Security zSecure Admin and Audit for RACF
バージョン 2.2.0

スタートアップ・ガイド

GI88-4318-02

Security zSecure Admin and Audit for RACF
バージョン 2.2.0

スタートアップ・ガイド

GI88-4318-02

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、 155 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。

2015 年 11 月

本書は、IBM Security zSecure Admin (製品番号 5655-N16) および 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 0 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： GI13-2324-02
Security zSecure Admin and Audit for RACF
Version 2.2.0
Getting Started

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™ Admin and Audit for RACF® (リソース・アクセス管理機能) は、RACF システムで繰り返し行われる管理タスクと監査レポート処理の多くを自動化します。これらの製品は zSecure Collect プログラムを使用して RACF および z/OS® システムからデータを収集、分析します。これにより、ユーザー・アクセス権限のモニター、管理者権限を制限するための範囲の実装、およびユーザー動作の監査を容易に実行できるようになります。また、これらの製品では RACF システムの管理機能とレポート機能の拡張により、セキュリティー監視が促進され、システム管理が分散されます。

本書は、ユーザーが IBM Security zSecure Admin and Audit for RACF について迅速に理解できるようにすることを目的としています。本書を一通り読むことで、これらの製品に関する実際的な知識を習得し、製品のその他の機能を使用できるようになります。本書は完全なリファレンス・マニュアルではなく、すべての機能を説明しているわけではありません。本書では、(ISPF パネルを使用した) 対話式機能を中心に、IBM Security zSecure Admin and Audit for RACF の主要な機能を説明します。

いくつかの概要ページを除き、本書は IBM Security zSecure Admin and Audit for RACF を使用する際の実践的なガイドとして使用されることを目的としています。本書は、IBM Security zSecure Admin and Audit for RACF を使用して一般的な管理タスクを実行する方法、および RACF システムで監査とレポートを実行する方法を説明しています。

本書の対象読者には、セキュリティー管理者とメインフレーム・システム・プログラマーなどが含まれます。本書の対象読者は、RACF システム管理についての実践的な知識があり、Interactive System Productivity Facility (ISPF) を問題なく使用できる必要があります。

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 Security zSecure Suite または IBM Security 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、vi 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 Security zSecure Suite	http://www.ibm.com/support/knowledgecenter/SS2RWS/welcome
IBM Security 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 2.2.0 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 Security 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 Security zSecure Suite 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 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。
  - *新機能*: zSecure V2.2.0 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/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

  IBM Security zSecure Audit for ACF2 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

  メインフレームのセキュリティーとモニターに IBM Security zSecure Audit for ACF2 を使用する方法を説明します。新規ユーザーの場合、このガイドには、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。上級ユーザーのために、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

  IBM Security zSecure Audit for Top Secret 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*, LC27-6533

  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 で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に使用する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、ライセンス交付済みの製品資料およびライセンス未交付の製品資料が収録されています。この「*IBM Security zSecure: Documentation CD*」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。

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 Security zSecure Suite 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。

- 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。

IBM Security 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 Security 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 Security 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*

  この製品のインストール、構成、およびデプロイについての情報を提供します。

- *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)*

  この製品のインターフェースおよび RACF 管理と監査機能の使用法について説明します。本書には、CARLa コマンド言語と SELECT/LIST フィールドの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 コンポーネントの使用方法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*, LC27-6533

R CARLa Auditing and Reporting Language (CARLa) についての、一般ユーザーと
R 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 でセキ
R 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に使用するプログ
R 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
R 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
R 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
R 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、ライセンス交付済みの製品資料およびライセンス未交付の製品資料が収録されています。

- *Program Directory for IBM Security zSecure Manager for RACF z/VM, GI11-7865*

  この資料の情報を効率的に利用するには、プログラム・ディレクトリーから取得できる一定の前提知識が必要です。「*Program Directory for IBM Security zSecure Manager for RACF z/VM*」は、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としています。ソフトウェア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。この「Program Directory」はプロダクト・テープで提供されます。 IBM Security 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

IBM Security zSecure Admin and Audit for RACF コンポーネントについて詳しくは、「*IBM Security zSecure Admin and Audit for RACF ユーザー・リファレンス・マニュアル*」(LA88-7161) を参照してください。

この資料は、IBM Security zSecure Admin and Audit for RACF に付属の「*IBM Security zSecure Documentation CD*」(LCD7-5373) で提供されています。「*Documentation CD*」は、製品の発注およびダウンロード時にダウンロードできます。

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することもできます。

技術研修

R 技術研修の情報については、IBM Education Web サイト (http://www.ibm.com/
R training) を参照してください。

R 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、
R zSecure CARLa Training (https://www.ibm.com/developerworks/community/wikis/
R home?lang=en#!/wiki/Wa6857722838e_491e_9968_c8157c8cf491/page/zSecure%20CARLa
R %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、およびインストールまたは使用方法に関する短時間の定型質問に対する支援を提供します。IBM ソフトウェア・サポートのサイトには、http://www.ibm.com/software/support/probsub.html で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 システムまたは IT 製品は存在せず、また単一の製品、サービス、または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 概要

IBM Security zSecure Admin および IBM Security zSecure Audit for RACF は、2 つの別個の製品ですが、相互補完製品として RACF システムの管理および監査に使用できます。

zSecure Admin には、システム・レベル、グループ・レベル、および個別レベルでの RACF 管理機能に加え、RACF コマンド生成機能が組み込まれています。zSecure Audit は、RACF および z/OS のモニター機能、システム管理機能 (SMF) のレポート作成機能、z/OS 整合性検査機能、変更トラッキング機能、およびライブラリー変更検知機能を提供します。いずれの製品にも、RACF プロファイルの表示、レポート作成、および検証機能があり、Trusted Computing Base (TCB) を記述した z/OS テーブルを表示します。図 1 に、各製品で使用可能な機能と、両方の製品の相互補完機能を示します。

zSecure Admin および zSecure Audit for RACF は個別にライセンスされますが、組み合わせて使用できます。

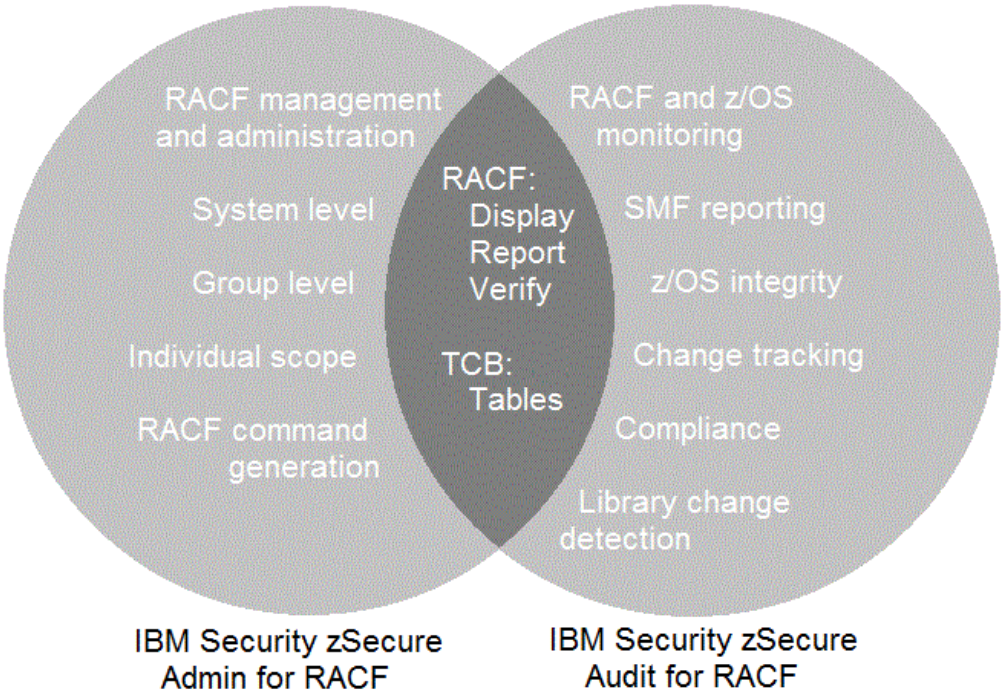


図 1. zSecure Admin および zSecure Audit のプロダクト機能

基本の処理プログラムは、バッチ・モードまたは対話モードで使用できる大規模モジュールです。対話モードが最も一般的ですが、バッチ・モードは、自動化された定期的な検査または日次レポートの生成に便利な場合があります。

zSecure Admin と zSecure Audit は、zSecure に付属のパネル、スケルトン、およびメッセージ・ライブラリーを使用して ISPF で実装された対話式ユーザー・インターフェースを備えています。 ISPF は、対話式セッション中に実行されるメインプ

ログラムであり、必要に応じて zSecure アプリケーション・プログラムを呼び出します。対話式パネルは必要に応じて CKRCARLA ロード・モジュールを呼び出します。

図 2 に、zSecure Admin および zSecure Audit の一般的なデータ・フローを示します。ユーザーは ISPF パネルで作業を行います。これにより、CKRCARLA プログラムへ送られるコマンドが生成されます。このプログラムから戻される結果は、ISPF パネルに表示されます。

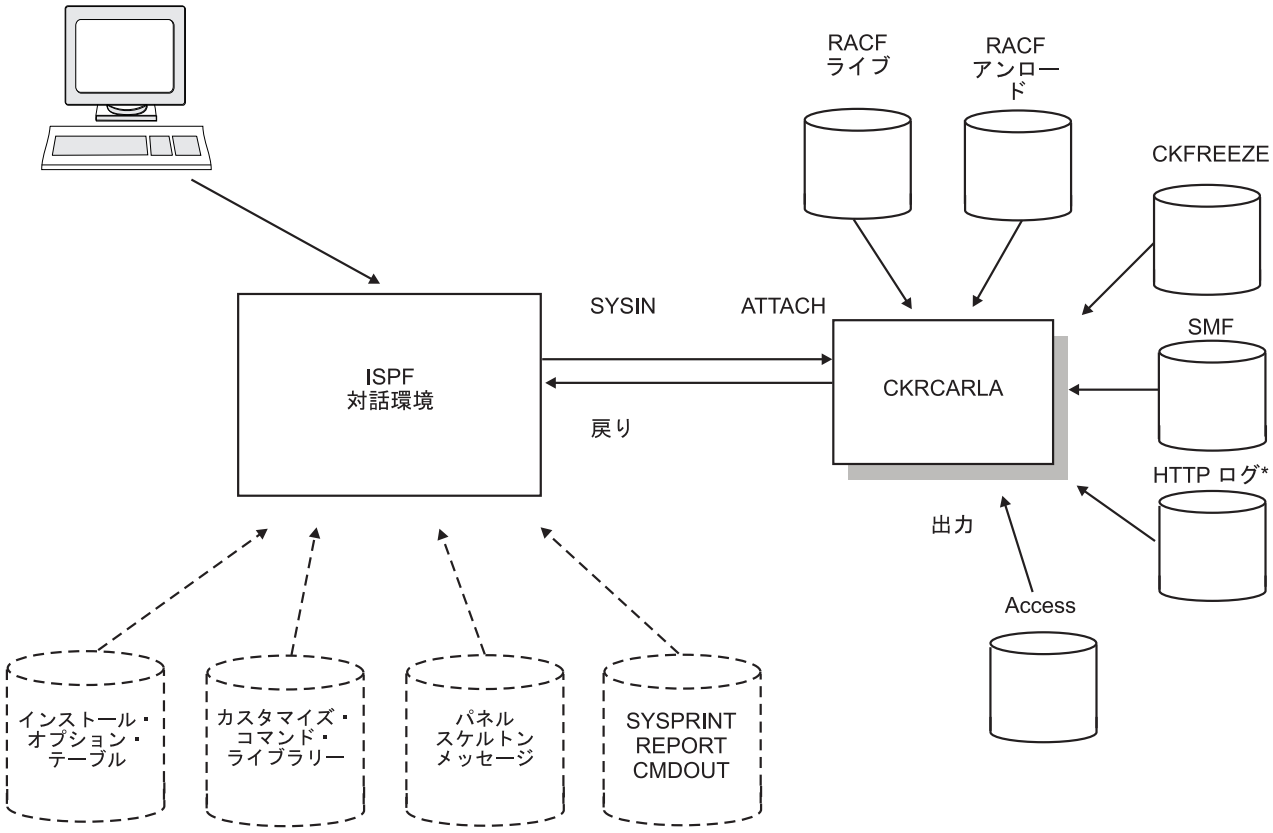


図 2. データ・フロー概念

個々の対話式コンポーネントおよび非対話式コンポーネントを使用したこの基本設計には、さまざまな実用的なメリットがあります。

- 対話式インターフェースをアプリケーション・プログラムから切り離します。こうして切り離すことにより、特に ISPF インターフェースをカスタマイズする場合に、インターフェースとプログラムの設計と使用における柔軟性が向上します。
- 対話式に実行できるすべての機能を、バッチ・モードでも実行できます。
- zSecure Admin と zSecure Audit for RACF では、ISPF パネルから、CARLa Auditing and Reporting Language (CARLa) を使用してカスタマイズされたレポートを作成し、これらのレポートを実行できます。
- TSO 接続が可能でないか、または実用的でない場合、この製品を (例えば NJE ネットワーク内で) リモートから使用できます。

CARLa Auditing and Reporting Language

IBM Security zSecure Audit for RACF はコマンド駆動型製品で、CARLa Auditing and Reporting Language (CARLa) を使用します。

ISPF を使用する標準的なユーザーは、CARLa について特に注意する必要はありません。コマンドは自動的に生成され、アプリケーション・プログラムに送られます。いくつかのコメントを除き、本書では、CARLa コマンド言語については説明しません。代わりに、本書では ISPF を介した zSecure Admin and Audit の使用法について重点的に説明します。

このコマンド言語は一般に以下の理由から使用されます。

- カスタマイズされたレポートを作成する
- バッチ・モードで製品を使用する

CARLa コマンドについては、「*IBM Security zSecure CARLa コマンド・リファレンス*」(LC27-6533) で説明しています。

標準レポートが包括的であるため、カスタマイズされたレポートは必要にならないかもしれませんが、これらのレポートを作成できます。バッチを、セキュリティー・モニター機能の一部として使用するのは魅力的です。例えば、モニター検査とレポートを自動的に実行するために、スケジュールされたバッチ・ジョブを利用できます。

CARLa ライブラリー (SCKRCARL の低位修飾子、およびデフォルトの DD 名 CKRCARLA を使用してよく参照される) に、包括的なサンプル・レポートのセットがあります。

データ・ソース

zSecure Admin および zSecure Audit for RACF は、さまざまな異なるタイプのデータを使用します。

4 ページの図 3 に、データソースと、製品によって実行される処理の概要を示します。

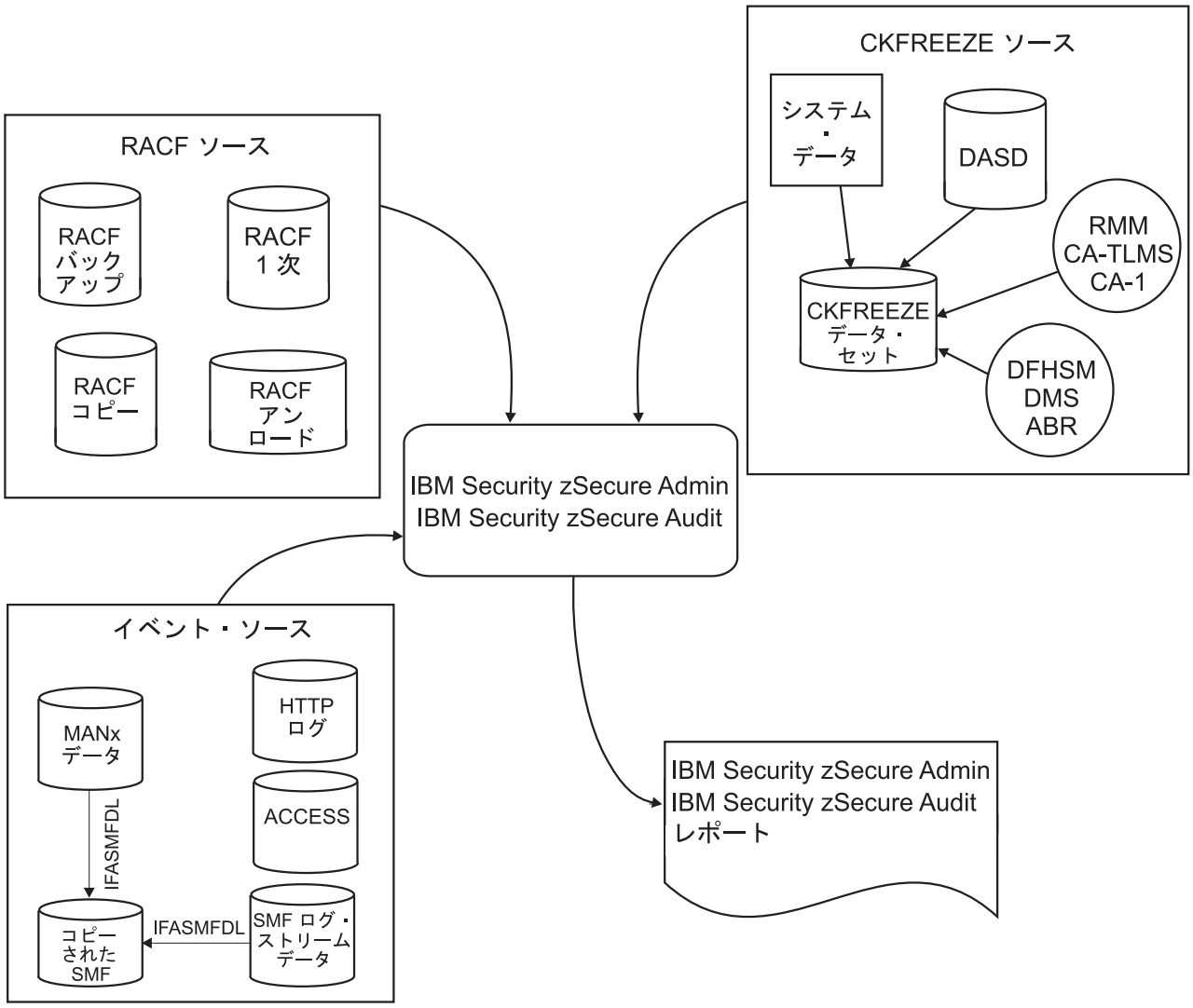


図 3. データ入力ソース

zSecure Admin および zSecure Audit for RACF には通常、RACF データが必要です。このデータは以下のソースから得ることができます。

- 基本ライブ RACF データベース
- バックアップ・ライブ RACF データベース
- アンロードされた RACF データ
- RACF データベースのコピー、または別のシステムにあるアクティブ RACF データベースのコピー

zSecure は、ライブ RACF データベースを読み取り、高速検索に適した独自仕様の形式でコピーを作成することによって、アンロードされた RACF データを作成します。

zSecure Audit for RACF の機能を使用している場合、プログラムで SMF データが必要な場合があります。SMF データは、ライブ SMF データ・セットまたは SMF ログ・ストリームから得ることも、**IFASMFDP** または **IFASMFDL** プログラムを使用して作成された順次 SMF データ・セットから得ることもできます。これらの IBM

プログラムは、ライブ SMF データ・セットと SMF ログ・ストリームから SMF レコードをアンロードします。順次 SMF データ・セットはディスクまたはテープ上に格納できますが、多くのインストール済み環境では、TSO ユーザーがテープを対話式に使用するためにマウントできない場合があります。 zSecure Audit は、RACF **REPORT WRITER** または **IRRADU00 SMF** アンロード・プログラムによって作成される疑似 SMF ファイルを処理できません。

CKFREEZE データ・セット

zSecure Audit for RACF は、DASD データを使用します。このデータは、zSecure Collect によって収集され、CKFREEZE データ・セットに書き出されます。

zSecure Collect プログラムはバッチ・ジョブとして実行され、すべてのオンラインのボリューム目録 (VTOC)、VSAM ボリューム・データ・セット (VVDS)、カタログ、選択された区分データ・セット (PDS) ディレクトリーを読み取り、要求された場合にメンバー・レベルおよびデータ・セット・レベルでデジタル署名を計算します。プログラムは、このすべてのデータを CKFREEZE データ・セットに書き込みます。

zSecure Admin および zSecure Audit for RACF は、z/OS 制御ブロック・データも使用します。zSecure Collect は、DASD データの収集時にこのデータも収集します。APF 許可機能を使用して、他のアドレス・スペースと読み取り保護された共通ストレージからデータを取り出します。また、バッチ・コレクションにより、データの収集元のリモート・システムを分析することもできます。

zSecure Admin および zSecure Audit for RACF の入力セットを定義します。例えば、1 つのセットがライブ RACF データのみから構成されることがあります。別のセットがライブ RACF データと CKFREEZE ファイルを使用します。さらに別のセットが、アンロードされた RACF データ、CKFREEZE データ・セット、および複数の SMF データ・セットを使用します。ISPF 環境では入力セットを切り替えることができます。

リモート・データおよびコマンドのルーティング

zSecure Admin および zSecure Audit では、レポートおよび表示を作成する際の入力としてリモート・データ・セットを使用できます。マルチシステム・サポートと呼ばれるこの機能を使用すると、単一セッションで複数のシステムを報告および管理できます。また、この機能は、zSecure Admin での zSecure サービスまたは RACF リモート共有機能 (RRSF) サービスを使用した RACF コマンドのルーティングのサポートと統合されています。

リモート・データを使用したレポートの作成は、プロファイルまたは設定に関する随時レポート作成処理で役立ちます。ただし、このアクセス方式は、セキュリティー・データベース全体、または CKFREEZE データ・セット全体の処理を必要とする照会には適していません。これは、大量のリモート・データへのアクセスには、同程度の量のローカル・データへのアクセスよりも時間がかかるためです。

マルチシステム・サポートを使用するには、ご使用の環境で、個別のサーバー・アドレス・スペースで実行されているアクティブな zSecure Server が必要です。このサーバーは、コマンドのルーティングと、RACF データベース、SMF 入力ファイル、CKFREEZE データ・セット、およびその他の定義済みデータ・セットへのアク

セスのためのリモート・システムとの通信に必要な機能を実行します。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。

第 2 章 基本操作

以下の手順を検討して、zSecure Admin and Audit アプリケーションを開始する方法と、RACF データをナビゲート、選択、入力、および管理する方法について学習します。

以下の作業に関する内容が記載されています。

- ユーザー、グループ、およびデータ・セット用の RACF プロファイルの表示、管理、および保守
- アクセス権限の管理
- デジタル証明書に関するレポート作成
- ユーザーの比較

始める前に

開始する前に、TSO ログオン・パラメーターと画面フォーマットを確認します。

zSecure Admin および zSecure Audit for RACF を使用する前に、ここで概説する手順に従ってください。

TSO ログオン・パラメーター

十分な大きさの領域サイズで TSO にログオンしていることを確認してください。セキュリティーの分析を開始するのに適切な領域サイズの値は 256 MB です。準拠性あるいは大量の SMF データまたはアクセス・モニター・データを分析する場合、必要なサイズはこれより大きくなります。512 MB で開始してください。非制限モードで RACF プロファイルの表示のみを行う場合、必要なサイズはこれよりはるかに小さくなります。セキュリティー・データベースのサイズ、および照会が要求する追加のルックアップ情報の量によって異なりますが、64 MB または場合によっては 32 MB でも十分なことがあります。ただし、このように小さい領域では、「Full ACL」および `ACL EFFECTIVE` コマンドを使用できないことがあります。

画面フォーマット

zSecure Admin and Audit for RACF のパネルは、24 行の大きな画面で使用されます。24 行画面を最も効果的に使用するには、いずれかの ISPF パネルのコマンド行で **`PFSHOW OFF`** コマンドを入力します。Enter を押し、ISPF が画面の最後の 1 行または 2 行に自動的に表示する PF キーの定義情報を非表示にします。PF キー定義を復元するには、**`PFSHOW ON`** コマンドを使用します。

製品の開始

製品をインストールした後、以下のタスクを実行して、zSecure Admin and Audit アプリケーションを開始し、通常のタスクを実行するための準備をします。

手順

開始するには、次の手順で行います。

1. 「**オプション**」行に **6** を入力し、Enter を押して ISPF コマンド・シェルを開きます。
2. コマンド **CKR** を入力し、Enter を押してください。

   このコマンドによって、zSecure Admin および zSecure Audit for RACF が結合された製品が開始します。コマンドを入力した後、図 4 に示すようなメインメニューが開きます。

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
                          zSecure Admin+Audit for RACF - Main menu
Option ===> ____________________________________________________________________

SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
RE   Resource        Resource reports
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

Input complex:   Active backup RACF data base

Product/Release
5655-N16 IBM Security zSecure Admin 2.2.0
5655-N17 IBM Security zSecure Audit for RACF 2.2.0
```

A

図 4. zSecure Suite - メインメニュー

   このパネルに初めて入ったときは、主要な選択オプションのみが表示されます。

3. 必要に応じて、オプション SE.R を使用して、すべての設定をデフォルト設定にリセットします。
4. オプションを選択するには、コマンド行に 2 文字の省略形を入力して、Enter を押します。

   選択されたオプションに応じて、メニューが展開して詳細なオプションが表示されるか、次の選択のためのサブメニューが表示されます。

   製品の習熟度が高まると、当該機能内の任意の他のパネルに直接ジャンプするためのジャンプ・コマンド **=***X* を知っておくと役立つことがあります。ここで、*X* はパネル ID です。例えば、任意の RA パネル (RACF 管理) で、コマンド **=G** を入力することで、RA.G パネル (CKGRACF を使用したグループ管理) にジャンプできます。

次のタスク

以下のセクションでは、製品が正しく機能することを確認するために、一部の表示機能を使用する方法について説明します。入力には稼働中の RACF データベースが使用されます。通常、稼働中の RACF データベースと一緒に zSecure を使用しても、実稼働に目立った影響は生じません。

RACF プロファイルの保守

プロファイルの概要を表示してから、保守するものを選択することで、RACF プロファイルを保守できます。

このタスクについて

プロファイル選択パネルには、データを選択または除外するためのフィールド (フィルター とも呼ばれる) があります。デフォルトでは、すべてが選択されて、何も除外されていません。使用例を参照するには、以下のステップを実行します。

手順

1. メインメニューで、「**オプション**」行に **RA** (RACF 管理) と入力し、Enter を押して、RACF データベースの表示および保守のためのオプションを表示します。
2. 「オプション」行に **G** (グループ) と入力し、パネルにパラメーターを入力せずに Enter を押します。
3. デフォルト・プロンプトで、Enter を押します。

タスクの結果

この手順を実行した後、zSecure Admin および zSecure Audit for RACF は、パネルの機能に関する RACF データベース内のすべての情報 (この例ではグループ・プロファイル情報) を表示します。選択パラメーターまたは除外パラメーターを 1 つか 2 つ指定することによって、パネルに表示されるデータの量を削減することができます。

ヒント: レコード・レベル表示で **FORALL** 基本コマンドを使用して、コマンドを現行表示のすべてのプロファイルに適用することを指定できます。パラメーターを指定しない場合、基本コマンド **FORALL** では、コマンドを入力できるパネルが表示されます。**FORALL** コマンドで直接コマンドを入力することもできます。

この例では、稼働中の RACF データベースを使用して、稼働中の RACF データベースでの zSecure Admin and Audit の速度および非干渉性に関するデモンストレーションを行います。 61 ページの『データの追加』では、アンロードされた RACF データベースの作成についてガイドします。アンロードされたデータベースは、本書のテキストおよび例で使用します。

次のタスク

zSecure Admin は、グループ・レベル、ユーザー・レベル、および単一エントリー・レベルでのプロファイルの保守に役立ちます。グループおよびユーザーの構造を素早く見つけ出し、ご使用の組織構造に基づいて構造を変更することができます。

インターフェースの使用方法とコマンドの管理方法を学習した後は、一般的な保守
5 機能、権限を委譲した (または非集中型の) 保守、および特殊権限が不要なパスワードの保守を使用可能にして、ヘルプ・デスクで作業負荷をシフトする方法を学びます。

ユーザー・プロファイルの表示

手順

1. メインメニューが開いていない場合、PF3 を押してメインメニューに戻ります。
2. 「オプション」行に RA (RACF 管理) と入力し、Enter を押して、RACF データベースの表示および保守のためのオプションを表示します。
3. 「RA」メニューから、オプション **U** (ユーザー) を選択します。Enter を押すと、「ユーザー選択」パネルが開きます。図 5を参照してください。

   このパネルには、最も使用頻度の高い選択項目の一部が提供されています。これは次の部分で構成されます。

   - Add new user or segment
   - Additional selection criteria
   - Output/run options

   いずれかのオプションの前に「/」を指定して選択した選択基準または出力/実行オプションによっては、選択基準をさらに指定するための別のパネルが表示されることもあります。
4. 選択を行った後、PF3 を押して「ユーザー選択」パネルに戻るか、Enter を押して照会を実行します。

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
       zSecure Admin+Audit for RACF - RACF - User Selection
 Command ===> _____________________________________________   _ start panel

 _   Add new user or segment

 Show userids that fit all of the following criteria
 Userid  . . . . . ________     (user profile key or filter)
 Name  . . . . . . _____________________________ (name/part of name, no filter)
 Installation data . _____________________________ (data scan, no filter except *)
 Owned by  . . . . . ________     (group or userid, or filter)
 Default group . . . ________     (group or filter)
 Connect group . . . ________     (group or filter)

 Additional selection criteria
 _  Other fields       _  Attributes       _  Segment presence  _  Absence

Output/run options
_  Show segments       _ All               _ Specify scope
_  Show differences
_  Print format          Customize title     Send as e-mail
      Background run     Full page form      Sort differently     Narrow print
```

図 5. 「ユーザー選択」パネル

5. 「**ユーザー ID**」フィールドに、ユーザー ID を入力します。

   ヒント: 追加印刷オプションは「**Print format**」フィールドが活動化されている場合にのみ使用可能です。このフィールドを活動化するには、「**Print format**」選択フィールドに / を入力します。
6. Enter を押します。 zSecure Admin and Audit for RACF は RACF データベースを検索し、 11 ページの図 6 に示すようなユーザー・プロファイル概要パネル

を開きます。

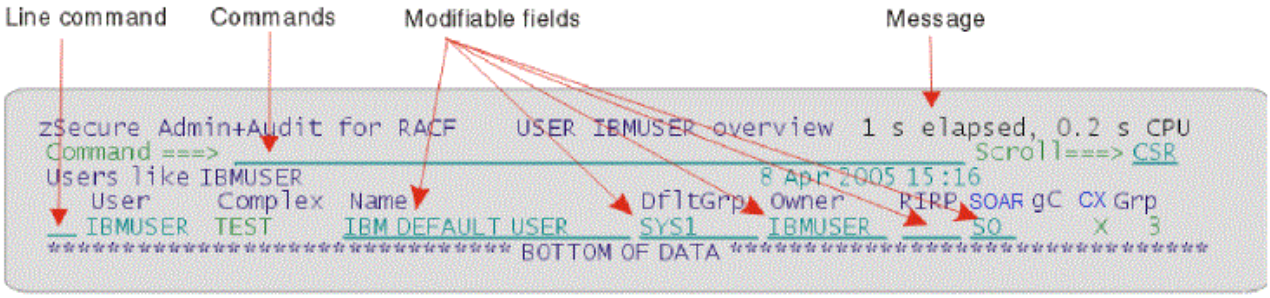


図 6. 選択されたユーザーの概要の表示

パネルの右上の行に表示されるメッセージは、照会の実行に使用された経過時間およびプロセッサー時間を示すパフォーマンス情報です。

この概要表示には、選択された各ユーザー・プロファイルが 1 行で表示されます。情報量が多い場合には、上下左右にスクロールして追加情報を表示できます。

一部のフィールド値は編集でき、例えば「**名前**」列の項目などが該当します。ISPF オプション設定および端末タイプによっては、編集 (変更) 可能なフィールドは、アンダースコアーで示されるか、または編集できないフィールド、例えば、「**ユーザー**」フィールド の色とは異なる色で表示されます。変更可能フィールドに新しい値を入力すると、zSecure Admin はプロファイルをその新しい値に変更する、該当するネイティブの RACF コマンドを生成します。

7. オプション: 以下の手順を使用することによって、ほとんどのパネルの ISPF の表示色を変更できます。
   a. メニュー・バーから「**オプション**」を選択します。
   b. 「オプション」メニューから、「**1. 設定**」を選択します。
   c. バーから「**Colors**」を選択します。
   d. 「**2. CUA attributes**」を選択します。
   e. 変更を指定した後、Enter を押して変更内容を適用します。 変更内容は次回照会を実行するときに有効になります。

プロファイル表示のラベルは表 1 に示すように短縮されています。

表 1. プロファイル表示ラベルの説明

ラベル	説明
RIRP	プロファイルが **R** (取り消し)、**I** (非アクティブ)、**R** (制限付き)、または **P** (保護) のどれであるかを示すフラグ・フィールド
SOAR	次の属性の設定を示します。**S** (特殊)、**O** (操作)、**A** (監査員)、および **R** (ROAudit)
gC	**g** (グループ権限が存在する) および **C** (クラス権限が存在する) を示します

表 1. プロファイル表示ラベルの説明 (続き)

ラベル	説明
CX	次の条件が真であるかどうかを示します。 • ユーザーが証明書を持つ (**C**) • パスワードが期限切れである (**X**)

これらのフィールド説明は、ISPF インターフェースで使用可能な統合型のヘルプ・パネルからも利用できます。ほとんどのパネルでは、パネル・レベル・ヘルプおよびフィールド・レベル・ヘルプにアクセスできます。パネル・ヘルプおよびフィールド依存のヘルプは、レコード・レベルおよび詳細レベルの両方で、すべてのセキュリティー・データベース表示において使用可能です。

- フィールド・ヘルプについては、興味のあるフィールド内にカーソルを置いて PF1 を押します。
- パネル・ヘルプについては、コマンド行にカーソルを置いて PF1 を押します。

ヒント: zSecure の多くのデータ表示は 80 行より幅が広くなります。右または左にスクロールするには、PF11 および PF10 キーを使用します。

8. プロファイルの詳細な情報を表示するには、以下のステップを実行します。
   a. 行コマンド・フィールド内の表示されているプロファイル行の先頭にカーソルを移動して、Enter を押します。
   b. 次のいずれかの方法を使用して、パネル内の項目を選択します。
      - 行コマンド・フィールドにカーソルを置き、Enter を押します。
      - **S** コマンドを入力して、Enter を押します。

      C (コピー) や **D** (削除) などの追加の行コマンドも使用可能です。これらのコマンドは、後で扱います。

      ヒント:

      - 特定のプロファイルについて使用可能な行コマンドが分からない場合、**/** と入力して Enter を押します。このアクションによって、適用可能なすべての行コマンドを示すパネルが開きます。
      - レコード・レベル表示で **FORALL** 基本コマンドを使用して、現行表示のすべてのプロファイルにコマンドを適用できます。パラメーターを指定しない場合、**FORALL** 基本コマンドはコマンドを入力するためのパネルを表示します。**FORALL** コマンドで直接コマンドを入力することもできます。
9. ユーザー選択パネルに戻るには、PF3 を押します。詳細概要を表示している場合は、PF3 を 2 回押します。
10. 次に、もう少し面白い操作を試してみます。例えば「**ユーザー ID**」フィールドに SYS* と入力して、SYS* で始まるすべてのユーザー・プロファイルを表示する操作を実行します。表示されたユーザー・プロファイルの行を選択して、これらのユーザーの詳細情報を検査できます。RACF データベースに対する適切な権限を持つ場合、パネルのフィールド値を編集してこれらのフィールドの多くを変更できます。新しい値を指定すると、zSecure は不注意による変更を回避するために検査を行います。この例では、変更を加えないでください。

注: フィールドに選択基準を指定する際、汎用文字のアスタリスク (*) およびパーセント記号 (%) を使用できます。

ユーザー選択パネルの使用

このタスクについて

ユーザー選択パネルは以下のセクションに分割されています。

- 最初のセクションを使用してユーザーまたはセグメントを追加します。
- 2 番目のセクションを使用して、最も一般的に使用される RACF 管理の選択基準を指定します。
- 3 番目のセクションは、ほとんどの場合、より拡張された選択基準を使用して RACF データベースに関するレポートを作成する場合に使用します。例えば、**SPECIAL** 属性と **OPERATIONS** 属性を持つすべてのユーザー・プロファイルに関するレポートを作成できます。
- 照会からの結果の出力をカスタマイズするには、4 番目のセクションを使用します。例えば、「**Show differences**」フィールドに **/** と入力して、2 つの入力ソースを比較できます。

  この比較を行うには、**SETUP FILES C** アクション・コマンドを使用して設定したベースライン入力を 1 つ、および **SETUP FILES S** アクション・コマンドを使用した通常メインセットを少なくとも 1 つ選択する必要があります。

  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。

手順

1. 拡張された選択基準 (3 番目のセクション) および出力のカスタマイズ (4 番目のセクション) についてフィールドを選択するには、フィールドの横に **/** を入力します。Enter を押します。

   注: パネルの 4 番目のセクションのほとんどは、「**Print format**」フィールドの前に **/** を入力して Enter を押すことによってこのフィールドを選択した場合にのみ変更できます。「**Send as email**」オプションを使用するには、SMTP 構成パラメーターを指定しておく必要があります。70 ページの『E メール出力の SMTP オプション』での説明に従って、「セットアップ」の出力定義パネルでパラメーターを指定します。ここでは、「**Print format**」オプションを選択せずに続行します。

   zSecure は、ユーザー選択パネルに入力された基準に一致するすべてのユーザー・プロファイルを表示します。特定のフィールドで何も指定しなかった場合、そのフィールドは検索中に無視されます。複数のフィールドで **/** を使用できます。 **/** の意味は、そのオプションが選択され、指定されたパラメーター (複数可) に一致するプロファイルが表示される (または追加の選択パネルが表示される) ということです。また、ほとんどのフィールドで選択オプションを活動化するための **S** コマンドも使用できます。ブランクは、プロファイルを選択する際に、そのオプションが無視されることを意味します。

例えば、「**Attributes**」フィールドで **/** と入力すると、図 7 に示されている「User Attributes」パネルが開きます。

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
                        zSecure Admin+Audit for RACF - RACF - User Attributes
Command ===> ____________________________________________________________________
All users
Specify groups of criteria that the userids must meet:
Systemwide and group authorizations
OR     _   Special       _   Operations    _   Auditor      _   RO-auditor
       _   Group-special _   Group-oper    _   Group-audit  _   Class auth

Logon status
OR     _   Revoked       _   Inactive      _   Protected    _   Passw expired
       _   Revoked group _   Certificate   _   Pass phrase  _   Phrase expired
       _   When day/time _   ID mapping    _   Passw legacy _   Phrase legacy

User properties
OR     _   Has RACLINK   _   Restricted    _   User audited _   Mixed case pwd

CKGRACF features
OR     _   Queued cmds   _   Schedules     _   Userdata     _   MultiAuthority

