zSecure CICS Toolkit

ユーザー・ガイド

SA88-7159-06

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、119 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM® Security zSecure CICS® Toolkit のバージョン 2 リリース 4 モディフィケーション 0 (製品番号 5655-N18)、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに 適用されます。

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

原典：
SC27-5649-06
zSecure CICS Toolkit
User Guide
December 2019

発行：
日本アイ・ビー・エム株式会社

担当：
トランスレーション・サービス・センター

目次

本書について

IBM Security zSecure CICS Toolkit では、CICS から直接 RACF® コマンドを実行できるようにして、TSO を使用する必要性をなくすことにより、CICS/RACF のセキュリティー機能が強化されています。アプリケーション・プログラムが、アプリケーションの内部セキュリティー機能に依存する代わりに、IBM Security zSecure CICS Toolkit をセキュリティー機能として使用することもできます。 このようにして、すべてのセキュリティー定義を一元的に維持管理することも、セキュリティー・コーディネーター間にセキュリティー定義を分散させることもできます。

本書では、IBM Security zSecure CICS Toolkit の 2 つのコンポーネントである、アプリケーション・プログラミング・インターフェース (API) とコマンド・インターフェースについて 説明します。また、この製品のインストール方法と使用方法について説明します。

本書は、以下のような読者を対象としています。

- IBM Security zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者
- IBM Security zSecure CICS Toolkit によって提供される追加の RACF コマンド制御の実装を担当する CICS セキュリティー管理者

また、本書の読者は、CICS 環境でセキュリティー・タスクおよび管理タスクを実行する方法、さらに RACF の概念とコマンドについての知識を持っている必要があります。

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

zSecure 資料

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

zSecure の非ライセンス出版物は、IBM Security zSecure Suite (z/OS) または IBM Security zSecure Manager for RACF z/VM の IBM Knowledge Center で提供されています。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。

製品の IBM Knowledge Center	URL
IBM Security zSecure Suite (z/OS)	www.ibm.com/support/knowledgecenter/SS2RWS/welcome
IBM Security zSecure Manager for RACF z/VM	www.ibm.com/support/knowledgecenter/SSQQGJ/welcome

ライセンス文書の入手

ライセンスの付いていない zSecure V2.4.0 資料は一般公開されています。zSecure のライセンス文書は、ライセンス交付を受けたお客様のみが入手できます。ライセンス文書へのアクセスを要求する方法については、この資料で説明します。

zSecure V2.4.0 のライセンス文書は、IBM Security zSecure Suite ライブラリーで提供しています。

zSecure V2.4.0 のライセンス文書にアクセスするには、お客様の IBM ID およびパスワードを使用して、IBM Security zSecure Suite ライブラリーにサインインする必要があります。 ライセンス文書が表示されない場合は、ご使用の IBM ID がまだ登録されていないと思われます。IBM ID を登録するには、zDoc@nl.ibm.com 宛にメールを送信してください。お客様ご自身のお名前および IBMid のほかに所属組織のお客様名およびお客様番号もお知らせください。IBMid をお持ちでない場合は、「IBM アカウントの作成」を行うことができます。登録の確認を知らせるメールをお送りいたします。

IBM Security zSecure Suite ライブラリー

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

非ライセンス出版物は、IBM Security zSecure Suite の IBM Knowledge Center から入手できます。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 (LC43-2107 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 V2.4.0 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-Driven Components* インストールおよびデプロイメント・ガイド, SA88-7162

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

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

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

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

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

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure CARLa-Driven Components (Admin、Audit、Visual、Alert および IBM Security zSecure Adapters for 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 Security zSecure Manager for RACF z/VM ライブラリー

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

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

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

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

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

  製品のインストール、構成、およびデプロイについての情報を提供します。
- *IBM Security zSecure Manager for RACF z/VM User Reference Manual*、*LC27-4364*

  製品のインターフェースの 使用方法、および RACF の管理機能と監査機能の使用方法を説明します。この資料には、CARLa コマンド言語および SELECT/LIST フィールドに関する参照情報が記載されています。また、トラブルシューティング・リソース、および zSecure Collect コンポーネントの使用方法も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。
- *IBM Security zSecure CARLa* コマンド・リファレンス*,* 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 Security 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 Security zSecure Manager for RACF z/VM*」は、製品のインストール、構成、およびデプロイを担当するシステム・プログラマーを対象としています。この資料には、ソフトウェアのインストールに関連する資料および手順に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 Security zSecure Manager for RACF z/VM の IBM Knowledge Center から最新のコピーをダウンロードすることもできます。

関連資料

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。 zSecure のライセンス文書を入手するには、ライセンス文書の入手を参照してください。
IBM Knowledge Center: z/OS	z/OS に関する情報。xi ページの表 1 に、zSecure で最も役立つ資料をいくつか示します。IBM Knowledge Center には、z/OSV2R4 ライブラリー が含まれています。
IBM Z Multi-Factor Authentication の資料	IBM Z Multi-Factor Authentication (MFA) の資料に関する情報。z/OS V2R4 ライブラリーには、IBM Z Multi-Factor Authentication の資料が含まれています。
z/OS Security Server RACF の資料	z/OS Security Server のリソース・アクセス管理機能 (RACF) の資料。 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。
QRadar DSM 構成ガイド	QRadar について詳しくは、IBM Knowledge Center で IBM QRadar Security Intelligence Platform を参照してください。
CICS Transaction Server for z/OS の資料	CICS Transaction Server for z/OS に関する資料。

表 *1. 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 構成ガイド	SC27-3650
z/OS Communications Server: IP 構成解説書	SC27-3651
z/OS Cryptographic Services ICSF Administrator's Guide	SC14-7506
z/OS Cryptographic Services ICSF System Programmer's Guide	SC14-7507
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 ISPF ダイアログ開発者 ガイドとリファレンス	SC19-3619
z/OS MVS プログラミング*:* アセンブラー・サービス解説書 第 *1* 巻 *(ABE-HSP)*	SA23-1369
z/OS MVS プログラミング*:* アセンブラー・サービス解説書 第 *2* 巻 *(IAR-XCT)*	SA23-1370
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 MVS システム管理機能 *(SMF)*	SA88-7082
z/OS Security Server RACF セキュリティー管理者のガイド	SA88-5804

表 1. 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 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	SA23-2288
z/OS Security Server RACF メッセージおよびコード	SA88-5839
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。 本製品では、インターフェースを 音声で聞いてナビゲートするための補助テクノロジーを使用できます。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 用に選択可能なコース・オファリングに関する情報、および CARLa とサンプル・アプリケーションを迅速に開始するための情報については、IBM Knowledge Center for zSecure V2.4.0 で zSecure Wiki 情報を参照してください。

サポート情報

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

zSecure CICS Toolkit は、多くのインストール済み環境で使用される CICS/RACF のセキュリティー機能を強化します。zSecure CICS Toolkit を使用すると、CICS セキュリティー管理者は CICS から直接 RACF コマンドを実行できるので、TSO を使用する必要がなくなります。アプリケーション・プログラムが、アプリケーションの内部セキュリティー機能に依存する代わりに、zSecure CICS Toolkit をセキュリティー機能として使用することができます。 このようにして、すべてのセキュリティー定義を一元的に維持管理することも、セキュリティー・コーディネーター間にセキュリティー定義を分散させることもできます。

zSecure CICS Toolkit は、アプリケーション・プログラミング・インターフェース (API) とコマンド・インターフェースの 2 つの部分で構成されています。

アプリケーションは、アプリケーションの内部セキュリティーの代わりに、zSecure CICS Toolkit をセキュリティーに使用することができます。すべてのセキュリティー定義を一元的に維持管理することも、セキュリティー・コーディネーター間にセキュリティー定義を分散させることもできます。

アプリケーション・インターフェース

CICS のシステム・プログラマーは、zSecure CICS Toolkit API を使用して、RACF コマンドやパネルをインストール済み環境の要件に合わせてカスタマイズできます。

セキュリティー定義を一元的に管理するフォーカル・ポイントを設定できることに加えて、CICS システム・プログラマーが、サインオン・テーブルを保守する必要がなくなりました。このテーブルは、CICS バージョン 2 *.x* 以降のバージョンでは不要です。RACF によってトランザクションのセキュリティー検査が実行されるとすぐに、サインオン・テーブルで必要な定義は DEFAULT 項目のみになります。必要なすべての情報は RACF に定義され、RACF によって保守されるため、アプリケーション・プログラマーがセキュリティー・テーブルやファイルを更新する必要がなくなります。このようなタスクをなくすことにより、時間を節約して他の作業にあてることができます。

zSecure CICS Toolkit のもう 1 つの固有の側面として、すべてのアプリケーション・トランザクションに RACF 保護を設定する機能があります。 zSecure CICS Toolkit は、以前は保護されていなかったトランザクションも保護します。 このような保護の例として、プリンター装置でレポートを印刷するトランザクションや、ATM トランザクションが挙げられます。 プリンターや ATM はサインオンを行わないため、セキュリティー検査を実行できません。このため、このような装置上で稼働するトランザクションは保護できませんでした。zSecure CICS Toolkit では、この制限をなくしたため、このようなトランザクションがすべて保護されます。zSecure CICS Toolkit は、MRO 環境をサポートしており、使いやすく、インストールおよび保守が容易です。

コマンド・インターフェース

CICS のシステム・プログラマーは、コマンド・インターフェースを 使用して、特定の RACF コマンドを TSO からではなく CICS から直接実行できます。コマンド・インターフェースを 使用すると、特定の能力や責務を CICS ユーザーに、より広範囲に分散させることができます。 これによって、TSO アプリケーションを使用する必要性がなくなり、CPU オーバーヘッドを削減できます。

コマンド・インターフェースを 検索に使用する場合、以下の利点があります。

- プロファイルに関する情報を取り出すために、より詳細な検索マスクを使用できる。
- 使用する基準に高い柔軟性がある。

注 : zSecure CICS Toolkit では、コマンドまたはコマンドの一部分を実行するユーザー権限を有効にする際の概念が異なります。例えば、ユーザーは許可を受けて他のユーザーのパスワードをリセットしたり、ユーザーを再開したりすることができますが、GROUPSPECIAL 権限によって使用できる他のタスクを実行するためのより広範な権限は必要としません。ユーザーには GROUPSPECIAL は必要なく、リセットするユーザーのグループに接続している必要もありません。コマンドまたはコマンドの一部分を実行するユーザー権限を有効にする際の概念が異なります。 例えば、GROUPSPECIAL の権限を持つことによって暗黙に指定

される可能性がある他の操作の実行権限がなくても、ユーザーは別のユーザーのパスワードをリセットしたり、ユーザーを再開させたりすることができます。ユーザーには GROUPSPECIAL 属性は必要なく、リセットするユーザーのグループに接続している必要もありません。

注 : zSecure CICS Toolkit では、コマンドまたはコマンドの一部分を実行するユーザー権限を有効にする際の概念が異なります。例えば、GROUPSPECIAL の権限によって使用可能となる他のタスクのより広範な実行権限を必要とせずに、ユーザーは別のユーザーのパスワードをリセットしたり、ユーザーを再開させたりすることができます。ユーザーには GROUPSPECIAL 属性は必要なく、リセットするユーザーのグループに接続している必要もありません。

この方法論においては、ユーザーのパスワードをリセットする責務を、CICS 端末へのアクセス権限を持つ他の任意の部門に分散することができます。その結果、データ・セキュリティー担当者が、時間と労力を他の領域に使うことができます。

RACF は、zSecure CICS Toolkit をコマンド・インターフェース 用に開始するためのトランザクションと、コマンドそのものの両方を保護します。zSecure CICS Toolkit トランザクションに対するセキュリティーがない場合でも、ユーザーが RACF でコマンドに対して許可 されていなければ、コマンドを開始することはできません。また、ユーザーは、 ユーザー ID をリセットする権限を持つことを許可 されている必要があります。唯一の例外は、SPECIAL 属性を持つユーザー、または TOOLKIT.SPEC 定義へのアクセス権限を持つユーザーです。この定義については、3 ページの『第 2 章 zSecure CICS Toolkit のインストール』を参照してください。

RACF プロファイルを変更すると必ず、SMF レコードが生成されます。

RRSF に関する考慮事項

zSecure CICS Toolkit のアクションと TSO-RACF コマンドとの間には相違点があります。

zSecure CICS Toolkit が実行する、RACF プロファイルに対する追加、更新、および削除はすべて、RACROUTE インターフェースまたは ICHEINTY インターフェースを 使用して行われます。本書ではこれ以降、こうした機能に、対応する RACF コマンド・プロセッサー名を使用します。例えば、本書でユーザーをグループに接続する API インターフェースについて 説明する際には、この機能を CONNECT コマンドと呼びます。実際の処理は CONNECT コマンドによるものでは**ありません**。これは、RACF CONNECT コマンドが使用された場合と同じ結果を発生させる類似のアクション・セットです。 したがって、更新はアプリケーションの更新とみなされます。TSO RACF コマンドと zSecure CICS Toolkit のアクションの間に明らかな違いがあるのは、RACF リモート共有機能 (RRSF) による更新の伝搬が必要な場合の、必要となる RRSF 定義に関してのみです。

RRSF によって変更を伝搬する場合は、コンソールから RACF SET AUTOAPPL オペレーター・コマンドを使用するか、PARMLIB によってこの機能を活動化します。RACF コマンドを伝搬する場合は、おそらくこれと同等の SET AUTODIRECT オプションが設定されています。アプリケーションの更新を自動的に伝搬するには、該当するプロファイルを RRSFDATA リソース・クラスに定義することも必要です。これらのプロファイルでは、CICS 領域で行われた RACF の更新を伝搬することが許可されている必要があります。RRSFDATA プロファイルへのアクセス権限を必要とするユーザーは、CICS 端末ユーザーや CICS デフォルト・ユーザー**ではなく**、CICS 領域ユーザーです。適切な RRSFDATA プロファイルの定義については、「*RACF* セキュリティー管理者のガイド」の『RACF リモート共有機能』の章の『自動ダイレクト』のセクションを参照してください。

2000 年前後の日付

REVOKEDATE および RESUMEDATE パラメーターに日付を指定した場合、zSecure CICS Toolkit は IBM の規則に従って日付を処理します。

日付の形式は *YYDDD* です。ここで、*YY* は年を表し、*DDD* は日番号を表します。

- *YY* に 71 以上の値を指定した場合、日付は 1971 年などの 20 世紀の日付として扱われます。
- *YY* に 70 以下の値を指定した場合、日付は 2070 年などの 21 世紀の日付として扱われます。

この規則では、以前のリリースとの互換性も提供されます。

第 2 章 zSecure CICS Toolkit のインストール

システム・サポート担当者は、この章の情報を使用して、zSecure CICS Toolkit のインストールを行ってください。インストール・プロセスには SMP/E を使用します。

インストールを開始する前に、プログラム・ディレクトリー: *IBM Security zSecure CICS Toolkit* に記載されている前提条件に関する情報を参照してください。その後、3 ページの『インストールおよびポストインストールのチェックリスト』を使用して、インストール・タスクとポストインストール・タスクの各段階に対応する説明を見つけてください。

インストールおよびポストインストールのチェックリスト

zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、インストール・タスクとポストインストール・タスクを実行する際に、以下のチェックリストを使用できます。

表 2. インストール・チェックリスト

ステップ	説明	手順	ジョブ名	状況
1	インストール JCL をロードする。	4 ページの『サンプル JCL』		
2a	SMP/E ゾーンを作成し、初期化する。	5 ページの『SMP/E ゾーンの作成と初期化』	CQTJSMPx (SCQTINST)	
2b	TARGET および DLIB データ・セットを割り振る。	6 ページの『TARGET データ・セットと DLIB データ・セットの割り振り』	CQTJALL (SCQTINST)	
3	SMP/E DDEF を更新する。	6 ページの『SMP/E DDDEF の更新』	CQTJDDD (SCQTINST)	
4a	zSecure CICS Toolkit を受け取る。	7 ページの『製品の受け取り』	CQTJREC (SCQTINST)	
4b	zSecure CICS Toolkit を適用する。	7 ページの『zSecure CICS Toolkit のコードの追加』	CQTJAPP (SCQTINST)	
4c	zSecure CICS Toolkit を受け入れる。	7 ページの『ご使用のシステムと zSecure CICS Toolkit の統合』	CQTJACC (SCQTINST)	
5	SVC をインストールする。	7 ページの『SVC のインストール』		
6	SVC を保護する。	8 ページの『SVC の保護』	CQTJRDEF (SCQTSAMP)	
7	データ・セットを APF 許可として定義する。	8 ページの『SCQTLOAD に対する APF 許可の定義』		
8	CICS 開始 JCL を更新する。	8 ページの『CICS 開始 JCL の更新』		
9	PARMLIB の **IFAPRD***xx* によって製品の使用可能化を確認する。	9 ページの『PARMLIB での zSecure CICS Toolkit の使用可能化』		
10	**CQTPCNTL** パラメーターを更新する。	9 ページの『CQTPCNTL パラメーターの定義』	CQTJCNTL (SCQTINST)	

表 2. インストール・チェックリスト (続き)				
ステップ	**説明**	**手順**	**ジョブ名**	**状況**
11	プログラム、マップ・セット、トランザクションを CICS に定義する。	10 ページの『プログラム、マップ・セット、トランザクションの CICS への定義』	CQTJRDO (SCQTSAMP)	
12	CICS テーブルを更新する。	11 ページの『CICS テーブルの更新』	CQTJPLT CQTJSRT (SCQTSAMP)	
13	zSecure CICS Toolkit 機能へのアクセス権限を制御する RACF プロファイルを定義する。	11 ページの『RACF プロファイルの定義』	CQTJRDEF (SCQTSAMP)	
14	CICS 開始タスクで USS 機能を実行できるように、追加の権限を付与する。	17 ページの『USS UID の自動割り当て (OMVS AUTOUID)』および 17 ページの『ホーム・ディレクトリーの自動作成 (OMVS MKDIR)』		
15	zSecure CICS Toolkit を再始動する。	18 ページの『zSecure CICS Toolkit の再始動』		

サンプル JCL

zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、*relfile 2* および SCQTSAMP データ・セットからインストール・ジョブにアクセスするか、テープ・ファイルまたはプロダクト・ファイルからジョブをコピーすることができます。

サンプルのインストール・ジョブにアクセスするには、SMP/E RECEIVE を実行します。次に、*relfile* にあるジョブを作業データ・セットにコピーして、編集および実行依頼します。SMP/E のステップで使用されるサンプル JCL は、*relfile 2* に含まれています。構成ステップ中に使用される残りのサンプル JCL は、インストールの初期ステップ中に作成される SCQTSAMP データ・セットに含まれています。

テープ・ファイルまたはプロダクト・ファイルからジョブをコピーするには、このパラグラフの後に示すジョブを実行依頼します。配布メディアに応じて、**//TAPEIN** または **//FILEIN DD** ステートメントのいずれかを使用し、他方のステートメントはコメント化するか、削除します。実行依頼を行う前に、ジョブ・カードを追加し、ご使用のサイトの要件に合わせて小文字のパラメーターを大文字の値に変更してください。

```
//STEP1    EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//TAPEIN   DD DSN=IBM.HCQT240.F2,UNIT=tunit,
//            VOL=SER=volser,LABEL=(x,SL),
//            DISP=(OLD,KEEP)
//FILEIN   DD DSN=IBM.HCQT240.F2,UNIT=SYSALLDA,DISP=SHR,
//            VOL=SER=filevol
//OUT      DD DSNAME=jcl-library-name,
//            DISP=(NEW,CATLG,DELETE),
//            VOL=SER=dasdvol,UNIT=SYSALLDA,
//            SPACE=(TRK,(5,5,5))
//SYSUT3   DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSIN    DD *
  COPY INDD=xxxxIN,OUTDD=OUT
/*
```

前のサンプルのステートメントを、以下のように更新します。

- TAPEIN を使用する場合:

  tunit
  プロダクト・テープに対応する装置の値です。

volser
プロダクト・テープに対応するボリューム通し番号です。

x
データ・セット名がテープ上にある場合のテープ・ファイル番号です。

IBM.HCQT240.F2 がテープ上のどこにあるかを確認するには、CBPDO 提供の資料を参照してください。

CBPDO 以外のプロダクト・テープからインストールする場合は、テープの *volser* は CQT240 で、*relfile 2* のファイル番号はテープ上の 3 になります。

- FILEIN を使用する場合:

filevol
ダウンロードしたファイルが存在する DASD 装置のボリューム通し番号です。

- OUT ステートメント内:

jcl-library-name
サンプル・ジョブが格納される出力データ・セットの名前です。

dasdvol
出力データ・セットが存在する DASD 装置のボリューム通し番号です。

- SYSIN ステートメント内:

xxxxIN
入力 DD ステートメントに応じて、TAPEIN または FILEIN のいずれかになります。

SMP/E ゾーンの作成と初期化

SMP/E によるインストールを開始する前に、zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、使用する SMP/E ゾーンを決定する必要があります。

以下のいずれかのオプションを選択できます。

- 新規の CSI 内の新規 (専用) ゾーンに zSecure CICS Toolkit をインストールする。

  このオプションでのみ、サンプル・ジョブが提供されます。
- 既存の CSI 内の新規 (専用) ゾーンに zSecure CICS Toolkit をインストールする。
- 既存の CSI 内の既存のゾーンに zSecure CICS Toolkit をインストールする。

CSI とゾーンの可能な組み合わせすべてで、提供されるサンプル・ジョブが使用できるわけではありません。サンプル・ジョブが提供されるのは、最初のオプションだけです。提供されるジョブを使用して、専用の TARGET ゾーンおよび DLIB ゾーンがある専用の GLOBAL および PRODUCT CSI をセットアップすることができます。詳しくは、6 ページの『プリインストール・ステップの実行』を参照してください。

サンプル・ジョブは、SCQTINST 内にあります。JCL を調整し、ジョブを実行依頼して、SMP/E 環境の作成と初期化を完了します。これらのジョブでは、ご使用のインストール済み環境の標準に合わせて調整する必要がある値はすべて小文字のストリング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 CICS Toolkit 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・セット接頭部は、zSecure CICS Toolkit に固有の 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 CICS Toolkit データ・セットを作成する DASD ボリュームの名前。

注 : SMS 環境では、ACS ルーチンによって、*volser* から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 CICS Toolkit 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する場合は、GLOBAL ゾーン用に補足の修飾子を追加します。例えば、次の 2 つの値を使用できます。

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

以下の表を使用して、ご使用の環境に適したインストールの変数値を記録してください。

表 *3. SMP/E* ゾーンを定義するためのプリインストール・ステップ	
変数	**使用する値**
Your-Global	
Your-Product	
sysallda	
volser	
tape	

プリインストール・ステップの実行
インストールを開始する前に、zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、必要な SMP/E ゾーンを定義する必要があります。

手順

1. 以下のようにして、グローバル CSI を作成します。
   新しい GLOBAL CSI を作成するためのサンプル・ジョブが、CQTJSMPA メンバー内に用意されています。このジョブでは、この新しい CSI 内に GLOBAL ゾーンも定義します。
   ► ジョブ CQTJSMPA を調整して実行依頼する。
2. 以下のようにして、製品 CSI を作成します。
   新しい製品 CSI を作成するためのサンプル・ジョブが、CQTJSMPB メンバー内に用意されています。このジョブでは、この新しい CSI 内に TARGET および DLIB ゾーンも定義します。
   ► ジョブ CQTJSMPB を調整して実行依頼する。
3. zSecure CICS Toolkit のオプション項目を定義します。
   zSecure CICS Toolkit に固有のオプション項目を定義するためのサンプル・ジョブが、CQTJSMPC メンバー内に用意されています。このジョブでは、SMP/E の残りのインストール・ステップ中に使用されるユーティリティーおよびデータ ・セット接頭部を指定します。
   ► ジョブ CQTJSMPC を調整して実行依頼する。

TARGET データ・セットと DLIB データ・セットの割り振り

zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、TARGET データ・セットと DLIB データ・セットを割り振る必要があります。

zSecure CICS Toolkit は、ご使用の SMP/E 環境に 6 つのターゲット・データ・セットと 6 つの配布データ・セットを追加します。JOB CQTJALL のサンプルには、必要な TARGET および DLIB データ・セットを割り振るために必要な JCL が含まれています。

► CQTJALL を実行依頼する。

SMP/E DDDEF の更新

zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、以下のステップを実行して、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 ジョブに対して、それぞれに応じた DD ステートメントを組み込むことを選択する場合は、このステップを省略できま

す。動的割り振りによるセットアップ (推奨) 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 CQTJDDD に、このステップに必要な JCL が含まれています。

インストール・プロセスでは、SMP/E CALLLIBS 処理も使用されます。この機能は、インストール中に外部参照を解決するために使用されます。 zSecure CICS Toolkit のインストール時に、CSSLIB ライブラリーの DDDEF が存在することを確認してください。

注 : DDDEF は、CALLLIBS を使用して zSecure CICS Toolkit のリンク・エディットを解決するためにのみ使用されます。これらのデータ・セットは、zSecure CICS Toolkit のインストール中には更新されません。提供されているサンプル・ジョブには、必要な DDDEF が含まれています。

► ジョブ CQTJDDD を実行依頼する。

製品の受け取り

システム・サポート担当者は、zSecure CICS Toolkit を正しくインストールするために、SMP/E 修正制御ステートメントを使用する必要があります。

zSecure CICS Toolkit プロダクト・テープからインストールする場合、その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 CICS Toolkit 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。

► ジョブ CQTJREC を実行依頼する。

zSecure CICS Toolkit のコードの追加

zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、コード、例、および資料をシステムに追加する必要があります。

必要な SMP/E ステートメントは次のとおりです。

```
APPLY GROUPEXTEND SELECT(HCQT240).
```

製品の FMID に対して SELECT が使用されるため、SMP/E では FUNCTIONS キーワードを使用する必要がありません。サンプル・ジョブは、CQTJAPP メンバーに含まれています。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。

► ジョブ CQTJAPP を実行依頼する。

ご使用のシステムと zSecure CICS Toolkit の統合

zSecure CICS Toolkit のインストールを担当するシステム・サポート担当者は、製品の実装に問題がなければ、製品に対して ACCEPT を実行してください。ACCEPT を実行すると、製品はシステムの一部となります。

通常は、zSecure CICS Toolkit で発生するシステムのプログラミング作業は他にはありません。サンプルの ACCEPT ジョブが、CQTJACC に用意されています。

► ジョブ CQTJACC を実行依頼する。

SVC のインストール

システム・サポート担当者は、zSecure CICS Toolkit で使用するタイプ 3 の SVC をインストールする必要があります。

手順

1. PARMLIB の LPALSTxx メンバーに SCQTLPA データ・セットを組み込みます。 提供されている SCQTLPA から SCQTSVC00 を既存の LPALIST データ・セットにコピーすることもできます。 例えば、SYS1.LPALIB などとします。
2. zSecure CICS Toolkit SVC に使用する SVC 番号を決定します。 この例では、222 を使用します。
3. 以下のステップを実行します。
   a) PARMLIB の IEASVC*xx* メンバーを、zSecure CICS Toolkit SVC を定義する項目で更新します。例えば、次のようにします。

```
SVCPARM 222,REPLACE,TYPE(3),APF(NO),EPNAME(CQTSVC00)
```

b) IPL を実行して、システムに SVC をインストールします。

注 : 一部のソフトウェア・パッケージには、IPL を実行せずに SVC テーブルを更新する機能が用意されています。 このようなソフトウェア・パッケージを使用する場合は、SVC の使用を開始するために IPL を実行する必要がないことがあります。

4. DFHSRT 項目を以下の形式で追加します。

```
DFHSRT TYPE=SYSTEM,ABCODE=FXX,ROUTINE=DFHSRTRR
```

ここで、*XX* は SVC を表す 16 進数です。

例えば、SVC に割り当てられている番号が 222 である場合、この項目は FDE になります。

DFHSRT テーブルの更新について詳しくは、11 ページの『CICS テーブルの更新』を参照してください。

► LPALST*xx* および IEASVC*xx* メンバーを更新し、システムの IPL を実行する。

SVC の保護

zSecure CICS Toolkit SVC の無許可の使用を防ぐために、SVC から RACHECK を実行して、呼び出し元が許可されていることを確認します。

このタスクについて

CICS が zSecure CICS Toolkit を使用できるようにするためには、事前に RACF を介して zSecure CICS Toolkit へのアクセス権限が付与されている必要があります。

手順

1. **RDEFINE** コマンドを使用して、SVC を RACF に定義します。 リソース・クラス FACILITY を使用する必要があります。

```
RDEFINE FACILITY TOOLKIT.SVC UACC(NONE)
```

2. ツールキットがインストールされる各 CICS 領域へのアクセス権限を SVC に付与します。以下のコマンドを使用します。

```
PERMIT TOOLKIT.SVC CLASS(FACILITY) ID(userid) ACCESS(READ)
```

ここで、*userid* は CICS 領域の ID です。

上記の RACF 定義のサンプルは、SCQTSAMP の CQTJRDEF メンバーに含まれています。

SCQTLOAD に対する APF 許可の定義

zSecure CICS Toolkit のサブタスク・プログラムは、RACF データベース内のプロファイルの取得と更新を行います。 これらの RACF 機能を使用するには、APF 許可が必要です。

このサブタスク・プログラムを含むデータ・セットは、SCQTLOAD です。このデータ・セットは、APF 許可を与えられていなければなりません。SCQTLOAD を APF 許可として定義するには、PARMLIB の IEAAPF*xx* または PROG*xx* メンバーを、SCQTLOAD データ・セットの名前で更新する必要があります。

► PROG*xx* を更新し、オペレーター・コマンド SET PROD=*xx* によって活動化する。

CICS 開始 JCL の更新

CICS 開始 JCL に、いくつかの変更を加える必要があります。

手順

1. zSecure CICS Toolkit プログラムおよびマップが含まれている SCQTRPL データ・セットを、DFHRPL 連結に追加します。
以下に例を示します。

```
//DFHRPL DD DISP=SHR,DSN=APPL1.LOADLIB
//       DD DISP=SHR,DSN=APPL2.LOADLIB
//       DD DISP=SHR,DSN=APPL3.LOADLIB
//       DD DISP=SHR,DSN=APPL4.LOADLIB
//       DD DISP=SHR,DSN=CICS.TOOLKIT.SCQTRPL
```

2. SCQTLOAD データ・セットには、MVS™ サブタスクとして使用される zSecure CICS Toolkit プログラムが含まれています。 このデータ・セットを CICS STEPLIB に追加します。
3. zSecure CICS Toolkit の loadlib を STEPLIB 連結に追加する場合は (モジュールを既存の loadlib にコピーするのではなく)、その loadlib を APF 許可にすることも必要です。これは、CICS STEPLIB 内のすべての loadlib が、APF 許可を与えられていなければならないためです。

   zSecure CICS Toolkit loadlib を APF 許可として定義するには、SYS1.PARMLIB の IEAAPF*xx* メンバーまたは PROG*xx* メンバーを、zSecure CICS Toolkit loadlib の名前で更新する必要があります。

   以下は JCL STEPLIB パラメーターを更新する場合の例です。

```
//STEPLIB DD DISP=SHR,DSN=LOADLIB1
//        DD DISP=SHR,DSN=LOADLIB2
//        DD DISP=SHR,DSN=CICS.TOOLKIT.SCQTLOAD
```

PARMLIB での zSecure CICS Toolkit の使用可能化

zSecure CICS Toolkit タスクの開始時に、zSecure CICS Toolkit は製品が使用可能であるか使用不可であるかを、PARMLIB 内の IFAPRD*xx* によって確認します。

製品が使用可能である場合、つまり IFAPRD*xx* に定義されていない場合は、zSecure CICS Toolkit の初期化が正常に続行されます。

製品が使用不可である場合は、メッセージ (CQT907) が出され、zSecure CICS Toolkit の初期化が終了します。 製品を使用不可にしても、その後の CICS の初期化に影響はありません。

zSecure CICS Toolkit を明示的に使用可能にするには、アクティブな IFAPRD*xx* メンバーに以下のような項目を挿入します。

```
PRODUCT OWNER('IBM CORP')
        NAME('zSecure Toolkit')
        ID(5655-N18)
        VERSION(*) RELEASE(*) MOD(*)
        STATE(ENABLED)
```

zSecure CICS Toolkit を使用不可にする場合は、上記のような項目を作成して、パラメーター STATE(ENABLED) をパラメーター STATE(DISABLED) に置き換えます。

► IFAPRD*xx* を更新し、オペレーター・コマンド SET PROD=*xx* によって活動化する。

CQTPCNTL パラメーターの定義

CQTPCNTL では、zSecure CICS Toolkit が使用するパラメーターの一部が定義されています。

このようなパラメーターには、SVC 番号や使用される RACF リソース・クラスなどがあります。 CQTPCNTL パラメーターの定義と、CQTPCNTL のカスタマイズに関する情報については、21 ページの『第 3 章 zSecure CICS Toolkit のパラメーター』を参照してください。

► CQTPCNTL を調整して CQTJCNTL を実行依頼する。

定義を作成した後、トランザクション RTCK を実行して、CQTPCNTL 内のパラメーターを検査することができます。

プログラム、マップ・セット、トランザクションの CICS への定義

zSecure CICS Toolkit が使用するプログラム、マップ・セット、およびトランザクションを定義する必要があります。この定義には引き続き CICS テーブルを使用できますが、推奨される方法は CICS のオンライン・リソース定義 (RDO) を使用することです。

これらの定義を作成するためのサンプル・ジョブが、SCQTSAMP の CQTJRDO メンバーに用意されています。以下のマップ・セットを定義する必要があります。

```
CQTBST0  CQTBCH0  CQTB000  CQTB100  CQTB200  CQTB300
CQTB400  CQTB500  CQTB550  CQTB560  CQTB580  CQTB590
CQTB600  CQTB700  CQTB800  CQTB860  CQTB900  CQTBA00
CQTBB00  CQTBC00  CQTBD00  CQTBE00
```

以下のプログラムを定義する必要があります。

```
CQTPAPI0  CQTPAPPL  CQTPSNP0  CQTPATCH  CQTPCHEK  CQTPDTCH
CQTPLT00  CQTPSTRT  CQTP0000  CQTP0010  CQTP0020  CQTP0030
CQTP0031  CQTP0040  CQTP0041  CQTP0042  CQTP0043  CQTP0044
CQTP0050  CQTP0055  CQTP0056  CQTP0058  CQTP0059  CQTP0060
CQTP0070  CQTP0080  CQTP0081  CQTP0082  CQTP0083  CQTP0084
CQTP0086  CQTP0090  CQTP0091  CQTP0100  CQTP0110  CQTP0111
CQTP0112  CQTP0113  CQTP0114  CQTP0120  CQTP0130  CQTP0131
CQTP0132  CQTP0133  CQTP0134  CQTP0135  CQTP0136  CQTP0140
```

通常の実行可能プログラムに加えて、いくつかのモジュールには、すべての zSecure CICS Toolkit プログラムが使用するデータが含まれています。 このデータは、すべての zSecure CICS Toolkit プログラムから永続的に使用可能でなければなりません。 データを永続的に使用可能にするには、これらのプログラムを常駐 として定義します。以下のプログラムを、常駐プログラムとして定義する必要があります。

- CQTPAPRM
- CQTPMSGE
- CQTPCNTL

すべての zSecure CICS Toolkit プログラム (通常のプログラムと常駐プログラムの両方) を EXECKEY(CICS) を使用して定義する必要があります。

互換性のために、以下のプログラムを定義することができます。アプリケーション・プログラムでは、これらのプログラムを、先行版の製品 Consul zToolkit で使用されていた名前で参照できます。これらのプログラムの名前は、Tivoli® zSecure CICS Toolkit バージョン 1.8.1 で変更されました。最良の結果を得るには、以下の名前を使用してください。

- CQTPAPI0
- CQTPSNP0
- CQTPAPPL

既存のアプリケーションに対し、そこで新しい名前が反映されるために必要な調整を行っていない場合は、以下のプログラムの定義も必要です。これらのプログラムは、新しいモジュールの別名です。

```
CRTKAPI  CRTKSNP    CRTKAPPL
```

必要な zSecure CICS Toolkit の機能を使用するために、オンライン・トランザクションを定義することが必要な場合もあります。API インターフェースの 機能のみを使用する場合は、これらのトランザクションの定義は不要です。以下に示すプログラムについて、以下のトランザクションを定義する必要があります。

```
RTCK  --> PROG(CQTPCHEK)
RTST  --> PROG(CQTPSTRT)
RTMM  --> PROG(CQTP0000)
```

► CQTJRDO を更新して実行依頼する。

開始時にこれらの定義をアクティブにする場合は、CICS リソースの活動化に使用される *list* に、*group* TOOLKIT を指定する必要もあります。

CICS テーブルの更新

CICS Toolkit SVC がインストールされていない場合は、以下の手順に従って CICS テーブルを更新して、異常終了を抑止し、CICS Toolkit 機能を自動的に開始および停止できるようにします。

CICS Toolkit SVC が利用できない場合に CICS の異常終了を回避するには、CICS システム・リカバリー・テーブル (SRT) に項目を追加する必要があります。

- DFHSRT ソースに以下の項目を追加します。

```
DFHSRT TYPE=SYSTEM,ABCODE=Fxx,RECOVER=YES
```

  パラメーター ABCODE=Fxx の厳密な定義については、7 ページの『SVC のインストール』を参照してください。SCQTSAMP のメンバー CQTSRTT1 内にサンプルが用意されています。

- インストール済み環境で使用されている CICS テーブル更新プロシージャーを使用して、SRT を変換する必要があります。通常、このプロシージャーは DFHAUPLE と呼ばれ、CICSTS54.XDFHINST に似た名前のデータ・セット内にあります。SCQTSAMP のメンバー CQTJSRT 内にサンプルが用意されています。

  ► CQTJSRT を調整して実行依頼する。

CICS の開始および停止時に、CICS Toolkit のサブタスクを自動的に開始および停止することができます。サブタスクを自動的に開始および停止しない場合は、19 ページの『RTST トランザクションの定義』に説明されているように、RTST トランザクションも使用できます。自動処理は、CICS プログラム・リスト・テーブル (PLT) に項目を追加することで活動化されます。

PLT プログラムは、CICS の開始時の検出が要です。これは、CQTPLT00 プログラムが既に CICS に定義されている必要があることを意味します。 RDO のサンプルではリソースを 定義しますが、この定義は自動的には活動化されません。リストに TOOLKIT グループ を指定するか、その他の方法でリソース定義が CICS の開始時に活動化されるようにする必要があります。

- PLTPI に以下の項目を追加します。

```
DFHPLT TYPE=ENTRY,PROGRAM=CQTPLT00
```

  この項目は、DFHDELIM 項目の後に置く必要があります。メンバー CQTPLTT1 内にサンプルが用意されています。

- PLTSD に以下の項目を追加します。

```
DFHPLT TYPE=ENTRY,PROGRAM=CQTPDTCH
```

  メンバー CQTPLTT2 内にサンプルが用意されています。

- CICS TS 5.4 以前のリリースにインストールする場合は、前に DFHSRT について説明したように、DFHPLT テーブルを変換する必要があります。SCQTSAMP のメンバー CQTJPLT 内にサンプルが用意されています。

  ► CQTJPLT を調整して実行依頼する。

  ► CICS SYSIN 内の PLTPI および PLTSD 指定を検査して調整する。

- CICS TS 5.5 リリースにインストールする場合は、DFHTABLE DD ステートメントに割り振られているデータ・セットに DFHPLT テーブルを追加する必要があります。

