# zSecure Visual

# クライアント・マニュアル

SA88-7157-06

**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、153 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 Visual (製品番号 5655-N20) のバージョン 2、リリース 4、モディフィケーション 0 に適用されます。また、改訂版などで特に断りのない限り、 これ以降のすべてのリリースおよびモディフィケーションにも 適用されます。

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

**原典：**
SC27-5647-06
zSecure Visual
Client Manual
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 Visual により、管理者はメインフレーム・サーバーへの Windows インターフェースを利用し、Microsoft Windows ワークステーションからメインフレームのセキュリティーや 処理の管理を行うことができます。IBM Security zSecure Visual には IBM Security zSecure Visual Server と IBM Security zSecure Visual Client の 2 つのコンポーネントがあります。 本書では、IBM Security zSecure Visual クライアントをインストール、構成、および使用する方法について説明します。

読者は、RACF® の管理用タスクと Microsoft Windows ベースのアプリケーションの 使用に習熟している必要があります。 本書では、IBM Security zSecure Visual サーバーのメインフレーム・コンポーネントがインストールされて構成されていることを前提としています。

**注 :** z/OS® システム 上での Visual サーバーのセットアップおよび 構成に関する情報は「*IBM Security zSecure CARLa-Driven Components* インストールおよびデプロイメント・ガイド」にあります。

## zSecure 資料

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

zSecure の非ライセンス出版物は、IBM Security zSecure Suite (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 ライブラリーから入手できます。

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、お客様ご使用の 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、zSecure_Documentation@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のほかに所属組織のお客様名および番号もお知らせください。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、およびデプロイに関する情報を提供します。
- *IBM Security zSecure Manager for RACF z/VM* ユーザー・リファレンス・マニュアル、*LC27-4364*

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

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

  IBM Security zSecure Manager for RACF z/VM 資料を提供します。これには、ライセンス交付された製品資料とライセンス交付されていない製品資料が含まれています。
- *Program Directory for IBM 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入手可能な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ついての情報が記載されています。プログラム・ディレクトリーは、プロダクト・テープで提供されます。IBM 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。<br>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。<br>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。 |

| 参照先 | 対象 |
| --- | --- |
| 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/OS V2R4 ライブラリーが含まれています。 |
| IBM Z 多要素認証の資料 | IBM Z 多要素認証 (MFA) の資料に関する情報の資料。z/OS V2R4 ライブラリーには、IBM Z 多要素認証の資料 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。 |

IBM Security zSecure Visual の使用方法について詳しくは、以下の資料を参照してください。

- *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*

  z/OS システムで IBM Security zSecure Visual Server をインストール、構成、およびデプロイするための参照情報を示します。

- *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 and Audit for RACF コンポーネントに関する情報を示し、ISPF パネルから機能を使用する方法を説明します。また、RACF の管理と監査のユーザー資料、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 CARLa* コマンド・リファレンス , LC43-2107

  CARLa Auditing and Reporting Language (CARLa) プログラミング言語についての、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。zSecure を用い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に使用できます。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。

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 Configuration Guide* | 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 |

| 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 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 |
| *z/OS Security Server RACF* 監査担当者のガイド | SA88-5718 |
| *z/OS Security Server RACF* コマンド言語 解説書 | SA88-6226 |
| *z/OS Security Server RACF* マクロおよびインターフェース | SC43-2673 |
| *z/OS Security Server RACF* メッセージおよびコード | SA88-5839 |
| *z/OS Security Server RACF* システム・プログラマーのガイド | SA88-7029 |
| *z/Architecture®* 解説書 | SA88-8773 |

## アクセシビリティー

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

## 技術研修

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 に関して提供されているコース、および CARLa とサンプル・アプリケーションをすぐに使い始めるための情報については、IBM Knowledge Center for zSecure V2.4.0 の zSecure Wiki の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 システムおよび IT 製品は存在せず、 また単一の製品、サービス、およびセキュリティー対策が、不適切な使用または アクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、包括的なセキュリティーの取り組みの 一部となるように設計されており、これらには必ず追加の運用手順が伴います。ま た、最高の効果を得るために、他のシステム、製品、またはサービスを必要とす る場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

# 第 1 章 IBM Security zSecure Visual のセットアップと構成

zSecure Visual をクライアントで使用するには、以下の作業が必要です。

- ビジュアル・クライアントとして使用するシステムに、クライアント・ソフトウェアをインストールします。
- Visual サーバーがインストールされているメインフレームでクライアントを 定義します。
- Visual サーバーに接続してセッションを確立するようにクライアントを構成します。

zSecure Visual サーバーをメインフレームにインストールする方法については、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照してください。既知の問題と制約事項については、IBM Security zSecure V2.4.0 の IBM Knowledge Center の「このリリースについて」のリリース・ノート (www.ibm.com/support/knowledgecenter/SS2RWS_2.4.0/com.ibm.zsecure.doc_2.4.0/welcome.html) を参照してください。

インストールと構成については、以下のトピックで説明します。



**関連概念**

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理
IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

## リリース情報

zSecure のリリース情報には、新機能と拡張機能、非互換性の警告、および資料の更新情報に関する詳細が含まれています。

最新版の『新機能』と『リリース・ノート』については、IBM Security zSecure V2.4.0 の IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SS2RWS_2.4.0/com.ibm.zsecure.doc_2.4.0/welcome.html) の『このリリースについて』を参照してください。

## インストールの前提条件

zSecure Visual クライアントをインストールする 前に、システムが以下のハードウェア要件とソフトウェア要件を満たしていることを確認してください。

**ハードウェア要件**

- 1 GHz 以上のプロセッサー
- 512 MB 以上の RAM
- 最低 350 MB のディスク・スペース
- 最低 S-VGA のディスプレイ
- メインフレームに接続するための TCP/IP アダプター
- .NET Framework バージョン 4 のクライアントの場合の最低ディスク・スペースは次のとおりです。
  - 32 ビット: 600 MB
  - 64 ビット: 1.5 GB

**ソフトウェア要件**

- Microsoft Windows 7、Windows 8、Windows 10、Windows Server 2008R2、Windows Server 2012、Windows Server 2016、または Windows Server 2019。

  オペレーティング・システムのレベルは、ワークステーション開始時に確認できます。
- IBM Knowledge Center ヘルプ・システムを操作するには、Internet Explorer 9 以上、Mozilla Firefox 17 以上、Google Chrome 20 以上、または Microsoft Edge 37 以上のいずれかのブラウザーを使用してください。IBM Knowledge Center ヘルプ・システムのすべての 機能を使用できるようにするには、以下の作業を行います。
  - ブラウザーで Cookie と JavaScript を有効にします。
  - ブラウザーでポップアップ・ウィンドウのブロックを無効にします。
- メインフレーム上の zSecure Visual サーバーに接続するには、以下を構成する必要があります。
  - メインフレームとの接続を提供する TCP/IP ネットワーク
  - クライアントがインストールされているローカル・ホストの名前

メインフレーム上の zSecure Visual サーバーに接続するには、メインフレーム上で以下のソフトウェアをインストールして構成します。

- サポートされている z/OS のリリース (V2R4 まで)
- RACF Security Server
- TCP/IP

- IBM Security zSecure Visual 2.4.0 サーバー

インストールの後に、クライアント上でメインフレームに接続するためのサーバー定義を作成する必要があります。サーバー定義の準備として、以下の設定を確認します。

- サーバーの IP アドレスまたは名前
- サーバーの TCP ポート番号
- クライアント ID
- 初期パスワード

この情報は、システム管理者から入手できます。

## IBM Security zSecure Visual のインストール

以下のタスクを実行して、Visual クライアント・コンポーネントをインストールします。

### このタスクについて

ワークステーションには、IBM Security zSecure Visual クライアントの新規バージョンを *1* 回 しかインストールできません。以前にインストールしたバージョンのクライアント (バージョン 2.3.1 など) については、アップグレードすることができます。クライアントのアップグレードのガイドラインについては、6 ページの『IBM Security zSecure Visual のアップグレード』および「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の『IBM Security zSecure Visual および zSecure コンポーネントの互換性』を参照してください。

新しい Visual クライアントを同じワークステーションに複数回インストールすることはできませんが、1 つのクライアントで複数の Visual サーバーの定義を設定し、複数の Visual クライアント・インスタンスを同時に実行することができます。9 ページの『複数の Visual サーバー定義』を参照してください。

Windows 用 zSecure Visual クライアント・ソフトウェアは、CD で提供されています。この CD には、 PDF 形式の zSecure Visual クライアント・マニュアルも収録されています。

**注 :** zSecure Visual サーバーのインストールと 構成については、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照してください。

zSecure Visual クライアント・プログラムの完全バージョンまたはカスタム・バージョンのいずれかをインストールできます。

完全バージョンのインストール・プログラムでは、Java ランタイムがインストールされます。現在使用しているバージョンの Java ランタイムを引き続き使用する場合は、カスタム・バージョンのインストールを使用して、Java ランタイムのインストールをバイパスするように指定します。

このセクションでは、各タイプのインストールを実行する手順を示します。

### 手順

Visual クライアント・プログラムをインストールするには、以下の手順を実行します。

1. Visual クライアントをインストールするシステムがハードウェア 要件およびソフトウェア要件を満たしていることを確認します。2 ページの『インストールの前提条件』に記載されている要件を確認します。
2. 以下のいずれかの操作を選択してインストールを開始します。
   - *CD* から直接インストールする。
     a. Visual クライアントをインストールするシステムで CD を挿入します。CD を挿入すると、インストールが自動的に開始されます。
     b. 自動インストールが失敗した場合や取り消された場合は、ルート・ディレクトリーから **zSecureVisualLauncher.exe** を実行してインストールを開始します。
   - *LAN* ディレクトリーからインストールする。
     a. CD イメージのネットワーク・ロケーションを指定する。

b. インストール・ディレクトリーに 1 つ以上のスペースが含まれる場合、ファイル・パスを以下の例のように引用符で囲んで指定する必要があります。

```
"C:¥installation dir¥visual240¥DISK1¥setup.exe"
```

3. 「Welcome」ウィンドウで「**Next**」をクリックします。
4. ご使用条件に同意して「**Next**」をクリックします。

   **注 :** 「**Print**」をクリックすると、使用条件の条項を印刷できます。 ライセンス・ファイルは ¥License サブディレクトリーにあります。ライセンスは、英語およびターゲット・マシンで構成されているロケール言語で表示できますが、それ以外の言語では表示できない場合があります。
5. 以下のオプションのいずれかを選択し、「**Next**」をクリックします。

   **Complete**
   すべてのプログラム・ファイルをデフォルト・ディレクトリーにインストールします。これは通常の使用のためのオプションで、より多くのディスク・スペースを使用します。

   **Custom**
   上級者に対して 2 つのオプションを提供します。

   - プログラム・ファイルをデフォルト・ディレクトリーにインストールしたくない 場合は以下を実行します。

     a. 「**Change...**」をクリックして、デフォルト・ディレクトリー (C:¥Program Files (X86)¥IBM ¥Security zSecure Visual¥2.4.0) 以外のインストール・ディレクトリーを指定します。

     **重要 :** Windows システム・フォルダーが宛先ドライブに配置されていない場合、宛先ドライブにファイルを受け取る十分なスペースがあることが判明していても、「**Next**」をクリックすると以下の警告が発生する場合があります。

     ```
     There is not enough space to install these option(s).
     Please free some disk space or modify your selections.
     ```

     この警告は、Windows システム・フォルダーを含むドライブを指しています。警告が発生した場合は、「Custom Setup」ダイアログの「Feature」説明領域を使用して選択したコンポーネントで必要となるスペース量を判定し、Windows システム・フォルダーが含まれているドライブにも十分なスペースがあることを確認してください。

     b. ファイルをインストールするディレクトリーを 参照するか、または「**Folder name**」フィールドに完全ファイル・パスを指定します。

     **注 :** 以前のバージョンの Visual クライアントをアップグレードする 場合、各バージョンはそれ専用のフォルダーに存在する必要があります。 異なるバージョンを区別できるように、フォルダー名称にバージョン番号が表示されていることを確認してください。

     c. 「**OK**」をクリックして「Custom Setup」ウィンドウに戻ります。
   - 製品に関連するヘルプ・ファイルをインストールしたくない場合 (宛先ドライブのスペースが限られている場合など) は、以下を実行します。

     a. 「**Help Files**」>「**This feature will not be available**」をクリックします。

     **注 :** -->最初の 2 つのオプション (先頭が「**This Feature**...」) は同じインストールを実行します。どちらの場合もすべてのヘルプ・ファイルがインストールされます。

     b. 「**Space**」をクリックしてヘルプ・ファイルのストレージ要件を表示します。

     c. 「**OK**」をクリックして「Custom Setup」ウィンドウに戻ります。
6. 「**Install**」をクリックしてインストールを開始します。
7. 「**Finish**」をクリックしてインストール・プログラムを終了するか、「**Launch zSecure Visual**」をクリックして Visual クライアントを開始し、Visual サーバーへ接続するようにクライアントをセットアップします。

### 次のタスク

zSecure Visual を使用するには、最初に構成を行う必要があります。構成は手動または自動で行うことができます。構成について詳しくは、7 ページの『IBM Security zSecure Visual の構成』を参照してください。

インストールがエラーなしで完了しなかった場合は、ログ・ファイルを調べることで原因のトラブルシューティングに役立つ情報が得られる場合があります。この情報は詳細にわたり、専門家による使用を目的としています。

## IBM Security zSecure Visual の保守

管理者は、以下の保守関連トピックに従って、IBM Security zSecure Visual のアンインストール、変更、および修復を行います。

IBM Security zSecure Visual のアンインストール、変更、および修復を行うことができます。このセクションでは、これらのタスクを実行する手順について説明します。

フィックスパックは zip ファイルで提供されます。有効にインストールすると、クライアントの既存のインスタンスが上書きされます。

### IBM Security zSecure Visual のアンインストール

管理者は、以下のタスクを実行して、IBM Security zSecure Visual をアンインストールしてください。

#### 手順

IBM Security zSecure Visual とそのすべてのコンポーネントを完全に除去するには、以下のステップを実行します。

1. 「コントロール パネル」に移動します。
2. 「**プログラムと機能**」を選択します。
3. 「**IBM Security zSecure Visual 2.4.0**」を選択します。
4. アンインストール・プログラムが共有ファイルを検出すると、警告メッセージが表示されます。「**Yes**」をクリックして続行します。

   保守プログラムが IBM Security zSecure Visual の除去を開始します。

   保守プログラムが完了すると、「Maintenance Complete」画面が表示されます。

### IBM Security zSecure Visual の変更

管理者は、以下のタスクを実行して、IBM Security zSecure Visual 内の選択したインストール済みコンポーネントを変更してください。

#### このタスクについて

上級者であれば、Visual クライアントのインストール済み環境を変更して、新規プログラム・コンポーネントを追加したり、現在インストール済みのコンポーネントを削除したりできます。

#### 手順

Visual クライアントのインストール済み環境を変更するには、以下のステップを実行します。

1. 「コントロール パネル」を開いて「**プログラムと機能**」を選択します。
2. 「**IBM Security zSecure Visual 2.4.0**」を右クリックして「**Modify**」を選択します。
3. 「Select Components」ウィンドウで、変更するコンポーネントを選択します。
4. 「**Next**」をクリックしてインストールを変更します。セットアップ・プロセスをモニターするための「Setup Status」ダイアログが表示されます。

   変更が完了すると、「Maintenance complete」画面が表示されて保守プログラムが終了します。

### IBM Security zSecure Visual の修復

管理者は、以下のタスクを実行して、IBM Security zSecure Visual のすべてのプログラム・コンポーネントを再インストールしてください。

#### このタスクについて

破損したファイルが見つかった場合は、すべてのプログラム・コンポーネントを再インストールします。すべてのプログラム・コンポーネントを再インストールするには、以下のステップを実行します。

#### 手順

1. 「コントロール パネル」を開いて「**プログラムと機能**」を選択します。
2. 「**IBM Security zSecure Visual 2.4.0**」を右クリックして「**Repair**」を選択します。
3. 修復プロセスが完了したら、「**Finish**」をクリックします。

## IBM Security zSecure Visual のアップグレード

zSecure Visual サーバーをアップグレードした後に、クライアント・マシン上の zSecure Visual クライアント・ソフトウェアをアップグレードし、新しいサーバー・インスタンスに接続することができます。

#### 始める前に

以下の情報について、Visual サーバー管理者に確認してください。

- サーバー名/IP アドレス
- サーバーの TCP ポート
- 推奨される zSecure Visual クライアントのバージョン

#### このタスクについて

3 ページの『IBM Security zSecure Visual のインストール』で説明されている方法を使って、IBM Security zSecure Visual をアップグレードすることができます。新しいインストールにサーバー定義はまったく含まれていません。サーバー定義は、前のバージョンからコピーすることができます。これについては 10 ページの『複数のサーバー定義のためのコピー機能』で説明します。自動化プロセスを使用することもできます。詳しくは、15 ページの『アップグレード・パスの自動化の例』を参照してください。

この手順によって、以前の証明書を使用し、かつ新しいサーバーを指す新しいサーバー定義が、新しいクライアントに作成されます。以前の証明書をコピーすると、クライアント用に新しい初期パスワードを作成することなくアップグレード・プロセスを実行できます。

#### 手順

zSecure Visual クライアント・ソフトウェアをアップグレードするには、以下のステップを実行します。

1. 新しいクライアント・ソフトウェアをインストールします。
2. クライアントを開始します。
3. 構成を更新してサーバー定義を作成します。
   a) ビジュアル・クライアント・メニューから、「**File**」>「**Configure**」>「**Copy**」を選択します。
   b) 「Copy configuration」パネルで、Visual サーバーの **IP アドレス**または**名前**および **TCP ポート**を更新して、アップグレードされたサーバーの 場所を指すようにします。
   c) 「**Test Connection**」をクリックして接続を検査します。
   d) 「**OK**」をクリックして、変更を保存し、新しいサーバー定義を作成します。

# IBM Security zSecure Visual の構成

Visual クライアントに対して Visual サーバーを定義するには、以下の構成タスクを使用します。

### このタスクについて

IBM Security zSecure Visual を構成するには、Visual サーバーをクライアントに対して定義し、Visual クライアントを Visual サーバーに対して定義します。このトピックでは、Visual サーバーのクライアントに対する定義方法を説明します。クライアント定義を Visual サーバーに追加する方法については、150 ページの『クライアント定義の保守』を参照してください。

Visual サーバーの定義が保管される場所は、「**View**」**->**「**Options**」メニューでの選択内容によって異なります。

「**Save server definitions in per-user folder**」チェック・ボックスを選択しないと、サーバー定義は ProgramData フォルダーの C:¥ProgramData¥IBM¥Security zSecure Visual¥2.4.0¥Servers (デフォルトの場所) に格納されます。ProgramData フォルダーには、システムの全ユーザーのアプリケーション・データが格納されています。Visual サーバー定義は、当該システムにログオンするすべてのユーザーが使用可能です。

「**Save server definitions in per-user folder**」チェック・ボックスを選択すると、サーバー定義はユーザー・レベルの AppData フォルダー (例えば、C:¥Users¥User1¥AppData¥Roaming¥IBM¥Security zSecure Visual¥2.4.0¥Servers) に格納されます。AppData フォルダーには、システムの特定のユーザーのアプリケーション・データが格納されています。Visual サーバー定義を使用できるのはこのユーザーのみです。AppData フォルダーに保管されたサーバー定義は、そのユーザーのローミング・プロファイルの一部になります。したがって、この同じユーザーが、ネットワーク環境内の複数のシステムでこのサーバー定義を、システムごとに構成することなく使用できます。

### 手順

1. サーバーがクライアントに定義されていない場合は、プログラムを開始すると自動的にプログラムの構成部分が開始されます。そうでない場合は、メインメニューから「**File**」**>**「**Configure**」を選択できます。

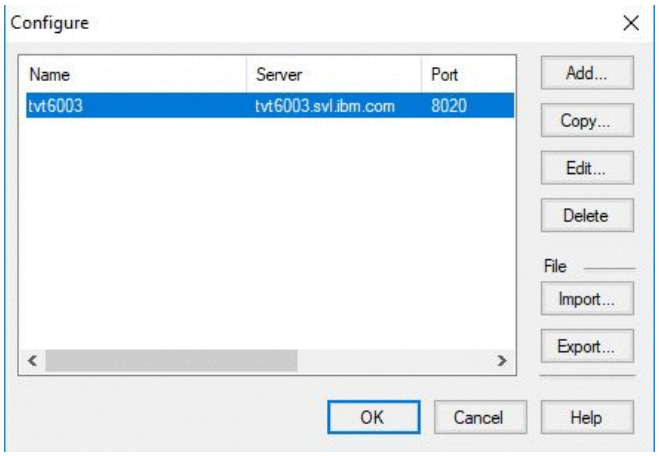



図 *1.* 「*Configure*」ダイアログ

構成ウィンドウでは、定義されているサーバーがすべて表示され、サーバー定義の追加、コピー、編集、および削除を行うことができます。リストに「Edit required」と表示された場合は、サーバーを使用する前に、対応するサーバー定義を完成させる必要があります。

「*Import*」機能では、用意された構成ファイルからサーバー定義情報を読み取ることができます。「*Export*」では、自動のセットアップと構成を可能にする構成ファイルを作成することができます。

2. 1 つのサーバー定義または複数のサーバー定義を追加、編集、または削除したら、「**OK**」をクリックしてすべての変更を適用します。状況ウィンドウが開き、プログラムを構成するために実行されたステップが表示されます。

## サーバー定義パラメーター

Visual クライアントの「**Add system**」ダイアログを使用して、Visual サーバー定義を作成および編集します。

サーバー定義は、このセクションにリストされたパラメーターで構成されます。 フィールドの入力が完了したら、「**OK**」をクリックして入力を確定します。「**Test connection**」を使用して、サーバーがアクティブかどうかを検査できます。「**Name**」以外のすべてのフィールドをブランクのままにして、IBM Security zSecure Visual を別途実行したときに定義を完成させることもできます。

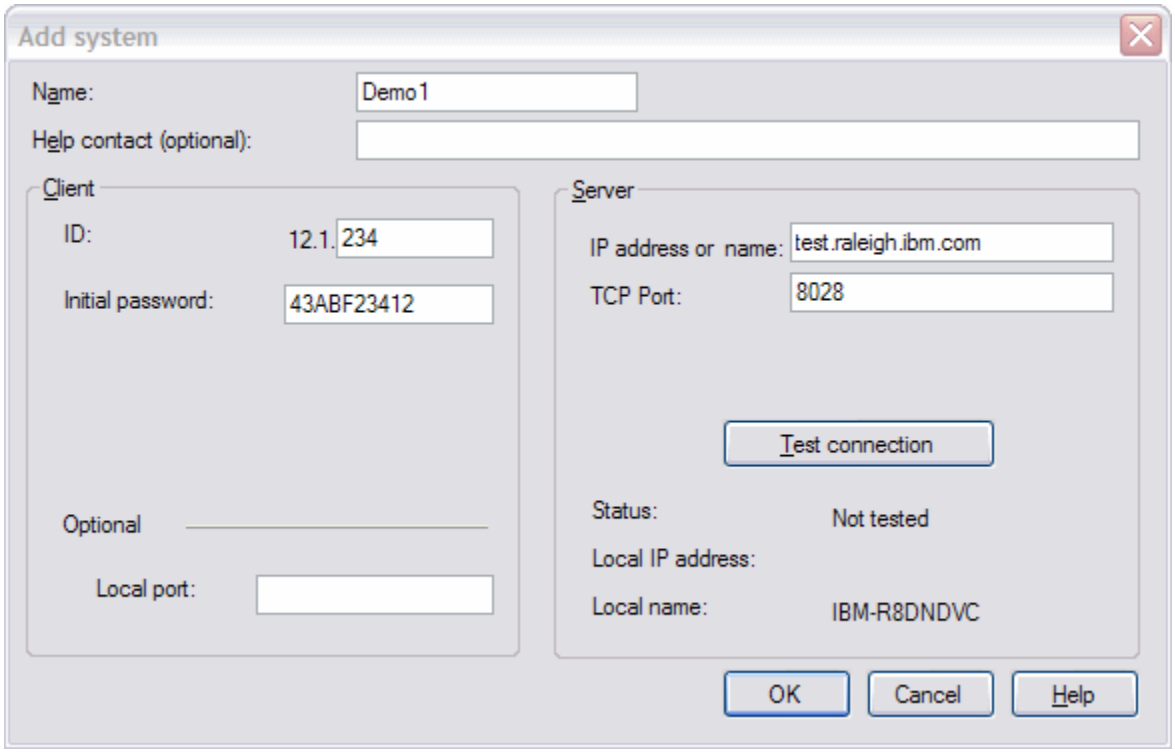



図 *2.* サーバー定義ダイアログ

サーバーを使用するには、証明書が必要です。正しい初期パスワードを入力すると、証明書を得られます。

**重要 :** 新しい証明書を取得する場合は、ローカル・ワークステーションの時計がメインフレーム・サーバーの時計と同期していることを確認してください。時計が同期していないと、エラーになる可能性があります。

サーバー定義パラメーターについては、以下のリストを参照してください。

**Name**
この任意の名前は、特定のサーバー定義を指します。この名前は「**Logon**」ダイアログに表示されます。この名前は、PC 上で固有でなければなりません。また、サーバーに関連するファイルを保管するサブディレクトリーが作成されるため、Windows で有効なファイル名にする必要があります。

**HelpContact (オプション)**
問題発生時の連絡先となるユーザーの個人名や所属名などの情報を入力します。このフィールドがブランクでなければ、その値が次のようにエラー・ダイアログに表示されます。「Error 3: Time Out. Contact *helpcontact*」

**クライアント ID**
この数値により、クライアントはそのサーバーで一意に識別されます。これは常に 12.1.*n* で、*n* は 2 から 2,147,483,647 の範囲の整数です。通常、この ID はサーバーで定義されます。クライアントを使用するには、事前にその ID を確認して入力する必要があります。

**サーバーの IP アドレスまたは名前**
サーバーの IP アドレスまたは完全修飾ホスト名です。

**サーバー・ポート**
サーバー・エージェントが listen するポート。 ポート番号は 0 から 65535 の整数です。 複数の zSecure サーバー・インスタンスに接続するために複数のサーバー定義を構成する場合は、9 ページの『複数の Visual サーバー定義』でポート値の指定に関するガイドラインを参照してください。

**Local port (オプション)**
クライアント・エージェントは、サーバーおよびユーザー・インターフェースと 通信するために 2 つのポート番号を使用します。 これらのポート番号のデフォルトは、サーバー・ポート番号およびサーバー・ポート番号 + 1 です。

2 つのサーバーが同じポート番号を使用している場合は、ポートの競合が発生します。このフィールドを使用して、デフォルトのローカル・ポート番号を指定変更することができます。ユーザー・インターフェースでは、ローカル・ポート番号 + 1 が使用されます。 複数の zSecure サーバー・インスタンスに接続するために複数のサーバー定義を構成する場合は、9 ページの『複数の Visual サーバー定義』でポート値の指定に関するガイドラインを参照してください。

組織で Cisco Jabber® を使用していて、それが zSecure Visual より前に始動された場合、ローカル・ポート 8001 を要求します。zSecure Visual サーバーの「**Test connection**」は正常に終了しますが、完全なログイン試行には失敗します。(デフォルトの) ポート 8000 と 8001 を使用できないためです。このため、まず zSecure Visual を始動するか、8000 と 8001 以外のローカル・ポートを指定してください。

**初期パスワード**
新しい証明書を取得するために必要な 10 桁の 16 進数のパスワード。証明書は、暗号化に使用されます。通常、初期パスワードはメインフレームのシステム 管理者から入手できます。

**接続のテスト**
サーバーの IP アドレスまたは完全修飾ホスト名、およびサーバー・ポートが正しいかどうかを検査するには、「**Test connection**」をクリックします。しばらくすると、「`Connect succeeded`」または「`Connect failed`」が状況フィールドに表示されます。

**注 :**

- サーバー・パラメーターが正しくても、サーバーが稼働していない場合は接続が失敗します。
- Cisco Jabber が zSecure Visual より前に始動され、8000 と 8001 以外のローカル・ポートが指定されていなかった場合、接続は正常に終了しますが、ログイン試行には失敗します。『Local port (オプション)』を参照してください。

## 複数の Visual サーバー定義

以下のガイドラインに従って、複数の Visual サーバー定義の実装を計画します。

同一ワークステーションに新規 Visual クライアントを複数回インストールすることはできません が、1 クライアントに複数の Visual サーバー定義を作成することができます。複数の Visual クライアント・インスタンス (セッション) を同時実行できます。Visual サーバーへのログオン時に選択するサーバー構成に基づいて、各セッションで別々の RACF データベースを管理できます。

zSecure Server を複数のノードに対してサービスを提供するよう構成した場合、その zSecure Server を使用する Visual サーバーは、単一セッションで複数のノードおよび RACF データベースを管理できます。単一セッションで複数のノード (および RACF データベース) を管理するには、クライアントをマルチシステム・モードで実行する必要があります。19 ページの『ローカルで作業するか多重システム環境で作業するかの選択』を参照してください。

複数の Visual サーバーを同時に管理するには、各 Visual サーバーで固有のポート番号が使用されるようにする必要があります。例えば、サーバー TCP 8000 を使用して複数の Visual サーバー定義を作成した場合、ビジュアル・クライアントは各サーバーから着信するトラフィックに同じローカル・ポート番号 (基本ポート + 1 = 8001) を使用しようとします。これは、ポート競合の問題の原因となるため、回避しなければなりません。ポート使用時の競合を回避するために、以下の 2 つの方法で複数の Visual サーバーを構成することができます。

- Visual サーバーを別々のポート番号で実行します。例えば、サーバー X がポート 8000 を、サーバー Y がポート 8010 を、サーバー Z がポート 8020 を使用する場合、ビジュアル・クライアントはローカル・ポート 8001、8011、および 8021 を自動的に使い分けて、この 3 つのサーバーと通信します。

- 複数の Visual サーバーが既に同じポート番号 (ポート 8000 など) を使用して稼働している場合は、サーバー定義ダイアログの「**Local port**」フィールドを使用して、異なるサーバーから着信するトラフィックを分離することができます。例えば、サーバー X のサーバー定義で「**Local port**」フィールドをブランクのままにすると、そのサーバーはポート 8001 を使用することになります。サーバー Y にはローカル・ポート番号 8010 を指定し、サーバー Z にはポート番号 8020 を指定できます。

### 複数のサーバー定義のためのコピー機能

コピー機能を使用して、複数の Visual サーバー定義を作成します。

クライアントは、アクセスするサーバーごとに定義を必要とします (8 ページの『サーバー定義パラメーター』を参照)。ただし、定義全体を常に最初から入力する必要はありません。異なるバージョンの IBM Security zSecure Visual 間で、サーバー定義をコピーすることができます。 その場合は、ポートが競合しないようにしてください。必要であれば、システム管理者に問い合わせてください。

コピー機能を使用すると、既存のサーバー定義の完全なコピーが表示されます。定義のフィールドの一部は、変更できないように使用不可になっています。

## 自動化セットアップおよび構成

自動化されたセットアップと構成を使用して、Visual クライアントの初期インストールを実行できます。

### 構成ファイル

構成ファイルを使用して、zSecure Visual の構成パラメーターを配布します。

構成ファイルを使用すると、同じ情報を再度入力する必要がなくなります。パラメーターはファイルに書き込みます。ターゲット・コンピューターは、セットアップと構成の際にそのファイルを読み取ります。

#### 構成ファイルの作成

構成ファイルを作成するには、zSecure Visual を使用します。

#### このタスクについて

構成ファイルを作成する際に、その変更内容によって PC が影響を受けることはありません。構成するサーバーおよびセットアップのデータ・オプションは、すべて 1 つのファイルに保存されます。

#### 手順

構成ファイルを作成するには、以下のステップを実行します。

1. メインメニューから「**File**」>「**Configure**」を選択して、構成ダイアログを表示します。
2. 「**Export**」をクリックしてエクスポート・モードに切り替えます。
   以下のウィンドウが表示されます。

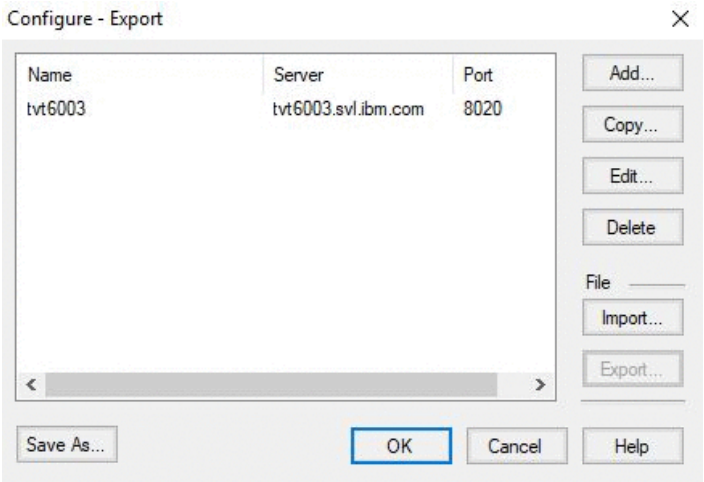



図 3. エクスポート・モードの構成ダイアログ

**注 :** エクスポート・モードとの切り替えが誤って行われないようにするために、「**Add**」、「**Edit**」、「**Delete**」、または「**Import**」のいずれかのアクションを実行すると、「**Export**」ボタンが使用不可になります。

この時点から、構成を変更しても PC には影響しませんが、「**OK**」をクリックすることで、変更したサーバーとセットアップのデータが構成ファイルに書き込まれるようになります。中間の状態を保存する場合は、「**Save As**」を使用します。

3. 手動構成または自動化構成のパラメーターを指定します。

   **手動セットアップ**
   サーバー・データを指定する場合は、「**Add**」、「**Copy**」、「**Edit**」、「**Delete**」、および「**Import**」の各機能を使用します。

   一般に、PC で定義したすべてのサーバーをファイルに保存することはありません。組み込まないサーバーをすべて削除したり、指定しないフィールド (クライアント ID など) をクリアしたりすることが可能です。
4. 構成プロセスの任意の時点で構成ファイルの暫定版を保存するには、「**Save As**」をクリックし、構成ファイル名を指定します。
5. 構成ファイルを保存するには、「**OK**」をクリックします。

### 構成ファイルのレイアウト

構成ファイルに内容を追加するには、構成ファイルのレイアウト・パラメーターの説明を使用します。

サーバーを定義する設定は、Server セクションにあります。構成ファイルには、複数の Server セクションを含めることができます。

**NAME=*server_definition_name***
サーバー定義名を指定します。

**CLIENTID=12.1.*n***
クライアント ID を指定します。ここで *n* は 2 から 2,147,483,647 の範囲の整数です。

**SERVERIP=*server_name***
サーバーの IP アドレスまたはホスト名を指定します。

**SERVERPORT=*port_nr***
サーバーの IP ポートを指定します。

**HELPCONTACT=*help_contact***
エラー・ダイアログに表示される、ヘルプの連絡先情報を指定します。

### ターゲット・マシンでの構成ファイルの実行

**setup** コマンドを実行して、システム上の zSecure Visual を構成できます。

#### 手順

- ターゲット・マシンでは、構成ファイル名をコマンド行引数としてセットアップを実行します。

  <絶対パス>¥setup /s /v"CMDVISUAL=<構成ファイルの絶対パス>"

  **重要 :**

  – CMDVISUAL オプションは大文字で指定してください。
  – 絶対パスを指定した場合にのみ、IBM Security zSecure Visual は構成ファイルを見つけることができます。
- インストールが終了すると、セットアップにより、構成ファイルを入力パラメーターとして IBM Security zSecure Visual が開始されます。

### 構成ファイルからのサーバー定義のアップデート

**c2racvn** コマンドを実行して、システム上の Visual サーバー定義を更新します。

#### 手順

- ターゲット・マシンでは、構成ファイル名をコマンド行引数として IBM Security zSecure Visual を実行します。

  <絶対パス>¥c2racvn <構成ファイルの絶対パス>

- サーバー定義は、構成ファイル内のパラメーターに従って更新されます。更新が終了すると、プログラムは直ちに終了します。

### 構成の制限

zSecure Visual の構成ファイルを作成する際は、以下の構成の制限のガイドラインに従ってください。

以下のような、構成に関する制限に注意してください。

**構成ファイルでの初期パスワードの保管**
セキュリティー上の理由から、初期パスワードは構成ファイルに保存できません。

**ターゲット・マシンでのサーバー名の変更**
ターゲット・マシンではシステムの名前を変更できません。これは、以前の名前を構成ファイルに書き込めないためです。

**構成ファイルの作成と使用には同じバージョンが必要**
IBM Security zSecure Visual は、同じバージョンを使用して作成された構成ファイルのみを読み取ることができます。バージョンが異なると、サーバー定義はコピーされません。

### 既存の構成ファイルの変更

管理者は、以下のタスクを実行して、zSecure Visual の構成ファイルを変更してください。

#### このタスクについて

既存の構成ファイルを変更できます。 構成ファイルの変更または使用に関するガイドラインについては、12 ページの『注記』 を参照してください。

#### 手順

既存の構成ファイルを変更するには、以下のステップに従ってください。

1. **エクスポート**・モードに切り替えます。
2. すべてのサーバーを削除します。
3. 編集する構成ファイルをインポートします。
4. データを編集します。
5. ファイルを同じ名前で保存します。

#### 注記

管理者は、以下のガイドラインに従って、zSecure Visual の構成ファイルを作成および変更してください。

**構成ファイルを使用した証明書のコピー**
構成ファイルを使用して、証明書をコピーできます。構成ファイルを準備する際、それがシステム上にあるかのようにコピーを実行します。コピーは、ターゲット・マシンで構成ファイルが読み取られるときに実行されます。構成ファイルを作成しているマシン上にない証明書をコピーするには、サーバー名とバージョンを直接入力します。

**構成ファイル内のブランク・フィールド**
ブランクのままにしたサーバー・パラメーターは、構成ファイルに保存されません。ターゲット・マシンに同じ名前のサーバーが存在する場合は、ブランク・フィールドが変更されないままとなります。

**構成ファイル内のクライアント ID**
ターゲット・コンピューターには固有のクライアント ID が必要です。 複数のターゲット・コンピューターで使用される構成ファイルにはクライアント ID を指定できません。「Client ID」フィールドで 12.1 の後にドットを指定すると、ターゲット・マシンによって、このドットが他のサーバー定義のクライア

ント ID で置換されます。この処理は、他のすべてのサーバー定義に同じクライアント ID が含まれている場合にのみ行われます。

**既存の構成ファイルの変更**
手順については、12 ページの『既存の構成ファイルの変更』 を参照してください。

**構成ファイルのタスク例**
zSecure Visual の構成ファイルを実装するには、以下のタスク例を使用します。

**手順**

1. 例 1: 複数のクライアントに対して 1 つのサーバーで自動化セットアップおよび構成を準備する
   a) IBM Security zSecure Visual を開始します。
   b) メインメニューから「**File**」>「**Configure**」を選択します。
   c)「**Export**」を選択し、構成ファイルの準備を行うことを確認します。
   d) ターゲット・マシンで構成するサーバー定義が得られるまで、「**Add**」、「**Edit**」、および「**Delete**」の各機能を使用してサーバー定義を編集します。

      指定できるのは、「**Name**」、「**Help contact**」、「**Server IP address**」または「**name**」、および「**TCP Port**」だけです。「**Client ID**」フィールドは、ターゲット・マシンごとに固有にする必要があるため、ブランクにします。この例では、「**Local Host**」と「**Local Port**」もブランクのままとなっています。
   e)「**OK**」をクリックし、構成ファイルを `setup2.cfg` として保存します。これで構成ファイルが完成しました。
   f) 各ターゲット・マシンで次のコマンドを実行します:

      ```
      c2racvn setup2.cfg
      ```
   g) 上記のステップが完了したら、ターゲット・マシンで正しいクライアント ID および初期パスワードを指定します。
2. 例 2: 複数のクライアントに 1 つの新しいサーバーを追加する
   a) IBM Security zSecure Visual を開始します。
   b) メインメニューから「**File**」>「**Configure**」を選択します。
   c)「**Export**」を選択し、構成ファイルの準備を行うことを確認します。
   d) ターゲット・マシンで構成するサーバー定義が得られるまで、「**Add**」、「**Edit**」、および「**Delete**」の各機能を使用してサーバー定義を編集します。

      指定できるのは、「**Name**」、「**Help contact**」、「**Server IP address**」または「**name**」、および「**TCP Port**」だけです。「**Client ID**」フィールドは、ターゲット・マシンごとに固有にする必要があるため、ブランクにします。この例では、「**Local Host**」と「**Local Port**」もブランクのままとなっています。
   e)「**OK**」をクリックし、構成ファイルを `setup2.cfg` として保存します。これで構成ファイルが完成しました。
   f) 各ターゲット・マシンで次のコマンドを実行します:

      ```
      c2racvn setup2.cfg
      ```
   g) 上記のステップが完了したら、証明書を取得するために、ターゲット・マシンで正しい初期パスワードを指定します。

## サイレント・インストール

zSecure Visual のサイレント・インストールを計画する際は、以下のガイドラインに従ってください。

サイレント・インストール とは、ユーザーとの対話なしで実行されるインストールです。

サイレント・インストールを成功させるには、最初のマシンとターゲット・マシンの構成がほぼ同じであることが必要です。インストールするターゲット・フォルダーの有無といった、セットアップ手順に影響する違いがあると、インストールが失敗する可能性があります。

サイレント・インストールでは、最初のインストールで記録されたご使用条件の受け入れが、すべてのターゲット・マシンに適用されることを前提としています。したがってサイレント・インストールでは、ユーザーとの対話なしにライセンス・ファイルがターゲット・システム上の指定されたディレクトリーにコピーされ、状況ファイルが作成されます。

サイレント・インストールの問題のトラブルシューティングに役立つように、インストール・プロセスをログに記録する必要があります。14 ページの『サイレント・インストールのログ・ファイル』を参照してください。

### サイレント・インストールのログ・ファイル

zSecure Visual のサイレント・インストールのログ・ファイルの場所を指定できます。このセクションでは、ログ・ファイルの指定方法について説明します。

サイレント・インストールごとにログ・ファイルが作成されます。場所を指定しないと、ログ・ファイルは、setup.log という名前で、zSecureVisualSetup.exe を含むフォルダーに作成されます。

ログ・ファイルの場所を指定するには、次のオプションを使用します。

-f2<ログ・ファイルの絶対パス>

診断のために、次のコマンド行オプションを使用して詳細ログを作成することができます。

/g<詳細ログの絶対パス>

詳細ログには、インストール・プロセスのステップがエラー・メッセージとともに記録されます。この情報は、インストール中の問題を解決するための手掛かりとなります。

**重要 :** セットアップ・ログのファイル名が競合しないように注意してください。

### サイレント・インストール・コマンドの例

サイレント・インストールを実行するには、適切なコマンド行オプションを指定してセットアップ・プログラムを実行します。このセクションでは、いくつかの例を示します。

以下の例では、標準の Microsoft コマンド行パラメーターを InstallShield セットアップ・コマンドと共に使用します。CMDVISUAL プロパティーのみが、zSecure Visual クライアント・アプリケーションの固有のものです。

パラメーターを必要とするコマンド行オプションは、オプションとそのパラメーターの間にスペースを入れずに指定します。例えば、以下のコマンドは有効です。

```
zSecureVisualSetup.exe /v"INSTALLDIR=c:¥MyDirectory"
```

以下のコマンドは無効です。

```
zSecureVisualSetup.exe /v "INSTALLDIR=c:¥MyDirectory"
```

オプションのパラメーターにスペースが含まれている場合にのみ、オプションを引用符で囲みます。

パラメーター内のパスにスペースが含まれている場合、次の例のように、引用符の中にさらに引用符を使用する必要がある場合があります。

```
zSecureVisualSetup.exe /v"INSTALLDIR=¥"c:¥My Directory¥""
```

#### デフォルト設定のサイレント・インストール

```
zSecureVisualSetup.exe /s /v"/qn”
```

#### 異なるターゲット・ディレクトリーを指定したサイレント・インストール

```
zSecureVisualSetup.exe /s /v"/qn INSTALLDIR=<c:¥target_directory>"
```

**異なるターゲット・ディレクトリーおよびログ・ファイルを指定したサイレント・インストール**

```
zSecureVisualSetup.exe /s /v"/l*v c:¥test.log
INSTALLDIR=<c:¥target_directory> /qb"
```

**デフォルト設定およびリブートなしを指定したサイレント・インストール**

```
zSecureVisualSetup.exe /s /v"/qn /norestart ”
```

## アップグレード・パスの自動化の例

/COPYSERVERS セットアップ・コマンド行オプションを使用して、zSecure Visual のアップグレードを自動化できます。

初期インストールが終了したら、ユーザーがサーバーにログオンする前に IBM Security zSecure Visual をある程度構成する必要があります。アップグレードの場合は、/COPYSERVERS セットアップ・コマンド行オプションを使用して構成を自動化できます。 システム上で既に定義されているすべてのサーバー定義が新規インストール・バージョンに複製されるので、インストール直後にそれらはすぐ使用できる状態です。

**例:**

以下の例の前提は次のとおりです。

- 対話式インストールにのみ適用されます。
- COPYSERVERS オプションを大文字で指定する必要があります。
- 最新のサーバー定義のみをコピーします。

  **注 :** マシンに複数のバージョンの zSecure Visual がインストールされている場合は、最も新しいバージョンのサーバー定義がコピーされます。それより古いバージョンはスキップされます。

**例 1:**

```
zSecureVisualSetup.exe /s /v"/qn CMDVISUAL=/COPYSERVERS”
```

**例 2:**

以下の例では、Visual クライアントの新規バージョンのインストール前に、既存のバージョンをアンインストールするよう指定しています。

```
zSecureVisualSetup.exe /x /s /v"/qn CMDVISUAL=/COPYSERVERS”
```

# 第 2 章 IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

IBM Security zSecure Visual は、IBM RACF セキュリティー・ データベースを Windows ワークステーションから保守します。 以下のトピックでは、カスタマイズ・タスクと基本タスクの一部について説明します。

**関連概念**

IBM Security zSecure Visual のセットアップと 構成

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理

IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

2 ページの『リリース情報』

19 ページの『ローカルで作業するか多重システム 環境で作業するかの選択』

タスクの範囲を制限または拡張するには、ローカルの RACF データベース上のユーザーおよびリソースを操作したり、 複数システム間の複数ノードに定義されているユーザーおよびリソースを操作したりできます。

19 ページの『ログオン』

プログラムがユーザーによる操作の範囲を判別できるように、Visual クライアントにログオンします。

20 ページの『使用可能なノードの選択』

多重システム・モードでログオンする場合、 使用可能なノードのリストを得るために、zSecure サーバーに対して照会が行われます。 zSecure サーバーに定義されているノードは、ビジュアル・クライアントから使用できるようになります。作業対象の zSecure ノードと RACF リモート共有機能 (RRSF) ノードを選択してください。

21 ページの『サンプルの最初のタスク』

サンプルの最初のタスクとして、ユーザー、グループ、およびリソースに関連するさまざまな操作を実行するためにユーザー・インターフェースを 使用することができます。

22 ページの『ログオフ』
タスクを完了したら、Visual クライアントをログオフします。

22 ページの『終了』
Visual クライアントは、Visual サーバーをログオフした後に終了してください。

22 ページの『サーバー定義名をオフにする』
簡単なファイルと項目を作成することで、Visual クライアントでのサーバー定義名の表示をオフにすることができます。

23 ページの『ログ・ファイルの表示』
cesys ファイルと ceaud ファイルでは、ログに記録された Visual アプリケーションに関する情報を確認できます。

24 ページの『「Communication」ウィンドウの使用』
「Communication」ウィンドウを使用して、zSecure Visual クライアントとメインフレーム 側のコンポーネントおよびプログラムとの間で交換された情報を表示します。

25 ページの『表示設定の指定』
IBM Security zSecure Visual の表示方法を指定するには、「**Options**」ダイアログを 使用します。

27 ページの『アクセス・レベルに応じたインターフェース ・オプションの設定』
自分に割り当てられたアクセス・レベルに応じて、特定のグループのオプションを 表示するようにインターフェースを 調整できます。

28 ページの『日付形式の設定』
日付を表示するために、独自の形式を定義することも、定義済みの形式を選択することもできます。

30 ページの『ドラッグ・アンド・ドロップ機能』
ユーザーは、ドラッグ・アンド・ドロップ機能を使用して、RACF データベース内のユーザーや接続を変更できます。

30 ページの『コピー・アンド・ペースト機能』
「**Copy**」、「**Paste**」、および 「**Paste Special**」の各機能を使用して、さまざまなコピー、マージ、および移動タスクを実行できます。

30 ページの『ツールバー・ボタン』
Visual クライアントのツールバー ・ボタンを使用すると、最も頻繁に使用されるメニュー・オプションを表示できます。

30 ページの『右マウス・ボタン』
行を右クリックすると、「**Navigate**」および「**Action**」の各オプションを表示できます。

30 ページの『命名規則』
ユーザーおよびグループの名前を作成するときは、以下のガイドラインに従ってください。

31 ページの『列の順序の変更』
クリック操作とドラッグ操作を使用して、テーブル列の配置を変更したり、列の境界線を変更したりできます。

31 ページの『サイト固有の列およびフィールド』
組織に固有の情報が構成されている場合は、その情報を参照することができます。

31 ページの『印刷可能なデータの保存とエクスポート』
印刷可能なテーブルを CSV 形式で保存したり、通信ウィンドウを RTF 形式でエクスポートしたりできます。

32 ページの『印刷』
Visual クライアントでデータの印刷および印刷プレビューの表示が可能です。

32 ページの『印刷ファイルのプレビュー』
Visual クライアントで、印刷ファイルのレイアウトをプレビューして変更できます。

32 ページの『印刷可能なテーブル』

Visual クライアントで以下のテーブルおよびリストを印刷できます。

33 ページの『「Server Information」ダイアログ』
「**Server Information**」ダイアログには、現在ログオンしているサーバーに関する情報が表示されます。

33 ページの『? 文字の表示』
フィールドがユーザーの範囲に含まれていない場合は、疑問符 (?) が表示されます。

## ローカルで作業するか多重システム環境で作業するかの選択

タスクの範囲を制限または拡張するには、ローカルの RACF データベース上のユーザーおよびリソースを操作したり、 複数システム間の複数ノードに定義されているユーザーおよびリソースを操作したりできます。

### 始める前に

管理者が多重システム環境でユーザーとリソースを操作するには、最初に以下のタスクを実行する必要があります。

1. zSecure サーバーおよび Visual サーバーを、複数のシステム上にある複数の RACF データベースを管理するように構成します。「*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」を参照してください。
2. Visual サーバーに接続するビジュアル・クライアント上で、サーバー定義を作成して検査します。7 ページの『IBM Security zSecure Visual の構成』を参照してください。

### 手順

- ローカルで作業する場合は、ビジュアル・クライアントの「Options」ダイアログで、「**Use zSecure Server for multi-system services**」オプションが 選択されていない ことを確認してください。 デフォルトでは、このオプションは選択されていません。ローカル・モードで 動作している場合、ビジュアル・クライアントは、 zSecure サーバーに対してノードの詳細情報を要求しません。
- 多重システム環境でユーザーおよびリソースを操作するには、多重システム・モードで動作するように Visual クライアントを設定します。多重システム・モードを指定するには、以下のステップを使用してください。
  a)「**スタート**」>「**すべてのプログラム**」>「**Security zSecure Visual**」の順に選択して、ビジュアル・クライアントを開始します。
  b)「**View**」>「**Options**」の順に選択して、 「Options」ダイアログを開始します (25 ページの『表示設定の指定』を参照)。
  c)「**Use zSecure Server for multi-system services**」>「**OK**」の順に選択します。

  この多重システム環境用に構成されたシステムのリストを受け入れるか、 または、セッションのアクションの適用対象とするシステムを指定することが求められます。

  **注 :** クライアントが zSecure サーバーとのセッションを確立できなかった場合、クライアントはサーバーがアクティブではないことを示すメッセージを出力します。クライアントは操作をローカル・モードで開始します。

## ログオン

プログラムがユーザーによる操作の範囲を判別できるように、Visual クライアントにログオンします。

### このタスクについて

プログラムを開始したら、RACF にログオンして、特定のコマンドに対するアクセス権を判別する必要があります。RACF データベースの CKG プロファイルにより、アクセス・レベルが制御されるためです。メインフレーム上の CKGRACF プログラムからの応答に基づいて、使用可能なスケジュールの名前がロードさ

