zSecure Command Verifier
バージョン 2.3.0

ユーザー・ガイド

SA88-7158-04

zSecure Command Verifier
バージョン 2.3.0

ユーザー・ガイド

IBM

SA88-7158-04

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、 265 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。

2017 年 **8** 月

本書は、IBM Security zSecure Command Verifier (製品番号 5655-N19) のバージョン 2 リリース 3、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： SC27-5648-04
zSecure Command Verifier
Version 2.3.0
User Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

本書について

本書では、IBM® Security zSecure™ Command Verifier のインストールと使用に関する情報を提供します。IBM Security zSecure Command Verifier は、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します。最初の 3 つの章では、製品の目的、プロダクト機能、およびインストール手順の概要を示します。残りの章では、監査機能とインストール・ポリシー・プロファイルについて説明し、ポリシー定義とメッセージに関する参照情報を提供します。

本書は、以下のような読者を対象としています。

- IBM Security zSecure Command Verifier のインストールを担当するシステム・サポート担当者。 11 ページの『第 3 章 zSecure Command Verifier のインストール』を参照してください。
- IBM Security zSecure Command Verifier によって提供される追加 RACF コマンド制御の実装を担当するセキュリティー管理者。 45 ページの『第 5 章 ポリシー・プロファイル』を参照してください。
- 端末ユーザーが発行または実行した RACF コマンドについて、そのレポートの設計と作成を担当する監査員。以下のセクションを参照してください。
  - 1 ページの『第 1 章 概要』
  - 7 ページの『第 2 章 製品の概要』
  - 21 ページの『第 4 章 コマンドおよびポリシーの効果の監査』
  - 45 ページの『第 5 章 ポリシー・プロファイル』

IBM Security zSecure Command Verifier ポリシーは、RACF プロファイルを使用して実装されます。読者は、RACFの概念と RACF コマンドを理解している必要があります。ポリシーを実装するユーザーは、通常の RACF (総称) プロファイルおよび RACF コマンド・キーワードを完全に理解している必要があります。

このマニュアルには、RACF の使用に関する説明は記載されていません。しかし、xiii ページの『関連資料』に RACF 文書リソースがリストされています。

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 zSecure Suite (z/OS) または IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から入手できます。IBM Knowledge Center は、IBM 製品資料のホームです。IBM Knowledge Center をカスタマイズし、独自の資料の集合を作成して、使用するテクノロジー、製品、およびバージョンを表示するように画面を設計できます。トピックにコメントを追加したり、Eメール、LinkedIn、Twitter で話題を共有したりすることで、

IBM や同僚と対話することもできます。ライセンス出版物の入手手順については、『ライセンス文書の入手』を参照してください。

表 *1.*

製品の **IBM Knowledge Center**	**URL**
IBM zSecure Suite (z/OS)	www.ibm.com/support/knowledgecenter/SS2RWS/welcome
IBM zSecure Manager for RACF z/VM	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 2.3.0 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 ファイルまたは個々のライセンス出版物の PDF ファイルを入手するには、tivzos@us.ibm.com まで E メールをお送りください。IBM Security zSecure Suite 2.3.0 のライセンス出版物のアクセスを要求してください。会社の IBM お客様番号と、ご希望の連絡先情報を合わせて記入してください。ご注文を処理するための詳細が送信されます。

IBM zSecure Suite ライブラリー

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

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

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

- 『このリリースについて』には、リリース固有の情報に加え、zSecure 固有ではない、より一般的な情報が含まれています。リリース固有の情報には、以下が含まれます。
  - 新機能: zSecure V2.3.0 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。
- 関連資料: zSecure に関連する情報のタイトルおよびリンクのリストです。
- 問題解決に対するサポート: 問題解決策が IBM の知識ベースで見つかる場合がよくあります。また、製品のフィックスが提供されている場合があります。IBM ソフトウェア・サポートに登録すると、IBM の週次 E メール通知サービスサービスを購読できます。IBM サポートでは、製品の問題点に関するサポートや、よくある質問への回答を提供するほか、問題解決の支援も行っています。

- *IBM Security zSecure CARLa* 駆動コンポーネント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/CA-Top Secret
  - IBM Security zSecure Alert for RACF and CA-ACF2
  - IBM Security zSecure Visual
  - IBM Security zSecure Adapters for SIEM for RACF/CA-ACF2/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, SC43-2894

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- プログラム・ディレクトリー*: IBM Security zSecure CARLa* 駆動コンポーネント (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 駆動コンポーネント (Admin、Audit、Visual、Alert および IBM Security zSecure Adapters for SIEM) のインストールに関連した資料と手順に関する情報が記載されています。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  製品インターフェースおよび RACF の管理機能と監査機能の使用方法について説明します。このマニュアルには、CARLa コマンド言語と SELECT/LIST フィールドの参照情報が掲載されています。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手順も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。
- *IBM Security zSecure CARLa* コマンド・リファレンス, LC43-2107

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

  ライセンス交付を受けた製品資料と受けていない製品資料が含まれる IBM Security zSecure Manager for RACF z/VM 資料を提供します。
- *Program Directory for IBM zSecure Manager for RACF z/VM, GI11-7865*

この資料の情報を効果的に使用するには、プログラム・ディレクトリーから取得できる一定の前提知識が必要です。「*Program Directory for IBM 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。ここには、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。プログラム・ディレクトリーは、プロダクト・テープで提供されます。IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から最新のコピーをダウンロードすることもできます。

関連資料

このセクションでは、zSecure に関連する情報のタイトルおよびリンクを記載します。

参照先	対象
IBM Knowledge Center: IBM Security zSecure	zSecure のすべての非ライセンス資料。 特定のリリースに固有の情報、システム要件、非互換性などについては、目的のバージョンを選択し、「このリリースについて」を選択します。『新機能』および『リリース・ノート』を参照してください。
IBM Knowledge Center: z/OS	z/OS に関する情報。表 2 に、zSecure で最も役立つ資料をいくつか示します。
z/OS Security Server Documentation	リソース・アクセス管理機能 (RACF)、および zSecure Admin and Audit を使用して報告されるイベントのタイプに関する詳細情報。 RACF コマンド、および各種キーワードの意味については、「*z/OS Security Server RACF* コマンド言語解説書」および「*z/OS Security Server RACF* セキュリティー管理者のガイド」を参照してください。RACF によって記録される各種イベントの情報については、「*z/OS Security Server RACF* 監査担当者のガイド」を参照してください。

表 2. *zSecure* で使用するのに最も役立つ *z/OS* の資料

資料タイトル	資料番号
z/OS Communications Server: IP 構成解説書	SC27-3651
z/OS Integrated Security Services エンタープライズ識別マッピング *(EIM)* ガイドおよび解説書	SA88-7076
z/OS MVS プログラミング*:* 高水準言語向け呼び出し可能サービス	SA88-7103
z/OS MVS システム・コマンド	SA88-5490
z/OS Security Server RACF セキュリティー管理者のガイド	SA88-5804
z/OS Security Server RACF 監査担当者のガイド	SA88-5718
z/OS Security Server RACF コマンド言語 解説書	SA88-6226
z/OS Security Server RACF マクロおよびインターフェース	SC43-2673
z/OS Security Server RACF メッセージおよびコード	SA88-5839
z/OS Security Server RACF セキュリティー管理者のガイド	SA88-5804

表 2. *zSecure* で使用するのに最も役立つ *z/OS* の資料 (続き)

資料タイトル	資料番号
z/OS Security Server RACF システム・プログラマーのガイド	SA88-7029
z/Architecture® 解説書	SA88-8773

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。この製品では、インターフェースを音声出力してナビゲートする支援技術を利用できます。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

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

zSecure の技術研修の情報については、zSecure 公開 Wiki の zSecure Training ページを参照してください。

サポート情報

IBM サポートは、コード関連の問題や、通常の短期インストールまたは使用方法に関する質問にお答えします。IBM ソフトウェア・サポート・サイトへは、www.ibm.com/software/support/probsub.html から直接アクセスできます。

適切なセキュリティーの実践に関する注意事項

IT システム・セキュリティーには、企業内外からの不正アクセスからの保護、検出、および対処によってシステムおよび情報を保護することが求められます。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは 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

MVS オペレーティング・システムのリソースとユーザーは、RACF 内でプロファイルを使用して記述することができます。ほとんどすべてのリソースは、データ・セットであっても、CICS トランザクションであっても、あるいはそれ以外であっても、リソース・プロファイルを使用して記述できます。RACF では、歴史的にデータ・セットが他のタイプのリソース (一般リソースと呼ばれます) と区別されます。この区別は RACF コマンド構文にも反映されており、データ・セット用と一般リソース用に 2 つの異なるコマンド・セットが使用されています。

ユーザー・プロファイルではユーザーが記述されます。ユーザーは、効率を高めるために RACF グループ に収集されます。これらのグループは、以下の目的に使用できます。

- リソースにアクセスするため
- プロファイルを変更する権限を与えるため

リソースへのアクセスは、リソース・プロファイルによって制御されます。リソース・プロファイルには、個別プロファイルと総称プロファイルがあります。

- 1 つの個別 プロファイルで 1 つのリソースが記述されます。
- 1 つの総称 プロファイルでゼロ個または複数個の異なるリソースが記述されます。

主に使用されるのは総称プロファイルです。リソース・プロファイルには、汎用アクセス権限 (UACC) および 2 つの形式のアクセス・リスト (ACL) が含まれています。UACC は、ユーザーが ACL に指定されていない場合に全員に付与されるアクセス権限を制御します。標準 ACL は、ユーザーとグループ、およびそれぞれのアクセス権限のリストです。条件付き ACL は、ユーザー、およびユーザー個々のアクセス権限と組み合わせられている条件 (プログラム、端末、コンソールなど) のリストです。

プロファイルを変更する権限は、プロファイルの所有権に基づいています。プロファイルの所有者は、既存の RACF ユーザーまたはグループであることが必要です。ユーザーを所有者として指定した場合は、その特定ユーザーのみがプロファイルの保守を許可されます。グループを所有者として指定した場合は、グループ内で管理権限 (つまり、**グループ** SPECIAL) を持つすべてのユーザーがプロファイルを保守できます。

ユーザーやリソースと同様に、グループも RACF でプロファイルによって記述されます。これらのグループ・プロファイルにも、同様に所有者があります。グループ・プロファイルの所有者は、グループの定義の変更をユーザーに許可することができます。ただし、**グループ** SPECIAL が許可方式として使用される場合は、**グループ** SPECIAL のユーザーには、そのグループのサブグループの多くに対する権限も与えられます。この**グループ** SPECIAL 権限のパーコレーションについて詳しくは、「*RACF* セキュリティー管理者のガイド」を参照してください。グループ・レベルのユーザー属性については、グループとユーザーの定義に関する章を参照してください。

RACF プロファイルを定義、変更、および削除する権限は、RACF プロファイル自体に基づいています。場合によっては、**システム** SPECIAL などの他の権限も使用できますが、これらの権限は通常のユーザーが使用できる標準の権限ではありません。ただし、プロファイルに保管される属性または新しい値を RACF が何らかの方法で制御することはほとんどありません。例えば、グループの所有者は、システム内の任意のユーザーを自分のグループに接続できます。RACF は、どのユーザーが接続または除去されるかを検査しません。もう 1 つの例として、プロファイルの所有者および ACL を変更する場合が挙げられます。所有者は、他のユーザーまたはグループを新しい所有者として指定することができます。事実上、所有者は自身の所有するすべてのプロファイルを任意のユーザーに引き渡すことができます。

これらの例は、インストールで発生を防止する必要のある典型的なタイプのアクションです。多くの場合、どのプロファイルと属性が変更されるかを制御するだけでなく、何に変更されるかも制御する必要があります。例えば、許可されたユーザーが所有者の値を Joe ではなく Mary に変更できるように指定したい場合があります。zSecure Command Verifier では、それを行うことができます。
任意のプロファイルの任意のフィールド、オプション、または属性の新しい値を制御します。

RACF コマンド

RACF コマンドを使用して、RACF プロファイルの追加、変更、削除、およびシステム全体のオプションの定義を行うことができます。

RACF コマンドを実行できるのは、RACF で定義されているユーザーだけです。ユーザーは、ほとんどの RACF コマンドを実行できますが、コマンドに指定したプロファイルに対するコマンドの実行が許可されているかどうかが RACF によって検査されます。ほとんどの RACF コマンドは、TSO 環境から実行できます。また、MVS™ オペレーター・コンソールからしか実行できない RACF コマンドもあります。現在、従来の TSO RACF コマンドは TSO 環境に限定されなくなりました。これらのコマンドは、オペレーター・コンソール、RACF パラメーター・ライブラリー、および R-Admin RACF 呼び出し可能サービスから実行することも可能です。オペレーター・コンソールから実行する場合は、コンソール・オペレーターがログオンしている必要があります。また、権限はオペレーターのユーザー ID に基づきます。

歴史的に、RACF コマンドはプロファイルのタイプによってグループ化されています。このグループ化は、ユーザーとグループには役立ちますが、データ・セットと一般リソースにはそれほど役立ちません。特に **PERMIT** コマンドは、一般リソース・プロファイルに対するアクセス権限を許可しようとする人を混乱させることがよくあります。RACF の長い歴史は、個別プロファイルの実装や、UACC などのデータ・セット属性の自動設定で使用可能なユーザー属性からも見て取ることができます。RACF ISPF パネル・インターフェースを使用することで、旧バージョンの RACF の来歴や互換性に起因する問題の一部が軽減されます。

コマンドに関連する問題の一部は、RACF の基本原理が原因です。

> プロファイルの所有者は、プロファイルの任意の属性を変更できますが、その属性を変更しても所有者の権限やアクセス権が高くならないことが条件となります。

一部のインストール済み環境では、この柔軟性をユーザーに与えるのは望ましくない場合があります。ユーザーは、アクセス規則を変更して、自分のリソースに対する RACF アクセス制御を事実上無効にすることができます。RACF コマンドを完全に禁止するか、出口コードを記述することにより、この脅威レベルを低下させることができます。どちらの解決策にも、それぞれに欠点があります。(RACF プログラム制御を使用するなどして) コマンドを禁止すると、リソースの所有者による正当な変更も妨げられます。標準の RACF 出口では、インストールに必要な制御量が提供されないことがよくあります。『RACF コマンド出口』を参照してください。以下のセクションでは、zSecure Command Verifier で導入された柔軟な制御点について説明します。

RACF コマンド出口

このセクションでは、RACF によってサポートされるいくつかのタイプの出口について説明します。これらのほとんどは、RACF プロファイル内のフィールドの値を検査する目的には適していません。zSecure Command Verifier は、フィールドおよびフィールド値を管理する権限を定義するために、単純なポリシー・プロファイルを使用するインターフェースを提供します。

1 つ目のカテゴリーは、RACF 出口ではなく MVS 出口、すなわちシステム許可機能 (SAF) 出口で構成されます。これらの出口は、システム・コンポーネントがセキュリティー製品の機能を必要とするすべてのインスタンスで開始されます。ただし、ほとんどの RACF コマンドについては、検査対象のプロファイルがまだ存在しないために、これらの出口は開始されません。それ以外の場合では、RACF コマンド自体が、ストレージ内に既にある情報または RACF データベースから直接取得した情報に基づいて、検査を行います。

出口の 2 つ目のカテゴリーは、RACF SVC 処理出口で構成されます。RACF SVC 処理が行われている間に、プリプロセッシング出口とポストプロセッシング出口が開始されます。これらの出口は、主に低レベル機能に対する RACF の動作を限定的に変更するためのものです。これらの出口を誤用し、追加の処理を組み込む可能性がありますが、それはこの出口の目的とする機能ではありません。また、一部の RACF コマンドでは、これらの出口を使用する特定の `RACROUTE` 要求が使用されません。

出口の 3 つ目のカテゴリーは、データ・セット命名規則用の出口です。その名前が示すように、これらの出口は、データ・セット名が存在する場合または暗黙指定されている場合にのみ RACF コマンド処理で開始されます。一方、ほとんどのコマンドの場合は、データ・セット・プロファイルが関係しないため、これらの出口は呼び出されません。

出口の次のカテゴリーは、パスワード関連出口で構成されます。新しいパスワード出口は、パスワードまたはパスワード・インターバルが変更されたときにのみ呼び出されます。暗号化出口は、RACF データベースで新規パスワードを暗号化する必要がある場合などに呼び出されます。これらの出口は、パスワードやその他の暗号化データが関係しないコマンドに対しては呼び出されません。

RACF には、ACEE 圧縮/拡張出口もありますが、この出口は RACFRW 出口と同様に RACF コマンド処理には関係しません。

OS/390® リリース 3 以降は、RACF で共通コマンド出口も提供されています。この出口は、ほとんどの RACF コマンドに対して呼び出されます。この出口が提供されるまでは、RACF コマンドにインストール制御を実装することは困難でした。この出口の主な欠点は、コマンド・ストリングが 1 つの引数として渡されるために、その内容を解析して解釈する複雑な作業がすべて出口に加えられることです。この出口については、以下が適用されます。

- コマンド・ストリングを禁止または変更できます。
- コマンド名を変更できません。
- 追加のコマンドを生成できません。

標準の RACF コマンド出口

標準の RACF コマンド出口を使用する理由はいくつかあります。

「*RACF* システム・プログラマーのガイド」に、RACF 出口の使用例がいくつか記載されています。

- パスワード品質の制御
- 再開とパスワード・リセットを行う SPECIAL ユーザーを限定

RACF 出口がその他の目的で使用される場合もあります。一部のインストールでは、RACF 出口は以下の目的で使用されます。

- 選択したユーザーに対してパスワード・インターバルを強制的に短縮する
- 非標準の権限を持つユーザーの監査属性を設定する
- データ・セットの UACC に対する変更を防ぐ
- アクセス・リストに対するユーザー ID「*」の追加を防ぐ

パスワード品質制御は、新規パスワードを、禁止されている単語のリストまたは現在のパスワード内の文字と比較することによって行うことができます。一例として、QWERTY や LKJHGF などのキーボード・パターンの検査や、MARCH や APRIL などの月名の検査が挙げられます。現在のパスワードとの比較では、「同じ位置の同一文字が 4 つ以上」などを使用できます。この 2 番目の検査では、例えば現在のパスワードが QP10AL である場合に QP11AL というパスワードが無効となります。

RACF 出口のさらに高度な利用法の 1 つを以下で説明します。この例では、データ・セットの UACC に対する変更を防止する試みについて説明します。

データ・セットの UACC に対する変更を防ぐ作業には、いくつかの RACF 出口が関係します。最初の出口は、RACF コマンド内部で使用される特殊な形式の `RACROUTE REQUEST=AUTH` のために呼び出されます。この出口は、それだけでは不十分です。`RACROUTE REQUEST=DEFINE` で呼び出される RACF 出口と組み合わせる必要があります。ただしこの組み合わせも、データ・セット・プロファイルの UACC 設定にユーザーが影響を与えるあらゆる状況に確実に対応できるわけではありません。

これらのタイプの出口は、プロファイルのすべての必要な側面を制御するには不十分です。このため、OS/390 リリース 3 で RACF が新たな出口点を持つようにな

りました。この共通コマンド出口は、ほとんどの RACF コマンドの実行前と実行後に呼び出されます。ただし、RACF ではこの出口に以下の制約事項があります。

- RRSF のキーワード AT および ONLYAT は事前に処理され、コマンドから取り除かれます。
- デフォルト値が既に指定されているため、端末ユーザーがどのキーワードを指定したかを確認できません。
- コマンドそのものを変更することはできません。

また、このような出口をコーディングすることは簡単ではありません。その主な理由は、キーワードが長い文字ストリングの形式で指定されるためです。TSO コマンド構文 (括弧と引用符付きストリングを含む) の処理については、多くの人々が複雑で難しい作業と考えています。zSecure Command Verifier が追加のセキュリティー管理を実装するための有効な方法であるのは、一部には、この理由によります。zSecure Command Verifier のもう 1 つの利点は、アセンブラーやその他のプログラミング・スキルが不要であることです。ポリシー・プロファイルによってインストール・ポリシー・ルールを定義できます。構文解析、検査、エラー・メッセージ、および監査証跡の生成が zSecure Command Verifier によって処理されます。

zSecure Command Verifier を使用して RACF をモニターすることの利点

ここでは、zSecure Command Verifier がどのように RACF コマンドにアクセスし、当該コマンドを処理するかについて説明します。

zSecure Command Verifier は、RACF で提供される他のほとんどの出口よりも早い段階で RACF コマンドをインターセプトします。このため、インストールでは、重要な RACF 処理が行われる前に、RACF コマンドのキーワードを検査できます。さらにインストールでは、RACF コマンド・プロセッサーが、これらの変更されたキーワードと、端末ユーザーが入力したキーワードとを区別できないようにキーワード変更を行うこともできます。一方、zSecure Command Verifier は、TSO コマンド・キーワードの通常のプロンプト表示を実行できるように、十分に遅い段階でインターセプトを行います。ただし、この後者の機能はすべてのキーワードでサポートされているわけではありません。一部のキーワード検証は、コマンドの最終処理中にしか行えず、したがって、端末のプロンプト表示に適格ではありません。

コンソール・オペレーターは RACF コマンドを実行できますが、すべてのオペレーター・コマンドが zSecure Command Verifier によってインターセプトされるわけではありません。zSecure Command Verifier は、**DISPLAY** や **SIGNOFF** などの元のオペレーター・コマンドはインターセプトしませんが、**ALTUSER** や **LISTUSER** などのその他の RACF コマンドはインターセプトします。

z/OS では、RACF 機能を実行するための USS 呼び出し可能サービスも提供しています。この R_Admin サービスは、一部の事前定義機能を実行できるほか、すべての TSO RACF コマンドにも使用できます。これらの RACF コマンドは、RACF アドレス・スペースにおいて、USS プロセスに関連付けられた RACF ユーザー ID

の権限の下で実行されます。これらのコマンドは、標準の RACF 共通コマンド出口 (IRREVX01) も呼び出すため、zSecure Command Verifier によって制御することもできます。

zSecure Command Verifier の現行バージョンでは、RACF コマンドや実行環境の各種ソースが区別されません。実行環境には、TSO、オペレーター・コマンド、RRSF 伝搬コマンド、R_Admin コマンドなどがあります。

前提ソフトウェア

zSecure Command Verifier ポリシー・プロファイルを実装する前に、このトピックに記載したソフトウェア・サポート・レベルが満たされていることを確認してください。

zSecure Command Verifier を正しくインストールして機能させるには、少なくとも表 3 に示すソフトウェア・レベルが必要です。これより低いリリースの RACF で製品の一部をインストールすることはできますが、そのような使用法はサポートされていません。zSecure Command Verifier は、以下のレベルでテストされており、サポートされています。

表 *3. zSecure Command Verifier* に必要なソフトウェアとレベル

製品	サポートされているレベル
z/OS	1.13 以降
SMP/E for z/OS	3.5 以降

第 2 章 製品の概要

zSecure Command Verifier は、RACF コマンドに対する出口として実装されます。使用されるのは、RACF 共通コマンド出口 (IRREVX01) です。

zSecure Command Verifier ルーチンは、RACF コマンド・プロセッサーによって開始されます。これらのルーチンは、端末ユーザーが入力したキーワードとパラメーターをスキャンし、それらを RACF コマンド・プロセッサーに渡します。受け入れられるキーワードのみが RACF コマンド・プロセッサーに渡されます。以降の説明では、コマンドを実行するユーザーのことを端末ユーザーと呼びます。この用語は、RACF コマンドを実行するその他すべての方法にも適用されます。例えば MVS オペレーター・コンソールやバッチ・ジョブからコマンドを実行する場合などです。実行されるステップは以下のとおりです。

1. 端末ユーザーによって入力されたコマンドが分析され、検査されます。明らかな構文エラーがユーザーに報告され、ユーザーはそのエラーを修正する必要があります。このプロセスは、標準の RACF コマンド・インターフェースに似ています。
2. コマンドが構文的に正しい場合は、キーワードとパラメーターが内部フォーマットに変換されます。このフォーマットにより、zSecure Command Verifier インストール・ポリシー変換処理および適用ルーチンが容易にキーワードとパラメーターにアクセスできるようになります。
3. キーワードとパラメーターは、`XFACILIT` リソース・クラス内の `C4R` プロファイルで指定されたインストール・ポリシーに対して評価され、突き合わされます。キーワードとパラメーターがインストール・ポリシーに違反している場合は、コマンドが拒否されるか、キーワードが抑止されます。

   インストール・ポリシー・プロファイルでは、ユーザーが入力した RACF コマンドの前に実行されるプリコマンド、およびユーザーが入力した RACF コマンドの後に実行されるポストコマンドを、1 つずつ指定できます。
4. 1 つ以上のコマンドが実行されます。通常は、コマンドを実行するための端末ユーザーの権限が zSecure Command Verifier によって変更されることはありません。権限が不十分であるためにコマンドが失敗する可能性があります。ポリシーで指定されたプリコマンドとポストコマンドは、端末ユーザーが指定したコマンド、キーワード、またはパラメーターの受け入れとは無関係に実行されるので注意が必要です。また、いずれかのコマンドが完全に ABEND (異常終了) すると、一連のコマンド全体 (プリコマンド、ポリシーで受け入れられたコマンド、ポストコマンドなど) が終了する可能性があります。
5. 監査は、`XFACILIT` リソース・クラス内の特定の C4R プロファイルに対する監査専用の `RACROUTE REQUEST=AUTH` によって行われます。これらのプロファイルと関連する監査オプションについて詳しくは、9 ページの『zSecure Command Verifier でのプロファイル監査』を参照してください。

RACF がコマンドを処理する方法

zSecure Command Verifier では、RACF 共通コマンド出口を呼び出すすべての RACF コマンドが検査されます。検査済みの RACF コマンドの処理において、RACF がこれらのコマンドを処理する通常の方法と軽微な不一致があります。この不一致は、反復キーワードの処理に関係しています。

場合によって、RACF で反復キーワードのすべてのパラメーター値が処理されたり、最後の指定のみが使用されたりします。以下に例を示します。

- ALTUSER *userid* CICS(ADDOPCLASS(01) ADDOPCLASS(02)) を指定すると、RACF によって両方の OPCLASS が追加されます。
- 一方、ALTUSER *userid* ADDCAT(cat1) ADDCAT(cat2) を指定すると、RACF によって 1 つのカテゴリーのみが追加されます。

zSecure Command Verifier では、キーワードの最後に指定された値のみが使用され、同じキーワードに対するそれ以外の指定はすべて無視されます。

共通コマンド出口を開始しない RACF コマンド

一部のコマンドは、zSecure Command Verifier によって処理できないか、例外的な方法で処理されます。

以下のリストに、これらのコマンドの説明を示します。

RVARY

RVARY コマンドに対して保護を実装すると、余計な問題が発生するリスクが高まるため、zSecure Command Verifier では **RVARY** のサポートが実装されていません。RACF 製品コードでは、可用性に関する同様の懸念に基づき、**RVARY** は特別な位置付けとなっています。

RACLINK

RACF での RACF リモート共有機能 (RRSF) の実装環境では、**RACLINK** コマンドとそのキーワードおよびパラメーターが、RRSFDATA リソース・クラス内の RACF プロファイルによって保護されています。

RACDCERT

RACF では、**RACDCERT** コマンドが RACF コマンド・エンベロープで処理されないコマンドとして実装されています。このため、このコマンドは共通コマンド出口点を開始しません。幸い、**RACDCERT** コマンドの使用は、SPECIAL 権限および FACILITY クラス内のプロファイルによって制御されます。以下の説明は、「*RACF* コマンド言語解説書」からの抜粋です。

RACDCERT コマンドを実行するには、以下のいずれかの権限が必要です。

- SPECIAL
- FACILITY クラス内のリソース IRR.DIGTCERT.*function* に対する十分な権限 (*function* は、LIST、ADD、ALTER、DELETE のいずれか)
- 機能を自分で実行する IRR.DIGTCERT.*function* に対する READ 権限
- 機能を他のユーザーのために実行する IRR.DIGTCERT.*function* に対する UPDATE 権限

このように既存の制御を組み合わせることで、zSecure Command Verifier の制御の必要が少なくなります。

RACPRIV

RACPRIV コマンドは、ユーザーのアドレス・スペースにおける書き込み特権の状況にのみ影響します。RACF データベース内のプロファイルには影響せず、他のシステムに伝搬することもできません。このコマンドの使用は、IRR.WRITEDOWN.BYUSER プロファイルによって部分的に制御されます。このため、zSecure Command Verifier では追加の制御が実装されていません。

RACMAP

RACMAP コマンドでは、分散 ID フィルターの作成、削除、およびリストを行います。このコマンドは、コマンド・ダイレクションを使用する他の RRSF ノードへのルーティングには適格ではなく、RACF 出口も開始しません。このコマンドは、FACILITY クラス内の IRR.IDIDMAP.*function* (*function* は MAP、DELMAP、LISTMAP のいずれか) という形式のプロファイルを使用して制御できます。

RACMAP コマンドについて詳しくは、「*RACF* コマンド言語 解説書」を参照してください。

インストール・ポリシー

zSecure Command Verifier では、コマンド、キーワード、およびパラメーターに関する決定のためのポイントが必要となります。多数のさまざまな選択肢が考えられるため、インストールでは、どの基準に基づいてどの 決定を行う必要があるかを指定しなければなりません。これを行うには、XFACILIT リソース・クラス内のポリシー・プロファイルの定義を使用します。

これらのプロファイルについて詳しくは、45 ページの『第 5 章 ポリシー・プロファイル』を参照してください。

zSecure Command Verifier でのプロファイル監査

XFACILIT リソース・クラス内の特定の C4R プロファイルの定義を使用することで、監査員は SMF にログとして記録されるイベントを指定できます。

この製品では、すべての RACF コマンドを対象に、端末ユーザーが入力したコマンド、および最終的に実行されたコマンドをログに記録できます。両方をログに記録するように指定することも可能です。監査員は、SMF による監査を、選択したユーザーと全ユーザーのどちらを対象に行うかを指定できます。生成された SMF レコードからは、各コマンドの最初の 255 文字のみが得られます。

端末ユーザーに出されたエラー・メッセージは、C4R.ERRMSG.*command* プロファイルから SMF レコード内の LOGSTR として入手できます。

監査の指定に使用されるプロファイルの例を以下に示しています。この例は、全ユーザーを対象に、**ADDUSER** コマンドを処理前にインストール・ポリシー・プロファイルに従って監査する必要があることを示しています。ユーザー **IBMUSER** によって実行された ADDUSER は、監査しないように指定しています。

```
C4R.PREAUD.ADDUSER UACC(READ) AUDIT(SUCCESS(READ))
             ACL: IBMUSER NONE
```

注: パスワードや暗号鍵などの機密フィールドは、SMF にログとして記録される前に RACF コマンドから除去されます。

詳細については、 21 ページの『第 4 章 コマンドおよびポリシーの効果の監査』を参照してください。

C4RSTAT コマンドによる製品のバージョンと状況の確認

C4RSTAT コマンドを使用して、zSecure Command Verifier の状況とバージョンを確認する必要があります。

C4RSTAT コマンドは、メインコードが RACF 共通コマンド出口の一部として活動化されているかどうか、および現行セッションのポリシー解釈/適用ルーチン (C4RPIER) が見つかるかどうかを検査します。また、ポリシー・プロファイルに使用されるリソース・クラス、定義されているポリシー・プロファイルの数も示されます。

以下の図は、**C4RSTAT** コマンドからの出力例です。

```
C4R982I zSecure Command Verifier is active
C4R971I EXIT version is 2.3.0
C4R973I PIER version is 2.3.0
C4R985I Resource class used for policy profiles is XFACILIT
C4R976I Resource class is active
C4R969I Generic profiles are enabled
C4R978I Number of policy profiles is 29
```

図 *1. CR4STAT* コマンドの出力

第 3 章 zSecure Command Verifier のインストール

以下のトピックのガイドラインに従って、zSecure Command Verifier を本番環境にインストールします。

zSecure Command Verifier のインストールは、SMP/E を介して行われます。

インストールの前に、使用する zSecure Command Verifier のバージョンが、システム上でアクティブな z/OS with RACF のレベルに一致することを確認してください。

インストールの準備

以下では、インストールのための zSecure Command Verifier のパッケージ方法について説明します。

zSecure Command Verifier は、2 つの SMP/E 機能の形式で出荷されます。1 つ目の機能には、構文解析とコマンド・ビルドのコードがすべて含まれています。2 つ目の機能には、ポリシー制御コードがすべて含まれています。製品を使用するには、両方の機能が必要です。

zSecure Command Verifier のインストールは、いくつかのステップで構成されています。システム・ライブラリーに実行可能モジュールを作成するほかに、製品を活動化するためにいくつかのオペレーター・コマンドを実行したり Parmlib メンバーを更新したりする必要があります。

リソース・クラスの選択

インストール・モジュール C4REXP を更新し、XFACILIT クラスと同じ属性でリソース・クラスを定義して、リソース・クラスを変更するには、以下のガイドラインに従ってください。

zSecure Command Verifier ポリシー・ルールは、XFACILIT リソース・クラス内のプロファイルによって定義されます。別のリソース・クラスを使用することも可能ですが、デフォルトのリソース・クラスを使用するのが最も推奨されます。

リソース・クラスを変更する場合は、インストール・モジュール C4REXP を更新し、XFACILIT クラスと同じ属性でリソース・クラスを定義する必要があります。

管理者は、XFACILIT リソース・クラス内のプロファイルを使用して zSecure Command Verifier のポリシー・ルールを定義します。別のリソース・クラスを使用することもできます。ただし、デフォルトのリソース・クラスを使用するのが最も適切です。

zSecure Command Verifier 制御プロファイルに必要なリソース・クラスには、以下の特性が必要です。

- プロファイルの長さは最大 246 文字。

- デフォルトの戻りコードには 4 または 8 を指定できます。多くの場合、zSecure Command Verifier ではデフォルトの戻りコードが無視されます。
- 最初の文字は英数字として、それ以外の文字は任意の文字として指定されている必要があります。
- パフォーマンス上の理由から、RACLIST が許可されている必要があります。SETROPTS によってリソース・クラスを RACLIST するかどうかを指定できます。リソース・クラスが SETROPTS で RACLIST されない場合は、最初の RACF コマンド呼び出し時に、そのクラスが GLOBAL ONLY RACLISTed されます。

インストール手順の概要

このチェックリストを使用して、zSecure Command Verifier インストール・プロセス中に実行するタスクを追跡します。このチェックリストには、インストール・プロセスの概要と、各タスクの詳細情報へのリンクが記載されています。

各タスクの実行方法については、次の表にある、手順へのリンクを参照してください。

表 *4. SMP/E* インストールのインストール・チェックリスト

ステップ	手順	ジョブ名
1	『ステップ 1: データ・セット命名規則の定義』	
2	13 ページの『ステップ 2: インストール JCL の読み込み』	
3	13 ページの『ステップ 3: SMP/E ゾーンの作成と初期化』	C4RJSMPA C4RJSMPB C4RJSMPC
4	15 ページの『ステップ 4: SYSMOD の受け付け』	C4RJREC
5	15 ページの『ステップ 5: TARGET データ・セットと DLIB データ・セットの割り振り』	C4RJALL
6	16 ページの『ステップ 6: SMP/E DDDEF の更新』	C4RJDDD
7	16 ページの『ステップ 7: zSecure Command Verifier コードの追加』	C4RJAPP
8	16 ページの『ステップ 8: ポリシー・プロファイル用のリソース・クラスの指定』	C4RJEXP
9	16 ページの『ステップ 9: APF 許可された TSO コマンドの Parmlib の更新』	C4RJIKJ
10	17 ページの『ステップ 10: zSecure Command Verifier の活動化とテスト』	Parmlib オペレーター・コマンド
11	19 ページの『ステップ 11: zSecure Command Verifier 製品の受け入れ』	C4RJACC

ステップ 1: データ・セット命名規則の定義

SMP/E をインストールする前に、インストール・プロセスで使用するデータ・セット命名規則を設定します。

以下のデータ・セットをはじめとする、すべての必要なデータ・セット・タイプの規則を定義します。

- インストール JCL を含んだデータ・セット (SC4RINST)
- SMP/E 制御データ・セット (CSI や PTS など)
- インストールされたソフトウェア用のシステム・データ・セット

ステップ 2: インストール JCL の読み込み

zSecure Command Verifier インストール・プロセスで使用される JCL は、SC4RINST データ・セットにあります。

テープからインストールする場合は、以下の JCL を使用して以下のデータを DASD データ・セットにコピーします。

```
//jobname   JOB (account info),'Copy install JCL',
//             CLASS=a,MSGCLASS=r
//*-------------------------------------------------------------------
//FILE8  EXEC PGM=IEBCOPY
//SYSUT2   DD DISP=(NEW,CATLG),UNIT=SYSALLDA,SPACE=(CYL,(1,1,10)),
//            DSN=userid.C4R230.INSTJCL
//SYSUT1   DD DISP=SHR,VOL=(,RETAIN,SER=C4R230),UNIT=3480,
//            LABEL=(6,SL),DSN=IBM.JC4R230.F3
//SYSPRINT DD SYSOUT=*
//SYSIN    DD DUMMY
```

このジョブが正常に実行されたら、『ステップ 3: SMP/E ゾーンの作成と初期化』に進むことができます。

ステップ 3: SMP/E ゾーンの作成と初期化

zSecure Command Verifier インストール・プロセスを開始する前に、インストール用の SMP/E ゾーンを決定します。

以下のインストール・オプションから選択できます。

- 既存の z/OS ゾーンにインストール
- 既存の CSI 内の新規 (専用) ゾーンにインストール
- 新規の CSI 内の新規 (専用) ゾーンにインストール

3 番目のオプションにのみ、サンプルのインストール・ジョブが用意されています。

既存のゾーンに製品をインストールする場合は、SMP/E CSI またはゾーンを定義する必要はありません。直ちに、 15 ページの『ステップ 4: SYSMOD の受け付け』の手順に進むことができます。

新規または既存の CSI を使用して専用の zSecure Command Verifier ゾーンにインストールする場合は、SC4RINST に用意されているサンプル・ジョブを使用してプリインストール・ステップを実行してから、インストール・プロセスに進みます。プリインストール・ステップについて詳しくは、 14 ページの『プリインストール・タスク』を参照してください。

SC4RINST に用意されているサンプル・ジョブでは、使用するインストール済み環境の基準に合わせて調整する必要がある値がすべて小文字で表記されています。現在使用されている値は以下のとおりです。

Your-Global
GLOBAL SMP/E データ・セットに使用するデータ・セット接頭部。この接頭部は、GLOBAL CSI の名前、およびすべての SMP/E ゾーンで共有される SMP/E データ・セットに使用されます。

Your-Product
zSecure Command Verifier データ・セットに使用するデータ・セット接頭部。このデータ・セットは、zSecure Command Verifier 固有の SMP/E データ・セットの接頭部にもなります。

SYSALLDA
すべてのデータ・セット割り振りに使用される装置名。

volser システム内で zSecure Command Verifier データ・セットを作成する DASD ボリュームの名前。SMS 環境では、ACS ルーチンによって、*volser* で指定されたボリュームとは別のボリュームが割り当てられることがあります。

tape zSecure Command Verifier 配布テープをマウントできるテープ装置の装置名。

注**:** *Your-Global* の値を *Your-Product* と同じにすることはできません。同じような接頭部を使用したい場合は、GLOBAL ゾーン用に修飾子を追加できます。例えば、以下の値を使用できます。

- *Your-Global* の値として SMPE.CMDVFY.GLOBAL
- *Your-Product* の値として SMPE.CMDVFY

表 *5. SMP/E* ゾーンの定義に使用されるプリインストール変数の値

変数	使用する値
Your-Global	
Your-Product	
sysda	
volser	
tape	

プリインストール・タスク

このリストには、zSecure Command Verifier をインストールする前に完了しておく必要があるタスクが示されています。

1. GLOBAL CSI および GLOBAL ZONE の作成と初期化

   既存の GLOBAL ゾーンを使用する場合は、GLOBAL CSI、GLOBAL ZONE、および関連するデータ・セットの定義をスキップできます。その場合は、次のステップに進んでください。GLOBAL ゾーンを作成する場合は、まずサンプル・ジョブ C4RJSMPA を実行して、GLOBAL ゾーン用のデータ・セットを定義し、初期化します。

C4RJSMPA を実行依頼

2. zSecure Command Verifier の TARGET ゾーンと DLIB ゾーンの作成

   zSecure Command Verifier の TARGET ゾーンと DLIB ゾーンは、それぞれ独自の CSI に作成できます。用意されているサンプル・ジョブでは、製品の CSI が作成され、その CSI 内に 2 つの SMP/E ゾーンが定義されます。

   C4RJSMPB を実行依頼

3. zSecure Command Verifier ZONE 内で OPTIONS 項目を作成します。

   次のジョブは、後続の SMP/E インストール・ステップで使用される OPTIONS 項目を指定するために使用されます。

   C4RJSMPC を実行依頼

ステップ 4: SYSMOD の受け付け

zSecure Command Verifier プロダクト・テープからインストールする場合、テープの最初のファイルは SMPMCS データ・セットです。

このデータ・セットには、zSecure Command Verifier を正しくインストールするために必要な SMP/E 修正制御ステートメントが含まれています。この場合は、サンプル・ジョブ **C4RJREC** を使用して製品を RECEIVE することができます。

C4RJREC を実行依頼

ステップ 5: TARGET データ・セットと DLIB データ・セットの割り振り

ジョブ **C4RJALL** を使用して必要なデータ・セットを割り振ることができます。

zSecure Command Verifier では、SMP/E 環境にターゲット・データ・セットと配布データ・セットが 4 つずつ追加されます。これらのデータ・セットのサイズと属性については、表 6を参照してください。

表 *6. zSecure Command Verifier* に必要な *Target* データ・セットと *Dlib* データ・セット

DDname	Type	Recfm	Blksize (推奨)	Lrecl	Space (トラック単位)	Dir
AC4RLNK	DLIB	U	32760	N/A	25	20
SC4RLNK	Target	U	32760	N/A	15	2
AC4RSMP	DLIB	FB	27920	80	2	2
SC4RSMP	Target	FB	27920	80	2	2
AC4RINST	DLIB	FB	27920	80	3	3
SC4RINST	Target	FB	27920	80	3	3

例えば、ジョブ **C4RJALL** には、必要な TARGET データ・セットと DLIB データ・セットを割り振るための JCL が含まれています。

C4RJALL を実行依頼

ステップ 6: SMP/E DDDEF の更新

ジョブ **C4RJDDD** を使用して、割り振られたデータ・セットを SMP/E に対して定義することができます。

このステップでは、前のステップで割り振ったデータ・セットを SMP/E に対して定義します。すべての SMP/E ジョブに適切な DD ステートメントを組み込むようにする場合は、このステップを省略できます。動的割り振りによって優先セットアップを使用する場合は、このステップが必要となります。サンプル・ジョブ **C4RJDDD** に、このステップに必要な JCL が含まれています。

C4RJDDD を実行依頼

ステップ 7: zSecure Command Verifier コードの追加

このステップでは、以下の SMP/E ステートメントを使用して zSecure Command Verifier のコード、サンプル、および資料をシステムに追加します。

```
APPLY  SELECT(JC4R230,HC4R230) GROUPEXTEND.
```

製品の FMID に対して **SELECT** を使用するため、SMP/E では **FUNCTIONS** キーワードを使用する必要がありません。メンバー **C4RJAPP** に、サンプル・ジョブが含まれています。このジョブを実行する前に、使用する GLOBAL CSI のデータ・セット名を指定します。

C4RJAPP を実行依頼

ステップ 8: ポリシー・プロファイル用のリソース・クラスの指定

zSecure Command Verifier では、すべてのインストール・ポリシー・プロファイルに使用されるリソース・クラスを指定することができます。デフォルトで設定される値は XFACILIT です。

通常はリソース・クラスを変更する必要はありません。インストール済み環境でリソース・クラスの異なる設定が必要な場合は、サンプル・ジョブ C4RJEXP を検討し、実行依頼します。このジョブを最初に実行したときに、戻りコード **12** で終了する可能性があります。これは、同じジョブを複数回実行できるようにするインライン SMP/E REJECT ステップが原因です。

```
Submit C4RJEXP
```

検討するフィールドは以下のとおりです。

RSVD*x*

これらのフィールドは予約済みです。zSecure Command Verifier サポート担当者から特に指示がない限り、変更しないでください。

CLASS

zSecure Command Verifier ポリシー・プロファイルに使用するリソース・クラスを入力します。デフォルト名は XFACILIT です。

ステップ 9: APF 許可された TSO コマンドの Parmlib の更新

parmlib を更新して、必要な TSO コマンドを含んだ APF 許可モジュールを使用できるようにすることができます。

zSecure Command Verifier では、APF 許可された 2 つの TSO コマンドが必要です。最初のコマンドでは、zSecure Command Verifier モジュールの現在の状態 (アクティブまたは非アクティブ) に関する情報、および現在使用中のリソース・クラスに関する情報を表示します。もう 1 つのコマンドでは、各種プロファイルのコマンド監査証跡情報を表示し、管理します。これらの APF 許可されたモジュールは、SC4RLNK ライブラリーにインストールされます。これらのモジュールを TSO コマンドとして使用できるようにするには、その名前を **PARMLIB** 内の TSO 許可されたコマンド・テーブルに追加する必要があります。以下のような行を、IKJTSOxx メンバー内の AUTHCMD セクションに追加します。メンバーを更新した後に、**TSO PARMLIBUPDATE xx** コマンドを使用してこのメンバーを活動化できます。

```
AUTHCMD NAMES(          /* AUTHORIZED COMMANDS      */      +
   ...  Leave the first part of this list of commands as is.
   ...  Insert the following line at the end of the list.
   C4RSTAT             /* zSecure Command Verifier status disp*/ +
   C4RCATMN            /* zSecure Command Verifier Audit Trail*/ +
   ...  Ensure that the last line in the AUTHCMD block ends
   ...  with a right parenthesis as shown below.
   ...                  /* SOME COMMENT             */)
   ...  Rest of member need not be modified.
```

必要な変更を記述しているサンプルの Parmlib メンバーが、メンバー **C4RJIKJ** に用意されています。

ステップ 10: zSecure Command Verifier の活動化とテスト

この情報を使用して、システムの IPL を実行せずに zSecure Command Verifier を活動化し、その動作をテストします。

zSecure Command Verifier は、動的出口機能によって実装されるため、事前にシステムの IPL を実行することなく直ちに zSecure Command Verifier を活動化することができます。このタイプの実装では、zSecure Command Verifier の 2 つのメインルーチンが標準のリンク・リスト・ライブラリーに置かれていることが前提条件となります。以下のいずれかの方法を使用できます。

- 製品をシステム・ライブラリーに直接インストールする。アクティブなシステム・ライブラリーに直接インストールすることはできますが、これはシステム・プログラミングの手法では推奨されません。
- SMP/E で制御される SC4RLNK データ・セットから、既にリンク・リスト に含まれている別のデータ・セットにモジュールをコピーする。
- z/OS 動的リンク・リスト 機能を使用して SC4RLNK データ・セットをアクティブなリンク・リスト に追加する。

前述のどのケースでも、**C4RMAIN** 出口の活動化を試みる前に、**F LLA,REFRESH** オペレーター・コマンドも実行する必要があります。 **SETPROG** コマンドの DSN キーワードによる指定読み込みは使用しないでください。**C4RPIER** モジュールはこの方法で活動化できず、アクティブなリンク・リスト・ライブラリーまたは STEPLIB に存在していなければなりません。

zSecure Command Verifier ライブラリーをアクティブな APF リストに追加するには、以下の例のようなメンバーを **PARMLIB** に追加し、**T PROG=xx** オペレーター・コマンドを実行します。

```
APF ADD DSNAME(Your-Product.SC4RLNK)                SMS
```

zSecure Command Verifier ライブラリーをアクティブなリンク・リスト に追加するには、以下の例のようなメンバーを **PARMLIB** に追加し、**T PROG=xx** オペレーター・コマンドを実行します。

```
LNKLST DEFINE NAME(LNKLSTC4) COPYFROM(CURRENT)
LNKLST ADD NAME(LNKLSTC4) DSN(Your-Product.SC4RLNK)
LNKLST ACTIVATE NAME(LNKLSTC4)
LNKLST UPDATE,JOB=*
```

zSecure Command Verifier を活動化するには、以下の例のようなメンバーを **PARMLIB** に追加し、**T PROG=xx** オペレーター・コマンドを実行します。

```
EXIT ADD EXITNAME(IRREVX01) MODNAME(C4RMAIN) STATE(ACTIVE)
```

あるいは、以下の**オペレーター**・コマンドを直接実行できます。

```
SETPROG EXIT,ADD,EXITNAME=IRREVX01,MODNAME=C4RMAIN,STATE=ACTIVE
```

この直接のオペレーター・コマンドは、IPL 全体にわたって持続するわけではないので注意してください。

zSecure Command Verifier を除去する必要がある場合は、以下の**オペレーター**・コマンドを使用します。

```
SETPROG EXIT,DELETE,EXITNAME=IRREVX01,MODNAME=C4RMAIN
```

C4RSTAT コマンドは APF 許可された TSO コマンドで、zSecure Command Verifier モジュールがアクティブかどうかを表示し、現在使用されているリソース・クラスに関する情報を確認するために使用できます。zSecure Command Verifier がインストールされてアクティブである場合、**C4RSTAT** コマンドの出力は以下の例のようになります。

```
C4R982I zSecure Command Verifier is active
C4R971I EXIT version is 2.3.0
C4R973I PIER version is 2.3.0
C4R985I Resource class used for policy profiles is XFACILIT
C4R976I Resource class is active
C4R969I Generic profiles are enabled
C4R978I Number of policy profiles is 0
```

zSecure Command Verifier を活動化した後でテストするには、予期したとおりに成功または失敗する RACF コマンドをいくつか実行します。例えば、キーワードを指定せずに **LISTUSER** コマンドを実行すると、自分の**ユーザー** ID の情報が引き続き表示されるはずです。また、zSecure Command Verifier ポリシー・プロファイルが望んだとおりに解釈されていることを確認したい場合は、**SC4RSMP** 内のサンプル・ジョブ C4RJTST を使用できます。このサンプル・ジョブでは、システム全体のポリシーがいくつか定義され、それらのポリシーの効果を示すコマンドがいくつか実行されます。これらのポリシーはすべてのユーザーに適用され、そのためにこのジョブが実行されるシステムまたはシスプレックス上の他のユーザーに影響する可能性があります。このサンプル内のポリシー・プロファイルを検査して、zSecure Command Verifier をインストールするシステムにとって適切であることを確認します。サンプルは、テスト環境でのみ使用してください。サンプル・ジョブは以下の部分で構成されています。

- いくつかのサンプル・ポリシー・プロファイルの定義。このうちの一部は、端末ユーザーに出されるメッセージにのみ影響し、それ以外はユーザー・プロファイルとデータ・セット・プロファイルの作成に影響します。

- 失敗する、または修正される複数の RACF コマンドの実行。成功したコマンドは、**C4R913I** メッセージの一部として端末にエコー出力される必要があります。定義されているポリシーのいずれかに違反するコマンドは、ポリシー・プロファイルへのアクセス権限が不十分であるために、RACF 違反メッセージ (ICH408I) を受け取ります。
- サンプル・ポリシー・プロファイルを除去し、システムをテスト・ジョブ実行前の状態に戻す処理。
- テスト・コマンドによって作成されたユーザー・プロファイルとデータ・セット・プロファイルの除去。

サンプル・テスト・ジョブを実行するには、非標準の RACF 権限が必要です。少なくとも、XFACILIT (または 16 ページの『ステップ 8: ポリシー・プロファイル用のリソース・クラスの指定』で指定した代替リソース・クラス) 内および USER クラス内の CLAUTH と、現行接続グループでのグループ SPECIAL が必要です。ジョブ全体でシステム SPECIAL 権限のみを使用することも可能です。その場合、CLAUTH とグループ SPECIAL は不要です。

重要**:** このサンプル・ジョブでは、システム全体のポリシーが定義されます。これらのポリシーはすべてのユーザーに適用され、そのためにこのジョブが実行されるシステム/シスプレックス上の他のユーザーに影響する可能性があります。実行されたコマンドを検査し、このサンプルのインストール検査手順の実行が使用する環境にとって適切かどうかを評価してください。

SC4RSMP のオプション・ジョブ C4RJTST を調整して実行依頼

コマンドが予期したとおりに機能して結果に問題がなければ、次のステップ (システムでの zSecure Command Verifier コードのインストールの受け入れ) に進みます。

ステップ 11: zSecure Command Verifier 製品の受け入れ

zSecure Command Verifier の実装に問題がなければ、**ACCEPT** ジョブを実行して、製品をシステムに統合します。

サンプルの **ACCEPT** ジョブが、C4RJACC に用意されています。このジョブの実行が終了したら、それ以上のシステム・プログラミング作業を行うことなく zSecure Command Verifier を使用できます。

C4RJACC を実行依頼

監査プロファイルのリソース

zSecure Command Verifier のインストール後、インストール済み環境の監査員は、zSecure Command Verifier の監査を活動化するためのポリシー・プロファイルを作成しなければならない場合があります。

監査員が監査のタイミングと対象を指定できるようにするために、zSecure Command Verifier ではダミー・リソースに対する追加の **RACROUTE REQUEST=AUTH** を実装しています。このリソースは、C4R という接頭部が付いた実行されるコマンドの名前です。このプロファイルは、XFACILIT クラス内で定義する必要がありま

す。プロファイルを定義しない場合は、zSecure Command Verifier で処理されたコマンドを追加で監査することができません。通常の RACF コマンド監査を、zSecure Command Verifier 設定を使用して変更することはできません。インストール・プロセス中に監査員に問い合わせて、定義する必要があるプロファイルと、それらのプロファイルに対して活動化する必要がある監査オプションを指定します。使用可能なプロファイルと監査オプションについて詳しくは、 21 ページの『第 4 章 コマンドおよびポリシーの効果の監査』を参照してください。

第 4 章 コマンドおよびポリシーの効果の監査

zSecure Command Verifier は、実行されたコマンドと実装されたポリシーの効果の両方を監査するための各種機能を備えています。

使用可能な監査機能を以下のリストに示します。

コマンド監査証跡機能
: 実行された RACF コマンドに関する情報を、関係するプロファイル自体に記録します。簡単な RACF リスト・コマンドを使用することで、プロファイルの特定の部分 (OWNER、UACC、アクセス・リストなど) を最後に変更したユーザーに関する情報を取得することができます。詳細については、『コマンド監査証跡』を参照してください。

ポリシー・プロファイル効果機能
: SMF レコードを使用して zSecure Command Verifier ポリシー・プロファイルの効果に関する情報を記録します。ポリシー・プロファイルの処理前と処理後の RACF コマンドが、特殊なポリシー・プロファイル効果記録プロファイルへのアクセスに関する LOGSTRING 情報に記録されます。詳細については、 38 ページの『コマンド監査用のポリシー・プロファイル』を参照してください。

SMF アクセス記録
: 通常の SMF アクセス記録をポリシー・プロファイル自体として使用することもできます。詳細については、 42 ページの『SMF による通常のアクセス記録』を参照してください。

コマンド監査証跡

zSecure Command Verifier には、実行されたコマンドに関する追加データを収集して、そのコマンドに関連する RACF プロファイルに保存する機能があります。

例えば、ユーザー C4RTEST がコマンド **ALTUSER IBMUSER RESTRICTED** を実行した場合は、情報が IBMUSER プロファイルに保存されます。情報には、RESTRICTED 属性、日時、およびユーザー ID C4RTEST の表示が含まれます。保存された情報は、コマンド監査証跡として使用できます。通常は、同じ情報を SMF 監査レコードから取得できます。しかし、zSecure Command Verifier の機能を使用すれば、同じ情報をより速く検出でき、大量になることもある SMF データを処理する必要もなくなるので便利です。zSecure Command Verifier で保守される、あるユーザーに関するこのコマンド監査証跡情報の例を、以下に示します。

```
Command Audit Trail for USER IBMUSER

Segment:  CICS    Added on 05.241/03:19 by C4RTEST
                  Changed on 05.241/03:20 by C4RTEST
          TSO     Changed on 05.241/03:19 by C4RTEST
Attrib:   PASSWRD Removed on 05.238/14:24 by C4RTEST
          INTERV  Changed on 05.241/04:42 by C4RTEST
          RESTR   Added on 05.238/14:24 by C4RTEST
Connect:          BCSC Added on 05.238/14:24 by IBMUSER
GrpAttr:  ADSP    BCSC Removed on 05.238/14:24 by IBMUSER
```

図 2. ユーザーのコマンド監査証跡データ

このデータは、各プロファイルの **USRDATA** フィールドに保持されます。**USRDATA** フィールドは、一般に通常の RACF コマンドの一部として表示されません。適切な制御が設定されていれば、コマンド監査証跡に使用される **USRDATA** フィールドが、各種の RACF リスト・コマンド (**LISTUSER** など) の一部として表示されます。このデータは、通常のコマンド出力の後に表示されます。

コマンド監査証跡データは、関係するプロファイル内で保守されるため、情報が収集されることはなく、プロファイルが削除されると既存の情報はすべて削除されます。

コマンド監査証跡機能の制御

=CMDAUD ポリシー・プロファイルを定義して、コマンド監査証跡機能を制御することができます。

これらのポリシーを作成する際に、zSecure Command Verifier ですべての端末ユーザーを対象にコマンド監査証跡情報を収集して保持するかどうか、またその情報を通常の LIST 出力の一部として表示するかどうかを制御できます。収集された情報は、特定の変更を誰がいつ行ったかを明らかにすることから、プロファイルへの変更に関する説明責任を実現します。=CMDAUD ポリシー・プロファイルを定義しない場合は、zSecure Command Verifier でコマンド監査証跡情報が収集されません。

ポリシー・プロファイル定義によって、コマンド監査証跡情報が収集されるかどうかが決まります。ほとんどの =CMDAUD ポリシー・プロファイルでは、アクセス・レベルが無視されます。唯一の例外は =CMDAUD.=MAINT ポリシー・プロファイルです。収集されたコマンド監査証跡データを除去するために使用できる **C4RCATMN** コマンドの権限用に、2 つのアクセス・レベルが確保されています。

=CMDAUD ポリシー・プロファイルの構造

以下の変数の詳細および例を使用して、コマンド監査証跡機能を制御するための =CMDAUD ポリシー・プロファイルを定義します。

=CMDAUD ポリシー・プロファイルの基本構造には、以下のフォーマットの独立したセクションが 5 つ含まれています。

C4R.*class.*=CMDAUD.*data-type.profile-identification*

class、*data-type*、およびプロファイル自体 (*profile-identification*) を使用して、どのタイプのコマンド監査証跡が収集されるかが選択されます。=CMDAUD ポリシー・プロファイルの各部分を、以下で説明します。

class ポリシー・プロファイル内のこの修飾子は、コマンドで使用または暗黙指定されるプロファイルのリソース・クラスを表します。

=CMDAUD
ポリシー・プロファイルのこの修飾子は、ここに示されているとおりのフォーマットで存在している必要があります。このポリシーと最もよく一致する総称プロファイルにこの修飾子が含まれていない場合、zSecure Command Verifier は、クラス修飾子が単一の総称文字 (*) で表されているポリシーを使用して、次によく一致するポリシー・プロファイルを検索します。例については、 24 ページの『例』を参照してください。

data-type
=CMDAUD ポリシー・プロファイルのこの部分には、以下のいずれかの値を指定できます。

=SEGMENT
セグメントの追加、変更、および削除に関する情報

技術的には、USER プロファイル内の MFA データは個別のセグメント内に保持されるのではありませんが、MFA データへの変更はコマンド監査証跡の =SEGMENT ポリシーに基づいて記録されます。

=ATTR
属性の追加と削除に関する情報

=CONNECT
ユーザーからグループへの接続の追加、変更、および削除に関する情報

=ACL **PERMIT** コマンドを使用したアクセス・リスト項目の管理に関する情報

=MEMBER
グループ化リソース・クラス・プロファイル内のメンバーの追加と削除に関する情報

=MAINT
コマンド監査証跡データの表示と除去を制御

profile-identification
=CMDAUD ポリシー・プロファイルのこの部分は、ターゲット・プロファイルの *class* に依存します。ユーザー・プロファイルとグループ・プロファイルの場合は、ここにプロファイルの所有者 が入ります。それ以外のプロファイルの場合は、リソース・プロファイル自体が入ります。

USER *owner.userid*

GROUP
owner.group

リソース
resource-profile

例

=CMDAUD ポリシー・プロファイルのこの最初の例では、コマンド監査証跡内で、GROUP SYS1 によって所有される USER プロファイル IBMUSER のセグメントへの変更が記録されます。この操作は、以下のポリシーで制御されます。

```
C4R.USER.=CMDAUD.=SEGMENT.SYS1.IBMUSER
```

より総称的なポリシー・プロファイルを定義することもできます。例えば、すべてのリソース・クラス内のすべてのプロファイルに対してコマンド監査証跡を活動化する場合は、ポリシー・プロファイル Policy Profile A (**PPA**) を定義できます。

```
PPA:  C4R.*.=CMDAUD.*.**
```

これらの例のどちらにも、必須の =CMDAUD 修飾子が存在します。

FACILITY クラス・プロファイルの管理を特定の管理者のみに制限する場合は、通常、Policy Profile B (**PPB**) などの追加のポリシー・プロファイルも定義します。

```
PPB:  C4R.FACILITY.**
```

ただし、FACILITY プロファイル BPX.SUPERUSER への PERMIT コマンドについてコマンド監査証跡が更新される場合、この操作は、以下のポリシーで制御されます。

```
C4R.FACILITY.=CMDAUD.=ACL.BPX.SUPERUSER
```

このポリシーと最もよく一致する総称プロファイルは **PPB** です。このポリシー・プロファイルには必須の修飾子 =CMDAUD が含まれていないため、zSecure Command Verifier は、この最もよく一致するプロファイルをバイパスし、代わりに、以下のポリシーと最もよく一致するポリシー・プロファイルを見つけます。

```
C4R.*.=CMDAUD.=ACL.BPX.SUPERUSER
```

この例では、通常の最もよく一致するプロファイルである **PPB** の代わりに、**PPA** が使用されます。

=CMDAUD ポリシー・プロファイルに対するアクセス・レベル

ほとんどの =CMDAUD ポリシー・プロファイルに対するアクセス権限は、コマンド監査証跡データの収集の制御には使用されません。監査証跡データが収集されるかどうかは、プロファイルの存在によってのみ決まります。コマンド監査証跡が表示されるかどうかは、=CMDAUD.=MAINT プロファイルに定義されているアクセス・レベルによって決まります。

このプロファイルに READ 権限がある場合は、各種 RACF リスト・コマンドの出力にコマンド監査証跡情報が追加されます。このポリシー・プロファイルに対するアクセス権限は、**C4RCATMN** コマンドの使用も制御します。このコマンドは、選択したプロファイルからコマンド監査証跡情報を表示または除去するために使用できます。詳しくは、 26 ページの『C4RCATMN コマンド』を参照してください。これ以外の =CMDAUD ポリシー・プロファイルには、アクセス・レベルは使用されません。

関連するポリシー・プロファイルが定義されている場合は、すべての端末ユーザーを対象にコマンド監査証跡情報が収集されて保持されます。このため、コマンド監査証跡は、プロファイルへの変更に関する説明責任を実現します。収集された情報

を使用して、特定の変更を誰がいつ行ったかを特定することができます。この情報が収集されないのは、コマンド実行時に zSecure Command Verifier がアクティブでなかった場合、およびポリシー・プロファイルが存在しなかった場合のみです。監査証跡の本質として、どの端末ユーザーも例外扱いしてはならないことになっています。このため、アクセス・レベルを使用してコマンド監査証跡の収集が制御されることはありません。

=CMDAUD.=MAINT 以外のポリシー・プロファイルに現在使用されるアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: コマンド監査データの収集や保持は行われません。

NONE
: コマンド監査証跡データの収集と保持が行われます。

READ
: NONE と同じ。

UPDATE
: NONE と同じ。

CONTROL
: NONE と同じ。

=CMDAUD.=MAINT ポリシー・プロファイルに現在使用されるアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: コマンド監査証跡データは、**C4RCATMN** コマンドを使用しても表示されず、保持することもできません。

NONE
: 監査証跡データは、**C4RCATMN** コマンドによって表示されず、保持することもできません。

READ
: 監査証跡データは、RACF リスト・コマンドの一部として表示されます。

UPDATE
: 監査証跡データは、RACF リスト・コマンドの一部として表示されます。また、**C4RCATMN** コマンドをによって表示することもできます。**C4RCATMN** コマンドでは有効範囲が検査されません。端末ユーザーに **C4RCATMN** による表示機能が許可されているときは、RACF データベース内のすべてのプロファイルのコマンド監査証跡を検査できます。

CONTROL
: 端末ユーザーに、**C4RCATMN** コマンドを使用したコマンド監査証跡データの除去も許可されます。

各タイプの情報のプロファイルは独立しています。例えば、インストール済み環境で、ユーザー属性に対する変更のみを記録し、ユーザー・セグメントに対する変更は記録しないようにすることができます。あるいは、グループ SYS1 が所有するユーザーに対する変更のみを記録するポリシーを、インストールで実装することができます。

RACF リスト・コマンドを使用する場合は、端末ユーザーが RACF BASE セグメント情報を抑止しなかった場合にのみ、コマンド監査証跡情報が表示されます。RACF BASE セグメント情報の抑止に **NORACF** キーワードが使用される場合は、コマンド監査証跡情報も抑止されます。RACF BASE セグメントなしのコマンド監査証跡を表示する場合は、**C4RCATMN** コマンドを使用できます。**C4RCATMN** コマンドでは有効範囲検査が行われないため、適用可能な =CMDAUD.=MAINT ポリシー・プロファイルに対する UPDATE 権限が必要になります。

ほとんどの場合、すべてのコマンド監査証跡ポリシー・プロファイルの UACC を NONE に設定します。=CMDAUD.=MAINT ポリシー・プロファイルに対する READ 権限や UPDATE 権限を必要とする監査員やシステム管理者はごくわずかです。このポリシー・プロファイルに対する CONTROL 権限は、通常は数名のユーザーにのみ付与されます。このアクセス・レベルは、エラーを修正したり、不要となったコマンド監査証跡情報を除去したりする場合に使用できます。

通常、コマンド監査証跡の収集と保守を制御するには、総称 =CMDAUD ポリシー・プロファイルがあれば十分です。

C4RCATMN コマンド

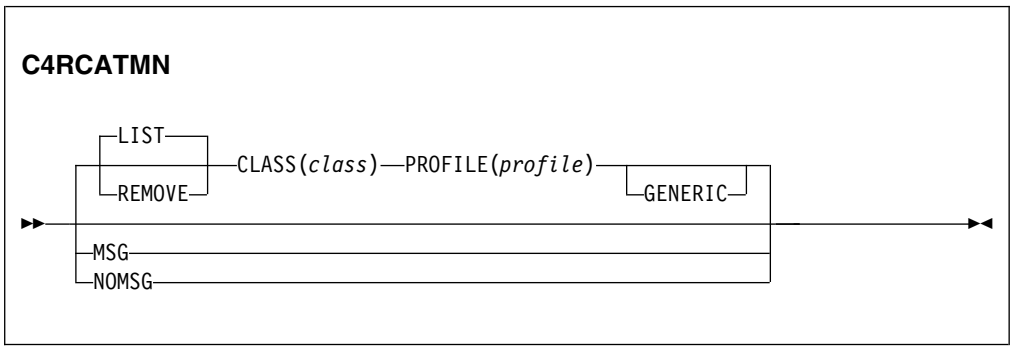
C4RCATMN コマンドを使用して、各種プロファイル内のコマンド監査証跡情報を表示または除去することができます。

コマンド監査証跡情報を表示または除去する前に、関連する =CMDAUD.=MAINT ポリシー・プロファイルが検査されます。端末ユーザーのアクセス権限が不十分である場合は、RACF アクセス違反イベントが生成されます。=CMDAUD.=MAINT ポリシー・プロファイルの形式は以下のとおりです。

C4R.*class*.=CMDAUD.=MAINT.*profile-identification*

C4RCATMN コマンドでは、コマンド監査証跡を表示する場合に UPDATE アクセス・レベル、コマンド監査証跡を除去する場合に CONTROL アクセス・レベルがそれぞれ必要となります。

C4RCATMN コマンドの構文は、次のとおりです。



キーワードとパラメーターの説明を以下に示します。

LIST このアクションはデフォルトです。クラス *class* 内の *profile* のコマンド監査証跡データが表示されます。このアクションを使用する場合は、

=CMDAUD.=MAINT ポリシー・プロファイルに対して少なくとも UPDATE 権限が必要となります。アクセス権限が不十分である場合、コマンド監査証跡は表示されません。

REMOVE
クラス *class* 内の *profile* のコマンド監査証跡データが除去されます。このアクションを使用する場合は、=CMDAUD.=MAINT ポリシー・プロファイルに対して少なくとも CONTROL 権限が必要となります。アクセス権限が不十分である場合は、RACF 違反が記録され、コマンド監査証跡は除去されません。

MSG このオプションは、コマンド監査証跡情報が通常の RACF リスト・コマンドの一部として表示されることを示します。このオプションはセッションをまたいで保存されます。このオプションが有効となるのは、コマンド監査証跡情報を表示するためのその他の要件 (該当する =CMDAUD.=MAINT ポリシー・プロファイルに対する十分なアクセス権限など) を満たしている場合に限られます。**C4RCATMN (NO)MSG** コマンドを実行していない場合の MSG/NOMSG の初期設定は MSG です。

NOMSG
このオプションは、コマンド監査証跡情報が通常の RACF リスト・コマンドの一部として表示されないことを示します。このオプションはセッションをまたいで保存されます。このオプションがアクティブになっている場合は、**C4RCATMN** コマンドによってのみコマンド監査証跡情報を表示できます。**C4RCATMN** コマンドでこの情報を表示するには、通常の RACF リスト・コマンドよりも高い権限が必要となります。**C4RCATMN (NO)MSG** コマンドを実行していない場合の MSG/NOMSG の初期設定は MSG です。

class コマンド監査証跡データを表示または除去するプロファイルのリソース・クラス。LIST または REMOVE キーワードを使用する場合は、このキーワードとパラメーターが必須となります。

profile コマンド監査証跡データを表示または除去するプロファイル。profile には、RACF データベースに保管されているプロファイルを正確に指定する必要があります。最も近い総称プロファイルの突き合わせは行われません。データ・セットの場合は、プロファイル名に接頭部が含まれていること、およびプロファイル名が引用符で囲まれていないことが必要です。 LIST または REMOVE キーワードを使用する場合は、このキーワードとパラメーターが必須となります。

GENERIC
このオプション・キーワードは、総称文字が含まれていない場合でも *profile* が総称プロファイルであることを示します。一般に、総称文字を含まない総称プロファイルは、DATASET クラスでのみ発生します。

28 ページの図 3では、**C4RCATMN** コマンドの例を示しています。**C4RCATMN LIST** コマンドの出力は、通常のRACF リスト・コマンドの最後に追加される行と同じです。

```
c4rcatmn list class(user) profile(ibmuser)

Command Audit Trail for USER IBMUSER
Segment:  CICS    Added on 05.241/03:19 by C4RTEST
                  Changed on 05.241/03:20 by C4RTEST
          TSO     Changed on 05.241/03:19 by C4RTEST
Attrib:   PASSWRD Removed on 05.238/14:24 by C4RTEST
          INTERV  Changed on 05.241/04:42 by C4RTEST
          RESTR   Added on 05.238/14:24 by C4RTEST
Connect:          BCSC Added on 05.238/14:24 by IBMUSER
GrpAttr:  ADSP    BCSC Removed on 05.238/14:24 by IBMUSER
```

図 *3. C4RCATMN LIST* コマンドの出力

以下の例は、コマンド監査証跡情報を除去する場合の **C4RCATMN** コマンドの出力を示しています。

```
c4rcatmn remove class(gcicstrn) profile(cicsa.spro)
Command Audit data for segments has been removed
Command Audit data for attributes has been removed
Command Audit data for access list unchanged
Command Audit data for members has been removed
```

図 *4.* コマンド監査証跡データを除去する場合の *C4RCATM* コマンドの出力

コマンド監査証跡データ表示のフォーマット

以下では、コマンド監査証跡データを抑止、フィルタリング、および解釈する方法について説明します。

図 3 の例では、**C4RCATMN** コマンドの出力が示されています。この出力は、通常の RACF リスト・コマンドの最後に追加される行と同じです。RACF リスト・コマンドでは、この情報は、ユーザーが =CMDAUD.=MAINT ポリシー・プロファイルへの READ アクセス権限を持っている場合に表示されます。RACF リスト・コマンドが複数の RACF プロファイルを指定する場合、全プロファイルの全 RACF 情報の後で、指定されたプロファイルのコマンド監査証跡情報が表示されます。このようなリスト・コマンドの例を以下に示します。

```
LISTDSD   DA(dsn1,dsn2)
LISTUSER  (user1,user2)
```

各コマンド監査証跡セクションは、以下のようなヘッダー行で識別されます。

```
C4R736I Command Audit Trail for USER user1
```

RACF リスト・コマンドが、表示されるプロファイルのパターンや接頭部を指定する場合は、コマンド監査証跡は含まれません。このようなリスト・コマンドの例を以下に示します。

```
LISTDSD   PREFIX(user1)
RLIST     FACILITY *
```

端末ユーザーに =CMDAUD.=MAINT ポリシー・プロファイルに対する READ アクセス権限がある場合は、コマンド監査証跡情報が表示されます。RACF リスト・コマンドには、これらの追加の行を抑止するオプションがありません。コマンド監査証跡情報を抑止するための間接的な方法が 2 つあります。

- **NOMSG** キーワードを指定して C4RCATMN コマンドを実行する。これでコマンド監査証跡情報は表示されなくなります。**C4RCATMN** コマンドを使用してこの情報を表示することも可能ですが、その場合は通常の RACF コマンドよりも高い権限が必要となります。**C4RCATMN MSG** コマンドを使用すると、コマンド監査証跡の表示を再活動化できます。MSG/NOMSG の設定は、セッションをまたいで保存されます。**C4RCATMN (NO)MSG** コマンドを実行していない場合の MSG/NOMSG の初期設定は MSG です。
- C4RNOCAT という名前の DD 名 (**ファイル名**) を割り振る。この DD 名は、特定のデータ・セット、SYSOUT クラス、またはデバイスに割り振る必要はありません。優先割り振り先は DUMMY です。この DD 名を割り振るだけで、すべてのコマンド監査証跡情報が通常の RACF リスト・コマンドの一部として表示されなくなります。**C4RCATMN** コマンドを使用してこの情報を表示することも可能ですが、その場合は =CMDAUD.=MAINT ポリシー・プロファイルに対してより高い権限が必要となります。

コマンド監査証跡情報は、いくつかのセクションから構成されます。

- ヘッダー

  ヘッダーには、リストされるクラスとプロファイルが表示されます。

- セグメント・セクション

  セグメント・セクションには、非基本セグメントに対する最終変更に関する情報が表示されます。1 行目は、*Segment:* で始まり、続いてセグメントの省略名が表示されます。この行の残りの部分には、変更のタイプ (追加、変更、削除など)、変更が行われた日時、およびコマンドを実行したユーザーが表示されます。また、プリコマンド、RACF コマンド、およびポストコマンドから返されたゼロ以外の最大戻りコードが表示されます。既存のセグメントに対する変更の場合は、最終変更のみが表示されます。

