **無視**（無効）であるアカウントを表示します。
無視済みの非表示	ステータスが **無視**（無効）であるアカウントを非表示にします。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートする場合に使用します。詳細は、「データのエクスポート」を参照してください。
更新	検出されたアカウントの最新リストを取得し、表示します。**［無視済みの非表示］**を選択した場合、無視済みのアカウントは表示されません。
検索	検索に使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

以下の情報が表示されます。

表：検出：検出されたアカウントプロパティグリッド

プロパティ	説明
ステータス	検出されたアカウントは以下の通りです： • **管理**：検出されたアカウントは管理されています。 • 空白（値なし）：検出されたアカウントは、検出時に自動管理されていません。 • **無視**：自動管理されておらず、検出時に無視された検出されたアカウント • **無効**：以前は管理されていたがその後無視された検出されたアカウント

プロパティ	説明
名前	資産に関連付けられた検出されたアカウントに対応する SPP のアカウントの名前。これはローカルアカウントまたは Active Directory アカウントです。
ドメイン名	アカウントが Active Directory アカウントの場合、そのアカウントのドメイン名
資産名	アカウントが検出された資産の名前
アカウント検出ジョブ	検出スケジュールの名前
アカウント検出ルール	アカウントの検出に適用されたアカウント検出ルールの名前
日付/時間が検出されました	サービスまたはタスクが検出された日付と時間

10.5.6 サービス検出結果

サービス検出のセットアップ

Windows サービスを検出するには、まず、アカウント検出ルールを含むアカウント検出ジョブを作成し、**［サービスの検出］**を選択する必要があります。検出ジョブが実行されると、サービスが検出されます。サービスの検出は、検出ルールに依存しません。詳細については、「アカウント検出ジョブの追加」を参照してください。

サービス検出結果の表示手順

1. **［資産管理］**>**［検出］**>**［アカウント］**>（アカウント検出ジョブの追加と編集）に移動します。
2. **［サービス検出結果］**タブで：
    - 表示したい完了したジョブの時間枠を選択します。過去 24 時間、過去 7 日間、過去 30 日間、過去 60 日間、過去 90 日間のいずれかを選択します。または、**「カスタム」**をクリックして、カスタム時間枠を作成します。
    - **［更新］**をクリックすると、結果が更新されます。
3. **［検索］**をクリックし、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

4. 各ジョブについて、以下の情報を確認します：
    - **日付/時刻**：アカウント検出ジョブが正常に実行された直近の日付
    - **ユーザー**：ジョブを実行したユーザー、またはジョブが自動スケジュールで実行されている場合は Automated System。
    - **イベント**：サービス検出開始、サービス検出成功、サービス検出失敗のいずれか。成功と失敗は、**［サービス検出結果］**ダイアログの**［イベント］**に表示されます。3 つのイベントはすべてアクティビティセンターに表示されます。
    - **資産**: 検出ジョブに関連付けられた資産
    - **パーティション**：検出されたサービスアカウントが管理されるパーティション
    - **プロファイル**：検出されたサービスアカウントを管理するパーティションプロファイル
    - **アプライアンス**：SPP アプライアンスの名前
    - **サービス数**：検出ジョブ中に検出されたサービスアカウントの数

10.5.7 検出されたサービス

検出されたサービスには、サービスが検出された選択されたパーティションの情報が表示されます。

資産管理者または委任された管理者は、Windows 資産をスキャンし、認証資格情報を必要とする可能性のある Windows サービスを検出するサービス検出ジョブを構成することができます。

管理された Windows 資産で検出できるサービスの種類は以下の通りです：

- Windows サービス
- スケジュールタスク
- IIS アプリケーションプール
- Com+アプリケーション

Windows 資産が Windows ドメインに参加している場合、認証情報は Windows 資産上のローカルか、Active Directory の認証情報である可能性があります。

> **重要**: Windows SSH 資産では、ローカルアカウントはドメインアカウントとして実行されているサービスを検出するのに必要なアクセス権を持っていません。そのため、Windows SSH 資産のサービスアカウントとしてローカルアカウントが使用されている場合、SPP はその資産上でローカルアカウントとして実行されているサービスのみを検出し、ドメインアカウントの依存関係は更新されません。

重要：資産の管理タイプが Windows または WinRM（デスクトップまたはサーバー）の場合、サービス検出を使用して IIS アプリプールを検出するには、Web サーバーロールの管理ツールセクションで次の機能のいずれかをインストールする必要があります。

- IIS 6 メタベース互換性および IIS 6 WMI 互換性（詳しくは、「Metabase Compatibility with IIS 7 and Above」を参照してください）。
- IIS 管理スクリプトとツール（詳しくは、「Managing Applications and Application Pools on IIS 7.0 with WMI」を参照してください）。

メモ: 検出機能は、Windows Server および Windows SSH プラットフォームの両方で、これらのサービスの種類ごとにサポートされていますが、IIS App プールおよび Com+ アプリケーションのアカウント依存性の更新をサポートしているのは Windows SSH プラットフォームのみです。

サービス検出ジョブの自動実行と手動実行

- **［サービスの検出］**チェックボックスが選択されている場合、サービス検出ジョブはバックグラウンドで自動的に実行されます。［**依存システムを自動的に構成する**］チェックボックスが選択されている場合、サービス検出ジョブで検出されたディレクトリアカウントは、サービスが検出された資産の依存アカウントとして自動的に構成されます。詳細については、「アカウント検出ジョブの追加」を参照してください。
- **［資産管理］＞［資産］＞［検出されたサービス］**からサービス検出ジョブを手動で実行することができます。詳細については、「検出されたサービス」タブ（資産）を参照してください。

検出されたサービスおよびタスクの既知の Safeguard アカウントへの関連付け

サービス検出ジョブは、Windows サービスを SPP ですでに管理されているアカウントと関連付けます。管理下に置かれたアカウントは、**［アカウントステータス］**に［管理済］と表示されます。

Active Directory を使用したサービス検出

Active Directory アカウントとして実行するように構成された検出されたサービスは、Safeguard によって管理されたアカウントで自動的に資産に関連付けることができます。実質的に、資産はそのアカウントに依存することになります。

自動的に関連付けるには、アカウント検出ジョブ（Safeguard がディレクトリを同期するときに実行される）で**［検出されたアカウントを自動的に管理］**チェックボックスを選択する必要があります。詳細については、「アカウント検出ルールの追加」を参照してください。アカウント依

存として構成されると、Active Directory アカウントのパスワードが Safeguard によって変更されたとき、Safeguard は資産のプロファイル変更設定に従って、資産上のサービスのパスワードを更新します。詳細については、「パスワード変更設定の追加」を参照してください。

サービス検出ジョブステータスの表示

アクティビティセンターから、サービス検出アクティビティというアクティビティカテゴリを選択すると、イベントの結果を表示することができます。「サービス検出に成功しました」、「サービス検出に失敗しました」、「サービス検出が開始されました」というイベント結果が表示されます。

検出されたサービスへのアクセス

［資産管理］ > **［検出］** > **［検出された項目］** > **［サービス］** タイルに移動します。

次のツールバーボタンを使用して、検出されたサービスを管理します。

表：検出：検出されたサービスツールバー

オプション	説明
▣ 表示 | ⊘ 無視	**［表示］** および **［無視］** ボタンは、このウィンドウの **［サービスが無視された］** 列を制御し、管理者は行を表示または無視することができます。 **［アカウントステータス］** 列は、**［検出されたアカウント］** グリッドの **［表示］** および **［無視］** ボタンで制御されます。詳細については、「検出されたアカウント」を参照してください。
無視済みの表示	ステータスが **無視**（無効）であるアカウントを表示します。
無視済みの非表示	ステータスが **無視**（無効）であるアカウントを非表示にします。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	検出されたアカウントの最新リストを取得し、表示します。**［無視済みの非表示］** を選択した場合、無視済みのアカウントは表示されません。
検索	検索に使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

グリッドには、SPP が検出した、検出されたサービスと一致する検出されたアカウントの**資産名**、**アカウント**、**ドメイン名**、**システム名**、**アカウントステータス**が表示されます。サービスは、サービス名（サービスタイプはサービス、IIS App pool、Com+ service、タスク）で識別されます。

表：検出：検出されたサービスプロパティグリッド

プロパティ	説明
資産名	サービスが検出された資産の名前
アカウント	**［検出されたアカウント］**列にマッピングされるアカウントの名前
ドメイン名	アカウントが Active Directory アカウントの場合、そのアカウントのドメイン名。依存アカウントとして設定できるのは、Active Directory アカウントのみです。
システム名	検出されたマッピングされたアカウントをホストしているシステムまたは資産
アカウントステータス	**［アカウントステータス］**列は、**［検出されたアカウント］**グリッドの**［管理］**および**［無視］**ボタンで制御されます。詳細については、「検出されたアカウント」を参照してください。 検出されたアカウントは、次の通りです： • **管理**：管理されている検出されたアカウント • 空白（値なし）：検出されたアカウントは、検出時に自動管理されていません。 • **無視**：自動管理されておらず、検出時に無視された検出されたアカウント • **無効**：以前は管理されていたが、その後無視された検出されたアカウント。無効なアカウントは、資産アカウントリストから削除されず、依存アカウントとして未構成にされません。無効とマークされたアカウントは、使用も操作もできません。
依存アカウント	アカウントが資産のアカウント依存として関連付けられている場合、✔ チェックが表示されます。アカウントが資産のアカウント依存として関連付けられていない場合、値は空白になります。この自動依存関係マッピングは、資産に関連付けられたプロファイルに関連付けられたアカウント検出ジョブで、**［検出されたアカウ**

プロパティ	説明
	ントを自動的に管理］オプションが選択されている場合にのみ発生します。詳細については、「アカウント検出ジョブの追加」を参照してください。
サービスタイプ	検出されたサービスのタイプ。値は、サービス、IIS App pool、Com+ service、タスクです。
サービス名	検出されたサービスの名前
サービスが有効化されました	資産上のサービスが対象マシン上で有効である場合、✔チェックマークが表示されます。チェックマークがない場合、そのサービスまたはタスクは対象マシン上で無効になっています。
サービスが無視されました	無視とは、そのサービスがグリッドに表示されないことを意味します。言い換えれば、サービスは非表示となります。これは、このグリッドの**［表示］**または**［無視］**アクションで制御されます。
検出されたアカウント	検出されたアカウント名。このアカウントのステータスが**「管理」**の場合、**「アカウント」**、**「ドメイン名」**、**「システム名」**が表示されます。
日付/時間が検出されました	サービスが検出された日付と時間

10.5.8 SSH キーの検出

SPP に追加したアカウントに対して、1 つまたは複数の SSH キーの検出ジョブをスケジュールして自動的に実行することができます。検出ジョブのスコープ内の SSH キーには、以前に SPP パーティションに（手動で）追加された SSH キーが含まれる場合があります。

詳細については、「SSH キーの検出設定」を参照してください。

SSH キー検出ジョブが実行されると、検出された SSH キーは、選択したパーティションの**［検出された SSH キー］**タイルに一覧表示されます。また、資産（**［検出された SSH キー］**タブの下）およびアカウント（**［検出された SSH キー］**タブの下）にも表示されます。

サポートされているプラットフォーム

SSH キー検出は、以下のプラットフォームでサポートされています：

- ハードウェア/カスタム（キーの処理方法に対応するために、カスタムスクリプトが必要です）。
- Drac
- Fortinet
- Junos
- PanOs
- Window OS
- 一般的な Unix 形式のプラットフォーム
    - Linux
    - Aix
    - Hpux
    - Solaris
    - F5BigIP
    - FreeBSD
    - MacOS

SSH キー検出へのアクセス

［資産管理］＞［検出］＞［SSH キー］に移動します。

次のツールバーボタンで SSH キー検出ジョブを管理します。

表：SSH キー検出：ツールバー

オプション	説明
新しい SSH キー検出ジョブ	SSH キー検出ジョブを追加します。詳細については、「SSH キー検出ジョブの追加」を参照してください。
削除	選択したアカウント検出ジョブを削除します。
詳細の表示	選択したアカウント検出ジョブを編集します。行をダブルクリックすると編集ダイアログが開きます。
SSH キーの検出	このボタンをクリックすると、新しいウィンドウが開き、選択した SSH キー検出ジョブを実行するアカウントを 1 つ選択することができます。
発生回数	選択した SSH キーの検出設定に関連するアカウント名と資産名で表示します。［継承］列には、割り当てが資産を介して継承された関連付けである場合にチェックマークが表示されます。継承されていない場合、アカウントはプロファイル

オプション	説明
	/SSH キー検出ジョブに明示的に割り当てられています。詳細については、「プロファイルとは」を参照してください。
エクスポート	このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
更新	SSH キー検出ジョブのリストを更新します。
検索	一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

SSH キー検出ジョブがグリッドに表示されます。

表：SSH キー検出：SSH キー検出ジョブグリッド

列名	説明
名前	検出ジョブの名前
作成者	SSH キー検出ジョブの作成者を示します。
パーティション	検出された SSH キーを管理するパーティション
スケジュール	SSH キー検出ジョブの実行タイミング
プロファイル	このジョブで構成されているプロファイルの数を一覧表示します。このリンクをクリックすると、この SSH キー検出ジョブに関連する SSH キープロファイルの名前と説明を一覧表示する **［SSH キープロファイル］**ダイアログに移動します。
アカウント	プロファイルの関連付けによってこの SSH キー検出ジョブに関連付けられたアカウントの数を一覧表示します。この SSH キー検出ジョブのアカウント名と親システム名を表示するには、このリンクをクリックします。
説明	SSH キー検出ジョブの説明

SSH キー検出ジョブワークフロー

SSH キー検出ジョブは、プロファイルのスコープ内にあるアカウントの SSH キーを検出します。SSH キー検出ジョブの構成、スケジュール、実行が可能です。ジョブが実行されると、その名前のタブの下に検出された SSH キーが表示されます。以下が表示されます：Key Fingerprint、Comment （鍵の中にあるもの）、Key Type、Key Length、Asset Name、Account Name、Account Status ("managed" は Safeguard for Privileged Passwords がそのアカウントを管理していること、"disabled" は SPP がそのアカウントを管理してないこと) が表示されます。

1. SSH キープロファイルを使用してパーティションを設定します。詳細については、「SSH キープロファイル」タブ（パーティション）を参照してください。
2. SSH キー検出ジョブを作成します。詳細については、「SSH キー検出ジョブの追加」を参照してください。
3. SSH キー検出ジョブは、自動的に実行されるようにスケジュールすることができます。また、1 つのアカウントでジョブを手動で起動することもできます。
    - **［資産管理］＞［検出］＞［SSH キー］**から、実行する SSH キー検出ジョブを選択し、**［SSH キーの検出］**をクリックします。
4. SSH キー検出ジョブが実行されたら、SSH キー検出結果タイルをクリックして、見つかった SSH キーを表示します。詳細については、「SSH キー検出結果」を参照してください。

    > **メモ：**検出ジョブは、検出ルールの基準に一致する現在のすべての SSH キーを検出します。SSH キーの検出では、既存のアカウントは更新されません。

実行された検出ジョブの情報については、アクティビティセンターを検索してください。SPP は、SSH キー検出アクティビティカテゴリに SSH キー検出イベントをリストアップしています。詳細については、「アクティビティセンター」を参照してください。

SSH キー検出ジョブの追加

SPP が SSH キー検出をどのように実行するかを規定するルールを設定するのは、資産管理者またはパーティションの委任管理者の責任となります。詳細については、「SSH キー検出ジョブワークフロー」を参照してください。

SSH キー検出ジョブの追加手順

1. **［資産管理］＞［検出］＞［SSH キー］**に移動します。
2. ＋ **［新しい SSH キー検出ジョブ］**をクリックし、**［新しい SSH キー検出ジョブ］**ダイアログを開きます。
3. 以下を入力します：
    a. **名前**：アカウント検出ジョブの名前を入力します。制限：50 文字。
    b. **説明**：SSH キー検出ジョブについての説明テキストを入力します。制限: 255 文字
    c. **パーティション**：［参照］を選択してパーティションを選択します。
    d. SSH キーの検出を行うタイミングを特定するには、**［スケジュール］**タブを選択します。
        ◦ 実行間隔を選択します：
            ◦ **なし**：設定されたスケジュールに従ってジョブが実行されることはありません。手動でジョブを実行することは可能です。
            ◦ **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
            ◦ **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、**［実行間隔 = 2/時間/正時@分 = 15］**と設定します。
            ◦ **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
            ◦ **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
            ◦ **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2 /月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

- 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。＋**［追加］**または **-［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、**［時間ウィンドウを使用］**を選択します。
  - 開始 22：00：00、終了 23：59：00
  - 開始 00：00：00、終了 2：00：00

  開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

  ［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

  隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

  日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

  スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行が終了すると、そのタスクは次の即時インターバルに再スケジュールされます。

4. **［OK］**をクリックします。

SSH キー検出結果

1 つまたは複数の SSH キー検出ジョブの実行結果を表示できます。検出の結果を表示するには、「検出された SSH キー」を参照してください。

SSH キーの検出結果の表示手順

1. **［資産管理］＞［検出］＞［SSH キー］＞**（SSH キー検出ジョブを追加または編集）に移動します。
2. **［SSH キーの検出結果］**タブで：
   - 過去 24 時間から過去 7 日、30 日、60 日、90 日の範囲で、表示する完了したジョブの時間枠を選択します。または、**［カスタム］**をクリックして、カスタムの時間枠を作成します。

- **［更新］**をクリックすると、結果が更新されます。

3. 必要なものをグリッドに表示するには、**［検索］**をクリックして、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。
4. 各ジョブについて、以下の情報表示を確認します：
    - **日付/時間**： SSH キー検出ジョブが正常に実行された直近の日付と時間
    - **ユーザー**：ジョブを実行したユーザー、またはジョブが自動化されたスケジュールで実行されている場合は、**Automated System**
    - **イベント**：SSH キー検出が成功しました、SSH キー検出が失敗しました、SSH キー検出が開始しました、という SSH キー検出ジョブイベントの実行結果が表示されます。
    - **アカウント**：SSH キー検出ジョブに関連付けられているアカウント
    - **資産**： SSH キー検出ジョブに関連付けられている資産
    - **パーティション**：検出された SSH キーが管理されるパーティション
    - **SSH キープロファイル**：検出された SSH キーを管理するプロファイル
    - **アプライアンス**：SPP アプライアンスの名前
    - **SSH キー数**：表示された数字をクリックすると、そのアカウントで検出された SSH キーのリストが表示されます。

検出された SSH キー

選択したパーティションの現在の SSH キー検出結果を表示することができます。アカウントで検出されたキーの数は、アカウントの認証キーファイルで検出された SSH キーの数を反映します。

アカウントで現在使用されている SSH キーは、**［検出された SSH キー］**プロパティグリッドの**［SSH キーが管理されています］**列にチェックマークが表示されます（下記を参照）。

検出された SSH キーへのアクセス：

［資産管理］＞［検出］＞［検出された項目］＞［SSH キー］タイルに移動します。

SSH キーの結果を表示するパーティションを選択します。

次のツールバーボタンを使用して、検出されたアカウントを管理します。

表：検出：検出された SSH キーツールバー

オプション	説明
取り消し	管理されていない SSH キーのアクセス権を取り消す場合に使用します。
エクスポート	このボタンを使用すると、リストされたデータを JSON または CSV ファイルとしてエクスポートできます。詳細については、「データのエクスポート」を参照してください。
更新	検出された SSH キーの更新されたリストを取得し、表示します。SSH キーがアカウントの認証キーファイルから削除された場合、検出ジョブの実行時に検出されたリストから削除されます。
検索	一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

次の情報が表示されます：

表：検出：検出された SSH キープロパティグリッド

プロパティ	説明
フィンガープリント	認証に使用される SSH キーのフィンガープリント
アカウントステータス	SSH キーが検出されたアカウントの状態
SSH キーが管理されています	現在そのアカウントで使用されている SSH キーにチェックマークが付きます。
コメント	SSH キーに含まれるフリーフォームのコメント
キータイプ	RSA や DSA などの SSH キーのタイプ。詳しくは、「SSH キープロファイル」を参照してください。
キー長	サポートされている RSA または DSA の鍵の長さが表示されます。詳しくは「SSH キープロファイル」を参照してください。
資産名	SSH キーが検出された資産の名前
アカウント	SSH キーが検出されたアカウントの名前
日付/時間が検出されました	SSH キーが検出された日付と時間

10.6 プロファイル

SPP で現在使用されている設定済みプロファイルの情報は**プロファイル**ページに表示されます。

プロファイルへのアクセス：

［資産管理］＞［プロファイル］に移動します。

プロファイルページはセクションに分かれています：

- パスワードプロファイル
- SSH キープロファイル

10.6.1 パスワードのプロファイル

プロファイルページの**［パスワードプロファイル］**タブに、SPP で現在使用されている設定済みのパスワードプロファイルの情報が表示されます。

プロファイルページにある**［パスワードプロファイル］**タブにアクセスする手順：

［資産管理］＞［プロファイル］に移動し、**［パスワードプロファイル］**タブを表示します。必要に応じて、パーティションのドロップダウンを使用して、プロファイルの親パーティションを選択できます（デフォルトではすべてのプロファイルが表示されます）。プロファイルを選択し、✎クリックすると追加情報とオプションが表示されます。

プロファイルの 1 つを選択すると、次の情報が表示されます：

- **プロパティ**タブ：選択したプロファイルの一般的な情報が表示されます。
- **資産**タブ：選択したプロファイルに割り当てられている資産が表示されます。
- **アカウント**タブ：選択したプロファイルに割り当てられているアカウントが表示されます。

ツールバー

次のツールバーボタンを使って、プロフィールを管理します：

- ＋ **新しいプロファイル**： プロファイルを SPP に追加します。
- 🗑 **削除**：選択したプロファイルを削除します。
- ✎ **詳細の表示**：プロファイルを選択し、このボタンをクリックすると、プロファイルの追加情報およびオプションが表示されます。

- **デフォルトとして設定**：プロファイルを選択し、このボタンをクリックすると、そのプロファイルがデフォルトのプロファイルとして設定されます。
- **エクスポート**：このボタンをクリックすると、リストされたデータが JSON または CSV ファイルとしてエクスポートされます。詳細については、「データのエクスポート」を参照してください。
- **更新**：プロファイルのリストを更新します。

プロファイルページの**［パスワードプロファイル］**タブを選択すると、**［パスワードプロファイル コンポーネントの表示］**リンクが利用できます。詳細については、「パスワードプロファイルコンポーネントの表示」を参照してください。

プロパティタブ

プロパティタブには、選択したプロファイルに関する情報が表示されます。

プロパティへのアクセス：

［資産管理］＞**［プロファイル］**＞**［パスワードプロファイル］**＞（詳細の表示）＞**［プロパティ］**

プロファイルの全般プロパティには以下の情報が表示されます。

表：プロパティタブ：全般プロパティ

オプション	説明
名前	プロファイルの名前
説明	プロファイルの説明
パーティション	選択されたプロファイルが属しているパーティションの名前
削除	選択されたプロファイルを削除します。

プロファイルの確認パスワードプロパティには以下の情報が表示されます。

表：プロパティタブ：確認パスワードプロパティ

プロパティ	説明
確認パスワード設定	確認パスワードルールの名前
説明	確認パスワードルールの説明

プロパティ	説明
スケジュール	確認パスワードルールのスケジュール

プロファイルの変更パスワードプロパティには以下の情報が表示されます。

表：プロパティタブ：変更パスワードプロパティ

プロパティ	説明
変更パスワード設定	変更パスワードルールの名前
説明	変更パスワードルールの説明
スケジュール	変更パスワードルールのスケジュール

プロファイルのアカウントパスワードルールプロパティには以下の情報が表示されます。

表：プロパティタブ：アカウントパスワードルールプロパティ

プロパティ	説明
アカウントパスワードルール	アカウントパスワードルールの名前
ルール概要	アカウントパスワードルールの概要

プロファイルのパスワード同期グループプロパティには以下の情報が表示されます。

表：プロパティタブ：パスワード同期グループプロパティ

プロパティ	説明
有効	有効の場合、プロファイルの変更スケジュールに合わせて同期が実行されます。
ステータス	すべてのアカウントのパスワードがパスワード同期グループと同期しているかどうかを表示します。同期グループ内のいずれかのアカウントのパスワードが共通パスワードと一致しない場合は、ステータスが表示されます。
名前	パスワード同期グループの名前
アカウント	共有のパスワードで同期するアカウントの数
次の同期	同期グループのパスワードがすべてのアカウントでどうきされる日付

プロパティ	説明
説明	ルールに関する情報

削除：選択されたプロファイルが削除されます。

資産タブ

資産タブには、選択したプロファイルに割り当てられている資産が表示されます。

詳細ツールバーの **［資産の追加］**をクリックすると、選択したプロファイルに 1 つまたは複数の資産を追加できます。

資産へのアクセス：

［資産管理］ > **［プロファイル］** > **［パスワードプロファイル］** > （詳細の表示）> **［資産］**に移動します。

表：プロファイル：資産タブプロパティ

プロパティ	説明
名前	資産名
プラットフォーム	選択された資産のプラットフォーム
無効	資産が無効の場合、チェックマークが表示されます。
製品ライセンス	該当する場合（Windows 資産の場合）、System または Desktop など、ライセンスモデルが表示されます。
説明	資産を追加した際に入力された説明情報
タグ	資産に関連するタグ

選択したパーティションに割り当てられた資産を管理するには、詳細ツールバーのボタンを使用します。

表：プロファイル：資産タブツールバー

プロパティ	説明
資産の追加	資産をプロファイルに追加します。
削除	選択した資産を削除します。

プロパティ	説明
詳細の表示	資産を選択した後、このボタンをクリックすると、詳細と設定オプションが表示されます。
アクセスリクエスト	選択した資産に対して、アクセスリクエストサービスを有効または無効にすることができます。メニューオプションには、［セッションリクエストの有効化］および［セッションリクエストの無効化］があります。
SSH ホストキー	このドロップダウンには、SSH ホストキーの状態に応じて、以下のオプションがあります。 • SSH ホストキーの取得 • SSH ホストキーの検出 • SSH ホストキーの設定 • SSH ホストキーのダウンロード
接続のテスト	SPP が提供したサービスアカウント情報を使用して、資産にログインできることを確認します。
今すぐ同期	資産とアカウントによるディレクトリ追加（インクリメンタル）同期処理を実行します。同期はプロバイダごとに資産ごとにキューに入れられ、その資産に対して一度に 1 つのディレクトリ同期が実行されます。異なる資産で複数の同期を並行して実行することができます。削除は同期されないので、これはディレクトリ同期の高速タイプです。タスクウィンドウには、タスクの進行状況と結果が表示されます。**［詳細］**をクリックしてさらに情報を確認したり、**［停止］**をクリックしてタスクをキャンセルしたりすることができます。API（Assets/Synchronize）を使用して、すべての削除、追加、および変更を含む削除（完全）同期を実行することができます。この同期には時間がかかります（おそらく数時間）。特に、ディレクトリの設定に基づいて初めて実行される場合は、時間がかかります。
アカウントの検出	関連するアカウント検出ジョブを実行します。詳細については、「アカウント検出」を参照してください。
有効化 – 無効化	次のいずれかを選択します。 **［有効］**を選択すると、SPP が無効な資産を管理できるようになります。アカウント検出ジョブは、過去に有効または無

プロパティ	説明
	効とマークされているかどうかに関係なく、検出ルールの基準に一致するすべてのアカウントを検出します。 選択した資産を SPP が管理しないようにするには、**［無効］**を選択します。資産を無効にすると、SPP はその資産を無効にし、関連するアカウントをすべて削除します。後で資産を管理することを選択した場合、SPP は関連するすべてのアカウントを再び有効にします。
無効化済みの表示	管理されていない、無効化され、関連するアカウントがない資産を表示します。資産の管理は、資産を選択し、**［有効化 – 無効化］**をクリックすることで制御することができます。
無効化済みの非表示	管理されておらず、無効化されており、関連するアカウントがない資産を非表示にします。資産管理は、資産を選択し、**［有効化 – 無効化］**をクリックすることでコントロールできます。
エクスポート	リストされたデータを JSON または CSV ファイルとしてエクスポートします。詳しくは、「データのエクスポート」を参照してください。
更新	選択したパーティションに関連する資産の最新のリストを取得し、表示します。
検索	このリストから特定の資産を見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

アカウントタブ

プロファイルの**［アカウント］**タブには、このプロファイルに関連付けられたアカウントが表示されます。

選択したプロファイルにアカウントを関連付けるには、詳細ツールバーから**［アカウントの追加］**／**［新しいアカウント］**をクリックします。

アカウントへのアクセス

［資産管理］＞**［プロファイル］**＞**［パスワードプロファイル］**＞（詳細の表示）＞**［アカウント］**の順に移動します。

表：プロファイル：アカウントタブプロパティ

プロパティ	説明
名前	選択した資産に関連するアカウント名です。 1 つのアカウントは 1 つの資産にしか関連付けられませんが、複数のアカウントで資産にログインすることができます。
ドメイン名	アカウントのドメイン名で、アカウントの一意性を判断するのに役立ちます。
親	選択したアカウントが子として所属するオブジェクトの名前。
パスワードプロファイル	パスワードプロファイルの名前
SSH キープロファイル	SSH キープロファイルの名前
サービスアカウント	アカウントがサービスアカウントである場合にチェックが表示されます。
パスワードリクエスト	そのアカウントでパスワードリリースリクエストが有効である場合にチェックが表示されます。 詳細ツールバーの**［アクセスリクエスト］**をクリックすると、選択したアカウントに対するユーザーのアクセスリクエスト機能を有効または無効にすることができます。
セッションリクエスト	そのアカウントに対してセッションアクセスリクエストが有効である場合にチェックが表示されます。 詳細ツールバーのアクセスリクエストをクリックすると、選択したアカウントに対するユーザーのアクセスリクエストが有効または無効になります。
SSH キーリクエスト	そのアカウントで SSH キーリリースリクエストが有効である場合にチェックが表示されます。
無効	資産が管理されていないこと、無効であること、および関連するアカウントがない場合にチェックが表示されます。
パスワード	アカウントにパスワードが設定されている場合にチェックが表示されます。詳細については、「アカウントパスワードの確認、変更、設定」を参照してください。

プロパティ	説明
SSH キー	そのアカウントに SSH キーが設定されている場合にチェックが表示されます。詳細は、「SSH キーの確認、変更、設定」を参照してください。
説明	アカウント追加時に入力した説明文
タグ	アカウントに関連付けられたタグ

資産アカウントは、次の詳細ツールバーボタンを使用して管理します。

表：プロファイル アカウントタブのツールバー

プロパティ	説明
＋ アカウントの追加	アカウントをプロファイルに追加します。
－ 削除	選択したアカウントを削除します。
詳細の表示	アカウントを選択した後、このボタンをクリックすると、詳細と設定オプションが表示されます。
アカウントセキュリティ	メニューのオプションは以下の通りです。 • **パスワードの確認**、**パスワードの変更**、**パスワードの設定**：詳細については、「アカウントパスワードの確認、変更、設定」を参照してください。 • **パスワードアーカイブ**：アカウントの**パスワードアーカイブ**を表示します。 • **SSH キーのアーカイブ**：アカウントの SSH キーアーカイブを表示します。
アクセスリクエスト	選択したアカウントに対してアクセスリクエストサービスを有効または無効にするオプションを選択します。値は、資産のプラットフォームが以下のいずれかをサポートしていることを示すかどうかで決まります。パスワードリクエスト、SSH キーリクエスト、セッションリクエスト。必要に応じて、パスワードリクエスト、セッションリクエスト、および SSH キーリクエストを有効または無効にすることができます。

プロパティ	説明
	サービスアカウントは、資産の作成時に作成され、デフォルトでは、セッションまたはパスワードアクセスは有効になっていません。 検出されたアカウントは、アカウントを検出する際に使用されるアカウント検出テンプレートによって制御されます。これらは、アカウント検出ジョブのルールテンプレートのプロパティです。詳細については、「アカウント検出ルールの追加」を参照してください。
有効化 – 無効化	次のいずれかを選択します。 **［有効化］**を選択すると、SPP が無効な資産を管理できるようになります。 **［無効化］**を選択すると、選択した資産を SPP が管理しないようになります。
無効化済みの表示	管理されていない、無効化されているアカウントを表示します。
無効化済みの非表示	管理されておらず、無効化されている、アカウントを非表示にします。
エクスポート	リストされたデータを JSON または CSV ファイルとしてエクスポートします。詳しくは、「データのエクスポート」を参照してください。
更新	選択した資産アカウントのリストを更新します。
検索	このリストから特定の資産アカウントまたはアカウントセットを検索するには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

パスワードプロファイルコンポーネントの表示

プロファイルページの**パスワードプロファイル**タブを選択すると、**［パスワードプロファイルコンポーネントの表示］**リンクが表示されます。このリンクには、SPP で使用されている、現在設定されているパスワードプロファイルコンポーネントに関する情報が表示されます。

プロファイルページで**［パスワードプロファイル コンポーネントの表示］**リンクを開くには、以下の手順に従います。

［資産管理］>**［プロファイル］**>**［パスワードプロファイル］**の順に移動し、**［パスワードプロファイル コンポーネントの表示］**リンクをクリックします。

パスワードプロファイル コンポーネントの表示には、以下のタブがあります。

- **パスワードの確認：**このタブには、現在構成されているパスワードの確認スケジュールに関する情報が表示されます。**［更新］**ボタンを使用すると、リストされたスケジュールを更新することができます。
- **パスワードの変更：**このタブには、現在構成されているパスワードの変更スケジュールに関する情報が表示されます。**［更新］**ボタンを使用すると、リストされたスケジュールを更新することができます。
- **アカウントパスワードルール：**このタブには、現在構成されているアカウントパスワードのルールに関する情報が表示されます。**［更新］**ボタンを使用すると、リストされたルールを更新することができます。
- **パスワード同期グループ：**このタブには、現在構成されているパスワード同期グループに関する情報が表示されます。このタブでは、以下のオプションが利用可能です。
    - **追加**：新しいパスワード同期グループを追加します。
    - **削除**：選択したパスワード同期グループを削除します。
    - **詳細の表示**：選択したパスワード同期グループの追加情報を表示します。
    - **有効化 – 無効化**：パスワード同期グループを有効または無効化します。
    - **同期グループのパスワードの変更**：
    - **更新**：リストされているパスワード同期グループを更新します。

10.6.2 パスワードプロファイルの管理

パスワードプロファイルを管理するには、プロファイルページのコントロールとタブページを使用して、次のタスクを実行します：

- パスワードプロファイルの追加
- パスワードプロファイル
- デフォルトパスワードプロファイルの設定
- パスワードプロファイルの削除

パスワードプロファイルの追加

SPP にパーティションを追加するのは、資産管理者の責任です。

パスワードプロファイルの追加手順

1. **［資産管理］＞［プロファイル］＞［パスワードプロファイル］**に移動します。
2. ツールバーの ＋ **［新しいプロファイル］**をクリックします。
3. **［全般］**ダイアログで、次の情報を入力します。
   a. **名前**：プロファイルの一意の名前を入力します。制限：50 文字
   b. **説明**：（任意）このプロファイルに関する情報を入力します。制限：255 文字
4. **［パスワードの確認］**タブで、ドロップダウンメニューから以前に定義したパスワード確認設定を選択するか、**［追加］**をクリックして新しいパスワード確認設定を追加します。これらは、アカウントパスワードの確認に使用されるルールです。詳細については、「パスワードの確認設定の追加」を参照してください。
5. **［パスワードの変更］**タブで、ドロップダウンメニューから以前に定義したパスワード変更設定を選択するか、**［追加］**をクリックして新しいパスワード変更設定を追加します。これらは、アカウントのパスワードをリセットするために使用されるルールです。詳細については、「パスワード変更設定の追加」を参照してください。
6. **［アカウントパスワードルール］**タブで、以前に定義したアカウントパスワードルールを選択するか、**［追加］**をクリックして新しいアカウントパスワードルールを追加します。アカウントパスワードルールは、パスワードの自動変更中に SPP によって作成される新しいパスワードの構築を管理する複雑性のルールです。詳細については、「アカウントパスワードのルールの追加」を参照してください。
7. **［OK］**をクリックして、パスワードプロファイルを保存します。
8. 新しいプロファイルを作成する場合、**［パスワード同期グループ］**タブは使用できません。このタブは、プロファイルの編集中に表示されます。**［パスワード同期グループ］**タブを使用して、プロファイル変更スケジュールで管理されるパスワード同期グループを追加または更新することができます。詳細については、「パスワード同期グループ」を参照してください。

パスワードプロファイル

パスワードプロファイルを使用して、アカウントパスワードのルール、パスワードの確認と変更のスケジュールなどのプロファイル構成設定を定義し、プロファイル定義で使用することができます。

［資産管理］＞［プロファイル］＞［パスワードプロファイル］の順に移動します。

表：プロファイル設定

プロパティ	説明
アカウントパスワードルール	アカウントパスワードの自動変更時に、SPP が新しいパスワードを作成する際に使用する複雑さのルールを定義する場所
パスワードの変更	SPP がアカウントのパスワードをリセットする際に使用するルールを定義します。
パスワードの確認	SPP がアカウントのパスワードの確認に使用するルールを定義します。
パスワード同期グループ	SPP がアカウント間でパスワードを同期できるように、パスワード同期グループと関連アカウントを定義する場所

パスワードの確認

パスワードの確認設定は、SPP がアカウントパスワードの確認に使用するルールです。

［資産管理］＞［プロファイル］＞［パスワードプロファイルコンポーネントの表示］＞［パスワードの確認］に移動します。

［パスワードの確認］ペインには、リストされたパスワードの設定ルールについて、以下が表示されます。

表：パスワードの確認: プロパティ

プロパティ	説明
名前	パスワードの確認ルールの名前
パーティション	ルールを使用するパーティション
説明	このルールについての説明
スケジュール	選択されたルールのスケジュール

パスワードの確認設定ルールを管理するには以下のツールバーボタンを使用します。

表：パスワードの確認: ツールバー

オプション	説明
追加	パスワードの確認ルールを追加します。詳しくは「パスワードの確認設定の追加」を参照してください。
削除	選択したルールを削除します。
編集	選択したルールを更新します。
更新	パスワードルールの確認のリストを更新します。
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

パスワードの確認設定の追加

SPP がアカウントパスワードの確認に使用するルールを定義するのは、資産管理者またはパーティションの委任管理者の責任です。

［資産管理］＞［プロファイル］＞［パスワードプロファイルコンポーネントの表示］＞［パスワードの確認］に移動します。

パスワード検証のスケジュールを追加する手順

1. **［追加］**をクリックして、**［確認パスワード設定］**ダイアログを開きます。
2. ルールの**［名前］**を 50 文字以内で入力します。
3. ルールの**［説明］**を 255 文字以内で入力します。
4. **［参照］**ボタンをクリックしてパーティションを選択します。
5. オプションで、これらの設定のいずれかを完了します。
    - **一致しない場合にパスワードをリセット**：このオプションを選択すると、SPP がアプライアンスデータベース内のパスワードと資産上のパスワードが異なることを検出した場合に、自動的にパスワードが変更されます。
    - **一致しない場合に所有者に通知**：このオプションを選択すると、SPP がパスワードの不一致を検出したときに通知をトリガーします。

> **メモ：**ユーザーにイベント通知を送信するには、SPP がアラートを送信するように設定する必要があります。詳細については、「アラートの構成」を参照してください。Password Check Mismatch イベント タイプのメール テンプレートを設定します。

6. **［スケジュール］**タブを開き、間隔を選択します。

7. **［スケジュール］**ダイアログで、**［実行間隔］**を選択すると、入力した実行の詳細に従ってジョブが実行されます。(**［実行間隔］**の選択を解除すると、スケジュールの詳細が失われます。)

    - 以下を設定します。

      開始時刻と終了時刻を指定せずに頻度を指定する場合は、以下のコントロールから選択します。開始時刻と終了時刻を指定する場合は、このセクションの**［時間ウィンドウを使用］**を選択します。

      ［実行間隔］の頻度を入力し、次に、時間枠を選択します。

        - **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
        - **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、**［実行間隔 = 2/時間/正時@分 = 15］**と設定します。
        - **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
        - **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
        - **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2 /月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

    - 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。**＋［追加］**または **- ［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複

しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、［**時間ウィンドウを使用］**を選択します。

- 開始 22：00：00、終了 23：59：00
- 開始 00：00：00、終了 2：00：00

開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

- **(UTC) Coordinated Universal Time** はデフォルトのタイムゾーンです。必要であれば、新しいタイムゾーンを選択してください。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行を終了すると、次の即時の時間間隔に再スケジュールされます。

8. **［OK］**をクリックします。

パスワードの変更

パスワードの変更設定は、SPP がアカウントパスワードをリセットするために使用するルールです。

［資産管理］＞［プロファイル］＞［パスワードプロファイルコンポーネントの表示］＞［パスワードの変更］に移動します。

パスワードの変更ペインには、パスワードの変更設定ルールについて、次の情報が表示されます。

表：パスワードの変更: プロパティ

プロパティ	説明
名前	ルールの名前
パーティション	ルールを使用するパーティション

プロパティ	説明
説明	このルールについての説明
スケジュール	選択されたルールのスケジュール

これらのツールバーボタンを使って、パスワードの変更設定ルールを管理します。

表：パスワードの変更: ツールバー

オプション	説明
追加	パスワードの変更ルールを追加します。詳しくは「パスワード変更設定の追加」を参照してください。
削除	選択したルールを削除します。
編集	選択したルールを更新します。
更新	パスワードルールの変更リストを更新します。
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

パスワード変更設定の追加

SPP がアカウントパスワードのリセットに使用するルールを設定するのは、資産管理者またはパーティションの委任管理者の責任です。

> **重要**: パスワード同期グループに関連付けられたアカウントのパスワードは、プロファイル変更スケジュールに基づいて管理され、同期グループを通じて処理されます。同期グループ内の個々のアカウントで同期に失敗すると、そのアカウントは複数回再試行され、その後失敗すると、同期タスクは停止して再スケジュールされます。同期タスクを続行するには、管理者が失敗の原因を修正する必要があります。詳細については、「パスワード同期グループ」を参照してください。

［資産管理］＞［プロファイル］＞［パスワードプロファイルコンポーネントの表示］＞［パスワードの変更］へ移動します。

パスワードのリセットスケジュールの追加手順

1. **＋［追加］**をクリックし、**［変更パスワード設定］**ダイアログを表示します。

2. ルールの［**名前**］を 50 文字以内で入力します。

3. ルールの［**説明**］を 255 文字以内で入力します。

4. ［**参照**］ボタンを使用して、パーティションを選択します。

5. 任意で、次のいずれかの設定を完了します。

    - **パスワードの手動変更**：詳細については、「サポートされていないプラットフォームのアカウントを管理できますか？」を参照してください。
    - **リリースがアクティブな場合でもパスワードを変更**：このオプションを選択すると、パスワードのリリースが有効な場合でも、パスワードの変更を許可します。
    - **現在のパスワードを必須とする**： このオプションを選択すると、現在のパスワードがリクエストされます。
    - **チェックイン時にアカウントを一時停止**：このオプションを選択すると、使用されていない管理対象アカウントが自動的に一時停止されます。つまり、SPP を通じてリクエストが行われ、その時点で SPP がアカウントを復元するまで、管理対象資産のアカウントは一時停止されます。リクエストがチェックインまたはクローズされると、アカウントは再び一時停止されます。

      サポートされているプラットフォームのリンクをクリックすると、この機能をサポートしているプラットフォームのリストが表示されます。

      > **メモ**：以下に示すすべての更新オプションは、資産のサービス検出ジョブによって検出されたサービスのリストに適用されます。ローカル管理アカウントまたは AD 依存アカウントとして実行される検出されたサービスは、更新されます。

    - **パスワードの変更時にサービスを更新（Windows のみ）**：資産のローカル管理アカウントまたは AD 依存アカウントとして実行するように構成されている Windows サービスの場合、このオプションを選択すると、そのアカウントが実行する各サービスにもパスワード変更が適用されるようになります。サービスが依存する AD アカウントとして実行されている場合、Windows 資産と依存する Active Directory アカウントは同じプロファイルである必要があります。
    - **パスワードの変更時にサービスを再起動（Windows のみ）**：資産のローカル管理アカウントまたは依存 AD アカウントとして実行するように構成されている Windows サービスの場合、このオプションを選択すると、パスワード変更後に自動再起動が行われるようになります。ローカルアカウントの場合、その

アカウントに割り当てられたプロファイルが使用されます。AD アカウントの場合、資産に割り当てられたプロファイルが使用されます。

- **パスワードの変更時に IIS アプリケーションプールを更新（Windows のみ）**：ローカル管理アカウントまたは資産に依存する AD アカウントとして実行するように構成されている IIS アプリケーションプールでは、このオプションを選択すると、そのアカウントが実行する各 IIS アプリケーションプールにもパスワード変更が適用されるようになります。サービスが依存 AD アカウントとして実行されている場合、Windows 資産と依存 Active Directory アカウントは同じプロファイルである必要があります。
- **パスワードの変更時に COM+ を更新 (Windows のみ)**：ローカル管理アカウントまたは資産上の依存 AD アカウントとして実行するように構成された COM+ アプリケーションの場合、このオプションを選択すると、パスワードの変更がそのアカウントが実行する各 COM+ アプリケーションにも適用されます。サービスが依存する AD アカウントとして実行されている場合、Windows 資産と依存する Active Directory アカウントは同じプロファイルである必要があります。
- **パスワードの変更時にタスクを更新（Windows のみ）**：資産のローカル管理アカウントまたは依存する AD アカウントとして実行するように構成されているスケジュールされたタスクの場合、このオプションを選択すると、そのアカウントが実行する各タスクにもパスワード変更が適用されるようになります。サービスが依存する AD アカウントとして実行されている場合、Windows 資産と依存する Active Directory アカウントは同じプロファイルである必要があります。
- **Reschedule for unscheduled password change**（スケジュールされていないパスワードの変更をリスケジュール）：このオプションを選択すると、パスワードが手動で変更されたときに、パスワードのスケジュールがリセットされます。例：パスワードのリセットは 10 日ごとに行われるようにスケジュールされているが、8 日目にパスワードが手動で変更された場合、この手動リセットのため、スケジュールは再起動し、次のパスワードリセットは、元のスケジュールされたリセット（2 日後）ではなく、10 日後に行われます。

6. **［スケジュール］**タブを開き**［実行間隔］**を選択すると、入力した実行の詳細に従ってジョブが実行されます。（**［実行間隔］**の選択を解除すると、スケジュールの詳細が失われます。）

   - 以下を設定します。

     開始時刻と終了時刻を指定せずに頻度を指定する場合は、以下のコントロールから選択します。開始時刻と終了時刻を指定する場合は、このセクションの**［時間ウィンドウを使用］**を選択します。

［**実行間隔**］の頻度を入力し、次に、時間枠を選択します。

- **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
- **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、［**実行間隔 = 2/時間/正時@分 = 15**］と設定します。
- **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
- **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
- **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2 /月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

- 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。＋**［追加］**または **-［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、［**時間ウィンドウを使用］**を選択します。
  - 開始 22：00：00、終了 23：59：00
  - 開始 00：00：00、終了 2：00：00

開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

- **(UTC) Coordinated Universal Time** はデフォルトのタイムゾーンです。必要であれば、新しいタイムゾーンを選択してください。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行を終了すると、次の即時の時間間隔に再スケジュールされます。

7. **［OK］**をクリックします。

アカウントパスワードルール

アカウントパスワードルールは、アカウントパスワードの自動変更時に SPP によって作成される新しいパスワードの作成を管理します。次のような、許可されるアカウントパスワードを管理するルールを作成できます。

- 許容されるパスワードの長さを 3 ～ 225 文字の範囲で設定します。

  > **重要：**macrocosm パーティションのデフォルトのパスワード長は、Azure AD のパスワード要件を満たしません。Azure AD で Starling Connect 機能を使用する場合、パスワードの範囲を 8 文字から 225 文字の間に設定する必要があります。

- 最初の文字の種類と最後の文字の種類を設定します。
- 大文字、小文字、数字、印刷可能な ASCII 記号を許可し、それぞれの最小量を設定します。
- 除外する大文字、小文字、数字、記号を指定します。
- 連続した文字、数字、記号の繰り返しを許可するかどうかを確認し、許可する場合は、繰り返しの最大回数を設定します。

> **メモ：**パーティションのプロファイルを定義するときに、アカウントのパスワードルールセットを選択します。詳細については、「パスワードプロファイルの作成」を参照してください。アカウントパスワードルールは、プロファイルによって管理されるすべてのアカウントに適用されます。

［資産管理］＞［プロファイル］＞［パスワードプロファイルコンポーネントの表示］＞［アカウントパスワードルール］に移動します。

これらのツールバーボタンを使用して、アカウントパスワードルールを管理します。

表：アカウントパスワードルール: ツールバー

オプション	説明
追加	アカウントパスワードの複雑さのルールを追加します。詳しくは「アカウントパスワードのルールの追加」を参照してください。
削除	選択したルールを削除します。
編集	選択したルールを更新します。
更新	アカウントパスワードルールのリストを更新します。
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

アカウントパスワードのルールの追加

アカウントパスワードの複雑性のルールを設定するのは、資産管理者またはパーティション委任管理者の責任です。

> **重要：**
> Unix システムの中には、パスワードを最大許容長まで無言で切り詰めるものがあります。たとえば、Macintosh OS X では、パスワードは 128 文字までしか許可されません。資産管理者がパスワードの長さを 136 文字に設定するアカウントパスワードルール付きのプロファイルを作成した場合、SPP がそのプロファイルによって管理されるアカウントのパスワードを変更すると、資産のオペレーティングシステムが新しいパスワードを許容される長さに切り捨て、エラーは返しませんが、136 文字分のパスワードが SPP に完全に保存されます。このため、次のような問題が発生します。
>
> - そのアカウントのパスワードの確認に失敗します。SPP が Unix ホストのパスワードと SPP のパスワードを比較すると、Unix ホストが SPP で生成したパスワードを切り捨てたため、両者が一致しません。
> - ユーザーは、オペレーティング ステムが課す許容長さまでパスワードを切り詰めない限り、SPP が提供するパスワードで Unix ホストのアカウントに正常にログインすることはできません。

［資産管理］＞［プロファイル］＞［パスワードプロファイルコンポーネントの表示］＞［アカウントパスワードルール］に移動します。

アカウントパスワードルールの追加手順

1. **［追加］**をクリックし、**［新しいアカウントパスワードルール］**ダイアログを表示します。
2. アカウントパスワードルールの**［名前］**を入力します（50 文字以内）。
3. アカウントパスワードルールの**［説明］**を入力します（最大 255 文字）。
4. **［参照］**ボタンを使用してパーティションを選択します。
5. **［パスワードルール］**タブで、パスワードの要件を設定します。
    - **パスワード長**
      パスワードの許容長さを 3 ～ 255 文字の範囲で設定します。デフォルトは 8 文字から 64 文字です。最大長は、次の手順で必要な最小文字数の合計と同じかそれ以上でなければなりません。たとえば、パスワードに大文字 2 文字、小文字 2 文字、数字 2 文字が必要な場合、パスワードの長さの最小値は 6 でなければなりません。なお、発音区分文字は 1 文字とする。
    - **最初の文字のタイプ**
      以下のいずれかを選択します。
        - **すべて**：アルファベット、数字、または記号
        - **英数字**：アルファベットまたは数字
        - **アルファベット**： アルファベットのみ
    - **最後の文字のタイプ**
      以下のいずれかを選択します。
        - **すべて**：アルファベット、数字、記号
        - **英数字**：アルファベットまたは数字
        - **アルファベット**：アルファベットのみ
    - **繰り返し文字**
      以下のいずれかを選択します。
        - **繰り返し文字を許可**
          任意の文字、数字、記号を、連続を含め、任意の順序で繰り返すことができます。
        - **連続する繰り返し文字はありません**
          文字、数字、記号をそれ自身の後に繰り返すことはできません。大文字、小文字、数字、記号、またはそれらの組み合わせによって、後に連続して繰り返される文字の数を制限することができます。

        - **繰り返し文字はありません**
          すべての文字、数字、記号は、パスワードの中で一度だけ使用することができます。

- **大文字を許可**
  大文字を許可するかどうかを選択します。

    - **最低文字数の大文字が必要です**
      最低限必要な大文字の数を数字で入力します。大文字を許可するが必要としない場合は、この値を 0 に設定します。

    - **連続する繰り返し大文字を制限**
      先に繰り返しを許可した場合、チェックボックスを選択して、連続して繰り返される大文字の数を制限します。**[許可される最大文字数]**の値を 1 以上入力する必要があります。

    - **これらの大文字を除外してください**
      パスワードから除外したい大文字を入力します。このフィールドでは、大文字と小文字が区別されます。

- **小文字を許可**
  小文字を許可するかどうかを選択します。

    - **最低文字数の小文字が必要です**
      小文字を最低限必要とする数を入力します。小文字を許可するが必要としない場合は、この値を 0 に設定します。

    - **連続する繰り返し小文字を制限**
      繰り返し文字を許可した場合、チェックボックスを選択すると、連続して繰り返される小文字の数が制限されます。**[許可される最大文字数]**に 1 以上の値を入力する必要があります。

    - **[これらの小文字を除外してください]**パスワードから除外したい小文字を入力します。このフィールドでは、大文字と小文字が区別されます。

- **連続する繰り返し小文字を制限**
  小文字と大文字を組み合わせた繰り返しの数を設定するには、**[許可される最大文字数]**を入力します。

  たとえば、**[許可される最大文字数]**に「2」に設定すると、パスワードの中で隣り合うアルファベットは 2 つまでとなります。この例では、Ab1Cd2EF は有効ですが、AbC1d2EF はアルファベットが 3 つ並んでいるため、無効となります。

- **数字（0-9）を許可**
  パスワードに数字を使用することを許可するかどうかを選択します。

- **最低文字数の数字が必要です**
  パスワードに必要な数字の量を示す数字を入力します。数字を許可するが要求しない場合は、この値を 0 に設定します。
- **連続する繰り返し数字を制限**
  連続して繰り返される数字の数を制限する場合は、チェックボックスをオンにします。**[許可される最大文字数]** に 1 以上の値を入力する必要があります。
- **これらの数値文字を除外してください**
  パスワードから除外したい数字を入力します。このフィールドでは、大文字と小文字が区別されます。

- **記号（@ # $ % &など）を許可**
  印刷可能な ASCII 文字を許可する場合は、このチェックボックスをオンにします。これらの文字には、次のようなものがよく含まれます。~ ` ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
  - **最低文字数の記号が必要です**
    必要な最小限の記号の数を示す数字を入力します。記号の使用を許可するが、記号を必要としない場合は、この値を 0 に設定します。
  - **連続する繰り返し記号を制限**
    チェックボックスを選択すると、連続して繰り返される記号の数が制限されます。**[許可される最大文字数]** に 1 以上の値入力する必要があります。
  - 以下を設定します。
    - **有効な記号**
      有効な特殊文字を入力する場合は、このオプションを選択します。**[記号リスト]** テキストボックスに、有効な記号を入力します。
    - **無効な記号**
      このオプションを選択すると、入力が禁止された特殊文字を入力できます。**[記号リスト]** テキストボックスに禁止されている記号を入力します。

6. **[ルールのテスト]** をクリックして、設定したルールを確認します。
7. ルールが完成したら、**[OK]** をクリックします。

パスワード同期グループ

パスワード同期グループは、関連するすべてのアカウントでパスワードの検証およびリセットを制御するために使用されます。同じパスワードは、同じまたは異なる資産に関連する 1 つまたは複数のアカウントに使用されます。たとえば、同期パスワードは、開発、テスト、本番の間で同期するクラスタまたはシステムをサポートするアカウントに使用することができます。1 つのアカウントは、1 つのパスワード同期グループにのみ所属することができます。1 つのプロファイルに複数のパスワード同期グループを追加することができます。

プロファイルの変更スケジュールは、同期グループに適用されます。同期グループは、同期グループ内のアカウントのパスワードを変更するタスクを制御します。変更タスクは、パスワード同期グループアカウントの優先順位の高い順に発生します。同期グループ内の個々のアカウントで同期に失敗すると、そのアカウントは複数回再試行され、その後失敗すると、同期タスクは停止して再スケジュールされます。同期タスクを続行するには、管理者が失敗の原因を修正する必要があります。

アカウントが、毎日確認するスケジュールのプロファイルに関連付けられ、パスワード同期グループにも関連付けられている場合、毎日の確認で不一致が発生すると、アカウントのパスワードを現在の同期グループのパスワードに設定するタスクが起動します。

詳しくは、「パスワードプロファイルの作成」を参照してください。

パスワード同期グループのアカウントの優先順位

アカウントがパスワード同期グループに追加されるとき、デフォルトの優先度は 0 であり、これは最も高い優先度です。それ以降の番号は優先順位が低くなります（たとえば、0、1、2 の場合、0 が最も高い優先順位、2 が最も低い優先順位です）。優先順位は、アカウントのパスワードが変更される順序を決定します。すべてのアカウントの優先順位が同じであれば、同時に同期されます。異なる優先順位が設定されている場合、最も高い優先順位（例えば 0）のアカウントが最初に同期されます。優先順位 0 が成功した場合、次の優先順位のアカウントが同期されます。ある優先順位のアカウントが失敗すると、同期処理は停止し、グループの同期再試行がスケジュールされます。たとえば、あるクラスタのシステムに、同じパスワードの admin アカウントがあるとします。1 つのプライマリシステムを優先度 0 に設定し、サブシステムを優先度 1 に設定した場合、サブシステムのパスワードが変更される前にプライマリのパスワード変更が成功する必要があります。プライマリのパスワード変更に失敗しても、下位システムは影響を受けず、クラスタは機能し続け、パスワード変更は再スケジュールされ、エラーがログに記録されます。

［資産管理］＞［プロファイル］＞［パスワードプロファイルコンポーネントの表示］＞［パスワード同期グループ］を開きます。

表：同期グループプロパティ

プロパティ	説明
有効	有効の場合、プロファイルの変更スケジュールに合わせて同期が実行されます。
ステータス	すべてのアカウントのパスワードがパスワード同期グループと同期している場合、✔が表示されます。同期グループ内のいずれかのアカウントのパスワードが共通パスワードと一致しない場合は、⚠が表示されます。
名前	パスワード同期グループの名前
アカウント	共通のパスワードで同期するアカウントの数
次の同期	同期グループのパスワードがすべてのアカウントで同期される日付
説明	ルールに関する情報

パスワードの変更設定ルールは、次のツールバーボタンを使って管理します。

> **メモ：[パスワード同期グループ]** ペインから行った変更は、プロファイルのパスワード同期グループに反映されます。「パスワードプロファイルの作成」を参照してください。

表：同期グループ：ツールバー

オプション	説明
追加	パスワード同期グループの追加。詳しくは「パスワード同期グループの追加」を参照してください。
削除	選択したパスワード同期グループを削除します。
詳細の表示	選択したパスワード同期グループルールを更新します。
同期グループのパスワード変更	選択した同期グループのパスワードを変更します。パスワード同期グループのすべてのアカウントが新しいパスワードで同期されます。
更新	パスワード同期リストを更新します。
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

パスワード同期グループの追加

資産管理者またはパーティション委任管理者は、パスワード同期グループを定義します。1 つのアカウントは、1 つのパスワード同期グループにのみ属することができます。パーティションにプロファイルを追加するときに同期グループと関連するアカウントを割り当てるには、「パスワードプロファイルの追加」を参照してください。

パスワード同期グループの作成手順

1. **新規パスワード同期グループ**ダイアログで、**［名前］**に 100 文字以内で固有の名前を入力します。
2. **［説明］**に 255 文字以内で説明を入力します。
3. パスワード同期グループを保存した後、**［編集］**をクリックします。
4. **アカウント**タブを開きます。
5. **［追加］**をクリックし、同期させるアカウントを 1 つ以上選択します。
6. アカウントリストが表示され、アカウントに関する情報が表示されます。いずれかの列をクリックすると、アカウントがソートされます。
7. **［アカウントの選択］**をクリックします。以下の値が表示されます：
    - **ステータス**：パスワードが同期グループと同じでない場合、⚠が表示されます。パスワードが同じである場合、✔が表示されます。アカウントが無視され、同期グループに入るべきでない可能性がある場合、⊘が表示されます。
    - **優先度**：デフォルトは優先度 0（最高）です。優先順位を変更するには、**［優先度］**の値をダブルクリックして、新しい優先順位を入力し、**［OK］**をクリックします。詳細については、「パスワード同期グループのアカウントの優先順位」を参照してください。
    - **システム名**：アカウントに関連付けられたシステム（資産）の名前
    - **アカウント名**：アカウントの名前
    - **ドメイン名**：ドメインの名前
    - **前回の同期時刻**：最後に同期を行った日時
8. **［OK］**をクリックします。

デフォルトパスワードプロファイルの設定

新しいパーティションを作成すると、SPP は、デフォルトのスケジュールとルールで対応するデフォルトのプロファイルを作成します。

別のパスワードプロファイルをデフォルトとして設定する手順

1. **［資産管理］＞［プロファイル］**を開きます。
2. パスワードプロファイルで、パーティションの現在のデフォルトプロファイルでないプロファイルを選択します。
3. 詳細ツールバーの **［デフォルトとして設定］**をクリックします。

パスワードプロファイルの削除

パスワードプロファイルを管理するのは、資産管理者の責任です。

パスワードプロファイルの削除手順

1. **［資産管理］＞［プロファイル］＞［パスワードプロファイル］**に移動します。
2. 削除するプロファイルを選択します。
3. **［削除］**をクリックします。
4. リクエストを確認します。

10.6.3 SSH キープロファイル

プロファイルページの**［SSH キープロファイル］**タブに、SPP が使用する現在設定済みの SSH キープロファイルの情報が表示されます。

プロファイルページの**［SSH キープロファイル］**タブへのアクセス手順：

［資産管理］＞［プロファイル］に移動し、**［SSH キープロファイル］**]タブを開きます。必要に応じて、パーティションのドロップダウンを使用して、プロファイルの親パーティションを選択できます（デフォルトでは、すべてのプロファイルが表示されます）。プロファイルを選択してクリックすると、追加情報とオプションが表示されます。

プロファイルの 1 つを選択すると、次の情報が表示されます：

- **全般タブ：**このプロファイルの名前と情報が表示されます。
- **SSH キーのチェック**タブ： SPP がアカウントの SSH キーを確認するために使用するルールです。詳細については、「SSH キーチェック設定の追加」を参照してください。
- **SSH キーの変更**タブ：アカウントの SSH キーをリセットするために使用されるルールです。詳細については、「SSH キー変更設定の追加」を参照してください。
- **SSH キーの検出**タブ：SSH キーを検出するために使用されるルールです。詳細については、「SSH キー検出の追加」を参照してください。
- **SSH キー同期グループ**タブ：［**SSH キー同期グループ**］タブを使用して、プロファイル変更スケジュールによって支配される SSH キー同期グループを追加または更新することができます。詳細については、「SSH キー同期グループの設定」を参照してください。

ツールバー

プロファイルの管理には、これらのツールバーボタンが使用されます：

- **新規プロファイル**： SPP にプロファイルを追加します。
- **削除：**選択したプロファイルを削除します。
- **詳細の表示**：プロファイルを選択し、このボタンをクリックすると、プロファイルの追加情報およびオプションが表示されます。
- **デフォルトとして設定**：プロファイルを選択し、このボタンをクリックすると、そのプロファイルがデフォルトのプロファイルとして設定されます。
- **エクスポート**：このボタンをクリックすると、リストされたデータが JSON または CSV ファイルとしてエクスポートされます。詳細については、「データのエクスポート」を参照してください。
- **更新**：プロファイルのリストを更新します。