れ、特定の機能が無効になります。その後、複合システム上で定義されているすべてのクラスのリストが表示されます。

### 手順

以下のステップに従って、メインフレームの RACF にログオンしてください。

1. メインメニューから「**File**」>「**Logon**」の順に選択して、IBM Security zSecure Visual にアクセスします。または、ツールバーの「**Logon**」をクリックします。「**Logon to RACF**」ダイアログが 表示されます。

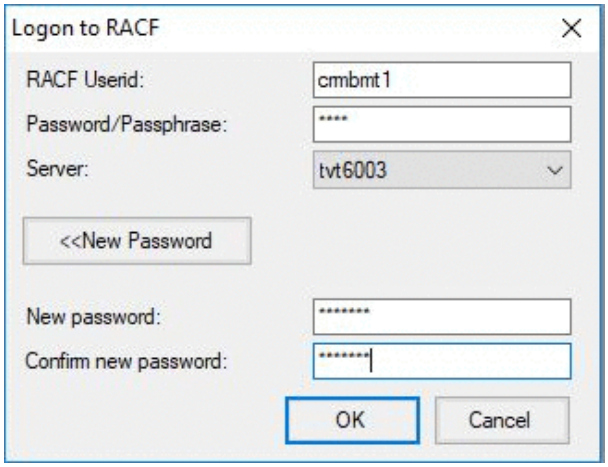



図 *4.* ログオン・ダイアログ

2. メインフレームのユーザー ID およびパスワードまたはパスフレーズを入力します。
   または、「**New Password/Passphrase**」を選択して、パスワードまたはパスフレーズを変更します。
3. 新規パスワードまたはパスフレーズを確認します。
4. 「**OK**」を クリックして先に進みます。

   **注 :** メインフレームへの初回ログオンである場合、暗号によるセキュアな通信チャネルをセットアップするのに 時間がかかります。
5. 多重システム・モードでログオンする場合は、作業を行うノードを選択することが求められます。20 ページの『使用可能なノードの選択』を参照してください。
6. ログオンに成功すると、「**Find**」ダイアログが表示されます。この「**Find**」ダイアログは、ユーザー、グループ、またはリソースを表示または変更する際に使用します。21 ページの『サンプルの最初のタスク』を参照してください。

## 使用可能なノードの選択

多重システム・モードでログオンする場合、使用可能なノードのリストを得るために、zSecure サーバーに対して照会が行われます。zSecure サーバーに定義されているノードは、ビジュアル・クライアントから使用できるようになります。作業対象の zSecure ノードと RACF リモート共有機能 (RRSF) ノードを選択してください。

ノードのリストには、zSecure ノードおよび RRSF ノードが含まれており、これらのノードが「**Node selection**」ダイアログに表示されます。作業対象のノードを決定するための一助として、次のガイドラインを使用してください。

- 処理を続行するには、少なくとも 1 つの zSecure ノードを選択する必要があります。ビジュアル・クライアント が要求をサーバーに送信すると、サーバーはその要求を zSecure ノードに送信します。ノードは、関連付けられている RACF データベースからデータを返します。クライアントは、データを受信した後、そのデータを変更するように zSecure ノードに対して要求を送信します。
- zSecure ノードとしてのみ操作が可能なノードは、「**zSecure Nodes**」列にのみリストされます。
- RRSF ノードとしてのみ操作が可能なノードは、「**RRSF Nodes**」列にリストされます。
- 「**zSecure Nodes**」列および「**RRSF Nodes**」列の下の同じ行にリストされているノードは、両方の環境で使用可能です。

- 選択したノードが、優先ノードのリストとなります。優先される zSecure ノードおよび RRSF ノードを変更するには、「Select Nodes」 ダイアログ (36 ページの『「Select Nodes」ダイアログ: 多重システムのオプション』を参照) を使用します。zSecure ノードの優先リストは、「**Find**」ダイアログの「**>>Advanced**」を選択して、変更することもできます。
- RRSF ノード上で行う操作については、 正常に完了したかどうかが検査されません。RRSF ノードを介して RACF データベースに編集要求を送信できます。ただし、クライアントは、そのアクションの最終的な結果に関するフィードバックを受け取りません。このため、 本ソフトウェアは RRSF の操作が正常終了したと想定します。

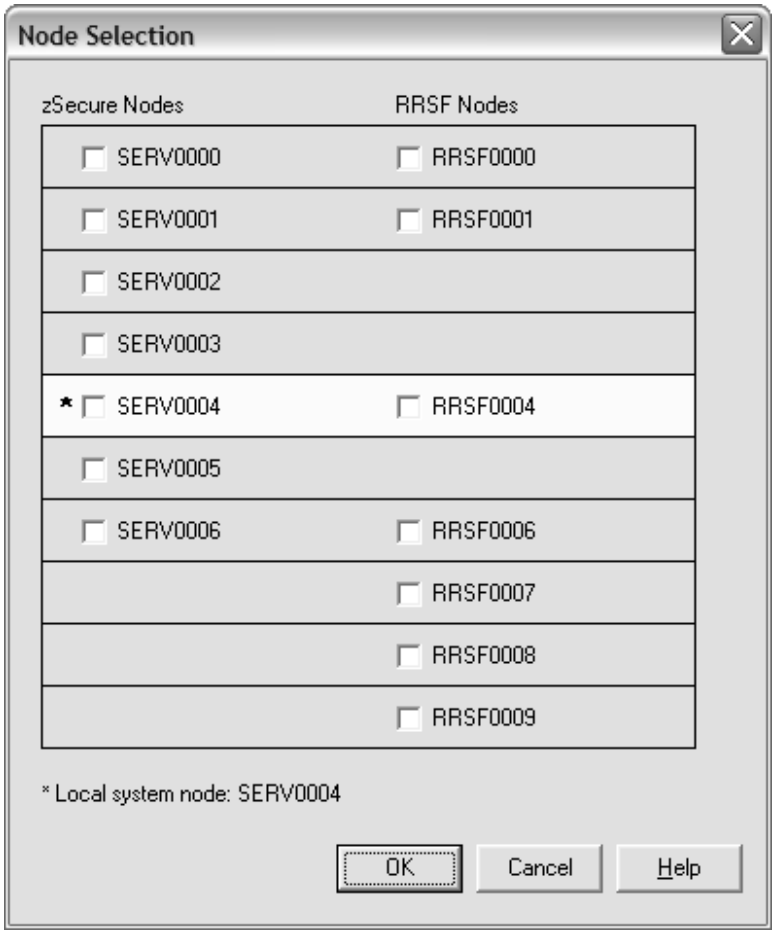



図 *5.* 「*Node Selection*」ダイアログ

## サンプルの最初のタスク

サンプルの最初のタスクとして、ユーザー、グループ、およびリソースに関連するさまざまな操作を実行するためにユーザー・インターフェースを 使用することができます。

### このタスクについて

以下の手順は、ユーザーとグループの間の接続を表示するためのユーザー・インターフェースの 使用方法を示すサンプル・タスクについて説明しています。接続に関するタスクの実行について詳しくは、91 ページの『第 6 章 接続の管理』 を参照してください。

### 手順

1. 「**Find**」ダイアログ・ウィンドウで、「**Class**」のドロップダウン・リストから 「**User**」または「**Group**」を選択します。
2. 「**Search**」フィールドに ユーザーまたはグループの名前を入力し、「**OK**」をクリックします。検索結果ウィンドウが 表示されます。

3. 選択したユーザーまたはグループの接続の内容を表示するには、以下のステップを実行します。
   a) 検索結果ウィンドウから、特定のユーザーまたはグループを選択します。
   b)「**Navigate**」>「**Connects**」の順に選択します。「Connects」ウィンドウに、この特定のユーザーまたはグループに関連するすべてのグループまたはユーザーが表示されます。
   c)「**Connects**」ウィンドウでユーザーまたはグループのいずれかをダブルクリックして 、そのプロパティーを確認します。

## ログオフ

タスクを完了したら、Visual クライアントをログオフします。

### 手順

メインメニューから「**File**」>「**Logoff**」の順に選択して、IBM Security zSecure Visual からログオフします。

## 終了

Visual クライアントは、Visual サーバーをログオフした後に終了してください。

### 手順

1. IBM Security zSecure Visual を終了するには、メインメニューから「**File**」>「**Exit**」を選択します。
2.「**Options**」ダイアログで、終了時に確認を求めるプロンプトをプログラムから出すかどうかを指定します。

   詳しくは、セクション 25 ページの『表示設定の指定』を参照してください。 IBM Security zSecure Visual にまだログオンしている時に「**Exit**」を押した場合、 プログラムは、ログオフしてから終了します。

## サーバー定義名をオフにする

簡単なファイルと項目を作成することで、Visual クライアントでのサーバー定義名の表示をオフにすることができます。

### このタスクについて

IBM Security zSecure Visual クライアントのアプリケーション ・タイトルには、 サーバー定義名が含まれます。サーバー定義名は、 大括弧で囲まれています。デフォルトでは、ログオン時に、アプリケーションが サーバー定義名の表示をオンにし、ログオフ時にオフにしますが、 この機能はオフにすることができます。

### 手順

アプリケーション・タイトル内の サーバー定義名の表示をオフにするには、以下のステップに従ってください。

1. アプリケーション・フォルダーに移動します。デフォルトのディレクトリーは、`C:¥Program Files (x86)¥IBM¥Security zSecure Visual¥2.4.0¥` です。
2. `c2racvn.cfg` という名前のテキスト・ファイルを作成します。
3. 次のオプションを追加します。`ShowHost=No`
4. ファイルを保存します。
5. 変更が有効になるように、終了してから再度ログオンします。

# ログ・ファイルの表示

cesys ファイルと ceaud ファイルでは、ログに記録された Visual アプリケーションに関する情報を確認できます。

### このタスクについて

zSecure Visual クライアントは、エラー、警告、および通知メッセージを取り込むログ・ファイルを提供します。これらのログ・ファイルは、 問題の原因を特定し、重大度を診断するのに有用です。

### 手順

ログ・ファイルにアクセスするには、以下のステップに従ってください。

1. 次に示すログ・ディレクトリーに移動します。
   *user_profile*¥AppData¥Roaming¥IBM¥Security zSecure Visual¥*version*¥Servers¥*ServerName*¥ClientLogs

   ディレクトリーの例: C:¥Users¥Administrator¥AppData¥Roaming¥IBM¥Security zSecure Visual¥*version*¥Servers¥*ServerName*¥ClientLogs

   このディレクトリーには、各種ログが記録されます。ログ・ファイルは、タイトル中にプロセス ID を含むので、クライアントでのさまざまな実行の複数のバージョンを、同じディレクトリーに格納できます。プロセス ID によって区別される、同じ名前のファイルの例を示します。

   ```
   About0480.log
   CKGPRINT0480.log
   Requests0480.log
   SYSPRINT0480.log
   SYSTERM0480.log

   About6412.log
   CKGPRINT6412.log
   Requests6412.log
   SYSPRINT6412.log
   SYSTERM6412.log
   ```

   zSecure Visual クライアントに 関連する問題について報告する際には、これらのログ・ファイルを提供する必要があります。
2. 別のログ・ファイル・ディレクトリーに移動します。ログ・ディレクトリーの場所は、サーバー定義が ProgramData フォルダーと AppData フォルダーのどちらに保管されているかによって異なります。これは、「**View**」 **->** 「**Options**」ダイアログの「**Save server definitions in per-user folder**」オプションで行った選択によって決まります。

   「**Save server definitions in per-user folder**」チェック・ボックスが選択されていなかった場合 (デフォルト)、ログ・ファイル・ディレクトリーは ProgramData フォルダーに格納され、そのディレクトリーは C:¥ProgramData¥IBM¥Security zSecure Visual¥*version*¥Servers¥*ServerName* になります。例: C:¥ProgramData¥IBM¥Security zSecure Visual¥2.4.0¥Servers¥Server_A.

   「**Save server definitions in per-user folder**」チェック・ボックスが選択されていた場合、ログ・ファイル・ディレクトリーは AppData フォルダーに格納され、そのディレクトリーは *user_profile*¥AppData¥Roaming¥IBM¥Security zSecure Visual¥*version*¥Servers¥*ServerName*¥ になります。例: C:¥Users¥Administrator¥AppData¥Roaming¥IBM¥Security zSecure Visual¥2.4.0¥Servers¥Server1¥

   cesys および ceaud という名前のログ・ファイルがこのディレクトリーに保管されます。これらのログ・ファイルには、クライアントとサーバーとの 間の通信層に関する情報が入っています。 この情報はユーザーが解釈するためのものではありませんが、通信関連の問題を診断するのに有用です。 zSecure Visual クライアントに関連する問題について報告する際には、これらのログ・ファイルも提供する必要があります。
3. これらのログ・ファイル内の最新の更新内容を、「Communication」ウィンドウ GUI のタブから参照します。

**注 :** クライアント始動時に、最近 7 日以内のものでないログ・ファイルは消去されます。

メッセージおよび解決案については、「*IBM Security zSecure:* メッセージ・ガイド」を参照してください。

## 「Communication」ウィンドウの使用

「Communication」ウィンドウを使用して、zSecure Visual クライアントとメインフレーム側のコンポーネントおよびプログラムとの間で交換された情報を表示します。

### このタスクについて

「**Communication**」ウィンドウでは、 zSecure Visual クライアントと、メインフレーム側のコンポーネントおよびプログラム (zSecure Visual サーバー、CKRCARLA、CKGRACF、および RACF を含む) との間で 交換された情報の大部分を表示できます。一般的に、クライアントは、 クライアントに関する情報を取得したり、 RACF データベースを変更したりするために、 CKRCARLA および CKGRACF プログラムに対して要求を発行します。「**Communication**」ウィンドウを使用して、 クライアントの要求とその結果に関するログをリアルタイムで表示できます。

「**Communication**」ウィンドウに表示される情報は、 印刷およびリッチ・テキスト・フォーマット (.rtf) へのエクスポートが可能です。32 ページの『印刷』 および 31 ページの『印刷可能なデータの保存とエクスポート』を参照してください。

### 手順

「**Communication**」ウィンドウを表示するには、以下のステップに従ってください。

1. 次のオプションのいずれかを使用して、「**Communication**」 ウィンドウを表示します。
   a) メインメニューから、「**View**」 **>** 「**Communication**」の順に選択します。 または、
   b) ツールバーの 「**Communication**」ボタンを 選択します。このボタンを使用した場合、 「**Communication**」ウィンドウが常に上に 表示されます。

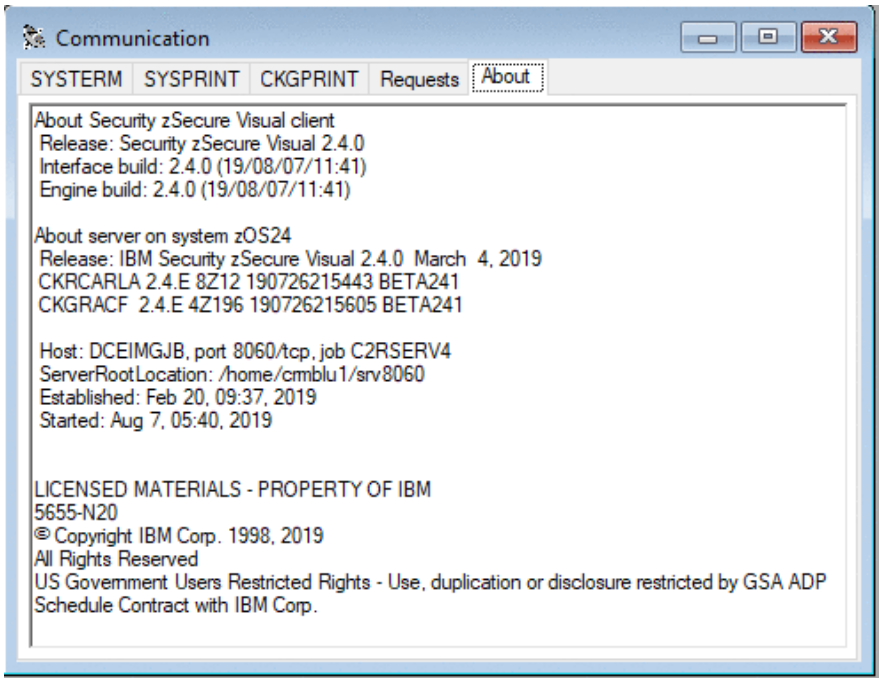



図 6. 「*Communication*」 ウィンドウ

2. 「**Requests**」タブを選択して、 クライアントから 発行されたすべての要求を表示します。これらの要求には、最後の CARLa コマンド、CKGRACF コマンド、およびサーバーに送信されたコマンドが含まれます。 サーバーに送信されたコマンドは、このタブの「*extension*」セクションに表示されます。

3. 「**SYSTERM**」タブを選択して、状況メッセージ、および戻りコード (RC) が 12 以上のメッセージを表示します。
   - 最後の要求が CKRCARLA に対するものであった場合、「*SYSPRINT*」タブに、 CKRCARLA プログラムの詳細な SYSPRINT 出力が入っています。この SYSPRINT 出力には、CKRCARLA リスト、 クリティカル・メッセージ、および通知メッセージが含まれます。この情報は、 問題を発生させているコマンドを特定するのに役立ちます。
   - 最後の要求が CKGRACF に対するものであった場合、「*CKGPRINT*」タブに、 CKGRACF プログラムの詳細な CKGPRINT 出力が入っています。CKGPRINT 出力には、CKGRACF コマンドおよび メッセージが含まれます。この情報は、問題を発生させているコマンドを特定するのに役立ちます。 また、RACF から直接返されたメッセージを表示することもできます。
4. 「**About**」タブを選択して、 クライアントおよびサーバーの 集約情報を表示します。この情報は、テキストとしてコピー・アンド・ペーストが 可能です。このタブには、次の情報が表示されます。
   - クライアント情報: zSecure Visual クライアントの特定のバージョン、 GUI および GUI エンジンのビルド情報。
   - サーバー情報。33 ページの『「Server Information」ダイアログ』を参照してください。
   - 著作権表示。

## 表示設定の指定

IBM Security zSecure Visual の表示方法を指定するには、「**Options**」ダイアログを 使用します。

### 手順

各オプションを設定するには、 以下のステップに従ってください。

1. メインメニューで「**View**」>「**Options**」を選択して、「Options」ダイアログを開始します。

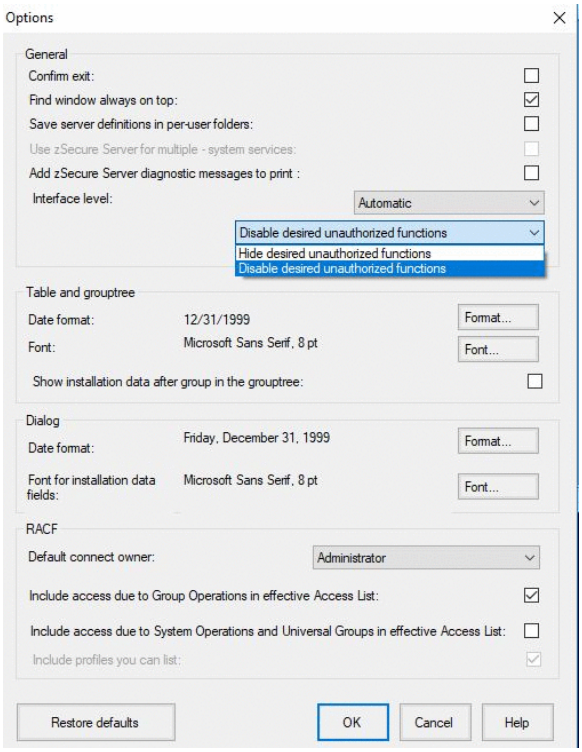



図 7. 「*Options*」ダイアログ

2. (オプション) 必要に応じて全般的な動作を変更します。

   **Confirm exit**
   終了時に確認を求めるプロンプトをプログラムから出すか、または そのまま終了するかを指定します。

**Find window always on top**
「**Find**」ダイアログを 常に上に表示するか、または毎回の検索後に閉じるかを指定します。

**Save server definitions in per-user folder**
サーバー定義の保管場所を指定します。

- このオプションを選択しない場合、サーバー定義は ProgramData フォルダーに保管されます。そのシステムにログオンできるすべてのユーザーが同一のサーバー定義を使用できます。
- このオプションを選択した場合、サーバー定義はユーザーごとの AppData フォルダーに保管されます。AppData フォルダーに保管されたサーバー定義は、そのユーザーのローミング・プロファイルの一部になります。したがって、この同じユーザーが、ネットワーク環境内の複数のシステムでこのサーバー定義を、システムごとに構成することなく使用できます。

**Use zSecure Server for multi-system services**
ビジュアル・クライアントがローカル・モードのみで動作するか、または 多重システム・モードで動作するかを指定します。デフォルトはローカル・モード (チェック・マークなし) です。この動作モードは、ログオンする前に指定しておく必要があります。ログオン中に、 別のモードに変更することはできません。多重システム・モードでの動作については、19 ページの『ローカルで作業するか多重システム環境で作業するかの選択』 を参照してください。

**Add zSecure diagnostic messages to print**
このオプションは、リモート・ノードに対する要求に DEBUG ステートメントを含める場合に選択します。DEBUG ステートメントは、ノードの問題のデバッグに役立つ情報を生成します。トラブルシューティング情報を生成する必要がない場合は、このオプションにチェック・マークを付けないままにしてください。

**Interface level**
ユーザーが使用および表示できる機能を決定します。

3. (オプション) テーブルおよびグループ・ツリーの動作を変更します。

**Date format**
すべてのテーブルに対する日付形式 (これは、列の幅が問題となります)、および すべてのダイアログに対する日付形式の 2 つの日付形式を指定できます。目的の日付形式を指定するには、 リストから日付形式を選択してください。

**Font selection**
2 つの異なるフォントを指定できます。1 つは、テーブルおよびグループ・ツリー用で、 もう 1 つはダイアログ用です。フォント・サイズは 8 から 12 ポイントでなければなりません。

4. (オプション) RACF 動作を変更します。

**Default connect owner**
新規接続のデフォルトの所有者を指定します。接続ダイアログの 「**Owner**」フィールドをブランクのままにした場合、 zSecure Visual は、ここに指定されている所有者を使用します。

**Include access due to Group Operations in effective Access List**
グループ OPERATIONS 属性によって、有効なアクセス・リストを決めるかどうかを 指定します。デフォルトで、このオプションは選択されています。

**Include access due to System Operations and Universal Groups in effective Access List**
システム OPERATIONS 属性および汎用グループのアクセス権限によって、 有効なアクセス・リストを決めるかどうかを指定します。デフォルトでは、 このオプションはオフになっています。

**注意 :** このオプションを選択した場合、zSecure Visual は、 有効なアクセス・リストを作成するために、 RACF データベース全体を読み取る必要があります。これによって、 パフォーマンスが大幅に低下する可能性があります。

**Include profiles you can list**
表示および編集を可能とするプロファイルを決定します。このオプションがオンになっている場合、 編集可能なプロファイルに加えて、 CKGLIST およびグループ AUDITOR の範囲内にあるプロファイルが表示されます。オフになっている場合、 編集可能なプロファイルのみが表示されます。デフォルトで、このオプションは選択されています。

5. 変更が終了したら、次のいずれかのステップを実行します。

a)「**Restore defaults**」をクリックして、 オプションを出荷時のデフォルト値に設定します。
b)「**OK**」をクリックして、変更を受け入れます。
c)「Cancel」をクリックして、設定を変更せずに「**Options**」ダイアログ・ウィンドウを閉じます。

## アクセス・レベルに応じたインターフェース・オプションの設定

自分に割り当てられたアクセス・レベルに応じて、特定のグループのオプションを 表示するようにインターフェースを 調整できます。

### このタスクについて

ユーザーの役割に応じてインターフェースを 調整するには、 「**Options**」ダイアログを使用します。

### 手順

- 「**Interface level**」ドロップダウン・リストから、 管理レベルを 1 つ選択できます。特定のレベルに含まれる全機能について 実行を許可されているわけではない場合、アクセスできないオプションは、非表示にされるか、またはぼかし表示されます。
  管理レベルを変更すると、そのレベルに対応して「**Find**」ダイアログが変わります。次のオプションが、選択できる管理レベルです。

  **Helpdesk**
  Helpdesk は最も低いレベルです。機能は以下に限られます。
  - ユーザーのリスト
  - ユーザーの再開
  - パスワードの設定
  - スケジュールの管理
  - マッピング・プロファイルのリスト
  - ユーザーのマッピング・プロファイルの表示

  **接続 (Connect)**
  このレベルは、**Helpdesk** レベルの機能を拡張して、次を追加したものです。
  - グループのリスト
  - 接続のリスト
  - グループ・ツリーの表示
  - 接続の作成
  - 接続属性の変更
  - 接続の除去

  **User**
  このレベルは、**Connect** レベルの機能を拡張して、次を追加したものです。
  - ユーザーの複写
  - ユーザーのプロパティーの変更
  - ユーザーへの削除マークの付加

  **Access list**
  このレベルは、**User** レベルの機能を拡張して、次を追加したものです。
  - リソースのリスト
  - アクセス・リストのリスト
  - 有効なアクセス・リストのリスト
  - アクセス・リストの変更 (RACF コマンド: permit)

**Group**
このレベルは、Permit レベルの機能を拡張して、次を追加したものです。

- サブグループの追加
- グループの複写
- グループ・プロパティーの変更
- グループの削除

**Full**
Full は、現行で最も高いレベルです。このレベルの機能には、次が含まれます。

- メンバー・リストのリスト
- 範囲のリスト
- リソース・プロファイルの作成
- リソース・プロファイルの複写
- リソース・プロファイルの変更
- リソース・プロファイルの削除
- メンバー・リストの変更
- セグメントの管理

**Automatic**
ユーザーがアクセス権限を持つ、最高の管理レベルを表示します。 CKGRACF SHOW MYACCESS コマンドによってアクセス権限を特定します。

- 右のフィールドで、インターフェースの 表示方法を選択できます。 メインフレーム上で、管理レベルの全コマンドについて許可されているわけではない場合、 次のいずれかのオプションを選択できます。

  **Disable desired unauthorized functions**
  許可されていないすべての機能をぼかし表示します。

  **Hide desired unauthorized functions**
  許可されないすべての機能を表示しません。この設定を使用して、 さまざまなレベル間でさらなるカスタマイズを行うことができます。 より高いレベルを選択し、メインフレーム上の 対応する CKG プロファイルへのアクセス権限を拒否することによって、不要な機能を除去できます。

  CKG プロファイルでは、リスト・コマンドを使用可能にするかどうかを制御できません。 リスト・コマンドは、管理レベルにのみ基づきます。

## 日付形式の設定

日付を表示するために、独自の形式を定義することも、定義済みの形式を選択することもできます。

### このタスクについて

日付形式ダイアログでは、日付の表示方法を指定します。 事前定義形式の 1 つを選択するか、あるいは独自の形式を作成することができます。

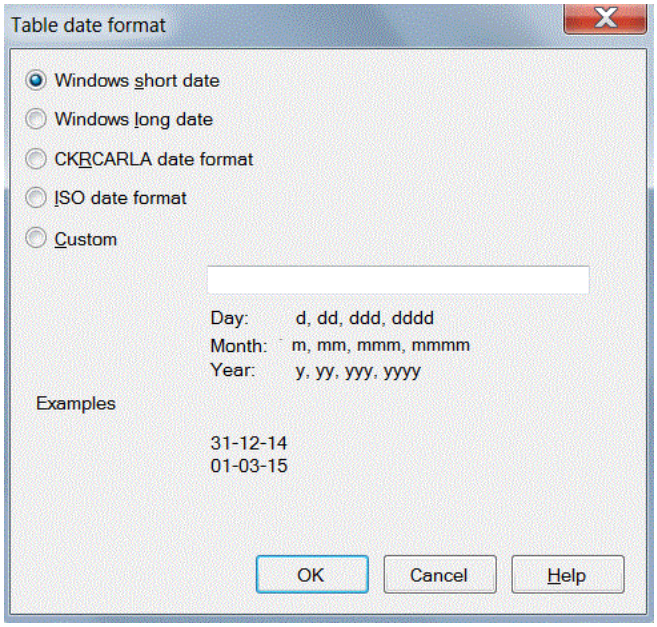



図 *8.* 日付形式ダイアログ

**手順**

- 事前定義形式を指定するには、以下のオプションを使用します。

  **Windows short date**
  Windows の日付形式が、 Windows の構成設定から取得されます。 これらの形式は変更できます。 変更するには、「**コントロール パネル**」>「**時計、言語、および地域**」を選択して、「**地域と言語**」オプションの下の 「**日付、時刻または数値の形式の変更**」をクリックします。形式の変更は、その形式を使用するすべてのアプリケーションに影響を与えます。

  **Windows long date**
  「Windows short date」に関する説明を参照してください。

  **CKRCARLA date format**
  この形式は、メインフレーム上の CKRCARLA プログラムで使用される、 *dd mmm yyyy* という形式です。 この形式に、特別な意味または利点はありません。

  **ISO date format**
  この形式は *yyyy-mm-dd* です。

- 事前定義形式を変更する必要がある場合は、「**Custom**」を選択し、書式制御ストリングの次の文字を使用して独自の形式を作成できます。

  **注 :** 分離文字として **/** および **-** の文字を使用できますが、 Windows の「**コントロール パネル**」>「**時計、言語、および地域**」の設定に定義されている分離文字に置き換えられる可能性があります。 文字の前に **/** を付けることで、 置換を防止できます。

| 表 *2.* 日付の書式制御文字 | |
|---|---|
| d | 1 桁の日付 (必要な場合のみ 2 桁) |
| dd | 2 桁の日付 |
| ddd | 曜日 (3 文字) |
| dddd | 曜日 (フルスペル) |
| m | 1 桁の月 (必要な場合のみ 2 桁) |
| mm | 2 桁の月 |
| mmm | 月の名前 (3 文字) |

| 表 2. 日付の書式制御文字 (続き) | |
|---|---|
| mmmm | 月の名前 (フルスペル) |
| yy | 2 桁の年 |
| yyyy | 4 桁の年 |

## ドラッグ・アンド・ドロップ機能

ユーザーは、ドラッグ・アンド・ドロップ機能を使用して、RACF データベース内のユーザーや接続を変更できます。

RACF データベース内のユーザーまたは接続を変更する場合は、 メニュー、ポップアップ・メニュー、またはツールバーを使用せずに、 ドラッグ・アンド・ドロップを使用します。 毎回のドロップ後に、予期しない変更を防止するために、確認を求めるダイアログまたはポップアップ・ウィンドウが表示されます。 ドラッグ・アンド・ドロップを使用して、 ユーザーの削除および変更、接続の削除、変更、コピー、マージ、および移動を実行できます。 また、サブグループの変更、アクセス・リストとメンバー・リストの変更も可能です。

## コピー・アンド・ペースト機能

「**Copy**」、「**Paste**」、および 「**Paste Special**」の各機能を使用して、さまざまなコピー、マージ、および移動タスクを実行できます。

メインメニューの「**Copy**」、「**Paste**」、および「**Paste Special**」の各オプションを使用して、次の作業を実行します。

- ユーザー、グループ、接続、アクセス・リスト、およびメンバー・リストのコピー
- 接続の作成、マージ、移動、およびコピー

## ツールバー・ボタン

Visual クライアントのツールバー ・ボタンを使用すると、最も頻繁に使用されるメニュー・オプションを表示できます。

ツールバー・ボタンに、最も頻繁に使用されるメニュー・オプションが表示されます。 マウスのカーソルを各ボタンの上に置くと、 説明を示す黄色いポップアップが表示されます。

## 右マウス・ボタン

行を右クリックすると、「**Navigate**」および「**Action**」の各オプションを表示できます。

ほとんどのテーブルおよびグループ・ツリーでは、行を右クリックすると、 ポップアップ・メニューが表示され、使用頻度の高い「**Navigate**」および「**Action**」オプションが示されます。

## 命名規則

ユーザーおよびグループの名前を作成するときは、以下のガイドラインに従ってください。

新規ユーザーまたはグループを追加する場合は、 次の命名規則に従ってください。

- 名前の長さは 1 文字から 8 文字でなければなりません。
- 文字は、A から Z の英字、0 から 9 の数字、または #、$、@ でなければなりません。
- 名前の先頭を数字にすることはできません。
- グループに、別のグループと同じ名前を付けることはできません。

- グループ名を、既存のユーザー ID と同じ名前にすることはできません。

## 列の順序の変更

クリック操作とドラッグ操作を使用して、テーブル列の配置を変更したり、列の境界線を変更したりできます。

### 手順

テーブルの列の再配置、および列のサイズ変更ができます。

- テーブルの列を再配置するには、列同士を比較できるように、列を目的の場所にドラッグします。再配置された列の並びが、 プログラムを次回起動する時のデフォルトの並びとなります。
- 列のサイズを変更するには、縦方向の境界線をクリックして、左または右に移動します。ダブルクリックすると、 列に最小限必要なサイズとなります。

## サイト固有の列およびフィールド

組織に固有の情報が構成されている場合は、その情報を参照することができます。

サイト管理者は、zSecure Visual をカスタマイズして、組織により定義されたユーザー情報を表示することができます。 例えば、サイトで従業員 ID と部門番号を表示したいとします。これらのフィールドは、「ユーザー」プロファイルで「INSTDATA 」列の前かまたはこの列の代わりに表示されます。

管理者が、サイト固有フィールドの数、順序、および特性を定義します。 ユーザーはこれらのフィールドを Visual クライアントでは構成しません。構成の手順はについては、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照してください。

サイト固有フィールドが定義されている場合、これらのフィールドは、ユーザー・プロパティー・ダイアログ、ユーザー・テーブル、および「Find」ダイアログに表示されます。

**ユーザー・プロパティー**
サイト固有列は、「InstData」フィールドを置き換えるか、または「InstData」フィールドに加えて含めることができます。サイト固有フィールドの数に応じて、これらのフィールドは別のタブに表示することができます。フィールドの内容は読み取り専用です。

**ユーザー・テーブル**
サイト固有列を表示するには右にスクロールします。サイトの構成によっては、いくつかのフィールドに対して検索を実行できる場合があります。

**「Find」ダイアログ**
サイト固有列が検索機能付きで指定されている場合、「**>>Advanced**」ボタンを選択すると、このダイアログにフィールドが表示されます。

## 印刷可能なデータの保存とエクスポート

印刷可能なテーブルを CSV 形式で保存したり、通信ウィンドウを RTF 形式でエクスポートしたりできます。

### このタスクについて

印刷可能なテーブルは、すべてコンマ区切り値 (CSV) 形式で保存できます。この形式は、Microsoft Excel などのさまざまなプログラムで 読み取り可能です。また、「Communication」ウィンドウを RTF 形式にエクスポートすることもできます。24 ページの『「Communication」ウィンドウの使用』を参照してください。

### 手順

CSV または RTF の形式でテーブルの情報を保存するには、以下のステップを実行してください。

1.「**File**」>「**Save As**」の順に選択します。
2.「**Save as**」ダイアログで、 ファイル名を入力します。同じ名前が存在する場合、警告ボックスが表示されます。名前を 変更しないと、元のファイルが上書きされます。
3.「**Save**」をクリックします。

# 印刷

Visual クライアントでデータの印刷および印刷プレビューの表示が可能です。

### このタスクについて

データの印刷および印刷プレビューの表示が可能です。

### 手順

データを印刷するには、 以下のステップを実行してください。

1. メインメニューから 「**File**」>「**Print**」を選択するか、 ツールバーのプリンター・アイコンをクリックします。
2. 印刷ダイアログで、該当するオプションを選択します。
   印刷プレビューから印刷する場合は、「**Current Page**」オプションのみが有効になります。
3.「**OK**」をクリックします。

   すべての印刷出力には以下の要素があります。

   - 左端にデータ・リスト名、右端に製品のバージョン番号 が示されたページ・ヘッダー
   - 日付
   - ページ番号

   すべてのリストを印刷して CSV にエクスポートできます。31 ページの『印刷可能なデータの保存とエクスポート』を参照してください。

## 印刷ファイルのプレビュー

Visual クライアントで、印刷ファイルのレイアウトをプレビューして変更できます。

### 手順

1. 印刷プレビューを表示するには、メインメニューから「**File**」>「**Print Preview**」を選択するか、 ツールバーの印刷プレビュー・アイコンをクリックします。
2. キーボードで「**PgUp**」または「**PgDown**」を選択して、プレビュー内をスクロールします。
3. アイコンのリストから、該当する印刷オプションを選択します。
   - 表示された情報を印刷するには、印刷アイコンをクリックします。すべてのページ印刷されます。
   - 印刷ページ上のテキストのサイズを指定するには、ズーム・アイコンを選択します。そのパーセント値は、10、25、50、75、100、150、200、および 500 パーセントです。
   - 印刷ファイルの 1 (デフォルト)、2、3、4、または 6 ページ分のページ・レイアウトを表示するには、ページ・アイコンの 1 つを選択します。
   -「**Close**」をクリックして、メインプログラムに戻ります。

## 印刷可能なテーブル

Visual クライアントで以下のテーブルおよびリストを印刷できます。

以下のトピックで説明されているテーブルを印刷できます。

- 54 ページの『ユーザー・テーブル 』
- 81 ページの『グループ・テーブル』

- 92 ページの『接続テーブル 』
- 104 ページの『リソース・プロファイル 』
- 44 ページの『Permits 機能による特定のユーザー ID またはグループのリソースの選択』.
- 51 ページの『アクセス・リストの表示』
- 52 ページの『有効なアクセス・リストの表示』
- 49 ページの『Scope * の使用』
- 52 ページの『メンバー・リストの表示』.

テーブルを印刷できない場合は、印刷オプションおよびプレビュー・オプションが アクティブではありません。

## 「Server Information」ダイアログ

「**Server Information**」ダイアログには、現在ログオンしているサーバーに関する情報が表示されます。

このサーバー情報を表示するには、メインメニューから「**Help**」>「**Server Information**」を選択します。以下の情報が使用可能です。

- サーバーの CKRCARLA および CKGRACF のリリース情報
- サーバーのホスト名および IP ポート
- zSecure 構成の C2RSERVE パラメーターの解決値として想定される値
- 認証局としてサーバーを確立した時刻
- サーバーを最後に起動した時刻

詳しくは、サーバーの文書を参照してください。

## ? 文字の表示

フィールドがユーザーの範囲に含まれていない場合は、疑問符 (?) が表示されます。

テーブルのフィールドに ? があった場合、 フィールドが範囲外であるためにロードされていないことを示します。

# 第 3 章 RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

この章では、データベースでの作業に使用できるさまざまなオプションについて説明します。 参照したいデータベースへは「**Navigate**」をクリックして移動できます。 個々のユーザー、グループ、およびリソースと、それらの関係、例えば「接続」、「許可」、「スケジュール」などを検索できます。

**関連概念**

IBM Security zSecure Visual のセットアップと 構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

グループ管理

IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

36 ページの『「Select Nodes」ダイアログ: 多重システムのオプション』

「**Select Nodes**」ダイアログでは、操作対象のシステムおよびノードを指定します。

38 ページの『複数システムにまたがるアクションの 検査』

「**Status of**」進行状況フォームを使用して、複数システム・タスクで選択した各ノードのアクションを検査します。

38 ページの『「Find」ダイアログの使用』

「**Find**」ダイアログを使用すると、1 つ以上の RACF データベースのユーザー、グループ、またはリソースを表示できます。

43 ページの『接続しているユーザーおよびグループの表示』

「**Navigate**」>「**Connects**」を選択して、ユーザーおよびグループの接続関係を表示します。

43 ページの『グループの表示』

グループ・ツリーを表示することで、グループおよびサブグループの 階層を把握できます。

44 ページの『Permits 機能による特定のユーザー ID またはグループのリソースの 選択』

特定のユーザー ID またはグループに関連するリソースを選択して、そのリソース・プロファイルを表示することができます。

45 ページの『Scope の使用』
「**Scope**」ダイアログのさまざまなフィルタリング・オプションを使用すると、特定のユーザー ID またはグループからアクセス可能なユーザー、グループ、およびリソースを表示できます。

49 ページの『Scope * の使用』
「**Scope ***」ダイアログのさまざまなフィルタリング・オプションを使用すると、すべてのユーザーからアクセス可能なユーザー、グループ、およびリソースを表示できます。

51 ページの『「RACF SETROPTS Settings」の表示』
SETROPTS コマンドで設定または取得された、システム全体の RACF オプションを表示するには、「RACF SETROPTS Settings」レポートを使用します。

51 ページの『アクセス・リストの表示』
「**Access List**」ウィンドウを使用して、リソース・プロファイルのすべてのユーザー ID のアクセス・リストを表示します。

52 ページの『有効なアクセス・リストの表示』
「**Effective Access List**」ウィンドウを使用して、自分の範囲内にあるリソース・プロファイルのユーザー・グループのアクセス・リストを表示します。

52 ページの『メンバー・リストの表示』
「**メンバー**」ウィンドウを使用して、一般リソース・プロファイルのメンバー・リストを表示します。

42 ページの『「Select class」ダイアログによるクラスの検索』
「**Select class**」ダイアログを使用して、特定のクラスを検索します。

## 「Select Nodes」ダイアログ: 多重システムのオプション

「**Select Nodes**」ダイアログでは、操作対象のシステムおよびノードを指定します。

ビジュアル・クライアントの開始時に、複数システムでの作業を選択すると、 アクションを開始するたびに「**Select Nodes**」ダイアログが表示されます。 例えば、ユーザーまたはグループを複写するために「**Duplicate**」を選択すると、 「**Select Nodes**」ダイアログには優先するノードのリストが表示されます。

**注 :** 多重システム・モードで処理するノードを 1 つだけ選択した場合 (これが優先リストになります)、「Select Nodes」ダイアログは、要求が処理されるまで表示されません。 クライアント要求の処理の前に「Select Nodes」ダイアログを表示するには、2 つ以上のノードを選択する必要があります。

既にアクションを実行している場合は、前のアクション用に選択したノードが表示されます。 アクションの適用先であるノードは、必要に応じて変更することができます。 処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。

ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択できます。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、コマンドを実行する代替ユーザー ID を選択できます。

RRSF ノードの場合、他のユーザー ID が (RACLINK コマンドによって) ご使用のユーザー ID と関連付けられている場合、これらの関連付けられている ID が表示されます。

「**OK**」をクリックすると、選択したノードのリストが検査され、選択したノードごとに指定されたアクションが実行されます。

どのノードも選択せずに前のダイアログに戻るには、「**Cancel**」をクリックします。

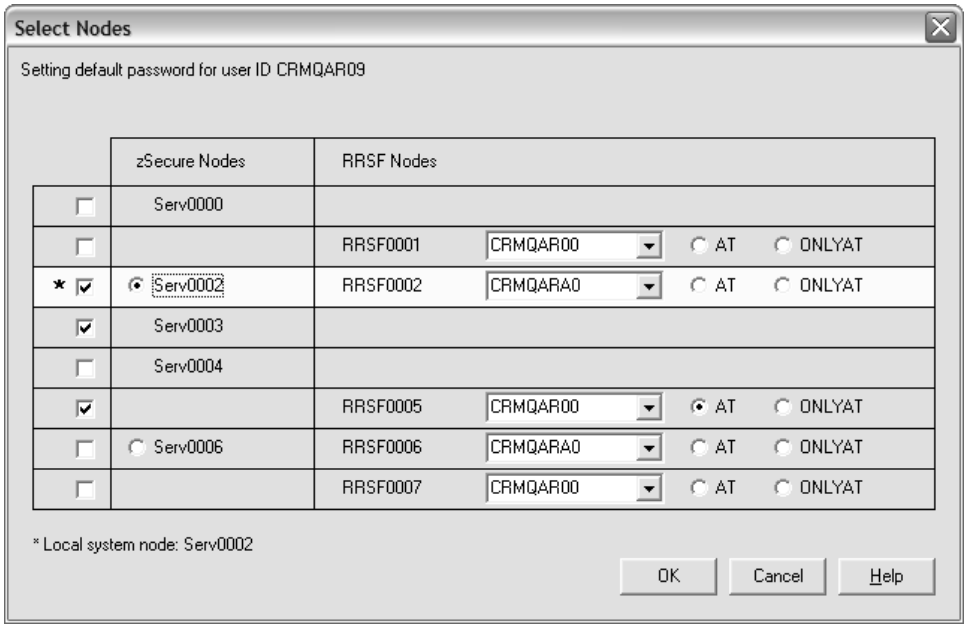



図 *9.* 「*Select Nodes*」ダイアログ

「**Select Nodes**」ダイアログには以下のフィールドとオプションがあります。

**チェック・ボックス列**
左側にあるチェック・ボックスによって、要求の適用対象のノードを選択できます。

**zSecure Nodes**
優先ノード・リストで使用可能な zSecure ノードをリストします。

**ラジオ・ボタン**
zSecure ノード用と RRSF ノード用の項目が行に含まれている場合、zSecure ノードの横にラジオ・ボタンが表示されます。このボタンで、zSecure ノードの選択およびクリアが可能になります。行とラジオ・ボタンを選択すると、zSecure ノードと RRSF ノードへの要求が処理されます。 行を選択してボタンをクリアすると、RRSF ノードへの要求のみが処理されます。

***System_name***
使用可能な zSecure システムの名前が表示されます。アクションの適用先のシステムの選択とクリアができます。

**RRSF Nodes**
優先ノード・リストで使用可能な RRSF ノードをリストします。

***System_name***
使用可能な RRSF システムの名前が表示されます。アクションの適用先のシステムの選択とクリアができます。

**代替 ID (ドロップダウン・リスト列)**
このドロップダウン・オプションを選択して、関連付けられているユーザー ID とは異なる ID を指定し、 選択した RRSF システムでアクションを実行します。RRSF システム上で関連付けられている ID は、 RACLINK コマンドを使用して定義されます。

アクションを実行する権限を持って定義された ID のみを指定します。 指定した ID に、選択したシステムにおいて、アクションに対応するコマンドを発行できる権限がない場合、RACF はそのコマンドを拒否します。

指定した代替ユーザー ID は、ログオン・セッション中の再使用に備えてドロップダウン・リストに保存されます。 代替 ID は、ログオン・セッションをまたいでは保存されません。

**AT**
選択された RRSF ノードで指示がどのように処理されるかを指定します。「**AT**」オプションを指定すると、 AT(RRSF0000.*userid*) のようなコマンドのビルドに使用されます。

**ONLYAT**
選択された RRSF ノードで指示がどのように処理されるかを指定します。「**ONLYAT**」オプションを指定すると、 ONLYAT(RRSF0000.*userid*) のようなコマンドのビルドに使用されます。

## 複数システムにまたがるアクションの検査

「**Status of**」進行状況フォームを使用して、複数システム・タスクで選択した各ノードのアクションを検査します。

複数システムに対するアクションを実行すると、選択されたノードごとのアクションの進行状況を示すために「**Status of**」進行状況フォームが表示されます。

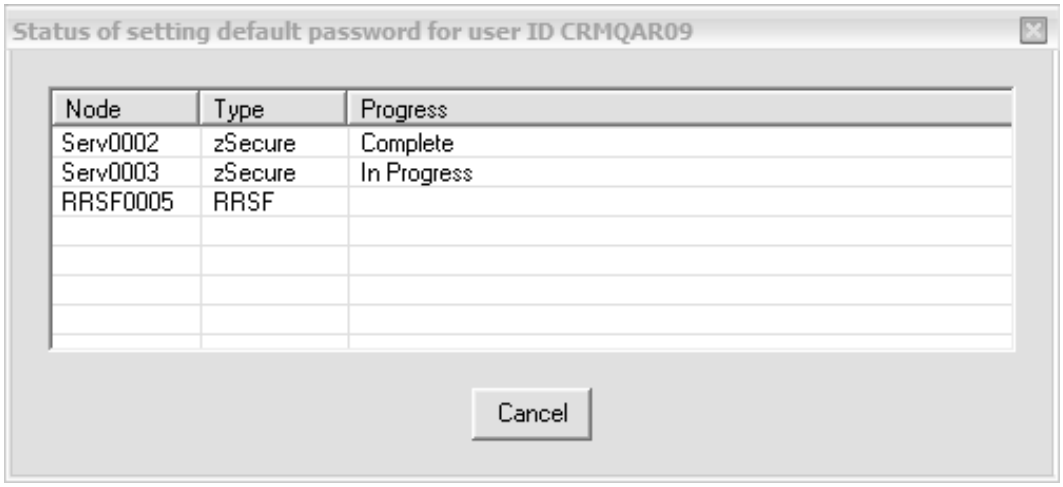



図 *10.* 複数システムの進行状況フォーム

個々のアクションが完了すると進行状況フォームが更新され、ノードごとにアクションの状況が示されます。 例えば、「**Progress**」フィールドには、アクションが完了しているか、失敗したか、または進行中であるかがノードごとに示されます。 「**Cancel**」をクリックすると、アクションが開始されていないノードで、アクションを開始しないようにすることができます。 進行中のアクションを取り消すことはできません。

アクションが失敗した場合、このフォームを閉じる前に、エラー・メッセージを検討することができます。リストされているすべてのノードでアクションが正常に完了している場合は「**Close**」をクリックします。

**注 :** 完了状況は RRSF ノードでは判別できません。そのため、すべての RRSF ノード要求は正常に行われたと想定されます。

## 「Find」ダイアログの使用

「**Find**」ダイアログを使用すると、1 つ以上の RACF データベースのユーザー、グループ、またはリソースを表示できます。

### 手順

以下のステップを実行して、「**Find**」ダイアログを開きます。

1. 「**Navigate**」 > 「**Find**」の順に選択します。
2. クラスと検索ストリングを入力します。
3. 検索ストリングの値をどのように解釈するか (「Exact」、「Filter」、「Mask」など) を指定します。
4. 検索するノードの範囲を選択します。
5. 「**OK**」をクリックします。

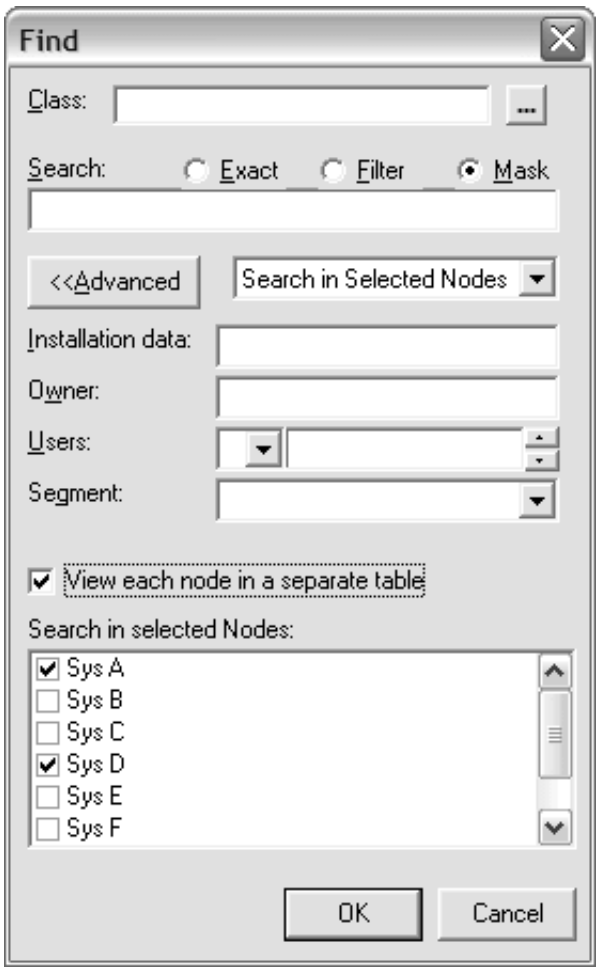



図 *11.* 「*Find*」ダイアログ

構成によっては、ユーザー情報に加えて 1 つ以上のサイト固有のフィールドが表示される場合があります。 この情報は、ダイアログの下部か、またはダイアログの右側に表示されます。インストール・データ (INSTDATA) が表示される場合、ダイアログの下部に最大 3 つのサイト固有検索フィールドが追加されます。インストール・データがない場合は、ダイアログの下部に最大 4 つのサイト固有検索フィールドが追加されます。4 個を超えるサイト固有の検索フィールドがある場合は、それらのフィールドはダイアログの右側に表示されます。