  ► CICS SYSIN 内の PLTPI および PLTSD 指定を検査して調整する。

RACF プロファイルの定義

以下の手順に従って、zSecure CICS Toolkit RACF コマンド・インターフェースを 使用して RACF プロファイルを定義します。

手順

1. zSecure CICS Toolkit コマンドを RACF に定義します。

   12 ページの表 4 に、zSecure CICS Toolkit コマンドと、各コマンドに必要な第 1 レベルの権限およびその下位にあたるレベルの権限 (下位レベルの権限) を示します。

表 *4. zSecure CICS Toolkit* コマンド*:* 必要な権限レベル		
コマンド	**レベル**	**下位レベル**
ADDGROUP	TOOLKIT.ADGR	ADGR.*grpname*
ADDUSER	TOOLKIT.ADUS	ADUS.*dfltgrp*
ALTGROUP	TOOLKIT.ALGR	ALGR.*grpname*
ALTUSER	TOOLKIT.AUSR 副次機能を使用してセグメントを管理する場合は、TOOLKIT.ACIC、TOOLKIT.ATSO、TOOLKIT.AOMV、またはTOOLKIT.AWRK へのアクセス権限も必要な場合があります。	AUSR.*dfltgrp*。OMVS セグメントに共有 UID を割り当てるときは、システム SPECIAL か、UNIXPRIV クラスの SHARED.IDS に対するアクセス権限も必要です。
CONNECT	TOOLKIT.CONN	CONN.*grpname*
DELDSD	TOOLKIT.DELD	DELD.*hlq*
DELGROUP	TOOLKIT.DELG	DELG.*grpname*
DELUSER	TOOLKIT.DELU	DELU.*dfltgrp*
LISTDATASET	TOOLKIT.LDSD	なし
LISTGROUP	TOOLKIT.LGRP	LGRP.*grpname*
LISTUSER	TOOLKIT.LUSR	LUSR.*dfltgrp*
PASSWORD	なし	PSWD.*grpname* **PASSWORD** コマンドは API からのみ使用できます。
PERMIT	TOOLKIT.PEMT	PEMT.*grpname* / *grpname* PERMIT が GROUP を対象とする場合、PEMT.*grpname* が使用されます。USERID が対象である場合は、PEMT.*grpname* が使用されます。 PERMIT を実行する場合、ユーザーには、アクセス権限を与える対象のリソースに対するアクセス権限も必要です。 リソースが CICS SIT に定義されていないクラスにある場合、ユーザーには PEMX.*cdtclass* へのアクセス権限も必要です。
RACLINK	TOOLKIT.RACL	RACL.*dfltgrp*
RALTER	TOOLKIT.RALT	RALT.*cdtclass*
RDEFINE	TOOLKIT.RDEF	RDEF.*cdtclass*
REMOVE	TOOLKIT.REMV	REMV.*grpname*
RDELETE	TOOLKIT.RDEL	RDEL.*cdtclass*
RLIST	TOOLKIT.RLST	RLST.*cdtclass*

表 *4. zSecure CICS Toolkit* コマンド*:* 必要な権限レベル *(*続き*)*		
コマンド	**レベル**	**下位レベル**
USRDATA	TOOLKIT.USRL 副次機能を使用して追加/更新/削除を行うとき、または API から直接これらの機能にアクセスするときには、TOOLKIT.USRA または TOOLKIT.USRD へのアクセス権限が必要です。	USRU.*grpname* USRN.*usrdata-name*
VERIFY	なし VERIFY は API からのみ使用可能です。このコマンドを使用すると、ユーザーがサインオンしなくても、アプリケーションはユーザーの ID およびパスワードを検証することができます。	なし

上記の定義における、各項目の意味を以下に示します。

- *grpname* は GROUP の名前です。
- *dfltgrp* は DEFAULT GROUP の名前です。
- *hlq* はデータ・セット名の高位修飾子です。
- *cdtclass* は CDT に定義されている GENERAL RESOURCE CLASS の名前です。

各コマンドは、トランザクションが定義されるのと同様の方法で、RACF にリソースとして定義されます。

以下の総称名を最初に定義し、UACC を NONE として指定するのが最も推奨されます。そうすることにより、コマンドへのアクセス権限がリソース・クラス内の他の総称の定義によってユーザーに与えられることがないようにすることができます。

CQTPCNTL の RSRCLASS パラメーターは TCICSTRN であるものとします。

```
RDEFINE TCICSTRN (TOOLKIT.*  ADGR.* ADUS.* ALGR.* AUSR.*
 CONN.* DELD.* DELG.* DELU.* LDSD.* LGRP.* LUSR.* PEMT.*
 PSWD.* RACL.* RALT.* RDEF.* RDEL.* REMV.* RLST.*
 USRU.* USRN.*) UACC(NONE)
```

RDEFINE コマンドを使用して、zSecure CICS Toolkit コマンドを RACF に定義します。 以下の例では、TCICSTRN が RSRCLASS パラメーターであることも前提としています。

```
RDEFINE TCICSTRN (TOOLKIT.ADGR TOOLKIT.ADUS TOOLKIT.ALGR TOOLKIT.AUSR
TOOLKIT.CONN TOOLKIT.DELD TOOLKIT.DELG TOOLKIT.DELU TOOLKIT.LDSD TOOLKIT.LGRP
TOOLKIT.LUSR TOOLKIT.PEMT TOOLKIT.REMV  TOOLKIT.RACL TOOLKIT.RALT TOOLKIT.RDEF
TOOLKIT.RDEL TOOLKIT.RLST TOOLKIT.USRL TOOLKIT.USRA TOOLKIT.USRD)
```

2. ユーザーに対して、使用を許可できるコマンドへのアクセス権限を付与します。
例えば、ADDUSER、ALTUSER、DELUSER などです。

ソフトウェアの使用時は、端末でサインオンしているユーザーの権限を使用して、実行できるコマンドおよび機能が判別されます。端末で実行中でないトランザクションがソフトウェアを使用して RACF 機能を実行する場合は、実行できるコマンドおよび機能の判別に、DEFAULT USERID の権限が使用されます。デフォルト・ユーザーの権限は、明示的にサインオンされていない端末でも使用されます。

必要に応じて、各コマンドへのアクセス権限をユーザーに付加します。例:

```
PERMIT TOOLKIT.LUSR CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.AUSR CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.LDSD CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.LGRP CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.CONN CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.REMV CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
```

```
PERMIT TOOLKIT.ADUS CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.PEMT CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
```

ユーザーがアクセス権限を持っているコマンドのみがパネルに表示されます。

例えば、ユーザーが LUSR コマンドのみに対してアクセス権限を持っている場合、他のコマンドは表示されません。

3. ユーザーがアクセスできるコマンド内の、下位の権限レベルを定義します。
例えば、ユーザーに ALTUSER コマンドへのアクセス権限を付与した後、そのユーザーが変更できるユーザーを指定する必要があります。

注 : コマンドの内部セキュリティー・リソース・クラスについては、14 ページの『内部セキュリティー・リソースのリスト』を参照してください。

ほとんどのコマンドでは、ユーザーに、下位の権限レベルを 1 つ以上付与する必要があります。このような下位の権限レベルによって、コマンドへのアクセス権限を付与されたユーザーがアクセスまたは制御できるユーザー、グループ、およびリソースが決まります。

例えば、ユーザーに ALTUSER へのアクセス権限が付与されている場合、そのユーザーがアクセス可能な ID も定義する必要があります。これを行うには、AUSR という接頭部を持つユーザーのデフォルト・グループをリソースとして定義します。これにより、ユーザーにこのリソースへのアクセス権限を付与できます。

14 ページの表 5 に、このタイプの能力を与えるために必要な定義の例を示します。

表 *5. RACF* コマンド内で使用されるリソース定義の例

USERID	**DEFAULT GROUP**	**RSRCLASS**
USER01	TECHSUPP	TCICSTRN
USER02	USERSUPP	TCICSTRN
USER03	QUALCNTL	TCICSTRN
USER04	AUDIT	TCICSTRN

この例での RACF コマンドは次のようになります。

```
RDEFINE TCICSTRN (AUSR.TECHSUPP AUSR.USERSUPP AUSR.QUALCNTL AUSR.AUDIT)
```

次に、以下のように各グループへのアクセス権限をユーザーに付加します。

```
PERMIT AUSR.TECHSUPP CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT AUSR.QUALCNTL CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT AUSR.AUDIT CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
```

上記の定義では、USER01 は、デフォルト・グループが TECHSUPP、QUALCNTL、または AUDIT であるすべてのユーザー ID に対して、ALTUSER を実行できますが、デフォルト・グループが USERSUPP であるユーザー ID やその他のデフォルト・グループを持つユーザー ID に対してはこのコマンドを実行できません。

内部セキュリティー・リソースのリスト

zSecure CICS Toolkit は、独自の内部セキュリティーを実現するために、リソース名を使用します。

14 ページの表 6 には、zSecure CICS Toolkit が独自の内部セキュリティーのために使用するリソース名がまとめられています。

表 *6. zSecure CICS Toolkit:* 内部セキュリティー・リソースのリスト

リソース名	**ユーザーが読み取り権限を持っている場合に許可される内容**
TOOLKIT.ADGR	ユーザーが、zSecure CICS Toolkit の ADDGROUP コマンドを実行することを許可します。

表 6. *zSecure CICS Toolkit:* 内部セキュリティー・リソースのリスト *(続き)*	
リソース名	**ユーザーが読み取り権限を持っている場合に許可される内容**
TOOLKIT.ADUS	ユーザーが、zSecure CICS Toolkit の ADDUSER コマンドを実行することを許可します。
TOOLKIT.ALGR	ユーザーが、zSecure CICS Toolkit の ALTGROUP コマンドを実行することを許可します。
TOOLKIT.AUSR	ユーザーが、zSecure CICS Toolkit の ALTUSER コマンドを実行することを許可します。
TOOLKIT.ACIC	ユーザーが、zSecure CICS Toolkit の ALTUSER コマンドにより、CICS セグメントを管理することを許可します。
TOOLKIT.ATSO	ユーザーが、zSecure CICS Toolkit の ALTUSER コマンドにより、TSO セグメントを管理することを許可します。
TOOLKIT.AOMV	ユーザーが、zSecure CICS Toolkit の ALTUSER コマンドにより、OMVS セグメントを管理することを許可します。
TOOLKIT.AWRK	ユーザーが、zSecure CICS Toolkit の ALTUSER コマンドにより、WORKATTR セグメントを管理することを許可します。
TOOLKIT.CONN	ユーザーが、zSecure CICS Toolkit の CONNECT コマンドを実行することを許可します。
TOOLKIT.DELD	ユーザーが、zSecure CICS Toolkit の DELETE DATASET コマンドを実行することを許可します。
TOOLKIT.DELG	ユーザーが、zSecure CICS Toolkit の DELETE GROUP コマンドを実行することを許可します。
TOOLKIT.DELU	ユーザーが、zSecure CICS Toolkit の DELETE USER コマンドを実行することを許可します。
TOOLKIT.DUPE	ユーザーが、2 つ目の端末にサインオンすることを許可しますが、最初の端末で強制的にサインオフするようにします。最初の端末で現在接続されているトランザクションがあった場合、そのトランザクションもすべてパージされます。
TOOLKIT.GPID	ユーザー ID をグループ ID として使用することを許可し、複数のユーザーがそのユーザー ID を使用して CICS にサインオンできるようにします。
TOOLKIT.LDSD	ユーザーが、zSecure CICS Toolkit の LISTDATASET コマンドを実行することを許可します。
TOOLKIT.LGRP	ユーザーが、zSecure CICS Toolkit の LISTGROUP コマンドを実行することを許可します。
TOOLKIT.LUSR	ユーザーが、zSecure CICS Toolkit の LISTUSER コマンドを実行することを許可します。
TOOLKIT.PEMT	ユーザーが、zSecure CICS Toolkit の PERMIT コマンドを実行することを許可します。
TOOLKIT.RACL	ユーザーが、zSecure CICS Toolkit の RACLINK コマンドを実行することを許可します。
TOOLKIT.RALT	ユーザーが、zSecure CICS Toolkit の RALTER コマンドを実行することを許可します。
TOOLKIT.RDEF	ユーザーが、zSecure CICS Toolkit の RDEFINE コマンドを実行することを許可します。

表 6. *zSecure CICS Toolkit:* 内部セキュリティー・リソースのリスト *(続き)*	
リソース名	**ユーザーが読み取り権限を持っている場合に許可される内容**
TOOLKIT.RDEL	ユーザーが、zSecure CICS Toolkit の RDELETE コマンドを実行することを許可します。
TOOLKIT.REMV	ユーザーが、zSecure CICS Toolkit の REMOVE コマンドを実行することを許可します。
TOOLKIT.RLST	ユーザーが、zSecure CICS Toolkit の RLIST コマンドを実行することを許可します。
TOOLKIT.USRL	ユーザーが、zSecure CICS Toolkit の USRDAT コマンドの一部として usrdata フィールドをリストすることを許可します。
TOOLKIT.USRA	ユーザーが zSecure CICS Toolkit の USRDAT コマンドの一部として、usrdata フィールドを追加および更新することを許可します。
TOOLKIT.USRD	ユーザーが zSecure CICS Toolkit の USRDAT コマンドの一部として、usrdata フィールドを削除することを許可します。
TOOLKIT.SPEC	zSecure CICS Toolkit からの RACF コマンドの実行時に、ユーザーに SPECIAL と同等の権限を付与します。 TOOLKIT.SPEC へのアクセス権限を持つユーザーは、特定のコマンド内ですべてのリソースに対するアクセスを許可されます。例えば、ユーザーが LISTUSER コマンドと TOOLKIT.SPEC へのアクセス権限を持っている場合、そのユーザーはすべての ユーザーをリストすることができ、LUSR.dfltgrp 定義の制限は受けません。TOOLKIT.SPEC は 1 つのコマンド内で すべての リソースに対するアクセス権限をユーザーに付与しますが、ユーザーにそのコマンドへのアクセス権限は付与しません。この例では、ユーザーが LISTUSER コマンドを使用するためには、ユーザーに TOOLKIT.LUSR へのアクセス権限が必要です。これは、zSecure CICS Toolkit インターフェースによって 実行される RACF コマンドのみに当てはまります。
TOOLKIT.SVC	領域で zSecure CICS Toolkit SVC を使用することを許可します。
ADGR.grpname	ユーザーが ADDGROUP を実行できる対象のグループを定義します。
ADUS.*dfltgrp*	ユーザーが ADDUSER を実行できるデフォルト・グループを定義します。
ALGR.*grpname*	ユーザーが ALTGROUP を実行できるデフォルト・グループを定義します。
AUSR.*dfltgrp*	ユーザーが ALTUSER を実行できる対象のグループを定義します。
CONN.*grpname*	ユーザーが CONNECT を実行できる対象のグループを定義します。
DELD.*hlq*	ユーザーが DELETE DATASET を実行できるデータ・セットの名前の高位修飾子を定義します。詳細については、46 ページの『データ・セットの削除 (DELETE DATASET コマンド)』を参照してください。
DELG.*grpname*	ユーザーが DELETE GROUP を実行できる対象のグループを定義します。
DELU.*dfltgrp*	ユーザーが DELETE USER を実行できるデフォルト・グループを定義します。
LGRP.*grpname*	ユーザーが LISTGROUP を実行できる対象のグループを定義します。
LUSR.*dfltgrp*	ユーザーが LISTUSER を実行できるデフォルト・グループを定義します。

表 6. *zSecure CICS Toolkit:* 内部セキュリティー・リソースのリスト *(続き)*	
リソース名	**ユーザーが読み取り権限を持っている場合に許可される内容**
PEMT.*dfltgrp* / *grpname*	ユーザーが PERMIT を実行できるデフォルト・グループまたはグループを定義します。
PEMX.*cdtclass*	リソースが CICS SIT に定義されているクラスにない場合に、ユーザーが PERMIT を実行できる一般リソース・クラス (DATASET クラスを含む) を定義します。
PSWD.*dlftgrp*	指定されたデフォルト・グループ内で、ユーザーの PASSWORD を変更する権限を付与します。
RACL.*dfltgrp*	ユーザーが RACLINK を実行できる対象のグループを定義します。
RALT.*cdtclass*	ユーザーが RALTER を実行できる一般リソース・クラスを定義します。
RDEF.*cdtclass*	ユーザーが RDEFINE を実行できる一般リソース・クラスを定義します。
RDEL.*cdtclass*	ユーザーが RDELETE を実行できる一般リソース・クラスを定義します。
REMV.*grpname*	ユーザーが REMOVE を実行できる対象のグループを定義します。
RLIST.*cdtclass*	ユーザーが RLIST を実行できる一般リソース・クラスを定義します。
SECL.*nnn*	ユーザーに許可されるユーザー ID に対して、そのユーザーが指定できる SECLEVEL を指定します。*nnn* は、001 から 254 までの SECLEVEL を示す数値です。
USRU.*dfltgrp*	ユーザーが USRDATA フィールドを表示できるデフォルト・グループを定義します。
USRN.*usrdata-name*	ユーザーが表示または追加/更新/削除することができる *usrdata* の名前を定義します。

USS UID の自動割り当て (OMVS AUTOUID)

一意の USS UID の自動割り当てを使用する場合は、以下の要件を満たしていることを確認する必要があります。

- RACF データベースを、アプリケーション識別マッピングに対して使用可能にしておく必要があります。必要な最小ステージは、ステージ 2 です。
- FACILITY クラスのプロファイル BPX.NEXT.USER が、適切な APPLDATA と共に定義されている必要があります。「*RACF* セキュリティー管理者のガイド」に、詳細な情報が記載されています。『*RACF* および *z/OS UNIX*』の章を参照してください。
- RACF TSO コマンドでの AUTOUID の使用時にも、プロファイル SHARED.IDS が定義されていること、および UNIXPRIV リソース・クラスがアクティブであり、RACLIST 処理されていることが必要です。

ホーム・ディレクトリーの自動作成 (OMVS MKDIR)

ユーザーの OMVS セグメントを作成するときに、ホーム・ディレクトリーの自動作成を使用するには、以下の追加の要件が満たされている必要があります。

- OMVS のホーム・ディレクトリーでは大/小文字が区別されるため、ご使用の端末で大/小文字混合が現在サポートされている必要があります。ご使用の端末で大文字のみが使用されている場合、OMVS セグメントで指定されている OMVS ホーム・ディレクトリーと zSecure CICS Toolkit で作成される実際のディレクトリーの両方で大文字が使用されます。
- CICS 領域のユーザー ID に、UID を割り当てる OMVS セグメントを定義している必要があります (あるいは、DEFAULT UID の使用を可能にしている必要があります)。

- CICS 領域のユーザー ID の現在のグループに、GID を割り当てる OMVS セグメントを定義している必要があります。 あるいは、DEFAULT GID の使用を可能にしている必要があります。
- CICS 領域のユーザー ID は、ホーム・ディレクトリーの作成に十分なアクセス権限を保持している必要があります。これは、次のいずれかの方法で実装することができます。

  UID=0
  このオプションによって、CICS 領域に、 USS 環境全体に対する完全制御が与えられます。 このオプションは、初期テスト時に受け入れられますが、通常の実稼働環境には適していません。

  UNIXPRIV
  UNIXPRIV プロファイル SUPERUSER.FILESYS に対する CONTROL アクセス権限を付与することもできます。これにより、CICS 領域に、ファイル・システム内のすべてのファイルへの READ/WRITE アクセス権限が与えられるためです。このオプションは、実動には使用しないでください。

  ユーザーのホーム・ディレクトリーを作成する必要があるディレクトリーへの WRITE アクセス権限
  このオプションでは、CICS 領域に、必要な権限だけが与えられます。 これは推奨されるオプションです。

  CICS 領域のユーザー ID に UID=0 を付与しないことを選択した場合は、新しく作成されるホーム・ディレクトリーの正しい所有者を設定する権限を、CICS 領域に付与することも必要になります。これを行わないと、目的のユーザーが新しいホーム・ディレクトリーを表示できないことがあります。通常は許可を必要とする CHOWN コマンドを使用して、正しい所有者を設定してください。

  UNIXPRIV SUPERUSER.FILESYS.CHOWN
  このプロファイルへの READ アクセス権限を付与することにより、システム内のすべてのファイルの所有者 (userid = dfltgrp) の変更を許可します。 これはかなり強力な権限であるため、この方法は使用しないことをお勧めします。

  UNIXPRIV CHOWN.UNRESTRICTED
  この個別プロファイルにより、すべてのユーザーが自分が所有するファイルまたはディレクトリーの所有者を変更することができます。これは、従来のデータ・セット・プロファイルに対する RACF の動作と同様です。 zSecure CICS Toolkit は最初に CICS 領域を所有者としてホーム・ディレクトリーを作成するため、所有者を目的のユーザーに変更する権限が付与されます。

zSecure CICS Toolkit の再始動

通常は、インストール済み環境に対して必要なすべての更新および定義を行った後、CICS システムを再始動して、すべての変更を有効にする必要があります。初期インストールの場合、SRT 定義などを有効にするために、再始動が必要です。zSecure CICS Toolkit の SVC の定義を反映させるために必要なシステム IPL とこの有効化を組み合わせて行うことができます。

zSecure CICS Toolkit は内部で MVS サブタスクを使用します。通常これらのサブタスクは、PLT プログラムによる CICS の初期化時に開始されます。これらの MVS サブタスクは、2 番目の PLT プログラムによる CICS の終了時に切り離されます。インストール・プロセスのこの部分で CICS を再始動する方法が推奨されます。

必要なすべての定義を行ったにもかかわらず、CICS を再始動できない場合は、代わりに以下の代替方法を使用してください。

重要 : このプロセスを使用して zSecure CICS Toolkit を最初に活動化した場合は、このプロセスを使用して非活動化してから CICS システムをシャットダウンする必要があります。これを行わないと、A03 の異常終了が起こり、その後システム・メモリー・ダンプが行われる可能性があります。

zSecure CICS Toolkit SVC がインストールされておらず、CICS SRT 定義が有効化されていない場合は、ソフトウェアのサブタスクをインストールしようとすると、CICS 開始タスクが終了する異常終了となることがあります。

zSecure CICS Toolkit プログラムの実行中にエラーが発生することがあります。 このようなエラーの中には、zSecure CICS Toolkit の処理に使用される MVS サブタスクの 1 つを終了させるものがあります。現在のバージョンの zSecure CICS Toolkit は、MVS サブタスクを停止し、再始動するトランザクションを提供します。以前のバージョンでは、手動によるプロセスを必要とします。 この手動によるプロセスについては、19 ページの『zSecure CICS Toolkit サブタスクの手動による再始動』で説明しています。

RTST トランザクションの定義

CRTKSTRT プログラムを実行するために、RTST トランザクションを定義することができます。このプログラムは、zSecure CICS Toolkit サブタスクを停止し再始動するために必要な機能を実行します。また、各種の zSecure CICS Toolkit プログラム、マップ、パラメーター・モジュールを更新する機能も提供します。

RTST トランザクションを実行すると、以下のパネルが表示されます。

```
                        IBM Security zSecure CICS Toolkit


 Press PF-Key to execute selected function

   PF1 De-Activate subtasks

   PF2 Activate subtasks

   PF4 Refresh (newcopy) modules







 Licensed Materials - Property of IBM
 5655-N18 Copyright IBM Corp. 1982, 2019  All Rights Reserved


  PF01:DeAct PF02:Act PF04:New  PF03/Clear:Exit
```

図 *1.* 「*RTST Transaction*」パネル

このパネルでは、以下の機能が提供されます。

PF1
現在アクティブなサブタスクを 終了させます。これは各タスクに対する通常の停止要求によって行われるため、この機能を実行するのに数秒かかる場合があります。

PF2
サブタスクを開始します。このプログラムは、サブタスクを開始する前に、サブタスクが現在アクティブでないことを確認します。

PF4
zSecure CICS Toolkit プログラム、マップ、およびパラメーター・モジュールの新しいコピーを取得します。このプロセスではまず、モジュールが使用中ではないことを確認します。いくつかの永続的に常駐するモジュールの解放も行われます。また、MVS サブタスクがこの時点ではアクティブではないことも確認されます。他の端末ユーザーが並行して zSecure CICS Toolkit インターフェースを 使用していると、操作が予測不能の結果になることがあります。

RTST トランザクションでは内部許可検査が行われないため、トランザクションへのアクセスを制御する必要があります。 zSecure CICS Toolkit サブタスクの停止と開始、またはモジュールの更新が可能であることが必要なユーザーに、アクセスを限定する必要があります。

zSecure CICS Toolkit サブタスクの手動による再始動

RTST トランザクションが使用できない場合は、手動のプロセスで zSecure CICS Toolkit サブタスクを停止および開始することもできます。このプロセスでは、CECI トランザクションが使用されます。

以下の 2 つのコマンドを実行します。

```
CECI LINK PROG(CQTPKDTCH)
CECI LINK PROG(CQTPLT00)
```

これらのトランザクションを実行する場合は、端末ユーザーが DCICSDCT の CSML へのアクセス権限を持っている必要があります。CQTPCNTL で別の DESTID を構成することにした場合は、CSML を、選択した DESTID に置き換える必要があります。

CICS Transaction Server と zSecure CICS Toolkit の併用

CICS Transaction Server を実行している場合に、注意する必要のある指定がいくつかあります。

以下の指定に注意してください。

- CQTPCNTL の RSRCLASS パラメーターに、正しい RACF リソース・クラスを指定する必要があります。デフォルトでは、SIT に定義された XTRAN パラメーターの値は設定されません。
- zSecure CICS Toolkit の DUPEUSER 機能を使用する場合、プログラム CQTPSNP0 を開始することが最も推奨されます。このプログラムは、以下のいずれかの方法で呼び出すことができます。
  - このプログラムに対して XCTL または LINK を実行する
  - このプログラムを自分のサインオン・プログラムからトランザクションとして開始する
  - サインオン出口点から

  DUPEUSER のサポートを使用する大きな目的は、2 つ目の端末にログオンするときに、既存のセッションを自動的に取り消すことができるためです。

注 : CICS TS バージョン 2.1 から、EXEC CICS SIGNON コマンドの動作が変更されました。現在のトランザクションが終了した後に初めて、新しい ID が有効になります。バージョン 1.8.1 のモジュール CQTPSNP0 には、サインオンしたユーザーの ID を取得して TOOLKIT.DUPE リソースおよび TOOLKIT.GPID リソースへのアクセス権限を検査する機能が追加されています。その他の zSecure CICS Toolkit 機能では、サインオン・トランザクションを開始したユーザーの権限を使用し、新しい ID は使用されません。

グローバリゼーション

zSecure CICS Toolkit が使用する BMS マップ・セットは、SCQTSAMP 内にサンプルとして提供されています。

新しいマップ・セットに既存のマップ・セットとの互換性がある場合、インストールによってこの BMS マップ・セットに変更が加えられることがあります。変更によって生成されたコピーブック (シンボル・マップ) は、zSecure CICS Toolkit プログラム・モジュールで使用される変更されていないコピーブックと 同一でなければなりません。 変更できる唯一の部分は、フィールド属性 (ある特定のフィールドの表示を抑止する属性など)、またはフィールドの初期値です。すべてのフィールドが存在する必要があるという点は変わらず、フィールド長は変更できません。CICS では、BMS マップのこの他の部分を変更できる場合がありますが、これは zSecure CICS Toolkit ではサポートされません。変更されたマップ・セットは、標準の DFHMAPS プロシージャーを使用して翻訳する必要があります。

第 3 章 zSecure CICS Toolkit のパラメーター

パラメーター・モジュール CQTPCNTL は、zSecure CICS Toolkit が使用するパラメーターを定義するために使用します。

パラメーターを設定したら、RTCK トランザクションを使用して、これらを検査します。エラーはエラー・メッセージとともに表示されます。zSecure CICS Toolkit を実装する前に、エラーをすべて解決してください。

注 : CQTPCNTL の内容は改訂されており、先行版の製品 Consul zToolkit で使用していたメンバー CRTKCNTL との互換性はなくなっています。

CQTPCNTL パラメーターのセットアップ例を以下に示します。

```
CQTPCNTL CSECT
CQTPCNTL AMODE 31
CQTPCNTL RMODE ANY
*
EXITPGM  DC    CL8'        '
DESTID   DC    CL4'CSML'
CICSAPPL DC    CL8'IGNOREIT'
RSRCLASS DC    CL8'TCICSTRN'
CMNDPFX  DC    CL8'TOOLKIT.'
SMFUID   DC    CL8'        '
SVCNUM   DC    CL3'222'
DUPEUSER DC    CL1'2'
RACFCMND DC    CL1'Y'
LOGGING  DC    CL1'Y'
PEMTALL  DC    CL1'Y'
LGDFLTU  DC    CL1'N'
         END
```

付属の CQTJCNTL のサンプル・ジョブを使用して、SMP/E からの更新を適用します。適用できない場合は、IBM 提供の DFHASMVS プロシージャーと DFHLNKVS プロシージャーを使用して、モジュールのアセンブルとリンクを行うこともできます。パラメーターは、例に示すとおりの順序で指定する必要があります。例に示した定義は、 インストール・モジュールでのデフォルトです。パラメーターは、ご使用のインストール済み環境に応じてカスタマイズできます。

パラメーターの説明

CQTPCNTL に記述するパラメーターを以下のリストに示します。

EXITPGM
メインの zSecure CICS Toolkit トランザクション (通常は RTMM) が終了したときに制御を受け取るプログラムの名前。出口プログラムを使用しない場合は、ブランクを指定します。出口プログラム機能について詳しくは、77 ページの『第 6 章 zSecure CICS Toolkit の出口点の指定』を参照してください。

DESTID
宛先。zSecure CICS Toolkit は、これをランタイム・メッセージの書き込みに使用します。デフォルトは CSML です。これは、他の任意のエントリーに変更できますが、CSML の定義に従う必要があります。「CICS リソース定義ガイド」を参照してください。

CICSAPPL
このパラメーターは、アプリケーションのセキュリティーで RSRC API インターフェースを 使用する場合に、トランザクション名の接頭部として使用されます。 IGNOREIT が指定されているかブランクになっている場合、このパラメーターは無視されます。パラメーターをコーディングする 場合の最大長は 8 バイトで、RACF の命名規則に従う必要があります。詳しくは、27 ページの『第 4 章 アプリケーション・セキュリティーの管理』を参照してください。

RSRCLASS
zSecure CICS Toolkit によって使用される RACF リソース・クラス。zSecure CICS Toolkit は、リソース検査の実行時にこのクラスを使用します。このクラスは、CICS による RACLIST 処理を行えるように、SIT で CICS に対して定義されているクラスのいずれかにします。 これは、グループ・クラスではな

く、MEMBER クラスの名前になっている必要があります (例えば、GCICSTRN **ではなく** TCICSTRN)。ブランクのままにしたり無効なクラスを指定したりすると、zSecure CICS Toolkit の初期化が失敗します。リソース・アクセス権限検査 (拡張) の実行時に API によって使用されるリソース・クラスは、API に渡すパラメーターとして定義することができ、それらのリソース検査の対応する定義をオーバーライドします。詳しくは、API の資料を参照してください。

CMNDPFX
ユーザーが使用できる zSecure CICS Toolkit コマンドと、ユーザーが zSecure CICS Toolkit トランザクション (RTMM) を入力したときに表示される zSecure CICS Toolkit コマンドは、11 ページの『RACF プロファイルの定義』 のステップ 1 で説明しているように RACF 定義によって決定されます。 これらの定義には、いずれも TOOLKIT. という接頭部が付いています。CMNDPFX パラメーターを使用すると、別の接頭部を指定することができます。ただし、この接頭部は、zSecure CICS Toolkit トランザクションを使用する場合のみ有効です。API 経由で zSecure CICS Toolkit にアクセスするときは、常に接頭部 TOOLKIT. が使用されます。

例えば、CMNDPFX が CICSONE で、ユーザーが ADDUSER を実行しようとする場合、このユーザーには以下の権限が必要です。

- zSecure CICS Toolkit トランザクションを使用する場合は、CICSONE.ADUS に対するアクセス権限
- API 経由で ADDUSER を実行する場合は、TOOLKIT.ADUS に対するアクセス権限

これにより、API を使用した操作の実行がより柔軟になり、zSecure CICS Toolkit トランザクション表示でのオプションが制限されます。

このパラメーターは 8 文字で指定し、ピリオド (.) で終了する必要があり、空白を含むことはできません。デフォルトは TOOLKIT です。

SMFUID
RACF データベースに対する変更を反映する SMF レコードを zSecure CICS Toolkit が作成する場合、端末にログオンしているユーザーの ID が SMF レコード内で使用されます。ただし、SMF レコード内の ID を別の ID にしたい場合もあります。例えば、他の RACF データベースを更新するために別のシステムに SMF レコードを転送する場合に、そのシステムで変更を行うために必要な権限をこのユーザーが持っていない可能性があります。このような場合、zSecure CICS Toolkit によって作成された SMF レコードで使用する別の ID を SMFUID で指定することができます。

このパラメーターをブランクにした場合は、端末ユーザーの ID が SMF レコード内で使用されます。

注 : この値は、SMF80UID フィールドとは異なります。SMF80UID フィールドは、常に値 TOOLKIT* に設定され、レコードが zSecure CICS Toolkit の機能の一部として生成されたことを示します。

SVCNUM
zSecure CICS Toolkit SVC に割り当てられた SVC 番号。

DUPEUSER
このパラメーターを使用して、ユーザー・サインオンを制御します。

- このパラメーターに 0 を指定した場合、ユーザーがサインオンするときの検査は実行されません。
- 1 を指定した場合、同じ RACF ユーザー ID が別の端末でサインオンしているかどうかが zSecure CICS Toolkit によって検査されます。該当する場合は、重複するサインオンが禁止され、そのユーザー ID がサインオフされます。
- このパラメーターに 2 を指定した場合は 1 の場合と同じ結果になりますが、端末のログオフ (CSSF LOGOFF の実行に相当) も行われる点が異なります。

重複ユーザー ID の検査を MRO 環境で実行する場合、検査は領域を所有する端末でのみ行われます。ユーザーが CRTE トランザクションを使用してアプリケーション領域に経路指定する場合、その領域での検査は実行されません。

ユーザーの許可:

DUPEUSER パラメーターに 1 または 2 を指定した場合、特定のユーザー ID をグループ ID として使用することを許可したり、特定のユーザー ID に対して 2 番目の端末へのログオンを許可する一方で現在サインオン中の端末からログオフするように指定することができます。この機能を使用するには、

RACF に対して以下のリソースを定義します (この例では、SIT の XTRAN パラメーターが CICSTRN であると想定しています)。

```
RDEFINE TCICSTRN (TOOLKIT.GPID TOOLKIT.DUPE) UACC(NONE)
```

ユーザー ID をグループ ID として使用できる (複数のユーザーが共有できる) ようにするには、TOOLKIT.GPID へのアクセスを許可します。

例えば次のとおりです。

```
PERMIT TOOLKIT.GPID CLASS(TCICSTRN) ID(GROUP01) ACCESS(READ)
```

これにより、CICS にサインオンするときに、複数のユーザーが GROUP01 を使用できるようになります。

ユーザーが 2 番目の端末にログオンできるようにする一方で最初の端末から強制的にログオフさせるには、TOOLKIT.DUPE へのアクセスを許可します。

例えば次のとおりです。

```
PERMIT TOOLKIT.DUPE CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
```

これにより、USER01 は 2 番目の端末にサインオンできるようになりますが、このユーザーがサインオンした最初の端末では強制的なサインオフが実行されます。

ユーザーが TOOLKIT.DUPE と TOOLKIT.GPID の両方にアクセスできる場合は、TOOLKIT.GPID が優先されます。

RACFCMND
アプリケーションが、内部セキュリティー検査とサインオン制御のいずれか、または両方の目的でのみ zSecure CICS Toolkit を使用する場合は、領域内のサブタスクすべてが必要になるわけではありません。それらのサブタスクは、zSecure CICS Toolkit または API を使用して RACF コマンドを実行する場合のみ、必要になります。 この場合、領域ごとに約 40K を節約できるため、zSecure CICS Toolkit が複数の領域に存在する場合は、さらに節約効果が大きくなります。

コマンドを使用する場合は Y を、使用しない場合は N を指定します。

LOGGING
アプリケーション・プログラムが API を使用してリソースのアクセス権限を検査するときには、zSecure CICS Toolkit はリソースの AUDIT パラメーターに基づいて SMF レコードを生成します。つまり、ユーザーがそのリソースに対するアクセス権限を持っておらず、失敗の監査が有効になっているか AUDIT が all である場合は、zSecure CICS Toolkit によって SMF レコードが生成されます。

これに伴い、不要な SMF レコードが大量に生成されてしまうことがあります。zSecure CICS Toolkit でこれらのレコードが生成されるようにするには、Y を指定します。これらのレコードが生成されないようにするには、N を指定します。RSRC 関数と RSRX 関数の場合は、S を指定することもできます。この値を指定した場合、アクセス違反があった場合に表示されるメッセージは出力されなくなりますが、これらの違反に関する SMF レコードは生成されます。それ以外の関数の場合、S は Y と同じものとして解釈されます。

このパラメーター設定は、ユーザーが RACF データベースのプロファイルを変更または更新したときに zSecure CICS Toolkit によって生成される SMF レコードには適用されません。

PEMTAL
このパラメーターを使用して、PERMIT コマンドの有効範囲を制御します。SIT に指定されていて (例えば、XDCT、XFCT、XJCT、SPPT、XTRAN などに指 定されている)、かつ、CICS によって RACLIST 処理が実行されたクラス内のリソースにしかアクセスできないように、PERMIT コマンドを制限することができます。その場合は N を指定します。PERMIT コマンドを DATASET を含むすべてのリソース・クラスで使用できるようにするには、Y を指定します。詳しくは、14 ページの『内部セキュリティー・リソースのリスト』と 64 ページの『リソースに対するアクセス権限の付与または除去 (PERMIT コマンド)』で説明している PEMX と PEMT の定義を参照してください。

LGDFLTU
このパラメーターを使用して、LISTGROUP 関数のサブ関数としての USERID の表示を制御します。この値を N に設定すると、指定された GROUP に接続しているすべてのユーザーが表示されます。この値を Y に設定すると、 端末ユーザーの DFLTGRP に接続しているユーザーだけが表示されます。

CQTPCNTL パラメーター値の検査

各領域は、専用のバージョンの CQTPCNTL を持つことができます。ただし、エラーを避けるため、CICSAPPL の値は慎重に選択してください。

CQTPCNTL をコーディングしたら、トランザクション **RTCK** を使用してパラメーターを検査してください。この操作は、zSecure CICS Toolkit を実装する前に行ってください。

「RTCK transaction」パネルを表示します。以下のパネルが表示され、発生した可能性のあるエラーがすべて表示されます。

```
                    IBM Security zSecure CICS Toolkit
                CICS level = 0690 Toolkit level = HCQT240

Exit program                          Has not been defined to CICS
Destination                 CSML      Destination id for messages
Prefix (Appl security)      IGNOREIT  Application prefix for security
Resource class              TCICSTRN  Member class name for Toolkit

LG users in DFLTGRP only    N         N=All users, Y=Only matching DFLTGRP
Duplicate Signon            2         0=Yes,1=No(Signoff),2=No(Logoff)
Toolkit SVC                 222       Required for RACF commands
RACF commands               Y         Region may issue RACF commands
Logging                     Y         SMF Records if audit specified
PEMTALL                     Y         Allow permits for all classes









 PF03/Clear=Quit      Check Highlighted fields for error messages
```

