Security zSecure CARLa-Driven Components
バージョン**2.2.1**

インストールおよびデプロイメント・ガイド

SA88-7162-03

Security zSecure CARLa-Driven Components
バージョン**2.2.1**

インストールおよびデプロイメント・ガイド

IBM

SA88-7162-03

注記

本書および本書で紹介する製品をご使用になる前に、 251 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 Security zSecure Admin (製品番号 5655-N16) のバージョン 2 リリース 2 モディフィケーション 1、IBM Security zSecure Audit (製品番号 5655-N17) のバージョン 2 リリース 2 モディフィケーション 1、IBM Security zSecure Visual (製品番号 5655-N20) のバージョン 2 リリース 2 モディフィケーション 1、IBM Security zSecure Alert (製品番号 5655-N21) のバージョン 2 リリース 2 モディフィケーション 1、IBM Security zSecure Adapters for QRadar SIEM (製品番号 5655-AD8) に適用されます。また、改訂版などで特に断りのない限り、これ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も適用されます。

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： SC27-5638-03
Security zSecure CARLa-Driven Components
Version 2.2.1
Installation and Deployment 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

目次

本書について

「*IBM Security zSecure CARLa-Driven Components* インストールおよびデプロイメント・ガイド」では、以下の IBM® Security zSecure™ コンポーネントのインストール・プロセスと構成プロセスについて説明します。

- IBM Security zSecure Admin
- IBM Security zSecure Audit for RACF®/ACF2/Top Secret
- IBM Security zSecure Alert for RACF/ACF2
- IBM Security zSecure Visual for RACF
- IBM Security zSecure Adapters for QRadar SIEM for RACF/ACF2/Top Secret

このマニュアルには、以下のタイプのインストールに関する情報が含まれています。

- 異なる構成を持つ複数の z/OS® イメージでの配布指向インストール。
- 同じ z/OS イメージから複数の構成を実行できる単一のインストール。

この資料は、zSecure 製品のインストールと保守の責任者、および各自のユーザー・コミュニティーに zSecure のコンポーネントをデプロイする責任者を対象としています。

読者は、インストールされる IBM Security zSecure 製品と、製品がインストールされているオペレーティング・システムに精通している必要があります。

エラー・メッセージ、その説明、および回避方法 (該当する場合) については、「*IBM Security zSecure:* メッセージ・ガイド」を参照してください。

zSecure 資料

IBM Security zSecure Suite ライブラリーおよび IBM Security zSecure Manager for RACF z/VM ライブラリーの資料には、非ライセンス出版物とライセンス出版物が含まれています。このセクションでは、両方のライブラリーと、それらへのアクセス手順をリストします。

zSecure の非ライセンス出版物は、IBM zSecure Suite または IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から入手できます。IBM Knowledge Center は、IBM 製品資料のホームです。IBM Knowledge Center をカスタマイズし、独自の資料の集合を作成して、使用するテクノロジー、製品、およびバージョンを表示するように画面を設計できます。トピックにコメントを追加したり、Eメール、LinkedIn、Twitter で話題を共有したりすることで、IBM や同僚と対話することもできます。ライセンス出版物の入手手順については、 viii ページの『ライセンス文書の入手』を参照してください。

製品の **IBM Knowledge Center**	**URL**
IBM zSecure Suite	http://www.ibm.com/support/knowledgecenter/SS2RWS/welcome
IBM zSecure Manager for RACF z/VM	http://www.ibm.com/support/knowledgecenter/SSQQGJ/welcome

IBM Terminology Web サイトに、製品ライブラリーの用語が 1 カ所にまとめられています。

ライセンス文書の入手

プログラム・ディレクトリーを除き、IBM Security zSecure Suite 2.2.1 および IBM Security zSecure Manager for RACF z/VM 1.11.2 のすべてのライセンス出版物および非ライセンス出版物は、*IBM Security zSecure Documentation CD*、*LCD7-5373* に含まれています。zSecure *Documentation CD* のディスク・イメージ (`.iso`) ファイルを直接ダウンロードする方法は、この製品資料に記載されています。

Documentation CD の `.iso` ファイルの追加コピー、または個々の資料の PDF ファイルを入手するには、以下のステップを実行します。

1. IBM Publications Center に移動します。
2. 国または地域を選択し、「**Go**」アイコンをクリックします。
3. 「**Publications** ホーム」ページで、左のナビゲーション・メニューの「フィードバック」をクリックします。
4. サポート・フォームに、連絡先の詳細、お客様番号、および注文するライセンス出版物の番号の情報を入力します。
5. 「送信する」をクリックしてフォームを送信します。フォームは、IBM Publications Center のお客様サポートに転送され、担当者からお客様のご注文を処理するための詳細が送信されます。

別の方法として、*zSecure Documentation CD* の `.iso` ファイルへのアクセスを要求する E メールを tivzos@us.ibm.com に送信することもできます。会社の IBM お客様番号と、ご希望の連絡先情報を合わせて記入してください。ご注文を処理するための詳細が送信されます。

IBM zSecure Suite ライブラリー

IBM Security zSecure Suite ライブラリーには、非ライセンス出版物とライセンス出版物が含まれています。

非ライセンス出版物は、IBM zSecure Suite の IBM Knowledge Center から入手できます。非ライセンス出版物は、クライアントのみが入手できます。ライセンス出版物の入手ライセンス出版物を入手については、ライセンス出版物の入手を参照してください。ライセンス出版物には、L で始まる資料番号 (LCD7-5373 など) があります。

IBM Security zSecure Suite ライブラリーには、次の資料があります。

- このリリースについて には、リリース固有の情報に加え、zSecure 固有ではない、より一般的な情報が含まれています。リリース固有の情報には、以下が含まれます。
  - *What's New*: zSecure V2.2.1 の新機能および機能拡張をリストします。
  - リリース・ノート: 各製品リリースのリリース・ノートで、IBM Security zSecure 製品の重要なインストール情報、非互換性の警告、制限事項、および既知の問題を提供しています。
  - 資料: zSecure Suite および zSecure Manager for RACF z/VM のライブラリーをリストして、簡潔に説明します。また、資料にはライセンス出版物を入手するための手順が含まれています。
- *IBM Security zSecure CARLa-Driven Components* インストールおよびデプロイメント・ガイド, SA88-7162

  次の IBM Security zSecure コンポーネントのインストールと構成に関する情報を記載しています。
  - IBM Security zSecure Admin
  - IBM Security zSecure Audit for RACF、CA-ACF2、および CA-Top Secret
  - IBM Security zSecure Alert for RACF and CA-ACF2
  - IBM Security zSecure Visual
  - IBM Security zSecure Adapters for QRadar SIEM for RACF、CA-ACF2、および CA-Top Secret
- *IBM Security zSecure Admin and Audit for RACF* スタートアップ・ガイド, GI88-4318

  IBM Security zSecure Admin および IBM Security zSecure Audit の製品機能、およびユーザーが標準的なタスクや手順を実行する方法を紹介する、実地のガイドが記載されています。このマニュアルは、新規ユーザーが基本的な IBM Security zSecure Admin and Audit for RACF システム機能の実用的な知識を身につけるとともに、使用可能な他の製品機能を調べる方法を理解するのに役立つことを目的としています。
- *IBM Security zSecure Admin and Audit for RACF* ユーザー・リファレンス・マニュアル, LA88-7161

  IBM Security zSecure Admin および IBM Security zSecure Audit の製品機能について説明しています。ユーザーが ISPF パネルから管理機能および監査機能を実行する方法が記載されています。このマニュアルには、トラブルシューティング・リソース、および zSecure Collect for z/OS コンポーネントのインストール手順も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。
- *IBM Security zSecure Admin and Audit for RACF* 行コマンドおよび基本コマンドの要約, SC27-6581

  簡略な説明とともに、行コマンドおよび基本 (ISPF) コマンドをリストしています。
- *IBM Security zSecure Audit for ACF2 Getting Started*, GI13-2325

zSecure Audit for CA-ACF2 の製品機能について説明し、ユーザーが標準的なタスクや手順 (ログオン ID、規則、グローバル・システム・オプションの分析など) を実行し、レポートを実行するための方法を記載しています。また、このマニュアルには、ACF2 用語に慣れていないユーザー向けに一般的な用語のリストも記載されています。

- *IBM Security zSecure Audit for ACF2 User Reference Manual*, LC27-5640

  メインフレーム・セキュリティーおよびモニタリングのために zSecure Audit for CA-ACF2 を使用する方法について説明しています。新しいユーザーのために、このガイドには、 CA-ACF2 の使用、および ISPF パネルからの機能のアクセスに関する概要と概念情報が記載されています。上級ユーザー向けに、このマニュアルには、詳細な参照情報、トラブルシューティングのヒント、zSecure Collect for z/OS の使用に関する情報、およびユーザー・インターフェースのセットアップに関する詳細情報が記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。

- *IBM Security zSecure Audit for Top Secret User Reference Manual*, LC27-5641

  zSecure Audit for CA-Top Secret の製品機能について説明し、ユーザーが標準的なタスクや手順を実行する方法を記載しています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。

- *IBM Security zSecure CARLa* コマンド・リファレンス, LC43-2107

  CARLa Auditing and Reporting Language (CARLa) についての、一般ユーザーと上級ユーザーの両方の参照情報が記載されています。CARLa は、zSecure を使用してセキュリティーの管理レポートおよび監査レポートを作成するためのプログラミング言語です。「*CARLa* コマンド・リファレンス」には、データの選択および zSecure レポートの作成のための NEWLIST タイプおよびフィールドに関する詳細情報も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。

- *IBM Security zSecure Alert* ユーザー・リファレンス・マニュアル, SA88-7156

  セキュリティー・サーバー (RACF) または CA-ACF2 で保護された z/OS システムのリアルタイム・モニターである IBM Security zSecure Alert の構成、使用、およびトラブルシューティングの方法を説明しています。

- *IBM Security zSecure Command Verifier* ユーザー・ガイド, SA88-7158

  RACF コマンドが入力されたときに RACF ポリシーを実施することによって、RACF メインフレーム・セキュリティーを保護するために IBM Security zSecure Command Verifier をインストールし、使用する方法を説明しています。

- *IBM Security zSecure CICS Toolkit* ユーザー・ガイド, SA88-7159

  CICS® 環境から RACF 管理機能を提供するために、IBM Security zSecure CICS Toolkit をインストールし、使用する方法を説明しています。

- *IBM Security zSecure* メッセージ・ガイド, SA88-7160

  すべての IBM Security zSecure コンポーネントのメッセージ解説を記載しています。このガイドは、各製品または機能に関連したメッセージ・タイプを記述し、すべての IBM Security zSecure 製品メッセージとエラーを、メッセージ・

タイプ別にソートされた重大度レベルと一緒にリストします。個々のメッセージに関する説明と追加のサポート情報も提供します。

- *IBM Security zSecure Visual* クライアント・マニュアル, SA88-7157

  Windows ベース GUI から RACF 管理用タスクを実行するために IBM Security zSecure Visual Client をセットアップし、使用する方法を説明しています。

- *IBM Security zSecure Documentation CD*, LCD7-5373

  IBM Security zSecure 資料を提供します。これには、ライセンス交付された製品資料とライセンス交付されていない製品資料が含まれています。「*Documentation CD*」はダウンロード可能な .iso ファイルとして使用できます。ライセンス出版物の入手を参照して、このファイルを取得してください。

プログラム・ディレクトリーはプロダクト・テープで提供されます。プログラム・ディレクトリーから最新のコピーをダウンロードすることもできます。

- プログラム・ディレクトリー*: IBM Security zSecure CARLa-Driven Components*、GI13-2277

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure CARLa-Driven Components (Admin、Audit、Visual、Alert および IBM Security zSecure Adapters for QRadar SIEM) のインストールに関連した資料と手順に関する情報が記載されています。

- プログラム・ディレクトリー*: IBM Security zSecure CICS Toolkit*、GI13-2282

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure CICS Toolkit のインストールに関連した資料と手順に関する情報が記載されています。

- プログラム・ディレクトリー*: IBM Security zSecure Command Verifier*、GI13-2284

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure Command Verifier のインストールに関連した資料と手順に関する情報が記載されています。

- プログラム・ディレクトリー*: IBM Security zSecure Admin RACF-Offline*、GI13-2278

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure Admin の IBM Security zSecure Admin RACF-Offline コンポーネントのインストールに関連した資料と手順に関する情報が記載されています。

- zSecure Administration、監査、およびコンプライアンスの各ソリューションのプログラム・ディレクトリー
  - 5655-N23: *Program Directory for IBM Security zSecure Administration*、GI13-2292

- 5655-N24: *Program Directory for IBM Security zSecure Compliance and Auditing*、GI13-2294
- 5655-N25: *Program Directory for IBM Security zSecure Compliance and Administration*、GI13-2296

IBM zSecure Manager for RACF z/VM ライブラリー

IBM Security zSecure Manager for RACF z/VM ライブラリーには、非ライセンス出版物とライセンス出版物が含まれています。

非ライセンス出版物は、IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から入手できます。ライセンス出版物には、L で始まる資料番号 (LCD7-5373 など) があります。

IBM Security zSecure Manager for RACF z/VM ライブラリーには、次の資料があります。

- *IBM Security zSecure Manager for RACF z/VM*リリース情報

  製品リリースごとに、「リリース情報」のトピックで、新機能と機能拡張、非互換性の警告、および資料の更新情報を提供します。最新バージョンのリリース情報は、zSecure for z/VM® 資料の Web サイト (IBM zSecure Manager for RACF z/VM の IBM Knowledge Center) から入手できます。
- *IBM Security zSecure Manager for RACF z/VM:* インストールおよびデプロイメント・ガイド*, SC27-4363*

  製品のインストール、構成、およびデプロイに関する情報を提供します。
- *IBM Security zSecure Manager for RACF z/VM* ユーザー・リファレンス・マニュアル、*LC27-4364*

  製品インターフェースと、RACF の管理および監査機能の使用方法を説明します。この資料には、CARLa コマンド言語および SELECT/LIST フィールドに関する参照情報が記載されています。また、トラブルシューティング・リソース、および zSecure Collect コンポーネントのインストール手順も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。
- *IBM Security zSecure CARLa* コマンド・リファレンス*,* LC43-2107

  CARLa Auditing and Reporting Language (CARLa) についての、一般ユーザーと上級ユーザーの両方の参照情報が記載されています。CARLa は、zSecure を使用してセキュリティーの管理レポートおよび監査レポートを作成するためのプログラミング言語です。「*zSecure CARLa* コマンド・リファレンス」には、データの選択および zSecure レポートの作成のための NEWLIST タイプおよびフィールドに関する詳細情報も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。
- *IBM Security zSecure Documentation CD*, LCD7-5373

  IBM Security zSecure Manager for RACF z/VM 資料を提供します。これには、ライセンス交付された製品資料とライセンス交付されていない製品資料が含まれています。
- *Program Directory for IBM zSecure Manager for RACF z/VM, GI11-7865*

この資料の情報を効果的に使用するには、プログラム・ディレクトリーから入手可能な一定の前提知識が必要です。「*Program Directory for IBM zSecure Manager for RACF z/VM*」は、この製品のインストール、構成、およびデプロイを担当するシステム・プログラマーを対象にしています。この資料には、ソフトウェアのインストールに関連する資料および手順についての情報が記載されています。プログラム・ディレクトリーは、プロダクト・テープで提供されます。IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から最新のコピーをダウンロードすることもできます。

関連資料

RACF 環境で IBM Security zSecure 製品を使用している場合には、いくつかの IBM マニュアルで RACF ユーザー情報および参照情報が説明されています。RACF コマンドおよび各種キーワードの影響については、「*RACF* コマンド言語解説書」および「*RACF* セキュリティー管理者のガイド」に説明されています。他の RACF 出口の記述方法については、「*RACF* システム・プログラマーのガイド」を参照してください。RACF の監査については、「*RACF* 監査担当者のガイド」に記載されています。これらの資料については、http://www.ibm.com/systems/z/os/zos/bkserv/ で使用可能な z/OS インターネット・ライブラリーからアクセスできます。

非互換性について詳しくは、IBM Security zSecure 資料の Web サイト (IBM Knowledge Center for IBM zSecure Suite) にある『このリリースについて』の『リリース・ノート』セクションを参照してください。

Identity Governance and Intelligence Adapter for zSecure RACF の実装方法については、*Identity Governance and Intelligence Adapter for zSecure RACF* を参照してください。

表 *1. RACF* 管理、監査、プログラミング、およびコマンドについての詳細情報

マニュアル	資料番号
z/OS Security Server RACF コマンド言語 解説書	SA88-6226
z/OS Security Server RACF セキュリティー管理者のガイド	SA88-5804
z/OS Security Server RACF 監査担当者のガイド	SA88-5718
z/OS Security Server RACF システム・プログラマーのガイド	SA88-7029
z/OS MVS プログラミング: 高水準言語向け呼び出し可能サービス	SA88-7103
z/OS MVS システム・コマンド	SA88-5490

アクセシビリティー

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。本製品では、支援機能を使用して、インターフェースを音声でナビゲートすることができます。また、マウスの代わりにキーボードを使用して、グラフィカル・ユーザー・インターフェースのすべての機能を操作できます。

技術研修

以下は英語のみの対応となります。技術研修の情報については、IBM Education Web サイト (http://www.ibm.com/training) を参照してください。

CARLa コマンド言語の基礎を理解するのに役立つハンズオン演習については、zSecure CARLa Training (https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Wa6857722838e_491e_9968_c8157c8cf491/page/zSecure%20CARLa%20Training) を参照してください。

サポート情報

IBM サポートは、コード関連の問題や、ルーチン、短期間でのインストール、または使用法に関する疑問をお持ちのお客様に、支援を提供します。IBM ソフトウェア・サポート・サイトへは、http://www.ibm.com/software/support/probsub.html から直接アクセスできます。

適切なセキュリティーの実践に関する注意事項

IT システム・セキュリティーには、企業内外からの不正アクセスからの保護、検出、および対処によってシステムおよび情報を保護することが求められます。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムおよび IT 製品は存在せず、また単一の製品、サービス、およびセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

第 1 章 インストール・ロードマップ

このトピックでのステップでは、IBM Security zSecure を新しくインストールして、それを構成およびデプロイするためのフレームワークについて説明します。

手順

1. 製品のインストール、構成、およびデプロイに関する重要な概念とリソースについて学習します。
   a. 単一のインストールと、配布指向インストールの概念について検討します。

      7 ページの『第 2 章 インストール、構成、およびデプロイメントの概要』を参照してください。
   b. CKRINST ライブラリーについて学習します。このライブラリーには、インストール・アクティビティーおよびポストインストール・アクティビティーをカスタマイズできるサンプル・ジョブが入っています。

      7 ページの『CKRINST ライブラリー』を参照してください。
   c. zSecure 構成データ・セットについて学習します。これを使用して、配布指向インストールをサポートすることができます。

      8 ページの『構成データ・セット』を参照してください。
2. インストールの準備をします。 9 ページの『第 3 章 インストールの準備タスク』を参照してください。
   a. リリースを確認します。

      リリースを確認しますを参照してください。
   b. zSecure データ・セットを命名して保護します。

      9 ページの『zSecure データ・セットの命名と保護』を参照してください。
   c. スペース所要量を評価します。

      10 ページの『スペース計画』を参照してください。
3. ソフトウェアをインストールします。以下のインストール方法のいずれかを使用します。
   - 正式インストール。

     「*Program Directory: IBM Security zSecure CARLa-Driven Components*」を参照してください。
   - 高速インストール。

     14 ページの『高速の方法を使用したインストール』を参照してください。
   - システム・パック、サーバー・パック、または CBPDO の一部としてのインストール。

15 ページの『システム・パック、サーバー・パック、または CBPDO によるインストール』を参照してください。

4. ユーザーが開始できるようにソフトウェアを使用可能な状態にします。

   概要情報は 23 ページの『第 5 章 製品の活動化と構成データ・セットのカスタマイズ』を参照してください。

   a. インストール先のデータ・セット以外のデータ・セットから zSecure を実行しようとする場合は、 zSecure データ・セットを配布します。

      23 ページの『z/OS 追加イメージへの zSecure データ・セットの配布』を参照してください。

   b. ライセンスを使用可能にします。

      24 ページの『ライセンス機能の使用可能化』を参照してください。

   c. ソフトウェアを APF 許可します。

      24 ページの『ソフトウェアの APF 許可』を参照してください。

   d. zSecure ソフトウェアを TSO/ISPF ユーザーが使用できるようにします。

      27 ページの『ソフトウェアの使用可能化 (TSO/ISPF ユーザー)』を参照してください。

   e. ソフトウェアをバッチで、または開始タスクとして実行できるようにします。

      28 ページの『ソフトウェアの使用可能化 (バッチ処理用)』を参照してください。

5. 構成ファイルを使用して、ソフトウェアをデプロイします。概要情報は 31 ページの『第 6 章 ソフトウェアのデプロイメント』を参照してください。

   a. zSecure 構成データ・セットについてさらに学習します。

      31 ページの『zSecure 構成データ・セットについて』を参照してください。

   b. zSecure 構成データ・セットを作成します。

      34 ページの『zSecure 構成 データ・セットの作成』を参照してください。

   c. zSecure 構成データ・セットをカスタマイズします。

      35 ページの『zSecure 構成 データ・セットのカスタマイズ』を参照してください。

   d. (オプション) アップグレード中の場合は、 36 ページの『既存の zSecure 構成 データ・セットの保守』を参照してください。

   e. zSecure 構成データ・セットを使用可能にし、構成ごとにセキュリティーを確立します。

      1) 構成を、適切な TSO/ISPF ユーザーに割り当てます。

         36 ページの『TSO/ISPF ユーザーへの構成の割り当て』を参照してください。

2) 構成を、適切なバッチ・ジョブおよび開始タスクに割り当てます。

37 ページの『バッチ・ジョブおよび開始タスクへの構成の割り当て』を参照してください。

3) 構成ごとにセキュリティーを確立して、製品機能とデータへのアクセスを制御します。

207 ページの『付録 B. zSecure のセキュリティー・セットアップ』を参照してください。

6. インストールを検査します。
   a. 基本の ISPF インターフェース機能およびメニュー構成を確認します。

39 ページの『基本の ISPF インターフェース機能およびメニュー構成』を参照してください。

   b. zSecure Collect 機能および zSecure の基本バッチ操作を確認します。

39 ページの『zSecure Collect 機能および zSecure の基本バッチ操作の確認』を参照してください。

   c. レポートを表示します。

39 ページの『レポートを表示する機能』を参照してください。

   d. CKGRACF を確認します。(zSecure Admin または zSecure Visual を使用しない場合、このステップはオプションです。)

39 ページの『セキュリティー・リソースを検査するための CKGRACF コマンド』を参照してください。

   e. ACF2 レポート作成を検査します。(zSecure Audit for ACF2 をインストールしていない場合、このステップはオプションです。)

40 ページの『ACF2 レポート作成の検査』を参照してください。

7. 必要なら実動のために、以下の項目をセットアップします。
   a. キャパシティー・プランニング情報を参照して、必要なシステム・リソースを特定してください。

41 ページの『キャパシティー・プランニング情報』を参照してください。

   b. デフォルトの入力セットを指定します。

41 ページの『第 8 章 実動のためのセットアップ』を参照してください。

   c. 夏時間調整に合わせてインストールをカスタマイズをします。

55 ページの『夏時間調整に関する考慮事項』を参照してください。

   d. CKFREEZE ファイルをリフレッシュします。

55 ページの『フレッシュな CKFREEZE および UNLOAD の毎日の使用』を参照してください。

   e. RACF Exit Activator をセットアップします。

56 ページの『RACF Exit Activator のセットアップ』を参照してください。

f. 独自のバージョンの新規パスワード出口をセットアップします。

57 ページの『zSecure の新規パスワード出口を他の新規パスワード出口と一緒に使用する』を参照してください。

g. TCP/IP ドメイン・ネームを解決できることを確認します。

57 ページの『TCP/IP ドメイン・ネームの解決』を参照してください。

h. SMTP サーバーの設定を確認します。

58 ページの『SMTP サーバーに関する考慮事項』を参照してください。

8. プロファイル、リソース、および設定を複数のシステムから管理および監査しようとする場合は、多重システム・サポートをセットアップします。

59 ページの『第 9 章 リモート・データ・アクセスおよびコマンド・ルーティングのためのセットアップ』を参照してください。

a. zSecure Server をインストール、構成、および活動化します。

59 ページの『zSecure Server のインストールおよび構成』を参照してください。

b. CKRCARLA または ISPF ユーザー・インターフェースで使用するためのリモート・データ・セットを指定します。

67 ページの『zSecure Server のオペレーター・コマンド』を参照してください。

c. RACF コマンドおよび選択された非 RACF コマンドを他のシステムにルーティングするためのセットアップを実行します。

68 ページの『AT-TLS を使用したセキュアなコミュニケーション』を参照してください。

9. 以下のコンポーネントをセットアップします。
   - zSecure Admin アクセス・モニター。

     75 ページの『第 10 章 zSecure Admin アクセス・モニターのセットアップ』を参照してください。
   - RACF-Offline.

     99 ページの『第 11 章 RACF-Offline のセットアップ』を参照してください。
   - zSecure Alert.

     107 ページの『第 12 章 zSecure Alert のセットアップ』を参照してください。
   - zSecure Visual Server。

     141 ページの『第 13 章 zSecure Visual Server のセットアップおよび使用』を参照してください。
   - トラッキングを変更します。

179 ページの『第 14 章 変更トラッキングのセットアップ』を参照してください。

- QRadar® SIEM 用データの準備。

  185 ページの『第 15 章 QRadar SIEM 用データの準備』を参照してください。

- Guardium Vulnerability Assessment 用にデータを準備する。

  199 ページの『第 16 章 Guardium Vulnerability Assessment 用にデータを準備する』を参照してください。

第 2 章 インストール、構成、およびデプロイメントの概要

zSecure は、ソフトウェアのインストールと製品のセットアップのためのサンプル・ジョブを提供します。インストール、構成、およびデプロイメントのプロセス中に、これらのジョブへのアクセスが必要になります。これらのジョブについて詳しくは、『CKRINST ライブラリー』を参照してください。

配布指向インストール

zSecure のインストール、構成、およびデプロイメントのプロセスは、単一インストールと配布指向インストールの両方をサポートします。

- 単一インストールでは、zSecure を各 z/OS イメージに別々にインストールします。
- 配布指向インストールでは、製品を 1 つの z/OS イメージにインストールし、次にさまざまな構成ファイルを使用して複数のイメージ上で実行します。また、複数の構成を単一の z/OS イメージ上で実行することもできます。例えば、以下の構成を希望する場合があります。
  - 中央管理者用の全機能 構成
  - 共通のユーザー管理タスクのみ実行し、「Quick Administration」メニュー (オプション RA.Q) へのアクセスのみ必要とする担当者用の簡素化された 構成

構成ファイルについて詳しくは、 8 ページの『構成データ・セット』を参照してください。

注**:** RACF 管理および監査タスクを z/VM システムと z/OS システムの両方で実行する場合には、各オペレーティング・システムに対して zSecure を別々にインストールする必要があります。z/VM バージョンの製品のインストールについて詳しくは、「*IBM Security zSecure Manager for RACF z/VM: Manager for RACF z/VM Installation and Deployment Guide*」を参照してください。

CKRINST ライブラリー

これらのサンプル・ジョブを使用して、ご使用のデータ・セットの命名規則、JOB ステートメント要件、およびその他の項目のインストール・パラメーターをカスタマイズできます。また、これらのパラメーターは、製品のインストール後に実行されるポストインストール・アクティビティーやその他のアクティビティーで使用されます。これらのパラメーターのカスタマイズはオプションです。しかし、ソフトウェアをインストールする前、またはポストインストール・アクティビティーを実行する前にカスタマイズする場合には、処理依頼する前に個々のジョブを編集するのではなく、サンプル・ジョブのパラメーター値を一度に更新するため、時間が節約されます。

CKRINST ライブラリーは、プロダクト・テープからサンプル・ジョブをコピーすることにより、または製品でインストールされた SCKRSAMP ライブラリーをコピ

ーすることにより作成されます。CKRINST ライブラリーを作成する指示は、インストールの説明で提供されています。 13 ページの『第 4 章 ソフトウェアのインストール』を参照してください。

構成データ・セット

このデータ・セットは、あるイメージの zSecure 構成を表し、そのイメージ上でソフトウェアがどのように作動するかを決定します。例えば、zSecure 構成 データ・セットは、どの zSecure フィーチャーが使用可能であるかと、入力データ・ソースのデータ・セット名を指定できます。

zSecure 構成データ・セットは、イメージ間で異なる唯一のデータ・セットです。これらのデータ・セットを使用して、以下の目的で構成を作成できます。

- zSecure Alert、アクセス・モニター、および Visual Server などのプロセスに対する特殊な目的の構成。
- 異なる z/OS イメージに zSecure をデプロイするための個別構成。
- 異なる入力データを必要とするユーザー・グループ、または特定の zSecure コンポーネントに対するアクセスを制限するユーザー・グループに対する構成。

zSecure 構成データ・セットは、インストール済みソフトウェアの一部でない区分データ・セットに保管されます。その結果、これらのデータ・セットは、ソフトウェアがアップグレードまたは再インストールされるときに更新されません。したがって、アップグレードの前後でカスタム構成設定を維持することができます。

zSecure は、ご使用の環境用にコピーおよび更新できるデフォルトの構成データ・セットを提供します。構成データ・セットの作成とカスタマイズの情報と指示について詳しくは、 31 ページの『第 6 章 ソフトウェアのデプロイメント』を参照してください。

第 3 章 インストールの準備タスク

- 『リリースの確認』
- 『zSecure データ・セットの命名と保護』
- 10 ページの『スペース計画』

リリースの確認

ソフトウェアをインストールする前に、以下を行います。

- インストールしようとしている製品およびリリースが最新のサポート対象リリースであることを確認します。
- 製品を使用するつもりのプラットフォーム上でその製品がサポートされていることを確認します。

http://www.ibm.com/software/support/lifecycle/ を参照してください。 (zSecure で検索してください。)

また、最新の製品更新およびすべての非互換性警告については、IBM Knowledge Center の zSecure Suite に掲載のリリース情報を確認してください。

zSecure データ・セットの命名と保護

1. データ・セット命名規則を決定します。
2. 製品データ・セットのセキュリティーを計画します。
3. (オプション) データ・セットにユーザー・カタログを指定します。

デフォルトおよびサイト固有のデータ・セット命名規則

zSecure には、zSecure がインストールされるデータ・セットにデフォルトの命名規則が用意されています。

デフォルトの命名体系では、例えば、データ・セット名 CKR.SCKRLOAD のように 2 つの修飾子を使用します。

CKR すべての zSecure 製品データ・セットに共通の接頭部。この接頭部は、独自に選択した 1 つ以上の修飾子で置換できます。

dddef 最後の修飾子は、SMP/E (SMP/E DDDEF) によって使用される DD 名定義と等しく、ターゲット・ライブラリーおよび配布ライブラリーの名前における低位修飾子です。それぞれの DDDEF は、S (ターゲット・ライブラリーの場合) または A (配布ライブラリーの場合) で始まり、後に製品接頭部が続きます。ターゲット・ライブラリーおよび配布ライブラリーの DDNAME のリストについては、「*Program Directory: IBM Security zSecure CARLa-Driven Components*」を参照してください。

インストール中に、独自の命名規則を指定して、これらのデフォルトを指定変更したい場合があります。接頭部 CKR は、異なる 1 つの修飾子または複数の修飾子に変更できます。例えば、zSecure を以降の配布のためにデッド・システムにインス

トールする場合は、接頭部 CKR を DEADSYS.CKR または DEADSYS.CKR.CKRvrm で置換できます。このようにして、DEADSYS.CKR.SCKRLOAD または DEADSYS.CKR.CKRvrm.SCKRLOAD などのデータ・セットを作成することができます。異なる名前をインストール時に使用すると、デフォルトの名前を使用して、アクティブ・システム・イメージへの配布を行うことができます。異なる名前をインストール時に使用することは、新規リリースをインストールまたはテストするときの名前の競合を避けるのにも役立ちます。データ・セット命名規則のカスタマイズの説明については、17 ページの『インストール・パラメーターのカスタマイズ』を参照してください。

zSecure インストール・データ・セットのためのセキュリティーのセットアップ

配布用にインストールする場合は、その製品をインストールまたは保守する人のみがアクセスするように zSecure データ・セットを保護します。

- システム保守を担当するユーザーに UPDATE アクセス権限を与えます。
- インストールまたはスペース管理を担当するユーザーに ALTER アクセス権限を与えます。

zSecure がインストール済みデータ・セットから直接実行される場合は、zSecure ユーザーに READ 権限を与えます。他のユーザーにはアクセス権限を与えないでください。

ユーザー・カタログ内への zSecure データ・セットのカタログ (オプション)

複数の z/OS イメージからの zSecure ソフトウェアへのアクセスが簡単になるように、ユーザー・カタログ内に zSecure データ・セットをカタログします。既存のユーザー・カタログを使用することも、新規のユーザー・カタログを作成することもできます。このようにして、そのユーザー・カタログへの別名を追加することにより、複数の z/OS イメージからソフトウェアに簡単にアクセスできます。そのユーザー・カタログへの別名を作成する TSO コマンドは、以下のとおりです。

```
DEFINE ALIAS (NAME('your-high-level-qualifier') REL('your-user-catalog'))
```

別名が定義されていなければ、インストール・ジョブはエラーなしでの実行が可能です。ただし、すべてのデータ・セットが、インストール・ジョブを実行する z/OS イメージのマスター・カタログにカタログされます。

スペース計画

プログラミング要件とスペース所要量については、以下の zSecure プログラム・ディレクトリーを参照してください。

- zSecure Admin RACF-Offline コンポーネントには、独自のプログラム・ディレクトリー「*Program Directory: IBM Security zSecure Admin RACF-Offline*」があります。
- zSecure のその他のすべての CARLa 駆動コンポーネントには、共通のプログラム・ディレクトリー「*Program Directory: IBM Security zSecure CARLa-Driven Components*」があります。

これらのプログラム・ディレクトリーは製品で提供されています。また、IBM Security zSecure Knowledge Center でオンラインで入手できます。http://www.ibm.com/support/knowledgecenter/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.1/welcome.htmlを参照してください。

Common Data Provider for z Systems (CDP) については、IBM Knowledge Center の IBM Common Data Provider for z Systems に掲載の Planning for installation and configuration of Common Data Provider for z Systems を参照してください。

第 4 章 ソフトウェアのインストール

zSecure ソフトウェアは、以下の方法のいずれかを使用してインストールできます。

- 正式インストール。

  正式インストールを使用する場合、以下のようになります。

  – SMP/E の RECEIVE、APPLY、および ACCEPT ジョブを完全に制御します。
  – zSecure を既存のグローバル・ゾーンおよび製品ゾーンにインストールできます。

  正式インストールの場合、「*Program Directory: IBM Security zSecure CARLa-Driven Components*」に示されている指示に従います。
- 高速インストール。

  この方法は、SMP/E の RECEIVE、APPLY、および ACCEPT ジョブを別々に実行するのではなく、ほとんどのインストール・プロセスを単一のジョブ CKRZINST で実行します。高速インストールでは、製品は新規のグローバル・ゾーンおよび製品ゾーンにインストールされます。

  注: 高速インストール方法では、Security zSecure Admin RACF-Offline のインストールはサポートされていません。RACF-Offline 機能を使用するつもりの場合は、正式インストール方法を使用してください。RACF-Offline のインストールについては、 99 ページの『第 11 章 RACF-Offline のセットアップ』を参照してください。
- システム・パック、サーバー・パック、または **CBPDO** の一部としてのインストール。

  システム・パック、サーバー・パック、または CBPDO を使用して zSecure をインストールする場合は、パッケージに付属の説明に従ってください。「*Program Directory: IBM Security zSecure CARLa-Driven Components*」の指示は使用しないでください。 zSecure のインストール後は、ポストインストール・アクティビティーを実行するためにインストール・ライブラリーのコピーが必要です。

インストールの方法については、以下の情報を参照してください。

- 正式インストールについては、「*Program Directory: IBM Security zSecure CARLa-Driven Components*」を参照してください。
- 高速インストールについては、 14 ページの『高速の方法を使用したインストール』を参照してください。
- システム・パック、サーバー・パック、または CBPDO の一部としてのインストールについては、 15 ページの『システム・パック、サーバー・パック、または CBPDO によるインストール』を参照してください。

高速の方法を使用したインストール

高速インストール方法では、zSecure は新規のグローバル・ゾーンおよび製品ゾーンにインストールされます。単一のジョブから RECEIVE、ACCEPT、および APPLY のステップを実行します。インストールは、単一のインストール・メディアからも、いくつかのタイプのインストール・メディアからも行えます。

この方法は、CKRINST ライブラリーにある zSecure 提供インストール・ジョブを使用して、インストール・パラメーターのカスタマイズとソフトウェアのインストールを行います。これらのジョブは、ポストインストール・タスクの実行にも使用されます。これらのジョブを入手する方法は、以下の手順に含まれています。

- 『単一のインストール・メディアからのインストール』
- 『複数のインストール・メディアからのインストール』

単一のインストール・メディアからのインストール

手順

1. CKRINST インストール・ライブラリーのコピーを作成します。 16 ページの『zSecure 提供インストール・ジョブ』を参照してください。
2. CKRINST ライブラリーのインストール・パラメーターをカスタマイズします。 17 ページの『インストール・パラメーターのカスタマイズ』を参照してください。
3. DASD からのインストールの場合は、資料「*Supplemental Installation Instructions for Performing an SMP/E Installation from DASD*」(IBM ソフトウェア・サポートから入手できます) に説明されているように、RECEIVE ステップの SMPPTFIN DD ステートメントを調整します。
4. ステップ 1 で作成した CKRINST インストール・ライブラリーにある CKRZINST ジョブを実行します。

複数のインストール・メディアからのインストール

このタスクについて

それぞれが 1 つの製品を含む、複数のインストール・ソース・メディアを受け取った場合は、それぞれのソース・メディアを別々のライブラリーにインストールするのではなく、ソース・メディアを結合して、製品を共有ライブラリーにインストールできるようにします。

手順

1. いずれかのテープ (またはダウンロード・ファイル) を使用して、CKRINST ライブラリーを作成してカスタマイズします。 16 ページの『zSecure 提供インストール・ジョブ』を参照してください。
2. CKRINST ライブラリーのインストール・パラメーターをカスタマイズします。 17 ページの『インストール・パラメーターのカスタマイズ』を参照してください。
3. CKRINST ライブラリーからジョブ CKRZINST を RECEIVE ジョブ・ステップまで実行します。

4. 他のすべてのテープを RECEIVE するか、ステップ 3 (14 ページ) でジョブ CKRZINST が作成した SMP/E ゾーンでダウンロード・ファイルを受信します。

   システムから出された**既に受信済み**のメッセージがあれば、それらは無視できます。
5. すべてを受け取った後で、`RESTART=ALLOCT` を JOB ステートメントに指定してジョブの再実行依頼を行うことにより、ジョブ CKRZINST の残りを実行します。

システム・パック、サーバー・パック、または CBPDO によるインストール

このタスクについて

システム・パック、サーバー・パック、または CBPDO を使用して zSecure をインストールする場合は、選択したパッケージに付属の説明に従ってください。「*Program Directory: IBM Security zSecure CARLa-Driven Components*」の指示は使用しないでください。

zSecure 提供サンプル・ジョブのコピーもポストインストール・アクティビティー用に必要です。これらのジョブは、製品と一緒にインストールされる SCKRSAMP ライブラリーにあります。これらのジョブをコピーする方法は、以下の手順を参照してください。

zSecure をシステム・パック、サーバー・パック、または CBPDO からインストールするには、以下の操作を行います。

手順

1. ソフトウェアをインストールするには、パッケージに付属の説明に従います。

   DASD からのインストールの場合は、RECEIVE ステップの SMPPTFIN DD ステートメントを調整します。その方法については、「*Supplemental Installation Instructions for Performing an SMP/E Installation from DASD*」(IBM ソフトウェア・サポートから入手できます) を参照してください。

   注**:** 複数の zSecure コンポーネントを別個のパッケージで (例えば、zSecure Admin と zSecure Visual をそれぞれ別々の CBPDO で) 受け取った場合は、以下のステップを実行し、ソースを結合して製品をインストールします。
   a. インストール・ジョブを RECEIVE ジョブ・ステップまで実行します。
   b. 他のすべてのテープを RECEIVE するか、またはインストール・ジョブが作成した SMP/E ゾーンにファイルをダウンロードします。

      システムから出された**既に受信済み**のメッセージがあれば、それらは無視できます。
   c. すべてを受け取った後で、`RESTART=ALLOCT` を JOB ステートメントに指定してジョブの再実行依頼を行うことにより、インストール・ジョブの残りを実行します。

2. 製品と一緒にインストールされた SCKRSAMP ライブラリーを新規データ・セットにコピーすることにより、zSecure 提供サンプル・ジョブのコピーを入手します。データ・セット名には、デフォルトの低位修飾子 CKRINST を使用します。
3. ポストインストール・アクティビティーに使用されるインストール・パラメーターをカスタマイズします。 17 ページの『インストール・パラメーターのカスタマイズ』を参照してください。

zSecure 提供インストール・ジョブ

正式インストールと高速インストールは両方の方法とも、zSecure 提供インストール・ジョブを使用します。これらのジョブは、ソフトウェアのインストールとセットアップに役立つように提供されています。これらのジョブは、ご使用のデータ・セットの命名規則、JOB ステートメント要件、および他の項目を指定するためにカスタマイズすることができます。サンプル・インストール・ジョブは以下の方法のいずれかで入手できます。

- テープから直接。
- SMP/E RECEIVE を実行した後で、編集および実行依頼のためにジョブを IBM.HCKR221.F1 から作業データ・セットにコピーすることによって。

以下のジョブは、両方の方法の JCL を提供します。このジョブのサンプルは http://www.ibm.com/support/knowledgecenter/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.1/landing/samples.html からダウンロードできます。

図 *1. zSecure* 提供インストール・ジョブを入手するためのサンプル *JCL*

```
//STEP1 EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//* //TAPEIN DD DSN=IBM.HCKR221.F1,UNIT=tunit,
//* //          VOL=SER=volser,LABEL=(x,SL),
//* //          DISP=(OLD,KEEP)
//* //FILEIN DD DSN=IBM.HCKR221.F1,UNIT=SYSALLDA,DISP=SHR
//OUT    DD DSNAME=your-prefix.CKRINST,
//          DISP=(NEW,CATLG,DELETE),
//          VOL=SER=dasdvol,UNIT=SYSALLDA,
//          SPACE=(TRK,(30,5,15))
//SYSUT3 DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSIN DD *
  COPY INDD=xxxxIN,OUTDD=OUT
```

このジョブを実行依頼する前に、インストール要件に基づいて以下の更新を行います。

- 配布メディアに応じて、//TAPEIN または //FILEIN DD ステートメントのいずれかをアンコメントして、他方のステートメントを削除します。次に、SYSIN DD ステートメントで、いずれのステートメントを指定したかに応じて、INDD パラメーターの値を xxxxIN から TAPEIN または FILEIN に変更します。
- ジョブ・カードを追加して、実行依頼の前に要件を満たすために小文字のパラメーターを大文字の値に変更します。

- OUT DSNAME には、出力データ・セットの高位修飾子を指定します。デフォルトの低位修飾子は CKRINST です。それは zSecure の資料全体を通して、このデータ・セットを指すために使用される名前なので、デフォルト修飾子を保持することをお勧めします。

インストール・パラメーターのカスタマイズ

グローバル更新プロセスは、高速インストール・ジョブ CKRZINST および正式インストール・ジョブ CKRZREC、CKRZAPP、および CKRZACC などの CKRINST メンバーで使用されるパラメーターの値を更新します。インストール・パラメーターはポストインストール・ジョブ CKRZPOST および後のジョブによっても使用されます。ソフトウェアをインストールする前、またはポストインストール・アクティビティーを実行する前にパラメーターをカスタマイズすると、ライブラリー内の個別のメンバーを編集するのではなく、CKRINST メンバーにまたがってパラメーター値を更新できるので時間の節約になります。表 2 に、インストール・パラメーターのカスタマイズと更新に必要な CKRINST メンバーのリストを示します。

表 2. *CKRINST* ライブラリー・メンバー: インストール・パラメーターをカスタマイズおよび更新するためのインストール・ジョブ

CKRINST メンバー	説明
CKRZUPDI	このメンバーは、正式インストール・ジョブと高速インストール・ジョブおよびポストインストール・ジョブ CKRZPOST で使用されるインストール・パラメーターの値を指定します。これらには、どの zSecure コンポーネントをインストールするかのほか、zSecure ソフトウェアのデータ・セット命名規則、および構成データ・セットを決定するパラメーターが含まれます。このジョブを編集して、インストール用のこれらのパラメーター値をカスタマイズします。
C2RIISPF	このメンバーは、 CKRINST ライブラリーの更新やトラック変更機能の使用などのタスクに zSecure が必要とする ISPF コンポーネントのロケーションを指定します。このジョブは、グローバル更新ジョブ CKRZUPDZ を実行する前に編集してください。
CKRZUPDZ	この更新ジョブは、CKRINST ライブラリーのグローバル更新を実行します。このジョブを実行して、CKRZUPDI メンバーで行った変更を適用します。

以下の手順は、インストール・パラメーターをカスタマイズして CKRINST のインストール・ジョブを更新するために使用します。

- 18 ページの『CKRZUPDI メンバーでのインストール・パラメーターの更新』
- 20 ページの『C2RIISPF での ISPF コンポーネントのロケーションの指定』
- 21 ページの『CKRZUPDZ の実行による CKRINST ライブラリー・メンバーの更新』

CKRZUPDI メンバーでのインストール・パラメーターの更新

このタスクについて

zSecure ジョブのジョブ・カード、インストール・パラメーター、および JCL は、CKRINST ライブラリーで提供される CKRZUPDI メンバーから更新できます。

```
//******* Jobcard updates ************************************
Jobcard1=//JOBNAME  JOB ACCT,ZSECURE,MSGCLASS=A,TIME=60,USER=,
Jobcard2=//         NOTIFY=&&SYSUID
Jobcard3=//*JOB3
//******* JCL updates ****************************************
TapeUnit                          = 3480
PrefixForTargetLibraries          = CKR
VolumeForTargetLibraries          =
PrefixForDistributionLibraries    = CKR.DLIB
VolumeForDistributionLibraries    =
JclLib                            = Yes
SmpeTargetZone                    = CKR221T
SmpeDistributionZone              = CKR221D
PrefixForSmpeGlobalZone           = CKR.SMPE.G
PrefixForSmpeOtherData            = CKR.SMPE
SmpeCsiAndSmptlibVolume           = SMS001
//******* Products/features to install *********************************
AdminRACF                         = No
AuditRACF                         = No
AuditACF2                         = No
AuditTopSecret                    = No
AlertRACF                         = No
AlertACF2                         = No
VisualRACF                        = No
QRadarAdaptersRACF                = No
QRadarAdaptersACF2                = No
QRadarAdaptersTopSecret           = No
```

図 2. *CKRZUPDI* メンバーおよび *JCL* 更新

以下のステップを実行して、インストールに必要な値でインストール・パラメーターを変更します。いずれのパラメーターにも大/小文字の区別がありません。

手順

1. すべてのインストール・ジョブに追加されるジョブ・パラメーターを変更します。

   ```
   Jobcard1=//JOBNAME  JOB ACCT,ZSECURE,MSGCLASS=A,TIME=10,USER=,
   Jobcard2=//         NOTIFY=&&SYSUID
   Jobcard3=//*JOB3
   ```

2. テープ装置に非公式装置名または総称装置名を指定します。

   DASD からのインストールの場合は、このパラメーターを現状のまま残します。代わりに、 16 ページの『zSecure 提供インストール・ジョブ』に説明されているように、ジョブ CKRZINST を調整します。

   ```
   TapeUnit                          = 3480
   ```

3. Security zSecure がインストールされるデータ・セットに高位修飾子を指定します。配布したい場合は、この接頭部を他の接頭部とは異なるものにして、PrefixForTargetDatasets を使用して配布の資格を有するデータ・セットを簡単に選択できるようにします。

   ```
   PrefixForTargetLibraries          = CKR
   ```

4. IBM Security zSecure ターゲット・ライブラリーのボリューム通し番号を設定します。このパラメーターをブランクのままにした場合、システムはボリュームを選択します。

   ```
   VolumeForTargetLibraries
   ```

5. IBM Security zSecure 配布ライブラリーに高位修飾子を指定します。

   ```
   PrefixForDistributionLibraries    = CKR.DLIB
   ```

6. IBM Security zSecure 配布ライブラリーのボリューム通し番号を設定します。このパラメーターをブランクのままにした場合、システムはボリュームを選択します。

   ```
   VolumeForDistributionLibraries    =
   ```

7. JCLLIB ステートメント・パラメーターを使用可能にします。

   ```
   JclLib                            = Yes
   ```

   このパラメーターを Yes に設定した場合、SCKRPROC データ・セットの JCLLIB ステートメントは CKRJOBS データ・セットのジョブに組み込まれます。 CKRJOBS データ・セットはカスタマイズ・ジョブ CKRZPOST の途中で作成されます。

   SCKRPROC データ・セットと、JES のプロシージャー・ライブラリー連結に構成メンバーが入っているデータ・セットを含めるつもりの場合、JCLLIB は必要なく、No を指定できます。

8. 必要な場合は、SMP/E ターゲットと Dlib の ゾーンに名前を指定します。通常は、デフォルト値を変更する必要はありません。

   ```
   SmpeTargetZone                    = CKR221T
   SmpeDistributionZone              = CKR221D
   ```

9. 必要な場合は、高位修飾子のデフォルト値を SMP/E 関連データ・セット用に変更します。通常は、これらの値を変更する必要はありません。

   ```
   PrefixForSmpeGlobalZone           = CKR.SMPE.G
   PrefixForSmpeOtherData            = CKR.SMPE
   ```

10. SMP/E CSI データ・セットと SMPTLIB のボリューム通し番号を指定します。 このパラメーターは、既存の SMP/E ゾーンにインストールする場合は無視されます。新規ゾーンを使用する場合、このパラメーターは SMP/E と IDCAMS で必要なため必須です。SMS 構成に応じて、指定する値は使用されることも使用されないこともあります。

    ```
    SmpeCsiAndSmptlibVolume           = SMS001
    ```

11. インストールする製品またはフィーチャーを選択します。ある製品またはフィーチャーをインストールするには、対応するそのパラメーターの値を Yes に変更します。

    ```
    AdminRACF                         = No
    AuditRACF                         = No
    AuditACF2                         = No
    AuditTopSecret                    = No
    AlertRACF                         = No
    AlertACF2                         = No
    VisualRACF                        = No
    QRadarAdaptersRACF                = No
    QRadarAdaptersACF2                = No
    QRadarAdaptersTopSecret           = No
    ```

C2RIISPF での ISPF コンポーネントのロケーションの指定

このタスクについて

CKRINST ライブラリーのインストール・パラメーターを更新するプロセスには、テーブルおよびメッセージなどの ISPF サービスが必要です。zSecure では、ISPF コンポーネントのロケーションは、インストール・メンバー C2RIISPF で定義されます。以下のデフォルトの ISPF データ・セット名は C2RIISPF に含まれています。

```
ISPMLIB ISP.SISPMENU
ISPSLIB ISP.SISPSENU
ISPPLIB ISP.SISPPENU
ISPTLIB ISP.SISPTENU
```

これらのデフォルト値は、データ・センターで使用される ISPF データ・セット名を指定するために編集します。以下のガイドラインは、これらのデータ・セット名に共通する変形パターンの説明です。

- 各データ・セットの高位修飾子は、SYS1 の代わりに ISP にすることができます。
- 一部のインストールでは、その ISPF 製品のレベルを識別する中位修飾子 (例えば、V5R2M0) が使用されます。
- 一部の ISPF データ・セットの低位修飾子は、各国語を反映することがよくあります。例えば、パネル・ライブラリーは低位修飾子 SISPPENU を (アメリカ) 英語に対して持つ場合があります。

手順

インストール用の ISPF データ・セット名を更新するには、以下の操作を行います。

1. システムで現在使用中の ISPF コンポーネントを確認して、ISPF コマンド行から次のコマンドを実行します。

   ```
   TSO ISRDDN
   ```

2. 基本 ISPF 製品 (ISPF を利用する他の製品、例えば SDSF、または TSO セッションに割り振られることがあるローカル・ソフトウェアとは対照的) を含むデータ・セットを識別します。 これらのデータ・セットは、以下のメンバーが存在することによって認識することができます。
   - ISPTLIB の場合: ISPCMDS、ISPPROF、ISPSPROF、および ISRKEYS
   - ISPMLIB の場合: ISPP00、ISPP02、ISPP10、ISPP20、ISPP32、ISPV01、ISRD23、ISRE00、ISRE64、ISRE65、ISRE70、および ISRLS12
3. インストール・メンバー C2RIISPF は、データ・センターで使用される ISPF データ・セット名を更新するために編集します。基本 ISPF 製品のみ必要です。ISPLOAD および ISPLPA データ・セットがそれぞれリンク・リストおよび LPA リストに存在する場合は、それらを含める必要はありません。存在しない場合は、C2RIISPF の DD ステートメント STEPLIB および ISPLLIB をアンコメントして調整します。

エンキューの競合を避けるには、他のいずれのデータ・セットも C2RIISPF に指定しないでください。特に、永続 ISPF プロファイル・データ・セットは割り振らないでください。

CKRZUPDZ の実行による CKRINST ライブラリー・メンバーの更新

このタスクについて

メンバー CKRZUPDZI のインストール・パラメーターと C2RIISPF の ISPF データ・セット名を更新した後で、検討を行ってジョブ CKRZUPDZ を実行し、インストール・メンバーのグローバル更新を実行します。

手順

1. CKRZUPDZ をチェック・モードで実行します。

   以下のいずれかのタイプのエラーが発生した場合、それらを修正します。

   - C2R8*xxxx* メッセージ。「*IBM Security zSecure:* メッセージ・ガイド」に、これらのメッセージの説明があります。
   - `RC=990; ISPP100 Panel 'C2RPUPDP' error -/-Panel not found`

     このエラーは、IBM Security zSecure インストール・ライブラリーを ISPPLIB 連結から削除することが原因です。更新プロセスは、IBM Security zSecure 提供パネル C2RPUPDP を使用します。このパネルが表示されることはありませんが、それが存在することはジョブ C2RZUPDZ に必要です。
   - エラーは以下のとおりです。
     - `Abend 04C; message ISPI021 Unrecoverable error in initialization of command tables`
     - `RC=990; ISPV010 Profile not loaded -/-Profile table 'ISPPROF' not read. Table service RC=8`
     - `RC=990; ISRxxxx -/-ISRxxxx message not found in 'ISPMLIB' library.`

     これらのエラーは、正しい ISPF データ・セットをメンバー C2RIISPF に指定しないことが原因です。正しいデータ・セットの指定については、 20 ページの『C2RIISPF での ISPF コンポーネントのロケーションの指定』を参照してください。
2. チェック・モードで CKRZUPDZ の実行がエラーなく正常に終了したら、そのジョブを更新モードで再び実行します。

   重要: CKRZUPDZ を更新モードで複数回実行することはサポートされていません。複数回の実行で JCL が破損する結果になる可能性があります。インストール・メンバーを最初の更新の後で再び更新する必要がある場合は、CKRZUPDI および C2RIISPF メンバーの両方を保存します。CKRINST データ・セットを再作成します。その後で、CKRZUPDZ ジョブを再び実行します。

第 5 章 製品の活動化と構成データ・セットのカスタマイズ

zSecure のインストール後、zSecure のターゲット・ライブラリーおよび配布データ・セットは、インストール時に作成された SMP/E 管理データ・セットで使用できます。以下に例を示します。

- デフォルトのデータ・セット命名規則を使用した場合、ターゲット・ライブラリーは高位修飾子 CKR から始まるデータ・セットに配置され、配布ライブラリーは高位修飾子 CKR.DLIB から始まるデータ・セットに配置されます。
- 独自のデータ・セット命名規則を指定した場合、ライブラリーは指定した高位修飾子から始まるデータ・セットに配置されます。

ターゲット・ライブラリーおよび配布ライブラリーの DD 名の完全なリストについては、「*Program Directory: IBM Security zSecure CARLa-Driven Components*」を参照してください。

zSecure のインストール後、以下のタスクを実行して、製品を活動化し、インストールの構成データ・セットをカスタマイズします。

- 『z/OS 追加イメージへの zSecure データ・セットの配布』
- 24 ページの『ライセンス機能の使用可能化』
- 24 ページの『ソフトウェアの APF 許可』
- 27 ページの『ソフトウェアの使用可能化 (TSO/ISPF ユーザー)』
- 31 ページの『第 6 章 ソフトウェアのデプロイメント』

z/OS 追加イメージへの zSecure データ・セットの配布

zSecure ソフトウェアを 1 つのイメージにインストールしたら、これを実行する他の z/OSイメージに関連データ・セットを配布できます。インストール先のデータ・セットから zSecure を実行する場合は、この手順を省略できます。

各イメージのシステムに製品のインストール先ボリュームへのアクセス権限がある場合、zSecure ソフトウェアを複数の z/OS イメージに配布して実行できます。以下の構成が使用可能であることを検査してください。

- ソフトウェアのインストール先である DASD ボリュームが、ソフトウェア配布先である z/OS イメージに対してオンラインであることが必要です。zSecure データ・セットがカタログされたカタログを含むボリュームもこれらのイメージからアクセス可能であることが必要です。
- zSecure データ・セットのユーザー・カタログが、他の z/OS イメージのマスター・カタログに接続されており、別名が正しく定義されている必要があります。

注**:** 配布前に 205 ページの『付録 A. サイト・モジュール』を参照してください。オプションのステップを実行してサイト・モジュールをカスタマイズすることに決めた場合、以下のいずれかの方法でそれを行うことができます。

- サイト・モジュールをカスタマイズしてから zSecure 構成データ・セットを配布することで、同じカスタマイズをすべてのイメージにコピーします。

- 配布後に各イメージごとに個別にサイト・モジュールをカスタマイズします。

配布では通常、ソフトウェアの実行元である実際のデータ・セット名はインストール先のデータ・セット名とは異なります。一部のサイトでは、実行元のデータ・セット名が各イメージごとに異なることもあります。データ・セット名を変更する場合、構成で新しい名前を使用してデータ・セット・セキュリティーをセットアップします。ストレージ管理ポリシーに適合したツールを使用すると、データ・セットをコピーできます。ターゲット・データ・セットのみが配布されます。

構成データ・セットにはイメージに依存するデータが含まれる場合があるため、構成データ・セット自体は配布しないでください。構成について詳しくは、31 ページの『zSecure 構成データ・セットについて』を参照してください。

ライセンス機能の使用可能化

このタスクについて

zSecure をインストールする予定の各 z/OS イメージについて、特定のフィーチャーを使用できないようにする場合は、parmlib メンバー IFAPRD*xx* を更新して、そのライセンス交付されたフィーチャーを使用不可にします。

手順

1. zSecure の使用可能化に必要な PRODUCT ステートメントを SCKRSAMP ライブラリー・メンバー CKRZPROD からコピーします。
2. 各 z/OS イメージごとにアクティブ・データ・セットの IFAPRD*xx* メンバーにステートメントを貼り付けます。
3. 各製品ごとに STATE パラメーターを更新して、z/OS イメージの使用可能化ポリシーを反映させます。

   IFAPRD*xx* メンバーが zSecure のライセンス交付済みフィーチャーの STATE を明示的に指定していない場合、そのフィーチャーは使用可能になります。

ソフトウェアの APF 許可

ほとんどの場合、zSecure を含むプログラム・オブジェクト・ライブラリーには、APF 許可を設定する必要があります。APF 許可は、以下のように zSecure コンポーネントに影響を与えます。

- zSecure Collect は関連情報にアクセスできます。
- 以下のコンポーネントは、APF 許可を使用して実行される場合にのみ機能します。
  - zSecure Admin および zSecure Visual のコンポーネントである CKGRACF プログラム
  - zSecure Alert
  - zSecure コマンド実行ユーティリティー CKX
  - zSecure Admin のオプション機能であるアクセス・モニター
  - zSecure Audit、Alert、および zSecure Admin 用アクセス・モニターで使用される RACF Exit Activator

– zSecure Server

- CKRCARLA プログラムおよび zSecure Audit 機能は、APF 許可なしに実行できます。ただし、この構成では以下の制約があります。
  – コマンドを直接実行できません。
  – 未許可の zSecure Collect プログラムで作成された CKFREEZE データ・セットを使用すると、不完全な結果が生じます。
- ERBSMFI プログラムを含むデータ・セット (デフォルトでは SYS1.SERBLINK) は、APF で許可されていることが必要です。ERBSMFI プログラム自体は APF を必要としませんが、zSecure Collect がこのプログラムを起動します。これは、ERBSMFI が 非 APF ライブラリー内にある場合には許可されません。多数のインストール済み環境では SYS1.SERBLINK はリンク・リストに含まれており、APF で許可されていますが、より安全な LNKAUTH=APFTAB 設定が有効な場合は、SYS1.SERBLINK またはローカルでそれに相当するものを APF リストに明示的に組み込む必要があります。

zSecure Admin の TSO コマンド・テーブルと ISPF コマンド・テーブル

CKGRACF (zSecure Admin と zSecure Visual によって使用されるコンポーネント) を実行するために、以下のセクションの説明に従って、TSO コマンド・テーブルと ISPF コマンド・テーブルを更新します。

- 『TSO コマンド・テーブルの更新』
- 26 ページの『ISPF TSO コマンド・テーブルの更新』

TSO コマンド・テーブルの更新

手順

1. プログラム名 CKGRACF を SYS1.PARMLIB メンバー IKJTSO*xx* の許可のある AUTHCMD および AUTHPGM テーブルに追加します。 オプションでプログラム名 CKGRACF を AUTHTSF テーブルに追加することもできます。CKGRACF を TSO 許可のあるコマンド・テーブルに組み込むことに失敗した場合、メッセージ CKG905I、CKR962F、または CKX962F が表示される可能性があります。

   26 ページの図 3 は、CKGRACF を更新した AUTHCMD NAMES テーブルの例です。

```
 /* IKJTSO00: TSO command tables                                    */
 /*                                                                 */
AUTHCMD NAMES(                      /* Authorized commands:     */   +
              CKGRACF               /* zSecure Admin            */   +
              RECEIVE               /*   TSO base               */   +
              XMIT     TRANSMIT     /*                          */   +
              LISTB    LISTBC       /*                          */   +
              LISTD    LISTDS       /*                          */   +
              SE       SEND         /*                          */   +
              RACONVRT              /*                          */   +
              IRRDPI00              /*                          */   +
              CONSOLE  CONSPROF     /*                          */   +
              SYNC                  /*                          */   +
              TESTAUTH TESTA        /*                          */   +
              PARMLIB)              /*                          */   +
```

図 *3. SYS1.PARMLIB* メンバー *IKJTSOxx* の例

2. テーブルを更新したら、TSO コマンド PARMLIB UPDATE((*xx*) を使用して、更新済みバージョンの IKJTSO*xx* を適用します。IPL は不要です。

   あるいは、CSECT IKJEFTE2、IKJEFTE8、IKJEFTAP、および IKJEFTNS を使用してプログラム名 CKGRACF を追加することもできます。詳しくは、資料「*TSO/E* カスタマイズ」(SA88-7050) を参照してください。

ISPF TSO コマンド・テーブルの更新

このタスクについて

CKGRACF を ISPF から実行する場合、デフォルトではその使用状況が SPFLOG*x*.LIST に記録されます。このログはパスワードを含む場合があります。このデータがログに記録されることを回避するには、ISPF TSO コマンド・テーブルを更新して ISPTCM 項目を組み込みます。この項目の追加後に変更を適用するには、ISPTCM テーブルを再アセンブルする必要があります。

手順

1. ISPF TSO コマンド・テーブルに ISPTCM 項目を追加し、FLAG の値を指定します。
   - 許可コマンドを示すビット 2 を設定します。
   - ロギングを使用不可にするビット 3 を設定します。
   - コマンド・プロセッサー用のビット 6 を設定します。

   ビットの番号は左から右に付加され、左端のビットはゼロになります。これらのビットは、合計して 50 (10 進数) または X'32' (16 進数) になります。

   27 ページの図 4 は、ISPTCM 項目の例です。

```
* HEADER
*
      ISPMTCM HEADER
*
* ONE ENTRY TYPE CALL FOR EACH COMMAND IN THE TCM.
* IT IS NOT REQUIRED THAT THE ENTRY NAMES BE IN ALPHABETIC ORDER
*

  ...

* OWN ENTRIES
       ISPMTCM  FLAG=32,ENTNAME=CKGRACF  TSO COMMAND, AUTH, NOLOG
* END CARD. STATEMENTS AFTER THIS CARD WILL BE IGNORED
       ISPMTCM  END
```

図 *4. ISPTCM* テーブルの例

2. 以下のいずれかの方法を使用して、新しい ISPTCM 項目を活動化します。
   - ISPTCM を STEPLIB に配置している場合は、ISPF を終了して再入し、変更を適用します。
   - ISPTCM をリンク・リストに配置している場合は、オペレーター・コマンド F LLA,REFRESH を実行して変更を適用します。
   - ISPTCM を LPA に配置している場合は、CLPA パラメーターを使用してシステムの IPL を実行し、ISPTCM データをリフレッシュします。
3. 変更を適用したら、STEPLIB または ISPLLIB に新しい ISPTCM を組み込んでテストします。

   ISPTCM の詳細については、マニュアル「対話式システム生産性向上機能 *(ISPF)* 計画とカスタマイズ」(GA88-7242) を参照してください。

ソフトウェアの使用可能化 (TSO/ISPF ユーザー)

別のバージョンの zSecure がご使用の z/OS イメージに既にインストールされている場合は、TSO/ISPF ユーザーのデフォルト SYSEXEC または SYSPROC 連結に指定されている zSecure REXX CKR プログラムの任意のコピーを引き続き使用できます。(CKR は以前は C2R と呼ばれていました。)CKR プログラムの既存のコピーを再利用することで、あらゆるカスタム・ロジックおよびサイト固有の zSecure 構成ファイルの参照を保持できます。このため、CKRPARM データ・セット内のコピーは自動的にはアップグレードされません。

zSecure の現行リリースとの互換性を確保するには、SCKRSAMP ライブラリーで使用可能な出荷済み CKR の現行バージョンを調べて、既存の CKR コピーに新しいロジックをコピーする必要があるかどうかを判断します。

新しい zSecure データ・セットを指すようにデータ・セット参照を変更します。

- リリースに依存するデータ・セット名を zSecure 配布のターゲットとして使用した場合、新しい zSecure が配置されるデータ・セットを指すように、CKR のすべてのコピー内およびすべての zSecure 構成内の CPREFIX パラメーターの値を変更します。
- リリースに依存しない別名をセットアップした場合、新しい zSecure データ・セットを指すように別名を再定義します。

- 以前に zSecure を使用していなかった場合、メンバーCKR を TSO/ISPF ユーザーの標準の SYSEXEC または SYSPROC 連結内のデータ・セットにコピーして調整します。

ユーザーが指定したデータ・セットを使用するカスタマイズしたバージョンの CKR REXX は、ジョブ CKRZPOST の実行後に CKRPARM データ・セットで使用できます。詳しくは、 34 ページの『zSecure 構成 データ・セットの作成』を参照してください。必要な変更内容については、 36 ページの『TSO/ISPF ユーザーへの構成の割り当て』を参照してください。

ISPF/PDF エディターを使用して CKR REXX をコピーします。ISPF/PDF エディターでは、コピー内容は SYSEXEC または SYSPROC データ・セットと同じフォーマット (固定ブロックまたは可変ブロック) で保存されます。 233 ページの『付録 E. ISPF インターフェースの構成』を参照してください。

zSecure 構成で LIBDEF を使用しない場合、別の方法で ISPF コンポーネントを使用可能にする必要があります。例えば、これらを TSO ログオン・プロシージャーに組み込むことができます。

ソフトウェアの使用可能化 (バッチ処理用)

バッチまたは開始タスクとしてプログラムを実行するには、「ユーザー・リファレンス・マニュアル」に記載されている zSecure 提供の JCL プロシージャーを使用します。このプロシージャーは、ソフトウェアのインストール先のデータ・セットを割り振ります。割り振りは、構成メンバー C2R$PARM または同メンバーのカスタム・コピー内の CPREFIX パラメーターを使用して実行されます。

以下のいずれかの方法を使用すると、バッチでプログラムを実行できます。

- zSecure で出荷される SCKRPROC データ・セットからプロシージャーを直接実行します。
- システム procilib 連結に SCKRPROC データ・セットを組み込みます。
- プロシージャーをシステム procilib 連結にコピーします。

システム proclib には、1 つの場所を更新するだけですべての JCL に変更を適用できるという利点があります。ただし、同時に有効にできるプロシージャーのバージョンが 1 つに制限されるという欠点もあります。例えば、proclib を共有している場合、イメージを 1 つずつアップグレードすることができません。

バッチ・ジョブの場合、zSecure 提供プロシージャーを JCLLIB ステートメントにより使用可能にします。通常、JCLLIB ステートメントでは、zSecure 提供の SCKRPROC データ・セットが後に続く構成を含むデータ・セットを最初に指定します。 37 ページの『バッチ・ジョブおよび開始タスクへの構成の割り当て』を参照してください。

ただし、開始ジョブとは異なり開始プロシージャーでは、z/OS は JCLLIB をサポートしません。したがって、SCKRPROC から JES proclib 連結に含まれるデータ・セットにいくつかのメンバーをコピーする必要があります。

- proclib 連結に多数のプロシージャーを組み込まないでください。特に、C2RC を使用するプロシージャーは組み込まないでください。:

  - C2RC には以下のメンバーが必要です。これらのメンバーはカスタマイズ可能であり、ユーザーが指定するパラメーターに依存します。
    - C2RI0CMD
    - C2RI0IOC
    - C2RI0SMF
    - C2RI0UNL
    - C2RI1CMD
    - C2RI1IOC
    - C2RI1SMF
    - C2RI1UNL

    通常、これらのカスタマイズされたメンバーは、SCKRPROC ではなく構成データ・セットから組み込まれます。
  - 複数の zSecure 構成データ・セットそれぞれにカスタマイズした独自のバージョンのメンバーを有効にすることが可能ですが、標準の JES proclib 連結では有効にできるバージョンは 1 つのみです。
- zSecure Alert および zSecure Admin のアクセス・モニターは開始タスクとして実行する必要があります。これらのコンポーネントのいずれかを使用する場合、以下のプロシージャーをコピーします。
  - Alert の C2POLICE および C2PCOLL
  - アクセス・モニターの C2PACMON

  プロシージャー C2PRECI も zSecure Alert の一部ですが、このプロシージャーは通常、バッチ・ジョブとして実行されます。このプロシージャーは内部でプロシージャー C2RC を使用するため、開始タスクとして実行しないでください。
- zSecure Server は通常、開始タスクとして運用されますが、これは必須ではありません。このコンポーネントを使用する場合、プロシージャー CKNSERVE をコピーします。
- zSecure Visual は通常、開始タスクとして運用されますが、これは必須ではありません。このコンポーネントを使用する場合、プロシージャー C2RSERVE、C2RSLOG、および C2RSTOP をコピーします。

プロシージャーをシステム proclib にコピーするときに、必要に応じてプロシージャーを変更することもできます。例えば、zSecure 出荷時のデフォルト値である CONFIG=C2R$PARM を独自の構成メンバーを示す値に変更することができます。特に、z/OS イメージ間で proclib を共有する場合、構成メンバー名またはその一部としてシステム・シンボルを使用することを考慮してください。その後でプロシージャーを共有して、イメージごとに異なる構成を持つことをサポートできます。

加えて、開始プロシージャーで使用する zSecure 構成、または JCLLIB なしで使用可能にしたい zSecure 構成は、JES プロシージャー連結に含まれるデータ・セットになければなりません。 37 ページの『バッチ・ジョブおよび開始タスクへの構成の割り当て』を参照してください。

注: SCKRPROC からメンバーをコピーすることは、zSecure のアップグレード時にコピーを検討して、場合によっては更新する必要があることを意味します。

第 6 章 ソフトウェアのデプロイメント

ほとんどのインストールに、いくつかの z/OS イメージが存在します。これらのイメージは、例えば、ワークロードを分離するものであったり、開発と実動とを切り分けるものであったりします。このような環境では、実際のソフトウェア・インストール・プロセスを一度のみ実行して、その後でそのソフトウェアをいくつかのイメージでデプロイすることが望ましいことです。

ソフトウェアを一度インストールしてそれを複数のイメージでデプロイするこの方法をサポートするために、zSecure では構成データ・セットを作成できます。これらのデータ・セットを使用して、ソフトウェアの特定のインスタンスに対するすべての構成オプションを別々のデータ・セットに指定することができます。構成データ・セットは、配布時にターゲット・ライブラリーと配布ライブラリーがコピーされるデータ・セットに新規データ・セット命名規則を指定するためにも使用できます。

zSecure 製品とフィーチャーの完全なセットをインストールすることができます。インストール後に、parmlib メンバー IFAPRDxx を使用して、それぞれの z/OS イメージで使用できない製品およびフィーチャーを指定できます。例えば、セキュリティー・マネージャーとして ACF2 を使用する z/OS イメージでは、zSecure Admin と zSecure Audit for RACF を使用不可にしたい場合があります。

配布指向インストールは、異なるライセンスを持つイメージ間、または異なるセキュリティー・マネージャー間でサポートされます。例えば、既に RACF 用の z/OS イメージに zSecure ソフトウェアがインストール済みの場合、その同じソフトウェアを、たとえ、別の z/OS イメージが ACF2 または Top Secret などの異なるセキュリティー・マネージャーを使用するときであっても、その別のイメージで使用することができます。このようなケースでは、以下のようにします。

1. 新規イメージに対して配布を実行します。
2. 1 つ以上の zSecure 構成ファイルを作成して、その環境で zSecure を作動させるために必要なオプションを指定します。

注**:** 配布指向インストールは、z/OS と z/VM の間ではサポートされません。zSecure を z/OS と z/VM の両方のプラットフォームで使用したい場合は、そのソフトウェアをそれぞれのプラットフォームに別々にインストールする必要があります。

zSecure 構成データ・セットについて

構成データ・セットは、イメージの zSecure 構成を表し、そのイメージ上でソフトウェアがどのように作動するかを決定します。例えば、zSecure 構成データ・セットは、どの zSecure フィーチャーが使用可能であるかと、入力データ・ソースのデータ・セット名を指定できます。

zSecure 構成データ・セットは、イメージ間で異なる唯一のデータ・セットです。これらのデータ・セットを使用して、以下の目的で構成を作成できます。

- zSecure Alert、アクセス・モニター、準拠性レポート、および Visual Server などのプロセスの特殊な目的の構成。
- 異なる z/OS イメージに zSecure をデプロイするための個別構成。
- 異なる入力データを必要とするユーザー・グループ、または特定の zSecure コンポーネントに対するアクセスを制限するユーザー・グループに対する構成。

zSecure 構成データ・セットは、インストール済みソフトウェアの一部でない区分データ・セットに保管されます。そのため、これらのデータ・セットはソフトウェアのアップグレードまたは再インストールのときに更新されません。したがって、カスタム構成設定をアップグレードの前後で維持できます。

表 3 に、それぞれのデプロイメント用にカスタマイズできる構成データ・セットのリストを示します。

表 *3. zSecure* 構成データ・セット

データ・セット名	説明
your.prefix.CKACUST	このデータ・セットには、オプション AU.R - ルール・ベースの準拠性評価で使用される「準拠した許可 ID 母集団」メンバーが含まれます。このオプションは、zSecure Audit でのみ使用可能です。
your.prefix.CKRPARM	このデータ・セットには、メイン構成メンバー C2R$PARM が含まれています。他の構成メンバーも作成できます。 CKRPARM データ・セットには REXX CKR (命名規則に応じて調整済み) も含まれています。このメンバーを SYSPROC または SYSEXEC データ・セットにコピーして調整します。 27 ページの『ソフトウェアの使用可能化 (TSO/ISPF ユーザー)』を参照してください。
your.prefix.CKRPROF	ISPF テーブル。ISPF トランザクションを SE.D の下で使用するつもりの場合に、このデータ・セットまたはそのコピーを C2R$PARM メンバーの PROFDSN パラメーターとして指定します。 233 ページの『ユーザー・グループのデフォルト・オプションのセットアップ (「セットアップ」メニュー)』を参照してください。
your.prefix.CKRJOBS	IBM 提供のジョブ (データ・セット命名規則に応じて調整済み)。