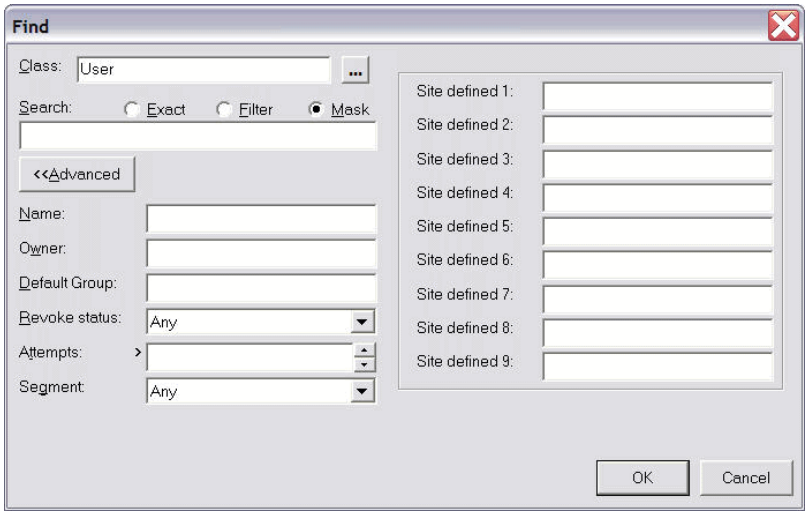



図 *12.* サイト固有フィールドが表示された「*Find*」ダイアログ

「Find」ダイアログには以下のフィールドとオプションがあります。

**Class**
クラスの名前を指定します。クラスがわからない場合は、「Class」フィールドの横にあるボタンをクリックして「**Select class**」ダイアログを開きます。42 ページの『「Select class」ダイアログによるクラスの検索』を参照してください。「Class」フィールドを空のままにすると、ユーザーまたはグループ以外のすべてのレコードを受け取ります。

「Class」フィールドの指定にはキーボード・ショートカット・キーを使用できます。

表 3. クラスのショートカット・キー

| ショートカット・キー | Class |
|---|---|
| Ctrl + D | Dataset |
| Ctrl + G | Group |
| Ctrl + U | ユーザー |

**Exact**
検索ストリングは、ロードされるユーザー ID、グループ ID、またはプロファイルのみです。

サイト固有のフィールドがある場合に、検索フィールドに指定したストリングに対する完全一致を検索する場合は、サイト固有のフィールドに値を指定しないでください。「**Exact**」を選択し、かつサイト固有フィールドに 1 つ以上の値を指定すると、Visual クライアントによりメッセージ C2RU163 が戻されます。 これは、完全一致を検索する際にサイト固有フィールドに値を指定できないことを警告するメッセージです。

**Filter**
検索ストリングがフィルターとして使用される場合、プロファイル・キーのすべての文字が一致する必要があります。 パーセント (%) 文字は、どの文字とも一致し、アスタリスク (*) 文字はすべての後続文字と一致します。 * 文字は、最後の文字としてのみ受け入れられます。 例えば、次のようになります。

- 「IBMUSER」は「IBMUSER」のみと一致します。
- 「I%MUSER」は、「IBMUSER」、「ICMUSER」、「IDMUSER」などと一致します。
- 「IBM*」は「IBM」、「IBMUSER」、「IBMGROUP」、「IBMSYS」などと一致します。

唯一の例外は、空ストリングをフィルターとして使用する場合で、空のマスクと同様にすべてが選択されます。

**Mask**
ストリングがマスクとして使用される場合、項目の先頭文字がストリングと一致する必要があります。 「IBM」は「IBMUSER」、「IBMGROUP」、「IBMSYS」などと一致します。

**Advanced**
「**<<Advanced**」をクリックすると、追加の検索基準を指定できます。これにより、選択範囲を減らすことができます。 すべての基準と一致するプロファイルのみを選択できます。

- ユーザー用の追加フィールドの説明については、53 ページの『第 4 章 ユーザー管理』を参照してください。
- グループ用の追加フィールドの説明については、81 ページの『第 5 章 グループ管理』を参照してください。
- リソース用の追加フィールドの説明については、103 ページの『第 7 章 リソース管理』を参照してください。

優先ノードのリストは、「**<<Advanced**」検索オプションに保持されます。 「**<<Advanced**」オプションを使用して、優先ノードを変更できます。

**モード選択のリスト・ボックス**
このドロップダウン・フィールドは、多重システム・モードで操作している場合にのみ表示されます。

**Search All Nodes**
このモードを選択すると、すべての優先 zSecure ノード上で操作を実行できます。 RRSF ノードはデータを返さないため、これを検索に含めることはできません。

**Search in Selected Nodes**
デフォルトのモードです。このモードを選択すると、特定の zSecure ノード上で操作を実行できます。 ノードはリスト順に検索されます。「**Search in Selected Nodes**」リスト・ボックスは、「**Search in Selected Nodes**」を指定した場合に有効になります。

**Segment**
「Segment」オプションによって、開くクラスが詳細化されます。選択したセグメントが含まれるプロファイルのみが選択されます。デフォルト・オプションは「any」で、これによって、セグメントのないプロファイルを含む完全なプロファイル・リストが得られます。

セグメントを表示する権限がないか、またはセグメントが存在しなければ、「Segment」オプションはぼかし表示され、使用できません。

「**Options**」ダイアログ内の「**Find window always on top**」オプションでは、 このダイアログが「**OK**」のクリック後に表示されなくなるかどうかを指定します。このインターフェース・オプションによって、どのフィールドとオプションがこのダイアログで 使用できるかが決まります。

**Site-specific fields**
ユーザー情報を持つサイト固有フィールドを組織により構成できます。構成した場合、サイト固有の名前と内容を持つ 1 つ以上のフィールドが右側に表示されます。

**View each node in a separate table**
このオプションは、多重システム・モードで操作している場合にのみ表示されます。 このオプションを選択すると、個々のノードの検索結果を別個のテーブルに表示できます。 このオプションを選択しない場合、すべてのノードが同じテーブルに表示されます。

**Search in Selected Nodes**
「**<<Advanced**」の横にあるドロップダウン・リストで「**Search in Selected Nodes**」を選択すると、優先ノードのリストがここに表示されます。 リストには優先ノードのみが含まれます。 必要に応じて検索ノードのリストを変更できます。 ノードは現在の要求用には選択されませんが、変更は指定した次のアクション用に使用されます。

## あいまいなクラス選択

目的の検索結果を表示するには、「**Find**」ダイアログで正確なクラス名を指定します。

「**User**」テーブルまたは「**Group**」テーブルを開き、「**Find**」ダイアログで誤った内容を指定した場合 (`User` ではなく `Users` と入力するなど)、ソフトウェアによって「`Ambiguous Class selection "class_name"`」という警告が表示されます。検索を続行すると、プログラムは入力したクラスのリソースを検索しようとします。 通常は、この検索の結果、メッセージ「`No matching resources found`」が戻ります。

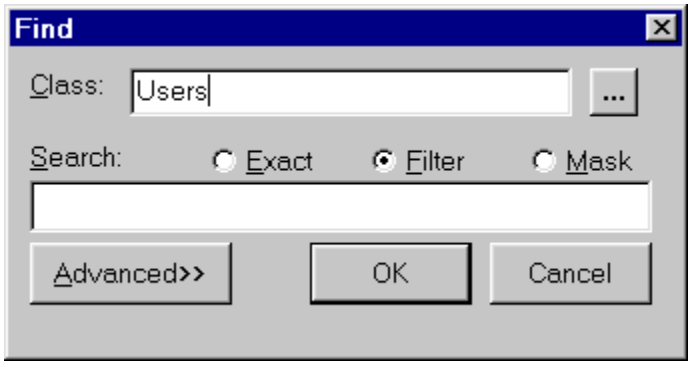



図 *13.* あいまいなクラス指定

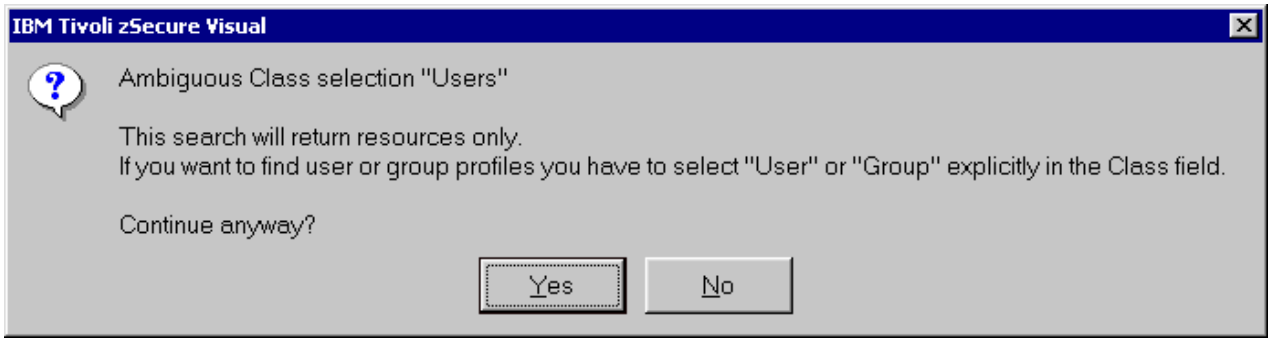



図 *14.* 警告

**ユーザー**・テーブルを表示するには、「**No**」を選択した後で、正しいクラスを選択します。

## 「Select class」ダイアログによるクラスの検索

「**Select class**」ダイアログを使用して、特定のクラスを検索します。

### このタスクについて

「**Select class**」ダイアログは必要なクラスの検索に役立ちます。

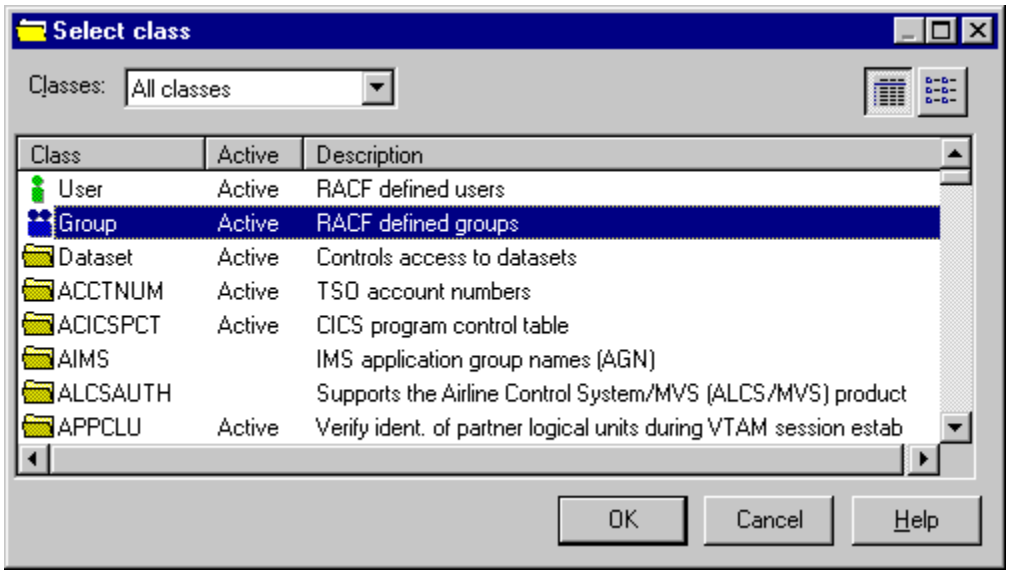



図 *15.* 「*Select class*」ダイアログ

### 手順

- 「**OK**」をクリックして、必要なクラスを選択します。

  このテーブルには以下の列が含まれます。

  **Class:**
  クラスの名前。

  **Active:**
  クラスの RACF 保護がアクティブであるかどうかを示すフラグ。

  **Description:**
  クラスの目的の説明。
- クラスのリストを制限するには、「Classes」フィールドを使用します。

**All classes**
ログオン中にクラス記述子テーブルから読み取られたすべてのクラスを表示します。

**Active classes**
メインフレーム上の SETROPTS CLASSACT コマンドおよび SETROPTS NOCLASSACT コマンドによって設定された、アクティブなクラスのみを表示します。

**Authorized classes**
ご使用のクラスの許可またはシステム全体の SPECIAL 属性に従って、変更する権限のあるクラスのみを表示します。

## 接続しているユーザーおよびグループの表示

「**Navigate**」>「**Connects**」を選択して、ユーザーおよびグループの接続関係を表示します。

### 手順

1. 接続しているユーザーまたはグループを表示するには、ユーザーまたはグループを選択します。
2. メインメニューから「**Navigate**」>「**Connects**」の順に選択します。
   結果テーブルの列の説明については、以下のトピックを参照してください。
   - 53 ページの『第 4 章 ユーザー管理』
   - 81 ページの『第 5 章 グループ管理』
   - 91 ページの『第 6 章 接続の管理』

## グループの表示

グループ・ツリーを表示することで、グループおよびサブグループの 階層を把握できます。

### このタスクについて

上位グループにはゼロ 個以上のサブグループがあります。グループは、SYS1 を除いて、常にただ 1 つの上位グループに属します。SYS1 は、ツリーのルートであるため上位グループを持ちません。

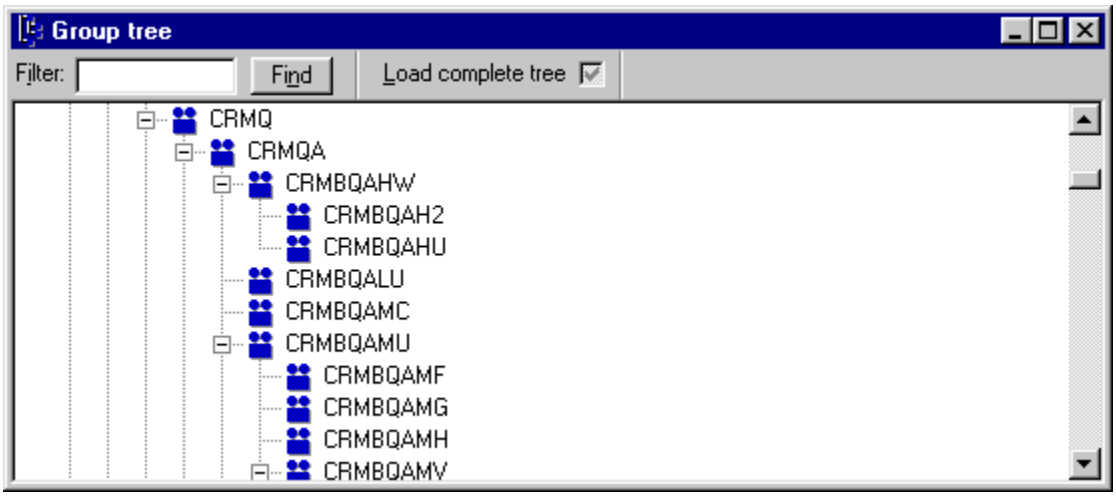



図 *16. Group tree*

「Group tree」を表示するには、以下の方法のいずれかを使用します。

### 手順

1. メインメニューから「**Navigate**」>「**Group tree**」の順に選択します。
2. ツールバーから「**Group tree**」ボタンをクリックします。

多重システム・モードで操作している場合は、「**Select Node**」ダイアログに zSecure 複合ノードのリストが表示されます。選択できる zSecure 複合ノードは 1 つのみです。 グループ・ツリーに表示する複合ノードを選択します。

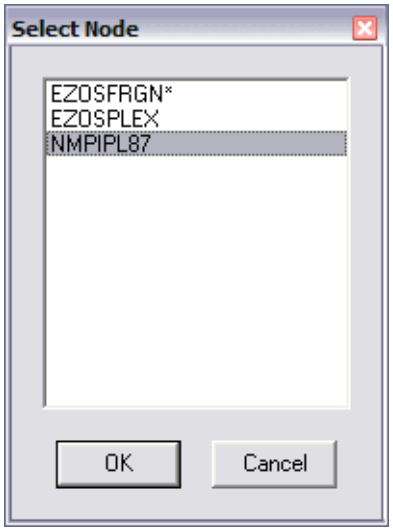



図 17. グループ・ツリー用の複合ノードの選択

セッションを閉じて再オープンすると、非ローカル・ノード用のグループ・ツリーを再オープンする必要があります。

「**Group tree**」ウィンドウには、通常、RACF データベースで定義されたグループがすべて含まれるわけではありません。 範囲にあるグループと、SYS1 までの上位グループのみが含まれます。 表示されている上位グループを確認することはできますが、範囲外の上位グループに関する情報を確認することはできません。

「*Load Complete*」は、時間節約機能です。この機能により、範囲内のすべてのグループと、その上位グループをメインフレームからロードします。 これらのグループは、ご使用の PC のメモリーに保管されるため、このセッション中に使用することができます。 このロードは、ご使用の PC に十分なメモリー容量がある場合にのみ可能です。

3. グループを選択するには、「Group tree」ウィンドウで「Filter」ボックスにフィルターを入力します。
4. 「**Find**」をクリックします。

グループ・ツリーは必要とするグループで拡張されます。フィルターと一致する最初のグループ・ツリーが強調表示されます。 グループを 1 つだけ選択する場合は、フィルターにその名前を使用します。「**Find**」コマンドにより、「**Load Complete**」オプションが使用されるときを除き、必要とする情報をメインフレームから直接ロードします。 次にご使用の PC のメモリーを検索します。

「**Options**」ダイアログで、グループの使用可能なインストール・データをツリーに表示するかどうか指定することができます。

## Permits 機能による特定のユーザー ID またはグループのリソースの選択

特定のユーザー ID またはグループに関連するリソースを選択して、そのリソース・プロファイルを表示することができます。

### 手順

リソースを選択するには以下のステップを実行します。

1. ユーザー ID またはグループを選択します。
2. 「**Navigate**」>「**Permits**」の順に選択します。

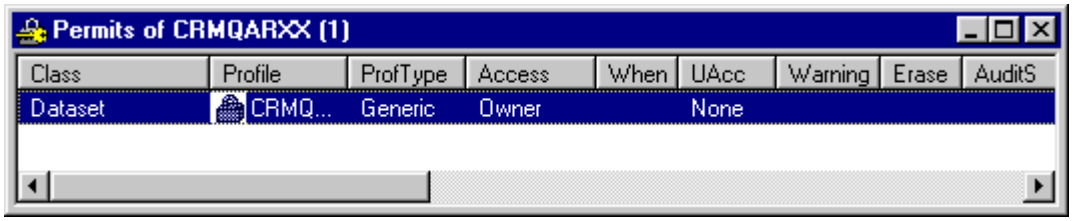



図 *18. Permits*

Permits を使用する場合、実質的に以下のプロファイルを選択します。

- アクセス・リストにあるユーザー ID またはグループが含まれるリソース・プロファイル
- ユーザー ID またはグループで所有されるリソース・プロファイル
- 最初の修飾子としてのユーザー ID またはグループを備えた DATASET プロファイル。 この修飾子は、高位修飾子 (HLQ) として頻繁に参照されます。これらのプロファイルは、RACF のユーザーおよびグループが、ユーザー ID またはグループを HLQ として備えているデータ・セットに対する変更アクセス権限を持っているため、選択されています。

**注 :** ユーザーの接続数が考慮されていないため、この手順によって、ユーザーにアクセス権限のあるすべてのリソースが選択されるわけではありません。 接続数を考慮したリストを入手するには、「View Scope」を使用してください。

103 ページの『第 7 章 リソース管理』で説明されているリソース・テーブルの列の他に、このテーブルには以下の列が含まれます。

**Access**
このフィールドには、ユーザーまたはグループがリソースに対して持っているアクセス権限が含まれます。 これは None と Alter の間のアクセス・レベルで、値は以下のいずれかになります。

**Owner**
ユーザー ID またはグループが、リソース・プロファイルの所有者です。

**QualOwner**
ユーザー ID またはグループが、DATASET プロファイルの最初の修飾子です。

**When**
このフィールドがブランクでなければ、アクセスが認可されるのは条件を満たしている場合のみです。 このフィールドがブランクであれば、アクセスは無制限で認可されます。

## Scope の使用

「**Scope**」ダイアログのさまざまなフィルタリング・オプションを使用すると、特定のユーザー ID またはグループからアクセス可能なユーザー、グループ、およびリソースを表示できます。

### このタスクについて

特定のユーザー ID またはグループによってアクセスできるユーザー、グループ、またはリソースは、ユーザー ID またはグループの範囲 内にあります。 すべてのユーザーが選択できるリソースを検索するには、「**Scope *** 」を使用します。49 ページの『Scope * の使用』を参照してください。

### 手順

ユーザーまたはグループの範囲内にあるユーザー、グループ、またはリソースを選択するには、以下のステップを実行します。

1. ユーザーまたはグループを選択します。
2. メインメニューから「**Navigate**」>「**Scope**」の順に選択します。

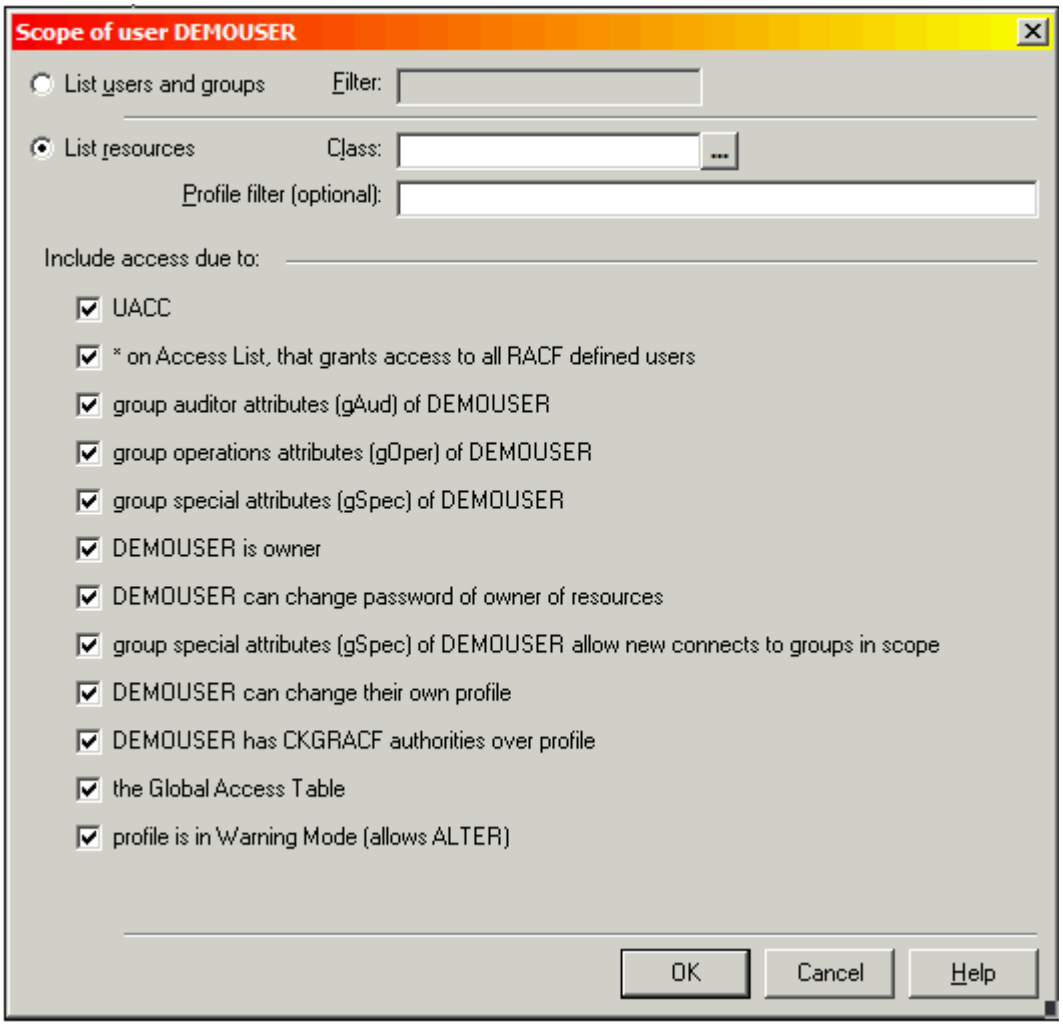



図 *19.* 範囲ダイアログ

「Scope」ダイアログには以下のフィールドとオプションが 表示されます。

**List users and groups**
指定されたユーザー ID またはグループの範囲内にあるユーザーとグループのリストを取得するには、このオプションを選択します。 このオプションを選択した場合、一部の他のオプションにはこれらのユーザーおよびグループが適用されないため、その一部のオプションは使用できなくなります。

**Filter**
このフィールドは、「**List users and groups**」を選択した場合にのみ使用します。IBM,* などのユーザーまたはグループのフィルターを 入力すると、範囲内にあり、フィルターと 一致するユーザーおよびグループのみを選択できます。 このフィールドを空のままにすると、範囲内にあるすべてのユーザーとグループが選択されます。この結果、テーブルのサイズが 大きくなります。

**List resources**
指定されたユーザー ID またはグループの範囲内にあるリソースのリストを取得するには、このオプションを選択します。

**Class**
このフィールドは、「**List resources**」を選択した場合にのみ使用します。クラス名またはクラス・フィルターを 入力して、フィルターと 一致するクラス内にあるリソース・プロファイルのみを選択できます。 このフィールドを空のままにすると、クラス・フィルターは 使用されません。この結果、テーブルのサイズが 大きくなります。

**Profile filter**
このフィールドは、「**List resources**」を選択した場合にのみ使用します。プロファイル・フィルターを入力して、フィルターと一致するリソース・プロファイルのみを選択できます。 このフィールドを空のままにすると、プロファイル・フィルターは使用されません。この結果、テーブルのサイズが大きくなります。

**UACC**
このオプションを選択すると、None 以外の UACC を持つリソースが範囲内にあるとみなされます。

*** on Access List, that grants access to all RACF defined users**
このオプションを選択すると、「None」以外のアクセス権限でアクセス・リスト上に * を持つリソースが範囲内にあるとみなされます。

**group auditor attributes (gAud) of *ID***
このオプションを選択することによって、ユーザー、グループ、またはリソースが範囲内にあるかどうか判別する際に、選択されたユーザーのグループ AUDITOR 属性が考慮されます。 グループを選択しても、グループには AUDITOR 属性がないため、このオプションは使用できません。

**group operations attributes (gOper) of *ID***
このオプションを選択することによって、ユーザー、グループ、またはリソースが範囲内にあるかどうか判別する際に、選択されたユーザーのグループ OPERATIONS 属性が考慮されます。 グループを選択しても、グループにはグループ AUDITOR 属性がないため、このオプションは使用できません。

**group special attributes (gSpec) of *ID***
このオプションを選択することによって、ユーザー、グループ、またはリソースが範囲内にあるかどうか判別する際に、選択されたユーザーのグループ SPECIAL 属性が考慮されます。 グループを選択しても、グループにはグループ SPECIAL 属性がないため、このオプションは使用できません。

***ID* is owner**
このオプションを選択すると、選択した ID が所有するユーザー、グループ、またはリソースが範囲にあるとみなされます。

***ID* can change password of owner of ...**
このオプションを選択すると、選択した ID が所有するユーザー、グループ、またはリソースが範囲にあるとみなされます。 これは、ID がパスワード、ログオン、ユーザー、グループ、またはリソースを変更し、パスワードを前の値に設定する可能性があるためです。

**group special attributes (gSpec) of *ID* allow new connects to groups in scope**
このオプションを選択することによって、ユーザー ID *ID* は、ユーザー ID の範囲にあるグループに接続できます。 ユーザー ID には、範囲内のグループに対するグループ SPECIAL 属性 (gSpec) があります。グループを選択しても、グループにはこのようなグループ SPECIAL 属性がないため、このオプションは使用できません。

***ID* can change their own profile**
このオプションを選択すると、範囲内となるユーザー、グループ、またはリソースが、ID が独自のプロファイルを変更した場合に範囲内にあるとみなされます。

***ID* has CKGRACF authorities over ...**
このオプションを選択すると、CKGRACF 範囲内のユーザー、グループ、またはリソースが範囲にあるとみなされます。

**Global Access Table**
このオプションを選択すると、グローバル・アクセス・テーブルがアクセスを許可した場合に、リソースが範囲にあるとみなされます。

**Profile is in Warning Mode (allows ALTER)**
このオプションをすると、警告モードのプロファイルによって保護されるすべてのリソースが範囲内にあるとみなされます。 警告モードは、すべてのアクセスが受け入れられますが、違反が発生した場合は警告メッセージが生成されることを意味します。

3. 「**OK**」をクリックします。

要求されたテーブルには、53 ページの『第 4 章 ユーザー管理』、81 ページの『第 5 章 グループ管理』、および 103 ページの『第 7 章 リソース管理』で説明されたユーザー、グループ、およびリソースの各テーブルで検出された列が含まれます。このテーブルには以下の列も含まれます。

**Access**
このフィールドには、ユーザー、グループまたはリソースへのアクセス権限が含まれます。 これは Execute-Read-Update-Control-Alter の範囲にあり、以下のオプションがあります。

**Owner**
ユーザー、グループ、またはリソースを所有するユーザーまたはグループ。

**QualOwner**
DATASET プロファイルの最初の修飾子であるユーザー ID またはグループ。

**Alter-Operations**
OPERATIONS 属性を使用してリソースを変更できるユーザー。

**CKGOwner**
CKGRACF によって認可されるアクセス。

**CKGList**
CKGRACF によって認可される読み取りアクセス。

**Alter-M**
ユーザーは「自分自身」を変更できます - ユーザーは、自分自身のユーザー・プロファイルの一部のフィールドを変更できます。

**Alter-P**
個別プロファイルに関する変更アクセス権限です。これにより、PERMIT を発行できます。

**When**
このフィールドがブランクでなければ、アクセスが認可されるのは条件を満たしている場合のみです。 このフィールドがブランクであれば、アクセスは無制限で認可されます。

**Via**
このフィールドには、指定されたアクセス権限が付与されたユーザー ID、グループ、または接続済みグループか、以下のいずれかのオプションが含まれます。

**警告**
プロファイルは警告モードになっているため、アクセスが認可されます。

*****
* は *None* 以外のアクセス権限でアクセス・リストに含まれているため、アクセスが認可されます。

**UACC**
UACC が *None* 以外であるか、グローバル・アクセス・テーブルがアクセスを許可しているため、アクセスが認可されます。

**Auditor**
ユーザーにグループ AUDITOR 属性があるため、アクセスが認可されます。

**Operations**
ユーザーにグループ OPERATIONS 属性があるため、アクセスが認可されます。

**SCP.G**
グループまたはユーザー、グループ、リソースの所有者が CKGRACF 範囲内にあるため、CKG .SCP.G.... 範囲プロファイルに応じてアクセスが認可されます。

**SCP.U**
ユーザーまたはユーザー、グループ、リソースの所有者が CKGRACF 範囲内にあるため、CKG.SCP.U... 範囲プロファイルに応じてアクセスが認可されます。

**SCP.ID**
ユーザーまたはグループ、あるいはユーザー、グループ、リソースの所有者が CKGRACF 範囲内にあるため、CKG.SCP.ID... 範囲プロファイルに応じてアクセスが認可されます。

**Global**
グローバル・アクセス・テーブルがアクセスを許可しているため、アクセスが認可されます。

**注 :**

- 「**Via**」列に *Global* が表示された場合、アクセス・リスト・オプションと有効なアクセス・リスト・オプションは使用できなくなっています。 これらのリストからは使用可能な情報は得られません。

- このリストはスナップショットです。リストの表示後に加えられた変更を見たい場合は、このリストをいったん閉じて再び表示する必要があります。

リソースの関連機能は有効なアクセス・リストで、プロファイルに応じたアクセス権限を持つすべてのユーザーとグループのリストが得られます。

## Scope * の使用

「**Scope ***」ダイアログのさまざまなフィルタリング・オプションを使用すると、すべてのユーザーからアクセス可能なユーザー、グループ、およびリソースを表示できます。

### このタスクについて

**Scope *** 機能を使用すると、すべてのユーザーがアクセス可能なリソースのリストを表示できます。 特定のユーザーのみがアクセス可能なユーザー、グループ、またはリソースを検索するには、**Scope** 機能を使用します。 45 ページの『Scope の使用』を参照してください。

### 手順

1. **Scope *** 機能を検索するには、メインメニューから「**Navigate**」>「**Scope**」の順に選択します。

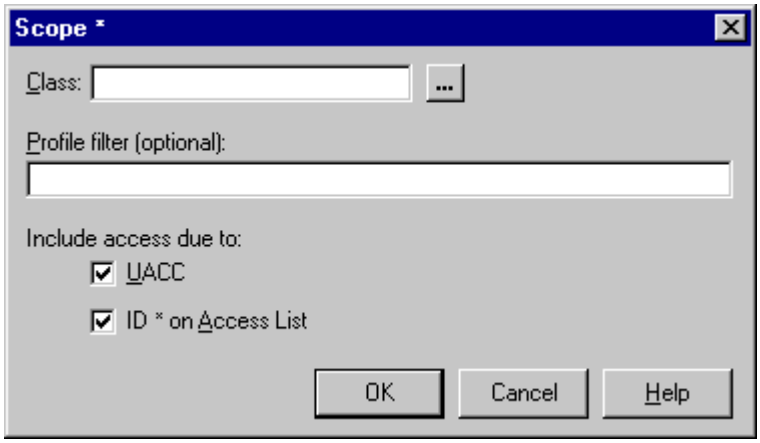



図 *20. Scope **

「Scope *」ダイアログには以下のフィールドとオプションが 表示されます。

**Class**
クラス名またはクラス・フィルターを入力して、フィルターと一致するクラス内にあるリソース・プロファイルのみを選択できます。 クラスがわからない場合は、「Class」フィールドの横にあるボタンをクリックして「**Select class**」ダイアログを表示します。42 ページの『「Select class」ダイアログによるクラスの検索』を参照してください。 このフィールドを空のままにすると、クラス・フィルターは使用されず、テーブルのサイズが大きくなる可能性があります。

**Profile filter**
プロファイル・フィルターを入力して、フィルターと一致するリソース・プロファイルのみを選択できます。 このフィールドを空のままにすると、プロファイル・フィルターは使用されず、テーブルのサイズが大きくなる可能性があります。

**UACC**
このオプションを選択すると、「**None**」以外の UACC を持つリソースが範囲内にあります。

**ID * on Access List**
このオプションを選択すると、「**None**」以外のアクセス権限でアクセス・リスト上に * を持つリソースが範囲内にあります。

2. 「**OK**」をクリックして要求されたテーブルを表示します。

このテーブルには、103 ページの『第 7 章 リソース管理』で説明されたリソース・テーブルで検出された列が含まれます。 このテーブルには以下の列も含まれます。

**Access**
このフィールドには、ユーザー、グループまたはリソースへのアクセス権限が含まれます。 これは Execute-Read-Update-Control-Alter の範囲にあり、以下のオプションがあります。

**Owner**
ユーザー、グループ、またはリソースを所有するユーザーまたはグループ。

**QualOwner**
DATASET プロファイルの最初の修飾子であるユーザー ID またはグループ。

**Alter-Operations**
OPERATIONS 属性を使用してリソースを変更できるユーザー。

**CKGOwner**
CKGRACF によって認可されるアクセス。

**CKGList**
CKGRACF によって認可される読み取りアクセス。

**Alter-M**
ユーザーは「自分自身」を変更できます - ユーザーは、自分自身のユーザー・プロファイルの一部のフィールドを変更できます。

**Alter-P**
個別プロファイルに関する変更アクセス権限です。これにより、PERMIT を発行できます。

**When**
このフィールドがブランクでなければ、アクセスが認可されるのは条件を満たしている場合のみです。 このフィールドがブランクであれば、アクセスは無制限で認可されます。

**Via**
このフィールドには、指定されたアクセス権限が付与されたユーザー ID、グループ、または接続済みグループか、以下のいずれかのオプションが含まれます。

**警告**
プロファイルは警告モードになっているため、アクセスが認可されます。

*****
* は *None* 以外のアクセス権限でアクセス・リストに含まれているため、アクセスが認可されます。

**UACC**
UACC が *None* 以外であるか、グローバル・アクセス・テーブルがアクセスを許可しているため、アクセスが認可されます。

**Auditor**
ユーザーにグループ AUDITOR 属性があるため、アクセスが認可されます。

**Operations**
ユーザーにグループ OPERATIONS 属性があるため、アクセスが認可されます。

**SCP.G**
グループまたはユーザー、グループ、リソースの所有者が CKGRACF 範囲内にあるため、CKG .SCP.G.... 範囲プロファイルに応じてアクセスが認可されます。

**SCP.U**
ユーザーまたはユーザー、グループ、リソースの所有者が CKGRACF 範囲内にあるため、CKG.SCP.U... 範囲プロファイルに応じてアクセスが認可されます。

**SCP.ID**
ユーザーまたはグループ、あるいはユーザー、グループ、リソースの所有者が CKGRACF 範囲内にあるため、CKG.SCP.ID... 範囲プロファイルに応じてアクセスが認可されます。

**Global**
グローバル・アクセス・テーブルがアクセスを許可しているため、アクセスが認可されます。

**注 :**

- 「**Via**」列に *Global* が表示された場合、アクセス・リスト・オプションと有効なアクセス・リスト・オプションは使用できなくなっています。 これらのリストからは使用可能な情報は得られません。

- このリストはスナップショットです。リストの表示後に加えられた変更を見たい場合は、このリストをいったん閉じて再び表示する必要があります。

リソースの関連機能は有効なアクセス・リストで、プロファイルに応じたアクセス権限を持つすべてのユーザーとグループのリストが得られます。

## 「RACF SETROPTS Settings」の表示

SETROPTS コマンドで設定または取得された、システム全体の RACF オプションを表示するには、「RACF SETROPTS Settings」レポートを使用します。

### このタスクについて

「RACF SETROPTS Settings」レポートは読み取り専用です。

### 手順

- メインメニューから「**Navigate**」>「**System Audit**」>「**RACF SETROPTS Settings**」 の順に選択し、「RACF SETROPTS Settings」レポートを表示します。

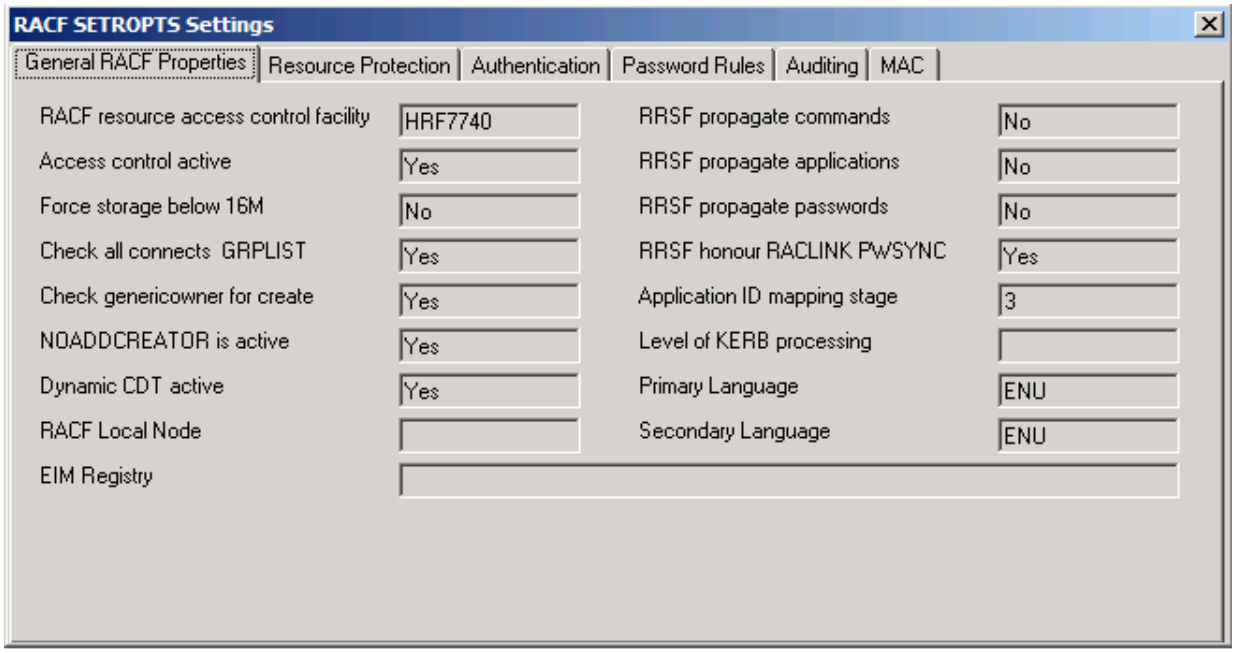



図 *21. RACF SETROPTS Settings*

## アクセス・リストの表示

「**Access List**」ウィンドウを使用して、リソース・プロファイルのすべてのユーザー ID のアクセス・リストを表示します。

### このタスクについて

アクセス・リストにはユーザー ID とグループが含まれます。 グループがアクセス・リストにある場合は、そのグループのすべてのユーザーがアクセス権限を取得します。

リソース・プロファイルのアクセス・リストを表示するには、以下のステップに従ってください。

### 手順

- リソース・プロファイルのアクセス・リストを表示するには、リソース・プロファイルを選択して「**Navigate**」>「**Access List**」の順に選択します。

結果テーブルの列については 113 ページの『アクセス・リスト (ACL) の変更』で説明しています。

- 範囲内のグループにあるユーザーを表示するには、「**有効なアクセス・リスト**」オプションを使用します。 52 ページの『有効なアクセス・リストの表示』を参照してください。

## 有効なアクセス・リストの表示

「**Effective Access List**」ウィンドウを使用して、自分の範囲内にあるリソース・プロファイルのユーザー・グループのアクセス・リストを表示します。

### このタスクについて

**有効なアクセス・リスト**には、 アクセス・リストのすべてのユーザー ID と、アクセス・リスト上のグループにあるすべてのユーザーが含まれます。 ユーザーがアクセス・リスト上の複数のグループに含まれている場合、RACF でアクセス権限が表示されるのと同時に、最大のアクセス権限が表示されます。

### 手順

リソース・プロファイルの**有効なアクセス・リスト**を表示するには、以下のステップに従ってください。

1. メインメニューからリソース・プロファイルを選択します。
2. 「**Navigate**」>「**Effective Access List**」の順に選択します。

   113 ページの『アクセス・リスト (ACL) の変更』では、「**Via**」列 (アクセス権限を得たユーザーの接続グループを含む列) を除いた、結果テーブルのすべての列が説明されています。

   **注 :**

   - 「**Options**」ダイアログで、**有効なアクセス・リスト**を判別する際に、グループ操作またはシステム操作 (汎用グループにまとめられます) を使用するかどうかを指定できます。
   - 最後のオプションをアクティブにした 場合、有効なアクセス・リストの作成中にパフォーマンスが大幅に低下することがあります。
   - アクセス・リスト上のグループが範囲外にある場合、アクセス・リストにはグループが表示されますが、そのユーザーは表示されません。
   - **有効なアクセス・リスト**をロードすると、アクセス・リストもロードされるため、 アクセス・リストへの切り替えがスムーズになります。
   - このリストはスナップショットです。リストの表示後に加えられた変更を見たい場合は、このリストをいったん閉じて再び表示する必要があります。

## メンバー・リストの表示

「**メンバー**」ウィンドウを使用して、一般リソース・プロファイルのメンバー・リストを表示します。

### 手順

1. 一般リソース・プロファイルのメンバー・リストを表示するには、メインメニューからプロファイルを選択します。
2. 「**Navigate**」>「**Members**」の順に選択します。

   結果テーブルの列については、119 ページの『メンバー・リストの表示および変更』を参照してください。

# 第 4 章 ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

**関連概念**

IBM Security zSecure Visual のセットアップと 構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

接続の管理
Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理
管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理
Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行
zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理
以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作
Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理
IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

54 ページの『ユーザー・テーブル 』
ユーザー・テーブルでユーザーのデータ (所有者や状況など) を確認します。

60 ページの『ユーザー・プロパティーの表示 』
ユーザー・プロパティー・ウィンドウを使用して、ユーザーの属性および状況の表示と編集を行います。

63 ページの『ユーザーの複写』
「**Duplicate user**」ウィンドウを使用して、既存のユーザーから新規ユーザーを作成します。

66 ページの『ユーザーの削除』
「**ユーザーの削除**」ダイアログを使用して、1 人以上のユーザーのアクセス権限を取り消します。

67 ページの『ユーザーの再開』
「**Resume user**」ダイアログを使用して、取り消し状況のユーザーを再開します。このトピックでは、その手順について説明します。

68 ページの『ユーザーの使用不可』
「**Disable user**」ダイアログを使用して、ユーザーがログオンできないようにします。

69 ページの『ユーザーの使用可能』
「**Enable user**」ダイアログを使用して、取り消されたユーザーまたは使用不可にされたユーザーがログオンできるようにします。

70 ページの『パスワード (またはパスフレーズ) の設定』

「**Set Password**」ダイアログまたは「**Set passphrase**」ダイアログを使用してユーザー・パスワードまたはパスフレーズを設定またはリセットします。

73 ページの『デフォルト・パスワード (またはパスフレーズ) の設定』
「**Edit default password**」ダイアログまたは「**Edit default passphrase**」ダイアログを使用して、ユーザーのデフォルト・パスワードまたはパスフレーズを設定します。

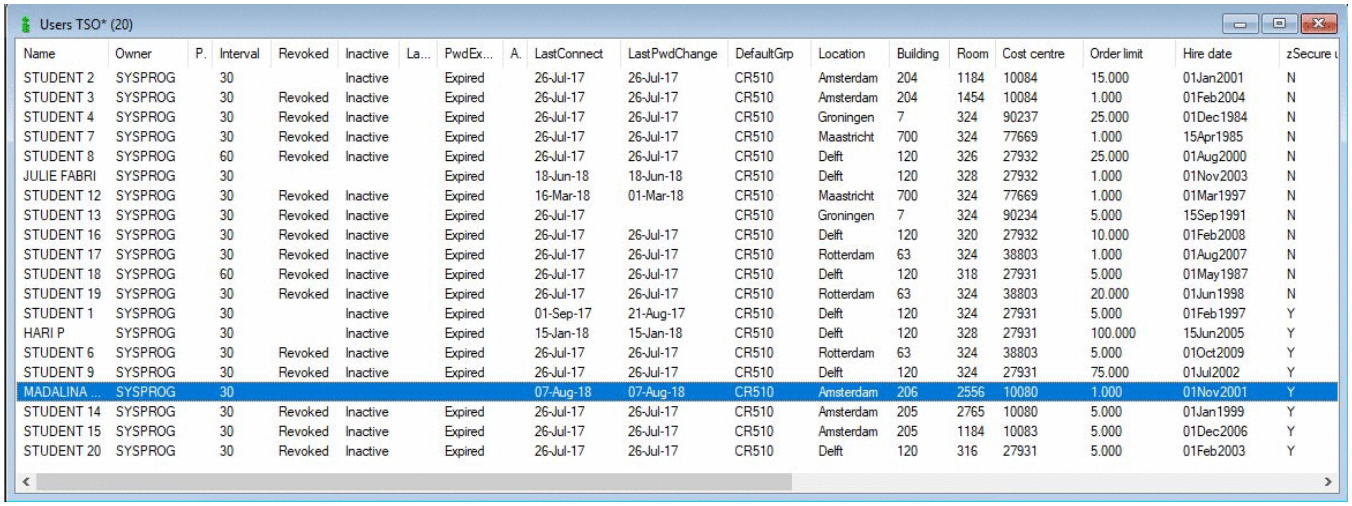
75 ページの『デフォルト・パスワード (またはパスフレーズ) の除去』
「**Edit default password**」ダイアログまたは「**Edit default passphrase**」ダイアログを使用して、ユーザーのデフォルト・パスワードまたはパスフレーズを除去します。

76 ページの『スケジュールについて』
スケジュールを使用して、ユーザーの取り消しまたは再開を実行するインターバルを指定します。

## ユーザー・テーブル

ユーザー・テーブルでユーザーのデータ (所有者や状況など) を確認します。

ユーザー・テーブルは、ユーザーおよびユーザー・プロパティーのリストで 構成されています。ユーザー・テーブルを開くには、「**Find**」ダイアログを使用します (38 ページの『「Find」ダイアログの使用』を参照)。リスト内の各アイコンの色は、赤または緑のいずれかです。 アイコンが緑色の場合、そのユーザーがアクティブであることを意味します。 一方、赤色の場合、そのユーザーが取り消されているか、または非アクティブであることを意味します。




| Name | Owner | P. | Interval | Revoked | Inactive | La... | PwdEx... | A. | LastConnect | LastPwdChange | DefaultGrp | Location | Building | Room | Cost centre | Order limit | Hire date | zSecure |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| STUDENT 2 | SYSPROG | | 30 | | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Amsterdam | 204 | 1184 | 10084 | 15.000 | 01Jan2001 | N |
| STUDENT 3 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Amsterdam | 204 | 1454 | 10084 | 1.000 | 01Feb2004 | N |
| STUDENT 4 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Groningen | 7 | 324 | 90237 | 25.000 | 01Dec1984 | N |
| STUDENT 7 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Maastricht | 700 | 324 | 77669 | 1.000 | 15Apr1985 | N |
| STUDENT 8 | SYSPROG | | 60 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Delft | 120 | 326 | 27932 | 25.000 | 01Aug2000 | N |
| JULIE FABRI | SYSPROG | | 30 | | | | Expired | | 18-Jun-18 | 18-Jun-18 | CR510 | Delft | 120 | 328 | 27932 | 1.000 | 01Nov2003 | N |
| STUDENT 12 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 16-Mar-18 | 01-Mar-18 | CR510 | Maastricht | 700 | 324 | 77669 | 1.000 | 01Mar1997 | N |
| STUDENT 13 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | | CR510 | Groningen | 7 | 324 | 90234 | 5.000 | 15Sep1991 | N |
| STUDENT 16 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Delft | 120 | 320 | 27932 | 10.000 | 01Feb2008 | N |
| STUDENT 17 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Rotterdam | 63 | 324 | 38803 | 1.000 | 01Aug2007 | N |
| STUDENT 18 | SYSPROG | | 60 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Delft | 120 | 318 | 27931 | 5.000 | 01May1987 | N |
| STUDENT 19 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Rotterdam | 63 | 324 | 38803 | 20.000 | 01Jun1998 | N |
| STUDENT 1 | SYSPROG | | 30 | | Inactive | | Expired | | 01-Sep-17 | 21-Aug-17 | CR510 | Delft | 120 | 324 | 27931 | 5.000 | 01Feb1997 | Y |
| HARI P | SYSPROG | | 30 | | Inactive | | Expired | | 15-Jan-18 | 15-Jan-18 | CR510 | Delft | 120 | 328 | 27931 | 100.000 | 15Jun2005 | Y |
| STUDENT 6 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Rotterdam | 63 | 324 | 38803 | 5.000 | 01Oct2009 | Y |
| STUDENT 9 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Delft | 120 | 324 | 27931 | 75.000 | 01Jul2002 | Y |
| MADALINA ... | SYSPROG | | 30 | | | | | | 07-Aug-18 | 07-Aug-18 | CR510 | Amsterdam | 206 | 2556 | 10080 | 1.000 | 01Nov2001 | Y |
| STUDENT 14 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Amsterdam | 205 | 2765 | 10080 | 5.000 | 01Jan1999 | Y |
| STUDENT 15 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Amsterdam | 205 | 1184 | 10083 | 5.000 | 01Dec2006 | Y |
| STUDENT 20 | SYSPROG | | 30 | Revoked | Inactive | | Expired | | 26-Jul-17 | 26-Jul-17 | CR510 | Delft | 120 | 316 | 27931 | 5.000 | 01Feb2003 | Y |

図 *22.* ユーザー・テーブル

ユーザー・テーブルには以下の列があります。

**Complex**
結果が検出された zSecure ノードの名前。この列は、多重システム・モードで操作している場合にのみ表示されます。

**ユーザー ID (Userid)**
RACF ユーザー ID。

**Name**
ユーザーの実名、またはその他の記述。

**Revoked**
取り消されたユーザーはログオンできませんが、プロファイルは残されます。 ユーザーは以下のような理由から取り消されます。

- 管理者がユーザーを取り消す。
- ユーザーが間違ったパスワード試行を多く実行し過ぎたため、自動的に取り消される。
- 管理者が、特定の日付での取り消しをスケジュールする。
- ユーザーが指定された時間フレーム内にログオンせず、自動的に取り消される。