  収集は、以下のポリシー・プロファイルによって制御されます。

  ```
  C4R.class=CMDAUD.=SEGMENT.profile-identification
  ```

  変更されたセグメントごとに個別のブロック (追加、変更、削除) が表示されます。現在サポートされているセグメントおよび疑似セグメントは、以下のとおりです。

  USER CICS、DFP、LANGUAGE、NETVIEW、OMVS、OPERPARM、TSO、WORKATTR、OVM、DCE、NDS、LNOTES、KERB、PROXY、EIM、CSDATA、MFA

  GROUP
  DFP、OMVS、OVM、TME、CSDATA

  DATASET
  DFP、TME

  一般リソース
  SESSION、DLFDATA、SSIGNON、STDATA、SVFMR、TME、KERB、PROXY、EIM、CDTINFO、ICTX、CFDEF、ICSF、SIGVER、MFA、MFPOLICY

- 属性セクション

属性セクションには、属性および属性に対する最終変更に関する情報が表示されます。1 行目は *Attrib* で始まり、続いて属性の省略名が表示されます。この行の残りの部分には、変更のタイプ (追加または除去)、変更が行われた日時、およびコマンドを実行したユーザーが表示されます。また、プリコマンド、RACF コマンド、およびポストコマンドから返されたゼロ以外の最大戻りコードが表示されます。プロファイルにその属性が既にある場合、予想される確認 コマンドは表示されません。表示される情報には、プロファイルを変更した日時と ID が反映されます。

収集は、以下のポリシー・プロファイルによって制御されます。

`C4R.`*`class`*`=CMDAUD.=ATTR.`*`profile-identification`*

変更された属性ごとに個別のブロック (追加、変更、除去) が表示されます。現在サポートされている属性は、以下のとおりです。

USER ADSP、SPECIAL、OPERATIONS、REVOKE、GRPACC、UAUDIT、AUDITOR、ROAUDIT、PASSWORD、OIDCARD、INTERVAL、EXPIRED、RESTRICTED、SECLEVEL、SECLABEL、MODEL、INSTDATA、CATEGORY、RESUME、OWNER、DFLTGRP、NAME、PHRASE

GROUP
TERMUACC、UNIVERSAL、MODEL、INSTDATA、OWNER、SUPGRP

DATASET
WARNING、NOTIFY、SECLEVEL、SECLABEL、ERASE、ACL、INSTDATA、CATEGORY、OWNER、 LEVEL、UACC

一般リソース
WARNING、NOTIFY、SECLEVEL、SECLABEL、SINGLEDS、TVTOC、TIMEZONE、APPLDATA、ACL、INSTDATA、CATEGORY、OWNER、LEVEL、UACC

- 接続セクション

接続セクションには、接続に対する最終変更に関する情報とともに、グループ、権限、および UACC が表示されます。

収集は、以下のポリシー・プロファイルによって制御されます。

`C4R.`*`class`*`=CMDAUD.=CONNECT.`*`profile-identification`*

接続セクションは、USER プロファイルの場合のみ表示されます。GROUP プロファイルの場合は表示されません。このセクションの 1 行目は、「*Connect:*」で始まります。各行には、GROUPNAME に続いて、UACC、GROUP 権限、変更が行われた日時、コマンドを実行したユーザー ID と、プリコマンド、RACF コマンド、およびポストコマンドから返されたゼロ以外の最大戻りコードが表示されます。UACC と GROUP 権限の両方がデフォルト値 (つまり、UACC=NONE および AUTH=USE) の場合、それらの値は明示的に表示されません。これにより、デフォルトでない設定を容易に識別できます。UACC および AUTH の設定について詳しくは、「*RACF* セキュリティー管理者のガイド」および「*RACF* コマンド言語 解説書」を参照してください。

サイズ上の制限から、接続グループに対する最後の 64 件の変更のみが表示されます。

- グループ属性セクション

  グループ属性セクションは、接続セクションの直後に表示され、あらゆるグループ属性に対する最終変更に関する情報が表示されます。1 行目は、*GrpAttr:* で始まり、続いて属性の省略名が表示されます。

  収集は、以下のポリシー・プロファイルによって制御されます。

  C4R.*class*=CMDAUD.=CONNECT.*profile-identification*

  グループ属性セクションは、ユーザー・プロファイルの場合のみ表示されます。グループ・プロファイルの場合は表示されません。各行には、属性に続いて、グループ名、変更が行われた日時、およびコマンドを実行したユーザーが表示されます。また、プリコマンド、RACF コマンド、およびポストコマンドから返されたゼロ以外の最大戻りコードが表示されます。同じ属性が追加されて除去された場合は、その属性について複数の行が表示されます。各属性の行は日時順に表示されるため、最後の行に状況が反映されます。

  サイズ上の制限から、接続グループに対する最後の 64 件の変更のみが表示されます。現在サポートされている属性は、以下のとおりです。

  ADSP、SPECIAL、OPERATIONS、REVOKE、GRPACC、AUDITOR、RESUME
- アクセス・リスト・セクション

  アクセス・リスト・セクションには、アクセス・リスト項目、およびアクセス・リスト項目に対する最終変更に関する情報が表示されます。各行には、付与されたアクセス・レベルに続いて、変更が行われた日時、およびコマンドを実行したユーザーが表示されます。また、プリコマンド、RACF コマンド、およびポストコマンドから返されたゼロ以外の最大戻りコードが表示されます。ユーザーまたはグループごとに 1 行のみが表示されます。アクセス権限を付与または除去した最後のインスタンスが表示されます。アクセス・リストからユーザーが除去された場合は、値 Removed が表示されます。PERMIT コマンドで RESET キーワードが使用された場合は、特殊な ID **ALL** が使用されます。サイズ上の制限から、アクセス・リストに対する最後の 64 件の変更のみが収集されます。

  収集は、以下のポリシー・プロファイルによって制御されます。

  C4R.*class*=CMDAUD.=ACL.*profile-identification*
- メンバー・セクション

  メンバー・セクションには、グループ化クラス・プロファイルの一部であるメンバーが表示されます。各行は、グループ化クラス・プロファイルのメンバー・リストに対する項目の追加または除去を示します。各行には、1 つのメンバーに続いて、変更が行われた日時、およびコマンドを実行したユーザーが表示されます。また、プリコマンド、RACF コマンド、およびポストコマンドから返されたゼロ以外の最大戻りコードが表示されます。各メンバーについて、最後のアクションを表す 1 つの行のみが表示されます。サイズ上の制限から、メンバー・リストに対する最後の 64 件の変更のみが表示されます。また、メンバー名の最初の 128 バイトのみが収集され、この表示に組み込まれます。

  収集は、以下のポリシー・プロファイルによって制御されます。

  C4R.*class*=CMDAUD.=MEMBER.*profile-identification*

ユーザー・プロファイルでの例を以下に示します。

```
Command Audit Trail for USER IBMUSER
Segment:  CICS    Added on 05.241/03:19 by C4RTEST
                  Changed on 05.241/03:20 by C4RTEST
          TSO     Changed on 05.241/03:19 by C4RTEST
Attrib:   PASSWRD Removed on 05.238/14:24 by C4RTEST
          INTERV  Changed on 05.241/04:42 by C4RTEST
          RESTR   Added on 05.238/14:24 by C4RTEST
Connect:          C4RGRP1 Added on 05.238/14:24 by IBMUSER
GrpAttr:  ADSP    C4RGRP1 Removed on 05.238/14:24 by IBMUSER
```

図 *5.* ユーザー・プロファイルのコマンド監査証跡データ

データ・セット・プロファイルでの例を以下の図に示します。この例では、DFP セグメントが追加され、プロファイルが WARNING モードに置かれ、複数のアクセス・リスト項目が変更または除去されています。2005 年 9 月 14 日 (05.257) に、アクセス・リスト全体が IBMUSER によって **PERMIT RESET** コマンドを使ってリセットされています。

図 *6.* データ・セット・プロファイルのコマンド監査証跡データ

```
Command Audit Trail for DATASET  IBMUSER.**
Segment:  DFP     Added on 05.245/05:21 by C4RTEST
Attrib:   WARNING Added on 05.245/05:20 by C4RTEST
Access:           C4RGRP1 access READ on 05.234/09:39 by C4RTEST
                  C4RGRP2 access READ on 05.234/09:39 by C4RTEST
                  C4RTEST access READ on 05.234/09:39 by C4RTEST
                  SYS1 access READ on 05.234/09:39 by C4RTEST
                  IBMUSER access READ on 05.234/09:39 by C4RTEST
                  * access UPD on 05.234/09:39 by C4RTEST
                  CRMBGUS access Removed on 05.234/09:39 by C4RTEST
                  **ALL** access Removed on 05.257/15:06 by IBMUSER
```

以下の例は、グループ化リソース・クラス内のプロファイルに対するメンバーの追加と除去に関するコマンド監査証跡情報を示しています。

```
Command Audit Trail for GCICSTRN CICSA.SPRO
Member:           CICSA.CEDA Added on 05.249/14:21 by C4RTEST
                  CICSA.CEMT Removed on 05.249/14:21 by C4RTEST
```

図 *7.* グループ化リソース・クラス内のプロファイルでのメンバー管理に関するコマンド監査証跡データ

セグメントまたは属性に関する情報は、日時順に表示されます。特定のセグメントまたは属性に対して表示される最後の行は、最後に記録されたアクションを示します。属性が付与された後に除去された場合は、最初の行に属性を付与したユーザーが示され、最後の行に属性を除去したユーザーが示されます。

アクセス・リスト項目およびメンバー・リストについては、最後の 64 件の変更のみが保持されます。この制限は、主にプロファイル・サイズとパフォーマンス上の理由によるものです。各 ID またはメンバーの最後のアクションのみが記録されます。

RRSF の概要

以下では、RRSF 環境でコマンド監査証跡データを管理する方法について説明します。

zSecure Command Verifier コマンド監査証跡機能が RRSF 環境で使用される場合は、コマンド監査証跡情報が RRSF 環境内の各システムで個別に保守されます。つまり、ターゲット・システムで定義されているポリシー・プロファイルによって、コマンド監査証跡が保守されるかどうか、またどのように保守されるかが制御されます。RRSF 全体でのデータ・フローは、RRSFDATA プロファイルおよびコマンド伝搬の運用設定に基づきます。ターゲット・システム上でコマンドが伝搬される場合は、zSecure Command Verifier によってコマンド監査証跡データが必要に応じて追加されます。コマンド監査証跡の個々の項目は伝搬されません。RRSF 環境内の各システムのコマンド監査証跡は、他のシステムのコマンド監査証跡から独立して保守されます。

zSecure Command Verifier がインストールされていない、またはアクティブになっていないシステムでは、コマンド監査証跡は保守されません。これは、必要なポリシー・プロファイルが存在しない場合も同様です。

結果的にコマンド監査証跡データの同期がわずかにずれる可能性があります。例えば、RRSF ノード SYSA 上の SPECIAL 属性がユーザー IBMUSER によって 05.283/14:13 に除去され、その数分後に RRSF ノード SYSB への RRSF コマンドの伝搬が完了した場合、SYSB 上のコマンド監査証跡データは 05.283/14:15 を示します。どのような場合でも、コマンド監査証跡には、現行システムで変更が有効となった日時が示されます。

ストレージ・スペースの計画

コマンド監査証跡機能用の RACF ストレージの割り振りを計画するには、以下のガイドラインに従ってください。

コマンド監査証跡機能は、RACF データベースに追加のスペースを必要とします。初期のスペース所要量は、プロファイルに変更が加えられるペースによって異なります。RACF コマンドが一定の回数実行されると、スペース所要量は安定化します。この場合、おそらく考えられる最大スペース所要量よりもはるかに少ない所要量で安定化します。例えば、あるユーザー ID に対してあらゆる属性を付与して除去するコマンドが実行された場合は、ユーザー・プロファイルのコマンド監査証跡に必要な最大スペースが使用されます。この場合、20 個の属性に 2 つのイベント (付与と除去) を記録するためのスペースが必要です。このスペースは合計で 20 * 58 バイト = 1160 バイトになります。

ただし、通常は各ユーザー ID に対して 1 つまたは 2 つの属性しか管理されません。この場合、見積もられるストレージはユーザー ID ごとに 60 バイトです。

データ・セットおよび一般リソースの場合は、ストレージ必要量が主にアクセス・リスト項目によって異なります。各アクセス・リスト項目には 34 バイトが必要です。最大数の 64 個のアクセス・リスト項目が記録されると、必要量は 2176 バイトとなります。ほとんどのプロファイルでは、全体的なアクセス・リスト・アクティビティーは 20 個の項目で安定化することが多いため、その場合の必要量は 680 バイトになります。

以下の表に、各タイプの情報のスペース所要量を示します。また、各プロファイルで平均的に必要となるストレージ量の見積もりも示します。RACF データベースで実際に必要となるスペースは、環境での RACF コマンド・アクティビティーに大きく依存します。

表 7. 監査データ・タイプごとのストレージの見積もり

データ・タイプ	クラス	最小	最大	最大項目数	合計	見積もり
Segment	ユーザー	33	80	15	1200	56
Segment	グループ	33	80	4	320	56
Segment	データ・セット	33	80	2	160	0
Segment	一般	33	80	10	800	56
Attr	ユーザー	33	58	20	1060	64
Attr	グループ	33	58	6	348	64
Attr	データ・セット	33	58	10	580	64
Attr	一般	33	58	13	754	64
Connect	ユーザー	43	2249	1	2057	168
GrpAttr	ユーザー	42	2185	7	15295	195
ACL	データ・セット	42	2185	1	2185	319
ACL	一般	42	2185	1	2185	319
Member	トランザクション・グループ	47	2505	1	2505	2505
Member	一般	47	2505	1	2505	369

USRDATA 項目の内部フォーマット

このセクションの情報は、zSecure Command Verifier によって保守される USRDATA 項目を手動で検査したいユーザー、またはこれらのフィールドでの問題を診断する必要があるユーザーにのみ関係します。

各プロファイルでは、関連情報が複数の USRDATA フィールドに保持されています。USRDATA は、名前/値ペアとしてアクセスされます。USRNAME フィールドは、対応する USRDATA フィールドに保持されている情報を表します。USRNAME には以下の値が使用されます。

```
$C4RS seg    profile segment seg
$C4RA att    profile attribute att
$C4RCONN     connect groups
$C4RC att    connect group attribute att
$C4RPACL     access list
$C4RRMEM     member list
```

対応するデータ・フィールドには、EBCDIC フォーマットの情報が入っています。これらのデータ・フィールドの情報は、プロファイル・クラスに固有です。例えば、USER の場合は属性が SPECIAL (省略形は SPC) となり、GROUP の場合は TERMUACC 属性が入ります ($C4RATRM で表されます)。

それぞれのセグメントや属性のデータ・フィールドは、複数の統計を含んだデータ・ブロックとして扱われます。その特定の属性またはセグメントのさまざまなイベント (追加、変更、除去) が、1 つの統計ブロックに保持されます。アクセス・リ

スト関連のフィールドについては、最後の 64 個の userid 値が 1 つのブロックにまとめて保持されます。データのフォーマットは以下のとおりです。

$C4RSseg

このフィールドは、1 つのセグメントに関する情報を保持するために使用されます。4 つのサブフィールドがあり、互いにコンマで区切られています。セグメントの追加、変更、削除に関する情報が、セミコロンで区切られます。以下のサブフィールドが存在します。

Action

この情報が、セグメントの追加 (A)、変更 (C)、または削除 (D) のどれに関連するかを示す文字。

DATETIME

コマンド発行日時の 10 文字。フォーマットは YYDDD/HHMM です。

User ID

セグメントを処理したユーザーの最大 8 文字の**ユーザー** ID。

RC RACF コマンド、またはプリコマンド、ポストコマンドの 2 桁の最大戻りコード。

TSO セグメントに対する項目の例を以下に示します。

```
A,09220/0801,CRMBTST,00;C,09221/0815,IBMUSER,00
```

$C4RAatt

このフィールドは、プロファイルに対して追加または除去された属性に関する情報を保持するために使用されます。4 つのサブフィールドがあり、互いにコンマで区切られています。それぞれのアクションに関する情報は、セミコロンで区切られます。以下のサブフィールドが存在します。

Action

この情報が、属性の追加 (A)、変更 (C)、または削除 (D) のどれに関連するかを示す文字。

DATETIME

コマンド発行日時の 10 文字。フォーマットは YYDDD/HHMM です。

User ID

属性を処理したユーザーの最大 8 文字の**ユーザー** ID。

RC RACF コマンド、またはプリコマンド、ポストコマンドの 2 桁の最大戻りコード。

SPECIAL 属性に対する項目の例を以下に示します。

```
A,09181/0917,IBMUSER,00;D,09181/0920,IBMUSER,00
```

$C4RCONN

このフィールドは、ユーザーからグループへの接続に関する情報を保持するために使用されます。このフィールドはユーザー・プロファイルに保持されます。最後の 64 件の変更のみがプロファイルに保持されます。5 つのサブフィールドがあり、互いにコンマで区切られています。それぞれの接続グループに関する情報は、セミコロンで区切られます。以下のサブフィールドが存在します。

Group
ユーザーが接続されているグループ。

Auth および **UACC**
これらの文字は、ユーザーがこの GROUP を現行接続グループとして使用してログオンしている場合に、グループでの権限と新規データ・セットの UACC を表します。権限には、
Use、c**R**eate、**C**onnect、または **J**oin を指定できます。UACC には、None、Execute、Read、Update、Control、または Alter を指定できます。

DATETIME
コマンドが実行された日時を示す 10 文字。フォーマットは YYDDD/HHMM です。

User ID
この接続を最後に変更したユーザーの最大 8 文字の**ユーザー** ID。

RC RACF コマンド、またはプリコマンド、ポストコマンドの 2 桁の最大戻りコード。

項目の例を以下に示します。

```
SYS1,JR,09245/0545,C4RTEST,08
```

$C4RCatt
このフィールドは、ユーザーのグループ属性に関する情報を保持するために使用されます。このフィールドはユーザー・プロファイルに保持されます。最後の 64 件の変更のみがプロファイルに保持されます。5 つのサブフィールドがあり、互いにコンマで区切られています。それぞれの接続グループに関する情報は、セミコロンで区切られます。以下のサブフィールドが存在します。

Group
この属性が適用されるグループ。

Action
この情報が、属性の追加 (A) または削除 (D) のどちらに関連するかを示す文字。

DATETIME
コマンド発行日時の 10 文字。フォーマットは YYDDD/HHMM です。

User ID
この接続を最後に変更したユーザーの最大 8 文字の**ユーザー** ID。

RC RACF コマンド、またはプリコマンド、ポストコマンドの 2 桁の最大戻りコード。

項目の例を以下に示します。

```
SYS1,A,09245/0550,C4RTEST,00;SYS1,D,09245/0555,C4RTEST,00
```

$C4RPACL
このフィールドは、データ・セットおよび一般リソース・プロファイルのアクセス・リストに関する情報を保持するために使用されます。最後の 64 件の変更のみがプロファイルに保持されます。5 つのサブフィールドがあり、

互いにコンマで区切られています。アクセス・リスト内のそれぞれのユーザー/グループに関する情報は、セミコロンで区切られます。以下のサブフィールドが存在します。

User ID
アクセス・リスト項目。RACF ユーザー ID、グループ ID、アスタリスク、または特殊値 &RACUID のいずれかです。

Access level
付与されたアクセス・レベルを表す文字 (N(one)、E(xecute)、R(ead)、U(pdate)、C(ontrol)、A(lter)、または D(elete))。

DATETIME
コマンド発行日時の 10 文字。フォーマットは YYDDD/HHMM です。

User ID
このアクセス・リスト項目を最後に変更したユーザーの最大 8 文字のユーザー ID。

RC RACF コマンド、またはプリコマンド、ポストコマンドの 2 桁の最大戻りコード。

項目の例を以下に示します。

```
IBMUSER,R,09245/0545,C4RTEST,00
```

$C4RRMEM
このフィールドは、グループ化リソース・クラス内のプロファイルのメンバー・リストに関する情報を保持するために使用されます。最後の 64 件の変更のみがプロファイルに保持されます。4 つのサブフィールドがあり、互いにコンマで区切られています。それぞれのメンバーに関する情報は、セミコロンで区切られます。以下のサブフィールドが存在します。

Member
メンバー名。この名前の通常のフォーマットは、対応するメンバー (非グループ化) クラス内のプロファイルのフォーマットと同じです。

Action
この情報が、メンバーの追加 (A) または削除 (D) のどちらに関連するかを示す文字。

DATETIME
コマンド発行日時の 10 文字。フォーマットは YYDDD/HHMM です。

User ID
このメンバーを最後に追加または削除したユーザーの最大 8 文字のユーザー ID。

RC RACF コマンド、またはプリコマンド、ポストコマンドの 2 桁の最大戻りコード。

項目の例を以下に示します。

```
'SYS1.LINKLIB'//NOPADCHK,A,09249/1419,C4RTEST,00
```

または

```
TEST.CEMT,A,09249/1421,C4RTEST,00;TEST.CEDA,A,09249/1421,C4RTEST,00
```

コマンド監査用のポリシー・プロファイル

インストール監査員がコマンドの詳細な監査を活動化できるように、zSecure Command Verifier には、いくつかの追加の RACROUTE REQUEST=AUTH 要求が含まれています。これらの要求の結果として、特殊な監査専用ポリシー・プロファイルへのアクセスの成功時に SMF のレコードが書き込まれるようになります。成功したアクセスのみが記録され、これらのポリシー・プロファイルへの失敗したアクセスは使用されません。監査専用ポリシー・プロファイルへのアクセスが、RACF コマンドまたはキーワードの使用を制御する目的で使用されることはありません。

以下のタイプの監査専用プロファイルがサポートされています。

- SMF レコードの LOGSTR 内の RACF コマンド全体を記録するために使用するポリシー・プロファイル。
- グループ SPECIAL のようなグループ・レベルの属性の使用を記録するために使用するポリシー・プロファイル。

これらのタイプについては、以降のセクションで説明します。

コマンド全体を監査するためのポリシー・プロファイル

コマンド全体の監査専用ポリシー・プロファイルは、XFACILIT リソース・クラスで定義することができます。これらのプロファイルには、監査するデータのタイプと、RACF コマンドが含まれています。監査は、XFACILIT クラス内の特定のポリシー・プロファイルに対する監査専用の RACROUTE REQUEST=AUTH によって行われます。zSecure Command Verifier が RACF コマンドを構文解析した後に、完全なコマンドが SMF レコード内に追加データとして記録されます。

以下のプロファイルが使用されます。

- 端末ユーザーによって実行された変更されていないコマンドのプロファイル
- 実行のために RACF に渡されたコマンドのプロファイル
- エラー・メッセージを記録するために使用されるプロファイル

AUDIT(SUCCESS) は、どのユーザーをどの環境で監査するかを制御する UACC およびアクセス・リストと組み合わせて使用できます。プロファイルに対するアクセス権限が、zSecure Command Verifier によるポリシーの決定に使用されることはありません。すべてのコマンドを完全に監査する場合に優先される設定は、**UACC(READ)** および **AUDIT(ALL(READ))** です。

- **C4R.PREAUD.***COMMAND* は、端末ユーザーから入力されたコマンド・ストリングを監査する必要があるかどうかを指定します。完全なコマンド・ストリングは、生成された SMF レコードの LOGSTRING で確認できます。
- **C4R.PSTAUD.***COMMAND* は、zSecure Command Verifier 処理の後のコマンド・ストリングを監査する必要があるかどうかを指定します。完全なコマンド・ストリングは、生成された SMF レコードの LOGSTRING で確認できます。
- **C4R.ERRMSG.***COMMAND* は、zSecure Command Verifier から出されたエラー・メッセージまたは警告メッセージを記録します。このメッセージは、このプロファイルに対して生成される SMF レコードの LOGSTRING で確認できます。

これらのプロファイルに対して成功したアクセスのみが記録されます。アクセス・リストを選択することで、どのユーザーによって実行されたどのコマンドを記録するかを制御できます。アクセス権限を持つユーザーのみが、SMF によって追跡されます。アクセス権限を持たないユーザーは追跡されません。

これらのコマンド監査プロファイルとそのアクセス・リスト (または UACC) の定義は、これらのコマンドの監査にのみ関係します。これらのプロファイルが、コマンドまたはキーワードの実行を制御するために使用されることはありません。

要約すると、監査員が監査を活動化するには、以下のアクションを実行する必要があります。

- RACF XFACILIT リソース・クラスでプロファイルを定義します (例: C4R.PREAUD.ADDUSER)。
- 監査対象のユーザーに対し、READ 以上の UACC およびアクセス・リスト (ACL) を設定します。
- コマンドの使用を監査する場合は、AUDIT(SUCCESS(READ)) を設定します。
- AUDIT(FAIL(....)) の設定は無効です。これは、zSecure Command Verifier がこれらのプロファイルに対する失敗したアクセスの監査をサポートしていないためです。

使用される XFACILIT プロファイルは、**C4R.PREAUD.***command* のように構成されます。修飾子は、以下のように設定できます。

最初の修飾子**:**

C4R これらのプロファイルが zSecure Command Verifier に関連することを示す固定の接頭部。

2 番目の修飾子**:**

PREAUD
端末ユーザーによって入力されたコマンドの場合

PSTAUD
ポリシー・ルーチンによって変更され承認された後のコマンドの場合

ERRMSG
コマンドがポリシー・ルーチンによって拒否された場合のエラー・メッセージ

3 番目の修飾子**:**

command
監査されるコマンドを示す可変部分。これは、端末ユーザーによって入力された、省略されていない完全な RACF コマンドです。

総称プロファイルを使用することが可能です。すべてのコマンドを監査する場合、インストール監査員は **UACC(READ)** および **AUDIT(SUCCESS(READ))** を指定したプロファイル C4R.PREAUD.* を定義します。これによって、これらのプロファイルへのアクセスに関する標準の RACF 監査レコードが生成されます。LOGSTR 監査

は、ユーザーによって実行されるコマンド、またはポリシーによる指定に従って変更されるコマンドです。コマンドが 255 文字を超えている場合は、最初の 255 文字のみが表示されます。

監査の指定に使用されるプロファイルの例を以下に示しています。このプロファイルでは、ポリシー・ルーチンによる検査や変更の前に、すべてのユーザーを対象に **ADDUSER** コマンドを監査する必要があることを示しています。ユーザー IBMUSER によって ADDUSER が実行された場合は、監査が行われないようにしています。

```
C4R.PREAUD.ADDUSER   UACC(READ) AUDIT(SUCCESS(READ))
                     IBMUSER(NONE)
```

機密フィールドは監査証跡に含まれません。例えば、システム管理者があるユーザー ID のパスワードをリセットするコマンドを実行した場合、新しいパスワード値は監査ストリングに含まれません。セッション鍵やパスチケット暗号鍵といったその他の機密フィールドも、同じく機密情報として抑止されます。

グループ SPECIAL の使用のためのポリシー・プロファイル

(グループ) SPECIAL の使用のための監査専用ポリシー・プロファイルを、XFACILIT リソース・クラスで定義することもできます。このプロファイルには、特定の RACF 管理範囲の使用を記録することが目的であることを示す特別な修飾子 USESCOPE が付きます。

AUDIT(SUCCESS) は、どのユーザーをどの環境で監査するかを制御する UACC およびアクセス・リストと組み合わせて使用できます。プロファイルに対するアクセス権限が、zSecure Command Verifier によるポリシーの決定に使用されることはありません。すべてのコマンドを完全に監査する場合に優先される設定は、UACC(READ) および AUDIT(ALL(READ)) です。以下のプロファイルが使用されます。

- **C4R.USESCOPE.***group*

  修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、コマンドのターゲット・プロファイルに対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 =SYSTEM が使用されます。

  これらのポリシー・プロファイルのすべての修飾子を、総称文字で表すことができます。

これらのプロファイルに対して成功したアクセスのみが記録されます。アクセス・リストを選択することで、どのユーザーによって実行されたどのコマンドを記録するかを制御できます。アクセス権限を持つユーザーのみが、SMF によって追跡されます。アクセス権限を持たないユーザーは追跡されません。

これらの USESCOPE プロファイルを使用して管理範囲の使用が記録されているポリシーは、この資料の残りの部分でそのように示されます。

zSecure Audit のレポートの例

zSecure Audit では、zSecure Command Verifier ポリシー・ルーチンの評価 (RACF コマンドの変更を伴う場合もある) の実行前後に入力された RACF コマンドに関するレポートを生成することができます。

このようなレポートは、zSecure Audit の対話式インターフェースから生成できます。「**EV.R**」を選択し、リソース・クラス XFACILIT およびリソース C4R.** を指定します。以下の画面は入力例を示しています。

```
   Menu         Options       Info     Commands     Setup
_____________________________________________________________________________
                  zSecure Suite - Events - Resource Selection
Command ===> _____________________________________________   _ start panel

Show records that fit all of the following criteria:
Resource  . . . . . C4R.**_____________________________________
Class . . . . . . . XFACILIT     (class or EGN mask)
Profile/rule/permit _____________________________________________
System  . . . . . . ____         (system name or EGN mask)

Advanced selection criteria
_  Date and time         _  Further resource 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 *8. zSecure Command Verifier* 監査レポートを生成するための入力

zSecure Command Verifier 用の zSecure Audit カスタム・レポートを作成することもできます。以下の例 (SC4RSMP 内のメンバー C4RCNA00 にもあります) は、zSecure Audit バージョン 2.3.0 を使用している場合にカスタム表示として使用できます。ほとんどのコマンドが、レポートに表示される情報に関連します。以下の行は、zSecure Command Verifier がポリシーを処理する前の RACF コマンドの選択基準です。

```
S CLASS=(XFACILIT) PROFILE=(C4R.PREAUD.**)
```

以下の行は、zSecure Command Verifier がポリシーを処理した後の RACF コマンドの選択基準です。

```
S CLASS=(XFACILIT) PROFILE=(C4R.PSTAUD.**, C4R.ERRMSG.**)
```

残りの zSecure Audit ステートメントは、レポートのレイアウトに関する詳細情報を提供します。変数を XFACILIT プロファイルのサブストリングと定義しているのはその一例です。このサブストリングは、端末ユーザーによって実行される RACF コマンドです。示されている例では、zSecure Command Verifier ポリシー処理の前後のすべての RACF コマンドの結合レポートが生成されます。MERGELIST/ENDMERGE ステートメントを削除すると、3 つの独立したレポートが生成されます。

結合レポートの出力例を以下に示しています。端末ユーザーは、OPERATIONS キーワードの指定を許可されていませんでした。このキーワードは、ポリシー・プロファイル処理の際に RACF コマンドから除去されます。

```
1S M F   R E C O R D   L I S T I N G    3May07 01:45 to 13May07 22:36
 RACF Commands processed by Command Verifier

 Date      Time               Resource

 08Dec2001 23:49 Before PIER   ALTUSER
 System ID                     SYS1 Fri 11 May 2007 23:49
 RACF userid/ACF2 logonid      BCSCGB2
 User name                     GUUS SECONDARY ID
 SAF profile key               C4R.PREAUD.*
 SAF resource name             C4R.PREAUD.ALTUSER
 RACF Command                  ALTUSER  BCSCGB3 OPER

 08Dec2001 23:49 After  PIER   ALTUSER
 System ID                     SYS1 Fri 11 May 2007 23:49
 RACF userid/ACF2 logonid      BCSCGB2
 User name                     GUUS SECONDARY ID
 SAF profile key               C4R.PSTAUD.*
 SAF resource name             C4R.PSTAUD.ALTUSER
 RACF Command                  ALTUSER  BCSCGB3
```

図 *9. zSecure Audit* レポート*: zSecure Command Verifier* ポリシー処理の前後の *RACF* コマンド

SMF による通常のアクセス記録

zSecure Command Verifier では、示されているプロファイルでコマンド全体が監査されるだけでなく、個々のキーワードも監査されます。zSecure Command Verifier は、決定プロセスで使用されたプロファイルに対して、成功したアクセスと失敗したアクセスのレコードを生成します。

例えば、プロファイル C4R.USER.ID.CRMB* で新規ユーザー CRMBTST の定義が許可された場合は、このプロファイルに対してアクセス成功イベントが記録されます。ポリシー・プロファイルがフィールドを指定された値に設定する処理を拒否した場合は、そのポリシー・プロファイルに対して違反イベントが記録されます。

これらのタイプの SMF レコードの作成は、プロファイルに対する標準の RACF 監査設定によって制御されます。つまり、RACF のデフォルトを使用する場合は、失敗したアクセスのみが監査されます。ただし、この設定を AUDIT(ALL(READ)) に変更することができます。これによって、成功したアクセスと失敗したアクセスの両方が記録されます。

一般に、zSecure Command Verifier では、ポリシー・プロファイルが決定プロセスで使用された場合にのみ、SMF イベントが作成されます。例えば、新しいユーザー ID の命名規則に関するいくつかのポリシー・プロファイルがあります。新しいユーザー ID が、あるポリシー・プロファイルで拒否され、別のプロファイルで受け付けられた場合は、その新しいユーザー ID の名前を許可したプロファイルのみが、SMF によって記録されます。その他のポリシー・プロファイルは、このユーザー ID の作成を許可していてもしていなくても、SMF によっては記録されません。

このプロセスを理解するために役立つ例を挙げます。2 つのユーザー ID 命名規則ポリシー・プロファイルがあるとします。最初のポリシー・プロファイルには、新しいユーザー ID の先頭の 3 文字が端末ユーザーと同じでなければならないことが

指定されています。2 番目のポリシー・プロファイルには、最初の 3 文字が C4R であれば、新しいユーザー ID が許可されることが指定されています。

```
C4R.USER.ID.&RACUID(3)        UACC(UPDATE)
C4R.USER.ID.C4R*              UACC(UPDATE)
```

ここで、ユーザー IBMUSER が、新しい userid を定義するとします。

```
ADDUSER C4RTEST DFLTGRP(C4R) OWNER(C4R)
```

端末ユーザー (IBMUSER) がターゲット・ユーザー (C4RTEST) と適合しないため、最初のポリシー・プロファイルは当てはまりません。ターゲットの USERID は C4R で始まっているため、2 番目のプロファイルは当てはまります。この場合 zSecure Command Verifier では、以下のように 2 番目のプロファイルに対するアクセスの成功が記録されます。

```
Resource:      C4R.USER.ID.C4RTEST
Profile:       C4R.USER.ID.C4R*
Access:        UPDATE
User           IBMUSER
```

通常、アクセス検査に使用されるリソース名、および SMF レコードには、端末ユーザーによって指定されたフィールドの値が入ります。例えば、IBMUSER をアクセス・リストに追加するための **PERMIT** コマンドが、以下のように C4RTEST によって実行され、それが許可されたとします。

```
PERMIT 'SYS1.PARMLIB' ID(IBMUSER) AC(UPDATE)
```

この場合は、以下のように成功のアクセス・イベントが作成されます。

```
Resource:      C4R.DATASET.ACL.IBMUSER.UPDATE.SYS1.PARMLIB
Profile:       C4R.*.ACL.*.UPDATE.**
Access:        UPDATE
User:          C4RTEST
```

ポリシー・プロファイルへのアクセスは、標準の SMF レポート作成ツール (IBM Security zSecure Audit など) または IRRADU00 を使用して報告できます。

第 5 章 ポリシー・プロファイル

zSecure Command Verifier では、XFACILIT リソース・クラス内のポリシー・プロファイルからインストール・ポリシーを定義できます。

最高のパフォーマンスを得るために、zSecure Command Verifier ポリシー・プロファイルに **RACLIST** 処理を行います。インストールでリソース・クラスの **RACLIST** 処理を行わない場合、zSecure Command Verifier は RACROUTE REQUEST=LIST を内部で発行します。プロファイルへの変更を有効にするには、RACLIST 処理が行われたリソース・クラスをリフレッシュする必要があります。zSecure Command Verifier ポリシー・プロファイルへの変更を完了した後は必ず、**SETROPTS RACLIST**(*class*) **REFRESH** コマンドを発行する必要があります。

zSecure Command Verifier リソース・クラスが SETROPTS 出力で GLOBAL RACLIST ONLY と表示される場合、RACF の一部のリリースでは、**SETROPTS RACLIST**(*class*) **REFRESH** コマンドを発行しなければならないことが管理者に警告されないことがあります。zSecure Command Verifier のパフォーマンスに関しては必要ありませんが、**SETROPTS RACLIST**(*class*) コマンドを発行して、関連するすべての zSecure Command Verifier ポリシー・プロファイルをデータ・スペースにロードすることができます。これを行うと、大部分の RACF コマンドで、プロファイルへの変更を有効にするにはプロファイルをリフレッシュする必要があることを知らせる警告メッセージが発行されます。

重要: C4R.** または ** などの最上位の総称プロファイルを定義しないでください。総称プロファイルを定義すると、指定されたアクセス権限に応じて、以下のアクションが発生します。

- 特定性の高いプロファイルが定義されていない RACF コマンドがすべて失敗します。
- zSecure Command Verifier の制御がすべてバイパスされます。

ポリシー・プロファイルの構文

zSecure Command Verifier で使用されるポリシー・プロファイルは、XFACILIT リソース・クラスで定義されている必要があります。または、zSecure Command Verifier で使用するために、別の RACF リソース・クラスを指定することもできます。

通常、ポリシー指定に使用されるプロファイルには 4 つの修飾子があります。最初の修飾子は常に C4R であり、これらのプロファイルが zSecure Command Verifier 用のものであることを示します。2 番目の修飾子は、制御の適用先となるプロファイルのタイプを示します。2 番目の修飾子の例として、USER、GROUP、データ・セット、TCICSTRN などがあります。3 番目の修飾子は、制御される機能またはフィールドの標識として使用されます。例えば、ID、OWNER、NOTIFY、ATTR、UACC などです。4 番目の修飾子は、特定の機能またはフィールドに値を指定することができます。例えば、READ、JOIN、*groupname* などです。一部のタイプのポリシー・プロファイルでは、このポリシーが適用されるプロファイルを指定するために追加の修飾

子もサポートされています。これらの追加修飾子は、主に規則に例外を許可することを目的としています。一般的なパターンに沿ったポリシー・ルールの 2 つの例を以下のリストに示します。

- **C4R.DATASET.UACC.READ.SYS1.****

  このプロファイルは、パターン SYS1.** と一致するデータ・セットに対して UACC を設定する権限を制御します。このポリシー・プロファイルによって明示的に制御される唯一の UACC 値は READ です。

- **C4R.USER.DFLTGRP.SYS1.****

  このプロファイルは、DFLTGRP としてグループ SYS1 を選択する権限を制御します。ポリシー・プロファイルの最後に付けられている ** は、これがすべてのユーザー ID に適用されることを示しています。

さらに、特定の修飾子用の特殊値がこれらのプロファイルに実装されます。範囲外のターゲット・プロファイル (ユーザー、グループ、データ・セットなど) を参照するには、/SCOPE を使用します。/SCOPE ポリシー・プロファイルは、範囲外 のプロファイルを処理する権限を制御します。その他の特殊修飾子は、= (等号) によって表されます。これらの修飾子は、同等 タイプのポリシーを記述するために使用されます。これらのタイプの特殊修飾子の例を以下のリストに示します。

- **C4R.USER.PASSWORD.=DFLTGRP**

  このプロファイルは、ユーザーのデフォルト・グループ DFLTGRP と等しいパスワードを設定する権限を制御します。

- **C4R.USER.=OWNER.IBM***

  このプロファイルは、パターン IBM* と一致するユーザー ID の所有者が、特定の値と等しくなければならないことを指定します。値は、ポリシー・プロファイルの **APPLDATA** フィールドに指定されます。

スラッシュ「/」や等号「=」などの特殊文字で始まる特殊修飾子がポリシー・プロファイルに含まれている場合は、その修飾子全体がポリシー・プロファイルに含まれている必要があります。総称文字を使用してこの修飾子を表すことはできません。ポリシー・プロファイル内のその他の修飾子は、総称文字で表すことができます。例えば、ユーザーのデフォルト・グループと等しいパスワードを設定する権限は、次のポリシーによって制御されます。

```
C4R.USER.PASSWORD.=DFLTGRP
```

このポリシーは、以下のポリシー・プロファイルによって表すことができます。

```
C4R.USER.*.=DFLTGRP
C4R.**.=DFLTGRP
C4R.*.PASS*.=DFLTGRP
```

このポリシーは、以下のいずれのプロファイルによっても表されません。

```
C4R.**
C4R.USER.PASSWORD.*
C4R.USER.*.=DFLT*
```

この規則には、いくつかの例外があります。これらの例外は、ポリシー・プロファイルの詳細説明に記載されています。

zSecure Command Verifier で使用されるポリシー・プロファイルは、2 つの異なるカテゴリーに分類されます。最初のカテゴリーは、製品全体で使用される一般プロファイルです。これは、コマンド自体ではなく、コマンドの結果を表します。ポリシー・プロファイルにはターゲット・プロファイルおよびフィールドを記述する修飾子 (**DATASET.ACL** など) が含まれますが、ACL の変更に使用された実際のコマンド (**PERMIT** コマンド) への参照は含まれません。2 番目のタイプのプロファイルは、特定のコマンド、またはコマンド・キーワードに焦点を当てたプロファイルです。これらのポリシー・プロファイルは、例えば **LISTUSER** コマンドの実行中にシステム Special を一時的に付与する場合などに使用されます。それらには、ポリシー・プロファイル内の修飾子として、**ALTUSER** のような実際のコマンドが含まれます。

フィールド値ポリシー・プロファイルは、特定のフィールドを追加または変更すること、あるいは特定のフィールドを特定のプロファイル用の指定された値に設定することを許可、不許可、または強制するために使用されます。コマンド関連のポリシー・プロファイルは、フィールドや値の制御を許可するのではなく、機能性のみをコマンド全体に提供します。

通常、プロファイルを定義しない場合は、zSecure Command Verifier は特定のポリシーが存在しないかのように動作し、権限の決定を RACF 委任します。その後、zSecure Command Verifier が実装されていないかのように、標準 RACF 処理が行われます。ポリシー・プロファイルが存在する場合は、アクセス・リストおよび UACC からのアクセス・レベルが以下のように解釈されます。

プロファイルが見つからない
: ポリシー・ルールが実装されていません。

NONE
: 端末ユーザーが、ポリシー・ルールによって記述されている要件を満たしていません。ほとんどの場合、コマンドは拒否されます。必須値ポリシー・プロファイルについては、77 ページの『必須値およびデフォルト値ポリシー・プロファイル』を参照してください。必須値は適用されません。

READ
: NONE と同じ。また多くの場合、属性を削除したり、初期値を指定したりするには、READ アクセス権限では十分です。

UPDATE
: 端末ユーザーは、ポリシー・ルールによって記述されているすべての要件を満たしています。コマンドは続行します。

CONTROL
: ポリシー・ルールは、この端末ユーザーに適用されません。

この一般的な使用法が特定のポリシー・ルールにどのように適用されるかについて詳しくは、各プロファイルごとの個別の説明を参照してください。

警告モードの回避

zSecure Command Verifier は、ポリシー・プロファイルでの警告モードの使用をサポートしていません。アクセスの決定は、標準アクセス・リスト (ACL) および汎用アクセス (UACC) に基づいて行われます。

zSecure Command Verifier ポリシー・プロファイルで警告モードを使用すると、紛らわしい結果が生じる可能性があります。例えば、警告モードを有効にすると、ICH408I メッセージ
WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED を受け取ります。ところが、ポリシーに対するアクセス権限は付与されず、処理は終了します。

このような紛らわしいメッセージが出される理由は、zSecure Command Verifier が必要なアクションを判別して処理が終了するときに、RACF 監査のみの要求を使用して SMF によって適切な監査証跡が作成されるためです。監査のみの要求によって、ICH408I WARNING メッセージが発行されます。zSecure Command Verifier は、この監査のみの要求に対する RACF の応答を無視します。

グローバル・アクセス検査 (GAC) の回避

zSecure Command Verifier は、ポリシー・プロファイルのグローバル・アクセス検査 (GAC) の使用をサポートしていません。アクセスの決定は、標準アクセス・リスト (ACL) および汎用アクセス (UACC) に基づいて行われます。

zSecure Command Verifier は、ポリシー・プロファイルのグローバル・アクセス検査 (GAC) の使用をサポートしていません。アクセスの決定は、標準アクセス・リスト (ACL) および汎用アクセス (UACC) に基づいて行われます。ほとんどのポリシーの決定では、GAC テーブルは完全に無視されます。しかし、SMF によって監査証跡を作成する監査のみの要求は、GAC テーブルで処理されます。GAC テーブルの項目が該当する場合、ポリシーによって許可されているキーワードおよびパラメーターの監査が抑止される場合があります。

RACFVARS プロファイル

必要なパターンに適合しない従来の文字を使用できるようにするために、ポリシー・プロファイルで RACFVARS を指定できます。RACFVARS プロファイルでは、ユーザー ID の命名規則用に複雑なパターンを指定することもできます。

一部のポリシー・プロファイル、および一部の APPLDATA 値において、zSecure Command Verifier は =RACUID、=RACGPID、=USERID、=GROUP などの特殊値を使用します。=RACUID は、RACF 組み込み変数 &RACUID のように機能します。しかし、RACF はアンパーサンド (&) を特殊文字として扱うため、zSecure Command Verifier ポリシー・プロファイルのような一般リソース・プロファイルではこの特殊文字を使用することはできません。このため、代わりに等記号 (=) が使用されています。以下に、4 つの特殊値とその一般的な意味を示します。

=RACUID
コマンドを発行する端末ユーザーの userid。

=RACGPID
コマンドを発行する端末ユーザーの接続グループのリスト。これは RACF &RACGPID を使用する場合とは異なります。RACF はその接続グループ・リストを使用して現行接続グループのみを表しますが、zSecure Command Verifier はすべての接続グループに対してそれを使用します。

=USERID
コマンドに指定されているRACF USERID。

=GROUP

コマンドに指定されている RACF GROUP。

大部分のポリシー・プロファイルでは、これらのデフォルト変数のほかに RACFVARS も使用できます。これらの変数は、通常の総称文字が許可されるが、従来の総称文字 (%、*、および .**) は必須パターンに合わないすべての場所で使用することができます。 RACF 変数の従来の使用例を以下に示します。ユーザー ID については、2 つのデフォルト・グループのみを使用できます。 2 つのプロファイルを定義できますが、1 つのポリシー・プロファイルを定義して、RACF 変数を使用して正確な値を指定することもできます。

```
RDEFINE XFACILIT C4R.USER.DFLTGRP.DEPTA.*
RDEFINE XFACILIT C4R.USER.DFLTGRP.DEPTS.*
```

または

```
RDEFINE RACFVARS &DFLTGRP ADDMEM(DEPTA, DEPTS)
RDEFINE XFACILIT C4R.USER.DFLTGRP.&DFLTGRP*
```

RACFVARS を使用する別の例として、ユーザー ID 命名規則に対応した、より複雑なパターンを指定する場合が挙げられます。インストールでは、以下の命名規則が使用されると想定します。

- 先頭文字は S、T、U、V、または W です。
- 先頭文字が S の場合、通常、その後に 3 桁の数字が続きます。ただし、3 桁目が 8 または 9 である場合は 1 桁追加され、計 4 桁の数字が使用されます。
- 最初の文字が T、U、V、または W の場合、その後に常に 4 桁の数字が続きます。

この命名規則は、時間に沿った増加を明確に示しています。以前は、S で示されるユーザーの数は限られていました。より多くの userid 値が必要になると、2 桁の未使用の数字が使用され、追加桁の使用がシグナル通知されました。以下の userid 値に関する正誤表は、命名規則の法則を示しています。

correct	incorrect	
S000	S0002	(S plus 4 digits)
S784	S003H	(non-numeric 5th char)
S0082	S128	(3rd digit is 8, but no 4th digit)
S9194	SAHJ	(non-numerics)
U3425	U10255	(5 digits)
U9865	X0126	(illegal 1st char)
W2314	W813	(W plus 3 digits)

図 *10.* ユーザー *ID* 命名規則の例

この命名規則を有効にするために、RACFVARS を使用する zSecure Command Verifier ポリシー・プロファイルを使用できます。最初のステップは、使用されているさまざまな文字を認識すること、およびこれらの各種タイプに対して RACFVARS を定義することです。

```
RDEFINE RACFVARS &S ADDMEM(S)                    Special character
RDEFINE RACFVARS &F ADDMEM(T U V W)              First characters
RDEFINE RACFVARS &N ADDMEM(0 1 2 3 4 5 6 7 8 9)  Normal digits
RDEFINE RACFVARS &X ADDMEM(8 9)                  eXtension digits
RDEFINE RACFVARS &Y ADDMEM(0 1 2 3 4 5 6 7)      non-extension digits
```

次のステップで、これらの変数を使用し、3 つの有効なパターンを定義します。

```
&S&N&N&Y                S plus three digits (non-extension)
&S&N&N&X&N              S plus four digits (extension)
&F&N&N&N&N              T,U,V,W plus four digits
```

各ユーザー ID に対して 1 つのパターンのみが適用されるように、パターンは設計されています。例えば、&X と &Y の定義は重複しないため、どちらの最初の 2 つのパターンが適用されるかについて、あいまいになることはありません。最初のパターンが &S&N&N&N である場合、3 桁目が 8 のときに、あいまいさが生じます。

最後のステップで、zSecure Command Verifier ポリシー・プロファイルのセットで 3 つのパターンを使用します。

```
C4R.USER.ID.*           UACC(NONE)
C4R.USER.ID.&S&N&N&Y    UACC(NONE)  UPDATE(RACFADM)
C4R.USER.ID.&S&N&N&X&N  UACC(NONE)  UPDATE(RACFADM)
C4R.USER.ID.&F&N&N&N&N  UACC(NONE)  UPDATE(RACFADM)
```

最初のプロファイルで、命名規則に沿っていないユーザー ID は作成できないことが保証されます。後続の 3 つのプロファイルによって、RACFADM は 3 つのパターンのいずれかに従ってユーザー ID を作成できるようになります。**SETROPTS REFRESH RACLIST** コマンドを、RACFVARS クラスと XFACILIT クラスの両方に対して必ず発行してください。 XFACILIT クラスより前に、RACFVARS クラスに RACLIST 処理と REFRESH 処理を行う必要があります。

前述の例は、RACFVARS をポリシー・プロファイルでどのように使用できるかを示しています。これには、命名規則に沿ってパターンを定義する場合の利点が明らかに示されています。このようにすると、少数のポリシー・プロファイルで、かなり複雑な規則を十分に実装することができます。

ポリシー・プロファイルの選択

実装する一般ポリシーを決定し、その一般ポリシーに例外を許可するかどうかを決定するには、以下のガイドラインに従ってください。

すべての RACF コマンドおよびキーワードには、以下の基本制御項目が含まれています。

- 影響を受けるフィールドまたは属性
- コマンドを発行してフィールドまたは属性を設定する端末ユーザー
- 影響を受けるプロファイル

次の例は、これらの制御項目を示しています。

```
IBMUSER:    ALTUSER CRMAHJB DFLTGRP(SYS1)
```

制御項目には以下のものがあります。

- *DFLTGRP* の選択
- 端末ユーザー *IBMUSER*
- オブジェクト・ユーザー *CRMAHJB*

通常、ポリシーの設計はコマンド自体に基づいて行われるのではなく、コマンドの結果に基づいて行われます。このため、ポリシーは属性の値がどのように設定され

ているかに関係なく、その値を制御しようとします。例えば **DFLTGRP** の場合、ユーザー ID の作成中に値が設定されるのか、または後でユーザー ID の変更によって設定されるのかは関係ありません。最終結果は、何が制御されるかです。これはまた、大部分のポリシーでシステム SPECIAL または同様の権限が考慮されない主な根拠の 1 つでもあります。

DFLTGRP に対してポリシーを実装したいが、いずれのユーザーの **DFLTGRP** に対しても変更を行いたくない場合は、次のようにしてプロファイルを実装できます。

```
C4R.USER.DFLTGRP.**   UACC(NONE)   ACL(empty)
```

一般規則に例外を設ける場合、作成する例外のタイプを決定する必要があります。コマンドを実行した端末ユーザーに基づく例外が必要である場合は、ACL を変更し、端末ユーザーか、もしくは端末ユーザーのグループの 1 つに対して、UPDATE 権限を付与する必要があります。**DFLTGRP** 自体に基づいて例外を作成する場合は、次のように、**DFLTGRP** の名前を含むプロファイルを定義できます。

```
C4R.USER.DFLTGRP.SYS1.**
```

DFLTGRP の追加ポリシー・プロファイルについて詳しくは、 101 ページの『デフォルト・グループに対する追加のポリシー制御』を参照してください。

要約

要約すると、**DFLTGRP** 制御について、少なくとも 3 つのプロファイルを定義する必要があります。

```
C4R.USER.DFLTGRP.**          UACC(???)   ACL(empty)
C4R.USER.DFLTGRP./SCOPE.**   UACC(???)   ACL(empty)
C4R.USER.DFLTGRP./OWNER.**   UACC(???)   ACL(empty)
```

一般規則に例外を設けるには、以下のいずれかを指定します。

- 最初のプロファイルに追加修飾子を指定し、特定のユーザーが DFLTGRP として特定のグループを持つことを許可する
- アクセス・リストに追加ユーザーまたはグループを指定する
- 上述の 2 つの方法の組み合わせ

その他のポリシー・プロファイルも、同様の方法で評価する必要があります。

一般機能

前述の結果に関連するポリシー・プロファイルに加えて、zSecure Command Verifier はいくつかの一般プロファイルも使用します。

この領域のプロファイルの例として、FIELD アクセス・レベルの権限を持つ端末ユーザーがすべての RACF プロファイルに対してコマンドを実行できるか、あるいは通常の範囲内のプロファイルに対してのみコマンドを実行できるかを決定するプロファイルが挙げられます。

重要: C4R.** または ** などの最上位の総称プロファイルを定義しないでください。総称プロファイルを定義すると、指定されたアクセス権限に応じて、以下のアクションが発生します。

- 特定性の高いプロファイルが定義されていない RACF コマンドがすべて失敗します。
- zSecure Command Verifier の制御がすべてバイパスされます。

ユーザーの免除、違反の抑止、エラー処理

一般プロファイルは、特定のユーザーがすべての zSecure Command Verifier ポリシー・ルールから免除されるかどうか、およびポリシー違反やその他のエラー状態が生じた場合に zSecure Command Verifier が取らなければならないアクションを指定するために使用します。

該当する一般プロファイルは以下のとおりです。

- **C4R.EXEMPT**

  このプロファイルは、特定のユーザーがポリシー適用から免除されるかどうかを制御します。端末ユーザーに十分なアクセス権限がある場合、それ以上ポリシーは検査されません。コマンドがポリシーに違反していないか、また、コマンドを正常に実行するために免除が必要であるかを検出することはできません。次のコマンドを使用して、このポリシー・プロファイルに正常にアクセスできるかを監査する必要があります。

  ```
  RALT XFACILIT C4R.EXEMPT AUDIT(SUCCESS(UPDATE))
  ```

  このポリシー・プロファイルに対するアクセス・イベント用の LOGSTR には、入力したとおりのコマンドが含まれます。

  多くの場合、C4R.ERROR.CONTINUE ポリシー・プロファイルを使用することをお勧めします。このプロファイルを使用する主な利点は、すべてのポリシー・プロファイルが検査されること、およびアクセス・イベントのログ・ストリングを介して C4R.ERRMSG.command 監査プロファイルに、潜在的なポリシー違反を記録できることです。

  以下のアクセス規則が C4R.EXEMPT ポリシー・プロファイル用に適用されます。

  プロファイルが見つからない
  : いずれのユーザーもポリシー適用から免除されません。

  NONE
  : この端末ユーザーはポリシー適用から免除されません。

  READ
  : NONE と同じ。

  UPDATE
  : ユーザーは、いずれのポリシー・ルール検査または適用の対象になりません。各種コマンド・キーワードおよびオプションの監査証跡は作成されません。

  CONTROL
  : UPDATE と同じ。

- **C4R.SUPPRESS**

  このプロファイルは、zSecure Command Verifier が、指定したポリシーに対する違反となるキーワードおよびパラメーター値の抑止を試行する必要があるかど

うかを制御します。抑止できない場合、コマンドは拒否されます。この状況として考えられるのが、コマンドの抑止により、正しくないコマンドやポリシーに違反するコマンドが実行される場合です。このような状況は、例えば、端末ユーザーが別のユーザーのパスワードをその別のユーザーの DFLTGRP に明示的に設定しようとする場合に生じる可能性があります。新規パスワードの値を抑止すると、ポリシーが回避しようとする、まさにその状況に陥ってしまう可能性があります。このような場合、C4R.SUPPRESS ポリシー・プロファイルに対するアクセス権限に関係なく、zSecure Command Verifier によってコマンド全体が失敗します。以下のアクセス規則が適用されます。

プロファイルが見つからない
: キーワード抑止は試行されません。何らかのポリシー違反があると、コマンドは失敗します。

NONE
: この端末ユーザーに対して、キーワード抑止は試行されません。

READ
: NONE と同じ。

UPDATE
: 可能な場合、ポリシーに違反するキーワードおよびパラメーター値は抑止されます。前述のとおり、この抑止は常に行えるわけではありません。

CONTROL
: UPDATE と同じ。

- **C4R.ERROR.CONTINUE**

このポリシー・プロファイルは、ポリシー・プロファイルおよびポリシー違反の解釈中に発生したエラーの処理方法を指定するために使用されます。ポリシー・プロファイル・エラーの例としては、新規ユーザー ID に対して所有者と *dfltgrp* の循環定義が使用された場合が挙げられます。ポリシー違反の例としては、新規ユーザー ID に対して許可されない所有者が指定された場合が挙げられます。このプロファイルに対する UPDATE アクセスでは、ポリシー違反の通常の処理がバイパスされます。この場合も ICH408I メッセージは生成されますが、通常の zSecure Command Verifier 違反メッセージは抑止されます。このポリシーは主に、実装期間中にポリシーを指定変更する場合や、誤ったポリシー定義に対する応急の権限が必要である場合に使用されます。以下のアクセス規則が適用されます。

プロファイルが見つからない
: この制御は実装されません。いずれかのキーワードが受け入れられない場合、コマンドは拒否されます。

NONE
: エラーまたはポリシー違反が発生した場合、コマンドは拒否されます。

READ
: NONE と同じ。

UPDATE
: エラーまたはポリシー違反の発生に関係なく、コマンドの続行が許可されます。キーワードを追加または変更するポリシーが実行されます。

CONTROL
UPDATE と同じ。

端末ユーザーがプロファイルのリストを指定した場合、このポリシーを有効にする必要はありません。このような場合、プログラムではコマンド全体を終了するしかないときもあります。

また、一部のポリシー・ルールにより、コマンドを複数のコマンドに分割しなければならない場合もあります。コマンドの分割はサポートされていません。コマンドを正しく実行することはできないため、拒否されます。

メッセージ制御

いくつかのプロファイルは、特定の警告メッセージおよび情報メッセージが発行されるかどうかを制御します。

このようなプロファイルは以下のとおりです。

- **C4R.DEBUG**

  現在、このプロファイルは非推奨です。代わりに、C4R.=MSG.CMD プロファイルを使用してください。

- **C4R.=MSG.CMD**

  このプロファイルは、実行される前に RACF に渡されるコマンドを指定します。端末ユーザーは、プロファイルに対する READ 以上のアクセス権限が必要です。READ アクセス・レベルのみを使用してください。

  表示される RACF コマンドは、入力したコマンドと若干異なる場合があります。例えば、コマンド自体は常にその 1 次形式で表示され、考えられる別名の 1 つとして表示されることはありません。

  プロファイルが見つからない
  この制御は実装されません。コマンドは、実行前に表示されません。

  NONE
  コマンドは、実行前に表示されません。

  READ
  zSecure Command Verifier によって承認または変更された RACF コマンドは、実行前に表示されます。

  UPDATE
  READ と同じ。

  CONTROL
  READ と同じ。

- **C4R.=MSG.SUPPRESSED**

  このプロファイルは、キーワードまたはパラメーター値が抑止される場合に、メッセージ **C4R899W** が発行されるかどうかを制御します。バージョン 1.12 より前のバージョンでは、C4R.SUPPRESS ポリシー・プロファイルが有効な場合、これらのメッセージは自動的に発行されていましたが、現在は、このプロファイルも有効な場合しかメッセージは発行されません。

プロファイルが見つからない
この制御は実装されません。**C4R899W** メッセージは発行されません。

NONE
C4R899W メッセージは発行されません。

READ
キーワード抑止が行われると、メッセージ **C4R899W** が発行されます。

UPDATE
READ と同じ。

CONTROL
READ と同じ。

- **C4R.=MSG.MANDATORY**

このプロファイルは、zSecure Command Verifier ポリシーによって、ユーザー指定のキーワードまたはパラメーターの必須キーワード値またはパラメーター値の指定変更が行われた場合に、メッセージ **C4R899W** が発行されるかどうかを制御します。

プロファイルが見つからない
この制御は実装されません。**C4R899W** メッセージは発行されません。

NONE
C4R899W メッセージは発行されません。

READ
必須キーワード値またはパラメーター値の指定変更が行われた場合に、メッセージ **C4R899W** が発行されます。

UPDATE
READ と同じ。

CONTROL
READ と同じ。

- **C4R.=MSG.DEFAULTS**

このプロファイルは、zSecure Command Verifier ポリシーによって、ユーザー指定のコマンドを実行するためのデフォルトのキーワード値またはパラメーター値が提供された場合に、メッセージ **C4R899W** が発行されるかどうかを制御します。

プロファイルが見つからない
この制御は実装されません。**C4R899W** メッセージは発行されません。

NONE
C4R899W メッセージは発行されません。

READ
デフォルトのキーワード値またはパラメーター値が指定された場合に、メッセージ **C4R899W** が発行されます。

UPDATE
READ と同じ。

CONTROL
READ と同じ。

サイト固有のポリシー・メッセージ

zSecure Command Verifier では、製品に用意されている標準メッセージ以外に、サイト固有のメッセージを発行することができます。このセクションでは、この機能の内容と、そのようなメッセージを指定するための方法を説明します。

zSecure Command Verifier がポリシー違反を検出すると、必ず特定のメッセージが発行されます。例えば、管理者が ALTUSER コマンドを以下のような許可されていないオプションとともに発行すると、

```
ALTUSER userx SPECIAL
```

以下のようなメッセージが発行されます。

```
C4R480E Special attribute not allowed, command terminated
```

この例で示した固定の C4R480E メッセージの他に、追加の C4R914I メッセージとして、ポリシーに関するサイト固有の情報を示すテキストを定義することもできます。

```
C4R914I SPECIAL Attribute cannot be delegated according to company standard S278-01
```

メッセージ番号は zSecure Command Verifier によって定義されますが、メッセージ・テキストは zSecure Command Verifier 管理者が定義します。この C4R914I メッセージは、標準の zSecure Command Verifier メッセージの前に発行されます。メッセージ・テキストが定義されていない場合は、メッセージ C4R914I は発行されません。

C4R メッセージの他に、SMF レコードが監査の目的で書き込まれます。この SMF レコードには、コマンドの実行が中止された原因となったポリシー・プロファイルが含まれています。RACF も、メッセージ ICH408I として違反の内容を表示します。このメッセージの例は以下のとおりです。

```
ICH408I USER(BCSCADM ) GROUP(BCSC    ) NAME(BCSC ADMINISTRATOR  )
  C4R.USER.ATTR.SPECIAL.USERS.USERX CL(XFACILIT)
  INSUFFICIENT ACCESS AUTHORITY
  FROM C4R.USER.ATTR.SPECIAL.USERS.* (G)
  ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

この例では、SPECIAL 属性の設定を制御したポリシー・プロファイルが総称プロファイルでした。C4R914I メッセージのサイト固有のテキストは、SMF レコードおよび ICH408I メッセージで示されているポリシー・プロファイルで定義できます。この方法を使用することで、組織で使用されるすべてのポリシー・プロファイルに固有のメッセージを指定することができます。

メッセージのテキストは、ポリシー・プロファイルの USRDATA 内に保管されます。zSecure Command Verifier は、複数の USRDATA 項目を使用して、コマンド監査証跡 (CAT) を維持します。サイト・メッセージ・テキストには、$C4RMSGT という USRDATA 項目が使用されます。この USRDATA 項目は、コマンド監査証跡に使用される項目からは独立しており、これらの項目と対話を行いません。USRDATA 項目にサイト・メッセージ・テキストを保管するために現時点で使用できる方法は以下の 2 つです。

- zSecure Admin に用意されている CKGRACF コマンドを使用する。
- ポリシー・プロファイルに対し、インストール・データを表す特定のプレフィックスを使用して RALTER コマンドを使用する。

これら 2 つの方法については、以降のセクションで詳しく説明します。

この USRDATA フィールドの名前は $C4RMSGT です。この名前は $ 記号で始まっています。これは US 国際コード・ページを基盤としています。別のコード・ページを使用している場合は、x'5B' を表す文字を使用する必要があります。

メッセージ・テキストでは変数を使用することができます。これらの変数は、RACF コマンド内で指定されているさまざまなキーワードまたはパラメーターに置き換えられます。ただし、すべてのコマンドですべての変数が指定されているわけではありません。変数に値が存在しない場合は、追加のブランク文字を含まない空ストリングに置き換えられます。以下の変数がサポートされます。

&PROFILE
コマンドで使用されているプロファイルを示します。コマンドで複数のプロファイルが指定されている場合、この変数にはポリシーに違反している単一のプロファイルが格納されます。これはコマンド置換関数で使用される &PROFILE 変数とは異なります。

&CLASS
コマンドに関連する RACF クラス名を示します。DATASET または一般リソースの場合は、プロファイルのリソース・クラスを特定する値が格納されます。ユーザー関連コマンドの場合は値 USER が格納され、グループ関連コマンドの場合は値 GROUP が格納されます。CONNECT コマンドの場合は、値が USER となります。

&USER
コマンドで使用されているユーザー ID を示します。ADDUSER コマンドまたは ALTUSER コマンドで指定されているユーザー ID の場合があります。CONNECT コマンドで指定されているユーザー ID の場合もあります。コマンドが複数のユーザー ID に影響する場合、この変数にはポリシーに違反している単一の ID が格納されます。一部のコマンドでは、&USER の値が &PROFILE の値と同じになります。

&GROUP
コマンドで使用されているグループを示します。ADDGROUP コマンドまたは ALTGROUP コマンドで指定されているグループの場合があります。CONNECT コマンドで指定されているグループの場合もあります。コマンドが複数のグループに影響する場合、この変数にはポリシーに違反している単一のグループが格納されます。一部のコマンドでは、&GROUP の値が &PROFILE の値と同じになります。

&ACLID
PERMIT コマンドで指定されている ID を示します。コマンドが複数の ID に影響する場合、この変数にはポリシーに違反している単一の ID が格納されます。これはコマンド置換関数で使用される &ACLID 変数とは異なります。=STAR という特殊値は、ID(*) にアクセス権限を付与することを表すために使用します。この変数に値が格納されるのは、アクセス関連のポリシー・プロファイルの場合のみです。

&ACLACC
PERMIT コマンドの ACCESS キーワードによって付与されるアクセス・レベルを表します。通常のアクセス・レベルに加えて、ACL 項目が削除されることを表す DELETE があります。 UACC を設定するコマンドの場合、この変数は UACC の値を示します。この変数に値が格納されるのは、アクセス関連のポリシー・プロファイルの場合のみです。

CKGRACF を使用したメッセージ・テキストの設定

サイト・メッセージ・テキストは、CKGRACF コマンドを使用して設定できます。

この必須コマンドの形式は以下のとおりです。

```
CKGRACF USRDATA class profile SET $C4RMSGT(message-text)
```

class
zSecure Command Verifier ポリシー・プロファイルのリソース・クラス。

profile
(総称) ポリシー・プロファイルの名前。

message-text
C4R914I メッセージに使用するテキスト。

message-text 全体を引用符で囲む必要があります。メッセージ・テキストを大/小文字混合で発行するには、引用符に囲まれたストリングの後に小文字の c を付ける必要があります。以下にそのコマンド例を示します。

```
ckgracf usrdata XFACILIT 'C4R.CONNECT.ID.**'c
   set $C4RMSGT('See Corporate Instruction CI278-01'c)
```

ユーザーは CKGRACF コマンドを実行するための十分な権限を保持している必要があります。これには 2 つのタイプの許可が必要です。つまり、CKG.CMD.USRDATA に対する更新権限と、以下のようないずれかの有効範囲プロファイルに対する更新権限を保持している必要があります。

```
CKG.USRDATA.scope-level.XFACILIT.$C4RMSGT
```

scope-level が SCP の場合は、該当するグループ・ツリー・ベースの CKG.SCP.** プロファイルに対する十分なアクセス権限も必要です。CKGRACF コマンドと必要な権限について詳しくは、「*zSecure Admin and Audit for RACF* ユーザー・リファレンス・マニュアル」の『CKGRACF コマンド言語』を参照してください。

CKGRACF コマンドを手動で入力する代わりに、zSecure Admin リソース・プロファイルの概要で MU 行コマンドを使用することもできます。以下のようなパネルが表示されます。

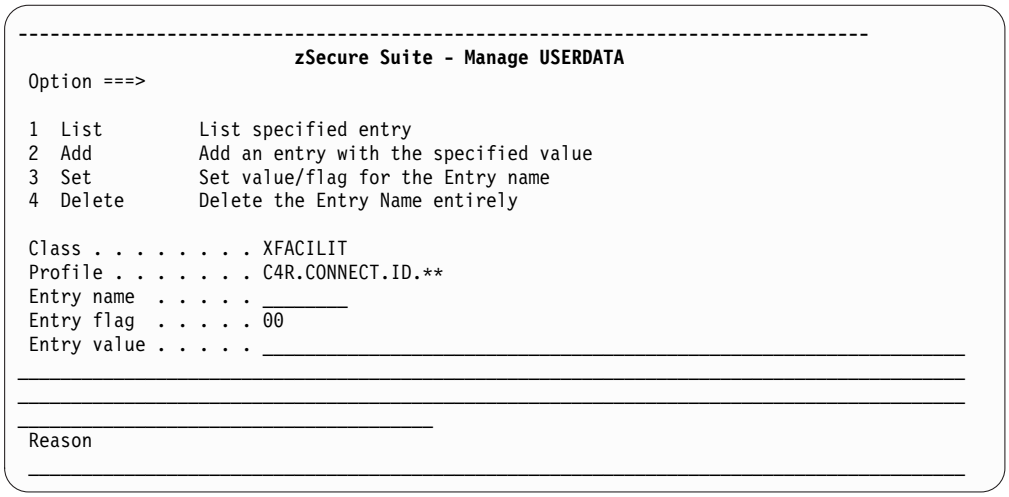


図 *11. Manage USERDATA*

「**Entry name**」には $C4RMSGT と指定し、「**Entry value**」には引用符で囲んだメッセージ・テキストの後に小文字の c を付けたものを指定します。この値を設定するには、オプション **3** (Set) を使用します。サイト・メッセージを削除するには、上記のフィールドに情報を入力して、オプション **4** (Delete) を使用します。このアプリケーションでは、オプション **2** (Add) は使用しないでください。

ポリシー・プロファイルの $C4RMSGT に既に値が設定されている場合は、USRDATA の詳細表示項目で S 行コマンドを使用することもできます。パネルが表示され、現在のメッセージ・テキストを上書きできるようになります。

既存のメッセージを削除するには、ポリシー・プロファイルの詳細表示で D 行コマンドを使用します。

RALTER を使用したメッセージ・テキストの設定

サイトのメッセージ・テキストは、RALTER コマンドを使用して設定できます。

RALTER コマンドを使用する方法の欠点は、RACF がサイト・メッセージ・テキストを大文字に変換してしまうことです。この方法は、zSecure Command Verifier がアクティブである場合にのみ使用できます。リソース・クラスが zSecure Command Verifier ポリシー・プロファイルのリソース・クラスである場合、zSecure Command Verifier はインストール・データに指定されている値を検査します。指定されたインストール・データが $C4RMSGT= で始まる場合は、等号の後のテキストが $C4RMSGT という USRDATA に格納されます。インストール・データの既存の値は変更されません。以下にこのコマンドの例を示します。

```
RALTER XFACILIT C4R.CONNECT.ID.**
   DATA('$C4RMSGT=See Corporate Instruction CI278-01')
```

インストール・データは USRDATA 項目の名前で始まります。現時点で認識される文字ストリングは $C4RMSGT= のみです。先頭文字 ($) は x'5B' を表す文字です。

等号の後の値が DELETE という特殊値である場合は、$C4RMSGT USRDATA フィールドに格納されている既存のサイト・メッセージ・テキストが削除されます。インストール・データ自体は変更されません。

指定されたインストール・データ・フィールドのプレフィックスが $C4RMSGT= と完全一致しない場合は、値が zSecure Command Verifier のサイト・メッセージ・テキストとして認識されません。指定された値全体が、ポリシー・プロファイルのインストール・データ・フィールドに格納されます。

一時システム・レベル属性

zSecure Command Verifier には、特定の RACF コマンドに対するシステム SPECIAL 権限またはシステム AUDITOR 権限を使用するための機能が備わっています。これは、端末ユーザーがこの属性を持っていなくても使用できます。

この機能は、2 つのタイプのポリシー・プロファイルで制御されます。最初のポリシー・プロファイルは、コマンドの存続中に無条件でシステム・レベル属性を付与します。2 番目のポリシー・プロファイルは、RACF コマンド内のすべての関連キーワードがポリシー・プロファイルによって明示的に対象とされている場合にのみ、システム・レベル属性を付与します。明示的に許可されていないキーワードまたはパラメーターが使用されると、コマンドは一時システム・レベル属性なしで実行されます。

無条件一時システム・レベル属性

RACF コマンドに対する無条件一時システム・レベル属性を実装するには、C4R.command.=SPECIAL プロファイルおよび C4R.command.=AUDITOR プロファイルを使用します。

- **C4R.***command*.**=SPECIAL**
- **C4R.***command*.**=AUDITOR**

これらのプロファイルに対する UPDATE アクセス権限を持つユーザーは、コマンドの実行中、および **PRE-** コマンドと **POST-** コマンドが実行される場合に、RACF システム SPECIAL 権限またはシステム AUDITOR 権限を持ちます。ポリシー・プロファイル内の修飾子 =SPECIAL および =AUDITOR を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。以下のアクセス規則が適用されます。

プロファイルが見つからない
: この機能は実装されません。コマンドは、端末ユーザーの通常の権限で実行されます。

NONE
: システム・レベル属性は割り当てられません。コマンドは、端末ユーザーの通常の権限で実行されます。

READ
: NONE と同じ。

UPDATE
: コマンドは、一時システム・レベル属性で実行されます。**PRE-** コマンドと **POST-** コマンドが実行される場合も、この権限で実行されます。

CONTROL
: UPDATE と同じ。

制御対象一時システム・レベル属性

制御対象一時システム・レベル属性と無条件一時システム・レベル属性の違いは、すべてのキーワードおよびパラメーターが、適用可能な zSecure Command Verifier ポリシー・プロファイルに含まれている必要があるかどうかという点です。そのようなプロファイルが 1 つも存在しない場合、制御対象一時属性ポリシーは適用されず、一時**システム** SPECIAL または一時**システム** AUDITOR は付与されません。