これらの構成データ・セットは通常、CKRINST ライブラリーまたは SCKRSAMP ライブラリーで使用可能な CKRZPOST ジョブを使用して作成されます。このジョブは、CKRPARM および CKRJOBS データ・セットの割り振り、埋め込み、更新を行います。また、ISPF インターフェースのカスタマイズに使用できる空の CKRPROF データ・セットの割り振りも行います。

CKACUST データ・セットが作成され、CKRINST ライブラリーまたは SCKRSAMP ライブラリーで使用可能なジョブ CKAZCUST を使用してデータが入力されます。

資料では、構成データ・セットは通常、低位修飾子 (例えば、CKRJOBS) によって参照されます。任意の好きなデータ・セット名を選択できますが、 デフォルトの低位修飾子を保持すると、構成の調整または JCL の指定変更の必要性が減ります。

your.prefix は、それぞれのデプロイメントで独自の値になります。以下の方法のいずれかを使用して、独自の値を接頭部に指定します。

- zSecure インストール・ジョブ CKRZPOST を編集する。
- 値をインストール・ライブラリーの C2$PARM メンバーに指定する。

メンバー C2R$PARM は、構成のデフォルトの開始点です。バッチおよび ISPF インターフェースの両方で使用することができるように、このメンバーは JCL SET ステートメント (これを ISPF インターフェースが解釈します) を使用します。以下の例を参照してください。

```
//  SET CPREFIX='CKR'
//  SET VOLSER=
//  SET PROFDSN='CKR.IPO1.CKRPROF'
//  SET SYS=IPO1
```

構成メンバーの完全な構文については、 223 ページの『付録 D. 構成パラメーターと構成メンバー』を参照してください。

通常は、以下のタスクの実行時に限って新規の zSecure 構成を作成します。

- 初めて zSecure をインストールする。
- zSecure を新規の z/OS イメージ上でセットアップする。
- 特殊目的構成をアクセス・モニターなどのプロセス用にセットアップする。
- zSecure を新規ユーザー・コミュニティー用にセットアップする。

zSecure の SCKRSAMP(C2R$PARM) に用意されているサンプル構成を使用できます。ただし、このサンプルは、最も基本的なインストール・シナリオ「ソフトウェアの配布または構成のカスタマイズを行わないで単一の z/OS イメージをインストールする」にのみ使用することを目的としています。

さまざまな z/OS イメージまたはさまざまなユーザー・グループのために zSecure を構成するには、これらの z/OS イメージまたはユーザー・グループの構成を作成します。詳しくは、 34 ページの『zSecure 構成 データ・セットの作成』を参照してください。新規バージョンへのアップグレード時または zSecure の再インストール時には、 36 ページの『既存の zSecure 構成 データ・セットの保守』を参照してください。

以下のセクションに、さまざまな z/OS イメージ、または RACF 管理者や RACF 監査員などのさまざまなユーザー・グループの構成を作成する方法についての情報が記載されています。以下の情報を参照してください。

zSecure 構成 データ・セットの作成

このタスクについて

この手順に説明されているように、さまざまな z/OS イメージ、または RACF 管理者や RACF 監査員などのさまざまなユーザー・グループの zSecure 構成を作成することができます。

注: zSecure Alert、zSecure Admin、アクセス・モニター、Visual Server などの zSecure コンポーネントに特殊目的構成を作成することもできます。これらのコンポーネントの構成の作成については、それぞれのコンポーネントのセットアップ資料を参照してください。

手順

1. 31 ページの『zSecure 構成データ・セットについて』を見直して、zSecure 構成データ・セットおよびそれらを管理するために使用する zSecure 提供ジョブについて確認します。
2. (オプション) グローバル更新メンバー CKRZUPDI および C2RIISPF をセットアップします。

   CKRZPOST ポストインストール・ジョブを使用した zSecure 構成データ・セットの作成に使用される値は、グローバル更新メンバー CKRZUPDI および C2RIISPF に指定された値に基づいています。インストール・プロセス中にグローバル更新を実行しなかった場合は、CKRZPOST を実行する前にその実行を行ってください。 17 ページの『インストール・パラメーターのカスタマイズ』を参照してください。
3. zSecure 構成データ・セットの高位修飾子を選択します。 実際のソフトウェアに設定する命名規則は構成データ・セットに最良の選択ではない場合があることを覚えておいてください。代わりに、構成データ・セットの対象になるユーザーのグループおよび z/OS イメージを示す高位修飾子を使用することを考慮してください。構成データ・セットは zSecure のアップグレードの前後で持続することになっているので、バージョンまたはリリースを表すデータ・セット名に修飾子を組み込まないでください。
4. CKRZPOST ジョブの説明に従って、インストールのジョブをカスタマイズします。 必ず以下のパラメーターを更新します。

   INSTLIB

   zSecure ソフトウェアが稼働する zSecure インストール・ライブラリー・データ・セットの高位修飾子を指定します。

   YOURPFX

   CKRZPOST を使用して作成された zSecure 構成データ・セットに使用したい高位修飾子でパラメーターを更新します。

   YOURPFX のデフォルト値を変更しないと、CKRZPOST ジョブを使用して作成された構成データ・セットは *your.prefix* を高位修飾子として使用します。インストール済みソフトウェアの単一コピーに複数の構成を作成できるので、CKRPROF は接頭部を提供しません。

   カスタマイズが必要ない構成データ・セットの DD ステートメントをコメント化します。

5. CKRZPOST を実行して zSecure 構成メンバーを作成します。

   ジョブ CKRZUPDZ をインストール以前に実行した場合、ジョブ CKRZPOST は戻りコード 4 で終了することがあります。その理由は、一部のデータ・セット更新が CKRZUPDZ 実行中に既に完了済みだったからです。この戻りコードは無視できます。
6. 個別のユーザー・コミュニティーまたは z/OS イメージの構成を作成します。『zSecure 構成 データ・セットのカスタマイズ』を参照してください。
7. オプション: オプション AU.R - ルール・ベースの準拠性評価を使用する zSecure Audit ユーザーの場合のみ。JCL のコメントに従ってジョブ CKAZCUST を更新し、CKACUST ライブラリーを作成するためのジョブを実行依頼します。すべての新規リリースについて、ジョブ CKAZCUST を実行し、AU.R に必要な、まだ存在していないすべてのメンバーを作成します。このジョブは既に存在するメンバーには影響を及ぼしません。作成されたメンバーには空のリストが含まれています。

zSecure 構成 データ・セットのカスタマイズ

zSecure 構成データ・セットを作成した場合、そのメンバーをカスタマイズして、異なるユーザー・コミュニティーまたは異なる z/OS イメージに使用するコピーを作成できます。例えば、同一イメージ上の RACF 管理者および RACF 監査員などの異なるユーザー・グループが使用するように zSecure を構成するには、メンバー C2R$PARM のコピーを作成します。次に、それぞれのメンバーを別々に構成します。メンバーをコピーして構成するとき、以下の規則とガイドラインが適用されます。

- C2R または CKR で始まるユーザー・メンバー名は使用しないでください。
- zSecure Admin ユーザーの場合、同じデータ・セット内のすべての構成メンバーは、新規の RACF **ユーザー** ID を作成するために使用される zSecure Admin 設定を指定する C2RSMUMA、C2RSMUMH、および C2RSMUMP メンバー共有します。 247 ページの『RACF データベースに新規ユーザー ID を作成するための zSecure Admin の構成』を参照してください。これらのメンバーに異なる値を指定するには、以下の操作を行います。
  1. CKRPARM データ・セット全体を zSecure Admin の実行元にしたいシステムにコピーします。
  2. 必要に応じて CKRPARM メンバーを更新します。
- CKRPROF の複数コピーを作成して、さまざまな z/OS イメージまたはさまざまなユーザー・コミュニティー用の ISPF インターフェースをカスタマイズすることができます。
- CKRJOBS データ・セットは更にカスタマイズされることになっています。例えば、各ジョブを実行する環境に応じて、各種の構成メンバーを指定することがあります。このため、CKRJOBS データ・セットの複数コピーを作成することを考慮してください。
- オプション AU.R - ルール・ベースの準拠性評価を使用する zSecure Audit ユーザーの場合: SET CKACUST パラメーターからコメントを削除し、データ・セット名を更新します。

既存の zSecure 構成 データ・セットの保守

zSecure 構成データ・セットはお客様の資産です。それらは、インストール済みソフトウェアの一部でない区分データ・セットに保管されます。例えば、Setup Default (SE.D) の実行時に、カスタマイズされたすべてのインターフェース設定は `your.prefix.SCKRPROF` に書き込まれます。これらのデータ・セットは zSecure インストール・プロセスでは自動的に更新されないので、アップグレードの前後で構成設定を維持できます。

新規バージョンへのアップグレード時には、既存の構成データ・セットから開始するか、または以前のリリースから構成データ・セットをコピーします。次に、これらの構成を手動で SCKRSAMP ライブラリーの C2R$PARM メンバーと比較し、新規パラメーターがあれば適用するかどうかを決定します。 233 ページの『ユーザー・グループのデフォルト・オプションのセットアップ (「セットアップ」メニュー)』で説明されているように、同じことが PROFDSN データ・セットに当てはまります。

サンプル構成データ・セットが存在する場合、それらはインストール環境に合わせて既にカスタマイズ済みであることが考えられます。 zSecure 構成データ・セットを確実に最新の状態にするには、ご使用の構成を手動で SCKRSAMP C2R$PARM メンバーと比較して、既存の zSecure 構成データを更新する必要があるかどうかを判断します。

構成の割り当て

インストールに必要な zSecure 構成を作成した後で、その構成を TSO/ISPF ユーザー、バッチ・ジョブ、および開始タスクに割り当てて、それらがユーザーおよびシステム処理に使用可能な状態にします。プロダクト機能およびデータへのアクセスを制御するために、構成ごとにセキュリティーを確立する必要もあります。その方法については、以下のセクションを参照してください。

- 『TSO/ISPF ユーザーへの構成の割り当て』
- 37 ページの『バッチ・ジョブおよび開始タスクへの構成の割り当て』
- 207 ページの『付録 B. zSecure のセキュリティー・セットアップ』

TSO/ISPF ユーザーへの構成の割り当て

構成は、ISPF インターフェースの開始に使用される REXX exec CKR のコピーによって割り当てられます。`CKR` exec は、構成データ・セット名およびメンバー名をパラメーターとして使用して `C2REMAIN` を開始します。`CKR` の異なるコピーを z/OS イメージごと、ユーザーのグループごとに作成できます。代わりに、`CKR REXX` のコピーを調整して、動的に構成を選択したり、構成メンバーを指定変更するパラメーターを渡したりできます。

例えば、単純な管理用タスクを対象に、指定変更パラメーター STARTTRX(MENU(RA.H)) のみを追加する `CKGHELP` REXX exec を作成できます。この exec は単一パネルのヘルプ・デスク・オプションに対応します。同様に、単純な管理用タスクを対象に、指定変更パラメーター STARTTRX(MENU(RA.Q)) のみを追加する `CKRQ` REXX exec を作成できます。この構成は、「*IBM Security*

zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル」に説明がある「クイック・ユーザー管理」オプションへのアクセス権限をユーザーに提供します。

バッチ・ジョブおよび開始タスクへの構成の割り当て

- zSecure ISPF トランザクションによって実行依頼されるジョブは、ソフトウェア・ロケーション (SCKRLOAD および SCKRSAMP) を TSO セッションから継承します。適用可能な場合、トランザクションは NJE ルーティングおよびシステム・アフィニティーを生成できます。ユーザーは、この情報の指定を求められることがあります。
- zSecure パネルから実行依頼されないバッチ・ジョブについては、JCLLIB ステートメントの構成データ・セットを指定して、必要なメンバーを「組み込み」ます。多くの場合に、NJE ルーティングおよびシステム・アフィニティーを指定する必要があります。 41 ページの『第 8 章 実動のためのセットアップ』を参照してください。
- ジョブ入力サブシステムのプロシージャー・ライブラリーに含まれるデータ・セットに、C2R$PARM などの構成メンバーを作成することもできます。類似した名前の構成メンバーが z/OS イメージによって異なる場合は、ジョブを実行する場所の同じ z/OS イメージ上で JCL が確実に変換されるためにシステム・アフィニティーが必要です。「*MVS™ JCL* 解説書」に、JES2 および JES3 にシステム・アフィニティーを指定する方法が文書化されています。
- 開始プロシージャーでは、 JCLLIB は使用不可です。したがって、開始プロシージャーをセットアップする場合には必ず、それが使用する構成メンバーを、ご使用のプロシージャー・ライブラリーにコピーする必要があります。
- 追加のカスタマイズの説明は、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」にあります。

第 7 章 インストールの検査

基本の ISPF インターフェース機能およびメニュー構成

ISPF/PDF コマンド・オプションの下で、 27 ページの『ソフトウェアの使用可能化 (TSO/ISPF ユーザー)』で作成した REXX を呼び出して、Security zSecure 1 次メニューを表示します。1 次メニューはライセンスと許可に基づいて構成されるため、表示されるメニューは「ユーザー・リファレンス・マニュアル」に示されているものとは異なる場合があります。

zSecure Collect 機能および zSecure の基本バッチ操作の確認

手順

1. Security zSecure 1 次メニューから、SE.1 (ファイルのセットアップ) と入力します。
2. 「Setup files」パネルで、選択したすべての入力セットから選択項目を削除します。
3. SE.2 (セットアップ - 新規ファイル) と入力して、新しい CKFREEZE データ・セットと UNLOAD データ・セットを作成します。
4. 割り振りパラメーターの入力を求められます。概算で、以下のように指定します。
   - CKFREEZE データ・セットの場合は、オンライン DASD ボリュームごとに 2 MB。
   - UNLOAD データ・セットの場合は、ご使用のセキュリティー・データベースと同じサイズ。
5. これらのデータ・セットに入力するバッチ・ジョブを実行依頼するには、REFRESH コマンドを使用します。このジョブは、必ず十分な許可を持つ**ユーザー ID** のもとで実行してください。ジョブの終了後に、エラー・メッセージが出ていないか、出力を調べます。

レポートを表示する機能

データを CKFREEZE データ・セットと UNLOAD データ・セットに追加するためのジョブを正常に実行依頼した後は、 AU.S、AU.V、および RA.U (ライセンスにより異なります) のようなレポート作成機能を使用できます。レポート作成機能の使用について詳しくは、「ユーザー・リファレンス・マニュアル」を参照してください。

セキュリティー・リソースを検査するための CKGRACF コマンド

注: この手順は、IBM Security zSecure Admin を使用する場合にのみ必要です。

TSO ライン・モードから、以下のコマンドを実行します。

```
alloc reuse file(systerm) dataset(*)
ckgracf show myaccess
```

コマンドを実行すると、セキュリティー・リソースのリストが提供され、現行のアクセス・レベルと、それぞれのアクセス・レベルの基になっているプロファイルが表示されます。

ACF2 レポート作成の検査

注: このステップは、zSecure Audit for ACF2 コンポーネントを使用する場合にのみ必要です。

zSecure Audit for ACF2 と ACF2 が ACF2 データベースの内容について完全に一致していることを検査するために、C2AJIVP ジョブを実行します。

第 8 章 実動のためのセットアップ

SCKRSAMP および SCKRJOBS データ・セット

37 ページの『バッチ・ジョブおよび開始タスクへの構成の割り当て』で説明したように、ジョブを SCKRSAMP および SCKRJOBS データ・セットから、ジョブ・スケジューリング・システムが使用するデータ・セットなどの独自のデータ・セットにコピーする必要があります。SCKRSAMP と SCKRJOBS は SMP/E で維持されているため、このデータ・セット内のジョブを直接編集しないでください。複数の z/OS イメージを使用する場合には、このデータ・セットを編集すると配布指向インストールにも違反します。

16 ページの『zSecure 提供インストール・ジョブ』 で説明するように、カスタマイズされた SCKRSAMP のコピーである CKRINST ライブラリーが、ソフトウェア・インストール・プロセス中に作成されます。

キャパシティー・プランニング情報

IBM Security zSecure 製品スイートは、複数の製品とコンポーネントで構成されています。このトピックでは、以前はさまざまな資料やアプリケーション・メモに記載されていた情報が使用されており、これらのアプリケーションの実行に必要なシステム・リソースの特定に役立てることができます。

概要

このトピックは、製品ごとに複数のセクションに分かれています。ほとんどのコンポーネント・セクションは、製品で使用されるシステム・リソースのタイプごとに複数のサブセクションに分かれています。ここでは、以下のタイプのシステム・リソースについて説明します。

- プログラムで使用または作成されるデータを格納するために必要な DASD ストレージ
- プログラムの実行に必要な仮想ストレージ
- プログラムで使用される CPU 時間
- ネットワーク上のデータ・トランスポート

DASD ストレージ

zSecure では、主に以下のタイプのデータ用に DASD (ディスク) 上のデータ・ストレージが使用されます。

CKFREEZE

このタイプのデータ・セットには、システムとリソースに関する情報が含まれます。これには、多数に上るシステム制御ブロック、データ・セットおよび UNIX ファイルの名前、さらにはいくつかのデータ・セットの内容 (の一部) が含まれます。CKFREEZE データ・セットは、zSecure CKFCOLL プログラムによって作成されます。この情報は、多くの zSecure 製品によって使用されます。

RACF データ

zSecure Admin および Audit では、RACF ソースからの情報が必要になります。このソースには、既存の RACF データベース、または UNLOAD データ・セットのいずれかを使用できます。zSecure CKRCARLA プログラムによって作成される UNLOAD データ・セットには、RACF データベースの専用形式のスナップショットが含まれています。そのサイズは、RACF データベースの使用済み部分のサイズとほぼ同じです。zSecure Admin の RACF-Offline・コンポーネントでは、システム RACF データベースのコピーが使用されます。オフライン RACF データベースのサイズは、使用方法によって異なります。

UNLOAD ファイルのすべての機密フィールドは常にアスタリスクで置換されます (マスクされます)。したがって、コピー操作および再作成操作中には複製されません。

ACF2 データ

zSecure Audit for ACF2 では、ACF2 データベースからの情報が必要になります。これには、BACKUP データベースの既存のセット、または UNLOAD データ・セットのいずれかを使用できます。zSecure CKRCARLA プログラムによって作成される UNLOAD データ・セットには、ACF2 データベースの専用形式のスナップショットが含まれています。そのサイズは、ACF2 データベースの使用済み部分のサイズとほぼ同じです。

SMF データ

このデータは、zSecure に固有のものではありません。SMF レコードは、システム内の環境およびイベントに関する情報を提供するために作成されます。これには、パフォーマンス制御、プランニング、および監査の目的で使用できる情報が含まれています。さまざまなタイプのイベントに関するデータが収集されます。zSecure Audit では、システム内のイベント履歴に関するレポートへの入力として SMF データを使用できます。

アクセス・データ

これらのデータ・セットには、記録されたアクセスに関する情報が含まれます。その内容は、一部のタイプの SMF レコードとよく似ています。アクセス・モニター・データ・セットは、zSecure C2PACMON プログラムによって作成されます。このデータの分析は、zSecure Admin で行うことができます。

zSecure に固有のデータのタイプは、CKFREEZE データ・セット、セキュリティー・データベースの UNLOAD データ・セット、およびアクセス・モニター・データ・セットです。

CKFREEZE データ・セットのさまざまなタイプ**:** CKFREEZE データ・セットは、CKFCOLL プログラムによって作成され、さまざまな用途に使用されます。ただし、CKFREEZE データ・セットを使用するすべてのプログラムが、同じ量やタイプの情報を必要としているわけではありません。このため、CKFREEZE データ・セットは、以下のリストに示す複数のタイプに分類されています。CKFCOLL プログラムが必要な情報をすべて収集するためには、APF の許可を受けてこのプログラムを実行する必要があります。非 APF モードでこのプログラムを実行すると、わずかな機能しかサポートされません。APF の許可を受けた実行と APF の許可を受けな

い実行について詳しくは、ご使用の製品の「ユーザー・リファレンス・マニュアル」の zSecure Collect for z/OS に関する章を参照してください。

フルサイズ

このタイプの CKFREEZE データ・セットは、パラメーターや選択基準を指定しておらず、かつユーザーが zSecure Admin または zSecure Audit のライセンスを保持している場合に作成されます。ユーザーが zSecure Admin のライセンスだけを保持している場合は、収集プログラムによって特定の監査固有の情報が自動的に除外されます。フルサイズ CKFREEZE データ・セットには、すべてのシステムおよびユーザー・カタログ、バックアップ、マイグレーション、およびテープの各カタログ、すべての VVDS、およびすべての VTOC からの情報が含まれます。また、すべての APF、Linklist、lpalib、parmlib、および proclib の各データ・セットからのディレクトリー情報も含まれます。このタイプの CKFREEZE データ・セットには、UNIX HFS データ・セットまたは ZFS データ・セットのすべてのファイルに関する情報も含まれます。zSecure 1.13 以上では、すべての CICS システムおよび IMS™ システムのすべてのプログラムおよびトランザクション情報が収集されます。zSecure 1.13.1 以降の場合、テーブル、パッケージ、およびその他の情報など DB2 サブシステム情報が収集されます。

フルサイズ CKFREEZE データ・セットには、この他に詳細なシステム監査に必要なデータも含まれています。

この CKFREEZE データ・セットには多くの情報が含まれているため、サポートされるすべての監査機能およびレポート機能で使用できます。しかし、多くの情報が含まれるために、すべてのデータの収集と処理に長い時間がかかる場合があるという欠点があります。このため、フルサイズ CKFREEZE データ・セットは、主に監査やシステム全体の分析に限って使用されます。

このタイプの CKFREEZE データ・セットがデフォルトです。これを作成するには、Admin または Audit のライセンスが必要です。パラメーターを指定する必要はありません。

共有 **DASD** を除くフルサイズ

この CKFREEZE データ・セットには、フルサイズ CKFREEZE ファイルの説明で示したすべての情報が含まれますが、複数システム間での共有が定義されているボリュームのカタログ、VVDS、および VTOC 情報は含まれません。

このタイプの CKFREEZE データ・セットには一部の情報が含まれていないため、必ずフルサイズ CKFREEZE データ・セットと組み合わせて使用してください。このタイプの CKFREEZE データ・セットの処理にも、多くの時間がかかる可能性があります。このタイプのデータ・セットは、主に共有データ (sysplex) 環境の監査およびシステム全体の分析に使用されます。

このタイプの CKFREEZE データ・セットを作成するには、Admin または Audit のライセンスが必要です。以下のパラメーターが指定されている必要があります。

```
SHARED=NO
```

通常管理

この CKFREEZE データ・セットには、通常の RACF 管理の目的に必要な

すべての情報が含まれます。ほとんどのカタログ、VVDS、および VTOC 情報は含まれません。MASTER カタログからの情報は含まれますが、UNIX ファイルとシステム・ライブラリーの内容に関する情報は含まれません。

このタイプの CKFREEZE データ・セットは、サイズがあまり大きくないため、短時間で処理できます。ただし、ユーザー・カタログの情報が含まれていないため、TSO ユーザー ID およびバッチ・ユーザー ID の削除には適していません。これは、既存のユーザー ID のコピーや、マスター・カタログ内での別名エントリーの定義に使用されます。また、詳細な情報が含まれていないため、このタイプの CKFREEZE データ・セットは、詳細な監査やシステム分析にも適していません。詳細なデータ・セットや UNIX ファイルの情報を必要としない、簡単な監査レポートは作成できます。

このタイプの CKFREEZE データ・セットを作成するには、Admin または Audit のライセンスが必要です。これは、以下のパラメーターを指定することで作成できます。

```
CAT=MCAT,VVDS=NO,VTOC=NO,UNIX=NO,BCD=NO,MCD=NO,
RMM=NO,TMC=NO,IMS=NO,CICS=NO,DB2=NO,MQ=NO
```

通常監査

この CKFREEZE データ・セットには、ほとんどの詳細な監査およびシステム分析に必要となる情報が含まれます。ほとんどのカタログ、VVDS、および VTOC 情報は含まれません。MASTER カタログからの情報、さらには UNIX ファイルに関する情報が含まれます。

通常監査 CKFREEZE データ・セットには、通常管理 CKFREEZE データ・セットよりも多くの情報が含まれています。処理にかかる時間も長くなりますが、フルサイズ CKFREEZE データ・セットの処理に比べると短時間で済みます。ほとんどの詳細な監査レポートを作成できますが、データ・セット、IMS、および CICS リソースなどのリソース情報を必要とするレポートには対応できません。ほとんどの監査では、レポートの作成に必要な時間はそれほど重要ではないため、多くの場合はフルサイズ CKFREEZE データ・セットが選択されます。

このタイプの CKFREEZE データ・セットを作成するには、Admin または Audit のライセンスが必要です。これは、以下のパラメーターを指定することで作成できます。

```
CAT=MCAT,VVDS=NO,VTOC=NO,BCD=NO,MCD=NO,RMM=NO,TMC=NO,IMS=NO,CICS=NO,DB2=NO,MQ=NO
```

ライブラリー分析

これは特殊目的の CKFREEZE データ・セットです。これには、指定されたデータ・セットのチェックサム情報が含まれます。チェックサム情報の計算には時間がかかるため、このタイプの CKFREEZE データ・セットは、ライブラリー分析を行う場合にのみ作成します。ライブラリー分析処理では、複数のポイント・イン・タイムから複数の CKFREEZE データ・セットが使用されます。フルサイズ CKFREEZE データ・セットには通常含まれているその他の情報 (カタログ、UNIX ファイルなど) は、除外する方がよい場合もあります。

このタイプの CKFREEZE データ・セットを作成するには、Audit のライセンスが必要です。これは、パラメーター CHECK=YES を指定して作成できます。その際、不要なデータを抑止するためにパラメーターおよびキーワードと組み合わせることができます。

```
CAT=MCAT,DASD=NO,TAPE=NO,SWCH=NO,RMM=NO,TMC=NO
UNIX=NO,PATH=NO,SMS=NO,IMS=NO,CICS=NO,DB2=NO,MQ=NO
```

ミニ　これは最も小さいサイズの CKFREEZE データ・セットですが、ほとんどの RACF 照会には十分な情報が含まれています。これには、ストレージ内にある情報だけが含まれます。含まれる情報の例としては、RACF 制御ブロック (CDT、動的解析、システム・オプション)、SMF オプション、および重要なシステム・データ・セットのリストからの情報が挙げられます。サイズは、通常、約 1 MB です。

このタイプの CKFREEZE データ・セットの目的は、主にリモート照会に対する情報提供です。

このタイプの CKFREEZE データ・セットを作成するには、Admin または Audit のライセンスが必要です。これは、以下のパラメーターを指定することで作成できます。

```
IO=NO,SMS=NO,TCPIP=NO,MOD=NO,CICS=NO,IMS=NO,NJE=NO,S=V=NONE,NOXMEM,DB2=NO,MQ=NO
```

特殊目的

特定のコンポーネント (zSecure Alert 製品など) が使用する特殊目的の CKFREEZE データ・セットがいくつか存在します。このような特殊目的 CKFREEZE データ・セットの内容はその目的専用であるため、これらのデータ・セットを他のアプリケーションと共有することはできません。

このタイプの CKFREEZE データ・セットを作成するには、多くの場合、Alert、Admin、または Audit のライセンスが必要です。パラメーターは、必要となる具体的な情報によって異なります。

CKFREEZE データ・セットのスペース所要量**:** CKFREEZE データ・セットに必要なスペースは、データ収集時に使用するオプションによって異なります。以下のリストは、各タイプの情報に必要なスペースの量をまとめたものです。これらの量を経験法則として利用してください。

- ベース・サイズとして 1 MB
- システムおよびユーザー・カタログのサイズ
- DFHSM MCDS、BCDS および OCDS のサイズ、または DMS カタログのサイズ
- DFRMM 制御データ・セットまたは TMC カタログのサイズ
- オンライン DASD ボリュームごとに 2 MB
- HFS/ZFS のスペース 1 ギガバイトごとに 2 MB
- IMS または CICS のトランザクションまたはプログラム 5000 個ごとに 1 MB

式では、次のようになります。

サイズ (MB) = 1 + C + H + T + 2*D + 2*U + O/5000

ここで、
C = システムおよびユーザー・カタログのサイズ

H = DFHSM または DMS カタログのサイズ
T = テープ・カタログのサイズ
D = オンライン・ディスクの数
U = HFS/ZFS スペースのギガバイト数
O = IMS および CICS のトランザクションおよびプログラムの数

セキュリティー・データのタイプ **(RACF** または **ACF2):** zSecure Admin および zSecure Audit の両製品では、アクティブな RACF データベースまたはバックアップ ACF2 データベースからの情報を使用できます。抽出やコピーは必要ありません。RACF データベースまたは ACF2 データベースの私的なバックアップ・コピーを使用することもできます。私的なバックアップ・コピーを使用する場合は、現在のデータベースのサイズと同等の DASD スペースを計画してください。

RACF データベースまたは ACF2 データベースの専用形式の UNLOAD コピーを使用することもできます。このような UNLOAD コピーは、Admin および Audit のレポートを生成するためのフリーズ済み入力として使用できます。UNLOAD コピーのサイズは、データベースの使用済み部分とほぼ同じです。UNLOAD データベースの利点は、すべての機密フィールド (パスワードなど) が UNLOAD コピーから除外されていることです。

zSecure Admin の RACF-Offline・コンポーネントでは、システム RACF データベースのコピーが使用されます。RACF データベースのサイズは、使用方法によって異なります。通常、オフライン用に使用される RACF データベースのサイズは、アクティブなシステム RACF データベースと同じです。

アクセス・モニター・データ: zSecure アクセス・モニターは、zSecure Admin の一部です。RACF システムでのみ使用可能です。アクセス・モニターは、ほとんどのアクセス・イベント、および一部のプロファイル管理イベントに関する情報を収集します。情報は、アクセス・モニター・データ・セットと呼ばれるデータ・セット内に保存されます。収集された情報は、以下に示すいくつかのデータ・セットで保持されます。

1 日の収集データ・セット
: これらのデータ・セットは、アクセス・モニター開始タスクによって作成され、通常はアクセス・モニターが実行されている間だけ存在します。これには、計測期間中に収集された複数ブロックのレコードが含まれます。計測期間は SMF 間隔と同じです。SMF 間隔は SMFPRM*xx* で指定可能で、デフォルト値は 30 分です。

1 日の統合データ・セット
: これらのデータ・セットも、アクセス・モニター開始タスクによって作成されます。これらには、1 日の統合レコードが単一のブロックとして含まれます。統合は、1 日 1 回、自動的に行われます。

サイト固有の統合データ・セット
: 1 日の統合データ・セットを複数統合して、1 週間、1 カ月間、さらには 1 年間の情報を含む単一のデータ・セットを作成できます。この統合プロセスの統合効率が 100% に近付いて行くことが理想です。つまり、期間を追加しても、統合データに必要なスペースは増加しない状態が理想です。実際の環境では、統合プロセスの効率は 90 % 程度、またはそれを下回る傾向が

あります。つまり、期間を追加すると、統合データに必要なスペースが、追加データのサイズの 10 % 以上増加します。

統合プロセスでは、すべてのタイプのイベントごとに、カウントと最終発生時の情報が保持されます。アクセス・モニター・データに必要なスペースは、環境によって大きく異なります。例えば、1 人のユーザーが同じデータ・セットに 1 日に 1000 回アクセスした場合は、単一のイベント・レコードに統合されますが、1000 人のユーザーが同じデータ・セットにそれぞれ 1 回だけアクセスした場合は、1000 個のイベント・レコードに統合されます。

アクセス・モニターが実際に実装されていない場合、アクセス・モニター・データ・セットに必要な DASD スペースの合計を予測する簡単な方法はありません。RACROUTE の SAFTRACE を実行すると、イベントの数は予測できますが、さまざまなリソース、ユーザー、ジョブ名、および要求オプションにまたがった要約のレポートはありません。最も適切な近似値は、SMF オフロード・データ・セットの現在のサイズです。初回の始動時に、データ・セットのサイズをモニターおよび調節することで、必要なスペースをより正確に予測できます。

zEDC を使用した DASD 要件の削減: zSecure データ・セットに対して適切な DATACLAS を指定して、DASD のスペース所要量を削減することができます。これは、CKFREEZE データ・セットおよび ACCESS データ・セットに対して効果的です。DATACLAS の指定は、適切な ALLOC コマンドまたは JCL で実行することも、DATACLAS ACS ルーチンを使用して自動的に実行することもできます。zEDC に関する背景情報については、 86 ページの『zSecure 用の zEnterprise Data Compression (zEDC)』を参照してください。

仮想ストレージ

プログラムの実行中には、仮想ストレージが必要です。必要な仮想ストレージの量は、レポート作成中または分析中に処理されるデータの量によって異なります。ほとんどのタイプのレポートでは、必要な仮想ストレージは、出力レポートのサイズと同程度です。例えば、400 万個の SMF レコードの詳細情報付きレポートを生成する場合は、プログラムがこれらのレコード内で発生するすべての固有のフィールド値を保持するだけの十分なスペースが必要です。

アクセス・モニター・データ・セットの統合など特殊なプロセスについては、それぞれのセクションを参照してください。

CKRCARLA プログラムは、ほとんどの zSecure 製品で使用されるメインプログラムです。zSecure 2.2.0 以降では、このプログラムは CKR4Z または CKR8Z196 のいずれかを呼び出すルーター・プログラムになっています。 CKR8Z196 プログラムは、8 バイトのストレージ・ポインター・モデルを使用して 64 ビット・モードで実行されます。CKR4Z プログラムは、4 バイトのストレージ・モデルを使用して 31 ビット・モードで実行されます。CKR8Z196 は、2 GB 境界より下のストレージではなく、CKR4Z で使用される 2 GB 境界より下のストレージと比較して 最大 2 倍の 2 GB 境界より上のストレージを使用することが予想されます。

2 GB 境界より上のストレージの最大量は、REGION パラメーターではなく MEMLIMIT パラメーターで設定されます (`REGION=0` が `MEMLIMIT=NOLIMIT` を要求する場合を除きます)。 CKR0039 メッセージには、実際の制限の内容と、どの機能が実際にどのような要求 (例えば、サイト出口 IEFUSI や PARMLIB メンバー) か

らそれを制限したかが示されます。TSO ユーザーは MEMLIMIT パラメーターを動的に指定できないため、TSO ユーザーが 2 GB 境界より上のストレージを要求する場合は、出口、PARMLIB 設定、またはログオン・プロシージャー・キーワードの変更が必要なことがあります。

CPU 時間

zSecure プログラムの実行に必要な CPU 時間の合計は、2 つの異なる方法で表現できます。1 つの方法は、プログラムの単一のインスタンスを 1 回使用して、単一のレポートを作成するか、単一の分析を実行するときに使用されます。もう 1 つの方法は、情報をリアルタイムで収集および処理する長時間にわたるタスクに使用されます。詳しくは、各コンポーネントに関するセクションを参照してください。

ネットワーク負荷

zSecure Admin and Audit では、大きなネットワーク負荷が発生することはありません。しかし、両アプリケーションには、zSecure サーバー (プログラム CKNSERVE) を使用して、リモートでレポート作成と分析を行うためのオプションも用意されています。zSecure サーバーを使用してリモート・データにアクセスする場合のネットワーク負荷は、レポートに必要なデータによって異なります。CKRCARLA を呼び出すたびに、選択したレポートに必要なすべてのデータが転送されます。標準的な監査レポートでは、CKFREEZE データ・セット全体と、RACF データベース全体が含まれることも少なくありません。CKFREEZE データ・セットを指定しない場合は、ミニ CKFREEZE が使用されます。ミニ CKFREEZE のサイズは約 1 MB です。このデータ・セットは、常に全体が転送されます。

RACF レポートでは、zSecure Server によってレポートに必要な数のプロファイルだけが転送される場合と、セキュリティー・データベース全体が転送される場合があります。これは、照会で使用する選択基準と、レポートの対象となる情報によって決まります。ACF2 レポートおよび SMF レポートでは、すべてのデータが転送され、選択はクライアント・アプリケーションで行われます。

zSecure Server は、TCP/IP を使用した Point-to-Point 接続を行います。このサーバーは、単一のリスニング・ポート (構成時に指定可能) と、構成済みのパートナー・サーバーごとに 1 つの一時ポートを使用します。情報の取得元、またはコマンドの送信先となるすべてのシステムで、サーバーがアクティブになっている必要があります。

zSecure Admin

zSecure Admin 製品は、複数のサブコンポーネントで構成されており、各コンポーネントには、それぞれ独自のストレージ特性があります。zSecure Admin および Audit では、zSecure サーバーによって提供されるサービスを利用できます。それによって発生するネットワーク負荷については、『ネットワーク負荷』を参照してください。以下の段落では、DASD ストレージと仮想ストレージの予想される使用量、および必要な CPU 時間について説明します。

プロファイルの使用に関する情報を収集する場合は、これらのプロファイルを使用できるすべてのシステムで zSecure アクセス・モニター開始タスクを実行する必要があります。

DASD ストレージ

zSecure Admin and Audit における DASD の使用法は、以下のセクションで示すカテゴリーに分類されます。

CKFREEZE データ・セット: zSecure Admin の日常的な使用法では、タイプ「通常管理」の CKFREEZE データ・セットを使用できます。管理対象の各システムにつき 1 つのデータ・セットが必要です。共有 DASD を使用する場合は、CKFREEZE データ・セットのうち 1 つだけに対して、SHARED=YES パラメーターを指定して作成する必要があります。

RACF データベース内のストレージ: キューに入れられたコマンドや時間調節されたコマンド用に追加のスペースが必要です。ほとんどの状況では、RACF データベース内の追加スペースは無視できる程度のものです。

RACF データベースのアンロード: RACF データベースの UNLOAD コピーは、Admin および Audit のレポートを生成するためのフリーズ済み入力として使用できます。アンロードのサイズは、RACF データベースまたは ACF2 データベースの使用済み部分とほぼ同じです。アンロード・データ・セットは、必要な数だけ保持できます。

UNLOAD ファイルのすべての機密フィールドは常にアスタリスクで置換されます (マスクされます)。したがって、コピー操作および再作成操作中には複製されません。

アクセス・モニター・データ・セット: アクセス・モニター・データ・セットのサイズは、環境によって大きく変動することがあります。情報を長期間にわたって保持する場合は、大量のデータが累積、保持される可能性があります。このデータの一部はテープ上に保存できますが、ほとんどのデータは並列アクセスの対象となるため、アクセス・モニター・データ・セットを複数のテープに保存し、同時にマウントする必要があります。統合プロセスによってデータ量を減らすこともできますが、構成プロセスを組織のニーズに合わせて調整する必要があります。

RACF データベースのコピー: RACF データベースのコピーは、オフライン・コンポーネントを使用するために必要です。サイズと数は、使用法によって異なります。多くの場合、オフライン RACF データベースは、システム RACF データベースのコピーです。RACF データベースのコピーは、Admin および Audit のレポートを生成するためのフリーズ済み入力としても使用できます。

仮想ストレージ

RACF ベースまたは ACF2 ベースの標準的な照会では、必要な仮想ストレージの量は出力レポートのサイズと同程度です。適切な SELECT ステートメントを使用することで、ほとんどのレポートを管理可能なサイズに抑えることができます。

アクセス・モニター・データの処理のリソース使用量: アクセス・モニター・イベントのレポート作成は、2 つのタイプのレポートで実行できます。つまり、RACF データベースのプロファイルに基づくレポート、または記録されたイベントに基づくレポートです。RACF データベースのプロファイルに基づくレポートは、他の RACF レポートと同様、サイズが小さく、必要な仮想ストレージの量もわずかです。記録されたイベントに基づくレポートは、イベントのタイプ、および入力データの統合レベルによっては、サイズが非常に大きくなる場合があります。そのた

め、レポートに必要な仮想ストレージの量も、非常に多くなる場合があります。1 GB の仮想ストレージを必要とするレポートも珍しくありません。レポートの対象となるイベント、ユーザー、プロファイル、またはリソースのタイプを慎重に選択することで、必要な仮想ストレージの量を大幅に減らすことができます。

アクセス・モニター・データ・セットの統合にも、大量の仮想ストレージが必要になる場合があります。サイズの制限を克服するため、アクセス・モニター・データ・セットの内部フォーマットが最近変更されました。2 つのフォーマットは、それらが導入された時のリリース番号によって、1.11 フォーマットまたは 1.13 フォーマットと呼ばれます。1.11 フォーマットのデータを統合するには、仮想ストレージ内ですべての入力データを処理し、保持する必要があります。1.13 フォーマットを使用すると、統合プロセスの開始時からレコードを直接出力データ・セットに書き込むことができるため、プログラムの存続期間を通してレコードをストレージに保持しておく必要がありません。1.13 フォーマットでは、統合プロセスを 32 MB 以下の領域サイズで実行できます。

すべての新しいアクセス・モニター・データ・セットでは、1.13 フォーマットのアクセス・モニター・データが使用されます。既存の 1.11 フォーマットのアクセス・モニター・データと、新しい 1.13 フォーマットのアクセス・モニター・データを、レポート作成や分析の目的で混合することもできます。1.11 フォーマットのデータを 1.13 フォーマットのデータに統合する場合は、まず既存の 1.11 フォーマットのデータ・セットを 1.13 フォーマットに変換する必要があります。変換プロセスのストレージおよび CPU 要件は、以前の統合プロセスとほぼ同じです。変換が終了すると、より効率的な新しい統合プロセスを使用してデータ・セットを統合できます。

アクセス・モニター・データの収集のリソース使用量**:** アクセス・モニター・データを収集する開始タスクでは、計測間隔中に発生するすべてのイベントの情報を保持できるだけの十分なバッファー・スペースが必要です。バッファー・スペースは、アクセス・モニター開始タスクのプライベート領域内にあります。デフォルトの計測間隔は 1 分です。必要なストレージの量は、1 分間に発生するイベントの数によって異なります。例えば、1 秒間に 1000 個の RACF アクセス・イベントが発生する場合、バッファー・ストレージのスペースは、1000 イベント/秒 * 60 秒 * 100 バイト = 6 MB と算出されます。通常、アクセス・モニターは、32 MB 以下の領域サイズで実行できます。

CPU 時間

zSecure プログラムの実行に必要な CPU 時間は、2 つの異なる方法のいずれかで表現する必要があります。1 つ目の方法は、プログラムの単一のインスタンスを 1 回使用して、単一のレポートを作成するか、単一の分析を実行するときに使用されます。これは、zSecure Admin および zSecure Audit を使用して、対話式の処理や一括処理を行う場合に適用されます。2 つ目の方法は、zSecure Admin アクセス・モニターのように、情報をリアルタイムで収集および処理する長時間にわたるタスクに使用されます。

zSecure Admin: zSecure Admin を使用した対話式またはバッチ形式レポートの作成に必要な CPU 時間は、分析対象データのサイズと結果のレポートのサイズに左右されます。標準的なレポートの作成にかかる時間は数秒間です。サイズの大きなレポートの場合は、数分かかる場合もあります。1.11 フォーマット (旧フォーマ

ット) のアクセス・モニター・データを統合する場合は、データの量が多いために、かなりの CPU 時間がかかる可能性があります (数 10 分)。同様に、収集された大量のアクセス・モニター・イベントのレポート作成にも、同程度の CPU 時間が必要になる可能性があります。

アクセス・モニター開始タスク: アクセス・モニター・イベントを収集するための長時間にわたるプロセスにも、CPU 時間が必要です。プロセッサーの速度やイベントの数が多岐にわたるため、この CPU 時間を絶対項で表現するのは困難です。情報の収集および記録に必要な時間の、CPU に依存しない指標は、CPU サービス単位 (SU) の数です。単一のイベントを収集して記録するには、約 1 CPU SU が必要です。

CPU サービス単位を CPU 時間に関連付けるには、プロセッサーに対して定義されている SU/SEC 定数、および IPS または WLM 構成で指定された CPU サービス定義係数を使用します。アドレス・スペースおよびシステムの報告された SU 数に、サービス定義係数 (SDC) を掛けます。SDC のデフォルト値は 10 です。以下の例を参照してください。

- インストール済み環境で、CPU の SDC に対してデフォルト値、IO および MSO の SDC に対して 0 が指定されているとします。
- アプリケーションは IBM zEnterprise 114 モデル Z01 (2818-Z01) 上で稼働しています。このプロセッサーの CPU モデル係数は 40100.2506 です。
- アプリケーションで現在発生している RACF イベントの数は 20 です。
- アプリケーションが現在使用している CPU 時間は 2 秒です。
- 報告されるこのアプリケーションのサービス単位の総数は、10 (SDC) * 40100 (CPU 係数) * 2 (秒) = 802000 サービス単位となります。
- アクセス・モニターの開始後、これらのイベントに関する情報の収集および報告に必要な CPU 時間の合計は、20 (イベント) * 1 (SU) / 40100 (CPU 係数) = 0.0005 秒となります。
- 報告されるこのアプリケーションのサービス単位の総数は、802000 (ベース) + 20 (イベント) *1 (SU) * 10 (SDC) = 804000 サービス 単位となります。

zSecure Audit

zSecure Audit 製品には、セキュリティー・データベース (RACF または ACF2) 内の情報に関するレポート作成、システム内で発生したイベント (SMF) に関するレポート作成、およびセキュリティー環境の詳細な分析のための機能が用意されています。zSecure Audit では、zSecure Server によって提供されるサービスを利用できます。それによって発生するネットワーク負荷については、前のセクションを参照してください。以下の段落では、データ・セットのサイズ、必要な仮想ストレージ、および CPU 時間の要件について説明します。

DASD ストレージ

DASD 上のデータ・ストレージは、主に CKFREEZE データ・セットに使用されます。zSecure Server を使用せずに複数の非共有システムからレポートを生成する場合は、追加のストレージが必要になる場合があります。その場合は、他のシステムの RACF データベースまたは ACF2 データベースのコピー用に DASD スペースが必要になります。

CKFREEZE: この情報には、多数のシステム制御ブロック、データ・セットおよび UNIX ファイルの名前、さらにはいくつかのデータ・セットの内容 (の一部) が含まれます。この情報は、多くの zSecure 製品によって使用されます。

ライブラリーの変更分析を実行する場合は、チェックサム情報付きの CKFREEZE データ・セットも必要です。これらのデータ・セットのうち複数が必要になる場合があります。

CKFREEZE データベースの標準的なサイズは、オンラインの DASD ボリュームの数と、UNIX ファイルの数に左右されます。

フルサイズ ***CKFREEZE:*** 共有 DASD 環境では、システムごとに 1 つの CKFREEZE データ・セットが必要です。以降のセクションで示すパラメーターのうちいくつかを使用することにより、必要な DASD の総量を減らすことができます。

SHARED=YES/NO: 共有 DASD を使用する場合は、CKFREEZE データベースの作成時に SHARED パラメーターを指定することで、必要なスペースを減らすことができます。DASD を共有するシステムのうちいずれか 1 つだけで、パラメーター SHARED=YES を指定します。その他すべてのシステムでは、SHARED=NO と指定します。これにより、共有ディスクのデータが 1 回だけ収集される一方で、非共有ディスクのデータも収集されます。

BCD=NO: 現在、バックアップ制御データ・セットは、個別データ・セット・プロファイルを削除するかどうかを決定するためだけに使用されます。これらの個別データ・セット・プロファイルは、各種の **AU.V** 検査機能で処理され、RACF プロファイル・レポート (**RA.3.1**) でレポートされます。いずれの個別データ・セット・プロファイルも使用しない場合、または RACF プロファイル・レポートを頻繁に実行しない場合には、このフィーチャーを使用不可にしても構いません。

この情報は、VERIFY ONVOLUME ステートメント (オプション **AU.V** で対話的に使用可能) および REPORT_PROFILE NEWLIST (オプション **RA.3.1** で対話的に使用可能) で使用されます。

UNIX=NO: UNIX データは、かなりの量のディスク・スペース (すべてのディレクトリー、所有者データ、およびファイル許可が格納される) を必要とします。UNIX データは、TRUSTED レポート、SENSITIVE データ・セット・レポート (HFS データ・セットの機密性)、および UNIX ファイル・システムの監査に使用されます。 UNIX ファイルに関連する SMF レコードには、そのファイルへのパスが含まれないことがよくあり、CKFREEZE 情報を使用して適切なパスを表示できます。UNIX データがない場合でも、大部分のレポートは依然として使用可能な結果を提供しますが、その結果は不完全です。HFS データ・セットまたは zFS データ・セットの監査を行わない場合は、この機能を無効にします。zFS データ・セットおよび HFS データ・セットのサイズによっては、UNIX 情報の収集に多くの時間がかかる場合があります。

この情報は、以下の NEWLIST タイプで使用されます。

- UNIX (RE.U)
- TRUSTED (AU.S)
- REPORT_SENSITIVE (AU.S)

- DSN (AU.S)
- SENSDSN (AU.S)
- SMF (EV)

TCPIP=No、***IMS=NO***、***CICS=NO***、***DB2=NO:*** IMS、CICS、および DB2 データは通常、大量のディスク・スペースを必要としません。システム上の TCP/IP スタックに関する情報についても同じです。しかし、TCP/IP、IMS、DB2、または CICS に関するレポートを作成しない場合は、関連情報を収集する必要もありません。TCP/IP、IMS、DB2、または CICS 環境の監査を行わない場合は、これらの機能を無効にします。

この情報は、主に以下の NEWLIST タイプで使用されます。
- IP_* (RE.I)
- IMS_* (RE.M)
- CICS_* (RE.C)
- DB2_* (RE.D)
- TRUSTED (AU.S/RACF user/TRUSTED および AU.S/RACF resource/Sensitive trust)
- REPORT_SENSITIVE (AU.S/RACF resource/Sensitive profiles)

SMF データ: SMF データは、zSecure Audit だけで使用されるデータではありません。言うまでもなく、特定期間のイベントに関するレポートを作成する場合は、その期間の SMF データを用意しておく必要があります。必要なデータは、テープまたは DASD に保存できます。SMF イベントに関するレポートを作成する場合は、SMF データ・セットが順次処理されます。このため、同じテープ上に SMF レコードを含む複数のデータ・セットが存在する場合があります。

仮想ストレージ

SMF イベントのレポートを作成する場合は、必要な仮想ストレージが膨大になる可能性があります。ほとんどのタイプのレポートでは、必要な仮想ストレージは、出力レポートのサイズと同程度です。例えば、400 万個の SMF レコードの詳細情報付きレポートを生成する場合は、プログラムがこれらのレコード内で発生するすべての固有のフィールド値を保持するだけの十分なスペースが必要です。標準的なレポートの必要仮想メモリーは、最大 250 MB です。必要な仮想ストレージは、レポートの対象となるイベント、ユーザー、またはリソースのタイプを慎重に選択することで、大幅に減らすことができます。

CPU 時間

zSecure Audit を使用した対話式またはバッチ形式レポートの作成に必要な CPU 時間は、分析対象データのサイズと結果のレポートのサイズに左右されます。標準的なレポートの作成にかかる時間は数秒間です。サイズの大きなレポートの場合は、数分かかる場合もあります。サイズの大きな SMF サマリー・レポートの場合は、データの量が多いため、生成にかなりの CPU 時間がかかる可能性があります。

- zSecure Admin
- zSecure Server
- アクセス・モニター
- RACF-Offline

zSecure Alert

zSecure Alert は複数のリソースを使用します。この製品には、少なくとも 1 つの CKFREEZE データ・セットが必要ですが、拡張モニタリング用に複数の専用 CKFREEZE データ・セットが使用される場合もあります。アラートの生成対象となるすべてのシステムで、zSecure Alert 開始タスクを実行する必要があります。

DASD ストレージ

zSecure アラートには、少なくとも 1 つの CKFREEZE データ・セットが必要です。これは専用の CKFREEZE データ・セットで、通常監査 CKFREEZE データ・セットと同等のサイズです。拡張モニタリングが有効になっている場合、zSecure Alert では、複数の一時 CKFREEZE データ・セットの作成および削除も行われます。これらの拡張モニタリング CKFREEZE データ・セットは、ミニ CKFREEZE データ・セットと同等のサイズです。これらの拡張モニタリング CKFREEZE データ・セットの数は構成可能です。これらのデータ・セットは、最低 2 つ必要です。

仮想ストレージ

アラート・イベントをインターセプトする開始タスクでは、計測間隔中に発生する選択したすべてのイベントの情報を保持できるだけの十分なバッファー・スペースが必要です。バッファー・スペースは、zSecure Alert 開始タスクのプライベート領域内にあります。デフォルトの計測間隔は 1 分です。通常、SMF イベントは、アクティブなアラートに基づいて、レコード・タイプごとに事前フィルタリングされます。WTO レコードは、同様の方法で、メッセージ ID ごとに事前フィルタリングされます。この事前フィルタリングは、ISPF ユーザー・インターフェースでのアラートの指定に基づいて自動的に行われます。必要なストレージの量は、1 間隔内に発生するイベントの数によって異なります。例えば、1 秒間に 500 個の SMF レコードが事前フィルタリングを通過する場合、バッファー・ストレージのスペースは、500 イベント/秒 * 60 秒 * 1000 バイト = 30 MB と算出されます。

必要なストレージの量は、長時間にわたるアラートにも影響されます。これらのアラートは、単一のイベントを基準にするのではなく、特定の間隔の間に発生するイベントの数をカウントします (5 分間に 20 回のログオンなど)。これらのタイプのアラートでは、より長時間にわたるデータを用意する必要があります。このため、必要なバッファー・スペースの量が多くなります。

通常、zSecure Alert のアドレス・スペースは、256 MB 以下の領域サイズで実行できます。

CPU 時間 zSecure Alert データ収集

アラート・イベントを収集するための長時間にわたるプロセスにも、CPU 時間が必要です。プロセッサーの速度やイベントの数が多岐にわたるため、この CPU 時間を絶対項で表現するのは困難です。情報の収集および記録に必要な時間の、CPU に依存しない指標は、CPU サービス単位 (SU) の数です。単一の SMF イベントまたは WTO イベントを収集して記録するには、約 1 CPU SU が必要です。

報告される CPU サービス単位を CPU 時間に関連付けるには、プロセッサーに対して定義されている SU/SEC 定数、および IPS または WLM 構成で指定された

CPU サービス定義係数を使用します。アドレス・スペースおよびシステムの報告された SU 数に、サービス定義係数 (SDC) を掛けます。SDC のデフォルト値は 10 です。次の例を参照してください。

- インストール済み環境で、CPU の SDC に対してデフォルト値、IO および MSO の SDC に対して 0 が指定されているとします。
- アプリケーションは IBM zEnterprise 114 モデル Z01 (2818-Z01) 上で稼働しています。このプロセッサーの CPU モデル係数は 40100.2506 です。
- アプリケーションで現在発生している SMF イベントの数は 50 個です。
- アプリケーションが現在使用している CPU 時間は 2 秒です。
- 報告されるこのアプリケーションのサービス単位の総数は、10 (SDC) * 40100 (CPU 係数) * 2 (秒) = 802000 サービス単位となります。
- zSecure Alert の開始後、これらのイベントに関する情報の収集および報告に必要な CPU 時間の合計は、50 (イベント) * 1 (SU) / 40100 (CPU 係数) = 0.002 秒となります。
- 報告されるこのアプリケーションのサービス単位の総数は、802000 (ベース) + 50 (イベント) * 1 (SU) * 10 (SDC) = 807000 サービス単位となります。

zSecure Alert アラート生成の CPU 時間

zSecure Alert のアラート発行フェーズでも、仮想ストレージや CPU 時間などのリソースが必要になります。非常に多くのアラートを同時に発行する場合を除き、仮想ストレージの量は、通常、無視できる程度のものです。アラート発行フェーズの CPU 時間は、事前フィルタリングを通過するイベント・レコード (SMF および WTO) の数に左右されます。通常、収集したレコードの処理とアラートの生成に必要な時間は、各アラート間隔 (デフォルトでは 1 分) につき 1 秒未満です。必要な CPU 時間は、選択したアラート・タイプに若干左右されます。

夏時間調整に関する考慮事項

zSecure Collect が時間帯情報を z/OS から収集し、zSecure Audit が時間帯を含むレポートでこの情報を使用します。したがって、夏時間 (DST) への変更など、時間帯が変更された場合には、CKFREEZE データ・セットをリフレッシュします。zSecure 製品の場合には、それ以上、夏時間調整に関する考慮事項はありません。

フレッシュな CKFREEZE および UNLOAD の毎日の使用

zSecure Audit のすべての機能、および zSecure Admin の多数の機能では、CKFREEZE データ・セットが必要です。いくつかの機能では、UNLOAD を使用することも提案できます。フレッシュ・コピーを使用可能にするには、実動プロセスにジョブ C2RJPREP を組み込みます。

DFSMShsm (または DFHSM) データ・セット・マイグレーションと並行して実行するように、ジョブ CKRJPREP をスケジュールしないでください。これを行うと、不完全な CKFREEZE が発生する場合があります。

複数のイメージを持っている場合には、各システムから CKFREEZE データ・セットを作成する必要があります。共有セキュリティー・データベースの場合には、最

上位の z/OS を持つシステムから UNLOAD データ・セットを作成します。NJE ルーティング、システム・アフィニティー、またはその両方を指定して、各ジョブが意図したシステム上で確実に実行されるようにする必要が生じる場合があります。

SMF レコードを処理するプロセスへの 2 次入力として、CKFREEZE データ・セットを使用する場合があります。そのようなプロセスの例として、QRadar LEEF データの生成があります。ご使用のインストール環境で DB2 監査レコードが SMF に書き込まれる場合、SMF レコードを CKFREEZE データ・セットからの情報を使用して拡充することができます。テーブルおよびデータベース名に対する DB2 オブジェクト ID (OBID) の解決を可能にするには、CKFCOLL プログラムでオプション DB2CAT=YES を使用するようにしてください。 このオプションは、CKFCOLL プログラムへの入力パラメーターとして明示的に指定したり、あるいはデフォルト値に設定することができます。

日次の CKGRACF ジョブ実行の要件

日次 CKGRACF ジョブ C2RJXRFR は、zSecure Admin コンポーネントにのみ適用されます。これは、zSecure Admin のキューに入れられたコマンドまたは複数権限機能を使用する場合、あるいは zSecure Visual を使用する場合に必要です。複数イメージで RACF データベースを共有する場合には、最上位の z/OS を持つシステム上で日次 CKGRACF ジョブを実行します。 NJE ルーティング、システム・アフィニティー、またはその両方を指定して、ジョブが意図したシステム上で確実に実行されるようにする必要が生じる場合があります。

RACF Exit Activator のセットアップ

RACF Exit Activator プログラム C2XACTV は、一部の RACF 出口に対する動的出口サポートを提供します。C2XACTV の主な目的は、各種 zSecure 製品で必要な出口をインストールすることです。例えば、zSecure Admin アクセス・モニター・コンポーネントは C2XACTV を使用して、アクセス・イベントおよび認証イベントをインターセプトするために必要な RACF 出口をインストールします。

ほとんどの場合は、RACF Exit Activator プログラムを使用して明示的に出口を制御する必要はありません。zSecure Admin でアクセス・モニター機能を使用する場合は、アクセス・モニターの開始時または停止時に、関連する出口が自動的にアクティブ化または非アクティブ化されます。

また、必要に応じて、上記プロシージャーの制御とは別に、C2XACTV プログラムを直接実行することもできます。C2XACTV を開始して出口をアクティブ化するには、zSecure に付属の以下の C2RCACTV プロシージャーを使用します。プロシージャー内のデータ・セット名とパラメーターを編集して、ご使用のサイトで使用する値を反映させます。

```
// JCLLIB ORDER=(MY.CKRPARM,CKR.SCKRPROC)
// EXEC  C2RCACTV,CONFIG=MYCONFIG,PARM='DYNEXIT ACTIVATE ICHPWX02'
```

C2XACTV プログラムを使用すると、提供されているステートメントを使用して、サポートされている出口を直接制御できます。C2XACTV の入力ステートメントに関する追加情報については、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」のプログラム資料を参照してください。

注: RACF Exit Activator プログラムは、RACF の前出口、主出口、および後出口に対する完全なサポートを提供するため、既に独自の RACF 出口ルーチンがある場合、それらはサブ出口として保持されます。

RACF Exit Activator プログラムの動的出口サポートの使用

RACF 出口を C2XACTV によってインストールする場合、MVS 動的出口モードまたは DIRECT モードを使用してインストールできます。メインルーチンは、複数のルーチンをサブ出口 として呼び出すルーター・プログラムからなります。 MVS 動的出口モードを使用する場合は、追加のサブ出口ルーチンを動的に追加、変更、および削除できます。例えば、zSecure によって提供されるものに加えて独自のバージョンの新規パスワード出口を提供するには、該当する PROG*xx* parmlib メンバーからの出口点を指す必要があります。以下に例を示します。

```
EXIT ADD EXITNAME(C2X.ICHPWX01) MODNAME(your-module-name)
     DSNAME(your-library) STATE(ACTIVE)
```

混乱を避けるため、ご使用のインストール用に定義された新規パスワード出口には、ICHPWX01 という名前を使用しないでください。ICHPWX01 という名前は、RACF によって呼び出されるモジュールのために予約されており、メインの zSecure RACF ルーター・プログラム自体で既に使用されている名前です。

zSecure の新規パスワード出口を他の新規パスワード出口と一緒に使用する

独自のバージョンの新規パスワード出口を提供するには、RACF Exit Activator によって提供されるものに加えて、該当する PROGxx parmlib メンバーからの出口を指す必要があります。以下に例を示します。

```
EXIT ADD EXITNAME(C2X.ICHPWX01) MODNAME(your-module-name)
         DSNAME(your-library) STATE(ACTIVE)
```

混乱を避けるため、ご使用のインストール用に定義された新規パスワード出口には、ICHPWX01 という名前を使用しないでください。その名前は、zSecure RACF 新規パスワード・ルーター自体によって既に使用されています。

TCP/IP ドメイン・ネームの解決

zSecure は、SNMP (Simple Network Management Protocol) および SMTP (Simple Mail Transport Protocol)、つまり E メールを含めて、各種のフォーマットでレポート作成を行うことができます。この点において、zSecure は TCP/IP サービスのユーザーとして動作します。その結果として、zSecure が稼働する環境では、ドメイン・ネームの解決が必要になる場合があります。環境は、TSO ユーザーまたは CMS ユーザー、バッチ・ジョブ、あるいは zSecure Alert または zSecure Visual の開始タスクとすることができます。ご使用の IP スタックのレベルに応じて、*userid*.TCPIP.DATA、または SYSTCPD DD ステートメント、または DNS 機能を提供する TCP スタックを指す何らかの方法をセットアップする必要があります。詳細については、ご使用の z/OS リリースの z/OS Knowledge Center にアクセスして、「**Communications Server**」->「**IP Configuration Reference** 」を参照してください。また、ドメイン・ネームの解決を必要とするプロセスが、TCPIP.DATA、/etc/resolv.conf、および /etc/hosts など、関連するすべてのファイルに対して READ アクセス権限を持つことを確認してください。

SMTP サーバーに関する考慮事項

レポートは、特に XML フォーマットの場合には大きくなる傾向があります。レポートを E メールで送信する場合には、サイズが問題になる場合があります。レポートが大きすぎると、SMTP サーバーによって拒否されたり、切り捨てられたりする可能性があります。大きすぎるファイルの送信での問題を防止するために、ご使用の SMTP サーバーの MAXMAILBYTES 設定と CHECKSPOOLSIZE 設定を確認し、場合によっては変更してください。

第 9 章 リモート・データ・アクセスおよびコマンド・ルーティングのためのセットアップ

zSecure は、複数システムからのプロファイル、リソース、および設定の管理と監査に使用できます。zSecure で各システムから直接情報を収集するように、対象システムの入力データ・ソースを構成することができます。それらのデータ・セットは、ISPF インターフェースまたは CARLa プログラムを通して使用できます。単一セッションからの複数システムのレポート作成と管理が可能になるため、この機能は、多重システム・サポートと呼ばれています。

多重システムのレポート作成に加えて、この製品は、zSecure サービスまたは既存の RACF RRSF サービスを使用して、リモート・システムで実行されるコマンドのルーティングもサポートしています。リモート・システム・ルーティングのサポートを含めて、zSecure は、コマンド・ルーティング・オプションとして、ローカル・システムへのルーティング、あるいは NJE バッチ・ジョブ、RACF RSSF サービスまたは zSecure サービスを使用したリモート・システムへのルーティングを提供しています。

これらの機能を提供するために、zSecure Admin and Audit は TCP/IP サービスを使用します。zSecure Server は接続を管理し、データ・トランスポートを処理します。zSecure サービスを使用してリモート・データへのアクセスとコマンド・ルーティングを行うために、zSecure Server をインストールして活動化する必要があります。以下のセットアップ・タスクは、リモート・システムに対するサポートを提供します。

- zSecure Server のインストール、構成、および活動化。『zSecure Server のインストールおよび構成』を参照してください。
- CKRCARLA または ISPF ユーザー・インターフェースで使用するためのリモート・データ・セットの指定。 67 ページの『zSecure Server のオペレーター・コマンド』を参照してください。
- RACF コマンドと選択された非 RACF コマンドを他のシステムにルーティングするためのセットアップ。 68 ページの『AT-TLS を使用したセキュアなコミュニケーション』を参照してください。

zSecure Server のインストールおよび構成

zSecure Server をインストールして構成するには、以下のセクションを参照してください。

インストール済みソフトウェアと多重システム・サポート

zSecure CARLa ベースのインストール・プログラムは、zSecure 多重システム・サポートで必要なコードとパネルをインストールします。SMP/E を適用した後、すべての必須ソフトウェアが標準ライブラリーで使用可能になります。zSecure 多重システム・サポートでは、新しいライブラリーは追加されません。SCKRLOAD ライブラリーには、APF 許可が必要です。

JCL プロシージャーとパラメーター

zSecure Server のコードは、CKNSERVE ロード・モジュールで提供されています。このプログラムは、開始タスクとして実行されますが、バッチ・ジョブとしても実行できます。再使用可能なアドレス・スペースでプログラムを実行できるため、開始タスクとして実行するのが望ましい方法です。バッチ・ジョブは、再使用可能なアドレス・スペースでは実行できません。開始タスクとしてプログラムを実行するプロシージャーは、サンプル CKNSERVE に提供されています。

CKNSERVE プロシージャーは、組み込みメンバー C2R$PARM を参照します。C2R$PARM は、JCL SET ステートメントを含むサンプル・メンバーであり、一般に *zSecure* 構成 と呼ばれます。メンバー C2R$PARM (または置換対象として選択する任意のメンバー) は、CKRPARM データ・セットに配置されています。 31 ページの『zSecure 構成データ・セットについて』を参照してください。

zSecure 構成は、組織によってデータ・セット名、メンバー、およびその他のオプションの指定に使用されるメイン構成ファイルです。zSecure 構成は、開始タスク JCL ファイルの INCLUDE で使用可能でなければなりません。通常、zSecure 構成ファイルは、開始タスク・プロシージャー・ライブラリー内のメンバーである必要があります。すべての zSecure プログラムで使用されるシンボルのほかに、zSecure 構成ファイルには、CKNSVPRM シンボル (CKNSERVE に固有) がセットされている必要があります。

```
//  SET CKNSVPRM=<installation-specified-parmlib>
```

<*installation-specified-parmlib*> は、通常、zSecure Server 用に準備した CKRPARM データ・セットで置換しますが、レコード・フォーマット FB の任意の区分データ・セットおよび論理行長 80 を指定できます。レコード内の位置 73 から 80 は無視されます。このデータ・セットは、JCL プロシージャー内の PPARM パラメーターと PCOMMON パラメーターによって示される 2 つのメンバーを含む必要があります。これらの 2 つのメンバーは、一緒に *zSecure-Server* の構成 ファイルを構成します。

注**:** zSecure 構成 (一般に C2R$PARM と呼ばれます) と zSecure Server 構成 (PPARM と PCOMMON によって識別される 2 つのメンバーで構成されます) を混同しないでください。

CKNSERVE プロシージャーは、CKNSVPRM データ・セット内のメンバー CKNCKFAI も参照します。CKNCKFAI メンバーには、ミニ CKFREEZE の作成を制御する zSecure Collect パラメーターが含まれています。通常、このメンバーに含まれているキーワードとパラメーターはいずれも変更する必要はありません。SCKRCARL ライブラリーからコピーすることができます。

PPARM によって指定されるメンバーは、zSecure Server の特定のインスタンスに固有の構成パラメーターを含むように意図されています。それとは対照的に、PCOMMON によって指定されるメンバーは、すべての zSecure Server に共通のパラメーターを含むように意図されています。サーバー固有の PPARM メンバーの例は、次のとおりです。

```
OPTION   Ownsys(PRODSYS2) servertoken(MyToken)
```

通常、PPARM メンバー内に存在する唯一のステートメントは、SERVERTOKEN を識別する OPTION ステートメントです。OPTION ステートメントには、通常は必要ではない複数の追加キーワードがあります。例えば、OWNSYS キーワードが必要になるのは、ローカル・システムの現在の TCPIP ドメイン・ネームまたは TCPIP ホスト名に一致する ZSECSYS 項目が複数ある場合のみです。 OPTION ステートメントについて詳しくは、 62 ページの『構成ファイル OPTION ステートメント』を参照してください。

以下の例は、共有 PCOMMON メンバーを示しています。

```
ZSECNODE NAME(ZSNODE1)
ZSECSYS  NAME(ZSSYST1) ZSECNODE(ZSNODE1) IPADDR(MyNode) IPPORT(7173)
ZSECNODE NAME(TSTNODE1)
ZSECSYS  NAME(TSTSYS1) ZSECNODE(TSTNODE1) IPADDR(MyTest) IPPORT(7173)
ZSECNODE NAME(PRODNODE)
ZSECSYS  NAME(PRODSYS1) ZSECNODE(PRODNODE),
 ipaddr(prodsys1.mydomain.com),
 IPPORT(7174)
ZSECSYS  NAME(PRODSYS2) ZSECNODE(PRODNODE),
 ipaddr(prodsys2.mydomain.com),
 IPPORT(7173)
```

例で説明したように、両方のファイル内のステートメントは、コンマを行継続文字として使用して、複数行にわたって分割することができます。

注: 行は、キーワード間でのみ分割することができ、キーワードやパラメーター中で分割することはできません。

構成ステートメントについて詳しくは、 62 ページの『構成ステートメント』を参照してください。

開始タスクのセキュリティー定義

タスクに割り当てられた**ユーザー ID** には、十分な許可があることを確認してください。これらの許可は次のとおりです。

- JCL プロシージャー内で参照されるすべてのデータ・セットを読み取る許可
- TCPDATA データ・セットおよびその他の TCP/IP 制御データ・セットを読み取る許可 (TCPXLBIN など)
- OMVS セグメントまたはデフォルトの OMVS UID を使用した、UNIX 機能に対するアクセス権限。userid は、任意の UID を持つことができます。これは、特定の UNIX 許可、ファイル・アクセス、さらにホーム・ディレクトリーも必要としません。
- 現行 TCP/IP スタックを記述する SERVAUTH リソースに対する READ アクセス権限。これらのリソースのフォーマットは、次のとおりです。

  EZB.STACKACCESS.*<sysname>*.*<stackname>*
- FACILITY クラスの IRR.DIGTCERT.LISTRING リソースに対する READ アクセス権限。

zSecure Server をデプロイするすべてのシステム上で、CKNRACF1 ジョブを使用してこれらの正規の許可をセットアップします。

加えて、userid に対して、他の zSecure Server との通信を検証および暗号化するための証明書を割り当てる必要があります。ネットワーク接続を保護するための要件については、 68 ページの『AT-TLS を使用したセキュアなコミュニケーション』を参照してください。

構成ステートメント

zSecure Server の構成ステートメントは、zSecure-Server の構成ファイルに提供されています。サンプル STC プロシージャーに示すように、このファイルは、連結された複数のメンバーやデータ・セットにわたって分割できる論理ファイルです。構成ファイルでは、2 つの必須ステートメントと 2 つのオプションのステートメントが使用されます。

- 必須ステートメントは、ZSECNODE と ZSECSYS です。
- オプションのステートメントは、OPTION です。

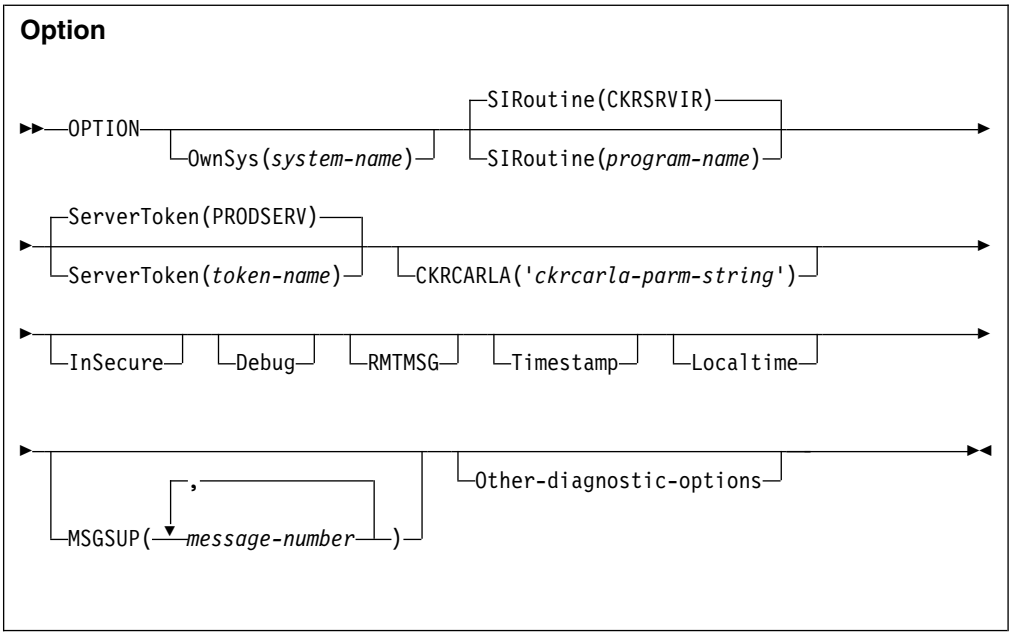
ZSECNODE ステートメントは、RACF データベースを共有するシステムのセットを定義します。ZSECSYS ステートメントは、zSecure Server アドレス・スペースを実行できる個々のシステムを定義します。ご使用の環境を記述するのに必要な数の ZSECNODE ステートメントと ZSECSYS ステートメントを記述できます。ほとんどの場合、ユーザーは zSecure UI セットアップに ZSECNODE を指定します (またはデフォルトでそうなります) が、ユーザーによっては、特定のシステムにのみ存在する特定のデータ・セットを参照する ZSECSYS を使用する場合があります。

zSecure-Server の構成ファイル内のステートメントの順序は重要です。ZSECNODE ステートメントは、ZSECNODE を参照する ZSECSYS ステートメントの前にある必要があります。

大部分のインストールでは、ステートメントは、ZSECNODE ステートメントと ZSECSYS ステートメントを、すべての zSecure Server で共有できるように編成されています。OPTION ステートメントのみ、特定の zSecure Server に固有です。システム上でアクティブなサーバーが 1 つのみの場合は、OPTION ステートメントも複数の zSecure Server で共有できます。zSecure Server は、ZSECSYS 定義上の IP アドレスおよび名前を、システムの TCP/IP ドメイン・ネームおよび IP ホスト名と比較します。一致が検出された場合、ZSECSYS 定義はローカル・システムで使用されます。同じ IP アドレスを使用する zSecure Server が複数定義されている場合は、いずれかのシステムが選択されます。どのシステムが使用されるかは、予測不能です。この場合、OPTION ステートメントに OWNSYS キーワードを付けて使用する方法が推奨されます。

構成ファイル OPTION ステートメント

通常は、OPTION ステートメントを使用する必要はありません。ただし、同じシステム上で複数のサーバーを実行する場合は、OPTION ステートメントを使用して、各サーバーに対して固有のパラメーターを指定する必要があります。また、OPTION ステートメントは、診断設定の指定にも使用できます。



キーワードとパラメーターには、次の意味があります。

OwnSys

このキーワードは、現行サーバーのシステム名を指定します。この値は、現行 TCP/IP スタックのホスト名に一致する ZSECSYS エントリーが複数存在する場合にのみ必要です。通常、ローカル・システム名は、ZSECSYS 定義の IPADDRESS に基づいて決定されます。同じ IPADDRESS 指定を持つ複数の ZSECSYS ステートメントが存在する場合で、OWNSYS が指定されていない場合には、可能な ZSECSYS エントリーの 1 つが現行サーバー用に使用されます。その場合、どの名前が使用されるかは予測不能です。

