Sun™ Mainframe Security Facility 管理者ガイド

リリース 1.1.0

Sun Microsystems, Inc.
www.sun.com

Part No. 819-2359-10
2005 年 6 月, Revision A

コメントの送付: http://www.sun.com/hwdocs/feedback

原典: *Sun™ Mainframe Security Facility Administrator's Guide*
Part No: 817-7448-10
Revision A

目次

図目次

表目次

コード例

はじめに

このマニュアルでは、Sun™ Mainframe Security Facility (Sun MSF) をインストール、設定、および管理する方法について説明します。

お読みになる前に

このマニュアルに記載された情報を最大限に活用するには、次の内容を十分に理解しておく必要があります。

- 『Sun Mainframe Transaction Processing ソフトウェア 管理者ガイド』の「セキュリティー」の章
- 『Sun Mainframe Transaction Processing ソフトウェア 管理者ガイド』の「Sun MTP Secure」の章

マニュアルの構成

このマニュアルは、以下の章で構成されています。

第 1 章では、Sun Mainframe Security Facility (Sun MSF) のセキュリティーモデルについて説明します。

第 2 章では、Sun MSF のインストール方法について説明します。

第 3 章では、セキュリティーリポジトリの設定方法について説明します。

第 4 章では、Sun MSF ソフトウェアの設定方法について説明します。

第 5 章では、セキュリティーリポジトリの生成と管理の方法について説明します。

第 6 章では、セキュリティーシステムの管理方法について説明します。

第 7 章では、Sun MSF を Sun Mainframe Transaction Processing ソフトウェア (Sun MTP) に統合する方法について説明します。

第 8 章では、Sun MSF に問題が発生した場合の解決方法について説明します。

第 9 章 では、Sun MSF のエラーメッセージとその対応策を一覧にします。

付録 Aでは、IBM の RACF と Sun MSF の類似点と相違点について説明します。

用語集には、このマニュアルで使用する単語および語句とその定義を一覧にしてまとめてあります。

UNIX コマンド

このマニュアルには、システムの停止、システムの起動、およびデバイスの構成などの基本的な UNIX® コマンドと操作手順に関する説明はありません。これらについては、以下を参照してください。

- ご使用のシステムに付属のソフトウェアマニュアル
- 下記にある Solaris™ オペレーティングシステムのマニュアル

  `http://docs.sun.com`

シェルプロンプトについて

シェル	プロンプト
UNIX の C シェル	**マシン名**%
UNIX の Bourne シェルと Korn シェル	$
スーパーユーザー (シェルの種類を問わない)	#

書体と記号について

書体または記号*	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	% **su** Password:
AaBbCc123 または **ゴシック**	コマンド行の可変部分。実際の名前や値と置き換えてください。	rm *filename* と入力します。 rm **ファイル名** と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅をこえる場合に、継続を示します。	% **grep '^#define ** **XV_VERSION_STRING'**

* 使用しているブラウザにより、これら設定と異なって表示される場合があります。

関連マニュアル

製品	タイトル	Part No.
Sun Mainframe Transaction Processing ソフトウェア	『Sun Mainframe Transaction Processing ソフトウェア 管理者ガイド』	819-2514-10
	『Sun Mainframe Transaction Processing ソフトウェア 構成ガイド』	819-2515-10
	『Sun Mainframe Transaction Processing ソフトウェア 開発者ガイド』	819-2516-10
	『Sun Mainframe Transaction Processing ソフトウェア インストールガイド』	819-2517-10
	『Sun Mainframe Transaction Processing ソフトウェア メッセージガイド』	819-2518-10
	『Sun Mainframe Transaction Processing ソフトウェア リファレンスマニュアル』	819-2519-10
	『Sun Mainframe Transaction Processing ソフトウェア 障害追跡とチューニング』	819-2520-10
	『Sun Mainframe Transaction Processing ソフトウェア XA リソースマネージャーの使用』	819-2358-10
	『Sun Mainframe Transaction Processing ソフトウェア ご使用にあたって（Solaris プラットフォーム用）』	819-2521-10
	『Sun Mainframe Transaction Processing ソフトウェア 高可用性 (HA) データサービス (Sun Cluster 用)』	819-2522-10
Sun Mainframe Security Facility	『Sun Mainframe Security Facility ご使用にあたって（Solaris プラットフォーム用）』	819-2513-10
	『Sun Mainframe Security Facility 高可用性 (HA) データサービス (Sun Cluster 用)』	819-2512-10

Sun のオンラインマニュアル

各言語対応版を含む Sun の各種マニュアルは、次の URL から表示または印刷、購入できます。

`http://www.sun.com/documentation`

Sun 以外の Web サイト

このマニュアルで紹介する Sun 以外の Web サイトの可用性については、Sun では責任を負いかねます。そのようなサイトやリソースの内容、広告、製品、またはそこから入手できるその他の資料については、推薦も保証も行なっておりません。それらのサイトやリソースあるいはそのリンク先が提供しているコンテンツ、商品、サービスなどを使用または信用した結果生じた損害や損失については、その真偽にかかわらず、Sun は一切責任を負いません。

Sun の技術サポート

このマニュアルに記載されていない技術的な問い合わせについては、次の URL にアクセスしてください。

`http://www.sun.com/service/contacting`

コメントをお寄せください

弊社では、マニュアルの改善に努力しており、お客様からのコメントおよびご忠告をお受けしております。コメントは下記よりお送りください。

`http://www.sun.com/hwdocs/feedback`

コメントには下記のタイトルと Part No. を記載してください。

『Sun Mainframe Security Facility 管理者ガイド』、Part No. 819-2359-10

第1章

Sun Mainframe Security Facility の概要

この章では、Sun MSF の概念について説明します。この章の内容は、次のとおりです。

外部セキュリティーの概要については、『Sun Mainframe Transaction Processing ソフトウェア 管理者ガイド』を参照してください。

Sun MSF のセキュリティーモデル

Sun MSF は、Sun MTP Secure に外部セキュリティーマネージャー (ESM) の管理サービスとランタイムサービスを提供します。また、デフォルトで ESM が有効で、Sun MTP Secure が付属しています。Sun MSF は、役割に基づくアクセス制御 (RBAC) セキュリティーモデルを提供します。このモデルでは、リソースへのアクセス権が役割に関連付けられ、ユーザーが適切な役割に割り当てられます。Sun MSF は、*inclusive permissions* モデルを使用しています。つまり、すべてのリソースをセキュリティーリポジトリで定義し、それらにアクセスする必要のあるユーザーや役割のすべてにアクセス権を与えます。リソースがセキュリティーリポジトリに定義されていない場合、そのリソースにはどのユーザーおよび役割からもアクセスできません。

Sun MSF のセキュリティーモデルのエンティティーは次のとおりです。

主体。セキュリティーシステムに定義されている個々のユーザー。

役割。テストグループなど、共通の責務を持つユーザーグループ。

リソースドメイン。共通のアクセス権要件を持つリソースグループ。

リソース。ファイルやプログラムなど、特定タイプの名前付きコンポーネント。ユーザーがトランザクションを実行するときや、ほかの作業を実行するときにアクセスします。

リソースドメインへの**アクセス権**は、主体と役割に与えられます。

図 1-1 は、主体、役割、リソースドメイン、リソース、アクセス権の関係を示しています。

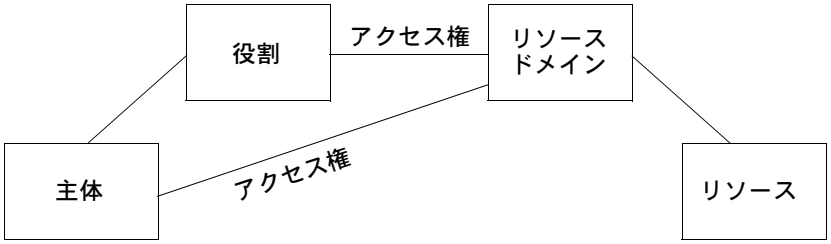

図 1-1　主体、役割、リソースドメイン、リソース、アクセス権の関係

これらのエンティティー間には次のような関係があります。

- 主体は役割のメンバーになれます。複数の役割に属しても、役割に属していなくもかまいません。
- 役割は 1 つまたは複数の主体をメンバーにできます。
- リソースとは 1 つのリソースドメインのメンバーです。
- 1 つのリソースドメインは 1 つまたは複数のリソースをメンバーにできます。
- リソースドメインは、任意の数の役割や主体のアクセス権を保有しています。

図 1-2 は、Sun MSF コンポーネントが相互に作用する仕組みを示しています。

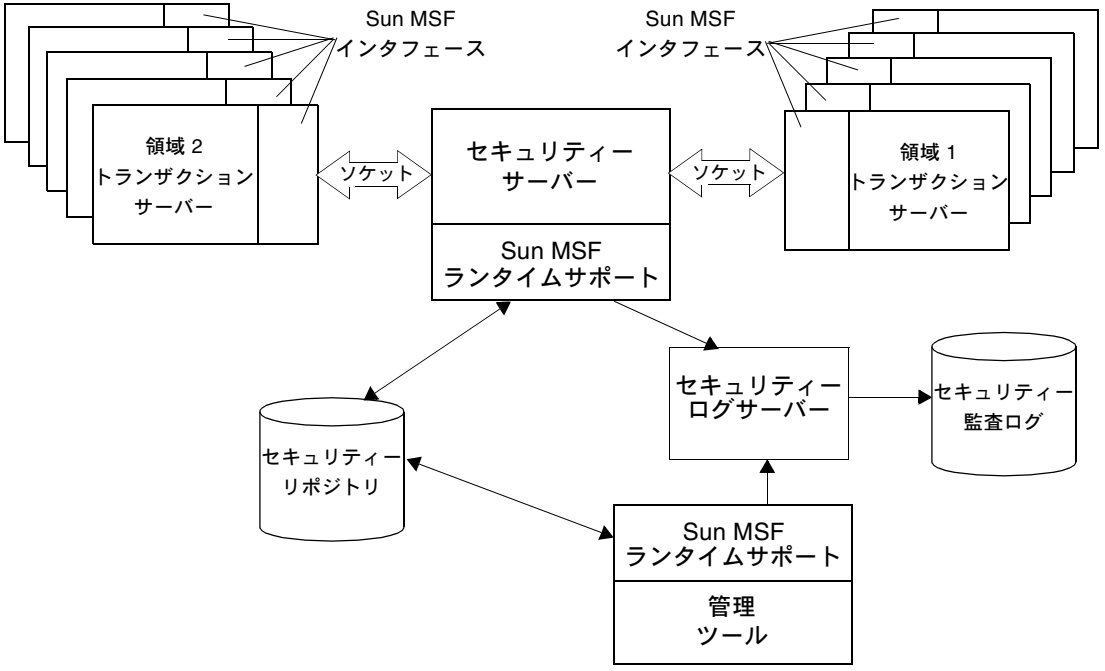

図 1-2 Sun MSF のコンポーネント

Sun MSF は、次のコンポーネントで構成されています。

セキュリティーリポジトリ。このリポジトリは、Sun 以外のリレーショナルデータベース管理システム (RDBMS) または LDAP ディレクトリで、Sun MSF が管理する主体、役割、リソースドメイン、リソースなどが含まれています。また、ドメインとリソースにアクセスするためのアクセス権やルールも含まれています。このリポジトリは、Sun MSF ランタイムと同じホストに置くことも、別のホストに置くことも可能です。ただし、このリリースでは、少なくともシステムのセキュリティーファイアウォールの背後に置く必要があります。詳細は、第 3 章 を参照してください

管理ツールセット。これらのコマンド行ツールは、セキュリティーリポジトリの初期化と管理に使用します。セキュリティーリポジトリの設定については、第 3 章 と 51 ページの「SecAdmin アプリケーション」を参照してください。

セキュリティーサーバー。セキュリティーサーバーは、Sun MTP の領域とセキュリティーリポジトリ間の認証と承認の相互作用を管理するプロセスです。有効な Sun MTP ユーザーすべてについてセキュリティールールの**キャッシュ**を保持し、使用するリポジトリのセキュリティールールを更新する再表示機能を提供します。

Sun MSF ランタイムサポート。このサービスを使用すると、セキュリティーサーバーと管理ツールがリポジトリと通信できるようになります。

セキュリティーサーバーへの Sun MSF のインタフェース。これらのインタフェースを使用して、領域のトランザクションサーバーがセキュリティーサーバーと通信します。また、**結果キャッシュ**をローカルに保持しているため、セキュリティーサーバーへのアクセスが最適化されます。このキャッシュは、`CEMT PERFORM SECURITY REBUILD` の実行後に再生成されます。詳細は、『Sun Mainframe Transaction Processing ソフトウェア 管理者ガイド』を参照してください。

各領域は、Sun MSF インタフェースからセキュリティーランタイムを使用して、ユーザー認証とリソースアクセス制御の判定を行います。Sun MSF インタフェースは、中央のセキュリティーサーバーへのソケットインタフェースを使用します。

セキュリティーログサーバー。セキュリティーログサーバーは、Sun MSF ランタイムサポートサービスが生成する監査メッセージをすべて収集し、それらをセキュリティー監査ログファイルに書き込みます。このログサーバーは、`msflog` コマンドで起動します。詳細は、93 ページの「セキュリティーログ収集の管理」と 97 ページの「セキュリティーイベントのログ記録」を参照してください。

Sun MSF インスタンス

Sun MSF のアーキテクチャーでは、1 回のソフトウェアインストールで外部セキュリティーマネージャーの複数のインスタンスを装備できます。インスタンスは Sun MSF のプロパティーの一意のセットで定義されます。たとえば、開発、テスト、本稼動というインスタンスを作成できます。これらのインスタンスはそれぞれ別のリポジトリを使用するか、共通のリポジトリを使用します。また、各インスタンスを別の管理者が担当することも、同じ管理者が全部を管理することもできます。インスタンスを選択するには、管理者が適切な環境を用意してからセキュリティーサーバーを起動するだけです。

図 1-3 は、3 つのインスタンスが含まれた Sun MSF のインストールを示しています。各インスタンスは、プロパティーファイルを格納している一意のディレクトリで表されます。

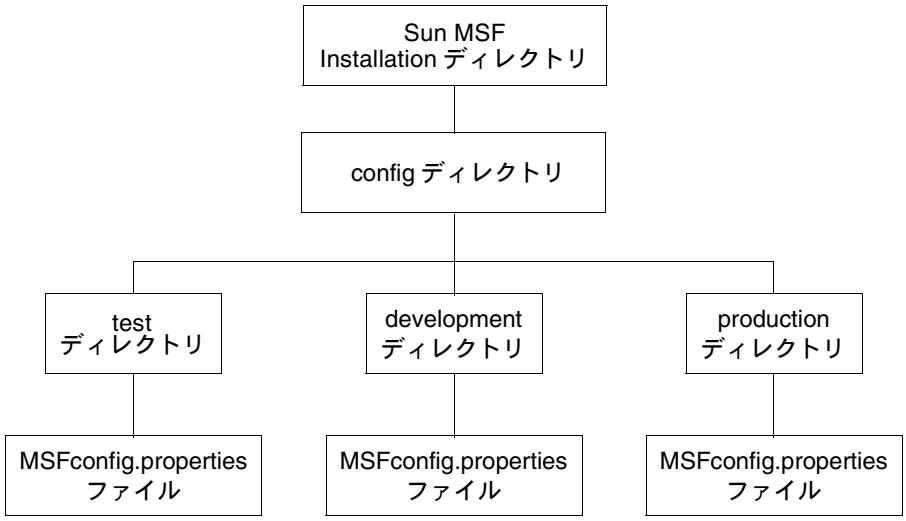

図 1-3　Sun MSF インスタンス

ユーザープロファイル

セキュリティーシステムでは、ユーザーを次の 4 つのカテゴリに分類します。

- スーパー管理者
- セキュリティー管理者
- セキュリティーサーバーオペレータ
- Sun MSF ユーザー

スーパー管理者

スーパー管理者は、セキュリティーリポジトリの作成と破棄以外に、ほかの 2 つのユーザーカテゴリ、Sun MSF セキュリティー管理者と Sun MSF ユーザーにアクセス権の付与ができなければなりません。それには、セキュリティーリポジトリとして使用する RDBMS または LDAP ディレクトリに全権限を持っていることが必要です。MakeAnAdministrator アプリケーションを起動する `msfinitr` コマンドを実行できるのは、スーパー管理者だけです。したがって、Sun MSF ソフトウェアインストールを使用するための UNIX ファイルアクセス権を持っています。この要員は、セキュリティーリポジトリの構成プロパティーの設定も担当するので、Sun MSF インスタンスディレクトリのファイルに書き込むための UNIX ファイルアクセス権が必要になります。詳細は、32 ページの「リポジトリの初期化とセキュリティー管理者の作成」を参照してください。

セキュリティー管理者

セキュリティー管理者は、SecAdmin アプリケーションを使用してセキュリティーリポジトリを保守します。したがって、Sun MSF ソフトウェアインストールと自分の Sun MSF インスタンス構成ファイルを使用するための UNIX ファイルアクセス権を持っています。セキュリティー管理者は、主体、役割、リソースドメイン、リソースの作成と保守を、それぞれに関連付けられたアクセス権ルールを使用して行います。スーパー管理者は、MakeAnAdministrator アプリケーションを使用してセキュリティー管理者を作成します。

セキュリティー管理者はリポジトリの編成も行います。通常、管理者は次の手順で要件を分析します。

1. ユーザーとリソースを特定します。
2. ユーザーがアクセスする必要のあるリソースを判断し、この情報を基に役割を作成します。共通のアクセス要件を持つユーザーをグループ化して 1 つの役割にします。
3. これらの役割に必要なリソースのアクセス権を判断し、それらの権限を基にリソースドメインを作成します。
4. リソースをリソースドメインに割り当てます。
5. 役割に (必要であれば主体にも) アクセス権を割り当てて、さまざまなリソースドメインにアクセスできるようにします。

この分析が完了したら、セキュリティー管理者はリポジトリの生成を開始できます。

セキュリティー管理者はセキュリティーサーバーも管理できますが、この権限をセキュリティーサーバーのオペレータに委任することもできます。

セキュリティーサーバーオペレータ

セキュリティーサーバーオペレータはセキュリティーサーバーを管理する権限を与えられています。管理タスクには、セキュリティーサーバーの起動と停止、セキュリティールールの更新、セキュリティーサーバーの統計情報の表示などがあります。このユーザーの作成は省略してもかまいません。セキュリティー管理者がセキュリティーサーバーの管理タスクも実行できるからです。ただし、Sun Cluster 用 の Sun MSF 高可用性データサービスを使用している場合は、このユーザーを作成する必要があります。詳細は、88 ページの「セキュリティーサーバーのオペレータとしての UNIX ユーザー ID の設定」を参照してください。Sun MSF 高可用性データサービスを使用している場合は、『Sun Mainframe Security Facility 高可用性データサービス (Sun Cluster 用)』マニュアルを参照してください。

Sun MSF ユーザー

Sun MSF ユーザーは、セキュリティーリポジトリの主体の集まりであり、管理的な権限を持ちません。ユーザー名とパスワードを使用してサインオンし、ビジネスアプリケーションを実行する一般ユーザーです。これらのユーザーは、領域の起動、停止、管理の権限を持つ Sun MTP 領域の管理者を兼任している場合もあります。これらのユーザーは、Sun MSF ツールを使用する必要がないため、Sun MSF ソフトウェアインストールを使用するための UNIX ファイルアクセス権は持っていません。

ユーザーが認証されると、Sun MSF で、役割とリソースドメインに基づいて、そのユーザーがリソースに持つアクセス権が決定されます。ユーザーが処理を要求すると、アクセスしようとするリソースごとに、セキュリティーランタイムによってアクセス権がチェックされます。ユーザーは、アクセス権に基づいてアクセスを承認、または拒否されます。

実装 Sun MSF

このタスクマップは、Sun MSF の実装に必要なタスクについて示しています。

表 1-1 タスクマップ: Sun MSF の実装

タスク	手順の参照先
使用しているアプリケーション環境のセキュリティーポリシーを定義します。	このポリシーは多くの場合、サイトのセキュリティー管理者と共同で作成します。ポリシーには、アプリケーションのすべてのセキュリティー要件を定義しておく必要があります。
Sun MSF ソフトウェアをインストールします。	第 2 章を参照してください。
セキュリティーリポジトリとして RDBMS を設定します。	第 3 章を参照してください。
Sun MSF ソフトウェアを設定します。	第 4 章を参照してください。
セキュリティーリポジトリを初期化して、セキュリティー管理者を作成します。	32 ページの「リポジトリの初期化とセキュリティー管理者の作成」を参照してください。
ログ記録を設定します。	93 ページの「セキュリティーログ収集の管理」を参照してください。
セキュリティーポリシーに基づいてリポジトリを生成します。	第 6 章を参照してください。
セキュリティーサーバーを起動します。	89 ページの「セキュリティーサーバーを起動する」を参照してください。

Sun MTP への統合を検討している場合は、第 7 章を参照してください。

第2章

Sun MSF ソフトウェアのインストール

Sun MSF ソフトウェアは Java Archive (JAR) ファイル一式で構成されています。ソフトウェアを使用するには、Java Development Kit (JDK™) のリリース 1.4 以降のインストールも必要です。

この章の内容は、次のとおりです。

導入ガイド

Sun MSF ソフトウェアは、zip ファイルか圧縮 tar ファイルとして配布されます。MakeAnAdministrator や SecAdmin など、Sun MSF ツールを実行する各システムにこれをインストールします。

次のガイドラインに沿って Sun MSF をインストールします。

- ルートユーザーとして Sun MSF をインストールしないでください。
- スーパー管理者と Sun MSF 管理者は、Sun MSF ディレクトリ構造への UNIX アクセス権が必要です。この権限を与えるには、両者を同じグループに割り当てます。
- 一般ユーザーは Sun MSF インストールへのアクセス権は必要ありませんし、持つべきでもありません。
- Sun MSF は、Sun MTP のインストールで使用したのと同じ場所にインストールするのが便利です。たとえば、Sun MTP を `/pkgs/mtp` ディレクトリにインストールした場合は、Sun MSF を `/pkgs/msf` ディレクトリにインストールします。ただし、これは必須要件ではありません。

▼ Sun MSF をインストールする

1. トップレベルのインストールディレクトリを作成します。

```
$ mkdir -p /pkgs/msf
```

2. インストールディレクトリに変更します。

```
$ cd /pkgs/msf
```

3. zip または tar 圧縮ファイルから Sun MSF ファイルを解凍します。

   たとえば、Solaris システムでは次のコマンドを入力します。

```
$ unzip /cdrom/MSF1.1.0.zip
```

   次のディレクトリ構造が作成されます。VERSION ファイルには Sun MSF のバージョン情報が含まれています。

```
/pkgs/msf/MSF1.1.0
/pkgs/msf/MSF1.1.0/bin
/pkgs/msf/MSF1.1.0/config
/pkgs/msf/MSF1.1.0/etc
/pkgs/msf/MSF1.1.0/lib
/pkgs/msf/MSF1.1.0/scbin
/pkgs/msf/MSF1.1.0/VERSION
```

   ディレクトリ MSF1.1.0 は、インストールした Sun MSF のバージョンを示します。

アップグレード Sun MSF

この節では、Sun MSF の新しいリリースにアップグレードする場合に実行するタスクについて説明します。

RDBMS リポジトリのアップグレード

Sun MSF 1.0.0 (任意のパッチレベル) からアップグレードする場合、既存のリポジトリデータベースを新しいリリースでも使用するには、`msfconvdb` ユーティリティーを実行する必要があります。

書式:

`msfconvdb {oracle|sybase|db2}` *schema-pw admin-pw user-pw*

schema-pw は、Sun MSF リポジトリスキーマユーザーのデータベースパスワード

admin-pw は、Sun MSF リポジトリ管理者のデータベースパスワード

user-pw は、Sun MSF リポジトリ一般ユーザーのデータベースパスワード

▼ 変換ユーティリティーを実行する

1. **使用環境が正しく設定され、パスに *MSF-home*`/bin` があることを確認します。**

   MSF-home が新しいバージョンのソフトウェアを参照している必要があります。

2. **次の情報を用意します。**

   - データベースの種類 (Oracle、Sybase、または DB2 UDB)
   - スキーマのパスワード
   - 管理者のパスワード
   - ユーザーのパスワード

   13 ページの「データベースユーザー名とパスワード」を参照してください。

3. **セキュリティーログサーバーを起動するかどうかを判断します。**

   - `MSFconfig.properties` ファイルの `com.sun.emp.security.logMessageOn` プロパティーが `true` に設定されている場合は (デフォルト)、セキュリティーログサーバーを起動する必要があります。
   - この設定を `false` に変更した場合は、ユーティリティーの実行前にセキュリティーログサーバーを起動する必要はありません。

4. **変換ユーティリティーを実行します。**

   たとえば、リポジトリが Oracle データベースで、スキーマのパスワードが spw、管理者のパスワードが apw、ユーザーのパスワードが upw の場合は、UNIX のプロンプトで次のコマンドを入力します。

```
$ msfconvdb oracle spw apw upw
```

   次の出力が表示され、移行に成功したことを示します。

```
(SecSvc_WARN) Updating the RDBMS repository
(SecSvc_WARN) Completed updating the RDBMS repository
```

   エラーが表示された場合は、ご購入先に連絡してください。

   リポジトリのアップデートが不要、またはアップデート済みであることが検出された場合は、次のメッセージが表示されます。

```
(SecSvc_WARN) RDBMS repository conversion not necessary -- now terminating
```

第3章

セキュリティーリポジトリの設定

Sun MSF は、セキュリティーリポジトリとしてリレーショナルデータベース管理システム (RDBMS) と LDAP ディレクトリの使用をサポートしています。この章では、Oracle®、IBM DB2 Universal Database (UDB)、および Sybase RDBMS 用のセキュリティーリポジトリを設定する方法について説明します。セキュリティーリポジトリとして LDAP ディレクトリを使用する場合の情報も含まれています。

この章の内容は、次のとおりです。

セキュリティーリポジトリとしての RDBMS の設定

この節では、セキュリティーリポジトリとしてデータベースを設定する方法について説明します。内容は次のとおりです。

データベースユーザー名とパスワード

RDBMS のデータベース管理者 (DBA) は、適切なツールを使用してセキュリティーリポジトリを構築する必要があります。また、ユーザーとパスワードの組も作成する必要があります。ユーザーにはスーパー管理者のほかに、セキュリティーリポジトリ

のデータベーステーブルに対する読み取り権と書き込み権のみを持つセキュリティー管理者と、すべてのセキュリティーテーブルへの読み取り権とユーザーテーブルへの書き込み権以外を持たなくてもログインできる一般ユーザーがあります。

データベースのユーザー名は、これらの項目について `MSFConfig.properties` ファイルの次の値と一致する必要があります。

- `com.sun.emp.security.adapterSchema` (スーパー管理者)
- `com.sun.emp.security.adapterAdmin` (管理者)
- `com.sun.emp.security.adapterUser` (エンドユーザー)

MakeAnAdministrator アプリケーションを実行してセキュリティーリポジトリを設定する場合は、これらのユーザー名のそれぞれにパスワードが必要です。また、MakeAnAdministrator アプリケーションでは、各ユーザーに必要なデータベースアクセス権を設定するために、JDBC 呼び出しを使用して SQL コマンドの `grant` または `revoke` を実行します。

Oracle データベースの使用法

この節では、セキュリティーリポジトリとして Oracle データベースを使用する場合のテーブル領域とユーザー ID の作成方法について例を挙げて説明します。この節の手順を完了したら、第 4 章に進んで Sun MSF を設定してください。

▼ テーブル領域を作成する

Oracle 管理者は、次の手順でセキュリティーデータベースを作成できます。これらのタスクを実行するツールやユーティリティーは、使用する Oracle のリリースによって異なる場合があります。

- **DBA 権限を持つ Oracle ユーザーを使用して、次のコマンドを実行します。**

注 – ディレクトリが存在する必要があります。

```
CREATE TABLESPACE secure_ts
DATAFILE '/opt/database/file01.dbf' SIZE 100M
MINIMUM EXTENT 500K
DEFAULT STORAGE (
       INITIAL 400K
       NEXT 400K
       MINEXTENTS 1
       MAXEXTENTS 200
       PCTINCREASE 0 )
PERMANENT
ONLINE ;
```