プロファイルページの［**SSH キープロファイル**］タブを選択すると、［**SSH キープロファイルコンポーネントの表示**］リンクが利用できます。詳細については、「SSH キープロファイルコンポーネントの表示」を参照してください。

SSH キープロファイルコンポーネントの表示

プロファイルページの［**SSH キープロファイル**］タブを選択すると、［**SSH キープロファイルコンポーネントの表示**］リンクが使用できます。このリンクには、SPP で使用されている現在設定されている SSH キープロファイル コンポーネントに関する情報が表示されます。

プロファイルページで［**SSH キープロファイル コンポーネントの表示**］リンクを開くには、次のようにします。

［**資産管理**］＞［**プロファイル**］＞［**SSH キープロファイル**］に移動し、［**SSH キープロファイル コンポーネントの表示**］リンクをクリックします。

SSH キープロファイルコンポーネントの表示ビューには、以下のタブがあります。

- **SSH キーのチェック**：このタブは、現在構成されている SSH キーの確認スケジュールに関する情報を提供します。［**更新**］ボタンを使用すると、リストされたスケジュールを更新することができます。
- **SSH キーの変更**：このタブは、現在構成されている SSH キーの変更スケジュールに関する情報を提供します。一覧表示されたスケジュールを更新するには、［**更新**］ボタンを使用することができます。
- **SSH キーの検出**：このタブには、現在検出されている SSH キーの情報が表示されます。［**更新**］ボタンを使って、リストされたキーを更新することができます。
- **SSH キー同期グループ**：このタブには、現在構成されている SSH キー同期グループに関する情報が表示されます。このタブでは、以下のオプションが利用できます。
    - **削除**：選択した SSH キー同期グループを削除します。
    - **詳細の表示**：選択した SSH キー同期グループの詳細を表示します。
    - **有効化-無効化**：これらのボタンを使って、SSH キー同期グループを有効化または無効化します。
    - **同期グループのパスワードを変更**
    - **更新**：リストされた SSH キー同期グループを更新します。

10.6.4 SSH キープロファイルの管理

プロファイルページのコントロールとタブページを使用して、以下のタスクを実行し、SSH キープロファイルを管理します。

- SSH キープロファイルの追加
- SSH キープロファイル

- デフォルト SSH キープロファイルの設定
- SSH キープロファイルの削除

SSH キープロファイルの追加

SPP に SSH キープロファイルを追加するのは、資産管理者の責任です。

SSH キープロファイルを追加手順

1. **［資産管理］＞［プロファイル］＞［SSH キープロファイル］**に移動します。
2. ツールバーの**［新しいプロファイル］**をクリックします。
3. **新しい SSH キープロファイル**ダイアログで、次の情報を入力します：
   a. **名前**：パーティションに一意の名前を入力します。制限：50 文字。
   b. **説明**：（任意）このパーティションに関する情報を入力します。制限：255 文字。
4. **［参照］**ボタンを使用して、SSH キープロファイルのパーティションを選択します。
5. **［SSH キーのチェック］**タブで、ドロップダウンメニューから以前に定義した SSH キーチェック設定を選択するか、**［追加］**をクリックして新しい SSH キーチェック設定を追加します。詳細については、「SSH キー設定のチェック」を参照してください。
6. **［SSH キーの変更］**タブで、ドロップダウンメニューから以前に定義した SSH キー変更設定を選択するか、**［追加］**をクリックして新しい SSH キーの変更設定を追加してください。詳細については、「SSH キー設定の変更」を参照してください。
7. **［SSH キーの検出］**タブで、ドロップダウンメニューから以前に定義した SSH キーの検出設定を選択するか、**［追加］**をクリックして新しい SSH キーの検出設定を追加します。詳細については、「SSH キーの検出設定」を参照してください。
8. **［OK］**をクリックして、SSH キーのプロファイルを保存します。
   保存されると、プロファイルを編集して SSH キーの同期グループを SSH キープロファイルに追加することができます。詳細については、「SSH キー同期グループの設定」を参照してください。

SSH キープロファイル

SSH 認証キーは、システム管理者、パワーユーザー、およびアクセスに SSH キーを使用する他の人によるサインオンだけでなく、自動化されたプロセスに対するセキュリティを最大化するために管理されます。SPP は、以下を実行します。

> **メモ：** SPP は、現在、authorized key のオプションを管理していません。インポートされた鍵に、資産上の authorized key ファイルで構成されたオプションがある場合、SPP によって鍵がローテートされたときに、これらのオプションは保持されません。

- SPP は、管理アカウントに関連付けられた新しいキーペアを作成することで、キーをプロビジョニングします。以下の方法のいずれかを使用できます。
    - ターゲットホスト上のターゲットアカウントに authorized key が追加されます。管理対象アカウントは複数の authorized key を持つことができますが、SPP が一度に管理できるキーは 1 つだけです。
    - SSH キーペアのために SSH キー同期グループが作成されます。新しいキーが同期グループ用に生成され、ターゲットホスト上の同期されたアカウントごとに設定されます。SSH キー同期グループ内のすべてのアカウントは、同じキーを使用してすべてのシステムにログインできるように、SSH キーを同期させます。
    - レガシーSSH の ID キーがアップロードされます。レガシーSSH キーは SPP に委託されます。レガシーSSH キーが公開されている場合、SPP はチェックイン後にキーをローテートします。**［資格ポリシー］＞［アクセス設定］**オプションで**［チェックイン後に SSH キーを変更］**が指定されている場合、SPP はチェックイン後にキーをローテーションさせることができます。
- A2A が SSH キーをリクエストおよび取得するように設定されている場合、SPP はアクセスリクエストポリシー（キーおよびセッション）に基づき、また A2A を介して SSH キーをリクエストおよびローテーションします。ローテーションはプロファイルベースです。各管理対象アカウントは、1 つの SSH キーを持つことができます。

対応する実装

次の SSH 実装がサポートされます：

- SSH ID キーによるアクセスリクエストは、OpenSSH、SSH2、PuTTY の各フォーマットを含みます。
- 管理用には、OpenSSH ファイル形式と Tectia をサポートしています。

対応するキーの種類と長さ

SPP では、SSH ID のキーとして RSA、Ed25519、ECDSA、DSA アルゴリズムをサポートしています。対応するキーの長さは以下のとおりです：

- RSA： 1024、2048、4096、8192 bit
  キーのサイズが大きくなると、生成に時間がかかります。特に、8192 ビットの鍵は数分かかることがあります。
- DSA： 1024 bit 固定
- Ed25519： 32 bit 固定
- ECDSA：256、384、521 bit

サポートされていないアルゴリズムとキー文字列

SPP は authorized_keys ファイルをパースする際に各行を読み、データの抽出を試みます。行が仕様に従って適切にフォーマットされている場合、SPP はそれを発見された ID キーとして報告します。SPP は、RSA または DSA アルゴリズムのキーを認識します。その他の有効なキータイプも SPP によって検出され、検出された SSH キーのプロパティグリッドのキータイプが不明であることが確認されます。

管理

アクセスリクエストと SSH キーパスフレーズ管理サービスを管理するのは、アプライアンス管理者の責任です。

SSH キーの変更、確認、検出は、オンまたはオフに切り替えることができます。詳しくは、「サービスの有効化または無効化」を参照してください。

［資産管理］＞［プロファイル］＞［SSH キープロファイル］に移動します。

表：SSH キー管理設定

設定	説明
SSH キー設定のチェック	SSH キー変更設定を追加、更新、スケジュール、削除できます。
SSH キー設定の確認	SSH キー確認設定を追加、更新、スケジュール、削除できます。
SSH キー設定の検出	SSH キー検出ジョブを追加、更新、スケジュール、削除できます。

設定	説明
SSH キー同期グループ設定	SSH キー同期グループ設定を追加、更新、スケジュール、削除できます。 資産管理者またはパーティションの委任管理者は、SSH キーペアの SSH キー同期グループを定義します。新しいキーは同期グループ用に生成され、ターゲットホスト上の同期されたアカウントごとに構成されます。SSH キー同期グループのすべてのアカウントが同期されるため、同じキーを使用してすべてのシステムにログインすることができます。

SSH キー設定のチェック

SPP は、アクセスリクエストポリシー（SSH キーまたは SSH セッションリクエスト）に基づいて、また SSH キーをリクエストおよび取得するように設定された A2A 構成を介して、SSH キーをリクエストおよびローテーションします。ローテーションはプロファイルベースです。各マネージドアカウントは、1 つのマネージド SSH キーを持つことができます。

SSH キーチェックは、オンまたはオフに切り替えることができます。詳細については、「サービスの有効化または無効化」を参照してください。

［資産管理］＞［プロファイル］＞［SSH キープロファイルコンポーネントの表示］に移動します。

表：SSH キーのチェックプロパティ

設定	説明
名前	SSH キーの名前
パーティション	SSH キーが管理されているパーティション
説明	SSH キーについての情報
スケジュール	SSH キーをチェックするタイミングを指定します。

次のツールバーボタンを使用して SSH キーを管理します。

表：SSH キーのチェック：ツールバー

設定	説明
追加	SSH キーのチェック設定を追加します。
削除	選択した SSH キーを削除します。
編集	選択した SSH キーを更新します。
更新	SSH キーのリストを更新します。
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

SSH キーチェック設定の追加

SPP が SSH キーを確認するために使用するルールを定義するのは、資産管理者またはパーティションの委任された管理者の責任です。

［資産管理］＞［プロファイル］＞［SSH キープロファイルコンポーネントの表示］＞［SSH キーのチェック］に移動します。

SSH キーの検証スケジュールを追加手順

1. **［追加］**をクリックして、**［SSH キー設定のチェック］**ダイアログを開きます。
2. **［名前］**を 50 文字以内で入力します。
3. **［説明］**を 255 文字以内で入力します。
4. **［参照］**をクリックして、パーティションを選択します。
5. 任意で以下のいずれかの設定を完了します：
    - **一致しない場合に SSH キーをリセット**：このオプションを選択すると、SPP がアプライアンスデータベース内の SSH キーパスフレーズと資産上の SSH キーパスフレーズが異なることを検出した場合に、SSH キーパスフレーズが自動的にリセットされます。
    - **一致しない場合に所有者に通知**： SPP が SSH キーパスフレーズの不一致を検出したときに通知をトリガーするには、このオプションを選択します。

> **メモ：** ユーザーにイベント通知を送信するには、SPP がアラートを送信するように設定する必要があります。詳細については、「アラートの構成」を参照してください。パスワードと SSH キーのパスフレーズの不一致チェックイベントタイプのメール テンプレートを設定します。

6. SSH キーのチェックのスケジュールを変更するには、**［スケジュール］**タブを開きます。デフォルトは**「なし」**です。

7. **［スケジュール］**ダイアログで、**［実行間隔］**を選択すると、入力した実行の詳細に従ってジョブが実行されます（**［実行間隔］**の選択を解除すると、スケジュールの詳細が失われます）。

    - 以下を設定します。

      開始時刻と終了時刻を指定せずに頻度を指定する場合は、以下のコントロールから選択します。開始時刻と終了時刻を指定する場合は、このセクションの**［時間ウィンドウを使用］**を選択します。

      ［実行間隔］の頻度を入力し、次に、時間枠を選択します。

        - **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
        - **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、［**実行間隔 = 2/時間/正時@分 = 15**］と設定します。
        - **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
        - **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
        - **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2 /月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

    - 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。＋**［追加］**または **-** **［削除］**をクリックして、複数の時間制限を制御す

ることができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、**［時間ウィンドウを使用］**を選択します。

- 開始 22：00：00、終了 23：59：00
- 開始 00：00：00、終了 2：00：00

開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

- **(UTC) Coordinated Universal Time** はデフォルトのタイムゾーンです。必要であれば、新しいタイムゾーンを選択してください。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行を終了すると、次の即時の時間間隔に再スケジュールされます。

8. **［OK］**をクリックします。

SSH キー設定の変更

SPP は、アクセスリクエストポリシー（SSH キーまたは SSH セッションのリクエスト）、および SSH キーをリクエストおよび取得するために設定された A2A 構成を介して、SSH キーをリクエストおよびローテートします。ローテーションは、プロファイルに基づいて行われます。各マネージドアカウントは、1 つのマネージド SSH キーを持つことができます。

SSH キーの変更は、オンまたはオフに切り替えることができます。詳細については、「サービスの有効化または無効化」を参照してください。

［資産管理］＞［プロファイル］＞［SSH キープロファイルコンポーネントの表示］＞［SSH キーの変更］の順に移動します。

表：SSH キーのチェックプロパティ

設定	説明
名前	SSH キーの名前
パーティション	SSH キーが管理されているパーティション
説明	SSH キーについての情報
スケジュール	SSH キーをチェックするタイミングを指定します。

次のツールバーボタンを使用して SSH キーを管理します。

表：SSH キーの変更：ツールバー

設定	説明
追加	SSH キー変更設定を追加します。詳しくは「SSH キー変更設定の追加」を参照してください。
削除	選択した SSH キーを削除します。
編集	選択した SSH キーを更新します。
更新	SSH キーのリストを更新します。
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

SSH キー変更設定の追加

SPP が SSH キーのパスフレーズをリセットするために使用するルールを設定するのは、資産管理者またはパーティションの委任管理者の責任となります。

> **重要**： SSH キー同期グループに関連付けられたアカウントのパスフレーズは、プロファイル変更スケジュールに基づいて管理され、SSH キー同期グループを介して処理されます。同期グループ内の個々のアカウントの同期に失敗した場合、そのアカウントは複数回再試行され、その後も失敗した場合は同期タスクが停止して再スケジュールされます。同期タスクを続行するには、管理者が失敗の原因を修正する必要があります。詳しくは、「SSH キー同期グループの設定」を参照してください。

SSH キーのリセットスケジュールの追加手順

1. **［資産管理］＞［プロファイル］＞［SSH キープロファイルコンポーネントの表示］＞［SSH キーの変更］**の順に移動します。
2. ＋**［追加］**をクリックして、**［SSH キー設定の変更］**ダイアログを開きます。
3. **［名前］**を 50 文字以内で入力します。
4. **［説明］**を 255 文字以内で入力します。
5. **［参照］**をクリックして、パーティションを選択します。
6. **［コメント］**を入力します。
7. **［キー長］**で、1024、2048、4096、8192 文字などのキーの長さを選択します。キーサイズが大きくなると、生成に時間がかかります。特に、8192 ビットのキーサイズでは数分かかる場合があります。
8. （任意）**［SSH キーの手動変更］**を選択します。

   詳細については、「サポートされていないプラットフォームのアカウントを管理できますか？」を参照してください。
9. （任意）**［チェックイン時にアカウントを一時停止］**：このオプションを選択すると、使用されていない管理対象アカウントが自動的に一時停止されます。つまり、SPP を通じてリクエストが行われるまで管理対象資産のアカウントは停止され、リクエストが行われた時点で SPP がアカウントを復元します。リクエストがチェックインまたはクローズされると、アカウントは再び一時停止されます。
10. （任意）**Reschedule for unscheduled SSH key change**（スケジュールされていない SSH キーの変更をリスケジュールする）：このオプションを選択すると、SSH キーの変更スケジュールが手動で変更されたときにリセットされます。たとえば、SSH キーが 10 日ごとに変更されるようスケジュールされているが、8 日目に SSH キーが手動で変更された場合、この手動リセットによりスケジュールが再開され、次の SSH キーの変更は、元のスケジュールされた変更（2 日後）ではなく、10 日後に行われます。
11. **SSH キーの変更**スケジュールを変更するには、**［スケジュール］**タブを開きます。デフォルトは**「なし」**です。
12. **［スケジュール］**ダイアログで、**［実行間隔］**を選択すると、入力した実行の詳細に従ってジョブが実行されます。（**［実行間隔］**の選択を外すと、スケジュールの詳細が失われます）。
    - 以下を設定します。

開始時刻と終了時刻を指定せずに頻度を指定する場合は、以下のコントロールから選択します。開始時刻と終了時刻を指定する場合は、このセクションの**［時間ウィンドウを使用］**を選択します。

［実行間隔］の頻度を入力し、次に、時間枠を選択します。

- **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
- **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、［**実行間隔 = 2/時間/正時@分 = 15**］と設定します。
- **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
- **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
- **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2/月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

- 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。**＋［追加］**または **- ［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、［**時間ウィンドウを使用］**を選択します。
  - 開始 22：00：00、終了 23：59：00
  - 開始 00：00：00、終了 2：00：00

開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

- **(UTC) Coordinated Universal Time** はデフォルトのタイムゾーンです。必要であれば、新しいタイムゾーンを選択してください。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行を終了すると、次の即時の時間間隔に再スケジュールされます。

13. **［OK］**をクリックします。

SSH キーの検出設定

資産上のアカウントに対して SSH キーが検出された場合、それは定義上、authorized key です。authorized key とは、資産上のユーザーのホームディレクトリにある関連ファイルに追加された公開 SSH キーのことで、ユーザーは対応する秘密キーを使用してログインすることができます。

SSH キー検出ジョブは、SSH キーを検出し管理するために実行されます。詳細については、「SSH キーの検出」を参照してください。

［資産管理］＞［プロファイル］＞［SSH キーの検出］に移動します。

表：SSH キープロパティの検出

設定	説明
名前	SSH キー検出ジョブの名前
パーティション	検出された SSH キーが管理されているパーティション
説明	ルールについての情報
スケジュール	SSH キー検出ジョブを実行するタイミングを指定します。

次のツールバーボタンを使用して SSH キー検出ジョブを管理します。

表：SSH キーの検出：ツールバー

設定	説明
＋ 追加	SSH キーの検出ジョブを追加します。詳しくは「SSH キー検出の追加」を参照してください。

設定	説明
削除	選択した SSH キー検出ジョブを削除します。
編集	選択した SSH キー検出ジョブを更新します。
更新	SSH キーの検出ジョブのリストを更新します。
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

SSH キー検出の追加

SPP が SSH キー検出を実行する方法を規定するルールを設定するのは、資産管理者またはパーティションの委任管理者の責任です。詳細については、「アカウント検出ジョブワークフロー」を参照してください。

SSH キー検出ジョブの追加手順

1. **［資産管理］＞［プロファイル］＞［SSH キープロファイルコンポーネントの表示］＞［SSH キーの検出］**の順に移動します。
2. ＋ **［追加］**をクリックして、**［SSH キー設定の検出］**ダイアログを開きます。
3. 以下を入力します：
    a. **名前**：SSH キー検出ジョブの名前を 50 文字以内で入力します。
    b. **説明**：SSH キー検出ジョブについて説明するテキストを 255 文字以内で入力します。
    c. **パーティション**：**［参照］**をクリックして、パーティションを選択します。
    d. SSH キー検出スケジュールを変更する場合は、**［スケジュール］**タブを開きます。デフォルトは**「なし」**です。
    e. **［スケジュール］**タブで、SSH キー検出ジョブを実行する間隔を選択します。

    ［実行間隔］を選択すると、入力した実行の詳細に従ってジョブが実行されます。（**［実行間隔］**の選択を解除すると、スケジュールの詳細が失われます）。

    - 以下を設定します。

      開始時刻と終了時刻を指定せずに頻度を指定する場合は、以下のコントロールから選択します。開始時刻と終了時刻を指定する場合は、このセクションの**［時間ウィンドウを使用］**を選択します。

［実行間隔］の頻度を入力し、次に、時間枠を選択します。

- **分**：指定した分単位の頻度でジョブが実行されます。たとえば、実行間隔を 30 分に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
- **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、**［実行間隔 = 2/時間/正時@分 = 15］**と設定します。
- **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
- **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
- **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2 /月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

- 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。**＋［追加］**または **-［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、**［時間ウィンドウを使用］**を選択します。
  - 開始 22：00：00、終了 23：59：00
  - 開始 00：00：00、終了 2：00：00

  開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

  ［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

  隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

  日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

- **(UTC) Coordinated Universal Time** はデフォルトのタイムゾーンです。必要であれば、新しいタイムゾーンを選択してください。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行を終了すると、次の即時の時間間隔に再スケジュールされます。

4. **［OK］**をクリックします。

SSH キー同期グループの設定

資産管理者またはパーティションの委任管理者は、SSH キーペアの SSH キー同期グループを定義します。新しいキーは同期グループ用に生成され、ターゲットホスト上の同期されたアカウントごとに設定されます。SSH キーの同期グループ内のすべてのアカウントは、同じキーを使用してすべてのシステムにログインできるように同期します。

SSH キーの同期グループは、関連するすべてのアカウントで検証とリセットを制御するために使用されます。同じ SSH キーは、同じまたは異なる資産に関連付けられた 1 つまたは複数のアカウントに使用されます。たとえば、同期された SSH キーは、クラスタまたは開発、テスト、本番の間で同期するシステムをサポートするアカウントに使用することができます。

1 つのアカウントは、1 つの SSH キー同期グループにのみ属することができます。1 つのプロファイルに複数の SSH キー同期グループを追加することができます。

プロファイルの変更スケジュールは、SSH キー同期グループに適用されます。SSH キー同期グループは、同期グループ内のアカウントの SSH キーを変更するタスクを制御します。SSH キー同期グループ内の個々のアカウントで同期に失敗すると、そのアカウントは複数回再試行され、その後も失敗すると、同期タスクは停止して再スケジュールされます。同期タスクを続行するには、管理者が失敗の原因を修正する必要があります。

アカウントが、毎日チェックするスケジュールのプロファイルに関連付けられ、SSH キーの同期グループにも関連付けられている場合、毎日のチェックで不一致があると、SSH キーを現在の SSH キーに設定するタスクが起動されます。

［資産管理］＞［プロファイル］＞［SSH キープロファイルコンポーネントの表示］＞［SSH キー同期グループ］に移動します。

表：SSH キー同期グループプロパティ

設定	説明
有効	有効の場合、プロファイルの変更スケジュールに合わせて同期が実行されます。

設定	説明
	次のツールバーボタンを使用して有効/無効を切り替えます： • ■ **有効** • ⊘ **無効**
ステータス	すべての SSH キーペアが SSH キー同期グループと同期している場合、✔が表示します。同期グループ内のいずれかのアカウントの SSH キーが同期されていない場合は、⚠が表示されます。
名前	パスワード同期グループの名前
パーティション	ルールを使用するパーティション
プロファイル	ルールを使用するプロファイル
アカウント	SSH キー同期グループで同期するアカウントの数
次の同期	SSH キー同期グループの SSH キーペアがすべてのアカウントで同期される日付
説明	ルールに関する情報

SSH キー同期グループは、次のツールバーボタンを使って管理します。

> **メモ：[SSH キー同期グループ]** ペインから行った変更は、プロファイルの SSH キー同期グループに反映されます。「SSH キープロファイルの作成」を参照してください。

表：SSH キー同期グループ：ツールバー

オプション	説明
+ 追加	SSH キー同期グループを追加します。詳しくは、「SSH キー同期グループの追加」を参照してください。
削除	選択した SSH キー同期グループを削除します。
詳細の表示	選択した SSH キー同期グループルールを更新します。
同期グループ SSH キーの変更	選択した SSH キー同期グループの SSH キーを変更します。SSH キー同期グループのすべてのアカウントが新しい SSH キーで同期されます。
更新	SSH キー同期グループのリストを更新します。

オプション	説明
検索	このリストの中から値を探すには、一致する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

SSH キー同期グループの追加

資産管理者またはパーティションの委任管理者は、SSH キー同期グループを定義します。1 つのアカウントは、1 つの SSH キー同期グループにのみ所属することができます。パーティションにプロファイルを追加するときに SSH キー同期グループと関連するアカウントを割り当てるには、「パスワードプロファイルの作成」を参照してください。

SSH キー同期グループの追加手順

1. **［資産管理］**>**［プロファイル］**>**［SSH キープロファイルコンポーネントの表示］**>**［SSH キー同期グループ］**の順に移動します。
2. ＋ **［追加］**をクリックして**［新規 SSH キー同期グループ］**ダイアログを開きます。
3. **［名前］**に固有の名前を 100 文字以内で入力します。
4. **［説明］**に 255 文字以内で入力します。
5. **［参照］**をクリックして、SSH キープロファイルを選択します。

   > **メモ**：1 つのプロファイルに複数の SSH 同期グループを追加することができます。プロファイルの変更スケジュールは、同期グループに適用されます。同期グループは、同期グループ内のアカウントの SSH ID キーを変更するタスクを制御します。

6. **［SSH キープロファイルの選択］**をクリックします。
7. **［OK］**をクリックして、グループを保存します。
8. 保存したら、リストから新しく追加された SSH キーの同期グループを選択し、**［詳細の表示］**をクリックします。
9. **［アカウント］**タブを開きます。
10. **［編集］**をクリックします。
11. ＋ **［追加］**をクリックし、同期する 1 つまたは複数の**アカウント**を選択します。
12. **［アカウントの選択］**をクリックします。

13. **［OK］**をクリックします。

デフォルト SSH キープロファイルの設定

新しいパーティションを作成すると、SPP は、デフォルトのスケジュールとルールでデフォルトのプロファイルを作成します。

別の SSH キープロファイルをデフォルトとして設定する手順

1. **［資産管理］＞［プロファイル］**に移動します。
2. **［SSH キープロファイル］**で、パーティションの現在のデフォルトプロファイルではないプロファイルを選択します。
3. 詳細ツールバーの **［デフォルトとして設定］**をクリックします。

SSH キープロファイルの削除

SSH キープロファイルを管理するのは、資産管理者の責任です。

SSH キープロファイルの削除手順

1. **［資産管理］＞［プロファイル］＞［SSH キープロファイル］**の順に移動します。
2. 削除するプロファイルを選択します。
3. **［削除］**をクリックします。
4. リクエストを確認します。

10.7 タグ

資産管理者は、タグを作成し管理することができます。

［資産管理］＞［タグ］を使用し、資産と資産アカウントのタグを作成および管理します。

さらに、資産管理者は、**[資産]**または**[アカウント]**ビューの**[全般]**タブで、資産とアカウントに静的タグを手動で追加できます。詳細については、「資産にタグを手動で追加」および「アカウントへのタグの手動追加」を参照してください。

[タグ]ページには、割り当て方法に関係なく、資産および資産アカウントに定義されたすべてのタグが一元的に表示されます。このページには、以下の詳細が表示されます。

表：タグ：プロパティ

プロパティ	説明
名前	タグの作成時に付けられた名前
パーティション	タグが所属する資産パーティション
アカウントルール	選択したタグに関連するルールがあるかどうかを示します。この欄にチェックマークがある場合は、そのタグにアカウントルールがあることを示します。
資産ルール	選択したタグに関連するルールがあるかどうかを示します。この欄にチェックマークがあるものは、そのタグに資産ルールがあることを示します。
説明	タグに関する情報
割り当てられた所有者	所有者に関する情報

タグを管理するには、これらのツールバーボタンを使用します。

表：タグ：ツールバー

オプション	説明
新しいタグ	タグを追加します。詳細については、「資産または資産アカウントの動的タグ付けのためのタグを追加」を参照してください。
削除	選択したタグを削除します。詳細については、「資産または資産アカウントのタグの削除」を参照してください。
詳細の表示	選択したタグの詳細が表示されます。詳細については、「資産または資産アカウントのタグの変更」を参照してください。 **メモ：[編集]**操作を使用して、既存のタグのパーティション割り当てを変更することはできません。**[コピー]**操作は、タグを複製して追加のパーティションに割り当てるために使用しま

オプション	説明
	す。既存のパーティションからタグを削除するには、**[削除]** 操作を使用します。
コピー	選択したタグを複製し、1 つまたは複数の追加のパーティションに割り当てます。詳細については、「資産または資産アカウントのタグを別のパーティションにコピー」を参照してください。 **メモ**：タグがパーティションにすでに存在する場合、タグは複製されたタグに置き換えられます。
発生回数	選択したタグに割り当てられている資産および資産アカウントの一覧を表示します。詳細については、「資産および資産アカウントのタグの割り当てを表示」を参照してください。
更新	タグのリストを更新します。
検索	このリストで特定のタグまたはタグのセットを検索します。

10.7.1 資産または資産アカウントのタグ付けのためのタグを追加

資産または資産アカウントのタグを追加するには、**[資産管理]** 設定ページの **[タグ]** ページにある ＋ **[新しいタグ]** ボタンを使用します。

資産または資産アカウントにタグを追加する手順

1. **[資産管理]** > **[タグ]** を選択します。
2. ＋ **[新しいタグ]** ツールバーボタンをクリックします。

   [タグ] ダイアログが表示されます。
3. **[全般]** タブで、次の情報を入力します：
   - **名前**：タグの一意の名前を入力します。
   - **説明**：タグの情報を入力します。タグに関する情報を入力します。
   - **パーティション：[参照]** をクリックして、このタグを割り当てるパーティションを選択します。

4. **［資産］**ルールタブで、資産ルールの条件を入力します。

   - **このタグのルールを有効にしてください**：このチェックボックスを選択すると、タグの設定されたルールが有効になります。
   - **ルールエディター：**ルールエディターを使用して、資産にタグをつけるための条件を定義します。

表：資産ルールタブ：ルールエディターコントロール

プロパティ	説明
および | または	**［および］**をクリックすると、複数の検索条件をまとめて表示することができ、すべての条件を満たす必要があります。 **［または］**をクリックすると、複数の検索条件をグループ化し、少なくとも 1 つの条件を満たす必要があります。
属性	最初の検索条件ボックスで、検索する属性を選択します。有効な属性は次のとおりです： • **セッションリクエストを許可** • **説明** • **ディレクトリコンテナ**（演算子「等しい」を使用した場合、1 つのレベルが検出されます） • **無効** • **検出されたグループの識別名**（検索対象がグループの属するドメインであることを指定するために使用します） • **検出されたグループ名**（検索時にドメインを指定しない場合は、この選択を使用します。ドメインを指定する場合は、**［検出されたグループの識別名］**を選択します） • **検出ジョブ名** • プロファイルの選択：プロファイルは継承することができます。たとえば、アカウントに特定のプロファイル（**プロファ**

プロパティ	説明
	イル名）を割り当てることも、親資産からプロファイルを継承することもできます（**有効なプロファイル名**）。継承された場合、プロファイル名は空になります。**「有効なプロファイル名」**は常に値を持ちます。 ◦ **有効なプロファイル名** ◦ **プロファイル名** • **名前**（デフォルト） • **ネットワークアドレス** • **パーティション名** • **プラットフォーム** • **タグ**
演算子	中間節クエリボックスで、検索に使用する演算子を選択します。使用できる演算子は、選択した属性のデータ型によって異なります。 文字列属性の場合、演算子には以下のものがあります。 • 次を含む（デフォルト） • 次を含まない • 次で開始 • 次で終了 • 等しい • 次と等しくない ブーリアン属性の場合、演算子には以下のものがあります。 • 真である • 偽である
検索文字列	最後の節のクエリボックスに、一致するものを見つけるために使用する検索文字列または値を入力します。

プロパティ	説明
＋ | －	検索条件の右側の ＋をクリックすると、検索条件に検索条件を追加することができます。 検索条件右側の －をクリックすると、検索条件から検索句が削除されます。
グループ化の追加 | 削除	＋**［グループ化の追加］**ボタンをクリックすると、満たすべき条件が追加されます。 新しいグループ化は、グループ内の最後のクエリ句の下に追加され、上位のクエリ条件に従属することを示す枠線付きのペインに表示されます。 **［削除］**ボタンをクリックすると、検索条件からグループ化が削除されます。
Preview	**［Preview］**をクリックすると、クエリを実行し、動的タグを追加する前にクエリの結果を確認することができます。

5. **［アカウントルール］**タブで、アカウントルールの条件を入力します。
   - **このタグのルールを有効にしてください**：アカウントルールを含める場合は、このチェックボックスを選択します。
   - **ルールエディター**：ルールエディターを使用して、資産アカウントにタグを付けるための条件を定義します。

表：資産アカウントルールタブ：ルールエディターのコントロール

プロパティ	説明
および | または	**［および］**をクリックすると、複数の検索条件をまとめて表示することができ、すべての条件を満たす必要があります。 **［または］**をクリックすると、複数の検索条件をグループ化し、少なくとも 1 つの条件を満たす必要があります。
属性	最初の検索条件ボックスで、検索する属性を選択します。有効な属性は次のとおりです： • **パスワードリクエストを許可**

プロパティ	説明
	• **セッションリクエストを許可** • **SSH キーリクエストを許可** • **資産名** • **資産タグ** • **説明** • **ディレクトリコンテナ**（演算子「等しい」を使用した場合、1 つのレベルが検出されます） • **無効** • **検出されたグループの識別名**（検索対象がグループの属するドメインであることを指定するには、この選択を使用します） • **検出されたグループ名**（検索でドメインを指定しない場合は、この選択を使用します。ドメインを指定する場合は、**[検出されたグループの識別名]**を選択してください。） • **検出ジョブ名** • **識別名** • **ドメイン名** • **名前** • **NetBIOS 名** • **パーティション名** • 特定のプラットフォームを選択。以下は検索の仕組みです： ◦ **プラットフォーム**：これは最も広い範囲の検索で、最も多くの結果を得ることができます。入力された値は、以下のうち 1 つ以上に該当する場合に一致します。

プロパティ	説明
	◦ **DisplayName** Windows などの（プラットフォーム名） ◦ PlatformType MicrosoftAD, Ubuntu, RacfLdap など ◦ PlatformFamily Windows, Linux, AIX など ◦ Platform.Version (プラットフォームバージョン) Server 2016, 10 例えば、Other と入力すると、以下のようなプラットフォームが返されます。Windows Other、Other Other、Other ◦ **プラットフォーム名：**より詳細な検索を行う場合は、Windows などのプラットフォーム名を入力してください。プラットフォームバージョンを入力せずに Windows と入力した場合、Windows Server 2019、Windows Server 2016、Windows 10 で一致する場合があります。 ◦ **プラットフォームバージョン：** Server 2016 など、プラットフォームのバージョンを入力します。例えば、**プラットフォーム名**を Windows、**プラットフォームバージョン**を Server 2016 と入力した場合、Windows Server 2016 のみが選択されます。 詳しくは、「Web 管理コンソールのシステム要件」を参照してください。

プロパティ	説明
	• **サービスアカウント** • **SID** • **タグ**
演算子	中間節クエリボックスで、検索に使用する演算子を選択します。使用できる演算子は、選択した属性のデータ型によって異なります。 文字列属性の場合、演算子には以下のものがあります。 • 次を含む（デフォルト） • 次を含まない • 次で開始 • 次で終了 • 等しい • 次と等しくない ブーリアン属性の場合、演算子には以下のものがあります。 • 真である • 偽である
検索文字列	最後の節のクエリボックスに、一致するものを見つけるために使用する検索文字列または値を入力します。
＋ | －	検索条件の右側の ＋ をクリックすると、検索条件に検索条件を追加することができます。 検索条件右側の － をクリックすると、検索条件から検索句が削除されます。
グループ化の追加 | 削除	＋ **［グループ化の追加］**ボタンをクリックすると、満たすべき条件が追加されます。 新しいグループ化は、グループ内の最後のクエリ句の下に追加され、上位のクエリ条件に従属することを示す枠線付きのペインに表示されます。 **［削除］**ボタンをクリックすると、検索条件からグループ化が削除されます。

プロパティ	説明
Preview	**［Preview］**をクリックすると、クエリを実行し、動的タグを追加する前にクエリの結果を確認することができます。

6. **［OK］**をクリックしてタグを作成し、ダイアログを閉じます。**タグ**ペインに戻ります。
7. タグを保存したあと、タグを選択して **［詳細の表示］**を選択します。
8. **［割り当てられた所有者］**タブで、タグに関連付けられたユーザーまたはグループを入力します。これは、タグに関連付けられたユーザーおよび/またはグループが、タグ自体の所有者になることを意味するものではありません。その代わり、タグが資産やアカウントに割り当てられると、リストアップされたユーザーやグループがその資産やアカウントの所有者になります。

表：割り当てられた所有者タブ：ルールエディターのコントロール

プロパティ	説明
+ | −	ユーザーまたはユーザーグループを追加するには、+ をクリックします。 追加されたユーザーまたはグループを削除するには、− をクリックします。
更新	ユーザーおよびグループのリストを更新します。

9. **［OK］**をクリックして割り当てられた所有者を保存し、ダイアログを閉じます。**タグ**ペインに戻ります。

資産または資産アカウントのタグの削除

タグは、複数のオブジェクトタイプに割り当てることができます。つまり、同じタグを資産とディレクトリアカウントを含む資産アカウントに割り当てることができます。削除すると、タグの割り当て方法（動的または手動）に関係なく、そのタグへのすべての参照が削除されます。

資産または資産アカウントのタグの削除手順

1. **［資産管理］＞［タグ］**を選択します。
2. 削除するタグを選択します。
3. **［削除］**ツールバーボタンをクリックします。
4. 確認ダイアログで、**［はい］**をクリックします。
5. タグが使用されている場合、タグを削除するとポリシー設定が変更される可能性があるため、削除操作を確認またはキャンセルする機会が提供されます。
    - タグを削除するには、**［強制削除］**を入力し、**［OK］**をクリックします。

資産または資産アカウントのタグの変更

資産または資産アカウントのタグを変更するには、**［資産管理］**設定ページの**［タグ］**ペインにある **［詳細を表示］**ボタンを使用します。

［詳細の表示］操作では、既存のタグのパーティション割り当てを**［編集］**操作で変更することはできません。タグを複製して追加のパーティションに割り当てるには、**［コピー］**操作を使用します。詳細については、「資産または資産アカウントのタグを別のパーティションにコピー」を参照してください。

資産または資産アカウントのタグの変更手順

1. **［資産管理］＞［タグ］**を開きます。
2. 変更するタグを選択します。
3. ツールバーボタンを選択します。**［タグ］**ダイアログが表示され、選択したタグの設定を変更することができます。詳細については、「資産または資産アカウントの動的タグ付けのためのタグを追加」を参照してください。

資産または資産アカウントのタグを別のパーティションにコピー

資産および資産アカウントのタグは、パーティションに属します。**［資産管理］**設定ページの**［タグ］**ペインの **［コピー］**ボタンを使って、資産または資産アカウントのタグを複製して、別のパーティションに割り当てます。

既存のタグのパーティション割り当てを**［編集］**操作で変更することはできません。このコピー操作を使用して、タグを複製し、それを追加のパーティションに割り当てます。

資産または資産アカウントタグを別のパーティションにコピーする手順

1. **［資産管理］＞［タグ］**に移動します。
2. ツールバーボタンをクリックします。**［コピー先］**ダイアログが表示され、1 つまたは複数のパーティションを選択できるようになります。
3. 選択したタグを割り当てるパーティションのチェックボックスを選択します。
4. **［パーティションの選択］**をクリックします。選択したパーティションにすでに同じ名前のタグが存在する場合、タグを置き換えるかどうか尋ねられます。

資産および資産アカウントのタグの割り当てを表示

タグに割り当てられたすべての資産と資産アカウントのリストを表示するには、**［資産管理］**ページの**［タグ］**ペインの **［発生回数］**ボタンを使用します。

資産と資産アカウントのタグの割り当てを表示する手順

1. **［資産管理］＞［タグ］**に移動します。
2. リストからタグを選択します。
3. ツールバーの **［発生回数］**ボタンをクリックします。

   選択した動的タグに割り当てられたすべての資産とアカウントのリストが含まれる**［発生回数］**ダイアログが表示されます。

   - **名前：**資産またはアカウントの名前
   - **ドメイン名：**ドメインの名前
   - **資産**：資産の名前
   - **動的：**タグが動的に割り当てられたものかどうかを示します。
   - **タイプ：**名前付き資産に関連する資産またはアカウントを識別しているかどうか。
4. **［検索］**ボックスを使用して、このリスト内の特定のタグまたはタグのセットを検索します。一致するタグを検索するために使用する文字列を入力します。

5. **［×］**をクリックすると、ダイアログが閉じられ、**［タグ］**ペインに戻ります。

10.8 接続およびプラットフォーム

10.8.1 登録済みコネクタ

資産管理者は、登録済みコネクタの追加と管理を行います。

［資産管理］＞［接続およびプラットフォーム］＞［登録済みコネクタ］に移動します。

SPP を One Identity Starling に参加すると（詳細については、「Starling」を参照）、「登録済みコネクタ」ペインに以下が表示されます。

表：登録済みコネクタ：プロパティ

プロパティ	説明
表示名	登録されたコネクタに入力された表示名が表示されます。
プラットフォーム名	プラットフォーム名が表示されます。
表示可能なパーティション	コネクタが可視化されているパーティションが表示されます。すべてのパーティションで可視化されている場合は、**すべてのパーティション**と表示されます。

登録済みコネクタの設定は次のツールバーボタンを使用して管理します。

表：登録済みコネクタ：ツールバー

オプション	説明
追加	登録済みコネクタを追加します。詳しくは「登録済みコネクタの追加」を参照してください。
削除	選択された登録済みコネクタを削除します。
編集	選択された登録済みコネクタを編集します。
更新	登録済みコネクタのリストを更新します。
表示	登録済みコネクタの有効なオペレーションを表示します。

登録済みコネクタの追加

登録済みコネクタを設定するのは、資産管理者の責任です。

登録済みコネクタの追加手順

> **重要**： 登録済みコネクタを追加する前に、SPP で使用するために Starling Connect 内でコネクタを構成する手順について、Starling Connect のドキュメントをお読みください。現在、SPP で使用可能なコネクタは、Starling Connect のドキュメントに記載されています。

1. **［資産管理］＞［接続およびプラットフォーム］＞［登録済みコネクタ］**に移動します。
2. ＋ **［追加］**をクリックします。
3. これらのフィールドが表示されます。
   a. **登録済みコネクタ**：SPP に登録するコネクタ（Starling Connect ですでに構成済み）を選択します。
   b. **Starling コネクタバージョン**：Starling コネクタのバージョンを選択します。
   c. **表示名：**コネクタの表示名を入力します。
   d. **すべてのパーティションに表示**：このチェックボックスを選択すると、登録されたコネクタがすべてのパーティションから見えるようになります。
   e. **パーティションに表示：［すべてのパーティションに表示］**が選択されていない場合に利用可能で、登録されたコネクタをどのパーティションに表示するかを定義します。
      - ＋（追加）：このボタンを使用して、新しいパーティションを追加します。
      - ー（削除）： このボタンを使用して、以前に選択したパーティションを削除します。
4. 登録済みコネクタを追加するには、**［OK］**をクリックします。

   これで、コネクタはプラットフォームとして登録され、資産の定義でプラットフォームタイプとして利用できるようになります。

> **重要**: 登録済みのコネクタを SPP で使用する場合、特定の機能を構成する際に追加の考慮が必要になる場合があります。たとえば、Azure AD はスロットリングを使用して、一定期間内に発生するパスワードの変更回数を制限します。これは、登録された Azure AD コネクタに関連

する多数のアカウントが、パスワード管理設定によりすべて自動的にパスワードを更新するようにスケジュールされている場合、SPP 内でエラーが報告されることを意味します。

10.8.2 カスタムプラットフォーム

資産管理者は、プラットフォームのコマンドと詳細を含むカスタムプラットフォームスクリプトをアップロードして、カスタムプラットフォームを追加します。監査人とパーティション管理者には、読み取り専用権限があります。カスタムプラットフォームは、すべてのパーティションにまたがってグローバルです。カスタムプラットフォームは、資産の追加や更新の際に選択できます。

［資産管理］＞［接続およびプラットフォーム］＞［カスタムプラットフォーム］で、カスタムプラットフォームを作成および管理します。

［カスタムプラットフォーム］ペインには、以下が表示されます。

表：カスタムプラットフォーム：ツールバー

オプション	説明
＋ 追加	カスタムプラットフォームを追加します。詳細については、「カスタムプラットフォームの追加」を参照してください。
削除	選択したカスタムプラットフォームを削除します。 **注意：カスタムプラットフォームが資産に関連付けられている場合、カスタムプラットフォームを削除すると、パスワードの検証およびリセットが停止されることがあります。資産が製品プラットフォームタイプの［Other］に割り当てられることを示す警告が表示されます。［強制削除］を入力して、削除を確認します。**
編集	選択したプラットフォームを編集します。
ダウンロード	選択されたカスタムプラットフォーム JSON スクリプトをダウンロードします。
更新	カスタムプラットフォームのリストを更新します。

カスタムプラットフォームスクリプトの作成

カスタムプラットフォームスクリプトは、プラットフォームのコマンドと関連する詳細を特定します。スクリプトは JSON で記述されます。スクリプトには、プラットフォームへの認証、パスワードの検証およびリセットを実行するためのメタデータ、パラメーター、機能ブロック、操作、および if/then 構成が含まれます。カスタムプラットフォームスクリプトは、カスタムプラットフォームを追加する際にアップロードされます。

資産管理者は、資産を作成し、関連するカスタムスクリプトのデフォルト値を受け入れることができます。後でデフォルト値が異なる新バージョンのカスタムプラットフォームスクリプトをアップロードしても、資産のデフォルト値は変更されません。

委任された管理者は、カスタムプラットフォームスクリプトを作成することはできません。

サンプルスクリプト

カスタムプラットフォームスクリプトのサンプルとコマンドの詳細は、GitHub 上の以下のリンクから入手可能です：

- Safeguard カスタムプラットフォームホーム（英語）
    - カスタムプラットフォームスクリプトの構造（英語）
    - カスタムプラットフォームスクリプトの書き方（英語）
    - コマンドリファレンス（英語）
- サンプルスクリプト（英語）

> ⚠ **注意：サンプルスクリプトは、情報提供のみを目的としています。実運用で使用する前に、更新、エラーチェック、およびテストが必要です。SPP は、値が文字列、ブーリアン、整数、パスワード（API スクリプトでは secret と呼ばれる）などのプロパティの型と一致しているかどうかをチェックします。SPP パスワードは、カスタムプラットフォームに入力された値の有効性やシステムへの影響をチェックすることはできません。**

開発時には、バリデータを用いて JSON をチェックしてください。

カスタムプラットフォームの追加

SPP がカスタムプラットフォームを処理するようにルールを設定するのは、資産管理者の責任です。カスタムプラットフォームスクリプトをアップロードできるようにする必要があります。詳細については、「カスタムプラットフォームスクリプトの作成」を参照してください。

カスタムプラットフォームの追加手順

1. カスタムプラットフォームスクリプトファイルをアップロードできるようにします。
2. **［資産管理］＞［接続およびプラットフォーム］＞［カスタムプラットフォーム］**の順に移動します。
3. ＋**［追加］**をクリックします。
4. 以下のフィールドが表示されます：
    a. **名前**：プラットフォームタイプの固有名（製品名でも可）を入力します。
    b. **プラットフォームスクリプト**：**［参照］**をクリックし、スクリプトファイルを選択して**［開く］**をクリックします。選択したカスタムプラットフォームスクリプトファイルが表示されます。
    c. セッションのアクセスリクエストを許可するには、**［セッションリクエストを許可］**チェックボックスを選択します。このチェックボックスは、通常 SSH の場合に選択されます。セッションアクセスリクエストを禁止するには、**［セッションリクエストを許可］**チェックボックスをオフにします
5. **［OK］**をクリックします。カスタムプラットフォームスクリプトにエラーがある場合は、次のようなエラーメッセージが表示されます。「定義が有効な json オブジェクトではありませんでした。」

11 セキュリティポリシー管理

左側のナビゲーションペインにある**［セキュリティポリシー管理］**セクションを展開します。

11.1 Access Request Activity

Access Request Activity（アクセスリクエストアクティビティ）ページでは、セキュリティポリシー管理者がアクセスリクエストを一箇所で確認、管理することができます。ページ上のアクセスリクエストタイルの 1 つをクリックすると、そのカテゴリに属するアクセスリクエストに関する追加情報が表示されます。さらに、リクエストのワークフローの確認、ライブセッションの開始、セッションの終了、特定のリクエストの取り消しを行うことができます。

このダッシュボードは、次の管理者権限が割り当てられている SPP ユーザーが利用できます。

- 監査人：読み取り専用
- セキュリティポリシー：フル コントロール

アクセスリクエスト：タイル

以下のタイルのいずれかをクリックすると、追加情報を表示するダイアログが表示されます。 ボタンをクリックすると、表示されるタイルをカスタマイズすることができます。

- **Open Requests（オープンリクエスト）**：セッションリクエストやパスワードリリースリクエストを含む、現在開かれているすべてのアクセスリクエストのリストが表示されます。
- **承認が保留中**：承認待ちのアクセスリクエストの一覧が表示されます。
- **レビューが保留中：**レビュー中のアクセスリクエストの一覧が表示されます。
- **Open Sessions（オープンセッション）**。現在開かれているセッションのリストが表示されます。
- **Password Out（パスワードアウト）**：現在チェックアウトされているすべてのパスワードリリースリクエストのリストが表示されます。
- **SSH Keys Out（SSH キーアウト）**：現在チェックアウトされているすべての SSH キーのリリースリクエストリストが表示されます。

アクセスリクエスト：ツールバー

タイルの 1 つを開いたら、詳細グリッドの上部にあるツールバーを使って、次のタスクを実行します。

- **詳細の表示**： リクエストに関する追加情報が表示されます。
- **リクエストワークフローの詳細**：選択したリクエスト：で発生したトランザクションを確認するために選択します。このボタンをクリックすると、リクエストワークフローダイアログが表示され、リクエストから承認、レビューまでのリクエストのワークフロー中に発生したトランザクションを監査することができます。
- **SPS のセッション監査ログ**： SPS のセッション監査ログが表示されます。
- **ライブセッションの表示**：選択したセッションリクエストのライブセッションを表示する場合に選択します。このボタンをクリックすると、Desktop Player (サポートされる最小バージョンは 1.11.15) が起動し、アクティブなセッションを追跡することができます。

  Desktop Player の使用方法の詳細については、「Safeguard Desktop Player ユーザーガイド」を参照してください。
- **Terminate Live Session（ライブセッションの終了）**：選択したセッションリクエストのライブセッションを終了する場合に選択します。
- **Close Request（リクエストを閉じる）**：選択したアクセスリクエストを撤回する場合に選択します。
- **エクスポート**：現在表示されているアクセスリクエストのグリッドの .csv または .json ファイルを作成し、任意の場所に保存する場合に選択します。時間は、ユーザーのタイムゾーンに従って設定されます。
- **表示する列の選択**：選択すると、グリッドに表示可能な列の一覧が表示されます。グリッドに表示させたいデータのチェックボックスを選択します。グリッドから除外したいデータのチェックボックスをオフにします。

11.2 アカウントグループ

SPP のアカウントグループは、アクセスリクエストポリシーのスコープに追加できるアカウントのセットです。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

監査人とセキュリティポリシー管理者には、**［アカウントグループ］**にアクセスする権限があります。

アカウントグループへのアクセス

［セキュリティポリシー管理］＞［アカウントグループ］

アカウントグループビューには選択したアカウントグループの以下の情報が表示されます：

- **プロパティ**タブ：選択したアカウントグループに関する全般的な情報が表示されます。
- **アカウント**タブ：選択したアカウントグループに関連するアカウントが表示されます。
- **アクセスリクエストポリシー**タブ：選択したアカウントグループに関連する資格およびアクセスリクエストポリシーが表示されます。
- **履歴**タブ：選択したアカウントグループに影響を与えた各操作の詳細が表示されます。

次のツールバーボタンを使用して、アカウントグループを管理します。

- **［アカウントグループ］**：アカウントグループを SPP に追加します。詳細については、「アカウントグループの追加」を参照してください。
- **［アカウントの動的グループ］**：SPP に動的アカウントグループを追加します。詳細については、「動的アカウントグループの追加」を参照してください。
- **［削除］**：選択したアカウントグループを SPP から削除します。詳細については、「アカウントグループの削除」を参照してください。
- **［詳細の表示］**：選択したアカウントグループの情報と構成オプションが表示されます。
- **［エクスポート］**：リストされたデータが JSON または CSV ファイルにエクスポートされます。詳しくは「データのエクスポート」を参照してください。
- **［更新］**：アカウントグループのリストを更新します。
- **［検索］**：文字列で検索するか、選択した属性で条件を入力して検索することができます。選択した属性で検索する場合は、**［検索］**をクリックし、検索する属性を選択します。詳しくは、「検索ボックス」を参照してください。

11.2.1 プロパティタブ

プロパティタブには、選択したアカウントグループに関する情報が一覧表示されます。

プロパティへのアクセス

［セキュリティポリシー管理］＞［アカウントグループ］＞（詳細の表示）**＞［プロパティ］**

表：アカウントグループプロパティタブ：全般プロパティ

プロパティ	説明
名前	選択したアカウントグループの名前
説明	選択したアカウントグループに関する情報
アカウントルール	動的アカウントグループの場合、定義された資産アカウントルールの概要

11.2.2 アカウントタブ

アカウントタブには、選択したアカウントグループに関連付けられているアカウントが表示されます。

アカウントへのアクセス

［セキュリティポリシー管理］＞［アカウントグループ］＞（詳細の表示）**＞［アカウント］**

表：アカウントグループ：アカウントタブプロパティ

プロパティ	説明
名前	選択したアカウントグループに属するアカウントの名前
親	アカウントが所属する資産
ドメイン名	ディレクトリアカウントの場合、アカウントが関連付けられているドメインの名前
無効	この列のチェックは、アカウントが管理されていないことを示しています。
サービスアカウント	この列のチェックは、アカウントがサービスアカウントであることを示しています。
パスワードリクエスト	この列のチェックは、このアカウントに対してパスワードリリースリクエストが有効になっていることを示しています。

プロパティ	説明
セッションリクエスト	この列のチェックは、このアカウントでセッションアクセスリクエストが有効になっていることを示します。
SSH キーリクエスト	この列のチェックは、このアカウントで SSH キーアクセスリクエストが有効になっていることを示します。
パスワード	この列のチェックは、選択したアカウントにパスワードが設定されていることを示します。詳細については、「アカウントパスワードの確認、変更、設定」を参照してください。
SSH キー	この列のチェックは、選択したアカウントに SSH キーが設定されていることを示します。詳細については、「SSH キーの確認、変更、設定」を参照してください。
説明	アカウントに関する情報

次の詳細ツールバーボタンを使用して管理します。

表：アカウントグループ：アクセスリクエストタブツールバー

オプション	説明
＋ アカウントの追加	選択したアカウントグループに 1 つ以上のアカウントを追加します。
ー 削除	選択したアカウントを削除します。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	アカウントリストを更新します。
検索	このリストから特定のアカウントを見つけるには、検索に使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

11.2.3 アクセスリクエストポリシータブ

アクセスリクエストポリシータブには、資格とポリシーが表示されます。これには、選択したアカウントグループに関連するパスワードと SSH キーのリリースに関するポリシーとセッションリクエストのポリシーが含まれる場合があります。

表：アカウントグループ：アクセスリクエストポリシータブプロパティ

プロパティ	説明
資格	アクセスリクエストポリシーの資格の名前
アクセスリクエストポリシー	選択したアカウントグループのアカウントに適用されるポリシーの名前
アカウント数	アクセスリクエストポリシーに関連付けられているアカウントグループ内の一意のアカウントの数
アカウントグループ数	アクセスリクエストポリシーに含まれる一意のアカウントグループの数

次の詳細ツールバーボタンを使用して、選択したアカウントグループに関連付けられたアクセスリクエストポリシーを管理します。

表：アカウントグループ：アクセスリクエストポリシータブツールバー

オプション	説明
＋ 追加	選択したアカウントグループを 1 つ以上のアクセスリクエストポリシーのスコープに追加します。このボタンをクリックすると、**[アクセスリクエストポリシー]** の選択ダイアログが表示され、ポリシーを選択することができます。
ー 削除	選択したアカウントグループを選択したアクセスポリシーのスコープから削除します。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	アクセスリクエストポリシーのリストを更新します。
検索	このリストから特定のポリシーまたはポリシーのセットを検索するには、一致するものを検索するために使用する文字列を入

オプション	説明
	力します。詳細については、「検索ボックス」を参照してください。

11.2.4 履歴タブ

履歴タブでは、選択したアカウントグループに影響を与えた各操作の詳細を表示またはエクスポートすることができます。

履歴へのアクセス

［セキュリティポリシー管理］＞［アカウントグループ］＞（詳細の表示）**＞［履歴］**

- **日付範囲：**デフォルトでは、履歴の詳細は過去 24 時間分表示されます。ドロップダウンから、時間間隔を一つ選択すると、その時間枠の履歴の詳細が表示されます。
- **エクスポート**：データを.csv ファイルにエクスポートします。
- **更新**：表示されているリストを更新します。
- **検索**：詳細については、「検索ボックス」を参照してください。

表：アカウントグループ：履歴タブプロパティ

プロパティ	説明
日付/時間	イベントの日時
ユーザー	イベントを発生させたユーザーの表示名
ソース IP	イベントを発生させた管理対象システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択したアカウントグループの名前
イベント	選択したアカウントグループに対して行われた操作のタイプ： • 作成 • 削除 • 更新 • メンバーシップの追加 • メンバーシップの削除

プロパティ	説明
	メモ： メンバーシップ操作は、選択したアカウントグループがポリシーのメンバーシップに追加または削除された、または選択したアカウントグループのメンバーシップからアカウントが追加または削除されたなど、関連オブジェクトまたは親オブジェクトとの関係が変更されたことを示します。
関連オブジェクト	関連するオブジェクトの名前
関連オブジェクトタイプ	関連するオブジェクトのタイプ
親	選択されたアカウントグループが子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

11.2.5 アカウントグループの管理

アカウントグループビューのコントロールとタブ付きページを使用して、次のタスクを実行し、SPP アカウントグループを管理します。

- アカウントグループの追加
- 動的アカウントグループの追加
- アカウントグループへの 1 つ以上のアカウントの追加
- アクセスリクエストポリシーへのアカウント追加
- アカウントグループの削除

アカウントグループの追加

SPP にアカウントグループを追加するのは、セキュリティポリシー管理者の責任です。

アカウントグループの追加手順

1. **［セキュリティポリシー管理］＞［アカウントグループ］**に移動します。
2. ツールバーから ＋ **［新しいアカウントグループ］＞［アカウントグループ］**をクリックします。
3. **新しいアカウントグループ**ダイアログで、次の情報を入力します：
    - **名前**：アカウントグループの一意の名前を 50 文字以内で入力します。
    - **説明**：（任意）このアカウントグループに関する情報を 255 文字以内で入力します。
4. **［OK］**をクリックします。

動的アカウントグループの追加

SPP に動的アカウントグループを追加するのは、セキュリティポリシー管理者の責任です。

動的アカウントグループは、該当するオブジェクトが作成または変更されたときに実行されるルールエンジンに関連付けられます。例えば以下のようになります：

- 資産アカウントを追加または変更するたびに、その資産アカウントに対して適用可能なすべてのルールが再評価されます。
- 資産アカウントルールを変更するたびに、そのルールの範囲内にあるすべての資産アカウントに対してルールが再評価されます。つまり、グループ化のためにすべての資産アカウントに対して、タグ付けのために指定されたパーティション内の資産アカウントに対して、ルールが再評価されます。

ルールなしで動的なアカウントグループを作成することもできますが、ルールを追加するまで、この動的アカウントグループにアカウントは追加されません。

大規模な環境では、すべてのルールが再評価される前にユーザーインターフェイスが返され、期待した結果が表示されない可能性があります。このような場合は、数分待ってから画面を**［更新］**して結果を表示してください。

動的アカウントグループの追加手順

1. **［セキュリティポリシー管理］＞［アカウントグループ］**に移動します。
2. ツールバーから ＋ **［新しいアカウントグループ］＞［アカウントの動的グループ］**をクリックします。

3. **［新しい動的アカウントグループ］**ダイアログで、次の情報を入力します。

タブ	説明
全般タブ	動的アカウントグループに関する全般情報を追加する場所
アカウントルールタブ	動的アカウントグループに含まれるアカウントを識別するために使用するルールを定義する場所

全般タブ

アカウントグループダイアログの**［全般］**タブで、動的アカウントグループに関する全般情報を入力します。

表：動的アカウントグループ：［全般］タブ

プロパティ	説明
名前	動的アカウントグループの一意の名前を 50 文字以内で入力します。
説明	動的アカウントグループに関する情報を 255 文字以内入力します。

アカウントルールタブ

アカウントグループダイアログの**［アカウントルール］**タブにあるルールエディターコントロールを使用して、動的アカウントグループに含めるアカウントを定義します。

表：動的アカウントグループ：資産アカウントルールタブ

プロパティ	説明
このグループのルールを有効にしてください	このチェックボックスをオンにすると、この動的アカウントグループに資産アカウントルールが追加されます。このチェックボックスを選択すると、ルールエディターコントロールが有効になります。 **メモ：** ルールなしで動的アカウントグループを作成することもできますが、ルールを追加するまでは、この動的アカウントグループにアカウントは追加されません。

プロパティ	説明
**および	または**	**［および］**をクリックすると、複数の検索条件をグループ化することができます。すべての条件を満たす必要があります。 **［または］**をクリックすると、複数の検索条件をグループ化し、少なくとも 1 つの条件を満たす必要がある場合に、その条件を含めることができます。
属性	最初のクエリ句ボックスで、検索する属性を選択します。有効な属性は次のとおりです。 • **名前**（デフォルト） • **説明** • **プラットフォーム** • **無効** • **タグ** • **サービスアカウント** • **パーティション名** • **資産名** • **資産タグ** • **ドメイン名** • **NetBIOS 名** • **識別名**（この属性を使用して 1 レベルの検索を実行することはできません。） • **SID** • **検出されたグループ名**（検索でドメインを指定しない場合は、この選択を使用します。ドメインを指定する場合は、**［検出されたグループの識別名］**を選択します。） • **検出されたグループの識別名**（検索対象がグループの所属するドメインであることを指定するには、この選択を使用します。） • **ディレクトリコンテナ**（演算子**［等しい］**を使用すると、1 つのレベルが検索されます。）
演算子	中央のクエリボックスで、検索に使用する演算子を選択します。使用可能な演算子は、選択した属性のデータ型に依存します。 文字列属性の場合、演算子には次のものが含まれます。 • **次を含む**（デフォルト）

プロパティ	説明
	• **次を含まない** • **次で開始** • **次で終了** • **等しい** • **次と等しくない** ブーリアン属性（サービスアカウントなど）の場合、演算子には次のものが含まれます。 • 真である • 偽である
検索文字列	最後の句のクエリボックスに、一致するものを見つけるために使用する検索文字列または値を入力します。 **［検出されたグループ名］**、**［検出されたグループの識別名］**、または**［ディレクトリコンテナ］**の属性を選択した場合： 1. **［参照］**をクリックして**［ディレクトリ資産の選択］**ダイアログに移動し、検索文字列を探します。各ディレクトリの名前、資産のパーティション、説明が表示されます。 2. ディレクトリを選択し、**［OK］**をクリックします。 3. **［検索場所］**ダイアログで、場所を選択して**［OK］**をクリックします。
＋ | －	検索句の左側の＋をクリックすると、検索条件を追加することができます。 －をクリックすると、検索条件から検索句が削除されます。
グループ化の追加｜削除	＋**［グループ化の追加］**ボタンをクリックすると、満たすべき条件を追加することができます。 新しいグループ化は、グループ内の最後のクエリ句の下に追加され、上位のクエリ条件に従属することを示す枠線付きのペインに表示されます。 －**［グループ化の削除］**ボタンをクリックすると、検索条件からグループを削除することができます。
Preview	動的グループを追加する前にクエリの結果を確認するには、**［Preview］**をクリックしてクエリを実行します。