この状況は、取り消し状況フラグ、現在日付、取り消し日付、 再開日付、およびユーザーが最後にログオンした日付から算出されます。

**Inactive**
ユーザー ID は、メインフレーム上で SETROPTS INACTIVE コマンドにより設定された期間にわたって使用されないと、非アクティブになります。ログオンしようとした 非アクティブ・ユーザーは、即時に取り消されます。このフィールドの表示には、RACF の非アクティブ設定と、最終使用日が考慮されます。

**注 :** 一度も使用しなかったユーザー ID の場合、 非アクティブにはなりません。

**Attempts**
無効なパスワードでログオンを試行した回数。この回数は、 RACF のユーザー取り消し設定が、メインフレーム上で RACF SETROPTS PASSWORD(REVOKE(nn)) コマンドによって アクティブにされている場合にのみ保持されます。無効なパスワードによる試行が nn 回行われると、そのユーザーは取り消されます。

**LastConnect**
このフィールドには、 ユーザーの接続先グループに対する最後の RACINIT 日付が入ります。

**注 :** RACF は、別の日付を使用して ユーザーの非アクティブ期間を計算します。

**LastPwdChange**
パスワードが最後に変更された日付。

**LastPhrChange**
このフィールドには、ユーザーの最後のパスフレーズ変更日が表示されます。

**PwdExpired**
このフィールドは、パスワードの有効期限が切れているかどうかを示します。パスワードの 有効期限が切れている場合、ユーザーは次回ログオン時にパスワードを変更する必要があります。 このフィールドの表示には、現在日付、ユーザーのパスワード・インターバル、システム全体のパスワード・インターバル、 およびパスワードが最後に変更された日付が考慮されます。

**PhrExpired**
このフィールドは、ユーザーのパスフレーズの 有効期限が切れているかどうかを示します。

**Interval**
ユーザーのパスワード変更が必要となる期間 (日数)。

**Owner**
所有者は、ユーザー定義を変更できます。

**DefaultGrp**
デフォルト・グループは、 ユーザーがログオン時に自動的に接続するグループです。

**InstData**
このフィールドのレイアウトおよび 目的は、各サイトで定義されます。通常、 ユーザー ID に関する組織データを含みます。組織で使用される構成によっては、`InstData` フィールドはサイト 固有フィールドで置き換えられる場合があります。

**Created**
ユーザーが定義された日付。

**MappingsCount**
ユーザー ID に関連付けられている分散 ID フィルターの数。

**LegacyPwdUsed**
このフィールドは、現在のユーザー・パスワードがレガシー・アルゴリズムを使用して暗号化されているかどうかを示します。レガシー・アルゴリズムは、DES か、または ICHDEX01 パスワード暗号化出口で示されるアルゴリズム (マスキング、DES、またはインストール定義の暗号化方式) です。

**LegacyPwdCount**
このフィールドは、レガシー・アルゴリズムを使用して暗号化されている、パスワード・ヒストリー内のパスワードの数を示します。

**Auth Method**
このフィールドは、ユーザーに対して許可されている、RACF にログオンするための認証メカニズムの組み合わせを示します。

**Pwd**
ユーザーはパスワードを使用できます。

**PPhr**
ユーザーはパスフレーズを使用できます。

**MFA**
ユーザーは IBM Z Multi-Factor Authentication (MFA) メカニズムを使用できます。

**Protected**
ユーザーは保護ユーザーです。

**Password Fallback**
このフィールドは、MFA サーバーが使用できない場合に、ユーザーがパスワードまたはパスフレーズを使用して RACF にログオンできるかどうかを示します。

**PwdExpireDate**
このフィールドには、ユーザーのパスワードの有効期限が表示されます。パスワードが明示的に期限切れになっているユーザーの場合、このフィールドには過去の日付が表示されます。そのような場合は、ユーザーの最後の使用日を示しています。一度も使用しなかったユーザー ID の場合、 このフィールドにはユーザー ID の作成日が表示されます。

**PhrExpireDate**
このフィールドには、ユーザーのパスフレーズの有効期限が表示されます。パスフレーズが明示的に期限切れになっているユーザーの場合、このフィールドには過去の日付が表示されます。そのような場合は、ユーザーの最後の使用日を示しています。一度も使用しなかったユーザー ID の場合、 このフィールドにはユーザー ID の作成日が表示されます。

**Site-specific fields**
組織の zSecure Visual サーバーは、サイト固有のフィールドとユーザー情報 (ロケーション、ビルディング、コスト・センター、zSecure ユーザー名、その他のサイト固有のコンテンツ) を表示するように構成されている可能性があります。その場合、ユーザー・テーブル・ウィンドウの「**PhrExpireDate**」フィールドと「**Attempts**」フィールドの間にこれらのフィールドが表示されます。

ユーザー・ウィンドウの「Find」ダイアログには、ユーザーを選択するための以下の追加フィールドが表示されます。

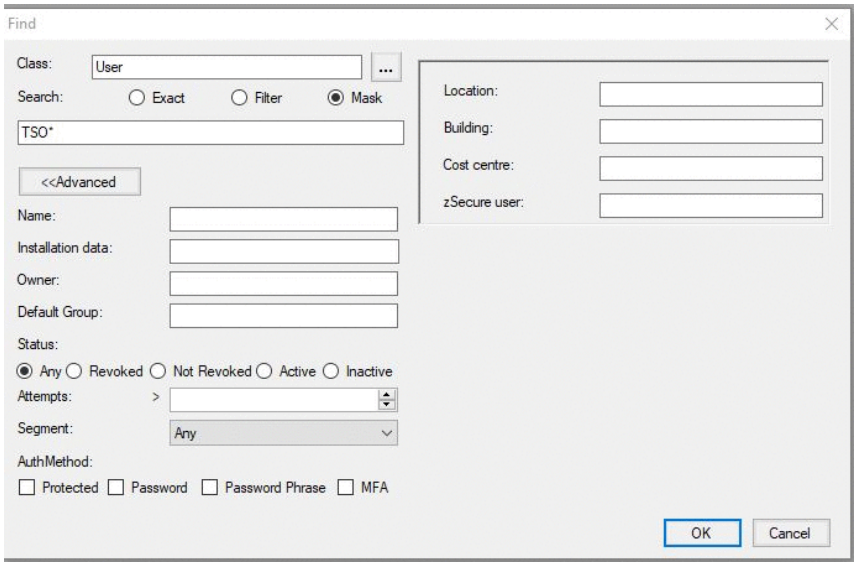



図 *23.* ユーザー用の 「*Find*」ダイアログ

**Name**
名前に含まれているサブストリング。

**Installation data**
インストール・データに含まれているサブストリング。

**Owner**
所有者を使用してユーザーを選択します。このフィールドはフィルターとして 使用されます。

**Default Group**
デフォルト・グループを使用してユーザーを選択します。このフィールドはフィルターとして 使用されます。

**Status**
取り消されているか、取り消されていないか、アクティブであるか、非アクティブであるユーザーを選択します。「**Any**」を選択すると、ユーザー・リスト全体が表示されます。

**Attempts**
パスワードの試行回数が特定の数より多い、または少ないユーザーを 選択します。フィールドをブランクにすると、 パスワードの試行回数とは関係なくユーザーを選択します。

**Segment**
指定したセグメントを持つユーザーを選択します。 このオプションが使用不可になっている場合、セグメントを表示できないか、セグメントがありません。「Any」を選択すると、 プロファイルにセグメントがあるかどうかにかかわらず、完全なユーザー・リストが得られます。

**AuthMethod**
認証方式 (Protected、Password、Password Phrase、および MFA) に基づいてユーザーを選択します。Protected、または Password と Password Phrase の組み合わせ、あるいは MFA を選択できます。何も選択しない場合は、ユーザーのリスト全体が表示されます。

組織の zSecure Visual サーバーがサイト固有のフィールドおよびユーザー情報を表示するように構成されている場合、これらのフィールドはユーザー・ウィンドウの「Find」ダイアログの右側に表示されます。

## IBM Z 多要素認証 (MFA) 要素管理

「IBM Z Multi-Factor Authentication (MFA) Factors」ウィンドウを使用して、さまざまな MFA 要素の管理タスク (MFA 要素の追加や削除、MFA 要素の活動化や非活動化、要素タグの編集など) を実行できます。

**注 :** MFA 要素は保護ユーザーには適用されません。

MFA 要素を管理するには、「**User table**」ウィンドウ (54 ページの図 22 を参照) で、ユーザー・プロファイルを選択します。右クリックし、次のサンプルに示すように「MFA Factors」を選択します。

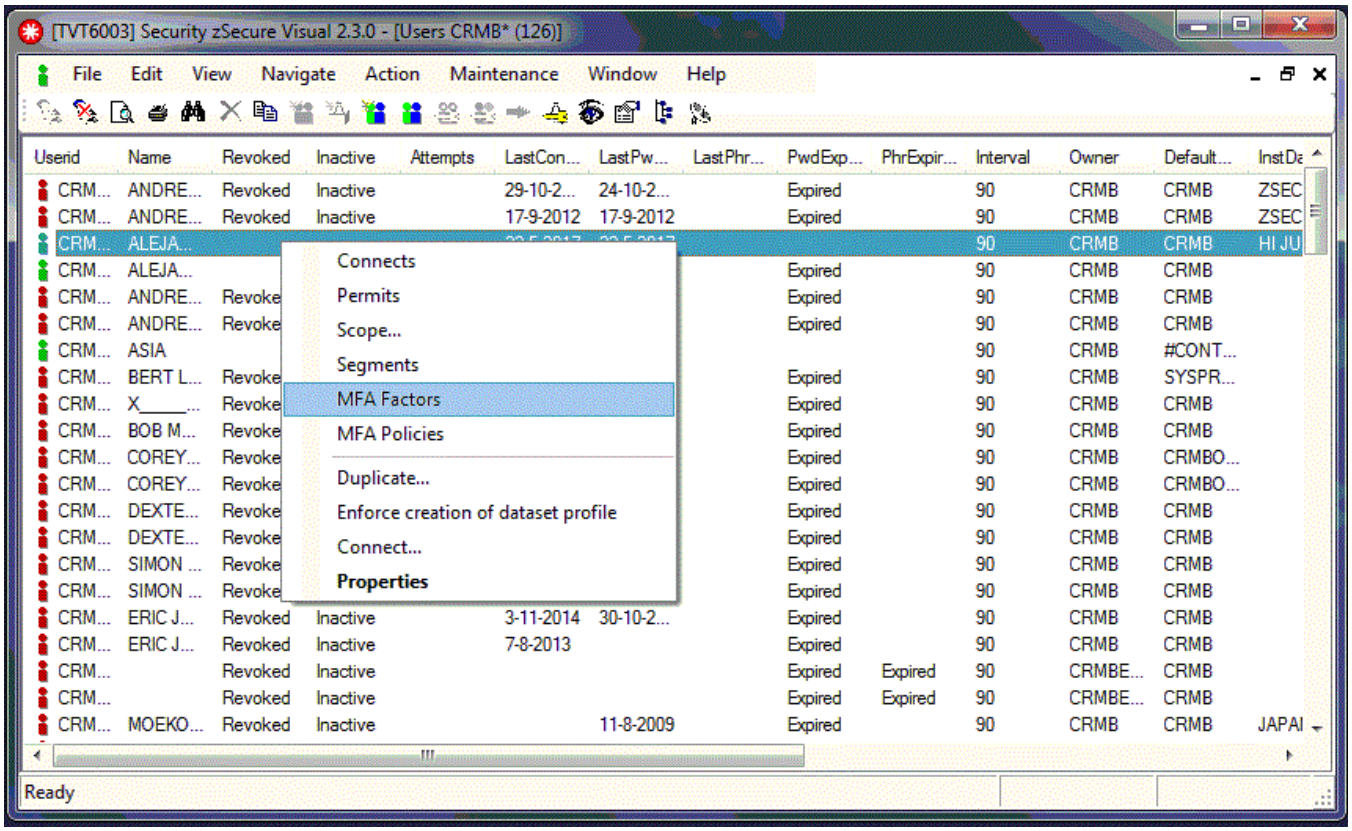



図 *24. MFA* ユーザー・テーブル

これで、「**MFA Factors dialog**」にすべての要素とそれらに対応する要素タグがリストされます。ユーザー・プロファイルに対する要素の追加や要素の削除、要素タグの編集、および要素の活動化と非活動化を実行できます。

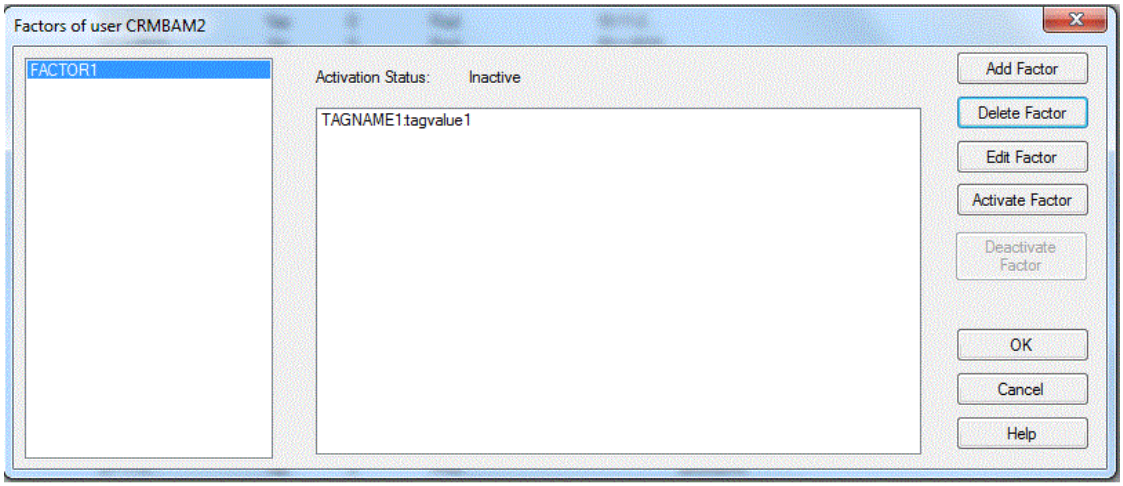



図 *25.* 「*MFA Factors*」ダイアログ

ユーザー・プロファイルに MFA 要素を追加するには、次の手順を実行します。

1. 「**MFA Factors**」ダイアログで、「**Add Factors**」をクリックします。「**Add MFA Factors**」ウィンドウが表示されます。

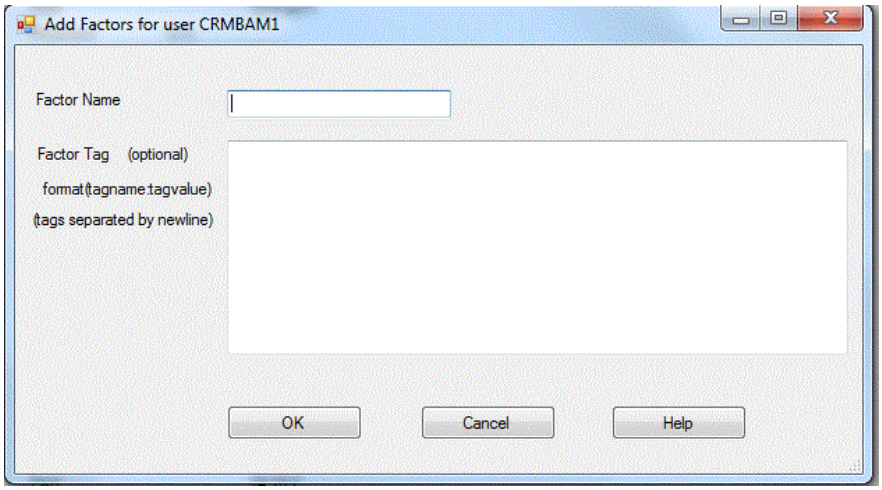



図 *26.* 「*Add MFA Factors*」ウィンドウ

2. 20 文字以内で要素名を入力します。
3. 要素タグを *TagName:TagValue* の形式で入力します。ここで、*TagName* は 20 文字以内、*TagValue* は 1024 文字以内で指定できます。各要素タグは、新しい行に入力する必要があります。

ユーザー・プロファイルから MFA 要素を削除するには、「**MFA Factors**」ダイアログで削除対象の要素を選択し、「**Delete Factors**」をクリックします。

MFA 要素を編集するには、次の手順を実行します。

1. 「**MFA Factors**」ダイアログで、「**Edit factor**」をクリックします。「**Edit MFA Factors**」ウィンドウが表示されます。

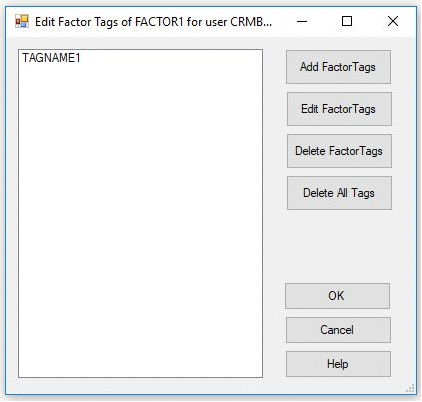



図 27. 「*Edit MFA Factors*」ウィンドウ

2. 要素タグを編集するには、その要素タグを選択し、「**Edit Factor Tags**」をクリックします。これにより、タグを編集できるようになります。
3. MFA 要素に要素タグを追加するには、「**Add Factor Tags**」をクリックし、「**MFA Factors**」ダイアログに表示される「**Add Factors**」の手順に従ってください。
4. MFA 要素からすべての要素タグを削除するには、「**Delete All Tags**」をクリックします。
5. 選択した MFA 要素をログオン中に使用するためにアクティブにするには、「**Activate Factor**」をクリックします。
6. 選択した MFA 要素を使用不可 (または非アクティブ) にするには、「**Deactivate Factor**」をクリックします。

## IBM Z 多要素認証 (MFA) ポリシー管理

「IBM Z Multi-Factor Authentication (MFA) Policies」ダイアログを使用して、さまざまなポリシー管理タスク (ポリシーの追加や削除など) を実行できます。

**注 :** MFA ポリシーは保護ユーザーには適用されません。

MFA ポリシーを管理するには、「**User table**」ウィンドウ (54 ページの図 22 を参照) で、ユーザー・プロファイルを選択します。右クリックし、「MFA Policies」を選択します (57 ページの図 24 を参照)。これで、「**MFA Policies**」ダイアログが表示され、ユーザーが使用できるすべてのポリシーがリストされます。ユーザー・プロファイルに対してポリシーの追加や削除を実行できます。

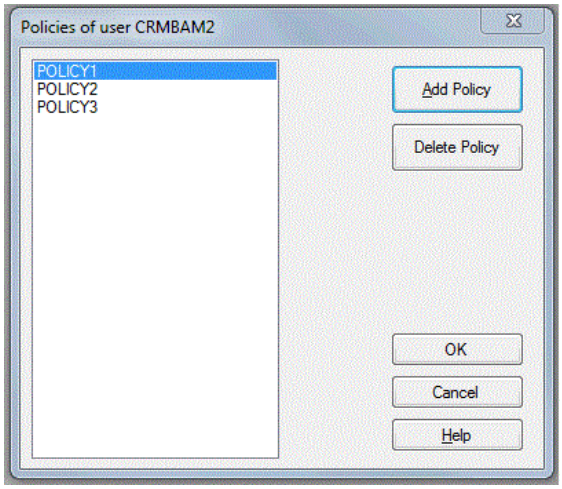



図 28. 「*MFA Policies*」ダイアログ

ユーザー・プロファイルに MFA ポリシーを追加するには、次の手順を実行します。

1. 「**MFA Policies**」ダイアログで、「**Add Policy**」をクリックします。「**Add policy**」ダイアログが表示されます。

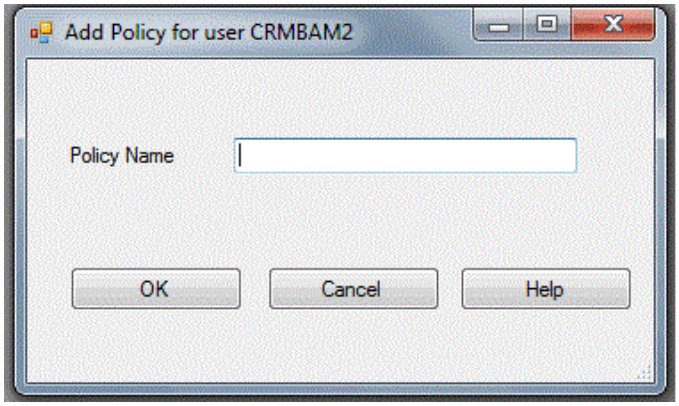



図 29. 「*Add policy*」ダイアログ

2. MFADEF クラスの MFA ポリシー・プロファイルに定義されているとおりに新しいポリシー名を 20 文字以内で入力し、「**OK**」をクリックします。

ユーザーの MFA ポリシーのリストから選択したポリシーを削除するには、「**Delete Policy**」をクリックします。

## ユーザー・プロパティーの表示

ユーザー・プロパティー・ウィンドウを使用して、ユーザーの属性および状況の表示と編集を行います。

### このタスクについて

ユーザー・プロパティーのダイアログには、「Attributes」、「More attributes」、および「Status」の 3 つのカテゴリーでユーザー・プロパティーが表示されます。

ユーザー・プロパティーを表示するには、 以下のステップに従ってください。

### 手順

1. メインメニューから「**Navigate**」>「**Properties**」の順に選択します。
   以下のアクションから開始することもできます。
   - ユーザーを選択してダブルクリックします。
   - ユーザー・テーブルからユーザーを選択し、**Enter** を押します。
   - ユーザーを右クリックし、ポップアップ・メニューから「**Properties**」を 選択します。
   - ツールバーの「**Properties**」をクリックします。

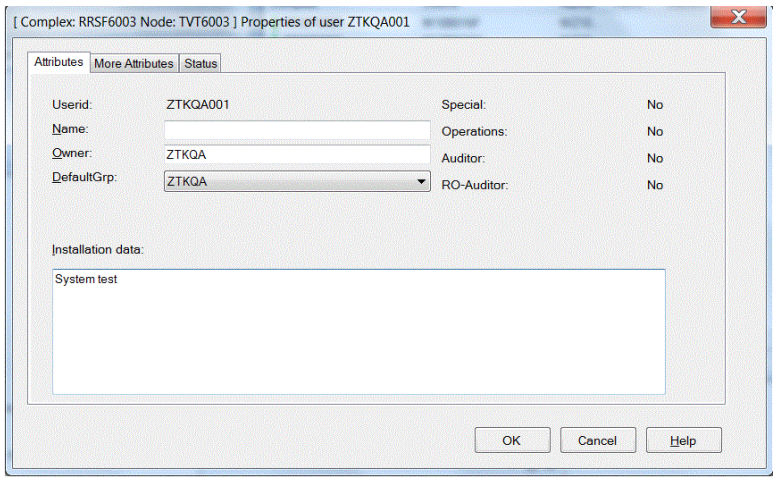



図 30. ユーザー・プロパティー・ ダイアログ

インストール・データ・フィールドに置き換わるものとして組織で構成したサイト固有フィールドが 4 個以下の場合、それらのフィールドはダイアログの 下部に表示されます。

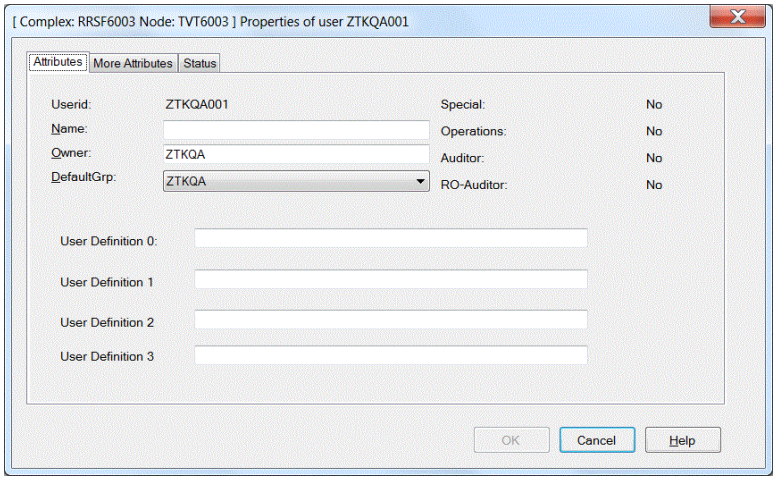



図 *31.* サイト固有フィールドが表示されたユーザー・プロパティー・ダイアログ

**注 :** 4 個を超えるサイト固有フィールドが構成されている場合、またはサイト固有フィールドがインストール・データに加えて構成されている場合は、それらのフィールドは「**Data**」という名前の別のタブのパネルに表示されます。

2. 必要に応じてフィールドの表示または編集を行い、「**OK**」をクリックして 変更を受け入れます。

   **注 :** ユーザー・プロパティーを編集できるかどうかは、 権限のレベルによって決まります。

   以下の情報は、多重システム・モードで操作している場合にのみ、ダイアログのヘッダーに表示されます。

   **Complex**
   ユーザー ID に関連付けられている複合システムの名前。

   **Node**
   ユーザー ID に関連付けられているノードの名前。

   次のフィールドが、「**Attributes**」タブに表示されます。

   **ユーザー ID (Userid)**
   RACF ユーザー ID。

   **Name**
   ユーザーの実名、またはその他の記述。

   **Owner**
   所有者は、ユーザー定義を変更できます。

   **DefaultGrp**
   デフォルト・グループ は、 ユーザーがログオン時に自動的に接続するグループです。

   **Site-specific fields**
   構成されている場合、サイト固有の名前と内容を持つユーザー情報のフィールドが 1 つ以上表示されます。この内容は読み取り専用です。

   **Installation data**
   このフィールドの目的とレイアウトは、サイトで定義されます。通常、ユーザー ID に関する組織データを含みます。「Installation data」フィールドは、 最大 255 文字含むことができます。このフィールドは、 RACF LISTUSER コマンドで表示したとき、複数行で表示されます。 最初の行は 62 文字を含み、以降の行は 80 文字を含みます。「Installation data」フィールドは変更して、別個の行に分けて構成することができます。このフィールドのフォントは 変更可能です。25 ページの『表示設定の指定』を参照してください。

   組織で使用される構成によっては、「インストール・データ」フィールドはサイト 固有フィールドで置き換えられる場合があります。

**Special**
システム全体の SPECIAL 属性。

**Operations**
システム全体の OPERATIONS 属性。

**Auditor**
システム全体の AUDITOR 属性。

**RO-Auditor**
システム全体の読み取り専用 AUDITOR 属性。

**Protected**
このフィールドは、ユーザーが保護ユーザーであるかどうかを示します。

「**More attributes**」タブには、 次のフィールドが表示されます。

**Security level**
セキュリティー・レベル。

**Categories**
ユーザーがアクセス権限を持つセキュリティー・カテゴリー。

**Security label**
セキュリティー・ラベル。

**Class authorizations**
ユーザーによるプロファイルの定義が許可されているクラス。

「**Status**」タブには、 次のフィールドまたはボタンが表示されます。

**Revoked**
取り消されたユーザーはログオンできませんが、ユーザーのプロファイルは 残されます。ユーザーは管理者が取り消したり、 パスワードの試行が何度も失敗した場合や、スケジュールされたアクションを使用した場合に、 自動的に取り消されたりします。この状況は、取り消し状況フラグ、現在日付、取り消し日付、 再開日付、および最終使用日付から算出されます。

**Inactive**
ログオンしようとした 非アクティブ・ユーザーは、即時に取り消されます。ユーザー ID は、メインフレーム上で SETROPTS INACTIVE コマンドにより設定された期間にわたって使用されないと、非アクティブになります。このフィールドの表示には、 RACF の非アクティブ設定と、 最終使用日が考慮されます。

**注 :** 一度も使用しなかったユーザー ID の場合、 非アクティブにはなりません。

**Password expired**
このフィールドは、ユーザーのパスワードの有効期限が切れているかどうかを示します。パスワードの 有効期限が切れている場合、ユーザーは次回ログオン時にパスワードを変更する必要があります。 このフィールドの表示には、現在日付、ユーザーのパスワード・インターバル、システム全体のパスワード・インターバル、 およびパスワードが最後に変更された日付が考慮されます。

**Passphrase expired**
このフィールドは、ユーザーのパスフレーズの有効期限が切れているかどうかを示します。

**Password interval**
ユーザーのパスワード変更が必要となる期間 (日数)。

**Password attempts**
無効なパスワードでログオンを試行した回数。この回数は、 RACF のユーザー取り消し設定が、メインフレーム上で RACF SETROPTS PASSWORD(REVOKE(*nn*)) コマンドによって アクティブにされている場合にのみ保持されます。無効なパスワードによる試行が *nn* 回行われると、そのユーザーは取り消されます。

**Last password change**
パスワードが最後に変更された日付。

**Last passphrase change**
このフィールドには、ユーザーの最後のパスフレーズ変更日が表示されます。

**Last connect**
このフィールドには、 ユーザーの接続先グループに対する最後の RACINIT 日付が入ります。

**注 :** RACF は、別の日付を使用して ユーザーの非アクティブ期間を計算します。

**Last logon**
ユーザーが RACF に最後にログオンした時刻。

**Created**
ユーザーが定義された日付。

**Mappings count**
ユーザー ID に関連付けられている分散 ID フィルターの数。

「**Data**」タブが表示されるのは、組織で「**インストール・データ**」フィールドに加えてサイト固有フィールドも使用するように構成した場合か、または 4 個を超えるサイト固有フィールドが構成されている場合のみです。サイト固有フィールドが「**インストール・データ**」フィールドに置き換わるものとして使用され、かつ構成されたサイト固有フィールドが 4 個以下である場合、サイト固有データは「**属性**」タブに表示されます。

対応するコマンドをメインフレーム上で実行する際、ユーザー ID に対するアクションに対して以下のボタンおよびチェック・ボックスを使用できます。

**Edit Default Password**
「**Edit Default Password**」ダイアログが開きます (73 ページの『デフォルト・パスワード (またはパスフレーズ) の設定』を参照)。

**Edit Default Passphrase**
「**Edit Default Passphrase**」ダイアログが開きます。『「Edit default passphrase」ダイアログ』を参照してください。

**Resume**
「**Resume**」ダイアログが表示されます。67 ページの『ユーザーの再開』を参照してください。

**Set Password**
「**Set Password**」ダイアログが表示されます。 70 ページの『パスワード (またはパスフレーズ) の設定』を参照してください。

**Set Passphrase**
「**Edit Passphrase**」ダイアログが表示されます。『「Set password」ダイアログ』を参照してください。

**Switch Password fallback**
このオプションは、パスワードのフォールバックが既に使用可能になっていない場合にパスワードのフォールバックをオンに切り替え、その逆も行います。

**スケジュール**
「**Schedules**」ダイアログが表示されます。 76 ページの『スケジュールについて』を参照してください。

**Mappings**
「Mappings」ウィンドウを表示します。79 ページの『Mappings』を参照してください。

## ユーザーの複写

「**Duplicate user**」ウィンドウを使用して、既存のユーザーから新規ユーザーを作成します。

### このタスクについて

既存のユーザーを複写することによって、新規ユーザーを生成できます。既存のユーザーを プロトタイプ・ユーザーとして使用できます。

**注 :** 多重システム・モードで操作している場合、ユーザーを複写できるのは、 zSecure ノード間のみです。複数の RRSF ノード間でユーザーを複写することはできません。

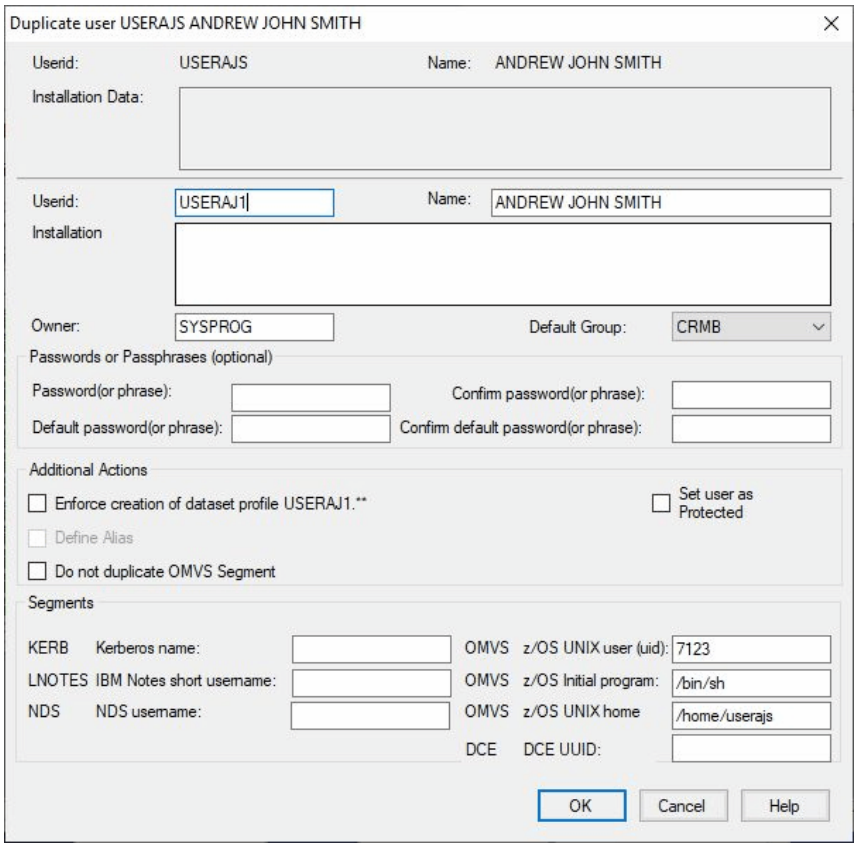



図 32. 「*Duplicate user*」 ダイアログ

### 手順

ユーザーを複写するには、以下のステップに従ってください。

1. ユーザー・ウィンドウでプロトタイプ・ユーザーを選択し、メインメニューから「**Action**」>「**Duplicate**」の順にクリックします。以下のアクションから開始することもできます。
   - ユーザーを選択し、ツールバーの「**Duplicate**」をクリックします。
   - ユーザーを右クリックし、ポップアップ・メニューから「**Duplicate**」を 選択します。
2. ダイアログの各フィールドに入力します。

   **ユーザー ID (Userid)**
   新規ユーザーのユーザー ID。

   **Name**
   新規ユーザーの名前。

   **Installation data**
   新規ユーザーのインストール・データ。

   **Owner**
   新規ユーザーの所有者。

   **Default Group**
   新規ユーザーのデフォルト・グループ。デフォルト・グループは、 プロトタイプ・ユーザーの接続グループのいずれかでなければなりません。

   **Passwords or passphrases (オプション)**
   パスワード・フィールドおよびパスフレーズ ・フィールドはオプションです。

   **Password (or phrase)**
   新規ユーザーのパスワード (またはパスフレーズ)。

   **Confirm password (or phrase)**
   新規ユーザーのパスワード (またはパスフレーズ) の確認。

**Default password (or phrase)**
オプション。新規ユーザーのパスワード (またはパスフレーズ) として設定できるデフォルト値。詳しくは、73 ページの『デフォルト・パスワード (またはパスフレーズ) の設定』を参照してください。

**Confirm default password (or phrase)**
デフォルト・パスワード (またはパスフレーズ) に指定した値を確認します。デフォルト・パスワード (またはパスフレーズ) と等しくなければなりません。

**Additional Actions**

**Enforce creation of dataset profile**
新規ユーザー ID を高位修飾子 (HLQ) として使用して、総称データ・セット・プロファイルを 作成します。このプロファイルの所有者は、新規ユーザー ID であり、UACC は NONE です。このコマンドは「Action」メニューでも選択できます。

**注 :** 既存のプロトタイプ・ユーザーに、 ユーザー ID と同じ HLQ を持つデータ・セット・プロファイルが 既に 1 つ以上ある場合は、作成する代わりに、それらのプロファイルをコピーできます。 このチェック・ボックスがオンまたはオフのいずれであるかにかかわらず、これは行われます。

**Define Alias**
ユーザー・カタログを指すユーザーの別名を定義します。 このオプションを使用するには、ユーザー・カタログ・データ・セット名がわかっている必要があります。このコマンドは「Action」メニューでも選択できます。

**注 :** このアクションは、XFACILIT クラスを検索するか、または「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の説明にあるように、サーバーのセットアップ時に Site Module 一般リソース・クラスとして構成したクラスを検索することによって、ユーザー・カタログ・データ・セット名を取得しようとします。 このとき、SHOW MYACCESS コマンドを使用して、「CKG .UCAT.」で始まる名前のプロファイルを検索します。該当するプロファイルが 1 つ以上見つかった場合は、このオプションをアクティブにすることができます。複数のデータ・セット名が見つかった場合は、このオプションをアクティブにする 際に、データ・セット名の 1 つを選択するように求められます。

**Do not duplicate OMVS Segment**
既存のユーザーの OMVS セグメントが複写されないようにします。

**Set user as Protected**
複写されたユーザーを保護ユーザーとして設定します。

**Segments**
「Segment」のフィールド、z/OS の特定のサブシステムまたはコンポーネントに 関する 情報を保管するために使用されます。これらのセグメントが、オリジナルのプロファイルにある場合は、 その値が新規ユーザーのプロファイルにコピーされます。

これらの値の中には、変更が必要なものもあれば、同じままでよいものもあります。 複写されたユーザー用の値がない場合、または セグメントが範囲内にない場合、そのフィールドは使用不可です。セグメントの管理に必要な権限について詳しくは、124 ページの『セグメント管理に必要な権限および設定』を参照してください。

このパネルに表示されるフィールドは、 セグメント内にある全フィールドのサブセットにすぎません。 範囲内にある他のすべてのフィールドは、変更されずにコピーされます。 セグメント・フィールドは、2 列に分かれています。

左の列には、 **固有**値を必要とするセグメントが示されます。 これらは、新規ユーザー・プロファイル用に値を変更する必要があります。

**KERB Kerberos name**
ユーザーのローカルな Kerberos プリンシパル名を定義する KERB KERBNAME フィールド。

**LNOTES IBM Notes short username**
IBM Notes アドレス帳で見つかった短縮名を示す IBM Notes の SNAME フィールド。LNOTES は IBM Notes を表します。

**NDS username**
Notes® ディレクトリー用の Novell Directory Services に保管されているユーザー名を定義する NDS UNAME フィールド。

右の列には、その他のセグメント・フィールドが表示されます。これらの値は、ユーザー・プロファイルごとに固有である必要はありません。

**UNIX user (uid)**
ユーザー ID 付きの z/OS UNIX フィールド。未使用の値がシステムによって割り当てられるようにするには、「auto」を使用します。この UID を複数のユーザーで共有する場合は、UID 値の最後に「s」を加えます。

**z/OS Initial program**
z/OS UNIX セッションの開始時に最初に開始するプログラムのパス名を示す z/OS UNIX プログラム・フィールド。

**z/OS UNIX home**
ユーザーのホーム・ディレクトリーである、階層ファイル・システム (HFS) または z/OS ファイル・システム (zFS) のディレクトリーのパス名を定義する z/OS UNIX ホーム・フィールド。

**DCE UUID**
DCE レジストリー内に定義されている ユーザーのプリンシパル名を示す DCE UUID フィールド。

3. 「**OK**」をクリックして複写を開始するか、 または「**Cancel**」をクリックして変更を行わずに ダイアログを終了します。フィールド値が検証され、固有フィールドが、オリジナルの値と異なっているかどうかが 判別されます。変更されているフィールドが存在しない場合、以下の警告が表示され、ダイアログは閉じられません。

```
Please change the <Name> field. It needs to be unique for this system.
```

**注 :** 値が RACF データベースにおいて固有であるかどうかは検査されません。この規模での検査を行うと、データベース全体の読み取りがトリガーされ、システムおよび ネットワークのリソースを長期間消費する可能性があります。

4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログに zSecure ノードの優先リストが表示されます。複数の RRSF ノード間でユーザーを複写することはできません。既にアクションを実行している場合は、以前に選択した zSecure ノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。
   b) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

## ユーザーの削除

「**ユーザーの削除**」ダイアログを使用して、1 人以上のユーザーのアクセス権限を取り消します。

### このタスクについて

zSecure Visual を使用している場合は、RACF データベースからユーザーを削除できません。 ただし、ユーザーに削除のマークを付けることによって、ユーザーのアクセス権限を取り消すことが可能です。1 ユーザーまたは複数のユーザーを選択して、そのアクセス権限を取り消すことができます。

ユーザーのアクセス権限を取り消すには、以下のステップに従ってください。

### 手順

1. ユーザー ID を選択し、メインメニューで「**Action**」>「**Delete**」の順にクリックします。
   また、以下のアクションを使用してユーザーのアクセス権限を取り消す こともできます。
   - ユーザー ID を右クリックしてポップアップ・メニューを表示し、「**Delete**」を選択します。

- ユーザー ID を選択し、ツールバーの「**Delete**」をクリックします。
- ユーザーを「Recycle Bin」にドロップします。

2. 削除の理由を入力します。この理由は、 「**Delete**」を取り消す場合に表示されます。
3. 「**OK**」をクリックするか、または「**Cancel**」をクリックしてダイアログを終了し、変更をすべて破棄します。選択されたユーザー ID が、そのユーザーの $DELETE スケジュールで使用不可にされます。

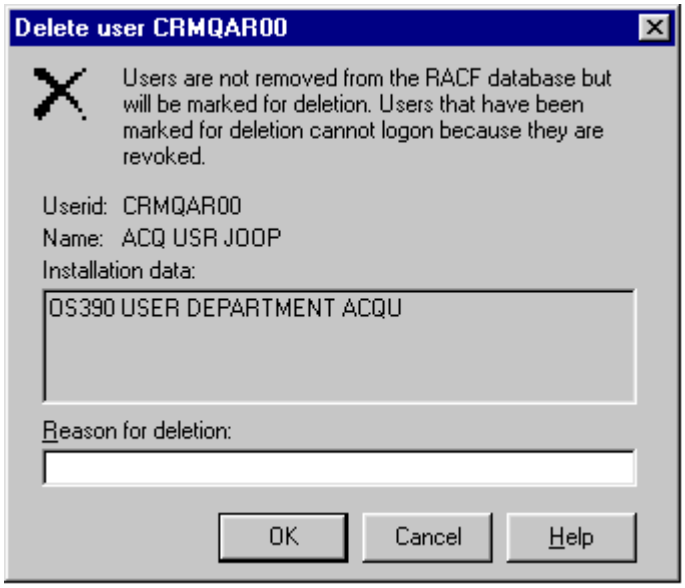



図 *33.* ユーザーに削除のマークを付ける ダイアログ

多重システム・モードを使用している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。

a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。

b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。

c) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

### タスクの結果

**削除**を取り消すには、 ユーザーのスケジュールに進み、$DELETE スケジュールで、使用不可にされているアクションを削除します。 他にスケジュールされているアクションがない場合は、そのユーザーを 再開する必要もあります。この場合は、関連するダイアログが表示されます。

## ユーザーの再開

「**Resume user**」ダイアログを使用して、取り消し状況のユーザーを再開します。このトピックでは、その手順について説明します。

### このタスクについて

再開すると、ユーザーの取り消し状況はリセットされます。これが正常に行われるのは、スケジュールされたアクションによらない取り消しの場合のみです。スケジュールされたアクションによる取り消しの場合は、 そのスケジュールされたアクションを削除しなければなりません。

単一ノード・モードで 1 つ以上のユーザーを再開するには、 以下のステップを実行します。

### 手順

1. ユーザー ID を選択し、メインメニューから「**Action**」>「**Resume**」の順にクリックします。以下のアクションを使用することもできます。
   - ユーザー ID を右クリックしてポップアップ・メニューを表示し、「**Resume**」を選択します。
   - ユーザー ID を選択し、ツールバーの「**Resume**」をクリックします。

   選択したユーザーのうち 1 ユーザーについて「**Resume user userid *userid***」ダイアログが表示されます。

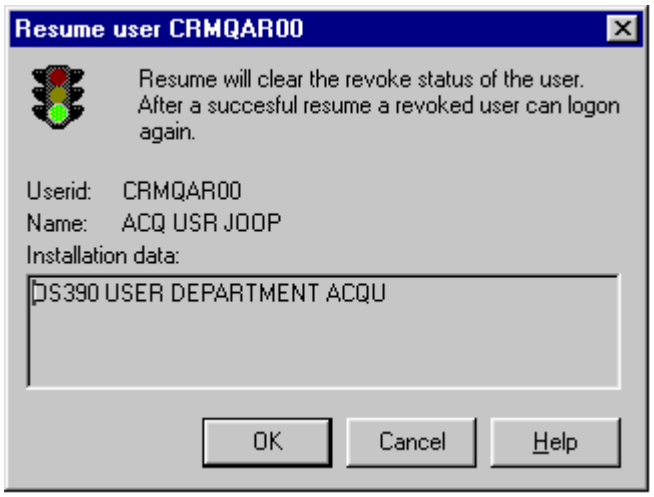



図 *34.* 「*Resume user*」ダイアログ

2. 「**OK**」をクリックして再開を実行するか、 または「**Cancel**」をクリックして前のダイアログに戻ります。
3. 複数のユーザーを再開する場合、選択したユーザーごとに、「**Resume user *userid***」ダイアログが表示されます。 各ダイアログで「**OK**」をクリックして、 選択したユーザーすべての再開を完了させます。

## ユーザーの使用不可

「**Disable user**」ダイアログを使用して、ユーザーがログオンできないようにします。

### このタスクについて

ユーザーは使用不可にしてログオンできないようにすることができます。使用不可スケジュールは、 このオプションを設定した当日に開始されます。このオプションを使用するには、 リソース CKG .CMD.USER.REQ.SCHEDULE と、範囲内にある少なくとも 1 つのスケジュール (予約されている $DELETE スケジュールを除く) に対する、UPDATE アクセス権限以上の権限が必要です。

ユーザーを使用不可にするには、以下のステップに従ってください。

### 手順

1. メインメニューからユーザー ID を選択します。
2. 「**Action**」>「**Disable**」の順に選択します。または、ユーザー ID を右クリックし、ポップアップ・メニューから「**Disable**」を選択します。

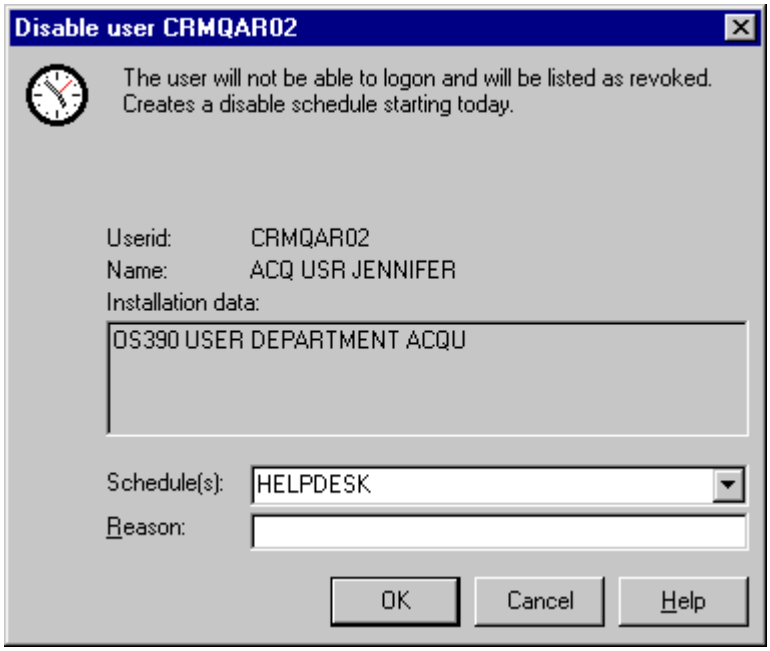



図 *35.* 「*Disable user*」ダイアログ

多重システム・モードで操作している場合は、ダイアログのヘッダーに、 ユーザーに関連付けられているノードが表示されます。

3. ユーザーを使用不可にする理由を入力します。ユーザーが既に使用不可にされている場合には、その理由を「**Details**」フィールドに表示できます。
4. 「**OK**」をクリックして終了します。

## ユーザーの使用可能

「**Enable user**」ダイアログを使用して、取り消されたユーザーまたは使用不可にされたユーザーがログオンできるようにします。

### このタスクについて

取り消されたユーザーまたは使用不可にされたユーザーは、再びログオンするように使用可能にできます。ユーザーを使用可能にすると、そのユーザーを使用不可にするスケジュールは期限切れとなります。 ユーザーを使用可能にするために利用できるスケジュールが複数存在する場合は、 いずれか 1 つを選択リストから選択できます。

このオプションを使用するには、 リソース CKG .CMD.USER.REQ.SCHEDULE と、範囲内にある少なくとも 1 つのスケジュール (予約されている $DELETE スケジュールを除く) に対する、UPDATE アクセス権限以上の権限が必要です。

ユーザーを使用可能にするには、以下のステップに従ってください。

### 手順

1. ユーザー ID を選択し、メインメニューから「**Action**」**>**「**Enable**」の順に選択します。または、ユーザー ID を右クリックし、 ポップアップ・メニューから「**Enable**」を選択します。

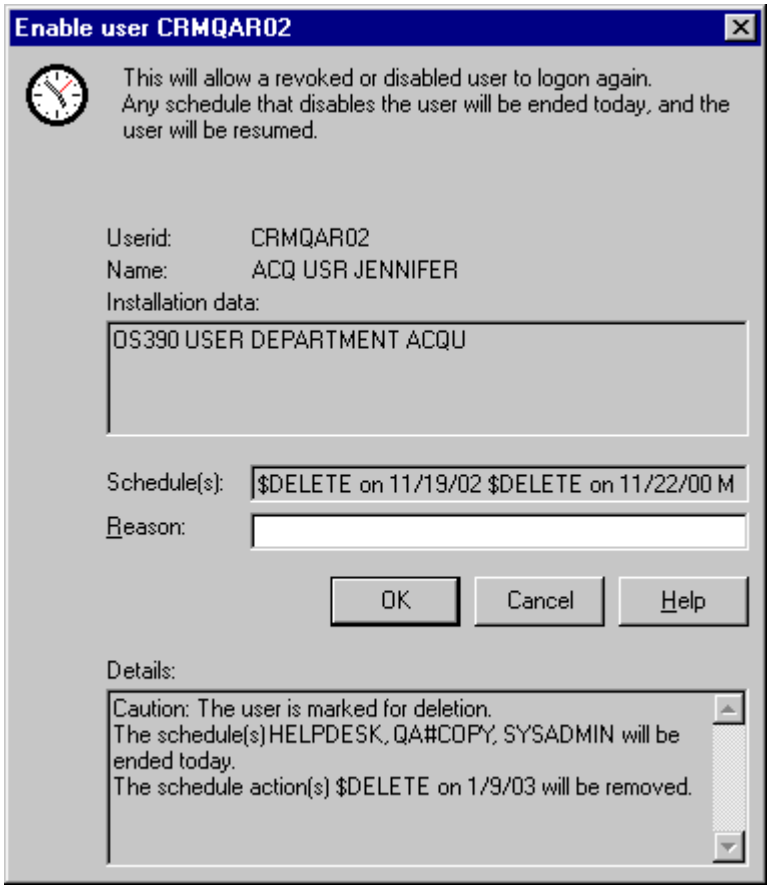



図 *36.* 「*Enable user*」ダイアログ

多重システム・モードで操作している場合は、ダイアログのヘッダーに、 ユーザーに関連付けられているノードが表示されます。

2. ユーザーを使用可能にする理由を入力します。今後のスケジュールによって再びユーザーが使用不可にされる場合に、 この理由を「**Details**」フィールドに表示できます。

   ユーザーを使用不可にするためのスケジュールが存在しなければ、通常の再開を行うことがダイアログに表示されます。

   **注 :** 「**Enable user**」ダイアログは、 再開する権限がない場合でも表示されます。
3. ユーザーに削除のマークが付けられている場合は、使用可能にするアクションを確認します。一度確認すると、そのユーザーの削除マークは解除されます。

   範囲外にある 1 つ以上のスケジュールによってユーザーが使用不可にされている場合は、それらの範囲外スケジュールをリストしたエラー・メッセージが表示されます。
4. 「**OK**」をクリックして終了します。
5. 複数のシステム上のユーザーを使用可能にする場合は、 ユーザー・リストから各ユーザーを個別に選択し、前述のステップを繰り返し行います。

