

IBM Endpoint Manager
バージョン 9.1

インストール・ガイド



IBM Endpoint Manager
バージョン 9.1

インストール・ガイド



お願い

本書および本書で紹介する製品をご使用になる前に、193 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM Endpoint Manager バージョン 9、リリース 1、モディフィケーション・レベル 0、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Endpoint Manager
Version 9.1
Installation Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

© Copyright IBM Corporation 2010, 2014.

目次

第 1 章 概要	1
V9.1 の新機能	1
Service Management Connect	3
アーキテクチャー・コンポーネントの概要	4
第 2 章 サンプルの適用シナリオ	7
基本的な適用環境	8
本社と支社を高速 WAN で接続	9
災害対応サーバー・アーキテクチャー	11
効率的なリレーのセットアップ	12
ハブ・アンド・スポーク	14
リモート Citrix またはターミナル・サービスの構成	15
第 3 章 前提事項と要件	19
前提事項	19
サーバーの要件	20
コンソールの要件	21
クライアントの要件	21
データベースの要件	21
セキュリティーの要件	22
ネットワーク構成の要件	24
第 4 章 セキュリティー構成シナリオ	27
Windows システムの場合	27
Linux システムの場合	30
第 5 章 インストールのタイプ	31
評価インストール	31
正規版インストール	31
基本インストール	33
標準インストール	35
複数のサーバーのインストール	35
第 6 章 ライセンスの管理	37
ライセンス認証ファイルの作成	39
ライセンス交付支援	40
更新されたライセンスとマストヘッドの配布	40
Windows サーバーからクライアントへのマストヘッ ドの配布	41
Linux サーバーからクライアントへのマストヘッ ドの配布	44
第 7 章 インストールを実行する前に	45
ローカル・ファイアウォールの構成	45
ポート番号の変更	45
第 8 章 Windows システムでのインスト ール	47
インストール手順	47

ステップ 1 - IBM Endpoint Manager のダウンロ ード	47
ステップ 2 - ライセンス証明書の要求とマストヘ ッドの作成	48
ステップ 3 - コンポーネントのインストール	54
Windows システム上のプライマリー・サーバーの削 除	91
Windows レプリケーション・サーバーのアンインス トール	91

第 9 章 Linux システムでのインストー ル	93
DB2 のインストールと構成	93
インストール手順	95
ステップ 1 - IBM Endpoint Manager のダウンロ ード	95
ステップ 2 - サーバーのインストール	96
ステップ 3 - サーバー・インストールの確認	101
インストール・コマンド・オプション	102
サイレント・インストール	103
インストール・フォルダーの構造	107
構成ファイル、マストヘッド・ファイル、およびロ グ・ファイル	108
Endpoint Manager サービスの管理	108
DB2 パスワードの変更	109
DB2 ポートの変更	109
追加サーバーの認証 (DSA)	110
DB2 認証の使用	110
追加 Linux サーバーのインストール (DSA)	111
サーバーのコンポーネントについて	112
コンソールのインストール	113
クライアント適用ツールのインストール	114
クライアントのインストール	114
クライアント・インストール・ツールの使用	115
クライアントの手動インストール	117
Endpoint Manager 管理ツールの実行	128
Linux システム上のプライマリー・サーバーの削除	132
Linux レプリケーション・サーバーのアンインスト ール	133

第 10 章 インストール後の構成手順	135
ポストインストール・ステップ	135
Fixlet サイトのサブスクライブ	138

第 11 章 リレーの管理	141
リレーの要件と推奨事項	141
リレーのセットアップ	142
クライアントへのリレーの割り当て	143
クライアント・インストール時のリレーの割り当 て	143
既存のクライアントへのリレーの手動割り当て	145

クライアント・インストール時のリレーの自動割り当て	146
既存のクライアントへのリレーの自動割り当て	146
リレー・アフィリエイトの使用	147
リレーの自動割り当てに関する注意事項	148
IBM Endpoint Manager サーバーおよびリレーの調整	149
動的な帯域幅スロットリング	150
サーバーに到達できない場合のリレーの割り当て	152
インターネット・リレーの設定	152
クライアント認証	155
認証リレー	156
鍵交換の処理	156
手動での鍵交換	156
クライアント証明書の取り消し	157
取り消されたクライアントの再登録	158
メール・ボックス	158
クライアントに割り当てられているリレーの表示	159
リレーの適用状態のモニタリング	160

第 12 章 プロキシ接続のセットアップ	161
プロキシ接続のサーバー上での設定	163
リレーでのプロキシ接続のセットアップ	165
クライアントまたは子リレーでのプロキシ接続の設定	166
V9.X でプロキシ接続を定義する際に考慮する必要があるベスト・プラクティス	168

第 13 章 バックアップとリストアの実行	169
Windows システムの場合	169
サーバー・バックアップ	169
サーバーのリカバリー	170
リストア結果の検証	171

DSA リカバリー	172
Linux システムの場合	173
サーバー・バックアップ	174
サーバーのリカバリー	174
リストア結果の検証	176
DSA リカバリー	176

第 14 章 Windows システムでのアップグレード	179
V9.1 へのアップグレード・パス	179
アップグレードの前に	180
手動アップグレード	181
インストール・ジェネレーターでのアップグレード	181
サーバーのアップグレード	181
コンソールのアップグレード	181
リレーのアップグレード	182
クライアントのアップグレード	182
Web レポートのアップグレード	182

第 15 章 Linux システムでのアップグレード	183
V9.1 へのアップグレード・パス	183
アップグレードの前に	184
手動アップグレード	184
サーバーのアップグレード	185
コンソールのアップグレード	185
リレーのアップグレード	185
クライアントのアップグレード	185
Web レポートのアップグレード	186

付録 A. 用語集	187
----------------------------	------------

付録 B. サポート	191
-----------------------------	------------

特記事項	193
-----------------------	------------

第 1 章 概要

重要なシステムを、最新で、互換性があり、かつセキュリティー上の問題がない状態に保つために対処すべき問題はますます複雑になっていますが、IBM® Endpoint Manager はそれらを解決することを目的としています。この製品は、Fixlet テクノロジーを使用して、企業内の脆弱なコンピューターを特定します。マウスを数回クリックするだけで、中央コンソールから、ネットワーク全体で問題のあるコンピューターを修正することができます。

Fixlet は強力で、柔軟性があり、容易にカスタマイズすることができます。Fixlet テクノロジーを使用して、以下を実行できます。

- 脆弱性を分析する (パッチが適用された構成またはパッチが適用されていない非セキュアな構成)
- ネットワーク接続されたすべてのエンドポイントを容易に、かつ自動的に修正する
- 構成ポリシーを設定してネットワーク全体に適用する
- ソフトウェア・パッケージを配布して更新する
- ネットワーク接続されたクライアント・コンピューターのプロパティの表示、変更、および監査を行う

Fixlet テクノロジーによって、構成のステータス、脆弱性、および企業全体のインベントリを分析し、ほぼリアルタイムで自動的にポリシーを適用することができます。さらに、管理者は、独自の Fixlet ソリューションおよびタスクを、作成したり、固有のネットワークのニーズに適合するようにカスタマイズしたりできます。

IBM Endpoint Manager はインストールしやすく、また、パブリック・キーとプライベート・キーの暗号化テクノロジーが組み込まれており、Fixlet およびアクションの確実性が保証されます。管理者に最大限の能力を持たせますが、ネットワーク・トラフィックおよびコンピューター・リソースへの影響は最小限に抑えます。IBM Endpoint Manager は、世界中に広がるネットワーク内の何十万という数のコンピューターを扱うことができます。

これをインストールすると、中央コンソールから、すべてのネットワーク・コンピューターが正しく構成され、更新され、パッチが適用された状態を容易に維持することができます。各コンピューターについて、更新または構成ポリシーが適用される進行状況を追跡することができ、企業全体でのコンプライアンスのレベルを容易に確認できます。ダウンロードおよびセキュリティー・パッチのほかに、特定の属性によって管理対象コンピューターを調べることもでき、アクション適用、実行中のポリシー、または資産管理のためにそれらをグループ化することができます。結果をログに記録して、監査証跡を保持し、Web ベースの便利なレポート作成プログラムを使用してアクティビティー全体を図表にすることができます。

V9.1 の新機能

IBM Endpoint Manager V9.1 では、以下の機能拡張が追加されています。

拡張セキュリティ

この機能拡張には以下の機能が含まれています。

- SHA-256 用に SHA-1 署名を無効にする機能。
- TLS 1.2 通信プロトコルのサポート。
- ルート証明書のキー強度の拡張 (1024 ビットから 4096 ビットに拡張)。

注: 拡張セキュリティを有効にすると、9.1 よりも前のバージョンのエージェントやリレー (プロキシ・エージェントを含む) が管理されなくなります。

この機能拡張について詳しくは、27 ページの『第 4 章 セキュリティー構成シナリオ』を参照してください。

Web レポートでの LDAP グループのサポート

この機能拡張について詳しくは、ステップ 2: Web レポートの役割を LDAP ユーザーまたは LDAP グループに割り当てるを参照してください。

Linux サーバー・プロセスの 64 ビット化

以下のサービスが 64 ビットになりました。

- ルート・サーバー
- Web レポート
- FillDB
- GatherDB

コモン・クライテリア・セキュリティ認証機能

この機能拡張には以下の機能が含まれています。

- コンソールと Web レポートの構成可能なログイン・バナー。

ログイン・バナーを構成するには、**loginWarningBanner** オプションを設定します。詳しくは、83 ページの『詳細オプション』 (Windows システムの場合) または 128 ページの『Endpoint Manager 管理ツールの実行』 (Linux システムの場合) を参照してください。

- コンソールと Web レポートの無操作状態のタイムアウト。

無操作状態のタイムアウトを構成するには、**timeoutLockMinutes** オプションを設定します。詳しくは、83 ページの『詳細オプション』 (Windows システムの場合) または 128 ページの『Endpoint Manager 管理ツールの実行』 (Linux システムの場合) を参照してください。

- サーバー監査ロギングの拡張。

サーバー監査ロギングを構成するには、**_BESRootServer_Audit_Verbosity** 設定を指定します。詳しくは、https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli_Endpoint_Manager/page/Configuration_Settingsを参照してください。

ダッシュボード API の拡張

この機能拡張には以下の機能が含まれています。

- StopAction API の警告の抑止。
- インポート中のタグ・アクション。
- 非同期 DownloadFile API。

- 非同期 UploadFile API。

クライアント UI 用の拡張スクリーン・リーダー・サポート

この機能拡張には以下の機能が含まれています。

- 「バージョン情報」ダイアログと「アクション履歴」ダイアログでのスクリーン・リーダーのサポート。
- クライアント UI での高コントラスト表示モードのサポート。

REST API の機能拡張

この機能拡張には以下の機能が含まれています。

- エージェントが収集したファイルをサイトに追加する機能。
- コンピューターを削除する機能。
- REST API 経由で作成されたユーザーに関するログイン機能 (このユーザーは、サーバー監査ログにログインするようになりました)。

REST API について詳しくは、Web ページ https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli_Endpoint_Manager/page/REST_API を参照してください。

新しいエージェント・インスペクター

この機能拡張には以下の機能が含まれています。

- 平方根 (例: sqrt of 4)。
- タイプ <time of day with time zone> に対する比較演算子の追加。
- グループ・メンバーシップ・インスペクター (例: manual groups of <client>)。
- 文字列のパーセント・エンコード機能とパーセント・デコード機能。
- Windows システムの場合: プロセスでデータ実行防止が有効になっているかどうかを調べる機能。
- Windows システムの場合: レジストリー・インスペクターでの **REG_QWORD** レジストリー・タイプのサポート。
- Windows システムの場合: サービスのプロセス ID (pid) の取得機能 (例: pid of <service>)。
- *nix: ネットワーク・ソケット・インスペクター。

エージェント・インスペクターについて詳しくは、Web ページ http://support.bigfix.com/inspectors/Action%20Objects_Any.html を参照してください。

V9.1 に付属するフィックスのリストについては、<http://support.bigfix.com/bes/changes/fullchangelist-91.txt> を参照してください。

V9.1 (9.1.1065) に影響する既知の制約のリストについては、<http://www-01.ibm.com/support/docview.wss?uid=swg21667537> を参照してください。

Service Management Connect

サービス・マネジメント専門家と情報交換、学習、および共有を行います。これらの専門家は製品サポート技術のエキスパートであり、さまざまな見通しや専門知識を提供します。

Endpoint Management (<http://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=it#/wiki/Tivoli%20Endpoint%20Manager>) の Service Management Connect にアクセスします。Service Management Connect を使用すると、以下のことを行うことができます。

- Tivoli 製品の他のユーザーと IBM 開発者の間の公開された進行中の取り組みである透過的開発に参加する。初期設計、スプリント・デモ、製品ロードマップ、プレリリース・コードにアクセスすることができます。
- 共同作業する専門家と 1 対 1 で情報を交換し、Tivoli と、自分が参加しているコミュニティに関するネットワークにアクセスする。
- ブログを読んで、他の人の専門知識や経験を参考にする。
- WiKi やフォーラムを使用して、より広範囲にわたるユーザー・コミュニティと共同作業を行う。

本書で使用される用語

次の用語は、すべて IBM Endpoint Manager の用語です。これらの用語は、本書全体で、IBM Endpoint Manager というラベルなしで随時使用されます。

エージェント (Agent)

IBM Endpoint Manager クライアントがインストールされているコンピューターを意味します。

コンソール (Console)

IBM Endpoint Manager コンソールを意味します。

クライアント (Client)

IBM Endpoint Manager クライアントを意味します。

サーバー (Server)

IBM Endpoint Manager サーバーを意味します。

リレー (Relay)

IBM Endpoint Manager リレーを意味します。

また、「BigFix」や「BigFix Enterprise Suite」(BES) というラベルが付いたコンポーネントが表示される場合がありますが、これらは以前に使用されていた用語で、現在は「IBM Endpoint Manager」が代わりに使用されています。

アーキテクチャー・コンポーネントの概要

IBM Endpoint Manager システムには、次の主要コンポーネントが含まれます。

IBM Endpoint Manager エージェント:

エージェントは、IBM Endpoint Manager を使用して管理するすべてのコンピューターにインストールされます。IBM Endpoint Manager エージェントがインストールされたコンピューターは、クライアント とも呼ばれます。これらのクライアントは、機密漏れや正しくない構成などの脆弱性を検出する Fixlet の集合にアクセスします。クライアントは、コンソールから受け取った修正アクションをサーバー経由で実行することができます。IBM

Endpoint Manager クライアントは、ユーザーによって意識されることなく実行でき、最小のシステム・リソースを使用します。

IBM Endpoint Manager を使用すると、ユーザー入力を必要とするアクションの画面プロンプトに、管理者が応答することも可能になります。IBM Endpoint Manager クライアントは、アップストリーム通信を暗号化できるため、機密情報が保護されます。IBM Endpoint Manager クライアント・ソフトウェアは、Windows、Linux、Solaris、HP-UX、AIX、および Macintosh オペレーティング・システムで実行できます。

IBM Endpoint Manager サーバー:

これは、アプリケーション・サービス、Web サーバー、データベース・サーバーなど、対話型サービスのコレクションを提供し、IBM Endpoint Manager システムの中核を形成します。これらのサーバーは、個々のコンピューターへの情報および個々のコンピューターからの情報の流れを調整し、結果を IBM Endpoint Manager データベースに保存します。IBM Endpoint Manager サーバー・コンポーネントはバックグラウンドでサイレントに動作し、管理者が直接介入することはありません。また、IBM Endpoint Manager サーバーには、組み込みの **Web レポート・モジュール**が搭載されており、権限があるユーザーは Web ブラウザーを通じて接続し、コンピューター、脆弱性、アクションなどに関するすべての情報を表示できます。IBM Endpoint Manager は、複数のサーバーをサポートし、システムに確固とした冗長性を与えます。

IBM Endpoint Manager リレー:

これによりシステムの効率性が向上します。これらのリレーによって負荷が分散されるため、各ネットワーク・コンピューターは IBM Endpoint Manager サーバーに直接アクセスせずに済みます。数百から数千の IBM Endpoint Manager クライアントが、ダウンロードのために 1 つの IBM Endpoint Manager リレーを参照でき、次に、そのリレーはサーバーに対して 1 つの要求のみ行います。IBM Endpoint Manager リレーは他のリレーにも接続できるため、さらに効率性が向上します。IBM Endpoint Manager リレーは、専用コンピューターである必要はありません。このソフトウェアは、Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8、Windows Server 2012、Red Hat Enterprise Linux 4、5、6、または Solaris 10 のいずれかで、IBM Endpoint Manager エージェントがインストールされているコンピューターにインストールできます。IBM Endpoint Manager リレーをインストールするとすぐに、ネットワーク内のクライアントがそのリレーを自動的に検出して接続できるようになります。

IBM Endpoint Manager コンソール:

これは、これらのすべてのコンポーネントを結び付け、ネットワーク内のすべてのコンピューターのシステム規模のビューを提供し、それに加えて、それらの脆弱性を示し、修正方法を提案します。IBM Endpoint Manager コンソールを使用することで、権限があるユーザーは、フィックスを必要とする各コンピューターにそれらのフィックスを迅速かつ簡単に配布できます。このとき、ネットワーク内の他のコンピューターは影響を受けません。IBM Endpoint Manager コンソールは、ネットワークで IBM Endpoint Manager サーバーにアクセスできる任意の Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、または Windows Server

2008 R2 コンピューターで実行することができます。大規模な適用環境では、コンソールは、通常、ターミナル・サーバーや Citrix サーバーによってホストされます。

第 2 章 サンプルの適用シナリオ

以下の適用のシナリオは、実際のケース・スタディーから得られたいくつかの基本的な構成を示しています。お客様の組織は、ネットワークのサイズ、クラスター間のさまざまな帯域幅制限、およびリレーとサーバーの数に応じて、以下の例のいずれかに類似する可能性があります。主な制約となるのは、CPU の処理能力ではなく、帯域幅です。

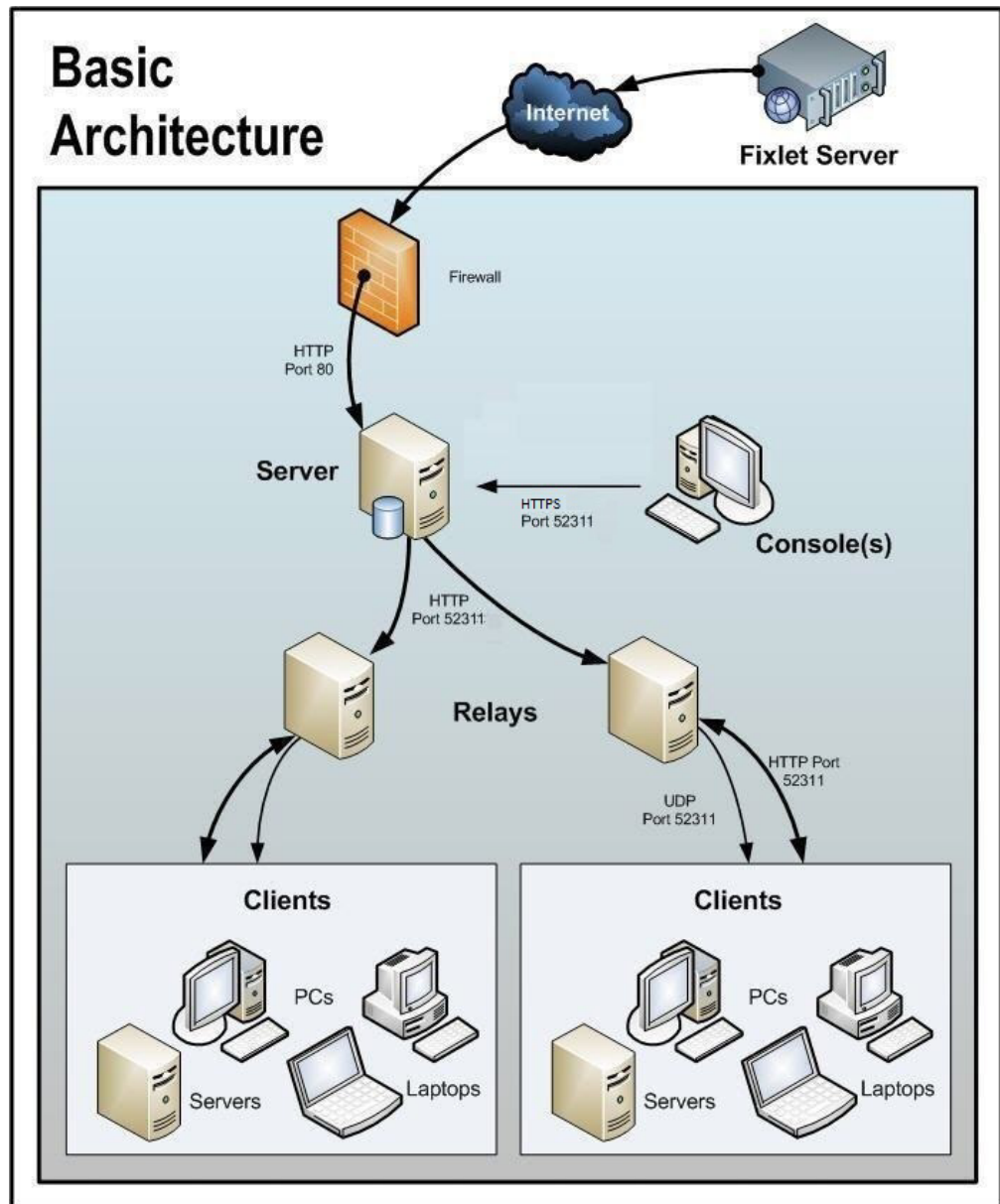
各シナリオで、リレーの配分に注意してください。リレーは、帯域幅の面で大幅な改善をもたらしますが、慎重に適用する必要があります (特に、通信が低速である状況の場合)。リレーは、一般に、かなり平坦な階層で最も効率よく機能します。最上位のリレーは、サーバーへの圧力を直接軽減し、その下の層は、負荷を分散するのに役立ちます。ただし、2 層よりも深い階層は、逆効果となる可能性があるため、注意して適用する必要があります。複数の層が必要となるのは、一般にリレーの数が 50 を超える場合のみです。このような場合、最上位層のリレーは、第 2 層の 50 から 200 個程度のリレーにサービスを提供する専用サーバーに適用されます。以下の例は、最も効率の良いネットワーク・レイアウトを導入するために役立ちます。

サーバーを追加すると、負荷を分散して冗長性をもたらすことにより、ネットワークの頑強性を高めることもできます。冗長サーバーを使用すると、フェイルバックとフェイルオーバーを自動化できるため、重大な状況であっても、データ損失を最小限に抑えることができます。

サーバーとリレーを正しく適用すると、どのようなサイズのネットワークにも対応できます。ここに示す例の範囲を超える場合は、IBM サポート技術者から、その他の構成について支援を受けることができます。

基本的な適用環境

以下の図は、基本的な階層と、コンポーネントの接続に使用されるポートを示す、非常に単純化された適用環境です。



図に関して、以下の事項に注意してください。

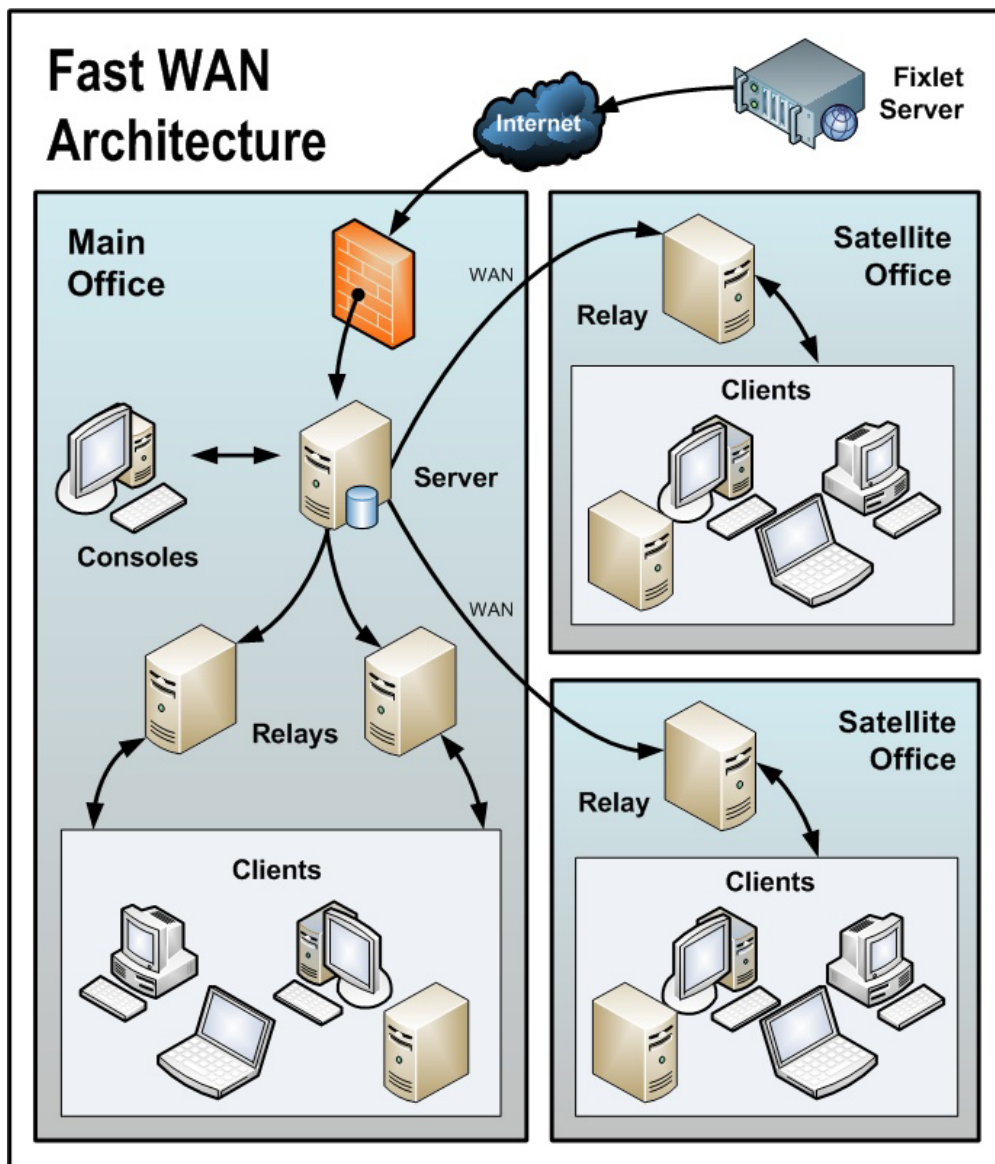
- ポート 80 は、IBM などの Fixlet プロバイダーからインターネットを介して Fixlet メッセージを収集するために使用されます。
- サーバー、リレー、およびクライアントの間の HTTP 通信には、専用ポート (デフォルトは 52311) が使用されます。
- サーバーとコンソールの間の HTTPS 通信には、専用のポート (デフォルトは 52311) が使用されます。

- リレーは、サーバー負荷を分担するために使用されます。この図では 2 つのリレーのみが示されていますが、類似した平坦な階層で数十あるいは数百のリレーを使用することができます。通常、500 台から 1,000 台のコンピューターごとに 1 つのリレーが適用されます。
- IBM Endpoint Manager リレーは、UDP ポートを利用して、更新に関するアラートをクライアントに送ることもできますが、これは絶対に必要というわけではありません。
- IBM Endpoint Manager クライアントは、通常 PC またはワークステーションですが、その他のサーバーや、ドッキング可能なラップトップなども使用できます。パッチおよび更新の恩恵を受ける可能性のあるデバイスはどれも、適用環境に組み込む候補となります。

IBM Endpoint Manager には、この単純な事例が示すよりも、さらに柔軟性と潜在的な能力があります。何十万という数のコンピューターを監視することが可能です。それらのコンピューターが世界中に分散していてもかまいません。次のシナリオは、この基本適用環境をベースとしています。

本社と支社を高速 WAN で接続

この構成は、多数の大学、政府機関、および各地に少数の支社を持つ小規模な企業で一般的に使用されています。このタイプの適用環境は、セットアップと管理を比較的簡単に行うことができます。これは、考慮する必要がある低速 WAN パイプが存在しない（またはほとんど存在しない）ためです。



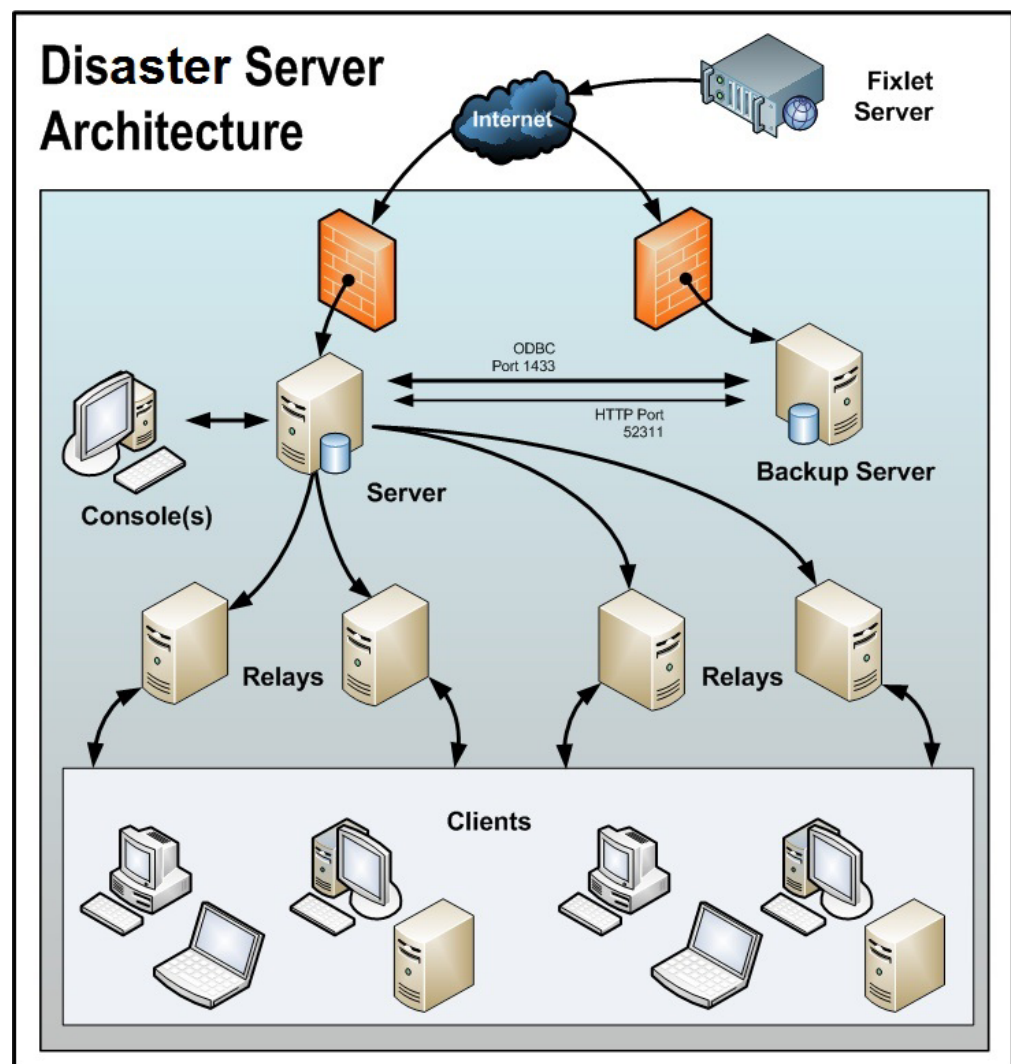
図に関して、以下の事項に注意してください。

- この構成では、サーバーの負荷を軽減するため、および通信を分散させ、帯域幅を最適化するために、リレーが使用されます。
- このシナリオでは、大規模な WAN パイプが使用されるため、オフィスのリレーはメイン・サーバーと直接通信できます。シン WAN を使用する場合、場合により、リレーのレイアウトを変更する必要があります (上記および下記のシナリオを参照)。
- 環境内にリレーが多ければ多いほど、ダウンロードおよび応答速度はより高速になります。
- このネットワークの特性のため、クライアントが「**最適なりレーを自動的に検出 (Automatically Locate Best relay)**」に設定されていると、多くのリレーとの距離が同じになります。このシナリオでは、クライアントは、近くにあるすべてのリレー間で自動的にロード・バランスを取ります。

- この高速 LAN では、すべてのリレーがメイン・サーバーに直接レポートする、比較的フラットな階層が推奨されます。階層内に余分なレベルがあると、不必要な遅延が発生するだけです。ただし、この環境内に 50 から 100 を超えるリレーがある場合、別のレベルにリレーを配置することを検討する必要があります。

災害対応サーバー・アーキテクチャー

機密性または高可用性のニーズがある企業では、複数の完全な冗長サーバーを設置して、重大な中断があった場合でも、継続的に運用できるようにしたいと考えます。複数のサーバーによって、負荷を分散し、さらに効率的な適用環境を作成することもできます。以下の単純な図は、冗長性を持たせるために複数サーバーをセットアップする方法を示しています。



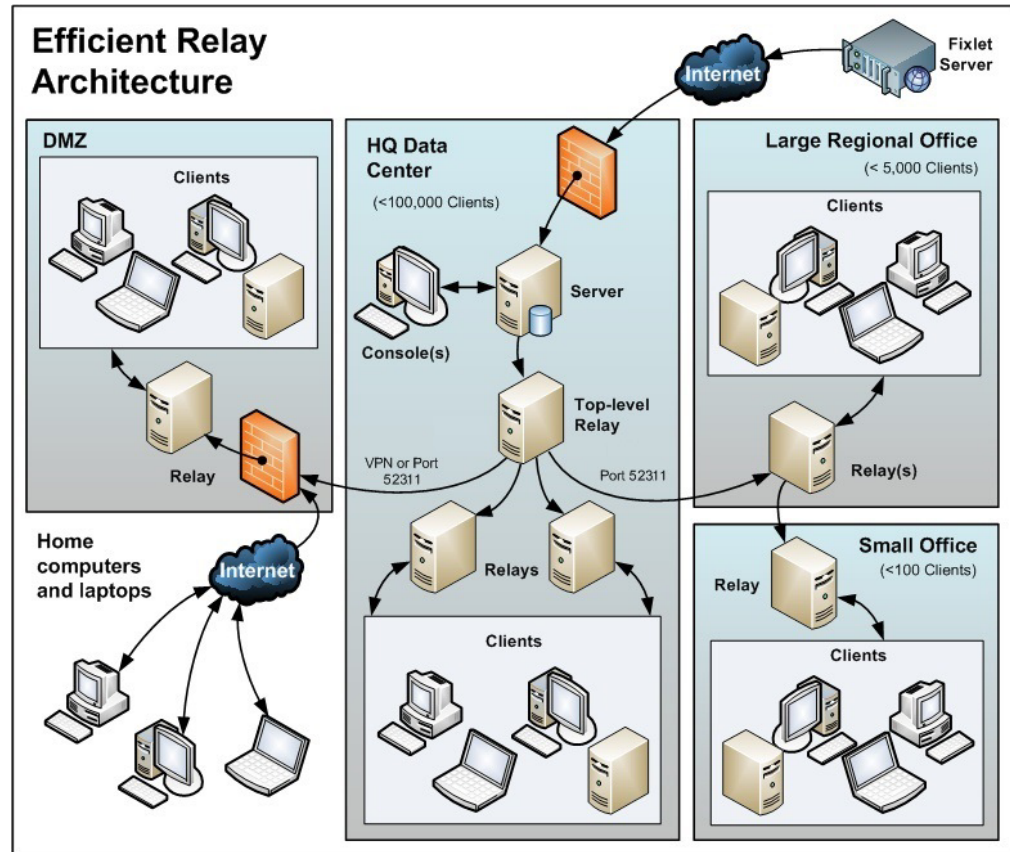
フェイルオーバーが発生した場合、構成されている特定のリレーがバックアップ・サーバーを自動的に検出し、ネットワークを再接続します。リレー構成について詳しくは、リレー・フェイルオーバーの構成を参照してください。

図に関して、以下の事項に注意してください。

- IBM Endpoint Manager サーバーは高速 WAN で接続されているため、1 時間に数回の同期が可能です。
- これらのサーバーには、正しく動作して複製を生成するために ODBC および HTTP の両方のリンクが必要です。
- ID が 0 (ゼロ) の 1 次サーバーがあります。これは最初にインストールするサーバーであり、IBM Endpoint Manager 管理ツールを実行するためのデフォルトのサーバーです。
- 分かりやすくするために、最小構成を示しています。より現実的な適用環境では、最上位のリレーが存在し、地域オフィスへの他の WAN 接続が存在する場合もあります。
- IBM Endpoint Manager サーバーおよびリレーは、サーバーの停止 (計画的またはその他の理由による) が発生した場合に制御が自動的に迂回され、フェイルオーバーの再接続時にデータベースが自動的にマージされるように構成されます。
- IBM Endpoint Manager サーバーは、データを複製するために定期的なスケジュールに基づいて通信します。「IBM Endpoint Manager 管理」>「レプリケーション」を使用して、現在のステータスを確認し、レプリケーション間隔を調整することができます。可能な範囲で最高のパフォーマンスを得るために、これらのパイプは太くする必要があります。
- この図では 2 台のサーバーのみを示していますが、追加のサーバーについてもそれぞれ同じ基本アーキテクチャーが適用されます。複数のサーバーがある場合、最短パス・アルゴリズムに従って複製が行われます。
- 停止またはその他の問題が原因でネットワークの分断が発生した場合、カスタム Fixlet または取得プロパティは、分断されたネットワークの両側で独立して変更できます。フェイルオーバー時にネットワークが再接続されると、最も小さいサーバー ID を持つサーバーのバージョンが優先されます。

効率的なリレーのセットアップ

効率を高め、遅延を減らすため、この会社では、サーバー負荷を軽減するためのリレー階層をセットアップしました。追加された各リレーは、パッチのダウンロードとデータのアップロードの両方で、余分な負荷をサーバーから取り除きます。リレーのセットアップは容易です。また、最も近いリレーを自動的に検出するようにクライアントを設定できるため、管理がさらに簡単になります。

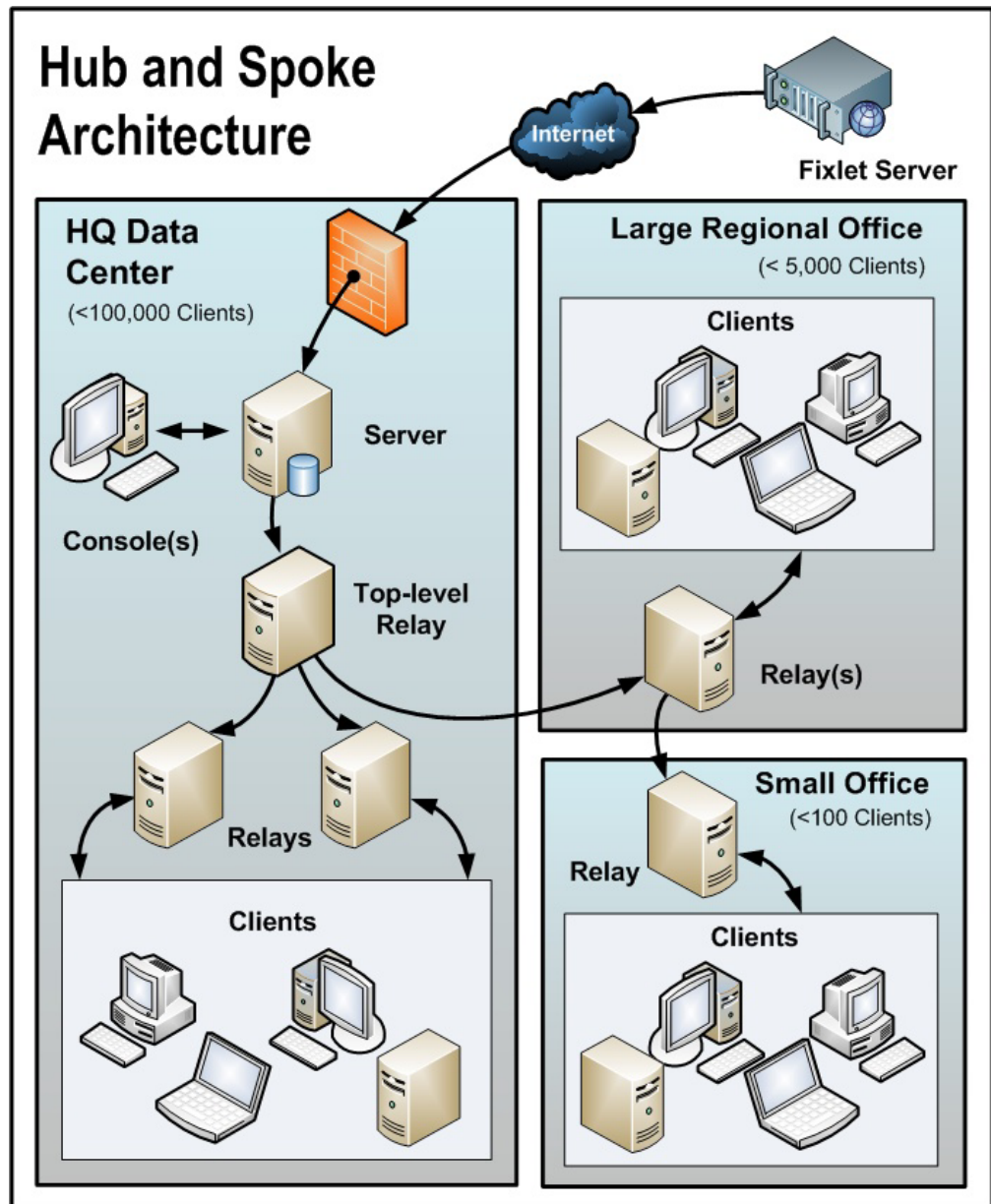


図に関して、以下の事項に注意してください。

- サーバー・コンピューターから負荷を取り除くために使用される、最上位リレーと呼ばれる専用サーバー・コンピューターがあります。
- すべてのリレーが、最上位リレーまたはより近くにある別のリレーのいずれかを指すように、手動で構成されます。リレーの構成の一般的なルールは、帯域幅のボトルネックがある場合を除き、リレーのレベルの数をできるだけ少なくすることです。細いパイプを介した通信は、リレーからリレーへの通信でなければなりません。最上位リレーはサーバーの負担を軽減し、セカンダリー・リレーは 1 回のダウンロードを数百のクライアントに分散します。
- サーバーとの特別な信頼関係によってセットアップされた DMZ 内にリレーがあります。このリレーは、DMZ 内またはパブリック・インターネット上のクライアントを、IBM Endpoint Manager が管理できるようにします。DMZ は、リレーと、インターネットからレポートを送信してくる一連のホーム・コンピューターおよびラップトップとの間に、セキュリティー・ファイアウォールを配置します。
- この図には、大規模な地域オフィス内の単一のリレーが示されています。ただし、数百を超えるクライアントがあるオフィスでは、負荷を効果的に分散させるために複数のリレーがあることが一般的です。
- 一般に、リレーの効率を最大にするためには、500 から 1000 個のクライアントごとに少なくとも 1 つのリレーを適用する必要があります。詳しくは、IBM Endpoint Manager サポート・サイトのリレーに関する記事を参照してください。

ハブ・アンド・スポーク

このシナリオには、メイン・データ・センター、少数の大規模地域オフィス、および多数の小規模地域オフィスが含まれます。この構成は、国際的な大規模組織で一般的に見られます。IBM Endpoint Manager クライアントは、世界中のオフィスにあるコンピューターにインストールされます。これらのロケーションの多くでは、低速の WAN 接続 (8 kbps から 512 kbps) を使用していますが、高速の WAN 接続 (1 Mbps から 45 Mbps) を使用するオフィスも数多く存在するようになります。



多くの場合、これらのロケーションは、ハブ・アンド・スポーク配置で構成されます。このシナリオは、前のシナリオをベースとしていますが、ハブ・アンド・スポーク構成により、リレー階層のレベルを増やすことができます。

図に関して、以下の事項に注意してください。

- このシナリオでは、帯域幅を最適化するために、WAN 内の適切なジャンクションにリレーが慎重に適用されます。リレーの配置が不適切な場合、ネットワークのパフォーマンスに悪影響を及ぼす可能性があります。
- 低速の WAN 接続を使用する各ロケーションに少なくとも 1 つのリレーをインストールすることが不可欠です。企業では、多くの場合、まさにこのような場所にサーバーが既に存在し、ファイル・サーバー、プリント・サーバー、AV 配布サーバー、SMS 配布サーバー、ドメイン・コントローラー、またはその他の任意のコンピューターとして機能しています。IBM Endpoint Manager リレーは通常、それらの既存のコンピューターにインストールされます。
- 一般的なオフィスで冗長性を提供するには、複数のリレーをインストールする必要があります。電源遮断やネットワークからの接続切断などの理由でリレーに障害が発生した場合、そのリレーに接続されたクライアントは、自動的に別のリレーに切り替えることができます。冗長リレーは、非常に小規模なオフィスでは重要性が低くなります。リレーの障害の影響を受けるコンピューターの数が少ないためです。
- クライアントが「**最適なリレーを自動的に検出 (Automatically Locate Best Relay)**」に設定されている場合、クライアントは最も近いリレーを選択します。いずれかのリレーに障害が発生した場合、クライアントは自動的に別のリレーを検出します。最初の自動セットアップ後に（およびその後も定期的に）リレー構成をモニターして、クライアントが適切なロケーションを指すようにする必要があります。IBM Endpoint Manager データによって WAN パイプ接続が過負荷にならないように保護する方法については、サポート技術者にお問い合わせください。
- この構成では、リレー・レベルでの帯域幅のスロットリングが非常に役立ちます。IBM Endpoint Manager リレーは、低速リンクを飽和させないように、WAN パイプ接続を介して低速でダウンロードするようにセットアップされています。詳しくは、IBM Endpoint Manager サポート・サイトのリレーに関する記事を参照してください。
- リレーは、メインのサーバーを指すのではなく、最上位のリレーを指すように構成されます。これによってサーバーが解放されて、コンソールとさらに緊密に結合されることで、レポート作成の効率が向上します。

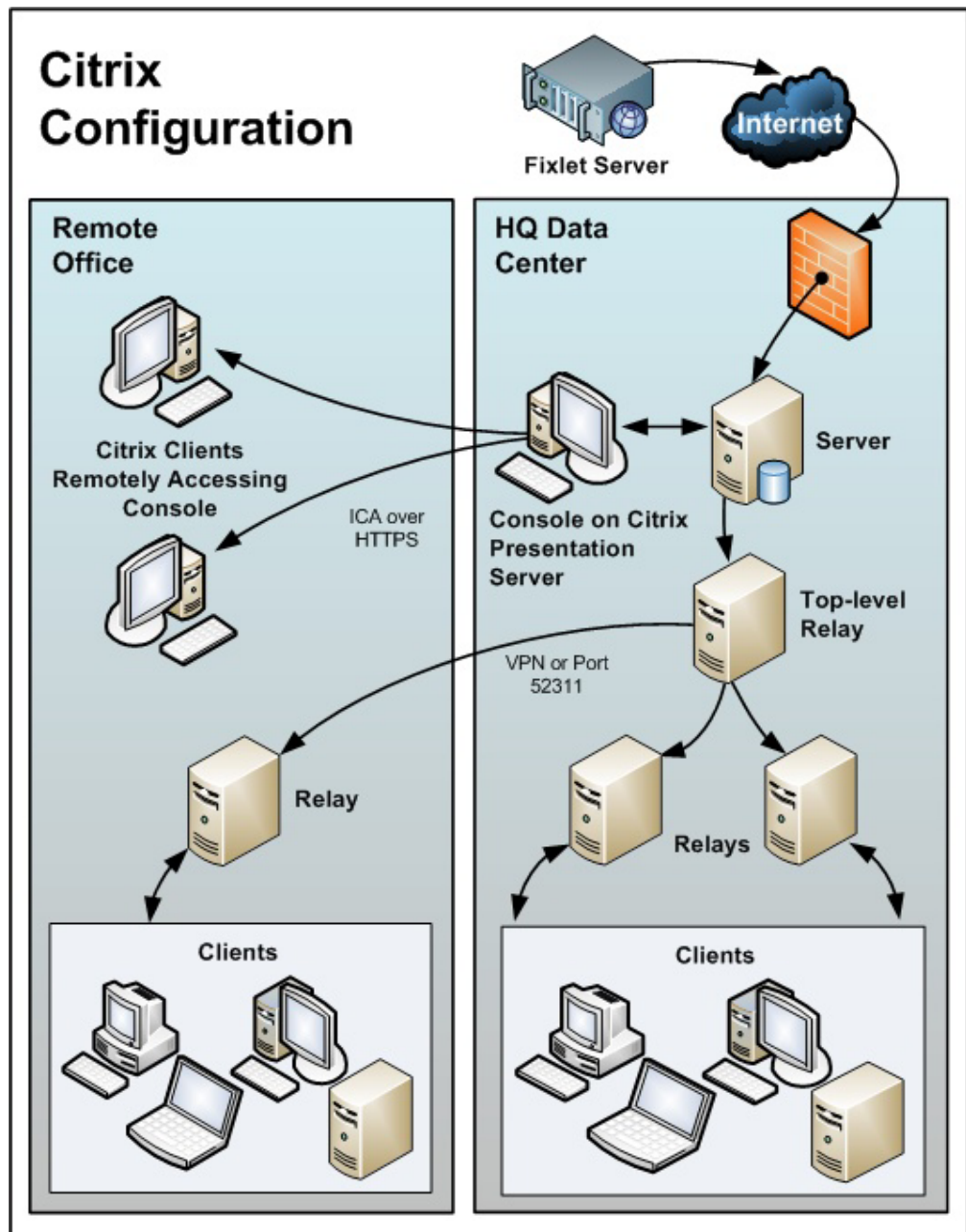
IBM Endpoint Manager リレーは、最適な階層を手動で作成するように構成されています。階層には以下の 3 つのレベルがあります（上位から下位）。

1. 直接サーバーに接続する最上位リレー
2. 最上位リレーに接続する地域オフィス・リレー
3. 指定された地域オフィス・リレーに接続する複数のブランチ・オフィス・リレー

リモート Citrix またはターミナル・サービスの構成

IBM Endpoint Manager は、低速接続でもコンテンツを効率的に配信できますが、コンソール自体にデータが集中すると、256 kbps よりも遅いリンクでは過負荷状態になる場合があります。クライアントをさらに追加すると、ラグ・タイムはさらに増えます。ただし、コンソールには、Citrix、ターミナル・サービス、VNC、または

Dameware スタイルのプレゼンテーション・サーバーからリモート・アクセスでき、優れたパフォーマンスを実現できます。以下に、この構成がどのようなものかを示します。



図に関して、以下の事項に注意してください。

- ・ 本社では、データを高速収集するために、サーバーに近いコンピューターにコンソールをセットアップします。これはプレゼンテーション・サーバーです。
- ・ 各リモート・ユーザーのユーザー・アカウントを作成する必要があります。これらのユーザーは、コンソールに迅速にアクセスすることができます。これは、速度が重視されるデータ・ロードが、高速リンクを使用して本社で実行されるためです。

- セキュリティーを向上させるために、リモート接続は HTTPS で実行できます。
- プライベート・キーを格納するプレゼンテーション・サーバーからコンソールを実行することは、キーがリムーバブル・ドライブに保存されている場合よりも本質的に危険ですので注意してください。
- リモート・アクセスを複数のサーバーに分散させるロード・バランシング・ソフトウェアを使用すると適切な場合があります。
- Citrix で実行されるコンソールの主なボトルネックは、メモリー・サイズです。コンソールでメモリー不足が発生すると、コンソールのパフォーマンスが急激に低下します。メモリー所要量を特定する適切な手法は、マスター・オペレーターとしてコンソールを開くことです。メモリーの使用状況を確認することで、ユーザー当たりの最大メモリー所要量が分かります。その後、通常のオペレーターとしてログインし、平均メモリー所要量としてこれを使用します。Citrix サーバーの最大メモリーですべての同時ユーザーをサポートできる場合、その Citrix サーバー 1 台で十分です。サポートできない場合、ユーザー当たりの平均メモリー所要量を使用して、必要とされる追加 Citrix サーバーの数を特定します。
- 2 番目の制約は CPU の処理能力です。コンソールは、更新中、CPU コアをフル活用した場合に最も適切に動作します。したがって、1 つの CPU コアで、それぞれの同時ユーザー用のコンソールを実行するように、プレゼンテーション・サーバーを最適化します。
- 最後の考慮事項は、コンソール・キャッシュのディスク・スペースです。ローカル・コンピューターで、¥Documents and Settings¥<USERNAME>¥Local Settings¥Application Data¥BigFix¥Enterprise Console¥BES_bfenterprise などを探ることにより、キャッシュのサイズを確認することができます。コンソール・オペレーターごとに 1 つのキャッシュ・ファイルを用意するために、十分なディスク・スペースが必要です。

第 3 章 前提事項と要件

IBM Endpoint Manager は、最小のサーバー、ネットワーク、およびクライアントのリソースを使用して効率的に実行されます。サーバーおよびコンソールで必要とされるハードウェアは、管理対象のコンピューターの数、およびコンソールの総数により決まります。IBM Endpoint Manager の分散アーキテクチャーにより、単一のサーバーで数十万のコンピューターをサポートできます。

前提事項

IBM Endpoint Manager を稼働するプロセスは、ご使用のネットワーク環境およびセキュリティ・ポリシーによって異なります。本書では、標準の適用環境に焦点を当てて説明します。これは、単一の単一の管理可能ドメイン内のワークグループおよび企業に適用されます。読みやすさと一般性のために、本書では次の制限を前提としています。

- IBM Endpoint Manager サーバーは、ポート 80 でインターネットに接続できます。IBM Endpoint Manager サーバーは、プロキシを使用するようにセットアップできます。これは一般的な構成です。詳しくは、161 ページの『第 12 章 プロキシ接続のセットアップ』を参照してください。

別の方法として、隔離を使用して、物理的に IBM Endpoint Manager サーバーをインターネットの Fixlet サーバーから分離することもできます。詳しくは、「構成ガイド」の『エアー・ギャップ環境でのファイルのダウンロード』を参照してください。

- 各 IBM Endpoint Manager サーバーは、SQL サーバー (ローカルのサーバー・マシンに配置された SQL サーバー、または個別のリモート SQL Server に配置された SQL サーバー) にアクセスできる必要があります。
- 各コンソール・オペレーターは、IBM Endpoint Manager サーバーに HTTP 接続できます。
- ネットワーク内の各 IBM Endpoint Manager クライアント・コンピューターは、指定のポート (デフォルト・ポートは 52311 ですが、使用可能な任意のポートを指定できます) でサーバーまたはリレーに HTTP 接続できる必要があります。
- ネットワーク内の各コンソールは、クライアントとして同じポート (デフォルト値は 52311) で、サーバーに HTTPS 接続できる必要があります。

これらの 1 つ以上の条件を満たしていない企業でも、現在の環境に IBM Endpoint Manager を適用することができます。詳しくは、**適用のシナリオ** (7 ページの『第 2 章 サンプルの適用シナリオ』) を参照してください。使用しているネットワーク構成がこの章のどのシナリオにも一致しない場合は、その他のオプションについてサポート技術者にお問い合わせください。

最小の IBM Endpoint Manager システム (サーバー、コンソール、および少数のクライアント) の最初のインストールは、約 1 時間で完了します。

システム全体をインストールする準備ができれば、効率的に実行するために、このマニュアルのクライアントおよびリレーのインストールに関するセクションに特に注意してください。

IBM Endpoint Manager をインストールするいくつかの手順は、前の手順が完了していることが前提となります。このため、本書では、記載されている順序に従うことをお勧めします。

サーバーの要件

サーバーの要件に関する最新情報については、「IBM Endpoint Manager for Lifecycle Management 9.1」を参照してください。

サポートされているオペレーティング・システム:

- Windows:
 - Windows 2008 R2 (x86, x64) Enterprise
 - Windows 2008 (x86, x64) Enterprise
 - Windows 2003 (x86, x64) Enterprise
 - Windows Server 2012

注: Windows ファイアウォールは必ずオフにしてください。Windows 2008 および Windows 2008 R2 のユーザー・アカウント制御は無効にするか低下させて、ローカル・システムとして実行されないサービスがユーザー・アカウント制御のポップアップ・メッセージに干渉されないようにする必要があります。

- Linux:

Red Hat Enterprise Linux (RHEL) Server x86-64 バージョン 6 フィックスパック 3 以上 (64 ビット・アーキテクチャー)

依存関係:

- IBM DB2 10.5。Red Hat Enterprise Linux Server 64 ビットに DB2 サーバーをインストールする方法については、93 ページの『DB2 のインストールと構成』および『IBM データ・サーバー・クライアントのインストール方法』を参照してください。
- IBM Endpoint Manager Linux サーバーおよび Web レポート・コンポーネントが必要とする以下の Red Hat パッケージ。

```
cyrus-sasl-lib.x86_64
libstdc++.x86_64 およびそのすべての前提条件
pam.x86_64
krb5-libs.x86_64
fontconfig.x86_64 (Web レポートのみ)
libXext.x86_64 (Web レポートのみ)
libXrender.x86_64 (Web レポートのみ)
zlib.x86_64 (Web レポートのみ)
```

注: Windows Endpoint Manager サーバーを Linux Endpoint Manager サーバーにマイグレーションすることはできません。

Linux に Endpoint Manager サーバーおよび Web レポートをインストールするための最小ディスク・スペース要件:

Endpoint Manager サーバー: 300MB、DB2: 1GB (6GB を推奨)

Endpoint Manager Web レポート: 250MB、DB2: 700MB

コンソールの要件

コンソールの要件に関する最新情報については、「IBM Endpoint Manager for Lifecycle Management 9.1」を参照してください。

IBM Endpoint Manager コンソールは、ラップトップや中程度の能力を持つコンピューターにインストールできます。ただし、コンソールを使用して管理するコンピューターの数が増えるにつれて、より強力なコンピューターが必要になる可能性があります。

IBM Endpoint Manager コンソールでは、コンソールに転送する必要があるデータの量が多いため、サーバーへの高帯域幅の接続 (LAN の速度が最も速い) も必要です。低帯域幅接続を介してリモートからサーバーに接続する必要がある場合は、サーバーへの接続が高速な、コンピューター (Citrix サーバーやターミナル・サービス・コンピューターなど) へのリモート制御接続を使用することをお勧めします。

コンソールのスケーリング要件について詳しくは、サポート技術者にお問い合わせください。

注: コンソールは、IBM Endpoint Manager への 1 次インターフェースであり、クライアントに関する大量の情報を管理します。コンソール・コンピューターの能力が低いか、その接続が低速である場合、パフォーマンスに悪影響を与えることがあります。

クライアントの要件

クライアントの要件に関する最新情報については、「Prerequisites of IBM Endpoint Manager for Lifecycle Management 9.1」を参照してください。.