アカウントグループへの 1 つ以上のアカウントの追加

アカウントグループビューでは、1 つ以上のアカウントをアカウントグループに追加することができます。

アカウントグループにアカウントを追加する手順

1. **［セキュリティポリシー管理］＞［アカウントグループ］**に移動します。
2. アカウントグループを選択し、**［詳細の表示］**をクリックします。
3. **［アカウント］**タブを選択します。
4. 詳細ツールバーから、**［アカウントの追加］**をクリックします。
5. **［グループに追加するアカウントを選択してください］**ダイアログのリストから 1 つ以上のアカウントを選択します。
6. **［アカウントの選択］**をクリックします。

アクセスリクエストポリシーへのアカウント追加

アクセスリクエストポリシーへのアカウント追加手順

1. **［セキュリティポリシー管理］＞［アカウントグループ］**に移動します。
2. リストからアカウントグループを選択し、**［詳細の表示］**をクリックします。
3. **［アクセスリクエストポリシー］**タブを開きます。
4. 詳細ツールバーから、**［追加］**をクリックします。
5. **［アクセスポリシー］**ダイアログのリストからポリシーを選択し、**［OK］**をクリックします。

アカウントグループの削除

アカウントグループを削除しても、SPP は関連するアカウントを削除しません。

アカウントグループの削除手順

1. **［セキュリティポリシー管理］＞［アカウントグループ］**を開きます。
2. リストからアカウントグループを選択します。
3. **［削除］**をクリックします。
4. リクエストを確認します。

11.3 アプリケーション – アプリケーション

サードパーティのアプリケーションがアプリケーション-アプリケーションサービスを使用して SPP のデータ保管庫と統合するためには、まずアプリケーションを SPP に登録する必要があります。これは、以下に説明する**［セキュリティポリシー管理］＞［アプリケーション – アプリケーション］**ページを使用して行うことができます。アプリケーションを登録したら、サービスを有効化または無効化することができます。詳細については、「サービスの有効化または無効化」を参照してください。

［アプリケーション - アプリケーション］ページには、以前に登録されたサードパーティ製アプリケーションのリストが表示されます。このページから、セキュリティポリシー管理者は、新しいアプリケーションの登録を追加したり、既存の登録を変更または削除したりすることができます。**［アプリケーション - アプリケーション］**ページには、アプリケーションの登録に関する次の詳細が表示されます。

表：アプリケーション - アプリケーション：プロパティ

プロパティ	説明
名前	アプリケーションの登録に割り当てられた名前
証明書ユーザー	登録されたアプリケーションに関連付けられた証明書ユーザーの名前 **メモ:** アプリケーションの登録に証明書ユーザーが表示されていない場合は、セキュリティポリシー管理者に連絡して、証明書ユーザーを追加してください。サードパーティアプリケーションのアプリケーション – アプリケーションサービスは、証明書ユーザーが指定されるまで、SPP 保管庫で機能しません。

プロパティ	説明
有効／無効 トグルオン トグルオフ	アプリケーションの登録が有効かどうかを示します。トグルは、サービスが有効な場合はスイッチが右側にある状態で青く表示され、サービスが無効な場合はスイッチが左側にある状態で灰色に表示されます。トグルをクリックすると、アプリケーションの登録が有効または無効になります。 **メモ：**アプリケーションの登録を無効にすると、その登録が再び有効になるまで、そのサードパーティアプリケーションのアプリケーション間アクセスは無効になります。
説明	アプリケーションの登録に関する情報

次のツールバーボタンを使用してアプリケーションの登録を管理します。

表：アプリケーション - アプリケーション：ツールバー

オプション	説明
追加	SPP にアプリケーション登録を追加します。詳細については、「アプリケーション登録の追加」を参照してください。
削除	選択したアプリケーション登録を SPP から削除します。詳細については、「アプリケーション登録の削除」を参照してください。
更新	アプリケーション登録のリストを更新します。
編集	選択したアプリケーションの登録を変更します。

11.3.1 アプリケーション - アプリケーション機能とは

アプリケーション – アプリケーションサービスを使用することで、サードパーティアプリケーションは以下の方法で SPP と対話することができます。

- 資格情報の取得：サードパーティアプリケーションは、対象資産に対して自動化された機能を実行するために、SPP の保管庫から資格情報を取得することができます。また、プロシージャ、スクリプト、およびその他のプログラム内のハードコードされたパスワードをプログラム呼び出しに置き換えることができます。

- アクセスリクエストブローカー：サードパーティのアプリケーションは、許可されたユーザーの代わりにアクセスリクエストを開始することができ、許可されたユーザーは利用可能なリクエストを通知され、SPP にログインしてパスワードを取得したりセッションを開始したりすることができるようになります。

> **メモ:** オフラインワークフローモードがトリガーされた場合、アプリケーション間の操作は、オフラインワークフローモードに移行するのにかかる分数だけ停止されます。詳細については、「オフラインワークフローモードとは」を参照してください。

資格情報取得

アプリケーション – アプリケーションサービスを使用した資格情報取得リクエストにより、サードパーティアプリケーションは通常のワークフロープロセスを経ることなく SPP の保管庫（Vault）から資格情報を取得することができます。

たとえば、24 時間ごとにデータセンター内のさまざまなサービスに対して定期的なシステム診断を行う自動化システムがあるとします。自動化システムが診断を行うには、まず対象サーバーに認証される必要があります。対象サーバーのすべての認証情報は SPP 保管庫（Vault）に保存されているため、自動化システムはアプリケーション – アプリケーションサービスを呼び出して、指定されたシステムの認証情報を取得します。

アクセスリクエストブローカー

アプリケーション – アプリケーションサービスを使用したアクセスリクエストブローカー要求は、アプリケーションが他のユーザーの代わりにアクセスリクエストを作成することを可能にします。

例えば、チケットシステムがあり、作成できるチケットの種類の 1 つが、特定の資産へのアクセスをリクエストするものであるとします。このチケットシステムは、アプリケーション – アプリケーションサービスを通じて SPP と統合され、システムにチケットを入力したユーザーに代わってアクセスリクエストを作成することができます。リクエストが作成されると、SPP の通常のアクセスリクエストのワークフローに従い、アクセスが許可されるとチケットを入力したユーザーに通知されます。

サードパーティアプリケーションがアプリケーション – アプリケーションサービスで提供されるタスクの 1 つを実行するためには、まずアプリケーションを SPP に登録する必要があります。この登録は、証明書ユーザーと関連付けられ、アプリケーション – アプリケーションサービスへの認証は、証明書と API キーを使用して行われます。登録されたアプリケーションは、指定された目的以外では SPP への認証が許可されません。アプリケーションの登録に関連するプロパティは次のとおりです:

- API キー：登録プロセスの一部として、API キーが生成されます。管理者は、この API キーをコピーして、サードパーティアプリケーションで使用できるようにする必要があります。
- 証明書ユーザー：API キーに加え、アプリケーションの登録には、証明書ユーザーとの関連付けが必要です。証明書ユーザーに関連付けられた証明書は、SPP からも信頼されている認証局によって署名されている必要があります。

> **メモ：** この証明書の発行とサードパーティ製アプリケーションへのインストールには、企業の PKI を使用してください。

アプリケーション – アプリケーションサービスはデフォルトで無効になっており、資格情報の取得やアクセスリクエストのブローカー機能を実行する前に有効にしておく必要があります。

Web クライアントを使用する場合

1. **［セキュリティポリシー管理］＞［アプリケーション – アプリケーション］**に移動します。
2. サービスの**［有効］**列で、トグルを右側に移動させてサービスを有効化します。

API を使用する場合

次の URL を使用します：

https://appliance/service/appliance/v3/A2AService/Enable

また、この同じクライアントページを使用するか、以下の URL を使用して、サービスの現在の状態を確認することができます：

https://appliance/service/appliance/v3/A2AService/Status

11.3.2 アプリケーション - アプリケーションのセットアップ

SPP でアプリケーション間統合を使用するには、次のタスクを実行する必要があります：

1. SSP と統合するサードパーティ製アプリケーションを準備します。
2. アプライアンス管理者が SPP でアプリケーション – アプリケーションサービスを有効にします。以下のいずれかの方法を使用します：

- **［セキュリティポリシー管理］＞［アプリケーション－アプリケーション］**に移動し、**［有効］**列のトグルを右側に移動させてサービスを有効に切り替えます。
- 次の URL を使用します：
  https://appliance/service/appliance/v3/A2AService/Enable

3. 資産管理者は、資産とアカウントを SPP に追加します。詳細については、「資産の追加」および「アカウントの追加」を参照してください。
4. ユーザー管理者は、証明書ユーザーを SPP に追加します。詳細については、「ユーザーの追加」を参照してください。
5. セキュリティポリシー管理者は、アプリケーション登録を SPP に追加します。詳細については、「アプリケーション登録の追加」を参照してください。
6. サードパーティアプリケーションから要求を行うために、API キーを取得し、サードパーティアプリケーションにコピー/貼り付けます。詳細については、「アプリケーション－アプリケーションサービスを使用したリクエストの作成」を参照してください。

11.3.3 アプリケーション登録の追加

サードパーティ製アプリケーションに「アプリケーション－アプリケーション」サービスで提供されるタスクのいずれかを実行させるには、サードパーティアプリケーションを SPP に登録する必要があります。

前提条件

- ユーザー管理者は、証明書ユーザーを SPP に追加します。
- 資産管理者は、資産とアカウントを SPP に追加します。

アプリケーション登録の追加手順

1. セキュリティポリシー管理者として SPP Web クライアントにログインします。
2. **［セキュリティポリシー管理］＞［アプリケーション－アプリケーション］**に移動します。
3. ＋**［追加］**をクリックします。**［新しい登録］**ダイアログが表示されます。
4. 次の情報を指定します：
   a. **名前**：アプリケーション登録の名前を入力します。

b. **説明**：アプリケーション登録に関する情報を入力します。

c. **証明書ユーザー**：**［参照］**をクリックして、登録するサードパーティアプリケーションに関連付けられた証明書ユーザーを選択します。

証明書ユーザーは必ず指定する必要があります。アプリケーション登録を最初に追加したときに指定されていない場合は、**［アプリケーション –アプリケーション］**ページで**［編集］**をクリックして、証明書ユーザーを指定します。

> **メモ**：SignIR の場合、Retrievable Accounts の A2A 登録が割り当てられている監視したい Retrievable Accounts の A2A API キーを使用して、証明書ユーザーとして接続します。接続された証明書ユーザーは、そのアカウントに関連するすべてのイベント（たとえば、パスワードの変更、更新、削除）のイベント通知を受け取ります。詳細については、「アプリケーション – アプリケーションサービスを使用したリクエストの作成」を参照してください。

d. **証明書ユーザーに表示**：このチェックボックスを選択すると、A2A 登録用に構成された証明書ユーザーによって API キーを含む登録が可視化されます。

5. **［OK］**をクリックします。これにより、最初のアプリケーション登録情報が保存され、追加の設定を行う新しいダイアログが開きます。

6. **［アクセスリクエストブローカー］**タブには、サードパーティアプリケーションが代理でアクセスリクエストを作成できるユーザーのリストが表示されます。

   - ＋をクリックして、ユーザーまたはユーザーグループをリストに追加します。
   - **［制限の編集］**をクリックすると、リスト内のすべてのユーザーとユーザーグループに対して IP アドレスの制限を指定できます。

     制限は、このタスクを実行するために「アプリケーション – アプリケーション」サービスの呼び出しを許可する IP アドレスまたは IP アドレスの範囲のリストです。つまり、制限が資格情報検索またはアクセスリクエストブローカータスクに追加されると、サービスは制限リストで指定された IP アドレスから開始される要求のみを許可します。

     IP アドレスの表記は以下の通りです：

     - IPv4 または IPv6 アドレス（例：10.5.32.4）
     - CIDR 表記のアドレス範囲（例：10.5.0.0/16）
   - － をクリックすると、選択したユーザーをリストから削除します。

7. **［資格情報取得］**タブには、サードパーティが通常のワークフロープロセスを経ずに SPP から資格情報を取得することができるリストが表示されます。

   - ＋をクリックすると、リストにアカウントが追加されます。

- 制限列の**［制限］**をクリックして、選択したアカウントの IP アドレスの制限を指定します。

  制限とは、このタスクを実行するために「アプリケーション – アプリケーション」サービスを呼び出すことを許可する IP アドレスまたは IP アドレスの範囲のリストです。つまり、資格情報取得またはアクセスリクエストブローカータスクに制限が追加されると、サービスは制限リストで指定された IP アドレスから開始するリクエストのみを許可するようになります。

  IP アドレスの表記は以下の通り：

  - IPv4 または IPv6 アドレス（例：10.5.32.4）
  - CIDR 表記のアドレス範囲（例：10.5.0.0/16）
- 選択したアカウントをリストから削除するには、ー をクリックします。

8. **［OK］**をクリックしてダイアログを閉じます。

アプリケーションの登録が SPP に追加されると、サードパーティのアプリケーションは、生成された API キーと登録に関連付けられた証明書を使用して SPP で認証することができます。リクエストを行うには、認可されたアカウントを使用してアプリケーションの関連する API キーを取得し（つまり、Bearer トークン認証を使用し）、リクエストを行うホストに正しい証明書をインストールする必要があります。詳細については、「アプリケーション – アプリケーションサービスを使用したリクエストの作成」を参照してください。

11.3.4 アプリケーション登録の削除

SPP から構成済みのアプリケーション登録を削除することができます。

アプリケーション登録の削除手順

1. **［セキュリティポリシー管理］＞［アプリケーションからアプリケーション］**に移動します。
2. 削除するアプリケーション登録を選択します。
3. 🗑ツールバーボタンをクリックします。
4. リクエストを確認します。

11.3.5 API キーの再生成

セキュリティポリシー管理者として、API キーが盗まれたり紛失したりしたことが判明した場合、いつでも API キーを再生成することができます。API キーを再生成すると、古い API キーが無効になり、そのキーを使用してアプリケーション – アプリケーションサービスにアクセスするサービスができなくなります。

API キーの再生成手順

1. セキュリティポリシー管理者として SPP Web クライアントにログインします。
2. **［セキュリティポリシー管理］＞［アプリケーション – アプリケーション］**に移動します。
3. リストからアプリケーション登録を選択し、**［編集］**をクリックします。
4. **［アクセスリクエストブローカー］**タブで、**［再生成］**をクリックします。

これで、新しい API キーを表示またはクリップボードにコピーして、この新しい API キーをサードパーティアプリケーションで使用して、アプリケーション – アプリケーションインターフェイスにアクセスすることができます。「アプリケーション – アプリケーションサービスを使用したリクエストの作成」を参照してください。

11.3.6 アプリケーション – アプリケーションサービスを使用したリクエストの作成

アプリケーション – アプリケーションサービスを使用すると、サードパーティのアプリケーションは以下の方法で SPP と対話することができます。

- 資格情報の取得：サードパーティアプリケーションは、対象資産に対して自動化された機能を実行するために、SPP の保管庫から資格情報を取得することができます。また、プロシージャ、スクリプト、その他のプログラム内のハードコードされたパスワードをプログラム呼び出しに置き換えることができます。
- アクセスリクエストブローカー：サードパーティのアプリケーションは、許可されたユーザーに代わってアクセスリクエストを開始し、許可されたユーザーが利用可能なリクエストを通知され、SPP にログインしてパスワードを取得したりセッションを開始したりできるようにすることができます。

サードパーティのアプリケーションは、SPP の API リクエストの認証に通常使用される Bearer トークンではなく、API キーとクライアント証明書を使用して SPP を認証します。リクエストを行うには、まず、認可されたユーザーアカウントを使用して SPP からアプリケーションの API キーを取得（つまり、Bearer トークン認証を使用）し、リクエストを行うホストに正しい証明書をインストールする必要があります。この証明書は、リクエストを行う認可された証明書ユーザーの証明書ストアにインストールされている必要があります。

前提条件

- サードパーティ製アプリケーションを SPP に登録します。詳細については、「アプリケーション登録の追加」を参照してください。
- サードパーティアプリケーションを既存の SPP 証明書ユーザーと関連付けます。

サードパーティアプリケーションから証明書取得リクエストを行う手順

1. アプリケーションの関連する API キーを SPP から取得します。API キーは、次の方法で取得することができます。

   Web クライアントを使用する場合：

   - セキュリティポリシー管理者として SPP のクライアントにログインします。
   - **［セキュリティポリシー管理］＞［アプリケーション - アプリケーション］**に移動します。
   - アプリケーションを選択し、**［編集］**をクリックします。
   - **［資格情報取得］**タブで をクリックします。

   SPP API を使用する場合：

   - 以下の URL を使用して、SPP API から登録されたアプリケーションの詳細を取得します。レスポンスの ID プロパティは、関連する API キーを取得するために使用されます。レスポンスの Certificate Thumbprint プロパティは、アプリケーションがリクエストの認証に使用する必要のある証明書を特定します。

     ```
     https://<Appliance IP>/service/core/V3/A2ARegistrations?filter=AppName%20eq%20%22<ApplicationName>%22
     ```

   - アプリケーション登録で取得した応答内の ID プロパティを使用して、SPP API から選択したアカウントの API キーを取得します。

```
https://<Appliance
IP>/service/core/V3/A2ARegistrations/<Id>/RetrievableAccounts?filter=Acc
ountName%20eq%20%22<account
name>%22%20and%20SystemName%20eq%20%22<system
name>%22&fields=ApiKey
```

2. アプリケーションに登録されている CertificateUserThumbprint に一致する証明書が、リクエストを行うホスト上にインストールされていることを確認します。

3. 選択した証明書が、SPP によって信頼されていることを確認します。つまり、SPP に信頼されたルート証明書をインストールします。

4. 取得した API キーと証明書のサムプリントで認証して、アプリケーションリクエストを作成します。

    - リクエストの Authorization ヘッダーを A2A <API key>に設定します。
    - タイプは Password または PrivateKey です。秘密鍵は、サービスアカウントに対してのみ取得できることに注意してください。
    - 証明書は、呼び出し方法に応じて、リクエストに添えて提示します。例えば、Invoke-WebRequest コマンドレットを使用する場合、オプションを使用します。

      -CertificateThumbprint <thumbprint>

      資格情報を取得するためには、以下のリクエストを使用します。

      ```
      GET https://<ApplianceIP>/service/A2A/V3/Credentials?type=Password
      Host: <ApplianceIP>
      Content-Type: application/json
      Accept: text/plain
      Authorization A2A <API Key>
      ```

      この URL は文字列のレスポンスを返します。

サードパーティアプリケーションからアクセスリクエストブローカーリクエストを行う手順

1. SPP からアプリケーションの関連する API キーを取得します。API キーは、次の方法で取得することができます。

   Web クライアントを使用する場合：

    - セキュリティポリシー管理者として SPP のクライアントにログインします。
    - **［セキュリティポリシー管理］＞［アプリケーション - アプリケーション］**に移動します。

- アプリケーションを選択し、 **［編集］**をクリックします。
- **［アクセスリクエストブローカー］**タブで、 をクリックします。

SPP API を使用する場合：

- 次の URL を使用して、SPP API から登録されたアプリケーションの詳細を取得します。レスポンスの Id プロパティは、関連する API キーを取得するために使用されます。レスポンスの Certificate Thumbprint プロパティは、アプリケーションがリクエストの認証に使用する必要のある証明書を特定します。

```
https://<Appliance IP>/service/core/V3/A2ARegistrations?filter=AppName%20eq%20%22<ApplicationName>%22
```

- アプリケーション登録のために取得した ID を使用して、Safeguard API から API キーを取得します。

```
https://<Appliance IP>/service/core/V3/A2ARegistrations/<Id>/AccessRequestBroker/ApiKey
```

2. アプリケーションの登録済み CertificateUserThumbprint に一致する証明書が、リクエストを行うホストにインストールされていることを確認します。

3. 選択した証明書が、SPP によって信頼されていることを確認します。つまり、SPP に信頼されたルート証明書をインストールします。

4. 取得した API キーと証明書のサムプリントで認証を行い、アプリケーションリクエストを作成します。

- リクエストの Authorization ヘッダーに A2A <API key>を設定する。
- 呼び出し方法に応じて、証明書をリクエストに添えて提示する。たとえば、Invoke-WebRequest コマンドレットを使用する場合、オプションを使用します。

  -CertificateThumbprint <thumbprint>
- アクセスリクエストを作成するには、以下のような要求を使用します:

```
POST
Host: <Appliance IP>
Accept            application/json
Content-type      application/json
Authorization         A2A <API key>
{
    "ForUser": "<user name>",
```

```
    "ForUserId": <user id>,
    "ForProvider": “<providername>”,
"SystemId": <system id>,
    "SystemName": "<system name>",
    "AccountId": <account id>,
    "AccountName": "<account name>",
    "AccessRequestType": "<request type>",
“RequestedDurationDays”: <days>
    "RequestedDurationHours": <hours>,
“RequestedDurationMinutes”: <minutes>,
“RequestedFor”: “<date>,
    "ReasonCodeId": <reason code id>,
    "ReasonCode": "<reason name>",
    "ReasonComment": "<reason comment>",
“IsEmergency”: <bool>,
“TicketNumber”: “<ticket>”

}
```

この URL は、成功した場合、新しいリクエストを返します。

例外事項

このアクセスリクエストのフィールドのほとんどは、ここに記した例外を除いて、通常のアクセスリクエストのフィールドと一致しています。

以下のフィールドは、リクエストを作成するために使用されるターゲット SPP ユーザーを識別するために使用されます。検索結果は、アプリケーションがアクセスリクエストを作成する権限を付与された有効な SPP ユーザーを一意に識別する必要があります。検索結果が複数一致する場合、または一致しない場合は、エラーが返されます。

- ForUserId：SPP ユーザーのデータベース ID。値が含まれている場合は、これが優先されます。
- ForUser: SPP ユーザーの名前です。ForUserId に値が含まれている場合、この値は無視されます。
- ForProvider： ForUser の検索を制限するために使用できるオプションのプロバイダ名

以下のフィールドは、対象システムを一意に識別するために使用されます。検索結果が複数一致する場合、または一致しない場合は、エラーが返されます。

- SystemId：SPP 資産のデータベース ID。このフィールドは、次の順序で一致する資産を検索するために使用されます。
  - システム名：システム名の完全一致
  - ネットワークアドレス：ネットワークアドレスの完全一致
  - 文字列検索：資産のすべての文字列プロパティを対象とした文字列検索

以下のフィールドは、対象アカウントを一意に識別するために使用されます。検索結果が複数一致する場合、または一致しない場合は、エラーが返されます。

- AccountId： SPP アカウントのデータベース ID。値が含まれている場合は、これが優先されます。
- AccountName： AccountId に値が含まれている場合、これは無視されます。このフィールドは、次の順序で一致するアカウントを検索するために使用されます。
  - アカウント名：アカウント名の完全一致
  - 文字列検索：アカウントのすべての文字列プロパティに対する文字列検索

以下のフィールドを使用して、理由コードを特定することができます。検索結果が複数一致する場合、あるいは一致しない場合、理由コードは null に設定されます。

- ReasonCodeId：定義済みの理由コードのデータベース ID。値を含む場合、これが優先されます。
- ReasonCode：定義済み理由コードの名前。ReasonCodeId が値を含む場合、これは無視されます。

アクセスリクエストの作成

対象ユーザーとアカウントが決定されると、アプリケーション – アプリケーションサービスはアクセスリクエストの作成を試行します。試行が成功するかどうかは、通常のポリシールールで決定されます。

11.4 Cloud Assistant

Cloud Assistant 機能は、アクセスリクエストのワークフローを Starling Cloud Assistant と統合し、アクセスリクエストが送信されると、承認者は設定されたチャネルを通じて通知を受けることができます。承認者は、SPP の Web アプリケーションにアクセスすることなく、チャネルを通じてアクセスリクエストを承認（または拒否）することができます。

Cloud Assistant 機能は、SPP を Starling に参加させると有効になります。詳細については、「Starling」を参照してください。有効化されたら、Cloud Assistant を使用してアクセスリクエストを承認する権限を持つユーザーを定義するのは、セキュリティポリシー管理者の責任になります。

Cloud Assistant へのアクセス

［セキュリティポリシー管理］＞［Cloud Assistant］に移動します。

［Cloud Assistant］ペインには、この機能の使用を許可されたユーザーについて、次のように表示されます。

表：Cloud Assistant プロパティ

設定	説明
名前	SPP ユーザーの名前 **メモ：**このユーザーは、アクセスリクエストポリシーの承認者としても追加される必要があります。
ユーザー名	アカウントに関連付けられたユーザー名
認証プロバイダ	認証プロバイダの種類
ID プロバイダ	アカウントの認証プロバイダの名前
ドメイン名	アカウントが置かれているドメイン名
メールアドレス	認証ユーザの有効なメールアドレス

次のツールバーボタンを使用して Cloud Assistant を使用するユーザー認証を管理します。

表：Cloud Assistant：ツールバー

オプション	説明
＋追加	この機能を使用してアクセスリクエストを承認（または拒否）することが許可されている SPP ユーザーを追加します。 **メモ：**このユーザーは、アクセスリクエストポリシーの承認者としても追加される必要があります。
ー 削除	選択したユーザーを正規のユーザーとして削除します。
更新	Cloud Assistant の使用が許可されているユーザーのリストを更新します。

11.4.1 Cloud Assistant の承認ユーザーの追加

SPP が Starling に参加したら、Cloud Assistant ページを使用して、Cloud Assistant 機能を使用してアクセスリクエストを承認できる SPP ユーザーを追加してください。

Cloud Assistant の使用を許可されたユーザーの追加手順

> **重要**： SPP で設定されたユーザー情報は、Starling Cloud Assistant チャンネルのユーザー情報と一致する必要があります。ユーザー情報が一致しない場合、**［セキュリティポリシー管理］＞［Cloud Assistant］と［Starling Cloud Assistant］**の［Recipients］ページの両方からユーザーを削除し、正しいユーザー情報を使用して SPP にユーザーを再追加する必要があります。

1. SPP クライアントにセキュリティポリシー管理者としてログインします。
2. **［セキュリティポリシー管理］＞［Cloud Assistant］**に移動します。
3. **［追加］**をクリックします。
4. **［ユーザー］**ダイアログで、リストからユーザーを選択し、**［OK］**をクリックします。
5. これらの Cloud Assistant ユーザーを、適切なアクセスリクエストポリシーの承認者として追加します。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

ユーザーが Cloud Assistant ユーザーとして、またアクセスリクエストポリシーの承認者として追加されると、アクセスリクエストが承認を必要とする場合、SPP は承認者の設定されたチャンネル（これは Starling Cloud Assistant サービスを通じて設定されます）に通知を送信します。承認者は、チャネルから直接アクセスリクエストを承認または拒否することができます。

> **メモ：**すでに承認されているアクセスリクエストを取り消すことは、チャネルではできません。そのアクションを実行するには、SPP Web クライアントを使用する必要があります。

11.5 資産グループ

SPP の資産グループは、アクセスリクエストポリシーのスコープに追加できる資産のセットです。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

資産グループと動的資産グループに追加できるのは、セッション管理をサポートする資産のみです。セッション管理をサポートしない資産には、ディレクトリ資産が含まれますが、これに限定されるわけではありません。資産を作成すると、セッションがサポートされている場合、**［管理］**タブに**［セッションリクエストの有効化］**チェックボックスが表示されます。詳細については、「サポート対象のプラットフォーム」を参照してください。このセクションでは、プラットフォームごとの SPP および SPS のサポートを示します。

監査人とセキュリティポリシー管理者には、資産グループにアクセスする権限があります。

資産グループへのアクセス

［セキュリティポリシー管理］＞［資産グループ］に移動します。

資産グループビューには選択した資産グループに関する次の情報が表示されます：

- プロパティタブ：選択した資産グループに関する全般情報が表示されます。動的グループの場合は、このタブに資産ルールの情報も表示されます。
- 資産タブ：選択した資産グループに関連付けられている資産が表示されます。
- アクセスリクエストポリシータブ：選択した資産グループに関連付けられている資格とアクセスリクエストポリシーが表示されます。
- 履歴タブ：選択した資産グループに影響を与えた各操作の詳細が表示されます。

これらのツールバーボタンを使用して、資産グループを管理します。

- **＋［新しい資産グループ］＞［資産グループ］**：SPP に資産グループを追加します。詳細については、「資産グループの追加」を参照してください。

- **［新しい資産グループ］＞［資産の動的グループ］**：SPP に動的資産グループを追加します。詳細については、「動的資産グループの追加」を参照してください。
- **［削除］**：選択した資産グループを SPP から削除します。詳細については、「資産グループの削除」を参照してください。
- **［詳細の表示］**：選択した資産グループの情報と構成オプションが表示されます。
- **［エクスポート］：**リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
- **［更新］**：資産グループのリストを更新します。
- **［検索］**：入力した条件を使用して、文字列または選択した属性で検索できます。選択した属性で検索するには、**［検索］**をクリックして、検索する属性を選択します。詳細については、「検索ボックス」を参照してください。

11.5.1 プロパティタブ

プロパティタブには、選択した資産グループに関する情報が表示されます。

プロパティへのアクセス

［セキュリティポリシー管理］＞［資産グループ］＞（詳細の表示）**＞［プロパティ］**

表：資産グループ：プロパティタブ：全般プロパティ

プロパティ	説明
名前	選択した資産グループの名前
説明	選択した資産グループに関する情報
資産ルール	動的資産グループの場合、定義された資産ルールの概要。この情報は**［資産ルール］**タブで利用可能です。

11.5.2 資産タブ

資産タブには、選択した資産グループに関連付けられている資産が表示されます。

資産へのアクセス

［セキュリティポリシー管理］＞［資産グループ］＞（詳細の表示）**＞［資産］**

詳細ツールバーの **＋［資産の追加］**をクリックすると、選択した資産グループに 1 つ以上の資産を追加することができます。

［検索］：詳細については、「検索ボックス」を参照してください。

表：資産グループ：資産タブのプロパティ

プロパティ	説明
名前	管理対象システムに割り当てられた資産名
プラットフォーム	管理対象システムのプラットフォーム
セッションリクエスト	この列のチェックは、資産に対してセッションアクセスリクエストが有効になっていることを示します。
無効	この列のチェックは、その資産が管理されていないこと、無効であること、および関連するアカウントがないことを示します。
説明	資産に関する情報

表：資産グループ：資産タブツールバー

オプション	説明
＋資産の追加	選択した資産グループに、1 つまたは複数の資産を追加します。
ー 削除	選択した資産を削除します。
エクスポート	このボタンを使って、リストされたデータを JSON または CSV ファイルとしてエクスポートします。詳しくは、「データのエクスポート」を参照してください。
更新	資産リストを更新します。
検索	このリストから特定の資産を見つけるには、一致するものを検索するために使用する文字列を入力します。詳しくは、「検索ボックス」を参照してください。

11.5.3　アクセスリクエストポリシータブ

アクセスリクエストポリシータブには、選択した資産グループに関連付けられている資格とアクセスリクエストポリシーが表示されます。

アクセスリクエストポリシーへのアクセス

［セキュリティポリシー管理］＞［資産グループ］＞（詳細の表示）**＞［アクセスリクエストポリシー］**

表：資産グループ：アクセスリクエストポリシータブのプロパティ

プロパティ	説明
資格	アクセスリクエストポリシーの資格の名前
アクセスリクエストポリシー	選択した資産グループの資産を管理するポリシーの名前
資産グループ数	アクセスリクエストポリシー内の一意の資産グループの数
資産数	アクセスリクエストポリシーに関連付けられている資産グループ内の一意の資産の数

次の詳細ツールバーボタンを使用して、選択した資産グループに関連付けられたアクセスリクエストポリシーを管理します。

表：資産グループ：アクセスリクエストポリシータブのツールバー

オプション	説明
＋ 追加	選択した資産グループをアクセスリクエストポリシーのスコープに追加します。
－ 削除	選択したポリシーを削除します。詳細については、「アクセスリクエストポリシーの削除」を参照してください。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	アクセスリクエストポリシーのリストを更新します。
検索	このリストで特定のポリシーまたはポリシーのセットを見つけるには、一致するものの検索に使用する文字列を入力しま

オプション	説明
	す。詳細については、「検索ボックス」を参照してください。

11.5.4 履歴タブ

履歴タブでは、選択した資産グループに影響を与えた各操作の詳細を表示またはエクスポートすることができます。

履歴へのアクセス

［セキュリティポリシー管理］＞［資産グループ］＞ （詳細の表示）**＞［履歴］**

履歴タブの上部には、次の情報が含まれています。

- **日付範囲：**デフォルトでは、履歴の詳細は過去 24 時間分表示されます。ドロップダウンから、時間間隔を一つ選択すると、その時間枠の履歴の詳細が表示されます。
- **エクスポート**：データを.csv ファイルにエクスポートします。
- **更新**：表示されているリストを更新します。
- **検索**：詳細については、「検索ボックス」を参照してください。

表：資産グループ：履歴タブのプロパティ

プロパティ	説明
日付/時間	イベントの日時
ユーザー	イベントを発生させたユーザーの表示名
ソース IP	イベントを発生させた管理対象システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択した資産グループの名前
イベント	選択したアカウントグループに対して行われた操作のタイプ： • 作成 • 削除 • 更新

プロパティ	説明
	• メンバーシップの追加 • メンバーシップの削除 **メモ：** メンバーシップ操作とは、選択した資産グループがポリシーのメンバーシップに追加または削除された、または資産が選択した資産グループのメンバーシップに追加または削除されたなど、関連オブジェクトまたは親オブジェクトとの「関係」の変更を示します。
関連オブジェクト	関連オブジェクトの名前
関連オブジェクトタイプ	関連オブジェクトのタイプ
親	選択した資産グループが子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

11.5.5 資産グループの管理

SPP の資産グループを管理するために、資産グループビューのコントロールとタブページを使用して、次のタスクを実行します。

- 資産グループの追加
- 動的資産グループの追加
- 資産グループに資産を追加
- 資産グループの削除

資産グループの追加

SPP に資産グループを追加するのは、セキュリティポリシー管理者の責任です。

SPP に新しい資産グループを追加するには、**[資産グループ]** ビューを使用します。

資産グループと動的資産グループに追加できるのは、セッション管理をサポートする資産のみです。セッション管理をサポートしない資産には、ディレクトリ資産が含まれますが、これに限定されるわけではありません。資産を作成すると、セッションがサポートされている場合、**[管**

理］タブに［**セッションリクエストの有効化**］チェックボックスが表示されます。詳細については、「サポート対象のプラットフォーム」を参照してください。このセクションでは、プラットフォームごとの SPP および SPS のサポートを示します。

資産グループの追加手順

1. ［**セキュリティポリシー管理**］>［**資産グループ**］に移動します。
2. ＋［**新しい資産グループ**］をクリックします。
3. ドロップダウンリストから＋［**資産グループ**］をクリックします。
4. ［**新しい資産グループ**］ダイアログで、次の情報を入力します：
    a. ［**名前**］：資産グループの一意の名前を 50 文字以内で入力します。
    b. ［**説明**］：（任意）この資産グループに関する説明を 255 文字で入力します。
5. ［**OK**］をクリックします。

動的資産グループの追加

SPP に資産グループを追加するのは、セキュリティポリシー管理者の責任です。

資産グループと動的資産グループに追加できるのは、セッション管理をサポートする資産のみです。セッション管理をサポートしない資産には、ディレクトリ資産が含まれますが、これに限定されるわけではありません。資産の作成時に、セッションがサポートされている場合は、［**管理**］タブに［**セッションリクエストの有効化**］チェックボックスが表示されます。詳細については、「サポート対象のプラットフォーム」を参照してください。このセクションでは、プラットフォームごとの SPP および SPS のサポートを示します。

動的資産グループの追加手順

1. ［**セキュリティポリシー管理**］>［**資産グループ**］を開きます。
2. ツールバーから＋［**新しい資産グループ**］>［**資産の動的グループ**］をクリックします。
3. ［**新しい資産グループ**］ダイアログのそれぞれのタブで情報を入力します。

場所	説明
全般タブ	動的資産グループの一般的な情報を追加する場所

場所	説明
資産ルールタブ	動的資産グループに含まれる資産を特定するために使用するルールを定義する場所

全般タブ（動的資産グループの追加）

［新しい資産グループ］ダイアログの**［全般］**タブで、動的資産グループに関する一般情報を入力します。

表：動的資産グループ：全般タブ

プロパティ	説明
名前	動的資産グループの一意の名前を 50 文字以内で入力します。
説明	動的資産グループに関する情報を 255 文字以内で入力します。

資産ルールタブ（動的資産グループの追加）

［新しい資産グループ］ダイアログの**［資産ルール］**タブにあるルールエディターコントロールを使用して、動的資産グループに含める資産を定義します。

表：動的資産グループ：資産ルールタブ

プロパティ	説明
および｜または	**［および］**をクリックすると、複数の検索条件をグループ化することができます。すべての条件を満たす必要があります。 **［または］**をクリックすると、複数の検索条件をグループ化することができ、少なくとも 1 つの条件を満たす必要があります。
属性	最初のクエリ句ボックスで、検索する属性を選択します。有効な属性は次のとおりです。 • **名前**（デフォルト） • **説明**

プロパティ	説明
	• **プラットフォーム** • **無効** • **タグ** • **検出ジョブ名** • **パーティション名** • **プロファイル名** • **ネットワークアドレス** • **検出されたグループ名**（検索でドメインを指定しない場合はこの選択を使用します。ドメインを指定する場合は、**[検出されたグループの識別名]**を選択します。） • **検出されたグループの識別名**（検索対象をグループの所属するドメインに指定する場合は、この選択を使用します。） • **ディレクトリコンテナ**（演算子**[等しい]**を使用すると、1 つのレベルが検索されます。）
演算子	中央の句のクエリボックスで、検索に使用する演算子を選択します。使用できる演算子は、選択した属性のデータ型によって異なります。 文字列属性の場合、演算子には次のものが含まれます。 • 次を含む（デフォルト） • 次を含まない • 次で開始 • 次で終了 • 等しい • 等しくない ブール属性の場合、演算子には次のものが含まれます。 • 真である • 偽である
検索文字列	最後の句のクエリボックスに、一致するものを見つけるために使用する検索文字列または値を入力します。
+ | −	検索句の左側の + をクリックすると、検索条件を追加することができます。 − をクリックすると、検索条件から検索句が削除されます。

プロパティ	説明
グループ化の追加 | 削除	**［グループ化の追加］**ボタンをクリックし、満たすべき条件を追加します。 新しいグループがグループ内の最後のクエリ句の下に追加され、上位のクエリ条件の下位にあることを示す枠付きペインに表示されます。 **［削除］**ボタンをクリックすると、検索条件からグループを削除することができます。
Preview	**［Preview］**をクリックすると、クエリを実行し、動的グループを追加する前にクエリの結果を確認することができます。

資産グループに資産を追加

資産グループビューの**［資産］**タブから、1 つ以上の資産を資産グループに追加することができます。

資産グループに資産を追加する手順

1. **［セキュリティポリシー管理］>［資産グループ］**を開きます。
2. リストから資産グループを選択し、**［詳細の表示］**をクリックします。
3. **［資産］**タブを開きます。
4. **［資産の追加］**をクリックします。
5. **［グループに追加する資産を選択してください］**ダイアログのリストから 1 つ以上の資産を選択します。

   > **メモ：**プラットフォームがセッション管理に対応している資産のみ利用できます。

   > **メモ：**探している資産が見つからない場合、管理者のアクセス許可権限によっては、［新しい資産］ダイアログ（［新規しい資産］ボタン）で作成することができます。（資産を作成するには、資産管理者の権限が必要です。）資産を作成するには、資産管理者の権限が必要です。

6. **［資産の選択］**をクリックして選択を保存します。

資産グループの削除

資産グループを削除することができます。資産グループを削除しても、SPP は関連する資産を削除しません。

資産グループの削除手順

1. **［セキュリティポリシー管理］>［資産グループ］**を開きます。
2. **［資産グループ］**でリストから資産グループを選択します。
3. **［削除］**をクリックします。
4. リクエストを確認します。

11.6 資格

SPP の資格とは、システムアクセスを許可されたユーザーに制限するアクセスリクエストポリシーのセットです。一般的に、様々な職務のために資格を作成します。つまり、ヘルプデスク管理者、Unix 管理者、Oracle 管理者のような特定のロール（役割）に特定の操作を実行する権限を割り当てます。パスワードリリースの資格は、ユーザー、ユーザーグループ、アクセスリクエストポリシーで構成されます。セッションアクセスリクエストの権限は、ユーザー、ユーザーグループ、資産、資産グループ、アクセスリクエストポリシーで構成されます。

監査人とセキュリティポリシー管理者は、資格にアクセスする権限を持っています。管理者は、資格を作成し、資格に関連する 1 つまたは複数のアクセスリクエストポリシーを作成し、最後にユーザーまたはユーザーグループを追加します。

資格へのアクセス

［セキュリティポリシー管理］>［資格］を選択します。

無効または期限切れのポリシーが 1 つ以上ある場合、警告と「資格に無効なポリシーが 1 つ以上含まれています」というメッセージが表示されます。**［アクセスリクエストポリシー］**タブを開き、無効なポリシーを確認します。詳細については、「アクセスリクエストポリシータブ」を参照してください。

選択した資格について、次の情報が表示されます：

- **［全般］**タブ：選択した資格に関する一般および時間制限の設定情報が表示されます。

- **［ユーザー］**タブ：選択した資格のポリシー範囲内でアカウントまたは資産へのアクセスをリクエストする権限を持つユーザーグループまたはユーザーが表示されます。SPS リンク中に作成され、SPS アプライアンスによって割り当てられ使用されている場合、証明書ユーザーが表示に含まれます。リンク中に作成された証明書ユーザーは**［ユーザー］**タブに追加できますが、デフォルトでは追加されていません。
- **［アクセスリクエストポリシー］**タブ：セッションアクセスポリシーを含め、選択した資格内のアカウントまたは資産を管理するアクセスリクエストポリシーが表示されます。
- **［履歴］**タブ：選択した資格に影響を与えた各操作の詳細が表示されます。

これらのツールバーボタンを使用して、資格を管理します。

- **［新しい資格］**：資格を SPP に追加します。詳細については、「資格の追加」を参照してください。
- **［削除］**：選択した資格を削除します。詳細については、「資格の削除」を参照してください。
- **［編集］**：選択した資格の追加情報とオプションが表示されます。
- **［選択した行から新しい資格を作成］**：選択した資格が複製されます。
- **［エクスポート］**：リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
- **［更新］**：エンタイトルリストを更新します。
- **［検索］**：文字列、または選択した属性で条件を入力して検索することができます。選択した属性で検索するには、**［検索］**をクリックし、検索する属性を選択します。詳細については、「検索ボックス」を参照してください。

11.6.1 全般タブ

全般タブへのアクセス

［セキュリティポリシー管理］＞［資格］＞（詳細の表示）**＞［全般］**

［全般］タブには、選択した資格に関する情報が表示されます。

- **名前**：資格の名前
- **説明**：選択された資格についての情報

- **優先度**：他の資格との関連で資格の処理順序を決定する一意の番号。詳細については、「SPP は、ユーザーがアクセスリクエストを送信する際に、どのようにポリシーを評価するのか」を参照してください。
- **日時に基づく資格の失効：**有効期限を設定するには、このオプションを選択し、日付と時刻を入力します。資格が期限切れになると、その資格に関連するすべてのアクセスリクエストポリシーも期限切れになります。ポリシーに有効期限を設定するには、「アクセスリクエストポリシーの作成」を参照してください。
- **時間ウィンドウを使用：**このオプションを選択すると、時間枠が強制されます。選択してドラッグすると、許可する時間帯がハイライト表示されます。色のついたタイルはブロックされる時間帯です。色がついていないタイルは使用可能な時間帯です。

11.6.2 ユーザータブ

［ユーザー］タブには、選択した資格のポリシーのスコープ内にあるアカウントおよび資産に対してアクセスをリクエストする権限を持つユーザーおよびユーザーグループが表示されます。SPS リンク中に作成されたユーザーが SPS アプライアンスによって割り当てられ使用されている場合、証明書ユーザーも表示に含まれます。リンク中に作成された証明書ユーザーは、**［ユーザー］**タブに追加できますが、デフォルトでは追加されません。

ユーザータブへのアクセス

［セキュリティポリシー管理］>**［資格］**> （詳細の表示）>**［ユーザー］**に移動します。

詳細ツールバーの **［ユーザーの追加］**または**［ユーザーグループの追加］**をクリックして、1人または複数のリクエストユーザーまたはユーザーグループを選択した資格に追加します。

表：資格：ユーザータブプロパティ

プロパティ	説明
タイプ	メンバーの種類： • グループ • ユーザー
表示名	選択した資格に含まれるユーザーまたはユーザーグループの表示名
ユーザー名	選択された資格に含まれるユーザーまたはユーザーグループの名前
プロバイダ	認証プロバイダの名前： • Local

プロパティ	説明
	• Certificate • Microsoft Active Directory ドメイン名のような外部プロバイダの名前

選択した資格に関連するリクエストユーザーを管理するために、詳細ツールバー上の以下のボタンを使用します。

表：資格：ユーザータブツールバー

オプション	説明
＋ユーザーまたはユーザーグループの追加	リクエストユーザーグループまたはリクエストユーザーを資格に追加します。詳細については、「ユーザーまたはユーザーグループを資格に追加」を参照してください。
ー 削除	選択したユーザーまたはユーザーグループを資格から削除します。
エクスポート	このボタンを使用して、リストされたデータを JSON または CSV ファイルのいずれかとしてエクスポートします。詳細は、「データのエクスポート」を参照してください。
検索（大文字小文字区別あり）	この一覧から特定のユーザー（またはユーザーグループ）、またはユーザー（またはユーザーグループ）の集合を探すには、検索に使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

11.6.3 アクセスリクエストポリシータブ

アクセスリクエストポリシータブには、選択した資格内のアカウントを管理するパスワードと SSH キーのリクエストポリシーが表示されます。

アクセスリクエストポリシーへのアクセス

［セキュリティポリシー管理］＞［資格］＞（編集）**＞［アクセスリクエストポリシー］**

> **重要**: **［資格］＞［アクセスリクエストポリシー］**タブで行われた選択は、**［アプライアンス管理］＞［クラスタ］＞［管理対象ネットワーク］**ページの選択より優先されます。**［管理対象ネットワーク］**ルールに異なる SPS クラスタのノードが含まれている場合、SPP は**［アクセ**

スリクエストポリシー］タブの［**セッション設定**］ページで割り当てられた同じクラスタのノードのみを選択します。

詳細ツールバーから ＋［**新しいアクセスポリシー**］をクリックし、選択した資格にポリシーを追加します。

次の詳細ツールバーボタンを使用して、アクセスリクエストポリシーを管理します。

表：資格：アクセスリクエストポリシータブのプロパティ

オプション	説明
＋新しいアクセスポリシー	選択した資格にアクセスリクエストポリシーを追加します。詳細については、「アクセスリクエストポリシーの作成」を参照してください。
削除	選択されたポリシーを選択された資格から削除します。詳細については、「アクセスリクエストポリシーの削除」を参照してください。
編集	選択したポリシーを変更します。詳細については、「アクセスリクエストポリシーの変更」を参照してください。
アクセスポリシーのコピー	選択したポリシーのコピーを作成します。詳細については、「アクセスリクエストポリシーのコピー」を参照してください。
他の資格からアクセスポリシーをインポート	別の資格で設定されたアクセスポリシーをインポートします。
エクスポート	このボタンを使用して、リストされたデータを JSON または CSV ファイルのいずれかとしてエクスポートします。詳細については、「データのエクスポート」を参照してください。
検索（大文字小文字区別あり）	このリストから特定のポリシーまたはポリシーのセットを見つけるには、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

11.6.4 履歴タブ

履歴タブでは、選択した資格に影響を与えた各操作の詳細を表示またはエクスポートすることができます。

履歴へのアクセス

［セキュリティポリシー管理］> ［資格］> ［編集］**> ［履歴］**

- **日付範囲：**デフォルトでは、履歴の詳細は過去 24 時間分表示されます。ドロップダウンから、時間間隔を一つ選択すると、その時間枠の履歴の詳細が表示されます。
- **エクスポート**：データを JSON または CSV ファイルにエクスポートします。
- **更新**：表示されているリストを更新します。
- **検索**：詳細については、「検索ボックス」を参照してください。

表：資格：履歴タブのプロパティ

プロパティ	説明
日付/時間	イベントの日時
ユーザー	イベントを発生させたユーザーの表示名
ソース IP	イベントを発生させた管理対象システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択した資産グループの名前
イベント	選択したアカウントグループに対して行われた操作のタイプ： • 作成 • 削除 • 更新 • メンバーシップの追加 • メンバーシップの削除 **メモ：** メンバーシップ操作とは、選択した資産グループがポリシーのメンバーシップに追加または削除された、または資産が選択した資産グループのメンバーシップに追加または削除されたなど、関連オブジェクトまたは親オブジェクトとの「関係」の変更を示します。

プロパティ	説明
関連オブジェクト	関連オブジェクトの名前
関連オブジェクトタイプ	関連オブジェクトのタイプ
親	選択した資産グループが子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

11.6.5 資格の管理

資格ページのコントロールとタブページを使用して、SPP の資格を管理するための以下のタスクを実行します。

- 資格の追加
- ユーザーまたはユーザーグループを資格に追加
- アクセスリクエストポリシーの作成
- アクセスリクエストポリシーの削除
- アクセスリクエストポリシーの変更
- アクセスリクエストポリシーのコピー
- 資格の削除

資格の追加

SPP に資格を追加するのは、セキュリティポリシー管理者の責任です。

資格の追加手順

1. **［セキュリティポリシー管理］＞［資格］**に移動します。
2. ツールバーから ＋ **［新しい資格］**をクリックします。
3. **［新しい資格］**ダイアログで、全般タブに情報を入力します。
    - **名前**：資格に固有の名前を 50 文字以内で入力します。

- **説明**：資格に関する説明を 255 文字以内で入力します。
- **優先度**：他の資格と比較したこの資格の優先度を入力します。

  ユーザーが 2 つの異なる資格のスコープ内でアカウントにアクセスすることを望む場合、最も高い優先度（つまり、最も低い数字）を持つ資格が優先されます。詳細については、「SPP は、ユーザーがアクセスリクエストを送信する際に、どのようにポリシーを評価するのか」を参照してください。
- **日時に基づく資格の失効**：このオプションを選択して有効期限を強制し、日付と時刻を入力します。

  資格が期限切れになると、その資格に関連するすべてのアクセスリクエストポリシーも期限切れになります。ポリシーに有効期限を設定するには、「アクセスリクエストポリシーの作成」を参照してください。

  > **メモ：**資格の時間制限は、SPP がポリシーを使用するときに実施されます。ポリシーの時間制限は、ユーザーがアカウントのパスワードにアクセスできるタイミングを強制します。資格とポリシーの両方に時間制限がある場合、ユーザーは重複する時間枠のパスワードのみをチェックアウトすることができます。
  >
  > 時間制限は、ユーザーのタイムゾーンに関連して、資格またはポリシーがいつ有効であるかを制御します。SPP アプライアンスは協定世界時（UTC）で動作しますが、ユーザーのタイムゾーンは資格またはポリシーで設定された時間制限を強制的に実行します。つまり、アプライアンスとユーザーが異なるタイムゾーンにいる場合、SPP は、アカウントプロファイルで設定されたユーザーのタイムゾーンでポリシーを適用します。
  >
  > ユーザーは、デフォルトでタイムゾーンを変更することができます。または、ユーザー管理者は、ポリシーの遵守を確実にするために、ユーザーがタイムゾーンを変更することを禁止することができます。詳しくは、「タイムゾーン」を参照してください。
- **タイムウィンドウを使用**：このオプションを選択すると、タイムウィンドウが適用されます。
  選択してドラッグし、許可する時間をハイライト表示します。色のついたタイルはブロックされる時間帯です。色のついていないタイルは使用可能な時間帯です。

4. 以下のいずれかを選択します：
   - **保存して閉じる：**資格を保存し、資格ページに戻ります。
   - **保存して実行**：資格を保存し、［アクセスリクエストポリシー］タブを開きます。これらの設定は、資格を編集するために選択した時にも利用できます。

SPP は、ユーザーがアクセスリクエストを送信する際に、どのようにポリシーを評価するのか

資格とは、どのユーザーが、そのアカウントのポリシーのスコープ内で、アカウントのパスワードをチェックアウトする権限を持つかを定義するものです。ポリシーは、範囲（つまり、どのアカウント）と、期間、何回承認が必要か、などのパスワードをチェックアウトするためのルールを定義します。

1 つのアカウントは複数の資格で制御したり、資格内の複数のポリシーのスコープ内においたりすることができます。アクセスを許可するリクエストがどのポリシーで制御されているかを評価するとき、SPP はまず、リクエストが緊急アクセスかどうかを判断し、緊急アクセスを許可するポリシーのみに対して評価します。次に、リクエストが行われる時間を考慮し、さらに、時間制限を持つポリシーのうち、リクエストを許可するものだけに照らして評価します。最後に、残りのポリシーの間に矛盾がある場合、優先度を使用して、どのポリシーがリクエストに適用されるべきかを決定します。

サンプルシナリオ：

- 資格 A（優先度 1）
    - ポリシー：平日ポリシー
        - ポリシーの時間制限：月曜日から金曜日の 8:00 から 17:00
        - スコープ： アカウント X
- 資格 B（優先度 2）
    - ポリシー1：日曜午前（優先度 1）
        - ポリシーの時間制限： 日曜日 8:00～12:00
        - スコープ： アカウント X
    - ポリシー2：日曜午後（優先度 2）
        - ポリシーの時間制限: 日曜日 13:00 から 17:00
        - スコープ: アカウント X

アカウント X は、これら 3 つのポリシーのすべてのスコープにあることに注意してください。

ユーザーが日曜日の 16:00 にアカウント X のパスワードをリクエストした場合、SPP は優先度 1 であるため、まず資格 A を検討します。ポリシーの時間制限によりパスワードのリリースができないと判断し、次に資格 B を検討します。

SPP は、まず、資格 B の優先度 1 のポリシーを検討します。時間的制限によりパスワードのリリースができないと判断し、次にポリシー2 を検討します。リリースが満たされると、SPP はリクエストを許可します。

しかし、もし資格 B のポリシー1 の時間が 08:00 から 17:00 であれば、ポリシー1 の方が、優先度が高いため優先されます。そして、もし権限 B のポリシー2 が緊急アクセスを許可するように設定されていて、リクエストに緊急アクセスがあった場合、ポリシー1（より高い優先度 1 を持っていますが）は選択から除外され、ポリシー2 が再び優先されます。

アクセスリクエストポリシーの作成

SPP でアクセスリクエストポリシーを定義するのは、セキュリティポリシー管理者の責任です。

ポリシーは、以下を定義します：

- スコープ（資産、資産グループ、アカウント、またはアカウント グループ）
- アクセスタイプ：
    - 資格情報アクセスタイプ：
        - パスワードリリース
        - SSSH キー
    - セッションアクセスタイプ：
        - RDP（リモートデスクトッププロトコル）
        - RDP アプリケーション
        - SSH（Secure SHell）
        - Telnet
- パスワードのチェックアウトに関するルール（期間、必要な承認回数など）

考慮事項

- アクセスリクエストポリシーは、1 つのクラスタにのみ割り当てられます。
- アクセスリクエストポリシーは、それが作成された資格でのみ使用されます。資格を削除すると、その資格に関連するすべてのアクセスリクエストポリシーが削除されます。

アクセスリクエストポリシーを資格に追加する手順

1. **［セキュリティポリシー管理］＞［資格］**に移動します。

2. リストから資格を選択して**［編集］**を選択し、**［アクセスリクエストポリシー］**タブを開きます。

3. 詳細ツールバーから ＋ **［新しいアクセスポリシー］**をクリックします。

4. **［アクセスリクエストポリシーの作成］**ダイアログで、各タブに情報を入力します。

タブ	説明
全般タブ	アクセスリクエストポリシーに関する一般的な情報を追加し、リクエストされるアクセスの種類を指定します。
セキュリティタブ	ユーザーがそれぞれのリンクされたアカウントからパスワードをリクエストすることを許可するなど、選択したリクエストのタイプのアクセス設定を定義します。
スコープタブ	アクセスリクエストポリシーに、資産、資産グループ、アカウント、アカウントグループを割り当てます。
ワークフロータブ	アクセスリクエストポリシーの要求者、承認者、レビュー担当者の設定を行います。

全般タブ

全般タブで、アクセスリクエストポリシーの次の情報を入力します。

全般タブへのアクセス

［セキュリティ管理］＞［資格］＞［アクセスリクエストポリシー］（ポリシーの作成または編集）に移動します。

表：アクセスリクエストポリシー：全般タブプロパティ

プロパティ	説明
名前	アクセスリクエストポリシーの一意の名前を 50 文字以内で入力 k します。
説明	アクセスリクエストポリシーを説明するテキストを 255 文字以内で入力します。
優先度	このポリシーの優先度は、この資格内の他のポリシーと比較されます。

プロパティ	説明
	1 つの資格内で 2 つの異なるリクエストポリシーのスコープ内でユーザーがアカウントにアクセスすることを希望する場合、最も高い優先度（つまり、最も小さい番号）を持つポリシーが優先されます。詳細については、「SPP は、ユーザーがアクセスリクエストを送信する際に、どのようにポリシーを評価するのか」を参照してください。
リクエストポリシータイプの選択	リクエストポリシーのタイプを指定します： • 資格情報 ◦ パスワード ◦ SSH キー • セッション ◦ RDP（リモートデスクトッププロトコル） ◦ RDP アプリケーション ◦ SSH(Secure SHell) ◦ Telnet
資格情報タイプの選択	リクエストポリシーのタイプを指定します： • パスワード • SSH キー **メモ**：パスワードリリースのためのアクセスリクエストポリシーを設定できますが、SPP モジュールのライセンスがインストールされていない場合、パスワードリリースリクエストを送信することはできません。 同様に、セッションリクエスト用のアクセスリクエストポリシーも設定できます。
日時に基づいて失効するアクセスポリシーがあります	該当する場合、このチェックボックスを選択してポリシーの有効期限を強制します。有効期限の日付と時間を入力します。
時間ウィンドウを使用	このオプションを選択すると、時間ウィンドウが強制されます。選択してドラッグし、許可する時間をハイライト表示します。色のついたタイルは、ブロックされる時間帯です。色のついていないタイルは使用可能な時間帯です。

セキュリティタブ

セキュリティタブでは、**[全般]**タブで指定されたアクセスタイプに基づいて、リクエストされたアクセスタイプのアクセス設定を行うことができます。

セキュリティタブへのアクセス：

[セキュリティ管理] > **[資格]** > **[アクセスリクエストポリシー]**（ポリシーの作成または編集）に移動します。

表：アクセスリクエストポリシー：セキュリティタブのプロパティ

プロパティ	説明
セッションリクエストにパスワードリリースを含める	**アクセスタイプ**が RDP、SSH、Telnet の場合、このチェックボックスを選択すると、セッションのアクセスリクエスト時にパスワードリリースが含まれます。
セッションリクエストに SSH キーリクエストを含める	**アクセスタイプ**が RDP、SSH、Telnet の場合、このチェックボックスを選択すると、セッションのアクセスリクエストに SSH キーのリリースを含めることができます。
失効したセッションを閉じる	**アクセスタイプ**が RDP、SSH、Telnet の場合、このチェックボックスを選択すると、期限切れのセッションを閉じることができます。
チェックイン後にパスワードを変更	ユーザーがチェックインし直した後にパスワードを変更する場合は、このチェックボックスをオンにします。デフォルトでは、このチェックボックスが選択されています。
チェックイン後に SSH キーを変更	ユーザーがチェックインし直した後に SSH キーを変更する場合は、このチェックボックスを選択します。デフォルトでは、このチェックボックスが選択されています。
SSH キーのパスフレーズの保護	**アクセスタイプ**が SSH Key の場合、SSH Key のパスフレーズを要求する場合は、このチェックボックスを選択します。
同時アクセスを許可	このポリシーで管理されるアカウントと資産への複数のユーザーのアクセスを許可する場合は、このチェックボックスを選択します。次のチェックボックスを使用して、一度にアクセスできるユーザーの数を確認します。

プロパティ	説明
最大同時ユーザー数	**［同時アクセスを許可］**オプションが選択されている場合、一度にアクセスをリクエストできるユーザーの最大数を入力します。
資産ベースのセッションアクセス	**アクセスタイプ**が RDP、SSH、Telnet の場合、次のオプションのいずれかを選択して、セッションがリクエストされたときにポリシースコープで定義されたアカウントに加えて、ポリシースコープで定義された資産のいずれかにアクセスするために使用するアカウント資格情報の種類を定義します。 • なし (既定)：なし (既定): セッションが要求されたときに、認証情報が保管庫から取得されます。 • ユーザー指定：ユーザー提供： セッションが要求されたときに、要求元のユーザーが資格情報を提供する必要があります。 • リンクアカウント：要求元ユーザーのアカウントは、セッションが要求されたときに使用されるディレクトリアカウントにリンクされています。 ◦ リンクアカウントのスコープフィルタリングの有効化：選択すると、この設定により、リクエスト可能なアカウントの数を、ポリシースコープにも定義されているリンクされたアカウントに制限することができます。 **メモ**： ポリシースコープに資産/資産グループのみが含まれ、アカウントが含まれない場合、スコープフィルタリング設定は効果がなく、ポリシーは各スコープ付きポリシー資産上のすべてのリンクされたディレクトリアカウントで使用できます。 • ディレクトリアカウント：**［参照］**を使用して、セッションがリクエストされたときに使用される 1 つ以上のディレクトリアカウントを選択します。 ディレクトリアカウントが SPP バージョン 2.7 より前のバージョンから移行された場合、ディレクトリアカ

プロパティ	説明
	ウントの識別子が空白になることがあります。これは、以前の SPP バージョンでは 1 つの割り当てのみを理解し、バージョン 2.7 では複数の割り当てが発生するためです。
リンクアカウントへのパスワードアクセスを許可	**アクセスタイプ**がパスワードリリースの場合、このチェックボックスを選択すると、ユーザーはそれぞれのリンク先アカウントのパスワードをリクエストすることができるようになります。各ユーザーのリンク先アカウントへのアクセスは、このポリシーで定義された他の設定によって管理されます。 さらに、**［リンクアカウントのスコープフィルタリングの有効化］**を選択すると、リクエスト可能なアカウントの数を、同じくスコープに定義されているリンクされたアカウントに制限することができます。
SPS 接続ポリシー	このドロップダウンを使用して、アクセスリクエストポリシーで使用する SPS 接続ポリシーを選択します。
RDP ホスト資産	アクセスタイプが RDP アプリケーションの場合、このフィールドに関連する**［参照］**ボタンを使用して、Windows アプリケーションサーバーと接続するように構成された資産を選択します。
ホストアカウントを必須とする	**アクセスタイプ**が RDP アプリケーションの場合、このチェックボックスを選択し、**［参照］**をクリックして、使用するホストアカウントを探します。選択を解除すると、セッションの初期化時に情報の入力を求められます。
アプリケーションの表示名	**アクセスタイプ**が RDP アプリケーションの場合、これはリモートアプリケーションが Windows アプリケーションサーバーで公開されたときに提供されたアプリケーションの表示名です。
アプリケーションのエイリアス	**アクセスタイプ**が RDP アプリケーションの場合、これは Windows アプリケーションサーバーでリモートアプリケーションを公開するときに定義されたエイリアス名です。エイリアス名の前にある 2 本の縦棒を含め、完全なエイリアスパスが使用されていることを確認してください（例：||OISGRemoteAppLauncher）。