制御対象一時属性ポリシーを使用することにより、システム・レベル権限で実行する必要がある機能とそうでない機能を、インストール済み環境でさらに細かく制御できます。ただし、現在、個々のポリシー・プロファイルの定義には二重の効果があるため、制御対象一時属性を有効利用するための正しい制御を設計することはかなり複雑です。つまり、この定義は、キーワードまたはパラメーターを使用する権限があるかどうか、および一時システム・レベル権限を付与する必要があるかどうかを決定します。この二重性に対処する最も簡単な方法は、一時システム・レベル権限に影響せずにどのキーワードおよびパラメーターが存在可能であるかを指定する方法として、ポリシー・プロファイルの定義を扱うことです。例えば、以下の方法を使用して、ポリシーを定義できます。

- 関係のないキーワードおよびパラメーター (ユーザー・プロファイル内の ADSP 属性など) を制御するためにポリシーを定義しないでください。
- 特定のキーワードおよびパラメーター (ユーザー・プロファイルの OWNER など) が使用されないように適切なポリシー・プロファイルを定義してください。
- 選択されたコマンドに対して、制御対象一時 SPECIAL ポリシー・プロファイルまたは制御対象一時 AUDITOR ポリシー・プロファイルを定義してください。

一時属性は、許可されていて、かつポリシー・プロファイルが存在するコマンドに対してのみ適用されるようになりました。このため、ADSP 属性を変更したいが、この属性を設定するためのポリシー・プロファイルがない場合、コマンドは RACF に渡されます。ここで、コマンドを受け入れるか拒否するかを決定できます。ADSP 属性に適用可能なポリシー・プロファイルがないため、コマンドは一時 SPECIAL または一時 AUDITOR では実行されません。ユーザー・プロファイルの OWNER を変更したい場合、zSecure Command Verifier は、OWNER ポリシー・プロファイルに対するアクセス権限を基に、コマンドを受け入れるか拒否するかを決定できます。指定された OWNER 値が許可される場合、ポリシー・プロファイルがあるため、コマンドは一時 SPECIAL または一時 AUDITOR で実行できます。指定された OWNER 値が許可されない場合、コマンドは拒否されます。コマンドが一時権限で実行されるように指定されていたかどうかは問題になりません。

永続 RACF 権限の元のコンテキストだけでなく、一時権限のコンテキストでも、現在許可されているキーワードおよびパラメーターの正確なリストに注目することが、制御対象一時システム・レベル属性ポリシー・プロファイルを使用する際に重要です。

制御対象一時 SPECIAL または制御対象一時 AUDITOR を付与する場合は、プロファイルに対する現在許可されているすべての変更を実際に SPECIAL 権限または AUDITOR 権限で実行する必要があるかどうかを慎重に確認してください。意図し

ない副次作用を回避する上で効果的なのは、ポリシー・プロファイルがない場合に許可される機能と同じ機能を明示的に許可するポリシー・プロファイルを、決して定義しないようにすることです。

以下のポリシー・プロファイルを使用して、制御対象一時システム・レベル属性を実装できます。サポートされるアクセス権限レベルが詳細に説明されています。

- **C4R.***command*.**=CTLSPEC**
- **C4R.***command*.**=CTLAUD**

これらのプロファイルのうちの 1 つに対する UPDATE アクセス権限を持つユーザーは、コマンドの実行中、および **PRE-** コマンドと **POST-** コマンドが実行される場合に、RACF **システム** SPECIAL または**システム** AUDITOR を持ちます。すべてのキーワードおよびパラメーターが zSecure Command Verifier ポリシー・プロファイルによって制御されている場合のみ、ポリシーは適用されます。ポリシー・プロファイル内の修飾子 =CTLSPEC および =CTLAUD を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

コマンド自体がシステム・レベル属性に依存していない場合でも、このポリシーを使用できます。そのような場合、システム・レベル属性は、オプションの PRE- コマンドと POST- コマンドの権限には影響を及ぼすことがあります。これを使用して、例えば、CONNECT コマンドが機密グループに対して発行される場合に、ユーザーの UAUDIT 属性を設定できます。

以下のアクセス規則が適用されます。

プロファイルが見つからない
: この機能は実装されません。コマンドは、端末ユーザーの通常の権限で実行されます。

NONE
: システム・レベル属性は割り当てられません。コマンドは、端末ユーザーの通常の権限で実行されます。

READ
: NONE と同じ。

UPDATE
: コマンドは、一時**システム** SPECIAL 権限または一時**システム** AUDITOR 権限で実行されます。**PRE-** コマンドと **POST-** コマンドが実行される場合も、この権限で実行されます。

CONTROL
: UPDATE と同じ。

制御対象一時システム・レベル属性ポリシー・プロファイルを使用する場合、可能性のあるすべての zSecure Command Verifier ポリシー・プロファイルが定義される必要はありません。必要なのは、特定のキーワードまたはパラメーターを使用する権限を実際に判別するポリシー・プロファイルだけです。例えば、データ・セット MYHLQ.TEST.DSN に対する READ アクセス権限をユーザー USRXYZ に付与する場合、アクセス・リストで GROUP の代わりにユーザー ID を使用できるよう

にするポリシー・プロファイル (ACL./GROUP ポリシー・プロファイル) は必要ありません。この例で必要な制御プロファイルは、次のリソース用のプロファイルだけです。

```
C4R.DATASET.ACL.USRXYZ.READ.MYHLQ.TEST.DSN
```

このリソースは、以下のポリシー・プロファイルで制御できます。

```
C4R.*.ACL.USRXYZ.READ.**
```

以下のリストには、制御対象一時システム・レベル属性を適用するかどうかを判別するために使用されるすべてのポリシー・プロファイルが示されています。このリスト内では、複数の値を持つ可能性のある 1 つ以上の修飾子を示すために、総称が使用されています。

C4R.USER.ID.*	C4R.USER.DELETE.*	C4R.USER.DFLTGRP.*
C4R.USER.OWNER.*	C4R.USER.ATTR.*	C4R.USER.MFA.*
C4R.USER.PASSWORD.*	C4R.USER.PWINT.*	C4R.USER.PWEXP.*
C4R.USER.NAME.*	C4R.USER.INSTDATA.*	C4R.USER.CLAUTH.*
C4R.USER.SECLABEL.*	C4R.USER.SECLEVEL.*	C4R.USER.CATEGORY.*
C4R.USER.MODEL.*	C4R.USER.WHEN.*	C4R.USER.*segment*.*
C4R.USER.*segment*./SCOPE		
C4R.GROUP.ID.*	C4R.GROUP.DELETE.*	C4R.GROUP.SUPGRP.*
C4R.GROUP.OWNER.*	C4R.GROUP.ATTR.*	C4R.GROUP.INSTDATA.*
C4R.GROUP.MODEL.*	C4R.GROUP.*segment*.*	C4R.GROUP.*segment*./SCOPE
C4R.CONNECT.*	C4R.REMOVE.*	C4R.CONNECT.OWNER.*
C4R.CONNECT.AUTH.*	C4R.CONNECT.UACC.*	C4R.CONNECT.ATTR.*
C4R.*class*.ID.*	C4R.*class*.OWNER.*	C4R.*class*.UACC.*
C4R.*class*.ACL.*	C4R.*class*.CONDACL.*	C4R.*class*.VOLUME.*
C4R.*class*.UNIT.*	C4R.*class*.RACFIND.*	C4R.*class*.TYPE.*
C4R.*class*.ATTR.*	C4R.*class*.INSTDATA.*	C4R.*class*.NOTIFY.*
C4R.*class*.APPLDATA.*	C4R.*class*.SECLABEL.*	C4R.*class*.CATEGORY.*
C4R.*class*.SECLEVEL.*	C4R.*class*.LEVEL.*	C4R.*class*.RETPD.*
C4R.*class*.*segment*.*	C4R.*class*.*segment*./SCOPE	

図 *12.* 制御対象一時システム・レベル属性を割り当てることができるかどうかを判別するために使用されるポリシー・プロファイル

多要素認証 (MFA) データを管理するためのプロファイル

RACF は、RACF と SAF の両方に対する新機能 APAR によって多要素認証のサポートを実装しました。必要なデータは、USER プロファイルと、MFADEF リソース・クラスの一般リソース・プロファイルに追加できます。

USER プロファイルでは、関連するデータは BASE セグメント内の複数の MFA 関連フィールドに保持されます。技術的には、USER プロファイル内の MFA データは個別のセグメント内に保持されませんが、zSecure Command Verifier は独立したセグメントが使用されているかのように情報を扱います。これは、USER MFA データに対して、セグメントの既存のポリシー・プロファイルに類似するポリシー・プロファイルが使用されるということを意味します。そのため、USER プロファイル内の MFA データは、以下の 2 つのタイプのポリシー・プロファイルの対象とされます。

- セグメント管理ポリシー・プロファイル （ 64 ページの『非基本セグメントの管理を制御するプロファイル』を参照)

- MFA 関連フィールド (130 ページの『USER MFA データ管理用のポリシー・プロファイル』を参照)

MFADEF 一般リソース・クラス内にあるプロファイルの MFA 情報は、MFA セグメントおよび MFPOLICY セグメント内に保持されます。MFA セグメントに対して RACF が提供する機能は、そのセグメントの追加または削除のみです。この MFA セグメントの内容は、RACF コマンドを使用して管理することはできません。したがって、Command Verifier で提供されるポリシーは、MFA セグメントの存在を管理するためのポリシーのみです。一方、MFPOLICY セグメントの内容は、RACF を使用して管理されます。Command Verifier は、MFPOLICY セグメントの存在の管理と、キーワードおよびパラメーターの設定を制御するためのポリシー・プロファイルを提供します。詳しくは、『非基本セグメントの管理を制御するプロファイル』および 237 ページの『MFPOLICY セグメント管理用のポリシー・プロファイル』を参照してください。

非基本セグメントの管理を制御するプロファイル

RACF では、すべてのシステム SPECIAL ユーザーおよび FIELD クラス内のプロファイルへの十分なアクセス権限を持つすべてのユーザーが、OMVS セグメントや TSO セグメントなどの非基本セグメント内の情報を管理することができます。後者の方法は、フィールド・レベル・アクセス検査 と呼ばれることがよくあります。

場合によっては、これらのタイプのセグメントの管理をさらに制限する方が好ましい場合があります。 USER プロファイル内の MFA データは、技術的には個別のセグメント内にありませんが、zSecure Command Verifier は情報がセグメント内に格納されているかのように扱います。このセクションの残りの部分では、変数セグメントは USER プロファイル内の MFA データにも該当します。非基本セグメントの制御を可能にするために、zSecure Command Verifier は以下の 3 つのタイプのプロファイルを実装しています。

- **C4R.***class.segment*.**=RACUID**

  このポリシー・プロファイルは、自分のセグメント情報を管理するための権限を制御するために使用されます。このポリシー・プロファイルの効果は、FIELD クラス内の対応するプロファイルのアクセス・リスト上に &RACUID を配置することに類似しています。

- **C4R.***class.segment*

  このポリシー・プロファイルは、自分以外のユーザーのプロファイルのセグメント情報を管理するための権限を制御するために使用されます。

- **C4R.***class.segment*.**/SCOPE**

  このポリシー・プロファイルを使用して、セグメント情報の管理を行うための権限範囲を制御できます。

非基本セグメントを管理する端末ユーザーの権限を決定するために、最初のプロファイルまたは 2 番目のプロファイルのいずれかが使用されます。 システム SPECIAL を持たないユーザーの場合、3 番目のプロファイルも使用され、制御範囲が狭められます。端末ユーザーが自分の TSO 情報を表示できる必要がある場合は、以下の 2 つのプロファイルを設定する必要があります。

```
XFACILIT     C4R.USER.TSO.=RACUID           userid(READ)
FIELD        USER.TSO.**                    &racuid(READ);
```

同じ端末ユーザーが他のユーザーの TSO 情報を表示できるようにするには、以下の 2 つのプロファイルを設定する必要があります。

```
XFACILIT     C4R.USER.TSO                   userid(READ)
FIELD        USER.TSO.**                    userid(READ)
```

これらのシナリオでは、zSecure Command Verifier とフィールド・プロファイルの両方を設定する必要があります。以下の例のように、組み合わせて実装することもできます。

```
XFACILIT     C4R.USER.TSO.=RACUID           uacc(NONE) userid(READ)
XFACILIT     C4R.USER.TSO                   uacc(NONE)
FIELD        USER.TSO.**                    uacc(READ)
```

この場合、端末ユーザーは、最初の zSecure Command Verifier プロファイルに従って、ユーザー自身のユーザー・プロファイルの TSO セグメントを管理することができます。このコマンドは、フィールド・プロファイルによっても許可されます。このフィールド・プロファイルによって、その他のすべてのユーザーの TSO セグメントを表示することもできます。ただし、表示されている 2 番目の zSecure Command Verifier ポリシー・プロファイルによってこれは回避されます。

重要**:** 非基本セグメント内の特定のフィールド値割り当てを制限する方法に関する重要な情報については、 261 ページの『USS セグメント管理用のポリシー・プロファイル』を参照してください。適切なプロファイルが設定されていない場合、フィールド・レベルのアクセス権限を使用して UPDATE アクセス権限を付与すると、望ましくない影響が生じる可能性があります。

次のセクションでは、プロファイルとアクセス・レベルについて詳しく説明します。

- **C4R.***class.segment***.=RACUID**

  このプロファイルは、端末ユーザーが自分のユーザー・プロファイル内の *segment* の表示または変更を試行する際に使用されます。 =RACUID 修飾子は端末ユーザー自体を指すため、ポリシー・プロファイルは USER *class* に対してのみ適用できます。プロファイルが存在しない場合、またはプロファイルへのアクセスが許可されていない場合は、次の項目で説明する、すべてのユーザー用の一般プロファイル (**C4R.***class.segment*) を使用して、許可検査が続行されます。総称文字を使用して、ポリシー・プロファイル内の =RACUID 修飾子を表すことはできません。ここに示されているとおりの形式で存在している必要があります。

  セグメント名の総称値を定義する際には注意してください。結果として得られたポリシー・プロファイルは、自分のパスワードまたはパスフレーズを変更する権限にも一致する可能性があるためです。パスワードおよびパスフレーズ用のポリシー・プロファイルについて詳しくは、 121 ページの『ユーザー・パスワードおよびパスフレーズ管理用のポリシー・プロファイル』を参照してください。

  以下のアクセス規則が適用されます。

  プロファイルが見つからない
  : この制御は実装されません。zSecure Command Verifier は、*segment* に

対するアクセス権限を制御しません。RACF は、フィールド・クラスの定義に従って *segment* に対するアクセス権限を制御します。

NONE
端末ユーザーは、自分のユーザー ID の *segment* 情報にアクセスできません。ただし、この制限は一般セグメントのアクセス・ポリシー・プロファイルによって解除することができます。この制限は、フィールド・クラスのプロファイル定義による影響を受けません。

READ
端末ユーザーは、ユーザーの *segment* 情報を表示できます。この機能は、フィールド・クラスに定義されたプロファイルに対する適切なアクセス権限によっても影響を受けます。

UPDATE
端末ユーザーは、ユーザーの *segment* 情報を更新できます。この機能は、フィールド・クラスに定義されたプロファイルに対する適切なアクセス権限によっても影響を受けます。

CONTROL
UPDATE と同じ。

- **C4R.***class.segment*

このプロファイルは、端末ユーザーがいずれかのユーザー・プロファイル内の *segment* 情報の表示または変更を試行する際に使用されます。このプロファイルは、端末ユーザーがユーザー ID の *segment* にアクセスを試みたものの、前述のプロファイルによって許可されなかった場合にも使用されます。以下のアクセス規則が適用されます。

プロファイルが見つからない
この制御は実装されません。zSecure Command Verifier は、*segment* に対するアクセス権限を制御しません。RACF は、フィールド・クラスの定義に従って *segment* に対するアクセス権限を制御します。

NONE
端末ユーザーは、ターゲット・ユーザー ID の *segment* 情報にアクセスできません。この制限は、フィールド・クラスのプロファイル定義による影響を受けません。

READ
端末ユーザーは、*segment* 情報を表示できます。この機能は、フィールド・クラスに定義されたプロファイルに対する適切なアクセス権限によっても影響を受けます。ターゲット・ユーザー ID が端末ユーザーの**グループ** SPECIAL の範囲外である場合、または端末ユーザーが**グループ** SPECIAL 属性を持たない場合は、次のセクションで説明する /SCOPE ポリシー・プロファイルが適用されます。

UPDATE
端末ユーザーは、*segment* 情報を更新できます。この機能は、フィールド・クラスに定義されたプロファイルに対する適切なアクセス権限によっても影響を受けます。ターゲット・ユーザー ID が端末ユーザーの**グループ** SPECIAL の範囲外である場合、または端末ユーザーが**グループ**

SPECIAL 属性を持たない場合は、次のセクションで説明する /SCOPE ポリシー・プロファイルが適用されます。

CONTROL
UPDATE と同じ。

現在、前述のプロファイル内の修飾子 *segment* に対して、以下の値がサポートされています。

USER CICS、DFP、LANGUAGE、NETVIEV、OMVS、OPERPARM、TSO、WORKATTR、OVM、DCE、NDS、LNOTES、KERB、PROXY、EIM、CSDATA、MFA

GROUP
DFP、OMVS、OVM、TME、CSDATA

DATASET
DFP、TME

一般リソース
SESSION、DLFDATA、SSIGNON、STDATA、SVFMR、TME、KERB、PROXY、EIM、CDTINFO、ICTX、CFDEF、ICSF、SIGVER、MFA

セグメントを管理するための範囲設定規則

RACF では、フィールド・クラスのプロファイルに対するアクセス権限が、すべてのプロファイルの非基本セグメントのフィールドに対するアクセス権限を制御します。分散管理者が、例えば、その管理者のグループ SPECIAL 適用範囲内に入るユーザーのみの TSO セグメントを管理できるようにすることはできません。

z/OS 2.3.0 以降、RACF では、非基本セグメントに対するアクセス権限を付与する前に、基本セグメントに対する端末ユーザーの権限の検査を追加するためのメソッドが提供されています。存在および FIELD クラスのプロファイル FLAC.SKIP.BASECHECK へのアクセス権限によって、基本セグメントへのアクセス権限が使用されているかどうかが判別されます。この権限はすべての非基本セグメントに適用され、セグメント・タイプによる細分性はありません。このセクションで説明する zSecure Command Verifier の範囲設定ポリシーでは、セグメント・タイプに基づくセグメント範囲設定が提供されます。また、zSecure Command Verifier の範囲設定ポリシーはシステム SPECIAL 属性およびグループ SPECIAL 属性に基づいており、ターゲット・プロファイルの直接所有権は無視されます。

zSecure Command Verifier には、非基本セグメントに対して、通常の RACF (つまり BASE) セグメントに使用されるのと同じ範囲規則を強制できる機能が備わっています。/SCOPE プロファイルを使用して、それらのユーザーを、BASE セグメントの適用範囲内にあるプロファイルのみに制限することができます。

zSecure Command Verifier は RACF アクセス制御を非基本セグメント情報に置き換えません。分散管理者がフィールド・レベル・アクセス検査によるアクセス権限を持っていない場合、その管理者は非基本セグメントの表示または変更を行うこともできません。セグメント管理の範囲設定 の完全実装環境では、自分のプロファイルの非基本セグメントを保守する必要のあるすべての分散管理者が、対応するフィールド・プロファイルに対するアクセス権限を持っていなければなりません。

技術的には、USER プロファイル内の MFA データは個別のセグメント内には保持されませんが、zSecure Command Verifier は USER プロファイル内の MFA データがセグメント内に格納されているかのように扱います。このセクションで説明されている /SCOPE ポリシー・プロファイルは、USER プロファイル内の MFA データの管理をグループ SPECIAL またはシステム SPECIAL のユーザーに制限するために使用できます。FIELD クラス内のプロファイルへのアクセス権限は必要ありません。

zSecure Command Verifier は、この範囲設定規則で、ターゲット・プロファイルの直接的な所有権を考慮しません。制御範囲を決定するために使用されるのは、グループ SPECIAL のみです。

システム SPECIAL 権限を持つ端末ユーザーは、システム内のすべてのプロファイルがそれらの適用範囲内にあると見なされるため、この制御の対象外とされます。

グループ SPECIAL またはシステム SPECIAL の端末ユーザーが、ターゲット・プロファイルの基本セグメントに対して自己の管理権限を使用すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

- **C4R.USESCOPE.***group*

このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、コマンドのターゲット・プロファイルの基本セグメントに対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

重要**:** 非基本セグメント内の特定のフィールド値割り当てを制限する方法に関する重要な情報については、 261 ページの『USS セグメント管理用のポリシー・プロファイル』を参照してください。適切なプロファイルがない場合、セグメント管理範囲設定の活動化を行ったり、フィールド・レベルのアクセス権限を使用して分散管理者に UPDATE アクセス権限を付与したりすると、望ましくない影響が生じる可能性があります。

- **C4R.***class.segment***./SCOPE**

  ポリシー・プロファイル内の修飾子 /SCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。以下のアクセス規則が適用されます。

  プロファイルが見つからない
  : この制御は実装されません。標準 RACF 規則が適用されます。すべてのプロファイルの非基本セグメントには、フィールド・クラスの定義に従ってアクセスすることができます。

  NONE
  : 端末ユーザーは、標準の RACF 適用範囲外にあるいずれの非基本セグメントにもアクセスできません。適用範囲内のプロファイルの場合、それぞれのフィールド・クラス・プロファイルに対するアクセス・レベルによって、フィールドを表示または変更できるかどうかが制御されます。

  READ
  : 端末ユーザーは、システム内のすべてのプロファイルにある、許可され

ている非基本セグメントを表示できます。適用範囲外のプロファイルの場合、リスト・コマンドのみが許可されます。適用範囲内のプロファイルについては、すべてのコマンドが許可されます。それぞれのフィールド・クラス・プロファイルに対するアクセス・レベルによって、フィールドを表示または変更できるかどうかが制御されます。

UPDATE
端末ユーザーは、システム内のすべてのプロファイルにある、許可されている非基本セグメントを変更できます。ただし、フィールド・クラス内のプロファイルによって、特定の端末ユーザーが表示または変更の目的でフィールドにアクセスできるかどうかが制御されます。

CONTROL
UPDATE と同じ。

RACF コマンドの置き換え

zSecure Command Verifier では、追加/置換を組み合わせた方法を使用して、コマンドを他のコマンドに置き換えることができます。

最初のステップで、プリコマンドまたはポストコマンドを指定します。 2 番目のステップでは、元のコマンドを (場合によってはいくつかのキーワードを取り除いて) 実行する必要があるかどうかを指定します。これは、3 つのプロファイルで制御できます。プリコマンドおよびポストコマンドでは、元の RACF コマンドのいくつかのフィールドを変数によって参照することができます。例えば、ターゲット・クラスおよびプロファイルは、`&CLASS` および `&PROFILE` によって指定できます。

指定されたプリコマンドとポストコマンドは、元の RACF コマンドと同じ権限で実行されます。一時 SPECIAL 権限または一時 AUDITOR 権限が元の RACF コマンドで指定されていた場合は、プリコマンドとポストコマンドも一時 SPECIAL または一時 AUDITOR で実行されます。これは、制御対象一時属性にも適用されます。実行される環境にとって適切なプリコマンドとポストコマンドを指定することは、Command Verifier ポリシー管理者の責任です。

注**:** 現在、この機能は以下のコマンドおよびキーワードに対してのみ使用できます。

表 *8.* コマンド/キーワード置き換え機能によってサポートされているコマンドおよびキーワード

コマンド	キーワード	**keyword-qualification**
ALTUSER	RESUME	RESUME
ALTUSER	REVOKE	REVOKE
ALTUSER	RESUME(date) NORESUME	RESUMEDT
ALTUSER	REVOKE(date) NOREVOKE	REVOKEDT
ADDUSER **ALTUSER**	SPECIAL	SPECIAL
ADDUSER **ALTUSER**	OPERATIONS	OPERATIONS

表 8. コマンド/キーワード置き換え機能によってサポートされているコマンドおよびキーワード (続き)

コマンド	キーワード	**keyword-qualification**
ADDUSER **ALTUSER**	AUDITOR	AUDITOR
ADDUSER **ALTUSER**	*segment* **no***segment*	*segment.action* *action*={Add | Alt | Del}
CONNECT	GROUP(grpname)	GROUP.*grpname*
PERMIT	CLASS(*class*)	CLASS.*class*
REMOVE	GROUP(grpname)	GROUP.*grpname*

コマンド置き換えポリシー・プロファイルの一般形式は、以下のとおりです。

```
C4R.command.function.keyword-qualification
```

command は、端末ユーザーによって発行された、省略されていない RACF コマンドです。*function* は、このポリシー・プロファイルによって制御されるコマンド置き換え機能の部分を示します。*function* に指定できる値は、**=PRECMD**、**=PSTCMD**、および **=REPLACE** です。これらは、PRE- コマンドと POST- コマンドを指定し、元の RACF コマンドを発行するかどうか、およびその発行方法を示すために使用されます。

keyword-qualifier に指定できる値は、コマンドによって異なります。

- **ADDUSER** コマンドまたは **ALTUSER** コマンドを使用して属性を設定する場合、*keyword-qualifier* には 1 つの修飾子のみが含まれます。例えば、REVOKE、RESUME、および SPECIAL 修飾子です。
- ユーザー・セグメントを管理する場合、*keyword-qualifier* には 2 つの修飾子が含まれます。最初の修飾子はセグメントの名前であり、2 番目の修飾子はアクション修飾子です。アクション修飾子には、ADD、ALT、または DEL を指定できます。
- **CONNECT** コマンドまたは **REMOVE** コマンドを使用してユーザーからグループへの接続を管理する場合、*keyword-qualifier* には、固定値 GROUP に続いて、コマンド内で使用されるグループの名前が含まれます。
- **PERMIT** コマンドを使用してアクセス・リストを変更する場合、*keyword-qualifier* には 2 つの修飾子が含まれます。最初の修飾子は固定値 CLASS であり、2 番目の修飾子はリソース・クラス名です。

特殊修飾子 =PRECMD、=PSTCMD、または =REPLACE は、ポリシー・プロファイルに明示的にコード化される必要があります。これは、総称文字によって一致させることはできません。これらのポリシー・プロファイルのその他の修飾子 (コマンドやリソース・クラスなど) は、総称文字で記述できます。

サンプルのポリシー・プロファイルを以下に示します。

```
C4R.*.=PRECMD.SPECIAL
C4R.ALTUSER.=PRECMD.REVOKE
C4R.ALTUSER.=PSTCMD.TSO.ADD
C4R.A*.=PRECMD.*.A*
C4R.PERMIT.=PSTCMD.CLASS.DATASET
```

プロファイルおよびサポートされるアクセス・レベルについて詳しくは、以下のリストを参照してください。

- **C4R.***command***.=PRECMD.***keyword-qualification*

  このプロファイルは、元の RACF コマンドの前に実行する必要があるコマンドを指定します。プリコマンドは、プロファイルの APPLDATA によって指定されます。このプロファイルは、**ALTUSER RESUME** コマンドを **CKGRACF RESUME** コマンドによって置き換える際に最も頻繁に使用されます。

  複数のキーワードが **=PRECMD** プロファイルと一致する場合は、プリコマンドを指定するためにどのプロファイルも使用できます。 zSecure Command Verifier によって使用されるプロファイルは予測不能です。

  ポリシー・プロファイル内の修飾子 =PRECMD を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  実行中にプリコマンドが失敗すると、元のまたは変更された RACF コマンドは抑止されます。このように、変更された RACF コマンド内の従属アクションは、プリコマンドで実行される前提条件のアクションが完了した場合にのみ実行されます。

  以下のアクセス規則が適用されます。

  プロファイルが見つからない
  : この制御は実装されません。プリコマンドは発行されません。

  NONE
  : このプロファイルに指定されたプリコマンドは、この端末ユーザーに対して実行されません。

  READ
  : APPLDATA によって定義されているプリコマンドは、元の RACF コマンドの前に実行されます。

  UPDATE
  : READ と同じ。

  CONTROL
  : UPDATE と同じ。

- **C4R.***command***.=REPLACE.***keyword-qualification*

  このプロファイルは、元のキーワードを保持するか抑止するか、あるいは RACF コマンド全体を抑止する必要があるかどうかを指定します。プリコマンドが失敗すると、元の RACF コマンドは実行されません。これは、=REPLACE プロファイルの定義による影響を受けません。

  keyword がコマンド内にある場合、アクションは、以下のリストに指定したアクセス規則によって制御されます。複数のキーワードが **=REPLACE** プロファイルと一致する場合は、キーワードまたはコマンド全体を抑止するために、これらのプロファイルのすべてを使用できます。

  CONNECT コマンドおよび **REMOVE** コマンドの場合は、グループのキーワード修飾のみがサポートされます。GROUP キーワードの抑止は無効です。これは、GROUP

キーワードがないと、RACF は自動的に端末ユーザーの現行接続グループをコマンドで使用するためです。その結果、コマンドによって、意図したとおりの効果が得られなくなります。このため、**CONNECT** コマンドおよび **REMOVE** コマンドは、抑止をサポートしていません。

ポリシー・プロファイル内の修飾子 =REPLACE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

以下のアクセス規則が適用されます。

プロファイルが見つからない
: この制御は実装されません。キーワードは削除されません。

NONE
: この端末ユーザーに対して、キーワードの抑止は実行されません。

READ
: キーワードは抑止されます。この抑止により、コマンド内に有効なキーワードは設定されなくなります。 **CONNECT** コマンドおよび **REMOVE** コマンドの場合、READ の効果は NONE と同じです。キーワードは抑止されません。

UPDATE
: コマンド全体が抑止されます。この抑止により、端末ユーザーにエラー・フラグを表示し、コマンドが失敗したことを示すことができます。

CONTROL
: UPDATE と同じ。

- **C4R.***command***.=PSTCMD.***keyword-qualification*

  このプロファイルは、元の RACF コマンドの後に実行する必要があるコマンドを指定します。ポストコマンドは、プロファイルの APPLDATA によって指定されます。コマンド内に、ターゲット・クラスおよびプロファイルを &CLASS および &PROFILE によって指定できます。

  複数のキーワードが **=PSTCMD** プロファイルと一致する場合は、ポストコマンドを指定するために、どのプロファイルも使用できます。 zSecure Command Verifier によって使用されるプロファイルは予測不能です。

  ポリシー・プロファイル内の修飾子 =PSTCMD を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  以下のアクセス規則が適用されます。

  プロファイルが見つからない
  : この制御は実装されません。ポストコマンドは発行されません。

  NONE
  : このプロファイルに指定されたポストコマンドは、この端末ユーザーに対して実行されません。

  READ
  : APPLDATA によって定義されているポストコマンドは、元の RACF コマンドの後に実行されます。元の RACF コマンドによって警告メッセージが出される場合、ポストコマンドは抑止されます。このアクセス・レベ

ルは、コマンドが完全に失敗した場合でも警告メッセージしか出さない一部の RACF コマンド (**ALTUSER** や **ALTGROUP** など) に使用すると便利です。

UPDATE
APPLDATA によって定義されているポストコマンドは、元の RACF コマンドの後に実行されます。元の RACF コマンドがエラー・メッセージを出して失敗するか、異常終了すると、ポストコマンドは抑止されます。

CONTROL
UPDATE と同じ。

=PRECMD プロファイルおよび =PSTCMD プロファイルの APPLDATA を使用して、元の RACF コマンドの前および後に実行するコマンドを指定できます。RACF が **APPLDATA** フィールドを処理する方法に準拠して、入力された値は大文字に変換されます。指定したコマンド・ストリング内では、変数を使用して元の RACF コマンドの一部を参照することができます。変数には接頭部としてアンパーサンド記号 (&) が付けられます。以下の変数がサポートされます。

&CLASS
PROFILE の CLASS を表します。**ALTUSER** コマンドの場合、この値は USER になります。**PERMIT** コマンドの場合、この値はデータ・セット、または指定した一般リソース・クラスになります。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER,C4RTEST) ACCESS(READ)
&CLASS ---> FACILITY

ALTUSER IBMUSER REVOKE
&CLASS ---> USER
```

&PROFILE
PROFILE を表します。**ALTUSER** コマンドの場合、これは添付された user ID になります。**PERMIT** コマンドの場合、これは完全修飾データ・セット名、または一般リソース・プロファイル名になります。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER,C4RTEST) ACCESS(READ)
&PROFILE ---> STGADMIN.**

ALTUSER IBMUSER REVOKE
&PROFILE ---> IBMUSER
```

&PROFILE(1)
1 つの PROFILE を表します。**ALTUSER** コマンドの場合、これは添付された複数の user ID の 1 つになります。**PERMIT** コマンドの場合、これは完全修飾データ・セット名、または一般リソース・プロファイル名の 1 つになります。どのプロファイルが使用されるかは予測不能です。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER,C4RTEST) ACCESS(READ)
&PROFILE(1) ---> STGADMIN.**

ALTUSER (IBMUSER) REVOKE
&PROFILE(1) ---> IBMUSER

ALTUSER (IBMUSER, C4RTEST) REVOKE
&PROFILE(1) ---> C4RTEST (maybe)
```

&SEGMENT
このコマンドで管理されている USER SEGMENT のリストを表します。

```
ALTUSER IBMUSER TSO OMVS(UID(0))
&SEGMENT ---> TSO OMVS
```

&SEGMENT(1)

このコマンドで管理されている USER SEGMENT の 1 つを表します。どの SEGMENT が使用されるかは予測不能です。

```
ALTUSER IBMUSER TSO OMVS(UID(0))
&SEGMENT(1) ---> OMVS (maybe)
```

&RACUID

コマンドを発行する端末ユーザーのユーザー ID を表します。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER,C4RTEST) ACCESS(READ)
&RACUID ---> CRMAHJB (maybe)

ALTUSER IBMUSER REVOKE
&RACUID ---> CRMAHJB (maybe)
```

&RACGPID

コマンドを発行する端末ユーザーの現行接続 GROUP を表します。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER,C4RTEST) ACCESS(READ)
&RACGPID ---> CRMA (maybe)

ALTUSER IBMUSER REVOKE
&RACGPID ---> CRMA (maybe)
```

&DATE

現在日付をユリウス形式 (YY.DDD) で表します。ユリウス日付は、LISTUSER 出力で RACF によって使用される形式と同じです。

```
ALTUSER IBMUSER REVOKE
&DATE ---> 04.060 (maybe)
```

&TIME

現在時刻を 24 時間形式 (HH:MM:SS) で表します。この時刻形式は、LISTUSER 出力で RACF によって使用される形式と同じです。

```
ALTUSER IBMUSER REVOKE
&TIME ---> 08:17:31 (maybe)
```

&SYSID

現行システムの SMF システム ID を表します。この変数は、Parmlib の SMFPARMxx によって指定される 4 文字のストリングです。これは、PROGRAM プロファイルの条件付きアクセス・リスト内に使用できる値と同じです。

```
ALTUSER IBMUSER REVOKE
&SYSID ---> IDFX (maybe)
```

&ACLID

PERMIT コマンドの ID キーワードに指定されている ID (ユーザーと GROUP の両方) のリストを表します。このリストは、単一の値で構成することも、ブランクで分離されたリストで構成することもできます。先行ブランクおよび末尾ブランクは含まれません。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER,C4RTEST) ACCESS(READ)
&ACLID ---> IBMUSER C4RTEST
```

&ACLID(1)

PERMIT コマンドの ID キーワードに指定されている ID (ユーザーと GROUP の両方) の 1 つを表します。どの ID が使用されるかは予測不能です。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER,C4RTEST) ACCESS(READ)
&ACLID(1); ---> C4RTEST (maybe)
```

&ACLACC

PERMIT コマンドの ACCESS キーワードによって付与されるアクセス・レベルを表します。通常のアクセス・レベルに加えて、ACL 項目が削除されることを表す DELETE があります。

ACCESS レベルのサブストリングを使用して置き換えることもできます。この置き換えは、ストリング &ACLACC のすぐ後にスペースを空けずに括弧内に 1 桁の数字を入れて指定することができます。1 から 8 までの 1 桁の数字しか使用できません。また、サブストリング全体を正確に 3 文字で構成して指定する必要があります。これ以外の形式は、通常の文字ストリングと見なされます。

```
PERMIT STGADMIN.** CLASS(FACILITY) ID(IBMUSER C4RTEST) ACCESS(UPDATE)
&ACLACC    ---> UPDATE
&ACLACC(3); ---> UPD
```

例 1

この例では、2 つのプロファイルによって、**ALTUSER RESUME** コマンドを zSecure Admin の Resume 機能で置き換えます。

```
XFACILIT:   C4R.ALTUSER.=PRECMD.RESUME
  UACC:     UPDATE
  APPLDATA: 'CKGRACF &class &profile RESUME'

XFACILIT:   C4R.ALTUSER.=REPLACE.RESUME
  UACC:     READ
```

2 つのプロファイルを使用すると、以下の置き換えが行われます。

```
Input:   ALTUSER userid PASSWORD(password) RESUME
Precmd:  CKGRACF USER userid RESUME
Maincmd: ALTUSER userid PASSWORD(password)
```

注: この置き換えを使用する場合は、CKGRACF (SYSTERM) に必要なファイルが使用可能であることを確認してください。

例 2

REVOKE キーワードに対して行える、コマンド置き換えの例がもう 1 つあります。このキーワードは、**CKGRACF DISABLE** で置き換えることができます。この **DISABLE** は、**CKGRACF ENABLE** コマンドでしか取り消せません。

RESUME 機能が **CKGRACF RESUME** に変換されると、**DISABLE** スケジュールにより、ほとんどの場合、再開を試行しても失敗します。REVOKE は、以下のようにプロファイルを定義することで変換できます。

```
XFACILIT:   C4R.ALTUSER.=PRECMD.REVOKE
  UACC:     UPDATE
  APPLDATA: 'CKGRACF &class &profile SCHEDULE GRPADMIN DISABLE TODAY'

XFACILIT:   C4R.ALTUSER.=REPLACE.REVOKE
  UACC:     UPDATE
```

2 つのプロファイルを使用すると、以下の置き換えが行われます。

```
Input:   ALTUSER userid REVOKE
Precmd:  CKGRACF USER userid SCHEDULE GRPADMIN DISABLE TODAY
Maincmd: none
```

CKGRACF コマンドの詳細な説明、および取り消し/再開スケジュールの管理に必要な権限について詳しくは、「*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。

例 3

この例では、**REVOKE** が **CKGRACF DISABLE** で変換されるときに、プリコマンドを使用して **ALTUSER RESUME** のユーザーを **ENABLE** に設定します。

REVOKE が変換されるシナリオ (75 ページの『例 2』 で説明) では、**ALTUSER RESUME** のユーザーを自動的に **ENABLE** に設定することができます。この場合、プリコマンドを使用してユーザーを **ENABLE** に設定することをお勧めします。**CKGRACF ENABLE** コマンドが発行されると、**CKGRACF** は、他のスケジュールによってユーザーが再開できなくなっているのかどうかを判別します。そうではない場合は、**CKGRACF** は自動的にユーザーを **ENABLE** に設定されている日付 (=today) で再開します。**RESUME** は、以下のようにプロファイルを定義することで変換できます。

```
XFACILIT:   C4R.ALTUSER.=PRECMD.RESUME
  UACC:     UPDATE
  APPLDATA: 'CKGRACF &class &profile SCHEDULE GRPADMIN ENABLE TODAY'

XFACILIT:   C4R.ALTUSER.=REPLACE.RESUME
  UACC:     READ
```

2 つのプロファイルを使用すると、以下の置き換えが行われます。

```
Input:   ALTUSER userid PASSWORD(password) RESUME
Precmd:  CKGRACF USER userid SCHEDULE GRPADMIN ENABLE TODAY
Maincmd: ALTUSER userid PASSWORD(password)
```

CKGRACF コマンドの詳細な説明、および取り消し/再開スケジュールの管理に必要な権限について詳しくは、「*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。

例 4

この例では、複数の **PERMIT** コマンドが **CONNECT** によって適切なグループに置き換えられます。

グループの名前は、アクセス・レベルから派生されます。現在の実装環境では、ACCESS の切り捨てのみ行えます。指定した **ACCESS** が DELETE である場合、REMOVE コマンドを作成するためのプロビジョンは行われません。

```
XFACILIT:   C4R.PERMIT.=PRECMD.CLASS.SDSF
  UACC:     UPDATE
  APPLDATA: 'CONNECT &ACLID GROUP(SDSF#ACLACC(1))'

XFACILIT:   C4R.PERMIT.=REPLACE.CLASS.SDSF
  UACC:     UPDATE
```

プロファイルを使用すると、以下の置き換えが行われます。

```
Input:   PERMIT profile CLASS(SDSF) ID(IBMUSER) ACCESS(READ)
Precmd:  CONNECT IBMUSER GROUP(SDSF#R)
Maincmd: none
```

グループ Special 権限の制約事項

以下のガイドラインでは、zSecure Command Verifier のポリシー・プロファイルの範囲について説明します。

このバージョンの zSecure Command Verifier では、コマンド権限に関するシステム全体およびグループ関連の SPECIAL 属性のみが認識されます。それ以外のコマンド権限方式は、zSecure Command Verifier ではすべて無視されます。例えば、グループ操作、グループ接続権限 (JOIN、CONNECT、CREATE)、および直接所有権 (影響を受ける RACF プロファイルの所有者が端末ユーザーである場合) などは無視されます。**RDEFINE** コマンドと **ADDUSER** コマンドについては、指定されたポリシーにコマンドが他の点では準拠していれば、zSecure Command Verifier は **CLAUTH** 属性を認識します。

必須値およびデフォルト値ポリシー・プロファイル

zSecure Command Verifier では、キーワードに対して特定の値を強制するプロファイルを使用することができます。この値は、端末ユーザーによって指定された値よりも優先されます。

これらのプロファイルは、必須値 ポリシー・プロファイルと呼ばれています。これらは、RACF コマンドがキーワードを必要とする場合、またはデフォルト値を使用する場合にのみ使用できます。つまりこの制限により、大部分のキーワードに関して、必須値ポリシー・プロファイルは作成または追加のコマンド・タイプ (例えば、**ADDUSER**) に対してしか使用できません。これらにはすべて = で始まる 3 番目の修飾子があります (例えば、=DFLTGRP)。必須値ポリシー・プロファイルの例を以下に示します。

- **C4R.DATASET.=UACC.SYS1.LINKLIB**

  このプロファイルは、SYS1.LINKLIB データ・セットの UACC に必須値を指定します。UACC の値は、ポリシー・プロファイルの **APPLDATA** フィールドに指定されます。

- **C4R.USER.=OWNER.IBM***

  このプロファイルは、パターン IBM* と一致するユーザー ID の OWNER が、特定の値と等しくなければならないことを指定します。値は、ポリシー・プロファイルの **APPLDATA** フィールドに指定されます。

必須値ポリシー・プロファイルがある場合、それらによって、端末ユーザーが指定した値はすべて指定変更されます。このため、2 番目の例 (**C4R.USER.=OWNER.IBM***) では、端末ユーザーが次のコマンドを入力した場合、

```
ADDUSER IBMTEST OWNER(CMDVFY)
```

また、必須値ポリシー・プロファイルの **APPLDATA** に値 SYS1 が含まれている場合、RACF には実際に次のコマンドが渡されます。

```
ADDUSER IBMTEST OWNER(SYS1)
```

端末ユーザーは、ユーザー・プロファイルを作成するための十分な RACF 権限を持っている必要があります。アクセス権限が不十分な場合、RACF は通常のエラー・メッセージを出します。

プロファイルを使用することで、端末ユーザーが値を指定しなかった場合にデフォルト値を提供することができます。これらのプロファイルは**デフォルト**・ポリシー・プロファイルと呼ばれます。この場合も、RACF が値を必要とする場合、または特定の値をデフォルトとして使用する場合にのみ、これらのプロファイルを使用できます。RACF アクションが既存の値を変更しないことである場合、このプロファイルは使用されません。これらは、作成または追加タイプのコマンドに使用されます。これらのプロファイルの 3 番目の修飾子は / で始まります (/OWNER など)。必須値ポリシー・プロファイルがある場合、それらの方がデフォルト・ポリシー・プロファイルより優先されます。例えば、次のデフォルト・ポリシー・プロファイルの場合を考えてみましょう。

```
C4R.USER./OWNER.IBM*
```

このプロファイルがある場合、その APPLDATA 値は決して使用されません。必須値ポリシー・プロファイルによって値が提供されるため、デフォルト値は必要ありません。

必須値ポリシー・プロファイルとデフォルト値ポリシー・プロファイルを使用することで、単一のコマンドで複数のプロファイルを定義または変更できなくなる場合があります。大部分の RACF コマンドでは、単一のコマンドで複数のプロファイルを操作できます。

```
ADDUSER (AHJBTST, IBMTEST) OWNER(CMDVFY)
```

同じ必須値ポリシー・プロファイルを使用することで、2 番目のユーザー ID に必要な実際のコマンドは、以下のサンプルのようになります。

```
ADDUSER IBMTEST OWNER(SYS1)
```

ただし、OWNER の新しい値は、AHJBTST ユーザー ID に受け入れられない場合があります。単一の RACF コマンドでは、2 つの異なる OWNER を指定することはできません。競合を解決することができないため、コマンド全体が拒否されます。このような状況を回避するには、以下のようにします。

- インストール済み環境で、単一の RACF コマンドによって処理される可能性の高いすべてのプロファイルに対して、競合しないポリシーを指定する必要があります。例えば、必須値ポリシー・プロファイルをすべてのユーザー ID (C4R.USER./OWNER.**) に適用すれば、競合は生じません。
- 端末ユーザーは、RACF コマンドを分割して、それらが単一のプロファイルで機能するようにするか、一致するポリシー・プロファイルを持つプロファイルのみが単一の RACF コマンドにグループ化されるようにする必要があります。

前述のプロファイルについて詳しくは、端末ユーザーが指定したキーワード値の検査プロセスとともに以下のセクションで説明します。

SETROPTS 関連プロファイル

zSecure Command Verifier ポリシー・プロファイルの一般的な設計は、特定のプロファイルに対するコマンドの結果が中心に置かれています。しかし、一部のコマンドは、プロファイルまたはある範囲のプロファイルを明示的に管理しません。その最も明らかな例は SETROPTS コマンドで、これは、RACF データベース内のプロファイルでなく、RACF 設定に対して機能します。

SETROPTS コマンドのキーワードとパラメーターの制御には、疑似リソース・クラス RACF が使用されます。通常のプロファイル関連ポリシー・プロファイルは、45 ページの『ポリシー・プロファイルの構文』で説明されているように、4 つの修飾子から構成されています。

SETROPTS コマンドには多数のオプションがあるため、それらのオプションを管理するキーワードは広範なカテゴリーに分割されています。したがって、結果のポリシー・プロファイルは、以下の形式になります。

C4R.RACF.*category.field.value*

以下のカテゴリーは、現在、RACF オプションに使用されています。

LIST このカテゴリーは、**SETROPTS LIST** コマンドを記述するためにのみ使用されます。このカテゴリーでは、1 つのプロファイルだけが実装されています。

OPTION
このカテゴリーは、一般的な RACF オプション (ERASE、ADDCREATOR、および GRPLIST など) に使用されます。

AUDIT
このカテゴリーは、すべての監査関連 RACF 設定 (SAUDIT および CMDVIOL など) に使用されます。 LOGOPTIONS 設定は、このカテゴリーの一部ではありません。ログ・オプションはクラスごとに設定され、したがって、*class* カテゴリーの一部です。

JES このカテゴリーは、JES 関連設定に使用されます。

USER このカテゴリーは、InActive インターバルやパスワード・ヒストリーなどの USER およびパスワード・オプションに使用されます。

MLS このカテゴリーは、マルチレベル・セキュリティーの実装に関連するすべてのオプションに使用されます。

class すべての *class* 関連設定は、クラスごとに分類されています。これにより、1 つのポリシー・プロファイルを使用して、特定のリソース・クラスについて、すべてのクラス関連設定を制御できます。

多数のオプションと監査設定では、ポリシー・プロファイル内の *value* 修飾子は使用されません。以下のページの 7 つの表は、現在 zSecure Command Verifier ポリシー・プロファイルによって制御できるすべての RACF オプションを、カテゴリーごとに要約したものです。

これらのポリシー・プロファイルに見られる 1 つの重要な点は、REFRESH キーワードを記述する別個のポリシー・プロファイルが存在しないことです。REFRESH キーワードは、CLASS 関連キーワードの修飾子として取り扱われます。すべての CLASS 関連プロファイルについての説明を参照してください。

SETROPTS コマンドの複雑さのために、エラーおよび権限の失敗を抑止するための一般的な zSecure Command Verifier ポリシー・プロファイルは、実装されていません。zSecure Command Verifier は、権限の不足を検出した場合、C4R.SUPPRESS プロファイルおよび C4R.ERROR.CONTINUE プロファイルに対するユーザーの端末権限にかかわらず、コマンド全体を拒否します。

SETROPTS 関連プロファイルの実装例を以下に示します。

```
C4R.RACF.AUDIT.**             UACC(NONE) SYSAUDIT(UPDATE)
C4R.RACF.USER.**              UACC(NONE)
C4R.RACF.OPTION.**            UACC(NONE)
C4R.RACF.JES.**               UACC(NONE)
C4R.RACF.XFACILIT.**          UACC(NONE) CMVFYADM(UPDATE)
C4R.RACF.%CICS*.**            UACC(NONE) CICSADM(UPDATE)
C4R.RACF.PROGRAM.*            UACC(NONE) SPROGK(UPDATE)
C4R.RACF.*.RACLIST            UACC(READ)
C4R.RACF.**                   UACC(NONE)
```

場合によっては、必要なリソース・クラスのすべての側面を完全に管理できるよう、製品管理者にシステム SPECIAL またはシステム AUDITOR 属性を与える必要があります。また、多くの組織では、すべてのユーザーとグループの全プロファイルを管理できるように、中央のユーザー管理者にシステム SPECIAL が与えられています。そのようなユーザーの権限を制限するために、上記の例に示したようなプロファイルを実装できます。基本的に、それらのユーザーの制御範囲から、RACF システム全体の設定の管理を除外します。上記の例のプロファイルには、以下のような直接の効果があります。

- C4R.RACF.AUDIT.**

  SYSAUDIT グループ内のユーザーだけが、監査設定を変更できます。そのグループ外のその他のユーザーは、システム Auditor 属性を (例えば、それらのユーザーが各種の監査設定を表示できるようにするために) 与えられている場合でも、RACF グローバル監査設定を一切変更できません。

- C4R.RACF.USER.**

  誰もシステム・パスワードの規則およびオプションを変更できません。

- C4R.RACF.XFACILIT.**

  zSecure Command Verifier 管理者だけが XFACILIT リソース・クラスの設定を変更できます。この class は、classact および refresh ストレージ内プロファイルを含んでいます。

- C4R.RACF.PROGRAM.*

  システム・プログラミング部門の特定のユーザーだけが、PROGRAM 制御の SETROPTS 設定 (ストレージ内プロファイルの **REFRESH** を含む) を変更することができます。

- C4R.RACF.*.RACLIST

  すべてのシステム SPECIAL ユーザー、およびそれ以外で十分な RACF 権限を持っているすべてのユーザーは、RACLIST にあるリソース・クラスを **REFRESH** することができます。RACF は、CLAUTH またはグループ SPECIAL を持つユーザーが、それらのリソース・クラスを **REFRESH** することを許可します。

- C4R.RACF.**

  残りのすべての SETROPTS キーワードおよびパラメーターは、すべてのユーザーについて禁止されます。それらのオプションの 1 つを変更する必要がある場合は、CMVFYADM グループ内の誰かが一致するプロファイルを定義し、アクセスを提供し、XFACILIT リソース・クラスの REFRESH を発行する必要があります。SETROPTS 制御を実装する場合は、必ず、少なくとも 1 人のユーザーに XFACILIT クラスの管理権限を持たせる必要があります。

表 9 は、**SETROPTS LIST** コマンドを制御するために使用されるポリシー・プロファイルを示しています。説明は、簡単に検索できるよう、別の表に示してあります。

表 *9. SETROPTS LIST* 権限の検査に使用されるプロファイル： この表の項目は、特定のオプションを設定するために使用される SETROPTS キーワードを反映します。

キーワード	値	プロファイル
LIST	**N/A**	**C4R.RACF.LIST**

表 10 は、一般的な RACF オプションに使用されるすべてのポリシー・プロファイルの説明です。これらのオプションは、特定のシステムについて 1 回だけ設定され、後で変更されることはありません。

表 *10. RACF* オプションの検証に使用されるプロファイル： この表の項目は、特定のオプションを設定するために使用される SETROPTS キーワードを反映します。

キーワード	値	プロファイル
(NO)ADDCREATOR	**N/A**	**C4R.RACF.OPTION.ADDCREATOR**
(NO)ADSP	**N/A**	**C4R.RACF.OPTION.ADSP**
CATDSNS	*mode*	**C4R.RACF.OPTION.CATDSNS.***mode* *mode* ={ FAILURES, WARNING }
NOCATDSNS	**N/A**	**C4R.RACF.OPTION.CATDSNS.FAILURES** **C4R.RACF.OPTION.CATDSNS.WARNING**
(NO)EGN	**N/A**	**C4R.RACF.OPTION.EGN**
ERASE	*type*	**C4R.RACF.OPTION.ERASE.***type* *type* = { PROFILE, SECLEVEL, ALL }
(NO)GENERICOWNER **ENHANCEDGENERICOWNER**	**N/A**	**C4R.RACF.OPTION.GENERICOWNER**
(NO)GRPLIST	**N/A**	**C4R.RACF.OPTION.GRPLIST**
KERBLVL	*level*	**C4R.RACF.OPTION.KERBLVL**
PROTECTALL	*mode*	**C4R.RACF.OPTION.PROTECTALL.***mode* *mode* = { FAILURES, WARNING }
NOPROTECTALL	**N/A**	**C4R.RACF.OPTION.PROTECTALL.FAILURES** **C4R.RACF.OPTION.PROTECTALL.WARNING**
(NO)REALDSN	**N/A**	**C4R.RACF.OPTION.REALDSN**
RETPD	*period*	**C4R.RACF.OPTION.RETPD**
SESSIONINTERVAL **NOSESSIONINTERVAL**	*interval* **N/A**	**C4R.RACF.OPTION.SESSIONINTERVAL**
(NO)TAPEDSN	**N/A**	**C4R.RACF.OPTION.TAPEDSN**
TERMINAL	*access*	**C4R.RACF.OPTION.TERMINAL.***access*
RVARYPW	**SWITCH(***password***)**	**C4R.RACF.OPTION.RVARYPW.SWITCH**
RVARYPW	**STATUS(***password***)**	**C4R.RACF.OPTION.RVARYPW.STATUS**

次の表は、非クラス固有の監査オプションに使用されるすべてのポリシー・プロファイルについての説明です。これらのオプションは既に、システム AUDITOR 属性を持つユーザーだけに制限されています。ただし、ユーザーにこの属性を割り当てて監査設定を表示できるようにした場合は、ここに示すプロファイルを定義する必要があります。

表 *11. RACF* 監査設定の検査に使用されるプロファイル： この表の項目は、特定のオプションを設定するために使用される SETROPTS キーワードを反映します。

キーワード	値	プロファイル
(NO)APPLAUDIT	**N/A**	**C4R.RACF.AUDIT.APPLAUDIT**
(NO)CMDVIOL	**N/A**	**C4R.RACF.AUDIT.CMDVIOL**
(NO)INITSTATS	**N/A**	**C4R.RACF.AUDIT.INITSTATS**
(NO)OPERAUDIT	**N/A**	**C4R.RACF.AUDIT.OPERAUDIT**
(NO)SAUDIT	**N/A**	**C4R.RACF.AUDIT.SAUDIT**
(NO)SECLABELAUDIT	**N/A**	**C4R.RACF.AUDIT.SECLABELAUDIT**
SECLEVELAUDIT	*seclevel*	**C4R.RACF.AUDIT.SECLEVELAUDIT.***seclevel*
NOSECLEVELAUDIT	**N/A**	**C4R.RACF.AUDIT.SECLEVELAUDIT**

次の表は、JES 関連設定に使用されるすべてのポリシー・プロファイルについての説明です。通常、これらのオプションは 1 回だけ設定され、変更が必要になることはありません。

表 *12. JES* 関連設定の検査に使用されるプロファイル： この表の項目は、特定のオプションを設定するために使用される SETROPTS キーワードを反映します。

キーワード	値	プロファイル
(NO)BATCHALLRACF	**N/A**	**C4R.RACF.JES.BATCHALLRACF**
(NO)EARLYVERIFY	**N/A**	**C4R.RACF.JES.EARLYVERIFY**
(NO)XBMALLRACF	**N/A**	**C4R.RACF.JES.XBMALLRACF**
NJEUSERID	*userid*	**C4R.RACF.JES.NJEUSERID.***userid*
UNDEFINEDUSER	*userid*	**C4R.RACF.JES.UNDEFINEDUSER.***userid*

次の表は、USER および PASSWORD 関連の設定に使用されるすべてのポリシー・プロファイルについての説明です。

表 *13. USER* 関連設定の検査に使用されるプロファイル： この表の項目は、特定のオプションを設定するために使用される SETROPTS キーワードを反映します。

キーワード	値	プロファイル
(NO)INACTIVE	*days*	**C4R.RACF.USER.INACTIVE**
PASSWORD	**ALGORITHM(KDFAES)** **NOALGORITHM**	**C4R.RACF.USER.PASSWORD.ALGORITHM**
PASSWORD	**HISTORY(***count***)**	**C4R.RACF.USER.PASSWORD.HISTORY**
PASSWORD	**INTERVAL(***period***)**	**C4R.RACF.USER.PASSWORD.INTERVAL**
PASSWORD	**MINCHANGE(***period***)**	**C4R.RACF.USER.PASSWORD.MINCHANGE**
PASSWORD	**(NO)MIXEDCASE**	**C4R.RACF.USER.PASSWORD.MIXEDCASE**
PASSWORD	**REVOKE(***count***)**	**C4R.RACF.USER.PASSWORD.REVOKE**
PASSWORD	**RULEn(***rule-spec***)** **NORULEn** **NORULES**	**C4R.RACF.USER.PASSWORD.RULES**
PASSWORD	**(NO)SPECIALCHARS**	**C4R.RACF.USER.PASSWORD.SPECIALCHARS**
PASSWORD	**WARNING(***period***)**	**C4R.RACF.USER.PASSWORD.WARNING**

次の表は、マルチレベル・セキュリティー関連設定の制御に使用されるすべてのポリシー・プロファイルについての説明です。マルチレベル・セキュリティーを実装する場合を除いて、これらのオプションを変更してはなりません。

表 *14. MLS* 関連設定の検査に使用されるプロファイル： この表の項目は、特定のオプションを設定するために使用される SETROPTS キーワードを反映します。

キーワード	値	プロファイル
(NO)COMPATMODE	**N/A**	**C4R.RACF.MLS.COMPATMODE**
MLACTIVE	*mode*	**C4R.RACF.MLS.MLACTIVE.***mode* *mode***= {FAILURES, WARNING }**
NOMLACTIVE	**N/A**	**C4R.RACF.MLS.MLACTIVE.FAILURES** **C4R.RACF.MLS.MLACTIVE.WARNING**
MLS	*mode*	**C4R.RACF.MLS.MLS.***mode* *mode***= { FAILURES, WARNING }**
NOMLS	**N/A**	**C4R.RACF.MLS..FAILURESC4R.RACF.MLS.WARNING**
(NO)MLSTABLE	**N/A**	**C4R.RACF.MLS.MLSTABLE**
MLFSOBJ	*mode*	**C4R.RACF.MLS.MLFSOBJ**
MLIPCOBJ	*mode*	**C4R.RACF.MLS.MLIPCOBJ**
(NO)MLNAMES	**N/A**	**C4R.RACF.MLS.MLNAMES**
(NO)MLQUIET	**N/A**	**C4R.RACF.MLS.MLQUIET**
(NO)SECLABEL CONTROL	**N/A**	**C4R.RACF.MLS.SECLABELCONTROL**
(NO)SECLBYSYSTEM	**N/A**	**C4R.RACF.MLS.SECLBYSYSTEM**

次の表は、クラス固有オプションに使用されるすべてのポリシー・プロファイルについての説明です。通常、これらのオプションは、多数の異なるユーザーによって頻繁に設定されます。このカテゴリーのポリシー・プロファイルは、ストレージ内プロファイルを REFRESH する権限も記述します。

表 *15.* クラス固有設定の検査に使用されるプロファイル： この表の項目は、特定のオプションを設定するために使用される SETROPTS キーワードを反映します。

キーワード	値	プロファイル
(NO)AUDIT	*class*	**C4R.RACF.***class***.AUDIT**
(NO)CLASSACT	*class*	**C4R.RACF.***class***.CLASSACT**
(NO)GENCMD	*class*	**C4R.RACF.***class***.GENCMD**
(NO)GENERIC	*class*	**C4R.RACF.***class***.GENERIC**
(NO)GENLIST	*class*	**C4R.RACF.***class***.GENLIST**
(NO)GLOBAL	*class*	**C4R.RACF.***class***.GLOBAL**
(NO)RACLIST	*class*	**C4R.RACF.***class***.RACLIST**
(NO)STATISTICS	*class*	**C4R.RACF.***class***.STATISTICS**
(NO)WHEN	*class*	**C4R.RACF.***class***.WHEN**
LOGOPTIONS	*condition(class)*	**C4R.RACF.***class***.LOGOPTIONS.***condition*** *condition* **= { ALWAYS, NEVER, SUCCESSES, FAILURES, DEFAULT }**

以下のリストでは、プロファイルの詳しい説明と必要なアクセス権限を示します。

- **C4R.RACF.LIST**

  SETROPTS LIST コマンドを発行する権限を指定します。以下のアクセス規則が適用されます。

  プロファイルが見つからない
  : 通常の RACF 権限だけを使用して、現在の RACF 設定を **LIST** するための端末ユーザーの権限を決定する必要があります。

  NONE
  : 端末ユーザーは、現在の RACF 設定を **LIST** することを許可されません。

  READ
  : 端末ユーザーに十分な RACF 権限がある場合は、現在の RACF 設定をリストすることができます。

  UPDATE
  : READ と同じ。

  CONTROL
  : READ と同じ。

- **C4R.RACF.***category.keywords.values*

  ほとんどのポリシー・プロファイルのアクセス要件は、以下のとおりです。ポリシー・プロファイルの使用については、追加の注の説明を参照してください。

  プロファイルが見つからない
  : この制御は実装されません。通常の RACF 権限だけを使用する必要があります。

  NONE
  : 端末ユーザーは、RACF 設定を任意に変更することは許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーに十分な RACF 権限がある場合は、RACF 設定を変更できます。

  CONTROL
  : UPDATE と同じ。

- **C4R.RACF.OPTION.CATDSNS.***mode*

  CATDSNS オプションの設定を変更する権限を指定します。 CATDSDN オプションを *mode* パラメーターなしで使用した場合、RACF のデフォルトとして、FAILURES モードが使用されます。NOCATDSNS オプションを使用した場合、zSecure Command Verifier は現行の *mode* の有無を検査せず、両方の *mode* に対するアクセス権限を必要とします。ほとんどの環境では、総称 (「.**」) を最後の修飾子 (*mode*) に使用してください。

- **C4R.RACF.OPTION.ERASE.***mode*

スクラッチ設定で ERASE のオプションを変更する権限を指定します。ERASE がサブパラメーターなしで指定された場合、RACF は個々のデータ・セット・プロファイルの ERASE 設定を使用します。 zSecure Command Verifier では、*mode* PROFILE によってこれが記述されます。このモードは、NOERASE 設定にも使用されます。その他の ERASE 設定は、*modes* SECLEVEL および ALL によって記述されます。SECLEVEL ポリシー・プロファイルは、コマンドで指定された実際の *seclevel* を含んでいません。また、このプロファイルは NOSECLEVEL オプションの使用も記述します。ほとんどの状態では、最後の修飾子に総称 (".**") を使用します。

- **C4R.RACF.OPTION.GENERICOWNER**

  このポリシー・プロファイルは、GENERICOWNER オプションおよび ENHANCEDGENERICOWNER オプションの設定と削除を制御するために使用されます。

- **C4R.RACF.OPTION.KERBLVL**

  コマンドで指定された実際の *level* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.OPTION.PROTECTALL.***mode*

  PROTECTALL オプションの設定を変更する権限を指定します。 PROTECTALL オプションを *mode* パラメーターなしで使用した場合、RACF のデフォルトとして、FAILURES モードが使用されます。NOPROTECTALL オプションを使用した場合、zSecure Command Verifier は現行の *mode* の有無を検査せず、両方の *mode* に対するアクセス権限を必要とします。ほとんどの環境では、総称 (「.**」) を最後の修飾子 (*mode*) に使用してください。

- **C4R.RACF.OPTION.RETPD**

  コマンドで指定された実際のデフォルトの保存期間は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.OPTION.SESSIONINTERVAL**

  SESSIONINTERVAL オプションの設定を変更する権限を指定します。このプロファイルは、NOSESSIONINTERVAL と SESSIONINTERVAL 設定の両方に使用されます。

  コマンドで指定された実際のセッション *interval* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.OPTION.RVARYPW**.*action*

  このポリシー・プロファイルは、RVARY パスワードを設定する権限を記述します。RACF は、SWITCH と STATUS *action* の両方に別個のパスワードをサポートします。コマンドで指定された実際の RVARY パスワードは、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.AUDIT.SECLEVELAUDIT.***level*

  SECLEVELAUDIT オプションの設定を変更する権限を指定します。監査を行う必要のある上記の SECLEVEL を設定すると、*level* が zSecure Command Verifier ポリシー・プロファイルの最後の修飾子として組み込まれます。SECLEVELAUDIT を

無効にする場合、この *level* 修飾子は使用されません。ほとんどの環境では、総称 (「`.**`」) をこの最後の修飾子 (*level*) に使用してください。

- **C4R.RACF.USER.INACTIVE**

  コマンドで指定された実際の INACTIVE *days* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.USER.PASSWORD.ALGORITHM**

  このポリシー・プロファイルは、パスワード暗号化アルゴリズムの選択を制御します。選択された ALGORITHM (KDFAES) の名前は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.USER.PASSWORD.HISTORY**

  コマンドで指定された実際の HISTORY *count* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.USER.PASSWORD.INTERVAL**

  コマンドで指定された実際の INTERVAL *period* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.USER.PASSWORD.MINCHNAGE**

  コマンドで指定された実際の MINCHANGE *period* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.USER.PASSWORD.MIXEDCASE**

  このポリシー・プロファイルは、ユーザー・パスワードの `mixedcase`オプションの設定を制御します。

- **C4R.RACF.USER.PASSWORD.REVOKE**

  コマンドで指定された実際の REVOKE *count* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.USER.PASSWORD.RULES**

  この単一のポリシー・プロファイルを使用して、任意の RACF パスワード規則に対するすべての変更を記述します。このポリシー・プロファイルは、一部または全部のパスワード規則を無効にするときにも使用されます。現行バージョンの zSecure Command Verifier は、実際のパスワード規則の内容についてのサポートを提供しません。

- **C4R.RACF.USER.PASSWORD.SPECIALCHARS**

  このポリシー・プロファイルは、ユーザー・パスワードで追加の特殊文字を使用できるようにするオプションの設定を制御します。

- **C4R.RACF.USER.PASSWORD.WARNING**

  コマンドで指定された実際の WARNING *period* は、zSecure Command Verifier ポリシー・プロファイル内では表記されません。

- **C4R.RACF.MLS.MLACTIVE.***mode*

MLACTIVE オプションの設定を変更する権限を指定します。 MLACTIVE オプションを *mode* パラメーターなしで使用した場合、RACF のデフォルトとして、WARNING モードが使用されます。NOMLACTIVE オプションを使用した場合、zSecure Command Verifier は現行の *mode* の有無を検査せず、両方の *mode* に対するアクセス権限を必要とします。ほとんどの環境では、総称 (「.**」) を最後の修飾子 (*mode*) に使用してください。

- **C4R.RACF.MLS.MLS.***mode*

  MLS オプションの設定を変更する権限を指定します。 MLS オプションを *mode* パラメーターなしで使用した場合、RACF のデフォルトとして、 WARNING モードが使用されます。NOMLS オプションを使用した場合、zSecure Command Verifier は現行の *mode* の有無を検査せず、両方の *mode* に対するアクセス権限を必要とします。ほとんどの環境では、総称 (「.**」) を最後の修飾子 (*mode*) に使用してください。

- **C4R.RACF.MLS.MLFSOBJ**

  MLFSOBJ 処理のモードを変更する権限を指定します。両方のモード (ACTIVE および INACTIVE) が、同じ zSecure Command Verifier ポリシー・プロファイルによって記述されます。

- **C4R.RACF.MLS.MLIPCOBJ**

  MLIPCOBJ 処理のモードを変更する権限を指定します。両方のモード (ACTIVE および INACTIVE) が、同じ zSecure Command Verifier ポリシー・プロファイルによって記述されます。

- **C4R.RACF.***class.function*

  これらのプロファイルは、クラス関連オプションの活動化と非活動化、およびストレージ内プロファイルの REFRESH を行う権限を記述するために使用されます。 *function* は、上記の表に示されているどの機能でもかまいません。WHEN は、PROGRAM クラスにのみ適用されます。

  これらのポリシー・プロファイルのアクセス要件は、他のほとんどのポリシー・プロファイルのアクセス要件とは異なっています。READ アクセス・レベルは重要であり、ストレージ内プロファイルを REFRESH する権限を提供します。これは、リストされている *function* にのみ使用されます。

  ほとんどのインストールでは、最後の修飾子に総称 (.**) を使用します。LOGOPTIONS の場合、このオプションは監査レコードを作成する必要がある場合の *condition* を反映しています。追加の修飾子を使用すると、指定のユーザーへの委任が容易になります。

  プロファイルが見つからない
  : この制御は実装されません。通常の RACF 権限だけを使用する必要があります。

  NONE
  : 端末ユーザーは、その *class* について、*function* の活動化、非活動化、またはリフレッシュを行うことを許可されません。

  READ
  : 端末ユーザーは、その *class* について、ストレージ内プロファイルを

REFRESH することを許可されます。その場合、GENERIC、GENLIST、GLOBAL、RACLIST、および WHEN の各 *function* に適用されます。それ以外のすべての *function* では、このアクセス・レベルの効果はアクセス NONE と同じです。このアクセス・レベルでは、リストにあるどの *function* でも、REFRESH キーワードなしに使用することは許可されません。

UPDATE
端末ユーザーは、その *class* について、*function* を実行することを許可されます。この設定が適用されるのは、ユーザーが *function* を実行するのに十分な RACF 権限を持っている場合だけです。

CONTROL
UPDATE と同じ。

ユーザー ID を管理するためのプロファイル

以下のセクションのプロファイルは、ユーザー ID に関連するコマンドを管理するために使用されます。

指定可能なすべてのキーワードおよび対応するプロファイルが、いくつかのカテゴリーに分けられています。最初のプロファイル・グループでは、新規 userid の命名規則と、新規または既存の userid の RACF グループ階層内の場所について説明します。それ以後のセクションでは、ユーザーからグループへの接続と、ユーザーの属性および権限について説明します。

ユーザー ID の命名規則を実装したい場合は、命名規則を適用するためのプロファイルを使用する必要があります。新規ユーザー ID の RACF 階層内の位置を指定するには、ユーザー ID を RACF 階層に配置するためのプロファイルを使用します。ユーザーの属性と権限、およびその他のユーザー関連ポリシーを指定するために、追加のポリシー・プロファイルを使用できます。詳しくは、以下のトピックを参照してください。

- 89 ページの『ユーザー ID の命名規則』
- 91 ページの『既存のユーザーの削除』
- 93 ページの『RACF グループ階層での新規 ID の配置』
- 94 ページの『デフォルト・グループに対するポリシー・プロファイルの選択』
- 103 ページの『所有者のポリシー・プロファイル』
- 111 ページの『新規ユーザー・ポリシーの実装』
- 113 ページの『既存ユーザー・ポリシーの実装』
- 114 ページの『ユーザーの属性と権限に関するポリシー・プロファイル』
- 121 ページの『ユーザー・パスワードおよびパスフレーズ管理用のポリシー・プロファイル』
- 133 ページの『その他のユーザー関連ポリシー・プロファイル』

ユーザー ID の命名規則

多くのインストールには、ID の所属先の部門を示すユーザー ID 命名規則があります。zSecure Command Verifier は、それらの命名規則のいくつかを実装します。それらの規則は、新規ユーザー・プロファイルを作成するための ADDUSER コマンドにのみ適用されます。

表 16は、userid 自体を制御するプロファイルを要約したものです。 93 ページの表 17 および 94 ページの表 18 では、一部のキーワードの必須値とデフォルト値を説明します。 94 ページの表 19 では、端末ユーザーが指定した値を検査するためのプロファイルについて説明します。

表 *16. RACF* ユーザー *ID* の検査に使用されるプロファイル： この表の項目は、新規および削除された USERID の名前を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDUSER	*userid*	**C4R.USER.ID.=RACUID(n)**
ADDUSER	*userid*	**C4R.USER.ID.=RACGPID(n)**
ADDUSER	*userid*	**C4R.USER.ID.***userid*
DELUSER	*userid*	**C4R.USER.DELETE.***userid*

この表のプロファイルは、定義できる新規 userid を記述します。userid 自体については、zSecure Command Verifier は命名規則を適用するための制御を提供します。既存のユーザー ID を変更する権限は、命名規則では制御されません。この権限は、既に通常の RACF 範囲設定規則によって十分に制限されています。ユーザーを削除する権限は、通常の RACF 所有権規則によっても制御されますが、追加制御が必要です。したがって、その制御を実装するために別の名前ベースの規則が使用されます。新規 userid を定義するために、端末ユーザーは引き続き、CLAUTH(USER) と少なくとも 1 つのグループ関連権限 (JOIN、グループ SPECIAL 属性または直接所有権) を必要とします。

ユーザー ID ベースの制御は、新規 ID の命名規則を適用します。この最初のプロファイル・セットは、ユーザーの userid を制御します。これらのプロファイルは、どの userid を定義できるかを指定するためのものです。一般に、これらのプロファイルのうちの 1 つだけを使用して、命名規則を指定します。それより総称的なプロファイルを使用して、指定した命名規則に従わない新規 userid の定義をブロック化する必要があります。その場合、より限定的な個別プロファイルまたは総称プロファイルの定義によって、例外を実装できます。次の例で、それらのプロファイルの実装を示します。