SIRoutine

このキーワードは、サーバー・インターフェース・ルーチンの名前を指定します。現在、このキーワードとパラメーターは無視されます。

ServerToken

このキーワードは、このサーバー用に使用されるグローバル・データ域のアンカーとして使用される名前付きトークンの名前に 8 文字の接尾部を指定します。指定された値には、値 CKNSERVE による接頭部が付きます。2 つのサーバーに対して同じ値が指定された場合、2 番目に始動されるインスタンスは失敗します。トークンのデフォルト値は PRODSERV です。このキーワードが指定されていない場合、デフォルト値が使用されます。複数の zSecure Server を同じシステム上で実行している場合のみ、**ServerToken** の値を指定する必要があります。

CKRCARLA

CKRCARLA キーワードを使用して、CARLA ステートメントを CKRCARLA 呼び出しパラメーターに追加することができます。このキーワードは、プログラム呼び出しパラメーターでのみ有効なデバッグ・パラメーターでの使用を意図したキーワードです。*ckrcarla-parm-string* の最大長は 80 文字で、引用符で囲む必要があります。

InSecure

このキーワードは、他の zSecure Server へのセキュアでない通信が受け入れられることを指定します。2 つの zSecure Server 間でセキュアでない通信を使用可能にするには、両方のサーバーで INSECURE オプションを指定する必要があり、さらにサーバー・タスクの userid が、XFACILITY リソース・クラスの該当する CKNADMIN プロファイルに対する READ アクセス権限を持っていなければなりません。このオプションは、初期セットアップ中にのみ使用され、実動では使用されません。

Debug

このキーワードは、追加診断メッセージをサーバー CKNPRINT 出力ファイルに送出することを指定します。このキーワードを使用するのは、IBM ソフトウェア・サポート要員から要求があった場合だけです。

RMTMSG

このキーワードを使用して、zSecure Server に対して、ローカル CKNPRINT 出力ファイル内のリモート・アプリケーションからの SYSPRINT 出力および SYSTERM 出力を組み込むようシグナル通知することができます。

例えば、クライアントがリモート RACF データベースからのデータにアクセスする場合、リモート・サーバーは、CKRCARLA を使用して RACF データベースを読み取ります。リモート CKRCARLA の出力は、クライアント・アプリケーションの SYSPRINT ファイル内で常に使用可能です。これと同じ出力を、ローカル・サーバーの CKNPRINT に組み込むのはオプションです。DEBUG オプションを指定すると、RMTMSG も選択されます。

Timestamp

このキーワードは、サーバー CKNPRINT 出力ファイル内に発行されるメッセージにタイム・スタンプの接頭部を付けるよう指定します。タイム・スタンプ情報は UTC で示され、固定フォーマットを使用します。実行しているシステムの現地時間が必要な場合は、代わりにキーワード Localtime を使用します。両方が表示される場合、実質的に効力があるのは現地時間です。

Localtime

このキーワードは、サーバー CKNPRINT 出力ファイル内に発行されるメッセージにタイム・スタンプの接頭部を付けるよう指定します。タイム・スタンプ情報はサーバーが稼働するシステムの現地時間で示され、固定フォーマットを使用します。UTC が必要な場合は、Localtime を指定せず、代わりにキーワード Timestamp を使用します。

MSGSUP

このキーワードは、サーバー CKNPRINT 出力ファイル内で抑制されるメッセージ番号のリストを指定します。これは、DEBUG コマンドとの組み合わせで使用できます。このキーワードを使用するのは、IBM ソフトウェア・サポート要員から要求があった場合だけです。

Other-diagnostic-options

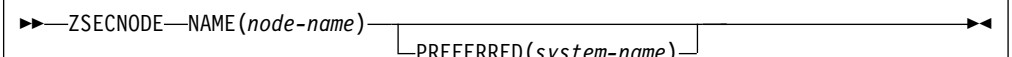
CKNSERVE プログラムのパラメーター・ストリングに指定することで、いくつかの追加診断オプションを使用できます。これらのオプションを使用するのは、IBM ソフトウェア・サポート要員から要求があった場合だけです。お客様が使用することは意図していません。現在実装されているオプシ

ョンには、 NOESTAE、 NOCLOSE、 NODUMP、 NOCLEANUP、 NODUMPEXIT、 NOGUARD、および STORAGEGC があります。

構成ファイル ZSECNODE ステートメント

単一の ZSECNODE が、共通の RACF データベースを共有するすべてのシステムを記述します。データにアクセスする要求またはプロファイルを更新する要求が、同じ ZSECNODE に所属する任意のシステムに効果的に送信されます。通常の状態では、zSecure Server は、指定された優先サーバーを使用します。しかし、そのサーバーが使用不可の場合には、zSecure Server は、同じノードに含まれる別のサーバーを使用します。その状態では、使用可能な最初の ZSECNODE が、すべてのノードの通信に使用されます。

zSecNode



キーワードとパラメーターには、次の意味があります。

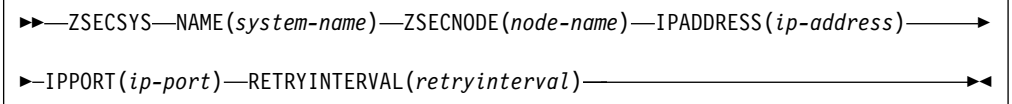
Name このキーワードは、この zSecure ノードの名前を提供します。RRSF を持っている場合には、この名前を RRSF ノード名と同じにします。代替名は、同じ名前を使用する複数の RRSF プレックスを持っている、まれな場合にのみ使用します。

Preferred
このキーワードは、このノードの優先 zSecure Server が稼働しているシステムの名前を指定します。このシステムは、通常、この zSecure ノードの RACF データベースへのアクセスに使用されます。zSecure-Server の構成ファイル内に定義されていないサーバー名を指定するか、現行 zSecure ノードを参照しないサーバーを指定すると、エラーになります。

構成ファイル ZSECSYS ステートメント

ZSECSYS ステートメントは、zSecure Server が稼働するシステムを定義します。ZSECNODE の優先システムが指定されていない場合、または優先システムが使用不可の場合には、特定のノードに関する ZSECSYS ステートメントの順序によって接続優先シーケンスが定義されます。ZSECSYS ステートメントは、必要なシステム名の数だけ繰り返すことができます。複数の ZSECSYS ステートメントが同じシステム名を参照する場合、エラー・メッセージが発行され、実行が停止します。

zSecSys



キーワードとパラメーターには、次の意味があります。

Name このキーワードは、zSecure システムに割り当てられる名前を提供します。この名前は、MVS SYSNAME または SMF-id が固有の場合には、それと同じにします。同じ MVS SYSNAME のシステムが複数存在する場合のみ、別の名前を指定する必要があります。

zSecNode

このキーワードは、このシステムが所属するノード名を提供します。RRSF を持っている場合には、この名前を RRSF ノード名と同じにします。代替名は、同じ名前を使用する複数の RRSF プレックスを持っている、まれな場合にのみ使用します。

IPAddress

このキーワードは、zSecure Server との接続に使用できる IP アドレスを指定します。IP アドレスは、ホスト名、または IPV4 フォーマットまたは IPV6 フォーマットのアドレスとすることができます。推奨値は、TCP/IP スタックの TCPIP.DATA HOSTNAME ステートメントおよび DOMAINORIGIN ステートメントからの値です。この値は大文字小文字が区別されます。指定値の例としては、`ourhost.company.com` があります。

IPPort

このキーワードは、使用されるポート名を指定します。

- ローカル・システムの場合、ローカル zSecure Server が入力接続を listen するポート名です。
- リモート・システムの場合、リモート・システムへの接続に使用されるポート名を指定します。

指定された `IPPort` 値は、複数の zSecure Server で同じにすることができます (ただし、同じにする必要はありません)。特定の ZSECSYS に対して指定された `IPPort` 値は、zSecure ネットワーク全体にわたって同じでなければなりません。`IPPort` に対して Internet Assigned Numbers Authority (IANA) が割り当てたポート番号は `7173` です。

RETRYINTERVAL

このキーワードは、この ZSECSYS への接続が、何らかの理由で接続がアクティブでなくなったときに再始動されるように指定します。
RETRYINTERVAL パラメーターの値は、接続が再始動されるまでの時間 (分) を指定します。次の値を取ることができます。

0 自動再始動が行われないことをシグナル通知します。この値がデフォルトです。

1 から **1440** の間
1 から 1440 の間の値は、接続の自動再始動を試行するまでに、接続が非アクティブである長さ (分) を指定します。このパラメーターの値は、一般に 5 分から 60 分の間です。

zSecure Server のオペレーター・コマンド

現在サポートされているオペレーター・コマンドは次のとおりです。

- START
- MODIFY *<taskname>,<action>*
- STOP

START

zSecure Server CKNSERVE は、クロスメモリー・サービスを使用してユーザーがサーバー機能にアクセスできるようにするため、CKNSERVE アドレス・スペースは、システム・レベルのリンケージ索引に関連付けられています。このシステム・レベルのリンケージ索引は、各サーバーが停止し、それに続く各サーバーの始動中に再使用された後も保持されるリソースです。このシステム・レベルのリンケージ索引は、サーバー制御ファイルに指定された ServerToken に基づきます。システム・リソースを保持したい場合には、それに続く同じ zSecure Server の各始動に対して同じ ServerToken を指定します。zSecure-Server の構成ファイル OPTION ステートメントを使用して ServerToken を指定できます。

また、クロスメモリー・サービスを使用すると、サーバーに使用されるアドレス・スペースに、使用後に UNAVAILABLE とマークが付けられます。これは以下のメッセージを通じて監視できます。

```
IEF352I ADDRESS SPACE UNAVAILABLE
```

このメッセージは、サーバーの終了後にシステム・ログで確認できます。zSecure Server の始動と停止を繰り返すことによってアドレス・スペースを失うのを防止するため、REUSASID キーワードを使用して zSecure Server を始動することが重要です。zSecure Server の始動コマンドの例は、次のようになります。

```
START CKNSERVE,PPARM=CKNSRV00,REUSASID=YES
```

この例では、次のようになります。

- zSecure Server プロシージャーは CKNSERVE と呼ばれます。
- サーバーのこのインスタンスのプライベート・パラメーター・メンバーは、CKNSRV00 です。
- 使用されるアドレス・スペースは、再使用可能なアドレス・スペースのプールから取得されます。

再使用可能なアドレス・スペースについて詳しくは、以下の資料を参照してください。

- *z/OS MVS* システム・コマンド
- *z/OS MVS* 初期設定およびチューニング解説書

MODIFY

MODIFY コマンドとともに以下のアクションを使用できます。

DEBUG
診断メッセージが、CKNPRINT 出力ファイルにプリントされます。

NODEBUG
診断メッセージは、これ以降 CKNPRINT 出力ファイルにプリントされません。

RMTMSG
リモート・アプリケーション (例えば、CKRCARLA) からの出力をローカル・サーバー CKNPRINT 出力ファイルに組み込みます。

リモート・アプリケーションの出力は、クライアントの SYSPRINT ファイルで常に使用可能です。RMTMSG を指定すると、サーバーの CKNPRINT でも同じ出力が使用可能です。

NORMTMSG
以前の RMTMSG オペレーター・アクションの効果、または OPTION RMTMSG 構成ステートメントの効果を反転させます。

STOP このアクションは、STOP コマンドと同じです。

STOP

また、`MODIFY <taskname>,STOP` 要求を使用することにより、このような停止を要求することもできます。

AT-TLS を使用したセキュアなコミュニケーション

zSecure Server 間のデータ交換は、機密的な性質のものであることがよくあります。例えば、RACF パスワードやパスフレーズが含まれる場合があります。したがって、データ通信がセキュアであり、データが公開されないように保証することが重要です。zSecure ネットワークでは、データは以下の方法で保護されます。

- 証明書を使用したパートナー検査
- 証明書が zSecure での使用を意図したものであることの追加検査
- データ暗号化

これらの方法は、AT-TLS および追加検査を使用して zSecure Server に実装されています。各 zSecure Server ペア間のセッションは、TCP/IP TTLS (Tunneled Transport Layer Security) ポリシーを使用して定義されている必要があります。z/OS では、TTLS ポリシーは、Policy Agent を使用して管理されます。*IBM Configuration Assistant for z/OS Communications Server* を使用して Policy Agent 用の構成ファイルを作成するか、または SCKRSAMP 内のメンバー CKNTTLS を開始点として使用できます。

`TTLSRule` ステートメントは、保護対象のセッションを識別し、また鍵リングを通して、AT-TLS が必要な証明書を検出できる場所を指定します。

セッションは、いかのいずれかの項目で識別できます。

- (RACF) **ユーザー** `ID`
- ジョブ名
- ローカル IP アドレス・ポート
- リモート IP アドレス・ポート
- 上記項目の組み合わせ

サンプル CKNTTLS はユーザー ID によってフィルタリングされ、またユーザー ID は、接続の両側で同じであると想定されています。

証明書は、TTLSConnectionAdvancedParms ステートメントで直接指定するか、または鍵リングを通して間接的に指定できます。CKNTTLS は、鍵リング方式を使用します。

検査対象の証明書については、トラステッド・ルート証明書によって署名されている必要があり、かつ、そのルート証明書が接続の受信側でアクセス可能である必要があります。商用のルート証明書を使用することも、ジョブ CKNRACF2 を使用してルート証明書を作成することもできます。ジョブ CKNRACF2 を使用する場合、次のようになります。

1. ジョブ CKNRACF2 を、zSecure Server のデプロイ先とするシステム・イメージの 1 つでのみ実行します。
2. エクスポート・データ・セットを別のイメージにコピーし、ジョブ CKNRACF3 を実行して、他のすべての RACF データベースにインポートします。
3. インポート後に、データ・セットを削除します。データ・セットを保持したままだと、他の人もそのルート証明書をインポートして、偽造した証明書への署名に使用する可能性があります。

NJE (TSO/E コマンドの TRANSMIT と RECEIVE) を通して転送することも、また FTP を使用することもできます。FTP を使用する場合には、バイナリー・モードで転送し、データ・セットがレコード・フォーマット VB を持ち、レコード長が 84 であることを確認してください。

このエクスポート/インポート方法により、ルート証明書が両側で同じ鍵を持つことが保証され、したがって片側で署名された証明書は、他の側でも検査できます。

ルート証明書を作成または取得した後、ジョブ CKNRACF4 を使用して証明書と鍵リングを作成します。zSecure サーバーをデプロイするすべてのシステムに対してこのジョブを実行します。このジョブは、インストールに適用する名前に調整します。特に、zSecure Server 用に生成される証明書は、zSecure Server アプリケーションによる使用に特有のものでなければなりません。これは、ALTNAME 証明書拡張で指定される DOMAIN 名によって実行されます。ドメイン・ネームは、zSecure Server 用に使用される OWNSYS に対応する ZSECSYS の値でなければなりません。

他の zSecure サーバー用に使用される証明書は、ローカル・システム上の取り消されていないユーザーにマップされなければなりません。これは、以下を使用して実行できます。

- ユーザー ID アソシエーションに対する 1 対 1 の証明書
- 証明書名のフィルタリング
- hostIdMappings 証明書拡張

証明書マッピングについて詳しくは、「*RACF* セキュリティー管理者のガイド」の RACF およびデジタル証明書に関する章を参照してください。1 対 1 の証明書マッピングは最もセキュアな方法であり、1 つのシステムに対して証明書をエクスポートし、別のシステムに証明書をインポート (追加) する必要があります。ローカルに

定義されたユーザーに証明書をマッピングする要件は、AT-TLS ポリシー内の ClientAuthType の SAFCHECK 値によって強制されます。

証明書をローカル・ユーザーにマップしなければならないという要件により、既知の証明書だけが使用されることが保証されます。この要件がない場合は、ご使用の zSecure Server 証明書用のトラステッド CA (認証局) によって署名されていると、(意図しない、および未知の) 新しい証明書が受け入れられます。

デジタル証明書を使用するには、サーバー・ユーザー ID も FACILITY リソース・クラス内の IRR.DIGTCERT.LISTRING に対する READ アクセス権限を持つ必要があります。

追加のセキュリティー手段

ユーザー ID マッピング規則を使用して、このようなシステムのすべてのユーザーに、低い権限を持つ**ユーザー ID** を割り当てることができます。代わりに、 210 ページの『zSecure Server の使用時における許可およびユーザー ID のマッピング』に説明されている CKNADMIN.FROMNODE.<*nodename*> を使用して、ZSECNODE 全体に対し**ユーザー ID** を割り当てる方法があります。一致するプロファイルの APPLDATA に値が入っている場合、それは ZSECNODE の **ユーザー ID** として使用されます。その**ユーザー ID** が存在する場合、それはログオン・ユーザーを表す通常のマップされた**ユーザー ID** のほかに、個々の CKNDSN リソースに対するアクセス権限も持っている必要があります。そのセットアップでは、2 つのユーザーがアクセス権限を持つ必要があります。

- ログオン・ユーザーを表すマップされた**ユーザー ID**
- ZSECNODE 全体に割り当てられた**ユーザー ID**

CKNDSN リソースに対するいずれかのユーザーのアクセス権限が不十分な場合、アクセスは否認されます。

要求の発生元の *nodename* が現在の zSecure ノード名と同じである場合、ZSECNODE 全体に割り当てられたユーザー ID の追加テストは迂回されます。このため、ソース・サーバーがターゲット・サーバーと同じ ZSECNODE 上で実行されている場合、ログオン・ユーザーを表すマップされたユーザー ID のみが、CKNDSN リソースにアクセスできる必要があります。

これらの追加のセキュリティー手段を使用すると、要求の発生元であるシステムに基づいて、入力ファイルに対するアクセス権限とコマンドの実行権限を制御することができます。また、ログオン・ユーザーに基づいて細分性を保持することもできます。以下のような環境例を考えてみます。

- 2 つの実動システム (PRD1SYS と PRD2SYS) および 1 つの外部システム (EXT1SYS) があります。
- PRD1SYS が zSecure ノード PRD1NODE の一部として定義されており、PRD2SYS が zSecure ノード PRD2NODE の一部として定義されています。
- ユーザー IBMUSER がシステム PRD1SYS にログオンし、PRD2SYS にアクセスしています。

以下のプロファイルが、システム PRD2SYS に定義されています。

```
CKNDSN.RACF.PRD2NODE.PRD2SYS.ACTIVE.    READ(IBMUSER,EXT1USER)
CKNDSN.CKRCMD.PRD2NODE.PRD2SYS.CKRCMD    READ(IBMUSER)
CKNADMIN.FROMNODE.PRD1SYS  NOAPPLDATA       READ(IBMUSER)
CKNADMIN.FROMNODE.EXT1SYS  APPLDATA(EXT1USER) READ(IBMUSER)
CKNUMAP.*.*.*    APPLDATA(=USERID)
```

最後のプロファイル (CKNUMAP) は、**ユーザー ID** マッピング規則です。これは識別マッピングを指定し、したがってログオン・ユーザー IBMUSER の ID も、PRD2SYS システム上での許可を必要とする ID として使用されます。

3 番目のプロファイル (CKNADMIN.FROMNODE.PRD1SYS) は、PRD1SYS から PRD2SYS にアクセスする権限を記述します。IBMUSER はアクセス権限を持ちます。プロファイルは APPLDATA フィールドを持っておらず、したがって追加のシステム・レベルの許可はありません。

最初の 2 つのプロファイル (CKNDSN.RACF.PRD2NODE.PRD2SYS.ACTIVE. と CKNDSN.CKRCMD.PRD2NODE.PRD2SYS.CKRCMD) は、RACF データベースにアクセスする権限、およびコマンドを発行する権限を記述します。IBMUSER は、両方のプロファイルにアクセス権限を持ちます。

別のシナリオでは、ユーザー IBMUSER がシステム EXT1SYS にログオンし、やはり PDR2SYS にアクセスしています。同じ**ユーザー ID** マッピング規則が、EXT1SYS 上の IBMUSER から PRD2SYS 上の IBMUSER へのマップに使用されます。

4 番目のプロファイル (CKNADMIN.FROMNODE.EXT1SYS) は、その APPLDATA フィールドに、システム・レベルの**ユーザー ID** EXT1USER がアクセスの検査に使用されることを指定します。EXT1USER は、2 番目のプロファイル (CKRCMD リソースを記述する CKNDSN.CKRCMD.PRD2NODE.PRD2SYS.CKRCMD) にアクセス権限を持たないため、EXT1SYS (IBMUSER を含む) からは、誰も PRD2SYS のコマンドの発行を許可されません。

ユーザー ID がノードの FROMNODE プロファイルの APPLDATA に指定されている場合、**ユーザー ID** は、そのノードの証明書に関連付けられている**ユーザー ID** に一致する必要があります。

サーバー・セキュリティーを使用不可にするためのセットアップ

他の zSecure Server との通信に対する適切なセキュリティーなしで zSecure Server を実行することができます。この方法で zSecure Server を実行するには、zSecure-Server の構成ファイル内の zSecure Server OPTION ステートメントに INSECURE キーワードを指定します。両方のサーバーに、INSECURE キーワードを指定する必要があります。特定の接続にセキュアでない接続は、XFACILIT リソース・クラス内の CKNADMIN.INSECURE.<zsecsys-name> リソースによって制御されます。<zsecsys-name> は、パートナー・ノードであり、開始タスク・ユーザーは、READ 以上の権限を持っている必要があります。一致するプロファイルが見つからない場合、または開始タスク・ユーザーに十分なアクセス権限がない場合には、接続は拒否されます。

```
CKNADMIN.INSECURE.<zsecsys-name> READ(server-userid)
```

また、証明書の ALTNAME 内に存在するホスト名とパートナー zSecure Server との間の zsecsys 不一致を許可することができます。これは、リソース CKNADMIN.CERTOKAY.<zsecsys-name> に一致するプロファイルに対するサーバー・ユーザー ID のアクセスによって制御されます。一致するプロファイルが見つからない場合、または開始タスク・ユーザーに十分なアクセス権限がない場合には、接続は拒否されます。プロファイルは、そのパートナーが一致する証明書を持っていないことを検出するシステム上で定義されていなければなりません。

```
CKNADMIN.CERTOKAY.<zsecsys-name> READ(server-userid)
```

Secure Server 通信の要約

次の表に、各種のセキュリティー関連設定の要約を示します。

表 4. セキュリティー関連設定

領域	サブエリア	フィールド	設定	効果
TTLSRule	TTLSGroupAction	TTLSEnabled	オン	証明書の使用を強制
	TTLSKeyringParms	Keyring	値	鍵リングの名前を指定
	TTLSEnvironmentAdvancedParms	ClientAuthType	SAFCHECK	証明書が RACF ユーザーにマップされている必要があることを指定
		ApplicationControlled	オフ	AT-TLS を常に使用すること、それがアプリケーション・コードに依存しないことを指定
	TTLSConnectionAdvancedParms	CertificateLabel	値	証明書のラベルを指定
	TTLSCipherParms	V3CipherSuites	値のリスト	暗号化方式のリストを指定。省略した場合には、単純な暗号化を使用。
証明書	ALTNAME(DOMAIN(zsecsys- name))			zsecsys 名と一致する必要がある
	RACF ユーザーへのマッピング		証明書ユーザー ID	TTLS ポリシー内の SAFCHECK によって強制

表 4. セキュリティー関連設定 (続き)

領域	サブエリア	フィールド	設定	効果
RACF	IRR.DIGTCERT.LISTRING	Access list	サーバー・ユーザー ID	証明書の取得を許可
	CKNDAMIN.FROMNODE.<zsecnode-name>	APPLDATA	ノード・ユーザー ID	追加の CKNDSN verification.node-userid は certificate-userid に一致している必要がある。ソース・システムの zsecnode-name がターゲット (現在の) システムの zsecnode-name と異なる場合にのみ適用
	CKNDSN.<type>.<nodename>.<sysname>.<dsname>	Access list	node-useridclient-userid	データ・ソースへのアクセスを制御
	CKNDSN.CKRCMD.<nodename>.<sysname>.CKRCMD	Access list	node-useridclient-userid	コマンド実行のアクセス権限を制御
	CKNADMIN.INSECURE.<zsecsys-name>	Access list	サーバー・ユーザー ID	証明書の欠落を許可。ソース・システムの zsecsys-name がターゲット (現在の) システムの zsecsys-name と異なる場合にのみ必須
	CKNADMIN.CERTOKAY.<zsecsys-name>	Access list	サーバー・ユーザー ID	不正な ALTNAME(DOMAIN (zsecsys-name)) を許可。証明書が接続で使用される場合にのみ適用。
zSecure Server	構成ファイル	OPTION	INSECURE	証明書の欠落を許可

zSecure Server を使用したセキュリティー・データベースへのアクセスの必要性の限定

zSecure Server を自己接続 モードで使用できます。このモードでは、単一の zSecure Server でそれ自身に要求を送信できます。この方法により、元のユーザーは、セキュリティー・データベースを読み取る許可を必要としません。原則的に、このような許可は機密漏れになり、この機密漏れは PADS モードでのアクセスまたは zSecure Server によって解決できます。 PADS モードについて詳しくは、220 ページの『プログラム制御および PADS アクセスのセットアップ』を参照してください。自己接続モードの zSecure Server は、PADS モードの完全な代替となります。

zSecure Server の自己接続モードでは、データにアクセスするためのユーザーの許可は、(マルチシステム・モードの場合と同様に) XFACILIT クラスのプロファイルによって制御されます。セキュリティー・データベース (またはその他のデータ) の実際の読み取りは、元のユーザーではなく、サーバー・アドレス・スペースによって行われます。

zSecure Server を組み合わせて、自己接続モードとマルチシステム・モードで同時に実行することができます。また専用サーバーをセットアップすることもできま

す。例えば、単一の z/OS イメージで、単一の zSecure Server のみをセットアップし、自己接続モードで排他的に実行します。

自己接続モードのサーバーをセットアップするには、以下のステップを実行します。 (詳しい説明については、前のセクションを参照してください。)

- システム proclib 内の JCL プロシージャーをセットアップします。
- ServerToken の値、ZSECNODE の名前、および ZSECSYS を決定します。
- 専用サーバーの場合、ローカル・サーバーのみを定義します。リモート接続は定義しないでください。
- 専用サーバーの場合、サーバーで AT-TLS は不要です。 INSECURE パラメーターも不要です。AT-TLS ポリシーが自己接続にも適用される場合は、前のセクションで説明した関連アクションがすべて完了していることを確認する必要があります。
- **SE.D** で、デフォルト・セットアップ・ファイルを更新して、`zsecnode/sys` の名前を含めます。
- デフォルト実行オプションを更新して、ServerToken を含めます。
- オプションとして、明示的な総称 CKNUMAP プロファイルを定義します。例:
  `CKNUMAP.<zsecnode>.*.<zsecnode> with appldata('=USERID')`
- 必要な CKNDSN プロファイルを定義します。例: RACF の場合、CKFREEZE ファイル、ACCESS ファイル、およびアンロード SMF ファイル。

第 10 章 zSecure Admin アクセス・モニターのセットアップ

アクセス・モニターは、リソース・プロファイルの実際の使用状況に関する情報を収集するために使用できる zSecure Admin のコンポーネントです。このデータは、zSecure Admin で提供されているアクセス・モニター・オプションからのレポート作成と分析に使用できます。管理者は、収集された情報を使用して未使用のアクセスやリソース・プロファイルを特定し、RACF データベースから除去できます。アクセス・モニターについて詳しくは、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」を参照してください。

アクセス・モニターのセットアップと操作については、以下のセクションを参照してください。

- 76 ページの『インストール要件とポストインストール要件』
- 83 ページの『アクセス・モニターの操作』
- 89 ページの『アクセス・モニター機能のコマンド・リファレンス』

以前のリリースのアクセス・モニターからアップグレードする場合の考慮事項

このトピックのガイドラインを使用して、以前のリリースのアクセス・モニターからアップグレードします。

以前のリリースのアクセス・モニターからアップグレードする場合、正しいソフトウェアの現行リリースを確実に使用するためには、以下の手順のいずれかを使用する必要があります。システムで最後に IPL を実行して以降、zSecure Admin アクセス・モニターの開始タスク (C2PACMON) を始動していない場合には、アップグレード・ステップは特に必要ではありません。

- 以前のバージョンの C2PACMON を停止する場合は、SIPL コマンドを使用する必要があります。例えば、次のオペレーター・コマンドを使用できます。

  ```
  MODIFY C2PACMON,SIPL
  ```

  C2PACMON 開始タスクの停止後には、RECOVER キーワードを使用して C2XACTV ジョブを実行する必要があります。この C2XACTV ジョブでは、以前のリリースのソフトウェア・レベルが含まれるデータ・セットを STEPLIB として使用する必要があります。完了後、ソフトウェアの現行リリースを使用して C2PACMON を開始できます。 C2XACTV ジョブの例を以下に示します。

  ```
  //RECOV  EXEC PGM=C2XACTV
  //STEPLIB  DD DISP=SHR,DSN=<loadlib.zsecure.2.2.1>
  //C2XPRINT DD SYSOUT=*
  //C2XIN    DD *
   DYNEXIT RECOVER ICHRCX02
   DYNEXIT RECOVER ICHRDX02
   DYNEXIT RECOVER ICHRFX04
   DYNEXIT RECOVER ICHRIX02
  ```

以前のリリースに戻る必要がある場合には、再度 SIPL コマンドを使用して C2PACMON を停止する必要があります。 開始タスクを正常に停止した後には、以前のリリースのソフトウェアを使用して C2PACMON をすぐに開始できます。

- zSecure Admin アクセス・モニター開始タスクの現行バージョンを停止した後、システムをシャットダウンしてから IPL を実行します。IPL の実行後、アップグレード済みのコードを使用して、zSecure Admin アクセス・モニター開始タスクを開始します。このシナリオでは、追加ステップを実行する必要はありません。

この手順のどちらも使用しない場合、始動が失敗して C2PACMON 開始タスクの ABEND (異常終了) が発生する可能性があります。始動が失敗してメッセージ C2P0183E と C2P0123E が表示された場合、FORCE 開始パラメーターを使用するとリカバリーできる場合があります。

インストール要件とポストインストール要件

このトピックのガイドラインを使用して、アクセス・モニターを使用するように zSecure インストールを正しく構成してください。

アクセス・モニターをセットアップするには、事前に zSecure をインストールする必要があります (13 ページの『第 4 章 ソフトウェアのインストール』を参照)。このインストール・プロセス中に、以下の構成が行われていることを確認します。

- zSecure Admin がインストールされている必要があります。この製品をインストールするには、メンバー CKRZUPDI でインストール・パラメーター AdminRACF を有効にしてから、高速インストール・ジョブまたは正式インストール・ジョブを実行します。 17 ページの『インストール・パラメーターのカスタマイズ』を参照してください。
- AdminRacf ライセンスを使用可能にする必要があります。 24 ページの『ライセンス機能の使用可能化』を参照してください。
- SCKRLOAD コンポーネントには APF 許可が必要です。
- アクセス・モニターを使用可能にする zSecure 構成データ・セットが必要です。
  - この構成を作成するには、ジョブ CKRZPOST を実行します (34 ページの『zSecure 構成 データ・セットの作成』を参照)。アクセス・モニターに専用の zSecure 構成を使用する場合、必要なのは CKRPARM データ・セットを作成することのみです。CKRZPOST ジョブ内の他のデータ・セットに対する DD ステートメントをコメント化することができます。
  - アクセス・モニターに対して有効になっている zSecure 構成が既にある場合は、引き続きその構成を使用します。
  - zSecure 1.10 またはそれより前のバージョンで作成した zSecure 構成は使用しないでください。1.10 の構成には、アクセス・モニターに必要なメンバーとパラメーターが一部含まれていません。
- アクセス・モニターを複数の z/OS イメージで使用する場合は、イメージごとに別々の CKRPARM データ・セットを使用します。各イメージのアクセス・モニター・データ・セットには、必ず異なる名前を付けてください。名前をセットアップするには、CKRPARM の C2PAMCNT メンバーと C2PAMCLT メンバー

で指定されるデータ・セット名に、少なくとも SYS パラメーター (&SYS や &SYSCLONE など) が異なるイメージ依存の変数を使用します。

- あるいは、インスタンスごとに、メンバー C2R$PARM、C2PAMP、またはその両方のコピーを個別に作成できます。共有 JES プロシージャー・ライブラリーがある場合は、MVS システム・シンボルを使用して別々の構成を設定できます。

アクセス・モニターの構成

アクセス・モニターを開始し、データの収集と統合を開始するには、このトピックの構成タスクを実行します。

- JCL を準備します。
- セキュリティー・リソースおよび許可を定義します。
- 必要なアクセス・モニター・データ・セットを作成します。
- データ収集と統合のパラメーターをカスタマイズします。
- アクセス・モニターを開始します。

JCL の準備

このタスクについて

アクセス・モニターは開始タスクとして実行する必要があります。このため、SCKRPROC データ・セットから開始タスク・プロシージャー・ライブラリーに C2PACMON プロシージャーをコピーする必要があります。

手順

1. C2PACMON を開始タスクとして実行するために、SCKRPROC データ・セットから開始タスク・プロシージャー・ライブラリーに C2PACMON プロシージャーをコピーします。作成するセキュリティー・リソースを更新する場合は、異なるメンバー名を選択できます。
2. C2PACMON プロシージャーのコピーで、使用する zSecure 構成のメンバー名を指定します。デフォルトは C2R$PARM です。ただし、プロシージャー・ライブラリーが複数の z/OS イメージ間で共有されている場合は、プロシージャーで MVS システム・シンボルを使用して、アクセス・モニターのインスタンスごとに別々の構成メンバーを割り当てます。
3. データ収集と統合のパラメーターをインスタンスごとに分ける場合は、JCL の PPARM パラメーターでメンバーを指定します。必要であれば、パラメーター・メンバー名でシステム・シンボルを使用できます。例えば、次の例に示すデフォルトの PPARM ステートメントを、システム・シンボルを使用するように変更することができます。

   ```
   // PPARM=C2PAMP,        C2PACMON パラメーター・メンバー
   ```

   次の例は、変更後のコマンドを示しています。

   ```
   // PPARM=C2PAMP&SYSCLONE,     C2PACMON parameter member
   ```

4. 構成メンバーを開始タスク・プロシージャー・ライブラリーに保管します。構成メンバー内で、C2PACPRM パラメーターを設定する行のコメントを外します。

セキュリティー・リソースおよび許可の定義

このセクションでは、zSecure Admin のアクセス・モニター機能に必要なセキュリティー・リソースと許可について説明し、そのセットアップ手順を示します。セキュリティー・データベースを共有していない場合は、アクセス・モニターを実行するすべてのシステムに対してこれらの許可を設定する必要があります。

必要なセキュリティー・リソースと許可は以下のとおりです。

- C2PACMON アドレス・スペースを実行するために選択したユーザー ID とグループが使用可能であることが必要です。
- 必要なユーザー ID とグループを開始タスクに割り当てることができる STDATA セグメントを含んだ STARTED プロファイル。
- C2PACMON のユーザー ID には、XFACILIT リソース C2X.ICHRCX02、C2X.ICHRDX02、C2X.ICHRFX04、および C2X.ICHRIX02 に対する UPDATE 権限が必要です。また、このユーザー ID には、XFACILIT リソース CKR.CKRCARLA.APF に対する READ 権限も必要です。
- 開始タスクの出力の保護。
- データ・セット名およびそれらを対象として含むプロファイル。データ・セットへのプログラム・アクセス (PADS) 権限が使用されている場合は、これに PROGRAM プロファイルが含まれることがあります。

SCKRSAMP データ・セットのジョブ C2PZRIN0 を、これらのセキュリティー・リソースのセットアップに利用することができます。ただし、作成するセキュリティー・リソースは、使用するセキュリティー・ポリシー (総称プロファイルか個別プロファイルかの選択など) に従っている必要があるので注意してください。RACF コマンドの確認後に、このジョブを実行するかどうかを決定できます。

このジョブでは、一部の内容が想定されており、zSecure 構成中にカスタマイズされません。このため、場合によっては以下の情報に基づいてジョブを変更する必要があります。

- グループ名 SYSAUDIT は、システム監査員を含むグループと想定されていますが、別のグループを選択してもかまいません。ユーザー (インストーラー) は、SYSAUDIT グループに接続されているものと想定されます。このグループに接続されていないと、ジョブ C2PZRIN1 を使用したアクセス・モニターに対するデータ・セットの割り振りは失敗します。
- グループ所有者は、SYSAUTH に設定されます。
- SCKRLOAD データ・セットに対してプロファイルがセットアップされていること、および他のデータ・セットに別のプロファイルが存在することが想定されます。異なるセットアップがある場合は、ご使用の環境の要件に合わせてこのジョブの JCL を調整する必要があります。
- PROGRAM プロファイル CKRCARLA が存在するものと想定されます。PROGRAM プロファイルを使用しない場合は、それらのプロファイルに対する rdefines、ralters、および permits を除去できます。

必要なアクセス・モニター・データ・セット

日次収集および日次統合のプロセスに使用されるデータ・セットは、アクセス・モニター・データを保持できるだけの大きさであることが必要です。必要なサイズ

は、使用する環境によって異なります。データ損失を防ぐために、これらのデータ・セットを注意深くモニターして、十分なスペースが割り振られるようにしてください。

アクセス・モニター機能に必要なデータ・セットは以下のとおりです。

- C2PACMON アドレス・スペースの中間データを含んだデータ・セット。JCL では、これらのデータ・セットが SYSPRST1 および SYSPRRPT として識別されます。C2PACMON アドレス・スペースでは、これらのデータ・セットが共有対象として割り振られるため、許可を受けたユーザー (管理者など) はトラブルシューティングでこれらのデータ・セットを参照できます。ただし、それ以外でこれらのデータ・セットを共有しないでください。デフォルトでは、これらのデータ・セットの名前にシステム ID が含まれています。
- zSecure 構成ファイルに指定されているパラメーター・データ・セット。zSecure 構成ファイルについて詳しくは、 34 ページの『zSecure 構成 データ・セットの作成』を参照してください。

これらのデータ・セットの作成を支援するために、CKRINST ライブラリーにジョブ C2PZRIN1 が用意されています。このジョブを実行依頼する前に、JCL を以下のようにカスタマイズします。

- デフォルトの zSecure 構成ファイルを更新しなかった場合は、準備した zSecure 構成ファイルを指定するために JCLLIB および INCLUDE ステートメントを変更します。
- zSecure Admin のアクセス・モニター機能を複数の z/OS イメージで実行する場合は、このジョブを複数回 (イメージごとに 1 回ずつ) 実行します。可能であれば、対応するアクセス・モニター機能を実行する z/OS イメージの下で、それぞれのジョブを実行してください。
- パラメーター・データ・セットを複数の z/OS イメージ間で共有する場合は、C2PACPRM の割り振りが 1 回だけ行われるようにします。通常このデータ・セットは、ジョブ CKRZPOST によって割り振られます。

データ収集と統合のパラメーターのカスタマイズ

これらのパラメーターをカスタマイズして、データ収集と統合の時間間隔を制御できます。アクセス・モニターのパラメーターを指定する前に、必要なアクセス・モニター・データ・セットを作成します。の説明に従って、パラメーター・データ・セットを作成しておく必要があります。

アクセス・モニター開始タスクのパラメーター・ファイル

アクセス・モニター機能には、開始タスク用のパラメーター・ファイルが必要です。このパラメーター・ファイルは、PPARM JCL を使用してアクセス・モニター開始タスク・プロシージャーに組み込まれます (JCL を準備します。を参照)。パラメーター・ファイルは常に必須です。パラメーターのデフォルト値を一切変更しない場合は、少なくとも 1 行 (コメント行でかまいません) を含んだパラメーター・ファイルを指定します。デフォルト値を示すサンプルのパラメーター・ファイルが、SCKRSAMP データ・セットのメンバー C2PAMP にあります。

構成パラメーターについて詳しくは、 91 ページの『構成コマンド』を参照してください。

zSecure Alertへの VERIFY イベント・レコードの引き渡し

zSecure Access Monitor は RACF イベントのルーチンを代行受信することで、通常は入手できない情報を収集します。サインオン (つまり、より一般的には RACF VERIFY 処理) がこのようなイベントの最も明らかなものの 1 つです。この RACF 機能では、デフォルトでイベントの SMF レコードの書き込みがスキップされます。アプリケーションで SMF レコードの作成を明示的に要求する必要があります。zSecure Access Monitor は、アプリケーションが SMF レコードを要求しない場合でも当該イベントに関する情報を収集します。zSecure Alert の機能を拡張するために、収集された情報が zSecure Alert に渡されるように、zSecure Access Monitor を構成できます。現在サポートされているイベント・タイプは、RACF VERIFY イベントのみです。

アクセス・モニターの OPTION ステートメントで EventsToAlert パラメーターを指定すると、アクセス・モニターが検出した VERIFY イベントがすべて zSecure Alert に渡されるようになります。 zSecure Alert をアクティブにしていないときにこのパラメーターを含めると、メッセージの転送が失敗したことを示すメッセージが発行されます。EventsToAlert パラメーターについて詳しくは、 91 ページの『構成コマンド』で OPTION コマンドを参照してください。

詳細データを収集する対象のユーザーまたはクラスの定義

C2PACMON 開始タスクの手順には、C2PACPRM 構成パラメーターによってポイントされたデータ・セット内の 3 つのメンバーを参照する 3 つの DDNAME が組み込まれています。このデータ・セットのデフォルト値は、zSecure 構成に使用される CKRPARM データ・セットです。3 つのメンバーは、C2PAMJOB、C2PAMRCL、および C2PAMPCL です。これらは、ジョブ名情報の収集対象となるユーザー ID、および Port Of Entry (POE) 情報の収集対象となるリソース・クラスと POE クラスを指定するために使用されます。収集されたアクセス・モニター・イベントのユーザーと話し合って、詳細情報が必要なイベントを特定してください。使用されているジョブ名や Port of Entry によっては、この詳細情報を収集することで、収集したデータとデータ統合プロセスによるリソースの使用量が大幅に増加する可能性があります。デフォルトの構成メンバーでは、ジョブ名情報も POE 情報も収集しないように指定されています。

- ジョブ名情報の収集は、C2PAMJOB メンバーの内容によって制御されます。このメンバーのレイアウトは 2 列で構成されます。この段落の後に例を示します。メンバー名とルーラー・ラインはメンバーに含まれませんが、ここでは内容をわかりやすくするためだけに示されています。ルーラー・ラインは、2 番目の列をレコードの位置 10 から始める必要があることを強調しています。

  ```
  C2PAMJOB
     ----+----1----+----2
     IBMUSER  YES
     C2PSUSER NO
  ```

  最初の列は、ジョブ名情報の制御対象であるユーザー ID を示しています。2 番目の列には、値 YES またはその他の値を指定できます。ジョブ名情報は、値 YES が指定されているユーザーについてのみ収集されます。C2PAMJOB メンバーに含まれないユーザー、または YES 以外の値が指定されているユーザーのジョブ名情報は収集されません。このメンバー内の情報はすべて大文字で指定してください。

ジョブ名情報は、RACF 定義ユーザー ID なしで実行されるジョブまたは開始タスクについて常に収集されます。

- Port Of Entry 情報の収集は、C2PAMRCL メンバーと C2PAMPCL メンバーの内容によって制御されます。これらのメンバーのレイアウトは、それぞれ 2 列で構成されます。この段落の後に例を示します。メンバー名とルーラー・ラインはメンバーに含まれませんが、ここでは内容をわかりやすくするためだけに示されています。ルーラー・ラインは、2 番目の列をレコードの位置 10 から始める必要があることを強調しています。

```
C2PAMRCL
   ----+----1----+----2
   OPERCMDS YES
C2PAMPCL
   ----+----1----+----2
   CONSOLE  YES
   TERMINAL YES
```

  最初の列は、POE 情報の制御対象となるリソース・クラスを示しています。2 番目の列には、値 YES またはその他の値を指定できます。C2PAMRCL メンバーは、アクセスの検査が行われるリソース・クラスを指定します。これには、任意の RACF リソース・クラス (DATASET、FACILITY、OPERCMDS など) を指定できます。C2PAMPCL メンバーは、POE のリソース・クラス (タイプ) を指定します。認識される POE クラスは、
  TERMINAL、CONSOLE、JESINPUT、APPCPORT、および SERVAUTH です。POE 情報は、リソース・クラスと POE クラスの両方に対して値 YES が指定されているイベントについてのみ収集されます。いずれかのクラスで他の値が指定されている場合、このアクセス・モニター・イベントの POE 情報は収集されません。これらの構成メンバー内の情報はすべて大文字で指定してください。

ここで説明した 3 つの構成メンバーに対する更新は、C2PACMON 開始タスクの再開後、または同開始タスクが統合実行を完了した後に収集されるデータに対して有効になります。C2PACMON 開始タスクの再開方法、または C2PACMON 開始タスクによって実行される統合プロセスについて詳しくは、 90 ページの『オペレーター・コマンド』を参照してください。

データ収集ファイルとデータ統合ファイルの定義

収集されたアクセス・モニター・レコードは、各 SMF インターバルで 1 日に数回ディスクに保存されます。PARMLIB の SMFPRMxx メンバーで INTVAL パラメーターに指定されるデフォルトの SMF インターバルは 30 分です。収集されたデータは、構成プロセスで指定されて割り振られたデータ・セットに保管されます。

収集されたアクセス・モニター・ファイルは、1 日に 1 回統合されます。統合プロセスでは、複数のインターバルのデータが 1 つのインターバルへと結合されます。デフォルトでは、24 時間のアクティビティーと 30 分の SMF インターバルに基づいて、1 日に 48 個のインターバルが収集されます。このデータ統合は、毎晩 consolidatetime で指定された時刻に自動的に行われます。収集されたデータは、構成プロセスで指定されて割り振られたデータ・セットに保管されます。

アクセス・モニター機能では、データ収集データ・セットと統合データ・セットに対し、名前およびその他の割り振りパラメーターを柔軟に指定できます。割り振りパラメーターは、2 つの Parmlib メンバーで指定します。1 つは、日次収集データ・セット用の C2PAMCLT メンバー、もう 1 つは統合データ・セット用の

C2PAMCNT メンバーです。この 2 つの Parmlib メンバーには、TSO ALLOCATE コマンドが含まれている必要があります。zSecure で提供されている SCKRSAMP データ・セットにサンプルのメンバーがあります。以下の 2 つの例は、このサンプル・ファイルの内容を示しています。

例: データ収集ファイルを割り振るための **C2PAMCLT Parmlib** メンバー

```
alloc reuse fi(c2pamcol) -
DA('your_prefix.C2PACMON.D&LYR2.&LMON.&LDAY..T&LHR.&LMIN.') -
mod space(1,1) cylinders release -
recfm(v b) lrecl(584) blk(27998) storclas(your_class)
```

例: データ統合ファイルを割り振るための **C2PAMCNT Parmlib** メンバー

```
alloc reuse fi(c2pacmon) -
DA('your_prefix.DATA.C2PACMON.D&LYR2.&LMON.&LDAY.') -
mod space(1,1) cylinders release -
recfm(v b) lrecl(584) blk(27998) storclas(your_class)
```

前の例の ALLOC コマンドでは、以下の規則が適用されます。

- 複数の行を入力できます。
- 負符号 (-) は継続行を表します。
- 列 73 - 80 は無視されます。
- コマンドの長さは合計で 255 文字未満にする必要があります。この長さには、行の最後の有効な文字と、その後の行継続文字 (負符号 (-)) との間にあるすべてのブランクが含まれます。
- これらのメンバーに入力されるコマンドは、シンボル置換を除いて、完全かつ有効な TSO ALLOCATE コマンドでなければなりません。不要なキーワードはすべて除去してください (例えば VOLUME キーワード)。
- reuse キーワードと file キーワードは、例に示されているままにしておく必要があります。データ収集ファイルには C2PAMCOL、データ統合ファイルには C2PACMON というファイル名を、それぞれ指定しなければなりません。
- システム・シンボルは、コマンドの任意の位置に挿入できます。これは大文字で指定しなければなりません。ユーザー・シンボルと JCL シンボルはサポートされていません。
- データ・セットのレコード・フォーマットは、`RECFM(V B)` キーワードで示されているように、ブロック化可変でなければなりません。
- データ・セット名の指定は、ストリング `DA('` で始める必要があります。
- データ・セット名の指定は、ストリング `')` で終了する必要があります。
- メンバー C2PAMCLT でのデータ・セット名の指定は、`D&LYR2&LMON&LDAY.T&LHR&LMIN` で終了する必要があります。この結果、タイム・スタンプのフォーマットは `Dyymmdd.Thhmm` となります。
- メンバー C2PAMCNT でのデータ・セット名の指定は、`D&LYR2&LMON&LDAY` で終了する必要があります。この結果、タイム・スタンプのフォーマットは `Dyymmdd` となります。
- 置換後のデータ・セット名が有効である限り、必要な任意の先行修飾子を指定できます。
- メンバー C2PAMCLT の日次収集ファイルとメンバー C2PAMCNT の日次統合ファイルに、異なる接頭部を指定することには明らかな利点があります。主な利

点は DSNPREF キーワードを使用すると特定タイプのファイルを参照できることです。日次統合ファイルは UNLOAD ステートメントを使用するとより高度な統合が可能です。ただし、UNLOAD ステートメントを使用する高速統合を可能にするには、まず SUMMARY ステートメントを使用して日次収集ファイルを変換する必要があります。(このような SUMMARY ステートメントを使用する CARLa の例が、メンバー C2PAMCVT に示されています。) 異なる接頭部を使用することで、異なる処理要件を容易に分けることができます。

- 割り振り用に追加のパラメーターを指定できます。例えば、ご使用のインストール済み環境で zEDC 圧縮用の STORCLAS や MGMTCLAS、DATACLAS などの SMS 構造の指定がサポートされている場合は、ここでそれらの構造を使用できます。zEDC データ圧縮について詳しくは、 86 ページの『zSecure 用の zEnterprise Data Compression (zEDC)』を参照してください。
- オプションのコメント行は最後に組み込む必要があります。コメントはコメント区切り文字の `/*` と `*/` の間に挿入します。

上記の規則に従っていないと、日次統合プロセスでエラー・メッセージが表示され、正しいデータ・セットを割り振ることができなくなる場合があります。

アクセス・モニターの操作

RACF アクセス・モニター機能を管理するには、開始時およびタスクの実行中にオペレーター・コンソールからコマンドを実行します。また、開始プロシージャーの Parmlib DD ステートメントに入力パラメーターを指定することで、アクセス・モニター機能の操作環境を制御できます。その方法については、以下のセクションを参照してください。

- 『アクセス・モニター STC の開始』
- 84 ページの『アクセス・モニター開始タスクをモニターまたは変更するための MODIFY コマンド』
- 85 ページの『アクセス・モニター STC の停止』
- 85 ページの『parmlib を使用したアクセス・モニター機能の構成』
- 85 ページの『アクセス・モニター・データの処理時におけるメモリーまたはデータ・ストレージの問題』
- 88 ページの『アクセス・モニターによってインストールされた RACF 出口の管理』

主に PARMLIB ファイルの一部として実行するためのコマンドがあります。これらのコマンドとそのキーワード、およびパラメーターについては、 91 ページの『構成コマンド』で説明しています。

アクセス・モニター STC の開始

zSecure Admin のアクセス・モニター機能を開始するには、オペレーター・コンソールから以下の例のように START コマンドを実行します。

```
S C2PACMON
```

本番環境では、自動化オペレーション・ソフトウェアまたは Parmlib メンバー COMMNDxx を使用して、各 IPL の直後にアクセス・モニター・タスクが自動的に開始されるようにします。

このコマンドによって、該当するシステム proclib からプロシージャーが実行されます。 START コマンドを入力する際に、診断テストやプログラムの強制的な初期化を行うための開始パラメーターを指定することもできます。これらのパラメーターについては、『アクセス・モニターの START パラメーター』で説明しています。

アクセス・モニターの START パラメーター

アクセス・モニターの通常の実行では、開始パラメーターを指定する必要はありません。アクセス・モニターは、デフォルトでは、それが既にアクティブであるかどうかを検出し、終了する前に適切なエラー・メッセージを出します。アクセス・モニターは、システム・リソースを効率的に使用するように設計されています。アクセス・モニター開始タスクが以前にシャットダウンされている場合は、1 回しか取得できず、かつシステムに返すことができない重要なシステム・リソースが、新たに開始されたタスクで再使用されます。

エラー状態によっては、アクセス・モニター開始タスクが初期化に失敗します。このような状態では、START にオプションのパラメーターのいずれかを指定する必要があります。

以下の例では、START コマンドに DEBUG パラメーターを指定しています。

```
S C2PACMON,,,DEBUG
```

DEBUG
: 初期化の最初の部分で診断メッセージを出します。この診断メッセージを使用して、標準の PARMLIB パラメーターを処理する際に発生する可能性がある問題を特定することもできます。この設定は、オペレーター・コンソールまたは PARMLIB を使用して次の DEBUG コマンドが実行されるまで有効です。

FORCE
: 前の実行に関係なく、強制的に初期化を行って処理を続行します。FORCE オプションは、アクセス・モニター開始タスクを他の方法で開始できず、かつシステムの IPL を実行することが望ましくない場合にのみ使用してください。通常の運用では、FORCE コマンドを使用してシステムを開始する必要はありません。このコマンドを使用する必要がある場合は、問題報告書を作成して問題を調査できるようにしておきます。

DEBUG-FORCE
: 開始時に DEBUG と FORCE の両方のオプションをアクティブにします。

zSecure で提供されている開始タスク・プロシージャー C2PACMON では、PPARM パラメーターを使用して、アクセス・モニター開始タスクを初期化するメインの Parmlib メンバーを指定することもできます。このパラメーターを使用して、プロシージャーに指定された値を指定変更できます。このパラメーターに対してプロシージャーで指定されるデフォルト値は C2PAMP です。

アクセス・モニター開始タスクをモニターまたは変更するための MODIFY コマンド

アクセス・モニター開始タスクがアクティブである場合、コンソール・オペレーターは MODIFY コンソール・コマンドを使用してアクセス・モニターの操作をモニ

ターまたは変更できます。MODIFY コマンドの別名として F コマンドを使用できます。以下の例は、アクセス・モニターの現在の状況とオプションを表示する MODIFY コマンドを示しています。

```
MODIFY C2PACMON,DISPLAY
```

コンマの後のテキストが、アクセス・モニター開始タスクでサポートされているオペレーター・コマンドであることを確認します。これらのコマンドについては、90 ページの『オペレーター・コマンド』を参照してください。

アクセス・モニター STC の停止

アクセス・モニター開始タスクを停止するには、コンソールから STOP コマンドを実行します。STOP コマンドの別名として P コマンドを使用できます。

```
P C2PACMON
```

STOP コマンドは、MODIFY コマンドのパラメーターとして実行することもできます。

```
F C2PACMON,STOP
```

アクセス・モニターのオペレーター・コマンドについて詳しくは、91 ページの『構成コマンド』を参照してください。

parmlib を使用したアクセス・モニター機能の構成

デフォルトでは、DD ステートメントは C2PACPRM データ・セットの C2PAMP メンバーを参照します。Parmlib に指定できるコマンドの例を以下に示します。

- 問題を診断するための DEBUG
- メモリー内データ・バッファーを管理するための OPTION
- データ取り込みインターバルや CARLa ステートメント・メンバーなどの項目を指定するための REPORT

入力パラメーターは、キーワード付きのコマンドの形式で指定できます。これらのコマンドを指定するときは、TSO の規則を使用します。C2PAMP パラメーター・ファイルについて詳しくは、79 ページの『アクセス・モニター開始タスクのパラメーター・ファイル』を参照してください。

アクセス・モニター・データの処理時におけるメモリーまたはデータ・ストレージの問題

メモリーまたはデータの保管で問題が発生した場合は、以下に示すアクセス・モニター・プログラムの構成設定の一部を調整する必要があります。

- アクセス・モニター・レコードに収集されたデータは、ディスクに保存するために CKRCARLA プログラムに転送されます。インターバルの期間は、Parmlib の SMFPRMxx の INTVAL パラメーターで制御されます。デフォルト値は 30 分です。
- アクセス・モニターは開始タスクとして実行され、システム内のすべてのタスクの RACF イベントを取り込みます。大量のアクティビティーが発生する大規模なシステムでは、このプログラムで必要となるバッファー・スペースの量が膨大になる可能性があります。バッファー・スペースが、アクセス・モニターの収集

を実行するには不十分であることがわかった場合は、インストール環境に合う値を指定するためにバッファー・スペース・パラメーターを調整できます。詳しくは、 79 ページの『アクセス・モニター開始タスクのパラメーター・ファイル』を参照してください。アクセス・モニター開始タスクからは、インストール環境に最適なバッファー・サイズを選択する際に役立つ、バッファー使用量統計メッセージが出力されます

- 日次収集と日次統合に使用されるデータ・セットは、必要なデータを保持できるだけの大きさであることが必要です。これらのデータ・セットの必要サイズは、環境に大きく依存します。必要であれば、アクセス・モニターの Parmlib メンバー C2PAMCLT および C2PAMCNT を使用して、これらのデータ・セットの割り振りと特性を調整できます。データ損失を防ぐために、これらのデータ・セットを注意深くモニターして、十分なスペースが割り振られるようにしてください。

zSecure 用の zEnterprise Data Compression (zEDC)

このトピックのガイドラインを使用して、組織での zEnterprise Data Compression の実装を計画します。

DFSMS (BSAM/QSAM) では、非 VSAM 拡張形式のデータ・セット用に、zEnterprise Data Compression (zEDC) という新しいタイプの圧縮機能が導入されました。zEDC 圧縮では、辞書がデータ・ストリーム内で非表示になるため、辞書を個別に作成する必要はありません。圧縮単位ごとに新しい辞書が開始されます。システムは、セグメントをそのまま解凍することができます。

zEDC 圧縮は、zSecure Admin アクセス・モニターの統合されたデータ・セットに対して正しく機能します。10 倍を超える圧縮率が可能です。

新規データ・セットに対する新規 zEDC 圧縮の要求は、既存の圧縮タイプ (汎用 (GENERIC) 圧縮と調整 (TAILORED) 圧縮) の要求に類似しています。要求は、データ・セット・レベルで選択することも、システム・レベルで選択することもできます。または、両方のレベルで選択することもできます。

データ・セット・レベル

既存の TAILORED (T) 値と GENERIC (G) 値のほかに、新しい zEDC 必須値 (zEDC Required: ZR) と zEDC 推奨値 (zEDC Preferred: ZP) を、データ・クラスの COMPACTION オプションで使用することができます。これらの値は、作成対象のデータ・セットに対して zEDC 機能を使用できない場合に、システムがどのように処理を続行するかを指定します。以下の説明を参照してください。

ZR zEDC 必須。システムで zEDC 機能がサポートされていない場合、または最小割り振り量の要件 (5 MB、2 次がない場合は 1 次が 8 MB) が満たされていない場合は、割り振り要求が失敗します。

ZP zEDC 推奨。割り振り要求が失敗することはありません。システムで zEDC 機能がサポートされていない場合は、TAILORED で圧縮したデータ・セットが作成され、最小割り振り量の要件 (5 MB、2 次がない場合は 1 次が 8 MB) が満たされていない場合は、非圧縮拡張形式のデータ・セットが作成されます。

システム・レベル
既存の TAILORED 値と GENERIC 値のほかに、新しい zEDC 必須値 (ZEDC_R) 値と zEDC 推奨値 (ZEDC_P) を、SYS1.PARMLIB の IGDSMSxx メンバー内の COMPRESS パラメーターで使用することができます。

zEDC_P
割り振り要求が失敗しないように、システムに対して指示を出します。システムで zEDC 機能がサポートされていない場合は、TAILORED で圧縮したデータ・セットが作成され、最小割り振り量の要件 (5 MB、2 次がない場合は 1 次が 8 MB) が満たされていない場合は、非圧縮拡張形式のデータ・セットが作成されます。

zEDC_R
システムで zEDC 機能がサポートされていない場合、または最小割り振り量の要件 (5 MB、2 次がない場合は 1 次が 8 MB) が満たされていない場合に、割り振り要求が失敗するよう、システムに対して指示を出します。

zEDC 圧縮をアクティブにするには、SET SMS=*xx* を使用するか、IPL で行います。データ・クラスは、引き続きシステム・レベルよりも優先されます。デフォルトは、引き続き GENERIC のままになります。

これまでに説明したマイクロコード更新が適用されている zEC12 GA2/zBC12 カードや zEDC Express カードがない場合でも、DFSMS は、データ・クラス内または PARMLIB 内のユーザー・オプションに基づいて、zEDC 圧縮形式のデータ・セットを作成することができます。この場合、BSAM/QSAM は、圧縮されていないデータを書き込みます。BSAM/QSAM は、ソフトウェア・インフレートを使用して、既存の圧縮データを解凍します。

zEDC 圧縮について詳しくは、「*z/OS MVS プログラミング:* 高水準言語向け呼び出し可能サービス」を参照してください。

QSAM/BSAM を介した zEDC Express – セットアップ: PARMLIB

新しい圧縮形式のデータ・セットを作成する際に (データ・クラスで COMPACTION=Y を指定)、システム・レベルで zEDC 圧縮の使用を要求するには、SYS1.PARMLIB: `COMPRESS(TAILORED|GENERIC|zEDC_R|zEDC_P)` の IGDSMS*xx* メンバー内の COMPRESS パラメーターに対して新しい値を定義します。 zEDC_P と zEDC_R の説明については、『システム・レベル』を参照してください。

zSecure Access Monitor で zEDC を使用するには

統合データ・セットの作成時に使用される SCKRSAMP(C2PAMCNT) に、適切な DATACLAS を SCKRSAMP(C2PAMCNT) に追加することができます。月次統合の場合は、適切な DATACLAS を C2PECDTE REXX に追加することができます。生成された TSO `ALLOC` コマンドの **MGMT** を、`MGMTCLAS` と `DATACLAS` で置き換えてください。 Y12MON データ・セットについても、同様の処理を実行します。

アクセス・モニターによってインストールされた RACF 出口の管理

アクセス・モニター開始タスクは、追加の RACF 出口を動的にインストールします。内部では、アクセス・モニター・プログラム (C2PACMON) が C2XACTV プログラムを呼び出し、必要な変更を完了します。C2XACTV プログラムは、スタンドアロン・プログラムとして呼び出すこともできます。アクセス・モニター RACF 出口は、2 レベルのアプローチを使用して実装されています。トップレベルは、RACF 制御ブロックにより直接示される出口ルーター・モジュールです。出口ルーター・モジュールは、最大 3 つの機能サブ出口 (プリプロセッシング、メイン、およびポストプロセッシングのサブ出口) を呼び出します。アクセス・モニターの開始時に RACF 出口がすでにアクティブな場合、オリジナル出口ルーチンはレベルが下がりメインのサブ出口になります。アクセス・モニターは、そのデータ収集出口をポストプロセッシング・サブ出口としてインストールします。

通常、アクセス・モニター・プログラムは、終了処理中にサブ出口と出口ルーター・モジュールを削除します。ただし、出口の削除に失敗する場合があります。それは、サブ出口がまだインストールされており、関連 RACF イベント用に呼び出されているような場合です。これらの出口は、開始タスクがアクティブではない場合は何の機能も実行しないため、削除するためのアクションを実行する必要はありません。当然、オリジナルのインストール・システム出口 (存在する場合) が、出口ルーター・モジュールによって呼び出されます。動的にインストールされたアクセス・モニター出口を削除する場合は、以下のようなジョブを実行できます。

```
//RUNIT    EXEC PGM=C2XACTV
//STEPLIB  DD DISP=SHR,DSN=<hlq.SCKRLOAD>
//SYSTSPRT DD SYSOUT=*
//C2XPRINT DD SYSOUT=*
//C2XIN    DD *
DYNEXIT DEACTIVATE   ICHRCX02
DYNEXIT DEACTIVATE   ICHRFX04
DYNEXIT DEACTIVATE   ICHRDX02
DYNEXIT DEACTIVATE   ICHRIX02
```

アクセス・モニター RACF 出口ルーター・モジュールは、機能サブ出口を呼び出す際に z/OS 動的出口サポートまたは直接分岐メソッドのどちらかを使用します。

z/OS 動的出口サポートが使用される場合、サブ出口は、標準の z/OS リカバリー・サービスを使用してそれぞれ保護されます。サブ出口が異常終了する場合、以降の異常終了を防ぐためにそのサブ出口は自動的に使用不可になります。サブ出口の使用不可はすぐには実施されず、同じサブ出口が 255 回異常終了した後でのみ実施されます。サブ出口が使用不可になった場合、以下のようなメッセージがオペレーター・コンソールとシステム・ログに示されます。

```
CSV430I MODULE ICHRCX02 FOR EXIT C2X.ICHRCX02 HAS BEEN MADE INACTIVE DUE TO
 ABEND=0C1000 REASON=00000001
```

この場合、サブ出口は以下のどちらかの方法で再度アクティブにすることができます。

- C2XACTV ユーティリティー・プログラムを使用して、影響を受ける出口を非アクティブおよびアクティブにします。これには、以下のような JCL が必要です。

  ```
  //RUNIT    EXEC PGM=C2XACTV
  //STEPLIB  DD DISP=SHR,DSN=<hlq.SCKRLOAD>
  //SYSTSPRT DD SYSOUT=*
  ```

```
//C2XPRINT DD SYSOUT=*
//C2XIN    DD *
DYNEXIT DEACT        ICHRCX02
DYNEXIT ACT          ICHRCX02
```

このジョブを実行するユーザーには、XFACILIT リソース・クラスの C2X.ICHRCX02 に対する UPDATE 権限が必要です。

- 場合によっては、次のようなオペレーター・コマンドを発行することも可能です。

  ```
  SETPROG EXIT,modify,exitname=c2x.ichrcx02.pst,modname=c2prcx02,state=active
  ```

- 次のオペレーター・コマンドを発行して、アクセス・モニター処理を再始動することも可能です。

  ```
  MODIFY C2PACMON,RESTART
  ```

  アクセス・モニター開始タスクはすべての内部サブタスクを停止して、C2XACTV プログラムを呼び出し、その RACF 出口を削除します。次に、プログラムの通常の開始時にこれらと同様のすべての必須機能を実行します。RESTART 機能は、C2PACMON タスク全体を停止および開始する効率的なメソッドとしての役割を果たし、再使用不可アドレス・スペースの損失など副次作用がありません。

動的出口のオプションについて詳しくは、93 ページの『OPTION コマンド』 を参照してください。 C2XACTV プログラムについて詳しくは、*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル の関連セクションを参照してください。

RACF EXIT 呼び出しモードの変更

アクセス・モニター OPTION ステートメントは、開始タスクの初期化時に使用されます。サブ出口呼び出しメソッドを切り替える場合は、C2XACTV プログラムを使用できます。DEACTIVATE 機能は、ストレージから出口を削除します。ACTIVATE 機能で CSVDYNEX または DIRECT のキーワードを使用して、希望のモードのルーター出口モジュールをインストールします。以下のようなジョブを使用すると、DIRECT モードに切り替えることができます。

```
//RUNIT    EXEC PGM=C2XACTV
//STEPLIB  DD DISP=SHR,DSN=<hlq.SCKRLOAD>
//SYSTSPRT DD SYSOUT=*
//C2XPRINT DD SYSOUT=*
//C2XIN    DD *
DYNEXIT DEACTIVATE ICHRFX04
DYNEXIT RECOVER    ICHRFX04
DYNEXIT ACTIVATE   ICHRFX04 DIRECT
```

C2XACTV プログラムについて詳しくは、*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル の関連セクションを参照してください。

アクセス・モニター機能のコマンド・リファレンス

- オペレーター・コマンドについては、90 ページの『オペレーター・コマンド』を参照してください。
- 構成コマンドについては、91 ページの『構成コマンド』を参照してください。

オペレーター・コマンド

これらのコマンドをオペレーター・コマンドとして指定する場合、追加のキーワードは必要ありません。コマンドは、最初の 4 文字に省略することもできます。例えば、CONSOLIDATE コマンドの場合は CONS と入力します。

CONSOLIDATE

日次統合プロセスを実行します。これには、以下のステップが含まれます。

1. 日次収集処理タスクが停止され、開始されます。
2. 日次収集データ・セットがクローズされ、C2PAMCLT テンプレート・ファイルに従って再割り振りされ、日次データ収集を続行するために再オープンされます。
3. 統合タスクが再始動されます。
4. 前日の日次収集データ・セットが、前日の要約データ・セットに統合されます。

日次収集処理タスクが再始動されると、Parmlib (デフォルト・メンバー C2PAMP) に指定されたアクセス・モニターのコマンドとパラメーターが、再始動プロセスによって活動化されます。この時点で、OPTION コマンドは処理されません。それ以外のコマンド (DEBUG や REPORT など) は処理されます。統合プロセスは、関連するすべての RACF イベントを継続して収集できるように、中断されないように設計されています。このため、プロセス全体が完了するまでに数分を要することがあります。

DEBUG

プログラムで生成される診断メッセージとモニター・メッセージを制御します。このコマンドは直ちに有効となり、次の日次統合が実行されるまで有効となります。

DEBUG コマンドのキーワードについて詳しくは、 91 ページの『DEBUG コマンド』を参照してください。

DISPLAY

アクセス・モニター機能の現在の状況とオプション設定を表示します。表示されるのは、現在のオプション設定、使用されているバッファー・スペース、現在使用中のバッファー数、および複数のエラー標識 (設定されている場合) の状況です。

DISPLAY コマンドでは、追加のキーワードがサポートされていません。

REPORT

取り込まれたデータの処理を制御するキーワードの値を設定します。新しい値は、次にその値が必要になるときに使用されます。MODIFY オペレーター・コマンドを使用してこのコマンドを実行する場合は、新しい値がほとんど瞬時に必要となることもあれば、まったく必要とならないこともあります。例えば、*Interval* パラメーターの新しい値は、次のインターバル の開始時点から使用されます。一方、*consolidatetime* の新しい値は使用されることがありません。このパラメーターは日次統合の実行が完了したときにのみ参照されるためです。その時点で、値は Parmlib に指定された値にリセットされます。

REPORT コマンドのキーワードについて詳しくは、 97 ページの『REPORT コマンド』を参照してください。

RESTART

アクセス・モニターのデータ収集処理を正常にシャットダウンし、直ちにタスクを再初期化します。アクセス・モニター開始タスクが実行されているアドレス・スペースは停止されません。したがって、アクセス・モニター機能の処理を再活動化するためにコンソール・オペレーター・コマンドを追加で実行する必要はありません。

開始タスクに対して RESTART コマンドを実行する場合と、STOP コマンドと START コマンドを続けて実行する場合の主な違いは、アドレス・スペース ID (ASID) が保持されるかどうかです。また、RESTART 処理では、開始タスク・プロシージャーで行われた変更が有効となりません。

RESTART コマンドを処理するために必要な時間の間は、一部の RACF アクセス要求または定義要求が記録されません。

STOP/START を続けて実行するとアドレス・スペースが再使用不可とマークされるため、多くの場合 RESTART コマンドが推奨されます。このコマンドを使用すると、潜在的に重要なシステム・リソースが失われるのを防止できます。

RESTART コマンドでは追加のキーワードがサポートされていません。

SIPL このコマンドは、IBM ソフトウェア・サポート担当者から要求された場合、またはリリース・マイグレーションで明確に必要となった場合にのみ実行します。このコマンドを実行すると、メモリー内のデータ構造がすべて解放され、システム・レベルのリンケージ索引 (LX) が失われ、アドレス・スペースが再使用不可とマークされます。システム・レベルの LX は、システムの IPL を実行しないとリカバリーできない限定リソースです。

アクセス・モニター・プログラムをアップグレードする場合は、インストール指示によって、この SIPL コマンドを使用して前のバージョンのアクセス・モニターをシャットダウンするように要求されることがあります。

SIPL コマンドでは、追加のキーワードがサポートされていません。

STOP アクセス・モニター開始タスクを正常にシャットダウンします。タスク終了後も一部のメモリーが予約されたままとなるため、アクセス・モニター開始タスクを次に再始動するときに重要なシステム・リソースを使用できます。STOP MODIFY コマンドの効果は、MVS STOP コマンドの場合と同じです。

STOP コマンドでは追加のキーワードがサポートされていません。

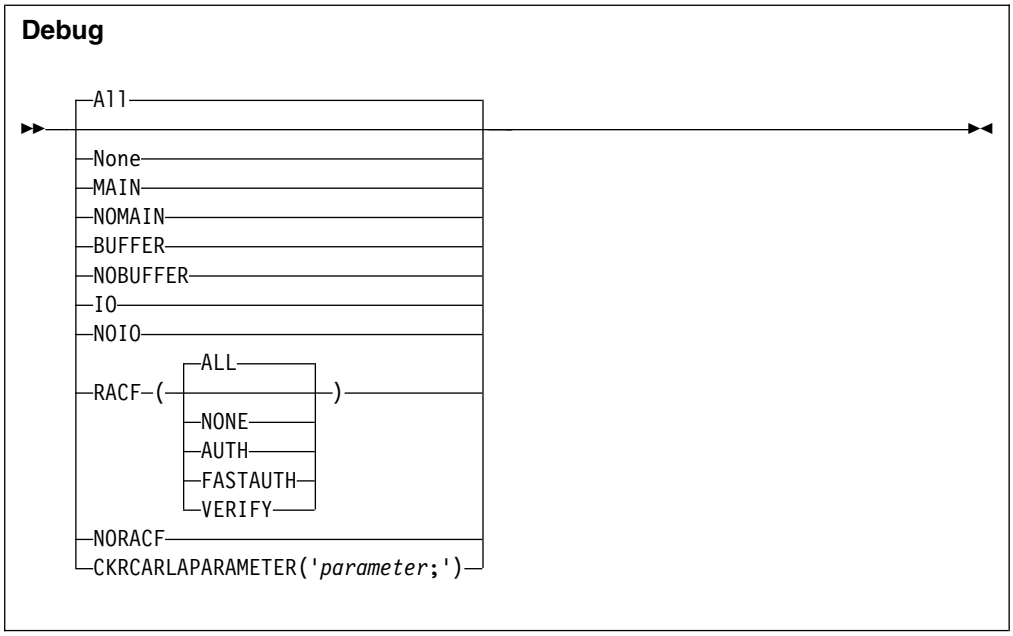
構成コマンド

通常は、OPTION コマンドと REPORT コマンドのみが必要となります。診断情報が必要である場合は、DEBUG コマンドを使用します。

DEBUG コマンド

コマンド構文を以下の図に示します。

注: 一度に指定できるオプションは 1 つだけです。複数のデバッグ・オプションを有効にするには、DEBUG コマンドを複数回実行します。DEBUG コマンドは、オペレーター・コンソールまたは Parmlib から実行できます。



このキーワードおよび変数は以下の値をとります。

All すべての診断メッセージをコンソールに出力します。ALL は、DEBUG コマンドにパラメーターを指定しなかった場合のデフォルトのメッセージ表示設定です。これらのメッセージのほとんどは、問題判別を支援するためのものであり、お客様が日常的に利用するものではありません。DEBUG BUFFER コマンドによって表示されるメッセージは、データ・バッファーに必要な最小サイズを確認するために日常的に使用されます。

None すべての診断メッセージの作成を非活動化します。

MAIN

メインライン処理に関連する診断メッセージをコンソールに出力します。これには、オペレーター・コマンドへの応答、すべてのサブタスクの初期化と管理、および主要なバッファー管理機能が含まれます。

NOMAIN

メインライン処理に関連する診断メッセージをコンソールに出力しません。これを設定すると、以下のタイプのメッセージが表示されなくなります。

- オペレーター・コマンドへの応答
- すべてのサブタスクの初期化と管理
- 主要なバッファー管理機能

BUFFER

各レポート作成間隔の最後に、バッファー使用統計をコンソール (および joblog と syslog) に出力します。これらのメッセージは、取り込まれたアクセス・モニター・レコードの数、および必要なストレージの量を特定するのに役立ちます。これらのメッセージを使用して、必要なバッファー・ストレージの最小量と最大量を追跡できます。

NOBUFFER

バッファー使用統計をコンソールに出力しません。

IO CKRCARLA に対するアクセス・モニター・インターフェース・ルーチンに

よって処理されたすべての操作を、SYSLOG を使って追跡します。このパラメーターを使用すると、大量のオペレーター宛 (WTO) メッセージが生成される場合があります。この機能は、IBM ソフトウェア・サポート担当者が、製品の内部的な問題を診断するためのものです。