プロパティ	説明
代替ログイン名を使用	このチェックボックスを選択すると、アカウントの代替ログイン名が使用されます。

スコープタブ

アクセスリクエストポリシーにアカウント、アカウントグループ、資産、資産グループを割り当てるには、**［スコープ］**タブを使用します。

［セキュリティポリシー管理］＞［資格］＞［アクセスリクエストポリシー］＞（ポリシーの作成または編集）に移動します。

1. **［スコープ］**タブで：
    a. 詳細ツールバーの ＋ **［このポリシーにスコープ項目を追加］**をクリックし、次のオプションのいずれかを選択します：
        - **このポリシーにアカウントを追加**
        - **このポリシーにアカウントグループを追加**
        - **このポリシーに資産を追加**
        - **このポリシーに資産グループを追加**

    b. 選択ダイアログで選択し、**［OK］**をクリックします。

    探している選択が表示されない場合、管理者の権限に応じて、ダイアログで作成することができます。(アカウントと資産を作成するには、資産管理者の権限が必要です。アカウントグループと資産グループを作成するには、セキュリティポリシー管理者の権限が必要です)。

2. 追加の選択を行うには、手順 1 を繰り返します。ポリシーに複数の種類のオブジェクトを追加することができますが、アカウントやアカウントグループなどのオブジェクトは一度に 1 種類しか追加できません。

選択されたすべてのオブジェクトは、アクセスリクエストポリシーダイアログの**［スコープ］**タブに表示されます。リストからオブジェクトを削除するには、オブジェクトを選択し、**［削除］**をクリックします。

ワークフロータブ

ワークフロータブは 3 つのタブに分かれており、アクセスリクエストポリシーの要求者、承認者、レビュー担当者の設定を行うことができます。

ワークフローへのアクセス

［セキュリティポリシー管理］＞［資格］＞［アクセスリクエストポリシー］＞ (ポリシーの作成または編集)

要求者タブ

［要求者］タブを使用してアクセスリクエストポリシーの要求者設定を構成します。

表：アクセスリクエストポリシー：要求者タブのプロパティ

プロパティ	説明
アクセス承認の期間	要求者がこのポリシーで管理されるアカウントと資産にアクセスできるデフォルトの期間（日、時間、分）を入力または選択します。アクセス期間は、合計で 31 日（44,640 分）を超えることはできません。
要求者に期間の変更を許可	このチェックボックスをオンにすると、要求者はアクセス期間を変更することができます。
要求者がアクセスできる最長時間	**［要求者に期間の変更を許可］**オプションを選択すると、要求者がこのポリシーで管理されるアカウントと資産にアクセスできる最大期間（日、時間、分）を設定できます。 デフォルトのアクセス期間は 7 日間です。最大アクセス期間は 31 日です。 ユーザーはアクセス期間を変更できますが、最大アクセス期間より長い時間、このポリシーによって管理されるアカウントまたは資産にアクセスすることはできません。

プロパティ	説明
緊急アクセスを許可	このオプションは、このポリシーによって管理されるアカウントと資産への緊急アクセスをユーザーがリクエストすることを許可する場合に選択します。**緊急アクセス**を許可しない場合は、このオプションをオフにします。 つまり、ユーザーが**緊急アクセス**を使用してアクセスをリクエストした場合、要求者設定などの他の制約が満たされていれば、その要求は直ちに承認されます。複数のユーザーが、同じアカウントまたは資産に対して同時に緊急アクセスを要求することができます。
時間制限を無視	ユーザーが緊急アクセスをリクエストしたときに、時間制限を無視するには、このオプションを選択します。このポリシーに設定された時間制限を適用し、指定された時間帯にのみ緊急アクセスを許可する場合は、このオプションをオフにします。
緊急アクセスでアカウントがリリースされたときに通知	（任意）緊急アクセスが有効な場合、メール アドレスを入力するか、[宛先] を選択して SPP ユーザーのメール アドレスを選択し、エスカレーション通知連絡先リストを作成します。 SPP 以外のユーザーのメール アドレスを入力することもできます。 ユーザーにイベント通知を送信するには、SPP がアラートを送信するように設定する必要があります。詳細については、「アラートの構成」を参照してください。 **重要**: SPP は、エスカレーション通知連絡先リストのメールアドレスを動的に維持しません。ポリシー作成後に SPP ユーザーのメールアドレスを変更したり、SPP ユーザーを削除したりする場合は、エスカレーション通知連絡先リストのメールアドレスを手動で更新する必要があります。詳細については、「ユーザーに通知されない」を参照してください。
コメントを必須とする	このチェックボックスを選択すると、アクセスリクエスト時に要求者がコメントを提供することを要求できます。

プロパティ	説明
理由	＋［追加］をクリックして、選択したアクセスリクエストポリシーに 1 つまたは複数の理由を追加すると、パスワード、SSH キー、セッションへのアクセスをリクエストするときに、ユーザーはリストから定義済みの理由を選択できるようになります。［OK］をクリックして、理由を追加します。 **メモ：**このオプションを使用するには、SPP で理由が構成されている必要があります。詳細については、「理由」を参照してください。探している理由が見つからない場合は、ツールバーの＋［新規］ボタンをクリックして、理由ダイアログから理由を作成することができます。
理由コードを必須とする	アクセスリクエストの際に、要求者に理由を要求する場合は、このチェックボックスをオンにします。このオプションは、ポリシーで［理由］を選択した場合のみ使用できます。ポリシーに理由を追加し、このオプションをクリアしたままにすると、ユーザーは理由を選択することができます。 ユーザーは理由を選択することができますが、理由の選択は要求されません。

承認者タブ

承認者タブで、アクセスリクエストポリシーの承認者設定を設定します。

表：アクセスリクエストポリシー：承認者タブのプロパティ

プロパティ	説明
自動承認済み	このオプションは、このポリシーによって管理されるアカウントと資産に対するすべてのアクセスリクエストを自動的に承認するために選択します。
アカウントが自動承認されたときに通知	（任意）承認が不要な場合、メールアドレスを入力するか、［宛先］を選択して、アクセスが自動承認されたときに通知するユーザーを選択します。 ［宛先］ボタンを使用して SPP ユーザーを追加した場合、このリストから個々のアドレスを削除するには ✖［クリア］ア

プロパティ	説明
	イコンを使用してこのリストから個々のアドレスを削除することができます。 **メモ:** ユーザーにイベント通知を送信するには、SPP がアラートを送信するように設定する必要があります。詳細については、「アラートの構成」を参照してください。
必要な承認数	このポリシーが適用されるアカウントと資産についてのすべてのアクセスリクエストに対して、承認を要求します。以下の情報を入力します： • **Qty**： **［承認者］**としてリストされている選択されたユーザーまたはユーザーグループから必要な最小の承認数を入力または選択します。 • **承認者**： **［参照］**し、このポリシーが適用されるアカウントと資産へのアクセスリクエストを承認できる 1 人以上のユーザーまたはユーザーグループを、選択します。 承認者セットを追加または削除するには、**［承認者グループの追加］**または**［削除］**をクリックします。 承認者セットの順番は重要ではありませんが、すべての要件を満たす必要があります。つまり、リクエストは定義された各承認者セットから必要な数の承認を得る必要があります。 承認者として承認したユーザーは、SPP がアラートを送信するように構成されている場合、アクセスリクエストが承認を必要とするときにアラートを受け取ります。 **ヒント**: ベストプラクティスは、個人ではなくユーザーグループを承認者として追加することです。これにより、保留中のアクセスリクエストに個人の承認者を追加することができます。また、ポリシーを編集することなく承認者リストを変更することができます。
承認者に保留中の承認がある場合、次の期間が経過したら通知	（任意）通知を有効にするには、このチェックボックスを選択します。

プロパティ	説明
	• 保留中の承認についてエスカレーション通知の連絡先リストに通知するまでの時間（日、時間、分）を設定します。 • メールアドレスを入力するか、**［宛先］**を選択して、SPP ユーザーのメールアドレスを選択します。SPP 以外のユーザーのメールアドレスを入力することもできます。 **重要**:SPP は、エスカレーション通知連絡先リストのメールアドレスを動的にメンテナンスしません。ポリシーの作成後に SPP ユーザーのメールアドレスを変更したり、SPP ユーザーを削除したりする場合は、エスカレーション通知連絡先リストのメールアドレスを手動で更新する必要があります。詳細については、「ユーザーに通知されない」を参照してください。 **注:** ユーザーにイベント通知を送信するには、SPP でアラートを送信するように設定する必要があります。詳細については、「アラートの構成」を参照してください。
Cloud Assistant が有効になりました。有効なユーザーを表示します。	SPP が Starling に参加し、Cloud Assistant で承認者として登録されていることを示します。［ユーザー］リンクをクリックすると、この機能を使用してリクエストを承認する権限を持つユーザーのリストが表示されます。 Cloud Assistant Users ダイアログの**［追加］**ツールバーボタンをクリックすると、Cloud Assistantの承認者としてユーザーを追加することができます。

レビュー担当者タブ

レビュー担当者タブで、アクセスリクエストポリシーのレビュー担当者設定を定義します。

表：アクセスリクエストポリシー：レビュー担当者タブプロパティ

プロパティ	説明
レビューを必須としない	このチェックボックスはデフォルトで選択されており、このポリシーが適用されるアカウントと資産に対する完了したアクセスリクエストに対して、レビューが必要ないことを示します。
レビューを必須とする	このチェックボックスを選択すると、このポリシーが適用されるアカウントと資産に対する完了したアクセスリクエストのレビューが要求されます。 • **Qty**: 完了したアクセスリクエストのレビューに必要な最小人数を入力または選択します。 • **レビュー担当者**： **［参照］**し、このポリシーが適用されるアカウントと資産に対するアクセスリクエストをレビューできる 1 人以上のユーザーまたはユーザーグループを選択します。 レビュー担当者は、アクセスリクエストが完了した後にのみレビューを行うことができます。 レビュー担当者として承認したユーザーは、SPP がアラートを送信するように設定されている場合、アクセスリクエストにレビューが必要なときにアラートを受け取ります。 **ヒント:** ベストプラクティスは、個人ではなくユーザーグループをレビュー担当者として追加することです。これにより、保留中のアクセスリクエストに個人のレビュー担当者を追加することが可能になります。また、ポリシーを編集することなく、レビュー担当者リストを変更することができます。
コメントを必須とする	アクセスリクエストのレビュー時にレビュー担当者によるコメントの入力が必要な場合は、このチェックボックスを選択します。
レビューを保留中にしてもアクセスはブロックされません	事前のリクエストが承認されたかどうかにかかわらず、新しいアクセスリクエストを許可する場合、このチェックボックスを選択します。つまり、事前のリクエストの承認状況によって、リクエストがブロックされることはありません。

プロパティ	説明
レビュー担当者に保留中のレビューがある場合、次の期間が経過したら通知	（任意）通知を有効にするには、このチェックボックスを選択します。 • エスカレーション通知の連絡先リストに保留中のレビューについてリマインドするまでの時間（日、時間、分）を設定します。 • メールアドレスを入力するか、**［宛先］**を選択して SPP ユーザーのメールアドレスを選択します。 SPP 以外のユーザーのメールアドレスを入力することもできます。 ユーザーにイベント通知を送信するには、アラートを送信するように SPP を構成する必要があります。詳細については、「アラートの構成」を参照してください。 **重要：** SPP は、エスカレーション通知連絡先リストのメールアドレスを動的にメンテナンスしません。ポリシーの作成後に SPP ユーザーのメールアドレスを変更したり、SPP ユーザーを削除したりする場合は、エスカレーション通知連絡先リストのメールアドレスを手動で更新する必要があります。詳細については、「ユーザーに通知されない」を参照してください。

ユーザーまたはユーザーグループを資格に追加

資格にユーザーを追加すると、選択した資格のアクセスリクエストポリシーによって管理されるアカウントのパスワードをリクエストできる人、または選択した資格のアクセスリクエストポリシーによって管理されるアカウントおよび資産のセッションをリクエストできる人が指定されます。ユーザーは、セッションアプライアンスの証明書ユーザーとなることができます。詳細については、「SPS リンクのあるセッションアプライアンス」を参照してください。

資格にユーザーを追加するのは、セキュリティポリシー管理者の責任です。セキュリティポリシー管理者には、グループを追加する権限のみがあり、ユーザーを追加する権限はありません。詳細については、「管理者のアクセス許可」を参照してください。

要求者ユーザーを資格に追加する手順

1. **［セキュリティポリシー管理］＞［資格］**に移動します。
2. リストから資格を選択し、**［編集］**をクリックします。
3. **［ユーザー］**タブをクリックします。
4. 詳細ツールバーから ＋ **［ユーザーの追加］**または**［ユーザーグループの追加］**をクリックします。
5. **［ユーザー/ユーザーグループ］**ダイアログのリストから 1 人または複数のユーザーまたはユーザーグループを選択し、**［OK］**をクリックします。

アクセスリクエストポリシーの削除

> **重要:** ポリシーを削除すると、SPP はポリシーを永久に削除しますが、ポリシーによって管理されるアカウントは削除されません。

資格からアクセスリクエストポリシーを削除する手順

1. **［セキュリティポリシー管理］＞［資格］**に移動します。
2. リストから資格を選択し、**［編集］**をクリックします。
3. **［アクセスリクエストポリシー］**タブを選択します。
4. ポリシーを選択します。
5. 🗑 **［削除］**をクリックします。
6. 確認ダイアログで内容を確認し、**［はい］**を選択します。

アクセスリクエストポリシーの変更

アクセスリクエストポリシーは、移行することができます。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

アクセスリクエストポリシーの変更手順

1. **［セキュリティポリシー管理］＞［資格］**に移動します。
2. リストから資格を選択し、**［編集］**をクリックします。
3. **［アクセスリクエストポリシー］**タブを選択します。
4. ポリシーをダブルクリックするか、ポリシーを選択して**［編集］**をクリックします。
5. 変更したいポリシー情報のタブを選択します。

アクセスリクエストポリシーのコピー

ポリシーをコピーして別の資格に追加することはできません。ポリシーは資格に固有です。

アクセスリクエストポリシーのコピー手順

1. **［セキュリティポリシー管理］＞［資格］**の順に選択します。
2. リストから資格を選択し、**［編集］**をクリックします。
3. **［アクセスリクエストポリシー］**タブを選択します。
4. ポリシーを選択し、**［選択した行から新しいアクセスポリシーを作成］**をクリックします。
5. 必要に応じて、新しいポリシーの設定を編集します。

資格の削除

> **重要:** 資格を削除すると、SPP はその資格に関連するすべてのアクセスリクエストポリシーを削除します。

資格の削除手順

1. **［セキュリティポリシー管理］＞［資格］**の順に選択します。
2. リストから資格を選択します。

3. **［削除］**をクリックします。

4. 確認ダイアログで**「削除」**と入力します。

5. **［削除］**をクリックします。

11.7 リンクアカウント

リンクアカウントページに、ディレクトリアカウントとそれに関連付けられたユーザーに関する情報が表示されます。

リンクアカウントへのアクセスする方法

［セキュリティポリシー管理］＞［リンクアカウント］

リンクアカウントページは、2 つのタブに分かれています：

- ユーザー（リンクアカウント）
- アカウント(リンクアカウント)：このページでは、リンクアカウントが一覧表示されます。

11.7.1 ユーザー（リンクアカウント）

リンクアカウントページの**［ユーザー］**タブに、リンクアカウントに関連付けられたユーザーに関する情報が表示されます。

リンクアカウントページの［ユーザー］タブへのアクセス方法

［セキュリティポリシー管理］＞［リンクアカウント］の順に選択すると、デフォルトで**［ユーザー］**タブが表示されます。

ツールバー

次のツールバーボタンを使用して、ユーザーを管理します。

- **編集**：ユーザーを選択してこのボタンをクリックすると、ユーザーへのアカウントのリンクなど、追加の情報とオプションが表示されます。
- **更新：**ユーザーのリストを更新します。

- **検索：**文字列または選択した属性で、条件を入力して検索することができます。選択した属性で検索するには、「検索」をクリックして、検索する属性を選択します。詳しくは、「検索ボックス」をご覧ください。

11.7.2 アカウント(リンクアカウント)

リンクアカウントページの**［アカウント］**タブには、現在ユーザーにリンクされているアカウントの情報が表示されます。

リンクアカウントページの［アカウント］タブへのアクセス

［セキュリティポリシー管理］＞［リンクアカウント］の順に選択し、**［アカウント］**タブを開きます。

ツールバー

次のツールバーボタンを使用して、アカウントを管理します。

- **編集**：アカウントを選択してこのボタンをクリックすると、ユーザーとアカウントのリンクなど、追加の情報とオプションが表示されます。
- **更新：**アカウントのリストを更新します。
- **検索：**文字列または選択した属性で、条件を入力して検索することができます。選択した属性で検索するには、「検索」をクリックして、検索する属性を選択します。詳しくは、「検索ボックス」をご覧ください。

11.7.3 リンクアカウントの管理

リンクアカウントを管理するには、**リンクアカウント**ページのコントロールとタブページを使用します。

- ユーザーをアカウントにリンクさせる
- アカウントとユーザーの関連付け
- ユーザーからのリンクアカウント削除
- リンクアカウントからのユーザーの削除

ユーザーをアカウントにリンクさせる

ユーザーをアカウントにリンクさせることができるのは、セキュリティポリシー管理者です。リンクアカウントは、アクセスリクエストポリシーのスコープ内で、資産やアカウントにアクセスするために使用されます。

ユーザーをアカウントにリンクさせる手順

1. **［セキュリティポリシー管理］＞［リンクアカウント］**の順に選択します。
2. **［ユーザー］**タブで、リストからユーザーを選択し、**［編集］**をクリックします。
3. 詳細ツールバーから **［追加］**をクリックします。

   ［ディレクトリアカウントの選択］ダイアログが表示され、SPP で利用可能なディレクトリアカウントが一覧表示されます。
4. **［ディレクトリアカウントの選択］**ダイアログのリストから 1 つまたは複数のアカウントを選択し、**［OK］**をクリックします。

アカウントとユーザーの関連付け

アカウントをユーザーにリンクさせることができるのは、セキュリティポリシー管理者です。リンクアカウントは、アクセスリクエストポリシーのスコープ内で資産やアカウントにアクセスするために使用されます。

アカウントをユーザーにリンクする手順

1. **［セキュリティポリシー管理］＞［リンクアカウント］**の順に選択します。
2. **［アカウント］**タブを選択し、リストからアカウントを選択して **［編集］**をクリックします。
3. 詳細ツールバーから **［追加］**をクリックします。

   ［ユーザー］ダイアログが表示され、SPP で利用可能なユーザーが一覧表示されます。
4. **［ユーザー］**ダイアログのリストから 1 人または複数のユーザーを選択し、**［OK］**をクリックします。

ユーザーからのリンクアカウント削除

ユーザーからリンクアカウントを削除することができるのは、セキュリティポリシー管理者です。

ユーザーからリンクされたアカウント削除する手順

1. **［セキュリティポリシー管理］＞［リンクアカウント］**の順に選択します。
2. **［ユーザー］**タブで、リストからユーザーを選択し **［編集］**をクリックします。
3. リストからリンクアカウント（または複数のアカウント）を選択します。
4. 詳細ツールバーの**［削除］**をクリックします。
5. 確認するダイアログで、**［はい］**をクリックします。

リンクアカウントからのユーザーの削除

セキュリティポリシー管理者は、リンクアカウントからユーザーを削除することができます。

リンクアカウントからユーザーを削除する手順

1. **［セキュリティポリシー管理］＞［リンクアカウント］**の順に移動します。
2. **［アカウント］**タブで、リストからアカウントを選択し、**［編集］**をクリックします。
3. リストからユーザー（または複数のユーザー）を選択します。
4. 詳細ツールバーの**［削除］**をクリックします。
5. 確認ダイアログで、**［はい］**をクリックします。

11.8 ユーザーグループ

メモ：ユーザーグループページには以下の場所からアクセスできます：

- **［セキュリティポリシー管理］＞［ユーザーグループ］**

- **［ユーザー管理］＞［ユーザーグループ］**

SPP では、SPP 内にのみ存在し管理されるローカルユーザーグループを作成するか、外部の Active Directory または LDAP サーバーから同期されるディレクトリグループを追加することができます。セキュリティポリシー管理者は、資格に 1 つ以上のユーザーグループを追加することができ、資格のアクセスリクエストポリシーによって制御されるアカウントと資産へのアクセスをリクエストするグループのメンバーを認可することができます。

ユーザーグループは、権限許可者管理者、ユーザー管理者、セキュリティポリシー管理者、ヘルプデスク管理者、監査人、資産管理者が利用できます。ただし、すべてのユーザータイプですべての機能が利用できるわけではありません。

ユーザーグループビューには、選択したユーザーまたはディレクトリグループに関する次の情報が表示されます。

- プロパティタブ：選択したユーザーグループに関する全般的な情報が表示されます。
- ユーザータブ：選択したグループのメンバーが表示されます。
- 資格タブ：選択したユーザーグループに割り当てられている資格が表示されます。グループのすべてのメンバーは、その資格のリクエストポリシーにへのアクセスを継承します。

  メモ：［資格］タイルは、監査人とセキュリティポリシー管理者にのみ表示されます。

- 履歴：選択したグループに影響を与えた各操作の詳細が表示されます。

次のツールバーボタンを使用して、ユーザーを管理します。

- **＋ ユーザーグループ**：SPP にユーザーグループを追加します。詳細については、「ユーザーグループの追加」を参照してください。
- **＋ ディレクトリユーザーグループ**：ディレクトリユーザーグループを SPP に追加します。詳細については、「ディレクトリユーザーグループの追加」を参照してください。
- **削除**：選択したユーザーグループを削除します。詳細については、「ユーザーグループの削除」を参照してください。
- **編集：**選択したユーザーグループを編集します。
- **エクスポート**：リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートする場合に使用します。詳しくは、「データのエクスポート」を参照してください。
- **更新**：ユーザーグループのリストを更新します。
- **検索**：文字列または入力した条件で選択した属性で検索できます。選択した属性で検索するには、**［検索］**をクリックして、検索する属性を選択します。詳細については、「検索ボックス」を参照してください。

11.8.1 プロパティタブ

［プロパティ］タブには、選択したユーザーグループに関する情報が表示されます。

プロパティタブへのアクセス手順

［セキュリティポリシー管理］>**［ユーザーグループ］**>＋**［新しいユーザーグループ］**または **［編集］**>**［プロパティ］**

または

［ユーザー管理］>**［ユーザーグループ］**>**［プロパティ］**

表：ユーザーグループ：プロパティタブプロパティ

プロパティ	説明
名前	グループ名
説明	選択したユーザーグループの情報
削除	このボタンをクリックすると、ユーザーグループが削除されます。

［プロパティ］>**［アクセス許可］**タブには、ユーザーの管理者権限、または管理者権限がない場合は「標準ユーザー」が表示されます。

11.8.2 ユーザータブ

ユーザータブには、選択したグループのメンバーが表示されます。

詳細ツールバーから＋**［ユーザーの追加］**をクリックして、選択したローカルユーザーグループに 1 人以上のユーザーを追加します。

> **メモ：**ディレクトリグループの場合、グループメンバーシップは読み取り専用です。つまり、**ユーザー**タブを使用してディレクトリグループにユーザーを追加または削除したり、ディレクトリグループからユーザーを削除したりすることはできません。

ユーザータブへのアクセス

［セキュリティポリシー管理］>**［ユーザーグループ］**>（編集）>**［ユーザー］**または**［ユーザー管理］**>**［ユーザーグループ］**>（編集）>**［ユーザー］**に移動します。

表：ユーザーグループ：ユーザータブプロパティ

プロパティ	説明
ユーザー名	ユーザーの表示名
名前	情報がユーザーのプロパティに存在する場合は、ユーザーの名前と姓。それ以外の場合は、ユーザーの表示名
説明	ユーザーの説明
プロバイダ	認証プロバイダの名前：**Local**、**Certificate**、または Microsoft Active Directory ドメイン名などの外部プロバイダの名前
識別名	ユーザーの識別名
姓	ユーザーの姓
名	ユーザーの名まえ
メール	ユーザーのメールアドレス
勤務先電話	ユーザーの勤務先電話番号
携帯電話	ユーザーの携帯電話番号
タイムゾーン	ユーザーのタイムゾーン
ID プロバイダ	ユーザーの ID プロバイダ
ドメイン名	ユーザーのドメイン名
ログイン名	ユーザーのログイン名
非アクティブ化	ユーザーが現在無効化されているかどうか
アクセス許可	ユーザーのアクセス許可

詳細ツールバーの次のボタンを使用して、ユーザーグループ内のユーザーを管理します。

表：ユーザーグループ：ユーザータブツールバー

オプション	説明
＋ ユーザーの追加	選択したユーザーグループに 1 人以上のユーザーを追加します。詳細については、「ユーザーをユーザーグループに追加」を参照してください。
ー 削除	選択したユーザーをユーザーグループから削除します。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	ユーザーグループ内のユーザーのリストを更新します。
検索	このリストで特定のユーザーまたはユーザーのセットを見つけるには、一致するものの検索に使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

11.8.3 資格タブ

［資格］タブには、グループが割り当てられた資格が表示されます。グループのすべてのメンバーはその資格のリクエストポリシーへのアクセスを継承します。

> **メモ：［資格］**タブは、監査人またはセキュリティポリシー管理者の権限を持つユーザーのみが使用できます。

選択したユーザーグループを 1 つまたは複数の資格のユーザーとして追加するには、＋**［追加］**をクリックしします。

資格へのアクセス

［セキュリティポリシー管理］＞［ユーザーグループ］＞（編集）**＞［資格］**または**［ユーザー管理］＞［ユーザーグループ］＞**（編集）**＞［資格］**に移動します。

表：ユーザーグループ：資格タブのプロパティ

プロパティ	説明

名前	資格に割り当てられた名前
アカウント	この資格の一意のアカウントの数
ユーザー	この資格の一意のユーザーとユーザーグループの数
ポリシー	この資格の一意のポリシーの数

詳細ツールバーの次のボタンを使用して、選択したユーザーグループに関連付けられた資格を管理します。

表：ユーザーグループ：資格タブツールバー

オプション	説明
＋ 追加	選択したユーザーグループを 1 つ以上の資格に追加します。詳細については、「資格にユーザーグループを追加」を参照してください。
ー 削除	選択した資格からユーザーグループを削除します。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	資格のリストを更新します。
検索	このリストで特定の資格または資格のセットを見つけるには、一致するものの検索に使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

11.8.4 履歴タブ

［履歴］タブでは、選択したグループに影響を与えた各操作の詳細を表示またはエクスポートすることができます。

履歴へのアクセス

［セキュリティポリシー管理］>**［ユーザーグループ］**>（編集）>**［履歴］**または**［ユーザー管理］**>**［ユーザーグループ］**>（編集）>**［履歴］**に移動します。

- **日付範囲：**デフォルトでは、履歴の詳細は過去 24 時間分表示されます。ドロップダウンから、時間間隔を一つ選択すると、その時間枠の履歴の詳細が表示されます。
- **エクスポート**：データを JSON または CSV ファイルにエクスポートします。
- **更新**：表示されているリストを更新します。
- **検索**：詳細については、「検索ボックス」を参照してください。

表：ユーザーグループ：履歴タブのプロパティ

プロパティ	説明
日付/時間	イベントの日時
ユーザー	イベントを発生させたユーザーの表示名
ソース IP	イベントを発生させた管理対象システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択したグループの名前
イベント	選択したユーザーグループに対して行われた操作のタイプ： • 作成 • 削除 • 更新 • メンバーシップの追加 • ディレクトリグループ同期の完了 **メモ：**メンバーシップ操作は、ユーザーが選択されたユーザーグループのメンバーシップに追加または削除された、あるいは選択されたグループが資格に追加または削除されたなど、関連または親オブジェクトとの関係変更を示すものです。
関連オブジェクト	関連オブジェクトの名前
関連オブジェクトタイプ	関連オブジェクトのタイプ
親	選択したユーザーグループが子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

11.8.5 ユーザーグループの管理

SPP ユーザーグループは、ユーザーグループページのコントロールとタブ付きページを使用して、管理します。

- ユーザーグループの追加
- ディレクトリユーザーグループの追加
- ユーザーグループへのユーザーの追加
- 資格にユーザーグループを追加
- ユーザーグループの削除

ユーザーグループの追加

SPP にユーザーのグループを追加することができるのは、セキュリティポリシー管理者、権限許可者管理者、ユーザー管理者です。

> **メモ：**ディレクトリグループを追加できるのは、権限許可者管理者またはユーザー管理者です。詳細については、「ディレクトリユーザーグループの追加」を参照してください。

ユーザーグループの追加手順

1. **［セキュリティポリシー管理］＞［ユーザーグループ］**または**［ユーザー管理］＞［ユーザーグループ］**の順に選択します。
2. ツールバーから ＋ **［新しいユーザーグループ］＞［ユーザーグループ］**をクリックします。
3. **新しいユーザーグループ**ダイアログで、次の情報を入力します：
    a. **名前**：ユーザーグループの一意の名前を 50 文字以内で入力します。
    b. **説明：**（任意）このユーザーグループに関する情報を 255 文字以内で入力します。
4. **［アクセス許可］**タブで、グループの各メンバーに割り当てる Help Desk および/または**個人用パスワードボールト**のアクセス許可を選択します。各グループメンバーに対して、グループの選択されたアクセス許可は、すでに明示的に付与された既存のアクセス許可、または所属する他のグループによって結合されます。詳細については、「アクセス許可タブ（ユーザーの追加）」を参照してください。

グループの同期中（15 分ごと）に、あるユーザーがメンバーでなくなったことが確認される場合があります。この場合、そのユーザーが他のグループのメンバーで、そのグループからアクセス許可を継承していない限り、そのグループの選択されたアクセス許可はそのユーザーから削除されます。SPP は、明示的に割り当てられたアクセス許可とグループ経由で割り当てられたアクセス許可を追跡したり区別したりすることはありません。

> **重要**：個人用パスワードボールトアクセス許可は、他のアクセス許可と同様に、ユーザーに対して明示的に設定するか、グループから継承することができます。個人用パスワードボールトアクセス許可を持つユーザーが 1 つまたは複数の個人用パスワードを保存し、その後、どちらか明示的またはそれを継承したすべてのグループから削除されたことによって、アクセス許可を無効にしている場合、ユーザーは**個人用パスワードボールト**機能にアクセスすることができなくなります。しかし、データボールト内のユーザーのデータはまだ維持されます。ある時点でユーザーに個人用パスワードボールトのアクセス許可が再び付与された場合、ユーザーは既存のすべてのデータへのアクセスを回復します。

5. **［OK］**をクリックします。インポート時に、ユーザーグループが作成され、インポートプロセスが完了すると、割り当てられたユーザーが表示されます。

ディレクトリユーザーグループの追加

ディレクトリユーザーグループを追加するには、アプライアンス管理者が Active Directory または LDAP サーバーを ID プロバイダとして追加する必要があります。

［アプライアンス管理］＞［Safegaurd アクセス］＞［ID と認証］

詳細については、「ID と認証」を参照してください。

次に、権限許可者管理者またはユーザー管理者は、ディレクトリユーザーグループを追加できます。

セキュリティポリシー管理者は、権限許可者管理者、ユーザー管理者はローカルユーザーグループを追加できます。詳細については、「ユーザーグループの追加」を参照してください。

インポートに関する考慮事項

ディレクトリインポートのユーザーグループに属するすべてのユーザーは、完全かつ有効な属性を持っている必要があります。ユーザーの属性が完全かつ有効でない場合、そのユーザーはインポートされず、インポートが続行されます。

ポート

ディレクトリ管理タスク（ディレクトリアカウント、ディレクトリユーザーアカウント、ディレクトリユーザーグループの追加など）のために、環境内のすべての Windows グローバルカタログサーバーと SPP アプライアンスが通信するには、ファイアウォールで標準グローバルカタログポート 3268（LDAP）を開放する必要があります。LDAP は、暗号化されていない接続にポート 389 を使用します。詳細については、Microsoft 社のパブリケーション『How the Global Catalog Works』を参照してください。

時間

Microsoft Active Directory にはタイムゾーン属性がないため、ディレクトリユーザーグループを追加すると、SPP はインポートしたすべてのアカウントのデフォルトのタイムゾーンを(UTC) Coordinated Universal Time に設定します。タイムゾーンをリセットするには、インポートした各アカウントを**［ユーザー］**で開き、**［場所］**タブの**［タイムゾーン］**を変更します。

ディレクトリユーザーグループを追加する手順

1. **［セキュリティポリシー管理］**＞**［ユーザーグループ］**または**［ユーザー管理］**＞**［ユーザーグループ］**の順に選択します。
2. ツールバーから＋**［新しいユーザーグループ］**＞**［ディレクトリユーザーグループ］**をクリックします。
3. **［ディレクトリグループ］**タブ：
    a. ディレクトリを選択します。
    b. **［検索場所のフィルタ］**で、**［参照］**を使用してディレクトリ内のコンテナを選択します。このオプションは、Starling ディレクトリでは使用できません。
    c. **［サブコンテナのオブジェクトを含める］**チェックボックスは、デフォルトで選択されており、子オブジェクトが検索に含まれることを示します。このチェックボックスをオフにすると、子オブジェクトが検索対象から除外されます。このオプションは、Starling ディレクトリでは使用できません。
    d. **［次を含む］**フィールドに、ディレクトリグループ名の全体または一部を入力し、**［検索］**をクリックします。または空白のままにしておくと、最初の 1,000 件が返されます。

テキスト検索では、大文字と小文字は区別されず、ワイルドカードは使用できません。SPP は、フォレストの各ドメインを検索します。部分的な文字列で検索することができます。たとえば、検索ボックスに "ad" と入力すると、"ad" を含むディレクトリグループがすべて検索されます。

e. **［ディレクトリプロファイルの選択］**に表示された結果から、グループ名を選択し、**［OK］**を選択します。

f. **［管理対象ディレクトリアカウントを自動的にリンク］**チェックボックスを選択すると、インポートしたユーザーに既存の管理対象ディレクトリアカウントがリンクアカウントとして設定されます。このオプションは Starling ディレクトリでは使用できません。

ID プロバイダの Managed Objects 属性の設定に基づき、Safeguard の既存の管理対象ディレクトリアカウントと一致するように属性値が使用されます。Safeguard ユーザーのリンクアカウントのセットは、定期的にディレクトリと同期され、ディレクトリからの値で上書きされます。ユーザーに対して手動で行われたリンクアカウントへの変更は、次回のディレクトリ同期時に失われます（[管理タブ（資産の追加）]の「追加同期間隔」を参照してください）。

4. **［認証］**タブで、プライマリ認証とセカンダリ認証を設定します。ユーザーをインポートする場合、Safeguard は新しいユーザーに対してプライマリ認証とセカンダリ認証のプロバイダを設定します。ディレクトリユーザーグループメンバーがすでに Safeguard にユーザーとして存在する場合、その認証プロパティは変更されません。グループのメンバーである既存の Safeguard ユーザーの認証設定を変更するには、/UserGroups/{id}/SynchronizeAndUpdateProviders API メソッドを手動で呼び出す必要があります。

ディレクトリグループにはフォレストルートドメインが表示され、**［アプライアンス管理］＞［ID と認証］**で設定した ID および認証で利用可能であることが必要です。詳細については、「ID と認証に使用可能なドメイン（Active Directory の場合）」を参照してください。

a. **認証プロバイダ**フィールドのデフォルトは、グループ由来のディレクトリ（Active Directory の場合はフォレストルート名）です。

ディレクトリユーザーグループからインポートされた新規作成 Safeguard ユーザーはすべて、プライマリ認証プロバイダがそのユーザー由来のディレクトリドメインを使用するように設定されます。複数のドメインがある Active Directory フォレストの場合、ドメインは「ID と認証に使用可能なドメイン」としてマークされている必要があります。ユーザーがグループのメンバーであっても、そのドメインが**［ID と認証に使用可能なドメイン］**としてマ

ークされていない場合、そのユーザーはインポートされません。詳細については、「ID と認証プロバイダの追加」を参照してください。

各ユーザーのプライマリ認証プロバイダとして、外部フェデレーションまたは Radius サーバーのいずれかを使用することができます。インポート処理中、外部フェデレーション認証または Radius 認証に指定されたディレクトリ属性が、ユーザーのメールアドレスまたは名前請求（外部フェデレーションの場合）またはログイン名（Radius の場合）プロパティの設定に使用されます。詳細については、「外部フェデレーション設定」および「Radius 設定」を参照してください。

b. **［証明書認証を必須とする］**チェックボックスを選択すると、ユーザーがドメイン発行のユーザー証明書またはスマートカードを使用して Safeguard にログインすることが要求されます。このオプションは、ディレクトリのユーザーグループが Microsoft Active Directory のもので、認証プロバイダもそのディレクトリとして設定されている場合にのみ使用できます。

c. ユーザーに 2 要素認証でのログインを要求することができます。Safeguard でユーザーを正常に作成するには、インポートするユーザーの連絡先情報が完全である必要があります。

   i. **［セカンダリ認証を要求する］**チェックボックスを選択します。詳細については、「セカンダリ認証ログインの要求」を参照してください。

   ii. ディレクトリユーザーグループのすべてのユーザーに対して、セカンダリ認証プロバイダを選択します。ID プロバイダと認証プロバイダの有効な組み合わせを使用します。詳細については、「ID と認証」を参照してください。

5. **［アクセス許可］**タブで、ディレクトリグループの各メンバーに割り当てる管理権限および/または個人用パスワードボールトアクセス許可権限を選択します。各グループメンバーに対して、グループの選択されたアクセス許可は、すでに明示的に付与されている既存のアクセス許可と結合されます。詳細については、「アクセス許可タブ（ユーザーの追加）」を参照してください。

   ディレクトリグループの同期中に、ユーザーがメンバーでなくなったことが確認される場合があります。この場合、ディレクトリグループの選択されたアクセス許可は、そのユーザーがアクセス許可を継承する他のグループのメンバーでない限り、そのユーザーから削除されます。SPP は、明示的に割り当てられたアクセス許可とグループ経由で割り当てられたアクセス許可を追跡したり区別したりすることはありません。

> **重要**：個人用パスワードボールトアクセス許可は、他の権限と同様に、ユーザーに対して明示的に設定するか、グループから継承することができます。個人用パスワードボールドアクセス許可を持つユーザーが 1 つまたは複数の個人用パスワードを保存し、その後、どちらか明示的または彼らがそれを継承したすべてのグループから削除されたことによって、アクセス許可を無効にしている場合、ユーザーはもはや個人用パスワードボールトの機能にアクセスすることができません。しかし、データボールト内のユーザーのデータは維持されます。ある時点でユーザーに個人用パスワードボールトのアクセス許可が再び付与された場合、ユーザーは既存のすべてのデータへのアクセスを回復します。

6. **［OK］**をクリックします。インポート時に、ディレクトリユーザーグループが作成され、インポート処理が完了すると、割り当てられたユーザーが表示されます。

7. 情報を追加した後、以下のディレクトリグループ設定を編集すると、バックグラウンドでディレクトリ同期処理が開始されます。
    - **［ディレクトリグループ］**タブ：**［管理対象ディレクトリアカウントを自動的にリンク］**チェックボックスを選択またはクリアする。
    - **［認証］**タブ：認証プロバイダを変更する。

      > **メモ：**認証プロバイダを変更すると、新しくインポートされたユーザーにのみ影響があります。既存のユーザーには、認証プロバイダは更新されません。グループのメンバーである既存の Safeguard ユーザーの認証設定を変更するには、/UserGroups/{id}/SynchronizeAndUpdateProviders API メソッドを手動で呼び出す必要があります。
    - **アクセス許可**タブ：アクセス許可を変更する。

ユーザーグループへのユーザーの追加

ローカルの SPP グループにユーザーを追加できるのは、権限許可者管理者、ユーザー管理者、セキュリティポリシー管理者です。ディレクトリユーザーグループについては、ユーザーを手動で追加または削除することはできません。これらのグループは、由来する Active Directory または LDAP サーバーと自動的に同期されます。

ユーザーをユーザーグループに追加する手順

1. **［セキュリティポリシー管理管］＞［ユーザーグループ］**または**［ユーザー管理］＞［ユーザーグループ］**の順に選択します。

2. リストからユーザーグループを選択し、**［編集］**を選択します。
3. **［ユーザー］**タブを選択します。
4. 詳細ツールバーの **［ユーザーの追加］**をクリックします。
5. **ユーザー**選択ダイアログのリストから 1 人または複数のユーザーを選択し、**［OK］**をクリックします。

> **重要**：ユーザーグループのメンバーシップにグループを追加することはできません。グループのメンバーシップをネストすることはできません。

資格にユーザーグループを追加

資格にユーザーグループを追加すると、資格のポリシーによって管理されるアカウントと資格へのアクセスをリクエストできる人を指定することになります。資格にユーザーグループを追加することができるのは、セキュリティポリシー管理者です。

資格にユーザーグループを追加する手順

1. **［セキュリティポリシー管理］＞［ユーザーグループ］**または**［ユーザー管理］＞［ユーザーグループ］**の順に選択します。
2. リストからユーザーグループを選択し、**［編集］**をクリックします。
3. **［資格］**タブを開きます。
4. 詳細ツールバーから **［追加］**をクリックします。
5. **資格**ダイアログから 1 つ以上の資格を選択し、**［OK］**をクリックします。

ユーザーグループの削除

ローカルおよびディレクトリのユーザーグループを削除することができるのは、権限許可者管理者とユーザー管理者です。セキュリティポリシー管理者は、アクセス許可を持たないローカルグループのみを削除することができます。

ユーザーグループを削除しても、SPP はそのグループに関連付けられたユーザーを削除しません。

ユーザーグループの削除手順

1. **［セキュリティポリシー管理］＞［ユーザーグループ］**または**［ユーザー管理］＞［ユーザーグループ］**の順に選択します。
2. リストからユーザーグループを選択します。
3. **［削除］**をクリックします。
4. 確認ダイアログで**［はい］**をクリックします。

11.9 設定

設定では、セッションパスワードアクセスと監査ログストリームサービスを管理することができます。パスワード、SSH キー、セッションへのアクセスをリクエストする理由を管理することもできます。

［セキュリティポリシー管理］＞［設定］の順に選択します。

11.9.1 セキュリティポリシー設定

表：セキュリティポリシー設定

設定	説明
最大通知受信者数	通知先の最大数を設定します。
有効期限の警告期間	警告の有効期限を日数で入力します。
Show User Name in Access Request Conflict Messages（アクセスリクエストの競合メッセージにユーザー名を表示する）	チェックボックスをオンにすると、ユーザーがリクエストしたい時間帯に競合するアクセスリクエストがある場合、エラーメッセージに競合するアクセスリクエストをしたユーザーの名前が表示されます。チェックボックスがオフの場合は、エラーメッセージにアクセリクエスト ID が表示されます。このチェックボックスはデフォルトでオフになっています。
セッションのパスワードアクセスが有効になりました	このトグルを使用して、セッションパスワードアクセスを有効または無効にします。この機能はデフォルトで無効になっています。

設定	説明
監査ログストリームサービス	SPP のデータを SPS に送信して、Safeguard 特権管理ソフトウェアスイートを監査するには、このトグルを使用します。この機能はデフォルトで無効になっています。 SPP データを受け入れるには、SPS アプライアンス管理者が監査ログの同期をオンにする必要があります。詳細については、「Safeguard for Privileged Sessions 管理ガイド」を参照してください。 この機能を使用するには、SPP と SPS がリンクされている必要があります。詳しくは、「SPP と SPS セッションアプライアンスリンクガイダンス」を参照してください。 SPP と SPS の同期は継続されますが、多少の遅延があるため、SPS が任意の時点ですべての監査データを持つことは保証されません。 **メモ：**この設定は、**［アプライアンス管理］＞［サービスの有効化または無効化］**でも使用できます。詳細については、「サービスの有効化または無効化」を参照してください。
理由	このペインでは、パスワード、SSH キー、セッションへのアクセスをリクエストする理由を管理できます。詳細については、「理由」を参照してください。

11.9.2 理由

セキュリティポリシー管理者は、アクセスリクエストポリシーで、要求者がパスワード、SSH キー、セッションへのアクセスをリクエストする理由を提供するよう求めることができます。アクセスをリクエストするときに、ユーザーはリストから定義済みの理由を選択することができます。たとえば、次のようなアクセスリクエストの理由を使用できます。

- ソフトウェア更新
- システムメンテナンス
- ハードウェア問題
- 問題チケット

アクセスリクエストの理由の設定手順

1. **［セキュリティポリシー管理］＞［設定］＞［理由］**の順に選択します。
2. ＋ **［追加］**をクリックして、新しい理由を追加します。
3. **［新しい理由］**ダイアログで、以下を入力します。
   a. **名前**：理由の名前を 50 文字以内で入力します。
   b. **説明**：理由の説明を 255 文字以内で入力します。
4. **［保存］**をクリックします。

理由を編集するには、既存の理由を選択し、**［編集］**をクリックします。

理由を削除するには、既存の理由を選択し、**［削除］**をクリックします。

12 ユーザー管理

画面左のナビゲーションペインで**［ユーザー管理］**を選択して展開します。

12.1 ユーザー

ユーザーとは、SPP にログインできる人のことです。ローカルユーザーとディレクトリユーザーの両方を追加することができます。ディレクトリユーザーとは、Microsoft Active Directory などの外部 ID ストアからのユーザーです。詳細については、「ユーザーとユーザーグループ」を参照してください。

［ユーザー］に表示される内容は管理者のアクセス許可権限によって決まります。色あせた色で表示されているユーザーは、無効です。次の表は、各タイプの管理者が利用できるタブを示しています。

- 権限許可者管理者：全般、履歴
- ユーザー管理者：全般、ユーザーグループ（ディレクトリユーザーのみ）、履歴
- Help Desk 管理者：全般、履歴
- 監査人管理者：全般、所有オブジェクト、ユーザーグループ、資格、リンクアカウント、履歴
- 資産管理者：全般、所有オブジェクト
- セキュリティポリシー管理者：全般、ユーザーグループ、資格、リンクアカウント、履歴

権限許可者管理者は、通常、**有効/無効**の状態を制御します。詳細については、「ユーザーの有効化または無効化」を参照してください。

ユーザーへのアクセス手順

［セキュリティポリシー管理］＞［ユーザー］

ユーザービュー

ユーザービューには、選択したユーザーに関する次の情報が表示されます。

- プロパティタブ：選択したユーザーの認証、連絡先、場所、アクセス許可が表示されます。
- ユーザーグループタブ：選択したユーザーがメンバーであるユーザーグループが表示されます。
- 資格タブ：選択されたユーザーがメンバーである資格、つまり資格 "ユーザー"が表示されます。
- 履歴タブ：選択したユーザーに影響を与えた各操作の詳細が表示されます。

ツールバー

次のツールバーボタンを使用してユーザーを管理します：

- **新しいユーザー**： SPP にユーザーを追加します。詳細については、「ユーザーの追加」を参照してください。
- **削除**： 選択したユーザーを削除します。詳細については、「ユーザーの削除」を参照してください。
- **詳細の表示**：選択したユーザーの詳細を表示または編集します。
- **アクセス許可**：選択したユーザーに適用される管理者権限を示す**［アクセス許可］**ダイアログを表示します。
- **パスワードの設定：**ローカルユーザーのパスワードを設定します。
- **ユーザーのロック解除：**ローカルユーザーのアカウントのロックを解除します。
- **ユーザーのアクティブ化：**選択したユーザーのアカウントを有効にします。
- **ユーザーの非アクティブ化：**選択したユーザーのアカウントを無効にします。
- **エクスポート：**リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
- **更新**: ユーザーのリストを更新します。
- **検索：** 文字列または選択した属性で、条件を入力して検索することができます。選択した属性で検索するには、**［検索］**をクリックし、検索する属性を選択します。詳細については、「検索ボックス」を参照してください。

12.1.1 プロパティタブ

［プロパティ］タブには、選択したユーザーに関する情報が表示されます。

プロパティへのアクセス

［ユーザー管理］>**［ユーザー］**>［詳細の表示］>**［プロパティ］**

表：ユーザープロパティタブ

プロパティ	説明
ID	
ID プロバイダ	ユーザーの個人情報の出所および同期元
ユーザー名	ユーザーの表示名
名	ユーザーのファーストネーム
姓	ユーザーのラストネーム
勤務先電話	ユーザーの勤務先電話番号
携帯電話	ユーザーの携帯電話番号
メール	ユーザーのメールアドレス
説明	説明テキストは、ユーザー情報が追加または更新されたときに入力されます。これは、ユーザーダイアログの ID タブの説明テキストボックスで入力することができます。
場所	ユーザーは、タイムゾーンを変更することができます。または、ユーザー管理者は、ポリシーの遵守を保証するために、ユーザーがタイムゾーンを変更することを禁止することができます。詳しくは、「タイムゾーン」を参照してください。
認証	
認証プロバイダ	ユーザーが SPP で認証する方法 • **証明書**: 証明書を使用 • **Local**: ユーザー名とパスワード • **ディレクトリ名**: ディレクトリの認証情報
ログイン名	ユーザーがログインする識別子
ドメイン名	プライマリ**認証プロバイダ**がディレクトリの場合、そのディレクトリのドメイン名
識別名	認証に使用する識別名

プロパティ	説明
セカンダリー認証	二次認証が必要なユーザーを設定した場合、このユーザーの二次認証サービスプロバイダの名前
二次認証ユーザー名	ログイン時に必要な二次認証サービスプロバイダのユーザーアカウント名
パスワード有効期限なし	有効な場合、このフィールドは、ユーザーに関連付けられたパスワードが有効期限切れでないことを示します。
ユーザーは次回のログイン時にパスワードを変更する必要があります	有効な場合、ユーザーは次回ログイン時にパスワードを変更するよう促されることを示します。
アクセス許可	
アクセス許可	ユーザーの管理者アクセス許可の一覧、または管理者権限がない場合は「標準ユーザー」が表示されます。

12.1.2 ユーザーグループタブ

[ユーザーグループ]タブには、選択したユーザーがメンバーであるユーザーグループが表示されます。

[ユーザーグループ]タブは、監査人またはセキュリティポリシー管理者のアクセス許可を持つユーザーと、（ローカルユーザーではなく）ディレクトリユーザーのユーザー管理者が利用できます。

表：ユーザー：ユーザーグループツールバー

オプション	説明
追加	ユーザーを 1 つまたは複数のユーザーグループに追加します。詳細については、「ユーザーをユーザーグループに追加」を参照してください。
削除	選択したユーザーから、選択したユーザーグループを削除します。
エクスポート	リストされたデータを JSON または CSV ファイルとしてエクスポートします。詳しくは、「データのエクスポート」を参照してください。

オプション	説明
更新	選択したユーザーに関連するユーザーグループの最新の一覧を取得し、表示します。
検索	この一覧から特定のユーザーグループを探すには、一致する文字列を入力します。詳細については、「検索ボックス」を参照してください。

12.1.3 資格タブ

［資格］タブには、選択されたユーザーがメンバーである資格が表示されます。**［資格］**タブは、監査人またはセキュリティポリシー管理者のアクセス許可権限をもつユーザーのみが利用できます。

資格へのアクセス

［ユーザー管理］>**［ユーザー］**>［詳細の表示］>**［資格］**

表：ユーザー：資格タブプロパティ

プロパティ	説明
名前	選択したユーザーがユーザーとして割り当てられている資格の名前
説明	資格の説明
ポリシー	資格内の一意のアクセスリクエストポリシーの数
アカウント	選択された資格内のユニークなアカウントの数
ユーザー	資格内の一意のユーザーの数
ユーザーグループ	選択されたユーザーを資格に関連付けるユーザーグループの名前 **メモ:** 選択されたユーザーがユーザーグループのメンバーシップを通してではなく、明示的に資格と関連付けられている場合、この列は空白で**［直接メンバー］**列は真になります。

プロパティ	説明
直接メンバー	選択されたユーザーが明示的にユーザーとして資格に追加された場合、真を示します。詳細については、「ユーザーまたはユーザーグループを資格に追加」を参照してください。

詳細ツールバーの次のボタンを使用して、選択したユーザーと関連する資格を管理します。

表：ユーザー：資格タブツールバー

オプション	説明
＋ 追加	選択したユーザーを 1 つまたは複数の資格のユーザーとして追加します。詳細については、「資格にユーザーを追加」を参照してください。
ー 削除	選択した資格からユーザーを削除します。
エクスポート	リストされたデータを JSON ファイルまたは CSV ファイルとしてエクスポートするには、このボタンを使用します。詳細は、「データのエクスポート」を参照してください。
更新	資格のリストを更新します。
検索	このリストで特定の資格または資格のセットを見つけるために、一致するものを検索するために使用する文字列を入力します。詳細については、「検索ボックス」を参照してください。

12.1.4 履歴タブ

［履歴］タブでは、選択したグループに影響を与えた各操作の詳細を表示またはエクスポートすることができます。

履歴へのアクセス

［ユーザー管理］＞**［ユーザー］**＞（編集）＞**［履歴］**に移動します。

- **日付範囲：**デフォルトでは、履歴の詳細は過去 24 時間分表示されます。ドロップダウンから、時間間隔を一つ選択すると、その時間枠の履歴の詳細が表示されます。

- **エクスポート**：データを JSON または CSV ファイルにエクスポートします。詳しくは「データのエクスポート」を参照してください。
- **更新**：表示されているリストを更新します。
- **検索**：詳細については、「検索ボックス」を参照してください。

表：ユーザー：履歴タブのプロパティ

プロパティ	説明
日付/時間	イベントの日時
ユーザー	イベントを発生させたユーザーの表示名
ソース IP	イベントを発生させた管理対象システムのネットワーク DNS 名または IP アドレス
オブジェクト名	選択したユーザーの名前
イベント	選択したユーザーに対して行われた操作のタイプ： • 作成 • 削除 • 更新 • メンバーシップの追加 • メンバーシップの削除 **メモ：**メンバーシップ操作は、ユーザーが選択されたユーザーグループのメンバーシップに追加または削除された、あるいは選択されたグループが資格に追加または削除されたなど、関連または親オブジェクトとの関係変更を示すものです。
関連オブジェクト	関連オブジェクトの名前
関連オブジェクトタイプ	関連オブジェクトのタイプ
親	選択したユーザーグループが子であるオブジェクトの名前
親オブジェクトタイプ	親オブジェクトのタイプ

12.1.5 ユーザーの管理

SPP のユーザーを管理するには、**［ユーザー］**ページのコントロールとタブページを使用して、次のタスクを実行します。

- ユーザーの追加
- セカンダリ認証ログインの要求
- ユーザーをユーザーグループに追加
- 資格にユーザーを追加
- ユーザーの有効化または無効化
- ユーザーの削除
- ローカルユーザーのパスワード設定
- ユーザーのアカウントのロック解除

ユーザーの追加

SPP のユーザーを追加できるのは、権限許可者管理者とユーザー管理者です。

ユーザーの追加手順

1. **［ユーザー管理］＞［ユーザー］**を開きます。
2. ツールバーの ＋ **［新しいユーザー］**をクリックします。
3. **［新しいユーザー］**ダイアログで、各タブに情報を入力します。
    - ID タブ：ID プロバイダ、ユーザーの連絡先、所在地を定義します。
    - 認証タブ：認証プロバイダ、ログイン名、パスワード（必要な場合）を定義します。
    - アクセス許可：ユーザーの管理者権限を設定します。

ID タブ

ID タブで、利用可能なプロバイダの一覧から ID プロバイダを選択します。Microsoft Active Directory などの外部 ID プロバイダからユーザーを追加する場合、SPP はソースから読み取り専用で連絡先をインポートしますが、ユーザー写真は変更することが可能です。

ID プロバイダと認証プロバイダの有効な組み合わせを使用します。詳細については、「ID と認証」を参照してください。

表：ユーザー：ID タブプロパティ

プロパティ	説明
ID プロバイダ	ユーザーの ID のソース。SPP には、Local という ID プロバイダが内蔵されており、SPP に直接保存されているユーザー情報を手動で入力することができるようになります。または、事前に設定した Active Directory または LDAP サーバーを選択し、ユーザーを参照することもできます。SPP は定期的にディレクトリと同期し、情報を最新に保ちます。 ユーザーの ID が SPP によってどのように管理されるかを示します。 • Local • Active Directory • LDAP • Starling
［参照］（Active Directory または LDAP）	ID プロバイダが Active Directory または LDAP の場合、**［参照］**ボタンをクリックしてユーザー名を選択します。残りのフィールドは自動入力されます。
名（Local プロバイダ）	ユーザーの名前を入力します。30 文字以内、ダブルクォーテーションは使用できません。
姓（Local プロバイダ）	ユーザーの姓を入力します。30 文字以内、ダブルクォーテーションは使用できません。
勤務先電話（Local プロバイダ）	ユーザーの勤務先電話番号を入力します。半角英数字で 30 文字以内
携帯電話（Local プロバイダ）	ユーザーの携帯電話番号を入力します。30 文字以内
メール（Local プロバイダ）	ユーザーのメールアドレスを入力します。255 文字以内

プロパティ	説明
	メモ：Cloud Assistant 機能を使用し、認証プロバイダとして OneLogin MFA を使用している承認者には必須です。また、OneLogin MFA では、このフィールドに入力したメールアドレスが、OneLogin で設定したメールアドレスと同一であることが必要です。
説明（Local プロバイダ）	このユーザーに関する情報を 255 文字以内で入力します。
タイムゾーン	ユーザーのタイムゾーンを選択します。 Microsoft Active Directory にはタイムゾーン属性がないため、ディレクトリグループを追加すると、インポートされたすべてのアカウントのデフォルトのタイムゾーンは（UTC）協定世界時（Coordinated Universal Time）に設定されます。タイムゾーンをリセットするには、インポートした各アカウントを**［ユーザー］**で開き、**［タイムゾーン］**を変更します。

認証タブ

［認証］タブで、ユーザーの認証設定を指定します。認証プロバイダは、ユーザーの ID プロバイダと同じでも異なっていてもかまいません。

ID プロバイダと認証プロバイダの有効な組み合わせを使用します。詳細については、「ID と認証」を参照してください。

表：ユーザー：認証タブプロパティ

プロパティ	説明
認証プロバイダ	このユーザーが SPP に対してどのように認証を行うかを示します。オプションは次のとおりです。 • Certificate：証明書を使用 **メモ:** SPP では、公開鍵証明書をユーザーアカウントにマップすることができます。その後、証明書を使用して、API を使用してアプライアンスに認証された要求を行うことができます。詳細については、「API の使用」を参照してください。

プロパティ	説明
	• **Local：**ユーザー名とパスワード付き（デフォルト） • <ディレクトリ名>: ディレクトリアカウントの認証情報を使用（Active Directory や LDAP など、1 つ以上のディレクトリが SPP に追加されており、ユーザーの ID プロバイダもそのディレクトリである場合のみ使用可能）。 • <外部フェデレーションサービスプロバイダ名>: 外部フェデレーションまたは Radius サーバーが必要とする認証情報（これらの認証プロバイダの 1 つ以上が SPP で構成されている場合のみ利用可能）を指定します。
証明書のサムプリント（SHA-1）（Certificate ユーザー）	**Certificate** ユーザーを追加する場合、証明書の一意のハッシュ値（16 進数で 40 文字）を入力します。サムプリントの値は、スペースを含めて、証明書から直接コピー＆ペーストできます。
メールアドレスまたは Name Claim（外部フェデレーション）	外部フェデレーションユーザーアカウントを追加する場合、認証されたユーザーの STS から返されるメールアドレスまたは名前のクレームを入力します。ユーザーがログインする際に、大文字と小文字を区別しない比較が実行されます。 **メモ：**STS にメールアドレスクレームまたは名前クレームのいずれかが含まれるように設定または確認する必要があります。SPP は、まずクレームトークンでメールアドレスのクレームを探します。そのクレームが存在しない場合、名前のクレームが使用されます。SPP では、STS から返されたクレームに従ってユーザーアカウントを作成する必要があり、メールアドレスのクレームが優先されます。
ローカルまたは Radius がプライマリプロバイダーの場合：ログイン名	認証に Local または Radius as Primary を使用する場合、これはユーザーのログイン名です。デフォルトは、**［ID］**タブの**［ユーザー名］**フィールドに入力された値です。

プロパティ	説明
	ディレクトリ認証を使用している場合、ログイン名は自動入力されます。
［パスワード設定］ボタン（既存のローカルプロバイダの編集）	**Local** プロバイダの既存ユーザを編集している場合、**［パスワードの設定］**をクリックして、ユーザのパスワードを変更することができます。このボタンは、新規ユーザの作成時や、Microsoft Active Directory などの外部 ID プロバイダのユーザーアカウントを編集する際には使用できません。
パスワード（Local プロバイダの追加）	**Local** ユーザーを追加する場合、そのユーザーのパスワードを入力します。ダイアログで指定されたパスワードの要件に準拠する必要があります。詳細については、「ローカルパスワードルール」を参照してください。
証明書認証の必要性 (プロバイダが MS AD の場合、Active Directory プロバイダ)	このチェックボックスを選択すると、ユーザーがドメイン発行のユーザー証明書またはスマートカードを使用して SPP にログオンすることを要求します。このオプションは、認証プロバイダが Microsoft Active Directory の場合のみ利用可能です。
パスワード有効期限なし	このチェックボックスを選択すると、有効期限のないパスワードが設定されます。
ユーザーは次回のログイン時にパスワードを変更する必要があります	このチェックボックスは、認証に Local を使用している場合のみ使用できます。このチェックボックスをオンにすると、ユーザーは次回のログイン時にパスワードを変更する必要があります。
セカンダリ認証を必須とする	このチェックボックスを選択すると、このユーザーは 2 要素認証で SPP にログインすることが要求されます。詳細については、「セカンダリ認証ログインの要求」を参照してください。 次に、このユーザーの 2 次認証プロバイダを選択します。ID と認証プロバイダを有効に組み合わせて使用します。詳細については、「ID と認証」を参照してください。
ログイン名（セカンダリ認証用：FIDO2 用ではない）	• 二次認証にディレクトリを選択した場合、二要素認証で SPP にログインする際にこのユーザー

プロパティ	説明
	が使用する必要のある二次認証プロバイダのアカウントを参照し選択します。 • 二次認証プロバイダとして Radius を選択した場合、この値にはあらかじめログイン識別子が入力されています。詳細については、「Radius の設定」を参照してください。 ベストプラクティスは、正しいユーザーが設定されていることを検証するために、ユーザーにログインしてもらうことです。

アクセス許可タブ

［アクセス許可］タブで、該当する場合は、ユーザーの管理者アクセス許可権限を選択します。アクセス許可権限の詳細については、「管理者のアクセス許可」を参照してください。

複数のユーザーグループにまたがるユーザーのアクセス許可

ユーザーは、割り当てられたユーザーグループに基づくアクセス許可権限を持っています。ユーザーがユーザーグループから削除された場合、そのグループに関連するアクセス許可権限は削除されますが、そのユーザーが割り当てられている他のすべてのグループのアクセス許可権限はそのまま維持されます。

インポート時のユーザーアクセス許可

ディレクトリユーザーグループがインポートされると、新しく作成された Safeguard ユーザーには選択されたアクセス許可権限が割り当てられます。Safeguard にユーザーが存在する場合、選択されたアクセス許可権限は既存のユーザーアクセス許可権限に追加されます。詳細については、「ディレクトリユーザーグループの追加」を参照してください。

アクセス許可の割り当て

ユーザーにアクセス許可を割り当てる場合、適切なアクセス制御を選択します。ダイアログの下部にある**［Select All］**（すべて選択）または**［Select None］**（なにも選択しない）を選択することができます。

