Oracle® Solaris 11.2 でのユーザーとプロセスのセキュリティー保護

Part No: E53954
2014 年 7 月

ORACLE

目次

例目次

このドキュメントの使用法

- **概要** – ユーザーへの追加権利の割り当て、役割の作成と使用、および Oracle Solaris システム上の特定のリソースおよびプログラムへの権利の割り当ての方法について説明します。
- **対象読者** – セキュリティー管理者。
- **前提知識** – サイトのセキュリティー要件。

製品ドキュメントライブラリ

この製品に関する最新情報および既知の問題については、ドキュメントライブラリ (http://www.oracle.com/pls/topic/lookup?ctx=E56342) に記載されています。

Oracle サポートへのアクセス

Oracle ユーザーは My Oracle Support から電子サポートにアクセスできます。詳細は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info を参照してください。聴覚に障害をお持ちの場合は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs を参照してください。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

♦ ♦ ♦ 第 1 章

1 権利を使用したユーザーとプロセスの制御について

Oracle Solaris には、ユーザー、役割、プロセス、および一部のリソースに割り当てることができる権利があります。これらの権利は、スーパーユーザーモデルの代替となるよりセキュアな管理手法です。

この章では、ユーザー権利とプロセス権利の管理を支援する要素について説明し、ユーザーの権利拡大、ユーザーの権利の制限、コマンドへの特権の追加、必要な特権のみへのアプリケーションの制限の方法について説明します。

Oracle Solaris 11.2 での権利の新機能

このセクションでは、ユーザー権限における重要な新機能である権限ベースのアクセス制御 (RBAC) と、プロセス権限における新機能でる特権について、既存のお客様を対象に説明します。

- 管理者が*認証*権利プロファイルとして割り当てる権利プロファイルにより、ユーザーに対し特権コマンドの実行前にパスワードを入力することが要求されます。ユーザーがパスワードを入力しないと、コマンドは特権なしで実行されます。このパスワードは、構成可能な一定期間において有効です。例3-11「ユーザーに対し DHCP 管理の前にパスワード入力を求める」を参照してください。

  システムにログインしている任意のユーザーに認証権利プロファイルを割り当てるには、`policy.conf` ファイルの `AUTH_PROFS_GRANTED` キーワードの値としてそのプロファイルを追加します。
- 時間と時間帯に基づいてホストへのユーザーとグループのアクセスを制限するには、`access_times` および `access_tz` 権利を割り当てます。例については、`user_attr`(4) のマニュアルページを参照してください。

- Oracle Solaris では、armor パッケージに Authorization Roles Managed on RBAC (ARMOR) の標準役割セットが含まれています。詳細は、14 ページの「スーパーユーザーモデルの代替としてのユーザー権利およびプロセス権利」および 例3-1「ARMOR の役割の使用」 を参照してください。
- ユーザーと役割の権利の管理には、ユーザーマネージャー GUI を使用できます。詳細は、『Oracle Solaris 11.2 のユーザーアカウントとユーザー環境の管理 』の第 3 章「ユーザーマネージャー GUI を使用したユーザーアカウントの管理」を参照してください。

ユーザー権管理

ユーザー権管理は、通常はroot 役割に限定されるタスクへのユーザーアクセスを制御するためのセキュリティー機能です。セキュリティー属性、つまり*権利*をプロセスとユーザーに適用することで、サイトでは管理者間でスーパーユーザー特権を分けることができます。プロセス権管理は、「特権」を介して実装されます。ユーザー権管理は、ユーザーと役割に割り当てられる権利をまとめた*権利プロファイル*によって実装されます。キオスクやゲストユーザーなどのユーザー権利も制限できます。

- カーネルプロセスでの権利の説明については、24 ページの「プロセス権管理」を参照してください。
- 権利管理の手順については、第3章「Oracle Solaris での権利の割り当て」を参照してください。
- 参照情報については、第8章「Oracle Solaris 権利リファレンス」を参照してください。

スーパーユーザーモデルの代替としてのユーザー権利およびプロセス権利

従来の UNIX システムでは、root ユーザー (スーパーユーザーとも呼ばれる) が全権を有します。多数の setuid プログラムと同様に、root として実行されるプログラムにも全権があります。root ユーザーは全ファイルの読み取り権とアクセス権、全プログラムの実行権を持ち、任意のプロセスに終了シグナルを送ることができます。実際、スーパーユーザーになるユーザーは、使用するサイトのファイアウォールの変更、監査トレールの変更、機密レコードの読み取り、ネットワーク全体の停止などを行えます。setuid root プログラムがハイジャック (強奪) されると、システム上で何が起きても不思議はありません。

ユーザー、リソース、およびプロセスへの権利の割り当ては、全権を持つスーパーユーザーモデルに代わるセキュアな代替機能です。権利を使用することで、セキュリティーポリシーをきめ細かく適用できます。権利では、*最小特権*というセキュリティー原則が使用されます。最小特権は、ジョブを行う上で必要な特権だけをユーザーに与えることを意味します。通常のユーザーには、アプリケーションの使用、実行中のジョブのステータスチェック、ファイルの印刷、新しいファイルの作成などを行うための十分な特権が与えられます。通常のユーザー権利以外の権利は、権利プロファイルにグループ化されます。スーパーユーザー権利の一部が必要なジョブを行うユーザーには、権利プロファイルを割り当てることができます。

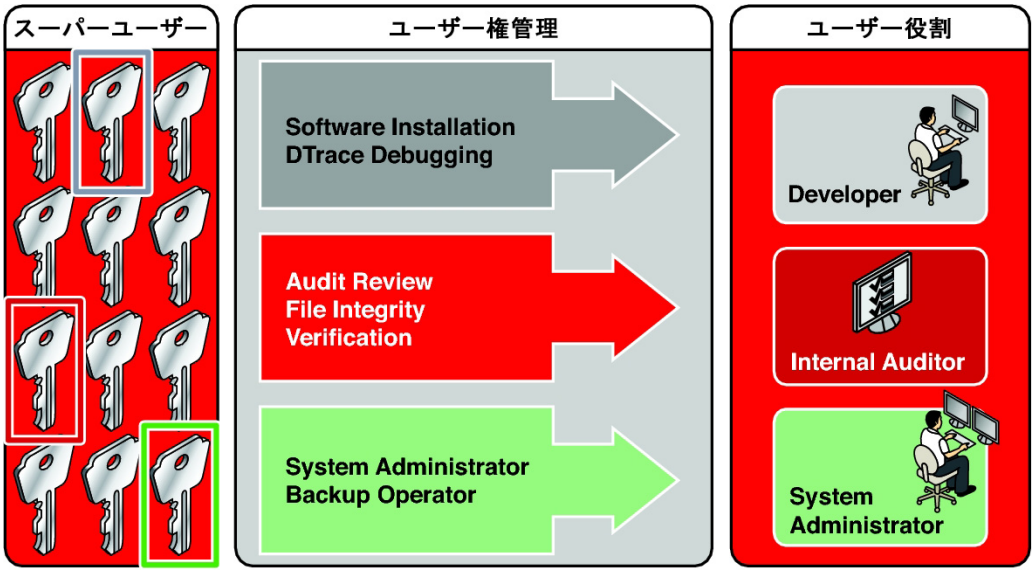
プロファイルにグループ化された権利は、ユーザーに直接割り当てることができます。間接的に割り当てるには、*役割*と呼ばれる特殊アカウントを作成します。これにより、ユーザーは一部の管理特権を必要とするジョブを実行するときに役割を引き受けることができます。Oracle Solaris には事前定義の権利プロファイルが多数用意されています。管理者は役割を作成し、プロファイルを割り当てます。

ARMOR パッケージには、一連の標準化された役割が含まれています。このパッケージを自動インストールし、役割をユーザーに割り当てることで、ブート時に責務分離を実施するシステムを作成できます。詳細は、Authorization Rules Managed On RBAC (ARMOR)、44 ページの「選択した権利モデルへの準拠」、および 例3-1「ARMOR の役割の使用」を参照してください。

権利プロファイルは、広範な管理権利を提供できます。たとえば System Administrator 権利プロファイルにより、アカウントはプリンタ管理や cron ジョブ管理などのセキュリティーに関連しないタスクを実行できます。権限を限定して権利プロファイルを定義することもできます。たとえば、Cron Management 権利プロファイルは `at` ジョブと `cron` ジョブを管理します。役割を作成すると、その役割に広範な管理権利または限定された権利を割り当てることができます。

次の図に、Oracle Solaris が役割を作成して権利を信頼できるユーザーに割り振る方法を示します。スーパーユーザーは、信頼できるユーザーに権利プロファイルを直接割り当てることで、権利を割り振ることもできます。

図 1-1 権利の割り振り



図に示す権利モデルでは、スーパーユーザーが 3 つの役割を作成します。役割は、権利プロファイルに基づいて作成されます。続いてスーパーユーザーは、役割のタスクに適したユーザーにその役割を割り当てます。ユーザーは、各自のユーザー名でログインします。ユーザーはログイン後に、管理コマンドとグラフィカルユーザーインタフェース (GUI) ツールを実行できる役割を引き受けます。

役割は柔軟に設定できるため、さまざまなセキュリティーポリシーに対応できます。Oracle Solaris には標準装備された役割がほとんどありませんが、役割は簡単に構成できます。例3-1「ARMOR の役割の使用」に、ARMOR 標準ベースの役割の使用法を示します。ARMOR の役割に追加して使用する役割、または ARMOR の役割の代わりに使用する役割として、Oracle Solaris に用意されている権利プロファイルに基づくユーザー独自の役割を作成できます。

- **root** – `root` ユーザーと同等の強力な役割。ただし、ほかのすべての役割と同様に、`root` 役割はログインできません。通常のユーザーは、ログインしてから、割り当てられた `root` 役割を引き受ける必要があります。デフォルトでは、この役割は構成され初期ユーザーに割り当てられます。
- **System Administrator** – セキュリティーに関係のない管理作業を行う役割で、権利が限定されています。この役割ではファイルシステム、メール、ソフトウェアのインストールなどを管理できます。ただし、パスワードの設定は行えません。

- **Operator** – バックアップやプリンタ管理などが行える、補佐的な管理者向けの役割。

注記 - Media Backup 権利プロファイルは、ルートファイルシステム全体へのアクセスを提供します。したがって、Media Backup 権利プロファイルと Operator 権利プロファイルは補佐的な管理者向けに設計されていますが、この管理者が信頼できるユーザーであることを確認する必要があります。

---

1 つ以上のセキュリティー役割を構成することもできます。セキュリティーは、Information Security、User Security、および Zone Security の 3 つの権利プロファイルと、それらの補助プロファイルによって処理されます。ネットワークセキュリティーは、Information Security 権利プロファイル内の補助プロファイルです。

役割は実装する必要はありません。役割は、組織のセキュリティー要件に応じて設定する機能です。1 つの方法として、セキュリティー、ネットワーク、ファイアウォール管理などの領域における専用の管理者のための役割を設定します。別の方法として、強力な管理者役割を 1 つと上級ユーザー役割を作成することもできます。この上級ユーザー役割は、自分のシステムの各部を修正することを認められたユーザーに割り当てます。また、権利プロファイルをユーザーに直接割り当てて、役割を作成しないでおくこともできます。

スーパーユーザーモデルと権利モデルは共存できます。次の表では、権利モデルで設定できる権利 (スーパーユーザーから制限された通常のユーザーまで) を順に挙げます。両モデルで監視できる管理アクションを示しています。プロセス権利 (*特権*) の影響のサマリーについては、表 1-2「特権を持つシステムと特権を持たないシステムとの明白な違い」を参照してください。

表 1-1 スーパーユーザーモデルと特権モデルの対比

システムにおけるユーザー権限	スーパーユーザーモデル	権利モデル
すべてのスーパーユーザー特権を持つスーパーユーザーになることができる	可能	可能
すべてのユーザー権利を持つユーザーとしてログインできる	可能	可能
権利が限定されたスーパーユーザーになることができる	不可能	可能
ユーザーとしてログインし、散発的にスーパーユーザー特権を持つことができる	可能 (`setuid root` プログラムのみを使用)	可能 (`setuid root` プログラムと権利を使用)
すべてのスーパーユーザー特権ではなく、管理権利だけを持つユーザーとしてログインできる	不可能	可能 (権利プロファイル、役割、および直接割り当てられた特権と承認を使用)

システムにおけるユーザー権限	スーパーユーザーモデル	権利モデル
通常のユーザーよりも少ない権利を持つユーザーとしてログインできる	不可能	可能 (権利を削除)
スーパーユーザーの処理を監視する	可能 (su コマンドを監査することによって)	可能 (pfexec() への呼び出しを監査することによって) また、root 役割を引き受けたユーザーの名前も監査トレールに含まれる

ユーザー権利およびプロセス権利の基本情報

*特権のない*または*権利のない*という用語は Oracle Solaris には適用されません。通常のユーザープロセスを含む Oracle Solaris のすべてのプロセスには、少なくとも何らかの特権またはユーザー権利 (承認など) が設定されています。Oracle Solaris がすべての UNIX プロセスに付与する特権の基本セットについては、24 ページの「プロセス権管理」を参照してください。

Oracle Solaris では次の要素によってユーザー権利が適用されます。これらの権限は、許容セキュリティーポリシーまたは制限セキュリティーポリシーを適用するように構成できます。

- **承認** – ユーザーまたは役割が、追加の権利を必要とするクラスのアクションを実行できるようにする許可です。たとえばデフォルトのセキュリティーポリシーでは、コンソールユーザーに対し solaris.device.cdrw 承認が付与されます。この承認によってユーザーは CD-ROM デバイスの読み取りと書き込みが行えます。承認のリストについては、auths list コマンドを使用してください。承認はカーネルではなく、ユーザーアプリケーションレベルで適用されます。22 ページの「ユーザー承認に関する詳細」を参照してください。
- **特権** – コマンド、ユーザー、役割、または特定のリソース (ポートや SMF メソッドなど) に付与できる権利です。特権はカーネルで実装されます。たとえば、proc_exec 特権によってプロセスは execve() を呼び出すことができます。通常のユーザーには基本特権が与えられます。自分の基本特権を確認するには、ppriv -vl basic コマンドを実行します。詳細は、24 ページの「プロセス権管理」を参照してください。
- **セキュリティー属性** – プロセスが操作を実行できるようにする属性 (権利の実装)。標準的な UNIX 環境では、セキュリティー属性によって、通常のユーザーには禁止されている操作をプロセスで実行できるようになります。たとえば、setuid プログラムと setgid プログラムはセキュリティー属性を持ちます。権利モデルでは、setuid および setgid プログラムに加えて、承認と特権がセキュリティー属性です。これらの属性、つまり権利は、ユーザーに割り当てることができます。たとえば、solaris.device.allocate 承認が与えられたユーザーは、デ

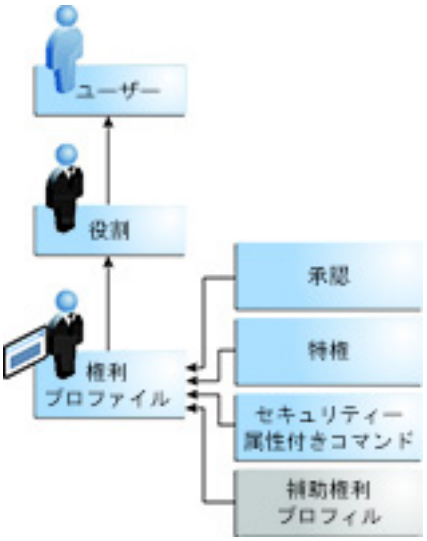
バイスを独占的に使用するためにそのデバイスの割り当てを行うことができます。特権をプロセスに割り当てることができます。たとえば、`file_flag_set` 特権を持つプロセスは、変更不可能な、リンク解除できない、または追加のみのファイル属性を設定できます。

セキュリティー属性によって権利を制限することもできます。たとえば `access_times` および `access_tz` セキュリティー属性は、特定のセキュリティー関連操作が許可される日時と、オプションで時間帯を設定します。ユーザーを制限するには、直接制限するか、またはこれらのキーワードが含まれている認証権利プロファイルにユーザーを割り当てます。詳細は、`user_attr`(4) のマニュアルページを参照してください。

- **特権付きアプリケーション** – 権利を確認してシステム制御をオーバーライドできるアプリケーションまたはコマンド。詳細は、39 ページの「権利を確認するアプリケーション」および『Oracle Solaris 11 セキュリティー開発者ガイド 』を参照してください。
- **権利プロファイル** – 役割またはユーザーに割り当てることができる権利の集合です。権利プロファイルには、承認、直接割り当てられた特権、セキュリティー属性を持つコマンド、およびほかの権利プロファイルを含めることができます。別のプロファイル内に存在するプロファイルは、*補助権利プロファイル*と呼ばれます。権利プロファイルは、権利をグループ化する手段として便利です。ユーザーに直接割り当てるか、または*役割*と呼ばれる特殊アカウントに割り当てることができます。権利プロファイルのコマンドを使用できるのは、プロセスで権利が認識される場合に限ります。また、パスワードの入力が必要な場合があります。あるいは、デフォルトでパスワード認証が提供されることがあります。23 ページの「権利プロファイルの詳細」を参照してください。
- **役割** – *特権付きアプリケーション*を実行するための特殊な識別情報です。この特殊な識別情報を取得できるのは、あらかじめ割り当てられたユーザーだけです。役割により実行されるシステムでは、初期構成後にはスーパーユーザーが不要となることがあります。23 ページの「役割の詳細」を参照してください。

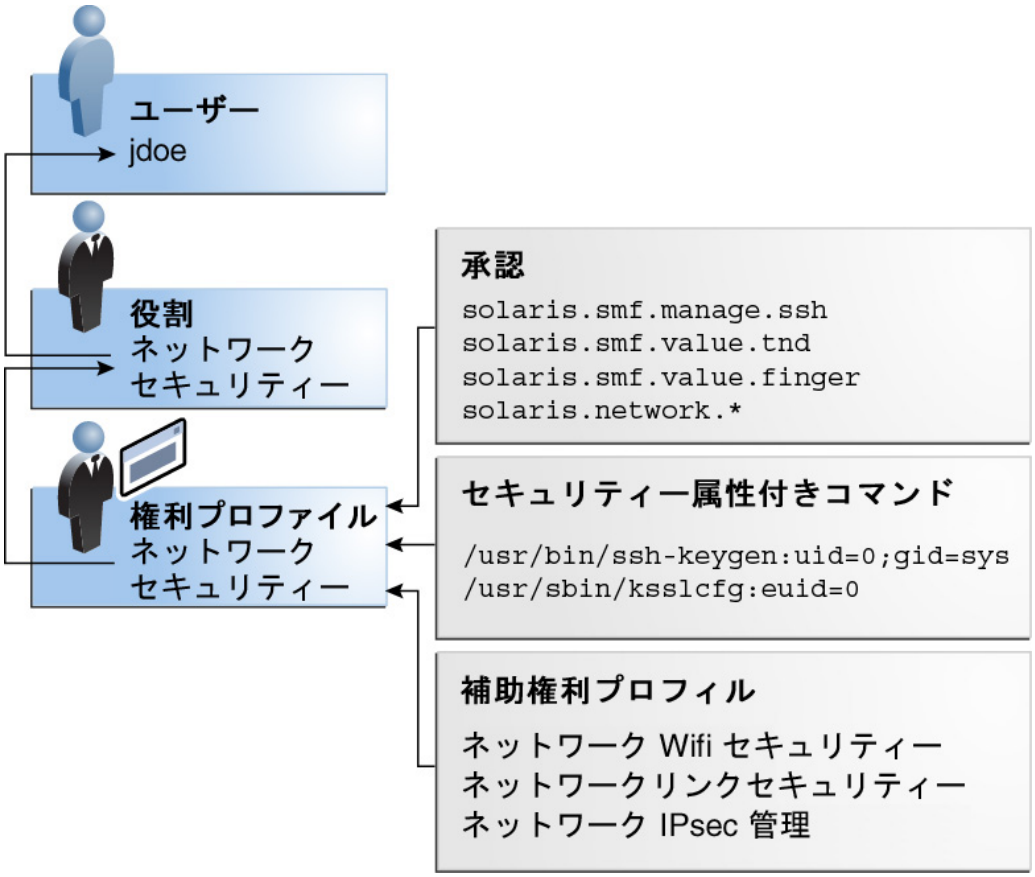
次の図に、ユーザー権利とプロセス権利がどのように連携するかを示します。

図 1-2 ユーザー権利とプロセス権利の連携



次の図は、Network Security 役割と Network Security 権利プロファイルを使用して、割り当てられた権利がどのように機能するかを示します。

図 1-3　ユーザー権利とプロセス権利の割り当ての例



Network Security 役割は、IPsec、wifi、およびネットワークリンクの管理に使用します。この役割は、ユーザー `jdoe` に割り当てられています。`jdoe` は、この役割に切り替えてから役割のパスワードを指定することによって、この役割になることができます。管理者は、この役割で役割のパスワードではなくユーザーパスワードでの認証を可能にするようにできます。

この図では、Network Security 権利プロファイルが Network Security 役割に割り当てられています。Network Security 権利プロファイルには、Network Wifi Security、Network Link Security、および Network IPsec Management という、順番に評価される補助プロファイルが含まれています。これらの補助プロファイルには、役割の主要なタスクを実行する権利が含まれています。

Network Security 権利プロファイルには、直接割り当てられた 3 つの承認と、セキュリティー属性を持つ 2 つのコマンドがありますが、直接割り当てられた特権はありません。補助権利プロファイルには、直接割り当てられた承認があり、それらの 2 つにはセキュリティー属性を持つコマンドがあります。

jdoe が Network Security 役割を引き受けると、シェルがプロファイルシェルに変化します。プロファイルシェルプロセスは権利の使用を評価できるため、jdoe はネットワークセキュリティーを管理できます。

ユーザー権利の詳細

このセクションでは、ユーザーレベルでの権利の実装と使用についてさらに詳しく説明します。

ユーザー承認に関する詳細

*承認*とは、役割、プログラム、ゾーン、またはユーザーに付与できる権利です。承認は、ユーザーアプリケーションレベルでポリシーを適用します。特権と同様に、承認の割り当てを誤ると、本来予定していたよりも多くの権利が付与される結果となる可能性があります。詳細は、35 ページの「特権エスカレーションとユーザー権利」を参照してください。

承認と特権の違いは、セキュリティーポリシーが適用されるレベルにあります。プロセスに適切な特権がないと、特権化された処理の実行がカーネルによって防止される可能性があります。適切な承認が与えられていないユーザーは、特権付きアプリケーションを使用できなかったり、特権付きアプリケーションに含まれるセキュリティーの厳しい処理を実行できなかったりする可能性があります。特権の詳しい説明については、24 ページの「プロセス権管理」を参照してください。

権利に準拠したアプリケーションは、ユーザーの承認を確認してから、アプリケーションまたはアプリケーション内の特定の操作に対するアクセス権を許可します。この確認は、従来の UNIX アプリケーションが行なっていた UID=0 の確認に代わるものです。

承認についての詳細は、次のセクションを参照してください。

- 121 ページの「承認のリファレンス」
- 125 ページの「auth_attr データベース」
- 128 ページの「承認を必要とする特別なコマンド」

権利プロファイルの詳細

*権利プロファイル*は、管理権利が必要なタスクを実行するために役割またはユーザーに割り当てることができる権利の集合です。権利プロファイルには、承認、特権、セキュリティー属性が割り当てられたコマンド、およびほかの権利プロファイルを含めることができます。権利プロファイルにはまた、特権の初期継承可能セットを削減または拡張したり、制限セットを削減したりするためのエントリも含まれています。

*認証権利プロファイル*は、ユーザーに対しパスワードの入力、つまり*再認証*を求める権利プロファイルです。管理者は、再認証なしで使用できるプロファイルを決定します。再認証が不要なプロファイルの例として、Basic Solaris User 権利プロファイルがあります。サイトのセキュリティー要件に基づき、セキュリティーの厳しいタスクのための権利プロファイルでは、再認証が必要になることがあります。