NOIO
I/O 診断メッセージを生成しません。

RACF 収集データに関する診断情報をシステム・オペレーター・コンソール上に表示する RACF イベントを指定します。サブキーワードは、イベントのタイプを指定します。イベントが指定されていない場合、すべてのイベント・タイプの診断情報が表示されます。この機能は、IBM ソフトウェア・サポート担当者が、製品の内部的な問題を診断するためのものです。

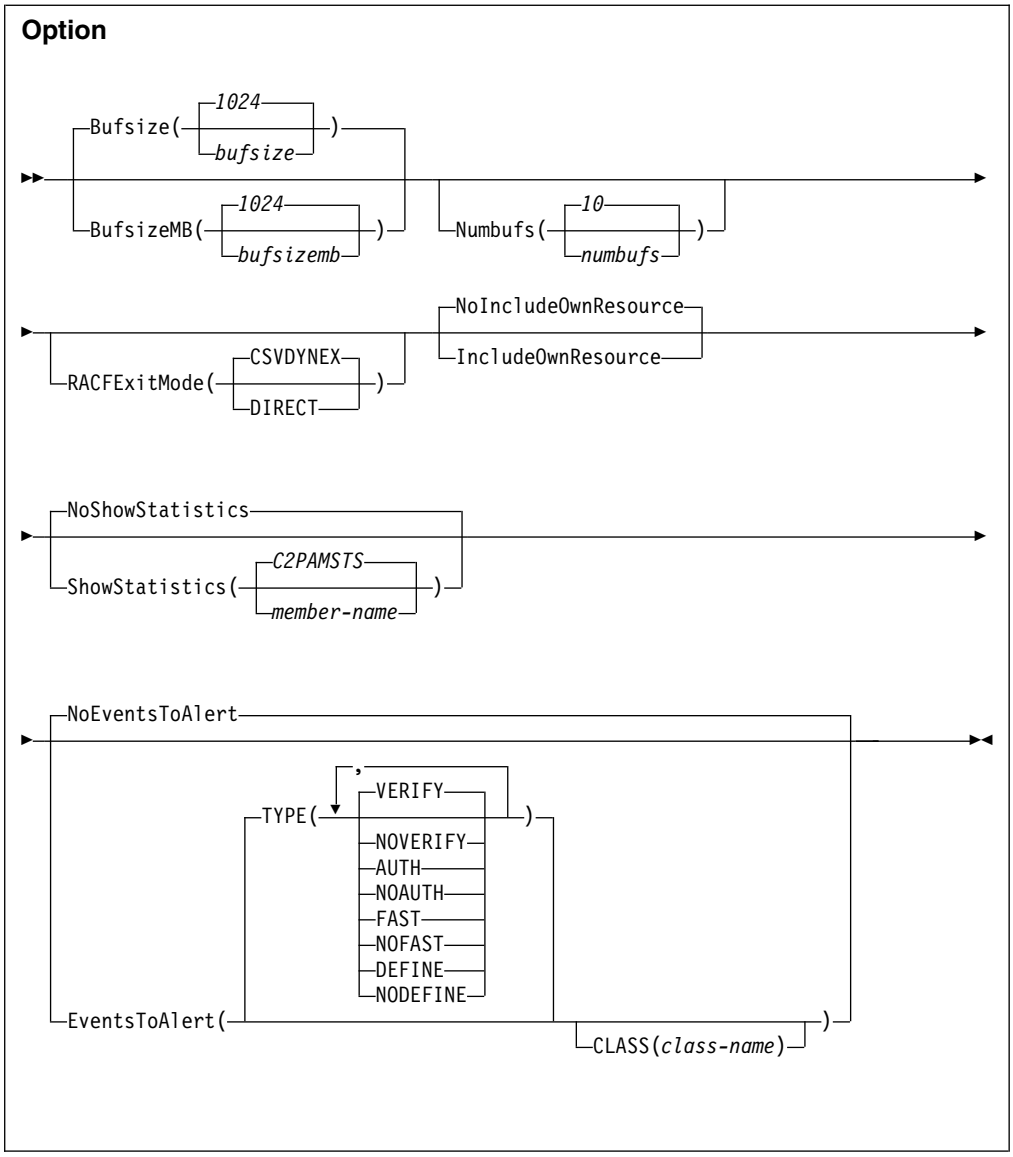
NORACF
RACF のデータ収集プロセスに関連するイベントに関するメッセージが発行されません。この機能は、IBM ソフトウェア・サポート担当者が、製品の内部的な問題を診断するためのものです。

CKRCARLAPARAMETER
C2PACMON 開始タスク内で使用される CKRCARLA のすべてのインスタンスに渡されるストリングを指定します。このストリングを指定する場合、末尾にセミコロンを付け、引用符で囲む必要があります。このパラメーターは、IBM ソフトウェア・サポート担当員が問題を診断するためのものです。ストリングの最大長は 63 文字です。

OPTION コマンド

OPTION ステートメントは、Parmlib からの場合のみ有効です。OPTION ステートメントの主な目的は、メモリー内データ・バッファーの数とサイズを指定することです。このステートメントを使用すると、アクセス・モニター開始タスク全体の所要時間に有効なその他の処理オプションも指定することができます。

OPTION ステートメントの構文は次のとおりです。



このキーワードおよび変数は以下の値をとります。

Bufsize/BufsizeMB

Bufsize/BufsizeMB キーワードを指定できるのは、起動時または RESTART 処理の実行時に OPTION ステートメントが使用される場合だけです。CONSOLIDATE 処理の実行中は、このキーワードは無視されます。

Bufsize/BufsizeMB により、*interval* 期間内におけるアクセス・モニター・レコードの保管に使用されるメモリー内バッファーのサイズを指定します。この期間に収集されるすべてのアクセス・モニター・レコードを格納する十分な大きさのバッファーになるようにしてください。バッファーが小さすぎる場合、アクセス・モニターのデータ取り込みルーチンは、未使用のバッファーに切り替えようとします。未使用のバッファーがない場合は、バッファー・オーバーフロー・メッセージが発行され、最も古いデータを含んでいるバッファーが代わりに使用されます。

Bufsize キーワードを使用する場合は、必要なバッファー・サイズをキロバイトで指定します。BufsizeMB キーワードを使用する場合は、サイズをメガバイトで指定します。バッファーの有効なサイズは、1 キロバイトと 1 ギガバイトの間です。指定したサイズは、最も近いメガバイトに丸められます。OPTION ステートメントで両方のキーワードを使用した場合は、最後に指定された値がプログラムによって使用されます。バッファーは、64 ビットのストレージに割り振られ、開始タスクの指定された MEMLIMIT の一部としてカウントされます。アクティビティーが多い期間に複数のバッファーを使用すると、必要なバッファー・サイズを大幅に削減できます。一般に、例えば、5 メガバイトのバッファーを 2 個指定するよりも、1 メガバイトのバッファーを 10 個指定するほうが効率的です。

Numbufs

Numbufs キーワードを指定できるのは、起動時または RESTART 処理の実行時に OPTION ステートメントが使用される場合だけです。
CONSOLIDATE 処理の実行中は、このキーワードは無視されます。

Numbufs により、割り振るバッファーの数を指定します。*numbufs* に対して有効な値は 2 と 32 の間です。バッファーの総数は、アクティビティーが多い期間中に取り込まれるすべてのアクセス・モニター・レコードを保持する十分な数になるようにしてください。

アクティビティーが多い期間に収集されるすべてのデータを保存するのに必要な *bufsize* を削減するには、複数のバッファーを指定します。追加のバッファーがない場合は、最も古いバッファーが代わりに使用されるため、データの損失が発生します。

INCLUDEOWNRESOURCE、NOINCLUDEOWNRESOURCE

ユーザーが自分のリソースへのアクセスを要求したときにログに記録されたアクセス・モニター・イベントについて、アクセス・モニター・レコードを作成するかどうかを決定します。対象となるリソースには、プライベート・データ・セットや、ユーザーのユーザー ID で実行されるジョブなどがあります。INCLUDEOWNRESOURCE オプションは、欠落しているイベントで問題が疑われる場合の診断に役立ちます。ただし、このオプションを指定すると、収集されるデータの量が大幅に増えるため、必要な場合のみ使用してください。このオプションのデフォルトは、
NOINCLUDEOWNRESOURCE です。

RACFEXITMODE

RACFEXITMODE キーワードを指定できるのは、起動時または RESTART 処理の実行時に OPTION ステートメントが使用される場合だけです。
CONSOLIDATE 処理の実行中は、このキーワードは無視されます。

RACFEXITMODE キーワードは、機能サブ出口が呼び出される場合、z/OS 動的出口サービスを使用するか、または直接的分岐命令を使用するかを指定します。z/OS 動的出口サービスを使用すると、柔軟性が増してリカバリーが可能になりますが、より多くのリソースを消費します。直接分岐命令を使用すると効率性は増しますが、呼び出されるサブ出口により提供されるものを上回る柔軟性やリカバリーを提供しません。パラメーターで選択可能な値は以下のとおりです。

CSVDYNEX

このキーワードは、RACF 出口ルーター・モジュールが z/OS 動的出口サービスを使用して、機能サブ出口を呼び出すことを指定します。このオプションは、呼び出されたサブ出口の柔軟性を高め、リカバリーを可能にします。

DIRECT

このキーワードは、RACF 出口ルーター・モジュールが直接分岐命令を使用して機能サブ出口を呼び出すことを指定します。このオプションは、呼び出されるサブ出口へのファスト・パスを提供します。

RACFEXITMODE キーワードを指定しない場合、または値を指定しない場合は、RACF 出口は z/OS 動的出口サービスを使用して呼び出されます。

SHOWSTATISTICS、NOSHOWSTATISTICS

このキーワードにより、指定した CARLa メンバーを含めるかどうか、各 SMF インターバルの終了時にその CARLa メンバーを実行するかどうかを指定します。SMF インターバルの終了時に、ストレージ内に収集されたデータが日次収集データ・セットに書き出されます。デフォルト・メンバーの *C2PAMSTS* は、このインターバル内に収集されたイベントの数とタイプに関する情報を、z/OS のシステム・ログと STC のジョブ・ログに書き出します。サンプルの出力を以下に示します。

```
C2P8000I Access data for period 31Aug2016 21:40:23 - 31Aug16 21:45:30
C2P8001I Totals           1365
C2P8001I        Auth      1090
C2P8001I        Fast         7
C2P8001I        Define       2
C2P8001I        Verify     266
C2P8002I Output records    100
```

SHOWSTATISTICS キーワードと付属の *C2PAMSTS* メンバーを使用する場合は、日次収集用の付属の C2PAMCOL メンバーを使用する必要があります。C2PAMCOL メンバーには、出力レコードの件数を計算する *C2PAMSTS* で使用される DEFTYPE ステートメントと DEFINE ステートメントが含まれています。*C2PAMSTS* メンバーは、開始タスク・プロシージャーの SC2PSAMP 連結によって組み込まれます。このキーワードのデフォルト値は NOSHOWSTATISTICS です。

EventsToAlert、NoEventsToAlert

特定の複数のイベントの情報を zSecure Alert に転送するかどうかを指定します。デフォルトでは、どのイベント情報も転送されません。詳細なキーワードやパラメーターなしで `EventsToAlert` キーワードのみを指定すると、zSecure Alert に VERIFY イベントが転送されます。現行リリースのアクセス・モニターでは、詳細指定として TYPE(VERIFY) のみがサポートされます。その他のイベントや選択項目での詳細なキーワードやパラメーターは構文で予約されています。これらのキーワードやパラメーターは現在サポートされていません。これらを使用すると、エラー・メッセージが表示されます。

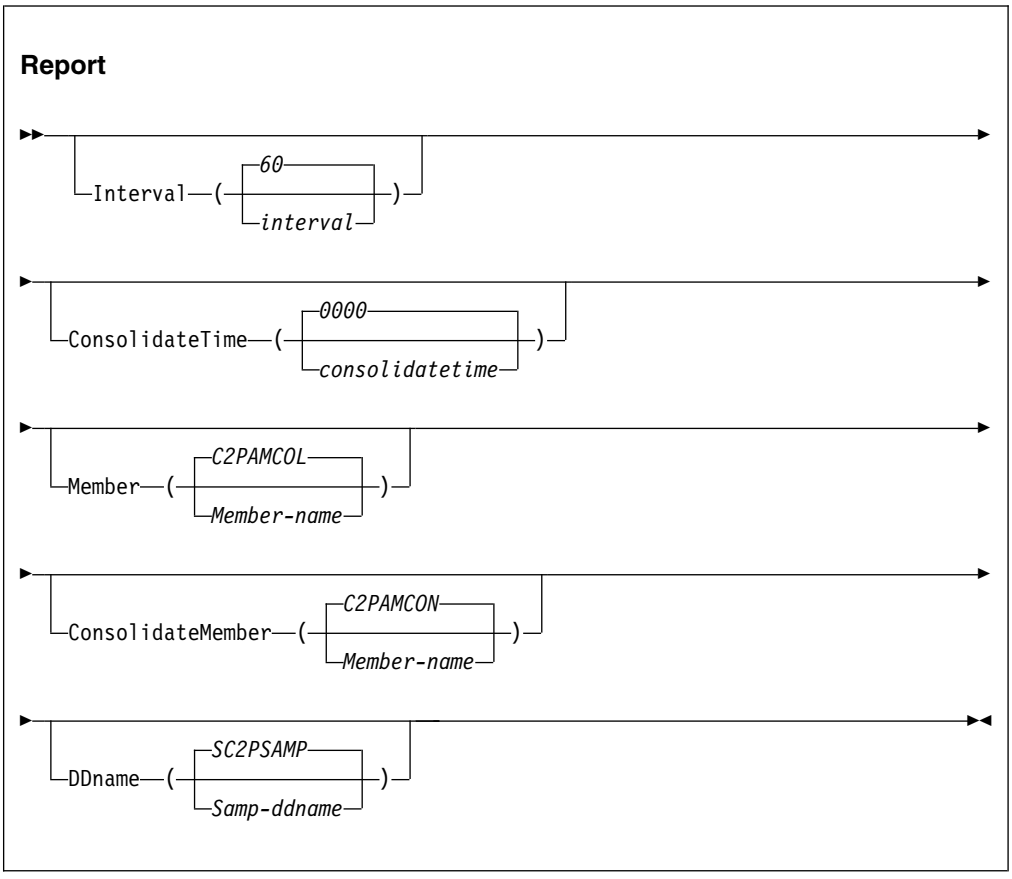
サポートされる取り込まれたイベントの転送をアクティブにするには、Option EventsToAlert または Option EventsToAlert(Type(Verify)) を指定します。サポートされる取り込まれたイベントの転送を非アクティブにするには、Option NoEventsToAlert または Option EventsToAlert(Type(NoVerify)) を指定します。

zSecure Alert へのイベント転送をアクティブにすると、アクセス・モニター開始タスクが追加の処理を実行します。この開始タスクは、REPORT ステートメントで定義された各間隔の開始時に、イベントを zSecure Alert に転送できるか確認します。アラート開始タスクがアクティブになっていない場合は、エラー・メッセージが発行されます。アラートを生成するためにイベント・データ (事前定義アラート 1122 など) を使用する場合にのみ、イベント転送をアクティブにします。

zSecure Alert へのイベント転送は、アクセス・モニターの ACCESS ファイルへのイベントの記録に影響しません。

REPORT コマンド

このコマンドでは、バッファー管理プロセスのタイミング、日次統合プロセスのタイミング、およびデータ収集プロセスと統合プロセスに使用される CARLa ステートメントのソースが制御されます。アクセス・モニター機能の各種タスクは周期的であることから、REPORT コマンドの効果は遅れて現れる場合があります。例えば、変更した *Interval* の値は、現在のインターバルが終了した後に初めて使用されます。REPORT コマンドの構文は、次のとおりです。



このキーワードおよび変数は以下の値をとります。

Interval

アクセス・モニター開始タスクが、収集したレコードを統計分析のために CKRCARLA タスクに転送するインターバルを指定します。値 *interval* では、時間間隔を秒単位で指定します。指定できる時間間隔は、10 から 3600 秒までです。デフォルト値は 60 秒です。

ConsolidateTime

アクセス・モニターが日次データ統合プロセスを開始する時刻を指定します。この指定された時刻に、現在の日次レコード収集データ・セットがクローズされます。前日の日次レコードは、C2PAMCNT ファイルを使って指定されたデータ・セットに統合されます。

consolidatetime の基本デフォルト値は、0000 (深夜 0 時) です。

メンバー **(Member)**

日次データ収集に使用される区分データ・セット内のメンバー名を指定します。ここには、SMF インターバル期間中にアクセス・モニター・レコードを合計する CARLa ステートメントが含まれています。SMF インターバルの最後に、収集されたレコードがディスクに書き込まれます。通常の状態では、このキーワードを指定する必要はありません。プログラムでデフォルトのメンバー名 C2PAMCOL が使用されます。

ConsolidateMember

日次統合プロセスで使用される区分データ・セット内のメンバー名を指定します。統合プロセスでは、SMF インターバル期間中のすべての個別レコードが合計されます。このプロセスによって、日次データを保管するために必要なスペースの量が大幅に削減されます。`ConsolidateMember` のデフォルト値は C2PAMCON です。通常このデフォルト値は、`C2PAMP` メンバー内で上書きされて、値 C2PAMCMP になります。このメンバーには、データ・セットのサイズを小さくするための追加の CARLa ステートメントが含まれています。また、メンバー `C2PAMMAP` で定義されている、インストール済み環境に固有のマッピング・ルールへの参照も含まれています。

DDName

アクセス・モニターの日次収集プロセスおよび統合プロセスを実行する CARLa ステートメントを含んだ区分データ・セットを指す JCL DD 名を指定します。`DDName` には、*member* および *consolidateMember* で指定されたメンバーが最低限含まれている必要があります。

第 11 章 RACF-Offline のセットアップ

RACF-Offline 機能は、システム内のアクティブでない RACF データベースで RACF コマンドを実行しテストできるようにする、zSecure Admin のコンポーネントです。このプログラムを使用すると、システムで実行する他のソフトウェアに影響を与えることなく、また専用のテスト・システムを使用することなく、RACF 定義の変更をテストすることができます。RACF-Offline について詳しくは、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」を参照してください。

RACF-Offline のインストールに関する手順は、「*Program Directory: IBM Security zSecure Admin RACF-Offline*」に記載されています。この製品をインストールしたら、追加のポストインストール・アクティビティーを実行して機能を活動化する必要があります。詳しくは、『RACF-Offline のインストールおよび活動化』を参照してください。

デフォルトのインストール・データ・セット名

RACF-Offline は、2 つのシステム・ライブラリーにインストールされます。

- ロード・ライブラリー SB8RLNK (APF 許可が必要)
- JCL サンプル・ライブラリー SB8RSAMP

詳しくは、「*Program Directory: IBM Security zSecure Admin RACF-Offline*」を参照してください。

RACF-Offline のインストールおよび活動化

このタスクについて

各タスクの実行方法については、表に示す手順を参照してください。

表 *5.* インストール・チェックリスト

ステップ	説明	ジョブ名	状況
1	RACF-Offline をインストールします。 「*Program Directory: IBM Security zSecure Admin RACF-Offline*」を参照してください。		
2	デフォルトのオプション・モジュール (B8ROPT) のビルド	B8RJOPT	
3	APF ライブラリーの Parmlib メンバーの更新	B8RSPROG	
4	TSO 許可のあるコマンドに対する Parmlib メンバーの更新 (オプション)	B8RSIKJ	
5	SMF 出口の Parmlib メンバーの検査		
6	テスト用の最小限の RACF 許可の定義	B8RJRDF	
7	RACF Offline のテスト	B8RJTST	

表 5. インストール・チェックリスト (続き)

ステップ	説明	ジョブ名	状況
8	105 ページの『RACF-Offline 使用可能化の確認』		

デフォルトのオプション・モジュール (B8ROPT) のビルド

このタスクについて

B8ROPT オプション・モジュールでは、製品で実行される許可の検査に使用される RACF 一般リソース・クラスを指定します。使用されるデフォルト・リソース・クラスは、XFACILIT クラスです。このオプション・モジュールには、以下を指定する追加の RACF-Offline コマンドを入れることもできます。

- デフォルトの RACF データベース。
- デフォルトの LOG データ・セット。
- SMF 処理オプション。

これらのオプション・コマンドは、リソース・クラスを指定する CLASS と、END コマンドの間に指定します。

以下に示すサンプル・ジョブ B8RJOPT を変更して、この情報を指定することができます。このジョブは、B8ROPT のインライン・ソースを持つアセンブリーおよびリンク・エディット JCL で構成されます。このジョブは、RACF-Offline をインストールしたデータ・セット内の B8ROPT メンバーにあります。

```
B8ROPT  CSECT
B8ROPT  AMODE 31
B8ROPT  RMODE ANY
CLASS   DC CL80'XFACILIT'                            RACF RESOURCE CLASS
RACFDB  DC CL80'RACFDB ''<your-offline-racfdb>'' '  DSNAME
SMF     DC CL80'SMF ID($B8R)'                        SMF OPTIONS
END     DC CL80'END'                                 MANDATORY END
        END
```

このジョブを実行する前に、使用する環境に適切なオプション設定でインライン・ソースを調整します。このジョブを実行しない場合は、RACF-Offline でデフォルトのリソース・クラスが使用され、デフォルトの RACF データベースは使用されません。

手順

以下の 2 ステップのプロセスに従い、ご使用の環境用のデフォルト・オプション・モジュールをビルドします。

1. B8RJOPT メンバーを編集して、使用するシステム環境向けのオプションを設定します。
   a. CLASS ステートメントで、製品で行われる許可の検査に使用されるリソース・クラス名を指定します。サンプル・ジョブで使用されているリソース・クラスは、XFACILIT です。

b. RACFDB ステートメントに対し、ユーザーが他の RACF データベースを選択しなかった場合に使用されるデフォルトの RACF データベースのデータ・セット名を指定します。この名前は、以下の例のように 2 つの単一引用符 (') で囲んで指定します。

```
RACFDB  DC CL80'RACFDB ''BCSC.ROFFLINE.TESTDB1'' SEQ(1)'   Dsname
        DC CL80'RACFDB ''BCSC.ROFFLINE.TESTDB2'' SEQ(2)'   Dsname
```

c. SMF ステートメントに対し、ご使用の環境に必要な SMF 処理を指定します。SMF ステートメントの完全な構文については、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」の RACF-Offline の章で説明されています。使用可能な SMF 処理オプションの 1 つは、SMFID を変更することです。以下に例を示します。

```
SMF     DC CL80'SMF ID($B8R)'                       SMF options
```

d. END ステートメントは変更しないでください。 RACF データベースが物理的に複数のデータベースに分割されている場合は、編集後の B8ROPT モジュールが以下の例のようになります。

```
B8ROPT  CSECT
B8ROPT  AMODE 31
B8ROPT  RMODE ANY
CLASS   DC CL80'$B8R'                                Resource class
RACFDB  DC CL80'RACFDB ''BCSC.ROFFLINE.TESTDB1'' SEQ(1)'   Dsname
        DC CL80'RACFDB ''BCSC.ROFFLINE.TESTDB2'' SEQ(2)'   Dsname
SMF     DC CL80'SMF ID($B8R)'                        SMF options
END     DC CL80'END'                                 Mandatory
        END
```

注:

1) RACFDB は RACF-Offline 制御コマンドです。dsname を引用符で囲んで指定すると、標準構文解析処理に役立ちます。この名前はアセンブラー・ソース内のリテラル・ストリングに含まれているため、B8ROPT ソース内ではこの値を 2 つの単一引用符 (') で囲みます。

2) SMF オプションは、RACF-Offline 制御コマンドです。このオプションを指定しないと、システム RACF データベースでの変更に対する SMF レコードを、オフライン・データベースでの変更に対して作成されたレコードと区別できなくなります。いくつかの処理オプションがサポートされています。SMF オプションについて詳しくは、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」の RACF-Offline の章を参照してください。

2. B8RJOPT ジョブを実行依頼します。 B8RJOPT の設定を環境に合わせて調整したら、ジョブを実行依頼して B8ROPT オプション・モジュールに変更を適用します。

APF ライブラリーの PARMLIB メンバーの更新

このタスクについて

RACF-Offline 機能を活動化するには、プログラム・ライブラリーを APF 許可にして、リンク・リスト内に配置します。どちらの操作も、オペレーター・コマンドまたは PARMLIB 内の準備済みメンバーを動的に使用して実行できます。インストール・ライブラリーには、環境に合わせて調整できるサンプルの Parmlib メンバー B8RSPROG が用意されています。

手順

1. ライブラリーをアクティブな APF リストに追加するために、以下の作業を行います。
   a. プログラム・ライブラリーのメンバーを Parmlib メンバーに追加します。

      ```
      APF ADD DSNAME(SYS1.SB8RLNK)                SMS
      ```

   b. T PROG=*xx* オペレーター・コマンドを実行して、Parmlib メンバーを更新します。
2. B8RACF プログラムを実行するために、STEPLIB ステートメントを使用するか、プログラム・ライブラリーをリンク・リストに追加します。

   初期テストを行う場合、または B8RACF を付随的に使用する場合は、steplib を使用します。
3. ライブラリーをアクティブなリンク・リストに追加するために、以下の作業を行います。
   a. 以下のようなメンバーを PARMLIB に追加します。

      ```
      LNKLST DEFINE NAME(LNKLSTB8) COPYFROM(CURRENT)
      LNKLST ADD NAME(LNKLSTB8) DSN(SYS1.SB8RLNK)
      LNKLST ACTIVATE NAME(LNKLSTB8)
      LNKLST UPDATE,JOB=*
      ```

   b. T PROG=*xx* オペレーター・コマンドを実行して、Parmlib メンバーを更新します。

TSO 許可のあるコマンドに対する Parmlib メンバーの更新 (オプション)

このタスクについて

RACF-Offline は、TSO コマンドとして、またバッチ・ジョブ内のメインプログラムとして実行できます。バッチ環境でジョブ・ステップ・プログラムとしてのみ RACF-Offline を実行する場合は、活動化プロセスでこのステップをスキップできます。

手順

RACF-Offline を TSO コマンドとして実行するには、TSO から実行できる APF 許可のあるコマンドのリストにいくつかのコマンドを追加します。

1. Parmlib メンバー IKJTSO*xx* で、以下のコマンドを AUTHCMD リストに追加します。

   ```
   B8RACF              /* zSecure Admin RACF-Offline */ +
   B8RVARY             /* zSecure Admin RACF-Offline */ +
   B8REPLAY            /* zSecure Admin RACF-Offline */ +
   B8RACFLG            /* zSecure Admin RACF-Offline */ +
   ```

   これらの行を、AUTHCMD ステートメントの最後に挿入する場合は、以下の作業を行います。
   - 正符号 (+) を使用して前の行から適切に継続されていることを確認します。
   - 右括弧 ()) を使用して行が適切に終了していることを確認します。

   説明とともにサンプルが、メンバー B8RSIKJ に用意されています。

2. TSO PARMLIB UPDATE(*xx*) コマンドを実行して、この Parmlib メンバーを活動化します。

SMF 出口の Parmlib メンバーの検査

システム RACF データベースに対して実行された通常の RACF コマンドで作成される SMF レコードは、RACF-Offline からオフライン RACF データベースに対して発行されたレコードと区別が付きません。識別を可能にするために、動的な SMF 出口 IEFU83、IEFU84、および IEFU85 を使用して、RACF-Offline で作成された SMF レコードを変更することができます。これらの出口は、システムで有効にしておく必要があり、また、システム全体あるいは関連するサブシステム (TSO、JES2、JES3 など) に対して指定しておく必要があります。以下の例は、動的な SMF 出口をセットアップするように構成された SMFPRM*xx* メンバーを示しています。

```
ACTIVE                          /* ACTIVE SMF RECORDING            */
DSNAME(SYS1.MAN1,
       SYS1.MAN2,
       SYS1.MAN3)
NOPROMPT                        /* DO NOT PROMPT OPERATOR          */
REC(PERM)                       /* TYPE 17 PERM RECORDS ONLY       */
MAXDORM(3000)                   /* WRITE IDLE BUFFER AFTER 30 MIN  */
STATUS(010000)                  /* WRITE SMF STATS AFTER 1 HOUR    */
JWT(0100)                       /* 522 AFTER 1 HOUR                */
SID(IDFX)
LISTDSN                         /* LIST DATA SET STATUS AT IPL     */
SYS(NOTYPE(40,42,99),EXITS(IEFU83,IEFU84,IEFU85,IEFACTRT,
           IEFUSI,IEFUJI,IEFU29),NOINTERVAL,NODETAIL)
SUBSYS(STC,NOTYPE(40,42,99),EXITS(IEFU29,IEFU83,IEFU84,IEFU85))
```

SMF 出口が有効になっていないと、オフライン RACF データベースを更新するコマンドに対して作成された SMF レコードが、システム RACF データベースを変更するように見えます。つまり、オフライン RACF データベースで変更されたレコードの SMF ID が、RACF データベースで変更されたレコードの SMF ID と同じになります。

最小限のテストのための RACF 許可

テスト段階では、UACC(NONE) と、アクセス・リスト上で UPDATE が指定されているテスト・ジョブ用のユーザー ID を使用して、最上位の総称プロファイルを定義します。XFACILIT リソース・クラスを RACF-Offline プロファイルのリソース・クラスとして使用していた場合は、以下のコマンドを使用できます。

```
SETR GENERIC(XFACILIT)
SETR CLASSACT(XFACILIT)
RDEF XFACILIT B8R.**        UACC(NONE)  OWNER(owner-of-your-choice)
PE   B8R.** CLASS(XFACILIT) ACCESS(UPDATE) ID(userid-of-the-tester)
SETR GENERIC(XFACILIT) REFRESH
SETR RACLIST(XFACILIT) REFRESH
```

ジョブ例 B8RJRDF には、このテスト用プロファイルの最小セットを定義するために使用できる JCL が含まれています。

RACF-Offline データベースを作成、テスト、およびトラブルシューティングするためのコマンド

RACF-Offline 環境でいくつかの RACF コマンドを実行することにより、RACF-Offline をテストできます。いずれかの RACF-Offline 機能を実行するには、許可プロファイルに対する RACF アクセス権が必要です。また、オフライン RACF データベースに対するアクセス権も必要です。

オフライン RACF データベースの作成

サンプル・ジョブ B8RJUT2 には、RACF データベースのコピーを作成する JCL が含まれています。

```
//STEP1   EXEC PGM=IRRUT200
//SYSPRINT  DD SYSOUT=*
//SYSIN     DD DUMMY
//SYSUT2    DD SYSOUT=*
//SYSRACF   DD DISP=SHR,DSN=Your-System-RACF-database
//SYSUT1    DD DISP=(NEW,CATLG),DSN=Your-Offline-database,
//             UNIT=3390,SPACE=(4096,space,,CONTIG,ROUND),
//             DCB=(LRECL=4096,RECFM=F)
```

このジョブを使用する環境に合わせて調整するか、または RACF データベースのコピーを作成するための標準インストール・ジョブを使用できます。サンプル・ジョブ B8RJUT2 を使用する場合は、RACF データベースの正しい名前とサイズを指定します。この JCL サンプルでは、4 KB のブロックに *space* が指定されています。現行の RACF データベースが IBM 3390 直接アクセス・ストレージ・デバイス上にシリンダー単位で割り振られている場合は、シリンダー数に 180 を掛けることで必要なブロック数がわかります。

オフライン RACF データベースに対するコマンドの実行

RACF データベースのコピーを作成した後に、その RACF データベースを使用していくつかの RACF-Offline コマンドを実行できます。RACF-Offline インストール・ライブラリー内のメンバー B8RJTST には、RACF-Offline コマンドを実行する以下のテスト JCL が含まれています。

```
//RUNIT    EXEC PGM=B8RACF
//STEPLIB  DD DISP=SHR,DSN=Your-Product.SB8RLNK
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
LU
END
//B8RPARM  DD *
RACFDB 'Your-Offline-database'
SMF ID($B8R)
//
```

この JCL を使用する環境に合わせて調整し、ジョブを実行します。以下の例は、このジョブの出力を示しています。

```
B8R121I B8ROPT options module successfully processed
B8R274I RACF DB used is BCSC.ROFFLINE.TESTDB
B8R304I New SMF-ID: $B8R
B8R143I B8RPARM file processed
B8R200A Enter RACF Command or "END"
LU
USER=B8RTEST  NAME=UNKNOWN  OWNER=B8R       CREATED=03.169
```

```
 ...
SECURITY-LABEL=NONE SPECIFIED
B8R200A Enter RACF Command or "END"
END
```

トラブルシューティング

RACF エラー・メッセージ (IRR51004I、IRR51011I、IRR52115I など) が出された場合や、ABEND 483-024 が発生した場合は、IRRMIN00 を PARM=UPDATE を指定して実行することで、オフライン RACF データベースを現行のテンプレートで更新します。

RACF-Offline 使用可能化の確認

開始時に、B8RACF コマンドで PARMLIB 内の IFAPRD*xx* がチェックされて RACF-Offline が使用可能か使用不可であるかが検査されます。

- RACF-Offline が使用可能である、つまり IFAPRD*xx* で定義されていない場合は、RACF-Offline の初期化が正常に続行されます。
- RACF-Offline が使用不可である場合は、メッセージ (B8R106E) が出されて、処理が停止します。

RACF-Offline を明示的に使用可能にするには、以下のような項目をアクティブな IFAPRD*xx* メンバーに追加します。

```
OWNER('IBM CORP')
        NAME('zSecure Admin')
        ID(5655-T01)
        VERSION(*) RELEASE(*) MOD(*)
        FEATURENAME('RACF-Offline')
        STATE(ENABLED)
```

RACF-Offline を使用不可にするには、上記のような項目を IFAPRDxxに追加します。その後に、STATE(ENABLED) パラメーターを STATE(DISABLED) パラメーターで置き換えます。

IFAPRDxx を更新したら、オペレーター・コマンド SET PROD=XX を実行してその更新を適用します。

第 12 章 zSecure Alert のセットアップ

zSecure Alert は、セキュリティー・サーバー (RACF) または CA-ACF2 で保護された z/OS システムのリアルタイム・モニターです。zSecure Alert は、システムのセキュリティーに関連する重要イベントの発生時に、アラートを発行します。zSecure Alert は IBM Security zSecure Suite の一部であり、zSecure Audit 上に構築されています。zSecure Alert について詳しくは、「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」を参照してください。

製品およびリリースの確認

IBM ソフトウェア・サポート・ライフサイクルについては、http://www.ibm.com/software/support/lifecycle/ を参照してください。 (「zSecure in all products」で検索してください。)

以前のリリースの zSecure Alert からアップグレードする場合の考慮事項

以前のリリースの zSecure Alert からアップグレードする場合、正しいソフトウェアの現行リリースを確実に使用するため、以下の手順のいずれかを使用する必要があります。システムで最後に IPL を実行して以降、zSecure Alert の開始タスク (C2POLICE) を始動していない場合には、アップグレード・ステップは特に必要ではありません。

- 以前のバージョンの C2POLICE を停止する場合は、SIPL コマンドを使用する必要があります。例えば、次のオペレーター・コマンドを使用できます。

  ```
  MODIFY C2POLICE,SIPL
  ```

  以前のリリースに戻る必要がある場合には、再度 SIPL コマンドを使用して C2POLICE を停止する必要があります。開始タスクを正常に停止した後には、以前のリリースのソフトウェアを使用して C2POLICE をすぐに開始できます。
- zSecure Alert 開始タスクの現行バージョンを停止した後、システムをシャットダウンしてから IPL を実行します。IPL の実行後、アップグレード済みコードを使用して、zSecure Alert 開始タスクを開始します。このシナリオでは、追加ステップを実行する必要はありません。

この手順のどちらも使用しない場合、始動が失敗して C2POLICE 開始タスクの ABEND (異常終了) が発生する可能性があります。始動が失敗してメッセージ C2P0183E と C2P0123E が表示された場合、FORCE 開始パラメーターを使用するとリカバリーできる場合があります。

zSecure Alert を構成および使用するための前提条件

このタスクについて

zSecure Alert は、zSecure 製品ファミリーの CARLa 駆動コンポーネントの 1 つです。 13 ページの『第 4 章 ソフトウェアのインストール』および「*Program Directory: IBM Security zSecure CARLa-Driven Components*」で説明されているよう

に、すべての CARLa 駆動コンポーネントで、SMP/E インストールが同時に行われます。すべての CARLa 駆動コンポーネントは、zSecure 構成を使用します。

手順

zSecure Alert を構成または使用する前に、以下の手順を完了しておく必要があります。

1. 13 ページの『第 4 章 ソフトウェアのインストール』および「*Program Directory: IBM Security zSecure CARLa-Driven Components*」に記載されている基本インストール・ステップを完了します。インストール・プロセスの基本的な共有部分については、13 ページの『第 4 章 ソフトウェアのインストール』で説明されています。
2. インストール・プロセスの一環として、低位修飾子 CKRINST を使用して、ライブラリーを作成およびカスタマイズします。このライブラリーには、zSecure アラートのセットアップ・ジョブが置かれます。
3. SCKRLOAD コンポーネントには APF 許可が必要です。24 ページの『ソフトウェアの APF 許可』を参照してください。
4. zSecure Alert を有効にする zSecure 構成が必要です。 デフォルトの zSecure 構成は、出荷時に *your.prefix*.CKRPARM(C2R$PARM) に収められています。独自の構成を使用することもできます。zSecure Alert を複数の z/OS イメージ上で使用したい場合は、少なくとも異なる SYS パラメーターを使用して、イメージごとに別々の zSecure 構成を用意する必要があります。追加情報については、23 ページの『z/OS 追加イメージへの zSecure データ・セットの配布』を参照してください。

   ISPF パネルにアクセスして zSecure Alert を構成し、その構成を C2POLICE および C2PCOLL 開始タスクに渡すためには、アラートに対応する zSecure 構成が必要です。詳しくは、31 ページの『第 6 章 ソフトウェアのデプロイメント』を参照してください。また、zSecure Alert にデータ・セットを割り振るときにも、この構成を使用できます。

   構成において、zSecure Alert に関連するパラメーターは以下のとおりです。

   ```
   //* Parameters only used for zSecure Alert
   //* SET C2PCUST='C2R.DATA.C2POLICE.C2PCUST'
   //* SET C2POLICE='C2POLICE'
   //* SET SIMESM=
   ```

   出荷時には、これらのパラメーターはコメント化されています。それらのコメントを外し、zSecure Alert 構成データ・セットおよびアドレス・スペース名について、独自の選択項目を指定する必要があります。

zSecure Alert アドレス・スペースの概要

zSecure Alert は開始タスクとして実行します。アラート生成に関するすべての情報を収集するために、SMF 出口を動的に定義します。また、それ自体を EMCS コンソールとしてインストールし、定期的に zSecure Collect プログラムを開始して、システム環境に関する情報を入手します。さらに、分析とレポートの生成のために、それぞれのレポート作成間隔で zSecure Audit を呼び出します。

以下のセクションでは、使用可能なコマンドとオプション、製品を構成するためのガイドライン、および関連するパフォーマンスへの影響について説明します。

インフラストラクチャー

zSecure Alert は、永続的にアクティブな開始タスク (STC) として稼働します。 1 つの z/OS システム・イメージ内で活動化できる zSecure Alert アドレス・スペースは、1 つだけです。これは、通常の開始コマンドを使用して、オペレーター・コンソールから開始されます。

SMF 出口は、システム内のすべてのタスクから、SMF ログ (つまり、MAN*x* データ・セットまたはシステム・ロガー LOGSTREAM) に書き込まれる前のすべての SMF レコードを取り込みます。それらのレコードは、可能な他の SMF 出口および後続の SMF 処理へ無変更のまま渡されます。アクティブな SMFPRM*xx* Parmlib メンバーで指定された SMF レコードだけを、SMF 出口によって取り込むことができます。

EMCS コンソールは、ハードコピー・セット (一般に SYSLOG と同じ) へ向けられたすべての WTO メッセージを取り込みます。そのメッセージをいずれも変更せずに、標準処理の進行を許可します。

取り込まれた SMF レコードおよび WTO メッセージは、オプションとして、フィルターに掛けられます。残りのレコードとメッセージは、その後の処理のために、STC の専用領域に割り振られたメモリー内バッファーに保存されます。

zSecure Collect プログラムは、zSecure Audit に付属しています。これは、システム・ライブラリー、UNIX ファイル、現行 Parmlib オプションなどに関する情報を定期的に収集するために使用されます。この情報は、いわゆる CKFREEZE ファイルに収集されます。この情報は、重要なシステム・データ・セットおよびリソースに関連した特定のイベントに関するアラートを生成するために使用されます。インストールによって明示的に、どのデータ・セットおよびリソースが重要あるかを指定する必要はありません。

一部のアラートは、その選択基準がシステム上のセキュリティー・データベースの内容と CKFREEZE ファイルの内容に基づいています。この情報は、プリプロセッシング・タスクによって定期的にリフレッシュされます。このタスクは、実際のレポート作成ステップに組み込まれる照会を準備します。

それぞれのレポート作成間隔中に、分析とアラート生成のためのデータが zSecure Audit に渡されます。アラートは以下の方法で発行できます。

- E メール
- ポケットベルまたは携帯電話への短いテキスト・メッセージ
- WTO。これは、例えば、自動化操作パッケージで取り込めます。
- SNMP トラップ。これは、Tivoli NetView や Tivoli Enterprise Console などのネットワーク・コンソールで取り込めます。
- UNIX Syslog メッセージ。これは例えば QRadar に送信できます。

注: コマンドが RRSF または CPF によって送られる場合、SMF レコードは (したがって、アラートも) 送信側と受信側のシステムで生成されます。

分析およびレポート作成機能は、レコード選択基準のタイプ、しきい値の使用、およびアラート・メッセージのフォーマット設定において高い柔軟性を備えています。また、アノテーションも許可します。例えば、関連するインストール・データまたはセキュリティー・データベースからのユーザー・データの部分を持つユーザー ID などです。さらに、他の外部ファイル内で一般的なキー・ベースの検索もできます。CARLa Auditing and Reporting Language (CARLa) について詳しくは、「*IBM Security zSecure: CARLa Command Reference*」を参照してください。

zSecure Alert は動的 SMF 出口を使用して、システム内のすべてのタスクから、すべての SMF レコードを取り込みます。しかし、それが可能になるのは、PARMLIB 内の SMF パラメーター・メンバーによって、それらの EXITS を有効にした場合だけです。ユーザーは、出口ルーチン IEFU83、IEFU84、および IEFU85 が、SYS およびすべてのサブシステムについて有効にされていることを確認する必要があります。 SMFPRM での EXITS の指定について詳しくは、「*MVS* 初期設定およびチューニング解説書」の関連する章を参照してください。

SMF EXIT 定義を変更し、`SET SMF` コマンドを使用してそれらを動的に活動化した場合は、`RESTART` コマンドによって開始タスクを再初期設定することも必要です。`RESTART` コマンドについて詳しくは、 121 ページの『zSecure Alert オペレーター・コマンド』を参照してください。

zSecure Alert 開始タスクでサポートされている DD 名

zSecure Alert 開始タスクでは、以下の DD ステートメントが使用されます。すべての環境ですべての DD ステートメントが必要になるわけではありません。SCKRPROC のメンバー C2POLICE は、zSecure Alert 開始タスクのサンプル・プロシージャーを提供します。

`C2P1OUT`
DD ステートメント `C2P1OUT` は、プリプロセッシング CARLa ステップの出力用作業データ・セットを識別します。この作業データ・セットは、アラートを生成する CARLa ステップに渡されます。

`C2PDEBUG`
DD ステートメント `C2PDEBUG` は、CKRCARLA、CKFCOLL、C2POLICE によって発行されるエラー・メッセージで使用される出力ストリームを識別します。

`C2PEMFRB`
DD ステートメント `C2PEMFRB` は、拡張モニターで使用される現在の基本構成に関する情報を保管するデータ・セットを識別します。このステートメントは、拡張モニターが有効になっている場合のみ必要です。

`C2RCMD`
DD ステートメント `C2RCMD` は、「Action Customization」パネルで「**Write TSO-RACF command to C2RCMD DD**」オプションを選択した場合に、各種のコマンドで使用される出力ストリームを識別します。

`C2RSMTP`
DD ステートメント `C2RSMTP` は、「Alert Destination」パネルで「**Write e-mails to C2RSMTP DD**」オプションまたは「**Write text messages to C2RSMTP DD**」オプションを選択した場合に、SMTP メッセージで使用される出力ストリームを識別します。

C2RSNMP

DD ステートメント C2RSNMP は、「Alert Destination」パネルで「**Write SNMP traps to C2RSNMP DD**」オプションを選択した場合に、SNMP トラップで使用される出力ストリームを識別します。

C2RSYSLG

DD ステートメント C2RSYSLG は、「Alert Destination」パネルで「**Write messages to C2RSYSLG DD**」オプションを選択した場合に、UNIX タイプの SYSLOG メッセージで使用される出力ストリームを識別します。

C2RWTO

DD ステートメント C2RWTO は、「Alert Destination」パネルで「**Write WTOs to C2RWTO DD**」オプションを選択した場合に、WTO メッセージで使用される出力ストリームを識別します。

CKFREEZE

DD ステートメント CKFREEZE は、標準のアラート生成プロセスで使用される CKFREEZE データ・セットを識別します。このデータ・セットは、C2PCOLL 開始タスクによって毎日更新されます。

CKGPRINT

DD ステートメント CKGPRINT は、CKGRACF プログラムが発行するエラー・メッセージで使用される出力ストリームを識別します。この DD ステートメントが必要になるのは、CKGRACF コマンドをアラート・アクション・コマンドとして指定した場合だけです。

PARMLIB

DD ステートメント PARMLIB は、1 次アラート構成メンバーを格納する C2PCUST データ・セットを識別します。

SC2PSAMP

DD ステートメント SC2PSAMP は、アラートの生成時に使用される標準の CARLa メンバーとカスタマイズされた CARLa メンバーを格納するデータ・セットを識別します。このデータ・セットには、2 次アラート構成メンバーも格納する必要があります。

STEPLIB

DD ステートメント STEPLIB と JOBLIB は、C2POLICE プログラムと CKRCARLA プログラムが格納されているライブラリーを識別します。

SYSINCKF

DD ステートメント SYSINCKF は、CKFCOLL 入力ステートメントを持つデータ・セットを識別します。 zSecure ソフトウェアのサポート・チームから依頼された場合のみ、この DD ステートメントを使用してください。

SYSPRCKF

DD ステートメント SYSPRCKF は、拡張モニター・プロセスのデータ収集で使用される CKFCOLL プログラムの出力用作業データ・セットを識別します。このステートメントは、拡張モニターが有効になっている場合のみ必要です。

SYSPRRPT

DD ステートメント SYSPRRPT は、アラート生成 CARLa ステップ (レポート作成フェーズともいいます) の出力用作業データ・セットを識別します。

SYSPRST1
DD ステートメント SYSPRST1 は、プリプロセッシング CARLa ステップ (ステージ 1 フェーズともいいます) の出力用作業データ・セットを識別します。

SYSTCPD
DD ステートメント SYSTCPD は、zSecure Alert 開始タスクで使用する必要がある TCP/IP 構成データ・セットを識別します。

SYSTSIN
使用されていません。

SYSTSPRT
DD ステートメント SYSTSPRT は、zSecure Alert 環境で実行される TSO コマンドのメッセージとデバッグ出力で使用される出力ストリームを識別します。これらは主に、拡張モニターのデータ・セットで使用される ALLOCATE コマンドです。

構成

デフォルトでは、zSecure Alert はシステム内のすべてタスクから、すべての SMF レコードを取り込みます。分析は、指定したインターバルで行われます。アクティビティーが多い大規模システムでは、必要なバッファー・スペースがかなりの大きさになる場合があります。ストレージの量を削減し、処理を高速化するために、開始パラメーターの一部として filterlist を指定し、特定のレコードだけを SMF レコード分析ルーチンに渡すことができます。そうすることにより、必要な処理時間も大幅に短縮できます。同様に、zSecure Alert はデフォルトですべての WTO メッセージを取り込むため、それらのメッセージをフィルターに掛けることができます。

デフォルトでは、データ分析は 60 秒ごとに行われます。環境データの読み取りは、1 時間ごとに行われます。入出力構成データを持つ CKFREEZE ファイルは、1 日 1 回リフレッシュされます。さらに、ヒストリー・データを使用するアラートを平均化するための時間枠 インターバルがあります。

フィルター処理、分析インターバル、およびバッファリングの値の指定は、PARMLIB およびコンソール・オペレーター・コマンドによって行うことができます。zSecure Alert 処理を制御する各種インターフェースについては、この章で説明されています。zSecure Alert ISPF インターフェースを構成定義に使用する場合、ほとんどの PARMLIB ステートメントは自動的に設定され、必要に応じて更新されます。

zSecure Alert ISPF インターフェースを使用すると、拡張モニター設定を構成できます。拡張モニター・アラートを選択できるのは、このソフトウェアのインストールとデプロイメントの担当者が、拡張モニター・アラートを有効にするプロセスを既に完了している場合だけです。

前に『インフラストラクチャー』の項で述べたように、SMF レコードの分析は zSecure Admin and Audit の機能を使用して行われます。可能なすべてのアラート状態は、CARLa スクリプトを使用して定義されます。それらは、始動 JCL 内の SYSIN DD ステートメントによって指定されます。インストールでは、定義されたアラートの選択基準としきい値を変更すること、また、その環境に固有のアラートを追加することができます。zSecure Alert に添付されているアラートの概要について

詳しくは、「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」で事前定義アラートに関する情報を参照してください。

制御

プログラムの起動時および実行中に、オペレーター・コンソールからのコマンドを使用して、プログラムの実行を制御できます。開始タスクを管理する直接オペレーター対話用のコマンドについては、 120 ページの『zSecure Alert 開始タスクの開始、停止、および変更』で説明されています。その他のコマンドについては、 128 ページの『その他のコマンド』で説明されています。それらのコマンドは、DEBUG、OPTION、REPORT、FILTER などです。DEBUG は診断用で、OPTION は、メモリー内データ・バッファーと zSecure Collect バックグラウンド・データ収集プロセスを管理するためのものです。REPORT は、レポート作成間隔とレポート対象のイベントを指定するために使用します。FILTER は、収集する SMF レコード・タイプと WTO メッセージを制限するために使用します。

ポストインストール・タスク

zSecure Alert のインストールの後に、以下のセクションで説明されているタスクを実行します。

開始タスクのセットアップ

zSecure Alert は開始タスクとして実行する必要があります。SCKRPROC に入っている C2PCOLL および C2POLICE プロシージャーと、zSecure Alert 対応 zSecure 構成メンバーを、zSecure Alert を使用するシステム上の開始タスク・プロシージャー・ライブラリーにコピーしてください。これらのプロシージャーをコピーする場合、異なる名前を選択できます。

- zSecure Collect 開始タスクの場合、選択する名前は、アラート構成のときに指定した名前です。「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」で、アラート構成時の一般設定の指定に関するセクションを参照してください。
- zSecure Alert アドレス・スペース (デフォルトは C2POLICE) の場合は、zSecure 構成の C2POLICE パラメーターで指定した名前を使用します。
- どちらのプロシージャーでも、アラート対応の zSecure 構成を指定する必要があります。
- zSecure Alert JCL 内で、PPARM パラメーターを更新し、実行に使用するアラート構成の名前を反映させる必要があります。PPARM パラメーターは、zSecure Alert 構成名に P を付加したものに等しくなければなりません。また、使用する zSecure Alert 構成の名前の中に、システム・シンボルを使用することもできます。 以下に例を示します。

  ```
  // PPARM=C2PDFLP        C2POLICE parameter member <setname>P
  ```

  これは、次のように変更できます。

  ```
  // PPARM=&SYSNAME.P     C2POLICE parameter member <setname>P
  ```

さらに JCL をカスタマイズする場合は、DEFAULT=YES を指定した OUTPUT ステートメントや、PURGE または HOLD の OUTDISP を決して組み込まないようにしてください。そのようにすると、すべての E メールおよびテキスト・メッセージ・アラートが送信されなくなります。

セキュリティー・リソース

許可は、zSecure Alert を実行しようとしているすべてのシステムに対して設定する必要があります。ただし、セキュリティー・データベースを共有している場合は除きます。zSecure Alert 開始タスクのセキュリティー要件には、以下が含まれます。

- C2POLICE および C2PCOLL アドレス・スペースを実行する予定のユーザー ID およびグループまたはログオン ID、あるいはそれらに選択した名前。C2PCOLL の場合、ユーザー ID またはログオン ID は RACF の OMVS セグメントか、ACF2 の OMVS レコードを持っている必要があります。
- 開始タスク名と、それらの開始タスクに必要なユーザー ID およびグループまたはログオン ID を割り当てるためのセキュリティー・リソース。
- RACF と ACF2 のどちらのシステムでも、XFACILIT リソース CKR.READALL および CKR.CKRCARLA.APF に対する READ 権限が必要です。ユーザー ID には、いくつかの OPERCMDS リソースに対する READ 権限も必要です。RACF 用のジョブ C2PZAIN0、または ACF2 用のジョブ C2PZAINA を参照してください。
- C2PCOLL のユーザー ID またはログオン ID は、XFACILIT リソース CKF.AUDIT および CKF.ALERT に対する READ 権限を持っている必要があります。ただし、ご使用のインストール済み環境で別のセキュリティー・クラスが構成された場合は除きます。 205 ページの『付録 A. サイト・モジュール』を参照してください。
- 開始タスクの出力の保護。
- データ・セット名と、それを対象とするプロファイル。PADS アクセスが使用されている場合、これには、PROGRAM プロファイルが含まれることもあります。

zSecure Alert を構成するユーザーには、以下のセキュリティー要件が適用されます。

- zSecure ソフトウェアが入っているデータ・セットに対する READ 権限。
- 使用できるオプションとアクションを決定する zSecure 固有のリソースに対するアクセス権限。 207 ページの『付録 B. zSecure のセキュリティー・セットアップ』を参照してください。
- 構成を実行するには、zSecure Alert 構成データ・セットに対する ACF2 用の UPDATE または WRITE 権限が必要です。READ 権限を持つユーザーは、構成を検査できます。
- ユーザーは、以下のリソースに対する READ 権限を持っている必要があります。

```
OPERCMDS: MVS.MODIFY.STC.C2POLICE.C2POLICE
OPERCMDS: MVS.MCSOPER.<userid>*  (the actual resource depending on the ISPF screen id)
TSOAUTH: CONSOLE
```

現在どのアラート構成がアクティブであるかを判別し、アラート構成をリフレッシュするためには、このアクセス権限が必要です。このアクセス権限がない場合は、次の両方が発生します。

- 「Managing alert configurations」パネルの「Act」標識がブランクのままになります。「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」で、オプション SE.A.A を使用したアラート構成の管理に関する情報を参照してください。
- アラート構成に対する更新は、オペレーターが `F C2POLICE,REFRESH` コマンドを発行するか、zSecure Alert アドレス・スペースが再始動されるまで、有効になりません。

zSecure Alert を複数の z/OS イメージ上で使用する場合、イメージ相互間の通信はありません。したがって、「Act」列は、アラート構成が別の z/OS イメージ上で使用中であってもブランクになり、他のイメージ上での自動リフレッシュはありません。

SCKRSAMP ライブラリーにある RACF 用のジョブ C2PZAIN0 と ACF2 用のジョブ C2PZAINA は、これらのセキュリティー・リソースのセットアップに役立つように提供されています。ただし、ユーザーが作成するセキュリティー・リソースは、総称プロファイルか個別プロファイルかの選択など、ユーザーのセキュリティー・ポリシーに従ったものであることが必要です。ユーザーは、RACF または ACF2 コマンドを検討した後に、このジョブの実行を決めることができます。

これらのジョブでは、一部は想定されたもので、zSecure 構成時にカスタマイズされたものではありません。ユーザーが、これらに変更を加えることがあります。

- zSecure Alert の開始タスクは、共通のユーザー ID またはログオン ID の下で実行されます。
- RACF システムでは、グループ名 SYSAUDIT はシステム監査員を格納するグループとして想定されていますが、ユーザーは別のグループを選択できます。SYSAUDIT グループに接続します。接続しなかった場合、zSecure Alert 用のデータ・セットの割り振り (ジョブ C2PZAIN1) は失敗します。
- RACF システムでは、グループ所有者は SYSAUTH に設定されます。
- プロファイルまたは規則は、SCKRLOAD データ・セット用にセットアップされており、その他のデータ・セットについては、別のプロファイルまたはルールが存在すると想定されています。異なるセットアップを使用する場合は、これをこのジョブで調整してください。
- RACF システムでは、PROGRAM プロファイル CKRCARLA が存在すると想定されています。PROGRAM プロファイルを使用しない場合は、PROGRAM プロファイルについての rdefine、ralter、および permit を削除できます。

必要なデータ・セット

zSecure Alert には、以下のデータ・セットが必要です。

- 専用の CKFREEZE データ・セット。このデータ・セットは、zSecure Alert を実行している z/OS イメージに関連したものでなければならず、したがって、他の z/OS イメージ上の zSecure Alert と共有することはできません。シリアライゼーションの問題のために、このデータ・セットを zSecure Admin または

zSecure Audit と共有することはできません。 C2PCOLL アドレス・スペースは、この CKFREEZE データ・セットの内容を定期的にリフレッシュします。

- C2POLICE アドレス・スペースの中間データを含んだデータ・セット。JCL 内では、これらのデータ・セットは SYSPRST1、SYSPRRPT、SYSPRCKF、C2P1OUT、および C2PEMFRB として識別されます。C2POLICE アドレス・スペースは、ユーザーがこれらを診断目的で表示できるよう、共有として割り振りますが、それ以外の場合、共有にしてはなりません。デフォルトでは、これらのデータ・セットの名前にシステム ID が含まれています。
- アラート構成データ・セット。これは、前に zSecure 構成で指定したデータ・セットです。これは、zSecure Alert をカスタマイズするために、オプション SE.A(zSecure Alert の構成) が使用されたときに、ISPF インターフェースから書き込まれます。このデータ・セットは、スペースの異常終了を防止するために PDS/E であることが必要です。PDS/E は、複数のシステム・イメージ間で共有できます。このデータ・セットが複数のシステム・イメージ間で共有される場合、異なる構成を異なるイメージに使用できますが、それらを同じものにすることもできます。

  アラート構成データ・セットが、その構成への侵入の試みに対して十分に保護されていることを確認してください。例えば、侵入者はアラート・メッセージに使用されている携帯電話番号を解明し、実際の侵入を開始する前に、それらのメッセージに侵入とは無関係に見えるメッセージをいっぱいに紛れ込ませる可能性があります。

  以前のリリースの zSecure からアップグレードする場合は、新しい構成データ・セットを作成しないでください。代わりに、以前に行った構成の結果を含むデータ・セットを引き続き使用してください。

  zSecure 1.13 では、アラート構成データ・セットに C2PXPARM という名前のメンバーが含まれている必要があります。次の方法のいずれかを使用して、このメンバーを作成できます。
  - ISPF でアラート設定トランザクションを実行し、アラート構成を検証およびアクティブ化します。ただし、共有構成では、この構成データ・セットを使用するすべてのアラート・インスタンスが新しいリリースで実行されるまで、このアクションを実行しないでください。
  - SCKRSAMP ライブラリーからメンバー C2PXPARM をコピーします。

SCKRSAMP ライブラリー内のジョブ C2PZAIN1 は、これらのデータ・セットの作成を支援するために提供されています。実行依頼する前に、以下のようにカスタマイズしてください。

- デフォルトの zSecure 構成を更新しなかった場合は、準備した zSecure Alert 対応 zSecure 構成を指定するために JCLLIB および INCLUDE ステートメントを変更します。
- zSecure Alert を複数の z/OS イメージ上にインストールする場合は、それぞれの zSecure 構成ごとに 1 回ずつ、ジョブを複数回実行する必要があります。できれば、対応する zSecure Alert を実行する z/OS イメージの下で、そのジョブを実行してください。それが (例えば、まだ IPL を実行していない z/OS イ

メージにインストールしているなどの理由で) 不可能な場合は、必ず、予定している z/OS イメージからアクセスできるボリュームに、すべてのデータ・セットが割り振られるようにしてください。

- zSecure Alert 構成データ・セットを複数の z/OS イメージ間で共有したい場合は、1 つを除くすべての C2PZAIN1 実行から、C2PCUST 割り振りを削除してください。

SMF 要件

zSecure Alert は、動的に定義された SMF 出口を使用して、システム内のすべてのタスクから、SMF ログ (つまり MANx データ・セット) に書き込まれる前のすべての SMF レコードを取り込みます。それらのレコードは、可能な他の SMF 出口および後続の SMF 処理に無変更のまま渡されます。SMF は、SMFPRM*xx* から選択されたレコードだけを作成します。また、SMF 動的出口は、その出口が SMFPRM*xx* で有効にされた場合にのみ、呼び出されます。先へ進む前に、選択したアラートに必要な SMF レコードを特定し、必要な SMF 出口を SMFPRM*xx* で有効にしてください。大部分のアラートには、以下のいずれかが必要です。

- RACF システムでは SMF レコード・タイプ 30 および 80。
- ACF2 によって書き込まれるタイプ。これはデフォルト・タイプが 230 ですが、インストールによって異なる場合があります。

詳しくは、「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」のアラートの説明を参照してください。有効にする必要がある SMF 出口は、IEFU83、IEFU84、および IEFU85 です。それぞれの出口点は、特定の環境内で、特定の SMF レコードに対して使用されます。これらの 3 つの出口点がシステム全体について、また定義済みのすべてのサブシステムについて有効になるようにしてください。

```
SYS(EXIT(IEFU83,IEFU84,IEFU85))
```

SMFPRM*xx* の指定が正しくないと、一部のアラート状態を検出できない場合があります。

拡張モニターのデータ・セット・パラメーターの指定

このタスクについて

拡張モニターの場合、C2POLICE 開始タスクは環境リフレッシュ・インターバルごとに CKFREEZE スナップショット・データ・セットを作成します。これらのデータ・セットを割り振るためのパラメーターは、C2PCUST データ・セットのメンバー C2PEMFRT に特殊なテンプレート形式で入力します。

手順

C2PEMFRT メンバーを作成するには、次のステップを行います。

1. SCKRSAMP データ・セットのメンバー C2PEMFRT を、使用している構成メンバー内の C2PCUST に指定したデータ・セットにコピーします。
2. コピーした C2PEMFRT メンバーを編集します。サンプルのメンバーは、以下の行で始まります。

```
alloc reuse fi(ckfreeze) -
DA('your.prefix.DATA.CKFREEZE.D&LYR2.&Lmon.&Lday..T&LHR.&LMIN.') -
mod space(2,1) cylinders release -
recfm(v b s) lrecl(X) blk(27998)
```

3. サンプル・メンバー内で、データ・セット名、スペース・パラメーター、およびデータ・セット配置パラメーターを、使用する環境のインストール規則に従うように編集します。
   - 複数の行を入力できます。
   - 継続行は負符号 (-) で示します。
   - 列 73 - 80 は無視されます。
   - コマンドの長さは合計で 255 文字未満にする必要があります。この長さには、行の最後の有効な文字と、その後の行継続文字 (負符号 (-)) との間にあるすべてのブランクが含まれます。
   - これらのメンバーに入力されるコマンドは、シンボル置換を除いて、完全かつ有効な TSO ALLOCATE コマンドでなければなりません。不要なキーワード、例えば、VOLUME キーワードなどは削除してください。
   - REUSE キーワードと FILE キーワードは、例に示されているままにしておく必要があります。指定するファイル名は CKFREEZE でなければなりません。
   - システム・シンボルは、コマンドの任意の位置に挿入できます。ユーザー・シンボルと JCL シンボルはサポートされていません。
   - データ・セットのレコード・フォーマットは、RECFM(V B S) キーワードで示されているように、ブロック化可変スパンでなければなりません。
   - データ・セット名の指定は、ストリング DA(' で始める必要があります。
   - データ・セット名の指定は、ストリング ') で終了する必要があります。
   - 指定されたデータ・セット名は、D&LYR2&LMON&LDAY.T&LHR&LMIN で終わる必要があります。この方法でデータ・セット名を指定すると、タイム・スタンプが Dyymmdd.Thhmm のフォーマットになります。
   - シンボル置換後のデータ・セット名が有効である限り、必要な任意の先行修飾子を指定できます。
   - サンプル・データ・セット名の中の修飾子 DATA を S&sysclone. によって置き換えて、スナップショット・データ・セットを作成したシステムを反映させることができます。
   - 割り振り用に追加のパラメーターを指定できます。例えば、ご使用のインストール済み環境で STORCLAS や MGMTCLAS などの SMS 構造の指定がサポートされている場合は、ここでそれらの構造を使用できます。
   - オプションのコメント行は最後に組み込む必要があります。コメントは、コメント区切り文字の /* と */ の間に組み込みます。

   注: 意図した CKFREEZE スナップショット・データ・セットだけが一致するよう、修飾子を最後の日時修飾子の前に指定することが重要です。これらの修飾子で始まるすべてのデータ・セットは、一時的な CKFREEZE データ・セットと見なされ、最終的には削除されます。
4. C2PEMFRT メンバーを保存します。

アラート構成データ・セットのセットアップ

「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」で説明されているように、アラート構成をセットアップしてください。 zSecure ISPF インターフェースに入る前に、まず、zSecure Alert 構成データ・セットを作成します。

zSecure Alert アドレス・スペースの開始

すべての構成ステップの状況が「OK」の場合、MVS コマンド `START C2POLICE` で zSecure Alert 開始タスクを開始することができます。デフォルトの C2PDFL 以外の zSecure Alert 構成を使用する場合は、C2POLICE 開始タスク JCL 内の `PPARM` パラメーターを変更してください。つまり、`PPARM` は、構成名の後に接尾部 P を付けたものでなければなりません。別の方法として、開始コマンドで `PPARM` を指定することもできます。

zSecure Alert アドレス・スペースを初めて開始した後、次の MVS コマンドを発行します。

```
F C2POLICE,COLLECT
```

このコマンドを発行することにより、zSecure Alert アドレス・スペースは確実に、一致する CKFREEZE ファイルを使用するようになります。それ以後のリフレッシュは、自動的に実行されます。

自動化操作ソフトウェアまたは `PARMLIB` メンバー `COMMND`*xx* を使用して、各 IPL の直後に zSecure Alert を開始します。ただし、OMVS が完全に初期化されるまでは、zSecure Alert を開始しないでください。次のメッセージは、OMVS が完全に初期化されたことを示しています。

```
BPXI004I OMVS INITIALIZATION COMPLETE
```

zSecure Alert は TCP/IP サービスを必要とするため、待機が必要です。

プリアンブル・メンバー C2PXDEF1

C2PXDEF1 メンバーは、まだ存在しておらず、更新が許可されている場合、SE.A トランザクションによって zSecure Alert 構成データ・セット内に自動的に (空で) 作成されます。このメンバーは、zSecure Alert 処理のプリアンブルとして、zSecure Alert アドレス・スペース内で、しかも「検査」時に使用されます。これは、IBM ソフトウェア・サポートによる指示に従ってのみ使用するように作られています。

他のソフトウェア内のエラーが原因で、有効でないデータが書き込まれる場合もあります。例えば、正しくフォーマット設定されていない SMF レコードのために、zSecure Alert でエラー・メッセージが発生することがあります。しかし、それらのエラー・メッセージは、エラーの原因が無効な入力にあることを明確に示していないため、通常、 IBM ソフトウェア・サポートへの問い合わせが行われます。そのような場合、IBM では、OEM ベンダーで問題が解決されるまで、一時的に C2PXDEF1 内で使用できる一連の CARLa ステートメントをお客様にお送りしています。

zSecure Alert 開始タスクの開始、停止、および変更

zSecure Alert は、オペレーター・コンソールから、START コマンドによって開始されます。このコマンドは、該当するシステム proclib からプロシージャーを実行します。開始パラメーターを指定することが可能です。それらのパラメーターは、START コマンド自体で指定できます。そのような START コマンドの例を以下に示します。

```
S C2POLICE,PARM.C2POLICE=DEBUG
```

使用可能な開始パラメーターについては、『zSecure Alert START パラメーター』を参照してください。

zSecure Alert は、開始プロシージャーでの PARMLIB DD ステートメントからのパラメーター入力もサポートしています。PARMLIB DD ステートメントは、通常の稼働環境を決定するパラメーターに使用されます。これらのパラメーターは、キーワードを伴ったコマンドの形式で指定できます。これらのコマンドには、TSO 規則が使用されます。サポートされるコマンド、キーワード、およびパラメーターについて詳しくは、以下のページの各セクションを参照してください。

開始タスクの実行中に、コンソール・オペレーターは zSecure Alert の機能をモニターまたは変更するコマンドも発行できます。これらのコマンドはすべて、MODIFY コンソール・コマンドによって発行できます。MVS では、F コマンドを MODIFY コマンドの別名として使用できます。そのようなコマンドの例を以下に示します。

```
MODIFY C2POLICE,DISPLAY
```

コンマの後のテキストは、サポートされている zSecure Alert オペレーター・コマンドのいずれかでなければなりません。

開始タスクを終了するために、コンソール・オペレーターは STOP コマンドを発行できます。MVS では、P コマンドを STOP コマンドの別名として使用できます。以下に例を示します。

```
P C2POLICE
```

STOP コマンドは、MODIFY コマンドのパラメーターとして実行することもできます。

```
F C2POLICE,STOP
```

zSecure Alert で使用できるオペレーター・コマンドについて詳しくは、 121 ページの『zSecure Alert オペレーター・コマンド』を参照してください。

zSecure Alert START パラメーター

zSecure Alert は、2 つの開始パラメーターをサポートしています。開始パラメーターは、オペレーターが START コマンドの一部として使用できます。

```
S C2POLICE,PARM.C2POLICE=FORCE
```

zSecure Alert の通常の実行では、開始パラメーターを指定する必要はありません。デフォルトでは、zSecure Alert は既に実行されているかどうかを検出し、適切なエラー・メッセージを発行して終了します。また、zSecure Alert が以前にシャットダ

ウンされている場合は、1 回だけ取得できる重要なシステム・リソースが再利用されます。それらのシステム・リソースをシステムに戻すことはできません。このため、システム・リソースが浪費されることがありません。

一部のエラー状態では、zSecure Alert の初期化が失敗します。そのような状態では、オプションの START パラメーターの 1 つが必要になることがあります。

DEBUG
初期化の最初の部分で、診断メッセージを発行する必要があることを指定します。この診断メッセージを使用して、標準の PARMLIB パラメーターを処理する際に発生する可能性がある問題を特定することもできます。この設定は、オペレーター・コンソールまたは PARMLIB から後続の DEBUG コマンドが発行されるまで効力を持ちます。

FORCE
前回の実行に関係なく、初期化を続行する必要があることを指定します。FORCE オプションを使用するのは、zSecure Alert を正常に開始できない場合のみにしてください。 FORCE オプションにより、システムの IPL を実行することなく zSecure Alert を開始できる場合があります。通常の操作中は、FORCE オプションが必要になることはありません。

DEBUG-FORCE
DEBUG と FORCE の両方のオプションを開始時にアクティブにする必要があることを指定します。

zSecure Alert オペレーター・コマンド

MODIFY コンソール・コマンドの中で使用できる zSecure Alert オペレーター・コマンドについては、次のリストで説明します。

STOP zSecure Alert 開始タスクの実行を停止します。この結果、タスクの正常シャットダウンが行われます。一部のメモリーは、タスクの終了後も予約済みのままで残ります。これは、開始タスクを後で再始動するとき、一部の重要なシステム・リソースを再利用できるようにするためです。STOP MODIFY コマンドの効果は、MVS STOP コマンドの場合と同じです。

STOP コマンドでは、追加のキーワードがサポートされていません。

RESTART
このコマンドを実行すると、zSecure Alert 処理が正常シャットダウンされ、それに続いて即時に再初期設定が行われます。開始タスクを実行しているアドレス・スペースは、終了しません。zSecure Alert 処理を再活動化するために、追加のコンソール・オペレーター・コマンドは必要ありません。開始タスクの場合、再始動と直後に START コマンドを伴う STOP コマンドの主な違いは、ASID の保存です。また、開始タスク・プロシージャー内に変更があっても、それは RESTART 処理のときに影響を受けません。RESTART コマンドの処理に必要な時間中、アラート状態は認識されず、レポートは生成されません。

STOP/START を続けて実行するとアドレス・スペースが再使用不可 とマークされるため、多くの場合 RESTART コマンドが推奨されます。このコマンドを使用すると、潜在的に重要なシステム・リソースが失われるのを防止できます。

RESTART コマンドでは追加のキーワードがサポートされていません。

REFRESH

このコマンドを実行すると、PARMLIB で指定されたコマンドとパラメーターの再処理が行われ、一部のサブタスクがリフレッシュされます。すべての PARMLIB コマンドを処理できるわけではありません。OPTION コマンドは、REFRESH 時にはサポートされません。プリプロセッシング・サブタスクが開始され、レポート作成タスクが終了して再始動されます。アラートを生成するレポート作成タスクは、プリプロセッシング・タスクが完了しないと再始動できないため、リフレッシュ・プロセスが完了するまでに数分かかる場合があります。この間にも、アラートは既存の構成に従って生成されます。

zSecure 収集プロセスの実行中は、REFRESH コマンドは受け入れられますが、ほとんどの処理は遅延します。収集プロセスが終了すると、説明したサブタスクの開始処理と再始動処理が実行されます。

REFRESH コマンドでは、追加のキーワードがサポートされていません。

COLLECT

このコマンドを実行すると、zSecure Collect 開始タスクが即時に同期実行されます。処理は、通常の zSecure Collect タスクのスケジュールされた開始の場合と同じです。開始タスクの名前は、*CollectSTCName* パラメーターによって制御されます。通常の STC のスケジュールされた開始は影響を受けず、*CollectTime* によって指定された時刻のままです。

zSecure Collect プロセスの実行中は、レポート作成タスクはアクティブのままになります。アラートは通常どおりに発行され続けます。プリプロセッシング・タスクは、収集タスクが完了するまで遅延する場合があります。

COLLECT コマンドでは追加のキーワードがサポートされていません。

SIPL このコマンドは、緊急の状態でのみ使用すべきものです。このコマンドを実行すると、すべてのメモリー内データ構造が解放され、システム・レベル LX、つまりリンケージ索引が失われ、アドレス・スペースには再使用不可のマークが付きます。システム・レベル LX は限定リソースであり、システムの IPL なしにはリカバリーできない場合があります。zSecure Alert のリリースをアップグレードする場合、インストール構造は、この SIPL コマンドを使用して以前のバージョンをシャットダウンすることを必要とします。

SIPL コマンドでは、追加のキーワードがサポートされていません。

DISPLAY

このコマンドを実行すると、zSecure Alert 処理の状況とオプションが表示されます。現行オプション、使用されているバッファー・スペース、その時点で使用中のバッファー数、いくつかのエラー標識 (設定されている場合) の状況が表示されます。

DISPLAY コマンドでは、追加のキーワードがサポートされていません。

REPORT

このコマンドを使用すると、取り込んだデータの処理を制御するキーワードの値を設定できます。新しい値は、次にプログラムがその値を参照するときに使用されます。MODIFY オペレーター・コマンドで指定された値は、次

の REFRESH 中に PARMLIB からの値で上書きされます。REFRESH はコンソール・オペレーターによって開始される場合もあれば、各 *Stage1Interval* の最後に自動的に開始される場合もあります。

FILTER

このコマンドを使用すると、SMF レコードおよび WTO メッセージがメモリー内バッファーに取り込まれる前に、それらについてのフィルター処理基準を設定できます。これらのフィルター基準を効率的に使用すると、必要なバッファー・スペースの量を大幅に削減できます。新しいフィルター基準は、即時に有効になります。すべてのキーワードの完全な記述については、135 ページの『FILTER コマンド』を参照してください。

注**:** MODIFY オペレーター・コマンドで指定された値は、次の REFRESH 中に PARMLIB からの値で上書きされます。REFRESH はコンソール・オペレーターによって開始される場合もあれば、各 *Stage1Interval* の最後に自動的に開始される場合もあります。

DEBUG

このコマンドは、プログラムによって生成できる診断メッセージおよびモニター・メッセージを制御します。すべてのメッセージは、「*IBM Security zSecure:* メッセージ・ガイド」で説明されています。このコマンドは、即時に有効になります。すべてのキーワードの完全な記述については、128 ページの『DEBUG コマンド』を参照してください。