- **権限許可者**：そのユーザーが他のユーザーにアクセス許可を付与できるようにします。このアクセス許可により、ユーザーは自分自身のアクセス許可を変更することができます。
- **ユーザー**：管理者以外のユーザーに対して、新しいユーザーの作成、パスワードのロック解除、リセットすることができます。
- **Help Desk**：管理者以外のユーザーに対して、パスワードのロック解除と再設定を許可します。
- **アプライアンス**：アプライアンスの編集と更新、メール、SNMP、Syslog、チケットなどの外部統合設定の構成をユーザーに許可します。
- **操作**：アプライアンスの再起動と監視を許可します。
- **監査人**：ユーザーに読み取り専用アクセスを許可します。このアクセス許可を選択した場合、アプリケーション監査人とシステム監査人のアクセス許可が有効になります。
    - **アプリケーション監査人**：資産管理およびセキュリティポリシー管理への読み取り専用アクセスをユーザーに許可します。
    - **システム監査人：**アプライアンス管理およびユーザー管理への読み取り専用アクセスをユーザーに許可します。
- **資産**：パーティション、資産、アカウントを追加、編集、削除することをユーザーに許可します。
- **セキュリティポリシー**：アカウントと資産へのアクセスを制御する資格とポリシーの追加、編集、削除をユーザーに許可します。
- **個人用パスワードボールド：**個人用パスワードボールトの追加、編集、削除、共有、およびアクセスを許可します。このチェックボックスは、ユーザー管理者とセキュリティポリシー管理者のみが使用できます。詳細については、「個人用パスワードボールト」を参照してください。

セカンダリ認証ログインの要求

ユーザーレコードで**［セカンダリ認証を必須とする］**オプションを有効にすると、二要素認証を使用したログインをユーザーに要求できます。

セカンダリ認証を使用したログインをユーザーに要求する手順

1. **［アプライアンス管理］＞［Safeguard アクセス］＞［ID と認証］**で、二次認証プロバイダを設定します。詳細については、「ID と認証プロバイダの追加」を参照してください。
2. SPP ユーザーを**［セカンダリ認証を必須とする］**に設定します。詳細については、「認証タブ（ユーザーの追加）」を参照してください。
    a. ユーザーのプロパティの**［認証］**タブで**［セカンダリ認証を必須とする］**チェックボックスを選択します。
    b. **［認証プロバイダ］**を選択します。
    c. 選択した認証プロバイダの種類に応じて、このユーザーが二要素認証で SPP にログインする際に使用する必要がある追加情報を指定します。
3. セカンダリ認証でログインします。

    二次認証が必要なユーザーとして SPP にログインする場合、SPP のユーザーアカウントに設定されているパスワードを使用して通常通りログインします。その後、SPP は 1 つまたは複数の追加のログイン画面を表示します。システム管理者が二次認証プロバイダをどのように設定したかによって、二次認証サービスプロバイダアカウントの追加の認証情報（安全なパスワード、セキュリティトークンコード、またはその両方）を入力する必要があります。

    > **メモ：**二次認証プロバイダの種類と構成（たとえば、RSA SecureID、FIDO2 など）により、二次認証に何を提供する必要があるかが決まります。二次認証で SPP にログインする方法の詳細については、システム管理者に確認してください。

ユーザーをユーザーグループに追加

パスワードポリシーに割り当てるユーザーをユーザーグループに追加することは、セキュリティポリシー管理者の責任です。

ユーザーをユーザーグループに追加する手順

1. **［ユーザー管理］＞［ユーザー］**を開きます。
2. リストからユーザーを選択して**［詳細の表示］**をクリックします。
3. **［ユーザーグループ］**タブを選択します。

4. 詳細ツールバーから ＋ **［追加］**をクリックします。

5. **［ユーザーグループ］**ダイアログのリストから 1 つまたは複数のグループを選択し、**［OK］**をクリックします。

資格にユーザーを追加

資格にユーザーを追加できるのは、セキュリティポリシー管理者です。資格にユーザーを追加すると、資格のポリシーによって管理されるアクセスを要求できる人を指定することになります。

資格にユーザーを追加する手順

1. **［ユーザー管理］＞［ユーザー］**を開きます。

2. リストからユーザーを選択し、**［詳細の表示］**を選択します。

3. **［資格］**タブを開きます。

4. 詳細ツールバーから ＋ **［追加］**をクリックします。

5. **資格**ダイアログの一覧から 1 つ以上の資格を選択し、**［OK］**をクリックします。

ユーザーの有効化または無効化

ユーザーを有効または無効にできるのは、権限許可者管理者またはユーザー管理者です。ただし、状態を SPP 内で変更できるのは、ID ソースがローカルプロバイダに設定されているユーザーのみです。ディレクトリユーザーの状態は変更できません。ディレクトリユーザーの状態はディレクトリで変更した後に SPP と同期させる必要があります。

ユーザーを無効にすると、SPP にログインできなくなり、現在ログインしているセッションも終了します。ただし、管理者は自分自身のユーザーを無効化することはできません。

SPP は、設定した期間内にログインしていないユーザーを自動的に無効化するように設定することもできます。ただし、これはディレクトリユーザーには適用されません。詳細については、「ローカルログイン制御」を参照してください。

ユーザーを有効または無効にする手順

1. **［ユーザー管理］＞［ユーザー］**の順に選択します。

2. リストからユーザーを選択します。
3. ツールバーオプションで ✳ **［ユーザーのアクティブ化］**または ⊘ **［ユーザーの非アクティブ化］**をクリックして、設定に切り替えます。

ユーザーの削除

通常、管理者ユーザーを削除するのは権限許可者管理者で、非管理者ユーザーを削除するのはユーザー管理者です。

> **重要：**ローカルユーザーを削除すると、SPP はそのユーザーを完全に削除します。ディレクトリユーザーグループの一部であるディレクトリユーザーを削除すると、次にデータベースをディレクトリと同期するときに、SPP がそのユーザーを再び追加します。

ユーザーの削除手順

1. **［ユーザー管理］＞［ユーザー］**の順に移動します。
2. リストからユーザーを選択します。
3. 🗑 **［削除］**をクリックします。
4. 確認メッセージを確認して、**［はい］**を選択します。

ローカルユーザーのパスワード設定

管理者のパスワードを設定するのは、主に権限許可者管理者です。ユーザー管理者とヘルプデスク管理者は、管理者ではないローカルユーザーのパスワードを設定することができます。これらの管理者は、ローカルユーザーのパスワードのみを設定できます。ディレクトリユーザーのパスワードは、Microsoft ActiveDirectory などの外部プロバイダで管理されます。

ローカルユーザーのパスワード設定手順

1. **［ユーザー管理］＞［ユーザー］**に移動します。
2. リストからローカルユーザーを選択し、次のいずれかを実行します：
    - ツールバーオプションから **［パスワードの設定］**を選択します。

- **［詳細の表示］**をクリックして**［プロパティ］**を開き、**［認証］**タブで**［パスワードの設定］**を選択します。

3. **［パスワードの設定］**ダイアログで新しいパスワードを入力しします。
4. 次回ログイン時にパスワードの変更をユーザーに要求する場合は、**［ユーザーは次回のログイン時にパスワードを変更する必要があります］**チェックボックスが選択されていることを確認します。
5. **［パスワードの設定］**をクリックします。ダイアログで指定されたパスワード要件に準拠する必要があります。詳細については、「ローカルパスワードルール」を参照してください。
6. **［OK］**をクリックします。

ユーザーのアカウントのロック解除

ログインできない場合、アカウントが「ロック」されていて、無効になっている可能性があります。たとえば、アカウントのロックアウトしきい値設定で指定された最大回数、間違ったパスワードを入力すると、SPP がアカウントをロックします。詳細については、「ローカルログイン制御」を参照してください。

通常、管理者アカウントのロックを解除するのは権限許可者管理者です。管理者以外のローカルユーザーのロックを解除するのはユーザー管理者とヘルプデスク管理者です。

ユーザーのアカウントのロック解除方法

ユーザーアカウントのロック解除には、次の 2 つの方法があります：

1. **［ユーザー管理］＞［ユーザー］**を選択します。
2. リストから「ロックされた」ユーザーを選択します。
3. ツールバーオプションから**［ユーザーのロック解除］**を選択します。

12.2 ユーザーグループ

ユーザーグループについては、「ユーザーグループ」を参照してください。

12.3 設定

12.3.1 タイムゾーン

SPP は、セットアップを行う人の所在地に基づいて、デフォルトのタイムゾーンを設定します。タイムゾーンは UTC +または -時：分で表され、時間指定アクセスに使用されます（たとえば、アクセスを午前 9 時から午後 5 時までに制限するなど）。Bootstrap 管理者は、セットアップ時に希望するタイムゾーンを設定することをお勧めします。権限許可管理者も、タイムゾーンを変更することができます。

タイムゾーンの設定手順

1. **［ユーザー管理］＞［設定］＞［タイムゾーン］**の順に選択します。
2. 希望するタイムゾーンを検索して選択します。
3. **［ユーザーは、自分のタイムゾーンを変更できます］**設定を変更することができます。
    - この設定を有効にすると、ユーザーは自分のタイムゾーンを変更することができます（デフォルトは有効）。
    - この設定を無効にすると、ユーザーが自分のタイムゾーンを変更することを禁止することができます。

13 レポート

レポートでは、選択したユーザーがどの資産、アカウント、ユーザー、タグ、パーティションを管理しているかを示すレポートを表示およびエクスポートすることができます。レポートは、.csv または .json 形式でエクスポートすることができます。

レポートセクションには、次のサブページがあります。

- **アクティビティセンター**：アクティビティセンターは、特定のイベントまたはユーザーアクティビティの詳細を表示する場所です。アプライアンスは、SPP 内で実行されたすべてのアクティビティを記録します。管理者は誰でも監査ログ情報にアクセスできますが、管理者アクセス許可セットによって、アクセスできる監査データが決まります。
- **資格**：SPP は、以下の種類の資格レポートを提供します。詳細については、「資格レポート」を参照してください。

  > **メモ：** タブタイトルに表示される数字は、一意のユーザー、資産、アカウントの数を示しています。レポートの検索条件を入力すると、タブに表示される数はそれに応じて調整されます。

  - **ユーザー**：選択したユーザーがリクエストする権限を持つアカウントに関する情報が一覧表示されます。
  - **資産**： 選択した資産に関連付けられたアカウントと、それらのアカウントをリクエストする権限を持つユーザーに関する情報が一覧表示されます。
  - **アカウント**： 選択したアカウントをリクエストする権限を持つユーザーに関する詳細情報が一覧表示されます。資産、ポリシー、アクセスタイプ、パスワードを含む、パスワード変更、時間制限、有効期限、グループ、リンクアカウント、最終アクセス
- **所有権**：SPP は、次の所有権レポートを提供します。詳細については、「所有権レポート」を参照してください。

  > **メモ:** タブタイトルに表示される数字は、一意のユーザー、パーティション、資産、アカウント、タグの数を示しています。レポートの検索条件を入力すると、それに応じてタブに表示される数字が調整されます。

  - **ユーザー**：各所有者に基づく所有権に関する情報を一覧表示します。
  - **パーティション**：パーティションの所有権に関する情報を一覧表示します。
  - **資産**： 資産に対する所有権情報を一覧表示します。

- **アカウント**：アカウントの所有権情報を一覧表示します。
- **タグ**：タグに割り当てられた資産やアカウントの所有者に関する情報を一覧表示します。

13.1 アクティビティセンター

アクティビティセンターは、特定のイベントまたはユーザーアクティビティの詳細を表示するための場所です。アプライアンスは、SPP 内で実行されたすべてのアクティビティを記録します。管理者は誰でも監査ログ情報にアクセスできますが、管理者アクセス許可セットによって、アクセスできる監査データが決まります。詳細については、「管理者のアクセス許可」を参照してください。

アクティビティセンターページには、次のオプションがあります：

- **保存された検索の選択**：以前に保存された検索およびスケジュールされたレポートにアクセスし、管理することができます。
- **検索を保存またはスケジュール**：現在の検索条件を保存し、後でレポートを生成するために使用できます。詳細については、「検索条件の保存と保存済み検索条件の読み込み」を参照してください。
- **検索条件の消去**：現在の検索条件をデフォルト設定（過去 24 時間以内に発生したすべてのアクティビティ）にリセットします。
- **アクティビティカテゴリ**：このドロップダウンを使用して、カテゴリに基づいて検索対象のアクティビティをフィルタリングします。「すべてのアクティビティ」を選択すると、すべてのカテゴリが検索されます。
- **日付範囲**：このドロップダウンを使用して、検索する時間枠を指定します。

利用可能な検索フィールドを使用して、探している情報を取得するための追加のクエリ条件を指定します。詳しくは、「検索条件の適用」を参照してください。

アクティビティセンター 結果ツールバー

アクティビティ監査ログレポートが生成されると、結果セクションには、検索結果グリッドとこれらのツールバーオプションが含まれます。

- **詳細の表示**：結果を選択した後、このボタンをクリックすると、詳細が表示されます。

- **リクエストワークフローの詳細**：アクセスリクエストに関連する結果を選択した後、このボタンをクリックすると、そのリクエストのすべてのアクション（例：承認、パスワードのチェックアウト、セッションログ）の詳細が表示されます。
- **エクスポート**：表示された基準の .csv または .json ファイルを作成し、任意の場所に保存することを選択します。
- **更新**：検索結果ページを更新します。
- **検索**：文字列、または選択した属性から、条件を入力して検索することができます。選択した属性で検索するには、**［検索］**をクリックし、検索する属性を選択します。詳しくは、「検索ボックス」を参照してください。

13.1.1 検索条件の適用

アクティビティセンターのクエリビルダーを使用して、アクティビティ監査ログレポートにデータを追加および削除し、必要な情報を取得します。

デフォルトでは、アクティビティ監査ログレポートには、過去 24 時間以内に発生したすべてのアクティビティが含まれます。しかし、提供されるクエリオプションを使用して、検索条件を指定し、アクティビティ監査ログから特定の情報を取得することができます。利用可能な検索条件は以下のとおりです。

- **アクティビティカテゴリ**：このドロップダウンを使用して、パラメーターとイベントの詳細を絞り込みます。
- **日付範囲**：このドロップダウンを使用すると、時間、日、設定したカスタム時間枠で結果を絞り込むことができます。
- **ユーザー名**：このフィールドをクリックすると、ダイアログが開き、アクティビティレポートのユーザーを選択することができます。
- **資産名**：このフィールドをクリックすると、ダイアログが開き、アクティビティレポートの資産を選択することができます。
- **アカウント名**：このフィールドをクリックすると、ダイアログが開き、アクティビティレポートのアカウントを選択することができます。

監査ログに検索条件を適用する手順

アクティビティカテゴリと時間枠は、レポートを作成するために必要です。その他の検索条件は任意で、提供された正確なパラメーターにレポートを絞り込むことができます。

1. **［レポート］＞［アクティビティセンター］**の順に選択します。

2. **［アクティビティカテゴリ］**のデフォルトは、**「すべてのアクティビティ（概要のみ）」**です。ドロップダウンをクリックしてレポートを制限し、レポートに含めるアクティビティカテゴリを選択します。

3. **［日付範囲］**のデフォルトは**「過去 24 時間」**です。別の時間枠を指定するには、ドロップダウンをクリックし、レポートに含める時間枠を選択します。**［カスタム］**オプションを使用する場合、カスタムの日付と時間の範囲を指定します。

4. **［ユーザー名］**フィールドをクリックすると、ダイアログが開き、アクティビティレポートのユーザーを選択することができます。

5. 利用可能な場合、**［資産名］**フィールドをクリックすると、ダイアログが開き、アクティビティレポート用の資産を選択することができます。

6. **［アカウント名］**フィールドをクリックすると、ダイアログが開き、アクティビティレポート用のアカウントを選択することができます。

7. 選択した項目を削除するには、**［検索条件のクリア］**を使用して、検索をデフォルトに戻してください。

13.1.2 検索条件の保存と保存済み検索条件の読み込み

現在定義されている検索条件を保存して、後でアクティビティ監査ログレポートの作成に使用することができます。現在の検索条件は、アクティビティセンターのメインビュー（クエリビルダーのページ）または結果ビューから保存することができます。

現在の検索条件の保存手順

1. **［レポート］＞［アクティビティセンター］**の順に選択します。

2. 目的のレポートを作成するために使用する検索条件を指定します。詳細については、「検索条件の適用」を参照してください。

3. **［検索を保存またはスケジュール］**をクリックします。

4. **［スケジュール済みレポートを保存］**ダイアログで、次の情報を入力します。

   a. **名前**：検索の名前を入力します。

   b. **説明**：任意で、検索を説明するためのテキストを入力します。

c. **実行間隔**：デフォルトでは**「なし」**に設定されています。ドロップダウンから別のオプションを選択すると、追加の設定オプションが有効になります。詳細については、「アクティビティ監査ログレポートのスケジューリング」を参照してください。

5. **［OK］**をクリックします。

保存済みの検索条件の読み込手順

1. **［レポート］＞［アクティビティセンター］**の順に選択します。
2. **［保存された検索の選択］**をクリックします。
3. リストから保存済みの検索を選択します。
4. **［レポートをロード］**を選択します。
   選択した検索の検索条件がアクティビティセンターページに表示されます。

13.1.3 アクティビティ監査ログレポートの生成

アクティビティ監査ログレポートの生成手順

1. **［レポート］＞［アクティビティセンター］**の順に選択します。
2. クエリオプションを使用して、レポートの内容を指定します。デフォルトでは、監査ログは過去 24 時間以内に発生したすべてのアクティビティを返します。詳細については、「検索条件の適用」を参照してください。
3. デフォルトで表示される情報は、生成されたアクティビティレポートの種類によって異なります。結果リストの右上にある **［表示する列の選択］**を選択すると、表示される列を変更できます。

レポートが生成された後の操作

レポートが生成されると、次のグリッド上部のボタンを使用することができます。

- **詳細の表示**：結果を選択した後、このボタンをクリックすると、詳細なサマリーが表示されます。
- **リクエストワークフローの詳細**：アクセスリクエストイベントを選択し、このボタンをクリックすると、リクエストから承認、レビューまでのリクエストのワークフロ

ー中に発生したトランザクションを監査することができます。セッションリクエストの場合、リクエストワークフローダイアログから、記録されたセッションまたはライブセッションを再生することもできます。

- **エクスポート**：データを CSV または JSON で任意の場所にエクスポートする場合は、クリックします。CSV と JSON のどちらを選択したかに応じて、異なる情報が返される場合があります。例えば、JSON には検出されたアカウントの詳細が含まれますが、CSV にはアカウントの数のみが含まれます。詳しくは、「データのエクスポート」を参照してください。時刻は、ユーザーのタイムゾーンに従って設定されます。
- **更新**：詳細を閉じ、検索結果ページを更新します。
- **表示する列の選択**：このボタンを選択すると、グリッドに表示可能な列のリストが表示されます。レポートに含めるデータのチェックボックスを選択します。レポートから除外するデータのチェックボックスをオフにします。利用可能な追加カラムは、レポートに含まれるアクティビティの種類によって異なります。

13.1.4 アクティビティ監査ログレポートのスケジューリング

SPP では、アクティビティ監査ログレポートの生成をスケジュールすることができ、そのレポートはメールで送信されます。メール送信されるレポートは、選択した .csv または .json 形式の添付ファイルです。

アクティビティ監査ログレポートのスケジューリング

1. **［レポート］＞［アクティビティセンター］**の順に選択します。
2. クエリオプションを使用して、レポートの内容を指定します。デフォルトでは、監査ログは、過去 24 時間以内に発生したすべてのアクティビティを返します。詳細については、「検索条件の適用」を参照してください。
3. **［検索を保存またはスケジュール］**をクリックします。
4. **［スケジュール済みレポートを保存］**ダイアログで、以下の情報を入力します：
    a. **名前**：レポートの名前を入力します。
    b. **説明**：任意で、レポートの説明テキストを入力します。
    c. スケジュールを設定するには、以下のオプションを使用します：
        ◦ 時間枠を選択します。

［実行間隔］の頻度を入力し、次に、時間枠を選択します。

- **なし**：設定されたスケジュールに従ってジョブが実行されません。手動でジョブを実行することは可能です。
- **分**：指定した分単位の頻度でジョブが実行されます。たとえば、**実行間隔**を **30 分**に設定すると、24 時間にわたって 30 分ごとにジョブが実行されます。テストなどの特殊な状況を除いて、分単位の頻度は使用しないでください。
- **時間**：指定した時間から経過した分単位でジョブが実行されます。たとえば、午前 9 時 15 分から 2 時間おきに、正時 15 分にジョブを実行する場合は、**［実行間隔 = 2/時間/正時@分 = 15］**と設定します。
- **日数**：入力された日数と時間の頻度でジョブが実行されます。たとえば、隔週で真夜中の直前にジョブを実行するには、**［実行間隔 = 2/日数/開始 = 23:59:00］**と設定します。
- **週**：指定した時刻と曜日に、週の頻度でジョブが実行されます。たとえば、隔週で月、水、金の午前 5 時にジョブを実行する場合は、**［実行間隔 = 2 週/開始 = 5:00:00］**、**［次の日に繰り返し = 月曜、水曜、金曜］**と設定します。
- **月**：指定した時刻と曜日に月の頻度で実行されます。たとえば、隔月の第 1 土曜日の午前 1 時にジョブを実行する場合は、**［実行間隔 = 2 /月/開始 = 1:00:00/その月の曜日/First/Saturday］**と設定します。

- 開始時刻と終了時刻を入力する場合は、**［時間ウィンドウを使用］**を選択します。**＋［追加］**または **- ［削除］**をクリックして、複数の時間制限を制御することができます。各時間ウィンドウは、1 分以上の間隔が必要であり、重複しないようにしてください。たとえば、毎日 22 時から 2 時まで 10 分ごとにジョブを実行する場合、次の値を入力します**。［実行間隔 = 10/分］**、**［時間ウィンドウを使用］**を選択します。
  - 開始 22：00：00、終了 23：59：00
  - 開始 00：00：00、終了 2：00：00

開始 22:00:00 と 終了 2：00：00 と設定すると、終了時刻が開始時刻より後でなければならないというエラーが発生します。

［日数］、**［週］**、**［月］**を選択した場合は、入力した時間ウィンドウでジョブを繰り返す回数を選択できます。

隔日で 4 時から 20 時までの 10 時 30 分に 2 回実行するジョブの場合は、次の値を入力します。

日数には**［実行間隔 = 2/日数］**、**［時間ウィンドウを使用］**を選択し、**［開始 = 4:00:00/終了 = 20:00:00］**に設定し、**［繰り返し 2］**に設定します。

スケジューラがスケジュールされた時間内にタスクを完了できない場合、タスクの実行を終了すると、次の即時の時間間隔に再スケジュールされます。

5. **フィールド：**クリックするとダイアログが開き、結果に含めるフィールドを選択することができます。

6. **ソート基準**：クリックすると、ダイアログが開き、選択したフィールドのソート順を選択できます。

7. **レポートの送信先**：SPP クライアントに現在ログインしているユーザーのメールアドレスを表示する読み取り専用フィールドです。このフィールドは必須です。このフィールドが空白の場合、**［私のアカウント］**でメールアドレスを設定する必要があります。

8. **レポート形式：**CSV と JSON のどちらを選択したかに応じて、異なる情報が返される場合があります。例えば、JSON には検出されたアカウントの詳細が含まれますが、CSV にはアカウント数のみが含まれます。

9. **詳細レポート（すべてのアクティビティで有効ではありません）**：このチェックボックスを選択すると、より長い詳細なレポートが生成されます。

10. **［OK］**をクリックします。

13.1.5 保存済みの検索またはスケジュール済みのレポートの編集または削除

保存済みの検索またはスケジュール済みのレポートを編集または削除する手順

ツールバーの **［保存された検索の選択］**ボタンをクリックすると、保存済みの検索とスケジュール済みのレポートのリストが表示されます。このダイアログから、保存済みの検索またはスケジュール済みのレポートを検索、削除、編集することができます。

1. **［レポート］＞［アクティビティセンター］**の順に選択します。

2. **［保存された検索の選択］**をクリックします。**［保存された検索の選択］**ダイアログに保存された検索とスケジュールされたレポートのリストが含まれます。

3. リストから保存済みの検索またはスケジュール済みのレポートを選択します。

4. ツールバーボタンのいずれかをクリックします。

    - 保存済みの検索を削除する場合は、 **［削除］**をクリックし、確認ダイアログで**［はい］**をクリックします。
    - 保存済みの検索の名前と説明を変更するには、 **［編集］**をクリックし、**［編集］**ダイアログで**［スケジュール済みレポートを保存］**ダイアログを表示します。また、スケジュール済みのレポートのスケジュール設定を変更することもできます。
    - リストが更新する場合は、 **［更新］**をクリックします。

> **メモ：**検索を選択した後、ダブルクリックするか、**［レポートをロード］**ボタンをクリックすると、**［保存された検索の選択］**ダイアログが閉じられ、検索結果が表示されます。

13.1.6 イベントの詳細表示

一部のアクティビティイベントでは、追加の詳細情報を利用できます。

特定のイベントの詳細を表示する手順

1. イベントの詳細を表示するには、次のいずれかの方法を使用します。

    - イベントをダブルクリックします。
    - イベントを選択し、 **［詳細の表示］**をクリックします。

2. イベントの詳細ペインを閉じるには、**［閉じる］**をクリックします。

13.1.7 リクエストワークフローの監査

アクティビティのレビューに加えて、アクティビティセンターを使用して、リクエストから承認、レビューまでのリクエストワークフロープロセス中に発生したトランザクションを監査することができます。セッションリクエストの場合、資格のポリシーでセッションの記録が有効になっていれば、記録されたセッションまたはライブセッションを再生することもできます。

権限のあるレビュー担当者であれば、ホームページから、レビュー待ちの完了したアクセスリクエストのワークフローを監査することもできます。

リクエストワークフローの監査手順

1. **アクティビティセンター**を開き、クエリオプションを使用してレポートの内容を指定します。
2. アクセスリクエストイベントを選択して、**［リクエストワークフローの詳細］**をクリックすると、リクエストから承認、レビューまでのリクエストワークフローで発生したトランザクションが監査されます。
3. ポリシーでセッションの記録を有効にしているセッションリクエストの場合、ボタンをクリックすると、SPS 経由でイベントセッションログにアクセスできます。

13.1.8 レポート結果の並べ替え

グリッド見出し行のコントロールを使用して、レポート結果の並べ替えやデータ列の並べ替えを行います。列見出しの矢印は、情報の表示に使用されるソート基準および昇順または降順を表します。

列の並べ替え手順

1. ソート基準に使用する列の見出しをクリックします。
2. ソート順は昇順です。降順に変更する場合は、もう一度見出しをクリックします。

表示する列の変更手順

右上の **［表示する列の選択］**をクリックすると、グリッドに表示できる列のリストが表示されます。レポートに含めるデータのチェックボックスを選択します。レポートから除外するデータのチェックボックスをオフにします。利用可能な追加の列は、レポートに含まれるアクティビティの種類によって異なります。

13.2 資格レポート

資格レポートは、セキュリティポリシー管理者、監査人、アプリケーション監査人が実行できます。

資格レポートからデータをエクスポートする手順

1. **［レポート］＞［資格］**の順に選択します。
2. **資格** ページの上部にある、**［ユーザー］、［資産］、［アカウント］**タブを選択します。

   > **メモ：**タブタイトルに表示されている数字は、一意のユーザー、資産、アカウントの数を示しています。レポートの検索条件を入力すると、それに応じてタブに表示される数字が調整されます。

3. （任意）必要なフィルターを表に適用します。
4. リストされたすべての項目のデータをエクスポートするか、1 つの項目のデータをエクスポートするかを選択できます：
   - すべての項目のデータをエクスポートするには、ツールバーで **［エクスポート］**を選択します。
   - 単一の項目のデータをエクスポートするには、項目を選択し、**［詳細の表示］**をクリックします。詳細ダイアログから、**［エクスポート］**を選択します。
5. **エクスポート**ダイアログで、データを JSON ファイルまたは CSV ファイルとしてエクスポートするよう選択します。詳細は、「データのエクスポート」を参照してください。時刻は、ユーザーのタイムゾーンに従って設定されます。
6. **［エクスポート］**をクリックして、レポートファイルを生成します。

13.2.1 詳細なユーザー資格レポートのエクスポート

セキュリティポリシー管理者、監査人、アプリケーション監査人は、関連する各アカウントの詳細情報を含むユーザー資格レポートをエクスポートできます。

詳細なユーザー資格レポートのエクスポート手順

1. **［レポート］＞［資格］**の順に選択します。
2. 資格ページの上部から、**［ユーザー］**タブを選択します。

   > **メモ：**タブタイトルに表示されている数字は、一意のユーザーの数を示しています。レポートの検索条件を入力すると、それに応じてタブに表示される数字が調整されます。

3. （任意）必要なフィルタを表に適用します。

4. ボタンをクリックして、データを含む CSV ファイルをエクスポートします。

13.3 所有権レポート

所有権レポートを実行することができるのは、資産管理者、監査人、アプリケーション監査人です。

所有権レポートからデータをエクスポートする手順

1. **［レポート］＞［所有権］**の順に選択します。

2. **所有権**ページの上部で、**［ユーザー］、［資産］、［アカウント］、［パーティション］、［タグ］**のいずれかのタブを選択します。

   > **メモ：**タブタイトルに表示されている数字は、一意のユーザー、パーティション、資産、アカウント、タグの数を示しています。レポートの検索条件を入力すると、それに応じてタブに表示される数字が調整されます。

3. （任意）必要なフィルタをテーブルに適用します。

4. リストされたすべての項目のデータをエクスポートするか、1 つの項目のデータをエクスポートするかを選択できます。

   - すべての項目のデータをエクスポートするには、ツールバーで **［エクスポート］**を選択します。
   - 単一の項目のデータをエクスポートするには、リストされた項目を選択し、**［詳細を表示］**をクリックします。詳細ダイアログから、**［エクスポート］**を選択します。

5. エクスポートダイアログで、データを JSON ファイルまたは CSV ファイルとしてエクスポートするよう選択します。詳細については、「データのエクスポート」を参照してください。時刻は、ユーザーのタイムゾーンに従って設定されます。

6. **［エクスポート］**をクリックして、レポート ファイルを生成します。

14 ディザスタリカバリとクラスタ

SPP アプライアンスは、高可用性を確保するためにクラスタ化することができます。クラスタ化することで、自然災害や人為的な災害が発生した場合でも、重要な技術インフラやシステムの復旧や継続が可能になります。これにより、ダウンタイムとデータ損失が削減されます。

クラスタリングのもう 1 つの利点は、負荷分散です。管理対象ネットワークでクラスタリングすると、負荷が分散されるため、クラスタトラフィックを最小限に抑え、ターゲット資産に最も近いアプライアンスがタスクの実行に使用されるようになります。アプライアンス管理者は、クラスタリング環境における資産、アカウント、およびサービスのアクセスリクエストを効率的に管理するために、管理対象ネットワーク（ネットワークセグメント）を定義して、タスクの負荷を分散させます。

プライマリアプライアンスとレプリカアプライアンス

SPP のクラスタは、3 台または 5 台のアプライアンスで構成されます。アプライアンスは、1 つのクラスタにしか所属できません。クラスタ内の 1 つのアプライアンスは、プライマリとして指定されます。プライマリ以外のアプライアンスは、レプリカと呼ばれます。プライマリアプライアンスに保存されているすべての重要なデータは、レプリカにも保存されています。プライマリアプライアンスが機能しなくなるような災害が発生した場合、レプリカを新しいプライマリアプライアンスに昇格させることができます。ネットワーク構成は、プライマリまたはレプリカのいずれであっても、固有の各アプライアンスで行われます。

レプリカは、セキュリティポリシー設定の読み取り専用ビューを提供します。レプリカアプライアンスでは、オブジェクトやセキュリティポリシー構成を追加、削除、変更することはできません。パスワードと SSH キーの確認と変更、パスワードの設定、SSH キーの設定（インポートおよび生成の両方）を実行できます。ユーザーは、レプリカにログインして、アクセスのリクエスト、レポートの作成、データの監査を行うことができます。また、パスワード、SSH キー、セッションは、Safeguard クラスタ内のどのアプライアンスからもリクエストすることができます。

サポートされるクラスタ構成

現在サポートされているクラスタ構成は以下のとおりです。

- 3 ノードクラスタ（1 プライマリ、2 レプリカ）：3 台のアプライアンスのうち 2 台がオンラインであり、通信が可能な場合にコンセンサスが成立します。有効な状態は次のとおりです。Online または ReplicaWithQuorum。詳細については、「アプライアンスの状態」を参照してください。

- 5 ノードクラスタ（1 プライマリ、4 レプリカ）：5 台のアプライアンスのうち 3 台がオンラインかつ通信可能な状態になると、コンセンサスが達成されます。有効な状態は次のとおりです。有効な状態は、Online または ReplicaWithQuorum です。詳細については、「アプライアンスの状態」を参照してください。

コンセンサスとクォーラムの失敗

一部のメンテナンスタスクでは、クラスタがコンセンサス（クォーラム）を持つことが必要です。コンセンサスとは、大多数のメンバー（プライマリまたはレプリカアプライアンス）がオンラインであり、通信可能であることを意味します。有効な状態は次のとおりです。Online または ReplicaWithQuorum です。詳細については、「アプライアンスの状態」を参照してください。

サポートされているクラスタは、アプライアンスの数が奇数であるため、クラスタのコンセンサスが 50%以上のアプライアンスがオンラインであり、通信可能な状態であることを意味します。

クラスタがコンセンサスを失うと（クォーラム障害とも呼ばれる）、以下が自動的に発生します。

- プライマリアプライアンスは読み取り専用モードになります。
- パスワードと SSH キーのチェックと変更は無効になります。

クラスタ内の大多数のメンバー間で接続性が回復すると、コンセンサスが自動的に回復します。コンセンサスメンバーにプライマリアプライアンスが含まれている場合、自動的に読み書きモードに変換され、パスワードのチェックと変更が可能になります。

ヘルスチェックと診断

以下のツールを使用して、クラスタとアプライアンスのヘルスチェックを実行し、診断することができます。

- ヘルスチェックを実行して、クラスタの正常性とアプライアンスの状態を監視します。詳細については、「クラスタメンバーの保守と診断」を参照してください。
- クラスタとアプライアンスを診断します。アプライアンス情報の表示、診断テストの実行、ネットワーク設定の表示と編集、およびサポートバンドル生成の各機能を使用できます。詳細については、「クラスタメンバーの診断」を参照してください。
- 診断パッケージをアップロードする必要があるが、UI または API にアクセスできない場合は、管理 Web キオスク（MGMT）に接続します。MGMT 接続では、サポートバンドルの抽出やアプライアンスの再起動など、認証なしで機能にアクセスできるため、アクセスはできるだけ少数のユーザーに制限する必要があります。

アプライアンスのシャットダウンと再起動

アプライアンスをシャットダウンして再起動することができます。

- アプライアンスのシャットダウン：詳細については、「アプライアンスのシャットダウン」を参照してください。
- アプライアンスの再起動：詳細については、「アプライアンスの再起動」を参照してください。

オフラインワークフローモードで切り離されたアプライアンスでアクセスリクエストワークフローを実行する

自動または手動でオフラインワークフローモードを有効にすると、クォーラムを持たなくなったアプライアンスが、クラスタの残りから分離してキャッシュされたポリシーデータを使用してアクセスリクエストを処理するよう強制することができます。アプライアンスはオフラインワークフローモードになります。

- オフラインワークフローモードの一般的な情報については、「オフラインワークフローモードとは」を参照してください。
- オフラインワークフローを手動で有効にしたり、オンラインワークフローを手動で再開したりするには、「オフラインワークフローモードの手動制御」を参照してください。
- オフラインワークフローモードを自動的に設定し、オプションでオンラインワークフローを自動的に再開するには、「オフラインワークフロー（自動）」を参照してください。自動化がオンになっている場合でも、オフラインワークフローモードを手動で制御することは可能です。

プライマリアプライアンスの障害：フェイルオーバーとバックアップの復元

プライマリが通信できない場合、手動でフェイルオーバーを実行します。それが不可能な場合、バックアップを使用してアプライアンスを復元できます。

- フェイルオーバー：プライマリが通信していない場合、クォーラム（過半数にコンセンサス）があれば、手動でフェイルオーバーを実行することができます。詳細については、「レプリカを新しいプライマリに昇格させることによるフェイルオーバー」を参照してください。
- バックアップリストア：フェイルオーバーを使用してリストアできるアプライアンスがない場合、バックアップリストアを実行します。詳細については、「クラスタ化されたアプライアンスを復元するためのバックアップの使用」を参照してください。

参加解除とアクティベーション

クラスタアプライアンスが通信可能な場合、レプリカの参加を解除してから、プライマリをアクティブにしてレプリカを参加できるようにすることができます。

- どの状態でもレプリカの参加を解除し、スタンドアロン読み取り専用モード（StandaloneReadOnly 状態）にすることができます。詳細については、「クラスタからのレプリカの参加解除」を参照してください。
- 他の Safeguard クラスタで管理されていない場合、参加を解除してスタンドアロン読み取り専用モード（StandaloneReadOnly 状態）にしたアプライアンスをアクティブにすることができます。詳細については、「読み取り専用アプライアンスの有効化」を参照してください。

クラスタリセット

アプライアンスがオフラインの場合、またはクラスタメンバーが通信できない場合は、**[クラスタのリセット]**を使用してクラスタを再構築する必要があります。クラスタから削除する必要があるアプライアンスがあるが、安全に参加を解除できるクォーラムがない場合、クラスタリセットはクラスタからノードを強制的に削除します。詳細については、「コンセンサスが失われたクラスタのリセット」を参照してください。

ファクトリーリセット（工場出荷時へのリセット）

大きな問題から回復するため、またはハードウェアアプライアンスのデータと構成設定をクリアするために、ファクトリーリセットを実行します。すべてのデータと監査履歴が失われ、ハードウェアアプライアンスはメンテナンスモードになります。

ファクトリーリセットは、以下から実行できます：

- リカバリキオスク：詳細については、「リカバリキオスクからの工場出荷時リセット」を参照してください。
- 仮想アプライアンスのサポートキオスク：詳細については、「サポートキオスク」を参照してください。

14.1 レプリカのクラスタへの登録

アプライアンス管理者がクラスタメンバーを SPP クラスタに登録する前に、次の登録に関する注意事項を確認してください。

14.1.1 クラスタメンバーを登録する際の考慮点

- オフラインワークフローモードのアプライアンスがある場合、別のレプリカを追加する前にオンライン操作を再開してください。詳細については、「オフラインワークフローモードとは」を参照してください。
- クラスタを構築する前に、すべてのアプライアンスを同じアプライアンスビルドに更新（パッチ）してください。クラスタパッチ操作中、アクセスリクエストワークフローが利用できるので、許可されたユーザーはパスワードおよび SSH キーのリリースとセッションアクセスをリクエストすることができます。
- アプライアンスをクラスタに登録するには、アプライアンスがポート 655 UDP およびポート 443 TCP で通信し、IPv4 または IPv6 ネットワークアドレスを持つ必要があります（混在不可）。IPv4 と IPv6 の両方が接続可能な場合は、IPv6 が使用されます。詳細については、「Safeguard ポート」を参照してください。
- レプリカアプライアンスのクラスタへの登録は、プライマリアプライアンスにログインしているとき（アプライアンス管理者権限を持つアカウントを使用しているとき）にのみ行うことができます。
- 一度に追加できるアプライアンスは 1 台のみです。レプリカを追加する前に、メンテナンス操作が完了している必要があります。
- レプリカの登録には、レプリケートするデータの量やネットワークに応じて、最短で 5 分、最長で 24 時間かかることがあります。
- レプリカを登録する操作の間、レプリカアプライアンスはメンテナンスモードに移行します。クラスタの既存のメンバーは、メンバーがクォーラムを持っている限り、アクセスリクエストを処理できます。プライマリアプライアンスでは、クラスタビューのステータスバーに、クラスタ全体の操作が進行中であることを示す登録中通知が表示されます。このクラスタロックにより、追加のメンテナンス操作を行うことができなくなります。
- メンテナンス操作（レプリカの登録操作）が完了すると、クラスタビューの図（左ペイン）にコネクタのリンクレイテンシが表示されます。クラスタのアプライアンスはロックが解除され、ユーザーは再び SPP で利用できる機能を使用できるようになります。

  > **ヒント**: アクティビティセンターには、登録プロセスの開始と完了のイベントが含まれます。

- プライマリアプライアンスのオブジェクトとセキュリティポリシー構成は、クラスタ内のすべてのレプリカアプライアンスにレプリケートされます。レプリカで定義されたオブジェクト（ユーザー、資産など）またはセキュリティポリシー構成は、登録中に削除されます。プライマリの既存の構成データは、登録時にレプリカにレプリケートされま

す。プライマリで今後行われる設定変更は、すべてのレプリカにレプリケートされます。

レプリカの登録手順

1. レプリカをクラスタに登録する前に、プライマリアプライアンスのバックアップを作成することをお勧めします。
2. プライマリアプライアンスにアプライアンス管理者としてログインします。
3. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に選択します。
4. SPP アプライアンスをクラスタに参加させるには、＋**［レプリカの追加］**をクリックします。
5. **［レプリカの追加］**ダイアログで、ネットワーク DNS 名またはレプリカアプライアンスの IP アドレスを**ネットワークアドレス**フィールドに入力し、**［接続］**をクリックします。
6. Web ブラウザがレプリカのログインページにリダイレクトされます。二要素認証を含め、通常通りログインします。ログインに成功すると、Web ブラウザは、Web クライアントにリダイレクトされます。
    a. アプライアンス管理者権限を持つ有効なアカウントを入力します。
    b. **［レプリカの追加］**ダイアログで**［レプリカの追加］**と入力し、**［OK］**をクリックして操作を続行します。

    SPP は、登録するアプライアンスの横に（同期アイコン）と（ロックアイコン）を表示し、レプリカアプライアンスをメンテナンスモードにして、クラスタに登録します。

    クラスタ内のすべてのアプライアンスで、クラスタビューの上部に「レプリカを登録しています」バナーが表示され、クラスタ全体の操作が進行中であること、クラスタ内のすべてのアプライアンスがロックされていることが示されます。
7. メンテナンス操作（レプリカの登録操作）が完了すると、アプライアンスをクリックしてリンクレイテンシーを確認します。クラスタ内のアプライアンスはロックが解除され、ユーザーは再びアクセスリクエストを行うことができます。
8. レプリカアプライアンスにアプライアンス管理者としてログインしてください。

    アプライアンスの状態がレプリカ（読み取り専用モードであることを意味する）であり、プライマリアプライアンスで定義されたオブジェクトとセキュリティポリシー構成が含まれていることに注意してください。

14.2 クラスタからのレプリカの参加解除

SPP では、アプライアンス管理者がレプリカアプライアンスをクラスタから参加解除することができます。SPP クラスタからレプリカを参加解除する前に、次の参加解除に関する考慮事項を確認してください。

14.2.1 クラスタメンバーの参加を解除する際の注意事項

- クラスタから参加解除できるレプリカアプライアンスは 1 つだけです。
- レプリカを新しいプライマリに昇格させてから「古い」プライマリアプライアンスを参加解除するには、クラスタにコンセンサス（アプライアンスの大部分がオンラインで通信可能）がある場合、フェイルオーバーオプションを使用することができます。詳細については、「レプリカを新しいプライマリに昇格させることによるフェイルオーバー」を参照してください。クラスタにコンセンサスがない場合は、クラスタリセットオプションを使用してクラスタを再構築します。詳細については、「コンセンサスが失われたクラスタのリセット」を参照してください。
- 参加解除操作を実行するには、参加解除するレプリカアプライアンスはどのような状態でもかまいません。ただし、クラスタの残りのアプライアンスはコンセンサス（オンラインかつ通信可能な状態）である必要があります。
- レプリカアプライアンスの参加解除は、クラスタ内のオンライン状態にあるアプライアンスに、アプライアンス管理者権限を持つアカウントでログインしているときに実行できます。
- クラスタのレプリカアプライアンスを参加解除すると、そのアプライアンスは、参加解除前に含まれていたすべてのデータとセキュリティポリシー設定情報を保持したまま、スタンドアロンアプライアンスとしてクラスタから削除されます。レプリカが参加解除された後、アプライアンスは、読み取り専用モードの機能で特定された機能を備えた読み取り専用モードになります。読み取り専用モードのアプライアンスをアクティブにして、データの追加、削除、変更、アクセスリクエストのワークフローの適用などを行うことができます。詳細については、「読み取り専用アプライアンスの有効化」を参照してください。

クラスタからレプリカを参加解除する手順

1. クラスタ内のアプライアンスに、アプライアンス管理者としてログインします。
2. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に選択します。

3. リストからクラスタから参加を解除するレプリカノードを選択します。
4. **［参加解除］**をクリックします。
5. **参加解除**ダイアログで、**「参加解除」**と入力し、**［OK］**をクリックして続行します。

   SPP は、参加を解除するアプライアンスの横に（同期アイコン）と（ロックアイコン）を表示し、クラスタから参加を解除する間、レプリカアプライアンスをメンテナンスモードにします。

   操作が完了すると、レプリカアプライアンスはクラスタビューには表示されなくなります。

SPP が参加解除操作を処理している間に、レプリカアプライアンスにログインすると、「メンテナンス」モード画面が表示されます。メンテナンスモードの最後に、参加解除が正常に完了したことを示すボタンが表示されます。

14.3 クラスタメンバーの保守と診断

クラスタ管理からクラスタメンバーを保守、診断します。

［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］の順に選択します。

クラスタビューでノードを選択すると、ペインの右側に選択したアプライアンスの詳細が表示されます。このペインから、選択したアプライアンスに対して、以下の保守および診断タスクを実行できます。

- **参加解除**：クリックすると、クラスタからレプリカが削除されます。詳細については、「クラスタからのレプリカの参加解除」を参照してください。
- **フェイルオーバー**：クリックすると、レプリカがプライマリアプライアンスに昇格されます。詳細については、「レプリカを新しいプライマリに昇格させることによるフェイルオーバー」を参照してください。
- ✳ **アクティブ化**：クリックすると、読み取り専用のアプライアンスがアクティブになり、データの追加、変更、削除ができるようになります。詳細については、「読み取り専用アプライアンスの有効化」を参照してください。

  > ⚠ **注意: 読み取り専用モードのアプライアンスをアクティブ化すると、読み取り専用状態から解除され、管理アカウントのパスワードおよび SSH キーの確認と変更が可能になります。他の SPP アプライアンスがこれらのアカウントをアクティブに監視していないことを確認してください。**

- **診断**： クリックすると、診断ペインが開き、以下を実行することができます。

- アプライアンス情報の表示：詳細については、「アプライアンス情報」を参照してください。
- アプライアンスに対して診断テストを実行する：詳細については、「ネットワーク診断」を参照してください。
- ネットワーク設定の表示または編集：詳細については、「ネットワーク」を参照してください。
- 工場出荷時リセットの実行：詳細については、「工場出荷時リセット」を参照してください。
- OS ライセンスの確認（仮想マシンのみ）：詳細については「オペレーティングシステムのライセンス」を参照してください。
- パッチの更新：詳細については「パッチの更新」を参照してください。
- アプライアンスの電源オフと再起動：詳細については「電源」を参照してください。
- サポートバンドルの作成：詳細については、「Support Bundle」を参照してください。
- 時間設定の表示または編集：詳細については「時間」を参照してください。

- **正常性の確認**：クリックすると、選択したアプライアンスの現在の状態がキャプチャして表示されます。
- **再起動**：クリックすると、選択したアプライアンスが再起動されます。**[理由]** を入力し、**[再起動]** をクリックして、意図を確認します。

クラスタに関するより深刻な問題を解決するために、クラスタメンバーの状態に応じて追加の操作を実行することができます。追加の操作には次のようなものがあります。

- クラスタメンバーへのパッチ適用
- クラスタ化されたアプライアンスを復元するためのバックアップの使用
- 工場出荷時リセットの実行
- コンセンサスが失われたクラスタのリセット
- オフラインワークフローモードとは

14.3.1 オフラインワークフローモードとは

特権アカウントのパスワードの一貫性と個々のアカウンタビリティを確保するために、アプライアンスがクラスタ内でコンセンサスを失うと、アクセスリクエストが無効になります。ネットワ

ークパーティションが拡張された場合、アプライアンス管理者は、自動的または手動でアプライアンスをオフラインワークフローモードにし、そのアプライアンス上でクラスタの残りから分離してアクセスリクエストワークフローを実行することができます。ネットワークの問題が解決され、接続性が再確立されると、アプライアンス管理者は自動的または手動でオンライン操作を再開して、監査ログをマージし、インフライトアクセスリクエストを削除し、アプライアンスをクラスタの完全参加に戻すことができます。

オフラインワークフローの考慮事項

- オフラインワークフローモードでは、アプライアンスはクラスタの他のメンバーから分離して機能します。ユーザーはパスワードとセッションをリクエストすることができます。
- オフラインワークフローの設定は、個々のアプライアンスで設定されます。
- サスペンド/リストアアカウントは、オフラインワークフローモードでは機能しません。

オフラインワークフローモードのパスワードと SSH キー

- オフラインワークフローモードでは、アプライアンスはキャッシュされたポリシーデータを使用して、クォーラムなしでパスワード、SSH キー、セッションをリクエスト、承認、およびリリースすることが可能になります。
- オフラインワークフローモードでは、チェックイン後にポリシーの変更が必要な場合、その要件はバイパスされ、その後のチェックアウトを可能にします。この場合、アクセスリクエストパスワードまたは SSH キーのリセットバイパスイベントが生成され、次のように表示されます。「パスワード（または SSH キー）のリセットがバイパスされたため、アクセスリクエストの後続のチェックアウトが可能になりました。」
- パスワードと SSH キーの変更は再スケジュールされ、アプライアンスがオフラインのワークフローモードであっても、ネットワーク接続が回復したときに完了する可能性があります。
- ユーザーは、プライマリまたはクラスタ上の別のレプリカからパスワードまたは SSH キーをコンセンサスでリクエストすることができます。その結果、オフラインワークフローモードを実行しているアプライアンスでパスワードまたは SSH キーが同期されなくなることがあります。これは予想される動作です。パーティションが回復するまでパスワードは同期されないままです。
- 1 つまたは複数のアプライアンスがオフラインワークフローモードにあるネットワークパーティションでは、2 人の個人が同時に同じパスワードと SSH キーを持つことが可能

です。アクションを 1 人の責任者に関連付けることはできません。それでも、その時点でパスワードにアクセスできた各個人を特定することは可能です。

オフラインワークフローモードのポリシー

- 現在オフラインワークフローモードにあるアプライアンスが、クラスタの残りとのネットワーク接続を失った時点で存在していたポリシーが適用されます。
- チェックイン後にパスワードと SSH キーの変更をリクエストするポリシーはバイパスされ、オフラインワークフローモードのアプライアンスからのその後のチェックアウトが許可されます。
- ポリシーは読み取り専用です。したがって、オフラインワークフローモードのアプライアンスでは、更新および削除の構成操作は許可されません。
- ポリシーの変更は、クラスタ内のオンラインプライマリに向けられた場合にのみ許可されます。オンラインプライマリでのポリシー変更は、オフラインワークフローモードのアプライアンスに影響を与えません。オフラインワークフローアプライアンスがオンライン操作を再開すると、ポリシーの変更が配布されます。

オフラインワークフローモードのワークフロー

- 通常のワークフロー承認ルールが適用されます。
- 時間ベースの制約と緊急アクセスが適用されます。
- アプライアンスがオフラインワークフローモードに切り替わる、またはオフラインワークフローモードから切り替わる数分間、アプリケーションからアプリケーション、およびコマンドラインパスワードまたは SSH キーのフェッチ操作は中断されます。
- オフラインワークフローモードでは、プラットフォームタスク（アカウントの一時停止と復元を含む）が無効になります。

ユーザーエクスペリエンス：オフラインワークフローモードの有効化

Safeguard でパスワードと SSH キーをリクエストしているユーザーは、ホームページに戻されます。オフラインワークフローモードに切り替える前のパスワードと SSH キーのリクエストは表示されません。

- オフラインワークフローモードへの切り替えが開始されると、次のようなメッセージが表示されます：⚠ Safeguard はオフラインワークフローモードに切り替わっています。このプロセスが完了するまで、現在の作業を続行する前にお待ちください。ホームページの下部には、この情報が表示されます：（オフラインワークフローモードに切り替わ

っています...）と 切断されました。ユーザーが［更新］をクリックすると、バナーは次のように切り替わります：サービスをご利用いただけません。

- オフラインワークフローモードへの切り替えが完了すると、このような情報を含むバナーが表示されます：Safeguard は現在オフラインワークフローモードです。以前のアクセスリクエストは一時的に利用できません。オフラインワークフローモードで作業を継続するために、新しいリクエストを送信することができます。ホームページの下部には、次のメッセージが表示されます:（オフラインワークフローモード）と接続状態：接続中、接続済みの順に表示されます。

管理者は、**クラスタビュー**ペインでワークフローの状態を確認することができ、次のようなメッセージが表示されます：オフラインワークフロー有効（このアプライアンスは、クラスタから分離してアクセスワークフローを実行しています。）詳細については「クラスタ管理」を参照してください。

ユーザーエクスペリエンス：オンライン操作の再開

オンライン操作の再開への切り替えが開始されると、次のメッセージが表示されます：Safeguard は通常のオペレーションに戻ります。このプロセスが完了するまで、現在の作業を続行する前にお待ちください。ホームページの下部には、この情報が表示されます:（通常の操作に戻る）と 切断されました。

オンライン操作が回復すると、ホームページの下部に次の情報が表示されます：接続済

通知

- アプライアンスがコンセンサス（クォーラム）を失った場合、アプライアンス管理者に ApplianceStateChangedEvent で通知されます。
    - プライマリは、Online から PrimaryNoQuorum に変更されます。
    - レプリカは、Online から次のいずれかに変更されます。
        - ReplicaNoQuorum （プライマリに接続されているが、クォーラムを持っていない）
        - ReplicaDisconnected （プライマリから切断され、クォーラムを持っていない）
        - ReplicaWithQuorum （プライマリから切断されているが、クォーラムを保持している）

    詳細については、「アプライアンスの状態」を参照してください。
- 以下のイベントは、メール通知の設定が可能で、監査ログに書き込まれます。
    - ClusterPrimaryQuorumLostEvent

    - ClusterPrimaryQuorumRestoredEvent
    - ClusterReplicaQuorumLostEvent
    - ClusterReplicaQuorumRestoredEvent
- すべてのアクセスリクエストの通知は引き続き生成されます。
- 通知サービスは、IsPasswordRequestAvailable および IsSessionsRequestAvailable プロパティを介して、アプライアンスでアクセスワークフローが利用可能かどうかを識別します。次の API エンドポイントを使用して、この判定を行うことができます。

  https://<ホスト名または IP>/service/notification/v3/Status/Availability

オフラインワークフローモードでの監査ログ

- ネットワーク接続が復元される前に、オフラインワークフローモードで実行中のアプライアンスで発生したすべてのことは、そのアプライアンスでのみ監査されます。
- 監査ログは、オフラインワークフローモードであっても、オフラインメンバーとクラスタの他のメンバーとの間のネットワーク接続が復元されると結合（マージ）されます。
- オフラインワークフローモードで動作しているクラスタメンバーの監査データは、オンライン操作の再開の手順を使用してアプライアンスをクラスタに戻さない限り失われます。
- クラスタ全体の監査履歴を維持するために、アクセスおよびセッションのリクエストを処理できるすべてのクラスタメンバーは、クラスタの残りへのネットワーク接続を復元する必要があります。

クラスタ構成への変更を避ける

- アプライアンスがオフラインワークフローモードである間は、クラスターメンバーシップを変更しないことをお勧めします。アプライアンスをクラスタにシームレスに再統合できるように、他のノードを追加または削除する前に、オンライン操作を自動的または手動で再開する必要があります。

  アプライアンス管理者は、個々のパスワードまたは SSH キーの説明責任、ポリシーの遵守、および監査の完全性のために、できるだけ早くオンライン操作を再開することが推奨されます。

クラスタパッチの適用が許可されない

クラスタパッチ中は、クラスタアプライアンスでオフラインワークフローモードを手動または自動でトリガすることはできません。

オンライン操作を再開するための考慮事項

- ネットワークパーティションは、完全な機能でオンライン操作を再開する前に修正する必要があります。
- オフラインワークフローモードにあるアプライアンスのオンライン操作をクォーラムなしで再開することができます。オンライン操作を再開するには、オフラインワークフローモードのメンバーを含むクラスタメンバーの大多数間でネットワーク接続を復元することが強く推奨されます。
- オンライン操作を再開すると、オフラインワークフローモードで動作しているアプライアンスで進行中のアクセスリクエストはすべてドロップされます。
- アプライアンスが接続されていない場合、オンライン操作を再開することは可能ですが、アクセスリクエストを作成することはできなくなります。

自動ワークフローと手動ワークフロー

- オフラインワークフローモードの自動トリガーおよびオンラインワークフローの自動再開を設定できます。詳細については、「オフラインワークフロー（自動）」を参照してください。
- 手動でオフラインワークフローモードを有効にし、手動でオンラインワークフローを再開することができます。

オフラインワークフローモードの手動制御

アプライアンス管理者は、以下の手順でオフラインワークフローモードを手動で制御できます。手動による介入は、自動的なオフラインワークフローモードが有効になっている場合に可能です。詳細については、「オフラインワークフロー（自動）」を参照してください。

オフラインワークフローモードを手動で有効化する手順

1. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に移動します。
2. オフラインになっているクラスタのメンバーをクリックします。
3. アプライアンスの詳細とクラスタの正常性ペイン（右ペイン）で、エラーと警告を確認し、アプライアンスのコンセンサスが失われたことを確認します。

4. オフラインのアプライアンスで、**［オフラインワークフローの有効化］**をクリックします。（このオプションは、アプライアンスがクラスタとのコンセンサスを失った場合にのみ利用可能です）。

   次のようなメッセージが表示されます：

   アプライアンスはクラスタから独立してアクセスワークフローを実行し、クラスタとのコンセンサスが失われるのを回避します。ユーザーはキャッシュされたデータを使用してこのアプライアンスからパスワードおよびセッションのリクエスト、承認、リリースを行うことができます。接続が復元されたらオンライン操作を再開し、このアプライアンスをクラスタと再統合して監査ログをマージする必要があります。詳細は、管理者ガイドを参照してください。

   下のボックスに「オフラインワークフローの有効化」と入力してください。

   詳細については、KB263580 を参照してください。

5. ダイアログで、「**オフラインワークフローの有効化**」と入力し、**［Enter］**を押します。アプライアンスはオフラインワークフローモードになり、メンテナンスに入ります。アクティビティセンターで、アプライアンスのイベントが**［オフラインワークフローの有効化の開始］**から**［オフラインワークフローの有効化済み］**になります。

6. 新しいリクエストが有効になっていることを確認し、**クラスタ管理**ウィンドウで次の正常性チェックを表示することができます。

   - オフラインワークフローモードのメンバーに接続しているときに、クラスタの他のメンバーとの通信がある場合、メッセージの先頭に次のようなメッセージが表示されます：クラスタ接続が検出されました。通信が再確立されると、アプライアンスに対するオンライン操作を手動で再開することができます。
   - オフラインワークフローモードのアプライアンスの横に、⚠ 警告アイコンが表示されます。クラスタの他のメンバーから見た場合、そのメンバーがオフラインワークフローモードにあるメンバーと通信できない場合は、✖ エラーアイコンが表示されます。いつでも ♥ **［正常性の確認］**をクリックして、情報を更新できます。
   - 次のような警告メッセージが表示されます。ワークフローをリクエストします：このアプライアンスのアクセスワークフローは、クラスタからオフラインで分離されて動作しています。この警告は、アプライアンス管理者によってオンライン操作が再開されるまで継続されます。

手動でオンライン操作を再開する手順

オンライン操作を再開する前に、「オンライン操作を再開するための考慮事項」を参照してください。

1. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に移動します。
2. オフラインになっているクラスタのメンバーをクリックします。
3. オフラインワークフローモードのアプライアンスで、**［オンライン操作の再開］**をクリックします（この操作は、アプライアンスがオフラインワークフローモードの場合にのみ利用可能です）。

   次のようなメッセージが表示されます：

   アプライアンスはオンライン操作用に再設定されます。アプライアンスはクラスタとの再統合と監査ログの結合を試みます。詳細については、管理者ガイドを参照してください。

   下のボックスに「オンライン操作の再開」と入力してください。
4. ダイアログで、**「オンライン操作の再開」**と入力し、**［Enter］**を押します。
5. メンテナンスが完了したら、**［再起動］**をクリックします。アプライアンスがメンテナンスモードに戻ります。
6. **クラスタ管理**ウィンドウで正常性を確認することができます。アプライアンスの横にまだ⚠警告アイコンが表示されている場合、アプライアンスを選択して♥**［正常性の確認］**をクリックすると、クラスタの正常性確認が再実行され、最新の正常性情報が表示されます。

14.3.2 レプリカを新しいプライマリに昇格させることによるフェイルオーバー

SPP では、レプリカアプライアンスを新しいプライマリに昇格させることでフェイルオーバーすることができます。

> **メモ：**レプリカを新しいプライマリに昇格させることは、クラスタのコンセンサス（クラスタノードの大半がオンラインであり、通信可能な状態）であればいつでも可能です。クォーラムに障害が発生した場合（つまり、クラスタメンバーの過半数がコンセンサスを得られなかった場合）、代わりにクラスタのリセットを実行する必要があります。詳細については、「コンセンサスが失われたクラスタのリセット」を参照してください。

クラスタでレプリカを新しいプライマリに昇格させる手順

1. 正常なクラスタメンバーにアプライアンス管理者としてログインします。
2. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に選択します。
3. 新しくプライマリにするレプリカノードを選択します。
4. **［フェイルオーバー］**をクリックします。
5. **フェイルオーバー**ダイアログで、**「フェイルオーバー」**と入力し、**［OK］**をクリックして次に進みます。

   フェイルオーバー操作の間、クラスタ内のすべてのアプライアンスはメンテナンスモードになります。

   フェイルオーバー操作が完了すると、選択したレプリカアプライアンスがプライマリとして表示され、オンライン状態になります。クラスタの（「古い」プライマリを含む）他のすべてのアプライアンスは、オンライン状態のレプリカとして表示されます。

14.3.3 読み取り専用アプライアンスの有効化

SPP クラスタから参加解除された、またはバックアップからリストアされたアプライアンスは、読み取り専用モードになります。

読み取り専用モードのアプライアンスをアクティブにして、データの追加、削除、変更、アクセスリクエストのワークフローの適用などを行うことができます。

有効化タスクを使用するには、読み取り専用モードのアプライアンスがオンラインである必要があります。オフラインの場合、またはクラスタにコンセンサスがない場合（つまり、残りのメンバーの大半がオフライン/通信不能の場合）、クラスタリセットオプションを使用してクラスタを再構築する必要があります。詳細については、「コンセンサスが失われたクラスタのリセット」を参照してください。

> ⚠ **注意: 読み取り専用モードのアプライアンスをアクティブにすると、読み取り専用状態が解除され、管理アカウントのパスワードの確認と変更が可能になります。他の SPP アプライアンスがこれらのアカウントをアクティブに監視していないことを確認してください。**