Connect authority . __    _  1. Use   2. Create   3. Connect  4. Join
```

図 7. 「User Attributes」パネル

2. システム全体の権限を持つすべてのユーザー・プロファイルを表示するには、「**Systemwide and group authorizations**」セクションの「**Operations**」フィールドに **/** を入力します。次に、Enter を押します。 この操作により、システム全体の操作権限を持つすべてのユーザー・プロファイルが表示されます。
3. 「**Connect authority**」フィールドで、指定された接続権限に基づいてユーザーを選択します。 接続権限に適用されている比較演算子を満たすグループ接続を少なくとも 1 つ持っているユーザーのみが表示されます。 表 2 に示されている比較演算子を使用してください。

*表 2. 「**Connect authority**」フィールドの比較演算子*

演算子	説明
<	指定されたアクセス権限より低い
<=	指定されたアクセス権限より低いか、(最高でも) それと同じ
>	指定されたアクセス権限より高い
>=	指定されたアクセス権限より高いか、(最低でも) それと同じ
=	正確に一致するアクセス権限
~= または <>	指定されたアクセス権限以外のすべて

ヒント: zSecure Admin および zSecure Audit for RACF は、特に指定のない限り、指定したすべてのプロパティーを AND ロジックで結合します。

/ を使用するほかに、xxx Y および N も使用できます。グループ内の入力フィールドで、AND 演算子を指定して Y および N の値を使用することによって、Y で選択された属性を持ち、N で選択されたいずれの属性も持たないユーザーを検索できます。

「**Logon status**」セクションの「**Revoked**」オプションは、現在取り消されているユーザーを検査します。

「**Password interval**」フィールドは、パスワードが期限切れになる対象のユーザーをチェックします。このフィールドは、「RA.U」パネルの「**Other fields**」フィールド内で / を指定したときに表示されるパネルで使用できます。このフィールドを選択した後、Enter を押すと、データを選択するための属性を指定する「User Attributes」パネルが開きます。パスワードが期限切れでなく特殊権限を持つユーザーを検索するか、パスワードが期限切れでなく操作権限を持つユーザーを検索します。そのようなユーザーを検出した場合 (おそらく IBMUSER でないユーザー)、ユーザーがそのように定義された理由を調査する場合もあります。

別の例として、「**Specify scope**」フィールドに / を入力して、別のユーザー ID またはグループの範囲内のプロファイルを検査することができます。このオプションを選択すると、ユーザー ID またはグループ ID を指定するためのパネルが開きます。

フィルターの記法

入力データを選択または除外するためのフィルター基準を指定するには、以下のガイドラインに従ってください。

多くのパネルの入力フィールドでは、データの選択または除外にフィルターを使用できます。これらのフィルターは、次に示す任意のワイルドカード文字を含めることができるストリングです。

% 非ブランクの 1 文字に相当します。

***** 単一ストリング内の任意数の文字 (ドット以外) に相当し、例えば単一のデータ・セット名修飾子またはユーザー名などが該当します。

****** プロファイル名の末尾にある任意数の修飾子に相当します。

: 名前の内部にある指定された文字を検索しますが、クラス名またはデータ・セット修飾子は検索しません。

zSecure Admin および zSecure Audit for RACF では、RACF が拡張総称命名 (EGN) モードであるかどうかにかかわらず、EGN 表記を使用します。

日付の表記

さまざまな操作で日付および日付範囲を指定するには、以下のガイドラインに従ってください。

いくつかの選択フィールドは日付を意味します。さまざまな値と演算子を使用できます。ただし、すべての年の値は 4 桁で指定する必要があります。表 3 に、日付選択の値と演算子の例を示します。

表 3. 日付選択の値と演算子の例

操作	意味
= 04jul2004	2004 年 7 月 4 日
< 04jul2004	2004 年 7 月 4 日より前の任意の日付

表 3. 日付選択の値と演算子の例 (続き)

操作	意味
= never	日付の設定なし
= today	今日発生した活動
= today-3	今日から 3 日前
< today-30	30 日以前
> 01jan2005	2005 年 1 月 1 日より後の任意の日付

値 **DUMPDATE** による日付は、 RACF データベースがアンロードされた日付です。稼働中の RACF データベースを使用している場合、値 **DUMPDATE** を指定することは、値 **TODAY** を使用することと同じです。

注: 日付を選択フィールドに入力するとき、演算子は 2 文字の小さい入力フィールドに指定し、日付の値は大きいフィールドに指定する必要があります。

アプリケーション・セグメントの表示

手順

1. ユーザー・プロファイルのアプリケーション・セグメントを表示するには、アプリケーション・セグメントを表示する対象のユーザー ID を「User Selection」パネルに指定します。
2. ユーザー・プロファイルの前にアクション・コマンド **SE** を入力します。このユーザーに対して定義されたアプリケーション・セグメントのリストを含むパネルが開きます。

   ヒント: SE アクション・コマンドを使用する代わりに、ユーザー選択パネルの「**Output/run options**」セクションで、「**Show segments**」の前に **/** を入力できます。このアクションによって「User Segments」パネルが開き、表示するセグメントを指定できます。「**Additional selection criteria**」セクションで「**Show segments**」と一緒に「**Segment presence**」を選択した場合、セグメントのリストを含むパネルが開きます。セグメント情報に基づいてセグメントを選択し、追加の選択基準を指定できます。例えば、TSO セグメントの出力設定に基づいてユーザーを選択できます。

グループ・プロファイルの表示

このタスクについて

このセクションでは、グループ・プロファイルを表示および照会する手順について説明します。

グループ・プロファイルを表示するには、以下のステップを実行します。

手順

1. End または Enter を押してメインメニューに戻ります。
2. RA メニューから、 オプション **G** (グループ) を選択し、Enter を押して、「Group Selection」パネルを開きます。

図 8 に示されているこのパネルは、グループ・プロファイルに適用される、最も頻繁に使用される選択の一部を提供します。「ユーザー選択」パネルと同様に、このパネルにも以下のセクションがあります。

- **Add New Group or Segment**
- 共通の選択基準
- **Additional selection criteria**
- **Output/run options**

R / 文字を使用して選択した、追加の選択基準または出力/実行オプションによって
R は、選択基準をさらに指定するための別のパネルが表示されます。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
          zSecure Admin+Audit for RACF - RACF - Group Selection
Command ===> _____________________________________________________   _ start panel

_   Add new group or segment

Show groups that fit all of the following criteria
Group id  . . . . . ________     (group profile key or filter)
Owner . . . . . . . ________     (group or userid, or filter)
Subgroup of . . . . ________     (group or filter)
With subgroup . . . ________     (group or filter)
Installation data . ________________________ (data scan, no filter except *)

Additional selection criteria
_  Profile fields     _  Connect fields   _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Expand universal  _  Specify scope
_  Show differences
_  Print format          Customize title     Send as e-mail
      Background run     Full detail form    Sort differently     Narrow print
      Print connects     Print names         Print subgroups
```

図 8. 「グループ選択」パネル

R 3. 「**グループ ID**」フィールドに、デフォルト・グループ名、またはグループ名の
R ストリングを入力します。例えば、ストリング「C≠MC*」で始まるすべてのグル
R ープ・プロファイルの場合は「**グループ ID**」フィールドに「C≠MC*」と入力しま
R す。

4. Enter を押して RACF データベースを検索すると、グループ・プロファイル情報が「Group Overview」パネルに表示されます。

   表示内容 (18 ページの図 9 を参照) は、表示される列が異なることと、ユーザー・プロファイルでなくグループ・プロファイルが表示されることを除いて、「ユーザー選択」の概要と似ています。

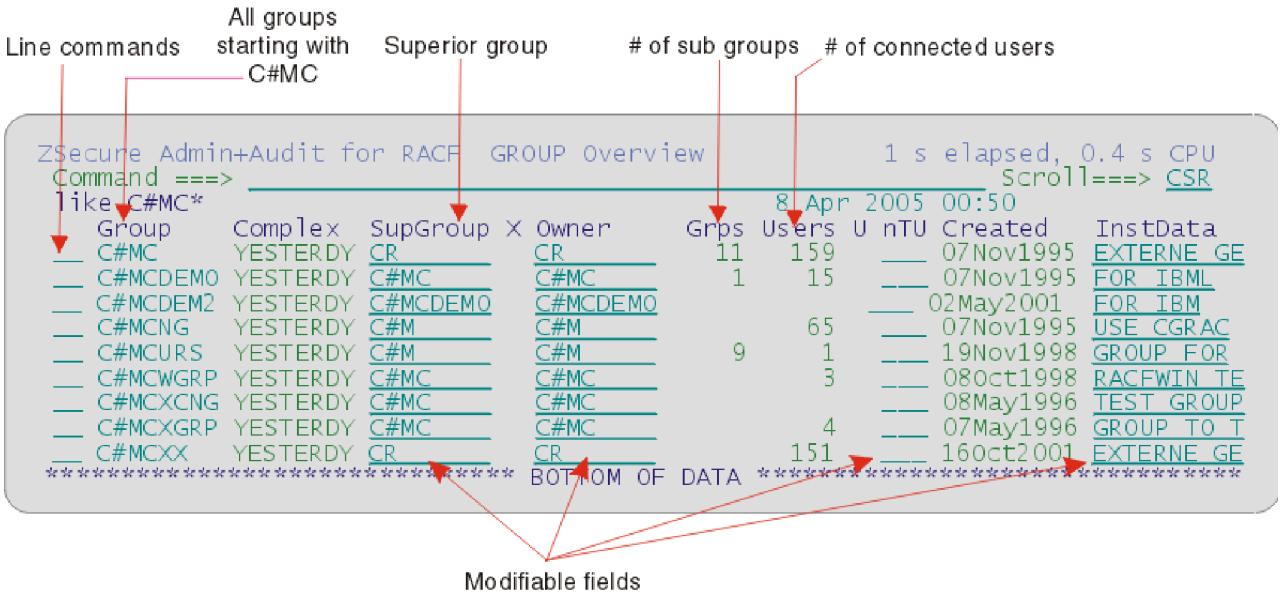


図 9. 「Group Overview」パネル

汎用グループ

すべての RACF プロファイルには最大サイズがあります。すべての接続済みユーザーの接続情報は、通常のグループ・プロファイルに格納されます。つまり、グループ・プロファイルに接続できるユーザーの最大数が存在することを暗黙に示しています。最大数は約 6000 ユーザーです。大きい RACF データベースの場合、この数では十分でないことがあります。 この制限が、*汎用グループ* が存在する理由です。 **汎用**属性がグループ・プロファイルに割り当てられると、*デフォルト接続* のユーザー (**USE** 権限でグループに接続し、接続属性を持たない) は、グループ・プロファイルに保管されません。グループ **SPECIAL**、グループ **OPERATIONS** などの接続属性、または **USE**を超える接続権限があるユーザーのみが、グループ・プロファイルに保管されます。

汎用グループの利点は、無制限の数のユーザーを接続でき、グループ・プロファイルの最大サイズに到達することがないことです。したがって、大規模な RACF データベースにおいて、大きなグループを分割する必要はなくなりました。大きなグループを分割する場合は、グループのコピーを作成し、追加のユーザーをこの新規グループに接続します。

汎用グループの欠点は、グループ・プロファイルを表示してもグループに接続しているユーザーを判別できないことです。この汎用グループに接続しているユーザーを見つけるには、すべてのユーザー・プロファイルを検索する必要があります。zSecure Admin および zSecure Audit では、「Expand universal」機能を使用してこの検索を自動化できます。

注: この機能を使用すると完全なデータベース読み取りを行うことが暗黙に指定されるため、応答時間が大幅に延長する可能性があります。

グループ・プロファイルの **UNIVERSAL** 属性には、「**汎用グループ**」と「**Expand universal**」の 2 つのフィールドが関連します。「**プロファイル**」フィールドの前に **/** を入力すると、図 10 に示すパネルに類似したパネルが開きます。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
        zSecure Admin+Audit for RACF - RACF - Group Selection
Command ===>
All profiles
Show groups that also fit all of the following criteria:
Selection by date
Creation date . . . __   __________          (date: yyyy-mm-dd/ddMMMyyyy/
                                                   DUMPDATE/DUMPDATE-nnn/
                                                   TODAY/TODAY-nn/NEVER)


Miscellaneous fields
Complex . . . . . ________     (complex name or filter)
# connected users . __   ____                (operator: < <= > >= = <> = ¬=)
# subgroups . . . . __   ____

Enter "/" to specify selection criteria
_  Universal group
_  Queued commands
_  Userdata
```

図 10. グループ・プロファイル・フィールド選択パネル

汎用グループ機能を使用するには、以下のいずれかのアクションを実行します。

- 図 10 に示すパネルで、「**汎用グループ**」フィールドに **/** を入力します。

  この選択では RACF データベースの汎用グループのみを検索します。
- 17 ページの図 8 に示す「Group Selection」パネルの「**Expand universal**」フィールドに **/** を入力します。

  この選択によって、デフォルト以外の接続ユーザーだけでなく、接続されているすべてのユーザーが詳細概要に表示されます。

ヒント: 「Expand universal」オプションの機能を理解するには、汎用グループを 2 回リストします。ここで、最初はオプションを使用可能に設定してグループをリストし、次にオプションを使用不可に設定してグループをリストします。接続されているユーザーのリストの差異に注目します。

ユーザーの接続および削除

ユーザーをグループに接続するには、以下のいくつかの方法があります。

- グループ・プロファイルまたはユーザー・プロファイルの概要パネルで **CO** 行コマンド (接続) を発行します。
- グループ・プロファイルまたはユーザー・プロファイルの詳細パネルにおいて、ユーザーあるいはグループの接続詳細を含む行の先頭で、**C** (コピー) または **D** (削除) の行コマンドを使用する。
- 接続情報を含む行の現行値を編集 (上書き) する。このアクションでは、入力された新しい値についての新規接続コマンドが生成され、上書きされた値の削除コマンドが生成されます。**削除**コマンドを実行したくない場合は、コマンド確認パネルから削除コマンドを削除した後、Enter を押します。

ユーザー・プロファイルまたはグループ・プロファイルで行コマンド **CO** を使用すると、図 11 に示すような接続パネルが開きます。(グループ・プロファイルの場合、最大 10 ユーザーまでの接続を 1 回の操作で追加できます。)

```
  Menu         Options       Info    Commands     Setup
 ____________________________________________________________________________
                          zSecure Suite - RACF - Add connect
 Command ===> ____________________________________________________________

 Create new connect
Userid . . . . . . . . CRMCKF1

Group . . . . . . . . . ________ (group or filter)

Optional connect attributes
Authority . . . . . . . ________ (USE ,CREATE ,JOIN or CONNECT)
Default UACC  . . . . . ________ (N/R/U/C/A)
Connect owner . . . . . ________
Future revoke date  . . ________ (MM/DD/YY)
Future resume date  . . ________ (MM/DD/YY)
_  Revoke           _  Norevoke
_  Special          _  Operations      _  Auditor

Enter a group for a single connect.
Leave the field blank or enter a filter (e.g. IBM*) to get a selection
list.
```

図 11. 「Add / copy connect」パネル

- ユーザーを別のグループに接続するには、このパネル (図 11 を参照) を使用します。このパネルでは、「**ユーザー ID**」フィールドを変更できません。グループ・プロファイルに対して **CO** コマンドを発行する場合は、その代わりに「**グループ名**」フィールドを変更できません。
- オプションで、パネルの下半分で接続属性を指定できます。
- **CO** コマンドの代わりにユーザー・プロファイルまたはグループ・プロファイルの詳細パネルで行コマンド **C** を使用すると、同じユーザーを別のグループに接続できます。また、別のユーザーを同じグループに接続することもできます。接続パネルの「**ユーザー ID**」フィールドと「**グループ**」フィールドを同時に変更して、別のユーザーを別のグループに接続することもできます。

データ・セット・プロファイルのレビュー

手順

データ・セット・プロファイルを表示するには、以下のステップを実行します。

1. メインメニューに戻るには、「Group Selection」パネルで「終了」(PF3) を押します。
2. オプション **D** を選択して「Data set Selection」パネルを開きます。

   現在の状態は、RACF のサブ選択パネルのままです。このパネル (21 ページの図 12 を参照) は、通常はデータ・セット・プロファイルについて照会する場合に使用され、使用方法はユーザー・プロファイル・パネルとほぼ同じです。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
       zSecure Admin+Audit for RACF - RACF - Data set Selection
Command ===> _____________________________________________________   _ start panel

_   Add new DATASET profile or segment

Show dataset profiles that fit all of the following criteria
Dataset profile . . _____________________________________________ 1 1 EGN mask
Owned by  . . . . . ________     (group or userid, or filter)       2 Exact
High level qual . . ________     (qualifier or filter)              3 Match
Installation data . ________________________ (substring or *)     4 Any match

Additional selection criteria
_  Profile fields     _  Access list      _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Enable full ACL   _  Specify scope
_  Show differences
_  Print format          Customize title     Send as e-mail
      Background run     Full detail form    Sort differently     Narrow print
      Print ACL          Resolve to users    Incl operations      Print names
```

図 12. 「Data set Selection」パネル

3. フィールドを必要な数だけ基準として指定できます。 フィールドに何も入力しないと、そのフィールドはデータベース検索中に選択または除去の基準として使用されません。何も情報を指定せずに Enter を押すと、すべての既存のデータ・セット・プロファイルが表示され、通常はデータが多すぎる結果になります。

   「**データ・セット・プロファイル**」は「Data set Selection」パネルで最も重要なフィールドです。探しているプロファイルの名前が分かっている場合、「**Exact**」を指定できます。また、プロファイルを含む「**EGN mask**」を指定したり、「**Match**」を使用してデータ・セットを含むプロファイルとデータ・セット名のマッチングを行ったり、一致するすべてのプロファイルを探したり (「**Any match**」) することができます。例えば、次のようになります。

   a. SYS1.** と入力し、「**EGN mask**」を表す「**1**」以外は、他のすべてのフィールドを空白にします。

      EGN では、名前パターン SYS1.* (アスタリスク 1 つ) は、SYS1 の後ろに単一修飾子を持つすべての名前に一致することを思い出してください。SYS1.**(アスタリスク 2 つ) と指定した場合、この値は SYS1 の後ろに任意の数の修飾子を持つ名前に相当します。例えば、SYS*.** というフィルターを使用することによって、SYS で始まるすべてのプロファイルを見つけることができます。

   b. Enter を押します。

      この例では、SYS1 で始まるすべてのデータ・セット・プロファイルを表示するパネルが開きます。このパネルは、 22 ページの図 13 に示すパネルに似たものです。

```
zSecure Admin+Audit for RACF DATASET Overview          1 s elapsed, 0.2 s CPU
Command ===> _____________________________________________ Scroll===> CSR_
like SYS1.**                                    8 Apr 2005 00:25
   Profile key                                 Type    UACC    Owner    S/F W
__ SYS1.ACDS                                   GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.BRODCAST                               GENERIC UPDATE_ SYSPROG_ __R _
__ SYS1.CMDLIB                                 GENERIC READ___ SYSPROG_ U_R _
__ SYS1.COMMDS                                 GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.C#M.LINKLIB                            GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.CSSLIB                                 GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.DFQLLIB                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.DGTLLIB                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.DUMP*.**                               GENERIC NONE___ SYSPROG_ R_R _
__ SYS1.HASPACE                                GENERIC NONE___ SYSPROG_ R_R _
__ SYS1.IBM.PARMLIB                            GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.IBM.PROCLIB                            GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ICEDGTL                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ICEISPL                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ISAMLPA                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ISP*                                   GENERIC NONE___ SYSPROG_ __R _
__ SYS1.JESCKPT*.**                            GENERIC NONE___ SYSPROG_ R_R _
__ SYS1.LINKLIB                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.LOCAL.LINKLIB                          GENERIC READ___ SYSPROG_ U_R _
__ SYS1.LOCAL.VTAMLIB                          GENERIC READ___ SYSPROG_ U_R
```

図 13. データ・セット・プロファイル

以下に示す他の選択基準も使用できます。

- 最適一致の結果

a. データ・セット概要を終了して「data set Selection」パネルに戻るには、PF3 を押します。

b. 「**データ・セット・プロファイル**」フィールドに、SYS1.DUMP00 と入力して、「**一致**」を表す **3** を選択し、Enter を押します。

図 14 に示すパネルのようなパネルが開き、SYS1.DUMP00 に最も一致するプロファイルが表示されます。

```
zSecure Admin+Audit for RACF DATASET Overview            1 s elapsed, 0.4 s CPU
 Command ===> _____________________________________________ Scroll===> CSR_
 exact match SYS1.DUMP00                        8 Apr 2005 00:25
    Profile key                                 Type    UACC    Owner    S/F W
 __ SYS1.DUMP*.**                               GENERIC NONE___ SYSPROG_ R_R _
 ****************************** BOTTOM OF DATA ********************************
```

図 14. 最適一致の結果

- すべての一致の結果

a. データ・セット概要を終了して「data set Selection」パネルに戻るには、PF3 を押します。

b. 「**データ・セット・プロファイル**」フィールドは SYS1.DUMP00 の値のままにし、「**Any match**」を表す **4** を選択して Enter を押します。

23 ページの図 15 に示すパネルのようなパネルが開き、SYS1.DUMP00 に一致するすべてのプロファイルが表示されます。最も適合したプロファイルは先頭行に表示されます。さらに、先頭のプロファイルが削除された場合、リソースに一致する可能性がある、固有性の低いプロファイルが表示されます。

```
zSecure Admin+Audit for RACF RACF DATASET Overview         1 s elapsed, 0.5 s CPU
 Command ===> ____________________________________________________ Scroll===> CSR_
 any match SYS1.DUMP00                                 8 Apr 2005 00:25
    Profile key                                        Type    UACC    Owner    S/F W
 __ SYS1.DUMP*.**                                      GENERIC NONE___ SYSPROG_ R_R _
 __ SYS1.*.**                                          GENERIC NONE___ SYSPROG_ U_R _
 ****************************** BOTTOM OF DATA ********************************
```

図 15. すべての一致の結果

- マスクおよびマッチング選択オプションの他に、別の選択基準も使用できます。これらの基準は、特定のタイプのデータ・セット・プロファイルを検索するときに役立ちます。例えば、次のようになります。

a. PF3 を押して、「data set Selection」パネルに戻ります。

b. 「**Additional selection criteria**」領域の「**プロファイル**」フィールドに / と入力します。このアクションによって別のパネルが開き、さらに選択基準を指定できます。

警告モードでのプロファイルのリスト表示

このタスクについて

警告モードでは、すべてのアクセス権限が許可されますが、アクセスによって通常は違反が生じる場合に警告メッセージが発行されます。警告モードは、プロファイルによってカバーされるデータ・セットに対する任意のアクションを許可するため、通常は一時的な手段です。警告モードのプロファイルをすべてリストするには、以下のステップを実行します。

手順

1. 「**Warning mode**」フィールドの横に / が存在することを確認し、「**No warning**」フィールドの横の選択 (/) を解除します。Enter を押します。

   警告モードのすべてのプロファイルがリスト表示されます。検索は、HLQ=PAYROLL と警告モードなどを使用して、さらに特定できます。

2. PF3 を押して「Data set Selection」パネルに戻ります。
3. 「**データ・セット・プロファイル**」フィールドに PROD.** またはご使用のインストール済み環境において意味のあるデータを入力し、「**UACC または ID(*)**」選択フィールドに = 3 (READ) を入力します。 このフィールドは、前に警告モードを選択したのと同じパネルにあります。
4. 基準組み込みセクションの「**No warning**」フィールドの横に / を再適用して、Enter を押します。

   このアクションでは、すべてのユーザーが読み取ることができる実動データ・セットのリストが生成されます。

5. PF11 を押します。

   このアクションでは、「**ERASE**」 (**E**) フィールドなどの追加のフィールドが表示されます。プロファイルに RACF の**「開始時に消去 (EOS)」**属性が設定されている場合、プロファイルによって保護されるすべてのデータ・セットは、削除されるときにデータの機密性を確保するために物理的に消去されます。

6. **S** 行コマンドを使用するか、表示されているデータ行の先頭にカーソルを移動して、その特定のプロファイルの詳細情報を取得します。

   注: 表示されている行の多くが展開可能です。行の最初のフィールドに **S** を入力するか、最初のフィールドにカーソルを置いて Enter を押します。

個別プロファイルの表示

手順

1. 「Data set Selection」パネルに戻ります。
2. 「**データ・セット・プロファイル**」フィールドを消去します。
3. 「**Additional selection criteria**」セクションの「**Profile fields**」の前に **/** と入力します。Enter を押します。
4. 「**UACC or ID(*)**」フィールドに何も指定されていないことを確認します。
5. 「Data set Selection」パネルの「**個別**」セクションに **/** が付いていることを確認します。
6. 「**Generic selection**」フィールドから **/** を削除します。その他の選択基準はすべてそのままにして、Enter を押します。

   このアクションでは、既存のすべての個別データ・セット・プロファイルのリストが生成されます。

   ヒント: zSecure Audit for RACF では複数プロパティーを選択するとき、**AND** 関数を使用することを思い出してください。

アクセス制御リスト (ACL) の表示

このタスクについて

次の手順では、データ・セット・プロファイルのリストを開きます。特定のプロファイルを選択して、アクセス制御リスト (ACL) や、ACL の各項目に関連した情報、その特性などの詳細情報を取得します。RACF データベース内で複数の複合的な使用許可を持つことが分かっているデータ・セット・プロファイルを選択します。ワイルドカード文字を使用して選択基準を指定できます。以下の例では、名前のパターンが SYS1.** と一致するデータ・セット・プロファイルを例として選択しますが、ご使用のインストール済み環境に応じた名前パターンを使用してください。「data set Selection」パネル内で、次の手順で行います。

手順

1. 「**データ・セット・プロファイル**」フィールドにプロファイル名を入力します。
2. 「**Output/run options**」セクションの「**Enable full ACL**」フィールドの横に **/** を入力します。
3. Enter を押して、一致するすべてのプロファイルのリストを開きます。
4. リストから最も複雑なデータ・セット・プロファイルを選択します。
5. その行に S 行コマンドを入力します。Enter を押します。

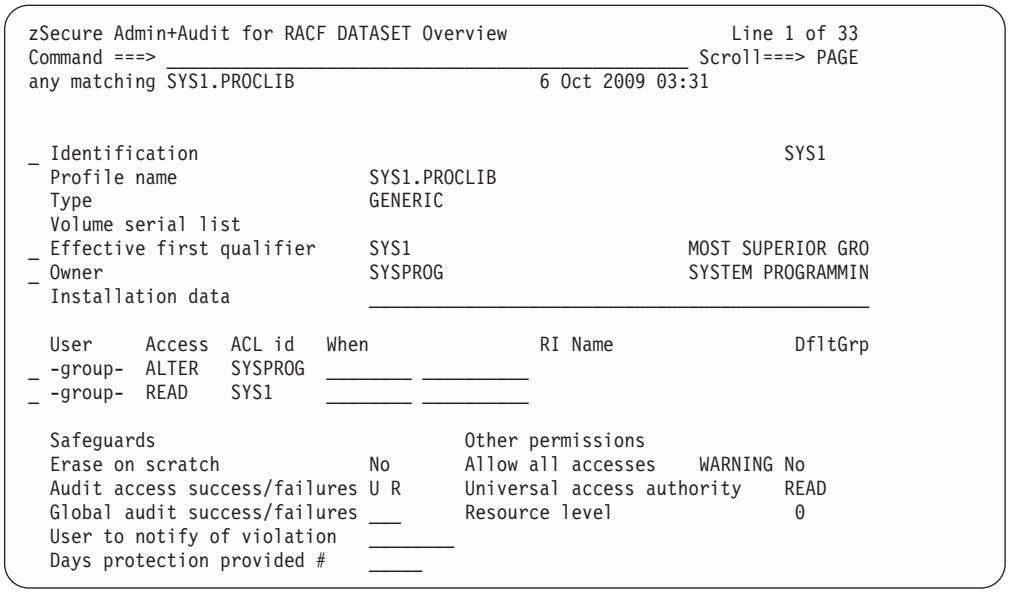


図 16. 通常の ACL

図 16 から、この例では ACL にグループ項目のみが含まれていることが確認できます。

アクセス制御リストのフォーマット

RACF では、リソースに対して整合性を持たない複数のアクセス権限を簡単に持つことができます。例えば、グループを介してデータ・セット XXX に対する読み取り権限を持つことができます。また、XXX に対する更新権限を持つ別のグループに属することもできます。RACF は、このような複数の権限の中で可能な最も高いアクセス・レベルをユーザーに付与します。上記の例では、ユーザーは更新権限を持つことになります。

また、特定のユーザー許可が優先されます。RACF では複数のアクセス権限を解決して効力のある権限を判別します。zSecure Admin and Audit では解決済みの権限を表示できますが、存在するすべての権限を表示する展開された権限も表示できます。解決済みの権限だけが、リソースへのアクセス権限を付与するために考慮されます。展開リストは、ユーザーがリソースに対する特定のレベルのアクセス権限を持つ理由を判別する上で不可欠です。デフォルトでは、zSecure Admin and Audit はアクセス制御リストを、RACF でアクセス制御リストを表示するように表示しますが、**グループ ID** または**ユーザー ID** によって順序付けし、**ユーザー ID**、プログラマー名、およびインストール・データを含めます。

これらの許可されたグループに接続されているすべてのユーザーと、他の理由で許可を持つ任意のユーザーのリストを表示するには、コマンド行に ACL EXPLODE または ACL X と入力します。このコマンドにより、このプロファイルへのアクセス権限を持つユーザーを示す展開されたリストが開きます (ユーザーあたり複数行になることもあります)。詳細表示では、ユーザーに提供するアクセス制御リスト項目ごとのアクセス・レベルを示します。

データ・セットへのアクセス権限を持つすべてのユーザーが、ユーザーの接続グループと共に表示されます。 26 ページの図 17 を参照してください。システム全体お

よびグループの **OPERATIONS** によるアクセス権限も示されます。

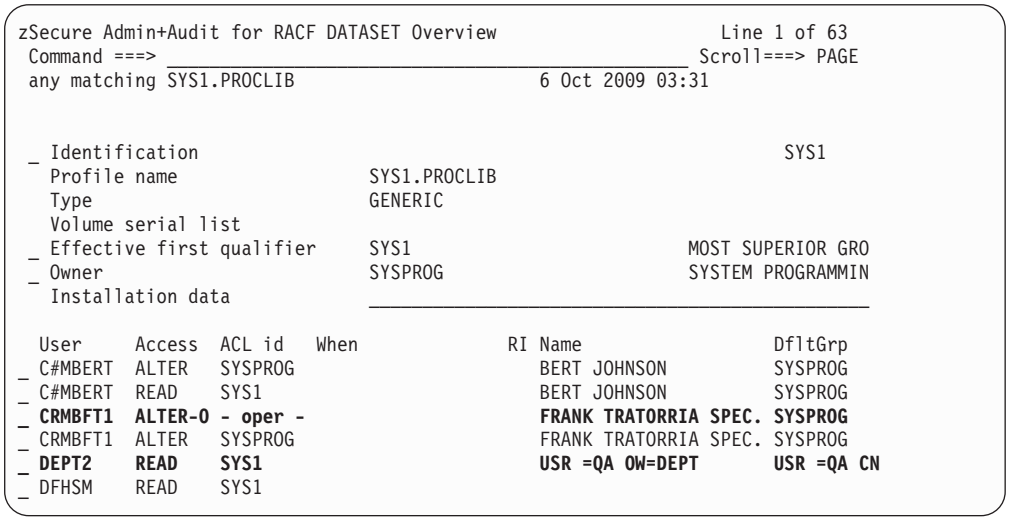


図 17. 展開された ACL

図 17 に、以下の行があります。

```
_ CRMBFT1  ALTER-O - oper -                    FRANK TRATORRIA SPEC. SYSPROG
```

上記の例は、ユーザーに**操作**権限があるため、アクセスが許可されていることを示しています。以下の行は、ユーザー DEPT2 がグループ SYS1 に接続され、データ・セット・プロファイルに対して READ アクセス権限を持っていることを示しています。

```
DEPT2    READ    SYS1                     USR =QA OW=DEPT      USR =QA CN
```

ユーザーは、同じデータ・セット・プロファイルに対して異なるパス経由で複数のアクセス権限を持つ可能性があります。1 つの行は、ユーザーのそれぞれのアクセス権限およびグループ接続を示しています。例えば、図 17 で示すように、ユーザー C#MBERT は 2 つの別の行に表示されていますが、これはこのユーザーがグループ SYS1 に接続されて READ アクセス権限を持つ上に、このユーザーがグループ **SYSPROG** にも接続されて **ALTER** アクセス権限を持つためです。

ヒント: EXPLODE オプションは使用しないでください。一般的な使用の場合は **SORT** オプションが最適です。

ユーザーが持つ最高レベルのみ表示するには、次の ACL コマンドを使用します。

- コマンド行に **ACL RESOLVE (R)** と入力します。

  各ユーザーが持つアクセス権限を正確に示す、1 ユーザーあたり 1 項目だけを記載するリストが表示されます。ただし、システム全体属性およびグループの OPERATIONS 属性を使用したアクセス権限は、解決済み概要の表示には含まれないことに注意してください。
- コマンド行に **ACL EFFECTIVE (F)** と入力します。

  各ユーザーが持つアクセス権限を正確に示す、1 ユーザーあたり 1 項目だけを記載するリストが表示されます。ただし、このリストには、OPERATIONS 属性を所有するという理由でアクセス権限を持つユーザーも含まれます。

- コマンド行に **ACL SORT ACCESS** と入力します。

  アクセス・レベルの降順で、ユーザー ID 別にアクセス・レベルごとのアクセス制御リストを示すリストが表示されます。図 18を参照してください。

```
zSecure Admin+Audit for RACF DATASET Overview                    Line 1 of 44
Command ===>  ____________________________________________________ Scroll===> CSR
like SYS1.                                  ** 8 Apr 2005 12:17
 Identification                                                    DEMO
 Profile name                 SYS1.PROCLIB
Type                         GENERIC
   Volume serial list
 _ Effective first qualifier    SYS1                          MOST SUPERIOR GRO
 _ Owner                        SYSPROG                       SYSTEM PROGRAMMIN
   Installation data            ____________________________________________
   User     Access  ACL id   When            RI  Name                 InstData
 _ C#MBERT  ALTER   SYSPROG                      BERT JOHNSON
 _ C#MBMR1  ALTER   SYSPROG                      M RONTEL             AAAAAAAAAA
 _ R##SLIN  ALTER   SYSPROG                      BERT JOHNSON SPEC.
 _ SYSPSTC  ALTER   SYSPROG                      STC USER SYSPROG
 _ CNRUNL   READ    SYS1                         JUST A USER TO BE US
 _ DEPT     READ    SYS1                         USR =QA OW=SYS1       USR =QA CN
 _ DEPT1    READ    SYS1                         USR =QA OW=DEPT       USR =QA CN
 _ DEPT2    READ    SYS1                         USR =QA OW=DEPT       USR =QA CN
 _ DFHSM    READ    SYS1
```

図 18. 有効な ACL

ACL EFFECTIVE コマンドは、システムおよびグループ操作を通じてのアクセスを含む個別ユーザーの持つ有効なアクセス権限を表示します。また、所有者、修飾子、またはグループ SPECIAL を使用して所有者権限も含める場合、**ACL SCOPE** および **ACL NOSCOPE** コマンドを使用してオン/オフを切り替えることができます。アクセス権限および所有権を別々に表示するが解決済み表示する場合、**ACL EFFECTIVE** の代わりに **ACL TRUST** を指定します。

ヒント: 表示を印刷するには、コマンド行に移動して、**PRT** と入力します。このコマンドは、現在の表示を印刷します。レポートの全体幅 (標準的なユーザーの画面よりも広い場合があります)、およびこのパネルに至るまでの上位レベルの情報が含まれます。印刷された出力は ISPF LIST データ・セットに配置されます。ISPF を終了するとき、このデータ・セットを忘れずに印刷してください。ISPF を終了せずに ISPF LIST データ・セットを印刷する場合は、コマンド行に **LIST** と入力し、表示されるパネル内で印刷オプションを選択します。

アクセス・リストの表示設定

解決と展開に関するこの短い説明は重要な特徴を示しているため、覚えておいてください。アクセス制御リストのレイアウトは、以下の方法で変更できます。

- 「セットアップ」パネルの**オプション 5** を使用して「Setup View」パネルにアクセスする。
- アクセス制御リスト表示のコマンド域で **SET** と入力する。
- アクセス制御リスト表示のコマンド域で **ACL RESOLVE**、**ACL EXPLODE**、または **ACL EFFECTIVE** コマンドを入力する。

最初の 2 つの方式は、将来使用するために新しいモードを記憶します。最後の方式は、現在の表示を変更するのみです。

アクセス・リスト表示設定の変更について詳しくは、以下を参照してください。

- 『セットアップ表示パネルでのアクセス・リスト表示設定の変更』
- 『セットアップ・パネルでのアクセス・リスト表示設定の変更』

セットアップ表示パネルでのアクセス・リスト表示設定の変更

手順

1. コマンド行で **SETUP VIEW** と入力して、図 19 に示す「Setup View」パネルを開きます。

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                      zSecure Suite - Setup - View
Command ===> ____________________________________________________________

 Access list format . . . . 2  1. No       3. Explode  5. Effective
                               2. Sort     4. Resolve

 ACL/Connect sort . . . . . 2  1. Id       2. User     3. Access
 Show OS specific options   /  z/OS        _  z/VM
 /  Add user/group info to view
     (Selecting this will use some additional storage - normally on )
 /  Add summary to RA displays for multiple complexes (normally on)
 _  Add connect date and owner to RA.U/G connects section
 _  Show complete subsystem class information for RA.S (reads entire CKFREEZE)

 Select view
 3  1. View only profiles you are allowed to change (administrator view)
    2. View all profiles you are allowed to change or list
    3. View all profiles (normal view)
```

図 19. 「Setup View」パネル

2. 「**Access list format**」フィールドで、オプション 5 を指定します。
3. PF3 を押して、新しい値を受け入れます。この値は、次回照会を実行するときに有効になります。これ以降、1 ユーザーあたり 1 行だけが表示されます。この行は各ユーザーの有効なアクセス・レベルを表します。

   設定した解決または展開の表示レベルは変更するまで有効です。「Setup View」パネルは「セットアップ」パネルの 1 つです。このパネルには、「セットアップ」メニューからもアクセスできます。

セットアップ・パネルでのアクセス・リスト表示設定の変更

手順

1. PF3 を使用してメインメニューに戻ります。
2. オプション「**SE**」(セットアップ) を選択します。
3. オプション「**5**」(表示) を選択します。

   ヒント: これらのコマンドを入力する代わりに、コマンド行に =SE.5 と入力すると、「Setup View」パネルにすぐに移動できます。
4. アクセス制御リストのフォーマットを「**ソート**」に戻すには、「**Access list format** 」フィールドに 2 を入力します。 「ソート」フォーマットは一般的な使用に最も適したフォーマットです。
5. PF3 を押して、パネルを終了します。

アクセス・コマンドを使用したリソースへのアクセスの検査

このタスクについて

注: このコマンドは zSecure Admin 製品にのみ該当します。

A アクセス機能 **RA.1** またはアクセス基本コマンドを使用して、特定のユーザーまた
A はグループがアクセスできるデータ・セットまたはリソース (および RACF プロフ
A ァイル) を表示できます。以下の情報が指定されると、アクセス機能は、リソース
A をカバーするプロファイル、および結果としてユーザーが得られるアクセス権限に
A 関する情報を提供します。

- ユーザーID
- リソース・クラス
- データ・セット名、リソース名、またはプロファイル名

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                 zSecure Admin - RACF - Access Check
Command ===> ____________________________________________________________

Id  . . . . . . . . IBMUSER_

Specify profile for Access Check
 Class  . . . . . . DATASET_  (DATASET or class)
 Profile  . . . . . SYS1.LOADLIB_____________________________ (EGN mask)
```

図 20. 「Access check entry」パネル

手順

1. 「**Id**」フィールドに、ユーザー ID またはグループ ID を入力します。
2. リソース・クラス (データ・セットまたは一般リソース・クラス名) を指定し、
R データ・セット名、リソース名、またはプロファイル名を「**プロファイル**」フィ
R ールドに指定します。Enter を押します。 「Access check detail」パネル (図 21)
R に、RACF がこの ID に付与したアクセス・レベルと、アクセス権限が決定され
R る根拠となったプロファイルが表示されます。
R

```
   Menu  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 BROWSE    IBMUSER.CKRACF1.SDEMO.CKXOUT               Line 00000000 Col 001 080
 Command ===> ____________________________________________ Scroll ===> CSR_
******************************** Top of Data ********************************
CKGRACF ACCESS IBMUSER DATASET SYS1.LOADLIB
CKG582I 00 IBMUSER has ALTER access to DATASET SYS1.LOADLIB
           profile DATASET SYS1.**
****************************** Bottom of Data ******************************
```

図 21. 「Access check detail」パネル

アクセス権の管理

データ・セット・プロファイルのアクセス制御リストを管理するには、以下に示すいくつかの方法があります。

- データ・セット・プロファイルの概要パネルで **PE** (許可) 行コマンドを発行する。
- データ・セット・プロファイルの詳細パネルで、**C** (コピー)、**D** (削除)、**I** (挿入)、**R** (繰り返し)、または **S** (変更) の行コマンドを使用する。
- 値を変更するには、アクセス制御リストの現行値を上書きします。

  値を変更すると、**許可**コマンドおよび**削除の許可**コマンドが生成されて、新しい値が追加され、上書きされた値が削除されます。

  削除の許可コマンドを実行しない場合は、コマンド確認パネルからそのコマンドを削除した後、Enter を押します。次のパネル (zSecure Admin - Confirm command) で Enter を再び押すと、**許可**コマンドが処理されます。この時点で RACF コマンドを実行しないでください。

デジタル証明書テンプレートの作成

以下のタスクを実行して、デジタル証明書テンプレートおよび新規証明書を作成したり、証明書を表示するための基準を指定したりします。

このタスクについて

メニュー・オプション **SE.9** を使用してデジタル証明書テンプレートを作成します。定義済みテンプレートを使用して新しい証明書を生成するか (オプション RA.5.2 および RA.5.3)、または証明書の表示の基準を選択します (オプション RA.5.1)。定義パネルで、**F** 選択フィールドを使用して、フィールドの値を修正します。値を修正した場合、証明書を生成するためにテンプレートを使用するときに、その値を変更することはできません。