## パスワード (またはパスフレーズ) の設定

「**Set Password**」ダイアログまたは「**Set passphrase**」ダイアログを使用してユーザー・パスワードまたはパスフレーズを設定またはリセットします。

### このタスクについて

パスフレーズを設定するための手順は、パスワードを設定するための手順とよく似ています。そのため、パスフレーズを設定するには、このセクションのパスワードを設定するための手順に従ってください。ただし、「Set password」ダイアログではなく「Set passphrase」ダイアログを使用してください。

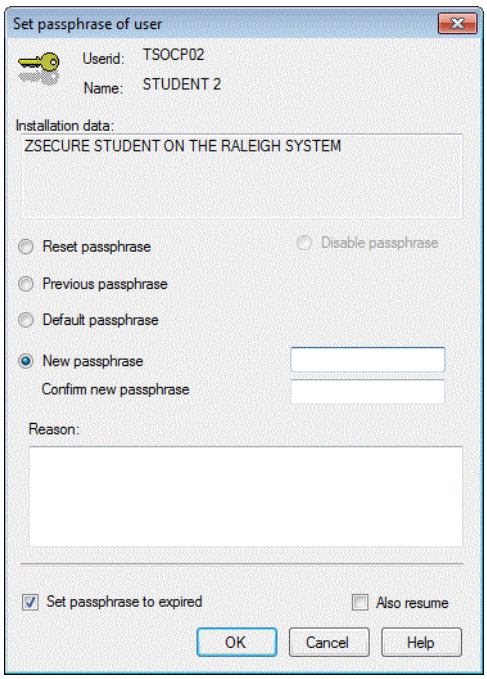



図 *37.* 「*Set passphrase*」ダイアログ

**手順**

パスワードを設定するには、以下のステップに従ってください。

1. ユーザー ID を選択し、メインメニューから「**Action**」>「**Set Password**」の順に選択します。
   以下のアクションから開始することもできます。
   - ユーザー ID を右クリックしてポップアップ・メニューを表示し、「**Set Password**」を選択します。
   - ユーザー ID を選択し、ツールバーの「**Set Password**」をクリックします。

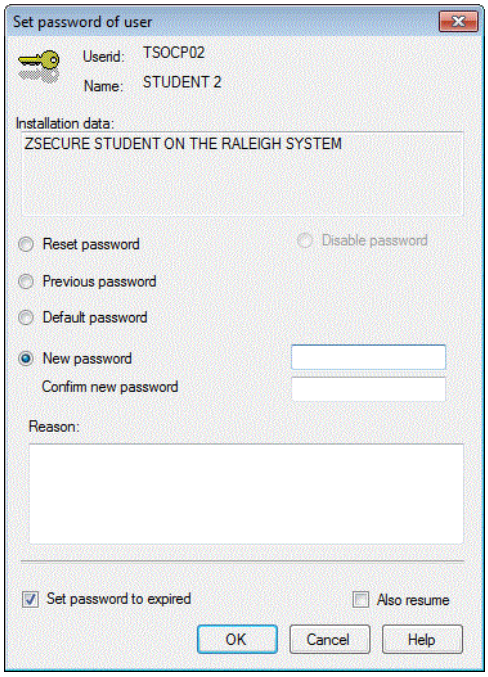



図 *38.* 「*Set password*」ダイアログ

多重システム・モードで操作している場合は、ダイアログのヘッダーに、 ユーザーに関連付けられている複合システムおよびノードが表示されます。

使用可能なオプションとチェック・ボックスは、更新アクセス権限のレベルに依存します。クライアントの表示が、「**Disable desired unauthorized functions**」に設定されている場合は、無効なオプションを表示できます。クライアントの表示が、「**Hide desired unauthorized functions**」に設定されている場合は、使用可能なオプションとチェック・ボックスのみが表示されます。27 ページの『アクセス・レベルに応じたインターフェース・オプションの設定』を参照してください。 次の手順で、使用できるすべてのオプションとチェック・ボックスについて説明します。

2. ダイアログの該当するフィールドに入力します。

   **Reset Password**
   パスワードをデフォルト・パスワードに設定し、 そのパスワードを「Expired」に設定します。

   **Previous password**
   パスワードを前の値に戻します。この設定が機能するのは、 パスワード・ヒストリーが RACF に維持されていて、ユーザーが前のパスワードを覚えている場合のみです。

   **Default password**
   パスワードを、管理者が以前設定した デフォルト・パスワードに設定します。

   **New password**
   パスワードに新しい値を設定します。「**Confirm new password**」フィールドにパスワードを再入力して、 新しい値の確認を行う必要があります。 この値は、パスワード規則に準拠したものでなければなりません。 パスワード・ヒストリー内に存在するものであってはいけませんが、 対応するリソースへのアクセス権限を持っていて、検査をバイパスできる場合は別です。パスワードの指定について詳しくは、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照してください。

   **Reason**
   パスワード変更の理由を記録します。企業の方針によっては、 入力が必要な場合があります。例として、「パスワード紛失 」、「未使用」、「取り消し」などがあります。

   **Set password to expired**
   このオプションをアクティブにすると 、新規パスワードは有効期限切れとなります。 ユーザーはログオン時に新規パスワードを指定する必要があります。

   **Also resume**
   パスワードをリセットするのと同時にユーザー ID を再開します。 何度もパスワードの試行に失敗したためにユーザーが取り消された場合、 そのログオンを再度有効にするには、再開する必要があります。パスワードの設定を行わない場合は、 「Resume」を実行してください。

   **Disable password**
   このオプションを選択すると、パスワードを無効にすることができます。ユーザーのパスワードが設定されていない場合、このオプションは使用できません。

   **Set user as protected**
   このオプションを選択すると、ユーザーを保護状態にすることができます。ユーザーが既に保護ユーザーである場合、このオプションは使用できません。

3. 「**OK**」をクリックして終了するか、 または「**Cancel**」をクリックして変更を行わずに ダイアログを終了します。

   多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。

4. 多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。
   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。
   c) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

# デフォルト・パスワード (またはパスフレーズ) の設定

「**Edit default password**」ダイアログまたは「**Edit default passphrase**」ダイアログを使用して、ユーザーのデフォルト・パスワードまたはパスフレーズを設定します。

### このタスクについて

デフォルト・パスフレーズを設定するための手順は、デフォルト・パスワードを設定するための手順とよく似ています。そのため、デフォルト・パスフレーズを設定するには、このセクションのデフォルト・パスワードを設定するための手順に従ってください。ただし、「Edit default password」ダイアログではなく「Edit default passphrase」ダイアログを使用してください。

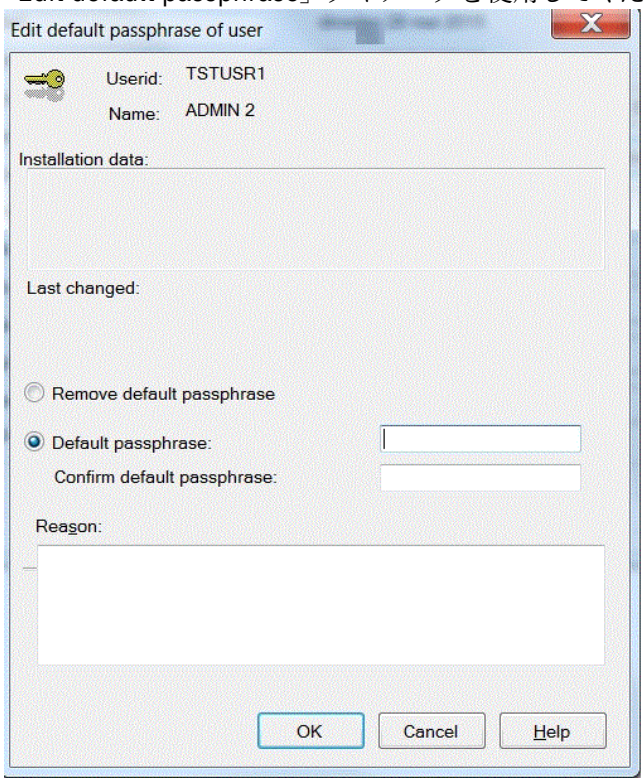



図 *39.* 「*Edit default passphrase*」ダイアログ

デフォルト・パスワード (およびパスフレーズ) は、ユーザーが設定できる固定値です。デフォルトでは、デフォルト・パスワード (およびパスフレーズ) はシステム全体で設定されています。これは、zSecure Visual の範囲外です。ただし、個別のデフォルト・パスワード (またはパスフレーズ) をユーザーごとに設定すると、重要な役割を持つユーザーの場合は特に、よりセキュアになります。

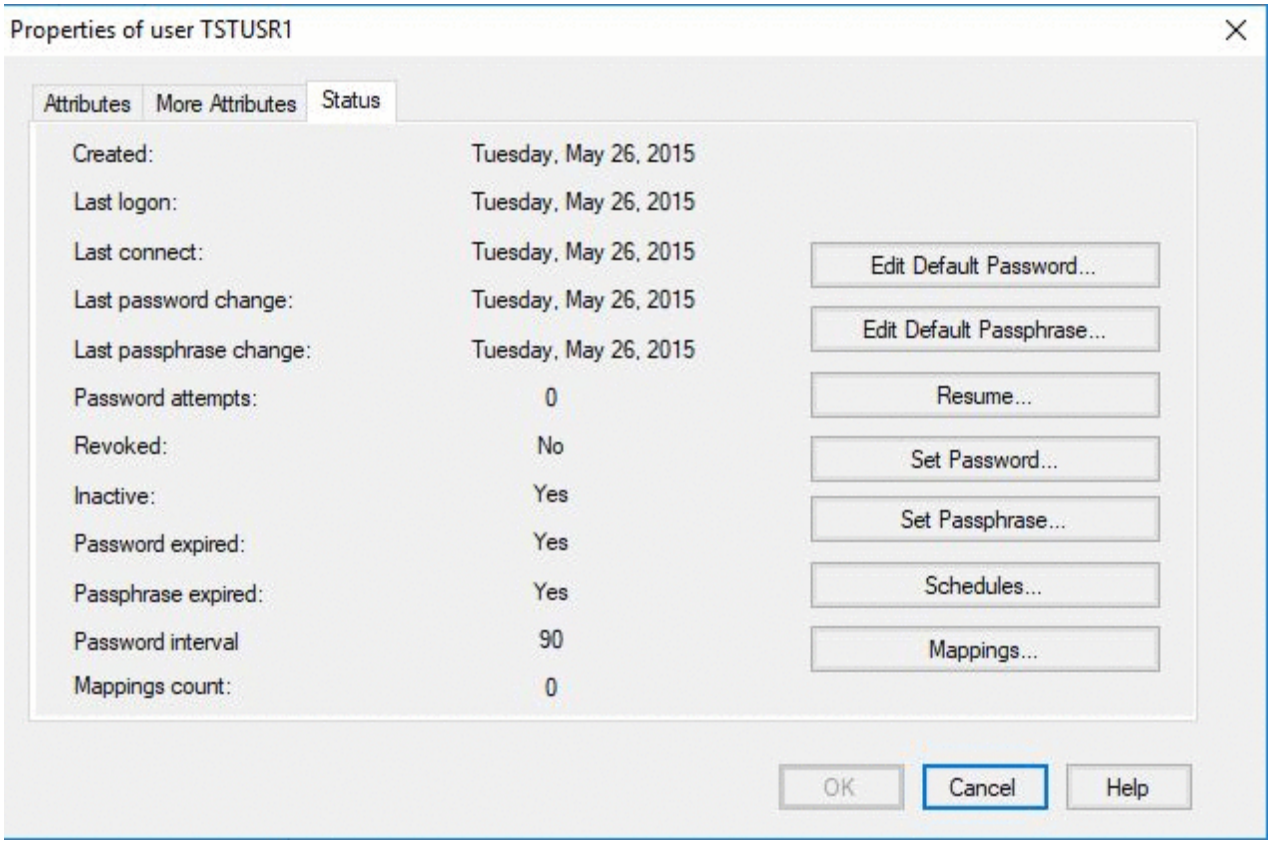



図 *40.* 状況

デフォルト・パスワードを設定するには、以下のステップを実行してください。

**手順**

1. ユーザー ID を選択し、メインメニューから「**Navigate**」>「**Properties**」の順に選択して、プロパティー・ダイアログを開きます。
2. 「**Status**」タブを選択します。
3. 「**Edit Default Password**」をクリックして、 「**Edit Default Password**」ダイアログを開きます。


図 *41.* 「*Edit default password*」ダイアログ

4. 「**Default Password**」ボックスにチェック・マークを付けます。
5. デフォルト・パスワードを入力し、確認します。
6. オプションで、デフォルト・パスワードを変更する理由を入力します。
7. 「**OK**」をクリックして終了するか、 または「**Cancel**」をクリックして変更を行わずに ダイアログを終了します。
8. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。
   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。
   c) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

## デフォルト・パスワード (またはパスフレーズ) の除去

「**Edit default password**」ダイアログまたは「**Edit default passphrase**」ダイアログを使用して、ユーザーのデフォルト・パスワードまたはパスフレーズを除去します。

### このタスクについて

デフォルト・パスワード (およびパスフレーズ) を除去または変更しても、通常のパスワード (およびパスフレーズ) は影響を受けません。通常のパスワード (またはパスフレーズ) がデフォルト・パスワード (またはパスフレーズ) に変更されるのは、デフォルト・パスワード (またはパスフレーズ) にリセットした場合のみです。リセットの後でデフォルト・パスワード (またはパスフレーズ) を変更した場合、通常のパスワード (またはパスフレーズ) は影響を受けることなく、古いデフォルト値を保持します。

パスフレーズを除去するための手順は、パスワードを除去するための手順とよく似ています。そのため、パスフレーズを除去するには、このセクションのパスワードを除去するための手順に従ってください。た

だし、「Edit default password」ダイアログではなく「Edit default passphrase」ダイアログを使用してください。

**手順**

以下のステップを使用して、デフォルト・パスワードを除去できます。

1. ユーザー ID を選択し、メインメニューから「**Navigate**」>「**Properties**」の順に選択して、プロパティー・ダイアログを開きます。
2. 「**Status**」タブを選択します。
3. 「**Edit Default Password**」をクリックして、 「**Edit Default Password**」ダイアログを開きます。
4. 「**Remove Default Password**」ボックスを選択します。
5. オプションで、デフォルト・パスワードを除去する理由を入力します。
6. 「**OK**」をクリックします。
   デフォルト・パスワードが設定されている場合は、「**Edit default password**」ダイアログに次の情報が表示されます。
   - パスワードを変更した人のユーザー ID
   - 変更日時

## スケジュールについて

スケジュールを使用して、ユーザーの取り消しまたは再開を実行するインターバルを指定します。

zSecure Visual でユーザーを取り消す唯一の方法は、 スケジュールを使用する方法です。スケジュールとは、CKGRACF メインフレーム・プログラム が提供する機能であり、これによって、さまざまな管理者グループが、ユーザーの取り消し状況を設定 できるようになります。

ユーザーの取り消しおよび再開は別々に実行することも、これら 2 つのアクションを組み合わせて 実行することもできます。これらは、「インターバル」と呼ばれます。 CKGRACF プログラムは、スケジュールに基づいてユーザーの取り消しフラグを更新します。 使用不可インターバルは、取り消しで開始して、再開で終了します。使用可能インターバルは、再開で開始して、取り消しで終了します。単一の取り消しまたは再開は、 終了日を持たないインターバルに相当します。インターバルのアクションはすべてが、 スケジュール名、日付、作成者、および理由と一緒に RACF データベースに書き込まれます。スケジュール名によってインターバルは分類されます。新規インターバルは、 同じスケジュール内でのみ、競合する以前のアクションを消去します。スケジュールされた過去のすべての アクションが削除されると、CKGRACF は、そのユーザーの取り消し状況を 未変更のままにします。

ユーザーの取り消しに相当するのは、現時点から永久に使用不可にすることです。 ユーザーの削除に相当するのは、スケジュール名 $DELETE によって現時点から永久に使用不可にすることです。 「Schedules」ダイアログで「OK」をクリックすると、 削除することがメインフレームに送信されます。

ユーザーがログオンできるのは、スケジュールされたすべてのアクションでそれが許可される場合に限られます。スケジュールは、集中管理者と分散管理者による設定が可能です。 定義されたスケジュール名の一部にアクセス権限が付与される一方で、 集中管理者専用に予約されたものがある場合、 分散管理者は、集中管理者によって設定されたインターバルを 取り消すことはできません。

### スケジュールの表示および編集

「**Schedules**」ダイアログを使用して、ユーザーの取り消しまたは再開を行うスケジュールを表示、設定、または編集します。

**手順**

- ユーザーのスケジュールを表示するには、次のいずれかのステップを実行します。
  a) ユーザーを選択し、メインメニューから「**Navigate**」>「**Schedules**」の順に選択します。
  b) ユーザーを右クリックしてポップアップ・メニューを表示し、 「**Schedules**」を選択します。
  c) ユーザーを選択し、ツールバーの「**Schedules**」をクリックします。

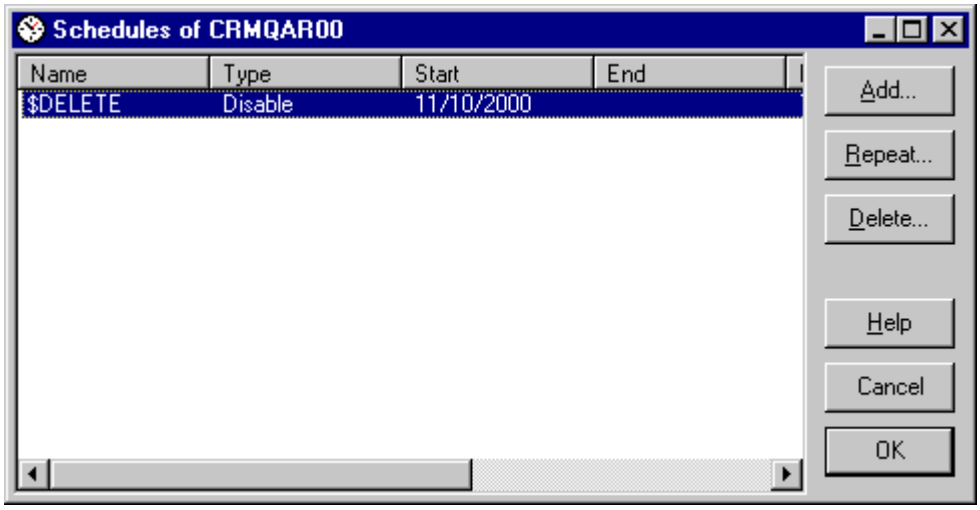



図 *42.* 「*Schedules*」ダイアログ

「Schedules」ダイアログ・ウィンドウには、次の列が表示されます。

**Name**
スケジュールの名前。

**Type**
インターバルのタイプ。「Enable」または「Disable」のいずれか。

**Start**
インターバルの開始日。

**End**
インターバルの終了日。

**Reason 列**
スケジュールの理由。

**Author**
スケジュールを入力した管理者。

**Created**
作成者がこのインターバルを入力した日時。

- スケジュールを編集するには、以下のステップを実行してください。
  a) インターバルをテーブルに追加するには、「**Add**」をクリックします。
  b) 同様のインターバルをテーブルに入力するには、インターバルを選択し、「**Repeat**」をクリックします。
  c) インターバルをテーブルから削除するには、インターバルを選択し、「**Delete**」をクリックするか、または **Delete** キーを押します。
  d) スケジュールを編集したら、「**OK**」をクリックして変更を RACF データベースに適用するか、「**Cancel**」をクリックして変更を取り消します。

## スケジュール・インターバルの追加

「**Add schedule**」ダイアログを使用して、ユーザーを使用可能または使用不可にする新規スケジュールを追加します。

### 手順

スケジュール・インターバルを追加するには、以下のステップに従ってください。

1. ユーザーを選択し、メインメニューから「**Navigate**」>「**Schedules**」>「**Add**」の順に選択します。「**Add schedule interval**」ダイアログが表示されます。

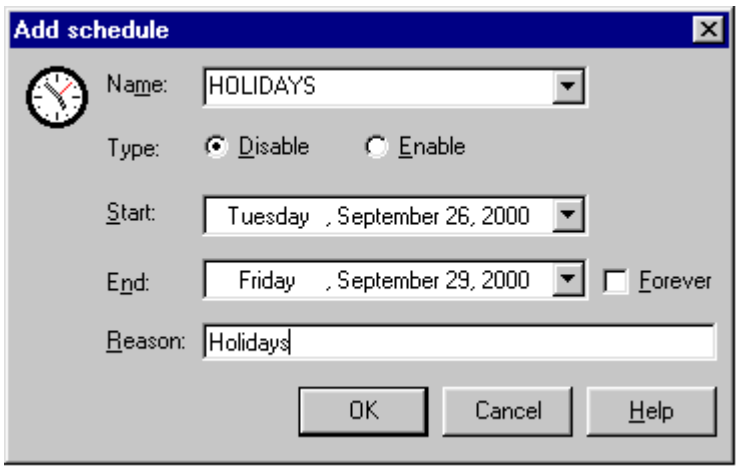



図 *43.* スケジュール・インターバル追加ダイアログ

2. 各フィールドに入力し、「**OK**」をクリックして スケジュールをテーブルに追加します。

「**Schedules**」ダイアログで「**OK**」をクリックすると、この新規スケジュール・インターバルはアクティブになります。

このダイアログには、次のフィールドがあります。

**Name**
スケジュールの名前。事前定義名の 1 つを選択することも、 新規の名前を入力することもできます。

**Type**
特定の期間ユーザーを使用不可にするには、「**使用不可にする**」を選択します。ユーザーを使用可能にするには、「**使用可能にする**」を選択します。

**Start**
インターバルの開始日を入力します。開始日は、 インターバルに含まれます。

**End**
終了日を入力するか、または、 このインターバルには終了日がないことを示す 「**Forever**」を選択します。 終了日は、インターバルに含まれます。

**Reason**
ユーザーを使用可能または使用不可にする理由を入力します。

## スケジュール・インターバルの繰り返し

「**Repeat**」機能を使用して、既存のスケジュールに基づいて新規スケジュールを作成します。

既存のスケジュールは編集できませんが、「**Repeat**」機能を使用すると、 既存のものに基づいて新規スケジュールを作成できます。既存のスケジュールおよび新規スケジュールが 重なり合う場合、プログラムは新しくスケジュールを作成します。その新規スケジュールは、 最も早い開始日に開始され、最も遅い終了日に終了します。

既存のスケジュールを使用して新規スケジュールを作成するには、メインメニューから「**Navigate**」> 「**Schedules**」>「**Repeat**」の順に選択します。

## スケジュール・インターバルの削除

「**Delete schedule**」ダイアログを使用して、既存のスケジュール・インターバルを削除します。

### 手順

スケジュールを削除するには、以下のステップに従ってください。

1. スケジュール・インターバルを選択し、「**Delete**」をクリックします。

インターバルの「**Delete schedule**」ダイアログに、スケジュールのプロパティーが表示されます。

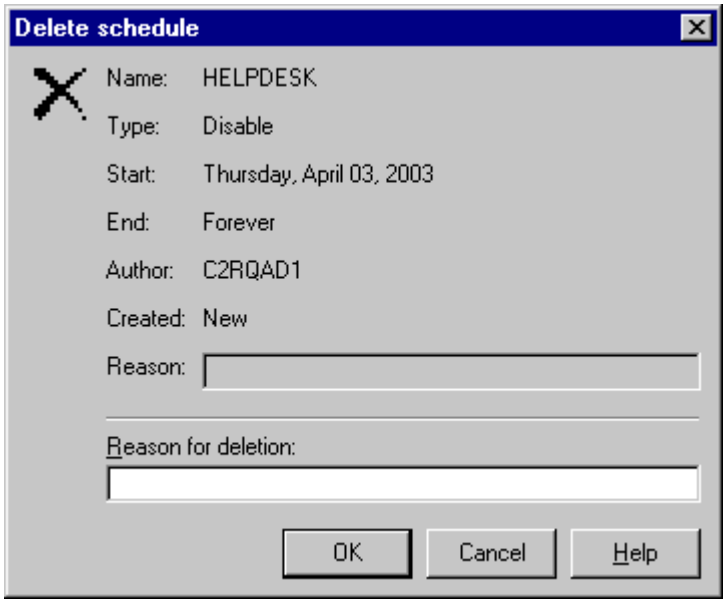



図 *44.* スケジュール・インターバル削除ダイアログ

2. 監査の目的のため、削除する理由を入力してください。
3. 「**OK**」をクリックして、スケジュール・インターバルを削除します。
   「Schedules」ダイアログで「**OK**」をクリックすると、 削除することがメインフレームに送信されます。

# Mappings

マッピング・プロファイルを使用して、RACF ユーザー ID に関連付けられた分散 ID フィルターを判別します。

RACF は、 分散 ID フィルターをサポートします。 これは、RACF ユーザー ID と 1 つ以上の 分散ユーザー ID との間の関連性をマッピングするものであり、 Web ベース・アプリケーション・サーバーから認識され、分散ユーザー・レジストリーに定義されます。「**Mappings**」ウィンドウに、 RACF ユーザー ID と関連付けられている 分散 ID フィルターの情報が示されます。これらのフィルターの実体は、 IDIDMAP プロファイルです。この章の残りの部分では、 このようなプロファイルのことを、マッピング・プロファイルと呼びます。

## マッピングの表示

「**Mappings**」の各種の選択項目を使用して、ユーザーのマッピング・プロファイルに関する情報を表示します。

### 手順

ユーザーのマッピング情報を表示するには、次のいずれかのステップを実行します。

- ユーザーを選択し、メインメニューから「**Navigate**」>「**Mappings**」の順に選択します。
- ユーザーを右クリックしてポップアップ・メニューを表示し、 「**Mappings**」を選択します。
- 「**User Properties**」ダイアログの「**Mappings**」ボタンをクリックします。

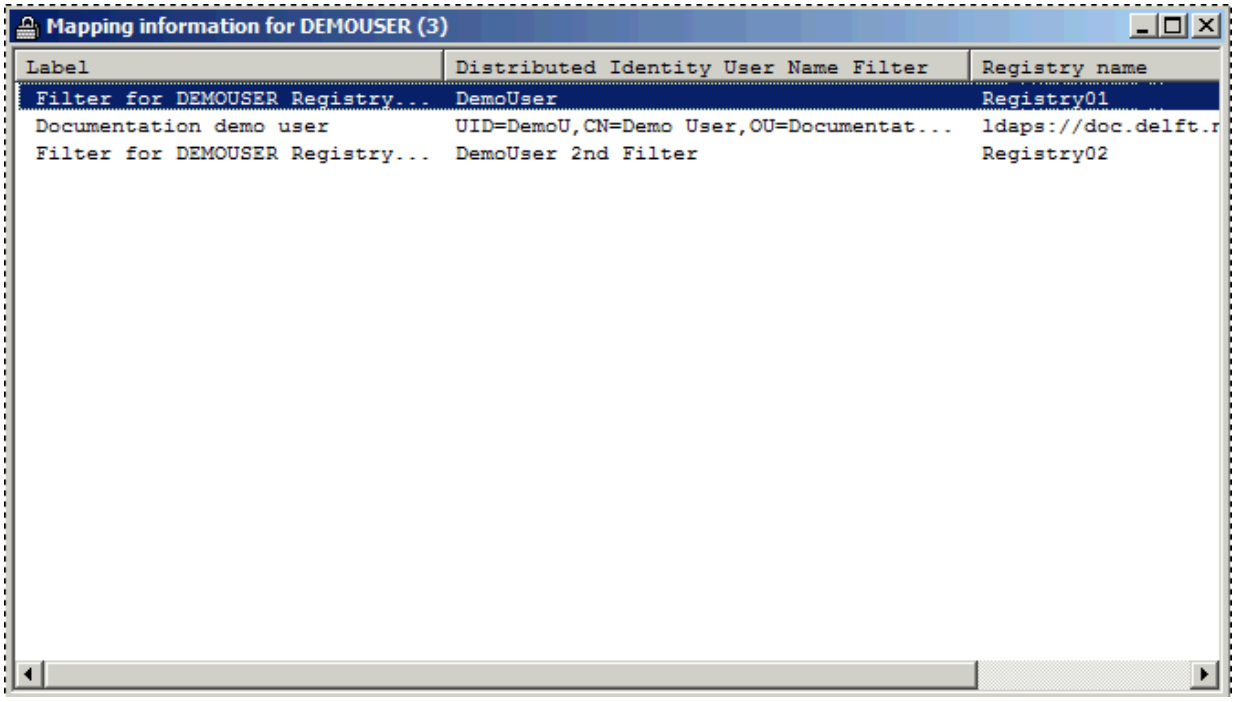



図 *45.* ユーザーの マッピング情報

「Mappings」ウィンドウには、以下の列が表示されます。

**Label**
このマッピング・プロファイルに関連付けられているラベル。

**Distributed Identity User Name Filter**
マッピング・プロファイルの名前。

**Registry name**
マッピング・プロファイルのレジストリー名。

# 第 5 章 グループ管理

IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

**関連概念**

IBM Security zSecure Visual のセットアップと構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

81 ページの『グループ・テーブル』

グループ・テーブルでグループのデータ (所有者や接続ユーザーなど) を確認できます。

83 ページの『グループ・プロパティーの表示』

「**Properties of group**」ウィンドウを使用して、グループの属性と状況を表示および編集します。

85 ページの『サブグループの追加』

「**Add subgroup**」ダイアログを使用して、グループに新規サブグループを追加します。

87 ページの『グループの複写』

「**Duplicate group**」ウィンドウを使用して、既存のグループから新規グループを作成します。

90 ページの『グループの削除』

「**グループの削除**」ダイアログを使用して、グループを削除するか、ユーザーがグループを使用できないようにします (不完全な削除)。

## グループ・テーブル

グループ・テーブルでグループのデータ (所有者や接続ユーザーなど) を確認できます。

グループのリストを表示するには、「**Find**」ダイアログを使用します。グループは 2 色で表示されます (デフォルトでは青、グループのインストール・データがロードされていないときはグレー)。

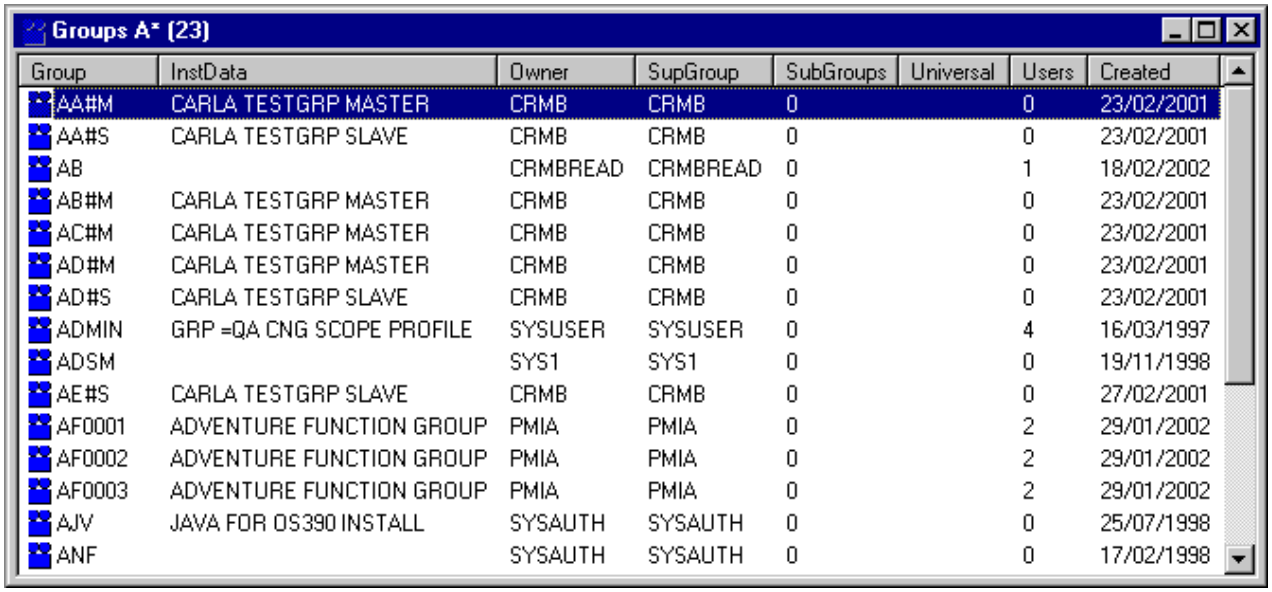



図 *46.* グループ・テーブル

グループのリストには、以下の列が表示されます。

**Complex**
結果が検出された zSecure ノードの名前。この列は、多重システム・モードで操作している場合にのみ表示されます。

**Group**
RACF グループの ID。

**InstData**
このフィールドの目的とレイアウトは、サイトで定義されます。一般には、グループの組織データが表示されます。

**Owner**
所有者はグループ定義を変更できます。

**SupGroup**
グループの上位グループ。グループ SYS1 を除くすべてのグループは、1 つの上位グループに属しています。

**SubGroups**
グループのサブグループの 数。サブグループとは、別のグループに属しているグループです。

**Universal**
汎用グループには、USE 権限を持つユーザーを数に制限なく接続できます。

**注 :**

1. グループは、汎用グループとして作成することができます。この属性を作成後に変更することはできません。
2. ほとんどの場合、汎用グループを削除することは不可能です。
3. USE より高い権限を持つユーザー、またはグループ・レベルで属性 SPECIAL、OPERATIONS、または AUDITOR を持つユーザーの接続数については、以前からの制限である 5957 が引き続き適用されます。
4. 汎用グループの場合、「Connected Users」テーブルには、USE より高い権限を持つユーザー、またはグループ・レベルで属性 SPECIAL、OPERATIONS、または AUDITOR を持つユーザーのみが表示されます。
5. 汎用グループがまだサポートされていないサイトでは、「Universal」列またはフィールドが空白で使用不可のままとなります。

**Users**
グループに接続されているユーザーの数。

**Created**
グループの作成日。

「**Find**」ダイアログでのグループ用の追加の選択フィールドは以下のとおりです。

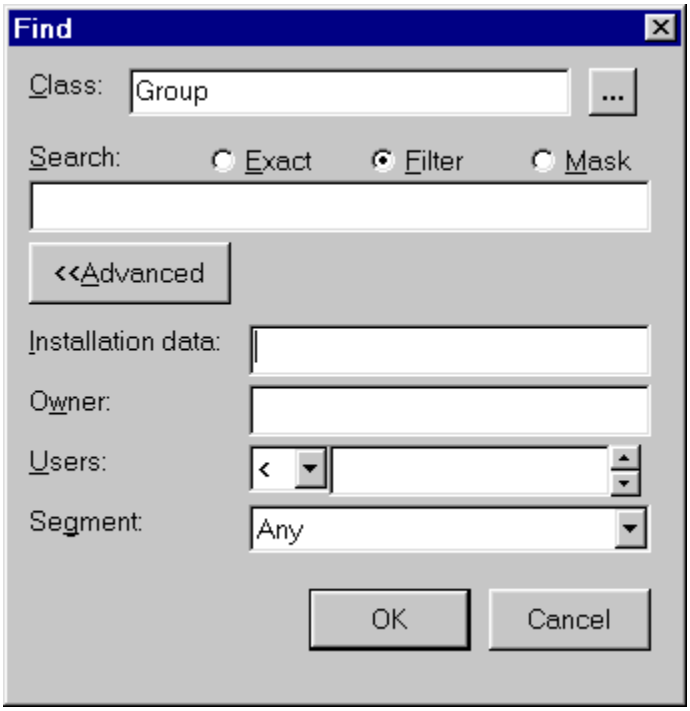



図 *47.* グループ用の「*Find*」ダイアログ

**Installation data**
インストール・データに出現するサブストリング。

**Owner**
所有者でグループを選択します。このフィールドはフィルターとして 使用されます。

**Users**
接続ユーザーが一定の数より多いまたは少ないグループを選択します。この数値フィールドをブランクにすると、数値とは関係なくグループが選択されます。この数値フィールドに < または > を入力すると、対応する演算子が選択されます。

**Segment**
指定したセグメントを持つグループを選択します。このオプションが使用不可になっている場合、セグメントを表示できないか、セグメントがありません。オプション「Any」を指定すると、プロファイルにセグメントがあるかどうかに関係なく、完全なグループ・リストが表示されます。

## グループ・プロパティーの表示

「**Properties of group**」ウィンドウを使用して、グループの属性と状況を表示および編集します。

### このタスクについて

グループのプロパティーのダイアログには、特定のグループに関する詳細情報が表示されます。

グループのプロパティーを 表示するには、以下の手順を実行します。

### 手順

1. グループを選択し、メインメニューから「**Navigate**」>「**Properties**」を選択します。

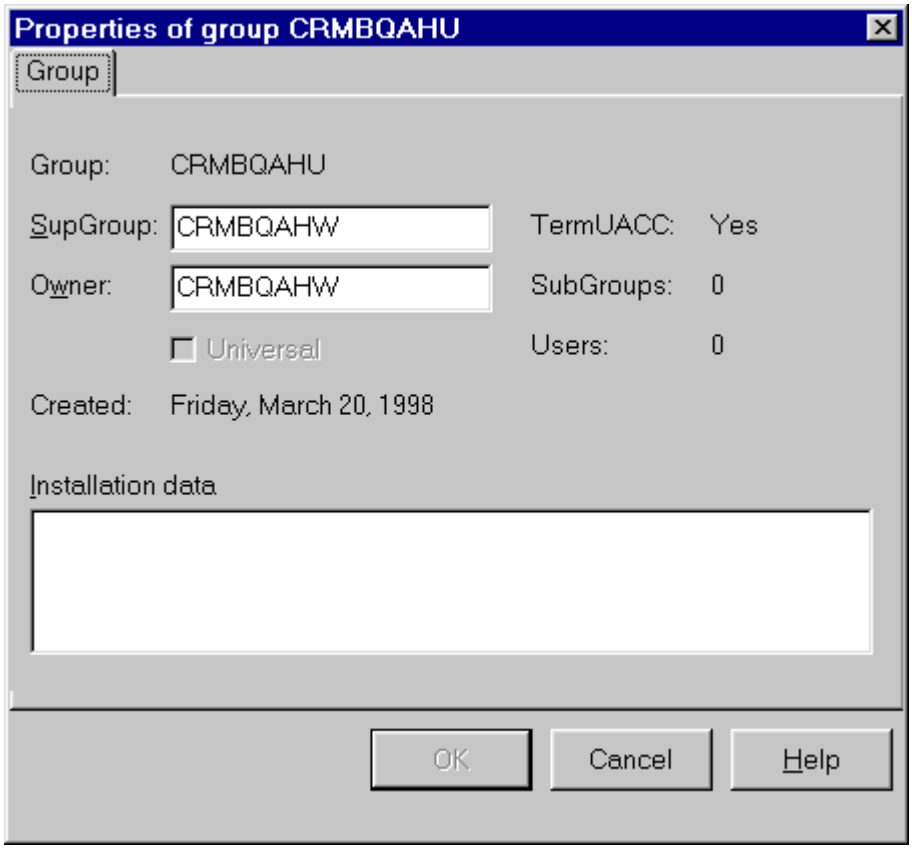



図 *48.* グループ・プロパティー・ダイアログ

2. グループをダブルクリックします。
3. グループを選択し、**Enter** を押します。
4. グループを右クリックし、ポップアップ・メニューから「**Properties**」を選択します。
5. グループを選択し、ツールバーの「**Properties**」をクリックします。

以下の情報は、多重システム・モードで操作している場合にのみ、ダイアログのヘッダーに表示されます。

**Complex**
ユーザー ID に関連付けられている複合システムの名前。

**Node**
ユーザー ID に関連付けられているノードの名前。

「**Properties**」ダイアログは、以下のフィールドで構成されています。

**Group**
RACF グループの ID。

**SupGroup**
グループの上位グループ。グループ SYS1 を除くすべてのグループは、1 つの上位グループに属しています。このフィールドは、既存の別のグループ名に変更できます。

**TermUACC**
端末アクセス権限は、端末プロファイルの UACC、およびアクセス・リスト項目によって付与されます。

**Owner**
所有者はグループ定義を変更できます。このフィールドは、既存の別のグループ名に変更できます。

**SubGroups**
グループのサブグループの 数。サブグループとは、別のグループに属しているグループです。

**Universal**
汎用グループには、USE 権限を持つユーザーを数に制限なく接続できます。このフィールドは読み取り専用です。

**注 :**

a. グループは、汎用グループとして作成することができます。この属性を作成後に変更することはできません。

b. ほとんどの場合、汎用グループを削除することは不可能です。

c. USE より高い権限を持つユーザー、またはグループ・レベルで属性 SPECIAL、OPERATIONS、または AUDITOR を持つユーザーの接続数については、以前からの制限である 5957 が引き続き適用されます。

d. 汎用グループの場合、「Connected Users」テーブルには、USE より高い権限を持つユーザー、またはグループ・レベルで属性 SPECIAL、OPERATIONS、または AUDITOR を持つユーザーのみが表示されます。

e. 汎用グループがまだサポートされていないサイトでは、「Universal」列またはフィールドが空白で使用不可のままとなります。

**Created**
グループの作成日。

**Installation data**
このフィールドの目的とレイアウトは組織により定義されます。 このフィールドの内容は変更できます。

## サブグループの追加

「**Add subgroup**」ダイアログを使用して、グループに新規サブグループを追加します。

### 手順

グループに新しいサブグループを追加するには、以下のステップを実行します。

1. グループを選択し、メインメニューから「**Action**」>「**Add subgroup**」を選択します。
   以下のアクションから開始することもできます。
   - ツールバーの「**Add subgroup**」をクリックします。
   - グループを右クリックし、ポップアップ・メニューから「**Add subgroup**」を選択します。

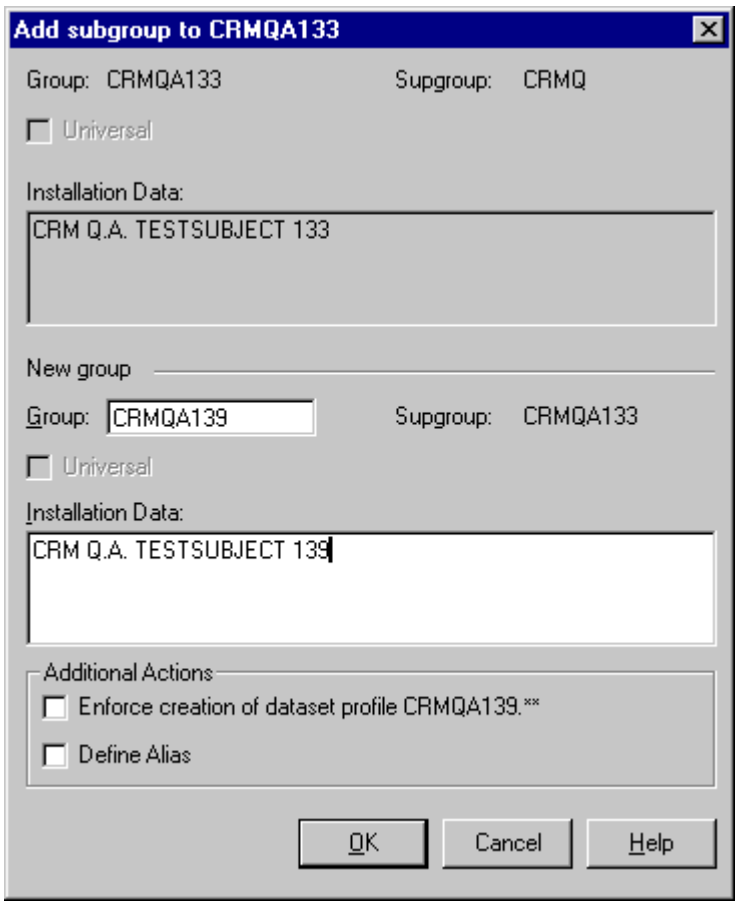



図 *49.* 「*Add subgroup*」ダイアログ

以下の情報は参照用として表示されます。

**Complex: Node**
このアクションが適用される複合システムとノードの名前は、多重システム・モードで操作している場合にのみダイアログのヘッダーに表示されます。

**Group**
サブグループを追加するグループの名前が表示されます。

**上位グループ (Supgroup)**
サブグループを追加するグループの上位グループが表示されます。

**Universal**
選択されたグループが汎用グループかどうかを示します。

**Installation Data**
新しいサブグループを追加するグループのデータが表示されます。

2. 必要に応じて、以下のフィールドを変更します。

**New group**

**Group**
必須。コピーされた名前を新しい名前に変更する必要があります。

**Installation Data**
必須。コピーされたデータを新しいデータに変更する必要があります。

**Additional Actions**

**Enforce creation of data set profile**
オプション。新しいグループ名を高位修飾子 (HLQ) とする総称データ・セット・プロファイルを作成します。このプロファイルは、新しいグループを所有者に持ち、UACC は NONE です。このコマンドは「Action」メニューでも選択できます。

**Define Alias**
オプション。ユーザー・カタログを指すグループの別名を定義します。このオプションを使用するには、ユーザー・カタログ・データ・セット名がわかっている必要があります。このコマンドは「Action」メニューでも選択できます。 このアクションは、XFACILIT クラスを検索するか、または「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の説明にあるように、サーバーのセットアップ時に Site Module 一般リソース・クラスとして構成したクラスを検索することによって、ユーザー・カタログ・データ・セット名を取得しようとします。 このとき、 SHOW MYACCESS コマンドを使用して、「CKG .UCAT.」で始まる名前のプロファイルを検索します。 該当するプロファイルが 1 つ以上見つかった場合は、このオプションをアクティブにすることができます。複数のデータ・セット名が見つかった場合は、このオプションをアクティブにする 際に、データ・セット名の 1 つを選択するように求められます。

**注 :** 注: ユーザーのアクセス権限が NONE である場合、名前が「CKG.UCAT.」で始まるプロファイルは無視されます。

3. 「**OK**」をクリックしてサブグループを 作成するか、「**Cancel**」をクリックして変更を取り消します。
4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。

   既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。

   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。

   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。

   c) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

## グループの複写

「**Duplicate group**」ウィンドウを使用して、既存のグループから新規グループを作成します。

### このタスクについて

グループを複写するか、またはグループに新しいサブグループを追加して、グループを作成することができます。複写されたグループには、元のグループと同じ接続、許可、および属性が設定されます。グループへのサブグループの 追加については、85 ページの『サブグループの追加』で説明しています。

**注 :** 多重システム・モードで操作している場合は、zSecure ノード間でのみグループを複写できます。複数の RRSF ノード間でグループを複写することはできません。

### 手順

グループを複写するには、以下のステップを実行します。

1. グループを選択し、メインメニューで「**Action**」**>**「**Duplicate**」をクリックします。

   以下のアクションから開始することもできます。

   - グループを選択し、ツールバーの「**Duplicate**」をクリックします。
   - グループを右クリックし、ポップアップ・メニューから「**Duplicate**」を選択します。

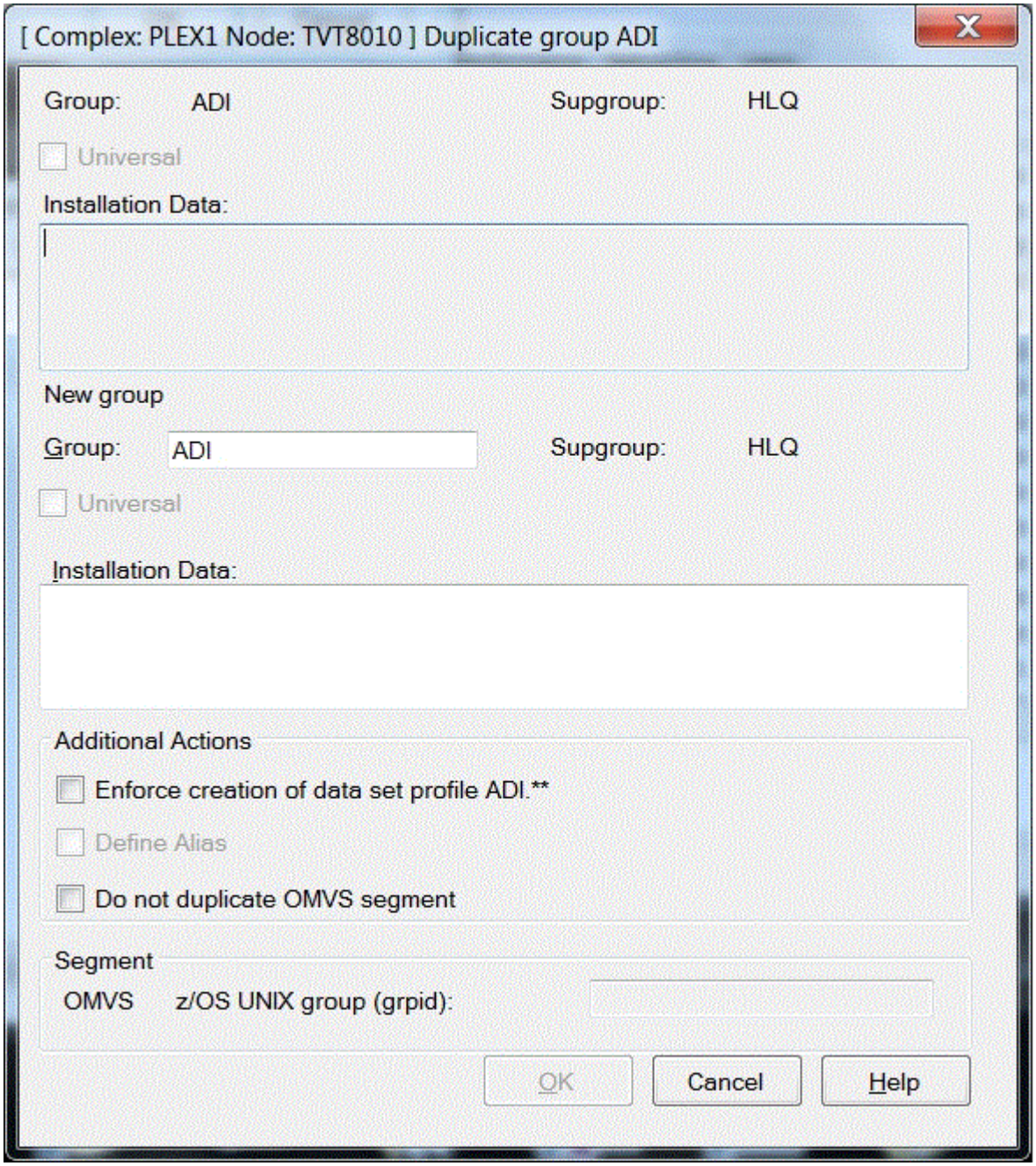



図 *50.* 「*Duplicate group*」ダイアログ

以下の情報は参照用として表示されます。

**Complex: Node**
このアクションが適用される複合システムとノードの名前は、多重システム・モードで操作している場合にのみダイアログのヘッダーに表示されます。

**Group**
新しいグループの作成元となるグループの名前が表示されます。

**上位グループ (Supgroup)**
グループの作成元となるグループの上位グループが表示されます。このグループは、新しいグループの上位グループになります。

**Universal**
選択されたグループが汎用グループかどうかを示します。

**Installation Data**
新しいグループの作成元となるグループのデータが表示されます。

2. 必要に応じて、以下のフィールドを変更します。

**New group**

**Group**
必須。コピーされた名前を新しい名前に変更します。

**Installation Data**
必須。表示されるデータは、新しいグループの作成元として使用するグループからコピーされたものです。コピーされたデータを新しいデータに変更することができます。

**Additional Actions**

**Enforce creation of data set profile**
オプション。新しいグループ名を高位修飾子 (HLQ) とする総称データ・セット・プロファイルを作成します。このプロファイルは、新しいグループを所有者に持ち、UACC は NONE です。このコマンドは「Action」メニューでも選択できます。

**Define Alias**
オプション。ユーザー・カタログを指すグループの別名を定義します。このオプションを使用するには、ユーザー・カタログ・データ・セット名がわかっている必要があります。このコマンドは「Action」メニューでも選択できます。