図 2. 「*RTCK transaction*」パネル

実行するタスクのファンクション・キーを以下から選択します。

- メインメニューで PF01 を押すと、zSecure CICS Toolkit コマンドに対する自分のアクセス権限が表示されます。
- メインメニューで PF02 を押すと、zSecure CICS Toolkit プログラムとその状況、および PTF レベルが表示されます。
- メインメニューから PF04 を押すと、zSecure CICS Toolkit サブタスクとその状況、および PTF レベルが表示されます。
- CLEAR または PF03 を押すと、トランザクションが終了します。他のいずれかのキーを押すと、メインメニューが再表示されます。

プログラムとサブタスクの出力例を以下の 2 つのパネルに示します。

プログラムの状況を出力したパネルの例 (部分):

```
Program  PTFlevl ST Program  PTFlevl ST Program  PTFlevl ST Program  PTFlevl ST

CQTPAPRM         OK CQTPCNTL         OK CQTPMSGE         OK CQTPLT00 HCQT240 OK
CQTPATCH HCQT240 OK CQTPDTCH HCQT240 OK CQTPCHEK HCQT240 OK CQTPAPI0 HCQT240 OK
CQTP0000 HCQT240 OK CQTP0010 HCQT240 OK CQTP0020 HCQT240 OK CQTP0030 HCQT240 OK
CQTP0040 HCQT240 OK CQTP0041 HCQT240 OK CQTP0042 HCQT240 OK CQTP0043 HCQT240 OK
CQTP0044 HCQT240 OK CQTP0050 HCQT240 OK CQTP0055 HCQT240 OK CQTP0056 HCQT240 OK
CQTP0058 HCQT240 OK CQTP0059 HCQT240 OK CQTP0060 HCQT240 OK CQTP0070 HCQT240 OK
CQTP0080 HCQT240 OK CQTP0081 HCQT240 OK CQTP0082 HCQT240 OK CQTP0083 HCQT240 OK
CQTP0084 HCQT240 OK CQTP0086 HCQT240 OK CQTP0090 HCQT240 OK CQTP0091 HCQT240 OK
CQTP0100 HCQT240 OK CQTP0110 HCQT240 OK CQTP0111 HCQT240 OK CQTP0112 HCQT240 OK
CQTP0113 HCQT240 OK CQTP0114 HCQT240 OK CQTP0120 HCQT240 OK CQTP0130 HCQT240 OK
CQTP0131 HCQT240 OK CQTP0132 HCQT240 OK CQTP0133 HCQT240 OK CQTP0134 HCQT240 OK
CQTP0140 HCQT240 OK
```

図 *3. zSecure CICS Toolkit:* プログラムの状況の出力

サブタスクの状況を出力したパネルの例 (部分):

```
Program  PTFlevl ST Program  PTFlevl ST Program  PTFlevl ST Program  PTFlevl ST

CQTSUBS  HCQT240 AV CQTS000  HCQT240 AV CQTS010  HCQT240 AV CQTS020  HCQT240 AV
CQTS030  HCQT240 AV CQTS041  HCQT240 AV CQTS042  HCQT240 AV CQTS043  HCQT240 AV
CQTS044  HCQT240 AV CQTS050  HCQT240 AV CQTS055  HCQT240 AV CQTS056  HCQT240 AV
CQTS058  HCQT240 AV CQTS059  HCQT240 AV CQTS060  HCQT240 AV CQTS070  HCQT240 AV
CQTS081  HCQT240 AV CQTS082  HCQT240 AV CQTS083  HCQT240 AV CQTS084  HCQT240 AV
CQTS086  HCQT240 AV CQTS090  HCQT240 AV CQTS100  HCQT240 AV CQTS111  HCQT240 AV
CQTS112  HCQT240 AV CQTS113  HCQT240 AV CQTS114  HCQT240 AV CQTS120  HCQT240 AV
CQTS131  HCQT240 AV CQTS132  HCQT240 AV CQTS133  HCQT240 AV CQTS134  HCQT240 AV
CQTS135  HCQT240 AV CQTS136  HCQT240 AV CQTS140  HCQT240 AV
```

図 *4. zSecure CICS Toolkit:* サブタスクの状況の出力

第 4 章 アプリケーション・セキュリティーの管理

zSecure CICS Toolkit では、1 回のシステム呼び出しで複数のリソースへのアクセスを要求できます。

従来、CICS で実行されるアプリケーションは、なんらかの独自の内部セキュリティーを使用してきました。CICS と外部セキュリティー・マネージャーがトランザクションへのアクセスを制御できる場合であっても、それらのトランザクションのサブ関数へのアクセスは、アプリケーションによって管理するしかありませんでした。

この方式では、以下のような望ましくない結果が発生します。

- アプリケーションごとに異なる形式のセキュリティーが実装される。 そのため、複数のアプリケーションにアクセスする必要があるユーザーは、複数の制御点から頻繁にアクセスを要求しなければならない。
- アクセス権限の付与が遅くなり、どのユーザーがどの権限を持っているかの管理が行き届かない。
- 作業負荷が増大する。
- 多くの場合、1 人のユーザーが複数の ID を必要とする。

数年前からは、アプリケーションには、EXEC CICS QUERY SECURITY 関数を実行するというオプションも用意されるようになりました。しかし、アプリケーションが多くのリソースに対する許可を設定する必要がある場合 (例えば、選択パネルに表示するオプションを判別するなど)、許可の要求に時間がかかることがあります。そのような場合は、zSecure CICS Toolkit を使用すると効果的です。zSecure CICS Toolkit の RSRC 関数または RSRX 関数を使用すると、1 回のシステム呼び出しで複数のリソースへのアクセスを要求することができます。

オペレーター ID (OPID) の検査

さまざまなアプリケーションで採用されている、セキュリティー検査を実行するための従来の方法は、ユーザーに設定された 3 バイトのオペレーター ID に基づいています。この ID は、このユーザー (オペレーター ID) が実行できる機能の配列やマトリックスが格納されたテーブルまたはファイルに対して照合されます。

このような社内セキュリティー方式は、膨大な機密漏れが発生する原因となります。オペレーター ID が固有であることを保証する機能は、CICS には用意されていません。また、OPID には 3 文字を使用しますが、多くの場合、すべてのユーザーに対応するには不十分です。アプリケーション・セキュリティーの検査に zSecure CICS Toolkit を使用することにより、このような機密漏れを防ぐことができます。それ以外にも、セキュリティー定義が集約され、すべてのアプリケーションで 1 つのセキュリティー・システム (RACF) が使用されるという利点があります。

アプリケーションの変換

zSecure CICS Toolkit を使用して OPID を検査するには、既存のアプリケーションを変換する必要があります。

これを行うには、これからセキュリティーの検査を行うアプリケーションに対し、コーディング変更を行う必要があります。アプリケーションがパッケージである場合は、ベンダーに連絡して、セキュリティー検査を実行する出口点をパッケージ内に作成します。セキュリティー検査で RACF のセキュリティー機能を使用するには、zSecure CICS Toolkit API を使用します。この API を使用すると、1 回の呼び出しで 2000 を超えるリソースを検査することができます。API とそのさまざまな関数および機能の使用について詳しくは、79 ページの『第 7 章 アプリケーション・プログラミング・インターフェース (API)』を参照してください。アプリケーション・プログラムでは、ユーザーがアクセスしようとする関数を指定するパラメーターを使用して、CQTPAPI0 にリンクすることができます。 次に CQTPAPI0 は、ユーザーがこの関数にアクセスできるかどうかを調べ、該当する戻りコードで呼び出し元アプリケーションに戻ります。この例では、アプリケーションによる CQTPAPI0 の使用方法と RACF に対する定義の使用方法、および CQTPAPI0 からの戻りコードを示します。

ユーザーによって実行されるトランザクションが複数の関数を持っている場合、通常は、ユーザーに対してメニュー・パネルが表示されます。ユーザーは、その中からいずれかのオプションを選択します。以下の例では、ユーザーがトランザクション ABCD を実行したとします。アプリケーションにより、以下のようなオプション・メニューがユーザーに対して表示されます。

```
               OPTION DESCRIPTION

               1      READ PAYROLL MASTER RECORDS
               2      UPDATE PAYROLL MASTER RECORDS
               3      ADD PAYROLL MASTER RECORDS
               4      DELETE PAYROLL MASTER RECORDS

               ENTER OPTION : _
```

図 *5.* オプション・メニューの例

このトランザクション ABCD はすべての関数を実行しますが、それらすべての関数に対するアクセス権限をすべてのユーザーが持っている必要はありません。RACF に対して個々の関数を定義するため、各関数に別名を割り当てます。これらの関数は、オプション 1 の場合は READ、オプション 2 の場合は UPDT、オプション 3 の場合は ADDS、オプション 4 の場合は DELT であるとします。ユーザーがこれらのオプションのいずれかを選択すると、アプリケーション・プログラムは COMMAREA を使用して、CQTPAPI0 に対する LINK を実行します。以下に、例を示します。この例では、READ、UPDT、ADDS、および DELT の中のいずれかの別名を使用できます。戻りコードは CQTPAPI0 によって設定されます。

```
*
                MVC API_FUNC,=CL4'RSRC'             MOVE FUNCTION CODE FOR
*                                                   A RESOURCE  CHECK
                MVC   API_RESOURCE_NAME,=CL13'READ' OPTION REQUESTED BY USER
                MVI   API_END,X'FF'                 END OF RESOURCE NAMES
*
                EXEC CICS LINK PROGRAM('CQTPAPI0') COMMAREA(API-COMM)
*
                CLI   API_RESOURCE_RC,X'00'         ACCESS ALLOWED ?
                BE    ACCESSOK                      YES
                B     ERROR                         NO
*
*
API_COMM        DS 0CL99
API_FUNC        DS CL4                              FUNCTION CODE
API_RC          DS XL1                              RETURN CODE
API_MSG         DS CL79                             MESSAGE AREA
*
API_RESOURCE_NAME  DS CL13                          RESOURCE NAME
API_RESOURCE_RC    DS XL1                           RACF RETURN CODE
API_END            DS XL1                           X'FF' END OF LIST
*
```

戻りコードは 1 バイトの 16 進コードで、以下の意味を持っています。

戻りコードの意味:

X '00'
リソースへのアクセスが許可されました。

X '94'
リソースまたはクラス名が RACF に対して定義されていません。

X '08'
ユーザーまたはグループは、リソースの使用を許可されていません。

X '0C'
RACF はアクティブではありません。

X '10'
Fracheck インストール・システム出口エラーです。

X '14'
RACF がインストールされていないか、レベルが無効です。

COMMAREA の値が小さすぎる場合、APU_RC フィールドには X '02' が設定されます。

別名の定義

アプリケーション・セキュリティーの検査に使用される別名 (ニーモニック) は、トランザクションと同じ方法で RACF に対して定義されます。

アプリケーションの別名を定義する場合は、CICSAPPL の CQTPCNTL で定義されている値を接頭部として付加する必要があります。CICSAPPL が IGNOREIT であるかブランクである場合は、13 バイトの別名が接頭部なしで RACF に対して定義されます。右側にはブランクを埋め込む必要があります。RACF 定義は、zSecure CICS Toolkit で使用するものと同じ RACF クラス名を使用して入力する必要があります。CQTPCNTL の RSRCLASS パラメーターでの指定に従ってください。

API_FUNCTION が RSRX である場合のリソース名の長さは 246 文字までです。ただし、クラス記述子テーブル内のリソース・クラスに定義された最大限度を超えることはできません。

CICSAPPL にコーディングされた値が PRODAPPL> で、RSRCLASS の値が TCICSTRN であると仮定すると、別名は以下のように定義されます。

```
RDEFINE TCICSTRN (PRODAPPL.READ PRODAPPL.UPDT PRODAPPL.ADDS PRODAPPL.DELT)
```

ユーザーは、必要に応じて以下のようにリソースへのアクセスが許可されます。

```
PERMIT PRODAPPL.READ CLASS(TCICSTRN) ID(USER01) ACCESS (READ)
PERMIT PRODAPPL.UPDT CLASS(TCICSTRN) ID(USER02) ACCESS (READ)
PERMIT PRODAPPL.ADDS CLASS(TCICSTRN) ID(USER03) ACCESS (READ)
PERMIT PRODAPPL.DELT CLASS(TCICSTRN) ID(USER03) ACCESS (READ)
```

CICS 表での定義は不要です。RACF プロファイルが作成されると、zSecure CICS Toolkit によるアプリケーション・セキュリティー検査の実行準備が整います。

単純なアプリケーション・セキュリティー・インターフェース

第 5 章で説明するように、zSecure CICS Toolkit では CQTPAPI0 により提供される全機能 API に代わるものとして、コマンドを直接実行できるインターフェースが 用意されています。

この単純なインターフェースは、以下 2 つの機能のみを備えています。

- 現在サインオンしているユーザーのユーザー・プロファイル、現行のグループ・プロファイル、および InstData へのアクセス
- リソースに対するアクセス権限の検査

これらの 2 つの機能には、最新の CICS サービス (EXEC CICS ADDRESS ACEE や EXEC CICS QUERY SECURITY など) からもアクセスできます。従来からのユーザーがこれらの標準の CICS サービスに移行できるように、CQTPAPPL インターフェースが 用意されています。

ユーザー情報の取得

ユーザー情報取得関数を使用するには、22 バイト以上の commarea を用意する必要があります。commarea が 286 バイトを超える場合は、ユーザー用の DFTLGRP と INSTDATA も返されます。

この関数を使用するには、commarea の先頭 4 バイトに値 '????' (4 つの疑問符) を格納する必要があります。この関数の使用例は以下のとおりです。

```
                MVI       COMMAREA,' '                      Clear commarea
                MVC       COMMAREA+1(L'COMMAREA-1),COMMAREA
                MVC       COMM_FUNC,=CL4'????'              Move function code
                EXEC      CICS LINK PROGRAM('CQTPAPPL')
                            COMMAREA(COMMAREA)
                          LENGTH(COMALEN)
                CLI       COMM_RC,X'00'                     Ok?
*
*      Further processing
*
COMMAREA  DS         0CL286                          Space for COMMAREA
COMM_FUNC DS         CL4                             Function code ????
COMM_RSVD DS         CL9                             Unused
COMM_RC   DS         XL1                             Return code
COMM_USER DS         CL8                             Userid
```

```
COMM_GRP  DS         CL8                          Group
COMM_IDL  DS         XL1                          Length of instdata
COMM_IDA  DS         CL255                        Instdata
COMALEN   DC         AL2(*-COMMAREA)              Length of COMMAREA
```

戻りコードの値は以下の 2 つです。

- X'00' ユーザー情報が返されました。
- X'10' 無効であるか ACEE が存在しません。

commarea が小さすぎる場合は、COMM_RESN の先頭バイトに値「*」(アスタリスク) が返されます。commarea の長さが 0 である (存在しない) 場合、情報は返されません。

リソース・アクセス権限検査

リソース・アクセス権限検査関数を使用するには、14 バイト以上の commarea を用意して、リソースの名前を格納する必要があります。

現行ユーザーが READ アクセス権限以上の権限を持っているかどうかが検査され、その結果に応じて COMM_RC が設定されます。リソース名は、左寄せしてブランクで埋め込む必要があります。要求を処理するときには、CQTPCNTL の CICSAPPL で指定されている値が接頭部としてリソース名に付加されます。CICSAPPL の値が IGNOREIT またはブランクの場合、接頭部は付加されません。アクセス権限検査要求で使用されたリソース名は、フィールド COMM_RESN に返されます。この関数の使用例は以下のとおりです。

```
                MVI       COMMAREA,' '                      Clear commarea
                MVC       COMMAREA+1(L'COMMAREA-1),COMMAREA
                MVC       COMM_RESN,=CL13'PAYROLL'          Move resource name
                EXEC      CICS LINK PROGRAM('CQTPAPPL')
                          COMMAREA(COMMAREA)
                          LENGTH(COMALEN)
                CLI       COMM_RC,X'00'                     Access?
*
*      Further processing
*
COMMAREA  DS         0CL14                        Space for COMMAREA
COMM_RESN DS         CL13                         Resource name
COMM_RC   DS         Xl1                          Return code
COMALEN   DC         AL2(*-COMMAREA)              Length of COMMAREA
```

戻りコードの値は以下の 3 つです。

- X'00' リソースへのアクセスが許可されました。
- X'04' リソースまたはクラス名が RACF に対して定義されていません。
- X'08' ユーザーはこのリソースの使用を許可されていません。

commarea が小さすぎる場合は、COMM_RESN の先頭バイトに値「*」(アスタリスク) が返されます。commarea の長さが 0 である (存在しない) 場合、情報は返されません。

第 5 章 zSecure CICS Toolkit コマンド・インターフェース

zSecure CICS Toolkit は、CICS から RACF コマンドを実行する機能を提供します。

以下のコマンドを実行できます。ADDGROUP (ADGRP)、ADDUSER (ADUSER)、ALTGROUP (ALTGRP)、ALTUSER (ALUSER)、CONNECT (CONNCT)、manage CSDATA、DELETE GROUP (DELGRP)、DELETE USER (DELUSER)、LISTDSD (LDSD)、LISTGRP (LGRP)、LISTUSER (LUSER)、PASSWORD、PERMIT、REMOVE、RALTER、RDEFINE、RDELETE、REMOVE、RLIST、RACLINK、および manage USRDATA。

プロファイルを変更するために使用したオプションごとに、その変更内容と変更を行ったユーザーを示す SMF レコードが生成されます。これらのレコードは、通常の RACF レポートに出力されます。

すべての SMF レコードの SMF80UID フィールドで、値 TOOLKIT* が表示されます。この特殊値を使用して、レコードが zSecure CICS Toolkit 機能の一部として生成されたことが示されます。

PASSWORD および **VERIFY** コマンドは、API からのみ使用できます。zSecure CICS Toolkit API は、使用するインストール済み環境でのパネルをカスタマイズするために使用できます。詳しくは、API の資料を参照してください。

3 ページの『第 2 章 zSecure CICS Toolkit のインストール』で説明したように、ユーザーが zSecure CICS Toolkit を使用できるようにするには、そのユーザーに 1 つ以上の zSecure CICS Toolkit コマンドへのアクセス権限を付与する必要があります。

メインメニューのナビゲート

コマンド・インターフェースのメインメニューを 表示するには、これを実行するトランザクションに対するアクセス権限が必要です。有効な RACF ユーザー ID を使用して CICS へのサインオンを完了していない場合、トランザクションはメッセージ CQT006 を表示して自動的に終了します。

手順

1. コマンド・インターフェースのメインメニューを 表示するには、初期パネルで RTMM を入力します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2019/094
Userid = BCSCGB1                    MAIN MENU                   Time = 11:09:18
Name   = John Smith



PF01 ADGRP   PF02 ADUSER  PF03 ALTGRP  PF04 ALUSER  PF05 CONNCT  PF06 DELDSD

PF07 DELGRP  PF08 DELUSR  PF09 LDSD    PF10 LGRP    PF11 LUSER   PF12 PERMIT

PF13 RALTER  PF14 RACLNK  PF15 RDEFNE  PF16 RDELTE  PF17 REMOVE  PF18 RLIST

PF19 USRDAT

                          Number ===> __


Licensed Materials - Property of IBM
5655-N18 Copyright IBM Corp. 1982, 2019. All Rights Reserved.



Use PF key or enter NUMBER for desired command. Press CLEAR to exit
```

図 6. メインメニュー

2. 選択するには、PF キーを押すか、使用するコマンドの番号を入力して **Enter** を押します。

プロファイルに含まれるフィールド (例えば、ユーザーが接続されているグループなど) を表示するときに、複数のパネルに項目が表示されている場合は、PF08 を使用してページ送りできます。

グループの追加、変更、または削除 (ADDGROUP、ALTGROUP、または DELGROUP コマンド)

ADDGROUP、**ALTGROUP**、および **DELGROUP** コマンドを使用して、システムへの新規グループの追加、または既存のグループの変更または削除を行います。

このタスクについて

ユーザーは、zSecure CICS Toolkit コマンド (実行するコマンドに応じて、TOOLKIT.ADGR/TOOLKIT.ALGR/TOOLKIT.DELG/TOOLKIT.LGRP) に対するアクセス権限、およびグループ (ADGR.*grpname*/ALGR.*grpname*/DELG.*grpname*/LGRP.*grpname*) に対するアクセス権限を持っている必要があります。

手順

1. **ADDGROUP**、**ALTGROUP**、および **DELGROUP** コマンドには、メインメニューに示された指定の **PF** キーを押すことによってアクセスします。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                  GROUP =                       Time = 11:09:39

Owner =            Supgroup =            Termuacc = Y Universal = N

----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----


                |<===
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----









PF1=Addgroup 3=Delgroup 4=Altgroup ENTER=Listgroup CLEAR=Main menu
```

図 *7. ADDGROUP / ALTGROUP /DELGROUP* パネル

2. 選択したタスクを実行するために必要な値を指定します。それぞれのフィールドとその意味については、LISTGROUP コマンドで説明します。

   各種のコマンドを実行する際の必須フィールドは、以下のとおりです。

   ADDGROUP
   新規グループを定義するには、「GROUP」にグループ名を入力する必要があります。グループ名は固有であり、現在グループ名またはユーザー名として使用されていない名前でなければなりません。「所有者」は、入力されていない場合、デフォルトでユーザー ID に設定されます。グループ名を所有者として入力する場合、その名前は上位グループ (SupGroup) と同じでなければなりません。「SupGroup」は、入力されていない場合、デフォルトで現行接続グループに設定されます。「TERMUACC」は Y または N のいずれかに設定する必要があります。「UNIVERSAL」も同じく Y または N に設定する必要があります。「INSTALLATION DATA」フィールドはオプションです。必要な情報を入力した後、PF01 を押して新規グループを追加します。

   ALTGROUP
   グループ・プロファイルを変更します。「GROUP」以外の任意のフィールドを変更できます。 変更するデータを入力した後、PF04 を押してプロファイルを更新します。

DELGROUP
グループ・プロファイルを削除します。削除する GROUP の名前を入力して、PF03 を押します。このグループには、サブグループ、接続されたユーザー、またはグループ・データ・セットがあってはなりません。zSecure CICS Toolkit には、グループに接続されている可能性のあるすべてのユーザーを検出する手段がありません。このため、グループが汎用グループではない可能性があります。zSecure CICS Toolkit は、サブグループおよびユーザーの有無を確認しますが、グループ・データ・セットの有無は確認しません。

ユーザー・プロファイルの追加 (ADDUSER コマンド)

ADDUSER コマンドを使用してユーザー・プロファイルをシステムに追加します。

このタスクについて

ユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.ADUS) に対するアクセス権限と、追加するユーザー・プロファイルのデフォルト・グループ (ADUS.*dfltgrp*) に対するアクセス権限を持っている必要があります。

手順

1. **ADDUSER** コマンドには、メインメニューに示された指定の **PF** キーを押すことによってアクセスします。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                 Adduser =                      Time = 11:09:56

 Name =                      Dfltgrp =          Authority = U
 Seclevel =
 SMTWTFS FROM TILL
 YYYYYYY 0000 0000           Password =          Owner =

 Password Phrase =
                                          |<===

----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----


               |<===
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----




CQT020 -Enter details of user to be added
PF5=AddUser ENTER=Redisplay CLEAR=Main menu
```

図 *8. ADDUSER* パネル

2. ユーザーを追加するには、以下のフィールドにデータを入力します。

USERID
「ADDUSER」フィールドに入力します。ユーザー ID は、1 文字から 8 文字にできます。

NAME
通常はユーザー名です。1 から 20 文字で指定します。

DFLTGRP
ユーザーのデフォルト・グループ。 有効なグループ名を指定する必要があります。

AUTHORITY
グループ内のユーザーの権限。デフォルトは U (使用) ですが、C (作成) に変更することもできます。

SECLEVEL
ユーザーの「SECLEVEL」を指定するか、ブランクのままにします。選択可能な SECLEVEL を表示するには、RLIST コマンドを使用して SECDATA クラスおよびリソース名 SECLEVEL を表示した後、MEMBERS 表示を選択します。

LOGON DAYS
Y または N を入力して、ユーザーにシステムへのアクセスを許可する曜日を指定します。特定の曜日に N を指定すると、その曜日には、ユーザーがシステムにアクセスできなくなります。

LOGON TIME
「LOGON TIME」は、ユーザーにログオンを許可する時刻を指定します。 ユーザーが随時ログオンできるようにするには、「FROM」フィールドと 「TILL」フィールドをゼロのままにします。時刻を指定する場合は、0001 から 2359 までの範囲で指定する必要があります。

PASSWORD
ユーザーの初期パスワード。初期パスワードは、常に、有効期限が切れるように設定されます。

OWNER
プロファイルの所有者。

PASSWORD PHRASE
ユーザーの初期パスフレーズ。初期パスフレーズは、常に、有効期限が切れるように設定されます。末尾ブランクは削除されます。

注 : パスフレーズがサポートされるのは、z/OS 1.8 以上だけです。パスフレーズをサポートしていないレベルの z/OS でパスフレーズを設定しようとすると、メッセージ CQT184 が表示されます。ユーザーは、指定したように定義されますが、パスフレーズは設定されません。

INSTALLATION DATA
このフィールドには、ユーザーに関する情報を入力できます。データを入力する場合は、最後の文字を入力した後に EOF キーを押す必要があります。このフィールドはオプションです。

3. PF05 を押して新規ユーザーをシステムに追加します。

ユーザーの初期パスワードを指定しなかった場合は、デフォルト・グループの名前を初期パスワードとして使用できます。ユーザーは初めてログオンするときに、新規パスワードを入力する必要があります。

プロファイルの変更 (ALTUSER コマンド)

ALTUSER コマンドを使用して特定のユーザーのプロファイルを変更します。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、対象のユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。 プロファイルが任意のユーザーによって変更されると、常に SMF レコードが生成されます。

手順

1. **ALTUSER** コマンドには、メインメニューに示された指定の **PF** キーを押すことによってアクセスします。

```
 Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
 Userid = BCSCGB1               ALTUSER  =                       Time = 11:10:09

  Password =  ******** Resume user? (Y/N) = N Expire PW? (Y/N) = Y

  Name = ********************      Revokedt = ***** Resumedt = *****

  Password Phrase = ************************************************************
************************************* |<===

----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----
********************************************************************************
********************************************************************************
********************************************************************************
***************  |<===
 ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  CLAuth =                    NoCLauth =
  Special   = * Operations = * Auditor = * Restr = * Grpacc = * Adsp = *
  Protected = * Uaudit     = * Dfltgrp = ********    Owner = ********

  SMTWTFS From Till
  ******* **** **** Model = ******************************************
 CQT009 -Enter userid to be updated
 PF5=Update 6=CICS 7=TSO 8=OMVS 9=WORK ENTER=Redisplay CLEAR=Main menu
```

図 *9. ALTUSER* パネル

2. プロファイルを変更したいユーザーを指定します。

   ユーザーを表示するときに、そのユーザーを再開するかどうかを選択するオプションが与えられます。
3. ユーザー・パスワードを「デフォルト・グループ」の名前にリセットするには、「パスワード」フィールドの先頭位置にカーソルを置き、EOF を押してから PF05 を押して、フィールドをクリアします。
4. 特定の「パスワード」を設定するには、フィールドをクリアし、フィールドの先頭位置にカーソルを置き、新規パスワードを入力してから PF05 を押します。

   デフォルトでは、新規パスワードは期限が切れるように設定されます。SPECIAL 属性を持つユーザーは、新規パスワードを即時に変更する必要がないことを指示することができます (「**Expire PW**」を N に設定します)。

   z/OS 1.8 からは、ユーザーがパスフレーズを発行できるようにもなっています。パスフレーズを変更する必要がある場合、新しい値を指定すると変更できます。 末尾の余分な文字は必ず削除してください。zSecure CICS Toolkit は末尾ブランクを削除しますが、末尾にある疑問符 (?) またはアスタリスク (*) については、パスフレーズの一部として含めます。既存のパスフレーズを削除する場合は、「パスフレーズ」フィールドをブランクにするか、またはフィールド 全体を消去します。現行値を保持するには、表示されているすべての疑問符をそのまま残します。
5. 「REVOKEDT」を指定してユーザーを取り消すには 2 つの方法があります。
   - 「REVOKEDT」を現在日付に設定する場合、これは「ALTUSER *userid* REVOKE」の指定に相当します。取り消しフラグが設定され、取り消し日と再開日がクリアされます。
   - 「REVOKEDT」を現在日付以外の日付に指定します。ユーザーはその指定され た日付に取り消されます。
6. 「RESUMEDT」を使用してユーザーを再開します。

   特殊値 00000 (5 つのゼロ) を使用して、すべての取り消し日または再 開日を削除することもできます。このフィールドをブランクまたは空白に設定するか、あるいは表示されている値をそのまま残すと、現行値が保持されることになります。

   ユーザーを即時に再開するには、「**Resume User**」に **Y** を指定します。
7. サポートされているセグメントのいずれかを更新するには、そのセグメントに指定されている PF キーを押します。
   - ユーザーの CICS 情報を変更するには、PF06 を押します。
   - TSO セグメントを更新するには、PF07 を押します。
   - OMVS セグメントおよび WORKATTR セグメントの場合には、それぞれ PF08、PF09 を使用します。
8. SPECIAL 権限または TOOLKIT.SPEC に対するアクセス権限を持っていない限り、*+++++++* の区切り線の下にあるフィールドを変更することはできません。

DFLTGRP 値および RESTRICTED 属性には例外があります。この 2 つのフィールドは、通常の管理者が変更できます。SPECIAL 権限は必要ありません。もう 1 つの例外は、新規パスワードの期限切れの設定です。 期限切れのないパスワードを設定するユーザーには、システム SPECIAL 権限または TOOLKIT.SPEC に対するアクセス権限が必要です。SPECIAL 権限を持っている場合は、パネル上のフィールドを変更し、PF05 を押して更新することができます。

9. 指定されたクラスの権限を付与または除去するために「CLAUTH」または「NOCLAUTH」に項目を指定します。

   zSecure CICS Toolkit は、指定されたクラスが有効であるかどうかは確認しません。

ユーザーの CICS セグメントの変更 (ALTUSER CICS SEGMENT)

ALTUSER コマンドと CICS SEGMENT オプションを使用すると、特定のユーザーの CICS セグメントを変更できます。

このタスクについて

ユーザーは以下の権限を持っている必要があります。

- このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、対象のユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。
- CICS セグメントを管理するには、ユーザーは TOOLKIT.ACIC に対するアクセス権限を持っている必要があります。

手順

1. ALTUSER CICS SEGMENT コマンドにアクセスするには、メイン ALTUSER パネルで PF06 キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                ALTUSER  = BCSCGB2              Time = 11:10:47

 OPIdent = 123
 OPPrty  = 123
 Timeout = 000
 XRFSoff = NOFORCE
 OPClass =

 RSLKey  =
 TSLKey  =









CQT074 -Command completed successfully
PF5=Update 6=User 11=Delete    Enter=Redisplay CLEAR=Main menu
```

図 *10. ALTUSER (CICS SEGMENT)* パネル

OPIDENT
このユーザーに割り当てる 1 文字から 3 文字のオペレーター ID。

OPPRTY
このユーザーのオペレーター優先順位。使用できる値の範囲は、000 から 255 です。

TIMEOUT
ユーザーが最後に端末を使用した後、CICS が端末をタイムアウトにするまでの経過時間 (分数)。

2.2 リリースより前の RACF の場合、値は 000 から 255 までの範囲でなければなりません。それより後の RACF のリリースの場合、値の範囲は 000 から 999 です。いずれの場合も、ゼロの値は、端末がタイムアウトにならないことを意味します。

XRFSOFF
CICS 拡張リカバリー機構のサインオフ・オプションです。XRF テークオーバーの発生時にオペレーターをサインオフするには、FORCE を指定します。オペレーターをサインオンしたままにするには、NOFORCE を指定します。

OPCLASS
演算子クラスは、CICS が基本マッピング・サポート・メッセージをルーティングする 際に使用します。有効なクラスは、01 から 24 までの範囲です。複数の演算子クラスを指定する場合は、各クラスをコンマで区切る必要があります (例: 01,04,05,16,24)。

RSLKEY
RSL キーは、分散プラットフォーム上で CICS が使用します。 CICS リソースごとに、1 つの RSL キーが割り当てられます。ユーザーがリソースにアクセスするには、そのリソースに割り当てられた RSL キーと同じ RSL キーを持っている必要があります。有効なキーは、01 から 24 までの範囲です。値 00 および 99 には特殊な意味があります。複数の「RSLKEY」を指定する場合は、各キーをコンマで区切る必要があります (例: 01,04,05,16,24)。

注 : 現行リリースの zSecure CICS Toolkit で提供されているスペースには、「RSLKEY」の値を 22 個しか指定できません。

TSLKEY
TSL キーは、分散プラットフォーム上で CICS が使用します。CICS トランザクションごとに、1 つの TSL キーが割り当てられます。ユーザーがトランザクションを実行するには、そのトランザクションに割り当てられた TSL キーと同じ TSL キーを持っている必要があります。有効なキーは、01 から 64 の範囲です。値 00 および 99 には特殊な意味があります。複数の「TSLKEY」を指定する場合は、各キーをコンマで区切る必要があります (例: 01,04,05,16,24)。

注 : 現行リリースの zSecure CICS Toolkit で提供されているスペースには、「TSLKEY」の値を 22 個しか指定できません。

2. ユーザーの CICS セグメントの現在の情報を表示するには、ユーザー ID を入力して Enter キーを押します。
3. この情報の一部またはすべてを変更するには、新規データを入力してから、PF5 を押します。
   エラーがある場合は、その問題を示すエラー・メッセージが表示されます。
4. CICS セグメントを削除するには、PF11 を押します。

   注 : CICS セグメントを削除しても、ユーザーが CICS サービスにアクセスできなくなることはありません。 CICS サービスへのアクセスは、APPL リソース・クラスのプロファイルによって制御される場合があります。

   CICS セグメントのない CICS ユーザーは、CICS デフォルト・ユーザーの CICS セグメントから特定の値を継承します。

   OPCLASS、RSLKEY、または TSLKEY パラメーターを更新すると、前の値は常に、完全に置き換えられます。例えば、ユーザーに OPCLASS 01,02,03 が定義されている場合、02,05,06 を指定してプロファイルを更新すると、ユーザーには 02、05、および 06 だけが定義されることになります。 前の値 01、02、03 は削除されます。

ユーザーの TSO セグメントの変更 (ALTUSER TSO SEGMENT)

ALTUSER コマンドと TSO SEGMENT オプションを使用すると、特定のユーザーの TSO セグメントを変更できます。

このタスクについて

ユーザーには以下の権限が必要です。

- このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、対象のユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。

- TSO セグメントを管理するには、ユーザーは TOOLKIT.ATSO に対するアクセス権限を持っている必要があります。

FUNCTION

AUTHORITY

手順

1. ALTUSER TSO SEGMENT コマンドにアクセスするには、メイン ALTUSER パネルで PF07 キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                ALTUSER  = BCSCGB2              Time = 11:11:05

 Acctnum = *
 Destid  =
 HClass  =            JClass  =            MsgClass=            SClass  =
 Size    = 0000000    Maxsize = 0000000    Seclabl =
 Proc    = ISPFPROC   Unit    =            Udata   = 0000









CQT074 -Command completed successfully
PF5=Update 7=User 11=Delete    Enter=Redisplay CLEAR=Main menu
```

図 *11. ALTUSER (TSO SEGMENT)* パネル

ACCTNUM
ユーザーのデフォルト TSO アカウント番号。

DESTID
動的に割り振られる SYSOUT データ・セットのデフォルト宛先。

HCLASS
ユーザーのデフォルト保留クラス。

JCLASS
ユーザーのデフォルト・ジョブ・クラス。

MSGCLASS
ユーザーのデフォルト・メッセージ・クラス。

SCLASS
ユーザーのデフォルト SYSOUT クラス。

SIZE
ユーザーがログオン時に領域サイズを要求しない場合の最小領域サイズ。

MAXSIZE
ユーザーがログオン時に要求できる最大領域サイズ。

SECLABL
ユーザー・セキュリティー・ラベル。

PROC
ユーザーのデフォルト・ログオン・プロシージャーの名前。

UNIT
プロシージャーが割り振りに使用する装置、または装置のグループのデフォルト名。

UDATA
ユーザーのインストール・データ。

2. ユーザーの TSO セグメントの現在の情報を表示するには、ユーザー ID を入力して Enter キーを押します。
3. この情報の一部またはすべてを変更するには、新規データを入力してから、PF5 を押します。

   エラーがある場合には、その問題を示すエラー・メッセージが表示されます。フィールドをブランクに設定すると、そのパラメーターはユーザーの TSO セグメントから削除されます。

   「Acctnum」、「Proc」、および「Seclabl」の各パラメーターを指定するには、ユーザーが、該当する RACF リソース・クラスに含まれるこれらの定義に対するアクセス権限を持っている必要があります。

   完全な情報およびその他の TSO セグメント・フィールドについては、「RACF コマンド言語解説書」を参照してください。
4. TSO セグメントを削除するには、PF11 を押します。

   注 : TSO セグメントを削除すると、ユーザーは TSO 対話式サービスにアクセスできなくなります。

ユーザーの OMVS セグメントの変更 (ALTUSER OMVS SEGMENT)

ALTUSER コマンドと OMVS セグメント・オプションを使用すると、特定のユーザーの OMVS セグメントを変更できます。

このタスクについて

ユーザーには以下の権限が必要です。

- このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、対象のユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。
- OMVS セグメントの管理には、ユーザーは TOOLKIT.AOMV に対するアクセス権限を持っている必要があります。

手順

1. **ALTUSER OMVS SEGMENT** コマンドにアクセスするには、メイン ALTUSER パネルで **PF08** キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1               ALTUSER  = BCSCGB2               Time = 11:11:22

 UID     = 0000002009  (# or AUTOUID)  Shared  = N    MKDIR   = N
 Home    =
 Program =

 ASSizeMax   =
 CPUTimeMax  =
 FileProcMax =
 MMapAreaMax =
 ProcUserMax =
 ThreadsMax  =
 MemLimit    =
 SHMemMax    =









CQT074 -Command completed successfully
PF5=Update 8=User 11=Delete    Enter=Redisplay CLEAR=Main menu
```

図 *12. ALTUSER OMVS* セグメント・パネル

UID
ユーザーの OMVS UID。UID を別の値に変更する場合、このフィールドに AUTOUID を入力することができます。 必要なプロファイルが定義されている場合、zSecure CICS Toolkit は次の使用可能な UID を割り当てます。UID を別のユーザーに割り当て済みの値に変更しようとすると、コマンドは拒否されます。権限を持つユーザーは、「共有」パラメーターを使用することによってオーバーライドできます。

Shared
UID をユーザーに割り当てる場合、その UID は固有でなければなりません。端末ユーザーに、システム SPECIAL 属性が設定されているか、UNIXPRIV クラス内の SHARED.IDS に対するアクセス権限が与えられている場合、そのユーザーは、UID 値を複数ユーザー間で共有可能にするように要求できます。つまり、UID 値が固有である必要はありません。共有 UID を割り当てるには、「共有」フィールドに Y を入力します。

MKDIR
ホーム・ディレクトリーをユーザーに割り当てる場合、そのディレクトリーはファイル・システム内になければなりません。オプション Y を選択すると、zSecure CICS Toolkit のタスクはディレクトリーを作成して、その所有者をユーザー ID および DfltGrp に設定しようと試みます。必要な USS コマンドを実行する権限は、CICS 領域ユーザーに基づいており、CICS 端末ユーザーの権限には基づきません。インストール済み環境でこの関数が使用可能になっていない場合は、このフィールドの値を N のままにします。