手順

1. メインメニューの「オプション」行に SE (セットアップ) と入力し、**Enter** を押します。 「セットアップ」メニューが表示されます。

```
     Menu         Options       Info    Commands     Setup             Startpanel
--------------------------------------------------------------------------------
                          zSecure Suite - Setup
 Option ===> ____________________________________________________________________
                                                                        More:     +
 0    Run             Specify run options
 1    Input files     Select and maintain sets of input data sets
 2    New files       Allocate new data sets for UNLOAD and CKFREEZE
 3    Preamble        CARLa commands run before every query
 4    Confirm         Specify command generation options
 5    View            Specify view options
 6    Instdata        Customize installation data appearance
 7    Output          Specify output options
 8    Command files   Select and maintain command library
 9    Certificates    Specify templates for new digital certificates
 B    Collections     Select and maintain collections of input sets
 U    User defined    User defined input sources
 C    Change Track    Maintain Change Tracking parameters
 N    NLS             National language support
 T    Trace           Set trace flags and CARLa listing for diagnostic purposes
 D    Default         Set system defaults
 R    Reset           Reset to system defaults
 I    Installation    Specify installation defined names
```

図 22. 「セットアップ」メニュー

2. 「セットアップ」メニューの「オプション」行に 9 と入力し、**Enter** を押します。 このオプションの選択時にテンプレートを定義しなかった場合、「セットアップ」の証明書テンプレート定義パネルが表示されます。

```
  Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Setup - Certificates
Command ===> ___________________________________________________________________

   Name for template  . . . . ________
   Description  . . . . . . . ________________________________________________

F  Enter the following defaults for the new certificate:
_  Certificate label prefix   ________________________________
_  Certificate type . . . . . _  1. Site  2. Certauth  3. Personal  ________
_  Size of new private key     ____  (Default 1024 for RSA/DSA; 192 for ECC)
_  Start validity date  . . . __________  (yyyy-mm-dd, default is today)
_  Start validity time  . . . ________    (Default is 00:00:00)
_  End validity date  . . . . __________  (yyyy-mm-dd, nYEAR, default 1YEAR)
_  End validity time  . . . . ________    (Default is 23:59:59)

F  Enter the following defaults for the Signing Authority:
_  Digital certificate label  ________________________________
_  Signing certificate type   _  1. Site  2. Certauth  3. Personal  4. Self

Optional actions  . . . . . _  1. Connect to key ring
                               2. Export certificate
                               3. Generate certificate request


Press ENTER to continue or END to exit
```

図 23. 「セットアップ」の証明書テンプレート定義パネル

このパネルおよびすべての後続パネル上のフィールドの説明については、フィールド・ヘルプ機能 (PF1) を使用します。

3. **Enter** を押します。 次のパネルが表示されます。

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Certificates
Command ===> ____________________________________________________________

   Name for template  . . . . MQ
   Description  . . . . . . . MQ certificate template

F  Enter the following defaults for the new certificate:
_  Key usage  . . . . . . . . _  Handshake     _  Docsign       _  Keyagree
                              _  Data encrypt  _  Certsign
   Select the key type to be generated:
_  _  1. RSA(default)
      2. RSA Modulus-Exponent in PKDS
      3. DSA
      4. NIST ECC
      5. Brainpool ECC
_  _  1. Store in PKDS with an optional PKDS label or * (types 1,2,4, and 5)
      2. Store in TKDS using existing TKDS token (types 1,4, and 5):
_  ________________________________________________________________

Press ENTER to continue or END to return to previous panel
```

図 24. 「セットアップ」の証明書テンプレート定義パネル

4. **Enter** を押して、次のパネルを表示します。

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Certificates

Command ===> ____________________________________________________________

   Name for template  . . . . MQ
   Description  . . . . . . . MQ certificate template

F  Enter the Subject's X.509 Distinguished Name:
   Common Name: (ex: 'John Q. Public' )
   ____________________________________________________________
   Title: (ex: 'Systems Programmer' )
_  ____________________________________________________________
   Organizational Unit: (ex: 'S390','MVS' )
_  ____________________________________________________________
_  ____________________________________________________________
_  ____________________________________________________________
   Organization: (ex: 'IBM' )
_  ____________________________________________________________
   Locality: (ex: 'Poughkeepsie' )
_  ____________________________________________________________
   State/Province: (ex: 'New York'  )
_  ____________________________________________________________
   Country: (ex: 'US'  )
_  ____________________________________________________________

Press ENTER to continue or END to return to previous panel
```

図 25. 「セットアップ」の証明書テンプレート定義パネル

5. **Enter** を押します。 次のパネルが表示されます。

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Certificates

Command ===> ____________________________________________________________

   Name for template  . . . . MQ
   Description  . . . . . . . MQ certificate template

F  Enter the subjectAltName extension:
   Enter the IPv4 or IPv6 address
_  ____________________________________________________________________
   Enter the internet domain name
_  ____________________________________________________________________
   Enter the fully qualified email address
_  ____________________________________________________________________
   Enter the universal resource identifier
_  ____________________________________________________________________

Press ENTER to continue or END to return to previous panel
```

図 26. 「セットアップ」の証明書テンプレート定義パネル

6. 31 ページの図 23 のオプション「**Connect to key ring**」を選択すると、以下のパネルが表示されます。

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Certificates

Command ===> ____________________________________________________________

   Name for template  . . . . MQ
   Description  . . . . . . . MQ certificate template

F  F  Enter key ring data
_  _  Connect to key ring
   _  Key ring name  . . . . . . ____________________________________
      ____________________________________________________________________
      ____________________________________________________________________
      ____________________________________
   _  Key ring owner . . . . . . ________
   _  Use as default certificate _  (Y/N)
   _  Certificate usage  . . . . _  1. Installed usage (default)
                                    2. Use as a PERSONAL certificate
                                    3. Use as a CERTAUTH certificate
                                    4. Use as a SITE certificate
```

図 27. 「セットアップ」の証明書テンプレート定義パネル

7. テンプレートが定義されると、以下のパネルが表示されます。

```
  Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Certificates  Row 1 to 1 of 1

Command ===> ____________________________________________________________________
 Select certificate template (E (edit), B (browse), I (insert),  C (copy),
 D (delete))


     Name      Description                                                Type
_    MQ        MQ certificate template                                    User
 ------------------------------------------------------------------------------
 ****************************** Bottom of data ********************************
```

図 28. 「セットアップ」の証明書テンプレート定義パネル

以下のアクション・コマンドが使用できます。

B
既存の定義間をブラウズできます。

C
既存のテンプレートに基づいて新規テンプレートを作成します。

D
テンプレートを削除する前に、確認パネルを表示します。

E および I
証明書定義パネルを表示します。

証明書、鍵リング、フィルター、およびトークンの処理

証明書、鍵リング、フィルター、およびトークンを管理するには、以下のガイドラインおよびタスクの手順に従ってください。

このタスクについて

デジタル証明書は、認証、検査、暗号化などに使用されます。通常、証明書には、サブジェクトの説明、公開/秘密鍵、および「信頼できる関係者」の署名が含まれます。

RACDCERT コマンドは複雑です。例えば、25 個の 1 次オプションがあり、また一部の機能では複数のコマンドが必要です。zSecure では、標準の zSecure インターフェース (選択-表示-アクション、および行コマンドと上書きを使用したアクション) を使用します。新しいオブジェクトを直接作成するオプションも提供しています。

RACDCERT の実行前にほとんどのパラメーターが検査され、最後に指定されたパラメーターが、簡単に修正できるように保持されます。テンプレートを使用してデフォルト値を指定することができます。また、zSecure には、以下の 2 つのデフォルトのテンプレートが含まれています。

None
空のフィールドを使用します。

Previous
前回のオプションを使用します。

RA.5 (RACDCERT) メニューを使用して、デジタル証明書、鍵リング、フィルター、およびトークンを処理します。

手順

メインメニューに移動するまで PF3 を押します。RA.5 を選択して、RACDCERT メニューを表示します。

```
     Menu         Options       Info    Commands     Setup             Startpanel
-------------------------------------------------------------------------------
                          zSecure Suite - RACF - RACDCERT
Option ===> ____________________________________________________________________

1    Certificates    Work with digital certificates
2    Generate        Generate new certificate and a public/private key pair
3    Sign            Generate new certificate using an existing public key
4    Add             Add or update existing digital certificate
5    Check           Check whether digital certificate has been added to RACF
6    Key rings       Work with key rings
7    Name filtering  Work with certificate name filters
8    Tokens          Work with tokens
9    Criteria        Work with certificate mapping criteria
```

図 29. RACDCERT メニュー

このパネルのオプションについて、以下で簡潔に説明します。RACDCERT 機能について詳しくは、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」の RA.5 に関するセクションを参照してください。オプションを選択すると、後続のパネルが表示されます。これらのパネル上のフィールドの説明については、フィールド・ヘルプ機能を使用します。
後続の詳細表示で、任意の行を選択して、完全な詳細ビューを表示することができます。詳細を選択するには、カーソルを行選択フィールドの先頭文字に置いて Enter キーを押すか、そこに明示的に S と入力して Enter キーを押します。

RA.5.1 Certificates - Work with digital certificates

デジタル証明書に対するアクションを選択して実行するには、オプション **RA.5.1** を使用します。次のパネルが表示されます。

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                          zSecure Suite - RACDCERT - Certificates
Command ===> ___________________________________________________________________

Show certificates that fit all of the following criteria:
Certificate label  . . . _____________________________________  (label or filter)
Certificate type/owner   _  Site       _  Certauth   _  Personal  ________
Trust  . . . . . . . . . _  1. TRUST  2. NOTRUST   3. HIGHTRUST
Start validity . . . . . __  ___________  (operator: > >= < <= = <> ^= )
End validity . . . . . . __  ___________  (date: yyyy-mm-dd/ddMMMyyyy/
Creation date  . . . . . __  ___________         TODAY/TODAY-nn/NEVER)
Complex  . . . . . . . . ________  (complex or filter)
_  Match on template

Additional selection criteria
_  Other fields       _  SubjectsDN       _  IssuersDN

Output/run options
_  0. No summary      1. Summary by owner
_  Show differences
   Print format       _  Customize title  _  Send as e-mail
   _  Background run  _  Full page form   _  Sort differently  _  Narrow print
```

図 30. デジタル証明書の選択パネル

「Match on template」オプションは、「セットアップ」(デフォルト) の証明書で定義されたテンプレートに証明書を一致させる場合に使用します。パネルが表示され、そこでテンプレートを選択します。証明書パネルの選択フィールドには、選択したテンプレートの値が事前に入力されています。図 31 に、デジタル証明書表示のサンプルを示します。

```
zSecure Suite DIGTCERT CERTDATA segments
 Command ===>                                                Scroll===> CSR
 All certificates                              27 Mar 2013 09:14
    User     Digital certificate labels       Tru Cert. sta Cert. end Complex
 __ irrcerta Entrust Secure Server Root CA    No  25May1999 25May2019 PROD
 __ irrcerta Entrust.net Secure Server CA     No  21Aug2001  1Jan2006 PROD
 __ irrcerta Equifax Secure CA                No  22Aug1998 22Aug2018 PROD
 __ irrcerta GTE CyberTrust Root CA           No  23Feb1996 23Feb2006 PROD
 __ irrcerta Identrus Interoperability CA     No   8Feb2000  5Feb2010 PROD
 __ irrcerta Integrion CA                     No  20May1997 20May2017 PROD
```

図 31. デジタル証明書のテーブル表示のパネル

以下のいくつかの行コマンドを使用できます。

BI - トークンへの証明書のバインド
RACF 証明書を既存のトークンにバインドします。

CO - 鍵リングへの証明書の接続
証明書を鍵リングに接続します。

EX - 証明書のエクスポート
デジタル証明書をデータ・セットに書き込みます。

GR - 認証要求の生成
指定された証明書に基づいた PKCS #10 Base64 エンコードの認証要求を作成するか、要求をデータ・セットに書き込みます。

LC - 証明書の RACDCERT LISTCHAIN
RACDCERT LISTCHAIN コマンドを発行します。このコマンドにより、証明書チェーン内のユーザー ID、SITE、または CERTAUTH が所有する証明書に関する証明書情報、および CERTAUTH が所有する、その発行者の証明書に関する証明書情報がリストされます。

RK – 証明書の鍵再設定
新しい公開鍵/秘密鍵ペアを使用してデジタル証明書を複製 (鍵再設定) します。一般的に、証明書の鍵再設定後には、RO アクション・コマンドを発行して、古い証明書を鍵再設定済みの新しい証明書で置き換え、古い秘密鍵を失効させます。

RO – 証明書のロールオーバー
ある証明書 (ソース証明書) を別の証明書 (ターゲット証明書) で置き換えます。一般的に、RK アクション・コマンドを発行した後に RO アクション・コマンドを発行して、有効期限が切れる古い証明書を鍵再設定済みの新しい証明書で置き換え、有効期限が切れる証明書の秘密鍵を失効させます。

UB - トークンからの証明書のアンバインド
既存のトークンから RACF 証明書をアンバインドします。

RA.5.2 Generate - Generate new certificate and a public/private key pair
新規証明書および公開鍵/秘密鍵ペアを生成するには、このメニュー・オプションを使用します。まず、テンプレート選択パネルが表示されます。このパネルには、「セットアップ」の証明書で定義されたテンプレートが表示され、デフォルトでは以下のようになっています。

None
GENCERT パネル上のすべてのフィールドをクリアします。

Previous
前回入力された値を使用します。

RA.5.3 Sign - Generate new certificate using an existing public key
既存の公開鍵を使用する新しい証明書を生成するには、このメニュー・オプションを使用します。

RA.5.4 Add - Add or update existing digital certificate
指定したデータ・セットに含まれている証明書または証明書パッケージを使用してデジタル証明書を定義するには、このメニュー・オプションを使用します。

RA.5.5 Check - Check whether digital certificate has been added to RACF
指定されたデータ・セット内のデジタル証明書が RACF データベースに追加されていて、ユーザー ID に関連付けられているかどうかを評価するには、このオプションを使用します。引用符で囲んだデータ・セット名を入力する必要があります。該当する証明書が PKCS12 フォーマットである場合は、パスワードも必要になります。

RA.5.6 Key rings - Work with key rings
鍵リングを処理するには、このメニュー・オプションを使用します。このパネルを空のままにして **Enter** を押した場合、すべての鍵リング・レコードが表示されます。

```
                zSecure Suite Key rings display                 Line 1 of 10
Command ===> ____________________________________________________ Scroll===> CSR
All key rings                                  12 Mar 2013 06:00
   Owner    Key ring name                                      #Cert CreateDat
__ CRMQA401 ER80810                                               0 06Jul2001
__ CRMQA402 ER80810                                               1 06Jul2001
__ TCPSRV   telnetSSL                                             2 28Nov2007
****************************** Bottom of Data ********************************
```

図 32. 鍵リングの概要

RA.5.7 Tokens - Work with tokens
このメニュー・オプションを使用してトークンを処理します。このパネルを空のままにして Enter キーを押すと、すべてのトークン・レコードが表示されます。 38 ページの図 33 に、トークンのテーブル表示のサンプルを示します。

```
                zSecure Suite Tokens display                    Line 1 of 1
Command ===> ____________________________________________ Scroll===> CSR
All tokens                                    15 Mar 2013 03:12
   Token                          Sequence Complex  Manufacturer
__ FIRSTTESTTOKEN                 00000001 ADCDPL   ICSF PKCS11 token browser
****************************** Bottom of Data ********************************
```

図 33. トークンの概要

次の行コマンドを使用できます。

BI - トークンへの証明書のバインド
RACF 証明書を既存のトークンにバインドします。

D – トークンの削除
RACDCERT DELTOKEN コマンドを生成します。

L - トークンのリスト表示
RACDCERT LISTTOKEN コマンドを生成します。

UB - トークンからの証明書のアンバインド
既存のトークンから RACF 証明書をアンバインドします。

RA.5.8 Name filtering - Work with certificate name filters
証明書名フィルター・リングを処理するには、このメニュー・オプションを使用します。図 34 に、名前フィルター表示のサンプルを示します。

```
             zSecure Suite Certificate name filters
Command ===> ____________________________________________________ Scroll===> CSR
All name mappings                             12 Mar 2013 06:00
   Certificate filter name (issuer and subject name separated by ¢)
__ ¢OU=CRM.O=Consul Risk Management
__ ¢OU=Sysprog.OU=CRM.O=Consul Risk Management
__ OU=CICS Individual Subscribers.O=Verisign,Inc.L=Internet¢
__ OU=VeriSign Class 1 Individual Subscribers.O=Verisign,Inc.L=Internet¢OU=Sysp
****************************** Bottom of Data ********************************
```

図 34. 名前フィルターの概要

RA.5.9 Criteria - Work with certificate mapping criteria
証明書マッピング基準を処理するには、このメニュー・オプションを使用します。図 35 に、基準表示のサンプルを示します。

```
                                                      1 s elapsed, 0.2 s CPU
zSecure Suite Certificate mapping criteria
Command ===> ____________________________________________________ Scroll===> CSR
All criteria                                   12 Mar 2013 06:00
   Criteria                                 MapToID  Owner    CreateDat Lv Cl
__ APPLID=CICSA                             CRMQA205 CRMBMR1  14Apr2000  0 DI
__ APPLID=CICSB                             CRMQA206 CRMBMR1  14Apr2000  0 DI
****************************** Bottom of Data ********************************
```

図 35. 基準の概要

ユーザーの比較

このタスクについて

ユーザーからのよくある質問に、「周囲のユーザーはこの機能を使用できるのに、どうして私は使用できないのですか。私たちはこの製品に対して同じアクセス権限

を持っているはずです」といったものがあります。zSecure Admin および zSecure Audit for RACF を使用すると、4 人までのユーザーを対象に、アクセス権限および接続状況を素早く比較できます。

ユーザーのアクセス権限および接続状況を比較するには、以下のステップを実行します。

手順

1. メインメニューに移動するまで PF3 を押します。
2. メインメニューで、「RA」パネルからオプション「**REPORTS (RA.3)**」を選択します。結果のパネルからオプション「**G ユーザーの比較**」を選択して、図 36 に示す「ユーザーの比較」パネルを開きます。

```
 Menu  Options  Info  Commands     Setup
 ------------------------------------------------------------------------------
          zSecure Admin+Audit for RACF - Reports - Compare users
 Command ===>

Enter up to 4 userids to compare access and/or connects
 Userid  . . . . ________    ________    ________    ________

Select report(s)
/  Compare access through user-specific permits
   _  Include group permits
/  Compare connects

_  Output in print format
```

図 36. 「ユーザーの比較」パネル

このパネルでは、最大 4 ユーザーを指定し、実行する比較を正確に指定できます。許可について 1 つ、グループ接続について 1 つの最大 2 つのレポートが生成されます。

例

許可レポートは以下の 3 つの層で提供されます。

- クラス内の任意のプロファイルに対して各ユーザーの最高のアクセス権限を持った許可が提供されるクラス。
- 最高のアクセス権限を持つ選択されたクラス内のプロファイル。
- 特定のプロファイルについての選択されたユーザーのすべての許可を含むリスト。

この詳細レポートには、 40 ページの図 37 で示すように、この 1 つの特定項目についての上位の層からの情報も表示されます。

```
Compare PERMITs for users                                        Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR
                                          10 Oct 2006 00:07
   Class    Profiles C#MBDV1 C#MBDV2
   DATASET        32 ALTER   ALTER
   Profile key                            C#MBDV1 C#MBDV2
   C#MA.D.HLLDV1.PADS.**                  READ    ALTER
   Scope of Access  Via      When
__ C#MBDV1  READ    CR#BDV1  PROGRAM  CKRCARLA
__ C#MBDV2  ALTER   CR#BDV2
****************************** Bottom of Data ********************************
```

図 37. 許可の比較の詳細パネル

接続レポートには、図 38 に示すように、少なくともいずれかのユーザーが接続されているすべてのグループのマトリックスが表示されます。

```
Compare CONNECTs for users                                       Line 1 of 6
Command ===> _____________________________________________ Scroll===> CSR
                                          10 Oct 2006 00:07
   Group    C#MBDV1  C#MBDV2
__ C#MARACF No       Yes
__ C#MB     Yes      Yes
__ C#MBREAD Yes      Yes
__ C#MBZDEV Yes      Yes
__ C#MCKG   No       Yes
__ C#MGRACF Yes      Yes
****************************** Bottom of Data ********************************
```

図 38. 接続の比較マトリックス

第 3 章 ユーザーおよびプロファイルの管理

注: このセクションの内容は、zSecure Admin 製品にのみ適用されます。

zSecure Admin では、RACF データを次の方法で変更できます。

- プロファイル表示のフィールドの既存の値を上書きして、値を変更することができます。
- プロファイル表示で行コマンド (**C** (コピー)、**D** (削除)、**R** (再作成)、**L** (リスト)、および **SE** (セグメント) など) を使用できます。
- 「大量更新」パネルを使用できます。
- さまざまな**レポート**機能や検査機能によって自動的に生成されたフォアグラウンドまたはバックグラウンド RACF コマンドを実行依頼できます。
- 分散機能を使用できます。分散機能については 53 ページの『第 4 章 分散管理機能および範囲付き管理機能』で説明します。

値の上書き、行コマンド、および大量更新は、「セットアップ - 確認」パネルの「**Confirmation**」設定によって制御されます。『RACF コマンドの生成と確認』を参照してください。「確認」パネルでは、**Overtype** 機能を有効または無効にし、データベースを変更する RACF コマンドの実行前に必要な検証を判別します。**確認**制御は、任意に設定できます。ただし、ルーチン製品の使用方法を十分理解するまでは、設定 **ALL** または設定 **PASSWORDS** を使用してください。

RACF コマンドの生成と確認

手順

1. オプション「**SE**」(セットアップ) を選択します。
2. **オプション 4** (確認) を選択します。 42 ページの図 39 に示すように「確認」パネルが開き、現在の設定が表示されます。

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
             zSecure Admin+Audit for RACF - Setup - Confirm
Command ===> ____________________________________________________________

Action on command . . 2  1. Queue    2. Execute  3. Not allowed
                      _ Execute display commands (for option 1 only)
Confirmation  . . . . 4  1. None     2. Deletes  3. Passwords      4. All
Command Routing . . . 3  1. Ask      2. Normal   3. Local only

Command generation
Enter "/" to select option(s)
/  Overtype fields in panels
/  Change generated commands
/  Specify start/end date
/  Generate SETROPTS REFRESH commands
   /  Issue prompt before generating SETROPTS REFRESH commands

Commands to generate
/  RACF commands
/  CKGRACF commands
/  CKGRACF ASK for later execution
/  CKGRACF REQUEST for later execution
_  CKGRACF WITHDRAW queued commands
_  CKGRACF RDELETE queued commands
```

図 39. 「確認」パネル

3. 「**Action on command**」フィールドに **2** (Execute) を設定します。
4. 「**Confirmation**」フィールドに **4** (All) を設定します。
5. 「**Command Routing**」フィールドに **3** (Local only) を設定します。
6. 「**Overtype fields in panels**」に **/** を設定します。 このオプションは、以降の例で使用されます。その他の設定 (特に「**Commands to generate**」セクション) は変更しないでおきます。

   ヒント: 変更可能フィールドのオン/オフを切り換えることもできます。切り替えるには、プロファイル表示のコマンド行に **MODIFY** コマンド (または **M**) を入力します。
7. PF3 を押して、パラメーターの変更内容を受け入れます。
8. PF3 を再度押して、メインメニューに戻ります。

   ヒント: いずれかのパネルでコマンド行に SETUP CONFIRM または =SE.4 と入力すると、いつでも「確認」パネルを表示できます。

次のタスク

ユーザー ID を使用して zSecure Admin から RACF データベースを管理するには、RACF データベースに対する正しい権限が付与されている必要があります。試行する変更を選択して行う場合、通常必要な権限は RACF SPECIAL ですが、グループ SPECIAL を使用できることがあります。あるいは、SPECIAL 権限の代わりに、独自のセキュリティー機構を備えた **CKGRACF** プログラムを使用することもできます。55 ページの『CKGRACF を使用したグループ管理』を参照してください。

大量更新の実行

手順

1. オプション **RA** (RACF 管理) を選択します。

2. **オプション 4** (大量更新) を選択します。図 40 に示す「大量更新」パネルが開きます。

次のタスク

「大量更新」パネルのオプション **0** から **5** を使用して、エンティティー・レベル (ユーザーやグループなど) でプロファイルを管理できます。例えば、ユーザーを削除する場合、ユーザー・プロファイルだけでなく、元のユーザー ID に関連するすべてのプロファイルが削除されます。また、PERMITS、CONNECTS、およびマスター・カタログ内の ALIAS が削除されます。すべての情報は一括に管理されます。なお、ALIAS を削除するには、CKFREEZE が存在している必要があります(45 ページの『ユーザーとすべての参照の削除』を参照)。

```
   Menu   Options   Info   Commands   Setup    StartPanel
------------------------------------------------------------------------------
           zSecure Admin+Audit for RACF - RACF - Mass update
Option  ===> ____________________________________________________________

0    Copy user       Copy existing user(s) to new user(s)
1    Copy group      Copy existing group(s) to new group(s)
2    Copy dataset    Copy dataset profile(s) to another high level qualifier
3    Copy resource   Copy general resource profile(s) to another class
4    Delete user     Delete user(s)
5    Delete group    Delete group(s)
6    Recreate user   Recreate user(s)
7    Recreate grp    Recreate group(s)
8    Recreate ds     Recreate data set profile(s)
9    Recreate res    Recreate general resource profile(s)
C    Copy CICS       Copy CICS prefixed profile(s) or member(s)
```

図 40. 大量更新

「大量更新」のパネルには、標準の RACF コマンドでは実行することが難しいさまざまな機能があります。その中でも特に重要な機能については、強調表示されています。

ユーザーのコピー

このタスクについて

「**ユーザーのコピー**」オプション (オプション 0) を使用して既存のユーザーを複製できます。このコマンドでは、ユーザー・プロファイルに加えて、モデル・ユーザーの許可と接続もコピーされます。zSecure Admin には、マスター・カタログにユーザー ALIAS を作成するオプションがあります。

手順

ユーザーをコピーするには、以下のステップを実行します。

1. 「大量更新」パネルからオプション **0** (ユーザーのコピー) を選択します。44 ページの図 41 に示す「User Multiple copy」パネルが開きます。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
        zSecure Admin+Audit for RACF - RACF - User Multiple copy
Command ===> ____________________________________________________________

Create new user(s) like existing user(s):

_ Specify password phrases

Model
User     New user Password Name                 Owner    Dfltgrp  Data
IBMUSER_ NEWUSER1 PSWD1___ PERSON_1____________ C#MB____ ________ ____________
=_______ NEWUSER2 PSWD2___ PERSON_2____________ =_______ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________


Enter = to copy value from preceding line, leave blank to copy from model.
Press ENTER to specify optional parameters.
```

図 41. 「User multiple copy」パネル

一度に最大 10 ユーザーまで複製できますが、評価のため、最初の行のみを入力してください。

2. パスフレーズを指定するには、「**パスフレーズの指定**」選択フィールドに **/** を入力してください。

   Enter を押すと、ユーザー ID のパスフレーズを入力できるパネルが続いて表示されます。パスフレーズを指定する場合は、保護オプションは使用できません。

3. モデル・ユーザーを指定します。ユーザー ID、新規ユーザー ID、名前、およびパスワードを入力します。Enter を押します。

   ヒント: パスワード列では、新規ユーザーを保護するために * を使用できます。

4. 次のパネルで Enter を押します。

   このパネルには、新規ユーザーに対して次の機能を実行するためのオプションが表示されます。

   - さらなるグループ接続を省略または追加する。
   - ユーザー・データをコピーする。
   - 新規ユーザーを取り消す。
   - 1 つ以上のカタログ別名を作成する。
   - 1 つ以上のデータ・セットおよび一般リソース・プロファイルをコピーする。
   - 新規ユーザーの RACF 変数 (*RACFVARS*) の 1 人以上のメンバーをコピーする。

   モデル・プロファイルからユーザーを作成するために必要なすべてのコマンドが生成されます。しばらくしてから「SPF edit」パネルが開きます。このパネルには、すべての RACF コマンドが表示されます。必要に応じて PF8 と PF7 を使用してスクロールして前方または後方に移動し、変更を行います。

5. PF3 を押して、エディターを終了します。
6. PF3 を押して、「結果」パネルをスキップします。

   「結果」パネルについては、 77 ページの『第 6 章 レポートの作成および表示』で説明します。
7. 「大量更新」パネルに戻るまで PF3 を押します。

タスクの結果

コマンドが実行された場合、新規ユーザーはモデル・ユーザーとして正確に定義されています。生成されたコマンドを後から実行できるように、これらのコマンドをデータ・セットに保存しておくこともできます。

ユーザーとすべての参照の削除

ユーザー ID を完全に削除するには、以下のガイドラインに従ってください。

オプション **RA.4.4** (ユーザーの削除) を使用してユーザーを完全に削除することができます。標準の RACF コマンドを使用する場合、ユーザーを完全に削除する操作は冗長で単調な操作です。ユーザーを完全に削除すると、プロファイルが削除されるほかに、すべてのアクセス制御リスト、所有者フィールド、および通知フィールドからユーザー ID が削除されます。 CKFREEZE ファイルを割り振っている場合、必須選択のオプションを選択すると、この操作によりユーザーのカタログ別名と既存のデータ・セットも削除されます。 64 ページの図 56を参照してください。

プロファイルの再作成

アンロードされた RACF データ・セットまたは RACF データベース自体のバックアップ・コピーに基づいて、オプション **RA.4.6** から **RA.4.9** を使用してプロファイルを再作成できます。エラーにより破損したプロファイルまたは誤って削除したプロファイルを修復するときに、このアクションを使用できます。

プロファイルのマージおよび比較

そのほかにも、さまざまな RACF データベース・マージ機能および RACF データベースの比較機能があります。マージでは、1 つの RACF データベースのアンロード・コピーを作成し、このコピーを使用して別の RACF データベースのプロファイルを変更および追加します。確認または編集のため、RACF プロファイルのマージに使用されるすべての RACF コマンドがリストされます。このコマンド・リストは、RACF とアンロード・データ・セットの関連プロファイルの比較です。完全なマージ操作は、ここで説明されているよりも複雑です。これについて詳しくは「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」で説明しています。

冗長プロファイル管理

ご使用の RACF データベースで定義されているデータ・セット・プロファイルを定期的に調べることをお勧めします。どのデータ・セット・プロファイルが廃止されているか、または廃止の可能性があるかを判別するには、**RA.3.3** 機能を使用できます。この機能を使用すると、図 42 に示されている「Reports - REDUNDANT」パネルが開きます。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
          zSecure Admin+Audit for RACF - RACF - Reports REDUNDANT
Command ===> ____________________________________________________________

Show profiles that fit all of the following criteria:
Profile pattern . . _____________________________________________ (EGN mask)
High level qual . . SYSA____     (qualifier or EGN mask; reduces time)
Complex . . . . . . ________     (complex name or filter)

Enter "/" to select option(s)
_  Show data sets covered by each profile
   _  Including data sets on scratch tapes

_  Output in print format
   _  Start each user or group on a new page

_  Remove redundant profiles
```

図 42. 「Reports - REDUNDANT」パネル

図 42 に示すパネルでは、どのデータ・セット・プロファイルまたは高位修飾子 (HLQ) をレポートに組み込むかを指定できます。これらのフィールドをブランクのままにすると、すべてのデータ・セット・プロファイルが自動的に処理されます。また、データ・セット・プロファイルによりカバーされるすべてのデータ・セットの名前をレポートに組み込むかどうかも指定できます。

「Report Redundant」機能では、データ・セット・プロファイル・セキュリティー定義 (UACC、アクセス制御リスト、監査設定、「開始時に消去」設定など) を、次に固有性の低い総称データ・セット・プロファイルのセキュリティー定義と比較します。

セキュリティー設定が異ならない場合、プロファイルが `-redundant-` として報告されます。この値が示されている場合、この固有性の高いデータ・セット・プロファイルが削除されると、対応するデータ・セットのセキュリティー定義を変更せずに、データ・セットの保護が (`-candidate-` として示された) より一般的な総称データ・セット・プロファイルに自動的に引き継がれます。

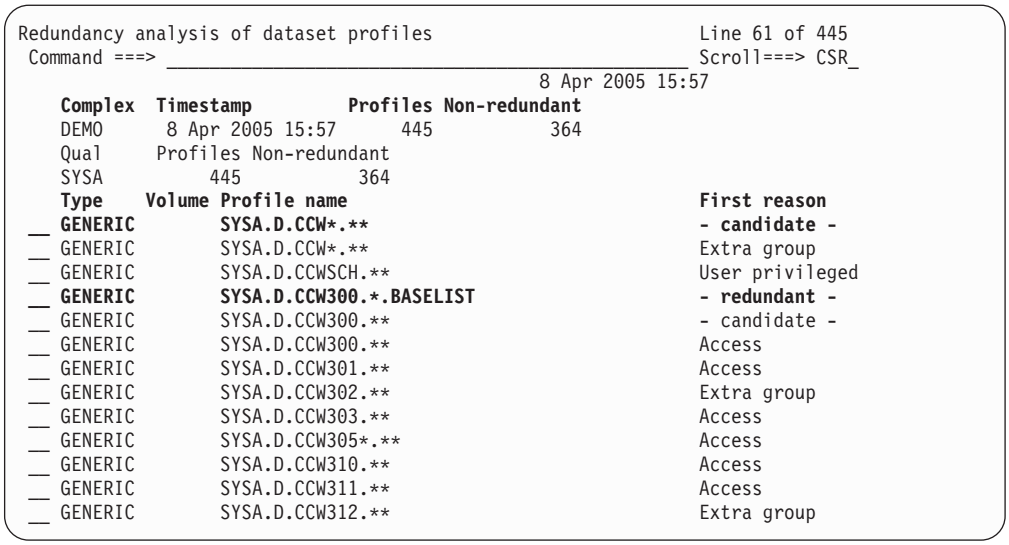


図 43. 「Report redundant details」パネル

図 43 では、以下の行は、-redundant- としてマークされているプロファイルが削除されるときに、データ・セットの保護を引き継ぐプロファイルの例を示します。

```
__ GENERIC        SYSA.D.CCW*.**                          - candidate -
```

以下の行は、セキュリティー設定が、自動的に保護を引き継ぐ候補プロファイルのセキュリティー設定に類似しているために、削除可能なプロファイルの例を示します。

```
__ GENERIC        SYSA.D.CCW300.*.BASELIST                - redundant -
```

冗長性に関するレポートの出力は、すべてのデータ・セット・プロファイルの概要であり、「**First reason**」というヘッダーが付いた列に標識が示されます。「First reason」列には、次のいずれかの値が含まれます。

-redundant-
: 現行のセキュリティー定義では、このプロファイルは必要ではないため削除できます。冗長プロファイルの対象であるデータ・セットの保護は、より固有性の低いデータ・セット・プロファイル (-candidate- のマークが付いたプロファイル) に自動的に引き継がれます。このプロファイルは、同じレポートで、-redundant- プロファイルとして報告されるプロファイルよりも前の位置に表示されます。

- candidate -
: このプロファイルは、より固有な総称データ・セット・プロファイルが削除される場合に、現在この総称データ・セット・プロファイルによって保護されているデータ・セットの保護を引き継ぎます。

reason
: このフィールドには、このプロファイルが、より一般的な総称データ・セット・プロファイルと大幅に異なり、冗長として見なされない理由を示すテキスト記述が表示されます。理由値の例としては、Extra group、User privileged、および Access などがあります。複数の差異が存在する場合は、最初の理由のみが報告されます。

冗長性に関するレポートから、現在の RACF データベース内にある古くなったデータ・セット・プロファイルを判別できます。

オプションで、-redundant- として報告されたプロファイルを削除する RACF コマンドを生成できます。ただし、-redundant- としてマークされたすべてのプロファイルを削除しないことがある点に注意してください。このデータ・セット・プロファイルの定義時に何らかの誤りが生じた可能性があります。つまり、ユーザーまたは別の RACF 管理者が「開始時に消去」をアクティブにすることを忘れたり、監査設定を意図したとおりに変更しなかったりした場合などです。

ヒント: 冗長性分析は、データ・セット・プロファイルを定義する際の誤りを特定する場合に役立つことがあります。

データ構造の表示

このタスクについて

RACF データベースを管理する際に役立つもう 1 つのレポートは、グループ・ツリー・レポートです。ネイティブ RACF で RACF データベース構造を表示する唯一の方法は、**DSMON** ユーティリティーを使用してグループ・ツリー・レポートを処理する方法です。このレポートには、要求されたグループごとに、すべてのサブグループ、サブグループのすべてのサブグループなどがリストされます。さらに、レポートにリストされている各グループの所有者が上位グループではない場合には、この所有者もリストされます。**DSMON** ユーティリティーを使用できるのは、**AUDITOR** 属性が設定されているユーザーのみです。ただし、グループ・ツリー・レポートを処理する場合は **AUDITOR** 属性は必要ありません。

zSecure Admin には、グループ・ツリー・レポートを処理するための標準機能があります。グループ・ツリーでグループ・ツリー構造が視覚化される方法は、ブラウザーにハード・ディスクやネットワーク・ドライブの内容が表示される方法に似ています。

手順

グループ・ツリー・レポートを処理するには、以下のステップを実行します。

1. オプション「**RA**」(RACF 管理) を選択します。
2. オプション「**3.8**」(グループ・ツリー) を選択します。 49 ページの図 44 に示す「Reports Group tree」パネルが表示されます。

```
Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
         zSecure Admin+Audit for RACF - RACF - Reports Group tree
Command ===> ____________________________________________________ _ start panel

Show structured group tree display:
Group id  . . . . . ________     (group profile key or filter)
Start at  . . . . . ________     (group or filter, show only groups below)
Scope of  . . . . . ________     (group special, show only groups in scope)
Exclude . . . . . . ________     (group or filter)
Complex . . . . . . ________     (complex name or filter)

Enter "/" to include data in output
/  Installation data
/  Users/Subgroups

Enter "/" to select option
_  Output in print format


'Start at' is only allowed with an unload as data source, not a live database
```

図 44. 「Group tree selection」パネル

RACF グループ・ツリーの特定のブランチのみを表示するには、「**Start at**」フィールドにグループ名 (またはフィルター) を入力します。このオプションは、アンロード・データ・ソースを使用して実行する場合にのみ使用可能です。すべてのフィールドをブランクのままにすると、RACF データベースのグループ・ツリー全体が表示されます。

a. オプション: インストール・データをグループ・ツリー・レポートに組み込むことを指定するには、「**インストール・データ**」の前に / を入力します。「インストール・データ」は、通常、グループ記述を格納するために使用されます。

b. サブグループと接続ユーザーの詳細情報を詳細レベル・パネルに組み込むには、「**Users/Subgroups**」フィールドの前に / を入力します。

3. Enter を押して、「Group tree report」パネルを開きます。このパネルには、現在の RACF データベースのすべてのグループが表示されています。 50 ページの図 45を参照してください。

```
zSecure Admin+Audit for RACF GROUP TREE DISPLAY        1 s elapsed, 0.5 s CPU
 Command ===> _____________________________________________ Scroll===> CSR_
                                          8 Apr 2005 16:57
   Complex  Groups
   DEMO        267
   Group structure                      Lvl Subgrp Connct SupGroup Owner    X
__  SYS1                                 1     19     11 ........ IBMUSER_ X
__  BOOKS                                2      0      0 SYS1____ SYS1____
__   C#                                  2      7      1 SYS1____ SYS1____
__    C#ADMIN                            3      0     10 CR______ CR______
__    C#M                                3      9      2 CR______ CR______
__     C#MBCCW                           4      0      5 C#M_____ C#M_____
__     C#MCKG                            4      0     33 C#M_____ C#M_____
__     C#MPC2E                           4      0      9 C#M_____ C#M_____
__     C#MPC4R                           4      0      0 C#M_____ C#M_____
__     C#MQ                              4     23      0 C#M_____ C#M_____
__      C#MQA                            5      8    241 C#MQ____ C#MQ____
__       C#MBQAHW                        6      2      1 C#MQA___ C#MBWTK_ X
__        C#MBQAHU                       7      0      0 C#MBQAHW C#MBQAHW
__        C#MBQAH2                       7      0      1 C#MBQAHW C#MBWTK_ X
__       C#MBQALU                        6      0      1 C#MQA___ C#MQA___
__       C#MBQAMC                        6      0     12 C#MQA___ C#MQA___
__       C#MQA#HI                        6      0      0 C#MQA___ C#MQA___
__       C#MQAT#1                        6      0      0 C#MQA___ R##SLIN_ X
```

図 45. 「Group tree report」パネル

図 45 に示す「Group tree report」パネルの X 列の Xは、グループの SPECIAL ユーザーの有効範囲から外れていることを示します。有効範囲から外れた理由は、所有者が上位グループと等しくないためです。

4. インストール・データを要求した場合は、PF11 を押して情報を確認します。
5. PF8 を数回押して、グループ・ツリー構造の他の部分を確認します。
6. 詳細情報がレポートに含まれている場合にこの情報を表示するには、グループの前に **S** 行コマンドを入力します。このアクションにより、図 46 に示すグループ・ツリー・レポート詳細パネルが表示されます。

```
zSecure Admin+Audit for RACF RACF GROUP TREE DISPLAY            Line 1 of 11
Command ===> _____________________________________________ Scroll===> CSR_
                                          8 Apr 2005 16:58
   Group structure                      Lvl Subgrp Connct SupGroup Owner    X
       C#MCDEMO                          4      1      5 C#MC     C#MC
  User     Auth    R SOA AG Uacc    Name                 InstData
_ C#MCCW1  USE     _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW2  USE     _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW3  USE     _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW4  USE     _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW5  USE     _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
   SubGroup
_ C#MCDEM2
```