```
C4R.USER.ID.=RACUID(4)        UACC(UPDATE)
C4R.USER.ID.TEST*             UACC(NONE) IBMUSER(UPDATE)
C4R.USER.ID.*                 UACC(NONE)
```

これらのプロファイルは、新規 userid の最初の 4 文字が、その ID を定義しようとしている端末ユーザーの最初の 4 文字と同じものでなければ、新規 userid を定義できないようにします。TEST で始まる userid は例外です。このユーザー ID は、端末ユーザー IBMUSER が定義できるほか、最初のプロファイルに従って、userid が TEST で始まるすべての端末ユーザーも定義できます。 3 番目のプロファイルは、指定された命名規則の外部での新規 userid の定義を停止するために必要です。 3 番目のプロファイルがない場合は、最初または 2 番目のプロファイル

によって明示的に、または一致するプロファイルがないことによって暗黙に、ほとんどすべての userid が受け入れられます。

- **C4R.USER.ID.=RACUID(n)**

  新規 userid の特殊な総称ポリシーを指定します。=RACUID は、端末ユーザーの userid を表しています。 substring(=RACUID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが userid の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁の数字だけが可変です。これは、1 から 8 までの範囲の値として指定する必要があります。真の総称プロファイルを使用することはできません。

  以下のアクセス規則が適用されます。

  プロファイルが見つからない
  : 端末ユーザーの userid は、新規 userid の命名規則として使用されません。検査は =RACGPID*(n)* プロファイルを使用して続行されます。

  NONE
  : 新規 userid は許可されません。コマンドはリジェクトされます。

  READ
  : NONE と同じ。

  UPDATE
  : 新規 userid は受け入れられます。

  CONTROL
  : UPDATE と同じ。

- **C4R.USER.ID.=RACGPID(n)**

  新規 userid の特殊な総称ポリシーを指定します。=RACGPID は、端末ユーザーの接続先グループのリストを表します。「**グループ・アクセス権限検査のリスト**」の設定とは関係なく、そのユーザーのすべてのグループが使用されます。このプロファイルが使用されるのは、=RACUID(*n*) プロファイルが存在しないか一致しない場合に限ります。substring(=RACGPID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが以降のパラグラフで示された他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが userid の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  : 端末ユーザーのグループは、新規 userid の命名規則として使用されません。検査は、C4R.USER.ID.userid プロファイルを使用して続行されます。

  NONE
  : 新規 userid は許可されません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
新規 userid は受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.USER.ID.***userid*

  端末ユーザーが作成できる新規 *userid* を指定します。このプロファイルは、=RACUID(*n*) と =RACGPID(*n*) がどちらも存在しないか一致しない場合に、ADDUSER コマンドについてのみ使用されます。この規則は、総称プロファイルによって表すことができます。

  プロファイルが見つからない
  新規ユーザー ID に命名規則は適用されません。

  NONE
  指定された userid は許可されません。 コマンドはリジェクトされます。

  READ
  NONE と同じ。

  UPDATE
  指定された userid を作成する許可。

  CONTROL
  UPDATE と同じ。

既存のユーザーの削除

このトピックに記載した **C4R.USER.DELETE.***userid* プロファイルを使用して、既存のユーザー ID を削除するための権限を制御します。

ユーザー・プロファイルを削除する権限は、通常、何らかの形の所有権によって (直接に、またはグループ SPECIAL 属性の範囲内で) およびシステム SPECIAL 権限によって制御されます。一部の組織では、既存のユーザーを削除する権限について、厳格な制御を保持したいと考えています。その理由は、ほとんどの場合、そのような組織ではデータ・セットの保存や名前変更、あるいは非 RACF 情報との対話といった追加のプロシージャーを実装していることにあります。このセクションで説明しているポリシー・プロファイルは、ユーザー ID の削除権限に対して追加の制約を課します。そのグループの削除が、構文エラーまたは不十分な権限のために RACF によって既に拒否されている場合、このプロファイルは検査されません。

ユーザー ID の削除は、ユーザー ID に対する =NOCHANGE ポリシーによっても制御できます。DELETE ポリシーによって ID の削除が許可されていても、=NOCHANGE ポリシー・プロファイルによってコマンドを拒否することができます。

- **C4R.USER.DELETE.***userid*

  このプロファイルを使用して、範囲内で削除可能とするユーザー ID を制御できます。総称プロファイルの使用時は、ユーザー ID の削除を完全に不可能にする

こともできます。このプロファイルを通じてアクセス権限を与えられた端末ユーザーのみが、それらのユーザー ID を削除できます。この制御は、通常の RACF 削除権限を縮小します。

プロファイルが見つからない
: この制御は実装されません。指定された userid の削除に対する追加制限はありません。

NONE
: その userid を削除することはできません。コマンドはリジェクトされます。

READ
: その userid を削除できるのは、端末ユーザーにシステム SPECIAL 属性がある場合だけです。

UPDATE
: その userid を削除できます。

CONTROL.
: UPDATE と同じ。

ユーザー・プロファイルに対するすべてのアクションの禁止

このトピックで説明している C4R.USER.=NOCHANGE.*owner.userid* プロファイルは、ユーザー ID に対するすべての変更またはアクションを禁止するために使用します。

前のセクションで説明したユーザー・プロファイルの削除禁止に加えて、zSecure Command Verifier には、選択したユーザーまたは一定範囲のユーザーに対するすべてのアクションを完全に禁止するオプションも備わっています。これを実行するには、ユーザー ID に対して =NOCHANGE ポリシー・プロファイルを定義します。=NOCHANGE ポリシー・プロファイルを定義すると、端末ユーザーが十分なアクセス権限を持っていない限り、以下の変更は禁止されます。

- ユーザー ID の属性の変更。
- ユーザー ID のパスワード、フレーズ、またはインターバルの設定または変更。
- グループへのユーザーの接続またはグループからのユーザーの削除。
- ユーザー ID の削除。
- ユーザー ID の直接アクセスの付与または削除。

これらの変更は個々のポリシー・プロファイルによって制御することもできます。=NOCHANGE ポリシー・プロファイルの利点は、単一のポリシー・プロファイルを使用してユーザー ID に関連するすべてのアクションを制御できることです。=NOCHANGE ポリシー・プロファイルを使用して、ユーザー ID の現在の定義を効果的にロックまたはフリーズすることができます。ポリシー・プロファイル内の修飾子 =NOCHANGE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。ユーザーのための =NOCHANGE ポリシー・プロファイルのフォーマットを以下に示します。

- **C4R.USER.=NOCHANGE.***owner.userid*

  このポリシー・プロファイルを使用して、ユーザー ID に対するすべての変更またはアクションを禁止できます。制御されるアクションは、ユーザー ID の変更

または削除、グループへの ID の接続またはグループからの ID の削除、データ・セットまたは一般リソースに対するユーザー ID の直接アクセスの付与または削除です。ポリシー・プロファイルを定義すると、このプロファイルを通じてアクセス権限を与えられた端末ユーザーのみが、それらのユーザー ID を変更できます。サポートされているアクセス・レベルは以下のとおりです。

プロファイルが見つからない
: この制御は実装されません。ターゲット・ユーザー ID の変更は禁止されません。

NONE
: 端末ユーザーには、ターゲット・ユーザー ID に対するアクションの実行が許可されません。

READ
: NONE と同じ。

UPDATE
: ターゲット・ユーザー ID が端末ユーザーの通常の RACF 範囲内にあれば、端末ユーザーはターゲット・ユーザー ID を変更できます。

CONTROL
: UPDATE と同じ。

RACF グループ階層での新規 ID の配置

上記のプロファイルに従って userid を作成する場合、RACF グループ階層内の新規 ID の配置に追加の規則を適用できます。

zSecure Command Verifier には、この側面を制御するために、以下のタイプのプロファイルが用意されています。

- 必須値プロファイルは、新規 `userid` に特定の所有者およびデフォルト・グループを強制します。
- デフォルト・プロファイルは、端末ユーザーが値を指定しなかった場合にデフォルト値を提供します。
- 最後のプロファイル・セットは、端末ユーザーが指定した値が受け入れ可能であるかどうかを検査します。

以下の情報では、これらのプロファイルを一緒に使用する方法と、どのキーワードを抑止または追加できるかについて説明します。

必須値プロファイルの場合、3 番目の修飾子は等号 (=) とそれに続くキーワードで構成されます。このため、`DFLTGRP` の場合、プロファイルの修飾子は `=DFLTGRP` です。表 17 で、必須値プロファイルを説明します。

表 *17. RACF* ユーザー *ID* の場所に関連したコマンド/キーワードの必須値ポリシー・プロファイル： この表の項目は、新規 `USERID` の必須値の場所を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDUSER	*userid*	**C4R.USER.=DFLTGRP.***userid*
ADDUSER	*userid*	**C4R.USER.=OWNER.***userid*

表 18 では、端末ユーザーが RACF グループ階層内の場所を制御するキーワードを何も指定しなかった場合に使用されるデフォルト・プロファイルについて説明します。デフォルト・プロファイルの場合、3 番目の修飾子はスラッシュとそれに続くキーワードで構成されます。このため、DFLTGRP の場合、ポリシー・プロファイルは /DFLTGRP を持ちます。

表 *18. RACF* ユーザー *ID* の場所に関連したコマンド/キーワードのデフォルト値に使用されるプロファイル： この表の項目は、新規 USERID のデフォルトの場所を記述するキーワードのデフォルト値を反映しています。

コマンド	キーワード	プロファイル
ADDUSER	*userid*	**C4R.USER./DFLTGRP.***userid*
ADDUSER	*userid*	**C4R.USER./OWNER.***userid*

表 19 では、端末ユーザーが指定した値の受け入れ可能性を検査するために使用されるプロファイルを説明しています。この表は、どのキーワードまたは関数に、どのプロファイルが使用されるかを要約したものです。

表 *19. RACF* ユーザー *ID* の検査に使用されるプロファイル： この表の項目は、新規または変更されたユーザー ID の名前と場所を記述するために端末ユーザーによって指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDUSER ALTUSER	**DFLTGRP**	**C4R.USER.DFLTGRP.=RACUID(n)**
ADDUSER ALTUSER	**DFLTGRP**	**C4R.USER.DFLTGRP.=RACGPID(n)**
ADDUSER ALTUSER	**DFLTGRP**	**C4R.USER.DFLTGRP.=USERID(n)**
ADDUSER ALTUSER	**DFLTGRP**	**C4R.USER.DFLTGRP.***group.userid*
ADDUSER ALTUSER	**DFLTGRP**	**C4R.USER.DFLTGRP./SCOPE.***group.userid*
ADDUSER ALTUSER	**DFLTGRP**	**C4R.USER.DFLTGRP./OWNER.***group.userid*
ADDUSER ALTUSER	**OWNER**	**C4R.USER.OWNER.=RACUID(n)**
ADDUSER ALTUSER	**OWNER**	**C4R.USER.OWNER.=RACGPID(n)**
ADDUSER ALTUSER	**OWNER**	**C4R.USER.OWNER.=USERID(n)**
ADDUSER ALTUSER	**OWNER**	**C4R.USER.OWNER.***owner.userid*
ADDUSER ALTUSER	**OWNER**	**C4R.USER.OWNER./SCOPE.***owner.userid*
ADDUSER ALTUSER	**OWNER**	**C4R.USER.OWNER./GROUP.***owner.userid*
ADDUSER ALTUSER	**OWNER**	**C4R.USER.OWNER./DFLTGRP.***owner.userid*

デフォルト・グループに対するポリシー・プロファイルの選択

デフォルト・グループに対するポリシー・プロファイルを実装するには、以下のガイドラインに従ってください。

新規ユーザーを定義するとき、または既存のユーザーを変更するときは、新規ユーザー ID の名前以外に、次の 2 つの側面が重要です。

- RACF 階層内での ID の場所 (OWNER)。
- ID のデフォルト・グループ (DFLTGRP)。

デフォルト・グループ自体は、いかなる意味でも決して特殊なものではありません。これが重要になるのは、ユーザーを定義するときだけです。なぜなら、これはユーザーを作成する権限を制御するからです。RACF では、端末ユーザーがそのグ

ループ内で JOIN 権限を持っているか、そのグループがグループ SPECIAL 属性の範囲内にあるか、端末ユーザーがそのグループを所有している必要があります。zSecure Command Verifier では、デフォルト・グループに対するいくつかの追加制御が実装されました。新規ユーザー・プロファイルを定義するには、端末ユーザーはシステム SPECIAL またはユーザー・クラスの CLAUTH も必要です。以下の段落では、上記の表にある zSecure Command Verifier プロファイルの使用方法について説明します。

最初のプロファイル・セットは、**ADDUSER** コマンドの新規 userid のデフォルト・グループ DFLTGRP を制御します。zSecure Command Verifier は、ALTUSER コマンドの OWNER および **DFLTGRP** に必須値またはデフォルト値プロファイルを使用しません。**ALTUSER** コマンドではこれらの既存の値は強制的に変更されないため、特定の値を強制する必要はありません。

新規ユーザー・プロファイルを定義するとき、zSecure Command Verifier は新規ユーザーを指定された DFLTGRP に CONNECT する権限も検査します。新規ユーザーの作成時に GROUP を DFLTGRP として指定すると、userid は GROUP に自動的に CONNECT されます。必須権限は、独立に検査されます。詳細については、 168 ページの『CONNECT の管理』を参照してください。

DFLTGRP の必須値およびデフォルト値ポリシー・プロファイル

新規 userid の DFLTGRP の必須値とデフォルト値を指定するには、以下のポリシー・プロファイルを使用します。これらのプロファイルは、**ADDUSER** コマンドにのみ使用されます。

- **C4R.USER.=DFLTGRP.***userid*

  このプロファイルは、新規に定義されるすべての userid の DFLTGRP について、必須値を指定するために使用されます。これは、ADDUSER コマンドにのみ使用されます。使用される DFLTGRP は、プロファイル内の APPLDATA フィールドから取得されます。この値は、端末ユーザーが指定した値を指定変更するために使用されるか、端末ユーザーが値を指定しなかった場合は、コマンドに追加されます。この必須値プロファイルによって取得された DFLTGRP 値は、追加の DFLTGRP 関連ポリシー・プロファイルの支配を受けません。

  値 *userid* は、影響を受けるユーザーを表します。この値は、一般規則への例外の指定を可能にします。最も限定的なプロファイルだけが zSecure Command Verifier によって使用されます。総称プロファイルを使用して、ユーザーの DFLTGRP を指定できます。

  ポリシー・プロファイル内の修飾子 =DFLTGRP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。必須値は強制されません。

  NONE
  : この制御は、端末ユーザーに対してアクティブにはされません。必須値は強制されません。

READ

APPLDATA フィールドが抽出され、コマンドで使用されます。このプロセスで有効なグループが生成されない場合、端末ユーザーの現行接続グループが代わりに使用されます。

UPDATE

READ と同じ。

CONTROL

この制御は、端末ユーザーに対してアクティブにはされません。必須値は強制されません。端末ユーザーがグループの値を指定した場合は、それが使用されます。値が指定されていなければ、端末ユーザーの現在のグループが RACF によって使用されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。ただし、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値プロファイルでは、これはアクセス権限 NONE が最終的にアクセス権限 CONTROL と同じ結果になるという変則的な状態になります。

APPLDATA フィールドで受け入れられる値は、以下のリストに示すとおりです。端末ユーザーには、新規グループを定義するための十分な権限が、割り当て済み `DFLTGRP` 内で引き続き必要です。この権限は、zSecure Command Verifier では検査されません。権限が不十分であると、RACF によってコマンドが失敗する場合があります。

BLANK

これは、RACF のデフォルト処理を使用する必要があることを示すために使用されます。つまり、端末ユーザーの現在のグループが RACF によって使用されます。

userid この項目は無効です。これは端末ユーザーによる誤入力が原因ではないため、コマンドは端末ユーザーの現在のグループを使用して続行することができます。

group このグループが挿入されます。端末ユーザーが、このグループに対する十分なアクセス権限を持っていない場合、コマンドは RACF によって拒否されます。

=OWNER

コマンドの OWNER キーワードによって指定された (またはデフォルトとして指定された) OWNER を反映します。この値は、zSecure Command Verifier によって挿入された OWNER 値である場合もあります。OWNER が特殊値 =DFLTGRP (デフォルト・グループを示します) へと解決された場合、コマンドは拒否されます。

=MYOWNER

端末ユーザーの OWNER を反映します。この値は、グループでなければなりません。それ以外のすべての状態は、エラーと見なされます。これは端末ユーザーによる誤入力が原因ではないため、コマンドは端末ユーザーの現在のグループを使用して続行することができます。

=USERID(n)

新規 USERID 自体の最初の *n* 文字を反映します。この値は GROUP である必要があります。その他の状態はエラーとしてみなされ、端末ユーザーの現在の GROUP が代わりに使用されます。

=RACGPID

C4R.USER.ID.=RACGPID(n) の =RACGPID(*n*) による userid の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、APPLDATA 値 =RACGPID はエラーと見なされ、端末ユーザーの現在のグループが代わりに使用されます。

zSecure Command Verifier は、このプロファイルを処理して DFLTGRP の必須値を判別した後で、指定された接続の権限を検査します (このことについては、すべてのユーザーからグループへの接続に関して解説する 168 ページの『CONNECT の管理』に説明があります)。

- **C4R.USER./DFLTGRP.***userid*

このプロファイルは、端末ユーザーが ADDUSER コマンドで DFLTGRP を指定しなかった場合に、DFLTGRP のデフォルト値を指定するために使用されます。上記の必須値ポリシー・プロファイルを使用して値が指定された場合、/DFLTGRP プロファイルは使用されません。

デフォルトとして使用される DFLTGRP は、プロファイル内の **APPLDATA** フィールドから取得されます。この必須値プロファイルによって取得された DFLTGRP 値は、追加の DFLTGRP 関連ポリシー・プロファイルの支配を受けません。

ポリシー・プロファイル内の修飾子 /DFLTGRP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。デフォルト値は提供されません。

NONE
: デフォルト値は提供されません。RACF によって通常提供されるデフォルトの使用も受け入れられず、コマンドは拒否されます。このアクセス・レベルを使用すると、インストールで端末ユーザーに DFLTGRP の値を明示的に指定するよう強制できます。

READ
: **APPLDATA** フィールドが抽出され、コマンドで使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。デフォルト値は提供されません。端末ユーザーの現在のグループが RACF によって使用されます。

APPLDATA フィールドで受け入れられる値は、以下のリストに示すとおりです。端末ユーザーには、新規グループを定義するための十分な権限が、割り当て済み DFLTGRP 内で引き続き必要です。権限が不十分であると、コマンドが失敗する場合があります。

BLANK
これは、RACF のデフォルト処理を使用する必要があることを示すために使用されます。端末ユーザーの現在のグループが使用されます。

userid この項目は無効です。これは端末ユーザーによる誤入力が原因ではないため、コマンドは端末ユーザーの現在のグループを使用して続行することができます。

group そのグループが挿入されます。

=OWNER
コマンドの OWNER キーワードによって指定された (またはデフォルトとして指定された) OWNER を反映します。この値は、zSecure Command Verifier によって挿入された OWNER 値である場合もあります。OWNER が特殊値 =DFLTGRP (デフォルト・グループを示します) へと解決された場合、コマンドは拒否されます。

=MYOWNER
端末ユーザーの所有者を表します。この値はグループでなければなりません。それ以外のすべての状態は、エラーと見なされます。このエラーは、端末ユーザーによる誤った入力によって起きるものではないため、コマンドは、端末ユーザーの現在のグループを使用して続行を許可されます。

=USERID(n)
新規 USERID 自体の最初の *n* 文字を反映します。この値は、グループでなければなりません。その他の状態はエラーとしてみなされ、端末ユーザーの現在のグループが代わりに使用されます。

=RACGPID
C4R.USER.ID.=RACGPID(n) の =RACGPID(*n*) による userid の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、APPLDATA 値 =RACGPID はエラーと見なされ、端末ユーザーの現在のグループが代わりに使用されます。

zSecure Command Verifier は、このプロファイルを処理して DFLTGRP のデフォルト値を判別した後で、指定された接続の権限を検査します (このことについては、すべてのユーザーからグループへの接続について解説する 168 ページの『CONNECT の管理』に説明があります)。

デフォルト・グループの検査

このトピック内のプロファイルは、新規ユーザーおよび既存ユーザーのデフォルト・グループの選択を制御するために使用されます。

これらのプロファイルは、端末ユーザーによる DFLTGRP の指定を検査するために使用されます。**ALTUSER** コマンドによるデフォルト・グループの選択に対する制限は、ほとんどの場合、大部分の RACF 処理とは関係ありません。ユーザーは、ログ

オン処理時に、依然としてそのグループのいずれかを現在のグループとして選択できます。デフォルト値の指定のみが、**ALTUSER** RACF コマンドによって制御されます。

ADDUSER コマンドを使用してシステムにユーザーを追加すると、DFLTGRP に対する 2 番目の検査が実行されます。DFLTGRP を選択すると、指定したグループに新規ユーザーも即時に接続されます。このため、そのユーザーを指定されたグループに接続する権限も検査されます。同じことがグループ権限についても当てはまります。ユーザーからグループへの接続および権限について詳しくは、 168 ページの『CONNECT の管理』を参照してください。

- **C4R.USER.DFLTGRP.=RACUID(*n*)**

  ADDUSER および ALTUSER コマンド内で、DFLTGRP の特殊な総称ポリシーを指定します。 =RACUID は、端末ユーザーの USERID を表しています。 substring(=RACUID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけがユーザー ID の値の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  : 端末ユーザーのユーザー ID は、DFLTGRP の命名規則または制限として使用されません。

  NONE
  : 指定された DFLTGRP は許可されません。 この決定は、プロファイル *group.userid* (**C4R.USER.DFLTGRP.***group.userid* を参照) に対する権限によって却下することができます。

  READ
  : NONE と同じ。

  UPDATE
  : 指定された DFLTGRP は受け入れられます。

  CONTROL
  : UPDATE と同じ。

- **C4R.USER.DFLTGRP.=RACGPID(*n*)**

  ADDUSER および **ALTUSER** コマンド内で、**DFLTGRP** の特殊な総称ポリシーを指定します。 =RACGPID は、端末ユーザーの接続先グループのリストを表します。「グループ・アクセス権限検査のリスト」の設定とは関係なく、そのユーザーのすべてのグループが使用されます。このプロファイルが使用されるのは、上記の =RACUID(*n*) プロファイルが存在しないか一致しない場合だけです。 substring(=RACGPID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルがリストの後に記載されている他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが USERID の突き合わせに使用されます。

このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

プロファイルが見つからない
: 端末ユーザーの現在のグループは、DFLTGRP の命名規則または制限として使用されません。

NONE
: 指定された DFLTGRP は許可されません。 この決定は、プロファイル *group.userid* (**C4R.USER.DFLTGRP.***group.userid* を参照) に対する権限によって却下することができます。

READ
: NONE と同じ。

UPDATE
: 指定された DFLTGRP は受け入れられます。

CONTROL
: UPDATE と同じ。

- **C4R.USER.DFLTGRP.=USERID(*n*)**

  ADDUSER および **ALTUSER** コマンド内で、**DFLTGRP** の特殊な総称ポリシーを指定します。 =USERID は、定義または変更されるユーザー ID を表します。 substring(=USERID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他の総称プロファイルに優先して使用されます。このプロファイルは、=RACUID(*n*) と =RACGPID(*n*) が存在しない場合、または一致しない場合にのみ使用されます。

  このプロファイルは個別プロファイルです。括弧内の 1 桁の数字だけが可変です。これは、1 から 8 までの範囲の値として指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  : userid の最初の *n* 文字は、ユーザーの DFLTGRP に対する制限として使用されません。

  NONE
  : 指定された DFLTGRP は許可されません。 この決定は、プロファイル *group.userid* (**C4R.USER.DFLTGRP.***group.userid* を参照) に対する権限によって却下することができます。

  READ
  : NONE と同じ。

  UPDATE
  : 指定された DFLTGRP は受け入れられます。

  CONTROL
  : UPDATE と同じ。

上記の 3 つのプロファイルのいずれかが、選択された DFLTGRP を許可する場合、次のプロファイルはスキップされます。処理は、 101 ページの『デフォルト・グループに対する追加のポリシー制御』で説明されている /SCOPE および /OWNER ポリ

シーを使用して続行されます。上記のプロファイルが特定の DFLTGRP の使用を許可しなかった場合、次のプロファイルが代替の許可方式として使用されます。

- **C4R.USER.DFLTGRP.***group.userid*

  このプロファイルは、前に定義した 3 つの規則とは関係なく使用されます。これを使用して、総称名ベースのポリシーに対する例外を指定できます。これは、*group* を新規 *userid* の DFLTGRP として使用できるかどうかを制御します。既存の ID の場合、このプロファイルは、そのユーザーのどのグループを ALTUSERコマンドで DFLTGRP として選択できるかを指定します。

  ほとんどの状態では、総称によって *userid* を指定します。明示的なプロファイルを使用して、特定の userid の例外を定義できます。

  このプロファイルは、前の 3 つのプロファイルのいずれかが、既に指定された DFLTGRP の使用を許可している場合には、使用されません。

  プロファイルが見つからない
  : この制御は実装されません。名前ベースのポリシーは適用されません。

  NONE
  : 指定された DFLTGRP は許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : groupname を使用できます。

  CONTROL
  : UPDATE と同じ。

デフォルト・グループに対する追加のポリシー制御

以下のプロファイルは、デフォルト・グループ (DFLTGRP) についての一般的な制約事項を定義するために使用されます。

1. 最初のプロファイル (**C4R.USER.DFLTGRP./SCOPE.***group.userid*) は、DFLTGRP をグループ SPECIAL 属性の範囲内だけに制限します。これは、事実上、JOIN 権限と GROUP の直接所有権を、新規ユーザー・プロファイルの作成を許可する手段としては無効にします。通常のユーザーはグループ SPECIAL を持たないことが普通なので、DFLTGRP に対するすべての変更は、それらのユーザーの範囲外と見なされます。このプロファイルは、通常のユーザーが自身の DFLTGRP を変更することも事実上禁止します。各ユーザーは、ログオン・プロセス中に、依然としてそのグループのいずれかを現在のグループとして選択できます。
2. 2 番目のプロファイル (**C4R.USER.DFLTGRP./OWNER.***group.userid*) は DFLTGRP を USERID の OWNER と比較します。これは、突き合わせを実施するために使用できますが、この一般規則に対する例外も許可します。

- **C4R.USER.DFLTGRP./SCOPE.***group.userid*

  このプロファイルは、新規ユーザーのデフォルト・グループが、グループ SPECIAL の範囲内に存在しなければならないことを指定するために使用されます。これは、既存のどのグループをデフォルト・グループとして選択できるかも制御します。このプロファイルの主な目的は、分散管理者が DFLTGRP を自身の制御しないグループに変更できないようにすることです。

変数 *userid* および *group* は、影響を受けるユーザー・プロファイルと、その新規 DFLTGRP を表します。これにより、一般規則への例外の指定が可能になります。zSecure Command Verifier は、最も限定的なプロファイルを使用します。

ポリシー・プロファイル内の修飾子 /SCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

グループ SPECIAL またはシステム SPECIAL を持つ端末ユーザーが、そのユーザーの新規デフォルト・グループを指定すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

– **C4R.USESCOPE.***group*

このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、ユーザーに対して指定されたデフォルト・グループに対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

/SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: この制御は実装されません。

NONE
: ADDUSER と **ALTUSER** のどちらのコマンドでも、端末ユーザーの範囲内にあるグループだけを **DFLTGRP** として指定できます。それ以外の GROUP が指定された場合、コマンドは拒否されます。

READ
: NONE と同じ。

UPDATE
: **ADDUSER** と **ALTUSER** のどちらのコマンドでも、端末ユーザーの範囲外にあるグループを使用できます。端末ユーザーが、指定されたグループ内で十分な権限を持っていない場合、コマンドは RACF によって拒否されます。

CONTROL
: このポリシーは、端末ユーザーには効果がありません。

- **C4R.USER.DFLTGRP./OWNER.***group.userid*

新規ユーザーの DFLTGRP が userid の OWNER と同じでなければならないことを指定します。ユーザーが DFLTGRP の値として所有者以外を指定するには、このプロファイルに対するアクセス権限が必要です。

既存のユーザーの場合、これは、**ALTUSER** コマンドによる DFLTGRP の選択を、ユーザー・プロファイルの現在の OWNER であるグループだけに制限します。OWNER が同じ **ALTUSER** コマンドの中で同時に変更される場合、新規 DFLTGRP は、新規 OWNER と突き合わせて検査されます。

新規 userid の場合は、前に述べた **C4R.USER.=DFLTGRP.***userid* の使用をお勧めします。 この必須値ポリシー・プロファイルは、端末ユーザーによって指定

されたすべての値にオーバーレイします。現行の /OWNER プロファイルは、端末ユーザーが正しい値を指定することを必要とします。必須値ポリシー・プロファイルを使用した場合、現行プロファイルはスキップされます。/OWNER プロファイルの主な目的は、特定のユーザーが DFLTGRP=OWNER 要件を免除されるようにすることです。

変数 *userid* および *group* は、影響を受けるユーザー・プロファイルと、その新規 DFLTGRP を表します。これらの変数により、一般規則の例外を指定することができます。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。

NONE
: ユーザーの DFLTGRP は、ユーザー ID の OWNER と同じでなければなりません。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、DFLTGRP にユーザー ID の現在の (または新規の) OWNER とは異なる値を指定することを許可されます。

CONTROL
: このポリシーは、端末ユーザーには効果がありません。

所有者のポリシー・プロファイル

新規に定義されたユーザー ID を記述するその他の情報部分は OWNER です。このセクション内のプロファイルは、所有者の指定を制御するために使用されます。

これらのプロファイルは、**ADDUSER** と **ALTUSER** の両方のコマンドに適用されます。一般に、これらのプロファイルの処理では、インストール済み環境のポリシーが GROUP を OWNER として使用することが想定されています。『OWNER の必須値およびデフォルト値プロファイル』で説明する最後のプロファイル /GROUP は、インストール済み環境でそのようなポリシーの適用が必要かどうかを表すために使用できる制御を提供します。ここでも、説明はいくつかのプロファイル・セットに分割されています。最初のプロファイル・セットは、所有者の必須値またはデフォルト値を指定します。2 番目のプロファイル・セットは、所有者に指定された値に対する制御を記述します。最後の 3 つのプロファイルからなるセットでは、ユーザー ID の OWNER に使用できる一般的なポリシーを説明します。

OWNER の必須値およびデフォルト値プロファイル

新規ユーザー ID の OWNER の必須値とデフォルト値を指定するには、以下のポリシー・プロファイルを使用します。これらのプロファイルは、**ADDUSER** コマンドにのみ使用されます。

- **C4R.USER.=OWNER.***userid*

このプロファイルは、新規に定義されたユーザー ID の OWNER の必須 (優先) 値を指定するために使用されます。これは、**ADDUSER** 処理のときにだけ使用されます。この必須値プロファイルから取得された OWNER 値は、追加の OWNER 関連ポリシー・プロファイルの支配を受けません。

ポリシー・プロファイル内の修飾子 =OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。必須値は強制されません。

NONE
: アクションは実行されません。必須値は強制されません。

READ
: **APPLDATA** フィールドが抽出され、コマンドで使用されます。プロセスで生成される ID が有効でない、つまり存在しない項目である場合は、端末ユーザーの現在のグループが代わりに使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーによって指定された OWNER の値が、コマンド内で使用されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。ただし、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値プロファイルでは、これはアクセス権限 NONE が最終的にアクセス権限 CONTROL と同じ結果になるという変則的な状態になる可能性があります。

APPLDATA フィールドで受け入れられる値は、以下のとおりです。OWNER は、ユーザー ID または GROUP です。

BLANK
: 指定された新規 OWNER 値は抑止され、端末ユーザーのユーザー ID によって置き換えられます。この値は、OWNER が指定されなかった場合に RACF が使用するデフォルト値です。/GROUP プロファイルに対するアクセス・レベルに応じて、zSecure Command Verifier は新規 OWNER としての端末ユーザーの使用を許可します。

userid
: /GROUP プロファイルに対するアクセス・レベルに応じて、*userid* が新規ユーザー ID の所有者として挿入されます。

group
: 指定された GROUP は、新規ユーザー ID の OWNER として使用されます。

=DFLTGRP
: コマンドで指定されたまたはデフォルトとして指定されたデフォルト・グループ DFLTGRP を表します。この値が特殊値 =OWNER (決定されようとしている OWNER) へと解決された場合、コマンドは失敗します。

=MYOWNER

端末ユーザーの OWNER を反映します。この値が GROUP の場合、値は新規ユーザー ID の OWNER として使用されます。この値がユーザー ID の場合、それ以上の処理は、端末ユーザーが /GROUP プロファイルに対して持つアクセス・レベルによって異なります。

=USERID(n)

新規ユーザー ID 自体の最初の *n* 文字を反映します。この値は GROUP のユーザー ID でなければなりません。その他の状態はエラーとしてみなされ、端末ユーザーの現在の GROUP が代わりに使用されます。

=RACGPID

C4R.USER.ID.=RACGPID(n) のユーザー ID の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、値 =RACGPID はエラーと見なされ、端末ユーザーの現在の GROUP が代わりに使用されます。

- **C4R.USER./OWNER.***userid*

このプロファイルは、新規に定義されたユーザー ID プロファイルの OWNER のデフォルト値を指定するために使用されます。これは、**ADDUSER** 処理のときにだけ使用されます。デフォルト値として使用される OWNER は、プロファイルの **APPLDATA** フィールドから取得されます。このデフォルト値プロファイルによって取得された OWNER 値は、追加の OWNER 関連ポリシー・プロファイルの支配を受けません。上記の =OWNER プロファイルを使用して値が指定された場合、/OWNER プロファイルは使用されません。

ポリシー・プロファイル内の修飾子 /OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない

この制御は実装されません。デフォルト値は提供されません。この場合、RACF から OWNER (端末ユーザー自身) のデフォルトが提供されます。

NONE

アクションは実行されません。デフォルト値は提供されません。zSecure Command Verifier は、RACF が OWNER の値を提供するのを許可しません。コマンドはリジェクトされます。このアクセス・レベルを使用すると、インストールで端末ユーザーに OWNER の値を明示的に指定するよう強制できます。

READ

APPLDATA フィールドが抽出され、コマンドで使用されます。プロセスで生成される ID が有効でない、つまり存在しない項目である場合は、端末ユーザーの現在のグループが代わりに使用されます。

UPDATE

READ と同じ。

CONTROL

この制御は、端末ユーザーに対してアクティブにはされません。デフォ

ルト値は提供されません。端末ユーザーが OWNER の値を指定しなかったため、RACF は端末ユーザーを新規プロファイルの OWNER にします。

APPLDATA フィールドで受け入れられる値は、以下のリストに示すとおりです。ユーザー ID またはグループを OWNER として指定できます。

BLANK
/GROUP プロファイルに対するアクセス・レベルに応じて、端末ユーザーは新規プロファイルの OWNER になることができます。

userid /GROUP プロファイルに対するアクセス・レベルに応じて、指定されたユーザー ID が新規ユーザー ID の OWNER として挿入されます。

group 指定された GROUP は、新規ユーザー ID の OWNER として使用されます。

=DFLTGRP
コマンドで指定されたまたはデフォルト設定されたデフォルト・グループ DFLTGRP を表します。この値が特殊値 =OWNER (新規プロファイルの OWNER) へと解決された場合、コマンドはリジェクトされます。詳細については、=DFLTGRP の説明を参照してください。

=MYOWNER
端末ユーザーの所有者を反映します。この値が GROUP の場合、値は新規ユーザー ID の OWNER として使用されます。この値がユーザー ID の場合、それ以上の処理は、端末ユーザーが /GROUP プロファイルに対して持つアクセス・レベルによって異なります。

=USERID(n)
新規ユーザー ID 自体の最初の *n* 文字を反映します。この値は GROUP のユーザー ID でなければなりません。その他の状態はエラーとしてみなされ、端末ユーザーの現在の GROUP が代わりに使用されます。

=RACGPID
C4R.USER.ID.=RACGPID(n) の USERID の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、値 =RACGPID はエラーと見なされ、端末ユーザーの現在の GROUP が代わりに使用されます。

指定された所有者の検査

以下に示すプロファイルのセットは、ADDUSER コマンドまたは **ALTUSER** コマンドで新規の **OWNER** が指定された場合に使用されます。

RACF 自体は、新規所有者の値に何も制約を課しません。新規所有者は、既存のユーザー ID か既存の GROUP である必要があります。この制限を除けば、すべての値が許可されます。このプロファイル・セットを使用して、新規 OWNER の選択を制限できます。指定された OWNER の使用が、これらの一般ポリシー・ルールのどれにも受け入れられない場合は、次のセクションの明示的プロファイルが使用されます。

- **C4R.USER.OWNER.=RACUID(*n*)**

このプロファイルは、ADDUSER および ALTUSER コマンド内で OWNER の特殊な総称ポリシーを指定します。=RACUID は、端末ユーザーの userid を表しています。 substring=(RACUID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが userid の突き合わせに使用されます。

このプロファイルは、個別プロファイルです。括弧内の 1 桁の数字だけ可変です。これは、1 から 8 までの範囲の値として指定する必要があります。真の総称プロファイルを使用することはできません。

端末ユーザーによって指定された OWNER が受け入れられた場合は、説明されている追加の検査 (/SCOPE および /GROUP など) を使用して処理が続行されます。

プロファイルが見つからない
: 端末ユーザーのユーザー ID は、OWNER の命名規則や制約事項としては使用されません。

NONE
: 指定された OWNER は許可されません。コマンドはリジェクトされます。この決定は、プロファイル *owner.userid* に対する権限によって、却下することができます。

READ
: NONE と同じ。

UPDATE
: 指定された OWNER は受け入れられます。

CONTROL
: UPDATE と同じ。

- **C4R.USER.OWNER.=RACGPID(*n*)**

  このプロファイルは、**ADDUSER** および **ALTUSER** コマンド内で OWNER の特殊な総称ポリシーを指定します。=RACGPID は、端末ユーザーの接続先グループのリストを表します。「グループ・アクセス権限検査のリスト」の設定とは関係なく、そのユーザーのすべてのグループが使用されます。substring=(RACGPID,1,*n*) が一致した場合は、*n* の値に関係なく、このプロファイルが他のプロファイルに優先して使用されます。これが使用されるのは、=RACUID(*n*) が存在しないか一致しない場合に限ります。これらのプロファイルを複数定義した場合は、*n* の値が最も小さいプロファイルだけが使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  端末ユーザーによって指定された OWNER が受け入れられた場合は、説明されている追加の検査 (/SCOPE および /GROUP など) を使用して処理が続行されます。

プロファイルが見つからない
端末ユーザーの GROUP は、OWNER の命名規則や制約事項としては使用されません。

NONE
指定された OWNER は許可されません。コマンドはリジェクトされます。この決定は、プロファイル *owner.userid* に対する権限によって、却下することができます。

READ
NONE と同じ。

UPDATE
指定された OWNER は受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.USER.OWNER.=USERID(*n*)**

このプロファイルは、ADDUSER および ALTUSER コマンド内で OWNER の特殊な総称ポリシーを指定します。特殊値 =USERID は、影響を受けるユーザー・プロファイル自体を表します。このプロファイルは、ユーザー ID の最初の *n* 文字が、その所有者の最初の *n* 文字と一致しなければならないことを示す命名規則を適用するために使用できます。

=USERID は、コマンド内の userid を表します。substring=(USERID,1,*n*) が指定された OWNER と一致した場合、*n* の値とは関係なく、このプロファイルが他の総称プロファイルに優先して使用されます。これは =RACUID(*n*) と =RACGPID(*n*) が存在しないか、一致しない場合にのみ使用されます。これらのプロファイルを複数定義した場合は、*n* の値が最も小さいプロファイルだけが使用されます。

このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

端末ユーザーによって指定された OWNER が受け入れられた場合は、説明されている追加の検査 (/SCOPE および /GROUP など) を使用して処理が続行されます。

プロファイルが見つからない
ターゲット・ユーザー ID 自体は、OWNER の命名規則または制限として使用されません。

NONE
指定された OWNER は許可されません。コマンドはリジェクトされます。この決定は、以下に述べるプロファイル *owner.userid* に対する権限によって、却下することができます。

READ
NONE と同じ。

UPDATE
指定された OWNER は受け入れられます。

CONTROL
UPDATE と同じ。

上記の 3 つのプロファイルのいずれかが、指定された OWNER を許可する場合、次のプロファイル規則はスキップされます。以下で説明する /SCOPE、/GROUP、および /DFLTGRP の各ポリシーで処理が続行されます。上記のプロファイルが特定の OWNER の使用を許可しなかった場合は、次のプロファイルが代替の許可方式として使用されます。

- **C4R.USER.OWNER.***owner.userid*

  この制御の主な目的は、前述の一般ポリシーがどれも適用されない場合に、ポリシーを指定することです。変数 *owner* は、*userid* の新規 OWNER を表します。その場合、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

  このポリシー・プロファイルで検査された OWNER には、さらに追加のポリシー /SCOPE、/GROUP、/DFLTGRP が適用されます。

  プロファイルが見つからない
  この制御は実装されません。

  NONE
  コマンドはリジェクトされます。

  READ
  NONE と同じ。

  UPDATE
  指定された OWNER は受け入れられます。

  CONTROL
  UPDATE と同じ。

所有者に対する追加のポリシー制御

命名規則を適用するためのプロファイルのほかに、既存の RACF グループ階層に基づいたポリシーを実装することもできます。

以下のプロファイルを使用すると、新規 OWNER の一般的な規則を指定できます。より限定的なプロファイル (または完全修飾プロファイル) を使用することにより、一部のユーザーまたはグループにそのような制限を免除することを指定できます。

3 つのプロファイル規則が、追加のポリシー・セットとして使用されます。指定された OWNER が上記のいずれかの規則で受け入れられた場合、その OWNER はこの 3 つのポリシーに対して検査されます。これらのポリシーのいずれかに失敗した場合、コマンドは拒否されます。

- **C4R.USER.OWNER./SCOPE.***owner.userid*

  このプロファイルは、端末ユーザーによって指定された新規 OWNER がグループ SPECIAL 属性の範囲内にある必要があるどうかを制御するために使用されます。その場合、**ADDUSER** コマンドと **ALTUSER** コマンドの両方に適用されます。このプロファイルは、端末ユーザーがグループ SPECIAL 属性の範囲内にあるユーザー ID プロファイルを「引き渡す」ことを防止できます。

変数 *userid* および *owner* は、影響を受けるユーザー・プロファイルと、その新規 OWNER を表します。このステップでは、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /SCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

新規所有者としてユーザー ID を指定することは、常に、端末ユーザーの管理範囲外と見なされます。

プロファイルがグループ SPECIAL 権限の範囲内にある場合、この権限の使用はプロファイルによって記録されます。

– **C4R.USESCOPE.***group*

このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。このポリシー・プロファイルでは、修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、指定された所有者に対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

/SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: 端末ユーザーのグループ SPECIAL 範囲は、ユーザー・プロファイルの新規 OWNER の制御に使用されません。

NONE
: 指定された新規 OWNER が端末ユーザーのグループ SPECIAL 属性の範囲外にある場合、コマンドは拒否されます。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーの範囲に関係なく、指定された OWNER は受け入れられます。

CONTROL
: UPDATE と同じ。

- **C4R.USER.OWNER./GROUP.***owner.userid*

このプロファイルは、指定された OWNER が RACF グループでなければならないかどうかを制御するために使用されます。このプロファイルは、上記の他のプロファイルとは関係なく検査されます。=OWNER と /OWNER のどちらのプロファイルが使用された場合でも、このポリシー・ルールはバイパスされます。

変数 *userid* および *owner* は、影響を受ける USERID と、その新規 OWNER を表します。このステップでは、一般規則への例外の指定が許可されます。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /GROUP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。指定の OWNER はグループまたはユーザー ID です。

NONE
: 指定された所有者が既存の RACF グループである場合、コマンドは受け入れられます。それ以外のすべての状態では、コマンドは拒否されます。

READ
: NONE と同じ。

UPDATE
: 指定された OWNER は、既存のグループを表していない場合でも受け入れられます。指定された OWNER が有効な項目でない場合、コマンドは RACF によって拒否されます。

CONTROL
: UPDATE と同じ。

- **C4R.USER.OWNER./DFLTGRP.***owner.userid*

  このプロファイルは、端末ユーザーによって指定された OWNER が、ユーザー ID の DFLTGRP と同じであることが必要かどうかを制御するために使用されます。その場合、**ADDUSER** コマンドと **ALTUSER** コマンドの両方に適用されます。

  値 *userid* および *owner* は、影響を受ける USERID と、その新規 OWNER を表します。このステップでは、一般規則への例外の指定が許可されます。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

  ポリシー・プロファイル内の修飾子 /DFLTGRP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。現在の DFLTGRP と異なる OWNER を指定できます。

  NONE
  : 指定される新規 OWNER は、現在または新規の DFLTGRP と同じでなければなりません。

  READ
  : NONE と同じ。

  UPDATE
  : DFLTGRP の値に関係なく、指定された OWNER は受け入れられます。

  CONTROL
  : UPDATE と同じ。

新規ユーザー・ポリシーの実装

以下のシナリオのガイドラインを使用して、新規ユーザー ID の指定でポリシー・プロファイルを実装します。

これまでのセクションでは、ユーザー ID と、RACF グループ階層内の場所の決定プロセスで使用されるプロファイルについて説明しました。これらのプロファイルを使用すると、端末ユーザーが作成できるユーザー ID を非常に柔軟に指定できます。新規ユーザー・ポリシーを実装するために必要なステップを記述するには、以下のシナリオを使用します。

- 中央管理者は、すべてのユーザーを定義できる。
- 分散管理者は、自分自身の部門についてのみ、ユーザーを定義できる。
- 部門は、RACF グループ構造 (所有権) によって認識できる。
- すべてのユーザー・プロファイルは、部門の構造に従って、RACF グループによって所有される必要がある。
- userid の最初の 3 文字が部門名の最初の 3 文字と同じ場合は、ユーザー ID 命名規則が使用される。

上記の組織には、以下のプロファイルを実装することができます。

c4r.user.id.* uacc(none) sysadmin(update)
このプロファイルにより、システム管理者だけが正規の命名規則の外部で新規ユーザー・プロファイルを定義することが許可されます。

c4r.user.id.=racuid(3) uacc(update)
このプロファイルにより、すべての分散管理者は、最初の 3 文字がその分散管理者と同じ文字の新規ユーザーを定義できます。CLAUTH(USER) とグループ SPECIAL 属性を持つ分散管理者だけが、新規ユーザーを定義できます。

注: =RACGPID(3) プロファイルによるこのポリシーの実装は、それほど効果的ではありません。端末ユーザーのすべてのグループが命名規則として使用されます。端末ユーザーが、異なる接頭部を持つ別の部門の機能グループに接続されていない、という保証はありません。

c4r.user.delete. uacc(none) sysadmin(update)**
このプロファイルにより、中央システム管理者だけが既存のユーザーの削除を許可されます。

c4r.user.=dfltgrp. uacc(update) sysadmin(control) appldata('=myowner')**
このプロファイルは、どの分散管理者が何を指定したかに関係なく、新規に定義される userid は常にその分散管理者自身を所有する GROUP に接続されることを指定します。中央システム管理者は、DFLTGRP を指定する必要があります。この制御は中央システム管理者には適用されないからです。ただし、次のプロファイルを参照してください。

c4r.user./dfltgrp. uacc(none) sysadmin(update) appldata('USERS')**
中央システム管理者が新規ユーザーの DFLTGRP を指定しなかった場合、そのユーザーは USERS と呼ばれるグループに割り当てられます。

c4r.user.=owner. uacc(update) sysadmin(control) appldata('=myowner')**
このプロファイルにより、新規ユーザー ID プロファイルの OWNER は、分散管理者の OWNER と同じものであることが保証されます。この場合も、この制御は中央システム管理者には適用されません。次のプロファイルは、それらの管理者の利用のために特に定義されています。

c4r.user./owner. uacc(none) sysadmin(update) appldata('=dfltgrp')**

=DFLTGRP を APPLDATA の値として使用することにより、OWNER の値が指定されなかった場合に、zSecure Command Verifier によって新規ユーザー ID の DFLTGRP と同じ値が OWNER に対して指定されます。

既存ユーザー・ポリシーの実装

以下のシナリオのガイドラインを使用して、既存のユーザー ID の指定でポリシー・プロファイルを実装します。

111 ページの『新規ユーザー・ポリシーの実装』の新規ユーザー・ポリシーの例で使用したポリシーに続いて、既存のユーザーを処理するためのポリシーをセットアップすることもできます。この例では、前に定義した新規ユーザー・ポリシーを、いくつかの追加規則によって以下のように拡張します。

- 中央管理者は、すべてのユーザーを変更できる
- 中央管理者は、任意のユーザーまたはグループを所有者として指定できる
- 分散管理者は、自分自身の部門内の所有者だけを変更できる
- 分散管理者は、既存のユーザーを**部門内にない** プールに戻すことができる
- **部門内にない** プールは、RACF グループ HOLDING によって実装される

この例では、ユーザーをグループに接続したり削除したりするために必要なプロファイルや、ユーザーの権限および属性を変更する方法については説明しません。次のセクションで、**CONNECT** および **REMOVE** コマンドを制御するために必要なプロファイルを示します。この例では、ユーザー ID は何らかの方法で RACF GROUP HOLDING に接続するものとします。

上記の組織には、以下のプロファイルを実装することができます。

c4r.user.dfltgrp./scope. uacc(none) sysadmin(control)**

このプロファイルにより、システム管理者だけがデフォルト・グループをすべての値に変更できます。分散管理者は、自己の制御範囲内にあるグループだけを指定できます。この /SCOPE プロファイルが定義されているため、通常のユーザーは自分自身のデフォルト・グループを永続的に変更できなくなります。ただし、ログオン時に現在の接続 GROUP を選択できることに変わりはありません。

c4r.user.owner./scope. uacc(none) sysadmin(control)**

このプロファイルにより、システム管理者だけが既存ユーザーの OWNER を変更する無制限の権限を持ちます。分散管理者は、自己の範囲内だけで OWNER を変更できます。自己のユーザー ID を引き渡すことはできません。通常のユーザーは、グループ SPECIAL を持たないため、自己が所有するユーザー ID の OWNER を変更することはできません。すべてがそのユーザーの範囲外にあります。

c4r.user.dfltgrp.HOLDING.* uacc(update)

このプロファイルは、RACF GROUP HOLDING を例外的なグループとして識別します。システム内のすべてのユーザーは、既に GROUP に接続している場合、RACF GROUP HOLDING を自己のデフォルト・グループとして選択できます。

c4r.user.owner.HOLDING.* uacc(control)

このプロファイルは、RACF GROUP HOLDING を例外的なグループとして識別します。これにより、すべての分散管理者は、既存のユーザーを現在の OWNER から HOLDING グループに転送できます。

ユーザーの属性と権限に関するポリシー・プロファイル

このセクションでは、ユーザーの属性と権限に関して実装できる制御について説明します。

同様な属性と権限が GROUP 接続についても存在します。 **ADDUSER** コマンドおよび **ALTUSER** コマンドで使用できるキーワードの一部は、DFLTGRP または指定された GROUP の GROUP 接続に適用されます。CONNECT 属性および権限については、168 ページの『CONNECT の管理』を参照してください。ユーザー/システム・レベルのキーワードは、以下の表にまとめています。

表 *20. RACF* 属性に使用されるプロファイル： この表の項目は、**ADDUSER** および **ALTUSER** コマンドで指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDUSER	**N/A**	**C4R.USER.=ATTR.***owner.userid*
ADDUSER ALTUSER	**SPECIAL**	**C4R.USER.ATTR.SPECIAL.***owner.userid*
ADDUSER ALTUSER	**OPERATIONS**	**C4R.USER.ATTR.OPERATIONS.***owner.userid*
ADDUSER ALTUSER	**AUDITOR**	**C4R.USER.ATTR.AUDITOR.***owner.userid*
ADDUSER ALTUSER	**ROAUDIT**	**C4R.USER.ATTR.ROAUDIT.***owner.userid*
ADDUSER ALTUSER	**RESTRICTED**	**C4R.USER.ATTR.RESTRICTED.***owner.userid*
ALTUSER	**UAUDIT**	**C4R.USER.ATTR.UAUDIT.***owner.userid*
ADDUSER ALTUSER	**ADSP**	**C4R.USER.ATTR.ADSP.***owner.userid*
ADDUSER ALTUSER	**GRPACC**	**C4R.USER.ATTR.GRPACC.***owner.userid*
ADDUSER ALTUSER	**NOPASSWORD NOPHRASE**	**C4R.USER.ATTR.PROTECTED.***owner.userid*
ADDUSER ALTUSER	**OIDCARD**	**C4R.USER.ATTR.OIDCARD.***owner.userid*
ALTUSER	**REVOKE**	**C4R.USER.ATTR.REVOKE.***owner.userid*
ALTUSER	**RESUME**	**C4R.USER.ATTR.RESUME.***owner.userid*
ALTUSER	**REVOKE**(*date*) **NOREVOKE**	**C4R.USER.ATTR.REVOKEDT.***owner.userid*
ALTUSER	**RESUME**(*date*) **NORESUME**	**C4R.USER.ATTR.RESUMEDT.***owner.userid*

ユーザー属性の必須値プロファイル

インストール済み環境では、ユーザー属性に対して必須ポリシー・プロファイルを使用することで、**ADDUSER** コマンドで使用されるキーワードに関係なく、新しいユーザーには常に特定の属性が必要であることを指定できます。

この機能の最も一般的な用途は、NOADSP 値と NOGRPACC 値の設定です。標準ポリシー・プロファイルを使用して、端末ユーザーが値 ADSP または GRPACC を指定できないようにすることができます。端末ユーザーが誤ってそのような値を指定した場合は、コマンドを拒否できます。必須値ポリシー・プロファイルを使用すると、受

け入れ不能な値を事実上、無視することができます。必須属性ポリシー・プロファイルおよび適用可能なアクセス・レベルを以下に示します。

ポリシー・プロファイル内の修飾子 =ATTR を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

- **C4R.USER.=ATTR.***owner.userid*

  プロファイルが見つからない
  : この制御は実装されません。アクションは実行されません。

  NONE
  : 必須属性は端末ユーザーには適用されません。

  READ
  : 必須値ポリシー・プロファイルの APPLDATA は、新規ユーザーの属性のリストとして使用されます。

  UPDATE
  : READ と同じ。

  CONTROL
  : この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーによって指定された属性がコマンド内で使用されます。

注**:**

1. 他の必須値ポリシー・プロファイルとは異なり、=ATTR ポリシー・プロファイルを使用して割り当てられた属性は、通常の属性のポリシー・プロファイルと照らして検査されます。例えば、 =ATTR ポリシーを使用して OPERATIONS 属性を割り当てる場合、端末ユーザーは、対応する **C4R.USER.=ATTR.OPERATIONS.***owner.userid* ポリシー・プロファイルに対するアクセス権限も持っている必要があります。
2. このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値プロファイルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

必須値ポリシー・プロファイルの **APPLDATA** フィールドは、ユーザー属性のリストを指定します。認識されるユーザー属性は以下のとおりです。

- SPECIAL および NOSPECIAL
- OPERATIONS および NOOPERATIONS
- AUDITOR および NOAUDITOR
- ROAUDIT および NOROAUDIT
- PASSWORD および NOPASSWORD
- RESTRICTED および NORESTRICTED
- OIDCARD および NOOIDCARD
- ADSP および NOADSP
- GRPACC および NOGRPACC

属性には省略形を使用できません。複数の属性を割り当てる必要がある場合は、個々の属性を単一のコンマで区切り、間にブランクを入れないようにする必要があります。以下に例を示します。