**注 :** このアクションは、XFACILIT クラスを検索するか、または「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント ・ガイド」の説明にあるように、サーバーのセットアップ時に Site Module 一般リソース・クラスとして構成したクラスを検索することによって、ユーザー・カタログ・データ・セット名を取得しようとします。 このとき、SHOW MYACCESS コマンドを使用して、「CKG .UCAT.」で始まる名前のプロファイルを検索します。該当するプロファイルが 1 つ以上見つかった場合は、このオプションをアクティブにすることができます。複数のデータ・セット名が見つかった場合は、このオプションをアクティブにする 際に、データ・セット名の 1 つを選択するように求められます。

**Do not duplicate OMVS Segment**
既存のグループの OMVS セグメントが複写されないようにします。

**Segment**
元のグループ・プロファイルにセグメントが存在する場合は、その値が新しいグループにコピーされ、このフィールドに表示されます。複写されたグループにセグメントが存在しない場合、またはセグメントが自分の範囲内にない場合は、このフィールドが使用不可になります。このフィールドが使用不可になっている場合は、このダイアログで新しいグループに対してこのセグメントを作成することはできません。セグメントの管理に必要な権限について詳しくは、124 ページの『セグメント管理に必要な権限および設定』を参照してください。

**OMVS z/OS UNIX group (grpid)**
z/OS UNIX グループ ID。未使用の値がシステムによって割り当てられるようにするには、「auto」を使用します。複数のグループでグループ ID を共有する場合は、grpid 値の末尾に「s」を加えます。

3.「**OK**」をクリックして重複グループを作成するか、「**Cancel**」をクリックして変更を取り消します。
4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。

既にアクションを実行している場合は、以前に選択した zSecure ノードが表示されます。

多重システム・モードを使用している場合は、以下のステップを実行します。

**注 :** 複数の RRSF ノード間でグループを複写することはできません。

a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。
b)「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

# グループの削除

「**グループの削除**」ダイアログを使用して、グループを削除するか、ユーザーがグループを使用できないようにします (不完全な削除)。

### このタスクについて

グループがリソースを所有していない場合にのみグループを削除できます。リソースを所有しているグループは、そのまま残されます。ただし、許可と接続はすべて除去されているため、ユーザーはそのグループにアクセスできません。削除が不完全であることをユーザーに通知するダイアログが表示されます。

### 手順

グループを削除するには、以下のステップを実行します。

1. グループを選択し、メインメニューで「**Action**」>「**Delete**」をクリックします。
   以下のアクションを使用することもできます。
   - グループを選択し、**Delete** キーを押します。
   - グループを右クリックしてポップアップ・メニューを表示し、「**Delete**」を選択します。
   - グループを選択し、ツールバーの「**Delete**」をクリックします。

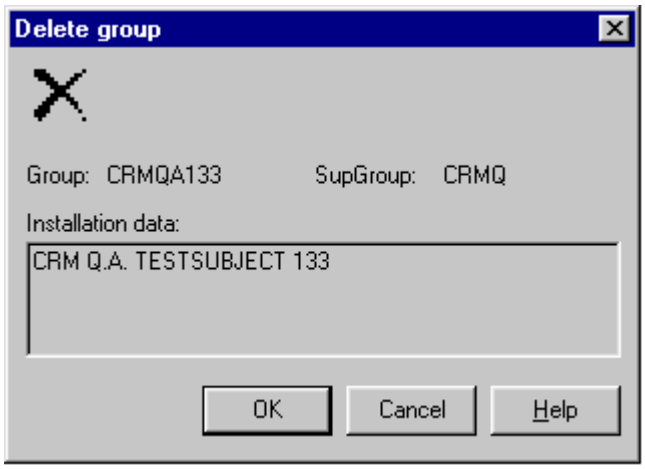



図 *51.* 「*Delete group*」ダイアログ

   このダイアログには、削除するグループの「**Group**」、「**SupGroup**」、および「Installation Data」が表示されます。多重システム・モードで操作している場合は、ダイアログの上部に関連する複合システムとノードの名前が表示されます。
2. 「**OK**」をクリックしてグループを削除するか、または「**Cancel**」をクリックして変更を行わずにダイアログを終了します。
3. 多重システム・モードを使用している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。
   既にアクションを実行している場合は、以前に選択したノードが表示されます。
   多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されます。
   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。
   c) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

# 第 6 章 接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

RACF ユーザーは、1 つ以上のグループに接続されています。接続の種類が異なると、ユーザーに対する許可も異なります。ユーザーには、少なくとも所属するグループの許可の一部が与えられます。ユーザーの許可は接続の属性によって異なりますが、ユーザーは所属するグループがアクセスできるリソースを 使用できます。ユーザーとグループの間の接続関係については、以下のトピックで説明します。

**関連概念**

IBM Security zSecure Visual のセットアップと 構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理

IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

92 ページの『接続テーブル 』

接続テーブルでユーザーまたはグループの 接続とアクセス・レベルを確認します。

93 ページの『マルチシステム・モードでの接続』

マルチシステム・モードでユーザーとグループの接続を作成および変更する際は、以下のガイドラインに従ってください。

93 ページの『接続プロパティーの表示および変更』

ユーザーおよびグループの「**Properties**」ダイアログを使用して、接続のプロパティーを表示または変更します。

97 ページの『接続の作成』

接続のプロパティーを表示または変更するには、ユーザーおよびグループの「**Properties**」ダイアログを使用します。

99 ページの『接続の削除』

「**Delete connect**」ダイアログを使用して、ユーザーおよびグループの接続を削除します。

100 ページの『接続のコピー、マージ、および移動の機能』

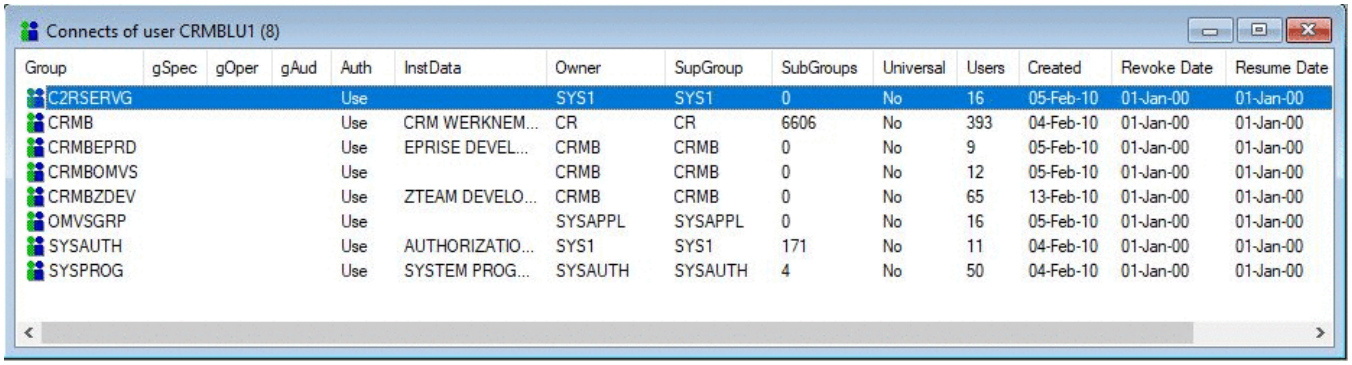
**ドラッグ・アンド・ドロップ**機能または**コピー・アンド・ペースト**機能を使用して、接続のコピー、マージ、および移動を実行します。

## 接続テーブル

接続テーブルでユーザーまたはグループの 接続とアクセス・レベルを確認します。

**接続**テーブルには、ユーザーまたはグループの接続が表示されます。接続テーブルを開くには、以下の方法を使用します。

- ユーザーまたはグループを選択し、メインメニューから「**Navigate**」>「**Connects**」を選択します。
- ユーザーまたはグループを右クリックし、ポップアップ・メニューから「**Connects**」を選択します。
- ユーザーまたはグループを選択し、ツールバーの「**Connect**」をクリックします。




| Group | gSpec | gOper | gAud | Auth | InstData | Owner | SupGroup | SubGroups | Universal | Users | Created | Revoke Date | Resume Date |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C2RSERVG | | | | Use | | SYS1 | SYS1 | 0 | No | 16 | 05-Feb-10 | 01-Jan-00 | 01-Jan-00 |
| CRMB | | | | Use | CRM WERKNEM... | CR | CR | 6606 | No | 393 | 04-Feb-10 | 01-Jan-00 | 01-Jan-00 |
| CRMBEPRD | | | | Use | EPRISE DEVEL... | CRMB | CRMB | 0 | No | 9 | 05-Feb-10 | 01-Jan-00 | 01-Jan-00 |
| CRMBOMVS | | | | Use | | CRMB | CRMB | 0 | No | 12 | 05-Feb-10 | 01-Jan-00 | 01-Jan-00 |
| CRMBZDEV | | | | Use | ZTEAM DEVELO... | CRMB | CRMB | 0 | No | 65 | 13-Feb-10 | 01-Jan-00 | 01-Jan-00 |
| OMVSGRP | | | | Use | | SYSAPPL | SYSAPPL | 0 | No | 16 | 05-Feb-10 | 01-Jan-00 | 01-Jan-00 |
| SYSAUTH | | | | Use | AUTHORIZATIO... | SYS1 | SYS1 | 171 | No | 11 | 04-Feb-10 | 01-Jan-00 | 01-Jan-00 |
| SYSPROG | | | | Use | SYSTEM PROG... | SYSAUTH | SYSAUTH | 4 | No | 50 | 04-Feb-10 | 01-Jan-00 | 01-Jan-00 |

図 *52.* 接続テーブル

**接続**テーブルは以下の列で構成されます。

グループの場合、その他の列は 81 ページの『グループ・テーブル』で説明しているグループ・テーブルと同じです。

**注 :** 汎用グループの場合、「Connected Users」テーブルには、USE より高い権限を持つユーザー、またはグループ・レベルで SPECIAL、OPERATIONS、または AUDITOR 属性を持つユーザーのみが表示されます。

ユーザーの場合、その他の列は、取り消された列を除き、54 ページの『ユーザー・テーブル 』で説明しているユーザー・テーブルと同じです。取り消された列とは、グループへの接続が取り消されたユーザーを指します。

**Complex**
結果が検出された zSecure ノードの名前。この列は、多重システム・モードで操作している場合にのみ表示されます。

**Auth**
接続権限。値は以下のいずれかです。

**Use**
ユーザーは、グループがアクセスできるリソースにアクセスできます 。

**作成**
ユーザーは、「**Use**」と同じ許可を持ち、さらにグループ名を高位修飾子 (HLQ) とするデータ・セットおよびデータ・セット・プロファイルを作成することを許可されます。

**接続 (Connect)**
ユーザーは、「**Create**」と同じ許可を持ち、さらに既存のユーザーをグループに接続することを許可されます。

**Join**
ユーザーは、「**Connect**」と同じ許可を持ち、さらに新しいサブグループを作成することを許可されます。

**gSpec**
グループ SPECIAL 属性。グループ SPECIAL 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースに関するあらゆる操作を行うことができます。ただし、監査属性は変更できません。

**gOper**
グループ OPERATIONS 属性。グループ OPERATIONS 属性を持つグループに接続されているユーザーは、そのグループの範囲内のリソースに関するあらゆる操作を行うことができます。

**gAud**
グループ AUDITOR 属性。グループ AUDITOR 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースの監査属性を変更できます。

## マルチシステム・モードでの接続

マルチシステム・モードでユーザーとグループの 接続を作成および変更する際は、以下のガイドラインに従ってください。

ユーザーとグループは、同じノードにある場合にのみ接続できます。異なるノードにまたがってユーザーとグループを接続することはできません。ただし、別のノードに同じ名前のグループとユーザーが存在する場合は、そのノードに接続を伝搬できます。

**注 :** ノード間で接続を伝搬する場合は注意が必要です。名前とグループが同一でないと、意図しない結果が生じる可能性があります。

**意図しない結果の例:**

ユーザー ID が同じで名前が異なる 2 人のユーザーが別々のノードに存在する場合、一方のユーザーの接続プロパティーをもう一方のユーザーに意図せず伝搬してしまう可能性があります。ビジュアル・クライアントでは、ユーザー ID が同じユーザー名またはグループ名を参照することは保証されません。

## 接続プロパティーの表示および変更

ユーザーおよびグループの「**Properties**」ダイアログを使用して、接続のプロパティーを表示または変更します。

**手順**

1. グループの接続ユーザーのプロパティーを表示するには、以下のいずれかのステップを実行します。
   - ユーザーを選択し、メインメニューから「**Navigate**」>「**Show Connects**」を選択します。
   - ユーザーを右クリックし、ポップアップ・メニューから「**Show Connects**」を選択します。
   - ツールバーの「**Show Connects**」をクリックします。

   グループとそのユーザーの間の接続を表示する場合は、表示されるテーブルの列の説明を 53 ページの『第 4 章 ユーザー管理』で参照してください。

   あるユーザーのグループ間の接続を表示する場合は、表示されるテーブルの列の説明を 81 ページの『第 5 章 グループ管理』で参照してください。
2. 接続のプロパティーを表示または変更するには、以下のいずれかのステップを実行します。
   - 接続ユーザーまたは接続グループを選択し、メインメニューから「**Navigate**」>「**Properties**」を選択します。
   - 接続ユーザーまたは接続グループを右クリックし、ポップアップ・メニューから「**Properties**」を選択します。
   - ツールバーの「**Properties**」をクリックします。

   表示されるダイアログは、ユーザーまたはグループのどちらのプロパティーの 表示を選択するかによって異なります。
3. グループのプロパティーを 表示するように選択した場合、次のダイアログが表示されます。

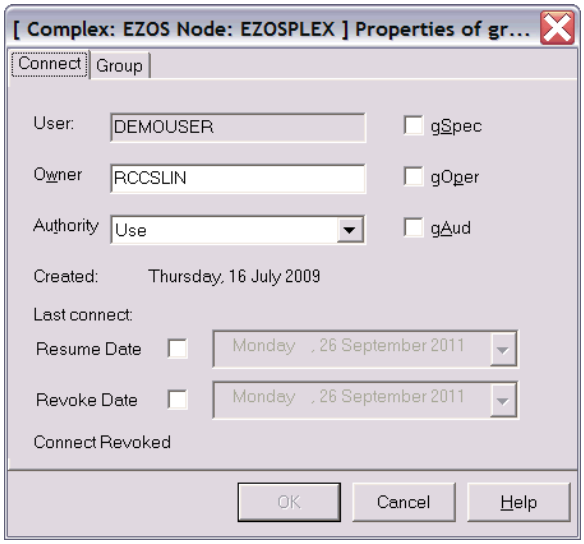



図 *53.* グループの接続プロパティー・ダイアログ

複合システムとノードの 名前は、多重システム・モードで操作している場合にのみダイアログのヘッダーに表示されます。

グループの「**Properties**」ダイアログには、「**Connect**」と「**Group**」の 2 つのタブがあります。 メインフレーム上で接続を作成するための許可の内容によって、どのフィールドを編集できるかが決まります。

グループ・プロパティーの「**Connect**」タブには、以下のフィールドが表示されます。

**User**
選択したグループの接続ユーザー。

**Owner**
グループを所有するユーザーまたはグループ。

**Authority**
接続権限。接続権限のドロップダウン・リストから、「**Use**」、「**Connect**」、「**Create**」、または「**Join**」を選択できます。

**Use**
ユーザーは、グループがアクセスできるリソースにアクセスできます。

**作成**
ユーザーは、「**Use**」と同じ許可を持ち、さらにグループ名を高位修飾子 (HLQ) とするデータ・セットおよびデータ・セット・プロファイルを作成することを許可されます。

**接続 (Connect)**
ユーザーは、「**Create**」と同じ許可を持ち、さらに既存のユーザーをグループに接続することを許可されます。

**Join**
ユーザーは、「**Connect**」と同じ許可を持ち、さらに新しいサブグループを作成することを許可されます。

**gSpec**
グループ SPECIAL 属性。グループ SPECIAL 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースに関するあらゆる操作を行うことができます。ただし、監査属性は変更できません。

**gOper**
グループ OPERATIONS 属性。グループ OPERATIONS 属性を持つグループに接続されているユーザーは、そのグループの範囲内のリソースに関するあらゆる操作を行うことができます。

**gAud**
グループ AUDITOR 属性。グループ AUDITOR 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースの監査属性を変更できます。

**Created**
接続が作成された日付。

**Last connect**
ユーザーがグループに接続されていた最新の日付。

**Resume Date**
「**User**」フィールドのユーザー ID に対してグループへの接続が再開される日付を指定します。RESUME 属性が必須である場合は、チェック・ボックスが選択されて、カレンダー (日付選択機能) が使用可能になります。カレンダーを使用して日付を指定します。

**Revoke Date**
「**User**」フィールドのユーザー ID に対してグループへの接続が取り消される日付を指定します。REVOKE 属性が必須である場合は、チェック・ボックスが選択されて、カレンダー (日付選択機能) が使用可能になります。カレンダーを使用して日付を指定します。状況をアクティブから取り消しに変更するには、現在日付と同じか、またはそれ以前の 日付を指定します。 今日の日付または以前の日付を指定すると、Visual Client は、REVOKE コマンドを未来の日付にスケジューリングする代わりに、コマンドを即座に実行します。

**Connect Revoked**
「**ユーザー**」フィールド内のユーザーの取り消し状況を示します。このフィールドは読み取り専用です。「**取り消し**」は、現在取り消された状況であることを示します。値なし (ブランク) は、状況がアクティブまたは中断状態であることを示します。 取り消し状況を変更するには、Revoke Date と Resume Date を更新する必要があります。

「Group」タブには、グループ・プロパティーのフィールドが 表示されます。詳しくは、83 ページの『グループ・プロパティーの表示』を参照してください。

4. 「**OK**」をクリックして、変更を適用します。
5. ユーザーのプロパティーを表示するように選択した場合、次のダイアログが表示されます。

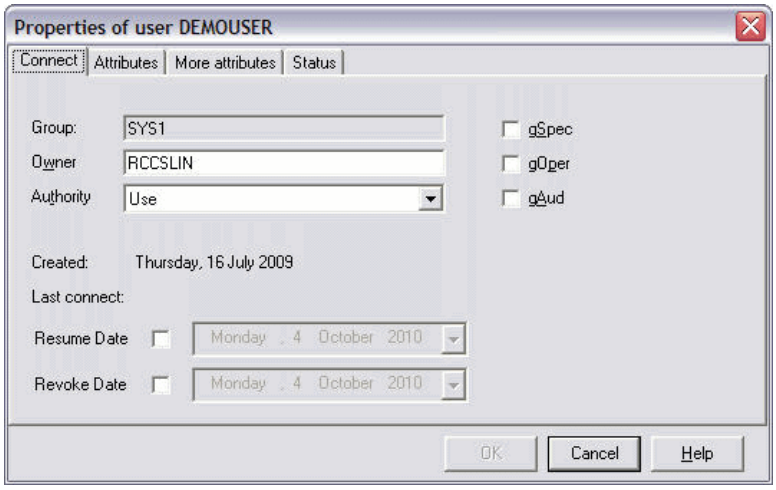



図 *54.* ユーザーの接続プロパティー・ダイアログ

複合システムとノードの 名前は、多重システム・モードで操作している場合にのみダイアログのヘッダーに表示されます。

ユーザーの「**Properties**」ダイアログには、「**Connect**」、「**Attributes**」、「**More Attributes**」、および「**Status**」の 4 つのタブがあります。メインフレーム上で接続を作成するための許可の内容によって、これらのタブのどのフィールドを編集できるかが決まります。

ユーザー・プロパティーの「**Connect**」タブには、以下のフィールドが表示されます。

**Group**
選択したユーザーの接続グループ。

**Owner**
ユーザーを所有するユーザーまたはグループ。

**Authority**
接続権限。接続権限のドロップダウン・リストから、「**Use**」、「**Connect**」、「**Create**」、または「**Join**」を選択できます。

**Use**
ユーザーは、グループがアクセスできるリソースにアクセスできます 。

**作成**
ユーザーは、「**Use**」と同じ許可を持ち、さらにグループ名を高位修飾子 (HLQ) とするデータ・セットおよびデータ・セット・プロファイルを作成することを許可されます。

**接続 (Connect)**
ユーザーは、「**Create**」と同じ許可を持ち、さらに既存のユーザーをグループに接続することを許可されます。

**Join**
ユーザーは、「**Connect**」と同じ許可を持ち、さらに新しいサブグループを 作成することを許可されます。

**gSpec**
グループ SPECIAL 属性。グループ SPECIAL 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースに関するあらゆる操作を行うことができます。ただし、監査属性は変更できません。

**gOper**
グループ OPERATIONS 属性。グループ OPERATIONS 属性を持つグループに接続されているユーザーは、そのグループの範囲内のリソースに関するあらゆる操作を行うことができます。

**gAud**
グループ AUDITOR 属性。グループ AUDITOR 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースの監査属性を変更できます。

**Created**
接続が作成された日付。

**Last connect**
ユーザーがグループに接続されていた最新の日付。

**Resume Date**
「**Group**」フィールドのグループ ID に対してユーザー ID への接続が再開される日付を指定します。RESUME 属性が必須である場合は、チェック・ボックスが選択されて、カレンダー (日付選択機能) が使用可能になります。カレンダーを使用して日付を指定します。

**Revoke Date**
「**Group**」フィールドのグループ ID に対してユーザー ID への接続が取り消される日付を指定します。REVOKE 属性が必須である場合は、チェック・ボックスが選択されて、カレンダー (日付選択機能) が使用可能になります。カレンダーを使用して日付を指定します。状況をアクティブから取り消しに変更するには、現在日付と同じか、またはそれ以前の 日付を指定します。 今日の日付または以前の日付を指定すると、Visual Client は、REVOKE コマンドを未来の日付にスケジューリングする代わりに、コマンドを即座に実行します。

**Connect Revoked**
ユーザーの取り消し状況を示します。このフィールドは読み取り専用です。「**取り消し**」は、現在取り消された状況であることを示します。値なし (ブランク) は、状況がアクティブまたは中断状態であることを示します。 取り消し状況を変更するには、Revoke Date と Resume Date を更新する必要があります。

「Attributes」、「More Attributes」、「Status」の各タブについては、60 ページの『ユーザー・プロパティーの表示 』で説明しています。

6. 「**OK**」をクリックして、変更を適用します。

## 接続の作成

接続のプロパティーを表示または変更するには、ユーザーおよびグループの「**Properties**」ダイアログを使用します。

### このタスクについて

接続とは、ユーザーとグループの間の関係です。ユーザーとグループの関係の種類は、その属性によって決まります。

### 手順

1. 接続を作成するには、ユーザーまたはグループを選択し、以下のいずれかのステップを実行します。
   - メインメニューから、「**Action**」>「**Connect**」を選択します。
   - ユーザーまたはグループを右クリックし、ポップアップ・メニューから「**Connect**」を選択します。
   - ツールバーの「**Connect**」をクリックします。

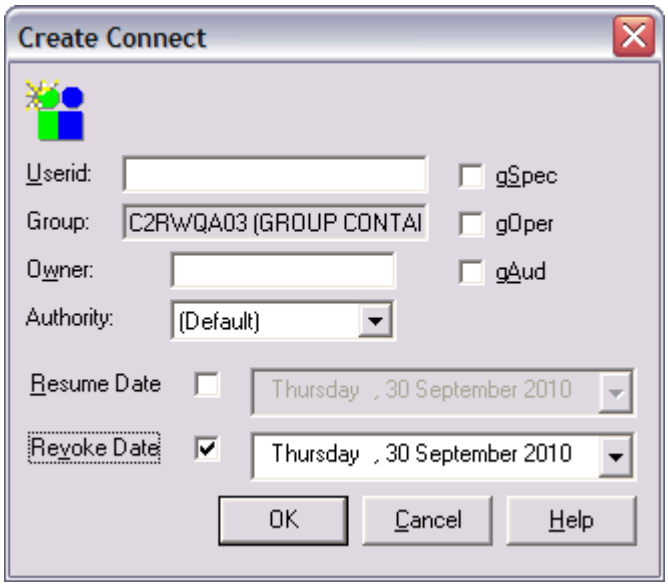



図 55. 「*Create Connect*」ダイアログ

複合システムとノードの 名前は、多重システム・モードで操作している場合にのみダイアログのヘッダーに表示されます。

2. ユーザー ID またはグループを入力します。
   以下のいずれかのオプションを選択できます。

**Authority**
接続権限。接続権限は、「Use」、「Connect」、「Create」、または「Join」のいずれかです。

**Use**
ユーザーは、グループがアクセスできるリソースにアクセスできます。

**作成**
ユーザーは、「**Use**」と同じ許可を持ち、さらにグループ名を高位修飾子 (HLQ) とするデータ・セットおよびデータ・セット・プロファイルを作成することを許可されます。

**接続 (Connect)**
ユーザーは、「**Create**」と同じ許可を持ち、さらに既存のユーザーをグループに接続することを許可されます。

**Join**
ユーザーは、「**Connect**」と同じ許可を持ち、さらに新しいサブグループを作成することを許可されます。

**gSpec**
グループ SPECIAL 属性。グループ SPECIAL 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースに関するあらゆる操作を行うことができます。ただし、監査属性は変更できません。

**gOper**
グループ OPERATIONS 属性。グループ OPERATIONS 属性を持つグループに接続されているユーザーは、そのグループの範囲内のリソースに関するあらゆる操作を行うことができます。

**gAud**
グループ AUDITOR 属性。グループ AUDITOR 属性を持つグループに接続されているユーザーは、そのグループの範囲内のユーザー、グループ、およびリソースの監査属性を変更できます。

**Resume Date**
「**Userid**」フィールドのユーザー ID に対してグループへの接続が再開される日付を指定します。RESUME 属性が必須である場合は、チェック・ボックスが選択されて、カレンダー (日付選択機能) が使用可能になります。カレンダーを使用して日付を指定します。

**Revoke Date**
「**Userid**」フィールドのユーザー ID に対してグループへの接続が取り消される日付を指定します。REVOKE 属性が必須である場合は、チェック・ボックスが選択されて、カレンダー (日付選択機能) が使用可能になります。カレンダーを使用して日付を指定します。

3. 「**OK**」をクリックすると接続されます。
4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。

   既にアクションを実行している場合は、以前に選択したノードが表示されます。必要であれば、接続作成アクションを適用するノードを変更できます。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されることに注意してください。

   **注 :** 接続は、同じノード上に存在するユーザーとグループに対してのみ作成できます。異なるノードにまたがってユーザーとグループの接続を作成することはできません。ただし、別のノードに同じ名前のグループとユーザーが存在する場合は、複数のシステムを選択することで、指定したノードに新しい接続が伝搬されます。ノード間で新しい接続を伝搬する場合は注意が必要です。93 ページの『マルチシステム・モードでの接続』を参照してください。

   ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択できます。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。

   a) 「**OK**」をクリックします。
   選択した一連のノードが検査され、選択したノードごとに接続作成アクションが実行されます。
5. どのノードも選択せずに前のダイアログに戻るには、「**Cancel**」をクリックします。

## 属性 gSpec、gOper、および gAud

「**GrpSpecial**」、「**GrpOperations**」、および「**GrpAuditor**」の各範囲属性が、使用不可になっている場合があります。

属性 **GrpSpecial**、**GrpOperations**、および **GrpAuditor** がぼかし表示されている場合は、それらの属性を指定できません。接続がこれらの属性とともに存在しない限り、新しい接続にそれらの属性を持たせることはできません。

## ドラッグ・アンド・ドロップおよびコピー・アンド・ペースト

ドラッグ・アンド・ドロップ機能またはコピー・アンド・ペースト機能を使用して、接続を作成できます。

ドラッグ・アンド・ドロップで接続を作成することもできます。グループ上のあるリストから別のリストに (あるいはその逆に) ユーザーをドロップすると、ポップアップ・メニューが表示されます。「**Connect**」を選択すると、接続が作成されます。

**注 :** 新しい接続にはいずれも同じ属性が設定されます。

メインメニュー・バーのコピー・アンド・ペースト機能を使用することもできます。この機能では、すべての属性がコピーされます。詳しくは、30 ページの『コピー・アンド・ペースト機能』を参照してください。

## 接続の削除

「**Delete connect**」ダイアログを使用して、ユーザーおよびグループの接続を削除します。

### 手順

接続を削除するには、以下のステップを実行します。

1. **接続**テーブルで接続を選択し、以下のいずれかのステップを実行します。
   - メインメニューから、「**Action**」>「**Delete**」を選択します。
   - 接続を右クリックし、ポップアップ・メニューから「**Delete**」を選択します。
   - ツールバーの「**Delete**」をクリックします。
   - **Delete** キーを押します。
   - 接続をドラッグし、ごみ箱にドロップします。

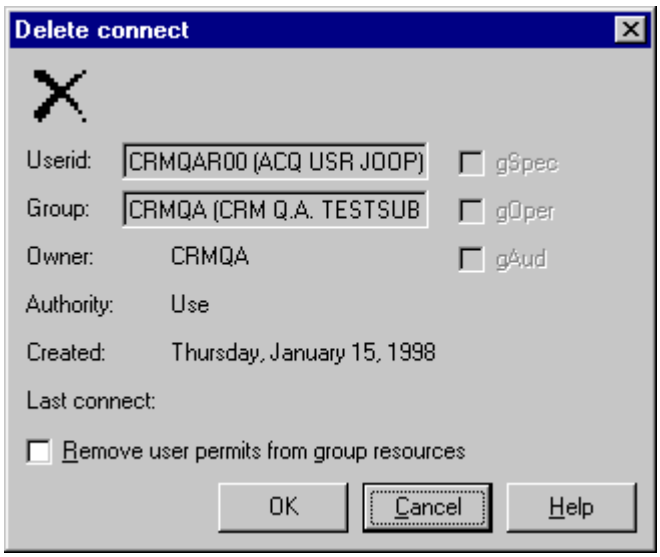



図 56. 「*Delete connect*」ダイアログ

2. 「**Remove user permits from group resources**」オプションでは、グループ・リソースのすべてのアクセス・リストからユーザーを除去する必要があることを指定します。
3. 「**OK**」をクリックして接続を削除または除去します。
4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。
   a) 接続削除アクションを適用するノードを選択します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。ローカル・ノード項目が強調表示されることに注意してください。

   **注 :** 接続は、同じノード上に存在するユーザーとグループに対してのみ削除できます。異なるノードにまたがってユーザーとグループの接続を削除することはできません。ただし、別のノードに同じ名前のグループとユーザーが存在する場合は、複数のシステムを選択することで、指定したノードに接続削除アクションが伝搬されます。ノード間で接続削除アクションを伝搬する場合は注意が必要です。93 ページの『マルチシステム・モードでの接続』を参照してください。

   ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択できます。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。

b)「**OK**」をクリックします。選択した一連のノードが検査され、選択したノードごとに接続削除アクションが実行されます。

c) どのノードも選択せずに前のダイアログに戻るには、「**Cancel**」をクリックします。

## 接続のコピー、マージ、および移動の機能

**ドラッグ・アンド・ドロップ**機能または**コピー・アンド・ペースト**機能を使用して、接続のコピー、マージ、および移動を実行します。

**ドラッグ・アンド・ドロップ**または**コピー・アンド・ペースト**を使用して、接続をコピー、マージ、および移動することができます。**ドラッグ・アンド・ドロップ**を使用する場合は、あるテーブルから接続をドラッグして同様のテーブルにドロップできます。ドロップすると、以下のオプションを含んだポップアップ・メニューが表示されます。

**コピー**

ドラッグした接続が、ターゲット・テーブルにコピーされます。接続が存在し、ドラッグした接続よりも高い権限を持っている場合は、接続をコピーするかマージするかを選択できます。コピーを選択すると、ドラッグした接続でターゲットの接続が置換されます。マージを選択すると、すべての新しい接続に、両方の接続の属性が設定され、最も高い接続権限が与えられます。

**注 :** 接続をコピーする際に、Revoke Date または Resume Date が現在日付と同じかそれ以前の場合、RACF により日付のコピーや入力ができなくなります。100 ページの表 4 に、接続のコピー操作でどのように Revoke と Resume の値が管理されるかを示します。

表 *4.* 接続のコピー操作前後での、*Revoke* と *Resume* の値

| **元の値** | | | **コピー出力の値** | | |
|---|---|---|---|---|---|
| **取り消しフラグ** | **Revoke Date** | **Resume Date** | **取り消しフラグ** | **新規 Revoke Date** | **新規 Resume Date** |
| | None | None | | None | None |
| | GT 今日 | None | | *Revoke Date をコピー | None |
| | GT 今日 | GT Revoke Date | | *Revoke Date をコピー | Resume Date をコピー |
| | LT 今日 | LE 今日 & GT Revoke Date | | (1)None | None |
| Yes | LE 今日 | None | **Yes | (2)None | None |
| | LT 今日 | 今日 | | None | None |
| Yes | LE 今日 | GT 今日 | **Yes | (3)None | Resume Date をコピー |
| Yes | None | None | **Yes | None | None |
| | None | LT 今日 | | None | None |
| | None | 今日 | | None | None |
| Yes | None | GT 今日 | **Yes | None | Resume Date をコピー |
| 凡例: LT = より前、LE = より前か等しい、GT = より後、None = 指定されない | | | | | |

| 表 4. 接続のコピー操作前後での、*Revoke* と *Resume* の値 (続き) | |
|---|---|
| **元の値** | **コピー出力の値** |
| *一時的な接続の場合、Revoke Date を削除してコピー操作で永続的な接続を作成できるようにする必要があります。<br>**コピーされた値に取り消しフラグが設定された場合、その接続の初期状態は取り消しに設定されます。<br>**コピー結果の例:**<br>(1)Resume Date は今日の日付と同じかそれ以前のため、Resume Date が優先されます。 新規接続に取り消しおよび再開は設定されません。<br>(2)接続は既に取り消し済み (過去の日付) のため、新規接続は取り消しに設定され、Revoke Date または Resume Date は設定されません。<br>(3) 接続の現在の状況は取り消し (過去の日付) ですが、明日以降の Resume Date が指定されます。新規接続は取り消しになり、指定された日付で再開するよう設定されます。 | |

**マージ**

接続のマージ操作の結果は、Resume Date と Revoke Date のさまざまな組み合わせに基づきます。目的は、以下のような状況により意図せずに接続がアクティブになることを防ぐことです。

- 取り消しが遅すぎる。
- 再開が早すぎる。
- 永続的な取り消しが必要な時に再開を行う。

マージによる結果が予期せぬもの、または望まないものである場合は、ユーザーまたはグループのプロパティー・ダイアログを開いて日付を変更します。以下の例は、結果がどのように導き出されるかを示しています。

**接続のマージ例:**

接続のマージが以下のような接続間で実行されます:

- 現在日付は 11 月 1 日である。
- アクティブなソース 接続は、Revoke Date が 11 月 15 日で、Resume Date が設定されていない。
- アクティブなターゲット 接続は、Revoke Date が 11 月 5 日、Resume Date が 12 月 1 日に設定されている。

この操作の結果は、現在から取り消される 11 月 5 日までアクティブで、再開日付が設定されない接続となります。

**移動**

移動アクションでは、コピーまたはマージと、それに続いて正常にコピーまたはマージされた接続の削除が組み合わせて行われます。移動オプションを指定できるダイアログが表示されます。「**Remove user permits from group resources**」オプションでは、削除アクションでグループのリソース・プロファイルのアクセス・リストからユーザーを除去する必要があるかどうかを指定します。

コピーして貼り付ける操作を実行する場合は、メインメニューから「**Copy and Paste**」を選択します。「**Copy and Paste**」について詳しくは、30 ページの『コピー・アンド・ペースト機能』を参照してください。

# 第 7 章 リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

**関連概念**

IBM Security zSecure Visual のセットアップと構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理

IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

104 ページの『リソース・プロファイル』

各種リソースに対するアクセス規則は、リソース・クラスにプロファイルとして保持されています。このセクションでは、これらのリソース・プロファイルについて説明します。

107 ページの『リソース・プロファイルの追加』

「**Add resource profile**」ダイアログを使用して、リソース・プロファイルを最初から作成します。

109 ページの『リソース・プロファイルの複写』

「**Duplicate resource profile**」ダイアログを使用して、既存のプロファイルからリソース・プロファイルを作成します。

110 ページの『リソース・プロファイル・プロパティーの編集』

「**Properties of resource profile**」ダイアログを使用して、リソース・プロファイルのプロパティーを変更します。

112 ページの『リソース・プロファイルの削除』

「**Delete resource profile**」ダイアログを使用して、リソース・プロファイルを削除します。

113 ページの『アクセス・リスト (ACL) の変更』

「**アクセス・リスト**」ウィンドウを使用して、リソース・プロファイルのアクセス・リストの項目を表示、追加、および変更します。

115 ページの『アクセス・リストへのユーザーまたはグループの追加』

「**Add to access list**」ダイアログを使用して、リソース・プロファイルのアクセス・リストにユーザーまたはグループを追加します。

116 ページの『アクセス・リスト項目の編集』
「**Edit Access List**」ダイアログを使用して、リソース・プロファイルのアクセス・リストに含まれるユーザー項目またはグループ項目を編集します。

117 ページの『アクセス・リスト項目の削除』
「**削除**」オプションを使用して、リソース・プロファイルのアクセス・リストに含まれるユーザーまたはグループの項目を削除します。

117 ページの『プロファイル・メンバー』
管理者は、以下のガイドラインに従って、グループ化クラスの使用を計画および実装してください。

119 ページの『メンバー・リストの表示および変更』
「**メンバー**」ウィンドウを使用して、一般リソース・プロファイルのメンバー・リストを表示および変更します。

120 ページの『メンバーの追加』
リソース・プロファイルのメンバー・リストに新規メンバーを追加するには、「**Add member**」ダイアログを使用します。

120 ページの『メンバーの編集』
「**Edit member**」ダイアログを使用して、リストのメンバーを変更します。

121 ページの『メンバーの削除』
「**削除**」機能を使用して、リストからメンバーを削除します。

121 ページの『クラスのリフレッシュ』
「**リフレッシュ**」機能を使用して、RACF データベース内のリソース・プロファイルを変更した後にクラスを更新します。

## リソース・プロファイル

各種リソースに対するアクセス規則は、リソース・クラスにプロファイルとして保持されています。このセクションでは、これらのリソース・プロファイルについて説明します。

アクセス権限検査は、アクセス権限検査の対象となるリソースのタイプに応じて、特定のリソース・クラスに対して行われます。例えば、データ・セットを読み込むための DATASET や、ユーザーが特定のマシンを使用してログオンできるかどうかを調べるための TERMINAL などについて検査が行われます。各クラス内のプロファイルは、一連のアクセス権限設定を表しています。プロファイル名には、汎用の名前 (マスク指定など) を使用できます。RACF は、特定のクラス内のリソース名に最も近いプロファイル名を検索することで、適用するアクセス権限設定を判別します。

RACF では、DATASET プロファイルとその他のすべてのリソース・プロファイルは区別されます。DATASET プロファイルは、データ・セットへのアクセスを制御する DATASET クラスにあります。 その他のすべてのリソース・プロファイルは、一般リソース・プロファイル と呼ばれます。zSecure Visual では、両方のタイプのプロファイルを処理できます。

プロファイルでリソースを保護するには、そのプロファイルが適切なクラスにある必要があります。 プロファイルの名前は、リソースの名前と一致する必要があります。 例えば、データ・セット CKR.CKR240.SCKRLOAD を保護するには、CKR.CKR240.SCKRLOAD という名前のプロファイルを DATASET クラスに作成します。

すべてのリソースに対してリソース・プロファイルを作成しなくて済むように、RACF では、プロファイル名に汎用文字を使用することができます。 文字「*」を使用して、1 つの修飾子、または現在の修飾子の残りの部分を表すことができます。 連続した「**」は、ゼロ個以上の修飾子を表します。 以下の例は、文字「*」を使用した場合にどのように一致するかを示しています。

```
CKR.CKR*.SCKRLOAD matches CKR.CKR240.SCKRLOAD.
CKR.CKR240.SCKRLOAD.* does not match CKR.CKR240.SCKRLOAD,
                                 because it has no fourth qualifier.
CKR.** matches CKR.CKR240.SCKRLOAD.
CKR.**.SCKRLOAD matches CKR.CKR240.SCKRLOAD.
```

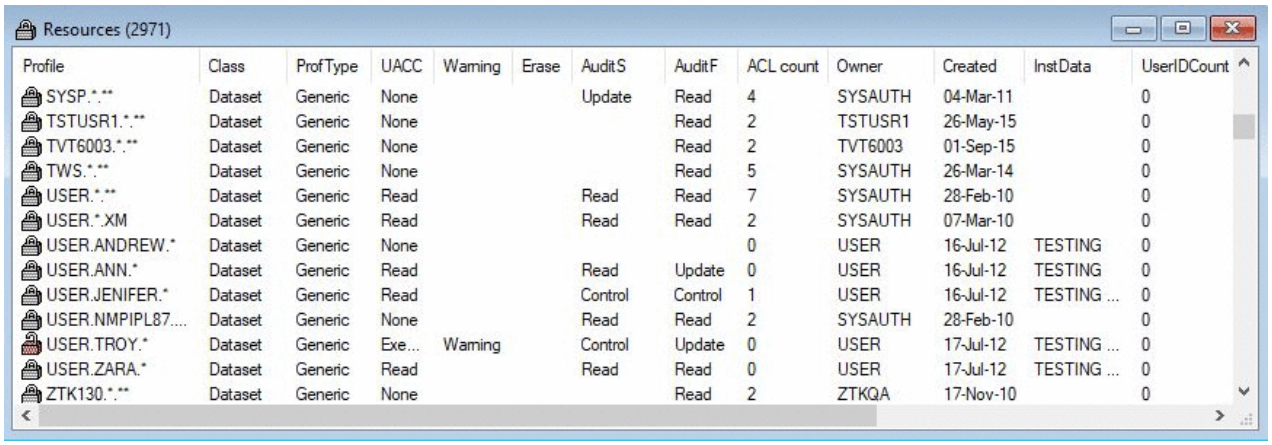
特定のリソースと一致するリソース・プロファイルが複数ある場合、RACF は最も具体的なプロファイルを使用します。 つまり、最初の汎用文字の左側に最も多くの文字を持つプロファイルを使用します。

## リソース・テーブル

リソース・テーブルでは、リソース・プロファイルの内容を確認することができます。

通常、プロファイルには、そのプロファイルに含まれているリソースに対してユーザーおよびグループが持っているアクセス権限を指定するアクセス・リストが含まれています。 一部の一般リソース・クラスでは、別の手順によってアクセス権限が付与されます。

「**Find**」ダイアログを使用して、すべてのリソースのリストを見つけます。 クラス内に「*」を使用して、さまざまなリソース・クラスのプロファイルを 1 つのテーブル内に取得できます。 「Class」フィールドを空のままにすると、ユーザーまたはグループを除く、すべてのリソースを取得できます。




| Profile | Class | ProfType | UACC | Warning | Erase | AuditS | AuditF | ACL count | Owner | Created | InstData | UserIDCount |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SYSP.*.** | Dataset | Generic | None | | | Update | Read | 4 | SYSAUTH | 04-Mar-11 | | 0 |
| TSTUSR1.*.** | Dataset | Generic | None | | | | Read | 2 | TSTUSR1 | 26-May-15 | | 0 |
| TVT6003.*.** | Dataset | Generic | None | | | | Read | 2 | TVT6003 | 01-Sep-15 | | 0 |
| TWS.*.** | Dataset | Generic | None | | | | Read | 5 | SYSAUTH | 26-Mar-14 | | 0 |
| USER.*.** | Dataset | Generic | Read | | | Read | Read | 7 | SYSAUTH | 28-Feb-10 | | 0 |
| USER.*.XM | Dataset | Generic | Read | | | Read | Read | 2 | SYSAUTH | 07-Mar-10 | | 0 |
| USER.ANDREW.* | Dataset | Generic | None | | | | | 0 | USER | 16-Jul-12 | TESTING | 0 |
| USER.ANN.* | Dataset | Generic | Read | | | Read | Update | 0 | USER | 16-Jul-12 | TESTING | 0 |
| USER.JENIFER.* | Dataset | Generic | Read | | | Control | Control | 1 | USER | 16-Jul-12 | TESTING ... | 0 |
| USER.NMPIPL87.... | Dataset | Generic | None | | | Read | Read | 2 | SYSAUTH | 28-Feb-10 | | 0 |
| USER.TROY.* | Dataset | Generic | Exe... | Warning | | Control | Update | 0 | USER | 17-Jul-12 | TESTING ... | 0 |
| USER.ZARA.* | Dataset | Generic | Read | | | Read | Read | 0 | USER | 17-Jul-12 | TESTING ... | 0 |
| ZTK130.*.** | Dataset | Generic | None | | | | Read | 2 | ZTKQA | 17-Nov-10 | | 0 |

図 *57.* リソース・テーブル

**リソース**・テーブル内の結果フィールドは、以下のようになります。

**Complex**
結果が検出された zSecure ノードの名前。この列は、多重システム・モードで操作している場合にのみ表示されます。

**Class**
プロファイルが置かれているクラス。

**Profile**
プロファイルの名前。

**ProfType**
プロファイル・タイプ。一般リソースの場合、discrete または generic にすることができます。 データ・セットの場合、generic、nonvsam、vsam、tapedsn、または model にすることができます。

**UACC**
アクセス・リストからアクセス権限を決定できないユーザーに、プロファイルによって付与されるアクセス権限。

**Warning**
警告モードのプロファイルは、常にリソースへのアクセスを許可しますが、アクセス権限がアクセス・リストまたは UACC によって許可されている権限を超える場合、監査ログ・レコードが書き込まれます。

**Erase**
削除時にデータ・セットを上書きします。このフラグが考慮されるのは、SETROPTS ERASE コマンドを使用して中央の「Erase」フラグが設定された場合に限られます。

**AuditS**
成功用の監査レベル。

**AuditF**
失敗用の監査レベル。

**ACLCount**
プロファイルのアクセス・リストにあるユーザー ID およびグループの数。

**Owner**
プロファイルを変更できるユーザー ID またはグループ。

**Notify**
監査違反が起こった場合にメッセージを受け取るユーザー ID。

**InstData**
このフィールドの内容と手段は組織により定義されます。

**Appldata**
このフィールドは、DATASET クラスにあるプロファイルを除く、すべてのリソース・プロファイルである一般リソース・プロファイルに対してのみ定義されます。 その内容と手段は、クラスによって異なります。

**Volser**
個別 DATASET プロファイルの場合、プロファイルが保護するボリュームが含まれます。

**Created**
プロファイルが作成された日付。

**UserIDcount**
IDIDMAP プロファイルの場合、このプロファイルに関連するユーザー ID の数を示します。

「**Find**」ダイアログにある、リソース用のその他の選択フィールドは、以下のとおりです。

**Installation data**
インストール・データ内で指定されたパターンを持つリソースのみを選択します。

**Owner**
指定したフィルターに所有者が一致するリソースのみを選択します。

**Segment**
指定したセグメントを持つリソースを選択します。このオプションが使用不可になっている場合、セグメントを表示できないか、セグメントがありません。オプション「*any*」を指定すると、プロファイルにセグメントがあるかどうかにかかわらず、完全なリソース・リストが得られます。

## マッピング情報の表示

「**Mappings**」選択項目を使用して、IDIDMAP プロファイルのマッピング情報を表示します。

### 手順

IDIDMAP プロファイルの場合、以下のステップに従って、それらに関連するマッピング情報を表示することができます。

1. メインメニューから IDIDMAP プロファイルを選択します。
2. 「**Navigate**」>「**Mappings**」の順に選択します。
   あるいは、IDIDMAP プロファイルを右クリックして、ポップアップ・メニューを表示し、「**Mappings**」を選択します。

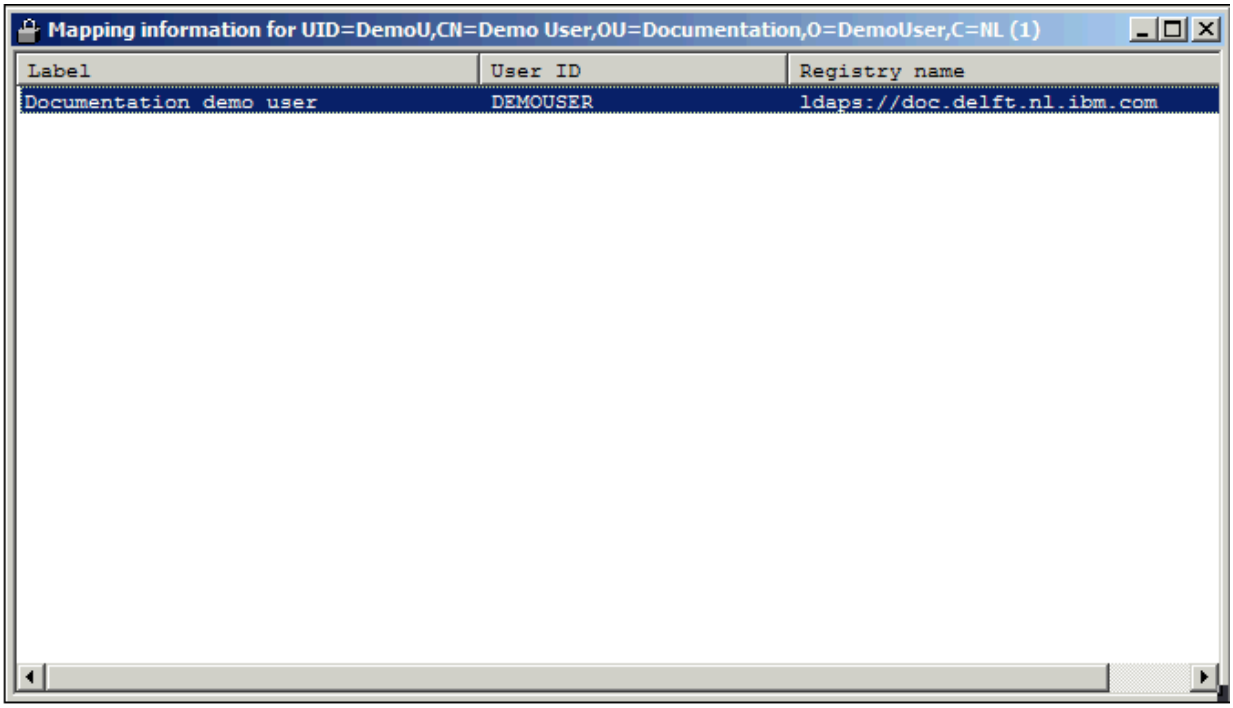



図 *58. IDIDMAP* プロファイルのマッピング情報

表示されるウィンドウで、以下のフィールドを表示できます。

**Complex**
結果が検出された複合システムの名前。このフィールドは、多重システム・モードで操作している場合にのみ表示されます。

**Label**
識別マッピングに関連付けられたラベル。

**User ID**
識別マッピングに関連付けられたユーザー ID。

**Registry name**
識別マッピングのレジストリー名。

**注 :** IDIDMAP プロファイルの複写、追加、編集、または削除を行うことはできません。詳しくは、79 ページの『マッピングの表示』を参照してください。

## リソース・プロファイルの追加

「**Add resource profile**」ダイアログを使用して、リソース・プロファイルを最初から作成します。

### このタスクについて

リソース・テーブルを使用して新規のリソース・プロファイルを作成することができます。

**注 :** 完全修飾の総称など、総称 DATASET プロファイルのみを作成することができます。

### 手順

最初からリソース・プロファイルを作成するには、 以下のステップを実行します。

1. リソース・テーブルを開きます。
2. リソース・テーブルからプロファイルを選択し、「**Action**」>「**Add Resource**」を選択します。