▼ テーブル領域に関連付けられたユーザー ID を作成する

この例では、スーパー管理者の名前は SUPERADMIN、セキュリティー管理者の名前は ADMIN、ユーザーの名前は ENDUSER です。

- **次のコマンドを実行します。**

```
connect internal;
create user SUPERADMIN identified by SUPERADMINPW default tablespace secure_ts;
grant connect,resource to SUPERADMIN;
create user ADMIN identified by ADMINPW default tablespace secure_ts;
grant connect,resource to ADMIN;
create user ENDUSER identified by ENDUSERPW default tablespace secure_ts;
grant connect,resource to ENDUSER;
commit;
```

これでログインが作成され、これらのユーザーが `SECURITY` データベースにアクセスできるようになります。

DB2 UDB データベースの使用法

この節では、セキュリティーリポジトリとして UDB データベースを使用する場合の、テーブル領域とユーザー ID の作成方法について例を挙げて説明します。この節の手順を完了したら、第 4 章に進んで Sun MSF を設定してください。

UNIX ログインの作成

DB2 UDB データベースのホストシステムで UNIX のログインを 3 つ作成するには、UNIX システム管理者に連絡してください。ログインは 1 つのグループ、たとえば `dbtwo` に属している必要があります。ホストシステムの DB2 UDB グループについては、UDB 管理者に問い合わせてください。たとえば、UNIX の 3 つのログイン形式を次のようにできます。

- udbsec
- udbadmin
- udbuser

▼ テーブル領域 (データベース) を作成する

UDB 管理者は、次の手順でセキュリティーデータベースを作成できます。これらのタスクを実行するツールやユーティリティーは、使用する UDB のリリースによって異なる場合があります。

1. **ホストシステムに udbsec としてログインします。**
2. **パスに `db2` コマンドがあることを確認してください。**

   DB2 UDB 管理者から入手した `db2profile` ファイルを用意します。
3. **`db2` コマンドを入力します。**

   `db2 =>` プロンプトが表示されます。
4. **`CREATE DATABASE` コマンドを実行します。**

   たとえば、データベース MSFSECUDB を作成するには、次のコマンドを入力します。

```
db2 => CREATE DATABASE MSFSECUDB
DB20000I  The CREATE DATABASE command completed successfully.
db2 => connect to MSFSECUDB

Database Connection Information

       Database server        = DB2/SUN 8.1.0
       SQL authorization ID   = UDBSEC
       Local database alias   = MSFSECUDB
```

Sybase データベースの使用法

この節では、セキュリティーリポジトリとして Sybase データベースを使用する場合の設定方法について例を挙げて説明します。この節の手順を完了したら、第 4 章に進んで Sun MSF を設定してください。

▼ Sybase データベースを設定する

Sybase 管理者は、次の手順でセキュリティーデータベースを作成できます。これらのタスクを実行するツールやユーティリティーは、使用する Sybase のリリースによって異なる場合があります。

1. **セキュリティーデータベースを格納するデータベースデバイスを決めます。**

   データベースは、複数のデータベースデバイスに、それぞれ異なる容量で格納できます。たとえば、デフォルトのデータベースデバイスの論理名を表示するには、次のように入力します。

```
isql> select name from sysdevices where status & 1 = 1 order by name
```

2. **次のコマンド構文を使用して、データベースを作成します。**

```
create database database_name
       [on {default | database_device} [= size] ...
```

   たとえば、DBA 権限を持つ Sybase ユーザー名を次のように使用します。

```
$ isql -Udba_user -Pdba_pw
isql> create database SECURITY on default = "4M"
```

3. **データベースの所有権を割り当て、3 つのすべてのセキュリティーユーザーにデフォルトのデータベースを設定します。**

```
isql> sp_addlogin secuser, secuser, SECURITY
isql> go
isql> sp_addlogin secadmin, secadmin, SECURITY
isql> go
isql> sp_addlogin superadmin, superadmin, SECURITY
isql> go
isql> use SECURITY
isql> go
isql> sp_changedbowner superadmin
isql> go
isql> sp_adduser secuser
isql> go
isql> sp_adduser secadmin
isql> go
```

   これでログインが作成され、SECURITY データベースに関連付けられます。

セキュリティーリポジトリとしての LDAP ディレクトリの設定

セキュリティーリポジトリとして LDAP ディレクトリを設定する前に、LDAP ディレクトリの管理者は次のタスクを実行する必要があります。

- データベースのルート識別名 (DN) を定義します。次に例を示します。

  dc=secdb, dc=mycorp, dc=com

- スキーマのパスワードを定義します。これは LDAP ディレクトリ DN に関連付けられているパスワードです。次に例を示します。

  “uid=*schema*,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot”

  この例では、*schema* は、`MSFconfig.properties` ファイルの `com.sun.emp.security.adapterSchema` プロパティーに割り当てられている値です。Sun Java Directory Server を使用する場合、この uid はディレクトリがインストールされて初期化されるときに設定されます。多くの場合、「uid=admin」に類似したものになります。

LDAP ディレクトリの管理者は、`msflog`、`msfladapschema`、および `msfldapcr` ユーティリティーを実行するための UNIX ファイルアクセス権も必要です。

セキュリティーリポジトリとしての LDAP ディレクトリを設定するには、第 4 章 を参照してください。

第4章

Sun MSF の設定

Sun MSF は、Sun MTP のデフォルトの外部セキュリティーマネージャーですが、有効になっていません。Sun MSF を有効にして実行するには、設定タスクをいくつか完了する必要があります。この章の内容は、次のとおりです。

タスクマップ: Sun MSF の設定

次の表に、Sun MSF の設定タスクを一覧表示します。

表 4-1 タスクマップ: Sun MSF の設定

タスク	手順の参照先
Java-home/lib/security ディレクトリにある java.policy ファイルと java.security ファイルが正しく設定されていることを確認します。 Sun MSF はそのセキュリティープロパティーとセキュリティーポリシーを設定するとき、$PATH にある *Java-home* ディレクトリを使用して、すでに設定されているセキュリティープロパティーを拡張します。したがって、ほかの Java アプリケーションを実行するために java.policy ファイルと java.security ファイルを変更した場合は、Sun MSF を実行するときに *Java-home* が $PATH にあることを確認してください。	システム管理者以外のユーザーは、これをシステム管理者に確認してもらってください。
Sun MSF インスタンスのディレクトリを 1 つまたは複数作成します。	20 ページの「Sun MSF のインスタンスの作成」

表 4-1　タスクマップ: Sun MSF の設定 (続き)

タスク	手順の参照先
セキュリティー管理者の環境を設定します。	21 ページの「管理者の設定ファイルの作成」
Sun MSF 構成ユーティリティーを実行して、リポジトリの種類を選択します。	23 ページの「構成ユーティリティーの実行」
ほかのセキュリティープロパティーを設定します。	28 ページの「セキュリティープロパティーの設定」
リポジトリを初期化して、Sun MSF セキュリティー管理者を作成します。	32 ページの「リポジトリの初期化とセキュリティー管理者の作成」

Sun MSF 環境の作成

Sun MSF に関連するタスクを実行する前に、環境を設定する必要があります。次の 2 つのタスクが必要です。

- 1 つまたは複数の Sun MSF のインスタンスの作成
- Sun MSF 管理者の設定ファイルの作成

Sun MSF のインスタンスの作成

Sun MSF のインスタンスは、そのセキュリティーサーバー、ログサーバー、その他のサービスのために、リポジトリの特性と運用の設定を定義した一意のプロパティーセットです。インスタンスを作成するには、サブディレクトリを*MSF-home*/config に作成し、ここに一意の Sun MSF プロパティーファイルを格納します。このサブディレクトリに有効な UNIX 名を付けます。このサブディレクトリは MSF_INSTANCE 環境変数によって参照されます。たとえば、*MSF-home*/config に production というディレクトリを作成した場合は、$MSF_INSTANCE が production の値に設定されます。

production、test、development のように、複数のディレクトリを *MSF-home*/config に格納することもできます。各ディレクトリには Sun MSF 管理者の場合は読み取り権のみ、スーパー管理者の場合は読み取り権と書き込み権があります。各ユーザーが使用できる環境変数は一度に 1 つだけですが、3 つのインスタンスをすべて同時に運用することが可能です。

管理者の設定ファイルの作成

Sun MSF を設定して管理する場合、通常は一度だけ実行すればよいタスクと、継続的に実行するタスクとがあります。管理環境において、これらのタスクは 1 人または複数の要員で行います。関係する人数によっては、管理者タイプごとに異なる設定ファイルを作成することもできます。次の表に、各タスクの説明、実行頻度、および実行者を示します。

表 4-2　管理タスク

タスク	頻度	実行者
`$MSF_INSTANCE` ディレクトリの作成	各インスタンスにつき 1 回	システム管理者または Sun MSF スーパー管理者
Sun MSF 構成ユーティリティーを実行するための設定ファイルの作成または変更	各インスタンスにつき 1 回	Sun MSF スーパー管理者またはデータベース管理者
構成ユーティリティーの実行	各インスタンスにつき 1 回	Sun MSF スーパー管理者またはデータベース管理者
`MSFconfig.properties` ファイルの編集	各インスタンスにつき 1 回以上	Sun MSF スーパー管理者
リポジトリの初期化と Sun MSF 管理者の作成	各インスタンスにつき 1 回	Sun MSF スーパー管理者
Sun MSF 管理者用の設定ファイルの作成	各インスタンスにつき 1 回	Sun MSF スーパー管理者
セキュリティーリポジトリの保守	各インスタンスにつき継続的	Sun MSF 管理者
ログサーバーの管理	各インスタンスにつき継続的	Sun MSF 管理者またはセキュリティーサーバーオペレータ
セキュリティーサーバーの管理	各インスタンスにつき継続的	Sun MSF 管理者またはセキュリティーサーバーオペレータ

設定ファイルに含める情報は、管理者が実行するタスクの種類によって異なります。

Sun MSF スーパー管理者

Sun MSF 構成ユーティリティーを実行する Sun MSF スーパー管理者には、次のエントリが含まれた設定ファイルが必要です。

- JDK 実行可能ファイルの `bin` ディレクトリが `PATH` 変数にあること。
- *MSF-home*`/bin` ディレクトリが `PATH` 変数にあること。*MSF-home* は Sun MSF のインストールディレクトリです。必要に応じて、Sun MSF のインストールディレクトリを示す `MSF_HOME` という変数を定義することもできます。

- MSF_INSTANCE 環境変数。これは、設定する MSFconfig.properties ファイルを格納するディレクトリです。
- 使用するリポジトリに固有の環境変数 (ORACLE_HOME など)。詳細は、リポジトリソフトウェアのマニュアルを参照してください。

次の例では、MSF_INSTANCE のエントリが 3 つあり、それぞれが異なるプロパティーセットを表します。エントリの 2 つはコメント付きです。Sun MSF の production インスタンスのプロパティーは、この設定ファイルが提供されると使用されます。

```
MSF_INSTANCE=production;export MSF_INSTANCE
#MSF_INSTANCE=test;export MSF_INSTANCE
#MSF_INSTANCE=development;export MSF_INSTANCE
PATH=MSF-home/bin:Java-home/bin:$PATH;export PATH

ORACLE_HOME=/opt/oracle10g;export ORACLE_HOME
...
...
```

Sun MSF 管理者と Sun MSF セキュリティーサーバーオペレータ

Sun MSF 管理者とセキュリティーサーバーオペレータを作成した場合は、次のエントリが含まれた設定ファイルが必要です。

- JDK 実行可能ファイルの bin ディレクトリが PATH 変数にあること。
- *MSF-home*/bin ディレクトリが PATH 変数にあること。*MSF-home* は Sun MSF のインストールディレクトリです。必要に応じて、Sun MSF のインストールディレクトリを示す MSF_HOME という変数を定義することもできます。
- MSF_INSTANCE 環境変数。これは、管理するインスタンスの MSFconfig.properties ファイルを格納するディレクトリです。

```
MSF_INSTANCE=production;export MSF_INSTANCE
PATH=MSF-home/bin:Java-home/bin:$PATH;export PATH
```

構成ユーティリティーの実行

Sun MSF 構成ユーティリティーを使用すると、設定タスクが簡略化されるので、さまざまなファイルを手作業で編集する手間が省けます。この節の最初の手順では、構成ユーティリティーを使用して、RDBMS を Sun MSF リポジトリとして指定する方法について説明します。LDAP ディレクトリをリポジトリとして使用している場合は、その次の手順を適用してください。

RDBMS の値

構成ユーティリティーでは、設定する RDBMS に特定の値が想定されます。次の表に、それらの値を示します。JDBC のパスについてはデータベースのマニュアルを、サポートされているデータベースリリースについては Sun MSF のリリースノートを参照してください。

表 4-3　RDBMS JDBC の値

RDBMS	JDBC ドライバのクラス	JDBC のパス
Oracle	`oracle.jdbc.OracleDriver`	`$ORACLE_HOME/jdbc/lib/classes12.zip`
UDB	`com.ibm.db2.jdbc.app.DB2Driver`	`$INSTHOME/java/db2java.jar`
Sybase	`com.sybase.jdbc2.jdbc.SybDriver`	`$SYBASE/jConnect-5_5/classes/jconn2.jar`

▼ RDBMS をリポジトリとして使用するように Sun MSF を設定する

1. **Sun MSF 環境を作成します。**
   詳細は、20 ページの「Sun MSF 環境の作成」を参照してください。
2. **21 ページの「Sun MSF スーパー管理者」 で作成した設定ファイルを用意します。**
3. **次のコマンドを実行してユーティリティーを起動します。**

```
$ msfconfig
```

次の処理が実行されます。

- `$MSF_INSTANCE` が正しく設定されていること、Java の必要バージョンがインストールされていることを確認します。
- `jaas.config`、`java.security`、または `java.policy` ファイルが *MSF-home*`/config` で設定されているかどうか調べます。いずれかのファイルがない場合は、ツールで構築するというメッセージが表示されます。
- *MSF-home*`/etc/java.security` ファイル (または `java.policy`、あるいは両方) の内容をそのファイルの JDK バージョンにマージし、マージしたファイルを *MSF-home*`/config` ディレクトリに保存します。JDK ファイルは通常、*Java-home*`/jre/lib/security/java.security` または *Java-home*`/jre/lib/security/java.policy`、あるいはその両方です。
- *MSF-home*`/etc/jaas.config` の内容を *MSF-home*`/config` ディレクトリにコピーします。

注 – `jaas.config`、`java.security`、または `java.policy` ファイルに、顧客特有の変更が必要な場合は、構成ユーティリティーを実行するときに、それらのファイルバージョンが *Java-home* ディレクトリにあることを確認してください。

---

4. **「Sun MSF 構成ユーティリティー」メニューが表示されたら、使用するリポジトリのオプション番号を入力し、Return キーを押します。**

   RDBMS の選択肢は次のとおりです。

   1. Oracle JDBC ドライバのプロパティーを定義する
   2. DB2 UDB JDBC ドライバのプロパティーを定義する
   3. Sybase JDBC ドライバのプロパティーを定義する

   次の妥当性検査が実行されます。

   - リポジトリに必要な環境変数が設定されていることを確認します。
   - JDBC のクラスと JDBC ドライバのパスの値を確認して報告します。次に例を示します。

```
JDBC drivers path = /database/oracle/ORAHOME9.2/jdbc/lib/classes12.zip
JDBC drivers class = oracle.jdbc.driver.OracleDriver
```

   - JDBC ドライバをサポートするために共有ライブラリがデータベース製品に必要な場合は、次のようなメッセージでパスの値が報告されます。

```
JDBC shared libraries = /database/db2/sqllib/lib
```

   妥当性検査に失敗した場合は、それを説明するエラーメッセージが表示され、ユーティリティーは終了します。

5. データベース接続に使用する URL の要素を指定するようにプロンプトが表示された場合は、次の表に示す情報を入力します。

プロンプト	入力内容
JDBC connection URL host name/IP	ホスト名または IP アドレス
JDBC connection URL port number	URL のポート番号
JDBC connection URL database identifier (SID or name)	データベース識別子

プロンプトへの応答から作成された URL を示す確認メッセージが表示されます。たとえば、次のいずれかになります。

```
JDBC connection URL = jdbc:oracle:thin:@machine1:1521:msfdb
JDBC connection URL = jdbc:db2://machine1:50000/msfdb
JDBC connection URL = jdbc:sybase:msfdb:machine1:4100
```

次に、`$MSF_INSTANCE` ディレクトリ内の `MSFconfig.properties` ファイルが更新されます。旧バージョンのプロパティーファイルがあった場合は、そのディレクトリに `MSFconfig.properties.bkup` として保存されます。以前に保存されたバックアップファイルは、すべて上書きされます。必要に応じて、`Sun MSF` 固有の `java.security`、`java.policy` ファイルと `jaas.config` ファイルも作成されます。次のようなメッセージでユーティリティーの処理が報告されます。

```
Building /pkgs/msf/MSF1.1.0/config/java.security file
Building /pkgs/msf/MSF1.1.0/config/java.policy file
Building /pkgs/msf/MSF1.1.0/config/jaas.config file
Making backup file:
/pkgs/msf/MSF1.1.0/config/production/MSFconfig.properties.bkup
Working base file: /pkgs/msf/MSF1.1.0/config/production/MSFconfig.properties
Sun MSF Configuration completed successfully!
```

6. 28 ページの「セキュリティープロパティーの設定」に進んで、リポジトリの設定を続けます。

▼ LDAP ディレクトリリポジトリを使用するように Sun MSF を設定する

注 – サイトの LDAP 管理者は、セキュリティーリポジトリとして使用する LDAP サーバーの初期設定を実行し、ディレクトリのインストール先となるシステムのホスト名とポート番号を提供する必要があります。

---

1. **Sun MSF 環境を作成します。**

   詳細は、20 ページの「Sun MSF 環境の作成」を参照してください。

2. **21 ページの「Sun MSF スーパー管理者」で作成した設定ファイルを用意します。**

3. **次のコマンドを実行してユーティリティーを起動します。**

```
$ msfconfig
```

   バックグラウンドで次の処理が実行されます。

   - `$MSF_INSTANCE` が正しく設定されていること、Java の必要バージョンがインストールされていることを確認します。
   - `jaas.config`、`java.security`、または `java.policy` ファイルが *MSF-home*`/config` で設定されているかどうか調べます。いずれかのファイルがない場合は、ツールで構築するというメッセージが表示されます。
   - *MSF-home*`/etc/java.security` ファイル (または `java.policy`、あるいは両方) の内容をそのファイルの JDK バージョンにマージし、マージしたファイルを *MSF-home*`/config` ディレクトリに保存します。JDK ファイルは通常、*Java-home*`/jre/lib/security/java.security` または *Java-home*`/jre/lib/security/java.policy`、あるいはその両方です。
   - *MSF-home*`/etc/jaas.config` の内容を *MSF-home*`/config` ディレクトリにコピーします。

注 – `java.security` または `java.policy` ファイルに、顧客特有の変更が必要な場合は、構成ユーティリティーを実行するときに、それらのファイルバージョンが *Java-home* ディレクトリにあることを確認してください。

---

4. **「Sun MSF 構成ユーティリティー」メニューが表示されたら、オプション `4` を選択して Return キーを押します。**

   次のメッセージが表示されます。

```
Creating file: MSF-home/config/MSF-instance/jndi.properties
Building Sun Java System Directory Server configuration
```

注 – jndi.properties ファイルが $MSF_INSTANCE ディレクトリにすでに存在する場合は、ファイルのバックアップコピーが作成され、jndi.properties.bkup という名前が付けられます。

5. **LDAP ディレクトリへの接続に使用する URL の要素を指定するようにプロンプトが表示された場合は、次の情報を入力します。**

プロンプト	入力内容
LDAP connection URL host name/IP	ホスト名または IP アドレス
LDAP connection URL port number [389]	URL のポート番号。デフォルト値は 389 です

プロンプトへの応答から作成された URL を示す確認メッセージが次のように表示されます。

```
LDAP URL = ldap://machine1:389
```

6. **ルート DN を指定するようにプロンプトが表示されたら、ディレクトリのルート識別名を入力します。**

入力したルート DN を示す確認メッセージが表示されます。次に例を示します。

```
LDAP root DN = dc=abcdb,dc=xyz,dc=com
```

次に、$MSF_INSTANCE ディレクトリ内の MSFconfig.properties ファイルが更新されます。旧バージョンのプロパティーファイルがあった場合は、そのディレクトリに MSFconfig.properties.bkup として保存されます。以前に保存されたバックアップファイルは、すべて上書きされます。必要に応じて、java.security、java.policy、および jaas.config ファイルも作成されます。次のようなメッセージでユーティリティーの処理が報告されます。

```
Building /pkgs/msf/MSF1.1.0/config/java.security file
Building /pkgs/msf/MSF1.1.0/config/java.policy file
Building /pkgs/msf/MSF1.1.0/config/jaas.config file
Making backup file:
/pkgs/msf/MSF1.1.0/config/production/MSFconfig.properties.bkup
Working base file: /pkgs/msf/MSF1.1.0/config/production/MSFconfig.properties
Sun MSF Configuration completed successfully!
```

7. **28 ページの「セキュリティープロパティーの設定」に進んで、リポジトリの設定を続けます。**

セキュリティープロパティーの設定

構成ユーティリティーでは、MSFconfig.properties ファイルで必要なプロパティーのすべての設定が表示されるわけではありません。次のプロパティーの値だけが生成されます。

- com.sun.emp.security.adapterDriver (JDBC)
- com.sun.emp.security.adapterLibrary (JDBC)
- com.sun.emp.security.adapterPath (JDBC)
- com.sun.emp.security.adapterRoot (LDAP)
- com.sun.emp.security.adapterType (JDBC and LDAP)
- com.sun.emp.security.adapterURL (JDBC and LDAP)

残りの必要プロパティーとオプションのプロパティーの値を表示するには、ファイルを手動で編集する必要があります。

▼ セキュリティーのプロパティーを設定する

1. **該当する $MSF_INSTANCE ディレクトリ内の MSFconfig.properties ファイルを開きます。**
2. **ファイルの文を確認します。**

   表 4-4 の情報を使用して、プロパティーの値を決定します。
3. **次の必要プロパティーのすべてに有効な値を入力します。**
   - com.sun.emp.security.logDirectory

   注 – 複数のインスタンスを同時に実行している場合は、混乱を防ぐために各インスタンスに一意のログディレクトリを定義してください。すべてのログを同じディレクトリ (たとえば /tmp) に書き込むと、どのログがどのインスタンスに適用されるのか区別しにくくなります。

   - com.sun.emp.security.logMessagePort
   - com.sun.emp.security.logPeriod
   - com.sun.emp.security.logTracePort
   - com.sun.emp.security.adapterSchema
   - com.sun.emp.security.adapterAdmin
   - com.sun.emp.security.adapterUser
   - com.sun.emp.security.adapterKeyFile
   - com.sun.emp.security.serverPortNumber
4. **その他のプロパティーに有効な値を入力します。**

5. **ファイルを保存して閉じます。**

表 4-4 に、ファイルに含まれる各プロパティーと有効な値を示します。ファイル内の各プロパティーには `com.sun.emp.security.` という接頭辞が付きますが、表では省略しています。

表 4-4 `MSFconfig.properties` ファイル (1 / 4)

プロパティー名	説明
`logTraceOn`	デバッグトレースを有効にします。 値: `True` または `False` (デフォルト) True に設定すると、生成されるメッセージを収集するためにセキュリティーログサーバーを実行する必要があります。実行していない場合でも、ほかの Sun MSF アプリケーションは使用できます。必要な収集サービスが応答していないことが報告されますが、トレースログ記録なしで実行が継続します。
`logTraceLevel`	デバッグトレースのレベル。値: `0` - FATAL レベル (例外を含む) のトレースのみを示します (デフォルト) `1` = FATAL と ERROR レベルを示します `2` = FATAL、ERROR、WARNING レベルを示します `3` = INFO を含むすべてのトレースレベルを示します
`logTraceDest`	トレースロガーのホスト名 (たとえば、IP アドレス) デフォルトは `localhost` です (推奨)
`logTracePort`	トレースロガーが使用するポート番号。 必須 (デフォルト値は設定されていない)
`logMessageOn`	監査ログ記録を有効にします。 値: `True` (デフォルト、推奨) または `False` (推奨されない)。 True に設定した場合、生成されるメッセージを収集するにはセキュリティーログサーバーを実行する必要があります。実行していない場合は、ほかの Sun MSF アプリケーションもすべて使用できなくなります。アプリケーションは必要な収集サービスが応答していないことをレポートし、即座に終了します。
`logMessageLevel`	監査メッセージのレベル。値: `0` - FATAL レベル メッセージのみを示します (デフォルト) `1` = FATAL と ERROR レベルを示します `2` = FATAL、ERROR、WARNING レベルを示します `3` = INFO を含むすべての監査メッセージレベルを示します
`logMessageDest`	メッセージロガーのホスト名 (たとえば、IP アドレス)。 デフォルトは `localhost` です (推奨)。
`logMessagePort`	メッセージロガーが使用するポート番号。 必須 (デフォルト値は設定されていない)
`logDirectory`	メッセージとトレースログが書き込まれるディレクトリ。必須。

表 4-4　MSFconfig.properties ファイル (2 / 4)

プロパティー名	説明
logPeriod	自動ログファイルを切り替える間隔 (時間)。0 ～ 24 の値。0 はログファイルの自動切り替えがないことを示します。必須。
passwordExpiresDate	主体のパスワードが期限切れになる日付 (ほかに指定されていない場合)。デフォルトの動作ではパスワードは期限切れになりません。 書式: *mm/dd/yyyy*
passwordMaxDaysAllowed	主体のパスワードが変更されずに有効であり続ける最大日数。 デフォルトは 0 (ゼロ) です。これは、定期的にパスワードを変更する必要がないことを示します。
passwordMinDaysRequired	パスワードを (再度) 変更できるまでの最小日数 デフォルトは 0 (ゼロ) です。これは、パスワードをいつでも変更できることを示します。
initialSuspendState	作成時に主体を最初の停止状態にします (指定されていない場合)。 値: T(rue) または F(alse)。デフォルト値は F で、停止しません。
loginFailures	連続してログインパスワードに失敗できる許容回数。この回数を超えると、主体は停止されます。 デフォルトは 0 (ゼロ)。これは制限がないことを示します。
passwordMaxLength	パスワードに使用できる最大文字数。値を設定しない場合は、Sun MSF のデフォルト値の 0 (ゼロ) になり、パスワードの最大長はチェックされません。 Sun MTP に統合する場合、パスワードの最大長を設定するには 1 ～ 8 の値を使用してください。 無効な値を入力すると (たとえば、8 より大きい値)、このプロパティーは passwordMinLength と同じ値に設定されます。
passwordMinLength	パスワードに必要な最小文字数。 デフォルトは 0 (ゼロ) です。これは最小限度がなく、空のパスワードも有効であることを示します。
logGrants	許可 (承認) されたアクセス権の監査ログ記録を WARN メッセージとして有効にします。 値: True (デフォルト) または False
denialReaction	拒否されたアクセスに対するアプリケーションの対応と監査ログの記録。値: FAIL (デフォルト) は、FATAL 監査ログメッセージを生成し、要求元アプリケーションに拒否を返します。 ALERT は、ERROR 監査ログメッセージだけを生成します。Sun MSF を最初に設定するときにこの値を使用すると、予期しないアクセス拒否を受け取ることなく領域を確実に起動できます。 NONE は、監査ログメッセージも要求元アプリケーションへの拒否も生成しません。

表 4-4　MSFconfig.properties ファイル (3 / 4)