データベースの要件

データベースには、クライアントから取得したすべてのデータが保存されます。IBM Endpoint Manager サーバーをインストールする前に、データベースの要件が満たされていることを確認します。

- Windows システム上の IBM Endpoint Manager サーバーでは、以下の構成がサポートされます。
 - ローカルまたはリモートの SQL Server 2005、2008、2008 R2、または SQL Server 2012。

重要: ログインして IBM Endpoint Manager サーバーをインストールするユーザーは、MSSQL Server でデータベースと表を作成するための sa 権限を持っている必要があります。

- Red Hat Enterprise Linux システム上の IBM Endpoint Manager サーバーでは、以下の構成がサポートされます。
 - DB2 Server をローカルにインストールする場合: DB2 10.5 Enterprise Server Edition 64 ビットまたは Workgroup Server Edition 64 ビット。
 - DB2 Server をリモートにインストールする場合: IBM Data Server Client 10.5。

注: db2licm -l コマンドを実行して、サーバーまたはクライアントがインストールされているかどうかと、DB2 のエディションを確認できます。DB2 サーバーがインストールされているコンピューターマシンでは詳細なレポートを受け取り、クライアントのみがインストールされている場合は空のレポートを受け取ります。インストールされている DB2 のバージョンを確認するには、db2level コマンドを実行します。

サポートされるデータベースのバージョンについて詳しくは、『Prerequisites of IBM Endpoint Manager for Lifecycle Management 9.1』を参照してください。

セキュリティの要件

システムは、安全な Public Key Infrastructure (PKI) 署名を使用するすべての Fixlet およびアクションを認証します。PKI では、確実に認証を行うために、パブリック・キーとプライベート・キーのペアが使用されます。

IBM Endpoint Manager をインストールするには、その前に、Windows 上ではインストーラー、Linux 上ではスクリプト `install.sh` を使用して自身の**プライベート・キー**を生成してから、**パブリック・キー**を含む署名証明書を IBM に申し込む必要があります。プライベート・キー (ユーザーのコンピューターにのみ存在し、IBM を含む他者に知られていない) は、ユーザーが選択するパスワードにより暗号化されるため、誰かがプライベート・キーを盗んだとしても、そのプライベート・キーを使用するにはさらにパスワードを知る必要があります。ただし、プライベート・キーも適切に保護する必要があります。サイトのプライベート・キーとパスワード、サーバーへのアクセス権、およびデータベース・ログインを所有するユーザーは誰でも、クライアント・コンピューターに対してアクションを適用できます。

プライベート・キーは、会社の玄関の鍵と同様に扱います。共有ディスクには保存しないでください。代わりに、リムーバブル・ディスクなどの安全な場所に保管し、それ自体を紛失しないようにしてください。物理的な世界でマスター・キーを紛失した場合、建物のすべての鍵を交換する必要があります。同様に、デジタル・キーを紛失した場合も、新しい許可キーに移行するか、または (すべてのクライアントを含む) システム全体をフレッシュ・インストールする必要があります。サイト・レベルのキー・ファイルのバックアップ・コピーを安全な金庫に保管することは不適切ではありません。

インストール・プロセス中、サーバーの署名キーが作成され、ファイルとしてサーバー・マシンに保存されます。オペレーターがアクションを実行すると、そのアク

ションに対して、サーバーの署名キーによりデジタル署名が行われ、クライアントはそのキーで署名されたアクションのみを信頼します。クライアントは、サーバーの署名キーにより署名されたアクションを信頼するため、サーバーの署名キー・ファイルを保護することが重要です。サーバーの署名キー・ファイルを保護するために、サーバー・マシンへの管理者権限を制限する必要があります。

Fixlet にもデジタル署名が行われます。Fixlet サイトの作成者は、認証のために IBM Endpoint Manager ルートにトレースバックできるキーを使用して各メッセージに署名します。この署名は、Fixlet サイトのマストヘッドと一致している必要があります。マストヘッドは、サイトのサブスクリプション時にクライアントのインストール・フォルダー内に配置されます。この手順により、スプーフィングおよび中間者攻撃が防止され、受信した Fixlet が元の認定済みの作成者からのものであることが保証されます。

組織に IBM Endpoint Manager をインストールする前に、セキュリティ関連の解決すべき問題がいくつかあります。

- サーバー・コンピュータで、Microsoft から入手可能な最新の Service Pack を適用した Windows Server 2003 以降が実行されていることを確認します。
- SQL Server が最新のセキュリティ関連のパッチを使用して保護されていることを確認します。
- すべての内部ルーターおよび内部ファイアウォールで、指定のポート（デフォルト値は、コンソールを含むすべてのコンポーネントで 52311）での TCP/IP および UDP が完全にブロック解除されていることを確認します。
- 外部ルーターで、指定のポート（デフォルト値は、すべてのコンポーネントで 52311）でのインバウンド・トラフィックおよびアウトバウンド・トラフィックが禁止されていることを確認します。これは、IBM Endpoint Manager 関連のトラフィックがネットワーク内に流れ込まないようにするため、およびネットワークから流れ出ないようにするためです。

DMZ 内に認証リレーを配置することで、ローミング・ラップトップを管理できます。追加の詳細については、『Internal Relays』を参照してください。

- ネットワーク管理者に問い合わせ、ユーザー本人が、サーバーがポート 80 を通じてインターネットにアクセスするように設定できることを確認します。
Windows 上の BES ルート・サーバー・サービスおよび Linux 上の beserver サービスは、インターネットにアクセスして、デフォルトで SYSTEM アカウント (Windows の場合) および root (Linux の場合) として実行されます。

注: ご使用の環境で、プロキシ経由でインターネットに接続する場合は、161 ページの『第 12 章 プロキシ接続のセットアップ』の説明に従って、接続を構成します。ファイアウォールの制限がある場合は、45 ページの『ローカル・ファイアウォールの構成』を参照してください。

インターネットからの物理的な切断を維持するには、「構成ガイド」の『エアー・ギャップ環境でのファイルのダウンロード』を参照してください。

- 会社または業界規模の標準を使用して、サーバー・コンピュータおよび SQL データベースを保護します。詳しくは、ネットワーク管理者またはデータベース管理者にお問い合わせください。

注: ほとんど使用されない特定のロックダウン手順が原因で、サーバーが適切に機能しなくなる場合があります。ロックダウン手順について具体的な質問がある場合は、IBM ソフトウェア・サポートにお問い合わせください。

ネットワーク構成の要件

セキュリティーおよびパフォーマンス上の理由から、次のネットワーク構成が推奨されています。

- すべての内部ネットワーク通信を、1 つの指定ポート (デフォルトのポートは、コンソールを含むすべてのコンポーネントで 52311) で実行します。これにより、適用環境が簡素化され、柔軟になります。すべての内部ルーターおよび内部ファイアウォールで、このポートの TCP/IP および UDP を完全にブロック解除する必要があります (オプションとして UDP を無効にできますが、その場合、パフォーマンスに悪影響を与える可能性があります)。
- IBM Endpoint Manager サーバーは 100 mbps 以上でネットワークに接続する必要があります。
- コンソールは IBM Endpoint Manager サーバーに高速接続 (100 mbps 以上) する必要があります。
- IBM Endpoint Manager サーバー・マシンでは Windows ファイアウォールはオフにする必要があります。
- IBM Endpoint Manager クライアントは、IBM Endpoint Manager サーバー・マシンにインストールする必要があります。

ネットワークに関するこれらの推奨事項は、適度なセキュリティー方針を維持しているほとんどの組織では、通常、容易に満たすことができます。組織でこれらの要件を満たすことができない場合は、「構成ガイド」を参照してください。大規模なインストールについて詳しくは、『適用のシナリオ』を参照してください。

クライアントの数とともに、その他の要因も、IBM Endpoint Manager サーバーの要件およびパフォーマンスに影響を与える場合があります。それらの要因を以下に示します。

コンソール・オペレーターの数

ネットワーク・コンピューターのサブセットを管理するために、複数のコンソール・オペレーターが同時にサーバーに接続できます。一部の適用環境では、オペレーターが数百人になる場合があります。オペレーターが 30 人を超える場合、追加の負荷をサポートするために、より強力なサーバーを使用することをお勧めします。

リレー クライアントからの接続を受信し、データをサーバーに転送することにより、リレーを使用してサーバーの負荷を軽減します。ほとんどの適用環境では、メインのサーバーに直接レポートするクライアントは非常に少数です。

注: パフォーマンスを向上させるには、500 から 1000 のクライアントを各リレーに接続し、親子リレー構成を使用します。

取得プロパティーおよび分析の数とタイプ

カスタム取得プロパティーおよび分析は、極めて有益なデータを提供できますが、カスタム・プロパティーを不適切に実装した場合、または過度に使用

した場合、帯域幅やクライアント・リソースが非常に多く必要になることで、システムで過度の負荷が発生する場合があります。例えば、すべてのコンピューターにあるすべてのファイルの名前を返すカスタム取得プロパティを作成することは、クライアント・コンピューターおよびネットワークに負荷をかけるため、賢明ではありません。

これらの問題について詳しくは、「Performance Configurations」を参照してください。

第 4 章 セキュリティー構成シナリオ

コンピューター・セキュリティーを強化するために、Endpoint Manager V9.1 では、拡張セキュリティー・オプションを構成して NIST セキュリティー標準に準拠する機能を提供しています。この設定により、デジタル署名とコンテンツ検証のハッシュ・アルゴリズムとして SHA-256 を使用できるようになります。また、Endpoint Manager コンポーネント間の TLS 1.2 通信が可能となります。

Endpoint Manager V9.1 をインストールした場合、またはすべてのコンポーネントを Endpoint Manager V9.1 にアップグレードした場合にのみ、拡張セキュリティー・オプションを設定できます。混合環境の場合は、前のバージョンの Endpoint Manager コンポーネントとの製品互換性を保持するために、拡張セキュリティー・オプションを設定しないようにするか、または設定する前に Endpoint Manager コンポーネントを V9.1 にアップグレードしてください。

注: このオプションを設定すると、厳しく制限されたセキュリティー環境を構成することになり、製品のパフォーマンスが低下する場合があります。このセキュリティー設定は、マストヘッド・ファイルを編集することでいつでも有効または無効にすることができます。追加情報については、「構成ガイド」を参照してください。

拡張セキュリティー設定に加えて、SHA-256 アルゴリズムを使用してファイル・ダウンロードの整合性を検証するためのチェックを設定できるようになりました。このオプションを設定しない場合、ファイル・ダウンロードの整合性チェックは SHA-1 アルゴリズムを使用して実行されます。この新しいオプションによって Endpoint Manager V9.0 コンポーネントとの互換性が失われることはありません。このオプションは、拡張セキュリティー・オプションを設定した場合にのみ設定できます。

複雑な環境では、すべての DSA サーバーが Endpoint Manager V9.1 にアップグレードされ、新しいライセンスを取得した場合にのみ、拡張セキュリティー・オプションを有効にすることができます。

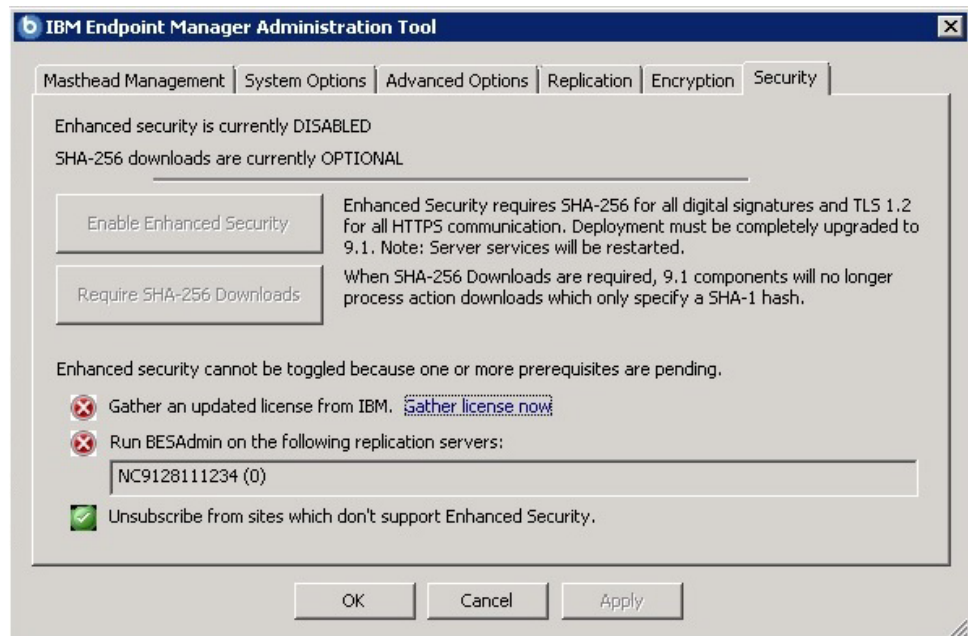
重要: 拡張セキュリティー・オプションをオンにした後は、オプションをオフにしても、以前のバージョンの Endpoint Manager にロールバックできません。ただし、必要な場合は、拡張セキュリティー・オプションの設定にかかわらず、Endpoint Manager V9.1 から V9.1 への災害復旧リストアを実行することができます。追加情報については、169 ページの『第 13 章 バックアップとリストアの実行』を参照してください。

Windows システムの場合

拡張セキュリティー・オプションを設定するには、以下の手順を実行します。

1. 「スタート」>「すべてのプログラム」>「IBM Endpoint Manager」>「IBM Endpoint Manager 管理ツール」をクリックして管理ツールを実行します。
2. サイト・ライセンス (license.pvk) のロケーションを参照し、「OK」をクリックします。

3. 「セキュリティー」タブを選択します。以下のウィンドウが表示されます。



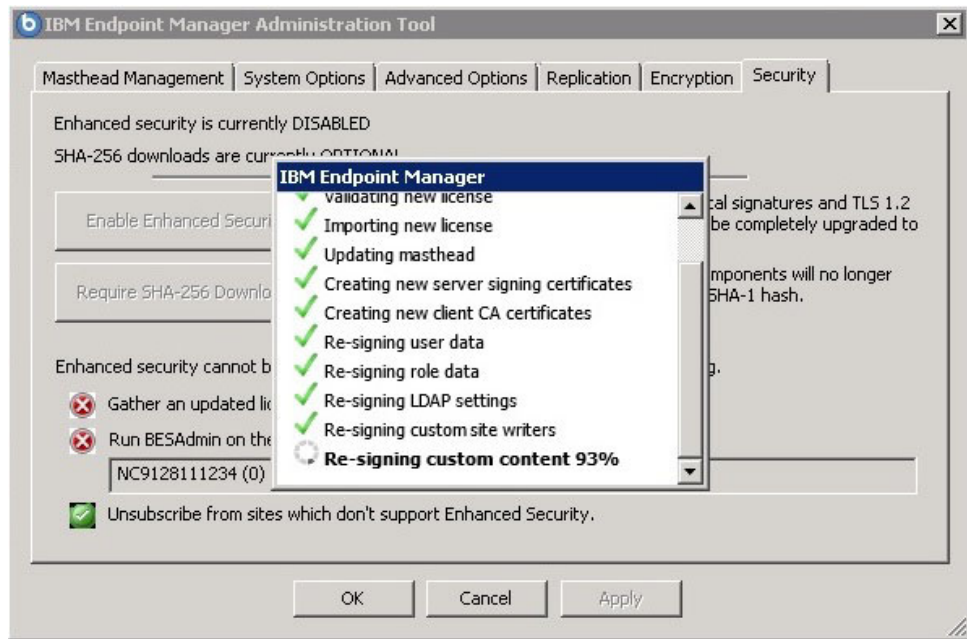
これで、拡張セキュリティー・オプションを有効にすることができます。

IBM Endpoint Manager を旧バージョンからアップグレードしたときに、サブスクライブしていたサイトで拡張セキュリティー・オプションがサポートされている場合は、「拡張セキュリティーをサポートしていないサイトのサブスクリプションを解除します」が選択されません。

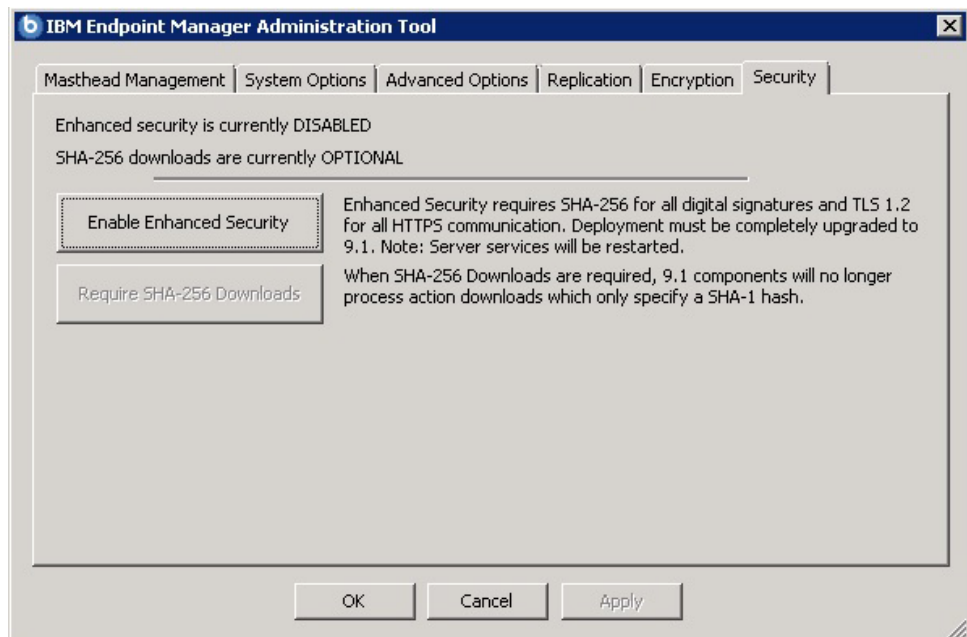
災害対応サーバー・アーキテクチャー (DSA) に関係するすべての IBM Endpoint Manager サーバーがバージョン 9.1 であり、更新されたライセンスを保有していることが製品によって検証されるまで、チェック・ボックス「次の複製サーバー上で BESAdmin を実行してください」にチェック・マークは付きません。

4. IBM Endpoint Manager バージョン 9.1 で提供されるセキュリティー機能拡張を使用する場合は、「今すぐライセンスを収集する (Gather license now)」をクリックします。クリックしない場合は、IBM Endpoint Manager バージョン 9.0 によって提供されるセキュリティー動作を使用することになります。

「今すぐライセンスを収集する (Gather license now)」をクリックすると、更新されたライセンスが IBM サイトから収集され、IBM Endpoint Manager クライアントに配布されます。このステップを実行することにより、インストール・ステップ中に既存のライセンス・ファイルを指定した場合に、更新されたライセンス認証が確実に使用されます。



5. 3 つのチェック・マークが緑色の場合は、「**拡張セキュリティーを有効にする**」をクリックして、拡張セキュリティーを設定できます。



6. SHA-256 アルゴリズムを使用してダウンロードした後もデータが変更されていないようにするには、「**拡張セキュリティーを有効にする**」をクリックします。このオプションを選択しない場合、ダウンロードされたファイルの整合性チェックは SHA-1 アルゴリズムを使用して実行されます。

注: 「**拡張セキュリティーを有効にする**」オプションを有効にした場合にのみ、「**SHA-256 ダウンロードが必要 (Require SHA-256 Downloads)**」オプションを有効にすることができます。

マストヘッ드의作成方法または編集方法に関する追加情報については、48 ページの『ステップ 2 - ライセンス証明書の要求とマストヘッ드의作成』または「構成ガイド」を参照してください。

Linux システムの場合

Endpoint Manager V9.1 をインストールしてから（または V9.1 にアップグレードしてから）セキュリティー・オプションを設定するには、スーパーユーザーとして以下のコマンドを実行します。

```
./BESAdmin.sh -securitysettings -sitePvkLocation=<ath+license.pvk>  
-enableEnhancedSecurity -requireSHA256Downloads
```

./BESAdmin.sh -securitysettings の完全な構文は以下のとおりです。

```
./BESAdmin.sh -securitysettings -sitePvkLocation=<path+license.pvk>  
[-sitePvkPassword=<password>]  
{ -status | {-enableEnhancedSecurity|-disableEnhancedSecurity}  
| {-requireSHA256Downloads|-allowSHA1Downloads} }
```

指定の内容は以下のとおりです。

status IBM Endpoint Manager 環境のセキュリティー設定のステータスを示します。

例:

```
BESAdmin.sh -securitysettings -sitePvkLocation=/root/backup/license.pvk  
-sitePvkPassword=mypassw0rd -status
```

```
Enhanced security is currently ENABLED  
SHA-256 downloads are currently OPTIONAL
```

enableEnhancedSecurity | disableEnhancedSecurity

すべてのデジタル署名とコンテンツ検証に SHA-256 暗号ダイジェスト・アルゴリズムが採用され、Endpoint Manager コンポーネント間通信に TLS 1.2 プロトコルが採用される、拡張セキュリティーを有効または無効にします。

注: この設定を使用する場合、IBM Endpoint Manager バージョン 9.0 以前のコンポーネントは IBM Endpoint Manager バージョン 9.1 のサーバーやリレーと通信できないため、後方互換性が失われます。

requireSHA256Downloads

SHA-256 アルゴリズムを使用してダウンロードした後もデータが変更されていないようにします。

注: **requireSHA256Downloads** の設定は、**enableEnhancedSecurity** も設定した場合にのみ可能です。

allowSHA1Downloads

必ず SHA-1 アルゴリズムを使用してファイル・ダウンロードの整合性チェックが実行されるようにします。

第 5 章 インストールのタイプ

製品をインストールする前に、評価版インストールと正規版インストールのどちらを行うかを決定してください。

評価版インストールを選択する場合は、30 日間の試用版 Endpoint Manager サーバーをインストールすることになるため、ライセンスを購入する必要はありません。

正規版インストールを選択する場合は、ライセンスを購入する必要があります。IBM Endpoint Manager のライセンス認証ファイルを受け取ったら、個別設定されたアクション・サイト・マストヘッドを作成することができます。これにより、IBM Endpoint Manager をインストールして使用できるようになります。

マストヘッドには、サーバー CGI プログラムの URL、および署名済み MIME ファイル内のその他のサイト情報が含まれます。マストヘッドは、アクション・サイトへのアクセスおよび認証の中心となるものであり、サーバー・マシンのホスト名または IP アドレスにリンクされます。

評価インストール

評価版インストールを選択する場合は、30 日間の試用版 Endpoint Manager サーバーをインストールすることになるため、IBM からライセンス・ファイルを購入する必要はありません。

このタイプのインストール中には、自動的に評価ライセンスの要求が送信され、そのライセンスを使用してインストールが完了します。評価版インストールを行うには、インストールを実行している Linux システムがインターネットに（直接またはプロキシ経由で）接続できる必要があります。

このインストールでは、すべての構成パラメーターに事前定義値を使用します。構成できるパラメーターは以下のものに限られます。

- サーバー ID ポート番号 (デフォルトは 52311)
- Web レポート・サーバーのポート (デフォルトは 80)

評価版インストールを行うと、IBM Endpoint Manager コンソールと IBM Endpoint Manager Web レポートの両方にログオンするための EvaluationUser というユーザーが作成されます。

注: 評価版のインストールでは、拡張セキュリティー・オプションがサポートされません。この機能について詳しくは、27 ページの『第 4 章 セキュリティー構成シナリオ』を参照してください。

正規版インストール

IBM Endpoint Manager の正規版コピーをインストールするには、最初に、IBM または許可された販売店からライセンスを購入する必要があります。

所有しているライセンス入力ファイルに応じて、インストール中に以下の 3 種類のセットアップを選択できます。

```
I want to install with a BES license authorization file  
I want to install with a Production license that I already have  
I want to install with an existing masthead
```

BES ライセンス認証ファイル

IBM からライセンスを購入した後、IBM Endpoint Manager ライセンス認証ファイルを受け取ります。正規版インストールを初めて実行するときには、このファイルを使用する必要があります。ライセンスをまだ購入していない場合は、IBM Endpoint Manager の Web サイト (<http://www-01.ibm.com/software/tivoli/solutions/endpoint>) にアクセスしてください。

販売代理店は、インストールしようとするクライアントの数を知りたいと考えます。この数に基づいて、代理店は**ライセンス認証ファイル** (CompanyName.BESLicenseAuthorization などのファイル名) を作成して署名し、電子メールで送信します。

このインストールの実行時にインターネットにアクセスしていない場合は、IBM Endpoint Manager ライセンス・サーバーからの正規版ライセンス (license.crt) および license.pvk プライベート・キー・ファイルを要求するための一時要求 (beslicense.request) が生成されます。正規版ライセンスを取得するまでは、インストールを保留状態にしておくことができます。

インターネットにアクセスできるマシン上に request.BESLicenseRequest という要求をコピーし、IBM Endpoint Manager Web サイトにアクセスしてこの要求を送信し、自分の証明書をダウンロードしてください。証明書をダウンロードしたら、サーバーをインストールするマシンにその証明書をコピーして、インストールを続行してください。インストールを途中で終了した場合に、後でサーバーをインストールするには、既存の**正規版ライセンス・ファイル**を要求するオプションを使用してインストールを実行する必要があります。

注: 選択した DNS/IP アドレスは、適用環境のうちで永続的な部分となり、変わることはありません。柔軟性を持たせるために、固定 IP アドレスではなく、DNS 名を使用することを強くお勧めします。

インストール・プログラムは、適用環境に関する詳細な情報を収集してから、デジタル署名キー license.pvk と、アクション・サイト・マストヘッドと呼ばれるファイルを作成します。このファイルは、構成情報 (IP アドレスやポートなど) とライセンス情報 (許可されるクライアントの数と許可される期間) を、デジタル署名の検証に使用されるパブリック・キーと共に結合したものです。

正規版ライセンス

サーバーをインストールするマシン上に正規版ライセンスの license.crt とプライベート・キー・ファイルが既に存在するが、サーバー・インストールが完了していない場合は、このオプションを使用します。

既存のマストヘッド

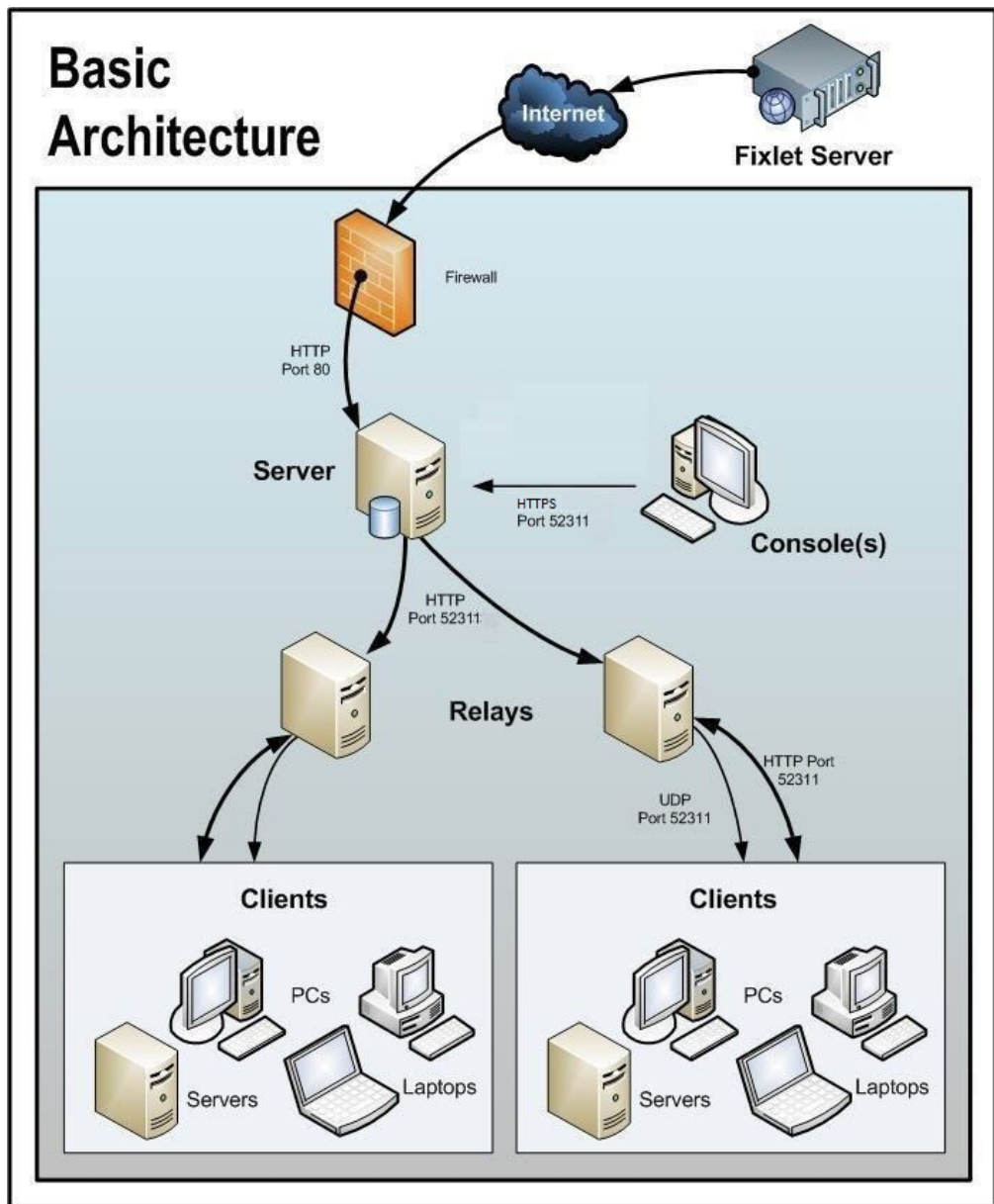
Endpoint Manager サーバーまたは DSA サーバーを再インストールする場合には、このタイプのインストールを使用します。このインストールを実行するために必要な入力ファイルは、最初のインストール時に生成されたアクション・サイト・マストヘッド・ファイルです。アクション・サイト・マス

トヘッドには、拡張子 .afxm が付いています。これは、Endpoint Manager サーバーの IP アドレスまたはサーバー名、ポート番号、ロック動作などのパラメーターが含まれる構成ファイルとして機能します。ここには、Endpoint Manager が使用するデジタル署名セキュリティ機構に必要な情報（マストヘッドに公開鍵が含まれる）が格納されます。これは、指定された数の Endpoint Manager ユーザーに対して、指定された期間だけ Endpoint Manager の実行を許可するためのライセンス情報です。Endpoint Manager サーバーのインストーラーを実行するには、マストヘッド・ファイルがサーバーのインストール・フォルダーに格納されている必要があります。

正規版をインストールすると、IBM Endpoint Manager コンソールと IBM Endpoint Manager Web レポートにログオンするためのユーザー（デフォルト名は IEMAdmin）が作成されます。

基本インストール

IBM Endpoint Manager の簡単な適用環境を以下の図に示します。インターネットから Fixlet を収集するサーバーが少なくとも 1 つあります。そのサーバーでは、メッセージをコンソール・オペレーターに対して表示し、リレーに分配することができます。各クライアントは、自分のローカル・コンピューター環境を調べて、適用対象の Fixlet があればそれをリレーに折り返しレポートします。



このウィンドウには基本的なインストール済み環境が表示されています。IBM Endpoint Manager の簡単な適用環境を以下の図に示します。インターネットから Fixlet を収集するサーバーが少なくとも 1 つあります。そのサーバーでは、メッセージをコンソール・オペレーターに対して表示し、リレーに分配することができます。各クライアントは、自分のローカル・コンピューター環境を調べて、適用対象の Fixlet があればそれをリレーに折り返しレポートします。

IBM Endpoint Manager コンソールは、このすべてのアクティビティを監視します。サーバーに接続し、表示を定期的に更新して、ネットワークに関する変更または新しい情報を反映させます。

これにより、IBM Endpoint Manager コンソール・オペレーターは、アクションを適切なコンピューターに振り向けて、脆弱性の修正、構成ポリシーの適用、ソフトウェアのインストールなどを行います。アクションがすべての関連コンピューターに

広がり、それらの重大な問題に 1 つずつ対処しているときに、その進行状況を、ほぼリアルタイムで追跡することができます。

この図では、IBM Endpoint Manager が使用するすべてのデフォルト・ポートにはラベルが付けられているため、どのポートをどこで開く必要があるかを確認することができます。これらのポートは、競合を避けるように選択されましたが、これらのポートのいずれかを現在使用している場合は、インストール時にカスタマイズすることができます。

注: 図中の矢印は、企業全体での情報のフローを示します。Fixlet サーバーからサーバーへの矢印は、ユーザーのネットワークへの Fixlet のフローを表します。クライアントは、リレーから Fixlet およびアクション情報を収集します。次に、少量の情報を、リレーを通じてサーバーに送り返します。リレーからクライアントへの UDP パケットは、収集すべき新しい情報があることを通知するために各クライアントに送信される小規模なパケットです。UDP メッセージは、IBM Endpoint Manager が正しく機能するために絶対に必要というわけではありません。詳細については、IBM Endpoint Manager サポート・サイトのネットワーク・トラフィックに関する記事を参照するか、またはサポート技術者に問い合わせてください。

標準インストール

前述の基本インストールでは、IBM Endpoint Manager ネットワークを確立するために必要な特定のポートの多くが示されていますが、多くの適用環境で重要となる DMZ および直接接続という 2 つの側面については示されていません。DMZ の例では、VPN によって接続されたオフィスは、リレーまたはサーバーからのコンテンツを共有できます。直接接続では、専用のプライベート・ファイアウォールを通じて Fixlet サーバーのコンテンツにアクセスするために、ホーム PC およびラップトップをインターネットに直接接続できます。分かりやすくするため、それらの追加的な接続が示されていない図もありますが、通常は、ほとんどの適用環境に存在します。

複数のサーバーのインストール

IBM Endpoint Manager には、複数の完全冗長サーバーを追加するという重要な機能が含まれています。これは、分散サーバー・アーキテクチャー (DSA) と呼ばれる機能です。各サーバーは IBM Endpoint Manager データベースのレプリカを保持し、世界中のどこにでも配置できます。ネットワークの分断が発生しても、これらのサーバーは、ローカル・ネットワークに対して中断することなくサービスを提供し続けます。接続が再び確立されると、サーバーは直ちに自動的に再接続して同期されます。IBM Endpoint Manager のリレーおよびクライアントも、このような切断から正常に復旧することができます。DSA によって以下の機能が提供されます。

- 分断されたネットワークの両側での継続的なサービス可用性 (自動フェイルオーバー)
- サーバーの停止が発生した場合の継続的な可用性
- 通常動作時におけるコンソール・データベースの負荷の分散
- 再接続時の自動フェイルバック

この機能を利用するには、少なくとも 1 次サーバーと同等の機能を持つ、1 つ以上の追加のサーバーが必要です。適用環境内のすべての IBM Endpoint Manager サーバーが、同じバージョンの SQL Server を実行する必要があります。既存のサーバーが SQL 2005 を実行している場合、新しいサーバーも SQL 2005 を実行する必要があります。

サーバーの冗長性の使用について詳しくは、「構成ガイド」を参照してください。

第 6 章 ライセンスの管理

IBM Endpoint Manager をインストールして使用する前に、ライセンス・キーを取得する必要があります。ライセンスは、以下の 2 つのファイルで構成されています。

- パブリック・キー・ファイル: license.crt
- プライベート・キー・ファイル: license.pvk (パスワードで保護されています)

以下の表には、ライセンス・キーの購入、生成、および管理に必要なタスクが一覧表示されています。

タスク	説明
製品のライセンス要件を確認する	保護するシステムのライセンス要件を把握することは重要です。ライセンスを使用して、指定された数のコンピューターに Endpoint Manager クライアントをインストールできます。
ライセンスを購入する	以下の場合、ライセンスを購入する必要があります。 • Endpoint Manager を購入する場合。 • 試用ライセンスの有効期限が切れた場合。 • 支払い済みのライセンスの有効期限が切れた場合。 • ライセンスが超過適用されており、さらにライセンスを購入するために、更新された license.crt が必要な場合。 • アップグレード・ライセンスの有効期限が切れた場合。 購入後、数時間の間に 2 通の電子メールを受け取ります。1 通は購入を確認するために IBM から送信されるものです。もう 1 通の電子メールには、IBM Endpoint Manager License Key Center へのアクセス方法に関する説明が記載されています。これらの電子メールは、アカウントの IBM カスタマー番号に関連付けられた技術担当者に送信されます。
ライセンス認証ファイルを取得する	製品ライセンスを取得するには、IBM Endpoint Manager License Key Center のサイトから認証ファイル入手する必要があります。39 ページの『ライセンス認証ファイルの作成』を参照してください。

インストール中にライセンス・ファイルを生成するには、以下の手順を実行します。 ・ プライベート・キー・ファイルを作成します ・ ライセンス証明書を要求して取得します ・ マストヘッド・ファイルを生成します	サーバーのインストール中に、ライセンス認証ファイルを指定した後、プライベート・キー・ファイルである <code>license.pvk</code> ファイルを生成します。パブリック・キー・ファイルである <code>license.crt</code> ファイルも要求して取得します。これらの 2 つのファイルを共に使用して、ライセンス取得を完了します。 Windows でのライセンス・ファイルの要求方法と『ステップ 2 - サーバーのインストール』を参照してください。
ライセンス・ファイルをバックアップする	<code>license.crt</code> (パブリック・キー) ファイルを既存の <code>license.pvk</code> (プライベート・キー) ファイルとともに保存します。これらの 2 つのキーは一緒に保存し、安全な場所にバックアップ・コピーを作成してください。これが、ライセンス・キーを完全に制御するための唯一の方法です。ライセンス・ファイルをバックアップすると、データベースまたはコンピューターのハード・ディスクが損傷した場合に、ライセンス・ファイルが保持されません。 特に、<code>license.pvk</code> ファイルはキー・ファイルの一部であり、保護された状態に保っておく必要があります。<code>license.crt</code> ファイルはパブリック・キー・ファイルであり、ライセンス取得を完了するには、プライベート・キー・ファイルと組み合わせる必要があります。テキスト・エディターでライセンス・ファイルを開き、その内容を確認することができます。
ライセンスのステータスを確認し、新しいライセンス・ファイルおよびマストヘッド・ファイルを配布する	コンソールにインポートしたライセンスに関するライセンスの期限切れや他のライセンス問題についての通知を確認できます。 40 ページの『更新されたライセンスとマストヘッドの配布』を参照してください。

ライセンス・キー・ファイルを取得する手順を簡単に説明します。

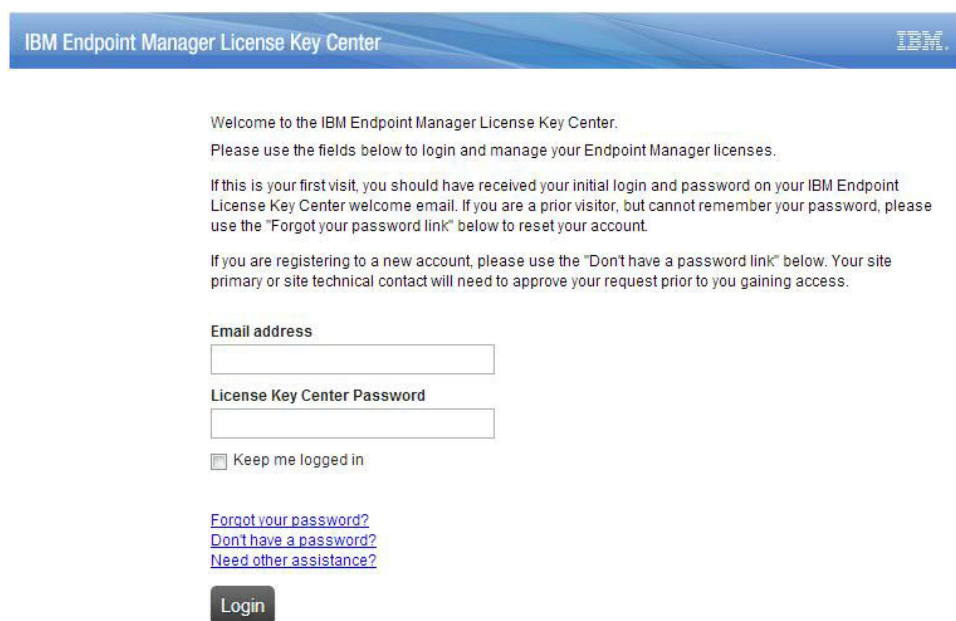
1. ライセンスを購入します。
2. IBM Endpoint Manager License Key Center のサイトから、認証ファイルを入手します。
3. Endpoint Manager のインストールを開始し、`license.crt` ファイルの取得を要求されたら、認証ファイルを入力します。プロセスの最後に、パブリック・キーとプライベート・キーの両方のライセンス・ファイルが、マストヘッド・ファイルとともに生成されます。このファイルには、信頼された Fixlet コンテンツを取得できる場所を指す URL を含む、構成、ライセンス、およびセキュリティ情報が含まれています。このファイルは DSA サーバーのインストールに使用され、そのサーバーを使用するすべてのクライアントに配布されます。

ライセンス認証ファイルの作成

適用環境情報とライセンス情報を持ち、ライセンス・ファイルを作成するためにインストール時に使用されるライセンス認証ファイル (.BESLicenseAuthorization) を作成するには、IBM Endpoint Manager License Key Center にアクセスしてください。このサイトはオンラインでライセンス・キーの配信および管理サービスを提供します。このサイトから、製品を使用するために必要なライセンス・キーを取得して、管理できます。

認証ファイルを作成するには、以下の手順を実行します。

1. 次のリンクにアクセスします: <http://tem.subscribenet.com/>
2. 自分の電子メール・アドレスを入力し、Tivoli Endpoint Manager License Key Center へのアクセス方法の説明と一緒に受け取ったパスワードを入力してください。



The screenshot shows the login interface of the IBM Endpoint Manager License Key Center. At the top, there is a blue header bar with the text "IBM Endpoint Manager License Key Center" and the IBM logo. Below the header, the page contains the following text:

Welcome to the IBM Endpoint Manager License Key Center.
Please use the fields below to login and manage your Endpoint Manager licenses.

If this is your first visit, you should have received your initial login and password on your IBM Endpoint License Key Center welcome email. If you are a prior visitor, but cannot remember your password, please use the "Forgot your password link" below to reset your account.

If you are registering to a new account, please use the "Don't have a password link" below. Your site primary or site technical contact will need to approve your request prior to you gaining access.

Below the text, there are two input fields: "Email address" and "License Key Center Password". Under these fields is a checkbox labeled "Keep me logged in". At the bottom, there are three links: "Forgot your password?", "Don't have a password?", and "Need other assistance?". A "Login" button is located at the bottom center.

3. 製品ごとに、割り当てられたクライアント数を指定します。これを 0 のままにすると、関連製品をインストールできません。

Product	Allocated Quantity	Available Quantity
Core Protection Module (Trend) (*) (Client Device) Order Date: Jul 22, 2011 License Expiration: December 30, 2021 Maintenance Expiration: Dec 30, 2021	0	817040
Core Protection Module (Trend) (*) (Client Device) Order Date: Aug 24, 2011 License Expiration: December 31, 2037 Maintenance Expiration: Dec 31, 2037	50000	6124989
Lifecycle Management (Client Device) Order Date: Jul 22, 2011 License Expiration: December 30, 2023 Maintenance Expiration: Dec 30, 2023	0	776570
Lifecycle Management (Client Device) Order Date: Aug 24, 2011 License Expiration: December 31, 2037 Maintenance Expiration: Dec 31, 2037	50000	5520016
Lifecycle Management (Client Device) Order Date: Jan 25, 2012 License Expiration: Does not expire. Maintenance Expiration: Jan 25, 2099	0	659385
Lifecycle Management (Client Device) Order Date: Aug 31, 2012 License Expiration: Does not expire. Maintenance Expiration: Aug 31, 2013	0	2475
Mobile Device Management (Client Device) Order Date: Mar 29, 2012 License Expiration: Does not expire. Maintenance Expiration: Mar 29, 2013	0	8848
Mobile Device Management Beta (Client Device) Order Date: Jan 25, 2012 License Expiration: Does not expire. Maintenance Expiration: Jan 25, 2099	0	684057
OtherSitesAllowed (Client Device) Order Date: Aug 24, 2011	50000	5373793

ライセンス交付支援

ライセンスの有効期限、資格数、または認証ファイルの紛失など、ライセンスに関する具体的な問題については、IBM Endpoint Manager ライセンス・チーム (TEM@dk.ibm.com) にお問い合わせください。一般的なインストールに関する問題、セットアップ構成、適用環境に関する質問など、ライセンスに関係のないサポート関連の質問については、このアドレスに送信するのではなく、通常のサポート窓口か販売リソース・チャネルに問い合わせてください。

更新されたライセンスとマストヘッドの配布

Endpoint Manager を V9.1 にアップグレードすると、既存のライセンス証明書がすべて更新されて SHA-1 署名と SHA-256 署名の両方を含むようになります。インターネットに接続している場合は、定期的な自動収集または手動での確認後に、新しいライセンスがマストヘッドとともにクライアントに配布できる状態にあることを通知するメッセージが「**ライセンスの概要**」ダッシュボードに表示されます。

今すぐにサーバーを確認させるには、以下の手順を実行します。

1. Endpoint Manager コンソールを開きます。
2. 「BigFix 管理」ドメインに移動します。
3. 「ライセンスの概要」ノードをクリックします。

4. 「ライセンスの更新を確認」をクリックします。Endpoint Manager 適用環境によってライセンスに対する更新 (新しい license.crt ファイル) が収集されたという通知を受け取ることがあります。

BigFix License Overview

Last Update: 2/27/2014 1:21:57 PM

For questions about the products listed on your license or their expiration dates please email TEM@dk.ibm.com. You can also manage your license at the [TEM License Key Center](#).

▼ BES Platform

The server has gathered a new version of your platform license, but it has not yet been distributed to clients. The site administrator must log into Tivoli Endpoint Manager Administration Tool to propagate a new masthead with the updated license.

Serial Number:

Organization:

Start Date:

Gather URL:

Check for license update

Update Status:

2/13/2014 12:44:45 PM

<http://nc125145.romelab.it.ibm.com:52311/cgi-bin/bfgather.exe/actionsite>

Site certificate update detected, BESAdmin must be run to propagate the change.

注: このメッセージが表示される理由としては、IBM がライセンスを更新する必要があるか、または、お客様がライセンスの更新を要求したことが考えられます。お客様がライセンスの更新を要求した場合は、サーバー・コンピュータに保存する必要がある新規 license.crt ファイルを受け取ります。

更新されたライセンスを配布し、SHA-1 署名と SHA-256 署名の両方を使用してマストヘッドとデータベース内のオブジェクトに再署名するには、スーパーユーザーとして管理ツール (Linux 上の ./BESAdmin.sh) を実行します。

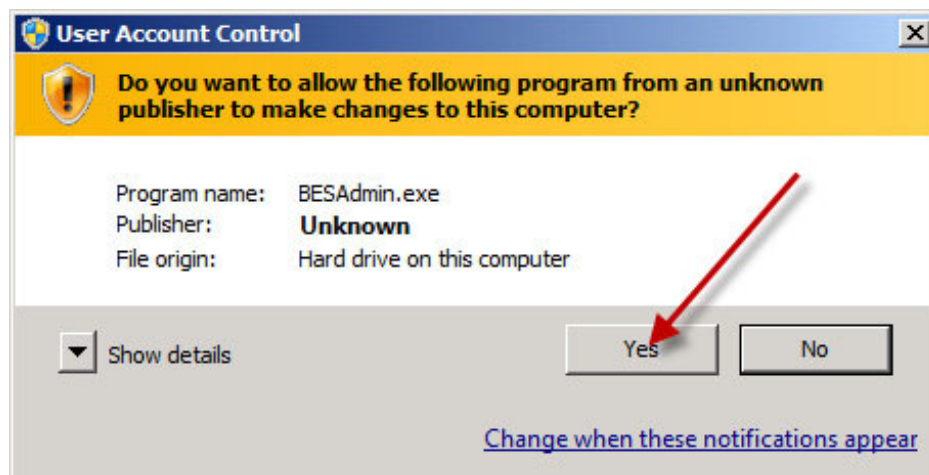
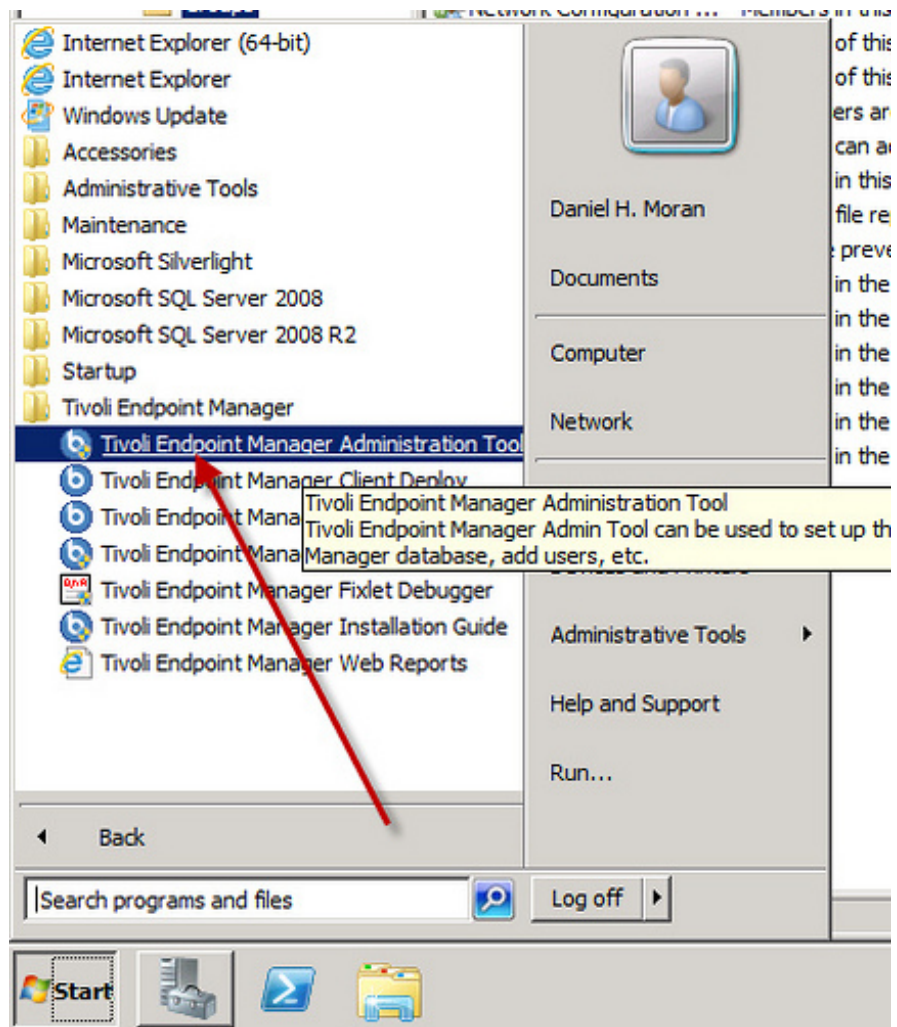
エア・ギャップ環境の場合、ライセンスの更新は自動的に処理されません。AirgapTool ユーティリティを使用して、IBM サイトからライセンスを取得できます。ライセンスをインポートすると、ライセンス更新が配布できる状態にあることがライセンス・ダッシュボードで通知されます。管理ツール (Linux 上の ./BESAdmin.sh) を実行して、更新されたライセンスを配布し、マストヘッドとデータベース・オブジェクトに再署名する必要があります。

マストヘッドをクライアントに配布する方法については、『Windows サーバーからクライアントへのマストヘッドの配布』および 44 ページの『Linux サーバーからクライアントへのマストヘッドの配布』を参照してください。

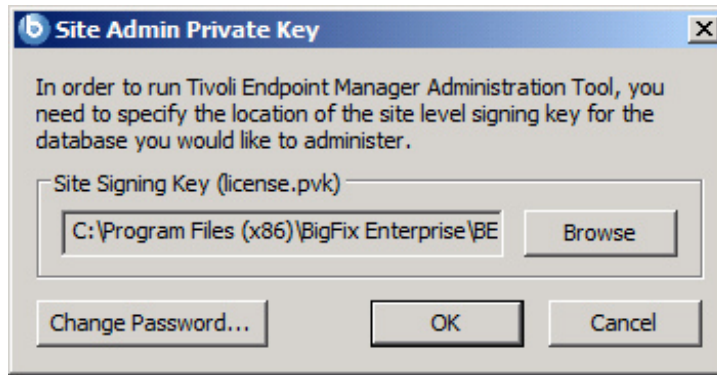
Windows サーバーからクライアントへのマストヘッドの配布

ライセンス、シート数、または資格を拡張する、更新されたライセンス証明書を含む新しいマストヘッド・ファイルを、Endpoint Manager Windows サーバーからクライアントに以下のように配布できます。

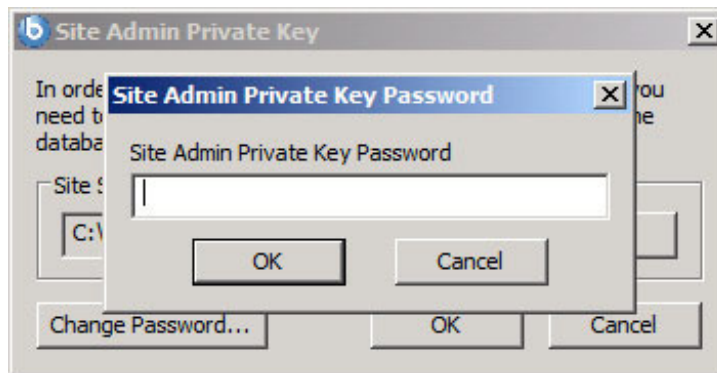
1. 「スタート」>「すべてのプログラム」>「IBM Endpoint Manager」>「IBM Endpoint Manager 管理ツール」を選択して管理ツールを開きます。ログインすると、インストール用の管理アカウントによって、マストヘッドがクライアントに配布されます。



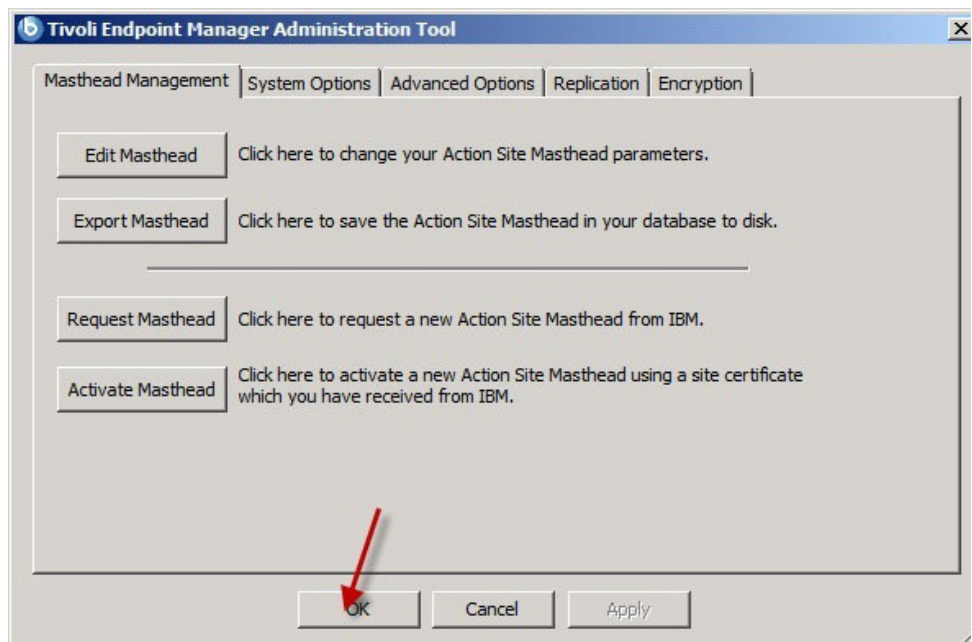
2. license.pvk ファイルを選択します。



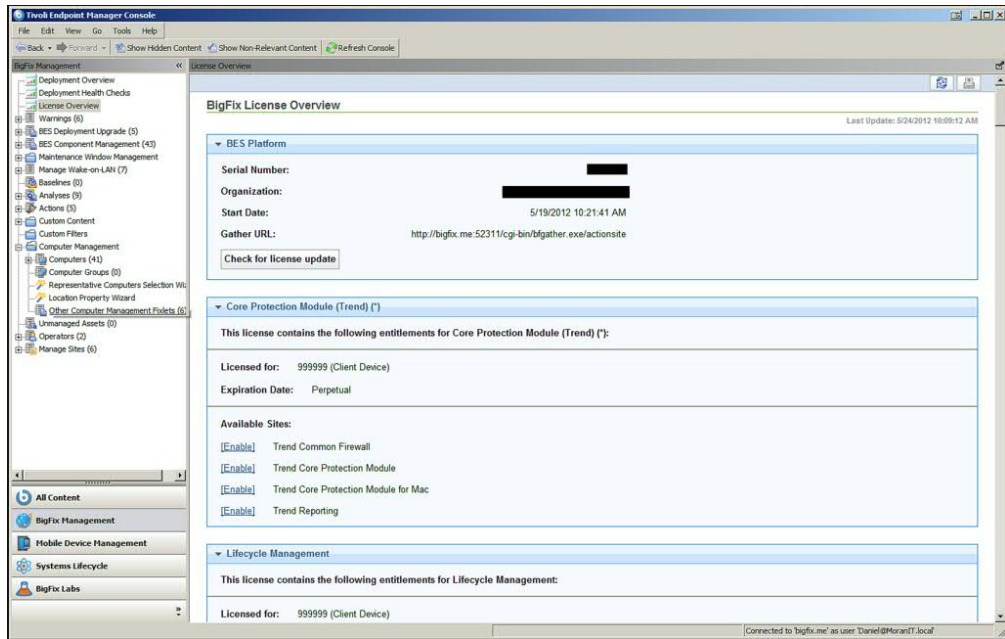
3. マスター (サイト・レベル) パスワードを入力します。



4. 「マストヘッドの管理」で、「OK」をクリックします。



クライアントが新しいマストヘッドを受け取るとすぐに、更新されたライセンス情報を受け取ります。



Linux サーバーからクライアントへのマストヘッドの配布

Endpoint Manager Linux サーバーからクライアントに対して、更新されたライセンスを配布し、マストヘッドとデータベース・オブジェクトに再署名するには、スーパーユーザーとして以下のコマンドを実行します。

```
./BESAdmin.sh -syncmastheadandlicense -sitePvkLocation=<path+license.pvk>
-sitePvkPassword=<password>
```

第 7 章 インストールを実行する前に

インストールを実行する前に以下のトピックを読み、必要な作業を行ってください。

ローカル・ファイアウォールの構成

Endpoint Manager サーバーをインストールするコンピューター上にアクティブなファイアウォールを定義した場合は、次のいずれかの方法で、Endpoint Manager サーバーのインストール中にこのファイアウォールを構成することを決定できます。

- 対話式インストール中に、ローカル・ファイアウォールがアクティブかどうかをインストール・プログラムによって検出され、このファイアウォールを Endpoint Manager サーバー用に構成するかどうかを指定できます。
- サイレント・インストール中に、ファイアウォールの構成を要求するように `CONF_FIREWALL=YES` を応答ファイル内に設定できます。詳細については、103 ページの『サイレント・インストール』を参照してください。

ファイアウォールを構成するように指定すると、次の 2 つのポートが開きます。

- UDP および TCP/IP 用のポート 52311
- Web レポートおよび TCP/IP 用のポート 80

ポート番号の変更

デフォルトでは、サーバーはポート **52311** を使用してクライアントと通信しますが、任意のポート番号を選択することができます (ただし、予約ポート 1 から 1024 は使用しないでください。これは、ポートの競合が発生する可能性があるという理由と、ネットワーク・トラフィックの管理が困難になるという理由のためです)。