図 46. 「Group tree report detail」パネル

SETROPTS レポートの実行およびクラス設定の表示

以下のタスクにより、ISPF **RA.S** 機能を使用して、SETROPTS レポートの実行、およびクラス設定の表示を行うことができます。

このタスクについて

zSecure Admin 内で **RA.S** 機能と **AU.S** 機能を使用して、現在のシステム全体の RACF オプションまたはクラス記述子テーブル (CDT) を管理できます。 SETROPTS レポートまたは RACFCLAS レポートの **AU.S** バージョンについて詳しくは、 89 ページの『第 8 章 システムの保全性とセキュリティーの監査』で説明します。詳しくは、 90 ページの図 72および 92 ページの図 74を参照してください。

注: RA.S オプションは zSecure Admin でのみ使用可能です。

手順

SETROPTS レポートを実行してクラス設定を表示するには、以下のステップを実行します。

1. オプション「**RA**」(RACF 管理) を選択します。
2. オプション「**S**」(設定) を選択して、図 47 の SETROPTS 設定およびクラス情報のパネルを開きます。 SETROPTS レポートおよび RACFCLAS レポートが自動的に生成されます。

```
                zSecure Suite Display Selection
Command ===> ____________________________________________________________

  Name     Summary Records Title
_ SETROPTS       2       2 RACF SETROPTS system settings
_ RACFCLAS     512     512 RACF class settings
_ RRSFNODE       1       5 RACF remote sharing facility nodes
********************************** Bottom of Data ****************************
```

図 47. SETROPTS 設定とクラス情報

3. 「**SETROPTS**」選択フィールドに **S** コマンドを入力し、図 48 に示す SETROPTS レポートを開きます。

```
RACF SETROPTS system settings                                  Line 1 of 68
Command ===>_____________________________________________ Scroll===> CSR_
                                          15 Apr 2005 11:19

Complex  System
DEMO     DEMO

General RACF properties                Data set protection options
Access Control active         Yes      Prevent duplicate datasets    No
Force storage below 16M       No       Protectall                    Yes/fail
Check all connects  GRPLIST   Yes      Automatic Dataset Protect     No
Check genericowner for create Yes      Enhanced Generic Naming       Yes
NOADDCREATOR is active        Yes      Prefix one-level dsns         ONEQUAL
Dynamic CDT active            No       Prevent uncataloged dsns      Yes/fail
RACF local node               DEMO     GDG modelling                 No
RRSF propagate RACF commands  No       USER modelling                No
RRSF propagate applications   No       GROUP modelling               No
RRSF propagate passwords      No
RRSF honour RACLINK PWSYNC    Yes
Application ID mapping stage  0
Level of KERB processing        0
Primary Language              ENU
Secondary Language            ENU
```

図 48. RACF 設定 SETROPTS レポート

このレポートを使用して、RACF システム全体の設定を調べることができます。レポートを上下にスクロールするには、PF7 と PF8 を使用します。

また、**SETROPTS** のオプションのほとんどは、このパネルから管理できます。管理するには、変更する **SETROPTS** 設定の値に、必要な値を上書き入力します。このアクションでは、変更を適用する適切な **SETROPTS** コマンドが自動的に生成されます。

4. 「Setropts およびクラスの設定」パネルに戻るには、PF3 を押します。
5. クラス設定レポートを表示するには、以下のステップを実行します。
   a. **RACFCLAS レポート選択**フィールドに **S** コマンドを入力します。図 49 に示す「RACF クラス設定」パネルが開きます。

```
RACF class settings                                          Line 1 of 197
Command ===>_____________________________________________ Scroll===> CSR_
                                              15 Apr 2005 11:19
  Class    Active Description
_ ACCTNUM  Active TSO account numbers
_ ACICSPCT Active CICS program control table
_ AIMS     Active IMS application group names (AGN)
_ ALCSAUTH ______ Supports the Airline Control System/MVS (ALCS/MVS) product
_ APPCLU   Active Verify ID of partner logical units during VTAM session estab
_ APPCPORT Active Controls which user IDs can access the system from a given L
_ APPCSERV Active Controls whether a program being run by user can act as a se
_ APPCSI   ______ Controls access to APPC side information files
_ APPCTP   ______ Controls the use of APPC transaction programs
_ APPL     Active Controls access to applications
_ BCICSPCT Active Resource group class for ACICSPCT class
_ CACHECLS ______ Profiles for saving and restoring cache contents
_ CBIND    ______ Controls the client's ability to bind to the server
_ CCICSCMD Active Used to verify that user is permitted to use CICS syst prog
_ CIMS     ______ IMS command resource group
_ CONSOLE  Active Controls access to MCS consoles
_ CPSMOBJ  ______ Used by CICSPlex SysMgr for operational controls
```

図 49. RACF 設定 RACFCLAS レポート

   b. 関係するリソース・クラスの詳細設定を表示するには、「**クラス**」選択フィールドに **S** 行コマンドを入力します。
   c. オプション: **R** 行コマンドを入力し、関係するリソース・クラスをリフレッシュするか、または「**アクティブ**」列の既存の値に対して新しい値を上書き入力します。非アクティブなリソース・クラスをアクティブにするには、Y、A、または Active と入力します。アクティブなリソース・クラスを非アクティブにするには、N またはブランクを入力します。

第 4 章 分散管理機能および範囲付き管理機能

このセクションでは、使用可能な管理機能の中で唯一選択されたサブセットである分散管理機能について説明します。このセクションでは、グループ監査員ビューについても説明します。

RACF 範囲を使用したグループ管理

注: この機能は Security zSecure Admin でのみ使用可能です。

グループ管理者の手を加えていない RACF 範囲に機能を限定するには、プログラムを制限モードで実行する必要があります。この要件は、以下のいずれかの方式を使用して実現できます。

方式 1 UACC(NONE) を使用して XFACILIT プロファイル **CKR.READALL** を作成し、中央管理者のみに READ 許可を与える。

この方式が最も簡単で、評価目的に最適です。

方式 2 データ・セットへのプログラム・アクセス (PADS) または zSecure サーバー (自己接続モードなどで) を使用して、RACF データベースにアクセスする。

これらの方式は最も安全ですが、相当なセットアップが必要になります。両方式のセットアップについては、「*IBM Security zSecure Admin and Audit for RACF: 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

方式 3 **SETUP PREAMBLE** で SIMULATE RESTRICT コマンドを使用する。

この方式は、独自の範囲をテストする場合にのみ有効です。

方式 4

SETUP VIEW コマンドを発行し、「**Select view**」で **1** または **2** を選択する。

1. 変更が許可されたプロファイルだけを表示する (管理者ビュー)。
2. 変更またはリストが許可されたプロファイルだけを表示する。

この方式は、追加の範囲制限を提供します。ただし、この範囲制限は制限モードではなく、管理者ビューと言います。

方式 3 のように、この方式は、独自の範囲をテストする場合にのみ有効です。これにより、READ アクセス権限のみを持つプロファイルを表示できなくなります。また、システム全体の特権を無視するため、手を加えていない RACF 範囲よりもさらに制限が強くなります。

「クイック管理」パネル

注: この機能は zSecure Admin でのみ使用可能です。

クイック管理機能には以下の 2 つのいずれかの方式を使用してアクセスできます。

- 『スタンドアロンの方法を使用した「クイック管理」パネルへのアクセス』
- 『RA.Q を使用した「クイック管理」パネルへのアクセス』

スタンドアロンの方法を使用した「クイック管理」パネルへのアクセス

手順

1. メインメニューからオプション **X** (終了) を選択します。
2. ISPF オプション **6** のコマンド行で `CKR,STARTTRX(MENU(RA.Q))` と入力して「クイック管理」アプリケーションを開始する。図 50を参照してください。

RA.Q を使用した「クイック管理」パネルへのアクセス

手順

1. メインメニューで、**RA.Q** を選択して、図 50 に示されている「クイック管理」パネルを開きます。
2. 「クイック管理」パネルを使用すると、詳細は表示せず、集中型または非集中型のユーザー管理者に必要な最も使用頻度の高い機能にアクセスできます。

   「クイック管理」パネルは、システムまたは管理者のグループ SPECIAL 属性に依存します。パネルのオプションは、`CKR.OPTION.RA.Q...` プロファイルによって非表示にできますが、この指定をしない場合、メニューは表示されるとおりに機能します。

```
  Menu   Options   Info   Commands   Setup     StartPanel
------------------------------------------------------------------------------
               zSecure Admin – RACF - Quick admin
 Command ===> ____________________________________________________________

1    Password        Set new password for user
2    Resume          Make sure user can work
3    Display         List user definition
4    Modify          Change user definition
5    Connect         Add group to a user
6    Add user        Create new userid from scratch
7    Add user copy   Create new userid like existing model
8    Phrase          Set new password phrase for user

Userid  . . . . . . ________     (type userid and press enter)
New password  . . .              (type new password, option 1 only)
Verify password . .              (type new password again, option 1 only)
Group   . . . . . . ________     (type connect group, option 5 only)
```

図 50. クイック管理

CKGRACF を使用したグループ管理

注: この機能は zSecure Admin でのみ使用可能です。

zSecure Admin では、分散型の RACF 制御のベースとして **CKGRACF** プログラム、つまり**ヘルプ・デスク**と**グループ管理**を提供しています。**CKGRACF** プログラムは以下の機能を提供するように設計されています。

- パスワード・リセットなどの一般的に使用される**ヘルプ・デスク**機能へのメニュー経由でのアクセス。
- 許可および接続などの共通的に使用される**グループ管理**機能へのメニュー経由でのアクセス。
- グループ SPECIAL 権限を付与しない、これらの機能へのアクセス。
- **CKGRACF** 機能を使用するためのユーザー権限へのきめ細かい制御。

CKGRACF がメイン **CKRCARLA** プログラムと異なる点は、CKGRACF がほとんどのタスクを APF 許可インターフェース経由で実行するのに対し、メインプログラムは可能な場合は常に、通常の RACF コマンドを生成するということです。APF 許可が必要であることから、メイン **CKRCARLA** プログラムのユーザーは生成された RACF コマンドを実行するための十分な管理 RACF 権限が必要です。これらのコマンドは、パラメーターを上書きするか、プロファイルを変更する行コマンドを使用した場合に生成されます。zSecure Admin ISPF のメイン・パネルでは、必要な変更
R を実行するための標準の RACF コマンドを生成できないとき、**CKGRACF** プログラムを呼び出して RACF 変更を実行する場合があります。ユーザー・データ・フィールドの更新がこのシナリオの最も適した例です。

CKGRACF ユーザーは、SPECIAL 属性またはグループ SPECIAL 属性などの特殊な RACF 権限が不要です。**CKGRACF** プログラムは、APF インターフェースを使用して、タスクに必要なあらゆる権限を持つことができます。そのため、それぞれの **CKGRACF** ユーザーまたはユーザー・グループを複数の XFACILIT クラス・プロファイルのアクセス制御リストに入れることによって、**CKGRACF** プログラムを使用するユーザーを制御する必要があります。これらのプロファイルを作成して、選択されたユーザーを PERMIT (許可) することで、**CKGRACF** を経由して特定の機能を使用できるユーザーを制御できます。

このセクションでは、以下の 2 つの **CKGRACF** ユーザーのカテゴリーを扱います。

- パスワード・リセットおよび再開などのコマンドを発行するヘルプ・デスク・ユーザー。
- 許可または接続を発行する非集中管理者。

ヘルプ・デスク機能は別個のパネルから実行されますが、グループ管理者の機能は通常の zSecure Admin パネルから使用できます。メニューは、RACF プロファイルを XFACILIT クラスに追加することによって調整できます。各プロファイルが機能を表します。アクセス権限は通常のアクセス規則を使用して付与されます。デフォルトでは、すべてのオプションが表示されますが、メニューの調整を行った後は、権限付与された機能だけが zSecure Admin ユーザーに表示されます。

自分で評価する場合、すべての **CKGRACF** 機能についての全権限を自分自身に与えてから機能を検討します。現実的な分散**管理者**のグループ向けに XFACILIT クラス制

御を設定することは一回限りの作業とはいえ、大変な作業になる場合があります。これには、以下のプロセスが含まれます。

1. どの RACF グループをどの管理者に関連付けるかを正確に定義する。
2. どの **CKGRACF** 機能をどの管理者に与えるかを定義する。
3. この環境を作成するために必要な **RDEFINE** コマンドと **PERMIT** コマンドを作成する。

クラス制御の定義には長い時間を要するため、初期の製品評価時には細かい制御を設定せずに実行します。

完全な **CKGRACF** 権限を自分自身に付与するには、自分または RACF SPECIAL 属性を持つ別のユーザーが以下の RACF コマンドを発行する必要があります。

```
permit ckg.** class(xfacilit) acc(update) id(yourid)
```

単一パネルのヘルプ・デスク機能

注: この機能は zSecure Admin でのみ使用可能です。

ヘルプ・デスク機能には以下の 2 つのいずれかの方式を使用してアクセスできます。

- 『スタンドアロンの方法を使用したヘルプ・デスク機能へのアクセス』
- 『RA.H を使用したヘルプ・デスク機能へのアクセス』

スタンドアロンの方法を使用したヘルプ・デスク機能へのアクセス

手順

1. メインメニューからオプション **X** (終了) を選択します。
2. ISPF オプション **6** のコマンド行で **CKR,STARTTRX(MENU(RA.H))** を入力して**ヘルプ・デスク**機能を開始します。 57 ページの図 51を参照してください。

RA.H を使用したヘルプ・デスク機能へのアクセス

手順

1. メインメニューから **RA.H** を選択して、 57 ページの図 51 に示す「ヘルプ・デスク」パネルを開きます。

```
 Menu   Options   Info   Commands   Setup     StartPanel
--------------------------------------------------------------------------------
                zSecure Admin – RACF - Helpdesk
Option  ===> ____________________________________________________________

1    List           List RACF profile information
2    Password/Phrase Set a new password or phrase
3    Default        Set the password or phrase to the user's default value
4    Previous       Set the password or phrase to the previous value
5    Resume         Resume a userid after too many invalid attempts
6    Disable        Temporarily disable logon for a userid
7    Enable         Allow user to logon after a Disable
8    Set default    Define a default password or phrase for a userid

Userid  . . . . . ________     (type userid and press enter)
Password or phrase . . . .  _  1. Password  2. Phrase
New password . . . . . .           Verify password  .
Reason  . . . . . ____________________________________________________________
Workflow option . . 1      1. Request  2. Withdraw  3. Approve  4. Deny
```

図 51. 単一パネルのヘルプ・デスク

このパネルを使用すると、集中型または非集中型のヘルプ・デスク従業員に必要な最も使用頻度の高い機能を実行できます。

2. ヘルプ・デスク機能の動作を確認するには、以下のステップを実行します。
   a. 「**ユーザー ID**」フィールドにユーザー ID を入力します。
   b. Enter を押して、図 51 に示すようなユーザー ID について選択された情報を表示する「ヘルプ・デスク」パネルを開きます。
   c. ユーザーの詳細を表示するには、「ヘルプ・デスク」パネルの **1** を選択します。

A ユーザー ID の状況を確認した後で、新規パスワードの設定やパスワード・
A フレーズの設定などの変更を実行できます (オプション **2**)。

初期構成では、**CKGRACF** コマンドが実行される前に表示されます。個別の管理者に対してこの確認プロンプトを抑止するには、コマンド行で `setup confirm` と入力します。あるいは、すべての管理者に対してこのプロンプトを抑止するには、`setup default` と入力し、オプション **4** を選択します。次のパネルで、確認設定を変更します。

ヘルプ・デスクのパスワードまたはフレーズの管理機能

注: この機能は zSecure Admin でのみ使用可能です。

R ヘルプ・デスクの **CKGRACF** 機能のうち最も重要と考えられるものは、パスワードま
R たはフレーズの使用可能化、設定、取り消し、および再開です。次の表には使用可
R 能な機能のリストと、機能の仕組みが説明されています。

表 4. ヘルプ・デスクのパスワード関連機能

ヘルプ・デスク機能	説明
新規パスワードまたはフレーズの設定 (オプション 2)	新規パスワードまたはフレーズを設定し、それを 2 回入力します。「**フレーズ**」を選択した場合、後続のパネルが表示されます。zSecure Admin および zSecure Audit for RACF では、ユーザー・プロファイルを更新するために RACF を使用しません。**CKGRACF** 権限が代わりに使用されます。また、ユーザーは再開されます。
デフォルト・パスワードまたはフレーズの使用可能化 (オプション 3)	パスワードまたはフレーズが、ユーザーのデフォルト・パスワードまたはフレーズに設定されます。中央管理者は、ユーザーの個人用デフォルト・パスワードまたはフレーズを事前に設定しておく必要があります。ヘルプ・デスク管理者にはパスワードが表示されません。また、ユーザーは再開されます。
以前のパスワードまたはフレーズの使用可能化 (オプション 4)	以前のパスワードまたはフレーズが再び有効になります。この場合、管理者がパスワードまたはフレーズを設定することはありません。以前のパスワードまたはフレーズは自動的に期限切れのマークが付けられ、ユーザーは次回のログオン時に以前のパスワードをもう一度だけ使用できます。また、ユーザーは再開されます。
デフォルトに設定 (オプション 8)	ユーザー ID に対するデフォルト・パスワードまたはフレーズを定義します。

デフォルト・パスワードまたはフレーズ (オプション 3) は RACF では新しい概念です。この目的は、ユーザーごとに単純な (品質の低い) パスワードまたはフレーズを定義することです。各ユーザーは、いつまでも覚えておくことができる単語や番号を選択します。この単語は、**CKGRACF** を使用して設定されたときに、中央の RACF 管理者のみが確認できます。機能が呼び出されたとき、他の管理者には表示されません。ユーザーの通常のパスワードが何らかの理由で使用できなくなった場合、任意のヘルプ・デスク管理者がユーザーのデフォルト・パスワードまたはフレーズを使用可能にすることができます。ユーザーは通常の新規パスワードをできるだけ早く作成することが求められます。このアプローチは、**SYS1**、**SECRET**、**PSWPSW** などのシステム全体のリセット・パスワードを使用するよりも優れています。

ヘルプ・デスクの調整

インストール済み環境の「ヘルプ・デスク」パネルを調整するには、以下のガイドラインに従ってください。

インストール済み環境の「ヘルプ・デスク」パネルは以下のいずれかの方法で調整できます。

- `CKR.OPTION.RA.H` で開始する `XFACILIT` プロファイルを通じて、ヘルプ・デスクのオプションを選択的に使用可能または使用不可にすることができます。
- **SETUP NLS** を使用して、パネルのテキストおよびオプションを変更できます。

一部の機能はユーザー管理機能であり、限定された数のユーザーだけが使用できるようにする必要があります。これらの機能の例としては、デフォルト・パスワードまたは新規パスワードの設定や、権限レベルの設定などがあります。 XFACILIT クラスの CKR.OPTION プロファイルを定義して、管理機能の使用を制限することができます。したがって、インストール済み環境では、各ユーザーに対して「ヘルプ・デスク」パネルで表示されるオプションを指定し、組織内での責任を選択的に委任することができます。

対応するプロファイルのアクセス制御リストでユーザー・アクセスの権限が付与されている場合、ユーザーは機能を実行できます。そうでない場合、アクション・リストには行コマンドが表示されず、行コマンドの使用は禁止されます。図 52 に、オプション 2、6、8 が含まれていない、調整された「ヘルプ・デスク」パネルの例を示します。これらのオプションが含まれていないのは、ユーザーが該当する CKR.OPTION.RA.H プロファイル内で必要なアクセス権限を持たないためです。

```
   Menu   Options   Info   Commands   Setup     Startpanel
--------------------------------------------------------------------------------
                  zSecure Admin - RACF - Helpdesk
Option  ===> ____________________________________________________________________

1    List           List RACF profile information
3    Default        Set the password or phrase to the user's default value
4    Previous       Set the password or phrase to the previous value
5    Resume         Resume a userid after too many invalid attempts
7    Enable         Allow user to logon after a Disable

Userid . . . . . .  ________  (type userid and press enter)
Password or phrase . . . .  _  1. Password  2. Phrase

Reason . . . . . .  ____________________________________________________
Workflow option . . 1      1. Request  2. Withdraw  3. Approve  4. Deny
```

図 52. 調整された「ヘルプ・デスク」パネル

第 5 章 データを管理するためのセットアップ機能

「**セットアップ**」の機能により、zSecure Admin および zSecure Audit for RACF により使用されるデータを制御できます。

データ・ソースは、使用中に切り替えることができます。「**セットアップ**」には、グローバル・スイッチおよびパラメーターを設定する機能もあります。これらの機能のいくつかは、「**Resolve**」オプションと「**Explode**」オプションにも備わっています。

データの追加

このタスクについて

これまでは、さまざまなプロファイルを表示するときにライブ RACF データのみを使用していました。以下のデータ・ソースを作成および使用できます。

- アンロードされた RACF データベース。
- CKFREEZE データ・セット。このデータ・セットには、すべての DASD および各種内部 z/OS テーブルから抽出された情報が保管されています。

このプロセスを開始するには、以下のステップを実行します。

手順

1. メインメニューに戻ります。必要に応じて PF3 を使用します。
2. 「**SE (セットアップ)**」オプションを選択します。 62 ページの図 53 に示す「セットアップ」パネルが開きます。
3. 24 行表示の場合、パネル内を上下にスクロールするには PF8 および PF7 を押します。

   ヒント: 続行する前に、「セットアップ」パネルでオプション **0** から **5** を 1 つずつ選択すると、各種セットアップ・オプションの概要を表示できます。

```
   Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                zSecure Admin+Audit for RACF - Setup
Command ===> ____________________________________________________________

0    Run             Specify run options
1    Input files     Select and maintain sets of input data sets
2    New files       Allocate new data sets for UNLOAD and CKFREEZE
3    Preamble        Carla commands run before every query
4    Confirm         Specify command generation options
5    View            Specify view options
6    Instdata        Customize installation data appearance
7    Output          Specify output options
8    Command files   Select and maintain command library
9    Certificates    Specify templates for new digital certificates
A    Alert           Configure zSecure Alert
B    Collections     Select and maintain collections of input sets
U    User defined    User defined input sources
C    Change Track    Maintain Change Tracking parameters
N    NLS             National language support
T    Trace           Set trace flags and CARLa listing for diagnostic purposes
W    Windows         zSecure Visual RACF configuration
D    Default         Set system defaults
R    Reset           Reset to system defaults
I    Installation    Specify installation defined names
```

図 53. セットアップ

新規ファイルの追加

手順

1. 初期セットアップ・パネル (図 53 を参照) から、オプション「**2 (New files)**」を選択して、図 54 に示されている「新規ファイル」パネルを開きます。

```
   Menu   Options   Info   Commands     Setup
--------------------------------------------------------------------------------
                         zSecure Admin+Audit for RACF - Setup - New files
 Command ===> ____________________________________________________________

 Create new unload file from the RACF database, and/or CKFREEZE file


 Data set with unload from RACF database, use UNLOAD as last qualifier
 Unload . . . . . ____________________________________________

 I/O configuration file, use CKFREEZE as last qualifier
 Ckfreeze . . . . . ____________________________________________

 Description for this set of input files
  Description  . . . ____________________________________________________________




 Enter data set names and description and press ENTER
```

図 54. 「新規ファイル」パネル

2. 「**Unload**」行にデータ・セット名を入力します。

   データ・セット名の入力時に、データ・セット名の上位修飾子としてユーザー ID を使用しないようにする場合には引用符を使用してください。これは、デー

A タ・セットが既に存在しているかどうかには関係ありません。ただし、データ・
A セットが存在している場合、これらのデータ・セットはカタログされている必要
A があります。

3. CKFREEZE 行にデータ・セット名を入力します。必要に応じて引用符を使用します。
4. 「**説明**」行に、ファイルの簡潔な固有の説明を入力します。例えば「UNLOAD and CKFREEZE data sets created on 8 Apr 2005」などです。

   ヒント: 入力ファイルの「**説明**」フィールドを使用して、このセットに含まれているデータ・セットの種類を記述しておくと便利です。以後、この習慣により、含まれているデータ・セットを調べるためにブラウズ・モードまたは編集モードでセットが開かなくてもよくなります。
5. Enter を押します。

   指定したデータ・セット名のいずれかまたは両方が存在しない場合、図 55に示されている割り振り入力パネルが開きます。このパネルで、新規データ・セットを割り振り、カタログします。

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - New files
Command ===> ____________________________________________________________

CKFREEZE file not found. Change dataset name, or specify allocation parameters

 Dataset name . . . MYNAME.CKFREEZE_____________________________

Allocation parameters to create new dataset:
 Volume serial  . . ______      (Blank for authorized default volume)
 Generic unit   . . ________    (Generic group name)
 Space units  . . . _____       (KB, TRKS, or CYLS)
 Primary quantity   ________    (In above units, press HELP for suggestion)
 Secondary quantity ________    (In above units)

 Record format  . . VBS__       (VB or VBS)
 Block size   . . . 27998__
 Logical Record Len X______     (X or maximum record length)

Press ENTER to allocate dataset, press END to stop processing
```

図 55. 一般的な割り振りパネル

6. 適切な割り振りパラメーターを入力して、Enter を押します。ただし、DCB 属性は変更しないでください。

   指定したデータ・セットが両方とも新規の場合は、割り振りパネルがもう一度表示されます。これらのパネルを実行すると、動的割り振りを使用して新規データ・セットが割り振られ、カタログされます。アンロードされた RACF コピーおよび CKFREEZE データ・セットを初めて作成するときは、十分なディスク・スペースを指定する必要があります。RACF アンロードの場合は、可能な限りライブ RACF データベースの使用スペースと同程度の容量のスペースを確保してください。 CKFREEZE ファイルの場合、オンラインの DASD ボリュームごとに少なくとも 2 MB が必要になります。また、カタログ用および HSM 情報用のスペースも必要です。さらに、1GB の HFS/ZFS スペースごとに 2 MB、5000 の IMS または CICS トランザクションまたはプログラムごとに 1 MB を用意して

ください。CKFREEZE データ・セットのスペース所要量について詳しくは、「*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。

DCB パラメーターは変更しないでください。必要なディスク・スペースを十分に把握できるようになるまでは、大きな 2 次割り振り容量 (例: 100 MB) を指定してください。

ヒント: アンロードされた RACF コピーと CKFREEZE データ・セットを初めて作成した場合は、ISPF を使用してこれらのコピーとデータ・セットを調べ、使用されたディスク・スペース容量を判別します。この情報を使用して、将来の使用量を見積もることができます。

ファイルを割り振った後、図 56 に示すパネルが開きます。

```
 Menu   Options   Info   Commands
--------------------------------------------------------------------------------
                     zSecure Admin and Audit - Setup - Input files
Command ===> ____________________________________________________ Scroll ===> CSR_

Description . . . . UNLOAD and CKFREEZE data sets created on 8 Apr 2005.
Complex . . . . . ________   Version  . . . .  ____
Enter data set names and types.         Type END or press F3 when complete.
Enter dsname with .* to get a list      Type SAVE to save set, CANCEL to quit.
Valid line commands: E I R D            Type REFRESH to submit unload job.

   Data set name or DSNPREF=, or Unix file name           Type or ?   NJE node
_  'MYNAME.UNLOAD'                                       UNLOAD      ________
_  'MYNAME.CKFREEZE'                                     CKFREEZE    ________
****************************** Bottom of data ********************************
```

図 56. zOS での入力ファイル・セットの初期表示

ファイルのリフレッシュとロード

このタスクについて

1 つの入力セットを構成するデータ・セットがリストされます。入力セットには、複数の CKFREEZE データ・セット、複数の SMF ファイル、および複数の HTTP ログ・ファイルを含めることができます。ただし 1 つの入力セットには、1 つの RACF アンロードのみ、または 1 つの分割データベースからの 1 つ以上の RACF データ・セットを含めることができます。

ファイルをリフレッシュしてロードするには、以下のステップを実行します。

手順

1. 入力ファイル・パネル (図 56) で、コマンド行に REFRESH と入力します。Enter を押すと、「Job submission」パネルが開きます。
2. 「Job submission」パネルの「**Job statement information**」セクションに、有効なジョブ・カードを入力します。
3. 「**Edit JCL Option (2)**」を使用して標準 ISPF エディターを開き、JOB ステートメントをカスタマイズし、ジョブに対して必要な変更を行います。 例えば zSecure Admin および zSecure Audit for RACF にアクセスするには、JOBLIB ま

たは STEPLIB ステートメントが必要な場合があります。zSecure Collect for z/OS (CKFCOLL) を LNKLST 内の許可ライブラリーにコピーした場合、そのための JOBLIB または STEPLIB ステートメントは不要です。ジョブ・クラスには、大きい領域サイズまたは無制限の領域サイズを割り当ててください。

4. ジョブを実行依頼してください。

次のタスク

ジョブが実行されるまで待機します。実行を待機しているジョブのキューが長い場合は、ジョブ実行中に zSecure Admin and Audit を終了できます。構成が大きな場合を除き、ジョブ自体の実行にかかる時間はわずか数分です。ジョブ・カードに NOTIFY= *yourid* を追加できます。通常、ジョブが失敗する場合の原因はストレージが不足していることにあります。zSecure Collect for z/OS の実行には、通常は 64 MB の領域サイズで十分です。

ジョブが完了したら、次の手順に進みます。

入力セットの選択

手順

1. 「Input file」パネルを開き、**Command** 行で「**SE.1** (「セットアップ」パネルのオプション **1**) と入力します。

   「Input file」パネルの内容は、作成した入力セットと、入力ファイルに対して入力した説明から成ります。例を 図 57 に示します。

```
 Menu   Options   Info   Commands     Setup
------------------------------------------------------------------------------
                      zSecure Admin+Audit for RACF - Setup - I Row 1 from 4
Command ===> ____________________________________________ Scroll ===> CSR_

(Un)select (U/S/C/M) set of input files or work with a set (B, E, R, I, D or F)

   Description                                              Complex
_  UNLOAD and CKFREEZE data sets created 8 Apr 2005                 selected
_  Active backup RACF data base                             DEMO
_  Active primary RACF data base                            DEMO
_  Active backup RACF data base and live SMF data sets      DEMO
****************************** Bottom of data ********************************
```

図 57. 入力ファイルの選択

図 57 で selected とマークされている入力ファイル・セットは、 zSecure Admin および zSecure Audit for RACF で、現在これらの入力セットが入力データとして使用されていることを示します。他の入力セットも必ず存在します。次のものがあります。

- アクティブ・バックアップ RACF データベース
- アクティブ 1 次 RACF データベース
- アクティブ・バックアップ RACF データベースおよびライブ SMF データ・セット

この表示では定義されている任意の入力セットに切り替えることができます。例えば、作成したアンロード・ファイルとライブ RACF データベースとの間で切り替えるには、このパネルに進んで該当する入力セットを選択します。

2. 以下の使用可能な行コマンドのいずれかを使用します。

S – 処理する入力セットの選択
入力セットを選択すると、そこに含まれるデータ・セットが処理のために選択されます。データ・セットが配置されると、そのセットに選択済みのマークが付けられます。また、このオプションは、A (セットの Add または Addition) の指定によっても選択されます。選択したセットは、既に選択されているセットに追加されます。セッション中には入力選択内容を複数回にわたって変更することができますが、通常の使用法ではこのような変更は行いません。

C - 比較ベースとしてのセットの選択
事前定義された入力ファイルのセットを比較の基本セットとして設定します。1 つのセットのみを比較の基本セットとして選択できます。

M – マージ・ソースとしてのセットの選択
事前定義された入力ファイルのセットをマージのソース・セットとして設定します。

U – 入力セットを選択から除去
選択されている「**アクティブ・バックアップ RACF データベースおよびライブ SMF データ・セット**」の選択を解除します。そのセットは選択状態ではなくなり、今後の照会で使用されません。

入力セットのコレクションの指定

以下のタスクにより、プログラム用の入力データ・セットのコレクションを指定できます。

このタスクについて

「SETUP Collections」で、プログラムが使用する入力セットのコレクションを指定できます。コレクションを使用した場合、SETUP FILES で以前に選択された入力ファイル・セットが使用されなくなります。これ以降に SETUP FILES で入力ファイル・セットを選択すると、コレクションが選択解除されます。

手順

1. メインメニューの「オプション」行に SE (セットアップ) と入力し、**Enter** を押します。 セットアップ・メニューが表示されます。

```
    Menu         Options       Info    Commands     Setup             Startpanel
-------------------------------------------------------------------------------
                        zSecure Suite - Setup
 Option ===> ____________________________________________________________________
                                                                        More:     +
 0    Run             Specify run options
 1    Input files     Select and maintain sets of input data sets
 2    New files       Allocate new data sets for UNLOAD and CKFREEZE
 3    Preamble        CARLa commands run before every query
 4    Confirm         Specify command generation options
 5    View            Specify view options
 6    Instdata        Customize installation data appearance
 7    Output          Specify output options
 8    Command files   Select and maintain command library
 9    Certificates    Specify templates for new digital certificates
 B    Collections     Select and maintain collections of input sets
 U    User defined    User defined input sources
 C    Change Track    Maintain Change Tracking parameters
 N    NLS             National language support
 T    Trace           Set trace flags and CARLa listing for diagnostic purposes
 D    Default         Set system defaults
 R    Reset           Reset to system defaults
 I    Installation    Specify installation defined names
```

図 58. 「セットアップ」メニュー

2. 「セットアップ」メニューの「オプション」行に B と入力し、**Enter** を押します。 コレクションが定義されていない場合は、「セットアップ」のコレクション定義パネルが表示されます。

```
    Menu         Options       Info    Commands     Setup             Startpanel
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Collections
Command ===> ___________________________________________________________________

Enter description for new collection of input sets
_____________________________________________________
```

図 59. 「セットアップ」のコレクション定義パネル

1 つ以上のコレクションが定義されている場合は、次のパネルが表示されます。

```
    Menu         Options       Info    Commands     Setup             Startpanel
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Collections      Row 1 from 2
Command ===> _____________________________________________ Scroll ===> CSR

(Un)select (U/S) collection or work with a collection (E, R, I, or D)

   Description
_  Collection for systems of SYSPLEX TEST                          selected
_  Collection for systems of SYSPLEX PROD
****************************** Bottom of data ********************************
```

図 60. 「セットアップ」のコレクション表示

コレクション表示を使用して、処理する入力ファイル・セットのコレクションを選択し、コレクションを追加または削除します。次の行コマンドを使用できます。

S コレクションを選択します。コレクション内に含まれている入力セットが処理のために選択されます。データ・セットがシステム内で検出され

ると、コレクションは選択済みとしてマークされます。SETUP FILES を使用して選択されたセットは、クリアされます。同時に選択できるコレクションは 1 つのみです。

U コレクションをクリアします。このコレクションは選択状態ではなくなります。これは、今後の照会では使用されません。

E コレクションの内容を編集します。結果の表示で、コレクションの入力セットを選択またはクリアできます。

R コレクションを繰り返します。選択したコレクションの内容が新規コレクションにコピーされます。

I 新規コレクションを挿入します。

D コレクションを削除します。コレクションは、ダイアログの管理から削除されます。コレクション内の入力セットはシステムから削除されません。

3. コレクションを編集するには、コレクションの前で E アクション・コマンドを入力し、**Enter** を押します。 次のパネルが表示されます。

```
     Menu         Options       Info     Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Collections    Row 1 from 6
Command ===> _____________________________________________ Scroll ===> CSR

Description . . Collection for systems of SYSPLEX TEST

(Un)select (U/S/C/M) input sets to be added to or removed from collection

   Description
_  CKFREEZE for system TST1                                          selected
_  CKFREEZE for system TST2                                          selected
_  CKFREEZE for system TST3                                          selected
_  CKFREEZE for system PRD1
_  CKFREEZE for system PRD2
_  CKFREEZE for system PRD3
****************************** Bottom of data ********************************
```

図 61. 「セットアップ」のコレクション・セット表示

セット表示を使用して、入力ファイル・セットを処理するためにコレクションに追加します。セットは、SETUP FILES を使用して追加、編集、および削除できます。次の行コマンドを使用できます。

B 入力ファイル・セットの内容をブラウズします。セットをブラウズすることで、セットの定義を確認できます。詳細パネルを終了する際、このセットは選択されません。

C 入力ファイル・セットを比較ベースとして設定します。

M 入力ファイル・セットをマージ・ソースとして設定します。

S コレクションに追加する入力ファイル・セットを選択します。セットを選択すると、そこに含まれるデータ・セットが処理のために選択されます。データ・セットがシステム内で検出されると、そのセットは選択済みとしてマークされます。このオプションは、A を指定することでも選択されます。選択されたセットが、既に選択されている他のセットに追加されます。

U 入力ファイル・セットをクリアして、コレクションから削除します。そのセットは選択状態ではなくなり、今後の照会で使用されません。

次のタスク

zSecure Admin は、RACF データベースを保守するための機能を備えています。それぞれの例では、zSecure ISPF インターフェースを使用すること、およびこのインターフェースから発行されたコマンドに応答して製品で生成される RACF コマンドまたは **CKGRACF** コマンドを制御することが、いかに簡単に実行できるかを示します。

「セットアップ」のその他のパラメーター

「セットアップ」パネルでは、zSecure Admin および zSecure Audit のさまざまな割り振り/フォーマット特性を設定します。

これらの設定値を調べて、必要な変更を行います。ほとんどのユーザーにはデフォルト設定が適しています。「セットアップ」で最もよく使用されるオプションは、「確認」と「表示」です。

INSTDATA パラメーター

標準パネルでインストール・データ・フィールドがビジネス用語で表示されるようにこれらのフィールドのレイアウトを定義するには、**INSTDATA** パラメーターを使用します。

表示オプションおよび確認オプション

「表示」のオプションに関する情報は、27 ページの『アクセス・リストの表示設定』に記載されています。以下のセクションでは、「表示」のオプションのその他の設定と「確認」オプションについて説明します。

「**ACL/Connect sort**」選択項目は、アクセス制御リストと接続のソート順序を定義します。これは以下のタイプのソートを行います。

- オプション **1** を選択した場合は、ID (アクセス制御リストのユーザーまたはグループ) によるソートが実行されます。
- オプション **2** を選択した場合は、(展開後に) ユーザー ID によるソートが実行されます。
- オプション **3** を選択した場合は、アクセス・レベル (Alter-None) または接続権限 (Join-Use) の降順でのソートが実行されます。

これらのソート・オプションを使用すると、ACL と接続のスキャンが容易になり、検索対象を素早く検出できるようになります。

選択項目「**Show OS specific options**」を使用すると、z/OS と z/VM の固有オプションを切り替えることができます。あるいは、両方にタグを付けると、すべてのオプションを表示できます。

「**Add summary to RA displays for multiple complexes**」オプションを選択すると、オプション「**RA.U**」、「**RA.G**」、「**RA.D**」、および「**RA.R**」の表示パネルに要約セクションが 1 つ追加されます。マルチ複合システムを選択する場合、この要約

情報にはプロファイルの相違点が表示されます。この設定は ISPF プロファイルに保存されません。このオプションはデフォルトで有効です。

「**Add connect date and owner to RA.U connect group section**」オプションを使用して、**RA.U** 接続グループ・セクションに接続日と接続所有者を追加します。

「**Add user/group info to view**」パラメーターは、ACL のユーザーとグループ (接続グループを含む) の情報を表示するかどうかを指定します。この設定を使用すると、詳細な情報が表示されます。ただし、zSecure Admin と zSecure Audit for RACF が使用する仮想ストレージが大幅に増加するため、必要な TSO 領域が大きくなります。

このパラメーターの選択フィールドに **/** と入力するとスイッチがオンに設定され、ブランクを入力するとスイッチがオフに設定されます。

E メール出力の SMTP オプション

SMTP オプションを指定してレポートを E メールで送信するには、以下のガイドラインに従ってください。

「出力」パネル (「セットアップ」パネルのオプション **7**) には、**SMTP オプション**が表示されます。「**Send as e-mail**」パネル・オプションまたは「結果」パネルの **M (E-mail report)** アクション・コマンドを使用してレポートを E メールで送信する場合は、**SMTP** オプションを指定する必要があります。正しい設定については、システム・プログラマーにお問い合わせください。

```
   Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                  zSecure Admin+Audit for RACF - Setup
Command ===> ____________________________________________________________

Report options for following runs
Pagelength . . . . _____
Linelength . . . . _____