```
NOADSP,NOGRPACC
```

ユーザー属性およびアクセス・レベルの説明

以下のガイドラインおよびポリシー・プロファイルの属性を使用して、使用可能なキーワードと値を制御するためのアクセス・レベルを設定します。

一般に、必要となるアクセス・レベルは、属性を与えるための UPDATE か、属性を除去するための READ です。**ADDUSER** コマンドの場合は、RACF で使用されるデフォルト値が zSecure Command Verifier で検査されません。ただし、デフォルト以外の値は、**ALTUSER** コマンドで行われる検査と同様の方法で検査されます。

- **C4R.USER.ATTR.SPECIAL.***owner.userid*
- **C4R.USER.ATTR.OPERATIONS.***owner.userid*
- **C4R.USER.ATTR.AUDITOR.***owner.userid*
- **C4R.USER.ATTR.ROAUDIT.***owner.userid*
- **C4R.USER.ATTR.ADSP.***owner.userid*
- **C4R.USER.ATTR.GRPACC.***owner.userid*

  プロファイルが見つからない
  : この制御は実装されません。アクションは実行されません。

  NONE
  : 端末ユーザーは、**ALTUSER** コマンドにどちらのキーワードも指定することを許可されません。**ADDUSER** コマンドでは非属性キーワードが許可 (デフォルトで指定) されます。

  READ
  : 端末ユーザーは、**ALTUSER** コマンドで明示的に非属性キーワードを指定することを許可されます。この設定は、これらの属性の除去を可能にします。

  UPDATE
  : 端末ユーザーは、**ALTUSER** コマンドで、どちらのキーワードでも指定することを許可されます。この設定は、これらの属性の通常の保守が可能となります。

  CONTROL
  : この制御は、端末ユーザーに対して実装されません。端末ユーザーは、**ADDUSER** および **ALTUSER** コマンドで、どちらのキーワードでも指定することを許可されます。この設定は、これらの属性の通常の保守が可能となります。

  上記のすべての場合において、端末ユーザーがキーワードを指定するためには十分な RACF 権限が必要です。例えば、ほとんどのキーワードの場合、端末ユーザーは SPECIAL 属性を持っている必要があります。

- **C4R.USER.ATTR.RESTRICTED.***owner.userid*

  プロファイルが見つからない
  : この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、**(NO-)RESTRICTED** オペランドを指定することを許可されません。デフォルト値 **NORESTRICTED** は、**ADDUSER** コマンドで許可されます。

READ
端末ユーザーは、ADDUSER および **ALTUSER** コマンドで **RESTRICTED** キーワードを指定することを許可されます。この設定により、ターゲット・ユーザーの標準アクセスの対象が、明示的に使用を許可されたリソースのみに削減されます。

UPDATE
端末ユーザーは、ALTUSER コマンドで **NORESTRICTED** キーワードを指定することを許可されます。この設定は、RESTRICTED 属性の通常の保守を可能にします。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、**ADDUSER** および **ALTUSER** コマンドで、どちらのキーワードでも指定することを許可されます。

- **C4R.USER.ATTR.UAUDIT.***owner.userid*

UAUDIT 属性は、**システム** AUDITOR 属性を持つ端末ユーザーだけが表示でき、割り当てることができます。この結果、すべての RACF 検査は SMF によって監査されます。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、**(NO-)UAUDIT** オペランドを指定することを許可されません。

注**: (NO-)UAUDIT** キーワードは、**ADDUSER** コマンドでは使用できません。

READ
端末ユーザーは、ALTUSER コマンドで **NOUAUDIT** キーワードを指定することを許可されます。

UPDATE
端末ユーザーは、ALTUSER コマンドで **UAUDIT** キーワードを指定することを許可されます。この設定は、UAUDIT 属性の通常の保守を可能にします。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、**ALTUSER** コマンドで、どちらのキーワードでも指定することを許可されます。

- **C4R.USER.ATTR.PROTECTED.***owner.userid*

PROTECTED 属性は、PASSWORD も PHRASE 持たないユーザーの事実上のステータスです。技術的には OIDCARD も関連がありますが、OIDCARD は最新システムでは使用されなくなりました。パスワードしか持たないユーザーは、パスワードを削除することによって保護できます。KDFAES パスワード・アルゴリ

ズムを導入することにより、フレーズのみのユーザー を作成できるようになりました。このようなユーザーからパスフレーズを削除することでも、保護ユーザーが作成されます。

NOPASSWORD キーワードまたは NOPHRASE キーワードを指定した **ALTUSER** コマンドが、保護ユーザーを作成する場合があります。同様に、PASSWORD または PHRASE キーワードを使用すると、保護ステータスが削除される場合があります。**ALTUSER** コマンドによってユーザーの保護ステータスが変更される場合は、現在のセクションの PROTECTED ポリシーが使用されます。保護ステータスがコマンドの影響を受けない場合は、通常の PASSWORD ポリシーまたは PHRASE ポリシーが使用されます。 121 ページの『ユーザー・パスワードおよびパスフレーズ管理用のポリシー・プロファイル』を参照してください。

ADDUSER コマンドが保護ユーザーの作成をもたらす場合は、このコマンドにもこのセクションで説明するポリシーが適用されます。このポリシーを使用すると、新規ユーザー ID に常にパスワードまたはフレーズが割り当てられるようにすることができます。**ADDUSER** コマンドを使用して最初に PROTECTED として作成されたユーザー ID は、このポリシーの特殊なアクセス・レベル要件の適用対象です。このようなユーザー ID が使用されていない場合は、保護属性の削除に必要な権限は READ 権限のみです。これは、保護ユーザー ID の作成に必要なアクセス・レベルと同じです。ユーザー ID が使用された場合や、ユーザー ID に対して **ALTUSER RESUME** コマンドが実行された場合、この特殊なステータスはリセットされます。この場合、保護ステータスの削除には、現行ポリシーへの通常の UPDATE 権限が必要です。

保護ステータスを変更するには、以下のアクセス・レベルが使用されます。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: NOPASSWORD または NOPHRASE キーワードによってターゲット・ユーザーが保護される場合、端末ユーザーはこれらのキーワードを指定することを許可されません。ターゲット・ユーザーが現在保護されている場合、PASSWORD および PHRASE キーワードの使用も禁止されます。

READ
: 端末ユーザーは、NOPASSWORD または NOPHRASE キーワードを指定して、保護ユーザーを作成することを許可されます。ターゲット・ユーザーが現在、保護ステータスであるが、使用されたことがない (**RACF LISTUSER** 出力に LAST-ACCESS=UNKNOWN と表示される) 場合は、PASSWORD または PHRASE の割り当てが許可されます。ターゲット・ユーザーが現在、保護ステータスであり、使用されたことがある (**RACF LISTUSER** 出力に LAST-ACCESS 日時が表示される) 場合は、PASSWORD または PHRASE キーワードによる保護ステータスの削除は許可されません。

UPDATE
: 端末ユーザーは、NOPASSWORD または NOPHRASE キーワードを指定して、保護ユーザーを作成することを許可されます。PASSWORD ま

たは PHRASE キーワードとともに **ALTUSER** コマンドを使用して保護ステータスを削除することも許可されます。このアクセス・レベルが必要になるのは、保護ステータスで作成され、その後使用されたユーザー ID、または ALTUSER RESUME コマンドの対象となったユーザー ID に、PASSWORD または PHRASE を割り当てる場合です。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、ID の保護ステータスに影響するすべてのキーワードを指定することを許可されます。

- **C4R.USER.ATTR.OIDCARD.***owner.userid*

このプロファイルは、NOOIDCARD および OIDCARD キーワードの使用を制御するために使用されます。ADDUSER コマンドの場合、デフォルト・キーワード **NOOIDCARD** は、検査されません。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、**ALTUSER** コマンドで **(NO-)OIDCARD** オペランドを指定することを許可されません。ADDUSER コマンドでは、**NOOIDCARD** キーワードが許可 (デフォルトで指定) されます。

READ
端末ユーザーは、**ALTUSER** コマンドで NOOIDCARD キーワードを指定して、既存のユーザーの OIDCARD をリセットすることを許可されます。

UPDATE
端末ユーザーは、OIDCARD キーワードを指定して、新規または既存のユーザーの oidcard を設定することを許可されます。このコマンドが成功するのは、端末ユーザーが、端末に接続した磁気カード・リーダーに物理的にアクセスできる場合だけです。

CONTROL
この制御は、端末ユーザーに対して実装されません。

- **C4R.USER.ATTR.REVOKE.***owner.userid*

このポリシー・プロファイルは、将来の**取り消し** 日がない REVOKE 属性にのみ適用されます。取り消し日の管理は、REVOKEDT ポリシー・プロファイルによって制御されます。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、ユーザーを取り消すことを許可されません。この設定は、将来の取り消し日が指定されていない REVOKE キーワードに適用されます。

READ
端末ユーザーは、userid を REVOKE することを許可されます。この設定は、将来の取り消し日が指定されていない REVOKE キーワードに適用されます。

UPDATE
READ と同じ。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、userid を取り消すことを許可されます。

- **C4R.USER.ATTR.RESUME.***owner.userid*

このポリシー・プロファイルは、将来の再開日がない RESUME 属性にのみ適用されます。再開日の管理は、RESUMEDT ポリシー・プロファイルによって制御されます。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、ユーザーを再開することを許可されません。この設定は、将来の再開日が指定されていない RESUME キーワードに適用されます。

READ
NONE と同じ。

UPDATE
端末ユーザーは、userid を RESUME することを許可されます。この設定は、将来の再開日がない即時の RESUME にのみ適用されます。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、userid を再開することを許可されます。

- **C4R.USER.ATTR.REVOKEDT.***owner.userid*

このポリシー・プロファイルは、将来の**取り消し** 日がある REVOKE 属性に適用されます。また、これは、既存の取り消し日を削除するための NOREVOKE キーワードの使用にも適用されます。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、ユーザーの**取り消し** 日の管理を許可されません。この設定は、REVOKE(*date*) と NOREVOKE オプションの両方に適用されます。

READ
NONE と同じ。

UPD 端末ユーザーは、REVOKE(*date*) または NOREVOKE によって**取り消し** 日を管理することを許可されます。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、userid の取り消し日の管理を許可されます。

- **C4R.USER.ATTR.RESUMEDT.***owner.userid*

このポリシー・プロファイルは、将来の再開日がある RESUME 属性に適用されます。また、これは、既存の再開日を削除するための NORESUME キーワードの使用にも適用されます。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: 端末ユーザーは、ユーザーの**再開** 日の管理を許可されません。この設定は、RESUME(*date*) と NORESUME オプションの両方に適用されます。

READ
: NONE と同じ。

UPD 端末ユーザーは、RESUME(*date*) または NORESUME によって**再開** 日を管理することを許可されます。

CONTROL
: この制御は、端末ユーザーに対して実装されません。端末ユーザーは、userid の再開日の管理を許可されます。

ユーザー・パスワードおよびパスフレーズ管理用のポリシー・プロファイル

このセクションでは、ユーザーのパスワードおよびパスフレーズに関連する、すべてのキーワードと制御プロファイルについて要約します。

PROTECTED 属性は (NO)PASSWORD および (NO)PHRASE キーワードによっても制御されますが、それについては 116 ページの『ユーザー属性およびアクセス・レベルの説明』で他の属性と一緒に説明されています。

ここで説明するポリシー・プロファイルのうち、1 つはパスワードを設定または変更する権限の制御に使用されるポリシー・プロファイルであり、もう 1 つはパスフレーズの設定または変更に使用されるポリシー・プロファイルです。管理者により設定されたパスワードに対して制限された品質制御を行うために、2 つの特殊なポリシー・プロファイルが用意されています。残りのパスワード・ポリシーは、パスワード/フレーズのインターバルの設定と expired/noexpired キーワードの使用を制御します。

重要**:** この制御は、ユーザーがログオン時に自己のパスワードを変更するために設定するパスワードに対しては、いかなる標準も適用しません。

zSecure Command Verifier には、ALTUSER コマンドで PWCONVERT キーワードおよび PWCLEAN キーワードを使用できるユーザーを制御するための 2 つのポリシー・プロファイルも備わっています。これら 2 つのオプションは通常のパスワード管理では使用しないため、これらのポリシー・プロファイルについては、他のユーザー関連ポリシー・プロファイルに関する一般的なセクションで説明しています。 133 ページの『その他のユーザー関連ポリシー・プロファイル』を参照してください。

次の表は、RACF ユーザー・パスワードおよびパスフレーズを管理するために使用できるポリシー・プロファイルのリストです。インターバルと有効期限のポリシー・プロファイルは、パスワードのみに適用することが推奨されますが、パスワー

ドとフレーズにも適用されます。パスワード・インターバルとフレーズ・インターバルを制御する個別のポリシーはありません。表内の各プロファイルの詳しい説明は、表の後に示してあります。

表 *21. RACF* パスワードに使用されるプロファイル： この表の項目は、**ADDUSER**、**ALTUSER**、および **PASSWORD** コマンドで指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDUSER ALTUSER	**PASSWORD**	**C4R.USER.PASSWORD.***owner.userid*
ADDUSER ALTUSER	**PASSWORD**	**C4R.USER./PASSWORD.***owner.userid*
PASSWORD	**PASSWORD**	**C4R.USER.PASSWORD.=RACUID**
ADDUSER ALTUSER	**PHRASE**	**C4R.USER.PHRASE.***owner.userid*
PASSWORD	**PHRASE**	**C4R.USER.PHRASE.=RACUID**
ADDUSER ALTUSER	**PASSWORD**	**C4R.USER.PASSWORD.=DFLTGRP**
PASSWORD	**USER(***userid***)**	**C4R.USER.PASSWORD.=DFLTGRP**
ADDUSER ALTUSER	**PASSWORD**	**C4R.USER.PASSWORD.=USERID**
PASSWORD PHRASE	**(NO)INTERVAL**	**C4R.USER.=PWINT.***owner.userid*
PASSWORD PHRASE	**(NO)INTERVAL**	**C4R.USER.PWINT.***owner.userid*
ALTUSER	**(NO)EXPIRED**	**C4R.USER.PWEXP.***owner.userid*

以下の項目は、zSecure Command Verifier のパスワード関連機能を制御するために使用されるポリシー・プロファイルとアクセス・レベルについての説明です。

- **C4R.USER.PASSWORD.***owner.userid*

  このポリシー・プロファイルは、**ADDUSER** コマンドまたは **ALTUSER** コマンドを使用した管理者によるパスワードの設定を制御します。 **PASSWORD** コマンドによる自分のパスワードの設定は、=RACUID プロファイルによって制御されます。一部のレベルの RACF では、**PASSWORD** コマンドで別のユーザーのパスワードを設定できます。これは、値 =DFLTGRP のパスワード品質プロファイルによって制御されます。

  (NO)PASSWORD キーワードを使用しても保護ステータスが変わらない場合は、現行のプロファイルが使用されます。これらのキーワードによってユーザーが保護されたり、保護ステータスが削除されたりする場合は、代わりに **C4R.USER.ATTR.PROTECTED** プロファイルが使用されます。詳細については、116 ページの『ユーザー属性およびアクセス・レベルの説明』を参照してください。ここで説明するプロファイルは、通常の (NON-PROTECTED) ユーザーのパスワードを管理する権限を制御します。

  プロファイルが見つからない
  : この制御は実装されません。アクションは実行されません。

  NONE
  : 端末ユーザーは、**PASSWORD** オペランドを指定することを許可されません。**ADDUSER** コマンドを使用する場合、RACF のレベルによっては、このアクセス・レベルは、RACF のデフォルト・パスワード (=DFLTGRP) を持つユーザー、または PROTECTED ユーザーになる場合があります。どちらも、パスワード品質または保護ステータス用に適切なポリシーを定義することで回避できます。

READ

NONE と同じ。

UPDATE

端末ユーザーは、**ALTUSER** コマンドで **PASSWORD** オペランドを指定して、既存のユーザーのパスワードをリセットすることを許可されます。ただし、ターゲット・ユーザーが現在 PROTECTED 属性を持っている場合、**PASSWORD** オペランドは許可されません。このアクセス・レベルでは通常のパスワード保守は許可されますが、PROTECTED userid が NON-PROTECTED になるのは防止されます。

CONTROL

この制御は、端末ユーザーに対して実装されません。端末ユーザーは、ターゲット userid が現在 PROTECTED 属性を持っている場合以外、PASSWORD キーワードを指定することを許可されます。

- **C4R.USER./PASSWORD.***owner.userid*

このポリシー・プロファイルは、**ADDUSER** コマンドまたは **ALTUSER** コマンドが PASSWORD キーワードと一緒に使用され、パスワードの値が指定されていない場合に使用されます。この場合、ターゲット・ユーザーの DFLTGRP がパスワードとして使用されます。RACF のレベルによっては、このような **ADDUSER** コマンドによって PROTECTED ユーザーが定義される場合もあります。**ADDUSER** コマンドの場合、パスワードの値を設定せずに PASSWORD キーワードを使用することで、現行ポリシーの適用を強制できます。 114 ページの『ユーザー属性の必須値プロファイル』で説明したように、必須属性ポリシーを使用して PASSWORD キーワードを自動的に挿入することもできます。

現行ポリシーを適用する場合は、パスワードに値を自動的に割り当てることができます。APPLDATA の値 RANDOM を使用すると、パスワードのランダム値の挿入が Command Verifier に指示されます。生成されるパスワードの長さは必ず 8 文字であり、各文字は以下の使用可能なすべてのタイプから選択されます。

– デフォルトでは、パスワード文字は、大文字の英字、数字、および 3 つの国別文字 (@、#、$) から成るセットから選択されます。
– 大/小文字混合パスワードが使用可能である (SETROPTS PASSWORD(MIXEDCASE)) 場合は、小文字の英字も使用できます。
– 特殊文字が使用可能である (SETROPTS PASSWORD(SPECIALCHARS)) 場合は、「*RACF* セキュリティー管理者のガイド」に記載されている特殊文字も使用できます。

SETROPTS コマンドによって指定されるパスワード規則は、主にユーザーに各セットから文字を強制的に選択させたり、一般的な単語を使用させないようにしたりすることを目的としています。Command Verifier で生成されたパスワードは全くランダムです。そのため、パスワードが、文字の長さや選択を制限するパスワード規則に準拠することは保証されません。インストール済み環境がパスワード規則を定義しているか、新規パスワード出口を使用している場合、RACF は、NOEXPIRE オプションと組み合わせて使用されると、生成されたランダム・パスワードを受け入れない場合があります。すべての混合のパスワード規則に違反するランダム・パスワードの例は、$%QyaFXi です。これは数字がないためです。数字を強制すると、パスワードのブルート・フォース・アタックに必要な時間が約 8 倍節約されます。

ADDUSER または ALTUSER のコマンドで PASSWORD の値が指定された場合、/PASSWORD ポリシー・プロファイルは使用されません。

ポリシー・プロファイル内の修飾子 /PASSWORD を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: デフォルト値は提供されません。

READ
: 生成されたパスワード値がコマンドに挿入されます。パスワードは端末ユーザーには開示されません。

UPDATE
: 生成されたパスワード値がコマンドに挿入されます。端末ユーザーに対して、新しいパスワードを示すメッセージが発行されます。

CONTROL
: この制御は、端末ユーザーに対して実装されません。パスワードのデフォルト値は提供されません。RACF は、ターゲット・ユーザーの DFLTGRP をパスワードの新しい値として割り当てます。

以下の APPLDATA 値がサポートされます。

BLANK
: この値は、RACF のデフォルト処理を使用する必要があることを示すために使用されます。これによって、パスワード品質や保護ユーザーの作成などのその他のポリシーがトリガーされる可能性があります。

RANDOM
: zSecure Command Verifier は、パスワードのランダム値を生成します。生成されるパスワードの長さは必ず 8 文字であり、使用可能なすべてのタイプから文字を選択します。

Other この値はエラーと考える必要がありますが、処理は、APPLDATA に値が指定されなかったかのように続行されます。これによって、パスワード品質や保護ユーザーの作成などのその他のポリシーがトリガーされる可能性があります。

- **C4R.USER.PASSWORD.=RACUID**

このプロファイルは、ユーザーが **PASSWORD** コマンドを使用して、自分自身のパスワードを変更する権限を記述します。総称文字を使用して、ポリシー・プロファイル内の =RACUID 修飾子を表すことはできません。ここに示されているとおりの形式で存在している必要があります。

PASSWORD 修飾子の総称値を定義する際には注意してください。結果として得られたポリシー・プロファイルは、自分自身の非基本セグメントを変更する権限にも一致する可能性があるためです。非基本セグメントのポリシー・プロファイルについて詳しくは、 64 ページの『非基本セグメントの管理を制御するプロファイル』を参照してください。

以下のアクセス規則が適用されます。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: 端末ユーザーは、**PASSWORD** オペランドを指定することを許可されません。この設定は、ユーザーがログオン時にのみパスワードを変更できることを意味します。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、**PASSWORD** コマンドで **PASSWORD** オペランドを指定することを許可されます。

CONTROL
: この制御は、端末ユーザーに対して実装されません。

- **C4R.USER.PHRASE.***owner.userid*

  このポリシー・プロファイルは、**ADDUSER** コマンドまたは **ALTUSER** コマンドによるパスフレーズの設定を制御します。**PASSWORD** コマンドまたは **PHRASE** コマンドによる自分のパスフレーズの設定は、=RACUID プロファイルによって制御されます。

  コマンド内の PHRASE キーワードを使用しても PROTECTED ステータスに影響がない場合は、現行プロファイルが使用されます。 PHRASE キーワードの使用によってユーザーが保護されたり、保護ステータスが削除されたりする場合は、代わりに **C4R.USER.ATTR.PROTECTED** プロファイルが使用されます。詳細については、 116 ページの『ユーザー属性およびアクセス・レベルの説明』を参照してください。ここで説明するプロファイルは、通常の (NON-PROTECTED) ユーザーのパスフレーズを管理する権限を制御します。

  保護ステータスの変更には、以下のアクセス・レベルが使用されます。

  プロファイルが見つからない
  : この制御は実装されません。アクションは実行されません。

  NONE
  : 端末ユーザーは、**PHRASE** オペランドを指定することを許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、**ADDUSER** コマンドまたは **ALTUSER** コマンドで **PHRASE** オペランドを指定して、パスフレーズを設定することを許可されます。

  CONTROL
  : この制御は、端末ユーザーに対して実装されません。端末ユーザーは、**PHRASE** キーワードを指定することを許可されます。

- **C4R.USER.PHRASE.=RACUID**

このプロファイルは、ユーザーが **PASSWORD** コマンドまたは **PHRASE** コマンドを使用して、自分自身のパスフレーズを変更する権限を記述します。RACF は、**PASSWORD** コマンドまたは **PHRASE** コマンドによってパスフレーズを追加することを許可しません。既存のパスフレーズの値のみを変更できます。総称文字を使用して、ポリシー・プロファイル内の =RACUID 修飾子を表すことはできません。ここに示されているとおりの形式で存在している必要があります。

PHRASE 修飾子の総称値を定義する際には注意してください。結果として得られたポリシー・プロファイルは、自分自身の非基本セグメントを変更する権限にも一致する可能性があるためです。非基本セグメントのポリシー・プロファイルについて詳しくは、64 ページの『非基本セグメントの管理を制御するプロファイル』を参照してください。

以下のアクセス規則が適用されます。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: 端末ユーザーは、**PHRASE** オペランドを指定することを許可されません。この設定は、ユーザーがログオン時にのみ自己のパスフレーズを変更できることを意味します (この設定がアプリケーションでサポートされている場合)。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、**PASSWORD** コマンドまたは **PHRASE** コマンドで **PHRASE** オペランドを指定して、自己のパスフレーズを変更することを許可されます。

CONTROL
: この制御は、端末ユーザーに対して実装されません。

- **C4R.USER.PASSWORD.=DFLTGRP**

  このプロファイルは、**ADDUSER** および **ALTUSER** コマンドでパスワード値をブランクのままにすることができる権限を制御するために使用されます。パスワード値をブランクのままにすると、 RACF はユーザーの DFLTGRP を新規パスワードに使用します。PASSWORD を明示的に DFLTGRP に設定することは、このポリシーによっても制御されます。

  RACF のレベルによっては、**PASSWORD** コマンドは、INTERVAL キーワードを指定せずに別のユーザーについて発行された場合、パスワードをそのユーザーのデフォルト・グループにリセットします。このポリシー・プロファイルは、その形態の **PASSWORD** コマンドにも適用されます。

  ポリシー・プロファイル内の修飾子 =DFLTGRP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  上記の /PASSWORD ポリシーをアクティブにすると、このポリシーが回避されます。デフォルト値ポリシーを実装すると、パスワードの値が設定される結果にな

る場合があります。その場合、パスワード値はもはや DFLTGRP に一致せず、現行ポリシー・プロファイルは適用されません。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: 端末ユーザーは、パスワードの値を明示的に指定せずに **ADDUSER** コマンドを使用することを許可されません。**ALTUSER** コマンドで PASSWORD キーワードを使用して、値を指定しなかった場合も、コマンドは拒否されます。

READ
: 端末ユーザーは、ADDUSER コマンドでパスワード値をブランクのままにするまたは明示的に **DFLTGRP** を指定することを許可されます。**ALTUSER** コマンドでは、明示的な値を指定せずに PASSWORD キーワードを使用することは許可されません。

UPDATE
: 端末ユーザーは、ADDUSER コマンドと **ALTUSER** コマンドのどちらでも、パスワード値をブランクのままにするまたは明示的に **DFLTGRP** を指定することを許可されます。

CONTROL
: この制御は、端末ユーザーに対して実装されません。DFLTGRP と同等なパスワードは受け入れられます。

- **C4R.USER.PASSWORD.=USERID**

このプロファイルは、**ADDUSER**、**ALTUSER**、および**PASSWORD** コマンドで userid を新規パスワードの一部として指定する権限を制御するために使用されます。

ポリシー・プロファイル内の修飾子 =USERID を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: 端末ユーザーは、新規パスワードの値の一部として userid を使用することを許可されません。コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、パスワードの新しい値の一部としてユーザー ID を使用することを許可されます。

CONTROL
: この制御は、端末ユーザーに対して実装されません。ユーザー ID と同等なパスワードは受け入れられます。

- **C4R.USER.=PWINT.***owner.userid*

このポリシー・プロファイルを使用して、ユーザーのパスワードおよびフレーズのインターバルに特定の値を強制することができます。このポリシー・プロファ

イルによって定義されたインターバルは、端末ユーザーによって指定された値を指定変更するために使用されます。**PASSWORD** または **PHRASE** コマンドを INTERVAL キーワードなしで使用した場合、インターバルは変更されません。修飾子 =PWINT は、このポリシー・プロファイルがパスワード・インターバルにのみ適用されることを示しますが、RACF はパスワードとフレーズに同じインターバルを使用します。したがって、このポリシー・プロファイルは両方にも適用されます。

ポリシー・プロファイル内の修飾子 =PWINT を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: アクションは実行されません。必須値は強制されません。

READ
: **APPLDATA** フィールドが取り出されて、ユーザーの新規インターバルに使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対して実装されません。必須値は強制されません。

APPLDATA フィールドに指定できる値は、以下のとおりです。

BLANK
: この値は、RACF SETROPTS 値をデフォルトとして使用する必要があることを示すために使用されます。

interval
: *interval* は、先行ゼロを含む 3 桁の数字で指定する必要があります。この値は、必ず RACF SETROPTS 値以下にしてください。そうでない場合、結果としてのコマンドが失敗する可能性があります。

NEVER
: パスワード・インターバルは never に設定されます。この結果、パスワードおよびパスフレーズに有効期限がなくなります。この値を指定するために、RACF は追加権限を必要とします。端末ユーザーにその権限がない場合、コマンドは RACF によって拒否されます。

other この値はエラーです。RACF SETROPTS 値は、最大値として使用されます。

- **C4R.USER.PWINT.***owner.userid*

このプロファイルを使用して、パスワードおよびパスフレーズ・インターバルの最大値を制御できます。最適プロファイルでは、インターバルの最大値を APPLDATA によって指定する必要があります。*interval* は、先行ゼロを含む 3 桁の数字で指定する必要があります。端末ユーザーが指定した値は、APPLDATA で定義された値と比較されます。コマンド内の値がプロファイル内の値より大きい

場合、コマンドは拒否されます。端末ユーザーに CONTROL 権限がある場合、定義された最大値は無視されます。修飾子 PWINT は、このポリシー・プロファイルがパスワード・インターバルにのみ適用されることを示しますが、RACF はパスワードとフレーズに同じインターバルを使用します。したがって、このポリシー・プロファイルは両方にも適用されます。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: インターバルの変更は許可されません。端末ユーザーによって指定された値は、すべて拒否されます。

READ
: NONE と同じ。

UPDATE
: **APPLDATA** からの値が、インターバルの最大値として使用されます。端末ユーザーの指定した値が定義された値以下である場合、コマンドは受け入れられます。インターバルをシステム全体のデフォルトより大きく設定することはできません。

CONTROL
: この制御は、端末ユーザーに対して実装されません。端末ユーザーが指定した値は、すべて受け入れられます。

APPLDATA フィールドに指定できる値は、以下のとおりです。

BLANK
: この値は、RACF SETROPTS 値を最大値として使用する必要があることを示すために使用されます。

interval
: *interval* は、先行ゼロを含む 3 桁の数字で指定する必要があります。

NEVER
: インターバルを NEVER に設定できます。この結果、パスワードおよびパスフレーズに有効期限がなくなります。RACF は、この値に追加権限を必要とします。SETROPTS 値以下のインターバルを指定することもできます。

other
: この値はエラーです。RACF SETROPTS 値は、最大値として使用されます。

- **C4R.USER.PWEXP.***owner.userid*

このポリシー・プロファイルを使用して、**ALTUSER** コマンドでの EXPIRED および NOEXPIRED オプションの使用を制御できます。RACF は既に、NOEXPIRED オプションを、システム SPECIAL 属性を持つ端末ユーザーと、**IRR.PASSWORD.RESET** プロファイルに対する UPDATE 権限を持つユーザーに制限しています。現行のポリシー・プロファイルでは、ターゲット・ユーザーに対してさらに制限することができます。パスワードまたはフレーズに新たに値を設定せずに、パスワードまたはフレーズを期限切れにする権限も制御します。修飾子 PWEXP は、このポリシー・プロファイルがパスワードの有効期限にのみ適用されることを示しますが、フレーズにも適用されます。

以下のアクセス規則が適用されます。

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: 端末ユーザーは、ALTUSER コマンドで **EXPIRED** キーワードを使用して、現行のパスワードおよびフレーズを期限切れにすることを許可されません。パスワードまたはフレーズに新しい値が指定された場合、デフォルト値 EXPIRED が許可されます。パスワードまたはフレーズに新しい値を指定する場合、端末ユーザーは NOEXPIRED を指定することを許可されません。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、パスワードまたはフレーズに新しい値を指定せずに EXPIRED キーワードを使用することで、現行のパスワードおよびフレーズを期限切れにすることを許可されます。パスワードまたはフレーズに新しい値を指定する場合、端末ユーザーは NOEXPIRED のほかに EXPIRED を指定することを許可されます。このアクセス・レベルでは、パスワードおよびフレーズの通常のメンテナンスが許可されます。

CONTROL
: このポリシーは、端末ユーザーに対して実装されません。このアクセス・レベルでは、パスワードおよびフレーズの通常のメンテナンスが許可されます。

USER MFA データ管理用のポリシー・プロファイル

RACF は、いくつかの新機能によって多要素認証のサポートを実装しました。必要なデータの一部は USER プロファイルに追加する必要があります。

USER プロファイルでは、関連するデータは BASE セグメント内の複数の MFA 関連フィールドに保持されます。USER プロファイル内の MFA 固有フィールドの管理の制御には、以下のポリシー・プロファイルが使用されます。

表 *22. USER* プロファイル内の *MFA* 固有フィールドの管理を制御するポリシー・プロファイル

キーワード	値	プロファイル
(NO)PWFALLBACK	n/a	**C4R.USER.MFA.PWFALLBACK.***owner.userid*
(DEL)FACTOR	*factor-name*	**C4R.USER.MFA.FACTOR.ID.***factor-name.owner.userid*
(NO)ACTIVE	*factor-name*	**C4R.USER.MFA.FACTOR.ACTIVE.***factor-name*
TAG	*factor-name* *tag-name*	**C4R.USER.MFA.FACTOR.TAG.***factor-name.tag-name*
DELTAG	*factor-name* *tag-name*	**C4R.USER.MFA.FACTOR.TAG.***factor-name.tag-name*
NOTAGS	n/a	**C4R.USER.MFA.FACTOR.TAG.***factor-name*.+
ADDPOLICY DELPOLICY	*policy-name*	**C4R.USER.MFA.POLICY.***policy-name.owner.userid*

上記の表のプロファイルは、端末ユーザーが入力したキーワードと値の検証に使用できるポリシーを記述します。以下のリストに、これらのポリシーとサポートされているアクセス・レベルについての詳細を示します。

- **C4R.USER.MFA.PWFALLBACK.***owner.userid*

  このプロファイルでは、ユーザーの PWFALLBACK 属性を設定する権限が記述されます。PWFALLBACK 属性が使用されるのは、MFA サーバーが使用不可である場合や、アクティブな要素の妥当性を判別できない場合のログオン時です。以下のアクセス・レベルが使用されます。

  プロファイルが見つからない
  : この制御は実装されません。PWFALLBACK または NOPWFALLBACK 属性の設定の制御には、RACF 権限だけが使用されます。

  NONE
  : 端末ユーザーは、PWFALLBACK も NOPWFALLBACK も割り当てることを許可されません。コマンドはリジェクトされます。

  READ
  : 端末ユーザーは、NOPWFALLBACK を割り当てることを許可されます。これは ALTUSER コマンドのデフォルト値です。

  UPDATE
  : 端末ユーザーは、PWFALLBACK およびNOPWFALLBACK を割り当てることを許可されます。

  CONTROL
  : UPDATE と同じ。

- **C4R.USER.MFA.FACTOR.ID.***factor-name.owner.userid*

  このプロファイルでは、ユーザーの MFA 要素の追加、指定された MFA 要素のオプションの変更、または MFA 要素の削除を行う権限が記述されます。ACTIVE ステータスの設定または TAG リストの変更を行うためのキーワードは、指定された要素に適用されます。以下のアクセス・レベルが使用されます。

  プロファイルが見つからない
  : この制御は実装されません。指定された要素 *factor-name* の追加、変更、または削除の制御には、RACF 権限だけが使用されます。

  NONE
  : 端末ユーザーは、指定された要素 *factor-name* の追加、変更、および削除を行うことを許可されません。コマンドはリジェクトされます。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、指定された要素 *factor-name* の管理を許可されます。

  CONTROL
  : UPDATE と同じ。

- **C4R.USER.MFA.FACTOR.ACTIVE.***factor-name*

  このプロファイルでは、ユーザーの MFA 要素を活動化する権限が記述されます。このポリシー・プロファイルは、FACTOR.ID ポリシー・プロファイルと一

緒に使用されます。FACTOR.ID ポリシー・プロファイルは、特定のユーザーの FACTOR を管理するための権限を制御します。現行のポリシー・プロファイルは、要素の ACTIVE ステータスの使用を制御します。

プロファイルが見つからない
: この制御は実装されません。指定された要素のステータスの制御には、RACF 権限だけが使用されます。

NONE
: 端末ユーザーは、指定された要素 *factor-name* のステータスを変更することを許可されません。コマンドはリジェクトされます。また、端末ユーザーは、要素のステータスにデフォルト値 NOACTIVE を明示的に指定することも許可されません。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、指定された要素 *factor-name* の ACTIVE ステータスを変更することを許可されます。

CONTROL
: UPDATE と同じ。

- **C4R.USER.MFA.FACTOR.TAG.***factor-name.tag-name*

  このプロファイルでは、指定された要素の TAG を管理する権限が記述されます。このポリシー・プロファイルは、FACTOR.ID ポリシー・プロファイルと一緒に使用されます。FACTOR.ID ポリシー・プロファイルは、特定のユーザーの FACTOR を管理するための権限を制御します。現行のポリシー・プロファイルは、要素の TAG の管理を制御します。単一コマンド内で複数のタグを設定または削除する場合、端末ユーザーはすべてのタグに対する十分な権限を持つ必要があります。1 つ以上のタグに対する端末ユーザーの権限が不十分な場合、コマンド全体がリジェクトされます。NOTAGS キーワードの使用を指定するには、*tag-name* に特殊な値 + (正符号) を使用します。

  プロファイルが見つからない
  : この制御は実装されません。TAG の管理の制御には、RACF 権限だけが使用されます。

  NONE
  : 端末ユーザーは、要素 *factor-name* のタグ *tag-name* を管理することを許可されません。コマンドはリジェクトされます。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、要素 *factor-name* のタグ *tag-name* を管理することを許可されます。

  CONTROL
  : UPDATE と同じ。

- **C4R.USER.MFA.POLICY**.*policy-name.owner.userid*

このプロファイルでは、ユーザーの MFA ポリシーを追加または削除する権限が記述されます。以下のアクセス・レベルが使用されます。

プロファイルが見つからない
: この制御は実装されません。指定された *policy-name* の追加、変更、または削除の制御には、RACF 権限だけが使用されます。

NONE
: 端末ユーザーは、指定されたポリシー *policy-name* の追加と削除を許可されません。コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、指定されたポリシー *policy-name* の管理を許可されます。

CONTROL
: UPDATE と同じ。

その他のユーザー関連ポリシー・プロファイル

このユーザー関連の制御に関する最終セクションでは、残りの設定値について説明します。主に取り上げるのは、名前、インストール・データ、およびクラス権限 (CLAUTH) を設定するための制御です。

表 *23.* ユーザー設定に使用されるプロファイル： この表の項目は、**ADDUSER** および **ALTUSER** コマンドで指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDUSER **ALTUSER**	**ADD/DEL CATEGORY**	**C4R.USER.CATEGORY.***category.owner.userid*
ADDUSER **ALTUSER**	**(NO)CLAUTH**	**C4R.USER.CLAUTH.***class.owner.userid*
ADDUSER **ALTUSER**	**(NO)DATA**	**C4R.USER.INSTDATA.***owner.userid*
ADDUSER **ALTUSER**	**(NO)MODEL**	**C4R.USER.MODEL.***owner.userid*
ADDUSER **ALTUSER**	**NAME**	**C4R.USER.NAME.***owner.userid*
ADDUSER **ALTUSER**	**(NO)SECLABEL**	**C4R.USER.SECLABEL.***seclabel.owner.userid*
ADDUSER **ALTUSER**	**(NO)SECLEVEL**	**C4R.USER.SECLEVEL.***seclevel.owner.userid*
ADDUSER **ALTUSER**	**(NO)WHEN**	**C4R.USER.WHEN.***owner.userid*
ALTUSER	**PWCLEAN**	**C4R.USER.PWCLEAN.***owner.userid*
ALTUSER	**PWCONVERT**	**C4R.USER.PWCONVERT.***owner.userid*

以下の段落では、zSecure Command Verifier によってサポートされる残りのポリシー・プロファイルについて説明します。

現時点では、SECLABEL および SECLEVEL に対するサポートが限られています。これら 2 つの設定の割り当てを制御することはできますが、これらの設定の除去を制御することはできません。

- **C4R.USER.CATEGORY.***category.owner.userid*

  このプロファイルを使用して、セキュリティー・カテゴリーの割り当てを制御できます。通常、RACF 管理者は、自分自身の CATEGORY を自己の範囲内の別のユーザーに割り当てることができます。セキュリティー・カテゴリーは、リソースへのアクセスを防止する追加の方法として使用できます。ユーザーは、少なくともリソースに割り当てられたすべてのセキュリティー・カテゴリーを持っている必要があります。現行プロファイルを使用すると、ユーザーに対する CATEGORY の割り当てと削除を制御できます。

  プロファイルが見つからない
  : この制御は実装されません。*category* を割り当てられている管理者は、自分の範囲内のユーザーに対して、この CATEGORY の割り当てと除去を行うことができます。

  NONE
  : CATEGORY *category* のユーザー *userid* への割り当てと除去は許可されません。コマンドはリジェクトされます。この設定は、**ADDUSER** と **ALTUSER** コマンドの両方に適用されます。

  READ
  : システム SPECIAL ユーザーは、この userid に対して *category* の割り当てと除去を行うことができます。

  UPDATE
  : *category* を割り当てられている管理者は、自分の範囲内の他のユーザーに対してこの値を割り当てることができます。それらの管理者は、*category* を除去する権限も持ちます。

  CONTROL
  : この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.USER.CLAUTH.***class.owner.userid*

  このプロファイルを使用して、システム内のどのユーザーに、指定された一般リソース・クラス内に新規ユーザー ID およびプロファイルを定義する権限を与えることができるかを制御できます。通常、クラスの CLAUTH を持つユーザーは、自己の権限を他のユーザーに渡すことができます。現行プロファイルを使用して、これを防止することができます。このプロファイルに使用できるアクセス・レベルは以下のとおりです。

  プロファイルが見つからない
  : この制御は実装されません。CLAUTH を持つユーザーは、自己の権限を組織内の他のユーザーに渡すことができます。また、システム SPECIAL を持つユーザーも、すべてのクラスについての CLAUTH をすべてのユーザーに割り当てることができます。

  NONE
  : CLASS *class* の CLAUTH をユーザー *userid* に委任することは許可さ

れません。コマンドはリジェクトされます。この設定は、**ADDUSER** と **ALTUSER** コマンドの両方に適用されます。

READ
端末ユーザーは、自己の範囲内のユーザーから、 *class* の CLAUTH を削除できます。

UPDATE
CLASS *class* の CLAUTH を持つ端末ユーザーは、自己の権限をユーザー *userid* に渡すことができます。これは、標準の RACF 権限の方法です。

CONTROL
この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.USER.INSTDATA.***owner.userid*

このプロファイルは、ユーザーのインストール・データを変更する権限を制御するために使用されます。通常、この権限はプロファイルの所有者と **グループ** SPECIAL 権限を持つユーザーだけに既に制限されています。このプロファイルは、それ以外の制約事項を実装します。

INSTDATA ポリシー・プロファイルには、インストール・データに必要なフォーマットの参照を含めることもできます。フォーマットの名前は、最適ポリシー・プロファイルの APPLDATA によって指定できます。このフォーマットの名前を使用して、適切な一連のフォーマット指定ポリシー・プロファイルが決定されます。フォーマット指定ポリシー・プロファイル (または短形式プロファイル) では、以下のような名前が使用されます。

C4R.*class*.INSTDATA.=FMT.*format-name*.POS(*start*:*end*)

複数のフォーマット・プロファイルを使用して、RESOURCE プロファイルのインストール・データのさまざまな部分を指定できます。フォーマット・プロファイルについて詳しくは、 254 ページの『インストール・データ・フィールドのフォーマットの制約事項』を参照してください。

INSTDATA プロファイルに使用できるアクセス・レベルは以下のとおりです。

プロファイルが見つからない
この制御は実装されません。RACF 許可のあるすべてのユーザーが、それぞれの制御の範囲内でユーザーのインストール・データを変更できます。

NONE
インストール・データの指定は許可されません。コマンドはリジェクトされます。この設定は、**ADDUSER** と **ALTUSER** コマンドの両方に適用されます。

READ
ADDUSER コマンドでインストール・データを指定することは許可されます。その後に **ALTUSER** コマンドで値を変更することはできません。

UPDATE
インストール・データの変更が許可されます。

CONTROL
この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

APPLDATA で指定されるオプションの値を以下で説明します。

フォーマット名
userid のインストール・データに使用する必要があるフォーマットの名前。フォーマット名は、適切なフォーマット・プロファイル・セットを見つけるために使用されます。

- **C4R.USER.MODEL.***owner.userid*

モデル・データ・セット名は、この userid で始まる新規データ・セット・プロファイルが定義されたときに、RACF によって使用されます。新規データ・セット・プロファイルが定義された場合、指定されたモデル・データ・セット名の前に userid が付きます。RACF は、各ユーザーがモデル・プロファイルの名前を指定することを許可します。ユーザー・データ・セットのモデル化は、SETROPTS によって活動化されている場合にのみ使用されます。zSecure Command Verifier では、モデルとして使用する必要があるデータ・セット・プロファイルを選択する権限を制御することができます。 245 ページの『その他のポリシー・プロファイルとアクセス・レベルの説明』で説明している **C4R.***class.***TYPE.***type.profile* プロファイルを使用すると、MODEL データ・セット自体の定義を制御できます。

プロファイルが見つからない
この制御は実装されません。すべてのユーザーは、自分自身のモデル・データ・セットを選択できます。モデル・データ・セットは、MODEL(USER) が SETROPTS で活動化されている場合にのみ使用されます。

NONE
ユーザー MODEL データ・セット名の選択は許可されません。

READ
MODEL は、**ADDUSER** コマンドで指定できます。これを後から **ALTUSER** コマンドで変更することはできません。

UPDATE
MODEL の指定の設定、変更、および削除が許可されます。

CONTROL
この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.USER.NAME.***owner.userid*

このプロファイルを使用して、ユーザー ID の NAME (PGMRNAME と呼ばれることもあります) の変更を制御できます。このポリシーは主に、ユーザーが自分自身の **NAME** フィールドを変更できないようにするために適用されます。このプロファイルに使用できるアクセス・レベルは以下のとおりです。

プロファイルが見つからない
この制御は実装されません。すべてのユーザーは、自分自身の NAME

を変更できます。RACF 管理者およびユーザーは、自己の制御下にあるすべてのユーザー ID の NAME を変更できます。

NONE
NAME を指定することは許可されません。コマンドはリジェクトされます。この設定は、**ADDUSER** と **ALTUSER** コマンドの両方に適用されます。

READ
ADDUSER コマンドで NAME を指定することは許可されます。**ALTUSER** コマンドによって NAME を変更することは許可されません。

UPDATE
ユーザー ID の NAME の変更は受け入れられます。

CONTROL
この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.USER.SECLABEL.***seclabel.owner.userid*

このプロファイルを使用して、セキュリティー・ラベルの割り当てを制御できます。通常、RACF 管理者は、自分自身の SECLABEL を自己の範囲内の別のユーザーに割り当てることができます。このラベルは単にデフォルトのセキュリティー・ラベルです。ユーザーは LOGON プロセス中に、自己の SECLABEL を選択できます (定義された SECLABEL に対するアクセス権限を持っている場合)。

現時点では、zSecure Command Verifier に SECLABEL の完全な削除を制御するポリシー・プロファイルはありません。管理者は、自己の範囲内にいる任意のユーザーから、割り当てられたセキュリティー・ラベルを削除できます。

プロファイルが見つからない
この制御は実装されません。*seclabel* に対するアクセス権限を持つ管理者は、この値を範囲内のユーザーのデフォルト SECLABEL として割り当てることができます。

NONE
SECLABEL *seclabel* のユーザー *userid* への割り当ては、許可されません。コマンドはリジェクトされます。この設定は、**ADDUSER** と **ALTUSER** コマンドの両方に適用されます。

READ
システム SPECIAL ユーザーは、*seclabel* をこの userid に割り当てることができます。

UPDATE
seclabel に対するアクセス権限を持つ管理者は、この値を範囲内のユーザーのデフォルト SECLABEL として割り当てることができます。

CONTROL
この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.USER.SECLEVEL.***seclevel.owner.userid*

このプロファイルを使用して、セキュリティー・レベルの割り当てを制御できます。通常、RACF 管理者は、自分自身の SECLEVEL までの SECLEVEL を自分の範

囲内の別のユーザーに割り当てることができます。セキュリティー・レベルは、リソースへのアクセスを防止する追加の方法として使用できます。ユーザーのセキュリティー・レベルは、リソースに割り当てられているセキュリティー・レベルと同じかそれ以上でなければなりません。zSecure Command Verifier ポリシー・プロファイルを使用すると、ユーザーに対する SECLEVEL の割り当てを制御できます。検査プロセスでは、*seclevel* の正確な名前だけが使用されます。対応する数値は評価されません。また、より小さい値の別の *seclevel* の割り当ても、その特定の *seclevel* に対応する zSecure Command Verifier ポリシー・プロファイルによってのみ制御されます。

現時点では、zSecure Command Verifier に SECLEVEL の削除を制御するポリシー・プロファイルはありません。管理者は、自己の範囲内にいる任意のユーザーから、割り当てられたセキュリティー・レベルを削除できます。

プロファイルが見つからない
: この制御は実装されません。*seclevel* を割り当てられている管理者は、自己の範囲内のユーザーに対して、この SECLEVEL を割り当てることができます。

NONE
: SECLEVEL *seclevel* のユーザー *userid* への割り当ては、許可されません。コマンドはリジェクトされます。この設定は、**ADDUSER** と **ALTUSER** コマンドの両方に適用されます。

READ
: システム SPECIAL ユーザーは、*seclevel* をこの userid に割り当てることができます。

UPDATE
: *seclevel* を割り当てられている管理者は、自分の範囲内の他のユーザーに対してこの値を割り当てることができます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.USER.WHEN.***owner.userid*

この単一のポリシー・プロファイルは、ユーザー ID に対する WHEN(DAYS) および WHEN(TIME) 指定の両方の設定を制御します。これらの 2 つのオプションは、ユーザー ID がログオンできる曜日と時刻を制御します。このオプションは対話式作業にのみ適用され、しかも LOGON 自体の正確な時刻および曜日に対してのみ適用されます。

プロファイルが見つからない
: この制御は実装されません。WHEN(DAYS) および WHEN(TIME) を指定できます。

NONE
: LOGON 制約事項の指定は許可されません。

READ
: NONE と同じ。

UPDATE
LOGON 制約事項の指定と除去が許可されます。

CONTROL
この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.USER.PWCLEAN.***owner.userid*

このプロファイルを使用すると、ユーザーのパスワード・ヒストリーのクリーンアップを制御することができます。このポリシー・プロファイルには、以下のアクセス・レベルを使用できます。

プロファイルが見つからない
この制御は実装されません。システム SPECIAL ユーザーは、パスワードおよびパスフレーズのヒストリーをクリーンアップすることができます。

NONE
パスワードおよびパスフレーズのヒストリーをクリーンアップすることは許可されていません。

READ
NONE と同じ。

UPDATE
パスワードおよびパスフレーズのヒストリーをクリーンアップすることができます。RACF では引き続き、端末ユーザーがシステム SPECIAL 属性を持っていることが必要です。

CONTROL
この制御は、この端末ユーザーに対して実装されません。RACF では引き続き、端末ユーザーがシステム SPECIAL 属性を持っていることが必要です。

- **C4R.USER.PWCONVERT.***owner.userid*

このプロファイルを使用すると、ユーザーの現在のパスワードおよびヒストリー項目の変換を制御することができます。このポリシー・プロファイルには、以下のアクセス・レベルを使用できます。

プロファイルが見つからない
この制御は実装されません。任意のシステム SPECIAL ユーザーが、パスワードおよびパスフレーズのヒストリーを変換できます。

NONE
現在のパスワードおよびパスフレーズのヒストリーを変換することは許可されていません。

READ
NONE と同じ。

UPDATE
現在のパスワードおよびパスフレーズのヒストリーを変換することができます。RACF では引き続き、端末ユーザーがシステム SPECIAL 属性を持っていることが必要です。

CONTROL
この制御は、この端末ユーザーに対して実装されません。RACF では引き続き、端末ユーザーがシステム SPECIAL 属性を持っていることが必要です。

グループ管理のためのプロファイル

このセクションのトピックでは、グループ関連コマンドを管理するためのポリシー・プロファイルを実装する方法について説明します。

ユーザー ID 定義と同様に、グループ関連コマンド用にいくつかのプロファイルが使用されます。以下のセクションでは、それらのプロファイルについて説明します。わかりやすくするために、指定可能なすべてのキーワードと対応するプロファイルを、いくつかのカテゴリーに分けています。最初のセクションでは、グループの命名規則と、新規または既存のグループの RACF グループ階層内の場所を記述したプロファイルについて集中的に説明します。それ以後のセクションでは、ユーザーからグループへの接続とグループの属性について説明します。

グループの命名規則を実装したい場合は、『グループに命名規則を適用するプロファイル』のプロファイルを使用する必要があります。RACF 階層内の場所については、 145 ページの『RACF 階層での新規グループの配置』のプロファイルを適用できます。 164 ページの『グループ属性および権限のポリシー・プロファイル』では、グループ属性とその他のグループ関連の設定について説明します。

グループに命名規則を適用するプロファイル

グループの作成に関する制御を設定するためのポリシー・プロファイルを作成するには、以下のガイドラインに従ってください。

新規または既存のグループの名前と場所については、インストールでグループ自体に基づいた命名規則を使用できます。最初の表では、新規グループの名前を制御するプロファイルを要約しています。これらのプロファイルは、新規グループを作成する **ADDGROUP** コマンドにのみ適用されます。 147 ページの『SUPGRP の必須値およびデフォルト値ポリシー・プロファイル』および 155 ページの『OWNER の必須値およびデフォルト値ポリシー・プロファイル』では、上位グループおよび所有者の必須値とデフォルト値について説明します。最後の表では、端末ユーザーによって指定された値の検査に使用されるプロファイルについて説明します。

表 *24. RACF GROUP* の検査に使用されるプロファイル： この表の項目は、新規および削除されたグループの名前を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDGROUP	*groupname*	**C4R.GROUP.ID.=RACUID(n)**
ADDGROUP	*groupname*	**C4R.GROUP.ID.=RACGPID(n)**
ADDGROUP	*groupname*	**C4R.GROUP.ID.***group*
DELGROUP	*groupname*	**C4R.GROUP.DELETE.***group*

上記の表のプロファイルは、定義できる新規 GROUP を記述するために使用されます。GROUP 自体については、zSecure Command Verifier は新規グループの名前に基づいた制御を提供します。グループを変更する権限は、名前ベースの規則では

制御されません。この権限は、既に通常の RACF 範囲設定規則によって十分に制限されています。グループを削除する権限は、通常の RACF 所有権規則でも制御されますが、追加の制御が必要です。この権限は、別の名前ベースの規則によって実装されています。新規グループを定義するために、端末ユーザーは引き続き 1 つ以上のグループ関連権限 (JOIN、グループ SPECIAL、または直接所有権) を必要とします。

上記の *groupname* ベースの制御は、新規グループに命名規則を課します。この最初のプロファイル・セットは、新規に定義されるグループの名前を制御するために使用されます。これらのプロファイルは、どのグループを定義できるかを指定するためのものです。一般に、これらのプロファイルのうちの 1 つだけを使用して、命名規則を指定します。それ以外の、より限定的でない総称プロファイルは、指定した命名規則に従わない新規グループの定義をブロックするために使用する必要があります。その場合、より限定的な個別プロファイルまたは総称プロファイルの定義によって、例外を実装できます。これらのプロファイルの実装例を次に示します。

```
C4R.GROUP.ID.=RACGPID(4)       UACC(UPDATE)
C4R.GROUP.ID.TEST*             UACC(NONE) IBMUSER(UPDATE)
C4R.GROUP.ID.*                 UACC(NONE)
```

これらのプロファイルは、新規グループの最初の 4 文字が、そのグループを定義する端末ユーザーのいずれかのグループの最初の 4 文字と同じでない限り、新規グループを定義できないようにします。TEST で始まる GROUP について、例外が作成されます。これらのプロファイルは、ユーザー IBMUSER が定義できるほか、(最初のプロファイルに従って) TEST で始まるグループに接続されているすべてのユーザーも定義することができます。3 番目のプロファイルは、許可された命名規則の外部での新規グループの定義を停止するために必要です。3 番目のプロファイルがない場合は、最初または 2 番目のプロファイルによって明示的に、または一致するプロファイルがないことによって暗黙に、ほとんどすべての groupname が受け入れられます。

- **C4R.GROUP.ID.=RACUID(n)**

  新規グループの特殊な総称ポリシーを指定します。=RACUID は、端末ユーザーの userid を表しています。 substring(=RACUID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが使用されます。

  このプロファイルは個別ポリシー・プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  : 端末のユーザー ID は、新規グループの命名規則として使用されません。

  NONE
  : 新規 groupname は許可されません。コマンドは失敗します。

  READ
  : NONE と同じ。

UPDATE
新規 groupname は受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.GROUP.ID.=RACGPID(n)**

  新規 groupname の特殊な総称ポリシーを指定します。 =RACGPID は、端末ユーザーの接続先グループのリストを表します。「グループ・アクセス権限検査のリスト」の設定とは関係なく、そのユーザーのすべてのグループが使用されます。このプロファイルが使用されるのは、上記の `=RACUID(n)` プロファイルが存在しないか一致しない場合だけです。`substring(=RACGPID,1,n)` が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが `userid` の突き合わせに使用されます。

  このプロファイルは個別ポリシー・プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  端末ユーザーの現在のグループは、新規グループの命名規則として使用されません。

  NONE
  新規 groupname は許可されません。コマンドは失敗します。

  READ
  NONE と同じ。

  UPDATE
  新規グループは受け入れられます。

  CONTROL
  UPDATE と同じ。

- **C4R.GROUP.ID.*group***

  端末ユーザーによって作成できる新規グループを指定します。

  プロファイルが見つからない
  新規グループについて適用される命名規則はありません。

  NONE
  指定された groupname は許可されません。コマンドは失敗します。

  READ
  NONE と同じ。

  UPDATE
  指定されたグループは、作成が許可されます。

  CONTROL
  UPDATE と同じ。

既存のグループの削除

このトピックに記載した C4R.GROUP.DELETE プロファイルを使用して、既存のグループを削除するための権限を制御します。

グループ・プロファイルを削除する権限は、通常、何らかの形の所有権によって (直接に、またはグループ SPECIAL 属性の範囲内で) およびシステム SPECIAL 権限によって制御されます。一部の組織では、既存のグループを削除する権限について、厳格な制御を保持したいと考えています。その理由は、ほとんどの場合、そのような組織ではデータ・セットの保存や名前変更、あるいは非 RACF 情報との対話といった追加のプロシージャーを実装していることにあります。このセクションで説明しているポリシー・プロファイルは、グループ削除権限に対して追加の制約を課します。

グループの削除は、グループに対する =NOCHANGE ポリシーによっても制御できます。DELETE ポリシーによってグループの削除が許可されていても、=NOCHANGE ポリシー・プロファイルによってコマンドを拒否することができます。

- **C4R.GROUP.DELETE.***group*

  このプロファイルは、範囲内のどのグループ を削除できるかを制御するために使用されます。総称プロファイルの使用時は、グループの削除を完全に不可能にすることもできます。このプロファイルを介したアクセス権限がある端末ユーザーのみが、それらのグループを削除できます。この制御は、通常の削除権限を縮小します。

  そのグループの削除が、構文エラーまたは不十分な権限のために RACF によって既に拒否されている場合、このプロファイルは検査されません。

  以下のアクセス権限に関する規則がポリシー・プロファイルに適用されます。

  プロファイルが見つからない
  : この制御は実装されません。指定されたグループの削除に対する追加の制限はありません。

  NONE
  : そのグループを削除することはできません。コマンドはリジェクトされます。

  READ
  : そのグループを削除できるのは、端末ユーザーにシステム SPECIAL 属性がある場合だけです。

  UPDATE
  : そのグループを削除できます。

  CONTROL
  : UPDATE と同じ。

- **C4R.GROUP.DELETE.=UNIVERSAL**

  このプロファイルは、汎用グループの削除を制御するために使用されます。汎用グループには、グループに接続されている通常のユーザーのリストは含まれていません。このようなグループは未使用または空であるように見える場合がありますが、多くのユーザーがまだグループに接続されています。汎用グループを削除

する場合は、これらのユーザー・プロファイルを変更するために追加のステップが必要です。参照に関する問題が誤って発生しないように、汎用グループの削除を制限するポリシーを実装できます。ポリシー・プロファイルに対して十分なアクセス権限を持つ端末ユーザーのみが、汎用グループを削除することができます。システム SPECIAL ユーザーに必要なアクセス権限が READ である一方、通常のユーザーに必要なアクセス権限は UPDATE 以上です。

不十分な権限、あるいはグループが空でないためにグループの削除が RACF によって既に拒否されている場合、このポリシー・プロファイルは検査されません。グループが空でないと RACF が判別するのは、グループに接続済みユーザーが示される場合、または 1 つ以上のサブグループがある場合です。

以下のアクセス権限に関する規則がポリシー・プロファイルに適用されます。

プロファイルが見つからない
: この制御は実装されません。汎用グループの削除に追加の制限は適用されません。

NONE
: 汎用グループを削除できません。汎用グループを削除するための **DELGROUP** コマンドは拒否されます。

READ
: 汎用グループを削除できるのは、端末ユーザーにシステム SPECIAL 属性がある場合に限ります。汎用グループを削除するための **DELGROUP** コマンドは他のすべてのユーザーに対して拒否されます。

UPDATE
: 汎用グループを削除できます。

CONTROL
: UPDATE と同じ。

グループ・プロファイルに対するすべてのアクションの禁止

このトピックで説明している C4R.GROUP.=NOCHANGE.*owner.group* プロファイルは、グループに対するすべての変更またはアクションを禁止するために使用します。

前のセクションで説明したグループ・プロファイルの削除禁止に加えて、zSecure Command Verifier には、選択したグループまたは一定範囲のグループに対するすべてのアクションを完全に禁止するオプションも備わっています。これを実行するには、グループに対して `=NOCHANGE` ポリシー・プロファイルを定義します。`=NOCHANGE` ポリシー・プロファイルを定義すると、端末ユーザーが十分なアクセス権限を持っていない限り、以下の変更は禁止されます。

- グループの属性の変更。
- グループへのユーザーの接続またはグループからのユーザーの削除。
- グループの削除。
- グループの直接アクセスの付与または削除。
- グループでの DFLTGRP としての新規ユーザーの定義。

これらの変更は個々のポリシー・プロファイルによって制御することもできます。=NOCHANGE ポリシー・プロファイルの利点は、単一のポリシー・プロファイルを使用してグループに関連するすべてのアクションを制御できることです。=NOCHANGE ポリシー・プロファイルを使用して、グループの現在の定義を効果的にロックまたはフリーズすることができます。

ポリシー・プロファイル内の修飾子 =NOCHANGE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。グループのための =NOCHANGE ポリシー・プロファイルのフォーマットを以下に示します。

- **C4R.GROUP.=NOCHANGE.***owner.group*

  このプロファイルを使用して、リソースのアクセス制御リストに対するグループの変更、削除、追加、除去の禁止、および、グループに対するユーザーの接続および削除の禁止を確実に実施できます。ポリシー・プロファイルを定義すると、このプロファイルを通じてアクセス権限を与えられた端末ユーザーのみが、それらのグループを変更できます。サポートされているアクセス・レベルは以下のとおりです。

  プロファイルが見つからない
  : この制御は実装されません。ターゲット・グループの変更は禁止されません。

  NONE
  : 端末ユーザーには、ターゲット・グループに対するアクションの実行が許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : ターゲット・グループが端末ユーザーの通常の RACF 範囲内にあれば、端末ユーザーはターゲット・グループを変更できます。

  CONTROL
  : UPDATE と同じ。

RACF 階層での新規グループの配置

前出のプロファイルに従ってグループが作成されるときに、RACF グループ階層での新規グループの場所に対して、追加の規則が適用される場合があります。

zSecure Command Verifier には、この側面を制御するために 3 つのタイプのプロファイルが用意されています。必須値ポリシー・プロファイルは、新規グループに特定の OWNER および SUPGRP を強制します。デフォルト値プロファイルは、端末ユーザーが値を指定しなかった場合に値を提供し、最後のプロファイル・セットは、端末ユーザーが指定した値が受け入れ可能であるかどうかを検査します。以下のセクションでは、これらのプロファイルを一緒に使用する方法と、どの値が自動的に提供されるかについて説明します。zSecure Command Verifier ポリシー・プロファイルは、上位グループに省略形 SUPGRP を使用します。これは、省略形 SUPGROUP を使用する RACF コマンドと異なります。

必須値ポリシー・プロファイルの場合、3 番目の修飾子は、等号とそれに続くキーワードで構成されます。このため、SUPGRP の場合、プロファイルの修飾子は =SUPGRP です。表 25 で、必須値ポリシー・プロファイルを説明します。

表 *25. RACF GROUP* の場所に関連したコマンド/キーワードの必須値ポリシー・プロファイル： この表の項目は、新規グループの階層を記述するキーワードの必須値を反映しています。

コマンド	キーワード	プロファイル
ADDGROUP	*group*	**C4R.GROUP.=SUPGRP.***group*
ADDGROUP	*group*	**C4R.GROUP.=OWNER.***group*

表 26 では、端末ユーザーが RACF グループ階層内の場所を制御するキーワードを何も指定しなかった場合に使用されるデフォルト値プロファイルについて説明します。デフォルト・プロファイルの場合、3 番目の修飾子はスラッシュとそれに続くキーワードで構成されます。このため、SUPGRP の場合、プロファイルは /SUPGRP を持ちます。

表 *26. RACF GROUP* の場所に関連したコマンド/キーワードのデフォルト値に使用されるプロファイル： この表の項目は、新規グループの階層を記述するキーワードのデフォルト値を反映しています。

コマンド	キーワード	プロファイル
ADDGROUP	*group*	**C4R.GROUP./SUPGRP.***group*
ADDGROUP	*group*	**C4R.GROUP./OWNER.***group*

最後に、表 27 では、端末ユーザーが指定した値の受け入れ可能性を検査するために使用されるプロファイルを説明しています。次の表は、どのキーワードまたは機能に、どのプロファイルが使用されるかを要約したものです。

表 *27. RACF GROUP* の検査に使用されるプロファイル： この表の項目は、新規または変更されたグループの名前と場所を記述するために端末ユーザーによって指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDGROUP **ALTGROUP**	**SUPGRP**	**C4R.GROUP.SUPGRP.=RACUID(n)**
ADDGROUP **ALTGROUP**	**SUPGRP**	**C4R.GROUP.SUPGRP.=RACGPID(n)**
ADDGROUP **ALTGROUP**	**SUPGRP**	**C4R.GROUP.SUPGRP.=GROUP(n)**
ADDGROUP **ALTGROUP**	**SUPGRP**	**C4R.GROUP.SUPGRP.***supgrp.group*
ADDGROUP **ALTGROUP**	**SUPGRP**	**C4R.GROUP.SUPGRP./SCOPE.***supgrp.group*
ADDGROUP **ALTGROUP**	**SUPGRP**	**C4R.GROUP.SUPGRP./OWNER.***supgrp.group*
ADDGROUP **ALTGROUP**	**OWNER**	**C4R.GROUP.OWNER.=RACUID(n)**
ADDGROUP **ALTGROUP**	**OWNER**	**C4R.GROUP.OWNER.=RACGPID(n)**
ADDGROUP **ALTGROUP**	**OWNER**	**C4R.GROUP.OWNER.=GROUP(n)**

表 27. *RACF GROUP* の検査に使用されるプロファイル (続き): この表の項目は、新規または変更されたグループの名前と場所を記述するために端末ユーザーによって指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDGROUP **ALTGROUP**	**OWNER**	**C4R.GROUP.OWNER.***owner.group*
ADDGROUP **ALTGROUP**	**OWNER**	**C4R.GROUP.OWNER./SCOPE.***owner.group*
ADDGROUP **ALTGROUP**	**OWNER**	**C4R.GROUP.OWNER./GROUP.***owner.group*
ADDGROUP **ALTGROUP**	**OWNER**	**C4R.GROUP.OWNER./SUPGRP.***owner.group*

上位グループ (SUPGRP) 用のポリシー・プロファイル

新規グループの名前を除いて、その他の重要な 2 つの側面は RACF 階層内の場所 (= OWNER) と上位グループです。

標準 RACF では、端末ユーザーがそのグループ内で JOIN 権限を持っているか、そのグループがグループ SPECIAL 属性の範囲内にあるか、端末ユーザーがそのグループを所有している必要があります。さらに、所有者が RACF GROUP である場合、そのグループは、SUPGRP と同じものであることが必要です。zSecure Command Verifier では、上位グループに対するいくつかの追加の制御が実装されています。以降のセクションでは、 145 ページの『RACF 階層での新規グループの配置』の表にリストされているプロファイルの使用方法について説明します。

SUPGRP の必須値およびデフォルト値ポリシー・プロファイル

最初のプロファイル・セットは、ADDGROUP コマンド用のグループの上位グループ (**SUPGRP**) を制御します。この最初のセットは必須値またはデフォルト値を指定するので、**ALTGROUP** コマンドには使用されません。

- **C4R.GROUP.=SUPGRP.***group*

  このプロファイルは、新規に定義されたすべてのグループの SUPGRP について、必須値を指定するために使用されます。これは、**ADDGROUP** コマンドにのみ使用されます。使用される上位グループは、プロファイルの **APPLDATA** フィールドから取得されます。これは、端末ユーザーが指定した値を指定変更するために使用されるか、端末ユーザーが値を指定しなかった場合は、コマンドに追加されます。この必須値プロファイルによって取得された SUPGRP 値は、追加の SUPGRP 関連ポリシー・プロファイルの支配を受けません。

  値 *group* は、影響を受けるグループを表します。この設定は、一般規則への例外の指定を可能にします。最も限定的なプロファイルだけが zSecure Command Verifier によって使用されます。

  ポリシー・プロファイル内の修飾子 =SUPGRP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。必須値は強制されません。

NONE
この制御は、端末ユーザーに対してアクティブにはされません。必須値は強制されません。

READ
APPLDATA フィールドが抽出され、コマンドで使用されます。このプロセスで有効なグループが生成されない場合、端末ユーザーの現行接続グループが代用されます。

UPDATE
READ と同じ。

CONTROL
この制御は、端末ユーザーに対してアクティブにはされません。必須値は強制されません。端末ユーザーが GROUP に値を指定した場合は、それが使用されます。値が指定されていなければ、端末ユーザーの現在のグループが RACF によって使用されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値ポリシー・プロファイルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

APPLDATA フィールドで受け入れられる値は、以下のとおりです。端末ユーザーには、新規グループを定義するための十分な権限がこのグループ内で引き続き必要です。この権限は、zSecure Command Verifier では検査されません。権限が不十分であると、RACF によってコマンドが失敗する場合があります。

BLANK
この値は、RACF のデフォルト処理を使用する必要があることを示すために使用されます。RACF は、端末ユーザーの現在のグループを使用します。

userid この項目は、無効な項目です。これは端末ユーザーによる誤入力が原因ではないため、コマンドは端末ユーザーの現在のグループを使用して続行することができます。

group この *group* が挿入されます。このグループに対する端末ユーザーの権限が不十分な場合、コマンドは RACF によってリジェクトされます。

=OWNER
コマンドの OWNER キーワードによって指定された (またはデフォルトとして指定された) OWNER を反映します。この値は、zSecure Command Verifier によって挿入された OWNER 値である場合もあります。OWNER が特殊値 `=SUPGRP` (上位グループ) へと解決された場合、コマンドはリジェクトされます。

=MYOWNER
端末ユーザーの OWNER を反映します。この値は `GROUP` である必要があります。それ以外のすべての状態は、エラーと見なされます。この状況は端末ユーザーによる誤入力が原因ではないため、コマンドは端末ユーザーの現在の GROUP を使用して続行することができます。

=GROUP(n)

新規 GROUP 自体の最初の *n* 文字を反映します。この値は GROUP である必要があります。その他の状態はエラーとしてみなされ、端末ユーザーの現在の GROUP が代わりに使用されます。

=RACGPID

C4R.GROUP.ID.=RACGPID(n) の =RACGPID(*n*) による GROUP の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、**APPLDATA** 値 =RACGPID はエラーと見なされ、端末ユーザーの現在の GROUP が代わりに使用されます。

- **C4R.GROUP./SUPGRP.***group*

このプロファイルは、端末ユーザーが ADDGROUP コマンドで SUPGRP を指定しなかった場合に、**SUPGRP** のデフォルト値を指定するために使用されます。デフォルトとして使用される SUPGRP は、プロファイルの **APPLDATA** フィールドから取得されます。この必須値プロファイルによって取得された SUPGRP 値は、追加の SUPGRP 関連ポリシー・プロファイルの影響を受けません。上記の SUPGRP プロファイルを使用して値が指定された場合、/SUPGRP プロファイルは使用されません。

ポリシー・プロファイル内の修飾子 /SUPGRP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない

この制御は実装されません。デフォルト値は提供されません。

NONE

アクションは実行されません。デフォルト値は提供されません。RACF は、SUPGRP の値を提供しません。コマンドはリジェクトされます。このアクセス・レベルをインストールで使用して、端末ユーザーに SUPGRP の値を明示的に指定するよう強制できます。

READ

APPLDATA フィールドが抽出され、コマンドで使用されます。

UPDATE

READ と同じ。

CONTROL

この制御は、端末ユーザーに対してアクティブにはされません。デフォルト値は提供されません。端末ユーザーの現在のグループが RACF によって使用されます。

APPLDATA フィールドで受け入れられる値は、以下のとおりです。端末ユーザーには、新規 GROUP を定義するための十分な権限がこの GROUP 内で必要です。権限が不十分であると、コマンドが失敗する場合があります。

BLANK

この値は、RACF のデフォルト処理を使用する必要があることを示すために使用されます。端末ユーザーの現在の GROUP が使用されます。

userid この項目は、無効な項目です。これは端末ユーザーによる誤入力が原因ではないため、コマンドは端末ユーザーの現在の GROUP を使用して続行することができます。

group *group* が挿入されます。

=OWNER
コマンドの OWNER キーワードによって指定された (またはデフォルトとして指定された) OWNER を反映します。この値は、zSecure Command Verifier によって挿入された OWNER 値である場合もあります。OWNER が特殊値 =SUPGRP (上位グループを示します) へと解決された場合、コマンドはリジェクトされます。

=MYOWNER
端末ユーザーの OWNER を反映します。この値は GROUP である必要があります。それ以外のすべての状態は、エラーと見なされます。これは端末ユーザーによる誤入力が原因ではないため、コマンドは端末ユーザーの現在の GROUP を使用して続行することができます。

=GROUP(n)
新規 GROUP 自体の最初の *n* 文字を反映します。この値は GROUP である必要があります。その他の状態はエラーとしてみなされ、端末ユーザーの現在の GROUP が代わりに使用されます。

=RACGPID
C4R.GROUP.ID.=RACGPID(n) の =RACGPID(*n*) による GROUP の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、APPLDATA 値 =RACGPID はエラーと見なされ、端末ユーザーの現在の GROUP が代わりに使用されます。

指定された上位グループの検査

新規 GROUP の上位グループの選択、および既存グループの上位グループの変更を制御するには、以下のプロファイルを使用します。

以下のプロファイルは、端末ユーザーによる上位グループの指定を検査するために使用されます。

- **C4R.GROUP.SUPGRP.=RACUID(*n*)**

  ADDGROUP および **ALTGROUP** コマンド内の **SUPGRP** に対する特殊な総称ポリシーを指定します。=RACUID は端末のユーザー ID を表しています。substring(=RACUID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが SUPGRP とユーザー ID の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  端末のユーザー ID は、SUPGRP の命名規則または制限として使用されません。

NONE
指定された SUPGRP は許可されません。この決定は、以下に述べるプロファイル *supgrp.group* に対する権限によって却下することができます。

READ
NONE と同じ。

UPDATE
指定された SUPGRP は受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.GROUP.SUPGRP.=RACGPID(*n*)**

  ADDGROUP および **ALTGROUP** コマンド内の **SUPGRP** に対する特殊な総称ポリシーを指定します。=RACGPID は、端末ユーザーの接続先グループのリストを表します。「グループ・アクセス権限検査のリスト」の設定とは関係なく、そのユーザーのすべてのグループが使用されます。このプロファイルが使用されるのは、上記の =RACUID(*n*) プロファイルが存在しないか一致しない場合だけです。substring(=RACGPID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが userid の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  端末ユーザーの現在のグループは、SUPGRP の命名規則または制限として使用されません。

  NONE
  指定された SUPGRP は許可されません。この決定は、以下に述べるプロファイル *supgrp.group* に対する権限によって却下することができます。

  READ
  NONE と同じ。

  UPDATE
  指定された SUPGRP は受け入れられます。

  CONTROL
  UPDATE と同じ。

- **C4R.GROUP.SUPGRP.=GROUP(*n*)**

  ADDGROUP および **ALTGROUP** コマンド内の **SUPGRP** に対する特殊な総称ポリシーを指定します。=GROUP は、定義または変更されるグループを表します。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが、SUPGRP とターゲット GROUP の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用

することはできません。このプロファイルが使用されるのは、=RACUID(*n*) および =RACGPID(*n*) が存在しないか一致しない場合だけです。

プロファイルが見つからない
: GROUP の最初の *n* 文字は、userid の SUPGRP に対する制限として使用されません。

NONE
: 指定された SUPGRP は許可されません。この決定は、以下に述べるプロファイル *supgrp.group* に対する権限によって却下することができます。

READ
: NONE と同じ。

UPDATE
: 指定された SUPGRP は受け入れられます。

CONTROL
: UPDATE と同じ。

上記の 3 つのプロファイルのいずれかが、選択された SUPGRP を許可する場合、次のプロファイルはスキップされます。引き続き、/SCOPE ポリシーと /OWNER ポリシーで処理が進められます。上記のプロファイルが特定の SUPGRP の使用を認可しなかった場合、次のプロファイルが代替の許可方式として使用されます。

- **C4R.GROUP.SUPGRP.***supgrp.group*

  このプロファイルは、前に定義した 3 つの規則とは関係なく使用されます。これを使用して、総称名ベースのポリシーに対する例外を指定できます。これは、*group* を新規グループの SUPGRP として使用できるかどうかを制御します。既存のグループの場合、これはどの GROUP が新規 SUPGRP になることができるかを指定します。

  ほとんどの状態では、総称から *group* を指定します。明示的なプロファイルを使用して、特定のグループの例外を定義できます。

  このプロファイルは、前のいずれかのプロファイルが既にコマンドの続行を許可している場合には、使用されません。

  プロファイルが見つからない
  : この制御は実装されません。名前ベースのポリシーは適用されません。

  NONE
  : コマンドはリジェクトされます。

  READ
  : NONE と同じ。

  UPDATE
  : groupname を使用できます。

  CONTROL
  : UPDATE と同じ。

上位グループ用の追加のポリシー・プロファイル

以下のプロファイルは、SUPGRP についての一般的な制約事項を定義するために使用されます。

最初のプロファイルは、上位グループをグループ SPECIAL 属性の範囲内だけに制限します。これは、事実上、join 権限と GROUP の直接所有権を、新規 GROUP の作成を許可する手段としては無効にします。通常のユーザーはグループ Special を持たないことが普通なので、SUPGRP に対するすべての変更は、それらのユーザーの範囲外と見なされます。

2 番目のプロファイルは、SUPGRP をグループの OWNER と比較します。これは、突き合わせを実施するために使用できますが、この総称規則に対する例外を許可することもできます。RACF 自体は既に、OWNER が GROUP である場合、それが SUPGRP と同じものでなければならないことを強制します。

- **C4R.GROUP.SUPGRP./SCOPE.***supgrp.group*

  このプロファイルは、新規および既存のグループの上位グループが、グループ SPECIAL の範囲内に存在しなければならないことを指定するために使用されます。このプロファイルの主な目的は、分散管理者が SUPGRP を自身の制御しないグループに変更できないようにすることです。

  変数 *supgrp* および *group* は、影響を受けるグループと、グループの指定された (=new) SUPGRP を表します。この設定は、一般規則への例外の指定が可能になります。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

  ポリシー・プロファイル内の修飾子 /SCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  グループ SPECIAL またはシステム SPECIAL を持つ端末ユーザーが、新規上位グループに対して自己の管理権限を使用すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

  – **C4R.USESCOPE.***group*

  このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、このグループの新規上位グループに対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

  /SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : **ADDGROUP** と **ALTGROUP** のどちらのコマンドでも、端末ユーザーの範囲内にある GROUP だけを SUPGRP として指定できます。それ以外の GROUP が指定された場合、コマンドは拒否されます。

READ
NONE と同じ。

UPDATE
ADDGROUP と **ALTGROUP** のどちらのコマンドでも、端末ユーザーの範囲外にある GROUP を使用できます。端末ユーザーが、指定された GROUP 内で十分な権限を持っていない場合、コマンドは RACF によって拒否されます。

CONTROL
このポリシーは、端末ユーザーには効果がありません。

- **C4R.GROUP.SUPGRP./OWNER.***supgrp.group*

このプロファイルは、新規および既存のグループの上位グループが、グループの OWNER と同じでなければならないことを指定するために使用されます。端末ユーザーは、OWNER 以外を SUPGRP の値として指定するためには、このプロファイルに対するアクセス権限が必要です。

OWNER が同じ **ALTGROUP** コマンド内で同時に変更される場合、新規 SUPGRP は、新規 OWNER と突き合わせて検査されます。

新規グループの場合は、前に述べた必須値ポリシー・プロファイル **C4R.GROUP.=SUPGRP.***supgrp.group* の使用をお勧めします。この必須値ポリシー・プロファイルは、端末ユーザーによって指定されたすべての値にオーバーレイします。現行の SUPGRP./OWNER プロファイルは、端末ユーザーが正しい値を指定することを必要とします。必須値プロファイルを使用した場合、現行プロファイルはスキップされます。現行プロファイルの主な目的は、特定の GROUP が SUPGRP=OWNER 要件を免除されるようにすることです。

変数 *supgrp* および *group* は、影響を受ける userid と、グループの指定された (=new) SUPGRP を表します。この設定によって、一般規則の例外を指定できるようになります。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
この制御は実装されません。

NONE
GROUP の SUPGRP は、GROUP の OWNER と同じでなければなりません。

READ
NONE と同じ。

UPDATE
端末ユーザーは、グループの現在の (または新規の) OWNER と異なる SUPGRP の値を指定することを許可されます。

CONTROL
このポリシーは、端末ユーザーには効果がありません。

グループ所有者のポリシー・プロファイル

新規に定義された GROUP を記述するその他の情報部分は、OWNER です。

以下のプロファイルは、**ADDGROUP** と **ALTGROUP** の両方のコマンドに適用されます。一般に、これらのプロファイルの処理では、インストールのポリシーが GROUP を所有者として使用することが想定されています。プロファイル /GROUP は、インストール済み環境でそのようなポリシーの適用が必要かどうかを表すために使用できる制御を提供します。

以下の説明は、いくつかのプロファイル・セットに分割されています。最初のセットは、OWNER の必須値またはデフォルト値を指定するために使用されます。2 番目のプロファイル・セットは、OWNER について指定された値に対する制御を記述するために使用されます。最後の 3 つのプロファイルからなるセットでは、GROUP の OWNER に使用できる一般的なポリシーを記述します。

OWNER の必須値およびデフォルト値ポリシー・プロファイル

このトピックで説明するプロファイルは、新規 GROUP の OWNER に対する必須値ポリシー・プロファイルとデフォルト値ポリシー・プロファイルを指定します。これらのプロファイルは、**ADDGROUP** コマンドにのみ使用されます。

- **C4R.GROUP.=OWNER.***group*

  このプロファイルは、新規に定義されたグループ・プロファイルの OWNER の必須 (優先) 値を指定するために使用されます。これは、**ADDGROUP** 処理のときにだけ使用されます。この必須値プロファイルによって取得された OWNER 値は、追加の OWNER 関連ポリシー・プロファイルの影響を受けません。

  ポリシー・プロファイル内の修飾子 =OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。必須値は強制されません。

  NONE
  : アクションは実行されません。必須値は強制されません。

  READ
  : **APPLDATA** フィールドが抽出され、コマンドで使用されます。プロセスで生成される ID が有効でない、つまり存在しない項目である場合は、端末ユーザーの現在のグループが代わりに使用されます。

  UPDATE
  : READ と同じ。

  CONTROL
  : この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーによって指定された OWNER の値が、コマンド内で使用されます。

  注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値プロファ

イルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

APPLDATA フィールドで受け入れられる値は、以下のとおりです。所有者はユーザーまたはグループです。

BLANK
zSecure Command Verifier は、RACF のデフォルト (端末ユーザー) を OWNER の明示的な値として挿入します。

userid 検出されたユーザー ID が OWNER として挿入されます。

group 指定された GROUP が、新規グループの OWNER として使用されます。

=SUPGRP
コマンドで指定された (またはデフォルトとして指定された) 上位グループ (SUPGRP) を反映します。この値が特殊値 =OWNER (新規プロファイルの OWNER) へと解決された場合、コマンドは失敗します。

=MYOWNER
端末ユーザーの OWNER が所有者の値として挿入されます。

=GROUP(n)
新規 GROUP 自体の最初の *n* 文字を反映します。この値は GROUP の有効なユーザー ID でなければなりません。その他の状態はエラーとしてみなされ、端末ユーザーの現在の GROUP が代わりに使用されます。

=RACGPID
C4R.GROUP.ID.=RACGPID(n) の =RACGPID(*n*) による GROUP の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、**APPLDATA** 値 =RACGPID はエラーと見なされ、端末ユーザーの現在の GROUP が代わりに使用されます。

- **C4R.GROUP./OWNER.***group*

このプロファイルは、新規に定義されたグループ・プロファイルの OWNER のデフォルト値を指定するために使用されます。これは、**ADDGROUP** 処理のときにだけ使用されます。デフォルト値として使用される OWNER は、プロファイルの **APPLDATA** フィールドから取得されます。このデフォルト値プロファイルによって取得された OWNER 値は、追加の OWNER 関連ポリシー・プロファイルの支配を受けません。上記の =OWNER プロファイルを使用して値が指定された場合、/OWNER プロファイルは使用されません。

ポリシー・プロファイル内の修飾子 /OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
この制御は実装されません。デフォルト値は提供されません。この設定では、RACF から OWNER (端末ユーザー自身) のデフォルトが提供されます。

NONE
デフォルト値は提供されません。RACF は、OWNER の値を提供しませ

ん。コマンドはリジェクトされます。このアクセス・レベルを使用すると、インストールで端末ユーザーに OWNER の値を明示的に指定するよう強制できます。

READ
APPLDATA フィールドが抽出され、コマンドで使用されます。プロセスで生成される ID が有効でない、つまり存在しない項目である場合は、端末ユーザーの現在のグループが代わりに使用されます。

UPDATE
READ と同じ。

CONTROL
この制御は、端末ユーザーに対してアクティブにはされません。デフォルト値は提供されません。端末ユーザーが OWNER の値を指定しなかったため、RACF は端末ユーザーを新規プロファイルの OWNER にします。

APPLDATA フィールドで受け入れられる値は、以下のとおりです。ユーザー ID または GROUP を OWNER として指定できます。

BLANK
zSecure Command Verifier によって、RACF のデフォルトの端末ユーザーが OWNER の明示的な値として挿入されます。

userid 検出されたユーザー ID が OWNER として挿入されます。

group 指定された GROUP が、新規 GROUP の OWNER として使用されます。

=SUPGRP
コマンドで指定されたまたはデフォルト設定された上位グループ DFLTGRP を表します。この値が特殊値 =OWNER (新規プロファイルの OWNER) へと解決された場合、コマンドはリジェクトされます。詳しくは、前出の =SUPGRP の説明を参照してください。

=MYOWNER
端末ユーザーの OWNER が所有者の値として挿入されます。

=GROUP(n)
新規 GROUP 自体の最初の *n* 文字を反映します。この値は GROUP である必要があります。その他の状態はエラーとしてみなされ、端末ユーザーの現在の GROUP が代わりに使用されます。

=RACGPID
C4R.GROUP.ID.=RACGPID(n) の =RACGPID(*n*) による GROUP の定義を許可するために使用された GROUP を反映します。この値が使用されるのは、定義を許可するために =RACGPID(*n*) が使用された場合だけです。それ以外のすべての状態では、**APPLDATA** 値 =RACGPID はエラーと見なされ、端末ユーザーの現在のグループが代わりに使用されます。

指定されたグループ所有者の検査

ADDGROUP コマンドまたは **ALTGROUP** コマンドで新規所有者が指定された場合にグループ所有者を検査するには、以下のポリシー・プロファイルを使用します。

RACF は、所有者が GROUP である場合に限り、所有者を制限します。その場合、所有者は SUPGRP と同一でなければなりません。新規所有者がユーザー ID である場

合、RACF はどのような制限も課しません。このプロファイル・セットを使用して、新規 OWNER の選択を制限できます。指定した OWNER の使用が 3 つの一般ポリシー・ルールのどれにも受け入れられない場合は、明示的なプロファイルが使用されます。

- **C4R.GROUP.OWNER.=RACUID(*n*)**

  ADDGROUP および **ALTGROUP** コマンド内の **OWNER** に対する特殊な総称ポリシーを指定します。=RACUID は端末のユーザー ID を表しています。substring(=RACUID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけがユーザー ID と OWNER の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  : 端末ユーザーの userid は、OWNER の命名規則または制限として使用されません。

  NONE
  : 指定された OWNER は許可されません。この決定は、以下に述べるプロファイル *owner.group* に対する権限によって、却下することができます。

  READ
  : NONE と同じ。

  UPDATE
  : 指定された OWNER は受け入れられます。

  CONTROL
  : UPDATE と同じ。

- **C4R.GROUP.OWNER.=RACGPID(*n*)**

  ADDUSER および **ALTUSER** コマンド内の **OWNER** に対する特殊な総称ポリシーを指定します。 =RACGPID は、端末ユーザーの接続先グループのリストを表します。「グループ・アクセス権限検査のリスト」の設定とは関係なく、そのユーザーのすべてのグループが使用されます。このプロファイルが使用されるのは、上記の =RACUID(*n*) プロファイルが存在しないか一致しない場合だけです。substring(=RACGPID,1,*n*) が一致した場合、*n* の値とは関係なく、記載された他のプロファイルに優先してこのプロファイルが使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが OWNER の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  プロファイルが見つからない
  : 端末ユーザーの現在のグループは、OWNER の命名規則または制限として使用されません。

NONE
指定された OWNER は許可されません。この決定は、以下に述べるプロファイル *owner.group* に対する権限によって、却下することができます。

READ
NONE と同じ。

UPDATE
指定された OWNER は受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.GROUP.OWNER.=GROUP(*n*)**

このプロファイルは、ADDGROUP および **ALTGROUP** コマンド内で、**OWNER** の特殊な総称ポリシーを指定します。=GROUP は、グループ自体を表します。これらのプロファイルを複数定義した場合は、*n* の値が最も小さいプロファイルだけが使用されます。このプロファイルが使用されるのは、=RACUID(*n*) および =RACGPID(*n*) が存在しないか一致しない場合だけです。

このプロファイルは個別ポリシー・プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

指定された OWNER が受け入れられると、一般ポリシー (/SCOPE や /GROUP など) に対する追加の検査が実行されます。

特殊値 =GROUP は、影響を受けるユーザー・プロファイル自体を表します。このプロファイルは、GROUP の最初の *n* 文字が、その OWNER の最初の *n* 文字に一致しなければならないことを述べた命名規則を適用するために使用できます。

プロファイルが見つからない
ターゲット GROUP 自体は、OWNER の命名規則または制限として使用されません。

NONE
指定された OWNER は許可されません。この決定は、プロファイル *owner.group* に対する権限によって、却下することができます。

READ
NONE と同じ。

UPDATE
指定された OWNER は受け入れられます。

CONTROL
UPDATE と同じ。

上記の 3 つのプロファイルのいずれかが、指定された OWNER を許可する場合、次のプロファイル規則はスキップされます。処理は、以下で説明する /SCOPE、/GROUP、および /SUPGRP ポリシーを使用して続行されます。上記の 3 つのプロファイルが特定の OWNER の使用を認可しなかった場合、次のプロファイルが代替の許可方式として使用されます。

- **C4R.GROUP.OWNER.***owner.group*

この制御の主な目的は、前述の一般的なグループ・ベースのポリシーがどれも適用されない場合にポリシーを指定することです。変数 *owner* は、*group* の新規 OWNER を表します。この設定は、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

このポリシー・プロファイルで検査された OWNER には、さらにポリシー /SCOPE、/GROUP、/SUPGRP が適用されます。

プロファイルが見つからない
: この制御は実装されません。

NONE
: コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 指定された OWNER は受け入れられます。

CONTROL
: UPDATE と同じ。

グループ所有者用の追加のポリシー・プロファイル

命名規則を適用するためのプロファイルのほかに、既存の RACF グループ階層に基づいたポリシーを実装することもできます。以下のプロファイルを使用すると、新規 OWNER の一般的な規則を指定できます。より限定的なプロファイル、または完全修飾プロファイルを使用することにより、一部のユーザー ID または GROUP にそのような制限を免除することを指定できます。

以下の 3 つのプロファイル規則は、追加の OWNER ポリシー・セットとして使用されます。指定した OWNER が上記の 4 つの規則のいずれかによって受け入れられた場合、それは以下の 3 つのポリシーに準拠するかどうか再び検査されます。これらの追加ポリシーのいずれかに失敗した場合、コマンドは拒否されます。

- **C4R.GROUP.OWNER./SCOPE.***owner.group*

  このプロファイルは、端末ユーザーによって指定された新規 OWNER がグループ SPECIAL 属性の範囲内にある必要があるどうかを制御するために使用されます。その場合、**ADDGROUP** コマンドと **ALTGROUP** コマンドの両方に適用されます。このプロファイルは、端末ユーザーがグループ SPECIAL 属性の範囲内にあるグループ・プロファイルを引き渡すことを防止できます。

  変数 *group* と *owner* は、影響を受ける GROUP と、GROUP の新しい OWNER を表します。この設定は、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

  ポリシー・プロファイル内の修飾子 /SCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  新規所有者としてユーザー ID を指定することは、常に、端末ユーザーの管理範囲外と見なされます。

グループ SPECIAL またはシステム SPECIAL を持つ端末ユーザーが、新規所有者に対して自己の管理権限を使用すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

– **C4R.USESCOPE.***group*

このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、このグループに対して指定された新規所有者に対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

/SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: 端末ユーザーのグループ SPECIAL 範囲は、グループ・プロファイルの新規 OWNER の制御に使用されません。

NONE
: 指定された新規 OWNER が端末ユーザーのグループ SPECIAL 属性の範囲外にある場合、コマンドは拒否されます。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーの範囲に関係なく、指定された OWNER は受け入れられます。

CONTROL
: UPDATE と同じ。

- **C4R.GROUP.OWNER./GROUP.***owner.group*

このプロファイルは、指定された所有者が RACF グループでなければならないかどうかを制御するために使用されます。このプロファイルは、他のプロファイルとは無関係に検査されます。=OWNER または /OWNER プロファイルのいずれかが使用される場合は、このポリシー・ルールがバイパスされます。

変数 *group* と *owner* は、影響を受ける GROUP と、GROUP の新しい OWNER を表します。この設定は、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /GROUP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。指定の所有者はグループとユーザーです。

NONE
: 指定された所有者が既存の RACF グループである場合、コマンドは受け入れられます。それ以外のすべての状態では、コマンドは拒否されます。

READ
NONE と同じ。

UPDATE
指定された所有者は、既存のグループを表していない場合でも受け入れられます。指定された所有者が有効な項目でない場合、コマンドは RACF によって拒否されます。

CONTROL
UPDATE と同じ。

- **C4R.GROUP.OWNER./SUPGRP.***owner.group*

  このプロファイルは、端末ユーザーによって指定された OWNER が、GROUP の SUPGRP と同じであることが必要かどうかを制御するために使用されます。このプロファイルは、**ADDGROUP** コマンドと **ALTGROUP** コマンドの両方に適用されます。

  group と *owner* の値は、それぞれ影響を受ける GROUP と GROUP の新しい OWNER を表します。この設定は、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

  ポリシー・プロファイル内の修飾子 /SUPGRP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  この制御は実装されません。現在の SUPGRP と異なる OWNER を指定できます。

  NONE
  指定された新規の OWNER は、現在または新規の SUPGRP と同じでなければなりません。

  READ
  NONE と同じ。

  UPDATE
  SUPGRP の値に関係なく、指定された OWNER は受け入れられます。

  CONTROL
  UPDATE と同じ。

新規グループ・ポリシーの実装

RACF グループ階層の一部ではないポリシー・プロファイルの組織を計画するには、以下のガイドラインに従ってください。

これまでのセクションでは、GROUP と、RACF グループ階層内の場所の決定プロセスで使用されるプロファイルについて説明しました。これらのプロファイルを使用すると、定義できる、または定義できない GROUP を非常に柔軟に指定できます。1 つの例として、次のような組織を考えてみましょう。

- 中央管理者は、すべてのグループを定義できる
- 分散管理者は、自分自身の部門についてのみ、グループを定義する必要がある
- 部門は、RACF グループ構造 (所有権) によって認識できる。

- すべてのグループ・プロファイルは、部門の構造に従って、RACF グループによって所有される必要がある
- グループの最初の 3 文字が部門名の最初の 3 文字と同じ場合は、グループ命名規則が使用される

このような組織には、以下のプロファイルを実装することができます。

C4R.group.id.* uacc(none) sysadmin(update)
このプロファイルにより、システム管理者だけが正規の命名規則の外部で新規グループ・プロファイルを定義することが許可されます。

C4R.group.id.=racuid(3) uacc(update)
このプロファイルにより、すべての分散管理者は、最初の 3 文字がその分散管理者と同じ文字の新規グループを定義できます。=RACGPID(3) プロファイルからのこのポリシーの実装は、それほど効果的ではありません。端末ユーザーのすべてのグループは、命名規則として使用されます。端末ユーザーが、異なる接頭部を持つ別の部門で機能しているグループに接続していないことは保証されません。

C4R.group.delete. uacc(none) sysadmin(update)**
このプロファイルにより、中央システム管理者だけが既存のグループの削除を許可されます。

C4R.group.=supgrp. uacc(update) sysadmin(control) appldata('=myowner')**
このプロファイルは、どの分散管理者が何を指定したかに関係なく、新規に定義されるグループは常にその分散管理者自身を所有する同じグループの下に配置されることを指定します。中央システム管理者は、SUPGRP を指定する必要があります。この制御は中央システム管理者には適用されないからです。ただし、次のプロファイルを参照してください。

C4R.group./supgrp. uacc(none) sysadmin(update) appldata('DEPTS')**
中央システム管理者が新規グループの SUPGRP を指定しなかった場合、そのグループは DEPTS と呼ばれるグループに割り当てられます。

C4R.group.=owner. uacc(update) sysadmin(control) appldata('=myowner')**
このプロファイルにより、新規 /GROUP プロファイルの OWNER は、分散管理者の OWNER と同じであることが保証されます。この場合も、この制御は中央システム管理者には適用されません。次のプロファイルは、それらの管理者の利用のために特に定義されています。

C4R.group./owner. uacc(none) sysadmin(update) appldata('=supgrp')**
=SUPGRP を APPLDATA の値として使用することにより、OWNER の値が指定されなかった場合に、zSecure Command Verifier によって新しいグループの SUPGRP と同じ値が OWNER に対して指定されます。

既存グループ・ポリシーの実装

以下のシナリオを使用して、既存のグループの指定で追加の制御をセットアップするポリシー・プロファイルを実装します。

既存のグループの処理方法を決定するポリシー・プロファイルをセットアップすることができます。既存グループ・ポリシーに対する追加のルールは以下のとおりです。

- 中央管理者は、すべてのグループを変更できる

- 中央管理者は、任意のユーザーまたはグループを所有者として指定できる
- 分散管理者は、自分自身の部門内の所有者だけを変更する必要がある

このような組織には、以下のプロファイルを実装することができます。

C4R.group.supgrp./scope. uacc(none) sysadmin(control)**
このプロファイルにより、システム管理者だけが上位グループをすべての値に変更できます。分散管理者は、自己の制御範囲内にあるグループだけを指定できます。

C4R.group.owner./scope. uacc(none) sysadmin(control)**
このプロファイルにより、システム管理者だけが既存グループの OWNER を変更する無制限の権限を持ちます。分散管理者は、自己の範囲内だけで OWNER を変更できます。自己のグループを引き渡すことはできません。通常のユーザーは、グループ SPECIAL を持たないので、自己が所有するグループの OWNER を変更することはできません。すべてが、そのユーザーの範囲外にあります。

グループ属性および権限のポリシー・プロファイル

以下の要約リストに示すポリシー・プロファイルを使用して、グループの属性および権限に対する制御を実装します。

ユーザーからグループへの接続のすべての属性と権限については、 168 ページの『CONNECT の管理』を参照してください。コマンド、キーワード、およびプロファイルは、以下の表にまとめています。各プロファイルについて詳しくは、表に続く各セクションを参照してください。

表 *28. RACF* 属性に使用されるプロファイル： この表の項目は、**ADDGROUP** コマンドおよび **ALTGROUP** コマンドで指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDGROUP		**C4R.GROUP.=ATTR.***owner.group*
ADDGROUP	*UNIVERSAL*	**C4R.GROUP.ATTR.UNIVERSAL.***owner.group*
ADDGROUP **ALTGROUP**	*(NO)TERMUACC*	**C4R.GROUP.ATTR.TERMUACC.***owner.group*
ADDGROUP **ALTGROUP**	*(NO)DATA*	**C4R.GROUP.INSTDATA.***owner.group*
ADDGROUP **ALTGROUP**	*(NO)MODEL*	**C4R.GROUP.MODEL.***owner.group*

新規グループの必須属性

インストール済み環境では、グループ属性に対して必須ポリシー・プロファイルを使用することで、**ADDGROUP** コマンドで使用されるキーワードに関係なく、新しいグループに常に特定の属性が必要であることを指定できます。

この機能の最もわかりやすい使用例は、NOTERMUACC 値の設定です。必須属性ポリシー・プロファイルおよび適用可能なアクセス・レベルを以下で説明します。

- **C4R.GROUP.=ATTR.***owner.group*

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
必須属性は端末ユーザーには適用されません。

READ
必須値ポリシー・プロファイルの APPLDATA が、新しいグループの属性のリストとして使用されます。

UPDATE
READ と同じ。

CONTROL
この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーによって指定された属性がコマンド内で使用されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値プロファイルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

必須ポリシー・プロファイルの **APPLDATA** フィールドでは、グループ属性のリストを指定します。認識されるグループ属性は以下のとおりです。

- TERMUACC および NOTERMUACC
- UNIVERSAL

属性には省略形を使用できません。複数の属性を割り当てる必要がある場合は、個々の属性を単一のコンマで区切り、間にブランクを入れないようにする必要があります。以下に例を示します。