権利プロファイルの参照情報については、次のセクションを参照してください。

- 119 ページの「権利プロファイルのリファレンス」
- 125 ページの「prof_attr データベース」
- 126 ページの「exec_attr データベース」

役割の詳細

「役割」は、特権付きアプリケーションを実行できる特別な種類のユーザーアカウントです。役割は、ユーザーアカウントと同じ方法で作成され、ホームディレクトリ、グループ割り当て、パスワードなどを持ちます。権利プロファイルと承認により、役割に管理権利が提供されます。役割は、ほかの役割やその役割を引き受けるユーザーから権利を継承することはできません。役割によりスーパーユーザー特権が割り振られるため、セキュリティーが強化された管理を実施できます。

各役割は、複数のユーザーに割り当てることができます。同じ役割になるすべてのユーザーは、同じ役割のホームディレクトリを持ち、同じ環境で動作し、同じファイルへのアクセス権を持ちます。ユーザーは、役割を引き受けるにはコマンド行で su コマンドを実行し、役割名と役割のパスワードを入力します。管理者は、ユーザーが、そのユーザーのパスワードを指定することによって認証できるようにシステムを構成できます。例3-16「役割パスワードでのユーザー独自のパスワード使用の有効化」を参照してください。

役割は直接ログインすることはできません。ユーザーがまずログインし、続いて役割を引き受けます。役割を引き受けたあとで別の役割を引き受けるには、まず現在の役割を終了する必要があります。

また、権利プロファイルはユーザーの環境に権利を追加しますが、役割はユーザーに対し、その役割を引き受けることができるほかのユーザーと共有するクリーンな実行環境を提供します。ユーザーが役割に切り替わっても、ユーザーの承認または権利プロファイルはすべて役割には適用されません。

passwd、shadow、および user_attr データベースに、静的な役割情報が格納されます。ユーザーは役割のアクションを監査できるので、この監査を実行すべきです。

役割の設定についての詳細は、次のセクションを参照してください。

- 44 ページの「選択した権利モデルへの準拠」
- 47 ページの「ユーザーへの権利の割り当て」

Oracle Solaris では root は役割であるため、匿名の root ログインが回避されます。プロファイルシェルコマンド pfexec が監査されると、監査トレールにはログインユーザーの実 UID、ユーザーが引き受けている役割、および実行された特権付き操作が含まれています。特権付き操作についてシステムを監査するには、88 ページの「管理アクションの監査」を参照してください。

プロセス権管理

Oracle Solaris でのプロセス権管理は、*特権*により実装されます。特権により、コマンド、ユーザー、役割、および特定のシステムリソースのレベルにプロセスを制限できます。特権は、システムに対するすべてのスーパーユーザー権限を 1 人のユーザーまたは 1 つのプロセスだけが持っている場合に伴うセキュリティーリスクを軽減します。プロセス権利とユーザー権利は、従来のスーパーユーザーモデルの代替となる強力なモデルを提供します。

従来、特権は権利を追加するために使用されました。ただし、権利を制限する場合、たとえば setuid root プログラムを特権認識プログラムに変更する場合などにも特権を使用できます。また*拡張特権ポリシー*により、管理者は指定の特権のみをファイルオブジェクト、ユーザー ID、またはポートで使用できるように許可できます。このきめ細かな特権割り当てでは、このようなリソースに対し基本特権以外のそのほかのすべての特権が拒否されます。

- 拡張特権ポリシーと制限特権については、35 ページの「拡張特権ポリシーを使用した特権使用の制限」を参照してください。
- ユーザー権利については、14 ページの「ユーザー権管理」を参照してください。
- 特権を管理する方法については、第3章「Oracle Solaris での権利の割り当て」を参照してください。

- 特権に関する参照情報については、129 ページの「特権のリファレンス」を参照してください。

カーネルプロセスを保護する特権

特権とは、プロセスが操作を実行するために必要とする権利です。この権利はカーネルにおいて実効性があります。特権の*基本セット*の範囲内で動作するプログラムは、システムセキュリティーポリシーの範囲内で動作します。`setuid root` プログラムは、システムセキュリティーポリシーの範囲を超えて動作するプログラムの例です。特権を使用することで、プログラムは `setuid root` を呼び出さなくてすみます。

特権は、システム上で行える処理をエミュレートします。プログラムは、その実行に必要な最小限の特権で実行できます。たとえば、ファイルを操作するプログラムには、`file_dac_write` および `file_flag_set` 特権が必要になることがあります。プロセス上のこれらの特権により、`root` としてプログラムを実行する必要がなくなります。

これまでシステムは、18 ページの「ユーザー権利およびプロセス権利の基本情報」で導入された特権モデル、つまり権利モデルに準拠していませんでした。むしろ、システムはスーパーユーザーモデルを使用していました。スーパーユーザーモデルでは、プロセスは `root` またはユーザーとして実行されていました。ユーザープロセスは、ユーザーのディレクトリとファイルにだけ作用するように限定されました。`root` プロセスは、システム上の任意の場所にディレクトリとファイルを作成できました。ユーザーのディレクトリ以外の場所にディレクトリを作成する必要があるプロセスは、`UID=0` を使用して (つまり `root` として) 実行されました。セキュリティーポリシーは、システムファイルを保護するのに、任意アクセス制御 (Discretionary Access Control、DAC) に依存していました。デバイスノードは、DAC によって保護されました。たとえば、グループ `sys` が所有しているデバイスをオープンできるのはこのグループのメンバーだけでした。

しかし、`setuid` プログラムやファイルアクセス権、管理アカウントなどは悪用される危険性があります。`setuid` プロセスに許可されているアクションは、このプロセスがその処理に必要な数を上回っています。`setuid root` プログラムが侵入者に攻撃された場合には、全権を有する `root` ユーザーとしてふるまわれてしまいます。同様に、`root` パスワードにアクセスできるユーザーは誰でもシステム全体に損害を与えかねません。

対照的に、特権付きポリシーを適用するシステムでは、ユーザー権利から`root` 権利までの間が段階的です。あるユーザーに通常のユーザーの権利を超える動作を実行するための特権を付与したり、`root` の特権を `root` が現在所有している数より少ない数に制限したりできます。権利に

より、特権で実行されるコマンドを権利プロファイルとして分離し、これを 1 人のユーザーまたは 1 つの役割に割り当てることができます。表1-1「スーパーユーザーモデルと特権モデルの対比」は、権利モデルが提供する root 特権とユーザー権利の間の段階を示しています。

権利モデルでは、スーパーユーザーモデルより高いレベルのセキュリティーが実現されます。プロセスから削除された特権が悪用される可能性はありません。プロセス特権は、弱点を突かれてアクセス権が取得される可能性がある DAC 保護だけの場合と比較して、重要なファイルとデバイスの保護を強化できます。

特権を使用することで、必要な権利しか持たないようにプログラムとプロセスを制限できます。最小特権が実装されたシステムでは、プロセスを取得した侵入者がアクセスできるのはそのプロセスに割り当てられた特権だけです。システムのほかの部分を攻撃することはできません。

特権の説明

特権は、それぞれの領域に基づいて論理的にグループ化されます。

- **FILE 特権** – 文字列 `file` で始まる特権は、ファイルシステムオブジェクトに対して作用します。たとえば、`file_dac_write` 特権は、ファイルへの書き込みの際に任意アクセス制御をオーバーライドします。
- **IPC 特権** – 文字列 `ipc` で始まる特権は、IPC オブジェクトアクセス制御をオーバーライドします。たとえば、`ipc_dac_read` 特権を使用すると、DAC によって保護されているリモート共有メモリーを読み取るプロセスが可能となります。
- **NET 特権** – 文字列 `net` で始まる特権は、特定のネットワーク機能へのアクセスを可能にします。たとえば、`net_rawaccess` 特権を使用すると、デバイスをネットワークに接続できます。
- **PROC 特権** – 文字列 `proc` で始まる特権は、プロセスがそれ自体の限定されたプロパティーを変更できるようにします。`PROC` 特権の中には、ごくわずかな効果しかない特権もあります。たとえば、`proc_clock_highres` 特権は、プロセスが高分解能タイマーを使用できます。
- **SYS特権** – 文字列 `sys` で始まる特権は、各種のシステムプロパティーに対する無制限のアクセス権をプロセスに付与します。たとえば、`sys_linkdir` 特権を使用すると、プロセスはディレクトリに対するハードリンクの確立と解除が行えます。

その他の論理グループには、CONTRACT、CPC、DTRACE、GRAPHICS、VIRT、WIN などがあります。

特権の中にはシステムに対する影響が少ないものもあれば、大きな影響を与えるものもあります。次の proc_taskid 特権の定義は、この特権の影響が小さいことを示しています。

```
proc_taskid
        Allows a process to assign a new task ID to the calling process.
```

net_rawaccess 特権の定義は、その影響が広範囲に及ぶことを示しています。

```
net_rawaccess
        Allows a process to have direct access to the network layer.
```

privileges(5) のマニュアルページに、すべての特権の説明が記載されています。104 ページの「特権の一覧表示」も参照してください。

特権を使用したシステムにおける管理上の相違点

特権を持つシステムと特権を持たないシステムとでは、明白な違いがいくつかあります。次の表に相違点の一部を示します。

表 1-2 特権を持つシステムと特権を持たないシステムとの明白な違い

機能	特権なし	特権
デーモン	デーモンが root として実行されます。	デーモンが、ユーザー daemon として実行されます。 たとえば、デーモン lockd および rpcbind には限定された特権が割り当てられており、daemon として実行されます。
ログファイルの所有権	ログファイルは root によって所有されます。	ログファイルは、そのログファイルを作成する daemon によって所有されます。root ユーザーがこのファイルを所有することはありません。
エラーメッセージ	エラーメッセージでスーパーユーザーが言及されます。 たとえば、chroot: not superuser。	エラーメッセージで特権の使用が言及されます。 たとえば、chroot エラーと同等のエラーメッセージは chroot: exec failed。
setuid プログラム	プログラムは、通常のユーザーが実行を許可されていないタスクを完了するために setuid root を使用します。	多くの setuid root プログラムは、必要な特権のみで実行されます。 たとえば、コマンド audit、ikeadm、ipadm、ipsecconf、ping、traceroute、および newtask は特権を使用します。
ファイルアクセス権	デバイスアクセス権は DAC によって制御されます。たとえば、グループ sys のメンバーは /dev/ip を開くことができます。	デバイスを開くことができるユーザーをファイルアクセス権 (DAC) が予測することはありません。デバイスは、DAC とデバイスポリシーによって保護されます。 たとえば、/dev/ip ファイルには 666 アクセス権がありますが、デバイスを開くことができるのは適切な特権を持つプロセスだけです。

機能	特権なし	特権
監査イベント	su コマンドの使用の監査によって、多くの管理機能がカバーされます。	特権の使用の監査によって、ほとんどの管理機能がカバーされます。cusa 監査クラスには、管理機能をモニターする監査イベントが含まれています。
プロセス	プロセスは、プロセス所有者の権利によって保護されます。	プロセスは特権によって保護されます。プロセス特権とプロセスフラグは、/proc/<pid>/priv ディレクトリ内の新しいエントリとして確認できます。
デバッグ	コアダンプ内で特権の言及はありません。	コアダンプの ELF 注記セクションで、NT_PRPRIV および NT_PRPRIVINFO の注記にプロセス特権とフラグについての情報が示されます。 ppriv コマンドやその他のコマンドでは、適切にサイズ設定されたセットの正しい数が示されます。これらのコマンドでは、ビットセット内のビットが特権名に正しく対応付けられます。

権限の詳細

このセクションでは、特権の実装、使用、および割り当てについて詳しく説明します。

特権の実装方法

各プロセスには、プロセスが特定の特権を使用できるかどうかを判断する 4 つの特権セットがあります。カーネルは、特権「有効セット」を自動的に計算します。初期の特権「継承可能セット」は変更できます。特権を使用するように作成されているプログラムは、そのプログラムで使用する特権の「許可されたセット」を減らすことができます。特権「制限セット」は縮小できます。

- **有効特権セット (E)** – 現在有効である特権の集合です。プロセスは、許可されたセット内の特権を有効セットに追加できます。プロセスは、E から特権を削除することもできます。
- **許可された特権セット (P)** – 使用できる特権の集合です。プログラムは、継承または割り当てを通して特権を使用できます。実行プロファイルは、プログラムに特権を割り当てる方法の 1 つです。setuid コマンドは、root が持つすべての特権をプログラムに割り当てます。許可されたセットから特権を削除することはできますが、追加することはできません。P から削除された特権は、E からも自動的に削除されます。

  *特権を認識する*プログラムは、そのプログラムがまったく使用することのない特権をそのプログラムの許可されたセットから削除します。この方法では、不要な特権がそのプログラムや悪質なプロセスによって悪用されることが防止されます。特権を認識するについての詳細

は、『Oracle Solaris 11 セキュリティー開発者ガイド 』の第 2 章「特権付きアプリケーションの開発」を参照してください。

- **継承可能な特権セット (I)** – exec への呼び出しでプロセスが継承できる特権の集合です。exec への呼び出しのあと、継承された特権は許可されたセットと有効セット内に配置されるため、setuid プログラムという特殊なケースを除き、これらのセットが等しくなります。

  setuid プログラムの場合は、exec への呼び出しのあと、継承可能セットがまず制限セットによって制限されます。続いて、継承された特権のセット (I) から制限セット (L) が除かれたものが、そのプロセスの P と E に割り当てられます。

- **制限特権セット (L)** – プロセスとその子プロセスでどの特権が利用できるかを示す上限を定義する集合です。デフォルトでは、制限セットはすべての特権です。プロセスは制限セットを縮小することはできますが、制限セットを拡張することはできません。L は I の制限に使用されます。このため、L は exec の時点で P と E を制限します。

  特権が割り当てられたプログラムを含むプロファイルがユーザーに割り当てられている場合、通常そのユーザーはそのプログラムを実行できます。未変更のシステムでは、プログラムの割り当て済み特権はユーザーの制限セットの範囲内です。プログラムに割り当てられている特権は、ユーザーの許可されたセットの一部になります。特権を割り当てられたプログラムを実行するには、ユーザーはプロファイルシェルからそのプログラムを実行する必要があります。

カーネルは、基本特権セットを認識します。変更されていないシステムの場合、各ユーザーの初期の継承可能セットはログイン時の基本セットと同じです。基本セットを変更することはできませんが、ユーザーが基本セットからどの特権を継承するかは変更できます。

未変更のシステムでは、ログイン時のユーザーの特権セットは次のようになります。

```
E (Effective): basic
I (Inheritable): basic
P (Permitted): basic
L (Limit): all
```

ログイン時には各ユーザーの基本セットは、それぞれの継承可能セット、許可されたセット、および有効セットに含まれます。ユーザーの制限セットは、ゾーン (大域または非大域) のデフォルトの制限セットと同等です。

追加の特権をユーザー、正確にはユーザーのログインプロセスに直接割り当てるか、権利プロファイルを介して複数のユーザーに間接的に割り当てるか、またはユーザーに対して特権付きコマンドを割り当てることで間接的に割り当てることができます。また、ユーザーの基本セットから特権を削除できます。手順と例については、第3章「Oracle Solaris での権利の割り当て」を参照してください。

特権の使用法

特権は Oracle Solaris に組み込まれています。このセクションでは、Oracle Solaris がデバイス、リソース管理、およびレガシーアプリケーションで特権をどのように使用するかを説明します。

プロセスが特権を取得する方法

プロセスが特権を継承するか、またはプロセスに特権を割り当てることができます。プロセスは、その親から特権を継承します。ログイン時に、ユーザーの初期継承可能特権セットによって、そのユーザーのプロセスで使用できる特権が決まります。ユーザーの当初のログインの子プロセスはすべて、このセットを継承します。

また、プログラム、ユーザー、役割、および特定のリソースに特権を直接割りてることもできます。プログラムで特権が必要な場合は、権利プロファイル内でそのプログラムの実行可能ファイルに特権を割り当てます。そのプログラムの実行を許可されたユーザーまたは役割には、そのプログラムが入ったプロファイルを割り当てます。ログイン時、あるいはプロファイルシェルが開かれている場合、プログラムの実行可能ファイルがプロファイルシェルで入力されると、そのプログラムは特権を使用して実行されます。たとえば、Object Access Management プロファイルが含まれる役割は、`file_chown` 特権を使用して `chmod` コマンドを実行できるため、その役割が所有していないファイルの所有権を変更できます。

付加的な特権が直接割り当てられたプログラムを役割またはユーザーが実行する場合、割り当てられているその特権は役割またはユーザーの継承可能セットに追加されます。特権が割り当てられたプログラムの子プロセスは、親プロセスの特権を継承します。子プロセスが親プロセスよりも多くの特権を必要とする場合には、子プロセスに直接それらの特権を割り当てる必要があります。

特権を使用するように作成されているプログラムは、特権を認識すると呼ばれます。特権を認識するプログラムは、プログラム実行中の特権の使用を有効または無効にできます。本番環境で使用するためには、プログラムに対し、そのプログラムが有効または無効にする特権を割り当てる必要があります。特権を認識するプログラムを使用可能にする前に、そのプログラムに必要な特権だけを実行可能ファイルに割り当てます。続いて管理者はこのプログラムのテストを行い、タスクが正常に行われるか確認します。また、プログラムが特権を悪用しないかも確認します。

特権を認識するコードの例については、『Oracle Solaris 11 セキュリティー開発者ガイド 』の第 2 章「特権付きアプリケーションの開発」を参照してください。特権を必要とするプログラム

に特権を割り当てる場合は、例4-1「レガシーアプリケーションへのセキュリティー属性の割り当て」と例5-7「特権付きコマンドを含む権利プロファイルの作成」を参照してください。

特権とデバイス

スーパーユーザーモデルではファイルアクセス権によってのみ保護されるシステムインタフェースを、権利モデルでは特権によって保護します。特権を使用したシステムでは、インタフェースを保護するほどの強さはファイルアクセス権にありません。`proc_owner` などの特権は、ファイルアクセス権をオーバーライドした上でファイルシステムへのフルアクセス権を取得する可能性があります。

このため、Oracle Solaris では、デバイスを開くにはデバイスディレクトリの所有権では不十分です。たとえば、グループ `sys` のメンバーには、`/dev/ip` デバイスを開くことが自動的には許可されなくなります。`/dev/ip` のファイルアクセス権は `0666` ですが、デバイスを開くには `net_rawaccess` 特権も必要です。

デバイスポリシーは特権によって制御されるため、デバイスを開くためのアクセス権を付与する際の柔軟性が高くなります。特権要件は、デバイスポリシーに合わせて構成することも、ドライバ本体に合わせて構成することもできます。デバイスドライバのインストール、追加、または更新時に、特権要件を構成できます。

詳細は、`add_drv`(1M)、`devfsadm`(1M)、`getdevpolicy`(1M)、および `update_drv`(1M) のマニュアルページを参照してください。

特権およびリソース管理

Oracle Solaris では、`project.max-locked-memory` および `zone.max-locked-memory` リソース制御を使用して、`PRIV_PROC_LOCK_MEMORY` 特権が割り当てられているプロセスのメモリー消費を制限できます。プロセスはこの特権を使うことで、物理メモリー内のページをロックできます。

`PRIV_PROC_LOCK_MEMORY` 特権を権利プロファイルに割り当てると、この特権を持つプロセスに、すべてのメモリーをロックする権限を与えることになります。安全対策として、この特権ユーザーがすべてのメモリーをロックできないように、リソース制御を設定してください。特権付きプロセスが非大域ゾーン内で実行される場合には、`zone.max-locked-memory` リソース制御

を設定します。特権付きプロセスがシステム上で実行される場合には、プロジェクトを作成し、project.max-locked-memory リソース制御を設定します。これらのリソース制御の詳細については、『Oracle Solaris 11.2 でのリソースの管理 』の第 6 章「リソース制御について」および『Oracle Solaris ゾーンの紹介 』の第 2 章「非大域ゾーンの構成の概要」を参照してください。

レガシーアプリケーションと特権の使用

レガシーアプリケーションに対応するために、特権の実装はスーパーユーザーモデルと権利モデルの両方で動作します。カーネルは、プログラムが特権で動作するように設計されていること示す PRIV_AWARE フラグを自動的に追跡します。特権を認識しない子プロセスについて検討してください。親プロセスから継承された特権はどれも、子の許可されたセットおよび有効なセットで使用可能です。子プロセスで UID が 0に設定されていると、その子プロセスが完全なスーパーユーザー権利を持たない場合があります。プロセスの有効なセットおよび許可されたセットは、子の制限セットの特権に限定されます。このように、特権を認識するプロセスの制限セットによって、特権を認識しない子プロセス root 特権が制限されます。

特権の使用のデバッグ

Oracle Solaris には、特権のエラーを修正するツールが用意されています。ppriv コマンドと truss コマンドを使用して、デバッグ結果を出力できます。例については、ppriv(1) のマニュアルページを参照してください。例については、109 ページの「権利に関するトラブルシューティング」を参照してください。また、dtrace コマンドを使用することもできます。詳細は、dtrace(1M) のマニュアルページと『Oracle Solaris 11.2 Dynamic Tracing Guide 』を参照してください。

特権の割り当て

「特権」という用語は従来、権利の強化を意味します。Oracle Solaris システムの各プロセスは何らかの権利を使用して実行されるため、特権を削除することでプロセスの権利を減らすことができます。このリリースでは、*拡張特権ポリシー*を使用することで、特定のリソースにデフォルトで付与されている特権を除くほとんどの特権を削除できます。

ユーザーおよびプロセスへの特権の割り当て

セキュリティー管理者として、特権の割り当てを担当します。既存の権利プロファイルでは、プロファイル内のコマンドに特権がすでに割り当てられています。権利プロファイルを役割またはユーザーに割り当てます。

特権はまた、ユーザー、役割、または権利プロファイルに直接割り当てることもできます。セッションで特権を適切に使用すると信頼できるユーザーには、特権を直接割り当てることができます。直接の割り当てが適するものとしては、影響の少ない特権 (`proc_clock_highres` など) が挙げられます。直接の割り当てに適しない候補としては、`file_dac_write` などの、影響が広範囲に及ぶ特権があります。詳細は、41 ページの「権利の割り当てにおけるセキュリティーに関する考慮事項」を参照してください。

ユーザー、役割、またはプロセスに対する特権が拒否されることもあります。ユーザーまたは役割の初期継承可能セットまたは制限セットから特権を削除する場合は、注意が必要です。

ユーザーまたは役割の特権の拡張

ユーザーや役割には、継承可能な特権セットがあります。制限セットには初めにすべての特権が設定されるため、このセットは削減のみ可能です。ユーザー、役割、およびプロセスの初期継承可能セットは、その継承可能セットにない特権を割り当てることで拡張できます。

使用可能な特権を 3 つの方法で拡張できます。

- 初期継承可能セットには含まれていないが制限セットに含まれている特権は、ユーザーと役割に割り当てることができます。この割り当ては、権利プロファイルの特権付きコマンドを使用して間接的に行うか、または直接行うことができます。
- 継承可能セットに含まれていない特権は、スクリプトまたはアプリケーションへの特権の追加などのように、プロセスに明示的に割り当てることができます。
- 継承可能セットに含まれていないが制限セットに含まれている特権は、ネットワークポート、UID、またはファイルオブジェクトに明示的に割り当てることができます。このような特権の使用は*拡張特権ポリシー*と呼ばれ、使用可能な特権を制限する手段でもあります。詳細は、35 ページの「拡張特権ポリシーを使用した特権使用の制限」を参照してください。

特権を必要とする管理タスクにのみその特権を割り当てることは、ユーザーまたは役割の特権をもっとも的確に拡張する方法です。コマンドまたはスクリプトとその必要な特権が含まれている権利プロファイルを作成します。次に、ユーザーまたは役割にその権利プロファイルを割り当

てます。このように割り当てることで、ユーザーまたは役割はその特権付きコマンドを実行できます。このようにしないと、ユーザーはその特権を使用できません。

ユーザーまたは役割の初期継承可能特権セットの拡張は、特権を割り当てる方法として適切とは言えません。継承可能セット内の特権はすべて、許可されたセットと有効セット内に存在します。シェル内でユーザーまたは役割が入力するコマンドはすべて、直接割り当てられた特権を使用できます。詳細は、41 ページの「権利の割り当てにおけるセキュリティーに関する考慮事項」を参照してください。