_  Convert all printed output to uppercase

Print options                       SMTP options
Destination . . .  ________________  SMTP node . . . .  ________
Sysout class  . .  _                 SMTP sysout . . .  _
Writer id . . . .  ________          SMTP writer . . .  ________
Copies  . . . . .  ___
Character set . .  ____
FCB . . . . . . .  ____
Forms . . . . . .  ____
Output descriptor  ________
Forms overlay . .  __
```

図 62. 出力定義をセットアップするパネル

図 62 に示すセットアップ出力パネルでは、「**SMTP node**」フィールドに、最終処理のための E メールのルーティング先としてジョブ入力サブシステム (JES) を指定します。SMTP サーバーがローカル・システムで実行されている場合は、このフィールドをブランクのままにするか、または `local` と指定できます。

SMTP sysout フィールドは、E メールの SMTP 出力処理に使用される JES 出力クラスを指定します。

「**SMTP writer**」フィールドには、E メールの SYSOUT データ・セットを選択する際に SMTP で使用する名前を指定します。外部書き出しプログラムの名前は、SMTP または CSSMTP アドレス・スペースの名前と同じです。通常、この名前は SMTP または CSSMTP です。

出力ソースとして E メールを使用する場合は、これらの **SMTP** オプションを定義する必要があります。

コマンドの実行制御

「確認」パネル (「セットアップ」パネルのオプション **4**) は重要です。

注: 「確認」パネルについて詳しくは、41 ページの『RACF コマンドの生成と確認』を参照してください。

最初の 2 つのパラメーターは zSecure Admin に適用され、さまざまなプロファイルを表示する際に、行コマンド (**D** (削除) や **C** (コピーまたは複製) など) とフィールド **Overtype** を参照します。これらの行コマンドから、RACF コマンドが生成されます。コマンドのステップと実行を制御するには、「確認」パネルで必要な値を選択します。プロファイルの前に **/** と入力し、Enter を押すと、使用可能なコマンドが表示されます。

表 5 に、「**Action on command**」オプションの設定値と説明を示します。

表 5. 「Action on command」オプションの設定値と説明

Action on command	説明
1. Queue	RACF 変更コマンド (行コマンドを使用すると自動的に生成されるコマンド) は、CKRCMD ファイルに書き込まれます。
2. Execute	自動的に生成された RACF コマンドは、確認後、RACF で直ちに実行されます。
3. Not allowed	プロファイル詳細パネルで「更新」行コマンド (**C** や **D** など) を実行できません。発行される行コマンドはすべて拒否されます。
Execute display commands (for option 1 only)	このオプションは、「**Action on command**」フィールドにオプション「**1** (Queue)」を指定する場合にのみ有効です。 このオプションを指定すると、「**Action on command**」が「**Queue**」に設定されている場合でも、**LISTUSER**、**PING**、**TRACERTE**、**RLIST** などのリスト・コマンドは実行されます。このオプションは、プログラムによってリスト・コマンドとして生成されたコマンドにのみ適用されます。ユーザー自身でコマンドを変更または追加した場合には適用されません。例えば、**FORALL** では、LISTUSER と入力した場合でもすべての種類のコマンドが通常のコマンドとして扱われます。

confirmation 設定は、zSecure Admin により生成される RACF コマンドの処理を示します。72 ページの表 6 に、「**confirmation**」オプションの設定値と説明を示します。

表 6. confirmation の設定値と説明

Confirmation	説明
1. None	RACF 変更コマンドはすべて確認してはなりません。「**None**」を選択すると検証プロンプトが使用不可になります。このオプションは zSecure Admin の使用法を理解している場合にのみ使用してください。
2. Deletes	削除コマンドのみを確認する必要があります。
3. Passwords	*読み取り可能な* RACF パスワードが含まれているコマンドは確認されません。その他のコマンドをすべて確認する必要があります。
4. All	ユーザーはすべての変更コマンドを確認する必要があります。

ヒント: 上記の設定に関係なく、必要な権限がない状態では、ここで説明する機能を使用して RACF データベースを変更することはできません。この権限の一例はグループ SPECIAL で、その目的は RACF プロファイルの変更です。

「**Command Routing**」オプションにより、生成されたコマンドの処理方法が決定します。表 7 に、使用可能な「Command Routing」のオプションを示します。

表 7. 「Command Routing」の設定値と説明

Command routing	説明
1. Ask	**Ask** は最大プロンプト・レベルです。すべてのコマンドまたはコマンド・ファイルで、ユーザーに対してコマンド・ルーティング情報の入力を求めるプロンプトが出されます。この設定は、ローカル・システムに対して生成されるコマンド、およびその他のシステムのものであると分かっているデータ・ソースから生成されるコマンドに適用されます。

表 7. 「Command Routing」の設定値と説明 (続き)

Command routing	説明
2. Normal	**Normal** は、コマンド・ルーティングのデフォルト・プロンプト・レベルです。内部生成コマンドと、常にキューに入れられるバルク・コマンドの両方が、コマンド・ルーティング・オプションの入力を求めるプロンプトを出さずに実行されます。確認プロンプトとコマンド・キューイングは、ユーザーの設定に基づいて実行されます。RACF データ・ソースがローカル・システムに適用される場合、コマンドはローカル・システムにルーティングされます。ユーザーは、ローカル・データ・ソースに対してリモート・オプション RRSFNODE、ZSECNODE、JESNODE のいずれかを指定できます。ローカル以外のデータ・ソースでは、これらのリモート標識は無視されます。ローカル・システムを対象としていないコマンドは、優先順位に基づいて次のいずれかのシステムにルーティングされます。 1. このプロファイルに使用される RACF データ・ソースに指定されている ZSECNODE または ZSECSYS。 2. このプロファイルに使用される RACF データ・ソースに関連付けられている RRSFNODE ノード。このコマンドは AT キーワードを使用し、端末ユーザーがターゲット RRSFNODE のユーザー ID に関連付けられている場合はその関連ユーザー ID、それ以外の場合は現行ユーザー ID を指定します。 3. RACF データ・ソースに指定されている NJE ノード 特定のルーティング・メカニズムが選択されており、このメカニズムが失敗する場合、別のルーティング・メカニズムに自動的にフォールバックしません。
3. Local only	このオプションを選択すると、入力ソースに関係なく、コマンドがローカル・システムにルーティングされます。ローカル・システムが RRSF 自動コマンド環境の一部である場合、RRSF 処理によってこのコマンドが他の RRSF ノードにルーティングされることがあります。

パネルの「Command generation」セクション内で「**Overtype fields in panels**」オプションを指定して zSecure Admin を実行している場合は、プロファイルの表示中に多くのフィールドを変更できます。 zSecure Admin および zSecure Audit for RACF では、変更内容に基づいて、変更に必要な RACF コマンドが自動的に生成されます。これらの変更コマンドには、前述の「Action on command」と「Confirmation」の設定も適用されます。フィールドを変更できる機能は、最も重要なユーザビリティー機能の 1 つです。この変更機能により、既存の RACF プロファイルの細かな変更を容易に実行できます。

zSecure Admin および zSecure Audit for RACF のすべてのセットアップ・パラメーターは、個人 ISPF プロファイル・データ・セットに保存されます。したがって、セットアップ・パラメーターの設定内容はユーザーによって異なります。複数のユーザー ID を使用して zSecure Admin および zSecure Audit for RACF にアクセスする場合、ユーザー ID ごとにセットアップ・パラメーターが異なることがあります。

値の変更および検証

このタスクについて

この例では、既に説明した **RA.U** 機能を使用し、**上書き**機能と検証オプションを使用して値を変更する方法を説明します。

これらのオプションを実際に使用するには、以下のステップを実行します。

手順

1. メインメニューに移動します。(必要に応じて PF3 を押します。)
2. メインメニューからオプション「**RA**」(RACF 管理) を選択します。
3. オプション「**U**」(ユーザー) を選択します。
4. **ユーザー ID** の値を入力します。複数のプロファイルを表示する場合は**デフォルト・グループ**の値 (例: SYS1) を入力します。

   下線が付いているフィールドでは値を上書きできます。例えば、プロファイルの 1 つについてパスワード・インターバルを変更するには、「**PwInt**」列に新しい値を入力します。

   ヒント: 下線が付いているフィールドがない場合は、コマンド行に **SET** と入力して Enter を押します。「**Overtype fields in panels**」オプションが選択されていること (このオプションの前に / が入力されていること) を確認します。

   この方法でフィールドに下線が表示されない場合は、次の手順で行います。

   a. 「**Command**」フィールドに **SETUP** と入力し、「セットアップ」パネルに移動します。
   b. 「セットアップ」パネルのバーから「**オプション**」を選択します。Enter を押して「**1 設定**」を選択します。
   c. バーから「**Colors**」を選択し、「**2. CUA attributes**」を選択します。
   d. すべての入力フィールド行で、「Highlight」列の値を USCORE に変更します。
   e. 照会を再発行します。

      それでもまだ下線が表示されない場合は、拡張データ・ストリーム・サポートがない端末タイプを使用している (または端末タイプをエミュレートしている) 可能性があります。
5. Enter を押します。

   zSecure Admin により、該当ユーザーのパスワード・インターバルを変更するための適切な RACF コマンドが生成され、実行する前にこのコマンドを検証するかどうか尋ねるプロンプトが出されます。

   標準 ISPF ファンクション・キーを使用して左右にスクロールし、詳細情報を確認するには **S** (選択) 行コマンドを実行してください。
6. PF3 を押して RACF コマンドを拒否する (実行しない) か、または Enter を押して RACF コマンドを実行依頼します。

コマンドを実行依頼する場合、zSecure Admin for RACF では、TSO コマンド行でコマンドを入力する場合と同様にコマンドが実行依頼されます。RACF によりコマンドが受け入れられるためには、適切な権限 (例えば、SPECIAL または所有権) が付与されている必要があります。適切な権限が付与されていない場合、RACF 違反エラー・メッセージが返されます。

プロファイルのインストール・データ・フィールドの値を上書きできます。これにより、変更したい文字のみを変更できます。あるいは、**MI** (ユーザー ID 情報管理) 行コマンドを実行して、フィールド全体を編集することもできます。また、インストール・データ内のユーザー定義フィールドを編集することもできます。

一般的なタスク用の行コマンド

プロファイルを表示している場合、行コマンドを発行できます。行コマンドを発行するには、表示されているプロファイル行の先頭文字位置に 1 つの文字を入力して Enter を押します。

最もよく使用される機能を以下に示します。

C コピー

D 削除

L リスト

S 選択

行コマンドを発行すると、zSecure Admin および zSecure Audit for RACF により、必要な機能を実行する適切な RACF コマンドが生成されます。一般的な手法としては、**Copy** 行コマンドを使用してプロファイルを再作成します。その後、新規プロファイル内で変更するフィールドの値を上書きします。

L 行コマンドは、**L** の実行対象プロファイルの 1 次 RACF データベース内で、RACF のリスト・コマンドを実行します。このコマンドは詳細表示でも使用できます。

注: L 行コマンドを実行すると、常に 1 次 RACF データベースから報告されます。

プロファイル概要表示で使用可能な行コマンドのリストを表示するには、**/** 行コマンドを入力します。**RA.U** 機能では、アプリケーション行コマンドをすべて表示するにはスクロールダウン (PF8) する必要があります。

第 6 章 レポートの作成および表示

このタスクについて

このタスクでは、レポートを生成して結果を表示するための基本的な手順を説明します。この例では、指定したユーザー ID の有効範囲を調べるためのレポートを生成します。

手順

1. IBM Security zSecure Admin and Audit for RACF メインメニューから、以下のステップを実行します。
   a. オプション「**RA**」(RACF 管理) を選択します。
   b. オプション **3** (レポート) を選択します。 次のパネルで、事前定義レポートを 1 つ選択できます。
   c. オプション **4** (許可/有効範囲) を選択します。
2. 「レポート」パネルで、指定したユーザーの有効範囲を示すレポートを作成します。
   a. ユーザー ID を入力します。この演習では、どのユーザー ID を入力しても構いません。
   b. 「**3**」を指定します (許可のタイプは「範囲」-「アクセス権限」または任意の管理権限です)。
   c. 画面の「**出力オプションの指定**」セクションの「**印刷形式での出力**」の前に **/** を入力し、Enter を押します。
   d. 次のパネルで Enter を押します。 このパネルでは、入力したグループまたはユーザーが特定のリソースにアクセスするための方法の中から一部を除外できます。ただしこの評価においては、どのオプションも除外しないでください。グループまたはユーザーがリソースにアクセスするために使用できる、すべての方法を調べてください。

タスクの結果

zSecure Admin and Audit for RACF は、RACF データを検索します。レポート結果が概要パネルに表示されます。このパネルには、指定されたユーザー ID に対するクラスとアクセス権限の範囲がリストされます。 78 ページの図 63 に、選択したクラスに関する詳細情報を示します。

```
 BROWSE - IBMUSER.C2R10FE.REPORT ——-------------- LINE 0000 0.8 s CPU, RC=0
 COMMAND ===> _____________________________________________ SCROLL ===> PAGE
******************************** Top of Data ***********************************
U S E R   A U T H O R I Z A T I O N   F O R   I D  IBMUSER  IBM DEFAULT USER

Class    Type    Profile name                                    Volume Access  Via
ACCTNUM  GENERIC **                                                    ALTER   IBM
APPCTP   GENERIC **                                                    READ    - U
CONSOLE          SDSF                                                  ALTER   - W
DATASET  GLOBAL  &RACUID*.**                                           ALTER   - U
DATASET  GENERIC ANF.*.**                                              READ    - U
DATASET  GENERIC ANF.SANFLOAD                                          READ    - U
DATASET  GENERIC AOP.*.**                                              READ    - U
DATASET  GENERIC API.*.**                                              READ    - U
DATASET  GENERIC ASM.*.**                                              READ    - U
DATASET  GENERIC ASM.SASMMOD1                                          READ    - U
DATASET  GENERIC ASM.SASMMOD2                                          READ    - U
DATASET  GENERIC ASM.SASMSAM1                                          READ    - U
DATASET  GENERIC ASMA.*.**                                             READ    - U
DATASET  GENERIC ASMA.V1R2M0.SASMMOD1                                  READ    - U
DATASET  GENERIC ASMA.V1R3M0.SASMMOD1                                  READ    - U
DATASET  GENERIC ASMA.V1R3M0.SASMSAM1                                  READ    - U
DATASET  GENERIC ASMT.*.**                                             READ    - U
DATASET  GENERIC ASMT.V1R2M0.SASMMOD2                                  READ    - U
```

図 63. SCOPE レポート

レポートを確認したら、PF3 を押すと「結果」パネルが生成されます。結果パネルはすべてのレポートに対して生成されます。 79 ページの図 64を参照してください。

ヒント: ユーザー ID またはグループ接続によってユーザーに付与されたアクセス権限のみを表示する有効範囲レポートを作成するには、オプション **2** (Direct permit or Connect (Id or Connect Group on access list)) を選択してください。

「結果」パネル

多数の照会または機能が実行された後、「結果」パネルが表示されます。このパネルの操作に慣れてください。このパネルを使用すると、さまざまな方法で結果を確認し、機能から有用な情報を保存できます。有用な情報には、最後の機能の処理中に zSecure Admin および zSecure Audit for RACF により生成される RACF コマンドなどがあります。

レポートは、毎回同じファイルを上書きします。つまり、SYSPRINT、REPORT、および CKRCMD のようなファイルは、1 次モジュールが呼び出されるたびに再書き込みされます。別の照会または機能を開始する前に、「結果」パネルで **W** 行コマンドを使用して重要な結果を保存します。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
               zSecure Admin+Audit for RACF - Results
Command ===> ____________________________________________________________

The following selections are supported:
 B Browse file                S Default action (for each file)
 E Edit file                  R Run commands
 P Print file                 J Submit Job to execute commands
 V View file                  M E-mail report
 W Write file into seq. or partitioned data set

Enter a selection in front of a highlighted line below:
_  SYSPRINT  messages
_  REPORT    printable reports
_  CKRTSPRT  output from the last TSO command(s)
_  CKRCMD    queued TSO commands
_  CKR2PASS  queued commands for IBM Security zSecure Admin
_  COMMANDS  zSecure Admin input commands from last query
_  SPFLIST   printable output from PRT primary command
_  OPTIONS   set print options
```

図 64. 「結果」パネル

表示上のファイルのうちいくつかのファイル名が強調表示されます。これは、最後の操作によりこれらのファイルにデータが生成されたことを示します。該当する場合は、「結果」パネルの最上部にあるコマンドの 1 つを使用して、これらのうちの任意のファイルを参照、編集、保存、実行、または実行依頼できます。

ヒント: ほとんどのパネルでは、コマンド行で **RESULTS** 基本コマンドを使用すると、最新の「結果」パネルを取得できます。

DISPLAY 結果を印刷するには、**PRT** コマンドを使用します。

レポート出力のアーカイブ

このタスクについて

存在しないデータ・セット名を指定すると、割り振りパラメーターを入力するためのプロンプトが zSecure Admin and Audit から出されます。

手順

1. 「結果」パネルで、**REPORT** キーワードの前に **W** と入力します。アーカイブ・データ・セットのデータ・セット名を指定するためのパネルが開きます。

```
   Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
         zSecure Admin+Audit for RACF - Results of last query
Command ===> ____________________________________________________________

Write the zSecure Admin+Audit for RACF report file to the following dataset:
Data set name . . . . . ____________________________________________
Member  . . . . . ________
Disposition . . . . . _________  (Append, Overwrite, or Generate)

Processing option after Write completed:
Go into Edit  . . . . . N__        (Yes/No)
```

図 65. データ・セットへの出力のアーカイブ

2. 順次データ・セットまたは区分データ・セットの作成に必要なパラメーターを指定します。
   a. 順次データ・セットでは、コンテンツを上書き入力 (処理「**Overwrite**」を選択) するか、または現行コンテンツの終わりに追加 (処理「**Append**」を選択) することができます。
   b. 区分データ・セットでは、メンバー名と処理 (「**Overwrite**」または「**Append**」) を指定するか、または処理「**Generate**」を選択してメンバー名をブランクのままにします。「**Generate**」では、各レポートに固有のメンバー名が割り当てられるため、メンバー名を選択する必要はありません。
3. Enter を押してデータ・セットを作成します。
4. PF3 を押して「結果」パネルを終了します。

検索の実行後には常に「結果」パネルが存在します。ただし、このパネルが自動的に表示されるのは、SYSPRINT 以外のファイルに出力が含まれている場合のみです。

ヒント: 次に実行する機能により、この結果データ・セットは上書きされます。データ・セットを保存する必要がある場合は、次の検索の実行前に保存してください。

レポート出力のメール送信

このタスクについて

「メール」オプションは、出力定義をセットアップするパネル (**SE.7**) で SMTP 構成オプションを指定した場合にのみ有効です。 70 ページの『E メール出力の SMTP オプション』を参照してください。SMTP ルーティング・パラメーターが定義されていない場合は、E メールの送信を試行しないでください。

手順

1. 「結果」パネルで、**REPORT** キーワードの前に `M` と入力します。 81 ページの図 66 が開きます。

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                                    zSecure Admin+Audit for RACF - E-mail
Command ===> ____________________________________________________________

Specify e-mail data
From  . . . . &jobname at &system <mbox@domain>_____________________________
Mail to . . . ____________________________________________________________
CC  . . . . . ____________________________________________________________
BCC . . . . . ____________________________________________________________
Reply to  . . ____________________________________________________________
Output format 1  1. Normal (MIME/HTML)
                 2. Plain text (formatting may be lost)
                 3. Attachment
Font size . . _
Subject . . . ____________________________________________________________

Additional data (e.g. signature)
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
```

図 66. E メール指定パネル

2. E メールの受信者、および追加のフォーマット設定や注記を指定します。
3. Enter を押して、E メールを送信します。

第 7 章 「検査」の機能

「検査」機能を使用すると、RACF および z/OS の保全性およびセキュリティー・データを分析できます。

例えば、多くの機能では、RACF データを、ディスク上に実際に存在するデータ (zSecure Collect for z/OS によって読み取られるデータ) と比較します。また、ほとんどの機能では分析中に検出された問題を訂正する RACF コマンドが自動的に生成されます。これらのコマンドは、自動的には実行されません。ユーザーが確認または使用できるように提示されるだけです。

初めて「検査」機能を使用する場合、特に DASD および RACF のクリーンアップ・ポリシーが厳格でない大規模なインストール済み環境においては、予想よりも多い出力を受け取ることがあります。デフォルトではディスク・ボリュームあたりのメッセージ数は 50 に制限されていますが、下位レベルのパネルでこの制限をオーバーライドすることもできます。製品メッセージは簡潔かつ正確ですが、理解するまでに多少知識の習得が必要となることがあります。また、ご使用のインストール環境で、「検査」のすべての機能により報告されるすべての 異常が訂正されなければならないとは*想定しない*でください。例えば、ご使用のインストール環境が一部のレポートの暗黙的なセキュリティー・ポリシーとは合致しない場合があります。この情報は必要に応じて使用し、**無条件で受け入れないようにしてください。**

「検査」機能が完了すると、その結果が「結果」パネルに表示されます。通常、RACF コマンドが生成された場合は、これらのコマンドが最初に表示されます。場合によっては、「検査」機能の完了直後に SYSPRINT 出力が表示されることがあります。

SYSPRINT ファイルには、「検査」機能による分析中に検出された問題に関する詳細情報 (分析中に検出された異常および問題に関する簡潔な説明など) が含まれます。コマンド行にコマンド **find 'v e r i f y'** を入力すると、SYSPRINT ファイルの「M E S S A G E S V E R I F Y」セクションに直接移動します。文字と区切り文字である単一引用符との間にスペースが 1 つ必要です。

- 『検査機能の実行』
- 86 ページの『検査機能の初めての実行』

検査機能の実行

このタスクについて

検査機能を実行する前に、『第 7 章 「検査」の機能』で説明している検査機能の概要を参照してください。

検査機能を初めて実行する場合は、86 ページの『検査機能の初めての実行』の手順に従ってサンプルを段階的に実行してください。

手順

検査機能を表示および選択するには、次の手順で行います。

1. メインメニューからオプション「**AU**」(監査) を選択します。
2. オプション「**V**」(検査) を選択します。図 67 に示す「検査」選択パネルが開きます。

```
   Menu  Options  Info  Commands  Setup          StartPanel
------------------------------------------------------------------------------
        zSecure Admin+Audit for RACF - Audit - Verify
Command ===> ____________________________________________________________

Enter "/" to select one or more options
_  Permit            Find undefined users and groups and their profiles
_  User permit       Find and remove redundant permits to userids
_  Connect           Compare USER, GROUP and CONNECT profiles
_  PADS              Programs on conditional access list have PROGRAM profile
_  Group tree        Loops in grouptree
_  Password          Userids with trivial passwords (not from an unloaded db)
_  Protect all       All datasets are protected by a (discr or gen) profile
_  On volume         Datasets defined by discrete profiles actually exist
_  Not empty         Generic profile has matching disk or tape datasets
_  All not empty     As above, even 'outer' generic profiles
_  Indicated         Discrete profile exists for RACF-indicated datasets
_  Program           Datasets as members in PROGRAM profile exist on disk
_  Pgm exists        PROGRAM profiles cover actual load modules
_  Started task      Check that procedures can indeed be started, etc.
_  TSO all RACF      All TSO users should have RACF password and TSO segment
_  Sensitive         Sensitive datasets not protected properly
```

図 67. 「検査」選択パネル

実行する検査機能は 1 つ以上選択できますが、一度に 3 つを超える機能を選択する操作は一般的ではありません。検査機能を使用する前に、表 8 および 85 ページの表 9 に示す機能の説明を確認してください。

表 8. 「検査」の機能

機能	説明
Permit	RACF アクセス制御リストまたは所有者フィールドで使用されており、現在有効な ID として定義されていないすべての ID (ユーザーまたはグループ) を報告します。新規ユーザーに対してこのような無効な ID が定義されて再度有効にされると、この新規ユーザーは、このユーザー ID の以前の所有者の権限を直ちにすべて継承します。これは、重大な機密漏れになる可能性があります。さらに重大な機密漏れは、グループ SPECIAL 権限または JOIN 権限が付与されているすべてのユーザーは、アクセス制御リストにこの ID と同じ名前のグループを作成し、この ID の権限を取得できてしまうことです。
User Permit	アクセス制御リストのユーザー ID が含まれており、このユーザーが、同じアクセス制御リスト内にある 1 つ以上のグループにも接続されているリソース・プロファイルをすべて報告します。ユーザー ID とグループの両方のアクセス・レベルが比較されます。その特定のユーザー ID のアクセス権限が、すべての接続グループの最上位アクセス権限と同等の場合、このユーザー ID エントリーは重複となり、削除対象となります。
Connect	ユーザー・プロファイルとグループ・プロファイルの接続情報に一貫性があることを確認します。

表 8. 「検査」の機能 (続き)

機能	説明
PADS	RACF 条件付きアクセス制御リストに含まれるすべてのプログラムに、対応する Program プロファイルがあることが確認されます。 PADS 管理はしばしば複雑な場合がありますが、「検査」のさまざまな機能がこれに対処します。
Group tree	グループ定義内のループを検出します。これらのループは、通常、RACF 管理が集中化されていない場合、または管理者が頻繁に変更される場合に発生します。 RACF では、**ALU** コマンドまたは **ALG** コマンドによりループが発生するかどうかを検査することで、ループの発生が防止されます。
Password	RACF データベースのすべてのユーザー・パスワードを、いくつかの単純な値を使用して検査します。パスワードはアンロードされないため、Unload ファイルに対して「パスワード」機能を実行することはできません。

CKFREEZE データ・セットを必要とする「検査」機能を表 9 に示します。

表 9. CKFREEZE データ・セットを必要とする検査機能

機能	説明
Protect all	総称または個別の RACF プロファイルで保護されていないすべてのディスク・データ・セットをリストします。ご使用のインストール済み環境で RACF PROTECT ALL 環境が使用されている場合は、この機能を試してみてください。PROTECT ALL 環境ではない場合は、大量のデータが出力される状況に備えてください。
On Volume	個々の個別 RACF プロファイルに対応するデータ・セットが DASD 上にあることを検証します。データ・セットの削除後、長期にわたって古い個別プロファイルが RACF に残ることがよくあります。
Not empty	古い総称プロファイルを特定します。この機能は、より汎用的な総称プロファイルのサブセットを保護する総称データ・セット・プロファイルのもとで、既存のデータ・セットが総称プロファイルによって保護されているかどうか検査します。(この機能を使用するときには注意してください。検査が行われる時点では、今後の割り振りおよび定期的な割り振りを保護するためのプロファイルが空 である (プロファイルにデータ・セットがない) 場合があります。)
All not empty	この機能は、「**Not empty**」検査のより一般的な検査です。実際のデータ・セットを保護するためにすべての総称プロファイルが使用されていることを検証します。この機能を使用して、不要な総称プロファイルを検出できます。RACF および z/OS には、総称プロファイルを自動的に除去するメカニズムがないため、時間の経過に伴い不要なプロファイルが多数蓄積する可能性があります。
Indicated	DSCB またはカタログで RACF 標識ビットが設定されているすべての RACF データ・セットに、対応する個別プロファイルがあることを検証します。
Program	Program プロファイルのメンバーとしてリストされている各データ・セットが存在することを検証します。

表 9. *CKFREEZE* データ・セットを必要とする検査機能 *(続き)*

機能	説明
Pgm exists	各 Program プロファイルが、プロファイルに指定されたとおりに、データ・セット内のロード・モジュールを少なくとも 1 つカバーしていることを検証します。ライブラリー間でモジュールを移動する場合、RACF Program プロファイルは自動的に更新されず、モジュールは保護されなくなります。「**プログラム**」および「プログラムが存在」機能により、クリーンな PADS 環境を維持できます。
Started task	始動プロシージャー・テーブル (ICHRIN03) と、各種 RACF ユーザー、グループ、および STARTED クラス・プロファイルの定義との整合性、および JES2 と MSTR に対して定義されているプロシージャー・メンバーとの整合性を検査します。 「**TSO all RACF**」および「**Sensitive**」は、zSecure Audit でのみ使用可能です。
TSO all RACF	SYS1.UADS データ・セットで RACF のユーザー定義を使用して定義されているユーザーを調べ、RACF の制御をバイパスしてログオンできるすべての UADS ID を報告します。
Sensitive	z/OS 機密データ・セットの保護をベースライン・ポリシーに突き合わせて検査します。保護が十分ではない場合には、正しいプロファイルを追加することによって、または問題のプロファイルを修正または改善することによって、この状況を修正する RACF コマンドが生成されます。

「検査」の一部の機能は、他の機能よりも重要です。PROTECT ALL 環境でない場合は、「**Permit**」機能と「**Protect All**」機能が最も重要になることが考えられます。

検査機能の初めての実行

手順

1. 検査パネルの「**標識付き**」行に / を入力して Enter を押します。 図 68 に示す CKRCMD コマンド・ファイルが自動的に開きます。

```
 File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       IBMUSER.C2R10FE.CKRCMD                        Columns 00001 00072
Command ===> _____________________________________________ Scroll ===> CSR_
Press PF3, Enter R at the cursor location, press ENTER to run these commands
000001         /* CKRCMD file CKR1CMD complex YESTERDY NJE JES2TEST generated
000002          /* Commands generated by VERIFY INDICATED  */
000003         addsd 'IBMUSER.DISCRETE.DSN1' vol(TSTUS1) unit(3390) noset from(
000004         deldsd 'IBMUSER.DISCRETE.DSN1' vol(TSTUS1)
000005         addsd 'IBMUSER.DISCRETE.DSN2' vol(TSTUS1) unit(3390) noset from(
000006         deldsd 'IBMUSER.DISCRETE.DSN2' vol(TSTUS1)
****** **************************** Bottom of Data ****************************
```

図 68. 標識付き CKRCMD ファイルの検証

この例では、インストール済み環境に含まれている 2 つのデータ・セットは RACF 標識付きですが、対応する個別データ・セット・プロファイルが RACF

データベースにありません。必要に応じて、ISPF 機能 PF7、PF8、PF10、および PF11 を使用してパネルをスクロールします。これによりすべてのデータを確認できます。

生成されたコマンドを実行して、「Verify Indicated」機能により検出された矛盾を修正できます。

2. PF3 を押すと、「結果」パネルが開きます。
3. 「検査」の機能の詳細を表示するには、SYSPRINT ファイルを選択します。 図 69 に示すように、「MESSAGES VERIFY INDICATED」というヘッダーが付いたセクションに追加情報が表示されます。
4. 複数のパネルをスクロールダウンする代わりに、コマンド行に `find 'v e r i f y'` と入力し、SYSPRINT ファイルのメッセージ・セクションにジャンプします。あるいは、ファイルの終わりまでスクロールしてから、1 ページまたは 2 ページ上にスクロールすることもできます。 図 69 に、MESSAGES VERIFY INDICATE セクションの例を示します。

```
M E S S A G E S   V E R I F Y   I N D I C A T E D      EEND  2 Jun 2015 06:00    page   12

CKR0040 04 RACF indicator set but no discrete profile found for DEMOU1 CRXAR.DISCR.DATASET
CKR0040 04 RACF indicator set but no discrete profile found for DEMOU1 CRXART.DISCR.DATASET
```

図 69. SYSPRINT ファイルの MESSAGES VERIFY INDICATE セクションの例

注: SYSPRINT ファイルには、VERIFY メッセージに関する詳細情報が含まれています。

5. 「検査」選択パネルに戻るには、PF3 を 2 回押します。
6. 「**許可**」行に / を入力します。
7. 「**標識付き**」行から / を削除します。zSecure Admin および zSecure Audit for RACF が機能を実行するまで、表示されるパネルを 1 つずつ操作します。

エラーのないデータベースを維持していない限り、zSecure Admin and Audit for RACF によってデータベース内に無効なユーザー ID が検出されることが考えられます。無効なユーザー ID が多数検出される場合は、レポートを印刷してオフラインでこのレポートを調べることができます。無効なユーザー ID が存在している場合、その場で簡単には修復できない複雑な問題が存在している可能性があります。

ヒント: RACF コマンドがいずれかの検査機能によって生成される場合、zSecure Admin and Audit for RACF によって提示される解決法が適切ではなかったり、ご使用の環境に合わせてこの解決法を調整する必要が生じたりする可能性があります。常にコマンドを注意して確認してください。必要に応じて、実行前に SYSPRINT ファイルで詳細情報を確認してください。

第 8 章 システムの保全性とセキュリティーの監査

現行 RACF システム・オプションでレポートを表示するには、以下のガイドラインおよびタスクの手順に従ってください。

このタスクについて

AU.S 機能を使用して現行 SETROPTS 設定を表示できます。1 次メニューの **AU.S** オプションから、z/OS の一連の保全性およびセキュリティー検査が使用できます。例えば、この機能を使用して現在の SETROPTS 設定を表示できます。

手順

AU.S 機能を使用するには、以下のステップを実行します。

1. メインメニューからオプション「**AU**」(監査) を選択します。
2. オプション **S** (状況) を選択して「監査 - 状況」パネルを開きます。

   このパネルを使用して、1 つから 5 つまでのレポート・カテゴリーを選択できます。最初に、「**RACF 制御**」 (RACF 指向テーブル) カテゴリーを検討します。

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                      zSecure Admin+Audit for RACF - Audit - Status
Command ===> ____________________________________________________________

Enter / to select report categories
_  MVS tables           MVS oriented tables (reads first part of CKFREEZE)
_  MVS extended         MVS oriented tables (reads whole CKFREEZE)
/  RACF control         RACF oriented tables
_  RACF user            User oriented RACF tables and reports
_  RACF resource        Resource oriented RACF tables and reports

Select options for reports:                                  Audit policy
/  Select specific reports from selected categories          /  zSecure
_   Include audit concern overview in overall prio order     _  C1
_   Only show reports that may contain audit concerns        _  C2
__  Minimum audit priority for audit concerns (1-99)        _  B1
_   Print format              _  Concise (short) report
_   Show differences
_  Background run
```

図 70. 監査 - 状況

3. カテゴリー「**RACF 制御**」を選択し、「**選択したカテゴリーから特定のレポートを選択**」の前に / を入力します。Enter を押します。

   注: 監査ポリシーを設定できます。C1、C2、および B1 ポリシーは、米国国防総省によって「オレンジ・ブック」として知られている資料に記載されているセキュリティー標準です。デフォルト・ポリシーは、ほとんどの企業に適用できる実用的かつ達成可能なセキュリティー・レベルである標準です。ポリシーでは、公開として分類される対象を定義します。

4. このインストール済み環境の現行 RACF システム・オプションのレポートを生成するには、レポート **SETROPTS** を選択します。また、クラス記述子テーブルおよびプロファイル数のレポートを作成するには、**RACFCLAS** を選択します。
5. Enter を押して、要求したレポートを生成します。

   図 71 に示すパネルが開き、レポートを選択および表示できるようになります。

```
                zSecure Admin+Audit for RACF Display   1 s elapsed, 0.6 s CPU
Command ===> ____________________________________________________ Scroll===> CSR_

  Name     Summary Records Title
_ SETROPTS       1       1 RACF system, ICHSECOP, and general SETROPTS settings
_ SETROPAU       1       3 SETROPTS settings - audit concerns
_ RACFCLAS       1     168 RACF CDT, SETROPTS class info and number of profiles
****************************** BOTTOM OF DATA ********************************
```

図 71. 監査レポートの概要

6. **SETROPTS** レポートを選択します。次に、Enter を押すと、図 72 に示す SETROPTS 設定パネルが開きます。

```
RACF system, ICHSECOP, and general SETROPTS settings              Line 1 of 58
Command ===> ____________________________________________________ Scroll===> CSR_
                                          8 Apr 2005 08:46
   Complex  System   Collect timestamp
   DEMO     DEMO      8 Apr 2005 00:50

General RACF properties                 Data set protection options
Access Control active          Yes      Prevent duplicate datasets    No
Force storage below 16M        No       Protectall                    Yes/fail
Check all connects  GRPLIST    Yes      Automatic Dataset Protect     No
Check genericowner for create  Yes      Enhanced Generic Naming       Yes
NOADDCREATOR is active         Yes      Prefix one-level dsns         ONEQUAL
Dynamic CDT active             No       Prevent uncataloged dsns      No
RACF local node                DEMO     GDG modelling                 No
RRSF propagate RACF commands   No       USER modelling                No
RRSF propagate applications    No       GROUP modelling               No
RRSF propagate passwords       No
RRSF honour RACLINK PWSYNC     Yes
Application ID mapping stage   0
Level of KERB processing
Primary Language               ENU
Secondary Language             ENU
RACF software release level    HRF7703 HRF7703
RACF DB template level         HRF7703
```

図 72. 監査 - 状況 SETROPTS レポート

   現行の SETROPTS (**=SET RACF** オプション) がこのレポートにリストされます。PF8 を使用してスクロールダウンし、システム全体の監査設定およびパスワード規則などの現在アクティブな他の SETROPTS パラメーターを表示できます。
7. PF3 を押してレポートの概要に戻ります。
8. **SETROPAU** を選択すると、 91 ページの図 73 に示すレポートが開きます。

   このレポートには、現行の SETROPTS 設定に関連した監査に関する考慮事項がリストされます。監査に関する考慮事項は、現行のインストールで起こりうる機密漏れの兆候を示します。

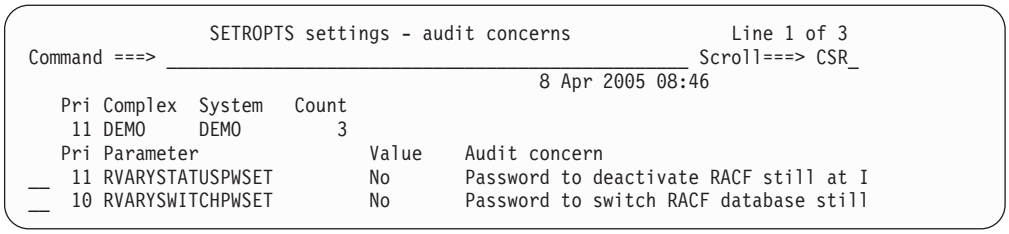


図 73. SETROPTS 監査に関する考慮事項の概要

zSecure Audit for RACF では、検出された問題の重大度をランク付けします。これらの問題は「**Pri**」フィールドにあり、0 から 255 までの範囲内の数値です。ただし、これらのランキングの理由を理解するには、z/OS の内部に関する一部の知識と、システム全体のコンテキストの判断が必要です。表 10 に、監査に関する考慮事項の優先順位の大まかなカテゴリーを示します。

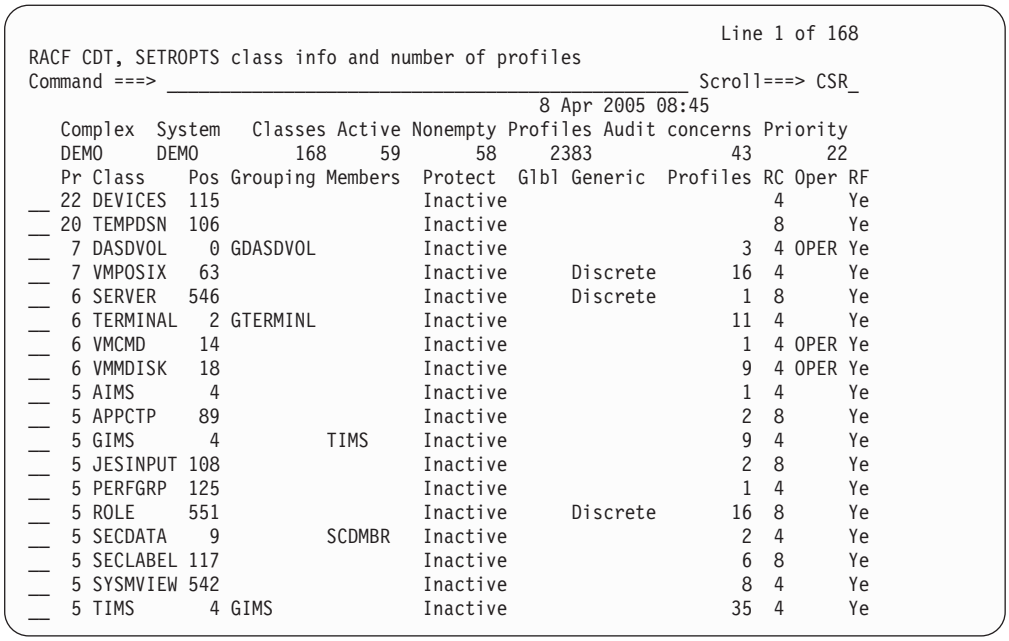
表 10. 監査に関する考慮事項の優先順位カテゴリー

優先度	**タイプ**	**説明および必要なアクション**
40-255	機密漏れ	重大な機密漏れが生じている可能性があり、監査員の注意を必要とします。即時アクションが必要です。
20-39	問題	重大なセキュリティー脅威。アクションは必要ですが、緊急性は低くなります。
11-19	ハウスキーピング	軽微な問題や、監査、検討、および承認あるいは否認が必要な権限。RACF のハウスキーピングでは、このような考慮事項の多くを削除できます。
1-10	監視	懸念事項を読み、時間があるときに解決します。
0	OK	監査問題はありません。

デフォルトでは、監査に関する考慮事項は優先順位が降順になるようにソートされます。監査に関する考慮事項の詳細は、表示する考慮事項の前に S または / を入力して表示できます。監査問題を表示するには、以下のステップを実行します。

a. PF3 を再び押して、レポートの概要に戻ります。
b. レポート **RACFCLAS** を選択して Enter を押し、 92 ページの図 74 に示す 監査 - 状況 RACFCLAS レポートが開きます。