```
TERMUACC,UNIVERSAL
```

グループ属性とアクセス・レベルの説明

以下の情報では、使用できるキーワードと値を制御するために使用されるアクセス・レベルについて説明します。

一般に、RACF が新しいグループにデフォルトで適用する値を指定する場合は READ アクセス・レベル、属性を設定または変更する場合は UPDATE アクセス・レベルが必要となります。また、**ADDGROUP** コマンドの場合は、RACF で使用されるデフォルト値が zSecure Command Verifier で検査されません。ただし、デフォルト以外の値は、**ALTGROUP** コマンドの場合と同様に検査されます。

- **C4R.GROUP.ATTR.UNIVERSAL.***owner.group*

  このプロファイルでは、RACF 汎用**グループ**の定義を制御します。汎用**グループ**とは、完全なメンバーシップ情報がそのグループ・プロファイルに保管されていないユーザー・**グループ**のことです。汎用**グループ**を使用する利点は、GROUP に接続される通常のユーザー ID の数が RACF で制限されないことです。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、汎用**グループ**の作成を許可されません。

READ
NONE と同じ。

UPDATE
端末ユーザーは、汎用**グループ**の作成を許可されます。

CONTROL
この制御は、端末ユーザーに対して実装されません。

上記のいずれの場合も、端末ユーザーには GROUP を作成するための十分な RACF 権限がまず必要です。また、実装されている zSecure Command Verifier ポリシーに GROUP が準拠している必要があります。

- **C4R.GROUP.ATTR.TERMUACC.***owner.group*

このプロファイルは、新規および既存のグループの (NO)TERMUACC 属性の設定を制御します。TERMUACC は、端末許可検査中に RACF がその端末の汎用アクセス権限 (UACC) に基づいてグループ内のユーザーに端末へのアクセスを許可するように指定します。TERMUACC はデフォルト値です。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、**ALTGROUP** コマンドにどちらのキーワードも指定することを許可されません。TERMUACC 設定は、**ADDGROUP** コマンドで許可されます (デフォルトで指定されます)。

READ
端末ユーザーは、ALTGROUP コマンドで **TERMUACC** 属性を明示的に指定することを許可されます。この設定は、属性をそのデフォルトの状態にリセットできます。

UPDATE
端末ユーザーは、**ALTGROUP** コマンドでどちらのキーワードも指定することを許可されます。この設定は、これらの属性の通常の保守が可能となります。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、**ADDGROUP** および **ALTGROUP** コマンドでどちらのキーワードも指定することを許可されます。この設定により、TERMUACC 属性の通常の保守が可能となります。

- **C4R.GROUP.INSTDATA.***owner.group*

このプロファイルは、GROUP のインストール・データを変更する権限を制御するために使用されます。通常の場合、これを使用できるのは、プロファイルの所有者とグループ **SPECIAL** 権限を持つユーザーだけに既に制限されています。このプロファイルは、それ以外の制約事項を実装します。

INSTDATA ポリシー・プロファイルには、インストール・データに必要なフォーマットの参照を含めることもできます。フォーマットの名前は、最適ポリシー・プロファイルの APPLDATA によって指定できます。フォーマットの名前を使用して、適切な (一連の) フォーマット指定ポリシー・プロファイルを決定します。フォーマット指定ポリシー・プロファイル (または短形式プロファイル) では、以下のような名前が使用されます。

C4R.*class*.INSTDATA.=FMT.*format-name*.POS(*start*:*end*)

複数のフォーマット・プロファイルを使用して、グループ・プロファイルのインストール・データのさまざまな部分を指定することができます。フォーマット・プロファイルについて詳しくは、 254 ページの『インストール・データ・フィールドのフォーマットの制約事項』を参照してください。

このプロファイルに使用できるアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: この制御は実装されません。RACF 許可のあるすべてのユーザーが、それぞれの制御の範囲内でグループのインストール・データを変更できます。

NONE
: インストール・データの指定は許可されません。コマンドはリジェクトされます。この設定は、**ADDGROUP** コマンドと **ALTGROUP** コマンドの両方に適用されます。

READ
: **ADDGROUP** コマンドでのインストール・データの指定が許可されます。その後に **ALTUSER** コマンドで値を変更することはできません。

UPDATE
: インストール・データの変更が許可されます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

APPLDATA で指定されるオプションの値を以下に示します。

format グループ のインストール・データに使用する必要があるフォーマットの名前。このフォーマット 名は、適切な一連のフォーマット・プロファイルを見つけるために使用されます。

- **C4R.GROUP.MODEL.***owner.group*

モデル・データ・セット名は、このグループで始まる新しいデータ・セット・プロファイルが定義されるときに RACF によって使用されます。指定されるモデル・データ・セットには、接頭部としてグループが付加されます。グループ・データ・セットのモデル化は、SETROPTS で活動化されている場合にのみ使用されます。zSecure Command Verifier では、モデルとして使用する必要があるデータ・セット・プロファイルを選択する権限を制御することができます。 245 ページの『その他のポリシー・プロファイルとアクセス・レベルの説明』で説明している **C4R.***class.***TYPE.***type.profile* プロファイルを使用すると、MODEL データ・セット自体の定義を制御できます。

プロファイルが見つからない
: この制御は実装されません。

NONE
: グループの MODEL データ・セット名を選択することはできません。

READ
: ADDGROUP コマンドで **MODEL** を指定することができます。これを後から **ALTGROUP** コマンドで変更することはできません。

UPDATE
: MODEL の指定の設定、変更、および削除が許可されます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

CONNECT の管理

ユーザーからグループへの接続 (グループ・メンバーシップ) については、属性付きで新規接続を定義すること、および既存の接続属性を変更することを区別する必要があります。

zSecure Command Verifier では、この 2 つの状態に 2 つの制御セットが実装されています。新規接続の場合は、命名規則および類似のポリシーが適用されます。新規接続と既存接続のどちらの場合も、接続の権限および属性に関してポリシーを適用できます。

もう 1 つ留意する必要がある問題は、インストールにおいて、ユーザーからグループへの接続をユーザーの視点から制御する必要があるのか、それともグループの視点から制御する必要があるのかという点です。zSecure Command Verifier では、ポリシー・プロファイルにグループとユーザーの両方の修飾子があります。ただし、ポリシー実装を簡素化するには、総称文字によってこれらの修飾子のうちの 1 つのみを実装します。両方のタイプの総称を一緒に使用した場合は、制御側のプロファイルの判別がより複雑になる可能性があります。

170 ページの『新規 CONNECT』で、新規 CONNECT の zSecure Command Verifier ポリシー・プロファイルの詳細について説明しています。後続のセクションでは、既存の CONNECT の要件と、CONNECT の権限および属性について説明します。

自分自身を接続するための権限

管理者間での責任の分離を強制するための自己許可プロファイルを実装するには、以下のガイドラインに従ってください。

この機能は、セキュリティー管理者とデータまたはアプリケーション管理者の間で責任を厳密に分けたいと考えている多数の組織から求められています。システム・セキュリティー・ポリシーで、セキュリティー管理者にアプリケーション・リソースへのアクセス権限を付与してはならないことを指定している場合が少なくありません。標準 RACF では、システム SPECIAL またはグループ SPECIAL を持つユーザーは、自己の制御下にあるプロファイルを変更できます。このため、セキュリ

ティー管理者は、アプリケーション・リソースに対するアクセス権限を現在持っていない場合でも、アクセス権限を簡単に取得できます。その場合、アクセス権限を持っている GROUP に接続することによって、アクセス権限を取得できます。一部の組織では、SMF データを分析して、特定のグループから自己を接続または削除する管理者についてレポートを作成します。zSecure Command Verifier では、セキュリティー管理者が自己の接続先である GROUP のリストを変更できないようにする、いくつかのポリシーがあります。

表 29. 自己許可の制御に使用されるプロファイル： この表の項目は、ACL 項目または CONNECT を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
PERMIT	*userid*	**C4R.***class.***ACL.=RACUID.***access.profile*
PERMIT	*group*	**C4R.***class.***ACL.=RACGPID.***access.profile*
CONNECT	*userid*	**C4R.CONNECT.ID.***group.***=RACUID**
REMOVE	*userid*	**C4R.REMOVE.ID.***group.***=RACUID**

上記のプロファイルは、*userid* が端末ユーザーであるか、または *group* がユーザーの接続グループのいずれかである場合にのみ適用されます。この状態が当てはまる場合、zSecure Command Verifier は、 170 ページの『新規 CONNECT』で説明されている CONNECT プロファイルに優先して上記のプロファイルを使用します。最後の 2 つのプロファイルとサポートされるアクセス・レベルについては、以下で詳しく説明します。PERMIT 用のプロファイルについて詳しくは、 196 ページの『自己許可に対するポリシー・プロファイルの選択』を参照してください。

- **C4R.CONNECT.ID.***group.***=RACUID**

  このプロファイルは、端末ユーザーが自分自身を *group* に CONNECT する権限を指定するために使用されます。*group* に総称パターンが使用される場合、このプロファイルは自分自身を任意の *group* に接続する権限を記述します。このプロファイルの主な目的は、管理者がアプリケーションまたはシステム・リソースへの高度なアクセス権限を持つ機能グループへの CONNECT によって、自己の権限を増大させるのを防止することです。このプロファイルを最も効果的に使用できるのは、 196 ページの『自己許可に対するポリシー・プロファイルの選択』で述べるように、アクセス・リストを変更するために =RACGPID のポリシー・プロファイルと組み合わせた場合です。

  プロファイルが見つからない
  : この制御は実装されません。すべての端末ユーザーは、自己の制御下にあるに任意の GROUP に自分自身を CONNECT することができます。

  NONE
  : 端末ユーザーは、自分自身を *group* に CONNECT することを、たとえその GROUP が範囲内であっても、許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、自分自身を *group* に CONNECT することを、その GROUP が範囲内であれば許可されます。

CONTROL
UPDATE と同じ。

- **C4R.REMOVE.ID.*group*.=RACUID**

  このプロファイルは、端末ユーザーが自分自身を *group* から REMOVE する権限を指定するために使用されます。*group* に総称パターンが使用される場合、このプロファイルは自分自身を任意の *group* から削除する権限を記述します。このプロファイルは主に、(グループ) OPERATIONS 属性を持つユーザーのアクセス権限を削減するために特定の GROUP を使用する場合を意図しています。このプロファイルを最も効果的に使用できるのは、 196 ページの『自己許可に対するポリシー・プロファイルの選択』で述べるように、アクセス・リストを変更するために =RACGPID のポリシー・プロファイルと組み合わせた場合です。

  プロファイルが見つからない
  この制御は実装されません。すべての端末ユーザーは、範囲内の任意の GROUP から自分自身を REMOVE することができます。

  NONE
  端末ユーザーは、自分自身を *group* から REMOVEすることを、たとえその GROUP が範囲内であっても、許可されません。

  READ
  NONE と同じ。

  UPDATE
  端末ユーザーは、自分自身を *group* から REMOVE することを、その GROUP が範囲内である場合に限って、許可されます。

  CONTROL
  UPDATE と同じ。

新規 CONNECT

以下の接続関連ポリシー・プロファイルを使用して、作成可能なユーザーとグループの接続を制御します。

この表の項目は、新規に定義される接続のユーザーおよびグループを反映しています。

表 *30. RACF* 接続に関連したコマンド/キーワードに使用されるプロファイル

コマンド	キーワード	プロファイル
CONNECT	**GROUP(***group***)**	**C4R.CONNECT.ID.=USERID(***n***)**
CONNECT	*userid* **GROUP(***group***)**	**C4R.CONNECT.ID.***group.userid*
CONNECT	*userid* **GROUP(***group***)**	**C4R.CONNECT.ID./USRSCOPE.***group.userid*
CONNECT	*userid* **GROUP(***group***)**	**C4R.CONNECT.ID./GRPSCOPE.***group.userid*
CONNECT	*userid* **GROUP(***group***)**	**C4R.CONNECT.ID.=DSN.***group.userid*
REMOVE	*userid* **GROUP(***group***)**	**C4R.REMOVE.ID.***group.userid*

CONNECT を作成するための権限

CONNECT ポリシーの最初の部分では、新規 CONNECT の作成規則を扱います。 RACF は GROUP 内の端末ユーザーの権限だけを調べます。接続されるユーザー ID は関係ありません。

zSecure Command Verifier では、ユーザー ID に基づいて権限を制御できる追加の制御がインストールで実装されます。

- **C4R.CONNECT.ID.=USERID(*n*)**

  このプロファイルを使用して、USER から GROUP への CONNECT に関する一般的な命名規則ベースのポリシーを実装できます。修飾子 =USERID(*n*) は、ユーザー ID (または GROUP) の最初の *n* 文字を表します。GROUP の最初の *n* 文字は、ユーザー ID の最初の *n* 文字と突き合わされます。それらが一致した場合、このプロファイルを使用して、新規 CONNECT を作成できるかどうかが決定されます。これらのプロファイルが複数定義されている場合は、*n* の数値が最も小さいプロファイルだけが使用されます。

  このプロファイルは、個別プロファイルでなければなりません。数値 *n* は、1 から 8 までの単一の数字で指定する必要があります。

  注: プロファイル =USERID(*n*) は、機能的に =GROUP(*n*) と同等になります。zSecure Command Verifier には、=USERID(*n*) プロファイルのみが実装されています。

  プロファイルが見つからない
  : この制御は実装されません。GROUP の最初の何文字かは、ユーザー ID のそれと突き合わされません。

  NONE
  : 端末ユーザーは、USER を、同じ何文字かで始まる GROUP に CONNECT することを許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、USER を、似たような名前 (最初の *n* 文字) が付いた GROUP に CONNECT することを許可されます。

  CONTROL
  : この制御は、端末ユーザーに対して実装されません。USER から GROUP への CONNECT に使用される一般的な命名規則はありません。

- **C4R.CONNECT.ID.*group.userid***

  このプロファイルを使用して、その他の命名規則ベースのポリシーを実装できますpolicies。また、これを一般的な =USERID(*n*) ポリシーに対する例外を指定するための方法として使用することもできます。

  プロファイルが見つからない
  : この制御は実装されません。*userid* を *group* に接続できます。

NONE
端末ユーザーは、*userid* を *group* に CONNECT することを許可されません。

READ
NONE と同じ。

UPDATE
端末ユーザーは、*userid* を *group* に CONNECT することを許可されます。

CONTROL
UPDATE と同じ。

新規 CONNECT に対する追加のポリシー制御

新規接続が上記のポリシー・ルールによって承認された後、新規接続を追加制御の支配下に置くことができます。RACF グループ SPECIAL 範囲および命名規則に基づいたポリシーも実装できます。

実装できるポリシーについて、以下で説明します。

- **C4R.CONNECT.ID./USRSCOPE.***group.userid*

  このプロファイルは、端末ユーザーのグループ SPECIAL 範囲の外部にいる USER が *group* に接続できるかどうかを制御するために使用されます。

  ポリシー・プロファイル内の修飾子 /USRSCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  グループ SPECIAL またはシステム SPECIAL を持つ端末ユーザーが、自己の管理範囲内のユーザーを接続すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

  – **C4R.USESCOPE.***group*

  このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、このグループに接続されたユーザーに対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

  /SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

  プロファイルが見つからない
  この制御は実装されません。端末ユーザーのグループ SPECIAL 範囲は、*group* に CONNECT される *userid* について考慮されません。

  NONE
  端末ユーザーは、その範囲外のユーザーを *group* に CONNECT することを許可されません。

  READ
  NONE と同じ。

UPDATE
端末ユーザーは、その範囲外のユーザーを *group* に CONNECT することを許可されます。

CONTROL
UPDATE と同じ。

- **C4R.CONNECT.ID./GRPSCOPE.***group.userid*

  このプロファイルは、端末ユーザーのグループ SPECIAL 範囲の外部にある GROUP が、この *userid* に接続できるかどうかを制御するために使用されます。このプロファイルは、通常の RACF 権限要件と部分的にオーバーラップします。主な相違点は、zSecure Command Verifier ポリシーが CONNECT 権限と GROUP の直接所有権を考慮に入れないことです。グループ SPECIAL だけを考慮して権限が決定されます。

  ポリシー・プロファイル内の修飾子 /GRPSCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  グループ SPECIAL またはシステム SPECIAL を持つ端末ユーザーが、自己の管理範囲内のグループにユーザーを接続すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

  – **C4R.USESCOPE.***group*

  このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、ユーザーが接続されているグループに対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

  /SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

  プロファイルが見つからない
  この制御は実装されません。端末ユーザーのグループ SPECIAL の範囲は、USER の CONNECT 先となる *group* については考慮されません。

  NONE
  端末ユーザーは、その範囲外の GROUP にユーザーを CONNECT することを許可されません。

  READ
  NONE と同じ。

  UPDATE
  端末ユーザーは、その範囲外の GROUP にユーザーを CONNECT することを許可されます。

  CONTROL
  UPDATE と同じ。

- **C4R.CONNECT.ID.=DSN.***group.userid*

このプロファイルは、USER をデータ・セットの高位修飾子 (HLQ) として使用された GROUP に接続できるかどうかを制御するために使用されます。

ポリシー・プロファイル内の修飾子 =DSN を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。GROUP がデータ・セットの HLQ として使用されていることは、考慮されません。

NONE
: 端末ユーザーは、データ・セットの HLQ として使用された GROUP にユーザーを CONNECT することを許可されません。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、データ・セットの HLQ として使用された GROUP にユーザーを CONNECT することを許可されます。

CONTROL
: UPDATE と同じ。

既存の接続の削除

zSecure Command Verifier は、グループから削除できるユーザーを制御するポリシーも備えています。

標準 RACF 権限は、CONNECT 権限と、GROUP の直接または間接の (グループ SPECIAL からの) 所有権に基づいています。一部の組織では、グループからユーザー ID を削除すると、クリティカル・ジョブから必須アクセス権限が削除される場合があります。ユーザーが誤って削除されないように、以下のポリシーを実装できます。

- **C4R.REMOVE.ID.***group.userid*

  このプロファイルを使用して、USER が特定の GROUP から削除されないようにすることができます。通常、CONNECT 権限または GROUP に対するその他の制御権を持つすべてのユーザーは、GROUP からすべてのユーザーを削除できます。このポリシー・プロファイルを使用して、CONNECT を管理するための標準の権限に対する例外を指定します。

  プロファイルが見つからない
  : この制御は実装されません。*userid* を *group* から削除できます。

  NONE
  : 端末ユーザーは、*userid* を *group* から REMOVE することを許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、*userid* を *group* から REMOVE することを許可されます。

CONTROL
UPDATE と同じ。

CONNECT 属性および権限のポリシー・プロファイル

RACF CONNECT コマンドを使用して、新規のユーザーからグループへの接続を定義し、既存のユーザーからグループへの接続を変更することができます。ユーザーのリストを指定できます。

ただし、CONNECT コマンドは、コマンド上の他のキーワードの値のリストをサポートしていません。これは、すべての接続に、コマンド上で指定されたのと同じ OWNER および属性が割り当てられることを意味します。あるキーワード値が 1 つ以上の接続で許可されない場合は、コマンド全体が拒否され、「C4R551E GrpSpecial 属性は使用できません。コマンドが終了しました (C4R551E GrpSpecial attribute not allowed, command terminated)」のようなメッセージが発行されます。必須値またはデフォルト値ポリシー・プロファイルを使用している場合は、「C4R690E OWNER 値を割り当てることができません。コマンドを分割してください (C4R690E Cannot assign OWNER value, please split command)」のようなメッセージが発行されることがあります。

次の 2 つの表は、新規および既存の CONNECT に使用されるポリシー・プロファイルを要約したものです。最初の表では、すべての必須値およびデフォルト値プロファイルを示します。これらは、新規のユーザーからグループへの CONNECT に主に使用されます。2 番目の表では、その他のすべてのプロファイルを示します。これらは、CONNECT を作成するとき、または既存の CONNECT を変更するときに使用されます。これらのポリシーの主な目的は、ユーザーからグループへの CONNECT に使用される権限および属性を制御することです。最も重要な属性は、ほぼ確実にグループ SPECIAL 属性です。

必須値およびデフォルト値ポリシーは、新規のユーザーからグループへの接続のために使用されます。既存の接続については、端末ユーザーによって指定されなかったキーワード値は影響を受けません。そのため、許可された管理者によって割り当てられた非標準値が、他の管理者によって間違ってリセットされることはありません。CONNECT コマンドで新規の接続と既存の接続が混在して指定されている場合は、すべての接続が新規として扱われ、すべての接続について必須値およびデフォルト値ポリシーが評価されます。その結果、許可された管理者によって設定された OWNER、UACC、または AUTH の非標準値が、ポリシーによって要求される値にリセットされる可能性があります。

表 *31. RACF* 接続に関連したコマンド/キーワードに使用されるプロファイル： この表の項目は、**ADDUSER**、**ALTUSER**、および **CONNECT** コマンドで指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
CONNECT	**OWNER**	**C4R.CONNECT.=OWNER.***group.userid*
CONNECT	**OWNER**	**C4R.CONNECT./OWNER.***group.userid*
CONNECT ADDUSER	**AUTH(***auth***)**	**C4R.CONNECT.=AUTH.***group.userid*
CONNECT ADDUSER	**AUTH(***auth***)**	**C4R.CONNECT./AUTH.***group.userid*
CONNECT ADDUSER	**UACC(***uacc***)**	**C4R.CONNECT.=UACC.***group.userid*
CONNECT ADDUSER	**UACC(***uacc***)**	**C4R.CONNECT./UACC.***group.userid*

表 32. *RACF* 属性および権限に使用されるプロファイル： この表の項目は、**CONNECT** コマンドで指定されるキーワードを反映しています。

コマンド	キーワード	プロファイル
CONNECT	**OWNER(***owner***)**	**C4R.CONNECT.OWNER.***owner.group.userid*
CONNECT ADDUSER ALTUSER	**AUTH(***auth***)**	**C4R.CONNECT.AUTH.***auth.group.userid*
CONNECT ADDUSER ALTUSER	**UACC(***uacc***)**	**C4R.CONNECT.UACC.***uacc.group.userid*
CONNECT	**SPECIAL**	**C4R.CONNECT.ATTR.SPECIAL.***group.userid*
CONNECT	**OPERATIONS**	**C4R.CONNECT.ATTR.OPERATIONS.***group.userid*
CONNECT	**AUDITOR**	**C4R.CONNECT.ATTR.AUDITOR.***group.userid*
CONNECT	**ADSP**	**C4R.CONNECT.ATTR.ADSP.***group.userid*
CONNECT	**GRPACC**	**C4R.CONNECT.ATTR.GRPACC.***group.userid*
CONNECT	**REVOKE**	**C4R.CONNECT.ATTR.REVOKE.***group.userid*
CONNECT	**RESUME**	**C4R.CONNECT.ATTR.RESUME.***group.userid*
CONNECT	**REVOKE(***date***)**	**C4R.CONNECT.ATTR.REVOKEDT.***group.userid*
CONNECT	**RESUME(***date***)**	**C4R.CONNECT.ATTR.RESUMEDT.***group.userid*

CONNECT の必須値およびデフォルト値ポリシー・プロファイル

いくつかのプロファイルは、新規 CONNECT の OWNER、AUTH、および UACC の必須値とデフォルト値ポリシー・プロファイルを記述します。

これらのプロファイルは、ユーザーからグループへの CONNECT を作成するときに、**CONNECT** コマンド用にのみ使用されます。既存の接続を変更するための **CONNECT** コマンドの使用は、これらのポリシー・プロファイルの支配を受けません。

- **C4R.CONNECT.=OWNER.***group.userid*

  プロファイルからの **APPLDATA** フィールドは、新規のユーザーからグループへの接続の接続 OWNER に値を指定するために使用されます。このプロファイルは **CONNECT** コマンドにのみ、しかも新規 CONNECT にのみ使用されます。新規 CONNECT が新規ユーザー ID の作成の一環として作成される場合、このプロファイルは使用されず、RACF はユーザー ID の所有者を CONNECT の OWNER として使用します。使用されるアクセス・レベルを以下に示します。

  ポリシー・プロファイル内の修飾子 =OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。アクションは実行されません。

  NONE
  : アクションは実行されません。CONNECT OWNER に指定変更の値は提供されません。ユーザーが指定した値、または RACF のデフォルト値が使用されます。

  READ
  : APPLDATA 値は、新規 CONNECT の OWNER として挿入されます。

UPDATE
READ と同じ。

CONTROL
この制御は、端末ユーザーに対して実装されません。ユーザーが指定した値、または RACF のデフォルト値が保持されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。デフォルト値プロファイルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

APPLDATA フィールドで認識される特殊値は以下のとおりです。

BLANK
この値は、RACF のデフォルト動作が受け入れられる必要があることを明示的に示します。端末ユーザーは、ユーザーからグループへの接続の所有者として挿入されます。

=GROUP
CONNECT のグループ部分が、CONNECT プロファイルの所有者になります。

=USERID
CONNECT のユーザー部分が、CONNECT プロファイルの所有者になります。

value 指定された値が挿入されます。指定された値が既存の RACF userid または GROUP でない場合は、端末ユーザーの現在のグループが代わりに使用されます。

- **C4R.CONNECT./OWNER.***group.userid*

プロファイルからの **APPLDATA** フィールドは、新規のユーザーからグループへの接続の接続 OWNER に値を指定するために使用されます。このプロファイルは **CONNECT** コマンドにのみ、しかも新規 CONNECT にのみ使用されます。新規 CONNECT が新規ユーザー ID の定義の一環として作成される場合、RACF はユーザー ID の指定された所有者を GROUP の OWNER として使用します。

ポリシー・プロファイル内の修飾子 /OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
アクションは実行されません。CONNECT OWNER のデフォルト値は提供されません。この場合、新規接続では RACF のデフォルトが使用されることになります。つまり、端末ユーザーが新規接続の OWNER として使用されます。

READ
端末ユーザーが OWNER の値を指定しなかった場合は、**APPLDATA** の値が新規 CONNECT の OWNER として挿入されます。

UPDATE
端末ユーザーが OWNER の値を指定しなかった場合は、**APPLDATA** フィールドからの値が代わりに使用されます。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーが値を指定しなかった場合、RACF は端末ユーザーを OWNER として使用します。zSecure Command Verifier は明示的な所有者を挿入しません。

注: このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。デフォルト値プロファイルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

APPLDATA フィールドで認識される特殊値は以下のとおりです。

BLANK
この値は、RACF のデフォルト動作が受け入れられる必要があることを明示的に示します。端末ユーザーは、ユーザーからグループへの接続の所有者として挿入されます。

=GROUP
CONNECT のグループ部分が、CONNECT プロファイルの所有者になります。

=USERID
CONNECT のユーザー部分が、CONNECT プロファイルの所有者になります。

value 指定された値が挿入されます。指定された値が既存の RACF **ユーザー ID** またはグループでない場合は、端末ユーザーの現在のグループが代わりに使用されます。

- **C4R.CONNECT.=AUTH.***group.userid*

このプロファイルは、新規 CONNECT の AUTH の必須値を指定するために使用されます。これは、**ADDUSER** および **CONNECT** コマンドにのみ、しかも新規 CONNECT にのみ使用されます。使用される AUTH 値は、プロファイルの **APPLDATA** フィールドから取得されます。これは、端末ユーザーが指定した値を指定変更するために使用されるか、端末ユーザーが値を指定しなかった場合は、コマンドに追加されます。この必須値プロファイルから取得された AUTH 値は、その他の AUTH 関連ポリシー・プロファイルの影響を受けません。

値 *userid* は、影響を受けるユーザーを表します。この値は、一般規則への例外の指定を可能にします。最も限定的なプロファイルだけが zSecure Command Verifier によって使用されます。総称プロファイルを使用して、グループ内のユーザーの AUTH を指定することができます。

ポリシー・プロファイル内の修飾子 =AUTH を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。必須値は強制されません。

NONE
: アクションは実行されません。必須値は強制されません。

READ
: **APPLDATA** フィールドが抽出され、コマンドで使用されます。このプロセスで有効な AUTH レベルが生成されない場合、USE が代わりに使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーが CONNECT AUTH を指定した場合は、それが使用されます。値が指定されなかった場合、RACF は値 USE を使用します。

注: このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値ポリシー・プロファイルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

APPLDATA フィールドで受け入れられる値は以下のとおりです。端末ユーザーには、指定された AUTH レベルを割り当てるための十分な権限が GROUP 内で引き続き必要です。この権限は、zSecure Command Verifier では検査されません。権限が不十分であると、RACF によってコマンドが失敗する場合があります。

auth
: 指定可能な接続権限レベル (USE、CREATE、CONNECT、JOIN) のいずれか。この値は、この USER CONNECT の CONNECT 権限として挿入されます。

other
: この値はエラーと考えられます。RACF のデフォルト CONNECT 権限 (USE) が代わりに使用されます。

- **C4R.CONNECT./AUTH.***group.userid*

  このプロファイルは、端末ユーザーが ADDUSER コマンドまたは **CONNECT** コマンドで接続権限レベルを指定しなかった場合に、接続 **AUTH** のデフォルト値を指定するために使用されます。必須値ポリシー・プロファイルを使用して値が指定された場合、/AUTH プロファイルは使用されません。また、新規ユーザー・プロファイルを定義する場合、RACF は DFLTGRP 内の権限に値 USE を挿入します。その結果、zSecure Command Verifier は端末ユーザーによって指定されたコマンドに値がないことを一切検出しません。代わりに、zSecure Command Verifier は端末ユーザーが値 USE を入力したものとして、コマンドを処理します。

デフォルトとして使用される AUTH 値は、プロファイル内の **APPLDATA** フィールドから取得されます。この必須値プロファイルから取得された CONNECT 値は、その他の CONNECT 関連ポリシー・プロファイルの影響を受けません。

ポリシー・プロファイル内の修飾子 AUTH を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。デフォルト値は提供されません。

NONE
: デフォルト値は提供されません。しかし、RACF も CONNECT 権限の値を提供できません。コマンドはリジェクトされます。このアクセス・レベルを使用すると、インストールで端末ユーザーに CONNECT AUTH の値を明示的に指定するよう強制できます。

READ
: **APPLDATA** フィールドが抽出され、コマンドで使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。デフォルト値は提供されません。RACF は、そのデフォルト権限 (USE) を使用します。

APPLDATA フィールドで受け入れられる値は以下のとおりです。端末ユーザーには、CONNECT 権限を割り当てるための十分な権限が引き続き必要です。権限が不十分であると、コマンドが失敗する場合があります。

auth
: 指定可能な接続権限レベル (USE、CREATE、CONNECT、JOIN) のいずれか。この値は、この USER の CONNECT 権限として挿入されます。

other
: これはエラーと考えられます。RACF のデフォルト CONNECT 権限 (USE) が代わりに使用されます。

- **C4R.CONNECT.=UACC.***group.userid*

このプロファイルは、新規 CONNECT の UACC の必須値を指定するために使用されます。Connect-UACC は、データ・セットおよびその他の一部のリソース・クラスについて、新規リソース・プロファイルのデフォルトの UACC を指定します。端末ユーザーが新規リソース・プロファイルの UACC に値を指定しなかった場合は、RACF によってデフォルト値が使用されます。Connect-UACC の設定によって RACF の動作が混乱する可能性があるため、推奨される設定は NONE です。

zSecure Command Verifier は、=UACC ポリシー・プロファイルを使用して、Connect-UACC 設定を制御します。このポリシー・プロファイルは、**ADDUSER** および **CONNECT** コマンドにのみ、しかも新規 CONNECT にのみ使用されます。強制される UACC 値は、ポリシー・プロファイルの **APPLDATA** フィールドから取得されます。これは、端末ユーザーが指定した値を指定変更するために使用されるか、端末ユーザーが値を指定しなかった場合は、コマンドに追加されま

す。この必須値プロファイルから取得された UACC 値は、追加の UACC 関連ポリシー・プロファイルの支配を受けません。

値 *userid* および *group* は、影響を受けるユーザーおよびグループを表します。この設定は、一般規則への例外の指定を可能にします。最も限定的なプロファイルだけが zSecure Command Verifier によって使用されます。総称プロファイルを使用して、グループ内のユーザーの UACC を指定することができます。

ポリシー・プロファイル内の修飾子 =UACC を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。必須値は強制されません。

NONE
: アクションは実行されません。必須値は強制されません。

READ
: **APPLDATA** フィールドが抽出され、コマンドで使用されます。このプロセスで有効な UACC レベルが生成されない場合、NONE が代わりに使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーが `CONNECT UACC` を指定した場合は、それが使用されます。値が指定されなかった場合、RACF は値 NONE を使用します。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値ポリシー・プロファイルでは、このためにアクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

APPLDATA フィールドで受け入れられる値は以下のとおりです

uacc
: 指定可能な UACC レベル (`NONE`、`READ`、`UPDATE`、`CONTROL`、`ALTER`) のいずれか。この値は、この `CONNECT` の UACC として挿入されます。

other
: この値はエラーと考えられます。RACF のデフォルト UACC (NONE) が代わりに使用されます。

- **C4R.CONNECT./UACC.***group.userid*

  このプロファイルは、端末ユーザーが **`ADDUSER`** コマンドまたは **`CONNECT`** コマンドで UACC 値を指定しなかった場合に、 UACC のデフォルト値を指定するために使用されます。上記の必須値ポリシー・プロファイルを使用して値が指定された場合、`/UACC` プロファイルは使用されません。また、新規ユーザー・プロファイルを定義する場合、RACF は `DFLTGRP` の UACC として値 NONE を挿入します。その結果、zSecure Command Verifier は端末ユーザーによって指定さ

れたコマンドに値がないことを一切検出しません。代わりに、zSecure Command Verifier は端末ユーザーが値 NONE を入力したものとして、コマンドを処理します。

デフォルトで使用される UACC 値は、プロファイル内の **APPLDATA** フィールドから取得されます。この必須値プロファイルから取得された UACC 値は、追加の UACC 関連ポリシー・プロファイルの支配を受けません。

ポリシー・プロファイル内の修飾子 /UACC を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。デフォルト値は提供されません。

NONE
: デフォルト値は提供されません。しかし、RACF も UACC レベルの値を提供できません。コマンドはリジェクトされます。このアクセス・レベルを使用すると、インストールで端末ユーザーに UACC の値を明示的に指定するよう強制できます。

READ
: **APPLDATA** フィールドが抽出され、コマンドで使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。デフォルト値は提供されません。RACF は、そのデフォルト権限 (NONE) を使用します。

APPLDATA フィールドで受け入れられる値は以下のとおりです

uacc
: 指定可能な接続権限レベル (NONE、READ、UPDATE、CONTROL、ALTER) のいずれか。この値は、この CONNECT の UACC 値として挿入されます。

other
: この値はエラーと考えられます。RACF のデフォルト UACC レベル (NONE) が代わりに使用されます。

端末ユーザーによって指定された CONNECT 値の検査

端末ユーザーによって指定された CONNECT 権限および UACC 値を検査するには、以下のプロファイルを使用します。

- **C4R.CONNECT.OWNER.***owner.group.userid*

  このプロファイルは、端末ユーザーによって指定された OWNER 値を検査するために使用されます。このポリシーは、**CONNECT** コマンドについてのみ実装できます。一般ポリシーを定義するには、*owner* 修飾子および *userid* 修飾子の両方の総称パターンを含むプロファイルを使用します。特定のユーザー ID の例外を定義するには、より特定された (個別の) プロファイルを使用します。値 *owner* は、RACF で定義されたいずれかのユーザー ID または GROUP にすることができます。

  必須値またはデフォルト値のポリシー・プロファイルを使用して **CONNECT** 所有者が割り当てられた場合、このプロファイルは使用されません。

プロファイルが見つからない
この制御は実装されません。RACF によって許可されたすべての **CONNECT** 所有者を、この接続に割り当てることができます。

NONE
コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
指定された OWNER は、この GROUP およびユーザー ID について受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.CONNECT.AUTH.***auth.group.userid*

このプロファイルは、端末ユーザーによって指定された AUTH 値を検査するために使用されます。このポリシーは、**ADDUSER**、**ALTUSER**、および **CONNECT** コマンド用に実装できます。ほとんどの場合、*owner* と *userid* の両方に総称プロファイルを使用することができます。明示的なプロファイルを使用して、特定のユーザー ID の例外を定義できます。値 *auth* は、RACF が受け入れる任意の **CONNECT** 権限 (つまり、USE、CREATE、CONNECT、および JOIN) とすることができます。

必須値またはデフォルト値のポリシー・プロファイルを使用して CONNECT 権限が割り当てられた場合、このプロファイルは使用されません。また、新規ユーザー・プロファイルを定義するか、CONNECT を作成する場合、値 USE は、これらのポリシー・プロファイルの検査なしに受け入れられます。

プロファイルが見つからない
この制御は実装されません。RACF によって許可されたすべての CONNECT 権限を、この接続に割り当てることができます。

NONE
コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
指定された *auth* は、この GROUP およびユーザー ID について受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.CONNECT.UACC.***uacc.group.userid*

このプロファイルは、端末ユーザーによって指定された UACC 値を検査するために使用されます。このポリシーは、**ADDUSER**、**ALTUSER**、および **CONNECT** コマンド用に実装できます。ほとんどの場合、*owner* と *userid* の両方に総称プロファイルを使用することができます。明示的なプロファイルを使用して、特定のユーザー ID の例外を定義できます。

必須値またはデフォルト値ポリシー・プロファイルを使用して UACC が割り当てられた場合、このプロファイルは使用されません。また、新規ユーザー・プロファイルを定義するか、CONNECT を作成する場合、値 NONE は、これらのポリシー・プロファイルの検査なしに受け入れられます。

プロファイルが見つからない
: この制御は実装されません。任意の UACC 値を、この接続に割り当てることができます。

NONE
: コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 指定された *uacc* は、この GROUP およびユーザー ID について受け入れられます。

CONTROL
: UPDATE と同じ。

CONNECT 属性およびアクセス・レベルの説明

以下の段落では、ユーザーとグループの間の CONNECT にどの属性を割り当てることができるかを制御するために使用されるアクセス・レベルについて説明します。

一般に、必要となるアクセス・レベルは、属性を与えるための UPDATE か、属性を除去するための READ です。

- **C4R.CONNECT.ATTR.SPECIAL.***group.userid*
- **C4R.CONNECT.ATTR.OPERATIONS.***group.userid*
- **C4R.CONNECT.ATTR.AUDITOR.***group.userid*
- **C4R.CONNECT.ATTR.ADSP.***group.userid*
- **C4R.CONNECT.ATTR.GRPACC.***group.userid*

プロファイルが見つからない
: この制御は実装されません。アクションは実行されません。

NONE
: 端末ユーザーは、**CONNECT** コマンドにどちらのキーワードも指定することを許可されません。

READ
: 端末ユーザーは、**CONNECT** コマンドに非属性キーワードを明示的に指定することを許可されます。この設定は、これらの属性の除去を可能にします。

UPDATE
: 端末ユーザーは、**CONNECT** コマンドに両方のキーワードを指定することを許可されます。この設定は、これらの属性の通常の保守が可能となります。

CONTROL
UPDATE と同じ。

上記のすべての場合において、端末ユーザーがキーワードを指定するためには十分な RACF 権限が必要です。例えば、ほとんどのキーワードの場合、端末ユーザーはグループ内でグループ SPECIAL 属性を持っている必要があります。

- **C4R.CONNECT.ATTR.REVOKE.***group.userid*

このポリシー・プロファイルは、将来の**取り消し**日が指定されていない REVOKE 属性にのみ適用されます。取り消し日の管理は、以下で述べる REVOKEDT ポリシー・プロファイルによって制御されます。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、ユーザーの **CONNECT** を取り消すことを許可されません。この設定は、将来の**取り消し**日が指定されていない REVOKE キーワードに適用されます。

READ
端末ユーザーは、ユーザーの CONNECT を **REVOKE** することを許可されます。この設定は、将来の**取り消し**日が指定されていない REVOKE キーワードに適用されます。

UPDATE
READ と同じ。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、userid を取り消すことを許可されます。

- **C4R.CONNECT.ATTR.RESUME.***group.userid*

このポリシー・プロファイルは、将来の**再開**日が指定されていない RESUME 属性にのみ適用されます。再開日の管理は、以下で述べる RESUMEDT ポリシー・プロファイルによって制御されます。

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、ユーザーの CONNECT を再開することを許可されません。この設定は、将来の再開日が指定されていない RESUME キーワードに適用されます。

READ
NONE と同じ。

UPDATE
端末ユーザーは、ユーザーの CONNECT を RESUME することを許可されます。この設定は、将来の再開日が指定されていない即時の RESUME にのみ適用されます。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、ユーザーの CONNECT を再開することを許可されます。

- **C4R.CONNECT.ATTR.REVOKEDT.***group.userid*

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、*user* と *group* の間の CONNECT について、取り消し日を管理することを許可されません。この設定は、REVOKE(*date*) と NOREVOKE オプションの両方に適用されます。

READ
NONE と同じ。

UPDATE
端末ユーザーは、REVOKE(*date*) または NOREVOKE によって取り消し日を管理することを許可されます。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、*userid* から *group* への CONNECT の取り消し日を管理することを許可されます。

- **C4R.CONNECT.ATTR.RESUMEDT.***group.userid*

プロファイルが見つからない
この制御は実装されません。アクションは実行されません。

NONE
端末ユーザーは、*user* と *group* の間の CONNECT について、再開日を管理することを許可されません。この設定は、RESUME(*date*) と NORESUME オプションの両方に適用されます。

READ
NONE と同じ。

UPDATE
端末ユーザーは、RESUME(*date*) または NORESUME によって再開日を管理することを許可されます。

CONTROL
この制御は、端末ユーザーに対して実装されません。端末ユーザーは、*userid* から *group* への CONNECT の再開日を管理することを許可されます。

DATASET および一般リソースのプロファイルを管理するためのポリシー・プロファイル

このセクションのトピックでは、DATASET および一般リソースのプロファイルを管理するためのポリシー・プロファイルを実装する方法について説明します。

一般リソース・プロファイルは、RACF で 2 つの異なるコマンド・セットによって処理されます。 zSecure Command Verifier では、両方のタイプを指す用語として

リソース・プロファイル が使用されます。また、すべての zSecure Command Verifier ポリシー・プロファイルに関して、さまざまなタイプのリソース・プロファイルは実際に区別されていません。ただし、特定のリソース・クラスにとっては意味がないポリシーもあります。例えば、時間帯の設定はデータ・セットには適用されません。各ポリシーの説明では、このような個別の詳細は無視して、一般的な規則に焦点を合わせています。

以下に示すセクションでは、リソース・プロファイルに使用できる zSecure Command Verifier のさまざまなポリシー・プロファイルについて説明しています。新しいリソース・プロファイルを作成する権限に関するポリシーについては、204 ページの『リソース・プロファイルを作成するためのユーザー権限』で説明しています。これらのポリシーでは、グループ化リソース・クラス・プロファイルに対してメンバーを追加または削除する権限も記述されます。GCICSTRN に対する ADDMEM は、対応する TCICSTRN に対する RDEFINE とまったく同じように処理されます。ある特殊なポリシーが、データ・セットだけに実装されます。このポリシーでは、端末ユーザーを HLQ とするデータ・セット・プロファイルを保守する権限が記述されます。詳しくは、195 ページの『自分のデータ・セット・プロファイルを管理するためのポリシー・プロファイル』を参照してください。

DATASET プロファイルのポリシー・プロファイルが使用されるセクションでは、多くの場合、ターゲット・プロファイルが HLQ および残りの修飾子 (rest-of-profile) で表されます。

- HLQ は、RACF コマンドで使用される実際の DATASET プロファイルの高位修飾子を表します。これは、RACF コマンド内の引用符で囲まれたデータ・セット名に指定される最初の修飾子です。ポリシー・プロファイルで使用される HLQ には、命名規則テーブルからの変更が反映されません。この HLQ は、既存の**ユーザー** ID またはグループでなければなりません。
- rest-of-profile の値は、HLQ の後のすべての修飾子を示します。ほとんどの TSO ユーザーにとって、これは引用符で囲まれていないデータ・セット名として使用できる DATASET プロファイル名の一部分です。

プロファイルを 2 つの部分に分割すると、ほとんどのインストールにおいて rest-of-profile の部分を表すために総称が使用されるという事実が強調されます。一部のポリシー・プロファイルでは、HLQ に特殊な修飾子 =RACUID が反映される場合があります。HLQ という用語は、ある特定のポリシー・プロファイルの **APPLDATA** で指定されていることもあります。その場合は、RACF データベースで定義されている実際の DATASET プロファイルの最初の修飾子も表します。

リソース・プロファイルに関する次の重要事項はアクセスです。UACC およびアクセス・リストによるアクセスについては、220 ページの『UACC およびアクセス・リストの制御』で説明しています。

それ以外の項目 (リソース・プロファイルの所有者、リソース・プロファイルの詳細な識別情報 (ボリューム、装置、プロファイル・タイプ、RACF 標識)、属性、および監査など) については、以降のセクションを参照してください。

ポリシー・プロファイルでの総称文字と特殊文字

ポリシー・プロファイルのリソース・プロファイル部分を定義するには、以下のガイドラインに従ってください。

ポリシー・プロファイルのほとんどは、その名前にポリシーが適用されるリソース・クラスおよびリソース・プロファイルが含まれています。リソース・プロファイル部分には、総称パターンを使用できます。ただし、場合によっては、一般リソース・プロファイル (FACILITY クラス内のプロファイル ** など) に適用するポリシーを定義する必要があります。このリソース・プロファイルに特定のポリシー・プロファイルを定義することは簡単ではありません。総称プロファイルを効率よく保護できるようにするために、zSecure Command Verifier によってポリシー・プロファイルのリソース・プロファイル部分が変更されます。すべての総称文字が正符号 (+) で置き換えられます。このように、インストールでは特定の一般リソース・プロファイルに、ポリシーを実装する特定のポリシー・プロファイルを定義することができます。この変換を使用して、上記の FACILITY プロファイルを定義する権限が次のように記述されます。

```
C4R.FACILITY.ID.++
```

このプロファイルでは、FACILITY クラス内のプロファイル ** (およびプロファイル %% と %*) を作成する権限が記述されます。このポリシー・プロファイルは以下のように指定することもできます。

```
C4R.FACILITY.ID.**
```

ただし、この 2 番目のプロファイルは、FACILITY クラスに任意のプロファイルを作成する権限を制御します。%% で終わる総称プロファイル (C4R.FACILITY.ID.%%) は、FACILITY クラス内の 2 文字のプロファイルすべてを制御します。

この変換プロセスは、一部の特殊文字にも影響します。単一引用符は正符号に、スラッシュはピリオドに、それぞれ変換されます。特殊文字の変換は、GLOBAL リソース・クラス内のメンバーを効率よく処理できるようにするために行われます。

小文字の名前を持つプロファイル

zSecure Command Verifier のポリシーは、一致するポリシー・プロファイルが定義されているすべてのターゲット・クラスとターゲット・プロファイルに適用されます。

ポリシー・プロファイルのリソース・クラスとリソース・プロファイルで構成される部分は、総称パターンで表されることがよくあります。リソース・プロファイルの一部分を個別文字で指定することで、例外を実装できます。ただし、大/小文字混合プロファイルを許可しているクラスでは、特定の大/小文字混合プロファイルだけに例外を定義することはできません。代わりに、大文字、小文字、大/小文字混合の各リソース・プロファイルに、結果として得られた大文字のポリシー・プロファイルが適用されます。

zSecure Command Verifier ポリシー・プロファイルは、小文字をサポートしていないクラスで定義されます。小文字のリソース・プロファイルにポリシー・プロファイルを定義しようとすると、RACF コマンド・プロセッサーによってポリシー・プロファイルが直ちに大文字に変換されます。zSecure Command Verifier は、この動作に従って、リソース・プロファイルを大文字に変換してから一致するポリシー・プロファイルを特定します。以下の例は、この実装を表しています。

```
Resource profile     EJBROLE         Test.Role-       EJBROLE         TEST.ROLE
                     EJBROLE         test.role
```

```
Policy profile       C4R.EJBROLE.ID.TEST.ROLE

Command              rdefine xfacilit c4r.ejbrole.id.test.role
```

この例では、3 種類の EJBROLE プロファイルがすべて同じ zSecure Command Verifier ポリシー・プロファイルによって制御されます。ポリシー・プロファイルの作成に使用されるコマンドの大/小文字は、結果として得られるポリシー・プロファイルとは無関係です。

機能を追加する一般ポリシー・プロファイル

zSecure Command Verifier では現在 2 つの一般ポリシーが用意されており、これを使用して機能を追加することができます。

1 番目のポリシーは、一致する個別プロファイルが存在しない場合に、あいまいな LISTDSD コマンドに **GENERIC** キーワードを自動的に挿入します。これにより端末ユーザーは、**LISTDSD** コマンドを使用する際に個別プロファイルや総称プロファイルの有無を把握する必要がなくなります。2 番目のポリシーは、新規データ・セット・プロファイルまたは一般リソース・プロファイルを作成する際に使用できます。このポリシーは、現在の最適プロファイルを基に新しいプロファイルをモデル化するための FROM キーワードを自動的に挿入します。これにより、所有者、監査オプション、UACC、および ACL が、既存のプロファイルからコピーされるようにします。以下の表に、機能を追加するために使用できるコマンド、キーワード、およびプロファイル名を示します。

表 *33.* 機能を追加するために使用されるプロファイル

コマンド	キーワード	プロファイル
LISTDSD	*hlq.rest-of-profile*	**C4R.LISTDSD.TYPE.AUTO.***hlq.rest-of-profile*
ADDSD RDEFINE	*hlq.rest-of-profile*	**C4R.***class***.=FROM.***hlq.rest-of-profile*
ADDSD RDEFINE	*hlq.rest-of-profile*	**C4R.***class***./FROM.***hlq.rest-of-profile*
ADDSD RDEFINE	*hlq.rest-of-profile*	**C4R.***class***.FROM.***hlq.rest-of-profile*

最適総称プロファイルの自動検索

データ・セット・プロファイルの最適総称プロファイルを見つけるには、zSecure Command Verifier の自動検索を使用します。

これまでの経緯から、RACF ではデータ・セット・プロファイルが他のリソースとは別に処理されます。例えば、データ・セット・プロファイルの表示を要求すると、RACF はそのプロファイルが個別プロファイルであると見なします (総称文字が含まれる場合を除く)。この個別プロファイルが存在しない場合は、RACF から以下のメッセージが出力されます。

```
ICH35003I NO RACF DESCRIPTION FOUND FOR dataset_name
```

多くの場合、同じ **LISTDSD** コマンドに GEN キーワードを追加したものが次に実行されます。このキーワードを使用することで、最適総称プロファイルを表示できます。

同様に、一般リソース・プロファイルでは、**RLIST** コマンドによって個別プロファイルが表示されます (存在する場合)。ただし、**LISTDSD**コマンドとは異なり、**RLIST** では、個別プロファイルが見つからなかった場合に、最適総称プロファイルが自動

的に表示されます。RACFのユーザビリティー機能のように、zSecure Command Verifier でもデータ・セット・プロファイルに対して最適総称プロファイルを自動的に検索することができます。

- **C4R.LISTDSD.TYPE.AUTO.***hlq.rest-of-profile*

  このプロファイルが存在する場合、zSecure Command Verifier は要求されたプロファイルが存在するかどうかを検査します。要求されたプロファイルが存在しなければ、zSecure Command Verifier は LISTDSD コマンドに **GEN** キーワードを挿入して、最適プロファイルを検索します。アクセス・レベルによって、この機能を端末ユーザーに対してアクティブにするかどうかが制御されます。コマンドと存在しないプロファイルの特定の組み合わせには、いくつかの考慮事項があります。ほとんどのインストール済み環境では、*profile* が **.**** のような総称パターンで表されます。サポートされているアクセス・レベルは以下のとおりです。

  プロファイルが見つからない
  : この機能は実装されません。

  NONE
  : この機能は端末ユーザーに対して活動化されません。

  READ
  : 個別プロファイルが見つからなかった場合は、最適総称プロファイルが代わりに表示されます。

  UPDATE
  : READ と同じ。

  CONTROL
  : READ と同じ。

注**:**

1. 指定されたプロファイルに総称文字が含まれている場合は、この特定の zSecure Command Verifier 処理がバイパスされます。ユーザーが、次の最適総称プロファイルではなく、指定されたプロファイルの表示を望んでいるものと見なされます。このプロファイルが存在しない場合は、RACF から適切なエラー・メッセージが表示されます。
2. 端末ユーザーが特定のボリュームの個別プロファイルを要求した場合に、個別プロファイルが存在しなかったときは、最適総称プロファイルが表示されます。
3. 端末ユーザーが特定のボリュームの個別プロファイルを要求したとき、別のボリュームに個別プロファイルが定義されていると、RACF により、ボリュームの個別プロファイルが見つからなかったことを端末ユーザーに通知するエラー・メッセージが表示されます。
4. 最適総称の自動検索が望ましくない場合は、LISTDSD コマンドに **NOGENERIC** キーワードを指定することによって、コマンド単位で自動検索機能を使用不可にできます。
5. 個別プロファイルが存在する場合でも、それが特定のデータ・セットの保護に使用されるわけではありません。また、保護は、正しい volser、および VTOC (または ICF カタログ) での RACF 標識付きビットの設定にも依存します。

最適総称に基づいたプロファイルのモデル化

MODEL ポリシー・プロファイルを、対応するユーザー・プロファイルおよびグループ・プロファイルとともに使用して、データ・セットなどのリソースへのアクセス管理に役立てます。

RACF 管理者は、特定のリソースへのアクセスを制御する新しいプロファイルの定義を頻繁に依頼されます。ほとんどの場合、リソースへのアクセスは既に何らかのプロファイルによって制御されています。例えば PROTECTALL 環境では、すべてのデータ・セット・プロファイルをプロファイルで制御する必要があります。RACF は、新規データ・セット・プロファイルまたは一般リソース・プロファイルを定義する際に、UACC(NONE) のプロファイルと空のアクセス・リストをデフォルトで作成します。この一般規則に例外が発生する可能性があるのは、NOADDCREATOR オプションが設定されていない場合、端末ユーザーの UACC の設定が NONE 以外である場合、または端末ユーザーに GRPACC 属性がある場合です。データ・セットには、対応するユーザー・プロファイルおよびグループ・プロファイルとともに**モデル**・プロファイルがインストール済み環境で明確に定義されていて、その**モデル**・プロファイルが使用されるように設定されている場合があります。ただし、**モデル**・プロファイルを使用するには、現在のアクセス権限が適切に記述されるようにモデル・プロファイルを保守する必要があります。また、それは一般リソース・プロファイルに適用されることはありません。

新しいプロファイルをより柔軟に作成できるようにするために、RACF では **ADDSD**、**RDEFINE**、および **PERMIT** の各コマンドに FROM キーワードを用意しています。ただし、この機能を効果的に使用するためには、RACF 管理者による手間が必要となります。多くの場合、プロファイルを作成するには、まだ一連のコマンドが必要です。管理者は、新規のユーザー・プロファイルまたは特定性の高いプロファイルを定義する際、現行ユーザーをロックアウトすることは避けます。これは、ユーザーをロックアウトすると、本番環境に深刻な影響が生じる可能性があるためです。以下の例では、最初のコマンドで、データ・セットへのアクセスを現在制御しているプロファイルを検出します。この例では、データ・セットがプロファイル PAYROLL.EMPLOYEE.** によって制御されていました。2 番目のコマンドでは、このプロファイルが新しいプロファイルのモデルとして使用されています。3 番目のコマンドでは、Q4 ファイルへのアクセスを必要としていたユーザー ID またはグループにアクセス権限が付与されています。

```
LISTDSD DA('PAYROLL.EMPLOYEE.Q4.Y2003') GEN
ADDSD 'PAYROLL.EMPLOYEE.Q4.**' FROM('PAYROLL.EMPLOYEE.**')
PERMIT 'PAYROLL.EMPLOYEE.Q4.**' ID(PAYTMP) AC(UPDATE)
```

zSecure Command Verifier には、現在のリソース・プロファイルに基づいて FROM キーワードを自動的に挿入する機能があります。例えば、この機能を DATASET クラス全体に対して使用可能にすると、管理者はリソースの現在のアクセス・リストや UACC を確認しなくても、以下の 2 つのコマンドを実行できます。

```
ADDSD 'PAYROLL.EMPLOYEE.Q4.**'
PERMIT 'PAYROLL.EMPLOYEE.Q4.**' ID(PAYTMP) AC(UPDATE)
```

自動モデル化機能は、リソース・クラス単位またはリソース・プロファイル単位で活動化できます。ほとんどのインストール場所では、プロファイルの *class* または HLQ のみが使用され、ポリシー・プロファイルの残りのリソース・プロファイル部分にはおそらく総称が使用されます。

- **C4R.***class***.=FROM.***hlq.rest-of-profile*

  このポリシー・プロファイルが存在し、端末ユーザーに適切なアクセス権限があれば、zSecure Command Verifier によってプロファイルの APPLDATA を取得して、**RDEFINE** コマンドまたは **ADDSD** コマンドで使用されるリソース・プロファイルを見つけます。*hlq.rest-of-profile* では、定義される新しいプロファイルが記述されます。このプロファイルは必須値ポリシー・プロファイルであるため、端末ユーザーが FROM キーワードに指定した値を上書きします。代わりに、**APPLDATA** フィールドで検出された値が使用されます。

  ポリシー・プロファイル内の修飾子 =FROM を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

  プロファイルが見つからない
  : この機能は実装されません。

  NONE
  : この機能は端末ユーザーに対して活動化されません。端末ユーザーが入力した RACF コマンドに、必須の FROM モデル・プロファイルは挿入されません。

  READ
  : ポリシー・プロファイルの APPLDATA が取得され、モデルとして使用されるプロファイルを決定するために使用されます。

  UPDATE
  : READ と同じ。

  CONTROL
  : この制御は、端末ユーザーに対してアクティブにはされません。端末ユーザーが入力した RACF コマンドに、FROM モデル・プロファイルは挿入されません。

  端末ユーザーが必須値ポリシー・プロファイルに対する READ 権限または UPDATE 権限を持っている場合は、zSecure Command Verifier によってポリシー・プロファイルの APPLDATA が取得され、使用されます。現在サポートされている APPLDATA の値を、次のセクションで示します。

- **C4R.***class***./FROM.***hlq.rest-of-profile*

  このポリシー・プロファイルが存在し、端末ユーザーに適切なアクセス権限があれば、zSecure Command Verifier によってプロファイルの APPLDATA を取得して、**RDEFINE** コマンドまたは **ADDSD** コマンドで使用されるリソース・プロファイルを見つけます。*hlq.rest-of-profile* では、定義される新しいプロファイルが記述されます。

  ポリシー・プロファイル内の修飾子 /FROM を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。サポートされているアクセス・レベルは以下のとおりです。

  プロファイルが見つからない
  : この機能は実装されません。

NONE
この機能は端末ユーザーに対して活動化されません。コマンドにデフォルトの FROM モデル・プロファイルは挿入されません。

READ
ポリシー・プロファイルの APPLDATA が取得され、モデルとして使用されるプロファイルを決定するために使用されます。

UPDATE
READ と同じ。

CONTROL
この制御は、端末ユーザーに対してアクティブにはされません。端末ユーザーが入力した RACF コマンドに、FROM モデル・プロファイルは挿入されません。

端末ユーザーがデフォルト値ポリシー・プロファイルに対する READ 権限または UPDATE 権限を持っている場合は、zSecure Command Verifier によってポリシー・プロファイルの APPLDATA が取得され、使用されます。現在サポートされている APPLDATA の値を、次のセクションで示します。

- **C4R.***class***.FROM.***hlq.rest-of-profile*

このポリシー・プロファイルは、端末ユーザーが新規のデータ・セットまたは一般リソース・プロファイルを追加する際に、FROM キーワードの使用を許可されるかどうかを制御します。上記の必須値ポリシー・プロファイルまたはデフォルト値ポリシー・プロファイルのいずれかが使用される場合、このプロファイルは使用されません。*hlq.rest-of-profile* では、定義される新しいプロファイルが記述されます。このポリシー・プロファイルには、コマンドで使用されるモデル・プロファイルの名前が含まれません。サポートされているアクセス・レベルは以下のとおりです。

プロファイルが見つからない
この機能は実装されません。

NONE
FROM キーワードは許可されません。

READ
NONE と同じ。

UPDATE
指定された FROM キーワードは許可されます。

CONTROL
この制御は、端末ユーザーに対してアクティブにはされません。

端末ユーザーが必須値またはデフォルト値ポリシー・プロファイルに対する READ 権限または UPDATE 権限を持っている場合は、zSecure Command Verifier によってポリシー・プロファイルの APPLDATA が取得されます。
C4R.*class***.FROM.***hlq.rest-of-profile* の **APPLDATA** フィールドは使用されません。

APPLDATA フィールドは、以下の値タイプにすることができます。

BLANK
このタイプは、FROM プロファイルを明示的に挿入してはならないことを

示すために使用されます。必須値ポリシー・プロファイルの場合は、端末ユーザーが入力したコマンドに指定されている FROM 値が除去されることを意味します。後続の RACF デフォルト処理では、USER または GROUP 固有の MODEL プロファイルが使用される可能性があります (このプロファイルが定義され、かつモデル化が有効である場合)。

=BESTFIT
この値は、zSecure Command Verifier が現在の最適プロファイルを探し、検出したプロファイルを FROM プロファイルの値として使用することを指定します。このプロファイルは、新しいリソース・プロファイルと同じリソース・クラスにあります。プロファイルが見つからない場合は、APPLDATA の値が BLANK である場合と同じように処理が行われます。

profile それ以外の値は、モデルとして使用されるリソース・プロファイルであると見なされます。このリソース・プロファイルが存在しない場合は、最終的にコマンド全体が失敗し、RACF メッセージ ICH09036I が表示されます。

RACF プロファイル管理

zSecure Command Verifier には、RACF プロファイル管理用にいくつかのポリシーが用意されています。

これらのポリシーのリストを表 34 に示しています。これらを使用して、以下の権限を制御することができます。

- 自分のデータ・セットを管理する権限
- 自身に権限を与える権限 (**ユーザー** ID または**グループ**で)
- 特定性の高いプロファイルを作成する (切り捨てる) 権限
- システム・リソースを管理する権限 (レベルで識別)
- リソースに UPDATE 権限を付与する権限 (レベルで識別)

プロファイルの詳しい説明については、表に続く各セクションを参照してください。

表 *34.* プロファイル管理に使用される一般プロファイル

コマンド	キーワード	プロファイル
ADDSD DELDSD ALTDSD PERMIT	*profile*	**C4R.DATASET.ID.=RACUID.***rest-of-profile*
PERMIT	*userid*	**C4R.***class.***ACL.=RACUID.***access.profile*
PERMIT	*group*	**C4R.***class.***ACL.=RACGPID.***access.profile*
CONNECT	*userid*	**C4R.CONNECT.ID.***group.***=RACUID**
REMOVE	*userid*	**C4R.REMOVE.ID.***group.***=RACUID**
ADDSD RDEFINE	*profile*	**C4R.***class.***=UNDERCUT.***current-profile*
ADDSD DELDSD ALTDSD PERMIT	*profile*	**C4R.DATASET.=NOCHANGE.***dsname*
RDEF RDEL RALT PERMIT	*profile*	**C4R.***class.***=NOCHANGE.***profile*
ADDSD DELDSD ALTDSD PERMIT	*profile*	**C4R.DATASET.=NOUPDATE.***dsname*

表 34. プロファイル管理に使用される一般プロファイル (続き)

コマンド	キーワード	プロファイル
RDEF RDEL RALT PERMIT	*profile*	**C4R.***class.***=NOUPDATE.***profile*

自分のデータ・セット・プロファイルを管理するためのポリシー・プロファイル

自分のデータ・セット・プロファイルを管理する権限を制御する機能は、*No-Store* 機能とも呼ばれます。この名前は、ACF2 システムで使用可能な制御が元になっています。

標準の RACF では、すべてのユーザーが、HLQ がユーザー ID と同じであるデータ・セット・プロファイルを追加、削除、および変更することができます。RACF ではこの動作を簡単に変更することができません。主な方法は、命名規則テーブルを作成して、HLQ がユーザー ID と同じにならないようにすることです。この方法には、命名規則テーブルの使用に関連する明らかな欠点があります。代わりに、いくつかのインストール・システム出口を作成する方法もあります。zSecure Command Verifier では、RACF コマンドに対するこの機能が外部化されています。以下の表に、自分のデータ・セット・プロファイルを管理するためのコマンド、キーワード、およびプロファイルを示します。表に続くセクションで、このプロファイルについて詳しく説明します。

表 35. *RACF* リソースの検証に使用されるプロファイル： この表の項目は、新しいリソースの名前を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD DELDSD ALTDSD PERMIT	*profile*	**C4R.DATASET.ID.=RACUID.***rest-of-profile*

No-Store 機能を使用した場合に、分散システム管理者に、その管理者が所属する部門のすべてのユーザー (管理者自身は除く) のすべてのデータ・セット・プロファイルを作成および保守する権限が付与されるという、予期しない結果が生じる可能性があります。

- **C4R.DATASET.ID.=RACUID.***rest-of-profile*

  データ・セット・プロファイルの HLQ が端末ユーザーのユーザー ID と一致する場合は、208 ページの『RACF リソース・プロファイルを作成するためのポリシー・プロファイル』で説明している他のどのポリシー検査よりも前に、このポリシーが検査されます。ユーザーが十分なアクセス権限を持っていない場合、コマンドが拒否され、処理が停止します。このポリシーがターゲット・プロファイルの管理を妨げない場合、他の適用可能なポリシー (例えば、ACL 用) が後続の処理中に評価されます。*rest-of-profile* の値は、HLQ の後のすべての修飾子を示します。ほとんどの TSO ユーザーにとって、*rest-of-profile* はデータ・セット名の一部分であり、引用符で囲まれていないデータ・セット名として使用できます。ほとんどの場合、** などの総称文字を使用して *rest-of-profile* を表します。

  ポリシー・プロファイル内の修飾子 `=RACUID` を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

アクセス・レベルには以下のものがあります。

プロファイルが見つからない
: この制御は実装されません。コマンド処理を続行します。

NONE
: 端末ユーザーは、自身の DATASET プロファイルを管理するための権限を持っていません。コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、自身のデータ・セット・プロファイルを管理することを妨げられません。コマンド処理は、他のポリシーの検査を続けます。

CONTROL
: UPDATE と同じ。

自己許可に対するポリシー・プロファイルの選択

自己許可機能は、セキュリティー管理者とデータ (またはアプリケーション) 管理者の間で責任を厳密に分ける必要がある多くの組織で必要となります。

システム・セキュリティー・ポリシーで、セキュリティー管理者にアプリケーション・リソースへのアクセス権限を付与してはならないことを指定している場合が少なくありません。標準 RACF では、システム SPECIAL またはグループ SPECIAL を持つユーザーは、自己の制御下にあるプロファイルを変更できます。セキュリティー管理者に現時点でアプリケーション・リソースへのアクセス権限がなくても、管理者は容易にアクセス権限を取得できます。組織によっては、SMF データを分析して、アプリケーション・データやリソースへのアクセス権限を自身に付与した管理者に関するレポートを作成しています。zSecure Command Verifier では、セキュリティー管理者がリソース・プロファイルの ACL を変更してリソースへのアクセス権限を取得することを防ぐ、いくつかのポリシーが提供されています。

以下の表に、自己許可を制御するためのコマンド、キーワード、およびプロファイルを示します。各プロファイルについて詳しくは、表に続くセクションを参照してください。

表 *36.* 自己許可の制御に使用されるプロファイル： この表の項目は、ACL 項目または CONNECT を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
PERMIT	*userid*	**C4R.***class*.**ACL.=RACUID.***access.profile*
PERMIT	*group*	**C4R.***class*.**ACL.=RACGPID.***access.profile*
CONNECT	*userid*	**C4R.CONNECT.ID.***group*.**=RACUID**
REMOVE	*userid*	**C4R.REMOVE.ID.***group*.**=RACUID**

これらのプロファイルは、*userid* が端末ユーザーであるか、または *group* がユーザーの接続グループのいずれかである場合にのみ適用されます。この状態が当てはまる場合、zSecure Command Verifier は前述のプロファイルを使用します。アクセス・リストの変更がポリシーによって防止されていない場合は、 220 ページの『UACC およびアクセス・リストの制御』 に記載されているように、処理が続行

され、他の ACL ポリシーが検査されます。最初の 2 つのプロファイルとサポートされるアクセス・レベルについては、このセクションで詳しく説明します。CONNECT および REMOVE 用のポリシー・プロファイルについて詳しくは、168 ページの『自分自身を接続するための権限』を参照してください。

- **C4R.***class*.**ACL.=RACUID.***access.profile*

  このプロファイルは、端末ユーザーが PERMIT コマンドを実行して自分のアクセス・レベルを変更するための権限を指定するために使用されます。また、**PERMIT** コマンドの **DELETE** オプションにも適用されます。このプロファイルを実装する場合は、必ず SETROPTS NOADDCREATOR オプションを設定してください。これを設定しないと、RACF 管理者がリソース・プロファイルのアクセス・リストに自動的に追加されるおそれがあります。この場合、管理者がその問題のアクセス・レベルを除去する可能性はありません。

  ポリシー・プロファイル内の修飾子 =RACUID を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。端末ユーザーは、アクセス・リストで自分自身を追加、変更、または削除することを妨げられません。

  NONE
  : 端末ユーザーは、アクセス・リストで自分自身を追加、変更、または削除することができません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、アクセス・リストで自分自身を追加、変更、または削除することを妨げられません。

  CONTROL
  : UPDATE と同じ。

- **C4R.***class*.**ACL.=RACGPID.***access.profile*

  このプロファイルは、端末ユーザーが **PERMIT** コマンドを実行して自身が接続されているグループのアクセス・レベルを変更するための権限を指定するために使用されます。また、**PERMIT** コマンドの **DELETE** オプションにも適用されます。このオプションを実装する場合は、端末ユーザーまたはすべてのグループ接続に GRPACC 属性が指定されていないことを確認してください。そうでないと、RACF 管理者の現在のグループがデータ・セット・プロファイルのアクセス・リストに自動的に追加されるおそれがあります。この場合、管理者がその問題のアクセス・レベルを除去する可能性はありません。

  ポリシー・プロファイル内の修飾子 =RACGPID を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。端末ユーザーは、アクセス・リストで自身の接続グループを追加、変更、または削除することを妨げられません。

NONE
端末ユーザーは、アクセス・リストで自身の接続グループを追加、変更、または削除することができません。

READ
NONE と同じ。

UPDATE
端末ユーザーは、アクセス・リストで自身の接続グループを追加、変更、または削除することを妨げられません。

CONTROL
UPDATE と同じ。

特定性の高いプロファイルを作成するためのユーザー権限

リソース・プロファイルを作成する権限を制御するのに役立つ切り捨てプロファイル を作成するには、以下のガイドラインに従ってください。

204 ページの『リソース・プロファイルを作成するためのユーザー権限』で説明しているように、RACF では複数の方法でプロファイルの作成 (定義) が制御されます。データ・セット・プロファイルの場合は、HLQ のみを使用して権限が決定されます。この許可プロセスでは、既存の総称プロファイルが使用されません。一般にこのような場合、グループ管理者または GROUP 内の CREATE 権限を持つユーザーが、既存のアクセス制御の効果を損なうような特定性の高い総称プロファイルを (場合によっては、個別プロファイルさえも) 定義するおそれがあります。特定性の高いプロファイルは RACF で使用され、それまでの最適プロファイルは、その UACC と ACL も含めて、一部のリソースに対して使用されなくなります。

一般リソースの場合、RACF は CLAUTH を `GENERICOWNER` と組み合わせて使用して、新しいプロファイルを定義できるユーザーを制御します。

zSecure Command Verifier には、特定性の高いプロファイルの作成を防ぐために使用できる汎用機能があります。特定性の高いプロファイルを作成するプロセスを、既存のプロファイルの切り捨て と呼ぶ場合があることから、このマニュアルの残りの部分では、これらのプロファイルを切り捨てプロファイル と呼びます。

注**:** 現時点では、zSecure Command Verifier には ADDMEM を使用した既存のグループ化プロファイル内の既存のメンバーの切り捨てを防ぐ同様の機能はありません。

以下の表に、特定性の高いプロファイルの作成を防ぐために zSecure Command Verifier で提供されている制御を示します。リソース・クラスの状況 (RACLIST 処理されているかどうか) によっては、`RDEFINE` の使用が制限される場合があります。

表 *37. RACF* リソースの検証に使用されるプロファイル： この表の項目は、新しいリソースの名前を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD RDEFINE	*profile*	**C4R.***class***.=UNDERCUT.***current-profile*

プロファイルを作成する権限は、現在の最適プロファイルを含んでいるポリシー・プロファイルによって制御されます。この最適プロファイルに総称文字が含まれている場合は、zSecure Command Verifier ポリシー・プロファイル内でそれらの総称文字が正符号 (+) で表されます。ポリシー・プロファイルでの総称文字の変換については、 187 ページの『ポリシー・プロファイルでの総称文字と特殊文字』で説明しています。例えば、以下のデータ・セット・プロファイルが存在するとします。