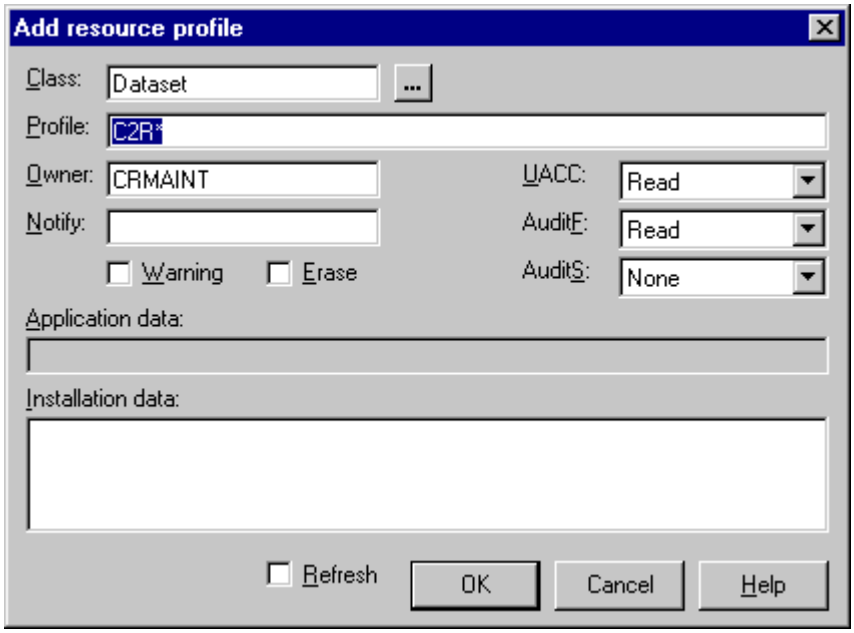



図 59. リソース・プロファイルの追加のダイアログ

3. プロファイル・データを入力します。

   フィールドおよびオプションの 説明を以下に示します。

   **Complex: Node**
   このアクションが適用される複合システムとノードの 名前は、多重システム・モードで操作している場合にのみダイアログのヘッダーに表示されます。

   **Class**
   プロファイルが置かれているクラス。zSecure Visual は、ユーザーが選択したプロファイルのクラスをデフォルト・クラスとして使用します。 このクラスは変更できます。

   **Profile**
   プロファイルの名前。

   **UACC**
   アクセス・リストからアクセス権限を決定できないユーザーに、プロファイルによって付与されるアクセス権限。

   **Warning**
   警告モードのプロファイルは、常にリソースへのアクセスを許可しますが、アクセス権限がアクセス・リストまたは UACC によって許可されている権限を超える場合、監査ログ・レコードが書き込まれます。

   **Erase**
   このフラグは、クラスが DATASET である場合にのみ有効です。このフラグが設定されている場合、データ・セットは削除時に上書きされますが、それは SETROPTS ERASE コマンドを使用して中央の「Erase」フラグが設定された場合に限られます。

   **AuditS**
   成功用の監査レベル。

   **AuditF**
   失敗用の監査レベル。

   **Owner**
   プロファイルを変更できるユーザー ID またはグループ。

   **Notify**
   監査違反が起こった場合にメッセージを受け取ることができるユーザー ID。

   **InstData**
   このフィールドの内容と手段は組織により定義されます。

**Appldata**
このフィールドは、DATASET クラスにあるプロファイルを除く、すべてのリソース・プロファイルである一般リソース・プロファイルに対してのみ定義されます。 その内容と手段は、クラスによって異なります。

**Refresh**
クラスのキャッシュされたプロファイルを持つユーザーに対しても、新規プロファイルが即時に有効になるように、クラスをリフレッシュします。 「**Refresh**」を指定しなければ、プロファイルは、キャッシュされたプロファイルを持たないユーザーに対してのみアクティブになります。

4. すべてのユーザーに対してプロファイルの変更を即時に有効にする必要がある場合は、「**Refresh**」をクリックして、クラスをリフレッシュします。クラスをリフレッシュしない場合、プロファイルは、プロファイルをキャッシュしていないユーザーに対してのみアクティブになります。
5. 「**OK**」をクリックしてプロファイルを作成するか、「**Cancel**」をクリックして新規プロファイルを取り消します。

   単一ノード・モードで操作している場合、1 つ以上の値を変更するまで「**OK**」は使用できません。

   多重システム・モードで操作している場合は、「**OK**」を使用して、別のノードで選択したリソース・プロファイルを作成することができます。

## リソース・プロファイルの複写

「**Duplicate resource profile**」ダイアログを使用して、既存のプロファイルからリソース・プロファイルを作成します。

### このタスクについて

既存のプロファイルを複写して、プロファイルを作成できます。プロファイルを複写すると、元のプロファイルのアクセス・リストとメンバー・リストが新規プロファイルにコピーされます。 必要に応じて、新規プロファイルをカスタマイズして、データを変更することができます。

**注 :** リソース・プロファイルを DATASET クラスから一般リソース・クラスへ (あるいはその逆に) コピーすることはできません。

### 手順

リソース・プロファイルを複写するには、以下のステップを実行します。

1. リソース・テーブルからリソース・プロファイルを選択し、メインメニューから「**Action**」>「**Duplicate**」を選択します。

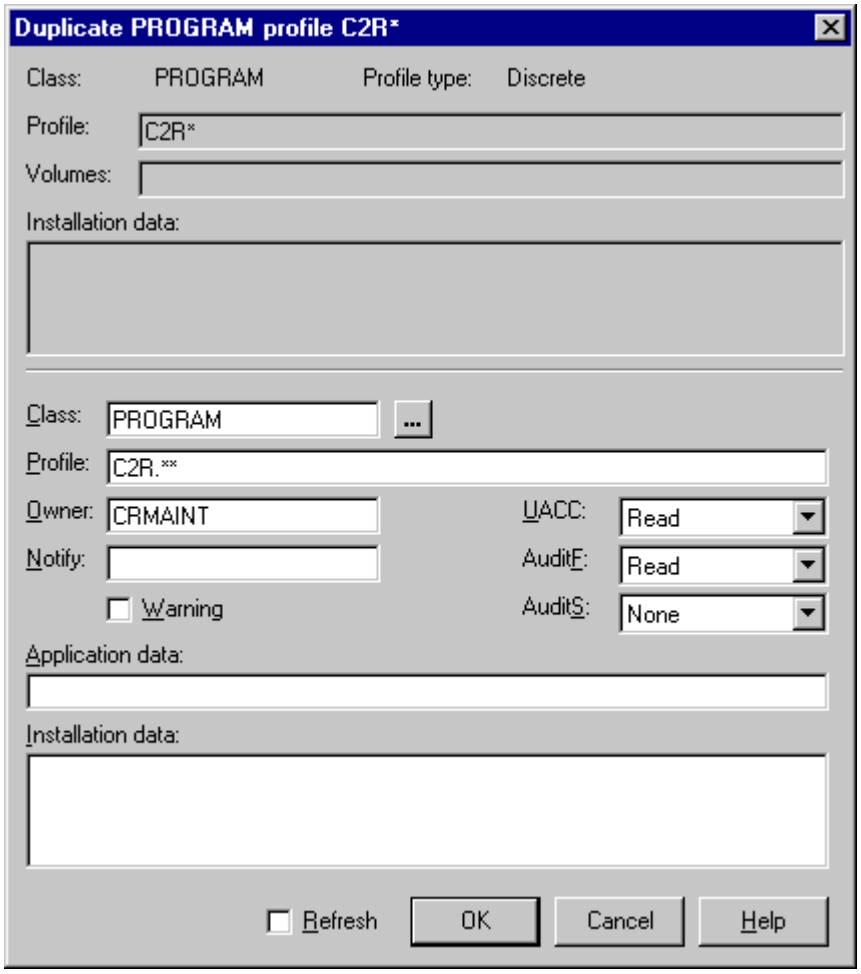



図 *60.* リソース・プロファイルの複写のダイアログ

2. プロファイルを複写して単一ノード用の新規プロファイルを作成する場合は、フィールド内のデータを変更してください。 フィールドの説明については、107 ページの『リソース・プロファイルの追加』を参照してください。
3. すべてのユーザーに対して新規プロファイルを即時に有効にする必要がある場合は、「**Refresh**」をクリックして、クラスをリフレッシュします。 クラスをリフレッシュしない場合、プロファイルは、プロファイルをキャッシュしていないユーザーに対してのみアクティブになります。
4. 「**OK**」をクリックして、プロファイルを作成します。別のノード用にプロファイルを複写する場合は、プロファイルを適用するノードを選択してから、「**OK**」をクリックします。

## リソース・プロファイル・プロパティーの編集

「**Properties of resource profile**」ダイアログを使用して、リソース・プロファイルのプロパティーを変更します。

### 手順

リソース・プロファイルのプロパティーを変更するには、以下のステップを実行します。

1. プロファイルを選択し、メインメニューから「**Navigate**」>「**Properties**」を選択します。

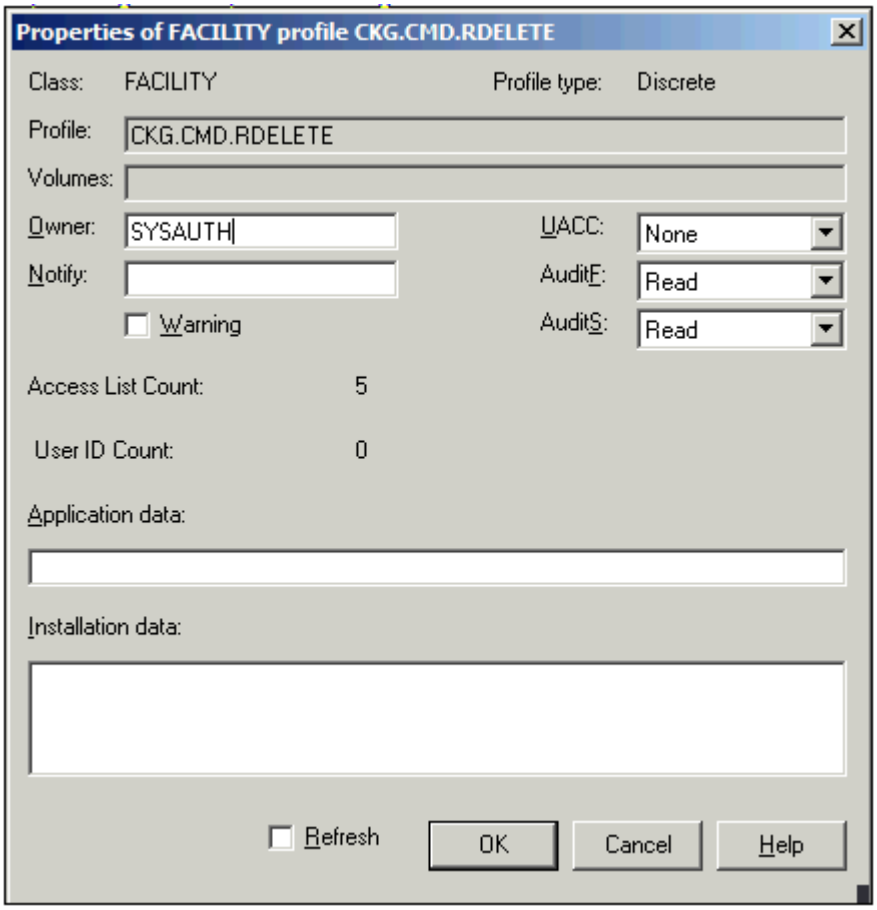



図 *61.* リソース・プロファイルの *Properties* ダイアログ

2. 必要に応じて、プロパティーを編集します。

**注 :** このダイアログでは、以下のプロパティーは編集できません。

- Class
- Profile
- Volumes
- Access List Count
- User ID Count

多重システム・モードで操作している場合は、選択項目の適用先となる複合システムおよびノードがダイアログのヘッダーに表示されます。

以下のプロパティーが表示されます。

**Class**
プロファイルが置かれているクラス。

**Profile type**
RACF プロファイルのタイプ。例えば、Generic、VSAM、Non VSAM、Model、Type DSN などがあります。

**Profile**
プロファイルの名前。

**Volumes**
個別 DATASET プロファイルの場合、このフィールドにはそのプロファイルが保護するボリュームが含まれます。

**Owner**
プロファイルを変更できるユーザー ID またはグループ。

**Notify**
監査違反が起こった場合にメッセージを受け取るユーザー ID。

**Warning**
警告モードのプロファイルは、常にリソースへのアクセスを許可しますが、アクセス権限がアクセス・リストまたは UACC によって許可されている権限を超える場合、監査ログ・レコードが書き込まれます。

**Erase**
削除時にデータ・セットを上書きします。このフラグが考慮されるのは、SETROPTS ERASE コマンドを使用して中央の「Erase」フラグが設定された場合に限られます。

**ACLCount**
プロファイルのアクセス・リストにあるユーザー ID およびグループの数。ここで、数を直接変更することはできません。ただし、プロファイルを選択して、メインメニューから「**Navigate**」>「**Access List**」と選択すると、アクセス・リストを拡張または縮小することができます。

**Application data**
このフィールドは、DATASET クラスにあるプロファイルを除く、すべてのリソース・プロファイルである一般リソース・プロファイルに対してのみ定義されます。 その内容と手段は、クラスによって異なります。

**Installation data**
このフィールドの内容と手段は組織により定義されます。

**Profile type**
プロファイルのタイプ。

**UACC**
アクセス・リストからアクセス権限を決定できないユーザーに、プロファイルによって付与されるアクセス権限。

**AuditF**
失敗用の監査レベル。

**AuditS**
成功用の監査レベル。

**User ID count**
IDIDMAP プロファイルの場合、このプロファイルに関連するユーザー ID の数を示します。

3. プロファイルの変更を即時に有効にする必要がある場合は、「**Refresh**」をクリックして、クラスをリフレッシュします。
4. 「**OK**」をクリックして、変更を適用します。
5. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されることに注意してください。
   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。
   c) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

## リソース・プロファイルの削除

「**Delete resource profile**」ダイアログを使用して、リソース・プロファイルを削除します。

### 手順

リソース・プロファイルを削除するには、以下のステップを実行します。

1. リソース・テーブルからリソース・プロファイルを選択し、メインメニューから「**Action**」>「**Delete**」を選択します。

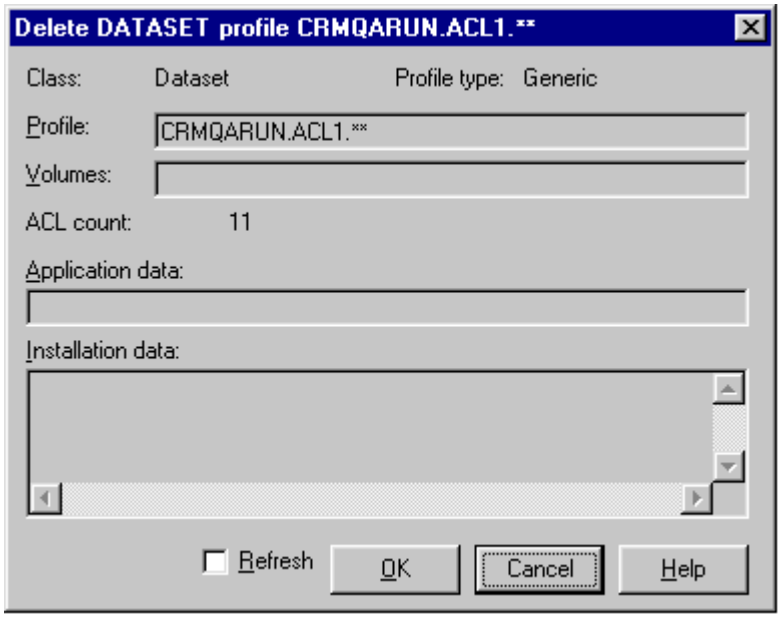



図 62. リソース・プロファイルの削除のダイアログ

2. 「**Refresh**」を選択して、プロファイルの削除を即時に適用します。
3. 「**OK**」をクリックして、プロファイルを削除します。
4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されることに注意してください。
   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。
   c) 「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

## アクセス・リスト (ACL) の変更

「**アクセス・リスト**」ウィンドウを使用して、リソース・プロファイルのアクセス・リストの項目を表示、追加、および変更します。

### このタスクについて

アクセス・リストの名前は ACL のように省略されることがよくあります。通常、リソース・プロファイルにはアクセス・リストが含まれており、このリストにはユーザー ID とグループ ID、それらに付与されているアクセス権限、およびオプションで条件が含まれています。

### 手順

1. リソース・プロファイルのアクセス・リストを表示するには、プロファイルを選択して、メインメニューから「**Navigate**」>「**Access List**」とクリックします。

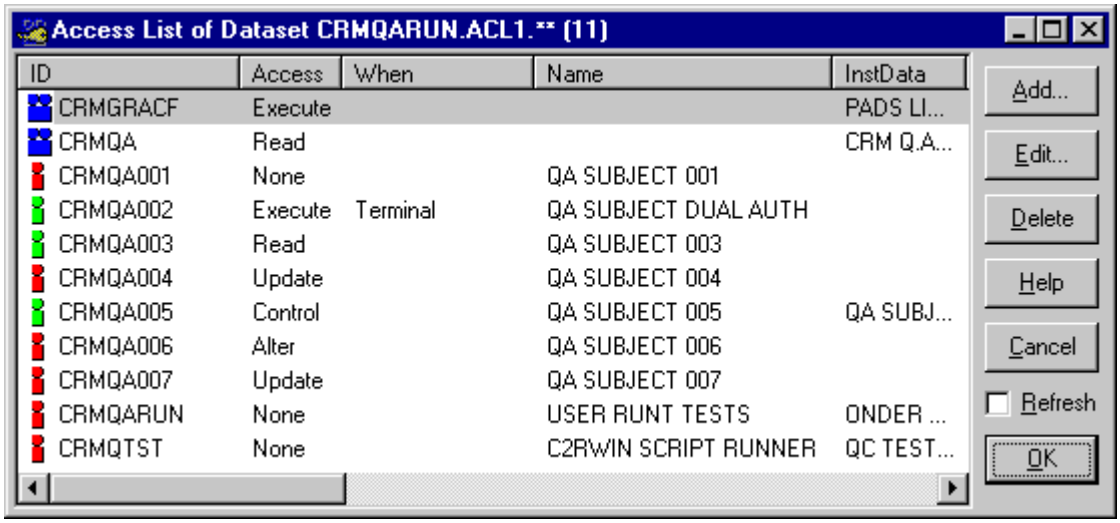



図 *63. Access list*

グループをアクセス・リストに入れると、そのグループのすべてのユーザーはアクセス権限を得ます。詳しくは、52 ページの『有効なアクセス・リストの表示』を参照してください。ユーザーおよびグループの列については、17 ページの『第 2 章 IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク』および 53 ページの『第 4 章 ユーザー管理』で説明しています。アクセス・リスト・テーブルには、以下の列もあります。

**Node**
ID に関連付けられたノードの名前。

**ID**
ユーザー ID またはグループ。

**Access**
付与されているアクセス権限。これには、常に以下のオプションの中の 1 つが設定されます。

**None**
指定されたユーザーまたはグループに対して、すべてのアクセス手段が拒否されます。

**Execute**
指定されたユーザーまたはグループが、リソースを実行できます。これは、データ・セットおよびプログラムに対してのみ有効です。

**Read**
指定されたユーザーまたはグループが、リソースの実行および読み取りを行えます。

**Update**
指定されたユーザーまたはグループが、リソースの実行、読み取り、および更新または書き込みを行えます。

**Control**
指定されたユーザーまたはグループが、リソースの実行、読み取り、更新または書き込み、および作成または除去を行えます。

**Alter**
指定されたユーザーまたはグループが、リソースの所有者のように、リソースに対してすべての操作を行うことができ、リソース・プロファイルを変更できます。

**When**
フィールドがブランクである場合は条件がないことを意味するため、制限なくアクセス権限が付与されます。 このフィールド項目の形式は、以下のようになります。

`APPCPort` *`appcport`* `Console` *`console`* `JESInput` *`class`* `Program` *`program`* `SYSID` *`id`* `Terminal` *`terminal`*

2. 以下のステップを実行して、リスト内の ID 項目の追加、削除、または変更を行い、変更を処理します。
   a) リスト項目 (ID) を選択します。

b) 「**Add**」、「**Edit**」、または「**Delete**」をクリックして、リスト項目を変更します。
選択したタスク用のダイアログが表示されます。

- 115 ページの『アクセス・リストへのユーザーまたはグループの追加』
- 116 ページの『アクセス・リスト項目の編集』
- 117 ページの『アクセス・リスト項目の削除』

c) 変更を行うと、「**OK**」および「**Cancel**」ボタンがメインの「Access List」ウィンドウで使用可能になります。

3. 「**Refresh**」をクリックして、クラスをリフレッシュします。 クラスのキャッシュされたプロファイルを持つユーザーに対しても、新規アクセス・リストは即時に有効になります。

**注 :** 影響を受けるプロファイルがキャッシュされているユーザーに対しては、クラスをリフレッシュするまで変更は有効になりません。

4. 「**OK**」をクリックして、アクセス・リストへの変更をメインフレームに適用します。
5. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。

a) 変更を適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。ローカル・ノード項目が強調表示されることに注意してください。

b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。

c) 「**OK**」をクリックして、選択したノードのリストを確認します。現在のノードの ID を選択した場合、変更内容を使用して更新されます。 その後、現在のノードへの変更が、選択したその他のノードに複製されます。

**注 :**

- RACF データベースにわたって、ID データにおける相違を把握する必要があります。つまり、現在のノードとその他のノードで、初期アクセス・リストが異なる場合があります。
- 現在のノードと異なる ID は、そのままその他のノードに残ります。
- クライアントは、ユーザー ID またはグループ ID がその他のノードに存在することを検査しません。 ID がターゲット・データベースに存在しない場合、その ID は RACF によってエラーとして拒否され、無視されます。

## アクセス・リストへのユーザーまたはグループの追加

「**Add to access list**」ダイアログを使用して、リソース・プロファイルのアクセス・リストにユーザーまたはグループを追加します。

### 手順

アクセス・リストにユーザーまたはグループを追加するには、以下のステップを実行します。

1. アクセス・リストを表示して、テーブル・ウィンドウの「**Add**」をクリックします。

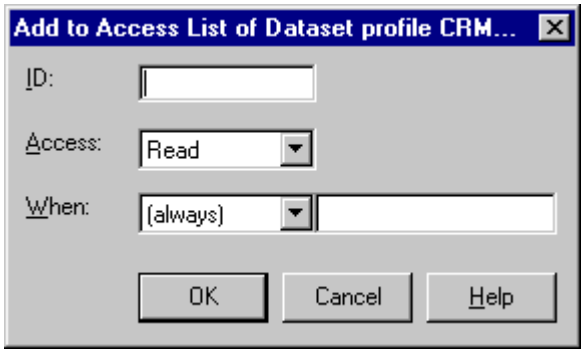



図 *64.* アクセス・リストへの追加のダイアログ

2. 以下の情報を指定します。

   **ID**
   ユーザー ID またはグループ ID。

   **Access**
   ID に設定されたアクセス権限のレベル。

   **When**
   アクセス権限の付与に使用される条件。

3. 「**Refresh**」を選択して、すべてのユーザーに対して新規 ID を即時にアクティブに設定します。 リフレッシュしなければ、ID は、ID をキャッシュしていないユーザーに対してのみアクティブになります。
4. 異なる条件を持つ同じ ID をアクセス・リストに追加するには、「**OK**」をクリックします。同じ条件を持つが、異なるアクセス権限を持つ同じ ID を追加すると、新しいアクセス権限が前のアクセス権限に優先します。

   変更は、アクセス・リストのメイン・フォームで更新されます。 メインの「Access List」ダイアログで「**OK**」をクリックしてすべての変更を処理するまで、変更は処理されません。

## アクセス・リスト項目の編集

「**Edit Access List**」ダイアログを使用して、リソース・プロファイルのアクセス・リストに含まれるユーザー項目またはグループ項目を編集します。

### 手順

アクセス・リストのユーザー項目またはグループ項目を編集するには、以下のステップを実行します。

1. 項目を選択して、テーブル・ウィンドウの「**Edit**」をクリックします。

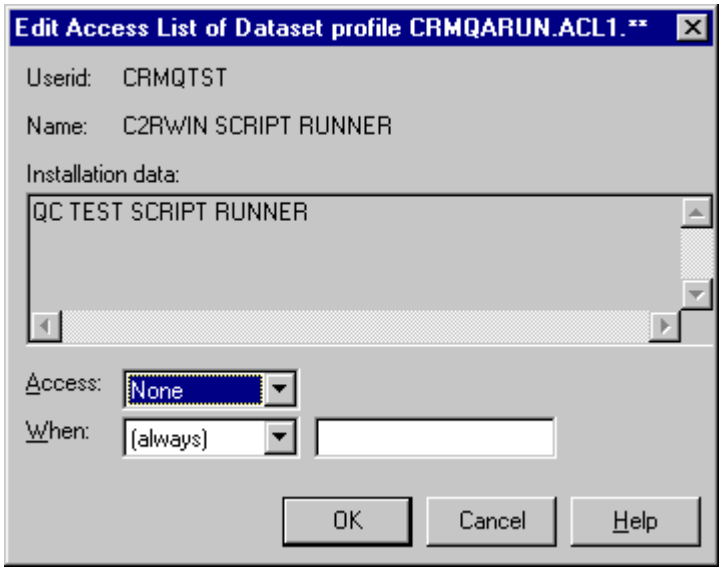



図 65. アクセス・リストの編集のダイアログ

2. 必要に応じて、以下のフィールドを編集します。

   **ID**
   ユーザー ID またはグループ ID。

   **Access**
   ID に設定されたアクセス権限のレベル。

   **When**
   アクセス権限の付与に使用される条件。

3. 「**OK**」をクリックして、アクセス・リストに変更を適用します。

   変更は、アクセス・リストのメイン・フォームで更新されます。 メインの「Access List」ダイアログで「**OK**」をクリックしてすべての変更を処理するまで、変更は処理されません。

## アクセス・リスト項目の削除

「**削除**」オプションを使用して、リソース・プロファイルのアクセス・リストに含まれるユーザーまたはグループの項目を削除します。

### 手順

項目を削除するには、以下のステップに従います。

1. アクセス・リストで、ユーザー項目またはグループ項目を選択します。
2. テーブル・ウィンドウで「**Delete**」をクリックするか、「**Action**」 > 「**Delete**」を選択します。
3. 「**OK**」をクリックして、選択した内容を削除します。

   変更は、アクセス・リストのメイン・フォームで更新されます。 メインの「Access List」ダイアログで「**OK**」をクリックしてすべての変更を処理するまで、変更は処理されません。

## プロファイル・メンバー

管理者は、以下のガイドラインに従って、グループ化クラスの使用を計画および実装してください。

DATASET プロファイル以外のすべてのリソース・プロファイルに、メンバー・リストを含めることができます。 実際には、数種類のクラスにしか、メンバーを含むプロファイルはありません。通常、プロファイル・メンバーは、個々のリソースではなく、リソースのグループにアクセスするために使用されます。 メンバーと、グループ化クラスが必要です。

メンバーとグループ化クラスは、クラス記述子テーブルで一緒にリンクされます。 メンバー・クラスには、通常の方法のアクセスを受け入れるプロファイルを含めることができます。 グループ化クラスは、リソースのグループに対するアクセス権限を付与するために使用されます。 グループは、クラス内のプロファイルによって表されます。このグループ・プロファイルには、メンバーのリストを入れることができ、それぞれにリソース名が含まれます。 グループ・プロファイルに付与されたすべての権限によって、メンバーに指定されているすべてのリソースに対するアクセス権限が受け入れられます。

**重要 :** グループ構造の設計は重要です。 使いやすさを考慮して、グループ名には、リソース・グループの内容または使用法のいずれかを示す分かりやすい名前を付ける必要があります。 以下のような使用は避けてください。

- 同じリソースに対して、メンバーとグループ化クラスの両方を同時に使用する。
- 複数のリソース・グループに対するアクセス権限をユーザーまたはグループに付与するときに、複数のグループで同じリソースを繰り返し使用する。

複数のリソースに対してアクセス権限を組み合わせる場合に生じるさまざまな問題は複雑であり、予期しない結果や好ましくない結果を生じる場合もあります。 また、明確な結果レポートも入手できません。

## グループ化クラスの例

管理者は、以下に示すシナリオ例を使用して、グループ化クラスを計画および実装してください。

グループ化を使用する主な理由は、過度な管理オーバーヘッドを避けることです。 このグループ化が役立つ可能性のある例として、CICS トランザクションの管理が挙げられます。メンバー・クラス TCICSTRN を使用して、個々のトランザクションへのアクセス権限を付与できます。 すべてのトランザクションに対して、プロファイルが必要です。ただし、これにより、すぐに煩雑な状況になってしまいます。 個々のトランザクション・プロファイルが大量に作成されるのを回避するために、GCICSTRN グループ化クラスにプロファイルを編成することができます。 CICS システムおよびジョブの記述によってグループ分割を行うと便利な場合があります。

**GCICSTRN class**

| Profile | Members |
|---|---|
| CICSPROD.OPER | CICSPROD.CEMT<br>CICSPROD.CSOT<br>CICSPROD.CSFR<br>... |
| CICSPROD.DEV | CICSPROD.CEMT<br>CICSPROD.CEDA<br>CICSPROD.CAUT<br>... |
| CICSTEST.DEV | CICSTEST.CEMT<br>CICSTEST.CAUT<br>... |
| ... | ... |

図 66. グループ化クラスの例

グループ化を慎重に計画して実装するのであれば、個々のトランザクションに権限を付与するより、リソース・グループに権限を付与する方が簡単に行え、エラーも少なくなります。

## 例外

管理者は、特別な考慮を要する、これらの例外的なグループ化クラスについて認識しておく必要があります。

クラスの中には、前述の方法とは異なる方法でプロファイル・メンバーが使用されるクラスがあります。これに関連するメカニズムについては、本マニュアルでは説明しません。 以下に、よく知られている例外を示します。

- グローバル・アクセス・テーブル (GLOBAL クラス、DATASET プロファイル)
- NODES クラス

- PROGRAM クラス
- RACFVARS クラス

## メンバー・リストの表示および変更

「**メンバー**」ウィンドウを使用して、一般リソース・プロファイルのメンバー・リストを表示および変更します。

### 手順

リソース・プロファイルのメンバー・リストを表示して、リストを変更するには、以下のステップを実行します。

1. プロファイルを選択し、メインメニューから「**Navigate**」>「**Members**」を選択します。

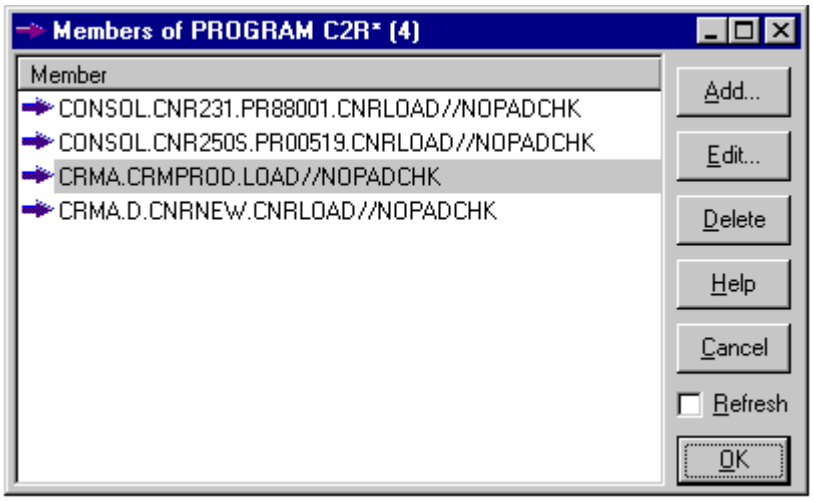



図 67. メンバー・リスト

2. 「**Add**」、「**Edit**」、または「**Delete**」をクリックして、メンバー・リストを変更します。
3. 「**Refresh**」をクリックして、変更を即時に有効にします。 同じクラスのキャッシュされたプロファイルを持つユーザーに対しては、クラスをリフレッシュするまで変更は有効にならない場合があります。
4. 「**OK**」をクリックして、変更をメインフレームに適用します。
5. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されることに注意してください。
   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。
   c) 「**OK**」をクリックして、選択したノードのリストを確認します。現在のノードのメンバーを選択した場合、変更内容を使用して更新されます。 選択したその他のノードのメンバー・リストは、現在のメンバー・リストで置き換えられます。
   d) どのノードも選択せずに前のダイアログに戻るには、「**Cancel**」をクリックします。

## メンバーの追加

リソース・プロファイルのメンバー・リストに新規メンバーを追加するには、「**Add member**」ダイアログを使用します。

### 手順

メンバーを追加するには、以下のステップを実行します。

1. メンバー・テーブル・ウィンドウで「**Add**」をクリックします。

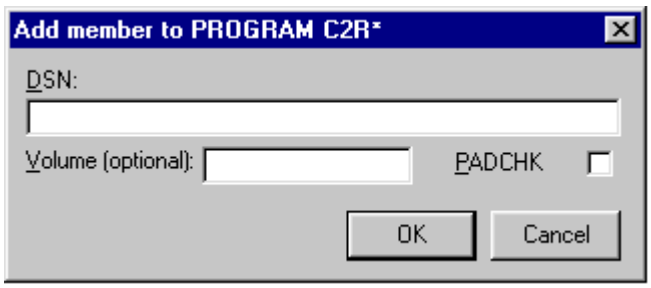



図 68. 「*Add member*」ダイアログ

2. 新規メンバーを入力します。

   **注 :** メンバーを PROGRAM クラスに追加するときは、「**DSN**」、「**Volume**」、および「**PADCHK**」の各フィールドを使用して、新規メンバー・ストリングを構成します。

3. 「**OK**」をクリックして、新規メンバーをリストに追加します。 影響を受けるプロファイルがキャッシュされているユーザーに対しては、メイン・メンバー・リストでクラスをリフレッシュするまで変更は有効になりません。

## メンバーの編集

「**Edit member**」ダイアログを使用して、リストのメンバーを変更します。

### 手順

メンバーを編集するには、以下のステップを実行します。

1. メンバーを選択して、メンバー・テーブル・ウィンドウで「**Edit**」をクリックします。


図 69. 「*Edit member*」ダイアログ

2. メンバーを変更し、「**OK**」をクリックして、メンバーをリストに配置します。

   **注 :** PROGRAM クラスのメンバーを編集するときは、「**DSN**」、「**Volume**」、および「**PADCHK**」の各フィールドを使用して、メンバー・ストリングを構成します。

3. 「**OK**」をクリックして、変更をメンバー・リストに適用します。 影響を受けるプロファイルがキャッシュされているユーザーに対しては、メイン・メンバー・リストでクラスをリフレッシュするまで変更は有効になりません。

## メンバーの削除

「**削除**」機能を使用して、リストからメンバーを削除します。

### 手順

メンバーを削除するには、以下のステップを実行します。

1. メンバーを選択して、メンバー・テーブル・ウィンドウで「**Delete**」をクリックします。あるいは、メインメニューから「**Action**」>「**Delete**」を選択します。
2. 「**Refresh**」をクリックして、変更を即時に有効にします。 キャッシュされているプロファイルを持つユーザーに対しては、クラスをリフレッシュするまで変更は有効になりません。
3. 「**OK**」をクリックして、削除をメインフレームに送信します。
4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。
   a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されることに注意してください。
   b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。
   c) 「**OK**」をクリックして、選択したノードのリストを確認します。現在のノードのメンバーを選択した場合、変更内容を使用して更新されます。 選択したその他のノードのメンバー・リストは、現在のメンバー・リストで置き換えられます。
   d) どのノードも選択せずに前のダイアログに戻るには、「**Cancel**」をクリックします。

## クラスのリフレッシュ

「**リフレッシュ**」機能を使用して、RACF データベース内のリソース・プロファイルを変更した後にクラスを更新します。

### このタスクについて

RACF データベースでリソース・プロファイルを変更したら、リフレッシュを行って、すべてのユーザーのキャッシュされているプロファイルに変更を伝搬する必要があります。

### 手順

クラスをリフレッシュするには、以下のステップを実行します。

1. メインメニューから、「**Action**」>「**Refresh**」を選択します。

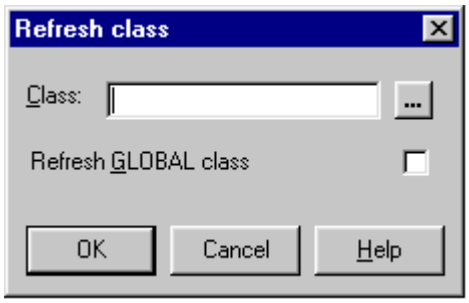



図 *70.* 「*Refresh class*」ダイアログ

2. 「**Class**」フィールドにクラス名を入力します。

3.「**Refresh GLOBAL**」クラスを選択して、このクラス自体ではなく、クラスのグローバル・アクセス・テーブルをリフレッシュします。 クラスが不明な場合は、「Class」フィールドの横にあるボタンをクリックして、「**Select**」クラス・ダイアログを表示してください。

詳しくは、42 ページの『「Select class」ダイアログによるクラスの検索』 を参照してください。

# 第 8 章 セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

アプリケーション・セグメントとは、RACF 以外の、TSO または z/OS UNIX のようなメインフレーム・アプリケーションについての情報を含むプロファイルの一部です。ユーザー、グループ、およびリソースは、すべて独自のセグメントを持っています。セグメントを管理するには、以下のタスクを実行します。

**関連概念**

IBM Security zSecure Visual のセットアップと 構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理

IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

124 ページの『セグメント管理に必要な権限および設定』

セグメントを管理するには、権限および設定を表示して編集する必要があります。

124 ページの『セグメント・タイプの表示および編集』

セグメントの表示および編集を行うには、「**Segmenttypes**」テーブルを開きます。

126 ページの『セグメント・リストの表示』

「**Segment list**」オプションを使用して、特定のセグメント・タイプを持つクラスのセグメントを表示します。

127 ページの『セグメント詳細ウィンドウの使用』

「**セグメント**」オプションを使用して、単一プロファイルのセグメントに関する情報を表示します。ここでは、その手順について説明します。

129 ページの『セグメントの追加』

「**Add segment**」オプションを使用して、プロファイルにセグメントを直接追加します。

130 ページの『例外』

このトピックのリストを使用して、セグメント詳細ウィンドウで編集できないセグメントを判別します。

131 ページの『セグメント・フィールド』

このトピックに記載されているセグメント・フィールドの説明を使用して、セグメント・タイプに関する情報を入手してください。

## セグメント管理に必要な権限および設定

セグメントを管理するには、権限および設定を表示して編集する必要があります。

セグメントを表示するには、管理レベル「Full」で「**Interface level**」オプションを設定する必要があります。このレベルを選択するには、メインメニューで「**View**」>「**Options**」と移動します。

セグメント管理の特定の許可要件について詳しくは、*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイドにある『ユーザー用のセグメント編集』のセクションを参照してください。

## セグメント・タイプの表示および編集

セグメントの表示および編集を行うには、「**Segmenttypes**」テーブルを開きます。

### このタスクについて

IBM Security zSecure Visual では、セグメントの表示と編集を行えます。[**Segmenttypes**」テーブルには、zSecure Visual が表示可能なすべてのセグメントの概要が表示されます。

### 手順

セグメント・タイプを表示して編集するには、以下のステップに従ってください。

1. メインメニューから「**Navigate**」>「**Segmenttypes**」を選択します。

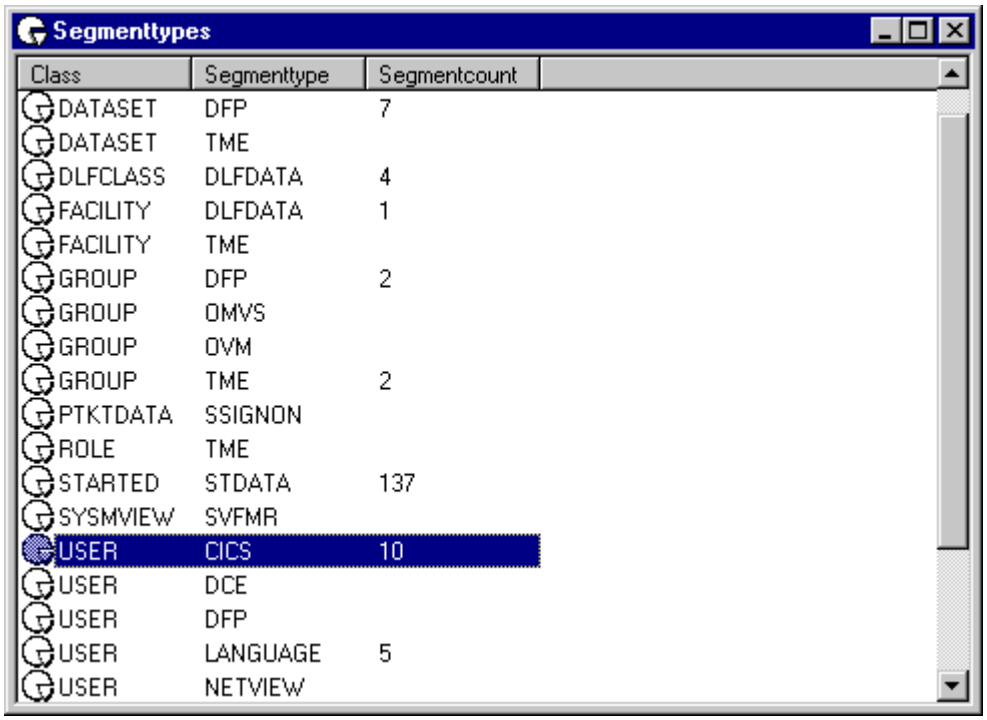



図 *71.* セグメント・タイプ

「**Segmenttypes**」テーブルには、以下の列があります。

**Complex**
セグメントを適用する zSecure ノードの名前。この列は、多重システム・モードで操作している場合にのみ表示されます。

**Class**
セグメントが属するクラス。

**Segmenttype**
セグメント・タイプ。

**Segmentcount**
セグメントの数。

**注 :** この数は、最初は指定されていません。 あるセグメントに関する情報が表示されるたびに、そのセグメントに関連する数が「**Segmenttypes**」リストで更新されます。

2. セグメントに関する情報を表示するには、行を右クリックして、「**Segment List**」を選択します。126 ページの『セグメント・リストの表示』を参照してください。

## アプリケーション・セグメント

管理者は、以下のテーブルを使用して、ユーザー、グループ、およびリソースの各プロファイルに関連付けるセグメントを決定します。

以下の表には、関連するクラスにおけるリソース・プロファイルのセグメントがリストされています。リソース・クラス内のプロファイルには、CSDATA セグメントも指定できます。

| クラス | セグメント |
|---|---|
| APPCLU | SESSION |
| CDT | CDTINFO |
| CFIELD | CFDEF |
| CSFKEYS | ICSF |
| DATASET | DFP |
| DATASET | TME |
| DIGTCERT | CERTDATA |
| DIGTRING | CERTDATA |
| DLFCLASS | DLFDATA |
| EJBROLE | TME |
| FACILITY | DLFDATA |
| FACILITY | EIM |
| FACILITY | PROXY |
| FACILITY | TME |
| GCSFKEYS | ICSF |
| GXCSFKEY | ICSF |
| IDTDATA | IDTPARMS |
| JESJOBS | JES |
| LDAPBIND | EIM |
| LDAPBIND | ICTX |
| LDAPBIND | PROXY |
| MFADEF | MFPOLICY |
| PROGRAM | SIGVER |
| PTKTDATA | SSIGNON |
| REALM | KERB |

| クラス | セグメント |
|---|---|
| ROLE | TME |
| STARTED | STDATA |
| SYSMVIEW | SVFMR |
| XCSFKEY | ICSF |

グループ・プロファイルのセグメントは、以下のとおりです。

- CSDATA
- DFP
- OMVS
- OVM
- TME

ユーザー・プロファイルのセグメントは、以下のとおりです。

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

## セグメント・リストの表示

「**Segment list**」オプションを使用して、特定のセグメント・タイプを持つクラスのセグメントを表示します。

### 手順

セグメント・リストを表示するには、以下のステップを実行します。

1. 「Segment Types」ウィンドウを開きます。
2. クラスとセグメント・タイプの組み合わせを選択し、メインメニューから「**Navigate**」>「**Segment list**」を選択します。または、
3. クラスとセグメント・タイプを右クリックし「**Segment list**」を選択します。

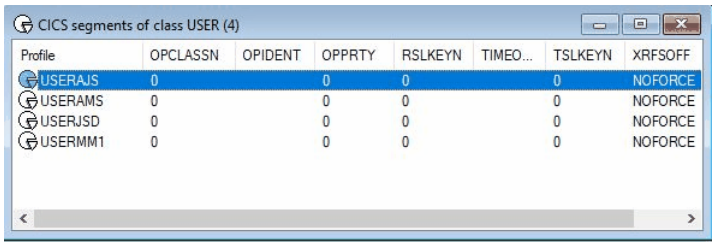



図 72. セグメント・リスト

セグメント・リストは、常にプロファイル名から始まります。 その他のフィールドは、セグメントに固有のものです。名前は省略形です。 完全な名前は、セグメント詳細ウィンドウにあります。セグメントのフィールドについて詳しくは、131 ページの『セグメント・フィールド』を参照してください。

4. セグメント・リストからプロファイルを選択して、以下を行うことができます。
   - 以下のステップのいずれかを実行して、プロファイルのプロパティーを表示します。
     - メインメニューで、「**Navigate**」>「**Properties**」と選択し、プロファイルをダブルクリックします。または、
     - プロファイルを右クリックして、「**Properties**」オプションを選択します。
   - 以下のステップのいずれかを実行して、プロファイルのセグメント詳細ウィンドウを表示します。
     - メインメニューから、「**Navigate**」>「**Segments**」を選択します。または、
     - プロファイルを右クリックして、「**Segments**」オプションを選択します。
   - セグメントをプロファイルに追加します。詳しくは、129 ページの『セグメントの追加』を参照してください。

## セグメント詳細ウィンドウの使用

「**セグメント**」オプションを使用して、単一プロファイルのセグメントに関する情報を表示します。ここでは、その手順について説明します。

### このタスクについて

セグメント詳細ウィンドウには、単一プロファイルのセグメントに関するすべての情報が表示されます。このウィンドウから、プロファイルを編集することもできます。 セグメント詳細ウィンドウにアクセスするには、セグメント・リストを表示しているか、あるいはユーザー、グループ、リソース、接続ユーザー、または接続グループのテーブルを 表示している必要があります。

### 手順

セグメント詳細ウィンドウを開くには、以下のステップを実行します。

1. 編集または表示する特定のプロファイルを選択します。
2. メインメニューから、「**Navigate**」>「**Segments**」を選択します。または、
3. プロファイルを右クリックして、ポップアップ・メニューから「**Segments**」を選択します。

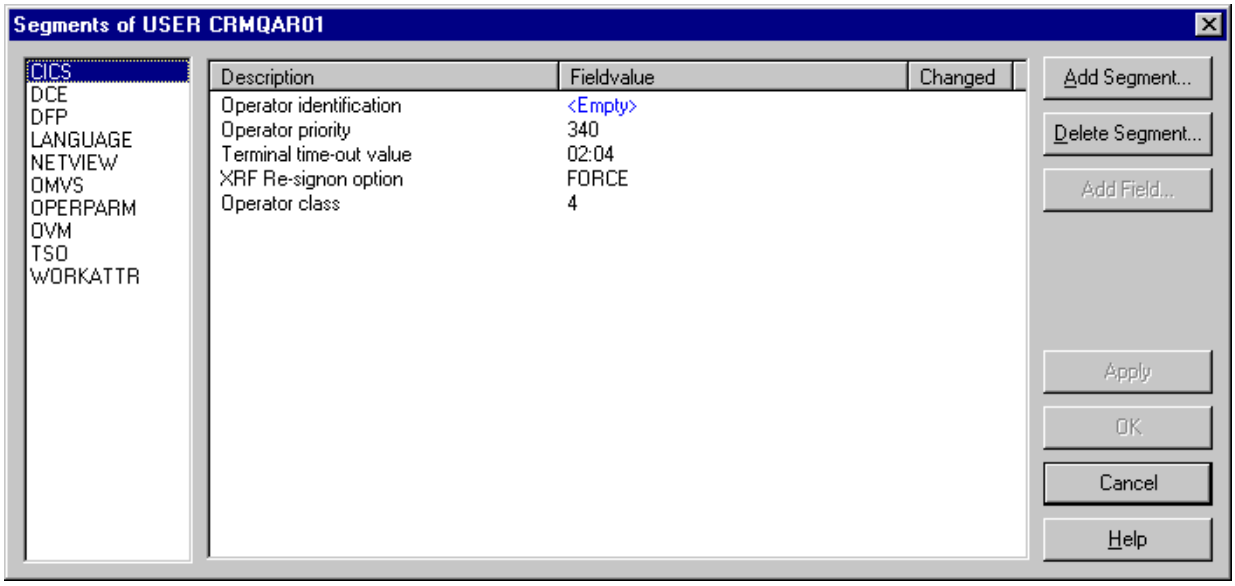



図 73. セグメント詳細ウィンドウ

セグメント詳細ウィンドウを開くと、左ペインにプロファイルのすべてのセグメントが表示されます。ここでセグメントを選択すると、右ペインに詳細情報が表示されます。 以下のように、右ペインには 3 つの列があります。

**Description**
セグメントの説明。

**Fieldvalue**
フィールドの値。この値は編集できます。空のフィールドにはすべて、この列に青色で <Empty> が表示されます。 反復フィールド・カウントがゼロの場合、フィールドがまだ存在していなくても、単一の <Empty> フィールドがここに表示されます。 これにより、ユーザーは値を入力するだけで、最初の反復フィールドを作成できます。

**Changed**
この列は、行った変更が、「**Apply**」をクリックすることでメインフレームに既に適用されているかどうかを示します。

右のボタンは、編集オプションです。

4. フィールドを編集するには、以下のステップを実行します。
   a) 以下のいずれかの方法で、変更する行を選択します。
   - 変更する行をクリックし、もう一度その行をクリックします。一時停止後、「**Fieldvalue**」フィールドが開き、編集開始できます。
   - 編集する行をタブ・キーおよび矢印キーを使って選択し、「**Ins**」キーを押して編集ダイアログを開きます。

   b) 編集をキャンセルするには、「**Esc**」キーを使用するか、別の行を選択します。
   c)「**Enter**」キーを押して変更を保存します。

編集オプションは、以下のとおりです。

**Add segment**
このボタンをクリックすると、ポップアップ・メニューの「**Add segment**」が開きます。追加するセグメントを選択できます。

**Delete segment**
削除するセグメントを選択して、このボタンをクリックします。 選択したセグメントを削除するかどうかを確認する質問が、警告ボックスに表示されます。 「**Yes**」をクリックして削除するか、「**Cancel**」をクリックして削除を取り消します。

**Add Field**
このオプションは、反復フィールドに関してのみ使用できます。新しい、空のフィールドを追加するには、追加するフィールドを選択します。「**Add Field**」ボタンが使用可能になります。このボタンをクリックして、フィールドを追加します。

**Refresh**
フィールドを変更したら、このボックスにチェックマークを入れて、フィールドをリフレッシュし、すべてのユーザーのキャッシュされているプロファイルに変更を伝搬します。 プロファイルをリフレッシュするのに適切な権限を持っている必要があります。

**Apply**
変更をメインフレームに適用するには、「**Apply**」をクリックします。「Changed」列内の表示は、変更が有効になる間、すべてが消えます。

## セグメントの追加

「**Add segment**」オプションを使用して、プロファイルにセグメントを直接追加します。

### このタスクについて

プロファイルに直接セグメントを追加したり、セグメント詳細ウィンドウからセグメントを追加したりすることができます。 セグメント詳細ウィンドウでのセグメントの追加について詳しくは、127 ページの『セグメント詳細ウィンドウの使用』を参照してください。

### 手順

プロファイルにセグメントを直接追加するには、以下のステップを実行します。

1. テーブルで、セグメントを追加するプロファイルを右クリックします。
2. メインメニューから「**Action**」>「**Add segment**」と選択するか、ポップアップ・メニューから「**Add segment**」を選択します。