サーバーのポート番号の選択は、アクション、登録、レポート、およびミラー・サーバーの URL を指定するマストヘッドの生成の要素となります。したがって、インストールの前 にポート番号を決定する必要があります。

コンソールは、ポート **52311** を使用してサーバーに接続します。

第 8 章 Windows システムでのインストール

用語と管理役割について理解すると、許可を受けて、プログラムをインストールする準備が整います。

IBM Endpoint Manager が強力であるため、アクセスを、信頼できる許可されたスタッフのみに制限したいと考えます。この製品は、「アクション・サイト」と呼ばれる Fixlet アクションの中央リポジトリに依存します。このリポジトリは、パブリック・キー/プライベート・キーの暗号化を使用して、スプーフィングなどの許可されていない使用法から保護します。開始するには、**ライセンス認証ファイル** (このファイルには `CompanyName.BESLicenseAuthorization` などの名前が付いています) を取得して、IBM から許可を受ける必要があります。

インストール・プログラムは、適用環境に関する詳細な情報を収集してから、**アクション・サイト・マストヘッド**と呼ばれるファイルを作成します。このファイルは、組織内の IBM Endpoint Manager の root からコンソール・オペレーターまでの権限のチェーンを設定します。マストヘッドは、構成情報 (IP アドレス、ポートなど) とライセンス情報 (許可されるクライアントの数および許可される期間) を、デジタル署名を確認するために使用されるパブリック・キーと共に結合したものです。デジタル署名キーおよびマストヘッドを作成して保守するために、**IBM Endpoint Manager インストーラー**を使用します。これは、IBM からダウンロードできます。

インストール手順

製品をインストールするには、以下の手順を実行します。

1. IBM Endpoint Manager をダウンロードします。
2. インストーラー・プログラムを使用して、ライセンスを要求し、マストヘッドを作成します。認証ファイルの指定を求めるプロンプトが表示されたら、License Key Center のアカウントを使用して作成したライセンス認証ファイル (`*.BESLicenseAuthorization`) を使用します。PoC (概念検証) 評価版の場合、このファイルは IBM の技術営業担当員によって提供されています。
3. IBM Endpoint Manager のインストールを実行します。

ステップ 1 - IBM Endpoint Manager のダウンロード

IBM のパスポート・アドバンテージ・ポータルから IBM Endpoint Manager をダウンロードします。

IBM Endpoint Manager は、サポート・サイト (<http://support.bigfix.com/bes/install/downloadbes.html>) または DeveloperWorks トライアル・サイト (<http://www.ibm.com/developerworks/downloads/tiv/endpoint/>) からダウンロードすることもできます。このデモンストレーション用のトライアル・インストーラーは、通常の正規版インストール用のものと同じインストーラー・プログラムです。

サーバー・コンポーネントをインストールするには、パスポート・アドバンテージから以下の e- イメージをダウンロードします。

表 1. Endpoint Manager サーバーのインストールに必要なソフトウェア

ソフトウェア名	パーツ番号	イメージ
IBM Endpoint Manager Platform Install V9.1 for Multiplatforms	CITM5ML	IBM Endpoint Manager 9.1.1065.0.zip

Endpoint Manager Windows サーバーのインストール・ファイルを抽出するには、以下の手順を実行します。

1. Endpoint Manager サーバーの zip ファイル IBM Endpoint Manager 9.1.1065.0.zip を Windows サーバーにコピーします。
2. 以下のコマンドを使用して、zip ファイルを展開します。
`unzip "IBM Endpoint Manager 9.1.1065.0.zip"`

IBM Endpoint Manager 9.1.1065.0 フォルダに Windows サーバーをインストールするための setup.exe ファイルがあります。

ステップ 2 - ライセンス証明書の要求とマストヘッドの作成

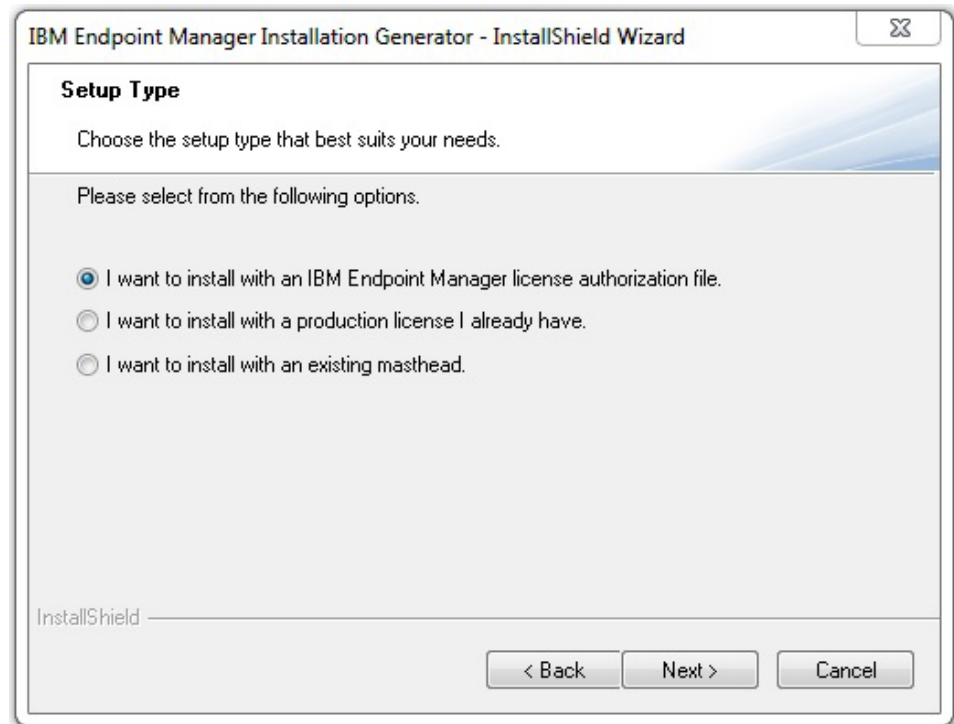
下記の手順を実行する前に、ライセンスを購入し、License Key Center のアカウントを使用して IBM Endpoint Manager ライセンス認証ファイル (*.BESLicenseAuthorization) を入手しておく必要があります。PoC (概念検証) 評価版の場合、このファイルは IBM の技術営業担当員によって提供されています。

ライセンス認証ファイルを手に入れたら、ライセンス証明書を要求した上で、個別設定されたサイト・マストヘッドを作成できます。これにより、IBM Endpoint Manager をインストールおよび使用することができます。マストヘッドには、サーバー CGI プログラムの URL、および署名済み MIME ファイル内のその他のサイト情報が含まれます。マストヘッドは、アクション・サイトへのアクセスおよび認証の中心となるものです。マストヘッドを作成し、サイトをアクティブにするには、以下の手順に従います。

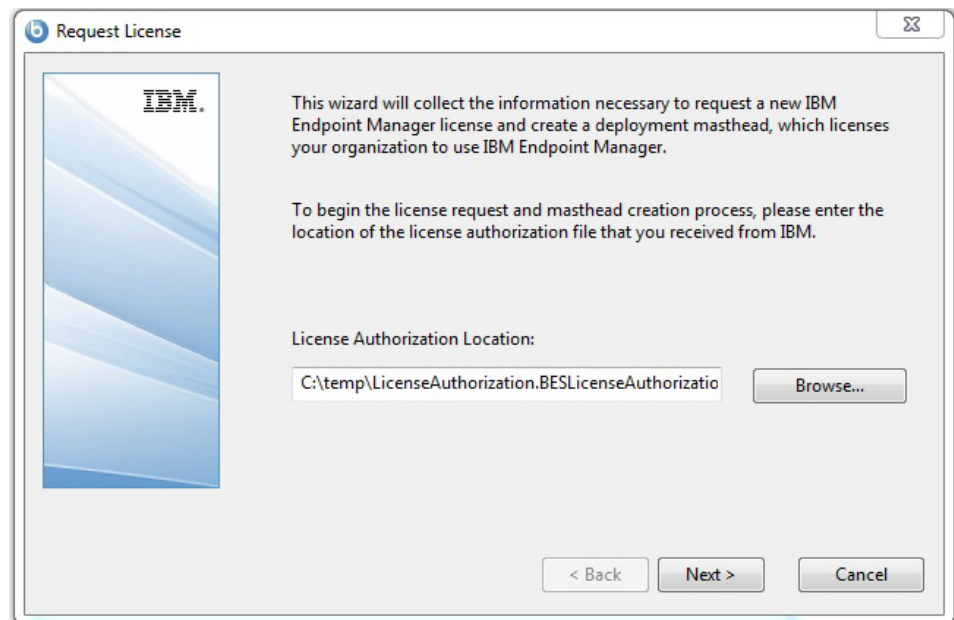
1. IBM Endpoint Manager インストーラー BigFix-BES-n.n.nnnn.n.exe を実行します。*n.n.nnnn.n* はインストーラーのバージョンです。プロンプトが表示されたら、「**正規版**」インストールを選択し、ソフトウェア使用許諾契約に同意します。初期画面で「**次へ**」をクリックします。

注: 「評価」のインストールを選択する場合は、そのタイプのインストールでは拡張セキュリティー・オプションがサポートされないことを念頭に置いてください。この機能について詳しくは、27 ページの『第 4 章 セキュリティー構成シナリオ』を参照してください。

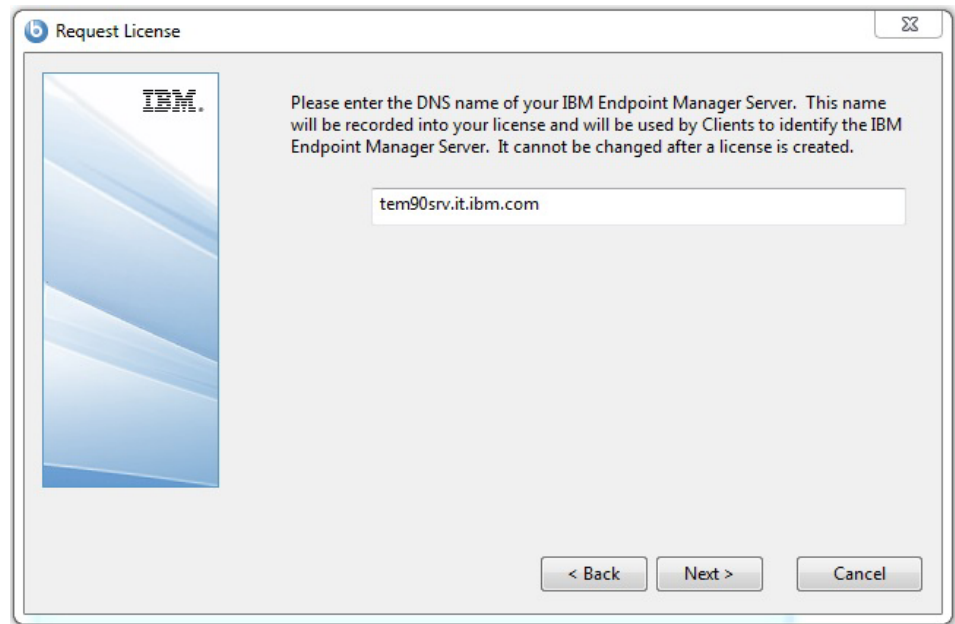
2. 使用許諾契約を読み、承諾したら、「**IBM Endpoint Manager ライセンス認証ファイルを使用してインストールします。**」を選択し、プライベート・キーとマストヘッドを作成します。



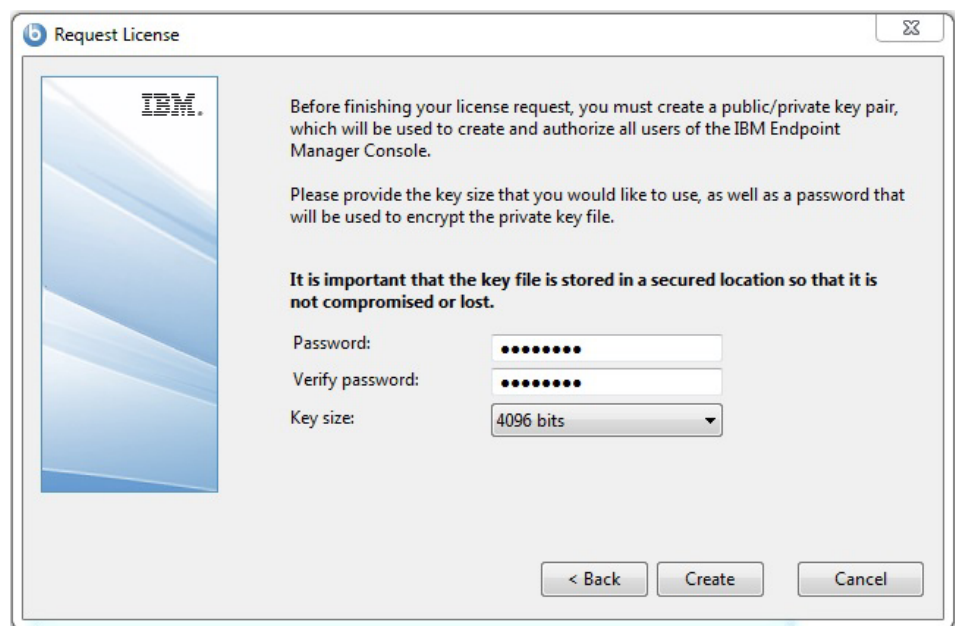
3. `CompanyName.BESLicenseAuthorization` のような名前が付いているライセンス認証ファイルの場所を入力します。



4. Endpoint Manager サーバーの「DNS 名」または「IP アドレス」を指定して、「次へ」をクリックします。



- 注: サーバー・コンピューターを変更したり、拡張ネットワーク構成を行ったりする場合の柔軟性を考慮して、bes.companyname.com などの DNS 名を入力します。この名前は、ライセンス証明書に記録され、クライアントによって Endpoint Manager サーバーを識別するために使用されます。ライセンス証明書を作成してからは、DNS 名を変更することはできません。DNS 名を変更する場合は、新しいライセンス証明書を要求する必要があります。そのためには、完全な新規インストールを行う必要があります。
5. サイトの資格情報のパスワードを入力すると、適用環境用のサイト管理キーを作成できるようになります。パスワードを (確認のために) 2 回入力し、プライベート・キー・ファイルを暗号化するためのキー・サイズ (2K ビットから 4K ビット) を指定します。「作成」をクリックします。

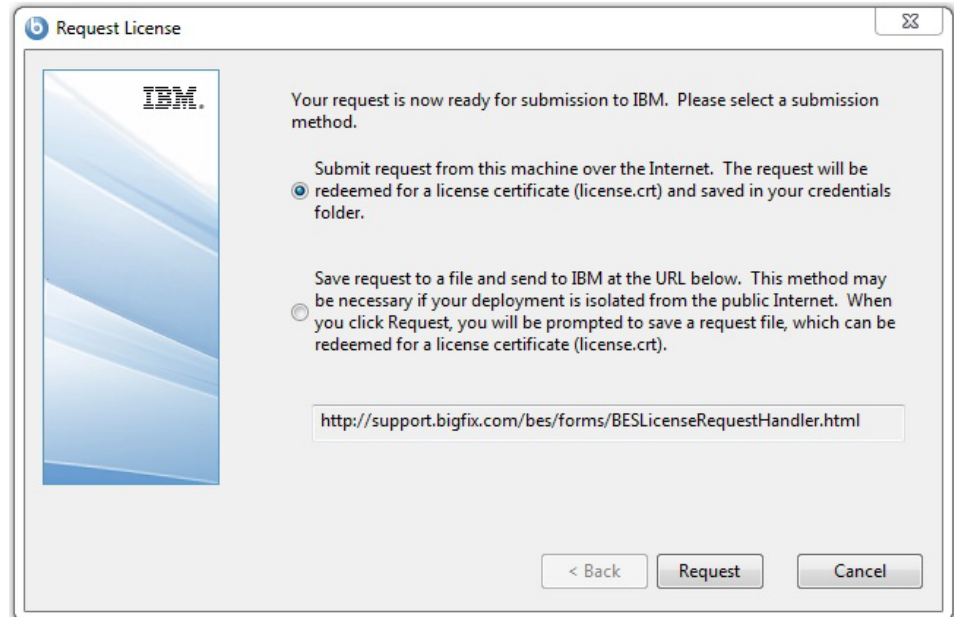


この方法で、すべての Endpoint Manager ユーザーの作成および許可に使用されるパブリック・キーとプライベート・キーのペアを生成します。

6. 「フォルダーの参照」ダイアログで、安全なアクセス許可が設定されたフォルダーまたはリムーバブル・ドライブ (PGPDisk や USB ドライブなど) にプライベート・キー (license.pvk) ファイルを保存します。「OK」をクリックします。

重要: プライベート・キー・ファイルを失った場合は、新しいライセンス証明書を作成する必要がありますが、これを行うには完全に新しいインストールを実行する必要があります。また、プライベート・キー・ファイルとパスワードを持つすべてのユーザーは、IBM Endpoint Manager クライアントがインストールされているすべてのコンピューターに対する完全な制御ができるようになっているため、管理者は、プライベート・キー・ファイルとパスワードが保護されているようにしておく必要があります。

7. インターネット接続がある場合、インターネット経由で IBM に要求を送信することもできます。



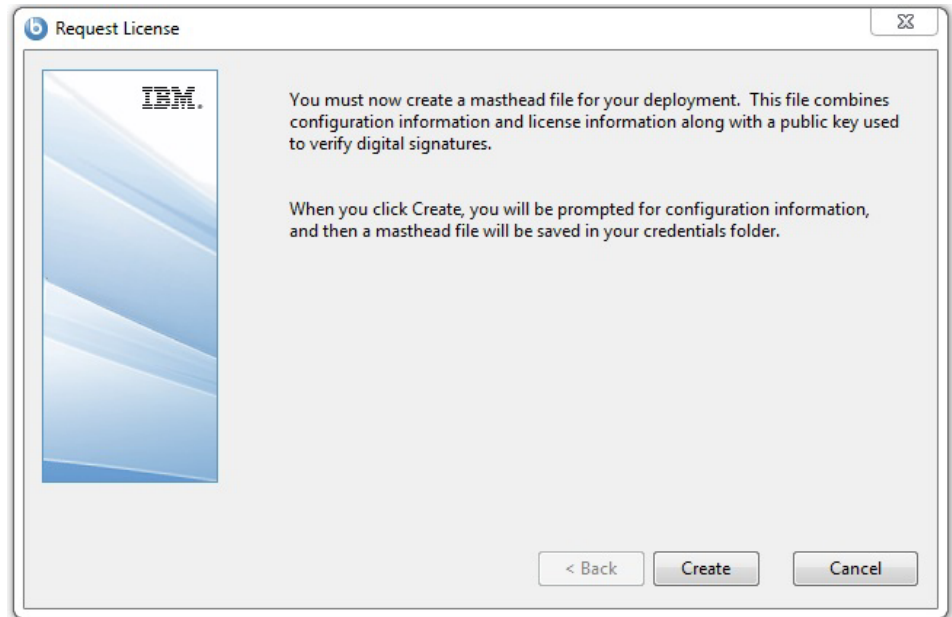
結果として得られるライセンス証明書ファイル (license.crt) を保存するための場所を指定するよう、プロンプトが出されます。また、要求ファイルはライセンス検証のため IBM Endpoint Manager に送信されます。通常は、最初の選択項目 (要求の送信) を選択して、インターネットを通じて要求を送ります。この要求は、元の認証ファイル、サーバー DNS 名、およびパブリック・キーで構成されており、すべて単一のファイルにパッケージ化されます。

8. 「要求」をクリックします。ウィザードは、IBM Endpoint Manager ライセンス・サーバーからライセンス証明書 (license.crt) を取得します。

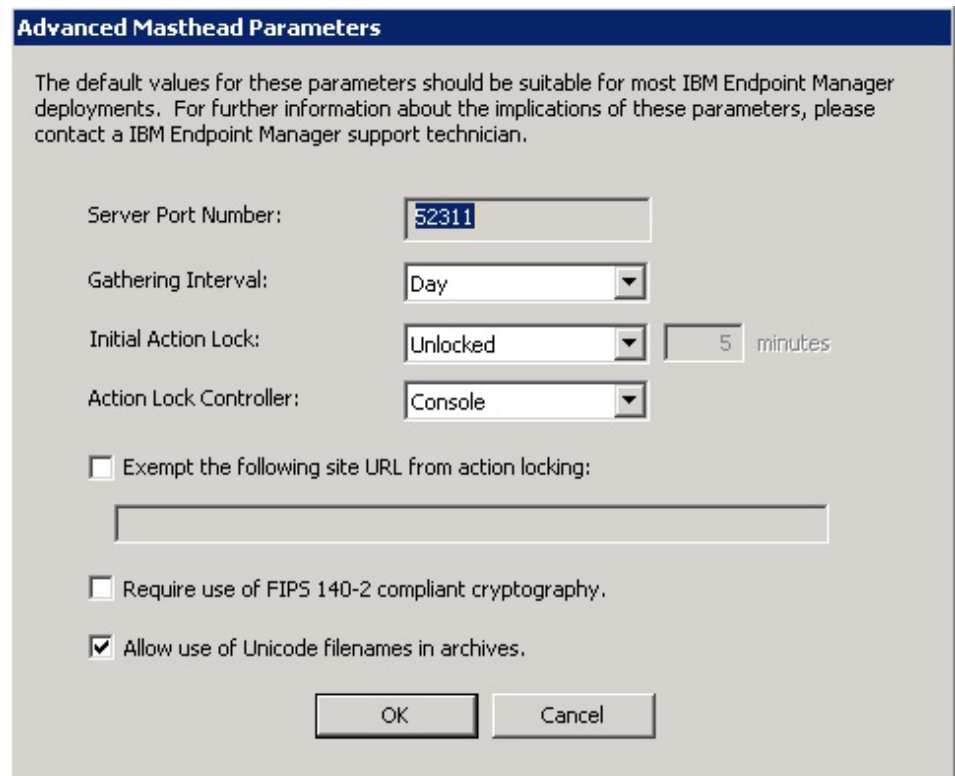
あるいは、インターネット接続がないエアギャップにいる場合、request.BESLicenseRequest という名前のファイルとして要求を保存するオプションを選択します。インターネット接続を使用してファイルをマシンにコピーし、インストーラーに表示される Endpoint Manager の Web サイトの URL

に要求を送信します。表示されるページで `license.crt` ファイルを取得できます。このファイルをインストール・コンピューターにコピーし直して、インストーラーにインポートします。

9. 「ライセンス要求」ダイアログで「作成」をクリックして、マストヘッド・ファイルを作成します。



10. デジタル署名を確認するために使用されるパブリック・キーとともに構成およびライセンスの情報が含まれる、マストヘッド・ファイルのパラメーターを入力します。このファイルは資格情報フォルダーに保存されます。

A screenshot of the 'Advanced Masthead Parameters' dialog box. The title bar is dark blue with the text 'Advanced Masthead Parameters'. Below the title bar, there is a paragraph of text: 'The default values for these parameters should be suitable for most IBM Endpoint Manager deployments. For further information about the implications of these parameters, please contact a IBM Endpoint Manager support technician.' The main area contains several configuration options: 'Server Port Number:' with a text box containing '52311'; 'Gathering Interval:' with a dropdown menu set to 'Day'; 'Initial Action Lock:' with a dropdown menu set to 'Unlocked' and a text box containing '5' followed by 'minutes'; 'Action Lock Controller:' with a dropdown menu set to 'Console'; a checkbox labeled 'Exempt the following site URL from action locking:' with an empty text box below it; a checkbox labeled 'Require use of FIPS 140-2 compliant cryptography.'; and a checked checkbox labeled 'Allow use of Unicode filenames in archives.' At the bottom, there are 'OK' and 'Cancel' buttons.

以下のオプションを設定できます。

サーバーのポート番号:

通常、この番号を変更する必要はありません。52311 が推奨ポート番号ですが、異なるポートの方が特定のネットワークでの利便性が高い場合は、異なるポートを選択できます。通常、ポートは、IANA が管理するプライベート・ポートの範囲 (49152 から 65535) から選択します。予約済みのポート番号 (ポート 1 から 1024) を使用できますが、トラフィックを正常にモニターする機能または制限する機能が低下する可能性があり、特定のアプリケーションについてポート番号を使用できなくなります。クライアントの適用後にこの番号を変更すると、IBM Endpoint Manager が正しく機能しなくなります。追加情報については、次のセクションの『ポート番号の変更』を参照してください。

注: ポート番号 52314 はプロキシ・エージェント用として予約されているため、Endpoint Manager のコンポーネント間のネットワーク通信には使用しないでください。

収集間隔:

このオプションは、サーバーからの通知がない状態でクライアントが待機する時間を決定します。この時間が経過すると、クライアントは、新規コンテンツが使用可能であるかどうかを確認します。一般にサーバーは、新規コンテンツを収集するたびに、UDP 接続を通じて新規コンテンツが提供されていることをクライアントに通知することを試み、この遅延を回避します。ただし、UDP がファイアウォールによってブロックされているか、またはネットワーク・アドレス変換 (NAT) によってサーバーの観点からクライアントの IP アドレスが再マップされる状況では、クライアントからタイムリーに応答を得るためには、間隔を短くすることが必要になります。収集レートが高くても、差分のみが収集されるため、サーバーのパフォーマンスへの影響はほんのわずかです。クライアントは、既に保有する情報は収集しません。

初期アクション・ロック:

インストール後にクライアントが自動的にロックされるようにする場合、すべてのクライアントの初期ロック状態を指定します。ロックされたクライアントは、どの Fixlet メッセージがそのクライアントの適用対象であるかをレポートしますが、アクションを適用しません。デフォルトでは、クライアントがロックされないままにして、後から特定のクライアントをロックします。ただし、新規にインストールされたクライアントを制御しやすくするため、最初からクライアントをロックした状態にしており、その後個別にロック解除したい場合もあります。あるいは、一定の期間 (分単位) だけ、クライアントがロックされるように設定することもできます。

アクションのロックから次のサイト URL を除外する:

まれに、特定の URL を、すべてのアクション・ロックから除外することが必要な場合があります。このボックスにチェック・マークを付け、除外する URL を入力します。

注: 指定できるサイト URL は 1 つのみであり、先頭を http:// にする必要があります。

FIPS 140-2 に準拠した暗号を使用する必要がある

ネットワークを連邦情報処理標準に準拠させるには、このボックスにチェック・マークを付けます。これにより、すべての IBM Endpoint Manager コンポーネントが FIPS モードへの移行を試みるように、マストヘッドが変更されます。デフォルトでは、クライアントは、正しく FIPS モードに入ることができない場合、非 FIPS モードのままとなります。これは、特定のレガシー・オペレーティング・システムでは問題となる場合があります。このボックスにチェック・マークを付けると、クライアントの起動時間が 2 秒から 3 秒ほど長くなる可能性があります。

アーカイブでの Unicode ファイル名の使用を許可する (Allow use of Unicode filenames in archives):

この設定は、IBM Endpoint Manager のアーカイブにファイル名を書き込む際に使用されるコード・ページを指定します。ファイル名を UTF-8 コード・ページで書き込むには、このボックスにチェック・マークを付けます。

ローカル適用環境のコード・ページ (例えば、Windows-1252 や Shift JIS) を使用してファイル名を書き込む場合は、このボックスにチェック・マークを付けしないでください。IBM Endpoint Manager V9.1 のフレッシュ・インストールを実行する場合、デフォルトでは、ファイル名は UTF-8 で書き込まれます。

注: IBM Endpoint Manager 環境を V9.1 にアップグレードした場合、デフォルトでは、ファイル名はローカル適用環境のコード・ページに書き込まれます。

完了したら「OK」をクリックします。

11. IBM Endpoint Manager コンポーネント・インストーラーのインストール先フォルダーを選択します。IBM Endpoint Manager インストール・ガイド・ウィザードが起動し、IBM Endpoint Manager コンポーネントをインストールするためのガイドが表示されます。

注: このステップによって、IBM Endpoint Manager クライアント、IBM Endpoint Manager コンソール、および IBM Endpoint Manager サーバーのインストーラーが作成されますが、コンポーネントはインストールされません。

注: プライベート・キー (license.pvk) により、すべてのエージェントによって信頼されるサーバー署名キーの作成権限とローテーション権限が付与されます。このキーは、ライセンス証明書の作成処理中には IBM に送信されないため、慎重に保護する必要があります。サーバーをワークステーションに再インストールするには、保管されている IBM Endpoint Manager 資格情報を再使用する必要があります。資格情報を保存しなかった場合は、サーバーの再インストール時にもう一度生成する必要があります。

ステップ 3 - コンポーネントのインストール

プライベート・キーの作成、証明書の要求と受け取り、その証明書を使用したマストヘッドの作成、および各種インストール・コンポーネント (「IBM Endpoint Manager インストール・ガイド」を含む) の生成を完了しました。

コンポーネントが保存されると、「**IBM Endpoint Manager インストール・ガイド**」が自動的に起動します。これは、「スタート」メニューから選択することでいつでも実行できます。

IBM Endpoint Manager の 3 つの主要コンポーネント (サーバー、コンソール、およびクライアント) をインストールするには、次の手順に従います。

1. インストール・ガイドをまだ実行していない場合は、それを起動します (「**スタート**」>「**すべてのプログラム**」>「**IBM Endpoint Manager**」>「**IBM Endpoint Manager インストール・ガイド**」)。
2. ダイアログ・ボックスが開き、インストールするコンポーネントを選択するよう要求するプロンプトが出されます。左側にある複数のリンクを上から下に順番にクリックして、IBM Endpoint Manager コンポーネントをインストールします。インストール・フォルダーを参照することもできます。コンポーネント・インストーラーには、以下が含まれます。
 - サーバーのインストール
 - コンソールのインストール
 - クライアントのインストール
3. IBM Endpoint Manager サーバー、コンソール、およびクライアントには、すべて専用のインストーラーがあります。以下のセクションで説明されているように、それぞれの指示に従ってください。

Windows プライマリー・サーバーのインストール

IBM Endpoint Manager サーバーは、システムの中核です。ネットワーク上のサーバー・クラス・コンピューターで実行されます。このコンピューターは、インターネットに直接アクセスできるだけでなく、ネットワーク内のすべてのクライアント・コンピューターに直接アクセスできなければなりません。ご使用のサーバーが「IBM Endpoint Manager for Lifecycle Management 9.1」で概説する要件を満たしていることを確認してください。

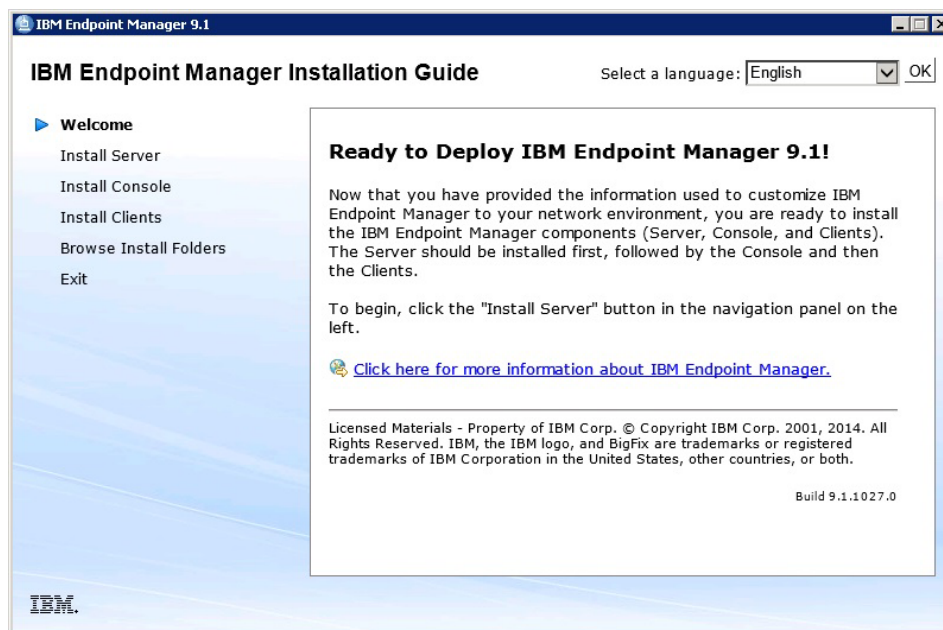
重要: ログインして IBM Endpoint Manager サーバーをインストールするユーザーは、MSSQL Server でデータベースと表を作成するための sa 権限を持っている必要があります。

IBM Endpoint Manager コンポーネントのデフォルトのインストール・パスは以下のとおりです。

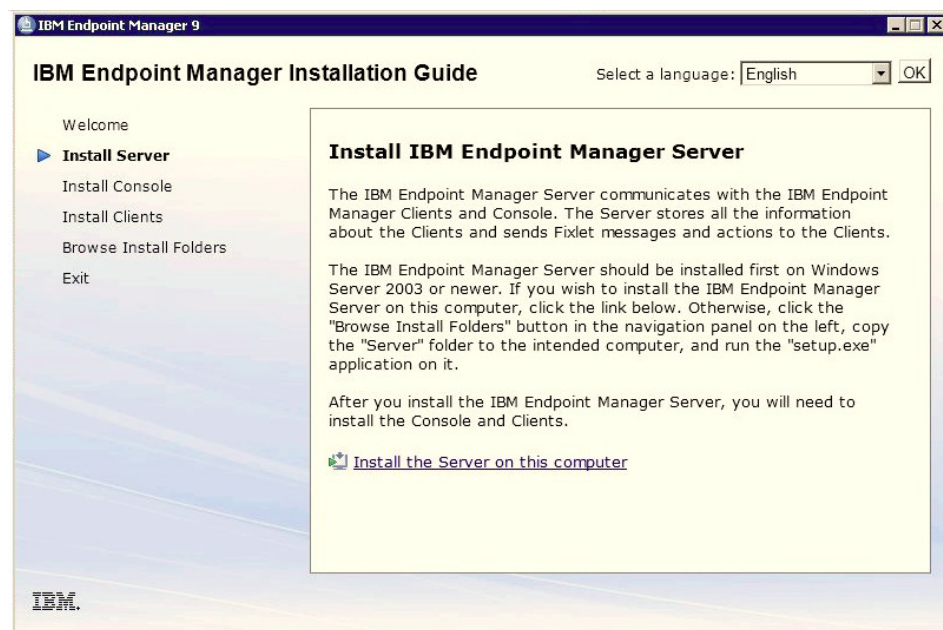
- C:\Program Files\BigFix Enterprise\BES Server (32 ビット Windows システム)
- C:\Program Files (x86)\BigFix Enterprise\BES Server (64 ビット Windows システム)

サーバーをインストールするには、以下の手順に従います。

1. インストール・ガイドをまだ実行していない場合は、実行します (「**スタート**」>「**すべてのプログラム**」>「**IBM Endpoint Manager**」>「**IBM Endpoint Manager インストール・ガイド**」)。新規パネルが開きます。



2. 「サーバーのインストール」をクリックします。



IBM Endpoint Manager サーバー・インストール・ウィザードのウェルカム・パネルが表示されます。ローカル環境にサーバーをインストールするには、「このコンピューターにサーバーをインストールする」をクリックします。別のコンピューターにサーバーをインストールするには、「インストール・フォルダーの参照」をクリックして IBM Endpoint Manager のインストーラー・フォルダーを開き、サーバー・フォルダーを表示します。サーバー・フォルダーを対象のコンピューターにコピーしたら、そのフォルダーにある `setup.exe` をダブルクリックしてインストーラーを起動します。

3. 「使用許諾契約」を読んでから、「はい」をクリックして同意し、操作を続行します。

4. ダイアログに、インストールされるサーバー・コンポーネントのリストが表示されます。通常は、デフォルト・コンポーネントをそのまま使用して「次へ」をクリックします。
5. ダイアログで、「シングル・データベースまたはマスター・データベース」または「複製したデータベース」を選択するよう求めるプロンプトが出されます。後で複製するためのマスター・データベースを作成する場合、または適用環境で単一のデータベースのみが必要な場合は、1 番目のボタンをクリックします。既存のマスターのレプリカを作成するには、2 番目のボタンをクリックします。これが初回のインストールである場合は、最初のボタンをクリックします。「次へ」をクリックします。
6. ダイアログで、「ローカル・データベースを使用」または「リモート・データベースを使用」のいずれかを選択するよう求めるプロンプトが出されます。
IBM Endpoint Manager データベースをホストするために別のコンピューターを使用する場合は、そのコンピューターに SQL Server が既にインストールされている必要があります。最も一般的に選択されるのは、ローカル・データベースを使用することです。リモート・データベースを使用して IBM Endpoint Manager をインストールする場合は、58 ページの『リモート・データベースを使用したサーバーのインストール』を参照してください。
7. 「ローカル・データベースを使用」を選択すると、データベース・サーバー・コンポーネントの宛先を指定するよう求めるプロンプトが表示されます。デフォルトのロケーションは C:\Program Files (x86)\Microsoft SQL Server です。
8. インストーラーにより、サーバー・コンポーネントの宛先を指定するためのプロンプトが表示されます。デフォルトのロケーションは C:\Program Files (x86)\BigFix Enterprise\BES Server ですが、「参照」ボタンをクリックして、別のロケーションを指定することができます。宛先を選択したら、「次へ」をクリックします。
9. 「サーバー・プロパティ」ダイアログで、サーバーの Web ルート・フォルダーのロケーションの入力を求めるプロンプトが出されます (デフォルトと異なる場合)。これは、クライアント用のダウンロード済みファイルが格納されるロケーションです。デフォルトの URL も表示され、変更したい場合は編集することができます。

注: 他のアプリケーションが IBM Endpoint Manager ポートを listen することはできません。他のアプリケーションが listen していた場合、エラーが発生します。ポート番号 52314 はプロキシ・エージェント用として予約されているため、Endpoint Manager のコンポーネント間のネットワーク通信には使用しないでください。

10. 「Web レポートのプロパティ」ダイアログで、Web レポートの Web ルート・フォルダーのロケーション (デフォルトと異なる場合) と、使用するポート番号の入力を求めるプロンプトが出されます。デフォルトおよびポート番号も表示され、変更したい場合は編集することができます。

注: IIS がインストールされている場合は、代わりにポート 52312 が選択されます。

11. サーバー・インストーラーで、インストール対象のコンポーネントについて選択されたインストール・パラメーターを表示するウィンドウが開きます。「次へ」をクリックして、インストールを続行します。
12. license.pvk ファイルを見つけるように求めるプロンプトが出されます。デフォルト・パス (指定されている場合) を受け入れるか、「参照」ボタンをクリックして異なるロケーションを見つけます。パスワードを入力してデータベースを初期化し、「OK」をクリックして続行します。
13. データベースの初期化が完了すると、コンソール用の初期ユーザー名およびパスワードの入力を求めるプロンプトが出されます。これは、コンソールに最初にログインするときに使用されるアカウントです。また、すべての特権を持つマスター・オペレーター・アカウントです。
14. IBM Endpoint Manager サーバーのインストールが、これで完了しました。
「IBM Endpoint Manager 診断ツールを実行してください」というボックスのチェック・マークが外れていることを確認し、「完了」をクリックしてウィザードを終了します。

注: この段階で診断ツールの実行を選択すると、一部のステップが失敗する可能性があります (例えば、まだクライアントがインストールされていない、など)。ただし、サービスおよび Web レポートは正しく実行されているはずで
す。

15. 74 ページの『クライアントの手動インストール』に示す説明に従って、サーバーがインストールされている同じ Windows システムに IBM Endpoint Manager クライアントをローカルにインストールします。
16. インターネットにアクセスするためのプロキシを構成した場合は、161 ページの『第 12 章 プロキシ接続のセットアップ』で説明する手順に従って、IBM Endpoint Manager 環境にプロキシを構成します。

注: プロキシ構成が更新され、プロキシ経由での通信の使用が開始されるまで、待つ必要があります。

17. Windows デスクトップで、「スタート」>「IBM Endpoint Manager 診断ツールの実行 (Run the IBM Endpoint Manager Diagnostic Tool)」を選択します。
IBM Endpoint Manager 診断ツールのタブに、ご使用の環境で実行された検証の結果が示されます。このツールについて詳しくは、『IBM Endpoint Manager 診断ツールの実行』を参照してください。

リモート・データベースを使用したサーバーのインストール:

リモート・データベースを使用して IBM Endpoint Manager サーバーをインストールする前に、以下の事項を確認する必要があります。

- SA 特権を持つユーザーとして IBM Endpoint Manager サーバーをインストールしている。
- SQL Server Browser が実行されている。
- SQL Server 認証が有効である。

新規データベース・ユーザーの作成:

Microsoft SQL Server がインストールされているマシンにデータベース・インスタンスを作成した後、その SA ユーザーをデータベース接続に使用しない場合は、SA 特権を持つ新規ユーザーを作成する必要があります。

特定のデータベース・インスタンス (例えば、TEM91) に対して新規ユーザーを作成する場合は、以下の手順を実行します。

1. Microsoft SQL Server Management Studio を開始します。
2. 「サーバーへの接続」パネルで、以下のパラメーターを指定します。

サーバーの種類

データベース・エンジン

サーバー名

<DB_HOSTNAME>¥<INSTANCE_NAME>。サーバーのホスト名が NC118103 で、インスタンス名が TEM91 の場合、サーバー名は NC118103¥TEM91 です。

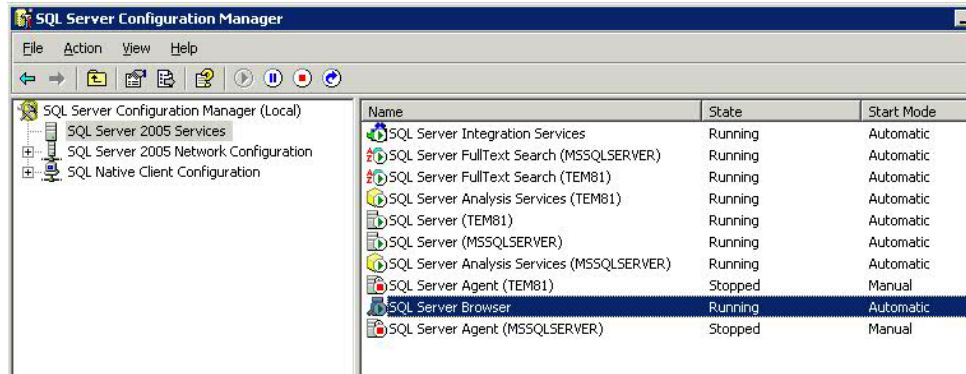


3. ポートフォリオから、「セキュリティ」->「ログイン」->「新しいログイン」を選択します。
4. 「全般」タブで、ユーザー名と SQL Server 認証用の資格情報を指定します。
5. 「サーバー・ロール」タブで、「sysadmin」を選択し、「OK」をクリックします。

SQL Server Browser の開始:

Microsoft SQL Server がインストールされたコンピュータで、以下の手順を実行して、SQL Server Browser が確実に実行されているようにします。

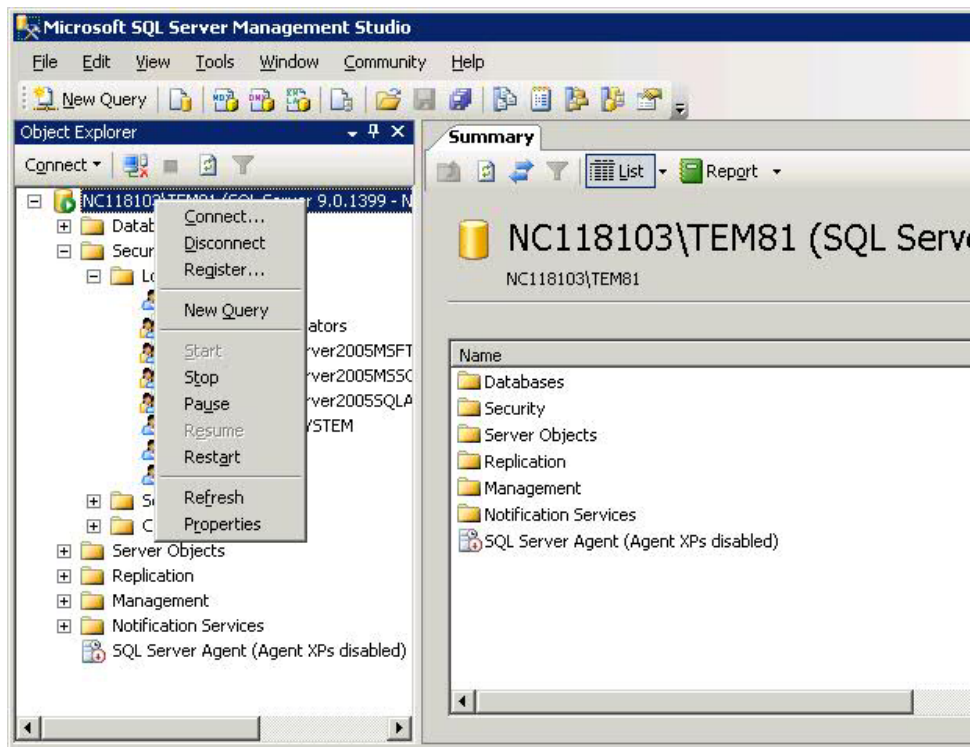
1. 「SQL Server 構成マネージャー」を開始します。
2. 以下のように、「SQL Server 2005 のサービス」を選択し、SQL Server Browser が実行されていない場合は開始します。



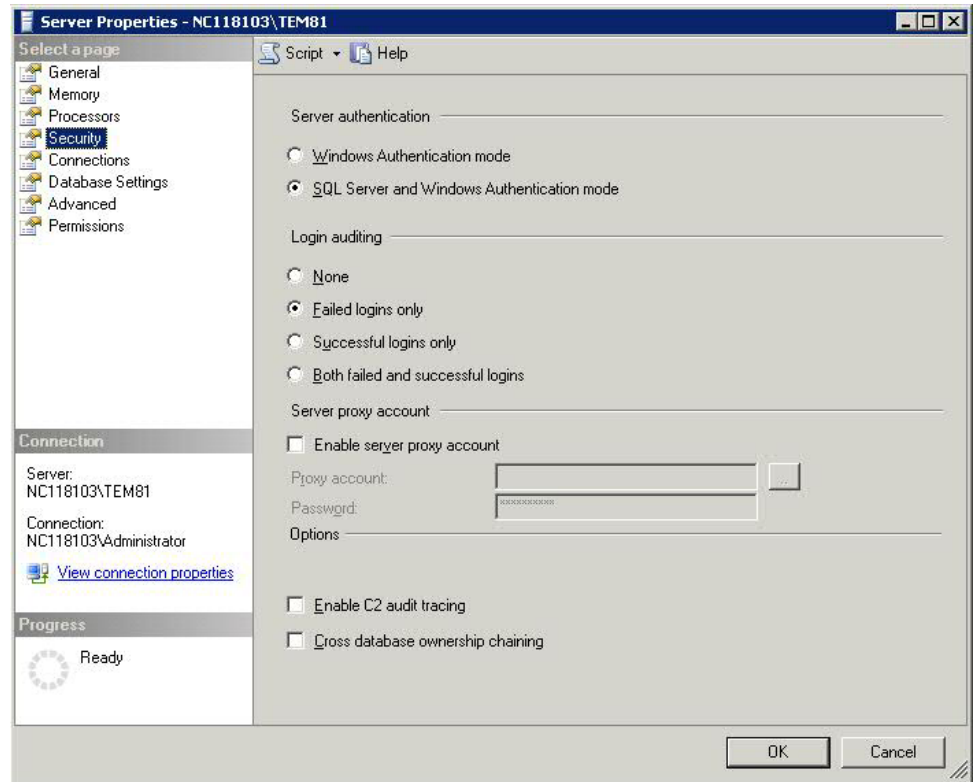
SQL Server 認証モードの有効化:

Microsoft SQL Server がインストールされたコンピュータで、以下の手順を実行して、SQL Server 認証モードが有効であることを確認します。

1. Microsoft SQL Server Management Studio を開始します。
2. データベース・インスタンスを選択します。
3. 「プロパティ」>「セキュリティ」を選択します。



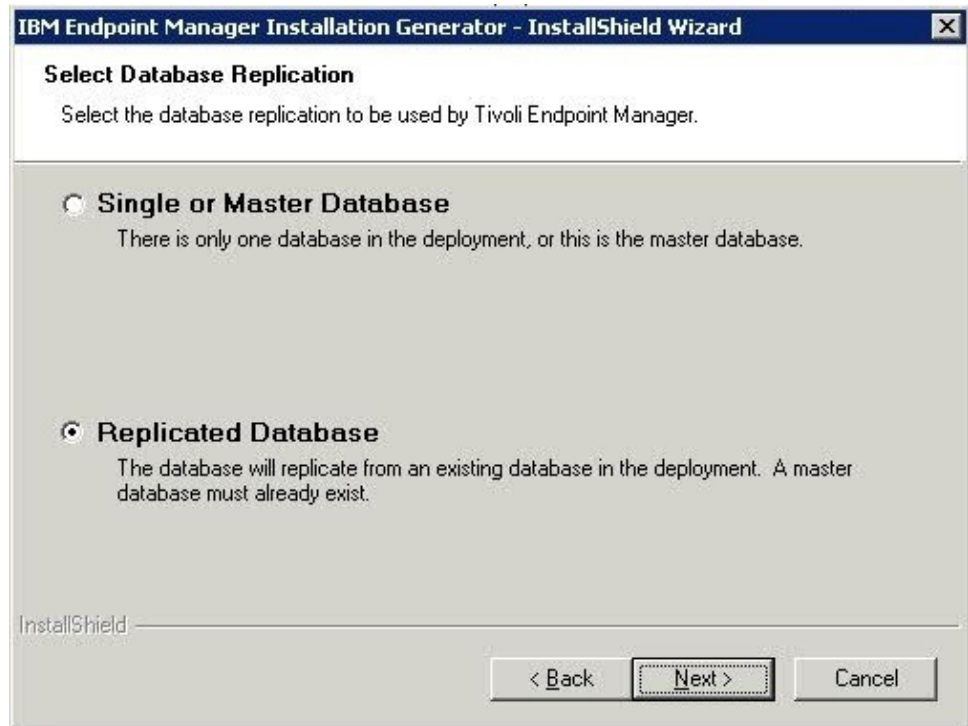
4. 「SQL Server 認証モードと Windows 認証モード」が選択されていることを確認します。



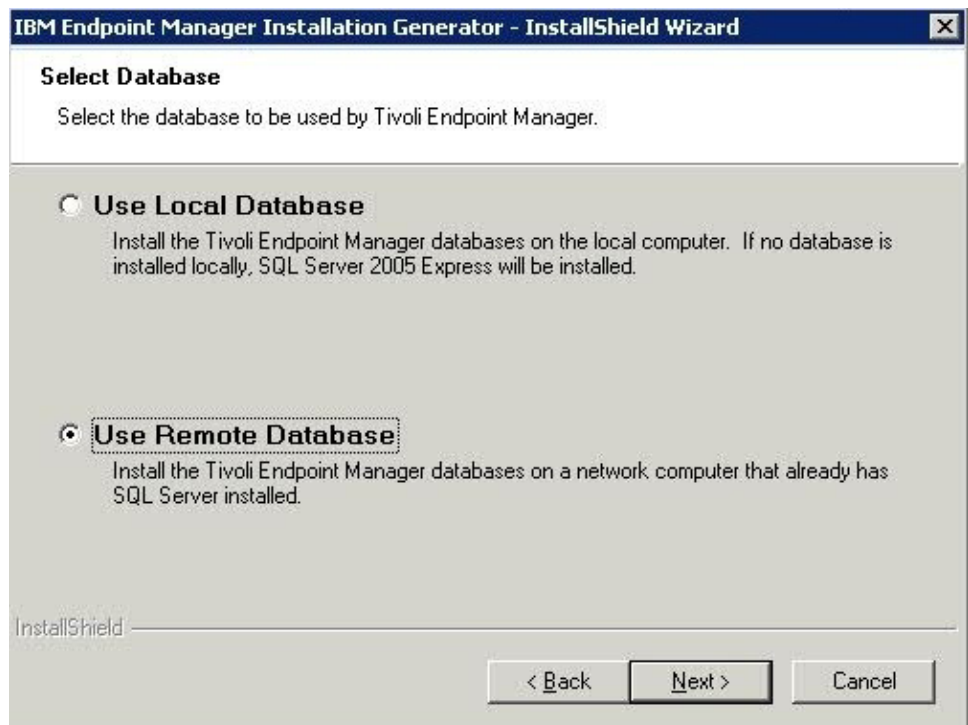
リモート・データベース SQL 認証を使用したサーバーのインストール:

リモート・データベースを使用して IBM Endpoint Manager サーバーをインストールするには、以下の手順を実行します。

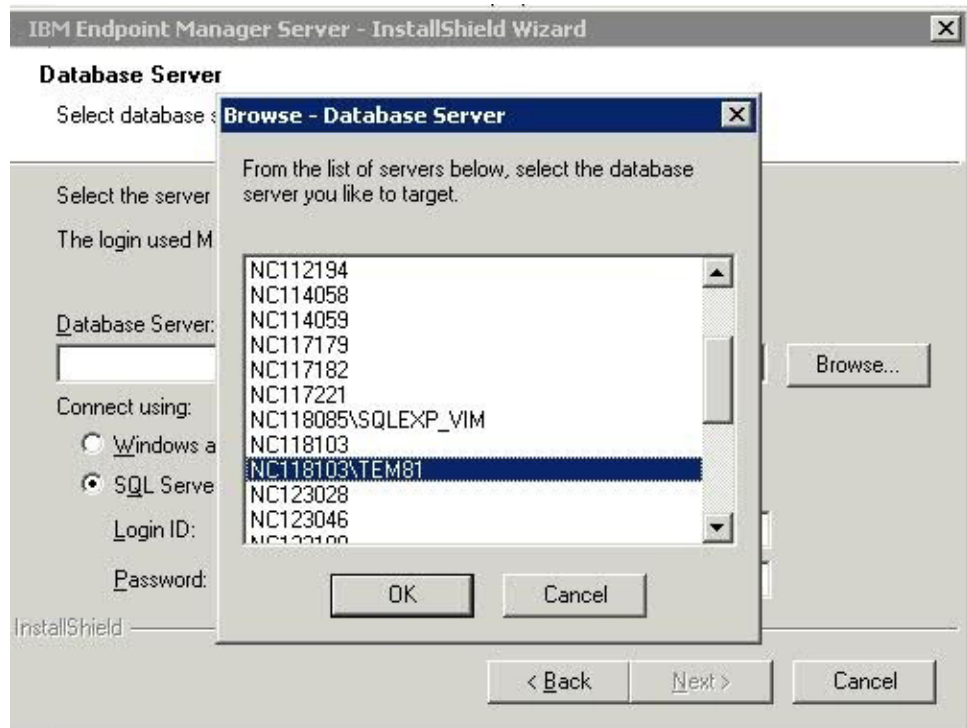
1. IBM Endpoint Manager サーバーをインストールするコンピュータで、インストールを実行します。
2. サーバーのインストール中に、データベースのレプリケーションとして「**シングル・データベース**または**マスター・データベース**」を選択します。



3. データベースの種類として「リモート・データベースを使用」を選択します。

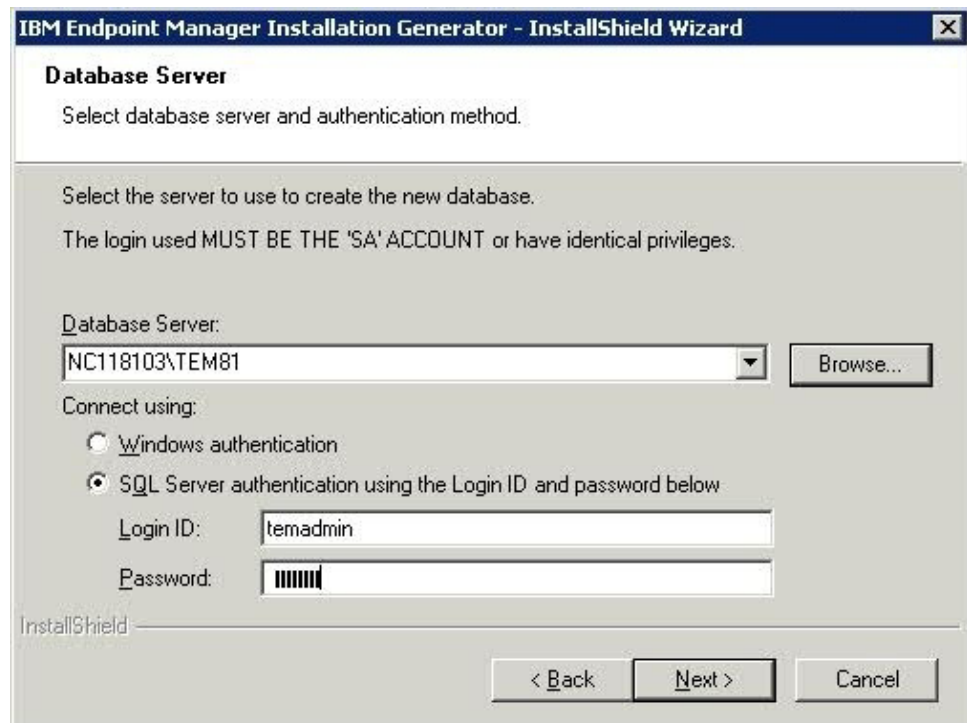


4. 次のウィンドウで、以下のように、「参照」をクリックし、使用するデータベース・サーバー・インスタンスを選択します。



5. 「SQL Server 認証に以下のログイン ID とパスワードを使用 (SQL Server Authentication using the login ID and password below)」をクリックし、SA 特権を持つユーザーの資格情報を指定します。

注: これらの資格情報は、Windows レジストリーに平文で格納されます。



Microsoft SQL Server がインストールされているリモート・マシンに、データベースが作成されます。IBM Endpoint Manager サーバーがインストールされるマ

The screenshot shows the Windows Registry Editor with the following tree structure expanded:

- HARDWARE
- SAM
- SECURITY
- SOFTWARE
 - BigFix
 - BES Installation
 - BESRelay
 - BigFix Server
 - Brand
 - ClientCompliance
 - Enterprise Server
 - BESReports
 - ClientRegistration
 - Database (selected)

The right pane displays the following registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
Password	REG_SZ	dtm33dtm
User	REG_SZ	temadmin

The screenshot shows the Windows Registry Editor with the following structure:

- File Edit View Favorites Help
- Left pane (tree view):
 - SAM
 - SECURITY
 - SOFTWARE
 - BigFix
 - BES Installation Generator
 - BESRelay
 - BigFix Server
 - Brand
 - ClientComplianceAPI
 - Enterprise Server
 - BESReports
 - ClientRegister
 - Database
 - FillAggregateDB** (selected)
 - FillDB

- Right pane (table view):

Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalDBDSN	REG_SZ	LocalBESReportingSe
Password	REG_SZ	dtm33dtm
Username	REG_SZ	temadmin