不必要に特権が使用可能である状況を減らすには、*拡張特権*をネットワークポート、UID、およびファイルオブジェクトに割り当てることができます。このように割り当てることで、拡張特権割り当てに含まれない特権が有効セットから削除されます。詳細は、35 ページの「拡張特権ポリシーを使用した特権使用の制限」を参照してください。

ユーザーまたは役割の特権の制限

信頼できないユーザーの権利を制限するため、特権と権利プロファイルを信頼できないユーザーに適用することもできます。特権を削除することで、ユーザーと役割による特定のタスク実行を不可能にできます。特権は、初期継承可能セットから削除することも、制限セットから削除することもできます。デフォルトセットよりも小さい初期継承可能セットまたは制限セットを配布する場合は、あらかじめ特権の削除を慎重にテストすることが望まれます。たとえば、初期継承可能セットから特権を削除したためにユーザーがログインできなくなる可能性があります。制限セットから特権を削除すると、削除した特権を必要とする古い `setuid root` プログラムが失敗する可能性があります。特権削除の例については、例3-21「ユーザーの制限セットからの特権の削除」および例5-6「Sun Ray Users 権利プロファイルの作成」を参照してください。

ユーザー ID、ポート、またはファイルオブジェクトに対して使用可能な特権を制限するには、35 ページの「拡張特権ポリシーを使用した特権使用の制限」を参照してください。

スクリプトへの特権の割り当て

スクリプトは、コマンドと同様に実行可能ファイルです。このため、コマンドに特権を追加する場合と同じ方法で、権利プロファイルでスクリプトに特権を追加できます。権利プロファイルが割り当てられたユーザーまたは役割がプロファイルシェルでスクリプトを実行すると、スクリプトは、それらの追加された特権で実行されます。スクリプトに特権が必要なコマンドが含まれている場合は、特権が追加されたコマンドも、割り当てられた権利プロファイルに含まれている必要が

あります。例については、69 ページの「アプリケーションおよびスクリプトへの権利の割り当て」を参照してください。

拡張特権ポリシーを使用した特権使用の制限

拡張特権ポリシーは、基本特権および明示的に付与した特権を除き、ポート、ユーザー ID、またはファイルオブジェクトへのアクセスを制限できます。少ない数の特権では、システムを攻撃する目的でリソースを容易に使用することはできません。実際に、ユーザーは所有するファイルとディレクトリを、悪意のあるプロセスによるアクセスから保護できます。拡張特権ポリシーの例については、69 ページの「アプリケーション、スクリプトおよびリソースの特定の権利への制限」を参照してください。

特権エスカレーションとユーザー権利

Oracle Solaris では、管理者がセキュリティーを構成するとき、高い柔軟性が提供されます。このソフトウェアがインストールされている場合、特権エスカレーションが防止されます。*特権エスカレーション*は、意図していたよりも多くの管理権利がユーザーまたはプロセスに与えられたときに発生します。この場合「特権」とはカーネル特権だけではなく、すべての権利を意味します。36 ページの「特権エスカレーションとカーネル特権」を参照してください。

Oracle Solaris ソフトウェアには、`root` 役割にのみ割り当てられる権利が含まれています。ほかのセキュリティー保護が存在する状態で、`root` 役割用に設計された属性を管理者がほかのアカウントに割り当てる可能性がありますが、このような割り当ては慎重に行う必要があります。次に示す権利プロファイルと一連の承認により、root 以外のアカウントの特権がエスカレートされる可能性があります。

- **Media Restore 権利プロファイル** – このプロファイルはほかのどの権利プロファイルにも含まれていません。Media Restore はルートファイルシステム全体へのアクセスを提供するため、これを使用することで特権のエスカレーションが可能です。故意に改ざんされたファイルや交換したメディアを復元できます。デフォルトでは、`root` 役割にはこの権利プロファイルが含まれています。
- `solaris.*.assign` **承認** – これらの承認はどの権利プロファイルにも割り当てられていません。`solaris.*.assign` 承認を持つアカウントは、そのアカウント自体に割り当てられていない権利をほかのユーザーに割り当てることができます。たとえ

ば、solaris.profile.assign 承認を持つ役割は、その役割自体に割り当てられていない権利プロファイルをほかのアカウントに割り当てることができます。デフォルトでは、solaris.*.assign 承認を持つのは root 役割だけです。

solaris.*.assign 承認ではなく solaris.*.delegate 承認を割り当てます。solaris.*.delegate 承認を使用すると、委託者は、その委託者が所有する権利のみをほかのアカウントに割り当てることができます。たとえば、solaris.profile.delegate 承認が割り当てられた役割は、その役割自体に割り当てられている権利プロファイルをほかのユーザーや役割に割り当てることができます。

カーネル特権のエスカレーションの防止については、36 ページの「特権エスカレーションとカーネル特権」を参照してください。

特権エスカレーションとカーネル特権

カーネルにより特権エスカレーションが防止されます。プロセスが必要な特権以外の特権を取得することを防ぐために、無防備なシステム変更に特権の完全セットがあるかどうかが確認されます。たとえば、root (UID=0) が所有するファイルまたはプロセスは、特権の完全セットを備えたプロセスによってのみ変更できます。root アカウントは、特権がなくても root が所有するファイルを変更することができます。しかし、root ユーザー以外は、root が所有するファイルを変更するにはすべての特権が必要です。

同様に、デバイスへのアクセスを提供する操作には、有効なセットのすべての特権が必要です。特に file_chown_self および proc_owner は、特権エスカレーションが生じやすい特権です。

- file_chown_self は、プロセスがそのファイルを渡せるようにする特権です。proc_owner は、プロセス自身が所有しないプロセスを調査できるようにする特権です。

  file_chown_self 特権は、rstchown システム変数によって制限されます。rstchown 変数が 0 に設定されると、file_chown_self 特権は、システムイメージの全ユーザーの初期継承可能セットから削除されます。rstchown システム変数の詳細については、chown(1) のマニュアルページを参照してください。

  file_chown_self 特権は、特定のコマンド、権利プロファイルに配置されているコマンド、および役割または信頼できるユーザーに割り当てられているプロファイルにもっとも安全に割り当てることができます。

- proc_owner 特権は、プロセス UID を 0 にするには十分ではありません。任意の UID のプロセスを UID=0 にするには、すべての特権が必要です。proc_owner 特権はシステム上の

すべてのファイルに無制限の読み取りアクセス権を与えるので、この特権の特定コマンドへの割り当て、プロファイルに配置されているコマンドへの割り当て、および役割に割り当てられているプロファイルへの割り当てはもっとも安全に行います。

注意 - `file_chown_self` 特権または `proc_owner` 特権がユーザーの初期継承可能セットに含まれるように、ユーザーのアカウントを構成できます。ただし、このような強力な特権をユーザーや役割の継承可能セットに配置するには、セキュリティー上の相応の理由がなければなりません。

デバイスでの特権エスカレーションを防止する方法については、31 ページの「特権とデバイス」を参照してください。一般的な説明については、`privileges`(5) のマニュアルページを参照してください。

権利の検証

割り当てられた権利を評価するかどうかは、プロセスが実行されるシェル、ネームサービスのスコープ、および検索順序の影響を受けます。権利を評価できないプロセスは失敗します。権利割り当ての確認の補足情報については、109 ページの「権利に関するトラブルシューティング」を参照してください。

プロファイルシェルと権利の検証

ユーザーと役割は、プロファイルシェルから特権付きアプリケーションを実行できます。*プロファイルシェル*は、権利を認識する特殊シェルです。管理者は、プロファイルシェルをログインシェルとしてユーザーに割り当てることができます。そうでない場合は、そのユーザーが役割を引き受けるために `pfexec` コマンドまたは `su` コマンドを実行したときに、プロファイルシェルが起動されます。Oracle Solaris では、どのシェルにも、対応するプロファイルシェルがあります。プロファイルシェルのリストについては、`pfexec`(1) のマニュアルページを参照してください。

権利プロファイルが直接割り当てられており、ログインシェルがプロファイルシェルではないユーザーが、割り当てられている特権付きコマンドを実行するには、プロファイルシェルを開く必要があります。認証権利プロファイルが割り当てられているユーザーと役割は、コマンド実行前に認証 (パスワード入力) するように求められます。操作性とセキュリティーに関する考慮事項については、41 ページの「権利の割り当てにおける考慮事項」を参照してください。

ネームサービススコープと権利の検証

ネームサービススコープは、割り当てられている権利がいつ使用可能になるかに影響します。役割の適用範囲は、個々のホストに限定されることがあります。また、LDAP などのネームサービスからサービスを受けるすべてのホストが適用範囲に含まれることもあります。あるシステムのネームサービスの適用範囲は、ネームスイッチサービス `svc:/system/name-service/switch` で指定されます。検索は、最初に一致した時点で停止します。たとえば、権利プロファイルが 2 つのネームサービススコープに存在する場合、最初のネームサービススコープに含まれるエントリだけが使用されます。最初に一致したものが `files` の場合、役割の適用範囲はローカルホストに限定されます。ネームサービスの詳細については、`nsswitch.conf`(4) のマニュアルページ、『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS 』、および『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』を参照してください。

割り当てられた権利の検索順序

ユーザーまたは役割に対し、セキュリティー属性を直接割り当てるか、または権利プロファイルを介して割り当てることができます。検索の順序は、使用されるセキュリティー属性の値に影響を及ぼします。その属性の最初に見つかったインスタンスの値が使用されます。

注記 - 承認の順序は重要ではありません。承認は累積されます。

ユーザーがログインすると、次に示す検索順序で権利が割り当てられます。

- `useradd` および `usermod` コマンドを使ってユーザーに直接割り当てられる**権利**。可能な権利割り当てのリストについては、123 ページの「`user_attr` データベース」を参照してください。
- **useradd** および `usermod` コマンドを使ってユーザーに割り当てられる**権利プロファイル**。これらの割り当ては順番に検索されます。
  - 最初に、認証権利プロファイルが検索されます。

    この順序は、認証プロファイルリストの最初のプロファイル、その補助プロファイル、認証プロファイルリストの 2 番目のプロファイル、その補助プロファイル、のようになります。累積される `auths` 値を除き、最初のインスタンスの値がシステムで使用される値になります。権利プロファイルに割り当てることができる属性には、ユーザーに割り

当てることができるすべての権利と、補助プロファイルが含まれます。リストについては、123 ページの「user_attr データベース」を参照してください。

- 次に、再認証を必要としない権利プロファイルが同様の方法で検索されます。

- **Console User 権利プロファイル**の値。詳細は、119 ページの「権利プロファイルのリファレンス」を参照してください。
- **Stop 権利プロファイル**が割り当てられた場合、セキュリティー属性の評価は停止します。Stop プロファイルが割り当てられたあとは属性は一切割り当てられません。Stop プロファイルは、Console User 権利プロファイルの後、policy.conf ファイル内のほかのセキュリティー属性 (AUTHS_GRANTED など) の前に評価されます。詳細は、119 ページの「権利プロファイルのリファレンス」を参照してください。
- **policy.conf** ファイル内の Basic Solaris User 権利プロファイル の値。
- policy.conf ファイル内の AUTHS_GRANTED の値。
- policy.conf ファイル内の AUTH_PROFS_GRANTED の値。
- policy.conf ファイル内の PROFS_GRANTED の値。
- policy.conf ファイル内の PRIV_DEFAULT の値。
- policy.conf ファイル内の PRIV_LIMIT の値。

権利を確認するアプリケーション

システム制御をオーバーライドするアプリケーションとコマンドは、特権付きアプリケーションとみなされます。アプリケーションは、UID=0 のようなセキュリティー属性、特権、および承認によって特権化されます。

UID と GID を確認するアプリケーション

root (UID=0) やその他の特殊な UID または GID を確認する特権付きアプリケーションは、UNIX 環境に古くから存在します。権利プロファイルのメカニズムによって、特定の ID を必要とするコマンドを分離できます。任意のユーザーがアクセスできるコマンドの ID を変更する代わりに、UID が割り当てられたコマンドを権利プロファイル内に配置できます。その権利プロファイルを持つユーザーまたは役割であれば、スーパーユーザー以外でもその UID としてプログラムを実行できます。

ID は*実* ID または *実効* ID として指定できます。実効 ID を割り当てた場合は、実 ID より優先されます。実効 ID は、ファイルアクセス権ビットの setuid 機能に相当します。実行 ID は、

監査のために UID の識別も行います。ただし、root の実 UID を要求するシェルスクリプトやプログラムのために、実 ID も設定できます。たとえば、reboot コマンドには実効 UID ではなく、実 UID が必要です。

ヒント - あるコマンドを実行するために実効 ID では十分でない場合は、そのコマンドに実 ID を割り当てます。

特権を確認するアプリケーション

特権付きアプリケーションは、特権の使用を確認できます。権利プロファイルメカニズムを使用すると、セキュリティー属性を必要とする特定のコマンドの特権を指定できます。次に、セキュリティー属性が割り当てられたコマンドを権利プロファイル内に分離できます。この権利プロファイルを持つユーザーまたは役割は、そのコマンドに必要な特権だけを使用してコマンドを実行できます。

特権を確認するコマンドとして次のようなものがあります。

- Kerberos コマンド (kadmin、kprop、kdb5_util など)
- ネットワークコマンド (ipadm、routeadm、snoop など)
- ファイルコマンドとファイルシステムコマンド (chmod、chgrp、mount など)
- プロセスを制御するコマンド (kill、pcred、rcapadm など)

特権を持つコマンドを権利プロファイルに追加するには、89 ページの「権利プロファイルを作成する方法」および profiles(1) のマニュアルページを参照してください。特定のプロファイル内の特権を確認するコマンドを判断するには、第6章「Oracle Solaris の権利の一覧表示」を参照してください。

承認を確認するアプリケーション

次を含む一部の Oracle Solaris コマンドは、承認を確認します。

- 監査管理用のコマンド (auditconfig、auditreduce など)
- プリンタ管理用のコマンド (cupsenable、lpadmin など)
- バッチジョブコマンド (at、atq、batch、crontab など)
- デバイス向けのコマンド (allocate、deallocate、list_devices、cdrw など)

スクリプトまたはプログラムでの承認の確認のガイダンスについては、例4-3「スクリプトまたはプログラム内の承認の確認」を参照してください。承認が必要なプログラムを作成するに

は、『Oracle Solaris 11 セキュリティー開発者ガイド 』の「承認について」を参照してください。

権利の割り当てにおける考慮事項

セキュリティーと操作性の問題が、管理者による役割の割り当て方法に影響する可能性があります。

権利の割り当てにおけるセキュリティーに関する考慮事項

一般に、ユーザーまたは役割は権利プロファイルを介して管理権利を取得しますが、権利を直接割り当てることもできます。

- 役割とユーザーには、特権を直接割り当てることができます。

  特権の割り当てを直接行うことは安全とは言えません。特権が直接割り当てられたユーザーと役割は、カーネルがその特権を要求するときにはいつでもセキュリティーポリシーをオーバーライドできます。また、ユーザーまたは役割のプロセスに損害を与える悪質なプロセスが、カーネルでこの特権が必要な場合はいつでもこの特権を使用できます。

  安全なやり方は、特権をコマンドのセキュリティー属性として権利プロファイル内で割り当てる方法です。そうすると、その特権は、その権利プロファイルを持つユーザーが、そのコマンドでのみ使用できます。

- 役割とユーザーには、承認を直接割り当てることができます。

  承認はユーザーレベルで評価されるため、承認の直接割り当ては特権の直接割り当てよりリスクが小さいと言えます。しかし、承認が与えられることで、ユーザーは監査フラグの割り当てなどの高いセキュリティーが求められるタスクも実施できるようになります。セキュリティー強化のため、コマンド実行前にユーザーがパスワードを入力する必要がある認証権利プロファイル内で、承認を割り当てます。

権利の割り当てにおける操作性に関する考慮事項

権利を直接割り当てると、操作性に影響を及ぼす可能性があります。

- 直接割り当てられた承認、およびユーザーの権利プロファイル内のコマンドと承認を有効にするには、プロファイルシェルでこれらを解釈する必要があります。デフォルトでは、ユーザー

にはプロファイルシェルが割り当てられません。したがってユーザーは忘れずにプロファイルシェルを開き、そのシェルでコマンドを実行する必要があります。

- 承認を個々に割り当てる方法には拡張性がありません。また、直接割り当てられた承認は、タスクを実行するには十分でない可能性があります。タスクに特権付きコマンドが必要な場合もあります。

  権利プロファイルは、承認と特権付きコマンドをまとめるように設計されています。また、ユーザーグループに合わせて適切に拡大縮小します。

♦ ♦ ♦ 第 2 章

2 管理権利構成の計画

この章では、システムの管理に従来の権利モデルを使用するか、または Oracle Solaris の権利モデルを活用するかを決定する上で役立つ情報を提供します。この章の内容は次のとおりです。

権利の概要については、14 ページの「ユーザー権管理」を参照してください。参照情報については、第8章「Oracle Solaris 権利リファレンス」を参照してください。

管理に使用する権利モデルの決定

Oracle Solaris の権利には、権利プロファイル、承認、および特権が含まれます。Oracle Solaris ではさまざまな方法でシステムの管理権利を構成できます。

次のリストでは、セキュリティーがもっとも高いモデルから、セキュリティーが低い従来のスーパーユーザーモデル の順に示します。

1. それぞれが限られた権利を持つ複数の信頼できるユーザーの間で管理タスクが分けられます。この方式は Oracle Solaris の権利モデルです。

   この方式を実施する方法については、44 ページの「選択した権利モデルへの準拠」を参照してください。

   この方式の利点については、第1章「権利を使用したユーザーとプロセスの制御について」を参照してください。
2. デフォルトの権利構成を使用します。この方式では権利モデルが使用されますが、モデルはサイトに合わせてカスタマイズされません。

   デフォルトでは、初期ユーザーはいくつかの管理権利を持ち、root 役割を引き受けることができます。root 役割は、オプションで別の信頼できるユーザーに root 役割を割り当てるこ

とができます。セキュリティーを強化するため、root 役割は管理コマンドの監査を有効にすることがあります。

このモデルを使用する管理者にとって役立つタスクを次に示します。

- 84 ページの「割り当てられている管理権利の使用」
- 47 ページの「ユーザーへの権利の割り当て」
- 88 ページの「管理アクションの監査」
- 55 ページの「役割のパスワードの変更」
- 第6章「Oracle Solaris の権利の一覧表示」

3. sudo コマンドを使用します。

   sudo コマンドを使い慣れている管理者が sudo を構成して使用できます。オプションで、sudo ユーザーが一定期間にわたり再認証なしで管理コマンドを実行できるように、/etc/sudoers ファイルを構成できます。

   sudo のユーザーにとって役立つタスクを次に示します。

   - 84 ページの「割り当てられている管理権利の使用」
   - 88 ページの「管理アクションの監査」
   - 認証のキャッシュ – 例5-2「役割の使用を容易にするために認証をキャッシュする」

   sudo コマンドは、権利プロファイルほどカーネルにフックしていません。このコマンドは、すべての特権を持つ root として実行されるため、/etc/sudoers ファイル内で各プログラムに対して指定されている権利を現在のユーザーに付与できます。sudo はプログラムの後続の子プロセスの属性を指定することはできませんが、子プロセスの実行をブロックできます。Oracle Solaris バージョンの sudo は、プロセスから PRIV_PROC_EXEC 特権を削除します。詳細は、次の Oracle Solaris バージョンを参照してください sudo(1M) のマニュアルページ。

4. root 役割をユーザーに変更してスーパーユーザーモデルを使用します。

   従来の UNIX モデルを使用する管理者は、96 ページの「root 役割をユーザーに変更する方法」を完了する必要があります。オプションで root ユーザーは監査を構成できます。

選択した権利モデルへの準拠

ユーザーおよびプロセスの権利の管理は、システム配備の管理に不可欠となることがあります。計画を行うには、組織のセキュリティー要件に関する詳細な知識と、Oracle Solaris での権利

を理解しておく必要があります。このセクションでは、サイトでの権利使用の計画の一般的なプロセスを説明します。

1. 権利に関する基本概念を理解します。

   第1章「権利を使用したユーザーとプロセスの制御について」を参照してください。権利を使用したシステムの管理は、従来の UNIX 管理方法を使用する場合と大幅に異なります。

2. セキュリティーポリシーを調査します。

   組織のセキュリティーポリシーでは、システムに対する潜在的な脅威を詳細に記述し、各脅威のリスクを評価して、それらの脅威に対抗するための方策を提供します。この戦略の一環として、権利を使用してセキュリティー関連タスクを切り離すことがあります。

   たとえば、サイトでセキュリティー管理とセキュリティー以外の管理を切り分ける必要がある場合などです。責務分離の実施については、例3-3「責務を分離するための役割の作成」を参照してください。

   セキュリティーポリシーで Authorization Rules Managed On RBAC (ARMOR) を使用する場合は、ARMOR パッケージをインストールして使用する必要があります。Oracle Solaris での使用については、例3-1「ARMOR の役割の使用」を参照してください。

3. デフォルトの権利プロファイルを確認します。

   デフォルトの権利プロファイルには、タスクの実行に必要な権利がまとめられています。使用可能な権利プロファイルを確認するには、101 ページの「権利プロファイルの一覧表示」を参照してください。

4. 役割を使用するか、またはユーザーに権利プロファイルを直接割り当てるかを決定します。

   役割では、権利の管理が容易になります。役割名は、その役割が実行できるタスクを識別し、ユーザー権利から役割権利を切り離します。役割を使用する場合には 3 つのオプションがあります。

   - ARMOR パッケージをインストールできます (この場合 Authorization Roles Managed on RBAC (ARMOR) 標準により定義される 7 つの役割がインストールされます)。例3-1「ARMOR の役割の使用」を参照してください。
   - ユーザー独自の役割を定義したり、ARMOR 役割を使用したりできます。49 ページの「役割の作成」および 例3-1「ARMOR の役割の使用」を参照してください。
   - ユーザー独自の役割を定義し、ARMOR 役割は使用しないでおくことができます。49 ページの「役割の作成」を参照してください。

   サイトで役割が不要な場合は、権利プロファイルをユーザーに直接割り当てることができます。ユーザーが各自の権利プロファイルから管理タスクを実行するときにパスワードを求める

には、認証権利プロファイルを使用します。例3-11「ユーザーに対し DHCP 管理の前にパスワード入力を求める」を参照してください。

5. 追加の権利プロファイルを作成する必要があるかどうかを判断します。

   使用するサイトで、アクセスを制限する必要があるアプリケーションを調べます。セキュリティーに影響するアプリケーション、サービス拒否の問題を発生させる可能性のあるアプリケーション、特別な管理者教育を必要とするアプリケーションには、権利を使用することをお勧めします。たとえば Sun Ray システムのユーザーには、すべての基本特権が必要であるわけではありません。ユーザーを制限する権利プロファイルの例については、例3-22「権利プロファイルからの基本特権の削除」を参照してください。

   a. 新しいタスクに必要な権利を決定します。
   b. 既存の権利プロファイルがこのタスクに対して適切であるかどうかを判断します。
   c. コマンドがその必要な特権を使用して実行されるように権利プロファイルを順序付けます。

      順序付けについては、38 ページの「割り当てられた権利の検索順序」を参照してください。

6. どのユーザーにどの権利を割り当てるかを決定します。

   最少特権の原則に従って、ユーザーの信頼レベルに適した役割にユーザーを割り当てます。実行する必要のないタスクをユーザーが実行できないようにすると、問題が発生する可能性が減少します。

注記 - システムのすべてのユーザーに適用する役割は、`/etc/security/policy.conf` ファイルに指定されています。

計画が完成したら、権利プロファイルまたは役割を割り当てることができる信頼できるユーザーのログインを作成します。ユーザーの作成の詳細については、『Oracle Solaris 11.2 のユーザーアカウントとユーザー環境の管理 』の「CLI を使用したユーザーアカウントの設定と管理のタスクマップ」を参照してください。