```
ABC.**
ABC.TEST*.**
```

データ・セット・プロファイルの定義:

```
ABC.TEST1.PROF*
```

は、以下の定義によって制御されます。

```
C4R.DATASET.=UNDERCUT.ABC.TEST+.++
```

これは、以下の zSecure Command Verifier ポリシー・プロファイルによる対象とすることができます。

```
C4R.DATASET.=UNDERCUT.**
```

以下のセクションでは、RACF リソース・プロファイルを切り捨てるためのポリシー・プロファイル、および対応するアクセス・レベルについて説明します。これらのプロファイルは、他の zSecure Command Verifier ポリシー・プロファイルおよび定義済みのポリシーに対する標準の RACF プロファイル作成権限 (204 ページの『リソース・プロファイルを作成するためのユーザー権限』を参照) に加えて使用されます。

- **C4R.***class***.=UNDERCUT.***current-profile*

  このプロファイルでは、*current-profile* を切り捨てるリソース・プロファイルを作成する権限が記述されます。*current profile* は、新しいプロファイルの対象とされるリソースを保護するために RACF で使用されているプロファイルです。つまり、*current-profile* は切り捨てられる既存のプロファイルであって、切り捨てを行う新しいプロファイルではありません。

  ポリシー・プロファイル内の修飾子 `=UNDERCUT` を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  アクセス・レベルには以下のものがあります。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : ユーザーは、新規プロファイルの定義を許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、十分な RACF 権限があれば、プロファイルを作成できます。

CONTROL
UPDATE と同じ。

ロックされたリソース・プロファイルを管理するためのユーザー権限

特定のプロファイル (APF 許可データ・セットを保護するプロファイルなど) に対する変更を制御するのに役立つプロファイルを作成するには、以下のガイドラインに従ってください。

この機能は、*No-Change* 機能とも呼ばれます。この名前は、この制御を使用して特定のプロファイルへの変更を防止できることを意味します。この機能が最もよく使用されるのは、APF 許可データ・セットなどのシステム・リソースを保護するプロファイルをユーザーが更新できないようにする場合です。予想されるすべてのリソースを個々の RACF コマンドで自動的に認識することは困難であるため、zSecure Command Verifier では間接的な方法を実装してこの問題に対応しています。特殊な =NOCHANGE ポリシー・プロファイルを使用して、ターゲット・プロファイルの特性が定義されます。この特性がターゲット・プロファイルにある場合は、以下のシナリオで示すように、ターゲット・プロファイルを変更するためにポリシー・プロファイルに対する追加のアクセス権限が必要になります。

データ・セット SYS1.LINKLIB に対してこの追加の制御を実装すると想定して、以下のポリシー・プロファイルを定義します。

```
C4R.DATASET.=NOCHANGE.SYS1.** APPLDATA('LEVEL=99')
```

このポリシー・プロファイルは、LEVEL の指定が 99 であるすべての SYS1 データ・セットに、この追加の制御が必要であることを表しています。SYS1.LINKLIB に対してこの制御を活動化するには、データ・セット・プロファイルの LEVEL に値 99 を指定します。このデータ・セットがプロファイル SYS1.LINK* の対象とされると想定して、以下のコマンドを使用します。

```
ALTDSD 'SYS1.LINK*' LEVEL(99)
```

=NOCHANGE プロファイルで SYS1.** を使用することで、特定のレベルのすべての SYS1 データ・セットが制御されることを 1 つのポリシー・プロファイルだけで指定できます。同時に、SYS1 以外のすべてのデータ・セットが制御されないことも暗黙的に指定できます。この No-Change 機能ですべてのデータ・セットを制御する場合は、代わりに以下のポリシー・プロファイルを使用できます。

```
C4R.DATASET.=NOCHANGE.** APPLDATA('LEVEL=99')
```

ほとんどのコマンドで、リソース・プロファイルが制御されるかどうかを決定するために使用される特性が、RACF コマンドで指定されるプロファイルから取得されます。ただし、**ADDSD** コマンドと **RDEFINE** コマンドからはこの特性を取得できません。この 2 つのコマンドに関しては、現在の最適プロファイルからこの特性が取得されます。

事実上、これによって、 198 ページの『特定性の高いプロファイルを作成するためのユーザー権限』で説明している切り捨て制御が適用されます。No-Change ポリシーの効果を損なう、より適切なプロファイルを追加することはできません。同様に、現在 No-Change ポリシーを適用しているプロファイルを除去することもできません。これは複数の制御ポリシーの混合と見ることもできますが、1 つのプロファイルの使用によって、特定のリソース・ブロックが立ち入り禁止であることを効

果的に示せます。前述の例では、次の最適プロファイルを使用することで、以下の例に示すような LEVEL(00) が指定された SYS1.LINKLIB などのプロファイルの作成が防止されます。

```
ADDSD 'SYS1.LINKLIB' GENERIC LEVEL(00)
```

LEVEL(00) を指定すると、リソース・プロファイルが =NOCHANGE ポリシーから事実上外されます。これは許可してはならないステップです。=NOCHANGE ポリシーに最適プロファイルを使用すると、このルールが適用されます。同様に、コマンド

```
DELDSD 'SYS1.LINK*' GENERIC
```

は、そのプロファイルの対象とされるすべてのデータ・セットから現在の No-Change ポリシーも除去してしまうため、許可されません。次の最適プロファイル (SYS1.**) には、LEVEL(99) が指定されていない可能性が高いため、これらのデータ・セットに対しては =NOCHANGE ポリシーが無効になります。これは許可されません。

ポリシー・プロファイルへのアクセス権限によって、プロファイルの変更が許可されるかどうかが決まります。

以下の表は、データ・セット dsname 用の行と一般リソース (プロファイル) 用の行の 2 行に分かれています。このトピックの残りの部分では、データ・セットを別途取り上げるのではなく、*class* の値が DATASET となっている特殊なケースとして扱います。

表 *38. RACF* リソースの検証に使用されるプロファイル： この表の項目は、新しいリソースの名前を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD DELDSD ALTDSD PERMIT	*profile*	**C4R.DATASET.=NOCHANGE.***dsname*
RDEF RDEL RALT PERMIT	*profile*	**C4R.***class***.=NOCHANGE.***profile*

現在使用可能な **APPLDATA** のアクセス・レベルと値は以下のとおりです。

- **C4R.***class***.=NOCHANGE.***profile*

  ポリシー・プロファイルの **APPLDATA** は、権限を追加しないと変更できないプロファイルを識別するために使用するターゲット・プロファイルの特性を示すために使用されます。*profile* の値は、データ・セット名または一般リソース・プロファイルを表します。ほとんどの場合、*profile* は「.**」などの総称文字で表されます。

  ポリシー・プロファイル内の修飾子 =NOCHANGE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  1 タイプの特性のみが実装されています。**APPLDATA** に指定できる値は以下のとおりです。

  LEVEL= *nn*
  プロファイルの LEVEL は、プロファイルの変更に対する追加の制御が

必要かどうかを示すために使用されます。ターゲットの LEVEL に *nn* が指定されている場合は、ターゲット・プロファイルを変更するために少なくともポリシー・プロファイルに対する UPDATE 権限が必要となります。

アクセス・レベルには以下のものがあります。

プロファイルが見つからない
: この制御は実装されません。ターゲット・プロファイルの変更は防止されません。

NONE
: ターゲット・プロファイルが **APPLDATA** で指定された要件に適合する場合、端末ユーザーはターゲット・プロファイルの変更を許可されません。

READ
: NONE と同じ。

UPDATE
: ターゲット・プロファイルが端末ユーザーの通常の RACF 権限の範囲内にあれば、端末ユーザーはターゲット・プロファイルを変更できます。

CONTROL
: UPDATE と同じ。

UPDATE 権限を制御するためのポリシー・プロファイルの選択

特定のプロファイルへの UPDATE 権限の付与を制御するポリシー・プロファイルを作成するには、以下のガイドラインに従ってください。

この機能は、*No-Update* 機能とも呼ばれます。この名前は、この制御を使用して特定のプロファイルへの UPDATE 権限の付与を防止できることを意味します。このポリシーの対象とされるリソースは、リソース・プロファイルの LEVEL とリソースの名前の組み合わせで識別できます。通常の**アクセス** 制御機構との主な違いは、プロファイルの LEVEL でリソースを選択できる点です。この選択方法を使用することで、1 つのポリシー・プロファイルを使用してこの規則を別々のリソース・セットに適用できます。

このプロセスを、例を使ってわかりやすく説明します。この追加の制御を以下のデータ・セットに対して実装するとします。

```
ACCPAY.JCLLIB
ACCPAY.PARMLIB
```

以下のポリシー・プロファイルを定義できます。

```
C4R.DATASET.=NOUPDATE.ACCPAY.**         APPLDATA('LEVEL=98')
```

このポリシー・プロファイルは、LEVEL の指定が「98」であるすべての ACCPAY データ・セットに、この追加の制御が必要であることを示します。この制御を 2 つの ACCPAY データ・セットに対して実行するには、データ・セット・プロファイルの LEVEL に値「98」を指定する必要があります。データ・セットが完全修飾総称プロファイルの対象とされると想定して、以下の 2 つのコマンドを使用できます。それ以外の ACCPAY を含むデータ・セットはいずれも、個別プロファイルまたは総称プ

ロファイルで定義できます。また、この 2 つのデータ・セット・プロファイルを 1 つの総称プロファイルの対象にすることは簡単ではありません。

```
ALTDSD 'ACCPAY.JCLLIB'  GEN LEVEL(98)
ALTDSD 'ACCPAY.PARMLIB' GEN LEVEL(98)
```

=NOUPDATE プロファイルで ACCPAY.** を使用することにより、1 つのポリシー・プロファイルを複数のリソースに適用できます。追加のリソースを同じく UPDATE アクセスから保護する必要がある場合は、適切な LEVEL 値を指定した対応する総称 (または個別) プロファイルを追加します。既存のポリシー・プロファイルを変更する必要はありません。ポリシー・プロファイルは、他の高位修飾子 (HLQ) が関係する場合にのみ拡張する必要があります。複雑さを軽減し、起こり得る混乱を避けるために、すべての =NOUPDATE ポリシー・プロファイルで、**APPLDATA** によって該当する LEVEL に同じ値を指定するようにしてください。

ほとんどのコマンドで、RACF コマンドで指定されるプロファイルから LEVEL が取得されます。ただし、**ADDSD** コマンドと **RDEFINE** コマンドではそれが不可能です。この 2 つのコマンドに関しては、現在の最適プロファイルから LEVEL が取得されます。事実上、これによって、 202 ページの『UPDATE 権限を制御するためのポリシー・プロファイルの選択』で説明している切り捨て制御が適用されます。これは複数の制御ポリシーの混用と見ることもできますが、特定のリソース・ブロックが立ち入り禁止であることを 1 つのプロファイルで効果的に示すことができます。前述の例では、これによって、例えば LEVEL(00) が指定された ACCPAY.JCLLIB に対して以下のコマンドで個別プロファイルが作成されることを防ぎます。

```
ADDSD 'ACCPAY.JCLLIB' LEVEL(00)
```

LEVEL(00) を指定すると、リソース・プロファイルが =NOUPDATE ポリシーから事実上外されます。これは、zSecure Command Verifier によって明示的に防止されます。

UPDATE アクセスに対する、選択したすべてのデータ・セットの完全で一貫した制御を実現するには、関係するすべてのデータ・セットの LEVEL 値の管理も制御する必要があります。適用可能なポリシー・プロファイルについて詳しくは、 245 ページの『その他のポリシー・プロファイルとアクセス・レベルの説明』の **C4R.***class*.**LEVEL.***level*.*profile* の説明を参照してください。

ポリシー・プロファイルに対するアクセス権限によって、UPDATE 権限の付与が許可されるかどうかが決まります。

表 *39. NOUPDATE* 制御に使用されるプロファイル： この表の項目は、影響を受けるプロファイルを記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD DELDSD ALTDSD PERMIT	*profile*	**C4R.DATASET.=NOUPDATE.***dsname*
RDEF RDEL RALT PERMIT	*profile*	**C4R.***class*.**=NOUPDATE.***profile*

この表は、データ・セット用と一般リソース用の 2 行に分かれています。データ・セットは別途提供されるわけではありませんが、*class* の値が DATASET となっている特殊なケースとして扱われます。現在使用可能な **APPLDATA** のアクセス・レベルと値は以下のとおりです。

- **C4R.***class*.**=NOUPDATE.***profile*

  ポリシー・プロファイルの **APPLDATA** を使用して、ターゲット・プロファイルの LEVEL が指定されます。これは、UPDATE アクセスから保護する必要があるリソース・プロファイルの ID として使用されます。*profile* の値は、データ・セット名または一般リソース・プロファイルを表します。ほとんどの場合、「**.****」などの総称文字を使用してプロファイルを表します。

  ポリシー・プロファイル内の修飾子 =NOUPDATE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  現時点では、1 タイプの特性のみが実装されています。**APPLDATA** に指定できる値は以下のとおりです。

  LEVEL= *nn*
  ターゲット・リソース・プロファイルの LEVEL は、そのプロファイルの変更に対する追加の制御が必要かどうかを示すために使用されます。ターゲットの LEVEL に *nn* が指定されている場合は、ターゲット・プロファイルへの UPDATE 権限の付与を許可するために、少なくともポリシー・プロファイルに対する UPDATE 権限が必要となります。

  アクセス・レベルには以下のものがあります。

  プロファイルが見つからない
  この制御は実装されません。ターゲット・プロファイルへの UPDATE 権限の付与は防止されません。

  NONE
  ターゲット・プロファイルが **APPLDATA** で指定された LEVEL と一致する場合、端末ユーザーはターゲット・プロファイルへの UPDATE 権限の付与を許可されません。

  READ
  NONE と同じ。

  UPDATE
  ターゲット・プロファイルが端末ユーザーの通常の RACF 権限の範囲内にあれば、端末ユーザーはターゲット・プロファイルに UPDATE 権限を付与できます。

  CONTROL
  UPDATE と同じ。

リソース・プロファイルを作成するためのユーザー権限

RACF では、いくつかの方法で、ユーザーに新しいリソース・プロファイルの作成を許可することができます。

データ・セットの場合、RACF は HLQ をメインの基準として使用します。以下のいずれかの条件が真である場合に、データ・セット・プロファイルの作成が許可されます。

- HLQ がユーザー ID と同じである。
- HLQ がグループであり、そのグループ内で端末ユーザーに CREATE 権限が付与されている。
- HLQ が、グループ SPECIAL の範囲内にあるユーザー ID またはグループである。
- HLQ が、グループ OPERATIONS の範囲内にあるグループである。

一般リソースの場合、RACF はリソース・クラス内の CLAUTH をメインの基準として使用します。通常の一般リソース・クラスの場合は、新しいリソース・プロファイルを作成する権限を、SETROPTS コマンドの GENERICOWNER 設定によってさらに制限することができます。最も単純な形式では、それは自分のものでない既存の総称プロファイルを切り捨てることを防止する方法として記述することができます。ただし、リソース・クラスをグループ化して新しい総称メンバーを追加する場合には機能しません。

注**:** RACF の一部のリリースでは、GENERICOWNER がアクティブでない場合でも、最上位に総称プロファイルがあるために、個別の一般リソース・プロファイルをユーザーが定義できません。GENERICOWNER がアクティブでない場合は、以下のステップを実行することで、この制約事項を迂回できます。

1. 特定性の高い総称プロファイルを一時的に追加します。
2. 個別プロファイルを追加します。
3. 中間の一時的な総称プロファイルを削除します。

zSecure Command Verifier には、一般リソースとデータ・セットの両方に対して特定性の高いプロファイルが作成されないようにするための汎用機能があります。この機能については、 198 ページの『特定性の高いプロファイルを作成するためのユーザー権限』で説明しています。

リソース命名規則の適用

データ・セットおよび一般リソースを命名するための追加制御を HLQ 制限内で設定するためのポリシーを作成するには、以下のガイドラインに従ってください。

ユーザー ID とグループに命名規則が必要であるように、データ・セットと一般リソースにも命名規則が必要です。ただしデータ・セットについては、データ・セット・プロファイルの名前に関する厳密な制約事項が既に RACF で実装されているため、その必要性はかなり低くなります。RACF では、あらゆるデータ・セット・プロファイルの HLQ が、端末ユーザーの範囲内にある既存の userid または GROUP と一致している必要があります。

HLQ が ABCX であるデータ・セット・プロファイルの作成を制御したい場合は、ユーザー ABCX1、ABCX2、および XYZA1 のみがこのようなデータ・セット・プロファイルを作成できるようにする必要があります。zSecure Command Verifier を使用すると、以下のポリシー・プロファイル定義を使用してこの制約事項を実装できます。

```
C4R.DATASET.ID.ABCX.**  UACC(NONE)  UPDATE(ABCX1,ABCX2,XYZA1)
```

ただし、既に RACF によって、HLQ は強制的に既存の RACF **ユーザー** ID または**グループ**となっています。つまり、考えられる HLQ のほとんどが、この基本的な要件を満たしていないために既に制御されています。RACF は、端末ユーザーが何らかの形でデータ・セット・プロファイルを作成する権限を受けていることを必要とします。この例のように HLQ がグループである場合は、ユーザーは最低でも CREATE 権限でグループに接続されているか、またはグループに対するグループ SPECIAL 権限を持っていることが必要となります。つまり、インストール済み環境で定義されているすべての GROUP およびユーザー ID (データ・セット HLQ として出現する可能性があるもの) のうち、特定の端末ユーザーに対して許可されるものはごくわずかということです。例えば、RACF データベースに**グループ** SYS1 が登録されていても、SYS1 を HLQ とするデータ・セット・プロファイルの作成を許可されるユーザーはごくわずかです。このため、上記のプロファイルが有効になるのは、3 人のユーザーがグループ SPECIAL 権限を持っているか、または CREATE 権限で接続されている場合に限ります。そのどちらでもない場合は、zSecure Command Verifier ポリシー・プロファイルの有無に関係なく、ユーザーにデータ・セット・プロファイルの作成が許可されません。

現行の RACF 実装では、CREATE 権限の使用は推奨されません。この権限には二重の機能があり、セキュリティーを制御するデータ・セット・プロファイルの作成を制御する手法としての機能と、ディスクやテープ上での新規データ・セットの作成または割り振りを行う機能の双方を備えているためです。最新の RACF 実装環境では、アプリケーション・データ・セット・プロファイルを作成する権限はグループ SPECIAL で管理され、ディスクやテープでのデータ・セットの作成は、該当するデータ・セット・プロファイルでの ALTER 権限 (セキュリティー管理者が設定) によって制御されます。

インストール済み環境において、RACF のグループ SPECIAL 権限を持つユーザーが作成できる HLQ 内のデータ・セット・プロファイルをさらに制御する必要がある場合は、zSecure Command Verifier ポリシー・プロファイルを使用できます。前述の例では、通常、ポリシー・プロファイルを単独では使用せずに、以下のように複数のプロファイルとともに定義します。

```
C4R.DATASET.ID.ABCX.**              UACC(NONE)      UPDATE(XYZA1)
     Only user XYZA1 can create within ABCX.
C4R.DATASET.ID.ABCX.TEST*.**        UACC(NONE)      UPDATE(ABCX1,ABCX2,XYZA1)
     All three users can create "test" dataset profiles.
```

注: この例でも、3 人のユーザー全員に、データ・セット・プロファイルを作成するための基本的な RACF 権限が必要です。zSecure Command Verifier ポリシー・プロファイルによって命名規則が適用されますが、一般には端末ユーザーの権限は引き上げられません。

推奨されてはいませんが、前述の一連のプロファイル例を使用して、CREATE レベルの接続許可に固有の権限を制限することもできます。ユーザー ABCX1 と ABCX2 がグループ ABCX に CREATE 権限で接続されていても、これらのユーザーにはデータ・セット・プロファイルの作成が許可されません。テスト・データ・セット・プロファイルには、例外が実装されています。

リソース命名規則を適用するためのポリシー・プロファイル

zSecure Command Verifier では、プロファイルの作成の許可に関する問題が、ポリシー・プロファイルによって解決されます。

これらのプロファイルについて、以下の表に要約します。ほとんどの場合、これらのプロファイルは必要ありませんが、RACF によって既に適用されているプロファイル作成の制限をさらに強化する場合に役立ちます。

表 *40. RACF* リソースの検証に使用されるプロファイル： この表の項目は、新しいリソースの名前を記述するキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD DELDSD	*profile*	**C4R.DATASET.ID.***hlq.rest-of-profile*
RDEFINE RDELETE	*profile*	**C4R.***class***.ID.***profile*
RDEFINE RALTER	*ADDMEM*	**C4R.***class***.ID.***member*
RDEFINE RALTER	*DELMEM*	**C4R.***class***.ID.***member*

これらのプロファイルでは、変数 *class* が、**RDEFINE** コマンドで指定されたクラスを表します。ADDMEM および DELMEM キーワードに使用されている *class* は、対応するメンバー・クラスを表します。以下の各例では、ポリシー・プロファイルで使用されている *class* を明らかにしています。

表 *41. RACF* リソースの検証に使用されるプロファイル： この表は、特定のコマンドに使用されるプロファイルとクラスの例を示しています。

コマンド	プロファイル	クラス
RDEFINE DASDVOL xyzzyx	*xyzzyx*	**DASDVOL**
RDEFINE GDASDVOL pool1	*pool1*	**GDASDVOL**
RALTER GDASDVOL pool1 ADDMEM(xyzzyx)	*xyzzyx*	**DASDVOL**
RDEFINE GDASDVOL pool1 ADDMEM(xyzzyx)	*xyzzyx pool1*	**DASDVOL GDASDVOL**

ポリシー・プロファイルでは、変数 *profile* が定義されているプロファイルを示し、変数 *member* が操作中のメンバーを示しています。上記の例では、それぞれ `pool1` と `xyzzyx` になっています。データ・セット・プロファイルの場合は、*profile* が 2 つの部分に分割される場合があります。

- 高位修飾子 (HLQ)。この修飾子は、データ・セット・プロファイルの最初の修飾子です。RACF では、最初の修飾子が既存の**ユーザー** `ID` または**グループ**でなければなりません。
- 残りの修飾子 (「rest-of-profile」と呼ばれます)。

データ・セット・プロファイル名をこのように分割しているのは、HLQ の特殊な使い方を強調するとともに、No-Store プロファイル (195 ページの『自分のデータ・セット・プロファイルを管理するためのポリシー・プロファイル』で説明) と標準のポリシー・プロファイル (次のセクションで説明) の形式が似ていることを強調するためです。

RACF リソース・プロファイルを作成するためのポリシー・プロファイル

このセクションのトピックでは、RACF リソース・プロファイルを作成するためのポリシー・プロファイル、および対応するアクセス・レベルについて説明します。

端末ユーザーのユーザー ID が HLQ となっているデータ・セット・プロファイルを作成するための権限については、 195 ページの『自分のデータ・セット・プロファイルを管理するためのポリシー・プロファイル』を参照してください。

- **C4R.DATASET.ID.***hlq.rest-of-profile*

  このプロファイルでは、*hlq.rest-of-profile* によって指定されるデータ・セット・プロファイルを作成する権限が記述されます。このポリシー・プロファイルは、総称プロファイルにも個別プロファイルにもできます。ポリシー・プロファイルを定義する際には、プロファイル部分には標準の総称文字の代わりに正符号を使用することができます。

  zSecure Command Verifier では、データ・セット・プロファイルを作成するための通常の RACF 権限が事前に検査されません。zSecure Command Verifier で特定のデータ・セット・プロファイルの作成が承認された場合でも、RACF によって独自の権限検査が実行されます。したがって、データ・セット・プロファイルに対しては、 204 ページの『リソース・プロファイルを作成するためのユーザー権限』で説明しているように、端末ユーザーにも権限が必要です。アクセス・レベルには以下のものがあります。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : ユーザーは、新規データ・セット・プロファイルの定義を許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、十分な RACF 権限があれば、データ・セット・プロファイルを作成できます。

  CONTROL
  : UPDATE と同じ。

- **C4R.***class*.**ID.***profile*
- **C4R.***class*.**ID.***member*

  この 2 つのポリシー・プロファイルは、同じ基本ポリシー・プロファイルを参照します。変数 *profile* と *member* には、値を取得する 2 つの場所を記述する別々の名前が使用されます。最初のプロファイルでは、*class* で *profile* を作成する権限が記述されます。このプロファイルは、**RDEFINE** コマンドに使用されます。同じポリシー・プロファイルの 2 番目の形式は、RDEFINE および RALTER コマンドの **ADDMEM** キーワードと **DELMEM** キーワードに使用されます。概要と例については、前のセクションを参照してください。アクセス・レベルには以下のものがあります。

プロファイルが見つからない
: 実装されていません。クラス *class* で *profile* を作成する権限が、zSecure Command Verifier で検査されません。

NONE
: ユーザーは、新しい *profile* の定義を許可されません。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは *profile* を作成できます。ただし、端末ユーザーには **clauth(***class***)** などの十分な RACF 権限がまだ必要です。

CONTROL
: UPDATE と同じ。

特殊なアプリケーション用のリソース・ポリシー・プロファイル

前のセクションで説明したプロファイルとその変換を、いくつかの特殊なアプリケーションに使用することができます。プロファイルに関する 2 つの特殊なアプリケーションの例を以下に示します。

最初のアプリケーションは、グローバル・アクセス検査テーブル内のプロファイルに関連します。2 番目のアプリケーションは、PROGRAM クラス内のプロファイルに関連します。

グローバル・アクセス検査テーブル**:**

最初の特殊アプリケーションは、GAC テーブル内の項目の定義に関係します。

zSecure Command Verifier では、ADDMEM キーワードの使用に関する追加の検査も実行されます。 GAC テーブルへの特定の項目の取り込みを許可または禁止することができます。例えば、許可を受けたシステム管理者が誤って項目 **/ALTER を GAC テーブルに作成した結果、システム内のすべてのデータ・セットに対する ALTER 権限が設定されたケースがあります。この状況は、2 つのポリシー・プロファイルで防止することができます。1 つは、GAC テーブルに項目が定義されないようにするプロファイルです。もう 1 つは、READ アクセスを許可する GAC テーブル項目の定義を可能にする特定性の高いプロファイルです。使用可能なポリシー・プロファイルは、以下のとおりです。

- **C4R.GMBR.ID.**.* UACC(NONE)**

  このプロファイルでは、不特定数の修飾子が存在する可能性を示すためにプロファイルの中ほどで「.**」を使用できるようにする EGN 機能を明示的に使用しています。また、最後の修飾子として「*」を明示的に使用して、次のプロファイルとの違いを強調しています。このプロファイルの UACC は NONE です。この設定により、どのユーザーも GAC テーブルに項目を定義できません。

- **C4R.GMBR.ID.**.R* UACC(UPDATE)**

  このプロファイルは、前のプロファイルよりも特定的です。この 2 つのプロファイルは、総称文字でない R までまったく同じです。このプロファイルの UACC は UPDATE です。この設定により、最後の修飾子が R で始まる項目をどのユーザーでも追加できます。

許可を受けた RACF 管理者が GAC テーブル項目 (SYS1.LINKLIB/READ など) を追加する場合のコマンドは、以下のとおりです。

```
RALT GLOBAL DATASET ADDMEM('SYS1.LINKLIB'/READ)
```

GLOBAL リソース・クラスは、RACF 内で疑似メンバー・クラス GMBR (RACF の内部的な理由で必要なクラス) と一致するため、zSecure Command Verifier では以下のポリシー・リソース名で検査が実行されます。

```
C4R.GMBR.ID.+SYS1.LINKLIB+.READ
```

187 ページの『ポリシー・プロファイルでの総称文字と特殊文字』で説明した変換機構によって、すべての総称文字と一部の特殊文字が正符号に変換されます。また、スラッシュ (/) 文字はピリオドに変換されます。このポリシー・リソースは、プロファイル 2 による対象とされるため、許可されます。管理者が誤って以下のコマンドを実行したとします。

```
RALT GLOBAL DATASET ADDMEM('SYS1.LINKLIB'/UPDATE)
```

この場合、ポリシー・リソース名は以下のようになります。

```
C4R.GMBR.ID.+SYS1.LINKLIB+.UPDATE
```

このポリシー・リソースはプロファイル 1 の対象となるため、GAC テーブル項目の作成は拒否されます。

ADDMEM キーワード内のデータ・セット名は常に正規化されます。正規化プロセスの一部として、データ・セット名が引用符で囲まれ、必要に応じて接頭部が付加されます。ポリシー・プロファイルでは、正規化されたデータ・セット名を変換した値が使用されます。前述の SYS1.LINKLIB の例には、ポリシー・プロファイルで使用される、正規化されたデータ・セット名を変換した名前が示されています。

ADDMEM キーワード内のアクセス・レベルは正規化されません。RACF では、1 文字に省略されたアクセス・レベル (R=READ、U=UPDATE) も使用可能です。サンプルのプロファイルで総称値 R* が最後の修飾子として指定されているのは、アクセス・レベルが正規化されないためです。この総称パターンは、READ のすべての省略形と一致します。

PROGRAM クラス**:**

2 番目の特殊なアプリケーションは、必須値プロファイルが総称プロファイル変換と組み合わせて UACC に使用されるものです。

この特殊なアプリケーションの目的は、PROGRAM クラス内の総称プロファイルで誤って UACC=NONE が定義されないようにすることです。例えば、管理者がリンク・リスト・データ・セットなどに対する総称プログラム・プロファイルを定義する際に、誤って UACC を除外したケースがあります。この場合、システム全体が使用不能になるおそれがあります。SYS1.LINKLIB 内のすべてのプログラムが使用されないように保護されている場合は、RACF コマンドを含むすべての TSO コマンドが、アクセス違反で失敗します。必須プロファイルを使用することで、このような事態を回避できます。以下のプロファイルは、PROGRAM クラス内の新しい総称プロファイルに対して UACC=NONE がデフォルトで割り当てられるのを防ぎます。

```
C4R.PROGRAM.=UACC.+             UACC(READ)      APPLDATA('READ')
C4R.PROGRAM.=UACC.%+            UACC(READ)      APPLDATA('READ')
C4R.PROGRAM.=UACC.%%+           UACC(READ)      APPLDATA('READ')
 ...
C4R.PROGRAM.=UACC.%%%%%%%+      UACC(READ)      APPLDATA('READ')
```

上記のプロファイルは、PROGRAM クラス内の使用可能なすべての総称プロファイルの UACC を制御します。これらのプロファイルを、個別プロファイルを含めた全プロファイルに拡張したい場合は、それらのプロファイルを以下の 1 つのプロファイルで置き換えることが可能です。

```
C4R.PROGRAM.=UACC.*             UACC(READ)      APPLDATA('READ')
```

どちらにしても、これらのプロファイルによって、新しい PROGRAM プロファイルに UACC=READ が指定されます。これにより、許可された管理者が後で UACC を他の任意の値にリセットできなくなることはありません。ただし、それにはその管理者が意識的に決断してコマンドを実行する必要があります。これは、プロファイルの定義中に使用されるデフォルトの割り当てとは異なります。

リソース・プロファイルの所有者に対するポリシー・プロファイルの選択

OWNER では、新たに定義されたリソース・プロファイルを誰が制御するかが記述されます。以下のプロファイルおよびガイドラインを使用して、所有者の指定を制御します。

これらのプロファイルは、OWNER を指定できる 4 つのコマンド (**ADDSD**、**RDEFINE**、**ALTDSD**、および **RALTER**) すべてに適用されます。一般に、これらのプロファイルの処理では、HLQ を OWNER として使用することがインストールのポリシーであると想定されます。以下のセクションで説明する最後のプロファイル (/HLQ) は、インストール済み環境でこのようなポリシーを適用するかどうかを示すために使用できる制御となります。ここでも、以下の説明を複数のプロファイル・セットに分けています。最初のセットは、OWNER の必須値またはデフォルト値を指定するために使用されます。

必須値ポリシー・プロファイルの場合、3 番目の修飾子は、等号とそれに続くキーワードで構成されます。つまり、OWNER の場合は、プロファイルのこの修飾子が =OWNER となります。デフォルト・プロファイルの場合、3 番目の修飾子はスラッシュとそれに続くキーワードで構成されます。つまり、OWNER の場合は、プロファイルの 3 番目の修飾子が /OWNER となります。

表 42. リソース・プロファイルの所有者に対する必須値ポリシー・プロファイル： この表の項目は、新しいリソース・プロファイルの OWNER の必須値またはデフォルト値を記述するコマンドとキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD	*profile*	**C4R.DATASET.=OWNER.***profile*
ADDSD	*profile*	**C4R.DATASET./OWNER.***profile*
RDEFINE	*profile class*	**C4R.***class***.=OWNER.***profile*
RDEFINE	*profile class*	**C4R.***class***./OWNER.***profile*

2 番目のプロファイル・セットは、端末ユーザーによって指定された OWNER の値に対する制御を記述するために使用されます。また、リソース・プロファイルの OWNER に対して使用できる一般ポリシーも記述されます。

表 *43.* リソース・プロファイルの所有者に使用されるプロファイル： この表の項目は、端末ユーザーによって指定された、新しいまたは変更されたリソース・プロファイルの所有者を記述するコマンドとキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD **ALTDSD**	*profile owner*	**C4R.DATASET.OWNER.=RACUID(***n***)**
ADDSD **ALTDSD**	*profile owner*	**C4R.DATASET.OWNER.=RACGPID(***n***)**
ADDSD **ALTDSD**	*profile owner*	**C4R.DATASET.OWNER.=HLQ(***n***)**
ADDSD **ALTDSD**	*profile owner*	**C4R.DATASET.OWNER.***owner.profile*
ADDSD **ALTDSD**	*profile owner*	**C4R.DATASET.OWNER./SCOPE.***owner.profile*
ADDSD **ALTDSD**	*profile owner*	**C4R.DATASET.OWNER./GROUP.***owner.profile*
ADDSD **ALTDSD**	*profile owner*	**C4R.DATASET.OWNER./HLQ.***owner.profile*
RDEFINE **RALTER**	*profile class owner*	**C4R.***class.***OWNER.=RACUID(***n***)**
RDEFINE **RALTER**	*profile class owner*	**C4R.***class.***OWNER.=RACGPID(***n***)**
RDEFINE **RALTER**	*profile class owner*	**C4R.***class.***OWNER.=HLQ(***n***)**
RDEFINE **RALTER**	*profile class owner*	**C4R.***class.***OWNER.***owner.profile*
RDEFINE **RALTER**	*profile class owner*	**C4R.***class.***OWNER./SCOPE.***owner.profile*
RDEFINE **RALTER**	*profile class owner*	**C4R.***class.***OWNER./GROUP.***owner.profile*
RDEFINE **RALTER**	*profile class owner*	**C4R.***class.***OWNER./HLQ.***owner.profile*

所有者に対する必須値ポリシー・プロファイルとデフォルト値ポリシー・プロファイル

新規リソース・プロファイルの OWNER の必須値とデフォルト値を指定するには、以下のポリシー・プロファイルを使用します。

これらのプロファイルは、**ADDSD** コマンドと **RDEFINE** コマンドにのみ使用されます。

- **C4R.***class.***=OWNER.***profile*

このプロファイルは、新規に定義されるリソース・プロファイルの OWNER の必須 (優先) 値を指定します。このプロファイルは、**ADDSD** および **RDEFINE** の処理中にのみ使用されます。この必須値プロファイルによって取得された OWNER 値は、追加の OWNER 関連ポリシー・プロファイルの影響を受けません。

ポリシー・プロファイル内の修飾子 =OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。必須値は強制されません。

NONE
: アクションは実行されません。必須値は強制されません。

READ
: **APPLDATA** フィールドが抽出され、コマンドで使用されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーによって指定された OWNER の値が、コマンド内で使用されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値プロファイルでは、これはアクセス権限 NONE が最終的にアクセス権限 OWNER と同じ結果になるという変則的な状態になります。

APPLDATA フィールドで受け入れられる値は、以下のとおりです。OWNER は、ユーザー ID または GROUP です。

BLANK
: 新しい OWNER に指定された値が抑止され、端末ユーザーの現在の**グループ**で置き換えられます。

=HLQ
: リソース・プロファイルの高位修飾子 (HLQ) を表します。通常この設定は、データ・セット・プロファイルの場合にのみ意味があります。HLQ が既存のユーザー ID または GROUP でない場合は、端末ユーザーの現在の GROUP が代わりに使用されます。

=MYOWNER
: 端末ユーザーの OWNER を反映します。この OWNER が既存のユーザー ID または GROUP である場合は、その値が新しいリソース・プロファイルの OWNER として使用されます。そうでない場合は、端末ユーザーの現在の**グループ**が代わりに使用されます。

other
: 指定されたユーザー ID または GROUP が、新しいリソース・プロファイルの OWNER として使用されます。この所有者が既存のユーザー ID または GROUP でない場合は、端末ユーザーの現在の GROUP が代わりに使用されます。

- **C4R.***class.***/OWNER.***profile*

  このポリシー・プロファイルは、新規に定義されるリソース・プロファイルの OWNER のデフォルト値を指定します。このプロファイルは、**ADDSD** および **RDEFINE** の処理中にのみ使用されます。デフォルト値として使用される OWNER は、プロファイルの **APPLDATA** フィールドから取得されます。このデフォルト値プロファイルによって取得された OWNER 値は、その他の OWNER 関連ポリシー・プロファイルの影響を受けません。=OWNER プロファイルを使用して値が指定された場合、/OWNER プロファイルは使用されません。

  ポリシー・プロファイル内の修飾子 /OWNER を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  : この制御は実装されません。デフォルト値は提供されません。この設定では、RACF から OWNER (端末ユーザー自身) のデフォルトが提供されます。

  NONE
  : デフォルト値は提供されません。RACF は、OWNER の値を提供しません。コマンドはリジェクトされます。このアクセス・レベルを使用すると、インストールで端末ユーザーに OWNER の値を明示的に指定するよう強制できます。

  READ
  : **APPLDATA** フィールドが抽出され、コマンドで使用されます。

  UPDATE
  : READ と同じ。

  CONTROL
  : この制御は、端末ユーザーに対してアクティブにはされません。デフォルト値は提供されません。端末ユーザーが OWNER の値を指定しなかったため、RACF は端末ユーザーを新規プロファイルの OWNER にします。

  APPLDATA フィールドで受け入れられる値は、以下のとおりです。ユーザー ID または GROUP を OWNER として指定できます。

  BLANK
  : 端末ユーザーの現在の**グループ**が、OWNER の値として挿入されます。

  =HLQ
  : リソース・プロファイルの高位修飾子 (HLQ) を反映します。通常この設定は、データ・セット・プロファイルの場合にのみ意味があります。HLQ が既存のユーザー ID または GROUP でない場合は、端末ユーザーの現在のグループが代わりに使用されます。

  =MYOWNER
  : 端末ユーザーの OWNER を反映します。この OWNER が既存の**ユーザー** ID または**グループ**である場合は、その値が新しいリソース・プロファイルの OWNER として使用されます。そうでない場合は、端末ユーザーの現在のグループが代わりに使用されます。

  other　指定された**ユーザー** ID または **グループ**が、新しいリソース・プロファ

イルの OWNER として使用されます。この所有者が既存の**ユーザー** ID または**グループ**でない場合は、端末ユーザーの現在のグループが代わりに使用されます。

リソース・ポリシー・プロファイル所有者の検査

ADDSD、**RDEFINE**、**ALTDSD**、または **RALTER** の各コマンドに指定された新規の OWNER を検査するには、以下のポリシー・プロファイルを使用します。

データ・セットの場合は、RACF によって、所有者が CREATE 以上の権限で HLQ-GROUP に接続されていなければならないという制約が課されることがあります。一般リソースまたは HLQ=USERID データ・セットの場合は、RACF によって OWNER に関する制約が課されることはありません。ここで示すポリシー・プロファイルを使用して、新しい OWNER の選択を制限することができます。指定された OWNER の使用が、どの一般ポリシー・ルール (=RACUID、=RACGPID、=HLQ) でも受け入れられなかった場合は、明示的なポリシー・プロファイルが使用されます。

- **C4R.***class*.**OWNER.=RACUID(***n***)**

  このプロファイルは、OWNER に特殊な総称ポリシーを指定します。=RACUID は、端末ユーザーのユーザー ID を意味します。substring(=RACUID,1,*n*) が一致した場合、*n* の値とは関係なく、このプロファイルが他のプロファイルに優先して使用されます。これらのプロファイルが複数定義されている場合は、数値の指定が最も小さいプロファイルだけが userid の突き合わせに使用されます。

  このプロファイルは、個別プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

  指定された OWNER が受け入れられると、一般ポリシー (/SCOPE や /GROUP など) に対する追加の検査が実行されます。

  プロファイルが見つからない
  : 端末ユーザーのユーザー ID は、OWNER に対する命名規則や制約事項として使用されません。

  NONE
  : 指定された OWNER は許可されません。コマンドは失敗します。この決定は、以下に述べるプロファイル *owner.profile* に対する権限によって、却下することができます。

  READ
  : NONE と同じ。

  UPDATE
  : 指定された OWNER は受け入れられます。

  CONTROL
  : UPDATE と同じ。

- **C4R.***class*.**OWNER.=RACGPID(***n***)**

  このプロファイルは、OWNER に特殊な総称ポリシーを指定します。=RACGPID は、端末ユーザーの接続先グループのリストを表します。「グループ・アクセス権限検査のリスト」の設定とは関係なく、すべてのユーザーのグループが使用さ

れます。substring(=RACGPID,1,*n*) が一致した場合は、*n* の値に関係なく、このプロファイルが他のプロファイルに優先して使用されます。これが使用されるのは、=RACUID(*n*) が存在しないか一致しない場合に限ります。これらのプロファイルを複数定義した場合は、*n* の値が最も小さいプロファイルだけが使用されます。

このプロファイルは個別ポリシー・プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

指定された OWNER が受け入れられると、一般ポリシー (/SCOPE や /GROUP など) に対する追加の検査が実行されます。

プロファイルが見つからない
: 端末ユーザーのグループは、OWNER に対する命名規則や制約事項として使用されません。

NONE
: 指定された OWNER は許可されません。コマンドは失敗します。この決定は、以下に述べるプロファイル *owner.profile* に対する権限によって、却下することができます。

READ
: NONE と同じ。

UPDATE
: 指定された OWNER は受け入れられます。

CONTROL
: UPDATE と同じ。

- **C4R.***class*.**OWNER.=HLQ(***n***)**

  このプロファイルは、OWNER に特殊な総称ポリシーを指定します。特殊値 =HLQ は、リソース・プロファイル自体の高位修飾子を表します。通常このポリシー・プロファイルは、データ・セット・プロファイルの場合にのみ意味があります。このプロファイルを使用して、データ・セット・プロファイルの最初の *n* 文字がその所有者の最初の *n* 文字と一致している必要があることを指定する命名規則を適用できます。

  =HLQ は、コマンドにおけるリソース・プロファイルの HLQ を意味します。substring(=HLQ,1,*n*) が指定された OWNER と一致した場合、*n* の値とは関係なく、このプロファイルが他の総称プロファイルに優先して使用されます。これは =RACUID(*n*) および =RACGPID(*n*) が存在しないか、一致しない場合にのみ使用されます。これらのプロファイルを複数定義した場合は、*n* の値が最も小さいプロファイルだけが使用されます。

  このプロファイルは個別ポリシー・プロファイルです。括弧内の 1 桁のみが変数であり、1 から 8 の範囲で指定する必要があります。真の総称プロファイルを使用することはできません。

指定された OWNER が受け入れられると、一般ポリシー (/SCOPE や /GROUP など) に対する追加の検査が実行されます。zSecure Command Verifier では、指定された OWNER が有効なユーザー ID またはグループであるかどうかが検査されません。

プロファイルが見つからない
: ターゲット・リソース・プロファイルは、その OWNER に対する命名規則や制約事項として使用されません。

NONE
: 指定された OWNER は許可されません。コマンドは失敗します。この決定は、以下に述べるプロファイル *owner.profile* に対する権限によって、却下することができます。

READ
: NONE と同じ。

UPDATE
: 指定された OWNER は受け入れられます。

CONTROL
: UPDATE と同じ。

上記の 3 つのプロファイルのいずれかが、指定された OWNER を許可する場合、次のプロファイル規則はスキップされます。引き続き、/SCOPE、/GROUP、および /HLQ の各ポリシーで処理が進められます。上記のプロファイルが特定の OWNER の使用を許可しなかった場合は、次のプロファイルが代替の許可方式として使用されます。

- **C4R.***class*.**OWNER.***owner.profile*

この制御の主な目的は、一般ポリシーがどれも適用されない場合にポリシーを指定することです。変数 *owner* は、リソース *profile* の新規 OWNER を表します。これは、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

このポリシー・プロファイルで検査された OWNER にも、ここで説明した追加のポリシー・プロファイル (/SCOPE、/GROUP、/HLQ) が適用されます。

プロファイルが見つからない
: この制御は実装されません。

NONE
: コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 指定された OWNER は受け入れられます。

CONTROL
: UPDATE と同じ。

リソース・プロファイルの所有者に対する追加のポリシー・プロファイル

新しい OWNER に対する一般規則を指定するためのプロファイルを実装するには、以下のガイドラインに従ってください。特定性の高いプロファイル、または完全修飾プロファイルを使用することで、一部のリソース・プロファイルがこのような制限から除外されるように指定できます。

命名規則を適用するためのプロファイルのほかに、既存の RACF グループ階層に基づいたポリシーを実装することもできます。

以下のプロファイル規則は、追加のポリシー・セットとして使用されます。指定された OWNER が上記のどの規則でも受け入れられなかった場合は、以下の 3 つのポリシーに対して OWNER が検査されます。これらのどのポリシーでも不合格の場合は、コマンドが拒否されます。

C4R.*class*.**OWNER./SCOPE.***owner.profile*

このプロファイルは、端末ユーザーによって指定された新規 OWNER が**グループ** SPECIAL 属性の範囲内にある必要があるどうかを制御するために使用されます。このプロファイルは、端末ユーザーが**グループ** SPECIAL 属性の範囲内にあるリソース・プロファイルを「引き渡す」ことを防止できます。

変数 *profile* と *owner* は、影響を受けるリソース・プロファイルと、そのリソース・プロファイルの新しい OWNER を表します。これは、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /SCOPE を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

新規所有者としてユーザー ID を指定することは、常に、端末ユーザーの管理範囲外と見なされます。

グループ SPECIAL またはシステム SPECIAL を持つ端末ユーザーが、新規所有者に対して自己の管理権限を使用すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

- **C4R.USESCOPE.***group*

このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、データ・セットまたはリソースに対して指定された新規所有者に対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

/SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: 端末ユーザーの**グループ** SPECIAL の範囲を使って、ユーザー・プロファイルの新しい OWNER が制御されることはありません。

NONE
指定された新規 OWNER が端末ユーザーのグループ SPECIAL 属性の範囲外にある場合は、コマンドは失敗します。

READ
NONE と同じ。

UPDATE
端末ユーザーの範囲に関係なく、指定された OWNER は受け入れられます。

CONTROL
UPDATE と同じ。

C4R.*class*.**OWNER./GROUP.***owner.profile*
このプロファイルは、指定された OWNER が RACF グループでなければならないかどうかを制御するために使用されます。このプロファイルは、他のプロファイルとは無関係に検査されます。=OWNER または /OWNER プロファイルのいずれかが使用される場合は、このポリシー・ルールがバイパスされます。

変数 *profile* と *owner* は、影響を受けるリソース・プロファイルと、そのリソース・プロファイルの新しい OWNER を表します。これは、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /GROUP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
この制御は実装されません。指定の OWNER はグループとユーザー ID です。

NONE
指定された所有者が既存の RACF グループである場合、コマンドは受け入れられます。それ以外の状態では、コマンドは失敗します。

READ
NONE と同じ。

UPDATE
指定された OWNER は、既存のグループを表していない場合でも受け入れられます。指定された OWNER が有効な項目でない場合、コマンドは RACF によって拒否されます。

CONTROL
UPDATE と同じ。

C4R.*class*.**OWNER./HLQ.***owner.profile*
このプロファイルは、端末ユーザーの指定した OWNER がリソース・プロファイルの HLQ と同じでなければならないかどうかを制御するために使用されます。通常このプロファイルは、データ・セット・プロファイルの場合にのみ意味があります。

profile と *owner* の値は、影響を受けるリソース・プロファイルと、そのプロファイルの新しい OWNER を表します。これは、一般規則への例外の指定を可能にします。最も限定的なプロファイルが zSecure Command Verifier によって使用されます。

ポリシー・プロファイル内の修飾子 /HLQ を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。指定された OWNER は、HLQ と異なっていてもかまいません。

NONE
: 指定された新規 OWNER は、現在の (または新しい) HLQ と同じでなければなりません。

READ
: NONE と同じ。

UPDATE
: 指定された OWNER は、HLQ の値に関係なく受け入れられます。

CONTROL
: UPDATE と同じ。

UACC およびアクセス・リストの制御

プロファイルを作成する権限を除いて、リソース・プロファイルの最も重要な部分は、そのアクセス仕様です。zSecure Command Verifier では、あらゆる形式のアクセス管理がポリシー・プロファイルによってサポートされます。

RACF では、グローバル・アクセス検査 (GAC) テーブルでファスト・パス・オプションも選択できます。zSecure Command Verifier では、このテーブルがアクセス機構として直接制御されることはありません。ただし、GAC テーブルは、GLOBAL リソース・クラス内の RACF プロファイルによって定義されるため、zSecure Command Verifier ポリシー・プロファイルによって制御することも可能です。

注: **PERMIT** コマンドまたは **ALTDSD** コマンドを実行する権限は、 195 ページの『自分のデータ・セット・プロファイルを管理するためのポリシー・プロファイル』で説明している No-Store 制御の対象にもなります。

以下の表は、さまざまなアクセス機構で使用される各種ポリシー・プロファイルをまとめたものです。最初の表は、UACC 制御および標準アクセス・リストの概要です。表では、また、アクセス管理用の追加のポリシーについても要約しています。追加のポリシーは、他の ACL ポリシーに従ってコマンドが承認された後に適用されます。

この追加のポリシー・プロファイルを使用して、データ・セット・グループがリソースのアクセス・リストに追加されないようにしたり、グループ SPECIAL の範囲外にある個々のユーザーやグループにアクセス権限が付与されないようにしたりすることができます。データ・セット・プロファイルがグループを HLQ として定義されている場合は、そのグループがデータ・セット・グループと見なされます。

表 *44. RACF* アクセスの検証に使用されるプロファイル： この表の項目は、アクセスの管理に使用されるコマンドとキーワードを反映しています。

コマンド	キーワード	プロファイル
ADDSD **RDEFINE**	*profile*	**C4R.***class*.**=UACC.***profile*
ADDSD **RDEFINE**	*profile*	**C4R.***class*.**/UACC.***profile*
ADDSD **RDEFINE** **ALTDSD** **RALTER**	*profile*	**C4R.***class*.**UACC.***uacc.profile*
PERMIT	*userid*	**C4R.***class*.**ACL.=RACUID.***access.profile*
PERMIT	*group*	**C4R.***class*.**ACL.=RACGPID.***access.profile*
PERMIT	*profile* **ID(***id***)**	**C4R.***class*.**ACL.=PUBLIC.***profile*
PERMIT	*profile* **ID(***userid***) AC(***access***)**	**C4R.***class*.**ACL.***userid.access.profile*
PERMIT	*profile* **ID(*) AC(***access***)**	**C4R.***class*.**ACL.=STAR.***access.profile*
PERMIT	*profile* **FROM(model)**	**C4R.***class*.**ACL.=FROM.***profile*
PERMIT	*profile* **RESET(Standard)**	**C4R.***class*.**ACL.=RESET.***profile*
PERMIT	*profile* **ID(***group***)**	**C4R.***class*.**ACL.=DSN.***group.profile*
PERMIT	*profile* **ID(***userid***)**	**C4R.***class*.**ACL./GROUP.***userid.profile*
PERMIT	*profile* **ID(***userid***)**	**C4R.***class*.**ACL./SCOPE.***userid.profile*

注**:** この表には、完全な内容を示すために、ユーザーが自身にアクセス権限を付与するためのポリシー・プロファイルが再度掲載されています。これらのポリシー・プロファイルについては、 196 ページの『自己許可に対するポリシー・プロファイルの選択』で説明しています。

以下の表は、条件付きアクセス・リストに使用されるポリシー・プロファイルをまとめたものです。この要約では、特定の when 条件クラスを使用する権限、および条件付きアクセス・リストをリセットする権限について説明しています。

表 *45. RACF* アクセスの検証に使用されるプロファイル： この表の項目は、アクセスの管理に使用されるコマンドとキーワードを反映しています。

コマンド	キーワード	プロファイル
PERMIT	*profile* **WHEN(***whenclass***)**	**C4R.***class*.**CONDACL.***whenclass.profile*
PERMIT	*profile* **RESET(when)**	**C4R.***class*.**CONDACL.=RESET.***profile*

この表では、一部の一般ポリシー・ルールで、ACL 項目に使用されている修飾子と同じ修飾子が特殊キーワードに使用されています。例えば、/SCOPE 修飾子は、通常のユーザー *ID* の修飾子と同じです。あるグループ管理者に対し、グループ GROUPX を任意のアクセス・リストに追加することを明示的に許可する場合は、これらの一般ポリシーを明示的に処理するプロファイルをいくつか定義する必要があります。

例えば、以下のルールについて考えてみます。

```
ADMINX is only allowed to put GROUPX on any ACL.
Any other ACLid is "protected" and can only be permitted by SUPERADM.
```

このポリシー・ルールには、以下のプロファイルが必要となります。

```
C4R.*.ACL.*.**            uacc(none) update(superadm)
C4R.*.ACL.groupx.**       uacc(none) update(superadm,adminx)
```

この 2 つのポリシー・プロファイルによって、SUPERADM に対してすべての ACL 項目が許可され、ADMINX に対して GROUPX が許可されます。以下の追加のポリシー・プロファイルを明示的に規定することもできます。

```
C4R.*.ACL./SCOPE.**       uacc(update)
C4R.*.ACL./GROUP.**       uacc(update)
C4R.*.ACL.=STAR.**        uacc(update)
C4R.*.ACL.=DSN.**         uacc(update)
C4R.*.ACL.=RESET.**       uacc(update)
```

/SCOPE や /GROUP などの修飾子に総称を使用することはできません。この 5 つのプロファイルによって、一般ポリシーは実装されないようになります。アクセス権限 CONTROL を付与することもできます。**ユーザー** ID「*」をアクセス・リストに追加する権限を明示的に否認する場合は、以下のプロファイルを使用します。

```
C4R.*.ACL.=STAR.** uacc(none) update(superadm)
```

このポリシー・ルールの例では、ADMINX に対して任意の ACL への GROUPX の追加がどのように許可されるかが指定されていません。通常 RACF では、ACL 項目に基づくのではなく、リソース・プロファイル自体に基づいたアクセス・リスト項目の管理のみが許可されます。すべての ACL を管理するには、端末ユーザーに**システム** SPECIAL 権限、またはいくつかの GROUP での**グループ** SPECIAL 権限が必要になります。

リソース・プロファイル UACC へのアクセスの制御

3 つのプロファイルは、新たに定義されたリソース・プロファイルの UACC の設定を制御します。

最初のプロファイルは、UACC の必須値を指定するために使用できます。このプロファイルの主な目的は、管理者がプログラム・クラス内に誤って UACC=NONE でプロファイルを定義しないようにすることです。このようなプロファイルを定義するとシステム全体がシャットダウンされて簡単に復旧できなくなる可能性があります。必須 UACC プロファイルを使用すると、このような状態を回避できます。必須値プロファイルは、**ADDSD** および **RDEFINE** コマンドにのみ使用されます。

2 番目のポリシー・プロファイルは、UACC の指定がなく、かつ適用される必須プロファイルがない場合に、デフォルトの UACC を提供します。

最後のポリシー・プロファイルは、端末ユーザーが指定した値を検査するためのものです。これは、新しいリソース・プロファイルを作成するとき、および既存のリソース・プロファイルの UACC 値を変更するときに使用されます。

- **C4R.***class*.**=UACC.***profile*

  このプロファイルは、UACC の必須値を指定します。このプロファイルの **APPLDATA** フィールドが抽出され、値として挿入されます。**APPLDATA** フィールドには、標準の RACF アクセス・レベル値 NONE、EXECUTE、READ、UPDATE、CONTROL、または ALTER のいずれかが入っている必要があります。それ

以外の値は、すべて NONE と解釈されます。ポリシー・プロファイルに対する端末ユーザーのアクセス権限によって、検出された値が使用可能かどうかが決まります。

ポリシー・プロファイル内の修飾子 =UACC を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: この制御は実装されません。必須値は強制されません。

NONE
: 必須値は使用されません。端末ユーザーの指定した値が受け入れられるか、RACF からデフォルト値が提供されます。

READ
: ポリシー・プロファイルの **APPLDATA** が抽出され、新しいプロファイルの UACC 値として挿入されます。

UPDATE
: READ と同じ。

CONTROL
: この制御は、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーによって指定された UACC の値が、コマンド内で使用されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値プロファイルでは、これはアクセス権限 NONE が最終的にアクセス権限 CONTROL と同じ結果になるという変則的な状態になります。

この必須値プロファイルによって取得された UACC 値は、追加の UACC 関連ポリシー・プロファイルの支配を受けません。

- **C4R.***class.***/UACC.***profile*

  このプロファイルは、UACC のデフォルト値を指定します。このポリシー・プロファイルは、RACF コマンドで UACC の値が指定されていない場合にのみ使用されます。このポリシー・プロファイルの **APPLDATA** フィールドが抽出され、値として挿入されます。

  ポリシー・プロファイル内の修飾子 /UACC を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。**APPLDATA** フィールドには、標準の RACF アクセス・レベル値 NONE、EXECUTE、READ、UPDATE、CONTROL、または ALTER のいずれかが入っている必要があります。それ以外の値は、すべて NONE と解釈されます。端末ユーザーのアクセス権限によって、検出された **APPLDATA** 値をコマンドに挿入する必要があるかどうかが決まります。

  プロファイルが見つからない
  : ポリシーは実装されません。

NONE
デフォルト値は使用されません。RACF から提供されるデフォルト値が使用されます。

READ
ポリシー・プロファイルの **APPLDATA** が抽出され、新しいプロファイルの UACC 値として挿入されます。

UPDATE
NONE と同じ。

CONTROL
この端末ユーザーには、デフォルトの UACC ポリシー・ルールが適用されません。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。デフォルト値プロファイルでは、これはアクセス権限 NONE が最終的にアクセス権限 CONTROL と同じ結果になるという変則的な状態になります。

この必須値プロファイルによって取得された UACC 値は、追加の UACC 関連ポリシー・プロファイルの支配を受けません。

- **C4R.***class.***UACC.***uacc.profile*

このプロファイルは、端末ユーザーによって指定された UACC 値を検査するために使用されます。変数 *uacc* は、指定された UACC レベルを表します。受け入れられる値は、いずれも RACF で許可された UACC の値です (つまり NONE、EXECUTE、READ、UPDATE、CONTROL、または ALTER)。**ADDSD** および **RDEFINE** コマンドで、端末ユーザーが RACF のデフォルト値 NONE を明示的に指定した場合、このプロファイルは使用されません。値 NONE は、対応する UACC ポリシー・ルールの指定に関係なく、新しいリソースを定義する際に必ず受け入れられます。**ALTDSD** および **RALTER** コマンドの場合は、UACC のすべての値が UACC ポリシー・ルールを使用して検査されます。

プロファイルが見つからない
この制御は実装されません。端末ユーザーの指定した値が受け入れられます。

NONE
指定された UACC は許可されません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
端末ユーザーの指定した UACC 値が受け入れられます。

CONTROL
UPDATE と同じ。

リソース・プロファイル ACL に対するポリシー・プロファイル

zSecure Command Verifier では、いくつかのポリシー・プロファイルを使用して、アクセス・リストおよび条件付きアクセス・リスト内の項目が制御されます。

2 つの主要なプロファイル・タイプが使用されます。1 番目のタイプは、ID (RACF の用語では、ユーザー ID。ただし実際にはユーザー ID または GROUP) とアクセス・レベルの組み合わせを指定します。2 番目のタイプのプロファイルは、WHEN (when-class) キーワードの使用法を制御します。このセクションでは、標準 ACL と条件付き ACL の両方で使用されるアクセス・レベルと ID について説明しています。次のセクションでは、条件付きアクセス・リストで使用されるクラス について説明します。

アクセス・リストのプロファイルでは、ACL での `ID(*)` の使用に対応して特殊な修飾子がサポートされています。ポリシー・プロファイルでは、これが特殊な修飾子 `=STAR` で表されます。プロファイルのデフォルト変換が使用される場合は、アクセス・リストでのアスタリスクの使用を表すために、ポリシー・プロファイルで正符号が使用されます。

ユーザーが自身にアクセス権限を付与するためのポリシー・プロファイルは、参考のために前出の表に示されています。これらのポリシー・プロファイルについては、196 ページの『自己許可に対するポリシー・プロファイルの選択』で説明しています。

このセクションのポリシー・プロファイルはいずれも、非公開リソース、およびポリシー・プロファイルで端末ユーザーによるアクセス・リストの変更が許可されている公開リソースに対してのみ評価されます。リソース・プロファイルが公開と見なされるのは、その UACC が NONE より高いか、または `ID(*)` に NONE より高いアクセス権限が付与されている場合です。公開リソース・アクセス制御の説明については、228 ページの『ACL に対する一般ポリシー・プロファイル』を参照してください。該当する公開 ポリシー・プロファイルでアクセス・リストの更新が拒否された場合、このセクションで説明するポリシー・プロファイルはどれも評価されません。

ポリシー・プロファイルでは、修飾子 *user* は、コマンド内で指定された ID を表します。RACF ユーザー ID または RACF GROUP のいずれかを指定できます。修飾子 *access* は、アクセス・レベルを表します。指定できる値は、ALTER、CONTROL、UPDATE、READ、EXECUTE、NONE、または特殊値 DELETE です。DELETE は、PERMIT コマンド上の DELETE キーワードを表すために使用されます。

- **C4R.***class*.**ACL.***user.access.profile*

  このプロファイルでは、ユーザー ID またはグループに、リソース・クラス *class* 内の *profile* に対する *user* アクセス権限を *access* レベルで付与する権限が記述されます。ポリシー・プロファイルの例を以下に示します。

  ```
  C4R.DATASET.ACL.IBMUSER.UPDATE.SYS1.**
  C4R.FACILITY.ACL.IBMUSER.UPDATE.ICHBLP
  C4R.DATASET.ACL.*.*.**
  ```

  一般に、リソース・プロファイルは HLQ に続く 2 つのアスタリスクで構成される総称パターンで表されることが予想されます。すべてのリソース・プロファ

イルを補強するプロファイルとして、上記の 3 番目の例に似たプロファイルが使用されることが予想されます。その場合、単一アスタリスクの総称文字を使用して、必須の修飾子が明示的にコーディングされます。

プロファイルが見つからない
: このポリシーは、この状態に対して実装されません。

NONE
: 指定されたアクセス権限は許可されません。コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 指定されたアクセス権限は、このユーザー およびリソース・プロファイルに対して許可されます。

CONTROL
: UPDATE と同じ。

- **C4R.***class*.**ACL.=STAR.***access.profile*

  このプロファイルは、アクセス・リストで ID(*) が使用されていることを表します。一般に、ID(*) では UACC を使用した場合と最終的に同じ結果になります。組織によっては、システムのすべてのユーザーと、システムのすべての RACF 定義ユーザーを明白に区別することが必要となる場合があります。適切に保護されたシステムでは、この 2 つのカテゴリーが区別されません。このため、zSecure Command Verifier では ID(*) のアクセス・レベルを迅速に認識して制御するための特殊な修飾子を実装しています。

  一般規則とは異なり、特殊値 =STAR は総称パターンで表すことができます。例えば、プロファイル **C4R.***class*.**ACL.*.***profile* を使用して、ACL に対するすべての変更を防止することができます。

  多くのインストールにおいて、以下のようなプロファイルの定義が予想されます。

  ```
  C4R.DATASET.ACL.=STAR.*.**   UACC(NONE)
  ```

  これによって、すべてのデータ・セット・アクセス・リストで ID(*) が使用されないようにします。このポリシー・プロファイルに対してサポートされているアクセス・レベルは、通常のアクセス・リスト・ポリシー・プロファイルのレベルと同じです。

  プロファイルが見つからない
  : このポリシーは、この状態に対して実装されません。

  NONE
  : 指定されたアクセス権限は許可されません。コマンドはリジェクトされます。

  READ
  : NONE と同じ。

UPDATE
指定されたアクセス権限は、ID(*) およびこのリソース・プロファイルに対して許可されます。

CONTROL
UPDATE と同じ。

- **C4R.***class.***ACL.=FROM.***profile*

  このプロファイルは、既存の ACL をプロファイル間でコピーする権限を制御します。RACF の **PERMIT FROM** 機能を使用すると、複数の ACL 項目に対して簡単に **PERMIT** コマンドを実行できます。モデル・プロファイルの ACL 項目は、ターゲット・プロファイルの既存の ACL に追加されるだけです。ターゲット・プロファイルの既存の ACL 項目は変更されません。

  このポリシーの実装がインストールで選択される主な理由は、コピーされた ACL にポリシー・ルールに適合しない項目が含まれる可能性があるためです。ACL.=FROM プロファイルは、アクセス・リストに対してこのコピー機能を使用する権限を制御するために使用されます。モデル・プロファイル名は、ポリシー・プロファイルに含まれません。

  一般規則とは異なり、特殊値 =FROM は総称パターンで表すことができます。例えば、プロファイル **C4R.***class.***ACL.*.***profile** を使用して、ACL に対するすべての変更を防止することができます。

  プロファイルが見つからない
  このポリシーは、この状態に対して実装されません。

  NONE
  端末ユーザーは、既存の ACL をこの *profile* にコピーすることを許可されません。

  READ
  NONE と同じ。

  UPDATE
  既存の ACL のコピーが許可されます。

  CONTROL
  UPDATE と同じ。

- **C4R.***class.***ACL.=RESET.***profile*

  このプロファイルは、アクセス・リスト全体をリセットしてアクセス・リストからすべての項目を除去する権限を制御します。RACF の **PERMIT RESET** 機能を使用すると、アクセス・リスト内のすべての項目に対して **PERMIT DELETE** コマンドを簡単に実行できます。ACL.=RESET プロファイルは、標準アクセス・リストをリセットする権限を制御するために使用されます。次のセクションでは、**条件付き** アクセス・リストをリセットする権限に関する同様のプロファイルについて説明します。

  一般規則とは異なり、特殊値 =RESET は総称パターンで表すことができます。例えば、プロファイル **C4R.***class.***ACL.*.***profile** を使用して、ACL に対するすべての変更を防止することができます。

プロファイルが見つからない
このポリシーは、この状態に対して実装されません。

NONE
端末ユーザーは、*class* 内の *profile* の ACL をリセットすることを許可されません。

READ
NONE と同じ。

UPDATE
標準 ACL のリセットが許可されます。

CONTROL
UPDATE と同じ。

ACL に対する一般ポリシー・プロファイル

多くのインストールにおいて、アクセス・リストに追加できる項目に関する一般ポリシー・ルールを使用しています。zSecure Command Verifier では現在、このような一般ポリシーをいくつか実装しています。

これらのポリシーを使用すると、以下のことを実行できます。

- 1 番目のポリシーは、いわゆる公開 リソースのアクセス・リストに対する更新を防止するために使用します。アクセス・リストに対する更新は、重複していたり、例外的な状態でのみ必要となることが少なくありません。
- 2 番目のポリシーは、データ・セット・グループへのアクセス権限の付与を防止するために使用します。データ・セット・プロファイルがグループを HLQ として定義されている場合は、そのグループがデータ・セット・グループと見なされます。
- 3 番目、4 番目、および 5 番目のポリシーは、ユーザー ID がアクセス・リストに追加されるのを防止するために使用します。グループの追加のみが許可されます。
- 最後のポリシーは、分散管理者のグループ SPECIAL 権限の範囲外にある項目に対するアクセス権限の付与を防止するために使用します。

zSecure Command Verifier では現在、以下の一般ポリシーを実装しています。

- **C4R.***class*.**ACL.=PUBLIC.***profile*

  このポリシー・プロファイルは、公開リソースのアクセス・リストに対する変更を防止するために使用できます。リソース・プロファイルが公開と見なされるのは、その UACC が NONE より高いか、または `ID(*)` に NONE より高いアクセス権限が付与されている場合です。ポリシーが適用される場合に、端末ユーザーのアクセス権限が不十分であると、コマンドは拒否され、ポリシー・プロファイルに関連する他のアクセス・リストはどれも評価されません。このポリシーは、PERMIT コマンドによって行われるアクセス・リストへの変更にのみ適用されます。UACC 自体に対する変更 (このためにリソースが公開リソースと見なされることがあります) は、このポリシー・プロファイルで制御されません。ACL に対する変更は、`ID(*)` のアクセス権限も含めて、すべてこのポリシーの適用対象です。`ID(*)` に付与されるアクセス権限は、`=STAR` ポリシーによっても制御されます。

ポリシー・プロファイル内の修飾子 =PUBLIC を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: ポリシーは実装されません。

NONE
: 端末ユーザーは、リソース・プロファイルのアクセス・リストを管理することを許可されません。

READ
: 端末ユーザーは、リソース・プロファイルのアクセス・リストから項目を削除することを許可されます。つまり、コマンド