複数のサーバーを使用することによって、IBM Endpoint Manager のインストール済み環境に、さらに高いレベルのサービスを提供できます。ご使用のインストール済み環境に Distributed Server Architecture (DSA) を追加することを選択すると、ローカル・サービスの提供を続行しながら、ネットワークおよびシステムの障害から自動的に復旧することができるようになります。この機能を利用するには、少なくとも 1 次サーバーと同等の機能を持つ、1 つ以上の追加のサーバーが必要です。追加の費用と設置が必要となるため、DSA に取り組む前に、ニーズについて慎重に検討する必要があります。

64 IBM Endpoint Manager: インストール・ガイド

ドメイン・ユーザーおよびユーザー・グループでの NT 認証の使用:

この方法では、各サーバーは指定のドメイン・ユーザーまたは指定のユーザー・グループのメンバーを使用して、適用環境内の他のすべてのサーバーにアクセスします。ドメイン・ユーザーおよびユーザー・グループを使用してサーバーを認証するには、次の手順に従います。

1. ドメインでサービス・アカウント・ユーザーまたはユーザー・グループを作成します。ユーザー・グループの場合、権限があるドメイン・ユーザーをサーバーに追加します。これを実行するには、ドメイン管理特権が必要な場合があります。
2. マスター・サーバーにおいて、SQL Server Management Studio を使用して、デフォルト・データベースの **BFEnterprise** でドメイン・サービス・アカウント・ユーザーまたはユーザー・グループのログインを作成し、このログインに、システム管理者 (sa) 権限、または **BFEnterprise** データベースおよびマスター・データベースの **DBO** (データベース所有者) 役割を付与します。
3. マスター・サーバーで、FillDB、BES ルート、および Web レポートのサービスの **LogOn** 設定を、ステップ 2 で作成したドメイン・ユーザーまたはユーザー・グループのメンバーに変更し、サービスを再始動します。

注: Endpoint Manager サーバーのインストールを完了し、製品サイトを使用し始めた後に、**BES Server Plugin Service** や **BES NMAP Unmanaged Asset Importer** などの追加コンポーネントをインストールする場合があります。このどちらのサービスにも、リモート・データベースにアクセスできるように **LogOn** 設定が NT ユーザー用に設定されています。

ドメイン・コンピューター・グループでの NT 認証の使用:

この方法では、各サーバーが指定のドメイン・コンピューター・グループに追加され、各サーバーはそのドメイン・グループのメンバーのログインを受け付けます。ドメイン・コンピューター・グループを使用してサーバーを認証するには、次の手順に従います。

1. 選択したサーバーが存在するドメインで、グローバル・セキュリティー・グループを作成します。これを実行するには、ドメイン管理特権が必要な場合があります。
2. グループの作成後、各サーバーを再起動して、各サーバーのドメイン認証情報を更新する必要があります。
3. マスター・サーバーにおいて、SQL Server Management Studio を使用して、デフォルト・データベースの **BFEnterprise** でドメイン・グループのログインを作成し、このログインに、システム管理者 (sa) 権限、または **BFEnterprise** データベースおよびマスター・データベースの **DBO** (データベース所有者) 役割を付与します。

SQL 認証の使用:

この方法では、各サーバーにログイン名とパスワードが付与され、それらのサーバーが適用環境内の他のすべてのサーバーのログイン名およびパスワードを受け付けるように構成されます。このアカウントのパスワードは平文で入力しますが、FillDB サービスの再始動後に、各サーバーのレジストリーの HKLM ブランチに難読化して保存されます。

SQL 認証を使用してサーバーを認証するには、次の手順に従います。

1. サーバー間認証のために、適用環境内のすべてのサーバーが使用する単一のログイン名 (例えば `besserverlogin`) および単一のパスワードを選択します。
2. マスター・サーバーで、SQL Server Management Studio を使用して、この名前を持つ SQL Server ログインを作成します。認証オプションとして「SQL Server 認証」を選択し、パスワードを指定します。デフォルト・データベースを BFEnterprise に変更し、それにシステム管理者 (sa) 権限、または BFEnterprise データベースおよびマスター・データベースの `db_owner` 役割を付与します。
3. マスター・サーバーで、以下のストリング値を
HKLM¥Software¥BigFix¥Enterprise Server¥FillDB キー (Windows 32 ビット・システムの場合) および HKLM¥Software¥Wow6432Node¥BigFix¥Enterprise Server¥FillDB キー (Windows 64 ビット・システムの場合) の下に追加します。

```
ReplicationUser = <login name>  
ReplicationPassword = <password>  
ReplicationPort = <SQL_port>
```
4. FillDB サービスを再始動します。

注:

この選択は、適用環境単位で行う必要があります。ドメインで認証されるサーバーと SQL で認証されるサーバーを混在させることはできません。

ReplicationUser、ReplicationPassword、および ReplicationPort は、DSA 環境のすべてのサーバー・レジストリーで一意的に定義する必要があります。

適用環境内のすべての IBM Endpoint Manager サーバーが同じバージョンの SQL Server を実行している必要があります。

追加 Windows サーバーのインストール

このセクションの操作を続行する前に、認証方式を決定し、64 ページの『追加サーバーの認証』内の該当する手順を実行してください。

適用環境に追加するサーバーごとに、そのサーバーが他のサーバーと通信できることを確認してから、以下の手順を実行します。

1. マスター・サーバーによって使用されているものと同じ SQL Server バージョンをインストールします。
2. 追加サーバーとして構成する各マシンで、「サーバーのインストール・プログラム」を実行します。ローカル SQL Server のインストールで使ったドメイン管理特権を使用して、sa 権限を持っていることを確認してください。
3. インストール生成プログラムからサーバー・インストーラーを抽出している場合、「**実動適用環境 (Production Deployment)**」および「**既存のマストヘッドを使ってインストールします**」を選択します。マスター・サーバーから `masthead.afxm` ファイルを指定します。それ以外の場合は、マスター・サーバー上の BESInstallers フォルダのサーバー・インストール・パッケージを使用します。
4. サーバー・インストーラーの「**データベース・レプリケーションの選択**」ページで、「**複製したデータベース**」を選択します。

5. 「データベースの選択ページで、「ローカル・データベース (Local Database)」を選択して、サーバーでデータベースをホストします (ほとんどのアプリケーションで一般にこのようにします)。
6. インストーラーが「新規インストールの構成 (Configuring your new installation)」まで進み、「データベース接続」ダイアログ・ボックスが表示されるまで、インストーラー画面で操作を続行します。マスター・サーバーのホスト名を入力し、BFEnterprise データベースに対する DBO 許可を持つマスター・サーバーにログインできるアカウントの資格情報を入力します。「レプリケーション・サーバー (Replication servers)」ウィンドウに、現在の適用環境のサーバー構成が表示されます。デフォルトでは、新規にインストールされたサーバーは、5 分ごとにマスター・サーバーから直接複製するように構成されています。この構成は、必要に応じて調整できます。大規模なインストールの場合、最初のデータベースのレプリケーションには数分かかることがあり、中断される可能性があります。この問題が発生した場合は、IBM ソフトウェア・サポートにご相談ください。
7. BFEnterprise をデフォルト・データベースとし、BFEnterprise データベースおよびマスター・データベース上のシステム管理者 (sa) 権限または DBO 役割を使用して、前にマスター・サーバーで作成したものと同一 SQL Server ログインを、SQL Server Management Studio を使用して作成します。
8. ドメイン・ユーザーまたはユーザー・グループを通じた NT 認証の場合、FillDB サービス用の LogOn 設定を、ドメイン・ユーザー、または上記で作成したユーザー・グループのメンバーに変更し、サービスを再始動します。
9. SQL 認証の場合、次のストリング値を FillDB レジストリー・キーに追加して、FillDB サービスを再始動します。HKLM¥Software¥BigFix¥Enterprise Server¥FillDB (64 ビット・システムのキーは HKLM¥Software¥Wow6432Node¥BigFix¥Enterprise Server¥FillDB)。

ReplicationUser = <login name>

ReplicationPassword = <password>

10. 新規にインストールされたサーバーで、**IBM Endpoint Manager 管理ツール**を実行し、「レプリケーション」タブを選択して、現在のサーバーのリストと、それらのレプリケーション期間を表示します。新規にインストールされたサーバーをプルダウン・メニューから選択し、下のリストで、そのサーバーがマスター・サーバーに正常に接続されていることを確認します。次に、サーバー・ドロップダウンでマスター・サーバーを選択し、それが新規サーバーに正常に接続されていることを確認します。両方のサーバーが正常な接続を示すまで、次のレプリケーション期間になるのを待機しなければならない場合があります。

注: 最初のレプリケーションは、データベースのサイズによって、数時間かかる可能性があります。レプリケーションが完了するまで待機してから、レプリカ・サーバーに接続されたコンソールから任意のアクションを実行してください。

11. 「レプリケーション グラフの編集」ボタンをクリックすると、サーバーとその接続のグラフを表示できます。接続の矢印をドラッグすることにより、サーバー間の接続を変更できます。

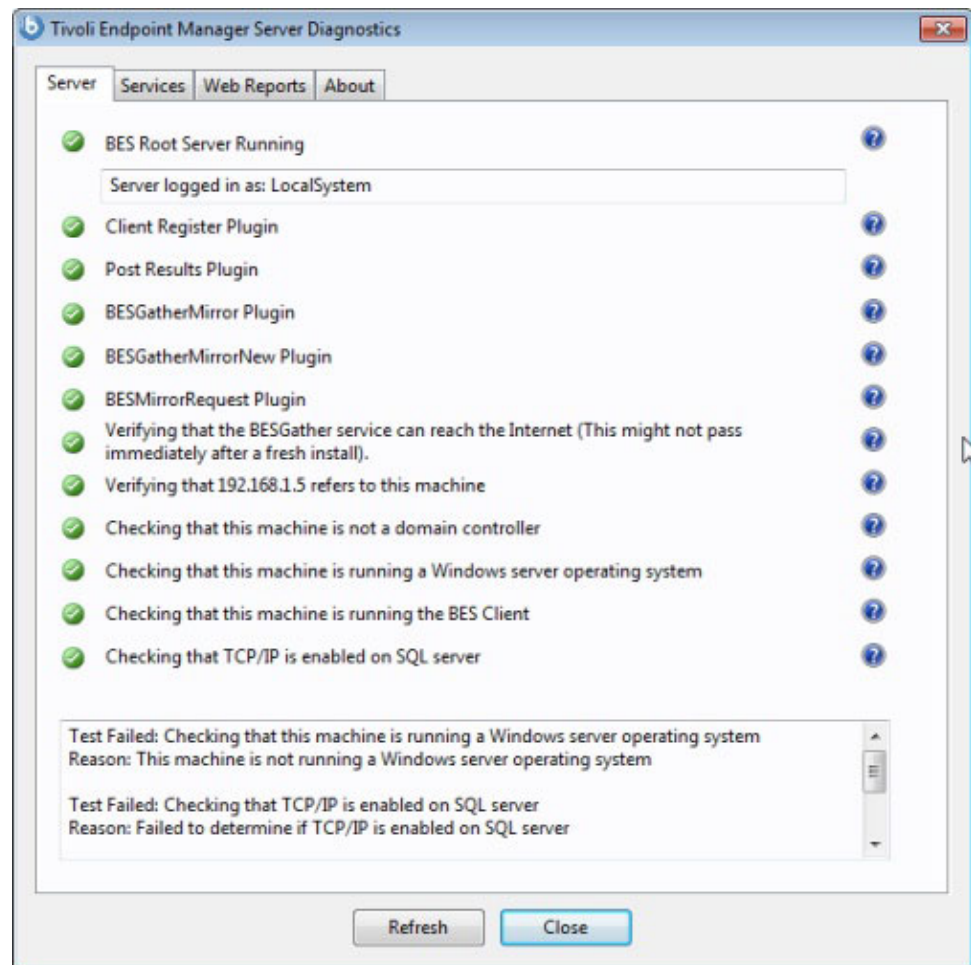
IBM Endpoint Manager 診断ツールの実行

IBM Endpoint Manager 診断ツールは、サーバー・コンポーネントが正しく機能しているかどうかを検査します。このツールは、正しく構成されていないコンポーネントや機能していないコンポーネントを識別し、結果を表示します。診断を実行するには、次の手順に従います。

1. サーバーをインストールした直後には、この診断ツールは既に実行されています。実行されていない場合、サーバーに管理者としてログオンして、プログラムを起動してください。

「スタート」 > 「すべてのプログラム」 > 「IBM Endpoint Manager」 > 「IBM Endpoint Manager 診断ツール」を選択してください。プログラムにより、サーバー・コンポーネントが分析され、レポートが作成されます。

2. 詳しい情報が必要な場合は、「フルインターフェース」をクリックします。「IBM Endpoint Manager 診断」コントロール・パネルが表示されます。このウィンドウには、「サービス」、「Web レポート」など、サーバー診断のカテゴリに対応するタブがあります。

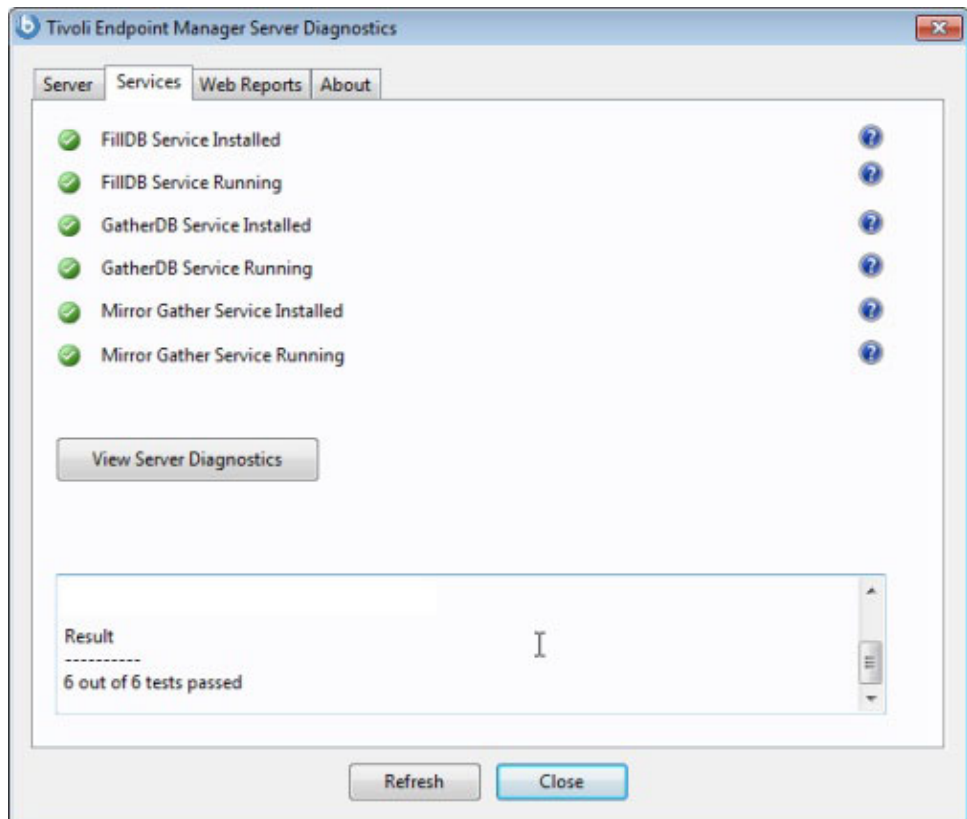


注: プロキシを使用していて、フレッシュ・インストールの実行後に「BESGather サービスがインターネットに接続可能かどうかを確認」というメッ

セージが表示された場合は、161 ページの『第 12 章 プロキシ接続のセットアップ』の説明のとおりプロキシが構成されているかどうかを確認してください。

クライアントをまだインストールしていない場合、警告ライトが表示されます。クライアントをインストールすると、これは直ちに緑色になります。

3. 「サービス」タブで、データベース・サービスと収集サービスが正しくインストールされて稼働しているかどうかを確認します。



項目の横に赤色のライトが表示された場合、そのコンポーネントで障害が発生していることを示します。サーバーが正しく機能しているか確認する前に、示されている問題を解決する必要があります。同様に、**Web レポート・サーバー**を診断するためのタブもあります。

4. 詳しい情報を表示するには、項目の右側にある疑問符 (?) ボタンをクリックします。これらのボタンは、IBM Endpoint Manager サポート・サイトにある知識ベースの記事にリンクされています。
5. すべてのボタンが緑色になったら、「閉じる」をクリックして診断を終了します。

注: サーバー・コンピューターがドメインのメンバーである一方で、ユーザーがローカル・ユーザーとしてログインしている場合、この診断ツールにより、アクセス許可が正しくないと誤ってレポートされる場合があります。アクセス許可のテストが間違って失敗している場合、その診断警告は無視してかまいません。

サーバーのコンポーネントについて

この時点で、IBM Endpoint Manager サーバーは正常にインストールされており、各種のコンポーネントを使用して、リレー、クライアント、コンソールの各コンピューターからのメッセージと要求に応答しています。

サーバーの実行内容を適切に理解するために、以下に示すいくつかのコンポーネントの説明を確認してください。

クライアント登録コンポーネント

クライアントは、新しいコンピューターにインストールされると、サーバーのクライアント登録コンポーネントにクライアント自体を登録します。クライアントには、固有 ID が付与されます。コンピューターの IP アドレスが変更されると、クライアントは、その新しい IP アドレスを、クライアント登録コンポーネントに自動的に登録します。

結果ポストサーバー・コンポーネント

クライアントは、Fixlet が適用対象であることを検出すると、HTTP POST 操作を使用して、結果ポストサーバー・コンポーネントにレポートします。このコンポーネントは、クライアント・コンピューターの登録済み ID と共に、適用対象の Fixlet を識別します。この情報は、FillDB サービスを通じて IBM Endpoint Manager データベースに渡され、その後、コンソールで表示できるようになります。クライアントは、その他の状態の変更についても、直接またはリレーを通じて定期的にサーバーにレポートします。

収集サーバー・コンポーネント

このコンポーネントは、サブスクライブしたすべての Fixlet サイトでの Fixlet コンテンツの変更を監視します。このコンポーネントは、これらの変更をサーバーにダウンロードします。これにより、GatherDB コンポーネントがそれらの変更を使用できるようになります。

FillDB コンポーネント

このコンポーネントは、クライアントの結果をデータベースに送ります。

GatherDB コンポーネント

このコンポーネントは、Fixlet ダウンロードをインターネットからデータベース内に収集し、保存します。

ダウンロード・ミラーリング・サーバー・コンポーネント

ダウンロード・ミラーリング・サーバー・コンポーネントは、リレーおよびクライアントのために Fixlet サイト・データをホストします。このコンポーネントは、IBM Endpoint Manager トラフィック用の簡素化されたダウンロード・サーバーとして機能します。

コンソールのインストール

IBM Endpoint Manager コンソールでは、オペレーターが、ネットワーク全体のすべての管理対象コンピューターでの問題をモニターし、修正することができます。このコンソールは、HTTPS ポート 52311 経由でサーバーへのネットワーク接続が可能であれば、いずれのコンピューターにもインストールすることができます。テスト環境と評価環境の場合を除き、サーバー・コンピューター自体でコンソールを実行しないでください。これは、データベースまたは Web サーバーを実行している

コンピューターで発行者キーの資格情報を持つことにより、パフォーマンス上の影響とセキュリティ上の影響があるためです。

コンソールをインストールするには、以下の手順に従います。

1. インストール・ガイドを実行します (「スタート」>「すべてのプログラム」>「IBM Endpoint Manager」>「IBM Endpoint Manager インストール・ガイド」)。「IBM Endpoint Manager コンポーネントのインストール」をクリックします。
2. 次のパネルで、「コンソールのインストール (Install Console)」をクリックします。
3. プロンプトが出されたら、コンソールのインストール・ロケーションを入力します。デフォルトのロケーションは C:\Program Files\BigFix Enterprise\BES Console です。別のインストール先を選択するには、「参照」をクリックし、希望するロケーションにナビゲートします。「次へ」をクリックして先に進みます。
4. ファイルがインストールされたら、「完了」をクリックして、インストールを終了します。ここで、コンソールを起動するか、次のセクションに進んでクライアントをインストールするかを選択できます。

コンソール・プログラムの使用について詳しくは、「IBM Endpoint Manager コンソール・オペレーター・ガイド」を参照してください。

クライアントのインストール

管理対象のネットワークにあるすべてのコンピューター (コンソールを実行するコンピューターを含みます) に IBM Endpoint Manager クライアントをインストールします。これにより、そのコンピューターで、セキュリティ・パッチ、構成ファイル、アップグレードなどの重要な Fixlet メッセージを受信できます。

コンソールを実行している場合は、「IBM Endpoint Manager コンポーネントのインストール」>「クライアントのインストール」>「ローカルにインストール」を選択して、ローカル・マシン上の指定したディレクトリーにクライアントをインストールします。

クライアント適用ツール (BESClientDeploy.exe) を実行する場合、以下の 3 つの方法でクライアントを適用することができます。

Active Directory を使用してコンピューターを検索する

IBM Endpoint Manager クライアント・インストール・ツールは Active Directory サーバーにアクセスし、ドメイン内のすべてのコンピューターのリストを取得します。このツールは、各コンピューターをチェックして、クライアントが既にインストールされているかどうかを確認し、その情報をリスト形式で表示します。

NT 4.0 ドメインを使用してコンピューターを検索する

ドメイン内のすべてのコンピューターが、クライアントがインストールされているかどうか示すステータス・フラグ付きでリストされます。

リスト内で指定されたコンピューターを検索する

ネットワークでのコンピューター・アドレスの解決方法に基づいて、コンピューター名、IP アドレス範囲、またはホスト名のリストを指定する必要があります。

あります。このリストでは、行ごとに 1 つの名前、IP アドレス範囲、またはホスト名を指定する必要があります。このオプションを使用すると、クライアント・インストール・ツールはコンピューターのディスカバーを試行しませんが、代わりに、リストされているすべてのコンピューターへの直接インストールを試行します。

クライアント・インストール・ツールの使用:

Active Directory ドメインまたは NT Directory ドメインに接続されている小規模なネットワーク (おおよそ 5,000 台未満のコンピューター) では、クライアント・インストール・ツールを使用して Windows クライアントをインストールできます。大規模なネットワークでは、その他のインストール方法を使用した方が簡単な場合があります。クライアント・インストール・ツールは、クライアントを簡単な方法で展開できるよう支援しますが、以下に示す要件および条件があります。

- Active Directory ドメインまたは NT Directory ドメインが必要です (コンピューターの管理者アカウントを所有している場合、一連のコンピューターにインストールするオプションもあります)。
- IBM Endpoint Manager クライアント・インストール・ツールは、Windows 2000、XP、Server 2003、Vista、Server 2008、7、または Server 2008 R2 を実行しているコンピューターのみを対象にすることができます。
- クライアント・インストール・ツールを実行するコンピューターはドメインに接続する必要がありますが、そのコンピューター自体はドメイン・コントローラーにしないでください。
- サービス・コントロール・マネージャー (SCM) サービスおよびリモート・プロシーチャー・コール (RPC) サービスがターゲット・マシンで実行されている必要があります。
- SCM へのリモート接続またはリモート・プロシーチャー・コールの発行を防ぐセキュリティ・ポリシーはコンピューターに対して使用しないでください。
- Active Directory 内のすべての対象のコンピューターの dnsName プロパティを正しく定義する必要があります。

クライアント・インストール・ツールを使用すると、クライアントをコンピューターに容易にプッシュできますが、クライアント・インストール・ツールは、多数の機能を備えた企業クラスのソフトウェア配布ツールではありません。ソフトウェア配布ツールが既にある場合、その既存のソフトウェア配布ツールを代わりに使用することをお勧めします。

IBM Endpoint Manager クライアント・インストール・ツールは、Active Directory サーバーからコンピューターのリストを取得し、それらのコンピューターにリモート接続して (一度に 100 台のコンピューターにアクセスします)、クライアント・サービスが各コンピューターに既にインストールされているかどうかを確認することにより、処理を開始します。インストールされている場合、「**インストール済み**」とレポートし、それとともにクライアント・サービスの状況 (「**実行中**」、「**停止**」など) もレポートします。アクセス許可の問題が原因で、または何らかの理由で状況を特定できない場合、「**状況が不明**」とレポートします。インストールされていない場合、「**インストールされていません**」とレポートします。ただし、コンピューターとまったく通信できない場合は除きます。その場合は、「**応答なし (Not Responding)**」とレポートします。

クライアントがまだインストールされていない場合、このツールは、共有インストーラーにアクセスするリモート・プロシージャ・コールを発行できるインターフェースを提供し、適切なドメイン管理認証情報を使用して、このリモート・プロシージャ・コールをサイレントで実行します。ユーザー操作は必要ありません。このツールを使用するには、次の手順を実行します。

1. IBM Endpoint Manager クライアント・インストール・ツールは、インストール生成プログラムによって作成されます。このツールは、インストール・ガイドから起動することができます。「**IBM Endpoint Manager コンポーネントのインストール**」>「**IBM Endpoint Manager クライアントのインストール**」>「**リモート・インストール**」ボタンをクリックします。または、「**スタート**」>「**すべてのプログラム**」>「**IBM Endpoint Manager**」>「**IBM Endpoint Manager クライアント適用**」を選択して、直接起動することもできます。
2. 表示されるダイアログでは、クライアントをインストールするための次の 3 つの方法が提供されます。

Active Directory を使用してコンピューターを検索する

IBM Endpoint Manager クライアント・インストール・ツールは Active Directory サーバーにアクセスし、ドメイン内のすべてのコンピューターのリストを取得します。このツールは、各コンピューターをチェックして、クライアントが既にインストールされているかどうかを確認し、その情報をリスト形式で表示します。

NT 4.0 ドメインを使用してコンピューターを検索する

ドメイン内のすべてのコンピューターが、クライアントがインストールされているかどうか示すステータス・フラグ付きでリストされます。

リスト内で指定されたコンピューターを検索する

ネットワークでのコンピューター・アドレスの解決方法に基づいて、コンピューター名、IP アドレス範囲、またはホスト名のリストを指定する必要があります。このリストでは、行ごとに 1 つの名前、IP アドレス範囲、またはホスト名を指定する必要があります。このオプションを使用すると、クライアント・インストール・ツールはコンピューターのディスカバリーを試行しませんが、代わりに、リストされているすべてのコンピューターへの直接インストールを試行します。

3. コンピューターへの管理アクセス権限を持つ「**ユーザー名**」および「**パスワード**」を入力します。ほとんどの場合、これはドメイン管理者アカウントです。コンピューター・リスト・オプションを使用する場合、管理者特権を持つリモート・コンピューターのローカル・アカウント（ローカル管理者アカウントなど）を指定することができます。残りのクライアント・インストール・プロセスでは、このユーザー名およびパスワードが使用されます。このため、アカウントにリモート・コンピューターへの適切なアクセス権限がない場合は、アクセス拒否エラーを受け取ります。
4. コンピューターのリストが表示されたら、IBM Endpoint Manager で管理するコンピューターを、Shift キーまたは Ctrl キーを押しながらクリックして選択します。「**次へ**」をクリックします。
5. 選択したコンピューターのリストが表示されます。通常はデフォルトのオプションで十分ですが、「**詳細オプション**」を選択して、次のインストール・パラメーターを構成することが望ましいです。

ファイルの転送

インストールのためにリモート・サーバーにファイルを「プッシュ」すること、またはローカル・コンピューターからファイルを「プル」することを選択できます。プッシュを許可しないセキュリティ・ポリシーが適用されている場合を除き、ほとんどのケースで、ファイルのプッシュを選択します。

接続方式

リモート・コンピューターに接続するには、**サービス・コントロール・マネージャー (SCM)** を使用することをお勧めします。SCM が動作しない場合は、**タスク・スケジューラー**を使用してください。

インストール先のパス

クライアントのパスを指定します。またはデフォルトをそのまま使用します (推奨)。

確認 インストールが完了するまで待機した後にクライアント・サービスが実行されていることを確認し、インストールが正常に完了したかどうかを識別するには、このボックスにチェック・マークを付けます。

カスタム設定

名前と値のペアの形式で、インストールする各クライアントにカスタム設定を追加します。

6. インストールを開始するには、「**開始**」をクリックします。
7. 完了すると、成功と失敗のログが表示されます。単に再試行することで、一部の失敗は解決できます。これで解決されない場合は、詳細オプションを使用します。詳しくは、**IBM Endpoint Manager サポート・サイト**のクライアントのインストールに関する記事を参照してください。

クライアントの手動インストール:

各コンピューターでクライアント・インストーラーを実行することにより、**IBM Endpoint Manager** クライアントを手動でインストールすることができます。少数のコンピューターにクライアントをインストールする場合に、この方法を使用します。

1. 以下のいずれかの方法でクライアントをインストールすることができます。
 - 管理者特権を持ってコンピューターにログオンし、**BES Installers¥Client** フォルダーを、インストール・コンピューターからローカル・ハード・ディスクにコピーします。
 - インストール・ガイド (「**スタート**」>「**すべてのプログラム**」>「**IBM Endpoint Manager**」>「**IBM Endpoint Manager インストール・ガイド**」を選択) を実行し、「**インストール・フォルダーの参照**」ボタンをクリックして **IBM Endpoint Manager** のインストーラー・フォルダーを開き、**クライアント・フォルダー**を表示します。
2. 「クライアント」フォルダーを対象のコンピューターにコピーしたら、そのフォルダーから **setup.exe** をダブルクリックしてインストーラーを起動します。
3. ウェルカム・パネルが表示された後、ソフトウェアをインストールするロケーションの入力を求めるプロンプトが出されます。デフォルトを受け入れることも、「**参照**」をクリックして、異なるロケーションを選択することもできます。

4. ファイルが移動されたら、「終了」をクリックしてインストーラーを終了します。これで IBM Endpoint Manager クライアント・アプリケーションがインストールされ、バックグラウンドで自動的に作業を開始します。ネットワーク内の、IBM Endpoint Manager の管理下に置きたいすべてのコンピュータで、このプロセスを繰り返します。

MSI を使用したクライアントのインストール:

クライアントの Microsoft Installer (MSI) パージョンを使用して、パッケージを解釈し、インストールを自動的に実行することができます。クライアントの MSI パージョン (BESClientMSI.msi) は、Windows サーバーの BESInstallers¥ClientMSI フォルダーまたは Linux サーバーの /ServerInstaller_9.1.xxx.x-rhe6.x86_64/repos/ClientMSI フォルダーに格納されています。

Windows クライアントをインストールするには、以下の手順を実行します。

1. Windows システムの c:¥BESInstallers¥ClientMSI フォルダーに BESClientMSI.msi プログラムをコピーします。
2. 以下のいずれかの方法で BESClientMSI.msi プログラムを実行します。

- `msiexec.exe /i c:¥BESInstallers¥ClientMSI¥BESClientMSI.msi /T=TransformList /qn`

¥qn コマンドはサイレント・インストールを実行します。

- `msiexec.exe /i c:¥BESInstallers¥ClientMSI¥BESClientMSI.msi INSTALLDIR="c:¥myclient" /T=TransformList`

このコマンドは、指定されたディレクトリー (INSTALLDIR="c:¥myclient") にプログラムをインストールします。

注: /T=TransformList は、パッケージに適用する必要があるトランスフォーム・ファイル (.mst) を指定します。TransformList は、セミコロンで区切られたパスのリストです。以下の表に、提供されているトランスフォーム・ファイル、結果として得られる言語、および **msiexec** コマンド行で使用する数値を示します。

表 2. トランスフォーム・ファイル・リスト

言語	トランスフォーム・ファイル名	値
米国英語	1033.mst	1033
ドイツ語	1031.mst	1031
フランス語	1036.mst	1036
スペイン語	1034.mst	1034
イタリア語	1040.mst	1040
ブラジル・ポルトガル語	1046.mst	1046
日本語	1041.mst	1041
韓国語	1042.mst	1042
中国語 (簡体字)	2052.mst	2052
中国語 (繁体字)	1028.mst	1028

Microsoft のサイト **Command-Line Options** に、インストール・オプションの全リストが掲載されています。BESClientMSI 適用環境のグループ・ポリシー・オブジェクト (GPO) を作成する方法については、Microsoft サポート技術情報の記事 (<http://support.microsoft.com/kb/887405>) を参照してください。

3. クライアントを開始する前に、Endpoint Manager サーバーにある `actionsite.afxm` マストヘッドをクライアントのインストール・ディレクトリー (デフォルトのインストール・ディレクトリー `C:\Program Files (x86)\BigFix Enterprise\BES Client` または特定のインストール・ディレクトリー `INSTALLDIR="c:\myclient"` にすることができます) にコピーします。
4. BES クライアント・サービスを開始します。

ソフトウェア配布ツールの使用:

Microsoft SMS、IBM Tivoli、CA Unicenter、Novell ZENworks などのソフトウェア配布ツールにアクセスでき、インストール先のすべてのコンピューターでそのツールが有効になっている場合、そのツールを使用してクライアントのインストール・パッケージをインストールすることができます。

注: インフラストラクチャーおよびインストール手順が既に確立されているため、これは、企業にインストールするための最も効率的な方法です。

グループ・ポリシーの使用:

Active Directory グループ・ポリシー・オブジェクト (GPO) を使用して、特定のグループ (組織単位やドメインなど) 内のすべてのマシンにクライアントをインストールすることを必須とするポリシーを定義することができます。GPO が有効である場合、このポリシーは、ユーザーが指定のドメインにログインするたびに適用されます。このため、このポリシーは、クライアントをインストールする非常に効果的な方法です。詳しくは、Active Directory 管理者にお問い合わせください。

ログイン・スクリプトの使用:

NT ドメインまたは AD ドメインで、クライアントの存在の有無を検査するログイン・スクリプトを作成することができます。ユーザーがログインし、クライアントが存在しないことを検出した場合、そのコンピューターは、グローバル・ファイル共有の指定のロケーションにあるクライアント・インストーラーに自動的にアクセスできます。サポート・サイトに、ログイン・スクリプトのサンプルに関する知識ベースの記事 (キーワード: `example login script`)、およびクライアントをインストールするためのログイン・スクリプトの使用法に関する指示があります。

ネットワークに新しいコンピューターを必要に応じて追加する予定の場合、この方法を使用すると、新しいマシンが自動的にサーバーによって検出されて管理されます。ただし、Windows 2000 または XP を使用している一部のネットワークでこの方法を実行するには、ユーザーは管理者特権を使用してログインする必要があります。

これらのログイン・スクリプトは、Windows インストーラーに基づくセットアップに引数を渡します。setup.exe のコマンド・ライン・オプションについて詳しくは、InstallShield のサポート Web サイト (<http://kb.flexerasoftware.com/doc/Helpnet/>)

isxhelp12/IHelpSetup_EXECmdLine.htm) を参照してください。ここには、ログイン・スクリプトで利用できる、クライアント・インストーラー用のコマンド・ライン・スイッチの例がいくつかあります。

- ・ クライアントをサイレントでインストールし、一方でログをディレクトリー C:\%書き込むには、次の形式の DOS コマンドを実行します。

```
setup.exe /s /v/l*voicewarmup %"C:\%besclientinstall.log%" SETUPEXE=1 /qn"
```

- ・ デフォルトのインストール・ロケーションを変更するには、次の形式のコマンドを使用します。

```
setup.exe /s /v/l*voicewarmup %"C:\%besclientinstall.log%"  
INSTALLDIR=%"<InstallPath%" SETUPEXE=1 /qn"
```

<InstallPath> は、クライアントをインストールする先のフォルダーの Windows 形式の絶対パスです。

注: setup.exe を実行する Windows ユーザーは、コンピューターの管理者特権を所有している必要があり、また「setup.exe」ファイルが含まれる同じフォルダーにログ・ファイルを書き込むことができる必要があります。そうでない場合、インストールは失敗し、ログ・ファイルは作成されません。

一般的なビルドへの埋め込み:

組織で、CD 上の特定のビルド・イメージまたは共通操作環境 (COE) か、あるいは新規コンピューターの準備に使用されるイメージを使用している場合、クライアントをこのビルドに含めることができます。イメージを作成するには、以下の手順に従います。

Windows オペレーティング・システムの場合:

1. イメージを作成するコンピューター上にクライアントをインストールします。
IBM Endpoint Manager クライアントは、直ちにサーバーへの接続を試みます。サーバーに正常に接続した場合、**ComputerID** が割り当てられます。この **ComputerID** は、その特定のコンピューターに固有であるため、共通ビルド・イメージの一部であってはなりません。次の手順によって、この ID が削除されます。
2. 「Windows サービス」ダイアログを開き、「**BES クライアント・サービス**」を停止することによって、クライアントを停止します。
3. レジストリーの HKLM\Software\BigFix\EnterpriseClient\GlobalOptions (64 ビット・システムの場合、レジストリーは HKLM\Software\Wow6432Node\BigFix\EnterpriseClient\GlobalOptions) を開き、ComputerID、RegCount、および ReportSequenceNumber の各値を削除して、コンピューター固有の ID (コンピューター ID) を削除します。

これで、IBM Endpoint Manager クライアントのイメージを作成できるようになります。

注: クライアントが何らかの理由で再度始動された場合 (システム再始動を含む)、クライアントはサーバーに再登録するため、**ステップ 2 から 3 までを再度実行する必要があります**。サーバーには競合検出機能と解決機能が組み込まれているため、何らかの理由で ID を削除できなかった場合、サーバーは、同じ **ComputerID**

を持つ複数のクライアントが存在することを検出し、すべて正常に機能するようにクライアントを強制的に再登録します。ただし、上記の手順を実行して、コンソールのコンピューター・リスト内に灰色で表示されるクライアント（最初にイメージが作成されたコンピューター）が含まないようにすることをお勧めします。

Linux オペレーティング・システムの場合:

1. イメージを作成するコンピューター上にクライアントをインストールします。
2. `/etc/init/besclient stop` を実行して、クライアントを停止します。
3. コンピューター固有の ID を `.config` ファイルから削除して、マシンのすべてのコピーが同じクライアント ID でサーバーに登録されないようにします。

これで、IBM Endpoint Manager クライアントのイメージを作成できるようになります。

Macintosh オペレーティング・システムの場合:

1. イメージを作成するコンピューター上にクライアントをインストールします。
2. **`sudo systemstarter stop BESClient`** を使用して、クライアントを停止します。
3. コンピューター固有の ID を削除して、マシンのすべてのコピーが同じクライアント ID でサーバーに登録されないようにします。
 - それらが存在する場合は、**RegCount**、**ReportSequenceNumber**、および **ComputerID** をクライアント環境設定フォルダー `/Library/Preferences/com.bigfix.besagent.plist` から削除します。
 - `__BESData` フォルダーを削除します。デフォルトのロケーションは `¥Library¥Application Support¥BigFix¥BES Agent` です。

これで、IBM Endpoint Manager クライアントのイメージを作成できるようになります。

電子メールの使用:

URL が記載され、ネットワークへのログイン時に、その URL を使用してクライアントをインストールするように要求する電子メールをユーザーに送信できます。Win9x プラットフォームではユーザー権限に関する制限がないため、電子メールの使用は Win9x コンピューターに対して有効な方法です。ただし、管理権限が実行される場合、この方法では、ユーザーは管理者特権を使用してログインする必要があります。

クライアントでの暗号化の有効化:

クライアントがインストールされたら、出力されるすべてのレポートを暗号化して、クレジット・カード番号、パスワード、およびその他の機密情報などのデータを保護するように、クライアントをセットアップすることができます。

注: クライアント用に暗号化を有効にする前に、適用環境で暗号化を有効にしておく必要があります。特に、最初に適用環境を設定せずに必須オプションを有効にした場合、クライアントは動作を停止します。

暗号化を有効にするには、以下の手順に従います。

1. 「BigFix 管理」ドメインから、「コンピューター管理」フォルダーを開き、「コンピューター」ノードをクリックします。
2. 暗号化を使用するコンピューターまたはコンピューターのセットを選択します。
3. 右クリック・コンテキスト・メニューから、「コンピューターの設定を編集」を選択します。
4. 「設定の編集」ダイアログから「追加」をクリックします。
5. 「カスタム設定を追加」ダイアログで、設定名を次のように入力します。

BESClient_Report_Encryption (名前の先頭がアンダーラインであることに注意してください)。

以下に、この設定で利用できる 3 つの値を示します。

必須 クライアントが常に暗号化を行います。マストヘッドに使用可能な暗号化証明書がない場合、または対象のコンピューター (リレーまたはサーバー) が暗号化を受け入れることができない場合、クライアントはレポートを送信しません。

オプション

クライアントは、可能な場合は暗号化を行い、暗号化できない場合はレポートを平文で送信します。

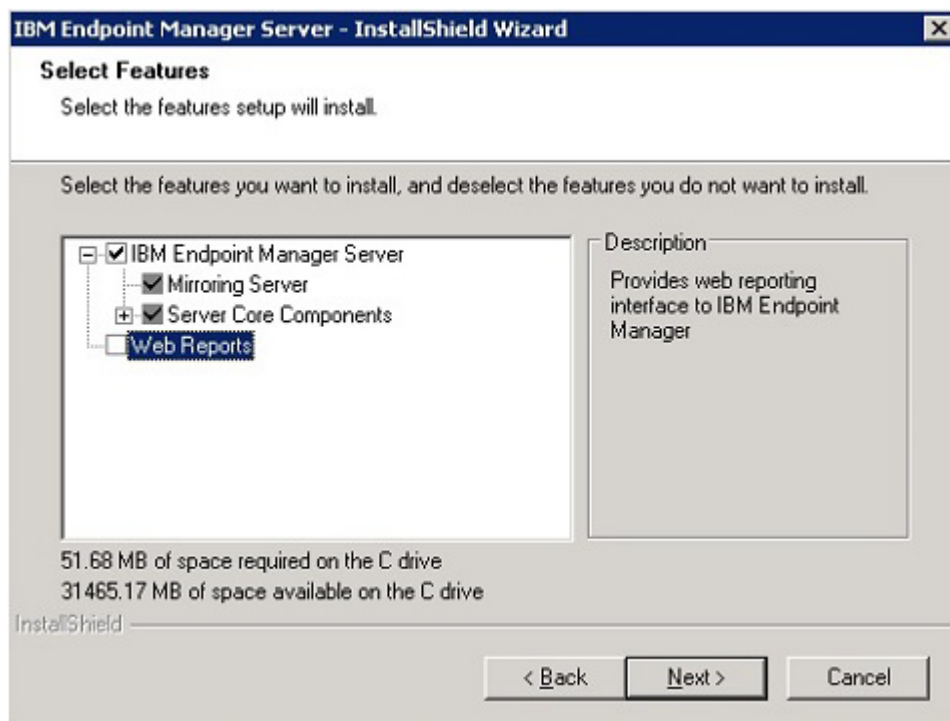
なし 暗号化証明書が存在する場合でも、暗号化は行われません。この設定により、暗号化を有効にした後で、暗号化をオフにすることができます。

6. 「OK」をクリックして値を受け入れ、もう一度「OK」をクリックして設定を完了します。設定アクションを適用するには、プライベート・キー・パスワードを入力する必要があります。

暗号化に関する追加情報については、85 ページの『暗号化』を参照してください。

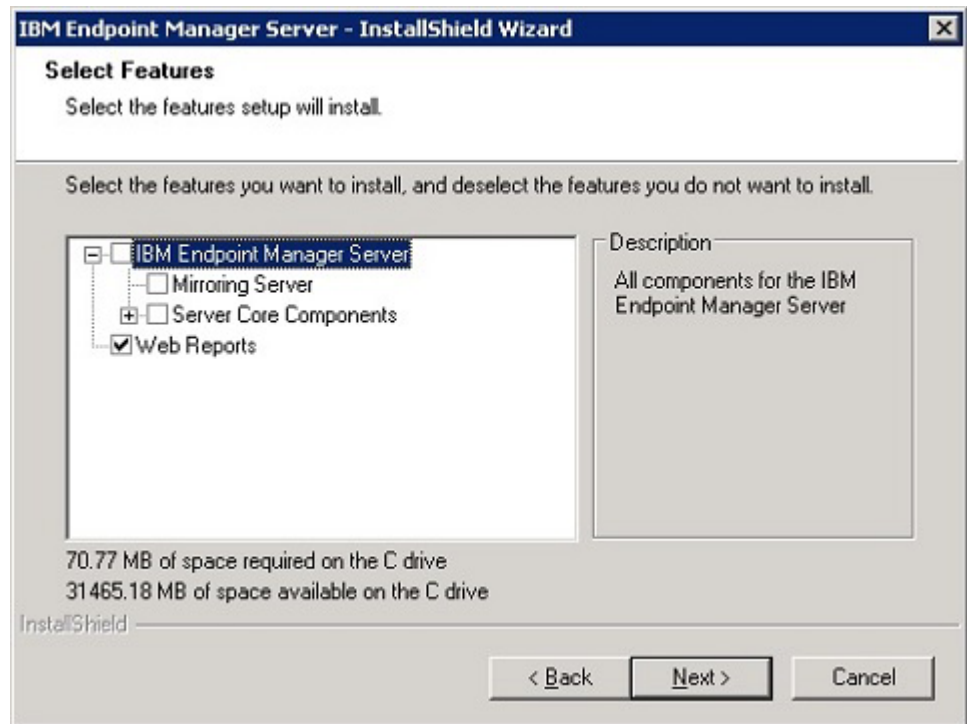
Web レポートのインストール

デフォルトでは、Web レポート・コンポーネントは IBM Endpoint Manager サーバーとともにインストールされます。ただし、以下のインストール・パネルでチェック・マークを外すと、このコンポーネントはインストールされません。



後で IBM Endpoint Manager サーバーと同じシステムにインストールする場合や、別のシステムにスタンドアロンとしてインストールする場合は、以下の手順を実行します。

1. インストール・ガイドを実行します (「スタート」>「すべてのプログラム」>「IBM Endpoint Manager」>「IBM Endpoint Manager インストール・ガイド」)。
2. 「サーバーのインストール」を選択します。
3. IBM Endpoint Manager サーバーのインストール時に生成されたマストヘッドを使用することを選択します。
4. 以下のパネルで、Web レポート・コンポーネントのみをインストールすることを選択します。



5. 構成に適用されるデータベース・オプションを選択して、完了します。
6. インストール・パラメーターを確認し、「次へ」をクリックしてインストールを起動します。

IBM Endpoint Manager 管理ツールの実行

IBM Endpoint Manager 管理ツールは、インストーラーでコンソール・プログラムの他のコンポーネントをインストールすると、自動的に作成されます。このプログラムは、管理オペレーター専用であり、コンソールとは独立して動作します。このプログラムには「スタート」メニューからアクセスできます（「スタート」>「すべてのプログラム」>「IBM Endpoint Manager」>「IBM Endpoint Manager 管理ツール」）。このプログラムを実行するには、最初にプライベート・キー (license.pvk) を参照する必要があります。

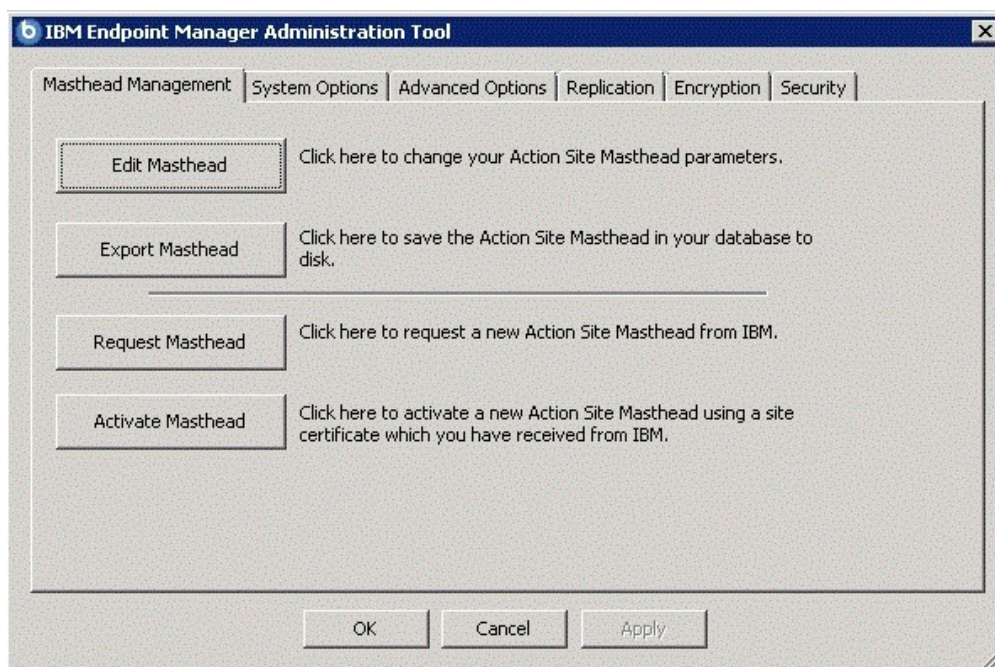
このインターフェースを通じて、管理者パスワードを変更することもできます。プライベート・キー・ファイルを選択した後、「OK」をクリックして続行します。先に進むには、プライベート・キーのパスワードを指定する必要があります。

注： 秘密鍵のパスワードの変更では、ローカル・ファイルのパスワードのみが変更され、それ以外の DSA Endpoint Manager サーバーは更新されません。変更後のライセンス・ファイルで置き換えない限り、それらには引き続き各自のライセンス・ファイルおよびパスワードが使用されます。

ユーザー管理タスクの実行には Endpoint Manager コンソールを使用します。

マストヘッドの管理:

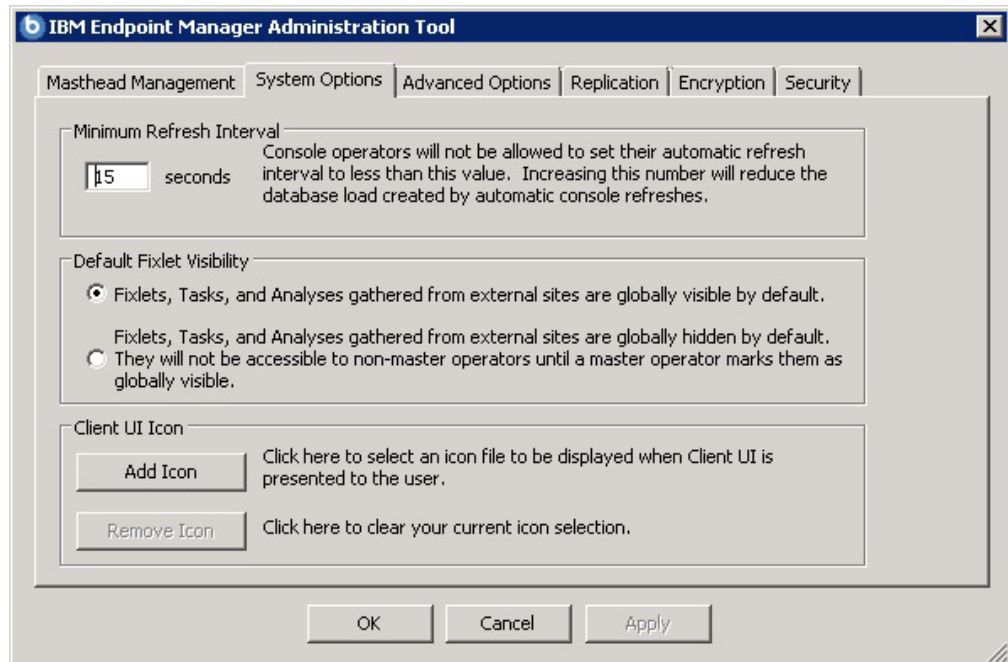
最初のタブをクリックして、「マストヘッドの管理」ダイアログを表示します。



コンソールを実行するために必要なマストヘッドがまだない場合、このダイアログにより、新しいマストヘッドを**要求**してから**アクティブ化**するためのインターフェースが表示されます。既存のマストヘッドがある場合、それを編集して収集間隔とロック設定を変更できます。マストヘッドの管理について詳しくは、「*IBM Endpoint Manager 構成ガイド*」を参照してください。マストヘッドはエクスポートすることもできます。これは、IBM Endpoint Manager ネットワークを他のサーバーに拡張する場合に便利です。

システム・オプション:

2 番目のタブでは、「システム・オプション」ダイアログが開きます。1 番目のオプションで、更新間隔の基準最小値が設定されます。これは、コンソールの「環境設定」ダイアログで指定された、Fixlet リストの更新間隔を示します。デフォルトの間隔は 15 秒ですが、ネットワークの帯域幅に余裕がある場合、この数値を小さくすることで、コンソールの応答性を向上させることができます。反対に、ネットワークに余裕がない場合、この最小値を増やすことが望ましいです。

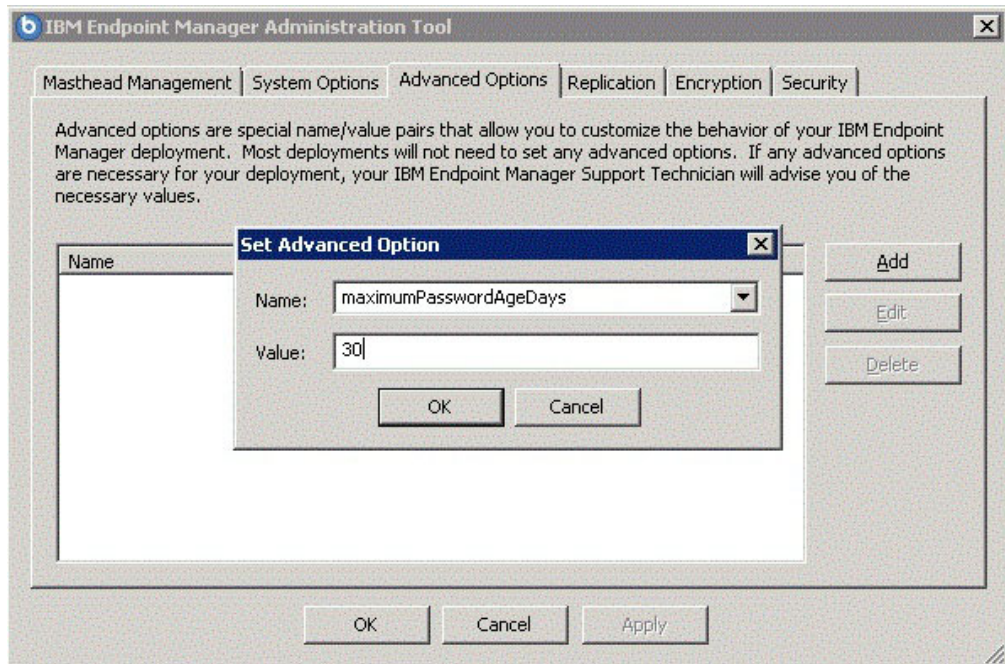


このダイアログを使用して、外部サイトのデフォルトの表示設定を指定します。外部サイトは、デフォルトで、すべてのコンソール・オペレーターに対してグローバルに表示されます。表示設定をさらに制御するには、表示設定を非表示に設定してから、コンソールを通じて表示設定を個別に調整することができます。非表示のサイトを表示可能にするには、管理者またはマスター・オペレーターである必要があります。

このダイアログを使用して、クライアント経由でユーザーに表示されるコンテンツに独自のロゴを追加します。商標の追加は重要です。これは、情報に企業の承認があるとユーザーが安心できるからです。

詳細オプション:

3 番目のタブで、「詳細オプション」ダイアログが開きます。このダイアログでは、ご使用の特定のインストール済み環境に適用されるグローバル設定がリストされます。



これらのオプションは名前と値のペアであり、通常 IBM ソフトウェア・サポートによって提供されます。例として、電源管理サイトをサブスクライブしている場合、これらのオプションの 1 つによって、WakeOnLAN 機能を有効にすることができます。指定可能な詳細オプションの一部を以下に示します。

表 3. 詳細設定の名称

名前	値
loginWarningBanner	テキストを設定すると、コンソールまたは Web レポートにログインしたすべてのユーザーに対して、そのテキストが表示されます。ユーザーが次に進むには「 OK 」をクリックする必要があります。
timeoutLockMinutes	コンソールで再認証が必要になるまでのアイドル時間 (分単位)。これは loginTimeoutSeconds とは異なります。このタイムアウト・ロックではコンソール全体が表示されなくなるため、他のユーザーは、コンソールを表示することも使用することもできなくなります。アイドル時間は、キー・ボタン、マウス・クリック、マウス移動など、セッション内でどのような種類の入力も行われない状態を指します。

注: 非効率的な MIME 拡張オプションは 9.1 サーバーでサポートされなくなりました。既存のアクションは引き続きクライアントで実行されますが、サーバーは非効率的な MIME アクションを生成することはできません。

レプリケーション:

4 番目のタブでは、「レプリケーション」ダイアログが開きます。このダイアログを使用して、レプリケーション・サーバーを視覚化します。詳しくは、「構成ガイド」を参照してください。

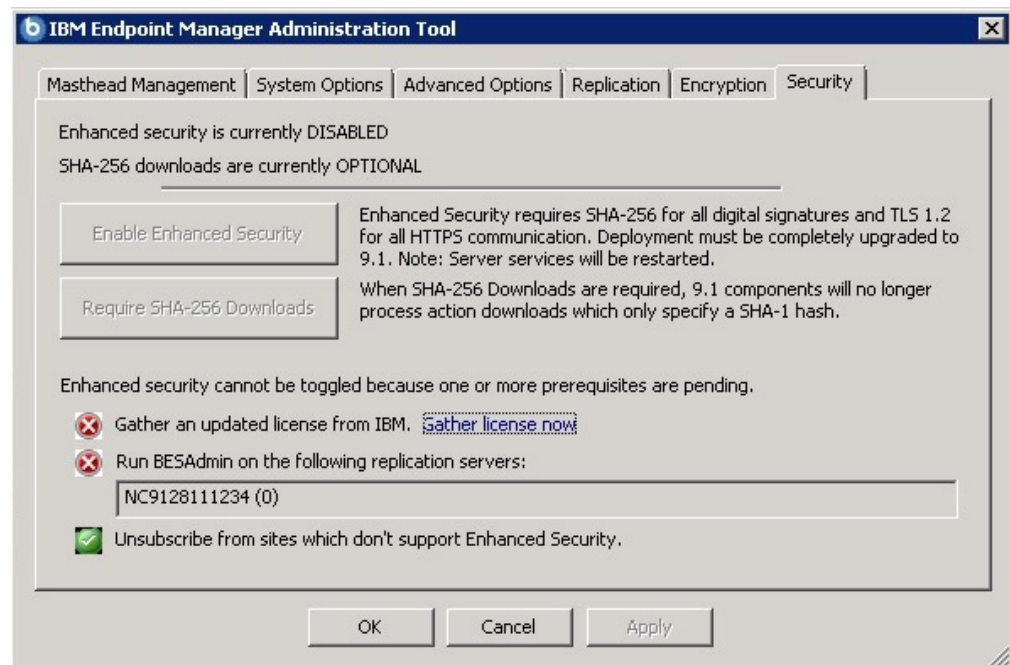
暗号化:

5 番目のタブで、「暗号化」ダイアログが開きます。このダイアログを使用して、新しい暗号化キーを生成するか、暗号化を完全に無効にします。詳しくは、「構成ガイド」を参照してください。

セキュリティー:

6 番目のタブをクリックして「セキュリティー」ダイアログを開きます。

サーバーをインストールした後、初めて「セキュリティー」タブにアクセスするときに、以下の情報が表示されます。



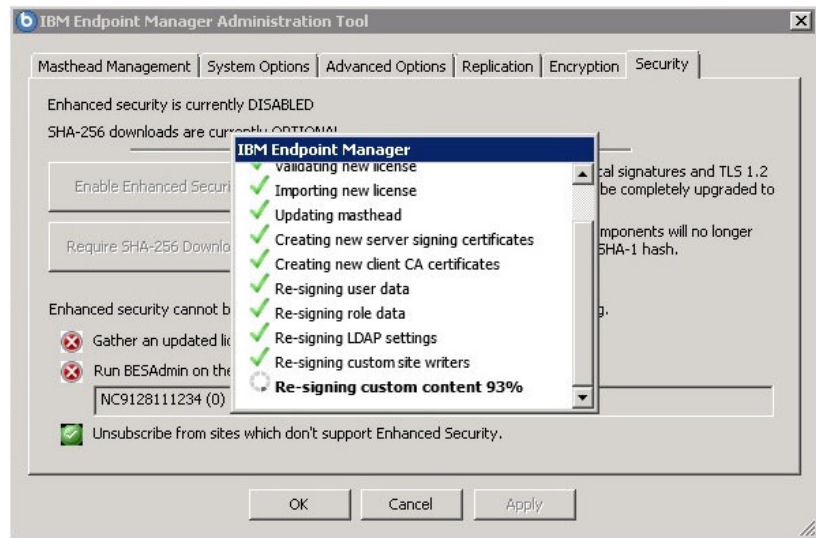
以下のチェック・マークは、製品によって自動的に更新されます。

更新ライセンスを IBM から収集します

このチェック・マークは、以下の状態を示します。

緑色 更新されたライセンスが IBM サイトからダウンロードされ、すべてのクライアントに配布されました。

赤色 サーバーに保管されているライセンスが、IBM サイトに保管されているライセンスと同期していません。サーバー上のライセンスを更新するには、「**今すぐライセンスを収集する (Gather license now)**」をクリックします。「**今すぐライセンスを収集する (Gather license now)**」をクリックすると、更新されたライセンスが IBM サイトから自動的に収集され、IBM Endpoint Manager クライアントに配布されます。



ライセンス処理が完了すると、チェック・マークのステータスは自動的に更新されます。

次の複製サーバー上で BESAdmin を実行してください

レプリケーション・サーバーを定義した場合、このチェック・マークは以下の状態を示します。

緑色 すべてのレプリケーション・サーバーに IBM Endpoint Manager バージョン 9.1 がインストールされていて、更新されたライセンスがあります。

赤色 DSA 構成内の少なくとも 1 つのサーバーが上記の条件を満たしていません。この状態を修正するには次のようにします。

1. 「更新ライセンスを IBM から収集します」チェック・マークが緑色であることを確認します。
2. チェック・マークの下にリストされたレプリケーション・サーバーに IBM Endpoint Manager バージョン 9.1 がインストールされていることを確認します。
3. デフォルトでは、レプリケーションは 5 分間隔で発生しますが、「IBM Endpoint Manager 管理ツール」の「レプリケーション」タブで別の間隔を指定できます。すべてのサーバーでレプリケーションが実行され、更新されたライセンスが配布された後に、それらのレプリケーション・サーバーで **BESAdmin** を実行して、それぞれのライセンスを更新します。
4. **IBM Endpoint Manager 管理ツール**を再起動すると、「セキュリティ」タブのチェック・マークのステータスが更新されます。

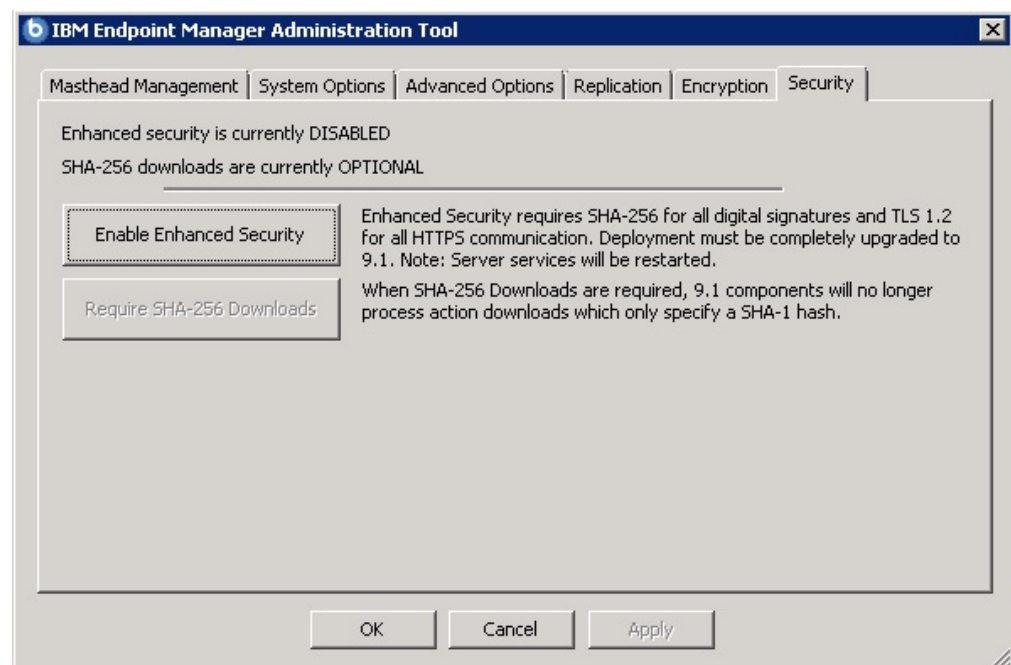
拡張セキュリティーをサポートしていないサイトのサブスクリプションを解除します このチェック・マークは、以下の状態を示します。

緑色 サブスクリプションしているすべてのサイトで拡張セキュリティー機能がサポートされています。つまり、すべてのデジタル署名とコンテンツ検証で SHA-256 暗号ダイジェスト・アルゴリズムがサポートされます。

赤色 サブスクライブしているサイトの少なくとも 1 つで、拡張セキュリティ機能がサポートされていません。この状態を修正するには、チェック・マークの下にリストされたサイトからサブスクライブを解除します。その後、管理ツールにもう一度アクセスして、チェック・マークのステータスを更新します。

3 つのチェック・マークのいずれかが赤色の場合、製品は、IBM Endpoint Manager バージョン 9.0 によって提供されるセキュリティ動作を使用します。

3 つの前提条件が満たされていると、「セキュリティ」タブで「拡張セキュリティを有効にする」ボタンが有効になり、IBM Endpoint Manager 環境で「拡張セキュリティを有効にする」機能を使用することを選択できます。



「拡張セキュリティを有効にする」ボタンをクリックすると、すべてのデジタル署名とコンテンツ検証に SHA-256 暗号ダイジェスト・アルゴリズムが採用され、Endpoint Manager コンポーネント間通信に TLS 1.2 プロトコルが使用されます。

注: この設定を使用する場合、IBM Endpoint Manager バージョン 9.0 以前のコンポーネントは IBM Endpoint Manager バージョン 9.1 のサーバーやリレーと通信できないため、後方互換性が失われます。

「拡張セキュリティを有効にする」ボタンをクリックするまで、「SHA-256 ダウンロードが必要 (Require SHA-256 Downloads)」ボタンは無効になっています。

「SHA-256 ダウンロードが必要 (Require SHA-256 Downloads)」ボタンをクリックすると、すべてのダウンロード検証で SHA-256 アルゴリズムのみを使用するように変更されます。既存のカスタム・アクションは、V9.1 用に更新された **prefetch** アクション・スクリプト構文に準拠するように編集しなければならない可能性があります。

注: このオプションを選択しない場合、ファイル・ダウンロードの整合性チェックは SHA-1 アルゴリズムを使用して実行されます。

IBM Endpoint Manager の拡張セキュリティー機能およびサポートされるセキュリティー構成については、27 ページの『第 4 章 セキュリティー構成シナリオ』を参照してください。

追加の管理コマンド

インストールを実行すると、IBM Endpoint Manager 管理ツールのプログラム BESAdmin.exe が C:\Program Files (x86)\BigFix Enterprise\BES Server ディレクトリーに自動的にダウンロードされます。

スクリプト BESAdmin.exe により、追加の操作を実行することができます。このスクリプトをコマンド・プロンプトから実行するには、以下のコマンドを実行します。

```
.\BESAdmin.exe /service { arguments | /h }
```

指定の内容は以下のとおりです。

service は以下のいずれかにすることができます。

```
converttoldapoperators  
createuser  
deleteuser  
edituser  
findinvalidsignatures  
resignsecuritydata  
rotateserversigningkey  
setproxy
```

各サービスには、以下の引数 があります。

converttoldapoperators

ローカル・オペレーターは、LDAP オペレーターに変換することができます。そのため、このオペレーターは LDAP 資格情報を使用してログインすることができます。オプションで、*-mappingFile* 引数を使用してファイルを指定することができます。これをマッピング・ファイルと呼びます。マッピング・ファイルの各行に、変換対象のユーザー名、タブ、LDAP/AD でのユーザー名を順に記述します。名前は、ユーザーがコンソールにログインする際に使用する形式で指定してください (*domain\user*、*user@domain*、または *user*)。マッピング・ファイルを指定しなかった場合は、LDAP/AD でのユーザー名がローカルのユーザー名と同じであるという前提ですべてのユーザーが変換されます。

このサービスを実行するための構文は以下のとおりです。

```
.\BESAdmin.exe /convertToLDAPOperators [/mappingFile:<file>]
```

createuser

コンソールにアクセスするオペレーターのアカウントを作成することができます。セキュリティーのために、パスワードで保護されたパブリック・キーとプライベート・キーも生成され、新規オペレーターが正しくアクションを作成して署名できるようになります。

このサービスを実行するための構文は以下のとおりです。

```
.\BESAdmin.exe /createUser <UserName>  
/userPassword:<UserPassword>  
/masterOp:<yes|no>
```



```
/customContent:<yes|no>  
/showotherusersactions:<yes|no>  
/unmanagedAssetPrivilege:<all|none|scanpoint>
```

オプションで、以下のパラメーターを指定することができます。

masterOp

ユーザーがマスター・オペレーターであるかどうかを指定します。デフォルト値は **yes** です。

customContent

ユーザーがカスタム・コンテンツを作成できるかどうかを指定します。デフォルト値は **yes** です。

showotherusersactions

ユーザーが、管理対象コンピューターに影響する他のユーザーによるアクションを表示できるかどうかを指定します。デフォルト値は **yes** です。

unmanagedAssetPrivilege

ユーザーが表示できる非管理資産を定義します。デフォルト値は **scanpoint** です。

deleteuser

マスター以外のオペレーターに削除済みのマークを付けることができます。このコマンドを実行するとオペレーター・インスタンスがデータベースから削除されますが、オペレーターが作成したコンテンツは削除されません。

このサービスを実行するための構文は以下のとおりです。

```
.\BESAdmin.exe /deleteUser <UserName>
```

editUser

このサービスを実行するための構文は以下のとおりです。

```
.\BESAdmin.exe /editUser <UserName>  
/loginPermission:<always|never|role>  
/customContent:<yes|no>  
/showOtherUsersActions:<yes|no>  
/unmanagedAssetPrivilege:<all|none|scanpoint>
```

オプションで、**createUser** でサポートされるパラメーターと同じパラメーターを指定することができます。ただし、**masterOp** は **createUser** でのみサポートされます。また、**loginPermission** は **editUser** でのみサポートされ、以下のよう動作します。

loginPermission

どの場合にユーザーがログインできるかを指定します。デフォルト値は **always** です。この場合、ユーザーはいつでもログインすることができます。値に **never** を指定すると、ユーザーは一切ログインできなくなります。値に **role** を指定すると、ユーザーが特定の役割のメンバーである場合にログインすることができます。このパラメーターを使用して、オペレーターのログインを無効にしたり、特定の役割を LDAP グループに割り当ててその LDAP グループ内のすべてのユーザーがログインできるようにしたりします。

findinvalidsignatures

以下のパラメーターを指定することにより、データベース内のオブジェクトの署名を検査することができます。

-resignInvalidSignatures (オプション)

BESAdmin が検出したすべての無効な署名への再署名を試行します。

-deleteInvalidlySignedContent (オプション)

無効な署名を持つコンテンツを削除します。

無効な署名について詳しくは、<http://www-01.ibm.com/support/docview.wss?uid=swg21587965>を参照してください。

このサービスを実行するための構文は以下のとおりです。

```
.¥BESAdmin.exe /findinvalidsignatures  
[ /resignInvalidSignatures | /deleteInvalidlySignedContent ]
```

resignsecuritydata

データベース内のすべてのユーザー・コンテンツに再署名して、コンソールへのユーザー・ログインを可能にすることができます。このコマンドは、既存のキー・ファイルを使用してセキュリティー・データに再署名します。以下のパラメーターを指定することができます。

/mastheadLocation=<path+/actionsite.afxm>

このサービスを実行するための完全な構文は以下のとおりです。

```
.¥BESAdmin.exe /resignsecuritydata /sitePvkLocation=<path+license.pvk>  
[ /sitePvkPassword=<password> ] /mastheadLocation=<path+/actionsite.afxm>
```

rotateserversigningkey

サーバー・プライベート・キーをローテーションして、ファイル・システム内のキーをデータベース内のキーに一致させることができます。このコマンドは、新しいサーバー署名キーを作成し、その新しいキーを使用してすべての既存のコンテンツに再署名し、古いキーを取り消します。

このサービスを実行するための構文は以下のとおりです。

```
.¥BESAdmin.exe /rotateserversigningkey /sitePvkLocation=<path+license.pvk>  
[ /sitePvkPassword=<password> ]
```

setproxy

企業でプロキシを使用してインターネットにアクセスする場合は、プロキシ接続を設定して、IBM Endpoint Manager サーバーがサイトからコンテンツを収集できるようにする必要があります。また、コンポーネント間通信やファイルのダウンロードもできるようにする必要があります。

インターネットにアクセスする BES コンポーネントは、デフォルトでは、Windows サーバーの SYSTEM アカウントとして実行されます。

プロキシ構成は、レジストリー内でキー

HKEY_LOCAL_MACHINE¥SOFTWARE¥BigFix¥Enterprise Server¥Proxy によって管理されます。

以下のコマンドを実行して、レジストリーで

HKEY_LOCAL_MACHINE¥SOFTWARE¥BigFix¥Enterprise Server¥Proxy キーを作成または変更します。

```
BESAdmin /setproxy /proxy:<proxy_host> /user:<proxy_username>  
/pass:<proxy_password> [/exceptionlist:<proxy_exceptionlist>]
```

コマンドの実行方法と各引数で使用する値については、163 ページの『プロキシ接続の サーバー上での設定』を参照してください。

Windows システム上のプライマリー・サーバーの削除

IBM Endpoint Manager サーバーをアンインストールするには、サーバー、クライアント、Web レポート・コンポーネント、および関連するデータベースを削除する必要があります。

Windows システム上のプライマリー・サーバーをアンインストールするには、以下の手順を実行します。

1. 『TEM Remove Utility』から **BESRemove.exe** ユーティリティをダウンロードします。
2. **BESRemove.exe** をダブルクリックしてユーティリティを実行します。

注: **BESRemove.exe** ユーティリティでは、IBM Endpoint Manager V9.1 と共にインストールされた Microsoft SQL Server 2005 インスタンスは削除されません。

Windows レプリケーション・サーバーのアンインストール

レプリケーション・サーバーをアンインストールするには、データベース・ストアド・プロシージャ **delete_replication_server** を呼び出します。これにより、指定した ID がレプリケーション・セットから削除されます。対象外のサーバーを削除しないように注意してください。削除すると、ユーザー本人がロックアウトされる場合があります。このプロシージャの詳細は本書の対象範囲外ですが、基本的には、SQL Server Management Studio を使用してデータベースにログインする必要があります。このプロシージャは以下のようにして呼び出すことができます。

```
call dbo.delete_replication_server(n)
```

ここで *n* は、削除するサーバーの ID です。

サーバーの完全な削除に関する手順は本書の対象範囲外ですが、IBM Endpoint Manager サポート・サイトの KB の記事で完全な手順を参照できます。

第 9 章 Linux システムでのインストール

用語と管理役割について理解すると、実際に許可を受けてプログラムをインストールする準備が整います。

IBM Endpoint Manager が強力であるため、アクセスを、信頼できる許可されたスタッフのみに制限したいと考えます。このプログラムは、「**アクション サイト**」と呼ばれる Fixlet アクションの中央リポジトリに依存します。このリポジトリは、パブリック・キー/プライベート・キー暗号化を使用して、スプーフィングやその他の許可されない使用法から保護します。開始するには、**ライセンス認証ファイル** (このファイルには `CompanyName.BESLicenseAuthorization` などの名前が付いています) を取得して、IBM から許可を受ける必要があります。

インストール・プログラムは、適用環境に関する詳細な情報を収集してから、**アクション・サイト・マストヘッド**と呼ばれるファイルを作成します。このファイルは、組織内の IBM Endpoint Manager の root からコンソール・オペレーターまでの権限のチェーンを設定します。マストヘッドは、構成情報 (IP アドレス、ポートなど) とライセンス情報 (許可されるクライアントの数および許可される期間) を、デジタル署名を確認するために使用されるパブリック・キーと共に結合したものです。

DB2 のインストールと構成

インストールする DB2 のバージョンに従い、Endpoint Manager サーバーをインストールする前に DB2 をインストールするか、または同時にインストールします。

- **DB2 V10.5 Enterprise Server Edition:** Enterprise Server Edition をインストールする場合は、Endpoint Manager サーバーをインストールする前に、このバージョンの DB2 をインストールする必要があります。この DB2 は、Endpoint Manager サーバーのインストール先となるローカル・ワークステーションにインストールするか、またはリモート・ワークステーションにインストールしてください。Red Hat Enterprise Linux Server 64 ビットに DB2 サーバーをインストールする方法と、そのインストール済み環境を検証する方法について詳しくは、『*DB2 サーバーと IBM データ・サーバー・クライアント*』を参照してください。Endpoint Manager サーバーをインストールする前に、以下に示す手順で、DB2 V10.5 Enterprise Server Edition がインストールされて稼働していることを確認してください。
 - DB2 V10.5 Enterprise Server Edition がローカルにインストールされている場合:
 1. 以下のコマンドを実行して、ローカルの DB2 管理ユーザー (デフォルトは `db2inst1`) に切り替えます。

```
su - db2inst1
```
 2. コマンド `db2start` を実行して、DB2 インスタンスがアクティブであることを確認します。DB2 インスタンスが実行されている場合、以下のメッセージが表示されます。

SQL1026N データベース・マネージャーはすでにアクティブになっています

アクティブではない場合、DB2 インスタンスが開始されます。また、以下のコマンドを使用して、db2sysc プロセスがアクティブであることを確認することで検証することもできます。

```
ps -ef | grep db2sysc
```

- DB2 V10.5 Enterprise Server Edition がリモートにインストールされている場合:

1. DB2 10.5 クライアントをローカルにインストールし、リモート・ワークステーションにインストールされている DB2 10.5 サーバーにこのクライアントを接続します。追加の DB2 構成 (リモート・データベースのカatalog など) は必要ありません。DB2 クライアントをインストールするには、インストール・ウィザードを実行するか、応答ファイルを使用してサイレント・インストールを実行します。詳しくは、IBM データ・サーバー・クライアントのインストール方法を参照してください。
2. リモートの DB2 で、DB2 管理サーバー db2admin が開始され、リモート管理を行うことができることを確認します。db2admin を開始するには、以下のコマンドを実行します。

```
# su - dasusr1
# $ db2admin start
```

- **DB2 V10.5 Workgroup Server Edition:** これは、Endpoint Manager インストール・パッケージに含まれている DB2 バージョンです。ダウンロードする Endpoint Manager インストール・パッケージによっては、このバージョンの DB2 を、Endpoint Manager サーバーのインストール前に上記の手順に従ってインストールすることも、ダウンロード後に Endpoint Manager サーバーと一緒にインストールすることもできます。この DB2 は、Endpoint Manager サーバーのインストール先となるローカル・ワークステーションにダウンロードしてください。Endpoint Manager サーバーのインストール時に、以下の情報を指定する必要があります。

DB2 セットアップ・ロケーション

DB2 をダウンロードした場所のパス。デフォルトは ../wser/db2setup です。

DB2 管理ユーザー・パスワード

DB2 管理ユーザーのパスワード。

これにより、DB2 を構成するためのすべてのステップが、Endpoint Manager サーバーのインストール・プログラムによって実行されます。

リブート後に DB2 インスタンスを自動的に開始するには、以下の手順を実行します。

1. 以下のコマンドを実行します。

```
/opt/ibm/db2/V10.1/bin/db2iauto -on db2inst1
```

または、/etc/init.d ディレクトリーに、以下のコードが記述された db2auto.sh などのシェル・スクリプトを作成します。

```
#!/bin/sh
for i in `ls /opt/ibm/db2/V10.1/bin/db2ilist`;
do
su - $i -c "db2start"
done
```

2. 実行権 3 をスクリプトに付与し、「システム」->「環境設定」->「Startup Applications」を選択して、それを Linux **Startup Applications** に追加します。

データベース要件について詳しくは、『DB2 データベース製品のインストール要件』および 21 ページの『データベースの要件』を参照してください。

インストール手順

Endpoint Manager サーバーをインストールするには、以下の手順を実行します。

1. IBM Endpoint Manager をダウンロードします。
2. License Key Center で作成したライセンス認証ファイル (*.BESLicenseAuthorization) を使用するか、PoC 評価版の場合は IBM の技術営業担当員によって提供されたライセンス認証ファイルを使用して、サーバーをインストールします。インストール中に、ライセンスを要求し、マストヘッド・ファイルを作成します。

注: インストールを実行する前に、DB2 が稼働中であることを確認してください。

3. インストールが正常に完了したことを確認してください。

ステップ 1 - IBM Endpoint Manager のダウンロード

IBM のパスポート・アドバンテージ・ポータルから IBM Endpoint Manager をダウンロードします。

IBM Endpoint Manager は、サポート・サイト (<http://support.bigfix.com/bes/install/downloadbes.html>) または DeveloperWorks トライアル・サイト (<http://www.ibm.com/developerworks/downloads/tiv/endpoint/>) からダウンロードすることもできます。このデモンストレーション用トライアル・インストーラーは、通常の正規版インストール用のものと同じインストーラー・プログラムです。

サーバー・コンポーネントをインストールするには、パスポート・アドバンテージから以下の e- イメージをダウンロードします。

表 4. Endpoint Manager サーバーのインストールに必要なパーツ

ソフトウェア名	パーツ番号	イメージ
IBM Endpoint Manager Platform Install V9.1 for Multiplatforms	CITM5ML	IBM Endpoint Manager 9.1.1065.0.zip
IBM Endpoint Manager Platform Install V9.1 for Linux および DB2	CITM6ML	IEM-9.1.1065-Linux-DB2.tgz

Endpoint Manager Linux サーバーのインストール・ファイルを抽出するには、以下の手順を実行します。

1. Endpoint Manager サーバーの圧縮 zip ファイル IBM Endpoint Manager 9.1.1065.0.zip を Linux サーバーにコピーします。
2. 以下のコマンドを使用して、圧縮 zip ファイルを展開します。

```
unzip "IBM Endpoint Manager 9.1.1065.0.zip"
```
3. 以下のコマンドを使用して、*linux_server* フォルダーから *ServerInstaller_9.1.1065.0-rhe6.x86_64.tgz* ファイルを Red Hat Enterprise Linux サーバーに展開します。

```
tar -zxvf ServerInstaller_9.1.1065.0-rhe6.x86_64.tgz
```

ServerInstaller_9.1.1065.0-rhe6.x86_64 フォルダーに Linux サーバーをインストールするための *install.sh* ファイルがあります。

Endpoint Manager Linux サーバーのインストール・ファイルを DB2 とともに抽出するには、以下の手順を実行します。

1. tar ファイル *IEM-9.1.1065-Linux-DB2.tgz* を Linux サーバーにコピーします。
2. 以下のコマンドを使用して、圧縮ファイルを展開します。

```
tar -zxvf IEM-9.1.1065-Linux-DB2.tgz
```
3. *IEM-9.1.1065-Linux-DB2.tgz* イメージを展開すると、コンピューター上の *IEM-9.1.1065-Linux-DB2* フォルダーに DB2 イメージ *v10.5fp2_linuxx64_server_r.tar.gz* が置かれます。Linux サーバーをインストールするには、*ServerInstaller_9.1.1065.0-rhe6.x86_64* フォルダーから *install.sh* コマンドを実行します。

注: *install.sh* コマンドによって DB2 アーカイブ *.gz が検索されるため、*v10.5fp2_linuxx64_server_r.tar.gz* ファイルは展開しないでください。

ステップ 2 - サーバーのインストール

インストールを実行する前に、すべての前提条件を満たしていることを確認するには、20 ページの『サーバーの要件』を参照してください。

注: インストール・プログラムは、Yum を使用して、すべての必要な前提条件をインストールします。Yum の構成方法と Yum のリポジトリについては、『Configuring Yum and Yum Repositories』を参照してください。

Endpoint Manager サーバーを運用環境にインストールするには、以下の手順を実行します。

1. サーバー・パッケージを解凍したシェルからインストール・ディレクトリー *ServerInstaller_n.n.nnn.n-rhe6.x86_64* に移動して、以下のコマンドを入力します。

```
./install.sh
```
2. 「使用許諾契約」を読んだ後、「1」を入力して同意し、操作を続行します。
3. 正規版をインストールするには、2 を入力します。

```
Select Install Type
[1] Evaluation: Request a free evaluation license from IBM Corp.
This license allows you to install a fully functional copy of the
IBM Endpoint Manager on up to 30 clients, for a period of 30 days.
```

[2] Production: Install using a production license or an authorization for a production license
Choose one of the options above or press Enter to accept the default

注: 1 を入力して評価版のインストールを実行する場合は、そのタイプのインストールでは拡張セキュリティー・オプションがサポートされないことを念頭に置いてください。この機能について詳しくは、27 ページの『第 4 章 セキュリティー構成シナリオ』を参照してください。

4. すべてのコンポーネントをインストールするには、1 を入力します。

Select the IBM Endpoint Manager Features you want to install:
[1] All Components (Server, Client, and WebReports)
[2] Server and Client Only
[3] WebReports Only
Choose one of the options above or press <Enter> to accept the default: [1]

5. インストール・プログラムによって、DB2 インスタンスが既にインストールされているかどうかチェックされます。既にインストールされている場合は、ステップ 7 にスキップしてください。

データベースが検出されなかった場合は、1 を入力して DB2 ダウンロード・パッケージを指定し、これをインストールします。

```
#####
DB2 Installation Check
The installer does not detect DB2 as installed on the system. Determine which
of the options corresponds to your installation:
[1] DB2 is not installed, install it
[2] DB2 is installed, use the installed instance
[3] Exit from the installation
Choose one of the options above or press <Enter> to accept the default: [1]
```

If the user chooses the option1 then the user will be prompted with the following question with details of the settings that will be used.

6. DB2 のデフォルトの設定値を受け入れる場合は、1 を入力します。

```
#####
DB2 Installation
DB2 will be installed using the following settings:
    DB2 Instance owner: db2inst1
    DB2 Fenced user: db2fenc1
    DB2 Administration Server user: dasusr1
    DB2 communication port: 50000
    DB2 Installation directory: /opt/ibm/db2/V10.5
If you need to use settings different from those proposed above, you can
specify them in the installation response file. Refer to the product
documentation for further details.
[1] Proceed installing also DB2
[2] Exit from the installation
Choose one of the options above or press <Enter> to accept the default: [1]
```

7. 後で複製するためのマスター・データベースを作成したり、適用環境にデータベースが 1 つだけ必要な場合に単一データベースを作成したりするには、1 を入力します。

Select Database Replication:
[1] Single or Master Database
[2] Replicated Database
Choose one of the options above or press <Enter> to accept the default: [1]

2 を入力すると、既存のマスターのレプリカを作成することになります。追加情報については、「*IBM Endpoint Manager 構成ガイド*」を参照してください。

8. ローカル・データベースを使用するには、1 を入力します。

Select Database:

[1] Use Local Database

[2] Use Remote Database

Choose one of the options above or press <Enter> to accept the default: [1]

Endpoint Manager サーバーのローカル・データベース名は BFENT です。Web レポートのローカル・データベース名は BESREPOR です。

注: IBM Endpoint Manager に外部データベースを使用する場合は、以下の手順を実行する必要があります。

- リモート・ワークステーションに DB2[®] サーバーをインストールします。
 - Endpoint Manager サーバーのインストールを実行するワークステーションに DB2 クライアントをインストールします。
 - DB2 サーバーを、インストールを実行するワークステーションにインストールされた DB2 クライアントに接続します。そのため、DB2 データベースのポート (デフォルトは 50000) は、インストールを実行するワークステーションからアクセスできるポートでなければなりません。
9. クライアント用にダウンロードしたファイルの保管場所を入力します。

Choose the Web Server's Root Folder:

Specify the location for the Web Server's Root Folder or
press <Enter> to accept the default: /var/opt/BESServer

10. Web レポート・サーバーのファイルを保管する場所を入力します。

Choose the WebReports Server's Root Folder:

Specify the location for the WebReports Server's Root Folder or
press <Enter> to accept the default: /var/opt/BESWebReportsServer

11. Web レポート・サーバーのポートを入力します。

Choose the WebReports Server's Port:

Specify the Port Number or press <Enter> to accept the default: 80

デフォルトは 80 です。

12. ローカル DB2 の管理ユーザーのユーザー名を入力します。デフォルトは db2inst1 です。
13. ローカル DB2 の管理ユーザーのパスワードを入力します。
14. DB2 インスタンスの構成を入力します。
15. ユーザー ID とパスワードを入力して、初期管理ユーザーを定義します。ユーザー名のデフォルトは IEMAdmin です。
16. ローカル・ファイアウォールが稼働している場合、インストール・プログラムは、ローカル・ファイアウォール構成を入力するよう求めます。
17. BES ライセンス認証ファイルを使用してインストールを実行するには、1 を入力します。

Choose the setup type that best suits your needs:

[1] I want to install with a BES license authorization file

[2] I want to install with a Production license that I already have

[3] I want to install with an existing masthead

注: 最初のインストール (またはその一部) を既に実行している場合は、オプション 2 または 3 と、既存の正規版ライセンス (license.crt、license.pvk) ま

または既存のマストヘッド (masthead.afxm) を指定して、インストール・ステップの一部だけを実行することができます。

18. 前のステップでオプション 1 を選択した場合は、生成されたライセンス認証ファイルが配置される場所を指定します。

```
License Authorization Location
Enter the location of the license authorization file that you received
from IBM or press <Enter> to accept the default:
./license/LicenseAuthorization.BESLicenseAuthorization
```

19. サーバーのインストール先となるマシンの DNS 名または IP アドレスを指定します。この名前はライセンスに保存され、クライアントが Endpoint Manager サーバーを識別するために使用されます。ライセンスの作成後に変更することはできません。

20. 関連するサイト管理用プライベート・キーのパスワードを指定します。

21. 資格情報の暗号化に使用するキーのサイズ (ビット数) を指定します。

```
Key Size Level
Provide the key size that you want to use:
[1] 'Min' Level (2048 bits)
[2] 'Max' Level (4096 bits)
Choose one of the options above or press <Enter> to accept the default: [2]
```

22. インストールによって生成される license.crt、license.pvk、および masthead.afxm を保存するライセンス・フォルダーを入力します。

```
Choose License Folder:
Specify a folder for your private key (license.pvk), license certificate
(license.crt), and site masthead (masthead.afxm) or press <Enter> to accept
the default: ./license
```

23. 生成されるファイルの保存先を指定したら、マシンがインターネットに接続されているかどうかに応じて以下のいずれかのオプションを選択することにより、ライセンス証明書を取得するための要求を IBM に送信することができます。

- [1] Submit request from this machine over the Internet. The request will be redeemed for a license certificate (license.crt) and saved in your credential folder.
- [2] Save request to a file and send it to IBM at the URL:
'http://support.bigfix.com/bes/forms/BESLicenseRequestHandler.html'.
This method might be necessary if your deployment is isolated from the public Internet.

1 を選択した場合、次のインストール・ステップを続行できます。

2 を選択した場合、request.BESLicenseRequest 要求が生成されます。ライセンス証明書の場所 (例えば、./license/license.crt) を指定して証明書をインポートすることによってインストールを続行することも、インストールを終了し、後でインストール手順の説明に従ってインストールを再実行することもできます。

Info: The following License Request file was successfully generated:

```
./license/request.BESLicenseRequest
```

```
#####
```

```
Import License Certificate
```

- [1] Continue with the installation importing the certificate (license.crt).
- [2] Exit from the installation, I will import the certificate at a later time.

インストールを終了する場合は、後で `./install.sh` をもう一度実行し、オプション 2 を使用して、生成されたライセンスを使用することを指定し、すべてのステップを繰り返すことができます。

Choose the setup type that best suits your needs:

- [1] I want to install with a BES license authorization file
- [2] I want to install with a Production license that I already have
- [3] I want to install with an existing masthead

ファイルをインポートするには、ライセンス証明書ファイル (`./license/license.crt`) と、データベースを管理するためのサイト管理用プライベート キー (`./license/license.pvk`) を指定する必要があります。

License Certificate Location

Enter the location of the license certificate file or
press <Enter> to accept the default: `./license/license.crt`

Site Admin Private Key:

Specify the site Level Signing Key file (license.pvk) for the database you want to administer or press <Enter> to accept the default: `./license/license.pvk`

- 24. インターネット要求が行われるたびにユーザー名とパスワードの入力が必要になるプロキシが存在する場合、161 ページの『第 12 章 プロキシ接続のセットアップ』の説明に従ってプロキシ接続を設定して、Endpoint Manager サーバーまたはリレーがインターネットに接続できるようにします。
- 25. デフォルトのマストヘッド値を受け入れます。

```
Server Port Number: 52311
Use of FIPS 140-2 compliant cryptography: Disabled
Gather Interval: 1 Day
Initial Action Lock: Unlocked
Action Lock Controller: Console
Action Lock exemptions: Disabled
```

または、2 を入力して変更します。

- [1] Use Defaults Values
- [2] Use Custom Values

以下のマストヘッド・パラメーターは変更することができます。

サーバーのポート番号

サーバーのポート番号を指定します。デフォルト値は 52311 です。

注: ポート番号 52314 はプロキシ・エージェント用として予約されているため、Endpoint Manager のコンポーネント間のネットワーク通信には使用しないでください。

FIPS 140-2 に準拠した暗号を使用を有効にする

有効にするには 1 を入力し、無効にするには 2 を入力します。デフォルト値は 2 です。

収集間隔

以下のいずれかの値を入力して、間隔の時間を指定します。

- [1] Fifteen Minutes
- [2] Half Hour
- [3] One Hour
- [4] Eight Hours
- [5] Half Day
- [6] One Day
- [7] Two Days

- [8] One Week
- [9] Two Weeks
- [10] One Month
- [11] Two Months

デフォルト値は 6 (1 日) です。

初期アクション・ロック

ロック、一定期間のロック、またはロック解除を選択できます。

- [1] Locked
- [2] Lock Duration
- [3] Unlocked

デフォルト値は 3 (ロック解除) です。

ロックの除外対象の有効化

- [1] Lock Exemption Enabled (fairly unusual)
- [2] Lock Exemption Disabled

デフォルト値は 2 (ロックの除外対象の無効化) です。

前のステップで 1 を選択した場合は、ライセンス・ファイル (license.pvk ファイルおよび license.crt ファイル) が作成されています。このステップの後には、指定したパラメーターで masthead.afxm ファイルが作成されます。

26. DB2 インスタンスを作成するための DB2 接続のポート番号を入力します。

```
#####
DB2 Connection:
Specify the DB2 Port Number or press <Enter> to accept the default: 50000
```

IBM Endpoint Manager サーバーのインストールが、これで完了しました。これで、IBM Endpoint Manager コンソールを Windows システムにインストールして、サーバーのインストール中に作成したアカウントを使用してログオンすることができま

す。

/var/log ディレクトリー内にある、BESinstall.log でインストール・エラーを確認でき、また、BESAdminDebugOut.txt ファイルで BESAdmin コマンド・ライン・トレースを確認できます。

注: インターネットにアクセスするためのプロキシを構成した場合は、161 ページの『第 12 章 プロキシ接続のセットアップ』で説明する手順に従って、IBM Endpoint Manager 環境にプロキシを構成します。

ステップ 3 - サーバー・インストールの確認

インストールが正常に完了したことを確認するには、以下の手順を実行します。

1. 標準出力またはインストール・ログ・ファイル /var/log/BESInstall.log で、以下のメッセージが表示されていることを確認します。

```
The installation of IBM Endpoint Manager was completed successfully.
You can now proceed to install the IEM Console on a Windows System and log on
as 'EvaluationUser', the user just created.
The IEM Console installer is available in the folder '/var/opt/BESInstallers
```

2. /etc/init.d から以下のコマンドを入力して、インストールされている各コンポーネントに関連するサービスが開始されて稼働していることを確認します。


```
./besserver status
./besfilldb status
./besgatherdb status
./besclient status
./beswebreports status
```

- ローカルの DB2 管理ユーザー (デフォルトは db2inst1) に切り替えて、list database コマンドを実行することで、ローカルまたはリモートのデータベースが作成されていることを確認します。

```
su - db2inst1
db2 list db directory
```

以下のデータベースが作成されていることを確認します。

- サーバー・コンポーネント: BFENT
- WebReports コンポーネント: BESREPOR

- IBM Endpoint Manager コンソールを起動し、インストール時に作成された最初の IBM Endpoint Manager ユーザーの資格情報を指定して、コンソールがサーバーに接続していることを確認します。ユーザーのデフォルト値は、評価版のインストールでは EvaluationUser で、正規版のインストールでは IEMAdmin です。サーバー・マシンにデフォルトでインストールされているクライアントが登録されていることを確認します。
- 「ツール」->「Web レポートの起動」を選択し、インストール時に作成された最初のユーザーの資格情報を指定して、コンソールから Web レポートにログインできることを確認します。

インストール・コマンド・オプション

正規版と評価版のインストールは、対話モードで実行することも、サイレント・モードで実行することもできます。各タイプのインストールを実行するための完全なコマンドは以下のとおりです。

```
./install.sh [ -f <input_response_file> ] [ -g <output_response_file> ]  
[ -upgrade | -upgradeNoClient ] [ -reuseDb ]
```

指定の内容は以下のとおりです。

-f <input_response_file>

使用する応答ファイルの絶対パスおよびファイル名を指定します。

-g <output_response_file>

応答ファイルを生成します。

-upgrade

すべてのコンポーネントをアップグレードするためのスクリプトを実行します。

-upgradeNoClient

クライアント以外のすべてのコンポーネントをアップグレードするためのスクリプトを実行します。

-reuseDb

既存のデータベースを使用できるようにします。災害復旧中にインストール・プログラムが BFENT データベースまたは BESREPOR データベースを検出した場合は、それらのデータベースが使用されます。

サイレント・インストール

サイレント・インストールを実行するには、以下のコマンドを入力します。

```
./install.sh -f response_file
```

ここで *response_file* は、製品をインストールするためのキーワードを含むファイルです。

Endpoint Managerサーバーをインストールする場合、またはインストールの失敗時に問題判別を実行する場合には、サイレント・モードを使用します。

注: 応答ファイルでは、キーワードのサブセット (各種のシステムに共通のキーワードなど) を指定することができます。欠落しているキーワードや無効なキーワードは、インストール・プログラムによって要求されます。サイレント・インストールが無人で実行されるのは、必要なすべてのキーワードが応答ファイルで指定されている場合のみです。

以下のコマンドを使用して応答ファイル内のインストール・パラメーターをリダイレクトすることにより、インストール中に応答ファイルを作成できます。

```
./install.sh -g response_file
```

実動サーバーをインストールするための応答ファイルの例を以下に示します。

```
##IEM GENERATED RESPONSE FILE
LA_ACCEPT="true"
IS_EVALUATION="false"
COMPONENT_SRV="true"
COMPONENT_WR="true"
SINGLE_DATABASE="true"
LOCAL_DATABASE="true"
BES_WWW_FOLDER="/var/opt/BESServer"
WR_WWW_FOLDER="/var/opt/BESWebReportsServer"
WR_WWW_PORT="80"
INSTALL_DB2="yes"
DB2_INSTANCE_NAME="db2inst1"
DB2_DAS_USERNAME="dasusr1"
DB2_FENCED_USERNAME="db2fenc1"
DB2_INSTALL_DIR="/opt/ibm/db2/V10.5"
DB2_PORT="50000"
DB2_SETUP_FILE="../../server_r/db2setup"
DB2_USERS_PWD="Bigfix11"
TEM_USER_NAME="IEMAdmin"
TEM_USER_PWD="Bigfix11"
CONF_FIREWALL="no"
BES_SETUP_TYPE="authfile"
BES_AUTH_FILE="/opt/iemlic/LicenseAuthorization.BESLicenseAuthorization"
SRV_DNS_NAME="NC9128110090.romelab.it.ibm.com"
BES_LICENSE_PVK_PWD="Bigfix11"
PVK_KEY_SIZE="max"
BES_LIC_FOLDER="/opt/iemlic"
SUBMIT_LIC_REQUEST="yes"
USE_PROXY="true"
PROXY_USER="proxyuser"
PROXY_PWD="Bigfix11"
PROXY_HOST="nc114087.romelab.it.ibm.com"
PROXY_PORT="3128"
ADV_MASTHEAD_DEFAULT="true"
```

評価版サーバーをインストールするための応答ファイルの例を以下に示します。

```

##IEM GENERATED RESPONSE FILE
LA_ACCEPT="true"
IS_EVALUATION="true"
CREDENTIAL_USER="John Smith"
CREDENTIAL_EMAIL="john.smith@us.ibm.com"
CREDENTIAL_ORG="IBM US"
SRV_DNS_NAME="NC9128110090.romelab.it.ibm.com"
BES_SERVER_PORT="52311"
WR_WWW_PORT="80"
CONF_FIREWALL="no"
DB2_ADMIN_USER="db2inst1"
DB2_ADMIN_PWD="Bigfix11"
DB2_PORT="50000"
BES_LIC_FOLDER="/opt/iemlic"
USE_PROXY="true"
PROXY_USER="none"
PROXY_HOST="nc114087.romelab.it.ibm.com"
PROXY_PORT="3128"

```

指定の内容は以下のとおりです。

表 5. 応答ファイルのキーワード

キーワード	値
LA_ACCEPT	ご使用条件に同意します。 true は同意して続行します false はインストールを終了します
IS_EVALUATION	インストールのタイプを指定します。 true は評価版のインストールを実行します false は実動インストールを実行します 注: 評価版のインストールでは、拡張セキュリティー・オプションがサポートされません。この機能について詳しくは、27 ページの『第 4 章 セキュリティー構成シナリオ』を参照してください。
CREDENTIAL_USER	ユーザー名を指定します。例: John Smith。 注: 評価版インストールの場合にのみ有効です
CREDENTIAL_EMAIL	ユーザーの電子メール・アドレスを指定します。例: john.smith@us.ibm.com。 注: 評価版インストールの場合にのみ有効です
CREDENTIAL_ORG	ユーザーの組織を指定します。例: IBM US。 注: 評価版インストールの場合にのみ有効です
COMPONENT_SRV	Endpoint Manager サーバー・コンポーネントをインストールするように指定します。 true は、サーバーおよびクライアントをインストールします false は、サーバーおよびクライアントをインストールしません
COMPONENT_WR	Endpoint Manager Web レポート・コンポーネントをインストールするように指定します。 true は Web レポートをインストールします false は Web レポートをインストールしません
SINGLE_DATABASE	後で複製するためのマスター・データベースを作成するか、適用環境で単一のデータベースのみが必要な場合。 true は単一のデータベースを作成します false は複製したデータベースを作成します

表 5. 応答ファイルのキーワード (続き)

キーワード	値
LOCAL_DATABASE	ローカルまたはリモートのデータベースを使用します。 true はローカル・データベースを使用します false は、DB2 クライアント経由でリモート・データベースを使用します
DB2_ADMIN_USER	ローカル DB2 管理ユーザーのユーザー名を指定します。既に DB2 がインストールされている場合に限りします。
DB2_ADMIN_PWD	ローカル DB2 管理ユーザーのパスワードを指定します。既に DB2 がインストールされている場合に限りします。
DB2INST_CONFIGURE	Endpoint Manager のインストール中にデータベースを構成します。 yes は DB2 を構成します no は DB2 を構成しません 既に DB2 がインストールされている場合に限りします。
BES_WWW_FOLDER	Endpoint Manager サーバーのインストール・フォルダーを指定します。デフォルト値は /var/opt/BESServer です。
WR_WWW_FOLDER	Web レポートのインストール・フォルダーを指定します。デフォルト値は /var/opt/BESWebReportsServer です。
WR_WWW_PORT	Web レポートのポート番号を指定します。デフォルト値は 80 です。
INSTALL_DB2	Endpoint Manager サーバーとともに DB2 をインストールします。 yes は DB2 をインストールします no は DB2 をインストールしません
DB2_INSTANCE_NAME	Endpoint Manager データベース・インスタンスの名前を指定します。デフォルト値は db2inst1 です。
DB2_DAS_USERNAME	DB2 管理サーバー (DAS) を実行するアカウントのユーザー名を指定します。デフォルト値は dasusr1 です。
DB2_FENCED_USER	Endpoint Manager データベースが使用するアドレス・スペースの外部でユーザー定義関数 (UDF) およびストアド・プロシージャを実行するために使用するアカウントのユーザー名を指定します。デフォルトのユーザーは db2fenc1 です。
DB2_INSTALL_DIR	DB2 をインストールするディレクトリを指定します。例: /opt/ibm/db2/V10.5。
DB2_PORT	DB2 のポートを指定します。デフォルト値は 50000 です。
DB2_SETUP_FILE	DB2 をインストールするためのセットアップ・ファイルを指定します。例: ../server_r/db2setup。
DB2_USERS_PWD	DB2 ユーザーのパスワードを指定します。
TEM_USER_NAME	初期管理ユーザーを定義するための Endpoint Manager ユーザー ID を指定します。デフォルト値は IEMAdmin です。
TEM_USER_PWD	初期管理ユーザーを定義するためのパスワードを指定します。
CONF_FIREWALL	Endpoint Manager サーバーまたはリレーがインターネットに接続できるようにファイアウォールを構成します。 yes はファイアウォール構成を設定します no はファイアウォール構成を設定しません

表 5. 応答ファイルのキーワード (続き)

キーワード	値
BES_SETUP_TYPE	実行するセットアップのタイプを指定します。 authfile は、BES ライセンス認証ファイルを使用してインストールします prodlic は、既に有効である正規版ライセンスを使用してインストールします masthead は、既存のマストヘッドを使用してインストールします
BES_AUTH_FILE	認証ファイルのパスを指定します。パスの例: /opt/iemlic/LicenseAuthorization.BESLicenseAuthorization。
SRV_DNS_NAME	サーバーのインストール先となるマシンの DNS 名または IP アドレスを指定します。この名前はライセンスに保存され、クライアントが Endpoint Manager サーバーを識別するために使用されます。ライセンスの作成後に変更することはできません。
BES_LICENSE_PVK	license.pvk ファイルのパスワードを指定します。
PVK_KEY_SIZE	パブリック・キー (license.crt) のサイズ (ビット数) を指定します。 min 2048 ビットに対応します。 max 4096 ビットに対応します。これはデフォルト値です。
BES_LIC_FOLDER	インストール時に license.crt、license.pvk、および masthead.afxm を生成して保存するライセンス・フォルダーを指定します。ライセンス・フォルダーの例: /tmp/ServerInstaller_9.1-rhel/offlic。
SUBMIT_LIC_REQUEST	ライセンス証明書を取得するための要求を IBM に送信します。 yes は、このマシンからインターネット経由でライセンス証明書 (license.crt) の要求を送信し、資格情報フォルダーに保存します。 no は、要求をファイルに保存し、それを手動で IBM に送信します (http://support.bigfix.com/bes/forms/BESLicenseRequestHandler.html)。デプロイメント環境がインターネットから隔離されている場合に、この方法が必要になる場合があります。
USE_PROXY	プロキシ接続を指定して、Endpoint Manager サーバーがインストール中にインターネットに接続できるようにします。 true はプロキシを設定します。 false はプロキシを設定しません。
PROXY_USER	プロキシのユーザーを指定します。プロキシが認証不要の場合は、PROXY_USER を NONE に設定してください。
PROXY_PWD	プロキシ・ユーザーのパスワードを指定します。
PROXY_HOST	プロキシを実行するコンピューターのホスト名を指定します。
PROXY_PORT	プロキシを実行するコンピューターのポートを指定します。
ADV_MASTHEAD_DEFAULT	デフォルトのマストヘッド値を受け入れます。 true はデフォルト値を使用します。 false はカスタム値を使用します。

インストール・フォルダーの構造

Endpoint Manager のインストールが終わると、フォルダー構造は以下のようになります。

サーバー・フォルダー構造:

```
/var/opt/BESInstallers
/var/opt/BESInstallers/Client (Client installer)
/var/opt/BESInstallers/Console (Console installer)

/var/opt/BESServer
  besserver.config (Configuration file)
  besserver.config.default (Default configuration file)

/var/opt/BESServer/FillDBData/FillDB.log (FillDB service log)

/var/opt/BESServer/GatherDBData/GatherDB.log (GatherDB service log)

/opt/BESServer
/opt/BESServer/bin (Server binaries)
/opt/BESServer/reference (Rest API xsd templates)

/etc/opt/BESServer
  actionsite.afxm (Masthead file)

/etc/init.d
  besserver (Server service)
  besfilldb (FillDB service)
  besgatherdb (GatherDB service)
```

WebReports フォルダー構造:

```
/var/opt/BESWebReportsServer
  beswebreports.config (Configuration file)
  beswebreports.config.default (Default configuration file)

/opt/BESWebReportsServer
/opt/BESWebReportsServer/bin (WebReports binaries)

/etc/opt/BESWebReportsServer
  actionsite.afxm (Masthead file)

/etc/init.d
  beswebreports (WebReports service)
```

クライアント・フォルダー構造:

```
/var/opt/BESClient
  besclient.config (Configuration file)
  besclient.config.default (Default configuration file)

/opt/BESClient
/opt/BESClient/bin (Client binaries)

/etc/opt/BESClient
  actionsite.afxm (Masthead file)

/etc/init.d
  besclient (besclient service)
```

インストール・ログ・ファイル:


```
/var/log/  
  BESInstall.log      (Installer log file)  
  BESAdminDebugOut.txt (Administrator Tool debug information)  
  BESRelay.log        (Relay log file)
```

注: 以下のフォルダーのいずれかが存在しないと、インストール手順が失敗するので注意してください。

```
/opt  
/etc  
/var
```

構成ファイル、マストヘッド・ファイル、およびログ・ファイル

インストールが終了すると、インストール済みコンポーネントおよびインストール・メッセージの設定が含まれる、以下の Endpoint Manager ファイルがあることを確認できます。

表 6. Endpoint Manager の構成およびログ・ファイル

コンポーネント	ファイル
サーバー (Server)	- 構成ファイル: /var/opt/BESServer/besserver.config - マストヘッド・ファイル: /etc/opt/BESServer/actionsite.afxm - ログ・ファイル: /var/log/BESInstall.log、/var/log/BESAdminDebugOut.txt
Web レポート (Web Report)	- 構成ファイル: /var/opt/BESWebReportsServer/beswebreports.config - マストヘッド・ファイル: /etc/opt/BESWebReportsServer/actionsite.afxm
クライアント (Client)	- 構成ファイル: /var/opt/BESClient/besclient.config - マストヘッド・ファイル: /etc/opt/BESClient/actionsite.afxm
リレー (Relay)	構成ファイル: /var/opt/BESRelay/besrelay.config

構成ファイルには、トレース、データベース接続、およびプロキシ構成の設定が含まれます。BESServer、BESFillDB、および BESGatherDB サービスは、構成パラメーターを最初に besclient.config で検索し、次に besserver.config で検索します。BESWebReports サービスは、構成パラメーターを最初に besclient.config で検索し、次に beswebreports.config で検索します。

Endpoint Manager サービスの管理

以下のコマンドを使用して、Linux Endpoint Manager サービスを起動、停止、再起動したり、その状況を照会したりすることができます。

```
service service stop
service service start
service service restart
service service status

/etc/init.d/service stop
/etc/init.d/service start
/etc/init.d/service restart
/etc/init.d/service status
```

ここで、*service* は以下のいずれかのサービスです。

```
besfilldb
besgatherdb
besserver
beswebreports
```

DB2 パスワードの変更

Endpoint Manager サーバーの DB2 データベースをインストールした後、データベース・パスワードを変更し、それを Endpoint Manager 構成ファイルに設定するには、以下の手順を実行します。

1. *besserver* サービスと *beswebreports* サービスを以下のように停止します。

```
service besserver stop
service beswebreports stop
```

2. DB2 管理ユーザー・パスワードを以下のように変更します。

```
#passwd db2inst1
```

指定したユーザー・アカウントに対して新規パスワードを設定するよう求められます。

3. 構成ファイル `/var/opt/BESServer/besserver.config` を開きます。

4. `[Software¥BigFix¥EnterpriseClient¥Settings¥Client¥_BESServer_Database_Password]` に移動して、以下の部分を設定します。

```
value = "db2newpassword"
```

5. 構成ファイル `/var/opt/BESWebReportsServer/beswebreports.config` を開きます。

6. `[Software¥BigFix¥Enterprise Server¥FillAggregateDB]` に移動して、以下の部分を設定します。

```
value = "db2newpassword"
```

7. *besserver* サービスと *beswebreports* サービスを以下のように開始します。

```
#service besserver start
#service beswebreports start
```

再始動後にパスワードは難読化され、構成ファイル内では再び `""` に置き換えられます。

DB2 ポートの変更

Endpoint Manager サーバーの DB2 データベースをインストールした後、DB2 インスタンス接続ポートを変更し、それを Endpoint Manager 構成ファイルに設定するには、以下の手順を実行します。

1. DB2 インスタンスに接続するすべての Endpoint Manager サービスおよびすべてのアプリケーションを停止します。
2. DB2 接続ポートを以下のように変更します。

```
#su - db2inst1
$db2 update dbm cfg using SVCENAME <new_port_number>
$db2stop; db2start
```

3. 構成ファイル /var/opt/BESServer/besserver.config を開きます。
4. [Software¥BigFix¥EnterpriseClient¥Settings¥Client¥_BESServer_Database_Port] に移動して、以下のように新しいポート番号を設定します。

```
value = "<new_port_number>"
```

5. 構成ファイル /var/opt/BESWebReportsServer/beswebreports.config を開きます。
6. [Software¥BigFix¥Enterprise Server¥FillAggregateDB] に移動して、以下のよう新しいポート番号を設定します。

```
Port = "<new_port_number>"
```

7. すべての Endpoint Manager サービスを開始します。

追加サーバーの認証 (DSA)

複数のサーバーを使用することによって、IBM Endpoint Manager のインストール済み環境に、さらに高いレベルのサービスを提供できます。ご使用のインストール済み環境に災害対応サーバー・アーキテクチャー (DSA) を追加することを選択すると、ローカル・サービスの提供を続行しながら、ネットワークおよびシステムの障害から自動的に復旧できるようになります。この機能を利用するには、少なくとも 1 次サーバーと同等の機能を持つ、1 つ以上の追加のサーバーが必要です。追加の費用と設置が必要になるため、DSA を使用する前に、ニーズについて慎重に検討してください。

サーバーは、DB2 のサーバー間認証オプションを使用してお互いに通信できます。

追加の Linux サーバーをインストールする前に、適用環境に追加する各マシンに DB2 Server をインストールします。この DB2 Server のバージョンは、マスター・サーバーにインストールされる DB2 Server と同じバージョンである必要があります。

DB2 認証の使用

この手法では、各サーバーにログイン名とパスワードが付与され、それらのサーバーが適用環境内の他のすべてのサーバーのログイン名およびパスワードを受け付けるように構成されます。このアカウントのパスワードは平文で入力しますが、FillIDB サービスの再始動後に各サーバーの構成ファイルで難読化されます。DB2 認証を使用してサーバーを認証するには、次の手順に従います。

1. サーバー間認証のために、適用環境内のすべてのサーバーが使用する単一のログイン名 (例えば db2inst1) および単一のパスワードを選択します。
2. マスター・サーバーで /var/opt/BESServer/besserver.config ファイルを開きます。

3. [Software¥BigFix¥Enterprise Server¥FillDB] セクションで以下のキーワードを追加または変更します。

```
ReplicationUser = <login name>
ReplicationPassword = <password>
ReplicationPort = <DB2_port>
```

4. FillDB サービスを再始動します。

注:

この選択は、適用環境単位で行う必要があります。ドメインで認証されるサーバーと DB2 で認証されるサーバーを混在させることはできません。

ReplicationUser、ReplicationPassword、および ReplicationPort は、DSA 環境のすべてのサーバー構成ファイルで一意的に定義する必要があります。

適用環境内のすべての IBM Endpoint Manager サーバーが同じバージョンの DB2 Server を実行している必要があります。

追加 Linux サーバーのインストール (DSA)

DSA サーバーをインストールする前に、認証方法を決定し、64 ページの『追加サーバーの認証』で説明している手順を実行してください。

適用環境に追加するサーバーごとに、それらが相互に通信していることを確認してから、以下の手順を実行します。

1. 各サーバーが、マスター・サーバーによって使用されているものと同じ DB2 Server バージョンを使用していることを確認します。
2. license.pvk ファイルと masthead.afxm ファイルを、マスター・サーバーからインストール対象の各マシンのフォルダーにコピーします。
3. 追加サーバーとして構成する各マシンで、install.sh スクリプトを実行します。SA 権限を持つためには、ローカル DB2 Server のインストールに使用したのと同じドメイン管理を使用してください。
4. Select Install Type プロンプトが表示されたら、次を選択します。
[2] Production: Install using a production license or an authorization from a production license
5. 「インストールする IBM Endpoint Manager Features の選択 (Select the IBM Endpoint Manager Features you want to install)」プロンプトで、「すべてのコンポーネント (All Components)」または「サーバーとクライアントのみ (Server and Client only)」のいずれをインストールするかを選択します。
6. Select Database Replication プロンプトが表示されたら、次を選択します。
[2] Replicated Database.
7. Select Database プロンプトに対して、[1] Use Local Database を選択します (ほとんどのアプリケーションでは、一般にこれを選択します)。
8. 以前に「ローカル・データベースを使用」を選択した場合は、「DB2 ローカル管理ユーザー (DB2 Local Administrative User)」プロンプトで、インストール・スクリプトを実行しているコンピューターのデータベースに対する DB2 管理ユーザーのユーザー名とパスワードを入力します。
9. Web サーバー・ルートおよび Web レポート・サーバー・ルートのフォルダーを入力します。

10. Web レポート・サーバーのポート番号を入力します。
11. Web レポート管理ユーザーの資格情報を定義します。デフォルトは IEMAdmin です。
12. license.pvk の場所とパスワードを指定します。
13. マスター・サーバーのインストール時に生成された既存の masthead.afxm ファイルの場所を指定します。
14. Secondary Server DNS Name プロンプトに対して、新規サーバーの DNS 名を入力します。この名前は、他のサーバーおよびクライアントで解決できるものでなければなりません。
15. DB2 Connection プロンプトに対して、インストーラーを実行しているローカル DB2 インスタンスのポート番号を入力します。
16. 以下のように、マスター・サーバーの DB2 インスタンスに関する情報を入力し、新規サーバーがマスター・サーバー上の DB2 に接続できるようにします。