権利を割り当てるには、47 ページの「ユーザーへの権利の割り当て」の手順から開始します。以降のセクションでは、権利の拡張、権利の制限、リソースへの権利の割り当て、および権利割り当てのトラブルシューティングの例を示します。

♦ ♦ ♦ 第 3 章

3 Oracle Solaris での権利の割り当て

この章では、ユーザーと役割に権利を割り当てるためのタスクについて説明します。この章の内容は次のとおりです。

- 47 ページの「ユーザーへの権利の割り当て」
- 56 ページの「ユーザーの権利の拡張」
- 61 ページの「ユーザーの権利の制限」

権利の概要については、14 ページの「ユーザー権管理」を参照してください。参照情報については、第8章「Oracle Solaris 権利リファレンス」を参照してください。

ユーザーへの権利の割り当て

Oracle Solaris の権利はすべてのプロセスに存在します。ユーザーと役割に権利を追加したり、権利を削除したりできます。権利には、ユーザープロセスの特権、ユーザーが実行するコマンドの特権または特別な ID、および特定アクションの実行のための承認が含まれます。権利割り当てに伴う管理作業の負担を軽減するため、Oracle Solaris ではサービスと管理アクションに関する権利が*権利プロファイル*にまとめられています。個別の権利をユーザーと役割に割り当てる代わりに、管理タスクに必要なすべての承認と特権を含む権利プロファイルを割り当てることができます。

役割により、ユーザーが実行できる管理タスクに `auditadm` などの名前が指定されます。管理アクションを実行するため、ユーザーはそのアクションの実行のために割り当てられている役割を引き受けます。役割はセキュリティーポリシーで必要とされることがあり、単純に便利です。役割を作成するか、または 7 つの役割とそのローカルホームディレクトリを作成する `armor` パッケージをインストールできます。役割の詳細については、14 ページの「スーパーユーザーモデルの代替としてのユーザー権利およびプロセス権利」を参照してください。

役割を割り当てることができるユーザー

まず、ユーザーを作成して権利を追加するには root 役割である必要があります。

root 役割により、管理タスクが信頼できるユーザーとしてユーザーに配布されているか、または役割をユーザーに割り当てることで管理タスクが割配布されている場合、次に示す権利プロファイルが割り当てられると、ユーザーと役割の作成またはユーザーと役割への権利の割り当てが可能になります。

- ユーザーまたは役割を作成するには、User Management 権利プロファイルが割り当てられている管理者になる必要があります。
- ユーザーまたは役割にほとんどの権利を割り当てるには、User Security 権利プロファイルが割り当てられている管理者になる必要があります。

  監査フラグを割り当てることはできません。ユーザーまたは役割に監査フラグを割り当てることができるのは root 役割だけです。

  役割のパスワードは変更できません。役割のパスワードを変更できるのは root 役割だけです。

管理権利が割り当てられている場合は、管理コマンドを実行する前に 84 ページの「割り当てられている管理権利の使用」を参照してください。

ユーザーおよび役割への権利の割り当て

このセクションでは、役割とユーザーを作成および変更するコマンドについて説明します。権利プロファイルを作成または変更するには、89 ページの「権利プロファイルを作成する方法」および 91 ページの「システム権利プロファイルをクローニングおよび変更する方法」を参照してください。

役割の詳細については、18 ページの「ユーザー権利およびプロセス権利の基本情報」を参照してください。

役割とユーザーの作成または変更における主なアクションを次に示します。

- 役割の作成
- 信頼できるユーザーの作成
- 役割の権利の変更
- ユーザーの権利の変更
- ユーザー独自のパスワードを使用した役割の引き受けの有効化
- 役割のパスワードの変更

■ 役割の削除

役割の作成

役割を使用する場合にはさまざまなオプションがあります。ARMOR から事前定義の役割をインストールし、排他的に使用できます。また、役割を作成してパスワードを指定することもできます。ARMOR の役割と作成した役割をあわせて使用できます。

ARMOR の役割を使用するには、例3-1「ARMOR の役割の使用」を参照してください。

ユーザー独自の役割を作成するには、`roleadd` コマンドを使用します。このコマンドのすべての引数のリストについては、`roleadd`(1M) のマニュアルページを参照してください。

たとえば次のコマンドは、ローカルの User Administrator 役割とホームディレクトリ、`pfbash` ログインシェルを作成し、その役割のパスワードを作成します。

```
# roleadd -c "User Administrator role, local" \
-m -K profiles="User Security,User Management"  useradm
80 blocks
# ls /export/home/useradm
local.bash_profile     local.login     local.profile
# passwd useradm
Password: xxxxxxxx
Confirm Password: xxxxxxxx
```

各情報の意味は次のとおりです。

`-c` *comment*	役割を記述します。
`-m`	ホームディレクトリを作成します。
`-K profiles=`	1 つまたは複数の権利プロファイルを役割に割り当てます。権利プロファイルのリストについては、101 ページの「権利プロファイルの一覧表示」を参照してください。
rolename	役割の名前です。許容される文字列の制限については、`roleadd`(1M) のマニュアルページを参照してください。

注記 - 役割アカウントを複数のユーザーに割り当てることができます。そのため、管理者は役割パスワードを作成し、その役割パスワードを通常の通信手段以外の手段でユーザーに伝えます。役割のパスワードの代替については、54 ページの「役割パスワードでのユーザー独自のパスワード使用の有効化」、例3-16「役割パスワードでのユーザー独自のパスワード使用の有効化」および例3-17「ユーザーが役割パスワードとして独自のパスワードを使用できるようにするための権利プロファイルの変更」を参照してください。

例 3-1 ARMOR の役割の使用

この例では、セキュリティー管理者が ARMOR 標準により定義されている役割をインストールします。管理者は最初に、役割名が既存のアカウントと競合していないことを確認してから、パッケージのインストール、役割定義の表示、および信頼できるユーザーへの役割の割り当てを行います。

管理者は最初に、次の UID と名前がネームサービスに存在していないことを確認します。

- `57 auditadm`
- `55 fsadm`
- `58 pkgadm`
- `53 secadm`
- `56 svcadm`
- `59 sysop`
- `54 useradm`

管理者は UID と名前が使用されていないことを確認してから、パッケージをインストールします。

```
# pkg install system/security/armor
```

このパッケージは、7 つの役割とローカルホームディレクトリを `/export/home` ディレクトリに作成します。

各役割の権利を確認するため、管理者は各役割に割り当てられているプロファイルを一覧表示できます。

```
# profiles auditadm
# profiles fsadm
# profiles pkgadm
# profiles secadm
# profiles svcadm
# profiles sysop
# profiles useradm
```

これらの権利割り当ては変更できません。別の権利構成を作成するには、新しい役割を作成してから、91 ページの「システム権利プロファイルをクローニングおよび変更する方法」の手順に従って新しい権利プロファイルを作成する必要があります。

最後に、管理者は信頼できるユーザーに役割を割り当てます。役割の認証にはユーザー独自のパスワードが使用されます。一部のユーザーには複数の役割が割り当てられます。時間的制約のあるタスクを持つ役割は、複数の信頼できるユーザーに割り当てられます。

```
# usermod -R=auditadm adal
# usermod -R=fsadm,pkgadm bdewey
# usermod -R=secadm,useradm cfoure
# usermod -R=svcadm ghamada
# usermod -R=svcadm yjones
# usermod -R=sysop hmurtha
# usermod -R=sysop twong
```

例 3-2 LDAP リポジトリでの User Administrator 役割の作成

管理者は LDAP 内に User Administrator 役割を作成します。ユーザーは役割を引き受けるときにパスワードを入力するため、個々のコマンドにパスワードを入力する必要がなくなります。

```
# roleadd -c "User Administrator role, LDAP" -m -S ldap \
-K profiles="User Security,User Management"  useradm
```

例 3-3 責務を分離するための役割の作成

管理者は 2 つの役割を作成します。`usermgt` 役割は、ユーザーを作成したり、ユーザーにホームディレクトリを提供したり、その他のセキュリティー以外のタスクを実行したりできます。`usersec` 役割は、ユーザーの作成はできませんが、パスワードの割り当てとほかの権利の割り当て変更は実行できます。いずれの役割でも、ユーザーまたは役割の監査フラグの設定や、役割のパスワードの変更はできません。これらのアクションは `root` 役割が実行する必要があります。

```
# roleadd -c "User Management role, LDAP" -s /usr/bin/pfksh \
-m -S ldap -K profiles="User Management"  usermgt
# roleadd -c "User Security role, LDAP" -s /usr/bin/pfksh \
-m -S ldap -K profiles="User Security"  usersec
```

管理者は、例3-5「ユーザーへの役割の割り当て」の通常のユーザーをすべて作成するには 2 人のユーザーが必要であると確認できます。

例 3-4 暗号化サービス管理のための役割の作成と割り当て

この例では、LDAP ネットワーク上の管理者が暗号化フレームワークを管理するための役割を作成して、その役割を UID 1111 に割り当てます。

```
# roleadd -c "Cryptographic Services manager" \
-g 14 -m -u 104 -S ldap -K profiles="Crypto Management" cryptmgt
# passwd cryptmgt
New Password: xxxxxxxx
Confirm password: xxxxxxxx
# usermod -u 1111 -R +cryptmgt
```

UID が 1111 のユーザーは、ログイン後にその役割を引き受けて、割り当てられている権利を表示します。

```
% su - cryptmgt
Password: xxxxxxxx
# profiles -l
      Crypto Management
          /usr/bin/kmfcfg            euid=0
          /usr/sbin/cryptoadm        euid=0
          /usr/sfw/bin/CA.pl         euid=0
          /usr/sfw/bin/openssl       euid=0
#
```

暗号化フレームワークについては、『Oracle Solaris 11.2 での暗号化と証明書の管理 』の第 1 章「暗号化フレームワーク」を参照してください。フレームワークを管理するには、『Oracle Solaris 11.2 での暗号化と証明書の管理 』の「暗号化フレームワークの管理」を参照してください。

信頼できるユーザーのログインの作成

ログインを作成するには useradd コマンドを使用します。useradd コマンドのすべての引数のリストについては、useradd(1M) のマニュアルページを参照してください。このコマンドの権利関連の引数は roleadd コマンドと同じですが、さらに -R *rolename* オプションがあります。

役割をユーザーに割り当てる場合、ユーザーはその役割を引き受けたあとでその役割の権利を使用できます。たとえば次のコマンドは、52 ページの「信頼できるユーザーのログインの作成」で作成した useradm 役割を引き受けることが可能な信頼できるユーザーを作成します。

```
# useradd -c "Trusted Assistant User Manager user" -m -R useradm jdoe
80 blocks
# ls /export/home/jdoe
local.bash_profile     local.login     local.profile
```

各情報の意味は次のとおりです。

-s *shell*
: *username* のログインシェルを決定します。このシェルは pfbash などのプロファイルシェルにできます。信頼できるユーザーにプロファイルシェルを割り当てる理由については、41 ページの「権利の割り当てにおける操作性に関する考慮事項」を参照してください。プロファイルシェルのリストについては、pfexec(1) のマニュアルページを参照してください。

-R *rolename*
: 既存の役割の名前を割り当てます。

その他の例については、『Oracle Solaris 11.2 のユーザーアカウントとユーザー環境の管理 』の「CLI を使用したユーザーアカウントの設定と管理のタスクマップ」を参照してください。

ユーザーの権利の変更

ユーザーアカウントを変更するには、usermod コマンドを使用します。usermod コマンドのすべての引数のリストについては、usermod(1M) のマニュアルページを参照してください。このコマンドの権利関連の引数は useradd コマンドと同じです。

権利プロファイルをユーザーに割り当てると、そのユーザーはプロファイルシェルを開いたあとで権利を使用できます。たとえば、ユーザーに権利プロファイルを割り当てます。

```
# usermod -K profiles="User Management" kdoe
```

これらの変更は、そのユーザーの次回のログイン時に有効になります。ユーザーが割り当てられている権利を使用する方法を習得する場合は、84 ページの「割り当てられている管理権利の使用」を参照するように指示してください。

例 3-5 ユーザーへの役割の割り当て

この例では、通常のユーザーを作成するために 2 人の信頼できるユーザーが必要であることを管理者が確認します。役割は例3-3「責務を分離するための役割の作成」で作成されたものです。

```
# usermod -R +useradm jdoe
# usermod -R +usersec mdoe
```

役割の権利の変更

役割アカウントを変更するには、rolemod コマンドを使用します。rolemod コマンドのすべての引数のリストについては、rolemod(1M) のマニュアルページを参照してください。このコマンドの権利関連の引数は roleadd コマンドと同じです。

key=*value* ペアの値と、-A、-P、および -R オプションは、マイナス記号 (-) またはプラス記号 (+) を使用して変更できます。- 記号は、現在割り当てられている値から値を引くことを示します。+ 記号は、現在割り当てられている値に値を加えることを示します。権利プロファイルの場合、値は現在のプロファイルリストの先頭に付加されます。権利プロファイルが先の順序であることの影響については、38 ページの「割り当てられた権利の検索順序」を参照してください。

例 3-6 役割の最初の権利プロファイルとしての権利プロファイルの追加

たとえば、useradm 役割の先頭に権利プロファイルを付加します。

```
# rolemod -K profiles+="Device Management" useradm
# profiles useradm
useradm:
Device Management
User Management
User Security
```

例 3-7 ローカル役割に割り当てられているプロファイルの置換

この例では、セキュリティー管理者が prtmgt 役割を変更し、Printer Management プロファイルの後に VSCAN Management 権利プロファイルを組み込みます。

```
# rolemod -c "Handles printers and virus scanning" \
-P "Printer Management,VSCAN Management,All" prtmgt
```

例 3-8 役割への特権の直接割り当て

この例では、セキュリティー管理者は、システム時間に影響を及ぼすきわめて特殊な特権を realtime 役割に委ねます。特権をユーザーに割り当てるには、例3-14「ユーザーへの特権の直接割り当て」を参照してください。

```
# rolemod -K defaultpriv+='proc_clock_highres' realtime
```

defaultpriv キーワードの値は、常にその役割のプロセスに含まれる特権のリスト内にあります。

役割パスワードでのユーザー独自のパスワード使用の有効化

ユーザーが役割を引き受けるときに役割のパスワードではなくユーザー独自のパスワードを使用できるようにするには、その役割を変更します。

次のコマンドは、useradm 役割が割り当てられているすべてのユーザーが、useradm 役割を含め、割り当てられている任意の役割を引き受けるときに、ユーザー独自のパスワードを使用できるようにします。

```
# rolemod -K roleauth=user useradm
```

役割のパスワードの変更

役割は多数のユーザーに割り当てることができるため、役割が割り当てられているユーザーは、その役割のパスワードを変更できません。役割のパスワードを変更するには root 役割である必要があります。

```
# passwd useradm
Enter useradm's password: xxxxxxxx
New: xxxxxxxx
Confirm: xxxxxxxx
```

リポジトリを指定しない場合は、すべてのリポジトリでパスワードが変更されます。

コマンドオプションの詳細については、passwd(1) のマニュアルページを参照してください。

例 3-9 特定リポジトリでの役割のパスワードの変更

次の例では、root 役割がローカル devadmin 役割のパスワードを変更します。

```
# passwd -r files  devadmin
New password: xxxxxxxx
Confirm password: xxxxxxxx
```

次の例では、root 役割が LDAP ネームサービス内で devadmin 役割のパスワードを変更します。

```
# passwd -r ldap devadmin
New password: xxxxxxxx
Confirm password: xxxxxxxx
```

役割の削除

役割を削除すると、その役割は即時に使用不可になります。

```
# roledel useradm
```

役割の管理タスクを現在実行しているユーザーは、続行できなくなります。profiles コマンドは次の出力を表示します。

```
useradm # profiles
Unable to get user name
```

ユーザーの権利の拡張

このセクションのタスクと例では、ユーザーにデフォルトで付与される権利に権利を追加します。権利の詳細については、第1章「権利を使用したユーザーとプロセスの制御について」を参照してください。

- 信頼できるユーザーへ役割を割り当てる – 例3-1「ARMOR の役割の使用」、例3-4「暗号化サービス管理のための役割の作成と割り当て」、例3-5「ユーザーへの役割の割り当て」
- 信頼できるユーザーへ権利プロファイルを割り当てる – 例3-10「DHCP を管理できるユーザーの作成」、例3-19「信頼できるユーザーによる拡張アカウントファイル読み取りの有効化」、例4-1「レガシーアプリケーションへのセキュリティー属性の割り当て」
- 信頼できるユーザーへ認証権利プロファイルを割り当てる – 例3-11「ユーザーに対し DHCP 管理の前にパスワード入力を求める」、例4-2「割り当てられた権利でのアプリケーションの実行」
- 信頼できるユーザーまたは役割へ承認を割り当てる – 例3-12「ユーザーへの承認の直接割り当て」、例3-13「役割への承認の割り当て」
- ユーザーまたは役割へ特権を直接割り当てる – 例3-8「役割への特権の直接割り当て」、例3-14「ユーザーへの特権の直接割り当て」、例3-15「役割の基本特権への追加」

注意 - 直接割り当てられた特権と承認を不適切に使用すると、意図しないセキュリティー違反が発生することがあります。詳細は、41 ページの「権利の割り当てにおけるセキュリティーに関する考慮事項」を参照してください。

- ユーザーが役割を引き受けるときに独自のパスワードを使用できるようにする – 例3-16「役割パスワードでのユーザー独自のパスワード使用の有効化」、例3-17「ユーザーが役割パスワードとして独自のパスワードを使用できるようにするための権利プロファイルの変更」
- 権利プロファイルを変更する – 例3-22「権利プロファイルからの基本特権の削除」
- 権利プロファイルのコマンドにセキュリティー属性を追加する – 例3-26「選択したアプリケーションによる新規プロセス生成の防止」、例3-27「ゲストによるエディタサブプロセス生成の防止」、例5-7「特権付きコマンドを含む権利プロファイルの作成」
- ユーザーが `root` 所有ファイルを読み取れるようにする – 例3-19「信頼できるユーザーによる拡張アカウントファイル読み取りの有効化」、例3-20「`root` 以外のアカウントによる `root` 所有ファイルの読み取りの有効化」
- ユーザーまたは役割が `root` 所有ファイルを編集できるようにする – 例5-9「権利プロファイルでの選択した権利のクローニングおよび削除」

- 新しい承認が含まれている権利プロファイルを割り当てる – 例5-11「権利プロファイルへの承認の追加」

例 3-10 DHCP を管理できるユーザーの作成

セキュリティー管理者が、DHCP を管理できるユーザーを作成します。

```
# useradd -P "DHCP Management" -s /usr/bin/pfbash -S ldap  jdoe
```

ユーザーにはログインシェルとして `pfbash` が割り当てられるため、DHCP Management 権利プロファイル内の権利は常に評価され、DHCP 管理コマンドが正常に完了します。

例 3-11 ユーザーに対し DHCP 管理の前にパスワード入力を求める

この例では、セキュリティー管理者が `jdoe` に対し、DHCP を管理する前にパスワードを入力するよう求めます。

```
# usermod -K auth_profiles="DHCP Management" profiles="Edit Administrative Files" jdoe
```

`jdoe` が DHCP コマンドを入力すると、パスワードプロンプトが表示されます。`jdoe` の認証後に DHCP コマンドが完了します。検索順序に従って、通常のプロファイルの前に認証権利プロファイルが処理されます。

```
jdoe% dhcpconfig -R 120.30.33.7,120.30.42.132
Password: xxxxxxxx
    /** Command completes **/
```

例 3-12 ユーザーへの承認の直接割り当て

この例では、セキュリティー管理者が、画面の明るさを制御できるローカルユーザーを作成します。

```
# useradd -c "Screened KDoe, local" -s /usr/bin/pfbash \
-A solaris.system.power.brightness  kdoe
```

この承認は、ユーザーの既存の承認の割り当てに追加されます。

例 3-13 役割への承認の割り当て

この例では、セキュリティー管理者が DNS サーバーサービスの構成情報を変更できる役割を作成します。

```
# roleadd -c "DNS administrator role" -m -A solaris.smf.manage.bind" dnsadmin
```

例 3-14 ユーザーへの特権の直接割り当て

この例では、セキュリティー管理者が、システム時間に影響を及ぼすきわめて特殊な特権をユーザー kdoe に委ねます。特権を役割に割り当てるには、例3-8「役割への特権の直接割り当て」を参照してください。

```
# usermod -K defaultpriv='basic,proc_clock_highres' kdoe
```

既存の値が defaultpriv キーワードの値で置き換えられます。このため、ユーザーが basic 特権を保持するために、値 basic が指定されます。デフォルトの構成では、すべてのユーザーが基本特権を保持します。基本特権のリストについては、104 ページの「特権の一覧表示」を参照してください。

ユーザーは追加された特権とその定義を表示できます。

```
kdoe% ppriv -v $$
1800:   pfksh
flags = <none>
        E: file_link_any,…,proc_clock_highres,sys_ib_info
        I: file_link_any,…,proc_clock_highres,sys_ib_info
        P: file_link_any,…,proc_clock_highres,sys_ib_info
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,win_upgrade_sl
% ppriv -vl proc_clock_highres
        Allows a process to use high resolution timers.
```

例 3-15 役割の基本特権への追加

次の例では、役割 realtime に日時のプログラムを処理する特権が直接割り当てられます。例3-8「役割への特権の直接割り当て」では proc_clock_highres を realtime に割り当てました。

```
# rolemod -K defaultpriv='basic,sys_time' realtime

% su - realtime
Password: xxxxxxxx
# ppriv -v $$
1600:   pfksh
flags = <none>
        E: file_link_any,...,proc_clock_highres,sys_ib_info,sys_time
        I: file_link_any,...,proc_clock_highres,sys_ib_info,sys_time
        P: file_link_any,...,proc_clock_highres,sys_ib_info,sys_time
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

例 3-16 役割パスワードでのユーザー独自のパスワード使用の有効化

デフォルトでは、ユーザーが役割になるには、その役割のパスワードを入力する必要があります。ユーザーパスワードを要求することで、管理者は Linux 環境での役割の引き受けと同様に Oracle Solaris で役割を引き受けられるようにします。

```
# rolemod -K roleauth=user auditrev
```

割り当てられたユーザーは、この役割を引き受けるために、その役割用に特別に作成されたパスワードではなく、自分のパスワードを使用できるようになります。

ユーザーにほかの役割が割り当てられている場合は、ユーザーのパスワードによってそれらの役割への認証も行われます。

例 3-17 ユーザーが役割パスワードとして独自のパスワードを使用できるようにするための権利プロファイルの変更

```
# profiles -p "Local System Administrator"
profiles:Local System Administrator> set roleauth="user"
profiles:Local System Administrator> end
profiles:Local System Administrator> exit
```

Local System Administrator 権利プロファイルが割り当てられているユーザーがその役割を引き受ける場合、そのユーザーはパスワードの入力を求められます。次のシーケンスでは、役割名は `admin` です。

```
% su - admin
Password: xxxxxxxx
#       /** You are now in a profile shell with administrative rights**/
```

例 3-18 LDAP リポジトリ内の役割の `roleauth` の値を変更する

この例では、`root` 役割によって、役割 `secadmin` を引き受けることができるすべてのユーザーが役割の引き受け時に自分のパスワードを使用できるようになります。この機能は、LDAP サーバーによって管理されるすべてのシステムでこれらのユーザーに付与されます。

```
# rolemod -S ldap -K roleauth=user secadmin
```

例 3-19 信頼できるユーザーによる拡張アカウントファイル読み取りの有効化

信頼できるユーザーまたはユーザーグループによる、`root` アカウントが所有するファイルの読み取りを可能にできます。この権利は、`root` 所有ファイルを含む管理アプリケーションを実行でき

るユーザーにとって役立ちます。この例では、1 つまたは複数の Perl スクリプトを Extended Accounting Net Management 権利プロファイルに追加します。

管理者は root 役割を引き受けたあとで、名前が network で始まるアカウンティングファイルの読み取り機能を追加する権利プロファイルを作成します。

次のプロファイルは、拡張特権ポリシーを使用して file_dac_read 特権をスクリプトに付与し、これによりこのスクリプトは /var/adm/exacct/network* ファイルのみにアクセスできるようになります。このプロファイルは既存の Extended Accounting Net Management 権利プロファイルを補助プロファイルとして追加します。