DIAGNOSE

このコマンドは、詳細情報の表示や診断タスクの実行に使用します。このコマンドを使用すると、問題判別のために、一部の内部制御ブロックおよびテーブルをダンプすることができます。表示される制御ブロックは、IBM サポート担当員が特定の問題を診断するためのものです。すべてのキーワードの完全な記述については、130 ページの『DIAGNOSE コマンド』を参照してください。

SMF 出口のクリーンアップおよび非アクティブ化

通常、C2POLICE は、たとえ取り消された場合でも、その環境をクリーンアップします。C2POLICE を停止し、zSecure Alert SMF 出口が何らかの理由でアクティブであっても、以下の手順を使用して、それらの出口を非アクティブにすることができます。コマンド構文については、IBM *MVS* システム・コマンド のマニュアルを参照してください。コマンド権限については、「*MVS* 計画*:* 操作」を参照してください。

最初に、次のコマンドを発行して、SMF 出口モジュールがアクティブであるかどうか、およびその出口名を判別します。

```
d prog,exit,mod=c2psmfu8
```

出力は、以下の例のようになります。

```
CSV462I 13.11.54 PROG,EXIT DISPLAY 494
MODULE  C2PSMFU8
EXIT(S) SYS.IEFU85       SYS.IEFU84       SYS.IEFU83
EXIT(S) SYSTSO.IEFU83    SYSSTC.IEFU83    SYSASCH.IEFU83
EXIT(S) SYSJES2.IEFU83   SYSJES3.IEFU83   SYSTSO.IEFU84
```

```
EXIT(S) SYSJES3.IEFU84   SYSASCH.IEFU84   SYSJES2.IEFU84
EXIT(S) SYSSTC.IEFU84    SYSTSO.IEFU85    SYSSTC.IEFU85
EXIT(S) SYSASCH.IEFU85   SYSJES2.IEFU85   SYSJES3.IEFU85
```

次に、名前によってそれぞれの出口を非活動化します。

```
setprog exit,modify,en=<exit name>,mod=c2psmfu8,state=inactive
```

構成のガイドラインとパフォーマンスへの影響

zSecure Alert 処理は、いくつかの部分から構成されています。開始時に指定したパラメーターは、zSecure Alert の全体的なパフォーマンスとそれが他のユーザーに及ぼす影響を左右します。この点で最も重要なパラメーターは、*intervals* と *filters* です。

フィルター

112 ページの『構成』に示されているとおり、ほとんどの場合、フィルター処理にはパフォーマンス上の問題があります。ただし、フィルターを狭くしすぎると、アラートが失われる原因となります。フィルター処理は、WTO メッセージ ID および SMF レコード・タイプ、およびサブタイプのみに基づいて行われます。実際のイベント選択は、個々のアラートのスケルトン・メンバーの CARLa で行う必要があります。フィルターを指定しなかった場合は、すべての SMF レコードと WTO メッセージが取り込まれます。事前定義アラートには、事前設定されたフィルター設定があります。ユーザー独自のアラートの場合は、インターフェース・オプション SE.A.A から正しいフィルター設定を指定する必要があります。「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」で独自のアラートの追加に関する情報を参照してください。アラート構成を「検査」すると、「リフレッシュ」アクションによる活動化用に、正しい全体フィルター設定が生成されます。

インターバル

関連するインターバルは、以下のとおりです。

- データ分析を実行し、アラートを生成するためのレポート作成間隔
- 環境を再評価するための `stage 1` インターバル
- 「移動ウィンドウ」分析用の「平均」インターバル

デフォルトでは、データ分析は 60 秒ごとに行われます。このインターバルは、リアルタイム・アラート・メッセージが必要でなければ、長くすることができます。もっと高速の応答が必要な場合は、このインターバル時間を短くすることができます。

注: それぞれのレポート作成間隔ごとに、新しいバッファーが使用されます。次のセクションで説明するバッファーに関する考慮事項は、それと結び付いています。

`stage-1` プリプロセッシング・サブタスクは、システム環境とユーザー属性に関する現行情報を取得します。このタスクは、デフォルトでは 1 時間ごとに実行されます。古くなった情報が好ましくない場合は、セキュリティー・データベースと CKFREEZE ファイルをレポート作成間隔ごとに処理しなければなりません。しかし、それは必要ありません。 新しい入出力構成イメージを取得するのはコストがかかるプロセスであるため、zSecure Collect は通常、毎日特定の時刻に CKFREEZE

ファイルをリフレッシュするようにスケジュールされます。ただし、オペレーター・コマンド MODIFY C2POLICE,COLLECT によって、このタスクを zSecure Alert にディスパッチさせることもできます。

しきい値を持つ一部の「平均化」アラートでは、レポート作成間隔より長い時間枠を使用できます。これらのアラートの場合、例えば 5 回のレポート作成間隔の SMF レコードがヒストリー・バッファーに保持されます。この長期分析インターバルも、レポート作成の必要に応じて調整できます。

バッファー

zSecure Alert の構成に関する、もう 1 つの重要な考慮事項は、メモリー内バッファーの使用状況です。zSecure Alert によって使用されるバッファー・スペースは、zSecure Alert 開始タスク・アドレス・スペースの専用領域内にある通常のページング可能ストレージです。これは、すべての面で、データ・セットを編集する TSO ユーザーの作業用ストレージによく似ています。バッファー・サイズを計算するガイドラインとして、以下のステップを実行できます。

注**:** 各ステップに付いている番号は単なる例示用なので、システムの開始点としては使用しないでください。

1. SMF ダンプ・プログラムの出力に注目します。1 日に書き込まれる RACF SMF レコード (レコード・タイプ 80) または ACF2 SMF レコードの数とアカウンティング SMF レコード (レコード・タイプ 30) の数をまとめます。

   例えば、ある小規模なシステムで、平均的な 1 日に実行される MAN データ・セットの切り替えとダンプの回数が 5 回だとします。IFASMFDP プログラムの出力は、RACF または ACF2 SMF レコードの数を示します (50,000 32,000 69,000 49,000 および 27,000)。この平均的な 1 日に書き込まれた RACF または ACF2 SMF レコードの合計数は、227,000 になります。SMF 30 レコードの数は、19000 15000 31000 23000 および 17000 でした。SMF 30 レコードの 1 日の合計数は、105,000 になります。
2. アラート・レポート作成間隔が 1 分 (デフォルト) であるとして、1 インターバル当たりのレコード数を計算します。

   この例では、1 分当たり 227,000 / 1440 = 158 件の RACF または ACF2 レコードと、105,000 / 1440 = 73 件の SMF-30 レコードが生成されています。
3. これらの SMF レコードの平均的なレコード長を知るために、SMF ダンプ・プログラムの出力に注目します。それは、RACF レコードの場合は 250 - 300 バイト、ACF2 レコードの場合は 600 - 700 バイト、SMF-30 レコードの場合は 1000 - 1500 バイトのはずです。
4. 平均レコード数に平均レコード長を乗算すると、1 インターバル当たりの平均バッファー・サイズが分かります。

   この小規模システムの例では、結果は (158 * 274) + (73 * 1224) = 132,644 バイトになります。
5. 通常のシステム作業負荷の変動を考慮して、算出した平均値に 5 を掛け、最も近い切りのいい数値に切り上げると、*bufsize* パラメーターに最適の開始点が分かります。

この例では、*bufsize* パラメーターの設定値には 700 KB が適切です。

最小バッファー・サイズが分かったら、次の関心事は必要なバッファーの数です。前に述べたように、最小バッファー数も長期のイベント分析に関連しています。例えば、ユーザーが 10 分間に 10 回を超える RACF ログオン違反を生成したときに、アラートを生成したい場合は、バッファーに保持するデータの量は、少なくとも 10 分を表すものでなければなりません。1 つのバッファーには常に新しいイベントが書き込まれるため、平均化プロセスには使用できません。したがって、公式は次のようになります。

```
Numbufs > (AverageInterval / Interval) + 1
```

開始点としては、この公式に基づくバッファー数の 2 倍を使用します。したがって、デフォルト値を「インターバル」(60 秒) と「*AverageInterval*」(300 秒) に使用している場合は、最終的に 2*((300/60)+1) = 12 バッファーになります。

このプロシージャーによって割り振る追加バッファーは、システム・アクティビティーが多い期間のオーバーフロー・バッファーとして使用できます。一般に、そのような期間は長くは続きません。前に示した計算の例では、通常の量の 3 倍から 4 倍の SMF レコードを短期間 (1 分または 2 分) 取り込む必要がある場合を考慮しています。

これまでに示した例では、「インターバル」と「*AverageInterval*」にデフォルト値を使用することを想定しています。これらのパラメーターを決定するための主な基準は、レポート作成要件です。ほとんどのインストール済み環境では、約 1 分のアラート応答時間が適切と思われます。これは、E メールやその他のアラート配信方法に対する通常の応答時間にも適切です。「*AverageInterval*」の場合、5 分のインターバルを使用すれば、過度の偽アラームを回避するのに十分な長さです。また、これは、アラートを必要とするほとんどの状態を検出するのに十分な短さでもあります。

以下の値を、これらの OPTION および REPORT パラメーターの開始値として使用できます。

Bufsize

1024 (=1 MB)、または ACF2 の場合は 2048

これは、RACF または ACF2 SMF レコードの平均の長さ、下記の指定されたインターバル、および、アクティビティーが多い期間中の 1 秒当たり 40 件の RACF または ACF2 SMF レコードを平均したものに基づいています。

NumBufs

12

これは、長期のしきい値期間 (「*AverageInterval*」) および「インターバル」期間に基づいています。また、6 個の追加オーバーフロー・バッファーも考慮しています。

Interval

60 秒

AverageInterval

300 秒

zSecure Alert の初期実行時に、DEBUG BUFFER コマンドを使用して、メモリー内バッファーの使用状況をモニターします。その結果として、それぞれの「インターバル」期間の終わりに、3 つのメッセージが生成されます。C2P0325 および C2P0326 メッセージは、SMF レコードおよび WTO レコードに使用されたバッファー・スペースの量を示しています。SMF レコードおよび WTO レコードのスペースの合計量は、ステップ 4 で計算した予想スペースにほぼ一致する必要があります。ステップ 5 では、バッファー・サイズを、予想される平均必要スペースの 5 倍に指定しました。したがって、バッファーは、約 20% だけ使用されることが予想されています。これにより、システム・アクティビティーの変動に備えて、十分なスペースが残されます。

前の計算例で使用したのと同じ数値を使用すると、以下のメッセージを予想できます。

```
C2P0333I Buffer index is 09
C2P0325I Buffer stats: SMF(cnt,len) 00000214-00131928
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
```

これらのメッセージから、予想したレコード率がほぼ正しかったこと (つまり、予想した 231 レコードに対して 214 レコード)、およびレコードの平均サイズも大きさとして適切だったこと (つまり、予想した 132,644 に対して 131,928) を確認できます。

バッファー・デバッグ・メッセージを活動化した場合、zSecure Alert はオーバーフロー・バッファーが必要なときにもメッセージを生成します。以下のメッセージの例を見てください。

```
C2P0334I Extended buffer used
C2P0333I Buffer index is 02
C2P0325I Buffer stats: SMF(cnt,len) 00002728-01037650
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
C2P0333I Buffer index is 03
C2P0325I Buffer stats: SMF(cnt,len) 00000814-00307855
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
```

これらのメッセージは、通常のバッファー使用状況メッセージに追加して発行されます。メッセージで示されているバッファー「02」は、後続のバッファー (「03」) にオーバーフローしていたバッファーです。バッファー「03」は、それに続く通常の C2P0325 メッセージと C2P0326 メッセージで示されています。

前に概要を示したステップを使用して、過度なシステム・リソースを使用せずに、必要に合った最小バッファー・サイズとバッファー数を選択できます。この方法では、必要なときに大きくできる小さなバッファーから開始します。それに代わる手法は、多数の大きなバッファーで開始して、バッファーの統計メッセージをモニターすることです。数回のテストの後、バッファー・サイズをどれくらい削減できるかを判断できます。

バッファーを割り振る場合は、zSecure Alert 開始タスク JCL で指定される MEMLIMIT も考慮する必要があります。SCKRPROC 内の C2POLICE メンバーで指定されるデフォルトの MEMLIMIT 値は 8 GB です。この値は、*bufsize* と *numbufs* を使用して指定された合計バッファー・スペースより、少なくとも 64 MB 大きくする必要があります。

その他のコマンド

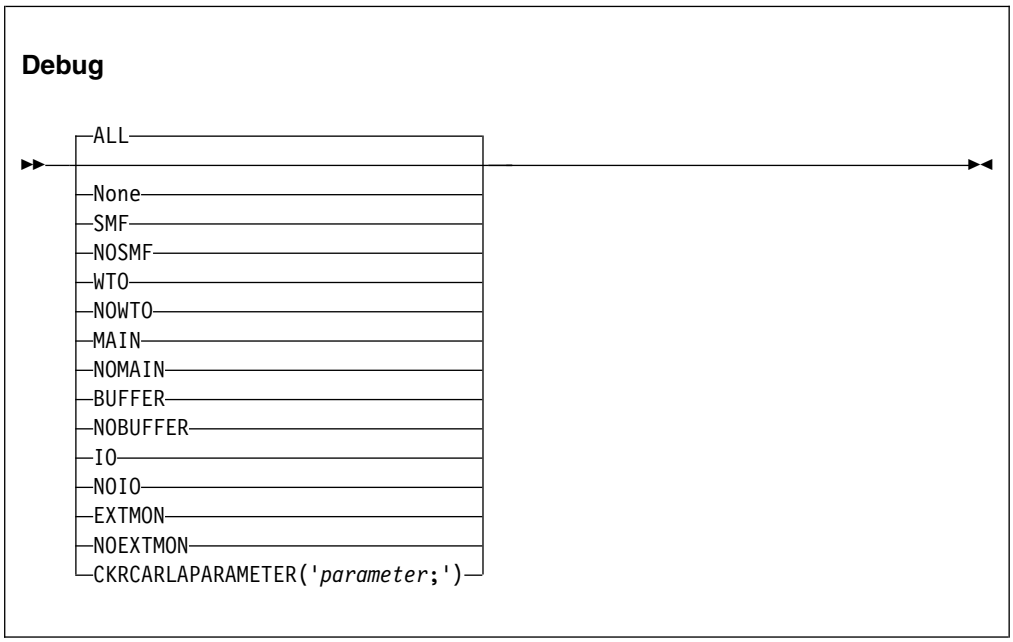
以下のコマンドは、通常、必要ありません。 DEBUG コマンドを使用すると、診断情報を入手できます。これらのコマンドは、アラート構成データ・セットの C2PXPARM メンバーで入力できます。 115 ページの『必要なデータ・セット』を参照してください。

それ以外のコマンドは、通常、インターフェースによって生成されます。「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」の構成に関する情報を参照してください。

DEBUG コマンド

DEBUG コマンドの構文は、次のとおりです。

注**:** 指定できるオプションは 1 つだけです。WTO 処理に関連したメッセージを除くすべてのメッセージを受信したい場合は、2 つの DEBUG コマンド (DEBUG ALL、およびその直後に DEBUG NOWTO) を発行する必要があります。DEBUG コマンドは、PARMLIB とオペレーター・コンソールのどちらからでも有効です。



このキーワードおよび変数は以下の値をとります。

All このデフォルト・レベルは、すべての診断メッセージをコンソールに書き込む必要があることを指定します。これらのメッセージの大部分は、問題判別時の支援が目的であり、お客様が日常的に使用するためのものではありません。DEBUG BUFFER の結果として生成されるメッセージは、データ・バッファーの最小サイズを判別するために日常的に使用してください。

None すべての診断メッセージの作成を非活動化します。

SMF 処理 SMF レコードに関連した診断メッセージは、コンソールに書き込まれます。

NOSMF
処理 SMF レコードに関連した診断メッセージは、コンソールに書き込まれません。

WTO 処理 WTO メッセージに関連した診断メッセージは、コンソールに書き込まれます。

NOWTO
処理 WTO メッセージに関連した診断メッセージは、コンソールに書き込まれません。

MAIN
メインライン処理に関連した診断メッセージは、コンソールに書き込まれます。これには、オペレーター・コマンドに対する応答、すべてのサブタスクの初期化と管理、および主要なバッファー管理機能が含まれます。

NOMAIN
メインライン処理に関連した診断メッセージは、コンソールに書き込まれません。これには、オペレーター・コマンドに対する応答、すべてのサブタスクの初期化と管理、および主要なバッファー管理機能が含まれます。

BUFFER
バッファー使用統計は、各レポート作成間隔の終わりに、コンソール、ジョブ・ログ、および syslog に書き込まれます。それらのメッセージを使用して、取り込まれた SMF レコードと WTO メッセージの数、およびそれぞれに必要なストレージの量を判別することができます。これらのメッセージを使用して、必要なバッファー・ストレージの最小量と最大量を追跡できます。

NOBUFFER
バッファー使用統計は、コンソールに書き込まれません。

IO zSecure Alert データ分析入出力ルーチンによって処理されたすべての操作を、SYSLOG によってトレースする必要があることを指定します。これによって、多数の WTO メッセージが生成される場合もあります。この機能は、製品の内部的な問題の診断を支援するために、IBM サポート担当員によって使用されることを目的としています。

NOIO
入出力診断メッセージは、生成されません。

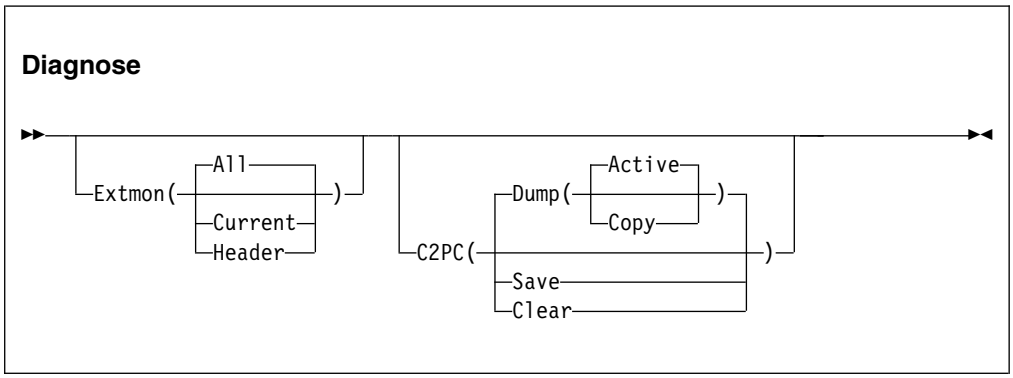
EXTMON
拡張モニター・アラート処理に関連した診断メッセージは、オペレーター・コンソールに書き込まれます。

NOEXTMON
拡張モニター・アラート処理に関連した診断メッセージは、オペレーター・コンソールに書き込まれません。

CKRCARLAPARAMETER
C2POLICE 開始タスク内で使用される CKRCARLA のすべてのインスタンスに渡されるストリングを指定します。このストリングを指定する場合、末尾にセミコロンを付け、引用符で囲む必要があります。このパラメーターは、IBM ソフトウェア・サポート担当員が問題を診断するためのものです。ストリングの最大長は 63 文字です。

DIAGNOSE コマンド

DIAGNOSE コマンドを使用すると、問題判別のために、一部の内部制御ブロックおよびテーブルがダンプされます。表示される制御ブロックは、IBM サポート担当員が問題を診断するためのものです。次の図は、DIAGNOSE コマンドの構文を示しています。



キーワードとパラメーターは、以下の値をとります。

Extmon

オペレーター・コンソールに拡張モニター・スナップショット・データ・セットの状況情報を表示することを指定します。使用可能なサブオプションは、次のとおりです。

All すべての CKFREEZE スナップショット・データ・セットの名前と状況が表示されます。状況情報のレイアウトは、以下のとおりです。

```
LCB..CED
L The data set is listed in the system catalog
C This is the CURRENT snapshot data set
B This is the BASE snapshot data set
. Reserved
. Reserved
C The snapshot data set is being created
E This is an expired snapshot data set
D This snapshot data set has been deleted
```

Current

「現行」および「Base」スナップショット・データ・セットの名前と状況が表示されます。

Header

内部 CKFT 制御ブロックからのヘッダー情報が、ダンプ形式でオペレーター・コンソールに表示されます。この情報は、IBM サポート担当員専用です。

C2PC 内部 C2PC 制御ブロックからの情報は、保存されるかオペレーター・コンソールに表示されます。この情報は、IBM サポート担当員専用です。使用できるサブオプションは、次のとおりです。

Dump

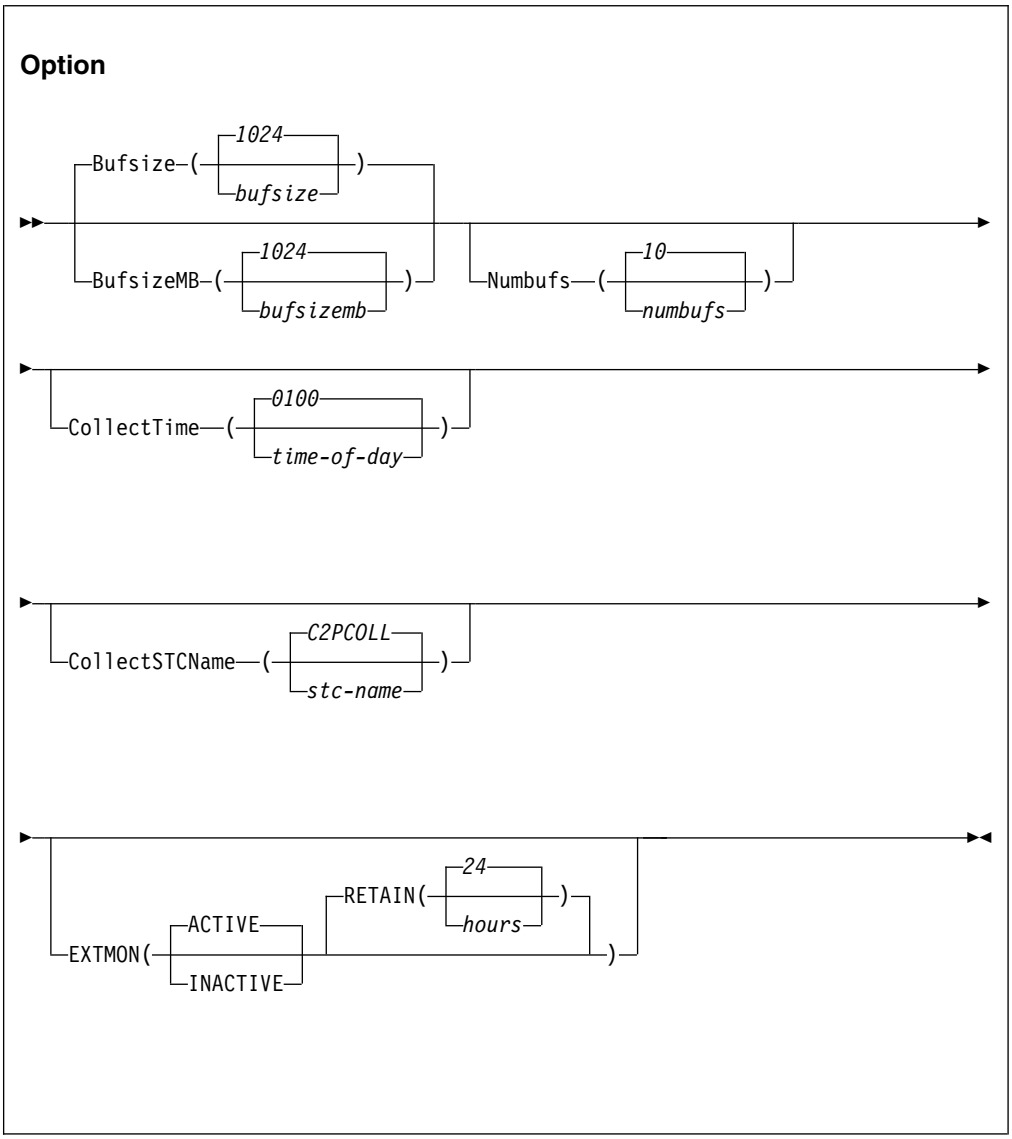
C2PC データ域のアクティブなコピーまたは保存されたコピーが、ダンプ形式でオペレーター・コンソールに表示されます。

Save アクティブな C2PC データ域が C2PC コピー領域に保存されます。

Clear C2PC データ域の保存されたコピーがクリア (2 進ゼロにリセット) されます。

OPTION コマンド

OPTION コマンドが有効になるのは、このコマンドが PARMLIB ステートメントに含まれている場合だけです。 OPTION コマンドの主な目的は、メモリー内データ・バッファーの数とサイズを指定することです。構文は次のとおりです。



このキーワードおよび変数は以下の値をとります。

Bufsize/BufsizeMB

Bufsize/BufsizeMB キーワードを指定できるのは、起動時または RESTART 処理の実行時に OPTION ステートメントが使用される場合だけです。 REFRESH 処理の実行中は、このキーワードは無視されます。

Bufsize/BufsizeMB より、*interval* 期間内における SMF レコードと WTO メッセージの保管に使用されるメモリー内バッファーのサイズを指定します。この期間に収集されるすべての SMF レコードおよび WTO メッセージを格納する十分な大きさのバッファーになるようにしてください。バッファーが小さすぎる場合、zSecure Alert は未使用のバッファーへの切り替えを試みます。使用可能な未使用のバッファーがない場合は、最も古いヒストリー・データが入っているバッファーが代わりに使用されます。この新しいバッファーが使用不可の場合は、バッファー・オーバーフロー・メッセージが発行されます。現行レポート作成間隔のレコードは失われます。

Bufsize キーワードを使用する場合は、必要なバッファー・サイズをキロバイトで指定します。BufsizeMB キーワードを使用する場合は、サイズをメガバイトで指定します。バッファーの有効なサイズは、1 キロバイトと 1 ギガバイトの間です。指定したサイズは、最も近いメガバイトに丸められます。OPTION ステートメントで両方のキーワードを使用した場合は、最後に指定された値がプログラムによって使用されます。バッファーは、64 ビットのストレージに割り振られ、開始タスクの指定された MEMLIMIT の一部としてカウントされます。オーバーフロー・バッファーの使用は、拡張バッファリングとも呼ばれ、必要なバッファー・サイズを大幅に削減できます。インストールに適したバッファー・サイズの選択方法については、124 ページの『構成のガイドラインとパフォーマンスへの影響』をガイドラインとして参照してください。一般に、例えば、5 メガバイトのバッファーを 2 個指定するよりも、1 メガバイトのバッファーを 10 個指定するほうが効率的です。

Numbufs

Numbufs キーワードを指定できるのは、起動時または RESTART 処理の実行時に OPTION ステートメントが使用される場合だけです。REFRESH 処理の実行中は、このキーワードは無視されます。

Numbufs により、割り振るバッファーの数を指定します。*numbufs* には、2 から 32 までの数値を指定する必要があります。バッファーの合計数は、レポート作成仕様で必要とされている、取り込み対象のすべての SMF レコードおよび WTO メッセージを保持するのに十分な値でなければなりません。

```
Numbufs > (AverageInterval / Interval) + 1
```

最小値より多くの数のバッファーを指定すると、それらのバッファーをオーバーフローの目的に使用できます。これにより、bufsize を削減して、アクティビティーが多い期間に収集したすべてのデータを保存できます。オーバーフロー・バッファーが使用可能でない場合は、代わりに最も古いヒストリー・バッファーを使用します。その結果、長期のしきい値分析に必要な一部のデータが失われます。 インストールに適したバッファー数の選択方法については、 124 ページの『構成のガイドラインとパフォーマンスへの影響』をガイドラインとして参照してください。

CollectTime

zSecure Collect 開始タスクを開始する必要がある時刻を指定します。この時刻は 24 時間形式で、4 桁の連続した数字 (つまり、HHMM) として指定する必要があります。例えば、午前 1 時は 0100 として指定し、午後 1 時は 1300 として指定する必要があります。

時刻は、0001 (深夜 0 時の 1 分後) から 2359 (深夜 0 時の 1 分前) までの間で指定します。時刻値 0000 は、zSecure Collect STC を開始しないことを示します。

CollectSTCName
システム proclib 内の開始タスク (STC) の名前を指定します。 これは、次の形式の内部 START コマンドを生成するために使用できます。

```
START name.name
```

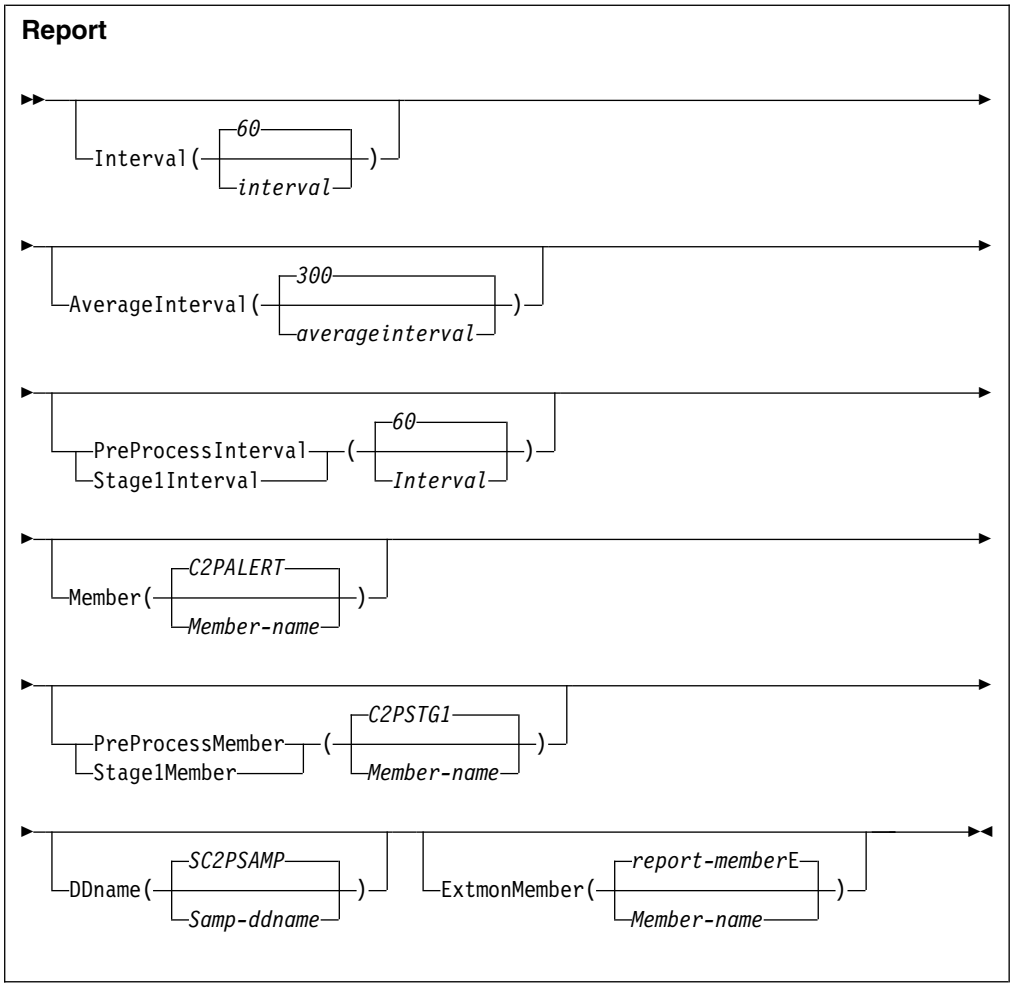
このフィーチャーを使用する前に、プロシージャーが存在し、正しいユーザー ID とグループが開始タスクに割り当てられており、開始タスクに zSecure Collect 機能を実行するための十分な権限があることを確認してください。

zSecure Alert 開始タスクには、開始コマンド用の十分な権限が必要です。必要なプロファイルを定義するには、 107 ページの『zSecure Alert を構成および使用するための前提条件』で説明されているステップを実行します。

EXTMON
拡張モニター・プロセスを使用することを指定します。それには、zSecure Alert ソフトウェアをインストールおよび構成したユーザーが、いくつかの構成ステップを完了する必要があります。これらのステップについては、113 ページの『ポストインストール・タスク』で説明しています。最初のサブパラメーターは、プロセスが ACTIVE か INACTIVE かを指定します。2 番目のサブパラメーターは、CKFREEZE スナップショット・データ・セットの保存期間を指定します。拡張モニター・プロセスがアクティブの場合、指定した保存期間より古い CKFREEZE スナップショット・データ・セットは自動的に削除されます。RETAIN パラメーターのデフォルト値は、24 時間です。

REPORT コマンド

REPORT コマンドは、レポートのタイミングと、環境情報およびレポート生成のプリプロセッシングに使用する CARLa ステートメントのソースを制御します。REPORT コマンドの効果は、zSecure Alert での各種タスクの循環的な性格のために、遅延する場合もあります。例えば、変更された「インターバル」値は、現行インターバルが満了した後にのみ使用されます。REPORT コマンドの構文は、次のとおりです。



このキーワードおよび変数は以下の値をとります。

Interval

収集したデータを zSecure Alert で分析し、適切なアラートを生成する間隔を指定します。値 *interval* では、時間間隔を秒単位で指定します。有効な時間間隔は、10 - 3600 秒です。デフォルト値は 60 秒です。

AverageInterval

移動ウィンドウ 分析のために、zSecure Alert が特定のイベントの発生を平均化する時間を指定します。この時間は、ヒストリー期間とも呼ばれます。一般に、この期間は *interval* の 5 倍の長さになります。numbufs パラメーターは、*AverageInterval* 期間のすべてのデータを取り込むのに十分な大きさでなければなりません。

```
Numbufs > (AverageInterval / Interval) + 1
```

値 *AverageInterval* は、秒単位の時間を指定します。有効な時間平均化期間は、10 - 9999 秒です。デフォルト値は 300 秒です。

PreProcessInterval または **Stage1Interval**

zSecure Alert でセキュリティー・データベースおよび CKFREEZE ファイルからの情報を処理する間隔を指定します。この処理の結果は、通常のレコード分析の選択基準として使用されます。このプロセスはアラートを直接生

成せず、後続のステップの入力としてのみ使用されるため、STAGE1 CARLa プロセスと呼ばれます。最新の選択基準を取得するために、レポート作成タスクは、STAGE1 プロセスの完了後にリフレッシュされます。STAGE1 プロセスがアクティブである間、オペレーター REFRESH および COLLECT コマンドは、そのプロセスが終了するまで延期されます。*Stage1Interval* は分単位で指定する必要があり、有効な値は 10 - 1440 です。デフォルト値は 60 分です。

Stage1Interval の最適値は、システムおよびセキュリティー・データベースに対する更新の頻度によって異なります。

Member
データ分析に使用する、区分データ・セット内の membername を指定します。これは、インストール用に指定された、適切なアラート生成用の CARLa ステートメントを含みます。

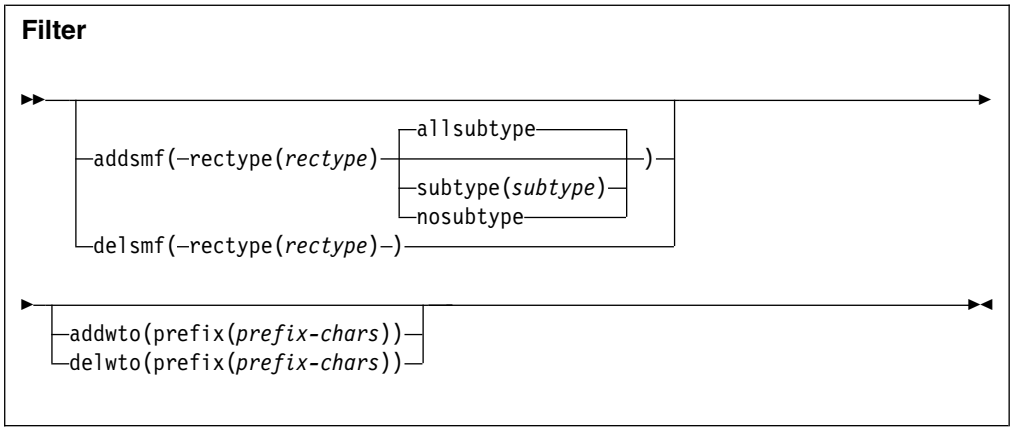
PreProcessMember または **Stage1Member**
セキュリティー・データベースおよび CKFREEZE ファイルの処理に使用する、区分データ・セット内の membername を指定します。これは、アラート生成プロセスで使用される選択基準を作成する CARLa ステートメントを含みます。STAGE1 プロセスの出力は、アラート生成プロセスで明示的に組み込む必要があります。

DDName
zSecure Admin and Audit によって使用される CARLa ステートメントを含んでいる区分データ・セットを指す JCL DD 名を指定します。これは、少なくとも、*member* と *Stage1Member* によって示されるメンバーを含む必要があります。

ExtmonMember
拡張モニター・アラートに使用する、区分データ・セット内の member-name を指定します。このメンバーには、CKFREEZE スナップショット・データ・セットの分析と適切なアラートの作成に使用する CARLa ステートメントが含まれています。ExtmonMember オプションを指定しなかった場合、または member-name を指定しなかった場合は、デフォルトのメンバー名が使用されます。デフォルトのメンバー名は、MEMBER キーワードに指定されたメンバー名の直後に英字の「E」を付けて作成されます。

FILTER コマンド

フィルター基準は、その後の処理用にメモリー内バッファーに収集されるデータの量を制限するために使用します。FILTER コマンドを使用すると、不要なイベントをプロセス内で早期に除去し、それによって全体の処理効率を高めることができます。SMF および WTO フィルター基準を指定しなかった場合は、すべての SMF レコードと WTO メッセージがその後の処理用に収集されます。この状態を回避するために、zSecure Alert ユーザー・インターフェースは、どのイベントにも一致しないダミー・フィルターを生成します。 FILTER コマンドの構文は、次のとおりです。



次のセクションでは、使用できるキーワードとパラメーターについて説明します。

ADDSMF

SMF レコードに使用する追加フィルター基準を指定します。 FILTER コマンドを繰り返して、必要な数だけフィルター基準を指定できます。指定した基準は、既にアクティブな基準に追加されます。選択する SMF レコード・タイプは、*rectype* および *subtype* パラメーターによって指定します。使用可能なサブオプションは、次のとおりです。

Allsubtype

すべての SMF レコード・サブタイプをレコード・フィルターに含めることを指定します (デフォルト)。この指定は、サブタイプでのフィルタリングが存在しないと解釈することもできます。サブタイプは、SMF レコード・タイプ 30、80、92、および ACF2 にのみ使用します。それ以外のすべての SMF レコード・タイプの場合、サブタイプの指定は無視されます。

Rectype

選択する必要がある SMF レコード・タイプ、またはもう選択してはならない SMF レコード・タイプを指定します。*rectype* パラメーターは、0 - 255 の数値か、ACF2 によって生成されたレコードを指定する値 **ACF2** でなければなりません。

Subtype

選択する必要がある SMF レコード・サブタイプを指定します。*subtype* は、SMF レコード・タイプ 30、80、92、および ACF2 にのみ使用します。それ以外のすべての SMF レコード・タイプの場合、サブタイプは無視されます。*subtype* の値は、数値か英字 1 文字でなければなりません。サブタイプは、以下のように解釈されます。

Rectype 30

subtype は、標準 SMF レコード・サブタイプです。現在、SMF レコード・タイプ 30 には 1 から 5 までのサブタイプだけが定義されていますが、zSecure Alert で受け入れられる範囲は 1 - 8 です。

Rectype 80

subtype は、RACF イベント・コードです。RACF イベン

ト・コードの完全なリストについては、「RACF 監査担当者のガイド」を参照してください。zSecure Alert で受け入れられる値の範囲は、1 - 255 です。

Rectype 92

subtype は、標準 SMF レコード・サブタイプです。現在、SMF レコード・タイプ 92 には 1 から 17 までのサブタイプだけが定義されていますが、zSecure Alert で受け入れられる範囲は 1 から 255 までです。

Rectype ACF2

subtype は ACF2 レコード・タイプです。ACF2 サブタイプの完全なリストについては、「*CARLa* コマンド・リファレンス」の『SELECT/LIST フィールド』の章を参照してください。NEWLIST TYPE=SMF の ACF2_SUBTYPE フィールドを参照してください。

Nosubtype

前に Subtype キーワードについて述べたような SMF レコード・サブタイプを、選択基準として使用してはならないことを指定します。このキーワードを使用すると、示された *rectype* に対して以前に指定したすべてのサブタイプがリセットされます。

DELSMF

指定した SMF レコード・タイプをもう選択しないことを指定します。SMF レコード・タイプは、*rectype* パラメーターによってのみ識別されます。SMF レコード選択をサブタイプごとに非活動化することはできません。

ADDWTO

WTO メッセージに使用するフィルター基準を指定します。最大 24 個までの異なるフィルター基準を指定できます。

DELWTO

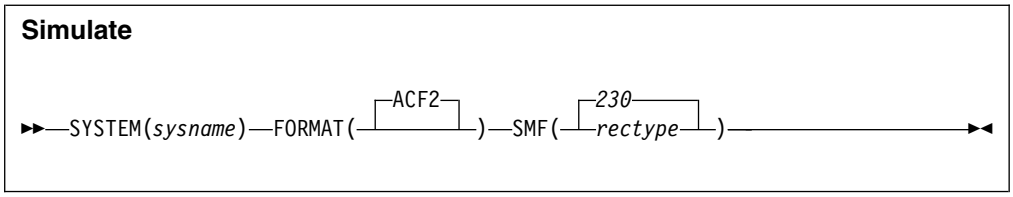
prefix-chars で始まるメッセージに対して、もう WTO メッセージ選択を行わないよう指示します。

Prefix

WTO メッセージ ID の最初の文字を指定します。すべての ICH メッセージを含めたい場合は、単に ICH を指定します。ICH408I メッセージだけを含めたい場合は、メッセージ ID の 7 文字すべてを指定します。メッセージ接頭部の最大の長さは 8 文字です。最小の長さは 1 文字です。

SIMULATE コマンド

通常の操作では、この SIMULATE コマンドは必要ありません。zSecure Alert は文書化されたインターフェースを使用して、ACF2 によって使用された SMF レコード・タイプを取得するからです。そのプロセスが失敗したときにだけ、SIMULATE コマンドが必要になります。このコマンドには、zSecure Alert で現在使用されていない各種のキーワードと必須パラメーターがあります。それらのキーワードとパラメーターは、SIMULATE コマンドの zSecure Admin and Audit 構文との整合性を保つために組み込まれています。それらは、将来のバージョンの zSecure Alert で使用できます。SIMULATE コマンドの構文は、次のとおりです。



次のセクションでは、使用できるキーワードとパラメーターについて説明します。

System

この SIMULATE コマンドを適用するシステム名を指定します。現在、*sysname* の値は無視されます。現行システムの SMF_ID を指定する必要があります。

Format

唯一サポートされているパラメーター **ACF2** は、この SIMULATE コマンドが ACF2 固有のオプションを指定するために使用されたことを示します。

SMF ACF2 で生成された SMF レコードの SMF レコード・タイプを指定します。パラメーター *rectype* は、値 1 - 255 の数値でなければなりません。デフォルト値は 230 です。

共存に関する考慮事項

zSecure Alert 構成データ・セットは、マイグレーションの目的から、異なるリリースの zSecure Alert を持つ複数の z/OS イメージ間で共有できます。しかし、異なるリリース間で構成データ・セットを共有するのは、限られた期間だけにしてください。なぜなら、新しいアラートおよび新しい機能は、すべての共用システムがアップグレードされるまで使用可能にならないからです。新しいアラートおよび新しい機能を使用したい場合、しかし、すべてのシステムを一度にアップグレードしたくない場合は、一時的に共有をやめ、異なる構成データ・セットを割り当ててください。

構成データ・セットを共有する場合は、使用中の最も低いレベルの ISPF インターフェースを使用して、zSecure Alert を構成します。構成データ・セットをアップグレードした後は、そのアップグレードをバックアウトしない限り、下位レベルのインターフェースから変更を加えることができなくなります。さらに、下位レベルの zSecure Alert アドレス・スペースは、新しい ISPF インターフェースを使用して作成または保守された構成で正しく機能する場合も、そうでない場合もあります。

サポートされているアップグレードは、新しいリリースが発行された時点でまだサポートされている下位のリリース・バージョンからのアップグレードです。

zSecure Alert のアップグレード

構成データ・セット内に現在あるアラート構成に使用されているものより高いレベルの zSecure Alert 構成インターフェースを使用した場合は、以下のパネルが表示されます。

```
                      zSecure - Setup - Alert

UPGRADE process about to start for C2R.IP01.C2PCUST
Warning: The current zSecure Alert data set was created using downlevel
panels. There might still be a downlevel zSecure Alert using it. After
upgrade, a downlevel zSecure Alert can no longer use this data set and
customization will only be possible from the zSecure Alert release 1.12.0
(or newer) User Interface.

The following downlevel table has been found:
User interface level : 1.11.0
Table name           : C2PIUACD
Creation date        : 2011/03/08
Last change date     : 2012/05/10
Last change time     : 08:49:01
Last changed by      : ALERTU1

Select upgrade option
3  1. Upgrade from downlevel table
   2. Create new table
   3. Cancel upgrade process.
```

図 5. 「*Setup Alert*」パネル: *zSecure Alert* のアップグレード

以下のアップグレード・オプションを選択できます。

1 - Upgrade from downlevel table
アラート構成は ISPF テーブルに保管されます。古い構成を、選択したアラートと各アラートの宛先と一緒に維持する場合は、このオプションを選択します。古い構成テーブルは新しいフォーマット・テーブルに変換されます。いずれかの構成ステップで追加情報が必要な場合は、そのステップを要求状態の「OK」でなく「Req」状況に設定できます。その場合、対応するアクション・コマンドを使用して、その情報を提供する必要があります。構成ステップ「Ver」(これは構成の検査を意味します) を「Req」(「必要」の意味) に設定すれば、いつでもアラート・コードをリフレッシュすることができます。このオプションを選択した後は、下位レベルの ISPF インターフェースで zSecure Alertを構成できなくなります。

2 - Create new table
古い構成を保持したくない場合は、このオプションを選択します。新規構成を使用中であり、ユーザーはすべての構成ステップを実行する必要があります。これは、すべての構成ステップの状況が「Req」であることを意味します。オプション 1 と同様に、下位レベルの ISPF インターフェースでは zSecure Alertを構成できなくなります。

3 - Cancel upgrade process
構成データ・セットを共有しているシステムの中に、まだ現行ソフトウェア・レベルへのアップグレードが済んでいないシステムがある場合は、このオプションを選択します。

アップグレードのバックアウト

zSecure Alert は、上位リリースのテーブルの存在を検査します。使用している構成より下位のレベルの ISPF インターフェースで zSecure Alert を構成しようとすると、以下のパネルが表示されます。

```
                      zSecure - Setup - Alert       Row 1 to 1 of 1
Command ===> ____________________________________________ Scroll ===> CSR

The current zSecure Alert data set is shared with a higher level User
Interface. The following uplevel table(s) are found. You should configure
zSecure Alert from the highest User Interface level, or delete the higher
level table(s) by using the D action command.
Warning: Deleting the higher level table(s) results in the loss of all
customization performed from the higher level User Interface!
------------------------------------------------------------------------------
    Level  Table            Created     Changed               ID
_   1.7.0  C2PIUACC         2005/05/08  2005/05/10  11:32:50  ALERTU1
****************************** Bottom of data ********************************
```

図 *6.* 正しい *ISPF* インターフェース・レベルの構成

D (削除) アクション・コマンドは、現行レベルをフォールバックしたい場合にだけ使用します。バックアウト後、古い ISPF インターフェースで「検査」と「リフレッシュ」を再実行し、zSecure Alert アドレス・スペースに対してバックアウトを有効にしてください。

第 13 章 zSecure Visual Server のセットアップおよび使用

zSecure Visual Server を使用して、RACF とのセキュア接続を直接確立します。これで、Windows ベースのグラフィカル・ユーザー・インターフェースである zSecure Visual クライアントを使用して、Windows 環境から RACF を分散管理できるようになります。

Visual Server のインストール、構成、および使用については、以下のセクションを参照してください。

Visual Server のセットアップ

以下のセクションで、zSecure Visual Server のインストールの前提条件および手順に関する情報を示します。

- 『インストール要件』
- 142 ページの『必要なシステム許可』
- 143 ページの『所有者、ディレクトリー、およびファイル・システムの準備』
- 144 ページの『zSecure Visual のための zSecure 構成』
- 145 ページの『zSecure Visual Server ソフトウェア』
- 146 ページの『新規 zSecure Visual Server のセットアップ』

インストール要件

zSecure Visual は、zSecure 製品ファミリーの CARLa 駆動コンポーネントの 1 つです。すべての CARLa 駆動コンポーネントで、SMP/E のインストールが同時に行われます。すべての CARLa 駆動コンポーネントが zSecure 構成を使用します。

zSecure Visual を構成または使用する前に、13 ページの『第 4 章 ソフトウェアのインストール』および「*Program Directory: IBM Security zSecure CARLa-Driven Components*」で説明されている基本インストール・プロセスを完了しておく必要があります。インストール時に、次のタスクを実行する必要があります。

- 低位修飾子 CKRINST を持つライブラリーを作成し、カスタマイズします。Visual 用のセットアップ・ジョブは、以下のとおりです。
- CKGRACF コンポーネントが、APF 許可を実行する必要があります。24 ページの『ソフトウェアの APF 許可』を参照してください。
- CKGRACF 日次ジョブを設定します。56 ページの『日次の CKGRACF ジョブ実行の要件』を参照してください。
- CKGRACF プログラムと CKRCARLA プログラムの両方がプログラム制御されていることを確認します。詳しくは、220 ページの『プログラム制御および PADS アクセスのセットアップ』 を参照してください。
- *hlq*.SCEERUN や *hlq*.SCEERUN2 (*hlq* は、デフォルトでは CEE) などのライブラリーのサポート・モジュールがプログラム制御されていることを確認します。

注: 通常、これらのデータ・セットはリンク・リストにあり、PROGRAM クラスのプロファイル * または ** のメンバーです。システムに適用されるデータ・セットを検査する必要があります。

- zSecure Visual 用に zSecure 構成を使用可能にします。その方法については、144 ページの『zSecure Visual のための zSecure 構成』を参照してください。
- サーバーの複数インスタンスを実行でき、これらのインスタンスが異なるリリースを実行できます。 149 ページの『既存の V1.*x* サーバーの、zSecure Visual 2.2.1 へのアップグレード』を参照してください。ただし、各サーバー・インスタンス内で、次のすべてのコンポーネントが同じレベルにある必要があります。
  - JCL
  - REXX
  - CARLa ライブラリー
  - ロード・モジュール
  - SCKRPAX ライブラリーから抽出された USS コード

  これらのコンポーネントを異なるレベルで使用することはサポートされていません。

必要なシステム許可

zSecure Visual を使用する前に、次のタスクを実行する必要があります。

- 必要なユーザー、グループ、ディレクトリー、およびファイル・システムをセットアップするための許可を設定します。その方法については、 143 ページの『所有者、ディレクトリー、およびファイル・システムの準備』を参照してください。
- サーバー・セットアップを実行するユーザーに対して、以下の FACILITY リソースに対する READ 権限をセットアップします。
  - BPX.FILEATTR.APF
  - BPX.FILEATTR.PROGCTL
- zSecure Visual データに必要な専用ファイル・システムを作成およびマウントするための許可を設定します。ファイル・システムは HFS または zFS です。
- プロダクション・プロセスの目的で、ジョブ・スケジューリングまたは自動化操作、またはその両方を行うシステムのエンティティーを作成するための許可を設定します。
- ジョブ入力サブシステムのプロシージャー・ライブラリーのいずれかへの UPDATE アクセス権限、および STARTED プロファイルをセットアップするための権限をセットアップします。これらの許可は、サーバーの開始タスクをセットアップするために必要です。または、サーバーをバッチ・ジョブとして実行することもできます。サーバーをバッチ・ジョブとして実行する場合は、適切な SURROGAT 権限が必要です。
- サーバーごとに使用可能な IP ポートのセットを選択し、許可します。詳しくは、 147 ページの『TCP/IP セキュリティー』 を参照してください。
- 新しいワークステーションをサーバーに追加するユーザーに、C2R.SERVER.ADMIN リソースでの READ アクセス権限を付与します (そのリソースは XFACILIT クラスにあり、ただし、それがインストールでカスタマイズされた場合は除きます。詳しくは、 205 ページの『付録 A. サイト・モジュール』を参照してください)。ジョブ C2RZWADM は、グループ MYGROUP

を使用します。 146 ページの『サーバー・プロセスのセットアップ』を参照してください。 BPX.DEFAULT.USER に有効なホーム・ディレクトリーがない場合は、これらのユーザーに有効な z/OS UNIX System Services ホーム・ディレクトリーも必要です。生成された他のユーザーのインストール・パスワードを読み取れないように、各ユーザーに固有のホーム・ディレクトリーを提供します。また、これらのユーザーのデフォルトの接続 GROUP プロファイルの OMVS セグメントに、有効な GID が設定されている必要があります。

- Visual クライアントを使用するが、新しいワークステーションを追加しない RACF 管理者の RACF ユーザー ID にも、UID と GID が必要です。ただし、これらのユーザーに対して個別の OMVS セグメントを定義する必要はありません。代わりに、ご使用の z/OS システムに応じて、BPX.DEFAULT または BPX.UNIQUE を利用することができます。また、これらのユーザーに独自のホーム・ディレクトリーは必要ありません。
- zSecure Visual クライアントのすべてのユーザーには、サーバー JCL 内の `C2RWCUST DD` ステートメントによって識別されたデータ・セット、およびそのデータ・セット内の C2RWASSC メンバーによって識別されたデータ・セットへの READ アクセス権限が必要です。

  注: `C2RWCUST DD` ステートメントは、zSecure 1.12 以降で必須となりました。

所有者、ディレクトリー、およびファイル・システムの準備

同時にアクティブになるクライアントの数が単一サーバーの制限を超える場合は、複数のサーバーが必要です。複数のサーバーは、別々の z/OS イメージで実行することも、ソフトウェアがあるファイル・システムを共有して単一の z/OS イメージ内で実行することもできます。

zSecure Visual Server の複数インスタンスを実行する場合、サーバーはソフトウェアがあるディレクトリーを共有できますが、各サーバー・インスタンスが独自のインスタンス関連データ (サブディレクトリー `run` および `log`) を持つ必要があります。結果として、クライアント用に生成した初期パスワード (一回限り使用可能の共有秘密鍵) は、その特定のサーバー・インスタンスでのみ有効になります。初期接続の後、証明書も同じサーバー・インスタンスでのみ有効になります。そのため、クライアントは、常に同じサーバー・インスタンスに関連付けられる IP アドレスまたは DNS 名でサーバーにアクセスする必要があります。

また、別々のディレクトリーまたはファイル・システムを使用すると、すべてのデータが適切な場所にある状態でシステムをアップグレードでき、zSecure Visual ソフトウェアを再インストールできるため、将来の z/OS および zSecure Visual ソフトウェアのアップグレードが簡単になります。

注: 最大 315 のクライアントが、同時にサーバーに接続できます。このように多くのクライアントに対応するには、zSecure Visual Server ユーザー ID のプロセスごとに許可されるオープン・ファイル記述子の最大数を 1594 以上に引き上げる必要があります。

UNIX の各ファイルまたはディレクトリーは所有ユーザーと所有グループの両方を備えている必要があるので、所有者を割り当てる必要があります。本書および IBM 提供のジョブでは、次のデフォルトを使用します。これらのデフォルトは、インストールの規則に合わせて調整できます。

表 6. ディレクトリーおよびファイルの所有者ユーザーおよびグループ *ID* の命名規則

	ソフトウェア	データ
所有ユーザー	C2RUSER	C2RSERVE
所有グループ	C2RGROUP	C2RSERVG
ディレクトリー	/usr/lpp/c2r/V2R2M1	/u/c2rserve/server1
マウント・ポイント	/usr/lpp/c2r	/u/c2rserve
ファイル・システム	OMVS.C2R.ZFS	OMVS.C2RSERVE.ZFS

表 6 で示すように、サーバーを実行するデフォルト・ユーザーの C2RSERVE がデータを所有します。ただし、サーバーは、ソフトウェアを含むファイルは所有しません。代わりに、サーバーには、グループ許可ビットおよびソフトウェア・ファイルを所有するグループへの接続を通じて、ソフトウェアに対する READ および EXECUTE アクセス権限が付与されます。クライアントを使用するユーザーにも、同じアクセス権限が必要です。同様に、サーバーとクライアント・ユーザーの両方に、zSecure がある OS データ・セットに対する READ アクセス権限が必要です。これらのデータ・セットのデフォルト高位修飾子は CKR です。

同じ方法で、セキュリティー・サポートおよび生産管理の担当者を C2RSERVG に接続して、それらの担当者にサーバー所有データ・ファイルへのアクセス権限を付与することができます。そのような担当者はログ・ファイルを表示する必要があるかもしれないからです。

注: 表 6 に示したデフォルトのマウント・ポイントは、ソフトウェアおよびデータ・ディレクトリーとは一致しません。この構成によって、複数のサーバーを単一のユーザー ID の下にセットアップできます。同様に、単一のファイル・システムの中に、将来のソフトウェア・リリースをインストールできます。リリースごとに、またはサーバーごとに個別のファイル・システムを使用するには、IBM 提供のジョブをテンプレートとして使用し、これを複数回実行します。

/u/c2rserve など、ホーム・ディレクトリーに使用されるファイル・システムでは自動マウントが一般的ですが、ソフトウェアの場合は、通常、そうではありません。自動マウントされないファイル・システムの場合は、後続の IPL の後でファイル・システムがマウントされるように、parmlib の `BPXPRM`*`xx`* メンバーを更新します。

zSecure Visual のための zSecure 構成

デフォルトの zSecure 構成は C2R$PARM です。別の構成を使用できます。次の zSecure 構成パラメーターは、zSecure Visual に特有です。

- C2RWCUST
- C2RW131A
- C2RWIN
- C2RSERVE

注: FIPS 140-2 暗号化標準は、NIST 800-131A 標準によって置き換えられました。その結果、C2RWFIPS 構成パラメーターは、C2RW131A パラメーターによって置き換えられました。

C2RWCUST によって識別されたデータ・セットに、現行リリースで必要なすべてのメンバーが含まれていることを確認してください。新規構成の場合は、ジョブ CKRZPOST によって空のメンバーが作成されますが、ユーザーが既に注力してきた構成に対しては、CKRZPOST は更新を行いません。

これらのパラメーターおよび C2RWCUST のメンバーの説明については、 223 ページの『付録 D. 構成パラメーターと構成メンバー』を参照してください。

zSecure Visual Server ソフトウェア

ソフトウェアの場所

143 ページの『所有者、ディレクトリー、およびファイル・システムの準備』で説明しているように、ソフトウェアのデフォルトの場所は `/usr/lpp/c2r/V2R2M1` です。ただし、別の場所を選択することもできます。例えば、パス名からリリース番号を除去したり、メンテナンス・レベルを追加したりできます。

C2RWIN パラメーターが、選択したソフトウェアの場所を反映するように、セットアップ・ジョブを実行する前に zSecure 構成を更新します。更新した構成は、後続のセットアップ・ジョブで指定します。

ソフトウェアの所有者と場所の準備

ジョブ C2RZCZFS を使用して、ソフトウェアをインストールするファイル・システムを準備します。

- 新規ファイル・システムを作成したくないことがあります。例えば、既にマウント済みのファイル・システムを以前のインストールから使用できます。既存のファイル・システムを使用するには、ファイル・システムを作成してマウントするジョブ・ステップをコメントにして取り除きます。ただし、この場合も、ディレクトリーをセットアップする他のジョブ・ステップを実行する必要があります。
- C2RZCZFS ジョブはファイル・システムをマウントするため、root として実行します。このマウントは、後続の IPL 後は持続しません。必要なときにファイル・システムがマウントされるようにしてください。例えば、`BPXPRM`*xx* メンバーにマウントを組み込むことができます。
- ファイル・システムは、SECURITY 属性および SETUID 属性を付けてマウントする必要があります。zSecure Visual はデーモンとして実行されるため、プログラム制御された環境が必要です。そのため、これらの属性が必要です。

アップグレード・インストールの場合は、通常、新規ファイル・システムを準備する必要はありません。ただし、ソフトウェアをアンパックする新しいディレクトリーを作成します。次に、zSecure 構成の `C2RWIN` パラメーターを変更し、サーバーを再始動することで、アップグレードしたソフトウェアの使用を開始できます。

ソフトウェアのアンパック

- C2RZWUNP ジョブを実行する前に、カスタマイズした `C2RWIN` パラメーターを含む zSecure 構成を指定します。
- ジョブ・ステップ `OS2ZFS` は、(SMP/E でインストールされた) ソフトウェアを UNIX ファイルにコピーします。
- アンパックした後、pax ファイルは不要なので破棄してかまいません。

新規 zSecure Visual Server のセットアップ

以降のセクションで、新しい zSecure Visual Server のセットアップに必要なプロセスに関する情報を示します。

- 『ユーザー ID およびファイル・システムのセットアップ』
- 『Security zSecure 構成 の更新: サーバー・ルート』
- 『サーバー・プロセスのセットアップ』
- 147 ページの『TCP/IP セキュリティー』
- 148 ページの『サーバーの初めての始動』
- 149 ページの『既存の V1.*x* サーバーの、zSecure Visual 2.2.1 へのアップグレード』

ユーザー ID およびファイル・システムのセットアップ

C2RZWUSR ジョブは、ファイル・システムをマウントし、作成したホーム・ディレクトリーの所有権をサーバーのユーザー ID に転送する必要があるため、root として実行します。`XFER` ジョブ・ステップが所有権を転送します。

各サーバーに独自の ServerRoot ディレクトリーがあれば、同じユーザー ID の下で複数サーバーを実行できます。すべてのサーバーが zSecure Visual 1.8.1 以降を実行する場合、単一のユーザー ID の下の複数サーバーで、異なるリリースのソフトウェアを実行できます。

Security zSecure 構成 の更新: サーバー・ルート

143 ページの『所有者、ディレクトリー、およびファイル・システムの準備』で概要を示したように、各 zSecure Visual Server にはサーバー・ルートとして使用する独自のディレクトリーが必要です。必要なディレクトリーを用意するために、セットアップするサーバーごとに zSecure 構成を編集します。通常は、サーバーを実行するユーザー ID のホーム・ディレクトリーのサブディレクトリーを使用します。以下に例を示します。

- サーバーを実行するデフォルトのユーザー ID は C2RSERVE です
- C2RSERVE ユーザーのホーム・ディレクトリーは `/u/c2rserve` です
- デフォルトのサーバー・ルートは `/u/c2rserve/server1` です

準備するサーバーごとに、次の作業を実行します。

1. zSecure 構成を準備し、この構成を後続のジョブで使用します。
2. ジョブ C2RZWRUT を実行して、サーバー・ルートを設定します。

サーバー・プロセスのセットアップ

開始タスクとして実行するには、以下のことが必要です。

- JCL プロシージャー C2RSERVE、C2RSTOP、および C2RSLOG を JES プロシージャー連結の一部になっているライブラリーにコピーする必要があります。また、開始タスクでは JCLLIB を使用できないため、すべてのサーバーの zSecure 構成を同じライブラリーにコピーする必要があります。

- サーバー・プロセスが適切なユーザー ID の下で実行されるようにします。サーバーを停止するプロセス (C2RSTOP)、またはサーバー・ログ・ファイルを印刷するプロセス (C2RSLOG) は、サーバー自体と同じユーザー ID の下で実行する必要があります。

開始タスクとして実行する代わりに、C2RSERVE、C2RSTOP、および C2RSLOG プロシージャーを実行するバッチ・ジョブを構成することもできます。例えば、ジョブ・スケジューリング・システムを使用して、zSecure Visual Server を始動および停止できます。または、セットアップ時に、最初の始動をバッチ・ジョブとして実行できます。バッチ・ジョブと開始タスクに関する考慮事項については、 28 ページの『ソフトウェアの使用可能化 (バッチ処理用)』を参照してください。

ジョブと開始タスクのいずれを選択した場合でも、以下のようにします。

- サーバー用に準備した zSecure 構成を反映するように、`EXEC` または `PROC` ステートメントの CONFIG=C2R$PARM を更新します。開始タスクの場合は、構成メンバー名または構成メンバー名の一部として System シンボルを使用することを検討します。
- プロシージャー C2RSTOP および C2RSLOG は、これらが動作するサーバーと同じ zSecure 構成 (同じサーバー・ルート・ディレクトリー) を参照する必要があります。
- `TIME=NOLIMIT` の指定が JCL 内に残っていることを確認します。サーバー・スターターは短時間のプロセスですが、サーバー自体は `MAXCPUTIM` の影響を受けないフォーク・プロセスで実行されます。CPU 時間の制限は、親から継承されます。

STARTED、SURROGAT、FACILITY、および XFACILIT リソースへの必要なアクセス権限を設定するために、ジョブ C2RZWADM が提供されています。 142 ページの『必要なシステム許可』を参照してください。 XFACILIT 以外のリソース・クラスを使用するようにサイト・モジュールをカスタマイズした場合は、それに応じてこのジョブを変更します。サイト・モジュールのカスタマイズについては、 205 ページの『付録 A. サイト・モジュール』を参照してください。

TCP/IP セキュリティー

サーバーには、IP スタックおよび選択されたポートを使用するための権限が必要です。ベース TCP ポートはジョブ C2RZWINI で構成できます。さらに、サーバーはベース +1 のポートを使用します。一時ポートのセットも使用しますが、これらのポートを予約する必要はありません。

TCP/IP 構成の `PORT` または `PORTRANGE` ステートメントで、SAF リソースを指定します。以下に例を示します。

```
PORTRANGE 8000 2 TCP * NOAUTOLOG SAF VISUAL
```

このステートメントは、TCP ポート 8000-8001 の使用を、SERVAUTH クラスの EZB.PORTACCESS.sysname.tcpname.VISUAL リソースに対して、READ 以上のアクセス権限を持っているユーザーだけに制限します。sysname は、MVS システム変数 SYSNAME に置き換えられます。tcpname は、TCP/IP ジョブ名に置き換えられます。

* の代わりに、サーバーおよび最初のサーバー始動ジョブとして使用するジョブ名を完全に、または部分的に指定できます。例えば、C2R* のように指定できます。ただし、SAF がアクティブの場合、通常はジョブ名制限を指定する必要はありません。

TCP/IP スタック内の未予約のポートの保護を活動化してある場合は、サーバーを実行するユーザー ID に、それらのポートを使用する権限を付与する必要があります。未予約ポートの保護について詳しくは、以下の URL の z/OS インターネット・ライブラリーにアクセスしてください。

http://www.ibm.com/systems/z/os/zos/library/bkserv/index.html

使用している z/OS のバージョンを選択し、「**Contents**」列で「**z/OS Communications Server**」 **->** 「**IP Configuration Reference**」を選択してください。

複数スタック (CINET) 環境では、zSecure Visual Server は、一度に 1 つのスタックにのみバインドされます。クライアント (および SE.W トランザクション) が接続できる予測可能な IP アドレスを使用するために、サーバーを始動するたびに必ず同じスタックが使用されるようにしてください。例えば、使用するスタックが ABC という名前であれば、C2RSERVE ジョブの C2RSERVE EXEC 行の前に以下のステップを追加することによって、スタック・アフィニティーをセットアップできます。

```
//STEP0    EXEC PGM=BPXTCAFF,PARM=ABC
```

サーバー (ジョブ C2RZWINI による最初の始動を含む) には、SERVAUTH クラスの EZB.STACKACCESS.sysname.tcpname リソースに対する READ 以上のアクセス権限が必要です。sysname は、MVS システム変数 SYSNAME に置き換えられます。tcpname は、TCP/IP ジョブ名に置き換えられます。

サーバーの初めての始動

最初のサーバー始動および認証局の設定を行うために、ジョブ C2RZWINI が提供されています。このジョブは、サーバーのユーザー ID の下で、かつサーバーを実行しようとする z/OS イメージで実行する必要があります。多重システム環境 (シスプレックスまたはそれ以前のマルチアクセス・スプール) では、ジョブが正しいシステム・イメージで実行されるようにシステム・アフィニティーを指定する必要が生じる場合があります。

別のユーザー ID の下でジョブ C2RZWINI を実行することもできますが、この場合は、サーバーを停止した後、ジョブ C2RZWXFR を実行します。

重要**:** 既に設定されているサーバーをアップグレードするときは、ジョブ C2RZWINI を実行しないでください。実行すると、以前に発行された証明書がすべて無効になります。

しばらくすると、次の行が <Server-root>/log/server.log) ファイルに表示されます。

```
P399M194V0.2.67L269A4S0E80:LCM: Initial certification completed successfully
```

認証局が設定されたら、ジョブ C2RSLOG を実行して、サーバー・ログを印刷し、出力をアーカイブします。問題が生じたときに、IBM ソフトウェア・サポートがこの出力を要求することがあります。

ジョブ C2RZWINI はサーバーの初期始動を実行しますが、ジョブ C2RZWINI 自体が終了しても、サーバーは終了しません。 167 ページの『zSecure Visual Server の操作』で説明するように、通常の始動と停止には、それぞれプロシージャー C2RSERVE と C2RSTOP を使用します。

既存の V1.*x* サーバーの、zSecure Visual 2.2.1 へのアップグレード

このタスクについて

すべてのアップグレードで、JCL のローカル・コピー (例えば、Visual Server を開始タスクとして実行するときの JES プロシージャー・ライブラリー) が zSecure コンポーネントのレベルと一致していることを確認する必要があります。これらのローカル JCL コピーには、Visual Server に使用する zSecure 構成が含まれています。新しいサーバー・インスタンスに対してはジョブ CKRZPOST が構成を準備しますが、アップグレードでは構成にカスタマイズが含まれるため、CKRZPOST が上書きしないように、この準備は行われません。

zSecure Visual 2.1.0 以上には C2RW131A スイッチが含まれています。このスイッチにより、通信が NIST 800-131A に準拠するように強制できます。ただし、古い Visual クライアントは使用可能になっていないことがあるので注意してください。このため、実際に準拠性を強制する前に新規バージョンをロールアウトする必要があります。スイッチを OFF に設定した場合でも、準拠しているプロトコルをサポートしているクライアントへの通信は準拠することになります。

手順

既存サーバー上の zSecure Visual ソフトウェアをアップグレードするには、以下のステップに従います。

1. 前のレベルをアンパックしたディレクトリーとは異なる新しいディレクトリーに、サーバー・ソフトウェアをアンパックします。
2. サーバー・ユーザー ID に、新しいディレクトリーおよびそのディレクトリーのファイルへの必要なアクセス権限があることを確認します。

   zSecure Visual クライアントのレベル 2.1.0 以上にすべてのクライアントをアップグレードし終えるまで、C2RW131A パラメーター値は必ず `OFF` に設定したままにしてください。
3. サーバーが使用する zSecure 構成を編集します。C2RWIN パラメーターが新しいソフトウェアの場所を反映していることを確認します。
4. サーバーを停止して再始動します。 NIST 800-131A 準拠のプロトコルをサポートしない zSecure Visual Server からサポートするものにアップグレードする場合は、log サブディレクトリー内の `server.log` ファイルに以下のメッセージが表示されるまで待ってから、クライアントの接続を試行してください。

- E160:LCM: The LCM certificate in current use, *certificate*, is not NIST 800-131A compliant. A new LCM certificate will be generated in about 300 seconds.
- E130:CA: The CA certificate in current use, *certificate*, is not NIST 800-131A compliant. A new CA certificate will be generated in about 300 seconds.
- E130:CA: The CA certificate in current use, *certificate*, is NIST 800-131A compliant.
- E160:LCM: The LCM certificate in current use, *certificate*, is NIST 800-131A compliant.