プロパティー名	説明
passwordFormat	パスワードに使用できる文字。値: alphaOnly: 使用できるのは、アルファベット文字だけ。 numericOnly: 使用できるのは、数字だけ。 mixedOK (デフォルト): 制限なし
serverPortNumber	セキュリティーサーバーが使用するポート番号。 必須。デフォルト値は設定されていません。
adapterType	アダプタのタイプ。値: JDBC: JDBC をサポートするリレーショナルデータベース。 JNDI: LDAP プロトコルをサポートするディレクトリ この値は設定ツールによって生成されます。
adapterRoot	LDAP セキュリティーリポジトリのルート接尾辞の識別名に相当する値。次に例を示します。 dc=security,dc=companyname,dc=com この値は設定ツールによって生成されます。
adapterPath	JDBC ドライバファイルのパス名。この値は設定ツールによって生成されます。
adapterDriver	必要な JDBC ドライバの Java クラス名。この値は設定ツールによって生成されます。
adapterLibrary	JDBC ドライバに必要な場合は、共有ライブラリディレクトリのパス名。この値は設定ツールによって生成されます。
adapterURL	RDBMS に必要な JDBC 設定ファイルの場所を示す URL、または LDAP ディレクトリのホスト名とポート番号。 この URL は設定ツールによって作成されます。
adapterSchema	セキュリティーリポジトリのスキーマユーザー ID の名前と、セキュリティースーパー管理者の名前。必須。デフォルト値は設定されていません。 RDBMS: 13 ページの「データベースユーザー名とパスワード」を参照してください。 LDAP ディレクトリ: 18 ページの「セキュリティーリポジトリとしての LDAP ディレクトリの設定」を参照してください。
adapterAdmin	MakeAnAdministrator ツールでリポジトリに作成されたセキュリティー管理者の名前。必須。デフォルト値は設定されていません。
adapterUser	MakeAnAdministrator ツールでリポジトリに作成されたセキュリティーエンドユーザーの名前。必須。デフォルト値は設定されていません。

表 4-4　MSFconfig.properties ファイル (4 / 4)

プロパティー名	説明
adapterKeyFile	秘密鍵 (データベースリポジトリの暗号化パスワード) の情報が含まれたファイルの完全修飾パス名。必須。次に例を示します。 /pkgs/msf/MSF1.1.0/keys/udbkey.txt
adapterMaxconn	JDBC サーバーからセキュリティーリポジトリへの最大接続数。
hostPrincipal	プラットフォームに固有の主体の実装を提供する Java クラスで、UNIX ユーザー ID を表します。このプロパティーは、オペレーティングシステムに適した値で事前に設定されています。この値は変更しないでください。値は次のとおりです。 Solaris: com.sun.security.auth.UnixPrincipal AIX: com.ibm.security.auth.AIXPrincipal

リポジトリの初期化とセキュリティー管理者の作成

設定プロセスの次のステップで、スーパー管理者は MakeAnAdministrator アプリケーションを使用して、セキュリティーリポジトリを初期化し、リポジトリの生成と保守を担当する Sun MSF セキュリティー管理者を作成します。使用しているリポジトリの種類によって、次の適切な手順に従ってください。

- 32 ページの「セキュリティー管理者を作成して RDBMS リポジトリを初期化する」
- 35 ページの「セキュリティー管理者を作成して LDAP リポジトリを初期化する」

Sun MSF の各インスタンスについて、この手順に従う必要があります。

▼ セキュリティー管理者を作成して RDBMS リポジトリを初期化する

1. **MSFconfig.properties ファイルに正しい値が含まれていることを確認します。**
2. **データベース管理者から入手したスキーマ、管理者、エンドユーザーの各パスワードがあることを確認します。**

   13 ページの「データベースユーザー名とパスワード」を参照してください。

注 – MSFconfig.properties ファイルでパスワードの最大長を設定した場合は、指定した長さ以内にする必要があります。

3. **設定ファイルを使用して、Sun MSF スーパー管理者の環境を設定します。**

   この設定ファイルで必要な値については、21 ページの「管理者の設定ファイルの作成」を参照してください。

4. **次のコマンドを使用して、ログサーバーを起動します。**

```
$ msflog -s
```

   ログサーバーの管理については、93 ページの「セキュリティーログ収集の管理」を参照してください。

5. **コマンドプロンプトで、**msfinitr **コマンドを実行します。**

```
$ msfinitr admin-domain
```

   admin-domain 引数のデフォルトは AdminResources です。これは、セキュリティー管理者が使用する Sun MSF のリソースがすべて含まれたリソースドメインの名前です。

   次のメッセージとプロンプトが表示されます。

```
(SecSvc_262) Loading security configuration data...

(SecSvc_250) Security SCHEMA name: schema-name
(SecSvc_253) Enter security SCHEMA password (or quit):
```

6. **データベース管理者から入手したスキーマのパスワードを入力します。**

   13 ページの「データベースユーザー名とパスワード」を参照してください。

7. **プロンプトで管理者パスワードを求められたら、データベース管理者から入手したパスワードを入力します。**

```
(SecSvc_250) Security ADMIN name: admin-name
(SecSvc_253) Enter security ADMIN password (or quit):
```

8. プロンプトでエンドユーザーのパスワードを求められたら、データベース管理者から入手したパスワードを入力します。

```
(SecSvc_250) Security END USER name: user-name
(SecSvc_253) Enter security END USER password (or quit):
```

9. リポジトリがすでに存在する場合は、次のメッセージに応答する必要があります。

```
(SecSvc_213) Repository not empty;
    ... do you want to destroy current contents and reinitialize (yes/no)?
```

- 初期化プロセスをキャンセルするには、no と入力します。
- 初期化プロセスを続行するには、yes と入力します。

リポジトリを初めて初期化している場合でも、次のすべてのメッセージが表示されます。

```
(SecSvc_263) Creating new secret key...
(SecSvc_259) Deleting old repository tables...
(SecSvc_260) Creating new repository tables...
(SecSvc_261) Granting accesses to repository...
(SecSvc_251) Creating security admin: admin-name...
(SecSvc_214) Security Administrator principal: admin-name
    ...successfully created with permissions to resource domain:AdminResources
```

リポジトリが初期化されると、あらかじめ定義されたエントリのセットが作成されます。次のものがあります。

- Sun MSF リポジトリのすべてのリソース (たとえば、主体、役割、リソース、リソースドメイン)
- リソースタイプ
- アクセス権タイプ
- セキュリティー管理者主体
- Sun MSF のすべてのリソースが含まれたリソースドメイン AdminResources と、セキュリティー管理者主体に与えられているすべてのアクセス権

Sun MSF セキュリティー管理者は、これで SecAdmin アプリケーションを起動してリポジトリを生成できます。51 ページの「SecAdmin アプリケーション」を参照してください。

参考 – セキュリティーリポジトリを再初期化して削除するには、msfinitr ユーティリティーを実行し、現在の内容を破棄するかどうか尋ねられたら yes と入力します。

▼ セキュリティー管理者を作成して LDAP リポジトリを初期化する

1. `MSFconfig.properties` ファイルに正しい値が含まれていることを確認します。
2. LDAP ディレクトリ管理者から入手したスキーマのパスワードがあることを確認します。

   ディレクトリマネージャーの名前とパスワードも必要になります。ディレクトリマネージャーの名前とパスワードを使用する権限がない場合は、LDAP ディレクトリの管理者が手順 5 と手順 6 でこのタスクを実行する必要があります。

   18 ページの「セキュリティーリポジトリとしての LDAP ディレクトリの設定」を参照してください。

   注 – `MSFconfig.properties` ファイルでパスワードの最大長を設定した場合は、指定した長さ以内にする必要があります。

3. 設定ファイルを使用して、Sun MSF スーパー管理者の環境を設定します。

   この設定ファイルで必要な値については、21 ページの「Sun MSF スーパー管理者」を参照してください。

4. 次のコマンドを使用して、ログサーバーを起動します。

```
$ msflog -s
```

   ログサーバーの管理については、93 ページの「セキュリティーログ収集の管理」を参照してください。

5. 次のコマンドを実行し、Sun MSF スキーマを作成します。

```
$ msfldapschema

Enter directory manager's name: name
Enter directory manager's password: password

msfldapschema completed successfully.
```

注意 – このコマンドはディレクトリ全体のスキーマを変更します。したがって、ディレクトリマネージャーとして実行する必要があり、LDAP の 1 つのインストールにつき 1 回だけ実行します。ディレクトリマネージャーでない場合は、ディレクトリマネージャーと一緒にこの操作を実行してください。

6. 次のコマンドを実行してディレクトリを初期化します。

```
$ msfldapcr suffix

Enter directory manager's name: name
Enter directory manager's password: password
```

suffix の値は com.sun.emp.security.adapterRoot プロパティーの最初のコンポーネントになる場合がありますが、有効であればどんな名前でも入力できます。データベース接尾辞 ldbm の詳細については、LDAP ディレクトリのマニュアルを参照してください。

7. プロンプトで管理者パスワードの入力を求められたら、Sun MSF セキュリティー管理者のパスワードを入力します。

```
(SecSvc_250) Security ADMIN name: admin-name
(SecSvc_253) Enter security ADMIN password (or quit):
```

8. プロンプトでエンドユーザーのパスワードの入力を求められたら、エンドユーザーのパスワードを入力します。

```
(SecSvc_250) Security END USER name: user-name
(SecSvc_253) Enter security END USER password (or quit):
```

管理者とエンドユーザーのパスワードを入力すると、次のメッセージが表示されます。

```
(SecSvc_INFO) CreateLdapRepository completed successfully.
```

9. コマンドプロンプトで、msfinitr コマンドを実行します。

```
$ msfinitr admin-domain
```

admin-domain 引数のデフォルトは AdminResources です。これは、セキュリティー管理者が使用する Sun MSF のリソースがすべて含まれたリソースドメインの名前です。

次のメッセージとプロンプトが表示されます。

```
(SecSvc_262) Loading security configuration data...

(SecSvc_250) Security SCHEMA name: schema-name
(SecSvc_253) Enter security SCHEMA password (or quit):
```

10. **ディレクトリ管理者から入手したスキーマのパスワードを入力します。**

    18 ページの「セキュリティーリポジトリとしての LDAP ディレクトリの設定」を参照してください。

11. **プロンプトで管理者のパスワードの入力を求められたら、手順 7 で入力したパスワードを入力します。**

```
(SecSvc_250) Security ADMIN name: admin-name
(SecSvc_253) Enter security ADMIN password (or quit):
```

12. **プロンプトでエンドユーザーのパスワードの入力を求められたら、手順 8 で入力したパスワードを入力します。**

```
(SecSvc_250) Security END USER name: user-name
(SecSvc_253) Enter security END USER password (or quit):
```

13. **リポジトリがすでに存在する場合は、次のメッセージに応答する必要があります。**

```
(SecSvc_213) Repository not empty;
    ... ... do you want to destroy current contents and reinitialize (yes/no)?
```

- 初期化プロセスをキャンセルするには、`no` と入力します。
- 初期化プロセスを続行するには、`yes` と入力します。

リポジトリを初めて初期化している場合でも、次のすべてのメッセージが表示されます。

```
(SecSvc_263) Creating new secret key...
(SecSvc_259) Deleting old repository tables...
(SecSvc_260) Creating new repository tables...
(SecSvc_261) Granting accesses to repository...
(SecSvc_251) Creating security admin: admin-name...
(SecSvc_214) Security Administrator principal: admin-name
    ...successfully created with permissions to resource domain:AdminResources
```

リポジトリが初期化されると、あらかじめ定義されたエントリのセットが作成されます。次のものがあります。

- Sun MSF リポジトリのすべてのリソース (たとえば、主体、役割、リソース、リソースドメイン)
- リソースタイプ
- アクセス権タイプ
- セキュリティー管理者主体
- Sun MSF のすべてのリソースが含まれたリソースドメイン AdminResources と、セキュリティー管理者主体に与えられているすべてのアクセス権

Sun MSF セキュリティー管理者は、これで SecAdmin アプリケーションを起動してリポジトリを生成できます。詳細は、51 ページの「SecAdmin アプリケーション」を参照してください。

参考 – セキュリティーリポジトリを再初期化して削除するには、`msfinitr` ユーティリティーを実行し、現在の内容を破棄するかどうか尋ねられたら `yes` と入力します。

第5章

リポジトリの生成と管理

リポジトリを初期化したあと、通常セキュリティー管理者はこの節で説明するタスクを実行します。セキュリティー管理者が Sun MSF のコマンドやユーティリティーを実行するためには、まず環境を設定する必要があります。21 ページの「管理者の設定ファイルの作成」を参照してください。

この章の内容は、次のとおりです。

主体の追加

主体をリポジトリに追加する際、ユーザー名とパスワードを指定する必要があります。オプションで、パスワードが有効な最大日数と最小日数、つまりパスワードの有効期限とユーザーを停止するかどうかを指定できます。また、主体に関する説明を含めることもできます。

パスワードが有効な最大日数と最小日数、つまりパスワードの有効期限または停止状態を指定しない場合、主体は `MSFconfig.properties` ファイルで定義された設定でリポジトリに追加されます。

68 ページの「createPrincipal」を参照してください。

主体をリポジトリに追加したあと、次の作業ができます。

- パスワードの有効期間と有効期限を変更する。
- 主体を停止または有効にする。
- 主体を削除する
- 主体を 1 つまたは複数の役割に割り当てる。
- 主体の一次役割を設定または削除する。これは主体のデフォルトの役割です。
- 主体のアクセス権をリソースドメインに割り当てる。
- リソースドメインへのアクセス権を削除する。

役割の追加

主体が実行する必要のある操作を判断し、主体を役割に分類する方法を決定したら、役割の作成を開始できます。役割を作成する際、名前と説明を指定する必要があります。72 ページの「createRole」を参照してください。

役割を作成したあと、次の作業ができます。

- 役割を削除する。
- 主体を役割に追加する。
- 役割のアクセス権をリソースドメインに割り当てる。これで、この役割に属する主体がドメインのリソースにアクセスできるようになります。
- リソースドメインへのアクセス権を削除する。
- 親の役割を定義する。親の役割は役割の階層を構成します。親の役割は多くの役割の親になれます。83 ページの「setRoleParent」を参照してください。

図 5-1 に、役割の階層関係を示します。この図では、財務の役割は人事部門と総勘定元帳の両方の役割の親です。総勘定元帳の役割には、2 つの子の役割があります。買掛勘定と売掛勘定です。買掛勘定と売掛勘定の役割のいずれかに属する主体は、その役割のアクセス権のみを持ちます。一方、総勘定元帳の役割に属する主体は、その役割のアクセス権と子の役割のアクセス権を持ちます。

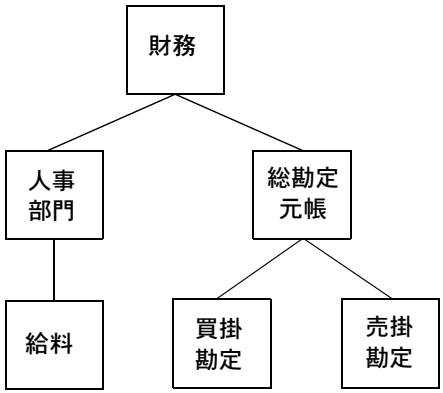

図 5-1　　役割の階層関係

LDAP ディレクトリリポジトリ:

LDAP ディレクトリをリポジトリとして使用している場合は、上位から下位に向かって役割の階層を構築する必要があります。親のいない役割は階層の最上位に位置します。たとえば、図 5-1 の財務がそうです。ほかの役割の親を構成する場合は、上位から下位に向かって順に割り当てていく必要があります。たとえば、人事部門を給料の親の役割として設定するには、その前に財務を人事部門の親の役割に設定する必要があります。親の役割を削除したり変更したりできるのは、それが階層の最下位にある場合のみです。

階層の中間位置にある親の役割を変更する場合は、変更の影響を受ける、下位にある子の役割をすべて削除する必要があります。親の役割を変更し終えたら、子の役割を作成し直し、新しく作成した階層の全レベルにわたって親の役割を割り当てる必要があります。たとえば、総勘定元帳役割が財務役割の下位レベルではなくなって総勘定元帳役割を変更する必要が生じた場合は、売掛勘定役割と買掛勘定役割を先に削除する必要があります。そのあとで、親役割である総勘定元帳をヌルに変更します。次に、売掛勘定役割と買掛勘定役割を作成し直します。最後に、両者の親役割を総勘定元帳に設定します。

RDBMS リポジトリ:

RDBMS をリポジトリとして使用している場合は、どんな順番で役割の階層を構築し、親役割を変更してもかまいません。

リソースの追加

リソースをリポジトリに追加するには、リソースタイプ、リソース名、および説明を指定する必要があります。

セキュリティーリポジトリを初期化すると、一連のリソースタイプがデフォルトで含まれています。次の表に、リソースタイプとそれに対応する Sun MTP Secure リソースクラスを示します。また、リソースクラスごとに確認を実行するかどうかを制御する Sun MTP Secure 環境変数も示します。

表 5-1 Sun MSF リソースタイプと Sun MTP Secure リソースクラスタイプ

Sun MSF リソースタイプ	Sun MTP Secure リソースクラスタイプ	Sun MTP Secure 環境変数
KIX_FILE	KIX-FILES	KIXFCTSEC
KIX_START_TRANS	KIX-START-TRANS	KIXSTTSEC
KIX_ATTACH_TRANS	KIX-ATTACH-TRANS	KIXPCTSEC
KIX_PROGRAM	KIX-PROGRAMS	KIXPPTSEC
KIX_TERMINAL	KIX-TERMINALS	KIXTCTSEC
KIX_TDQUEUE	KIX-TD-QUEUE	KIXDCTSEC
KIX_TSQUEUE	KIX-TS-QUEUE	KIXTSTSEC
KIX_JOURNAL	KIX-JOURNALS	KIXJCTSEC
KIX_COMMANDS	KIX-COMMANDS	KIXCMDSEC
KIX_REGION	UNIX-APPLS	KIXAPPSEC
ObjectReference	n/a	n/a
役割	n/a	n/a
主体	n/a	n/a
ResourceDomain	n/a	n/a
リソース	n/a	n/a
PermissionType	n/a	n/a
ResourceType	n/a	n/a

KIX_* リソースタイプについては、『Sun Mainframe Transaction Processing ソフトウェア 管理者ガイド』で説明します。独自のリソースタイプを定義するには、71 ページの「createResourceType」を参照してください。

注 – 表 5-1 に掲載されていないリソースタイプは、ユーザー定義のリソースタイプと見なされます。

リソースを作成したら、アクセス権を割り当てられるように、それをリソースドメインに追加する必要があります。

リソースドメインの追加

リソースドメインは、アクセス権の要件が共通するリソースの集まりです。リソースドメインを作成するときに、ドメイン名と説明を指定する必要があります。

ドメインを作成したあと、次の作業ができます。

- ドメインにリソースを追加する。
- ドメインからリソースを削除する。
- ドメインへのアクセス権を主体と役割に与える。
- ドメインへのアクセス権を主体と役割から削除する。
- ドメインを削除する。
- リソースドメインの親を設定する。親ドメインはリソースドメインの階層を構成します。親ドメインは多くのリソースドメインの親になれます。82 ページの「setResourceDomainParent」を参照してください。

図 5-2 に、リソースドメインの階層関係を示します。この図では、財務ファイルリソースドメインは、人事部門ファイルと GL ファイルリソースドメイン両方の親です。GL ファイルリソースドメインは、AP ファイルと AP ファイルの 2 つの子リソースドメインがあります。これらのリソースドメインのいずれかへのアクセス権を持つ主体または役割のみが、そのリソースドメインのリソースへのアクセス権を持ちます。一方、GL ファイルリソースドメインへのアクセス権を持つ主体または役割は、そのリソースドメインのリソースへのアクセス権と、子リソースドメインのリソースへのアクセス権を持ちます。

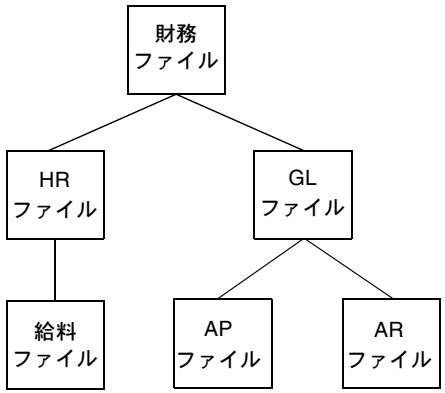

図 5-2　　リソースドメインの階層関係

LDAP ディレクトリリポジトリ:

LDAP ディレクトリをリポジトリとして使用している場合は、上位から下位に向かってリソースドメインの階層を構築する必要があります。親のいないリソースドメインは階層の最上位に配置します。たとえば、図 5-1 の「財務ファイル」がそうです。ほかのリソースドメインの親のリソースドメインを構成する場合は、上位から下位に向かって順に割り当てていく必要があります。たとえば、「HR ファイル」を「給料ファイル」の親のリソースドメインとして設定するには、その前に「財務ファイル」を「HR ファイル」の親のリソースドメインに設定する必要があります。親のリソースドメインを削除したり変更したりできるのは、それが階層の最下位にある場合のみです。

階層の中間位置にあるリソースドメインの親を変更する場合は、変更の影響を受ける、下位にある子のリソースドメインをすべて削除する必要があります。親のリソースドメインを変更し終えたら、子のリソースドメインを作成し直し、新しく作成した階層の全レベルにわたって親のリソースドメインを割り当てる必要があります。たとえば、「GL ファイル」リソースドメインが「財務ファイル」リソースドメインの下位レベルではなくなって「GL ファイル」リソースドメインを変更する必要が生じた場合は、「AP ファイル」リソースドメインと「AR ファイル」リソースドメインを先に削除する必要があります。そのあとで、親リソースドメインである「GL ファイル」をヌルに変更します。次に、「AP ファイル」リソースドメインと「AR ファイル」リソースドメインを作成し直します。最後に、両者の親リソースドメインを「GL ファイル」に設定します。

RDBMS リポジトリ:

RDBMS をリポジトリとして使用している場合は、どんな順番でリソースドメインの階層を構築し、親リソースドメインを変更してもかまいません。

主体と役割へのアクセス権の追加

主体または役割にアクセス権を追加すると、リソースドメインへの特定のアクセス権を与えることになります。これらのアクセス権は、1 つまたは複数の**アクセス権タイプ**で構成されます。リポジトリを初期化すると、アクセス権タイプのデフォルトのセットが追加されます。アクセス権タイプには、読み取り、書き込み、実行、管理があります。独自のアクセス権タイプも作成できます。67 ページの「createPermissionType」を参照してください。

主体や役割にアクセス権を追加するには、主体または役割の名前、リソースドメインの名前、1 つ以上のアクセス権タイプを指定する必要があります。

リポジトリへの複数オブジェクトの追加

多数のオブジェクトを一度にリポジトリに追加したい場合があります。SecAdmin の `loadFile` コマンドは、SecAdmin コマンドのテキストファイルを読み取り、オブジェクトをリポジトリに追加します。

テキストファイルには、同じタイプのエントリが含まれている必要はありません。たとえば、企業が新しいアプリケーションを導入する場合、リソースドメインとリソースを追加するコマンドを含んだテキストファイルを作成できます。これを行う場合は、リソースをリソースドメインに追加するコマンドの前に、リソースドメインを作成するコマンドがあることを確認してください。テキストファイルには、ほかのテキストファイルの `loadFile` コマンドを含めて、それぞれに SecAdmin の一連のコマンドを含めることができます。

リポジトリを最初に生成するとき、Sun MTP Sign-On Table (SNT) ですでにユーザーが定義されている場合は、`SecAdmin` プロンプトで各ユーザーをリポジトリに手動で追加するか、次の手順に従ってユーザーを一度に追加することができます。

▼ snt.lst ファイルを使用して複数のオブジェクトを追加する

1. **SNT を開き、テーブルをエクスポートします。**

   これで、snt.lst という名前の ASCII ファイルが作成されます。

2. **ファイルを編集して、各エントリに正しい createPrincipal 構文が含まれるようにします。**

   SNT を再度エクスポートする場合は、ファイルの名前を変更すれば、上書きされません。

3. **SecAdmin プロンプトで、このテキストファイルの名前で loadFile コマンドを入力します。**

   SNT エントリがリポジトリに追加されます。53 ページの「loadFile」を参照してください。

セキュリティーリポジトリへの変更のコミットと有効化

変更のコミットは RDBMS リポジトリと LDAP リポジトリで異なります。

RDBMS を使用している場合、SecAdmin ツールを使用してリポジトリに変更を加えると、それをコミットするか、変更をすべて破棄してロールバックするまで、変更はメモリに保存されます。SecAdmin アプリケーションの commit コマンドと rollback コマンドで、この操作を実行できます。複数の変更を加える場合は、それらを定期的にコミットして、予期しないエラーが生じても変更が失われないようにしてください。

LDAP ディレクトリを使用している場合は、変更のトランザクションを制御できません。各コマンドは実行に成功した時点で変更がコミットされます。RDBMS を実装している場合と異なり、変更をロールバックする機能はありません。したがって、SecAdmin の commit コマンドと rollback コマンドは機能せず、使用するとエラーが生成されます。たとえば、createPrincipal コマンドを使って主体を作成してから変更が必要になった場合は、deletePrincipal を実行して、その主体をリポジトリから削除する必要があります。

リポジトリのオブジェクトの一覧表示

SecAdmin アプリケーションには、リポジトリのオブジェクトをタイプ別に表示するコマンドと、役割とリソースドメインのテキストダイアグラムを表示するコマンドが用意されています。`listPrincipalsWithNoRole` と `listResourcesWithNoDomain` を除く `list*` コマンドでは、オブジェクトの全一覧の要求や検索文字列の入力ができます。出力の詳細レベルは、何を一覧表示するかによって異なります。`list*` コマンドには次のものがあります。

- `listPrincipals`
- `listPrincipalsWithNoRole`
- `listResourcesWithNoDomain`
- `listRoles`
- `listResourceDomains`
- `listResourceTypes`
- `listResources`
- `listPermissionTypes`

`print*` コマンドは、リポジトリの役割とリソースドメインのテキストダイアグラムを階層構造で表示します。

- `printRoleTree` コマンドは、役割間の関係と、それぞれに割り当てられた主体が一目でわかるツリーダイアグラムを表示します。
- `printDomainTree` コマンドは、下位のすべてのドメイン、および各ドメインに関連付けられたリソースタイプとリソースを一覧にしたリソースドメインのツリーダイアグラムを表示します。

リポジトリからのオブジェクトの削除

リポジトリからオブジェクトを削除しても、そのままアプリケーション環境に存在できます。たとえば、リポジトリから VSAM ファイルを削除した場合、それは Sun MTP File Control Table (FCT) からは削除されません。リポジトリからオブジェクトを削除すると、Sun MSF を使用しているアプリケーションからリソースとしてアクセスできなくなるという意味です。

役割とリソースドメインの階層を設定したあと、中間の役割やリソースドメインを削除する場合は、下位レベルを先に削除する必要があります。

役割の削除

図 5-3 に、主体、役割、およびリソースドメインの依存関係を示します。このダイアグラムで、R は読み取り権、RW は読み取り権と書き込み権という意味です。

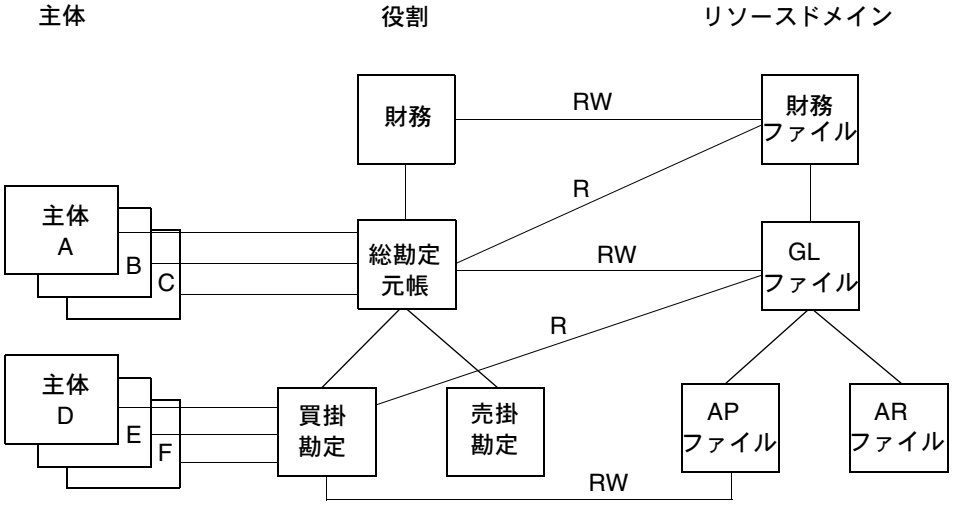

図 5-3 主体、役割、リソースドメインの相互関係

総勘定元帳の役割を削除する場合は、最初に買掛勘定と売掛勘定を削除する必要があります。これらの役割を削除すると、主体のすべてがそれらの役割との関連付けを失うため、財務ファイルドメインとその子ドメインすべてへのアクセス権を失います。図 5-4 に、これらの役割を削除した結果を示します。主体を新しい役割に再割り当てするのは、管理者の役目です。`listPrincipalsWithNoRole` コマンドは、役割を持たない主体を探す場合に使用します。