```
# profiles -p "Extended Accounting Perl Scripts"
profiles:Extended Accounting Perl Scripts >
set desc="Perl Scripts for Extended Accounting"
... Scripts> add profiles="Extended Accounting Net Management"
... Scripts> add cmd=/usr/local/bin/exacctdisp.pl
... Scripts:exacctdisp.pl> set privs={file_dac_read}:/var/adm/exacct/network*
... Scripts:exacctdisp.pl> end
... Scripts> commit
... Scripts> exit
```

サンプルスクリプトについては、『Oracle Solaris 11.2 でのリソースの管理 』の「libexacct に対する Perl インタフェースの使用」を参照してください。

管理者は、権利プロファイルエントリで、スペルミス、省略、繰り返しなどのエラーがないかどうかを確認してから、Extended Accounting Perl Scripts 権利プロファイルを役割またはユーザーに割り当てます。

```
# profiles -p "Extended Accounting Perl Scripts" info
Found profile in files repository.
name=Extended Accounting Perl Scripts
desc=Perl Scripts for Extended Accounting
profiles=Extended Accounting Net Management
cmd=/usr/local/bin/exacctdisp.pl
privs={file_dac_read}:/var/adm/exacct/network*

# rolemod -K profiles+="Extended Accounting Perl Scripts" rolename
# usermod -K profiles+="Extended Accounting Perl Scripts" username
```

例 3-20 root 以外のアカウントによる root 所有ファイルの読み取りの有効化

この例では、管理者が拡張特権ポリシーを使用する権利プロファイルを作成し、認証されるユーザーと役割が、root が所有する /var/adm/sulog ファイルを読み取ることができるようにします。管理者は、ユーザーがファイルの読み取りに使用できるコマンドを追加します。head コマンドなど、リストにないコマンドを使用不可にすることはできません。

```
# profiles -p "Read sulog File"
profiles:Read sulog File
set desc="Read sulog File"
... File> add profiles="Read Log Files"
... File> add cmd=/usr/bin/cat
... File:cat> set privs={file_dac_read}:/var/adm/sulog
... File:cat> end
... File> add cmd=/usr/bin/less
... File:less> set privs={file_dac_read}:/var/adm/sulog
... File:less> end
... File> add cmd=/usr/bin/more
... File:more> set privs={file_dac_read}:/var/adm/sulog
... File:more> end
... File> add cmd=/usr/bin/page
... File:page> set privs={file_dac_read}:/var/adm/sulog
... File:page> end
... File> add cmd=/usr/bin/tail
... File:tail> set privs={file_dac_read}:/var/adm/sulog
... File:tail> end
... File> add cmd=/usr/bin/view
... File:head> set privs={file_dac_read}:/var/adm/sulog
... File:head> end
... File> commit
... File> exit
```

view コマンドは、ユーザーによるファイル読み取りを可能にしますが、編集はできません。

ユーザーの権利の制限

このセクションの例では、通常のユーザーの権利を制限するか、または管理者から一部の管理権利を削除します。ユーザー、役割、および権利プロファイルを変更する方法を示します。権利の詳細については、第1章「権利を使用したユーザーとプロセスの制御について」を参照してください。

- ユーザーから制限特権を削除する – 例3-21「ユーザーの制限セットからの特権の削除」
- ユーザーから基本特権を削除する – 例3-22「権利プロファイルからの基本特権の削除」
- ユーザー独自のシェルプロセスから基本特権を削除する – 例3-23「ユーザー自身からの基本特権の削除」
- 使用が制限されたシステムを作成する – 例3-24「システムをそのユーザーが使用できる権限を制限するように変更する」
- 管理者を明示的に割り当てられている権利に制限する – 例3-25「明示的に割り当てられた権利への管理者の制限」

- システムのすべてのユーザーから権利を削除する – 例3-24「システムをそのユーザーが使用できる権限を制限するように変更する」、例3-28「全ユーザーへの Editor Restrictions 権利プロファイルの割り当て」
- アプリケーションがサブプロセスを作成できないようにする – 例3-26「選択したアプリケーションによる新規プロセス生成の防止」
- ユーザープロセスがサブプロセスを生成できないようにする – 例3-27「ゲストによるエディタサブプロセス生成の防止」
- ゲスト用の制限付きエディタを作成する – 例3-27「ゲストによるエディタサブプロセス生成の防止」
- パブリックシステムに制限付きエディタを割り当てる – 例3-28「全ユーザーへの Editor Restrictions 権利プロファイルの割り当て」
- 権利プロファイルの制限セットから特権を削除する – 例5-6「Sun Ray Users 権利プロファイルの作成」
- Sun Ray ユーザー向けの権利プロファイルを作成する – 例5-6「Sun Ray Users 権利プロファイルの作成」
- 権利プロファイルから権利を削除する – 例5-6「Sun Ray Users 権利プロファイルの作成」、例5-9「権利プロファイルでの選択した権利のクローニングおよび削除」
- ユーザーから承認を削除する – 例5-10「新しい承認のテスト」
- 役割割り当てを削除する – 例5-13「システム保守での `root` 役割の使用の防止」

例 3-21 ユーザーの制限セットからの特権の削除

次の例では、`jdoe` の最初のログインから開始されるすべてのセッションで `sys_linkdir` 特権を使用できないようにします。`su` コマンドの実行後でも、ユーザーはディレクトリへのハードリンクの作成やディレクトリのリンク解除を実行できません。

```
# usermod -K 'limitpriv=all,!sys_linkdir' jdoe
# userattr limitpriv jdoe
all,!sys_linkdir
```

例 3-22 権利プロファイルからの基本特権の削除

次の例では、徹底的なテストのあとで、セキュリティー管理者は Sun Ray Users 権利プロファイルから別の基本特権を削除します。管理者は例5-6「Sun Ray Users 権利プロファイルの作成」のプロファイルを作成したときに、制限セットから 1 つの特権を削除しています。ここでは、管理者は 2 つの基本特権を削除します。このプロファイルが割り当てられているユーザー

は、現在のセッションの外部ではどのプロセスも検査できず、さらに別のセッションを追加することもできません。

```
# profiles -p "Sun Ray Users"
profiles:Sun Ray Users> set defaultpriv="basic,!proc_session,!proc_info"
profiles:Sun Ray Users> end
profiles:Sun Ray Users> exit
```

例 3-23 ユーザー自身からの基本特権の削除

次の例では、通常のユーザーが .bash_profile を変更して proc_info 基本特権を削除します。ps や prstat などのプログラムの出力にはユーザー自身のプロセスだけが含まれており、有用な情報を示していることがあります。

```
##  .bash_profile
## Remove proc_info privilege from my shell
##
ppriv -s EI-proc_info $$
```

ppriv 行は、現在のシェルプロセス ($$) でユーザーの有効特権セットと継承可能特権セット (EI-) から proc_info 特権を削除します。

次の prstat 出力では、プロセスの合計が 74 から 3 に減少しています。

```
## With all basic privileges
Total: 74 processes, 527 lwps, load averages: 0.01, 0.00, 0.00

## With proc_info removed from the effective and inheritable set
Total: 3 processes, 3 lwps, load averages: 0.00, 0.00, 0.00
```

例 3-24 システムをそのユーザーが使用できる権限を制限するように変更する

この例では、管理者がネットワークの管理にのみ役立つシステムを作成します。管理者は、policy.conf ファイルから Basic Solaris User 権利プロファイルとすべての承認を削除します。Console User 権利プロファイルは削除されません。結果となる policy.conf ファイルで影響を受けた行は次のとおりです。

```
...
##AUTHS_GRANTED=
##AUTH_PROFS_GRANTED=
##PROFS_GRANTED=Basic Solaris User
CONSOLE_USER=Console User
...
```

承認、コマンド、または権利プロファイルが明示的に割り当てられているユーザーのみがこのシステムを使用できます。ログイン後、その承認ユーザーは管理責務を果たすことができます。承認されたユーザーがシステムコンソールの前に座っている場合、そのユーザーには Console User の権利があります。

例 3-25 明示的に割り当てられた権利への管理者の制限

2 つの方法で、ユーザーまたは役割を限られた数の管理操作に制限できます。

- ユーザーのプロファイルリストの最終プロファイルとして、Stop 権利プロファイルを割り当てます。

  Stop 権利プロファイルは、制限付きシェルを作成するもっとも簡単な方法です。`policy.conf` ファイル内の承認と権利プロファイルは、ユーザーまたは役割には割り当てられません。
- システム上の `policy.conf` ファイルを変更して、役割またはユーザーがそのシステムを管理タスクに使用するよう要求します。例3-24「システムをそのユーザーが使用できる権限を制限するように変更する」を参照してください。

次のコマンドは、`auditrev` 役割を監査レビューの実行のみに制限します。

```
# rolemod -P "Audit Review,Stop" auditrev
```

`auditrev` 役割には Console User 権利プロファイルがないため、監査担当者はシステムをシャットダウンできません。この役割には `solaris.device.cdrw` 承認がないため、監査担当者は CD-ROM ドライブに対して読み取りまたは書き込みを行うことができません。この役割には Basic Solaris User 権利プロファイルがないため、そのプロファイルのコマンドをこの役割で実行できません。All 権利プロファイルが割り当てられていないため、`ls` コマンドは実行されません。この役割は、ファイルブラウザを使用してレビューする監査ファイルを選択します。

詳細は、38 ページの「割り当てられた権利の検索順序」および119 ページの「権利プロファイルのリファレンス」を参照してください。

例 3-26 選択したアプリケーションによる新規プロセス生成の防止

この例では、適切な動作のためにサブプロセスが不要なアプリケーションの権利プロファイルを管理者が作成します。便宜上、管理者はこれらの実行可能ファイルを保管するディレクトリを作成します。サブプロセスを必要としない新しいアプリケーションが追加されたら、実行可能ファイルをこのディレクトリに追加できます。あるいは、実行可能ファイルが特定のディレクトリに存在

している必要がある場合、管理者は /opt/local/noex/*app-executable* からそれにリンクできます。

```
# profiles -p "Prevent App Subprocess"
profiles:Prevent App Subprocess> set desc="Keep apps from execing processes"
profiles:Prevent App Subprocess> add cmd=/opt/local/noex/mkmod
... Subprocess:mkmod> set limitprivs=all,!proc_exec
... Subprocess:mkmod> end
... Subprocess> add cmd=/opt/local/noex/gomap
... Subprocess:gomap> set limitprivs=all,!proc_exec
... Subprocess:gomap> end
... Subprocess> commit
... Subprocess> exit
```

例 3-27 ゲストによるエディタサブプロセス生成の防止

この例では、管理者がエディタコマンドから proc_exec 基本特権を削除して、ユーザーが 1 つまたは複数のエディタからサブシェルを作成することを防止します。

1. 管理者は、vim エディタの制限特権セットから proc_exec を削除する権利プロファイルを作成します。

   ```
   # profiles -p -S ldap "Editor Restrictions"
   profiles:Editor Restrictions> set desc="Site Editor Restrictions"
   ... Restrictions> add cmd=/usr/bin/vim
   ... Restrictions:vim> set limitprivs=all,!proc_exec
   ... Restrictions:vim> end
   ... Restrictions> commit
   ... Restrictions> exit
   ```

2. 管理者がほかの一般的なエディタを権利プロファイルに追加します。

   ```
   # profiles -p "Editor Restrictions"
   profiles:Editor Restrictions> add cmd=/usr/bin/gedit
   ... Restrictions:gedit> set limitprivs=all,!proc_exec
   ... Restrictions:gedit> end
   ... Restrictions> add cmd=/usr/bin/gconf-editor
   ... Restrictions:gconf-editor> set limitprivs=all,!proc_exec
   ... Restrictions:gconf-editor> end
   ... Restrictions> add cmd=/usr/bin/ed
   ... Restrictions:ed> set limitprivs=all,!proc_exec
   ... Restrictions:ed> end
   ```

```
... Restrictions> add cmd=/usr/bin/ex
... Restrictions:ex> set limitprivs=all,!proc_exec
... Restrictions:ex> end
... Restrictions> add cmd=/usr/bin/edit
... Restrictions:edit> set limitprivs=all,!proc_exec
... Restrictions:edit> end
... Restrictions> commit
... Restrictions> exit
```

3. 管理者は、権利プロファイルのエントリに誤字、脱字、繰り返しなどのエラーがないかどうかを確認します。

```
# profiles -p "Editor Restrictions" info
Found profile in files repository.
name=Editor Restrictions
desc=Site Editor Restrictions
cmd=/usr/bin/vim
limitprivs=all,!proc_exec
...
```

4. 管理者は Editor Restrictions 権利プロファイルを guest ユーザーに割り当てます。

```
# usermod -K profiles+="Editor Restrictions" guest
```

管理者は profiles+ を使用して、この権利プロファイルをアカウントの現在の権利プロファイルに追加します。

5. エディタ特権が制限されていることを確認するため、管理者はエディタを開き、別のウィンドウでエディタプロセスの特権を調べます。

```
# ppriv -S $(pgrep vi)
2805:   vi .bash_profile
flags = PRIV_PFEXEC      User is running a profile shell
        E: basic,!proc_info      proc_info is removed from basic set
        I: basic,!proc_info
        P: basic,!proc_info
        L: all,!proc_exec      proc_exec is removed from limit set
```

例 3-28 全ユーザーへの Editor Restrictions 権利プロファイルの割り当て

この例では、管理者が Editor Restrictions 権利プロファイルを `policy.conf` ファイルに追加します。管理者は、ゲストがログインできるパブリックシステムにこのファイルが配布されていることを確認します。

```
# cd /etc/security; cp policy.conf policy.conf.orig
# pfedit /etc/security/policy.conf
...
AUTHS_GRANTED=
AUTH_PROFS_GRANTED=
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=Editor Restrictions,Basic Solaris User
```

User Security 管理者により各ユーザーにプロファイルシェルが割り当てられています。理由と手順については、47 ページの「ユーザーへの権利の割り当て」を参照してください。

♦ ♦ ♦ 第 4 章

4 アプリケーション、スクリプト、およびリソースへの権利の割り当て

この章では、特権、拡張特権ポリシー、およびその他の権利をユーザー、ポート、およびアプリケーションに適用するタスクについて説明します。

権利の概要については、14 ページの「ユーザー権管理」を参照してください。

アプリケーション、スクリプトおよびリソースの特定の権利への制限

このセクションのタスクと例では、実行可能ファイルとシステムリソースに特権を割り当てます。通常、信頼できるユーザーが実行可能ファイルを実行できるようにする目的で、特権を実行可能ファイルに割り当てます。69 ページの「アプリケーションおよびスクリプトへの権利の割り当て」では、特権割り当てによって、プロファイルシェル内で信頼できるユーザーがアプリケーションまたはスクリプトを実行できるようになります。72 ページの「拡張特権を使用したリソースのロックダウン」では、拡張特権によって、ユーザー ID、ポート、またはファイルオブジェクトが、デフォルトの有効セットよりも小さな特権セットに制限されます。未指定の特権は、ユーザーのプロセス、ポート、またはオブジェクトに対して拒否されます。この割り当ては、最小特権ポリシーに近いものです。

アプリケーションおよびスクリプトへの権利の割り当て

アプリケーションとスクリプトは 1 つのコマンドまたは一連のコマンドを実行します。権利を割り当てるには、権利プロファイル内の各コマンドに対し、セット ID や特権などのセキュリティー属性を設定します。必要に応じて、アプリケーションは承認を確認できます。

注記 - スクリプトのコマンドで、正常な実行のために `setuid` ビットまたは `setgid` ビットセットを持つ必要がある場合、実行可能なスクリプト*および*コマンドに対して、権利プロファイルでセキュリティー属性を追加する必要があります。スクリプトがプロファイルシェルで実行されると、セキュリティー属性を使用してコマンドが実行されます。

- 権利を必要とするスクリプトを実行する – 70 ページの「特権付きのコマンドを含むシェルスクリプトの実行方法」
- `root` 以外のユーザーが特権認識アプリケーションを実行できるようにする – 例4-1「レガシーアプリケーションへのセキュリティー属性の割り当て」
- `root` 以外のユーザーが、`root` が所有するアプリケーションを実行できるようにする – 例4-2「割り当てられた権利でのアプリケーションの実行」
- スクリプト内で承認を確認する – 例4-3「スクリプトまたはプログラム内の承認の確認」

▼ 特権付きのコマンドを含むシェルスクリプトの実行方法

特権シェルスクリプトを実行するには、そのスクリプトとスクリプト内のコマンドに特権を追加します。このため、該当する権利プロファイルには、特権が割り当てられているコマンドが含まれている必要があります。

始める前に `root` 役割になる必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **1 行目に `/bin/pfsh` またはほかのプロファイルシェルが指定されているスクリプトを作成します。**

```
#!/bin/pfsh
# Copyright (c) 2013 by Oracle
```

2. **通常のユーザーとして、スクリプト内のコマンドに必要な特権を判断します。**

   特権なしでスクリプトを実行すると、`ppriv` コマンドの `debug` オプションにより不足している特権が一覧表示されます。

```
% ppriv -eD script-full-path
```

   詳細は、115 ページの「プログラムが必要とする特権を判断する方法」を参照してください。

3. **スクリプトの権利プロファイルを作成または変更します。**

シェルスクリプトとそのシェルスクリプトに含まれるコマンドを、それらの必要なセキュリティー属性とともに権利プロファイルに追加します。89 ページの「権利プロファイルを作成する方法」を参照してください。

4. **信頼できるユーザーまたは役割に権利プロファイルを割り当てます。**
   例については、47 ページの「ユーザーへの権利の割り当て」を参照してください。

5. **スクリプトを実行するには、次のいずれかを行います。**

   - **ユーザーとしてスクリプトが割り当てられている場合、プロファイルシェルを開いてスクリプトを実行します。**

     ```
     % pfexec script-full-path
     ```

   - **役割としてスクリプトが割り当てられている場合、役割を引き受けてスクリプトを実行します。**

     ```
      % su - rolename
     Password: xxxxxxxx
     # script-full-path
     ```

例 4-1 レガシーアプリケーションへのセキュリティー属性の割り当て

レガシーアプリケーションは特権を認識しないため、管理者は権利プロファイル内のアプリケーション実行可能ファイルにセキュリティー属性 `euid=0` を割り当てます。次に、管理者はそれを信頼できるユーザーに割り当てます。

```
# profiles -p LegacyApp
profiles:LegacyApp> set desc="Legacy application"
profiles:LegacyApp> add cmd=/opt/legacy-app/bin/legacy-cmd
profiles:LegacyApp:legacy-cmd> set euid=0
profiles:LegacyApp:legacy-cmd> end
profiles:LegacyApp> exit
# profiles -p LegacyApp 'select cmd=/opt/legacy-app/bin/legacy-cmd;info;end'
 id=/opt/legacy-app/bin/legacy-cmd
 euid=0

# usermod -K profiles+="Legacy application" jdoe
```

例 4-2 割り当てられた権利でのアプリケーションの実行

この例では、管理者は 例5-7「特権付きコマンドを含む権利プロファイルの作成」の権利プロファイルを信頼できるユーザーに割り当てます。ユーザーはスクリプトの実行時にパスワードを入力する必要があります。

```
# usermod -K auth_profiles+="Site application" jdoe
```

例 4-3 スクリプトまたはプログラム内の承認の確認

承認を確認するには、auths コマンドに基づくテストを作成します。このコマンドの詳細については、auths(1) のマニュアルページを参照してください。

たとえば、次の行では、$1 引数に指定した承認がユーザーに与えられているかどうかをテストします。

```
if [ `/usr/bin/auths|/usr/xpg4/bin/grep $1` ]; then
        echo Auth granted
else
        echo Auth denied
fi
```

より完全なテストには、ワイルドカードの使用を確認するロジックが含まれています。たとえば、solaris.system.date 承認がユーザーにあるかどうかをテストするには、次の文字列を確認する必要があります。

- solaris.system.date
- solaris.system.*
- solaris.*

プログラムを作成している場合は、getauthattr() 関数を使用して、承認をテストします。

拡張特権を使用したリソースのロックダウン

拡張特権ポリシーは、アプリケーションに対する攻撃が成功した場合のシステムへの攻撃者のアクセスを制限します。拡張ポリシールールは、特権割り当ての影響の範囲を、ルール内のリソースだけに制限します。拡張ポリシールールを記述するには、特権を中括弧で囲み、その後にコロンと関連付けられたリソースを記述します。詳細は、33 ページの「ユーザーまたは役割の特権の拡張」を参照してください。構文の例については、ppriv(1) および privileges(5) のマニュアルページを参照してください。

管理者と通常のユーザーはいずれも、拡張特権を使用してリソースをロックダウンできます。管理者はユーザー、ポート、およびアプリケーションに対する拡張特権ルールを作成できます。通常のユーザーはコマンド行を使用するか、または ppriv -r コマンドを使用するスクリプトを作成して、アプリケーションによるユーザー指定ディレクトリ外部のファイルへの書き込みを防止できます。

- ポートから侵入する悪意のあるユーザーが使用できるアクセスを制限する – 73 ページの「ポートに拡張特権ポリシーを適用する方法」
- 非 root デーモンとしてデータベースを実行する – 74 ページの「MySQL サービスをロックダウンする方法」
- 非 root デーモンとして Apache Web サーバーを実行する – 77 ページの「特定の特権を Apache Web サーバーに割り当てる方法」
- Apache Web サーバーが特権を使用して実行されていることを確認する – 78 ページの「Apache Web Server が使用している特権を判断する方法」
- Firefox によるシステムのディレクトリへの書き込みを防止する – 例4-4「保護されている環境でのブラウザの実行」
- アプリケーションをシステムの特定のディレクトリに制限する – 例4-5「アプリケーションプロセスからのシステム上のディレクトリの保護」

▼ ポートに拡張特権ポリシーを適用する方法

Network Time Protocol (NTP) のサービスは、udp トラフィックに対して特権ポート 123 を使用します。このサービスを実行するには特権が必要です。この例の手順では、ほかのポートを保護し、このポートに割り当てられている特権を取得した悪意のあるユーザーがアクセスできないように、サービスマニフェストを変更します。

始める前に root 役割になる必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **ポートのデフォルトのサービスマニフェストエントリを参照します。**

   次の /lib/svc/manifest/network/ntp.xml start メソッドエントリでは、net_privaddr、proc_lock_memory、および sys_time 特権をほかのプロセスで使用できます。

   ```
   privileges='basic,!file_link_any,!proc_info,!proc_session,net_privaddr,
   proc_lock_memory,sys_time'
   ```

   !file_link_any,!proc_info,!proc_session に指定されている削除された特権が原因で、サービスは、その他のプロセスに対するシグナル送信または監視と、ファイル名を変更する方法としてのハードリンクの作成を実行できません。つまり、このサービスによって起動されたプロセスは NTP のポート 123 にしかバインドできず、ほかのどの特権ポートにもバインドできません。

ハッカーがこのサービスを悪用してほかのプロセスを開始できる可能性がある場合、そのプロセスも同様に制限されます。

2. **start メソッドと restart メソッドを変更して、net_privaddr 特権をこのポートのみに制限します。**

```
# svccfg -s ntp editprop
```

   a. **文字列 net_privaddr を検索します。**

   b. **net_privaddr が含まれているエントリのコメントを解除します。**

   c. **両方のエントリで net_privaddr を {net_privaddr}:123/udp に置き換えます。**

      拡張特権ポリシーにより、指定されている特権と未指定の基本特権を除くすべての特権がこのサービスから削除されます。このため、80 を超える悪用される可能性がある特権が、8 個未満に減少します。

3. **拡張特権ポリシーを使用するため、サービスを再起動します。**