これらのメッセージの順序は重要であることに注意してください。準拠 LCM 証明書に関するメッセージが複数回表示されることがありますが、CA 証明書が NIST 800-131A 準拠であるというメッセージよりも前のメッセージはすべて無視します。「CA-compliant」メッセージよりも後に表示される最初の「LCM-compliant」メッセージが、サーバーにクライアントを接続する準備ができたことを示します。

重要: アップグレード時には、ジョブ C2RZWINI を実行しないでください。実行すると、以前に発行された証明書がすべて無効になります。

IBM Security zSecure Visual および zSecure コンポーネントの互換性

このトピックのガイドラインを使用して、IBM Security zSecure Visual のアップグレードを計画します。

zSecure Visual の機能を最適化するには、すべての関連コンポーネントが同一のバージョンである必要があります。最適なパフォーマンスを得るために、zSecure Visual クライアント 2.2.1 を以下と組み合わせてください。

- z/OS V2R2
- CKRCARLA 2.2.1
- CKGRACF 2.2.1
- zSecure Visual Server 2.2.1

zSecure Visual クライアントをアップグレードする際に、クライアントが zSecure Visual サーバーと同一のリリース・レベルである必要はありません。ただし、IBM は、Visual クライアントの以前のリリースと Visual サーバーの現行リリースの組み合わせはサポートしません。 151 ページの表 7を参照してください。

最初にサーバーを最新リリースへとアップグレードした後、新規クライアントのインストールを開始してください。すべてのクライアント・インスタンスをアップグレードするワークロードを管理している場合でも、サーバーのインスタンスが複数存在することが可能です。

同一のワークステーション上に複数の zSecure Visual クライアント・バージョンが共存できます。例えば、1 台のコンピューター上で、バージョン 2.1 のクライアン

トを削除せずに、バージョン 2.2.1 をインストールできます。通常は、ポートの競合が発生しないかぎり、1 台のコンピューター上に複数クライアントが同時に存在できます。

- 複数バージョンを並行して実行するには、デフォルト以外の異なるローカル・ポート番号を構成します。
- 各クライアント・バージョンのポート値が、それぞれが通信を行う Visual サーバーのポートと対応していることを確認します。

ポートの競合が発生しないように構成すれば、異なるバージョンの複数の zSecure サーバー・インスタンスもサポートされます。詳しくは、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照してください。

表 7 に、zSecure Visual Server のバージョンに基づく有効なサポートを示します。

表 *7. zSecure Visual* クライアント・バージョンの互換性

サーバー クライアント	**zSecure Visual2.2.1**	**zSecure Visual2.2.0**	**zSecure Visual2.1.1**	**zSecure Visual2.1.0**	**zSecure Visual 1.13.1**	**zSecure Visual 1.13.0**
zSecure Visual2.2.1	サポート	公式サポートなし	公式サポートなし	公式サポートなし	公式サポートなし	公式サポートなし
zSecure Visual2.2.0	互換性あり	サポート	公式サポートなし	公式サポートなし	公式サポートなし	公式サポートなし
zSecure Visual2.1.1	互換性あり	互換性あり	サポート	公式サポートなし	公式サポートなし	公式サポートなし
zSecure Visual2.1.0	互換性あり	互換性あり	互換性あり	サポート	公式サポートなし	公式サポートなし
zSecure Visual 1.13.1	互換性あり	互換性あり	互換性あり	互換性あり	サポート	公式サポートなし
zSecure Visual 1.13.0	互換性あり	互換性あり	互換性あり	互換性あり	互換性あり	サポート

注**:** 互換性あり とは、下位レベルのクライアントで新機能がサポートされていないことを意味しています。

サーバーによるクライアントの認識

サーバーにアクセスするには、zSecure Visual クライアントにローカル・サーバー定義と、そのサーバー上に対応するクライアント定義が必要です。メインフレーム環境では、クライアントの初期構成および同時構成のサポートが制限されます。少なくとも 1 つのクライアントをインストールして構成した後、このクライアントを使用して、さらにクライアント定義を作成し、保守します。 159 ページの『クライアント定義を管理するための権限』を参照してください。

ISPF を介した Visual サーバーへのアクセス

zSecure Visual 用の zSecure 構成のセットアップに関するガイドラインについては、 141 ページの『インストール要件』を参照してください。 zSecure 構成について詳しくは、 31 ページの『第 6 章 ソフトウェアのデプロイメント』を参照してください。

注: C2RWZINI ジョブは、特にそのサーバー・インスタンスに対して実行しておく必要があります。

Visual クライアントの構成

このタスクについて

管理者は、zSecure Visual クライアントを構成するために ISPF インターフェースを使用します。

手順

1. z/OS ISPF の IBM Security zSecure Admin に移動します。
2. **SE** (セットアップ) を入力し、**W** (Windows 構成) を選択します。
3. アクション **AP** を使用して、クライアントと初期パスワードを作成します。 ここではアクション **A** を使用して、後でアクション **P** を使用することもできます。ここでアクション **AP** を使用して、初期パスワードを紛失した場合、初期パスワードを取り消す場合、またはクライアントが正常にインストールされる前にパスワードの有効期間が経過した場合は、アクション **P** を使用して新しい初期パスワードを生成できます。

```
 Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
                           zSecure Visual - Configuration
Command ===> ____________________________________________________   _ start panel

 1  1. Add, delete, or install zSecure Visual Windows client

Server  . . . . . . IP01                                          (IP or DNS)
Server base port  . 8000____                              (IP base port of server)

Act Agent id
AP  12.1. 100_______

Act must be A, D, P, C, AP (A=add D=delete C=cancel pwd P=new pwd)
```

図 *7. zSecure Visual Windows* クライアントの構成画面

ユーザーの TSO セッションは、サーバーがアクティブ状態のシステム上にある必要はありません。そのため、解決可能な DNS 名または IP アドレスとポート番号によってサーバーを選択する必要があります。

IP アドレスを指定する場合は、クライアントが使用するのと同じ IP アドレスを使用してください。

注: 以下のアドレスは使用しないでください。

ループバック・アドレス
: 各スタックにループバック・アドレスの独自のコピーがあるため、使用しないでください。

動的 **VIPA** アドレス
: このようなアドレスはスタック間、さらには z/OS イメージ間で移動する可能性があるため、使用しないでください。

クライアント ID でクライアントを識別する必要があります。クライアント ID は、クライアントのサーバー定義ダイアログで使用される ID と一致している必要があります。

4. ユーザー ID と対応するパスワードを入力するようプロンプトが出されます。

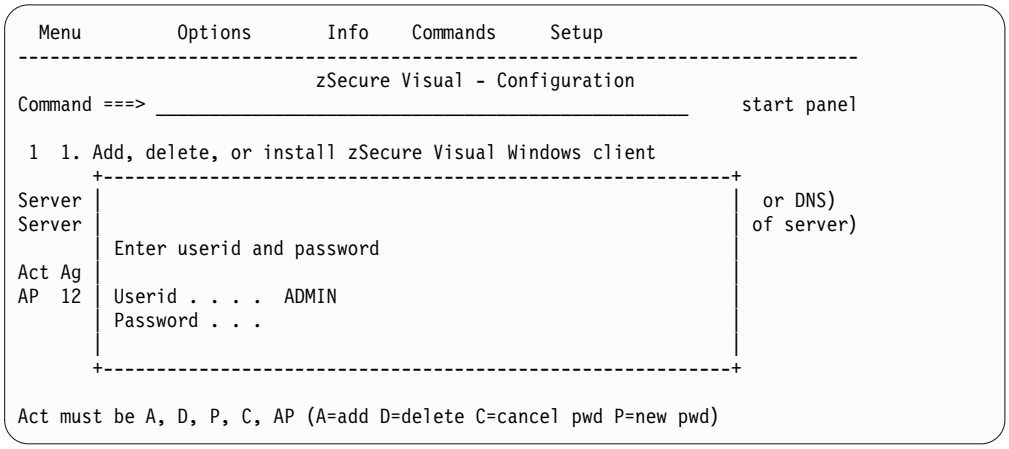


図 *8. zSecure Visual Windows* クライアントのユーザー *ID* およびパスワード構成

正常にログオンし、クライアントが存在する場合、クライアント・サイドのサーバー定義ダイアログで指定する必要がある初期パスワードが表示されます。初期パスワードの有効期間は 7 日間、またはサーバーの実行中です。有効期間が経過する前にパスワードを取り消すには、 154 ページの『パスワードの取り消し』を参照してください。

パスワード生成が失敗した場合、画面の右上に一般エラー・メッセージが表示されます。より説明的なエラー・メッセージも表示されます。問題診断については、 174 ページの『SE.W 通信の問題』を参照してください。

5. 「*IBM Security zSecure Visual:* クライアント・マニュアル」の説明に従って、パーソナル・コンピューターにクライアントをインストールします。 以前のリリースに次いで新しいクライアントをインストールできます。以前のリリースにおけるカスタマイズは、新しいリリースでは使用されません。ただし、「*IBM Security zSecure Visual:* クライアント・マニュアル」で説明するように、以前に定義したサーバーを証明書を含めてコピーできます。

注**:** 1.*x* サーバーのアップグレード時に、既存の証明書は自動的に 2.*x* サーバーの新規暗号化標準に変換されます。2.2.1 サーバー上に、1.*x* クライアントの新規証明書を作成することはできません。

タスクの結果

サーバーが予期しない動作をする場合は、log ディレクトリーにある次のファイルを確認します。

bbracf.log、server.log
これらのファイルによって、サーバーの直前の実行に関する情報が提供されます。

bbracf.log0、...、bbracf.log9
これらのログ・ヒストリー・ファイルは、サーバーの以前の実行に対応します。最大 10 のログ・ヒストリー・ファイルが保存されます。

zSecure Visual クライアントの問題のデバッグについて詳しくは、「*IBM Security zSecure Visual:* クライアント・マニュアル」を参照してください。

パスワードの取り消し

クライアント・インストールに既存のパスワードを使用しない場合は、Windows 構成パネルでアクション **C** を入力することで、パスワードを取り消すことができます。これを有効にするには、実際にそのパスワードを使用して誰かがクライアントをインストールする前に取り消します。新規パスワードを生成する前にアクション **P** および **AP** を実行した場合も、既にクライアントに対して発行されていたすべてのパスワードが取り消されます。

Visual クライアントの一括作成

このタスクについて

一括エージェント機能は、一括パスワード・リセットとしても機能します。エージェント ID が既に存在するかどうかのテストは行いません。

一括追加機能は、2 つのモードで作動します。

Autogen =yes
このモードでは、一括プロセスによって、次のような形式で生成されたエージェント ID と初期パスワードでデータ・セットが作成または上書きされます。

```
614 >CFC51AF4A7
615 >5171DCADCD
```

番号は、「zSecure Visual Configuration」パネルで固定定数 12.1 の後の列に入力できる番号に相当します。生成されたリストを使用して、各エージェント・ユーザーに初期パスワードを知らせることができます。サーバー定義の追加または編集については、「*IBM Security zSecure Visual:* クライアント・マニュアル」を参照してください。

Autogen = no
このモードでは、一括プロセスは、ここで示すようなデータ・セットを入力として受け付けます。パスワードと > 文字は省略することも、あるいは、以前の実行でデータ・セットに残された内容を含むこともできます。データ・セットは順次データ・セットで、レコード・フォーマットは F または FB である必要があります。

手順

1. 一括エージェントを起動するには、ISPF の下の任意の zSecure 製品パネルに移動し、コマンド行で次のコマンドを入力します。

```
TSO C2RELSI BULK
```

2. ライン・モード・ダイアログのプロンプトに対して、以下の情報を入力します。
   - サーバーのベース・ポート番号
   - Autogen モードを使用するかどうか
   - 最初のエージェントのエージェント番号と、生成するエージェントの数。これら 2 つの数値は、Autogen モードの場合にのみ必要です。
   - zSecure Visual クライアントのデータ・セット名。
     - 非 Autogen モードでは、このデータ・セットは既に存在している必要があり、生成するエージェントのリストが含まれている必要があります。
     - Autogen モードでは、このデータ・セットは存在していてもしていなくてもかまいません。
3. ダイアログの最後で、zSecure Visual 管理者のユーザー ID とパスワードを要求するプロンプトが出されます。これらの項目が正しく入力されると、初期パスワードのリストが表示されます。

クライアント権限の構成

デフォルトでは、クライアント権限は XFACILIT クラスを使用してチェックされます。ただし、インストール済み環境で zSecure 関連リソースに異なるリソース・クラスを使用するように選択した可能性があります。 205 ページの『付録 A. サイト・モジュール』を参照してください。 z/OS UNIX System Services でチェックされるリソース (すなわち、BPX.** で対象とされるリソース) は、再構成できません。これらのリソースは、常に FACILITY クラスでチェックされます。

ユーザーにインターフェース・レベルを割り当てるプロファイル

ほとんどの場合、zSecure Visual クライアント・アプリケーションのメニュー・オプション、ボタン、およびフィールドは、ユーザーが選択可能なインターフェース・レベルに基づいて、使用可能または使用不可にされます。中央管理者は、各ユーザーが選択できるインターフェース・レベルを構成できます。インターフェース・レベルには、ヘルプ・デスク、接続、ユーザー、アクセス・リスト、グループ、およびフルがあります。これらの各レベルで許可される正確な操作については、「*IBM Security zSecure Visual:* クライアント・マニュアル」に文書化されています。

クライアント・ユーザーに対してインターフェース・レベルを拒否するには、次の表にリストされたプロファイルに対して NONE 権限を付与します。

表 8. ユーザーにインターフェース・レベルを割り当てるプロファイル

プロファイル	**Interface level**
C2R.CLIENT.INTERFACE.HELPDESK	Helpdesk
C2R.CLIENT.INTERFACE.CONNECT	接続
C2R.CLIENT.INTERFACE.USER	ユーザー
C2R.CLIENT.INTERFACE.ACCLIST	アクセス・リスト
C2R.CLIENT.INTERFACE.GROUP	グループ
C2R.CLIENT.INTERFACE.FULL	Full

互換性の理由により、インターフェース・レベル用の個別プロファイルが必要です。対応するプロファイルがないインターフェース・レベルは、すべての zSecure Visual ユーザーが使用可能になります。

以降のトピックで説明するように、zSecure Visual クライアント・インターフェースは、この他にいくつかのセキュリティー・リソースを使用してその機能を構成します。これらのリソースのサブセットは、MYACCESS レポート出力を使用して確認できます。ユーザーの MYACCESS 出力を検査するには、次の TSO コマンドを使用します。

```
CKGRACF SHOW MYACCESS ID <id>
```

生成されるコマンドに必要なアクセス権限

155 ページの『ユーザーにインターフェース・レベルを割り当てるプロファイル』で説明したように、クライアント・アプリケーションのメニュー・オプション、ボタン、チェック・ボックス、およびフィールドは、プロファイルに基づいて使用可能または使用不可にされますが、さらにサーバー・サイドで権限が必要です。これらの権限がない場合、ボタンおよびチェック・ボックスに対応してクライアントが生成したコマンドが、サーバー・サイドで失敗します。そのため、中央管理者がユーザーに特定のインターフェース・レベルを付与する場合は、次の表で示すように、管理者は必ずそのユーザーにリソースへのアクセス権限が付与されていることを確認する必要もあります。

表 *9.* 役割ベースの権限のためのリソース

リソース	**Uacc**	**Helpdesk**	接続	**User**	アクセス・リスト	**Group**	**Full**
CKG.CMD.CMD.EX.ADDGROUP	n	n	n	n	n	u	u
CKG.CMD.CMD.EX.ADDSD	n	n	n	u	u	u	u
CKG.CMD.CMD.EX.ADDUSER	n	n	n	u	u	u	u
CKG.CMD.CMD.EX.ALTDSD	n	n	n	u	u	u	u
CKG.CMD.CMD.EX.ALTGROUP	n	n	n	n	n	u	u
CKG.CMD.CMD.EX.ALTUSER	n	n	n	u	u	u	u
CKG.CMD.CMD.EX.DELDSD	n	n	n	n	n	u	u
CKG.CMD.CMD.EX.DELGROUP	n	n	n	n	n	u	u
CKG.CMD.CMD.EX.PERMIT	n	n	n	u	u	u	u
CKG.CMD.CMD.EX.RACMAP	n	r	r	r	r	r	r
CKG.CMD.CMD.EX.RALTER	n	n	n	u	u	u	u
CKG.CMD.CMD.EX.RDEFINE	n	n	n	u	u	u	u
CKG.CMD.CMD.EX.RDELETE	n	n	n	n	n	u	u
CKG.CMD.CMD.EX.SETROPTS	n	n	n	u	u	u	u
CKG.CMD.CMD.REQ.CONNECT	n	n	u	u	u	u	u
CKG.CMD.CMD.REQ.PERMIT	n	n	n	n	u	u	u
CKG.CMD.CMD.REQ.REMOVE	n	n	u	u	u	u	u
CKG.CMD.COMMENT	n	r	r	r	r	r	r
CKG.CMD.LIST	r	r	r	r	r	r	r

表 9. 役割ベースの権限のためのリソース (続き)

リソース	Uacc	Helpdesk	接続	User	アクセス・リスト	Group	Full
CKG.CMD.SHOW.MYACCESS	n	r	r	r	r	r	r
CKG.CMD.USER.REQ.PWDEFAULT	n	n	n	u	u	u	u
CKG.CMD.USER.REQ.PWNOHIST	n	n	n	n	n	n	u
CKG.CMD.USER.REQ.PWNORULE	n	n	n	n	n	n	u
CKG.CMD.USER.REQ.PWRESET	n	u	u	u	u	u	u
CKG.CMD.USER.REQ.PWSET	n	u	u	u	u	u	u
CKG.CMD.USER.REQ.PWSET.DEFAULT	n	n	n	u	u	u	u
CKG.CMD.USER.REQ.PWSET.EXPIRED	n	n	n	u	u	u	u
CKG.CMD.USER.REQ.PWSET.NONEXP	n	n	n	u	u	u	u
CKG.CMD.USER.REQ.PWSET.PASSWORD	n	n	n	u	u	u	u
CKG.CMD.USER.REQ.PWSET.PREVIOUS	n	n	n	u	u	u	u
CKG.CMD.USER.REQ.RESUME	n	r	u	u	u	u	u
CKG.CMD.USER.REQ.SCHEDULE	n	u	u	u	u	u	u
CKG.RAC.SCP.CONNECT.BASE.AUTH.USE	n	n	u	u	u	u	u
CKG.RAC.SCP.CONNECT.BASE.AUTH.*	n	n	n	u	u	u	u
CKG.RAC.SCP.*.BASE.*	n	n	n	n	u	u	u
CKG.SCP.ID.**	n	n	n	n	n	n	u

- 必要なアクセス権限レベルは短縮形で示しています。n は NONE、r は READ、u は UPDATE です。
- 特に CKG.CMD.USER.REQ.PWNOHIST および CKG.CMD.USER.REQ.PWNORULE については、ユーザーに UPDATE アクセス権限を付与すると、それぞれ、RACF SETROPTS 設定で指定されているパスワード・ヒストリーおよびパスワード規則をバイパスすることになります。
- 表で示したその他のすべてのリソースについては、より高いアクセス権限を付与しても、影響はありません。ただし、ALTER アクセス権限は付与しないでください。このアクセス権限は、リソースだけではなく、プロファイルに対する完全な制御 (フル・コントロール) もユーザーに許可するからです。
- 総称プロファイルはサポートされます。
- 前の表のリソースで対象にすると判断したすべてのプロファイルに加えて、多くをキャッチするプロファイル CKG.CMD.USER.REQ.*、CKG.CMD.**、CKG.RAC.**、CKG.SCP.ID.*.SYS1.*、および CKG.** を UACC=NONE で作成し、さらに空のアクセス・リストを作成します。この方法を使用すると、将来の zSecure Visual のリリースで、委任管理者に新機能が誤って使用可能になることを予防できます。

スケジュール名選択リストのプロファイル

ユーザーが作成できるスケジュールは、CKG.SCHEDULE.<SCHEDULE NAME> 形式の個別プロファイルで定義されます。スケジュールを作成するとき、ユーザーは、使用可能なスケジュール名をリストから選択できます。スケジュール名

$DELETE を使用すると、ユーザーがユーザー・プロファイルに削除のマークを付けることができます。次の表で、考えられるスケジュール名の例をいくつか示します。

表 *10.* スケジュール名選択リストを提供するプロファイル

プロファイル	**Uacc**	ヘルプ・デスク	接続	ユーザー	アクセス・リスト	グループ	**Full**
CKG.SCHEDULE.$DELETE	n	n	n	u	u	u	u
CKG.SCHEDULE.GRPADMIN	n	n	u	u	n	u	u
CKG.SCHEDULE.HELPDESK	n	u	u	n	n	n	n
CKG.SCHEDULE.SYSADMIN	n	n	n	n	n	n	u

ユーザーの複写に必要な権限

通常、ユーザーを複写するには、少なくともグループ Special 権限および CLAUTH(USER) 権限が必要です。マスター・カタログに別名を作成するには、DATASET 権限も必要です。

Define Alias アクションを許可するプロファイル

Define Alias アクションを許可するには、CKG.UCAT.<USER CATALOG NAME> 形式の個別プロファイルを作成します。これらのプロファイルは、それがないと、ユーザー・カタログが存在するかどうかを zSecure Visual が確認できないため必要です。zSecure Visual ユーザーに、ユーザー・カタログを表すプロファイルに対する READ 以上のアクセス権限が付与されている場合、そのユーザーは、そのカタログを指すユーザー ID またはグループ ID の別名を定義できます。

表 *11. Define Alias* アクションを許可するプロファイル

プロファイル	**Uacc**	任意の役割
CKG.UCAT.<USER CATALOG NAME>	n	nr*

RACF 範囲設定のリソース

ユーザーのリソースへのアクセス権限が READ 以上である場合、システムはユーザーの CKGRACF 範囲を、READ アクセス権限があるユーザーの RACF 範囲に拡張します。ユーザーのアクセス権限が NONE である場合、範囲は拡張されません。

表 *12. RACF* 範囲設定を活動化するリソース

リソース	**Uacc**	任意の役割
CKG.SCP.RACF	n	nr*

zSecure Visual ユーザーのパスワード変更ポリシー

ローカル・ポリシーで、ユーザーがパスワードを変更するときに理由を指定する必要がある場合、次の表のプロファイルを使用して、ポリシーを適用できます。このプロファイルは、プロファイルへの NONE 権限を持つユーザーがパスワードの変

更を試行したときに起動されます。その他の場合、理由の指定は可能ですが必須ではありません。個別プロファイルが必要です。

表 *13.* パスワード変更ポリシーを適用するプロファイル

プロファイル	**Uacc**	任意の役割
C2R.CLIENT.EMPTYREASON.PWSET	n	n

ユーザー用のセグメント編集

セグメントを編集するには、 156 ページの『生成されるコマンドに必要なアクセス権限』で示すように、クラスの関連するリソースへの UPDATE アクセス権限がユーザーに必要です。 (具体的には、CKG.CMD.CMD.EX.ALTUSER、CKG.CMD.CMD.EX.ALTGROUP、 CKG.CMD.CMD.EX.ALTDSD、および CKG.CMD.CMD.EX.RALTER です。)さらに、ユーザーには FIELD クラス・リソース (または、システム Special) に対する UPDATE アクセス権限が必要です。

次の表に、セグメント編集の制御に使用されるリソースの構文を示します。

表 *14.* セグメント編集を制御するリソース

プロファイル	**Uacc**	任意の役割
<CLASS>..<FIELD>	n	u

クライアント定義を管理するための権限

安全なチャネルを通じてサーバーにアクセスするには、zSecure Visual クライアントにローカル・サーバー定義と、そのサーバー上に対応するクライアント定義が必要です。新しいチャネルをセットアップするには、初期パスワードが 1 回必要です。サーバー上にあるクライアント定義を管理するには、管理者は、C2R.SERVER.ADMIN リソースに対する READ 以上のアクセス権限を持っている必要があります。このアクセス権限によって、管理者はログオンできる任意のシステムで、新しいクライアント定義の作成、既存のクライアント定義の編集および削除、初期パスワードの生成ができます。この権限は、最小限のユーザーにのみ付与してください。

表 *15. zSecure Visual* サーバーおよびクライアント定義を保守するリソース

リソース	**Uacc**	任意の役割
C2R.SERVER.ADMIN	n	r

システム全体の **RACF** オプションを表示するプロファイル

システム全体の RACF オプションを表示するには、ユーザーは、次の個別プロファイルに対する READ アクセス権限を持っている必要があります。

表 *16.* システム全体の *RACF* オプションを表示するプロファイル

プロファイル	**Uacc**	任意の役割
C2R.CLIENT.SETROPTS	n	r

このプロファイルは、XFACILIT クラスの個別プロファイルとして定義されています。zSecure Visual クライアント・ユーザーにプロファイルへの READ アクセス権限がない場合、そのユーザーは、RACF SETROPTS 設定を表示できません。

サイト固有の機能の実装

zSecure Visual では、以下の 2 つのサイト固有の機能がサポートされます。

- Visual クライアントでのサイト固有のユーザー・データの表示。これは組織に固有の、ユーザー専用情報であるデータです (従業員番号や部署コードなど)。
- エンド・ユーザーに対する透過的な方法による、Visual クライアントからそのユーザー・インターフェースを介した、サイト固有の REXX スクリプトの呼び出し。これにより、組織の新機能をサポートするために Visual クライアントを完全にカスタマイズできます。

これらのサイト固有の機能を実装する場合は、Visual Server の追加構成が必要になります。

サイト固有のユーザー・データ

このトピックのガイドラインおよび設定を使用して、zSecure Visual のサイト固有のユーザー・データを構成します。

サイト固有のユーザー・データ を表示するように zSecure Visual を構成できます。このデータは、組織固有のユーザー専用情報です (従業員番号や部署コードなど)。その後、Visual クライアントの以下のパネルで、このデータの取得、表示、および検索を実行できるようになります。

- ユーザー・プロパティー・ダイアログ
- ユーザー・テーブル
- 「Find」ダイアログ

例えば、通常表示される他のフィールドと共に Visual クライアントに表示する従業員情報を取得するように、Visual Server を構成できます。

Visual クライアントでサイト固有のユーザー・データが表示されるように構成するには、以下のタスクを実行します。

- ユーザーに表示する情報と情報の特性を決定します。
  - Visual クライアントで表示するサイト固有のユーザー・データ・セットの場所、およびそのデータ・セット内の情報。
  - Visual クライアントでユーザー・データを表示するときの列順。
  - ユーザーが検索操作を実行できるデータの列。
  - サイト固有のユーザー情報を、INSTDATA 情報と共に表示するか、この情報の代わりに表示するか。
- アソシエーション構成ファイルとレコード・フォーマット構成ファイルを作成して、サイト固有のユーザー情報の場所とフォーマットを指定します。このセクションでは、これらのファイルについて説明します。
- C2RWCUST ALLOC パラメーターの C2RWASSC データ・セット・メンバーを使用して、データ・セットの Visual クライアントに対する割り当てを指定しま

す。 223 ページの『付録 D. 構成パラメーターと構成メンバー』の C2RWCUST パラメーターを参照してください。

アソシエーション構成ファイル

このファイルは、Visual Server がサイト固有のユーザー情報にアクセスできるようにするために、この情報をステージングするデータ・セットの名前を指定します。アソシエーション構成ファイルでは、ヘッダー行の後に 1 つ以上のデータ・ファイル定義と、1 つ以上のレコード・フォーマット・ファイル定義が指定されます。

ヘッダー行

ヘッダー行は、次のように大文字の H を先頭文字として指定され、その後にサイト・アソシエーション構成ファイルのバージョン番号 (現在は 1.13) が続きます。

```
H1.13
```

データ・ファイル定義

データの表示対象となるユーザー ID と、データ・レコードを格納するデータ・ファイルの名前を指定します。

```
Uuser_id DATA DSN='data.file'
```

U*user_id*

個別のユーザー ID、またはすべてのユーザーの汎用ユーザー ID を指定します。各行の先頭文字は、大文字の U とします。このキーワードと DATA キーワードは、1 つ以上のスペースで区切ります。

個別の *user_id*

単一のユーザー ID のユーザー情報を取得および表示する場合は、個別の RACF ユーザー ID を指定します。指定されたデータ・ファイルを使用するには、このユーザー ID とクライアントにログオンしているユーザー ID が一致している必要があります。個別のユーザー ID は、表示データの初期セットアップをテストする場合や、アクセスを特定のユーザーに制限する場合に使用します。

汎用の *user_id*

すべてのユーザー ID のユーザー情報を取得および表示する場合は、汎用のユーザー ID を指定します。汎用のユーザー ID は、アスタリスク (*) を使用して指定します (U*)。個別のユーザー ID が指定および検証された場合は、汎用のユーザー ID は使用されません。汎用のユーザー ID は、通常の操作の一環として、組織内の多くのユーザーにユーザー情報を表示する場合に使用します。

DATA

このキーワードは、データ・レコードを格納するデータ・ファイル名の前に指定する必要があります。このキーワードと DSN パラメーターは、1 つ以上のスペースで区切ります。

DSN='*data.file***'**
指定されたユーザー ID のデータ・レコードを格納するデータ・ファイルの名前を指定します。ファイル名は単一引用符で囲みます。

レコード・フォーマット・ファイル定義
データの表示対象となるユーザー ID と、レコード・フォーマット構成ファイルの名前を指定します。

```
Uuser_id RECFORMAT DSN='recordformat.file'
```

U*user_id*
個別のユーザー ID、またはすべてのユーザーの汎用ユーザー ID を指定します。各行の先頭文字は、大文字の U とします。このキーワードと RECFORMAT キーワードは、1 つ以上のスペースで区切ります。

個別の *user_id*
取得された単一のユーザー ID のユーザー情報に対してフォーマットを設定する場合は、個別の RACF ユーザー ID を指定します。

汎用の *user_id*
取得されたすべてのユーザー ID のユーザー情報に対してフォーマットを設定する場合は、汎用のユーザー ID を指定します。汎用のユーザー ID は、アスタリスク (*) を使用して指定します (U*)。

RECFORMAT
このキーワードは、レコード・フォーマット・ファイル名の前に指定する必要があります。このキーワードと DSN パラメーターは、1 つ以上のスペースで区切ります。

DSN='*record_format.file***'**
レコード・フォーマット構成ファイルの名前を指定します。ファイル名は単一引用符で囲みます。

アソシエーション構成ファイルの内容の例
この例では、2 つのデータ・セット名を指定する場合 (1 つは個別ユーザー用のエントリー、もう 1 つはすべてのユーザー用の汎用エントリー) を示します。

```
H1.13
UDEMOUSER   DATA        DSN='DEMO.DATA'
UDEMOUSER   RECFORMAT   DSN='DEMO.FORMAT1'
U*          DATA        DSN='SERV#1.DATA'
U*          RECFORMAT   DSN='SERV#1.RECFMT'
```

レコード・フォーマット構成ファイル
レコード・フォーマット構成ファイルは、サイト固有のデータ・ファイルからのユーザー情報を表示する方法を指定します。レコード・フォーマット・ファイルには、以下のレコード・タイプがあります。

FIELD キー・フィールド
この項目の構文は、以下のとおりです。

```
*FIELD 'field_name' (field_start,length)
```

ここで、

***FIELD**
必須。CARLa がローカル・サイトのユーザー・データと RACF 情報とを組み合わせるには、データ・ファイル内の各行に、RACF データベース内の値と一致するフィールドが含まれている必要があります。このフィールドは、*field_name* を使用して定義されます。 CARLa は、RACF から情報を抽出するときに、選択したフィールドの RACF 値を使用して、データ・ファイル内の関連行を検索します。

field_name
必須。データ・ファイル内の関連行を検索するために使用されるユーザー・プロファイル・フィールドを指定します。フィールド名を単一引用符で囲む必要があります。フィールド名を区切るには、*FIELD の後に少なくとも 1 つのスペースを含める必要があります。

field_start,length
field_name として指定された値に対応するデータ・ファイル内のフィールドの開始位置およびその名前の長さを指定します。どちらの値にも整数を指定する必要があります。
*FIELD を使用したレコード・フォーマット構成ファイルの内容の例に示されているように区切り文字を使用します。つまり、整数をコンマで区切り、両方の値を小括弧で囲みます。

ユーザー**ID** キー・フィールド
この項目の構文は、以下のとおりです。

```
*USERID (field_start)
```

ここで、

***USERID**
必須。CARLa がローカル・サイトのユーザー・データを RACF 情報に関連付けられるようにするには、データ・ファイル内の各行に、RACF データベース内の値 (RACF USERID) と一致するフィールドが含まれている必要があります。CARLa は、RACF から情報を抽出するときに、UserID の RACF 値を使用して、データ・ファイル内の関連行を検索します。その後、CARLa は、定義されたオフセット (例えば、*USERID を使用したレコード・フォーマット構成ファイルの内容の例では Department のオフセット 29) を使用してこれを抽出し、Visual クライアントに返される値に含めます。

field_start
必須。ユーザー ID フィールドの開始点を指定します。フィールドは常に 8 文字長であるため、フィールド長は指定しません (すべてのユーザー ID は 8 文字長です)。
*USERID プレフィックスの後に 1 つ以上のスペースを挿入して、*field_start* 値を区切る必要があります。

列定義

n '*column_title*' (*field_start*,*length*) **Y | N**

n
ユーザー・プロファイル・テーブルとユーザー・プロパティー・フォームで列を表示する順序を示す列のシーケンス番号を指定します。1 から 9 までの単一の整数を指定します。列の最大数は 9 です。

'*column_title*'
表示される列に割り当てる名前を指定します。単一引用符を使用する必要があります (例: 'Department')。最大 20 文字を指定できます。

(*field_start*,*length*)
列の開始点と、データ・ファイル内のフィールドの幅 (長さ) を指定します。どちらの値にも整数を指定する必要があります。上記に示すように、区切り文字として、各整数をコンマで区切り、両方の値を括弧で囲みます。列の定義が重複していないかどうかの検証は行われません。管理者が責任を持って正確に値を指定する必要があります。

Y | N
列に対する検索を有効にするかどうか (列を検索フォームに追加するかどうか) を指定します。検索を有効にする場合は Y、検索を無効にする場合は N を指定します。Y または N を指定しない場合、その列に対する検索は有効になりません。

インストール・データ

```
*INSTDATA
```

このフィールドを指定しない場合、Visual クライアントは、ユーザー・テーブルおよびユーザー・プロパティー・ダイアログ内のインストール・データ・フィールドの代わりにサイト定義の列を表示します。Visual クライアントでサイト固有のユーザー情報とインストール・データ情報を表示する場合は、レコード・レイアウトに *INSTDATA 行を追加します。

***FIELD** を使用したレコード・フォーマット構成ファイルの内容の例
この例では、サイト固有のユーザー情報を 4 つのフィールド (ダイアログによっては列) に表示し、そのうちの 1 つ (Employee) が検索可能フィールドであるレイアウトを示します。フィールドの順序が、列定義のリスト順序と異なっていても構いません (フィールドの順序は列シーケンス番号で指定されます)。ユーザー情報に加えて、インストール・データ (INSTDATA) 情報も表示されます。

この例では、データ (ソース) ファイル内での一連のオフセットに従ってフィールドがリストされています。

```
*FIELD 'pgmrname' (1,20)
1 'Employee No.' (21,7)
2 'Department' (29,5)   Y
4 'Cost Center' (34,7)
3 'State'  (42,3)
*INSTDATA
```

Visual クライアントは、レコード・フォーマット構成ファイルを読み取って、対応する CARLa コマンド (Visual Server に送信) を生成します。以下の例は、レコード・フォーマット構成ファイルの前述の例のフィールドによって参照される固定長のレコードを持つデータ・ソース・ファイルの内容を示しています。

```
Offsets:

1                  21      29   34      42

|                  |       |    |       |

A. Name One        1000405 203420002451 NSW

B. Name Two        0003050 300120002451 TAS

C. Name Three      2030060 203420030288 NSW

A. Name Four       2004078 300120002451 VIC

B. Name Five       1000407 510630030288 SA

C. Name Six        0060902 640620005624 WA
```

***USERID** を使用したレコード・フォーマット構成ファイルの内容の例

この例では、サイト固有のユーザー情報を 4 つのフィールド (ダイアログによっては列) に表示し、そのうちの 1 つ (Employee) が検索可能フィールドであるレイアウトを示します。フィールドの順序が、列定義のリスト順序と異なっていても構いません (フィールドの順序は列シーケンス番号で指定されます)。ユーザー情報に加えて、インストール・データ (INSTDATA) 情報も表示されます。

この例では、データ (ソース) ファイル内での一連のオフセットに従ってフィールドがリストされています。

```
*USERID             (1,8)
2 'Employee'       (9,20) Y
1 'Department'     (29,5)
4 'Cost Center'   (34,7)
3 'State'        (42,3)
*INSTDATA
```

この例では、Visual クライアントで表示したい順序に従ってフィールドがリストされています。

```
*USERID             (1,8)
1 'Department'     (29,5)
2 'Employee'       (9,20) Y
3 'State'        (42,3)
4 'Cost Center'   (34,7)
*INSTDATA
```

Visual クライアントは、レコード・フォーマット構成ファイルを読み取って、対応する CARLa コマンド (Visual Server に送信) を生成します。以下の例は、固定長レコードを含む RACF データ (ソー

ス) ファイルから取得したレコードに、前の例で示したレコード・フォーマット構成ファイルのフィールドとオフセットの場所で参照されているレイアウトを適用した表示画面を示しています。

```
offsets: 1       9                   29    34     42
         C2RWQA47QA-00000047         500654300510 SA
         C2RWQA46QA-00000048         500654301610 TAS
         C2RWQA40QA-00000040         500654300510 WA
```

サイト定義の REXX スクリプト

このトピックのガイドラインを使用して、zSecure Visual をカスタマイズし、エンド・ユーザーに対して透過的に、サイト定義の REXX スクリプトを zSecure Visual からそのユーザー・インターフェースを介して呼び出すことができます。現在、REXX スクリプトはローカル・ノードのみで実行できます。

バージョン 2.1.0 以降は、zSecure Visual をカスタマイズし、サイト定義の REXX スクリプトを zSecure Visual ユーザー・インターフェースを介して呼び出すことができます。このプロセスは、エンド・ユーザーに対して透過的です。サイト定義の REXX スクリプトを zSecure Visual からそのユーザー・インターフェースを介して呼び出すには、Visual クライアントが使用できるサイト定義のスクリプト構成情報が含まれた関連ファイルを使用して Visual Server を構成する必要があります。関連ファイルは、C2RWCUST データ・セットの C2RSCRPT メンバーとして定義されます。サイト定義のスクリプト自体もこのデータ・セットのメンバーにします。

以下に、そのような関連ファイルの例を示します。

```
2.1.0
$HOMEDIR  USER   OMVS   "Create home directory"
$ROLEAB   USER   *      "Add role ab"
$SCRIPT3  GROUP  BASE   "Disable passphrase"
$ALIAS    USER   *      "Define alias to resource"
```

関連ファイルの最初の行には、関連ファイルの異なるバージョンを区別するために使用されるバージョン ID が含まれています。現行バージョンは 2.1.0 です。関連ファイル (C2RSCRPT メンバー) の 1 つのバージョンのみがサポートされます。関連ファイルの今後のバージョンには、以前のバージョンとの後方互換性があります。

後続の行は、次のフィールドから構成されます。

スクリプト名
: サイト定義のスクリプトが入っている C2RWCUST メンバーの名前。サイト定義のスクリプトと C2RWCUST の他のメンバーとを区別するために、サイト定義のスクリプトを含むメンバーに接頭部として「$」文字を付けることをお勧めします。

クラス
: USER や GROUP など、スクリプトへの入力パラメーターとして提供するクラスを表します。

セグメント
: BASE や OMVS など、スクリプトへの入力パラメーターとして提供するセグメントを表します。セグメント選択が不要である場合は、この列にアスタリスク (*) を指定します。

説明
: サイト定義のスクリプトの簡略説明。この説明は、ユーザー・インターフェース内の対応するアクション・メニュー項目およびコンテキスト・メニュー項目のテキストとして表示されます。説明は二重引用符で囲む必要があります。説明は、1 つの単語、または多くても数単語でなければなりません。50 文字より長い説明は切り捨てられます。

関連ファイルの内容では、説明フィールドを除き、大/小文字の区別はありません。

以下のサンプルでは、DFSMS AMS (アクセス方式サービス・プログラム) コマンド **DEFINE ALIAS** を使用して、指定されたキーの最初の文字の値に基づいてリソース名に別名を定義する、REXX スクリプトを示します。

```
/* REXX */
/* In case CLASS=USER, the zSecure Visual client passes a key
   and a segment to the site-defined script */
/* The segment is not employed in this script */
parse arg class segment key
if class<>'USER'
then
do
 say 'CLASS must be USER'
 return 123
end
/* Derive a 'name' value from the key */
name = key
/* Derive a 'relate' value from the key */
if substr(key,1,1)='C'
 then
 do
  relate = "ICFCAT.C1"
 end
 else
 do
  relate = "ICFCAT." || key
 end
 /* Build the 'define' argument */
 define_argument = "alias (name('" || name || "') relate('" || relate
 define_argument = define_argument || "'))"
 /* Provide some feedback for when the 'define' fails */
 say "define" define_argument
 /* Execute the 'define' command */
 address tso
 define define_argument
 /* pass TSO command return code to the Visual client; 0 = success */
 return rc
```

zSecure Visual Server の操作

Visual Server の始動

以下のコマンドを発行して、Visual Server を開始タスクとして始動できます。

```
S C2RSERVE
```

または、SCKRSAMP(C2RJSERV) のように SURROGAT 権限を使用してバッチ・ジョブを実行依頼します。どちらの方法を使用する場合でも、コマンドまたはジョブは適切なサーバー・ユーザー ID の下で実行する必要があります。

サーバーは、z/OS UNIX System Services が使用可能な場合にのみ、始動できます。自動化されたプロシージャーを使用してサーバーを始動するには、次のシステム・メッセージを受信した後でこれらのプロシージャーが実行されるようにしてください。

```
BPXI004I OMVS INITIALIZATION COMPLETE
```

このメッセージを待機しなかった場合、 171 ページの『サーバーの始動の問題』で説明する症状が発生します。

同じ IP ポートで 2 回サーバーの始動を試行すると、2 番目の始動コマンドは強制終了されます。

初期化を確認するための Visual Server ログ

次の方法のいずれかを使用して、初期化の準備ができたかどうかを確認できます。

- ISPF OBROWSE コマンドを使用して、ログ・ファイルを定期的に表示する。

  ```
  OBROWSE <ServerRoot>/log/server.log
  ```

- C2RSLOG プロシージャーを使用して、ログを JES スプール・スペースにコピーする。

  ```
  S C2RSLOG
  ```

Visual Server の停止

サーバーを停止するには、次のコマンドを実行します。

```
S C2RSTOP
```

親タスクを取り消すことで、サーバーを停止することもできます。親タスクは、該当するステップ名を持つタスクです (*OMVSEX ではありません)。

問題判別

このセクションには、次のトラブルシューティング・トピックがあります。

- 『システムの問題を解決するためのリソース』
- 170 ページの『診断情報を収集するためのコマンド』
- 171 ページの『サーバー・セットアップ (ジョブ C2RZWINI) の問題』
- 171 ページの『サーバーの始動の問題』
- 172 ページの『サーバーの応答の問題』
- 174 ページの『zSecure Admin の終了の問題』
- 174 ページの『SE.W 通信の問題』

システムの問題を解決するためのリソース

次のいずれかのリソースを使用して、システムの問題の解決に役立つ情報を見つけることができます。

- ファイル **about-server.box**。これは、run サブディレクトリーにあり、サーバー全体に関する情報を提供します。同じ情報が、クライアントでは「**Help**」メニューの「**Server information**」オプションで使用できます。

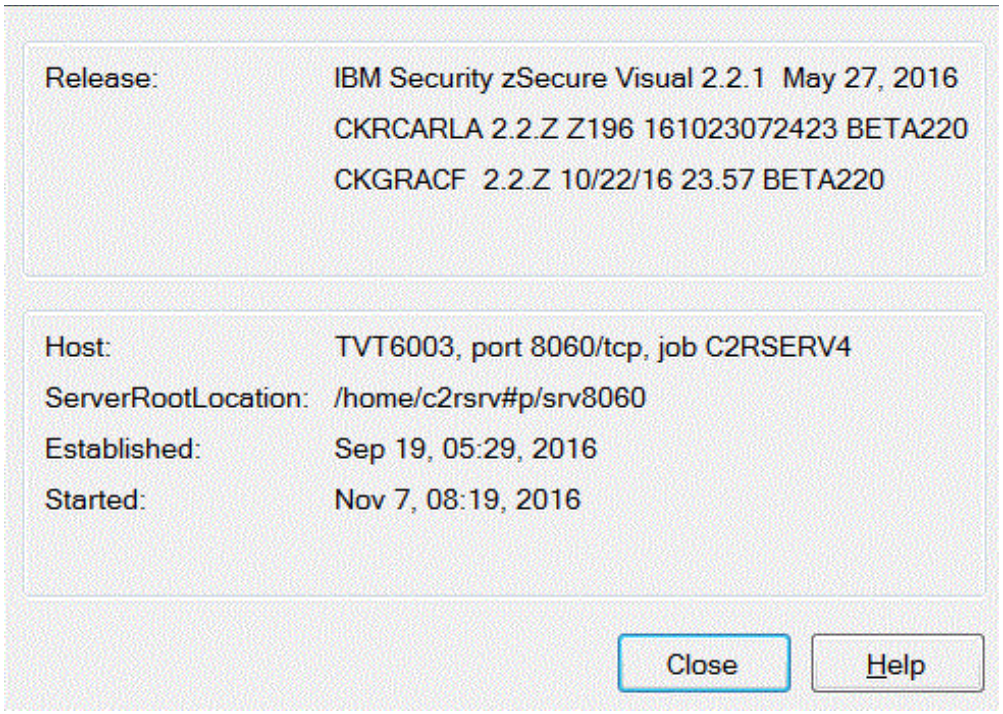


図 *9. zSecure Visual Client* の「*Server Information*」ダイアログ

上段のボックスには、サーバーが使用するソフトウェア・リリースが表示されます。上の行は、pax ファイルのリリースに対応しています。その他の 2 行は、サーバーが始動された時点での、zSecure コンポーネント CKRCARLA および CKGRACF のリリースとビルド日を示します。

注**:** サーバーがアクティブなときに、これらのコンポーネントをアップグレードしないでください。アップグレードすると、サーバーを再始動するまで、サーバー情報が表示されなくなります。

下段のボックスには、サーバー ID に関する以下の情報が表示されます。

Host サーバーのホスト名、ジョブ C2RZWINI で構成された IP ポート、およびサーバーを始動したアドレス・スペースのジョブ名。

ServerRootLocation
zSecure 構成の C2RSERVE パラメーターの (多くの場合、解決された) 値。

Established
サーバーがそれ自体を認証局として設定した時刻 (ジョブ C2RZWINI)。

Started
サーバーが最後に始動または再始動された時刻。

タイトル・バーのテキストは、**about-server.box** ファイルには含まれません。このテキストには、クライアント・サイドで、「**File**」->「**Configure**」メニューで指定された名前が含まれます。

- MVS syslog は、サーバー始動の問題に関するメッセージを提供します。さらに、セキュリティー違反に関するメッセージも、よく検出されます (ICH408I)。
- SMF は、セキュリティー違反の調査に役立ちます。また、SMF は、RACF プロファイルの AUDIT オプションに基づいて、成功したアクセスに関する情報も提供します。
- サーバー・ログは、サーバー・ルート・ディレクトリーの `log` サブディレクトリーで使用できます。このディレクトリーは、サーバーの zSecure 構成の C2RSERVE パラメーターで指定されます。サーバー・ログ・ディレクトリーも、クライアント・サイドでは、「**Help**」メニューを通じて「Server information」ボックスで識別されます。`log` サブディレクトリーの bbracf.log および server.log ファイルで、サーバーの直前の実行に関する情報が提供されます。タイプごとに、10 ログのヒストリーが保存されます。例えば、ファイル bbracf.log0 から bbracf.log9 が、サーバーの以前の実行に対応します。
- SE.W 中の問題については、TSO ユーザーのホーム・ディレクトリーを調べてください。 174 ページの『SE.W 通信の問題』を参照してください。
- クライアントが予期しない動作をした場合は、「*IBM Security zSecure Visual: クライアント・マニュアル*」を参照してください。
- 直前の CKRCARLA の実行による SYSPRINT、直前の CKGRACF の実行による CKGPRINT、および実行されたコマンドが、クライアントの通信ウィンドウで参照できます。

診断情報を収集するためのコマンド

c2rdiag コマンドは、zSecure Visual Server が実行中かどうかにかかわらず、いつでも実行できます。収集された情報は、ダンプ・ファイル **C2Rdiag_dump_*xxxx*.tar** に保管されます。ここで、*xxxx* はタイム・スタンプを表します。ダンプ・ファイルは、トラブルシューティングの目的で、IBM ソフトウェア・サポートに転送できます。

c2rdiag コマンドは、診断情報を収集するためにシステムのすべてのアクティブ・プロセスに関する情報を必要とするため、ルート権限を持つユーザー ID (uid=0) の下で実行する必要があります。ルート権限の下で実行すると、以下に示す必要な権限が付与されます。

- zSecure 構成ファイルの C2RSERVE パラメーターで識別される *<Server Root>* ディレクトリーへの READ および WRITE 権限。
- zSecure 構成ファイルの C2RWIN パラメーターで識別される zSecure Visual Server ソフトウェア・ディレクトリーへの READ および EXECUTE 権限。

トラブルシューティングのための診断情報の収集と IBM への送信手順

診断情報を収集して、ダンプ・ファイルを IBM に送信するには、次のステップを実行します。

注: システム・ログ出力 (SDSF) は、**c2rdiag** コマンドでは取り込まれません。この情報が関係あると考えられる場合は、疑わしいイベントが発生した前後のシステム・ログを抽出して、提供してください。

1. ルート権限を持つユーザー ID でシステムにログオンします。
2. OMVS コマンド・シェルを開き、*<Server Root>* ディレクトリーに移動します。
3. コマンド `./bin/c2rdiag` を実行します。
4. バイナリー・モードを使用して、ダンプ・ファイル **C2Rdiag_dump_***xxxx***.tar** を IBM に送信します。
5. IBM がファイルの受信を確認したら、ディスク・スペースの不足を防ぐために、ダンプ・ファイルを削除します。root がファイルを所有しているため、zSecure Visual Server はこれらのファイルを削除できません。

サーバー・セットアップ (ジョブ C2RZWINI) の問題

サーバーのセットアップ時に、次のエラー・メッセージが表示されることがあります。

FSUM2078

このメッセージは、サーバー・ユーザー ID のホーム・ディレクトリーを作成しなかった場合に、送出されることがあります。

FOM0303I rsn=0924041A

次のメッセージは、FACILITY リソース BPX.FILEATTR.APF への READ アクセス権限がないことを示しています。

```
FOMF0303I CKGRACF: chattr() error: rv=-1, errno=8B, rsn=0924041A
```

FOM0303I rsn=0924041B

次のメッセージは、FACILITY リソース BPX.FILEATTR.PROGCTL への READ アクセス権限がないことを示しています。

```
FOMF0303I ./bin/bbmini: chattr() error: rv=-1, errno=8B, rsn=0924041B
```

サーバーの始動の問題

サーバーの始動時に問題が発生すると、C2RW メッセージが表示されます。「*IBM Security zSecure:* メッセージ・ガイド」に、これらのメッセージの説明があります。次の始動時の問題では、C2RW エラー・メッセージは表示されません。

- z/OS UNIX System Services 初期化が完了する前にサーバーの始動を試行した場合 (IPL 後、早すぎた場合)、メッセージ ICH408I が表示されます。

  ```
  ICH408I USER(C2RSERVE) GROUP(C2R) NAME(ZSECURE VISUAL SERVR)
    CL(FSOBJ   )
    INSUFFICIENT AUTHORITY TO DUB
  ```

  タスクは実行されますが、z/OS UNIX System Services プロセスとしては実行されないため、意味がありません。このメッセージを受け取った場合は、次のようにします。

  1. タスクを取り消します。
  2. 167 ページの『Visual Server の始動』で説明されているように、BPX1004I メッセージを待機します。
  3. タスクを再度開始します。

- ポート番号を使用できないときにサーバーの実行を試行した場合、次のエラー・メッセージが表示されます。

  ```
  TCPIP Conn: can't bind to socket (errno 111)
  ```

  この場合、PROFILE.TCPIP データ・セットのパラメーターを使用して、サーバーが使用する TCP/IP ポート番号を予約した可能性があります。次のようなコマンドが考えられます。

  ```
  PORT xxxx TCP C2RSERVE NOAUTOLOG
  ```

  または

  ```
  PORTRANGE xxxx yy TCP C2RSERVE NOAUTOLOG
  ```

  この場合、C2RSERVE ジョブ名が、ポートをオープンできる唯一の ID になります。そのため、インストール・ステップが異なるジョブ名で実行された場合、「bind() errno=111」メッセージを受け取ります。

  この問題を避けるために、TCP/IP ポートの保護は、ジョブ名ではなくユーザー ID に基づきます。 147 ページの『TCP/IP セキュリティー』を参照してください。
- TCP/IP がまだ始動していないときにサーバーの実行を試行した場合、次のエラー・メッセージが表示されます。

  ```
  S8E220:TCPIP Conn: Socket error 112
  ```

  この場合、TCP/IP に問題があるか、TCP/IP が全くアクティブになっていない可能性があります。

サーバーは、zSecure Admin を正常に実行できないと、サーバー自体を異常終了させます。例えば、CKGRACF および CKRCARLA のプログラム制御化に失敗すると (141 ページの『インストール要件』を参照してください)、次のようなメッセージが表示されることがあります。

```
ICH420I  PROGRAM CKGRACF FROM LIBRARY CKR.SCKRLOAD
         CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED.
BPXP014I ENVIRONMENT MUST BE CONTROLLED FOR
         SERVER (BPX.SERVER) PROCESSING.
```

このメッセージと共に、ダンプ・ファイル (CEEDUMP.timestamp) が run ディレクトリーに作成されることがあります。この理由で書き込まれるダンプは、破棄してかまいません。

サーバーの応答の問題

サーバーが応答しない場合、まず、サーバーが待機中か、処理の実行に CPU 時間を費やしているかどうかを判別します。 SDSF DA で、この例を表示できます。サーバーは通常、SDSF の 3 つのアドレス・スペースとして表示されます (アイドリング時)。応答しない原因として考えられる原因には、以下があります。

- クライアントが間違ったポート番号またはマシン名を使用している。少なくともアクティブかどうかを検査するためのテスト接続ボタンがクライアントにあります。TSO の下で **netstat** コマンドを使用すると、サーバーが listen しているポートを表示できます。
- サーバー・ログに多数のメッセージが表示される。

```
E10:Crypt: Protocol violation. message from 12.1.4 and no secure channel
E18:Crypt: Unexpected message from 12.1.4 suspicious, so discarded
```

これらのメッセージの原因として可能性が高いのは、クライアント・エージェントの実行中に、サーバー・エージェントが停止して再開したことが考えられます。負荷が軽い 30 MIPS のマシンでは、クライアントは 6 分以内にサーバーに接続でき、クライアントによる再送信によって 6 つの E10/E18 メッセージ・ペアがサーバー・ログに出力されます。より早く復旧させるには、Windows タスク・マネージャの「プロセスの終了」ボタンを使用して **c2ragent.exe** タスクを終了し、IBM Security zSecure Visual アプリケーションを閉じてから再開します。

別の原因として、クライアントを構成した直後にログオンを試行したことが考えられます。その場合、セキュア・チャネルのセットアップがまだ完全でないため、サーバー・サイドで単一の E10/E18 メッセージ・ペアが出力される可能性があります。この場合の復旧にかかる時間は、高速マシンではわずかに 1 分です。ただし、クライアント構成の後、15 秒 (高速マシンの場合) 待ってログオンを試行すれば、この遅延を避けることができます。トレース・モードでは、ログオンを受け付ける準備ができると、サーバーは次のメッセージを表示します。

```
E0:CA: Finished certifying Agent Keys
```

- サーバー・ログに、次の再接続メッセージが表示される。

  ```
  E183:Route: reconnected from 12.1.4
  ```

  このメッセージは、同一のエージェント ID を持つ 2 つのクライアントがサーバーとの通信を試行していることを示しています。いずれかの **c2ragent.exe** プロセスを Windows タスク・マネージャで停止します。ほとんどの場合、プロセスは単一のコンピューターにありますが、別々のコンピューターにある場合もあります。
- サーバー・ログに、次のメッセージが表示される。

  ```
  E160:LCM: There are no valid LCM certificates. Please reconfigure the server
  ```

  最も考えられる原因として、サーバー初期化 (ジョブ C2RZWINI) が正常に実行されていません。低い可能性として、サーバーが直前の 9 カ月に実行されておらず、証明書が期間内にリフレッシュされなかったことが考えられます。サーバーを停止して、ジョブ C2RZWINI を実行または再実行し、サーバーが認証局として正常に初期化されたことを検査します。 148 ページの『サーバーの初めての始動』を参照してください。

これらの項目のどれも当てはまらず、問題が再現可能な場合は、TRACE オプションを指定してサーバーを始動できます。

```
S C2RSERVE,OPT=TRACE
```

TRACE オプションを使用すると、詳細な時間情報を含む大きなサーバー・ログが生成されます。この問題のデバッグに関して IBM ソフトウェア・サポートの支援を受ける場合は、クライアント・ログとサーバー・ログの両方を送信してください。

zSecure Admin の終了の問題

zSecure Visual クライアントのログオン後、ユーザーの権限に合わせて GUI を調整し、クラス記述子テーブルをダウンロードするために、いくつかの zSecure Admin トランザクションが実行されます。これらのアクションが失敗し、次のエラー・メッセージのいずれかが表示されることがあります。

- `CKR0010 OPEN abend hhh-hh on file ddname`

  表示されたファイルのオープンに失敗しました。ddname フィールドが空、または不要情報であることがあります。また、ユーザーが、RACF データベースに対する READ 以上のアクセス権限を持っていることを確認します。

- `CKR999I GETMAIN FAILED FOR HEAP name - INCREASE REGION`

  CKRCARLA プログラムが、USS で割り振られた仮想ストレージよりも多くの仮想ストレージを要求したときに、CKR999I または CKR0999 で終了しました。この問題を解決するには、次のようにします。

  1. サーバーのユーザー ID に許可される仮想ストレージの最大サイズを増やします。次の例で示すように、サーバーの OMVS セグメントの ASSIZEMAX 値をバイト単位で指定します。

     ```
     ALTUSER C2RSERVE OMVS(ASSIZEMAX(64000000))
     ```

  2. サーバーを再始動して、この変更を有効にします。

この問題に関する追加情報について、MVS システム・ログでセキュリティー違反メッセージを調べることもできます。

SE.W 通信の問題

SE.W 通信は、REXX C2RELSI プログラムで処理されます。このプログラムは、ユーザーのホーム・ディレクトリーに 4 つのファイルを作成します。

C2RELSI.userid.LST
: 公式の応答ファイル。このファイルには、通常、生成されたインストール・パスワードが含まれています。パスワードは通常、次の例で示すような、10 桁の 16 進数字が 1 行だけです。

  ```
  8337F93AD5
  ```

C2RELSI.userid.ERR
: ライン・モード出力ファイル。通常、ユーザー ID とパスワードのプロンプトだけが含まれています。

  ```
  userid:password:
  ```

C2RELSI.userid.LSI
: サーバー用のコマンドを含む入力ファイル。**P** コマンドの場合、入力ファイルには、次の記述が含まれています。

  ```
  minigenerateinstallpassword(12.1.100)
  echo(!R:)
  ```

C2RELSI.userid.LOG
: ソフトウェア・ログ・ファイル。通常、次の例で示すようなソフトウェア・レベルとオープン/クローズ・メッセージだけが含まれています。

```
<20010427 08:11:27 utc> P399M1V0.0L309A5S0E10:Opened C2RELSI.MYUSER.LOG.
Product: racfwin.product.server.app. Version: 1.4.
Builddate: 2001/04/23/13:02. Local time: Fri Apr 27 08:11:27 2001.
<20010427 08:11:28 utc> P399M1V0.0L164A2S0E20:Forced close of C2RELSI.MYUSER.LOG
<20010427 08:11:28 utc> P399M1V0.0L461A5S0E15:Closed C2RELSI.MYUSER.LOG
```

SE.W 通信プロセスのさまざまな段階で、次のエラー・メッセージが表示されることがあります。

Failure to execute

REXX C2RELSI がプログラム lsi を検出できない場合、または現行ユーザーによる実行が許可されていない場合、画面の右上にメッセージ「Failure to execute」が表示されます。PF1 (Help) を押すと、次の例で示すような、エラーの原因を説明する長いメッセージが表示されます。

```
/u/C2RSERVE/c2rserve/bin/lsi -t C2RELSI.MYUSER.LOG A:10.0.1.20:8011 C2RELSI.MYUSER.LSI - errno=81 53B006C
```

長いメッセージでは、その問題に関する情報を提供するエラー番号 (*errno*) が示されます。考えられるエラー・メッセージ、および関連する説明は、次のとおりです。

errno=81 594003D

このエラーは、**lsi** 実行可能ファイルのパスに含まれるいずれかのディレクトリーが検出されない場合に発生します。パスは、zSecure 構成の C2RWIN パラメーターで指定されます。問題を修正するには、パスが z/OS UNIX System Services zFS ファイル・システムに存在し、ジョブ C2RZWUNP でこのパスが使用されていることを確認します。

注: C2RWIN パラメーターには大/小文字の区別があります。

errno=81 53B006C

このエラーは、zSecure Visual プログラムのいずれかの場所が検出されない場合に発生します。問題を修正するには、パスが z/OS UNIX System Services zFS ファイル・システムに存在し、ジョブ C2RZWUNP でこのパスが使用されていることを確認します。

errno=6F 5B400002

このエラーは、現行ユーザーに、**lsi** 実行可能ファイルのパスに含まれるディレクトリーへの検索権限がない場合に発生します。この問題は、SYSLOG にもアクセス違反として表示されます。

```
ICH408I USER(MYUSER ) GROUP(MYGROUP ) NAME(VISUAL RACF ADMIN  )
/usr/lpp/c2r/V2R2M1/lsi
CL(DIRSRCH ) FID(01E2D4E2F0F0F833F409000000000003)
INSUFFICIENT AUTHORITY TO LOOKUP
ACCESS INTENT(--X)  ACCESS ALLOWED(OTHER ---)
```

問題を修正するには、SE.W を実行するユーザーに、zSecure Visual サーバー・コードがあるディレクトリーへのアクセス権限を付与します。ジョブ C2RZWUNP で、このディレクトリーの所有権がユーザー C2RUSER およびグループ C2RGROUP として設定されます (カスタマイズされていることがあります)。SE.W を実行するユーザー ID を所有グループに接続します。SE.W は、最初の

ワークステーションの構成にのみ必要であることに注意してください。後続のワークステーションは、このワークステーションを使用して構成できます。

Cannot browse an empty file

この ISPF エラー・メッセージによって、**lsi** の実行に失敗したことを報告する元のエラー・メッセージが隠されることがあります。このメッセージは、zSecure Visual サーバーがまだ実行されていない場合に表示されることがあります。

an error has occurred

パスワード生成が失敗した場合、画面の右上にこのメッセージが表示され、次のいずれかのより説明的なエラー・メッセージが表示されます。

couldn't open session with bluebook adapter

この説明的なメッセージは、サーバーが始動していないか、始動しているがパスワード生成要求を受け付ける準備ができていないことを示します。

サーバーが始動したばかりの場合、通常、負荷が軽い 30 MIPS のマシンで約 10 秒後にパスワード生成の準備ができます。数分遅らせた後で同じエラー・メッセージが表示される場合、サーバーが到達不可か、IP 番号が不正である可能性があります。

logon failed

このメッセージは、サーバーがパスワード要求を受け付けたが、パスワード生成の準備ができていない場合に表示されます。この問題を解決するには、失敗メッセージが表示された後、再度パスワード生成要求を試行する前に数秒待ちます (30 MIPS マシンの場合)。サーバーでパスワード生成の準備ができると、次のメッセージがサーバー・ログに表示されます。

```
E5:Dispatch: Started adapter 'RACF'
```

サーバーがトレース・モードで実行されている場合、次のトレース・メッセージが 2 回出力されたときに、パスワード生成の準備ができます。

```
E0: IpcSetState:setting state ( 6 -> 1 )
```

Must be numeric

このメッセージは、12.1.<*NN*> (<*NN*> は 10 進数字のシーケンス) 以外の形式でエージェント ID を入力したときに表示されます。この問題を修正するには、正しい形式 (12.1.100 など) でエージェント ID を入力します。

ユーザー **ID** およびパスワードのメッセージ

- Unknown userid <userid>.
- Userid <userid> is revoked.
- Invalid password.
- The password has expired.

Resource C2R.SERVER.ADMIN in the <class> class is not covered by a RACF profile.

このエラーが発生した場合は、JES SYSLOG に次のメッセージが表示されます。

```
ICH13003I C2R.SERVER.ADMIN NOT FOUND
```

EDC5139I Operation not permitted. Reason code: 00d8.

このメッセージと理由コードは、サーバー・ユーザー ID に FACILITY リソース BPX.SERVER への READ アクセス権限がないことを示しています。このエラーが発生した場合は、JES SYSLOG に次のメッセージが表示されます。

```
ICH408I USER(C2RSERVE)
  BPX.SERVER CL(FACILITY)
  INSUFFICIENT ACCESS AUTHORITY
  ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
```

EDC5139I Operation not permitted. Reason code: 02af.

このメッセージと理由コードは、Visual サーバーの制御下で実行されるモジュールのいずれかが、プログラム制御の要件を満たしていないためロードできないことを示します。 Visual サーバーのプログラム制御をセットアップする方法については、 141 ページの『インストール要件』を参照してください。

また、障害が発生した頃に生じたメッセージについて SDSF syslog を検索してください。例えば、以下のようなメッセージが存在することがあります。

```
ICH420I PROGRAM CKRCARLA FROM LIBRARY CKR.SCKRLOAD CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED.
ICH422I THE ENVIRONMENT CANNOT BECOME UNCONTROLLED.
BPXP014I ENVIRONMENT MUST REMAIN CONTROLLED FOR DAEMON (BPX.DAEMON) PROCESSING.
CSV042I REQUESTED MODULE CKRCARLA NOT ACCESSED. THE MODULE IS NOT PROGRAM CONTROLLED
```

特に、メッセージ ICH420I および CSV042I は、要件を満たしていないモジュールを識別します。そのモジュールをカバーする PROGRAM プロファイルを見つけ、そのモジュールのロード元のデータ・セットを見つけ、そのデータ・セットが、関連する PROGRAM プロファイルのメンバーであることを確認します。

C2RW018I The resource class for zSecure security checks cannot be determined

CKRSITE モジュールに、有効なセキュリティー・クラスが含まれていません。これらのクラスは、さまざまなリソースへのユーザーのアクセス権限を判別するために必要です。CKRSITE モジュールについては、 205 ページの『付録 A. サイト・モジュール』を参照してください。

<userid> has no READ access to C2R.SERVER.ADMIN resource in the <class> class.

このメッセージは、ユーザー ID が C2R.SERVER.ADMIN リソースに対する READ 以上のアクセス権限を持たないことを示しています。JES SYSLOG に次のメッセージが表示されます。

```
ICH408I USER(ABCDEFG)
  C2R.SERVER.ADMIN CL(FACILITY)
  INSUFFICIENT ACCESS AUTHORITY
  ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
```

The environment does not satisfy the requirements for program control.

必要なモジュールがプログラム制御されていません。Visual Server アドレス・スペースにロードされるすべてのロード・モジュール (およびプログラム・オブジェクト) は、プログラム制御される必要があります。また、Visual Server ソフトウェアを含むファイル・システムは、SECURITY 属性および SETUID 属性を付けてマウントする必要があります。制御されていないモジュールは、MVS syslog のメッセージ CSV0421I から識別できます。 141 ページの『インストール要件』および 145 ページの『ソフトウェアの所有者と場所の準備』を参照してください。プログラム制御を確立した後で、サーバーを再始動する必要があります。

The agent has not been added with A or AP.

このメッセージは、構成されていないクライアントのパスワードの生成を試行したことを示します。パスワードは生成されていません。 152 ページの『Visual クライアントの構成』で説明されているように、クライアントを追加します。

第 14 章 変更トラッキングのセットアップ

トラック変更システムは、システム・パラメーターおよびセキュリティー設定における変更を検査済みベースに照らしてモニターする特殊機能です。変更は ISPF インターフェースにより選択して承認、拒否、または据え置くことができます。

トラック変更は単一システム・イメージに対して実行することも、複数のイメージを単一のビューに結合して一元化されたトラック変更管理を行うこともできます。

変更トラッキングに必要なデータ・セット

表 17 に、トラック変更を実行するために必要なデータ・セットをリストします。

表 17. トラック変更に必要なデータ・セット

短縮名	**ISPF** アクセス	バッチ・アクセス	フルネーム	**Remarks**
構成ファイル	READ	READ	36 ページの『構成の割り当て』を参照してください。	モニター対象のシステム・イメージごとに、別々の構成ファイルが必要です。これらの構成ファイルはすべて、同一の DPREF パラメーターを持っている必要があります。通常、モニター対象となるシステム・イメージ間で異なる唯一のパラメーターは SYS です。これらの構成ファイルはすべて、トラック変更ジョブの JCLLIB ステートメントの中に含まれている単一の区分データ・セットの中になければなりません。デフォルトでは、この PDS は CKR.CKRPARM です。
マスター・ファイル	READ (UPDATE)	UPDATE	&DPREF..CT.CKACDATE	ISPF からの UPDATE は、システムを CT 管理から除去するためだけに必要とされます。
ローカル・セットアップ・テーブル	READ (UPDATE)	READ	&DPREF..CT.CKACTAB	ISPF トランザクション・セットアップ・トラック変更 (SE.C) により更新されます。
検査済みベース	UPDATE	READ (UPDATE)	&DPREF..CT.&SYS..CKAVERIF	モニター対象のシステム・イメージごとに、別々の検査済みベースが必要です。初回実行時のみ、バッチ処理がこのデータ・セットを更新します。
例外ファイル	UPDATE	UPDATE	&DPREF..CT.CKAEXCEP	

表 17. トラック変更に必要なデータ・セット (続き)

短縮名	**ISPF** アクセス	バッチ・アクセス	フルネーム	**Remarks**
据え置きファイル	UPDATE	-	&DPREF..CT.CKADEFER	
入力	-	READ	&DPREF..&SYS..CKFREEZE &DPREF..&SYS..UNLOAD	モニター対象のシステム・イメージごとに、定期的にリフレッシュされた CKFREEZE と UNLOAD が必要です。
中間ファイル	-	CREATE DELETE	&DPREF..CT.&SYS..CKATSYSI &DPREF..CT.&SYS..CKATCOMP &DPREF..CT.&SYS..CKATPRIN &DPREF..CT.&SYS..CKATEXCP &DPREF..CT.&SYS..CKATREPP &DPREF..CT.&SYS..CKATREPS &DPREF..CT.&SYS..CKATSIMS &DPREF..CT.&SYS..CKATSYSD	補足情報については、ジョブ CKAJTSYS の詳細を参照してください。ジョブ CKAJTSYS を参照してください。

マスター・ファイル、例外ファイル、据え置きファイル、およびローカル・セットアップ・テーブルを、ジョブ CKAJTCT1 がデータ・セット CKRJOBS にある状態で作成します。

複数のシステム・イメージをモニターするときも、必要とされるのはこれらデータ・セットのいずれか 1 つのみです。 179 ページの表 17 で説明されている構成のいずれかを使用するには、このジョブの JCLLIB ステートメントと INCLUDE ステートメントを調整します。

検査済みベースは、ジョブ CKAJTCT2 を使用して生成されます。モニター対象のシステム・イメージごとに、別々の検査済みベースが必要です。モニター対象のシステム・イメージの構成のすべてに使用するには、JCLLIB ステートメントと INCLUDE ステートメントを調整します。つまり、ジョブ CKAJTCT2 を、構成ごとに 1 回実行することになります。

トラック変更ジョブおよび ISPF コンポーネントの意図するユーザーが、これらのデータ・セットに必要なアクセス権限を持つような形で、トラック変更セキュリティー環境をセットアップします。適切なアクセスをセットアップするための JCL の例は、CKAJTCT3 ジョブを参照してください。作成するセキュリティー・リソースはすべてユーザーのセキュリティー・ポリシー (総称プロファイルにするか個別プロファイルにするかの選択など) に必ず従うようにしてください。

日次バッチ・スイートのセットアップ

トラック変更は、そのデータ・セットを以下のように使用します。

- バッチでは、定期的にリフレッシュされる CKFREEZE データ・セットと UNLOAD データ・セットが検査済みベースに照らして検査されます。
- 変更は、ISPF インターフェース (AU.C) で選択可能です。変更を、選択して承認することができます。承認された変更は、検査済みベースに追加されます。ただし、変更は拒否または据え置きされることもあります。

簡単に説明するために、すべてのトラック変更プロセスが単一の z/OS イメージのもとで実行されていると仮定します。フレッシュな CKFREEZE データ・セットと UNLOAD データ・セットは、このイメージからアクセス可能でなければなりません。ただし、CKFREEZE データ・セットの作成は、イメージ自体の内部からしか行えません。所定の位置に共有 DASD がない場合は、いずれかの転送方法 (テープ、NJE、FTP) を使用して、トラック変更が CKFREEZE データ・セットを使用できるように設定できます。ただし、これは転送方法に LRECL=X が保持されており、長いレコードを切り捨てまたはラップしていない場合に限ります。FTP を使用する場合、 EBCDIC オプションと BLOCK オプションの両方を使用する必要があります。

同様に、UNLOAD データ・セットは、セキュリティー・データベースへのアクセス権限を持つどのシステム・イメージからも作成できます。しかし、最良の結果を得るには、そのデータ・セットを使用する最高レベルのイメージでその作成を行ってください。 UNLOAD データ・セットは、 CKFREEZE データ・セットを転送するのと同じ方法で転送できます。

CKFREEZE データ・セットと UNLOAD データ・セットの作成方法について詳しくは、 55 ページの『フレッシュな CKFREEZE および UNLOAD の毎日の使用』を参照してください。

共有セキュリティー・データベースの場合、通常は単一の UNLOAD データ・セットのみが作成されます。ただし、トラック変更ジョブでは、そのデータ・セット名に &DPREF..&SYS..UNLOAD を想定しています。これは、システム・イメージごとに異なります。しかし、同じデータベースで複数の UNLOAD データ・セットを作成する必要はありません。その代わりに、IEBGENER のようなプログラムを使用して UNLOAD をコピーするか、単に別名を作成する方法があります。例えば、イメージ IPO1 と IPO2 がセキュリティー・データベースを共有しており、イメージ IPO1 でジョブ C2RJPREP を使用して UNLOAD を作成した場合、以下のようにして、別名を作成することができます。

```
DEFINE ALIAS (NAME('yourprefix.IPO2.UNLOAD') RELATE('yourprefix.IPO1.UNLOAD'))
```

トラック変更バッチ・スイートは、以下から構成されます。

- ジョブ CKAJTSYS。 CKACTSYS プロシージャーを呼び出し、マスター・ファイルと例外ファイルを更新します。このジョブは、モニター対象のシステム・イメージごとに 1 回 (順次) 実行します。このジョブは、モニター対象のシステム・イメージとは別のシステム・イメージで実行できます。リフレッシュされた CKFREEZE データ・セットと UNLOAD データ・セットが使用可能になるまでは、CKACTSYS を実行しないでください。つまり、これらのデータ・セットは、作成またはリフレッシュされ、必要に応じて、トラック変更ジョブが実行される場所であるシステム・イメージに転送されます。

  処理する予定のデータを持つイメージの構成を使用するように、このジョブの JCLLIB ステートメントと INCLUDE ステートメントを調整します。さらに、トラック変更によって特定のイメージが初めて処理されるときは、INIT#CT パラメーターを EQ に設定します。この設定を行うと、構成全体が検査済みベースに直ちにプロモートされて、構成全体が例外としてシグナル通知されなくなります。初回実行後に、INIT#CT の設定を NE に戻します。

ジョブ CKAJTSYS は、必要に応じて中間データ・セットを作成します。中間データ・セットについて詳しくは、 179 ページの表 17を参照してください。中間データ・セットは、通常、ジョブが完了した後に削除されますが、診断目的で保持しておくこともできます。これらを保持するには、プロシージャー CKACTSYS を開始するときに、TREMOVE=NE オプションを使用します。

- ジョブ CKAJTSRT は CKACTSRT プロシージャーを呼び出して、例外ファイルから重複を削除します。ジョブまたはシステムの障害が発生したときに、ジョブを再実行した結果として、重複情報を追加することができます。このジョブはすべての CKAJTSYS ジョブの終了後に実行して、例外ファイルから必ず重複情報が削除されるようにします。

  モニター対象のいずれかのシステムの構成を使用するには、このジョブの JCLLIB ステートメントと INCLUDE ステートメントを更新します。
- ジョブ CKAJTM は、CKACTPRT プロシージャーと CKACTM プロシージャーを呼び出します。このジョブは、トラック変更例外ファイルの印刷可能なレポートを生成して、このレポートを E メールのメモとして送信します。このジョブは、オプションでジョブ CKAJTSRT の後に実行するようにスケジュールすることができます。

  モニター対象のいずれかのシステムの構成を使用するには、このジョブの JCLLIB ステートメントと INCLUDE ステートメントを更新します。また、このジョブには、意図する E メール受信者の E メール・アドレスも追加する必要があります。

  プロシージャー CKACTPRT と CKACTM は、別々に使用できます。例えば、レポートを E メール送信するのではなく印刷するには、パラメーター RPTTYPE を SPOOL に設定して CKACTPRT ジョブを開始します。結合されたジョブ CKAJTM では、CKACTM が E メール送信のための入力としてファイルを必要とするため、この値は RPTTYPE=FILE で指定変更されます。

これらのジョブすべてについて、SCKRSAMP データ・セットでは直接更新しないことが想定されています。なぜなら、そのデータ・セットを直接更新することは、配布指向インストールの規則に違反するからです。その代わりに、必要なジョブをユーザーが自分のデータ・セット (ユーザーのスケジューリング・ソフトウェア用のジョブが入っており、ユーザーのローカル・コピーを更新するデータ・セットなど) にコピーすることが想定されています。

プロシージャー CKACTSYS は、プロシージャー CKAC を呼び出します。その結果、SCKRPROC のメンバー C2RI* が、 UNLOAD ファイルと CKFREEZE ファイルを割り振るために使用されます。z/OS は、ネストされたプロシージャーでは DD ステートメントの指定変更を許可しないため、ご使用の命名規則が C2RI* メンバーに適合しない場合、CKACTSYS を使用することはできません。この場合、独自の CKAC 呼び出しをコーディングする必要があります。

トラック変更スイートは順次実行しなければならないため、これらを単一のジョブに結合することがあります。例えば、モニター対象のイメージ IPO1、IPO2、および IPO3 でトラック変更を実行する場合、ジョブ CKAJTSYS および CKAJTSRT を以下のようにして結合することができます。

```
//JCLLIB   JCLLIB ORDER=(your.prefix.CKRPARM,
//         CKR.SCKRPROC)
//*
//*  Process input from systems IPO1, IPO2 and IPO3. Each of
//*  these needs to run under its own configuration.
// EXEC CKACTSYS,INIT#CT=NE,CONFIG=CFG#IPO1
// EXEC CKACTSYS,INIT#CT=NE,CONFIG=CFG#IPO2
// EXEC CKACTSYS,INIT#CT=NE,CONFIG=CFG#IPO3
//*
//*  Remove duplicates. This runs only once, under any of
//*  the above configurations.
// EXEC CKACTSRT,CONFIG=CFG#IPO1
```

ISPF インターフェースを使用した変更トラッキング

トラック変更用 ISPF インターフェースは、以下のパネル・オプションから構成されています。

AU.C シグナル通知された変更を検査して、以下のフォローアップ・アクションを実施します。このタスクの説明は、ユーザー・リファレンス・マニュアル にあります。このタスクにアクセスするには、ユーザーは XFACILIT リソース CKR.OPTION.AU.C に READ 権限を持っていなければなりません。別のリソース・クラスの使用について詳しくは、 205 ページの『付録 A. サイト・モジュール』を参照してください。

AU.C のユーザーも、CKR.ACTION.CH.* (例外概要に対するアクションの場合) および CKR.ACTION.CT.* (システム概要に対するアクションの場合) で対象とされるリソースへの READ 権限を必要とします。 207 ページの『どのオプションが表示されるかを構成するリソース』を参照してください。

SE.C ジョブ CKAJTSYS が使用するテーブル (機密とみなしたデータ・セットなど) を維持します。デフォルトでは、トラック変更は、機密データ・セットを CARLa REPORT SENSITIVE と同じデータ・セットとみなします。このタスクの説明は、ユーザー・リファレンス・マニュアル にあります。このタスクにアクセスするには、ユーザーは XFACILIT リソース CKR.OPTION.SE.C に READ 権限を持っていなければなりません。別のリソース・クラスの使用について詳しくは、 205 ページの『付録 A. サイト・モジュール』を参照してください。