   このレポートには、RACF クラス記述子テーブルの内容が表示されます。RACF に対して定義されたすべてのクラスについてのレコードが表示されます。



```
                                                                  Line 1 of 168
RACF CDT, SETROPTS class info and number of profiles
Command ===> _____________________________________________ Scroll===> CSR_
                                        8 Apr 2005 08:45
   Complex  System   Classes Active Nonempty Profiles Audit concerns Priority
   DEMO     DEMO         168     59       58     2383            43       22
   Pr Class    Pos Grouping Members  Protect  Glbl Generic  Profiles RC Oper RF
__ 22 DEVICES  115                   Inactive                      4      Ye
__ 20 TEMPDSN  106                   Inactive                      8      Ye
__  7 DASDVOL    0 GDASDVOL          Inactive                      3  4 OPER Ye
__  7 VMPOSIX   63                   Inactive      Discrete       16  4      Ye
__  6 SERVER   546                   Inactive      Discrete        1  8      Ye
__  6 TERMINAL   2 GTERMINL          Inactive                     11  4      Ye
__  6 VMCMD     14                   Inactive                      1  4 OPER Ye
__  6 VMMDISK   18                   Inactive                      9  4 OPER Ye
__  5 AIMS       4                   Inactive                      1  4      Ye
__  5 APPCTP    89                   Inactive                      2  8      Ye
__  5 GIMS       4          TIMS     Inactive                      9  4      Ye
__  5 JESINPUT 108                   Inactive                      2  8      Ye
__  5 PERFGRP  125                   Inactive                      1  4      Ye
__  5 ROLE     551                   Inactive      Discrete       16  8      Ye
__  5 SECDATA    9          SCDMBR   Inactive                      2  4      Ye
__  5 SECLABEL 117                   Inactive                      6  8      Ye
__  5 SYSMVIEW 542                   Inactive                      8  4      Ye
__  5 TIMS       4 GIMS              Inactive                     35  4      Ye
```

図 74. 監査 - 状況 RACFCLAS レポート

このレポートでは、クラスは監査に関する考慮事項の優先順位が降順になるようにソートされます。ただし、この概要は、目的の任意の列でソートできます。**sort pos** コマンドを入力すると、この概要は **posit** 番号に従って再配列されます。一方、**sort class** コマンドを入力すると、クラスはクラス名でアルファベット順にソートされます。

ヒント: ヘルプ・パネルには、背景情報および説明が提供されています。

第 9 章 ルール・ベースの準拠性評価

組織のセキュリティーのニーズに合わせて zSecure Audit Compliance Testing Framework をカスタマイズする方法を理解するには、以下のガイドラインに従ってください。

AU.R は、zSecure Audit Compliance Testing Framework のユーザー・インターフェースです。このフレームワークは、新しい外部標準だけでなく、サイト標準の準拠性検査の自動化を支援して、他のセキュリティー・タスクのために時間を節約できるようにするために導入されました。標準はカスタマイズすることができます。

ルール・ベースの準拠性評価を使用するには、適切なメンバーを使用して CKACUST データ・セットを作成し、どのユーザーまたはグループがどのタスクに対して準拠しているのかを定義しておく必要があります。以下に、サンプルの準拠ユーザー・メンバーを示します。

```
EDIT       CRMASCH.MY.CKACUST(SYSPAUDT) - 01.00            Columns 00001 00072
Command ===>                                                  Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001 * Systems Programmers or Systems Administrators *
000002 SYS1
000003 SYSPROG
****** **************************** Bottom of Data ****************************
```

図 75. サンプルの準拠ユーザー・メンバー

CKACUST には、さまざまなカスタマイズのメンバーも含めることができます。例えば、CLASSIFY メンバーは PCI-DSS 標準に依存するデータを保護するために使用される SIMULATE SENSITIVE ステートメントのリストを含みます。

デフォルトでは、製品の開始に使用される zSecure 構成で指定されている CKACUST データ・セットが使用されます。CO.1 にある CKACUST データ・セットを指定し、デフォルトをオーバーライドすることもできます。なお、データ・セットの連結が使用されるため、実際のオーバーライドを持つメンバーのみを作成する必要があります。zSecure 構成に CKACUST データ・セットがない場合は、SCKRSAMP メンバー CKAZCUST を使用して、メンバーの「空」のセットを作成できます。エラー・メッセージを防止するには、すべてのメンバー・セットが必要です。CKACUST データ・セットの作成については、「*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。

CARLa DEFTYPES は、準拠した母集団を示す CKACUST メンバー内の ID を検索するために使用されます。

標準は、事実上、事前定義された準拠性ルール・セットです。自動化された検査のために zSecure Audit に定義されている標準は、通常、より幅広い標準の一部になっています。この幅広い標準には、検査を自動化できない組織規則も含まれています。

標準は、CARLa ステートメント STANDARD を使用して定義します。サイト・ルールを追加する場合は、CARLa コマンド言語の高度な知識が必要です。各個別ルール・セット (= 外部標準ルール) について SCKRCARL ライブラリー内の別個のメンバーで、組み込みの標準検査が用意されています。これらのメンバーには、以下の命名規則があります。

- CKAG* メンバーは RACF STIG ルールです。
- C2AG* メンバーは ACF2 STIG ルールです。
- CKTG* メンバーは Top Secret STIG ルールです。
- CKAO* メンバーは GSD331 ルールです。
- CKAP* メンバーは RACF PCI-DSS ルールです。
- C2AP* メンバーは ACF2 PCI-DSS ルールです。

レポート作成

ルール・ベースの準拠性監査レポートを生成するには、以下のガイドラインおよびタスクの手順に従ってください。

このタスクについて

同時に複数の標準および複合システムについてレポートすることができます。大規模なシステムを分析する場合、並行分析の量は、TSO ユーザー ID が使用可能なメモリーの量 (REGION セッション・パラメーター) によって制限される可能性があります。

手順

1. メインメニューの「オプション」行に AU.R (監査 - ルール・ベースの準拠性評価) と入力し、**Enter** を押します。 以下の監査の準拠性のメニューが表示されます。

```
 Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Audit - Compliance
Command ===> ____________________________________________________________________

Action
_  1. Run evaluation below  2. Select rules for ESM     3. Customization

Compliance evaluation (action 1)
/  STIG (subset)
_  STIGplus (subset)
_  GSD (subset)
_  PCI-DSS (subset)
_  Other standard member                  ________
_  Test a single rule (set) member        ________  RACF   (RACF/ACF2/NONE)

Compliance result selection
_  Compliant          _  Non-compliant    _  Undecided

Output/run options
   Print format       _  Send as e-mail
   _  Background run  _  Include test details  _  Narrow print
```

図 76. 監査の準拠性のメニュー

2. 実行するアクションを「**Action**」セクションで選択します。

A **Select rules for ESM**
A 出荷時の準拠性評価から独自の規則サブセットを定義します。「*IBM*
A *Security zSecure Admin and Audit for RACF* ユーザー・リファレンス・
A マニュアル」の出荷時の準拠性評価からの独自の規則サブセットの定義
A に関するセクションを参照してください。

A **Run evaluation below**
A パネルの上半分で選択された準拠性評価を実行します。これはデフォル
A トです。

A **Customization**
A カスタマイズ・メンバーおよび集団メンバーを編集/表示します。これ
A は、ユーザー CKACUST ライブラリーとサイト CKACUST ライブラリ
A ーの連結表示です。

3. 「**Compliance evaluation**」セクションで、検査基準とする標準を選択します。

   STIG および **GSD** の選択項目は、以下の標準の事前定義のサブセットを指します。

   STIG US Defence Information Systems Agency 発行の『Security Technical Implementation Guide』(DISA-STIG)

   STIGplus
   STIGplus の主な目的は、STIG コントロールと同様のコントロールを実装することです。ただし、このコントロールは別のソフトウェア製品用です。例えば STIGplus コントロールを使用する目的は、磁気テープ管理です。

   GSD アウトソーシングでよく使用される IBM 標準 (GSD331)

   PCI-DSS
   Payment Card Industry Data Security Standard。

A 「**Other standard member**」選択項目は、独自のシステム定義標準、あるいは古
A いバージョンの STIG、GSD、または PCI-DSS に対する準拠性検査を実行する
A ために使用できます。表示されたフィールドに STANDARD ステートメントが
A 含まれているメンバー名を指定します。

「**Test a single rule**」選択項目は、サイト標準の開発時におけるテストを支援す
5 るために用意されています。zSecure で使用可能なコントロールのリストについ
5 ては、『IBM Security zSecure Audit controls』を参照してください。指定された
メンバーが、CKRCARLA ライブラリーの連結から組み込まれます。連結順序を
以下に示します。

a. CO.1 で選択された CKRCARLA ライブラリー
b. UPREFIX で指定された CKRCARLA ライブラリー (該当する場合)
c. WPREFIX で指定された CKRCARLA ライブラリー (該当する場合)
d. 製品に付属の CKRCARLA ライブラリー

A オプションで、「**Compliance result selection**」セクションを使用して、準拠性レ
A ポートに含める結果を制限できます。デフォルトでは、フィルターが選択されて
A いない場合、レポートには、準拠、非準拠、および未決定の結果が含まれます。

準拠性結果の選択内容により、表示される結果が決まります。

「**Print format**」を選択すると、2 つのレポートが作成されます。1 番目のレポートには、準拠性ルール・セットの要約が表示されます。2 番目のレポートには、テストされたオブジェクトの準拠性統計が表示されます。

「**Print format**」と「**Include test details**」を選択すると、3 つのレポートが作成されます。

a. 1 番目のレポートには、準拠性ルール・セットの要約が表示されます。
b. 2 番目のレポートには、テストされたオブジェクトの準拠性統計が表示されます。
c. 3 番目のレポートには、個々のルール・セットがそれぞれ別々のページに表示されます。

ルール・セットの影響を受けるオブジェクトは、それらの非準拠、未決定、および準拠の各属性によって配列されます。これらの属性は、ルール・セット内の規則のテストに対する個々のテスト結果の詳細を示します。

「**Print format**」と「**Narrow print**」の両方を選択すると、実際の印刷ファイルのレコード長とは関係なく、ページ幅が 79 文字に制限されます。

以下のレベルにズームインするために表示フォーマットを使用することができます。

a. セキュリティー複合システム・レベル。各セキュリティー・データベースとそのデータベースに関連するシステムに対してテストされた標準を表示
b. ルール・セット・レベル (ルール・セット当たりの非準拠オブジェクトの数を表示)
c. オブジェクト・レベル
d. 個別テスト結果概要レベル
e. 詳細レベル

4. 「**Compliance evaluation**」で、評価する際に照合するいずれかの標準 (例えば、「**STIG (subset)**」または規則のサブセット) を選択します。「**Print format**」のタグを付加しないでください。 図 77 が表示されます。これには 3 つのレポート・オプションが含まれています。

```
                zSecure Suite Display Selection        3 s elapsed, 1.8 s CPU
Command ===>                                                  Scroll===> PAGE

  Name     Summary Records Title
_ STDRULES       1     129 Standard rule set compliance summary
_ STDTYPES       1      20 Standard object type compliance summary
_ STDTESTS       1   17324 Standard compliance test
****************************** Bottom of Data ********************************
```

図 77. 「zSecure Suite Display Selection」パネル

- 97 ページの『STDRULES: Standard rule set compliance summary』: 準拠性ルール・セットの要約を表示します。この管理の要約は、ルール・セット準拠性の状況や向上度を判別するのに役立ちます。

- 99 ページの『STDTYPES: Standard object type compliance summary』: テストされたオブジェクトの準拠性統計を表示します。この管理の要約は、オブジェクト・タイプ準拠性の状況や向上度を判別するのに役立ちます。
- 100 ページの『STDTESTS: Standard compliance test results』: ルール・セット名によってソートされたオブジェクト・テスト結果を表示します。非準拠のテスト結果は、準拠のテスト結果よりも上にソートされます。これらの準拠性テストの詳細な結果は、準拠性を向上させるために、どのリソースに対してどのようなアクションを実行すべきかを判別するのに役立ちます。

STDRULES: Standard rule set compliance summary

ルール・セット準拠性テスト結果の管理の要約は、ルール・セット準拠性の大まかな状況や進捗を判別するのに役立ちます。

「zSecure Suite Display Selection」パネル (96 ページの図 77) で「STDRULES」を選択すると、図 78 が表示されます。これには、実際のテスト結果の詳細は含まれませんが、代わりに、より大まかな準拠性結果が示されます。STDRULES の要約には、テストする必要があるオブジェクトが見つからないルール・セットを含め、サポートされるすべてのルール・セットが含まれています。テストする必要があるオブジェクトが見つからない場合、そのルール・セットは準拠していると報告されます。zSecure Audit が該当の標準に対してサポートするルール・セットごとに 1 行表示されます。

```
                                                                Line 1 of 129
Standard rule set compliance summary
Command ===> ____________________________________________________ Scroll===> PAGE
                                              2 Sep 2015 23:45
   Complex  Ver  Pr Standards
   NMPIPL87      30         1
   Standard      Pr Rule sets
   RACF_STIG     30       129
   Rule set      Pr Cm% NS TestPnt Comply NonCom Unkn Caption
/  AAMV0030      20   0          1      0      1    0 LNKAUTH=APFTAB
__ AAMV0040      10  97        672    654     18    0 APF libraries exist
__ AAMV0050         100         14     14      0    0 APF libraries unique
__ AAMV0160      20  81        143    117     26    0 PPT programs exist
__ AAMV0380         100        288    288      0    0 SMF record (sub)types
__ ACP00010      30  33         12      4      8    0 PARMLIB protected
__ ACP00020      20  36         11      4      7    0 Update on SYS1.LINKLIB
__ ACP00030      30  36         11      4      7    0 Update on SYS1.SVCLIB
__ ACP00040      30  36         11      4      7    0 Update on SYS1.IMAGELIB
__ ACP00050      30  36         11      4      7    0 Update on SYS1.LPALIB
__ ACP00060      30  79       2827   2261    566    0 Update+alter on APF list
__ ACP00070      30  22         87     20     67    0 Update+alter on LPA list
__ ACP00080      30  36         11      4      7    0 Update+alter on Nucleus
__ ACP00110      20  36        193     70    123    0 Update+alter on Linklist
__ ACP00120      30  50          8      4      4    0 RACF db protected
```

図 78. 「STDRULES: Standard rule set compliance summary」パネル

この要約には、ルール・セットごとに、以下の列が含まれています。

Rule set
文書化された標準のルール・セット番号。

Pr 非準拠優先順位: 10 は低、20 は中、30 は高です。準拠として報告された各ルール・セットの場合、この列は空です。

Cm%
準拠性の割合 (パーセンテージ)。この列をモニターして、該当のルール・セットに準拠していく進捗状況を判別できます。

NS NS は連結された列です。N は、適用外として評価されるテストを含むルール・セットを表します。S は、ルール・セットが抑止されている場合に表示されます。

TestPnt
このルール・セット内のテストされたオブジェクトの数。

Comply
準拠オブジェクトの数。

NonCom
非準拠オブジェクトの数。

Unkn
結果が未決定/不明であるテストの数。

Caption
このルール・セットがテストする対象の簡略説明。

行コマンドの S または / を使用して、このルール・セットの詳細にアクセスすることができます。このパネルには、ルール・セットの十分な説明と、システムを評価したときに照合した標準名とバージョンが含まれています。

```
                                                                Line 1 of 30
Standard rule set compliance summary
Command ===> _____________________________________________ Scroll===> PAGE
AAMV0030       LNKAUTH=APFTAB                  2 Sep 2015 23:45



  Rule set
  Rule set                      AAMV0030
  Complex compliant with rules  No       Relative audit priority       20
  Rule set non-comply severity  Medium   Site overruling set severity

  Rule set description
  LNKAUTH=APFTAB must be active to provide granular APF control; since this is
  not default it must be specified explicitly in IEASYSxx.

  Suppression and exemption
  Rule set not applicable       No
  Rule set suppressed           No
  Reason rule set suppression

  Resource location
  Complex name                  NMPIPL87 Complex severity (importance) Medium

  Data points tested                     Percentage
  Compliant data points               0 Compliant data points     (%)   0
  Non-compliant data points           1 Non-compliant data points (%) 100
  Undecided/unknown data points       0 Undecided data points     (%)   0
  Number of data points tested        1

  Standard
  Standard name                 RACF_STIG
  Version of standard           6.24
****************************** Bottom of Data ********************************
```

図 79. STDRULES: rule set details

各ルール・セットまたは各規則には、重大度が割り当てられています。「**Rule set non-comply severity**」フィールドを参照してください。別の重大度値が組織に適用されると、別の重大度値を割り当てる SITE_SEVERITY ステートメントで元の重大度を指定変更できます。可能な値は、high、medium、および low です。

STDTYPES: Standard object type compliance summary

オブジェクト・タイプ準拠性テスト結果の管理の要約は、オブジェクト・タイプ準拠性の状況や進捗を判別するのに役立ちます。

「zSecure Suite Display Selection」パネル (96 ページの図 77) で「STDRULES」を選択すると、「Standard object type compliance summary」が表示されます。それには、STIG 準拠性評価に使用される newlist タイプについての統計が示されます。列の説明については、97 ページの図 78を参照してください。さらに、「**Exempt**」列には、例外がコーディングされていることが検出された除外オブジェクトの数が示されます。

```
                                                                Line 1 of 20
Standard object type compliance summary
Command ===> _____________________________________________ Scroll===> PAGE
                                          2 Sep 2015 23:45
   Complex  Ver  Types
   NMPIPL87             20
   Type                     System   Cm% Objects Comply  NoCompl Unknown Exempt
__ as                       PL87       0       2       0       2       0      0
__ as_dd                    PL87       0      26       0      26       0      0
__ cics_region              PL87       0       1       0       1       0      0
__ cics_transaction         PL87     100       0       0       0       0      0
__ class                    PL87      50       2       1       1       0      0
__ id                                 36      44      16      28       0      0
__ ip_ftp_region            PL87       0       1       0       1       0      0
__ ip_resolver              PL87       0       1       0       1       0      0
__ ip_stack                 PL87     100       1       1       0       0      0
__ mount                    PL87     100       0       0       0       0      0
__ r_ac1                    PL87      81     143     117      26       0      0
__ r_profile                          100       1       1       0       0      0
__ r_stc                    PL87      12     811      99     712       0      0
__ racf_access                        18    1111     210     901       0      0
__ resource                 PL87      66     410     274     136       0      0
S_ sensdsn                  PL87      59     916     547     369       0      0
__ smfopt                   PL87     100       4       4       0       0      0
__ system                   PL87       0       1       0       1       0      0
__ unix                     PL87     100       0       0       0       0      0
__ unix_ps                  PL87       0       1       0       1       0      0
****************************** Bottom of Data ********************************
```

図 80. STDTYPES: Standard object type compliance summary

行コマンドの S または / を使用して、特定の newlist タイプの STIG 準拠性評価を確認できます。100 ページの図 81には、該当する newlist タイプが使用されているルール・セットと、このルール・セットが準拠、非準拠、未決定/不明、または除外のいずれであるかが示されます。

```
                                                              Line 1 of 21
 タイプ
 Test domain newlist type      sensdsn
 Complex name                  NMPIPL87
 System name                   PL87

 Objects tested                         Percentage
 Compliant objects                553 Compliant objects         (%)  59
 Non-compliant objects            369 Non-compliant objects     (%)  40
 Undecided/unknown objects          0 Undecided/unknown objects (%)   0
 Exempt objects                     0 Exempt objects            (%)   0
 Number of objects tested         922

 Records read for type
 Number of records read          1630

 Rule sets
 Non-compliant rule sets       AAMV0040 ACP00010 ACP00020 ACP00030 ACP00040
 Non-compliant rule sets       ACP00050 ACP00060 ACP00070 ACP00080 ACP00110
 Non-compliant rule sets       ACP00120 ACP00130 ACP00135 ACP00150 ACP00170
 Non-compliant rule sets       ACP00230 ACP00250 ZSMS0022
 Undecided rule sets
 Compliant rule sets           ACP00180 ZSMS0032
****************************** Bottom of Data ********************************
```

図 81. STDTYPES: newlist の STIG 準拠性評価

STDTESTS: Standard compliance test results

準拠性テストの詳細な結果は、準拠性を向上させるために、どのリソースに対してどのようなアクションを実行すべきかを判別するのに役立ちます。

「zSecure Suite Display Selection」パネル (96 ページの図 77) で「STDTESTS」を選択すると、101 ページの図 82 が表示されます。STDRULES の要約には、サポートされるすべてのルール・セットが含まれますが、STDTESTS の要約には、テスト結果があるルール・セットのみが含まれます。テスト結果がないルール・セットは無視され、STDTESTS レポートには含まれません。

画面出力と印刷出力は、画面の幅と行の長さの影響を受けます。幅が狭い出力ではルール・セットの表題が表示されますが、幅が広い出力ではルール・セットの説明が表示されます (94 ページの図 76 の「AU.R」パネルの「**Narrow print**」オプションを参照してください)。101 ページの図 82 に、画面の幅が 80 のルール・セット・レベルの出力の例を示します。

列の説明については、97 ページの図 78を参照してください。

```
                                                                Line 1 of 109
Standard compliance test
Command ===> _____________________________________________ Scroll===> PAGE

   Complex  Ver  Pr Standards NonComp Unknown Exm Sup
   NMPIPL87      30         1       1       1   1
   Standard      Pr Rule sets NonComp Unknown Exm Sup Version
   RACF_STIG     30       109      69       2   4     6.20
   Rule set      Pr Objects   NonComp Unknown Exm Sup Caption
/  AAMV0030      20         1       1                 LNKAUTH=APFTAB
__ AAMV0040      10       672      18                 APF libraries exist
__ AAMV0050                14                         APF libraries unique
__ AAMV0160      20       143      26                 PPT programs exist
__ AAMV0380               288                         SMF record (sub)types
__ ACP00010      30         9       7                 PARMLIB protected
__ ACP00020      20         8       7                 Update on SYS1.LINKLIB
__ ACP00030      30         8       7                 Update on SYS1.SVCLIB
__ ACP00040      30         8       7                 Update on SYS1.IMAGELIB
__ ACP00050      30         8       7                 Update on SYS1.LPALIB
__ ACP00060      30       745     197                 Update+alter on APF list
__ ACP00070      30        27      25                 Update+alter on LPA list
__ ACP00080      30         8       7                 Update+alter on Nucleus
__ ACP00110      20        64      54                 Update+alter on Linklist
__ ACP00120      30         5       4                 RACF db protected
   ...
__ RACF0430                1                         SETROPTS PASSW HIST(10)
/  RACF0440      20         1       1                 SETROPTS PASSW INT(60)
__ RACF0445                1                         SETROPTS PASSW MINCHA>0
   ...
__ ZWMQ0049      20        20      18                 MQ RACF classes active
****************************** Bottom of Data ********************************
```

図 82. 「STDTESTS - Standard compliance test」パネル

複合システム別の準拠性には、標準の数と、この準拠性評価の実行で処理された結果が示されます。この例では、複合システム NMPIPL87 の場合、RACF_STIG と照合して準拠性がチェックされ、完全には準拠していないことが示されています。

標準が 1 つだけ評価された場合、2 番目の要約レベルの結果が示されます。複数の標準と照合して複合システムが評価された場合、システムが評価される際に照合された標準ごとに別個の要約レポートが生成されます。

標準別の要約には、最高の非準拠優先順位、報告されるルール・セットの総数、その標準内の非準拠、不明/未決定、および除外の規則の数が示されます。

ルール・セット別の要約には、ルール・セット内の 1 つ以上のテストの影響を受けたオブジェクトの数と、該当するルール・セットの特定の結果が示されます。

行コマンドの S または / を使用して、レポートの詳細にズームインすることができます。

```
                Standard compliance test results                Line 1 of 2
Command ===> ____________________________________________ Scroll===> PAGE
                                              10 Sep 2015 23:45
   Complex  Ver  Pr Standards NonComp Unknown Exm Sup
   NMPIPL87      30         1       1       1   1
   Standard      Pr Rule sets NonComp Unknown Exm Sup Version
   RACF_STIG     30       107      69       3   4     6.20
   Rule set      Pr Objects   NonComp Unknown Exm Sup Caption
   RACF0440      20         1       1                 SETROPTS PASSW INT(60)
   Non Unk Exm Class    System   Type    VolSer Resource
   Non         System   PL87                PL87
   Cmp Non Unk Ex  Test name               Member   Test description
/      Non          b.1b.PWDInterval60     CKAGR440 PASSWORD(INTERVAL) must be
__ Cmp              b.1a.PWDInterval0      CKAGR440 PASSWORD(INTERVAL) should
****************************** Bottom of Data ********************************
```

図 83. 「STDTESTS - Standard compliance test results」パネル

図 83 の例では、ご使用のシステムがルール・セット RACF0440 に対する 2 つのテストのいずれかに準拠していないことが示されています。行コマンドの S または / を使用して、このテストのすべての詳細情報を読み取ることができます。

```
                Standard compliance test results                Line 1 of 59
Command ===> ____________________________________________ Scroll===> PAGE
                                          10 Sep 2015 23:45


  Test description
  PASSWORD(INTERVAL) must be set to less than or equal to 60.

  Class    Resource
  System   PL87

  Test result
  Test value is compliant       No       Test is true                 No
  Non-compliant audit finding   Yes      Relative audit priority      20
  Lookup against
  Actual value of test field    90

  Test definition
  Test name                     b.1b.PWDInterval60
  Test lookup base field name
  Test field name               PWDINTERVAL
  Relational operator           <=
  Compliance comparison value   60

  Suppression and exemption
  Rule set not applicable
  Exempt from rule              No
  Rule suppressed
  Reason for rule suppression

  Domain
  Domain name                   System_options
  Domain description

  Rule
  Rule set                      RACF0440
  Rule name                     RACF0440
  Rule non-compliance severity  Medium   Site overruling rule severity

  Rule description
  The PASSWORD(INTERVAL) SETROPTS value must be set to 60 days.

  Rule set description
  The PASSWORD(INTERVAL) SETROPTS value must be set to 60 days.

  Resource location
  Complex name                  NMPIPL87 Complex severity (importance) Medium
  System name                   PL87     Profile or data set type
  Test domain newlist type      system




  Standard
  Standard name                 RACF_STIG
  Version of standard           6.24



  Test origin
  Test defined in CARLa member  CKAGR440
****************************** Bottom of Data ********************************
```

図 84. RACF0440 に対するテスト b.1b.PWDInterval60 の「STDTESTS - Standard compliance test results」

図 84 の例では、「**Test description**」に、パスワード・インターバルが 60 日以下でなければならないことが示されています。「**Test results**」には、検出された実際の値が 90 であることが示されています。「**Test definition**」には、該当するテスト

A の詳細が示されています。それは、パスワード・インターバルが 60 以下 (**<=** 60)
A でない場合、テストは非準拠として報告される必要があることを示しています。

4 「**Suppression and exemption**」には、この規則が除外されないことが示されていま
4 す。この規則が、該当する規則から除外されていることがテストによって示される
4 ように、この規則の CARLa コード内に除外定義をコーディングすることができま
4 す。

4 ある規則がルール・セットの一部である場合、該当する「Rule description」は通常
4 は「Rule set description」とは異なります。

4 「**Test origin**」には、このルール・セットの CARLa コードがどの SCKRCARL メ
4 ンバーに保管されているかが示されています。ご使用のシステム用にこのルール・
4 セットを検討したりカスタマイズしたりすることができます。

第 10 章 SMF データ照会

注: SMF Query 機能は、zSecure Audit 製品でのみ使用可能です。

SMF 表示では、ライブ SMF データ・セット、SMF ログ・ストリーム、または順次 SMF データを操作できます。SMF データは、IBM **IFASMFDP** プログラムまたは **IFASMFDL** プログラムによって作成されます。 zSecure Audit for RACF の操作に慣れるためにこの製品を実際に使用する際には、ライブ SMF ファイルではなく順次 SMF データを使用してください。静的な順次データを使用することで、パラメーターを少し変更して操作を試行する場合に、より一貫性のある結果を得ることができます。

どの SMF データを zSecure Audit で使用するか検討する必要があります。z/OS により収集される SMF データの量は、システム環境によって大きく異なります。場合によっては、適度な DASD 割り当て (例: 30 MB) で 1 週間分のデータを保持できることもあれば、その割り当てでは 1 時間分の SMF データ収集内容しか保持できない場合もあります。単に zSecure Audit for RACF の操作を試す場合は、10 MB から 30 MB の範囲内の SMF データのセットが適当です。フィルター処理を適用してデータ・セットのサイズを削減する必要がある場合は、表 11 に示すレコード・タイプがフィルターで除外されないようにしてください。

表 11. SMF データからフィルターで除去してはならない SMF レコード・タイプ

レコード・タイプ	説明
14	INPUT または RDBACK データ・セット・アクティビティー
15	OUTPUT、UPDATE、INOUT、または OUTIN データ・セット・アクティビティー
17	スクラッチ・データ・セット状況
18	名前変更データ・セット状況
30	共通アドレス・スペース作業
42	DFSMS 統計および構成
60	VSAM ボリューム・データ・セット更新済み
61	ICF 定義アクティビティー
62	VSAM コンポーネントまたはクラスター・オープン
63	VSAM カタログ項目の定義
64	VSAM コンポーネントまたはクラスター状況
65	ICF 削除アクティビティー
66	ICF 変更アクティビティー
67	VSAM カタログ項目削除
68	VSAM カタログ項目名前変更
69	VSAM データ・スペース、定義、拡張、または削除
80	RACF 処理
81	RACF 初期化

表 11. SMF データからフィルターで除去してはならない SMF レコード・タイプ (続き)

レコード・タイプ	説明
A 82	ICSF 統合暗号化
83-1	データ・セット用の RACF 監査レコード
90	システム状況
92	z/OS UNIX ファイル・システム・アクティビティー
102	DB2® パフォーマンスおよび監査
109	ファイアウォール
110	CICS 統計
119	TCP/IP 統計
120	WebSphere® Application Server のパフォーマンス

すべてのレコード・タイプが含まれている完全な SMF ファイルに対して zSecure Audit for RACF SMF 分析を実行することもできます。zSecure Audit for RACF は、約 100 種類の SMF レコード・タイプをサポートします。

入力データ・セットの定義

SMF データを処理する場合は、zSecure Audit for RACF に対してデータ・セットを定義する必要があります。データ・セットを指定するには、以下のタスクを実行します。

手順

SMF データを処理する前に、「Setup File (SE.1)」オプションを使用して、入力データを指定しておく必要があります。

1. メインメニューでオプション「**SE**」(セットアップ) を選択して、Enter を押します。
2. 「**1**」(入力ファイル) を選択して Enter を押します。「Setup Input」パネルが開きます。このパネルについて詳しくは、 65 ページの『入力セットの選択』を参照してください。
3. カーソルを行の入力フィールド (左端) に移動します。
4. 文字 I を入力して Enter を押し、新規入力セットを挿入します。 「Setup Input」パネルが開きますが、データはありません。
5. コマンド行の下の「**説明**」フィールドに、タイトル (例: `Filtered SMF data set`) を入力します。
6. カーソルを 1 番目の「**Data set or Unix file name**」フィールドに移動します。SMF データを含むデータ・セットの名前を入力します。次に、Enter を押します。

   データ・セット名が `.SMF` で終わる場合、ファイル・タイプ (SMF) が自動的に入力されます。`.SMF` で終わらないデータ・セット名の場合、 107 ページの図 85 などのパネルが開き、定義するファイルにタイプを割り当てることができます。

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Setu Row 1 to 13 of 13
Command ===> _____________________________________________ Scroll ===> CSR_


 Select the type of data set or file

     Type             Description
_    ACCESS           RACF ACCESS monitor data set
_    ACT.BACK         The backup RACF database of your active system
_    ACT.PRIM         The primary RACF database of your active system
_    ACT.SMF          The live SMF data set(s)
_    ACT.SYSTEM       Live settings
_    CKFREEZE         A CKFREEZE data set
_    CKRCMD           A file for generated RACF commands
_    COPY.RACF        A copy of a single data set RACF database
_    COPY.SEC         A non-first component of a multiple data set RACF database
_    COPY.TEMP        The first component of a multiple data set RACF database
_    SMF              VSAM or dumped SMF
_    SMF.LOGSTR       SMF logstream
_    UNLOAD           An unloaded RACF database
_    WEBACCESS        IBM HTTP Server access log
_    WEBERROR         IBM HTTP Server error log
```

図 85. ファイル・タイプの割り当て

7. オプション「**SMF**」を選択して Enter を押します。ライブ SMF データを参照する行が作成されます。
8. PF3 を押します。

   新しい入力セットが選択された「Input file」パネルに戻ります。

   ヒント: 同時に複数の入力セットを選択できます。各ファイルまたはいくつかのファイルに対して 1 つのセットを定義することを検討してください。例えば、ライブ SMF セットと、RACF データベースおよび CKFREEZE データ・セットの最新のアンロードとを定義し、その両方のセットを入力として選択します。

タスクの結果

入力ファイル設定は、図 86 に示すファイル設定のようになります。

```
 Menu   Options   Info   Commands  StartPanel
------------------------------------------------------------------------------
      zSecure Admin+Audit for RACF - Setup - Input file       Row 1 from 5
Command ===> _____________________________________________ Scroll ===> CSR_

(Un)select (U/S/C/M) set of input files or work with a set (B, E, R, I, D or F)

   Description                                            Complex
_  Filtered SMF data set                                           selected
_  Input set created 8 Apr 2005                                    selected
_  Active primary RACF data base                          DEMO
_  Active backup RACF data base                           DEMO
_  Active backup RACF data base and live SMF data sets    DEMO
****************************** Bottom of data ********************************
```

図 86. 入力ファイル設定

ライブ SMF データを使用するために、データ・セットを指定する必要はありません。「**タイプ**」フィールドに / を入力し、Enter を押します。図 85 に示すパネルが開き、オプション「**ACT.SMF**」を選択できます。

これは、最も基本的な SMF 入力の形式です。より複雑な状況では、ライブ SMF と、最新の *n* 世代を組み合わせることができます。アーカイブ SMF データの世代別データ・グループ (GDG) を使用するには、入力セット内の複数の行をリストします。

SMF レポートの作成

以下のタスクを実行して、指定した選択基準に一致する SMF レコードに関する SMF レポートを生成します。

手順

1. メインメニューでオプション「**EV**」(イベント) を選択し、Enter を押します。
2. オプション「**2**」(RACF イベント) を選択し、Enter を押します。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
             zSecure Audit for RACF - Events - RACF events
Option  ===> ____________________________________________________________

Enter "/" to select report(s)
_ All events       Overview of all following RACF events (except IPL)
_ Logging          RACF logging of all events except RACINIT
_ Not normal       RACF access not due to normal profile access
_ Warnings         RACF access due to profiles in warning modes
_ Violations       RACF access violations
_ Commands         RACF command auditing
_ CKGRACF          zSecure Admin CKGRACF commands
_ IPL RACF         RACF initialization
```

図 87. SMF RACF イベント表示

3. 「RACF イベント」パネルで「**全イベント**」を選択し、Enter を押します。

   さまざまな SMF レポートに共通する SMF 選択パネルを、109 ページの図 88 に示します。

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
                        zSecure Admin+Audit for RACF "DOWN    " is not active
Command ===> ____________________________________________________________________

Select SMF records that fit all of the following criteria
Use EGN masks for selection criteria
Userid  . . . . . . IBMUSER
Jobname . . . . . . ____________________________________________________________
Terminal  . . . . . ____________________________________________________________

Dataset name  . . . ____________________________________________________________

Profile class . . . ____________________________________________________________
Profile key . . . . ____________________________________________________________
Level . . . . . . . __  __      (installation defined resource level)

                    From         Until            Intended access at least
Time                ____       : ____             6  1. Execute  2. Read
Date                _________  : _________           3. Update   4. Control
Weekday             ____       : ____              5. Alter    6. All access

Show all            _  Success   _  Warning   _  Violation
```

図 88. SMF 選択基準

指定した選択基準に一致する SMF レコードのみが処理されます。このパネルで未使用のフィールドはすべて、選択処理に反映されません。このパネルについて以下に説明します。

- 「**Userid**」、「**Jobname**」、「**Terminal**」、「**Profile class**」、「**Profile key**」、「**Data set name**」の各フィールドには、1 つ以上の検索ストリングをブランクで区切って入力できます。%、*、** などのワイルドカードを使用できます。「**Userid**」フィールドに他のパラメーターが指定されていない単一のアスタリスクを入力した場合、RACF ユーザーに属することができるすべての SMF レコードが選択されます。
- 「**レベル**」フィールドを使用すると、データ・セット・レベルまたはリソース・レベルで選択できます。

  1 番目のフィールドを使用して、プロファイル内に存在するレベルを判別する演算子を指定します。そのレベルより小か等しいレベルを選択する場合は、< と <= を使用します。高いレベルの場合は > または >= を使用し、正確に一致するレベルの場合は =、指定したレベルを除くすべてのレベルを選択する場合は ¬= および <> を使用します。

  2 番目のフィールドには、データ・セット・レベルまたはリソース・レベルを示す数値を指定します。このレベルは IBM ユーティリティーによって設定も更新もされませんが、インストール先で使用することができます。
- データ・セット名の接頭部にユーザー ID が自動的には追加されません。
- 時刻は 24 時間の *HHMM* 形式で指定します。
- 日付は、*YYYY-MM-DD*、*DDMMMYYYY*、または *YYYY/DDD* として指定します (例えば、2012-03-01、01MAR2012、2012/301)。日付範囲はコロンで区切ります (例: 10APR2005:14APR2012)。
- 曜日は、英語の曜日名の先頭 3 文字で示します (例: 月曜日 (Monday) は Mon)。

- 「**Intended access at least**」フィールドでは、少なくとも指定した権限を必要とするアクセス・イベントのみを選択できます。

選択パネルの後に、除外パネルが表示されます。除外パネルの内容は、 109 ページの図 88 の選択パネルと同様です。SMF レコードは、選択プロセスを通過しても、除外パラメーターの設定によっては拒否されることがあります。除外パラメーターを指定する必要はありません。例えば、UPDATE 以上のアクセス・レベルで SYS*.* という名前のデータ・セットへのアクセスをすべて選択しますが、データ・セット SYS1.BRODCAST へのアクセスを除外します。

次のタスク

選択パネルと除外パネルの後に、生成されるレポートを制御するためのパネルが表示されます。これらのパネルを使用して、入力レコードの数を制限できます。特に SMF ファイルが巨大な場合に、出力レコードの数を制限し、表示または印刷の出力をフォーマットを設定します。

この例では、SMF レポートで使用するデータ・セットとして CKFREEZE データ・セットを選択しないでください。SMF プロセス・オプション・パネルの「**Use CKFREEZE data**」フィールドの前に / がないことを確認してください。RACF 専用の場合、このオプションは必要ありません。このオプションを指定すると、必要な TSO 領域サイズが増加する可能性があります。UNIX ファイル・システム・レコード (タイプ 92) のフォーマットを設定する場合には、このオプションが必要です。

SMF 検索により、概要レポートが作成されます。SMF レコードごとの 1 行と、統計要約が表示されます。レコードの詳細を表示するには、**S** 行コマンドを入力します。

zSecure Audit for RACF による SMF レコードの処理はきわめて単純です。選択パネルと除外パネルの適切な使用と、高速処理によりその力を発揮します。ただし、SMF 処理を効果的に使用するには、管理者が計画を立てる必要があります。オンラインでまたは HSM 機能を介して容易にアクセスできる十分な量の最新 SMF データが必要です。

zSecure Audit for RACF は、SMF イベント・レコードに RACF データ・ソースの情報がない場合に、SMF イベント・レコードにこの情報を補足します。このようにすることで、SMF レコードの Jobname が RACF ユーザー ID の形式に対応していない場合でも、z/OS イベント・レコード (タイプ 14 および 15 など) を RACF ユーザー ID に属させることが可能になります。

ユーザーの監査タイプ

始める前に

ユーザー・イベント証跡を監査するには、まず、SMF データが含まれている入力データ・セットを選択する必要があります。その後、次のステップを実行します。

手順

1. メインメニューに戻ります。

2. オプション「**EV.U**」(イベント、ユーザー・イベント) を選択します。図 89 に示す「User Selection」パネルが表示されます。

   このパネルから、1 つ以上の特定ユーザーの監査証跡の検索や、特定のタイプのユーザーによって引き起こされたイベントの検索を行います。

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
                zSecure Admin+Audit for RACF - Events - User Selection
Command ===> ____________________________________________________   _ start panel

Show records that fit all of the following criteria:
Userid  . . . . . ________     (userid or EGN mask)
Owned by  . . . . ________     (group or userid, or EGN mask)
System  . . . . . ____         (system name or EGN mask)
Name  . . . . . . _____________________________ (name/part of name, no filter)
Installation data . _____________________________ (scan of data, no filter)
Jobname . . . . . ________     (job name or EGN mask)
Terminal  . . . . ________     (Terminal id or EGN mask)

Advanced selection criteria
/  User actions            _  User attributes         _  Date and time
_  Data set selection      _  HFS selection           _  Resource selection
_  DB2 selection           _  CICS selection          _  Omegamon selection

Output/run options
_  Include detail          _  Summarize              _  Specify scope
_  Output in print format     Customize title           Send as e-mail
   Run in background          Sort differently
```