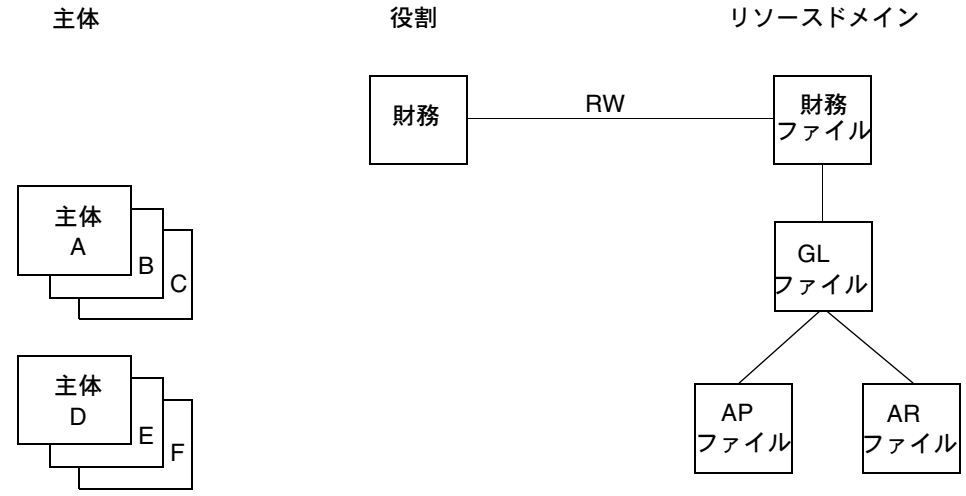

図 5-4　　役割を削除した結果

リソースドメインの削除

図 5-5 に、主体、役割、およびリソースドメインの依存関係を示します。このダイアグラムで、R は読み取り権、RW は読み取り権と書き込み権という意味です。

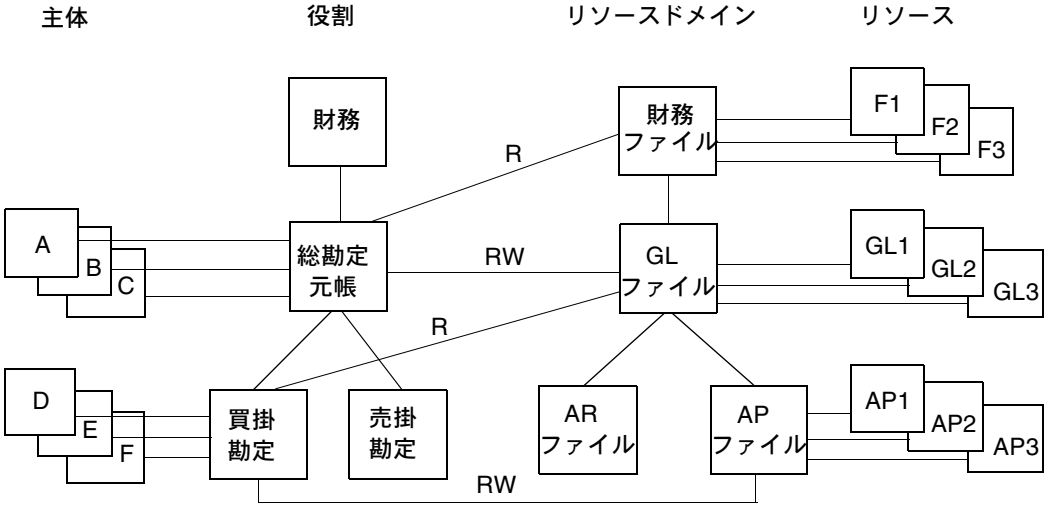

図 5-5　　主体、役割、ドメイン、リソースの相互関係

GL ファイルドメインを削除する場合は、最初に AR ファイルと AP ファイルのドメインを削除する必要があります。これらのドメインを削除すると、総勘定元帳、買掛勘定、および売掛勘定の各役割が VSAM データセット GL1、GL2、および GL3 と、AP1、AP2、および AP3 へのアクセス権を失います。リソース GL1、GL2、GL3 と AP1、AP2、および AP3 が別のドメインに追加されるまでは、それらにアクセスできません。図 5-6 に、ドメインを削除した結果を示します。親がなくなったリソースをドメインに再割り当てして、役割や主体のアクセス権でアクセスできるようにするのは、管理者の役目です。listResourcesWithNoDomain コマンドを使用すると、このような親がなくなったリソースを探すことができます。

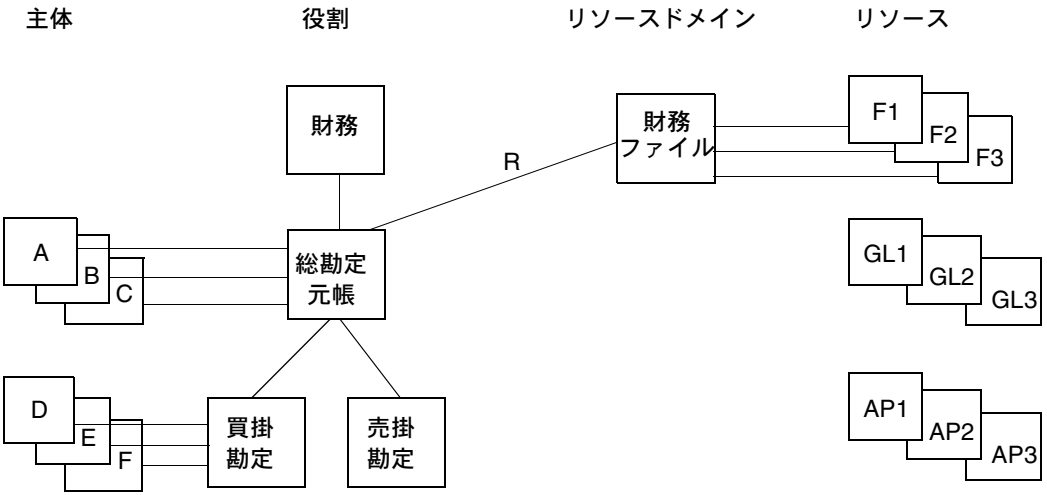

図 5-6 役割を削除した結果

SecAdmin アプリケーション

セキュリティー管理者は SecAdmin ツールを使用して、セキュリティーリポジトリに設定されているコンポーネントの追加、変更、削除、および一覧表示ができます。この節では、SecAdmin コマンドについて説明し、各コマンドの出力例を示します。

▼ SecAdmin セッションを開始する

1. **環境を設定します。**

   21 ページの「管理者の設定ファイルの作成」を参照してください。

2. **次のコマンドを入力します。**

```
$ msfadmin
```

3. `MSF Login username` **プロンプトが表示されたら、セキュリティー管理者のユーザー名を入力します。**

4. `MSF Login password` **プロンプトが表示されたら、セキュリティー管理者のパスワードを入力します。**

   ユーザー名またはパスワードが有効でない場合、次のメッセージが表示されて、アプリケーションが終了します。

```
[SecAdmin] Username or password provided is not valid
```

   ユーザー名とパスワードが有効な場合は、次のヘッダーとプロンプトが表示されます。

```
================================================================================
| Copyright (c) 2002 by Sun Microsystems, Inc. all rights reserved.            |
| Welcome to SecAdmin, the security administration command-line tool           |
|     Enter 'help' to see a list of commands, or 'help,<command>' for          |
|     help on a specific command.                                              |
================================================================================

SecAdmin:
```

   これでコマンドをサブミットできるようになります。コマンドが完了すると、`SecAdmin` プロンプトに戻ります。

SecAdmin コマンド

次のコマンド説明では、コマンドの省略形式も示します。SecAdmin プロンプトは表示されません。

help

使用できる SecAdmin コマンドを一覧表示します。

構文

```
help

?
```

出力

```
[SecAdmin] Commands:
loadFile (lf) ----------------------- load a file containing commands
listSummary (ls) -------------------- gives a summary of security system
listPrincipalsWithNoRole (lpwnr)----- list principals with no primary role
listPrincipals (lpr) ---------------- list all principals
listRoles (lrol) -------------------- list all roles
listResourceDomains (lrd) ----------- list all resource domains
listResources (lrs) ----------------- list all resources
listResourcesWithNoDomain (lrwnd) --- list resources with no domain
listResourceTypes (lrt) ------------- list all resource types
listPermissionTypes (lpt) ----------- list all permission types

addPrincipalPermissions (app) ------- give principal permissions
addPrincipalToRole (apr) ------------ give principal a role
addRolePermissions (arp) ------------ give role permissions
addResourceToDomain (ard) ----------- give resource a domain

createPermissionType (cpt) ---------- create a permission type
createPrincipal (cpr) --------------- create a principal
createResource (crs) ---------------- create a resource
createResourceDomain (crd) ---------- create a resource domain
createResourceType (crt) ------------ create a resource type
createRole (crol) ------------------- create a role

deletePermissionType (dpt) ---------- delete a permission type
deletePrincipal (dpr) --------------- delete a principal
```

```
deleteResource (drs) ---------------- delete a resource
deleteResourceDomain (drd) ---------- delete a resource domain
deleteResourceType (drt) ------------ delete a resource type
deleteRole (drol) ------------------- delete a role

enablePrincipal (epr) --------------- enable principal
modifyExpDate (med) ----------------- modify principal's exp date
suspendPrincipal (susp) ------------- suspend principal

printRoleTree (prt) ----------------- print role's hierarchy
printDomainTree (pdt) --------------- print domain's hierarchy

removePrincipalFromRole (rpfr) ------ remove principal from role
removePrincipalPermissions (rpp) ---- remove principal permissions
removeResourceFromDomain (rrfd) ----- remove resource from domain
removeRolePermissions (rrp) --------- remove role permissions

resetPassword (rpw) ----------------- reset password
resetPasswordDuration (rpd) --------- reset password duration

setPrimaryRole (spr) ---------------- set principal primary role
setResourceDomainParent (srdp) ------ set Resource Domain Parent
setRoleParent (srp) ----------------- set a role's parent

commit (com) ------------------------ commit all changes
rollback (roll) --------------------- rollback all changes since commit
quit (q) ---------------------------- exit SecAdmin
```

loadFile

セキュリティーコンポーネントの作成と設定を行うために、SecAdmin コマンドのテキストファイルを読み込みます。`loadFile` コマンドを使用すると、一部のコマンドで発生するダイアログがすべて無効になります。たとえば、ファイルに主体の一次役割を設定するコマンドが含まれているとき、役割がすでに設定されている場合は、操作を確認するために表示されるプロンプトが表示されなくなります。

次のファイルには、主体、役割、リソースドメインを作成するコマンドが含まれています。

```
*These are some create commands
cpr,doreen,password,2002-12-31,100,10,F,Principal abcxyz1
crol,rolexyz,Role X-Y-Z
crd,resDom1,This is Resource Domain #1
```

注 – コメントをテキストファイルに含めるには、コメント行の列「1」に * または # と入力します。

loadFile コマンドで読み込むテキストファイルには、それぞれに SecAdmin コマンド一式が含まれたテキストファイルのリストを含めることができます。例:

```
/home/user2/roles.txt
/home/user2/principals.txt
/home/user2/resdoms.txt
/home/user2/files.txt
/home/user2/programs.txt
```

構文

loadFile,*filename*

lf,*filename*

出力

/home/user2/sec_input.txt 入力ファイルで loadFile コマンドを発行すると、次の出力が表示されます。

```
SecAdmin:lf,/home/user2/sec_input.txt

[SecAdmin]: loadFile
File Name:/home/user2/sec_input.txt

[SecAdmin]: createPrincipal
[cpr,doreen,password,2002-12-31,100,10,F,Principal abcxyz1]
[SecAdmin]:Success creating principal:doreen

[SecAdmin]: createRole
[crol,rolexyz,Role X-Y-Z]
[SecAdmin]:Success creating role:rolexyz

[SecAdmin]: createResourceDomain
[crd,resDom1,This is Resource Domain #1]
[SecAdmin]:Success creating resource domain:resDom1
```

出力メッセージは画面と同様に、メッセージログにも書き込まれます。そのため、ログでコマンドのエラーを確認できます。

listSummary

上位レベルで構成されているコンポーネントである、役割、主体、リソース、リソースタイプ、アクセス権タイプ、リソースドメインの概要リストを表示します。

構文

```
listSummary

ls
```

出力

```
[SecAdmin] listSummary
============================================================
Global Attributes:
       Default Password Expires Date:2002-09-01
       Default Password Max Days Allowed:20
       Default Password Min Days Required:2
       Default Suspend State:F
       Login failures limit:2
       Password format:MIXED_OK
       Password Minimum Length:3
       Password Maximum Length:8
Number of Principals With No Role:
======================================
       25
Root Level Roles:
======================================
       newrole
 (+)role1
 (+)role4
Resources Types:
======================================
       Group
       KIX_ATTACH_MTP
       KIX_COMMAND
       KIX_FILE
       KIX_JOURNAL
       KIX_PROGRAM
       KIX_REGION
       KIX_START_MTP
       KIX_TDQUEUE
       KIX_TERMINAL
       KIX_TSQUEUE
       ObjectReference
```

```
       Principal
       Resource
       ResourceDomain
       Role
Number of Resources With No Domain:
=====================================
       14
Root Level Resource Domains:
=====================================
 (+)rd1
       rd3
 (+)rd4
Permission Types:
=====================================
       EXECUTE
       MANAGE
       READ
       WRITE
```

listPrincipalsWithNoRole

役割に割り当てられていない 1 つ以上の主体を一覧表示します。

構文

```
listPrincipalsWithNoRole
```

```
lpwnr
```

出力

```
[SecAdmin]: listPrincipalsWithNoRole
Principals With No Role:
=====================================
       angie
       dennis
       linda
```

listPrincipals

listPrincipals コマンドでは、すべての list コマンドと同様に、次の 3 つの機能を使用できます。

- すべての項目を一覧表示する (主体の場合)。この機能を使用するには、listPrincipals だけを入力します。
- 1 つの項目のみを表示する。たとえば、listPrincipals,steve と入力すると、Steve の詳細すべてが表示されます。
- 検索文字列と一致するすべての項目を検索する。たとえば、listPrincipals,s* と入力すると、名前の先頭に *s* が付いた主体すべてが一覧になります。

注 – このリリースでは、アスタリスク (*) だけがワイルドカードとしてサポートされています。

構文

listPrincipals[,*principalname*|*searchstring*]

lpr[,*principalname*|*searchstring*]

出力

次に、listPrincipals コマンドの出力例を示します。

```
Principals:
=======================================
       angie
       dennis
       linda
       secureguy
       shanan
       steve
```

次に、listPrincipals,steve コマンドの出力例を示します。リポジトリに目的の主体が存在する場合は、このコマンドによってその主体の詳細が表示されます。

```
[SecAdmin]: listPrincipals
       Principal Name:steve
        Primary Role:newrole
       Roles:
              role#0:newrole
              role#1:role1
       Suspended State:false
       Password Expiration Date:2005-08-31
       Maximum Password Duration:100
       Minimum Password Duration:10
       Description:Steve the security guy
       Granted Permissions:
```

最後に、検索文字列と listPrincipals コマンドを実行した出力例を示します。検索文字列は名前の一部でもかまいません。たとえば、listPrincipals,s* と入力すると、名前の先頭に s が付いた主体がすべて表示されます。

```
[SecAdmin] Principals matching 's*':
       secureguy
       shanan
       steve
```

listRoles

1 つまたは複数の役割エントリを一覧にします。役割名または検索文字列を指定しなかった場合は、listRoles によってすべての役割が返されます。

構文

listRoles[,*rolename*|*searchstring*]

lrol[,*rolename*|*searchstring*]

出力

役割名を指定すると、次の出力が表示されます。

```
SecAdmin:listRoles,role1
[SecAdmin] listRole for:role1
       Role Name:role1
       Parent Role: NULL
       Principals:
           principals#0:dennis
           principals#1:steve
       Sub-Roles:
           subRole#0:newrole
       Description:Role1
       Granted Permissions:
```

検索文字列を使用して役割名を指定すると (role* など)、次の出力が表示されます。

```
SecAdmin:listRoles,role*
[SecAdmin] Roles matching 'role*':
       role1
       role2
       role3
       role4
```

一致する名前が見つからない場合は、出力が得られません。

listResourceDomains

1 つまたは複数のリソースドメインエントリの概要リストが表示されます。

構文

`listResourceDomains[,`*resourcedomain*`|`*searchstring*`]`

`lrd[,`*resourcedomain*`|`*searchstring*`]`

出力

listResourceDomains コマンドにパラメータを付けない場合は、次のような出力が表示されます。

```
ResourceDomains:
    AdminResources
    FinancialResources
    ManagerResources
    TellerResources
```

lrd,AdminResources コマンドを実行すると、次のような出力結果になります。

```
[SecAdmin] listResourceDomain for: AdminResources
       Resource Domain Name:AdminResources
       Parent Domain: NULL
       Resources:
           resource#0:ApplicationRule,*
           resource#1:CalendarRule,*
           resource#2:Group,*
           resource#3:ObjectReference,*
           resource#4:PermissionType,*
           resource#5:Principal,*
           resource#6:Resource,*
           resource#7:ResourceDomain,*
           resource#8:ResourceType,*
           resource#9:Role,*
       Principals w/ Granted Permissions:
           principal#0:dsadmin
       Roles w/ Granted Permissions:
           NO Roles w/ Granted Permissions
       Sub-Domains:
           NO DOMAINS
       Description:Resources for this Administrator
```

検索文字列 (たとえば、lrd,*i*) でコマンドを実行すると、次のような出力が表示されます。

```
[SecAdmin] Resource Domains matching '*i*':
       AdminResources
       FinancialResources
```

検索文字列を指定し、一致するドメインが見つからない場合は、SecAdmin プロンプトが表示されます。

listResources

1 つまたは複数のリソースエントリを一覧表示します。

構文

`listResources[,{`*resourcetype*`|`*searchstring*`},{`*resourcename*`|`*searchstring*`}]`

`lrs[,{`*resourcetype*`|`*searchstring*`},{`*resourcename*`|`*searchstring*`}]`

出力

パラメータを何も指定しない場合は、`listResources` によってすべてのリソースの一覧が返されます。

```
Resources:
================================================
       ApplicationRule,*
       CalendarRule,*
       Group,*
       ObjectReference,*
       PermissionType,*
       Principal,*
       Resource,*
       ResourceDomain,*
       ResourceType,*
       Role,*
       TSQUEUE,Q1PT
       TSQUEUE,Q123
       TSQUEUE,Q333
       TSQUEUE,Q555
       TSQUEUE,Q444
```

2 つの検索文字列を使用して、検索する名前の一部を指定できます。たとえば、リソースタイプ検索文字列の B* とリソース名検索文字列の A* は、タイプが B で始まり、名前が A で始まるすべてのリソースを探します。一致するタイプと名前が見つかると、そのリソースの詳細が一覧表示されます。一致する名前が見つからない場合は、出力が得られません。

listResourcesWithNoDomain

ドメインに割り当てられていないリソースを一覧表示します。

構文

```
listResourcesWithNoDomain

lrwnd
```

出力

```
Resources with no Resource Domain:
==========================================
       TSQUEUE,Q1PT
       TSQUEUE,Q333
       combinator resource,Q1PT
       description resource,Q1PT
       permission resource,Q1PT
```

出力のコンマの左側にある語はリソースタイプ、コンマの右側にある語はリソース名です。これらが合わさって、リソースを形成しています。

listResourceTypes

リポジトリのすべてのリソースタイプを一覧表示します。コマンドの省略形は、`lrt` です。

構文

```
listResourceTypes

lrt
```

出力

```
Resource Types:
================================================
       ApplicationRule
       CalendarRule
       Group
       KIX_ATTACH_TRANS
       KIX_COMMAND
       KIX_FILE
       KIX_JOURNAL
       KIX_PROGRAM
       KIX_REGION
       KIX_START_TRANS
       KIX_TDQUEUE
       KIX_TERMINAL
       KIX_TSQUEUE
       ObjectReference
       PermissionType
       Principal
       Resource
       ResourceDomain
       ResourceType
       Role
```

リソースタイプが見つからない場合は、出力が得られません。

listPermissionTypes

すべてのアクセス権タイプのエントリの概要リストを表示します。

構文

`listPermissionTypes`

`lpt`

出力

```
[SecAdmin]: listPermissionTypes
Permission Types:
=========================================
       EXECUTE
       MANAGE
       READ
       WRITE
```

アクセス権タイプが見つからない場合は、出力が得られません。

addPrincipalPermissions

指定したリソースドメインに主体のアクセス権タイプを追加します。

構文

`addPrincipalPermissions`, *principalname*, *resourcedomain*, *perm1*, . . , *permN*

`app`, *principalname*, *resourcedomain*, *perm1*, . . , *permN*

オプション	説明
principalname	主体の名前
resourcedomain	主体がアクセス権を与えられているリソースドメイン
perm1,...,permN	アクセス権のタイプを指定するテキスト文字列。複数のアクセス権がある場合は、コンマで区切る必要がある。次の中から、1 つ以上のタイプを指定する。 READ WRITE EXECUTE MANAGE ユーザーが定義したアクセス権タイプの値

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success adding Principal Permission for resourcedomain
successfully added to Principal principalname
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Principal not found: principalname
Resource Domain not found: resourcedomain
```

addPrincipalToRole

指定した主体を役割に割り当てます。

構文

`addPrincipalToRole`, *principalname*, *rolename*

`apr`, *principalname*, *rolename*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success adding principal principalname to role: rolename
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Principal not found: principalname
Role not found: rolename
```

addRolePermissions

指定したリソースドメインに役割のアクセス権タイプを追加します。

構文

addRolePermissions,*rolename*,*resourcedomain*,*perm1*,...,*permN*

arp,*rolename*,*resourcedomain*,*perm1*,...,*permN*

オプション	説明
rolename	役割の名前
resourcedomain	役割がアクセス権を与えられているリソースドメイン
perm1,...,permN	アクセス権のタイプを指定するテキスト文字列。複数のアクセス権がある場合は、コンマで区切る必要がある。次の中から、1 つ以上のタイプを指定する。 READ WRITE EXECUTE MANAGE ユーザーが定義したアクセス権タイプの値

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success adding permissions for role: rolename to domain:
resourcedomain
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Role: rolename not found.
Resource Domain: resourcedomain not found.
Permission Type: permissiontype not found.
```

addResourceToDomain

リソースをリソースドメインに追加します。

注 – リソースは別のドメインに追加する前に、既存のドメインから削除する必要があります。

構文

`addResourceToDomain`, *resourcetype* , *resourcename* , *resourcedomain*

`ard`, *resourcetype* , *resourcename* , *resourcedomain*

出力

コマンドが成功すると、次のメッセージが表示されます。

`Success adding resource:` *resourcetype,resourcename* `to domain:` *resourcedomain*

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

`Resource not found:` *resourcetype,resourcename*

`Resource type not found:` *resourcetype*

`Resource:` *resourcetype* , *resourcename* `already belongs to domain:` *resourcedomain*

createPermissionType

新しいアクセス権タイプを作成します。

構文

`createPermissionType`, *permissiontype* , *description*

`cpt`, *permissiontype* , *description*

出力

コマンドが成功すると、次のメッセージが表示されます。

`Success creating permission type:` *permissiontype*

このアクセス権タイプがすでにリポジトリに存在する場合は、次のメッセージが表示されます。

```
Permission type: permissiontype already exists (try a different
name)
```

createPrincipal

リポジトリの主体にエントリを作成します。

注 – Sun MTP アプリケーションを使用する主体のパスワードの長さは、1 ～ 8 文字です。

構文

`createPrincipal,`*principalname*`,`*password*`,[`*p/w exp date*`],[`*p/w max days*`],[`*p/w min days*`],[T|F|M],`*description*

`cpr,`*principalname*`,`*password*`,[`*p/w exp date*`],[`*p/w max days*`],[`*p/w min days*`],[T|F|M],`*description*

オプション	説明
principalname	主体の名前
password	主体のパスワード
p/w exp date	パスワードが期限切れになる日付。次の形式を使用します。 *YYYY-MM-DD* NULL 値も使用できます。
p/w max days	パスワード変更期限までの最大日数。 ゼロ (0) を指定すると、主体はパスワードを変更する必要がありません。 このオプションが設定されていない場合、最大日数は `MSFconfig.properties` ファイルに設定されている値に基づいて決定されます。

オプション	説明
p/w min days	パスワード変更間隔の最小日数 ゼロ (0) を指定すると、主体はパスワードを変更する必要がありません。 このオプションが設定されていない場合、最小日数は MSFconfig.properties ファイルに設定されている値に基づいて決定されます。
T|F|M	主体を停止するかどうかを示します。 T: True は主体が停止されます。 F: False は主体が停止されません。 M: 主体は停止されませんが、最初のログインでパスワードを変更しなければなりません。 このオプションが設定されていない場合は、主体にデフォルトの停止状態が設定されます。デフォルトの状態は、MSFconfig.properties ファイルで設定されています。
説明	主体の説明

出力

主体が正常に作成されると、次のメッセージが表示されます。

```
Success creating principal: principalname
```

createPrincipal コマンドで無効な停止状態を入力した場合は、主体が作成されて、次のメッセージが表示されます。

```
WARNING: Invalid suspend state 'a'-- 'F' assumed
```

主体を作成できなかった場合は、次のいずれかのメッセージが表示されます。

```
ERROR: principal ExpDate should be: YYYY-MM-DD
```

```
ERROR: principal: principalname already exists (try a different name)
```

```
ERROR: Password format is not acceptable for principal: principalname
```

createResource

リポジトリにリソースのエントリを作成します。

構文

`createResource`, *resourcetype*, *resourcename*, *description*

`crs`, *resourcetype*, *resourcename*, *description*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success creating resource resourcetype, resourcename
```

コマンドが失敗すると、次のメッセージが表示されます。

```
Resource already exists (try a different name)
```

resourcetype は次のいずれかのテキスト文字列になります。

```
KIX-FILE
KIX-START-TRANS
KIX-ATTACH-TRANS
KIX-PROGRAM
KIX-TERMINAL
KIX-TDQUEUE
KIX-TSQUEUE
KIX-JOURNAL
KIX-COMMAND
KIX-REGION
ObjectReference
Group
Role
Principal
ResourceDomain
```

または、有効なユーザー定義の *resourcetype* になります。

createResourceDomain

リポジトリにリソースドメインのエントリを作成します。

構文

`createResourceDomain`, *resourcedomain*, *description*

`crd`, *resourcedomain*, *description*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
ResourceDomain resourcedomain successfully created
```

コマンドが失敗すると、次のメッセージが表示されます。

```
ResourceDomain: resourcedomain already exists (try a different
name)
```

createResourceType

ユーザー定義のリソースタイプを新規作成します。ユーザー定義のリソースタイプを作成すると、リソースへのアクセスをさらに細かく制御できます。たとえば、個人に関するレコードの特定のフィールドへのユーザーアクセスを制限する場合は、`persrec` という名前のリソースタイプを作成します。そのあと、このリソースタイプを使って、制御する各フィールドのリソースを作成します。次に、リソースドメインを作成し、リソースをドメインに追加します。これで、ドメインへのユーザーのアクセス権を定義できます。

構文

`createResourceType`, *resourcetypename*, *description*

`crt`, *resourcetypename*, *description*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success creating resource type: resourcetypename
```

このタイプのリソースがすでにリポジトリに存在する場合は、次のメッセージが表示されます。

```
Resource type already exists (try a different name)
```

createRole

役割のエントリをリポジトリに作成します。

構文

`createRole`,*rolename*,*description*

`crol`,*rolename*,*description*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success creating role: rolename
```

コマンドが失敗すると、次のメッセージが表示されます。

```
Role: rolename already exists (try a different name)
```

deletePermissionType

リポジトリからアクセス権タイプを削除します。

構文

`deletePermissionType`,*permissiontype*

`dpt`,*permissiontype*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success deleting permission type: permissiontype
```

このアクセス権タイプがリポジトリにない場合は、次のメッセージが表示されます。

```
Permission type not found: permissiontype
```

deletePrincipal

リポジトリから主体のエントリを削除し、役割とアクセス権への関連を削除します。

構文

`deletePrincipal`,*principalname*

`dpr`,*principalname*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success deleting Principal: principalname
```

コマンドが失敗すると、次のメッセージが表示されます。