「マスター・サーバー・データベースのホスト名 (Master Server Database Hostname)」プロンプトで、マスター・サーバー・データベースが存在するシステムのホスト名を指定します。

「マスター・サーバー・データベースのポート (Master Server Database Port)」プロンプトで、マスター・サーバー・データベースが存在するシステムのデータベース・ポート番号を指定します。

「マスター・サーバー・データベースの管理ユーザー (Master Server Database Administrative User)」プロンプトで、マスター・サーバー・データベースが存在するシステムの DB2 管理ユーザーのユーザー名を指定します。

「マスター・サーバー・データベースの管理ユーザーのパスワード (Master Server Database Administrative User Password)」プロンプトで、マスター・サーバー・データベースが存在するシステムの DB2 管理ユーザーのパスワードを指定します。

サーバーのコンポーネントについて

この時点で、IBM Endpoint Manager サーバーは正常にインストールされており、各種のコンポーネントを使用して、リレー、クライアント、コンソールの各コンピューターからのメッセージと要求に応答しています。

サーバーの実行内容を適切に理解するために、以下に示すいくつかのコンポーネントの説明を確認してください。

クライアント登録コンポーネント

クライアントは、新しいコンピューターにインストールされると、サーバーのクライアント登録コンポーネントにクライアント自体を登録します。クライアントには、固有 ID が付与されます。コンピューターの IP アドレスが変更されると、クライアントは、その新しい IP アドレスを、クライアント登録コンポーネントに自動的に登録します。

結果ポストサーバー・コンポーネント

クライアントは、Fixlet が適用対象であることを検出すると、HTTP POST

操作を使用して、結果ポストサーバー・コンポーネントにレポートします。このコンポーネントは、クライアント・コンピューターの登録済み ID と共に、適用対象の Fixlet を識別します。この情報は、FillDB サービスを通じて IBM Endpoint Manager データベースに渡され、その後、コンソールで表示できるようになります。クライアントは、その他の状態の変更についても、直接またはリレーを通じて定期的にサーバーにレポートします。

収集サーバー・コンポーネント

このコンポーネントは、サブスクライブしたすべての Fixlet サイトでの Fixlet コンテンツの変更を監視します。このコンポーネントは、これらの変更をサーバーにダウンロードします。これにより、GatherDB コンポーネントがそれらの変更を使用できるようになります。

FillDB コンポーネント

このコンポーネントは、クライアントの結果をデータベースに送ります。

GatherDB コンポーネント

このコンポーネントは、Fixlet ダウンロードをインターネットからデータベース内に収集し、保存します。

ダウンロード・ミラーリング・サーバー・コンポーネント

ダウンロード・ミラーリング・サーバー・コンポーネントは、リレーおよびクライアントのために Fixlet サイト・データをホストします。このコンポーネントは、IBM Endpoint Manager トラフィック用の簡素化されたダウンロード・サーバーとして機能します。

コンソールのインストール

IBM Endpoint Manager コンソールは、HTTPS ポート 52311 経由でサーバーへのネットワーク接続を確立できるすべての Windows コンピューターにインストールすることができます。テスト環境と評価環境の場合を除き、サーバー・コンピューター上でコンソールを実行することはお勧めしません。データベースまたは Web サーバーを実行しているコンピューターで発行者キーの資格情報を保持することにより、パフォーマンスとセキュリティ上の影響があるためです。IBM Endpoint Manager コンソールを使用すると、ネットワーク全体にわたり、すべての管理対象コンピューターでの問題をモニターして修正することができます。

コンソールをインストールするには、以下の手順に従います。

1. /var/opt/BESInstallers ディレクトリーに移動します。
2. Console フォルダを Windows ワークステーションにコピーします。同じビルド・レベルの Console フォルダを使用してください。
3. Windows ワークステーション上の Console ディレクトリーから setup.exe を実行します。

注: デフォルトでは、ローカル・オペレーティング・システムのファイアウォールが有効になっています。コンソールが IBM Endpoint Manager サーバーに接続できるようにするために、必ずサーバー・ポート (デフォルトでは 52311) を通じた TCP 通信および UDP 通信、Web レポート・ポート (デフォルトでは 80) を通じた TCP 通信を許可するようにファイアウォールを構成してください。

ローカル・ファイアウォールを手動で構成する必要がある場合は、以下のコマンドを実行できます。

```
iptables -I INPUT -p tcp --dport < Server_Port > -j ACCEPT
iptables -I INPUT -p udp --dport < Server_Port > -j ACCEPT
iptables -I INPUT -p tcp --dport < WebReports_Port > -j ACCEPT
service iptables save
```

コンソール・プログラムの使用について詳しくは、「*IBM Endpoint Manager* コンソール・オペレーター・ガイド」を参照してください。

クライアント適用ツールのインストール

クライアント適用ツールは Windows クライアントを適用するために使用されます。このツールは Linux サーバーでも使用することができ、Linux の Endpoint Manager コンソール・イメージに含まれています。

このツールを Linux サーバーの適用環境にインストールするには、以下の手順を実行します。

1. /var/opt/BESInstallers ディレクトリーに移動します。
2. Console フォルダーを、Endpoint Manager コンソールとしても使用される Windows ワークステーションにコピーします。
3. Windows ワークステーションの Console ディレクトリーから、**setup.exe** を実行し、コンソールとともに適用ツールをインストールします。ツールを開始するには、**C:\Program Files\BigFix Enterprise\BES Console\BESClientDeploy** ディレクトリーから、**BESClientDeploy.exe** プログラムを実行します。

クライアントのインストール

管理対象のネットワークにあるすべてのコンピューター (コンソールを実行するコンピューターを含みます) に IBM Endpoint Manager クライアントをインストールします。これにより、そのコンピューターで、セキュリティ・パッチ、構成ファイル、アップグレードなどの重要な Fixlet メッセージを受信できます。

コンソールを実行している場合は、「**IBM Endpoint Manager** コンポーネントのインストール」>「**クライアントのインストール**」>「**ローカルにインストール**」を選択して、ローカル・マシン上の指定したディレクトリーにクライアントをインストールします。

クライアント適用ツール (**BESClientDeploy.exe**) を実行する場合、以下の 3 つの方法でクライアントを適用することができます。

Active Directory を使用してコンピューターを検索する

IBM Endpoint Manager クライアント・インストール・ツールは Active Directory サーバーにアクセスし、ドメイン内のすべてのコンピューターのリストを取得します。このツールは、各コンピューターをチェックして、クライアントが既にインストールされているかどうかを確認し、その情報をリスト形式で表示します。

NT 4.0 ドメインを使用してコンピューターを検索する

ドメイン内のすべてのコンピューターが、クライアントがインストールされているかどうか示すステータス・フラグ付きでリストされます。

リスト内で指定されたコンピューターを検索する

ネットワークでのコンピューター・アドレスの解決方法に基づいて、コンピューター名、IP アドレス範囲、またはホスト名のリストを指定する必要があります。このリストでは、行ごとに 1 つの名前、IP アドレス範囲、またはホスト名を指定する必要があります。このオプションを使用すると、クライアント・インストール・ツールはコンピューターのディスカバーを試行しませんが、代わりに、リストされているすべてのコンピューターへの直接インストールを試行します。

クライアント・インストール・ツールの使用

Active Directory ドメインまたは NT Directory ドメインに接続されている小規模なネットワーク（おおよそ 5,000 台未満のコンピューター）では、クライアント・インストール・ツールを使用して Windows クライアントをインストールできます。大規模なネットワークでは、その他のインストール方法を使用した方が簡単な場合があります。クライアント・インストール・ツールは、クライアントを簡単な方法で展開できるよう支援しますが、以下に示す要件および条件があります。

- Active Directory ドメインまたは NT Directory ドメインが必要です（コンピューターの管理者アカウントを所有している場合、一連のコンピューターにインストールするオプションもあります）。
- IBM Endpoint Manager クライアント・インストール・ツールは、Windows 2000、XP、Server 2003、Vista、Server 2008、7、または Server 2008 R2 を実行しているコンピューターのみを対象にすることができます。
- クライアント・インストール・ツールを実行するコンピューターはドメインに接続する必要がありますが、そのコンピューター自体はドメイン・コントローラーにしないでください。
- サービス・コントロール・マネージャー (SCM) サービスおよびリモート・プロシージャー・コール (RPC) サービスがターゲット・マシンで実行されている必要があります。
- SCM へのリモート接続またはリモート・プロシージャー・コールの発行を防ぐセキュリティ・ポリシーはコンピューターに対して使用しないでください。
- Active Directory 内のすべての対象のコンピューターの dnsName プロパティを正しく定義する必要があります。

クライアント・インストール・ツールを使用すると、クライアントをコンピューターに容易にプッシュできますが、クライアント・インストール・ツールは、多数の機能を備えた企業クラスのソフトウェア配布ツールではありません。ソフトウェア配布ツールが既にある場合、その既存のソフトウェア配布ツールを代わりに使用することをお勧めします。

IBM Endpoint Manager クライアント・インストール・ツールは、Active Directory サーバーからコンピューターのリストを取得し、それらのコンピューターにリモート接続して（一度に 100 台のコンピューターにアクセスします）、クライアント・サービスが各コンピューターに既にインストールされているかどうか確認することか

ら始めます。インストールされている場合、「インストール済み」とレポートし、それとともにクライアント・サービスの状況（「実行中」、「停止」など）もレポートします。アクセス許可の問題が原因で、または何らかの理由で状況を特定できない場合、「状況が不明」とレポートします。インストールされていない場合、「インストールされていません」とレポートします。ただし、コンピューターとまったく通信できない場合は除きます。この場合、「応答なし (Not Responding)」とレポートします。

クライアントがまだインストールされていない場合、このツールは、共有インストーラーにアクセスするリモート・プロシージャ・コールを発行できるインターフェースを提供し、適切なドメイン管理認証情報を使用して、このリモート・プロシージャ・コールをサイレントで実行します。ユーザー操作は必要ありません。このツールを使用するには、次の手順を実行します。

1. C:\Program Files\BigFix Enterprise\BES Console\BESClientDeploy ディレクトリから、BESClientDeploy.exe プログラムを実行します。
2. 表示されるダイアログでは、クライアントをインストールするための次の 3 つの方法が提供されます。
 - **Active Directory を使用してコンピューターを検索する。** IBM Endpoint Manager クライアント・インストール・ツールは Active Directory サーバーにアクセスし、ドメイン内のすべてのコンピューターのリストを取得します。このツールは、各コンピューターをチェックして、クライアントが既にインストールされているかどうかを確認し、その情報をリスト形式で表示します。
 - **NT 4.0 ドメインを使用してコンピューターを検索する。** ドメイン内のすべてのコンピューターが、クライアントがインストールされているかどうかを示すステータス・フラグ付きでリストされます。
 - **リスト内で指定されたコンピューターを検索する。** ネットワークでのコンピューター・アドレスの解決方法に基づいて、コンピューター名、IP アドレス範囲、またはホスト名のリストを指定する必要があります。このリストでは、行ごとに 1 つの名前、IP アドレス範囲、またはホスト名を指定する必要があります。このオプションを使用すると、クライアント・インストール・ツールはコンピューターのディスカバリーを試行しませんが、代わりに、リストされているすべてのコンピューターへの直接インストールを試行します。
3. コンピューターへの管理アクセス権限を持つ**ユーザー名**および**パスワード**を入力します。ほとんどの場合、これはドメイン管理者アカウントです。コンピューター・リスト・オプションを使用する場合、管理者特権のあるリモート・コンピューターのローカル・アカウント（ローカル管理者アカウントなど）を指定できます。残りのクライアント・インストール・プロセスでは、このユーザー名およびパスワードが使用されます。このため、アカウントにリモート・コンピューターへの適切なアクセス権限がない場合は、アクセス拒否エラーを受け取ります。
4. コンピューターのリストが表示されたら、IBM Endpoint Manager で管理するコンピューターを、Shift キーまたは Ctrl キーを押しながらクリックして選択します。「次へ」をクリックします。
5. 選択したコンピューターのリストが表示されます。通常はデフォルトのオプションで十分ですが、「詳細オプション」を選択して、次のインストール・パラメーターを構成することが望ましいです。

- 「**ファイルの転送**」：インストールのためにリモート・サーバーにファイルをプッシュすること、またはローカル・コンピューターからファイルをプルすることを選択できます。プッシュを許可しないセキュリティー・ポリシーが実施されている場合を除いて、ほとんどのケースで、リモート・コンピューターへのファイルのプッシュが最も効果的に機能します。
 - 「**接続方式**」：リモート・コンピューターに接続する方法は 2 つあります。**サービス・コントロール・マネージャー (SCM)** を使用することが推奨されていますが、SCM が動作しない場合、**タスク・スケジューラー**を使用することもできます。
 - 「**インストール先のパス**」：クライアントのパスを指定します。またはデフォルトをそのまま使用します (推奨)。
 - 「**確認**」：インストールが完了するまで待機した後にクライアント・サービスが実行されていることを確認し、インストールが正常に完了したかどうかを識別するには、このボックスにチェック・マークを付けます。
 - 「**カスタム設定**」：名前と値のペアの形式で、インストールする各クライアントにカスタム設定を追加します。
6. インストールを開始するには、「**開始**」をクリックします。
 7. 完了すると、成功と失敗のログが表示されます。単に再試行することで、一部の失敗は解決できます。これで解決されない場合は、詳細オプションを使用します。詳しくは、IBM Endpoint Manager サポート・サイトのクライアントのインストールに関する記事を参照してください。

クライアントの手動インストール

IBM Endpoint Manager クライアントは、常に、各コンピューターでクライアント・インストーラーを手動で実行することによってインストールできます。これは、少数のコンピューターにクライアントをインストールするための、高速で効果的なメカニズムです。

SUSE (32 ビット) のインストール手順

1. 対応する Endpoint Manager クライアント RPM ファイルを SUSE コンピューターにダウンロードします。
2. 次のコマンドを実行して、RPM をインストールします。

```
rpm -ivh client_RPM_path
```
3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティーの情報が含まれています)。アクション・サイト・マストヘッド (actionsite.afxm) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client の下、Linux の場合は /var/opt/BESInstallers/Client/ の下) にあります。マストヘッドの名前が actionsite.afxm でない場合は、actionsite.afxm に名前を変更し、その場所をコンピューター上の /etc/opt/BESClient/actionsite.afxm にしてください。

注：ディレクトリー /etc/opt/BESClient/ は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、
`http://servername:port/masthead/masthead.afxm` (例: `http://bes.Endpoint
Manager.com:52311/masthead/masthead.afxm`) からダウンロードできます。

4. 以下のコマンドを実行して、エンドポイント・マネージャー Endpoint Manager クライアントを開始します。

```
/etc/init.d/besclient start
```

SUSE (32 ビット) Fixlet コンテンツ:

SUSE Endpoint Manager エージェント用の Fixlet コンテンツを取得するには、Endpoint Manager サーバーで適切な Fixlet サイトをサブスクライブします。新しい Fixlet サイトをサブスクライブするには、以下の手順を実行します。

1. Endpoint Manager コンソールがインストールされているコンピューターに移動します。
2. 該当するマストヘッドをダウンロードします。
3. ファイルのオープンまたは保存を求めるプロンプトが出されたら、「開く」をクリックして Endpoint Manager コンソールを開きます。
4. ユーザー名とパスワードを入力して Endpoint Manager コンソールにログインします。
5. ログインすると、Endpoint Manager コンソールから SUSE Linux Enterprise 向けパッチの Fixlet サイトをサブスクライブするかどうかを尋ねられるので、「OK」をクリックします。
6. プライベート・キーのパスワードを入力し、「OK」をクリックします。

Endpoint Manager コンソールは、このサイトをサブスクライブすると、サイトからの新たな Fixlet メッセージの収集を自動的に開始します。

SUSE (32 ビット) のコンテンツについて詳しくは、<http://support.bigfix.com/bes/sites/susepatches.html> を参照してください。

SUSE Linux Enterprise (64 ビット) のインストール手順

1. 対応する Endpoint Manager クライアント RPM ファイルを SUSE コンピューターにダウンロードします。
2. 次のコマンドを実行して、RPM をインストールします。

```
rpm -ivh client_RPM_path
```

3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (`actionsite.afxm`) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` の下、Linux の場合は `/var/opt/BESInstallers/Client/` の下) にあります。マストヘッドの名前が `actionsite.afxm` でない場合は、`actionsite.afxm` に名前を変更し、その場所をコンピューター上の `/etc/opt/BESClient/actionsite.afxm` にしてください。

注: ディレクトリー `/etc/opt/BESClient/` は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、
`http://servername:port/masthead/masthead.afxm` (例: `http://bes.Endpoint
Manager.com:52311/masthead/masthead.afxm`) からダウンロードできます。

1. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。
`/etc/init.d/besclient start`

Red Hat のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント RPM ファイルを Red Hat コンピューターにダウンロードします。
2. 次のコマンドを実行して、RPM をインストールします。

```
rpm -ivh client_RPM_path
```

3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (`actionsite.afxm`) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` の下、Linux の場合は `/var/opt/BESInstallers/Client/` の下) にあります。マストヘッドの名前が `actionsite.afxm` でない場合は、`actionsite.afxm` に名前を変更し、その場所をコンピューター上の `/etc/opt/BESClient/actionsite.afxm` にしてください。

注: ディレクトリー `/etc/opt/BESClient/` は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、
`http://servername:port/masthead/masthead.afxm` (例: `http://bes.Endpoint
Manager.com:52311/masthead/masthead.afxm`) からダウンロードできます。

4. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。
`/etc/init.d/besclient start`

Red Hat Fixlet コンテンツ:

Red Hat Endpoint Manager エージェント用の Fixlet コンテンツを取得するには、Endpoint Manager サーバーで適切な Fixlet サイトをサブスクライブする必要があります。新しい Fixlet サイトをサブスクライブするには、以下の手順を実行します。

1. Endpoint Manager コンソールがインストールされているコンピューターに移動します。
2. 該当するマストヘッドをダウンロードします。
3. ファイルのオープンまたは保存を求めるプロンプトが出されたら、「開く」をクリックして Endpoint Manager コンソールを開きます。
4. ユーザー名とパスワードを入力して Endpoint Manager コンソールにログインします。
5. ログインすると、Endpoint Manager コンソールから Red Hat Linux 向けパッチの Fixlet サイトをサブスクライブするかどうかを尋ねられるので、「OK」をクリックします。
6. プライベート・キーのパスワードを入力し、「OK」をクリックします。

Endpoint Manager コンソールは、このサイトをサブスクライブすると、サイトからの新たな Fixlet メッセージの収集を開始します。

Red Hat Enterprise Linux について詳しくは、<http://support.bigfix.com/bes/sites/rhelpatches.html> を参照してください。

Solaris のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント・パッケージ・ファイルを Solaris コンピューターにダウンロードします。
2. 次のコマンドを実行して、PKG をインストールします。

```
pkgadd -d package_client_path
```

3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (*actionsite.afxm*) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は *C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client* の下、Linux の場合は */var/opt/BESInstallers/Client/* の下) にあります。マストヘッドの名前が *actionsite.afxm* でない場合は、*actionsite.afxm* に名前を変更し、その場所をコンピューター上の */etc/opt/BESClient/actionsite.afxm* にしてください。

注: ディレクトリー */etc/opt/BESClient/* は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、<http://servername:port/masthead/masthead.afxm> (例: <http://bes.EndpointManager.com:52311/masthead/masthead.afxm>) からダウンロードできます。

4. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。

```
/etc/init.d/besclient start
```

注: すべての Solaris エージェントには、パッケージ *SUNWlibC* がインストールされている必要があります。

Solaris Fixlet コンテンツ:

1. Solaris BES エージェント用の Fixlet コンテンツを取得するには、Endpoint Manager サーバーで適切な Fixlet サイトをサブスクライブする必要があります。新しい Fixlet サイトをサブスクライブするには、Endpoint Manager コンソールがインストールされたコンピューターに移動します。
2. Solaris 評価版マストヘッドをダウンロードします。
3. ファイルのオープンまたは保存を求めるプロンプトが出されたら、「開く」をクリックします。これで Endpoint Manager コンソールが自動的に開きます。
4. ユーザー名とパスワードを入力して Endpoint Manager コンソールにログインします。
5. ログインすると、Endpoint Manager コンソールから Solaris 向けパッチの Fixlet サイトをサブスクライブするかどうかを尋ねられるので、「OK」をクリックします。

6. プライベート・キーのパスワードを入力し、「OK」をクリックします。
7. Endpoint Manager コンソールは、このサイトをサブスクライブすると、サイトからの新たな Fixlet メッセージの収集を自動的に開始します。

HP-UX PA-RISC のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント・パッケージ・ファイルを、HP-UX コンピューターにダウンロードしてコピーします (このコンピューターは PA-RISC システムであることが必要です)。ファイル名の形式は BESAgent-9.1.xxx.x.pa_risc_hpuxxxx.depot です (ダウンロードされたエージェントのバージョンに応じたバリエーションがあります)。

注: Internet Explorer では、ダウンロードされたファイルが .tar ファイルとしてラベル付けされる場合があります。Mozilla およびその他のブラウザでは、ファイルが .depot という拡張子付きでダウンロードされます。

2. 以下のコマンドを実行します。

```
/usr/sbin/swinstall -s HOSTNAME:/path/BESAgent_filename BESAgent
```

指定の内容は以下のとおりです。

HOSTNAME

エージェントがインストールされているシステムの名前です。

/path/ エージェント・インストール・ソースのパスです。

BESAgent_filename

ダウンロードしたファイルの名前です。

以下に例を示します。

```
/usr/sbin/swinstall  
-s hpsystemb:/tmp/BESAgent-9.1.xxx.x.pa_risc_hpuxxxx.depot BESAgent
```

3. アクション・サイト・マストヘッドを HP-UX Endpoint Manager クライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (actionsite.afxm) は、BES インストール・フォルダー (デフォルトの場所は C:¥BES Installers の下) にあります。マストヘッドの名前が actionsite.afxm でない場合は、actionsite.afxm に名前を変更し、その場所をコンピューター上の /etc/opt/BESClient/actionsite.afxm にしてください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、<http://servername:port/masthead/masthead.afxm> からダウンロードできます。

注: ディレクトリー /etc/opt/BESClient/ は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、<http://servername:port/masthead/masthead.afxm> (例: <http://bes.EndpointManager.com:52311/masthead/masthead.afxm>) からダウンロードできます。

4. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。

```
/sbin/init.d/besclient start
```

HP-UX Fixlet コンテンツ:

1. HP-UX BES エージェント用の Fixlet コンテンツを取得するには、Endpoint Manager サーバーで適切な Fixlet サイトをサブスクライブする必要があります。新しい Fixlet サイトをサブスクライブするには、Endpoint Manager コンソールがインストールされたコンピューターに移動します。
2. HP-UX 評価版マストヘッドをダウンロードします。
3. ファイルのオープンまたは保存を求めるプロンプトが出されたら、「開く」をクリックします。これで Endpoint Manager コンソールが自動的に開きます。
4. ユーザー名とパスワードを入力して Endpoint Manager コンソールにログインします。
5. ログインすると、Endpoint Manager コンソールから HP-UX 向けパッチの Fixlet サイトをサブスクライブするかどうかを尋ねられるので、「OK」をクリックします。
6. プライベート・キーのパスワードを入力し、「OK」をクリックします。
7. Endpoint Manager コンソールは、このサイトをサブスクライブすると、サイトからの新たな Fixlet メッセージの収集を自動的に開始します。

HP-UX Itanium のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント・パッケージ・ファイル (BESAgent-9.1.xxxx.x.pa_risc_hpuxxxxx.depot) を HP-UX Itanium コンピューターにダウンロードしてコピーします。
2. 以下のコマンドを実行します。

```
/usr/sbin/swinstall -x "allow_incompatible=true"  
-s HOSTNAME:/path/BESAgent-9.1.xxxx.x.pa_risc_hpuxxxxx.depot  
BESAgent
```

HOSTNAME はエージェントがインストールされているシステムの名前、*/path/* はエージェント・インストール・ソースへのパスです。

3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (actionsite.afxm) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client の下、Linux の場合は /var/opt/BESInstallers/Client/ の下) にあります。マストヘッドの名前が actionsite.afxm でない場合は、actionsite.afxm に名前を変更し、その場所をコンピューター上の /etc/opt/BESClient/actionsite.afxm にしてください。

注: ディレクトリー /etc/opt/BESClient/ は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、
`http://servername:port/masthead/masthead.afxm` (例: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`) からダウンロードできます。

4. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。
`/sbin/init.d/besclient start`

Mac のインストール手順

ディストリビューションには 1 つの DMG (マウント可能なディスク・イメージ・ファイル) が含まれ、そこにユーティリティと、インストール・パッケージまたはアップグレード・パッケージ用の個別の PKG ダウンロードが含まれています。これらのファイルは、ファイル名から 10.6 バージョンと識別されます。Mac クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント・パッケージ・ファイルを Mac コンピューターにダウンロードします。
2. PKG ファイルを任意のディレクトリーにコピーし、適用環境のマストヘッド・ファイルを同じディレクトリーにコピーします。マストヘッド・ファイルの名前が `actionsite.afxm` であることを確認してください。
3. 定義済み設定ファイル (`clientsettings.cfg`) をインストール・ディレクトリーに追加して、インストール時に Mac クライアント用のカスタム設定を作成することができます。
4. PKG ファイル (`BESAgent-9.1.xxx.x-BigFix_MacOSXxx.x.pkg` など) をダブルクリックして PKG インストーラーを起動し、インストーラーを実行します。マストヘッド・ファイルがインストール・ディレクトリーに含まれている場合は、インストール完了後にエージェントが起動されます。

OSX のインストール手順:

ディストリビューションには 1 つの DMG (マウント可能なディスク・イメージ・ファイル) が含まれ、そこにユーティリティと、インストール・パッケージまたはアップグレード・パッケージ用の個別の PKG ダウンロードが含まれています。

1. 対応する Endpoint Manager クライアント・パッケージ・ファイルを Mac コンピューターにダウンロードします。
2. PKG ファイルを任意のディレクトリーにコピーし、適用環境のマストヘッド・ファイルを同じディレクトリーにコピーします。マストヘッド・ファイルの名前が `actionsite.afxm` であることを確認してください。
3. オプションで定義済み設定ファイル (`clientsettings.cfg`) をインストール・ディレクトリーに追加して、インストール時に Mac クライアント用のカスタム設定を作成することができます。
4. PKG ファイル (`BESAgent-9.1.xxx.x-Endpoint Manager_MacOSXxx.x.pkg` など) をダブルクリックして PKG インストーラーを起動し、インストーラーを実行します。マストヘッド・ファイルがインストール・ディレクトリーに含まれている場合は、インストール完了後にエージェントが起動されます。

Mac Fixlet コンテンツ:

Mac Endpoint Manager エージェント用の Fixlet コンテンツを取得するには、Endpoint Manager サーバーで適切な Fixlet サイトをサブスクライブします。新しい Fixlet サイトをサブスクライブするには、以下の手順を実行します。

1. Endpoint Manager コンソールがインストールされているコンピューターに移動します。
2. マストヘッドをダウンロードします。

3. ファイルのオープンまたは保存を求めるプロンプトが出されたら、「開く」をクリックして Endpoint Manager コンソールを開きます。
4. ユーザー名とパスワードを入力して Endpoint Manager コンソールにログインします。
5. ログインすると、Endpoint Manager コンソールから Mac OS X 向けパッチの Fixlet サイトをサブスクライブするかどうかを尋ねられるので、「OK」をクリックします。
6. プライベート・キーのパスワードを入力し、「OK」をクリックします。
7. Endpoint Manager コンソールは、このサイトをサブスクライブすると、サイトからの新たな Fixlet メッセージの収集を開始します。

AIX のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント・パッケージ・ファイルを、IBM AIX コンピューターにダウンロードします。
2. BESAgent を IBM AIX コンピューターにコピーします。
3. 以下のコマンドを実行します。

```
installp -agqYXd ./BESAgent-9.1.xxx.x.ppc_aixxx.pkg BESClient
```

4. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (actionsite.afxm) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client の下、Linux の場合は /var/opt/BESInstallers/Client/ の下) にあります。マストヘッドの名前が actionsite.afxm でない場合は、actionsite.afxm に名前を変更し、その場所をコンピューター上の /etc/opt/BESClient/actionsite.afxm にしてください。

注: ディレクトリー /etc/opt/BESClient/ は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、
`http://servername:port/masthead/masthead.afxm` (例: `http://bes.EndpointManager.com:52311/masthead/masthead.afxm`) からダウンロードできます。

5. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。
`/etc/rc.d/rc2.d/SBESClientd start`

AIX Fixlet コンテンツ:

AIX Endpoint Manager エージェント用の Fixlet コンテンツを取得するには、Endpoint Manager サーバーで適切な Fixlet サイトをサブスクライブします。新しい Fixlet サイトをサブスクライブするには、以下の手順を実行します。

1. Endpoint Manager コンソールがインストールされているコンピューターに移動します。
2. マストヘッドをダウンロードします。
3. ファイルのオープンまたは保存を求めるプロンプトが出されたら、「開く」をクリックして Endpoint Manager コンソールを開きます。

4. ユーザー名とパスワードを入力して Endpoint Manager コンソールにログインします。
5. ログインすると、Endpoint Manager コンソールから AIX 向けパッチの Fixlet サイトをサブスクライブするかどうかを尋ねられるので、「OK」をクリックします。
6. プライベート・キーのパスワードを入力し、「OK」をクリックします。
7. Endpoint Manager コンソールは、このサイトをサブスクライブすると、サイトからの新たな Fixlet メッセージの収集を開始します。

ESX Fixlet コンテンツ

ESX Endpoint Manager エージェント用の Fixlet コンテンツを取得するには、Endpoint Manager サーバーで適切な Fixlet サイトをサブスクライブします。新しい Fixlet サイトをサブスクライブするには、以下の手順を実行します。

1. Endpoint Manager コンソールがインストールされているコンピューターに移動します。
2. マストヘッドをダウンロードします。
3. ファイルのオープンまたは保存を求めるプロンプトが出されたら、「開く」をクリックして Endpoint Manager コンソールを開きます。
4. ユーザー名とパスワードを入力して Endpoint Manager コンソールにログインします。
5. ログインすると、Endpoint Manager コンソールから ESX 向けパッチの Fixlet サイトをサブスクライブするかどうかを尋ねられるので、「OK」をクリックします。
6. プライベート・キーのパスワードを入力し、「OK」をクリックします。

Endpoint Manager コンソールは、このサイトをサブスクライブすると、サイトからの新たな Fixlet メッセージの収集を開始します。

注: 必ずファイアウォール・ポートが開いているようにしてください。

Ubuntu Debian (32 ビット) のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント DEB パッケージ・ファイルを、Ubuntu Debian コンピューターにダウンロードします。
2. 次のコマンドを実行して、DEB をインストールします。

```
dpkg -i client_package_path
```
3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (actionsite.afxm) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client の下、Linux の場合は /var/opt/BESInstallers/Client/ の下) にあります。マストヘッドの名前が actionsite.afxm でない場合は、actionsite.afxm に名前を変更し、その場所をコンピューター上の /etc/opt/BESClient/actionsite.afxm にしてください。

注: ディレクトリー `/etc/opt/BESClient/` は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、
`http://servername:port/masthead/masthead.afxm` (例: `http://bes.EndpointManager.com:52311/masthead/masthead.afxm`) からダウンロードできます。

4. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。

```
/etc/init.d/besclient start
```

Ubuntu/Debian (64 ビット) のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント DEB パッケージ・ファイルを、Ubuntu/Debian コンピューターにダウンロードします。
2. 次のコマンドを実行して、DEB をインストールします。

```
dpkg -i client_package_path
```

3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (`actionsite.afxm`) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` の下、Linux の場合は `/var/opt/BESInstallers/Client/` の下) にあります。マストヘッドの名前が `actionsite.afxm` でない場合は、`actionsite.afxm` に名前を変更し、その場所をコンピューター上の `/etc/opt/BESClient/actionsite.afxm` にしてください。

注: ディレクトリー `/etc/opt/BESClient/` は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、
`http://servername:port/masthead/masthead.afxm` (例: `http://bes.EndpointManager.com:52311/masthead/masthead.afxm`) からダウンロードできます。

4. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。

```
/etc/init.d/besclient start
```

CentOS のインストール手順

クライアントをインストールするには、以下の手順を実行します。

1. 対応する Endpoint Manager クライアント RPM ファイルを Red Hat コンピューターにダウンロードします。
2. 次のコマンドを実行して、RPM をインストールします。

```
rpm -ivh client_RPM_path
```

3. アクション・サイト・マストヘッドをクライアント・コンピューターにコピーします (マストヘッドには、構成、ライセンス、およびセキュリティの情報が含まれています)。アクション・サイト・マストヘッド (`actionsite.afxm`) は、BES インストール・フォルダー (デフォルトの場所は、Windows の場合は `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` の下、Linux の場合は `/var/opt/BESInstallers/Client/` の下) にあります。マストヘ

ッドの名前が actionsite.afxm でない場合は、actionsite.afxm に名前を変更し、その場所をコンピューター上の /etc/opt/BESClient/actionsite.afxm にしてください。

注: ディレクトリー /etc/opt/BESClient/ は、インストーラーで自動的に作成されません。存在していない場合は、手動で作成してください。

各 Endpoint Manager サーバーのマストヘッド・ファイルは、

http://servername:port/masthead/masthead.afxm (例: http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm) からダウンロードできます。

4. 以下のコマンドを実行して、Endpoint Manager クライアントを開始します。

```
/etc/init.d/besclient start
```

MSI を使用したクライアントのインストール

クライアントの Microsoft Installer (MSI) バージョンを使用して、パッケージを解釈し、インストールを自動的に実行することができます。クライアントの MSI バージョン (BESClientMSI.msi) は、Windows サーバーの BESInstallers¥ClientMSI フォルダーまたは Linux サーバーの /ServerInstaller_9.1.xxx.x-rhe6.x86_64/repos/ClientMSI フォルダーに格納されています。

Windows クライアントをインストールするには、以下の手順を実行します。

1. Windows システムの c:¥BESInstallers¥ClientMSI フォルダーに BESClientMSI.msi プログラムをコピーします。
2. 以下のいずれかの方法で BESClientMSI.msi プログラムを実行します。

- `msiexec.exe /i c:¥BESInstallers¥ClientMSI¥BESClientMSI.msi /T=TransformList /qn`

¥qn コマンドはサイレント・インストールを実行します。

- `msiexec.exe /i c:¥BESInstallers¥ClientMSI¥BESClientMSI.msi INSTALLDIR="c:¥myclient" /T=TransformList`

このコマンドは、指定されたディレクトリー (INSTALLDIR="c:¥myclient") にプログラムをインストールします。

注: /T=TransformList は、パッケージに適用する必要があるトランスフォーム・ファイル (.mst) を指定します。TransformList は、セミコロンで区切られたパスのリストです。以下の表に、提供されているトランスフォーム・ファイル、結果として得られる言語、および **msiexec** コマンド行で使用する数値を示します。

表 7. トランスフォーム・ファイル・リスト

言語	トランスフォーム・ファイル名	値
米国英語	1033.mst	1033
ドイツ語	1031.mst	1031
フランス語	1036.mst	1036
スペイン語	1034.mst	1034
イタリア語	1040.mst	1040

表 7. トランスフォーム・ファイル・リスト (続き)

言語	トランスフォーム・ファイル名	値
ブラジル・ポルトガル語	1046.mst	1046
日本語	1041.mst	1041
韓国語	1042.mst	1042
中国語 (簡体字)	2052.mst	2052
中国語 (繁体字)	1028.mst	1028

Microsoft のサイト **Command-Line Options** に、インストール・オプションの全リストが掲載されています。BESClientMSI 適用環境のグループ・ポリシー・オブジェクト (GPO) を作成する方法については、Microsoft サポート技術情報の記事 (<http://support.microsoft.com/kb/887405>) を参照してください。

3. クライアントを開始する前に、Endpoint Manager サーバーにある `actionsite.afxm` マストヘッドをクライアントのインストール・ディレクトリー (デフォルトのインストール・ディレクトリー `C:\Program Files (x86)\BigFix Enterprise\BES Client` または特定のインストール・ディレクトリー `INSTALLDIR="c:\myclient"` にすることができます) にコピーします。
4. BES クライアント・サービスを開始します。

Endpoint Manager 管理ツールの実行

インストール・スクリプト `install.sh` は、IBM Endpoint Manager 管理ツールの `bash` シェル・スクリプト `BESAdmin.sh` を `/opt/BESServer/bin` ディレクトリーに自動的にダウンロードします。このツールにより、マストヘッド・ファイルの編集、データベース内のオブジェクトの署名の確認、拡張セキュリティの有効と無効の切り替え、データベース内のすべてのユーザー・コンテンツへの再署名、サーバー・プライベート・キーのローテーション、コンソールと Web レポートのログインの構成、データベース・コンテンツへの再署名、マストヘッドと更新されたライセンスの同期を行うことができます。

このスクリプトを実行する場合は、以下の構文を使用してコマンド・プロンプトからスーパーユーザーとして実行してください。

```
./BESAdmin.sh -service { arguments | -h }
```

指定の内容は以下のとおりです。

`service` は以下のいずれかにすることができます。

```
editmasthead
findinvalidsignatures
repair
reportencryption
resignsecuritydata
rotateserversigningkey
securitysettings
setadvancedoptions
syncmastheadandlicense
```

各サービスには、以下の引数があります。

editmasthead

以下のパラメーターを指定することにより、マストヘッド・ファイルを編集できます。

advGatherSchedule (optional, integer)
values:
0=Fifteen Minutes,
1=Half Hour, 2=Hour,
3=Eight Hours,
4=Half day,
5=Day,
6=Two Days,
7=Week,
8=Two Weeks,
9=Month,
10=Two Months
advController (optional, integer)
values:
0=console,
1=client,
2=nobody
advInitialLockState (optional, integer)
values:
0=Locked,
1=timed (specify duration),
2=Unlocked
advInitialLockDuration (optional, integer)
values:
(duration in seconds)
advActionLockExemptionURL (optional, string)

advRequireFIPSCompliantCrypto (optional, boolean)

このサービスを実行するための構文は以下のとおりです。

```
./BESAdmin.sh -editmasthead -sitePvkLocation=<path+license.pvk>  
[ -sitePvkPassword=<password> ] [ -display ]  
[ -advGatherSchedule=<0-10> ] [ -advController=<0-2> ]  
[ -advInitialLockState=<0|2> ] [ -advInitialLockState=1  
-advInitialLockDuration=<num> ] [ -advActionLockExemptionURL=<url> ]  
[ -advRequireFIPSCompliantCrypto=<true|false> ]
```

追加情報については、「*IBM Endpoint Manager 構成ガイド*」を参照してください。

findinvalidsignatures

以下のパラメーターを指定することにより、データベース内のオブジェクトの署名を検査することができます。

-resignInvalidSignatures (オプション)

BESAdmin が検出したすべての無効な署名への再署名を試行します。

-deleteInvalidlySignedContent (オプション)

無効な署名を持つコンテンツを削除します。

無効な署名について詳しくは、<http://www-01.ibm.com/support/docview.wss?uid=swg21587965>を参照してください。このサービスを実行するための構文は以下のとおりです。

```
./BESAdmin.sh -findinvalidsignatures  
[ -resignInvalidSignatures | -deleteInvalidlySignedContent ]
```

repair

修復ユーティリティーを使用すると、データベースに保存されたキーとファイル・システムに保存されたキーとの間の不整合を処理することができます。以下のコマンドを実行すると、データベースに保存されたキーからファイル・システム上のキーが再作成されます。

```
./BESAdmin.sh -repair -sitePvkLocation=<path+license.pvk>  
[ -sitePvkPassword=<password> ]
```

reportencryption

レポート・メッセージの暗号化の生成、ローテーション、有効化、および無効化を行うには、以下のコマンドを実行します。

```
./BESAdmin.sh -reportencryption -sitePvkLocation=<path+license.pvk>  
[-sitePvkPassword=<password>]  
{  
  -status  
  -generatekey [-privateKeySize=<min|max>] [-deploynow=yes|-deploynow=no -outkeypath=<path>]  
  -rotatekey [-privateKeySize=<min|max>] [-deploynow=yes|-deploynow=no -outkeypath=<path>]  
  -enablekey | -disablekey }  
}
```

指定の内容は以下のとおりです。

status 暗号化のステータス、およびそのステータスで使用する引数を示します。

generatekey

新規の暗号化キーを生成することができます。

rotatekey

暗号化キーを変更することができます。

enablekey

暗号化キーを有効にすることができます。

disablekey

暗号化キーを「保留中」状態にすることができます。disablekey 引数を指定して reportencryption コマンドをもう一度実行すると、暗号化は「保留中」状態から「無効」状態に変更されます。

このコマンドおよび動作について詳しくは、クライアントの暗号化の管理を参照してください。

resignsecuritydata

データベース内のすべてのユーザー・コンテンツに再署名して、コンソールへのユーザー・ログインを可能にすることができます。このコマンドは、既存のキー・ファイルを使用してセキュリティ・データに再署名します。以下のパラメーターを指定することができます。

```
-mastheadLocation=<path+/actionsite.afxm>
```

このサービスを実行するための完全な構文は以下のとおりです。

```
./BESAdmin.sh -resignsecuritydata -sitePvkLocation=<path+license.pvk>  
[ -sitePvkPassword=<password> ] -mastheadLocation=<path+/actionsite.afxm>
```

rotateserversigningkey

サーバー・プライベート・キーをローテーションして、ファイル・システム内のキーをデータベース内のキーに一致させることができます。このコマンドは、新

しいサーバー署名キーを作成し、その新しいキーを使用してすべての既存のコンテンツに再署名し、古いキーを取り消します。

このサービスを実行するための構文は以下のとおりです。

```
./BESAdmin.sh -rotateserversigningkey -sitePvkLocation=<path+license.pvk>  
[ -sitePvkPassword=<password> ]
```

securitysettings

NIST セキュリティー標準に準拠するように拡張セキュリティー・オプションを構成するには、以下のコマンドを実行します。

```
./BESAdmin.sh -securitysettings -sitePvkLocation=<path+license.pvk>  
[ -sitePvkPassword=<password> ]  
{ -status | -enableEnhancedSecurity [-requireSHA256Downloads]  
  -disableEnhancedSecurity | -requireSHA256Downloads  
  -allowSHA1Downloads } }
```

指定の内容は以下のとおりです。

status IBM Endpoint Manager 環境に設定されたセキュリティー設定のステータスを示します。

例:

```
BESAdmin.sh -securitysettings -sitePvkLocation=/root/backup/license.pvk  
-sitePvkPassword=mypassw0rd -status
```

```
Enhanced security is currently ENABLED  
SHA-256 downloads are currently OPTIONAL
```

enableEnhancedSecurity | disableEnhancedSecurity

すべてのデジタル署名とコンテンツ検証に SHA-256 暗号ダイジェスト・アルゴリズムが採用され、Endpoint Manager コンポーネント間通信に TLS 1.2 プロトコルが採用される、拡張セキュリティーを有効または無効にします。

注: IBM Endpoint Manager バージョン 9.0 以前のコンポーネントは IBM Endpoint Manager バージョン 9.1 のサーバーやリレーと通信できないため、**enableEnhancedSecurity** 設定を使用すると後方互換性がなくなります。

requireSHA256Downloads

SHA-256 アルゴリズムを使用してダウンロードした後もデータが変更されていないようにします。

注: 「SHA-256 ダウンロードが必要 (Require SHA-256 Downloads)」オプションは、「拡張セキュリティーを有効にする」を選択した場合にのみ使用できます。

allowSHA1Downloads

必ず SHA-1 アルゴリズムを使用してファイル・ダウンロードの整合性チェックが実行されるようにします。

IBM Endpoint Manager の拡張セキュリティー機能およびサポートされるセキュリティー構成について詳しくは、27 ページの『第 4 章 セキュリティー構成シナリオ』を参照してください。

setadvancedoptions

特定のインストール済み環境に適用されるグローバル設定をリストするか、構成することができます。例えば、以下のコマンドを入力して、コンソールまたは Web レポートのログイン・バナーが表示されるように設定することができます。

```
./BESAdmin.sh -setadvancedoptions -sitePvkLocation=/root/backup/license.pvk  
-sitePvkPassword=pippo000 -update loginWarningBanner='new message'
```

このサービスを実行するための完全な構文は以下のとおりです。

```
./BESAdmin.sh -setadvancedoptions -sitePvkLocation=<path+license.pvk>  
[-sitePvkPassword=<password>]  
{  
  -list | -display  
  | [ -f ] -delete option_name  
  | [ -f ] -update option_name=option_value }  
}
```

指定可能な詳細オプションの一部を以下に示します。

表 8. 詳細設定の名称

名前	値
loginWarningBanner	テキストを設定すると、コンソールまたは Web レポートにログインしたすべてのユーザーに対して、そのテキストが表示されます。ユーザーが次に進むには「OK」をクリックする必要があります。
timeoutLockMinutes	コンソールで再認証が必要になるまでのアイドル時間 (分単位)。これは loginTimeoutSeconds とは異なります。このタイムアウト・ロックではコンソール全体が表示されなくなるため、他のユーザーは、コンソールを表示することも使用することもできなくなります。アイドル時間は、キー・ボタン、マウス・クリック、マウス移動など、セッション内でどのような種類の入力も行われない状態を指します。

注: 非効率的な MIME 拡張オプションは 9.1 サーバーでサポートされなくなりました。既存のアクションは引き続きクライアントで実行されますが、サーバーは非効率的な MIME アクションを生成することはできません。

syncmastheadandlicense

製品をアップグレードする場合は、このオプションを使用して更新ライセンスをマストヘッドと同期させ、データベース内のすべてのコンテンツを SHA-256 で再署名する必要があります。このサービスを実行するための構文は以下のとおりです。

```
./BESAdmin.sh -syncmastheadandlicense -sitePvkLocation=<path+license.pvk>  
[-sitePvkPassword=<password>]
```

Linux システム上のプライマリー・サーバーの削除

IBM Endpoint Manager サーバーをアンインストールするには、サービスを停止し、サーバー、クライアント、Web レポート・コンポーネント、および関連するデータベースを削除する必要があります。

Linux システム上のプライマリー・サーバーをアンインストールするには、以下の手順を実行します。

1. サーバー、クライアント、および Web レポートの rpms ファイルを削除します。

```
rpm -e BESRootServer-xxxx_rhel.i686
rpm -e BESClient-xxxxxx_rhel.x86-64
rpm -e BESWebReports-xxxx-rhel.i686
```

2. 以下のディレクトリーを削除します。

```
rm -fr /var/opt/BESClient
rm -fr /etc/opt/BESClient
rm -fr /var/opt/BESServer
rm -fr /etc/opt/BESServer
rm -fr /var/opt/BESWebReportsServer
```

3. ローカル・データベースの BFENT と BESREPOR を削除します。

```
su - db2inst1
db2 drop db BFENT
db2 drop db BESREPOR
```

または、BFENT および BESREPOR リモート・データベースを削除します。

```
db2 uncatalog db BFENT
db2 uncatalog db BESREPOR
db2 uncatalog node TEM_RER
```

Linux レプリケーション・サーバーのアンインストール

レプリケーション・サーバーをアンインストールするには、データベース・ストアド・プロシージャ `delete_replication_server` を呼び出します。これにより、指定した ID がレプリケーション・セットから削除されます。削除するサーバーの ID を必ず指定してください。DB2 データベースにログインして以下のプロシージャを実行する必要があります。

```
call dbo.delete_replication_server(n)
```

ここで *n* は、削除するサーバーの ID です。

第 10 章 インストール後の構成手順

インストールを実行したら以下のトピックを読み、必要な作業を行ってください。

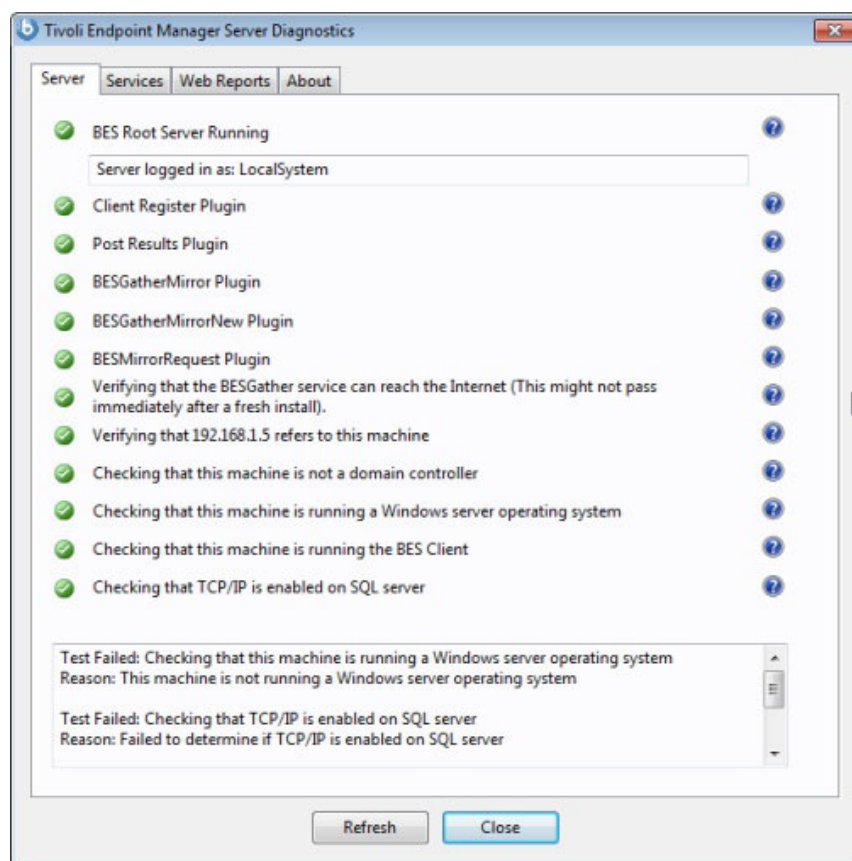
ポストインストール・ステップ

製品をインストールしたら、以下の手順を実行して、インストールが正しく実行されたことを確認し、基本構成ステップを完了してください。

1. 以下の手順を実行して、インストールが正しく実行されたことを確認します。

Windows の場合:

「スタート」>「すべてのプログラム」>「Tivoli Endpoint Manager」から IBM Endpoint Manager サーバー診断ツールを実行して、インストールと構成のすべてのステップが正常に完了したことを確認します。



すべてのボタンが緑色になっていれば、「閉じる」をクリックして診断ツールを終了します。緑色以外のボタンがある場合は、その問題に対処して、サーバーが正しく動作するようにしてください。

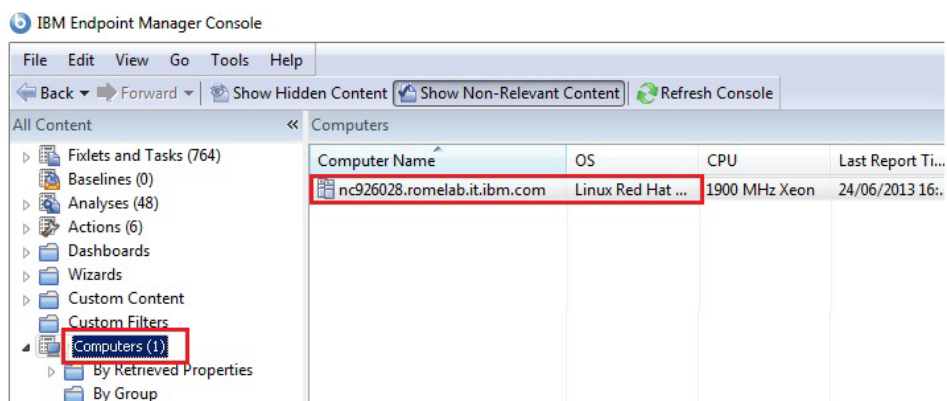
Linux の場合:

以下の各サービスが開始されて稼働していることを確認します。

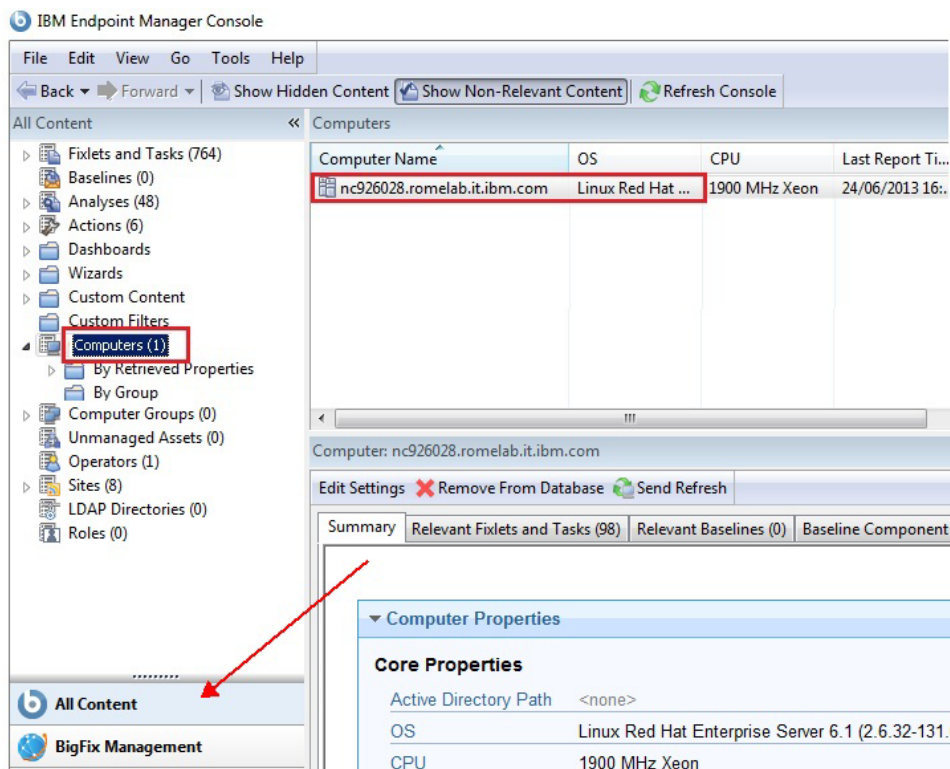
besfilldb
besgatherdb
besserver
beswebreports

service service status コマンドを使用して、各サービスの状況を確認します。

2. Endpoint Manager コンソールを開き、クライアントが登録されていることを確認します。

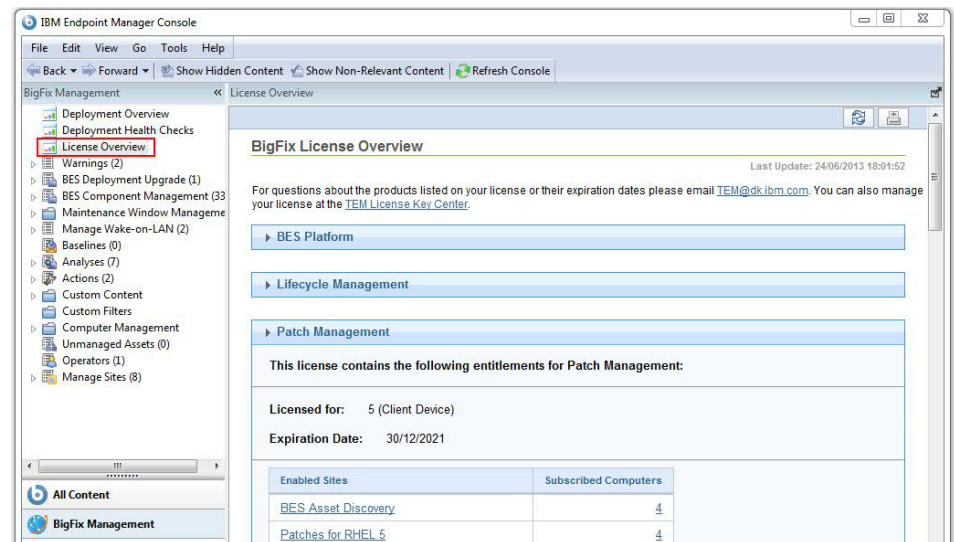


3. コンソールから、「すべてのコンテンツ」ドメインと「BigFix 管理」ドメインが作成されていることを確認します。



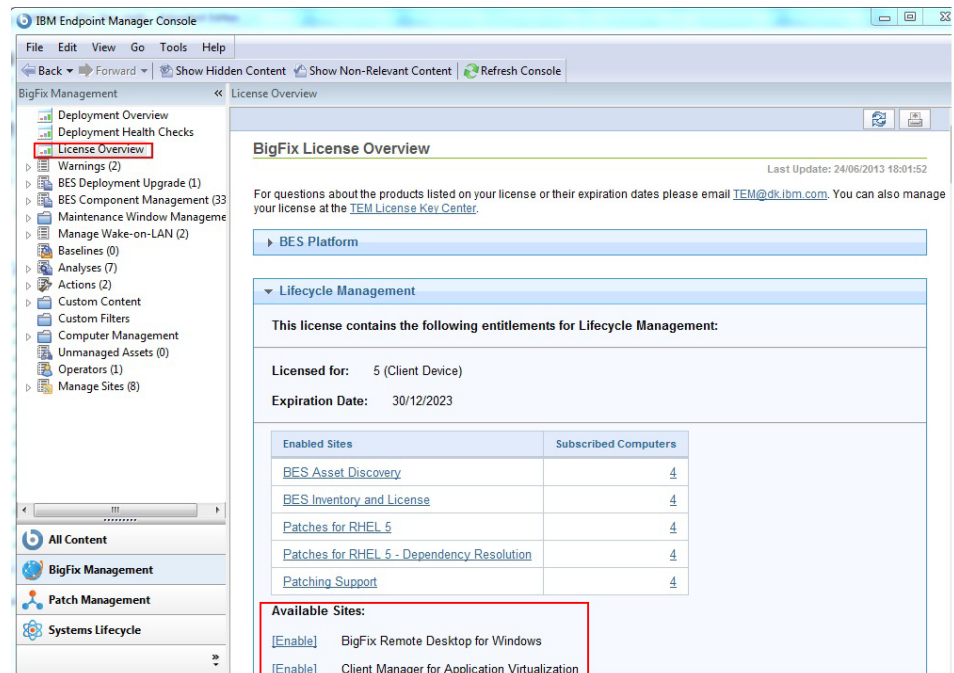
4. インストール後に、プログラムは、特定の管理サイトおよびメンテナンス・サイトをサブスクライブするように自動的にセットアップされます。ライセンスの条件によっては、他のサイトもサブスクライブする場合があります。この方法により、これらのサイトから企業内にコンテンツが自動的に送信され、

Endpoint Manager クライアントを実行しているすべてのコンピューターで、それらのコンテンツの関連度が評価されます。以下の図のように「**ライセンスの概要**」ダッシュボードを選択して、「**BigFix 管理**」ドメインからこれらのサイトをサブスクライブします。



「ライセンスの概要」ダイアログが表示され、使用可能なサイトがリストされます。

- サブスクライブしたいサイトに対応する「**有効化**」ボタンをクリックして、サブスクライブが許可されているサイトを有効にします。



- パスワードを入力してサイトをサブスクライブします。これで、新規サイトがドメイン・パネルの「**サイトを管理**」ノードにリストされます。マストヘッド・ファイルを使用してサイトをサブスクライブすることもできます。詳細については、コンソール・ガイドの『マストヘッドを使用したサブスクライブ』を参照してください。