```
# svcadm restart ntp
```

4. **サービスが拡張特権を使用していることを確認します。**

```
# svccfg -s ntp listprop | grep privileges
start/privileges    astring  basic,!file_link_any,!proc_info,!proc_session,
                    {net_privaddr}:123/udp,proc_lock_memory,sys_time
restart/privileges  astring  basic,!file_link_any,!proc_info,!proc_session,
                    {net_privaddr}:123/udp,proc_lock_memory,sys_time
```

▼ MySQL サービスをロックダウンする方法

インストール時に、MySQL データベースは保護されていないポート上で root のフル特権で実行されるように構成されます。このタスクでは、権利プロファイルで MySQL サービスに拡張特権ポリシーを割り当てます。権利プロファイルがサービスの exec メソッドになったあとで、MySQL は保護されているポート上で、MySQL 以外のプロセスによるデータベースアクセスを制限した状態でユーザー mysql として実行されます。

始める前に 初期ユーザーはパッケージをインストールできます。残りのステップは root 役割が実行する必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **MySQL パッケージをインストールします。**

```
# pkg search basename:mysql
...
basename ... pkg:/database/mysql-51@version
# pfexec pkg install mysql-51
```

注記 - バージョン 5.5 の MySQL データベースIにアップグレードする場合は、すべてのステップを、5.1 および 51 ではなく 5.5 および 55 を使用するように変更します。

2. **MySQL サービスの状態と FMRI を表示します。**

```
# svcs mysql
STATE          STIME    FMRI
disabled       May_15   svc:/application/database/mysql:version_51
```

3. **サービスの実行メソッドを変更する権利プロファイルを作成します。**

このサービスのサービスマニフェストは、実行メソッドがシェルスクリプトラッパー /lib/svc/method/mysql_51 であることを指定します。

```
# svccfg -s mysql listprop | grep manifest
... astring     /lib/svc/manifest/application/database/mysql_51.xml
# grep exec= /lib/svc/manifest/application/database/mysql_51.xml
                exec='/lib/svc/method/mysql_51 start'
                exec='/lib/svc/method/mysql_51 stop'
```

プロファイルのコマンドに /lib/svc/method/mysql_51 ラッパーを使用します。

```
% su -
Password: xxxxxxxx
# profiles -p "MySQL Service"
MySQL Service> set desc="Locking down the MySQL Service"
MySQL Service> add cmd=/lib/svc/method/mysql_51
MySQL Service:mysql_51> set privs=basic
MySQL Service:mysql_51> add privs={net_privaddr}:3306/tcp
MySQL Service:mysql_51> add privs={file_write}:/var/mysql/5.1/data/*
MySQL Service:mysql_51> add privs={file_write}:/tmp/mysql.sock
MySQL Service:mysql_51> add privs={file_write}:/var/tmp/ib*
MySQL Service:mysql_51> end
MySQL Service> set uid=mysql
MySQL Service> set gid=mysql
MySQL Service> exit
```

file_write 特権は、デフォルトですべてのプロセスに付与されている基本特権です。書き込み可能パスを明示的に列挙することで、書き込みアクセスがそれらのパスだけに制限されます。この制約は、指定されている実行可能ファイルとその子プロセスに適用されます。

4. **MySQL のデフォルトポートを特権ポートにします。**

```
# ipadm set-prop -p extra_priv_ports+=3306 tcp
# ipadm show-prop -p extra_priv_ports tcp
PROTO PROPERTY            PERM CURRENT     PERSISTENT   DEFAULT    POSSIBLE
tcp   extra_priv_ports    rw   2049,4045,  3306         2049,4045  1-65535
                                 3306
```

特権ポートにバインドするには net_privaddr 特権が必要です。MySQL の場合、デフォルトポート番号 3306 へのバインディングでは、通常はこの権限は不要です。

5. **権利プロファイルを MySQL サービスに割り当て、サービスに対してそれを使用するように指示します。**

```
# svccfg -s mysql:version_51
...version_51> setprop method_context/profile="MySQLService"
...version_51> setprop method_context/use_profile=true
...version_51> refresh
...version_51> exit
```

6. **サービスを有効にします。**

このサービスを一意に指定するには、FMRI の最後のコンポーネント mysql:version_51 で十分です。

```
# svcadm enable mysql:version_5
```

7. **(オプション) MySQL Service 権利プロファイルに指定されている権利を使用してサービスが実行されていることを確認します。**

```
# ppriv $(pgrep mysql)
103697:   /usr/mysql/5.1/bin/mysqld --basedir=/usr/mysql/5.1
                                    --datadir=/var/mysql/5.1/data
flags =   PRIV_XPOLICY
    Extended policies:
             {net_privaddr}:3306/tcp
             {file_write}:/var/mysql/5.1/data/*
             {file_write}:/tmp/mysql.sock
             {file_write}:/var/tmp/ib*
        E: basic,!file_write
        I: basic,!file_write
        P: basic,!file_write
        L: all
103609:  /bin/sh /usr/mysql/5.1/bin/mysqld_safe --user=mysql
                                --datadir=/var/mysql/5.1/data
flags =  PRIV_XPOLICY
    Extended policies:
             {net_privaddr}:3306/tcp
             {file_write}:/var/mysql/5.1/data/*
             {file_write}:/tmp/mysql.sock
             {file_write}:/var/tmp/ib*
        E: basic,!file_write
```

```
I: basic,!file_write
P: basic,!file_write
L: all
```

▼ 特定の特権を Apache Web サーバーに割り当てる方法

この手順では、必要な特権のみを Web サーバーデーモンに割り当てることで、その Web サーバーデーモンをロックダウンします。Web サーバーはポート 80 だけにバインドでき、また webservd デーモンが所有するファイルだけに書き込むことができます。root として実行される apache22 サービスプロセスはありません。

始める前に root 役割になる必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **Web サーバー権利プロファイルを作成します。**

```
# profiles -p "Apache2"
profiles:Apache2> set desc="Apache Web Server Extended Privilege"
profiles:Apache2> add cmd=/lib/svc/method/http-apache22
profiles:Apache2:http-apache22> add privs={net_privaddr}:80/tcp
...http-apache22> add privs={zone}:/system/volatile/apache2
...http-apache22> add privs={zone}:/var/apache2/2.2/logs/*
...http-apache22> add privs={zone}:/var/user
...http-apache22> add privs={file_write}:/var/user/webserv*
...http-apache22> add privs={file_write}:/tmp/*
...http-apache22> add privs={file_write}:/system/volatile/apache*
...http-apache22> add privs={file_write}:/proc/*
...http-apache22> add privs=basic,proc_priocntl
...http-apache22> set uid=webservd
...http-apache22> set gid=webservd
...http-apache22> end
---Apache2> exit
```

2. **(オプション) Apach2 で SSL カーネルプロキシを使用する場合、webservd 拡張ポリシーに SSL ポートを追加する必要があります。**

```
# profiles -p "Apache2"
profiles:Apache2> add privs={net_privaddr}:443/tcp
profiles:Apache2> add privs={net_privaddr}:8443/tcp
profiles:Apache2:http-apache22> end
```

SSL カーネルプロキシの手順については、『Oracle Solaris 11.2 でのネットワークのセキュリティー保護 』の「SSL カーネルプロキシ を使用するように Apache 2.2 Web サーバーを構成する方法」に説明されています。

3. **apache22 SMF 起動メソッドに権利プロファイルを追加します。**

```
# svccfg -s apache22
svc:/network/http:Apache2> listprop start/exec
start/exec  astring "/lib/svc/method/http-apache22 start"
...
svc:/network/http:Apache2> setprop start/profile="Apache2"
svc:/network/http:Apache2> setprop start/use_profile=true
svc:/network/http:Apache2> refresh
svc:/network/http:Apache2> exit
```

apache22 サービスが有効化されると、Apache2 プロファイルが使用されます。

4. **apache22 サービスを有効にします。**

```
# svcadm enable apache22
```

5. **Web サーバーが機能していることを確認します。**

ブラウザを開き、Firefox の URL フィールドに localhost と入力します。

次の手順 特権が正しく適用されていることを確認するため、78 ページの「Apache Web Server が使用している特権を判断する方法」に進みます。

▼ Apache Web Server が使用している特権を判断する方法

このタスクでは、Apache2 権利プロファイルのデバッグバージョンを作成して、Web サーバーが使用している特権を判断します。

始める前に 77 ページの「特定の特権を Apache Web サーバーに割り当てる方法」を完了しています。apache22 サービスが無効になっています。root に含まれています。

1. **別のコマンドを呼び出すため、Apache2 プロファイルをクローニングします。**

コマンドのデバッグは、SMF サービスのデバッグよりも単純です。apachectl コマンドは、Apache サービスを対話式に起動します。

```
# profiles -p "Apache2"
profiles:Apache2> set name="Apache-debug"
profiles:Apache-debug> sel <Tab><Tab>
profiles:Apache-debug:http-apache22> set id=/usr/apache2/2.2/bin/apachectl
profiles:Apache-debug:apachectl> end
profiles:Apache-debug> exit
```

詳細は、apachectl(8) のマニュアルページを参照してください。

2. **クローニングしたプロファイルを webservd アカウントに割り当てます。**

```
# usermod -K profiles+=Apache-debug webservd
```

3. **webservd 識別情報に切り替えます。**

```
# su - webservd
```

4. **(オプション) この識別情報を検証します。**

```
# id
uid=80(webservd) gid=80(webservd)
```

5. **プロファイルシェルで、Web サービスをデバッグモードで起動します。**
   SMF を直接使用しないでください。Apache-debug 権利プロファイルのコマンドを使用します。

```
% pfbash
# ppriv -De /usr/apache2/2.2/bin/apachectl start
```

6. **root 役割で、最初の http デーモンの特権を調べます。**

```
# ppriv $(pgrep httpd|head -1)
2999:   httpd
flags = PRIV_DEBUG|PRIV_XPOLICY|PRIV_EXEC
  5         Extended policies:
  6                 {net_privaddr}:80/tcp
  7                 {zone}:/system/volatile/apache2
  8                 {zone}:/var/apache2/2.2/logs/*
  9                 {zone}:/var/user
 10                 {file_write}:/var/user/webserv*
 11                 {file_write}:/tmp/*
 12                 {file_write}:/system/volatile/apache*
 13                 {file_write}:/proc/*
 14         E: basic,!file_write,!proc_info,proc_priocntl
 15         I: basic,!file_write,!proc_info,proc_priocntl
 16         P: basic,!file_write,!proc_info,proc_priocntl
 17         L: all
```

ユーザーによる自身が実行しているアプリケーションのロックダウン

ユーザーは、拡張特権ポリシーを使用してアプリケーションから基本特権を削除できます。このポリシーは、アプリケーションがアクセスすべきではないディレクトリへのアクセスを防ぎます。

注記 - 順序は重要です。ほとんどの$HOME/.* ディレクトリに対して限定的な特権を割り当てたあとで、$HOME/Download* などのディレクトリに対してより広範な特権を割り当てる必要があります。

例 4-4 保護されている環境でのブラウザの実行

この例では、保護されている環境でユーザーが Firefox ブラウザを実行できる方法を示します。この構成では、ユーザーの Documents ディレクトリが Firefox では非表示になります。

ユーザーは次のコマンドを使用して、/usr/bin/firefox コマンドから基本特権を削除します。ppriv -r コマンドの拡張特権引数は、ブラウザによる読み取りと書き込みを、ユーザーが指定したディレクトリに制限します。-e オプションとその引数により、拡張特権ポリシーを使用してブラウザが開かれます。

```
% ppriv -r "\
{file_read}:/dev/*,\
{file_read}:/etc/*,\
{file_read}:/lib/*,\
{file_read}:/usr/*,\
{file_read}:/var/*,\
{file_read}:/proc,\
{file_read}:/proc/*,\
{file_read}:/system/volatile/*,\
{file_write}:$HOME,\
{file_read}:$HOME/.*,\
{file_read,file_write}:$HOME/.mozill*,\
{file_read,file_write}:$HOME/.gnome*,\
{file_read,file_write}:$HOME/Downloa*,\
{file_read,file_write}:/tmp,\
{file_read,file_write}:/tmp/*,\
{file_read,file_write}:/var/tmp,\
{file_read,file_write}:/var/tmp/*,\
{proc_exec}:/usr/*\
" -e /usr/bin/firefox file:///$HOME/Desktop
```

拡張ポリシーで file_read および file_write 特権が使用されている場合は、読み取りまたは書き込みが必要なすべてのファイルに対する明示的なアクセス権を付与する必要があります。このようなポリシーではワイルドカード文字 * を使用する必要があります。

自動マウントされたホームディレクトリを操作するため、ユーザーが次の例のように自動マウントパスの明示的なエントリを追加することがあります。

```
{file_read,file_write}:/export/home/$USER
```

サイトで automount 機能が使用されていない場合は、保護ディレクトリの最初のリストで十分です。

ユーザーはシェルスクリプトを作成して、このコマンド行保護ブラウザを自動化できます。その後ブラウザを起動するには、ユーザーは /usr/bin/firefox コマンドではなくスクリプトを呼び出します。

例 4-5 アプリケーションプロセスからのシステム上のディレクトリの保護

この例では、通常のユーザーがシェルスクリプトラッパーを使用してアプリケーションのサンドボックスを作成します。このスクリプトの前半では、アプリケーションが特定のディレクトリに制限されます。Firefox などの例外の処理は、このスクリプトの後半で行われます。スクリプトの後に、スクリプトの各部分に関するコメントを示します。

```
1 #!/bin/bash
2
3 # Using bash because ksh misinterprets extended policy syntax
4
5 PATH=/usr/bin:/usr/sbin:/usr/gnu/bin
6
7 DENY=file_read,file_write,proc_exec,proc_info
8
9 SANDBOX="\
10 {file_read}:/dev/*,\
11 {file_read}:/etc/*,\
12 {file_read}:/lib/*,\
13 {file_read,file_write}:/usr/*,\
14 {file_read}:/proc,\
15 {file_read,file_write}:/proc/*,\
16 {file_read}:/system/volatile/*,\
17 {file_read,file_write}:/tmp,\
18 {file_read,file_write}:/tmp/*,\
19 {file_read,file_write}:/var/*,\
20 {file_write}:$HOME,\
21 {file_read}:$HOME/.*,\
22 {file_read,file_write}:$PWD,\
23 {file_read,file_write}:$PWD/*,\
24 {proc_exec}:/usr/*\
25 "
26
27 # Default program is restricted bash shell
28
29 if [[ ! -n $1 ]]; then
30     program="/usr/bin/bash --login --noprofile
       --restricted"
31 else
32     program="$@"
33 fi
34
35
36 # Firefox needs more file and network access
37 if [[ "$program" =~ firefox ]]; then
38     SANDBOX+=",\
39 {file_read,file_write}:$HOME/.gnome*,\
40 {file_read,file_write}:$HOME/.mozill*,\
41 {file_read,file_write}:$HOME/.dbu*,\
42 {file_read,file_write}:$HOME/.puls*\
43 "
```

```
44
45 else
46     DENY+=",net_access"
47 fi
48
49 echo Starting $program in sandbox
50 ppriv -s I-$DENY -r $SANDBOX -De $program
```

ポリシーを調整して、特定のアプリケーションに対して許可するアクセス権を増やすかまたは減らすことができます。行 38 から 42 での調整では、Firefox に対し、ユーザーのホームディレクトリ内のセッション情報を保持するドットファイルへの書き込みアクセスが付与されています。また Firefox は、ネットワークアクセスを削除する行 46 の対象ではありません。ただし Firefox は、ユーザーのホームディレクトリ内の任意のファイルの読み取りが制限されており、現行ディレクトリにのみファイルを保存できます。

保護を強化するため、行 30 でデフォルトプログラムが制限付き Bash シェルになっています。制限付きシェルは、その現行ディレクトリを変更したり、ユーザーのドットファイルを実行したりすることはできません。したがって、このシェルから開始するすべてのコマンドは同様にサンドボックスにロックされます。

スクリプトの最後の行で、`ppriv` コマンドに 2 つの特権セット `$DENY` および `$SANDBOX` がシェル変数として渡されます。

最初のセットである `$DENY` は、プロセスに対し、ファイルの読み取りと書き込み、サブプロセスの実行、ほかのユーザーのプロセスの監視、および (条件付きでの) ネットワークへのアクセスを禁止します。これらの制限は非常に厳しいため、2 番目のセットである `$SANDBOX` で、読み取り、書き込み、および実行が可能なディレクトリを列挙することでこのポリシーが調整されています。

また行 50 ではデバッグオプション `-D` が指定されています。アクセス失敗は端末ウィンドウにリアルタイムで表示され、これには名前付きオブジェクトと、正常な実行に必要な該当する特権が含まれています。このデバッグ情報は、ユーザーがほかのアプリケーション向けにポリシーをカスタマイズする際に役立ちます。

♦ ♦ ♦ 第 5 章

5 権利使用の管理

この章では、管理に権利モデルを使用するシステムを保守するタスクについて説明します。いくつかのタスクでは、新しい権利プロファイルと承認を作成することで、Oracle Solaris が提供する権利を拡張します。

この章の内容は次のとおりです。

権利の詳細については、第1章「権利を使用したユーザーとプロセスの制御について」を参照してください。ユーザーと役割に割り当てられた権利の保守については、第3章「Oracle Solaris での権利の割り当て」を参照してください。

権利使用の管理

このセクションのタスクと例では、割り当てられた権利を使用する方法と、デフォルトで提供される権利構成を変更する方法について説明します。

注記 - トラブルシューティングの詳細については、109 ページの「権利に関するトラブルシューティング」を参照してください。

- 割り当てられた権利を使用する – 84 ページの「割り当てられている管理権利の使用」
- 管理アクションを監査する – 例5-5「2 つの役割を使用した監査の構成」
- 権利プロファイルと承認を追加する – 89 ページの「権利プロファイルと承認の作成」
- root をユーザーとして構成する – 96 ページの「root 役割をユーザーに変更する方法」
- root を役割に再度変更する – 例5-12「root ユーザーを root 役割に変更する」

- root によるシステムの管理を阻止する – 例5-13「システム保守での root 役割の使用の防止」

割り当てられている管理権利の使用

root 役割では、初期ユーザーにすべての管理権限が与えられます。このユーザーは root として、役割、権利プロファイル、または特定の権限などの管理権利と承認を、信頼できるユーザーに割り当てることができます。このセクションでは、このようなユーザーが各自に割り当てられている権利を使用する方法を説明します。

注記 - Oracle Solaris には管理ファイル用の特殊なエディタがあります。管理ファイルを編集するときには pfedit コマンドを使用します。例5-1「システムファイルの編集」に、root 以外のユーザーが指定されたシステムファイルを編集できるようにする方法を示します。

管理タスクを実行するには、端末ウィンドウを開いて次のオプションのいずれかを選択します。

- sudo を使用する場合は、sudo コマンドを入力します。

  sudo コマンドを使い慣れている管理者の場合は、sudoers ファイルで管理者に割り当てられている管理コマンドの名前を使用してこのコマンドを実行します。詳細は、sudo(1M) および sudoers(4) のマニュアルページを参照してください。
- タスクにスーパーユーザー特権が必要な場合は、root になります。

```
% su -
Password: xxxxxxxx
#
```

注記 - このコマンドは、root がユーザーまたは役割のいずれであっても機能します。ポンド記号 (#) のプロンプトは、ユーザーが現在 root であることを示します。

- タスクが役割に割り当てられている場合、そのタスクを実行できる役割を引き受けます。

  次の例では、監査構成の役割になります。この役割には、Audit Configuration 権利プロファイルが含まれています。管理者からこの役割のパスワードを受け取っています。

```
% su - audadmin
Password: xxxxxxxx
#
```

ヒント - 役割のパスワードを受け取っていない場合は、管理者が、ユーザーのパスワードを求めるように役割を構成しています。役割を引き受けるには、ユーザーパスワードを入力します。このオプションの詳細については、例3-16「役割パスワードでのユーザー独自のパスワード使用の有効化」を参照してください。

このコマンドを入力したシェルは、プロファイルシェルになりました。このシェルでは、auditconfig コマンドを実行できます。プロファイルシェルの詳細については、37 ページの「プロファイルシェルと権利の検証」を参照してください。

ヒント - 役割の権利を表示するには、101 ページの「権利プロファイルの一覧表示」を参照してください。

- ユーザーとしてタスクが直接割り当てられている場合は、次のいずれかの方法でプロファイルシェルを作成します。
  - pfbash コマンドを使用して、管理権利を評価するシェルを作成します。

    次の例では、Audit Configuration 権利プロファイルがユーザーに直接割り当てられています。次のコマンドセットにより、pfbash プロファイルシェルで監査事前選択値と監査ポリシーを表示できます。

    ```
    % pfbash
    # auditconfig -getflags
    active user default audit flags = ua,ap,lo(0x45000,0x45000)
    configured user default audit flags = ua,ap,lo(0x45000,0x45000)
    # auditconfig -getpolicy
    configured audit policies = cnt
    active audit policies = cnt
    ```

  - 1 つの管理コマンドを実行するには、pfexec コマンドを使用します。

    次の例では、Audit Configuration 権利プロファイルが認証権利プロファイルとしてユーザーに直接割り当てられています。特権付きコマンドの名前を指定した pfexec コマンドを使用して、このプロファイルからその特権付きコマンドを実行できます。たとえば、ユーザーの事前選択監査フラグを表示できます。

    ```
    % pfexec auditconfig -getflags
    ```

```
Enter password:       Type your user password
active user default audit flags = ua,ap,lo(0x45000,0x45000)
configured user default audit flags = ua,ap,lo(0x45000,0x45000)
```

一般に、権利に含まれている別の特権付きコマンドを実行するには、その特権付きコマンドを入力する前に、pfexec を再度入力する必要があります。詳細は、pfexec(1) のマニュアルページを参照してください。パスワードキャッシュを使用して構成されている場合は、例5-2「役割の使用を容易にするために認証をキャッシュする」に示すように、構成可能な期間内ではパスワードを入力せずに後続のコマンドを実行できます。

例 5-1 システムファイルの編集

0 の UID を持つ root でない場合は、デフォルトでは、システムファイルを編集できません。ただし、solaris.admin.edit/*path-to-system-file* 承認が割り当てられている場合は、*system-file* を編集できます。たとえば solaris.admin.edit/etc/security/audit_warn 承認が割り当てられている場合は、pfedit コマンドを使用して audit_warn ファイルを編集できます。

```
# pfedit /etc/security/audit_warn
```

詳細は、pfedit(4) のマニュアルページを参照してください。このコマンドは、すべての管理者が使用できます。

例 5-2 役割の使用を容易にするために認証をキャッシュする

この例では、監査構成を管理するための役割を管理者が構成しますが、ユーザーの認証をキャッシュすることで使用が容易になります。最初に、管理者は役割を作成して割り当てます。

```
# roleadd -K roleauth=user -P "Audit Configuration" audadmin
# usermod -R +audadmin jdoe
```

jdoe が、その役割に切り替えるときに -c オプションを使用した場合は、auditconfig の出力が表示される前にパスワードが必要になります。

```
% su - audadmin -c auditconfig option
Password: xxxxxxxx
     auditconfig output
```

認証がキャッシュされない場合は、jdoe がコマンドを再度実行するときにパスワードプロンプトが表示されます。

管理者が、認証のキャッシュを有効にする su スタックを保持するファイルを、pam.d ディレクトリに作成します。認証をキャッシュするときには、初回はパスワードが必要ですが、その後は一定の時間が経過するまでは、パスワードは不要です。

```
# pfedit /etc/pam.d/su
## Cache authentication for switched user
#
auth required           pam_unix_cred.so.1
auth sufficient         pam_tty_tickets.so.1
auth requisite          pam_authtok_get.so.1
auth required           pam_dhkeys.so.1
auth required           pam_unix_auth.so.1
```

このファイルを作成したあと、管理者は、各エントリにタイポ、脱字、または繰り返しがないかチェックします。

管理者は、前の su スタック全体を提供する必要があります。pam_tty_tickets.so.1 モジュールにはキャッシュが実装されています。PAM の詳細については、pam_tty_tickets(5) および pam.conf(4) のマニュアルページと『Oracle Solaris 11.2 での Kerberos およびその他の認証サービスの管理 』の第 1 章「プラグイン可能認証モジュールの使用」を参照してください。

管理者が su PAM ファイルを追加してシステムをリブートしたあと、audadmin 役割を含むすべての役割は、一連のコマンドを実行しているときに 1 回だけパスワードの入力を要求されます。