読み取り専用アプライアンスの有効化手順

1. アプライアンス管理者として読み取り専用アプライアンスにログインします。

2. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に移動します。

   クラスタビューにプライマリアプライアンスが 1 台表示され、アプライアンスが読み取り専用モードであることを示す黄色の警告アイコンが表示されます。

3. アクティブ化する読み取り専用ノードを選択します。

4. ✳**［アクティブ化］**をクリックします。

5. **アクティブ化**ダイアログで、**「アクティブ化」**と入力し、**［OK］**をクリックして次に進みます。

   クラスタビューのアプライアンスのノードには、黄色の警告アイコンが表示されなくなり、状態はオンラインになります。

14.3.4 クラスタメンバーの診断

診断ツールは、アプライアンス管理者または操作管理者が、現在接続しているアプライアンスと、クラスタ内のその他のアプライアンス（レプリカ）に対して使用できます。

クラスタ化されたアプライアンスで診断を実行する手順

1. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**を選択します。

2. 診断するアプライアンスを選択します。

3. **［診断］**をクリックします。

4. **［ネットワーク診断］**を選択します。

5. 実行するテストの種類を選択し、手順を完了します。

   - **ARP**：アドレス解決プロトコル（ARP）を使用して、インターフェイス、インターネットアドレス、物理アドレス、およびタイプ（動的または静的）を検出します。
   - **Netstat**： Netstat を使用して、アクティブな接続プロトコル、ローカルアドレス、外部アドレス、およびステートを表示します。
   - **NSLookup**：ドメイン名または IP アドレスを取得します。
   - **Ping**：ネットワークの接続性と応答時間を確認します。
   - **ルートの表示**：ルーティングテーブルの情報を表示します。

- **Telnet**：インターネットのような TCP/IP ネットワーク上のリモートコンピューターにアクセスします。
- **スループット**：クラスタ内の他のアプライアンスへのスループットをテストします。
- **ルートの追跡（Trace Route）**：ルーター情報を取得します。ある IP アドレスから別の IP アドレスへのパケットの経路を決定します。

14.3.5 クラスタメンバーへのパッチ適用

アプライアンスの更新がリリースされたら、クラスタ内のすべてのアプライアンスが同じバージョンになるようにパッチを適用します。SPP がクラスタパッチプロセス中にアクセスリクエストとシステム障害を処理する方法の詳細については、「クラスタパッチ適用について」を参照してください。

クラスタに更新パッチをインストールする前に

- クラスタ内のすべてのアプライアンスがオンラインであり、正常であることを確認します。警告や問題がある場合は、クラスタパッチを適用する前に対処しておく必要があります。クラスタメンバーのいずれかが正常でない、または連絡できない場合、パッチインストールプロセスは失敗します。

  > **重要**：プライマリアプライアンスはクラスタのアップグレードをオーケストレーションするため、プライマリアプライアンスはオンライン状態を維持し、クラスタ内のすべてのレプリカアプライアンスとネットワーク接続されている必要があります。これが合理的に保証できない場合は、レプリカアプライアンスをクラスタから外し、個別にアップグレードしてから、クラスタに再登録する必要があります。

- パッチを適用する前に、プライマリアプライアンスのバックアップを取ることを強くお勧めします。詳細については、「バックアップと復元」を参照してください。
- バックアップアプライアンスとして使用するために、クラスタからレプリカをアンインストールすることもできます。致命的な障害が発生した場合、参加していないレプリカをプライマリとしてアクティブにすることができます。クラスタパッチプロセスが成功したら、参加していないレプリカをアップグレードし、クラスタに再登録します。

クラスタ内のアプライアンスにパッチを適用する手順

1. プライマリアプライアンスに、アプライアンス管理者としてログインします。

2. **［アプライアンス管理］＞［アプライアンス］＞［パッチの更新］**の順に選択します。

3. **［ファイルのアップロード］**をクリックし、更新ファイルを選択して開きます。

   パッチがアップロードされ、クラスタ内のすべてのアプライアンスに配布されます。

   > **メモ：** パッチがステージングされている間に、新しいレプリカを追加するなどクラスタに変更を加えた場合、パッチインストールプロセスを開始する前に、更新ファイルを新しいクラスタメンバーに配布する必要があります。SPP は、すべてのクラスタメンバーが更新ファイルをローカルに保存していることをレポートするまで、パッチインストールプロセスの開始を許可しません。

   > **メモ:** 配布プロセス中に**［キャンセル］**ボタンをクリックすると、レプリカへの更新ファイルの配布が停止されます。この時点で、次のボタンのいずれかをクリックできます。
   >
   > - **［削除］**は、クラスタ内のすべてのアプライアンスから更新ファイルを削除します。
   > - **［クラスタに配布］**は、クラスタ内の各レプリカに更新ファイルの配布を続行します。

4. クラスタ内のすべてのレプリカにファイルが正常に配布されたら、**［今すぐインストール］**ボタンをクリックします。

   プライマリアプライアンスはメンテナンスモードに移行し、更新操作を開始します。プライマリアプライアンスが正常に更新されると、SPP は各レプリカに対して一度に 1 つずつ更新操作を実行します。更新操作中は、他のクラスタ操作が更新操作に干渉しないように、クラスタがロックされます。すべてのクラスタメンバーで更新操作が完了すると、クラスタは自動的にロックが解除され、通常の操作が再開できるようになります。

   クラスタビュー（**[アプライアンス管理］＞［クラスタ］＞［クラスタ管理]**）には、更新操作が進行中であることと、ロックされ更新ファイルのインストールを待機しているクラスタメンバーが表示されます。

   また、**パッチの更新**ビュー（**[アプライアンス管理］＞［アプライアンス］＞［パッチの更新]**）には、更新操作に関与しているクラスタメンバーと、クラスタメンバーが正常に更新されるまでの経過が表示されます。

クラスタパッチ適用について

次の情報は、SPP がクラスタパッチ適用プロセス中にアクセスリクエストを処理する方法について説明するものです。また、クラスタパッチ適用プロセス中にクラスタメンバーが電源やネットワーク接続を失った場合に何が起こるかについても説明します。

サービスの保証

クラスタの更新中、クラスタは現在のバージョン（サイド A）と更新バージョン（サイド B）に論理的に分割されます。アクセスリクエストのワークフローは、一度に片側でのみ有効になります。監査ログは両側で実行され、クラスタのパッチが完了するとマージされます。初期状態では、アクセスリクエストワークフローはサイド A でのみ有効であり、PatchPending 状態のレプリカはアクセスリクエストを実行できます。アプライアンスがアップグレードされ、サイド B に移動すると、サイド B にアプライアンスの過半数がある場合、アクセスワークフローはサイド B に移行されます。アップグレードプロセスのこの時点で、PatchPending 状態のレプリカはアクセスリクエストを実行できなくなりますが、アップグレードされたすべてのクラスタメンバーはアクセスリクエストを実行することができます。データが片側からもう片側に移行するため、アクセスリクエストのワークフローが利用できない小さなウィンドウがあります。

故障のシナリオ

更新処理中にプライマリアプライアンスの電源が切れたりネットワーク接続が切れたりした場合は、再起動時に更新を再開しようとします。

更新処理中にレプリカの接続が切れたり電源が切れたりした場合、そのレプリカはほとんどの場合、隔離モードになります。プライマリアプライアンスはそのアプライアンスをスキップし、クラスタから削除します。このレプリカを回復するには、リセット、更新、クラスタへの再登録を手動で行う必要があります。

パスワードと SSH キーのチェックアウトの構成

パスワードまたは SSH キーの再度チェックアウトを行う前に、パスワードのリセットを行うようにポリシーが構成されている場合があります。この場合、パスワードがリセットされていないときにパスワードのチェックアウトを許可するように、クラスタのパッチ適用とアクセスリクエストの前に、一時的に次のように構成することができます。

- 複数のアクセスを許可するようにポリシーを設定することができます。
- チェックイン時にパスワードまたは SSH キーの変更をリクエストしないようにポリシーを設定することができます。

- パスワードまたは SSH キーのリセットを待つ必要がないように、緊急リクエストを許可することができます。

14.3.6 クラスタ化されたアプライアンスを復元するためのバックアップの使用

クラスタ環境では、クラスタバックアップの目的は、アクセスリクエストワークフロー、ユーザー/アカウント、監査ログなど、すべての運用データを保存し、復元できるようにすることです。クラスタ内のすべてのアプライアンス（プライマリとレプリカ）をバックアップすることができます。ただし、アプライアンスにバックアップをリストアするのは、フェイルオーバー操作でどのアプライアンスもリストアできない最悪のシナリオの場合のみにしてください。

バックアップがアプライアンスにリストアされると、プライマリでのリストアはプライマリのクラスタ構成をクリアしますが、レプリカのクラスタ構成は変更されません。問題を回避するために以下を行ってください：

1. 可能であれば、バックアップの復元前に、レプリカをクラスタから参加解除してください。
2. プライマリでクラスタバックアップをパスワードまたは GPG キーで暗号化するように設定されている場合、アップロードとリストア操作を完了するには、パスワードまたは GPG 秘密鍵が必要です。詳細については、「バックアップの保護設定」を参照してください。
3. プライマリとなるアプライアンスでバックアップをアップロードおよび復元します。
4. バックアップの復元前にレプリカを参加解除しなかった場合は、各レプリカでクラスタのリセットを実行してスタンドアロンにしてから、レプリカをクラスタに結合してください。

アプライアンスは、レプリカを使用しない読み取り専用モードのスタンドアロンプライマリアプライアンスとしてリストアされます。ただし、バックアップの取得時に存在したすべてのアクセスリクエストワークフロー、ユーザー/アカウント、および監査ログデータは保持されます。このプライマリアプライアンスをアクティブにして、レプリカを結合してクラスタを再作成することができます。

物理アプライアンスのバックアップを取る手順

1. アプライアンス管理者としてアプライアンスにログインします。

2. **［アプライアンス管理］＞［バックアップと保持］＞［バックアップと復元］**の順に選択します。

3. 必要に応じて、バックアップの実行、バックアップのスケジュール設定、プライマリからのクラスタ用バックアップの暗号化などを行います。詳細については、「バックアップと復元」を参照してください。

バックアップから物理アプライアンスを復元する手順

アプライアンス管理者は、SPP バージョン 6.0.0.12276 までのバックアップを復元することができます。データのみがリストアされ、実行中のバージョンは変更されません。

アプライアンスで実行中のバージョンより新しいバージョンからバックアップをリストアすることはできません。リストアは失敗し、次のようなメッセージが表示されます。「バックアップバージョン [バージョン] は現在実行中のものよりも新しいのです。リストアに失敗しました。」

バックアップバージョンと実行中のバージョンは、Safeguard がリストアを開始、完了、または失敗したときに生成されるアクティビティセンターのログに表示されます。

> **メモ:** 別のアプライアンスで取得したバックアップファイルを使用する場合、そのバックアップファイルはまず、バックアップを取得したアプライアンスでダウンロードする必要があります。ダウンロードされたバックアップファイルは、復元オプションを使用する前に、それを使用するアプライアンスにアップロードする必要があります。

1. アプライアンス管理者として、復元するアプライアンスにログインします。

2. **［アプライアンス管理］＞［バックアップと保持］＞［バックアップと復元］**の順に選択します。

3. 使用するバックアップを選択し、**［復元］**をクリックします。

   復元ダイアログが表示されたら、**「復元」**と入力し、**［OK］**をクリックします。問題のある状態が検出された場合、バックアップの復元に関する警告が、「復元の警告」「警告 X of X」メッセージの詳細とともに表示されます。**［キャンセル］**をクリックして復元プロセスを停止して警告に対処するか、**［続行］**をクリックして次の警告（ある場合）に進むか、プロセスを完了します。

4. バックアップがパスワードで保護されている場合は、**保護されたバックアップのパスワード**ダイアログが表示されます。**［バックアップパスワードの入力］**テキストボックスにパスワードを入力します。詳細については、「バックアップの保護設定」を参照してください。

5. **復元**ダイアログが表示されたら、**「復元」**と入力し、**［OK］**をクリックします。詳細については、「バックアップの復元」を参照してください。

アプライアンスは、レプリカを使用しない読み取り専用モードのスタンドアロンプライマリアプライアンスとしてリストアされます。

クラスタの再構築手順

1. アプライアンス管理者としてプライマリアプライアンスにログインします。
2. 読み取り専用のプライマリアプライアンスをアクティブにします。
    a. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**に移動します。
    b. **クラスタ**ビューからアクティブ化するノードを選択します。
    c. ✳**［アクティブ化］**をクリックします。
    d. アクティブ化の操作を確認します。

    詳細については、「読み取り専用アプライアンスの有効化」を参照してください。
3. 一度に 1 つずつ、レプリカアプライアンスを登録してクラスタを再構築します。
    a. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に選択します。
    b. ＋**［レプリカの追加］**をクリックして、レプリカアプライアンスをクラスタに参加させます。

    登録操作が完了したら、これを繰り返して、アプライアンスをレプリカとしてクラスタに再び追加します。

    > **メモ：**レプリカの登録は、レプリケートするデータの量やネットワークに応じて、最大で 24 時間かかることがあります。

    詳細については、「レプリカのクラスタへの登録」を参照してください。

14.3.7 コンセンサスが失われたクラスタのリセット

クラスタ構成をリセットすることで、コンセンサスを失ったクラスタを回復することができます。接続が回復した後にクラスタのコンセンサスが回復すると、プライマリは読み書きモードに戻り、パスワードと SSH キーのチェックと変更が再び有効になります。ただし、コンセンサスが回復しない場合、アプライアンス管理者はクラスタのリセットを実行して、クラスタからノードを強制的に削除する必要があります。

ネットワークの問題が懸念される場合は、新しいプライマリアプライアンスのみでクラスタをリセットしてください。クラスタリセット操作が完了したら、アプライアンスを 1 台ずつ登録して新しいクラスタを作成します。

> ⚠ **注意：クラスタのリセットは最後の手段です。クラスタをリセットするのではなく、バックアップから復元することをお勧めします。**

注意事項

問題を回避するために、以下の注意事項を考慮してください。

- クラスタのリセットは、コンセンサスが失われたことが確実な場合のみ行ってください。そうでない場合、スプリットブレインシナリオが発生する可能性があります（スプリットブレインシナリオとは、クラスタがより小さなクラスタに分割されることです。これらの小さなクラスタはそれぞれ、自分だけがアクティブなクラスタであると思い込み、同じデータにアクセスし、データの破損を引き起こす可能性があります）。
- どのクラスタメンバーもオフラインワークフローモードを有効にしていないことを確認します。詳細については、「オフラインワークフロー（自動）」を参照してください。

クラスタのリセット手順

1. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に選択します。
2. **［クラスタのリセット］**ボタンをクリックします。

   クラスタのリセットダイアログが表示され、クラスタのアプライアンス（プライマリとレプリカ）が一覧表示されます。
3. **クラスタのリセット**ダイアログで、リセット操作に含めるノードを選択し、**［新しいプライマリ］**を選択して、クラスタのプライマリアプライアンスを指定します。

   > **メモ：**リセット操作に含めるノードは、アプライアンスの状態がオンラインまたはオンライン読み取り専用であり、通信可能である必要があります。オンラインでない、または利用できないノードを選択した場合、エラーが発生し、リセット操作は失敗します。
4. **［クラスタのリセット］**をクリックします。
5. 確認ダイアログで**「クラスタのリセット」**と入力し、**［OK］**をクリックします。

   新しいプライマリアプライアンスに接続すると、SPP アプライアンスの進捗ページが表示され、クラスタをリセットするためのメンテナンスタスクの一部として実行されている手順が表示されます。

6. メンテナンスタスクが完了したら、**［再起動］**をクリックします。

7. アプライアンスがスタンドアロンアプライアンスとしてクラスタリセットされた場合、StandaloneReadonly モード（オンラインではない）になり、スプリットブレインシナリオを回避するためにアクティベーションが必要になります。詳細については、「読み取り専用アプライアンスの有効化」を参照してください。

リセットされると、クラスタにはリセット操作に含まれたアプライアンスのみが含まれます。

14.3.8 工場出荷時リセットの実行

アプライアンス管理者は、工場出荷時リセット機能を使用して、SPP アプライアンスをリセットして重大な問題から回復したり、アプライアンスのデータと構成設定をクリアしたりすることができます。物理アプライアンスの工場出荷時リセットは、Web クライアント、Recovery Kiosk、サポートキオスク、API から開始することができます。

SPP の仮想アプライアンスは、工場出荷時リセットではなく、再展開のための復元手順によってリセットされます。詳細については、「仮想アプライアンスのバックアップと復元」を参照してください。

> ⚠ **注意 この操作により、すべてのデータと監査履歴が削除され、工場から最初に出荷されたときの状態に戻るため、物理アプライアンスに対して工場出荷時リセットを実行するときは、注意が必要です。工場出荷時リセットの実行は、BMC/IPMI インターフェイスや IP アドレスをリセットしません。ただし、リセットの完了後、BMC/IPMI インターフェイスを再度有効にする必要があります（詳細については、「ライトアウト管理（BMC）」を参照してください）。アプライアンスは、工場から出荷時と同じように、再度設定を行う必要があります。詳細については、「SPP の初期設定」を参照してください。**
>
> **さらに、工場出荷時のリセットを実行すると、デフォルトの SSL 証明書とデフォルトの SSH ホスト鍵が変更される場合があります。**
>
> **アプライアンスは、現在の Long Term Support（LTS）バージョンにリセットされます。たとえば、バージョン 6.6（機能リリース）または 6.0.6 LTS（メンテナンスロングタームサポートリリース）を使用している場合に工場出荷時リセットを行うと、アプライアンスは 6.0 LTS にリセットされ、現在のバージョンにパッチアップする必要があります。詳細については、「長期サポート（LTS）とフィーチャーリリース」を参照してください。**

クラスタ化されたアプライアンスの工場出荷時リセット

クラスタ化されたハードウェアアプライアンスで工場出荷時リセットを実行しても、アプライアンスはクラスタから自動的に削除されません。推奨されるベストプラクティスは、アプライアンスで工場出荷時リセットを実行する前に、クラスタからアプライアンスを参加解除することです。参加解除と工場出荷時リセットの後、アプライアンスを再度構成する必要があります。詳細については、「SPP の初期設定」を参照してください。

工場出荷時リセットを実行する手順

1. **［アプライアンス管理］＞［アプライアンス］＞［工場出荷時リセット］**の順に移動します。
2. **［工場出荷時リセット］**をクリックします。
3. **工場出荷時リセット**ダイアログで、**「工場出荷時リセット」**と入力し、**［OK］**をクリックします。

   アプライアンスを元に戻すために、メンテナンスモードに入ります。アプライアンスがクラスタにあった場合、工場出荷時リセットアプライアンスを参加解除する必要がある場合があります。工場出荷時リセットのアプライアンスを再度構成する必要があります。詳細については、「SPP の初期設定」を参照してください。さらに、アプライアンスにログインすると、SPP ライセンスを追加するよう促されます。

Recovery Kiosk から工場出荷時リセットを実行する手順

> ⚠ **注意：工場出荷時リセットプロセスの一環として、チャレンジレスポンス操作を行うことになります。チャレンジレスポンスの無効化を避けるため、ページを移動したり更新したりしないでください。**
>
> **チャレンジレスポンス操作が無効になった場合、プロセスを再起動して新しいチャレンジレスポンスを生成してみてください。それができない場合、One Identity Support に連絡してください。**

1. ハードウェアの工場出荷時リセットを実行するには、Recovery Kiosk に移動します。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。
2. **［工場出荷時リセット］**を選択します。
3. 右矢印を押します。
4. **［id］**で、メールまたは名前を入力し、**［Tab］**キー（または下矢印）を押します。

5. **［Get Challenge］**で、**［Enter］**キーを押します。SPP からチャレンジが出力されます。(チャレンジが表示されない場合は、Putty を最大化してください)。

6. チャレンジをコピーして貼り付け、One Identity Support に送信してください。チャレンジ応答の有効時間は 48 時間です。

   チャレンジ応答操作中にページから移動したり、更新したりしないでください。そうすると、チャレンジ応答が無効になり、プロセスを再開する必要があります。

7. One Identity Support から応答が届いたら、応答を Kiosk 画面にコピーして貼り付け、**［出荷時リセット］**を選択します。応答は、One Identity によって生成されてから 24 時間のみ有効です。

8. 工場出荷時リセットが完了すると、アプライアンスを再設定する必要があります。

MGMT ネットワークインターフェイスを使用した工場出荷時リセットの詳細については、次のナレッジベース記事 KB 232766 を参照してください。

サポートキオスクから工場出荷時リセットを実行する手順

> ⚠ **注意：工場出荷時リセットプロセスの一環として、チャレンジレスポンス操作を行うことになります。チャレンジレスポンスの無効化を避けるため、ページを移動したり更新したりしないでください。**
>
> **チャレンジレスポンス操作が無効になった場合、プロセスを再起動して新しいチャレンジレスポンスを生成してみてください。それができない場合、One Identity Support に連絡してください。**

1. ハードウェアの工場出荷時リセットを実行するには、Web 管理コンソールで、**［サポートキオスク］**をクリックします。詳細については、「サポートキオスク」を参照してください。

2. **［工場出荷時リセット］**を選択します。（このオプションは、仮想マシンのコンソールに接続されている場合は使用できません。このオプションはハードウェアに対してのみ利用可能です）。

3. チャレンジ/レスポンスプロセスを完了します：

   a. **フルネームまたはメール**に、チャレンジの質問を受け取るための名前またはメールを入力します。

   b. **［チャレンジの取得］**をクリックします。

   c. チャレンジの応答を取得するには、次のいずれかを実行します（以下の図を参照）。

- **［チャレンジをコピー］**をクリックします。チャレンジがクリップボードにコピーされます。そのチャレンジを Safeguard サポートに送信します。サポートから、48 時間有効のチャレンジ応答が返送されます。画面を更新しないでください。
- QR コードをスクリーンショットして、サポートに送信します。サポートから 48 時間有効なチャレンジの回答が返送されます。画面を更新しないでください。
- 携帯電話の QR コードリーダーを使用して、チャレンジレスポンスを取得します。

4. One Identity Support から回答を得たら、回答をコピーしてキオスク画面に貼り付け、**［工場出荷時リセット］**を選択します。

14.3.9 ロックされたクラスタのロック解除

一貫性と安定性を維持するために、一度に実行できるクラスタ操作は 1 つだけです。これを確実にするために、SPP は、登録、未接続、フェイルオーバー、パッチ、リセット、および定期メンテナンスなどのクラスタ操作の実行中、クラスタをロックします。クラスタビューには、クラスタがロックされ、操作が完了するまでクラスタ構成への変更が許可されません。ロックは、アプライアンスの横にある赤いロックアイコン（🔒）で通知されます。

SPP の参加解除、フェイルオーバー、クラスタのリセット、復元、パッチ、IP アドレスの更新では、決してクラスタロックを解除しないでください。

その他、以下について考慮してください：

- SPP への参加（登録）に時間がかかっている場合は、監査データのストリーミングステップ中にそれをキャンセルすることができます。
- パッチの配布に時間がかかっている場合は、配布をキャンセルしてレプリカに直接パッチをアップロードすることができます。
- 監査ログの同期処理に時間がかかっている場合、またはクラスタ内のアプライアンスのダウンにより同期処理が完了しないと思われる場合は、その処理をキャンセルできます。この操作をキャンセルするには、「監査ログメンテナンス」ページの「監査ログメンテナンスのキャンセル」で詳しく説明されているように、監視が必要です。
- 監査ログアーカイブまたはパージ操作に長い時間がかかっている場合、またはクラスタ内のアプライアンスのダウンにより完了しないと思われる理由がある場合、この操作をキャンセルすることができます。この操作をキャンセルするには、「監査ログメンテナンス」ページの「監査ログメンテナンスのキャンセル」の詳細に従って監視する必要があります。

ロックされたクラスタをロック解除手順

1. **［アプライアンス管理］＞［クラスタ］＞［クラスタ管理］**の順に移動します。
2. 警告バナーの右上隅にある 🔒 ロックアイコンをクリックします。
3. **クラスタのロック解除**ダイアログで**「クラスタのロック解除」**と入力し、**［OK］**をクリックします。

   これにより、クラスタ内のすべてのアプライアンスにかけられたクラスタロックが解除され、操作が終了します。

> **重要**: ロックされたクラスタのロックを解除する際には、注意が必要です。クラスタ内の 1 つ以上のアプライアンスがオフラインで、現在の操作が終了されないことが確実な場合にのみ使用するようにしてください。クラスタのロックを強制的に解除すると、アプライアンスが不安定になり、工場出荷時のリセットが必要になり、クラスタの再構築が必要になる場合があります。実行中の操作に確信が持てない場合は、クラスタのロックを解除しないでください。多くの場合、最終的にタイムアウトになり、勝手にロックが解除されます。

14.4 トラブルシューティングのヒント

SPP クラスタに問題がある場合は、次のガイドラインに従ってください：

1. ハードウェアの電源が入り、オンラインになっていることを確認します。
2. ネットワークに問題がないか確認します。詳細については、「クラスタメンバーの診断」を参照してください。
3. すべてのクラスタ操作がログに記録されるので、アクティビティセンターのイベントを確認します。エラーおよび警告は、それ自体で解決される場合があります。エラーが 15 分以上続く場合は、おそらく自然には解決しません。アプライアンスを再起動し、エラーまたは警告が解消されるかどうかを確認します。
4. One Identity サポートに連絡してください。
    - アプライアンスが隔離モードになった場合、リカバリキオスクに接続し、サポートに連絡します。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。
    - クラスタの各アプライアンスについてサポートバンドルを生成および収集し、サポートに連絡します。詳細については、「Support Bundle」を参照してください。

14.4.1 アプライアンスの状態

次の表は、アプライアンスの状態と、アプライアンスが特定の状態にあるときに利用可能なアクションを一覧にしています。

表：アプライアンスの状態

アプライアンスの状態と説明	利用可能なアクション
EnrollingReplica（クラスタ内のレプリカアプライアンスにのみ適用されます。） レプリカアプライアンスをクラスタに追加中で、アクセスできない過渡的な状態。この状態から、アプライアンスはメンテナンスモー	操作が完了するまで待ってから、アプライアンスにログインしてください。

アプライアンスの状態と説明	利用可能なアクション
ドに移行して、登録操作を完了します。	
Initial Setup Required 仮想アプライアンスはデプロイされていますが、オンライン状態になるまで使用することはできません。	仮想アプライアンスをオンライン状態に移行させるには、アプライアンス管理者が初期セットアップを実行する必要があります。詳細については、「仮想アプライアンスのセットアップ」を参照してください。
Initializing アプライアンスを起動するために初期化を行っているが、まだアクセスできない過渡的な状態	アプライアンスにログインする前に、操作が完了するのを待ちます。
メンテナンス アプライアンスはメンテナンスタスクを実行中で、アクセスはできません。	メンテナンスタスクが完了するまで待ってから、アプライアンスにログインしてください。
LeavingCluster（クラスタ内のレプリカアプライアンスにのみ適用されます） レプリカアプライアンスがクラスタから参加解除され、アクセスできなくなる過渡的な状態です。この状態から、アプライアンスはメンテナンスモードに移行して、参加解除操作を完了します。	操作が完了するのを待ってから、アプライアンスにログインしてください。
オフライン アプライアンスはアクセスに利用できません。	アプライアンスがオンラインに戻るのを待ってから、ログインしてください。
オフラインワークフロー アプライアンスはクラスタと通信していませんが、アクセスリクエストワークフローを実行するために、自動または手動でオフラインワークフローモードに設定されています。	オフラインワークフローモードを有効にします。オンライン操作が再開されると、アプライアンスはメンテナンスモードに戻されます。詳細については、「オフラインワークフローモードとは」を参照してください。

アプライアンスの状態と説明	利用可能なアクション
オンライン アプライアンスはプライマリであり、コンセンサスを得ている、またはアプライアンスがレプリカで、コンセンサスとプライマリへの接続性の両方がある	アプライアンスにログインする。 この状態では、オンラインかつ通信可能なすべてのクラスタ化されたアプライアンスから、アクセスリクエストワークフローを利用できます。
PatchPending（クラスタ内のレプリカアプライアンスにのみ適用されます） クラスタパッチの際、プライマリアプライアンスは、すべてのレプリカに PatchPending 状態になるよう指示します。プライマリアプライアンスは次にパッチを適用し、完了すると、PatchPending 状態のレプリカにパッチを 1 つずつインストールするよう指示します。	PatchPending 状態のレプリカにログインすることができます。 当初は PatchPending 状態のレプリカでアクセスリクエストワークフローを実行できますが、クラスタのアップグレード中にクラスタメンバーの大半がアップグレードされると、アクセスリクエストワークフローはクラスタの PatchPending 側からクラスタのアップグレード側に移行されます。この間、PatchPending 状態にあるアプライアンスでは、アクセスリクエストワークフローは利用できません。
PrimaryNoQuorum（クラスタ内のプライマリアプライアンスにのみ適用されます。） プライマリアプライアンスは、リースの取得を試みている間、読み取り専用モードになっていますが、クラスタにコンセンサスがないため、取得することができません。アプライアンスはリースの取得を試み続け、取得すると、アプライアンスの状態はオンラインに戻ります。	アプライアンスの電源が入っている場合、PrimaryNoQuorum 状態のアプライアンスにログインすることはできますが、読み取り専用モードとなります。 この状態では、アクセスリクエストワークフローはプライマリアプライアンスからは利用できませんが、クラスタ内の他のアプライアンスからは利用できる可能性があります。 たとえば、プライマリがクラスタ内の他のノードと通信できないが、他のノードはノード間で通信できる場合（ReplicaWithQuorum 状態）、アクセスリクエストワークフローは、プライマリアプライアンスからは利用できなくても、これらのレプリカアプライアンスからは利用できるようになります。
隔離 アプライアンスが故障しているか、不明な状態にある。	復旧には手作業が必要です。

アプライアンスの状態と説明	利用可能なアクション
	リカバリキオスクにアクセスして回復します。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。
ReplicaDisconnected（クラスタのレプリカアプライアンスに適用されます） レプリカアプライアンスはアクセス可能ですが、次の両方の条件が適用されます。 ◦ レプリカアプライアンスは、クラスタ内のプライマリアプライアンスと通信できません。 ◦ レプリカアプライアンスが通信できるクラスタ内の残りのノードにコンセンサスがない。	ReplicaDisconnected 状態のレプリカにログインすることはできますが、アクセスリクエストワークフローは無効となります。 レプリカアプライアンスがクラスタ内の他のノードと通信できないが、残りのノードが互いに通信できる場合、通信できないアプライアンスからは利用できなくても、それらのアプライアンスからはアクセスリクエストワークフローが利用できます。
ReplicaNoQuorum（クラスタ内のレプリカアプライアンスに適用されます） レプリカアプライアンスはプライマリアプライアンスと通信できますが、クラスタ内の残りのノードはコンセンサスに達していません。クラスタがコンセンサスを回復すると、レプリカアプライアンスはオンライン状態になります。	ReplicaNoQuorum 状態のレプリカにログインすることはできますが、アクセスリクエストワークフローは無効となります。 この状態では、アクセスリクエストワークフローはプライマリアプライアンスからは利用できませんが、他のレプリカからは利用できる可能性があります。 たとえば、5 台のアプライアンスからなるクラスタにおいて、プライマリと 1 台のレプリカはクラスタの残りのレプリカと通信できませんが、クラスタの他の 3 台のレプリカは相互に通信できる場合（ReplicaWithQuorum 状態）、アクセスリクエストワークフローは、プライマリと通信できないレプリカから利用できなくても、オンラインかつ通信できるレプリカから利用できるようになります。

アプライアンスの状態と説明	利用可能なアクション
	ReplicaWithQuorum 状態のレプリカにログインすることができます。この状態では、オンラインかつ通信可能な任意のクラスタアプライアンスからアクセスリクエストワークフローを利用できます。パスワードのリクエストとチェックインが可能です。スケジュールされたタスクは、クラスタのパッチ適用が完了するまで発生しません。手動によるチェックと変更は利用できません。
ReplicaWithQuorum（クラスタ内のレプリカアプライアンスに適用されます） レプリカアプライアンスはプライマリアプライアンスと通信できませんが、クラスタ内の残りのノードはコンセンサスに達しています。	パスワードの再チェックアウトを行う前にパスワードのリセットが必要なようにポリシーが構成されている場合があります。その場合、クラスタパッチとアクセスリクエストの前に以下を一時的に設定することで、パスワードがリセットされていない場合にパスワードのチェックアウトを可能にすることができます。 • 複数のアクセスを許可するようにポリシーを設定することができます。 • チェックイン時にパスワードの変更を要求しないようにポリシーを設定することができます。 • パスワードがリセットされるのを待つ必要がないように、緊急リクエストを許可することができます。
TransitioningToPrimary（クラスタ内のレプリカアプライアンスにのみ適用） レプリカアプライアンスが新しいプライマリに昇格され、アクセスできない過渡的な状態。	操作が完了するのを待ってからアプライアンスにログインしてください。
TransitioningToReplica（クラスタ内のプライマリアプライアンスにのみ適用されます） プライマリアプライアンスがレプリカに降格され、アクセスできない過渡的な状態	操作が完了するのを待ってから、アプライアンスにログインしてください。

アプライアンスの状態と説明	利用可能なアクション
シャットダウンしています アプライアンスがシャットダウンしており、アクセスできない過渡的な状態	アプライアンスがオンラインに戻るのを待ってから、ログインしてください。
StandaloneReadOnly クラスタから結合されていないレプリカ、またはバックアップから復元されたプライマリアプライアンスに使用される状態。アプライアンスを起動することができます。	アプライアンスにログインします。 データの追加、削除、変更、アクセスリクエストワークフローの適用などができるように、読み取り専用アプライアンスをアクティブにする方法については、「読み取り専用アプライアンスの有効化」を参照してください。
不明 アプライアンスが壊れているか、不明な状態にあります。	復旧には手作業が必要です。 リカバリキオスクで復旧してください。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。
HardwareSecurityModuleError アプライアンスは、復号化のために構成されたハードウェアセキュリティモジュールにアクセスできなくなりました。この状態は、スタートアップ時または 4 時間ごとに実行される接続チェック時にのみ発生します。スタートアップ中、ハードウェアセキュリティモジュールへの接続にエラーが発生すると、アプライアンスがこの状態に移行します。接続チェックの間、ネットワークの問題によってアプライアンスがこの状態に移行することはありません。	ハードウェアセキュリティモジュールに関連するすべてのアクションを利用できます。これには、Hardware Security Module のクライアントおよびサーバー証明書の管理、Hardware Security Module 構成の更新、クラスタの健全性チェックの実行、Hardware Security Module 検証の実行が含まれます。 アプライアンスが復号化できる有効な構成が存在する場合、アプライアンスはこの状態から移行し、次のいずれかを実行します。 • 次の接続チェックが実行されます（4 時間ごと）。 • クラスタメンバーの正常性チェック、またはハードウェアセキュリティモジュールの外部統合メニューの更新より、ハードウェアセキュリティモジュールの検証が実行されます。

15 管理者のアクセス許可

お客様の IT 部門の資産（つまり管理対象システム）の制御を確保するために、SPP はロールベースのアクセス制御階層を使用します。SPP のさまざまなアクセス許可セットは、各タイプのユーザーが持つコントロールの量を制限します。

> **メモ:** 他の SPP ユーザーに管理者アクセス許可を付与することができるのは、権限許可者のアクセス許可を持つユーザーですが、ユーザー管理者は管理者ではないユーザーに Help Desk 管理者アクセス許可を付与することができます。

管理者アクセス許可には以下のものがあります：

- アプライアンス管理者
- 資産管理者
- 監査人管理者
- アプリケーション監査人
    - システム監査人
    - 権限許可管理者
- Help Desk 管理者
- 操作管理者
- セキュリティポリシー管理者
- ユーザー管理者

15.1 アプライアンス管理者

アプライアンス管理者は、次の作業を含む、アプライアンスの構成と保守に責任を負います。

- アプライアンスのラックとスタック
- アプライアンスの構成
- （任意）初期セットアップ、メンテナンス、バックアップ、復元のために仮想アプライアンスをセットアップして使用。詳細については、「仮想アプライアンスと Web 管理コンソールの使用」を参照してください。
- パフォーマンス、ハードウェア、ネットワークのトラブルシューティング

- クラスタ環境の作成とステータスの監視
- ライセンス、証明書、バックアップ、セッション設定の管理
- アクセスリクエストとパスワードおよび SSH キーの管理サービスの有効化/無効化

15.2 資産管理者

資産管理者は、すべてのパーティション、資産、アカウントを管理します。

- 資産とアカウントを作成（またはインポート）します。
- パーティションとパーティションプロファイルを作成します。
- パーティション所有権をユーザーに委任します。委任されたパーティション所有者は、資産管理者が持つアクセス許可のサブセットを持ちます。パーティションの所有権を委任されたユーザーは、特定のパーティションと、そのパーティションに割り当てられた資産およびアカウントを管理するアクセス許可を持ちます。
- パーティションに資産を割り当てます。
- アカウントのパスワードルールを管理します。
- 資産、アカウント、パーティションの所有権を管理します。

> **メモ**：資産管理者は、自分のアカウントのユーザーオブジェクト履歴のみを表示することができます。

15.3 監査人管理者

監査人管理者は、すべての機能に対する読み取り専用アクセス権を持っており、すべてのアクセスリクエストアクティビティを確認することができます。

- アプライアンス情報の監視
- すべてのレビュー
- オブジェクト履歴のエクスポート
- 資格レポートの実行

監査人が選択されると、 2 つの追加アクセス許可タイプが有効になります。

- アプリケーション監査人

- システム監査人

一部のページで、管理者がデータを編集できるように見えることがありますが、その変更は保存できません。次のようなメッセージが表示されます。「このリクエストには認可が必要です。」

15.3.1 アプリケーション監査人

アプリケーション監査人は、Safeguard の操作に関連する機能に読み取り専用でアクセスできます。アプリケーション監査人のアクセス許可は、以下のロール（役割）に対応していますが、読み取りアクセスのみが許可されています。

- セキュリティポリシー
- 資産

15.3.2 システム監査人

システム監査人は、Safeguard の操作に関連する機能への読み取り専用アクセスを提供します。システム監査人のアクセス許可は、次のロール（役割）に対応していますが、読み取りアクセスのみが許可されています。

- アプライアンス
- 操作
- Help Desk
- ユーザー
- グローバル

15.4 権限許可管理者

権限許可管理者は、アクセス許可管理者であり、次のことを実行します：

- SPP ユーザーの作成（またはインポート）
- ユーザーへのアクセス許可付与
- パスワード設定、ロック解除、ローカルとディレクトリの両方のユーザーアカウントの有効化または無効化

権限許可管理者は、ユーザー管理者および Help Desk 管理者のアクセス許可も持ちます。

> **重要**: 権限許可管理者は自分のアカウントのアクセス許可を変更することができますが、これは他のユーザーへのアクセス許可付与の能力に影響する場合があります。自分のアクセス許可に変更を加えると、次回ログイン時にその変更が有効になります。

15.5 Help Desk 管理者

- 非管理ユーザーアカウントのパスワード設定
- すべてのユーザーアカウントのアカウントのロック解除

> **メモ：** Help Desk 管理者は、自分のアカウントのユーザーオブジェクトの履歴のみを表示できます。

15.6 操作管理者

操作管理者は、アプライアンスの状態を監視し、アプライアンスを再起動することができます。

一部のページでは、管理者がデータを編集できると表示されることがありますが、変更を保存することはできません。次のようなメッセージが表示されます。「このリクエストには認可が必要です。」

> **メモ：** このユーザーは、非インタラクティブなユーザー、つまり自動化スクリプトまたは外部監視システムである可能性があります。

15.7 セキュリティポリシー管理者

セキュリティポリシー管理者は、アカウントや資産へのアクセス権を管理するセキュリティポリシーを設定します。これには、最大期間などのパスワードのチェックアウトに関する要件、パスワードや SSH キーの理由が必要な場合、緊急アクセスが許可される場合などが含まれます。このユーザーは、資産に関する詳細を知らない場合があります。

このユーザーは、資産の時間制限、および誰がアクセスリクエストを要求、承認、レビューできるかを設定します。

- アカウントグループ、資産グループ、ユーザーグループの作成

- 資格の作成
- アクセスリクエストポリシーの設定
- ユーザーまたはユーザーグループを資格に追加して、これらのアカウントがパスワードをリクエストすることを許可する
- 資格アクセスポリシーガバナンスのために、リンクアカウントをユーザーに割り当て

一部のページで、管理者がデータを編集できるように見えることがありますが、変更を保存することはできません。以下のようなメッセージが表示されます：「このリクエストには認可が必要です。」

15.8 ユーザー管理者

- SPP のユーザーの作成（またはインポート）
- ユーザーグループの作成
- ユーザーに Help Desk 管理者権限を付与
- パスワードの設定、ユーザーのロック解除、管理者以外のユーザーアカウントの有効化または無効化
- Help Desk 管理者のアクセス許可を持つ

考慮事項：

- ユーザー管理者は、自分自身を含む管理者パスワードを変更することはできません。
- ユーザー管理者は自分のアカウントのアクセス許可を変更することができますが、これは他のユーザーに Help Desk 管理者アクセス許可を付与する能力に影響を与える可能性があります。自分の権限に変更を加えると、次回ログイン時に有効になります。

16 管理のためのシステム準備

SPP にシステムを追加する（資産の追加）前に、システムが適切に構成されていることを確認する必要があります。

一般的に、SPP の資産を準備するには、次を行います：

1. 資産に機能アカウント（SPP では「サービス」アカウントと呼びます）を作成し、それにパスワードまたはプラットフォームが SSH キーをサポートしている場合は、SSH キーを割り当てます。

   > **メモ:** 資産を SPP に追加するには、その資産にサービスアカウントが必要です。詳細については、「サービスアカウントについて」を参照してください。

2. サービスアカウントに十分な権限を付与します。
3. サービスアカウントの接続をテストします。
4. セキュリティプロトコルを設定します。
5. SSL サーバー証明書の検証をサポートするプラットフォームでは、サーバーの署名機関証明書を SPP の［信頼できる証明書］ストアに追加します。詳細については、「信頼できる CA 証明書」を参照してください。

16.1 ACF -メインフレームシステムの準備

ACF2 - メインフレームと ACF2 - メインフレーム LDAP プラットフォームの両方に適用されます。

IBM ACF - メインフレームシステムを SPP 用に準備するには、次の手順を行ってください：

1. 資産にサービスアカウントを作成し、それにパスワードを割り当てます。サービスアカウントは、ACF2 ChangePassword が正しく動作するように SECURITY 属性を有効にしておく必要があります。
2. サービスアカウントに、他のプロファイルで ALTERUSER コマンドを使用するために必要な特権を与えます。

3. まだインストールされていない場合は、z/OS システム上に telnet サーバーをインストールします。必要であれば、SSL で telnet を保護します。

   > **メモ：** telnet サーバー（および SSL）のインストールと設定の詳細については、IBM z/OS システムのドキュメントを参照してください。

4. Windows ベースの 3270 エミュレーターを使用して telnet サーバーをテストするか、Linux で telnet-ssl または x3270 プログラムを使用して、z/OS システムへの SSL および非 SSL 接続をテストします。

5. SPP では、パスワード認証を使用して、z/OS システムの資産とアカウントを作成します。

telnet プロトコルの証明書サポートについて

SPP は、接続先が提供するサーバー証明書を自動的に受け入れ、telnet 証明書のトラストチェーンを検証することはありません。また、SPP はクライアント証明書の選択をサポートしていないため、telnet がクライアントに認識された機関によって署名された証明書を提示することを要求する場合、SPP はその設定をサポートできません。

16.2 Amazon Web Services プラットフォームの準備

SPP は、安全なクラウドサービスプラットフォームである Amazon Web Services (AWS) をサポートしています。

Amazon Web Services 資産を追加する場合、ネットワークアドレスに AWS Account ID または Alias を含める必要があります。

SPP 用に Amazon Web Services プラットフォームを準備するには、以下の手順を行ってください：

1. SPP で：

   a. Amazon の証明書と AWS 証明書のルート証明機関（CA）を SPP の信頼できる証明書ストアに追加します。

   b. サービスアカウントとして使用する Identity and Access Management （IAM）ユーザーを設定します。

   c. IAM サービスアカウントを AdministratorAccess セキュリティポリシーに割り当てます。

2. Amazon で:

    a. IAM サービスアカウント用のアクセスキーを作成します。Amazon では、シークレットキーと公開アクセスキーID と呼ばれるデータ項目のペアが作成されます。Access Key ID と Secret Key の両方をメモしておきます。Amazon Web Services 資産を SPP に追加するときに、これらが必要になります。

16.3 Cisco デバイスの準備

Safeguard for Privileged Passwords でサポートされる Cisco プラットフォームは 4 つです。

- Cisco ISE CLI プラットフォーム：SPP は、ローカル サービスアカウントを使用して、SSH を使用し ISE CLI プラットフォームのアカウントを管理します。
- Cisco IOS/ASA プラットフォーム：Cisco IOS/ASA プラットフォームは、SSH を使用してローカルアカウントを管理するために、次の方法で設定することができます：
    - SPP は、Cisco デバイスのアカウントを管理するために、ローカルのサービスアカウントを使用します。
    - Cisco デバイスが、SPP によって管理される Cisco ISE サーバーへのログインリクエストを認証および承認するように（AAA を使用して）構成されている場合、Cisco ISE ディレクトリ資産のディレクトリアカウントを使用して Cisco デバイスを管理できます。
    - SPP は、Cisco Private Internet eXchange （PIX）ファイアウォールセキュリティアプライアンスと PIX Internetwork Operating System （IOS）ルーターおよびスイッチの両方をサポートしています。Cisco PIX と Cisco IOS は、SPP アプライアンスへの接続に SSH プロトコルを使用します。SPP は、SSH バージョン 1 およびバージョン 2 の両方をサポートしています。
    - Cisco デバイスが、SPP で管理される Active Directory ドメインと統合された Cisco ISE サーバーへのログインリクエストを認証および承認するように（AAA を使用して）設定されている場合、Active Directory 資産のディレクトリアカウントを使用して Cisco デバイス上のアカウントを管理することができます。
- Cisco ISE プラットフォーム：Cisco ISE は、SPP のディレクトリ資産として管理されます。これは、REST と TACACS+ を使用してローカル アカウントを管理します。アカウント検出とパスワード管理をサポートします。ディレクトリ同期、資産ディスカバリー、サービスディスカバリーはサポートされません。

- Cisco NX-OS プラットフォーム：ユーザーに対して必要なすべての操作を実行するために、使用するサービスアカウントには少なくともネットワーク管理者権限が必要です。

16.3.1 Cisco ISE CLI プラットフォーム

SPP は、SSH を使用して ISE CLI プラットフォームのローカル アカウントを管理します。

Cisco ISE CLI プラットフォームのローカル アカウントを管理する手順

1. サービスアカウントがリモートでログインできるように、SSH サーバーを有効化し、設定します。
2. 資産にサービスアカウント（admin ロール付き）を作成し、それにパスワードを割り当てます。

16.3.2 Cisco IOS/ASA プラットフォーム

SPP は、Cisco Private Internet eXchange (PIX) ファイアウォール セキュリティアプライアンスと PIX Internetwork Operating System (IOS) ルーターおよびスイッチの両方をサポートしています。Cisco PIX と Cisco IOS は、SPP アプライアンスへの接続に SSH プロトコルを使用します。SPP は、SSH バージョン 1 およびバージョン 2 の両方をサポートしています。

以下が適用されます：

- SPP は、Cisco プラットフォームのアカウントを管理するために SSH を使用します。SSH サーバーは、サービスアカウントがリモートでログインできるように有効化し、設定する必要があります。
- SPP は、running 構成ファイルではなく、startup 構成ファイルで検出されたアカウントを管理します。
- 選択されたサービスアカウントは、構成を更新するのに十分な権限を持っている必要があります。ログイン時に十分な権限がない場合は、SPP で資産に対して特権レベルパスワード（system enable パスワード）を設定する必要があります。

ローカル設定

次の情報は、ローカルのサービスアカウントを使用して Cisco デバイスを準備するためのものです。

ローカルのサービスアカウントを使用して、SPP のために Cisco デバイスを準備する手順：

1. 資産にサービスアカウントを作成し、パスワードを割り当てます。
2. サービスアカウントがリモートでログインできるように SSH サーバーを有効化し、設定します。
3. 必要に応じて、特権レベル パスワード（system enable パスワード）を設定します。
4. パスワード認証を使用して、Cisco デバイスを SPP に追加します。

Cisco ISE ディレクトリを使用したディレクトリの構成

> **重要**: Cisco ISE サーバーと ISE ポリシーの構成方法の詳細については、お使いのシステムのドキュメントを参照してください。

Cisco デバイスが、SPP で管理される Cisco ISE サーバーへのログインリクエストを認証および承認するように（AAA を使用して）設定されている場合、Cisco ISE ディレクトリ資産のディレクトリアカウントを使用して Cisco デバイスを管理することが可能です。

または、Cisco ISE サーバーが SPP で管理される Active Directory ドメインと統合されている場合は、統合された AD ディレクトリのサービスアカウントを使用して資産を管理することができます。このシナリオでは、AD 資産を作成するだけで、SPP で Cisco ISE サーバーの資産を作成する必要はありません。

ディレクトリアカウントを使用して Cisco IOS/ASA 資産を管理するために Cisco ISE サーバーを準備する手順

1. Cisco ISE サーバーでサービスアカウントを作成します。

a. Cisco ISE サーバーに認証されるようにします：

   i. ローカル **Network Access** ユーザーを作成します。

   ii. **PasswordType** を **Internal Users** に設定します。これにより、ユーザーはローカルで認証されます。

   iii. ユーザーのパスワードを割り当てます。

b. Active Directory を認証するには、次の手順に従います：

   i. SPP で管理されるドメインの外部 ID ソースを作成します。

   ii. Cisco ISE サーバーをドメインに参加させ、ISE ポリシーで使用する任意の AD グループをインポートします。

   iii. AD のユーザー名と一致するユーザー名を持つ **Network Access** ユーザーを作成します。

   iv. **PasswordType** を<domainname>に設定します。ユーザーにパスワードを割り当てないでください（パスワードは AD に認証されます）。

2. Cisco デバイスから Cisco ISE サーバーへの TACACS+アクセスを許可するように、**Network Device** を設定します。TACACS+の共有シークレットを、Cisco デバイスで AAA を使用して構成した共有シークレットと一致するように構成します。

3. 選択した **Network Access** ユーザーに、選択した **Network Device** へのシェルログインを許可する **Device Admin Policy** ポリシーを設定します。ポリシーは、多くの異なるセッション、ユーザー、またはグループ設定に基づいて ISE で構成できます。

   > **メモ：**たとえば、次のようになります。
   >
   > a. SPP で管理するすべての **Network Access** ユーザーを表す **identity Group** を作成します。
   >
   > b. SPP がネットワークデバイスにアクセスするために使用するすべての AD ユーザーを表す AD グループをインポートします。
   >
   > c. これらのグループのすべてのメンバーにシェル ログインを許可するポリシーを作成します。
   > SPP からの CheckPassword リクエストまたは SPS セッションは、いずれのグループにも属さない **Network Access** ユーザーに対して失敗します。

ISE アカウントで管理する Cisco IOS/ASA 資産の準備する手順

1. SSH サーバーを有効にして、サービスアカウントがリモートでログインできるように設定します。

2. Cisco ISE サーバーでこのネットワークデバイス用に構成された共有シークレットを使用して、ディレクトリユーザーの Cisco ISE サーバーへのログインリクエストを承認するために、TACACS+ を使用するように AAA を構成します。

   > **メモ：**AAA を設定する方法の詳細については、お使いのシステムのマニュアルを参照してください。

3. 選択した Cisco ISE Network Access ユーザーが Cisco デバイスにログインできることをテストします。これは、SSH を使用してコマンドラインからログインすることでテストできます。

4. 必要に応じて、選択したサービスアカウントを、SPP の Cisco ISE または AD ディレクトリ資産に追加します。

5. 必要に応じて、Cisco IOS 資産の **Privilege Level Password** を設定します。

6. ディレクトリ認証を使用して、Cisco デバイスを SPP に追加します。

7. SPS セッションアクセス用に資産を設定する必要がある場合は、SPS で設定されたサーバー側の SSH アルゴリズムに Cisco デバイスでサポートされるアルゴリズムが含まれていることを確認します。

16.3.3 Cisco ISE プラットフォーム

Cisco ISE は、SPP のディレクトリ資産として管理されます。これは、アカウント検出とパスワード管理をサポートします。ディレクトリ同期、資産検出、サービス検出はサポートされません。

Cisco ISE ディレクトリユーザーは、Cisco ISE を管理するためのサービスアカウントとして使用できます：

- Cisco ISE サーバーへのログインリクエストを認証するように構成された Cisco IOS/ASA 資産を管理するためのサービスアカウントとして
- Cisco ISE サーバーへのログインリクエストを認証するように構成された Cisco IOS/ASA 資産上で SPS が管理する SSH セッションを実行するため

SPP は、Cisco ISE サーバーの **Network Access**（内部）ユーザーを管理します（ローカルの管理者ユーザーを管理することはありません）。**Network Access** ユーザーは、他のネットワークデバイス（例: Cisco IOS 資産）にログインするために使用できるディレクトリアカウントです。管理対象のネットワークデバイスは、AAA を使用して Cisco ISE サーバーへのリクエストを認証および承認するように設定する必要があります（詳しくは、お使いのシステムのマニュアルを参照してください）。

ISE プラットフォームのサービスアカウントは、管理者特権を持つ **Network Access** ユーザーである必要があります。

Cisco ISE の準備

1. SPP は、ISE REST API（ERS）を使用して Cisco ISE のパスワードを管理します。これはデフォルトで無効になっているため、Cisco ISE を構成する前に **System Settings** で読み取り/書き込みのアクセスを有効にする必要があります。

2. Safeguard は、Cisco ISE のパスワードの確認に TACACS+ プロトコルを使用します。これはデフォルトで無効になっているため、Cisco ISE サーバーの **Global Settings** で **Device Admin Service** を有効にして設定する必要があります。

3. **Network Access** ユーザーを作成し（**PasswordType** を **Internal Users** に設定）、それにパスワードを割り当てます。**Enable Password** は設定しないでください。

4. 新しいユーザーを作成する代わりに、既存の **Network Access** ユーザーのリストから新しいユーザーを選択して、**Admin User** を作成し、新しいユーザーに管理者アクセス権を割り当てます。

5. 選択した Admin User を以下の Admin グループのいずれかに追加します。
    - **Super Admin**
    - **ERS Admin** および **Elevated System Admin**

6. SPP クラスタの **Network Device** を設定します。
    a. SPP クラスタ内のアプライアンスの IP アドレスを追加します。
    b. クラスタが使用する TACACS+シークレットを設定します。

    > **メモ：**これは、この資産のディレクトリユーザーを使用して管理する Cisco IOS/ASA ネットワークデバイスに構成された TACACS+共有シークレットと一致する必要があります。

7. 以下を含む **Device Admin Policy Set** を構成します。
    - SPP クラスタに設定された **Network Device** に TACACS+アクセスを許可します。
    - すべての TACACS+プロトコルを許可します。
    - SPP を使用して管理したい **Network Access** ユーザーにシェルアクセスを許可する。ポリシーは、多くの異なるセッション、ユーザー、グループ設定に基づいて ISE で構成できます。

    > **メモ：**たとえば、次のようになります：
    >
    > a. SPP で管理するすべてのネットワークアクセスユーザーを表す **Identity Group** を作成します。

b. このグループの全メンバーにシェルログインを許可するポリシーを作成します。
SPP からの CheckPassword リクエストまたは SPS セッションは、いずれのグループにも属さない Network Access ユーザーの場合、失敗することになります。

8. TACACS+ 用にポート 49 を構成します。

16.3.4 Cisco NX-OS プラットフォーム

SPP は、NX-API を使用して Cisco NX-OS プラットフォームのローカルアカウントを管理します。

Cisco NX-OS プラットフォームでローカルアカウントを管理する手順

1. NX-API 機能を有効にして、サービスアカウントが NX-API を介してリモートでログインし、コマンドを実行できるようにします。
2. 資産に（network-admin ロールを持つ）サービスアカウントを作成し、パスワードを割り当てます。

16.4 Dell iDRAC デバイスの準備

SPP は、Dell PowerEdge サーバーに統合されている Dell Remote Access Controller をサポートします。SPP は、iDRAC デバイスへの接続に SSH プロトコルを使用します。

SPP 用に iDRAC デバイスを準備する手順

1. iDRAC を使用して、管理者権限を持つサービスアカウントを作成し、それにパスワードを割り当てます。

   サービスアカウントはログイン権限を持ち、ユーザーを設定できる必要があります。
2. iDRAC ネットワーク設定で SSH が有効になっていることを確認します。
3. SPP で、パスワード認証を使用して iDRAC デバイスの資産とアカウントを作成します。

16.5 VMware ESXi ホストの準備

SPP は、VMware ESXi ホストをサポートしています。

> **重要**：SPP は、VMware ホストのローカルユーザーのみを管理できます。

VMware ESXi ホストを SPP 用に準備する手順

1. 資産のサービスアカウントとして既存のアカウントを使用するか、新しいアカウントを作成し、それにパスワードを割り当てます。

   デフォルトの管理者アカウントが適しています。

2. サービスアカウントに、Web 管理 API を使用してユーザーパスワードを設定するために必要な権限を付与します。
3. VMware ESXi ホストを SPP に追加する場合：
   a. ネットワークアドレスを指定します。
   b. HTTPS ポートとしてポート 443 を指定します。

16.6 Fortinet FortiOS デバイスの準備

SPP は、Fortinet インターネットアプライアンスをサポートしています。SPP は、Fortinet デバイスへの接続に SSH プロトコルを使用します。

SPP 用に Fortinet FortiOS デバイスを準備する手順

1. 管理対象システムでサービスアカウントをローカルユーザーとして作成し、パスワードを割り当てます。
2. サービスアカウントを Fortinet Administrators グループに追加します。これにより、サービスアカウントは SSH でデバイスにアクセスし、ユーザーを管理できるようになります。

   > **重要**：SPP は、Fortinet Administrators グループのメンバーであるユーザーのパスワードのみを管理することができます。

3. サービスアカウントがリモートでログインできるように SSH サーバーを有効化し、設定します。

4. パスワード認証を使用して、Fortinet デバイスを SPP に追加します。

16.7 F5 Big-IP デバイスの準備

SPP は、F5 Big-IP デバイスをサポートしています。SPP は、F5 Big-IP デバイスに接続するために SSH プロトコルを使用します。

SPP 用に F5 Big-IP デバイスを準備する手順

1. F5 Big-IP 管理システムのローカルユーザーとしてサービスアカウントを作成し、それにパスワードを割り当てます。そのサービスアカウントに、すべてのパーティションで管理者権限を割り当てます。これにより、サービスアカウントはユーザーを管理できるようになります。
2. **Terminal Access** を **Advanced** または **tmsh** に設定してコンソールアクセスを有効にし、サービスアカウントが SSH 経由でリモートでログインできるようにします。
3. パスワードまたは SSH キー認証を使用して、F5 Big-IP デバイスを SPP に追加します。

16.8 HP iLO サーバーの準備

SPP では、HP iLO オペレーティングシステムは、HP Integrated Lights-Out (iLO) HP Proliant サーバーです。SPP は、SSH を使用して HP iLO システムに接続します。パスワードの確認と変更はサポートされています。アカウントの検出はサポートされていません。

SPP 用の HP iLO サーバーを準備する手順

1. ユーザーアカウントの管理特権でサービスアカウントを作成し、パスワードを割り当てます。

   サービスアカウントは、ログイン特権を持ち、ユーザーを設定できる必要があります。
2. SSH が有効になっていることを確認します。
3. SPP で、パスワード認証を使用して HP iLO サーバーの資産とアカウントを作成します。

16.9 HP iLO MP（管理プロセッサー）の準備

SPP では、HP iLO MP オペレーティングシステムは、HP Integrity Integrated Lights-Out (iLO) Management Processor です。SPP は、SSH を使用して HP iLO MP システムに接続します。

SPP 用に HP iLO Management Processor を準備する手順

1. Administer User Accounts 特権でサービスアカウントを作成し、パスワードを割り当てます。
2. SSH が有効になっていることを確認します。
3. SPP で、パスワード認証を使用して HP iLO MP 資産タイプ用の資産とアカウントを作成します。

16.10 IBM i (AS/400) システムの準備

SPP は IBM i (AS/400)システムをサポートします。

IBM i システムを SPP 用に準備する手順

1. 資産にサービスアカウントを作成し、それにパスワードを割り当てます。
2. サービスアカウントに、他のプロファイルで chgusrprf コマンドを使用するために必要な特権を与えます。
3. まだインストールされていない場合は、IBM iSeries（AS/400）システムに telnet サーバーをインストールします。必要であれば、SSL で telnet を保護します。

   > **メモ：** telnet サーバー（および SSL）のインストールと設定の詳細については、IBM iSeries (AS/400) システムのドキュメントを参照してください。IBM Knowledge Center を参照してください。

4. Windows ベースの 3270 エミュレーターを使用して telnet サーバーをテストするか、Linux 上で telnet-ssl または x3270 プログラムを使用して、IBM iSeries システムへの SSL および非 SSL 接続をテストしてください。
5. SPP で、パスワード認証を使用して IBM iSeries (AS/400)システムの資産とアカウントを作成します。

telnet プロトコルの証明書サポートについて

SPP は、接続先が提示するサーバー証明書を自動的に受け入れ、telnet 証明書のトラストチェーンを検証しません。また、SPP はクライアント証明書の選択をサポートしていないため、telnet でクライアントが公認機関によって署名された証明書を提示する必要がある場合、SPP ではその設定をサポートできません。

16.11 JunOS Juniper Networks システムの準備

SPP は Juniper Networks の JunOS オペレーティング システムを使用して Juniper Networks ルーターとスイッチを管理します。SPP は、SSH を使用して JunOS システムに接続します。

> ⚠ **注意: Shared configuration database modified というメッセージが表示された場合、Safeguard が configure private モードに入ることができるように、編集をコミットまたは破棄する必要があります。この問題を解決するには、SSH で対話的にボックスにログインし、configure を実行した後、status を実行して、現在グローバル構成を編集しているセッションを確認します。編集を破棄するには rollback を、変更をコミットするには commit を実行します。**

Juniper Networks JunOS システムの準備

1. super-user ログインクラスのメンバーであるサービスアカウントを作成し、それにパスワードを割り当てます。
2. SSH が有効になっていることを確認します。
3. SPP で、パスワード認証を使用して Juniper Networks JunOS の資産タイプの資産とアカウントを作成します。

16.12 MongoDB の準備

SPP は mongodb.conf ファイルで定義された TCP ポートと Bind IP アドレスを使用して MongoDB への SSL 接続を行います。MongoDB 資産を SPP に追加するときに、このポート番号を入力する必要があります。

MongoDB を SPP 用に設定する手順

1. サービスアカウントを作成し、パスワードを割り当てます。

   > **メモ:** サービスアカウントには、リモート接続の権限とパスワードの変更権限が必要です。組織に適した設定については、MongoDB セキュリティガイドを参照してください。

2. サービスアカウントでログインできることを確認します。

3. SPP で、パスワード認証を使用して、MongoDB 資産タイプの資産とアカウントを作成します。**データベースインスタンス名**と、データベースインスタンスが使用する**ポート**を指定する必要があります。

   > **メモ：** Dialog User または Communication Data タイプのアカウントを作成すると、SPP でアカウントのパスワードを設定したり、パスワードをリセットしたりすることができます。このアカウントのパスワードをリセットするには、**Reset Password** オプションを使用します。**Set Password** オプションを使用して、MongoDB で使用されているパスワードと同じパスワードを入力すると、SPP のパスワードチェックは失敗します。