Home
ユーザーのホーム・ディレクトリー。ユーザーの OMVS セグメントを変更するときには、このフィールドの大/小文字が正しいことを確実にしてください。OMVS セグメントをまったく更新しないようにするか、または端末で大/小文字混合を使用するようにします。あるいは、ユーザーの実際のホーム・ディレクトリーがすべて 大文字で定義されていることを確認します。(大/小文字が区別される) ホーム・ディレクトリーが見つからない場合、UNIX システム・サービスを使用できない場合があります。

Program
ユーザーの初期プログラム (シェル・プログラム)。ユーザーの OMVS セグメントを変更するときには、このフィールドの大/小文字が正しいことを確実にしてください。OMVS セグメントをまったく更新しないようにするか、または端末で大/小文字混合を使用するようにします。あるいは、プログラムが実際にすべて大文字で存在していることを確認します。このフィールドをブランクのままにすると、通常、USS は値 */bin/sh* をデフォルト値として使用します。

ASSizeMax
アドレス・スペース・サイズを、10 485 760 から 2 147 483 647 までの数値で定義します。指定した値は、BPXPRMxx の MAXASSIZE パラメーターで指定されている値をオーバーライドします。システム値が適切な場合には、このフィールドをブランクのままにしてください。

CPUTimeMax
プロセッサー時間を、7 から 2 147 483 647 までの数値で定義します。指定した値は、BPXPRMxx の MAXCPUTIME パラメーターで指定されている値をオーバーライドします。システム値が適切な場合には、このフィールドをブランクのままにしてください。

FileProcMax
プロセスあたりのファイル数を、3 から 524287 までの数値で定義します。通常のユーザーは、値 256 を使用できます。指定した値は、BPXPRMxx の MAXFILEPROC パラメーターで指定されている値をオーバーライドします。システム値が適切な場合には、このフィールドをブランクのままにしてください。

MMapAreaMax
メモリー・マップ・サイズを、1 から 16 777 216 までの数値で定義します。指定した値は、BPXPRMxx の MAXMMAPAREA パラメーターで指定されている値をオーバーライドします。システム値が適切な場合には、このフィールドをブランクのままにしてください。

ProcUserMax
UID あたりのプロセス数を、3 から 32 767 までの数値で定義します。指定した値は、BPXPRMxx の MAXPROCUSER パラメーターで指定されている値をオーバーライドします。システム値が適切な場合には、このフィールドをブランクのままにしてください。

ThreadsMax
プロセスあたりのスレッド数を、0 から 100 000 までの数値で定義します。値 0 を指定すると、このユーザーが実行するアプリケーションは、pthread_create サービスを使用できなくなります。指定した値は、BPXPRMxx の MAXTHREADS パラメーターで指定されている値をオーバーライドします。システム値が適切な場合には、このフィールドをブランクのままにしてください。

MemLimit
RACF の非共有メモリー・サイズを、0 から 16777215 までの数値の後に文字 M、G、T、または P を付けて定義します。

SHMemMax
RACF の共有メモリー・サイズを、1 から 16777215 までの数値の後に文字 M、G、T、または P を付けて定義します。「SHMEMMAX」に指定した値は、BPXPRMxx の IPCSHMNSEGS パラメーターで指定されている値をオーバーライドします。システム値が適切な場合には、このフィールドをブランクのままにしてください。

2. ユーザーの OMVS セグメントの現在の情報を表示するには、ユーザー ID を入力して Enter キーを押します。
3. この情報の一部またはすべてを変更するには、新規データを入力してから、PF5 を押します。

   エラーがある場合は、その問題を示すエラー・メッセージが表示されます。

   フィールドの値をすべてブランクに設定することによって、そのフィールドをユーザーの OMVS セグメントから削除することもできます。「UID」の値をゼロ (0) に設定するには、端末ユーザーに RACF システム SPECIAL 属性が設定されている必要があります。 TOOLKIT.SPEC に対するアクセス権限は、この特定の関数には適用されません。

   可能な場合は常に値 AUTOUID を使用してください。AUTOUID 関数は、z/OS 1.4 以上でのみ使用できます。使用するには、FACILITY クラスに BPX.NEXT.USER プロファイルを定義する必要があります。詳しくは、3 ページの『第 2 章 zSecure CICS Toolkit のインストール』を参照してください。
4. OMVS セグメントを削除するには、PF11 を押します。

   注 : OMVS セグメントを削除すると、ユーザーは UNIX システム・サービスにアクセスできなくなります。USS には、FACILITY クラスの BPX.DEFAULT.USER に指定されたデフォルト UID によってアクセスできる場合もあります。

ユーザーの WORKATTR セグメントの変更 (ALTUSER WORKATTR SEGMENT)

ALTUSER コマンドと WORKATTR SEGMENT オプションを使用すると、特定のユーザーの WORKATTR セグメントを変更できます。

このタスクについて

ユーザーには以下の権限が必要です。

- このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、対象のユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。
- WORKATTR セグメントの管理には、ユーザーは TOOLKIT.AWRK に対するアクセス権限を持っている必要があります。

手順

1. ALTUSER WORKATTR SEGMENT コマンドにアクセスするには、メイン ALTUSER パネルで PF09 キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                ALTUSER  = BCSCGB2             Time = 11:11:32

 Name    = John Smith
 Account =
 Bldg    =
 Dept    = CICS Toolkit Development
 Room    = Annex-1
 Addr1   = 't Zandt Labs
 Addr2   = The Netherlands
 Addr3   =
 Addr4   =









CQT074 -Command completed successfully
PF5=Update 9=User 11=Delete    Enter=Redisplay CLEAR=Main menu
```

図 *13. ALTUSER (WORKATTR SEGMENT)* パネル

Name
SYSOUT 情報が配布されるユーザーの名前を指定します。

Account
APPC/MVS 処理のアカウント番号を指定します。 RACF は最大 255 文字までの任意のストリングを受け入れますが、zSecure CICS Toolkit インターフェースで 使用できる最大文字数は 60 文字です。

Bldg
SYSOUT 情報が配布される事業所を指定します。

Dept
SYSOUT 情報が配布される部署を指定します。

Room
SYSOUT 情報が配布される部屋を指定します。

Addr1
アドレス行 1 は、SYSOUT 配布先の他のアドレス行を指定します。

Addr2
アドレス行 2 は、SYSOUT 配布先の他のアドレス行を指定します。

Addr3
アドレス行 3 は、SYSOUT 配布先の他のアドレス行を指定します。

Addr4
アドレス行 4 は、SYSOUT 配布先の他のアドレス行を指定します。

2. ユーザーの WORKATTR セグメントの情報を表示するには、Enter キーを押します。
3. この情報の一部またはすべてを変更するには、新規データを入力してから、PF5 を押します。
   エラーがある場合には、その問題を示すエラー・メッセージが表示されます。フィールドをブランクに設定すると、そのパラメーターはユーザーの WORKATTR セグメントから削除されます。

   ユーザーの WORKATTR セグメントを変更するときには、これらのフィールドの大/小文字が正しいことを確実にしてください。インストール済み環境で、これらのフィールドに大/小文字混合を使用する必要がある場合、WORKATTR セグメントをまったく更新しないか、または端末で大/小文字混合を使用するようにします。
4. WORKATTR セグメントを削除するには、PF11 を押します。

   注 : WORKATTR セグメントを削除しても、通常は、ユーザーがシステム・サービスを使用する権限に影響を与えることはありません。

グループへのユーザーまたはグループの 接続 (CONNECT コマンド)

CONNECT コマンドを使用して、グループにユーザーまたはグループを 接続します。

このタスクについて

ユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.CONN) およびターゲット・グループ (CONN.*grpname*) に対するアクセス権限を持っている必要があります。

手順

1. CONNECT コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。
2. ユーザーをグループに接続するには、指示されているように、ユーザーおよびグループ名を入力して PF05 を押します。
   ユーザーまたはグループ名が無効であるなどのエラーがある場合には、エラー・メッセージがその問題を示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                    CONNECT                     Time = 11:14:03

            Userid              Group
Connect  =             Group =             Authority = U    Owner = BCSCGB1

Special  = N   Operations = N     Revokedt =       Resumedt =









CQT016 -Enter userid and group name
PF5=Update ENTER=Redisplay CLEAR=Main menu
```

図 *14. CONNECT* パネル

AUTHORITY
デフォルトで U (使用) に設定されますが、C (作成)、N (接続)、または J (結合) に設定することもできます。

SPECIAL
ユーザーにグループ SPECIAL 属性が必要な場合には、Y を指定します。

OPERATIONS
ユーザーにグループ OPERATIONS 属性が必要な場合には、Y を指定します。

OWNER
デフォルトでは、このコマンドを実行するユーザーの ID に設定されますが、任意の有効なユーザー ID またはグループを入力することもできます。

REVOKEDT
ユーザーをグループに接続させない日付 (YYDDD) です。現在日付を指定すると、接続は即時に取り消されます。この場合、「RESUMEDT」の値は無視され、「RESUMEDT」と「REVOKEDT」の両方がリセットされます。 特殊値 00000 (5 つのゼロ) を使用して、既存の「REVOKEDT」を削除することもできます。このフィールドをブランクまたは空に設定すると、現行値がそのまま維持されます。

RESUMEDT
ユーザーがグループに接続できる日付 (YYDDD) です。 現在日付を指定すると、接続は即時に再開されます。この場合、「REVOKEDT」の値は無視され、「RESUMEDT」と「REVOKEDT」の両方がリセ

ットされます。 特殊値 00000 (5 つのゼロ) を使用して、既存の「RESUMEDT」を削除することもできます。このフィールドをブランクまたは空に設定すると、現行値がそのまま維持されます。

CSDATA フィールドの管理 (CSDATA コマンド)

CSDATA コマンドを使用して、CSDATA フィールドをリスト、追加、更新、または削除することができます。CSDATA フィールドは USER および GROUP に使用できます。z/OS 2.4 以降、CSDATA フィールドは、DATASET および一般リソース・プロファイルにも使用できます。

このタスクについて

ユーザーには、zSecure CICS Toolkit コマンド (TOOLKIT.CSDL)、指定されたクラスおよびプロファイル (CSDx.*owner*)、ならびに CSDATA 名 (CSDN.*csdata-name*) に対するアクセス権限が必要です。

クラス	有効範囲の許可
USER	CSDU.*owner*
GROUP	CSDG.*owner*
DATASET	CSDD.*owner*
一般リソース	CSDR.*owner*

ADD、UPDATE、および DELETE サブ関数には、対応するコマンド・プロファイルへのアクセス権限が必要です。システム SPECIAL またはプロファイル TOOLKIT.SPEC へのアクセス権限があるユーザーには、特定のサブ関数許可は不要です。

関数	許可で使用する TOOLKIT
List	TOOLKIT.CSDL
Add	TOOLKIT.CSDA
Update	TOOLKIT.CSDA
Delete	TOOLKIT.CSDD

手順

1. CSDATA コマンドにアクセスするには、指定されている PF キーを押すか、メイン RTMM メニューで番号を入力します。

```
 Termid = CP03           IBM Security zSecure CICS Toolkit       Date = 2019/324
 Userid = BCSCGB1                Custom Data Fields              Time = 05:05:52

 Fill in Profile and ENTER. For Add, fill in fields, select A and PF5
 _ Class = ________ Profile = ________________________________________________
                    Type =    * (G/*)
   Name =  ________ Value = ________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_____________________________________________|<===
   Name     Value   (Use S/L and ENTER for details, or D and PF5 for delete)
 -
 -
 -
 -
 -
 -
 -
 -
 -
 -
 CQT200 -Enter class and profile
 PF5=Update 8=Down ENTER=List CLEAR=Main menu
```

図 *15. CSDATA* メインパネル

2. プロファイルの CSDATA を表示するには、リソース・クラスとプロファイルを入力し、**Enter** キーを押します。

   プロファイルが完全修飾総称プロファイルである場合、タイプ・フィールドを使用してそれを指定する必要があります。

   - パネルの最下部に、CSDATA 名と、それぞれに対応する値の最初の 64 文字が表示されます。
   - CSDATA 名がパネルに表示しきれていない場合は、**PF8** を押してスクロールダウンします。
   - 切り捨てられた CSDATA 値の表示される文字を増やすには、CSDATA 名/値の前に S (または L) コマンドを入力して、**Enter** キーを押します。
   - CSDATA 値が 255 文字より長い場合、詳細パネルには、最初の 255 文字のみが表示され、切り捨て警告が発行されます。

```
 Termid = CP03           IBM Security zSecure CICS Toolkit       Date = 2019/324
 Userid = BCSCGB1                Custom Data Fields              Time = 05:05:52

   Class = USER     Profile =
BCSCGB3_____________________________________________
                    Type =    * (G/D/*)
   Name =  EMPNUM  Value =
788000001___________________________________________

_______________________________________________________________________________

_______________________________________________________________________________

_____________________________________________ |<===









 PF5=Update 11=Delete ENTER=Refresh CLEAR=Back
```

図 *16. CSDATA* 詳細表示パネル

3. CSDATA をプロファイルに追加するには、クラス、プロファイル、*csdata-name* および *csdata-value* を CSDATA メインパネルに入力します。次に「クラス」の前にあるフィールドに A と入力して、**PF05** を押します。

   このコマンド・フィールドで D または U を使用して CSDATA フィールドを削除する場合、または更新する場合にも、これと同じ方法を使用できます。D コマンドの場合、フィールド値は無視されます。46 ページの『4』 および 46 ページの『5』 で説明する方法はシンプルであり、エラーが起こりにくいため、この方法をお勧めします。
4. 表示された CSDATA 名と値の対を 1 つ削除するには、D、L、または S のいずれかの行コマンドを使用します。
   - CSDATA メインパネルで、目的の CSDATA の前に D 行コマンドを入力し、**PF05** を押します。
   - CSDATA メインパネルで、S または L 行コマンドを入力して CSDATA 値を表示し、**PF11** を押します。
5. 既存の CSDATA 値を更新するには、リストされた CSDATA 名の前に S (または L) 行コマンドを入力して、詳細パネルを表示します。詳細パネルで、値を新しい値で上書きし、**PF05** を押します。

   新しい CSDATA 値または更新された CSDATA 値を入力すると、zSecure CICS Toolkit は、CSDATA フィールドの最大長のみを検査します。最小または最大の数値などの他の特性は検査されません。ユーザーが有効な値を指定する必要があります。無効な 16 進文字はゼロで置き換えられます。

データ・セットの削除 (DELETE DATASET コマンド)

DELETE DATASET コマンドを使用してデータ・セット・プロファイルをシステムから削除します。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.DELD) に対するアクセス権限と、データ・セット・プロファイル名の高位修飾子 (DELD.hlq) に対するアクセス権限を持っている必要があります。 ユーザーが DELD.hlq に対するアクセス権限を持っていない場合は、標準の RACF 権限検査が使用されます。ユーザーによる削除が許可されるデータ・セット・プロファイルについては、「RACF コマンド言語解説書」を参照してください。

手順

DELETE DATASET コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                                                Time = 11:14:18

               Dsname
    Delete   =                                          Generic = Y









CQT144 -Enter dataset profile to be deleted. Specify Y if Generic, N if not
PF5=Update ENTER=Redisplay CLEAR=Main menu
```

図 *17. DELETE DATASET* パネル

ユーザー・プロファイルの削除

DELETE コマンドを使用してユーザー・プロファイルをシステムから削除します。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.DELU) に対するアクセス権限と、対象ユーザーのデフォルト・グループ (DELU.dfltgrp) に対するアクセス権限を持っている必要があります。

ユーザー・プロファイルを削除する前に、デフォルト・グループを除くすべての接続先グループから、そのユーザー・プロファイルを削除する必要があります。このユーザー ID を高位修飾子として持つデータ・セット・プロファイルは存在できなくなります。

zSecure CICS Toolkit は、グループ接続について検査しますが、データ・セット・プロファイルについては検査しません。

手順

DELETE コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                                                Time = 11:14:35

                Userid
    Delete   =




PF5=Update ENTER=Redisplay CLEAR=Main menu
```

図 *18. DELETE USER* パネル

1 つ以上のデータ・セットのプロファイルのリスト (LISTDSET コマンド)

LISTDSET コマンドを使用して特定のデータ・セットまたは複数のデータ・セットのプロファイルをリストします。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.LDSD) に対するアクセス権限を持っている必要があります。

手順

1. **LISTDSET** コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                  Listdset =                    Time = 11:14:47
G , D OR * *    ___________________________________________

Owner = ******** Cre = ***** Last ref = ***** Last chg = ***** Uacc = *******

Alter acc = ****** Cntrl acc = ****** Updte acc = ****** Read  acc = ******

Group ds = * WARN = * Cre grp  = ******** Dataset type = **** Level = ***

Audit = * Aud Succ = * Aud Fail = * Glbl audit = * Gaud Succ = * Gaud Fail = *

Secl = *** Numctgy = **** NumPgms = **** NumUsrs = ****



 ----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----
 ********************************************************************************
********************************************************************************
********************************************************************************
**************** |<===
 ----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

 PF1=Toggle 3=Chgopts 5=Userids 7=Programs 11=Search CLEAR=Main menu
```

図 *19. LISTDSET* パネル

LISTDSET
表示するデータ・セットの ID (**listuser** を実行する場合)。 検索を実行している場合には、このフィールドをバイパスできます。または、検索基準の一部として、任意の位置に任意の文字を入力することもできます。

注 : 通常の **listdset** を実行する場合、以降にリストするフィールドは入力として使用されません。これらのフィールドは、検索 (PF11) を行う場合にのみ、入力として使用されます。

G、D、または * を使用して、汎用 (G) または個別 (D) のプロファイル、あるいは両方 (*) のタイプのプロファイルを検索できます。

OWNER
データ・セットの所有者として定義されているユーザーまたはグループ。

CRE
データ・セットが作成された日付。フォーマットは YYDDD です。

LAST REF
データ・セットが最後に参照された日付。フォーマットは YYDDD です。

LAST CHG
データ・セットが最後に更新された日付。フォーマットは YYDDD です。

UACC
データ・セットの汎用アクセス。このフィールドの値は、*ALTER*、*CONTROL*、*UPDATE*、*READ*、または *NONE* です。

ALTER ACC
データ・セットが、*ALTER* を使用してアクセスされた回数。

CNTRL ACC
データ・セットが、CONTROL を使用してアクセスされた回数。

UPDTE ACC
データ・セットが、UPDATE を使用してアクセスされた回数。

READ ACC
データ・セットが、READ を使用してアクセスされた回数。

GROUP DS
このフィールドの値は、*Y* または *N* です。

WARN
データ・セットが警告モードであるかどうかを示します。このフィールドの値は、*Y* または *N* です。

CRE GROUP
このデータ・セットを作成したユーザーの現行接続グループ。

DATASET TYPE
このフィールドは、データ・セットのタイプを識別します。このフィールドの最初の 2 文字は、データ・セット・プロファイルが VSAM (*VS*) であるか、非 VSAM (*NV*) であるかを示します。3 番目の文字は、プロファイルがモデル・プロファイルであるか (*M*)、そうではないか (*N*) を示します。 最後の 4 番目の文字は、プロファイルがテープ・データ・セット用であるか (*T*)、そうではないか (*N*) を示します。

LEVEL
データ・セットのレベル標識。このフィールドは数値フィールドです。

AUDIT
データ・セットの監査フラグを指定します。設定できる値は、*A* (すべてのアクセスを監査)、*S* (成功アクセスを監査)、*F* (失敗を監査)、または *N* (監査なし) です。

AUD SUCC
監査の成功フラグです。設定できる値は、*R* (読み取り成功を監査)、*U* (更新成功を監査)、*C* (成功した制御アクセスを監査)、または *A* (成功した変更アクセスを監査) です。

AUD FAIL
監査の失敗フラグです。設定できる値は、*R* (読み取り失敗を監査)、*U* (更新失敗を監査)、*C* (失敗した制御アクセスを監査)、または *A* (失敗した変更アクセスを監査) です。

GLBL AUDIT
AUDITOR 属性を持つユーザーによって指定されたグローバル監査オプションです。設定できる値は、*A* (すべてのアクセスを監査)、*S* (成功アクセスを監査)、*F* (失敗を監査)、または *N* (監査なし) です。

GAUD SUCC
グローバル監査の成功フラグです。設定できる値は、*R* (読み取り成功を監査)、*U* (更新成功を監査)、*C* (成功した制御アクセスを監査)、または *A* (成功した変更アクセスを監査) です。

GAUD FAIL
グローバル監査の失敗フラグです。設定できる値は、*R* (読み取り失敗を監査)、*U* (更新失敗を監査)、*C* (失敗した制御アクセスを監査)、または *A* (失敗した変更アクセスを監査) です。

SECL
データ・セットのセキュリティー・レベル。このフィールドは数値フィールドです。

NUMCTGY
データ・セットが属するセキュリティー・カテゴリーの数。

NUMPGMS
データ・セットへのアクセスが許可されているプログラムの数。

NUMUSRS
データ・セットへのアクセスが許可されているユーザーとグループの数。

INSTALLATION DATA
データ・セットのデータ・フィールドに含まれる情報。このインストール・データは最大 255 文字です。

2. PF05 を押すと、このデータ・セット・プロファイルのアクセス・リスト (ユーザーおよびグループ) が表示されます。
3. PF07 を押すと、条件付きアクセス・リストに含まれるプログラムが表示されます。
4. PF01 を押すと、表示が切り替わり (検索を実行している場合)、基準と一致するすべてのデータ・セットが表示されます。
5. PF03 を押すと、フィールドがクリアされます。検索または LISTDSET の新しい基準を入力します。

LISTDSET の表示例

条件付きアクセス・リストに含まれるプログラムを表示できます。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                  Listdset =                    Time = 11:15:07
G , D OR * G    SYS1.**

Owner = SYS1     Cre = 05033 Last ref = 05033 Last chg = 05033 Uacc = READ

Alter acc = 000000 Cntrl acc = 000000 Updte acc = 000000 Read  acc = 000000

Group ds = Y WARN = N Cre grp  = SYS1     Dataset type = NVNN Level = 000

Audit = F Aud Succ = R Aud Fail = R Glbl audit = N Gaud Succ = R Gaud Fail = R

Secl = *** Numctgy = 0000 NumPgms = 0000 NumUsrs = 0003


----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----


                |<===
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

PF1=Toggle 3=Chgopts 5=Userids 7=Programs 11=Search CLEAR=Main menu
```

図 *20. LISTDSET* 表示パネル

ここでは、以下のいずれかを選択して実行できます。

- アクセス・リストのエントリーを表示する (PF05 の「ユーザー ID」)。
- 条件付きアクセス・リストのエントリーを表示する (PF07 の「Programs」)。
- 検索またはリスト・オプションを変更する (PF03)。
- メインメニューに戻る (CLEAR)
- 検索を実行している場合、基準と一致するすべてのデータ・セットを表示する (PF01)。

LISTDSET パネルの切り替え

検索を行っているときにパネルを切り替えることで、条件を満たすすべてのデータ・セットを表示することができます。

手順

- 検索を実行するには、PF01 を押します。
  基準に一致するすべてのデータ・セットが表示されます。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                  Listdset =                    Time = 11:21:14
                SYS1.ZTKTEST
G SYSAPPL.**
G SYS1.BRODCAST
G SYS1.MAN*.**
G SYS1.RACF*.**
G SYS1.ZTKTEST
G SYS1.**
D SYS1.ZTKTEST









CQT064 -End of entries matching this criteria
CQT015 -PF1=Toggle 3=Chgopts ENTER=Next CLEAR=Main Menu
```

図 *21. LISTDSET* 切り替えパネル

- 実行するタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - メインメニューに戻る (CLEAR)
  - このパネルにデータ・セットが表示しきれていない場合、次のパネルを表示する (ENTER)。
  - 任意の ID で LISTDSET を実行する場合、「LISTDSET」フィールドに ID を入力して PF01 を押す。

権限を持つユーザー、それらのユーザーのアクセス権限、およびアクセス・カウントの表示 (LISTDSET USERIDS)

LISTDSET のユーザー ID オプションを使用すると、そのデータ・セットへのアクセスが許可されているユーザーと、それぞれのユーザーのアクセス権限およびアクセス・カウントが表示されます。

手順

- LISTDSET パネルで PF05 を押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                  Listdset =   (USERIDS)        Time = 11:22:41
                SYSAPPL.**
STCUSER /A/00000     C2POLICE/U/00000     BCSCGB1 /A/00000









PF3=Chgopts 5=Userids 7=Programs 8=Down 9=Datasets ENTER=Next CLR=Main menu
```

図 *22. LISTDSET USERIDS* パネル

- 実行したいタスクの PF キーを以下から選択します。

- 検索またはリスト・オプションを変更する (PF03)。
- このデータ・セットにアクセスできるプログラムを表示する (PF07)。
- LISTDSET パネルに戻る (PF09)。
- 検索を実行している場合、次のデータ・セットを表示する (ENTER)。
- メインメニューに戻る (CLEAR)。

プログラム/ユーザー ID の組み合わせの表示 (LISTDSET Programs)

LISTDSET パネルを使用すると、そのデータ・セットへのアクセスが許可されているプログラム/ユーザー ID の組み合わせと、アクセス権限を表示できます。

手順

- LISTDSET パネルで PF07 を押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                  Listdset =   (PROGRAMS)       Time = 11:23:23
                 SYS1.RACF*.**
    C2RCARLA/*       /R









PF3=Chgopts 5=Userids 7=Programs 8=Down 9=Datasets ENTER=Next CLR=Main menu
```

図 *23. LISTDSET* プログラム

- 実行したいタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - アクセス・リストのエントリーを表示する (PF05)。
  - LISTDSET パネルに戻る (PF09)。
  - 検索を実行している場合は、次のデータ・セットを表示する (Enter)。
  - メインメニューに戻る (CLEAR)。

1 つ以上のグループのプロファイルのリスト (LISTGROUP コマンド)

LISTGROUP コマンドを使用して特定のグループまたは複数のグループのプロファイルをリストします。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.LGRP) に対するアクセス権限、およびターゲット・グループ (LGRP.*grpname*) に対するアクセス権限を持っている必要があります。

手順

1. **LISTGROUP** コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                LISTGROUP = ********            Time = 11:23:38


 Supgroup = ******** Owner = ******** Univ = * Cre = ***** Uacc = *******

 Termuacc = * Number of subgroups = ***** Number of users = *****


             Model = ****************************************


 ----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----
 ********************************************************************************
********************************************************************************
********************************************************************************
**************** |<===
 ----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

 PF1=Toggle 3=Chgopts 4=UserD 5=Users 6=Dfltu 7=Subgrps 11=Search CLR=Main menu
```

図 *24. LISTGROUP* パネル

LISTGROUP
表示するグループの ID (listgroup を実行する場合)。 検索を実行している場合には、このフィールドをバイパスできます。または、検索基準の一部として、任意の位置に任意の文字を入力することもできます。

注 : 通常の listgroup を実行する場合、以降にリストするフィールドは入力として使用されません。これらのフィールドは、検索 (PF11) を行う場合にのみ、入力として使用されます。

SUPGROUP
このグループの上位グループ。

OWNER
このグループの所有者として定義されているユーザーまたはグループ。

UNIV
汎用グループであるかどうかを示す標識。汎用グループに接続されているユーザーのリストには、グループ内で非標準の権限を持つユーザーのみが示されます。

CRE
このプロファイルが作成された日付。フォーマットは *YYDDD* です。

UACC
ユーザーがグループに接続されていない場合のグループに対するユーザーの権限。このフィールドの値は、JOIN、CONNECT、CREATE、USE、または NONE です。このフィールドを、RACF コマンドまたは zSecure CICS Toolkit を使用して設定することはできません。 固定グループ VSAMDSET を除くすべてのグループには、値 NONE を設定する必要があります。

TERMUACC
グループまたはユーザーに端末へのアクセスを明示的に許可する必要があるかどうかを指定します。このフィールドの値は、Y または N です。

NUMBER OF SUBGROUPS
このグループのサブグループの 数。このフィールドは数値フィールドです。

NUMBER OF USERS
このグループとの接続ユーザーの数。このフィールドは数値フィールドです。汎用グループの場合、これは、グループ内で非標準の権限を持つユーザーの数だけを反映します。

MODEL
新しい *groupname* データ・セットのモデルとして使用する、個別のデータ・セット・プロファイルの名前。このフィールドは英数字フィールドです。

INSTALLATION DATA
データ・セットのデータ・フィールドに含まれる情報。この情報は最大 255 文字です。

2. 特定のグループを入力してその ID を基準に LISTGROUP を実行することも、フィールドに検索基準として任意の文字を入力することもできます。
   - 検索基準を入力した場合には、**PF11** を押して検索を開始します。
   - 通常の LISTGROUP を実行する場合には、グループ名を入力した後に **Enter** キーを押して、LISTGROUP パネルを開きます。
3. **PF04** を押すと、このグループに接続されているユーザーが、DELETEUSER オプションと併せて表示されます。
4. **PF05** を押すと、このグループに接続されているユーザーが表示されます。
5. **PF07** を押すと、サブグループが表示されます。
6. **PF01** を押すと表示が切り替わり (検索を実行している場合)、基準と一致するすべてのグループが表示されます。
7. **PF03** を押すと、フィールドがクリアされます。検索または LISTGROUP の新しい基準を入力します。

LISTGROUP の表示例

リストするグループを入力した場合、または検索を開始した場合には、このパネルが表示されます。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                LISTGROUP = SYSPROG             Time = 11:24:02


 Supgroup = SYS1     Owner = SYS1     Univ = N Cre = 05033 Uacc = NONE

 Termuacc = Y Number of subgroups = 00000 Number of users = 00003


              Model =


----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----
SYSTEM PROGRAMMERS

                |<===
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

PF1=Toggle 3=Chgopts 4=UserD 5=Users 6=Dfltu 7=Subgrps 11=Search CLR=Main menu
```

図 *25. LISTGROUP* 表示パネル

以下の操作を選択できます。

- ユーザーを表示する (PF05)。
- デフォルト・グループにも接続されているユーザーのみを表示する。
- サブグループを表示する (PF07)。
- 検索またはリスト・オプションを変更する (PF03)。
- メインメニューに戻る (CLEAR)
- 検索を実行している場合、基準と一致するすべてのグループを表示する (PF01)。

LISTGROUP パネルの切り替え

検索を行っているときに LISTGROUP パネルを切り替えることで、条件を満たすすべてのグループを表示することができます。

手順

- 検索を実行するには、**PF01** を押します。
  基準に一致するすべてのグループが表示されます。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1           LISTGROUP = SYSADMA                  Time = 11:24:21

    SYSADMA  SYSAPPL  SYSAUDIT SYSCTLG  SYSOPRA  SYSPROG  SYS1









CQT064 -End of entries matching this criteria
CQT015 -PF1=Toggle 3=Chgopts ENTER=Next CLEAR=Main Menu
```

図 *26. LISTGROUP* 切り替えパネル

- 実行したいタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - メインメニューに戻る (CLEAR)
  - このパネルにグループ名が表示しきれていない場合、次のパネルを表示する (**Enter**)。

  ある名前に対して LISTGROUP を実行するには、「LISTGROUP」フィールドに名前を入力して、**PF01** を押します。

グループのユーザーのリスト (LISTGROUP コマンド、USERIDS オプション)

LISTGROUP コマンドと USERIDS オプションを使用して、グループに接続されたすべてのユーザーをリストすることができます。

手順

- LISTGROUP パネルで **PF05** を押してグループに接続されているすべてのユーザーを表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1           LISTGROUP = SYSPROG  (USERIDS)       Time = 11:24:47

BCSCGB1  BCSCWN1  BCSCWN2









PF3=Chgopts 4=UserD 5=Users 6=Dfltu 8=Down 9=Grps ENTER=Next CLEAR=Main menu
```

図 *27. LISTGROUP USERIDS* パネル

- 実行したいタスクの PF キーを以下から選択します。

- 検索またはリスト・オプションを変更する (PF03)。
- 代替ユーザー表示に切り替える (PF04)。
- サブグループを表示する (PF07)。
- LISTGROUP パネルに戻る (PF09)。
- 検索を実行している場合、次のグループを表示する (ENTER)。
- メインメニューに戻る (CLEAR)

LISTGROUP からのユーザー ID の削除

グループに接続されたユーザー ID のリストから、1 つ以上のユーザー ID を削除することができます。

手順

- LISTGROUP パネルから **PF04** を押して、グループに接続されているすべてのユーザーおよび、その中のユーザーを削除するためのオプションを表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1           LISTGROUP = SYSPROG  (USERS LIST)    Time = 11:25:05

S  Userid   Name                 Created  Last signon

_ BCSCGB1  JOHN SMITH          05033    07094
_ BCSCWN1  ####################### 05033    03126
_ BCSCWN2  ####################### 05033    02338
_
_
_
_
_
_
_
_
_
_
_
_
_


PF3=Chgopts 5=Users 8=Down 9=Grps 11=Deluser ENTER=Next CLEAR=Main menu
```

図 *28. LISTGROUP* ユーザー *ID* 削除パネル

- 実行したいタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - ユーザー表示に切り替える (PF05)。
  - サブグループを表示する (PF07)。
  - LISTGROUP パネルに戻る (PF09)。
  - 検索を実行している場合、次のグループを表示する (ENTER)。
  - メインメニューに戻る (CLEAR)。
- 選択したユーザーを削除するには、削除するユーザー・プロファイルの隣に D を入力してから、**PF11** を押します。

  ユーザー・プロファイルを削除する権限は、標準の zSecure CICS Toolkit DELUSER 権限で制御されます。

グループのサブグループのリスト

グループのすべてのサブグループをリストすることができます 。

手順

- LISTGROUP パネルで **PF07** を押してグループのすべてのサブグループを 表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1           LISTGROUP = SYS1     (GROUPS)        Time = 11:25:21

SYSCTLG  VSAMDSET TEST     OMVSGRP  IMWEB    EXTERNAL EMPLOYEE SPECIAL
DB2      DSN710   UUCPG    TTY      ADB210   ADCD     APS330   ASU
BPO110   CATALOG  CBC      CEE      CICSTS22 CICSTS23 CRMB     CSQ520
CSQ530   CSQ531   C2RSERVG DCF140   DIT130   DSNA     EOY      EUV
FAN130   FAN140   FMN410   FON210   GDDM     GIM      GLD      GLDGRP
HFS      HLA      ICQ      IGY310   IOE      ISF      ISP      P390
QMFA     QMF710   REVOKE   SCPTEST  SMTP     STCGRP   SYSADMA  SYSAPPL
SYSAUDIT SYSOPRA  SYSPROG  USER     USERCAT  #EMPLOY  #READ    AUT220
NETV     CDS      CIM      CMX      CSF      ECN      EPH      EUVF
GSK      ICA      IMO      IMW      ING      NFS      BIP210   BIP501
HPJ200   IEL330   IGY330   IXM140   JVA130   JVA140   AUT230   IXM160
NETV510  IXGLOGR  FMN510   IOA      EQA510   IPT110   FFST     AOP
IDI510   ITP110   OMVS     BCSC     ZTKQA    SLDMVSS  CRMA

PF3=Chgopts 4=UserD 5=Users 6=Dfltu 8=Down 9=Grps ENTER=Next CLEAR=Main menu
```

図 *29. LISTGROUP (サブグループ) パネル*

- 実行したいタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - 代替ユーザー表示に切り替える (PF04)。
  - ユーザーを表示する (PF05)。
  - デフォルト・グループにも接続されているユーザーを表示する (PF06)。
  - LISTGROUP パネルに戻る (PF09)。
  - 検索を実行している場合、次のグループを表示する (ENTER)。
  - メインメニューに戻る (CLEAR)

ユーザー ID のプロファイルのリスト (LISTUSER コマンド)

LISTUSER コマンドを使用して、特定のユーザー ID のプロファイルをリストすることができます。

このタスクについて

FUNCTION

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.LUSR) に対するアクセス権限と、対象ユーザーのデフォルト・グループ (LUSR.dfltgrp) に対するアクセス権限を持っている必要があります。

手順

1. LISTUSER コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1               LISTUSER = ********              Time = 11:25:41

 Name = ********************  Owner = ******** Password = ******** Cre = *****

 Dfltgrp = ********  Authority = *******  Uacc = *******  Classcnt = ****

 Special = * Operations = * Auditor = * Restr = * Grpacc = * Adsp = *

 Protected = * Uaudit = * Revoke = * Revokedt = ***** Resumedt = *****

 Lastacc = ************** Passdate = ***** Passint = *** PwTry = ** Secl = ***

 SMTWTFS From Till  Pwdgen = ***  Pwdcnt = ***  NumCtgy = ****  NumGrp = ****
 ******* **** ****  Model = ******************************************

----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----
 ********************************************************************************
********************************************************************************
********************************************************************************
**************** |<===
 ----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

 PF1=Toggle 3=Chgopts 5=Ctgy 6=Segments 7=Groups 11=Search CLEAR=Main menu
```

図 *30. LISTUSER* パネル

LISTUSER
表示するユーザーの ID (listuser を実行する場合)。 検索を実行している場合には、このフィールドをバイパスできます。または、検索基準の一部として、任意の位置に任意の文字を入力することもできます。

注 : 通常の listuser を実行する場合、以降にリストするフィールドは入力として使用されません。これらのフィールドは、検索 (PF11) を行う場合にのみ、入力として使用されます。

NAME
ユーザー名。 最大 20 文字の英数字。

名前または名前の一部を検索する場合には、「名前」フィールド内の任意の場所で、以下のフォーマットを使用します。

SMITH を検索する場合、「名前」フィールド内の任意の場所に *<>SMITH* と入力します。 これにより、「名前」フィールドに *SMITH* の文字が含まれるすべてのプロファイルが返されます。*<>* は zSecure CICS Toolkit に対し、この基準がワイルドカード文字「*」(使用している場合) とは異なるフィールド検索基準であることを指示します。

OWNER
ユーザーの所有者として定義されているユーザーまたはグループ。

PASSWORD
使用しません。

CRE
このプロファイルが作成された日付。フォーマットは YYDDD です。

DFLTGRP
ユーザーのデフォルト・グループの名前。

AUTHORITY
これは、デフォルト・グループ内でのユーザー権限です。このフィールドに使用できるエントリーは、*ASORGGAT* です。 サブフィールドの意味は、*A* は ADSP を表し、*GA* は GROUP AUDITOR を表し、*T* は端末アクセス権限が必要であることを表します。

UACC
デフォルト・グループに対するユーザーの汎用アクセス権限。このフィールドの値は、*ALTER*、*CONTROL*、*UPDATE*、*READ*、または *NONE* です。

CLASSCNT
ユーザーがプロファイルの定義を許可されているクラスの数。

SPECIAL
ユーザーが、SPECIAL 属性を持つかどうかを示す。 このフィールドの値は、Y または N です。

OPERATIONS
ユーザーが、OPERATIONS 属性を持つかどうかを示す。 このフィールドの値は、Y または N です。

AUDITOR
ユーザーが、AUDITOR 属性を持つかどうかを示す。 このフィールドの値は、Y または N です。

RESTR
このフィールドは、このユーザーに UACC、GAC、および ID(*) が適用されるかどうかを示します。このフィールドの値は、Y または N です。

GRPACC
このユーザーが作成するグループ・データ・セットに、グループ内の他のユーザーがアクセスできるかどうかを示します。このフィールドの値は、Y または N です。