```
Principal not found: principalname
```

deleteResource

リソースのエントリを削除し、主体、役割、リソースドメイン、アクセス権への関連を削除します。

構文

`deleteResource`,*resourcetype*,*resourcename*

`drs`,*resourcetype*,*resourcename*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success deleting resource: resourcetype,resourcename
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Resource type not found: resourcetype
Resource not found: resourcetype,resourcename
```

deleteResourceDomain

リソースドメインのエントリを削除し、リソース、親または子のリソースドメイン、アクセス権への関連を削除します。子を持つドメインを削除しようとすると、次のメッセージが表示され、ドメインは削除されません。現在のドメインを削除する前に、階層の最下位から順に子のドメインをすべて削除する必要があります。

構文

`deleteResourceDomain,`*resourcedomain*

`drd,`*resourcedomain*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success deleting ResourceDomain: resourcedomain
```

コマンドが失敗すると、次のメッセージが表示されます。

```
ResourceDomain: resourcedomain not found
```

子を持つドメインを削除しようとすると、次のメッセージが表示されます。

```
Domain not deleted because children present
```

deleteResourceType

リソースタイプを削除します。

構文

`deleteResourceType,`*resourcetypename*

`drt,`*resourcetypename*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success deleting resource type: resourcetypename
```

このタイプのリソースがリポジトリにない場合は、次のメッセージが表示されます。

```
Resource type not found: resourcetypename
```

deleteRole

リポジトリから役割のエントリを削除し、主体、役割、アクセス権への関連をすべて削除します。子を持つ役割を削除しようとすると、次のメッセージが表示され、役割は削除されません。現在の役割を削除する前に、階層の最下位から順に子の役割をすべて削除する必要があります。

構文

deleteRole,*rolename*

drol,*rolename*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success deleting role: rolename
```

コマンドが失敗すると、次のメッセージが表示されます。

```
Role: rolename not found
```

子を持つ役割を削除しようとすると、次のメッセージが表示されます。

```
Role not deleted because children present
```

enablePrincipal

主体の状態を停止から有効に変更すると、主体は正常にログインできるようになります。

構文

enablePrincipal,*principalname*[,M|R]

epr,*principalname*[,M|R]

オプション	説明
principalname	主体の名前。
M|R	主体がパスワードを変更する必要があるかどうかを示します。 M: 主体は最初のログインでパスワードを変更しなければなりません。 R: 主体がパスワードを変更しなければならない状態をリセットし、最初のログインでパスワードを変更するという必要条件を削除します。

出力

コマンドが成功すると、次のいずれかのメッセージが表示されます。

```
Principal: principalname enabled; must change password
Principal: principalname enabled; password change not required
Principal: principalname successfully unsuspended
Principal: principalname successfully unsuspended; must change
password
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Principal: principalname not found
Principal: principalname already enabled
```

modifyExpDate

主体のパスワードの有効期限を変更します。

構文

`modifyExpDate,` *principalname* `,` *newdate*

`med,` *principalname* `,` *newdate*

newdate には次の形式を使用する必要があります。*yyyy-mm-dd*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
New date successfully set for principal: principalname
is: yyyy-mm-dd
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Please use this date format: YYYY-MM-DD
Principal: principalname not found
```

suspendPrincipal

主体のエントリを停止し、ログインの成功を認めません。

構文

`suspendPrincipal,`*principalname*

`susp,`*principalname*

出力

コマンドが成功すると、次のメッセージが表示されます。

`Success suspending Principal:` *principalname*

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

`Principal not found:` *principalname*

`Principal:` *principalname* `already suspended`

printRoleTree

役割ツリーのテキストバージョンが、ルートの役割、またはコマンド行で指定した役割から表示されます。

構文

`printRoleTree[,`*rolename*`]`

`prt[,`*rolename*`]`

出力

出力では、各下位レベルに、役割の主体の概要リストと一緒にツリーが再帰的に表示されます。

```
Role Tree:
role1-->|linda|steve
       newrole-->|doug|steve
           role4-->|wally
role2-->|dennis|angie|shanan
role3-->|dennis|shanan
```

printDomainTree

リソースドメインツリーのテキストバージョンが、ルートドメイン、またはコマンド行で指定したドメインから表示されます。

構文

`printDomainTree[,`*resourcedomain*`]`

`pdt[,`*resourcedomain*`]`

出力

出力では、各下位ノードに、リソースドメインのリソースの概要リストと一緒にツリーが再帰的に表示されます。

```
Resource Domain Tree:
rd1--> KIX-FILE,resource77| KIX-START-TRANS,resource88
       rd2--> KIX-START-MTP,resource2
rd3--> KIX-FILE,resource2
rd4--> KIX-ATTACH-TRANS,resource1
```

removePrincipalFromRole

指定した主体を役割から削除します。

構文

`removePrincipalFromRole,`*principalname*`,`*rolename*

`rpfr,`*principalname*`,`*rolename*

出力

コマンドが成功すると、次のメッセージが表示されます。

`Principal:` *principalname* `successfully removed from role:` *rolename*

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

`Principal:` *principalname* `not found.`

`Role:` *rolename* `not found.`

removePrincipalPermissions

指定したリソースドメインに対して主体が持っているアクセス権をすべて削除します。

構文

`removePrincipalPermissions`, *principalname* , *resourcedomain*

`rpp`, *principalname* , *resourcedomain*

出力

コマンドが成功すると、次のメッセージが表示されます。

`Success removing permissions for principal:` *principalname* `from domain:` *resourcedomain*

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

`Principal:` *principalname* `not found.`

`Resource Domain:` *resourcedomain* `not found.`

removeResourceFromDomain

リソースドメインから、そのリソースを削除します。

構文

`removeResourceFromDomain`, *resourcetype* , *resourcename* , *resourcedomain*

`rrfd`, *resourcetype* , *resourcename* , *resourcedomain*

出力

コマンドが成功すると、次のメッセージが表示されます。

`Success removing resource` *resourcetype,resourcename* `from domain:` *resourcedomain*

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

`Resource not found:` *resourcename*

`Resource Domain not found:` *resourcedomain*

`Resource type not found:` *resourcetype*

removeRolePermissions

指定したリソースドメインに対して役割が持っているアクセス権をすべて削除します。

構文

`removeRolePermissions`, *rolename*, *resourcedomain*

`rrp`, *rolename*, *resourcedomain*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Success removing permissions for Role rolename from domain:
resourcedomain
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
ResourceDomain: resourcedomain not found
Role: rolename not found
```

resetPassword

主体のエントリに新しいパスワードを設定します。

注 – Sun MTP アプリケーションを使用する主体のパスワードの長さは、1 ～ 8 文字です。

構文

`resetPassword`, *principalname*, *newPassword*

`rpw`, *principalname*, *newPassword*

出力

パスワードが正常にリセットされると、次のメッセージが表示されます。

```
Principal principalname successfully updated with new password
```

パスワードのリセットに失敗すると、次のいずれかのメッセージが表示されます。

```
ERROR: Principal principalname not found
```

```
ERROR: Password format is not acceptable for principal:
principalname
```

resetPasswordDuration

主体のエントリのパスワード有効期間をリセットします。

構文

resetPasswordDuration, *principalname* , *max_days_valid* , *min_days_in_force*

rpd, *principalname* , *max_days_valid* , *min_days_in_force*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Principal principalname successfully updated with new values
```

コマンドが失敗すると、次のメッセージが表示されます。

```
Principal not found principalname
```

```
ERROR: max_days_valid,min_days_in_force must both be numbers,
not these:max...;min...
```

setPrimaryRole

主体の一次役割を設定します。

主体をその一次役割との関連付けから解除するには、*rolename* に値を指定せずにコマンドを実行します。

構文

setPrimaryRole, *principalname*[, *rolename*]

spr, *principalname*[, *rolename*]

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Principal: principalname now has primary role set from:rolename (or
null) to:rolename
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Role not found: rolename
```

```
Principal not found: principalname
```

一次役割がすでに設定されている場合は、次のメッセージが表示されます。

```
WARNING:Primary role already set for principal,role was:formerrole
```

```
Are you sure you want to set?
```

setResourceDomainParent

指定したリソースドメインに親リソースドメインを設定します。

構文

`setResourceDomainParent`, *resourcedomain*, *parentresourcedomain*

`srdp`, *resourcedomain*, *parentresourcedomain*

出力

コマンドが成功すると、次のメッセージが表示されます。

```
Resource Domain parentresourcedomain successfully set as parent to
resourcedomain
```

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

```
Resource Domain resourcedomain not found
```

```
Resource Domain parentresourcedomain not found
```

親を持つリソースドメインに親を設定しようとすると、次のメッセージが表示されます。

```
This resource domain has a parent! Set anyway? [y|n]
```

setRoleParent

指定した役割に親の役割を設定します。

構文

`setRoleParent`, *rolename*, *parentrolename*

`srp`, *rolename*, *parentrolename*

出力

コマンドが成功すると、次のメッセージが表示されます。

`Role:` *parentrolename* `successfully set as parent to:` *rolename*

コマンドが失敗すると、次のいずれかのメッセージが表示されます。

`Role not found:` *rolename*

`Role not found:` *parentrolename*

親を持つ役割に親役割を設定しようとすると、次のメッセージが表示されます。

`This role has a parent! Set anyway? [y|n]`

commit

注 – RDBMS リポジトリでのみ使用してください。

リポジトリに更新を生成するコマンド、たとえば主体の追加などは、コミットするまでその変更が保留状態になります。そのため、管理者は関連するセキュリティーの変更をすべて保留にしておき、同時に有効にできます。`commit` コマンドは、保留中のすべての変更をリポジトリに送信します。変更を有効にするには、`msfserver -r` コマンドを実行する必要があります。91 ページの「セキュリティールールを更新する」を参照してください。

構文

`commit`

`com`

出力

コマンドが成功すると、次のメッセージが表示されます。

```
commit SUCCESS!
```

コマンドが失敗すると、次のメッセージが表示されます。

```
Exception exceptiontype was thrown
```

管理者が更新内容を保留にしたまま SecAdmin アプリケーションを終了しようとすると、次の警告メッセージが表示されます。

```
[SecAdmin]WARNING:You have uncommitted changes!Do you really
want to quit?
[SecAdmin]Enter 'y' to exit WITHOUT committing,
[SecAdmin]Enter 'n' to return to command line,
[SecAdmin]Enter 'c' to commit and exit
[SecAdmin]Your answer:
```

管理者が `n` と入力すると、SecAdmin アプリケーションはプロンプトに戻って、ほかのコマンドを待機します。`y` と入力すると、保留中の変更を破棄 (ロールバック) して終了します。`c` と入力すると、変更をコミットして終了します。

rollback

注 – RDBMS リポジトリでのみ使用してください。

保留中のリポジトリの変更をすべてロールバック、つまり無効にします。

構文

```
rollback
roll
```

出力

コマンドが成功すると、次のメッセージが表示されます。

```
rollback SUCCESS!
```

コマンドが失敗すると、次のメッセージが表示されます。

```
Exception exceptiontype was thrown
```

quit

SecAdmin セッションを終了します。

構文

```
quit

q
```

リポジトリのパスワードの更新

リポジトリとして使用しているデータベースやディレクトリの管理者がそれらのパスワードを変更した場合は、新しいパスワードが認識されるように Sun MSF も更新する必要があります。`msfupdkey` ユーティリティーを使用して、パスワードを格納している Sun MSF の鍵ファイルを更新します。

形式:

```
msfupdkey [-h]
```

`-h` オプションは、コマンドとその用途について短い説明を表示します。

▼ リポジトリのパスワードを更新する

1. **管理者パスワードとエンドユーザーの新しいパスワードを持っていることを確認します。**
2. **Sun MSF 管理者の環境を設定します。**

   21 ページの「管理者の設定ファイルの作成」を参照してください。

3. **コマンドプロンプトで、`msfupdkey` コマンドを実行します。**

   次に、ユーザーとコンピュータの対話例を示します。

```
$ msfupdkey
(SecSvc_262) Loading security configuration data...
(SecSvc_250) Security ADMIN name: admin
(SecSvc_253) Enter security ADMIN password (or quit):
*******
(SecSvc_250) Security END USER name: user
(SecSvc_253) Enter security END USER password (or quit):
*******
(SecSvc_265) Keyfile successfully updated
```

   `MSFconfig.properties` ファイルから取得されるセキュリティー管理者名とエンドユーザー名が表示されます。

4. **それぞれの名前に新しいパスワードを入力します。**

   プロンプトのどちらかで `quit` と入力すると、鍵ファイルが更新されずにユーティリティーが終了します。

注 – 1 つのパスワードしか変更されていない場合でも、それぞれの名前にパスワードを入力する必要があります。

第6章

セキュリティー環境の管理

リポジトリを初期化したあと、セキュリティー管理者またはセキュリティーサーバーのオペレータはこの節で説明する作業を行います。セキュリティー管理者またはセキュリティーサーバーのオペレータが Sun MSF コマンドやユーティリティーを実行できるようにするには、まず環境を設定する必要があります。21 ページの「管理者の設定ファイルの作成」を参照してください。

この章の内容は、次のとおりです。

セキュリティーサーバーの管理

図 1-2 に示すように、セキュリティーサーバーは、Sun MSF サポートを必要とするアプリケーションがセキュリティーリポジトリに集中的にアクセスできるようにします。

このセキュリティーサーバーは、`msfserver` コマンドで管理します。

書式:

```
msfserver {-s|-t|-p|-r} [-n]
```

オプション	説明
`-s`	セキュリティーサーバーを起動します。詳細は、89 ページの「セキュリティーサーバーを起動する」を参照してください。
`-t`	セキュリティーサーバーを終了します。詳細は、90 ページの「セキュリティーサーバーを停止する」を参照してください。

オプション	説明
-p	セキュリティーサーバーの統計情報レポートを出力します。詳細は、91 ページの「セキュリティーサーバーの統計情報を表示する」を参照してください。
-r	セキュリティーリポジトリのルールを更新します。詳細は、91 ページの「セキュリティールールを更新する」を参照してください。
-n	ユーザー ID とパスワードの入力を求めるプロンプトが表示されなくなることを示します。詳細は、88 ページの「セキュリティーサーバーのオペレータとしての UNIX ユーザー ID の設定」を参照してください。

セキュリティーサーバーのオペレータとしての UNIX ユーザー ID の設定

msfserver コマンドには、プロンプトが表示されない -n オプションがあります。このオプションでは、ユーザー名とパスワードの入力を求めるプロンプトが表示されず、セッションの UNIX ユーザー ID が使用されます。この UNIX ユーザー ID は、認証されたユーザーとして認識されますこのオプションを使用する場合、または Sun MSF の高可用性データサービスを使用して環境を構成する場合、SecurityServer アプリケーションの ObjectReference リソースへの読み取り権と実行権が付与された UNIX ユーザー ID の主体エントリがセキュリティーリポジトリに含まれている必要があります。このリソースには、AdminResources リソースドメインを使用してアクセスできます。この主体をリポジトリに追加するには、自分のユーザー情報を使用して、次の SecAdmin コマンドを実行します。

```
cpr,joesmith,cx97052,,,,,UNIX user ID for Joe Smith
app,joesmith,AdminResources,READ,EXECUTE
```

この主体の特性を表示するには、次の lpr SecAdmin コマンドを使用します。

```
SecAdmin:lpr,joesmith
[SecAdmin] listPrincipal for:joesmith
    Principal Name:joesmith
    Primary Role: NULL
    Roles:
       NO ROLES
    Suspended State:false
    Password Expiration Date:2020-04-30
    Maximum Password Duration:0
    Minimum Password Duration:0
    Description:UNIX user ID for Joe Smith
    Granted Permissions:
        Granted perm #0
            Resource Domain Name: AdminResources
            Permissions: READ,EXECUTE
```

▼ セキュリティーサーバーを起動する

セキュリティー管理者は、Sun MTP 領域などのアプリケーションを起動する前に、セキュリティーサーバーを起動する必要があります。

1. **次のコマンドを入力します。**

```
$ msfserver -s
```

2. MSF Login username **プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているユーザー名を入力します。**

3. MSF Login password **プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているパスワードを入力します。**

   セキュリティーサーバーは、次のメッセージを表示します。

```
starting Security Server
(SecSvc_222) Security Server started, using port n
```

この *n* は、MSFconfig.properties ファイルの serverPortNumber プロパティーに設定されている値です。Sun MTP と統合する場合、この数字は、領域の KIXSEC_SERVERPORT 環境変数のポート番号と一致している必要もあります。

手順 1 に示したコマンド構文のほかに、次のいずれかのコマンドを使用して、ユーザー ID とパスワードの入力を求めるプロンプトを表示せずにセキュリティーサーバーを起動することができます。主体の UNIX ユーザー ID は、セキュリティーサーバーへのアクセスの承認に使用されます。

```
msfserver -ns
msfserver -sn
msfserver -s -n
```

▼ セキュリティーサーバーを停止する

セキュリティーサーバーを終了する必要がある場合は、Sun MSF を使用するすべてのアプリケーションを停止します。このあとで、セキュリティー管理者がセキュリティーサーバーを停止します。

1. **次のコマンドを入力します。**

```
$ msfserver -t
```

2. `MSF Login username` **プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているユーザー名を入力します。**
3. `MSF Login password` **プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているパスワードを入力します。**

   セキュリティーサーバーは、次のメッセージを表示して終了します。

```
(SecSvc_224) Security Server terminated
```

注 – セキュリティーサーバーを停止すると、自動的にすべてのユーザーがログオフされます。

手順 1 に示したコマンド構文のほかに、次のいずれかのコマンドを使用して、ユーザー ID とパスワードの入力を求めるプロンプトを表示せずにセキュリティーサーバーを停止することができます。主体の UNIX ユーザー ID は、セキュリティーサーバーへのアクセスの承認に使用されます。

```
msfserver -nt
msfserver -tn
msfserver -t -n
```

▼ セキュリティールールを更新する

Sun MSF では、セキュリティールールがセキュリティーリポジトリで保持されています。ユーザーのログイン時、セキュリティーサーバーは、そのユーザーのアクセスルールを、セキュリティーサーバーのシステム全体で適用するメモリに読み込みます。これらのセキュリティールールは、ユーザーがログインしている限りメモリに置かれます。ユーザーがログアウトすると、ユーザーのルールはクリアされます。セキュリティールールが変更されても、メモリのこの領域は自動的に更新されません。

1. **セキュリティールールを更新するには、次のコマンドを入力します。**

```
$ msfserver -r
```

2. `MSF Login username` **プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているユーザー名を入力します。**

3. `MSF Login password` **プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているパスワードを入力します。**

   セキュリティーサーバーは、次のメッセージを表示します。

```
refreshing Security Server
(SecSvc_228) Security Server successfully completed RefreshPolicy:
```

   手順 1 に示したコマンド構文のほかに、次のいずれかのコマンドを使用して、ユーザー ID とパスワードの入力を求めるプロンプトを表示せずにセキュリティールールを更新することができます。主体の UNIX ユーザー ID は、セキュリティーサーバーへのアクセスの承認に使用されます。

```
msfserver -nr
msfserver -rn
msfserver -r -n
```

▼ セキュリティーサーバーの統計情報を表示する

セキュリティー管理者は、セキュリティーサーバーの要求、有効なユーザー、Sun MTP 領域の概要を表示できます。

1. **次のコマンドを入力します。**

```
$ msfserver -p
```

2. `MSF Login username` プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているユーザー名を入力します。

3. `MSF Login password` プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているパスワードを入力します。

統計情報レポートは、次の例のようになります。

コード例 6-1　　セキュリティーサーバーの統計情報レポート

```
DumpEntries: global activity counters
=====================================
login:          13
logout:         4
checkAccess:    101
hostUser:       9
trustedServer:  8
refresh:        0
dump:           4
invalidRequest:0
exception:      0
=====================================

DumpEntries: userSessionList contents
=====================================
UserSession: ssadmin(default) sessionCount = 1
UserSession: tester2(default) sessionCount = 4
UserSession: chewy(default) sessionCount = 2
UserSession: tester1(default) sessionCount = 5
UserSession: vader(default) sessionCount = 6
UserSession: luke(default) sessionCount = 2
=====================================

DumpEntries: trustedServerList contents
=====================================
TrustedServer: /users/tester2/tests/abcd80
serverCount = 6
TrustedUser: tester2(default) sessionCount = 4
TrustedUser: chewy(default) sessionCount = 2
TrustedUser: tester1(default) sessionCount = 5
TrustedUser: vader(default) sessionCount = 6
TrustedUser: luke(default) sessionCount = 2
=====================================
```

手順 1 に示したコマンド構文のほかに、次のいずれかのコマンドを使用して、ユーザー ID とパスワードの入力を求めるプロンプトを表示せずにセキュリティーサーバーの統計情報を表示することができます。主体の UNIX ユーザー ID は、セキュリティーサーバーへのアクセスの承認に使用されます。

```
msfserver -np
msfserver -pn
msfserver -p -n
```

セキュリティーログ収集の管理

Sun MSF は、Sun MSF アプリケーションを実行するために セキュリティーログ収集サーバーに依存して、機能しています。デフォルトでは、監査ログ記録およびメッセージログ記録を実行するメッセージロガーは有効に設定され、アプリケーションで使用できます。トレースロガーも有効に設定できます。`MSFconfig.properties` ファイルに含まれる次のプロパティーは、ログサーバーの機能に影響します。

プロパティー	目的
`com.sun.emp.security.logMessageOn`	監査ログ記録を有効にします。
`com.sun.emp.security.logMessagePort`	メッセージロガーが使用するポート番号を指定します。
`com.sun.emp.security.logTraceOn`	デバッグトレースを有効にします。
`com.sun.emp.security.logTracePort`	トレースロガーが使用するポート番号を指定します。
`com.sun.emp.security.logDirectory`	メッセージおよびトレースログが書き込まれるディレクトリを指定します。
`com.sun.emp.security.logPeriod`	ログファイルを切り替える間隔 (時間) を定義します。

注 – `com.sun.emp.security.logPeriod` プロパティーは、ログファイルが切り替わる間隔を時間単位で定義します。このプロパティーを 1 ～ 24 の整数値に設定すると、指定した時間数の経過後、ログサーバーは自動的に新しいファイルへの書き込みを開始します。たとえば、このプロパティーを 12 に設定すると、12 時間ごとに新しいファイルが開かれ、古いファイルが閉じられます。0 (ゼロ) に設定すると、ファイルの切り替えは実行されません。新しいファイルに手動で切り替える方法については、96 ページの「同じディレクトリ内でのセキュリティーログサーバーファイルの変更」を参照してください。

セキュリティーログ収集サーバーは、msflog コマンドで制御します。

書式:

msflog {-s|-t|-p|-f|-d *directory*}

オプション	説明
-s	ロガーを起動します。
-t	ロガーを終了します。
-p	ログサーバー情報を出力します。
-f	ログファイルをスワップします。
-d *directory*	生成された収集ファイルを作成するディレクトリを変更します。

msflog コマンドは、日付と時間を含む一意のファイル名を持つ収集ファイルを生成します。収集ファイルにログ記録された監査メッセージ例は、97 ページの「セキュリティーイベントのログ記録」を参照してください。

監査メッセージを収集するには、セキュリティーログ収集サーバーを常に実行したままにします。

セキュリティーログサーバーの起動

セキュリティーログサーバーを起動する前に、メッセージロガー (さらに、必要に応じてトレースロガー) を MSFconfig.properties ファイルで有効にしておく必要があります。ロガーポート番号もプロパティーファイルで設定する必要があります。

セキュリティー管理者は、次のコマンドを使用して、セキュリティーログサーバーを起動します。

```
$ msflog -s
```

メッセージログとトレースログの両方が起動されると、次のメッセージが表示されます。

```
[SecurityLog] Message logger started successfully on port:pm
[SecurityLog] Trace logger started successfully on port:pt
```

変数 *pm* と *pt* はそれぞれ、MSFconfig.properties の com.sun.emp.security.logMessagePort と com.sun.emp.security.logTracePort に設定されている値です。

セキュリティーログサーバーの停止

セキュリティーログサーバーを終了する必要がある場合は、まずセキュリティーログ記録を使用しているすべてのアプリケーションを停止します。さらに、次のコマンドを使用して、セキュリティーログサーバーを停止します。

```
$ msflog -t
```

次のメッセージが表示されます。

```
[SecurityLog]:The Message logger has successfully terminated
[SecurityLog]:The Trace logger has successfully terminated
```

セキュリティーログサーバーのディレクトリの変更

ディスク容量の制約やその他の理由によって、ログを書き込むディレクトリを変更する必要がある場合、次のコマンドを実行します。

```
$ msflog -d directory
```

変数 *directory* はログの新しいディレクトリを示しています。このディレクトリには書き込み権が必要です。また、現在のディレクトリと異なる必要があります。このコマンドを実行すると、現在のログファイルが閉じられ、新しいタイムスタンプを持つ新しいファイルが新しいディレクトリで開かれます。コマンドが正常に完了すると、次のメッセージが表示されます。

```
[SecurityLog]:Message logger has changed directories
[SecurityLog]:Trace logger has changed directories
```

同じディレクトリ内でのセキュリティーログサーバーファイルの変更

現在のログファイルを、同じログ記録ディレクトリ内で、新しい名前の新しいログファイルに変更する必要性が生じる場合があります。このプロセスは、ファイルの**切り替え**と呼ばれることもあります。次のコマンドを実行し、ファイルを切り替えます。

```
$ msflog -f
```

古いファイルが閉じ、新しいファイルが開きます。次のメッセージが表示されます。

```
[SecurityLog]:Message logger has flipped files
[SecurityLog]:Trace logger has flipped files
```

セキュリティーログサーバー情報の表示

セキュリティーログサーバーのフルパス名とポート番号を表示するには、次のコマンドを実行します。

```
$ msflog -p
Print Status from Message
================================================
  Path:/tmp/SecMsg2002Sep12101708.txt
  Port:18888

Print Status from Trace
================================================
  Path:/tmp/SecTrc2002Sep12101708.txt
  Port:16969
```

セキュリティーイベントのログ記録

セキュリティーログサーバーは、Sun MSF セキュリティー監査メッセージを収集してログファイルに書き込みます。セキュリティーログサーバーは、`msflog` コマンドで起動します。Sun MSF ソフトウェアは、監査メッセージを生成してセキュリティーイベントを記録し、それらを次のいずれかのセキュリティーレベルに分類します。

表 6-1　監査メッセージのセキュリティーレベル

セキュリティーレベル	説明
TYPE_INFO	情報メッセージであり、アクションを必要としません。たとえば、メンバーである主体について役割が照会されていることを示すイベントの情報です。
TYPE_WARN	アクションを必要とすることがある、より重大なメッセージです (特にメッセージが予期しないものであった場合)。たとえば、管理者がリソースドメインからリソースを削除すると、警告イベントが生成されます。
TYPE_ERROR	要求を出しているアプリケーションが拒否されたことを示すイベントです。たとえば、ユーザーのリソースアクセス要求が拒否された場合、ユーザーのログインパスワードが無効である場合などがあります。これらのイベントは、管理者のアクションを必要とする場合、または必要としない場合があります。
TYPE_FATAL	予期しないソフトウェアエラーが発生しました。関連するセキュリティーサービスが使用できなくなる場合があります。通常、このイベントタイプには、管理者による迅速なアクションが必要です。

セキュリティー監査ログメッセージには、タイムスタンプとメッセージ番号が付けられます。詳細は、第 9 章のメッセージ番号を参照してください。

次のメッセージは、ログサーバーに関するものであり、収集ファイルに対して `msflog` コマンドが作成した生成ファイルの名前の例を示しています。

```
LOG0039I Starting the Log Server.
LOG0034I Creating a server socket on port 9995.
LOG0038I Sending output to the console and to the file SecMsg2002Feb05111326.txt
.
LOG0032I Established connection with localhost at 2002.02.05 11:13:52:228.
```

次のメッセージは、主体の認証に関連するものです。

```
2002.02.05 11:13:54.102 TYPE_WARN (SecSvc_016) Principal tester2 has been
granted access to (com.sun.emp.security.admin.PrincipalPermission ssuser read).
2002.02.05 11:13:54.541 TYPE_WARN (SecSvc_004) The password has been validated
for Principal ssuser.
```

次のメッセージは、セキュリティー管理者がセキュリティーリポジトリに追加を行なったときに表示されます。