図 89. 「EV.U User Selection」パネル

3. 「**Advanced selection criteria**」セクションで「**User actions**」を選択し、Enter を押します。 選択パネルが開き、認識されているアクション・タイプが表示されます。
4. 発行された **RACF/CKGRACF コマンド**の前に / を入力し、「**Successful**」の前にも / を入力します。次に、Enter を押すと、図 90 に示す RACF コマンド概要パネルが開きます。

   このパネルには、ご使用のシステムで発行され、正常に完了した RACF コマンドが表示されます。PF1 を使用すると右側にスクロールできます。

```
Event log record detail information                    1 s elapsed, 0.7 s CPU
Command ===> ____________________________________________ Scroll===> CSR_
                                          4Apr05 09:17 to  4Apr05 09:21
   Date      Time     Description
__ 04Apr2005 09:17:16 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:17:32 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:17:46 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:17:53 RACF SETROPTS success for IBMUSER
__ 04Apr2005 09:21:22 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:21:30 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:21:49 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:21:55 RACF SETROPTS success for IBMUSER
****************************** BOTTOM OF DATA ********************************
```

図 90. RACF コマンド・イベント・ログ・レコードの概要

5. レコードあたり 1 行の要約よりも詳細な情報を表示するには、図 89 に示されたパネルの「**Output/run options**」セクションのオプション「**Include detail**」を選択して、照会を再実行します。

6. RACF イベント・ログの概要パネルで、レコードを選択して、図 91 に示されたパネルを開きます。

   これで、詳細情報 (コマンド全体や、ユーザーを識別するフィールドなど) が表示されます。

```
Event log record detail information                              Line 1 of 43
Command ===> ____________________________________________________ Scroll===> CSR_
                                          4Apr05 09:17 to  4Apr05 09:21


  Description
  RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPTION.HD.8

  Record identification
_ Jobname + id:  IBMUSER
  SMF date/time: Wed  4 Apr 2005 09:17:46.59
_ SMF system:    DEMO       record type:  80   record no: CKR1SM01 3013

  Event identification
  RACF event description        Permit command (Success:No violations detected)
  RACF event qualifier          0
  RACF descriptor for event     Success
  RACF reason for logging       Class Special
  SAF authority used            Special
  Audit/message logstring

  RACF command
  PERMIT '$C2R.OPTION.HD.8' ACCESS(READ) CLASS(FACILITY) ID(IBMUSER)
```

図 91. RACF コマンドのイベント・ログ・レコード詳細パネル

変更トラッキング

「**変更トラッキング**」機能は、重要な RACF および SYSTEM 定義の変更を追跡するための強力な機能です。

Change Tracking 関数を使用すると、検査済みのベース構成と現行構成の差異をリストできます。

注: Change Tracking 関数は、zSecure Audit for RACF でのみ使用できます。

重要な RACF 定義にはいくつかの種類があります。例えば、システム全体の SPECIAL ユーザー、OPERATIONS ユーザー、機密データ・セットを保護するプロファイルなどです。 SYSTEM 関連の機密定義には、APFLIST などの APF 定義データ・セットがあります。また、既に機密としてマークされている定義以外にも、その他の RACF 定義や SYSTEM 定義を機密として指定できます。

モニター対象となるようなその他のシステム設定には、APF 許可ライブラリーのリストの変更や、RACF クラス記述子テーブルの変更などがあります。zSecure Audit for RACF で情報が表示されるほとんどの項目の変更は追跡することができます。

追跡される変更に対し、受け入れ、拒否、または据え置きのいずれかを実行する必要があります。変更を受け入れて検査済みベースを更新するか、または変更内容が

誤っている場合は変更を拒否します。変更を拒否する場合は、構成の変更も取り消す必要があります。そうしなければ、次の「変更のトラッキング」ステップで同じ変更が再度報告されます。

ライブラリー変更検出

注: この機能は zSecure Audit for RACF でのみ使用可能です。

現実的な方法で「**ライブラリー変更検出**」機能を使用するには、ある程度の計画と時間が必要です。以下の簡略説明を読んだ後で、評価の際にこの機能を使用するかどうかを決定してください。この機能について詳しくは、「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」の『ライブラリー監査』セクションを参照してください。

ライブラリー変更検出機能は、ライブラリー更新レポートを提供します。これは、ロード・モジュールから成るメンバーまたは区分データ・セットのソース・テキストに対する変更を検出および表示する場合に使用します。シスプレックス環境および SMS 管理環境で、共有 DASD 上のライブラリーを追跡するロジックが組み込まれています。基本機能は、モニター対象であるすべてのライブラリーに含まれるすべてのメンバーに関する zSecure Collect データに基づいて開発されています。すべてのシステム・ライブラリーが含まれています。ただし、それらを除外することもできます。また、モニターする他のライブラリーを指定することもできます。zSecure Collect for z/OS は、これらのライブラリーの各メンバーを調べ、メンバー内のデータのデジタル署名を算出します。このデジタル署名は、zSecure Collect for z/OS により作成される CKFREEZE データ・セットに記録されます。

ライブラリー変更検出は、内部監査員にとって役立つ機能です。**ライブラリー変更検出**機能は、特に社内監査員にとっては非常に強力なツールとなります。監査員は、データを月単位または年単位で比較することで、その期間内に変更されたすべてのプログラムを特定できます。プログラムは、ソース・コードまたはロード・モジュールのどちらかです。この機能は、システム・ライブラリーに限定されません。アプリケーション・ライブラリーもモニターできます。

デフォルトの CKFREEZE データ・セット (現行入力セットの作成時に作成したものなど) には、ライブラリー管理に必要なデータが含まれていません。ライブラリー・メンバー・データを収集するには、別の zSecure Collect for z/OS ジョブをサブミットする必要があります。この方法を試す場合は、114 ページの図 92 に示されているパネルで「**Freeze**」オプション (オプション **0**) を使用します。

このオプションを選択すると、パラメーターの入力が求められ、必要なジョブを実行依頼できます。おそらく、「**System Libraries**」を選択することが最良のオプションと考えられますが、任意のライブラリーを指定することもできます。既存の CKFREEZE データ・セットを再利用することを選択できます。新規 CKFREEZE データ・セットには、VTOC、VVDS、カタログなどからのものではなく、z/OS テーブルからのすべてのデフォルト・データが含まれます。新規ライブラリー・メンバー・データも含まれます。この zSecure Collect for z/OS ジョブの実行には数分かかります。選択したライブラリーの各メンバーを開いて読み取る必要があるためです。

```
  Menu   Options   Info   Commands   Setup   StartPanel
------------------------------------------------------------------------------
              zSecure Audit for RACF - Audit - Libraries
Option  ===> ____________________________________________________

0    Freeze          Calculate new digital signatures
1    Lib all         Overview of all libraries
2    Lib changes     Overview of all libraries with changes
3    Status          Show member status
4    Changes         Identify members with changes
5    Scan            Show members flagged by SCAN function
6    Duplicates      Identify identical members
7    Application     Members summarized by application
8    Prefix          Members summarized by member prefix (component code)
9    PTF - ZAP       Members touched by PTF or ZAP
```

図 92. 1 次ライブラリー更新分析パネル

ライブラリー変更検出を実行するには、CKFREEZE データ・セットの複数の世代が必要であるため、入力セット内に少なくとも 2 つを定義する必要があります。この目的のためには、計画を立てて GDG を使用する方法が理想的です。zSecure Audit for RACF は、さまざまな CKFREEZE データ・セットの署名を比較してレポートを作成します。ライブラリー更新分析の機能の中には、2 つの CKFREEZE データ・セットを必要としないものがあります。オプション 1、3、5、6、7、8、および 9 は、1 つ以上の CKFREEZE データ・セットに使用できます。その他のオプションは、ライブラリー・モニターの一部として使用可能です。例えば zSecure Collect for z/OS はライブラリー・メンバーについて、メンバー内に特定のテキストまたは 16 進数ストリングがあるか、または特定の監視プログラム呼び出し (SVC) の使用状況などを調査できます。それは、SVC がどのプログラムで使用されているかというよくある質問に対して回答する際に役立ちます。

これらのオプションについては、「*IBM Security zSecure Admin and Audit for RACF¥: ユーザー・リファレンス・マニュアル*」に説明があります。 CKFREEZE のデータの収集中に、16 進値検索機能を使用して典型的な許可コード・フラグメントを検出することもできます。重複メンバーを特定するオプションも便利です。このオプションにより、スキャン対象のすべてのライブラリーの中から、CKFREEZE データ・セットが重複するメンバー名を使用して作成されているか、またはメンバー名に関係なく重複するコンテンツを使用して作成されている場合に、ライブラリー・メンバーを検出できます。標準の z/OS ユーティリティーでは、これらの機能を妥当に実行できる方法がありません。ただし、効果的なソフトウェア保守と監査制御において、重複メンバーの検出は重要です。

「ライブラリー変更検出」機能を使用するための入力ファイルの設定は次の例のようになります。

```
  Menu   Options   Info   Commands
-------------------------------------------------------------------------------
               zSecure Audit for RACF - Setup - Input F      Row 1 from 5
Command ===> _____________________________________________ Scroll ===> CSR_

(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)

   Description                                                Complex
_  CKFREEZE dd 4 Apr 2005                                              selected
_  CKFREEZE dd 8 Apr 2005                                              selected
_  Active primary RACF data base                              DEMO
_  Active backup RACF data base                               DEMO
_  Active backup RACF data base and live SMF data sets        DEMO
****************************** Bottom of data ********************************
```

図 93. 入力セットの定義

これはやや基本的な入力構造ですが、評価に使用することができます。このセクションには、ライブラリー関数に不要な SMF データ・セットに関する情報は含まれていません。 **Freeze** オプションを使用して古いデータを最初に収集し、必要なジョブを生成してサブミットします。その後、数日経過してから新しいデータを収集します。長期にわたって使用する場合は、世代別データ・グループ(「HLQ.CKFREEZE (0)」や「HLQ.CKFREEZE (-1)」など) を使用します。

入力セットには、適切な数の SMF および CKFREEZE データ・セット、および 1 つの RACF データベースを含めることができます。RACF データベースは、アクティブな RACF データベース、アンロードされた RACF データ、RACF データベースのコピー、または別のシステムのアクティブな RACF データベースの場合があります。このデータベースは任意の数のデータ・セットで構成できます。

第 11 章 RACF リソースのリソース・ベース・レポート

リソース・レポート・オプション (**RE**) は、メインメニューから使用できます。

```
 Menu         Options       Info     Commands     Setup
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Main menu
Option  ===> ____________________________________________________________

SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
RE   Resource        Resource reports
  C    CICS            CICS region and resource reports
  D    DB2             DB2 region and resource reports
  I    IP stack        TCP/IP stack reports
  M    IMS             IMS control region and resource reports
  N    VTAM            VTAM reports
  Q    MQ              MQ region and resource reports
  T    Trusted         Trusted users and sensitive resources reports
  U    Unix            Unix filesystem reports
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

Input complex: DAILY
```

図 94. zSecure Audit for RACF のメインメニュー

以下の RACF リソースの表示およびレポート・オプションにアクセスできます。

- 『CICS 領域およびリソース・レポート』
- 120 ページの『DB2 領域およびリソース・レポート』
- 124 ページの『IP スタック・レポート』 (zSecure Audit でのみ使用可能)
- 125 ページの『IMS 領域およびリソース・レポート』
- 128 ページの『VTAM アプリケーション・レポート』 (zSecure Audit でのみ使用可能)
- 129 ページの『MQ 領域およびリソース・レポート』
- 132 ページの『信頼関係レポート』 (zSecure Audit でのみ使用可能)
- 133 ページの『UNIX ファイル・システム・レポート』

CICS 領域およびリソース・レポート

メインメニューの **RE.C** オプションを使用して、CICS の領域、トランザクション、およびプログラムのデータを選択および表示します。

レポート・データは、zSecure Collect APF 許可を実行して作成された `CKFREEZE` データ・セットから取得されます。

RE.C を選択すると、 118 ページの図 95 に示すパネルが表示されます。

T および **P** オプションは、zSecure Audit 製品で提供される機能です。

```
Menu         Options       Info    Commands     Setup      Startpanel
-------------------------------------------------------------------------------
                    zSecure Suite - Resource - CICS
Option  ===> ____________________________________________________________

R   Regions       CICS region reports
T   Transactions  CICS CICS transactions selection and reports
P   Programs      CICS programs selection and reports
```

図 95. CICS リソース・パネル

CICS 領域レポート

図 95 の CICS リソース・パネルで **R** オプションを選択すると、図 96 に示す CICS 領域選択パネルが表示されます。

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、CICS 領域の構成データを制限します。選択基準を指定すると、すべての選択基準に一致するレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (PF1) を使用します。

CICS 領域選択パネルでは、出力および実行オプションを選択することもできます。また、オプションを選択しない場合は、Enter を押すと同時にレポート・データが処理されます。表示される概要パネルには、選択基準に一致する CICS 領域レコードの要約が表示されます。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                    zSecure Suite - CICS - Regions
Command  ===> ____________________________________________________________

Show CICS regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
SYSIDNT . . . . . . . . ________  (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings  _  Region attributes   _  Classes

Output/run options
_  Show differences
_  Print format               Customize title       Send as e-mail
      Background run          Full page form
```

図 96. CICS 領域選択パネル

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」およびオンライン・ヘルプを参照してください。

CICS トランザクション・レポート

図 95 の CICS リソース・パネルで **T** オプションを選択すると、119 ページの図 97 に示す CICS トランザクション選択パネルが表示されます。

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、CICS トランザクション・データを制限します。選択基準を指定すると、すべての基準に一致するそれらのレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (PF1) を使用します。

シミュレート・レポートを作成するには、レポート・タイプ・オプション「**Simulate access for specified resource**」を使用します。

CICS トランザクション選択パネルでは、出力および実行オプションを選択することもできます。また、オプションを選択しない場合は、Enter を押すと同時にレポート・データが処理されます。表示される概要パネルには、選択基準に一致する CICS トランザクション・レコードの要約が表示されます。

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                zSecure Suite - CICS - Transactions
Command  ===> ____________________________________________________________

Show CICS transactions that fit all of the following criteria:
Transaction . . . . . ____      (transaction or filter)
Program . . . . . . . ________  (program name or filter)
Jobname . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . ________  (applid or filter)
SYSIDNT . . . . . . . ____      (identifier or filter)
Complex . . . . . . . ________  (complex or filter)
System  . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource
 Advanced transaction selection criteria
_  Security settings    _  Attributes


Output/run options
1  0. No summary        1. Summarize by region  2. Summarize by transaction
_  Show differences
_  Print format            Customize title         Send as e-mail
      Background run       Full page form
```

図 97. CICS トランザクション選択パネル

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*」およびオンライン・ヘルプを参照してください。

CICS プログラム・レポート

118 ページの図 95 の CICS リソース・パネルで **P** メニュー・オプションを選択すると、 120 ページの図 98 に示す CICS プログラム選択パネルが表示されます。

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、CICS プログラム・データを制限します。選択基準を指定すると、すべての基準に一致するそれらのレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (F1) を使用します。

シミュレート・レポートを作成するには、レポート・タイプ・オプション「**Simulate access for specified resource**」を使用します。

CICS プログラム選択パネルでは、出力および実行オプションを選択することもできます。また、オプションを選択しない場合は、Enter を押すと同時にレポート・データが処理されます。表示される概要パネルには、選択基準に一致する CICS プログラム・レコードの要約が表示されます。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
             zSecure Suite - CICS - Programs
Command  ===> ____________________________________________________________

Show CICS programs that fit all of the following criteria:
Program . . . . . . . . ________  (program name or filter)
Program type  . . . . . 4  1. Program  2. Mapset  3. Partitionset  4. All
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
SYSIDNT . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource
Advanced transaction selection criteria
_  Security settings    _  Attributes

Output/run options
_  0. No summary        1. Summarize by region  2. Summarize by program
_  Show differences
_  Print format            Customize title         Send as e-mail
          Background run    Full page form
```

図 98. CICS プログラム選択パネル

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」およびオンライン・ヘルプを参照してください。

DB2 領域およびリソース・レポート

メインメニューの **RE.D** オプションを使用して、DB2 領域およびリソース・データを選択して表示します。

図 99 に示す DB2 リソース・パネルが表示されます。

```
  Menu         Options       Info    Commands     Setup           Startpanel
-------------------------------------------------------------------------------
                          zSecure Suite - Resource - DB2
Option ===> ____________________________________________________________

R    Regions          Region overview and system privileges (DSNADM, MDSNSM)
BP   Buffer pools     Memory areas that can hold data pages
CL   Collections      Groups of packages with the same qualifier
DB   Databases        Sets of tables, indexes, and table spaces
GV   Variables        Global variables (session scope named memory variables)
JR   Java archives    Sets of files comprising Java applications
PK   Packages         Packages (pre-bound SQL statements)
PN   Plans            Plans (control structures created during BIND)
SC   Schemas          Logical classifications of database objects
SG   Storage groups   Sets of storage objects (volumes)
SP   Stored procs     Stored procedure and user function routines
SQ   Sequences        User defined objects defining a numerical sequence
TB   Tables/views     Tables and views
TS   Table spaces     Table spaces (data set name space for storing tables)
UT   User data types  Distinct types
```

図 99. DB2 リソース・パネル

注: zSecure Admin では、領域レポートのみが使用可能です。

DB2 領域レポート

R メニュー・オプションを選択し、レポート出力内の DB2 データを制限するための基準を指定します。

120 ページの図 99 の DB2 リソース・パネルで **R** メニュー・オプションを選択すると、 図 100 に示す DB2 領域選択パネルが表示されます。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - DB2
Command ===> ____________________________________________________________

Show DB2 regions that fit all of the following criteria:
Jobname . . . . . ________          (jobname or filter)
Local LU name . . . . . ________    (luname or filter)
Local site name . . . . ________    (name or filter)
DB2ID . . . . . ____                (identifier or filter)
Group attachment name   ____        (name or filter)
Complex . . . . . ________          (complex or filter)
System  . . . . . ____              (system or filter)

Advanced selection criteria
_  Region security settings

Output/run options
_  Show differences
_  Print format                Customize title       Send as e-mail
      Background run           Full page form
```

図 100. DB2 領域選択パネル

この選択パネルを使用して 1 つ以上のフィールドに選択基準を入力し、データを制限します。選択基準を指定すると、すべての選択基準に一致するレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (PF1) を使用します。

DB2 領域選択パネルでは、出力および実行オプションを選択することもできます。また、オプションを選択しない場合は、Enter を押すと同時にレポート・データが処理されます。表示される概要パネルには、選択基準に一致するレコードの要約が表示されます。

詳しくは、オンライン・ヘルプおよび「*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。

DB2 リソース・レポート

DB2 出力データを制限するための基準を指定するには、必要とするオプションを表す 2 文字を選択します。

120 ページの図 99 の DB2 リソースのパネルで、必要とするオプションを表す 2 文字を選択します。選択すると、特定の選択パネルが表示されます。例えば、DB2 バッファー・プールの場合は、次のようになります。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - DB2 - Buffer pools
Command ===> ____________________________________________________________

Show DB2 bufferpools that fit all of the following criteria:
Bufferpool name  . . . ________  (name or filter)
DB2ID  . . . . . . . . ____      (identifier or filter)
Complex  . . . . . . . ________  (complex or filter)
System . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  SAF settings          _  Further selection

Output/run options
_  0. No summary         1. Summary by region         2. Summary by bufferpool
_  Show differences
   Print format          _  Customize title        _  Send as e-mail
   _  Background run     _  Full page form
```

図 101. DB2 バッファー・プールの選択パネル

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、データを制限します。フィールドの詳細情報を表示するには、任意のフィールド上で **F1** キーを押します。このフィールド依存のヘルプ機能では、選択パネル上のどのフィールドでフィルターをサポートするかについても説明されます。また、「*IBM Security zSecure CARLa コマンド・リファレンス*」の 『SELECT/LIST Fields』で、各フィールド名の説明を参照することもできます。

選択基準を指定すると、すべての選択基準に一致するレコードのみが出力に含まれます。選択パネルによっては、次のような拡張された選択基準がいくつか含まれているものがあります。

SAF settings
「SAF settings」を選択すると、SAF 設定選択パネルが表示されます。例えば、DB2 バッファー・プールの場合は、次のようになります。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - DB2 - Buffer pools
Command ===> ____________________________________________________________

Show DB2 bufferpool records that fit all of the following criteria:
SAF resource class . . ________  (class or filter)
SAF resource name  . . ____________________________________________________
```

図 102. DB2 バッファー・プールの SAF 設定選択パネル

Further selection
「Further selection」を選択すると、詳細な選択パネルが表示されます。例えば、DB2 スキーマの場合は、次のようになります。

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - DB2 - Schemas
Command ===> ____________________________________________________________

Show DB2 schemas that fit all of the following criteria:
 Number of Datatypes    __  _____  (operator+number)
 Number of Indexes  . . __  _____  (operator+number)
 Number of JARs . . . . __  _____  (operator+number)
 Number of Routines . . __  _____  (operator+number)
 Number of Sequences    __  _____  (operator+number)
 Number of Tables . . . __  _____  (operator+number)
 Number of Triggers . . __  _____  (operator+number)
 Number of Views  . . . __  _____  (operator+number)
```

図 103. DB2 スキーマの詳細な選択パネル

Other settings

「Other settings」を選択すると、その次の選択パネルが表示されます。例えば、DB2 データベースの場合は、次のようになります。

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - DB2 - Databases
Command ===> ____________________________________________________________

Show DB2 databases that fit all of the following criteria:
Authid of owner  . . . ____________________________________________________
Authid of creator  . . ____________________________________________________
Creation date  . . . . __  __________  ________  (operator+yyyy-mm-dd or
Alter date . . . . . . __  __________  ________  ddMMMyyyy + hh:mm:ss or
                                                 hh:mm)

Select flag fields (Y/N/blank)
_  Implicitly created
```

図 104. DB2 データベースのセキュリティー設定選択パネル

出力オプションおよび実行オプションを選択できます。オプションをまったく選択しないことも可能です。レポート・データは、**Enter** キーを押すとすぐに処理されます。次に表示される概要パネルには、選択基準に一致するレコードの要約が表示されます。例えば、DB2 Java アーカイブ・レコード (JAR) の場合は、次のようになります。

```
                DB2 jars display                          Line 1 of 5
Command ===> ____________________________________________ Scroll===> CSR
All DB2 jar records                          3 Jan 2013 07:18
   JAR name                Complex  DB2I Schema   Owner    O Created
__ DS_20110622080035       ADCDPL   DBAG DPACK    DPACK      22Jun2011 08:06
__ DS_20110801131621       ADCDPL   DBAG DPACK    DPACK       1Aug2011 13:18
__ DS_20110822105345       ADCDPL   DBAG DPACK    DPACK      22Aug2011 10:59
__ DS_20110822110830       ADCDPL   DBAG DPACK    DPACK      22Aug2011 11:09
__ DS_20110920131946       ADCDPL   DBAG DPACK    DPACK      20Sep2011 13:21
****************************** Bottom of Data ********************************
```

図 105. DB2 JAR の概要表示レポート

このデータをリストできるのは、zSecure Collect (CKFCOLL プログラム) の APF 許可を受けた実行中に CKFREEZE ファイルが作成された場合のみです。このような CKFREEZE ファイルの作成については、「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」の『zSecure Collect for z/OS』を参照してください。

この概要表示パネルでは、アクション・コマンドを使用できます。例えば、次のようになります。

R 領域情報を表示します。

S 追加情報を表示します。

リソース・レポート、およびレポート・タイプごとの使用できるアクション・コマンドの完全なリストについて詳しくは、オンライン・ヘルプ (F1) および「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」内の 『z/OS のリソース・レポート』を参照してください。

IP スタック・レポート

TCP/IP 構成と統計のデータを選択して表示するには、**RE.I** オプションを使用します。

このデータは、TCPIP=YES パラメーターを指定して zSecure Collect APF 許可を実行して作成された CKFREEZE データ・セットから取得されます。**EV.I** メニュー・オプションを使用して、IP 構成データに関連する SMF イベントのレポートを作成することもできます。

メインメニューから **RE.I** を選択すると、図 106 に示すパネルが表示されます。

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Resource - IP stack Selection
Command ===> ____________________________________________________   _ start panel

Show TCP/IP stack configuration data that fit all of the following criteria:
Stack name . . . . . ________ (name or filter)
System . . . . . ________ (system or filter)
Sysplex  . . . . . ________ (sysplex or filter)

Output/run options
_  Ports                  /  Rules                  _  VIPA
_  Interfaces             _  Routes                 _  Netaccess
_  AUTOLOG                _  Resolver               _  FTP daemon
_  Telnet server/ports
_  Show differences
_  Output in print format     Customize title          Send as e-mail
_  Run in background
```

図 106. 「IP スタック選択」パネル

「IP スタック選択」パネルから、選択基準を入力して TCP/IP スタック構成データを 1 つ以上のフィールドに制限できます。選択基準を指定すると、すべての基準に一致するレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。選択フィールドの説明を表示したり、フィールドでフィルターがサポートされるかどうか判別するには、フィールド・ヘルプ機能 (PF1) を使用してください。

選択パネルでは、出力および実行オプションも指定できます。実行オプションを使用して、特定のタイプの IP 構成データの選択基準をさらに指定できます。出力実行オプションを使用して、レポート・オプションおよび印刷オプションを指定しま

す。これらのオプションのいずれかを選択すると、「IP スタック選択」パネルで Enter を押したときに対応するパネルが表示されます。

出力または実行オプションを選択しなかった場合は、「IP スタック選択」パネルで Enter を押すとすぐにデータが処理されます。概要パネルがすぐに表示され、指定した選択基準に一致した IP 構成レコードの要約が示されます。

これらのレポートについて詳しくは、「*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。

IMS 領域およびリソース・レポート

メインメニューの **RE.M** オプションを使用して、IMS™ の領域、トランザクション、およびプログラムのデータを選択および表示します。レポート・データは、zSecure Collect APF 許可を実行して作成された CKFREEZE データ・セットから取得されます。

RE.M を選択すると、図 107 に示す IMS リソース・パネルが表示されます。

T および **P** オプションは、zSecure Audit 製品で提供される機能です。

```
Menu         Options       Info    Commands     Setup      Startpanel
-------------------------------------------------------------------------------
                          zSecure Suite - Resource - IMS
Option  ===> ____________________________________________________________

R   Regions         IMS control region reports
T   Transactions    IMS transactions reports
P   PSBs            IMS program specification blocks
```

図 107. IMS リソース・パネル

IMS 領域レポート

R メニュー・オプションを選択して、IMS 領域の構成データを制限するための選択基準を指定します。

図 107 の IMS リソース・パネルで **R** メニュー・オプションを選択すると、 126 ページの図 108 に示す IMS 領域選択パネルが表示されます。

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、IMS 領域の構成データを制限します。選択基準を指定すると、すべての選択基準に一致するレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (F1) を使用します。

IMS 領域選択パネルでは、出力および実行オプションを選択することもできます。また、オプションを選択しない場合は、Enter を押すと同時にレポート・データが処理されます。表示される概要パネルには、選択基準に一致する IMS 領域レコードの要約が表示されます。

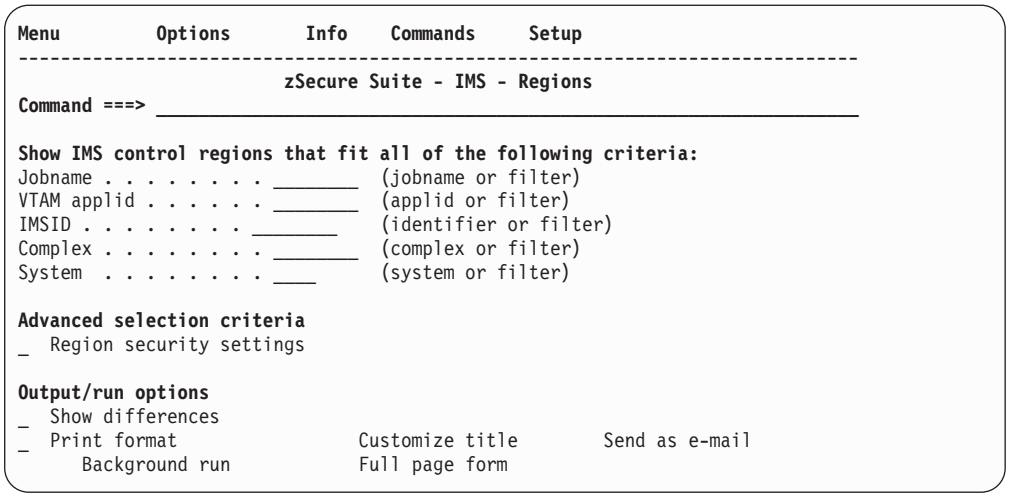


図 108. IMS 領域選択パネル

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*」およびオンライン・ヘルプを参照してください。

IMS トランザクション・レポート

125 ページの図 107 の IMS リソース・パネルで **T** メニュー・オプションを選択すると、 127 ページの図 109 に示す IMS トランザクション選択パネルが表示されます。

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、IMS トランザクション・データを制限します。選択基準を指定すると、すべての基準に一致するそれらのレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (F1) を使用します。

シミュレート・レポートを作成するには、レポート・タイプ・オプション「**Simulate access for specified resource**」を使用します。

IMS トランザクション選択パネルでは、出力および実行オプションを選択することもできます。また、オプションを選択しない場合は、Enter を押すと同時にレポート・データが処理されます。表示される概要パネルには、選択基準に一致する IMS トランザクション・レコードの要約が表示されます。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
              zSecure Suite - IMS - Transactions
Command ===> ____________________________________________________________

Show IMS transactions that fit all of the following criteria:
Transaction . . . . . ________  (transaction or filter)
Transaction class . . . ____    (class number or filter)
Program specif. block   ________  (PSB or filter)
Jobname . . . . . ________  (jobname or filter)
VTAM applid . . . . ________  (applid or filter)
IMSID . . . . . ____      (identifier or filter)
Complex . . . . . ________  (complex or filter)
System  . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced transaction selection criteria
_  Security settings
Output/run options
0  0. No summary   1. Summarize by region  2. Summarize by transaction
_  Show differences
_  Print format           Customize title      Send as e-mail
_     Background run    / Full page form
```

図 109. IMS トランザクション選択パネル

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*」およびオンライン・ヘルプを参照してください。

IMS PSB レポート

125 ページの図 107 の IMS リソース・パネルで **P** メニュー・オプションを選択すると、128 ページの図 110 に示す IMS PSB 選択パネルが表示されます。

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、IMS プログラム仕様ブロック・データを制限します。選択基準を指定すると、すべての基準に一致するそれらのレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (F1) を使用します。

シミュレート・レポートを作成するには、レポート・タイプ・オプション「**Simulate access for specified resource**」を使用します。

IMS PSB 選択パネルでは、出力および実行オプションを選択することもできます。また、オプションを選択しない場合は、Enter を押すと同時にレポート・データが処理されます。表示される概要パネルには、選択基準に一致する IMS PSB レコードの要約が表示されます。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
              zSecure Suite - IMS - PSBs
Command ===> ____________________________________________________________

Show IMS PSBs that fit all of the following criteria:
Program specif. block   ________  (PSB or filter)
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . ________  (applid or filter)
IMSID . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . ________  (complex or filter)
System  . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced PSB selection criteria
_  Security settings

Output/run options
0  0. No summary        1. Summarize by region  2. Summarize by transaction
_  Show differences
_  Print format            Customize title         Send as e-mail
      Background run    /  Full page form
```

図 110. IMS PSB 選択パネル

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」およびオンライン・ヘルプを参照してください。

VTAM アプリケーション・レポート

RE.N オプションを選択して、VTAM アプリケーション・データを制限するための選択基準を指定します。

メインメニューの「**RE VTAM reports**」オプションを使用して、VTAM 設定を選択および表示します。メインメニューから **RE.N** を選択して、図 111 の VTAM アプリケーションの選択パネルを表示します。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                   zSecure Suite - VTAM - Applications
Command ===> ____________________________________________________________

Show VTAM applications that fit all of the following criteria:
Logical Unit name   ________  (name or filter)
ACB name  . . . . . ________  (name or filter)
Current state . . . _____     (code like ACTIV, CONCT, etc, or hex value)
Conv.lvl.security   _  1. ALREADYV  2. PERSISTV  3. CONV  4. AVPV  5. NONE
Complex . . . . . . ________  (complex or filter)
System  . . . . . . ____      (system or filter)

Output/run options
_  1. Summary by system    2. Summary by major node  3. Summary by jobname
_  Show differences
   Print format             _  Customize title     _  Send as e-mail
   _  Background run        _  Full page form
```

図 111. VTAM アプリケーションの選択パネル

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、データを制限します。フィールドの詳細情報を表示するには、任意のフィールド上で **F1** キーを押します。このフィールド依存のヘルプ機能では、選択パネル上のどのフィールドでフィルターをサポートするかについても説明されます。また、「*IBM Security*

zSecureCARLa コマンド・リファレンス」の 『SELECT/LIST Fields』で、各フィールド名の説明を参照することもできます。

出力オプションおよび実行オプションを選択できます。オプションをまったく選択しないことも可能です。レポート・データは、 **Enter** キーを押すとすぐに処理されます。表示される概要パネルには、選択基準に一致する VTAM アプリケーション・レコードの要約が表示されます。

詳しくは、オンライン・ヘルプおよび「*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。

図 112 は、「VTAM application display」レポートの概要表示パネルのサンプルを示しています。

```
                VTAM application display                        Line 462 of 465
Command ===> ____________________________________________________ Scroll===> CSR
All VTAM application records                    1 May 2014 23:42
   LUname   ACBname  Major    System   CurSt DesSt VerifyLU Pre Acq CPa PPO SPO
__ TSO0149  TSO0049  A01MVS   IPO1     CONCT CONCT NONE             CPa
__ TSO0150  TSO0050  A01MVS   IPO1     CONCT CONCT NONE             CPa
__ TVT5004  TVT5004  VTAMSEG  IPO1     ACTIV ACTIV NONE         Acq
__ WUINCM01 WUINCM01 A01CICS  IPO1     CONCT CONCT NONE         Acq CPa
****************************** Bottom of Data ********************************
```

図 112. VTAM アプリケーションの詳細表示

このレポートのデータが使用可能になるのは、zSecure Collect (CKFCOLL プログラム) の APF 許可を受けた実行中に CKFREEZE ファイルが作成された場合のみです。 CKFREEZE ファイルの作成について詳しくは、「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」の『zSecure Collect for z/OS』を参照してください。

MQ 領域およびリソース・レポート

メインメニューの **RE.Q** オプションを使用して、MQ 領域およびリソース・データを選択して表示します。

RE.Q オプションを選択すると、図 113 に示す MQ リソース・パネルが表示されます。

```
 Menu        Options      Info    Commands     Setup          Startpanel
--------------------------------------------------------------------------------
                        zSecure Suite - Resource - MQ
Option ===>

R    Regions         MQ region level settings (MxADMIN)
CH   Channels        Channel definitions
CO   Connections     Applications connected to Queue Manager
IN   Initiators      Channel initiator overview and settings
NL   Namelists       Lists of names
PR   Processes       Process definitions and settings
QU   Queues          Queue definitions and settings
TO   Topics          Topics for Publish/Subscribe usage
```

図 113. MQ リソース・メニュー

注: zSecure Admin では、領域レポートのみが使用可能です。

MQ 領域レポート

R メニュー・オプションを選択して、MQ 領域の構成データを制限するための選択基準を指定します。

129 ページの図 113の MQ リソース・パネルで、**R** メニュー・オプションを選択すると、図 114 に示す MQ 領域選択パネルが表示されます。

```
  Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
                          zSecure Suite - MQ - Regions
Command ===> ____________________________________________________________________

Show MQ regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
Region userid . . . . . ________  (userid or filter)
MQ QMGR name/subsystem  ____      (name or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Output/run options
_  Show differences
_  Print format                Customize title       Send as e-mail
      Background run           Full page form
```

図 114. MQ 領域選択パネル

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、MQ 領域の構成データを制限します。選択基準を指定すると、すべての選択基準に一致するレコードのみが出力に含まれます。一部の選択フィールドではフィルターを使用することができます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (F1) を使用します。

MQ 領域の選択パネルでは、出力オプションおよび実行オプションを選択できます。オプションをまったく選択しないことも可能です。レポート・データは Enter を押すとすぐに処理されます。表示される概要パネルには、選択基準に一致する MQ 領域レコードの要約が表示されます。

詳しくは、オンライン・ヘルプおよび「*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。

MQ リソース・レポート

MQ リソース・レポート内のソース・データを制限するために、必要とするメニュー・オプションを選択できます。

129 ページの『MQ 領域およびリソース・レポート』 に示す MQ リソース・パネルで、必要とするメニュー・オプションを選択します。選択すると、対応する選択パネルが表示されます。例えば、MQ キューの場合は、次のようになります。

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - MQ - Queues
 Command ===> ____________________________________________________________

Show MQ queues that fit all of the following criteria:
Queue name  . . . . . . ____________________________________________________
Queue type  . . . . . . _  1. Alias    2. Local    3. Model    4. Remote
MQ QMGR name/subsystem  ____       (name or filter)
Complex . . . . . . . . ________   (complex or filter)
System  . . . . . . . . ____       (system or filter)

Advanced selection criteria
_  SAF/RACF settings          _  Further selection

Output/run options
_  0. No summary              1. Summary by region   2. Summary by queue
_  Show differences
   Print format               _  Customize title     _  Send as e-mail
   _  Background run          _  Full page form
```

図 115. MQ キュー選択パネル

このパネルを使用して 1 つ以上のフィールドに選択基準を入力し、データを制限します。フィールドの詳細情報を表示するには、任意のフィールド上で **F1** キーを押します。このフィールド依存のヘルプ機能では、選択パネル上のどのフィールドでフィルターをサポートするかについても説明されます。また、「*IBM Security zSecureCARLa コマンド・リファレンス*」の 『SELECT/LIST Fields』で、各フィールド名の説明を参照することもできます。

選択基準を指定すると、すべての選択基準に一致するレコードのみが出力に含まれます。選択パネルによっては、次のような拡張された選択基準が含まれているものがあります。

SAF/RACF settings

「**SAF/RACF settings**」を選択すると、SAF 設定選択パネルが表示されます。例えば、MQ キューの場合は、次のようになります。

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - MQ - Queues
 Command ===> ____________________________________________________________

 Show MQ queue records that fit all of the following criteria:
 SAF resource class  . . ________  (class or filter)
 SAF resource name . . . ____________________________________________________
 RACF Universal access       6  1. None     3. Update   5. Alter
                                2. Read     4. Control  6. Ignore
 RACF ID * access  . . .     6  1. None     3. Update   5. Alter
                                2. Read     4. Control  6. Ignore
 Failure audit access        6  1. None     3. Update   5. Alter
                                2. Read     4. Control  6. Ignore
 Success audit access        6  1. None     3. Update   5. Alter
                                2. Read     4. Control  6. Ignore
                                (operator: < <= > >= = <> ^= )
```

図 116. MQ キュー SAF 選択パネル

Further selection

「Further selection」を選択すると、詳細な選択パネルが表示されます。例えば、MQ チャネルの場合は、次のようになります。

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - MQ - Channels
 Command ===> ____________________________________________________________

Show MQ channels that fit all of the following criteria:
Transmit queue name    ____________________________________________
Userid for channel . . ________  (userid or filter)
Alter date . . . . . . __ __________  (operator+yyyy-mm-dd)

Select flag fields (Y/N/blank)
OR   (AND or OR relationship)
_  Password set for channel             _  SSL Client auth required
```

図 117. MQ チャネルの詳細な選択パネル

出力オプションおよび実行オプションを選択できます。オプションをまったく選択しないことも可能です。レポート・データは、 **Enter** キーを押すとすぐに処理されます。次に表示される概要パネルには、選択基準に一致するレコードの要約が表示されます。例えば、MQ 接続の場合は次のようになります。