ADSP
このユーザーが作成する新規データ・セットが自動的に個別プロファイルによって保護されるかどうかを示します。このフィールドの値は c です。

PROTECTED
このフィールドは、パスワードの指定でユーザー ID を使用できるかどうかを示します。保護ユーザー ID は、代理によってのみ、伝搬、開始、または使用できます。このフィールドの値は、Y または N です。

UAUDIT
ユーザーに対して実行されるすべての RACHECK および RACDEF をログに記録できるかどうかを示します。 このフィールドの値は、Y または N です。

REVOKE
ユーザーに REVOKE 属性が設定されているかどうかを示します。このフィールドの値は、Y または N です。

REVOKEDT
ユーザーが取り消される日付。フォーマットは *YYDDD* です。

RESUMEDT
ユーザーが再開される日付。フォーマットは *YYDDD* です。

LASTACC
ユーザーが RACINIT を使用して最後にシステムにアクセスした日時。フォーマットは *YYDDD/HH:MM:SS* です。ユーザーがログオンしたことがない場合、このフィールドの最初の位置に ? が含まれます。

PASSDATE
ユーザー・パスワードが最後に変更された日付。フォーマットは *YYDDD* です。または、フィールドがリセットされている場合はゼロになります。

PASSINT
ユーザーのパスワードが有効になっている間隔。このフィールドは数値フィールドです。

PWTRY
このユーザーのパスワード試行失敗回数。このフィールドは数値フィールドです。

SECL
ユーザーのセキュリティー・レベル。このフィールドは数値フィールドです。

SMTWTFS
ユーザーがログオンできる曜日。「Y」はユーザーがその曜日にログオンできることを示します。「N」は、その曜日にユーザーのログオンが制限されることを示します。

FROM
ユーザーがログオンできる時間が制限されている場合、「FROM」はユーザーがログオンできる時間帯の開始時刻です。フォーマットは *HHMM* です。時間による制限がない場合、「FROM」と「TILL」は両方とも *0000* になります。

TILL
ユーザーがシステムにログオンできる最終時刻。フォーマットは *HHMM* です。

PWDGEN
ユーザーの現在のパスワードの世代番号。このフィールドは数値フィールドです。

PWDCNT
このユーザーの旧パスワードの数。このフィールドは数値フィールドです。

NUMCTGY
ユーザーがアクセスできるセキュリティー・カテゴリーの数。このフィールドは数値フィールドです。

MODEL
このユーザーのデータ・セット・プロファイルのモデル。このフィールドは英数字フィールドです。

INSTALLATION DATA
ユーザーのデータ・フィールドに含まれる情報。この情報は最大 255 文字です。

2. 特定のユーザー ID を入力して、そのユーザーについて LISTUSER を実行することも、フィールドに検索基準として任意の文字を入力することもできます。
   - 検索基準を入力した場合には、PF11 を押して検索を開始します。
   - 通常の LISTUSER を実行するには、ユーザー ID を入力して **Enter** キーを押します。
3. PF05 を押すと、このユーザーのカテゴリーが表示されます。
4. PF07 を押すと、グループが表示されます。
5. PF01 を押すと表示が切り替わり (検索を実行している場合)、基準と一致するすべてのユーザーが表示されます。
6. PF03 を押すと、フィールドがクリアされます。検索または LISTUSER の新しい基準を入力します。

LISTUSER の表示例

この例は、ユーザー ID を指定して **Enter** を押した場合、または他の異なる基準を入力した後に **PF11** を押して検索を開始した場合の表示です。

注 : 完全なユーザー ID を入力して **PF11** をクリックした場合は、**Enter** キーを押すのと同じ結果となります。これは指定されたユーザー ID には 1 つのプロファイルしかないためです。

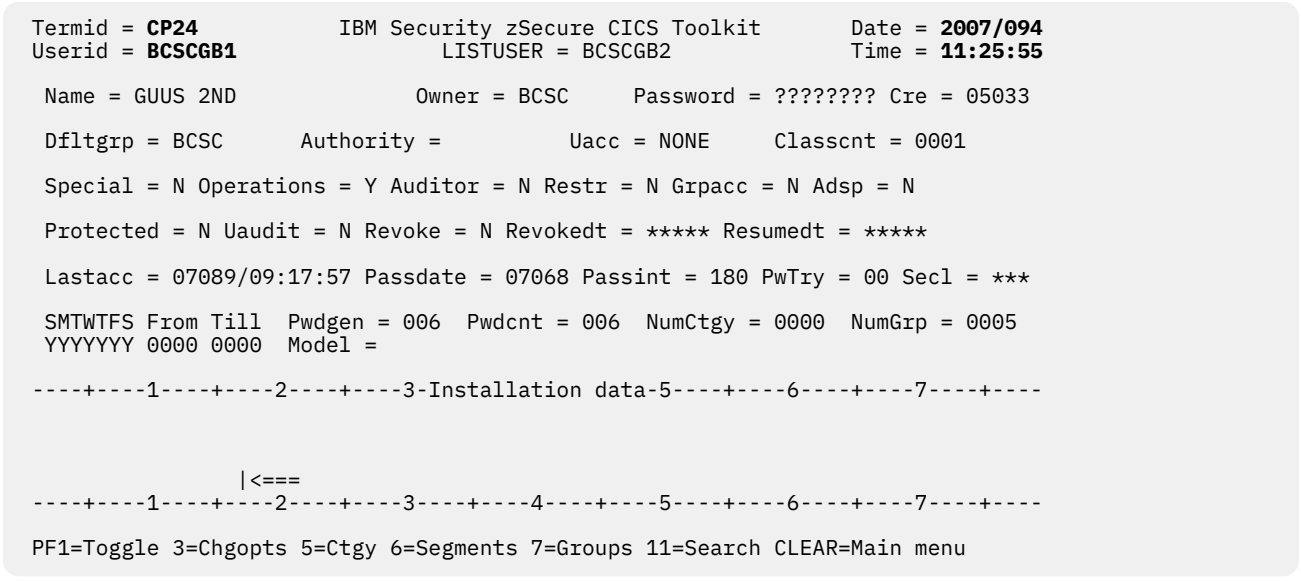

図 *31. LISTUSER* 表示パネル

この時点で、以下の操作を選択できます。

- カテゴリーを表示する (PF05)。
- グループを表示する (PF11)。
- 検索またはリスト・オプションを変更する (PF03)。
- メインメニューに戻る (CLEAR)

- 検索を実行している場合、基準と一致するすべてのユーザーを表示する (PF01)。

LISTUSER パネルの切り替え

LISTUSER パネルを使用して、入力した基準を満たすすべてのユーザーをリストすることができます。

手順

- 検索を実行するには、PF01 を押します。
  基準に一致するすべてのユーザーが表示されます。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1            LISTUSER = B8FU0142                 Time = 11:32:50

    B8FTEST  B8FU0000 B8FU0001 B8FU0002 B8FU0003 B8FU0004 B8FU0005 B8FU0006
    B8FU0007 B8FU0008 B8FU0009 B8FU0010 B8FU0011 B8FU0012 B8FU0013 B8FU0014
    B8FU0015 B8FU0016 B8FU0017 B8FU0018 B8FU0019 B8FU0020 B8FU0021 B8FU0022
    B8FU0023 B8FU0024 B8FU0025 B8FU0026 B8FU0027 B8FU0028 B8FU0029 B8FU0030
    B8FU0031 B8FU0032 B8FU0033 B8FU0034 B8FU0035 B8FU0036 B8FU0037 B8FU0038
    B8FU0039 B8FU0040 B8FU0041 B8FU0042 B8FU0043 B8FU0044 B8FU0045 B8FU0046
    B8FU0047 B8FU0048 B8FU0049 B8FU0050 B8FU0051 B8FU0052 B8FU0053 B8FU0054
    B8FU0055 B8FU0056 B8FU0057 B8FU0058 B8FU0059 B8FU0060 B8FU0061 B8FU0062
    B8FU0063 B8FU0064 B8FU0065 B8FU0066 B8FU0067 B8FU0068 B8FU0069 B8FU0070
    B8FU0071 B8FU0072 B8FU0073 B8FU0074 B8FU0075 B8FU0076 B8FU0077 B8FU0078
    B8FU0079 B8FU0080 B8FU0081 B8FU0082 B8FU0083 B8FU0084 B8FU0085 B8FU0086
    B8FU0087 B8FU0088 B8FU0089 B8FU0090 B8FU0091 B8FU0092 B8FU0093 B8FU0094
    B8FU0095 B8FU0096 B8FU0097 B8FU0098 B8FU0099 B8FU0100 B8FU0101 B8FU0102
    B8FU0103 B8FU0104 B8FU0105 B8FU0106 B8FU0107 B8FU0108 B8FU0109 B8FU0110
    B8FU0111 B8FU0112 B8FU0113 B8FU0114 B8FU0115 B8FU0116 B8FU0117 B8FU0118
    B8FU0119 B8FU0120 B8FU0121 B8FU0122 B8FU0123 B8FU0124 B8FU0125 B8FU0126
    B8FU0127 B8FU0128 B8FU0129 B8FU0130 B8FU0131 B8FU0132 B8FU0133 B8FU0134
    B8FU0135 B8FU0136 B8FU0137 B8FU0138 B8FU0139 B8FU0140 B8FU0141 B8FU0142


CQT015 -PF1=Toggle 3=Chgopts ENTER=Next CLEAR=Main Menu
```

図 *32. LISTUSER* 切り替えパネル

- 実行したいタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - メインメニューに戻る (CLEAR)
  - このパネルにユーザー ID が表示しきれていない場合、次のパネルを表示する (ENTER)。

  任意の ID で LISTUSER を実行する場合、「**LISTUSER**」フィールドに ID を入力して **PF01** を押す。

ユーザー ID のグループのリスト (LISTUSER コマンド、GROUPS オプション)

LISTUSER コマンドと Groups オプションを使用して、ユーザー ID の接続先グループを表示できます。

手順

- LISTUSER パネルで **PF07** を押して、ユーザーが接続されているグループを表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1            LISTUSER = BCSCGB1  (Groups)        Time = 11:33:30

BCSC     #READ    P390     SYSAUDIT SYSPROG  CRMA     CRMB




PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Down 9=User ENTER=Next CLEAR=Main menu
```

図 *33. LISTUSER GROUPS* パネル

- 実行したいタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - このユーザーのカテゴリーを表示する (PF05)。
  - LISTUSER パネルに戻る (PF09)。
  - 検索を実行している場合、次のユーザーを表示する。
  - メインメニューに戻る (CLEAR)

ユーザー ID のカテゴリーのリスト (LISTUSER コマンド、Categories オプション)

LISTUSER コマンドと Categories オプションを使用して、ユーザー ID の接続先カテゴリーをリストすることができます。

手順

- LISTUSER パネルで PF05 を押して、ユーザーが接続されているカテゴリーを表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1            LISTUSER = BCSCGB1  (Categories)    Time = 11:34:40

    00000001




PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Down 9=User ENTER=Next CLEAR=Main menu
```

図 *34. LISTUSER (*カテゴリー*)* パネル

- 実行したいタスクの PF キーを以下から選択します。

– 検索またはリスト・オプションを変更する (PF03)。
– このユーザーのグループを表示する (PF07)。
– LISTUSER パネルに戻る (PF09)。
– 検索を実行している場合、次のユーザーを表示する。
– メインメニューに戻る (CLEAR)

ユーザー ID の TSO セグメントおよび CICS セグメントのリスト (LISTUSER コマンド、Segments オプション)

LISTUSER コマンドと Segments オプションを使用して、ユーザー ID の TSO セグメントおよび CICS セグメントをリストすることができます。

手順

- LISTUSER パネルから **PF06** を押して、ユーザーの TSO セグメントおよび CICS セグメントを表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1            LISTUSER = BCSCGB2  (Segments-1)    Time = 11:34:54

TSO
 Acctnum = *
 Destid  =
 HClass  =            JClass  =            MsgClass=            SClass  =
 Size    = 0000000    Maxsize = 0000000    Seclabl =
 Proc    = ISPFPROC   Unit    =            Udata   = 0000

CICS
 OPIdent = 123
 OPPrty  = 123
 Timeout = 0000
 XRFSoff = NOFORCE
 OPClass =

 RSLKey  =
 TSLKey  =



PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Down 9=User ENTER=Next CLR=Main menu
```

図 *35. LISTUSER (*セグメント*)*

- **PF08** を押して OMVS セグメントおよび WORKATTR セグメントを表示します。
  もう一度 **PF08** を押すと、前のセグメントの表示にスクロールアップします。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1            LISTUSER = BCSCGB2  (Segments-2)    Time = 11:35:00

OMVS
 UID      = 0000002009
 Home     =
 Program  =
 ASSizeMax   =                          CPUTimeMax  =
 FileProcMax =                          MMapAreaMax =
 ProcUserMax =                          ThreadsMax  =
 MemLimit    =                          SHMemMax    =

WORKATTR
 Name    = JOHN SMITH
 Account =
 Bldg    =
 Dept    = CICS TOOLKIT DEVELOPMENT
 Room    = ANNEX-1
 Addr1   = 'T ZANDT LABS
 Addr2   = THE NETHERLANDS
 Addr3   =
 Addr4   =

PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Up   9=User ENTER=Next CLR=Main menu
```

図 *36. LISTUSER: OMVS* および *WORKATTR* パネル

- 実行したいタスクの PF キーを以下から選択します。
  - 検索またはリスト・オプションを変更する (PF03)。
  - このユーザーのグループを表示する (PF07)。
  - LISTUSER パネルに戻る (PF09)。
  - 検索を実行している場合、次のユーザーを表示する。
  - メインメニューに戻る (CLEAR)

リソースに対するアクセス権限の付与または除去 (PERMIT コマンド)

PERMIT コマンドを使用して、リソースに対するアクセス権限を付与または除去できます。

このタスクについて

リソースは、以下のクラスに含まれる場合が考えられます。

1. この CICS 実行に対して SIT に定義されているリソース・クラスのいずれか、または
2. その他の一般リソース・クラスまたは DATASET クラス

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド(TOOLKIT.PEMT) に対するアクセス権限、および対象のユーザー ID またはグループのデフォルト・グループ (PEMT.*dfltgrp*) に対するアクセス権限を持っている必要があります。

および

リソースが SIT に定義されているクラスに含まれる場合、ユーザーは、付与されているアクセス権限と同じレベル、またはそれよりも高いレベルのアクセス権限をそのリソースに対して持っている必要もあります。PERMIT の完了後、結果を即時有効にするには、リソース・クラスを再作成する必要があります。zSecure CICS Toolkit には、そのために必要な **SETROPTS REFRESH** コマンドを実行する手段がありません。

他のクラスにリソースが含まれる場合、ユーザーは、そのクラスで **PERMIT** コマンドを実行する権限 (PEMX.*classname*)、および付与されているアクセス権限と同じレベル、またはそれよりも高いレベルのアクセス権限をそのリソースに対して持っている必要もあります。

手順

1. **PERMIT** コマンドにアクセスするには、メインメニューで、指定されている **PF** キーを押します。

```
Termid = CP24          IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                    Permit                     Time = 11:35:10


    User/Grp =               Rsrclass =

    Resource =


                     <===

    Delete = N     Access = R   (R=Read,N=None,U=Update,A=Alter,C=Control)
    Specify "Delete = Y" to remove the user from the access list









CQT029 -Enter userid/group name and resource
PF5=Update ENTER=Redisplay CLEAR=Main menu
```

図 *37. PERMIT* パネル

USERID
アクセス権限を付与 (または除去) するユーザーまたはグループの名前。

RESOURCE
リソースの名前 (例えば、トランザクション CEMT の場合には、CEMT となります)。

RSRCLASS
リソース・クラス名。ブランクの場合、SIT に指定されている XTRAN パラメーターの値が使用されます。

DELETE
このリソースのアクセス・リストからユーザーまたはグループを除去するには、このフィールドに Y を指定します。

ACCESS
R (読み取り権限)、N (なし)、U (更新)、A (変更)、または C (制御) を指定します。N を指定すると、ユーザーがコマンドを実行する権限は、最小の読み取り権限に設定されます。

2. 情報を更新または指定して **PF5** を押します。

PERMIT コマンドを実行するユーザーは、変更するリソースに対するアクセス権限を持っている必要があります。例えば、CEMT を対象にアクセス権限を付与する場合、ユーザーには CEMT に対するアクセス権限が必要です。DELETE が **Y** と指定されている場合でも、コマンドを実行するユーザーには、そのリソースに対するアクセス権限が必要です。必要なアクセス権限のレベルは、「**ACCESS**」フィールドに指定されます。

関連の管理 (RACLINK コマンド)

RACLINK コマンドを使用して、ユーザーの関連を定義、リスト、定義解除、または承認します。

このタスクについて

RACLINK コマンドは、ローカル・ノードでのみ機能します。パネルに指定された NODE の値に関わらず、zSecure CICS Toolkit はこの値をローカル・ノードの名前であると見なします。

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.RACL) に対するアクセス権限を持っている必要があります。ユーザーが別のユーザーに対して **RACLINK** を実行するには、RACF SPECIAL 権限、TOOLKIT.SPEC、またはそのユーザーのデフォルト・グループ (RACL.*dfltgrp*) に対するアクセス権限が必要です。

手順

1. RACLINK コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2017/199
Userid = BCSCGB1          RACLINK =   BCSCGB1                   Time = 08:17:09

D PEER       STRX     BCSCGB4  YES (          ) <= Password(optional)
  ---TYPE--- --NODE-- -USERID- PWD
                                Sync   Status              Created by YYYY/MM/DD

_ PEER OF    IDFX     IBMUSER  NO     ESTABLISHED         BCSCGB1    2007/04/04
_ PEER OF    IDFX     BCSCGB2  NO     ESTABLISHED         BCSCGB1    2007/04/04
_ PEER OF    OBLX     BCSCGB2  NO     ESTABLISHED         BCSCGB1    2007/04/04
_
_
_
_
_
_
_
_
_
_
_
_
_

PF5=Update 8=Down ENTER=List CLEAR=Main menu
```

図 *38. RACLINK* パネル

TYPE
関連のタイプ。値は、PEER または MANAGED です。

NODE
関連を定義するノードの名前。

USERID
関連を定義する対象ユーザー。

PWD SYNC
関連のパスワードを同期するかどうかを指定します (*YES* または *NO* を入力します)。

PASSWORD
オプション・パラメーター。ユーザーに指定するパスワード。

2. 「RACLINK =」フィールドには、コマンドの実行依頼対象とするユーザーを入力します。**Enter** を押してそのユーザーの関連をリストします。
3. 関連の左側に U と入力してから PF05 を押すと、その関連の定義が解除されます。

- 操作する関連は、ユーザー自身の ID に関する関連でなければなりません。ユーザー自身の ID の関連ではない場合、システム SPECIAL 権限、TOOLKIT.SPEC、または RACL.*dfltgrp* が必要となります。
- 関連が承認待ちの状態となっていて、それがユーザー自身の ID の関連である場合 (または、ユーザーがシステム SPECIAL 権限あるいは zSecure CICS Toolkit SPECIAL 権限を持っている場合)、関連の左側に A と入力して PF05 を押すことによって、関連を承認できます。
- 上記の表示では、新しい関連が定義されようとしています。ユーザーが PF5 キーを押した後に、この新しい関連は定義されます。DEFINE を表す D が表示されるはずです。
- 有効なパスワードが指定された場合、またはコマンドの発行者が RACF SPECIAL 権限、TOOLKIT.SPEC、または RACL.dfltgrp を持っている場合には、関連は黙示的に承認されます。
- 新しいユーザーの関連を定義するには、TSO RACLINK コマンドに定義されている標準の RACLINK 権限が必要です。 これらの権限は、RACLINK.DEFINE.*nodename* および RACLINK.PWSYNC.*nodename* です。

一般リソース・クラスのプロファイルのリストおよび管理 (RALTER/RDEFINE/RDELETE コマンド)

RALTER、**RDEFINE**、および **RDELETE** コマンドを使用して CDT で定義されている一般リソース・クラスのプロファイルのリストと管理を行います。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (実行するコマンドに応じて、**TOOLKIT.RALT / TOOLKIT.RDEF / TOOLKIT.RDEL**) に対するアクセス権限と、一般リソース・クラス (RLST.*cdtclass* ならびに RALT.*cdtclass* / RDEF.*cdtclass* / RDEL.*cdtclass*) に対するアクセス権限を持っている必要があります。

手順

1. **RALTER / RDEFINE / RDELETE** コマンドにアクセスするには、メインメニューで、指定されている **PF** キーを押します。

```
Termid = CP24          IBM Security zSecure CICS Toolkit        Date = 2007/094
Userid = BCSCGB1         RES Class =            Type =          Time = 11:37:16
Profile



Member




Owner =          Notify =          Uacc = None    Warn = N Level = 000
Audit = F Aud succ = R Aud fail = R

----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----


                |<===
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

PF1=Rdef PF2=Addmem PF3=Rdel PF4=Delmem PF5=Updprof ENTER=Rlst CLEAR=Main menu
```

図 *39. RALTER / RDEFINE / RDELETE* パネル

RDEFINE
新規プロファイル/リソースを定義するには、「インストール・データ」フィールドを除くすべてのフィールドに入力する必要があります。これらの情報を入力した後、**PF01** を押して **RDEFINE** を実行します。

RDELETE
プロファイル/リソースを削除するには、「クラス」および「プロファイル」に名前を入力して、**PF03** を押します。

RALTER
グループへの新規メンバーの追加 (ADDMEM)、グループからのメンバーの削除 (DELMEM)、およびプロファイル情報の更新 (UPDPROF) を行うことができます。必要な情報は、実行するサブコマンドに依存します。

ADDMEM
「クラス」、「プロファイル」、および追加する「メンバー」を入力する必要があります。**PF02** を押して ADDMEM を完了します。

DELMEM
「クラス」、「プロファイル」、および削除する「メンバー」を入力する必要があります。**PF04** を押してメンバーを削除します。

UPDPROF
「インストール・データ」を除くすべてのフィールドを入力する必要があります。「**クラス**」および「**プロファイル**」フィールドを入力して **Enter** キーを押すと、各フィールドの現行エントリーが表示されます。これらのエントリーは上書きできます。 **PF05** を押して更新を完了します。

2. ステップ 1 のフィールドの説明を参照して実行したいアクションの値を指定してから、対応する **PF** キーを押して変更を開始します。

グループからのユーザー ID またはグループの削除 (REMOVE コマンド)

REMOVE コマンドを使用すると、グループからユーザー ID またはグループを削除することができます。ユーザー ID をそのデフォルト・グループから削除することはできません。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.REMV) に対するアクセス権限、およびターゲット・グループ (REMV.*grpname*) に対するアクセス権限を持っている必要があります。

手順

1. REMOVE コマンドにアクセスするには、メインメニューで、指定されている PF キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                                                Time = 11:37:31

                Userid                Group
    Remove   =               Group =




CQT016 -Enter userid and group name
PF5=Update ENTER=Redisplay CLEAR=Main menu
```

図 *40.* 「*REMOVE*」パネル

2. グループからユーザーを削除するには、指示されているようにユーザーおよびグループ名を入力して **PF05** を押します。
ユーザーをそのデフォルト・グループから削除することはできません。

一般リソース・クラスのプロファイルのリスト (RLIST コマンド)

RLIST コマンドを使用して、CDT で定義されている一般リソース・クラスのプロファイルをリストすることができます。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.RLST) に対するアクセス権限と、一般リソース・クラス (RLST.*cdtclass*) に対するアクセス権限を持っている必要があります。

手順

1. **RLIST** コマンドにアクセスするには、メインメニューで、指定されている **PF** キーを押します。

```
 Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
 Userid = BCSCGB1         Rlist class =          Type =          Time = 11:37:41
                                 Profile
 ------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------------------------------------------------------------------------
-------

 Owner = ******** Dte = ***** Last ref = ***** Last chg = ***** Uacc = *******

 Audit = * Aud succ = * Aud fail = * Notify = ******** Warn = * Level = ***

 Glbl Audit = * Gaud Succ = * Gaud Fail = * Secl = ***

 Members = **** NumUsrs = **** Condacc = ****

 ----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----
 ******************************************************************************
******************************************************************************
******************************************************************************
**************** |<===
 ----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

 PF1=Toggle 3=Chgopts 5=Members 7=Users 9=Condacc 11=Search CLEAR=Main menu
```

図 *41.* 「*RLIST*」パネル

RLIST CLASS
表示するリソース・クラスの名前です。これは、RACF クラス記述子テーブルに含まれる有効なエントリーでなければなりません。

TYPE
クラスをメンバー・クラス (TYPE=M) またはグループ・クラス (TYPE=G) として定義します。これは情報としてのみ提供されます。リストや検索の入力としては使用されません。

PROFILE
表示するプロファイルの名前。このフィールドには、表示するプロファイルの名前を入力します。検索を実行している場合には、このフィールドをバイパスできます。または、検索基準の一部として、任意の位置に任意の文字を入力することもできます。このフィールドは、最大 246 文字の長さにできます。

注 : RLIST を実行するだけの場合、残りのフィールドは無視されます。 残りのフィールドは、検索を行う場合にのみ (PF11)、入力として使用されます。

OWNER
プロファイルの所有者として定義されているユーザーまたはグループ。

DTE
このプロファイルが作成された日付。フォーマットは *YYDDD* です。

LAST REF
データ・セットが最後に参照された日付。フォーマットは *YYDDD* です。

LAST CHG
プロファイルが最後に更新された日付。フォーマットは *YYDDD* です。

UACC
プロファイルの汎用アクセス。このフィールドの値は、ALTER、CONTROL、UPDATE、READ、または NONE です。

AUDIT
プロファイルの監査フラグを指定します。設定できる値は、A (すべてのアクセスを監査)、S (成功アクセスを監査)、F (失敗を監査)、または N (監査なし) です。

AUD SUCC
これは監査の成功フラグです。設定できる値は、R (読み取り成功を監査)、U (更新成功を監査)、C (制御アクセスを監査)、または A (成功した変更アクセスを監査) です。

AUD FAIL
これは監査の失敗フラグです。 設定できる値は、R (読み取り失敗を監査)、U (更新失敗を監査)、C (失敗した制御アクセスを監査)、または A (失敗した変更アクセスを監査) です。

NOTIFY
このプロファイルへのアクセスが拒否された場合に通知するユーザー。

WARN
プロファイルが警告モードであるかどうかを示します。このフィールドの値は、**Y** または **N** です。

LEVEL
データ・セットのレベル標識。このフィールドは数値フィールドです。

GLBL AUDIT
AUDITOR 属性を持つユーザーによって指定されたグローバル監査オプションです。設定できる値は、A (すべてのアクセスを監査)、S (成功したアクセスを監査)、F (失敗を監査)、または N (監査なし) です。

GAUD SUCC
これはグローバル監査の成功フラグです。設定できる値は、R (読み取り成功を監査)、U (更新成功を監査)、C (成功した制御アクセスを監査)、または A (成功した変更アクセスを監査) です。

GAUD FAIL
これはグローバル監査の失敗フラグです。設定できる値は、R (読み取り失敗を監査)、U (更新失敗を監査)、C (失敗した制御アクセスを監査)、または A (失敗した変更アクセスを監査) です。

SECL
プロファイルのセキュリティー・レベル。このフィールドは数値フィールドです。

MEMBERS
プロファイルに含まれるメンバーの数 (グループ・プロファイルの場合)。

NUMUSRS
プロファイルへのアクセスが許可されているユーザーとグループの数。このフィールドは数値フィールドです。

CONDACC
条件付きアクセス・リストのユーザー/グループの数。このフィールドは数値フィールドです。

INSTALLATION DATA
プロファイルのデータ・フィールドに含まれる情報。最大 255 文字まで使用できます。

2. 以下の操作を選択できます。
   - プロファイルに対するアクセス権限を持つユーザー/グループを表示する (PF07)。
   - 条件付きアクセス・リストのユーザー/グループを表示する (PF09)。
   - **TYPE=** フィールドに、リソース・クラスがグループ・クラスであると示されている場合、プロファイルに含まれるメンバーを表示する (PF05)。

   複数のパネルにメンバー、ユーザー、または条件付きアクセス・リストが表示されている場合は、**PF08** を使用してページ送りできます。

RLIST の表示例

以下の例は、リストするプロファイルを入力したときに表示される内容を示しています。

リストするプロファイルを入力した場合、または検索を開始した場合は、次に以下のようなパネルが表示されます。

```
Termid = CP24          IBM Security zSecure CICS Toolkit        Date = 2007/094
Userid = BCSCGB1         Rlist class = GCICSTRN Type = G        Time = 11:38:02
                                Profile
CICSA.CAT1



Owner = SYS1     Dte = 05033 Last ref = 05033 Last chg = 05033 Uacc = NONE

Audit = F Aud succ = R Aud fail = R Notify = ******** Warn = N Level = 000

Glbl Audit = N Gaud Succ = R Gaud Fail = R Secl = ***

Members = 0051 NumUsrs = 0003 Condacc = 0000

----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----


               |<===
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----

PF1=Toggle 3=Chgopts 5=Members 7=Users 9=Condacc 11=Search CLEAR=Main menu
```

図 *42.* 「*RLIST Display*」パネル

この時点で、以下の操作を選択できます。

- メンバーを表示する (PF05)。
- ユーザーを表示する (PF07)。
- 条件付きアクセス・リストを表示する (PF09)。
- 検索またはリスト・オプションを変更する (PF03)。
- メインメニューに戻る (CLEAR)
- 検索を実行している場合、基準と一致するすべてのプロファイルを表示する (PF01)。

プロファイル内のメンバーのリスト (RLIST コマンド、MEMBERS オプション)

RLIST コマンドとメンバー・オプションを使用して、プロファイル内のメンバーをリストすることができます。

手順

- RLIST パネルで **PF05** を押してプロファイルに含まれるメンバーを表示します。

```
Termid = CP24          IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                 Rlist    =   (MEMBERS)       Time = 11:38:12
CICSA.CAT1

CICSA.CRTP
CICSA.CPIR
CICSA.CATA
CICSA.CATD
CICSA.CDBD
CICSA.CDBF
CICSA.CDBO
CICSA.CDBQ
CICSA.CDTS
CICSA.CESC
CICSA.CESD
CICSA.CEX2
CICSA.CFCL
CICSA.CFOR
CICSA.CFQR
CICSA.CFQS
CICSA.CFTL
CICSA.CFTS

PF1=Toggle 3=Chgopts 5=Memb 7=User 8=Down 9=Condacc ENTER=Next CLEAR=Main menu
```

図 *43.* 「*RLIST* メンバー」パネル

- この時点で、以下の操作を選択できます。
  - ユーザーを表示する (PF07)。
  - 条件付きアクセス・リストを表示する (PF09)。
  - 検索またはリスト・オプションを変更する (PF03)。
  - メインメニューに戻る (CLEAR)
  - 検索を実行している場合、次のプロファイルを表示する (ENTER)。

プロファイル内のユーザー ID とそのアクセス権限のリスト (RLIST コマンド、USERS オプション)

RLIST コマンドと Users オプションを使用して、プロファイル内のユーザー ID と、それらのユーザーに付与されたアクセス権限をリストすることができます。

手順

- RLIST パネルで **PF07** を押して、プロファイルに含まれるユーザーと、これらのユーザーが持つアクセス権限を表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                   Rlist    =   (USERS)         Time = 11:38:23
CICSA.CAT1

IBMUSER /A CICSA   /R CICSASTC/R









PF1=Toggle 3=Chgopts 5=Memb 7=User 8=Down 9=Condacc ENTER=Next CLEAR=Main menu
```

図 *44.* 「*RLIST Users*」パネル

- この時点で、以下の操作を選択できます。
  - メンバーを表示する (PF05)。
  - 条件付きアクセス・リストを表示する (PF09)。
  - 検索またはリスト・オプションを変更する (PF03)。
  - メインメニューに戻る (CLEAR)
  - 検索を実行している場合、次のプロファイルを表示する (ENTER)。

プロファイルの条件付きアクセス・リストに含まれるユーザー/グループのリスト (RLIST コマンド、CONDACC オプション)

RLIST コマンドと条件付きアクセス・オプションを使用して、プロファイルの条件付きアクセス・リストに含まれるユーザー/グループをリストすることができます。

手順

- RLIST パネルで **PF09** を押して、プロファイルの条件付きアクセス・リストに含まれるユーザー/グループを表示します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                  Rlist    =   (CONDACC)       Time = 11:39:04
CICSA.CAT1

BCSC    /R-TERMINAL=D20AK021









PF1=Toggle 3=Chgopts 5=Memb 7=User 8=Down 9=Condacc ENTER=Next CLEAR=Main menu
```

図 *45.* 「*RLIST Conditional Access*」パネル

- この時点で、以下の操作を選択できます。
  - メンバーを表示する (PF05)。
  - ユーザーを表示する (PF07)。
  - 検索またはリスト・オプションを変更する (PF03)。
  - メインメニューに戻る (CLEAR)
  - 検索を実行している場合、次のプロファイルを表示する (Enter)。

USRDATA フィールドの管理 (USRDATA コマンド)

USRDATA コマンドを使用すると、ユーザー・プロファイルの USRDATA フィールドをリスト、追加、更新、または削除することができます。USRDATA への更新のために作成される特殊な SMF レコードについては、79 ページの『zSecure CICS Toolkit で作成された SMF レコード』を参照してください。

このタスクについて

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.USRL)、対象のユーザー ID (USRU.dfltgrp) に対するアクセス権限、および USRDATA 名 (USRN.*usrdata-name*) に対するアクセス権限を持っている必要があります。 **ADD**、**UPDATE**、および **DELETE** サブ関数には、対応するコマンド・プロファイルへのアクセス権限が必要です (**ADD** および **UPDATE** の場合は TOOLKIT.USRA、**DELETE** の場合は TOOLKIT.USRD)。

手順

1. **USRDATA** コマンドにアクセスするには、メインメニューで、指定されている **PF** キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                     USRDATA                    Time = 11:39:16

Fill in Profile and ENTER. For Add, fill in fields, select A and PF5
_ Class = USER     Profile =
USRDATA
  Name =           Value =


                                            |<===
  Name     Value   (Use S/L and ENTER for details, or D and PF5 for delete)
-
-
-
-
-
-
-
-
-
-
CQT018 -Enter userid
PF5=Update 8=Down ENTER=List CLEAR=Main menu
```

図 *46.* 「*USRDATA*」パネル

2. ユーザーの USRDATA を表示するには、ユーザー ID を入力して **Enter** キーを押します。
   - パネルの最下部に、USRDATA 名と、それぞれに対応する値の最初の 64 文字が表示されます。
   - USRDATA 名がパネルに表示しきれていない場合は、**PF8** を押してスクロールダウンします。
   - 切り捨てられていない完全な USRDATA 値を 1 つ表示するには、目的の USRDATA 名/値の前に **S** (または **L**) コマンドを入力して、**Enter** キーを押します。

```
Termid = CP24           IBM Security zSecure CICS Toolkit       Date = 2007/094
Userid = BCSCGB1                     USRDATA                    Time = 11:41:00

  Class = USER     Profile = BCSCGB2
USRDATA
  Name =  PHONE    Value = +1 123-456-7890


                                          |<===









PF5=Update 11=Delete ENTER=Refresh CLEAR=Back
```

図 *47.* 「*USRDATA Display*」パネル

3. ユーザーの USRDATA を追加するには、USRDATA の名前と値を入力してから、「**クラス**」の前にあるフィールドに A と入力して、**PF5** を押します。

   このコマンド・フィールドで D または U を選択して「USRDATA」フィールドを削除する場合、または更新する場合にも、これと同じ方法を使用できます。後者の場合、これは代替策であり、以下に説明する方法が優先されます。
4. 表示された USRDATA 名と値の対を 1 つ削除するには、以下のいずれかの方法を使用します。
   - 目的の USRDATA の前に **D** コマンドを入力して、**PF5** を押します。
   - **S** または **L** 行コマンドを使用して USRDATA 値を表示し、詳細パネルで **PF11** を押します。

5. 既存の USRDATA 値を更新するには、リストされた USRDATA 名の前に **S** (または **L**) を入力して、詳細パネルを表示します。詳細パネルで、値を新しい値で上書きし、**PF5** を押します。

第 6 章 zSecure CICS Toolkit の出口点の指定

CQTPCNTL の EXITPGM パラメーターには、zSecure CICS Toolkit のメイン・トランザクション (通常は RTMM) が終了し、CICS に制御を戻すときに、常に制御を受け取るプログラムを指定することができます。

制御は XCTL コマンドを介して EXITPGM に渡されます。EXITPGM 実行の後、zSecure CICS Toolkit が再度制御を受け取ることはありません。これには、戻りコードおよびユーザーのパネルに送信されたデータ (存在する場合) も含まれます。COMMAREA のフォーマットは次のとおりです。

```
EXITRC       DC CL1          Return Code
                             0 = CICS Toolkit transaction has terminated
                             1 = Signon transaction failed or was
                                 terminated with the clear key
                             3 = Signon completed.  User was signed-on at a
                             second terminal but was not authorized (did not
                             have access to TOOLKIT.DUPE and DUPEUSER checking
                             is in effect).
                             4 = Signon completed.Same as 3, but terminal
                                 logged off CICS.
                             5 = Signon completed. No CICS segment
                                 found for user.
                             6 = Signon completed. CICS segment
                                 was found for user.
                             7 = Signon completed. Error in installation
                                 data being used for operator information.
*
EXITDATA     DC CL335        Data sent to users screen from signon or CICS
                             Toolkit transaction termination.  If the return
                             code is 0, this field is only 79 bytes in length.
                             For any other return code, this field
                             will contain the data, if any, that was
                             sent to the terminal user.
```

EXITPG のサンプルが、SCQTSAMP PDS に CQTXSNEX メンバーとして提供されています。

第 7 章 アプリケーション・プログラミング・インターフェース (API)

zSecure CICS Toolkit 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より、ユーザーは CICS アプリケーション・プログラムから RACF データベースに直接アクセスすることができます。RACF やデータベース形式に関する特別な知識は不要で、実行の許可をアプリケーションに設定する必要もありません。

API を使用すると、インストール済み環境で独自の要件に合わせて zSecure CICS Toolkit パネルを調整したり、別の種類のレポートを生成することができます。zSecure CICS Toolkit により、許可されたユーザーしか RACF データベースにアクセスできないことが保証されます。API を使用する場合は、zSecure CICS Toolkit を使用する場合と同じ規則が適用されます。API を使用するトランザクションを実行するユーザーは、使用する zSecure CICS Toolkit コマンドの許可を持っている必要があります。ユーザー情報を要求する場合は、表示するユーザー・プロファイルのデフォルト・グループに対するアクセス権限を、対象のユーザーが持っている必要があります。この件について詳しくは、31 ページの『第 5 章 zSecure CICS Toolkit コマンド・インターフェース』を参照してください。

API を使用する際に必要な手順は、CICS アプリケーション・プログラムでインターフェース ・モジュール CQTPAPI0 を呼び出し、このモジュールに対して COMMAREA で特定のパラメーターを渡すだけです。 これらのパラメーターは、要求されたコマンドを zSecure CICS Toolkit に通知し、要求された情報が返されるストレージ域を提供します。