```
2002.02.05 11:45:02.427 TYPE_WARN (SecSvc_110) BROD was added by Administrative
Principal ssuser.
2002.02.05 11:45:02.594 TYPE_WARN (SecSvc_110) TEST1 was added by Administrative
Principal ssuser.
2002.02.05 11:45:02.758 TYPE_WARN (SecSvc_110) chewy was added by Administrative
Principal ssuser.
2002.02.05 11:45:02.916 TYPE_WARN (SecSvc_110) luke was added by Administrative
Principal ssuser.
2002.02.05 11:45:03.097 TYPE_WARN (SecSvc_110) tester1 was added by
Administrative Principal ssuser.
2002.02.05 11:45:03.257 TYPE_WARN (SecSvc_110) vader was added by Administrative
Principal ssuser.
2002.02.05 11:45:03.545 TYPE_WARN (SecSvc_111) ABCD80production with parent NULL
was added by Administrative Principal ssuser.
2002.02.05 11:45:03.620 TYPE_WARN (SecSvc_111) ABCD80visitor with parent NULL
was added by Administrative Principal ssuser.
2002.02.05 11:45:07.508 TYPE_WARN (SecSvc_111) ABCD80filesDMVx with parent NULL
was added by Administrative Principal ssuser.
2002.02.05 11:45:11.151 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" CEMT was added
by Administrative Principal ssuser.
2002.02.05 11:45:11.222 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" CSMT was added
by Administrative Principal ssuser.
2002.02.05 11:45:11.299 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" CTBL was added
by Administrative Principal ssuser.
2002.02.05 11:45:11.368 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" CESF was added
by Administrative Principal ssuser.
2002.02.05 11:45:11.437 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" CESN was added
by Administrative Principal ssuser.
2002.02.05 11:45:11.507 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" CPLT was added
by Administrative Principal ssuser.
2002.02.05 11:45:11.581 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" DMDL was added
by Administrative Principal ssuser.
2002.02.05 11:45:11.652 TYPE_WARN (SecSvc_110) "KIX_ATTACH_TRANS" DMVA was added
by Administrative Principal ssuser.
2002.02.05 11:45:15.512 TYPE_WARN (SecSvc_110) "KIX_START_TRANS" DMV0 was added
by Administrative Principal ssuser.
```

```
2002.02.05 11:45:15.583 TYPE_WARN (SecSvc_110) "KIX_START_TRANS" DMV1 was added
by Administrative Principal ssuser.
2002.02.05 11:45:16.401 TYPE_WARN (SecSvc_110) "KIX_PROGRAM" CL2TCMB was added
by Administrative Principal ssuser.
2002.02.05 11:45:16.469 TYPE_WARN (SecSvc_110) "KIX_PROGRAM" INQSLINK was added
by Administrative Principal ssuser.
2002.02.05 11:45:27.700 TYPE_WARN (SecSvc_110) "KIX_FILE" DMVSAM was added by
Administrative Principal ssuser.
2002.02.05 11:31:47.333 TYPE_WARN (SecSvc_116) "KIX_FILE" DMVSAM was added to
ABCD80filesDMVx by Administrative Principal ssuser.
2002.02.05 11:45:17.406 TYPE_WARN (SecSvc_116) "KIX_ATTACH_TRANS" DMDL was added
to attachABCD80tx by Administrative Principal ssuser.
2002.02.05 11:45:17.538 TYPE_WARN (SecSvc_116) "KIX_ATTACH_TRANS" DMVA was added
to attachABCD80tx by Administrative Principal ssuser.
2002.02.05 11:45:26.863 TYPE_WARN (SecSvc_116) "KIX_START_TRANS" DMV0 was added
to startretrABCD80tx by Administrative Principal ssuser.
2002.02.05 11:45:27.001 TYPE_WARN (SecSvc_116) "KIX_START_TRANS" DMV1 was added
to startretrABCD80tx by Administrative Principal ssuser.
2002.02.05 11:45:16.860 TYPE_WARN (SecSvc_116) "KIX_PROGRAM" CL2TCMB was added
to linkABCD80progs by Administrative Principal ssuser.
2002.02.05 11:45:16.999 TYPE_WARN (SecSvc_116) "KIX_PROGRAM" INQSLINK was added
to linkABCD80progs by Administrative Principal ssuser.
2002.02.05 11:45:04.358 TYPE_WARN (SecSvc_116) luke was added to ABCD80admin by
Administrative Principal ssuser.
2002.02.05 11:45:04.551 TYPE_WARN (SecSvc_116) tester1 was added to
ABCD80default by Administrative Principal ssuser.
2002.02.05 11:45:04.738 TYPE_WARN (SecSvc_116) chewy was added to
ABCD80production by Administrative Principal ssuser.
2002.02.05 11:45:04.919 TYPE_WARN (SecSvc_116) vader was added to ABCD80visitor
by Administrative Principal ssuser.
2002.02.05 11:37:26.214 TYPE_WARN (SecSvc_130) Permissions [EXECUTE] to Resource
Domain attachABCD80tx for ABCD80visitor were added by Administrative Principal
ssuser.
2002.02.05 11:37:54.659 TYPE_WARN (SecSvc_130) Permissions [READ,EXECUTE] to
Resource Domain startretrABCD80tx for ABCD80visitor were added by Administrative
Principal ssuser.
2002.02.05 11:32:49.822 TYPE_WARN (SecSvc_130) Permissions [READ,WRITE] to
Resource Domain  ABCD80filesDMVx for ABCD80production were added by
Administrative Principal ssuser.
```

次の例は、tester1 という主体のログメッセージを示しています。最初のメッセージは、検証に失敗したことを示します。次のメッセージは、認証に成功したこと、およびあるリソースへのアクセスが許可または拒否されたことを示します。

```
2002.02.05 11:18:54.302 TYPE_ERR (SecSvc_005) Validation failed for Principal
tester1.
2002.02.05 12:05:54.662 TYPE_WARN (SecSvc_004) The password has been validated
for Principal tester1.
2002.02.05 16:08:59.650 TYPE_WARN (SecSvc_016) Principal tester1 has been
granted access to (com.sun.emp.security.admin.CICSResourcePermission
"KIX_ATTACH_TRANS" DMV0 execute).
2002.02.05 16:08:59.726 TYPE_FATAL (SecSvc_015) Principal tester1 has been
denied access to (com.sun.emp.security.admin.CICSResourcePermission "KIX_FILE"
DMVSAM read).
2002.02.05 16:14:57.221 TYPE_WARN (SecSvc_016) Principal tester1 has been
granted access to (com.sun.emp.security.admin.CICSResourcePermission
"KIX_ATTACH_TRANS" CESF execute).
```

セキュリティーログサーバーのモニターウィンドウの表示

Solaris プラットフォーム: dtterm 実行可能ファイルがパスに含まれている場合、セキュリティーログサーバーは有効なログを追跡するウィンドウを起動時に表示します。この実行可能ファイルがパスに含まれているかどうかを調べるには、次のコマンドを入力します。

```
$ echo $PATH
```

パス名 /usr/dt/bin が出力で一覧表示される必要があります。一覧表示されない場合、この機能が必要であれば、次のように実行可能ファイルへのパスを設定スクリプトの PATH 変数に追加します。

```
PATH=/usr/dt/bin:$PATH;export PATH
```

任意のプラットフォーム: dtterm 実行可能ファイルを使用できない場合、または使用しない場合は、シェルウィンドウを開いて、有効なログを追跡することができます。次に例を示します。

```
$ msflog -p
printing Security Loggers statistics...

Print Status from Message
================================================
    Path:/users/user1/SecurityProject/logs/SecMsg2004Jul13093653.txt
    Port:9994
$ tail -f SecMsg2004Jul13093653.txt
```

第7章

Sun MTP との統合

Sun MSF のインストールと設定を行なったあとは、Sun MSF の認証サービスと承認サービスを利用するために、以下のタスクを行なって Sun MTP 領域を有効にする必要があります。

表 7-1　タスクマップ: Sun MSF と Sun MTP の統合

タスク	手順の参照先
Sun MTP サインオンテーブル (SNT) でデフォルトのユーザーを設定します。	『Sun Mainframe Transaction Processing ソフトウェア管理者ガイド』
Sun MTP 端末管理テーブル (TCT) で、あらかじめ設定された、必要なセキュリティー端末を設定します。	『Sun Mainframe Transaction Processing ソフトウェアリファレンスマニュアル』
領域の設定ファイルを編集して、Sun MSF 環境変数を追加します。	104 ページの「Sun MSF 環境変数」
Sun MTP Secure を設定します。	『Sun Mainframe Transaction Processing ソフトウェア管理者ガイド』
SecAdmin アプリケーションを使用して、Sun MTP リソースをリポジトリに追加します。	104 ページの「Sun MTP のリソースの追加」
SecAdmin アプリケーションを使用して、ユーザーとアプリケーションのリソースをリポジトリに追加します。	52 ページの「SecAdmin コマンド」
ログサーバーが起動していない場合は、起動します。	94 ページの「セキュリティーログサーバーの起動」
セキュリティーサーバーを起動します。	89 ページの「セキュリティーサーバーを起動する」
Sun MTP 領域を起動します。	『Sun Mainframe Transaction Processing ソフトウェア構成ガイド』

領域の Sun MSF 環境の設定

Sun MSF 環境変数

Sun MSF はソケット接続でセキュリティーサーバーに接続するため、次の環境変数を領域の設定ファイルに入力し、セキュリティーサーバーのホスト名または IP アドレス、およびソケットポート番号を指定する必要があります。

`KIXSEC_SERVERHOST=`[*hostname* | *IP-address*]

`KIXSEC_SERVERPORT=`*port#*

Sun MTP Secure

Sun MTP Secure の変数の詳細については、『Sun Mainframe Transaction Processing ソフトウェア 構成ガイド』を参照してください。

Sun MTP Secure の詳細については、『Sun Mainframe Transaction Processing ソフトウェア 管理者ガイド』を参照してください。

Sun MTP のリソースの追加

この節では、Sun MSF 製品に付属するリソースファイルについて説明します。これらのリソースファイルをリポジトリに読み込むことができます。ここで、Sun MTP のシステムトランザクションや、Sun MTP のサンプルアプリケーションのトランザクションを実行することが可能になります。

システムリソース

システムトランザクションおよび VSAM カタログなどの、Sun MTP のシステムリソースへのアクセスを承認するために Sun MSF を使用している場合は、これらのリソースをリポジトリに追加する必要があります。Sun MTP のシステムリソースを追加する作業を簡単にするため、テンプレートファイルが *MSF-home*`/etc` ディレクトリに用意されています。これは `suppliedLoadFile.txt` というファイルで、リソースの作成、リソースドメインの作成、その各ドメインへのリソースの追加、および役割のアクセス権の追加を行うためのコマンドが含まれています。このテンプレー

トをそのまま使用することもできますが、環境で使用される役割名およびリソースドメイン名に合わせて修正することも可能です。修正する前に、元のファイルのバックアップを作成してください。

MSF-home/etc ディレクトリの README.txt ファイルには、Sun MTP のシステムリソースファイルと、その他のリソースファイルの情報が記載されています。

Primer サンプルアプリケーションのリソース

また、*MSF-home*/etc ディレクトリには、Sun MTP に付属する Primer サンプルアプリケーションのリソースファイルもあります。Primer アプリケーションは、$UNIKIX/examples/primer ディレクトリにあります。Primer アプリケーションの使い方については、言語別のディレクトリにある readme ファイルを参照してください。たとえば、Micro Focus COBOL バージョンの Primer アプリケーションの場合は、$UNIKIX/examples/primer/cobol_mf/README.txt を参照します。

MSF-home/etc ディレクトリの README.txt ファイルには、Primer サンプルアプリケーションのリソースファイルと、その他のリソースファイルの情報が記載されています。

MQ および MQ-JMS Bridge サンプルアプリケーションのリソース

MSF-home/etc ディレクトリには、Sun MTP に付属する MQ および MQ-JMS Bridge サンプルアプリケーションのリソースファイルもあります。MQ アプリケーションは $UNIKIX/examples/mq/cobol_mf ディレクトリにあります。MQ-JMS Bridge アプリケーションは $UNIKIX/examples/mq/jms ディレクトリにあります。このアプリケーションの使い方については、適切なディレクトリの readme ファイルを参照してください。

MSF-home/etc ディレクトリの README.txt ファイルには、MQ サンプルアプリケーションのリソースファイルと、その他のリソースファイルの情報が記載されています。

セキュリティーサーバーの起動

セキュリティーサーバーを起動するには、msfserver コマンドを実行します。

▼ セキュリティーサーバーを起動する

セキュリティー管理者は、領域を起動する前に、セキュリティーサーバーを起動する必要があります。

1. **次のコマンドを入力します。**

```
$ msfserver -s
```

2. **MSF Login username プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているユーザー名を入力します。**

3. **MSF Login password プロンプトが表示されたら、MakeAnAdminstrator アプリケーションで管理者に対して定義されているパスワードを入力します。**

   こうすると、セキュリティーサーバーは、次のメッセージを表示します。

```
(SecSvc_222) Security Server started, using port n
```

   ここで、*n* は、MSFconfig.properties ファイルの com.sun.emp.security.serverPortNumber に設定されている値です。この数字は、領域の KIXSEC_SERVERPORT 環境変数のポート番号とも一致している必要があります。

セキュリティーサーバーの停止および再起動

セキュリティー管理者が、領域を実行しながらセキュリティーサーバーを停止すると、セキュリティーサーバーを必要とするすべての認証および承認要求が失敗し、エラーメッセージが各領域の `unikixmain.log` ファイルに書き込まれます。

セキュリティーサーバーをいくつかの領域が有効な状態で再起動すると、それらの領域は認証および承認サービスに再接続して再開できます。ただし、領域にそれまでにログインしていたすべてのユーザーは、セキュリティールールを回復するためにログインし直す必要があります。

注 – セキュリティーサーバーを停止すると、自動的にすべてのユーザーがログオフされます。

ユーザーと役割の認証

ユーザーはログイントランザクション (`CESN` または `CSSN`) で領域に接続します。セキュリティーサーバーは、ユーザーがセキュリティーリポジトリに登録されていることを認証します。`CESN` トランザクションでは、ユーザーは特定の役割にサインオンすることもできます。`CESN` トランザクションは、ユーザーの認証後、パスワードを変更するのにも使用できます。

注 – Sun MTP では、8 文字までのパスワードと役割 (グループ) 名を使用できます。この制限は、文字数が 8 文字に制限されている CICS API と一致しています。

認証されたユーザーは、認証された接続のトランザクションを領域にサブミットできます。セキュリティーサーバーに問い合わせが行われ、各ユーザーに読み込まれたセキュリティールールが確認されて、要求したリソースへのアクセス権をユーザーが持っているかどうかが判断されます。

第8章

障害追跡

この章では、Sun MSF とそのアプリケーションの起動時および使用中に発生する可能性がある問題について説明します。また、問題を分析するために技術サポート担当が使用するスナップショットファイルを作成する方法についても説明します。この章の内容は、次のとおりです。

Sun MSF とは、一連の Java Archive (JAR) ファイルと、関連する Java プロパティーファイルがインストールされたものであり、Java プロパティーファイルにはサイトの設定が格納されています。また、Sun MSF は、Oracle とそれに付属する Java データベースコネクタ (JDBC) クラスファイルなどの、選択した RDBMS リポジトリと、プロパティーファイルへのアクセスに依存しています。このため、Sun MSF で問題が発生した場合の解決方法は、次の Sun MSF コマンドを実行して、インストール済みの Java ランタイム環境 (JRE) によって報告されたエラーや例外を識別し、解釈する作業が必要になることがほとんどです。

`msflog`

`msfadmin`

`msfinitr`

`msfserver`

JRE の Java クラスファイルの検出エラー

このエラーは、Sun MSF ツールを実行したときに発生することがあります。通常は、以下のいずれかのメッセージが表示されます。

`Exception in thread "main" java.lang.NoClassDefFoundError:` *classname*

`(SecSvc_FATAL) Unexpected error java.lang.NoClassDefFoundError:` *classname*

見つからなかった *classname* は、`CLASSPATH` 環境変数で指定された、付属の Sun MSF または JDBC のクラスファイルのいずれかに含まれているはずです。この *classname* が `com/sun/emp/security/...` で始まる場合、次の Sun MSF JAR ファイルのいずれかまたは両方が `CLASSPATH` 環境変数で正しく指定されていません。

MSF-home`/lib/secrt.jar`
MSF-home`/lib/secrtpa.jar`

それ以外の *classname* は、必要な JDBC クラスを識別する接頭辞で始まります。たとえば、Oracle では、*classname* は `oracle/sql/...` で始まります。この場合、`MSFconfig.properties` ファイルの `adapterPath` キーワードで JDBC クラスファイルが正しく指定されていません。

Java セキュリティーアクセスの拒否

このエラーは、Sun MSF ツールを実行したときに発生することがあります。このエラーにはさまざまな種類がありますが、すべてのメッセージに次の文字列が含まれています。

`java.security.AccessControlException: access denied (`*Java-class resource permission*`)`

この問題は、インストールされている JRE セキュリティーポリシーが *MSF-home*`/config/java.policy` ファイルで正しく指定されていないときに発生します。

このポリシーファイルを確認して、示された *Java-class*、*resource*、*permission* が、必要な `grant` 指示語で指定されているかどうかを調べてください。

port out of range メッセージによるセキュリティーサーバーのエラー

MSF-home/config/$MSF_INSTANCE/MSFconfig.properties ファイルで設定されている serverPortNumber の値が、指定可能な UNIX ソケットポート番号の最大値よりも大きいと、次のエラーが発生します。

```
java.lang.IllegalArgumentException: Port value out of range: nnnnn
```

この値は、65536 未満でなければなりません。MSFconfig.properties ファイルでこの値を修正し、サーバーを再起動します。

Permission denied メッセージによるセキュリティーサーバーのエラー

MSF-home/config/$MSF_INSTANCE/MSFconfig.properties ファイルで設定されている serverPortNumber の値が、許容範囲よりも小さく、予約済みの UNIX ソケットポート番号に一致するときに、次のエラーが発生します。

```
java.net.BindException: Permission denied
```

serverPortNumber の値は、通常は 1024 ～ 65535 でなければなりません。*Java-home*/lib/security/java.policy ファイルで "grant ... permission java.net.SocketPermission" という指示語を調べて、使用している JRE で許容されているソケットポート番号の範囲を確認します。MSFconfig.properties ファイルでこの値を修正し、サーバーを再起動します。

Address already in use メッセージによるセキュリティーサーバーのエラー

MSF-home/config/$MSF_INSTANCE/MSFconfig.properties ファイルで設定されている serverPortNumber の値がすでに使用されているときに、次のエラーが発生します。

```
java.net.BindException: Address already in use
```

これは、その UNIX ソケットポート番号を使用する別のセキュリティーサーバーが動作中であることを示しています。MSFconfig.properties ファイルでこの値を修正し、サーバーを再起動します。

JDBC の SQL エラーの報告

JDBC クラスを通じてアクセスされる RDBMS リポジトリに、テーブルの欠落、RDBMS のアクセス権の削除、または参照整合性の問題などの、何らかのエラーが発生したときに、SQL エラーが報告されることがあります。次に例を示します。

```
java.sql.SQLException: ORA-00942: table or view does not exist
```

このエラーは、非常に深刻な問題を示している場合があります。Sun MSF サービスを停止し、セキュリティーリポジトリを再読み込みして、問題を修正しなければならないことがあります。

アプリケーションの起動時の問題

この節には、セキュリティーサーバー、セキュリティーロガー、SecAdmin などの Sun MSF アプリケーションを初期化するときに問題が発生した場合に表示されるメッセージが記載されています。

`[SecurityConfiguration] can't set new SecurityManager: ...` *exception* `...`

説明: 起動時に内部エラーが発生しました。

対策: ご購入先に問い合わせます。

`[SecurityConfiguration] fatal SecurityManager Exception: ...` *exception* `...`

説明: 起動時に内部エラーが発生しました。

対策: ご購入先に問い合わせます。

`[SecurityConfiguration] Bad URL - ...`*URL* `...`

説明: 無効な URL が原因で、起動時に内部エラーが発生しました。

対策: ご購入先に問い合わせます。

`[SecurityConfiguration] Required Properties could not be loaded java.io.FileNotFoundException:` *MSF-home*`/config/`*$MSF_INSTANCE*`/MSFconfig.properties (Permission denied)`

説明: 指定されたディレクトリに置かれる `MSFconfig.properties` ファイルが見つからない、損傷している、または利用できない状態になっています。

対策: 指定されたディレクトリに `MSFconfig.properties` ファイルが存在するかどうかを調べます。存在する場合は、このファイルのアクセス権の設定を確認します。たとえば、アプリケーションを起動したユーザーに、このファイルの読み取り権があることを確認します。ファイルが存在しない場合、この Sun MSF インスタンスに対して構成ユーティリティーを実行していないことがほとんどです。`MSFconfig.properties` ファイルを作成するには、このユーティリティーを実行する必要があります。ファイルが存在し、アクセス権が正しく設定されている場合は、ファイルが損傷しているかどうかを調べます。損傷している場合は、管理者または ご購入先 と一緒に作業し、損傷したファイルを除去して、有効なファイルを作成します。

`[SecurityConfiguration] MSF-home/config/java.security unusable/non-existent`

説明: 指定されたディレクトリに置かれる `java.security` ファイルが見つからない、損傷している、または利用できない状態になっているかどうかを調べます。

対策: 指定されたディレクトリに `java.security` ファイルが存在するかどうかを調べます。存在する場合は、このファイルのアクセス権の設定を確認します。たとえば、アプリケーションを起動したユーザーに、このファイルの読み取り権があることを確認します。ファイルが存在しない場合、この Sun MSF インスタンスに対して構成ユーティリティーを実行していないことがほとんどです。`java.security` ファイルを作成するには、このユーティリティーを実行する必要があります。ファイルが存在し、アクセス権が正しく設定されている場合は、ファイルが損傷しているかどうかを調べます。損傷している場合は、管理者または ご購入先 と一緒に作業し、損傷したファイルを除去して、有効なファイルを作成します。

`[SecurityConfiguration] incorrect 'policy.allowSystemProperty' setting`

説明: `java.security` ファイルの `'policy.allowSystemProperty'` に対して指定されている値が正しくありません。

対策: スーパー管理者に問い合わせます。スーパー管理者は `'policy.allowSystemProperty'` の値を `false` に設定していなければなりません。

`[SecurityConfiguration] incorrect 'java.security.properties' setting`

説明: `'java.security.properties'` のパス名の値が無効です。

対策: `'java.security.properties'` のパス名を *MSF-home*`/config/java.security` に設定する必要があります。

`[SecurityConfiguration] can't determine MSF_HOME from CLASSPATH`

説明: Sun MSF がインストールされている場所を示す、アプリケーション起動スクリプトの `CLASSPATH` のコマンド行引数が、インストールディレクトリを正しく指定していません。

対策: `secrt.jar` の `CLASSPATH` は、*MSF-home*`/lib/secrt.jar` でなければなりません。

スナップショットの作成

Sun MSF のスナップショットユーティリティーである msfsnap は、Sun MSF の設定ファイルとログファイルを収集して、分析のために ftp または電子メール経由で別の場所に送信することが可能な圧縮ファイルを作成します。msfsnap ユーティリティーは、Sun MSF のインストール先の *MSF-home*/bin ディレクトリにあります。

書式:

```
msfsnap [-d directory] [-u userid]
```

オプション	説明
-d *directory*	スナップショットが書き込まれる場所のディレクトリパスです。ディレクトリが指定されていない場合、スナップショットの書き込み先は MSFSNAPDIR 環境変数で指定されているディレクトリパスになります。環境変数が設定されていない場合、このツールはスナップショットを取得せずに終了します。
-u *userid*	ツールがセキュリティーサーバーの統計情報を収集してスナップショットを作成するのに必要なユーザー ID です。これは、Sun MSF 管理者のユーザー ID です。このオプションは msfserver -p の要求を実行します。msfsnap ユーティリティーは、パスワードの入力を求める次のプロンプトを表示します。 MSF Login password: 入力したパスワードが正しくないか、-u オプションを指定していない場合は、セキュリティーサーバーの統計情報は取り込まれません。 詳細については、87 ページの「セキュリティーサーバーの管理」を参照してください。

スナップショットは圧縮され、-d オプションまたは MSFSNAPDIR 変数で指定されたディレクトリにファイルとして置かれます。このファイルの名前は、次のとおりです。

MSFsnapshot.*date_time*.zip

このファイルは分析のために解凍して、圧縮する前のコンポーネントファイルに戻すことができます。

次の例は、msfsnap ユーティリティーの使い方を示しています。

例 1: セキュリティーサーバーの統計情報が含まれないスナップショットを /tmp ディレクトリに書き込みます。

```
$ msfsnap -d /tmp
```

例 2: スナップショットを /tmp ディレクトリに書き込み、セキュリティーサーバーの統計情報を追加します。

```
$ msfsnap -d /tmp -u MSF-admin-userid
MSF Login Password: MSF-admin-password
```

例 3: セキュリティーサーバーの統計情報が含まれないスナップショットを $MSFSNAPDIR ディレクトリに書き込みます。

```
$ export MSFSNAPDIR=/snaps
$ msfsnap
```

例 4: スナップショットを $MSFSNAPDIR ディレクトリに書き込み、セキュリティーサーバーの統計情報を追加します。