```
                MQ connections display                              Line 1 of 1
Command ===> ____________________________________________________ Scroll===> CSR
All MQ connection records                      23 Jun 2014 14:23
   Connect identification                          ExtConn in C_ID  Complex  M
__ C3E2D8C3D8F7C7F14040404040404040CD57AD5515600001 CSQCQ7G1         PLEX1    Q
****************************** Bottom of Data ********************************
```

図 118. MQ 接続の表示

このデータをリストできるのは、zSecure Collect (CKFCOLL プログラム) の APF 許可を受けた実行中に CKFREEZE ファイルが作成された場合のみです。このような CKFREEZE ファイルの作成については、「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」の『zSecure Collect for z/OS』を参照してください。

この概要表示パネルでは、アクション・コマンドを使用できます。例えば、次のようになります。

R 領域情報を表示します。

S 追加情報を表示します。

リソース・レポート、およびレポート・タイプごとの使用できるアクション・コマンドの完全なリストについて詳しくは、オンライン・ヘルプ (F1) および「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」内の 『z/OS のリソース・レポート』を参照してください。

信頼関係レポート

RE.T オプションを選択して、信頼関係の選択基準を指定し、レコード出力を制限します。

メインメニューの **RE.T** オプションを使用して、信頼関係を選択および表示します。

RE.T を選択すると、図 119 に示す「トラステッド」パネルが表示されます。

このパネルを使用して信頼関係の選択基準を入力し、レコード出力を制限します。選択基準は 1 つ以上のフィールドに入力できます。すべての選択基準に一致するレコードのみが出力に含まれます。選択パネルをブランクのままにすると、すべてのレコードが選択されます。一部の選択フィールドでフィルターを使用できます。フィールドがフィルターをサポートするかどうかを調べるには、フィールド・ヘルプ機能 (PF1) を使用します。

信頼関係の選択パネルでは出力および実行オプションを選択することもできます。あるいはオプションを選択しない場合、レポート・データは Enter を押すとすぐに処理されます。表示される概要パネルには、選択基準に一致する信頼関係レコードの要約が表示されます。

```
Menu         Options       Info    Commands     Setup      Startpanel
------------------------------------------------------------------------------
                                  zSecure Suite - Trusted
Command ===> ____________________________________________________________

Show trust relations that fit all of the following criteria:
Complex . . . . . . . . . ________  (complex or filter)
Trust level . . . . . . . __ __     (operator: < <= > >= = <> ^= , number 1-10)

Selection criteria
_  Select/exclude users and access types
_  Select resources

Output/run options
_  1. Summarize by resource  2. Summarize by user
_  Show differences
_  Print format                 Customize title        Send as e-mail
      Background run
```

図 119. 「トラステッド」パネル

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*」およびオンライン・ヘルプを参照してください。

UNIX ファイル・システム・レポート

オプション **RE.U** を選択すると、図 120 に示されている「リソース - UNIX」パネルが開きます。

```
  Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                          zSecure Suite - Resource - Unix
Option  ===> ____________________________________________________________


F    Filesystem      Unix filesystem selection
R    Reports         Unix audit reports
```

図 120. 「リソース - UNIX」メニュー

ファイル・システム - UNIX ファイル・システム・レポート

このオプションは、UNIX ファイル・システムのレコードを選択して表示するときに使用します。完全な CKFREEZE データ・セット読み取り権限が必要

で、CKFREEZE データ・セットが **UNIX=Y** パラメーターを指定して作成されている必要があります。zSecure Collect の実行が APF 許可であった場合、詳細情報が表示されます。

オプション **F** を選択すると、図 121 に示されている「リソース - UNIX 選択」パネルが開きます。

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix Selection
Command ===> ____________________________________________________   _ start panel

Show Unix files that fit all of the following criteria:
Path name  . ____________________________________________________________________
_____________________________________________________________________________
____________________     (name or filter)
 File name  . ____________________________________________________ (name or filter)
 Complex . ________     (complex or EGN mask)

Advanced selection criteria
_  File attributes         _  File system             _  File ACL

Output/run options
_  Show differences
_  Output in print format  _  Customize title         _  Send as e-mail
  _  Run in background
```

図 121. リソース UNIX 選択パネル

選択パネルをブランクのままにすると、すべての UNIX ファイルが選択されます。選択基準として使用する 1 つ以上のフィールドに入力することにより、選択対象の UNIX ファイルを制限することができます。すべての基準と一致するレコードのみが選択されます。一部の選択フィールドではフィルターを使用することができます。「Advanced selection criteria」の 1 つを選択して、UNIX ファイルを選択して表示するためのフィルターを指定することができます。基準を選択すると、必要な属性を指定できるパネルが開きます。

「**Output/Run**」オプションを使用して、レポート実行と出力生成のための設定をカスタマイズします。指定した設定は、ISPF プロファイルに保存され、オプションを提供するすべての UNIX パネルのデフォルト設定になります。

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*」およびオンライン・ヘルプを参照してください。

指定された選択基準を使用した CKFREEZE ファイルの処理が完了すると、135 ページの図 122 に示す「UNIX 要約」パネルが開き、結果が表示されます。

```
IBM Security zSecure UNIX summary                            Line 1 of 26
Command ===> _________________________________________ Scroll===> CSR_
All Unix files                                     28 Aug 2008 00:07
   Complex System  Count
   EEND     EEND     70562
   Count FS mount point
__    24  /
__     2  /home
__     2  /home/crmbhg1
__   205  /u
__     5  /u/automount
__  1713  /u/automount/c2eaudit
__  3105  /u/automount/c2rnew
__   446  /u/automount/smpe
__   730  /u/automount/smpe/smpnts/STP82890/SMPPTFIN
__  1434  /u/automount/C2RSRV#P
__   283  /u/automount/C2RSRV#P/PZ00350
__     1  /u/automount2
__     1  /u/zosmapper
__    11  /EEND
```

図 122. 「UNIX 要約」の表示

図 122 に示されている要約パネル内にリストされているマウント・ポイントのいずれかを選択すると、図 123 に示されているように UNIX ファイルのリストが表示されます。

```
IBM Security zSecure UNIX summary                        Line 1 of 446
 Command ===> _________________________________________ Scroll===> CSR_
 All Unix files                                    28 Aug 2008 00:07
   Complex System  Count
   EEND     EEND     70562
   Count FS mount point
     446  /u/automount/smpe
   T FileMode +  apsl AuF Owner    Group    Relative pathname (within FS)
__ d rwx------        fff CRMBHJ1  ZSECUR   .
__ d rwx------        fff CRMBHJ1  LDAP     smpnts
__ l                  fff CRMBHJ1  LDAP     smpnts/zos19jpn
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/GIMPAF.XML
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/GIMPAF.XSL
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890/SMPHOLD
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPHOLD/S0004.ESMCP
__ d rwx------        fff CRMBHJ1  ZSECUR   smpnts/STP82890/SMPPTFIN
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
```

図 123. 「UNIX 要約」パネル - 選択したマウント・ポイントの UNIX ファイル・リスト

このパネルから以下のアクションを実行できます。

- 通常のファイルを参照するには、ファイルまたはディレクトリー・エントリーの選択フィールドに `B` と入力します。
- ファイルまたはディレクトリーに対して UNIX システム・サービス ISPF シェルを呼び出すには、そのファイルまたはディレクトリーの選択フィールドに `I` と入力します。
- ディレクトリーに対して z/OS UNIX ディレクトリー・リスト・ユーティリティーを開始するには、そのディレクトリーの選択フィールドに `U` と入力します。

135 ページの図 123 に示されているパネルからファイルを表示することを選択すると、 137 ページの図 124 に示されているパネルが開きます。このパネルのファイルの内容を表示するには、「**Absolute pathname**」フィールドの前に S と入力します。

```
IBM Security zSecure UNIX summary                          Line 1 of 57
Command ===> _____________________________________ Scroll===> CSR_
All Unix files                                  28 Aug 2008 00:07



  System view of file
  Complex name                  EEND
  Sysplex name                  NLDLPPLX
  System name                   EEND
_ Absolute pathname             /u/automount/smpe/smpnts/STP82890/GIMPAF.XML
  FS mounted with SECURITY      Yes
  FS mounted with SETUID        No
  FS mounted READ/WRITE         Yes
  Stickysug property profile
  File access attributes        go=,u=rw
  Security label
  Extended file attributes      +s -apl
  Effective audit flags         =f
_ Owner name                    CRMBHJ1 CRMQA097 HZSUSER LDAPSRV OMVS RCCSL01
_ Owner name                    SKRBKDC STRCONS STRTASK TCPSRV
_ Group name                    LDAP SMPE
  Home Directory for Users
  Device                        1648
  Relative audit priority
  Audit concern

  Physical file attributes
  Complex that owns file system EEND
  System that owns file system  EEND
  File system data set name     CRMBOMVS.U.SMPE.HFS
  Volume serial for file system SMPNTS
  File system DASD serial + id  IBM-68-000000065892-0062
  Relative pathname within FS   smpnts/STP82890/GIMPAF.XML
  File type                     -
  Physical access attributes    o=,u=rw,g=r
  Physical extended attributes  +s -apl
  User-requested audit flags    =f
  Auditor-specified audit flags =
  User id                       0
  Group id                      3
  Inode number                  98
  File audit id                 01E2D4D7D5E3E2000F05000000620000
  Number of hard links          1
  Link target

  User     TOrwx ACL id   UID/GID    Name                 InstData
  CRMBHJ1   urw- CRMBHJ1  0          JOHN FRANK
  CRMQA097  urw- CRMQA097 0          TEST QUOTED FORMAT   OMVS HOME TO TEST $QU
  HZSUSER   urw- HZSUSER  0                               Z/OS HEALTH CHECKER
  LDAPSRV   urw- LDAPSRV  0          LDAP SERVER USER
  OMVS      urw- OMVS     0
  RCCSL01   urw- RCCSL01  0          JOHN SMEDLINE SPEC.
  SKRBKDC   urw- SKRBKDC  0          KERBEROS STARTEDTASK NETW AUTH KERBEROS
  STRCONS   urw- STRCONS  0          STC VOOR TSO CONSOLE
  STRTASK   urw- STRTASK  0          DIV STARTED TASK USR
  TCPSRV    urw- TCPSRV   0          TCPIP STARTED TASK
  -group-   gr-- LDAP     3
  -group-   gr-- SMPE     3
  - any -   o--- -other-  n/a




******************************** Bottom of Data ********************************
```

図 124. UNIX 詳細表示

これらのレポートについて詳しくは、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」およびオンライン・ヘルプを参照してください。

レポート - 事前定義 UNIX 監査レポートの実行

zSecure で使用可能な事前定義 UNIX 監査レポートを生成するには、「**レポート**」オプションを使用します。このオプションを選択すると、パネルが開き、選択対象レポートのリストが表示されます。図 125を参照してください。特定のレポートに関する詳細を確認するには、レポート選択フィールドにカーソルを合わせて F1 を押します。オンライン・ヘルプが表示されます。

```
zSecure Suite Display Selection                          3 s elapsed, 0.8 s CPU
Command ===>_____________________________________________ Scroll===> PAGE

  Name     Summary Records Title
_ MOUNT          0       0 Effective UNIX mount points
_ UNIXAPF        0       0 UNIX files with APF authorization
_ UNIXCTL        0       0 UNIX files that are program controlled (daemons etc)
_ UNIXSUID       0       0 UNIX files with SETUID authorization
_ UNIXSGID       0       0 UNIX files with SETGID authorization
_ GLBWUNIX       0       0 UNIX files vulnerable to trojan horse & back door at
_ UIDNOUSR       0       0 UIDs not defined in the complex
_ GIDNOGRP       0       0 GIDs not defined in the complex
_ SHRDUIDS       1     196 OMVS UIDs shared between RACF users
_ OMVSNUID       1      21 RACF users with OMVS segment but no UID
_ SHRDGIDS       1      42 OMVS GIDs shared between RACF groups
_ OMVSNGID       1       2 RACF groups with OMVS segment but no GID
****************************** Bottom of Data ********************************
```

図 125. UNIX レポート・リスト

第 12 章 CARLa コマンド

zSecure Admin and Audit for RACF ISPF パネルでは、実行のために製品に送信されるコマンドが生成されます。これらは、システム・プログラマー向けの便利なツールである CARLa Auditing and Reporting Language (CARLa) のコマンドです。

コマンド生成プロセスは対話式ユーザーには意識されませんが、プロダクト機能をバッチ・モードで使用する場合は重要になります。一般的に、同一の CARLa コマンドを対話モードまたはバッチ・モードのいずれかで使用できます。例えば、基本オプションの 1 つである **CO.C** オプションを使用して、CARLa コマンドを直接指定できます。

ヒント: `=CO.C` と入力する代わりに、パネルのコマンド・プロンプトで基本コマンド `CARLA` を入力して CARLa コマンドを指定することもできます。

製品には多くの CARLa サンプルが提供されています。時間があるときにサンプルをランダムにブラウズして、興味を引くコード・サンプルを実行してください。`CKA$INDX` 索引メンバーを参照することもできます。ここには、CARLa ライブラリー内のすべてのメンバーのリストと簡単な説明が含まれています。また、`SCKRCARL` ライブラリーを参照することもできます。このライブラリーには、ニーズに合わせて使用または調整できる対話式 ISPF レポートおよびバッチ・レポートが含まれています。CARLa および `SCKRCARL` ライブラリ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。

ヒント: `SCKRCARL` ライブラリーを参照するには、以下の手順を実行します。 140 ページの『SCKRCARL ライブラリーのブラウズ』

マニュアルに加え、IBM では以下を提供しています。

- zSecure Admin および zSecure Audit for RACF を頻繁に使用するユーザーを対象とした CARLa プログラミングおよびカスタマー・イネーブルメント・コース。developerWorks® (http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255) には zSecure カスタマー・フォーラムも用意されています。
- developerWorks® 上の「*Hands-on exercises for understanding the basics of the zSecure CARLa Auditing and Reporting Language*」。developerWorks® (http://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home) で `zSecure CARLa training` を検索します。
- このフォーラムおよびその他のリソースへのリンクについては、zSecure IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS2RWS_2.2.0/com.ibm.zsecure.doc_2.2.0/welcome.html) の「**追加情報**」タブを参照してください。

CARLa を使用してカスタム・レポートを定義および書式設定できます。ユーザーが指定した見出しと行書式を使用して、RACF および SMF に認識されている任意のフィールドを使用します。代表的な使用例としては、ユーザーの要件をほぼ満た

す、事前に作成された表示またはレポートを指定します。また、CARLA を使用して、「結果」パネルから表示またはレポートを生成するために使用する CARLa を取り込んで保存します。必要な内容が正確に生成されるように変更することができます。zSecure Admin and Audit for RACF では、サンプルの CARLa 資料の完全なライブラリーである SCKRCARL ライブラリーが提供されています。このライブラリーに新規メンバーを追加したり、独自のライブラリーを作成したりできます。ライブラリーの既存のメンバーは、製品の対話式機能によって使用されるため、これらのメンバーを変更しないでください。

SCKRCARL ライブラリーのメンバーのいずれかを実行するには、『SCKRCARL ライブラリーのメンバーの実行』に記載されている手順のとおりに行います。

CARLa プログラムをカスタマイズするには、143 ページの『CARLa プログラムのカスタマイズ』に記載されている手順のとおりに行います。

サンプル CARLa プログラムを作成するには、144 ページの『サンプル CARLa プログラムの作成』に記載されている手順のとおりに行います。

CARLa プログラムを保存して後で使用するには、このプログラムをユーザー専用のデータ・セットにコピーします。

プログラムをコピーするには、最初の CARLa 行の行番号フィールドにコマンド C9999 を入力します。次に、コマンド域に CREATE を入力します。これで、PDS にメンバーを作成 (または置換) するための通常の ISPF 編集機能を使用できるようになります。

保存した CARLa プログラムを再実行するときは、145 ページの『保存された CARLa プログラムの実行』に記載されている手順のとおりに行います。

SCKRCARL ライブラリーのブラウズ

SCKRCARL ライブラリーをブラウズして、ISPF レポートとバッチ・レポートを対話式に表示できます。組織の要件に応じて、これらのレポートを使用および調整してください。

手順

1. ISPF のもとで、製品内から TSO ISRDDN コマンドを発行します。
2. F SCKRCARL と入力して、アクティブな SCKRCARL ライブラリーを探します。
3. 「**B**」(ブラウズ) 機能を使用して、SCKRCARL ライブラリーを開きます。

   最上部にある CKA$INDX メンバーでは、使用可能なメンバーとその機能がリストされます。

SCKRCARL ライブラリーのメンバーの実行

以下のタスクを実行して、SCKRCARL コマンド・ライブラリーからのメンバーを表示、編集、および実行できます。

このタスクについて

ISPF では、現行 SCKRCARL コマンド・ライブラリーからのメンバーを表示、編集、および実行できます。DD 名 CKRCARLA を介してアクセスします。

手順

1. メインメニューからオプション **CO** (コマンド) を選択します。Enter を押すと、図 126 に示されているパネルが開きます。

   このパネルはライブラリー・コマンドを実行するために使用されます。

```
 Menu         Options       Info    Commands     Setup           Startpanel
------------------------------------------------------------------------------
                         zSecure Admin+Audit for RACF - Commands
Option ===> ____________________________________________________________________

 1      Libraries       Select and maintain command library
 2      Members         Work with members from current command library
 3      Edit            Edit member from current command library
 4      Run             Run member from current command library
 5      Submit          Run member from current command library in background
 C      Command         Type in any CARLa command



 Member name . . . . ________     (If 3, 4 or 5 selected)
 Two pass query  . . N  (Y/N, option 4 only)

 Current library . . DD:CKRCARLA
 Input complex . . . Input set created 8 Apr 2005
 Current mask type . EGN
```

図 126. ライブラリー・コマンドを実行するために使用されるコマンド (CO)

2. オプション **2** (メンバー) を選択して Enter を押してメンバーを選択するか、実行するメンバーの名前をユーザー・リファレンス・マニュアルの中から見つけます。

   この例では、メンバー CKRLMTX3 を使用します。

3. メンバー機能を使用する場合、メンバー・リストからメンバー名 (CKRLMTX3 またはリファレンス・マニュアルから選択したメンバー名) を見つけるか、「コマンド」パネルの「**メンバー名**」フィールドにメンバー名を入力します。
4. メンバー・リストから、使用するメンバー (CKRLMTX3 など) の前で行コマンド **E** を発行します。「コマンド」パネルで、オプション **3** (編集) を入力して Enter を押します。

   142 ページの図 127 に示すように、選択された CARLa メンバーを示すパネルが表示されます。

```
EDIT       CKR.SCKRCARL(CKRLMTX3) - 01.00                        Columns 00001 00080
Command ===>                                                       Scroll ===> CSR
****** ********************************* Top of Data ***********************************
=NOTE= Enter GO or RUN to execute commands, SUB or SUBMIT to generate batch job
000001  /*************************************************BeginModule********
000002  * LICENSED MATERIALS - PROPERTY OF IBM
000003  * 5655-T01
000004  * Copyright IBM Corp. 1989, 2007
000005  * All Rights Reserved
000006  * US Government Users Restricted Rights - Use, duplication or
000007  * disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
000008  * File-stamp: <050621 MR 12:44:08 CKRLMTX3.SCKRCARL>
000009  * FMID: HCKR1C0 RMID: HCKR1C0 IBM Security zSecure Base 1.12.0
000010  * Purpose:
000011  *     List ACL matrix
000012  * Notes:
000013  *     Imbed this member after a selection newlist RACFSEL, e.g.:
000014  *
000015  *     n name=racfsel outlim=0
000016  *     select c=dataset s=base qual=SYS1
000017  *     sortlist qual
000018  *     i m=ckrlmtx3
000019  *
000020  * History:
000021  * 011015 1.2.0 SDG ERZ120: Created
000022  * 050621 1.7.0 MR  EZ0506016: Added execute & RACFSEL
000023  *************************************************EndModule********/
000024
000025  n type=racf title='Data set access matrix'
000026   def alter(aclid,8,'Alter')
000027    subselect acl(access=alter and missing(whenprof))
000028   def control(aclid,8,'Control')
000029    subselect acl(access=control and missing(whenprof))
000030   def update(aclid,8,'Update')
000031    subselect acl(access=update and missing(whenprof))
000032   def read(aclid,8,'Read')
000033    subselect acl(access=read and missing(whenprof))
000034   def exec(aclid,8,'Execute')
000035    subselect acl(access=execute and missing(whenprof))
000036   def condacc(aclaccess,1,'C')
000037    subselect acl(exists(whenprof))
000038   def hdr_o('o',1,hdr$blank) true where((key='^')) /* always FALSE */
000039   def cond(aclid,'nditional')
000040    subselect acl(exists(whenprof))
000041
000042   select c=dataset s=base likelist=racfsel
000043   sortlist key(35) uacc alter control update read exec condacc,
000044   | hdr_o | cond
****** ******************************** Bottom of Data ********************************
```

図 127. CKCARLA ライブラリーのメンバー CKRLMTX3

ソフトウェアを含むデータ・セットの更新は、インストール中および保守にのみ行ってください。カスタマイズされたメンバーが必要な場合は、そのメンバーを自分のデータ・セットに保存します。これらのデータ・セットを使用するには、構成パラメーター **WPREFIX** または **UPREFIX** を使用します。

次のタスク

選択された CARLa プログラムには、1 つ以上のプロファイルについて付与されるアクセス権限のマトリックスが表示されます。レポートを作成するプロファイルを選択するために、CARLa プログラムを一部カスタマイズする必要があります。元のメンバーの変更を避けるために、 143 ページの『CARLa プログラムのカスタマイズ』の手順では一時コピーを操作する方法を示します。

CARLa プログラムのカスタマイズ

始める前に

140 ページの『SCKRCARL ライブラリーのメンバーの実行』を完了します。

手順

1. メンバーを誤って変更せずに編集セッションを確実に終了するために、CANCEL コマンドを発行します。
2. オプション 4 (実行) を入力します。 カスタマイズはまだ実行されていないため、このオプションを使用すると、正しくない LIKELIST に関する構文エラーが出されます。
3. PF3 を押すと、「結果」パネルが開きます。「**コマンド**」行の前に E を入力して、Enter を押します。 ここからは、CARLa プログラムの一時的コピーを編集します。
4. プログラムをカスタマイズします。

   カスタマイズは、ヘッダーの **Notes** セクションに記載されています。このプログラムは、他のプログラムから組み込む目的で作成されています。このプログラムを組み込むには、選択 newlist (15 行から 17 行) を記述し、プログラムをその直後 (18 行) に組み込みます。

   選択 newlist を CARLa プログラムの先頭に追加しても、同じ結果が得られます。
5. 15 行から 17 行を 23 行の直後にコピーします。 (* を削除してコメントを外します。)
6. 表示するプロファイルに一致するように、クラス (c=data set) および HLQ (qual=sys1) 指定を変更します。
7. 「**コマンド**」行に Go または Run と入力して、このプログラムを実行します。144 ページの図 128 に示すレポートに類似したレポートが開きます。

```
BROWSE - IBMUSER.C2R10FE.REPORT  ------—------------ LINE 0000 0.5 s CPU, RC=0
 COMMAND ===>                                          SCROLL ===> CSR
******************************** Top of Data ***********************************
P R O F I L E   L I S T I N G    4 Apr 2005 00:50
Access matrix

Profile key                       UACC    Alter    Control  Update   Read
SYS1.*.**                         READ    SYS1                       C#MA
                                          SYSPROG
                                          P390
SYS1.*.MAN*.**                    NONE    SYSPROG  STRTASK           C#MBRACF
                                                                     C#MARACF
                                                                     C#MBDSCT


SYS1.BRODCAST                     NONE    SYSPROG           *
                                                            C#MBWTK
                                                            C#MBWT3
SYS1.CMDLIB                       READ    SYS1                       C#MA
                                          SYSPROG
SYS1.C#M.LINKLIB                  READ    SYS1                       C#MA
                                          SYSPROG
SYS1.CSSLIB                       READ    SYS1                       C#MA
```

図 128. CARLA アクセス・マトリックス

次のタスク

既存のサンプルを実行する代わりに、独自の CARLa プログラムを作成できます。『サンプル CARLa プログラムの作成』では、小さい CARLa プログラムを実行して、CARLa プログラミングの意味を理解します。

サンプル CARLa プログラムの作成

始める前に

140 ページの『SCKRCARL ライブラリーのメンバーの実行』および 143 ページの『CARLa プログラムのカスタマイズ』をお読みください。

手順

サンプル CARLa プログラムを作成するには、以下のステップを実行します。

1. メインメニューからオプション **CO** (コマンド) を選択し、ライブラリー・コマンドを実行できるようにするために、 141 ページの図 126 に示されているパネルを開きます。
2. オプション **C** (コマンド) を選択して、PDF エディターを開きます。
3. エディター・ワークスペースで、以下の CARLa ステートメントを入力します。*c#mb* は、ユーザー ID を所有するシステム内の RACF グループに変更します。

```
newlist type=racf file=ckrcmd nopage
  select class=user owner=c#mb segment=base
  list 'alu' key(8) 'owner(newowner)'
```

図 129. CARLa サンプル・プログラム

この小さい CARLa プログラムによって、所有者を変更する RACF コマンドが生成されます。*c#mb* の現在所有しているすべてのユーザー・プロファイルが選択され、所有者フィールドは newowner に変更されます。出力 (RACF コマンド) は CKRCMD ファイルに書き込まれ、**RUN** コマンドで処理できるようになります。78 ページの『「結果」パネル』を参照してください。

出力は、図 130 に示されるような出力になります。

```
/* CKRCMD file CKR1CMD complex DEMO NJE JES2DEMO generated 27
alu C#MBHEN  owner(newowner)
alu C#MBERT  owner(newowner)
alu C#MBJVO  owner(newowner)
```

図 130. CARLa サンプル・プログラムの出力

保存された CARLa プログラムの実行

始める前に

144 ページの『サンプル CARLa プログラムの作成』を読んでおきます。

手順

保存した CARLa プログラムを実行するには、次の手順で行います。

1. メインメニューで CO と入力し、Enter を押します。
2. 「コマンド」パネルで 1 (ライブラリー) を入力し、Enter を押します。
3. 任意の明細行で I (挿入) 行コマンドを入力し、Enter を押して行を挿入します。
4. 専用ライブラリーの名前を入力します。必要に応じて引用符を使用します。Enter を押します。
5. ライブラリーを行コマンド **S** で選択し、Enter を押します。
6. PF3 を押して「コマンド」パネルに戻ります。

   ライブラリーの名前が「**現行ライブラリー**」フィールドに表示されます。
7. CARLa プログラムのメンバー名を「**メンバー名**」フィールドに入力します。
8. オプション **4** (実行) を選択します。

第 13 章 標準的な管理および監査タスク

以下のトピックでは、Security zSecure Admin and Audit for RACF での標準的な管理および監査タスクを実行する方法について説明します。

- 『ユーザーの削除』
- 『ユーザーがアクセス可能なデータ・セットの表示』
- 『ロード・ライブラリー監査』
- 148 ページの『表示パネルのデータの印刷』
- 148 ページの『検索基準に基づくプロファイルの検索』
- 149 ページの『「すべて保護」検査機能』
- 149 ページの『コマンド機能』

ユーザーの削除

このタスクについて

あるユーザーの RACF アクセス資格情報を削除する必要があって、ユーザー ID が分からない場合、zSecure Audit for RACF **RA.U** 機能を使用できます。名前検索パターンを入力してユーザー ID を検索し、ユーザーがアクセスできるデータ・セットを判別します。その後、削除するユーザー・プロファイルを選択できます。

手順

1. 「**コマンド**」行に `RA.U` と入力して、「RACF ユーザー」パネルを開きます。
2. 「**Programmer Name**」フィールドに、「**Programmer Name**」フィールドの名前のどこかに一致するすべてのユーザー・プロファイルを表示するためのユーザー名または名前パターンを入力します。
3. Enter を押して、結果を表示します。
4. RACF からユーザーを削除するには、ユーザー・プロファイルの前に `D` と入力して、Enter を押します。

ユーザーがアクセス可能なデータ・セットの表示

手順

特定ユーザーがアクセス可能なすべてのデータ・セットをリストするには、RACF **レポート許可/有効範囲機能** (オプション **RA.3.4**) を使用します。

ロード・ライブラリー監査

zSecure Audit for RACF の**ライブラリーの監査**機能 (オプション **AU.L**) を使用すると、標準の z/OS ツールまたは RACF ツールでは検出が難しい状況を簡単に検出できます。

これらの状況 (ロード・ライブラリーとソース・ライブラリーの両方) には、以下のものがあります。

- ロード・ライブラリーがクリーンかどうか (特にシステム・ライブラリーおよび APF ライブラリー)。
- モジュールが複数存在するかどうか (別の名前で、おそらく別の所有者プロファイルを使用して)。
- 同じモジュールが複数のライブラリーに存在するかどうか。

注: 1 つのコピーが廃止されたものであるにもかかわらず、ライブラリー検索順序が原因で、何らかのジョブによって知らずに呼び出されると、重大な問題の原因になることがあります。

表示パネルのデータの印刷

PRT コマンドを使用して、表示出力の検査時にデータを印刷します。

表示機能の出力を検査するとき、データの印刷が必要になる場合があります。そのような場合は **PRT** コマンドを使用します。出力は ISPF LIST データ・セットに出されます。より複雑なレポートについては、**RESULTS** コマンドを使用して、最後の機能によって生成されたすべてのファイルを確認します。このパネルからも印刷できます。

検索基準に基づくプロファイルの検索

一致機能は非常に役立つ場合があります。この機能は、指定されたデータ・セットまたは一般リソースをカバーするすべてのプロファイルを検索します。

この機能は以下のパネルにあります。

- データ・セット・プロファイル: オプション「**RA.D**」データ・セット
- 一般リソース・プロファイル: オプション「**RA.R**」リソース
- RACF レポート一致: オプション「**RA.3.7**」

「**RA.D**」および「**RA.R**」の場合は次のようになります。

- 「**3 Match**」では、プロファイル・フィールドがリソース名として扱われ、そのリソース名と最もよく一致するプロファイルが選択されます。「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」の **BESTMATCH** パラメーターを参照してください。
- 「**4 Any match**」では、プロファイル・フィールドがリソース名として扱われ、そのリソース名と一致する可能性のあるすべてのプロファイルが選択されます。「*IBM Security zSecure Admin and Audit for RACF: ユーザー・リファレンス・マニュアル*」の **MATCH** パラメーターを参照してください。

「**RA.3.7**」は「**Any match**」と同様に動作します。RACF によって使用されるプロファイルは最初の行にあります。最初のプロファイルが削除されると、その他のプロファイルが使用されます。計画または管理が不十分であった場合、アクセス・リストおよび UACC の値が異なる複数のプロファイルが 1 つのデータ・セットをカバーする結果になります。

「すべて保護」検査機能

「すべて保護」環境の使用を検討する場合が生じます。多くの作業を伴う可能性があるものの、ほとんどの z/OS インストール済み環境ではその検討が行われます。「すべて保護」の検査機能を試してみてください。SMS、HSM、または ABR を使用する場合、「**すべて保護**」機能のサブメニューの MIGRAT ボリュームを除外する場合があります。このアクションにより、不要メッセージの数を大幅に削減することができます。特に、**PROTECT ALL** を使用しない RACF 環境で、この**検査**機能は役立ちます。この機能では、「すべて保護」を使用するために行う必要がある作業の概略を示し、RACF 保護を持たないすべてのデータ・セットの一覧を提供します。

コマンド機能

1 次パネルのオプション **CO** である**コマンド**機能を試します。

139 ページの『第 12 章 CARLa コマンド』を参照してください。

付録. よくある質問

このセクションでは、よくある質問と詳細な回答のリストを提供します。

表 12. よくある質問

Q: メインパネルが空白なのはなぜですか?

A: XFACILIT クラスの CKR.** プロファイルに対する READ アクセス権限が必要です。CKR.** プロファイルでは、機能の使用を許可または禁止できます。

Q: どの機能が zSecure Admin のもので、どの機能が zSecure Audit for RACF のものかが分かりません。これらの機能はどのように区別できますか?

A: 「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」を確認してください。マニュアルには、各機能がサポートする製品を示すチェック・ボックスが示してあります。LIMIT FOCUS=AUDITRACF をプリアンブル SETUP PREAMBLE (SE.3) に追加して、使用可能な機能を zSecure Audit の機能のみに制限することもできます。

Q: COPY USER アクションの一部として DEFINE ALIAS をどのように生成するのですか?

R **A:** カタログ情報は CKFREEZE データ・セットに由来します。したがって、使用する入力ファ
R イルのセットに CKFREEZE データ・セットを含める必要があります。CKFREEZE データ・セッ
R トを作成するには、パネルからオプション **SETUP NEWFILES** を使用して、JCL を生成する必
R 要があります。この JCL を保存し、Tivoli Workload Scheduler または類似の製品を使用し
R て、JCL を毎朝早くに実行します。CKFREEZE データ・セットは大きくなることがあるため、
R **SYSIN** パラメーターを使用してサイズを削減します。最初に大きな CKFREEZE を作成し、APF
R を使用して、パラメーターを指定せずにこれを実行します。

R この CKFREEZE 設定での zSecure Admin の実行が遅すぎる場合、パラメーター
R **VTOC=NO,CAT=MCAT,BCD=NO,MCD=NO,TMC=NO,RMM=NO,UNIX=NO** を追加します。ユーザー (ユーザーの
R データ・セットを含む) を削除する場合は、大きな CKFREEZE が必要になります。

R また、**RA.U** オプションのユーザー・プロファイルの前に、行コマンド **MT** (TSO の管理) を
R 入力することもできます。その後で、既存のユーザーのための別名と ISPF プロファイル・
R データ・セットを定義できます。ただし、この代わりの方法では、ユーザーの別名を追加する
R カタログの名前を知っておく必要があります。

Q: 別のシステム上のアンロード済み RACF および CKFREEZE ファイルの情報を収集して、この情報を特定のシステムに送信して表示および分析できますか?

A: すべてのシステムがライセンス交付を受けたものであれば可能です。これは、Security zSecure Admin and Audit for RACF の典型的な使用法です。

Q: 行コマンド **L** からの出力が、zSecure Admin および zSecure Audit for RACF によってレポートされた情報と一致しません。何が問題なのですか?

A: RACF の入力データ・ソースを確認してください。おそらく、アンロードされた RACF からレポートを作成しています。一方、**L** 行コマンドは、アクティブな RACF データベースからの情報を常に表示します。

表 12. よくある質問 (続き)

Q: 共有 JES2 スプール環境 (1 つの RACF データベースと複数の z/OS イメージ) はどのように扱うのですか?

A: ライブ RACF データを使用する場合を除いて、すべてのシステムから RACF アンロードを 1 回実行します。それぞれのシステム上で 1 つずつ、複数の zSecure Collect ジョブを実行します。2 番目以降の zSecure Collect for z/OS ジョブに対して **SHARED=NO** パラメーターを使用できます。**SHARED=NO** パラメーターを使用すると、作成される CKFREEZE データ・セットのサイズが減ります。このアクションを実行できるのは、共有環境を正確に反映するために、UCBが **SHARED** オプションを使用して正しく定義されている場合に限られます。そうでない場合、zSecure Collect for z/OS はすべてを処理します。これらの複数の CKFREEZE データ・セットが定義された INPUT SET を作成します。

Q: zSecure Admin および zSecure Audit for RACF とともに、稼働中の RACF データベースをいつ使用しますか? アンロードされたデータはいつ使用しますか? 古いデータベースのコピーはいつ使用しますか?

A: 稼働中の RACF データベースは、単純な*臨時の* 照会および日常的なルーチンの RACF 管理に使用します。RACF データベースのアンロードされたコピーを使用するのは、広い範囲の分析作業を行う場合と、RACF データをすぐに変更する意図がない場合です。「再作成」機能を使用する予定の場合、アンロードされたデータベースにはパスワードが含まれていないため、必ず古いデータベース・コピーから実行してください。RACF データを別のシステムから操作する場合、このデータはアンロードされます。ただし、その別のシステムの RACF データベースが共有 DASD 上にあり、通常のデータ・セットとして直接アクセスされている場合はアンロードされません。あえて簡単に表現すれば、*管理者* は通常、稼働中の RACF データベースを使用し、*監査員* は通常、アンロードされたコピーを使用するということになります。

Q: レポートされたすべてのプロファイルについて 2 行が含まれているレポートが生成されました。この問題は何が原因なのですか?

A: この問題の原因は 2 つ考えられます。パネルを使用してこの概要を作成した場合、行が二重に作成された原因としては、**SETUP** アプリケーションで 2 つの RACF データ・ソースを選択したことが考えられます。 CARLa を使用した場合、SELECT 文でキーワード SEGMENT=BASE を指定し忘れたことによってもこれと同じ問題が発生する場合があります。

Q: SETUP INPUT オプションを使用して入力セットを定義しました。zSecure Admin および zSecure Audit for RACF を次回使用するとき、セットアップ値が保存されていませんでした。これはなぜですか?

A: 2 回目に別の TSO ユーザー ID を使用した可能性があります。セットアップ情報はご使用の ISPF プロファイルに保存され、各 TSO ユーザー ID は独自の ISPF プロファイル・データ・セットを持っています。また、最後に使用した入力ファイルを使用する **SETUP** オプションもあります。このオプションの設定について調べるには、**SETUP RUN** を参照してください。

Q: Security zSecure Admin and Audit for RACF は、さまざまなレポートの多くの z/OS 制御を検査します。製品はこれらの制御をいつ z/OS ストレージから取得するのですか。また、CKFREEZE データ・セットをいつ使用しますか?

表 12. よくある質問 (続き)

A: 完全 チェックの場合、Security zSecure Admin and Audit for RACF は、CKFREEZE データ・セットにコピーされた z/OS 制御ブロックを使用します。これは、ストレージ内の z/OS データを使用するよりも複雑ですが、より一貫性の高い結果が得られます。結果は CKFREEZE データが収集されたタイミングで意味があります。このため、システムが完全にロードされて最もアクティブなときに CKFREEZE データを収集した方が良い場合もあります。リモート z/OS システムについて調べることができることも意味します。リモート・システムで作成された CKFREEZE ファイルおよびRACF アンロード・データを使用します。

Q: アンロードされた RACF データベースを分析作業に使用しています。修正が必要な箇所を見つけると、zSecure Admin および zSecure Audit for RACF によって生成される RACF コマンドを通常は使用します。場合によっては、これらのコマンドを編集して問題を修正することもあります。ただし、アンロードされた RACF データベースは履歴データを表しています。稼働中の RACF データベースで同じ問題がまだ生じているかどうか確認するには、どうすればよいですか?

A: 大規模な変更を RACF に送信する前に、「セットアップ」パネルで別の入力 セットを使用して稼働中の RACF データベースに切り替えます。問題を検出した表示を繰り返します。問題がやはり存在する場合、RACF の変更を実行します。

Q: 「AUDIT STATUS」パネルなどの一部のパネルでは、完全な CKFREEZE データ・セットと他のタイプの CKFREEZE データ・セットを区別します。これはなぜですか?

A: この評価ガイドの指示を使用して*新規*入力 ファイルを定義し、更新ジョブを実行すると、完全な CKFREEZE データ・セットが作成されます。大規模であるか広範囲に分散したインストール済み環境では、CKFREEZE データ・セットが大きくなる可能性があります。監査および比較の目的で複数の CKFREEZE データ・セットを保存する場合もあります。zSecure Collect for z/OS には、潜在的な CKFREEZE データの一部のみを収集するオプションがあります。複数の CKFREEZE データ・セットを使用すると役に立ちます。例えば、フリーズ機能を使用してさまざまなライブラリーの変更内容を検出する場合や、監査員が特定の定義された時点でのシステム・スナップショットを必要とする場合に有用です。

Q: **RACF/MASS UPDATE/COPY USER** 機能を使用してユーザーを複製しますが、ターゲット (新規ユーザー) が既に定義されています。この問題をどのように処理すればよいですか?

A: 既存のターゲット・ユーザーの一部の権限を保持する場合、**コピー**機能を使用し、「**Generate RACF commands when the target user exists**」の前に / を入力します。このアクションにより、ターゲットの既存の権限は、ソース・ユーザーの権限と矛盾しない限り、そのままになります。矛盾が発生する場合、最終的な権限は、コマンドが何であるか (追加または変更) に依存して、ソース・ユーザーまたはターゲット・ユーザーによって決定されます。ソース・ユーザーの権限レベルが低いと、ターゲット・ユーザーの既存の権限レベルが一部低下することもあります。

Q: 既存のユーザー ID にコピーを試行したとき、メッセージ CKR0536 を受け取ります。

A: 編集を開始する下準備としてコマンドのセットを用意しようとしているときは、「**Generate RACF commands when the target user exists**」の前に / を指定することで、メッセージを抑止できます。ユーザー属性をマージする標準の方法は、MERGE を使用することです。

Q: 日次のセキュリティー管理を実行する必要があります。どの RACF データ・ソースを使用しますか?

表 12. よくある質問 (続き)

A: 日次のセキュリティー管理の場合、最新の RACF データベースを使用します。このデータベースは、アクティブなプライマリー RACF データベースでもアクティブなバックアップ RACF データベースでもかまいません。アクティブなプライマリー・データベースへの変更は即時にアクティブなバックアップ RACF データベースに複製されます。アクティブなバックアップ・データベースはアクセス検査処理に使用されないため、これを入力データ・ソースとして使用することをお勧めします。これを実施することで、レポートの実行中に、システムの他のユーザーのためにアクセス検査処理を実行するとき、RACF データベースのパフォーマンスが低下しません。

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]

D

E

F

G

I

J

L

M

O

P

R

S

T

U

V

W

X

Z

Printed in Japan

GI88-4318-02

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