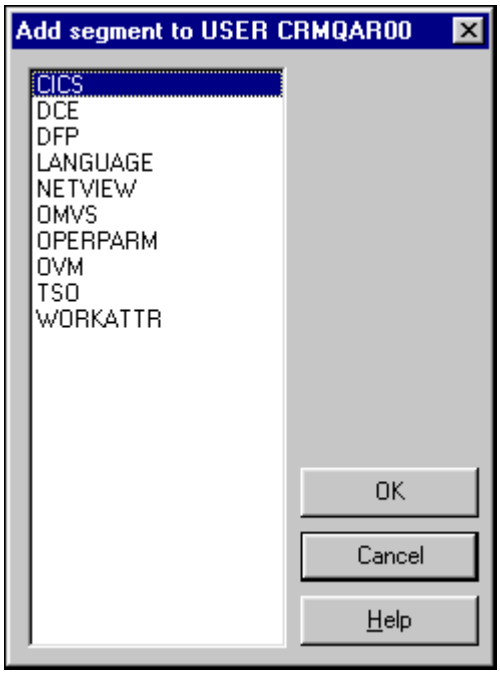



図 *74.* セグメントの追加のダイアログ

3. 追加するセグメントを選択します。次に、「**OK**」をクリックします。
4. 多重システム・モードで操作している場合は、「**Select Nodes**」ダイアログにノードの優先リストが表示されます。既にアクションを実行している場合は、以前に選択したノードが表示されます。多重システム・モードを使用している場合は、以下のステップを実行します。

a) アクションを適用するノードを指定します。処理を続行するには、少なくとも 1 つのノードを選択する必要があります。 ローカル・ノード項目が強調表示されることに注意してください。

b) ノードが zSecure ノードおよび RRSF ノードで定義されている場合は、それらのノード・タイプの 1 つのみを選択してください。RRSF ノードを選択すると、「**AT**」オプションまたは「**ONLYAT**」オプションを使用して、ドロップダウン・リストからコマンドを実行する代替ユーザー ID を選択できます。

c)「**OK**」をクリックして、選択したノードのリストを確認します。このアクションは、選択したノードごとに実行されます。

**注:**

- セグメントの追加アクションをノード全体に伝搬するには、セグメントが非常に類似する必要があります。
- 可能な場合は、セグメントはノードに追加されます。
- セグメントはノードに即時に追加されます。

## 例外

このトピックのリストを使用して、セグメント詳細ウィンドウで編集できないセグメントを判別します。

大部分のセグメントはセグメント・リストに含まれており、セグメント詳細ウィンドウで編集できます。これには、次のような例外があります。

- CSDATA セグメントは、「SegmentTypes」、「SegmentList」、および「Segment Detail」に表示されます (存在する場合のみ)。
- 「DIGTCERT-CERTDATA」は表示されますが、編集できません。
- その実行中にエラーの原因となるため、「DIGTCERT-CERTDATA-CERT」はメインフレームから読み取られません。
- 「DIGTCERT-CERTDATA-*RSV*」はメインフレームから読み取られません。これは予約フィールドであり、表示されてはなりません。
- 「DIGTCRIT」は編集できないため、「SegmentTypes」および「SegmentList」にしか表示されず、「Segment Detail」には表示されません。
- 「DIGTNMAP」は編集できないため、「SegmentTypes」および「SegmentList」にしか表示されず、「Segment Detail」には表示されません。
- 「DIGTRING」は編集できないため、「SegmentTypes」および「SegmentList」にしか表示されず、「Segment Detail」には表示されません。
- 「FACILITY PROXY-BINDPW」および「BINDPWKY」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。
- 「MFPOLICY」は表示されますが、編集できません。
- 「REALM-KERB-CURKEY」、「CURKEYV」、「ENCTYPE」、「PREVKEY」、「PREVKEYV」、および「SALT」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。
- 「PTKTDATA-SSIGNON」には暗号鍵しか含まれていないため、「SegmentTypes」にしか表示されず、「SegmentList」や「Segment Detail」には表示されません。
- 「USER-KERB-CURKEY」、「CURKEYV」、「DEFTKTLF」、 「ENCTYPE」、「MINTKTLF」、「PREVKEY」、「PREVKEYV」、「SALT」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。
- 「USER PROXY-BINDPW」および「BINDPWKY」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。
- 「USER-TSO-TCONS」、「TOPTION」、「TPERFORM」、「TRBA」、「TUPT」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。

# セグメント・フィールド

このトピックに記載されているセグメント・フィールドの説明を使用して、セグメント・タイプに関する情報を入手してください。

セグメントおよびセグメント・フィールドについて詳しくは、IBM Knowledge Center for z/OS で入手可能な資料「*z/OS Security Server RACF* マクロおよびインターフェース」のセクション『RACF データベースのテンプレート』を参照してください。

セグメント・タイプのセグメント・フィールドを表示するには、セグメント名をクリックします。 セグメント・フィールド・テーブルに、各列の説明が以下のように表示されます。

**Fieldname**
セグメント・リストに表示されるフィールド名。

**Repeats**
セグメントのフィールドが複数回表示される場合、それらはすべてセグメント詳細ウィンドウに表示されます。 セグメント・リストには、反復の回数が表示されます。

**Description**
セグメント詳細ウィンドウに表示されるフィールドの説明。

**Command parameter**

フィールドを操作する RACF コマンドのフィールドを特定するパラメーターをリストします。 この列には、このパラメーターが **Fieldname** と異なる場合にのみ値が入ります。

## リソース・プロファイルのセグメント

Visual クライアントを使用して、リソース・プロファイルの各セグメントの詳細を表示することができます。

以下のセクションには、リソース・プロファイルのセグメントがリストされています。

- 138 ページの『PTKTDATA - SSIGNON』
- 138 ページの『REALM - KERB』
- 139 ページの『ROLE - TME』
- 139 ページの『STARTED - STDATA 』
- 139 ページの『SYSMVIEW - SVFMR』

リソース・クラス内のプロファイルには、CSDATA セグメントを指定できます。

**任意のリソース・クラス - CSDATA**
CSDATA セグメントには、インストール済み環境ごとに CFIELD クラス・プロファイル *class*.CSDATA.*field* を介してクラスに定義されたカスタム・フィールドが含まれます。

**APPCLU - SESSION**
このテーブルを使用して、APPCLU- SESSION セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CONVSEC | No | Conversation security flags | |
| KEYDATE | No | Session key last change date | |
| KEYINTVL | No | Session key days to expiry # | INTERVAL |
| MAXFAIL | No | Failed tries before lockout # | |
| SENTCNT | No | Session entities in list # | |
| SENTFLCT | Yes | Failed attempts # | |
| SENTITY | Yes | Session entity name | |
| SESSKEY | No | Session key | |
| SLSFAIL | No | Invalid attempts # | |
| SLSFLAGS | No | Session flag byte | LOCK |

**CDT - CDTINFO**
動的 CDT 内でクラスを定義するには、CDT-CDTINFO セグメント・タイプのフィールドを 使用します。

CDTINFO セグメントは、CDT リソース・クラスに対してのみ有効です。このセグメントは、動的 CDT 内でクラスを定義するために使用します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CDTCASE | No | Profile names case sensitive | |
| CDTDFTRC | No | Default not-found RC | |
| CDTFIRST | No | Syntax 1st character (raw) | |
| CDTGEN | No | GENERIC/GENCMD status | |
| CDTGENL | No | GENLIST status | |
| CDTGROUP | No | Related grouping class | |
| CDTKEYQL | No | Generic scan limit (quals) | |
| CDTMAC | No | MAC checking | |
| CDTMAXLN | No | Maximum length with ENTITY | |
| CDTMAXLX | No | Maximum length | |
| CDTMEMBR | No | Related member class | |
| CDTOPER | No | OPERATIONS honored | |

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CDTOTHER | No | Syntax remainder (raw) | |
| CDTPOSIT | No | POSIT (options set id) | |
| CDTPRFAL | No | Profile definition ed | |
| CDTRACL | No | RACLIST status | |
| CDTSIGL | No | Send ENF signal | |
| CDTSLREQ | No | SECLABELs required | |
| CDTUACC | No | Default UACC | |

**CFIELD - CFDEF**
フィールドの特性を定義するには、CFIELD - CFDEF セグメント・タイプのフィールドを 使用します。

CFIELD クラス・プロファイルの CFDEF (Custom Field DEFinition) セグメントは、フィールドの特性を定義します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CFDTYPE | No | Custom field type | |
| CFFIRST | No | Custom field first char | |
| CFHELP | No | Custom field help text | |
| CFLIST | No | Custom field listing header | |
| CFMIXED | No | Custom field mixed chars | |
| CFMNVAL | No | Custom field min value | |
| CFMXLEN | No | Custom field max length | |
| CFMXVAL | No | Custom field max value | |
| CFOTHER | No | Custom field other chars | |
| CFVALRX | No | Custom field validation REXX | |

**CSFKEYS、 GCSFKEYS、 XCSFKEY、 GXCSFKEY - ICSF**
このテーブルを使用して、ICSF セグメント・タイプのフィールドを 判別します。

ICSF セグメントは、クラス CSFKEYS、GCSFKEYS、XCSFKEY、および GXCSFKEY 内の一般リソース・プロファイルによって制御されるキーの Integrated Cryptographic Service Facility ストレージ属性を定義します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CSFSEXP | No | Symmetric key export option. | SYMEXPORTABLE |
| CSFCSPW | No | Symmetric key CPACF wrap option. | SYMCPACFWRAP |
| CSFSKLCT | No | Count of PKDS labels. | |
| CSFSKLBS | Yes | PKDS labels which might be used to export this symmetric key. | SYMEXPORTKEYS |
| CSFSCLCT | No | Count of certificate labels. | |
| CSFSCLBS | Yes | Certificate labels which might be used to export this symmetric key. | SYMEXPORTCERTS |

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CSFAUSE | No | Asymmetric key usage. | ASYMUSAGE |

**DATASET - DFP**
以下の表を使用して、DFP セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| RESOWNER | No | DFP - resource owner | |

**DATASET - TME**
以下の表を使用して、TME セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| ROLEN | No | # TME role access specs | |
| ROLES | Yes | TME role access specs | |

**DIGTCERT - CERTDATA**
このテーブルを使用して、DIGTCERT - CERTDATA セグメント・タイプのフィールドを判別します。

このセグメントは編集できないため、セグメント・リストおよびセグメント・タイプにしか表示されません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CERT | No | Digital certificate | |
| CERTDFLT | Yes | Default cert for this keyring | |
| CERTEND | No | Certificate end date | |
| CERTLABL | Yes | Digital certificate labels | |
| CERTLSER | No | Certificate lse | |
| CERTNAME | Yes | Digital certificate names | |
| CERTPRVK | No | Private Key | |
| CERTPRVS | No | Private Key Size | |
| CERTPRVT | No | Private Key Type | |
| CERTSJDN | Yes | Distinguished name of Subject | |
| CERTSTRT | No | Certificate start date | |
| CERTUSAG | Yes | Certificate usage in this keyring | |
| RINGCT | No | Number of keyrings | |
| RINGNAME | Yes | Name of the keyring | |
| RINGSEQN | No | Ring sequence number | |

**DIGTRING - CERTDATA**
このテーブルを使用して、DIGTRING - CERTDATA セグメント・タイプのフィールドを判別します。

このセグメントは編集できないため、セグメント・リストおよびセグメント・タイプにしか表示されません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CERT | No | Digital certificate | |
| CERTCT | No | # Digital certificates | |

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CERTDFLT | Yes | Default cert for this keyring | |
| CERTEND | No | Certificate end date | |
| CERTLABL | Yes | Digital certificate labels | |
| CERTNAME | Yes | Digital certificate names | |
| CERTPRVK | No | Private Key | |
| CERTPRVS | No | Private Key Size | |
| CERTPRVT | No | Private Key Type | |
| CERTSJDN | Yes | Distinguished name of Subject | |
| CERTSTRT | No | Certificate start date | |
| CERTUSAG | Yes | Cert. usage in this keyring | |
| RINGCT | No | Number of keyrings | |
| RINGNAME | Yes | Name of the keyring | |
| RINGSEQN | No | Ring sequence number | |

**DLFCLASS - DLFDATA**
このテーブルを使用して、DLFCLASS - DLFDATA セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| JOBNAMES | Yes | Job names | |
| OBNMCNT | No | Job names # | |
| RETAIN | No | Retain flag byte | |

**EJBROLE - TME**
このトピックのテーブルを使用して、EJBROLE - TME セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CHILDN | No | # TME child roles | |
| CHILDREN | Yes | TME child roles | |
| GROUPN | No | #TME associated groups | |
| GROUPS | Yes | TME associated groups | |
| PARENT | No | TME parent role | |
| RESN | No | #TME resource access specs | |
| RESOURCE | Yes | TME resource access specs | |
| ROLEN | No | # TME role access specs | |
| ROLEN | Yes | TME role access specs | |

**FACILITY - DLFDATA**
このトピックのテーブルを使用して、FACILITY - DLFDATA セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| JOBNAMES | Yes | Job names | |
| JOBNMCNT | No | Job names # | |

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| RETAIN | No | Retain flag byte | |

**FACILITY - EIM**
このトピックのテーブルを使用して、FACILITY - EIM セグメント・タイプのフィールドを判別します。

Enterprise Identity Mapping (EIM) ドメインの定義。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| DOMAINDN | No | EIM Domain Distinguished Name | |
| FIELDNAME | REPEATS | Description | Command parameter |
| KERBREG | No | Kerberos registry for EIM | KERBREGISTRY |
| LOCALREG | No | Local RACF registry for EIM | LOCALREGISTRY |
| OPTIONS | No | EIM options | |
| X509REG | No | X509 registry for EIM | X509REGISTRY |

**FACILITY - PROXY**
このトピックのテーブルを使用して、FACILITY - PROXY セグメント・タイプのフィールドを判別します。

「BINDPW」および「BINDPWKY」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| LDAPHOST | No | LDAP Server URL | |
| BINDDN | No | Bind Distinguished Name | |
| BINDPW | No | Bind Password | |
| BINDPWKY | No | Bind Password Mask \| Encrypt Key | |

**FACILITY - TME**
このトピックのテーブルを使用して、FACILITY - TME セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CHILDN | No | # TME child roles | |
| CHILDREN | Yes | TME child roles | |
| GROUPN | No | # TME associated groups | |
| GROUPS | Yes | TME associated groups | |
| PARENT | No | TME parent role | |
| 2RESN | No | # TME resource access specs | |
| RESOURCE | Yes | TME resource access specs | |
| ROLEN | No | # TME role access specs | |
| ROLES | Yes | TME role access specs | |

**IDTDATA - IDTPARMS**
このトピックのテーブルを使用して、IDTDATA - IDTPARMS セグメント・タイプのフィールドを判別します。IDTPARMS セグメントは識別トークンの特定のフィールドがどのように生成されるか、および指定さ

れた識別トークンが識別トークン・タイプ、アプリケーション、ユーザー ID、および識別トークン発行者の組み合わせに照らしてどのように検証されるかを指定します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| IDTANYAP | No | 任意のアプリケーションの ID トークン | ANYAPPL |
| IDTCAT | No | 署名トークンのカテゴリー | SIGCAT |
| IDTSALG | No | ID トークン署名アルゴリズム | SIGALG |
| IDTSEQN | No | 署名トークンのシーケンス番号 | SIGSEQNUM |
| IDTTIMEO | No | ID トークンのタイムアウト (分) | IDTTIMEOUT |
| IDTTOKN | No | 署名トークン名 | SIGTOKEN |

**JESJOBS - JES**
このトピックのテーブルを使用して、JESJOBS - JES セグメント・タイプのフィールドを判別します。ジョブ入力サブシステム (JES) セグメントは JESJOBS クラスのプロファイル用であり、KEYLABEL フィールドがあります。データ・セット (パーベイシブ) 暗号化と同様に、ラベルは JES スプール・データの暗号化時に使用する ICSF 暗号鍵を示します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| KEYLABEL | No | ICSF のデータ鍵ラベル | |

**LDAPBIND - EIM**
このテーブルを使用して、LDAPBIND - EIM セグメント・タイプのフィールドを判別します。

Enterprise Identity Mapping (EIM) ドメインの定義。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| DOMAINDN | No | EIM Domain Distinguished Name | |
| OPTIONS | No | EIM options | |

**LDAPBIND - ICTX**
このテーブルを使用して、LDAPBIND - ICTX セグメント・タイプのフィールドを判別します。

LDAPBIND クラスの ICTX セグメントには、リモート・リソース管理に関する情報が格納されます。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| USEMAP | No | USEMAP | |
| DOMAP | No | DOMAP | |
| MAPREQ | No | MAPREQUIRED | |
| MAPTIMEO | No | MAPPINGTIMEOUT | |

**LDAPBIND - PROXY**
このテーブルを使用して、LDAPBIND - PROXY セグメント・タイプのフィールドを判別します。

PR0XY セグメントは、LDAP プロキシー・サーバー情報を保管するために使用します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| BINDDN | No | Bind information for LDAP server being contacted | |
| LDAPHOST | No | Host of LDAP server to contact | |

**MFADEF - MFPOLICY**
このテーブルを使用して、MFADEF - MFPOLICY セグメント・タイプのフィールドを判別します。

MFPOLICY セグメントは、MFADEF 情報を格納するために使用します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| MFFCTRN | No | MFA 要素の数 | |
| MFREUSE | No | 再使用可能な MFA トークン | |
| MFTIMEO | No | MFA トークンのタイムアウト (秒) | |
| MFFCTRS | No | MFA 要素名 | |

**PROGRAM - SIGVER**
このテーブルを使用して、PROGRAM - SIGVER セグメント・タイプのフィールドを判別します。

PROGRAM クラス・プロファイルの SIGVER (SIGnature VERification) セグメントには、プログラム・モジュールのデジタル署名を検査するために使用されるフィールドが含まれています。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| SIGREQD | No | Module must have a signature. | SIGREQUIRED |
| FAILLOAD | No | Loader failure conditions | |
| SIGAUDIT | No | RACF audit condition | |

**PTKTDATA - SSIGNON**
このテーブルを使用して、PTKTDATA - SSIGNON セグメント・タイプのフィールドを判別します。

「PTKTDATA - SSIGNON」には暗号鍵しか含まれていないため、「SegmentTypes」にしか表示されず、「SegmentList」や「Segment Detail」には表示されません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| SSKEY | No | Single Signon key | |

**REALM - KERB**
このテーブルを使用して、REALM - KERB セグメント・タイプのフィールドを判別します。

「REALM - KERB/CURKEY」、「CURKEYV」、「ENCTYPE」、「PREVKEY」、「PREVKEYV」、「SALT」は読み取り専用フィールドで あるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CURKEY | No | Current Kerberos key | |
| CURKEYV | No | Current Kerb key version | |
| DEFTKTLF | No | Default ticket life | |
| ENCTYPE | No | Kerberos encryption type | |
| ENCRYPT | No | ed encryption types | |
| KERBNAME | No | Kerberos name | |
| MAXTKTLF | No | Maximum ticket life | MAXTKTLFE |
| MINTKTLF | No | Minimum ticket life | MINTKTLFE |
| PREVKEY | No | Previous Kerberos key | |
| PREVKEYV | No | Previous Kerb key version | |
| SALT | No | Seed for Kerberos Randomizer | |

**ROLE - TME**
このテーブルを使用して、ROLE - TME セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CHILDN | No | # TME child roles | |
| CHILDREN | Yes | TME child roles | |
| GROUPN | No | # TME associated groups | |
| GROUPS | Yes | TME associated groups | |
| PARENT | No | TME parent role | |
| 2RESN | No | # TME resource access specs | |
| RESOURCE | Yes | TME resource access specs | |
| ROLEN | No | # TME role access specs | |
| ROLES | Yes | TME role access specs | |

**STARTED - STDATA**
このテーブルを使用して、STARTED - STDATA セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| FLAGPRIV | No | Privileged - any, nolog | PRIVILEGED |
| FLAGTRAC | No | Trace - issue IRR812I | TRACE |
| FLAGTRUS | No | Trusted - any, log all | TRUSTED |
| STGROUP | No | Started task RACF group | GROUP |
| STUSER | No | Started task RACF user ID | USER |

**SYSMVIEW - SVFMR**
このテーブルを使用して、SYSMVIEW - SVFMR セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| PARMN | No | SVFMR parameter list | PARMNAME |
| SCRIPTN | No | Default logon scripts | SCRIPTNAME |

## グループ・プロファイルのセグメント

このトピックに示すフィールドの説明を使用して、グループ・プロファイルの各セグメントの詳細を判別します。

このセクションでは、グループ・セグメント・タイプのフィールドについて 説明します。


- 139 ページの『GROUP - CSDATA』
- 140 ページの『GROUP - DFP』
- 140 ページの『GROUP - OMVS 』
- 140 ページの『GROUP - OVM 』
- 140 ページの『GROUP - TME』


**GROUP - CSDATA**
GROUP プロファイルの CSDATA セグメントには、そのプロファイルのカスタム・フィールドが追加されます。

RACF CFIELD クラスを使用して、新しいフィールドを GROUP プロファイルに定義し、新しいフィールドに使用するラベルを定義して、フィールドを追加することができます。 このセグメントのフィールドは、インストール定義フィールドです。

**GROUP - DFP**
このトピックのテーブルを使用して、GROUP - DFP セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| DATAAPPL | No | DFP - Data Application | |
| DATACLAS | No | DFP - Data Class | |
| MGMTCLAS | No | MDFP - Management Class | |
| STORCLAS | No | DFP - Storage Class | |

**GROUP - OMVS**
このトピックのテーブルを使用して、GROUP - OMVS セグメント・タイプのフィールドを判別します。

OMVS セグメントは z/OS UNIX Security コンテキストを提供します。これは、z/OS UNIX にログオンするときに必要です。OMVS は OpenMVS を表し、z/OS UNIX システム・サービスの旧称です。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| GID | No | z/OS UNIX group (grpid) | GID |

**GID**
OMVS グループ ID。未使用の値がシステムによって割り当てられるようにするには、「auto」を使用します。複数のグループが GID を共有するようにするには、GID 値の最後に「s」を加えます。

**GROUP - OVM**
このトピックのテーブルを使用して、GROUP - OVM セグメント・タイプのフィールドを判別します。

OVM セグメントは、UNIX システム・サービス情報を保管するために使用します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| GID | No | UNIX group (gid) | |

**GROUP - TME**
このトピックのテーブルを使用して、GROUP - TME セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| ROLEN | No | # TME role access specs | |
| ROLES | Yes | TME role access specs | |

## ユーザー・プロファイルのセグメント

以下に示すフィールドの説明を使用して、ユーザー・プロファイルの各セグメントの詳細を判別します。

このセクションでは、ユーザー・セグメント・タイプのフィールドについて 説明します。


- 141 ページの『USER - CICS』
- 141 ページの『USER - CSDATA 』
- 141 ページの『USER - DCE 』
- 141 ページの『USER - DFP 』
- 142 ページの『USER - EIM 』
- 142 ページの『USER - KERB』
- 142 ページの『USER - LANGUAGE 』
- 142 ページの『USER - LNOTES 』
- 143 ページの『USER - NDS 』
- 143 ページの『USER - NETVIEW 』

**USER - CICS**
このテーブルを使用して、USER - CICS セグメント・タイプのフィールドを判別します。

CICS セグメントは、CICS、オンライン・トランザクション処理システムに関する情報を表示します。 CICS は、大規模なコンピューターまたは端末ネットワークからの膨大なデータ・トランザクションを処理するために使用します。このトピックには、セグメントのフィールドが記載されています。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| OPCLASS | Yes | Operator class | |
| OPCLASSN | No | Operator class values # | |
| OPIDENT | No | Operator identification | |
| OPPRTY | No | Operator priority | |
| TIMEOUT | No | Terminal time-out value | |
| XRFSOFF | No | XRF Re-signon option | |

**USER - CSDATA**
USER プロファイルの CSDATA セグメントには、そのプロファイルのカスタム・フィールドが追加されます。

RACF CFIELD クラスを使用して、新しいフィールドを USER プロファイルに定義し、新しいフィールドに使用するラベルを定義して、フィールドを追加することができます。 このセグメントのフィールドは、インストール定義フィールドです。

**USER - DCE**
このテーブルを使用して、USER - DCE セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| DCEENCRY | No | DCE password encr. key no. | |
| DCEFLAGS | No | DCE Autologin | AUTOLOGIN |
| DCENAME | No | DCE username | |
| DPASSWDS | No | DCE password | |
| HOMECELL | No | DCE homecell | |
| HOMEUUID | No | DCE homecell UUID | |
| UUID | No | DCE UUID | |

**USER - DFP**
このテーブルを使用して、USER - DFP セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| DATAAPPL | No | DFP - Data Application | |
| DATACLAS | No | DFP - Data Class | |
| MGMTCLAS | No | DFP - Management Class | |

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| STORCLAS | No | DFP - Storage Class | |

**USER - EIM**
このテーブルを使用して、USER - EIM セグメント・タイプのフィールドを判別します。

LDAPBIND クラス・プロファイルの名前を保管するセグメント。このプロファイルには、EIM がある LDAP ホスト上の EIM ドメインに接続するために必要な情報が含まれています。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| LDAPPROF | No | LDAP Profile | |

**USER - KERB**
このテーブルを使用して、USER - KERB セグメント・タイプのフィールドを判別します。

「USER - KERB/CURKEY」、「CURKEYV」、「DEFTKTLF」、「 ENCTYPE」、「MINTKTLF」、「PREVKEY」、「PREVKEYV」、「SALT」は読み取り専用フィールドであるため、「SegmentList」にのみ表示され、「Segment Detail」には表示されません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CURKEY | No | Current® Kerberos key | |
| CURKEYV | No | Current Kerb key version | |
| DEFTKTLF | No | Default ticket life | DEFTKTLFE |
| ENCTYPE | No | Kerberos encryption type | |
| ENCRYPT | No | ed encryption types | |
| KERBNAME | No | Kerberos name | |
| MAXTKTLF | No | Maximum ticket life | MAXTKTLFE |
| MINTKTLF | No | Minimum ticket life | MINTKTLFE |
| PREVKEY | No | Previous Kerberos key | |
| PREVKEYV | No | Previous Kerb key version | |
| SALT | No | Seed for Kerberos Randomizer | |

**USER - LANGUAGE**
このテーブルを使用して、USER - LANGUAGE セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| USERNL1 | No | Primary language of a user | PRIMARY |
| USERNL2 | No | Secondary language of a user | SECONDARY |

**USER - LNOTES**
このテーブルを使用して、USER - LNOTES セグメント・タイプのフィールドを判別します。LNOTES は IBM Notes を表します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| SNAME | No | IBM Notes 短縮ユーザー名 | |

**USER - NDS**
このテーブルを使用して、USER - NDS セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| UNAME | No | NDS username | |

**USER - NETVIEW**
このテーブルを使用して、USER - NETVIEW セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| CONSNAME | No | Default console name | |
| CTL | No | Scope of control | |
| DOMAINS | Yes | Cross-domain authority | DOMAINS |
| DOMAINSN | No | # cross-domain authorities | |
| IC | No | Initial command list | |
| MSGRECVR | No | Receive undelivered messages | |
| NETVIEW | No | Admin auth Graphic Mon Fac | NGMFADMN |
| NGMFVSPN | No | View span opts Graph.Mon.Fac. | |
| OPCLASS | Yes | Operator class | |
| OPCLASSN | No | Operator class values # | |

**USER - OMVS**
このテーブルを使用して、USER - OMVS セグメント・タイプのフィールドを判別します。

OMVS セグメントは z/OS UNIX Security コンテキストを提供します。これは、z/OS UNIX にログオンするときに必要です。OMVS は OpenMVS を表し、z/OS UNIX システム・サービスの旧称です。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| ASSIZE | No | Max. address space size | ASSIZEMAX |
| CPUTIME | No | Maximum CPU time | CPUTIMEMAX |
| FILEPROC | No | Max. files open per proc | FILEPROCMAX |
| HOME | No | z/OS UNIX home path | |
| MMAPAREA | No | Max. data space for mapping | MMAPAREAMAX |
| PROCUSER | No | Max. nr. of active procs | PROCUSERMAX |
| PROGRAM | No | Conditional access program | |
| THREADS | No | Max. nr. of active threads | THREADSMAX |
| UID | No | z/OS UNIX user (uid) | |

**UID**
ユーザー ID 付きの z/OS UNIX UID フィールド。未使用の値がシステムによって割り当てられるようにするには、「auto」を入力します。この UID を複数のユーザーで共有する場合は、UID 値の最後に「s」を加えます。

**USER - OPERPARM**
このテーブルを使用して、USER - OPERPARM セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| OPERALTG | No | Alternate console group | ALTGRP |

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| OPERAUTH | No | Console authority | AUTH |
| OPERAUTO | No | Receive msgs automated by MPF | AUTO |
| OPERCMDS | No | System to send commands to | CMDSYS |
| OPERDOM | No | Delete operator messages type | OM |
| OPERKEY | No | KEY keyword of D,CONSOLES,KEY | KEY |
| OPERLEVL | No | LEVEL of msgs to be received | LEVEL |
| OPERLOGC | No | Command response logging | LOGCMDRESP |
| OPERMCNT | No | MSCOPE systems # | |
| OPERMFRM | No | Message format | MFORM |
| OPERMGID | No | Migration id to be assigned | MIGID |
| OPERMON | No | Events to be monitored | MONITOR |
| OPERMSCP | Yes | MSCOPE systems | MSCOPE |
| OPERROUT | No | ROUTCODEs for msg reception | ROUTCODE |
| OPERSTOR | No | STORAGE in MB for msg queuing | STORAGE |
| OPERUD | No | Receive undelivered messages | UD |

**USER - OVM**

このテーブルを使用して、USER - OVM セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| FSROOT | No | OpenVM file system root | |
| HOME | No | z/OS UNIX home path | |
| ROGRAM | No | Conditional access program | |
| UID | No | z/OS UNIX user (uid) | |

**USER - PROXY**

このテーブルを使用して、USER - PROXY セグメント・タイプのフィールドを判別します。

「BINDPW」および「BINDPWKY」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| LDAPHOST | No | LDAP Server URL | |
| BINDDN | No | Bind Distinguished Name | |
| BINDPW | No | Bind Password | |
| BINDPWKY | No | Bind Password Mask \| Encrypt Key | |

**USER - TSO**
このテーブルを使用して、USER - TSO セグメント・タイプのフィールドを判別します。

TSO は、タイム・シェアリング・オプション (Time Sharing Option) の略語であり、行コマンド (メインフレームの DOS プロンプトに相当) を入力して MVS™ と通信するための特定の方法です。TSO セグメントには、MVS へのログオン方法に関する情報が含まれています。

「USER - TSO/TCONS」、「TOPTION」、「TPERFORM」、「TRBA」、「TUPT」は読み取り専用フィールドであるため、「SegmentList」にしか存在せず、「Segment Detail」には存在しません。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| TACCNT | No | Default account number | ACCTNUM |
| TCOMMAND | No | Default command | COMMAND |
| TCONS | No | Consoles support | |
| TDEST | No | Destination identifier | DEST |
| THCLASS | No | Default held sysout class | HOLDCLASS |
| TJCLASS | No | Default job class | JOBCLASS |
| TLPROC | No | Default logon procedure | PROC |
| TLSIZE | No | Default logon region size(KB) | SIZE |
| TMCLASS | No | Default message class | SGCLASS |
| TMSIZE | No | Maximum region size | MAXSIZE |
| TOPTION | No | Mail/Notice/Recon/OID options | |
| TPERFORM | No | Performance group | |
| TRBA | No | RBA of user broadcast area | |
| TSCLASS | No | Default sysout class | SYSOUTCLASS |
| TSOSLABL | No | Default logon SECLABEL | SECLABEL |
| TUDATA | No | Site data TSO user (2 byte) | USERDATA |
| TUNIT | No | Default unit name | UNIT |
| TUPT | No | UPT control block data | |

**USER - WORKATTR**
このテーブルを使用して、USER - WORKATTR セグメント・タイプのフィールドを判別します。

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| WAACCNT | No | Account number | |
| WAADDR1 | No | SYSOUT address line 1 | |
| WAADDR2 | No | SYSOUT address line 2 | |
| WAADDR3 | No | SYSOUT address line 3 | |
| WAADDR4 | No | SYSOUT address line 4 | |
| WABLDG | No | Building for delivery | |
| WADEPT | No | Department for delivery | |
| WAEMAIL | No | User's fully qualified email address | |
| WANAME | No | User name for SYSOUT | |

| Fieldname | Repeats | Description | Command parameter |
|---|---|---|---|
| WAROOM | No | Room for delivery | |

# 第 9 章 REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

サイト定義 REXX スクリプトにアクセスするように Visual サーバーが構成されている場合は、Visual クライアントを使用して REXX スクリプトを選択および実行できます。詳しくは、以下のトピックを参照してください。

**関連概念**

IBM Security zSecure Visual のセットアップと構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

**関連情報**

RACF データベースでの操作

Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理

IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

147 ページの『Visual サーバーで REXX スクリプトを実行するための前提条件』

サイト定義 REXX スクリプトを Visual クライアントから実行できるようにするには、Visual サーバーで関連付けファイルを作成する必要があります。

148 ページの『Visual クライアントでの REXX スクリプトの実行』

Visual クライアント・インターフェースを 使用して、Visual サーバーで構成されている REXX スクリプトを実行します。このセクションでは、その手順について説明します。

## Visual サーバーで REXX スクリプトを実行するための前提条件

サイト定義 REXX スクリプトを Visual クライアントから実行できるようにするには、Visual サーバーで関連付けファイルを作成する必要があります。

「インストールおよびデプロイメント・ガイド」の『サイト定義の REXX スクリプト』の説明に従って、サイト固有の REXX スクリプトの関連付けファイルを構成します。これにより、Visual クライアントを使用して、ローカル・サーバー・ノードで REXX スクリプトを選択して実行できるようになります。リモート・ノードからの REXX スクリプトの実行はサポートされていません。

スクリプトは、このような関連付けファイルがサーバーで定義されている場合にのみ表示されます。関連付けファイルがサーバーで定義されていない場合、REXX スクリプトが定義されていないことを示すメッセージがクライアントで表示されることはありません。

## Visual クライアントでの REXX スクリプトの実行

Visual クライアント・インターフェースを 使用して、Visual サーバーで構成されている REXX スクリプトを実行します。このセクションでは、その手順について説明します。

### 始める前に

Visual クライアントを使用してスクリプトを実行できるようにするには、Visual サーバー上で REXX スクリプトが定義されている必要があります。147 ページの『Visual サーバーで REXX スクリプトを実行するための前提条件』を参照してください。

**注 :** Visual クライアントでは、スクリプトの実際の名前ではなく、スクリプトに対して構成された説明が表示されます。

### 手順

Visual クライアントで REXX スクリプトを実行するには、以下のいずれかの方法を使用します。

- REXX スクリプトの実行対象クラスに属するプロファイルを右クリックします。例えば、「**Navigate**」、「**Find**」、および「**Class:**」のユーザーを使用します。プロファイルを右クリックすると、使用可能なアクションのリスト、ナビゲーション・オプション、および Visual サーバー上で定義されている REXX スクリプトの説明が表示されます。スクリプトを実行するには、説明をクリックします。

  このオプションは、Visual サーバー上で REXX スクリプトが定義されているすべてのクラス (ユーザー、グループ、データ・セット、または XFACILIT などの特定のクラス) に対して使用できます。
- クライアントのメイン・ウィンドウで「**Navigate**」を選択して、使用可能な REXX スクリプトの説明のリストを表示します。次に、リストされた説明をクリックして、スクリプトを実行します。

  このオプションは、クラス「ユーザー」に対して実行されるように定義されているスクリプトについてのみ使用可能です。

# 第 10 章 クライアント定義の管理

以下の情報を参照して、Visual サーバーと Visual クライアント間の通信に必要なクライアント定義を管理することができます。

サーバーにアクセスするには、zSecure Visual クライアントにローカル・サーバー定義とサーバー上に対応するクライアント定義が必要です。 これらの定義を使用して、安全な通信チャネルが作成されます。 以前使用されていない新規のチャネルをセットアップするには、初期パスワードが一度必要です。 クライアント定義はサーバー定義より多くの情報を含み、それ以外は両者はほぼ同じです。

メインフレームは、クライアント定義の管理に制限付きサポートを提供します。 詳しくは、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」でサーバーの zSecure Visual クライアントの構成に関するセクションを参照してください。

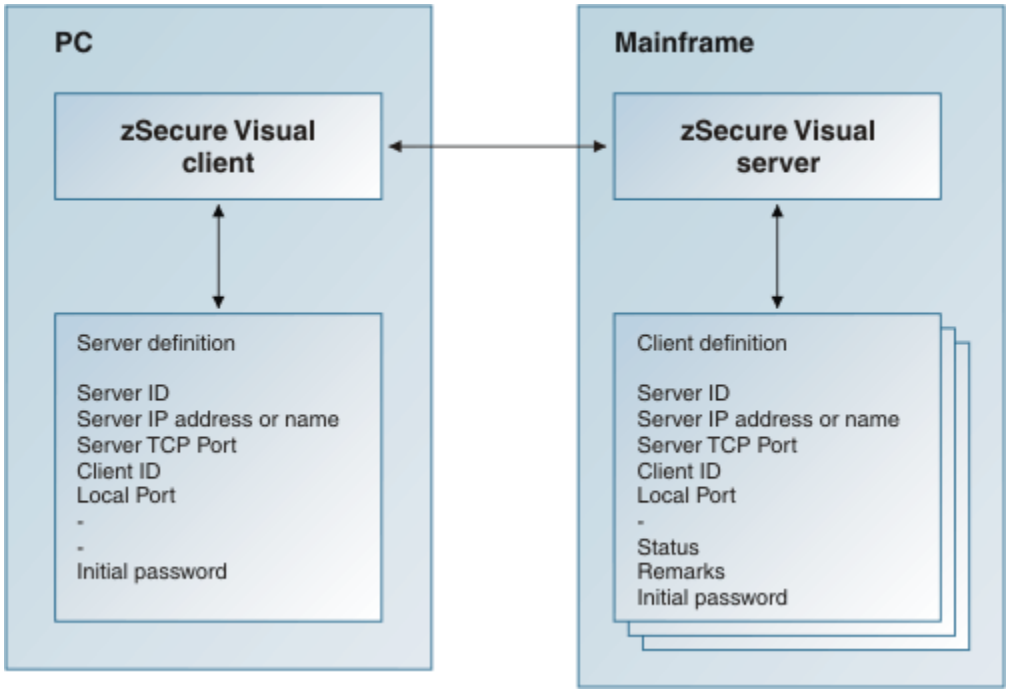



図 75. サーバーとクライアント間の通信に必要なサーバー定義とクライアント定義

**関連概念**

IBM Security zSecure Visual のセットアップと構成

IBM Security zSecure Visual のカスタマイズ・タスクと基本タスク

ユーザー管理

IBM Security zSecure Visual のユーザー管理タスクでは、ユーザー・テーブルおよびユーザー・プロパティーの表示、ユーザーの削除/複写/再開、パスワードの設定、スケジュールの使用などを行います。これらのタスクは、以下のトピックで説明します。

接続の管理

Visual クライアントで接続管理タスクを実行することで、ユーザーとグループの間の接続の関連付けを設定および保守します。

リソース管理

管理者は、zSecure のリソース管理タスクを実行して、さまざまなユーザーおよびグループが保持している、リソースに対するアクセス規則の保守を行います。

セグメントの管理

Visual クライアントを使用すると、ユーザー、グループ、およびリソースの zSecure セグメント管理タスクを実行できます。

REXX スクリプトの実行

zSecure Visual をカスタマイズして、サイト定義 REXX スクリプトを実行できるようにすることができます。

**関連情報**

RACF データベースでの操作
Visual クライアントの「**Navigate**」オプションを使用すると、ユーザー、グループ、およびリソースとそれらの接続、許可、およびスケジュールを検索および表示できます。

グループ管理
IBM Security zSecure Visual を使用すると、グループの表示、追加、複写、および削除を実行できます。これらのタスクは、以下のトピックで説明します。

## クライアント定義の保守

保守タスクにより、zSecure Visual のクライアント定義の作成、編集、および削除を行うことができます。

**このタスクについて**

「Maintain Client」ウィンドウでは、以下のアクションを実行できます。

- クライアント定義の作成
- 既存のクライアント定義の編集または削除
- 初期パスワードの生成

**手順**

- 「Maintain Client」ウィンドウを開くには、メインメニューから 「**Maintenance**」>「**Client**」の順に選択します。
  「Maintain Client」ウィンドウには、zSecure Visual サーバーのインスタンスの既存のクライアント定義がすべてリストされます。

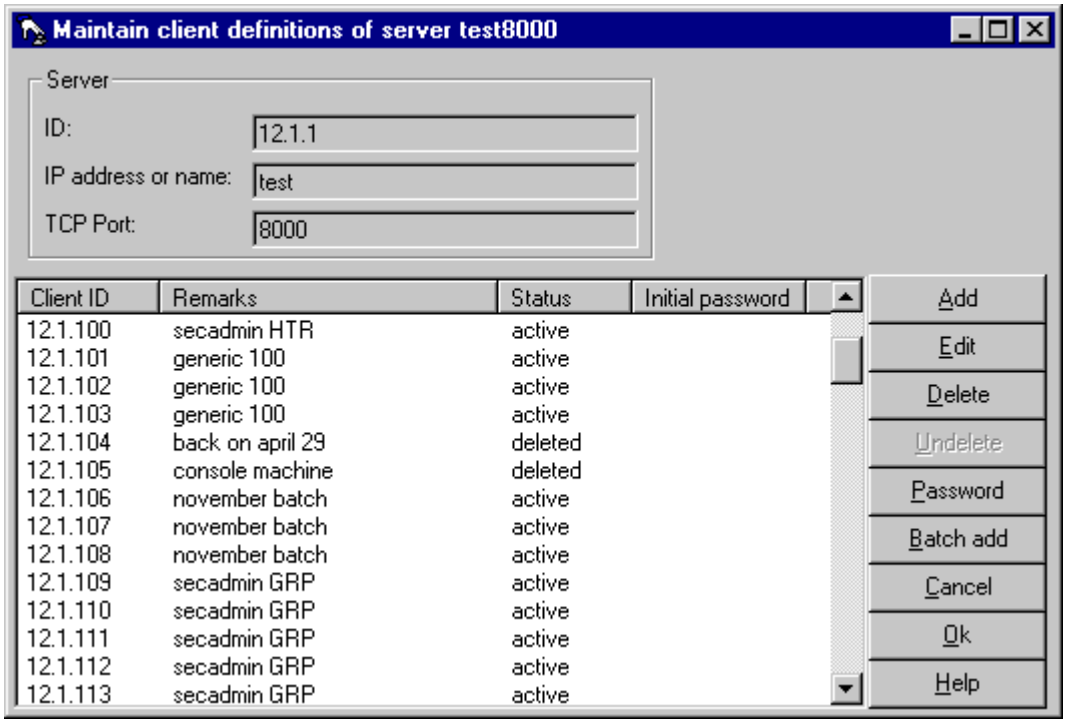



図 76. 「*Maintain Client*」ウィンドウ

クライアント・フィールドは以下のとおりです。

**クライアント ID**
オプション。サーバーで固有である必要があります。空のままにすると、サーバーが代わりに ID を作成します。 このフィールドは、サーバー上で「**Agent ID**」とも呼ばれます。

**Remarks**
オプション。クライアント定義の注釈を保管します。

**Status**
読み取り専用です。クライアントが削除されているかアクティブであるかを示します。削除されているクライアント定義を使用してログオンすることはできません。

**初期パスワード**
読み取り専用です。新規クライアントの通信を開始するために必要です。 これはサーバーによって生成されます。有効期間は、7 日間またはサーバー実行期間の長さのうち、先に終了する方に制限されます。

**注 :** 初期パスワードが表示されるのは、生成後で、かつウィンドウが開いている間のみに限られます。 新たに作成されたクライアント定義には、自動的に初期パスワードが割り当てられます。

サーバー属性 (「**Server ID**」、「**IP address or name**」、「**TCP Port**」) は、このウィンドウの上部に表示されます。 サーバー・フィールドおよびクライアントでのサーバー 定義の作成について詳しくは、8 ページの『サーバー定義パラメーター』を参照してください。

- 1 つの定義を追加する場合は「**Add**」ボタンを選択します。
- 1 つの定義を編集する場合は「**Edit**」ボタンを選択します。
- 1 つ以上の定義を削除する場合は、削除する項目を選択して「**Delete**」をクリックします。
- 削除された定義を活動化するには、「**Undelete**」ボタンを使用します。
- 新規パスワードを 1 つ以上生成する場合は、定義を選択して「**Initial password**」をクリックします。

## 複数のクライアント定義を追加するためのバッチ・モード

「**Batch add**」ダイアログを使用して、zSecure Visual の複数のクライアント定義をバッチ実行で作成します。

「**Batch Add**」ダイアログを使用すると、1 回のアクションで複数のクライアント定義を作成できます。

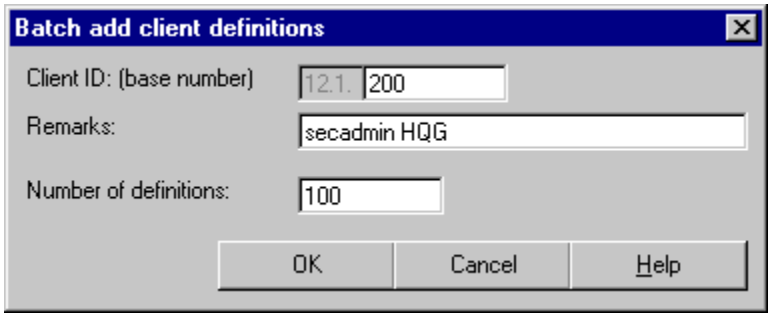



図 77. 「*Batch add client definitions*」ダイアログ

以下のフィールドが表示されます。

**Client ID base number**
オプション。クライアント ID の生成時に開始する値を指定します。

**Remarks**
オプション。ID のバッチの目的を識別するテキストです。

**Number of definitions**
生成するクライアント ID の総数を指定します。100 個までの値を指定できます。

バッチ実行が終了すると、「**Maintain Client**」ウィンドウに、新規項目が初期パスワードを伴って表示されます。 150 ページの図 76 を参照してください。

## クライアント定義属性

以下の属性を指定して、zSecure Visual 内で対応するサーバー定義を作成します。

クライアント定義の作成後、そのクライアントについて以下の属性を指定する必要があります。

- サーバーの IP アドレスまたは名前
- サーバーの TCP ポート番号
- クライアント ID
- 初期パスワード

上記の属性は、対応するサーバー定義の作成に使用されます。 クライアント定義とサーバー定義により、クライアントからサーバーへのログオンが可能になります。 詳しくは、8 ページの『サーバー定義パラメーター』 を参照してください。

## クリップボードへのクライアント定義のコピー

以下のクライアントのコピー手順に従って、特定の Visual クライアント定義を選択し、ユーザーに配布してください。

### このタスクについて

「**Maintain Client**」ウィンドウで、クライアント ID と初期パスワードを選択し、これをクリップボードにコピーして、ユーザーにメールで送信することができます。

### 手順

クライアント定義をクリップボードにコピーするには、以下のステップを実行します。

1. 「**Maintain Client**」ウィンドウを開きます。
2. 配布に必要なクライアント定義と初期パスワードを生成します。
3. 配布するクライアント定義を選択します。
4. 選択した定義をクリップボードにコピーします。サーバー属性はヘッダーとして上部に追加されます。クライアント情報はタブ付きの列で配列されます。列間隔を保ったままスプレッドシートに貼り付けることも、E メールで送信することもできます。E メールのレイアウトでは、均等なスペースのタブ桁揃えは保持されません。

   クリップボードの例:

```
Server
IP address or name:     test
TCP Port:       8000

Client ID       Remarks Status  Initial password
12.1.100        secadmin HTR    active  63F693FF96
12.1.101        generic 100     active  99F239EF6F
12.1.102        generic 100     active  01E671F0A6
```

# 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。

# 用語集

**CKG プロファイル (CKG profile)**
XFACILIT クラス内のいくつかのプロファイルによって、CKGRACF コマンドへのアクセスが制御される。プロファイル名は「CKG 」で始まる。**注:** Site Module 一般リソース・クラス名がサーバー・セットアップ時にカスタマイズされた場合 (「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照)、XFACILIT クラスではなく、指定された名前を持つクラスによって、CKGRACF コマンドへのアクセスが制御されます。

**アクセス権限 (Access authority)**
ユーザーが保護リソースにアクセスするために必要とする権限。権限が高いほど、ユーザーが実行できるアクションは多くなる。

**クラス (Class)**
ユーザーやリソースなどのすべての RACF エンティティーがクラスにカテゴリー 化される。クラス記述子テーブルには、USER、GROUP、および DATASET を除くすべてのクラスの記述が入っている。

**クラス記述子テーブル (Class Descriptor Table)**
すべての一般リソース・クラスの項目が含まれている、アセンブル済みの RACF テーブル。

**CKGRACF**
権限に依存する RACF コマンドを実行するユーティリティーの 短縮メインフレーム・プログラム名。IBM Security zSecure のコンポーネント。

**CKRCARLA**
IBM Security zSecure アプリケーションの短いメインフレーム・プログラム名。

**接続 (Connect)**
ユーザーをグループに接続するプロファイル。接続の属性に応じて、ユーザーに与えられる許可は異なる。

**一般リソース (General Resource)**
RACF で保護できる、ユーザー、グループ、およびデータ・セット以外の対象。例えば、CKG プロファイルは、デフォルトで一般リソース・クラスである XFACILIT クラスに存在する。

**グローバル・アクセス・テーブル (GAT) (Global Access Table (GAT))**
制限ユーザーを除くすべてのユーザーに、リソースのリストへのアクセスを手早く許可する手段。RACF 権限処理の大部分がバイパスされる。このリストは、GLOBAL クラスの DATASET プロファイル内に保管される。

**HLQ**
高位修飾子または最初の修飾子。データ・セット名の一番左の部分。最初のピリオドの前の文字ストリング。

**ID**
ユーザー ID またはグループ名。

**メンバー (Member)**
プロファイル・メンバーは、プロファイルに関連する項目のリストを作成するために使用される。

**MVS**
メインフレーム・オペレーティング・システム。

**所有者 (Owner)**
すべてのプロファイルには所有者が存在する。プロファイルを所有するユーザーまたはグループは、そのプロファイルを表示、変更、および削除することができる。

**許可 (Permit)**
指定のリソースに対してユーザーまたはグループに与えられる許可されたアクセス能力。

**プロファイル (Profile)**
1 つ以上のユーザー、グループ、またはリソースのセキュリティー関連特性の記述。プロファイルは複数のセグメントに分かれている。

**Proftype**
プロファイル・タイプ。一般リソースの場合、discrete または generic にすることができます。 データ・セットの場合、generic、nonvsam、vsam、tapedsn、または model にすることができます。

**RACF**
リソース・アクセス管理機能。MVS または VM 環境で、ユーザー ID 別、アクセス許可別などのアクセス制御を実現するセキュリティー・プログラム。SecureWay Security Server に名前が変更された。

**RRSF**
RACF リモート共有機能。IBM RRSF により、RACF を使用する他の IBM z/OS システムと RACF 間で通信を行うことができます。これにより、リモートの RACF データベースを保守できるようになります。RRSF ノードは、MVS システム・イメージです。つまり、RRSF ノードは、RACF データベースを共有する MVS システム・イメージのグループです。

**スケジュール (Schedule)**
スケジュールを使用して、取り消しインターバルなどの時刻指定コマンドを設定して実行することができる。例えば管理者は、ユーザーが休暇を取る期間に対して今後のインターバルを定義することができる。指定された休暇の開始日になると、ユーザーは自動的に取り消される。指定された期間が終了すると、ユーザーはシステムによって再開される。

**セグメント (Segment)**
識別情報の特定の部分が含まれているプロファイルの一部。

**Setropts**
リソース保護に関連するシステム規模の z/OS オプションを設定するためのコマンド (Set RACF Options)。

**Setropts erase**
RACF コマンド。

**サブグループ (Subgroup)**
グループは、その上位グループであるグループのサブグループとなる 。

**上位グループ (Supgroup)**
SYS1 を除くすべてのグループには、1 つの上位グループがある。こうして作成される階層は、アクセス権限が付与される方法において重要な役割を果たす。

**汎用アクセス権限 (UACC) (Universal Access Authority (UACC))**
ユーザーまたはグループに明示的アクセス権限が付与されない場合に付与されるデフォルトのアクセス権限を定義する、データ・セットまたはリソース・プロファイルの一部 (制限ユーザーを除く。これらのユーザーは UACC を通じたアクセス権限は持たない)。機密上重要なリソースに対しては、通常 UACC が NONE に設定される。

**ユーザー ID (Userid)**
ユーザー ID。RACF ユーザーの固有の ID。

**z/OS**
MVS をコンポーネントとして含むメインフレーム・オペレーティング・システム。

# 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

## [ア行]



## [カ行]

## [サ行]

## [タ行]

## [ナ行]



## [ハ行]

## [マ行]

## ［ヤ行］



## ［ラ行］

## A

## C



## D



## E

## F



## G



## H



## I



## J

## K



## L



## M



## N



## O



## P

## R



## S

## T



## U

## V



## W



## X



## Z



## [特殊文字]

部品番号:

(1P) P/N:

SA88-7157-06