```
$ export MSFSNAPDIR=/snaps
$ msfsnap -u MSF-admin-userid
MSF Login Password: MSF-admin-password
```

第9章

エラーメッセージ

この章では、Sun MSF によって生成されるメッセージを記載しています。ほとんどのメッセージが監査ログで使用されますが、MakeAnAdministrator や SecAdmin などのアプリケーションで使用されるメッセージもあります。

この章のエラーメッセージでは、ほかのメッセージで使用されている `%d` や `%s` などの記号の代わりに、`{0}`、`{1}`、`{2}` などの記号が使用されています。これらの記号の値は、各メッセージに固有のものです。

`(SecSvc_000) Constructed object for {0}.`

説明: エラーメッセージに示された ID を持つセキュリティーオブジェクトのタイプが有効にされています。

原因: 設定されたセキュリティーオブジェクトが最初に参照され、Sun MSF セキュリティーリポジトリから使用するために有効にされたときに、情報メッセージが表示されました。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

`(SecSvc_001) Result = {0}.`

説明: セキュリティーオブジェクトが、エラーメッセージに示された結果を要求元に返しました。

原因: 有効なセキュリティーオブジェクトに対して、エラーメッセージに示された情報を提示することを要求したときに、情報メッセージが表示されました。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_002) New password was set for Principal {0}.

説明: エラーメッセージに示された認証済みの主体が、Sun MSF セキュリティーリポジトリでパスワードを変更しました。

原因: 既存のパスワードで認証が正常に行われたあと、次回の認証で使用する新しいパスワードを主体が設定しました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_003) Password must be validated before setting new password for Principal {0}.

説明: エラーメッセージに示された認証済みの主体が、Sun MSF セキュリティーリポジトリでパスワードを変更しましたが、要求されたとおりに既存のパスワードで正しく認証されませんでした。

対策: 必要に応じて、エラーメッセージに示された主体を権限のないユーザーが利用しているかどうかを調べます。

(SecSvc_004) The password has been validated for Principal {0}.

説明: Sun MSF セキュリティーリポジトリで、エラーメッセージに示された主体がそのパスワードで問題なく認証されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_005) Validation failed for Principal {0}.

説明: Sun MSF セキュリティーリポジトリで、エラーメッセージに示された主体がそのパスワードで認証されませんでした。

対策: 必要に応じて、エラーメッセージに示された主体を権限のないユーザーが利用しているかどうかを調べます。

(SecSvc_006) Principal {0} is suspended.

説明: 停止されていることが原因で、エラーメッセージに示された主体が認証を拒否されました。

原因: エラーメッセージに示された主体が認証を試みましたが、拒否されました。この主体は、管理者によって停止されているか、パスワード認証の連続失敗回数の制限を超えたことが原因で停止されています。

対策: 主体が停止された理由を調べます。必要に応じて、SecAdmin アプリケーションの `enable` コマンドを使用して、停止状態をリセットすることができます。

(SecSvc_007) Principal {0} password has expired.

説明: パスワードが期限切れになっていることが原因で、エラーメッセージに示された主体が認証を拒否されました。

原因: エラーメッセージに示された主体が認証を試みましたが、拒否されました。主体のパスワードの有効期限を超過しているため、これを変更する必要があります。

対策: 管理者が作業するか、認証時に主体がパスワードを変更することによって、主体のパスワードを更新します。

(SecSvc_008) Improper password format for Principal {0}.

説明: 主体に対して、無効な書式の新しいパスワードが指定されています。

原因: 設定済みの有効なパスワード書式 (com.sun.emp.security.passwordFormat) を基準として、許可されない文字が、Sun MSF セキュリティーリポジトリで設定される主体のパスワードに含まれています。つまり、設定されている値が numericOnly である場合に、数字以外の文字がパスワードに含まれているか、設定されている値が alphaOnly である場合に、英字以外の文字がパスワードに含まれています。

対策: その主体に対して新しいパスワードを設定しようとしているユーザーに、有効な書式を通知します。

(SecSvc_009) Cannot activate Role {1}; Principal {0} has not been authenticated.

説明: エラーメッセージに示された主体が、設定済みの役割の使用を有効にしようとしましたが、その主体のパスワードで正しく認証されていませんでした。

対策: 役割を有効にする前に主体が認証されるようにします。

(SecSvc_010) Cannot deactivate Role; Principal {0} has not been authenticated.

説明: エラーメッセージに示された主体が、有効な役割の使用を無効にしようとしましたが、その主体のパスワードで正しく認証されていませんでした。

対策: 役割を無効にする前に主体が認証されるようにします。

(SecSvc_011) Cannot activate Role {1}; Principal {0} has been suspended.

説明: 停止されていることが原因で、エラーメッセージに示された主体が役割の使用を有効にする処理を拒否されました。

原因: エラーメッセージに示された主体が、エラーメッセージに示された役割の使用を有効にしようとしましたが、拒否されました。この主体は、管理者によって停止されているか、パスワード認証の連続失敗回数の制限を超えたことが原因で停止されています。

対策: 主体が停止された理由を調べます。必要に応じて、SecAdmin アプリケーションの enablePrincipal コマンドを使用して、停止状態をリセットすることができます。

(SecSvc_012) Cannot deactivate Role; Principal {0} has been suspended.

説明: 停止されていることが原因で、エラーメッセージに示された主体が役割の使用を無効にする処理を拒否されました。

原因: エラーメッセージに示された主体が、役割の使用を無効にしようとしましたが、拒否されました。この主体は、管理者によって停止されているか、パスワード認証の連続失敗回数の制限を超えたことが原因で停止されています。

対策: 主体が停止された理由を調べます。必要に応じて、SecAdmin アプリケーションの enablePrincipal コマンドを使用して、停止状態をリセットすることができます。

(SecSvc_013) Principal {0} not allowed to activate Role {1}.

説明: 主体の設定済みの役割ではないことが原因で、エラーメッセージに示された主体が役割の使用を有効にする処理を拒否されました。

原因: エラーメッセージに示された主体が、エラーメッセージに示された役割の使用を有効にしようとしましたが、拒否されました。役割が、その主体によって使用されるように設定されていません。

対策: 必要な役割を使用して主体が設定された状態にします。

(SecSvc_014) Principal {0} has logged off.

説明: エラーメッセージに示された主体がログアウトしており、認証された状態ではありません。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_015) Principal {0} has been denied access to {1}.

説明: エラーメッセージに示された主体が、エラーメッセージに示されたリソースタイプまたはリソース名へのアクセス権を拒否されました。

原因: エラーメッセージに示された主体が、アクセス権を使用して、エラーメッセージに示されたリソースタイプまたはリソース名にアクセスしようとしましたが、拒否されました。その主体に適用される設定済みの Sun MSF セキュリティーリポジトリのルールには、エラーメッセージに示された、リソースドメイン内のリソースタイプまたはリソース名へのアクセス権が含まれていないため、アクセスは拒否されます。Sun MSF のセキュリティーポリシーが、この要求を「受け入れない」ように設定されている場合 (この設定がデフォルト)、拒否されたことがアプリケーションに返されます。要求を受け入れるように設定されている場合は、拒否されたことがログに記録されるだけで、アプリケーションは拒否されていない状態と同じようにリソースにアクセスすることが可能です (com.sun.emp.security.denialReaction=FAIL|WARN)。

対策: 必要な役割に主体を割り当て、必要なリソースが含まれているリソースドメインへの適切なアクセス権を主体に指定します。

(SecSvc_016) Principal {0} has been granted access to {1}.

説明: エラーメッセージに示された主体に対して、エラーメッセージに示されたリソースタイプまたはリソース名へのアクセス権で、アクセスが許可されました。

原因: エラーメッセージに示された主体が、アクセス権を使用して、エラーメッセージに示されたリソースタイプまたはリソース名にアクセスし、許可されました。その主体に適用される設定済みの Sun MSF セキュリティーリポジトリのルールには、エラーメッセージに示された、リソースドメイン内のリソースタイプまたはリソース名へのアクセス権が含まれています。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。ただし、アクセスを許可しない場合は、主体が適切なアクセス権で設定されていることを確認するか、エラーメッセージに示されたリソースが含まれるリソースドメインへの適切なアクセス権が主体の役割に指定されていることを確認します。

(SecSvc_020) Principal {1} has primary Group {0}.

説明: エラーメッセージに示されたグループを一次グループとして使用して、エラーメッセージに示された主体が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_021) Principal {1} has primary Role {0}.

説明: エラーメッセージに示された役割を一次役割として使用して、エラーメッセージに示された主体が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_022) Groups for Principal {0} include: {1}.

説明: エラーメッセージに示されたグループのメンバーとして、エラーメッセージに示された主体が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_023) Groups for Role {0} include: {1}.

説明: エラーメッセージに示されたグループのメンバーとして、エラーメッセージに示された役割が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_024) Roles for Principal {0} include: {1}.

説明: エラーメッセージに示された役割のメンバーとして、エラーメッセージに示された主体が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_025) Group {0} has Role {1}.

説明: エラーメッセージに示された役割を使用して、エラーメッセージに示されたグループが Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_026) Principals with permissions to resource domain {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインへのアクセス権を使用して、エラーメッセージに示された主体が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_027) Groups with permissions to resource domain {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインへのアクセス権を使用して、エラーメッセージに示されたグループが Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_028) Roles with permissions to resource domain {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインへのアクセス権を使用して、エラーメッセージに示された役割が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_029) Permissions for {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインのアクセス権を使用して、エラーメッセージに示された役割が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_030) Parent of {0} is {1}.

説明: エラーメッセージに示された役割を階層内の親として使用して、エラーメッセージに示された役割が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_031) Children of {0} include: {1}.

説明: エラーメッセージに示された役割を階層内の子 (下位役割) として使用して、エラーメッセージに示された役割が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_032) Principals with Permissions to Resource Domain {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインへのアクセス権を使用して、エラーメッセージに示された主体が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_033) Groups with Permissions to Resource Domain {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインへのアクセス権を使用して、エラーメッセージに示されたグループが Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_034) Roles with Permissions to Resource Domain {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインへのアクセス権を使用して、エラーメッセージに示された役割が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_035) Principals for Group {0} include: {1}.

説明: エラーメッセージに示された主体をメンバーとして使用して、エラーメッセージに示されたグループが Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_036) Principals for Role {0} include: {1}.

説明: エラーメッセージに示された主体をメンバーとして使用して、エラーメッセージに示された役割が Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_037) Resources of Resource Domain {0} include: {1}.

説明: エラーメッセージに示されたリソースドメインのメンバーとして、エラーメッセージに示されたリソースが Sun MSF セキュリティーリポジトリで設定されています。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_040) Resource {0} requires {2} of Permissions {1}.

説明: エラーメッセージに示されたリソースは、Sun MSF セキュリティーリポジトリ上で、エラーメッセージに示された一部またはすべてのアクセス権の付与を必要とするように設定されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_100) Password was reset for Principal {0} by Administrative Principal {1}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体のパスワードが Sun MSF セキュリティーリポジトリで変更されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_101) Password duration was reset for Principal {0} by Administrative Principal {1}; min = {2} max = {3}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体のパスワードの有効期間の設定が Sun MSF セキュリティーリポジトリで変更されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_102) Principal {0} has been suspended by Administrative Principal {1}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体のパスワードが Sun MSF セキュリティーリポジトリで停止されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_103) Principal {0} has been enabled by Administrative Principal {1}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体のパスワードが Sun MSF セキュリティーリポジトリで有効にされました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_104) Password expiration date for Principal {0} was reset to {2} by Administrative Principal {1}

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体の停止中のパスワードが Sun MSF セキュリティーリポジトリで有効にされました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_110) {0} was added by Administrative Principal {1}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体、リソース、アクセス権タイプ、またはリソースタイプが Sun MSF セキュリティーリポジトリで作成されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_111) {0} with parent {1} was added by Administrative Principal {2}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された、階層内の親を使用して、エラーメッセージに示された役割、グループ、またはリソースドメインが Sun MSF セキュリティーリポジトリで作成されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_112) The attempt to add {0} by Administrative Principal {1} failed; duplicate.

説明: エラーメッセージに示されたセキュリティー管理者主体が、エラーメッセージに示された主体、役割、グループ、リソースドメイン、リソース、アクセス権タイプ、またはリソースタイプを Sun MSF セキュリティーリポジトリで作成しようとしましたが、すでに存在するために失敗しました。

対策: そのコンポーネントがすでに存在する理由を調べ、Sun MSF セキュリティーリポジトリの設定を修正する必要があるかどうかを判断します。

(SecSvc_113) {0} was set as parent for {1} by Administrative Principal {2}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された、階層内の親を使用して、エラーメッセージに示された役割、グループ、またはリソースドメインが Sun MSF セキュリティーリポジトリで更新されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_114) {0} was deleted by Administrative Principal {1}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体、役割、グループ、リソースドメイン、リソース、アクセス権タイプ、またはリソースタイプが Sun MSF セキュリティーリポジトリで削除されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_115) The attempt to delete {0} by Administrative Principal {1} failed; not found.

説明: エラーメッセージに示されたセキュリティー管理者主体が、エラーメッセージに示された主体、役割、グループ、リソースドメイン、リソース、アクセス権タイプ、またはリソースタイプを Sun MSF セキュリティーリポジトリで削除しようとしましたが、そのコンポーネントが存在しないために失敗しました。

対策: そのコンポーネントが見つからなかった理由を調べ、Sun MSF セキュリティーリポジトリの設定を修正する必要があるかどうかを判断します。

(SecSvc_116) {0} was added to {1} by Administrative Principal {2}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された、階層内の役割、グループ、またはリソースドメインに対して、エラーメッセージに示された主体またはリソースが Sun MSF セキュリティーリポジトリでメンバーとして追加されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_117) The attempt to use {0} to set parent by Administrative Principal {1} failed; not found.

説明: エラーメッセージに示されたセキュリティー管理者主体が、エラーメッセージに示された役割、グループ、またはリソースドメインを、エラーメッセージに示された、階層内の親を使用して Sun MSF セキュリティーリポジトリで更新しようとしましたが、その親が存在しないために失敗しました。

対策: そのコンポーネントが見つからなかった理由を調べ、Sun MSF セキュリティーリポジトリの設定を修正する必要があるかどうかを判断します。

(SecSvc_118) {0} was set to {1} by Administrative Principal {2}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示されたグループが、エラーメッセージに示された役割に設定されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_119) The attempt to add {0} to {1} by Administrative Principal {2} failed; not found.

説明: エラーメッセージに示されたセキュリティー管理者主体が、エラーメッセージに示された主体またはリソースを、エラーメッセージに示された役割、グループ、またはリソースドメインに対して Sun MSF セキュリティーリポジトリでメンバーとして追加しようとしましたが、そのコンポーネントが存在しないために失敗しました。

対策: そのコンポーネントが見つからなかった理由を調べ、Sun MSF セキュリティーリポジトリの設定を修正する必要があるかどうかを判断します。

(SecSvc_120) {0} was removed from {1} by Administrative Principal {2}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された役割、グループ、またはリソースドメインから、エラーメッセージに示された主体またはリソースが Sun MSF セキュリティーリポジトリでメンバーとして削除されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_121) The attempt to remove {0} from {1} by Administrative Principal {2} failed; not found.

説明: Sun MSF セキュリティーリポジトリで、エラーメッセージに示されたセキュリティー管理者主体が、エラーメッセージに示された主体またはリソースを、エラーメッセージに示された役割、グループ、またはリソースドメインからメンバーとして削除しようとしましたが、そのコンポーネントが存在しないために失敗しました。

対策: そのコンポーネントが見つからなかった理由を調べ、Sun MSF セキュリティーリポジトリの設定を修正する必要があるかどうかを判断します。

(SecSvc_122) {1} was set as primary for Principal {0} by Administrative Principal {2}.

説明: エラーメッセージに示されたセキュリティー管理者主体によって、エラーメッセージに示された主体の役割またはグループが Sun MSF セキュリティーリポジトリで一次役割または一次グループ (デフォルト) として設定されました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_123) The attempt to set {1} as primary of {0} by Administrative Principal {2} failed; not found.

説明: エラーメッセージに示されたセキュリティー管理者主体が、エラーメッセージに示された主体の一次役割または一次グループを Sun MSF セキュリティーリポジトリで設定しようとしましたが、そのコンポーネントが存在しないために失敗しました。

対策: そのコンポーネントが見つからなかった理由を調べ、Sun MSF セキュリティーリポジトリの設定を修正する必要があるかどうかを判断します。

(SecSvc_130) Permissions {0} to Resource Domain {1} for {2} were added by Administrative Principal {3}.

説明: エラーメッセージに示された主体または役割の、エラーメッセージに示されたリソースドメインのリソースのアクセス権は、エラーメッセージに示されたセキュリティー管理者主体によって Sun MSF セキュリティーリポジトリに追加されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_131) Permissions {0} to Resource Domain {1} for {2} were removed by Administrative Principal {3}.

説明: エラーメッセージに示された主体または役割の、エラーメッセージに示されたリソースドメインのリソースへのアクセス権は、エラーメッセージに示されたセキュリティー管理者主体によって Sun MSF セキュリティーリポジトリから削除されています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_200) {0} value must be a valid date, eg. {1}

説明: エラーメッセージに示された値は、有効なデータ形式で (ホストのロケールに対して) 指定されませんでした。

対策: 値が正しく指定されない原因 (MSFconfig.properties ファイルの com.sun.emp.security.passwordExpiresDate プロパティーなど) を修正します。

(SecSvc_201) {0} value cannot be less than zero

説明: エラーメッセージに示された値には、負の数値を指定できません。

対策: 値が正しく指定されない原因 (MSFconfig.properties ファイルの com.sun.emp.security.passwordMaxDaysAllowed プロパティーなど) を修正します。

(SecSvc_202) {0} value must be a positive integer

説明: エラーメッセージに示された値に、数値以外の値が指定されています。

対策: 値が正しく指定されない原因 (MSFconfig.properties ファイルの com.sun.emp.security.passwordMinDaysRequired プロパティーなど) を修正します。

(SecSvc_203) {0} invalid value: {1} acceptable value: {2}

説明: エラーメッセージに示された値が、無効な設定を使用して指定されています。有効な設定が一覧表示されます。

対策: 値が正しく指定されない原因 (MSFconfig.properties ファイルの com.sun.emp.security.denialReaction プロパティーなど) を修正します。

(SecSvc_204) {0} invalid value: {1} acceptable value range: {2} to {3}

説明: エラーメッセージに示された値が、無効な設定を使用して指定されています。有効な設定の範囲が一覧表示されます。

対策: 値が正しく指定されない原因 (MSFconfig.properties ファイルの com.sun.emp.security.passwordMaxLength プロパティーなど) を修正します。

(SecSvc_205) {0} non-zero value cannot be less than {1}

説明: エラーメッセージに示された 1 番目の値は、2 番目の値以上でなければなりません。

原因: エラーメッセージに示された 1 番目の値 (passwordMaxLength など) が、ゼロ以外の値で指定されており、指定されたゼロ以外の 2 番目の値 (passwordMinLength など) よりも小さいことが原因です。このような値の組み合わせは矛盾しているため、使用できません。

対策: 1 番目の値を、2 番目の値と等しくなるように設定し直します。この設定が有効であるかどうかを確認します。有効でない場合は、値が正しく指定されない原因 (1 番目または 2 番目の値) を修正しますが、場合によってはいずれかの値をゼロに設定します。

(SecSvc_211) Cannot create Security Administrator: ...repository not empty and Admin chose not to recreate.

説明: MakeAnAdministrator アプリケーションを使用して、セキュリティー管理者用にリポジトリを作成し、初期化しようとしたときに、空でないセキュリティーリポジトリがすでに存在していました。

原因: MakeAnAdministrator アプリケーションが、空でないセキュリティーリポジトリがすでに存在することを検出しましたが、そのリポジトリの削除または再作成は行われませんでした (詳細については、SecSvc_213 のメッセージを参照)。このメッセージが表示されると、MakeAnAdministrator アプリケーションは終了します。

対策: 既存のセキュリティーリポジトリの内容を調べて、このリポジトリを MakeAnAdministrator を使用して削除し、作成し直す必要があるかどうかを判断します。

(SecSvc_212) Exception trying to create Security Administrator principal {0}: {1}

説明: エラーメッセージに示されたセキュリティー管理者主体用のセキュリティーリポジトリを作成し、初期化しようとしたときに、エラーメッセージに示された例外が MakeAnAdministrator アプリケーションで発生しました。

対策: エラーメッセージに示された例外の原因を調査して修正し、`msfinitr` コマンドを再度実行します。サポートが必要な場合は、ご購入先に問い合わせてください。

(SecSvc_213) Repository not empty;
...do you want to destroy current contents and reinitialize (yes/no)?

説明: MakeAnAdministrator アプリケーションを使用して、セキュリティー管理者用にリポジトリを作成し初期化しようとしたときに、空でないセキュリティーリポジトリがすでに存在していました。

原因: MakeAnAdministrator アプリケーションが、空でないセキュリティーリポジトリがすでに存在していることを検出し、そのリポジトリを削除し、再作成するかどうかを尋ねるメッセージを表示しています。

対策: そのセキュリティーリポジトリの内容を保持せずに、このセキュリティー管理者用に新しいリポジトリを作成し、初期化する場合にのみ、`yes` と入力します。このように入力しない場合は、既存のリポジトリが保持されます (SecSvc_211 のメッセージを参照)。

(SecSvc_214) Security Administrator principal: {0}
...successfully created, with permissions to resource domain: {1}

説明: エラーメッセージに示されたセキュリティー管理者主体が、初期化されたセキュリティーリポジトリ上に作成され、セキュリティールールの追加設定を行うために必要な (エラーメッセージに示されたリソースドメインへの) アクセス権が設定されました。

原因: 指定したユーザー ID およびパスワードと、必要に応じて指定した管理リソースドメインへのアクセス権が設定されたセキュリティーリポジトリを、MakeAnAdministrator アプリケーションが作成し、初期化しました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_216) Unknown exception in MakeAnAdministrator: {0}

説明: このエラーメッセージは、MakeAnAdministrator アプリケーションの実行中に予期しないエラーが発生したことを示しています。

対策: MSFconfig.properties ファイルの設定情報を確認し、エラーを修正してから、このアプリケーションを再度実行します。問題が解決しない場合は、ご購入先に問い合わせてください。

(SecSvc_217) Cannot write to keyfile: {0}

説明: 鍵ファイルが書き込み可能になっていない場合、このエラーメッセージが MakeAnAdministrator アプリケーションの実行中に表示されます。

対策: 鍵ファイルとディレクトリの書き込み権を確認します。

(SecSvc_218) Cannot create security secret key: {0}

説明: 秘密鍵の作成に問題がある場合、このエラーメッセージが MakeAnAdministrator アプリケーションの実行中に表示されます。

対策: {0} のエラーを検査します。鍵ファイルとディレクトリの書き込み権を確認します。

(SecSvc_220) SecurityServer arguments incorrectly specified

説明: msfserver コマンドに指定したオプションが正しくなかったため、このコマンドが終了しました。

対策: 正しい構文を使用して、msfserver コマンドを再度実行します。

(SecSvc_221) Invalid port number {0}

説明: 指定したセキュリティーサーバーのポート番号が無効です。

原因: 指定したポート番号が無効であり、Sun MTP 領域からのソケット接続の待機に使用できないことをセキュリティーサーバーが検出しました。

対策: MSFconfig.properties ファイルの com.sun.emp.security.serverPortNumber プロパティーの値を、使用する正しいソケットポート番号に変更します。

(SecSvc_222) Security Server started, using port {0}

説明: セキュリティーサーバーが正常に起動し、エラーメッセージに示されたポート番号で Sun MTP 領域からソケット接続を待機しています。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_223) Security Server encountered exception from {0}: {1}

説明: セキュリティーサーバーが、エラーメッセージに示された内部サービスからの例外を検出しました。

原因: セキュリティーサーバーが実行したサービスで、予期しない例外が発生しました。セキュリティーサーバーは引き続き実行されますが、例外が発生した結果、その一部またはすべての機能が使用できなくなることがあります。

対策: 報告された例外を調査し、セキュリティーサーバーを停止する必要があるかどうかを判断します。サポートが必要な場合は、ご購入先に問い合わせてください。

(SecSvc_224) Security Server terminated

説明: セキュリティーサーバーを停止するコマンドに応じて、セキュリティーサーバーが正常に終了しました。

対策: 情報を示す監査メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_225) Security Server terminated, exception: {0}

説明: 予期しない内部の例外が原因で、セキュリティーサーバーが異常終了しました。

対策: 報告された例外を調査し、セキュリティーサーバーを稼動状態に戻すことが可能であるかどうか、またはその必要があるかどうかを判断します。サポートが必要な場合は、ご購入先に問い合わせてください。

(SecSvc_226) Security Server login failed for userid {0}

説明: msfserver コマンドとともに入力したユーザー ID とパスワードでセキュリティーサーバーへのログインおよび認証に失敗しました。

対策: 正しいユーザー ID とパスワードを使用して、コマンドを再度実行します。

(SecSvc_227) Invalid Security Server command: {0}

説明: 指定したコマンドオプションが、msfserver の有効なコマンドオプションではありません。

対策: msfserver コマンドの構文を確認し、有効なコマンドオプションを使用して再度実行します。

(SecSvc_228) Security Server successfully completed {0}

説明: このメッセージは、指定した msfserver コマンド (RefreshPolicy、DumpEntries、または ShutdownSecurity) が正常に完了したことを通知します。

対策: アクションは必要ありません。

(SecSvc_229) Security Server rejected {0}

説明: エラーメッセージに示されたセキュリティーサーバーコマンドが実行されませんでした。多くの場合、原因は msfserver コマンドの認証されたユーザー ID に、そのコマンド (RefreshPolicy など) を実行する権限がありません。

対策: セキュリティー監査ログを調べて、対応するアクセス拒否メッセージを確認し、必要な権限を持つユーザー ID とパスワードを使用して、この要求を再度実行します。

(SecSvc_230) Security Server protocol error: {0}

説明: 内部プロトコルエラーが、セキュリティーサーバーとこのコマンドとの間で発生しました。

対策: ご購入先に問い合わせてください。

(SecSvc_231) Security Server not responding on port {0}: {1}

説明: セキュリティーサーバーが、エラーメッセージに示されたソケットポート番号で応答しません。セキュリティーサーバーが実行されていないか、MSFconfig.properties ファイルで設定されているポートが、セキュリティーサーバーの起動時に使用されたポートと一致していません。

対策: 設定情報を確認し、エラーを修正してから、セキュリティーサーバーを起動します。問題が解決しない場合は、ご購入先に問い合わせてください。

(SecSvc_233) Unknown exception in CreateLdapRepository: {0}

説明: このエラーメッセージは、CreateLdapRepository ツールの実行中に予期しないエラーが発生したことを示しています。問題が解決しない場合は、ご購入先に問い合わせてください。

対策: MSFconfig.properties ファイルの設定情報を確認し、エラーを修正してから、このアプリケーションを再度実行します。問題が解決しない場合は、ご購入先に問い合わせてください。

(SecSvc_250) Security {0} name: {1}

説明: このメッセージには、スキーマ、管理者、およびユーザー名が代替文字列で示されます。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_251) Creating security admin: {0}...

説明: このメッセージは、MakeAnAdministrator アプリケーションから発行されるもので、リポジトリでセキュリティー管理者が作成されていることを示しています。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_253) Enter security {0} password (or 'quit'):

説明: これは、スキーマ、管理者、およびユーザーのパスワードの入力を求めるメッセージです。

対策: 各プロンプトに対して、適切な値を入力します。

(SecSvc_258) Authentication problem.Check username and password and try again.

説明: MakeAnAdministrator アプリケーションの実行中、このメッセージはパスワードが正しくないことを示します。

対策: パスワードを入力し直します。問題が解決しない場合は、quit と入力して MakeAnAdministrator アプリケーションを終了し、データベース管理者に問い合わせてください。

(SecSvc_259) Deleting old repository tables...

説明: このメッセージは、古いリポジトリテーブルの削除中であることを示しています。このメッセージが表示されるのは、MakeAnAdministrator アプリケーションが実行されているときです。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_260) Creating new repository tables...

説明: このメッセージは、新しいリポジトリテーブルの作成中であることを示しています。このメッセージが表示されるのは、MakeAnAdministrator アプリケーションが実行されているときです。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_261) Granting accesses to repository...

説明: このメッセージは、リポジトリテーブルへのアクセスの承認中であることを示しています。このメッセージが表示されるのは、MakeAnAdministrator アプリケーションが実行されているときです。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_262) Loading security configuration data...

説明: このメッセージは、設定値の読み込み中であることを示しています。このメッセージが表示されるのは、MakeAnAdministrator アプリケーションが実行されているときです。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_263) Creating new secret key...

説明: このメッセージは、秘密鍵の生成中であることを示しています。この鍵は、あとで鍵ファイルに追加されます。このメッセージが表示されるのは、MakeAnAdministrator アプリケーションが実行されているときです。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_264) This character not allowed in DB passwords: {0}

説明: このメッセージは、許可されていない文字が使用されていることを示しています。このメッセージが表示されるのは、MakeAnAdministrator アプリケーションが実行されているときです。

対策: quit と入力して MakeAnAdministrator アプリケーションを終了し、データベース管理者に連絡して、無効な文字が含まれていない新しいパスワードを入手します。

(SecSvc_265) Keyfile successfully updated

説明: このメッセージは、セキュリティーリポジトリとして使用されているデータベースの暗号化パスワードが含まれる鍵ファイルを msfupdkey ユーティリティーが正常に更新したことを示しています。鍵ファイルは、MSFconfig.properties ファイルの adapterKeyFile プロパティーで定義されています。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecSvc_266) Keyfile not found: {0}

説明: エラーメッセージに示された名前のファイルは存在しません。鍵ファイルは、MSFconfig.properties ファイルの adapterKeyFile プロパティーで定義されています。

原因: msfinitr ユーティリティーを実行して鍵ファイルと Sun MSF リポジトリを作成する作業を行なっていません。または、鍵ファイルが削除されているため、復元する必要があります。

対策: 鍵ファイルが見つからない理由を調べ、問題を修正してから、必要に応じて msfupdkey ユーティリティーを再度実行します。

SecSvc_300=(SecSvc_300) Security Repository Error occurred: {0}

説明: このメッセージは、セキュリティーリポジトリに問題がある場合に表示されます。たとえば、データベースが機能していない、テーブルが見つからない、またはリポジトリへのネットワーク接続が切断されている、といった問題があります。また、このメッセージは監査ログに書き込まれます。

対策: セキュリティーシステムのスーパー管理者に、この問題を通知し、適切なログ情報を提供します。

SecSvc_301=(SecSvc_301) Unknown Security Error occurred: {0}

説明: SecAdmin アプリケーションの動作中にリポジトリ以外のエラーが発生した場合、このメッセージが SecAdmin によって表示されます。SecAdmin アプリケーションは、msfadmin コマンドで起動します。また、このメッセージは監査ログに記録されます。

対策: ご購入先に問い合わせます。

(SecSvc_FATAL) {0}

説明: 予期しない状態 (通常は例外) が発生しました。

原因: このメッセージには、検出された FATAL 状態に関する情報が含まれています。関連するセキュリティーサービスは利用できなくなっています。

対策: ご購入先に問い合わせます。

(SecLog_001) Starting the Log Server.

説明: このメッセージは、ログサーバーが起動したときにトレースログとメッセージログのファイルに表示されます。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecLog_002) Creating a server socket on port {0}.

説明: このメッセージは、ログサーバーが起動したあと、ソケットが正常に作成されたときに表示されます。{0} は、ポート番号に置き換えられます。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecLog_003) Sending output to the console and to the file {0}.

説明: このメッセージは、ロガーが出力用のファイルとコンソールを正常に開いたときに表示されます。{0} は、ログファイル名に置き換えられます。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecLog_004) Unable to open the MessageCatalog properties file {0}.

説明: ロガーが、各国語版のメッセージが含まれるプロパティーファイルを開けませんでした。{0} には、ファイル名が示されます。

原因: ロガーが、secsvc_messages プロパティーファイルを見つけることができません。

対策: $CLASSPATH を確認します。問題が解決しない場合は、ご購入先に問い合わせてください。

(SecLog_005) Established connection with {0} at {1}.

説明: このメッセージは、クライアントがログサーバーに正常に接続したときに表示されます。{0} は、クライアントのホスト名です。{1} は、接続した日付と時刻です。

(SecLog_006) Connection from {0} closed at {1}.

説明: このメッセージは、接続が切断されたときに、ログのコンソールとファイルに表示されます。{0} は、クライアントのホスト名です。{1} は、接続が切断された日付と時刻です。

(SecLog_007) Unable to get the socket's input stream.

説明: このメッセージは、ソケットの入力ストリームエラーを示しています。

原因: ネットワークが輻輳しているか、ホスト名またはポートが正しくない可能性があります。

対策: MSFconfig.properties ファイルを調べて、ホスト名またはポートが正しいかどうかを確認します。

(SecLog_008) Unable to open the file {0}.

説明: このエラーメッセージは、ロガーが出力ファイルを開くことができなかった場合に表示されます。{0} には、ファイルの名前が示されます。

原因: ログファイルが存在するディレクトリへのアクセス権が正しくないか、ディレクトリが存在しない可能性があります。

対策: ディレクトリが存在することと、そのアクセス権が正しいかどうかを確認します。

(SecLog_009) Sending output to the console only.

説明: このメッセージは、出力がコンソールのみに送信され、ログファイルに記録されていないことを示しています。

対策: 情報メッセージであり、ユーザーのアクションは必要ありません。

(SecLog_100) Security Logging configuration errors, terminating

説明: このメッセージが表示されるのは、Sun MSF コマンドを実行したときに、MSFconfig.properties ファイルで設定されているログ記録のプロパティー値に問題がある場合です。このメッセージの前に、プロパティーが正しく設定されていないことを示すメッセージが表示されます。

対策: MSFconfig.properties ファイルで、ログ記録のプロパティーを修正し、Sun MSF コマンドを再度実行します。