互換性のために、CQTPAPI0 プログラムには CRTKAPI という別名が付いています。いずれの名前も同じモジュールを指しますが、すべてのアプリケーションで新しい名前 CQTPAIP0 を使用してください。

zSecure CICS Toolkit は、RACF データベースの読み取りまたは更新中に、CICS メインタスクを待機させることはありません。これらのコマンドは、すべて zSecure CICS Toolkit サブタスクによって処理されるため、CICS は、通常のトランザクション処理を自由に続行することができます。この CICS 領域は、常に許可状態で実行されるわけではなく、完全性に関する IBM の方針に従います。

zSecure CICS Toolkit で作成された SMF レコード

zSecure CICS Toolkit が RACF プロファイルに対して行った変更はすべて、SMF を介して記録されます。ALTUSER のように RACF コマンドに直接対応する変更は、その RACF コマンドで使用されるフォーマットと同じフォーマットを使用して記録されます。これらのレコードには変更を要求した端末ユーザーも含まれ、通常の RACF レポートに表示されます。これらのレコードを TSO ジョブやバッチ・ジョブで作成された SMF レコードと区別するために、フィールド SMF80UID には値 T0OLKIT* が組み込まれます。この特殊値を使用して、レコードが zSecure CICS Toolkit 機能の一部として生成されたことが示されます。

USRDATA フィールドに対する変更は、通常のどの RACF コマンドにも対応しません。そのため、同じレコード・フォーマットを使用することはできません。RACF 一般監査イベントの SMF レコードを LOGSTR と共に使用して、変更されたデータを表示します。ログ・ストリングは、単一ブランクで区切られた 6 個の文字ストリングで 構成されます。

フィールド	長さ	内容
ヘッダー	15	TOOLKIT USRDATA
クラス	4	USER
プロファイル	8	userid
アクション	6	{ADD, UPDATE, DELETE, LIST}
UserNm	8	フィールド名
UserData	最大 209	フィールド値 (切り捨て)

COMMAREA を使用したコマンド要求

COMMAREA は、要求されたコマンドを zSecure CICS Toolkit に通知するための手段です。COMMAREA のサイズは、実行するコマンドによって異なります。いずれの場合も、共通のヘッダーがあり、その後に関連コマンド固有の情報が続きます。

ヘッダーのフォーマットは次のとおりです。

```
API_FUNCT              DC  CL4         This field specifies the command
*                                      being requested.
*
API_RC                 DC  XL1         A one byte hexadecimal return
*                                      code.
*
API_MSG                DC  CL79        The message that would normally
*                                      be displayed on the terminal if
*                                      the user was using the standard
*                                      Toolkit transaction is returned
*                                      in this field.
```

アプリケーション・プログラムは、以下に示す標準の CICS LINK コマンドを使用して、API を呼び出します。

```
EXEC CICS LINK PROGRAM('CQTPAPI0')COMMAREA(APICOMM) LENGTH(APILEN)
```

COMMAREA が渡されなかった場合、CTKAPI は以後の処理を行うことなく、単に呼び出し元に戻ります。COMMAREA のレイアウトでエラーが検出された場合は、長さが無効であるか、要求されたコマンドが無効です。あるいは、ユーザーが zSecure CICS Toolkit コマンドの使用を許可されていません。この場合、API は API_RC に戻りコードを設定して、エラーの種類を示します。考えられる戻りコードは次のとおりです。

戻りコード

X'00'
COMMAREA は正常です。

X'01'
無効なコマンドが要求されました。API_FUNC に指定されているパラメーターか正しいかどうかを確認してください。

X'02'
COMMAREA の長さの値が、要求されたコマンドに対して小さすぎます。

X'03'
ユーザーがこの zSecure CICS Toolkit コマンドの使用を許可されていないか、端末にサインオンしていません。

X'04'
TOOLKIT.*function* リソースを保護するプロファイルがありませんでした。 そのため、許可を決定できず、API 関数は実行されませんでした。

X'05'
内部エラーです。技術サポートにお問い合わせください。

API に渡された commarea は正しいが、別の理由で関数が失敗した場合は、API_RC に値 x'00' が入ります。関数固有の戻りコード・フィールド (通常は API_*function*_RC) には、エラー標識が入ります。ほとんどの API 関数は、エラーが発生した場合の標識として値 -1 を使用します。フィールド API_MSG には、失敗を記述するエラー・メッセージが入ります。これらのメッセージの例を以下に示します。

- CQT039 は、指定された ID が存在しない場合に、**ALTUSER** コマンドについて出力されます。
- CQT080 は、要求されたプロファイルが見つからない場合に、**LIST** コマンドについて出力されます。

エラー・メッセージの完全なテキストについては、「*IBM Security zSecure:* メッセージ・ガイド」を参照してください。

資料内で特別に明記されていない限り、必ず COMMAREA のすべてのフィールドにブランクを埋め込んでください。

許可ユーザーの変更

API 経由でコマンドを実行するには、タスクに関連付けられたユーザー ID に、zSecure CICS Toolkit コマンドの権限を付与する必要があります。このユーザー ID は、通常、端末にログオンしているユーザーまたは CICS デフォルト・ユーザーの ID です。許可ユーザーの ID には、他のユーザー ID を指定することもできます。

許可ユーザーを変更するには、CQTPAPI0 を呼び出す前に、API-MSG 領域の先頭 24 バイトで以下の定義を行います。

表 7. 許可ユーザー *ID* を変更するための *API-MSG* 定義

API メッセージ変数	**値**	**説明**
API_MSG_USERAUTH	DC CL8'USERAUTH'	USERAUTH の定数
API_MSG_USERID	DC CL8'USERAUTH'	許可ユーザーとして使用するユーザー ID。
API_MSG_PASSWORD	DC CL8'*password*'	ユーザーのパスワード。

ユーザーのパスワードが間違っている場合はコマンドが失敗し、該当するメッセージが呼び出し側プログラムに返されます。

検索の実行

RACF データベースの検索は、**LISTUSER**、**LISTGROUP**、**LISTDATASET**、および **RLIST** の各コマンドを使用して実行できます。

これらの各コマンドの COMMAREA には、1 バイトのコード・フィールドがあります。このフィールドは、検索を実行しているかどうか、次のプロファイルを取得する必要があるかどうか、またはプロファイルに関する他の情報が必要かどうかを示します。

検索を要求する場合は、COMMAREA のプロファイル属性フィールドにアスタリスクを 埋め込む必要があります。検索マスクでは、フィールドの任意の組み合わせにある、有効な文字の任意の組み合わせにすることができます。zSecure CICS Toolkit は、一致するプロファイルを検出すると、そのプロファイル情報を COMMAREA に返します。検索条件に一致する次のプロファイルを取得するには、COMMAREA のコード・フィールドを N (Next) に設定して API を呼び出します。プロファイル自体にアスタリスクを埋め込まないでください。 代わりに、ブランク (x'40')、ヌル (x'00')、またはアンダースコアー (x'6D') を埋め込んでください。マスキングの一般規則にこの例外が設けられている理由は、汎用文字を含むプロファイルに特定した検索を実行できるようにするためです。

zSecure CICS Toolkit はプロファイル情報を COMMAREA に返すため、作業用ストレージに検索マスクを作成し、API を呼び出す前に、毎回 COMMAREA に移動する必要があります。また、検索中に API によって使用される API_RESERVED フィールドもあります。このフィールドの内容は、呼び出しを終えてから次の呼び出しを行うまで保持しておく必要があります。

すべてのプロファイル (例えば、すべてのユーザー・プロファイルなど) を取得するには、検索マスクをすべてアスタリスクにする必要があります。検索を開始するには、コード・フィールドに S を指定します。その後、残りのプロファイルを取得するには、コード・フィールドを N に設定します。ゼロ以外の戻りコードが返されるまで、API の呼び出しを続行します。API_MSG フィールドにも、条件に一致するプロファイルがそれ以上存在しないか、RACF データベースの終わりに達したことを示すメッセージが格納されます。呼び出しの前に、毎回検索マスクを再作成してください。

フィールド・レベルまたはレコード・レベルのセキュリティーの実装

特に、最大 246 バイトのリソース名を使用する場合は、API リソース権限検査機能を使用することにより、フィールド・レベルまたはレコード・レベルのセキュリティーを実装することができます。

このタスクについて

ファイル内で特定のフィールドまたはレコードを表すリソース名を定義することにより、それらのレコードやフィールドへのアクセスを制限することができます。アプリケーション・プログラムにより、API を呼び出してユーザーのアクセス権限を検査し、実行すべきアクションを判別することができます。アクションには、レコードの更新、レコードの表示、フィールドの更新、フィールドの消去などがあります。

PAYFILE という DD 名を持つファイルの例を示します。このファイルのキーは、社会保障番号です。

手順

1. 以下のように、DD 名と社会保障番号を RACF に定義します。

```
RDEFINE RSRCLASS PAYFILE.999-99-999 UACC(NONE)
```

2. 以下のように、レコードに対する許可をユーザーに付与します。

```
PERMIT PAYFILE.999-99-999 CLASS(RSRCLASS) ID(USERIDA) ACC(READ)
```

次のタスク

これにより、アプリケーションで API を呼び出してリソース・アクセス権限検査を実行し、レコードやフィールドに対するユーザーのアクセス・レベルを判別できるようになります。

アクセス権限検査関数

アクセス権限検査関数を使用すると、ユーザーが 1 つ以上のリソースに対するアクセス権限を保持しているかどうかを判別できます。権限は不要です。

COMMAREA

最小サイズは 99 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。例:

```
API_FUNC       DC  CL4'RSRC'  FUNCTION code for access check
API_RC         DC  XL01'00'   Return code
API_MSG        DC  CL79' '    Message area
*
API_RSRC_NAMES DC  XCL14      This is a list of resources for
*                             which the access authority of the user
*                             signed on at the terminal is to be checked.
*                             The size of this field depends on the
*                             number of resources being checked.  Each
*                             resource name requires thirteen bytes,
*                             padded with blanks, followed by a one byte
*                             return code field.
*
*                             The return code field may also specify the
*                             level access to be checked. This may be
*                             'R' (read), 'U' (update), 'C' (control) or
*                             'A' (alter). Read is the default.
*
*                             For example to check the users access to
*                             AUDIT and PAYROLL the following
*                             entries could be coded.
*
               DC  CL13'AUDIT'   First resource name
               DC  XL1'00'       Return Code
               DC  CL13'PAYROLL' Next resource name
               DC  XL1'00'       Return Code
*
```

```
                DC  XL1'FF'    The last field in the COMMAREA
*                              must be a one byte field containing X'FF',
*                              indicating the end of the list of
*                              resource names.
```

アクセス権限検査のときに使用されるリソース・クラスは、CQTPCNTL の RSRCLASS パラメーターで指定されたクラスです。

アプリケーション・リソース名に接頭部が指定されている場合 (CQTPCNTL の CICSAPPL パラメーターを参照)、CQTPAPI0 に渡されるリソース名にその接頭部が付加されます。アプリケーション・セキュリティーと RACF に対するリソースの定義について詳しくは、27 ページの『第 4 章 アプリケーション・セキュリティーの管理』を参照してください。

SMF レコードは、リソースに対して指定された AUDIT パラメーターに応じて生成されます。システム・コンソールと CICS ログに ICH408I メッセージを出力したくない場合は、API_RC フィールドに値 S を指定します。この値を指定した場合、アクセス違反があった場合に表示されるメッセージは出力されなくなりますが、それらの違反に関する SMF レコードは作成されます。

戻りコードは 1 バイトの 16 進フィールドで、以下の意味を持っています。

戻りコード

X'00'
リソースへのアクセスが許可されました。

X'04'
リソースが RACF に対して定義されていません。

X'08'
ユーザーは、リソースの使用を認可されていません。

X'0C'
RACF がアクティブではありません。

X'10'
FRACHECK インストール・システム出口エラーです。

X'14'
RACF がインストールされていないか、レベルが無効です。

アクセス権限検査 (拡張) 関数

アクセス権限検査 (拡張) 関数を使用すると、ユーザーが 1 つ以上のリソースに対するアクセス権限を保持しているかどうかを確認できます。権限は不要です。

COMMAREA
最小サイズは 348 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。例:

```
API_FUNC          DC  CL4'RSRX'   Function code for access check
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_RSRX_USERID   DC  CL8         Specify the USERID to be used to perform
*                                 third party authorization checking.
*                                 If blank the ACEE of the user Signed on
*                                 at the terminal is used.
*
API_RSRX_CLASS    DC  CL8         This field may be used to specify the
*                                 resource class to be used
*                                 the access checks. If used, it overrides
*                                 the definition x for RSRCLASS in CQTPCNTL.
*                                 It must be x a valid class defined in the
                                  SIT unless a userid has been specified
*                                 in API_RSRX_USERID. In this case
*                                 any class may be specified.
```

```
*
API_RSRX_NAMES    DC  XCL247      This is a list of resources for which
*                                the access authority of the user signed
*                                on at the terminal is to be checked.
*                                The size of this field depends on the number
*                                of resources being checked. Each
*                                resource name requires 246 bytes, padded with
*                                blanks, followed by a one byte return code
field.
*
*                                The return code field may also specify
*                                the level of access to be checked.
*                                This may be:'R' (read),'U' (update),
*                                'C' (control) or 'A' (alter).
*                                Read is the default.
*
API_RSRX_ACC      EQU API_RSRX_NAMES+246,1
                                 The access level
*
*                                For example to check the users access to
*                                AUDIT and PAYROLL the following  entries
*                                could be coded.
                  DC  CL246'AUDIT'    First resource name
                  DC  XL1'00'         Return Code
                  DC  CL246'PAYROLL'  Next resource name
                  DC  XL1'00'         Return Code
*
                  DC  XL1'FF'     The last field in the COMMAREA must be a
*                                 one byte field containing X'FF',
*                                 indicating the end of the list of
*                                 resource names.
```

アクセス権限検査のときに使用されるリソース・クラスは、CQTPCNTL の RSRCLASS パラメーターで指定されたクラスです。これを指定すると、API_RSRX_RSRCLASS の値によって CQTPCNTL の値がオーバーライドされます。

アプリケーション・リソース名に接頭部が指定されている場合 (CQTPCNTL の CICSAPPL パラメーターを参照)、CQTPAPI0 に渡されるリソース名にその接頭部が付加されます。アプリケーション・セキュリティーと RACF に対するリソースの定義について詳しくは、27 ページの『第 4 章 アプリケーション・セキュリティーの管理』を参照してください。

SMF レコードは、リソースに対して指定された AUDIT パラメーターに応じて生成されます。システム・コンソールと CICS ログに ICH408I メッセージを出力したくない場合は、API_RC フィールドに値 N を指定します。 この値を指定した場合、アクセス違反があった場合に表示されるメッセージは出力されなくなりますが、それらの違反に関する SMF レコードは作成されます。

戻りコードは 1 バイトの 16 進フィールドで、以下の意味を持っています。

戻りコード:

X'00'
リソースへのアクセスが許可されました。

X'04'
リソースが RACF に対して定義されていません。

X'08'
ユーザーは、リソースの使用を認可されていません。

X'0C'
RACF がアクティブではありません。

X'10'
FRACHECK インストール・システム出口エラーです。

X'14'
RACF がインストールされていないか、レベルが無効です。

リソース・プロファイル・リスト関数

リソース・プロファイル・リスト関数を使用して、ユーザーがアクセス可能なプロファイルのリストを提供できます。権限は不要です。

zSecure CICS Toolkit API が提供する関数を使用すると、指定されたリソース・クラス内の、権限を持つすべてのプロファイルのリストを高いパフォーマンスで実行できます。この API は、SEARCH インターフェースと RLIST インターフェースの 組み合わせに対する代替手段を提供します。この API を使用すると、ユーザーが特定のレベルのアクセス権限を持つ指定のリソース・クラス内のすべてのプロファイルをリストすることができます。この API は、内部的に、プロファイル名リスト関数 (IRRPNL00) や高速許可検査関数 (RACROUTE REQUEST=FASTAUTH) などの高性能な RACF 関数を基盤にしています。この関数は、API 経由でのみ使用することができます。

COMMAREA

最小サイズは 146 バイトです。

アプリケーション内では、SCQTMAC ライブラリーで提供される APICOMMA または APICOMMC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC   CL4'RSRL'  FUNCTION code for Resource List
API_RC            DC   XL1'00'    API Return code
API_MSG           DC   CL79' '    Message area
*
API_RSRL_RETC     DS   XL1        Return code
API_RSRL_REAS     DS   XL1        Reason code
API_RSRL_CLASS    DS   CL8        CLASS
API_RSRL_USERID   DS   CL8        USERID or blank
API_RSRL_GROUP    DS   CL8        GROUPID or blank
API_RSRL_TSQUEUE  DS   CL16       TSQUEUE name or blank
API_RSRL_Prefix   DS   CL16       Filter prefix or blank
API_RSRL_Retflag  DS   CL1        Processing flags
*                                 "C" Return data in Commarea
*                                 "T" Return data in TSQUEUE
*                                 "B" Return data in Comm/TSQ
*                                 "N" Don't return any data
API_RSRL_FL_PR    DS   CL1        Use filter prefix Y/N
API_RSRL_FL_AC    DS   CL1        Return all profiles Y/N
API_RSRL_ACCESS   DS   CL1        Requested Access
*                                 "R" Read
*                                 "U" Update
*                                 "C" Control
*                                 "A" Alter
API_RSRL_PROFCNT  DS   XL4        Returned number of entries
API_RSRL_PROFLST  DS   XL2        Length of the profile below (CLx)
                  DS   CL1        Flag byte
*                 Possible values for the flag byte
*                                 "A" Access to discrete profile
*                                 "N" READ to discrete profile
*                                 "B" Access to generic profile
*                                 "G" READ to generic profile
                  DS   CLx        Profile
```

この関数の出力は、プロファイル名のリストから構成されます。このリストは、用意された commarea または指定された一時ストレージ・キュー (TSQUEUE) に 返されます。どの戻り域が使用されるかは、API_RSRL_RETFLAG に設定された戻りオプションによって決まります。プロファイルのリストには、ユーザーが READ 権限以上の権限を持つすべてのプロファイルか、ユーザーが API_RSRL_ACCESS で指定されたアクセス権限以上の権限を持つプロファイルだけが含まれます。プロファイル・リストの内容は、API_RSRL_FL_AC フラグ・バイトによって制御されます。プロファイル名の先頭文字を基準として、プロファイルのリストをフィルターに掛けることができます。フィルターのパターンは、フィールド API_RSRL_Prefix で指定します。フィルター処理は、API_RSRL_FL_PR フラグ・バイトによって活動化されます。

プロファイルを CICS の TSQUEUE に返す必要がある場合は、必ずリカバリー不能な MAIN ストレージ TSQUEUE を指定する必要があります。リカバリー可能な TSQUEUE を使用すると、プログラムが ATSP ABEND で終了する場合があります。AUXILIARY ストレージ・キューを使用すると、補助ストレージに対する入出力が発生し、アプリケーションの応答時間に影響する可能性があります。関連するシステム・リソースを解放したい場合は、データを処理した後に、呼び出し側プログラムで TSQUEUE を削除する必要があります。

用意した COMMAREA にプロファイルを返す必要がある場合は、十分なサイズの commarea を確保してください。用意したスペースに出力データが収まらない場合は、データが切り捨てられてメッセージが出力されます。この RSRL API では、切り捨てられた残りのデータを取得することはできません。追加のデータが必要な場合は、より大きな commarea を用意する要求を再発行するか、出力を TSQUEUE に返す要求を再発行する必要があります。

指定するリソース・クラスは、RACF SETROPTS コマンドを使用して RACLIST 処理が実行されている必要があります。グローバルに RACLIST 処理が実行されたリソース・クラス (CICS リソース・クラスの TCICSTRN など) はサポートされません。

API commarea のフィールドは以下のとおりです。

API_FUNC
呼び出される関数を記述します。許可されているリソースをリストする関数の場合は、「RSRL」を格納する必要があります。

API_RC
API 戻りコード。これは、API インターフェースの戻りコードです。 RSRL 関数からの戻りコードは、API_RSRL_RETC フィールドに格納されます。有効な API_RETC の値については、80 ページの『COMMAREA を使用したコマンド要求』で説明しています。

API_MSG
警告またはエラー・メッセージ。

API_RSRL_RETC
RSRL 関数からの戻りコード。有効な戻りコードの説明については、88 ページの『戻りコードと理由コード』を参照してください。

API_RSRL_REAS
RSRL 関数からの理由コード。有効な理由コードの説明については、88 ページの『戻りコードと理由コード』を参照してください。

API_RSRL_CLASS
許可されたプロファイルを必要とするリソース・クラス。 このリソース・クラスは、SETROPTS RACLIST コマンドを使用して RACLIST 処理を実行する必要があります。 グローバルに RACLIST 処理が実行されたリソース・クラス (CICS リソース・クラスの TCICSTRN など) はサポートされません。リソース・クラスが SETROPTS RACLIST ではない場合、エラー・メッセージが出力されて実行が停止します。クラス名は、省略せずにすべて指定する必要があります。省略形と総称文字はサポートされていません。

API_RSRL_USERID
許可されたプロファイルのリストを判別する対象となるユーザー。このフィールドが空の場合は、ログオンしている端末ユーザーを対象として、許可されたプロファイルのリストが判別されます。フィールドの先頭位置にブランクまたは 16 進のヌルが入っている場合、そのフィールドは空であると見なされます。

API_RSRL_GROUP
API_RSRL_USERID に指定されたユーザーで使用する RACF グループ。このフィールドは、空にするか、指定されたユーザーの取り消されていない有効なグループ接続を格納する必要があります。API_RSRL_USERID フィールドが空の場合、このフィールドは無視されます。

API_RSRL_TSQUEUE
出力データ用に CICS 一時ストレージ・キュー (TSQUEUE) を使用することを指定します。TSQUEUE 名の最大長は 16 文字で、ブランクまたはヌルを埋め込む必要があります。名前は、必ずリカバリー不能 MAIN ストレージ TSQUEUE の名前にしてください。 リカバリー可能 TSQUEUE はサポートされません。AUXILIARY ストレージ・キューを使用すると、補助ストレージに対する入出力が発生し、アプリケーションの応答時間に影響する可能性があります。関連するシステム・リソースを解放したい場合は、データを処理した後に、呼び出し側プログラムで TSQUEUE を削除する必要があります。API_RSRL_RETFLAG の値が T でも B でもない場合、このフィールドは無視されます。

API_RSRL_PREFIX
許可されたプロファイルのフィルター処理に使用する接頭部フィルターを指定します。接頭部の最大長は 16 文字で、ブランクまたはヌルを埋め込む必要があります。この接頭部は、プロファイルとの比較に使用されます (TSO SEARCH MASK キーワードの場合に使用される処理と同様です)。プロファイ

ル名の先頭文字は、接頭部フィルターに指定された文字に一致している必要があります。これらの文字が一致しない場合、プロファイルはスキップされ、プロファイルのリストから除外されます。

API_RSRL_RETFLAG
処理フラグを指定します。処理フラグには以下の値を使用できます。

C
出力データを COMMAREA に返します。見つかったエントリーの数は、API_RSRL_PROFCNT フィールドに表示されます。COMMAREA が小さすぎる場合、この数値は、COMMAREA 内のプロファイルの実際の数より大きくなることがあります。

T
出力データを指定された TSQUEUE に返します。見つかったエントリーの数は、API_RSRL_PROFCNT フィールドに表示されます。

B
出力データを、COMMAREA と、指定された TSQUEUE に返します。見つかったエントリーの数は、API_RSRL_PROFCNT フィールドに表示されます。

N
出力データは、COMMAREA にも指定の TSQUEUE にも返されません。ただし、返されるはずのエントリーの数は、API_RSRL_PROFCNT フィールドに表示されます。

API_RSRL_FL_PR
接頭部フィルターを使用して、リストされるプロファイルを制限します。指定可能な値は、Y または N です。それ以外の値は、N と同様に処理されます。

API_RSRL_FL_AC
出力データには、ユーザーが READ 権限以上の権限を持つプロファイルだけが常に格納されます。ユーザーがアクセス権限を持たないプロファイルが表示されることはありません。API_RSRL_FL_AC フラグを使用すると、返されるプロファイルの数を減らすことができます。このフラグに指定可能な値は、Y と N です。それ以外の値は、N と同様に処理されます。

このフラグの値が N の場合は、要求されたアクセス権限以上の権限をユーザーが持っている プロファイルだけが返されます。このフラグの値が Y の場合は、ユーザーが READ 権限以上の権限を持つすべてのプロファイルが返され、ユーザーが READ 権限しか持っていないか、あるいは要求された権限を持っているかが、プロファイル・フラグで示されます。

API_RSRL_ACCESS
ユーザーの必要最低限のアクセス権限を指定します。指定可能な値は、R (READ)、U (UPDATE)、C (CONTROL)、または A (ALTER) です。このフィールドが空であるか他の値が入っている場合は、値 R が指定されたものと見なしてアクセス権限が判別されます。ユーザーが持つアクセス権限が要求されたアクセス・レベル以上である場合は、プロファイル・フラグの値が A または B になります。要求されたアクセス権限をユーザーが持っていない場合は、プロファイル・フラグの値が N または G になります。

API_RSRL_PROFCNT
この出力フィールドには、リストされたエントリーの数が表示されます。応答域が十分に大きい場合は、返されたプロファイルの数が格納されます。応答域が小さすぎる場合は、応答域が十分に大きい場合に返されたはずのプロファイルの数が格納されます。

API_RSRL_PROFLST
commarea のこの部分には、許可されたプロファイルのリストが格納されます。これは、以下の形式を使用したプロファイルの配列から構成されます。

NAME LENGTH
プロファイル名の 2 バイト長。この値には、長さフィールド自体の長さと FLAG バイトの長さは含まれません。

FLAG
1 バイトのフラグ・フィールド。この戻りフラグの有効な値は以下のとおりです。

A
ユーザーは、要求されたアクセス・レベル以上の個別プロファイルに対するアクセス権限を持っています。

B
ユーザーは、要求されたアクセス・レベル以上の総称プロファイルに対するアクセス権限を持っています。

N
ユーザーは、個別プロファイルに対する要求されたアクセス権限を持っていません。ユーザーは、このプロファイルに対する READ 権限を持っています。

G
ユーザーは、総称プロファイルに対する要求されたアクセス権限を持っていません。 ユーザーは、このプロファイルに対する READ 権限を持っています。

PROFILE NAME
可変長のプロファイル名

ユーザーが READ 権限以上の権限を持つプロファイルを返すようにアプリケーションが要求した場合、返されるプロファイルのプロファイル・フラグの値は A または B になります。この場合、値 N と値 G は使用されません。要求されたアクセス権限が他の値である場合は、プロファイル・フラグの 4 つの値がすべて使用されます。

プロファイルのための TSQUEUE の使用

アプリケーションが **API_RSRL_RETFLAG** フィールドに **T** または **B** のいずれかの値を指定した場合、**API_RSRL_TSQUEUE** フィールドに指定された TSQUEUE にプロファイルが返されます。

TSQUEUE は、リカバリー不能 MAIN ストレージ TSQUEUE でなければなりません。 リカバリー可能 TSQUEUE はサポートされません。AUXILIARY ストレージ・キューの使用はお勧めしません。補助ストレージに対する入出力が発生し、アプリケーションの応答時間に影響する可能性があるためです。API プログラムは、レコードを書き込む前に TSQUEUE 全体を消去します。関連するシステム・リソースを解放したい場合は、データを処理した後に、呼び出し側プログラムで TSQUEUE を削除する必要があります。

要求されたプロファイルは、それぞれ個別のレコードに書き込まれます。このレコードのレイアウトは、前出のリストに示した API_RSRL_PROFLST のレイアウトと同じです。

戻りコードと理由コード

この API によって返される戻りコードと理由コードには、この関数固有のコードや、RACF によって使用される IRRPNL00 関数のコードがあります。

固有の戻りコードと理由コードを、以下に要約します。IRRPNL00 関数の戻りコードと理由コードについて詳しくは、「*z/OS Security Server RACF* マクロおよびインターフェース」を参照してください。

RC=00
エラーは発生しませんでした。要求されたプロファイルは、指定された領域内で提供されます。

RC=04
IRRPNL00 の戻りコードと理由コードを参照してください。

RC=08
IRRPNL00 の戻りコードと理由コードを参照してください。

RC=0C

REAS=00 許可されたプロファイルの処理に使用される内部作業域が小さすぎます。128K バイト未満のデータを必要とするプロファイル・リスト要求しか処理できません。
REAS=04 プロファイルを TSQUEUE に返すように要求されましたが、TSQUEUE の名前が指定されていません。
REAS=08 端末ユーザーが、指定された TSQUEUE 名に対するアクセス権限を持っていません。
REAS=0C 用意された COMMAREA が小さすぎるため、許可されたプロファイルをすべて格納することができません。

RC=14 から RC=24
IRRPNL00 の戻りコードと理由コードを参照してください。

RC=32
指定されたユーザーに対する RACROUTE REQUEST=VERIFY が失敗しました。RACF の戻りコードと理由コードについては、メッセージ CQT030 を参照してください。

アクセス権限検査およびデータ取得 (RSRD)

RSRD 機能を使用して、ユーザー ID のアクセス権限指定に関連する USERDATA を取得できます。

ユーザー・アクセス権限は、個別の許可、グループ接続、ID(*) へのアクセス権限、または UACC を介して付与できます。該当するプロファイル内の USERDATA フィールドに、一致するエントリーが定義されている場合、関連する DATA が API 関数の呼び出し元に返されます。

USERDATA の取得

USERDATA は、クラスのリソース・プロファイルの RACLIST 処理中に使用された、最も具体的またはアルファベット順で最高位のメンバー・クラス・プロファイルまたはグループ化クラス・プロファイルから、アルファベット順で最高位にあり、最適の ACL エントリーについて取得されます。

USERDATA を取得する場所を判別するため、以下の項目が順番にチェックされます。

1. ユーザー ID に対する直接の許可。
2. ユーザー ID の接続先グループを介した間接的な許可。
3. アクセス権限が複数のグループを介して付与されている場合は、アルファベット順に最高位のグループ。
4. ID(*) を介して付与されたアクセス権限。
5. UACC を介して付与されたアクセス権限。
6. メンバー・クラス・プロファイルおよび 1 つ以上のグループ化クラス・プロファイルを介してアクセス権限が付与されている場合は、メンバー・クラス・プロファイル。
7. アクセス権限が複数のグループ化クラス・プロファイルを介して付与されている場合は、アルファベット順に最高位のグループ化クラス・プロファイル。

この戦略を、例を使ってわかりやすく説明します。 この最初の例の目的は、主に USERDATA の取得元プロファイルを示すことです。それ以降の例では、要求された DATA の探索に使用する USERDATA エントリーを決定することに焦点を当てています。

例として、リソース・クラス $GROUP および $MEMBER に以下のプロファイルが定義されているとします。

```
$GROUP GRPA Addmem(MEMA,MEMB) READ(USER1,USER2,GROUP1)
$GROUP GRPB Addmem(MEMA,MEMC) READ(USER1,USER3,GROUP2)
$MEMBER MEMA READ(USER4)
USER1 CONNECT(GROUP1,GROUP2)
USER2 CONNECT(GROUP1)
USER3 CONNECT(GROUP2)
USER4 CONNECT(GROUP4)
USER5 CONNECT(GROUP1,GROUP2)
```

リソース MEMA およびユーザー USER2 に対して RSRD API を呼び出すと、API 関数は USER2 にアクセス権限があるかどうかをチェックします。このユーザーには直接許可があるため、USER2 の USERDATA エントリーが取得されます。 また、USER2 には 1 つのプロファイルのみへのアクセス権限があります。したがって、その単一プロファイル $GROUP GRPA から USERDATA が取得されます。

MEMA およびユーザー USER1 に対して API を呼び出すと、API 関数は USER1 がプロファイル $GROUP GRPA および $GROUP GRPB を介してアクセス権限が付与されていることを検出します。両方のプロファイルに関連する ACL エントリーは同じ (USER1) です。 この場合、最高位のアルファベット順位を持つプロファイルが使用されます。したがって、プロファイル $GROUP GRPB から USERDATA が取得されます。

MEMA にアクセスする USER5 の場合、アクセス権限はグループ GROUP1 および GROUP2 を介して付与されています。2 つの異なるグループ化クラス・プロファイルが関係しており、アクセス権限は 2 つの異な

る GROUP を介して付与されています。異なる GROUP がアクセス権限を付与する場合、アルファベット順で最高位のグループ (GROUP2) が使用されます。

USER4 から MEMA へのアクセスの場合、関連するプロファイルは $MEMBER MEMA の 1 つのみです。

以下の表に、利用可能な USERDATA の取得に使用されるプロファイルを示します。

表 *8. USERDATA* の取得に使用されるプロファイル

ユーザー	**MEMA**	**MEMB**	**MEMC**
USER1	GRPB/USER1	GRPA/USER1	GRPB/USER1
USER2	GRPA/USER2	GRPA/USER2	なし
USER3	GRPB/USER3	なし	GRPB/USER3
USER4	MEMA/USER4	なし	なし
USER5	GRPB/GROUP2	GRPA/GROUP1	GRPB/GROUP2

アクセス権限を特定のレベルでチェックすることを API パラメーター・リストに指定することができます。このアクセス・レベルはアクセス権限の検査プロセスに使用されますが、最も適切な USERDATA エントリーを判別するためには使用されません。したがって、USER5 に GROUP1 を介する UPDATE アクセス権限と GROUP2 を介する READ アクセス権限がある場合、実際のアクセス権限は GROUP1 を介して付与されていても、常に GROUP2 の USERDATA が取得されます。

USERDATA エントリーの定義

USERDATA エントリーは、USRNM および USRDATA の 2 つの部分から構成されます。USRNM は、関連する USRDATA を見つけるためのインデックスとして使用されます。

この資料の残りの部分で、USRDATA という用語は RACF データベース内のデータ値フィールドを指すために使用し、USERDATA という用語は 2 つのフィールドの組み合わせを指すために使用します。

USERDATA は、例えば zSecure Admin の CKGRACF 機能を使用することで、RACF プロファイルに入力できます。 RSRD 機能を正しく実装するには、各 ACL エントリーが USERDATA エントリーによってミラーリングされている必要があります。追加の USERDATA エントリーは、UACC と、ID(*) を介して付与されたアクセス権限について定義できます。UACC 用に定義されるエントリーは -UACC- の USRNM で表され、ID(*) を介して付与されるアクセス権限用のエントリーは -STAR- の USRNM で表されます。 ACCESS=NONE であるユーザーまたはグループの ACL エントリーは、USERDATA エントリーで表してはいけません。

USRDATA には、これらの値をプロファイルに追加する際に使用するツールでサポートされている、任意の文字を含めることができます。 zSecure CICS Toolkit の RSRD 機能は、使用する文字に何の制限も課しません。 埋め込みブランクは許可されています。RSRD からアプリケーションに返される USRDATA の最大長は 64 文字です。

注 : 前述したように、RSRD 機能を正しく実装するには、NONE 以外のアクセス権限を持つ各 ACL エントリーが USERDATA エントリーによってミラーリングされている必要があります。 RSRD 機能は、情報が欠落している不整合を検出します。 ただし、一部のタイプの不整合は検出されないため、予期しない結果になる場合があります。例えば、アクセス権限を付与したメンバー・クラス・プロファイルで USERDATA エントリーが欠落しているが、適用可能なグループ化クラス・プロファイルのいずれかには存在する場合は、正しい USERDATA エントリーの欠落が検出されない可能性があります。 別の例としては、GROUP のデータが予期されていたときに ID(*) の DATA が返される場合が挙げられます。

その他の考慮事項

RSRD 機能を使用する場合は、このトピック内の情報も考慮してください。

リソース名は最大 246 文字にすることができますが、リソースへのアクセスの定義に使用されるプロファイル名は最大 40 文字です。これを超えるプロファイル名を使用すると、40 文字目の位置で切り捨てられます。プロファイルの切り捨てが発生すると、USERDATA について返される値は未定義になります。

グループ化クラス・プロファイルが使用されている場合、RSRD 機能の処理では、そのグループ化クラス・プロファイルの名前を判別する必要があります。ただし、SETROPTS RACLIST の処理中は、グループ化クラス・プロファイルの名前は除去され、メモリー内で使用できなくなります。グループ化クラス・プロファイルの代わりに、RSRD 機能はプロファイルの APPLDATA を使用します。APPLDATA は、SETROPTS RACLIST 処理中に作成されたメモリー内プロファイルに保持されます。RSRD 機能にプロファイル名を指定するには、プロファイル名をプロファイル自体の APPLDATA に指定する必要があります。 メンバー・クラス・プロファイルでは必要ありませんが、メンバー・クラス・プロファイルの APPLDATA にプロファイル名を追加することもサポートされています。そのような定義の例を以下に示します。

```
RDEFINE $GROUP GRP1 ADDMEM(RES1,RES2) APPLDATA('GRP1')
RDEFINE $GROUP GRP2 ADDMEM(RES3,RES4) APPLDATA('GRP2')
RDEFINE $MEMBER RES5 APPLDATA('RES5')
```

これらの定義の結果、RACLIST 処理中に以下のメモリー内論理プロファイルが作成されます。

```
$MEMBER RES1 APPLDATA(GRP1)
$MEMBER RES2 APPLDATA(GRP1)
$MEMBER RES3 APPLDATA(GRP2)
$MEMBER RES4 APPLDATA(GRP2)
$MEMBER RES5 APPLDATA(RES5)
```

この方法を使用すると、RSRD 機能は APPLDATA を使用して正しいグループ化クラス・プロファイルを見つけることができます。例えば、リソース RES1 のデータは、クラス $GROUP 内のプロファイル GRP1 から取得できます。

複数のグループ化クラス・プロファイル内で同じリソースがメンバーとして定義されている場合、APPLDATA の使用では不十分です。 RACLIST プロセス中に、プロファイルはメモリー内 (論理) プロファイルに結合されます。ただし、APPLDATA の値は 1 つしか保持されません。89 ページの『USERDATA の取得』で説明したプロファイル例を使用して、以下のメモリー内プロファイルが作成されます。

```
$MEMBER MEMA APPLDATA(MEMA) READ(USER1,USER2,USER3,USER4,GROUP1,GROUP2)
$MEMBER MEMB APPLDATA(GRPA) READ(USER1,USER2,GROUP1)
$MEMBER MEMC APPLDATA(GRPB) READ(USER1,USER3,GROUP2)
```

RACLIST プロセス中には、1 つの APPLDATA 値しか保持されません。例えば、MEMA のメモリー内論理プロファイルには MEMA の APPLDATA 値のみが含まれており、GRPA および GRPB の情報は使用できません。この状態は、RACLIST 出口を実装することで改善できます。91 ページの『RACLIST 出口の使用』を参照してください。

RACLIST 出口の使用

複数のグループ化クラス・プロファイルに定義されているメンバーに対応するために、RACLIST 出口を活用できます。

(複数のグループ化クラス・プロファイルに定義されているメンバーに対応する例は、89 ページの『USERDATA の取得』を参照してください。)

zSecure CICS Toolkit には、この目的で 2 つの RACLIST 出口が用意されています。

ICHRLX01
RACLIST プリプロセッシング出口およびポストプロセッシング出口。RACLIST 処理されているリソース・クラスに特別な処理が必要かどうかを判断する際に使用します。XFACILIT リソース・クラス内のプロファイル ICHRLX02.PROCESS.CLASS の APPLDATA にクラス名が含まれている場合、そのリソース・クラスは特殊な RACLIST 処理に適格です。このプロファイルの例を次に示します。

```
RDEFINE XFACILIT ICHRLX02.PROCESS.CLASS APPLDATA('$MEMBER')
```

ICHRLX02
RACLIST 選択または処理の出口。この実装では、メモリー内プロファイルの APPLDATA が更新されて、メモリー内論理プロファイルに貢献するすべてのプロファイルのリストが含まれています。RACF データベース自体の中にあるプロファイルは、この出口の影響を受けません。

RACLIST または SETROPTS REFRESH RACLIST コマンド時に両方の出口がアクティブである場合、以下のメモリー内論理プロファイルが作成されます。