```
PERMIT profile ID(any-id) DELETE
```

は、他のポリシーまたは RACF 権限によってコマンドの実行が防止されない限り、許可されます。

UPDATE
: 端末ユーザーは、この公開 ・リソース・プロファイルのアクセス・リストを管理することを許可されます。

CONTROL
: UPDATE と同じ。

- **C4R.***class*.**ACL.=DSN.***group.profile*

このポリシー・プロファイルは、データ・セット・グループに対するアクセス権限の付与を防止するために使用できます。データ・セット・プロファイルがグループを HLQ として定義されている場合は、そのグループがデータ・セット・グループと見なされます。変数 *group* は、アクセス・リストに追加される項目です。アクセス・リストでは、あらゆるタイプの項目 (ユーザー ID または GROUP) を示す用語として「user ID」が使用されます。このプロファイルでは、ポリシー・プロファイルがグループだけに適用されることを示すために、明示的に *group* という用語が使用されています。通常、ユーザー ID にはデータ・セット・プロファイルが定義されているため、アクセス・リスト項目がユーザー ID である場合は、このポリシー・プロファイルは適用されません。ほとんどのインストールで、2 つのアスタリスク (**) を使用して *group* と *profile* を表すことができます。追加の修飾子を指定することで、この一般規則の例外を作成できます。zSecure Command Verifier は、最も特定性の高いプロファイルのみを使用します。ポリシー・プロファイル内の修飾子 =DSN を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
: このポリシーは、この状態に対して実装されません。

NONE
: 端末ユーザーは、アクセス・リストにデータ・セット・グループを追加することを許可されません。

READ
: NONE と同じ。

UPDATE
端末ユーザーは、アクセス・リストに GROUP を追加することを許可されます。これは、この GROUP と等しい HLQ でデータ・セット・プロファイルが定義されている場合も同様です。

CONTROL
UPDATE と同じ。

- **C4R.***class*.**ACL./GROUP.***userid*.*profile*

  このポリシー・プロファイルは、ユーザー ID がアクセス・リストに追加されるのを防止するために使用できます。これは、標準アクセス・リストと条件付きアクセス・リストに適用されます。端末ユーザーにこのポリシー・プロファイルに対する十分なアクセス権限がない場合は、RACF グループのみをアクセス・リストに追加できます。変数 *userid* は、アクセス・リストに追加されるユーザーです。アクセス・リストでは、あらゆるタイプの項目 (ユーザー ID または GROUP) を示す用語として *userid* が使用されます。このプロファイルでは、user ID がユーザーの ID という限定された意味で使用されます。ほとんどのインストールにおいて、user ID と profile は 2 つのアスタリスクで表されます。追加の修飾子を指定することで、この一般規則の例外を作成できます。zSecure Command Verifier は、最も特定性の高いプロファイルのみを使用します。

  このポリシー・プロファイルを使用して、さらに 2 つの `/GROUP` ポリシー・プロファイル (**C4R**.*class*.**ACL./GROUP.=HLQTYPE.USER** と **C4R**.*class*.**ACL./GROUP.=HLQTYPE.GROUP**) を指定変更することもできます。

  ポリシー・プロファイル内の修飾子 `/GROUP` を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  プロファイルが見つからない
  このポリシーは、この状態に対して実装されません。

  NONE
  端末ユーザーは、アクセス・リストにユーザーを追加することを許可されません。

  READ
  NONE と同じ。

  UPDATE
  端末ユーザーは、個別のユーザー ID とグループを ACL に追加することを許可されます。

  CONTROL
  UPDATE と同じ。

- **C4R.***class*.**ACL./GROUP.=HLQTYPE.USER**

  このポリシー・プロファイルは、ユーザー・データ・セットのアクセス・リストへのユーザー ID の追加を防止するために使用できます。RACF で高位修飾子 (最初の修飾子) がユーザー ID として定義されている場合、データ・セットはユーザー・データ・セットと見なされます。このポリシー・プロファイルは、標準アクセス・リストと条件付きアクセス・リストに適用されます。アクセス・リストに追加する項目がユーザー ID であり、データ・セットがユーザー・データ・セットである場合は、端末ユーザーに現行のポリシー・プロファイルに対する十

分なアクセス権限が必要です。端末ユーザーに十分なアクセス権限がない場合は、**C4R.***class.***ACL./GROUP.***userid.profile* ポリシーを使用して現行のポリシーを指定変更することができます。**C4R.***class.***ACL./GROUP.***userid.profile* ポリシーでもアクセス・リストへのユーザー ID の追加が許可されない場合は、コマンドが拒否されます。この場合は、既存の RACF GROUP のみがアクセスを許可されます。

このポリシーは総称プロファイルを使用して定義できますが、ポリシー・プロファイル内の修飾子 /GROUP.=HLQTYPE は、ここに示されているとおりの形式で存在している必要があります。

プロファイルが見つからない
: このポリシーは、この状態に対して実装されません。

NONE
: 端末ユーザーは、アクセス・リストにユーザーを追加することを許可されません。ただし、**C4R.***class.***ACL./GROUP.***userid.profile* ポリシーにより、ユーザー・データ・セットのアクセス・リストにユーザーを追加することが許可される場合があります。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、個別のユーザー ID とグループをユーザー・データ・セットのアクセス・リストに追加することを許可されます。

CONTROL
: UPDATE と同じ。

- **C4R.***class.***ACL./GROUP.=HLQTYPE.GROUP**

このポリシー・プロファイルは、グループ・データ・セットのアクセス・リストへのユーザー ID の追加を防止するために使用できます。RACF で高位修飾子 (最初の修飾子) がグループとして定義されている場合、データ・セットはグループ・データ・セットと見なされます。このポリシー・プロファイルは、標準アクセス・リストと条件付きアクセス・リストに適用されます。アクセス・リストに追加する項目がユーザー ID であり、データ・セットがグループ・データ・セットである場合は、端末ユーザーに現行のポリシー・プロファイルに対する十分なアクセス権限が必要です。端末ユーザーに十分なアクセス権限がない場合は、**C4R.***class.***ACL./GROUP.***userid.profile* ポリシーを使用して現行のポリシーを指定変更することができます。**C4R.***class.***ACL./GROUP.***userid.profile* ポリシーでもアクセス・リストへのユーザー ID の追加が許可されない場合は、コマンドが拒否されます。この場合は、既存の RACF GROUP のみがアクセスを許可されます。

このポリシーは総称プロファイルを使用して定義できますが、ポリシー・プロファイル内の修飾子 /GROUP.=HLQTYPE は、ここに示されているとおりの形式で存在している必要があります。

プロファイルが見つからない
: このポリシーは、この状態に対して実装されません。

NONE
: 端末ユーザーは、アクセス・リストにユーザーを追加することを許可さ

れません。ただし、**C4R.***class.***ACL./GROUP.***userid.profile* ポリシーにより、グループ・データ・セットのアクセス・リストにユーザーを追加することが許可される場合があります。

READ
NONE と同じ。

UPDATE
端末ユーザーは、個別のユーザー ID とグループをグループ・データ・セットのアクセス・リストに追加することを許可されます。

CONTROL
UPDATE と同じ。

- **C4R.***class.***ACL./SCOPE.** *userid.profile*

  この一般ポリシー・プロファイルは、端末ユーザーがそのグループ SPECIAL の範囲外にあるユーザーをアクセス・リストに追加するのを防止するために使用できます。これは、標準アクセス・リストと条件付きアクセス・リストに適用されます。端末ユーザーにこのポリシー・プロファイルに対する十分なアクセス権限がない場合は、端末ユーザーの RACF グループ SPECIAL の範囲内にあるユーザーとグループのみをアクセス・リストに追加できます。変数 *userid* は、アクセス・リストに追加される項目です (ユーザー ID または GROUP のいずれか)。このプロファイルの記述では、RACF の用語 *userid* が、この特別な意味で使用されます。*profile* に追加の修飾子を指定することで、一般規則の例外を作成できます。ほとんどのインストールにおいて、*profile* は 2 つのアスタリスク (**) で表されることが予想されます。zSecure Command Verifier は、最も特定性の高いプロファイルのみを使用します。

  ポリシー・プロファイル内の `/SCOPE` 修飾子を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

  グループ SPECIAL またはシステム SPECIAL を持つ端末ユーザーが、自己の管理範囲内のユーザーまたはグループにアクセス権限を付与すると、そのことが監査専用ポリシー・プロファイルによって記録されます。

  – **C4R.USESCOPE.***group*

  このプロファイルに対して UPDATE 権限を使用して成功したアクセスが、SMF によって記録されます。修飾子 *group* は、RACF グループ・ツリーの最下位グループを表し、`PERMIT` コマンドで指定されたユーザーまたはグループに対するグループ SPECIAL 権限を付与します。端末ユーザーがシステム SPECIAL を持っている場合は、固定値 **=SYSTEM** が使用されます。

  /SCOPE ポリシー・プロファイルでは、RACF グループ SPECIAL 属性のみを使用して、項目を追加できるかどうかが決定されます。このプロファイルを実装すると、通常のユーザーが自分のデータ・セット・プロファイルのアクセス・リストを変更できなくなる可能性があります。これは、すべての項目がユーザーの範囲外と見なされるためです。 195 ページの『自分のデータ・セット・プロファイルを管理するためのポリシー・プロファイル』で説明した No-Store 機能を使用することで、同様の効果をより直接的に得られます。

/SCOPE ポリシー・プロファイルに対してサポートされているアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: このポリシーは、この状態に対して実装されません。

NONE
: 端末ユーザーは、グループ SPECIAL の範囲内にあるアクセス・リスト項目のみを追加または変更できます。端末ユーザーがグループ SPECIAL の範囲を持たない場合は、すべてのアクセス・リスト項目が範囲外と見なされます。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、グループ SPECIAL の範囲外にあるアクセス・リスト項目の追加または変更を許可されます。

CONTROL
: UPDATE と同じ。

条件付きアクセス・リストに対するポリシー・プロファイル

条件付きアクセス・リストの項目は、ID、アクセス・レベル、クラス、そのクラスのリソースという、複数の部分で構成されます。条件付きアクセス・リストで使用されているクラスおよびリソースは、他のクラスおよびリソースと区別するために、*when-class* および *when-resource* と呼ばれることがよくあります。

228 ページの『ACL に対する一般ポリシー・プロファイル』に記載した ID およびアクセス・レベル関連のポリシー・プロファイルは、条件付きアクセスにも適用されます。条件付きアクセス・リストで使用されるリソース名を制御するためのポリシー・プロファイルはありません。残る唯一のポリシー・プロファイルは when-class 用のものです。従来より、条件付きアクセス・リストに使用されていたクラスは PROGRAM クラスです。他のクラスを使用することも可能ですが、これが、今でも最もよく使用されています。when-class は、以下のポリシー・プロファイルを使用して記述されます。

- **C4R.***class*.**CONDACL.***whenclass.profile*

  このプロファイルは、条件付きアクセス・リストの項目を管理するための WHEN キーワードの使用を制御します。このプロファイルは、標準アクセス・リストに対するポリシー・プロファイルと組み合わせて使用されます。 CONDACL プロファイルは、*whenclass* の使用を制御します。プロファイル内の *whenclass* は、通常は **PERMIT** コマンドにおける WHEN キーワードの第 1 パラメーターです。CRITERIA 条件を使用する **PERMIT** コマンドの形式に対して例外を作成することができます。その場合は、基準名が代わりに使用されます。例えば、以下のコマンドを実行するとします。

  ```
  PERMIT DSND.USER01.HOMEWORK_GRADES.SELECT CLASS(MDSNTB) ID(STUDENT)
         WHEN(CRITERIA(SQLROLE('TEACHING ASSISTANT'))) ACCESS(READ)
  ```

  ポリシー・プロファイルで使用される *whenclass* は SQLROLE です。この設定によって、以下の 2 つのリソースに対するアクセス検査が行われます。

```
C4R.MDSNTB.ACL.STUDENT.READ.DSND.USER01.HOMEWORK_GRADES.SELECT
C4R.MDSNTB.CONDACL.SQLROLE.DSND.USER01.HOMEWORK_GRADES.SELECT
```

同様に、`WHEN(CRITERIA(SMS(DSENCRYPTION)))` を使用している場合は、以下の CONDACL ポリシー・リソースが使用されます。

`C4R.`*`class`*`.CONDACL.SMS.`*`profile`*

ポリシー・プロファイルでサポートされるアクセス・レベルは、以下のとおりです。

プロファイルが見つからない
: このポリシーは、この状態に対して実装されません。

NONE
: 端末ユーザーには、条件付きアクセス・リスト項目の指定が許可されません。

READ
: NONE と同じ。

UPDATE
: 条件付きアクセス・リスト項目の作成が許可されます。**ACL.***user.access* プロファイルによって、条件付きアクセス・リスト上のどの項目が許可されるかが決まります。

CONTROL
: UPDATE と同じ。

- **C4R.***class.***CONDACL.=RESET.***profile*

  このプロファイルは、条件付きアクセス・リスト全体をリセットして、条件付きアクセス・リストから全項目を除去する権限を制御します。RACF の **PERMIT RESET(WHEN)** 機能を使用すると、条件付きアクセス・リスト内のすべての項目に対して **PERMIT DELETE** コマンドを簡単に実行できます。`CONDACL.=RESET` プロファイルは、条件付きアクセス・リストをリセットする権限を制御するために使用されます。

  一般規則とは異なり、特殊値 `=RESET` は総称パターンで表すことができます。例えば、プロファイル **C4R.***class.***CONDACL.*.***profile* を使用して、条件付きアクセス・リストに対するすべての変更を防止することができます。

  プロファイルが見つからない
  : このポリシーは、この状態に対して実装されません。

  NONE
  : 端末ユーザーは、*class* 内の *profile* の条件付き ACL をリセットすることを許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : 条件付き ACL のリセットが許可されます。

  CONTROL
  : UPDATE と同じ。

リソースの追加的な識別情報

個別データ・セット・プロファイルには、RACF 標識が保存されているデバイスのボリュームとタイプに関する情報も含まれています。

以下の 2 つのプロファイルは、それぞれに示すキーワードの使用を制御します。

- **C4R.***class.***VOLUME.***dsname*

  このプロファイルは、ADDSD コマンドでの **VOLUME** キーワードの使用、および **ALTDSD** コマンドでの **ADDVOL**、DELVOL、**ALTVOL** の各キーワードの使用を制御します。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : **ADDSD** コマンドおよび **ALTDSD** コマンドでのボリューム名の指定または変更が許可されず、コマンドは失敗します。

  READ
  : NONE と同じ。

  UPDATE
  : 個別データ・セット・プロファイルでのボリュームの明示的な選択と管理が許可されます。

  CONTROL
  : UPDATE と同じ。

- **C4R.***class.***UNIT.***dsname*

  このプロファイルは、ADDSD コマンドでの **UNIT** キーワードの使用を制御します。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : **ADDSD** コマンドおよび **ALTDSD** コマンドでの装置タイプの指定または変更が許可されず、コマンドは失敗します。

  READ
  : NONE と同じ。

  UPDATE
  : 個別データ・セット・プロファイルでの装置タイプの明示的な選択と管理が許可されます。

  CONTROL
  : UPDATE と同じ。

DFP セグメント管理用のポリシー・プロファイル

DATASET DFP セグメントには、新規データ・セットの作成時にいくつかの属性のデフォルト情報が含まれます。このセクションで説明されている Command Verifier ポリシーを使用すると、ユーザーが新規データ・セットの以下の属性を管理できる制御が可能となります。

RESOWNER フィールドは、新規データ・セットの DATACLAS、MGMTCLAS、および STORCLAS のデフォルト値を決定するために使用する RACF ユーザーまたはグループを決定します。DATAKEY フィールドは、新規データ・セットを暗号化するために使用されるデフォルト暗号鍵のラベルを決定します。zSecure Command Verifier なしで、(システム SPECIAL か、FIELD プロファイルへのアクセスのいずれかによって) DFP セグメントへの更新アクセス権限を持つユーザーは、これらのフィールドを管理できます。Command Verifier により、データ・セットおよびユーザーのレベルでこのアクセスを制御できます。表 46 は、実装されたポリシー・プロファイルを示しています。

表 *46. DFP* セグメント情報を管理するためのキーワードおよびポリシー・プロファイル

キーワード	値	プロファイル
RESOWNER	n/a	**C4R.DATASET.DFP.RESOWNER.***profile*
DATAKEY	n/a	**C4R.DATASET.DFP.DATAKEY.***profile*

上記の表のプロファイルは、端末ユーザーが入力するキーワードの検証に使用できるポリシーを記述します。現在、Command Verifier は、これらのキーワードのパラメーターに指定される値のサポートを提供していません。以下のリストに、これらのポリシーとサポートされているアクセス・レベルについての詳細を示します。

- **C4R.DATASET.DFP.RESOWNER.***profile*

  このポリシー・プロファイルでは、データ・セット・プロファイルのデフォルト RESOWNER を設定する権限が記述されます。RESOWNER が指定されていない場合は、データ・セットの HLQ がデフォルト RESOWNER の決定に使用されます。RESOWNER の DFP セグメントは、新規データ・セットの DATACLAS、MGMTCLAS、および STORCLAS のデフォルト値を決定します。また、RESOWNER は、これらの SMS リソースへのアクセス権限を持つ必要がある ID も決定します。DFSMS がこれらのフィールドを使用する方法は、Parmlib メンバー IGDSMS*xx* 内の USE_RESOWNER オプションおよび ACSDEFAULTS オプションによって影響を受けることがあります。Command Verifier は、ポリシー・プロファイルに対して以下のアクセス・レベルをサポートします。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : 端末ユーザーは、RESOWNER の指定と削除を許可されません。コマンドはリジェクトされます。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、RESOWNER の指定と削除を許可されます。

  CONTROL
  : UPDATE と同じ。

- **C4R.DATASET.DFP.DATAKEY.***profile*

このポリシー・プロファイルでは、データ・セット・プロファイルのデフォルト DATAKEY を設定する権限が記述されます。指定された値は、データ・セット・プロファイルの対象とされる新規データ・セットを暗号化するために使用される CKDS 内の暗号鍵のラベルです。Command Verifier は、ポリシー・プロファイルに対して以下のアクセス・レベルをサポートします。

プロファイルが見つからない
: この制御は実装されません。

NONE
: 端末ユーザーは、DATAKEY の指定と削除を許可されません。コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 端末ユーザーは、DATAKEY の指定と削除を許可されます。

CONTROL
: UPDATE と同じ。

MFPOLICY セグメント管理用のポリシー・プロファイル

MFADEF リソース・クラスは、IBM Multi-Factor Authentication for z/OS が使用する情報の記録および定義を行うために使用されます。MFADEF クラスには、使用可能な要素およびポリシーを記述するプロファイルがあります。以下のセクションで、明示的なフレーズ「Command Verifier ポリシー」は、MFA ポリシーと zSecure ポリシーの間で混乱の可能性がある場合には必ず使用されます。

要素を記述する MFADEF プロファイルには、最初の修飾子としてストリング FACTOR があります。残りの修飾子は、IBM Multi-Factor Authentication for z/OS 製品がサポートする要素の名前です。ユーザーまたはポリシーの要素を指定する際、要素は MFADEF プロファイルによって定義される必要があります。また、要素の情報も、MFADEF プロファイルの MFA セグメント内で保守されます。この MFA セグメントの内容は、RACF コマンドを使用して管理することはできません。したがって、MFA セグメントを作成または削除する一般ポリシーを除いて、関連する zSecure Command Verifier ポリシーはありません。

ポリシーを記述する MFADEF プロファイルには、最初の修飾子としてストリング POLICY があります。残りの修飾子は、IBM Multi-Factor Authentication for z/OS 製品がサポートするポリシーの名前です。ユーザーにポリシーを割り当てる際、ポリシーは MFADEF プロファイルによって定義される必要があります。ポリシーに関する情報は、MFADEF プロファイルの MFPOLICY セグメントに定義されます。RACF コマンドを使用して、MFPOLICY セグメントを保守できます。zSecure Command Verifier は、MFPOLICY セグメントの内容の追加、削除、保守を制御するためのポリシーを提供します。

表 47. *MFPOLICY* 値の検査に使用されるプロファイル

キーワード	値	プロファイル
FACTOR ADDFACTOR DELFACTOR NOFACTOR	factor	**C4R.MFADEF.MFPOLICY.FACTOR.***factor-name.policy-profile* NOFACTOR の場合、Command Verifier ポリシー・プロファイル内の *factor-name* の値は、正符号 (+) です。
TOKENTIMEOUT	*value*	**C4R.MFADEF.MFPOLICY.ATTR.TOKENTIMEOUT.***policy-profile*
REUSE	YES/NO	**C4R.MFADEF.MFPOLICY.ATTR.REUSE.***policy-profile*

上記の表のプロファイルは、端末ユーザーが入力したキーワードと値の検証に使用できるポリシーを記述します。現在、Command Verifier は、ポリシーのサポートを FACTOR に指定される値に対して提供していますが、TOKENTIMEOUT および REUSE に指定される値に対しては提供していません。

- **C4R.MFADEF.MFPOLICY.FACTOR.***factor-name.policy-profile*

  このポリシー・プロファイルでは、ポリシーに対する要素名の指定、追加、または削除を行う権限が記述されます。端末ユーザーが NOFACTOR キーワードを使用すると、RACF はポリシーからすべての要素を削除します。このキーワードの場合は、Command Verifier でポリシーの名前が個別に検査されません。代わりに、特殊値 + (正符号) が *factor-name* に使用されます。特殊値 + を含む *factor-name* は、Command Verifier ポリシー・プロファイル内の総称パターンを使用して表すことができます。

  Command Verifier は、ポリシー・プロファイルに対して以下のアクセス・レベルをサポートします。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : 端末ユーザーは、ポリシーの FACTOR の指定と削除を許可されません。コマンドはリジェクトされます。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、ポリシーの FACTOR の指定と削除を許可されます。

  CONTROL
  : UPDATE と同じ。

- **C4R.MFADEF.MFPOLICY.ATTR.TOKENTIMEOUT.***policy-profile*

  このポリシー・プロファイルでは、TOKENTIMEOUT 値を指定する権限が記述されます。Command Verifier ポリシー・プロファイルは、TOKENTIMEOUT の新しい値を含んでいません。このポリシー・プロファイルは、(NOTOKENTIMEOUT キーワードを使用して) TOKENTIMEOUT 値をデフォルト値にリセットする場合にも使用されます。

  Command Verifier は、ポリシー・プロファイルに対して以下のアクセス・レベルをサポートします。

プロファイルが見つからない
この制御は実装されません。

NONE
端末ユーザーは、ポリシーの TOKENTIMEOUT 値の指定と削除を許可されません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
端末ユーザーは、ポリシーの TOKENTIMEOUT 値の指定と削除を許可されます。

CONTROL
UPDATE と同じ。

- **C4R.MFADEF.MFPOLICY.ATTR.REUSE.***policy-profile*

  このポリシー・プロファイルでは、トークン REUSE オプションを指定する権限が記述されます。Command Verifier ポリシー・プロファイルは、MFA トークンの再使用の許可および禁止に使用されます。

  Command Verifier は、ポリシー・プロファイルに対して以下のアクセス・レベルをサポートします。

  プロファイルが見つからない
  この制御は実装されません。

  NONE
  端末ユーザーは、ポリシーの REUSE オプションの管理を許可されません。コマンドはリジェクトされます。

  READ
  NONE と同じ。

  UPDATE
  端末ユーザーは、ポリシーの REUSE オプションの管理を許可されます。

  CONTROL
  UPDATE と同じ。

STDATA セグメント管理用のポリシー・プロファイル

STDATA セグメント内のいくつかの特定のフィールドは機密性が高いため、組織では STDATA プロファイルに対して、RACF によって既に提供されている以上の制御を維持しなければならない場合があります。

前述のように、RACF コマンド権限では、フィールド名自体は検査できますが、その値は検査できません。**フィールド・レベル・アクセス検査** を使用すると、端末ユーザーがシステム SPECIAL 属性を持っていない場合に、PRIVILEGED フラグの設定を特定のユーザーだけに制限することができます。**FIELD** クラスのプロファイルは、システム SPECIAL ユーザーの有無について検査されません。

さらに、一部のインストールでは、STDATA セグメント内の特定の USER 値および GROUP 値の割り当てを制限する必要があります。

zSecure Command Verifier では、STDATA セグメントに対する追加の制御を提供しています。これらの制御は、RACF 要件 (FIELD クラス内の該当するプロファイルへのシステム SPECIAL または UPDATE アクセス権限など) に追加されます。例えば、zSecure Command Verifier ポリシー・プロファイルを使用すると、システム SPECIAL を持つ RACF 管理者が PRIVILEGED 属性を偶発的に割り当てることを防止できます。

表 *48. STDATA* 値の検査に使用されるプロファイル： この表の項目は、クラス、セグメント、およびフィールドと、対応するポリシー・プロファイルを反映しています。

クラス	フィールド	プロファイル
STARTED	**PRIVILEGED**	**C4R.STARTED.STDATA.ATTR.PRIVILEGED.***started-profile*
STARTED	**TRUSTED**	**C4R.STARTED.STDATA.ATTR.TRUSTED.***started-profile*
STARTED	**TRACE**	**C4R.STARTED.STDATA.ATTR.TRACE.***started-profile*
STARTED		**C4R.STARTED.STDATA.=USER.***started-profile*
STARTED		**C4R.STARTED.STDATA./USER.***started-profile*
STARTED	*userid*	**C4R.STARTED.STDATA.USER.***userid.started-profile*
STARTED	**NOUSER**	**C4R.STARTED.STDATA.USER.=NONE**.*started-profile*
STARTED		**C4R.STARTED.STDATA.=GROUP.***started-profile*
STARTED		**C4R.STARTED.STDATA./GROUP.***started-profile*
STARTED	*group*	**C4R.STARTED.STDATA.GROUP.***group.started-profile*
STARTED	**NOGROUP**	**C4R.STARTED.STDATA.GROUP.=NONE**.*started-profile*

上記の表のプロファイルは、USER と GROUP の両方について、必須値とデフォルト値を記述します。また、端末ユーザーによって入力されたキーワードの値が受け入れ可能であるかどうかを検査するポリシーも記述します。

- **C4R.STARTED.STDATA.ATTR.PRIVILEGED.***started-profile*
- **C4R.STARTED.STDATA.ATTR.TRUSTED.***started-profile*
- **C4R.STARTED.STDATA.ATTR.TRACE.***started-profile*

これらのプロファイルは、STDATA セグメント内の属性の 1 つを設定する権限を指定します。「特権あり」属性は、結果的にほとんどの許可検査に合格します。インストール・システム出口は呼び出されず、SMF レコードも記録されません。これは、厳しく制御される必要があります。「トラステッド」属性は「特権あり」属性によく似ていますが、SMF レコードが書き込まれる場合があります。「トレース」属性は、STARTED プロファイルを使用して開始タスクに ID が割り当てられたときに、コンソールにレコードを書き込む必要があることを指定します。

プロファイルが見つからない
: 制御は実装されません。STDATA 属性の割り当ての制御には、RACF 権限だけが使用されます。

NONE
: 端末ユーザーは、この STARTED プロファイルに属性を割り当てることを許可されません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
属性設定が受け入れられます。ただし、依然として RACF 権限要件がコマンドの失敗の原因になる場合があります。

CONTROL
UPDATE と同じ。

- **C4R.STARTED.STDATA.=USER.***started-profile*
- **C4R.STARTED.STDATA.=GROUP.***started-profile*

これら 2 つの必須値ポリシー・プロファイルを使用して、これらの STDATA フィールドに必須値を割り当てることができます。必須値は、ポリシー・プロファイルの **APPLDATA** フィールドで指定する必要があります。zSecure Command Verifier は、**APPLDATA** の特殊値を認識しません。この設定は、値「=MEMBER」を USER に使用できます。この値は zSecure Command Verifier によって置換されず、STARTED プロファイルが使用された場合、RACF によって使用されます。

これらの必須値ポリシー・プロファイルは、STDATA セグメントを **RDEFINE** コマンドまたは **RALTER** コマンドによって追加する場合にだけ使用されます。既存の STDATA セグメントを変更する場合、必須値ポリシー・プロファイルは使用されません。この必須値プロファイルから取得された USER または GROUP は、追加のユーザーまたはグループ関連ポリシー・プロファイルによる支配を受けません。必須値プロファイルから取得された USER または GROUP 値は、追加のユーザーまたはグループ関連ポリシー・プロファイルによる支配を受けません。

ポリシー・プロファイル内の修飾子 =USER および =GROUP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
ポリシーは実装されません。結果として、必須値は強制されません。

NONE
アクションは実行されません。必須値は強制されません。

READ
APPLDATA フィールドが抽出され、コマンドで使用されます。

UPDATE
READ と同じ。

CONTROL
このポリシー・プロファイルは、端末ユーザーに対してアクティブにはされません。必須値は提供されません。端末ユーザーが USER または GROUP に指定した値が、コマンド内で使用されます。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。必須値

ポリシー・プロファイルでは、これらのプロファイルのために、アクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

•

現在、以下の **APPLDATA** 値が認識されます。

BLANK
この設定は、明示的な ID を挿入してはならないことを示すために使用されます。

id 他の値はすべて、STDATA セグメントに挿入する必要がある *userid* または *group* と見なされます。この値が有効なユーザー ID または GROUP であることを保証するための検査は、行われません。

- **C4R.STARTED.STDATA./USER.***started-profile*
- **C4R.STARTED.STDATA./GROUP.***started-profile*

これら 2 つのデフォルト値プロファイルを使用して、これらの STDATA フィールドにデフォルト値を割り当てることができます。デフォルト値は、ポリシー・プロファイルの **APPLDATA** フィールドで指定する必要があります。zSecure Command Verifier は、**APPLDATA** の特殊値を認識しません。この設定は、値「=MEMBER」を USER に使用できます。この値は zSecure Command Verifier によって置換されず、STARTED プロファイルが使用された場合、RACF によって使用されます。

これらのデフォルト値プロファイルは、USER または GROUP の値が指定されていない STDATA セグメントを、**RDEFINE** コマンドまたは **RALTER** コマンドによって追加する場合にのみ使用されます。既存の STDATA セグメントを変更する場合、デフォルト値ポリシー・プロファイルは使用されません。デフォルト値プロファイルから取得された USER または GROUP 値は、追加のユーザーまたはグループ関連ポリシー・プロファイルによる支配を受けません。

ポリシー・プロファイル内の修飾子 /USER および /GROUP を総称文字で表すことはできません。ここに示されているとおりのフォーマットで存在している必要があります。

プロファイルが見つからない
ポリシーは実装されません。デフォルト値は提供されません。

NONE
アクションは実行されません。デフォルト値は提供されません。

READ
APPLDATA フィールドが抽出され、コマンドで使用されます。

UPDATE
READ と同じ。

CONTROL
このポリシー・プロファイルは、端末ユーザーに対してアクティブにはされません。デフォルト値は提供されません。

注**:** このプロファイルのアクセス・レベルは階層的ではありません。一般的に、zSecure Command Verifier のポリシーは、CONTROL 以上のアクセス権限を持つユーザーには適用されません。また、アクセス権限が NONE である場合は、ポリシーが示す機能を端末ユーザーが使用できないことを示します。デフォルト値プロファイルでは、これらのプロファイルのために、アクセス権限 NONE の最終的な結果がアクセス権限 CONTROL と同じであるという変則的な状態になります。

現在、以下の **APPLDATA** 値が認識されます。

BLANK
この設定は、明示的な ID を挿入してはならないことを示すために使用されます。

id 他の値はすべて、STDATA セグメントに挿入する必要がある *userid* または *group* と見なされます。この値が有効なユーザー ID または GROUP であることを保証するための検査は、行われません。

- **C4R.STARTED.STDATA.USER.***userid.started-profile*
- **C4R.STARTED.STDATA.USER.=NONE**.*started-profile*

このポリシー・プロファイルは、*started-profile* の *userid* の有効値を指定します。特殊値 =NONE は、端末ユーザーが STDATA セグメントに NOUSER キーワードを指定したときに使用されます。この特殊値は、総称パターンで表すことができます。この設定は、ユーザーをある値に設定するのと同じポリシー・プロファイルからユーザー割り当てを解除することを処理できるようになります。以下のアクセス・レベルが使用されます。

プロファイルが見つからない
ポリシーは実装されません。ユーザーが指定した値は受け入れられます。

NONE
指定された USER は許可されません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
USER に指定された値は受け入れられます。

CONTROL
UPDATE と同じ。

- **C4R.STARTED.STDATA.GROUP.***group.started-profile*
- **C4R.STARTED.STDATA.GROUP.=NONE**.*started-profile*

このポリシー・プロファイルは、*started-profile* の *group* の有効値を指定します。特殊値 =NONE は、端末ユーザーが STDATA セグメントに NOGROUP キーワードを指定したときに使用されます。この特殊値は、総称パターンで表すことができます。この設定は、グループをある値に設定するのと同じポリシー・プロファイルからグループ割り当てを削除する処理ができるようになります。以下のアクセス・レベルが使用されます。

プロファイルが見つからない
ポリシーは実装されません。ユーザーが指定した値は受け入れられます。

NONE
指定された GROUP は許可されません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
GROUP に指定された値は受け入れられます。

CONTROL
UPDATE と同じ。

その他のリソース関連ポリシー・プロファイル

データ・セット・プロファイルおよび一般リソース・プロファイルには、カテゴリー化が容易ではないいくつかのフィールドがあります。これらの一部については、属性 という用語が適切です。このセクションでは、残りのフィールドおよび属性について説明します。

以下の表の「キーワード」列には、「コマンド」列に示す RACF コマンドで指定されるキーワードとパラメーターを示します。「プロファイル」列には、コマンド、キーワード、およびパラメーターの組み合わせに対して適用される Command Verifier のポリシー・プロファイルを示します。

表 *49.* リソース・プロファイル設定に使用されるプロファイル

コマンド	キーワード	プロファイル
ADDSD	*noset* *setonly*	**C4R.DATASET.RACFIND.***set-value.profile*
ADDSD **RDEFINE**	総称 モデル *tape* *discrete*	**C4R.***class.***TYPE.***type-value.profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	*level*	**C4R.***class.***LEVEL.***level.profile*
RDEFINE **RALTER**	**APPLDATA**	**C4R.***class.***APPLDATA.***profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**AUDIT(SUCCESS(***level***))**	**C4R.***class.***AUDIT.SUCCESS.***level.profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**AUDIT(FAILURES(***level***))**	**C4R.***class.***AUDIT.FAIL.***level.profile*

表 49. リソース・プロファイル設定に使用されるプロファイル (続き)

コマンド	キーワード	プロファイル
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**ADD/DEL CATEGORY**	**C4R.***class*.**CATEGORY.***category.profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**(NO)DATA**	**C4R.***class*.**INSTDATA.***profile*
ADDSD **ALTDSD**	**NO(ERASE)**	**C4R.DATASET.ATTR.ERASE.***profile*
ALTDSD **RALTER**	**GLOBALAUDIT(SUCCESS(***level***))**	**C4R.***class*.**GLOBALAUDIT.SUCCESS.***level.profile*
ALTDSD **RALTER**	**GLOBALAUDIT(FAILURES(***level***))**	**C4R.***class*.**GLOBALAUDIT.FAIL.***level.profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**(NO)NOTIFY**	**C4R.***class*.**NOTIFY.***notify-id.profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**(NO)SECLABEL**	**C4R.***class*.**SECLABEL.***seclabel.profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**(NO)SECLEVEL**	**C4R.***class*.**SECLEVEL.***seclevel.profile*
RDEFINE **RALTER**	**SINGLEDSN**	**C4R.***class*.**ATTR.SINGLEDSN.***profile*
RDEFINE **RALTER**	**TIMEZONE**	**C4R.***class*.**ATTR.TIMEZONE.***profile*
RDEFINE **RALTER**	**TVTOC**	**C4R.***class*.**ATTR.TVTOC.***profile*
ADDSD **ALTDSD**	**RETPD**	**C4R.DATASET.RETPD.***profile*
ADDSD **ALTDSD** **RDEFINE** **RALTER**	**NO(WARNING)**	**C4R.***class*.**ATTR.WARNING.***profile*
RDEFINE **RALTER**	**WHEN**	**C4R.***class*.**ATTR.WHEN.***profile*

その他のポリシー・プロファイルとアクセス・レベルの説明

このセクションでは、データ・セット・プロファイルおよび一般リソース・プロファイルの他のフィールドおよび属性で使用可能なポリシー・プロファイルに関して、サポートされるアクセス・レベルと具体的な処理について説明します。

- **C4R.DATASET.RACFIND.***value.profile*

  このポリシー・プロファイルでは、データ・セットに対する RACF 標識ビットの設定を制御できます。変数 *value* は、NOSET または SETONLY として指定できます。RACF では明示的な値 SET もサポートされていますが、この設定は、総称プロファイルを定義する場合のような適切ではない数多くの状況で、デフォルトとして設定され無視される可能性があります。NOSET キーワードは、個別プロファイルに対して RACF 標識を変更しないようにすることを指定します。SETONLY キーワードは、テープ・データ・セットが個別プロファイルの対象とされること、および TVTOC のみを更新する必要があることを指定します。以下のアクセス規則が適用されます。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : NOSET キーワードまたは SETONLY キーワードの指定は許可されず、コマンドは失敗します。

  READ
  : NONE と同じ。

  UPDATE
  : RACF 標識フラグの明示的な操作が許可されます。

  CONTROL
  : UPDATE と同じ。

- **C4R.***class.***TYPE.***type.profile*

  このポリシー・プロファイルは、作成されるプロファイルのタイプを制御します。このプロファイルは、**ADDSD** コマンドと **RDEFINE** コマンドにのみ適用されます。*type* に指定できる値は以下のとおりです。

  – **GENERIC**
  – **MODEL**
  – **TAPE**
  – **DISCRETE**

  最初の 3 つの値は、ほとんどの RACF コマンドでキーワードとして指定できます。これらのキーワードを使用すると、zSecure Command Verifier でそれらがポリシー・プロファイルのプロファイル・タイプとして使用されます。これらのキーワードを指定しなかった場合は、zSecure Command Verifier でリソース・プロファイルが検査されて、個別プロファイルと総称プロファイルのどちらが作成されるかが決定され、それに応じてプロファイル・タイプの値が設定されます。

  個別データ・セット・プロファイルは、操作上の特性とセキュリティー管理の煩雑さのために推奨されていません。ただし、個別プロファイルが優先される特別な状態もあります。インストール済み環境によっては、すべての個別プロファイルが自動的に総称プロファイルに変換されるようになっています。組織での運用手順が変更されない場合、RACF のパフォーマンスに深刻な影響が出る可能性があります。

一般リソースの個別プロファイルが、個別データ・セット・プロファイルに関連する望ましくない副次作用をもたらすことはありません。一般には、複数のリソースを保護する 1 つ以上のプロファイルの必要性に基づいて、個別プロファイルと総称プロファイルを選択する必要があります。

zSecure Command Verifier では、個別プロファイルまたは総称プロファイルの使用について管理者が意識的に決断できるようにするポリシーを提供しています。ポリシー・プロファイルを使用すると、個別データ・セット・プロファイルの作成をグローバルに禁止する一方で、例外の余地を残すことができます。これを行うには、リソース・プロファイルをポリシー・プロファイルに組み込みます。

多くの場合、以下のポリシー・プロファイルの例で示すように、2 つのアスタリスク (**) を使用して、ポリシー・プロファイルのプロファイル部分を表すことができます。

```
C4R.DATASET.TYPE.DISCRETE.**       UACC(NONE)
C4R.DATASET.TYPE.DISCRETE.SYS1.**  UACC(UPDATE)
C4R.FACILITY.TYPE.*.**             UACC(UPDATE)
```

上記の 3 番目のタイプのプロファイルは、このリソース・クラスに他のポリシーが実装されている場合にのみ必要となります。このプロファイルは、個別プロファイルと総称プロファイルの両方の作成を許可する特定性の高いプロファイルを作成する場合に必要となることがあります。

このポリシー・プロファイルに使用できるアクセス・レベルは以下のとおりです。

プロファイルが見つからない
: この制御は実装されません。すべてのユーザーが、個別プロファイル、総称プロファイル、およびその他のタイプのプロファイルを作成できます。

NONE
: 特定タイプのプロファイルの作成が許可されず、コマンドは失敗します。プロファイルのタイプは、端末ユーザーが指定するか、または zSecure Command Verifier によって自動的に決定されます。

READ
: NONE と同じ。

UPDATE
: このタイプのプロファイルの作成が許可されます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**LEVEL.***level*.*profile*

このポリシー・プロファイルを使用して、レベルの割り当てを制御できます。このポリシーは、LEVEL(00) で新しいリソース・プロファイルを作成するときには使用されません。アクセス・レベルに応じて、このポリシー・プロファイルは、他の値で、または既存のリソース・プロファイルの値を変更するときに、使用さ

れることがあります。リソース・プロファイルの LEVEL を SECLEVEL と混同しないようにしてください。LEVEL 値は、RACF ではどのような目的にも使用されません。

プロファイルが見つからない
: この制御は実装されません。

NONE
: LEVEL *level* を *profile* に割り当てることは許可されず、コマンドは失敗します。

READ
: NONE と同じ。

UPDATE
: リソース・プロファイルに対するこの LEVEL の割り当てが許可されます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**APPLDATA.***profile*

このプロファイルは、リソース・プロファイルのアプリケーション・データを変更する権限を制御するために使用されます。通常は、プロファイルの所有者および (グループ) SPECIAL 権限を持つユーザーが制限されます。このプロファイルは、それ以外の制約事項を実装します。このプロファイルに使用できるアクセス・レベルは以下のとおりです。

プロファイルが見つからない
: この制御は実装されません。RACF 許可のあるすべてのユーザーが、それぞれの制御の範囲内でリソース・プロファイルの **APPLDATA** を変更できます。

NONE
: インストール・データの指定は許可されず、コマンドは失敗します。これは、**RDEFINE** および **RALTER** の両方に適用されます。

READ
: **RDEFINE** コマンドでの **APPLDATA** の指定が許可されます。その後に **RALTER** コマンドで値を変更することはできません。

UPDATE
: **APPLDATA** の変更が許可されます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**AUDIT.SUCCESS.***level.profile*
- **C4R.***class*.**AUDIT.FAIL.***level.profile*

これらのポリシー・プロファイルを使用すると、AUDIT キーワードで指定されているように、アクセス監査 SUCCESSFUL または FAILED の設定を制御できます。AUDIT 値を表示したり設定したりすることは、通常は制限されません。

指定されたレベル以上のすべてのアクセス権限について、SMF による監査を指定できます。成功の監査を設定する場合用と失敗の監査を設定する場合用に別個のポリシー・プロファイルが存在します。このポリシー・プロファイルでは、以下のアクセス・レベルがサポートされています。

プロファイルが見つからない
: この制御は実装されません。

NONE
: 指定されたアクセス・レベルでの成功または失敗の監査の割り当てはサポートされません。コマンドはリジェクトされます。

READ
: NONE と同じ。

UPDATE
: 指定されたアクセス・レベルでの成功または失敗の監査を割り当てることができます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**CATEGORY.***category*.*profile*

このプロファイルを使用して、セキュリティー・カテゴリーの割り当てを制御できます。通常は、RACF 管理者が、自分の CATEGORY を自分の範囲内にあるリソース・プロファイルに割り当てることができます。セキュリティー・カテゴリーは、リソースへのアクセスを防止する追加の方法として使用できます。ユーザーは、少なくともリソースに割り当てられたすべてのセキュリティー・カテゴリーを持っている必要があります。現在のプロファイルでは、リソース・プロファイルに対する CATEGORY の割り当てと除去を制御できます。

プロファイルが見つからない
: この制御は実装されません。*category* を割り当てられている管理者は、自分の範囲内にあるリソース・プロファイルに対して、この CATEGORY の割り当てと除去を行うことができます。

NONE
: *profile* に対する CATEGORY *category* の割り当てと除去は許可されず、コマンドは失敗します。これは、カテゴリーの設定または変更に使用されるすべてのコマンドに適用されます。

READ
: システム SPECIAL ユーザーは、この *profile* に対して *category* の割り当てと除去を行うことができます。

UPDATE
: *category* を割り当てられている管理者は、自分の範囲内にあるリソース・プロファイルにこのレベルを割り当てることができます。それらの管理者は、*category* を除去する権限も持ちます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**INSTDATA.***profile*

  このプロファイルは、リソース・プロファイルのインストール・データを変更する権限を制御するために使用されます。通常は、プロファイルの所有者および (グループ) SPECIAL 権限を持つユーザーが制限されます。このプロファイルは、それ以外の制約事項を実装します。

  INSTDATA ポリシー・プロファイルには、インストール・データに必要なフォーマットの参照を含めることもできます。フォーマットの名前は、最適ポリシー・プロファイルの APPLDATA によって指定できます。フォーマットの名前を使用して、適切な (一連の) フォーマット指定ポリシー・プロファイルを決定します。フォーマット指定ポリシー・プロファイル (または短形式プロファイル) では、以下のような名前が付けられます。

  C4R.*class*.INSTDATA.=FMT.*format-name*.POS(*start*:*end*)

  複数のフォーマット・プロファイルを使用して、リソース・プロファイルのインストール・データのさまざまな部分を指定することができます。フォーマット・プロファイルについて詳しくは、 254 ページの『インストール・データ・フィールドのフォーマットの制約事項』を参照してください。

  このプロファイルには、以下のアクセス・レベルを使用できます。

  プロファイルが見つからない
  : この制御は実装されません。RACF 許可のあるすべてのユーザーが、それぞれの制御の範囲内でリソース・プロファイルのインストール・データを変更できます。

  NONE
  : インストール・データの指定は許可されず、コマンドは失敗します。これは、INSTDATA の設定または変更に使用されるすべてのコマンドに適用されます。

  READ
  : **ADDSD** および **RDEFINE** コマンドでのインストール・データの指定が許可されます。この値を後から **ALTDSD** または **RALTER** コマンドで変更することはできません。

  UPDATE
  : インストール・データの変更が許可されます。

  CONTROL
  : この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

  APPLDATA で指定されるオプションの値を以下で説明します。

  format *profile* のインストール・データに使用する必要があるフォーマットの名前。フォーマット 名を使用して、適切な一連のフォーマット・プロファイルを見つけます。

- **C4R.***class*.**ATTR.ERASE.***profile*
- **C4R.***class*.**ATTR.SINGLEDSN.***profile*
- **C4R.***class*.**ATTR.TIMEZONE.***profile*

- **C4R.***class*.**ATTR.TVTOC.***profile*

  これらの 4 つの属性関連のポリシー・ルールは、同じアクセス規則を使用します。指定可能な UACC および ACL の値を以下で説明します。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : 端末ユーザーは、**ADDSD** および **RDEFINE** コマンドで、どちらのキーワードの指定も許可されません。これらのコマンドでは、非属性キーワードが許可されます。

  READ
  : NONE と同じ。

  UPDATE
  : 端末ユーザーは、**ALTDSD**、**RALTER**、**ADDSD**、および **RDEFINE** の各コマンドによる属性の設定と除去を許可されます。これにより、これらの属性の通常の保守が可能となります。

  CONTROL
  : この制御は、端末ユーザーに対して実装されません。これにより、これらの属性の通常の保守が可能となります。

- **C4R.***class*.**GLOBALAUDIT.SUCCESS.***level.profile*
- **C4R.***class*.**GLOBALAUDIT.FAIL.***level.profile*

  これらのポリシー・プロファイルを使用すると、GLOBALAUDIT キーワードで指定されているように、アクセス監査 SUCCESSFUL または FAILED の設定を制御できます。GLOBALAUDIT 値を表示したり設定したりするのは、通常は、RACF AUDITOR 属性を持つユーザーに制限されています。指定されたレベル以上のすべてのアクセス権限について、SMF による監査を指定できます。成功の監査を設定する場合用と失敗の監査を設定する場合用に別個のポリシー・プロファイルが存在します。このポリシー・プロファイルでは、以下のアクセス・レベルがサポートされています。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : 指定されたアクセス・レベルでの成功または失敗の監査の割り当てはサポートされません。コマンドはリジェクトされます。

  READ
  : NONE と同じ。

  UPDATE
  : 指定されたアクセス・レベルでの成功または失敗の監査を割り当てることができます。

  CONTROL
  : この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**NOTIFY.***notify-id.profile*

このプロファイルでは、Notify-ID の設定を制御できます。通常は、RACF 管理者がアクセス違反メッセージを受け取る TSO ユーザーを指定します。このポリシー・プロファイルでは、Notify-ID の指定と選択を行う権限を制御できます。

プロファイルが見つからない
: この制御は実装されません。管理者が、通知メッセージを送る TSO ユーザーを指定し、選択します。

NONE
: Notify-ID の設定は許可されず、コマンドは失敗します。

READ
: NONE と同じ。

UPDATE
: Notify-ID の設定と選択が許可されます。

CONTROL
: この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**SECLABEL.***seclabel.profile*

  現在、SECLABEL に対するサポートは限定的であることに注意してください。データ・セット・リソースまたは一般リソースに対する SECLABEL の割り当てを制御することができます。ただし、SECLABEL の削除を制御することはできません。

- **C4R.***class*.**SECLEVEL.***seclevel.profile*

  現在、SECLEVEL に対するサポートは限定的であることに注意してください。データ・セット・リソースまたは一般リソースに対する SECLEVEL の割り当てを制御することができます。ただし、SECLEVEL の削除を制御することはできません。

- **C4R.***class*.**RETPD.***profile*

  このポリシー・プロファイルは、テープ・データ・セットの RETPD の設定を制御します。

  プロファイルが見つからない
  : この制御は実装されません。RETPD の設定と変更を行うことができます。

  NONE
  : 保存期間を設定または変更することはできません。JCL パラメーターの有無およびその値に基づいた RACF 保存期間の設定は防止されません。

  READ
  : NONE と同じ。

  UPDATE
  : テープ・データ・セットのRETPD の指定および除去が許可されます。

  CONTROL
  : この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

- **C4R.***class*.**ATTR.WARNING.***profile*

  このプロファイルでは、リソース・プロファイルの WARNING または NOWARNING 属性の設定を制御できます。WARNING 属性を指定すると、プロファイルで定義されたリソース・アクセス規則が事実上無効になります。システムのすべてのユーザーが、リソース・プロファイルで保護されたリソースに対してあらゆる操作を実行できます。UACC(ALTER) との唯一の違いは、通常のプロファイルである場合にアクセス権限が付与されていないことを通知する追加の警告メッセージが生成される点です。

  プロファイルが見つからない
  : この制御は実装されません。

  NONE
  : 端末ユーザーは、**ADDSD**、**ALTDSD**、**RDEFINE**、**RALTER** の各コマンドで WARNING や NOWARNING を指定することを許可されません。ADDSD および **RDEFINE** コマンドでは **NOWARNING** キーワードが許可 (デフォルトで設定) されます。

  READ
  : 端末ユーザーは、ALTDSD および **RALTER** コマンドで **NOWARNING** 属性キーワードを明示的に指定することを許可されます。これにより、これらの属性の除去が可能となります。

  UPDATE
  : 端末ユーザーは、4 つの関連コマンドすべてで、両方のキーワードを指定することを許可されます。これにより、これらの属性の通常の保守が可能となります。

  CONTROL
  : UPDATE と同じ。

- **C4R.***class*.**ATTR.WHEN.***profile*

  この単一のポリシー・プロファイルは、端末に対する WHEN(DAYS) 指定と WHEN(TIME) 指定の両方の設定を制御します。この 2 つのオプションによって、端末を使用できる曜日と時刻が制御されます。

  プロファイルが見つからない
  : この制御は実装されません。WHEN(DAYS) および WHEN(TIME) を指定できます。

  NONE
  : LOGON 制約事項の指定は許可されません。

  READ
  : NONE と同じ。

  UPDATE
  : LOGON 制約事項の指定と除去が許可されます。

  CONTROL
  : この制御は、この端末ユーザーに対して実装されません。制約事項は課せられません。

インストール・データ・フィールドのフォーマットの制約事項

このトピックに記載されているガイドラインでは、RACF プロファイルのインストール・データ・フィールドのフォーマット規則ポリシー・プロファイルを実装する方法について説明します。

すべての RACF プロファイルには、インストール用途のために予約されたフィールドがあります。多くの組織が、このインストール・データ・フィールドをさまざまな目的で使用しています。このインストール・データ・フィールドについて RACF が特定の使用法を推奨することはありません。業界においても、インストール・データ・フィールドの使用法に関する実質的な基準はありません。業界全体で唯一合意が存在しているのは、グループ・プロファイルに関してのようです。グループ・プロファイルでは、インストール・データによってグループの使用方法 (特定のアプリケーションの HLQ や、特定のアプリケーションに対する特定のジョブのアクセス権限など) がテキストで記述されます。

RACF では、インストール・データ・フィールドが単に可変長のテキスト・ストリングと見なされます。RACF コマンドに対する唯一の制約事項は、フィールドの長さ (最大 255 文字) および小文字の英字から大文字への自動変換です。ただし、組織がインストール・データ・フィールドの特定の位置を特定の目的に使用したいと考える場合もあります。zSecure Command Verifier は、インストール・データ・フィールドのフォーマットに対する制約事項の適用をサポートしています。この制限は、名前の付いた一連のフォーマット規則ポリシー・プロファイルを定義することで実装されます。これらのプロファイルには以下のような名前が付けられます。

C4R.*class*.INSTDATA.=FMT.*format-name*.POS(*start*:*end*)

format-name は、クラス *class* 内のターゲット・プロファイルのインストール・データを管理する権限を制御するポリシー・プロファイル (INSTDATA ポリシー・プロファイル) の APPLDATA で指定されます。例えば、*SYS1.* が所有する *IBMUSER* の INSTDATA プロファイルは以下のようになります。

```
C4R.USER.INSTDATA.SYS1.IBMUSER
       Appldata('SYS1FMT')
```

この例でのフォーマット名 は **SYS1FMT** です。したがって、IBMUSER のフォーマット・プロファイルは以下のようになります。

C4R.USER.INSTDATA.=FMT.SYS1FMT.POS(*start*:*end*)

複数のフォーマット・プロファイルを定義して、インストール・データ・フィールドのさまざまな部分を指定することができます。各部分は、*start* と *end* の位置で示されます。ユーザー ID、グループ、およびリソース・プロファイルのフォーマット指定は、すべて個別に指定する必要があります。特定のリソース・クラスにプロファイルが存在しない場合は、INSTDATA フォーマット用の総称ポリシー・プロファイルを使用することもできます。次の形式の総称プロファイルのみがサポートされています。

C4R.*.INSTDATA.=FMT.*format-name*.POS(*start*:*end*)

リソース *class* は、アスタリスクで置き換えることができます。リソース・クラスに部分的な総称を指定することはできません。特定のリソース・クラスにフォーマット・プロファイルが定義されている場合は、総称フォーマット・プロファイルがすべて無視されます。

フォーマットの zSecure Command Verifier ポリシー・プロファイルは、階層方式で設計されています。

- 以下に示すサンプルは、最上位ポリシー・プロファイルの構造です。

  C4R.*class*.INSTDATA.*profile*

  最上位ポリシー・プロファイルは、INSTDATA に対してユーザーが持つ必要があるアクセス権限を指定するとともに、FORMAT ポリシーを見つけるために使用されるフォーマット名 (*format-name*) を APPLDATA で指定します。
- 次のレベルのポリシー・プロファイルは、FORMAT ポリシーのセットを形成します。最大 10 個の FORMAT プロファイルを指定できます。これらのプロファイルは、以下のように構造化されています。

  C4R.*class*.INSTDATA.=FMT.*format-name*.POS(*start*:*end*)

  これらのプロファイルは、フォーマット規則と、それらのフォーマット規則へのユーザーのアクセス権限を指定します。フォーマット規則は、FORMAT ポリシー・プロファイルの APPLDATA の一部として組み込まれます。
- フォーマット規則は、コンマ区切り値のリストとして指定され、追加のブランクは含まれません。

  'NB,ALPHA'

  'NB,LIST(EXPIRED,DELETE,STARTED)'

  使用できるフォーマット規則については、 258 ページの『フォーマット規則』で説明しています。現在実装されているフォーマット規則は以下のとおりです。

  NB, NC, ALPHA, NUM, ALPHANUM, PICT, LIST, LISTX, =USERID, =GROUP
- 一部のフォーマット規則では、括弧で囲んだ追加の指定が必要です。対象となるフォーマット規則は、PICT(ピクチャー・ストリング)、LIST(ストリングのリスト)、および LISTX(ストリングのリスト) です。これらの規則については、以降のセクションで説明します。

関係するプロファイルを以下の 2 つの表にまとめています。その後のセクションでは、これらのプロファイルに対して必要なアクセス権限と、フォーマット規則 に指定できる値について説明します。

表 *50. INSTDATA* 検査に使用されるプロファイル： この表に示すプロファイルは、INSTDATA を管理する権限を記述するものであり、INSTDATA フォーマット・プロファイルを特定するために使用されます。

クラス	プロファイル	**Appldata**
USER	**C4R.USER.INSTDATA.***owner.userid*	フォーマット名
GROUP	**C4R.GROUP.INSTDATA.***owner.group*	フォーマット名
DATASET	**C4R.DATASET.INSTDATA.***hlq.rest-of-profile*	フォーマット名
class	**C4R.***class***.INSTDATA.***profile*	フォーマット名

次の表では、フォーマット規則に使用されるポリシー・プロファイルについて説明しています。これらのプロファイルは、フォーマット・プロファイルと呼ばれます。このプロファイルの APPLDATA を使用して、フォーマット規則が指定されます。

表 *51. INSTDATA* 検査に使用されるプロファイル： この表のプロファイルでは、INSTDATA のフォーマット・プロファイルが記述されます。APPLDATA は、フォーマット規則を記述するために使用されます。

クラス	プロファイル	**Appldata**
class	**C4R.***class***.INSTDATA.=FMT.***format-name***.POS(***start***:***end***)**	フォーマット規則
class	**C4R.*.INSTDATA.=FMT.***format-name***.POS(***start***:***end***)**	フォーマット規則

INSTDATA ポリシー・プロファイル

いくつかの zSecure Command Verifier ポリシー・プロファイルは、特定のプロファイルの INSTDATA を変更する権限の制御に使用します。これらのプロファイルを使用して、プロファイルのフォーマット名 (またはプロファイルのタイプ) を指定することもできます。

開始点となるのは、INSTDATA の変更を制御するために使用されるプロファイルです。このプロファイルを使用して、該当する INSTDATA フォーマット記述を見つけます。

- **C4R.***class***.INSTDATA.***profile*

  通常、権限は、プロファイルの所有者、および (グループ) SPECIAL 権限を持つユーザーだけに既に制限されています。このプロファイルは、それ以外の制約事項を実装します。INSTDATA プロファイルに使用できるアクセス・レベルは以下のとおりです。

  プロファイルが見つからない
  : この制御は実装されません。RACF 許可のあるすべてのユーザーが、それぞれの制御の範囲内でユーザーのインストール・データを変更できます。

  NONE
  : インストール・データの指定は許可されず、コマンドは失敗します。**INSTDATA** の変更が許可されないため、APPLDATA フィールドは使用されません。

  READ
  : **ADDUSER** や **RDEFINE** などの追加コマンドおよび定義コマンドで、インストール・データを指定することができます。その後に **ALTUSER** や **RALTER** などの変更コマンドを使用して値を変更することはできません。**APPLDATA** で指定されるフォーマット名を使用して、INSTDATA の適切な規則を見つけます。

  UPDATE
  : インストール・データの変更が許可されます。**APPLDATA** で指定されるフォーマット名を使用して、INSTDATA の適切な規則を見つけます。

  CONTROL
  : INSTDATA 制御は、この端末ユーザーに対して実装されません。ただし、**APPLDATA** で指定されるフォーマット名を使用して、INSTDATA の適切な規則を見つけます。

  APPLDATA で指定されるオプションの値を以下で説明します。

フォーマット名

profile のインストール・データに使用する必要があるフォーマットの名前。フォーマット名 を使用して、フォーマット規則を記述する適切な一連のフォーマット・プロファイルを見つけます。

フォーマット・プロファイル

INSTDATA フィールドのさまざまな部分のフォーマットを制御するプロファイルを実装するには、このトピックに記載されているガイドラインに従ってください。

フォーマット名ごとに最大 10 個の異なるフォーマット・プロファイルを定義して、プロファイルの INSTDATA を構成する 10 個の部分を制御できます。上記のプロファイルの **APPLDATA** フィールドにブランク以外の値が入っている場合、zSecure Command Verifier はフォーマット・プロファイルを見つけようとします。INSTDATA の各セクションは、フォーマット・プロファイル内の *start* 変数と *end* 変数によって定義されます。

あるフォーマット・プロファイルで指定されている **INSTDATA**フィールドの *start* から *end* の範囲が、他のフォーマット・プロファイルの同じフィールドとオーバーラップする可能性があります。その場合は、オーバーラップする部分が両方のフォーマット規則に従っている必要があります。フォーマット・プロファイルには、複数のフォーマット規則を含めることができます。これらの規則は、コンマで区切られたリストとして指定する必要があります。この結合されたフォーマット規則の例を以下に示します。

```
NB,NC,ALPHA,LISTX(EXPIRED)
```

このサンプルは、インストール・データ・フィールドのこの部分が必須指定であり (NB)、変更不可である (NC) ことを表しています。この NoChange (変更不可) 要件をバイパスすることをユーザーが許可されている場合、このフィールドにはすべて英字で、かつ **EXPIRED** 以外の値を指定する必要があります。

- **C4R.***class***.INSTDATA.=FMT.***format-name***.POS(***start***:***end***)**

  このプロファイルは、INSTDATA の一部分のフォーマットを記述するために使用されます。この部分は、*start* と *end* で指定されます。 *start* と *end* の値は、どちらも 3 桁の数字で指定する必要があります。*end* 値は *start* 値以上で、かつ 255 以下でなければなりません。*start* 値は 001 以上にする必要があります。フォーマット・プロファイルに使用できるアクセス・レベルは以下のとおりです。

  このプロファイルは個別ポリシー・プロファイルです。*class* は、単一の総称アスタリスクで置き換えることができます。ただし、この総称プロファイルは、一致するフォーマット・プロファイルが 1 つも存在しない場合にのみ使用されます。

  NONE

  フォーマット規則のセットがこの端末ユーザーに適用されます。新しい INSTDATA は、すべてのフォーマット規則に従っている必要があります。

  READ

  フォーマット規則のセットがこの端末ユーザーに適用されます。NB フォーマット規則は、指定されていても適用されません。それ以外のすべてのフォーマット規則に従っている必要があります。

UPDATE
フォーマット規則のセットがこの端末ユーザーに適用されます。NB および NC フォーマット規則は、指定されていても適用されません。それ以外のすべてのフォーマット規則に従っている必要があります。

CONTROL
フォーマット規則のセットはこの端末ユーザーに適用されません。

APPLDATA では、INSTDATA の特定のセクションに適用されるフォーマット規則が記述されます。

フォーマット規則のセット
INSTDATA の該当する部分に対して許容される内容を記述するフォーマット規則。指定可能なフォーマット規則について詳しくは、次のセクションを参照してください。

フォーマット規則

以下のフォーマット規則を使用して、INSTDATA フィールドのフォーマット・プロファイルを実装します。

表 52 は、zSecure Command Verifier で認識される使用可能なフォーマット規則をまとめたものです。指定したフォーマット規則がこの表にリストされていない場合は、フォーマット・プロファイルに指定したフォーマット規則のセット全体が無視されます。処理は、次のフォーマット・プロファイルから続行されます。複数のフォーマット規則を 1 つのフォーマット・プロファイルの **APPLDATA** で結合することができます。各種フォーマット規則の論理的な整合性は検査されません。例えば、フォーマット規則で ALPHA と NUM が指定されている場合は、すべての文字が拒否されますが、具体的なエラー・メッセージは表示されません。

表 *52. INSTDATA* 検査に使用されるフォーマット規則： この表の項目は、フォーマット規則とその説明で構成されます。

フォーマット規則	説明
NB	ブランク不可 (NonBlank)。インストール・データ・フィールドの指定された部分を、すべてブランクで構成することはできません。
NC	変更不可 (NoChange)。インストール・データの指定された部分の現行値は変更できません。
ALPHA	英字。インストール・データ・フィールドの指定された部分には、英字またはブランクのみを使用できます。
NUM	数字。インストール・データ・フィールドの指定された部分には、数字またはブランクのみを使用できます。
ALPHANUM	英数字。インストール・データ・フィールドの指定された部分には、英字、数字、またはブランクのみを使用できます。
PICT(*picture-string***)**	ピクチャー・フォーマット。インストール・データ・フィールドの指定された部分は、ピクチャー・ストリング ・フォーマットに対応していなければなりません。 259 ページの『ピクチャー・ストリング・フォーマット』を参照してください。

表 52. *INSTDATA* 検査に使用されるフォーマット規則 (続き): この表の項目は、フォーマット規則とその説明で構成されます。

フォーマット規則	説明
LIST(*list-of-strings***)**	インストール・データ・フィールドの指定された部分に使用できる値のリスト。『ストリングのリスト・フォーマット』を参照してください。
LISTX(*list-of-strings***)**	インストール・データ・フィールドの指定された部分に使用できない値のリスト。『ストリングのリスト・フォーマット』を参照してください。
=USERID	有効な任意の RACF ユーザー ID。
=GROUP	有効な任意の RACF グループ。

PICT(ピクチャー・ストリング)、LIST(ストリングのリスト)、および LISTX(ストリングのリスト) フォーマット規則では、括弧で囲んだ追加の指定が必要です。これらの指定については、以降のセクションで説明します。

ピクチャー・ストリング・フォーマット

INSTDATA フィールドのフォーマット規則で PICTURE ストリング文字を指定するには、以下のガイドラインに従ってください。

PICT フォーマット規則の場合、ピクチャー・ストリング 指定は、INSTDATA 内のそれぞれの位置で指定できる値を記述した単一の文字ストリングです。ピクチャー・ストリング がインストール・データ・フィールドの指定された部分より短い場合、残りの文字は検査されません。ピクチャー・ストリング がインストール・データ・フィールドの指定された部分より長い場合は、余分な文字が無視されます。

指定できるピクチャー文字は、表 53 に示されています。

注**:** 現在、ピクチャー・ストリング では右括弧をリテラル文字として使用することができません。インストール・データで右括弧を使用する場合は、その位置のパターン文字としてピリオドの使用に戻すことができます。

表 53. フォーマット規則に使用される *PICTURE* ストリング文字: この表の項目は、サポートされている・ストリング文字を示しています。

ピクチャー	説明
#	数字 (0-9)
@	英字 (A-Z)
*	英数字 (A-Z、0-9)
$	特殊文字 (@#$)
.	任意の文字。検査は行われません。
その他	リテラル値。インストール・データ文字がピクチャー・ストリング文字と同じでなければなりません。

ストリングのリスト・フォーマット

INSTDATA フィールドのフォーマット規則で複数のストリングを指定するには、以下のガイドラインに従ってください。

LIST および LISTX の場合、ストリングのリスト は、コンマ区切りストリングのリストです。コンマと括弧以外の各文字に意味があります。各ストリングは、コンマか、リストの先頭または末尾の括弧によって区切られます。各ストリングには最大 32 文字を指定できます。ストリングが、POSPOS(*start:end*) によって指定された範囲よりも短い場合、INSTDATA 内の残りの文字はブランクでなければなりません。ストリングが、POS(*start:end*) によって指定された範囲よりも長い場合、残りの文字は無視されます。指定可能な LIST 値として空ストリングを明示的に指定する必要はありません。NB フォーマット規則によって既に制御されているためです。

ストリングのリストの例を以下に示します。

```
EXPIRED,DELETE,STARTED
```

この例では、ストリングの長さが異なっており、埋め込みブランクが含まれていないことに注意してください。

ストリングの先頭または末尾であっても、ストリングにブランクを含めることができます。例えば、以下のストリング・リストには、ストリングの先頭、中間、および末尾にブランクが含まれています。二重引用符は構文の一部ではありません。この例では、末尾にブランク文字が含まれていることを示すためだけに二重引用符が使用されています。

```
 "EXPIRED USERID, TO BE DELETED, STARTED TASK "
```

この例では、フォーマット・プロファイルにおいて、POS(*start:end*) によって合計が少なくとも 14 文字となるように指定されていることを前提としています。そうでない場合は、各ストリングを正確に 14 文字で指定することは意味がありません。

LIST フォーマット規則の用途の 1 つとして、単一の位置に特殊な規則を実装することが考えられます。現在、zSecure Command Verifier では、母音または子音を指定するフォーマット規則が用意されていません。英字、数字、英数字、および国別文字を指定できますが、母音が必要であることは指定できません。ただし、単一の POS を指定することによって、およびすべての使用可能な文字をリストするフォーマット規則を組み込むことによって、このような要件を満たすことができます。以下に例を示します。

```
C4R.OPERCMDS.INSTDATA.=FMT.OPER.POS(001:001) APPLDATA('NB,LIST
(A,E,I,O,U,Y)')
```

この同じ例を使用して、2 つの文字位置についてこのフォーマット規則を実装したい場合、2 つの異なるフォーマット・ポリシーを指定する必要があります。

```
C4R.OPERCMDS.INSTDATA.=FMT.OPER.POS(001:001) APPLDATA('NB,LIST
(A,E,I,O,U,Y)')

C4R.OPERCMDS.INSTDATA.=FMT.OPER.POS(002:002) APPLDATA('NB,LIST
(A,E,I,O,U,Y)')
```

POS(001:002) と指定することもできますが、その場合、2 つの母音の 36 とおりの組み合わせをすべてリストする必要があります。

各フォーマット名に含めることができるフォーマット・ポリシーは 10 個までのため、このアプローチは、プロファイルの INSTDATA 内の限られた数の文字位置にのみ使用できます。

USS セグメント管理用のポリシー・プロファイル

RACF FIELD プロファイルを使用すると、どの管理者にセグメント情報を保守する権限を与えるかを制御できます。RACF では、「製品管理者」の作業を容易にする 1 つの手段としてこのステップが実装されています。

多くの組織から、グループ管理者がすべての製品にわたって各自のユーザーを保守できるようにしたいという要望が表明されてきました。RACF は、そのような実装をサポートしていません。 64 ページの『非基本セグメントの管理を制御するプロファイル』では、「製品管理者」をその RACF グループ SPECIAL の範囲内のプロファイルに限定することにより、「すべての製品にまたがる」グループ管理者を事実上作成するという機能が zSecure Command Verifier でどのように実装されるのかを説明しています。

しかし、中央管理者だけに制限したままにしておく必要がある特定のフィールドが特に USS 環境で存在します。最も重要なものは、OMVS セグメントによってユーザーに割り当てられる USS UID です。 UID(0) は、USS 環境におけるスーパーユーザー権限に相当します。分散管理者が自己の任意のユーザーに UID(0) を割り当てることができるのは、望ましいことではありません。

同様に、GROUP の GID は USS ファイルのアクセス検査プロセスで使用されます。したがって、これにも同様な制御が必要です。

UID または GID の値のほかに、特定の UID または GID が単一のユーザーまたはグループのみに割り当てられていることを確認することもできます。RACF では、SHARED キーワードを使用すると、同一の UID または GID を共有できます。RACF での SHARED キーワードの使用要件は、UNIXPRIV クラス内の SHARED.IDS リソースへのシステム SPECIAL 権限または READ 権限のいずれかです。zSecure Command Verifier には、システム SPECIAL 権限を持つユーザーの UID または GID の共有さえも制御するポリシーが含まれています。

表 *54. USS ID* 値の検査に使用されるプロファイル： この表の項目は、クラス、セグメント、およびフィールドと、対応するポリシー・プロファイルを反映しています。

クラス	セグメント	フィールド	プロファイル
USER	*OMVS*	*UID*	**C4R.USER.OMVS.UID.***uid.owner.userid*
USER	*OMVS*	*UID*	**C4R.USER.OMVS.SHARED.***owner.userid*
USER	*OVM*	*UID*	**C4R.USER.OVM.UID.***uid.owner.userid*
GROUP	*OMVS*	*GID*	**C4R.GROUP.OMVS.GID.** *gid.owner.group*
GROUP	*OMVS*	*GID*	**C4R.GROUP.OMVS.SHARED.***owner.group*
GROUP	*OVM*	*GID*	**C4R.GROUP.OVM.GID.** *gid.owner.group*

前の表で、UID または GID のポリシー・プロファイルの値 *uid* および *gid* は、10 桁の数値で指定する必要があります。総称も使用できます。任意のユーザーに対する UID(0) の割り当てを保護するプロファイルの例を、以下に示します。

C4R.USER.OMVS.UID.0000000000.**

システム・サポート担当者への UID(0) の割り当てを許可したい場合は、以下のようなプロファイルを使用することができます。

C4R.USER.OMVS.UID.0000000000.SYSSUP.*

10 桁のゼロを 1 つのアスタリスクで指定しても (すべての UID をシステム・サポート担当者に開放することを示します)、効果はありません。RACF は、数字をより限定的なものとして取り扱い、そのプロファイルをアスタリスクのプロファイルの代わりに使用します。UID 番号に総称を使用して 2 番目のプロファイルを指定した場合、それは、それ以外 のすべての UID がシステム・サポートの担当者に開放されることを意味します。実際の割り当てを実行している端末ユーザーは、ポリシー・プロファイルへのアクセス権限を必要とします。また、RACF 権限 (例えば、システム SPECIAL または FIELD プロファイルなど) も必要です。

- **C4R.USER.OMVS.UID.***uid.owner.userid*
- **C4R.USER.OVM.UID.***uid.owner.userid*
- **C4R.GROUP.OMVS.GID.** *gid.owner.group*
- **C4R.GROUP.OVM.GID.** *gid.owner.group*

  これらのプロファイルは、*owner* が所有する *userid* に特定の *uid* を設定する権限を指定します。*UID* および *GID* は、右寄せでゼロを埋め込んだ 10 桁の数字として指定する必要があります。特定範囲の *UID* および *GID* の管理を許可または禁止するために、総称を使用することもできます。

  プロファイルが見つからない
  : 制御は実装されません。USS ID 値の割り当ての制御には、RACF 権限だけが使用されます。

  NONE
  : 端末ユーザーは、この UID/GID を USERID または GROUP に割り当てることを許可されません。これを設定するとコマンドは失敗します。

  READ
  : NONE と同じ。

  UPDATE
  : UID/GID の値は受け入れられます。ただし、依然として RACF 権限要件がコマンドの失敗の原因になる場合があります。

  CONTROL
  : UPDATE と同じ。

- **C4R.USER.OMVS.SHARED.***owner.userid*

  このポリシー・プロファイルは、UID を USERID に割り当てるときに SHARED キーワードの使用を制御するために使用されます。同じ UID を複数のユーザーに割り当てると、個々のユーザー制御が失われることになるため、通常は推奨されません。RACF で SHARED キーワードを使用するには、UNIXPRIV クラス内のリソース SHARED.IDS に対するシステム SPECIAL アクセス、または定義されている場合は READ 権限以上が必要です。このポリシー・プロファイルでは、以下のアクセス規則が適用されます。

プロファイルが見つからない
制御は実装されません。すべての RACF 許可ユーザーは、ターゲット・ユーザー ID に SHARED UID を割り当てることができます。

NONE
UID をターゲット・ユーザー ID に割り当てる際に、端末ユーザーは SHARED キーワードを使用することを許可されません。これは、指定された UID が実際に共有されているかどうかには関係ありません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
端末ユーザーは、ターゲット・ユーザー ID に SHARED UID を割り当てることを許可されます。端末ユーザーには、十分な RACF 権限が引き続き必要です。

CONTROL
UPDATE と同じ。

- **C4R.GROUP.OMVS.SHARED.***owner.group*

このポリシー・プロファイルは、GID を GOUP に割り当てるときに SHARED キーワードの使用を制御するために使用されます。同じ GID を複数のグループに割り当てると、個々のグループ制御が失われることになるため、通常は推奨されません。RACF で SHARED キーワードを使用するには、UNIXPRIV クラス内のリソース SHARED.IDS に対するシステム SPECIAL アクセス、または定義されている場合は READ 権限以上が必要です。このポリシー・プロファイルでは、以下のアクセス規則が適用されます。

プロファイルが見つからない
制御は実装されません。すべての RACF 許可ユーザーは、ターゲット・グループに SHARED GID を割り当てることができます。

NONE
GID をターゲット・グループに割り当てる際に、端末ユーザーは SHARED キーワードを使用することを許可されません。これは、指定された GID が実際に共有されているかどうかには関係ありません。コマンドはリジェクトされます。

READ
NONE と同じ。

UPDATE
端末ユーザーは、ターゲット・グループに SHARED GID を割り当てることを許可されます。端末ユーザーには、十分な RACF 権限が引き続き必要です。

CONTROL
UPDATE と同じ。

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]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

A

C

D

E

F

G

I

J

L

M

N

O

P

R

S

T

U

V

X

Z

［特殊文字］

Printed in Japan

SA88-7158-04

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