ジョブ CKAJTCT3 は、このための RACF プロファイルのセットアップ例を提供しています。ただし、作成するセキュリティー・リソースは、ユーザーのセキュリティー・ポリシー (総称プロファイルにするか個別プロファイルにするかの選択など) に必ず従うようにしてください。

トラック変更に ISPF インターフェースを使用するには、適切な DPREF パラメーターを持った構成が必要です。例えば、ジョブ CKAJTSYS によって使用される構成はいずれも使用することができます。

外部変更管理システムに対するトラック変更インターフェース

変更が拒否、据え置き、または確認されるたびに、REXX CKAECHGM プログラムが呼び出されます。この REXX プログラムは、IBM Information Management などの外部変更管理システムに対するトラック変更インターフェースです。デフォルトでは、検査は行われません。このインターフェースは、インストールによって提供される必要があります。この出口点は、変更管理番号を検証するように設計されています。

第 15 章 QRadar SIEM 用データの準備

zSecure を使用すると、z/OS イベント・データを QRadar SIEM で使用可能にできます。

QRadar SIEM の場合、z/OS イメージには、z/OS 自体の、および RACF、ACF2、または Top Secret の複数のログ・ソースが含まれます。さらに、DB2 および CICS が z/OS イメージでアクティブな場合、それら製品のログ・ソースもイメージに含まれます。z/OS イメージ上では、QRadar で必要な Log Event Enhanced Format (LEEF) に、SMF レコードを変換する zSecure プロセスをセットアップする必要があります。

「フル」に強化された SMF フィードに対して 2 つの操作モードがあります。ニア・リアルタイム・モード (UNIX syslog プロトコルを使用して送信) と、FTP ファイル・ポーリングによるモードです。ニア・リアルタイムは、QRadar ダッシュボードを使用すると処理が向上しますが、ピーク期間中はより多くのオーバーヘッドも発生します。FTP ファイル・ポーリングを使用すると、比較的ビジーでない時間に処理を延期できます。ファイル・ポーリング・モードでは、QRadar SIEM の Device Support Modules (DSM) が QRadar コンソールで構成されているスケジュールに従って、これらの LEEF ファイルを取得します。ニア・リアルタイム・モードの場合は、syslog トラフィックを受け入れるように DSM を構成する必要があります。「フル」のニア・リアルタイム SMF フィードは、zSecure によって 2 つの方法で収集できます。SMF INMEM 機能を使用して直接収集する方法と、IBM Common Data Provider for z Systems (CDP) の System Data Engine (SDE) を介して収集する方法です。

zSecure Alert によって生成されたアラートは、QRadar SIEM に送信することもできます。このアラートは、SMF または他のソースに基づくことができます (例えば、システム変更の検出に基づくことができます)。アラートはニア・リアルタイムで QRadar SIEM に転送され、構成されているどのスケジュールにも依存しません。zSecure Alert では、UNIX syslog フォーマットを指定し、受信側として QRadar SIEM を指定します。zSecure Alert について詳しくは、「*IBM Security zSecure Alert:* ユーザー・リファレンス・マニュアル」を参照してください。

前提条件

ソフトウェアをインストールした後も、アクティビティーを実行して、構成の作成および変更を行う必要があります。以下の基準が満たされている必要があります。

- いくつかの zSecure コンポーネントを使用不可にするために PARMLIB メンバー IFAPRD*xx* を使用する場合は、zSecure Adapters for QRadar SIEM または zSecure Audit が使用不可に設定されていてはなりません。詳しくは、 24 ページの『ライセンス機能の使用可能化』を参照してください。
- SCKRLOAD ライブラリーには、APF 許可が必要です。詳しくは、 24 ページの『ソフトウェアの APF 許可』を参照してください。

- 直接の SMF INMEM リアルタイム・インターフェースを使用することに決めた場合は、必要なソフトウェアをインストールし (APAR OA49263)、SMFPRM*xx* メンバーをセットアップして、INMEM キーワードおよびパラメーターを含めるようにしておく必要があります。詳しくは、 188 ページの『ニア・リアルタイムのプロシージャー』を参照してください。CDP インターフェースを使用することに決めた場合は、CDP もインストールして稼働させておく必要があります。

  両方のリアルタイム・インターフェースで、QRadar SIEM を更新して z/OS 関連 DSM の syslog 入力を許可することが必要になる場合があります。
- CKFREEZE データ・セットおよび UNLOAD データ・セットを定期的にリフレッシュするプロセスをセットアップする必要があります。 55 ページの『フレッシュな CKFREEZE および UNLOAD の毎日の使用』を参照してください。UNLOAD を使用できるのは、QRADAR* 以外のライセンス (AUDIT* や ADMINRACF など) が製品に付属している場合だけであることに注意してください。ただし、製品に付属しているライセンスが QRADAR* だけの場合は、アクティブな RACF データベース、バックアップの RACF データベース、RACF データベースのコピー、ACF2 バックアップ・データベース、または非アクティブな ACF2 データベースを使用する必要があります。
- ファイル・ポーリング方式を使用して LEEF データを転送することに決めた場合は、QRadar SIEM がこれらの LEEF ファイルをダウンロードできるように、z/OS イメージ上にアクティブな FTP (または SFTP) サーバーが必要です。

zSecure 構成には、QRadar SIEM の特定パラメーターが含まれていることが必要です。 詳しくは、 193 ページの『構成ファイルの更新』を参照してください。

zSecure のインストールおよび構成の手順については、「*Program Directory: IBM Security zSecure CARLa-Driven Components*」、および「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」(本書) の最初の数章を参照してください。

データ収集プロセスの SMF レコード

データ収集プロセスを開始する前に、以下の作業が必要です。

1. SMF レコードの生成。『SMF レコードの生成』を参照してください。
2. SMF レコードの使用可能化 (QRadar)。 188 ページの『QRadar での SMF レコードの使用可能化』を参照してください。

SMF レコードの生成

始める前に

SMF 処理がオンになっており、適切なレコードが作成および保存される必要があります。標準の必須 SMF レコードは、以下のとおりです。

- 0、 7、 9、 11、 14、 15、 17、 18、 22、 26、 30、 36、 41、 42、 43、 45、 47、 48、 49、 52、 53、 54、 55、 56、 57、 58、 59、 61、 62、 64、 65、 66、 80 (RACF および Top Secret)、 81 (RACF)、 82、 90、ほとんどの 92、118、および 119

- 102 の選択されたサブタイプ (DB2 IFCids 4、 5、 6、 7、 8、 9、 10、 22、 23、 24、 25、 55、 83、 87、 90、 92、 104、 105、 107、 140、 141、 142、 143、 144、 145、169、 177、 219、 220、 258、 270、 314、および 319)
- CICS モニター・レコード・タイプ 110 サブタイプ 1
- ACF2 を使用している場合は、ACF2 レコード・タイプ (サイト定義番号)
- Linux for System z からのデータ用の 83 サブタイプ 4
- WebSphere Application Server からのデータ用の 83 サブタイプ 5
- IBM Security Key Lifecycle Manager からのデータ用の 83 サブタイプ 6

正確な SMF レコード選択は、CARLa メンバー CKQLEEF および C2ELEEF で指定されます。これらのメンバーは、通常の保守によって更新できます。

インストール定義イベントを使用する場合は、必ず CARLa メンバー CKQCES または C2EQCES に必要な SMF レコードを組み込んでください。

手順

- CICS トランザクションの SMF レコードを生成するために、CICS モニターをセットアップして使用可能にします。 モニターは、データ・タイプおよびクラス単位でセットアップできます。例えば、例外、パフォーマンス、およびリソースの各クラスをモニターできます。CICS モニターを使用するには、以下のようにします。
  1. DFHMCT*xy* CICS モニター管理テーブル (MCT) を作成します。
  2. `MCT=`*xy* をシステム初期設定テーブル (SIT) に追加します。
  3. CEMT INQ MON コマンドを実行して、以下のいずれか (または両方) を確認または設定します。
     - モニター・データおよびオプションのクラスに対するモニター
     - モニター・データおよびオプションのクラス

  詳しくは、CICS Transaction Server ライブラリー (http://www.ibm.com/software/htp/cics/tserver/v53/library) で CICS モニター機能に関する情報を参照してください。

  SET MONITOR コマンドは、モニター・クラスおよびオプションを変更するために使用することもできます。
- DB2 の場合は、必要な SMF レコードを生成するために、DB2 トレースを活動化する必要があります。次のコマンドを使用します。 (これらのコマンドは 1 つの例です。インストールによっては、IFCID が既に他のトレースによって SMF にログとして記録されている場合もあります。これらの例を検査および調整して、インストールの要件を満たしてください。)

```
-<subsysname> START TRACE(PERFM) DEST(SMF) CLASS(30) IFCID(6,7,8,9,10,22,90,107,
              177,314)
-<subsysname> START TRACE(STAT) DEST(SMF) CLASS(30) IFCID(258)
-<subsysname> START TRACE(AUDIT) DEST(SMF) CLASS(*)
```

QRadar での SMF レコードの使用可能化

ファイル・ポーリング方式を使用して LEEF データを転送することに決めて、かつ SMF MAN データ・セットを使用する場合は、唯一の入力データとしてライブ SMF データ・セットを指定しないでください。指定するとギャップが生じます。最後に QRadar のデータ収集が実行されてから、その後に SMF データ・セットの切り替えが発生するまでの間に書き込まれた SMF レコードが欠落します。

ニア・リアルタイムのプロシージャー

直接のニア・リアルタイム SMF インターフェースの使用では、SMF ログ・ストリームを使用する必要があります。SMFPRM*xx* をセットアップして IFASMF.CKQRADAR という SMF INMEM リソースが定義してあることを確認してください。また、TYPE() パラメーターに必要な SMF タイプを指定します。以下に例を示します。

```
INMEM(IFASMF.CKQRADAR,RESSIZMAX(128M),
    TYPE(0,7,9,11,14,15,17,18,22,26,30,36,41,42,
         43,45,47:49,52:59,61,62,64:66,80:83,90,
         92,102,110,118,119,230))
```

ファイル・ポーリングのプロシージャー

- SMF ログ・ストリームを使用している場合、データ収集を実行する際に最も便利な方法は、ログ・ストリームから直接読み取る方法です。QRadar のデータ収集は、ログ・ストリームに指定した SMF 保存期間以上の頻度で実行するようにしてください (ログ・ストリームの指定には、ログ・ストリーム管理ユーティリティー IXCMIAPU を使用します)。このために専用のログ・ストリームをセットアップすることが必要な場合があります。
- SMF データ・セットを使用している場合、SMF オフロード・プロセス時のデータ収集のための、入力データを準備する必要があります。次のとおりです。
  1. 別の DD ステートメントをご使用の IFASMFDP プログラムに、次のように追加します。

     ```
     //OUTDD2   DD DISP=(MOD,CATLG),DSN=your.prefix.D&YYMMDD..T&HHMMSS,UNIT=...,SPACE=...
     ```
  2. 既存の累算データ・セットと新規データ・セットに同時に書き込むように IFASMFDP の制御ステートメントを更新します。

  ここで QRadar の収集プロセスでは、DSNPREF パラメーターを使用して追加のデータ・セットを取得します。そしてプロセスが正常に完了した後にデータ・セットを削除します。

  この例で示すようなシステム・シンボルの使用は、開始タスクでのみサポートされています。SMF オフロードをバッチ・ジョブとして実行する場合、世代別データ・グループ (GDG) を使用できます。 ただし、この方法はシリアライゼーションに欠点があるので、開始タスクへの切り替えを検討してください。
- 日次 SMF 累積データ・セットを作成しており、1 日に 1 回 QRadar データを準備する予定がある場合は、入力データとしてこの累積データ・セットを使用できます。ただし、例えば月次累積データ・セットを日次の準備のための入力データとして使用しないでください。その場合、累積の初期の SMF レコードが何度も読み取られるためです。zSecure はすでに処理されたレコードはスキップしますが、処理リソースの読み取りコストが余分にかかります。特に、累積 SMF が

テープに書き込まれ、そのテープのデータ・セットがマルチボリュームとなる場合、SMF 累積を読み取るコストは、リソースの処理に関しても、テープ・ドライブとボリュームの競合に関しても法外なものになります。

- データ・セットに複数の z/OS イメージのレコードが含まれている場合、そのデータ・セットを直接 QRadar に送らないでください。これはサポートされていません。そうではなく、イメージごとに個別に収集プロセスを実行して、各収集データを別個のディレクトリーに書き込んでください。 QRadar の各収集プロセスは、その収集プロセスの関連イメージから SMF、CKFREEZE、および UNLOAD にアクセスできる限り、関連する z/OS イメージのもとで実行する必要はありません。以下の方法のいずれかを使用します。
  - メンバー CKQXES または C2EQXES に EXCLUDE ステートメントを指定します。 193 ページの『構成ファイルの更新』を参照してください。各収集プロセスは、それ自体の zSecure 構成データ・セット内に独自のメンバーを持っていることが必要です。この方法では、結合された SMF は複数回読み取られます。
  - まず累積データ・セットに対して、特殊 CARLa ジョブまたはジョブ・ステップを実行し、そのジョブまたはジョブ・ステップからの出力データを QRadar の別のインスタンスの準備のための入力データとして使用します。ジョブでは、各 z/OS イメージの個別のデータ・セットにレコードを書き込むため、SELECT ステートメントを使用して SMF ID および UNLOAD の各ステートメントを指定します。この方法では、結合された SMF は 1 回だけ読み取られます。
- 失われた SMF インターバルをリカバリーする場合、同様のジョブを実行して累積データ・セットからインターバルと SMF ID を選択します。

収集プロセスのセットアップ

以下のステップとガイドラインを使用して、QRadar SIEM との統合のためのデータ収集をセットアップします。

始める前に

zSecure では、LEEF による QRadar SIEM との統合を実現するために 3 つのメンバー・セットが用意されています。

- 1 つ目のセットは、ニア・リアルタイム用であり、CKQ 接頭部と、L (「Live」用) で終わるいくつかのバリアントを使用します。
- 2 つ目のセットも CKQ 接頭部を使用しますが、接尾部 L は使用しません。
- 3 つ目のセットは、C2E 接頭部を使用します。これは、zSecure Audit を使用する場合の統合用の後方互換のセットです。このメンバー・セットは、zSecure Adapters for QRadar SIEM 製品では使用できません。このセットは、現在非推奨であり、機能が固定されています。

どのデータ収集プロセスを使用するか決定し、適切なメンバー・セットを選択します。選択したプロセスに対して、以下のステップを実行します。ニア・リアルタイム・プロセスでは、zSecure は、開始タスクとして実行するための CKQRADAR プロシージャーを提供します。ファイル・ポーリング・プロセスのためのデータの収集と準備では、zSecure は、プロシージャーとそのプロシージャーを使用するサ

ンプルのバッチ・ジョブ (CKQCLEEF/CKQJLEEF と C2ECQRLF/C2EJQRLF) を提供します。プロシージャーによって作成されるファイルには、セキュリティー・イベントなどのイベントのログが含まれます。これらのファイルの許可ビットは、CKQCLEEF/C2ECQRLF プロシージャー本体内で UMASK ステートメントを使用して制御できます。デフォルトは UMASK=027 です。これにより、未指定のユーザーのアクセスが除外されます。

CKQCLEEF プロセスは、SCKRCARL (CKQLEEF) から CARLa スクリプトを実行します。このスクリプトには、以下のようなコードが記述されています。

```
imbed member=ckq0es

imbed member=ckqrenv esm=RACF

/* Primary selection of records                                      */
NewList type=SMF name=SMFSEL DDname=CKREPORT
  imbed DDname=SMFHWIN
  imbed member=ckqxes
  summary system "|" date MinTime MaxTime "|" SMFdd count(10)

NewList type=SMF DDname=CKREPORT ,
    title="Number of records per date per type"
  select likelist=SMFSEL
  summary type "|" date MinTime MaxTime "|" count(10)

/* optional report : number of records per type and SubType         */
NewList type=SMF DDname=CKREPORT ,
    title="Number of records per type and subtype"
  select likelist=SMFSEL
  summary type SubType "|" count(10)

/* One mergelist for all record types for "device type" z/OS        */
MergeList name=SMF DDname=CKQLOGZ
/* IPL - type 0                                                     */
NewList type=SMF name=IPL nodup
  select likelist=SMFSEL type=0
  SortList  datetime(nd) LEEF,
    | type(0) | '|' | dTF,
    | tab | 'devTime='   | datetime(Java_SimpleDate,0),
    | tab | 'job='       | system(0),
    | tab | 'sum='       | recorddesc(0)

...
EndMerge
```

SMFSEL newlist は、SMF イベントの中心的なフィルターとして機能します。この newlist は、CKQCLEEF の以前の反復によって処理された可能性のあるレコードを除外するためにカットオフのタイム・スタンプ (上限基準点 (HWM) とも呼ばれます) を適用します。これには、イベントを除外することを意図しているメンバー CKQXES の CARLa 出口コードも含まれます。ニア・リアルタイム CKQRADAR プロセスでは、CARLa メンバー CKQLEEFL を使用します。CKQLEEFL には、CARLa 出口メンバーの CKQ0ES、CKQXES、および CKQCES も含まれますが、収集されたレコードの上限基準点を処理するコードは含まれません。

CKQXES の EXCLUDE コマンドを実行すると、LEEF を生成するすべての newlist 内で一致するすべての SMF レコードが除外されます。EXCLUDE コマンドを実行する場合は、正確に入力する必要があります。正確に入力しないと、意図しない影響が発生する可能性があります。以下の例は、CARLa の exclude ステートメントを

示しています。このステートメントを CKQXES で使用すると、George というユーザーが生成したイベント・データを抑止することができます。

- `exclude user=George` というステートメントを CKQXES で使用すると、George が生成したすべてのイベントが抑止されます。
- `exclude user=George desc=viol` というステートメントを CKQXES で使用すると、RACF が戻りコード 8 を返したすべてのイベントが抑止されます。また、これ以降は、他の非 RACF レコードも抑止される可能性があります。
- `exclude user=George event=access(viol) class=dataset` というステートメントを使用すると、George の DATASET アクセス違反だけが除外されます。
- `exclude user=George event=access(success) racfauth=operations` というステートメントを使用すると、Operations 属性により、George に付与されている DATASET アクセス権と RESOURCE アクセス権がすべて除外されますが、LEEF での操作により、George が発行した RACF コマンドは除外されません。

以下の例は、CARLa の `exclude` ステートメントを示しています。このステートメントを CKQXES で使用すると、ユーザー ID のリストに対するイベントを抑止することができます。

- `exclude user=(known,user,ids), access<=read, desc=success event=allsvc(success)` というステートメントを使用すると、特定のユーザー ID について、QRadar に渡される 1 から 7 までの成功 RACF イベント・コードがすべて除外されます。
- `exclude user=(known,user,ids) access<=read, desc=success` というステートメントを使用すると、特定のユーザー ID について、正常なアクセス記録が除外されます。

`NEWLIST TYPE=SMF` の `ACCESS` フィールドに有効な値は、N/A、NONE、EXECUTE、READ、UPDATE、CONTROL、ALTER、または OWNER です (表「SMF レコードの ACCESS フィールド - 使用可能な値」を参照)。「*IBM Security zSecure CARLa* コマンド・リファレンス」の SMF NEWLIST のフィールドの説明を参照してください。`access<=read` というコードを使用すると、UPDATE レベル以上のアクセス権限は LEEF データに含まれます。

以下の例は、SMF レコード・タイプに基づいてイベントを抑止するために CKQXES で使用できる CARLa `exclude` ステートメントを示しています。

- `exclude type=(14,92(1))`: SMF タイプが 14 のレコード、または SMF タイプが 92 でサブタイプが 1 のレコードの READ ログが除外されます。

注**:**

1. 構成の更新を終了するまで、プロセスを開始しないでください。
2. カットオフ・ファイルがまだ存在していないので、最初の実行は失敗し CKR0945 メッセージが表示されます。この失敗は問題ではありません。ファイルは、この最初のジョブ中または開始タスク中に作成されます。やり直してください。

手順

- 収集プロセスをバッチで実行する場合、ジョブのコピーを発行するようにジョブ・スケジューリング製品を構成します。あるいは、このジョブを発行するように SMF オフロード・プロセスを調整することができます。
- 開始タスクとして収集プロセスを実行する場合、プロシージャーおよび zSecure 構成メンバーを、Job Entry Subsystem (JES) のプロシージャー・データ・セットに組み込んで、自動操作または JES 自動コマンドによって開始させます。
- インストール環境内で使用する規則に従い JCL のコピーをカスタマイズします。具体的には、選択した zSecure 構成メンバーを指定します。デフォルトは C2R$PARM ですが、zSecure Suite の複数の機能を使用する場合、機能ごとに個別の構成を使用することが必要になる場合があります。
- ジョブまたは開始タスクの JCL がアクセスできる場所に構成メンバーを保管します。開始手順の場合、これは JES プロシージャー・ライブラリーになります。ジョブの場合、JCLLIB ステートメントを使用して、他のいずれかのデータ・セットを指定します。 指定する必要がある QRadar 固有のパラメーターは以下の通りです。

  CKQCUST/C2EQCUST
  構成メンバーを含むデータ・セットの名前。 193 ページの『構成ファイルの更新』を参照してください。

  CKQPATH/C2EQPATH
  収集プロセスがそのデータを預ける UNIX ディレクトリー。

ユーザー ID の割り当てと LEEF データを保管するディレクトリーの準備

このタスクについて

ファイル・ポーリング・プロセスを使用して LEEF データを転送すると、そのデータは USS ファイル・システムに保管されます。このセクションでは、USS ファイル・システムの準備に必要なステップを説明します。SMF INMEM リアルタイム・インターフェース・プロセスを使用する場合は、このステップをスキップできます。

複数のデータ準備プロセスを (複数の z/OS イメージに対して) 実行する場合は、各プロセスに独自の (サブ) ディレクトリーが必要です。[1] 他の UNIX ディレクトリーと同様に、所有ユーザーと所有グループの両方が必要です。収集プロセスを実行するユーザー ID のホーム・ディレクトリー (またはホーム・ディレクトリーのサブディレクトリー) を使用したり、専用ファイル・システムを使用する場合があります。

zSecure には、必須ユーザーおよびグループ、ホーム・ディレクトリー、およびファイル・システムを作成するために、以下のジョブが用意されています。
- ジョブ CKQAUSA/C2EQAUSA (ACF2 用)
- ジョブ CKQAUSR/C2EQAUSR (RACF 用)
- ジョブ CKQAUST/C2EQAUST (Top Secret 用)

1. 各収集プロセスには独自の (サブ) ディレクトリーが必要です。

手順

1. 外部セキュリティー・マネージャー (RACF、ACF2、または Top Secret) に適用されるジョブを選択します。
2. ユーザー、グループ、UID、GID、およびデータ・セットの規則に応じてジョブを調整します。
3. バッチ・ジョブか開始タスクかのどちらを選択するかによって、 (RACF、または ACF2 や Top Secret に相当する物の) SURROGAT または STARTED プロファイルを作成するアクションのコメントを外します。 このステップにより、指定のユーザー ID でプロセスが確実に実行されるようになります。
4. QRadar SIEM による 2 回の連続した取得の間に生成される SMF データの量に基づいて、ファイル・システムのサイズを指定します。 SMF ピークや QRadar の障害に対応できるようなマージンを考慮します。
5. ジョブを実行します。ファイル・システムが後続の IPL 後にもマウントされることを確認します。自動マウント機能を使用することもできます。

構成ファイルの更新

このタスクについて

新規 zSecure 構成 データ・セット (CKRPARM という名前がよく使われますが、任意のデータ・セット名を使用してかまいません) を使用する場合、ジョブ CKRZPOST を実行してください。 31 ページの『第 6 章 ソフトウェアのデプロイメント』を参照してください。

既存の CKRPARM データ・セットを使用できますが、それが以前のレベルの zSecure で作成されていた場合、一部の構成メンバーが欠落している可能性があります。その場合は、SCKRCARL および SCKRSAMP ライブラリーから以下のメンバーをコピーします。

- CKQ セットの場合は、CKQRENV、CKQSPEC、CKQSPECL、CKQFIN、CKQCES、CKQXES、および CKQ0ES をコピーします。これらのメンバーは、ファイル・ポーリング・プロセスと ニア・リアルタイム・プロセスによって使用されます。
- C2E セットの場合は、C2EQENV, C2EQSPEC, C2EQFIN, C2EQRENV, C2EQAENV, C2EQTENV, C2EQCES, C2EQXES, および C2EQ0ES をコピーします。これらのメンバーは、非推奨の zSecure Audit ファイル・ポーリング・プロセスによって使用されます。

手順

以下のように、メンバーをカスタマイズします。

1. メンバー CKQSPECL を ニア・リアルタイム 用に調整するか、メンバー CKQSPEC/C2EQSPEC をファイル・ポーリング用に調整して、入力データと出力データを指定します。
   a. メンバー CKQSPECL/CKQSPEC/C2EQENV を調整して、入力データを指定します。つまり、適切な ESM のアクティブなセキュリティー・データベースを指定するか、C2RJPREP ジョブで毎日リフレッシュする UNLOAD データ・セットおよび CKFREEZE データ・セットを指定します。 55 ページの

ージの『フレッシュな CKFREEZE および UNLOAD の毎日の使用』を参照してください。アクティブなセキュリティー・データベースを使用すると、LEEF レコードについてより最新の強化が得られますが、セキュリティー・データベースへの READ アクセス権限が必要です。Top Secret を使用する場合、UNLOAD 割り振りは Top Secret に適用されないので削除します。製品に付属しているライセンスが QRADAR* だけである場合、UNLOAD の代わりに、アクティブな RACF データベース、バックアップの RACF データベース、RACF データベースのコピー、ACF2 バックアップ・データベース、または非アクティブな ACF2 データベースを使用する必要があります。QRADAR* 以外のライセンスも製品に付属している場合は、任意のものを選択できます。

b. ニア・リアルタイムの場合は、CKQSPECL 内の SYSLOGUDP または SYSLOGTCP パラメーターで QRadar SIEM システムの IP アドレスを指定します。IP v4 アドレスは、`::FFFF:`*`a.b.c.d`* のように指定できます。ここで、*a.b.c.d* は IP v4 構文のアドレスです。

c. ファイル・ポーリングの場合は、入力データとして選択した SMF を、ログ・ストリームの名前として、または DSNPREF パラメーターを使用して指定します。 188 ページの『QRadar での SMF レコードの使用可能化』を参照してください。 DSNPREF パラメーターを使用する場合は DELETE パラメーターを指定して、SMF オフロード中にこの目的のために作成したデータ・セットを、処理の正常な完了後には削除するようにしてください。

d. ファイル・ポーリングの場合は、LEEF ファイルの絶対パスを指定します。システム内では発生しないログ・ソースの場合 (システムで RACF を使用している場合の ACF2 や、システムで ACF2 を使用している場合の RACF など)、出力先を `/dev/null` に指定すると、zip ヘッダーしか含まれていない LEEF ファイルの書き出しを防ぐことができます。その他の LEEF ファイルでは、ファイル名を変更しないでください。そして、パスのディレクトリー部分が CKQPATH/C2EQPATH パラメーターと一致していることを確認してください。

e. ファイル・ポーリングの場合は、時間ベースのカットオフ・ファイルの絶対パスを指定します。 このファイルは、`TYPE=SMFHWIN` および `TYPE=SMFHWOUT` として識別されるファイルです。どちらの場合も同じファイルを指定するようにしてください。

   注: 失われた SMF インターバルをリカバリーする必要がある場合は、リカバリーする期間がスキップされないように、このファイルを空にします。リカバリーの完了後、編集して前の内容を戻します。

f. ファイル・ポーリングの場合は、新規ファイルのデフォルトの監査設定で、成功したアクセスと失敗したアクセスのログが生成されます。ご使用のインストール済み環境で、LEEF データを格納するファイルへのアクセスのロギングが必要ない場合は、CKQSPEC/C2EQSPEC 内で ALLOC FAUDIT 指定を変更します。

g. ファイル・ポーリングの場合、必要であれば、出力オプションを指定します。デフォルト・オプションは、zSecure 提供サンプル・メンバー内にあります。

2. C2E セットの場合のみ、メンバー C2EQENV を調整して、入力データを指定します。メンバー C2EQSPEC で指定したのと同じ UNLOAD および

CKFREEZE データ・セットを指定します。 55 ページの『フレッシュな CKFREEZE および UNLOAD の毎日の使用』を参照してください。 Top Secret を使用する場合、UNLOAD 割り振りは Top Secret に適用されないので削除します。

3. 環境の指定を調整します。
   - RACF システムの場合は、メンバー CKQRENV/C2EQRENV 内の特権ユーザー・グループを構成します。このメンバーは、特権役割を表すグループを指定します。このメンバーにリストされているグループにユーザーが接続されている場合、イベントにそのグループ名を示す注釈が付けられます。
   - ACF2 および Top Secret システムの場合、この構成は適用されません。
4. オプションで、メンバー CKQ0ES/C2EQ0ES、CKQXES/C2EQXES、および CKQCES/C2EQCES を以下のように調整します。

   CKQ0ES/C2EQ0ES

   処理の開始時に処理される CARLa。このメンバーを使用できるのは、例えば、IBM またはベンダーのソフトウェアがフォーマットの正しくない SMF レコードを書き込み、それが原因でエラーが起きる場合です。この場合、IBM ソフトウェア・サポートから、OEM ベンダーの問題が解決されるか、より永続的な解決策が構築されるまでの間使用する、一連の CARLa ステートメントが提供される場合があります。

   このメンバーを利用して、例えば、2 バイト文字セット (DBCS) 文字から UTF-8 への変換時などに、正しい CCSID を指定することもできます。例えば、日本語英数小文字拡張 Unicode の場合、次の CARLa ステートメントを組み込むことができます。

   ```
   OPTION MY_CCSID=1399
   ```

   CKQXES/C2EQXES

   SMF 選択の CARLa EXCLUDE。

   CKQCES/C2EQCES

   インストール定義イベントもマップするように z/OS ログ・リソースをカスタマイズするための CARLa。例えば、製品で独自の SMF レコードを使用することもできます。

ユーザー ID の割り当てと CKQRADAR 開始タスクのセットアップ

このタスクについて

これは、直接および CDP サーバーを介した場合の両方によるニア・リアルタイム QRadar サポートのためのタスクです。CKQRADAR の実行が開始タスクとして最適です。

手順

1. CKQRADAR プロシージャーを SCKRPROC から、ニア・リアルタイムでモニターする z/OS システムにコピーします。SYSOUT クラス A の適用可能性を確認します。クラス A は、STATOUT パラメーターと PRTOUT パラメーターのデフォルトです。

2. 開始タスクのユーザー ID に、FACILITY IFA.IFASMF.CKQRADAR への READ 権限、または構成タスクで選択したリソース名への READ 権限があることを確認します。SAF リソース名では、INMEM リソース名の前に修飾子 IFA が使用されます。

ユーザー ID の割り当てと CDP/SDE サーバー開始タスクのセットアップ

始める前に

System Data Engine は、未加工の SMF データを zSecure に渡すために使用できます。System Data Engine を zSecure とともに使用するための準備として、この手順にあるステップを実行する必要があります。次の両方の項目が該当することを確認してから、以下のステップを開始してください。

1. SMP/E を使用して、System Data Engine の FMID (例えば、HHBO11E) をインストールする必要があります。
2. zSecure を実行する APF 許可データ・セットに、System Data Engine のクライアント・ロード・モジュールをコピーするか、ライブラリーを CKQRADAR プロシージャーの STEPLIB 連結の最後に追加する必要があります。

このタスクについて

このタスクは、Common Data Provider (CDP) System Data Engine (SDE) を使用する場合のみの ニア・リアルタイム QRadar サポート向けです。

手順

1. STARTED クラスのプロファイルをセットアップして、開始タスクに使用する ID を指定します。
2. 指定した開始タスク ID に、FACILITY クラスのリソース IFA.*rname* または LOGSTRM クラスの適切な *logstreamname* へのアクセス権限があることを確認します。
3. 開始タスクとして System Data Engine を実行するプロシージャーを作成するための開始点として、HBOvrm.SHBOCNTL(HBOSMFU) の サンプル JCL を使用します。あるいは、System Data Engine をバッチ・モードで実行する場合、開始点として HBOvrm.SHBOCNTL(HBOJCOLU) のサンプル JCL を使用します。サンプル JCL を実行する前に、以下のようにカスタマイズする必要があります。
   a. ジョブ・カードをご使用のサイト標準に合わせて修正します (HBOJCOLU の場合のみ)。
   b. STEPLIB DD を変更して、System Data Engine プログラムがインストールされているデータ・セットを参照するようにします。このデータ・セットは、APF 許可を与えられていなければなりません。
   c. `DEFINE UPDATE` 制御ステートメントを変更して、System Data Engine サーバーと CKQRADAR との間の通信に使用するポート番号を指定します。`TO SERVER` 節の *ppppp* を置き換えてください。
   d. `COLLECT` 制御ステートメントを変更して、SMF データを提供する SMF ログ・ストリームまたはメモリー内のリソースの名前を指定します。`FROM` 節の IFASMF.*lsname* を置き換えてください。

e. オプションで、COLLECT制御ステートメントを変更して、EVERY 節に時間間隔を分または秒単位で指定します。1 分より短い収集間隔を使用すると、ログ・ ストリームからデータを提供するとき、オーバーヘッドが増大する可能性があります。

これで、System Data Engine の開始タスクを開始したり、System Data Engine のバッチ・ジョブを実行依頼したりする準備ができました。

CKQRADAR 開始タスクの操作

次のコマンドを使用して、リアルタイム SMF 収集を開始します。

```
START CKQRADAR
```

実行中、CKQRADAR 開始タスクはシステム・オペレーターからのコマンドを受け入れます。使用可能なオペレーター・コマンドは、STOP (つまり P) と MODIFY (つまり F) です。現在これらのオペレーター・コマンドは、SMF レコードの入力処理中にのみ認識されます。システムが SMF レコードをほとんど生成していないか、または生成していない場合は、オペレーター・コマンドへの応答が大幅に遅延することがあります。

STOP CKQRADAR

このプログラムは、SMF レコードの読み取りまたは待機を停止します。既に読み取られたレコードが処理され、適用可能な場合、サマリー・レポートが作成されます。STOP コマンドの効果は、SMF レコード入力ソースでの通常のファイルの終わりの処理と類似しています。

MODIFY CKQRADAR,*action*

MODIFY コマンドでは、必要なアクションを指定するための追加のキーワードが必要です。MODIFY コマンドでは以下のアクションがサポートされています。

STOP STOP オペレーター・コマンドと同じです。

ATTN

このアクションは、TSO セッションで ATTN キーを押すのと同じ効果があります。現在の処理が終了され、出力ファイルが正常に閉じられます。

CANCEL

ATTN コマンドと同じです。

DISPLAY

このアクションは、SMF 処理の現在の状況に関する情報を要求します。ジョブ・ログやシステム・ログへのメッセージの書き込みに WTO (オペレーター宛メッセージ) マクロを使用し、CKR3014 などのメッセージが書き込まれます。これらのメッセージは、ジョブ・ログと JES SYSLOG でも確認できます。

RESTART

この MODIFY コマンドは、例えば、セキュリティー・データベース内または CKFREEZE ファイル内の更新情報を取得するためにプログラムの再始動を要求する際に使用できます。このコマンドは、現在実行されているプログラムの出力データ・セットがスプールに

経路指定されたか、DISP=MOD を使用して割り振られた場合を除き、そのデータ・セットの現行内容を削除して置き換えることに注意してください。

Other *action* が認識不能であると、メッセージ CKR3015 が生成されます。

QRadar ログ・ソース・プロパティー

図 10 には、画面の例を示します。リアルタイムの場合は、「Service Type」に syslog を使用し、ファイル・ポーリングの場合は、「Service Type」に FTP を使用します。詳しくは、QRadar の「*DSM* の構成ガイド」を参照してください。

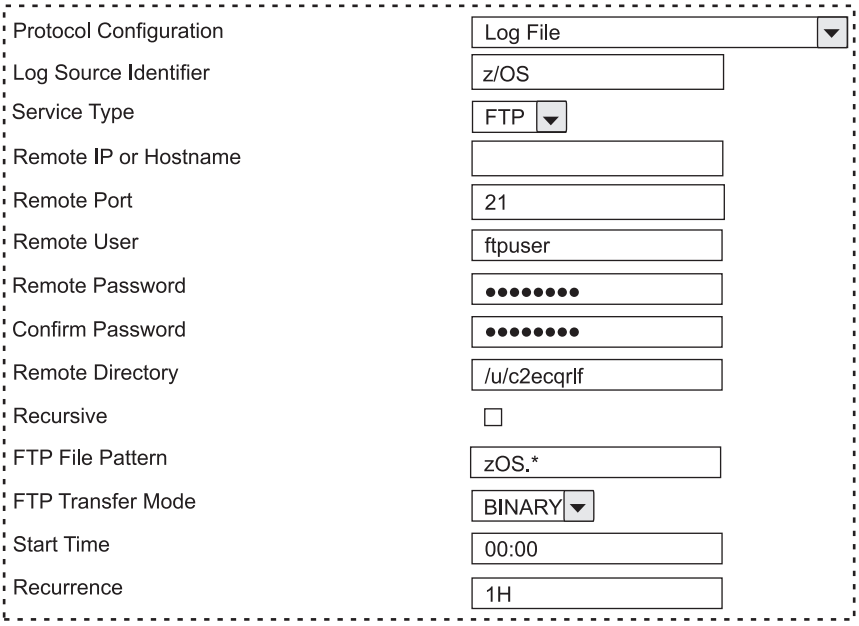


図 *10. QRadar* のログ・ソース・プロパティーの構成

SYSLOG をデータ・ソースとしてサポートするには、ログ・ソースで更新が必要になる場合があります。

第 16 章 Guardium Vulnerability Assessment 用にデータを準備する

このトピックでは、IBM InfoSphere® Guardium® Vulnerability Assessment (Guardium VA) を使用した DB2® 環境の拡張監査用の入力を提供する場合に、zSecure Audit を使用するために実行する必要があるアクションについて説明します。

DB2 オブジェクトの RACF 保護に関する情報と、ユーザーおよびグループに関する情報は、Guardium VA の使用のために DB2 テーブルにロードされます。この情報は、RACF グループを DB2 AUTHID として使用する場合、または RACF アクセス・コントロール・モジュール DSNX@XAC を使用する場合に、特に関連性があります。Guardium VA では、特定の DB2 サブシステムに関するデータが、その DB2 サブシステム自体で使用可能になっている必要があります。これにより、DB2 カタログの情報を、zSecure によって提供されるセキュリティー情報に直接結合することができます。DB2 サブシステム内のデータをロードするため、zSecure の SCKRSAMP 内にサンプルが用意されています。これらのサンプルを変更して使用する場合は、別のデータ・セットにサンプルをコピーしてください。SCKRSAMP のデータ・セットは SMP/E によって制御されるため、変更内容は今後の更新によって上書きされる可能性があります。

以下のステップを実行して適切な DB2 テーブルをロードすると、RACF の拡張情報を利用できるようになります。 Guardium VA では、Guardium VA のライセンス・レポートと脆弱性テストを使用できます。これらのレポートとテストの名前には、先頭に zSecure が付いています。

Guardium VA に対する zSecure の提供データを格納する DB2 データベースを作成して管理するには、以下のアクションを実行する必要があります。

1. 1 つ以上の DB2 データベースを作成する。
2. 1 つ以上の DB2 テーブル・スペースを作成する。
3. DB2 テーブルを作成する。
4. データをテーブルにロードする。

最初の 3 つのステップは、データベースの初期セットアップを行うためのステップです。これらのステップは、データ・マネージャーの初期化後に 1 回だけ実行する必要があります。テーブルの設定が完了したら、DB2 データベースにデータを繰り返しロードできるようになります。例えば、データを毎日更新することができます。これは、インストール済み環境に依存します。現行のテーブル・データはいつでも削除することができます。また、これらのテーブルを通常の DB2 ユーティリティーと SQL ステートメントを使用して管理することもできます。以下の各セクションでは、Guardium VA で使用する zSecure データの作成とロードを行う際に使用できるサンプルについて説明します。

サンプル・ジョブは、ローカルの DB2 サブシステムと直接対話するため、各システムでサンプル・ジョブを実行する必要があります。リモートの入力ソースを使用

したり、1 回の実行で複数のシステムを処理したりすることはできません。サンプル・ジョブを実行する前に、zSecure 構成 (つまり、メンバー C2R$PARM、またはこのメンバーのカスタム・コピー) が正しい値でカスタマイズされていることを確認してください。また、「!!」という値を、使用する DB2 の正しいレベルで置き換え、「!DSN!」という値を DB2 サブシステムの名前で置き換える必要があります。付属のサンプル・ジョブでは、SCKRSAMP データ・セットが使用されます。この名前を、変更後のサンプル・メンバーのコピーに対して使用したデータ・セットの名前に変更してください。

DB2 のステップでは、標準 DSNUTILB ユーティリティー・プログラムと DSNTEP2 生産性支援サンプル・プログラムが使用されます。これら 2 つのユーティリティー・プログラムが DB2 サブシステムに対して使用可能になっていて、バウンドされている必要があります。 DSNTEP2 サンプル・プログラムのインストールについては、「*DB2 for z/OS* ユーティリティー・ガイドおよび解説書」の『生産性支援サンプル・プログラム』セクションを参照してください。

このアプリケーションで使用される DB2 スキーマ名は CKADBVA で、テーブル名はすべて CKA で始まります。スキーマ名とテーブル名を変更することはできません。

付属のサンプル・ジョブを以下に示します。

CKAJVA00

DB2 データベースでは、テーブル・スペースの集合が指定されます。サンプル・ジョブ CKAJVA00 は、テーブル・スペースとテーブルを格納するために、DB2 内にデータベースを作成します。DB2 データベースを作成するための適切な DB2 権限を持つユーザーが、このジョブを実行する必要があります。Guardium VA では、DB2 サブシステムに関する情報が、DB2 サブシステム内のテーブルで使用可能な状態になっている必要があります。そのため、Guardium VA を使用して分析を行う各システム上で CKAJVA00 ジョブを実行する必要があります。

データベースは、以下の有効なデフォルト設定を使用して作成されます。

```
CREATE DATABASE CKADBVA;
```

データベースの名前は、インストール済み環境での基準に従って変更することができます。

CKAJVA01

テーブル・スペースとは、1 つ以上のテーブルが保管される 1 つ以上のデータ・セットのことです。サンプル・ジョブ CKAJVA01 には、2 つのステップがあります。最初のステップでは、テーブルとテーブル・スペースに対して SQL **DROP** ステートメントを使用して、以前の **LOAD** によるデータが残っていないことが確認されます。2 番目のステップでは、テーブル・スペースとテーブルが作成されます。このジョブを初めて実行すると、オブジェクトをドロップする DROP ステップが戻りコード 8 で終了します。このエラーは無視してかまいません。または、CREATE ステップだけを実行するようにジョブを編集することもできます。このジョブを実行するには、サンプル CKAJVA00 で作成された DB2 データベース内でこれらのオブジェクトのドロップと作成を行うための適切な DB2 権限が必要です。Guardium VA では、DB2 サブシステムに関する情報が、DB2 サブシステム内のテー

ブルで使用可能な状態になっている必要があります。そのため、Guardium VA を使用して分析を行う各システム上で CKAJVA01 ジョブを実行する必要があります。

テーブル・スペースは、以下の有効なデフォルト設定を使用して作成されます。

```
CREATE TABLESPACE CKADBVA in CKADBVA;
```

正しい *storagegroup* を割り当てるため、またはテーブルで使用可能なスペースを増やすために、以下の例のように、割り振りに関連するキーワードを指定しなければならない場合があります。

```
USING STOGROUP storagegroup
PRIQTY 20000
```

テーブルの作成例と、テーブル・スペース内での索引の作成例を以下に示します。

```
CREATE TABLE CKADBVA.CKA_OS_GROUP (
     COMPLEX                CHAR(8)    NOT NULL,
     GROUP                  CHAR(8)    NOT NULL,
     ADDITIONAL_INFO        VARCHAR(256) ,
     PRIMARY KEY (COMPLEX,GROUP)
     )
     in  CKADBVA.CKADBVA;
CREATE UNIQUE INDEX CKADBVA.IDX_CKA_OS_GROUP ON
       CKADBVA.CKA_OS_GROUP(COMPLEX, GROUP);
```

テーブルと索引が作成されると、テーブルに対する SELECT 権限をユーザー SQLGUARD (Guardium VA の SQL ID) に付与するために、**GRANT** ステートメントが発行されます。以下に例を示します。

```
GRANT SELECT ON CKADBVA.STATUS TO SQLGUARD;
```

テーブル・スペースの名前は、インストール済み環境での基準に従って変更することができます。スキーマ名とテーブル名を変更することはできません。

CKAJVA99

このジョブにも 2 つのステップがあります。最初のステップである CKFCOLL ステップでは、DB2 カタログ・テーブルの情報が CKFREEZE データ・セットに収集されます。2 番目のステップでは、CKRCARLA を使用して、2 番目のジョブ用の JCL と入力が作成されます。デフォルトでは、この 2 番目のジョブは即時に実行依頼されます。この 2 番目のジョブには、各 DB2 サブシステム用のステップがあります。このジョブでは、CKRCARLA を使用して特定の DB2 サブシステム固有の入力ファイルが作成され、DSNUTILB を使用して対象の DB2 サブシステムにこのファイルがロードされます。またこのジョブには、データの後処理を簡素化するためのいくつかの SQL ステップも含まれています。これらのステップは、DB2 サブシステムごとに繰り返して実行されます。指定された行で CARLa **SELECT** または **EXCLUDE** ステートメントを使用して、特定の DB2 サブシステムを包含または除外するようにジョブ CKAJVA99 を更新することができます。その場合、生成されたジョブには、選択した DB2 サブシステムだけを対象とするステップが含まれることになります。CKAJVA99 ジョブを実行するには、DB2 テーブルのロードと更新を行うための適切な DB2 権限が必要です。

DB2 の複数のリリースがアクティブになっている場合は、そのリリースごとにこのジョブのインスタンスを作成する必要があります。**STEPLIB DD** ステートメントでは、各リリースの正しい DB2 レベルが指定されている必要があります。この場合、サンプルの **SELECT** ステートメントまたは **EXCLUDE** ステートメントを使用して、STEPLIB ライブラリー内のリリースに一致するものだけに DB2 サブシステムを制限する必要もあります。

デフォルトでは、CKAJVA99 によって生成されるジョブは、即時に実行依頼されます。生成されたジョブを最初に確認したい場合は、DDNAME STAGE2 からの出力をデータ・セットまたは SYSOUT にリダイレクトします。

テーブルのロードに使用される **LOAD** ステートメントには、テーブルを繰り返しロードするための、データの静的な特性を反映したキーワードが含まれています。関連するキーワードは以下のとおりです。

```
LOAD DATA
     REPLACE
     REUSE
     LOG    NO
     NOCOPYPEND
```

これらのキーワードの意味については、「*DB2 for z/OS* ユーティリティー・ガイドおよび解説書」を参照してください。

このサンプル・ジョブでは、SCKRSAMP 内の以下のメンバーが入力として使用されます。

CKAVA000
このメンバーには、RACF 入力ソースと CKFREEZE データ・セットを指定するために必要な CARLa **ALLOC** ステートメントが含まれています。

CKAVA001
このメンバーには、RACF システムの RACF ユーザーと RACF グループの情報レコードと、DB2 オブジェクトのアクセス・マトリックスの通常の (効力のない) 形式を作成するための CARLa ステートメントが含まれています。

CKAVA002
このメンバーには、RACF システムの DB2 オブジェクトのアクセス・マトリックスの有効な形式を作成するための CARLa ステートメントが含まれています。

CKAVA100
このメンバーには、ACF2 入力ソースと CKFREEZE データ・セットを指定するために必要な CARLa **ALLOC** ステートメントが含まれています。

CKAVA101
このメンバーには、ACF2 システムの ACF2 ユーザーと ACF2 ソース・グループの情報レコードと、DB2 オブジェクトのアクセス・マトリックスの通常の (効力のない) 形式を作成するための CARLa ステートメントが含まれています。

CKAVA102

このメンバーには、ACF2 システムの DB2 オブジェクトのアクセス・マトリックスの有効な形式を作成するための CARLa ステートメントが含まれています。

CKAVALD0

このメンバーには、DB2 テーブルをロードするための SQL **LOAD** ステートメントが含まれています。

CKAVAMN0

このメンバーには、アクティブな外部セキュリティー・マネージャー (RACF または ACF2) に基づいて該当する CARLa メンバーを組み込むための CARLa **INCLUDE** ステートメントが含まれています。

CKAVASQ0

このメンバーには、通常形式のアクセス・マトリックスの必要な後処理を簡素化するための SQL ステートメントが含まれています。

CKAVASQ1

このメンバーには、有効な形式のアクセス・マトリックスの必要な後処理を簡素化するための SQL ステートメントが含まれています。

CKAVASQ9

このメンバーには、ロード・プロセスの状況を記録するための SQL ステートメントが含まれています。

DB2 と各ユーティリティーについて詳しくは、以下の資料を参照してください。

- *DB2 for z/OS* ユーティリティー・ガイドおよび解説書
- *DB2 for z/OS SQL* 解説書
- *DB2 for z/OS* 管理ガイド

付録 A. サイト・モジュール

サイト・モジュールの使用はオプションです。この製品は、サイト・モジュールなしで完全に作動可能です。 SCKRSAMP ライブラリーのジョブ CKRZSITE は、ユーザーによるサイト・モジュールの作成を支援するために提供されています。

表 18 に、サイト・モジュール CKRSITE でカスタマイズ可能な zSecure オプションをリストします。

表 18. サイト・モジュール・オプション

パラメーター	許可される値	説明	デフォルト
AUTH	SINGLE DOUBLE TRIPLE	デフォルトの複数権限設定。	SINGLE
CUSTSPEC	最大 100 文字までのテキスト	サイトまたはカスタマー固有の ID。このパラメーターは、さまざまな zSecure コンポーネントの SYSPRINT 出力に含まれています。 この値は zSecure Collect でデフォルトの CHECKPWD としても使用されるため、長期にわたって (10 年以上) 安定していることが期待できる値を選択してください。	<none>
CLASS	SAF クラス名	zSecure セキュリティー検査用のリソース・クラス。	XFACILIT
KEEPCOMMAND	数字	CKGRACF キューに入れられたコマンドの有効期限。	7
KEEPAUDIT	数字	完了し、有効期限が切れてキューに入れられたコマンド、および過去のスケジュールに入れられたアクションが CKGRACF によって保持される期間。この設定値は、有効期限より大きい値でなければなりません。	30
RESTRICT	Y N	制限モード。また、この設定ではなく、 CLASS パラメーターにより提供される一般リソース CKR.READALL を使用することもできます。	N

配布指向インストールを実行する場合、さまざまな z/OS イメージにさまざまな CKRSITE パラメーターを使用することがあります。この構成は、イメージごとに別々のライブラリーに CKRSITE モジュールを保管して、JCL または

WPREFIX/UPREFIX パラメーターを使用してこれらのライブラリーを SCKRLOAD ライブラリーに連結することによりセットアップできます。ライン・モードでは、 WPREFIX/UPREFIX パラメーターは SCKRCARL ライブラリーしかサポートしません。また、CKRSITE ディレクトリーを SCKRLOAD ライブラリーに格納することは、 SCKRLOAD ライブラリーが SMP/E により管理されているため、SMP/E 違反となるので注意してください。

付録 B. zSecure のセキュリティー・セットアップ

zSecure の APF 許可機能は、XFACILIT クラスのリソースによって保護されています (ただし、このセットアップを変更した場合は除く)。(その方法については、205 ページの『付録 A. サイト・モジュール』を参照してください。)

zSecure では、SAF を使用してメニューを構成して、どのデータ (プロファイル、規則、SMF レコード) を見ることをユーザーに許可するかを決定します。最低限必要なこととして、UACC=NONE で包括的プロファイル CKF.**、CKG.**、CKR.**、C2R.**、および C2X.**、または同等のリソース規則を作成して、zSecure のすべての機能を使用する資格を持つユーザーに READ 権限を付与します。さらなる詳細化については、 215 ページの『zSecure に固有のセキュリティー・リソース』を参照してください。特に、プロファイル CKG.** (CKRSITE で構成されるクラス内) は必須です。より汎用性の高い *.** などのプロファイルだけでは不十分です。また、zSecure では、FACILITY クラス内に IRR.** プロファイルが存在している必要があります。このプロファイルは、CKRSITE で構成できません。

データ表示制御

zSecure は、システム許可機能 (SAF) を使用して、ユーザーが表示できるデータ (プロファイル、規則、SMF レコード) を決定し、メニューを構成します。ユーザーに表示されるリソースおよびデータの範囲は、CKR.READALL リソースに対するアクセス権限を使用して制御されます。 217 ページの『付録 C. 制限モード』を参照してください。 ISPF ユーザー・インターフェース・メニューは、リソース CKR.OPTION.* を使用して決定され、使用可能な行コマンドは、リソース CKR.ACTION.* を使用して制御されます。すべてのプロファイルを要求する機能 (マスクまたは名前なし) は、CKR.CONTROL.MASK で制御されます。ユーザーには、少なくとも READ 権限が必要です。

どのオプションが表示されるかを構成するリソース

すべてのメニュー・オプションに対して、保護を定義することができます。対応するリソース名に対してユーザーが持っているアクセス権限に応じて、メニュー・オプションは表示される (READ 権限が許可される) か、または非表示になります (アクセス権限がない)。オプションが非表示の場合、ユーザーはそのオプションの実行を許可されていません。

リソース名は、同一の命名規則に従います。

```
first qualifier: 'CKR'
second qualifier: 'OPTION'
third qualifier: main panel option
fourth qualifier: secondary menu option
etc.
```

したがって、メインパネルに対するリソース名は以下のようになります。

```
CKR.OPTION.SE for SETUP
CKR.OPTION.RA for RACF
CKR.OPTION.AA for ACF2
CKR.OPTION.AU for AUDIT
CKR.OPTION.AM for ACCESS
CKR.OPTION.EV for EVENTS
CKR.OPTION.RE for RESOURCE
CKR.OPTION.CO for COMMANDS
CKR.OPTION.IN for INFORMATION
CKR.OPTION.LO for LOCAL
```

SETUP パネルに対するリソース名は以下のとおりです。

```
CKR.OPTION.SE.0 for OPTIONS
CKR.OPTION.SE.1 for INPUT FILES
CKR.OPTION.SE.2 for NEW FILES
CKR.OPTION.SE.3 for PREAMBLE
CKR.OPTION.SE.4 for CONFIRM etc.
```

SETUP DEFAULT パネルに対するリソース名は以下のとおりです。

```
CKR.OPTION.SE.D.0 for SETUP DEFAULT OPTIONS etc.
```

注**:** あるオプション用にチェックされるリソースが RACF または ACF2 で保護されていない場合、そのオプションは表示されます。

zSecure を始動する前にデータ・セットまたは端末に対して DD 名 C2RIMENU を割り振るか、「Setup trace」の下の「Debug action commands」オプションを選択することができます。 (ユーザー・リファレンス・マニュアル を参照してください。)選択されたすべてのメニュー・オプションについて、テスト済みのリソースを記述した 1 行が DD 名に書き込まれます。 C2RIMENU 基本コマンドを使用して、C2RIMENU DD 名を表示することができます。

また、ほとんどの zSecure パネルではコマンド行から FIELDS コマンドを入力すると、使用可能な概要タイプの最新の完全なリストを表示することができます。その次に表示されるパネルで BUILTIN を選択すると、リストが表示されます。

パネル・オプションにアクセスするときの制限があっても、セキュリティー制限があることにならない点に注意してください。ユーザーが独自のパネルを定義できる場合、または zSecure パネルを変更できる場合、そのユーザーはすべてのオプションを実行できます。そのため、厳密なセキュリティー許可が必要です。

どの行コマンドが許可されるかを構成するリソース

さまざまな概要表示にどの行コマンドが許可されるかを構成することができます。これは、データベース照会からの概要、および例えば zSecure Alert の構成が入っているデータ・セットからの概要の両方を保持するものです。コマンドごとに、リソース CKR.ACTION.*overview-type.entity.action-character* に対する READ 権限が検査されます。

概要のタイプとエンティティーのさまざまな組み合わせは、以下のとおりです。

```
AD.F: ACF2_RULE
AI.I: ACF2_INFOLINE
AK.F: ACF2_RULELINE
AL.L: ACF2_LID
AR.I: ACF2_INFORULE
CH.C: Action commands on Change tracking exceptions overview
CL.$: RACF CLASS
```

```
CP.$: CICS_PROGRAM
CR.$: CICS_REGION
CS.$: CICS_TRANSACTION
CT.C: Action commands on Change tracking systems overview
DA.$: DB2_TABLESPACE
DB.$: DB2_BUFFERPOOL
DC.$: DB2_COLLECTION
DD.$: DB2_DATABASE
DE.$: DB2_VARIABLE
DG.$: DB2_STOGROUP
DH.$: DB2_SCHEMA
DJ.$: DB2_JAR
DK.$: DB2_PACKAGE
DN.$: DB2_PLAN
DO.$: DB2_ROUTINE
DQ.$: DB2_SEQUENCE
DR.$: DB2_REGION
DS.$: DSN
DT.$: DB2_TABLE
DY.$: DB2_DATATYPE
FL.$: FIELD
IC.$: SETROPTS_CLASS
MB.$: MEMBER
MC.$: IMS_REGION
MP.$: IMS_PSB
MQ.$: MQ_REGION
MT.$: IMS_TRANSACTION
QC.$: MQ_CONNECT
QH.$: MQ_CHANNEL
QI.$: MQ_INIT
QN.$: MQ_NAMELIST
QP.$: MQ_PROCESS
QQ.$: MQ_QUEUE
QT.$: MQ_TOPIC
RA.$: RACF_ACCESS
R1.$: REPORT_AC1
RC.D: RACF (DATASET entities)
RC.G: RACF (GROUP entities)
RC.R: RACF (RESOURCE entities)
RC.U: RACF (USER entities)
RD.$: REPORT_NONDEFAULT
RO.$: REPORT_OUTOFGROUP
RN.$: REPORT_REDUNDANCY
RP.$: REPORT_PADS
RR.$: REPORT_PROFILE
RS.$: REPORT_SENSITIVE
SC.D: RACF REPORT_SCOPE (DATASET entities)
SC.R: RACF REPORT_SCOPE (RESOURCE entities)
SD.$: SENSDSN
SM.D: SMF (DATASET entities)
SM.G: SMF (GROUP entities)
SM.L: SMF (LOGONID entities)
SM.R: SMF (RESOURCE entities)
SM.U: SMF (USER entities)
SP.$: SPT
ST.$: REPORT_STC
TK.$: ICSF_TOKEN
TR.$: TRUSTED
UN.$: UNIX
ZA.B: zAlert action commands on alert categories display
ZA.C: zAlert action commands on alert configurations display
ZA.D: zAlert action commands on e-mail destination sets display
ZA.R: zAlert action commands on alerts display
```

zSecure を開始する前にデータ・セットまたは端末に対して DD 名 C2RIMENU を割り振るか、「Setup trace」の下の「Debug action commands」オプションを選

択することができます (「ユーザー・リファレンス・マニュアル」を参照)。選択されたすべてのアクション・コマンドについて、テスト済みのリソースを記述した 1 行が DD 名に書き込まれます。 C2RIMENU 基本コマンドを使用して、C2RIMENU DD 名を表示することができます。

アクションの文字または説明を変更するには、「ユーザー・リファレンス・マニュアル」を参照してください。

セキュリティー・データベースへのアクセス

Security zSecure を使用するユーザー ID は、セキュリティー・データベースの読み取り (またはおそらくはコピーまたはアンロード) に、許可が必要です。しかし、これにより機密漏れが起こる可能性があります。 217 ページの『付録 C. 制限モード』では、このタイプの機密漏れを説明し、改善策を説明しています。

zSecure Server の使用時における許可およびユーザー ID のマッピング

リモート・データを使用するため、およびコマンドをルーティングするためには、それぞれの許可が必要です。

- リモート・データ・アクセスの場合、ユーザーにはいくつかの許可が必要です。
  - ユーザーは、リモート宛先にアクセスする許可を持っていなければなりません。
  - ユーザーは、zSecure Server を使用してリモート・データ・セットを使用する許可を持っていなければなりません。
  - 稼働中のデータ・ソース以外のすべてのデータ・セットについて、ユーザーはそのデータ・セットへのアクセス権限を持っていなければなりません。
- ルーティング・コマンドの場合、ユーザーに必要な許可は、選択したルーティング方式によって異なります。
  - zSecure Server ベースのコマンド・ルーティングの場合、ユーザーには適切な zSecure リソースに対するアクセス権限が必要です。このセクションでは、これらのリソースについて説明します。
  - RRSF ベースのコマンド・ルーティングの場合、ユーザーには承認済みのユーザー・アソシエーションが必要です。必要な RRSF 許可について詳しくは、「*RACF* セキュリティー管理者のガイド」および「*RACF* コマンド言語解説書」を参照してください。
  - NJE ベースのコマンド・ルーティングの場合、ユーザーにはジョブをリモート・システムへルーティングする許可が必要です。

ユーザーがリモート・データにアクセスしたり、コマンドのルーティングをしたりできるようにするには、その前にこれらの許可を定義する必要があります。

許可は、ユーザーの**ユーザー ID** を使用して検査されます。リモート・システムでは、許可はそのリモート・システムに定義された**ユーザー ID** を使用して検査されます。リモート・システムの**ユーザー ID** は、リモート・システムに定義された**ユーザー ID** にログオンするために使用された**ユーザー ID** をリンクするマッピング規則から取得されます。この**ユーザー ID** マッピング規則について詳しくは、213 ページの『ユーザー ID マッピング』を参照してください。

現在の ZSECNODE 以外のリモート宛先の場合、リモート宛先への許可は、XFACILIT クラスのプロファイルを使用するか、RRSFDATA リソース・クラスのプロファイルを使用して制御できます。これらのプロファイルは、データ・アクセスおよびコマンド・ルーティングに使用されます。検査は、ユーザーがログオンしたシステムで行われます。宛先が現在の ZSECNODE に定義されているサーバーの場合は、ユーザーはサーバーへのアクセスが自動的に許可されます。 XFACILIT クラスのプロファイルは、リソース CKNADMIN.TONODE.<*node-name*> と一致しなければなりません。このリソース名では、以下の修飾子が使用されます。

CKNADMIN
固定接頭部。

TONODE
宛先ノード検査のための固定修飾子。

node-name
リモート・データに指定された ZSECNODE または指定された ZSECSYS が属する ZSECNODE。

XFACILIT クラス (ただし、これを変更した場合は除き、 205 ページの『付録 A. サイト・モジュール』を参照) にプロファイルが見つからない場合は、RRSFDATA リソース・クラスのプロファイルが使用されます。 RRSFDATA クラスのプロファイルは、リソース DIRECT.<*node-name*> と一致しなければなりません。<*node-name*> の値は、前述のリストで指定された値と同じです。 RRSFDATA プロファイルも見つからない場合は、リモート・システムへのアクセスが許可されます。プロファイルが見つかった場合、ユーザーは、リソースに対する READ 以上のアクセス権限を持っていなければなりません。

宛先サーバー上で、ソース・サーバーについて、同様の許可を実装する必要があります。ユーザーは、少なくとも READ 権限を持っている必要があります。ソース・サーバーが現行サーバーと同じ ZSECNODE に定義されている場合、ユーザーは現行サーバーへのアクセスが自動的に許可されます。アクセス検査に使用されるリソース名は、CKNADMIN.FROMNODE.<*node-name*> です。このリソースで、修飾子は以下のとおりです。

CKNADMIN
固定接頭部。

FROMNODE
ソース・ノード検査のための固定修飾子。

node-name
システム管理者により、ユーザーが照会を実行しているシステムに割り当てられた ZSECNODE。

プロファイルが見つからない場合、ユーザーはこのノードへのアクセスを許可されません。この検査は宛先システムで行われるため、ログオン**ユーザー ID** がマップされる先の**ユーザー ID** は、リソースに対する READ 以上のアクセス権限を持っていなければなりません。

リモート・データ・セットを使用するための許可は、 XFACILIT クラスのプロファイルを使用して制御できます。XFACILIT クラスのプロファイルは、リソース

CKNDSN.<*dstype*>.<*node-name*>.<*system-name*>.<*dsname*> と一致しなければなりません。このリソース名では、以下の修飾子が使用されます。

CKNDSN
固定接頭部。

dstype
データのタイプを記述します。この修飾子は、CARLa ALLOCATE ステートメントの `TYPE= keyword` に使用される値を持っています。値の例として、RACF、CKFREEZE、SMF、および UNLOAD があります。特殊値 DEFTYPE は、CARLa DEFTYPE ステートメントを使用して定義されたすべてのタイプに使用されます。

node-name
データ・セットがあるシステムに使用される `ZSECNODE`。

system-name
データ・セットがあるシステムに使用される `ZSECSYS`。

dsname
リモートにアクセスされるデータ・セットの名前。一部のデータでは、ここで使用される *dsname* は、本当のデータ・セット名ではなく、プレースホルダーです。プレースホルダー ACTIVE、PRIMARY、BACKUP および MANAGED は、正確なデータ・セット名が該当しないデータ・セットに使用されます。リモート・コマンドの場合は、*dsname* CKRCMD が使用されます。データ・セットの名前 MANAGED は、実際のデータ・セットが割り振られない予約名です。

この検査は宛先システムで行われるため、ログオン**ユーザー ID** がマップされる先の**ユーザー ID** は、リソースに対する READ 以上のアクセス権限を持っていなければなりません。

リモート・コマンドの実行も、リモート・システムで、 XFACILIT リソース・クラスの CKNDSN プロファイルを使用して制御されます。このリソース名は、データ・セットへのアクセスに使用されるリソース名に似ています。

CKNDSN.<*dstype*>.<*node-name*>.<*system-name*>.CKRCMD

この修飾子は、前述のリストで説明したものと同じ意味を持っています。最後の修飾子は以下のとおりです。

CKRCMD
このリソースが、コマンドを実行する権限を記述していることを示す固定接尾部。

アクセスされるデータ・セットが `ACTIVE`、`PRIMARY`、`BACKUP`、`MANAGED`、または `CKRCMD` でない場合、ユーザーはそのデータ・セット自体に対するアクセス権限も持っている必要があります。 zSecure Server はユーザーの許可を使用してデータ・セットを開き、通常の DATASET アクセス検査が行われます。ユーザーは、このデータ・セットにアクセスするための十分な許可を持っていなければなりません。持っていない場合、913 OPEN 異常終了の後に、アクセス違反メッセージが発行されます。データ・セットの名前 MANAGED は、実際のデータ・セットが割り振られない予約名です。

ユーザー ID マッピング

RACF データベースが異なればユーザーの命名規則も異なる場合があるため、 **ユーザー ID** マッピング規則を実装することは可能です。インストール済み環境では、いくつかある**ユーザー ID** マッピング・タイプのいずれかを使用している可能性があります。**ユーザー ID** マッピングは、以下の方法のいずれかで実装できます。

- XFACILIT クラス (ただし、これを変更した場合は除き、 205 ページの『付録 A. サイト・モジュール』を参照) のプロファイルを使用する。
- 既存の RRSF ユーザー・アソシエーションを使用する。

XFACILIT クラスのプロファイルは、以下のリソースと一致しなければなりません。

CKNUMAP.<*source-nodename*>.<*source-userid*>.<*target-nodename*>.