```
% su - audadmin -c auditconfig option
Password: xxxxxxxx
     auditconfig output
% su - audadmin -c auditconfig option
     auditconfig output
...
```

例 5-3 root 役割になる

次の例では、最初のユーザーが root 役割になり、その役割のシェルで特権を一覧表示します。

```
% roles
root
% su - root
Password: xxxxxxxx
#      Prompt changes to root prompt
# ppriv $$
1200:   pfksh
flags = <none>
        E: all
        I: basic
```

```
        P: all
        L: all
```

特権については、24 ページの「プロセス権管理」および ppriv(1) のマニュアルページを参照してください。

例 5-4 ARMOR 役割の引き受け

この例では、ユーザーは管理者が割り当てた ARMOR 役割を引き受けます。

端末ウィンドウで、ユーザーは割り当てられている役割を確認します。

```
% roles
fsadm
sysop
```

その後ユーザーは fsadm 役割を引き受け、ユーザーパスワードを入力します。

```
% su - fsadm
Password: xxxxxxxx
#
```

su - *rolename* コマンドは、端末のシェルをプロファイルシェルに変更します。これでユーザーは、この端末ウィンドウで fsadm 役割になりました。

この役割で実行できるコマンドを確認するため、ユーザーは 101 ページの「権利プロファイルの一覧表示」の手順に従います。

管理アクションの監査

しばしば、サイトのセキュリティーポリシーで管理アクションの監査が要求されることがあります。116:AUE_PFEXEC:execve(2) with pfexec enabled:ps,ex,ua,as 監査イベントはこのようなアクションを捕捉します。管理アクションを監査する際にもう 1 つのオプションとして、役割での使用に適したイベントグループを提供する cusa メタクラスがあります。詳細については、/etc/security/audit_class ファイルのコメントを参照してください。

例 5-5 2 つの役割を使用した監査の構成

この例では、2 人の管理者がサイトセキュリティー担当者の監査構成計画を実装します。この計画では、すべてのユーザーに pf クラスを使用し、個別の役割に cusa メタクラスを指定しま

す。root 役割は、監査フラグを役割に割り当てます。1 番目の管理者が監査を構成し、2 番目の管理者が新しい構成を有効にします。

1 番目の管理者に、Audit Configuration 権利プロファイルが割り当てられます。この管理者は現在の監査構成を表示します。

```
# auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
```

pf クラスには lo クラスが含まれていないため、管理者はこのクラスをシステム構成に追加します。

```
# auditconfig -setflags lo,pf
```

新しい監査構成をカーネルに読み込むには、Audit Control 権利プロファイルが割り当てられているユーザーが、監査サービスをリフレッシュします。

```
# audit -s
```

権利プロファイルと承認の作成

提供される権利プロファイルに必要な権利の集合が含まれていない場合は、権利プロファイルを作成または変更できます。限られた権利を持つユーザー、新しいアプリケーション、あるいはそのほかの目的で権利プロファイルを作成できます。

Oracle Solaris が提供する権利プロファイルは読み取り専用です。提供される権利プロファイルの一連の権利では不十分な場合は、その権利プロファイルをクローニングできます。たとえば、提供される権利プロファイルに solaris.admin.edit/*path-to-system-file* 承認を追加できます。背景情報については、23 ページの「権利プロファイルの詳細」を参照してください。

提供される承認に、特権付きアプリケーションでコーディングされている承認が含まれていない場合は、承認を作成できます。既存の承認は変更できません。背景情報については、22 ページの「ユーザー承認に関する詳細」を参照してください。

▼ 権利プロファイルを作成する方法

始める前に 権利プロファイルを作成するには、File Security 権利プロファイルが割り当てられている管理者になる必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **権利プロファイルを作成します。**

   # profiles -p [-S *repository*] *profile-name*

   説明を入力するよう求められます。

2. **権利プロファイルに内容を追加します。**

   1 つの値を持つプロファイルプロパティーには `set` サブコマンドを使用します (`set desc` など)。複数の値を指定できるプロパティーには `add` サブコマンドを使用します (`add cmd` など)。

   次のコマンドは、『Oracle Solaris 11.2 での Kerberos およびその他の認証サービスの管理 』の「変更された PAM ポリシーを割り当てる方法」のカスタム PAM 権利プロファイルを作成します。読みやすくするため、名前が短縮されています。

```
# profiles -p -S LDAP "Site PAM LDAP"
profiles:Site PAM LDAP> set desc="Profile which sets pam_policy=ldap"
...LDAP> set pam_policy=ldap
...LDAP> commit
...LDAP> end
...LDAP> exit
```

例 5-6 Sun Ray Users 権利プロファイルの作成

この例では、管理者は、LDAP リポジトリ内に Sun Ray ユーザーのための権利プロファイルを作成します。管理者は、すでに Basic Solaris User 権利プロファイルの Sun Ray バージョンを作成し、Sun Ray サーバー上の `policy.conf` ファイルからすべての権利プロファイルを削除しています。

```
# profiles -p -S LDAP "Sun Ray Users"
profiles:Sun Ray Users> set desc="For all users of Sun Rays"
... Ray Users> add profiles="Sun Ray Basic User"
... Ray Users> set defaultpriv="basic,!proc_info"
... Ray Users> set limitpriv="basic,!proc_info"
... Ray Users> end
... Ray Users> exit
```

管理者は、内容を確認します。

```
# profiles -p "Sun Ray Users" info
Found profile in LDAP repository.
        name=Sun Ray Users
        desc=For all users of Sun Rays
        defaultpriv=basic,!proc_info,
        limitpriv=basic,!proc_info,
        profiles=Sun Ray Basic User
```

例 5-7 特権付きコマンドを含む権利プロファイルの作成

この例では、セキュリティー管理者は、その管理者が作成した権利プロファイル内のアプリケーションに特権を追加します。このアプリケーションは特権を認識できます。

```
# profiles -p SiteApp
profiles:SiteApp> set desc="Site application"
profiles:SiteApp> add cmd="/opt/site-app/bin/site-cmd"
profiles:SiteApp:site-cmd> add privs="proc_fork,proc_taskid"
profiles:SiteApp:site-cmd> end
profiles:SiteApp> exit
```

確認するには、管理者は `site-cmd` を選択します。

```
# profiles -p SiteApp "select cmd=/opt/site-app/bin/site-cmd; info;end"
Found profile in files repository.
  id=/opt/site-app/bin/site-cmd
  privs=proc_fork,proc_taskid
```

次の手順 信頼できるユーザーまたは役割に権利プロファイルを割り当てます。例については、例 3-10「DHCP を管理できるユーザーの作成」および例3-19「信頼できるユーザーによる拡張アカウントファイル読み取りの有効化」を参照してください。

参照 権利割り当てのトラブルシューティングを行うには、109 ページの「権利割り当てをトラブルシューティングする方法」を参照してください。背景情報については、38 ページの「割り当てられた権利の検索順序」を参照してください。

▼ システム権利プロファイルをクローニングおよび変更する方法

始める前に 権利プロファイルを作成または変更するには、File Security 権利プロファイルが割り当てられている管理者になる必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **既存のプロファイルから新しい権利プロファイルを作成します。**

```
# profiles -p [-S repository] existing-profile-name
```

- **既存の権利プロファイルに内容を追加するには、新しいプロファイルを作成します。**

  新しいプロファイルに既存の権利プロファイルを補助権利プロファイルとして追加してから、拡張を追加します。例5-8「Network IPsec Management 権利プロファイルのクローニングと拡張」を参照してください。

- **既存の権利プロファイルから内容を削除するには、そのプロファイルをクローニングし、名前を変更して変更を行います。**

  例5-9「権利プロファイルでの選択した権利のクローニングおよび削除」を参照してください。

2. **補助権利プロファイル、承認、およびその他の権利を追加または削除して、新しい権利プロファイルを変更します。**

例 5-8 Network IPsec Management 権利プロファイルのクローニングと拡張

この例では、管理者がサイトの IPsec Management 権利プロファイルに `solaris.admin.edit` 承認を追加し、これにより `root` 役割が不要になります。この権利プロファイルは、信頼されており `/etc/hosts` ファイルを変更できるユーザーだけに割り当てられます。

1. 管理者は、Network IPsec Management 権利プロファイルを変更できないことを確認します。

```
# profiles -p "Network IPsec Management"
profiles:Network IPsec Management> add auths="solaris.admin.edit/etc/hosts"
Cannot add. Profile cannot be modified
```

2. 管理者は、Network IPsec Management プロファイルを含む権利プロファイルを作成します。

```
# profiles -p "Total IPsec Mgt"
... IPsec Mgt> set desc="Network IPsec Mgt plus /etc/hosts"
... IPsec Mgt> add profiles="Network IPsec Management"
... IPsec Mgt> add auths="solaris.admin.edit/etc/hosts"
... IPsec Mgt> end
... IPsec Mgt> exit
```

3. 管理者は、内容を確認します。

```
# profiles -p "Total IPsec Mgt" info
        name=Total IPsec Mgt
        desc=Network IPsec Mgt plus /etc/hosts
        auths=solaris.admin.edit/etc/hosts
        profiles=Network IPsec Management
```

例 5-9　権利プロファイルでの選択した権利のクローニングおよび削除

この例では、管理者は VSCAN サービスのプロパティーの管理を、このサービスを有効および無効にする機能から分離します。

最初に、管理者は、Oracle Solaris が提供する権利プロファイルの内容を一覧表示します。

```
# profiles -p "VSCAN Management" info
        name=VSCAN Management
        desc=Manage the VSCAN service
        auths=solaris.smf.manage.vscan,solaris.smf.value.vscan,
              solaris.smf.modify.application
        help=RtVscanMngmnt.html
```

次に、管理者はサービスを有効化および無効化できる権利プロファイルを作成します。

```
# profiles -p "VSCAN Management"
profiles:VSCAN Management> set name="VSCAN Control"
profiles:VSCAN Control> set desc="Start and stop the VSCAN service"
... VSCAN Control> remove auths="solaris.smf.value.vscan"
... VSCAN Control> remove auths="solaris.smf.modify.application"
... VSCAN Control> end
... VSCAN Control> exit
```

次に、管理者は、サービスのプロパティーを変更できる権利プロファイルを作成します。

```
# profiles -p "VSCAN Management"
profiles:VSCAN Management> set name="VSCAN Properties"
profiles:VSCAN Properties> set desc="Modify VSCAN service properties"
... VSCAN Properties> remove auths="solaris.smf.manage.vscan"
... VSCAN Properties> end
... VSCAN Properties> exit
```

管理者は、新しい権利プロファイルの内容を確認します。

```
# profiles -p "VSCAN Control" info
        name=VSCAN Control
        desc=Start and stop the VSCAN service
        auths=solaris.smf.manage.vscan
# profiles -p "VSCAN Properties" info
        name=VSCAN Properties
        desc=Modify VSCAN service properties
        auths=solaris.smf.value.vscan,solaris.smf.modify.application
```

次の手順　信頼できるユーザーまたは役割に権利プロファイルを割り当てます。例については、例 3-10「DHCP を管理できるユーザーの作成」および例3-19「信頼できるユーザーによる拡張アカウントファイル読み取りの有効化」を参照してください。

参照 権利割り当てのトラブルシューティングを行うには、109 ページの「権利割り当てをトラブルシューティングする方法」を参照してください。背景情報については、38 ページの「割り当てられた権利の検索順序」を参照してください。

▼ 承認を作成する方法

始める前に 開発者は、ユーザーがインストールするアプリケーションで承認を定義および使用しています。手順については、『Oracle Solaris 11 セキュリティー開発者ガイド 』および『Oracle Solaris 11 セキュリティー開発者ガイド 』の「承認について」を参照してください。

1. **(オプション) 新しい承認のヘルプファイルを作成します。**

   たとえば、ユーザーがアプリケーション内のデータを変更できるようにするための承認のヘルプファイルを作成します。

```
# pfedit /docs/helps/NewcoSiteAppModData.html
<HTML>
-- Copyright 2013 Newco.  All rights reserved.
-- NewcoSiteAppModData.html
-->
<HEAD>
     <TITLE>NewCo Modify SiteApp Data Authorization</TITLE>
</HEAD>
<BODY>
The com.newco.siteapp.data.modify authorization authorizes you
to modify existing data in the application.
<p>
Only authorized accounts are permitted to modify data.
Use this authorization with care.
<p>
</BODY>
</HTML>
```

2. **`auths add` コマンドを使用して承認を作成します。**

   たとえば次のコマンドは、`com.newco.siteapp.data.modify` 承認をローカルシステムに作成します。

```
# auths add -t "SiteApp Data Modify Authorized" \
-h /docs/helps/NewcoSiteAppModData.html com.newco.siteapp.data.modify
```

   これで承認をテストし、権利プロファイルに追加し、役割またはユーザーにそのプロファイルを割り当てることができます。

例 5-10 新しい承認のテスト

この例では、管理者が 例5-7「特権付きコマンドを含む権利プロファイルの作成」の SiteApp 権利プロファイルを使用して com.newco.siteapp.data.modify 承認をテストします。

```
# usermod -A com.newco.siteapp.data.modify -P SiteApp tester1
```

テストが正常に完了したら、管理者は承認を削除します。

```
# rolemod -A-=com.newco.siteapp.data.modify siteapptester
```

保守を容易にするため、管理者は 例5-11「権利プロファイルへの承認の追加」の SiteApp 権利プロファイルにこの承認を追加します。

例 5-11 権利プロファイルへの承認の追加

承認が適切に機能することをテストしたら、セキュリティー管理者は com.newco.siteapp.data.modify 承認を既存の権利プロファイルに追加します。例5-7「特権付きコマンドを含む権利プロファイルの作成」に、管理者がプロファイルを作成した方法を示します。

```
# profiles -p "SiteApp"
profiles:SiteApp> add auths="com.newco.siteapp.data.modify"
profiles:SiteApp> end
profiles:SiteApp> exit
```

確認するために、管理者はプロファイルの内容を一覧表示します。

```
# profiles -p SiteApp
Found profile in files repository.
  id=/opt/site-app/bin/site-cmd
  auths=com.newco.siteapp.data.modify
```

次の手順 信頼できるユーザーまたは役割に権利プロファイルを割り当てます。例については、例3-10「DHCP を管理できるユーザーの作成」および例3-19「信頼できるユーザーによる拡張アカウントファイル読み取りの有効化」を参照してください。

参照 権利割り当てのトラブルシューティングを行うには、109 ページの「権利割り当てをトラブルシューティングする方法」を参照してください。背景情報については、38 ページの「割り当てられた権利の検索順序」を参照してください。

root がユーザーまたは役割のいずれであるかの変更

デフォルトでは、root は Oracle Solaris の役割です。ユーザーに変更し、再度役割に変更するか、またはこれを削除して使用しないようにするオプションがあります。

Oracle Enterprise Manager を使用している場合、または権利モデルではなく従来のスーパーユーザーによる管理モデルに従っている場合は、root をユーザーに変更する必要があります。背景情報については、43 ページの「管理に使用する権利モデルの決定」を参照してください。

権利モデルに従っている場合は、ネットワークから取り外されたシステムを廃棄する場合に root をユーザーに変更することがあります。このシナリオでは、root としてシステムにログインするとクリーンアップが容易になります。

注記 - root 役割を使用してリモート管理を行う場合は、セキュリティー保護されたリモートログインの手順について『Oracle Solaris 11.2 での Secure Shell アクセスの管理 』の「Secure Shell を使用して ZFS をリモートで管理する方法」を参照してください。

一部のサイトでは、本番システムでは root が正当なアカウントではないことがあります。root を使用しないように削除するには、例5-13「システム保守での root 役割の使用の防止」を参照してください。

▼ root 役割をユーザーに変更する方法

この手順は、root がシステムに直接ログインできる必要があるシステムで行う必要があります。

始める前に root 役割になる必要があります。

1. **root 役割の割り当てをローカルユーザーから削除します。**

   たとえば、その役割の割り当てを 2 人のユーザーから削除します。

```
% su -
Password: xxxxxxxx
# roles jdoe
root
# roles kdoe
root
# roles ldoe
```

```
secadmin
# usermod -R "" jdoe
# usermod -R "" kdoe
#
```

2. **root 役割をユーザーに変更します。**

```
# rolemod -K type=normal root
```

現在 root 役割になっているユーザーはそのままです。root アクセスを持つほかのユーザーは、su を実行して root に変更することも、root ユーザーとしてシステムにログインすることもできます。

3. **変更内容を確認します。**

次のいずれかのコマンドを使用できます。

- **root の user_attr エントリを調べます。**

```
# getent user_attr root
root::::auths=solaris.*;profiles=All;audit_flags=lo\:no;lock_after_retries=no;
min_label=admin_low;clearance=admin_high
```

type キーワードが出力内に見つからないか、または normal に等しい場合、そのアカウントは役割ではありません。

- **userattr コマンドからの出力を表示します。**

```
# userattr type root
```

出力が空であるか、または normal が表示される場合、そのアカウントは役割ではありません。

例 5-12 root ユーザーを root 役割に変更する

この例では、root ユーザーが root ユーザーを役割に戻します。

最初に、root ユーザーは root アカウントを役割に変更し、その変更内容を確認します。

```
# usermod -K type=role root
# getent user_attr root
root::::type=role...
```

次に、root は root 役割をローカルユーザーに割り当てます。

```
# usermod -R root jdoe
```

例 5-13 システム保守での root 役割の使用の防止

この例では、root アカウントによるシステムの保守を防ぐように、サイトのセキュリティーポリシーで要求します。管理者は、システムを保守する役割をすでに作成し、テストしています。これらの役割には、すべてのセキュリティープロファイルと System Administrator 権利プロファイルが含まれています。信頼できるユーザーには、バックアップを復元できる役割が割り当てられています。ユーザー、役割、または権利プロファイルの監査フラグを変更するか、または役割のパスワードを変更することができる役割はありません。

root アカウントがシステムの保守に使用されないようにするために、セキュリティー管理者は、root 役割の割り当てを削除します。root アカウントはシングルユーザーモードでシステムにログインできる必要があるため、そのアカウントのパスワードは保持されます。

```
# usermod -K roles= jdoe
# userattr roles jdoe
```

注意事項 デスクトップ環境では、root が役割の場合は root として直接ログインすることはできません。このシステム上で root が役割になっていることを示す診断メッセージが表示されます。

root 役割を引き受けることができるローカルアカウントがない場合は、次のステップを実行します。

- root としてシングルユーザーモードでシステムにログインし、ローカルユーザーアカウントとパスワードを作成します。
- root 役割を新しいアカウントに割り当てます。
- この新しいユーザーとしてログインし、root 役割を引き受けます。

♦ ♦ ♦ 第 6 章

6 Oracle Solaris の権利の一覧表示

この章では、システムのすべての権利、特定ユーザーに割り当てられている権利、およびユーザー自身の権利を一覧表示する方法を説明します。

権利の概要については、14 ページの「ユーザー権管理」を参照してください。参照情報については、第8章「Oracle Solaris 権利リファレンス」を参照してください。

権利とその定義の一覧表示

このセクションのコマンドを使用すると、システムで定義されている権利を検索し、ユーザーのプロセスに対して有効な権利を一覧表示できます。

このセクションのコマンドの詳細については、次に示すマニュアルページを参照してください。

- `auths`(1)
- `getent`(1M)
- `ppriv`(1)
- `profiles`(1)
- `privileges`(5)
- `roles`(1)

承認の一覧表示

- `auths` – 現在のユーザーの承認を一覧表示します
- `auths list` – 現在のユーザーの承認を一覧表示します
- `auths list -u` *username* – *username* の承認を一覧表示します
- `auths list -x` – 認証が必要な現在のユーザーの承認を一覧表示します
- `auths list -xu` *username* – 認証が必要な *username* の承認を一覧表示します
- `auths info` – ネームサービス内のすべての承認名を一覧表示します
- `getent auth_attr` – ネームサービス内のすべての承認の完全な定義を一覧表示します

例 6-1 すべての承認の一覧表示

```
$ auths info
    solaris.account.activate
    solaris.account.setpolicy
    solaris.admin.edit
...
    solaris.zone.login
    solaris.zone.manage
```

例 6-2 承認データベースの内容の一覧表示

```
$ getent auth_attr | more
solaris.:::All Solaris Authorizations::help=AllSolAuthsHeader.html
solaris.account.:::Account Management::help=AccountHeader.html
...
solaris.zone.login:::Zone Login::help=ZoneLogin.html
solaris.zone.manage:::Zone Deployment::help=ZoneManage.html
```

例 6-3 ユーザーのデフォルト承認の一覧表示

次に示す承認は、デフォルトですべてのユーザーに割り当てられる権利プロファイルに含まれています。

```
$ auths
solaris.device.cdrw,solaris.device.mount.removable,solaris.mail.mailq
solaris.network.autoconf.read,solaris.admin.wusb.read
solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
```

権利プロファイルの一覧表示

- `profiles` – 現在のユーザーの権利プロファイルを一覧表示します
- `profiles -a` – すべての権利プロファイル名を一覧表示します
- `profiles -l` – 現在のユーザーの権利プロファイルの完全な定義を一覧表示します
- `profiles` *username* – *username* の権利プロファイルを一覧表示します
- `profiles -x` – 認証が必要な現在のユーザーの権利プロファイルを一覧表示します
- `profiles -x` *username* – 認証が必要な *username* の権利プロファイルを一覧表示します
- `profiles -p` *profile-name* `info` – 指定された権利プロファイルの内容をプリティプリントで出力します
- `getent prof_attr` – ネームサービス内のすべての権利プロファイルの完全な定義を一覧表示します

例 6-4 すべての権利プロファイル名の一覧表示

```
$ profiles -a
        Console User
        CUPS Administration
        Desktop Removable Media User
...
        VSCAN Management
        WUSB Management
```

例 6-5 権利プロファイルデータベースの内容の一覧表示

```
$ getent prof_attr | more
All:::Execute any command as the user or role:help=RtAll.html
Audit Configuration:::Configure Solaris Audit:auths=solaris.smf.value.audit;
help=RtAuditCfg.html
...
Zone Management:::Zones Virtual Application Environment Administration:
help=RtZoneMngmnt.html
Zone Security:::Zones Virtual Application Environment Security:auths=solaris.zone.*,
solaris.auth.delegate;help=RtZoneSecurity.html ...
```

例 6-6 ユーザーのデフォルト権利プロファイルの一覧表示

権利プロファイルを一覧表示します。デフォルトでは次の権利プロファイルがすべてのユーザーに割り当てられます。

```
$ profiles
```

```
Basic Solaris User
All
```

例 6-7 初期ユーザーの権利プロファイルの一覧表示

初期ユーザーにはさまざまな権利プロファイルが割り当てられます。

```
$ profiles Initial user
System Administrator
Audit Review
...
CPU Power Management
Basic Solaris User
All
```

初期ユーザーのプロファイルに割り当てられているセキュリティー属性をすべて表示するには、-l オプションを使用します。

```
$ profiles -l Initial user | more
Initial user:
System Administrator
 profiles=Install Service Management,Audit Review,Extended Accounting
Flow Management,Extended Accounting Net Management,Extended Accounting Process
Management,Extended Accounting Task Management,Printer Management,Cron Managem
ent,Device Management,File System Management,Log Management,Mail Management,
Maintenance and Repair,Media Catalog,Name Service Management,Network Management,
Project Management,RAD Management,Service Operator,Shadow Migration Monitor,So
Software Installation,System Configuration,User Management,ZFS Storage Management
          /usr/sbin/gparted          uid=0
Install Service Management
 auths=solaris.autoinstall.service
 profiles=Install Manifest Management,Install Profile Management,
Install Client Management
...
```

例 6-8 割り当てられている権利プロファイルの内容の一覧表示

初期ユーザーが、Audit Review プロファイルにより付与された権利を一覧表示します。

```
$ profiles -l
Audit Review
  solaris.audit.read

  /usr/sbin/auditreduce  euid=0
  /usr/sbin/auditstat    privs=proc_audit
  /usr/sbin/praudit      privs=file_dac_read
```

例 6-9 権利プロファイルのコマンドのセキュリティー属性の一覧表示

`profiles` コマンドのこのバリアントは、ユーザー自身に割り当てられていない権利プロファイル内のコマンドのセキュリティー属性を表示する場合に役立ちます。

最初に、プロファイル内のコマンドを一覧表示します。

```
% profiles -p "Audit Review" info
 name=Audit Review
 desc=Review Solaris Auditing logs
 help=RtAuditReview.html
 cmd=/usr/sbin/auditreduce
 cmd=/usr/sbin/auditstat
 cmd=/usr/sbin/praudit
```

次に、プロファイル内の 1 つのコマンドのセキュリティー属性を一覧表示します。

```
% profiles -p "Audit Review" "select cmd=/usr/sbin/praudit ; info; end;"
select: command is read-only
 id=/usr/sbin/praudit
 privs=file_dac_read
end: command is read-only
```

例 6-10 最近作成された権利プロファイルの内容の一覧表示

`less` オプションは、最近追加された権利プロファイルを最初に表示します。`profiles` コマンドのこのバリアントは、サイトで権利プロファイルを作成または変更する際に役立ちます。次の出力には、例4-1「レガシーアプリケーションへのセキュリティー属性の割り当て」で追加されたプロファイルの内容が示されています。通常のユーザーがこのコマンドを実行できます。

```
$ profiles -la | less
LegacyApp
         /opt/legacy-app/bin/legacy-cmd
                                   euid=0
OpenLDAP...
```

役割の一覧表示

- `roles` – 現在のユーザーの役割を一覧表示します
- `roles` *username* – *username* の役割を一覧表示します
- `logins -r` – 使用可能なすべての役割を一覧表示します

例 6-11 割り当てられている役割の一覧表示

デフォルトでは、root 役割が初期ユーザーに割り当てられます。No roles は、役割が割り当てられないことを示します。

```
$ roles
root
```

特権の一覧表示

- man privileges – 開発者により使用される特権の定義と特権の名前を一覧表示します
- ppriv -vl – 開発者により使用される特権の定義と特権の名前を一覧表示します
- ppriv -vl basic – 特権の基本セット内の特権の名前と定義を一覧表示します
- ppriv $$ – 現在のシェル ($$) 内の特権を一覧表示します
- getent exec_attr – 権利プロファイル名別にセキュリティー属性 (setuid または特権) を持つすべてのコマンドを一覧表示します

```
$ getent exec_attr | more
All:solaris:cmd:::*:
Audit Configuration:solaris:cmd:::/usr/sbin/auditconfig:privs=sys_audit
...
Zone Security:solaris:cmd:::/usr/sbin/txzonemgr:uid=0
Zone Security:solaris:cmd:::/usr/sbin/zonecfg:uid=0 ...
```

例 6-12 すべての特権とその定義の一覧表示

privileges(5) のマニュアルページで説明する特権フォーマットは開発者によって使用されます。

```
$ man privileges
Standards, Environments, and Macros                 privileges(5)

NAME
     privileges - process privilege model
...
     The defined privileges are:

     PRIV_CONTRACT_EVENT

         Allow a process to request reliable delivery  of  events
         to an event endpoint.