16.13 MySQL サーバーの準備

SPP 用の MySQL サーバーを準備するには、MySQL サーバーのドキュメントを参照して、暗号化の設定方法とセキュアな方法に関する情報を確認します。

SSL サーバー証明書の検証を有効にするには、サーバーの署名機関証明書を SPP の信頼できる証明書ストアに追加します。詳細については、「信頼できる CA 証明書」を参照してください。

SPP データベースサーバーが SSL を使用する方法の詳細については、「SPP データベースサーバーでどのように SSL を使用しますか？」を参照してください。

サポートされる SQL アカウント

Safeguard は、<username>または<username>@<IP アドレスの範囲>のフォーマットで作成された MySQL アカウントをサポートすることができます。許可された IP アドレスの範囲には、Safeguard アプライアンスの IP アドレスが含まれている必要があります。ワイルドカードとして%文字を使用することができます。

例：

- Sam : Sam に任意のホストからのログインを許可する（デフォルト）
- Sam@%: Sam に任意のホストからのログインを許可する

- Sam@10.1.%：10.1.xx の任意の IP アドレスからの Sam のログインを許可する

16.14 Oracle データベースの準備

Oracle データベースを SPP 用に準備するには、Oracle データベースのドキュメントを参照して、暗号化の設定方法と安全性を確保する方法を確認します。

SSL サーバー証明書の検証を有効にするには、Oracle サーバーで SSL 対応サービスを構成するときに、次のセキュリティ設定が構成されていることを確認します：

SSL_SERVER_CERT_DN="CN=<*address*>", <*address*>は SPP の資産のネットワークアドレスに一致します。

16.15 PAN-OS (Palo Alto) Networks の準備

SPP では、Palo Alto Networks のアプライアンスで PAN-OS オペレーティングシステムが使用されます。SPP は、SSH を使用して PAN-OS システムに接続します。

SPP 用に Palo Alto Networks システムを準備する手順

1. デバイス管理者であるサービスアカウントを作成し、Superuser ロールとパスワードを割り当てます。
2. SSH が有効になっていることを確認します。
3. SPP で、パスワード認証を使用する Palo Alto Networks 資産タイプの資産とアカウントを作成します。

16.16 PostgreSQL の準備

SPP は、postgresql.conf ファイルで定義された TCP ポートを使用して PostgreSQL への SSL 接続を行います。PostgreSQL 資産を SPP に追加する際に、このポート番号を入力する必要があります。

PostgreSQL を SPP 用に設定する手順

1. サービスアカウントを作成し、それにパスワードを割り当てます。

   > **メモ：**サービスアカウントには、リモート接続の権限とパスワードの変更権限が必要です。組織での適切な設定については、PostgreSQL セキュリティガイドを参照してください。

2. サービスアカウントでログインできることを確認します。

3. SPP で、パスワード認証を使用して PostgreSQL 資産タイプの資産とアカウントを作成します。**データベースインスタンス名**とデータベースインスタンスで使用される**ポート**を指定する必要があります。

   > **メモ**: Dialog User または Communication Data タイプのアカウントを作成すると、SPP でアカウントパスワードの設定またはパスワードのリセットを行うことができます。このアカウントのパスワードをリセットするには、**Reset Password** オプションを使用します。**Set Password** オプションを使用して、PostgreSQL で使用されているパスワードと同じパスワードを入力すると、SPP のパスワード確認は失敗します。

16.17 RACF メインフレームシステムの準備

RACF メインフレームと RACF メインフレーム LDAP プラットフォームの両方に適用されます。

IBM RACF メインフレームシステムを SPP 用に準備する手順

1. 資産にサービスアカウントを作成し、それにパスワードを割り当てます。

2. サービスアカウントに、他のプロファイルで ALTERUSER コマンドを使用するために必要な特権を付与します。

3. まだインストールされていない場合、z/OS システムに telnet サーバーをインストールします。必要であれば、SSL で telnet を保護します。

   > **メモ：**telnet サーバー（および SSL）のインストールと設定の詳細については、IBM z/OS システムのドキュメントを参照してください。

4. Windows ベースの 3270 エミュレーターを使用して telnet サーバーをテストするか、Linux で telnet-ssl または x3270 プログラムを使用して、z/OS システムへの SSL および非 SSL 接続をテストします。

5. SPP では、パスワード認証を使用して、z/OS システムの資産とアカウントを作成します。

telnet プロトコルの証明書サポートについて

SPP は、接続先が提供するサーバー証明書を自動的に受け入れ、telnet 証明書のトラストチェーンを検証することはありません。また、SPP はクライアント証明書の選択をサポートしないため、telnet でクライアントが公認の機関によって署名された証明書を提示する必要がある場合、SPP ではその設定をサポートできません。

16.18 SAP HANA の準備

SPP は、SAP システム番号（「インスタンス番号」とも呼ばれる）に応じて、30015 から 39915 の間の TCP ポートを使用して SAP HANA に SSL 接続を行います。詳細については、「Safeguard のポート」を参照してください。

SAP HANA を SPP 用に準備する手順

1. サービスアカウントを作成し、それにパスワードを割り当てます。

   このサービスアカウントには、リモート接続の権限とパスワードの変更権限が必要です。お客様の組織に適した設定については、SAP セキュリティガイドを参照してください。

2. サービスアカウントでログインできることを確認します。

   SAP では、Dialog User タイプまたは Communication Data タイプの新しいアカウントを作成すると、新しいパスワードを設定するよう求められます。

3. SPP で、パスワード認証を使用して、SAP 資産タイプの資産とアカウントを作成します。SAP インスタンスが使用する **SAP Client ID** 番号と **Port** を指定する必要があります。

   Dialog User または Communication Data タイプのアカウントを作成すると、SPP でアカウントパスワードの設定またはパスワードのリセットを行うことができます。このアカウントのパスワードをリセットするには、**Reset Password** オプションを使用します。**Set Password** オプションを使用して、SAP で使用されているパスワードと同じものを入力すると、SPP のパスワードチェックは失敗します。

16.19 SAP Netweaver アプリケーションサーバーの準備

SPP は、SAP システム番号（インスタンス番号とも呼ばれる）に応じて 3300 ～ 3399 の TCP ポートを使用して SAP Application Server への SSL 接続を行います。1 台のサーバーで複数の SAP インスタンスを実行し、それぞれが 3300 ～ 3399 の範囲で異なるネットワークポートを使用することができます。ポートの最後の 2 桁は、システム番号（またはインスタンス番号）と呼ばれます。詳細については、「Safeguard のポート」を参照してください。

アカウントにパスワードを割り当てた場合、ログインしてパスワードを管理者が割り当てた値から変更するまで、そのアカウントは使用できません。

資産の特権ユーザーが System タイプまたは Communication User タイプの場合、そのユーザーに対して PING 機能モジュールの RFC 権限を割り当てます。これにより、そのユーザーはパスワードの変更など、その機能をリモートで実行できるようになります。

SAP Netweaver アプリケーションサーバーの設定

1. サービスアカウントを作成し、それにパスワードを割り当てます。

   このサービスアカウントには、リモート接続の権限とパスワードの変更の権限が必要です。設定には以下が含まれる場合があります。

   - Cross-application Authorization Objects を RCF アクセスの認証チェックに設定する
   - Basis: Administration set to User Master Maintenance：変更とロックを含むユーザーグループ

   S_A.SYSTEM 認証プロファイルは機能しますが、必要以上に多くの権限が設定されている可能性があります。

   SAP のセキュリティガイドを参照して、組織に適した設定を確認してください。

2. サービスアカウントでログインできることを確認します。

3. SAP では、System または Communication User Type の新しいアカウントを作成すると、新しいパスワードを設定するよう促されます。

   SPP で、パスワード認証を使用して、SAP 資産タイプの資産とアカウントを作成します。**SAP Client ID** 番号と、SAP インスタンスで使用される **Port** を指定する必要があります。

   System または Communication User Type のアカウントを作成すると、Safeguard ではアカウントパスワードの設定またはパスワードのリセットを行うことができます。このアカウントのパスワードをリセットするには、**Reset Password** オプションを使用します。

Set Password オプションを使用して、SAP で使用されているパスワードと同じパスワードを入力すると、Safeguard のパスワードチェックは失敗します。

16.20 Sybase (Adaptive Server Enterprise) サーバーの準備

SPP のために Sybase ASE（Adaptive Server Enterprise）サーバーを準備するには、Sybase ASE サーバーのドキュメントを参照して、暗号化の設定方法と安全性について確認してください。使用するサービスアカウントに sso_role が割り当てられていることを確認してください。

SSL サーバー証明書の検証を有効にするには、サーバーの署名機関証明書を SPP の「信頼できる CA 証明書」ストアに追加します。詳細については、「信頼できる CA 証明書」を参照してください。

SPP データベースサーバーが SSL を使用する方法の詳細については、「SPP データベースサーバーでどのように SSL を使用しますか？」を参照してください。

16.21 SonicOS デバイスの準備

SPP は、SonicOS インターネットアプライアンスをサポートしています。SPP は、SonicOS デバイスに接続するために SSH プロトコルを使用します。

SPP のために SonicOS デバイスを準備する手順

1. 管理対象システムのローカルユーザーとしてサービスアカウントを作成し、それにパスワードを割り当てます。
2. サービスアカウントを SonicWALL Administrators グループに追加します。これにより、サービスアカウントが SSH でデバイスにアクセスし、ユーザーを管理できるようになります。

   > **重要：** SPP は、SonicWALL Administrators グループのメンバーであるユーザーのパスワードのみを管理できます。

3. SSH サーバーを有効化し、サービスアカウントがリモートでログインできるように設定します。
4. パスワード認証を使用して、SonicOS デバイスを SPP に追加します。

16.22 SonicWALL SMA または CMS アプライアンスの準備

SonicWALL SMA または CMS アプライアンスを SPP 用に設定する際の重要な注意事項を以下に示します。

1. サービスアカウントとして、ローカルの admin アカウントを使用してください。
2. SPP は admin アカウントのみを管理でき、他のローカルアカウントや外部プロバイダのアカウントは管理できません。

16.23 SQL サーバーの準備

SPP 用の Microsoft SQL Server を準備するには、SQL Server のドキュメントを参照して、暗号化の設定方法とセキュアな方法を確認します。

SSL サーバー証明書の検証を有効にするには、サーバーの署名機関証明書を SPP の「信頼できる証明書」ストアに追加します。詳細については、「信頼できる CA 証明書」を参照してください。

SPP データベースサーバーが SSL を使用する方法の詳細については、「SPP データベースサーバーでどのように SSL を使用しますか？」を参照してください。

SQL サーバーを SPP 用に設定する手順（認証タイプが Local System Account の場合）

> **メモ：**認証タイプがローカルシステムアカウントの Microsoft SQL サーバー資産を管理するには、SQL の Security Admin であるローカル Windows アカウントが必要です。この認証タイプを使用するには、SPP に Windows 資産と SQL Server 資産を追加する必要があります。

1. SPP Web クライアントに資産管理者としてログインします。
2. **［資産管理］＞［資産］**の順に選択します。
3. SQL データベースをホストしているサーバーの OS に一致する Windows 資産を追加します。
    a. **［接続］**タブで、**［認証タイプ］**を選択します。
        - **認証タイプ：［パスワード］**に設定します。

- **サービスアカウント：** Administrator グループのメンバーであるローカルユーザーに設定します。

b. 必要に応じて他のアカウントも追加します。

資産を保存します。

4. SQL Server 資産を追加します。

a. **［接続］**タブで：

- **認証タイプ**：［Local System Account］を設定します。
- **サービスアカウント**：**［アカウント選択］**をクリックし、リストからローカル システムアカウントを選択します。

  選択可能なアカウントは、手順 3 で追加した Windows 資産にリンクされている Windows アカウントです。
- **［接続テスト］**を実行し、接続が機能することを確認します。

資産を保存します。

SQL Server で SPP を設定する手順（認証タイプが Directory Account の場合）

> **メモ:** 認証タイプがディレクトリアカウントの Microsoft SQL 資産を管理するには、SQL の Security Admin であるドメインアカウントが必要です。この認証タイプを使用するには、SPP にディレクトリとディレクトリユーザーを追加する必要があります。

1. ディレクトリとディレクトリユーザーを追加します。

a. 資産管理者としてログインします。

b. **［資産管理］＞［資産］**の順に選択して、ドメインのディレクトリを追加します。

c. 追加したら、ドメインを選択し、**［アカウント］**タブを開いて、ドメインユーザーアカウントを追加します。詳細については、「資産にアカウントを追加」を参照してください。

2. SQL Server 資産とアカウント情報を追加します。

a. SPP Web クライアントに資産管理者としてログインします。

b. **［資産管理］＞［資産］**から、SQL Server 資産を追加します。

c. **［接続］**タブで、以下を完了します。

- **認証タイプ**：**［ディレクトリアカウント］**に設定します。

- **サービスアカウント**：**[参照]**をクリックし、リストからドメインユーザーアカウントを選択します。

  選択可能なアカウントは、手順 1 で追加したディレクトリにリンクされているドメインユーザーアカウントです。

- **[接続のテスト]**を実行し、接続がうまくいくことを確認します。

3. 資産を保存します。

16.24 Top Secret メインフレームシステムの準備

SPP は、TSO インターフェイスにログオンできるファシリティ TSO との有効な accessor ID (ACID) を持つ、許可された Top Secret ユーザーを管理することができます。

これは、Top Secret メインフレームと Top Secret メインフレーム LDAP プラットフォームの両方に適用されます。

SPP 用の CA Top Seret メインフレームシステムを準備する手順

1. 資産にサービスアカウントを作成し、それにパスワードを割り当て、「TSO」機能を付与します。
2. サービスアカウントに、その範囲内の ACID に対して以下の権限を付与します。
   a. ACID のセキュリティレコード情報をリストアップする権限
   b. MISC1(SUSPEND)権限、ACID から PSUSPEND 属性を削除するための権限
   c. 他の ACID のパスワードを更新するための ACID(MAINTAIN) または MISC8(PWMAINT) 権限
3. まだインストールされていない場合は、z/OS システム上に telnet サーバーをインストールします。必要であれば、SSL で telnet を保護します。

   > **メモ:** telnet サーバー（および SSL）のインストールと設定の詳細については、IBM z/OS システムのドキュメントを参照してください。

4. Windows ベースの 3270 エミュレーターを使用して telnet サーバーをテストするか、Linux で telnet-ssl または x3270 プログラムを使用して、z/OS システムへの SSL および非 SSL 接続をテストします。

5. SPP では、パスワード認証を使用して、z/OS システムの資産とアカウントを作成します。

telnet プロトコルの証明書サポートについて

SPP は、接続先が提供するサーバー証明書を自動的に受け入れ、telnet 証明書のトラストチェーンを検証することはありません。また、SPP はクライアント証明書の選択をサポートしないため、telnet でクライアントが公認の機関によって署名された証明書を提示する必要がある場合、SPP ではその設定をサポートできません。

16.25 Unix ベースシステムの準備

SPP は、SSH プロトコルを使用して Unix ベースのシステムに接続します。

Unix ベースのシステム（AIX、HP-UX、Linux、Macintosh OS X、Solaris、FreeBSD プラットフォーム）を準備するには、以下の手順に従います。

1. 十分な権限を持つサービスアカウントを資産上に作成します。

   少なくとも、サービスアカウントのパスワードまたは SSH キーを設定する必要があります。SPP で生成および設定した SSH キーを使用する場合は、サービスアカウントのホームディレクトリが存在することも確認する必要があります。

2. サービスアカウントが root 権限で次のコマンドのリストを非対話的に、つまり、パスワードの入力を要求されることなく実行できることを確認します。

   例えば、Linux システムでは、sudoers ファイルに以下の行を追加します。

   <SerAcctName> ALL=(root) NOPASSWD: /usr/bin/passwd

   サービスアカウントが非対話的に root 権限で実行しなければならないコマンドは以下の通りです。

   Linux およびほとんどの Unix 系システム

   - egrep
   - grep
   - passwd

   > **メモ：** Unix ベースのシステムでは、追加の sudo コマンドが必要な場合があります。例えば、管理されたシステムで SSH 認証キーを設定するために必要なコマンドのリストについては、「SSH キー」を参照してください。

AIX：

- sed
- grep
- passwd
- pwdadm

Mac OS X：

- dscl
- passwd

3. サービスアカウントがリモートでログインできるように、SSH サーバーを有効にして設定します。たとえば、Mac では、サービスアカウントのリモートログインを有効にします。

> **メモ：**Linux や Unix のバージョンが異なると、SSH の設定に若干異なるパラメーターが必要になる場合があります。Linux/Unix のシステム管理者に相談するか、システムのドキュメントを参照してください。

16.26 Windows システムの準備

SPP は、Windows システムをサポートしています。詳しくは、「How To: Configure Windows Assets in Safeguard (4314156)」を参照してください。

> **メモ：**Microsoft は、DCOM サーバーの強化を開始しました。
> https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26414
> および KB5004442 - Windows DCOM Server セキュリティ機能バイパスの変更を管理する (CVE-2021-26414) をご参照ください。

Windows システムの準備

1. 資産にサービスアカウントを作成し、それにパスワードを割り当てます。
   - ディレクトリ構成：

     Windows システムが SPP で管理されるドメインに参加している場合、Microsoft Active Directory アカウントなどのディレクトリアカウントを使用して、資産を管理することができます。**[パスワードを無期限にする]** オプションを有効にすることができます。SPP に資産を追加すると、サービスアカウントのパスワードが自動管理され、安全性を保つことができます。

   または

- ローカル設定

  Windows システムがドメインに参加していない場合、十分な権限を付与されたローカルのサービスアカウントを使用します。

2. サービスアカウントに十分な権限を与え、アカウントのパスワードの変更を許可するように、アカウントの権限を変更します。詳細については、「Windows 資産に最低限必要な権限」を参照してください。
3. システムのファイアウォールを設定して、次の定義済み受信ルールを許可します。
   - Windows Management Instrumentation (DCOM-In)
   - Windows Management Instrumentation (WMI-In)
   - NetLogon サービス(NP-In)

   これらのルールは、それぞれ TCP ポート 135 と TCP SMB 445 の受信トラフィックを許可します。
4. 以下のポートがアクセス可能であることを確認してください。
   - 389 ポートは、LDAP 接続用です。LDAP ポート 389 接続は、Active Directory 資産検出、およびディレクトリアカウント検出に使用されます。
   - 445 ポート SMB は、パスワードの確認と変更の実行に使用されます。
   - SPP が Windows プラットフォーム上でサービス検出を実行するために、RPC エフェメラルポートにもアクセスできる必要がある場合があります。（たとえば、Windows Server 2019 ではポートが必要ですが、Windows Server 2012 では不要です）。詳細については、「Windows のサービスの概要とネットワークポートの要件」を参照してください。
5. ローカルセキュリティポリシーを変更します。

   SPP が Windows システムで非ビルトイン管理者であるサービスアカウントを使用してローカルアカウントのパスワードをリセットする前に、ローカルセキュリティポリシーを変更してユーザーアカウント制御（UAC）の管理者承認モード（管理者承認モードですべての管理者を実行する）オプションを無効化する必要があります。詳細については、「パスワードまたは SSH キーの変更に失敗する」を参照してください。

ポートに関する追加情報については、「Safeguard ポート」を参照してください。

16.27 WinRM システムの準備

SPP は Windows Remote Management (WinRM) システムをサポートします。

SPP 用に Windows Remote Management (WinRM)システムを準備する手順

1. WinRM の初期構成要件は、SSL を使用するかどうかによって異なります。
    - SSL の場合（**SSL 暗号化の使用**と **SSL 証明書の検証**が資産に対して有効になっている場）：
        a. CA 署名付き証明書を資産に手動で追加する必要があります。

> **重要：**CA 証明書を Safeguard にアップロードする必要があります。
>
> 資産上で、証明書は LocalMachine\My store に、CA は LocalMachine\TrustedRoots ストアにインストールされる必要があります。中間証明書を使用する場合は、LocalMachine\Intermediate ストアにあるはずです。
>
> 証明書について、以下の要件が満たされていることを確認してください：
>
> - CN が資産のホスト名と一致する
> - CRL が存在し、解決可能である
> - サーバー認証の拡張鍵の使用が必要
>
> i. HTTPS リスナーは、次のコマンドで WinRM に登録する必要があります：
> winrm create winrm/config/Listener?Address=*+transport=HTTPS '@{Hostname="<hostname>";CertificateThumbprint="<thumbprint>"}'
>
> を使用して、WinRM で HTTPS リスナーを登録する必要があります。
>
> ii. winrm set winrm/config/service '@{CertificateThumbprint="<TUMBPRINT"}'
>
> コマンドで、証明書を設定します。
>
> iii. ファイアウォールで 5986 番ポートを開放します。
>
> iv. Windows Remoting サービスを再起動します。

    - 非 SSL の場合
        a. 資産上で、Enable-PSRemoting –Force コマンドを実行します。

2. 資産にサービスアカウントを作成し、パスワードを割り当てます。
    - ディレクトリ構成：

Windows システムが、SPP で管理されるドメインに参加している場合、Microsoft Active Directory アカウントなどのディレクトリアカウントを使用して、資産を管理することができます。**[パスワードを無期限にする]** オプションを有効にします。SPP に資産を追加すると、サービスアカウントのパスワードが自動管理され、安全性を保つことができます。

-または

- ローカル設定：

  Windows システムがドメインに参加していない場合、十分な権限を付与されたローカルのサービスアカウントを使用します。

3. サービスアカウントに、アカウントパスワードの変更を許可する十分なアクセス権を付与します。詳細については、「Windows 資産に最低限必要なアクセス許可」を参照してください。

16.28 Windows SSH システムの準備

SPP は Windows SSH システムをサポートします。Windows SSH は、プラットフォームでポート 22 を使用します。

SPP を使用するには、C:\Windows\System32\cmd.exe を SSH のデフォルトシェルとして設定する必要があります（詳細については、「Windows 10 1809 および Server 2019 用 OpenSSH Server 構成」を参照してください）。

Windows 8 での OpenSSH

Windows 8 の OpenSSH ポートは、コマンドの実行にサーバー側の制限があります。サーバー上でコマンドがすでに完了していても、タイムアウトが切れるまでコマンドが返されないため、パスワード操作の実行が遅く見えることがあります。TestConnection、ChangePassword、CheckPassword を実行する際に、接続タイムアウト (CommandTimeout) を調整して、これらのパスワード操作の実行時間を十分に確保しつつ、ネットワークに固有のその他の条件によるタイムアウトを回避するための時間を確保する必要がある場合があります。

SPP 用に Windows SSH システムを準備する手順

1. SSH サーバーサービスが実行されていることを確認します。
2. 資産にサービスアカウントを作成し、それにパスワードを割り当てます:

- **ディレクトリ構成**

  Windows SSH システムが SPP で管理されるドメインに参加している場合、Microsoft Active Directory アカウントなどのディレクトリアカウントを使用して、資産を管理することができます。**[パスワードを無期限に設定する]** オプションを有効にします。SPP に資産を追加すると、サービスアカウントのパスワードが自動管理され、安全性を保つことができます。

-または

- **ローカル設定**

  Windows SSH システムがドメインに参加していない場合、十分な権限を付与されたローカルのサービスアカウントを使用します。

  > **重要：**ローカルアカウントは、ドメインアカウントとして実行されているサービスを検出するために必要なアクセス権を持っていません。したがって、ローカルアカウントが使用されている場合、SPP はローカルアカウントとして実行されているサービスのみを検出および更新し、ドメインアカウントの依存性は更新されません。

3. サービスアカウントがローカルの Administrator グループに追加されていることを確認し、パスワードの変更権限を許可します。詳しくは、「Windows 資産に最低限必要なアクセス許可」を参照してください。

16.29 Windows 資産に最低限必要なアクセス許可

Windows Management Instrumentation（WMI）を使用してディレクトリのパスワード管理およびセッション管理のタスクを実行するために、Windows 資産には以下の最小限のアクセス許可権限が必要です。

> **メモ：**Microsoft は、DCOM サーバーの強化を開始しました。
> https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26414
> および KB5004442 - Windows DCOM Server セキュリティ機能バイパスの変更を管理する (CVE-2021-26414) をご参照ください。

資産のパスワード管理

ローカルアカウントまたはドメインアカウントを使用する：

- （Windows デスクトップおよび Window Server にのみ適用）接続のテスト、確認接続、パスワード確認、アカウント検出タスクには、以下のアクセス許可権限が必要です。
    - WMI の CIMV2 Namespace のリモート有効化権限
    - WMI の CIMV2 Namespace の Enable Account 権限
    - DCOM 経由のコンピューターにリモートアクティベーション権限

リモート有効化およびアカウント有効化権限の設定方法

1. wmimgmt.msc を開きます。
2. **［WMI コントロール（ローカル）］**を右クリックし、**［プロパティ］**を選択します。
3. **［セキュリティ］**タブを選択します。
4. **［Root］**ノードを展開します。
5. **［CIMV2］**ノードを選択します。
6. **［セキュリティ］**ボタンをクリックします。
7. ユーザー/グループを追加し、**［アカウントの有効化］**と**［リモートの有効化］**を選択します。
8. **［OK］**をクリックします。

リモートからのアクティブ化権限の設定方法

1. dcomcnfg を開きます。
2. **［コンポーネントサービス］＞［コンピューター］**を展開します。
3. **［マイコンピューター］**を右クリックし、**［プロパティ］**を選択します。
4. **［COM セキュリティ］**タブを開きます。
5. **［起動とアクティブ化のアクセス許可］**で、**［制限の編集］**を選択します。
6. ユーザー/グループを追加し、**［リモートからのアクティブ化］**を選択します。

7. **［OK］**をクリックします。

- パスワード変更タスクには、以下の権限が必要です：
    - ローカル Administrators グループのメンバー

ドメインパスワード管理

ドメインアカウントの使用

- 接続のテスト、接続のチェック、パスワード確認、アカウント検出の各タスクには、以下の権限が必要です：
    - ドメインユーザーのメンバー
- パスワード変更タスクでは、Service アカウントに以下の権限を委譲する必要があります。
    - LockoutTime（読み取り/書き込み）
    - アカウント制限（読み取り/書き込み）
    - パスワードのリセット

資産セッションアクセス

ローカルアカウントの使用

- Remote Desktop Users グループのメンバーであること
- （直接またはグループメンバーシップで）**［リモートデスクトップサービスを使ったログオンを許可］**ポリシーで定義されている
- （直接またはグループメンバーシップで）**［リモートデスクトップサービスを使ったログオンを拒否］**ポリシーで定義されていない

ドメインアカウントの使用

- Remote Desktop Users グループに定義されているか、その資産の Remote Desktop Users グループに対するグループポリシーの更新により、ドメインのセキュリティグループのメンバーである
- （直接またはグループメンバーシップで）**［リモートデスクトップサービスを使ったログオンを許可］**ポリシーで定義されている

- （直接またはグループメンバーシップで）**[リモートデスクトップサービスを使ったログオンを拒否]**ポリシー定義されていない

17 トラブルシューティング

One Identity では、SPP を導入して使用する際に遭遇する可能性のある一般的な問題に対して、以下の解決策を推奨しています。SPP のトラブルシューティング方法については、「アプライアンス」を参照してください。

17.1 アプライアンスシック（Appliance is sick）

アプライアンスの調子が悪い場合、さまざまな原因が考えられます。appliance is sick エラーが表示された場合は、次の手順を実行してください。

1. ノード間のネットワーク接続をチェックします。
2. エラーが自動的に解決されるかどうかを確認するために待ちます（最大 30 分）。
3. エラーが解消されない場合は、サポートバンドルを作成し、サポートに連絡します。詳細については、「Support Bundle」を参照してください。

アプライアンスシックイベントのエラーメッセージ接頭辞カテゴリ

アプライアンスシックイベントには 6 つのカテゴリがあり、エラーメッセージの接頭辞で区別できます。

Audit Log is sick : <理由>

基礎となる監査ログデータベースでエラーが発生しました。理由には、正確な問題についての詳細が記載されています。通常、これはネットワーク接続の結果、コンセンサスが失われることが原因です。これは一時的なネットワーク状態の結果である可能性があり、その場合は数分後に自動的に解決されます。そうでない場合は、Safeguard ノード間のネットワーク接続を確認してください。ネットワーク接続を除外した後、サポートバンドルを生成し、サポートに連絡してください。サポートに相談するまでは、アプライアンスを再起動しないでください。場合によっては、アプライアンスを再起動すると、状態が悪化することがあります。

Access Request Workflow is sick : <理由>

基礎となるパスワードワークフローデータベースでエラーが発生しました。理由には、正確な問題についての詳細が記載されます。通常、これはネットワーク接続の結果、コンセンサスが失われることが原因です。これは一時的なネットワーク状態の結果である可能性があり、その場合は数分後に自動的に解決されます。そうでない場合は、Safeguard ノード間のネットワーク接続を確認してください。ネットワーク接続を除外した後、サポートバンドルを生成し、サポートに連絡してください。

Policy Data is sick : <理由>

基礎となるポリシーデータベースでエラーが発生しました。理由には、正確な問題の詳細が記載されています。通常、これはレプリカがプライマリへのネットワーク接続を失ったときに発生します。これは一時的なネットワーク状況の結果である可能性があり、その場合、数分後に自動的に解決されます。そうでない場合は、Safeguard ノード間のネットワーク接続を確認します。ネットワーク接続を除外した後、サポートバンドルを生成し、サポートに連絡してください。

Cluster Connectivity is sick : <理由>

Safeguard ノード間の VPN 接続にエラーが発生しています。理由には正確な問題についての詳細が記載されます。一時的なネットワーク状況の結果である可能性があり、その場合は数分後に自動的に解消されます。そうでない場合は、VPN がパブリック IP 上でトンネルされているため、パブリック IP アドレス上の Safeguard ノード間のネットワーク接続を確認してください。ネットワーク接続を除外した後、サポートバンドルを生成し、サポートに連絡してください。

Appliance Resource Usage is sick : <理由>

Safeguard のプロセスまたは基礎となるデータベースが、予期せぬ高い OS リソース使用量 (CPU、メモリ、ディスク)を示しています。理由には、正確な問題についての詳細が記載されています。アプライアンスを再起動することで、この問題が解決する場合があります。問題が継続する、または頻繁に発生する場合は、サポートバンドルを生成してサポートに連絡してください。

17.2 接続障害

SPP の最も一般的な障害原因は、アプライアンスと管理システム間の接続性の問題、またはサービスアカウントに関する問題のいずれかです。

トラブルシューティングを行う前に、必ずネットワークの接続性と資産の電源を確認してください。

以下のトピックでは、パスワードの確認、パスワードの変更、パスワードの設定に失敗する理由として考えられるものを説明し、実行可能な修正手順を紹介します。

- パスワードの変更または SSH キーの変更に失敗する：パスワードの変更に失敗した場合に考えられる解決策について説明します。
- 認証資格情報が正しくない：サービスアカウントの認証情報が正しくない場合の解決方法について説明します。
- SSH ホストキーがない、または正しくない：SSH ホストキーの問題を解決する方法について説明します。
- サポートされている暗号がない：暗号のサポートに関する問題の解決方法を参照してください。
- サービスアカウントに十分な特権がない：サービスアカウントの権限の問題を解決する方法を参照してください。

17.2.1 パスワードまたは SSH キーの変更に失敗する

組み込みの Administrator 以外の Administrative 権限を持つサービスアカウントで構成された Windows 資産を使用している場合、ローカルアカウントのパスワードまたは SSH キーの変更に失敗することがあります。

> **メモ:** SPP が Windows システムで組み込みの Administrator 以外の管理者グループのメンバーを使用してローカルアカウントのパスワードを変更する前に、ローカルセキュリティポリシーを変更してユーザーアカウント制御（UAC）の 管理者承認モード（**管理者承認モードですべての管理者を実行する**）オプションを無効化する必要があります。

アカウントのパスワードを変更するように Windows 資産を設定する手順

1. **［ファイル名を指定して実行］**ダイアログから secpol.msc を実行します。

   -または

   Windows の**［スタートメニュー］**から、**［ローカルセキュリティポリシー］**を開きます。

2. **［ローカルポリシー］＞［セキュリティオプション］**を開きます。

3. **［ユーザーアカウント制御：管理者承認モードですべての管理者を実行する］**オプションを選択します。

4. コンピューターを再起動します。

詳細については、「Windows システムの準備」を参照してください。

17.2.2 不正な認証情報

資産に認証するためには、正しいユーザー名とパスワードまたは SSH キーが必要です。

誤ったサービスアカウントの認証情報を解決する手順

1. サービスアカウントの認証情報が SPP の資産情報（**［資産管理］＞［資産］＞［全般］タブ［接続］**）にある認証情報と一致することを確認します。詳細については、「サービスアカウントについて」を参照してください。

2. 接続を確認するために、**［接続のテスト］**を実行します。詳細については、「接続のテスト」を参照してください。

3. パスワードまたは SSH キーの確認、変更、および設定を再度試行します。詳細については、「アカウントパスワードの確認、変更、設定」「SSH キーの確認、変更、設定」を参照してください。

17.2.3 SSH ホストキーの欠落または不正確

SPP の資産が SSH ホストキーを必要とするがそれがない場合、SPP はその資産と通信することができません。詳細については、「証明書の問題」を参照してください。

SSH ホストキーの欠落を解決する方法

資産に SSH ホストキーがあることを確認するには、資産を選択し、**［全般］**ビューの**［接続］**の下を探します。SSH ホストキーのフィンガープリントが表示されていない場合は、追加する必要があります。

SSH ホストキーの追加手順

1. 資産の**［接続］**タブを開きます。

2. 任意の認証タイプ（**[なし]** を除く）を選択し、必要な情報を入力します。

   > **メモ：** サービスアカウントのパスワードまたは SSH キーを再度入力する必要があります。

3. **[接続のテスト]** をクリックします。

   [接続のテスト] は、アプライアンスが資産と通信できることを確認します。

4. SSH ホストキーを受け入れるかどうかを確認します。

   > **メモ：** SSH ホストキーの検証を回避し、キーを自動的に受け入れるには、**[SSH ホストキーの自動承認]** オプションをクリックします。

5. **[OK]** をクリックして、資産を保存します。

不正な SSH ホストキーを解決する方法

SPP は、キー交換に次のホストキーアルゴリズムを使用します：

- DSA
- ECDSA
- RSA

不一致の原因を調査し、**[接続のテスト]** を使用して不一致を解決します。

17.2.4 No cipher supported エラー

There is no cipher supported by both: client and server（クライアントとサーバーの両方でサポートされている暗号がない）というエラーメッセージを受信した場合は、「暗号のサポート」を参照してください。

17.2.5 サービスアカウントに十分な権限がない

サービスアカウントに問題がある場合、次のことを検討してください。

- サービスアカウントは、システムにアクセスするための適切な権限を与えられていますか？一般的な設定では、システム上でサービスアカウントの権限を昇格させるために sudo が使用されます。
- サービスアカウントがロックアウトされたり、無効化されたりしていないか？

- サービスアカウントがリモートログオンを許可するように設定されているか？

サービスアカウントは、他のアカウントのパスワードを編集するために十分な権限を必要とします。詳細については、「サービスアカウントについて」を参照してください。

不正または不十分なサービスアカウント権限を解決する手順

1. サービスアカウントが資産に対して十分な権限を持っていることを確認します。
2. 接続を確認するために、**［接続テスト］**を実行します。
3. 失敗したアカウントで、パスワードの手動確認、変更、設定を再度試行します。

資産が Windows オペレーティングシステムを実行している場合、組み込みの Administrator 以外の管理者権限を持つサービスアカウントで構成されている資産を使用していると、ローカルアカウントのパスワードまたは SSH キーのチェック、変更、設定に失敗することがあります。

SPP が Windows システム組み込みの Administrator 以外のサービスアカウントを使用してローカルアカウントのパスワードまたは SSH キーを変更する前に、ローカルセキュリティポリシーを変更して**［管理者承認モードですべての管理者を実行する］**オプションを無効にする必要があります。詳細については、「パスワードまたは SSH キーの変更に失敗する」を参照してください。

17.3 SSH または RDP でリモートマシンに接続できない

SSH または RDP でリモートマシンに接続できない場合は、SPP クライアントにアプライアンス管理者としてログインし、アクティビティセンターとログを確認して追加情報を確認します。

17.4 アカウントを削除できない

アカウントを削除できない場合は、以下の点をご確認ください。

アカウント名が間違っている

資産管理者として、アカウントを削除しようとすると、次のようなエラーが表示されることがあります：This entity has access requests which have not yet expired or have to be reviewed. It cannot be deleted now.（このエンティティには、まだ有効期限が切れていないアクセスリクエストがあるか、またはレビューが必要です。現在、削除することはできません。）このエラー

は、SPP が資産に存在しないアカウントのパスワードまたは SSH キーを変更しようとしていることを示す可能性があります。

このエラーメッセージの理由の 1 つは、Safeguard にアカウントを追加する際に間違ったアカウント名が使用されたことです。そのため、現在、誰かがこのアカウントのパスワードまたは SSH キーをリクエストすると、Safeguard は手動で設定されたパスワードまたは SSH キーを表示します。しかし、要求者が不正なアカウントとパスワードまたは SSH キーを使用して資産にログインしようとすると、失敗します。アクセスリクエストポリシーで**［チェックイン後にパスワードを変更する］**が指定されている場合、管理者が特権パスワード用 Safeguard からアカウントを削除しようとすると、上記のエラーメッセージが表示されます。

回避策：スペルミスのある名前を持つアカウントを削除するには、まず、そのアカウントのパスワードまたは SSH キーを手動で設定します。アカウントのパスワードがリセットされると、SPP はアカウントの削除を許可します。

詳細については、「アカウントパスワードの確認、変更、設定」、「SSH キーの確認、変更、設定」を参照してください。

17.5 セッションを再生できない

Cannot play session... The specified executable is not a valid application for this OS platform（セッションを再生できません... 指定された実行ファイルは、この OS プラットフォームで有効なアプリケーションではありません。）というメッセージが表示された場合、サポートされていない 32 ビットプラットフォームでデスクトッププレーヤーを実行しようとしている可能性が高いです。

17.6 ドメインユーザーが SPP へのアクセスを拒否される

Active Directory で**［ユーザーは次回ログオン時にパスワード変更が必要］**オプションを有効にしているディレクトリユーザーを追加すると、SPP によってそのユーザーのログインが阻害されます。ディレクトリユーザーが SPP に正常にログインできるようにするには、次の 2 つの方法があります。

- ディレクトリユーザーのドメインアカウントを使用して、Active Directory に参加した資産にログインさせます。プロンプトが表示されたら、パスワードを変更することができます。これは、**［ユーザーは次回ログオン時にパスワード変更が必要］**オプションを満たします。

  -または

- ドメイン管理者に、ディレクトリユーザーの Active Directory のオプションを無効にしてもらいます。

17.7 LCD ステータスメッセージ

SPP アプライアンスには LCD 画面があり、起動時や特定の操作の進行に応じてアプライアンスのステータスが表示されます。

さまざまな段階が進むと、次のような LCD ステータスメッセージが表示されます。初回起動時の設定とは、SPP の初期設定を意味し、通常、アプライアンスの導入時および工場出荷時のリセット後に行われるものです。

- **更新の適用 xx%**: アプライアンスの更新操作の進行に伴い、完了したパーセンテージが表示されます。
- **工場リセット xx%:** アプライアンスの工場出荷時リセットの進行に伴い、完了したパーセンテージが表示されます。
- **初回起動 ... <バージョン>**: SPP のロードを待っている間、最初のブートが完了した後に表示されます。
- **初回ブート設定 xx%:** アプライアンスが初めて設定される際に、完了したパーセンテージが表示されます。
- **初回ブートセットアップの準備中**：工場出荷時リセットの後、アプライアンスが初めて設定される前に表示されます。
- **検疫**：アプライアンスが隔離状態にあることを示します。詳細については、「アプライアンスが隔離された場合の対処法は？」を参照してください。
- **Starting core**:SPP がロード中であることを示します。
- **データベース開始中**：SPP データベースがロードされていることを示します。
- **再起動開始中**：アプライアンスが再起動中であることを示します。
- **サービス開始中**：SPP サービスがロード中であることを示します。
- **シャットダウン開始中**：アプライアンスがシャットダウン中であることを示します。
- **Web 開始中**： Web サービスがロード中であることを示します。

アプライアンスが実行中の場合、LCD ホーム画面に次のメッセージが表示されます：Safeguard for Privileged Passwords <version number>

17.7.1 アプライアンス LCD とコントロール

One Identity Safeguard for Privileged Passwords アプライアンスの前面パネルには、電源オン、電源オフ、および LCD ディスプレイのスクロールのための以下のコントロールが含まれています。

- 緑色の ✔チェックマークボタン：アプライアンスを起動するには、**緑色のチェックマークボタン**を使用します。アプライアンスの電源をオンにするには、**緑のチェックマーク**ボタンを 1 秒以上**押さないでください**。

  > ⚠ **注意 SPP アプライアンスが起動したら、緑色のチェックマークボタンを押し続けないでください。このボタンを 4 秒以上押し続けると、アプライアンスの電源がコールドリセットされ、損傷する可能性があります。**

- 赤い X ボタン：本機をシャットダウンするには、**赤い X** ボタンを使用します。LCD に POWER OFF と表示されるまで、**赤い X** ボタンを 4 秒間押し続けてください。

  > ⚠ **注意 SPP アプライアンスが起動したら、赤い X ボタンを 13 秒以上押し続けないでください。アプライアンスが強制シャットダウンされ、損傷する可能性があります。**

- 下、上、左、右矢印ボタン：アプライアンスが動作しているとき、LCD ホーム画面が表示されます：Safeguard for Privileged Passwords <version number>と表示されます。矢印ボタンを使用して、次の詳細をスクロールします：
  - Serial： <アプライアンスのシリアル番号>
  - X0： <アプライアンス IP アドレス>
  - MGMT：<管理用 IP アドレス>
  - MGMT MAC: <メディアアクセスコントロールアドレス>
  - IPMI：<IPMI 用 IP アドレス>

表：アプライアンス LCD とコントロール

コントロール	説明
緑色のチェックマークボタン	**緑色のチェックマーク**ボタンを使用して、アプライアンスを起動します。アプライアンスの電源を入れるために、**緑色のチェックマーク**ボタンを 1 秒以上押さないでください。 ⚠ **注意：SPP アプライアンスが起動したら、緑のチェックマークボタンを押したままにしないでください。このボタンを 4 秒以上押し続けると、アプライ**

コントロール	説明
	アンスの電源がコールドリセットされ、損傷する可能性があります。
赤い X ボタン	**赤い X** ボタンを使用して、アプライアンスをシャットダウンします。LCD 画面に POWER OFF と表示されるまで、**赤い X** ボタンを 4 秒間押し続けます。 **注意：** SPP アプライアンスが起動したら、赤い X ボタンを 13 秒以上押し続けないでください。これは、アプライアンスの強制シャットダウンとなり、破損の原因となる可能性があります。
↓、↑、←、→矢印ボタン	アプライアンスを実行すると、LCD ホーム画面が表示されます： • Safeguard for Privileged Passwords <バージョン番号> 矢印ボタンを使用して、以下の詳細をスクロールします： • Serial： <アプライアンスのシリアル番号> • X0： <アプライアンス IP アドレス> • MGMT：<管理用 IP アドレス> • MGMT MAC: <メディアアクセスコントロールアドレス> • IPMI：<IPMI 用 IP アドレス>

17.8 Mac のキーチェーンパスワードまたは SSH キーを紛失した

Macintosh OS X のキーチェーンは、Apple のパスワードと SSH キーの管理システムです。キーチェーンには、アプリケーション、サーバー、Web サイトのすべてのパスワードと SSH キー、あるいはクレジットカード番号や銀行口座の暗証番号など、コンピューターとは無関係の機密情報まで保存することができます。

Mac OS X システムを SPP に追加した場合、「ログインキーチェーンのロックを解除できませんでした」というメッセージが表示されることがあります。これは、SPP が、セキュリティポリシー管理者が設定したポリシーに基づいて、すべての管理対象システムのアカウントパスワードを自動的に更新しますが、キーチェーンパスワードは更新されないためです。

17.9 Unix ホストでパスワードが失敗する

一部の Unix システムでは、パスワードが許容される最大の長さまで暗黙で切り捨てられます。たとえば、Macintosh OS X では、パスワードは 128 文字までしか許可されません。資産管理者がパスワードの長さを 136 文字に設定するアカウントパスワードルール付きのプロファイルを作成した場合、SPP がそのプロファイルによって管理されるアカウントのパスワードを変更すると、資産の OS は新しいパスワードを許容長に切り捨ててエラーを返しませんが、136 文字の完全パスワードは SPP に保存されます。このため、次のような問題が発生します。

- アカウントのパスワード確認に失敗する：SPP が Unix ホストのパスワードと SPP のパスワードを比較すると、Unix ホストが SPP で生成したパスワードを切り捨てたため、両者が一致しません。
- ユーザーは、オペレーティングシステムが課す許容長までパスワードを切り詰めない限り、SPP が提供するパスワードで Unix ホストのアカウントに正常にログインすることはできません。

17.10 パスワードまたは SSH キーのリセットが保留されている

ユーザーが以下のいずれかの永続的なメッセージを受け取った場合、アカウントのパスワードはパスワードの変更を保留している状態で止まっています：

- You cannot checkout the password for this account while another request is pending password reset（別のリクエストがパスワードのリセットを保留している間は、このアカウントのパスワードをチェックアウトすることはできません。）
- This account has password requests which have not yet expired or have to be reviewed. It cannot be deleted now"（このアカウントには、まだ有効期限が切れていない、またはレビューが必要なパスワードリクエストがあります。今すぐ削除することはできません。）

考えられる解決策：

- このアカウントに関連付けられた資産のサービスアカウントが動作していることを確認します。その後、手動でアカウントのパスワードを変更します。詳細については、「アカウントパスワードの確認、変更、設定」および「SSH キーの確認、変更、設定」を参照してください。
- または、資産のサービスアカウントが正常に動作しており、そのアカウントを管理するポリシーで緊急アクセスを許可し、複数のユーザーの同時アクセスを有効にしてい

る場合、緊急アクセスを使用してパスワードをリクエストするようにユーザーに指示することができます。

事前のリクエストが承認されているかどうかにかかわらず、新しいアクセスリクエストを許可することができます。言い換えれば、事前のリクエストの承認状況に基づいて、リクエストがブロックされることはありません。**[保留中のレビューでアクセスをブロックしない]**チェックボックスを設定するのは、将来のリクエストにのみ関係します。詳細については、「要求者タブ」を参照してください。

17.11 パスワードまたは SSH キーのプロファイルが実行されない

パスワードおよび SSH キーの管理の設定（**[アプライアンス管理] > [サービスの有効化または無効化]**）は、パーティションでのプロファイルの自動チェックと変更スケジュールを有効にします。

プロファイルをスケジュールで実行するために、パスワード管理の設定が有効になっていることを確認します：

- パスワードのチェック管理が有効であること
- パスワードの変更管理が有効であること
- SSH キーのチェック管理が有効であること
- SSH キーの変更管理が有効であること

17.12 リカバリキオスク（Serial Kiosk）

SPP は、リカバリキオスク（Serial Kiosk）を提供しており、以下のオプションがあります：

- アプライアンス情報（Recovery Kiosk）：基本的なアプライアンス情報を表示します。
- 電源オプション：これらのオプションにより、アプライアンスをリモートで再起動またはシャットダウンすることができます。
- 管理者パスワードのリセット：Bootstrap 管理者のパスワードを初期値にリセットできます。
- リカバリキオスクからの工場出荷時リセット：大きな問題から回復したり、アプライアンスのデータと構成設定をクリアしたりできるようにします。

工場出荷時リセットは、仮想アプライアンスでは利用できません。仮想アプライアンスの場合は、バックアップし回復させてください。詳細については、「仮想アプライアンスのバックアップと復元」を参照してください。

> ⚠ **注意： この操作では、すべてのデータと監査履歴が削除され、工場から最初に出荷されたときの状態に戻るため、物理アプライアンスに対して工場出荷時リセットを実行する場合は、注意が必要です。工場出荷時リセットの実行は、BMC/IPMI インターフェイスや IP アドレスをリセットしませんが、リセット完了後、BMC/IPMI インターフェイスを再度有効にする必要があります（詳細については、「ライトアウト管理（BMC）」を参照してください）。アプライアンスは、工場から出荷されたばかりであるかのように、再度設定を行う必要があります。詳細については、「SPP の初期設定」を参照してください。**
>
> **さらに、工場出荷時のリセットを実行すると、デフォルトの SSL 証明書とデフォルトの SSH ホストキーが変更される場合があります。**
>
> **アプライアンスは、現在のロングタームサポート（LTS）バージョンにリセットされます。たとえば、バージョン 6.6（機能リリース）または 6.0.6 LTS（メンテナンスロングタームサポートリリース）を使用している場合に工場出荷時リセットを行うと、アプライアンスは 6.0 LTS にリセットされ、現在のバージョンまでパッチアップする必要があります。詳細については、「長期サポート（LTS）とフィーチャーリリース」を参照してください。**

- Support Bundle: Windows 共有にサポートバンドルを生成して送信できるようにします。

Recovery Kiosk を起動する手順

Recovery Kiosk を実行しているターミナルまたはラップトップで、以下のようにシリアルポートの設定を行う必要があります：

1. シリアルケーブルをラップトップまたはターミナルから、アプライアンスの背面にある **|0|0|** とマークされたシリアルポートに接続します。
2. ラップトップまたはターミナルで、シリアルポートの設定を以下のように構成します：
    - Speed： 115200
    - Data bits：8
    - Parity： None
    - Stop bit： 1
3. これらのオプションは、Recovery Kiosk の画面に表示されます：
    - **アプライアンス情報**

- **電源オプション**
  - **再起動**
  - **シャットダウン**
- **管理者パスワードのリセット**
- **ファクトリーリセット**（仮想アプライアンスは使用不可）
- **Support Bundle**

4. 上矢印と下矢印を使用して、これらのオプションのいずれかを選択します。
5. 右矢印を使用して、オプションを開始します。
6. 左矢印を使用して、オプションに戻ります。

Kiosk キーボードショートカット

SPP では、次のキーボードショートカットを提供しています。ウィンドウを小さくしすぎてキオスクの要素が表示されない場合、SPP はウィンドウサイズを再調整する方法を説明します。

- **Ctrl + D**：キオスクを元の状態にリセットします。チャレンジとオプションをクリアします。

  > ⚠ **注意： Bootstrap 管理者のパスワードをリセットするとき、または工場出荷時リセットを実行するとき、One Identity Support からの応答を受け取る前にキオスクをリセットすると、新しいチャレンジを提出する必要があります。**

- **Ctrl + R**：サイズを変更したウィンドウに合うようにキオスクを再描画します。ウィンドウのサイズを変更した場合、**Ctrl + R** を押してキオスクの要素を再編成し、新しいサイズのウィンドウに正しく適合させます。

17.12.1 アプライアンス情報（リカバリーキオスク）

アプライアンスの基本情報を表示し、IP アドレスを編集するには、Recovery Kiosk の**［アプライアンス情報］**オプションを使用します。

Azure を使用している場合、Azure で SPP VM を静的 IP アドレスで構成します。Safeguard アプライアンスの IP アドレスを変更する必要がある場合、または Azure の動的構成によって変更され、アプライアンスがクラスタの一部である場合、アプライアンスは次の起動時に自動的にスタンドアロン読み取り専用モードにリセットされます（効果的にクラスタを離脱）。管理者は、アプライアンスをクラスタに戻すことができます。

アプライアンス情報を表示または編集する手順

1. Recovery Kiosk から、**［アプライアンス情報］**オプションを選択します。
2. 右矢印で表示されます：
    - アプライアンスの状態：アプライアンスの現在の状態
    - 稼働時間：アプライアンスが稼働している時間（時間および分）
    - MGMT（Azure では使用不可）： MAC アドレスと IPv4（およびオプションで IPv6）プロパティを含む、管理ホストのネットワークインターフェイスのプロパティ
    - X0：アプライアンスをネットワークに接続するプライマリインターフェイスのネットワークインターフェイスプロパティ（MAC アドレスと IPv4（およびオプションで IPv6）プロパティを含む）
3. プライマリインターフェイス（X0）のネットワークプロパティを変更するには、該当する見出しの横にある**［編集］**をクリックします。**［編集］**をクリックすると、変更可能なネットワークインターフェイスのプロパティが表示されます。Azure を使用している場合、IP アドレスは変更できません。
4. ネットワークインターフェイスのプロパティを編集したら、**［送信］**をクリックします。

   更新が完了すると、Network interface update request accepted（ネットワークインターフェイスの更新リクエストが受理されました）メッセージが表示されます。

17.12.2 電源オプション

Recovery Kiosk の電源オプションを使用して、物理アプライアンス、AWS または Azure の仮想デプロイメントをリモートで再起動またはシャットダウンします。

- アプライアンスを再起動するには、Recovery Kiosk の**［再起動］**オプションを使用できます。SPP Web クライアントまたは API にアクセスできず、通常の手順を使用してアプライアンスを再起動できない場合は、Recovery Kiosk から再起動します。AWS または Azure の仮想配置を再起動します。
- 物理アプライアンスまたは AWS または Azure 仮想デプロイメントをシャットダウンするには、Recovery Kiosk で**［シャットダウン］**オプションを使用する必要があります。

アプライアンスの再起動

Recovery Kiosk からアプライアンスを再起動することができます。

通常の手順を使用してアプライアンスを再起動するために SPP Web クライアントまたは API にアクセスできない場合、Recovery Kiosk からアプライアンスまたは Azure VM を再起動することができます。

アプライアンスを再起動する手順

1. Recovery Kiosk から、**［Power Options］＞［Reboot］**オプションを選択します。
2. 右矢印を押します。
3. プロンプトが表示されたら、**［Yes］**を選択して再起動を開始するか、**［No］**を選択してメインオプション画面に戻ります。

アプライアンスのシャットダウン

Recovery Kiosk からアプライアンスをシャットダウンすることができます。SPP アプライアンスを手動でシャットダウンするには、Recovery Kiosk を使用する必要があります。また、Azure 仮想マシンデプロイメントをシャットダウンすることもできます。

アプライアンスのシャットダウン手順

1. Recovery Kiosk から、**［Power Options］＞［Shut Down］**オプションを選択します。
2. 右矢印を押します。
3. プロンプトが表示されたら、**［Yes］**を選択してアプライアンスをシャットダウンするか、**［No］**を選択してメインオプション画面に戻ります。

17.12.3　admin パスワードのリセット

ハードウェアアプライアンスまたは AWS や Azure の仮想デプロイメントを使用する際に、Bootstrap Administrator のパスワードがロックアウトされた場合、初期パスワードにリセットすることができます。

メモ: ユーザーが設定した日数、SPP にログオンしていない場合、SPP はそのユーザーアカウントを無効化します。これは、**［アプライアンス管理］＞［Safeguard アクセス］＞［ローカルログイン制御］の［次の期間が経過したら非アクティブ化］**設定を使用して設定します。

Bootstrap Administrator パスワードのリセット手順

1. シリアルケーブルを使用して物理的に、または IPMI ネットワークインターフェイスを使用して、Recovery Kiosk に接続します
2. Recovery Kiosk から、**［Admin Password Reset］**オプションを選択します。
3. 右矢印を押します。
4. **［id］**で、自分の ID を入力し、**［Tab］**キー（または下矢印）を押します。
5. **［Get Challenge］**で、**［Enter］**キーを押します。

   Safeguard for Privileged Passwords でチャレンジが生成されます。
6. チャレンジをテキスト文書にコピーして貼り付け、One Identity Support に送信します。
   - チャレンジレスポンスの有効期間は 48 時間です。
   - チャレンジレスポンスの操作中にページから移動したり、更新したりしないでください。チャレンジレスポンスが無効になります。シリアルケーブルは切断しないでください。
7. One Identity Support から応答が届いたら、その応答を Kiosk 画面にコピーして貼り付け、**［Reset Password］**(パスワードのリセット) を選択します。応答は、One Identity が生成してから 24 時間のみ有効です。
8. 操作が完了すると、管理者アカウントのパスワードはデフォルトの **Admin123** に戻ります。

メモ：ベストプラクティス：アプライアンスを安全に保つために、Bootstrap Administrator アカウントのデフォルトパスワードを変更してください。

MGMT ポートを使用して管理者パスワードをリセットするなどの詳細については、ナレッジベース記事 KB 279291 を参照してください。

17.12.4　リカバリキオスクからの工場出荷時リセット

Recovery Kiosk には、**工場出荷時リセット**の選択肢があります。**工場出荷時リセット**は、SPP ハードウェアアプライアンスをリセットして、大きな問題から回復したり、アプライアンスのデータや構成設定をクリアしたりすることができます。

工場出荷時リセットは、仮想アプライアンスのオプションにはありません。アプライアンスを再デプロイしてください。

> ⚠ **注意：この操作では、すべてのデータと監査履歴が削除され、工場から最初に出荷されたときの状態に戻るため、物理アプライアンスに対して工場出荷時リセットを実行する場合は、注意が必要です。工場出荷時リセットの実行は、BMC/IPMI インターフェイスや IP アドレスをリセットしません。ただし、リセットの完了後、BMC/IPMI インターフェイスを再度有効にする必要があります（詳細については、「ライトアウト管理（BMC）」を参照してください）。アプライアンスは、工場出荷時と同じく、再度設定を行う必要があります。詳細については、「SPP の初期設定」を参照してください。**
>
> **さらに、工場出荷時のリセットを実行すると、デフォルトの SSL 証明書とデフォルトの SSH ホストキーが変更される場合があります。**
>
> **アプライアンスは、現在のロングタームサポート（LTS）バージョンにリセットされます。たとえば、バージョン 6.6（機能リリース）または 6.0.6 LTS（メンテナンスロングタームサポートリリース）を使用している場合に工場出荷時リセットを行うと、アプライアンスは 6.0 LTS にリセットされ、現在のバージョンにパッチアップする必要があります。詳細については、「長期サポート（LTS）と機能リリース」を参照してください。**

クラスタ化されたアプライアンスでの工場出荷時リセット

クラスタ化されたハードウェアアプライアンスで工場出荷時リセットを実行しても、クラスタからアプライアンスが自動的に削除されるわけではありません。推奨されるベストプラクティスは、アプライアンスの工場出荷時リセットを実行する前に、クラスタからアプライアンスを参加解除することです。参加解除と工場出荷時リセットの後、アプライアンスを再度構成する必要があります。詳細については、「SPP の初期設定」を参照してください。

Recovery Kiosk から工場出荷時リセットを実行する手順

> ⚠ **注意：工場出荷時リセットプロセスの一部として、チャレンジレスポンス操作を実行します。チャレンジレスポンスの無効化を避けるため、ページから移動したり、更新したりしないでください。**

> **チャレンジレスポンス操作が無効になった場合、プロセスを再起動して新しいチャレンジレスポンスを生成してください。それができない場合は、One Identity サポートに連絡してください。**

1. ハードウェアの工場出荷時リセットを実行するには、Recovery Kiosk に移動します。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。
2. **［Factory Reset（工場出荷時リセット）］**を選択します。
3. 右矢印を押します。
4. **［id］**でメールまたは名前を入力し、**［Tab］**キー（または下矢印）を押します。
5. **［Get Challenge］**で、**［Enter］**キーを押します。SPP からチャレンジが表示されます。
6. チャレンジをコピーして貼り付け、One Identity Support に送信します。チャレンジレスポンスの有効期間は 48 時間です。チャレンジレスポンスの操作中に、ページから移動したり、更新したりしないでください。チャレンジレスポンスが無効になります。
7. One Identity Support からレスポンスが届いたら、レスポンスをコピーして Kiosk 画面にして貼り付け、**［Factory Reset］**を選択します。レスポンスは、One Identity によって生成されてから 24 時間のみ有効です。
8. 工場出荷時リセットが完了すると、アプライアンスを再設定する必要があります。

工場出荷時リセットのための MGMT ネットワークインターフェイスの使用に関する詳細は、ナレッジベース記事 KB 232766 を参照してください。

17.12.5 Support Bundle

Support Bundle 機能を使用する前に、サポートバンドルが送信される Windows 共有をセットアップします。

サポートバンドルの生成手順

1. Recovery Kiosk から、**［Support Bundle］**（サポートバンドル）オプションを選択します。
2. 右矢印を押します。
3. 生成するサポートバンドルの種類を選択します：

- Support Bundle
- Quarantine Bundle

4. プロンプトが表示されたら、次の情報を入力します:
    - アドレス：Support Bundle を保存する Windows 共有のアドレス(<IP アドレス>\<共有名>)を入力します。
    - ユーザー：Windows 共有にアクセスするために使用されるユーザー名を入力します。
    - パスワード：指定したユーザーアカウントに関連するパスワードを入力します。

    > **メモ：** Windows 共有が匿名アクセスを許可するように設定されている場合、ユーザー名またはパスワードの入力は要求されません。

5. **［Copy to Share］**（共有にコピー）を選択します。完了すると、指定した共有にサポートバンドルが送信されたことを示すメッセージが表示されます。

17.12.6 レプリカが追加されない

クラスタにアプライアンスを追加しようとしたときに、An internal request has timed out...（内部リクエストがタイムアウトしました...）というメッセージが表示される場合は、SPP アプライアンスがプライマリと同じバージョンであることを確認してください。クラスタのすべてのメンバーが同じである必要があります。

17.12.7 パスワードまたは SSH キーの変更後、システムサービスが更新または再起動されない

パスワードまたは SSH キーの自動変更後にシステムサービスが更新または再起動されない場合、まずアクティビティセンターの監査ログを確認してください。

> **メモ：** Support Bundle ログを確認することもできます。

監査ログで問題が適切に説明されない場合は、サービスアカウントを管理するプロファイルの**［パスワードの変更］**または**［SSH キーの変更］**タブのオプションを確認してください。

1. **［資産管理］＞［パーティション］**に移動します。

2. パーティションを選択して、**［詳細の表示］**を選択します。
3. **［パスワードプロファイル］**または**［SSH キープロファイル］**をクリックします。
4. グリッドで選択したものをダブルクリックします。
5. **［パスワードの変更］**または**［SSH キーの変更］**タブに移動します。

システムサービスまたはスケジュールされたシステムタスクを実行するサービスアカウントの場合、プロファイルの**［パスワードの変更］**タブまたは**［SSH キーの変更］**で、自動サービス更新、再起動を有効または無効にするオプションを確認します。これらのオプションを変更するには、設定を更新する必要があります。

17.12.8 接続のテストが失敗する

SPP の最も一般的な失敗の原因は、アプライアンスと管理システム間の接続の問題、またはサービスアカウントの問題のいずれかです。詳細については、「接続障害」を参照してください。

リモートホストでユーザーアカウント制御（UAC）の管理者承認モードを無効にすると、接続テストの失敗を解決することもできます。詳細については、「パスワードまたは SSH キーの変更に失敗する」を参照してください。

ドメインコントローラーの指定に値を入力し、SPP がリスト内でドメインコントローラーを見つけられない場合、テスト接続は失敗し、エラーが返されます。

以下のトピックでは、接続テストが失敗する可能性のある理由をいくつか説明します。

- アーカイブサーバーでの接続テスト失敗：アーカイブサーバーの接続のテストの失敗を解決する方法について説明します。
- 証明書の問題：SSL を必要とする資産に対する接続のテストの失敗を解決する方法について説明します。
- 暗号のサポート：SPP の暗号のサポートについて学びます。
- ドメインコントローラの問題：SPP がドメインコントローラ上のアカウントのパスワードをどのように管理するかについて学びます。
- ネットワークに関する問題：システム接続の問題を解決する方法について説明します。
- Windows WMI 接続： SPP が Windows 資産を管理できるようにする方法を学びます。