このリソース名では、以下の修飾子が使用されます。

CKNUMAP
固定接頭部。

source-nodename
システム管理者により、ユーザーが照会を実行しているシステムに割り当てられた zSecNode。

source-userid
ユーザーがログオンに使用した**ユーザー ID**。

target-nodename
データ・セットがあるシステム、またはコマンドを実行するシステムに使用する zSecNode。

このプロファイルには、リモート・システムで、ユーザーのために使用される**ユーザー ID** を指定する APPLDATA フィールドが必要です。 APPLDATA に可能な値は、以下のとおりです。

=USERID
識別マッピングが使用されます。

other ターゲット・**ユーザー ID** の値。

APPLDATA がない場合、または最初の文字がブランクの場合、ソース・ **ユーザー ID** は受け入れられません。

このようなマッピング規則には総称プロファイルを使用することができます。この方法で、単一のプロファイルを使用して、複数のシステムの複数の**ユーザー ID** をマップすることができます。

ユーザー ID マッピング・プロファイルが見つからない場合、zSecure は既存の RRSF ユーザー・アソシエーションを使用します。ログオン・ユーザーがリモート・**ユーザー ID** の MANAGER-OF または PEER である承認済みアソシエーションのみが考慮されます。 RRSF ユーザー・アソシエーションのセットアップについて詳しくは、「*RACF* セキュリティー管理者のガイド」および「*RACF* コマンド言語解説書」を参照してください。

RRSF ユーザー・アソシエーションに矛盾が見つかると、識別マッピングが使用されます。

CKNUMAP プロファイルがなく、RRSF ユーザー・アソシエーションもない場合に、識別マッピングが使用されます。

その他のセキュリティー・リソース

zSecure は SAF 呼び出しを発行して、メニューを構成し、許可された機能の使用を制限します。すべての SAF 呼び出しは XFACILIT クラスの中にあります。ただし、サイト・モジュールの CLASS オプションをカスタマイズした場合は除きます。 (205 ページの『付録 A. サイト・モジュール』を参照してください。)

- REMOVE USER コマンドを発行する、zSecure Admin コンポーネントのユーザーは、STGADMIN.IGG.DELETE.NOSCRTCH ファシリティー・リソースおよび STGADMIN.IGG.DEFDEL.UALIAS ファシリティー・リソースに対する READ 権限、またはマスター・カタログおよび該当するユーザー・カタログでの ALTER 権限が必要です。これは、VSAM データ・セットのすべてのコンポーネントを削除したり、カタログ別名を削除したりできるようにするために必要です。
- zSecure Admin コンポーネントのユーザーは、データ・セットにコマンド・ストリームを頻繁に作成します。これらのデータ・セットはパスワードを含むことができるため、次の例に示すように、それらの削除時に確実に消去されるようにしてください。

  ```
  ADDSD 'workprefix.C2R*.CKRCMD*.*' UACC(NONE) ERASE
  ADDSD 'workprefix.C2R*.CKR2PASS.*' UACC(NONE) ERASE
  ```

  workprefix が、zSecure 構成の WORKPREF パラメーターで指定されたとおりの ISPF 作業データ・セットの接頭部である場合は、 223 ページの『付録 D. 構成パラメーターと構成メンバー』を参照してください。
- ACF2 のもとで zSecure を実行するとき、C2RIMENU プログラムは SAF 呼び出しを実行できなければなりません。

  ```
  INSERT SAFDEF.C2RIMENU PROGRAM(C2RIMENU)
     RB(C2RIMENU) NOAPFCHK ID(C2RIMENU)
     RACROUTE(REQUEST=AUTH,CLASS=XFACILIT,STATUS=ACCESS)
  ```

  これが行われない場合、すべてのパネル・オプションがすべてのユーザーから見えるようになり、許可されていないオプションを使用しようとしたときにエラー・メッセージが出されます。 XFACILIT 以外のリソース・クラスを使用するためにサイト・モジュールを変更した場合は、これに合わせて上記の SAFDEF を調整する必要があります。
- CKGRACF REFRESH コマンドのユーザーは、 APPL クラスのリソース C2GRACF に対するアクセス権限が必要です。これには、日次 CKGRACF ジョブを実行するユーザー ID も含まれます。このジョブについて詳しくは、 56 ページの『日次の CKGRACF ジョブ実行の要件』を参照してください。

APPL クラスはデフォルトの RC=4 を持ち、対象プロファイルがなくてもプログラムを実行できるようになっています。ただし、C2GRACF リソース (例えば * など) を対象とする APPL プロファイルが存在する場合は、READ 権限が必要です。

- APF 許可された環境で CKRCARLA を実行しているユーザーは、リソース CKR.CKRCARLA.APF に対する READ 権限が必要です。
- RACF Exit Activator プログラムのユーザーは、C2X.exitname での UPDATE 権限が必要です。*exitname* は、「RACF システム・プログラマーズ・ガイド」に説明されている、出口モジュールの名前です。これは、動的活動化が使用されない場合に、対応するモジュールが持つ名前です。例えば、RACF 新規パスワード出口のリソースは C2X.ICHPWX01 です。

どのデータを表示できるか、または更新できるかを指定するリソース

READALL リソースの場合は、 217 ページの『付録 C. 制限モード』を参照してください。このカテゴリーの他のリソースの場合は、ご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」を参照してください。

zSecure Collect 関連のセキュリティー検査

zSecure Collect 関連セキュリティー検査については、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」を参照してください。zSecure Audit for ACF2 または for Top Secret を使用している場合は、これらの製品の「ユーザー・リファレンス・マニュアル」を参照してください。

---

zSecure に固有のセキュリティー・リソース

zSecure は SAF 呼び出しを発行して、メニューを構成し、許可された機能の使用を制限します。すべての SAF 呼び出しは XFACILIT クラスの中にあります。ただし、サイト・モジュールの CLASS オプションをカスタマイズした場合は除きます。 (205 ページの『付録 A. サイト・モジュール』を参照してください。)

付録 C. 制限モード

zSecure は、非制限モードと制限モードの 2 つの異なるモードで使用できます。

- 非制限モードでは、RACF または ACF2 セキュリティー・データベース内のすべての情報がレポートに含まれ、ISPF パネルから、または印刷されたレポートで参照できます。
- 制限モードでは、ユーザーの範囲内のデータだけが報告されます。例えば、制限モードでは、ヘルプ・デスク・オペレーターは、中央管理者が作成できるのと同じレポートを作成したり、また同じデータを参照したりするとはできません。

これら 2 つの操作モード間の選択は、インストール全体で、またはユーザーごと、またはグループごとに行うことができます。

ユーザーに非制限アクセスを許可する実質的な効果は、範囲のない「読み取り専用の」監査員を実際に作成することです。つまり、そのユーザーは、RACF AUDITOR 属性または ACF2 AUDIT 属性を持つユーザーと同じデータとオプションを参照できますが、グローバル・オプションや監査員設定を変更することはできません。

制限モードの条件

制限モードは、以下の方法で決定されます。

1. ユーザーが SIMULATE RESTRICT を指定すると、制限モードがアクティブになります。

   これは、SIMULATE RESTRICT を指定しなかった場合の動作に関する情報を出力する、以下のいずれかのメッセージ・バリアントにより表示されます。

   CKR0031 Restricted mode by simulation, although user *userid* has privilege *privilege*
   CKR0031 Restricted mode by simulation, although user *userid* READ access to *class profile*
   CKR0031 Restricted mode by simulation for user *userid*, although no profile *class profile*
2. いずれかの ALLOC ステートメントがリモート・ノードを参照しており、そのノードのユーザー ID (マップされているユーザー ID を含む) が SPECIAL 特権、AUDIT 特権、ROAUDIT 特権のいずれも所持しておらず、そのリモート・ノード上のセキュリティー・データベース内の CKR.READALL に対して READ 権限がない場合、制限モードがアクティブになります。リモート・ノード上の CKR.READALL リソースのクラスは、そのリモート・ノード上のサイト・モジュールによって決まります。 205 ページの『付録 A. サイト・モジュール』を参照してください。

   以下のいずれかのメッセージ・バリアント内に、制限モードがアクティブになっていることが表示されます。これらのメッセージ・バリアントには、リモート・ノードの制限が存在しない場合の動作に関する情報が記載されます。

CKR0031 Restricted mode by remote node, although user *userid* has privilege *privilege*
CKR0031 Restricted mode by remote node, although user *userid* READ access to *class profile*
CKR0031 Restricted mode by remote node for user *userid*, although no profile *class profile*

上記の 1 (217 ページ) と 2 (217 ページ) の両方に該当する場合、メッセージには simulation and remote node というセンテンスが表示されます。類似したメッセージが 2 回表示されることはありません。

3. 上記の 1 と 2 に該当せず、照会を実行しているシステム上のユーザーに対して、SPECIAL 属性、AUDITOR 属性、ROAUDIT 属性のいずれかが設定されている場合は、非制限モードがアクティブになります。これは以下のメッセージで示されます。

   CKR0031 Unrestricted mode active, user *userid* has privilege *privilege*

4. 上記すべてに該当しない場合は、XFACILIT クラス内で CKR.READALL リソースに対するアクセスがテストされます (XFACILIT クラスが変更されていない場合。詳しくは、 205 ページの『付録 A. サイト・モジュール』を参照)。プロファイルまたはクラスのデフォルト RC 経由で SAF 呼び出しによってアクセス権限が判断される場合、モードは以下のようになります。

   a. アクセス権限がない場合、制限モードがアクティブになります。これは以下のメッセージで示されます。

      CKR0031 Restricted mode active, user *userid* no READ access to *class profile*

   b. アクセス権限が READ 権限以上である場合、非制限モードがアクティブになります。これは以下のメッセージで示されます。

      CKR0031 Unrestricted mode active, user *userid* READ access to *class profile*

5. 上記すべてに該当しない場合 (つまり、CKR.READALL に対するアクセス権限がまだ決定されない場合) は、以下に示す条件の 1 つ以上に該当する場合に、制限モードがアクティブになります。

   a. RACF システムが稼働中で、入力 (の一部) に PADS 経由でのみアクセスできる場合 (詳しくは、 220 ページの『プログラム制御および PADS アクセスのセットアップ』を参照)。これが該当するのは、セキュリティー・データベース、CKFREEZE、SMF、DEFTYPE、アクセス・モニター入力ファイルです。これは以下のメッセージで示されます。

      CKR0031 Restricted mode active because of [PADS | program pathing] user *userid*

   b. サイト・モジュール (205 ページの『付録 A. サイト・モジュール』を参照) が制限モードを指定するように構成されている。これは以下のメッセージで示されます。

      CKR0031 Restricted mode active by installation option; user *userid*

6. 上記すべてに該当しない場合は、非制限モードがアクティブになります。これは以下のメッセージで示されます。

   CKR0031 Unrestricted mode active; user *userid*

注: RACF に対象プロファイルが存在しない場合で、かつサイト・モジュール内にデフォルトの戻りコード 4 のリソース・クラスが存在する場合には、アクセスは未決です。デフォルト・クラスは XFACILIT で、これはデフォルトの戻りコード 8 を持ち、アクセスが禁止されることを意味します。

上記のように、稼働中のシステムで SPECIAL 属性、AUDITOR 属性、または ROAUDIT 属性が設定されているユーザーの操作モードは、デフォルトで非制限モードになりますが、SIM RESTRICT を使用して制限モードに変更することができます。SIM RESTRICT を使用する場合は、AUDITOR 属性も ROAUDIT 属性も設定されていない SPECIAL ユーザーに対して、グローバル監査フィールドが非表示になります。

CKNSERVE を使用してリモート・システムにアクセスする場合は、システム全体のプロパティーと、リモート・システム上のマップされたユーザー ID の CKR.READALL 権限に基づいて、これまでに説明したような方法でアクセス権限が判断されます。

1 回の実行で複数のセキュリティー・データベース (リモートのセキュリティー・データベースを含む) を分析する場合、制限モードは複合システムまたはファイルに固有の条件ではないことに注意してください。照会対象であるいずれかのローカル・システムまたはリモート・システム上の不十分なユーザー権限に基づき制限モードがアクティブになると、すべての複合システムと該当するファイルに適用されます。

制限モードで実行する場合に使用される有効範囲は、非制限モードのトラステッド・レポートの有効範囲よりも狭くなります。そのため、有効範囲に関連する情報を使用するレポートの場合、レポートに表示されるレコードの件数が少なくなることがあります。この削減された有効範囲は、SUPPRESS REASON= (SELFCONNECT, PWDCHANGE, WARN, NOPROFILE, CKGRACMAP CKGRACDCERT) を有効範囲レポートに追加した場合と同じです。有効範囲ツリーを必要とする機能も使用している場合、有効範囲が狭くなることを示す CKR2245 メッセージが発行されます。

制限モードの効果: ユーザーの範囲

制限モードでのユーザーの範囲は、検査されているデータベースから評価されます。入力ソースにセキュリティー・データベースが含まれない場合、稼働中システム上のデータベースが範囲の評価に使用されます。

RACF 入力ソースについては、(いくつかの) CKG 範囲リソースに対する READ アクセス権限を認可することにより、ユーザーの範囲を拡大することができます。この方法では、きめ細かなアクセス許可を持つ監査員を定義できます。詳細については、ユーザー・リファレンス・マニュアル を参照してください。アクセス権限の認可は、稼働中データベースを入力として使用するシステム・イメージに対してのみ実行されるため、旧アンロードに対しては効果がありません。

プログラム制御および PADS アクセスのセットアップ

このタスクについて

この情報は、ご使用の稼働中システムが RACF を使用する場合にのみ適用されます。

最高レベルのセキュリティーは、データ・セットへのプログラム・アクセス (PADS) を使用することにより達成されます。PADS なしでは、ユーザーは、例えば ISPF ブラウズを使用して、RACF データベースを検査することも、また非制限モードで実行できるシステムにデータベースをコピーすることさえも可能です。ただし、RACF が実装する条件付きアクセスの方法のため、これは非常に使いにくいオプションでもあります。PADS の代替として、自己接続モードで zSecure Server を利用してセキュリティー・データベースにアクセスできます。 73 ページの『zSecure Server を使用したセキュリティー・データベースへのアクセスの必要性の限定』を参照してください。

PADS アクセス、または zSecure Server を介したアクセスを、CKR.READALL リソースの使用と組み合わせて、選択した (またはすべての) ユーザーに対する制限モードをオーバーライドできます。

条件付きアクセスまたは PADS モードを使用して、操作のために zSecure をセットアップする場合には、プログラム・クラスにプロファイルを定義し、RACF プログラム制御を活動化する必要があります。多くのインストールでは、これらのステップの大部分を USS (UNIX System Services) の実装の一部として実行します。

手順

以下のステップを使用して、条件付きアクセスまたは PADS モードをセットアップします。

1. 「*RACF* セキュリティー管理者のガイド」(z/OS RACF 用は SA88-5804) の説明に従って、プログラム制御およびデータ・セットへのプログラム・アクセスの原理を把握します。
2. インストール済み環境で使用している RACF プログラム制御が BASIC モードか、あるいは ENHANCED かを判断します。
   - ご使用のシステムで BASIC プログラム制御モードが使用されている場合、次のようなコマンドで、必須の PROGRAM プロファイルを追加する必要があります。

     ```
     RDEF PROGRAM CKR* ADDMEM('CKR.SCKRLOAD'//NOPADCHK)
     ```

   - ご使用のシステムで ENHANCED プログラム制御モード (z/OS 1.4 で使用可能) が使用されている場合、次のようなコマンドで、必須の PROGRAM プロファイルを追加することができます。

     ```
     RDEF PROGRAM CKR* ADDMEM('CKR.SCKRLOAD'//NOPADCHK) APPLDATA('MAIN')
     RALT PROGRAM **   ADDMEM('CKR.SCKRLOAD'//NOPADCHK)
     ```

   さまざまなロード・ライブラリー (例えば、複数バージョンのサイト・モジュール用に複数のロード・ライブラリーを作成する可能性がある場合、およびこれら

をメイン zSecure ロード・ライブラリーに連結する場合)、プログラム制御する必要のある各ロード・ライブラリーに対して ADDMEM を指定する必要があります。

ロード・モジュールに別名をセットアップした場合には、別名を対象とするプロファイルも作成します。

旧システムでは、以前のコマンド例内で、スラッシュ (//) の間にボリューム通し番号を挿入する必要があります。これにより、データ・セットが SMS 管理対象ボリューム上に配置されている場合、問題が発生する可能性があります。その場合、SMS がデータを別のボリュームに移動するのを防止するため、データ・セットは、確実に Guaranteed Space 属性を持つストレージ・クラス (または非 SMS 管理対象ボリューム) に割り当てます。

TSO/ISPF を介して zSecure を対話式に使用する場合には、zSecure の他のいくつかの実行可能モジュール用にもプログラム・プロファイルを追加します。この例では、** を使用して、関連するすべてのロード・モジュールが記述されています。または、例にあるように、PROGRAM プロファイル * または ** の定義にライブラリー全体を追加できます。

3. PADS モードでデータベースへのアクセスを許可されたユーザー用に使用される許可グループを追加します。
4. 条件付きアクセス・リストを、RACF データベースを記述するプロファイルに追加します。ユーザーに、バックアップ・データベースの使用を制限する場合があります。このためには、まずプロファイルを追加する必要があります。 サンプル・コマンドは次のとおりです。

   ```
   PE 'databaseprofile' WHEN(PROGRAM(CKRCARLA)) ID(authgroup)
   ```

5. SETROPTS LIST を発行してプログラム制御がアクティブであることを確認し、出力が WHEN(PROGRAM) を指定していることを検査します。そうでない場合には、プログラム制御の導入をスケジュールに入れてください。(まず、PROGRAM クラスの現行内容を検討します。) プログラム制御は、次のように活動化されます。

   ```
   SETROPTS WHEN(PROGRAM)
   ```

6. ご使用のサイト・リンク・リストから LPA にどの程度移動したかに応じて、オペレーティング・システム・モジュールを記述する PROGRAM プロファイルを追加する必要がある場合があります。(LPA モジュールについては、PROGRAM プロファイルは必要ありません。) 一般に、発行されるコマンドには次のものがあります。

   ```
   RDEF PROGRAM * ADDMEM('SYS1.LINKLIB'//NOPADCHK) UACC(READ)
   RALT PROGRAM * ADDMEM('SYS1.CMDLIB'//NOPADCHK)
   RALT PROGRAM * ADDMEM('SYS1.MIGLIB'//NOPADCHK)
   RALT PROGRAM * ADDMEM('SYS1.CSSLIB'//NOPADCHK)
   RALT PROGRAM * ADDMEM('cee.version.SCEERUN'//NOPADCHK)
   RALT PROGRAM * ADDMEM('TCPIP.SEZALINK'//NOPADCHK)
   RALT PROGRAM * ADDMEM('TCPIP.SEZATCP'//NOPADCHK)
   ```

PADS モードで対話式に 実行したい場合には、ISPF および PDF リンク・リスト・ライブラリーも追加する必要があります。ダーティー (非制御) モジュールのロード時には、多くの場合、次回の試行で再びログオンすることが必要になります。ときには、ISPF を終了した後、TSOEXEC を通して ISPF を起動することで、環境の制御を取り戻すのに十分な場合があります。

```
RALT PROGRAM * ADDMEM('CKR.SCKRLOAD'//NOPADDCHK)    /* IBM Security zSecure */
RALT PROGRAM * ADDMEM('FAN130.SEAGLMD//NOPADCHK)          /* REXX     */
RALT PROGRAM * ADDMEM('ISP.SISPLOAD//NOPADCHK)            /* ISPF/PDF */
```

SYS1.LINKLIB 内のすべてのモジュールに対して PROGRAM * または ** を定義する場合、削減された UACC を持つプログラム ICHDSM00 と IRRDPI00 用に 2 つの固有のプロファイルを作成すると考えます。これらの 2 つのプログラムは、ユーザーにプログラムの実行を許可するために、一致する PROGRAM プロファイルの存在を検査します。PROGRAM プロファイルが存在しない場合には、監査員だけが、ICHDSM00 (DSMON) の実行を認可されます。しかし、総称プロファイル * が UACC(READ) 付きで定義されている場合、すべてのユーザーが、ICHDSM00 の実行を許可されます。したがって、以下のコマンドも実行することが推奨されます。

```
RDEF PROGRAM ICHDSM00 UACC(NONE) ADDMEM('SYS1.LINKLIB'/'******'/NOPADCHK)
RDEF PROGRAM IRRDPI00 UACC(NONE) ADDMEM('SYS1.LINKLIB'/'******'/NOPADCHK)
PE ICHDSM00 CLASS(PROGRAM) ID(your-auditors) ACCESS(READ)
PE IRRDPI00 CLASS(PROGRAM) ID(your-dynamic-parse-initialization-userid) ACCESS(READ)
```

これらのコマンドについて詳しくは、「*RACF* セキュリティー管理者のガイド」のプログラム制御に関するセクションを参照してください。

7. システム内の任意の PROGRAM プロファイルに対する変更を活動化するには、次のコマンドを発行する必要があります。

   ```
   SETROPTS REFRESH WHEN(PROGRAM)
   ```

8. まず、バッチ・ジョブを通して PADS アクセスを試行します。これが機能する場合には、対話式アクセスに移動できます。まず、最小のクリーンな環境で機能するようにするため、TSO にログオンした直後で、ISPF を始動する前に、CKR コマンド (またはユーザーのローカル・コピー) を発行します。この方法で起動された場合、CKR は ISPLLIB ファイルを解放してダーティー・モジュールを確実に阻止し、また TSOEXEC コマンドを通してプログラムを 1 次 ISPF アプリケーションとして起動します。

   他の ISPF アプリケーション (SDSF など) は、TSOEXEC コマンドを使用してもクリーンアップできない環境を作成する可能性があることに注意する必要があります。この状態では、もう一度ログオンする必要があります。最もクリーンなモードで動作することを確認した後、独自の ISPF 環境を部分ごとに追加で戻して、使用可能な動作環境を獲得し、また 913 または 306 の異常終了がどこで始まったかを確認できます。

   代行受信された各 913 異常終了により、SYSPRINT ファイル内に、Job Pack Queue モジュールのデバッグ表示が生成されます。(これは、ISPF 下で、SYSPRINT 基本コマンドを使用して確認できます。)

   RACF ICH420I メッセージを使用して、ダーティー環境の原因を判別することもできます。

付録 D. 構成パラメーターと構成メンバー

34 ページの『zSecure 構成 データ・セットの作成』で説明されているように、ジョブ CKRZPOST は zSecure のスターター構成を作成します。必要ならば追加の構成を作成できます。例えば、z/OS イメージごと、コミュニティーごと、あるいは専用の構成を zSecure Alert、zSecure Visual、zSecure Adapters for QRadar SIEM、トラック変更などに提供する目的で、別個の構成を作成したい場合があります。

バッチおよび ISPF インターフェースの両方による使用が可能となるように、構成は JCL SET ステートメントを使用する必要があります。ISPF インターフェースが SET ステートメントを解釈できるようにするには、各パラメーターを別々の SET ステートメントに指定する必要があります。パラメーターは大/小文字を区別しません。ただし、UNIX ファイル名と DESC パラメーターについては、ISPF インターフェースが使用する場合に限り大/小文字を区別しません。JCL で使用されるパラメーターは JCL 標準に準拠する必要があります。

INCLUDE ステートメント (JCL の場合と同じ構文) は、構成データ・セットからのメンバーを組み込むために ISPF インターフェースによってサポートされています。ISPF インターフェースでは、JCL での場合と異なり、構成データ・セットは連結の一部になることは決してありません。構成データ・セットは、共通パラメーターを共通メンバーに保管するのと、必要に応じて必須パラメーターを指定変更するのに役立ちます。例えば、ヘルプ・デスク構成のユーザーは、zSecure を RA.H オプションで始める必要があります。他のすべてのオプションの構成はデフォルト設定から変更する必要はありません。このような構成は、CKR のコピー (この先を参照) で C2REMAIN 呼び出しを指定変更することによって、あるいは以下のような別の構成を指定することによって作成できます。

```
// INCLUDE MEMBER=your-common-member
// SET STARTTRX='MENU(RA.H)'
```

最後の割り当ては、それより前にあるすべての割り当てを指定変更します。

ISPF インターフェースは、シンボル &SYSUID. (ピリオドを含む)、アクティブ Parmlib メンバー IEASYMxx に指定されているシステム・シンボル、および REXX MVSVAR 機能が受け入れるすべてのシンボルをサポートします。他の JCL パラメーターおよび継続行は ISPF インターフェースではサポートされていません。サポートされないパラメーターと廃止パラメーターがあると、1 次メニューにメッセージが出されることがありますが、それらは特に機能に影響することはないので、異なるリリース間で構成を共有することができます。

構成にリストされているすべてのパラメーターも、C2REMAIN の呼び出し時の指定変更として (TSO/E 規則で) コーディングが可能です。一般に、ユーザーは C2REMAIN を使用する必要はありません。代わりに、REXX exec CKR またはそのコピーを開始することができます。例えば、単純な管理用タスクを対象に、指定変更パラメーター STARTTRX(MENU(RA.Q) のみを追加する REXX exec CKRQ を作

成できます。シンボリック・パラメーターは指定変更の一部としてサポートされていないので、代わりに CKR (そのコピー) 内のパラメーターを解決しなければなりません。

zSecure で出荷される CKR のバージョンは同じ指定変更をサポートします。例えば、Setup Default を特定の SE.D データ・セットに対して実行するために、以下を呼び出すことができます。

```
CKR PROFDSN('HELPDESK.CKRPROF')
```

以下のパラメーターがサポートされます。

BLKSIZE

VB データ・セットの BLKSIZE。システムが決定したブロック・サイズ (SDB) がシステム上でサポートされている場合は、これを省略するか、または BLKSIZE=0 を指定できます。それ以外の場合は、作業データ・セットが 3380 互換装置上で作成されるなら BLKSIZE=23476 を、3390 互換装置には BLKSIZE=27998 を指定することを提案します。

CKACUST

このパラメーターは、zSecure Audit オプション AU.R (ルール・ベースの準拠性評価) の「準拠した許可 ID 母集団」メンバーのデータ・セット名を指定します。ユーザーは、オプション CO.1 または SE.8 を使用して構成メンバーで指定したライブラリーの前に独自の CKACUST ライブラリーを連結できます。ご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」のトピック『CO.1 ライブラリー - データ・セット選択』を参照してください。

CPREFIX

このパラメーターは、zSecure ソフトウェアを含むデータ・セットの開始修飾子を指定します。ご使用の構成がソフトウェア・アップグレードの前後で使用できるようにするには、構成に別名を使用することを考慮してください。

代わりに、リリース ID をデータ・セット名に保持して、あるリリースから次のリリースへすべてのユーザーを切り替えたいときに、その ID を変更します。ただし、複数の構成がある場合は、それらをすべて更新する必要があります。

C2ECUST

z/OS Agent for Tivoli® Security Information and Event Manager 用のインストール提供 CARLa の区分データ・セット。

C2ECUST パラメーターは使用されなくなっています。ただし、zSecure 2.1.0 以前で同じ構成を使用する場合は、ご使用状況に関連がある可能性があります。

C2ELVLLQ

このパラメーターは、C2ELVPFX パラメーターによって参照される同じデータ・セットに低位修飾子を提供します。このオプション・パラメーターを使用して、SMF データ・セットの名前をデータ・セット命名規則に準拠させることができます。これは、低位修飾子に基づいて処理の決定を行う

ACS ルーチンがある場合に行うことがあります。非ブランク C2ELVLLQ を指定する場合は、例えば、.daily_smfdata のように、先頭文字がピリオドの値を指定してください。

C2ELVPFX

Agent for Tivoli Security Information and Event Manager が使用する SMF データ・セットの接頭部として使用する 1 つ以上の修飾子。このパラメーターは、このコンポーネントの使用時にのみ必須です。この接頭部を持つデータ・セットは SMF 累積処理で作成されてから、エージェントによって読み取られ、削除されます。必ず、エージェント所有のデータ・セットのみが接頭部 C2ELVPFX の下に存在するようにします。エージェントのユーザー ID を高位修飾子として使用することをお勧めします。

C2EPATH

Agent for Tivoli Security Information and Event Manager のエージェント・ルート・ディレクトリーのパス。このコンポーネントの使用時にのみ必須です。複数のエージェントを実行する場合は、それぞれ 1 つずつに、その独自のエージェント・ルートが必要です。

C2EQCUST

このパラメーターは、QRadar SIEM のデータ準備に適用されます。 189 ページの『収集プロセスのセットアップ』を参照してください。

C2EQPATH

このパラメーターは、QRadar SIEM のデータ準備に適用されます。 189 ページの『収集プロセスのセットアップ』を参照してください。

C2ESW

z/OS Agent for Tivoli Security Information and Event Manager ソフトウェアをアンパックしたディレクトリーのパス。複数の z/OS エージェントが、このディレクトリーを共有できます。このパラメーターは、このコンポーネントの使用時に必須です。

C2PACPRM

アクセス・モニター機能の構成パラメーター用のパラメーターを含むデータ・セットの名前。データ・セットは通常、ジョブ CKRZPOST によって作成され、アクセス・モニター・アドレス・スペースの JCL の PARMLIB DD ステートメントおよび SC2PCUST DD ステートメントによって参照されます。詳しくは、 75 ページの『第 10 章 zSecure Admin アクセス・モニターのセットアップ』を参照してください。

C2PCUST

zSecure Alert コンポーネントの使用時にのみ必須です。アラート CARLa および zSecure Alert パラメーター・ファイルが ISPF インターフェースによって生成され、このデータ・セットに書き込まれます。アラート定義は ISPF テーブルに保管され、それらもこのデータ・セットに書き込まれます。このデータ・セットは、zSecure Alert 開始タスクの SC2PSAMP DD に割り振る必要があります。詳しくは、zSecure Alert マニュアルを参照してください。

C2POLICE

zSecure Alert 開始タスクの名前。デフォルト名は C2POLICE です。このコンポーネントの使用時にのみ必須です。

C2RSERVE

C2RSERVE は、Visual Server インスタンスの Server ルート・ディレクトリーです。特定のサーバーが使用するすべてのデータが、このディレクトリーでアンカーされます。複数のサーバーを実行する場合は、それぞれのサーバーで C2RSERVE に、その独自の値が必要です。この要件を満たすには、通常はサーバーごとに別々の zSecure 構成を作成します。代わりに、共通の zSecure 構成をすべてのサーバーに使用し、システム・シンボルを C2RSERVE パラメーターの一部として使用できます。

このパラメーターは、zSecure Visual コンポーネントにのみ適用されます。追加情報については、 141 ページの『第 13 章 zSecure Visual Server のセットアップおよび使用』を参照してください。

C2RWCUST

このパラメーターは、Visual Server のローカル CARLa および CKGRACF 制御ステートメントのデータ・セットを指定します。新規サーバーでは、ジョブ CKRZPOST が、メイン構成 (例えば、C2R$PARM) が存在するデータ・セット名に埋め込まれています。CKRZPOST の実行については、 34 ページの『zSecure 構成 データ・セットの作成』を参照してください。

希望する場合には、以下のメンバーがカスタマイズに使用できます。

C2RWEXG1

クライアントが開始するトランザクション中に組み込まれる CKGRACF コマンド。

C2RWEXR1

クライアントが開始するトランザクション中に組み込まれる CARLa。

C2RWASSC

C2RWASSC メンバーの指定は、Visual クライアントでサイト固有のユーザー・データの表示を実装する場合にのみ 必要です。Visual クライアントでサイト固有のユーザー・データの表示を構成する方法については、 160 ページの『サイト固有のユーザー・データ』を参照してください。このメンバーは、CARLa ALLOCATION (ALLOC) ステートメントでアソシエーション構成ファイルの場所を指定します。このステートメントの形式は、以下のとおりです。

```
ALLOC TYPE=SITE_ASSOCIATIONS DSN='associations.file'
```

ここで、

SITE_ASSOCIATIONS

Visual クライアントは、この必須キーワードを使用して、指定されたアソシエーション・ファイルの内容を参照します。アソシエーション・ファイルは、Visual クライアントでサイト定義のユーザー情報を表示するために使用される顧客データ・ファイルと表示フォーマット・ファイルの名前を指定します。

associations.file

アソシエーション・ファイルのサイト定義名を指定します。

新規サーバーでは、空のメンバーがジョブ CKRZPOST によって作成されます。既存のサーバーでは、CKRZPOST は更新を行わないため、カスタマイズした構成の上書きは行われません。現在 zSecure 1.11 以前で稼働しているサーバーをアップグレードするときは、これらのメンバーを SCKRCARL ライブラリーからコピーして、C2RWCUST パラメーターを zSecure 構成に追加します。また、Visual Server をサーバー・コーディングのその他と同じレベルの JCL で実行することを確認します。

zSecure の複数システム機能を多重システム・サーバーの非デフォルト・トークンと一緒に使用する場合は、トークン付きの OPTION ステートメントをメンバー C2RWEXG1 および C2RWEXR1 に追加します。 59 ページの『第 9 章 リモート・データ・アクセスおよびコマンド・ルーティングのためのセットアップ』を参照してください。

このパラメーターは、zSecure Visual コンポーネントにのみ適用されます。追加情報については、 141 ページの『第 13 章 zSecure Visual Server のセットアップおよび使用』を参照してください。

C2RW131A = [ON | OFF]

このパラメーターが ON の場合、Visual Server とそのクライアント間の暗号化は NIST 800-131A 準拠になります。つまり、NIST Special Publication 800-131A (米国連邦情報・技術局発行) に準拠していない暗号化アルゴリズムは、受け入れられなくなります。

アップグレードの際、すべてのクライアントを zSecure Visual Client ソフトウェアの 2.1.0 レベル以上にアップグレードして、その後でクライアント/サーバー接続時に証明書をアップグレードし終えるまで、C2RW131A を ON に設定しないでください。

注**:** 通常、証明書のアップグレードにかかる時間は、クライアント/サーバー接続時間の 30 分以下です。ただし、上限の時間制限はありません。すべてのクライアントがその証明書をアップグレードするには、サーバーを非 NIST 800-131A モードで数日間または数週間実行することで普通は十分です。いずれかのワークステーションがそのアップグレードを非 NIST 800-131A 期間に完了しない場合、その原因は、計算にかかる時間が長すぎるのではなく、まったく接続していないことによる可能性が高いといえます。このようなワークステーションには新しい初期パスワードが必要です。 151 ページの『サーバーによるクライアントの認識』を参照してください。

このパラメーターが OFF の場合は、古い暗号化アルゴリズムが受け入れられます。この設定は、以下の目的で使用します。

- これまでバージョン 1.11.0 からバージョン 1.13.1 までであったサーバーの run ディレクトリーのアップグレード。
- zSecure Visual 1.11.0 から 1.13.1 までのレベルのクライアント・ソフトウェアを使用して接続するクライアント。
- 古いクライアントを zSecure Visual 2.1.0 以上にアップグレードした後の最初の接続 (既存の証明書を引き続き使用したい場合)。

アップグレード済みクライアントの初回接続の前に C2RW131A を ON に設定した場合、クライアントはその古い証明書を使用することも、アップグレードすることもできません。このようなことが起きた場合は、C2RW131A

を OFF に切り替えて戻してから、サーバーを停止して再始動します。それらのアクションが受け入れ不可の場合は、クライアントに対して新しい初期パスワードを発行する必要があります。 151 ページの『サーバーによるクライアントの認識』を参照してください。

注: C2RW131A パラメーターの値を変更した後で、その変更を有効にするためにサーバーを再始動する必要があります。

このパラメーターは、zSecure Visual コンポーネントにのみ適用されます。追加情報については、 141 ページの『第 13 章 zSecure Visual Server のセットアップおよび使用』を参照してください。

C2RWIN

C2RWIN は、zSecure Visual Server ソフトウェアが存在するディレクトリーです。同じレベルの製品を実行する条件下では、複数のサーバーが、このディレクトリーを共有できます。zSecure Visual Server はこのディレクトリーへの書き込みを行わないので、製品インストールの完了後にそのソフトウェアが読み取り専用で存在するファイル・システムをマウントできます。

C2RWIN パラメーターは、zSecure Visual を ISPF 下で使用して最初のクライアントを構成する場合にも必須です。 151 ページの『サーバーによるクライアントの認識』を参照してください。

このパラメーターは、zSecure Visual コンポーネントにのみ適用されます。追加情報については、 141 ページの『第 13 章 zSecure Visual Server のセットアップおよび使用』を参照してください。

C2XEXITS = [ACTIV | INACT]

このパラメーターは、Tivoli Security Information and Event Manager による zSecure 提供 ICHPWX02 出口のアクティブ化を制御します。

このパラメーターは使用されなくなっています。互換性の理由で保持されています。

CKNSVPRM

このパラメーターは、zSecure Server の構成ステートメントのデータ・セットを指定します。新規サーバーでは、ジョブ CKRZPOST が、メイン構成 (例えば、C2R$PARM) が存在するデータ・セット名に埋め込まれています。CKRZPOST の実行については、 34 ページの『zSecure 構成 データ・セットの作成』を参照してください。

このデータ・セットは、 59 ページの『第 9 章 リモート・データ・アクセスおよびコマンド・ルーティングのためのセットアップ』で説明されているように、zSecure Server プロシージャーの PPARM および PCOMMON パラメーターによって示される 2 つのメンバーを含む必要があります。

CKQCUST

このパラメーターは、QRadar SIEM のデータ準備に適用されます。 189 ページの『収集プロセスのセットアップ』を参照してください。

CKQPATH

このパラメーターは、QRadar SIEM のデータ準備に適用されます。 189 ページの『収集プロセスのセットアップ』を参照してください。

DATACLAS、STORCLAS、MGMTCLAS、TEMPUNIT

ISPF 作業データ・セットの割り振り用のデータ・クラス、ストレージ・クラス、管理クラス、および総称装置名または名非公式装置名。SMS では、これらのパラメーターは ACS ルーチンに渡されます。パラメーター TEMPUNIT は、一時データ・セットの割り振り時にのみ使用されます。ご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」を参照してください。TEMPUNIT を空のままにしたか、またはそれが指定されていない場合は、UNIT パラメーターの値が使用されます。

DPREF

SCKRSAMP のバッチ・ジョブで作成されたデータ・セットの接頭部。

EARLYWRN

サポートされないパラメーターまたは廃止パラメーターが構成メンバーにあるときにメッセージを受信する予定のユーザー ID のリスト。複数のユーザー ID を指定する場合は、それらをコンマで区切ります。例えば、`'ADMIN1,ADMIN2,ADMIN3'` のように、ユーザー ID のリスト全体を引用符で囲みます。このパラメーターを空のままにした場合、すべてのユーザーがこのメッセージを受信します。

INIT 同一ユーザーによる以前のセッションからの設定を保持するかどうかを示すために、`YES` (または `RESET`) あるいは `NO` にすることができます。

YES/RESET

すべてのパラメーターをそのデフォルトにリセットします。これらの値は、システム・デフォルトか、`SETUP DEFAULT` で設定された値のいずれかです。

NO 以前のセッションからの値 (ユーザー値) が使用されます。

JES このパラメーターは JES レベルを指定します。値は `2` または `3` で、それぞれ JES2 と JES3 を指します。このパラメーターは zSecure によって生成される JCL のタイプに影響します。

LIBDEF

LIBDEF パラメーターは、`ISPEXEC LIBDEF` を zSecure ユーザーおよび共通ライブラリーに発行する必要があるかどうかを示します。値は `YES` または `NO` です。デフォルト値は `YES` です。`LIBDEF=NO` がコーディングされた場合は、ライブラリーを ISPF に事前割り振りする必要があります。`DDNAME ISPTABLE` は、必ず `ISPEXEC LIBDEF` によって割り振られるので、事前割り振りすることはできません。

PROFDSN

`PROFDSN` パラメーターは、ISPF インターフェースをカスタマイズするために使用されるデータ・セットを指定します。指定されたデータ・セットの内容は、`SETUP DEFAULTS` ステートメントによって更新されます。区分データ・セットを `LRECL=80` および `RECFM=FB` で指定します。SETUP DEFAULT オプションは、このデータ・セットが指定されないと使用不可にされます。データ・セットが `PROFDSN` で指定されたが、そのデータ・セットが使用不可の場合、ISPF インターフェースは、意図しない設定 (例えば、間違った入力) をユーザーが誤って処理することがないように異常終了します。

STARTTRX='MENU(menu)' | STARTTRX='CMD(command)'
ISPF インターフェースの開始時に実行したいトランザクション。

MENU:
AU.S または CO のような、デフォルトの 1 次メニューで有効な任意のメニュー (2 レベルまで)。

CMD:
CARLA または RESULTS のような、デフォルトの 1 次メニューで有効な zSecure または TSO コマンド。複数のコマンドをセミコロンで区切って指定することができます。

SIMESM={RACF|ACF2|TSS}
このオプション・パラメーターは、ISPF インターフェース (特に、zSecure Alert の構成パネル) を、それが RACF でそれぞれ実行されたかのように動作させます。ACF2 がアクティブ外部セキュリティー・マネージャーです。このように、例えば、RACF 下の TSO セッションで実行しながら、zSecure Alert 構成を ACF2 に構成することができます。デフォルトでは、アクティブ外部セキュリティー・マネージャーが使用されます。

SYS 分析するシステムを識別します。それは、CKFREEZE および UNLOAD データ・セットの作成時に修飾子として使用され、さらに生成されたコマンドなどが保管される中間データ・セット用に使用されます。インストール・プロセスは、S が先頭に付いた SMF システム ID (SMF システム ID が数字で開始するため無効なデータ・セット名になる場合に備えて) でサンプル構成を更新します。このパラメーターは、CKRPARM データ・セットをインストール・システムから別のシステムに配布する場合には変更する必要があります。

UNIT UNLOAD、CKFREEZE、および永続 ISPF 作業データ・セット、例えば、SYSDA、DISK、または DASD に対する総称装置名または名非公式装置名。

UPREFIX
共通データ・セットに加えて使用する必要のあるインストールまたはユーザーに固有の zSecure ライブラリーを示すために指定できます。ISPF インターフェースは追加のライブラリーを検索します。それらのライブラリーは、存在する場合、対応する zSecure 共通ライブラリーの前に連結されます。検索対象のライブラリー名は、以下のとおりです。

```
&UPREFIX..SCKRPLIB
&UPREFIX..SCKRMLIB
&UPREFIX..SCKRSLIB
&UPREFIX..SCKRTLIB
&UPREFIX..SCKRCLIB
&UPREFIX..SCKRLOAD
&UPREFIX..SCKRCARL
&UPREFIX..SCKRCJPN
&UPREFIX..SCKRMJPN
```

古いデータ・セット (例えば、SCKRPLIB の代わりに SC2RPLIB を低位修飾子として持つデータ・セット) があり、そしてそれらを引き続き使用したい場合は、そのデータ・セットを名前変更するか、別名を作成します。単一の UPREFIX パラメーターの代わりに、コンマ区切りのリストを単一引用符で囲んで指定することもできます。

ライン・モードでは、UPREFIX パラメーターは SCKRCARL ライブラリーのみをサポートします。

USRDATA

USRDATA パラメーターを使用して、USER プロファイルに保管されるインストール定義ユーザー・データ・フィールドを指定できます。指定されたフィールドは、Security zSecure Group Administration の表示に示されます。電話番号と社会保障番号 (SSN) をその名前を持つユーザー・データ・フィールドに保管する場合は、次のようにコーディングします。

```
USRDATA='PHONE SSN'
```

VOLSER

UNLOAD、CKFREEZE、および作業データ・セットを割り振るボリューム通し番号を指定するために使用できます。

WORKLLQ

永続作業データ・セット名に付加される低位修飾子。

WORKPREF

ISPF 作業データ・セットの接頭部を設定するために指定できます。指定しないと、接頭部は、TSO PROFILE コマンドで設定された SYSPREF 変数の評価によって構成されます。SYSPREF が空でなく、また SYSUID に等しくなければ、接頭部は syspref.sysuid に設定されます。

それ以外の場合、作業データ・セットは sysuid で始まります。

WORKPREF パラメーター設定を使用すると、作業データ・セットを共有できないため、すべてのユーザーに固有の接頭部を持たせることができます。これは、SYSUID. (末尾にピリオド付き) 変数を以下の例のように使用して行えます。

```
WORKPREF='&SYSUID..C2R'
```

WPREFIX

WPREFIX パラメーターは、共通データ・セットおよびユーザー・データ・セットに加えて使用する必要のあるインストールまたはワークグループに固有の zSecure ライブラリーを指定します。(UPREFIX 構成パラメーターを参照してください。)ISPF インターフェースは追加のライブラリーを検索します。これらのライブラリーは、存在する場合、対応する zSecure 共通ライブラリーの前に連結されます。検索するライブラリー名は、以下のとおりです。

```
&WPREFIX..SCKRPLIB
&WPREFIX..SCKRMLIB
&WPREFIX..SCKRSLIB
&WPREFIX..SCKRTLIB
&WPREFIX..SCKRCLIB
&WPREFIX..SCKRLOAD
&WPREFIX..SCKRCARL
&WPREFIX..SCKRCJPN
&WPREFIX..SCKRMJPN
```

古いデータ・セット (例えば、SCKRPLIB の代わりに SC2RPLIB を低位修飾子として持つデータ・セット) があり、そしてそれらを引き続き使用したい場合は、名前変更するか、別名を作成します。単一の WPREFIX パラメー

ターの代わりに、コンマ区切りのリストを単一引用符で囲んで指定することもできます。ライン・モードでは、WPREFIX パラメーターは SCKRCARL ライブラリーのみをサポートします。

DESC、CKFREEZE、UNLOAD、SMF

これらのパラメーターは、この zSecure 構成のすべてのユーザーが使用可能な入力ファイル・セットを記述します。指定された入力ファイルはデフォルト・セットになります。これらのパラメーターは、組み合わせたときのみ機能します。すなわち、DESC をコーディングするときは、CKFREEZE、UNLOAD または SMF から少なくとも 1 つもコーディングします。zSecure Audit がライセンスに含まれている場合は、単に SMF を指定します。入力ファイル・セットは、zSecure への入力時に入力ソースを、最後のセッションで使用したものにリセットしないすべてのユーザーに対するアクティブ・セットです。入力ソースのリセットはデフォルト動作なので、新規ユーザーにとって、パラメーター DESC/CKFREEZE/UNLOAD/SMF が有効なのは、セットアップ・デフォルトも no reset に変更した場合のみです。この値は、「Setup Default」オプションを使用して変更できます。「Setup Default」オプションは、入力ファイル・セットをカスタマイズするための推奨方法でもあります。

例えば、以下のステートメントをコーディングした場合:

```
SET  DESC='Daily refreshed input files'
SET  CKFREEZE='sys2.cnr.daily.ckfreeze'
SET  UNLOAD=''
SET  SMF='sys2.cnr.daily.smf'
```

zSecure は、指定された CKFREEZE および SMF データ・セットを、稼働中 1 次 RACF データベースとともに使用します。

デフォルトのセットアップについて詳しくは、 233 ページの『付録 E. ISPF インターフェースの構成』を参照してください。

付録 E. ISPF インターフェースの構成

このセクションでは、zSecure ISPF パネルのデフォルト・オプションおよびその他の ISPF 関連機能の設定について説明します。

- 『ユーザー・グループのデフォルト・オプションのセットアップ (「セットアップ」メニュー)』
- 247 ページの『RACF データベースに新規ユーザー ID を作成するための zSecure Admin の構成』
- 248 ページの『ローカルで定義される機能』

ユーザー・グループのデフォルト・オプションのセットアップ (「セットアップ」メニュー)

Setup Default (SE.D) は、ユーザー・グループのオプションをカスタマイズするために推奨される方法です。これによって、PROFDSN パラメーターで指定されたデータ・セットを更新して、個々のユーザー・グループごとにさまざまなデフォルト設定を作成することができます。テストの目的で新規データ・セットに対して Setup Default を実行し、完了したらそのデータ・セットを名前変更またはコピーすることができます。これによって、ユーザーが不完全な変更による影響を受けることはありません。単一の PROFDSN データ・セットのみを使用する場合、Setup Default でシステム全体のオプションを設定します。デフォルト設定が PROFDSN データ・セットに存在しない場合は、標準の (zSecure 出荷時の) 設定が使用されます。ユーザー・インターフェースの破損を防止するには、「Setup default」メニュー・オプションへのアクセスを制限し、このプロセスを理解しているスタッフにのみ PROFDSN データ・セットに対する更新権限を付与します。メニュー・オプションへのアクセスの制限に関する追加情報については、 207 ページの『どのオプションが表示されるかを構成するリソース』を参照してください。

Setup Default を実行するには、PROFDSN データ・セットを選択した状態で ISPF インターフェースを開始します。このタスクは、PROFDSN=*selected.data.set* を指定した構成を選択するか、あるいは C2REMAIN の呼び出し時に PROFDSN (*selected.data.set*) を指定変更として使用して行うことができます。

次に、SE.D を実行します。通常の「セットアップ」パネルに似たパネルが表示されます。「SETUP DEFAULT」パネルを変更して終了すると、パネルに以下のプロンプトが出されます。

```
zSecure defaults, Profdsn: SELECTED.DATA.SET

Choose:     (N=only new users will use defaults)
            (Y=all users will receive new defaults)
            (D=discard all changes,
               not possible for INPUT FILES and NLS)
```

ユーザーが zSecure セッションに入るたびに、このデフォルト設定を使用する場合は、構成ファイルに INIT=YES を指定します。

新規ユーザーは、常にデフォルトのシステム設定を使用します。「N」を選択すると、新規ユーザーのみが新しい設定を使用します。「Y」を選択すると、この PROFDSN のすべてのユーザーが次回の Security zSecure 始動時に新しい設定を使用します。「D」を選択すると、すべての変更が破棄されます。ただし、NLS および INPUT FILES を除きます。これらのオプションの変更は破棄できません。

注: SE.D.1 に定義されているファイルのみが変更、追加、または削除され、SE.1 に追加されたその他のファイルは同じ状態のままです。

したがって、「Y」を選択しても、ユーザーの構成に対するその他の追加や変更には影響がありません。

セットアップ (デフォルト) による各国語サポート (SE.D.N)

zSecure は、パネル表示用の言語を選択する機能を備えています。言語の選択に加え、選択した言語を使用して表示するパネル上のテキストをカスタマイズすることもできます。現在、言語指定は選択パネル・オプションに制限されています。追加情報については、 236 ページの『各言語の選択』および 236 ページの『個々のメニュー・オプションのカスタマイズ』を参照してください。

zSecure は以下の DBCS サポートを提供します。

入力フィールド

- DBCS をサポートする入力フィールドに対する DBCS 文字は受け入れられます。例えば、RACF のプログラマー名とインストール・データの各フィールドの入力フィールドは、入力フィールドに対する DBCS 文字を受け入れます。
- 「COPY NEWNAME」や「NEWDATA」などの CARLa の入力フィールドに対する DBCS 文字は受け入れられます。
- 変更可能フィールド (つまり上書き可能フィールド) での DBCS 文字は受け入れられ、文字化けしません。
- 「CKGRACF REASON」フィールドは DBCS のデータを受け入れます。
- DBCS 文字は、引用符付きストリングまたはコメントの一部として入力されたときに、入力として受け入れられます。それらの文字は、一般に、ISPF FIND 基本コマンドや CARLa (監査およびレポート作成プログラム言語) の走査ストリングなど、特定の場合を除いて、引用符付きストリングの外側ではサポートされません。

コマンド・サポート

- DBCS ストリングを含む基本コマンドはすべてのパネルで受け入れられます。
- SELECT FIELD= SCAN= コマンドは DBCS ストリングに機能します。ただし、DBCS ストリングを引用符で囲む必要があります。
- ISPF の編集セッションおよびブラウズ・セッションは混合モードに対応しているため、DBCS ストリングが正しく編集されます。
- FIND コマンドは、区切り文字で囲まれた DBCS 検索値をサポートします。区切り文字に使用できるのは、単一引用符 (') または二重引用符 (") のいずれかです。

ISPF のメニュー、表示、およびレポート・パネル

- 「SETUP NLS」オプションを使用すると、言語に日本語を選択できます。このオプションを選択すると、メインメニュー、RA.H のメニュー・オプション、アクション・コマンド、アクション・バーなどの一部のユーザー・インターフェース項目が日本語で表示されます。
- ISPF パネルに DBCS ストリングが表示され、zSecure で生成する日本語のレポートが正しく表示されます。
- 作成または調整したレポートの完全な DBCS ストリングが正しく表示されます。ただし、切り捨てられたフィールドは正しく表示されない場合があります。
- 監査に関する考慮事項を含む zSecure の表示とレポートならびにオプション AU.V と AU.S は日本語に翻訳されます。メニュー・オプションを除き、他のほとんどのパネルは英語のままです。
- DBCS 文字を含む NLS テーブルは正しく処理されます。
- ISPF メッセージは日本語に翻訳されます。

フォーマット

- 大文字変換を実行しても DBCS はそのままです。
- WORDWRAP が指定された DBCS ストリングでは、可能な場合に改行に関する言語の制約が考慮されます (日本語のみ)。
- ユーザーが適切な (混合 DBCS) CCSID を渡すと、UTF-8 フォーマットの添付ファイルを含む E メールは、正しい DBCS 文字に変換されます。
- ユーザーが適切な (混合 DBCS) CCSID を渡すと、UTF-8 フォーマットの XML は、正しい DBCS 文字に変換されます。ただし、スタイル・シートの埋め込みを使用する場合、ユーザーの CCSID のスタイル・シートを使用する必要があります。
- CCSID スタイル・シート・サポート: ユーザーは自分の CCSID に含まれるスタイル・シートを使用する必要があります。スタイル・シート CCSID 939 および CCSID 1047 は相互に入れ換えて使用することができます。スタイル・シート CCSID 1388 は機能しません。
- zSecure は JIS X 0213:2004 の z/OS サポートを活用します。

制限

- CKRCARLA メッセージおよびヘルプ・テキストはすべて英語のままです。ISPF メッセージは日本語に翻訳されます。
- IP_PORT 監査に関する考慮事項は日本語に翻訳されません。
- RACF LISTUSER によってフォーマット設定された表示の長い DBCS INSTDATA は、MI パネルで文字化けしますが、LISTUSER でも文字化けするため、正しいものとして受け入れられます。
- 生成した E メール内のテキスト (件名など) は DBCS 文字を含むことができません。
- 大文字変換を実行しても DBCS はそのままです。つまり、PRINT CAPS は LANGUAGE ステートメントとともに DBCS を含む NEWLIST にのみ作用します。

- ISPF サービスを呼び出すには、端末モードが 3277KN または 3278KN のときにコマンドを大文字で実行する必要があります。zSecure では小文字の ISPF コマンドを使用します。zSecure の UI の障害を防止するために、zSecure では始動時に ISPF 端末モードが 3278 に動的に変更されます。端末モードは TSO セッション全体に設定されるため、それは分割画面セッションで実行される zSecure 以外のアプリケーションでもアクティブです。端末モードが変更されたことを示すために、以下の警告メッセージが発行されます。

  ```
  ISPF terminal type changed from 3278KN to 3278.
  Terminal type will be set back to 3278KN after exiting the
  zSecure UI. Please note that while zSecure is active, all logical
  screens (SPLIT SCREEN) will also use ISPF terminal type 3278.
  ```

  終了時に端末モードは元の設定に切り替わります。

SE.D.N パネル

「セットアップ」パネルから「**N**」を選択すると、以下のパネルが表示されます。

```
 Menu   Options   Info   Commands
--------------------------------------------------------------------------------
                        zSecure Suite - Setup - NLS
Command ===>

Change language to            Action on language items
1  1. English                 1  1. No action (only use specified language)
   2. Dutch                      2. Reset all items to company default
   3. French                     3. Reset all items to IBM Security zSecure default
   4. German                     4. Customise menu items
   5. Italian                    5. Customise action line commands
   6. Portuguese
   7. Spanish
   8. Japanese
   9. Other
   0. zSecure
Language used: User English
```

図 *11.* 「セットアップ *- NLS*」パネル

各言語の選択**:** 図 11 のパネルから、zSecure メニュー・パネル上で使用する言語を定義できます。**IBM Security zSecure** の言語オプションを定義すると、IBM ソフトウェア・サポートとの通信が円滑になり、質問や問題への対処が迅速になります。IBM ソフトウェア・サポートへの連絡時には、NLS サポート・オプションを IBM Security zSecure に変更するように指示されます。サポート呼び出しが完了したら、定義した独自のインストール言語に切り替えることができます。「**Other**」言語は、指定されていないその他の言語用です。

言語をデフォルト・オプション (zSecure で定義されたオプション) または会社で選択したオプションにリセットするには、「**Action on language items**」リスト内のいずれかのリセット・オプションを指定します。オプション **2** および **3** を使用すると、すべての言語項目を変更できます。

個々のメニュー・オプションのカスタマイズ**:** 日本語以外のすべての言語の場合、オプション「**SE.N** Action **4**」を選択すると 237 ページの図 12 のパネルが開き、メニュー項目をカスタマイズできます。このパネルに表示されるテキストは、ユーザーが独自に指定した内容に依存します。オプション **5** を選択すると、アクション

の行コマンドが表示され、それらをカスタマイズできます。オプション 4 および 5 は、言語が日本語の場合は使用できません。

注: zSecure の 2 バイト文字セット (DBCS) については、 234 ページの『セットアップ (デフォルト) による各国語サポート (SE.D.N)』を参照してください。

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - NLS    Row 1 to 17 of 171
Command ===>                                                 Scroll ===> CSR

Specify action for menu item(s): Edit, Insert, Copy, Delete

   Standard options   Option and text as shown on panel
_  SE            SE Setup           Options and input data sets
_  SE 0          0  Run             Specify run options
_  SE 1          1  Input files     Select and maintain sets of input data set
_  SE 2          2  New files       Allocate new data sets for UNLOAD and IOCO
_  SE 3          3  Preamble        Commands run before every query
_  SE 4          4  Confirm         Specify command generation options
_  SE 5          5  View            Specify view options
_  SE 7          7  Output          Specify output options
_  SE 8          8  Command files   Select and maintain command library
_  SE U          U  User defined    User defined input sources
_  SE C          C  Change Track    Maintain Change Tracking parameters
_  SE C  M       M  Site msgs       Site defined message table
_  SE C  C       C  zSecure msgs    zSecure defined message table
_  SE N          N  NLS             National language support
_  SE T          T  Trace           Set trace flags and CARLa listing for diag
_  SE V          VM VM Files        Copy RACF/VM database (VM only)
_  SE W          W  Windows         zSecure Visual configuration
```

図 *12.* すべてのメニュー項目が表示された「セットアップ - *NLS*」パネル

「zSecure Suite - セットアップ - NLS」パネルには、zSecure で使用可能なすべてのメニュー・オプションを含むテーブルが表示されます。このテーブルには、ライセンスやシステム仕様によりユーザーの使用が許可されていない項目も表示されます。このテーブルの任意の項目を編集、コピー、挿入、または削除できます。「セットアップ」パネルの表示順序により、zSecure 製品パネルを使用するときのメニュー項目の表示順序が決定します。現在行の下に行を追加するには、選択フィールドに **I** を入力します。項目を移動するには、項目を適切な位置に追加してから元の項目を削除します。

行コマンドを入力するたびに、以下のパネルが表示されます。

```
   Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - NLS
Command ===> ____________________________________________________________

Official option  . . SE 0         (also used for profile checking)

Specify action for menu item
1  1. Use as specified below        2. Delete menu item
   3. Reset to system defaults      4. Reset to IBM Security zSecure defaults

Menu option  . . . . 0              (as displayed on user menu)
Short description  . Run
Long description . . Specify run options
Command (or MENU ) . CMD(%C2REDFLL NO &C2RNSE0)
Panel for "MENU" . . ________________ New menu . .  N  (Y/N)


Press ENTER to continue.
```

図 *13.* 行コマンド選択後の「セットアップ - *NLS*」パネル

このパネルでは、以下のフィールドを指定できます。

Official option

このフィールドでは、このメニュー・オプションの検査が実行される SAF リソースのリンクを指定します。3 段階の深さまで指定できます。この指定により、オプションが配置されるメニューも決まります (つまり、RA 4 2 と指定するとオプションは「RA.4」メニューに配置されます)。「Official option」は、最初にメニュー・オプションを定義するときにのみ変更できます。したがって、オプションを変更できるのは、コピーまたは挿入の行コマンドのみであり、編集の行コマンドでは変更できません。「LO」メニューでの場合を除き、ユーザーが追加したメニュー項目には、「Official option」フィールドに @、#、または $ の少なくとも 1 文字を含める必要があります。そうしないと、追加したオプションは NLS のアップグレード時に削除されます。

Action

アクションにより、メニュー・オプションの処理内容が決定します。削除の行コマンドを使用した場合、アクションは以下のいずれかに初期化されます。

オプション **2** は、ENTER キーを押すとメニュー・オプションが削除されることを示します。

オプション **3** は、テーブル項目をシステム・デフォルトにリセットします。システム・デフォルトがない場合は、zSecure のデフォルトが使用されます。

オプション **4** は、ユーザーが指定した言語用の zSecure の元の設定に項目をリセットします。

Menu option

「Menu option」はそのままパネルに表示されます。同じオプションを含むメニュー項目を指定することが可能です。この場合、最後のメニュー・パネルの最初のオプションが使用されます。これによりプロファイルの柔軟性が向上します。例えば、メニューで同じオプションを複数使用して、あるユーザー・グループは 1 番目のメニュー項目を使用し、別のユーザー・グループは 2 番目のメニュー項目を使用できます。ユーザーがデフォルトのメニ

ュー・オプションを変更しても、NLS のアップグレード時にその変更は伝搬しません。ユーザー・オプションの場合、「Menu option」は「Official option」と一致させる必要があります。

Description
製品メニュー・パネルに表示する簡略説明および詳細説明を指定します。説明には ISPF 変数名を使用できます。これらの変数は、製品操作でメニューが表示されるときに解決します。ユーザーがデフォルトのメニュー・オプションを変更しても、NLS のアップグレード時にその変更は伝搬しません。

Command (or MENU)
オプションが指定されたときに実行するコマンドを指定します。この値に指定できるのは、コマンド (%CMD) またはパネルです。これは通常、ISPF パネル本体で指定されたものです。次のパネルがメニューであることを示すには、「MENU xx」と指定します。この場合、「xx」はメニュー項目が定義される「Official option」です。したがって、「**MENU SE**」と指定すると、「Official option」が「SE *xx*」であるすべての項目を含むメニューが表示されます。「**MENU SE D**」と指定すると、「Official option」が「SE D *zz*」であるすべての項目を含むメニューが表示されます。メインパネル以外のパネルに次のメニューを表示するには、「**Panel for "MENU"**」フィールドに独自のパネルを指定します。「LO」(ローカル) オプションを除き、コマンド・フィールドへのユーザーの変更は NLS のアップグレード時に伝搬しません。

Panel for "MENU"
メニュー・オプションの使用時に選択されるパネルです。

New menu
このオプションを使用すると、1 次メニュー・オプションを追加して、新規メニューに表示するか (**Y**)、またはメインメニューで展開可能にするか (**N**) を指定できます。展開可能にする場合、「Panel for "MENU"」フィールドはブランクのままにして、「Command (or Menu)」に MENU オプション名 (MENU R@ など) を使用します。

Enter キーを押すと、以下のパネルが表示されます。

```
   Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - NLS
Command ===> ____________________________________________________________

Display Menu option for any of the following programs
/  RACF Admin
/  RACF Audit
/  RACF Report
/  CKGRACF
/  ACF2 Admin
/  ACF2 Audit
/  ACF2 Report
_  TSS Audit
_  Visual
_  Alert
Select any of the following options
/  Menu option is supported on z/OS
/  Menu option is supported on z/VM
/  Menu option is a z/OS analyzing option
/  Menu option is a z/VM analyzing option
_  Menu option is only available on ISPF 5.0 and up
```

図 *14.* 表示メニュー・オプションが表示された「セットアップ - *NLS*」パネル

このパネルでは、以下のフィールドを指定できます。

Display Menu option for any of the following programs
このフィールドでは、メニュー項目を使用するライセンス交付を受けた機能を指定します。表 19 は、製品 (ライセンス) と機能の関係を示しています。

表 *19. NLS* でライセンス交付を受けた機能と製品の関係

製品	RACF Admin	RACF Audit	RACF Report	ACF2 Audit	ACF2 Report	TSS Audit	CKGRACF
zSecure Admin	/						/
zSecure Audit for RACF		/	/				
zSecure Audit for ACF2				/	/		
zSecure Audit for Top Secret						/	

「LO」(ローカル) オプションを除き、ユーザーがライセンスを変更しても NLS のアップグレード時にその変更は伝搬しません。

Menu option is supported on z/OS
このメニュー項目で使用する機能が z/OS でサポートされている場合、このフィールドにタグを付加します。

Menu option is supported on z/VM
このメニュー項目で使用する機能が z/VM でサポートされている場合、このフィールドにタグを付加します。

Menu option is a z/OS analyzing option
このメニュー項目を z/OS データの分析に使用する場合、このフィールドにタグを付加します。

Menu option is a z/VM analyzing option
このメニュー項目を z/VM データの分析に使用する場合、このフィールドにタグを付加します。

Menu option is only available on ISPF 5.0 and up
このメニュー項目で使用する機能が ISPF 5.0 以降でのみサポートされる場合 (CUA 属性など)、このフィールドにタグを付加します。

アクション行コマンドのカスタマイズ

オプション 5「Customize action line commands」を使用して、zSecure ユーザー・インターフェースのレポートで使用する行コマンドを追加、削除、および編集できます。このオプションは、主に行コマンドのローカリゼーションを可能にするためのものですが、zSecure に含まれていない機能のために新規の行コマンドを定義することも可能です。行コマンドのアクションには、以下の 2 つのタイプがあります。

- 行コマンドは ISPF パネルを呼び出すか、zSecure 組み込みの表示またはコマンド生成ルーチンを呼び出すことができます。呼び出された ISPF パネルは、生成された RACF コマンドを返すか、最終的に組み込みのルーチンを呼び出すために値を返すか、別のパネルまたは REXX を呼び出すために値を返すことができます。
- 呼び出されたパネルまたは REXX は、いくつかの事前定義 ISPF 変数を使用してデータを取得することができ、また CARLa マップ・フィールドを使用して、表示 (表示されるか、nondisplay 修飾子を使用して非表示とされる) の定義に使用される CARLa フィールドからの値を取得できます。

行コマンドをブロックとして構成することが可能ですが、特定の制限が適用されます。例えば、CARLa マップ・フィールドは使用できません。詳しくは、Map CARLa fields into ISPF variablesを参照してください。

オプション 5 を選択して Enter を押すと、定義されているすべての行コマンドのリスト、およびそれらのコマンドを主にどこで使用できるかが示されます。行コマンドには、特定のレコードで有効であることを示す 2 つの基本制御があります (NEWLIST TYPE と ENTITY TYPE)。ENTITY TYPE は主に USER (例えば、type=RACF)、DATASET (例えば、type=RACF) などとして表示できます。

行コマンドを有効または無効として構成できるのは、特定の場所のみです (例えば、特定の RACF クラスやセグメント)。このタイプの制限基準によって制限されている場合は、/ 行コマンドの結果として表示されるメニューに表示されません。以下のパネルに、クラスやセグメントによる追加制限ではなく、基本設定のみを示します。

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - NLS     Row 33 to 66 of 379
Command ===> _____________________________________________ Scroll ===> CSR_
Specify action for menu item(s): Edit, Insert, Copy, Delete
    Standard options   Option and text as shown on panel
 _  RC D  AC      AC Access          Access Check for one userid or group
 _  RC D  C       C  Copy            Copy data set profile
 _  RC D  D       D  Delete          Delete data set profile
 _  RC D  D       D  Delete          Delete data set segment
 _  RC D  E       E  Event           Display event logging
 _  RC D  L       L  List            RACF listdsd command
 _  RC D  LD      LD List profile    RACF listdsd DSNS command
```

図 *15.* アクション項目リストが表示された「セットアップ - *NLS*」パネル

- 最初の列は、行コマンドが有効である NEWLIST タイプをリストしています。
- 2 番目の列は、それが有効であるエンティティーをリストしています。
- 3 番目の列は、行コマンドのアクションをリストしています。
- 4 番目の列は、ユーザーが行コマンドとして入力する内容をリストしています。これは、6 番目の列 (説明) と組み合わせて、行コマンドとして / を入力したときに表示される内容になります。
- 5 番目の列は、行コマンドの区別に役立つようにするためだけのものです。

行コマンドの上にある入力フィールドに E と入力するときに最初の行コマンドを選択した場合、以下のパネルが表示されます。

```
   Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - NLS
Command ===> ____________________________________________________________

Newlist type . . . . RC             (i.e. RC for RACF)
Entity type  . . . . D              (i.e. U  for USER)
Action . . . . . . . AC             (i.e. C  for COPY)

Specify action for menu item
 1  1. Use as specified below        2. Delete menu item
    3. Reset to system defaults      4. Reset to IBM Security zSecure defaults

Used action  . . . . AC               (as displayed on user menu)
Used block action. . __               (optional; requires special support)
Short description  . Access
Long description . . Access Check for one userid or group
Panel  . . . . . . . C2RP&CKREREL.AC@ (panel to use for action specification)

/  Map CARLa fields into ISPF variables
_  Specify classes and segments for which this action is valid or not valid


Press ENTER to continue.
```

図 *16.* 新規リスト・タイプ、エンティティー・タイプ、およびアクションが表示された「セットアップ - *NLS*」パネル

このパネルでは、以下のフィールドが定義されます。

Newlist type
行コマンドが有効である新規リスト・タイプ。

Entity type
行コマンドが有効であるエンティティー・タイプ。

Action

アクション ID。これは、XFACILIT クラスのプロファイルによって制限するときに検査されるリソースを識別するために使用されます。このフィールドは、zSecure 組み込みの表示またはコマンド生成ルーチンを呼び出すための ID としても使用されます。NLS テーブルのアップグレード時に、アクションに文字 @、#、または $ が含まれている行コマンドのみが保持されます。

Specify Action for menu item

このオプションは、行コマンドを削除するか、それをデフォルトにリセットするために使用できます。

Used action

行コマンドを実行するために zSecure パネルで入力される実際の文字。これらは、単一のコマンドで使用される文字です (行コマンドがブロック行コマンドも許可した場合)。

zSecure 組み込み項目の「**Used action**」の変更は、NLS テーブルのアップグレード時に保持されません。

Used block action

1 回の実行で処理するレコードのブロックの開始と終了を指示するために zSecure パネルで入力される実際の文字。このフィールドに値がある場合は、すべての単一レコード行コマンドも、1 回の実行で処理されます。

ブロック・アクションは常に、呼び出された任意のパネルまたは REXX で使用される可能性がある事前定義の ISPF 変数が、ブロック内のすべてのレコードで同じ値を持つことを保証します。例えば、ブロックは、複数の複合システムにまたがっている場合、パネルまたは REXX の複数の呼び出しに分割され、指定したパネルが複数回表示されます。

ブロック内のレコードの CARLa マップ・フィールドは異なる値を持つ可能性が非常に高いため、zSecure では、ブロック・アクションの定義時にそのようなフィールドは許可されません。

Description

行コマンドの簡略説明と詳細説明。両方ともに、前のパネルに表示されます。詳細説明は、/ 行コマンドの実行時に表示されるメニューで使用されます。

なお、zSecure の行コマンドのデフォルト・セットに対する更新は、NLS テーブルの更新時に保持されません。

Panel このフィールドには、行コマンドを入力したときに呼び出されるパネルが含まれます。フィールドが空の場合は、「**Action**」で構成された組み込みアクションが呼び出されます。

変数 &CKREREL は、プルダウン・パネルと非プルダウン・パネルを区別するために zSecure によって使用されます。

Map CARLa fields into ISPF variable

このオプションは、表示からの値 (表示または非表示のいずれか) を表示パネルのデータとして使用することを許可します。「Used block action」が指定されている場合は、このオプションは使用できません。このフィールドを選択した場合は、Map CARLa fields into ISPF variablesに進みます。

Specify classes and segments for which this action is valid or not valid
レコードによって使用されるエンティティー・タイプに応じて、このオプションにより、この行コマンドが有効または無効であるクラスのリストおよびセグメントのリストを指定することができます。このフィールドを選択し、「**Map CARLa fields into ISPF variable**」フィールドを選択しなかった場合は、Specify classes and segments for which this action is valid or not validに進みます。

これらの最後の 2 つのフィールドのいずれも選択せずに **Enter** を押すと、 240 ページの図 14 が表示されます。

Map CARLa fields into ISPF variables:

前の NLS アクションのセットアップ・パネル (242 ページの図 16) で「**Map CARLa fields into ISPF variables**」フィールドを選択した場合は、**Enter** を押すと、以下のパネルが表示されます。

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - NLS
Command ===> ____________________________________________________________

Specify CARLa - ISPF matches
CARLa                     ISPF       CARLa                     ISPF
KEY                       CKRRPROF   ________________________  ________
________________________  ________   ________________________  ________
________________________  ________   ________________________  ________
________________________  ________   ________________________  ________
________________________  ________   ________________________  ________
________________________  ________   ________________________  ________

Press ENTER to continue.
```

図 *17. CARLa* 変数と *ISPF* パネル変数間のフィールド一致を構成するための「セットアップ - *NLS*」パネル

「**CARLa**」列には、照会からの CARLa 変数の名前が含まれます。「**ISPF**」列には、パネルで使用される ISPF 変数の名前が含まれます。CARLa 変数が照会内に存在することを確認してください。これが存在しない場合、アクションの実行時にパネルが表示された後にエラー・メッセージが表示されます。

Specify classes and segments for which the action is valid or not valid:

前の NLS アクションのセットアップ・パネル (242 ページの図 16) で「**Specify classes and segments for which this action is valid or not valid**」フィールドを選択した場合は、**Enter** を押すと、以下のパネルが表示されます。

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                zSecure Suite - Setup - NLS
Command ===> ____________________________________________________________

Newlist type . . . : RC
Entity type  . . . : R
Action . . . . . . : D

Specify classes for which this action is valid:
________ ________ ________ ________ ________ ________ ________ ________
________ ________ ________ ________ ________ ________ ________ ________
Specify classes for which this action is not valid:
________ ________ ________ ________ ________ ________ ________ ________
________ ________ ________ ________ ________ ________ ________ ________
Specify segments for which this action is valid:
BASE____ ________ ________ ________ ________ ________ ________ ________
________ ________ ________ ________ ________ ________ ________ ________
Specify segments for which this action is not valid:
________ ________ ________ ________ ________ ________ ________ ________
________ ________ ________ ________ ________ ________ ________ ________

Press ENTER to continue
```

図 *18. CARLa* 変数と *ISPF* パネル変数間のフィールド一致を構成するための「セットアップ - *NLS*」パネル

このパネルで、行コマンドを有効または無効にするクラスまたはセグメントを構成できます。同じ「NEWLIST type」、「Entity type」、および「Used action」に対して複数の行コマンド項目を定義することで、クラスおよびセグメントに応じて、同じ「Used action」に対して異なるアクションを作成できます。例えば、ある削除コマンド (D) は (「**Specify classes for which this action is valid**」フィールドで指定した) 特定のリソース・クラス用、別の削除コマンド (D) はその他のすべてのクラス用 (このパネルを空のままにする)、とすることができます。

BASE セグメントの表示を除いて、画面には、ほとんどのレコード要素で有効な行コマンド D (アクションであるため、組み込みの ID) が表示されます。

行コマンドのエンティティー・タイプに応じて、これにより、以下のことを行うことができます。

表 *20.* エンティティー・タイプと、許可される選択/除外

Entity type		用選択/除外可能な対象
D	DATASET	セグメント
G	GROUP	セグメント
R	一般リソース・クラス	クラスとセグメント
U	USER	セグメント
M	マルチ複合システムの要約	クラスとセグメント
Other		None

システムは NLS テーブルで一致性が最も高い項目を検索します。つまり、クラスおよびセグメントが指定されていてかつ正しい場合、正しいクラスのみを指定する別の項目が存在したとしても、その項目が適用されます。そのような固有の一致が存在しない場合は、一致率が最も高い最初の要素が使用されます。

セットアップ (デフォルト) によるインストール定義名 (SE.D.I)

一部のデータ・セット名およびプロファイル名はカスタマイズ可能であり、その名前自体をサイトごとに変更できます。このオプションにより、サイトで使用する名前をプログラムに通知できます。

次のパネルが表示されます。

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Installation
Command ===>

Installation specific names
 JES/328X data set mask . SYS1.JSXLOG.**_____________________________ (EGN mask)
```

図 *19. JES/328X* データ・セット・マスクが表示された「セットアップ - インストール」パネル

JES/328X data set mask

JES/328X ログ・データ・セットの名前を処理する EGN マスクを指定します。このマスクは、リモート印刷に JES/328X を使用する場合にのみ意味を持ちます。このマスクは、JES/328X 定義およびログ・データ・セット・レポートによって使用されます (オプション RA.3.D)。詳細については、「ユーザー・リファレンス・マニュアル」を参照してください。

セットアップ (デフォルト) によるコマンド・ファイル (SE.D.8)

SE.D.8 メニュー・オプションでは、今後使用するための既存のライブラリーの割り振りおよび選択を行うことができます。**SE.D** と一緒に使用すると、会社全体のデフォルトを設定できます。最初は、製品のサンプル・ライブラリーの DD:CKRCARLA のみが含まれます。**I** 行コマンドを使用して、新規データ・セット名を挿入することができます。セットを活動化するには、**S** 行コマンドを使用します。

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Command file Row 1 from 3
Command ===>                                                 Scroll ===> CSR

Select sample library or work with a library (E, R, I, or D)

   Sample library
_  DD:CKRCARLA_____________________________________________________
****************************** Bottom of data ********************************
```

図 *20.* ライブラリー選択が表示された「セットアップ - コマンド・ファイル」パネル

ライブラリー選択リストの各行には、TSO 規則を使用するデータ・セット名、または DD: とその後に続く割り振り済みファイル名が含まれる必要があります。選択済みのマークが付けられたライブラリーは、**CO** コマンド・メニューのオプションによって使用されます。連結はサポートされていません。

以下の行コマンドを使用できます。

表 21. 選択したライブラリーで使用する行コマンド

E	このライブラリーのメンバーを表示します
D	選択リストから行を削除します。データ・セットは削除されません。
I	この行の後に空の行を挿入します。自動的には選択されません。
R	この行で名前を繰り返します
S	ライブラリーを後続の使用のために選択します

データ・セットを選択すると、**E** 行コマンドまたはオプション **CO.2** でそのメンバー・リストを呼び出すことができます。

zSecure のアップグレード時のセットアップ・デフォルト・データの保持

使用中の PROFDSN データ・セットは、構成内の PROFDSN パラメーターで指定されています。追加情報については、 223 ページの『付録 D. 構成パラメーターと構成メンバー』を参照してください。

RACF データベースに新規ユーザー ID を作成するための zSecure Admin の構成

このタスクについて

注**:** この手順は、zSecure Admin を使用する場合にのみ実行する必要があります。

zSecure Admin を使用すると、RACF データベースに新規ユーザー ID を作成できます。この新規ユーザー ID で TSO および ISPF を使用する場合、ユーザー・カタログ、ISPF プロファイル・データ・セット、および新規ユーザーが所有するすべてのデータ・セットの DATASET を指定する必要があります。

手順

これらの値を指定するには、hlq.ckrparm 構成データ・セットの指定メンバーを以下のように更新します。

1. この構成のユーザー・カタログを選択するには、メンバー C2RSMUMA を更新して、マスター・カタログに含まれる、いずれかのユーザー・カタログを指す別名を指定します。
2. 新規ユーザーの ISPF プロファイル・データ・セットを指定するには、構成データ・セットのメンバー C2RSMUMP を UNIT およびデータ・セットの命名規則に応じて更新します。
3. 新規ユーザーが所有するすべてのデータ・セットの DATASET プロファイルを指定するには、必要に応じてメンバー C2RSMUMH を更新してインストールおよび配布の手順で実装したデータ・セット命名規則に準拠する必要があります。

   別名および ISPF プロファイルが作成されるのは、ユーザーのコピー時ではなく、RA.U 表示の MT 機能 (「TSO の管理」情報) の使用時です。マルチイメージ環境では、各 z/OS イメージで別名および ISPF プロファイル・データ・

セットが必要です。ISPF プロファイル・データ・セットは共有を前提としていないため、場合によっては、各 z/OS イメージで異なる名前を使用することが必要です。

ローカルで定義される機能

LOCAL オプションは、ISPF ダイアログの作成経験のあるユーザーによってカスタマイズされるように設計されています。CKRP3C* から始まるパネル名は、ユーザーがカスタマイズするヘルプ・パネル用に予約されています。新機能または変更された機能は、オプション **LO** のサブオプションとして NLS テーブルに追加できます (234 ページの『セットアップ (デフォルト) による各国語サポート (SE.D.N)』セクションを参照)。LO パネルには、最大 12 個のオプションを設定できるスペースがあります。オプション **LO** で使用されるパネル (C2RP3C@@) を変更または置換する場合、zSecure のアップグレード時に変更内容を上書きしないでください。提供パネルを追加または変更する場合、ユーザー独自のライブラリーを zSecure 製品ライブラリーの前に連結することをお勧めします。これらのライブラリーは、`WPREFIX` または `UPREFIX`パラメーターを使用して zSecure 構成で指定できます。223 ページの『付録 D. 構成パラメーターと構成メンバー』を参照してください。zSecure 提供パネル C2RPxC@@ をユーザー・パネルに置き換える場合、このユーザー・パネルに以下の行を必ず追加してください。

```
IF (.RESP=END)
     &C2RCOMM = 'MAIN'
     VPUT C2RCOMM SHARED
```

これらの行はメインメニューに正しく戻るために必要です。

LO パネルで提供される以下のオプションは、例を示すためのものです。

P - パネル
: 「パネル」フィールドに指定されたパネルを ISPF SELECT PANEL サービスを使用して選択します。このパネルは有効な選択パネルであることが必要です (つまり、ZSEL を必ず設定する必要があります)。

C - コマンド
: 「コマンド」フィールドに入力されたコマンドを ISPF SELECT CMD サービスを使用して選択します。

R - CKRERUN の開始
: CMD(%CKRERUN PANEL(*)) を使用して REXX exec CKRERUN を開始します。パネルからの入力データは使用されません。CKRERUN は共有プールの変数 CKRCMDV から CARLa コマンドを読み取り、その結果を表示します。CKRCMDV において複数行コマンドは、改行区切り文字 x'15' によって分離できます。提供されているため、CKRCMDV はオプション LO によって埋められません。

コマンド生成

CKRERUN プログラムは、指定されたダイアログ・パネルの表示、コマンドの実行、および結果の表示を行います。このプログラムはユーザー独自のプログラムから使用できます。CKRERUN の呼び出しには、以下のパラメーターを使用します。

PANEL(panel1 panel2)
選択パネルおよび (オプションの) 結果パネル

RESULT(panel)
結果パネルを表示します

REUSE(files)
指定されたファイルをクリアしません

SYSIN(member)
(同様に) CKRCARLA の組み込みメンバー

HELP(panel)
BROWSE で使用する SCKRPLIB のメンバー

PERFORM(command)
CKRCARLA の代わりに呼び出される TSO コマンド

例えば、インストールで独自の ISPF パネルを定義する場合、ユーザー出口を呼び出して TSO コマンドを生成できます。このコマンドはユーザーに表示されるため、zSecure で生成される TSO コマンドのように確認と実行、およびキューに入れることができます。

ユーザー出口を構成するには、以下のように PERFORM および PANEL パラメーターを使用して、ISPF パネルから CKRERUN コマンドを呼び出します。

```
CKRERUN PERFORM(xxxx) PANEL(yyyy)
```

xxxx は、インストール定義アクションを実装するコマンドです。以下に例を示します。

```
/* ADDALIAS REXX */
push "DEFINE ALIAS (NAME('" || uuser || "') RELATE('" || ucat || "'))"
'EXECIO 1 DISKW CKRCMD (FINIS'

'EXECIO 0 DISKW CKREPORT (FINIS OPEN'
```

EXECIO から CKREPORT までは、ユーザーが CKREPORT ファイルをブラウズすることを不要にしています。(「結果」パネルには、
CKREPORT、CKRCMD、CKR2PASS、および SYSPRINT から最初の空ではないファイルが表示されます。)

ISPF パネル *yyyy* の例を以下に示します。

```
%------------------- Define catalog alias for userid -------------------
%COMMAND ===>_ZCMD

+Userid           ===>_UUSER   +

+Usercatalog      ===>_UCAT                        +(no quotes)

)PROC
  VPUT (UUSER UCAT) SHARED
  &CKRNEXT = &Z              /* no continuation panel */
)END
```

図 *21. ISPF* パネル *yyyy* の例

CKRNEXT には次に表示するパネルのメンバー名を設定するか、変数をクリアしてこれが最後のパネルであることを示します。CKRNEXT が空である場合、PERFORM ス

テートメントで定義された機能が実行されます。また、PERFORM が指定されなかった場合は、zSecure が実行されます。後者の場合、変数 CKRCMDV が zSecure に渡され、ユーザー指定オプションが実行されます。

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で提供し、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が、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、単に目標を示しているものです。

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。

お客様は、IBM 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、Adobe ロゴ、PostScript、PostScript ロゴは、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 AXELOS Limited 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 AXELOS Limited の登録商標です。

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。

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。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

[数字]

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Printed in Japan

SA88-7162-03

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21