```
$MEMBER MEMA APPLDATA(MEMA GRPB GRPA) READ(USER1,USER2,USER3,USER4,GROUP1,GROUP2)
$MEMBER MEMB APPLDATA(GRPA) READ(USER1,USER2,GROUP1)
$MEMBER MEMC APPLDATA(GRPB) READ(USER1,USER3,GROUP2)
```

唯一の相違点はメモリー内の APPLDATA の値であることに注意してください。 ここには、貢献するすべてのプロファイルのリストが含まれています。

これらの RACLIST 出口を使用する場合は、RACF データベース内のプロファイルに APPLDATA 値を指定する必要がなくなりました。 出口はプロファイル名を直接使用して、RSRD 機能が使用するメモリー内リストを作成します。

制約事項

提供される RACLIST を使用して、複数のグループ化クラス・プロファイルまたはメンバー・クラス・プロファイルの一部としての同じメンバーの定義をサポートする際に、以下の制限が適用されます。

- リソースのメモリー内プロファイルに貢献するプロファイル名の合計の長さは、255 バイトを超えられません。それより多い文字が必要な場合、一部のプロファイル名は切り捨てられます。
- 単一リソースの効果的な保護を定義するには、最大 16 個のグループ化およびメンバー・クラス・プロファイルを使用できます。それより多いプロファイルを使用する場合、一部のプロファイル名は無視されます。
- 各プロファイル名の最大長は、40 文字です。 プロファイル名の文字がそれより多い場合、プロファイル名は切り捨てられます。

API 仕様

このセクションでは、RSRD API 関数に必要な COMMAREA について説明します。

FUNCTION
ユーザーがリソースへのアクセス権限を持っているかどうかをチェックし、USERDATA の関連する値を取得します。

AUTHORITY
不要です。

COMMAREA
最小サイズは 412 バイトです。

アプリケーションでは、SCQTSAMP ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC        DC  CL4'RSRD'  Function code for access check
API_RC          DC  XL01'00'   Return code
*                              On input, the following values are supported
*                              "S" Suppress ICH408I messages for violations
*                              "N" Suppress ICH408I messages and SMF Audit
API_MSG         DC  CL79' '    Message area
*
API_RSRD_USERID DC  CL8        Userid for which the access must be
*                              checked and for which the associated
*                              USRDATA must be retrieved.
*                              If blank, the ACEE of the userid signed
*                              on at the terminal is used. On return,
*                              this field contains the id that was used
*                              to retrieve the associated USRDATA.
*
API_RSRD_ACC    DC  Cl1        The required access level. Valid values are
*                              'R' (read),'U' (update), 'C' (control) or
*                              'A' (alter). Read is the default.
*                              On return, this field contains the
*                              return code from the function.
*
API_RSRD_CLASS  DC  CL8        This field specifies the resource class
*                              for the resource. This class must be
*                              RACLISTed through SETROPTS RACLIST. On
*                              return this field contains the resource
*                              class of the matching profile.
```

```
*
API_RSRD_NAMEL  DS  XL1        Length of the resource name. The specified
*                              length can be greater than the actual
*                              resource name, provided it is padded with
*                              blanks up to the specified length.
*
API_RSRD_NAME   DS  CL246      Name of the resource. On return, this field
*                              contains the name of the profile used.
*
API_RSRD_DATA   DS  CL64       On return, this field contains the USRDATA
*                              associated with the userid.
```

COMMAREA 内のほとんどのフィールドは、入出力に使用されます。出力時に、API_RSRD_CLASS および API_RSRD_NAME は API_RSRD_DATA の取得に使用したプロファイルを反映します。 また、API_RSRD_USERID には、API_RSRD_DATA の取得に使用した USERDATA 内の USRNM インデックスの値も含まれています。 ほとんどのフィールドは処理の一環として更新されるため、呼び出しごとに COMMAREA 全体を再初期化する必要があります。

SMF レコードを使用したアクセス権限検査の監査は、RACF プロファイルの AUDIT 設定に基づいて、または RACF SETROPTS LOGOPTIONS を介して行われます。システム・コンソールと CICS ログに ICH408I リソース・アクセス違反メッセージを出力したくない場合は、API_RC フィールドに値「S」を指定します。この値を指定した場合、アクセス違反があった場合に表示されるメッセージは出力されなくなりますが、それらの違反に関する SMF レコードは作成されます。API_RC フィールドに値「N」を指定することもできます。 この場合、ICH408I リソース・アクセス違反メッセージと SMF 監査の両方が抑止されます。「S」も「N」の文字も指定しない場合は、CQTPCNTL の設定に応じて、メッセージおよび SMF レコードを抑止できます。

戻りコード
戻りコードは、フィールド API_RSRD_ACC に返されます。

以下のリストで、戻りコードは 1 バイトの 16 進フィールドで示され、以下の意味を持ちます。

X'00'
リソースへのアクセスが許可されています。API COMMAREA は関連する USRDATA について取得された情報で更新されます。

X'04'
リソースが RACF に対して定義されていません。

X'08'
ユーザーは、指定されたアクセス・レベルでのリソースの使用を許可されていません。

X'0C'
USRDATA の指定エラーです。ユーザーは指定されたリソースへのアクセス権限を持っていますが、関連する USRDATA 値が見つかりませんでした。

X'10'
USERID の指定エラーです。API COMMAREA に指定されたユーザー ID が使用できませんでした。このユーザー ID のセキュリティー環境のセットアップが失敗した理由についての詳細は、システム・ログで対応する ICH408I メッセージを確認してください。

X'14'
プロファイルの整合性エラーです。RSRD 機能は、ストレージ内にある APPLDATA フィールドの情報を使用して、RACLISTed メモリー内プロファイルに貢献するグループ化クラス・プロファイルの名前を判別します。APPLDATA の情報が誤っており、存在しないプロファイル名が含まれています。

X'18'
CLASS の指定エラーです。API COMMAREA に指定されたリソース・クラスがシステムに 見つかりません。

インストールの注意点

RACLIST 出口を使用する場合は、最初の RACLIST または SETROPTS RACLIST REFRESH の実行時に出口をアクティブにする必要があります。

適切な時点でこれらの出口をアクティブにするには、RACF 名 ICHRLX*nn* を使用して SYSTEM ライブラリーに提供されている出口をインストールするか、zSecure Exit Activator 機能 (プログラム C2XACTV) を使用

してから SETROPTS RACLIST REFRESH コマンドを実行します。C2XACTV プログラムは、zSecure Admin、zSecure Audit、および zSecure Alert 製品の一部として提供されています。

複数の LPAR で同じリソース・クラスが使用され、RACF シスプレックス通信が有効になっている場合は、シスプレックス内のすべてのシステムに RACLIST 出口をインストールしてアクティブにする 必要があります。

現行のリソース・クラスを処理する必要がある場合、ICHRLX01 出口は、出口パラメーター・リストのオフセット 48 (X'30') にあるワードを使用して、ICHRLX02 出口と通信します。独自の RACLIST 出口が設定されている場合、同じ通信域は使用できません。

提供されている出口を通常の RACF 出口として使用することがサポートされるのは、現在アクティブな RACLIST 出口がない場合のみです。そうでない場合は、使用中の出口は前述の通信域を使用できないため、zSecure CICS Toolkit に付属の出口を呼び出すように、ご使用の出口を変更する必要があります。また、ICHRLX01 出口は、UACC、UADIT、GLOBALAUDIT、INSTDATA、および APPLDATA フィールドにデフォルト以外の RACLIST マージ規則を指定できません。

通常の RACF 出口としてインストールするには、以下の手順に従います。

1. 提供されている出口ルーチンを、CQTRLX01 および CQTRLX02 から ICHRLX01 および ICHRLX02 に名前変更します。 C2XRLZ*xx* ルーチンは使用しません。
2. 出口ルーチン ICHRLX01 および ICHRLX02 を LPALIST データ・セット (例えば zSecure CICS Toolkit SCQTLPA) にコピーします。
3. CLPA を使用してシステムで IPL を実行します。
4. 必要なリソース・クラスが RACLISTed としてセットアップされていることを確認します。

zSecure Exit Activator プログラムを使用して出口をインストールするには、以下の手順に従います。

1. zSecure Admin および zSecure CICS Toolkit のロード・ライブラリーを steplib として連結して、以下のようなジョブを実行します。

```
//C2XACTV EXEC PGM=C2XACTV
//STEPLIB DD DISP=SHR,DSN=<ZSECURE.SCQTLOAD>
//        DD DISP=SHR,DSN=<ZSECURE.SCKRLOAD>
//SYSTSPRT DD SYSOUT=*
//C2XPRINT DD SYSOUT=*
//C2XIN DD *
DYNEXIT DEACTIVATE ICHRLX01 DIRECT
DYNEXIT RECOVER ICHRLX01 DIRECT
DYNEXIT ACTIVATE ICHRLX01 DIRECT
DYNEXIT DEACTIVATE ICHRLX02 DIRECT
DYNEXIT RECOVER ICHRLX02 DIRECT
DYNEXIT ACTIVATE ICHRLX02 DIRECT
```

   このジョブを実行するユーザー ID には、以下のプロファイルへの UPDATE 権限が必要です。

```
XFACILIT C2X.ICHRLX01
XFACILIT C2X.ICHRLX02
```

2. 必要なリソース・クラスで SETROPTS RACLIST または SETROPTS RACLIST REFRESH を実行します。

提供されている RACLIST 出口は、プロファイルが XFACILIT リソース・クラスに定義されていないかぎり処理を実行しません。プロファイルの APPLDATA は、zSecure CICS Toolkit RSRD 機能で使用されるメモリー内 APPLDATA 値を出口が作成する必要があるリソース・クラスを指定します。このプロファイルの例を次に示します。

```
RDEFINE XFACILIT ICHRLX02.PROCESS.CLASS APPLDATA('$MEMBER')
```

ADDGROUP/ALTGROUP/DELGROUP 関数 (グループの追加、変更、または削除)

ADDGROUP、ALTGROUP、および DELGROUP 関数を使用して、システムへの新規グループの追加、または既存のグループの変更または削除を行います。

AUTHORITY

ユーザーは、zSecure CICS Toolkit コマンド (実行するコマンドに応じて、**TOOLKIT.ADGR/TOOLKIT.ALGR/TOOLKIT.DELG/TOOLKIT.LGRP**) に対するアクセス権限、およびグループ (ADGR.*grpname*/ALGR.*grpname*/DELG.*grpname*/LGRP.*grpname*) に対するアクセス権限を持っている必要があります。

COMMAREA

汎用グループをサポートするため、この関数の場合の最小サイズは 370 バイトになっています。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC           DC  CL4'ADGR'  Function code
API_RC             DC  XL01'00'   Return code
API_MSG            DC  CL79' '    Message area
*
API_AGRP_RC        DC  XL1        Return code from requested command
*                                 If non-zero the command failed.
*                                 API_MSG will give the reason for the failure.
*
API_AGRP_CODE1     DC  CL4"xxxx" 'ADGR' for ADDGROUP
*                                'ALGR' for ALTGROUP
*                                'DELG' for DELGROUP
*                                'LGRP' for LISTGROUP

*API_AGRP_GROUP    DC  CL8       Group name.
*
API_AGRP_OWNER     DC  CL8       Owner name
*
API_AGRP_SUPGRUP   DC  CL8       Superior Group name
*
API_AGRP_TERMUAC   DC  CL1       Terminal UACC ('Y' or 'N')
*
API_AGRP_INSTDATA  DC  CL255     Installation data
*
API_AGRP_UNIVERS   DC  CL1       Universal Group ('Y' or 'N')
*
```

グループに関する情報を取得するには、API_AGRP_CODE1 フィールドに **LGRP** を入力します。データを変更する場合、ブランクのフィールドは無視され、更新されません。インストール・データ・フィールドを削除するには、先頭バイトを 2 進ゼロ (X'00') に設定します。

ADDUSER 関数 (ユーザー・プロファイルの追加)

ADDUSER 関数を使用して新しいユーザー・プロファイルをシステムに追加します。

AUTHORITY

ユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.ADUS) に対するアクセス権限と、追加するユーザーのデフォルト・グループ (ADUS.*dfltgrp*) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは 408 バイトです。

CICS セグメントの自動作成 (現在はサポートされていません) 用のスペースをアプリケーションで 予約する場合に必要なサイズは 495 バイトです。

パスフレーズを指定する必要がある場合に必要なサイズは 595 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC         DC  CL4'ADUS'   Function code for ADDUSER
API_RC
                 DC  XL01'00'    Return code
API_MSG          DC  CL79' '     Message area
*
API_ADUS_RC     DC  XL1         Return code from ADDUSER.
*                               If non-zero the command failed.
*                               API_MSG will give the reason for the failure.
*
API_ADUS_USERID   DC  CL8         Userid being added.
API_ADUS_PGMRNAME DC  CL20        Users name.
*
API_ADUS_DFLTGRP  DC  CL8         The users default group.
*
API_ADUS_AUTHRTY  DC  CL1         Authority in the default group.
*                                 Must be 'U' (use)
                                  or 'C' (create).
*
API_ADUS_SMTWTFS  DC  CL7         The days of the week the user can
                                  logon.
*                                 Specify 'Y' for each
*                                 day the user may logon and 'N'
*                                 for the days they may not.
*
API_ADUS_FROM     DC  CL4         The time of day the user can logon
*                                 from (24 hour clock).
*
API_ADUS_TILL     DC  CL4         The time of day the user can logon
*                                 till (24 hour clock).
*
API_ADUS_INSTDATA DC  CL255       Installation data field.
*
API_ADUS_PASSWORD DC  CL8         Initial password for the user.
*                                 If it is omitted, the password
                                  defaults to the users default
                                  group.
*
API_ADUS_OWNER    DC  CL8         The owner of the profile.
*
*  THE FOLLOWING FIELDS ARE USED FOR AUTOMATIC ADD
*   OF CICS SEGMENT. THIS IS NO LONGER SUPPORTED. THE FIELDS
*   SHOULD BE BLANKS OR NULLS.
*
API_ADUS_OPIDENT  DC  CL3         Retained for compatibility
API_ADUS_OPPRTY   DC  CL3         Retained for compatibility
API_ADUS_TIMEOUT  DC  CL3         Retained for compatibility
API_ADUS_XRFSOFF  DC  CL7         Retained for compatibility
API_ADUS_OPCLASS  DC  CL71        Retained for compatibility
*
API_ADUS_PHRASE   DC  CL100       The password phrase of
*                                 the userid.
```

ユーザー・プロファイルを作成するときに値を指定しなかった場合、そのユーザーの初期パスワードは DEFAULT GROUP という値に設定されます。

ユーザーが初めてログオンするときは、新規パスワードを入力する必要があります。

ALTUSER 関数 (プロファイルの変更)

ALTUSER 関数を使用して特定のユーザーのプロファイルを変更します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、対象のユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。

一部のフィールドについては、ユーザーがシステムの特殊なアクセス権限または TOOLKIT.SPEC に対するアクセス権限も持っている必要があります。これらのフィールドには、アスタリスク (*) のマークが付いています。

COMMAREA

最小サイズは 487 バイトです。

パスフレーズを指定する必要がある場合に必要なサイズは 587 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC  CL4'AUSR'   Function code for ALTUSER
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_ALUS_RC       DC  XL1         Return code from ALTUSER
*                                 If non-zero the command failed.
*                                 API_MSG  will give the reason for
*                                 the failure.
*
API_ALUS_USERID   DC  CL8         The userid to be altered.
API_ALUS_PASSWRD  DC  CL8         Password
API_ALUS_RESUME   DC  CL1         Resume the userid (Y or N)
API_ALUS_PGMRNAME DC  CL20        Name
API_ALUS_INSTDATA DC  CL255       Installation data field.
API_ALUS_DFLTGRP  DC  CL8         Default group.
API_ALUS_REVOKED  DC  CL5         Revoke Date(YYDDD).
API_ALUS_RESUMED  DC  CL5         Resume Date(YYDDD).
API_ALUS_AUTHOR   DS  CL8         * OWNER
API_ALUS_GRPACC   DC  CL1         * Group access.
API_ALUS_ADSP     DC  CL1         * ADSP.
API_ALUS_SPEC     DC  CL1         * Special
API_ALUS_OPER     DC  CL1         * Operations
API_ALUS_AUDITOR  DC  CL1         * Auditor
API_ALUS_RESTR    DC  CL1         * UACC and similar not used.
API_ALUS_PROTECT  DC  CL1         * Password cannot be used.
API_ALUS_UAUDIT   DC  CL1         * Audit all RACHECK's/RACDEF's.
API_ALUS_LOGDAY   DC  CL7         * Days user can logon.
API_ALUS_LOGFROM  DC  CL4         * Starting time for logon.
API_ALUS_LOGTILL  DC  CL4         * Latest time for logon.
API_ALUS_MODEL    DC  CL44        * Dataset profile model.
API_ALUS_CLAUTH   DC  CL8         * Give class authority.
*API-ALUS-AUTH                   Name used in COBOL copybook
API_ALUS_NOCLAUTH DC  CL8         * Remove class authority.
*API-ALUS-NAUTH                  Name used in COBOL copybook
API_ALUS_PASSEXP  DC  CL1         * New password is expired (Y or N).
API_ALUS_PHRASE   DC  CL100       The password phrase of the userid.
*
```

commarea のフィールドは、2 進ゼロに初期化する必要があります。変更するフィールドのみ、データを格納する必要があります。フィールドの説明と、どのユーザーがどのフィールドを更新できるかの制限については、31 ページの『第 5 章 zSecure CICS Toolkit コマンド・インターフェース』を参照してください。CQTPAPI0 に リンクすると、2 進ゼロ以外のすべてのフィールドに 含まれている情報によって、ユーザー・プロファイルが更新されます。

パスフレーズの削除を指定するには、値として 100 個のブランクを指定します。それ以外の値を指定した場合、パスフレーズは指定の値に変更されるか、現在の値のまま保持されます。

特殊なゼロ日付 (c'00000' = x'F0F0F0F0F0') を使用すると、取り消し日や再開日を削除できます。この特殊値を使用すると、z/OS 1.7 RACF **ALTUSER** コマンドの NOREVOKE キーワードおよび NORESUME キーワードと同様の機能を実装することができます。

ALTUSER (CICS SEGMENT) 関数 (CICS セグメントの変更)

ALTUSER (CICS SEGMENT) 関数を使用して、特定のユーザーの CICS セグメントを変更します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、このユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。 また、CICS セグメントを管理する場合、ユーザーは TOOLKIT.ACIC に対するアクセス権限も持っている必要があります。Consul zToolkit バージョン 1.4 では、この要件が適用されるのは、TOOLKIT.ACIC プロファイルが定義されているか、総称プロファイルによってカバーされている場合だけでした。zSecure CICS Toolkit バージョン 1.8.1 以降では、リソース TOOLKIT.ACIC に対するアクセス権限が必要になります。

COMMAREA

最小サイズは 184 バイトです。アプリケーションで TSLKEY と RSLKEY にアクセスする必要がある場合の必要最小サイズは 316 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC               DC  CL4'ACIC'   Function code for CICS segment.
*                      For compatibity reasons, ACSG is also accepted
API_RC                 DC  XL01'00'    Return code
API_MSG                DC  CL79' '     Message area
*
API_ACSG_RC            DC  XL1         Return code from ALTUSER. If
*                                      non-zero the command failed.
*                                      API_MSG will give the reason for
*                                      the failure.
*
API_ACSG_CODE          DC  CL4         Specify LIST to retrieve the current
*                                      specifications for the user. See LISTUSER
*                                      (TSO/CICS)
*                                      UPDT to update the CICS segment
*                                      with the values in the COMMAREA.
*                                      DELT to delete the CICS segment.
API_ACSG_USERID        DC  CL8         The userid to be listed/updated.
API_ACSG_OPIDENT       DC  CL3         Three character opident
API_ACSG_OPPRTY        DC  CL3         Operator priority (000-255)
API_ACSG_TIMEOUT       DC  CL3         See ALTUSER command
API_ACSG_XRFSOFF       DC  CL7         FORCE or NOFORCE
API_ACSG_OPCLASS       DC  CL71        Operator classes (01-24, separated by a
*                                      comma, e.g.; 01,03,04)
API_ACSG_TSLKEY  DS  CL66              TSL KEYS (00, 99, or 01-64, separated
*                                      by a comma, e.g.; 01,03,04)
API_ACSG_RSLKEY  DS  CL66              RSL KEYS (00, 99, or 01-24, separated
*                                      by a comma, e.g.; 01,03,04)
```

CICS セグメントを更新すると、CICS セグメント内のすべてのフィールドが置き換えられます。そのため、すべてのパラメーターに対して、有効なデータを指定する必要があります。

注 : 現在のリリースの zSecure CICS Toolkit は、22 個の TSLKEY 値と RSLKEY 値を格納できるだけのスペースが、TSLKEY 値と RSLKEY 値に指定されているかどうかについては検査しません。

ALTUSER (TSO SEGMENT) 関数 (TSO セグメントの変更)

ALTUSER (TSO SEGMENT) 関数を使用して特定のユーザーの TSO セグメントを変更します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、このユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。 また、TSO セグメントを管理する場合、ユーザーは TOOLKIT.ATSO に対するアクセス権限も持っている必要があります。Consul zToolkit バージョン 1.4 では、この要件が適用されるのは、TOOLKIT.ATSO プロファイルが定義されている (または総称プロファイルによってカバーされている) 場合だけでした。zSecure CICS Toolkit バージョン 1.8.1 以降では、リソース TOOLKIT.ATSO に対するアクセス権限が必要になります。

COMMAREA

最小サイズは 191 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC               DC  CL4'ATSO'   Function code for TSO segment.
*                      For compatibity reasons, ATSG is also accepted
API_RC                 DC  XL01'00'    Return code
API_MSG                DC  CL79' '     Message area
*
API_ATSG_RC            DC  XL1         Return code from ALTUSER. If
*                                      non-zero the command failed.
*                                      API_MSG will give the reason for
*                                      the failure.
*
API_ATSG_CODE          DC  CL4         Specify LIST to retrieve the current
*                                      specifications for the user.
*                                      See LISTUSER (TSO/CICS)
*                                      UPDT to update the TSO segment
*                                      with the values in the COMMAREA.
*                                      DELT to delete the TSO segment.
API_ATSG_USERID        DC  CL8         The userid to be listed/updated.
API_ATSG_ACCTNUM       DC  CL40        The account number
```

```
API_ATSG_DESTID        DC  CL8         The destination id.
API_ATSG_HCLASS        DC  CL1         The hold class.
API_ATSG_JCLASS        DC  CL1         The job class.
API_ATSG_MSGCLASS      DC  CL1         The message class.
API_ATSG_SCLASS        DC  CL1         The sysout class.
API_ATSG_SECLABL       DC  CL8         The security label.
API_ATSG_SIZE          DC  CL7         The region size.
API_ATSG_MAXSIZE       DC  CL7         The maximum region size.
API_ATSG_PROC          DC  CL8         The logon proc.
API_ATSG_UNIT          DC  CL8         The allocation device.
API_ATSG_UDATA         DC  CL4         The installation data.
```

TSO セグメントを更新すると、TSO セグメント内のすべてのフィールドが置き換えられます。そのため、すべてのパラメーターに対して、有効なデータを指定する必要があります。フィールドが空 (ブランクまたはヌル) になっていると、TSO セグメント内の対応するフィールドが削除されます。

ALTUSER (OMVS SEGMENT) 関数 (OMVS セグメントの変更)

ALTUSER (OMVS SEGMENT) 関数を使用して特定のユーザーの OMVS セグメントを変更します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、このユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。 また、OMVS セグメントを管理する場合、ユーザーは TOOLKIT.AOMV に対するアクセス権限も持っている必要があります。

COMMAREA

最小サイズは 273 バイトです。アプリケーションで MEMLIM フィールドと SHMMAX フィールドにアクセスする場合の最小サイズは 291 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC  CL4'AOMV'   Function code for OMVS segment.
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_AOMV_RC       DS   XL01             Return code from command
*
API_AOMV_CODE     DS   CL04             UPDT = Update segment
*                                      LIST = Retrieve segment
*                                      DELT = Delete segment
API_AOMV_USERID   DS  CL08             The userid
API_AOMV_UID      DS  CL10             UID (1-10# Left align, AUTOUID)
API_AOMV_SHARED   DS  CL01             Shared UID N/Y
API_AOMV_MKDIR    DS  CL01             MKDIR N/Y
API_AOMV_HOME     DS  CL60             HOME (1-60 CHARS) mixed case
API_AOMV_PROGRAM  DS  CL60             SHELL PROGRAM (1-60 CHARS)
API_AOMV_ASSIZE   DS  CL10             ASSIZEMAX (1-10 Digits left al)
API_AOMV_CPUTIME  DS  CL10             CPUTIMEMAX  (1-10 Idem)
API_AOMV_FILEPROC DS  CL06             FILEPROCMAX (1-6 Idem)
API_AOMV_MMAPAREA DS  CL08             MMAPAREA    (1-8 Idem)
API_AOMV_PROCUSER DS  CL05             PROCUSER    (1-5 Idem)
API_AOMV_THREADS  DS  CL06             THREADS     (1-6 Idem)
API_AOMV_MEMLIM   DS  CL09             MEMLIMIT    (1-8 DIGITS + M/G/T/P)
API_AOMV_SHMMAX   DS  CL09             SHMEMMAX    (1-8 DIGITS + M/G/T/P)
```

OMVS セグメントを更新すると、OMVS セグメント内のすべてのフィールドが置き換えられます。そのため、すべてのパラメーターに対して、有効なデータを指定する必要があります。フィールドが空 (ブランクまたはヌル) になっていると、OMVS セグメント内の対応するフィールドが削除されます。

ALTUSER (WORKATTR SEGMENT) 関数 (WORKATTR セグメントの変更)

ALTUSER (WORKATTR SEGMENT) 関数を使用して、特定のユーザーの WORKATTR セグメントを変更します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.AUSR) に対するアクセス権限と、このユーザーのデフォルト・グループ (AUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。 また、OMVS セグメントを管理する場合、ユーザーは TOOLKIT.AWRK に対するアクセス権限も持っている必要があります。

COMMAREA

最小サイズは 637 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC         DC  CL4'AWRK'   Function code for WORKATTR segment.
API_RC           DC  XL01'00'    Return code
API_MSG          DC  CL79' '     Message area
*
API_AWRK_RC      DS   XL01             Return code from command
*
API_AWRK_CODE    DS   CL04             UPDT = Update segment
*                                      LIST = Retrieve segment
*                                      DELT = Delete segment
API_AWRK_USERID   DS  CL08             The userid
API_AWRK_NAME     DS  CL60             WANAME  (1-60 Chars)
API_AWRK_ACCNT    DS  CL60             WAACCNT (1-60 Chars)
API_AWRK_BLDG     DS  CL60             WABLDG  (1-60 Chars)
API_AWRK_DEPT     DS  CL60             WADEPT  (1-60 Chars)
API_AWRK_ROOM     DS  CL60             WAROOM  (1-60 Chars)
API_AWRK_ADDR1    DS  CL60             WAADDR1 (1-60 Chars)
API_AWRK_ADDR2    DS  CL60             WAADDR2 (1-60 Chars)
API_AWRK_ADDR3    DS  CL60             WAADDR3 (1-60 Chars)
API_AWRK_ADDR4    DS  CL60             WAADDR4 (1-60 Chars)
```

WORKATTR セグメントを更新すると、WORKATTR セグメント内のすべてのフィールドが置き換えられます。そのため、すべてのパラメーターに対して、有効なデータを指定する必要があります。フィールドが空 (ブランクまたはヌル) になっていると、WORKATTR セグメント内の対応するフィールドが削除されます。

CONNECT 関数 (グループへのユーザーまたはグループの 接続)

CONNECT 関数を使用して、グループにユーザーまたはグループを 接続します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.CONN) およびターゲット・グループ (CONN.*dfltgrp*) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは 112 バイトです。アプリケーションで取り消し日と再開日にアクセスする必要がある場合の最小サイズは 122 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC         DC  CL4'CONN'  Function code for CONNECT
API_RC           DC  XL01'00'   Return code
API_MSG          DC  CL79' '    Message area
API_CONN_RC      DC  XL1        Return code from CONNECT. If
*                               non-zero the command failed.
*                               API_MSG will give the reason for
*                               the failure.
*
API_CONN_USERID  DC  CL8        Userid/group being connected.
*
API_CONN_GROUP   DC  CL8        Group being connected to.
*
API_CONN_AUTH    DC  CL1        Connect authority
*                               Must be 'U' (use),
*                               'C' (create)
*                               'N' (connect) or
*                               'J' (join).
*
API_CONN_OWNER   DC  CL8        Owner of the connect profile. It
*                               must be a valid userid or group.
*
API_CONN_SPEC    DC  CL1        Specify 'Y' if the user should have the
*                               group-special attribute otherwise
                                specify 'N'.
*
API_CONN_OPER    DC  CL1        Specify 'Y' if the user should have the
```

```
*                               group-operations attribute otherwise
*                               specify 'N:'.
*
API_CONN_REVOKE  DC  CL5        The date (YYDDD) the user is to be REVOKED
*
API_CONN_RESUME  DC  CL5        The date (YYDDD) the user is to be RESUMED
```

API_CONN_REVOKE フィールドと **API_CONN_RESUME** フィールドを使用すると、接続の取り消し日と再開日の設定または削除が可能です。ブランクの値 (x'4040404040') を使用した場合、取り消し日と再開日は現行値のままになります。特殊なゼロ日付 (c'00000' = x'F0F0F0F0F0') を使用すると、現行の取り消し日や再開日を削除することができます。この最後の特殊値を使用すると、z/OS 1.7 RACF **ALTUSER** コマンドの NOREVOKE キーワードおよび NORESUME キーワードと同様の機能を実装することができます。REVOKEDT または RESUMEDT のいずれかに今日の日付を指定した場合は、ユーザーの取り消し状況が直ちに更新され、他の日付値は無視されます。RESUMEDT と REVOKEDT は、両方ともリセットされます。

CSDATA 関数 (CSDATA フィールドのリストおよび管理)

CSDATA 関数を使用して、USER、GROUP、DATASET および一般リソース・プロファイルの CSDATA フィールドをリスト、追加、更新、または削除します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンドに対するアクセス権限を持っている必要があります。次の表に示されているように、リソース名は要求される関数によって異なります。

関数	許可で使用する TOOLKIT
List	TOOLKIT.CSDL
Add	TOOLKIT.CSDA
Update	TOOLKIT.CSDA
Delete	TOOLKIT.CSDD

ユーザーは、少なくとも CSDN.*csdata-name* プロファイルに対する READ アクセス権限も持っている必要があります。単一のフィールドにアクセスするときに、ユーザーがそのフィールドに対する権限がない場合、メッセージ CQT194「この CSDATA フィールドに対する権限がありません (You are not authorized for this CSDATA field)」が出されます。リスト関数がすべてのフィールドに使用される場合、メッセージ CQT198「有効範囲外の CSDATA エントリーが抑止されました (CSDATA entries outside scope suppressed)」が出されることがあります。

ターゲット・プロファイルは、コマンド・ユーザーの有効範囲内でなければなりません。 他の zSecure CICS Toolkit 関数とは異なり、この許可は DFLTGRP によって制御されるのではなく、ターゲット・プロファイルの OWNER によって制御されます。ユーザーには、指定されたリソースに対して少なくとも READ アクセス権限が必要です。次の表は、有効範囲に関連するリソースをリストしています。

クラス	有効範囲の許可
USER	CSDU.*owner*
GROUP	CSDG.*owner*
DATASET	CSDD.*owner*
一般リソース	CSDR.*owner*

COMMAREA

最小サイズは 605 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC         DC  CL4'CSDA'  Function code for CSDATA management
API_RC           DC  XL01'00'   Return code
```

```
API_MSG          DC  CL79' '    Message area
*
API_CSDA_RC      DS  XL01       Return code from command
*
API_CSDA_CODE1   DS  XL01       "A" Add
*                               "D" Delete
*                               "U" Update
*                               "L" List
*
API_CSDA_CLASS   DS  CL08       Class
API_CSDA_PROF    DS  CL248      Profile
API_CSDA_GENERIC DS  CL01       Generic (G or anything else)
API_CSDA_CSDN    DS  CL08       CSDATA field name (at x'157')
API_CSDA_CSDV    DS  CL255      CSDATA field value
API_CSDA_CSDLST  DS  XL265      Space for returned CSDATA
*                    XL2        Length of data entry that
*                               follows. 0 to indicate end.
*                    CL8        CSDATA field name
*                    CLx        CSDATA field value
```

この API には、指定されたプロファイルの CSDATA をリストするための 2 つの方法が用意されています。CLASS および PROF のみの値を指定する場合、許可されているすべての CSDATA フィールドが CSDLST に返されます。CSDN の値も指定した場合は、指定された CSDATA フィールドの値が CSDV に返され、CSDLST は使用されません。

GENERIC フィールドは入力としてのみ使用されます。DATASET プロファイルが完全修飾総称であることを示すのに使用できます。その他のすべてのリソース・クラスでは無視されます。zSecure CICS Toolkit は、複数の個別 DATASET プロファイル (例えば、別々のボリュームにある同じ名前のデータ・セットの場合) をサポートしません。

LIST 関数を使用する場合は、CSDN.*csdata-name* によって権限が付与されている CSDATA の名前または値だけが返されます。 すべての CSDATA の名前または値を要求した場合、返されるリストからは、自分が権限を持っていない項目が除外されます。

すべての CSDATA の名前または値のリストを要求した場合は、用意した commarea 内に完全に収まる名前と値だけが提供されます。さらに、API_CSDA_RC が設定され、オーバーフロー条件が示されます。すべての値が必要な場合は、十分に大きな commarea を用意してください。

フラグ・フィールドは、単一の Y 文字または N 文字として表示されます。

フィールド CSDN および CSDV を使用して CSDATA 値を処理する場合、フィールド値の長さは常に 255 文字に制限されます。これは、すべての関数に適用されます。フィールドの現行値が 255 文字より長い場合、切り捨てられます。すべてのフィールドに LIST 関数を使用する (すなわち、CSDN をブランクのままにする) 場合、すべてのフィールドの切り捨てられていない完全な値は CSDLST で入手できます。フィールドが切り捨てられると、API_MSG フィールドにメッセージ CQT202:「CSDATA 値が切り捨てられました (CSDATA value truncated)」が表示されます。

DATASET および一般リソース・プロファイルの CSDATA フィールドは、z/OS 2.4 以上でのみ使用可能です。zSecure CICS Toolkit インターフェースを 使用して、これらのリソース・クラスでプロファイルの CSDATA フィールドを管理する場合、z/OS レベルで CSDATA フィールドがサポートされなければ、メッセージ CQT193「CSDATA フィールドが 見つかりませんでした (CSDATA field not found)」が返されます。

DELETE DATASET 関数 (データ・セット・プロファイルの削除)

DELETE DATASET 関数を使用してデータ・セット・プロファイルをシステムから削除します。

AUTHORITY
このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.DELD) に対するアクセス権限と、データ・セット・プロファイル名の高位修飾子 (DELD.hlq) に対するアクセス権限を持っている必要があります。ユーザーが DELD.hlq に対するアクセス権限を持っていない場合は、標準の RACF 権限検査が使用されます。ユーザーによる削除が許可されるデータ・セット・プロファイルについては、「RACF コマンド言語解説書」を参照してください。

COMMAREA
最小サイズは 130 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC  CL4'DELD'   Function code for DELDSD
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
API_DELD_RC       DC  XL01'00'    Return code from DELDSD.
*                                 If non-zero the command
*                                 failed.  API_MSG will give the reason for
*                                 the failure.
*
API_DELD_DSNAME   DC  CL44'DS-Profile'
                                  The dataset profile to be deleted.

API_DELD_GENERIC  DC  CL01'Y'     Specify 'Y' if the profile is Generic
*                                 or 'N' if it is not.
*
```

DELETE USERID 関数 (ユーザー・プロファイルの削除)

DELETE USERID 関数を使用してユーザー ID をシステムから削除します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.DELU) に対するアクセス権限と、このユーザー ID のデフォルト・グループ (DELU.*dfltgrp*) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは 93 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC         DC  CL4'DELU'   Function code for DELUSER
API_RC           DC  XL01'00'    Return code
API_MSG          DC  CL79' '     Message area
API_DELU_RC      DC  XL01'00'    Return code from DELUSER.
*                                If non-zero the command
*                                failed.  API_MSG  will give the
*                                reason for the failure.
*
API_DELU_USERID  DC  CL8'USERID' The userid to be deleted.
*
```

このユーザー ID がデフォルト・グループ以外のすべてのグループから削除されており、かつこのユーザー ID を高位修飾子として使用するデータ・セット・プロファイルが存在しない状態で、削除を実行してください。

zSecure CICS Toolkit は、グループ接続について検査しますが、データ・セット・プロファイルについては検査しません。

LISTDATASET 関数 (1 つ以上のデータ・セットのプロファイルのリスト)

LISTDATASET 関数を使用して特定のデータ・セット (複数可) のプロファイルをリストします。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.LDSD) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは、524 バイト (データ・セット・プロファイルを表示する場合) または 2374 バイト (ユーザーまたはプログラムを要求する場合) です。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

注 : 検索を実行する場合は、検索パターンに応じてすべてのフィールドを 初期化してください。フィールドの埋め込みにはアスタリスクを使用してください。ただし、**DSETID** フィールドの場合は、ヌル、ブランク、またはアンダースコアーを 埋め込んでください。

```
API_FUNC               DC  CL4'LDSD'   Function code for LISTDATASET
API_RC                 DC  XL01'00'    Return code
API_MSGDC              DC  CL79' '     Message area
*
API_LDSD_RC            DC  XL1         Return code from LISTDATASET.
*                                      If non-zero the command failed.
*                                      API_MSG will give the reason for
*                                      the failure.
*
API_LDSD_CODE1         DC  CL1         Request code.
*                                      'S' = start search
*                                      'N' = get next profile
*                                      'L' = retrieve this profile
*                                      'U' = retrieve users
*                                      'P' = retrieve programs
*
API_LDSD_RESERVED      DC CL46         This field is reserved for the
*                                      API and must be preserved between
*                                      calls.
*
API_LDSD_DTYPE         DC  CL1         Profile type (generic or discrete).
*
API_LDSD_DSETID        DC  CL44        The dataset to be retrieved.
*                                      Only required when the CODE
*                                      field is L, U or P; otherwise it is
*                                      used as part of the search criteria.
*
API_LDSD_AUTHOR        DC  CL8         Owner of the profile.
API_LDSD_CREADAT       DC  CL5         Creation date.
API_LDSD_LREFDAT       DC  CL5         Last reference date.
API_LDSD_LCHGDAT       DC  CL5         Last update date.
API_LDSD_ACSALTR       DC  CL6         # of alter accesses.
API_LDSD_ACSCNTL       DC  CL6         # of control accesses.
API_LDSD_ACSUPDT       DC  CL6         # of update accesses.
API_LDSD_ACSREAD       DC  CL6         # of read accesses.
API_LDSD_UACC          DC  CL7         Universal access to the dataset.
API_LDSD_GRPDST        DC  CL1         Group dataset.
API_LDSD_AUDIT         DC  CL1         Audit flag.
API_LDSD_GROUPNM       DC  CL8         Current connect group.
API_LDSD_DSTYPE        DC  CL4         Dataset type.
API_LDSD_LEVEL         DC  CL3         Level indicator.
API_LDSD_GAUDIT        DC  CL1         Global audit option.
API_LDSD_AUDITQS       DC  CL1         Audit success flag.
API_LDSD_AUDITQF       DC  CL1         Audit failure flag.
API_LDSD_GAUDQS        DC  CL1         Global audit success flag.
API_LDSD_GAUDQF        DC  CL1         Global audit failure flag.
API_LDSD_WARNING       DC  CL1         Warning mode.
API_LDSD_SECLEVL       DC  CL3         Security level.
API_LDSD_NUMCTGY       DC  CL4         Number of categories.
API_LDSD_NUMPGMS       DC  CL4         Number of programs.
API_LDSD_NUMUSER       DC  CL4         Number of users/groups.
API_LDSD_INSTDATA      DC  CL255       Installation data field.
                       ORG API_LDSD_RESERVED
API_LDSD_USERPGMS      DC  CL???       When the users or programs
*                                      are requested they will be returned
*                                      into this area.
```

プログラムのリストが返される場合の出力形式は以下のとおりです。