7. 「**サイトを管理**」ノードを開き、新しくサブスクライブしたサイトを選択します。
8. サイト・ダイアログで「**コンピューターのサブスクリプション**」タブをクリックして、そのサイトを適切なコンピューターに割り当てます。
9. 「**オペレーター許可**」タブで、このサイトに関連付けるオペレーターとそれらのオペレーターの許可レベルを選択します。
10. 完了したら、「**変更を保存**」をクリックします。

これで、製品を使用できるようになりました。

Fixlet サイトのサブスクライブ

サイトは、ユーザー本人、IBM、またはベンダーが内部的に作成した Fixlet のコレクションです。サイトをサブスクライブし、Fixlet の最新パッチをダウンロードするためのスケジュールに同意します。

ベンダーまたは IBM からマストヘッド・ファイルを取得することで、新しいサイト・サブスクリプションを追加できます。また、ライセンス・ダッシュボードを使用してサイトをサブスクライブすることもできます。

サイトは、通常、ソフトウェアまたはハードウェアの特定部分のセキュリティやメンテナンスなど、単一のトピックのみ取り上げます。ただし、一部のサイトには共通する特徴が存在する場合があります。そうしたサイトはドメインにグループ化されます。ドメインには、さまざまなコンソール・マネージャーの標準的なジョブ・タスク・セットが存在する場合があります。例えば、一般的な操作環境のパッチ適用と保守を行うユーザーは、パッチ管理ドメインにバンドルされている、各種オペレーティング・システムのすべてのサポート・サイトとパッチ・サイトにアクセスすることができます。

独自のカスタム・サイトをセットアップし、独自のネットワーク用に特別に開発した Fixlet を、そのサイトに配置することもできます。その後、ユーザー本人および他のオペレーターは、最新の組織内用パッチを送受信でき、それらを適切なロケーションおよび部門に迅速に適用できます。

インストール時に、プログラムは、特定の管理サイトおよびメンテナンス・サイトをサブスクライブするように自動的にセットアップされます。ライセンスの条件によっては、他のサイトもサブスクライブする場合があります。つまり、それらのサイトから企業内にコンテンツが自動的に流れ込み、IBM Endpoint Manager クライアントを実行しているすべてのコンピューターで、それらのコンテンツの関連度が評価されます。次に、それらのサイトは適切なドメインに自動的に登録され、コンテンツを機能セクションに分割するための簡単な方法が提供されます。

マストヘッドを使用したサブスクライブ

マストヘッド・ファイルを使用してサイトをサブスクライブするには、次の手順に従います。

1. 適切なサイトを検出します。サイトを検出することと、サイトのマストヘッド・ファイル (拡張子は .efxm) を検出することは同等です。以下に、これを行ういくつかの方法を示します。

Fixlet サイト:

IBM は、新しいサイトが使用可能になると、そのサイトへのリンクをリスト形式で通知します。

Fixlet サブスクリプション:

Fixlet メッセージにより、サブスクリプションが提供される場合があります。Fixlet アクションをクリックして、サブスクリプションを開始します。

マストヘッドのダウンロード:

ベンダーの Web サイトからマストヘッド・ファイルをダウンロードすることでもサイトをサブスクライブできます。マストヘッドをコンピューターに保存したら、以下のいずれかの方法でそのマストヘッドをアクティブにすることができます。

- マストヘッドをダブルクリックします。
- 「ツール」メニューの「外部サイト・マストヘッドの追加」を選択し、マストヘッドが含まれるフォルダーを参照し、「開く」をクリックします。

2. プライベート・キーのパスワードを入力するよう要求するプロンプトが出されます。パスワードを入力し、「OK」をクリックします。

マストヘッドはすべてのクライアントに伝達され、それらのクライアントは、新しいサイトからの Fixlet の評価を直ちに開始します。

ライセンス・ダッシュボードを使用したサブスクライブ

ドメイン・パネルの BigFix 管理のライセンス・ダッシュボードを使用して、Fixlet サイトをサブスクライブすることもできます。

1. 「BigFix 管理」ドメインを開き、上にスクロールして関連するダッシュボードを表示します。
2. 「ライセンス・ダッシュボード (Licensing Dashboard)」からサブスクライブするサイトを選択します。

第 11 章 リレーの管理

リレーにより、インストールのパフォーマンスを大幅に向上させることができます。リレーにより、サーバーのアップストリームとダウンストリームの両方の負荷が軽減されます。サーバーと直接通信する代わりに、指定のリレーと通信するようにクライアントに指示できます。これにより、サーバーの負荷が大幅に軽減され、クライアントとサーバーの間のネットワーク・トラフィックが大幅に削減されます。リレーによって以下が実現することで、パフォーマンスが向上します。

- **ダウンストリーム・トラフィックの削減。**リレーを使用すると、IBM Endpoint Manager サーバーはファイル（パッチやソフトウェア・パッケージなど）と Fixlet をすべてのクライアントに配布する必要がなくなります。代わりに、ファイルはリレーに 1 度だけ送信され、その後、リレーがそのファイルをクライアントに配布します。
- **アップストリーム・トラフィックの削減。**リレーは、アップストリーム方向では、効率性を向上させるために、クライアントからのデータ（Fixlet 関連、アクションの状態、取得プロパティなど）を圧縮し、パッケージ化できます。
- **低帯域幅接続での輻輳の削減。**リモート・オフィス内の複数のコンピューターと低速接続で通信するサーバーがある場合、それらのコンピューターのうちの 1 台をリレーに指定します。サーバーは、単一のコピーのみをリレーに送信します（リレーが必要とする場合）。そのリレーは、その後、専用高速 LAN を通じて、リモート・オフィス内の他のコンピューターにそのファイルを配布します。

適切なリレー構造を確立することは、IBM Endpoint Manager を大規模ネットワークにインストールするための最も重要な側面の 1 つです。リレーが全体に適用されている場合、大規模ダウンロードに伴うアクションを、最小限の WAN 使用量で、数万のコンピューターに迅速かつ容易に送信できます。

各リレーに 500 から 1000 クライアントを接続することと親子リレー構成を使用することが推奨される構成です。

注：リレーとサーバーの間の接続が非常に低速である場合、ダウンロードのためにリレーをインターネットに直接接続した方が適切な場合があります。

リレーに関する追加情報については、リレーのページを参照してください。

リレーの要件と推奨事項

通常、リレーは最小限のリソースしか使用しないため、リレーを実行しているコンピューターのパフォーマンスはほとんど影響を受けません。ただし、複数のクライアントが同一のリレーからのファイルを同時に要求した場合は、それらのファイルを提供するために、かなりの量のコンピューター・リソースを使用する可能性があります。

リレー・コンピューターの要件は、以下の 3 つの主要因に応じて大きく変わります。

- ファイルをダウンロードする接続クライアントの数

- 各ダウンロードのサイズ
- ダウンロードに割り振られた時間

リレーのシステム要件は、ワークグループ・ファイル・サーバーの要件と似ています。リレーの要件について詳しくは、「IBM Endpoint Manager 9.1 - System Requirements」を参照してください。

以下に、追加の推奨事項を示します。

- リレーを実行するコンピューターには、IBM Endpoint Manager エージェントがインストールされている必要があります。
- リレーのインストール候補として適しているのは、ワークグループ・ファイル・サーバーを始め、常時電源が入っているサーバー品質のコンピューターです。
- IBM Endpoint Manager リレーは、その親（サーバーまたは別のリレー）に対して両方向の TCP 接続を行う必要があります。
- リレーを実行するコンピューターでは、適切に動作するために Internet Explorer 4.0 以降を使用する必要があります。
- IBM Endpoint Manager リレーのキャッシュ・サイズは構成できますが、デフォルトでは 1 GB に設定されています。ハード・ディスクがボトルネックにならないようにするために、リレーのキャッシュとして 2 GB 以上使用できるようにすることをお勧めします。
- 帯域幅上の理由から、各地理的位置に少なくとも 1 つのリレーを配置することをお勧めします。
- 非常に低速のパイプでファイルをダウンロードするリレーについては、帯域幅使用量のスロットリングを検討してください。ダイヤルアップまたは低速の VPN 接続で接続しているクライアントについては、帯域幅使用量をスロットリングすることをお勧めします。帯域幅スロットリングについて詳しくは、「Bandwidth Throttling」を参照してください。

リレーのセットアップ

リレーをセットアップするには、クライアントを実行している Windows、Red Hat Enterprise Linux、または Solaris のコンピューターを、リレーとして機能するように指定する必要があります。サポートされるオペレーティング・システムについて詳しくは、「IBM Endpoint Manager 9.1 - System Requirements」を参照してください。

ネットワーク上の IBM Endpoint Manager クライアントは、新規リレーを検出し、自動的にそのリレーに接続します。クライアント・コンピューターをリレーとして構成するには、以下の手順を実行します。

1. IBM Endpoint Manager コンソールにログインします。
2. ドメイン・パネルで「Fixlet とタスク」アイコンを開き、「タスクのみ」をクリックします。
3. 「IBM Endpoint Manager リレーのインストール」というラベル（後にバージョン番号が含まれる場合があります）が付いたタスクをダブルクリックします。このタスクは、リレーの要件を満たすクライアントが少なくとも 1 つある場合に適用されます。

4. タスク内のアクションのいずれかを選択して、適用オプションを選択します。このアクションで、1 つまたは複数のコンピューターを対象として指定することができます。

リレーの作成が完了したら、クライアントはリレーを自動的にディスカバーして接続することができます。この場合は常に、経由するホップ数が最も少ないリレーが検出されます。

クライアントへのリレーの割り当て

リレーをセットアップする場合は、ネットワークの IBM Endpoint Manager クライアントに、サーバーからでなくそのリレーから情報を収集するように指示する必要があります。以下のことが可能です。

- リレーを手動で割り当てます。これについては以下のトピックを参照してください。
 - 『クライアント・インストール時のリレーの割り当て』
 - 145 ページの『既存のクライアントへのリレーの手動割り当て』
- リレーを自動で割り当てます。つまり、クライアントが最も近いリレーを識別して接続できるようにします。これについては以下のトピックを参照してください。
 - 146 ページの『クライアント・インストール時のリレーの自動割り当て』
 - 146 ページの『既存のクライアントへのリレーの自動割り当て』

この方法を選択した場合は、リレー・アフィリエーション機能を活用することもできます。この機能を使用して、アフィリエイトのあるクライアントのグループを作成し、そのアフィリエーション・グループにリレーを割り当てます。この機能および使用方法について詳しくは、147 ページの『リレー・アフィリエーションの使用』を参照してください。

リレーの自動割り当てについての詳細および考慮事項については、148 ページの『リレーの自動割り当てに関する注意事項』を参照してください。

クライアント・インストール時のリレーの割り当て

デフォルトで、Endpoint Manager クライアントはインストール時にメインの Endpoint Manager サーバーに接続するように設定されています。

必要に応じて、クライアントのインストール時に、特定の Endpoint Manager リレーを割り当てるように Endpoint Manager クライアントを構成できます。以下のトピックで説明されているように、クライアント・オペレーティング・システムによって、異なる手順を実行する必要があります。

- 144 ページの『Windows クライアント』
- 144 ページの『UNIX クライアント』
- 144 ページの『Mac クライアント』

Windows クライアント

clientsettings.cfg という名前で、以下のコンテンツを含む 3 行のファイルを作成し、そのファイルを Endpoint Manager クライアントのインストール・フォルダー (setup.exe) に格納して、プライマリーとバックアップのリレーを設定します。

```
IP:http://besrelayserver.domain.com:52311/bfmirror/downloads/  
__RelayServer1=http://relay.domain.com:52311/bfmirror/downloads/  
__RelayServer2=http://relay2.domain.com:52311/bfmirror/downloads/
```

注: この手法は、Endpoint Manager クライアントのインストール・パッケージの MSI バージョンに対しては機能しません。

Mac クライアント

clientsettings.cfg ファイルは、Mac クライアント上に設定を作成するために、Mac クライアント・インストーラーによっても使用されます。

リレーを設定するには、以下の行を clientsettings.cfg ファイルに追加します。

```
IP:http://besrelayserver.domain.com:52311/bfmirror/downloads/  
__RelayServer1=http://relay.domain.com:52311/bfmirror/downloads/
```

インストールを実行する前に、シェルから、BESAgent-9.1.xxx.x-BigFix_MacOSXxx.x.pkg/Contents/Resources にある Mac クライアント・インストーラー・パッケージに clientsettings.cfg ファイルを追加します。

Finder で、BESAgent-9.1.xxx.x-BigFix_MacOSXxx.x.pkg ファイルを右クリックし、「パッケージの内容を表示」を選択してパッケージ内をナビゲートします。

このインストール・パッケージは、BEAgent Installer Builder アプリケーションによって作成され、読み取り専用の .dmg 圧縮ファイルに組み込まれます。パッケージを編集する必要がある場合は、この読み取り専用ディスク・イメージからコピーしてください。

UNIX クライアント

インストール時にリレーを UNIX クライアントに割り当てるには、以下の手順を実行します。

1. 以下の行を使用して、/var/opt/BESClient/ の下に besclient.config ファイルを作成します。

```
[Software¥BigFix¥EnterpriseClient]  
EnterpriseClientFolder = /opt/BESClient  
  
[Software¥BigFix¥EnterpriseClient¥GlobalOptions]  
StoragePath = /var/opt/BESClient  
LibPath = /opt/BESClient/BESLib  
  
[Software¥BigFix¥EnterpriseClient¥Settings¥Client¥__RelayServer1]  
effective date = [Enter current date and time in standard format]  
value = http://relay.domain.com:52311/bfmirror/downloads/  
  
[Software¥BigFix¥EnterpriseClient¥Settings¥Client¥__RelayServer2]  
effective date = [Enter current date time in standard format]  
value = http://relay2.domain.com:52311/bfmirror/downloads/
```

```
[Software¥BigFix¥EnterpriseClient¥Settings¥Client¥__RelaySelect_Automatic]
effective date = [Enter current date time in standard format]
value = 0
```

2. このディレクトリーとファイルが root によって所有されており、他のユーザーが書き込めない設定になっていることを確認します。そのような設定であれば、UNIX クライアント・インストーラーを実行してクライアントをインストールするときに、以下のように設定されている /var/opt/BESClient/besclient.config がインストーラーによって再作成されたり、上書きされたりすることがなくなります。

```
[Software¥BigFix¥EnterpriseClient]
EnterpriseClientFolder = /opt/BESClient
```

```
[Software¥BigFix¥EnterpriseClient¥GlobalOptions]
StoragePath = /var/opt/BESClient
LibPath = /opt/BESClient/BESLib
```

3. effective date = [Enter current date and time in standard format] には、日時を設定します。例えば、日時の標準形式は次のようになります。

```
Wed, 06 Jun 2012 11:00:00 -0700
```

effective date = {now} は、{} 大括弧がインライン関連度の使用を暗黙指定し、**now** がキーワードであるため指定できません。

4. value = http://relay.domain.com:52311/bfmirror/downloads/ では、relay.domain.com の部分を希望するリレーに変更します。

ヒント: 特定の Linux クライアントに対してリレーを手動で割り当てることで、besclient.config の現在のコンテンツを取得して検証した後、特定の行を besclient.config ファイルからコピーして、他のシステムで使用できます。

注: Endpoint Manager リレーの選択に問題のあるクライアントのトラブルシューティングについて詳しくは、<http://www-01.ibm.com/support/docview.wss?uid=swg21506065> を参照してください。

詳細設定の追加

新しいクライアントのインストール中に他のクライアント設定を追加するには、クライアントのインストール中に設定されるクライアント設定ごとに 1 行を含めます。例えば、ファイルは以下のようになります。

```
__RelayServer1=http://relay.domain.com:52311/bfmirror/downloads/
__BESClient_Inspector_ActiveDirectory_Refresh_Seconds=43200
__BESClient_Log_Days=10
...
```

設定可能なクライアント設定について詳しくは、<http://www-01.ibm.com/support/docview.wss?uid=swg21506065> を参照してください。

既存のクライアントへのリレーの手動割り当て

どのクライアントがどのリレーに接続する必要があるか、手動で正確に指定することが必要な場合があります。これを行うには、以下の手順を実行します。

1. コンソールを起動し、「BigFix 管理」ドメインを選択します。「コンピューター管理」フォルダーで「コンピューター」をクリックして、リスト・パネルにクライアントのリストを表示します。
2. 特定のリレーに接続するコンピューターのセットを選択します。
3. この強調表示されたセットを右クリックし、ポップアップ・メニューから「コンピューターの設定を編集」を選択します。リレーを作成したとき (上記) と同様に、1 つのコンピューターを選択した場合と、複数のコンピューターを選択した場合では、ダイアログ・ボックスはわずかに異なります。
4. 「プライマリー・リレー」というボックスにチェック・マークを付け、使用可能なリレー・サーバーのドロップダウン・リストからコンピューター名を選択します。
5. 同様に「セカンダリー・リレー」も割り当てることができます。これは、プライマリー・リレー・サーバーが何らかの理由で使用不能になった場合に、いつでもバックアップとして動作します。
6. 「OK」をクリックします。

クライアント・インストール時のリレーの自動割り当て

クライアントをインストールする際に、最も近いリレーをデフォルトで自動的に検出したい場合があります。これを設定するには、以下の手順を実行します。

1. 「コンピューターの設定を編集」ダイアログを開きます。
2. 「対象」タブを選択します。
3. 「そのプロパティーを持つすべてのコンピューター (All computers with the property)」というボタンをクリックします。
4. 下のウィンドウで、「すべてのコンピューター」を選択します。
5. 「制約」タブを選択します。
6. 「失効日 (Expires On)」ボックスをクリアします。
7. 「OK」をクリックします。

新しいクライアントがインストールされると、そのクライアントは、追加のアクションを実行することなく、最も近いリレーを自動的に検出して接続します。

既存のクライアントへのリレーの自動割り当て

最も近いリレーを自動的に検出し、サーバーの代わりにそのコンピューターをポイントするように、クライアントを構成することができます。管理のオーバーヘッドを最小限にして、動的にシステムのバランスを取るため、この技法が推奨されます。クライアントは経由するホップ数が最も少ないリレーを判別できるので、トポロジーが最適化されます。

ラップトップの接続や切り離し、コンピューターの起動やシャットダウン、新規ハードウェアの追加やハードウェアの取り外しなどによって、ネットワーク構成が絶えず変化する場合は、この動作が重要となります。クライアントは、構成を動的に評価し、ネットワークの変更に応じて最も効率のよい接続を維持することができます。

クライアントが自動的にリレーを検出するようにセットアップするには、以下の手順を実行します。

1. コンソールを起動し、「**BigFix 管理**」ドメインを選択します。「コンピューター管理」フォルダーで「**コンピューター**」ノードをクリックして、リスト・パネルにクライアントのリストを表示します。
2. Shift キーまたは Ctrl キーを押しながらクリックして、自動的にリレーを検出させるコンピューターのセットを選択します。**Ctrl+A** を押すと、クライアントのセット全体が選択されます。
3. この強調表示されたセットを右クリックし、ポップアップ・メニューから「**コンピューターの設定を編集**」を選択します。1 つのコンピューターを選択したか、複数のコンピューターを選択したかによって、ダイアログ・ボックスは若干異なります。通常、ネットワーク内のすべてのクライアントを選択するため、複数選択ダイアログが表示されます。
4. 「**リレーの選択方法**」にチェック・マークを付けます。
5. 「**最適なリレーを自動的に検出**」をクリックします。
6. 「**OK**」をクリックします。

リレー・アフィリエイトの使用

リレー・アフィリエイトは、自動リレー選択用のより高度な制御システムを提供します。この機能は、非常に柔軟で、多様な方法で使用できますが、主に、IBM Endpoint Manager インフラストラクチャーを個別の論理グループに分割するために使用されます。クライアントとリレーのセットを同じアフィリエイト・グループに配置して、クライアントがそのアフィリエイト・グループ内のリレーのみの選択を試行するようにできます。リレー・アフィリエイト機能は、自動リレー選択に基づいて構築されています。このため、リレー・アフィリエイトを実施する前に、自動リレー選択のプロセスを理解する必要があります (前のセクションを参照)。

リレー・アフィリエイトは、自動リレー選択プロセスにのみ適用されます。コンピューターをリレー・アフィリエイト・グループに配置しても、手動リレー選択プロセス (次のセクションを参照) は影響を受けません。

リレー・アフィリエイト・グループ名の選択

事前定義済みのリレー・アフィリエイト・グループ名はありません。ご使用の IBM Endpoint Manager 適用環境に対応した分かりやすい任意のグループ名を選択できます。以下の命名規則に従ってください。

- 名前を選択するとき、特殊文字 (「.」など) は使用しないでください。
- グループ名では大/小文字は区別されません。
- 先頭および末尾の空白は、比較では無視されます。

リレー・アフィリエイト・グループを整理することは、クライアントにとって重要です。アスタリスク (*) は、リレー・アフィリエイト・リストでは特別な意味を持ちます。アスタリスクは、アフィリエイトなしのコンピューターのセットを表します。アフィリエイトなしのコンピューターとは、リレー・アフィリエイト

ョン・グループ割り当てのないクライアントまたはリレーです。または、アスタリスク・グループ・リストが適用されるクライアントまたはリレーです。

リレー・アフィリエーションについて詳しくは、IBM Endpoint Manager サポート・サイトの記事を参照してください。

リレー・アフィリエーション・グループへのクライアントの割り当て

クライアントは、以下のクライアント設定を通じて、1 つ以上のリレー・アフィリエーション・グループに割り当てられます。

```
_BESClient_Register_Affiliation_SeekList
```

このクライアント設定には、セミコロン (;) によって区切られたリレー・アフィリエーション・グループのリストを指定します。以下に例を示します。

```
AsiaPacific;Americas;DMZ
```

アフィリエーション・グループへのリレーとサーバーの関連付け

リレーおよびサーバーは、以下のクライアント設定を通じて、1 つ以上のアフィリエーション・グループに割り当てることができます。

```
_BESRelay_Register_Affiliation_AdvertisementList
```

クライアント設定には、セミコロン (;) によって区切られたリレー・アフィリエーション・グループのリストも指定します。以下に例を示します。

```
AsiaPacific;DMZ;*
```

注: リレーおよびサーバーには、SeekList 設定は不要です。SeekList はクライアントのみが使用します。

リレーの自動割り当てに関する注意事項

IBM Endpoint Manager クライアントは、高度なアルゴリズムを使用して、ネットワーク上の最も近いリレーを判別します。このアルゴリズムでは、最適なりレーをディスカバーして割り当てるために、各種の TTL を使用する小規模な ICMP パケットが使用されます。複数の最適リレーが検出された場合、アルゴリズムにより、自動的に負荷のバランスが取られます。リレーがダウンした場合、クライアントは自動フェイルオーバーを実行します。リレーを手動で指定して最適化することに比べて、これは大きな改善点です。ただし、自動リレー選択には、以下のいくつかの重要な注意事項があります。

- クライアントとリレーの間で ICMP を送受信できる必要があります。クライアントが ICMP メッセージをリレーに送信できない場合、クライアントは最適なりレーを検出できません (この場合、クライアントは、フェイルオーバー・リレーを使用するか (フェイルオーバー・リレーが指定されている場合)、またはランダム・リレーを選択します)。
- ネットワーク・ホップ数が少なければ少ないほど、帯域幅がより大きいということにはならない場合があります。このような場合、リレーの自動選択が適切に機能しない可能性があります。例えば、データ・センター内の、クライアントと同

じ高速 LAN に配置されているリレーと、低速 WAN リンクを使用するリモート・オフィスのリレーで、後者の方がホップ数が少ない場合があります。このような場合は、手動でクライアントを該当する最適なりレーに割り当てます。

- リレーは、オペレーティング・システムがレポートする DNS 名を使用します。この名前を、すべてのクライアントが解決できるようにする必要があります。解決できない場合、クライアントはリレーを検出しません。サポート・サイトのタスクを使用することで、この DNS 名を IP アドレスまたは別の名前でオーバーライドできます。
- クライアントは、対応するリレーへの距離をレポートできます。この情報は有用であり、変更されたかどうかモニターする必要があります。例えば、コンピューターでホップ数が 1 から 5 に突然変わった場合、それらのリレーで問題が発生している可能性があります。
- リレー、自動リレー選択、およびリレーのトラブルシューティングについて詳しくは、IBM Endpoint Manager サポート・サイトを参照してください。

IBM Endpoint Manager サーバーおよびリレーの調整

IBM Endpoint Manager で最高のパフォーマンスを得るには、サーバーとリレーの調整が必要になる場合があります。ネットワーク全体にわたってデータの流れを調整する 2 つの重要な方法として、スロットリングとキャッシングがあります。

送信ダウンロード・トラフィックのスロットリング

スロットリングでは、IBM Endpoint Manager サーバーの最大データ・レートを設定することができます。データ・レートを変更する方法を以下に示します。

1. ドメイン・パネルのナビゲーション・ツリーで「**Fixlet とタスク**」アイコンを開き、「**タスクのみ**」をクリックします。
2. タスク・リストの上の検索ウィンドウで、「スロットリング」と入力して該当するタスクを検索します。
3. 結果のリストで、「**サーバー設定: 送信ダウンロード・トラフィックのスロットリング**」というラベルの付いたタスクをクリックします。その下にタスク・ウィンドウが開きます。「**説明**」タブが選択されていることを確認します。以下の 3 つの選択肢があります。
 - **送信ダウンロード・トラフィック総量の上限を設定する。**これを選択すると、サーバーに許可する 1 秒あたりの最大キロバイト数を直接設定できます。
 - **設定を無効にする。**これを選択すると、IBM Endpoint Manager サーバーでのダウンロード・トラフィックを最大限までスロットリングできます。
 - **詳細情報を入手する。**このオプションを選択すると、帯域幅スロットリングに関する詳細情報を表示するブラウザー・ウィンドウが開きます。
4. スロットリングの上限を選択した場合は、続いて表示される「**アクションの実行**」ダイアログでスロットリングの対象となる一連のコンピューターを選択できます。「**OK**」をクリックしてタスクを伝達します。

ダウンロード・キャッシュ・サイズのダウンロード

IBM Endpoint Manager サーバーおよびリレーでは、クライアントから最後に要求されたダウンロードのキャッシュを保持することで、必要となる帯域幅を最小限に抑えています。

1. ドメイン・パネルのナビゲーション・ツリーで「**Fixlet とタスク**」アイコンを開き、「**タスクのみ**」をクリックします。
2. タスク・リストの上の検索ウィンドウで、「キャッシュ」と入力して該当するタスクを検索します。
3. 結果のリストで、「**リレー/サーバー設定: ダウンロード・キャッシュ・サイズ**」というラベルの付いたタスクをクリックします。その下にタスク・ウィンドウが開きます。「**説明**」タブが選択されていることを確認します。リスト内のコンピューターのダウンロード・キャッシュ・サイズを変更するためのリンクを選択します。このリストには、IBM Endpoint Manager サーバーだけでなくリレーが含まれている場合があります。
4. キャッシュするメガバイト数を入力します。デフォルトは 1024 MB (1 ギガバイト) です。
5. 続いて表示される「**アクションの実行**」ダイアログで、一連のコンピューターを選択し、「**OK**」をクリックします。

動的な帯域幅スロットリング

大容量のダウンロードが可能になると、デプロイメント内の個々のリンクに帯域幅の固有の問題が発生する場合があります。考慮の対象となるのは、サーバーからクライアント、サーバーからリレー、およびリレーからクライアントの各リンクで、場合によってはそれぞれのリンクに個別の調整が必要となります。別のセクションで説明したように、単純にデータ・レートの最大値を設定 (スロットリング) することが可能であり、そのために、順守可能な幅広いポリシーが用意されています。例えば、IBM Endpoint Manager クライアントでリレーからのホップ数が 3 を超えている場合は、クライアントを 2 KB/秒にスロットリングすることが考えられます。ただし、最適なデータ転送速度は、現在の階層およびネットワーク環境に応じて、大幅に変わる可能性があります。

より適切な手法は、ネットワーク容量全体を監視して分析する動的な帯域幅スロットリングを使用することです。標準的なスロットリングでは最大データ・レートを指定するだけですが、動的なスロットリングでは「**ビジー時間**」の比率が加わります。これは、ネットワークがビジーのときに割り振る帯域幅の一部です。例えば、ネットワーク・トラフィックの存在が検出された場合に、ダウンロードに使用される帯域幅を使用可能な帯域幅の 10% 以下に抑えるように指定できます。動的なスロットリングでは、ビジー率が低すぎて実際的でない場合のために、最小データ・レートも指定します。

任意のリンクに対して動的スロットリングを有効にすると、現在のデータ・スループットが監視され、分析されて、適切なデータ・レートが設定されます。競合するトラフィックが存在しない場合は、スループットが最大レートに設定されます。トラフィックが存在する場合は、指定したパーセンテージまたは最小レートのどちら

か高い方までデータ・レートがスロットリングされます。動的スロットリングを正しく機能させるには、サーバー側とクライアント側の両方で動的スロットリングを有効にする必要があります。

動的な帯域幅スロットリングは、コンピューター設定で制御します。リンクごとに、以下の 4 つの基本的な設定があります。

DynamicThrottleEnabled

この設定のデフォルトはゼロ (無効) です。その他の任意の値の場合、指定されたリンクの動的スロットリングが有効になります。

DynamicThrottleMax

この設定は、通常、デフォルトでは最大の符号なし整数値になります。これはフルスロットルを示します。リンクによっては、この値に、最大データ転送速度 (1 秒あたりのビット数または K ビット数) が設定されます。

DynamicThrottleMin

この設定のデフォルトはゼロです。リンクに応じて、この値に、最小データ転送速度 (1 秒あたりのビット数または K ビット数) が設定されます。この値は、以下に示すパーセンテージ・レートの下限を設定します。

DynamicThrottlePercentage

この設定は、デフォルトでは 100% です。100% は、通常の (動的ではない) スロットリングと同じ効果があります。これは、最大帯域幅のうち、ネットワークがビジーであるときに使用する部分の割合です。通常は、5% から 10% の値が使用され、既存のネットワーク・トラフィックよりも優先されることがないようにします。(この設定にゼロを使用すると、100% と同じことになります。).

動的帯域幅設定は、他の設定と同じように作成または編集することができます。つまり、任意のコンピューター・リストで項目 (または項目のグループ) を右クリックし、コンテキスト・メニューから「**コンピューターの設定を編集**」を選択します。

具体的な変数名には以下のものがあります。

IBM Endpoint Manager サーバーおよびリレーの設定:

```
_BESRelay_HTTPServer_DynamicThrottleEnabled  
_BESRelay_HTTPServer_DynamicThrottleMaxKBPS  
_BESRelay_HTTPServer_DynamicThrottleMinKBPS  
_BESRelay_HTTPServer_DynamicThrottlePercentage
```

IBM Endpoint Manager クライアントの設定:

```
_BESClient_Download_DynamicThrottleEnabled  
_BESClient_Download_DynamicThrottleMaxBytesPerSecond  
_BESClient_Download_DynamicThrottleMinBytesPerSecond  
_BESClient_Download_DynamicThrottlePercentage
```

一括設定:

```
_BESGather_Download_DynamicThrottleEnabled  
_BESGather_Download_DynamicThrottleMaxBytesPerSecond  
_BESGather_Download_DynamicThrottleMinBytesPerSecond  
_BESGather_Download_DynamicThrottlePercentage
```

注: 上記の設定を有効にするには、影響を受けるサービス (サーバー、リレー、またはクライアント) を再起動する必要があります。

サーバーとその接続先であるクライアントに異なる最大値または最小値を設定した場合、その接続では小さい方の値が選択されます。

サーバーに到達できない場合のリレーの割り当て

クライアントをインストールすると、それはメインの Endpoint Manager サーバーに接続され、登録されます。

クライアントがメイン・サーバーに登録されると、マスター・オペレーターはクライアントをプライマリー・リレーに割り当てることができます。さらに、プライマリー・リレーが使用できなくなった場合にセカンダリー・リレーにフェイルオーバーするように構成できます。

場合によっては、クライアントがインストールされるときに、ローカル・エリア・ネットワークまたはインターネットを介してメイン・サーバーに直接到達できないことがあります。例えば、クライアント・ワークステーションがリモート・オフィスにあり、企業のファイアウォールを通過してメイン・サーバーに到達する接続を構築できない場合があります。この場合、ファイアウォール内のホールを通してアクセスできる DMZ リレーを設定する必要があります。詳しくは、『インターネット・リレーの設定』を参照してください。

また、インストール中に、構成ファイルを使用してリモート・オフィスのクライアント・インストーラーを適用し、クライアントのプライマリー・リレーを設定する必要もあります。プライマリー・リレーを構成ファイルに指定し、クライアントを接続できるリレー (DMZ リレーなど) に登録します。詳しくは、『クライアント・インストール時のリレーの割り当て』を参照してください。

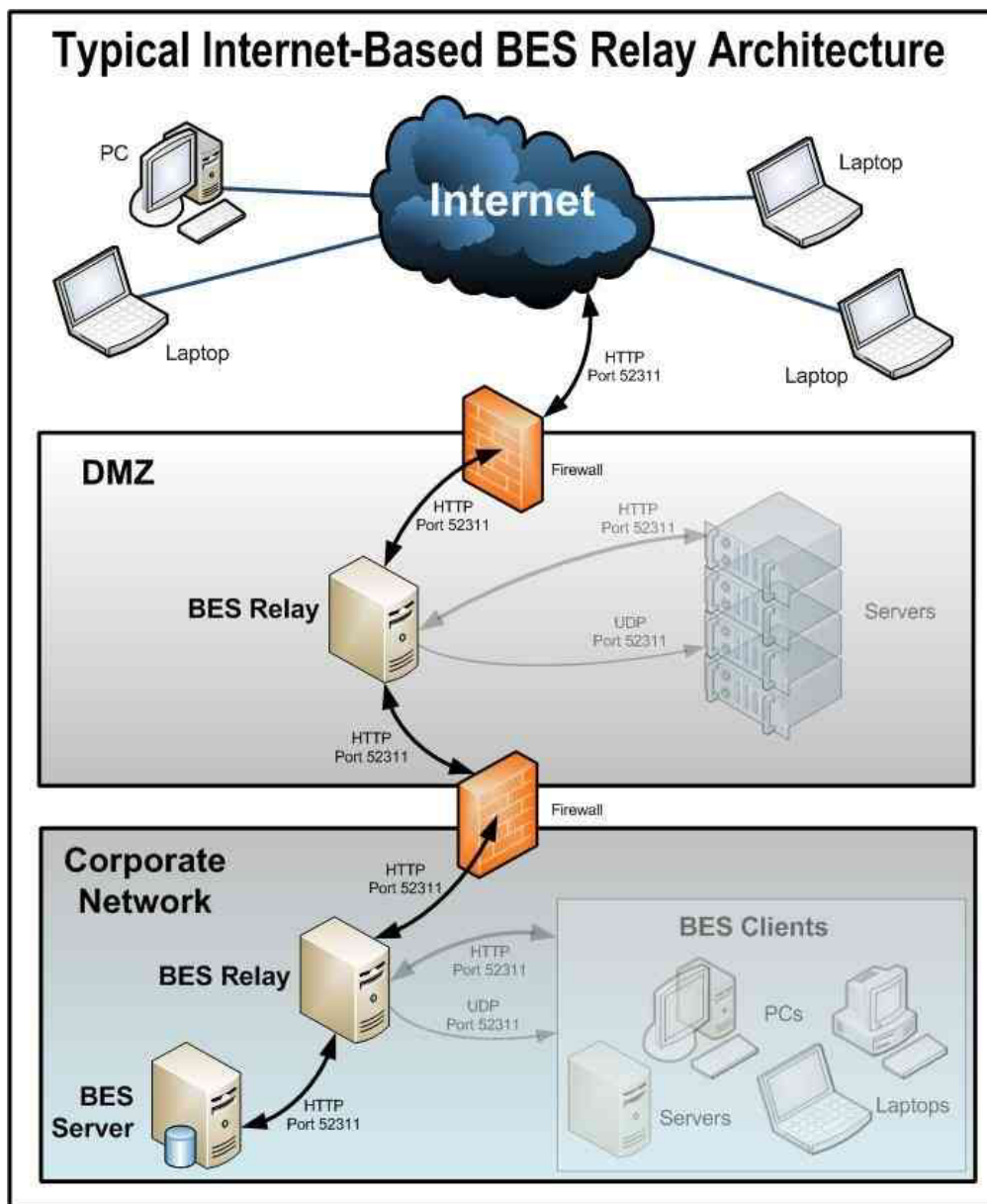
インターネット・リレーの設定

リレーを構成して、VPN を使用せずにインターネットにのみ接続しているクライアントを、企業ネットワーク内にあるかのように管理できます。

この方法により、企業ネットワークの外部 (自宅、空港、コーヒー・ショップなど) に存在するコンピューターを Endpoint Manager を使用して管理し、以下を処理を行うことができます。

- 更新されたプロパティと Fixlet ステータスをレポートする。
- コンソール・オペレーターによって定義された新しいセキュリティ・ポリシーを適用する。
- 新しいパッチまたはアプリケーションの適用環境を受け入れる。

この構成は、企業ネットワークから切断されることが多いモバイル・デバイスを管理する場合に特に便利です。以下の図は、DMZ ネットワークに存在する可能性のある、一般的なインターネット・ベースのリレーを示しています。



インターネットに接続されたリレーを設定することで、外部クライアントはリレーを検出して接続できるようになります。この図では、クライアントは以下のタイプのリレーを選択できます。

- **手動でのリレー選択:** コンソールを使用して、インターネットに接続されたリレーの DNS 別名 (または IP アドレス) をプライマリー、セカンダリー、またはフェイルオーバーのリレーとして手動で選択することで、クライアントを構成できます。フェイルオーバー・リレーの設定について詳しくは、『*Configuration Settings*』を参照してください。
- **自動リレー選択:** ICMP トラフィックでインターネットから DMZ ベースのインターネットのリレーを行うことができる場合、自動リレー選択を利用して、(企業ネットワーク内かインターネット上のいずれかで) クライアントが場所を移動する間に最も近いリレーを検出できるようになります。インターネット上の外部ク

クライアントの場合、インターネットに接続されたリレーのみ、検出して接続することができます (インターネットから企業ネットワーク内のリレーへの ICMP トラフィックはブロックされるため)。

注: リレー・アフィリエーション機能を使用して、最も適切なリレーを検出するようにクライアントを構成できます。詳細については、『リレー・アフィリエーション』を参照してください。

次に、一般的なインターネット・ベースの Endpoint Manager リレー・アーキテクチャーで、リレー、クライアント、およびファイアウォールがどのように構成されているかを説明します。

1. リレーは DMZ に適用され、内部 DMZ ファイアウォールによって、企業ネットワーク内の DMZ リレーと指定されたリレー間の Endpoint Manager トラフィック (HTTP ポート 52311) のみが許可されます。この設計は双方向トラフィックを示唆しており、内部企業ネットワーク内のリレーへのネットワーク接続を開始するために、インターネットに接続されたリレーのみを許可する設計とは対照的です。これにより、インターネットに接続されたリレーに対して新しいコンテンツを即時に通知し、コンテンツのリアルタイム同期を維持できるため、クライアントの応答時間を短縮することができます。インターネットに接続された Endpoint Manager リレーと、企業ネットワークのリレーの間に双方向通信を確立できない場合、インターネットに接続されたリレーを、新しいコンテンツを取得するためにその親 (企業ネットワーク内のリレー) を定期的にポーリングするように設定する必要がありますコマンド・ポーリングの構成について詳しくは、『Configuration Settings』を参照してください。
2. DMZ と内部企業ネットワーク間にリレー通信が構築されたら、外部ファイアウォールも開いて、インターネット・ベースのクライアント・トラフィック (HTTP ポート 52311) が DMZ リレーに到達できるようにする必要があります。また、ICMP トラフィックが外部ファイアウォールを通してインターネットに接続されたリレーに到達できるようにすることで、外部クライアントが自動リレー選択プロセスを実行できるようになります。
3. 外部クライアントが DMZ ベースのインターネット・リレーを検出できるようにするために、リレーに DNS 別名 (または IP アドレス) が割り当てられます。この DNS 別名は、特定の IP アドレスに解決する必要があります。
4. リレーに DNS 別名 (または IP アドレス) を認識させるには、「BES Relay Setting: Name Override」Fixlet を DMZ ベースのインターネット・リレーに適用します。
5. インターネットから DMZ ベースのインターネット・リレーを介して、最終的にはメイン・サーバーに到達するように構築されたすべての Endpoint Manager 通信パスを使用する次の手順は、所定の Endpoint Manager インフラストラクチャーで利用できるさまざまなリレー選択方法に応じて異なります。
6. 動的ポリシー設定をインターネット・ベースのクライアントに適用して、外部エージェントにより適した構成を行うことができます。例えば、新しいコンテンツについての通常の方法 (ポート 52311 での UDP ping) では外部のクライアントにアクセスできない可能性があるため、動的設定を使用して、デフォルトの 24 時間よりも短い間隔で、クライアントに新しいコンテンツをチェックさせる

ことができます。コマンド・ポーリングのセットアップについて詳しくは、
<http://www-01.ibm.com/support/docview.wss?uid=swg21505846> を参照してください。

注: クライアント設定 `_BESRelay_Diagnostics_Enable` をゼロに設定することで、インターネット・リレーのリレー診断 (<http://relayname:port/rd>) を無効にします。

クライアント認証

クライアント認証 (バージョン 9 で導入) は、IBM Endpoint Manager で使用されるセキュリティ・モデルを拡張して、信頼できるクライアント・レポートおよびプライベート・メッセージを実現します。この機能には後方互換性がなく、バージョン 9.0 より前のクライアントは、認証を行うリレーまたはサーバーとは通信できません。

オリジナルのセキュリティ・モデルには、以下の 2 つの中心となる機能があります。

- **クライアントはサーバーからのコンテンツを信頼する。** クライアントが受信するすべてのコマンドと質問は、クライアント上にインストールされたパブリック・キーに対して検証されるキーによって署名されます。
- **クライアントはサーバーに対してプライベート・レポートを送信できる。** クライアントはサーバーに送信するレポートの暗号化を選択でき、レポートに含まれた内容を攻撃者が解釈できないようにすることができます。この機能はデフォルトでは無効になっており、設定を使用してオンに切り替えます。

クライアント認証では、セキュリティ・モデルを拡張して、以上の 2 つの機能の次のようなミラー・イメージを提供します。

- **サーバーはクライアントからのレポートを信頼できる (否認防止)。** クライアントはサーバーに送信するレポートをすべて署名します。これにより、レポートが攻撃者からのものでないことを検証できます。
- **サーバーはクライアントにプライベート・データを送信できる (メールボックス)。** サーバーは、攻撃者がデータを解釈できないようにするために、個々のクライアントに送信するデータを暗号化することができます。

認証済みリレーを使用する通信は、SSL を使用してすべての通信を暗号化する、信頼できるプライベートな両方向の通信チャネルです。ただし、非認証リレーとその子間の通信は、その通信が暗号化されたレポートまたはメールボックス宛のアクションやファイルでないかぎり、暗号化されません。

このレベルのセキュリティは、さまざまな目的に役立ちます。企業において、インターネットに接続するノード、DMZ 内、または完全に信頼できないすべてのネットワーク接続に、認証を行うリレーを要求するセキュリティ・ポリシーを採用している場合があります。認証を行うことにより、まだご使用のデプロイメントに参加していないクライアントがデプロイメント情報を取得するのを防ぐことができます。

認証リレー

リレーは、エージェントを認証するための認証リレーとして構成することができます。この方法により、信頼されたエージェントだけが、サイトのコンテンツの収集やレポートの投稿を行うことができます。DMZ 内でインターネットに接続されたリレーに対して、認証リレーの構成を使用します。

エージェントの認証用に構成されたリレーは、サーバーによって発行および署名された SSL 証明書を鍵交換の実行中に提示する子エージェントまたはリレーとのみ、SSL 通信を実行します。

認証リレーを構成するには、クライアント設定の `_BESRelay_Comm_Authenticating` を 1 に設定するか、BES サポート・サイトの関連タスクを使用します。オープン・リレーをもう一度構成するには、`_BESRelay_Comm_Authenticating` を 0 に設定するか、BES サポート・サイトの関連タスクを使用します。デフォルト値は (0) です (オープン・リレー)。

鍵交換の処理

登録を試みたエージェントが鍵と証明書を持っていない場合、そのエージェントは、選択したリレーとの鍵交換を自動的に実行しようとします。そのリレーが非認証リレーである場合、エージェントはリレー・チェーンをたどってサーバーに要求を転送し、サーバーがエージェントの証明書に署名します。エージェントは、後で認証リレーへの接続時にこの証明書を使用できます。

認証リレーでは、このような鍵交換の自動操作は拒否されます。一般的なシナリオを以下に示します。

新規の Endpoint Manager 9.1 環境を適用した場合や、既存の Endpoint Manager 環境を 9.0 にアップグレードした場合、すべてのエージェントは、リレーとの鍵交換を自動的に実行します。管理者が、インターネットに接しているリレーを認証リレーとして構成している場合、既存のエージェントはすでに証明書を保有しており、正しく稼働します。これ以上のアクションは不要です。新規のエージェントを認証リレーに接続した場合、そのエージェントに対して手動の鍵交換手順を実行しない限り、そのエージェントは稼働しません。

手動での鍵交換

エージェントが証明書を保有しておらず、インターネットを介して接続されたネットワーク上の認証リレーにのみ到達できる場合、そのエージェントに対して以下のコマンドを手動で実行すれば、エージェントは認証リレーとの鍵交換を実行できるようになります。

```
BESClient -register <password> [http://<relay>:52311]
```

クライアントは認証リレーとの鍵交換にパスワードを含めます。これにより、鍵交換をその親に転送する前にクライアントが検証されます。

パスワードは、以下のように構成できます。

- リレーに対するクライアント設定 `_BESRelay_Comm_KeyExchangePassword` の単一パスワードとして。

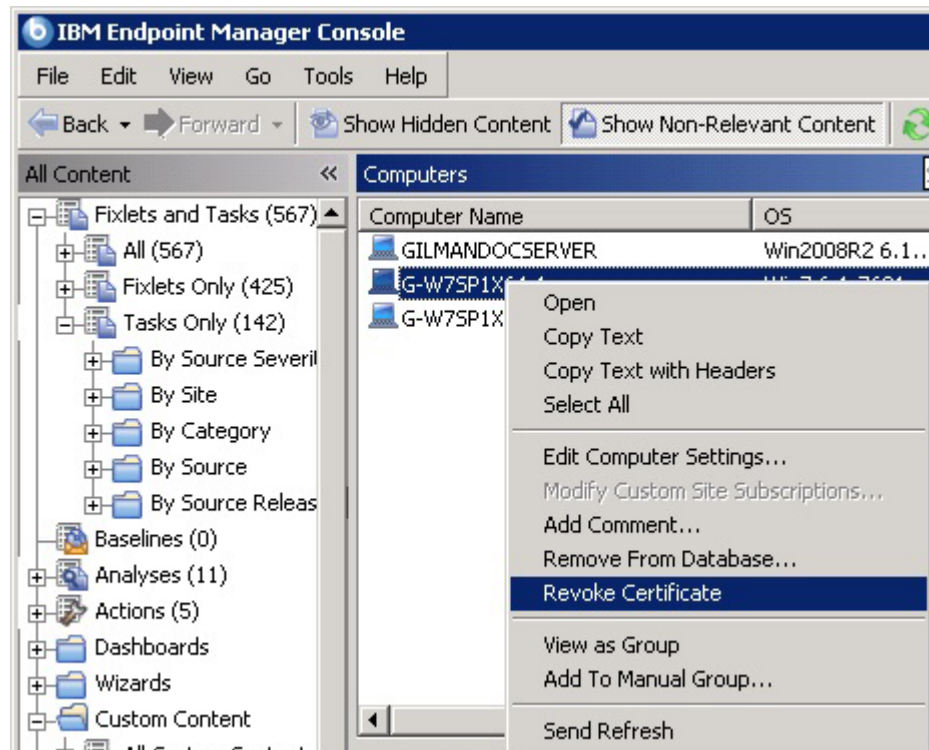
- リレー・ストレージ・ディレクトリー (HKLM¥SOFTWARE¥BigFix¥Enterprise Server¥GlobalOptions の値 **StoragePath**) 内の KeyExchangePasswords という名前のファイルに保管されるワнтаイム・パスワードの改行区切りリストとして。

クライアント証明書の取り消し

クライアントの認証後に、クライアントの有効性を疑う何らかの理由がある場合は、クライアントの証明書を取り消すことができます。証明書を取り消すと、そのクライアントは信頼できる通信に対して認証されなくなります。クライアントはコンソールから削除され、取り消しリストが更新されてすべてのリレーにより収集されることにより、そのクライアントの鍵は認証リレーとの通信には使用できなくなります。

コンピューターを取り消すには次のようにします。

1. コンピューターのリストで、コンピューターを右クリックします。



2. ポップアップ・メニューで、「証明書を失効する」をクリックします。
3. コンピューターの証明書を削除して問題がなければ、確認ダイアログで「OK」をクリックします。

これにより、取り消しがリレーへと通知されます。いったん取り消されると、そのクライアントは自身の秘密鍵を使用して認証リレーからコンテンツを収集することはできなくなります。取り消されたクライアントは、コンソールのコンピューター・リストに表示されなくなります。

取り消されたクライアントの再登録

ある証明書が取り消されると、暗号漏えいした鍵は破棄されます。ただし、クライアントは 2 つの方法でネットワークに再加入することができます。

- 認証環境では、クライアントが認証リレーのみにアクセス可能な場合、自動の鍵交換が事前に実行されていなければ、クライアントは手動の交換方法を使用する必要があります。
- オープン (非認証) 環境では、クライアントは非認証リレーに自身を再登録することができます。

いずれのケースでも、コンピューターは新しい証明書と新規コンピューター ID を取得します。

重要: 認証環境では、クライアントが非認証リレーまたはサーバーにアクセス可能な場合、クライアントは、明示的に取り消されていても、自動的に鍵を交換して再登録できます。

メール・ボックス

クライアント・メールボックスを使用すると、暗号化されたアクションを、すべてのクライアントにブロードキャストする代わりに特定のクライアントに送信できます。これにより、クライアントはすべてのアクションに対して資格を持つ必要がなくなるため効率性が向上し、ネットワーク・トラフィックが最小化されます。その結果、以下ようになります。

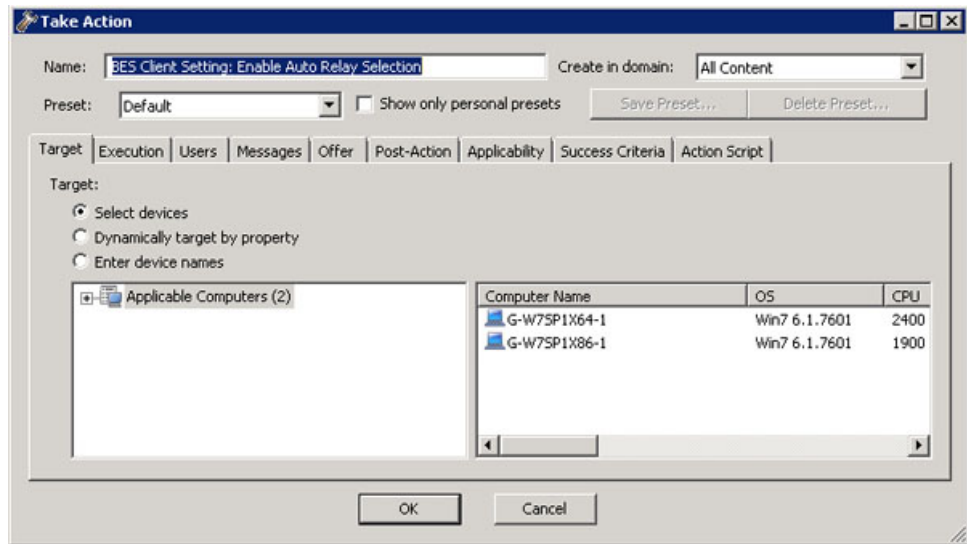
- クライアントは、ターゲットとなった場合にのみ中断される。
- クライアントは、自身に関連しないアクションについて、レポート、評価、収集、およびアクション処理を実行する必要がなくなる。

メッセージは受信者ごとに特別に暗号化されるためプライバシーが保証されます。ターゲット・クライアントのみがそのメッセージを復号できます。

クライアントのメールボックスは特別なアクション・サイトとして実装され、各クライアントは自動的にそのサイトをサブスクライブします。クライアントは、このサイトに加えてマスター・サイトおよびオペレーター・サイトでアクションをスキャンすることを知っています。

暗号化されたアクションをクライアント・メールボックスに直接送信するには、以下の手順を実行します。

1. 「**アクションの実行**」 ダイアログを開きます (「ツール」メニューやその他のダイアログで使用可能)。



2. 「ターゲット」タブをクリックします。
3. 「デバイスの選択」または「デバイス名の入力」をクリックします。クライアントの静的なリストを指定した場合にのみ、メールボックスが使用可能になります。動的にターゲットとなったコンピューターは暗号化されず、代わりにオープンな状態でマスター・サイトまたは特定のオペレーター・サイトに送信されます。バージョン 9.0 より前のクライアントをターゲットにした場合も、アクションはマスター・サイトまたはオペレーター・サイトに送信されます。
4. 「OK」をクリックします。コンピュータ ID またはコンピューター名によりターゲット設定されたアクションが、暗号化されてクライアント・メールボックスに送信されます。

アクションをデプロイするオペレーターの ID がアクションとともに含まれています。アクションを実行する前に、クライアントはまず現在そのオペレーターにより管理されているかどうかを判別します。そうでない場合、クライアントはアクションの実行を拒否します。

クライアントに割り当てられているリレーの表示

どのクライアントがどのリレーを選択しているか確認するには、以下の手順を実行します。

1. コンソールを起動し、「BigFix 管理」ドメインを選択します。
2. 「コンピュータ管理」フォルダーで「コンピュータ」をクリックして、クライアントのリストを表示します。
3. リスト・パネルで「リレー」列を確認します（この列は非表示になっている場合があります。その場合は、列ヘッダーを右クリックし、「リレー」にチェック・マークが付いているかどうか確認します）。IBM Endpoint Manager リレーの列には、リレー方式、サービス、コンピューターなどの情報が表示されます。

デフォルトでは、クライアントは、6 時間ごとに（最小のネットワーク・ホップ数に基づいて）最も近いリレーの検出を試行します。リレーについて詳しくは、IBM Endpoint Manager サポート・サイトを参照してください。

リレーの適用状態のモニタリング

IBM Endpoint Manager では、クライアントおよびリレーのセットアップをモニターして、それらが最適に機能していることを確認できます。大容量のパッチを適用する前には、スムーズに適用できるように、リレーのステータスを確認することをお勧めします。

以下に、リレーの適用をモニタリングするための提案事項を示します。

- 「**BigFix 管理**」ドメインおよび「**分析**」ノードをクリックし、リレーのステータス分析をアクティブにします。この分析には、リレーの適用状態を詳細に示す多数のプロパティが含まれます。
- 分析の「**結果**」タブをクリックして、リレーのステータス分析で「リレーへの距離」プロパティをモニターし、ネットワーク内でどのリレーが正常であるかを確認します。トポロジが突然変更された場合、または一部のクライアントが余分なホップを使用してサーバーに到達している場合、リレーで障害が発生している可能性があります。
- クライアントがサーバーに直接レポートすることは、リレーを使用するよりも通常は非効率であるため、サーバーに直接レポートするクライアントの数を最小限にします。分析を調べることで、どのコンピューターがどのリレーにレポートしているかを確認できます。

第 12 章 プロキシ接続のセットアップ

企業がプロキシを使用してインターネットにアクセスする場合は、プロキシ接続を設定して、IBM Endpoint Manager サーバーがサイトからコンテンツを収集できるようにする必要があります。

プロキシ接続は、IBM Endpoint Manager サーバーまたはリレーがコンポーネント間通信やファイルのダウンロードを行う際にも使用されます。

以下の構成は最も一般的なプロキシ構成であり、セットアップが必要となる可能性があります。

IBM Endpoint Manager サーバーがプロキシ経由でインターネットに接続して、コンテンツを収集する必要がある。

サーバー上で実行されるこの構成を設定するには、163 ページの『プロキシ接続の サーバー上での設定』で説明する手順を実行します。Windows システムでは、プロキシ経由の通信が機能していない場合はデバッグ・ツールによって通知されます。

重要: このステップをスキップすると、ご使用の環境が正しく動作しない可能性があります。この正しくない動作の症状としては、サイトのコンテンツがコンソールに表示されない状態が挙げられます。

リレーがプロキシ経由でインターネットに接続して、ファイルのダウンロードや親リレーとの通信を行う必要がある。

リレー上で実行されるこの構成を設定するには、165 ページの『リレーでのプロキシ接続のセットアップ』で説明する手順を実行します。

クライアントがプロキシ経由でインターネットに接続して親リレーと通信する必要がある。

この構成を設定するには、以下の手順を実行します。

- 165 ページの『リレーでのプロキシ接続のセットアップ』で説明する手順をリレーで実行します。
- 166 ページの『クライアントまたは子リレーでのプロキシ接続の設定』で説明する手順をクライアントで実行します。

リレーがプロキシ経由でインターネットに接続して子リレーと通信する必要がある。 この構成を設定するには、以下の手順を実行します。

- 165 ページの『リレーでのプロキシ接続のセットアップ』で説明する手順を親リレーで実行します。
- 166 ページの『クライアントまたは子リレーでのプロキシ接続の設定』で説明する手順を子リレーで実行します。

IBM Endpoint Manager 環境の構成に使用できる設定については、IBM Endpoint Manager サポート・サイトにある知識ベースの『configure the server』を参照してください。

注: エアー・ギャップ実装を使用して、インターネットからの物理的な切断を維持することもできます。この実装の詳細については、エアー・ギャップ環境でのファイルのダウンロードを参照してください。

プロキシ経由での通信を構成するための実行手順は、IBM Endpoint Manager バージョン 9.1 で初めて構成をセットアップするか、旧バージョンでセットアップしたかによって異なります。

以下の表は、各コンポーネントについて、プロキシ構成をセットアップするための実行手順を示します。

表 9. : IBM Endpoint Manager バージョン 9.1 サーバーにおけるプロキシ経由での通信の構成手順

サーバー (Server)	
Linux	Windows
besserver.config ファイル・セットで、以下のキーを追加します。 Proxy ProxyUser ProxyPass ProxyExceptionList 詳細については、163 ページの『プロキシ接続の サーバー上での設定』を参照してください。	163 ページの『プロキシ接続の サーバー上での設定』の説明に従って、BESAdmin コマンドを実行します。
または	
連結キーを設定します。 Proxy = [<proxy_user>:<proxy_password>@<proxy_hostname>[:<proxy_port>] これについては、163 ページの『プロキシ接続の サーバー上での設定』を参照してください。	

表 10. : IBM Endpoint Manager バージョン 9.1 リレーにおけるプロキシ経由での通信の構成手順

リレー	
Linux および Windows	
親コンポーネント (リレーまたはサーバー) と通信するための手順:	インターネットからファイルをダウンロードするための手順:
166 ページの『クライアントまたは子リレーでのプロキシ接続の設定』に記載されているクライアント接続設定を行います。 必要に応じてプロキシ例外リストを使用して、プロキシを使用せずにアクセスする必要があるローカル・コンピューターまたはドメインを指定します。	以下のように設定します。 _BESGather_Download_CheckInternetFlag = 1 _BESGather_Download_CheckParentFlag = 0 これについては、165 ページの『リレーでのプロキシ接続のセットアップ』を参照してください。