```
(SecLog_101) Security Message Log open error, terminating: {0}
(SecLog_102) Security Message Log close error, terminating: {0}
(SecLog_103) Security Message Log write error, terminating: {0}
(SecLog_104) Security Message Log flush error, terminating: {0}
(SecLog_105) Security Message Log failed, terminating: {0}
```

説明: これらのメッセージは、Sun MSF コマンドが実行されたコンソールに表示されます。また、Sun MSF のセキュリティーメッセージのログ記録に失敗したことを示しています。コマンドはすぐに終了します。

原因: コマンドの実行中にセキュリティーメッセージのログ収集サーバーが終了し、Sun MSF が必要なセキュリティーイベントをログに記録できませんでした。

対策: `msflog` コマンドを実行してセキュリティーメッセージのログ収集サーバーを再度起動し、終了されたコマンドを再度実行します。

```
(SecLog_111) Security Trace Log open error: {0}
(SecLog_112) Security Trace Log close error: {0}
(SecLog_113) Security Trace Log write error: {0}
(SecLog_114) Security Trace Log flush error: {0}
(SecLog_115) Security Trace Log failed: {0}
```

説明: トレースロガーに問題があり、トレースが有効になっている場合、これらのメッセージが、Sun MSF コマンドが実行されたコンソールに表示されます。メッセージは、Sun MSF のセキュリティートレースのログ記録に失敗したことを示しています。コマンドは引き続き実行されます。

原因: コマンドの実行中にセキュリティートレースのログ収集サーバーが終了し、内部のトレース処理を続行できませんでした。

対策: セキュリティートレースのログ収集サーバーを、`msflog` コマンドを実行して再度起動します。サーバーを再度起動すると、コンソールから実行された新しいコマンドでトレースが実行されます。失敗したときに実行されていたコマンドは、そのコマンドによって起動されたプロセスを停止して再度起動しない限り、トレース内容を記録しません。

```
(SecSvc_232) Security Server terminated unexpectedly
```

説明: セキュリティーサーバーが終了しましたが、内部的に生成された例外やエラーが原因ではありませんでした。

対策: このメッセージの前に表示されたほかのメッセージを調べて、セキュリティーサーバーが停止した原因を特定します。

付録 A

Sun MSF への RACF のマッピング

Sun MSF には、IBM の CICS 用メインフレーム RACF と似ている、Sun MTP 用の外部セキュリティーマネージャー (ESM) 機能が用意されています。この付録では、Sun MSF への RACF セキュリティーモデルおよびコマンドのマッピングについて説明します。この章の内容は、次のとおりです。

セキュリティーモデルのマッピング

RACF には、システムリソースの個々のユーザーに関する情報や、保護が必要なリソースに関する情報を記録したり照会したりする機能があります。この情報は、ユーザープロファイルとリソースプロファイルに格納されています。また、RACF には、プロファイルが定義されているリソースへのアクセスが許可されているユーザーやユーザーグループ、または許可されていないユーザーやユーザーグループを定義したり照会したりする機能もあります。この情報は、リソースを保護するプロファイル内のアクセスリストに保持されています。さらに、RACFでは、サブシステム、または MVS システムで実行されているジョブから発行された要求の処理、RACF に対して定義されているユーザーの識別情報の認証、およびリソースへのアクセスの承認のチェックを行うことができます。このほか、RACF には、ユーザーのサインオンやサインオフ、RACF コマンドの発行、および保護されたリソースへのアクセスなどの、セキュリティー関連のイベントをログに記録する機能もあります。

Sun MSF にも、グループ化された個々のユーザーやリソースに関する情報を記録したり照会したりする、同等の機能が SecAdmin ユーティリティーに用意されています。ユーザーは役割別にグループ化され、リソースはリソースドメイン別にグループ化されます。また、Sun MSF にも、保護されるリソースが含まれるリソースドメインに対する、これらのユーザーおよび役割のアクセス権を定義したり照会したりす

る、同等の機能があります。これらの付与されたアクセス権は、アクセスリストと同じです。Sun MSF と RACF との重要な相違点は、RACF にはアクセスを明示的に禁止するオプションがあるのに対して、Sun MSF ではアクセスを許可することしか行われないことです。Sun MSF では、アクセスの禁止は、リソースへのアクセス権を付与しないことによって実現されます。Sun MSF は、定義されているユーザーの認証要求を処理し、そのユーザーのリソースへのアクセス権をチェックすることができます。このほか、Sun MSF では、ユーザーのログインとログオフ、SecAdmin コマンドの実行、および保護されたリソースへのアクセスの試行といったセキュリティー関連のイベントが正常に行われたか、失敗したかが記録されます。

管理権限

RACF には、階層的な管理構造が用意されています。RACF セキュリティー管理者は、階層の最上位で定義され、システム全体のセキュリティーを管理する権限を持っています。その他のユーザーには、グループレベルで RACF 管理を実行する権限が委託されることがあります。これは、RACF 管理にのみ適用される `SPECIAL` という権限を通じて行われます。

Sun MSF にも階層的な管理構造がありますが、RACF とは異なり、専用の権限はありません。その代わり、保護されたリソースが含まれるリソースドメインへのユーザーおよび役割のアクセス権には、同じモデルが利用されています。この場合、リソースは Sun MSF ユーザー、役割、リソースドメイン、およびリソース自体であり、アクセス権は、所定のユーザーが実行可能な管理作業を定義します。Sun MSF のセキュリティー管理者は、システム全体のセキュリティーを管理する権限を持っており、すべてのリソースに共通のアクセス権モデルを使用して、ほかのユーザーにアクセス権を個別に委託することができます。

ユーザーの管理方法

RACF は、RACF データベースのユーザープロファイルという形式でユーザーのデータを保持しています。これらのユーザープロファイルは、次の 1 つまたは複数のセグメントで構成されています。

- RACF セグメント。RACF ユーザープロファイルの基本的な情報が保持されています。
- CICS セグメント。各 CICS ユーザーのデータが保持されています。

ユーザーの RACF セグメントは、英数字のユーザー ID で識別されます。このセグメントには、ユーザーの名前、ユーザーのプロファイルの所有者、ユーザーが所属するデフォルトのグループ、およびユーザーのパスワードが格納されています。

CICS セグメントで指定されている情報は、オペレータのクラス、各オペレータに割り当てられる 1 ～ 3 文字のオペレータ識別コード、オペレータの優先度の値、およびユーザーが最後に端末を使用してから CICS が端末をタイムアウトするまでに経過した時間です。

ユーザープロファイルの RACF セグメントとオプションの CICS セグメントは、`ADDUSER` コマンドを使用して定義します。次に例を示します。

```
ADDUSER CICSUSER  DFLTGRP(group-id) NAME(user-name)
         OWNER(user-id | group)
         PASSWORD(password)
         CICS(OPCLASS(1,2,...,n) OPIDENT(identifier) OPPRTY(priority)
                   TIMEOUT(timeout-value)  XRFSOFF(xrf-sign-off-option))
```

Sun MSF は、Sun MSF データベースの主体エントリという形式でユーザーのデータを保持しています。このエントリは、ユーザーの英数字のユーザー ID で識別されます。エントリには、ユーザーが所属するデフォルトの役割、ユーザーの説明、およびユーザーのパスワードとパスワードの有効期間の設定が格納されています。Sun MSF の主体エントリには、オプションの CICS 情報に相当する箇所はありません。そのような情報を必要とする場合、Sun MTP のサインオンテーブル (SNT) のユーザーエントリに保持されています。

ユーザーの Sun MSF 主体エントリは `createPrincipal` コマンドを使用して定義されており、そのデフォルトの役割は `setPrimaryRole` コマンドを使用して割り当てられています。次に例を示します。

```
cpr, user-id, password, pwexpdate, pwmaxdays, pwmindays, susp-flag, description
spr, user-name, role-id
```

ユーザーグループの管理方法

RACF では、グループプロファイルでユーザーグループが定義されています。グループプロファイルには、グループの所有者、そのグループのサブグループ、および接続されるユーザーのリストなどの、グループに関する情報を格納できます。グループのメンバーであるユーザーは、保護されたリソースへの共通のアクセス権限を共有できます。たとえば、次のコマンドを実行すると、新しいユーザーグループが作成され、既存のグループから新しいグループにユーザーが移動します。

```
ADDGROUP  group-name2
REMOVE  user1  GROUP(group-name1)
CONNECT  user1  GROUP(group-name2)
```

Sun MSF でも、同じようにユーザー (主体) を役割別にグループ化できます。各役割には、役割 ID、その役割のサブ役割、その役割のメンバーであるユーザー、役割の説明といった、役割に関する情報があります。役割のメンバーであるユーザーは、保護されたリソースへの共通のアクセス権限を共有できます。たとえば、次のコマンドでは、新しい役割が作成され、メンバーとして主体が割り当てられます。

```
createRole,group-name2,Role for users with basic access rights
addPrincipalToRole,user1,group_name2
```

リソースおよびアクセス権の管理方法

保護された CICS リソースを扱う RACF の多くのアクティビティーには、一般的なリソースプロファイルの作成、変更、削除が含まれます。一般的なリソースプロファイルは、RDEFINE コマンドを使用して作成します。プロファイルを作成したら、PERMIT コマンドを使用して、そのプロファイルのアクセスリストを作成します。次に例を示します。

```
RDEFINE   class-name   profile-name   UACC(NONE)
PERMIT    profile-name   CLASS(class-name)
          ID(user | group)   ACCESS(access-authority)
```

CICS に固有の各リソースクラスには、RACF に対して定義された 2 つのリソースクラス名があります。1 番目のクラス名は、CICS のトランザクションまたはプログラムなどのリソースと名前が一致するプロファイルが定義されているメンバークラスの名前です。たとえば、個々のリソース名のアクセスリストを定義するには、次のコマンドを実行します。

```
RDEFINE  TCICSTRN CEMT UACC(NONE)
PERMIT   CEMT CLASS(TCICSTRN) ID(group1, group2) ACCESS(READ)
```

2 番目のクラス名は、RACF のリソースグループクラスです。RDEFINE コマンドを ADDMEM オペランドとともに使用して、リソースグループクラスのプロファイルを定義するほか、グループのメンバーとしてリソースを追加します。次に例を示します。

```
RDEFINE  GCICSTRN CICSTRANS UACC(NONE)
         ADDMEM(CEMT, CEDA, CEDB)
PERMIT   CICSTRANS  CLASS(GCICSTRN) ID(group1, group2) ACCESS(READ)
```

Sun MSF にも、リソースドメインと呼ばれる、RACF の一般的なリソースプロファイルと同等の構造があります。リソースドメインは、メンバーとしてリソースを持っているという点で RACF のリソースグループクラスに似ています。また、リソースドメインは、それらのリソースのアクセスリストを保持しています。たとえば、次の一連のコマンドの場合、createResourceDomain コマンドでリソースドメインが作成され、createResource コマンドと addResourceToDomain コマンドでトランザクションリソースと同一の 3 つの CICS システムコマンドが作成されて割り当てられ、addRolePermission コマンドで 2 つの役割に対して同じアクセスリストが定義されます。

```
crd,resourceDomain_name,Domain for CICS system commands
crs,KIX_ATTACH_TRANS,CEMT,System transaction CEMT definition
ard,KIX_ATTACH_TRANS,CEMT,resourceDomain_name
crs,KIX_ATTACH_TRANS,CEDA,System transaction CEDA definition
ard,KIX_ATTACH_TRANS,CEDA,resourceDomain_name
crs,KIX_ATTACH_TRANS,CEDB,System transaction CEDB definition
ard,KIX_ATTACH_TRANS,CEDB,resourceDomain_name
arp,group1,resourceDomain_name,READ
arp,group2,resourceDomain_name,READ
```

RACF と同じく、リソースドメインは、あらかじめ定義された 1 つのリソースタイプだけに制限されているわけではありません。たとえば、同じリソースドメインを使用して、CICS プログラムおよび CICS 端末に対するアクセス権の共通のセットを管理できます。

RACF と Sun MSF には、リソースとアクセス権を管理する方法に、異なる点がいくつかあります。まず、Sun MSF にはメンバーリソースクラスという概念がありません。このため、アクセスリストを使用して RACF のメンバーリソースが定義されている場合、そのアクセス権を持つ一意の Sun MSF リソースドメインのメンバーとして、そのメンバーリソースがマッピングされます。次に、Sun MSF は、リソースの UACC (ユニバーサルアクセス権) 設定に相当するものをサポートしていません。UACC とは異なり、リソースのデフォルトのアクセス権を定義することはできません。Sun MSF では、inclusive permissions (包含的なアクセス権) モデルを使用してアクセスが実行されるため、ユーザーは、アクセス権が明示的に付与されたリソースにのみアクセスすることが可能です。これは、RACF の UACC(NONE) に相当します。

Sun MSF には、RACF リソースの管理コマンドとその機能に相当するもの以外に、いくつかの管理コマンドとその機能が存在します。次の例は、その一部を示しています。

例: ACCESS オペランドではなく、DELETE オペランドとともに RACF の PERMIT コマンドを使用して、ユーザーまたはグループのエントリをアクセスリストから削除します。

```
PERMIT  profile-name  CLASS(class-name)
        I(user | group)  DELETE
```

Sun MSF では、removePrincipalPermissions コマンドまたは removeRolePermissions コマンドを使用して、主体または役割のエントリをリソースドメインのアクセスリストから削除します。

```
rpp,user,profile-name
rrp,group,profile-name
```

例: RACF では、RDELETE コマンドを使用してプロファイルを削除します。

```
RDELETE class-name   profile-name
```

Sun MSF では、deleteResourceDomain コマンドを使用してリソースドメインを削除します。

```
drd,profile-name
```

例: 特定の RACF クラスのプロファイル名を一覧表示するには、SEARCH コマンドを使用します。次のコマンドでは、TCICSTRN クラスのプロファイルが一覧表示されます。

```
SEARCH  CLASS(TCICSTRN)
```

Sun MSF では、特定のリソースタイプのすべてのリソースを一覧表示することができます。使用するのは、listResources コマンドです。

```
lres,KIX_ATTACH_TRANS,*
```

Sun MSF では、list コマンドでの別のサーチキー指定もサポートされています。たとえば、次のコマンドを使用して、すべての CICS システムコマンド (文字 C で始まるトランザクション) を検索できます。

```
lres,KIX_ATTACH_TRANS,C*
```

Sun MSF では、リソースドメインの詳細の一覧表示もサポートされています。これは、リソースグループクラスを指定する、RACF の SEARCH コマンドと似ています。たとえば、listResourceDomain コマンドでは、リソースドメインのメンバーリソースと許可されているアクセス権 (アクセスリスト) がすべて一覧表示されます。

```
lrd,group2
```

例: RACF は、RACF クラスを有効にする管理コマンドを通じて、そのクラスのプロファイルで保護されているすべてのリソースの保護を開始するように指示されます。

```
SETROPTS CLASSACT(class-name)
```

Sun MSF では、リソースの保護を有効にするために別の方法が使用されます。リソースを定義し、リソースドメインのメンバーとして追加して、そのリソースドメインに対する役割および主体のアクセス権を付与したあと、`commit` コマンドを使用して、Sun MSF のリポジトリへの変更をコミットし、保護を有効にします。

```
commit
```

Sun MTP では、管理コマンドを使用して、それらのアクセスルールをインポートします。

```
CEMT PERFORM SECURITY REBUILD
```

注 – RACF の `SETROPTS` コマンドにはさまざまな機能がありますが、そのほとんどが Sun MSF の機能にマッピングされていないか、別の方法で Sun MSF に用意されています。いくつかの機能は、Sun MSF に用意されていません。

用語集

D

DIT 「ディレクトリ情報ツリー」を参照してください。

DNS 「ドメイン名システム」を参照してください。

I

inclusive permissions (名詞) セキュリティーモデルの一種。すべてのリソースをセキュリティーリポジトリで定義してから、アクセスが必要なユーザーや役割にアクセス権を与える必要があります。リソースがセキュリティーリポジトリで定義されていないと、ユーザーや役割がそのリソースにアクセスできません。

IP 「インターネットプロトコル」を参照してください。

IP アドレス (名詞) イントラネットやインターネットのコンピュータの実際の場所を指定する 4 組の番号で、192.168.255.255 のようにピリオドで区切られています。TCP/IP を使用しているホストに割り当てられる 32 ビットのアドレスで、8 ビットずつ 1 つの構成要素を表しています。

J

J.C.E. Java Cryptography Extension の略語。

J.N.D.I. 「Java Naming and Directory Interface」を参照してください。

JAAS 「Java Authentication and Authorization Service」を参照してください。

JAR ファイル 「Java Archive ファイル」を参照してください。

Java Archive (JAR) ファイル (名詞) 多数の Java クラスファイルを 1 つにまとめるために使用するファイル。JAR ファイルには拡張子 `.jar` が付いています。

Java Authentication and Authorization Service (JAAS) (名詞) ユーザーの認証とアクセス制御を実行するサービスを有効にする Java パッケージ一式。標準的な Pluggable Authentication Module (PAM) フレームワークの Java バージョンを実装し、互換性を保ちながら Java 2 Platform のアクセス制御アーキテクチャーを拡張して、ユーザー別の承認をサポートします。

Java Cryptography Extension (名詞) 暗号化、鍵の生成と鍵の一致、および Message Authentication Code (MAC) アルゴリズムの枠組みと実装を提供するパッケージセット。対称、非対称、ブロック、ストリームなどの暗号をサポートしています。このソフトウェアはセキュアストリームとシールドオブジェクトもサポートしています。

Java DataBase Connectivity (JDBC) ソフトウェア (名詞) クラスとインタフェースの標準セット。これを使用して開発者はデータ認識コンポーネントを作成します。JDBC の API は、プラットフォームやベンダーに依存せずにデータソースに接続してそれを操作する方法を実装しています。

Java Development Kit (JDK) (名詞) Java アプレットやアプリケーションプログラムの作成に使用するソフトウェアツール。

Java Naming and Directory Interface (JNDI) (名詞) Java プラットフォームの標準拡張機能。Java 技術を基盤とするアプリケーションに、複数のネーミングサービスやディレクトリサービスへの統一インタフェースを提供します。

Java System Directory Server (名詞) LDAP の Java Enterprise System バージョン。アプリケーションサーバーのインスタンスはすべて、ディレクトリサーバーを使用して、ユーザーとグループに関する情報などサーバーの共有情報を保管しています。

Java 実行環境 (JRE) (名詞) Java 仮想マシン、Java コアクラス、その他の関連ファイルで構成された JDK ソフトウェアのサブセット。Java プログラミング言語で記述されたアプリケーションのランタイムサポートを提供します。

JDBC 「Java DataBase Connectivity ソフトウェア」を参照してください。

JDK 「Java Development Kit」を参照してください。

JRE 「Java 実行環境」を参照してください。

L

LDAP 「Lightweight Directory Access Protocol」を参照してください。

LDAP URL (名詞) DNS を使用してディレクトリサーバーを検索し、LDAP からの問い合わせを完了する手段を提供する URL。`ldap://ldap.example.com` が LDAP URL の一例です。

Lightweight Directory Access Protocol (LDAP) (名詞) TCP/IP 上および複数のプラットフォーム間で実行するように設計されたディレクトリサービスプロトコル。X.500 Directory Access Protocol (DAP) を簡略化したもの。Java System の全サーバーのユーザープロファイル、配布リスト、構成データなどの保管、検索、配布を一元管理できます。Directory Server は LDAP プロトコルを使用しています。

P

PAM 「Pluggable Authentication Module」を参照してください。

Pluggable Authentication Module (PAM) (名詞) サービスを再コンパイルせずに複数の認証機構を可能にするフレームワーク。

R

RACF 「Resource Access Control Facility」を参照してください。

RBAC 「役割によるアクセス制御」を参照してください。

RDBMS (名詞) Relational Database Management System の略語。

Resource Access Control Facility (RACF)
: (名詞) ログインユーザーの確認、保護リソースへのアクセス許可、システム不正侵入の試みのログ検出、保護リソースへのアクセスのログ検出などによって、アクセス制御を提供するプログラム。IBM よりライセンス許諾されています。[1]

U

umask
: (名詞) 3 つの 8 進数のセットで、それぞれの数値がファイルモードに対応します。ファイルのアクセス権を決定します。

Uniform Resource Locator (URL)
: (名詞) サーバーとクライアントがドキュメントを要求するときに使用するアドレス指定の方法。「ロケーション」とも呼ばれます。URL の形式は *protocol*`://`*machine.port*`/`*document* です。
`http://www.example.com/index.html` が URL の一例です。

URL
: 「Uniform Resource Locator」を参照してください。

あ

暗号化
: (名詞) 情報を判読不能にして不正使用から保護するプロセス。情報の暗号化に、「鍵」と呼ばれるコードを使用する暗号化方式もあります。

い

入口セキュリティー
: (名詞) 特定の Sun MTP 領域のユーザーと特定の端末名が領域にアクセスするのを許可または拒否するセキュリティー機能。

インスタンスディレクトリ
: (名詞) Sun MSF の特定のインスタンスを定義したファイルを格納しているディレクトリ。

インターネットプロトコル (IP)
: (名詞) 世界中のネットワークを接続するための TCP/IP 群のプロトコル。米国国防省によって開発され、インターネットで使用されています。このプロトコル群で最も重要なものが IP プロトコルです。

1. "IBM Terminology," [`http://www-306.ibm.com/ibm/terminology/qr.htm`] 2005 年 2 月 16 日時点でアクセス

か

鍵ファイル (名詞) サーバーの証明書に使用する鍵ペアが含まれたファイル。鍵データベースとも呼ばれます。

け

結果キャッシュ (名詞) アクセス試行の結果が保存されている Sun MTP のキャッシュメモリ領域。

し

主体 (名詞) セキュリティーシステムに定義されている個々のユーザー。

承認 (名詞) 主体がサービスを使用できるかどうか、主体がアクセスできるリソース、各リソースに許可されるアクセス権の種類などを決定するプロセス。役割によるアクセス制御 (RBAC) では、セキュリティーポリシーで禁じられている種類の操作を実行するために、役割やユーザーに割り当てられるアクセス権を指します。

す

スーパー管理者 (名詞) セキュリティーリポジトリとして使用する RDBMS または LDAP ディレクトリの全権限を持っているユーザー。セキュリティーリポジトリの作成と破棄のほか、他の 2 つのユーザーカテゴリ (Sun MSF セキュリティー管理者と Sun MSF ユーザー) へのアクセス権の付与もこれに含まれます。MakeAnAdministrator アプリケーションを起動する `msfinitr` コマンドを実行できるのは、スーパー管理者だけです。

せ

セキュリティー管理者 (名詞) SecAdmin アプリケーションを使用してセキュリティーリポジトリの保守に従事するユーザー。

セキュリティー出口 (名詞) Sun MTP 領域で外部セキュリティーが有効になっている場合に、特定の時点で呼び出されるルーチン。これらのエントリポイントはセキュリティー要求と Sun MTP エグゼクティブを検査してから、セキュリティー検証に成功した操作を続行したり、セキュリティー検証に失敗した操作を終了したり、適切な処理を実行します。

セキュリティーポリシー (名詞) 主体や役割の権限を支配する一連の規則。

セキュリティーリポジトリ (名詞) このリポジトリは、Sun 以外のリレーショナルデータベース管理システム (RDBMS) または LDAP ディレクトリで、Sun MSF が管理する主体、役割、リソースドメイン、リソースなどが含まれています。また、ドメインとリソースにアクセスするためのアクセス権やルールも含みます。

て

ディレクトリ情報ツリー (DIT) (名詞) ディレクトリに格納されている情報を論理的に表したもの。DIT は多くのファイルシステムで使用されているツリーモデルと同様に、ツリーのルートポイントが階層の最上位に表示されます。

と

特権 (名詞) ユーザーまたはユーザーグループに与えられるリソースのアクセス権。

ドメイン名システム (DNS) (名詞) ネットワーク上のコンピュータが IP アドレス (00.120.000.168 など) をホスト名 (www.example.com など) に関連付けるために使用するシステム。クライアントは通常 DNS を使用して、接続するサーバーの IP アドレスを見つけます。DNS のデータはローカルのテーブルで、UNIX システムの NIS や `/etc/hosts` ファイルなどから補強されることが多くあります。「IP アドレス」も参照してください。

に

認証 (名詞) 主体の識別情報を識別するプロセス。

ふ

プロパティー (名詞) アプリケーションコンポーネントの動作を定義する 1 つの属性。`MSFconfig.properties` ファイルでは、プロパティーは名前と値のペアを含んだ要素です。

や

役割 (名詞) テストグループなど、共通の責務を持つユーザーグループ。

役割によるアクセス制御 (RBAC) (名詞) リソースへのアクセス許可を役割に関連付けて、ユーザーを適切な役割に割り当てるセキュリティーモデル。

ゆ

ユーザー (名詞) 特定のユーザーに帰属する主体。

り

リソース (名詞) ファイルやプログラムなど、特定タイプの名前付きコンポーネント。ユーザーがトランザクションやその他の作業を実行するときにアクセスします。

リソースドメイン (名詞) 共通のアクセス権要件を持つリソースグループ。

ろ

ログのローテーション　(名詞) 現在のログファイルとなる新しいログファイルの作成。以降、記録されたイベントはすべてこの新しいファイルに書き込まれます。以前のログファイルには書き込まれなくなりますが、ファイルはそのままログディレクトリに残ります。

索引

U

あ

い

え

お

ろ