アーカイブサーバーの接続のテストが失敗する

既存のアーカイブサーバーで**［接続のテスト］**を実行しようとしたときに、Unexpected copying error... というメッセージが表示される理由は複数ある可能性があります。

［接続のテスト］を実行すると、SPP は Safeguard_Test_Connection.txt というファイルをアーカイブサーバーの作成時に入力したアカウント名が所有するアーカイブサーバーの**ストレージパス**の場所に追加します。既存のアーカイブサーバーで新しいアカウント名で**［接続のテスト］**を実行するには、まず既存の Safeguard_Test_Connection.txt を削除する必要があります。

証明書の問題

SSL を使用している資産で**［接続のテスト］**に失敗する場合、以下の原因が考えられます。

- 資産の署名機関証明書が SPP の信頼できる CA 証明書ストアに追加されていない。
- 署名機関証明書期限切れ
- 与えられた名前と資産の証明書の名前に不一致がある。詳細については、「SSH ホストキーの欠落または不正確」を参照してください。

暗号のサポート

SPP のクライアントと SSH サーバーの両方が同じ暗号をサポートしている必要があります。SSH を使用する資産に対して**［接続のテスト］**を実行し、クライアントとサーバーの両方でサポートされている暗号がない場合、SPP は、Connecting to asset XXXXXXXXXXXXXX failed (There is no cipher supported by both: client and server) というエラーメッセージを表示します。これは、資産接続のセットアップ中に、SPP クライアントと SSH サーバーのメッセージ暗号化用の暗号が一致しなかったことを意味します。この場合、SPP がサポートする暗号を少なくとも 1 つ暗号のリストに追加して、SSH サーバーの設定を修正する必要があります。

SPP がサポートしている暗号は次のとおりです。

- 3des
- 3des-ctr
- aes128
- aes128-ctr
- aes192
- aes192-ctr
- aes256
- aes256-ctr
- arcfour
- arcfour128
- arcfour256

- blowfish
- blowfish-ctr
- cast128
- cast128-ctr
- des
- idea
- idea-ctr
- none
- serpent128
- serpent128-ctr
- serpent192
- serpent192-ctr
- serpent256
- serpent256-ctr
- twofish128
- twofish128-ctr
- twofish192
- twofish192-ctr
- twofish256
- twofish256-ctr

たとえば、暗号のデフォルトリストがある OpenSSH サーバーを使用している場合、OpenSSH の sshd_config ファイルにこれらの暗号を 1 つ以上追加してから、SSH サーバーを再起動する必要があります。OpenSSH の暗号についての詳しい情報は、http://www.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man5/sshd_config.5?query=sshd_config&sec=5 を参照してください。

ドメインコントローラーの問題

SPP はドメインコントローラー上のアカウントのパスワードを管理しません。SPP はドメインコントローラーをホストするディレクトリを通じて、ドメインコントローラー上のアカウントのパスワードを管理します。詳細については、「アカウントの追加」を参照してください。

ネットワークに関する問題

システムの接続性に問題がある場合、以下のことを確認してください。

- ネットワーク上のセキュリティルール（ファイアウォールやルーターなど）が、このトラフィックを妨げている可能性があるか？
- SPP からのトラフィックは、管理対象システムのネットワークアドレスにルーティング可能か？
- ケーブル、ハブ、スイッチなどに問題はないか？

以下のようなネットワークの問題が発生している可能性があります。

- ネットワーク障害
- ルーターの誤設定
- ケーブルが抜けている
- スイッチが動作していない

SPP がイベント通知を停止した場合、ログアウトしてログインし直し、SignalR を再受信してみてください。

Windows WMI 接続に失敗する

SPP による Windows 資産の管理を有効にするには、Windows Management Instrumentation (WMI) を許可するようにファイアウォールを設定する必要があります。

17.12.9　タイムアウトエラーによる操作の失敗

タイムアウトエラーが発生した場合は、数分待ってから操作を再試行してください。

クラスタへのレプリカの追加など、バックグラウンドでクラスタリング操作を実行している場合は、クラスタ操作が完了するのを待ってから、SPP で他の操作を実行します。

> **ヒント**：A timeout error can appear as a Request failed. というエラーメッセージが表示されることがあります。

17.12.10　ユーザーのロックアウト

ユーザーが設定した日数の間 SPP にログオンしていない場合、SPP はユーザーアカウントを無効化します。

> **メモ:** これは、**［アプライアンス管理］＞［Safeguard アクセス］＞［ローカルログイン制御］の［次の期間が経過したら非アクティブ化］**設定を使用して設定されます。詳細については、「ローカルログイン制御」を参照してください。

17.12.11 ユーザーに通知されない

ユーザーにメール通知が届かない場合、まず、SPP でメール通知が正しく機能するようにすべて正しく設定されているかどうかを確認します。詳細については、「メール通知の有効化」を参照してください。

通知リスト

SPP は、エスカレーション通知の連絡先リストのメールアドレスを動的に維持しません。

ポリシーの作成後に SPP ユーザーのメールアドレスを変更したり、SPP ユーザーを削除したりする場合は、エスカレーション通知連絡先リストのメールアドレスを手動で更新する必要があります。たとえば、ポリシーを作成するときに、緊急アクセスが使用された場合の連絡先を示すことができます。ユーザーがメールアドレスを変更した場合、その個人には通知が届きません。さらに、ユーザーが SPP から削除された場合も、そのユーザーには通知が届きます。

18 よくある質問

以下のトピックでは、SPP の管理に関するいくつかの質問に対する答えを見つけるのに役立ちます。

- トランザクションのアクティビティを監査できますか？
- 外部フェデレーション認証を設定できますか？
- サポートされていないプラットフォームのアカウントを管理できますか？
- アプライアンスの構成設定を変更できますか？
- RDP 接続時に SPP のメッセージを表示させないようにできますか？
- Telnet および TN3270/TN5250 over telnet を使用したセッションアクセスリクエスト手順は？
- SPP データベースサーバーでどのように SSL を使用しますか？
- アクセスリクエストの状態とは？
- アプライアンスが隔離された場合の対処法は？
- 動的なグループ化とタグ付けのためのルールエンジンはいつ実行されますか？
- オープンリクエスト中にパスワードまたは SSH キーが変更されました。なぜですか？

18.1 トランザクションのアクティビティを監査できますか？

アプライアンスは、SPP 内で実行されたすべてのアクティビティを記録します。管理者は誰でも監査ログ情報にアクセスできますが、管理者権限セットによって、アクセスできる監査データが決まります。詳細については、「管理者のアクセス許可」を参照してください。

SPP は、トランザクションアクティビティを監査するためのいくつかの方法を提供します。

- パスワードアーカイブ：特定の日付のアカウントの以前のパスワードにアクセスする場所。詳細については、「パスワードアーカイブの表示」を参照してください。
- SSH キーアーカイブ：特定の日付のアカウントの以前の SSH キーにアクセスする場所。詳細については、「SSH キーアーカイブの表示」を参照してください。
- 確認と変更ログ：アカウントのパスワードと SSH キーの検証およびリセットの履歴を表示する場所。**［アカウント］＞［確認と変更の記録］**にアクセスします。詳細については、「アカウント」を参照してください。

- 履歴：選択した項目に影響を与えた各操作の詳細が表示されます。詳細については、「履歴タブ（アカウント）」を参照してください。
- アクティビティセンター：特定の期間のアクティビティを検索し、確認することができます。詳細については、「アクティビティセンター」を参照してください。
- ワークフロー：特定のアクセスリクエストについて、リクエストから承認、レビューまでのワークフロープロセスの一部として実行されたトランザクションを監査することができる場所です。詳細は、「リクエストワークフローの監査」を参照してください。
- レポート：選択したユーザーがどの資産やアカウントへのアクセスを許可されているかを示す資格レポートを表示およびエクスポートできます。詳細については、「レポート」を参照してください。

18.2 外部フェデレーション認証を設定できますか？

SPP は SAML 2.0 Web Browser SSO Profile をサポートしており、Microsoft の AD FS など多くの異なるアイデンティティプロバイダ STS サーバーおよびサービスとのフェデレーション認証を設定することが可能です。フェデレーションメタデータの交換を通じて、2 つのシステム間で信頼関係を構築することができます。その後、SPP のユーザーアカウントを作成し、連携アカウントと関連付けます。

Safeguard は、サービスプロバイダ（SP）主導のログインとアイデンティティプロバイダ（IdP）主導のログインの両方をサポートしています。

- SP 主導の場合、ユーザーはまず Safeguard を参照し、認証プロバイダとして**外部フェデレーション**を選択します。メールアドレスを入力すると、外部 STS にリダイレクトされ、認証情報を入力し、STS で必要とされる二要素認証を実行します。認証に成功すると、SPP にリダイレクトされ、ログインされます。
- IdP によるログインの場合、ユーザーはまず IdP STS に移動して認証を受けます。通常、お客様は STS 内で Safeguard をアプリケーションとして設定しており、ユーザーはリンクやアイコンをクリックするだけで Safeguard にリダイレクトされ、追加の認証情報を入力することなく自動的にログインできるようになっています。

> **メモ：**関連する SPP のユーザーアカウントに追加の二要素認証を割り当てて、外部 STS からリダイレクトされて戻ってきたユーザーに再度認証させることができます。

外部フェデレーションを使用するには、まず STS のフェデレーションメタデータ XML をダウンロードし、ファイルに保存しておく必要があります。例えば、Microsoft の AD FS の場合、フェデレーションメタデータ XML は以下からダウンロードすることができます：

https://<adfs server>/FederationMetadata/2007-06/FederationMetadata.xml

18.2.1 外部フェデレーションプロバイダの信頼を追加する方法は？

SPP で外部フェデレーションサービスプロバイダを設定するのは、アプライアンス管理者の責任です。

外部フェデレーションサービスプロバイダを追加する手順

1. **［アプライアンス管理］＞［Safeguard アクセス］＞［ID と認証］**を選択します。
2. ＋**［追加］**をクリックし、**［外部フェデレーション］**を選択します。
3. **［外部フェデレーション］**ダイアログで、次の情報を入力します：
    a. **名前**：外部フェデレーションサービスプロバイダの一意の表示名を入力します。この名前は管理目的にのみ使用され、エンドユーザーには表示されません。制限：100 文字
    b. **領域：**この STS を認証に使用する予定のユーザーのメールアドレスに一致する、一意の領域値（通常は contoso.com などの DNS サフィックス）を入力します。Home Realm 検出を実行する際、この値に対して大文字と小文字を区別しない比較が使用されます。ワイルドカードは使用できません。制限：255 文字
    c. **フェデレーションメタデータファイル**：以前にダウンロードした STS フェデレーションメタデータファイルへのファイルパスを選択または入力します。
    d. Safeguard フェデレーションメタデータをダウンロードします。以前にダウンロードしたことがない場合は、リンクをクリックして SPP のフェデレーションメタデータ XML のコピーをダウンロードします。このファイルは、STS サーバーで対応する信頼関係を作成する際に必要になります。

        > **メモ：**フェデレーションメタデータ XML ファイルには通常、デジタル署名が含まれており、空白を含め、いかなる方法でも変更することはできません。メタデータの問題に関してエラーが発生した場合は、メタデータが編集されていないことを確認してください。

    e. **［OK］**をクリックします。

18.2.2 STS 証明書利用者信頼（Relying Party Trust）の作成方法は？

STS（Security Token Service）の Relying Party Trust を作成する手順は、アプリケーションやサービスによって異なります。ただし、前述のとおり、SPP に STS の情報を入力した際にリンクをクリックすると、SPP のフェデレーションメタデータのコピーをダウンロードすることが可能です。また、SPP のフェデレーションメタデータは、以下のいずれかの方法でいつでもダウンロードできます。

1. **［アプライアンス管理］＞［Safeguard アクセス］＞［ID と認証］**の順に選択します。
2. **［Safeguard フェデレーションメタデータのダウンロード］**をクリックします。
3. 次の URL からファイルをダウンロードします。

   https://<SPP サーバー>/RSTS/Saml2FedMetadata

STS がフェデレーションメタデータのインポートをサポートせず、値を手動で入力する必要がある場合、通常、アプリ ID およびログインまたはリダイレクト URL が必要になります。これらの値は両方とも、ダウンロードした SPP フェデレーションメタデータ XML ファイルからコピーすることができます。

- SPP の App ID は、XML ファイルの<EntityDescriptor>要素の entityID 属性から取得します。
- ログインまたはリダイレクト URL は、<SPSSODescriptor>要素内の<AssertionConsumerService>要素の Location 属性から取得されます。

> **メモ：**このエンドポイントでは、HTTP-POST バインディングのみがサポートされています。

次に、STS が認証されたユーザーのメールアドレスを SAML 属性要求として返すように構成するか、または保証する必要があります。メールアドレスは、標準的な SAML メールアドレス要求または名前要求のいずれかに表示される必要があります。

- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

emailaddress および name 属性クレームが SAML アサーションに存在しない場合、SAML Subject NameID を使用することができます。

> **メモ：**その他の属性またはクレームは無視されます。

SAML レスポンスまたはアサーションは、署名する必要があるが、暗号化されてはなりません。STS が使用する署名証明書の有効期限が切れた場合は、STS のメタデータファイルの新しいコピ

ーをアップロードして、SPP のメタデータを更新する必要があります。SPP は自動的にメタデータの更新を試みません。

> **メモ：**STS のメタデータには、有効期限切れの証明書と新しい証明書の間に猶予期間を設けるために、複数の署名証明書を含めることができます。

特定の STS サーバーに関する詳細については、One Identity サポートサイトの以下のナレッジベース記事を参照してください。

- Configuring Microsoft's AD FS Relying Party Trust for Safeguard for Privileged Passwords: KB Article 233669
- Configuring Microsoft's Azure AD for Safeguard for Privileged Passwords: KB Article 233671

18.2.3 外部フェデレーションユーザーアカウントを追加するには？

関連する外部フェデレーション SPP ユーザーを追加するのは、権限許可管理者またはユーザー管理者の責任です。

準備

外部フェデレーションユーザーを追加する前に、外部フェデレーションサービスプロバイダを SPP に追加する必要があります。

姓名、電話番号、メールアドレスなどのユーザー情報が STS クレームトークンからインポートされることはありません。その情報が必要な場合は、SPP でユーザーを作成するときに手動で入力する必要があります。

ユーザーの追加手順

1. **［ユーザー管理］＞［ユーザー］**の順に選択します。
2. ツールバーの ＋ **［新しいユーザー］**をクリックします。
3. 各タブに情報を提供します：
    - **ID** タブ：ここで ID プロバイダとユーザーの連絡先情報を定義します。
    - **認証**タブ：認証プロバイダ、ログイン名、パスワード（必要な場合）を定義します。
    - **アクセス許可**タブ：ユーザーの管理者権限を設定します。

18.3 サポートされていないプラットフォームのアカウントを管理できますか？

SPP は、サポートされていないプラットフォームやカスタムプラットフォームで対応されていないアカウントのパスワードと SSH キーを管理することができます。

手動で変更するパスワードまたは SSH キーの設定を持つプロファイルを使用します。

例えば、ネットワーク上にない資産があるとします。手動変更パスワードまたは SSH キー設定を使用すると、SPP の自動変更パスワードまたは SSH キー設定を使用せずに、定期的にアカウントパスワードを変更する企業ポリシーに準拠することができます。SPP は、設定されたスケジュールでメール、トースト通知、またはその両方でアカウントパスワードを手動で変更するように通知します。その後、自分でパスワードまたは SSH キーをリセットするか、SPP がプロファイルで選択されたパスワード規則に従ってランダムなパスワードまたは SSH キーを生成することを許可することができます。

> **重要**: SPP でパスワードまたは SSH キーを変更した後、アカウントのパスワードまたは SSH キーを忘れずに変更する必要があります。SPP が自動的に変更するわけではありません。

以下は、サポートされていないプラットフォームでアカウントを管理するための一般的なワークフローをまとめたものです。

アカウントのパスワードや SSH キーを手動で管理する手順

1. パスワードや SSH キーを手動で変更する設定をしたプロファイルを作成し、資産アカウントを割り当てます。詳細については、「パスワード変更設定の追加」と「SSH キー変更設定の追加」を参照してください。
2. トースト通知またはメール通知が適切に構成されていることを確認します。詳細については、「メール通知の有効化」を参照してください。
3. アカウントのパスワードまたは SSH キーを変更するように通知されたら、以下を選択します：
    - **パスワードの設定**：詳しくは「アカウントパスワードの確認、変更、設定」を参照してください。
    - **SSH キーの設定**：詳しくは「SSH キーの確認、変更、設定」を参照してください。

18.4 アプライアンスの構成設定を変更できますか？

> **メモ：**このトピックでは、ハードウェア機器と一緒に箱に入っている『One Identity Safeguard for Privileged Passwords アプライアンスセットアップガイド』で、最初のアプライアンスのインストールと構成の手順をすでに実行したものと仮定しています。

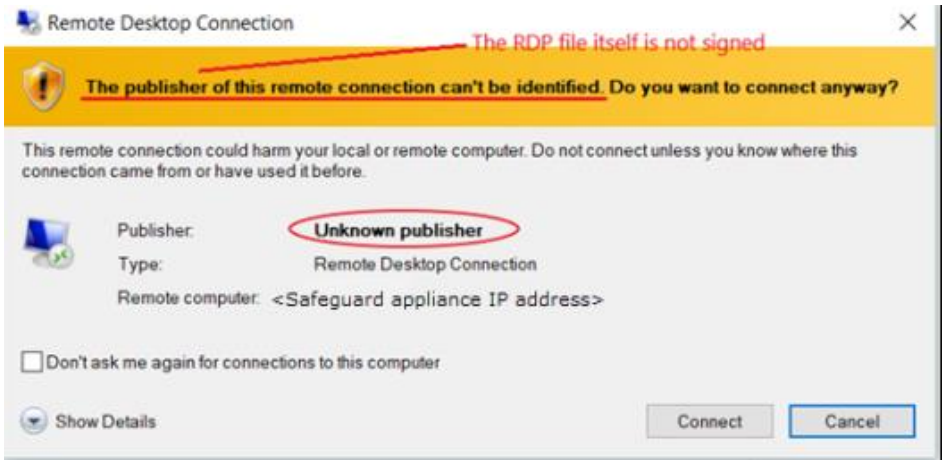
Web クライアントでアプライアンス構成設定を変更する手順

1. アプライアンス管理者アカウントを使用して SPP の Web クライアントにログインします。
2. **［アプライアンス管理］＞［アプライアンス］**の順に選択します。
3. アプライアンスを構成するには、**［ネットワーク］**をクリックします。詳細については、「ネットワーク」を参照してください。
    a. **ネットワーク（X0）**：プライマリインターフェイスの DNS サーバーのアドレス情報を入力します。
    b. **［保存］**をクリックします。
4. **［時間］**をクリックして、ネットワークタイムプロトコル（NTP）を有効にして情報を表示します。
    a. **［NTP の有効化］**を選択します。
    b. プライマリ NTP サーバーと必要に応じてセカンダリ NTP サーバーを設定します。
    c. **［前回の同期時刻］**が表示されます。詳細を表示または非表示にするには、**［詳細の表示］**または**［詳細の非表示］**をクリックします。詳細については、「時間」を参照してください。
    d. **［保存］**をクリックします。

18.5 RDP 接続時に SPP のメッセージを表示させないようにできますか？

RDP 接続の際に、2 種類の証明書メッセージが表示されることがあります。

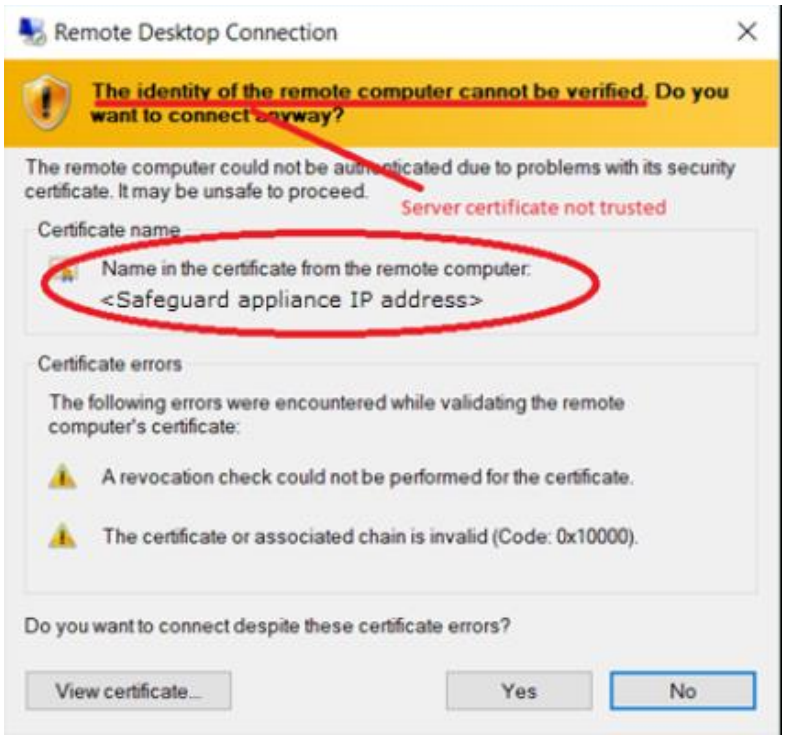
- 未署名の RDP ファイルメッセージ



このメッセージは、SPP のユーザーインターフェイスで ▶ **[再生]** をクリックしたときにダウンロードされた RDP ファイルをリモートデスクトップ接続で開くと発生します。

現在、このメッセージを回避するために、SPP がこの RDP ファイルに署名できるようにする解決策に取り組んでいます。

- 信頼できないサーバー証明書メッセージ



このメッセージは、ワークステーションが SPP の RDP 接続署名証明書を信頼していない場合に発生します。

> **メモ：**接続サーバーの IP アドレスは、Safeguard アプライアンスのものです。

このメッセージを回避するには、RDP 接続署名証明書とその信頼チェーン内の証明書を信頼するか、現在の証明書を信頼できるエンタープライズ証明書と信頼チェーンに置き換える必要があります。

One Identity では、構成全体を信頼できる独自のエンタープライズ PKI に置き換えることを推奨しています。この場合、以下のような構成になります：

- ルート認証局
  - 発行認証局
    - RDP 署名証明書（Safeguard CSR）
      - <証明書生成されたセッションモジュール>

ルート認証局、発行認証局、RDP 署名証明書は、グループポリシー、Active Directory、またはその他の配布手段を介して配布することができます。

telnet および TN3270/TN5250 セッションのアクセスリクエストを設定する方法

SPP は、telnet および TN3270/TN5250 over telnet を含むソフトウェアターミナルエミュレーションを使用するメインフレームとのセッションアクセスリクエストをサポートします。セッションの記録には、SPS バージョン 6.1 またはそれ以降が使用されます。

操作方法

- セキュリティ担当者は、IBM iSeries およびメインフレームコンピューター上で動作する重要なシステムを管理する管理者の活動を記録することができます。
- 資産管理者は、次のことができます：
  - TN3270/TN5250 のログイン画面のフィールド検出をカスタマイズして、Safeguard のカスタムログイン設定に対応させます。
  - Telnet セッションをサポートする資産としてマークを付け、資産が利用可能かどうかを指定します。
- セキュリティポリシー管理者は、telnet を使用したセッションアクセスおよび telnet を使用した TN3270/TN5250 セッションを含むアクセスポリシーを持つ資格を作成することができます。
- セッションが記録されている場合でも、要求者のログインエクスペリエンスは通常のクライアント telnet または TN3270/TN5250 インターフェイスに従います。セッションは SPP から起動されず、必要なログイン情報はすべて SPP から利用可能です。

18.6 Telnet および TN3270/TN5250 over telnet を使用したセッションアクセスリクエスト手順は？

重要：利用可能なプラグイン、ポリシー作成、パターンファイル、ショートカット、ベストプラクティスなどを含む構成やインストールについては、One Identity Professional Services のサポートが必要です。

SPS のセットアップ手順

SPS で次のセットアップ手順を完了させてください。操作の詳細については、『Safeguard for Privileged Sessions 管理者ガイド』を参照してください。

- SPP で認証し、SPP から資格情報を引き出すために、認証と承認（AA）および資格情報ストア（credstore）情報を供給するために必要なプラグインをインポートする。プラグインファイルと説明書は、GitHub の Safeguard Custom Platform Home wiki で入手できます。
- 各接続のログインエクスペリエンスに固有のパターンファイルを使用するパターンセットを作成し、割り当てます。パターンファイルは、特定のシステムのログインエクスペリエンスを記述します。パターンファイルには、ユーザー名の画面上の位置、パスワードフィールドの位置、ログイン結果、説明、状態、およびその他の必要な詳細が含まれる場合があります。ログインエクスペリエンスはメインフレームごとに異なるため、カスタムパターンファイルを作成してアップロードし、システム関連の接続ポリシーで参照する必要があります。テンプレートパターンファイルと説明書は、GitHub の Safeguard Custom Platform Home wiki で入手できます。

  ⚠ **注意：テンプレートパターンファイルは、情報提供のみを目的として提供されています。telnet および TN3270/TN5250 のパターンファイルは、カスタマイズして作成する必要があります。本番で使用する前に、更新、エラーチェック、テストが必要です。**

- 各認証ポリシーを指定し、接続で使用できる認証方式をリストアップします。
- 各接続ポリシーを作成し、設定します。TN3270/TN5250 over telnet では、inband の宛先が使用されないだけでなく、各システムのログオンエクスペリエンスや関連するパターンファイルが一意であるため、通常、複数の接続ポリシーが必要です。

  例えば、telnet は inband の宛先として使用することができます。しかし、TN3270/TN5250 over telnet では、inband の宛先は使用されません。その代わり、ポートやサーバーを含む固定アドレスを特定することができるため、メインフレームごとに

異なる接続ポリシーが必要になります。SPS の固定アドレスは、使用するポートを含みます。SPP の資産ポートは接続に使用されませんが、通常は同じものです。

- 必要であれば、設定ファイルをエクスポートします。
- SSH サーバー、クラスターインターフェース、クラスタ管理の基本設定を行います。

SPP のセットアップ手順

SPP で次のセットアップ手順を完了します。

- 資産管理者は、**［資産管理］＞［資産］＞［管理］**タブで識別される Telnet セッションポートを含むメインフレーム資産を追加します。詳細については、「資産の追加」を参照してください。
- セキュリティポリシー管理者は、**［セキュリティポリシー管理］＞［資格］＞［アクセスリクエストポリシー］**タブで**［アクセスタイプ（Telnet）］**を設定します。

SPP 要求者の手順

すべての構成が完了した後の SPP で、要求者が使用中のターミナルサービスアプリケーションに基づいて進行します。

- inband 接続文字列（telnet など）を使用するターミナルサービスアプリケーションの場合、**［コピー］**をクリックして**ホスト名接続**文字列をコピーし、パスワードをチェックアウトします。そして、その情報をログイン画面に貼り付けます。
- ターミナルサービスアプリケーションがログインのためにさらに多くの情報を必要とする場合（例えば、TN3270/TN5250 over telnet）。
    - **［表示］**をクリックし、**Vault Address**（SPP アドレス）、ワンタイムトークン、Username、Asset、Sessions Module（SPS アドレス）を含む値を表示します。
    - ターミナルサービスアプリケーションで必要な場合、いずれかの値のそばの**［コピー］**をクリックすると 1 つの値がコピーされます。または、すべての値の右側にある**［コピー］**をクリックすると、接続文字列全体がコピーされます。
    - 必要な情報をターミナルサービスアプリケーションに貼り付けます。
- **［チェックインリクエスト］**をクリックして、パスワードまたは SSH キーのチェックアウト処理を完了します。これにより、セッションリクエストがレビュー担当者に公開されます。
- **［非表示］**をクリックすると、情報が表示されなくなります。

メモ：たとえば、接続文字列を取得してターミナルサービスアプリケーションのプロファイルを起動するランチャーがある場合、ユーザーは接続文字列全体をコピーすることになります。

18.7 SPP データベースサーバーでどのように SSL を使用しますか？

一部のデータベースサーバーは、SPP と通信する際に Secure Socket Layer (SSL) を使用します。プラットフォームの種類、バージョン、構成によって、データベースサーバーはセッションの暗号化のみに SSL を使用するか、データベースサーバーの暗号化と認証に SSL を使用することができます。

18.7.1 ODBC トランスポート

次のプラットフォームは、ODBC トランスポートを使用します。SPP は、プラットフォームと通信するために、アプライアンスに適切なソフトウェアドライバをインストールします。SPP がサーバーとの接続を初期化するために使用する設定データは、コロンで区切られたドライバー固有のオプションのリストからなる接続文字列の形式をとっています。

デフォルトでは、データベースサーバーはログインデータを暗号化しますが、接続で渡される後続のデータは暗号化しません。セッションデータの暗号化を有効にするには、データベースサーバーで SSL を設定し、有効化する必要があります。

18.7.2 Microsoft SQL Server

Microsoft SQL Server は、常に SSL で接続を暗号化することが可能です。SSL 接続と非 SSL 接続の両方を 1 つのポートでリッスンします。

SQL Server で**［強制的に暗号化］**オプションを yes に設定した場合、SPP クライアントが要求するかどうかに関わらず、データを暗号化するために SSL が使用されます。

サーバー証明書を構成せずに、SQL Server で強制暗号化オプションを「yes」に設定することもできます。この場合、SQL Server は、SPP クライアントが暗号化を要求したときに使用する自己署名付き証明書を透過的に生成します。これにより、SQL Server はサーバー証明書を検証することなく、セッションの暗号化を提供するために SSL のみを使用することが可能になります。

メモ：実行中のセッション内では、SQL サーバーが SSL を使用して暗号化しているかどうかを検出することはできません。

表：Microsoft SQL Server の SSL サポート

SPP クライアントオプション		Microsoft SQL Server 構成		結果
SSL 暗号化使用	SSL 証明書検証	強制暗号化	構成済みサーバー証明書	
No	n/a	No	n/a	SQL Server はセッションを暗号化しない
Yes	No	n/a	No	SPP は、生成された自己署名証明書を使用してセッションを暗号化するよう SQL Server に要求します。
Yes	No	n/a	Yes	SPP は、SQL Server にサーバー証明書を使用してセッションを暗号化するよう要求します。
Yes	Yes	n/a	No	SQL Server は、検証するための証明書がないため、接続を拒否します。
Yes	Yes	n/a	Yes	SPP は、SQL Server にセッションを暗号化し、SPP の信頼できる CA 証明書と照合してサーバー証明書を検証するよう要求します。

18.7.3 MySQL サーバー

SSL をサポートするには、MySQL サーバーソフトウェアを SSL サポート付きでコンパイルし、CA 証明書とサーバー証明書を正しく設定する必要があります。証明書に何らかの問題がある場合、MySQL サーバーはエラーを記録し、SSL サポートなしで起動することがあります。この場合、MySQL サーバーは検証する証明書がないため、セッションの SSL を有効にする要求を拒否

し、セッションを暗号化しません。MySQL サーバーは、両方のタイプの接続に対して 1 つのポートでリッスンします。

MySQL サーバーの動作は、サーバーのバージョンと設定に依存します。MySQL の一部のバージョンでは、サーバーが設定されると、すべての SPP クライアントセッションでデフォルトで SSL が有効になります。

MySQL サーバーがデフォルトで SSL を使用する場合、またはユーザーに SSL を要求する場合、SPP クライアントが要求しなくても、MySQL サーバーはセッションを暗号化します。ただし、SPP クライアントは、暗号化のためだけに SSL の使用を要求することはできず、正しい CA 証明書を SPP にインポートした場合にのみ SSL を要求することができます。

> **メモ：**セッション変数を調べることで、セッション内から SSL が使用されていることを検出することができます。つまり、SPP クライアントは、SSL を使用する要求が受け入れられなかった場合にそれを検出し、エラーを表示することができます。

表： MySQL サーバー SSL サポート

SPP が SSL 暗号化オプションを使用	MySQL サーバーでサポートされる SSL	結果
No	No	暗号化されていないセッション
No	Yes	MySQL サーバーによって決定。サーバーは、デフォルトで SSL を使用する場合、またはこのユーザーに対して SSL を要求する場合、セッションを暗号化します。
Yes	No	SPP クライアントはこれを検出し、失敗を報告します。
Yes	Yes	SPP は、MySQL サーバーにセッションを暗号化し、SPP の信頼できる CA 証明書とサーバー証明書を照合するよう要求します。

18.7.4 Sybase ASE サーバー

SSL をサポートするには、CA 証明書とサーバー証明書を使用して Sybase サーバーを正しく設定する必要があります。Sybase サーバーは、SSL 接続と非 SSL 接続に対して異なるポートでリッスンし、SPP クライアントから特定のポートへのミスマッチのリクエストを拒否します。

SPP クライアントは、暗号化のためだけに SSL の使用を要求することはできません。SPP に正しい CA 証明書をインポートした場合のみ、SSL を要求することができます。

表：Sybase ASE サーバーSSL サポート

SPP が SSL 暗号化オプションを使用	Sybase Server のリスニングポートが SSL を使用	結果
No	No	暗号化されていないセッション
No	Yes	Sybase サーバーは、接続の試行を拒否します。 **メモ：**ODBC ドライバーは、これが SSL エラーであることを検出できず、client cannot connect エラーを表示します。
Yes	No	Sybase サーバーは、SSL エラーでセッションを拒否します。
Yes	Yes	SPP は、Sybase サーバーにセッションを暗号化し、SPP の信頼できる CA 証明書に対してサーバー証明書を検証するよう要求します。

18.8 アクセスリクエストの状態とは？

SPP のアクセスリクエストの状態は次の通りです。アクセスリクエストの状態はリクエストがワークフロープロセスを進むにつれ変化します。

表：アクセスリクエストの状態

状態	説明
利用可能	要求者の準備ができた承認済みリクエスト。つまり、パスワードまたは SSH キーのリリースリクエストの場合、要求者はパスワードまたは SSH キーを表示またはコピーすることができます。セッションアクセスリクエストの場合、要求者はセッションを起動することができます。
承認済み	リクエストは承認されたが、チェックアウト時刻が来ていないもの

状態	説明
拒否	承認者によって拒否されたリクエスト
期限切れ	チェックアウト時間が経過したリクエスト
保留	承認待ちのリクエスト
無効	承認者によって撤回された承認済みリクエスト **メモ：**承認者は、要求者がリクエストを閲覧してからチェックインしするまでの間に、リクエストを取り消すことができます。

18.9 アプライアンスが隔離された場合の対処法は？

SPP アプライアンスは、特定のアクティビティを実行中に何か問題が発生すると、隔離状態になることがあります。データを失ったり、隔離されたアプライアンスに関連する問題を悪化させたりしないための最善の防御策は、バックアップを取得しておくことです。SPP クラスタの少なくとも 1 つのアプライアンスは、定期的にバックアップを生成し、アーカイブサーバーに送信するようにスケジュールする必要があります。詳細については「バックアップと復元」を参照してください。

隔離状態からの復旧手順

1. 以下の手順に従って、Recovery Kiosk から Quarantine Bundle を作成します。詳細については、「リカバリキオスク（Serial Kiosk）」を参照してください。
    a. Quarantine Bundle 機能を使用する前に、Quarantine Bundle を送信する Windows 共有を設定します。
    b. Recovery Kiosk から、**［Support Bundle］**オプションを選択し、右矢印をクリックし、**［Quarantine Bundle］**を選択します。
    c. 以下の情報を入力します:
        - **アドレス**： サポートバンドルを保存する Windows 共有のアドレス（<IP Address>\<ShareName>）を入力します。
        - Windows 共有が匿名でない場合は、**［ユーザー名］**と**［パスワード］**または**［SSH キー］**を入力します。
    d. **[Copy to Share]** をクリックします。

2. これでアプライアンスを再起動することができます。多くの場合、隔離は、システムが応答を待っていたが時間内に戻らなかったために起こります。アプライアンスを再起動することで、再試行が可能になり、修正されることがあります。

    - 隔離されたアプライアンスを再起動するには、そのアプライアンスの Recovery Kiosk に接続し、そこから再起動します。アプライアンスが再起動すると、SPP が起動するまでに数分かかります。
    - SPP の起動中に、Web クライアントを使用してアプライアンスにログインすると、HTTP 503 エラーが通知されます。ログインサービスが実行されると、ログイン画面が表示されますが、アプライアンスがさらに進行するまで続行することはできません。アプライアンスが隔離状態から起動すると、ログインして通常通りに操作できるようになります。このとき、サポートバンドルが生成されるはずです。アプライアンスが隔離状態のままである場合、Web クライアントは引き続き HTTP 503 エラーのままです。
      Web クライアントがログイン画面を表示できない場合、One Identity テクニカルサポートに連絡して結果を報告してください。

      > **メモ：クラスタ化された環境**：隔離されたアプライアンスがプライマリアプライアンスだった場合、フェイルオーバーオプションを使用して、プライマリアプライアンスの役割をクラスタの正常なメンバーに再割り当てしてください。詳細については、「レプリカを新しいプライマリに昇格させることによるフェイルオーバー」を参照してください。

クラスタから隔離されたアプライアンスを削除する方法

クラスタから隔離されたアプライアンスを削除したい場合があります。

1. レプリカアプライアンスをクラスタから参加解除してみてください。詳細については、「クラスタからのレプリカの参加解除」を参照してください。
2. アプライアンスの参加解除に失敗した場合は、クラスタをリセットしてアプライアンスをクラスタから削除します。詳細については、「コンセンサスが失われたクラスタのリセット」を参照してください。

ハードウェアアプライアンスの工場出荷リセットに関する考慮事項

> ⚠ **注意 この操作により、すべてのデータと監査履歴が削除され、工場出荷されたときの状態に戻るため、物理アプライアンスに対して工場出荷時リセットを実行するときは、注意が必要です。工場出荷時リセットの実行は、BMC/IPMI インターフェイスや IP アドレスをリセットしません。ただし、リセットの完了後、BMC/IPMI インターフェイスを再度有効にする必要があります（詳細については、「ライトアウト管理（BMC）」を参照し**

てください）。アプライアンスは、工場出荷時と同じく、再度設定を行う必要があります。詳細については、「SPP の初期設定」を参照してください。

さらに、工場出荷時のリセットを実行すると、デフォルトの SSL 証明書とデフォルトの SSH ホストキーが変更される場合があります。

アプライアンスは、現在のロングタームサポート（LTS）バージョンにリセットされます。たとえば、バージョン 6.6（機能リリース）または 6.0.6LTS（メンテナンスロングタームサポートリリース）を使用している場合に工場出荷時リセットを行うと、アプライアンスは 6.0 LTS にリセットされ、希望のバージョンにパッチアップする必要があります。詳細については、「長期サポート（LTS）と機能リリース」を参照してください。

One Identity テクニカルサポートは、工場出荷時のリセットが必要であるかどうかを判断します。工場出荷時リセットは最後のオプションである場合、操作を完了するためにサポートに連絡してください。

1. 工場出荷時リセットを実行するには、Recovery Kiosk に接続し、**[Factory Reset]**（工場出荷時リセット）オプションを選択します。詳細については、「リカバリキオスクからの工場出荷時リセット」を参照してください。

   工場出荷時リセットを開始したら、終了するまで待つ必要があります（完了までに最大 30 分かかる場合があります）。工場出荷時リセットの完了後、キオスクはオンラインインジケータを返します。

2. 工場出荷リセットが完了したら：

   a. ネットワークインターフェイス設定を再設定します。

   b. インストールしたパッチをすべて再適用します。

   c. これがクラスタ化されていないアプライアンスの場合、データを取得するために最新のバックアップをアップロードして復元します。詳細については、「バックアップの復元」を参照してください。

   d. アプライアンスがクラスタのレプリカになる場合は、バックアップを復元する必要はありません。アプライアンスをクラスタに参加させます。詳細については、「レプリカのクラスタへの登録」を参照してください。SPP は、すべてのデータをアプライアンスにレプリケートする処理を行います。

18.10 動的なグループ化とタグ付けのためのルールエンジンはいつ実行されますか？

動的なアカウントグループは、関連するオブジェクトが作成または変更されたときに実行されるルールエンジンと関連付けられています。たとえば、次のような場合です：

- 資産アカウントを追加または変更するたびに、その資産アカウントに対して適用可能なすべてのルールが再評価されます。
- 資産アカウントのルールを変更するたびに、そのルールのスコープ内にあるすべての資産アカウントに対して、ルールが再評価されます。言い換えると、グループ化のためにすべての資産アカウントに対して、タグ付けのために指定されたパーティション内の資産アカウントに対して、ルールが再評価されます。

ルールなしで動的なアカウントグループを作成することもできますが、ルールを追加するまで、この動的なアカウントグループにはアカウントは追加されません。

大規模な環境では、すべてのルールが再評価される前にユーザーインターフェイスが戻り、期待していた結果が表示されない可能性があります。このような場合は、数分待ってから画面を更新して結果を表示してください。

18.11 オープンリクエスト中にパスワードまたは SSH キーが変更されました。なぜですか？

ユーザーがチェックアウトしている間にパスワードが変更されてしまう可能性は３つあります。

1. 資産管理者が手動でパスワードまたは SSH キーを変更した。詳細については、「アカウントパスワードの確認、変更、または設定」または「SSH キーの確認、変更、設定」を参照してください。

2. プロファイルが自動的にパスワードまたは SSH キーを変更するようにスケジュールされている。詳細は、「パスワードの変更」または「SSH キー設定の変更」を参照してください。

3. ポリシーで、同時アクセスを許可し、ユーザーがチェックインするときにパスワードまたは SSH キーの変更を要求している。

ユーザーがチェックアウトしている間にパスワードまたは SSH キーが変更され、現在のリクエストがまだ有効である場合、ユーザーは**コピー**または**パスワードの表示**または **SSH キーの表示**を再度選択して、新しいパスワードを取得することができます。

付録 A：Safeguard ポート

SPP では、さまざまなシステム操作のためにポートの可用性が必要です。

ポートの詳細

ネットワークポートの詳細は以下の表のとおりです：

表：Safeguard ポート

SPP で使用	アプライアンスポート	プロトコル	説明
	MGMT	TCP	アプライアンスの安全な初回構成に使用される HTTPS。IP アドレスは固定アドレスで、変更できません。プライマリインターフェイスが使用できなくなった場合に利用できます。 TCP/443 と IP アドレス:192.168.1.105
基本動作	25	TCP	SMTP：Simple Mail Transfer
基本動作	53	TCP/UDP	DNS（Domain Name Server）
基本動作	123		NTP 時刻同期
基本動作	88	UDP	Active Directory との通信では、Safeguard はポート 88 を使用します（例えば、Active Directory に対する Kerbos 認証など）。
基本動作： AD 資産、アカウント検出、パスワード確認と変更	389	TCP/UDP	Active Directory の資産検出とディレクトリアカウント検出に使用される LDAP。ディレクトリ管理タスク（ディレクトリアカウント、ディレクトリユーザーアカウント、またはディレクトリユーザーグループの追加など）のために、環境内のすべての Windows グローバルカタログサーバーと SPP アプライアンスが通信するには、ファイアウォールで標準グローバルカタログポート 3268（LDAP）を開放する必要があります。LDAP は、暗号化されていない接続にポート 389 を使用します。詳細に

SPP で使用	アプライアンスポート	プロトコル	説明
			ついては、Microsoft パブリケーション『How the Global Catalog Works』を参照してください。 OS アカウントのパスワードを変更する際の基本的な機能については、以下のポートが必要です： • Windows Active Directory：TCP/389 および TCP/445 • Windows、Windows デスクトップ：TCP/445 こちらも参照してください： • ID と認証プロバイダの追加 • Windows システムの準備 • ポート 445
基本動作（パスワードおよび SSH キー確認・変更）	445	TCP SMB	NetLogon Service（NP-In）を使用して実行します： • Windows Active Directory のパスワードチェックと変更 • Windows、Windows Desktop のパスワードと SSH キーのチェックと変更 ポート 389 と「Windows システムの準備」も参照してください。
LDAPS	636		AD LDAP プロバイダ以外でサポートされています。デフォルトの LDAPS ポートは 636 です。AD LDAP 以外のプロバイダで LDAPS を使用するには、ポート 636 を開放する必要があります。
WMI	135 (49152-65535 Windows)	TCP	ファイアウォールは、コンピューター名やその他の検索を行うための Windows Management Instrumentation (WMI) を許可するように設定されている必要があります。また、SPP が Windows マシン（それが依存シス

SPP で使用	アプライアンスポート	プロトコル	説明
			テムであるか、通常のターゲットプラットフォームであるかを問わず）上で以下に示すいずれかの機能を実行する場合、WMI が必要です。 • サービスアカウントパスワードの管理 • スケジュールされたタスクのパスワードの管理 • サービスの再始動 • ターゲットでのアカウント検出の使用 DPA からの WMI/DCOM は、ターゲット上で通信を開始するために TCP/135 にアクセスする必要があります。通信はランダムなネゴシエーションポートで継続されます。Windows 7 および Windows 2008（以上）では、この範囲にあります。49152 - 65535. WMI/DCOM が使用するポートを制限するには、以下の Microsoft 社の記事を参照してください。 ファイアウォールで動作する RPC 動的ポート割り当てを設定する方法 • How to configure RPC dynamic port allocation to work with firewalls • Setting Up a Fixed Port for WMI Windows Active Directory の場合、アカウント検出または自動検出 CLDAP を使用する場合は、UDP/389 の ping も必要です。次を参照してください： • 「Windows システムの準備」 • 「ネットワーク」
WMI	49152-65535		port 135 を参照してください

SPP で使用	アプライアンスポート	プロトコル	説明
SPP/SPS 内部通信	8649	TCP	SPS と SPP が結合している場合、SPP/SPS 内部通信に使用されます。 • SPS->SPP: ◦ SPS が SPP とポート 8649 で通信することにより、参加が完了します。 ◦ SPS が SPP とポート 8649 で通信し、新規セッションの認証と SPP からのパスワードの取得を行います。 ◦ SPS は SPP にクラスタ情報およびアプライアンスのバージョンを問い合わせます。 • SPP->SPS: ◦ SPP は SPS に対して、クラスタ情報とノードの役割を問い合わせます。 ◦ SPP は、セッションが開始されると、SSH ホストキーを SPS にプッシュします。 ◦ SPP は、セッションの再生、フォローモード、セッションの終了を SPS に問い合わせます。 SPS では、ノードは UDP ポート 500 と 4500、TCP 8649 を必要とします。最新の詳細については、『Safeguard for Privileged Sessions 管理者ガイド』を参照してください。
ファイアーウォール	655	UDP(X0)	WireGuard (655) は、クラスタ化された高可用性構成のアプライアンス間のセキュアな VPN 通信のために開かれています。

SPP で使用	アプライアンスポート	プロトコル	説明
			アプライアンスをクラスタに登録するには、アプライアンスがポート 655 UDP およびポート 443 TCP で通信し、IPv4 または IPv6 ネットワークアドレスを持っている必要があります（混在不可）。IPv4 と IPv6 の両方が接続可能な場合、IPv6 が使用されます。次を参照してください： • KB article 232289 • KB article 252260 • KB article 232671 • クラスタ • レプリカのクラスタへの登録
ファイアウォールとクライアントと Web ブラウザのポイント	443	TCP(X0)	HTTPS over TLS/SSL（443/TCP）は、Inbound リクエストを許可します（クライアント/Web/API アクセス用）。クラスタメンバーに参加するためにアプライアンスに最初にログオンするために使用されます。ユーザーは、ポート 443 でクラスタ X0 ポートにアクセスする必要があります。 アプライアンスをクラスタに登録するには、アプライアンスがポート 655 UDP およびポート 443 TCP で通信し、IPv4 または IPv6 ネットワークアドレスを持っている必要があります（混在不可）。次を参照してください： • KB article 232289 • KB article 252260 • KB article 232671 • KB article 229909 (Starling related endpoint) VMware ESXi ホストを準備するために使用するポートについては、次を参照してください： • VMware ESXi ホストの準備

SPP で使用	アプライアンスポート	プロトコル	説明
グローバルカタログ	3268		Active Directory の LDAP 標準グローバルカタログポートです。ディレクトリ管理タスク（ディレクトリアカウント、ディレクトリユーザーアカウント、ディレクトリユーザーグループの追加など）のために、環境内のすべての Windows グローバルカタログサーバーと SPP アプライアンスが通信するには、ファイアウォールで標準のグローバルカタログのポート 3268（LDAP）を開いておく必要があります。LDAP は、暗号化されていない接続にポート 389 を使用します。詳細については、Microsoft パブリケーション『How the Global Catalog Works』を参照してください。次も参照してください。 • アカウントの追加 • ディレクトリユーザーグループの追加 メンバー/サーバーワークステーション（ローカル構成）でこのポートをリッスンしているサービスはありません。
キオスク	DB9	SERIAL	Safeguard Kiosk に接続するため。KB 記事 233584 を参照してください。
Radius サーバー	1812		Radius サーバーが認証要求をリッスンするために使用するデフォルトのポート番号。「ID と認証プロバイダの追加」を参照してください。
SonicWALL SMA または CMS アプライアンス	8443	TCP/ UDP	SonicWALL SMA または CMS アプライアンスの場合。資産の認証に関連する情報については、「パスワード（ローカルサービスアカウント）」を参照してください。
SQL サーバー	1433		SQL サーバーが接続をリッスンするポートです。資産の認証に関連する情報については、

SPP で使用	アプライアンスポート	プロトコル	説明
			「パスワード（ローカルサービスアカウント）」を参照してください
Telnet	23	TCP	Telnet

プラットフォームポート

ACF2 – 23

ACF2 LDAP – 389

AIX – 22

AWS – 443

Cent OS – 22

Cisco Pix – 22

Debian – 22

IDRAC – 22

ESXi - 443 default

F5 - 22 default

Fortinet – 22 default

Free BSD – 22

HP iLO

IBM i – 23

JunOS – 22

MongoDB - https://docs.mongodb.com/manual/reference/default-mongodb-port/

MySQL – 3306

Oracle – 1521

Oracle Linux – 1521

OSX – 22

Other – ポートがプラットフォームでサポートされていません。

Other Managed - ポートがプラットフォームでサポートされていません。

Other Linux – 22

Pan OS – 22

PostgreSQL – 5432 default

RACF – 23

RACF LDAP – 389

RHEL – 22

SAP Hana – 39013 default

SAP Netweaver – 3300

Solaris – 22

SoniOS – 22

SonicWall SMA – 22

SQL – 1433

SUSE – 22

SyBase – 5002

Top Secret – 23

Top Secret LDAP – 389

Ubuntu – 22

Windows (OS の種類により異なる) - 135/389/445 およびおそらくダイナミックポート

アーカイブ

アーカイブは SFTP/SCP および CIFS を使用します。

- SFTP/SCP：22 TCP (X0) ポート詳細表を参照してください。ポート 22（X0）
- CIFS：UDP ポート 137、138 および TCP ポート 139、445

バックアップ

アーカイブと同じ

外部認証

Federation – ポート 443

Secondary Auth – Radius ポート 1812

Starling – ポート 443

外部統合

SNMP – ポート 162 UDP

SMTP - ポート 25 TCP Simple Mail Transfer

Syslog – ポート 514 UDP

パスワードおよび SSH キーワークフローのための外部統合

Cloud Assistant - 443

チケットシステム– ServiceNow 443

チケットシステム- Remedy 1433 （SQL サーバーとの直接通信）

その他

NTP – port 123 UDP

ディレクトリ– Ports 389 LDAP、3268 グローバルカタログ

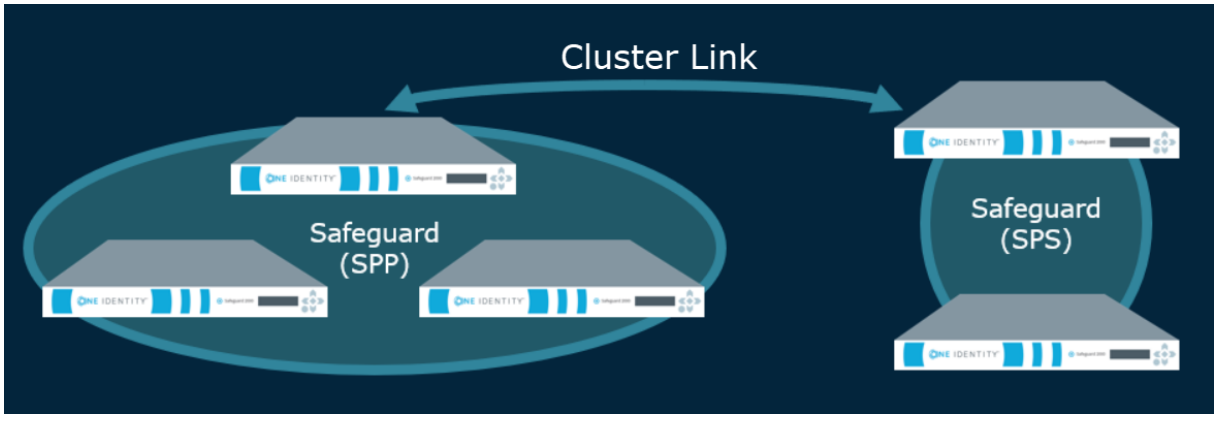
付録 B：SPP と SPS のリンクガイダンス

資産管理者は、セッションの記録と監査のために、SPS クラスタを 1 台以上のアプライアンスからなる SPP クラスタにリンクさせることができます。実際のリンクは、SPP プライマリと SPS クラスタマスタの間で行う必要があります。つまり、SPS クラスタは SPP クラスタの各ノードを認識し、SPP クラスタも SPS クラスタの各ノードを認識します。

リンクされると、すべてのセッションがアクセスリクエストを介して SPP アプライアンスによって開始され、SPS アプライアンスによって管理されます。セッションはセッションアプライアンスを介して記録されます。

> ⚠ **注意：SPS を SPP にリンクする場合、SPS と SPP のバージョンが完全に一致することを確認し、アップグレード中にバージョンを同期させてください。たとえば、SPS バージョン 6.6 は SPP バージョン 6.6 のみをリンクすることができ、SPS をバージョン 6.7 にアップグレードする場合は、SPP も 6.7 にアップグレードする必要があります。**
>
> **Long Term Supported (LTS) と機能リリースを混在させないように注意してください。たとえば、SPS バージョン 6.0.1 を SPP バージョン 6.1 とリンクさせないでください。**

> **メモ：**単一ノードの SPS クラスタで、中央管理ノードが検索マスタでもある場合、SPP はセッションを開始できません。クラスタ内に、セッションを記録できる SPS アプライアンスが少なくとも 1 つ存在する必要があります。「Safeguard for Privileged Sessions 管理者ガイド」SPS 管理ガイドの「Safeguard for Privileged Sessions（SPS）クラスタを管理する」を参照してください。



その他の概要情報は、『Safeguard for Privileged Sessions 管理者ガイド』の「SPP と SPS の使用」に記載されています。

リンク後のセッションの記録、再生、保存

- リンク後に記録されたセッションは、SPP を通して再生可能で、SPS アプライアンスに保存されます。アーカイブサーバーは、SPS から設定できます。

リンク後の機能

SPP のユーザーインターフェイスで処理される次の機能は、リンク後も SPS で使用できます。

- セッション証明書の割り当ては、SPS で行います。この証明書は、監査人による監査に利用できます。
- SPS が開始した SPP と RDP 接続では、プライマリプロバイダ名が一致している必要があります。ナレッジベース記事 KB311852 を参照してください。

リンク後の SPP では、次の機能が利用できます。

- リンク中、SPP は SPS 接続ポリシーを SSH の場合は safeguard_default、RDP の場合は safeguard_rdp に適宜設定します。変更する必要がある場合があります。これは、SSH または RDP のデフォルトポリシーにすぎません。
- **［アクセスリクエストポリシー］**ダイアログで設定されたその他の設定は、リンクの影響を受けません。これには、**［全般］、［スコープ］、［セキュリティ］、［ワークフロー］**タブが含まれます。
- アクティビティセンターには、設定されたすべての古いセッションと新しいセッションが表示されます。SPP からセッションを再生することができます。セッションプレーヤー 1.9.4 以降では、SPP でセッションをフルインデックス化（特権ユーザーのアクティビティを検索できるようにする）して再生することができます。ただし、以前のバージョンのセッションプレーヤーを使用している場合、インデキシング機能は SPS でのみ利用可能です。
- 資格レポートは変更されていません。
- ダッシュボードでは、管理者は通常通り、アクセスリクエストやアカウントの失敗タスクを表示および管理できます。

ステップ 1: SPS と SPP のリンク

リンクは、SPS から開始されます。リンクの手順と問題解決の詳細については、『One Identity Safeguard for Privileged Sessions 管理ガイド』を参照してください。

> **メモ:** SPP は、IP アドレスによって特定の SPS アプライアンスまたはネットワークインターフェイスをターゲットにすることができます。これは、SPS 接続ポリシーを構成して明示的な TO アドレス（たとえば、CIDR 表記 /32）を指定することによって行われます。その接続ポリ

> シーがアクセスポリシーの SPS 接続ポリシーとして選択されると、SPP はその特定の IP アドレスをターゲットとする接続文字列を構築します。

SPS ノードに割り当てられた役割に注意してください。SPP からのセッション再生を失わないために、次を注意してください。

> ⚠ **注意： SPS ノードの役割を、Search Local ロールから Search Minion ロールに切り替えないでください。この場合、Search Local ロールで記録されたセッションの再生は、SPP アプライアンスから再生されず、SPS Web ユーザーインターフェイス経由でのみ再生される可能性があります。Search Minion ロールのノードで行われた記録は、Search Master ノードにプッシュされ、SPP にダウンロードできるようになります。SPS のノードとロールの詳細については、『One Identity Safeguard for Privileged Sessions 管理ガイド』を参照してください。**

ステップ 2：SPS と SPP でリンク後のアクティビティを実行する

SPP で実行する手順

1. アプライアンス管理者が、セッション管理用の管理対象ネットワークを割り当てます。

   ［アプライアンス管理］＞［クラスタ］＞［管理対象ネットワーク］の順に選択します。詳細については、「管理対象ネットワーク」を参照してください。

2. アプライアンス管理者は、必要に応じてリンク接続を表示、削除、または編集することができます。

   ［アプライアンス管理］＞［クラスタ］＞［セッションアプライアンス］の順に選択します。詳細については、「SPS リンクのあるセッションアプライアンス」を参照してください。

   セッション接続をソフト削除してから再接続した場合、アクセスポリシーは引き続き使用できます。ハード削除した場合、セキュリティポリシー管理者は、SPS 接続ポリシーを再リンクして再確立する必要があります。詳細については、「接続の削除：ソフト削除とハード削除」を参照してください。

3. セキュリティポリシー管理者は、資格アクセスリクエストポリシーのセッション設定を識別します。

   次の手順を実行し、各ポリシーのセッション設定が正しく割り当てられていることを確認します。

   a. **［セキュリティポリシー管理］＞［資格］**の順に移動して資格を選択し、**［アクセスリクエストポリシー］**を開きます。

b. ポリシーをダブルクリックするか、ポリシーを選択して **［編集］**をクリックします。

c. **［セキュリティ］**タブで、**［SPS 接続ポリシー］**に移動します。クラスタマスタのホスト名が最初に表示され、その後に IP アドレス：safeguard_default が表示されます。

d. 必要に応じて、ポリシーが適用されるクラスタまたはアプライアンスを選択します。

4. **アクセスリクエストポリシー**ダイアログで、セキュリティポリシー管理者は、必要に応じて他のタブを確認します。全般、スコープ、セキュリティ、ワークフロータブを含むタブの設定に影響しません。

SPS で実行する手順

SPS で必要なセットアップを完了します（アーカイブサーバー、SSH バナー、SSH ホストキー、SSH 関連または RDP 関連のコマンド検出および制御のセットアップなど）。詳細については、『Safeguard for Privileged Sessions 管理者ガイド』を参照してください。

初期リンク後の標準的な操作手順

初期リンク後に別の SPS クラスタを追加する場合は、以下の標準的な操作手順に従います。

1. リンク接続を追加します。詳細については、「SPS リンクのあるセッションアプライアンス」を参照してください。

2. 資格アクセスリクエストポリシー（クラスタマスタの IP アドレスである SPS 接続ポリシー）のセッション設定を確認します。詳細については、「アクセスリクエストポリシーの作成」を参照してください。

3. 管理対象ネットワークを割り当てます。詳細については、「管理対象ネットワーク」を参照してください。

付録 C. 正規表現

正規表現は、大量のデータを解析して、一致するパターンを見つけ、定義済みのパターンを検証するために使用されます。たとえば、SPP では、正規表現が次のように使用されます。

- アカウント検出ルール（プロパティ制約、名前範囲、グループ範囲）。部分一致にも利用できます（ただし、正規表現自体が完全一致のみを返すよう定義されている場合を除く）。
- 外部チケットシステムを使用していない場合のチケット番号。完全一致である必要があります。

詳細については、以下の Microsoft リソースを参照してください。

- .NET 正規表現
- 正規表現言語 - クイックリファレンス

外部チケットシステムに関連付かないチケットのベストプラクティス

これらのベストプラクティスは、外部チケットシステムと関連付けられていないチケットのための正規表現を追加するためのものです。詳細については、「チケットシステム」を参照してください。

交替構文（"|" は "or"）を使用すると、Windows .Net 正規表現（regex）は最初に一致するものを見つけると停止するので、最も長く一致する表現が最も少なく一致する表現に最初に定義されます。

例えば、A{3}[0-9]{5}ZZZ|A{3}[0-9]{5} が（逆の順序ではなく）推奨されます。A{3}[0-9]{5}ZZZ|A{3}[0-9]{5} 式での入力結果の例は以下の通りです。

ユーザー入力	一致？
AAA12345	一致する。2 番目の正規表現に一致します。
AAA12345Z	一致しない。完全に一致するものはありません。
AAA12345ZZZ	一致する。1 つ目の正規表現に一致します。 式を逆にした場合(A{3}[0-9]{5}|A{3}[0-9]{5}ZZZ)、最初の式に部分一致があり、エントリは無効として返されます。

交替構文を使用する場合、各式をアンカー ^ と $ で囲むとよいでしょう。
例：^A{3}[0-9]{5}ZZZ$|^A{3}[0-9]{5}$.

? lazy 量指定子は、特に式の最後では避けるべきです。例えば、正規表現が A{3}[0-9]? で、ユーザーが AAA12345 を入力した場合、AAA12345 と完全一致しないが、一致した文字列として、AAA1 が返されます。

AAA12345 に対して greedy 数量化子（*）を使用すると、一致する文字列は AAA12345 となり、完全一致となります。

One Identity 社について

One Identity 社のソリューションは、アイデンティティの管理、特権アカウントの管理、アクセスの制御に必要とされる複雑で時間のかかるプロセスを排除します。One Identity 社のソリューションは、オンプレミス、クラウド、ハイブリッド環境における IAM の課題に対応しながら、ビジネスの俊敏性を向上させます。

お問い合わせ

ライセンス、サポート、更新などについては、こちらからお問い合わせください。

お問い合わせ

この資料についてご不明な点やお気づきの点などがございましたら、お問い合わせください。

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

URL：　https://www.jtc-i.co.jp/

購入前のお問い合わせ先：https://www.jtc-i.co.jp/contact/scontact.php

購入後のお問い合わせ先：https://www.jtc-i.co.jp/support/customerportal/

発行日 2023 年 3 月 13 日

本マニュアル原文 One Identity Safeguard for Privileged Passwords 7.0.2 LTS Administration Guide

ジュピターテクノロジー株式会社