表 11. : IBM Endpoint Manager バージョン 9.1 クライアントにおけるプロキシ経由での通信の構成手順

クライアント
Linux および Windows
『h』に記載されているクライアント接続を設定します。 必要に応じてプロキシ例外リストを使用して、プロキシを使用せずにアクセスする必要があるローカル・コンピューターまたはドメインを指定します。

注: IBM Endpoint Manager バージョン 9.1 で使用される構成設定では、BESGatherService は非推奨のため、使用されません。

既存の構成をバージョン 9.1 にアップグレードする場合は、プロキシ経由で通信するための構成が異なる可能性があります。例えば、バージョン 8.2 では、バージョン 9.X で非推奨の BESGatherService を使用してプロキシ経由での通信が構成されました。IBM Endpoint Manager バージョン 8.2 環境をバージョン 9.1 にアップグレードする場合は、後方互換性を保つために、プロキシ構成では引き続き BESGatherService を使用します。ただしこの場合は、バージョン 9.1 でサポートされるプロキシ構成を使用するまで、ProxyExceptionList などの新機能は使用できません。

プロキシ接続の サーバー上での設定

IBM Endpoint Manager バージョン 9.1 サーバーでは、サーバーがインストールされたプラットフォームによって、動作が以下のように異なります。

Windows システムの場合:

インターネットにアクセスする BES コンポーネントは、デフォルトでは、Windows サーバーの SYSTEM アカウントとして実行されます。

プロキシ構成は、レジストリー内でキー

HKEY_LOCAL_MACHINE¥SOFTWARE¥BigFix¥Enterprise Server¥Proxy によって管理されます。

以下のコマンドを実行して、レジストリーで

HKEY_LOCAL_MACHINE¥SOFTWARE¥BigFix¥Enterprise Server¥Proxy キーを作成または変更します。

```
BESAdmin /setproxy /proxy:<proxy_host> /user:<proxy_username>
/pass:<proxy_password> [/exceptionlist:<proxy_exceptionlist>]
```

Linux システムの場合:

インターネットにアクセスする BES コンポーネントは、デフォルトでは、Linux サーバーの root として実行されます。

プロキシ構成は、besserver.config ファイルの

[SOFTWARE¥BigFix¥Enterprise Server¥Proxy] セクションで、以下のキーを使用して定義します。

```
Proxy = <proxy_host>
ProxyUser = <proxy_username>
ProxyPass = <proxy_password>
ProxyExceptionList = <proxy_exceptionlist>
```

プロキシ経由での通信を構成するときに指定する値は、以下のとおりです。

proxy_host

プロキシ・マシンのホスト名または IP アドレスです。また、オプションでプロキシ・マシンのポート番号を指定します。この値は、以下の形式で指定してください。

`{hostname|IP_address}[:port]`

proxy_username

プロキシが認証を必要とする場合にプロキシでの認証に使用するユーザー名です。

IBM Endpoint Manager サーバーが Windows システムにインストールされていて、プロキシで Kerberos 認証が必要な場合は、`user@mydomain.com` という形式で指定してください。

IBM Endpoint Manager サーバーが Windows システムにインストールされていて、プロキシで NTLM 認証が必要な場合は、NTLM ユーザーを指定してください。

プロキシでドメインまたはレルムが必要な場合は、ユーザーを `user@mydomain.com` または `mydomain/user` として指定しなければならないことがあります。

注: Windows の場合、指定されたユーザーは、サーバーにログインし、プロキシを使用するようにインターネット・オプションを構成する必要があります。

IBM Endpoint Manager サーバーが Linux システムにインストールされていて、プロキシで NTLM 認証が必要な場合は、NTLM ユーザーを指定してください。Linux 上の IBM Endpoint Manager では、FIPS が有効になっている場合、NTLM 認証は機能しません。

proxy_password

プロキシが認証を必要とする場合にプロキシでの認証に使用するパスワードです。パスワードに割り当てられた値は、Windows システムの場合はレジストリー内で暗号化され、Linux システムの場合は構成ファイル内で難読化されます。

proxy_exceptionlist

これはオプション設定であり、この設定を使用すると、プロキシを経由せずにアクセスする必要があるコンピューター、ドメイン、サブネットワークを指定できます。この値は、以下の形式で指定してください。

`"hostname1, hostname2, IP_Addr_A, IP_Addr_B, domain_Z, domain_Y, ..."`

このリストにあるそれぞれの名前が、ドメイン (ホスト名を含みます) またはホスト名自体と比較されます。例えば `mydomain.com` は、`mydomain.com`、`mydomain.com:80`、`www.mydomain.com` などに一致しますが、`www.notmydomain.com` には一致しません。

<proxy_exceptionlist> に割り当てることができる値の例を以下に示します。

`example.com`
`example.com,8.168.117.0`
`"example.com, 8.168.117.0"`

内部通信がプロキシ・エージェントに向かうのを防ぐために、`<proxy_exceptionlist>` を指定する場合は `localhost`, `127.0.0.1` を追加してください。

プロキシ例外リストは、Windows システム版と Linux システム版のバージョン 9.0.835.0 (パッチ 5) で導入されました。IBM Endpoint Manager バージョン 9.0 を使用していて、ローカル・サーバーからファイルをダウンロードするコンテンツの使用に問題がある場合は、IBM Endpoint Manager バージョン 9.0.835.0 にアップグレードしてください。

IBM Endpoint Manager バージョン 8.1、8.2、および 9.0 でビルドが 9.0.835.0 よりも前の場合、プロキシの設定は Internet Explorer のプロキシ設定から取得されます。

重要: プロキシ経由で通信するように設定を作成または変更した後で、サーバー上の BESRootServer コンポーネントを必ず再起動してください。

例:

1. この例では、連結キー表記を使用して、プロキシ設定を指定します。

```
[Software¥BigFix¥Enterprise Server¥Proxy]
Proxy = [proxyuser:password@]{hostname|IP_address}[:port]
```

2. この例では、非認証プロキシ経由での通信を定義します。

```
[Software¥BigFix¥Enterprise Server¥Proxy]
Proxy = hostname:port
```

3. この例では、プロキシ経由の通信から除外する方法を示します。

- IBM Endpoint Manager クライアントは、プロキシ接続を定義するシステムにインストールされています。
- ホストの IP アドレスは **8.168.117.0** です。
- ホストはドメイン **example.com** に属します。

```
[Software¥BigFix¥Enterprise Server¥Proxy]
Proxy = username:password@hostname
ProxyExceptionList = "localhost, 127.0.0.1, 8.168.117.0, example.com"
```

プロキシ構成に関する追加情報については、『Proxy Server Settings』を参照してください。

リレーでのプロキシ接続のセットアップ

リレーがインストールされているシステムで、以下の手順を実行して、リレーがその親コンポーネントと通信できるようにします。

1. コンソールを開き、「すべてのコンテンツ」ドメインの下の「コンピューター」セクションに移動します。
2. リレーがインストールされているコンピューターを選択します。
3. コンピューターを右クリックして、「設定の編集」を選択します。
4. 「追加」を選択して、カスタム設定を作成します。
5. 166 ページの表 12 にリストされている「設定名」と「設定値」を入力します。
6. 「OK」をクリックして構成設定を送信すると、すぐに有効になります。

プロキシを経由することなくリレーが親リレーと通信する必要がある場合は、プロキシ例外リストの設定を指定します。リレーがインストールされているプラットフォームに応じて、以下のプロキシ例外リストの設定を追加してください。

Windows システムの場合:

レジストリーの HKEY_LOCAL_MACHINE¥SOFTWARE¥BigFix¥Enterprise Server¥Proxy キー。

Linux システムの場合:

besrelay.config ファイルの [SOFTWARE¥BigFix¥Enterprise Server¥Proxy] セクション。

プロキシ例外リストの指定で使用する構文については、163 ページの『プロキシ接続の サーバー上での設定』を参照してください。

リレーがプロキシ経由でファイルをダウンロードできるようにするには、以下の手順を実行します。

1. コンソールを開き、「すべてのコンテンツ」ドメインの下の「コンピューター」セクションに移動します。
2. リレーがインストールされているコンピューターを選択します。
3. コンピューターを右クリックして、「設定の編集」を選択します。
4. 「追加」を選択して、以下のカスタム設定を作成します。

```
_BESGather_Download_CheckInternetFlag = 1  
_BESGather_Download_CheckParentFlag = 0
```

5. 「OK」をクリックして構成設定を送信すると、すぐに有効になります。

注: リレーが Linux プラットフォームにインストールされている場合、設定が保存される構成ファイルは besrelay.config と呼ばれます。

クライアントまたは子リレーでのプロキシ接続の設定

クライアントまたはリレーがインターネット要求やコンポーネント間通信のためにプロキシ経由で親コンポーネント (リレーまたはサーバー) と通信しなければならない場合は、そのシステムで以下のようにプロキシ接続を設定します。

1. コンソールを開き、「すべてのコンテンツ」ドメインの下の「コンピューター」セクションに移動します。
2. クライアントまたは子リレーがインストールされているコンピューターを選択します。
3. コンピューターを右クリックして、「設定の編集」を選択します。
4. 「追加」を選択して、カスタム設定を作成します。
5. 下の構成テーブルに基づいて「設定名」と「設定値」を入力します。

表 12. プロキシ・クライアント構成の設定

設定名	設定値	詳細
_Enterprise Server _ClientRegister _ProxyServer	プロキシに到達するために使用されるホスト名を設定します。	デフォルト値: なし 設定の型: 文字列 値の範囲: 該当なし 使用可能なタスク: なし

表 12. プロキシ・クライアント構成の設定 (続き)

設定名	設定値	詳細
_Enterprise Server _ClientRegister _ProxyPort	プロキシ・サーバーによって使用されるポートを設定します。	デフォルト値: なし 設定の型: 文字列 値の範囲: 該当なし 使用可能なタスク: なし
_Enterprise Server _ClientRegister _ProxyUser	プロキシが認証を必要とする場合に、プロキシで認証するために使用するユーザー名を設定します。	デフォルト値: なし 設定の型: 文字列 値の範囲: 該当なし 使用可能なタスク: なし
_Enterprise Server _ClientRegister _ProxyPass	プロキシが認証を必要とする場合に、プロキシで認証するために使用するパスワードを設定します。	デフォルト値: なし 設定の型: 文字列 値の範囲: 該当なし 使用可能なタスク: なし

6. 「OK」をクリックして設定をアクティブにします。

コンピューターにインストールされているプラットフォームに応じて、以下の設定が保存されます。

Windows システムの場合:

レジストリー内。

Linux システムの場合:

besclient.config ファイル内 (クライアントを構成した場合)、または
besrelay.config ファイル内 (予リレーを構成した場合)。

クライアントのすべての通知には UDP プロトコルが使用されますが、このプロトコルは標準プロキシでは転送されません。クライアントとリレーの間にプロキシがある場合は、以下の設定を使用して、クライアントにアップストリーム通信を構成します。

表 13. プロキシ・クライアントのポーリング構成の設定

設定名	設定値	詳細
_BESClient_Comm _CommandPollEnable	クライアントが新規アクションについて親リレーをポーリングできるようにします。	デフォルト値: 0 (無効) 設定の型: ブール値 値の範囲: 1 (有効)、 0 (無効) 使用可能なタスク: あり
_BESClient_Comm_ CommandPollInterval Seconds	_BESClient_Comm_CommandPollEnable が有効になっている場合に、クライアントがコンテンツの収集または更新のために親リレーに問い合わせる頻度を決定します。パフォーマンスの低下を防ぐため、900 秒より小さい設定値を指定しないでください。	デフォルト値: 900 設定の型: 数値 (秒) 値の範囲: 0 から 4294967295 使用可能なタスク: あり

この構成を設定した場合、クライアントは、新しいアクションについての UDP ping を待つのではなく、新しい命令がないかどうかをそのリレーに照会します。

V9.X でプロキシ接続を定義する際に考慮する必要があるベスト・プラクティス

よくある問題を避けるためには、以下のヒントやアドバイスを考慮してください。

- Windows サーバー上にプロキシ経由の通信を設定した後、IBM Endpoint Manager 診断ツールを使用して、サーバー（現在も BESGatherService としてレポートされる）がインターネットに正常に接続できることを確認します。
- BES Server¥GatherDBData フォルダ内の GatherDB.log ファイルを調べて、サーバーがインターネットからデータを収集できることを確認します。
- ファイアウォールのルールで、ブロックされているファイル・タイプがあるかどうかを調べます。該当する場合は、サイトから収集するコンテンツにこのファイル・タイプのファイルが少なくとも 1 つ含まれていると、そのサイトのコンテンツ全体が収集されません。
- サーバー上の ProxyPass や、クライアントまたはリレー上の _Enterprise Server_ClientRegister_ProxyPass に指定されたパスワードの有効期限が切れていないことを確認します。
- プロキシがインターネットから任意のファイルをダウンロードできるようにします（例えば、.exe のダウンロードをブロックしない、不明な拡張子を持つファイルをブロックしない、など）。
- IBM Endpoint Manager のほとんどのファイルは bigfix.com または microsoft.com から HTTP ポート 80 を使用してダウンロードされますが、ダウンロードの中には HTTP、HTTPS、または FTP を使用するものもあるため、プロキシ・サービスがこれらのプロトコルを使用してどの場所からでもダウンロードできるようにすることをお勧めします。
- Windows システムの場合は、IBM Endpoint Manager プロキシ構成に指定されている資格情報を使用して Internet Explorer がインターネットに接続できるかどうかを確認し、esync.bigfix.com サーバー（例えば、http://esync.bigfix.com/cgi-bin/bfgather/bessupport）との接続をテストします。
- 内部ネットワーク通信およびコンポーネント間通信ではプロキシがバイパスされるようにしてください。これは、IBM Endpoint Manager サーバーの動作で問題を引き起こす可能性があり、プロキシにとって効率が悪いからです。必要に応じて **ProxyExceptionList** 設定を使用して、プロキシ経由での通信からローカル・システムを除外してください。
- 設定 ProxyExceptionList は、IBM Endpoint Manager バージョン 9.0.835.0 for Windows および Linux システムで導入されました。IBM Endpoint Manager バージョン 9.0 を使用していて、ローカル・サーバーからファイルをダウンロードするコンテンツの使用に問題がある場合は、IBM Endpoint Manager バージョン 9.0.835.0 にアップグレードしてください。

第 13 章 バックアップとリストアの実行

Endpoint Manager サーバーとデータベース・ファイルの定期的なバックアップ (通常は夜間バックアップ) をスケジュールしておく、問題が発生したときに最新バックアップをリストアすることにより、生産性やデータを失うリスクを低減できます。

ただし、災害復旧を実行するときは、以前の作業状態の Endpoint Manager のバックアップがサーバー・コンピューターまたは別のコンピューター上にリストアされることを考慮してください。バックアップの古さによっては、最新の変更またはデータを失う可能性があります。

重要: 最後のバックアップからデータをリストアした後、Endpoint Manager サーバーは以前の状態で再始動することにより、サーバーのメールボックスと各リレーのメールボックスの内容にずれが生じる可能性があります。この場合、Endpoint Manager サーバーは、要求の処理を続けてきたリレーと再同期させる必要があります。そうしないと、リレーはサーバーの要求を無視するおそれがあります。メールボックスを再調整するには、メールボックスのバージョンが同一になるまで、いくつかのアクションをクライアントに送信します。

リカバリー不能な障害が発生した場合は、単一の Endpoint Manager DSA サーバーをリストアすることもできます。

注: 障害の発生した DSA サーバーをバックアップから全面的にリストアする方法は行わないでください。DSA のレプリケーションは複雑であるため、同じ FQDN を持つ新しいサーバーをインストールし、Windows での DSA リカバリー手順や Linux での DSA リカバリー手順を実行することをお勧めします。

すべての DSA サーバーが失われた場合は、Endpoint Manager サーバーのリストア手順として、Windows でのサーバーのリカバリー手順や Linux でのサーバーのリカバリー手順を実行してください。

Windows システムの場合

データベースと Endpoint Manager サーバー・ファイルをバックアップする場合、必要に応じて Windows コンピューター上で Endpoint Manager 環境をリストアできます。

サーバー・バックアップ

1. SQL Server Enterprise Manager を使用して、BFEnterprise データベースと BESReporting データベースの夜間バックアップの保守計画を作成します。複数のバックアップ・コピーを用意しておく、リカバリー時の柔軟性が高まります。耐障害性を向上するために、リモート・システムへのバックアップを検討してください。
2. Endpoint Manager サーバーが使用する以下のファイルとフォルダーをバックアップします。

- [IEM サーバーのフォルダー]¥BESReportsData¥ArchiveData -- アーカイブされた Web レポート。
 - [IEM サーバーのフォルダー]¥BESReportsServer¥wwwroot¥ReportFiles -- カスタム Web レポートのサポート・ファイル。
 - [IEM サーバーのフォルダー]¥Encryption Keys -- プライベート暗号化キー (メッセージ・レベルの暗号化を使用する場合)。
 - [IEM サーバーのフォルダー]¥wwwrootbes¥Uploads -- クライアントに配布するためにシステムにアップロードされたカスタム・パッケージが含まれます。
3. Endpoint Manager サーバーによって使用される以下のファイルとフォルダーは、障害の発生時にサーバーによって自動的に再作成されますが、リカバリーをより迅速に行うためにこれらのファイルとフォルダーをバックアップしてください。
 - [IEM サーバーのフォルダー]¥ClientRegisterData¥registrationlist.txt。コンピュータの最新の既知の IP アドレスに関する情報。
 - [IEM サーバーのフォルダー]¥Mirror Server¥Inbox¥bfemapfile.xml。IBM Endpoint Manager エージェントがアクションと Fixlet を取得するために必要な情報。
 - [IEM サーバーのフォルダー]¥wwwrootbes¥bfsites。Endpoint Manager エージェントがアクションおよび Fixlet を取得するために必要な情報。
 - [IEM サーバーのフォルダー]¥wwwrootbes¥bfmirror¥bfsites。Endpoint Manager エージェントがアクションおよび Fixlet を取得するために必要な情報。
 - [IEM サーバーのフォルダー]¥wwwrootbes¥bfmirror¥downloads。ダウンロード・キャッシュが含まれています。
 4. サイトの資格情報、ライセンス証明書、発行者の資格情報、およびマストヘッドを安全にバックアップします。license.pvk、license.crt、および publisher.pvk の各ファイルは、Endpoint Manager のセキュリティと操作において非常に重要です。プライベート・キー (pvk) ファイルが失われると、リカバリーできません。masthead.afxm ファイルは、リカバリーに使用できる重要な構成ファイルです。このファイルは、管理ツールの「マストヘッドの管理」タブを介してエクスポートできます。
 5. LDAP 構成を使用している場合は、暗号化されたサーバー署名キーの [IEM サーバーのフォルダー]¥EncryptedServerSigningKey.pvk ファイルをバックアップします。

サーバーのリカバリー

1. 以前の Endpoint Manager サーバー・コンピューターか新しいコンピューターを使用して、SQL Server をインストールします (以前に使用していたものと同じ SQL Server のバージョンを使用してください)。最初の Endpoint Manager サーバーで混合モード認証を使用していた場合は、新しい SQL インストール済み環境のに対して混合モード認証を必ず有効にしてください。
2. 新しい Endpoint Manager サーバー・コンピューターが、マストヘッド・ファイルにあるものと同じ URL を使用してネットワークに到達できることを確認します (例えば、<http://192.168.10.32:52311/cgi-bin/bfgather.exe/actionsite> OR <http://bigfixserver.company.com:52311/cgi-bin/bfgather.exe/actionsite> など)。

注: 完全にリストアされる前に、Endpoint Manager クライアントが Endpoint Manager サーバーに接続して問題が発生するのを回避するために、リカバリーが完了するまで、Endpoint Manager サーバーをネットワーク上で確実に使用不可にします。

3. バックアップから BFEnterprise データベースと BESReporting データベースをリストアします。
4. ディレクトリー構造を作成するバックアップ・ファイルとフォルダーをリストアします。
5. 暗号化されたサーバー署名キー [IEM サーバーのフォルダー]¥EncryptedServerSigningKey.pvk のバックアップ・ファイルを、新しいサーバー・コンピューターの C:¥Program Files¥BigFix Enterprise¥BES Server ディレクトリーにコピーすることで、暗号化されたサーバー署名キーをリストアします。
6. マストヘッド・ファイルを使用し、元のインストール・オプションで使ったものと同じパスを指定して、Endpoint Manager サーバー・コンポーネントをインストールします。
7. コマンド・ウィンドウで、Endpoint Manager サーバー・ディレクトリーに移動し、BESAdmin.exe /rotateServerSigningKey を実行します。

注: HTTPS が有効になっている場合は、必ず Web レポートのサーバー設定をリストアしてください。

リストア結果の検証

Endpoint Manager サーバーがリストアされたことを確認するために、以下の手順を実行します。

1. Endpoint Manager 診断をチェックして、すべてのサービスが開始されていることを確認します。
2. Endpoint Manager コンソールにログインして、ログインが機能し、データベース情報がリストアされたことを確認します。
3. サーバーが使用可能になったら Endpoint Manager クライアントと Endpoint Manager リレーがサーバーに接続し、サーバーにデータをレポートすることを確認します。すべてのエージェント・レポートを含む完全リカバリーには、(適用環境のサイズとサーバーが使用できなかった期間によって) 数分から長時間かかる場合があります。少なくともいくつかのエージェントは、1 時間以内に更新済み情報をレポートします。
4. いくつかのエージェントがサーバーにレポートしていることを確認したら、「ツール」>「カスタム・アクションの実行」を使用して、すべてのコンピューターに空白のアクションを送信します。空白のアクションはエージェント・コンピューターに何も変更を加えませんが、エージェントは空白のアクションを受け取ったことをレポートします。
5. Web レポートにログインして、データがリストアされたことを確認します。

注: Web レポート構成にリモート・データ・ソースが定義されている場合は、Web レポートの「管理」>「データ・ソース設定」>「編集」ページでデータ・ソース資格情報を再入力して初めて、Web レポートがデータ・ソースに接続します。

DSA リカバリー

失われた DSA サーバーをリカバリーする場合は、すべての最上位 Endpoint Manager リレー (つまり適用環境全体) が、残りの DSA サーバーを既に指していないければなりません。このリカバリー手順中は、すべてのリレーおよびクライアントが、動作している DSA サーバーにレポートする状態にしておくことをお勧めします。既存のリレー設定ではこのようにできない場合は、リストアするサーバーをネットワーク上で分離して、動いている DSA サーバーのみがそのサーバーに接続できるようにします。

1. マスター DSA サーバーに障害が発生した場合は、BFEnterprise SQL データベースで以下のプロシーチャーを実行して、障害が発生したサーバーの修復および複製中はセカンダリー DSA サーバーをマスターにプロモートします。

```
declare @ServerID varchar(32)
select @ServerID = convert(varchar(32),ServerID) from DBINFO
execute [BFEnterprise].[dbo].[update_adminfields] 'Z:masterDatabaseServerID',@ServerID
```

このようにして、新規 DSA サーバーをインストールし、障害が発生したサーバーの修復中はセカンダリー DSA サーバーで管理ツールを実行することができます。

2. 既存の DSA サーバーで、障害が発生した DSA サーバー ID をデータベースから削除します。
 - a. 最初に、以下の SQL ステートメントを実行して、既存の DSA サーバーの ID を確認します。

```
select ServerID from DBINFO
```

- b. 以下のようにして、DSA サーバーの ID をリストします。

```
select * from REPLICATION_SERVERS
```

- c. 障害が発生したサーバー ID を特定した後に、以下のプロシーチャーを実行します。

```
execute BFEnterprise.dbo.delete_replication_server <ID>
```

3. サーバーのオペレーティング・システムおよびデータベース・ソフトウェアを、Endpoint Manager サーバーや Endpoint Manager データベースの残存物のない初期状態でリストアします。
4. 以下の項目をバックアップからリストアします。
 - [IEM サーバーのフォルダー]¥BESReportsServer¥wwwroot¥ReportFiles
 - [IEM サーバーのフォルダー]¥Encryption Keys (必要に応じてセカンダリー・サーバーからコピーしてリストアすることも、管理ツールで生成された新しい鍵を使用することもできます)
 - [IEM サーバーのフォルダー]¥UploadManagerData (オプション。失われたサーバーが SUA ソースであった場合に、SUA データをより迅速にリカバリーできます)
 - [IEM サーバーのフォルダー]¥wwwrootbes¥bfmirror¥downloads¥ActionURLs
 - [IEM サーバーのフォルダー]¥wwwrootbes¥bfmirror¥downloads¥sha1 (オプション。キャッシュされたファイルをより迅速にリカバリーできます)
 - Web レポート用の cert.pem ファイル (HTTPS を使用する場合)
 - SQL Server の BESReporting データベース

5. インストーラーおよび既存のマストヘッドを使用して、Endpoint Manager サーバーをインストールします。追加情報については、66 ページの『追加 Windows サーバーのインストール』を参照してください。
6. 以下のレジストリー値を設定して、BES FillDB サービスを再始動します。

32 ビット Windows システムの場合は [HKLM\Software\BigFix\Enterprise Server\FillDB] に移動し、64 ビット Windows システムの場合は [HKLM\Software\Wow6432Node\BigFix\Enterprise Server\FillDB] に移動して、以下の値を設定します。

```
"PerformanceDataPath"[REG_SZ] = "[IEM Server folder]\FillDB\FillDBperf.log"
"UninterruptibleReplicationSeconds"[DWORD] = 14400 (decimal)
```

7. Endpoint Manager クライアントおよびコンソールをインストールします。
8. 複製が完了したら、SQL データベースで以下のプロシーチャーを実行して、新規にリストアされたこの Endpoint Manager サーバーをマスター・サーバーにプロモートします。

```
declare @ServerID varchar(32)
select @ServerID = convert(varchar(32),ServerID) from DBINFO
execute [BFEnterprise].[dbo].[update_adminfields] 'Z:masterDatabaseServerID',@ServerID
```

9. プラグインを再インストールし、再構成します。構成情報は、現在動作している DSA サーバーから収集することも、管理者によって記録されたインストールのメモや構成詳細情報から収集することもできます。
10. 以下のレジストリー値を設定して、BES FillDB サービスを再始動します。

32 ビット Windows システムの場合は [HKLM\Software\BigFix\Enterprise Server\FillDB] に移動し、64 ビット Windows システムの場合は [HKLM\Software\Wow6432Node\BigFix\Enterprise Server\FillDB] に移動して、以下の値を設定します。

```
"PerformanceDataPath"[REG_SZ] = ""
"UninterruptibleReplicationSeconds"[DWORD] = 120 (decimal)
```

11. 管理ツールを起動して、このリストア対象サーバーのレプリケーション間隔を、望ましいレベルに更新します。通常、この値は、他の DSA サーバーに設定されている間隔と一致する必要があります。

注: 適用環境の大きさによっては、複製プロセスが完了するのに何日かかる場合があります。完了したかを確認するには、FillDBperf.log ファイルの Replication Completed メッセージを探します。両方の適用環境でデータが同期しているかを確認するもう一つの方法は、各 DSA サーバーに個別の Endpoint Manager コンソールを接続し、コンテンツを比較することです。

Linux システムの場合

データベースと Endpoint Manager サーバー・ファイルをバックアップする場合、必要に応じて Linux コンピューター上で Endpoint Manager 環境をリストアできます。

サーバー・バックアップ

Endpoint Manager サーバーをバックアップするには、以下の手順を実行します。

1. 以下のコマンドを使用して、Endpoint Manager サービスを停止します。

```
/etc/init.d/besfilldb stop
/etc/init.d/besgatherdb stop
/etc/init.d/besserver stop
/etc/init.d/beswebreports stop
/etc/init.d/besclient stop
```

2. db2stop コマンドを使用して、DB2 データベースを停止します。

3. 以下のコマンドを使用して、BFENT データベースと BESREPOR データベースをバックアップします。

```
db2 backup db BFENT
db2 backup db BESREPOR
```

次のコマンドを使用して、任意で絶対パスを追加します。

```
db2 backup db BFENT to /AbsolutePathExample
db2 backup db BESREPOR to /AbsolutePathExample
```

4. 以下のフォルダーを手動でバックアップします。

```
/var/opt/BESClient
/var/opt/BESServer
/var/opt/BESWebReportsServer
/opt/BESWebReportsServer
```

さらに、以下のファイルもバックアップします。

```
/etc/opt/BESClient/actionsite.afxm
/etc/opt/BESServer/actionsite.afxm
/etc/opt/BESWebReportsServer/actionsite.afxm
```

5. /etc/init.d で、以下のファイルをバックアップします。

```
besclient
besfilldb
besgatherdb
besserver
beswebreports
```

6. サイトの資格情報、ライセンス証明書、およびマストヘッド・ファイルをバックアップします。 license.pvk ファイルと license.crt ファイルは、Endpoint Manager のセキュリティと操作において非常に重要です。プライベート・キー (pvk) ファイルが失われると、リカバリーできません。

マストヘッド・ファイルは、リカバリーに使用する可能性がある重要な構成ファイルです。このファイルをバックアップするには、ファイル・システムから /etc/opt/BESServer/actionsite.afxm をコピーし、新規マストヘッド masthead.afxm として保存するか、あるいは、ブラウザーからマストヘッド・ファイル <http://hostname:52311/masthead/masthead.afxm> を開いて、それを保存します。

サーバーのリカバリー

1. すべての Endpoint Manager プロセスとデータベースを停止します。
2. Endpoint Manager rpm ファイルを削除します。
3. 以下のフォルダーを削除します。

```
/var/opt/BESClient
/var/opt/BESServer
/var/opt/BESWebReportsServer
/opt/BESWebReportsServer
```

さらに、以下のファイルも削除します。

```
/etc/opt/BESClient/actionsite.afxm
/etc/opt/BESServer/actionsite.afxm
/etc/opt/BESWebReportsServer/actionsite.afxm
/etc/init.d/besclient
/etc/init.d/besfilldb
/etc/init.d/besgatherdb
/etc/init.d/besserver
/etc/init.d/beswebreports
```

4. 以下のコマンドを実行して、BFENT データベースと BESREPOR データベースを削除します。

```
db2 drop db BFENT
db2 drop db BESREPOR
```

5. Endpoint Manager をインストールして、Endpoint Manager rpm ファイルを登録します。
6. Endpoint Manager プロセスとインストール済みのデータベースを停止します。
7. BFENT データベースと BESREPOR データベースをアンインストールします。
8. 以前に保存されたフォルダーとファイルをリストアします。

```
/var/opt/BESClient
/var/opt/BESServer
/var/opt/BESWebReportsServer
/opt/BESWebReportsServer

/etc/opt/BESClient/actionsite.afxm
/etc/opt/BESServer/actionsite.afxm
/etc/opt/BESWebReportsServer/actionsite.afxm
/etc/init.d/besclient
/etc/init.d/besfilldb
/etc/init.d/besgatherdb
/etc/init.d/besserver
/etc/init.d/beswebreports
```

9. 以下のようにして、以前に保存された BFENT と BESREPOR をリストアします。

```
db2 restore db BFENT
db2 restore db BESREPOR
```

絶対パスを使用して保存した場合は、以下のコマンドを使用します。

```
db2 restore db BFENT from /AbsolutePathExample
db2 restore db BESREPOR from /AbsolutePathExample
```

10. データベースを開始してから、Endpoint Manager プロセスを開始します。
11. コンソールにログオンします。「Connection to server could not be completed. Diagnostic Message: Unexpected server error: Bad sequence parameter」というエラー・メッセージが表示される場合は、Enterprise Console スtringを探して、コンソールがインストールされているディスクのコンソール・キャッシュを削除します。このディレクトリーで、Endpoint Manager サーバーのホスト名と同じ名前のディレクトリーを削除してから、もう一度ログオンします。

リストア結果の検証

Endpoint Manager サーバーがリストアされたことを確認するために、以下の手順を実行します。

1. Endpoint Manager 診断をチェックして、すべてのサービスが開始されていることを確認します。
2. Endpoint Manager コンソールにログインして、ログインが機能し、データベース情報がリストアされたことを確認します。
3. サーバーが使用可能になったら Endpoint Manager クライアントと Endpoint Manager リレーがサーバーに接続し、サーバーにデータをレポートすることを確認します。すべてのエージェント・レポートを含む完全リカバリーには、(適用環境のサイズとサーバーが使用できなかった期間によって) 数分から長時間かかる場合があります。少なくともいくつかのエージェントは、1 時間以内に更新済み情報をレポートします。
4. いくつかのエージェントがサーバーにレポートしていることを確認したら、「ツール」>「カスタム・アクションの実行」を使用して、すべてのコンピューターに空白のアクションを送信します。空白のアクションはエージェント・コンピューターに何も変更を加えませんが、エージェントは空白のアクションを受け取ったことをレポートします。
5. Web レポートにログインして、データがリストアされたことを確認します。

注: Web レポート構成にリモート・データ・ソースが定義されている場合は、Web レポートの「管理」>「データ・ソース設定」>「編集」ページでデータ・ソース資格情報を再入力して初めて、Web レポートがデータ・ソースに接続します。

DSA リカバリー

失われた DSA サーバーをリカバリーする場合は、すべての最上位 Endpoint Manager リレー (つまり適用環境全体) が、残りの DSA サーバーを既に指していないければなりません。このリカバリー手順中は、すべてのリレーおよびクライアントが、動作している DSA サーバーにレポートする状態にしておくことをお勧めします。既存のリレー設定ではこのようにできない場合は、リストアするサーバーをネットワーク上で分離して、動いている DSA サーバーのみがそのサーバーに接続できるようにします。

1. マスター DSA サーバーに障害が発生した場合は、BFEnterprise SQL データベースで以下のプロシージャを実行して、障害が発生したサーバーの修復および複製中はセカンダリー DSA サーバーをマスターにプロモートします。

```
db2
  set schema dbo
  select serverid from DBINFO (take count of SERVERID)
  set current function path dbo
  call update_adminFields('Z:masterDatabaseServerID','<serverid>') - Replace
  SERVERID with the value from the previous query
```

このようにして、新規 DSA サーバーをインストールし、障害が発生したサーバーの修復中はセカンダリー DSA サーバーで管理ツールを実行することができます。

2. 既存の DSA サーバーで、障害が発生した DSA サーバー ID をデータベースから削除します。

- a. 最初に、以下の SQL ステートメントを実行して、既存の DSA サーバーの ID を確認します。

```
select ServerID from DBINFO
```

- b. 以下のようにして、DSA サーバーの ID をリストします。

```
select * from REPLICATION_SERVERS
```

- c. 障害が発生したサーバー ID を特定した後に、以下のプロシーチャーを実行します。

```
call dbo.delete_replication_server(ID)
```

3. サーバーのオペレーティング・システムおよびデータベース・ソフトウェアを、Endpoint Manager サーバーや Endpoint Manager データベースの残存物のない初期状態でリストアします。

4. 以下の項目をバックアップからリストアします。

- /var/opt/BESWebReportsServer/
- [IEM サーバーのフォルダー]/Encryption Keys (必要に応じてセカンダリー・サーバーからコピーしてリストアすることも、管理ツールで生成された新しい鍵を使用することもできます)
- [IEM サーバーのフォルダー]/UploadManagerData (オプション。失われたサーバーが SUA ソースであった場合に、SUA データをより迅速にリカバリーできます)
- [IEM サーバーのフォルダー]/wwwrootbes/bfmirror/downloads/ActionURLs
- [IEM サーバーのフォルダー]/wwwrootbes/bfmirror/downloads/sha1 (オプション。キャッシュされたファイルをより迅速にリカバリーできます)
- Web レポート用の cert.pem ファイル (HTTPS を使用する場合)
- SQL Server の BESReporting データベース

5. インストーラーおよび既存のマストヘッドを使用して、Endpoint Manager サーバーをインストールします。追加情報については、111 ページの『追加 Linux サーバーのインストール (DSA)』を参照してください。

6. besserver.config ファイルに以下のキーワードを設定して、BES FillDB サービスを再始動します。

```
PerformanceDataPath = <Performance_Data_Path_filename>  
UnInterruptibleReplicationSeconds = 14400
```

ここで、<Performance_Data_Path_filename> には /var/opt/BESServer/FillDBData/FillDBPerf.log を指定できます。

7. Endpoint Manager クライアントおよびコンソールをインストールします。

8. 複製が完了したら、SQL データベースで以下のプロシーチャーを実行して、新規にリストアされたこの Endpoint Manager サーバーをマスター・サーバーにプロモートします。

```
db2  
set schema dbo  
select serverid from DBINFO (take count of SERVERID)  
set current function path dbo  
call update_adminFields('Z:masterDatabaseServerID','<serverid>') - Replace  
SERVERID with the value from the previous query
```

9. プラグインを再インストールし、再構成します。構成情報は、現在動作している DSA サーバーから収集することも、管理者によって記録されたインストールのメモや構成詳細情報から収集することもできます。
10. `besserver.config` ファイルに以下のキーワードを設定して、BES FillDB サービスを再始動します。

```
PerformanceDataPath = ""  
UnInterruptibleReplicationSeconds = 120
```

11. 管理ツールを起動して、このリストア対象サーバーのレプリケーション間隔を、望ましいレベルに更新します。通常、この値は、他の DSA サーバーに設定されている間隔と一致する必要があります。

注: 適用環境の大きさによっては、複製プロセスが完了するのに何日かかる場合があります。完了したかを確認するには、`FillDBperf.log` ファイルの `Replication Completed` メッセージを探します。両方の適用環境でデータが同期しているかを確認するもう一つの方法は、各 DSA サーバーに個別の `Endpoint Manager` コンソールを接続し、コンテンツを比較することです。

第 14 章 Windows システムでのアップグレード

重要: Fixlet によるアップグレードは、Endpoint Manager V9.1 では実行できません。Endpoint Manager のコンポーネントは手動でアップグレードする必要があります。

Endpoint Manager サーバーとすべての Endpoint Manager コンソールを同時にアップグレードする必要があります (コンソールのバージョンがサーバーのバージョンと異なっている場合、コンソールからサーバーやデータベースに接続できなくなります)。

他の Endpoint Manager コンポーネント (Endpoint Manager クライアントと Endpoint Manager リレー) は、アップグレードされたバージョンの Endpoint Manager サーバーと問題なく連携することができます。しかし、新しい機能を利用するために、可能な限り Endpoint Manager クライアントおよびリレーをアップグレードすることをお勧めします。

DSA 環境のアップグレードについては、181 ページの『手動アップグレード』を参照してください。

注: 拡張セキュリティー・オプションを使用可能にしなかった場合に限り、以前のバージョンの Endpoint Manager にロールバックすることができます。ご使用の環境で使用可能にした後は、使用不可にした場合であっても、以前のバージョンの Endpoint Manager にロールバックできません。

V9.1 へのアップグレード・パス

以下の表では、IBM Endpoint Manager V9.1 へのアップグレード・パスについて示します。

• サーバーのアップグレード

表 14. サーバーのアップグレード

アップグレード元	Windows アップグレード
7.x	不可
8.x	可
9.0	可

• クライアントのアップグレード

表 15. クライアントのアップグレード

アップグレード元	Windows アップグレード	UNIX のアップグレード	Mac のアップグレード
7.x	可	可	可
8.x	可	可	可
9.0	可	可	可

アップグレードの前に

Endpoint Manager コンポーネントをアップグレードする前に、以下の手順を実行します。

1. すべての IBM Endpoint Manager コンソールを閉じてください。
2. IBM Endpoint Manager サーバーおよびデータベースをバックアップしてください。
3. SQL データベースをアップグレードしてください。SQL 2000 データベースはサポートされなくなりました。
4. license.pvk、license.crt、および masthead.afxm を Endpoint Manager サーバーの別の場所または USB キーにバックアップしてください。
5. レプリケーション間隔を増やして、アップグレード中にレプリケーションが繰り返し失敗することを防いでください。追加情報については、「構成ガイド」を参照してください。
6. Endpoint Manager コンポーネントを以下の順序に従ってアップグレードしてください。
 - a. サーバーおよびコンソール。これらのコンポーネントはバージョンが一致している必要があり、また、同時にアップグレードする必要があります。
 - b. リレー
 - c. クライアント

サーバー、リレー、およびクライアントのバージョンは一致する必要はなく、これらのコンポーネントのアップグレードは別々の時に行えます。古いバージョンのクライアントはより新しいバージョンのリレーまたはサーバーに引き続きレポートできますが、それらの古いクライアントには新しいリリースの機能の一部がない場合があります。

7. DSA サーバーの場合、まず 1 つの DSA サーバーをアップグレードしてアップグレードを正常に行えることを確認してから、他の DSA サーバーをアップグレードしてください。
8. アップグレード後に、Endpoint Manager 管理ツールを実行して、SHA-2 署名でデータを更新し、リモート・データベースを更新し、必要に応じて NIST セキュリティ標準を設定します。

注:

- 大規模な適用環境の場合、サーバーのアップグレードに数分かかる場合があります。
- アップグレード後に適用環境の応答が遅くなる場合があります。これは、アップグレードのダウン時間にクライアント・レポートのバックログが生じて、アップグレードが完了した後に IBM Endpoint Manager サーバーがそのバックログを処理するために数時間かかる場合があるためです。

手動アップグレード

DSA 複数サーバー環境、またはリモート・データベースを使用する Endpoint Manager サーバーをアップグレードする場合は、Fixlet によるアップグレードではなく手動アップグレードを使用します。

注: DSA サーバーのアップグレード中は、アップグレード中のシステムに対するレプリケーション処理が開始されてシステムが不安定になるのを防ぐために、他のいずれの DSA サーバーでもサービスを実行しないでください。

インストール・ジェネレーターのアップグレード

1. IBM Endpoint Manager インストール・ジェネレーターをインストールしたコンピュータで、<http://support.bigfix.com/bes/install/downloadbes.html> から新しい IBM Endpoint Manager インストール・ジェネレーターをダウンロードして実行します。
2. アップグレードするかどうか確認するプロンプトが出されたら「はい」をクリックし、インストーラーの指示に従います。

サーバーのアップグレード

1. IBM Endpoint Manager サーバーのインストール・フォルダー (デフォルトの場所は C:\Program Files\BigFix Enterprise\BES Installers\Server) を IBM Endpoint Manager サーバー・コンピュータにコピーします。
2. IBM Endpoint Manager サーバー・コンピュータで IBM Endpoint Manager サーバーのインストーラー (setup.exe) を実行します。

注: リモート・データベースを使用している場合は、アップグレードを行う前に、<http://www-01.ibm.com/support/docview.wss?uid=swg21506063> の記事を参照してください。

3. インストーラーの指示に従ってアップグレードします。トラブルシューティングの情報については、C:\besserverupgrade.log を参照してください。
4. 8.0 リリース用の Trend Core Protection Module サーバーをアップグレードするには、<http://www-01.ibm.com/support/docview.wss?uid=swg21506219> を参照してください。

コンソールのアップグレード

1. IBM Endpoint Manager コンソールのインストール・フォルダー (デフォルトの場所は C:\Program Files\BigFix Enterprise\BES Installers\Console) を、IBM Endpoint Manager コンソールを実行するすべてのコンピュータにコピーします。
2. 現在 IBM Endpoint Manager コンソールを実行しているすべてのコンピュータで IBM Endpoint Manager コンソールのインストーラー (setup.exe) を実行します。

リレーのアップグレード

IBM Endpoint Manager のリレーを個別にアップグレードするには、IBM Endpoint Manager のリレーのアップグレード・ファイルをダウンロードして実行します。このファイルは <http://support.bigfix.com/bes/install/downloadbes.html> に格納されています。

クライアントのアップグレード

- IBM Endpoint Manager クライアントを個別にアップグレードするには、IBM Endpoint Manager クライアントのインストール・フォルダー（デフォルトの場所は C:\Program Files\BigFix Enterprise\BES Installers\Client）を、IBM Endpoint Manager クライアントを実行するすべてのコンピューターにコピーした後、setup.exe を実行します。
- IBM Endpoint Manager クライアントは、Tivoli Endpoint Manager クライアント適用ツール、ログイン・スクリプトまたは別の適用テクノロジーを使用してアップグレードすることもできます。新しい IBM Endpoint Manager クライアントのインストーラーを、古い IBM Endpoint Manager クライアントがあるコンピューターで実行するだけです。

Web レポートのアップグレード

スタンドアロン Web レポートをアップグレードするには、BigFix-BES-Server-9.1.xxx.x.exe を実行します。これにより、Web レポートのインストール済み環境が検出され、その環境に対するアップグレードが提供されます。

Endpoint Manager サーバーに Web レポートがインストールされている場合、Web レポートは Endpoint Manager サーバーと共にアップグレードされます。

注: リモート・データベースを使用している場合は、そのデータベースに対する DBO 許可を持つユーザーとしてアップグレードを実行してください。

第 15 章 Linux システムでのアップグレード

重要: Fixlet によるアップグレードは、Endpoint Manager V9.1 では実行できません。Endpoint Manager のコンポーネントは手動でアップグレードする必要があります。

Endpoint Manager サーバーとすべての IBM Endpoint Manager コンソールを同時にアップグレードする必要があります (コンソールのバージョンがサーバーのバージョンと異なっている場合、コンソールからサーバーやデータベースに接続できなくなります)。

他の IBM Endpoint Manager コンポーネント (IBM Endpoint Manager クライアントと IBM Endpoint Manager リレー) は、アップグレードされたバージョンの IBM Endpoint Manager サーバーと問題なく連携することができます。しかし、新しい機能を利用するために、可能な限り IBM Endpoint Manager クライアントおよびリレーをアップグレードすることをお勧めします。

DSA 環境のアップグレードについては、184 ページの『手動アップグレード』を参照してください。

注: 拡張セキュリティー・オプションを使用可能にしなかった場合に限り、以前のバージョンの Endpoint Manager にロールバックすることができます。ご使用の環境で使用可能にした後は、使用不可にした場合であっても、以前のバージョンの Endpoint Manager にロールバックできません。

V9.1 へのアップグレード・パス

以下の表では、IBM Endpoint Manager V9.1 へのアップグレード・パスについて示します。

• サーバーのアップグレード

表 16. サーバーのアップグレード

アップグレード元	UNIX のアップグレード
7.x	不可
8.x	不可
9.0	可

• クライアントのアップグレード

表 17. クライアントのアップグレード

アップグレード元	Windows アップグレード	UNIX のアップグレード	Mac のアップグレード
7.x	可	可	可
8.x	可	可	可
9.0	可	可	可

アップグレードの前に

Endpoint Manager コンポーネントをアップグレードする前に、以下の手順を実行します。

1. すべての IBM Endpoint Manager コンソールを閉じてください。
2. IBM Endpoint Manager サーバーおよびデータベースをバックアップしてください。
3. `license.pvk`、`license.crt`、および `masthead.afxm` を Endpoint Manager サーバーの別の場所または USB キーにバックアップしてください。
4. ご使用のサーバーが DSA 環境内で構成されている場合、レプリケーション間隔を増やして、アップグレード中にレプリケーションが繰り返し失敗することを防いでください。追加情報については、「構成ガイド」を参照してください。
5. Endpoint Manager コンポーネントを以下の順序に従ってアップグレードしてください。
 - a. サーバーおよびコンソール (コンソールとサーバーは同じバージョンである必要があります、また、同時にアップグレードする必要があります。)
 - b. リレー
 - c. クライアント

サーバー、リレー、およびクライアントのバージョンは一致する必要はなく、これらのコンポーネントのアップグレードは別々の時に行えます。古いバージョンのクライアントはより新しいバージョンのリレーまたはサーバーに引き続きレポートできますが、それらの古いクライアントには新しいリリースの機能の一部がない場合があります。

6. DSA サーバーの場合、まず 1 つの DSA サーバーをアップグレードしてアップグレードを正常に行えることを確認してから、他の DSA サーバーをアップグレードしてください。

注:

- 大規模な適用環境の場合、サーバーのアップグレードに数分かかる場合があります。
- アップグレード後に適用環境の応答が遅くなる場合があります。これは、アップグレードのダウン時間中にクライアント・レポートのバックログが発生し、アップグレードの完了後に IBM Endpoint Manager サーバーがそのバックログを処理するために数時間かかる場合があるためです。

手動アップグレード

DSA 複数サーバー環境をアップグレードする場合は、Fixlet によるアップグレードではなく、手動でアップグレードを行ってください。

注: DSA サーバーのアップグレード中は、アップグレード中のシステムに対するレプリケーション処理が開始されてシステムが不安定になるのを防ぐために、他のいずれの DSA サーバーでもサービスを実行しないでください。

サーバーのアップグレード

1. IBM Endpoint Manager サーバーのインストール可能イメージを Endpoint Manager サーバー・コンピューターにコピーして、任意のフォルダーに解凍します。
2. Endpoint Manager サーバー・コンピューターで、以下の Endpoint Manager サーバー・アップグレード・スクリプトを実行します。

```
./install.sh -upgrade [-opt BES_LICENSE_PVK=<path+license.pvk>]  
                  [-opt BES_LICENSE_PVK_PWD=<password>]
```

指定の内容は以下のとおりです。

-opt BES_LICENSE_PVK=<path+license.pvk>

プライベート・キー・ファイル (*filename.pvk*) を指定します。このプライベート・キー・ファイルとそのパスワードは、製品ライセンスを更新するとき、および Endpoint Manager データベースで必要な SHA-256 署名の更新を実行するときが必要となります。

-opt BES_LICENSE_PVK_PWD=<password>

プライベート・キー・ファイル (*filename.pvk*) に関連付けられたパスワードを指定します。

install.sh サーバー・スクリプトは、ローカル・サーバーで検出したすべてのコンポーネントをアップグレードします。

注: トラブルシューティングの情報については、*/var/log/BESInstall.log* ファイルと */var/log/BESAdminDebugOut.txt* ファイルを参照してください。

コンソールのアップグレード

1. Endpoint Manager コンソールのインストール・フォルダー (デフォルトは */var/opt/BESInstallers/Console*) を、Endpoint Manager コンソールを実行するすべての Windows コンピューターにコピーします。
2. 現在 Endpoint Manager コンソールを実行しているすべての Windows コンピューターで Endpoint Manager コンソールのインストーラー (*setup.exe*) を実行します。

注: Endpoint Manager コンソールは Linux コンピューターでは実行されません。

リレーのアップグレード

IBM Endpoint Manager のリレーを個別にアップグレードするには、IBM Endpoint Manager のリレーのアップグレード・ファイルをダウンロードして実行します。このファイルは <http://support.bigfix.com/bes/install/downloadbes.html> に格納されています。

クライアントのアップグレード

- Endpoint Manager クライアントは、個別にアップグレードすることができます。これは、Endpoint Manager クライアントのインストール可能イメージを、

Endpoint Manager クライアントを実行しているコンピューターそれぞれにコピーした後、セットアップ・プログラムを実行して行います。

- Endpoint Manager クライアントは、Endpoint Manager クライアント適用ツール、ログイン・スクリプト、または別の適用テクノロジーを使用してアップグレードすることもできます。単に新しい Endpoint Manager クライアントのインストーラーを、古い Endpoint Manager クライアントがあるコンピューターで実行するだけです。

Web レポートのアップグレード

スタンドアロンの Web レポート・サーバーをアップグレードするには、次の `install.sh` のサーバー・アップグレード・スクリプトを実行します。

```
./install.sh -upgrade
```

付録 A. 用語集

アクション・パスワード (Action Password)

署名パスワードを参照。

アクション・スクリプト言語 (Action Scripting Language)

アクション・スクリプトの作成に使用される言語。アクションは、AppleScript および Unix シェルなどの、さまざまなスクリプト言語で作成できます。

BigFix Enterprise Suite (BES)

IBM Endpoint Manager の以前の名前。

クライアント (Client)

IBM Endpoint Manager の下で管理される、各ネットワーク・コンピューターにインストールされているソフトウェア。クライアントは、Fixlet メッセージのプールにアクセスし、自身がインストールされているコンピューターで脆弱性をチェックし、脆弱性のある状態になったときにはサーバーにメッセージを送信します。以前は BES クライアントと呼ばれていましたが、現在は IBM Endpoint Manager クライアントまたは単にクライアントと呼ばれています。

コンソール (Console)

ネットワーク内の、クライアントがインストールされているすべてのコンピューターのステータスの概要を提供する管理プログラム。脆弱である可能性のある部分を特定し、修復アクションを提示します。以前は BES コンソールと呼ばれていましたが、現在は IBM Endpoint Manager コンソールまたは単にコンソールと呼ばれています。

カスタム・サイト (Custom Site)

独自のカスタム・コンテンツを作成し、それをカスタム・サイトでホストすることができます。これは、カスタム・コンテンツを作成する権限を付与されたマスター・オペレーターのみが実行できます (Admin プログラムを使用して、これらのユーザーを割り振る)。

DSA 分散サーバー・アーキテクチャー。複数のサーバーがリンクされ、障害発生時に備えて完全な冗長性を提供します。

Fixlet メッセージ (Fixlet message)

コンピューター上の問題のある状態を対象として説明し、その自動フィックスを提供するメカニズム。

Fixlet サーバー (Fixlet servers)

Fixlet サイトのサブスクリプションを提供する Web サーバー。企業のネットワーク内部にあっても、(外部への直接の Web アクセスが許可されている場合は) ネットワーク外部にあってもかまいません。

Fixlet サイト (Fixlet site)

クライアントが Fixlet メッセージの取得元とする信頼できるソース。

生成プログラム・インストール・フォルダー (Generator Install folder)

生成プログラムが IBM Endpoint Manager システム用のインストール・ファイルを配置するインストール・コンピューター上のディレクトリー。

インストール・コンピューター (Installation Computer)

インストール生成プログラムをホストして実行する、セキュリティーで保護されたコンピューター (IBM Endpoint Manager サーバー・コンピューターとは別のもの)。

インストール生成プログラム (Installation Generator)

IBM Endpoint Manager システムのコア・コンポーネント用のインストーラーを作成するアプリケーション。

管理権限 (Management Rights)

通常のコンソール・オペレーターを、指定されたコンピューターのグループに制限することができます。これらの制限は、そのユーザーの管理権限を表します。サイト管理者またはマスター・オペレーターのみが、管理権限を割り当てることができます。

マスター・オペレーター (Master Operator)

管理権限を持つコンソール・オペレーター。マスター・オペレーターは、サイト管理者が実行できることはほとんどすべて実行できますが、新規オペレーターを作成することはできません。

マストヘッド (Masthead)

信頼できる Fixlet コンテンツが提供されている場所を指す URL など、IBM Endpoint Manager プロセスのパラメーターを含むファイル。IBM Endpoint Manager クライアントは、サブスクライブされているマストヘッドに基づいてコンテンツを企業に取り込みます。

ミラー・サーバー (Mirror server)

企業で直接の Web アクセスは許可していないが、代わりにパスワード・レベルの認証を必要とするプロキシ・サーバーを使用する場合に、IBM Endpoint Manager システムで必要なサーバー。

オペレーター (Operator)

IBM Endpoint Manager コンソールを操作する人員。通常のオペレーターは、Fixlet アクションの適用および特定のコンピューター設定の編集を実行できます。マスター・オペレーターは、他のオペレーターに管理権限を割り当て可能であるなど、追加的な特権を持っています。

リレー (Relay)

特殊なサーバー・ソフトウェアを実行しているクライアント。リレーは、サーバーとクライアントの間の直接のダウンロードを最小限にし、アップストリーム・データを圧縮することによって、サーバーおよびネットワークの負荷を軽減します。リレーはクライアントによって自動的に検出され、クライアントは接続する最適のリレーを動的に選択します。以前は BES リレーと呼ばれていましたが、現在は IBM Endpoint Manager リレーまたは単にリレーと呼びます。

Relevance Language

関連句の記述に使用される言語。

ルート・サーバー (Root Server)

メイン・サーバーによって、IIS の代替として提供される HTTP または HTTPS サービスを指します。IBM Endpoint Manager ルート・サーバーは、特に Fixlet のトラフィックに合わせて調整されており、この用途では IIS よりも効率的です。以前は BES ルート・サーバーと呼ばれていましたが、現在は IBM Endpoint Manager ルート・サーバーまたは単にルート・サーバーと呼ばれています。

サーバー (Server)

IBM Endpoint Manager システム内の個々のコンピューター間でやり取りされる情報のリレーを調整する、相互作用するアプリケーション (Web サーバー、CGI-BIN、およびデータベース・サーバー) のコレクション。サーバー・プロセスは、単一のサーバー・コンピューターによってホストされるか、セグメント化されて別個のサーバー・コンピューターで実行されるか、または冗長サーバー上に複製される場合があります。以前は BES サーバーと呼ばれていましたが、現在は IBM Endpoint Manager サーバーまたは単にサーバーと呼ばれています。

署名パスワード (Signing password)

適用のアクションに署名するためにコンソール・オペレーターが使用するパスワード (IBM Endpoint Manager システムがインストールされるときに指定されたもの)。コンソールのインターフェースではアクション・パスワードと呼ばれます。

サイト管理者 (Site Administrator)

IBM Endpoint Manager のインストールの担当者であり、新規コンソール・オペレーターを作成する権限を保有しています。

SQL Server (SQL server)

Microsoft が提供する完全なデータベース・エンジン。取得して IBM Endpoint Manager システムへインストールすると、基本的なレポート作成およびデータ・ストレージのニーズを超えるものを満たすことができます。SQLite からのステップアップ。

標準適用環境 (Standard deployment)

単一の管理ドメインを持つワークグループおよび企業に適用される IBM Endpoint Manager の適用環境。すべてのクライアント・コンピューターが単一の社内サーバーに直接アクセスできる設定を目的としています。

システム・インストール・フォルダー (System install folder)

サーバー・ソフトウェアおよび関連ファイル (コンソール・インストーラーおよびクライアント・インストーラーを含む) がインストールされる IBM Endpoint Manager サーバー上のディレクトリー。

IBM Endpoint Manager データベース (IBM Endpoint Manager database)

個々のコンピューターに関するデータと Fixlet メッセージを格納するシステムのコンポーネント。SQL Server で実行されるこのデータベースには、IBM Endpoint Manager サーバーの相互作用が主に影響します。

IBM Endpoint Manager

複数のネットワークにわたるコンピューターをモニターして、数回のマウス・クリックのみで脆弱性を検出して修正する、エンタープライズ環境向けの予防保守ツール。

- VPN** 仮想プライベート・ネットワーク。安価なインターネット接続を使用して、企業がローカル・エリア・ネットワークを世界中に展開できるようにする暗号化チャネル (またはトンネル)。
- WAN** 広域ネットワーク。多数のオフィスが WAN によって接続されています。WAN の帯域幅によって、適用環境内のリレーの配置が決まります。広域ネットワーク内のシン・クライアント・コンピューティングの場合は、ダウンロードを集約してオーバーヘッドを減らすために、より多くのリレーが必要となります。

付録 B. サポート

この製品について詳しくは、以下の資料を参照してください。

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager サポート・サイト
- IBM Endpoint Manager Wiki
- 知識ベース
- フォーラムおよびコミュニティー

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態を提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

Adobe、PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、および Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は英国 The Minister for the Cabinet Office の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java™ およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc. の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open、LTO、LTO ロゴ、Ultrium、および Ultrium ロゴは、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。



Printed in Japan