```
Description                            Length

Length of program name                 4 bytes
Program name                           8 bytes
Length of userid                       4 bytes
Userid                                 8 bytes
Length of access field                 4 bytes
Access                                 1 byte  X'80' Alter access
                                               X'40' Control access
                                               X'20' Update access
                                               X'10' Read access
                                               X'08' Execute access
                                               X'01'  None
```

ユーザーのリストが返される場合の出力形式は以下のとおりです。

```
Description                          Length

Length of Userid                     4 bytes
Userid                               8 bytes
Length of access fied                4 bytes
Access                               1 byte  X'80' Alter access
                                             X'40' Control access
                                             X'20' Update access
                                             X'10' Read access
                                             X'08' Execute access
                                             X'01'  None

Length of access count               4 bytes
Access count                         2 bytes (binary)
```

いずれの場合も、最初のフィールドがゼロ (x'00000000') であれば、それがデータの終わりを示します。

LISTGROUP 関数 (グループのプロファイルのリスト)

LISTGROUP 関数を使用して特定のグループ (複数可) のプロファイルをリストします。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.LGRP) に対するアクセス権限と、グループ名 (LGRP.*grpname*) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは、441 バイト (グループ・プロファイルを表示する場合) または 2374 バイト (サブグループのユーザーを要求する場合) です。汎用グループのサポートを使用可能にする場合の最小サイズは 442 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

注 : 検索を実行する場合は、検索パターンに応じてすべてのフィールドを初期化してください。フィールドの埋め込みにはアスタリスクを使用してください。ただし、**GROUP** フィールドの場合は、ヌル、ブランク、またはアンダースコアーを 埋め込んでください。

```
API_FUNC               DC  CL4'LGRP'   Function code for LISTGROUP
API_RC                 DC  XL01'00'    Return code
API_MSG                DC  CL79' '     Message area
*
API_LGRP_RC            DC  XL1         Return code from LISTGROUP.
*                                      If non-zero the command failed.
*                                      API_MSG will give the reason for
*                                      the failure.
*
API_LGRP_CODE1          DC  CL1         Request code.
*                                      'S' = start search
*                                      'N' = get next profile
*                                      'L' = retrieve this profile
*                                      'G' = retrieve subgroups
*                                      'U' = retrieve users
*
API_LGRP_RESERVED      DC  CL9         This field is reserved for the
*                                      API and must be preserved between
*                                      calls.
*
API_LGRP_GROUP         DC  CL8         The group to be retrieved.
*                                      Only required when the CODE field
*                                      is L, G or U otherwise it is used
*                                      as part of the search criteria.
*
API_LGRP_SUPGRP        DC  CL8         This groups superior group.
API_LGRP_OWNER         DC  CL8         Owner of this group.
API_LGRP_DTE           DC  CL5         Date this profile was created.
API_LGRP_UACC          DC  CL7         Authority of a user to the group
*                                      if the user is not connected to
*                                      the group.
*
API_LGRP_TERMACC       DC  CL1         Authority to access a terminal* required.
*
API_LGRP_SUBGRPS       DC  CL5         Number of subgroups.
*
```

```
API_LGRP_USERS          DC CL5          Number of users.
*
API_LGRP_MODEL          DC CL44         Name of a profile to be used as
*                                       model for new group-name
*                                       datasets.
*
API_LGRP_INSTDATA       DC  CL255       Installation data field.
*
API_LGRP_UNIVERS        DC  CL1         Universal Group ('Y' or 'N')
*
                        ORG API_LGRP_RESERVED
API_LGRP_USERSUBG       DC  CL????      When the users or subgroups are
*                                       requested they will be returned
*                                       into this area.
```

ユーザーまたはサブグループのリストが返される場合の出力形式は以下のとおりです。

```
Description                             Length

Length of member                        4 bytes
User/Subgroup name                      8 bytes
```

いずれの場合も、先頭の長さフィールドがゼロ (x'00000000') であれば、それがデータの終わりを示します。

LISTUSER 関数 (ユーザー ID のプロファイルのリスト)

LISTUSER 関数を使用して特定のユーザーまたはユーザー ID のプロファイルをリストします。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.LUSR) に対するアクセス権限と、対象ユーザーのデフォルト・グループ (LUSR.*dfltgrp*) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは、544 バイト (グループ・プロファイルを表示する場合) または 2374 バイト (グループまたはカテゴリーを要求する場合) です。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

注 : 検索を実行する場合は、検索パターンに応じてすべてのフィールドを初期化する必要があります。フィールドの埋め込みにはアスタリスクを使用してください。ただし、**USERID** フィールドの場合は、ヌル、ブランク、またはアンダースコアーを 埋め込んでください。

```
API_FUNC          DC  CL4'LUSR'   Function code for LISTUSER.
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_LUSR_RC       DC  XL1         Return code from LISTUSER.
*                                 If non-zero the command failed.
*                                 API_MSG will give the reason for
*                                 the failure.
*
API_LUSR_CODE1    DC  CL1         Request code.
*                                 'S = start search
*                                 'N' = get next profile
*                                 'L' = retrieve this profile
*                                 'G' = retrieve groups
*                                 'A' = retrieve groups and authority to groups
*                                 'C' = retrieve categories
*
API_LUSR_RESERVED DC  CL9         This field is reserved for the
*                                 API and must be preserved between
*                                 calls.
API_LUSR_USERID   DC  CL8         The userid to be retrieved.
*                                 Only required when the CODE field
*                                 is L, G or C otherwise it is used
*                                 as part of the search criteria.
*
API_LUSR_PGMRNAME DC  CL20        Users name.
```

```
API_LUSR_AUTHOR   DC  CL8         Owner of the profile.
API_LUSR_PASSWRD  DC  CL8         Password field (will contain ?)
API_LUSR_AUTHDTE  DC  CL5         Creation date.
API_LUSR_DFLTGRP  DC  CL8         Default group.
API_LUSR_AUTHRTY  DC  CL7         Authority.
API_LUSR_UACC     DC  CL7         Universal access.
API_LUSR_CLASCNT  DC  CL5         Number of classes.
API_LUSR_ADSP     DC  CL1         ADSP.
API_LUSR_SPEC     DC  CL1         Special.
API_LUSR_OPER     DC  CL1         Operations.
API_LUSR_REVOKE   DC  CL1         Revoke.
API_LUSR_GRPACC   DC  CL1         GRPACC.
API_LUSR_AUDITOR  DC  CL1         Auditor.
API_LUSR_PROTECT  DC  CL1         Password cannot be used.
API_LUSR_RESTR    DC  CL1         UACC and similar not used.
API_LUSR_UAUDIT   DC  CL1         Audit all RACHECK's/RACDEF's.
API_LUSR_REVOKEC  DC  CL2         # unsuccessful pwd attempts.
API_LUSR_REVOKED  DC  CL5         Date user will be revoked.
API_LUSR_SECL     DC  CL2         Security level. This is a binary field that
*                                 represents the security level. Eg.:
*                                 X'00FE' would be a security level of 254.
API_LUSR_RESUMED  DC  CL5         Date user will be resumed.
API_LUSR_LASTACC  DC  CL14        Last access date and time.
API_LUSR_PASSDTE  DC  CL5         Date password last changed.
API_LUSR_PASSINT  DC  CL3         Password interval.
API_LUSR_PWDGEN   DC  CL3         Current password generation #.
API_LUSR_PWDCNT   DC  CL3         Number of old passwords.
API_LUSR_NUMCTGY  DC  CL4         Number of categories.
API_LUSR_NUMGRP   DC  CL4         Number of groups.
API_LUSR_LOGDAY   DC  CL7         Days user can logon.
API_LUSR_LOGFROM  DC  CL4         Starting time for logon.
API_LUSR_LOGTILL  DC  CL4         Latest time for logon.
API_LUSR_MODEL    DC  CL44        Dataset profile model.
API_LUSR_INSTDATA DC  CL255       Installation data field.
                  ORG API_LUSR_RESERVED
API_LUSR_GRUPCTGY DC CL????       When the groups or categories are
*                                 requested they will be returned
*                                into this area.
```

グループのリストが返される場合の出力形式は以下のとおりです。

```
Description                          Length

Length of group name                 4 bytes
Group name                           8 bytes
```

グループと権限のリストが返される場合の出力形式は以下のとおりです。

```
Description                                           Length

Combined length of the following 'group length/names'  4 bytes
Length of group name                                   4 bytes
Group name                                             8 bytes
```

以下の各フィールドは、各グループに対して 1 対 1 の関係を持っています。ユーザーが 2 つのグループに接続されていた場合は、2 つの ADSP フラグ、2 つの SPECIAL フラグ、2 つの OPERATIONS フラグ、2 つの REVOKE フラグ、2 つの GRPACC フラグ、および 2 つの GROUP AUDITOR フラグが存在します。フラグのビット 0 がオンになっている場合 (X'80' になっている場合)、ユーザーは、該当するグループ内でその属性を持っています。

```
Combined length of the ADSP lengths/flags            4 bytes
Length of the ADSP flag                              4 bytes
ADSP flag                                            1 byte


Combined length of the SPECIAL lengths/flags         4 bytes
Length of SPECIAL flag                               4 bytes
SPECIAL flag                                         1 bytes


Combined length of the OPERATIONS lengths/flags      4 bytes
Length of OPERATIONS flag                            4 bytes
OPERATIONS flag                                      1 byte
```

```
Combined length of the REVOKE lengths/flags          4 bytes
Length of the REVOKE flag                            4 bytes
REVOKE REVOKE flag                                   1 byte


Combined length of the GRPACC lengths/flags          4 bytes
Length of GRPACC flag                                4 bytes
GRPACC flag                                          1 byte


Combined length of the GROUP AUDITOR lengths/flags   4 bytes
Length of GROUP AUDITOR flag                         4 bytes
GROUP AUDITOR flag                                   1 byte
```

カテゴリーのリストが返される場合の出力形式は以下のとおりです。

```
Description                          Length

Length of category                   4 bytes
Category number                      2 bytes (binary)
```

いずれの場合も、先頭の長さフィールドがゼロ (x'00000000') であれば、それがデータの終わりを示します。

PASSWORD 関数 (パスワード変更)

PASSWORD 関数を使用してユーザーのパスワードを変更します。

AUTHORITY

インターバルの値として 255 (NOINTERVAL に対応) を指定する場合、または自分以外のユーザー ID の INTERVAL 値を変更する場合を除き、NONE になります。それぞれの場合に応じて、SPECIAL を持っているか、TOOLKIT.SPEC または PSWD.*dfltgrp* (*dfltgrp* は、変更するユーザー ID のデフォルト・グループ) に対するアクセス権限を持っている必要があります。自分以外のユーザー ID に対して **PASSWORD** コマンドを使用する場合に変更できるのは、INTERVAL 値のみです。別のユーザーのパスワードを 変更するには、**ALTUSER** コマンドを使用します。

COMMAREA

最小サイズは 112 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC           DC  CL4'PSWD'   Function code for PASSWORD.
API_RC             DC  XL01'00'    Return code
API_MSG            DC  CL79' '     Message area
*
API_PSWD_RC        DC  XL01'00'    Return code from PASSWORD.
*                                  If non-zero the command failed.
*                                  API_MSG will give the reason for the
                                   failure.
*
API_PSWD_USERID    DC  CL08'USERID '  The userid being altered.
*
API_PSWD_PASSWORD  DC  CL08'PASSWORD' The password for this userid.
*
API_PSWD_NEWPASS   DC  CL08'NEWPSWD'  The new password for this userid.
API_PSWD_PASSINT   DC  CL03'060'      The new password interval for this userid.
```

PASSWORD がユーザーに代わってサインオンを実行することはありません。この関数は、このユーザー ID に対して入力されたパスワードが正しいことを検査し、パスワードを新しい指定内容に変更して、パスワード・インターバルを変更するだけです。

システム・パラメーターによっては、ユーザーのパスワードの変更に何回か失敗すると、そのユーザー ID が取り消されてしまう場合があります。

ユーザーのパスワード・インターバルを変更することもできます。新しいインターバルは 001 から 254 までですが、グローバルに指定された最大値を超えることはできません。この最大値を超えてしまう場合は、許可された最大値に設定されます。インターバルに指定された値が無効な場合、パラメーターは無視されます。パスワード・インターバルだけを変更する場合、パスワードを指定する必要はありません。ただし、

インターバルが無効で無視される場合、zSecure CICS Toolkit は、この操作をパスワード変更要求と同じように処理するため、パスワードと新規パスワードが検査されます。新規パスワードが指定されていない場合に返されるエラー・メッセージには、パスワード・インターバルの誤りではなく、新規パスワードのエラーが反映されます。

このコマンドは、API 経由のみで使用することができます。

PERMIT 関数 (アクセス権限の付与または除去)

PERMIT 関数を使用して、CICS リソースに対するアクセス権限の付与または除去を行います。このリソースは、CICS のこの関数の実行用に SIT で定義されたリソース・クラスのいずれかに存在している必要があります。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.PEMT) に対するアクセス権限、アクセス権限を付与するユーザー ID またはグループのデフォルト・グループ (PEMT.*dfltgrp*) に対するアクセス権限、および当該リソースに対するアクセス権限を持っている必要があります。グループにアクセス権限を付与する場合に使用されるリソースは PEMT.*group* です。PERMIT 関数が終了したら、その内容を直ちに反映するために、リソース・クラスを更新する必要があります。そのためには、RACF **SETROPTS REFRESH** コマンドを使用してください。

COMMAREA

最小サイズは 116 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC  CL4'PEMT'   Function code for PERMIT.
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_PEMT_RC       DC  XL01'00'    Return code from PERMIT
*                                 If non-zero the command failed
*                                 API_MSG will give the reason for the failure
*
API_PEMT_USERID   DC  CL08'USERID' The userid or group.
*
API_PEMT_RSRC     DC  CL13'CEMT '  The name of the CICS resource.
*
API_PEMT_CLASS    DC  CL08'TCICSTRN'
*                                  The resource classname.
*                                  If blank the value of the XTRAN parameter
*                                  specified in the SIT is used.
*
API_PEMT_DELT     DC  CL01'Y'     Specify 'Y' in this field to remove
*                                 a person from the access list for
*                                 this resource.  The user or group
*                                 will no longer have access to the resource.
*
API_PEMT_ACC      DC  CL01'R'     Access allowed to the resource
*                                 Specify 'R' for read,
*                                 'N' for none,
*                                 'U' for update,
*                                 'A' for alter or
*                                 'C' for control.
*                                  Read is the default
```

PERMITX 関数 (任意のリソースに対するアクセス権限の付与または除去)

PERMITX 関数を使用して、任意のリソースに対するアクセス権限の付与または除去を行います。この関数を使用して、データ・セット・プロファイルに対するアクセス権限を付与することもできます。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.PEMT) に対するアクセス権限を持っている必要があります。アクセス権限の付与先のユーザー ID またはグループのデフォルト・グループ (PEMT.*dfltgrp*) も、当該リソースに対するアクセス権限を持っている必要があります。グ

ループにアクセス権限を付与する場合に使用されるリソースは PEMT.*group* です。ユーザーは、PEMX.*classname* プロファイルに対する権限も持っている必要があります。PERMIT 関数が終了したら、その内容を直ちに反映するために、リソース・クラスを更新する必要があります。そのためには、RACF **SETROPTS REFRESH** コマンドを使用してください。

PERMITX 関数を使用可能にするには、PEMTALL=Y を指定して、CQTPCNTL で有効にしておく必要があります。

COMMAREA

最小サイズは 349 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC  CL4'PEMX'   Function code for PERMITX
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_PEMX_RC       DC  XL01'00'    Return code from PERMIT
*                                 If non-zero the command failed
*                                 API_MSG will give the reason for the failure.
*
API_PEMX_USERID   DC  CL08'USERID'   The userid or group.
*
API_PEMX_RSRC     DC  CL246'CEMT '   The name of the resource.
*
API_PEMX_CLASS    DC  CL08'TCICSTRN' The resource class name.
*                                    If blank the value of the
*                                    XTRAN parameter.
*                                    specified in the SIT is used
API_PEMX_DELT     DC  CL01'Y'     Specify 'Y' in this field
*                                 to remove a person from the access
*                                 list for this resource.  The user
*                                 or group will no longer have access.
*                                 access to the resource.
API_PEMX_ACC      DC  CL01'R'     Access allowed to the resource.
*                                 Specify 'R' for read,
*                                'N' for none,
*                                'U' for update,
*                                'A' for alter,
*                                'C' for control.
*                                 Read is the default
```

RACLINK 関数 (ユーザーの関連の定義、リスト、定義解除、または承認)

RACLINK 関数を使用して、ローカル・システムの RRSF ユーザー ID アソシエーションのリスト、定義、承認、および定義解除を行います。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.RACL) に対するアクセス権限と、このユーザー ID のデフォルト・グループ (PEMT.*dfltgrp*) に対するアクセス権限を持っている必要があり、さらに DEFINE 関数の場合は、RRSFDATA リソース・クラスの RACLINK.DEFINE.*nodename* プロファイルに対するアクセス権限と、RACLINK.PWSYNC.*nodename* プロファイルに対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは 1150 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC              DC  CL4'RACL'   Function code for RACLINK
API_RC                DC  XL01'00'    Return code
API_MSG               DC  CL79' '     Message area
*
API_RACL_RC           DS  XL01        Return code from command
API_RACL_CODE1        DS  XL01        'D' DEFINE
*                                     'U' UNDEFINE
*                                     'A' APPROVE
*                                     'L' LIST ASSOCIATIONS
```

```
*
API_RACL_USERID        DC  CL8'userid  '       Userid on whose behalf
API_RACL_ATYPE         DC  CL8'PEER    '       Assoc. type (PEER/MANAGED
)
API_RACL_ANODE         DC  CL8'nodename'       Assoc. node
API_RACL_AUSERID       DC  CL8'ibmuser '       Assoc. Userid
API_RACL_PWSYNC        DC  CL4'yes '           yes/no
API_RACL_APSWD         DC  CL8'sys1    '       Assoc. Userid Password
API_RACL_ASSOCLST      DS  15CL68              List of 15 associations
*
```

ユーザーのアソシエーションのリストの形式は以下のとおりです。

```
API_RACL_ASSOCTYPE     DC  CL10         PEER/MANAG
API_RACL_ASSOCNODE     DC  CL8          node
API_RACL_ASSOCUSER     DC  CL8          USER
API_RACL_ASSOCPWSYNC   DC  CL4          pwsync
API_RACL_ASSOCSTAT     DC  CL20         status
API_RACL_ASSOCCREAT    DC  CL8          creator
API_RACL_ASSOCDATE     DC  CL10         date
```

アソシエーションのリストの終わりは、ブランクで構成された項目によって示されます。

REMOVE 関数 (グループからのユーザー ID またはグループの削除)

REMOVE 関数を使用してグループからユーザーまたはグループを 削除します。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.REMV) に対するアクセス権限および、ターゲット・グループ (REMV.*grpname*) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは 101 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC           DC  CL4'REMV'   Function code for REMOVE
API_RC             DC  XL01'00'    Return code
API_MSG            DC  CL79' '     Message area
*
API_REMV_RC        DC  XL1         Return code from REMOVE.
*                                  If non-zero the command failed.
*                                  API_MSG will give the reason for the
                                   failure.
*
API_REMV_USERID    DC  CL8         Userid/group being removed.
*
API_REMV_GROUP     DC  CL8         Group being removed from.
```

ユーザーは、デフォルト・グループからは削除されない場合があります。

RALTER/RDEFINE/RDELETE 関数 (プロファイルのリストおよび管理)

RALTER、RDEFINE、および RDELETE 関数を使用して CDT で定義されている一般リソース・クラスのプロファイルのリストと管理を行います。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (実行するコマンドに応じて、TOOLKIT.RALT、TOOLKIT.RDEF、TOOLKIT.RDEL のいずれか) に対するアクセス権限と、一般リソース・クラス (RALT.*cdtclass*、RDEF.*cdtclass*、RDEL.*cdtclass*、RLST.*cdtclass*) に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは 875 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC  CL4'Rxxx'   Function code:
*                                 RALT for RALTER
*                                 RDEF for RDEFINE
*                                 RDEL for RDELETE
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_RUPD_RC       DC  XL1         Return code.
*                                 If non-zero the command failed.
*                                 API_MSG will give the reason for* the failure.
*
API_RUPD_CODE1    DC  CL4         Type of command being performed
*                                 'RDEF to define a profile
*                                 'RDEL' to delete a profile
*                                 'AMEM' to add a member
*                                 'DMEM' to delete a member
*                                 'UPDP' to update fields in the profile
*
API_RUPD_CLASS    DC  CL8         The class containing the profile
API_RUPD_CTYPE    DC  CL1         Profile type (not used as input to the API).
API_RUPD_ENTRY    DC  CL246       The profile name
API_RUPD_MEMBER   DC  CL246       The member name
*
API_RUPD_OWNER    DC  CL8         Owner of the profile.
API_RUPD_NOTIFY   DC  CL8         User to be notified.
API_RUPD_UNIVACS  DC  CL7         Universal access to the dataset.
API_RUPD_WARNING  DC  CL1         Warning mode.
API_RUPD_LEVEL    DC  CL3         Level indicator.
API_RUPD_AUDIT    DC  CL1         Audit flag.
API_RUPD_AUDITQS  DC  CL1         Audit success flag.
API_RUPD_AUDITQF  DC  CL1         Audit failure flag.
API_RUPD_INSTDATA DC  CL255       Installation data field.
```

RLIST 関数 (一般リソース・クラスのプロファイルのリスト)

RLIST 関数を使用して、CDT で定義されている一般リソース・クラスのプロファイルの詳細をリストします。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンド (TOOLKIT.RLST) アクセス権限と、一般リソース・クラス (RLIST.*cdtclass*) に対するアクセス権限を持っている必要があります。

COMMAREA

プロファイルを表示する場合の最小サイズは 907 バイトです。メンバー、ユーザー、または condacc を対象とする要求の場合は、返されるデータをすべて保持できるだけの十分な大きさの commarea が必要です。サイズが十分でない場合、**API_RLST_RC** がゼロ以外の値になり、メッセージによってエラーが示されます。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

注 : 検索を実行する場合は、検索パターンに応じてすべてのフィールドを初期化する必要があります。フィールドの埋め込みにはアスタリスクを使用してください。ただし、**ENTRY** フィールドの場合は、ヌル、ブランク、またはアンダースコアーを埋め込んでください。

```
API_FUNC          DC  CL4'RLST'   Function code for RLIST
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_RLST_RC       DC  XL1         Return code from RLIST.
*                                 If non-zero the command failed.
*                                 API_MSG will give the reason for
*                                 the failure.
*
API_RLST_CODE1    DC  CL1         Request code.
*                                 'S' = start search
*                                 'N' = get next profile
*                                 'L' = retrieve this profile
*                                 'C' = retrieve conditional access list
```

```
*                                'M' = retrieve members
*                                'U' = retrieve users
*
API_RLST_RESERVED DC  CL248      This field is reserved for the
*                                API and must be preserved between calls.
*
API_RLST_CLASS    DC  CL8        The class containing the profile to be
*                                retrieved. This field is ***always*** required
*
API_RLST_CTYPE    DC  CL1        Profile type (not used as input to the API).
*
API_RLST_ENTRY    DC  CL246      The  profile to be retrieved. Only
*                                required when the CODE field is L, U, C
*                                or M otherwise it is used as part of the
*                                search criteria.
*
API_RLST_OWNER    DC  CL8        Owner of the profile.
API_RLST_DEFDATE  DC  CL5        Creation date.
API_RLST_LREFDAT  DC  CL5        Last reference date.
API_RLST_LCHGDAT  DC  CL5        Last update date.
API_RLST_UACC     DC  CL7        Universal access to the dataset.
API_RLST_AUDIT    DC  CL1        Audit flag.
API_RLST_AUDITQS  DC  CL1        Audit success flag.
API_RLST_AUDITQF  DC  CL1        Audit failure flag.
API_RLST_NOTIFY   DC  CL8        User to be notified.
API_RLST_WARNING  DC  CL1        Warning mode.
API_RLST_LEVEL    DC  CL3        Level indicator.
API_RLST_GAUDIT   DC  CL1        Global audit option.
API_RLST_GAUDQS   DC  CL1        Global audit success flag.
API_RLST_GAUDQF   DC  CL1        Global audit failure flag.
API_RLST_SECLEVL  DC  CL3        Security level.
API_RLST_NUMMEM   DC  CL4        Number of members.
API_RLST_NUMUSER  DC  CL4        Number of users/groups.
API_RLST_NUMPGMS  DC  CL4        Number of programs.
API_RLST_INSTDATA DC  CL255      Installation data field.
                      ORG API_RLST_RESERVED
API_RLST_MEMBUSRS DC  ???XL1     When the members, users or conditional
*                                access list is requested the data will be
*                                returned into this area.
```

プロファイルまたはメンバー名が返された場合、そのプロファイルまたはメンバー名は総称である可能性があります。その場合、表示可能な形式には変換できません。表示可能な形式に変換するには、汎用文字に関する RACF 命名規則の知識が必要です。

```
Generic Character                Converted To

The first'.'                     X'02'
Ending double asterisks          X'FD'
Ending single asterisks          X'FC'
Internal double asterisks        X'FBFC90'(when a general resource class)
                                 X'FCFC' (when not a general resource class)
Internal single asterisk         X'FBFC80'
Percent sign                     X'FB'
Ampersand                        X'FA70'
```

メンバーのリストが返される場合の出力形式は以下のとおりです。

```
Description                      Length

Length of member                 4 bytes
Member name                      ? bytes (length determined by length field)
```

ユーザーのリストが返される場合の出力形式は以下のとおりです。

```
Description                     Length

Length of userid                4 bytes
Userid                          8 bytes
Length of access field          4 bytes
Access                          1 byte  X'80' Alter access
                                        X'40' Control access
                                        X'20' Update access
                                        X'10' Read access
                                        X'01' None
```

条件付きアクセス・リストが返される場合の出力形式は以下のとおりです。

```
Description                       Length

Length                            14 bytes
Filler                            8 bytes
Length of userid                  4 bytes
Userid                            8 bytes
Length of access field            4 bytes
Access                            1 byte  X'80' Alter access
                                          X'40' Control access
                                          X'20' Update access
                                          X'10' Read access
                                          X'01' None
Device type length                3 bytes
Device type                       8 bytes
Device name length                3 bytes
Device name                       ? bytes (length determined by length field)
```

いずれの場合も、先頭の長さフィールドがゼロ (x'00000000') であれば、それがデータの終わりを示します。

USRDATA 関数 (ユーザーの USRDATA フィールドのリストおよび管理)

USRDATA 関数を使用して、ユーザー・プロファイルの USRDATA フィールドのリスト、追加、更新、または削除を行います。USRDATA への更新のために作成される特殊な SMF レコードについては、79 ページの『zSecure CICS Toolkit で作成された SMF レコード』を参照してください。

AUTHORITY

このコマンドを使用するユーザーは、zSecure CICS Toolkit コマンドに対するアクセス権限を持っている必要があります。要求された関数によってプロファイルは異なり、LIST 関数の場合は TOOLKIT.USRL、ADD 関数と UPDATE 関数の場合は TOOLKIT.USRA、DELETE 関数の場合は TOOLKIT.USRD です。 ユーザーは、USRN.*usrdata-name* 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。影響を受けるユーザー ID は、USRDATA 管理関数の有効範囲内に存在している必要があります。そのため、ユーザーは、USRU.*dfltgrp* に対するアクセス権限を持っている必要があります。

COMMAREA

最小サイズは 365 バイトです。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC        DC  CL4'USRD'   Function code for USRDATA management
API_RC          DC  XL01'00'    Return code
API_MSG         DC  CL79' '     Message area
*
API_USRD_RC     DC  XL1         Return code.
*                               01      Invalid function in CODE1 below
*                               03      Data from L(ist) function does
*                                         not fit in commarea
*
API_USRD_CODE1  DC  CL1         Type of command being performed
*                               'L' to list all or one USRDATA field
*                               'A' to add a USRDATA field
*                               'U' to update a USRDATA field
*                               'D' to delete a USRDATA field
*
API_USRD_CLASS  DC  CL8         Must be 'USER' followed by four blanks
API_USRD_PROF   DC  CL8         Profile (=USERID)
API_USRD_USRN   DC  CL8         The name of the USRDATA field
API_USRD_USRV   DC  CL255       The value for the USRDATA field
*
API_USRD_USRDLS DC  CL8         Space for returned USRDATA
                DC  CL255       names and values
```

この API には、指定されたユーザーの USRDATA を リストするための 3 つの方法が用意されています。CODE1 に L を選択し、**PROF** だけに値を指定した場合は、すべての **USRDATA** フィールドが USRDLST に返されます。**USRN** の値も指定した場合は、指定された USRDATA 名の値が USRV に返されます。**USRV** フィールドに値が存在する場合は、要求された USRDATA 値の先頭の数文字に、その値が使用されます。この

最後の関数に対して、zSecure CICS Toolkit は、最初に一致した USRDATA の名前と値のペアから取得した追加文字を USRV に付加します。

LIST 関数と DELETE 関数を除き、zSecure CICS Toolkit は、重複する USRDATA 名をサポートしません。同じ名前を持つ USRDATA の名前と値ペアが複数存在する場合は、重複する名前がなくなるまで、名前の検査と削除だけを行ってください。

LIST 関数を使用する場合は、USRN.*usrdata-name* によって権限が付与されている USRDATA の名前または値だけが返されます。 すべての USRDATA の名前または値を要求した場合、返されるリストからは、自分が権限を持っていない項目が除外されます。

すべての USRDATA の名前または値のリストを要求した場合は、用意した commarea 内に完全に収まる名前と値だけが提供されます。さらに、**API_USRD_RC** が設定され、オーバーフロー条件が示されます。すべての値が必要な場合は、十分に大きな commarea を用意してください。

注 : それぞれの USRDATA 値に対して予約されているスペースは、データの実際の長さにかかわらず 255 バイトです。

VERIFY 関数 (ユーザー ID とパスワードまたはフレーズの検査)

VERIFY 関数は、ユーザー ID とパスワードまたはパスワード・フレーズの検査に使用します。

AUTHORITY
NONE

COMMAREA
最小サイズは 101 バイトです。Newpass、Termid、または APPL を使用する場合は、最小サイズは 125 バイトです。パスワード・フレーズを使用して検査するには、最小 226 バイトが必要です。また、新規パスワード・フレーズの指定時には 327 バイトが必要です。

アプリケーション内では、SCQTMAC ライブラリーが提供する CQTMAPIA または CQTMAPIC のマッピング・マクロ (コピーブック) を使用します。

```
API_FUNC          DC  CL4'VERF'   Function code for VERIFY.
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_VERF_RC       DC  XL01'00'    Return code from VERIFY.
*                                 If  non-zero the command failed.
*                                 API_MSG will give the reason
*                                 for the failure.
*
API_VERF_USERID   DC  CL08'USERID  '      The userid being verified.
*
API_VERF_PASSWORD DC  CL08'PASSWORD'      The password for this userid.
*
API_VERF_NEWPASS  DC  CL08'NEWPASS'       The new password for this userid.
*
API_VERF_TERMID   DC  CL08'TERMINAL'      A terminal id.
*
API_VERF_APPL     DC  CL08'APPLNAME'      An application name.
* Next fields only if length=>226
API_VERF_PHRASE_LEN  DC XL1'09'           Length of phrase
API_VERF_PHRASE      DC CL100'ABCDEFGHI'  Password phrase
* Next fields only if length=>327
API_VERF_NPHRASE_LEN DC XL1'00'           Length of new phrase
API_VERF_NPHRASE     DC CL100' '          New password phrase
```

VERIFY 関数によってユーザーの CICS サインオンが実行されることはありません。この関数は、当該ユーザー ID に対して入力されたパスワードまたはフレーズが正しいかどうかだけを検査します。 この関数は、内部で RACROUTE REQUEST=VERIFY を、LOG=ASIS を指定して使用し、無効なパスワードやフレーズを検出した場合は、SMF レコードおよびメッセージ出力が生成されます。

システム・パラメーターによっては、ユーザー ID とパスワードまたはフレーズの検査に複数回失敗すると、そのユーザー ID が取り消される場合があります。

以下のオプション・パラメーターを指定することもできます。

API_VERF_NEWPASS
新規パスワードを指定すると、ユーザー・パスワードが指定の新規パスワードに変更されます。**API_VERF_PASSWORD** フィールドに現在の有効なユーザー・パスワードを入力しないと、新規パスワードは許可されません。

API_VERF_TERMID
端末 ID が存在し、RACF で端末検査がオンになっている場合は、この端末を使用するための ユーザー権限が、現在の日時で検査されます。

API_VERF_APPL
端末名が存在し、RACF でアプリケーション検査がオンになっている場合は、このアプリケーションを使用するためのユーザー権限が検査されます。

このコマンドは、API 経由のみで使用することができます。

API_VERF_PHRASE_LEN および API_VERF_PHRASE
ブランクのみを含む API_VERF_PASSWORD フィールドを指定する場合、VERIFY 関数にフレーズを使用できます。API_VERF_PASSWORD フィールドに非ブランク文字が含まれている場合、API_VERF_PHRASE フィールドは無視されます。検査にフレーズを使用するには、API_VERF_PHRASE_LEN フィールドにパスワード・フレーズの正確な長さを指定する必要があります。また、API_VERF_PHRASE フィールドにはユーザーの現行のフレーズを組み込み、ブランクを埋め込む必要があります。

API_VERF_NPHRASE_LEN および API_VERF_NPHRASE
VERIFY 関数にフレーズを使用する場合、新規フレーズを指定することもできます。パスワードを使用して検査する場合、新規フレーズは無視されます。新規フレーズを指定するには、API_VERF_NPHRASE_LEN フィールドに新規パスワード・フレーズの正確な長さを指定し、API_VERF_NPHRASE フィールドに、ユーザーの現行パスワード・フレーズおよび埋め込みブランクを組み込む必要があります。長さ API commarea が 327 バイト以上の場合、API_VERF_NPHRASE_LEN の値がゼロでない限り、新規パスワードが存在するとみなされます。

サンプル・プログラム

製品の一部として、ユーザーが使用できるいくつかのプログラム例が付属しています。

API インターフェースの 使用方法を示す一般的な例を 116 ページの『単純な API インターフェース』に示します。117 ページの『リソース・プロファイル・リスト・インターフェース』に示す例は、リソース・プロファイル・リスト API の使用法を示した単純なプログラムです。

単純な API インターフェース

API の使用方法を示すサンプル・プログラムは、SCQTSAMP データ・セットに収録されています。このプログラムは、RSRX という API インターフェースを 使用してリソース検査を実行する方法を示したものです。

これらのプログラムのユーザー・インターフェースは 単純であり、検証や追加の処理は実行されません。この例は、API とアプリケーション・プログラムとの間で情報を受け渡すための CQTMAPIA 領域の使用法を示すためのもので、それ以外の用途はありません。

このサンプル・プログラムをインストールするには、マップ・セットとプログラムを変換してコンパイルし、CICS に対してリソースを定義します。以下のリソース定義例を参照してください。

```
DEFINE PROG(CQTXAPIR) L(ASSEMBLER) EXECKEY(USER) DA(ANY) GROUP(CQTSAMP)
DEFINE TRANSACTION(XAPI) PROG(CQTXAPIR)
       PROFILE(CQTSAMP) GROUP(CQTSAMP) TASKDATALOC(ANY)
DEFINE MAPSET(CQTXAMP)  GROUP(CQTSAMP)
```

プログラム CQTXAPIR を使用して、リソース名とリソース・クラスを入力することができます。このプログラムにより、自分がリソースに対するアクセス権限を持っているかどうかが検査されます。代わりに、アクセス権限検査の実行対象として自分以外のユーザー ID を入力することもできます。

この例を現在の環境に合わせて修正したり、フィールドを編集したりすることができます。

リソース・プロファイル・リスト・インターフェース

リソース・プロファイル・リスト・インターフェースの 使用方法を示すプログラムの例は、SCQTSAMP のメンバー CQTXAPIL、CQTXAML、CQTXCPIL、および CQTXCML に収録されています。同じプログラムが、アセンブラーと COBOL の両方の形式で用意されています。

このタスクについて

このプログラムは、BMS マップを使用して初期パネルを表示します。ユーザーはこのパネルで、RSRL (リソース・プロファイル・リスト) API インターフェース 用の一部のフィルターとオプションを 入力することができます。BMS マップのソースは、異なる組み込みメンバーを生成するために 2 回提供されますが、それ以外の点では、これら 2 つのソース・メンバーは同じです。このプログラムは API を呼び出して、出力のいくつかの関連部分を表示します。このプログラムは、API の使用方法を説明し、インストールが正常に完了したかどうかを検査することを目的とするもので、実用的な機能は備えていません。

手順

サンプル・プログラムをインストールするには、以下のようにします。

1. マップ・セットとプログラムを変換してコンパイルし、リンク・エディットを行います。
2. 生成されたモジュールを CICS に対して定義します。

タスクの結果

以下のリソース定義例を参照してください。

```
DEFINE  PROG(CQTXCPIL)     L(COBOL)       EXECKEY(USER)  DA(ANY)  GROUP(CQTSAMP)
DEFINE  TRANSACTION(RSRC)  PROG(CQTXCPIL)
         PROFILE(CQTSAMP)   GROUP(CQTSAMP) TASKDATALOC(ANY)
DEFINE  PROG(CQTXAPIL)     L(ASSEMBLER)   EXECKEY(USER)  DA(ANY)  GROUP(CQTSAMP)
DEFINE  TRANSACTION(RSRA)  PROG(CQTXAPIL)
         PROFILE(CQTSAMP)   GROUP(CQTSAMP) TASKDATALOC(ANY)
DEFINE  MAPSET(CQTXAML)    GROUP(CQTSAMP)
```

注 :

- このプログラム例を使用するには、示したとおりにグループ CQTSAMP をインストールし、トランザクション RSRA または RSRC を実行してください。
- 出力を表示するには、CEBR を使用して、このプログラムの一部として作成される TSQUEUE 全体を表示しなければならない場合があります。
- 作成された TSQUEUE を削除するのは、呼び出し側プログラムの責任です。
- このプログラム例では、使用後に TSQUEUE は削除されません。そのため、トランザクションの終了後にデータを調べることができます。
- テストが完了したら、 手動で TSQUEUE を削除してください。

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、Intel Centrino、Intel Centrino ロゴ、Celeron、Intel 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

B

C

D

I

J

L

O

P

R

S

U

Z

部品番号:

(1P) P/N:

SA88-7159-06