         Allow a process to include events in the critical  event
```

```
        set  term  of  a  template  which  could be generated in
        volume by the user.
...
```

例 6-13 特権割り当てで使用される特権の一覧表示

ppriv コマンドは、すべての特権の名前を一覧表示します。定義を表示するには -v オプションを使用します。

この特権フォーマットは、useradd, roleadd、usermod、および rolemod コマンドを使用してユーザーと役割に特権を割り当てる場合、および profiles コマンドを使用して権利プロファイルに特権を割り当てる場合に使用されます。

```
$ ppriv -lv | more
contract_event
 Allows a process to request critical events without limitation.
 Allows a process to request reliable delivery of all events on
 any event queue.
...
win_upgrade_sl
        Allows a process to set the sensitivity label of a window
        resource to a sensitivity label that dominates the existing
        sensitivity label.
        This privilege is interpreted only if the system is configured
        with Trusted Extensions.
```

例 6-14 現在のシェル内の特権の一覧表示

デフォルトでは、どのユーザーにも基本特権セットが割り当てられます。デフォルトの制限セットはすべての特権です。

出力の最初の文字は、次の特権セットを指しています。

E 有効特権セット

I 継承可能な特権セット

P 許可された特権セット

L 制限特権セット

```
$ ppriv $$
1200:   -bash
flags = <none>
        E: basic
        I: basic
```

```
        P: basic
        L: all
$ ppriv -v $$
1200:   -bash
flags = <none>
 E: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
           proc_info,proc_session,sys_ib_info
 I: file_link_any,file_read,...,sys_ib_info
 P: file_link_any,file_read,...,sys_ib_info
 L: contract_event,contract_identity,...,sys_time
```

2 つのドル記号 (`$$`) により、親シェルのプロセス番号がコマンドに渡されます。この一覧表示には、割り当てられている権利プロファイル内のコマンドに制限されている特権は含まれません。

例 6-15 基本特権とその定義の一覧表示

```
$ ppriv -vl basic
file_link_any
 Allows a process to create hardlinks to files owned by a uid
 different from the process' effective uid.
file_read
 Allows a process to read objects in the filesystem.
file_write
 Allows a process to modify objects in the filesystem.
net_access
 Allows a process to open a TCP, UDP, SDP or SCTP network endpoint.
proc_exec
 Allows a process to call execve().
proc_fork
 Allows a process to call fork1()/forkall()/vfork()
proc_info
 Allows a process to examine the status of processes other
 than those it can send signals to.  Processes which cannot
 be examined cannot be seen in /proc and appear not to exist.
proc_session
 Allows a process to send signals or trace processes outside its
 session.
sys_ib_info
 Allows a process to perform read InfiniBand MAD (Management Datagram)
 operations.
```

例 6-16 ユーザーの権利プロファイル内のセキュリティー属性を持つコマンドの一覧表示

Basic Solaris User プロファイルには、ユーザーが CD-ROM への読み取りと書き込みを行えるコマンドが含まれています。

```
$ profiles -l
  Basic Solaris User
...
```

```
  /usr/bin/cdrecord.bin   privs=file_dac_read,sys_devices,
    proc_lock_memory,proc_priocntl,net_privaddr
  /usr/bin/readcd.bin     privs=file_dac_read,sys_devices,net_privaddr
  /usr/bin/cdda2wav.bin   privs=file_dac_read,sys_devices,
    proc_priocntl,net_privaddr
All
 *
```

修飾属性の一覧表示

- `man user_attr` – セキュリティー属性の修飾子を定義します
- `getent` – コマンドが実行されるシステム上の特定のユーザーまたは役割の修飾セキュリティー属性を一覧表示します
- `ldapaddent` – 特定のユーザーまたは役割の修飾セキュリティー属性をすべて一覧表示します

例 6-17 このシステム上のユーザーの修飾属性の一覧表示

```
machine1$ getent user_attr | jdoe:
jdoe:machine1:::profiles=System Administrator
```

例 6-18 LDAP 内のユーザーの全修飾属性の一覧表示

```
machine1$ ldapaddent -d user_attr | grep ^jdoe:
jdoe:machine1:::profiles=System Administrator
jdoe:sysopgroup:::profiles=System Operator
```

♦ ♦ ♦ 第 7 章

7 Oracle Solaris での権利のトラブルシューティング

この章では、Oracle Solaris で管理権利を管理および使用する際のトラブルシューティングについて提案します。

- 109 ページの「権利割り当てをトラブルシューティングする方法」
- 114 ページの「割り当てられている権利を並べ替える方法」
- 115 ページの「プログラムが必要とする特権を判断する方法」

権利の使用については、次の情報を参照してください。

- 第3章「Oracle Solaris での権利の割り当て」
- 48 ページの「役割を割り当てることができるユーザー」
- 14 ページの「ユーザー権管理」
- 24 ページの「プロセス権管理」

権利に関するトラブルシューティング

このセクションのタスクと例では、権利の割り当てに関する問題の解決策を提案します。バックグラウンド情報については、37 ページの「権利の検証」を参照してください。

▼ 権利割り当てをトラブルシューティングする方法

権利が評価されず正しく適用されない原因には、さまざまな要素の影響があります。この手順は、割り当てられている権利がユーザー、役割、プロセスに対して使用できない原因のデバッグを支援します。いくつかのステップは 38 ページの「割り当てられた権利の検索順序」に基づいています。

始める前に root 役割になる必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **ネームサービスを検証して再起動します。**

   a. **ユーザーまたは役割のセキュリティー割り当てが、システムで有効になっているネームサービス内にあることを確認します。**

   ```
   # svccfg -s name-service/switch

   svc:/system/name-service/switch>
   listprop config

   config                      application
   config/value_authorization  astring  solaris.smf.value.name-service.switch
   config/default              astring  files ldap
   config/host                 astring  "files dns mdns ldap"
   config/netgroup             astring  ldap
   config/printer              astring  "user files"
   ```

   この出力では、明示的に示されていないサービスはすべて、デフォルトの値 files ldap を継承します。そのため、passwd とその関連属性データベース user_attr、auth_attr、および prof_attr は、まずファイル内で検索され、次に LDAP 内で検索されます。

   b. **ネームサービスキャッシュ svc:/system/name-service/cache を再起動します。**

   nscd デーモンには長い有効期間を設定することができます。デーモンを再起動して、現在のデータでネームサービスを更新します。

   ```
   # svcadm restart name-service/cache
   ```

2. **userattr -v コマンドを実行して権利がユーザーに割り当てられる場所を特定します。**

   たとえば次のコマンドは、割り当てられている権利と、その割り当てがユーザー jdoe に対して行われた場所を示します。jdoe がデフォルトを使用していることを示す出力はありません。

   ```
   % userattr -v access_times jdoe
   % userattr -v access_tz jdoe
   % userattr -v auth_profiles jdoe
   % userattr -v defaultpriv jdoe
   % userattr -v limitpriv jdoe
   % userattr -v idlecmd jdoe
   % userattr -v idletime jdoe
   % userattr -v lock_after_retries jdoe
   % userattr -v pam_policy jdoe

   % userattr -v auths jdoe      Output indicates authorizations from rights profiles
   Basic Solaris User :solaris.mail.mailq,solaris.network.autoconf.read,
   ```

```
solaris.admin.wusb.read
Console User :solaris.system.shutdown,solaris.device.cdrw,
solaris.device.mount.removable,solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
% userattr -v audit_flags jdoe
user_attr: fw:no       Output indicates jdoe is individually assigned audit flags
# userattr -v profiles jdoe
user_attr: Audit Review,Stop       Output indicates two assigned rights profiles
# userattr roles jdoe
user_attr : cryptomgt,infosec       Output indicates two assigned roles
```

この出力は、jdoe に監査フラグ、2 つの権利プロファイル、および 2 つの役割が直接割り当てられていることを示しています。割り当てられた承認は、policy.conf ファイル内のデフォルト権利プロファイルのものです。

- jdoe には監査フラグが直接割り当てられるため、権利プロファイルの監査フラグ値は使用されません。
- 権利プロファイルは、Audit Review 権利プロファイルから始まり、次に Stop プロファイルという順序で評価されます。
- そのほかのすべての権利は、役割 cryptomgt と infosec で jdoe に割り当てられています。これらの権利を表示するには、jdoe が各役割を引き受けてから、権利を一覧表示する必要があります。

権利がユーザーに直接割り当てられていない場合は、次の確認作業に進みます。

3. **割り当てられている承認のスペルが正しいことを確認します。**

   承認はユーザーに対して累積されるため、承認の割り当てのソースは重要ではありません。ただし、スペルが正しくない承認は暗黙のうちに失敗します。

4. **自分が作成した権利プロファイルについて、そのプロファイル内のコマンドに適切なセキュリティー属性を割り当てたことを確認します。**

   たとえば、成功するには euid=0 ではなく uid=0 が必要なコマンドもあります。コマンドのマニュアルページを参照し、コマンドとそのオプションに承認が必要であるかどうかをか確認してください。

5. **ユーザーの権利プロファイルの権利を確認します。**

   a. **認証権利プロファイルのリストで権利を順に確認します。**

      リスト内のもっとも古い権利プロファイルに含まれる属性の値は、カーネル内の値です。この値が正しくない場合は、その権利プロファイル内の値を変更するか、またはプロファイルを正しい順序で再割り当てします。114 ページの「割り当てられている権利を並べ替える方法」を参照してください。

特権コマンドの場合、defaultpriv または limitpriv キーワードから特権が削除されていないことを確認します。

b. **標準権利プロファイルのリストで権利を順に確認します。**

認証権利プロファイルで実行したものと同じ検査を行います。

c. **検索する権利がリストにない場合は、ユーザーに割り当てられている役割を調べます。**

権利が 1 つの役割に割り当てられている場合、ユーザーはその役割を引き受けて権利を取得する必要があります。

6. **失敗したコマンドが成功するには承認が必要であるかどうかを確認します。**

a. **既存の権利プロファイルに必要な承認が含まれているかどうかを確認します。**

プロファイルが存在する場合は、そのプロファイルを使用します。認証権利プロファイルまたは標準権利プロファイルとしてユーザーに割り当てます。この承認が成功する必要があるコマンドを含むそのほかの権利プロファイルよりも前に、このプロファイルを配置します。

b. **コマンドのオプションに承認が必要であるかどうかを確認します。**

特権が必要なコマンドにその特権を割り当て、必要な承認を追加し、そのコマンドと承認を権利プロファイル内に配置してから、そのプロファイルをユーザーに割り当てます。

7. **特定のユーザーに対してコマンドが継続して失敗する場合は、そのユーザーがプロファイルシェルでそのコマンドを実行しているかどうかを確認します。**

管理コマンドは、プロファイルシェルで実行する必要があります。例7-1「プロファイルシェルを使用しているかどうかの判断」は、プロファイルシェルのテスト方法を示します。

ユーザーエラーが発生する可能性を削減するには、次を試してみることができます。

- プロファイルシェルをユーザーのログインシェルとして割り当てます。
- ユーザーに対し、すべての特権付きコマンドより前に pfexec コマンドを配置するように指示します。
- 管理コマンドをプロファイルシェルで実行するようユーザーに注意を促します。
- サイトで役割が使用されている場合は、ユーザーに対し、管理コマンドを実行する前にその役割を引き受けるように注意を促します。ユーザーではなく役割としてコマンドを正常に実行する例については、例7-3「役割での特権付きコマンドの実行」を参照してください。

8. **役割でコマンドが失敗する場合は、その役割を引き受け、ユーザーの権利を確認する場合と同じ手順を実行します。**

例 7-1 プロファイルシェルを使用しているかどうかの判断

特権付きコマンドが機能しない場合、ユーザーは PRIV_PFEXEC フラグをテストしてからそのコマンドを実行します。エラーメッセージに、この問題が特権の問題であると示されない場合があります。

```
% praudit 20120814200247.20120912213421.example-system
praudit: Cannot associate stdin with 20120814200247.20120912213421.example-system:
Permission denied

% ppriv $$
107219: bash
flags = <none>
...

% pfbash
# ppriv $$
1072232: bash
flags = PRIV_PFEXEC
...

# praudit 20120814200247.20120912213421.example-system
     /** Command succeeds **/
```

例 7-2 役割の特権付きコマンドの判断

この例では、ユーザーは割り当てられた役割を引き受け、いずれかの権利プロファイルに含まれている権利を一覧表示します。コマンドを強調するため、権利は切り捨てられています。

```
% roles
devadmin

% su - devadmin
Password: xxxxxxxx

# profiles -l
Device Security
        ...
 profiles=Service Configuration
          /usr/sbin/add_drv          uid=0
          /usr/sbin/devfsadm         uid=0
                                     privs=sys_devices,sys_config,
                                           sys_resource,file_owner,
                                           file_chown,file_chown_self,
                                           file_dac_read
          /usr/sbin/eeprom           uid=0
```

```
          /usr/bin/kbd
          /usr/sbin/list_devices     euid=0
          /usr/sbin/rem_drv          uid=0
          /usr/sbin/strace           euid=0
          /usr/sbin/update_drv       uid=0
          /usr/sbin/add_allocatable  euid=0
          /usr/sbin/remove_allocatable   euid=0
Service Configuration
          /usr/sbin/svcadm
          /usr/sbin/svccfg
```

例 7-3 役割での特権付きコマンドの実行

次の例では、admin 役割は useful.script ファイルに対するアクセス権を変更できます。

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 elsee eng 262 Apr 2 10:52 useful.script

% chgrp admin useful.script
chgrp: useful.script: Not owner

% su - admin
Password: xxxxxxxx

# chgrp admin useful.script
# chown admin useful.script
# ls -l useful.script
-rwxr-xr-- 1 admin admin 262 Apr 2 10:53 useful.script
```

▼ 割り当てられている権利を並べ替える方法

特権付きコマンドではなく特権なしのコマンドがユーザーに対して有効である場合は、ユーザーの権利プロファイルの割り当てを並べ替える必要があります。詳細は、38 ページの「割り当てられた権利の検索順序」を参照してください。

始める前に User Security 権利プロファイルが割り当てられている管理者になる必要があります。詳細は、84 ページの「割り当てられている管理権利の使用」を参照してください。

1. **現在ユーザーまたは役割に割り当てられている権利プロファイルのリストを表示します。**

   リストが順番に表示されます。

   ```
   % profiles username | rolename
   ```

2. **権利プロファイルを正しい順序で割り当てます。**

```
# usermod | rolemod -P "list-of-profiles"
```

例 7-4 権利プロファイルの特定の順序での割り当て

この例では、管理者は、特権付きコマンドを含む権利プロファイルが、役割 devadmin のすべての権利プロファイルのあとに一覧表示されるように決定します。

```
# profiles devadmin

    Basic Solaris User
    All
    Device Management
```

そのため、devadmin 役割は、その役割に割り当てられている特権でデバイス管理コマンドを実行できません。

管理者は、devadmin に権利プロファイルを再割り当てします。新しい割り当て順序では、割り当てられている特権を使用してデバイス管理コマンドが実行されます。

```
# rolemod -P "Device Management,Basic Solaris User,All"

# profiles devadmin

    Device Management
    Basic Solaris User
    All
```

▼ プログラムが必要とする特権を判断する方法

このデバッグ手順は、コマンドまたはプロセスが失敗した場合に使用します。最初の特権失敗を検出して修正したあとで、ppriv -eD *command* コマンドを再度実行し、追加の特権要件を見つける必要がある場合があります。

1. **ppriv デバッグコマンドへの引数として、失敗したコマンドを入力します。**

```
% ppriv -eD touch /etc/acct/yearly

touch[5245]: missing privilege "file_dac_write"
     (euid = 130, syscall = 224) needed at zfs_zaccess+0x258
touch: cannot create /etc/acct/yearly: Permission denied
```

2. **デバッグ出力の syscall 番号を使用して、どのシステム呼び出しが失敗したかを特定します。**

/etc/name_to_sysnum ファイルで syscall 番号の名前を見つけます。

```
% grep 224 /etc/name_to_sysnum

creat64                 224
```

この例ではcreat64() 呼び出しが失敗しています。正常に完了するには、/etc/acct/yearly ディレクトリ内にファイルを作成できる権利がプロセスに割り当てられている必要があります。

例 7-5 特権の使用を検査するための truss コマンドの使用

truss コマンドは、通常のシェルで特権の使用をデバッグすることができます。たとえば、次のコマンドは、失敗した touch プロセスをデバッグします。

```
% truss -t creat touch /etc/acct/yearly

creat64("/etc/acct/yearly", 0666)
                      Err#13 EACCES [file_dac_write
]
touch: /etc/acct/yearly cannot create
```

拡張された /proc インタフェースで、truss 出力のエラーコードの後に欠如している file_dac_write 特権がレポートされます。

例 7-6 プロファイルシェルで特権の使用を検査するための ppriv コマンドの使用

次の例で、jdoe ユーザーは、役割 objadminを引き受けることができます。objadmin 役割には、Object Access Management 権利プロファイルが含まれます。この権利プロファイルによって、objadmin 役割は objadmin が所有しないファイルに関するアクセス権を変更することができます。

次の抜粋では、jdoe は、useful.script ファイルに対するアクセス権の変更に失敗しました。

```
jdoe% ls -l useful.script

-rw-r--r--  1 aloe  staff  2303 Apr 10 10:10 useful.script
jdoe%
chown objadmin useful.script

chown: useful.script: Not owner
jdoe%
ppriv -eD chown objadmin useful.script

chown[11444]: missing privilege "file_chown"
            (euid = 130, syscall = 16) needed at zfs_zaccess+0x258
chown: useful.script: Not owner
```

jdoe が objadmin 役割を引き受けると、ファイルに関するアクセス権が変更されます。

```
jdoe% su - objadmin
Password: xxxxxxxx

# ls -l useful.script
-rw-r--r--  1 aloe  staff  2303 Apr 10 10:10 useful.script

# chown objadmin useful.script
# ls -l useful.script
-rw-r--r--  1 objadmin  staff  2303 Apr 10 10:10 useful.script
# chgrp admin useful.script

# ls -l objadmin.script
-rw-r--r--  1 objadmin  admin  2303 Apr 10 10:11 useful.script
```

例 7-7 root ユーザーが所有するファイルの変更

この例では、特権エスカレーションに対する保護について説明します。詳細は、36 ページの「特権エスカレーションとカーネル特権」を参照してください。ファイルは、root ユーザーが所有します。権限の弱い objadmin 役割ではファイルの所有を変更するためにはすべての特権が必要なので、処理は失敗します。

```
jdoe% su - objadmin
Password: xxxxxxxx

# cd /etc; ls -l system
-rw-r--r--  1 root  sys   1883 Oct 10 10:20 system

# chown objadmin system
chown: system: Not owner
# ppriv -eD chown objadmin system
chown[11481]: missing privilege "ALL"
     (euid = 101, syscall = 16) needed at zfs_zaccess+0x258
chown: system: Not owner
```

♦ ♦ ♦ 第 8 章

8 Oracle Solaris 権利リファレンス

この章は、Oracle Solaris での管理権利の使用に関する参照情報を提供します。

特権を含む権利の使用については、第3章「Oracle Solaris での権利の割り当て」を参照してください。概要については、14 ページの「ユーザー権管理」および 24 ページの「プロセス権管理」を参照してください。

権利プロファイルのリファレンス

このセクションでは、いくつかの標準的な権利プロファイルについて説明します。権利プロファイルとは、承認などのセキュリティー属性、セキュリティー属性を持つコマンド、および補助権利プロファイルを使いやすく集めたものです。Oracle Solaris では権利プロファイルが多数提供されています。それらがニーズを満たさない場合は、既存のものを変更して、新しいものを作成できます。

権利プロファイルは、もっとも権限のあるものからもっとも権限のないものへと順番に割り当てられる必要があります。詳細は、38 ページの「割り当てられた権利の検索順序」を参照してください。

次に示す権利プロファイルの内容を表示するには、121 ページの「権利プロファイルの内容の表示」を参照してください。

- **System Administrator 権利プロファイル** – セキュリティーで保護された状態で接続していないほとんどのタスクにアクセスできるようにします。このプロファイルには、権限のある

役割を作成するためにいくつかのほかのプロファイルが含まれます。All 権利プロファイルは、補助権利プロファイルのリストの最後にあります。

- **Operator 権利プロファイル** – ファイルおよびオフラインメディアを管理するための限られた権利を提供します。このプロファイルには、単純な役割を作成するための補助権利プロファイルが含まれます。
- **Printer Management 権利プロファイル** – 出力を処理するための限られた数のコマンドと承認を提供します。このプロファイルは、単一の管理領域を対象とする複数のプロファイルのうちの 1 つです。
- **Basic Solaris User 権利プロファイル** – セキュリティーポリシーの範囲内でユーザーがシステムを使用できるようにします。このプロファイルは、デフォルトで `policy.conf` ファイル内にリストされます。Basic Solaris User 権利プロファイルを使用するときは、サイトのセキュリティー要件を考慮する必要があります。高いセキュリティーを必要とするサイトでは、このプロファイルを `policy.conf` ファイルから削除するか、または Stop 権利プロファイルを割り当てることをお勧めします。Basic Solaris User 権利プロファイルの実装については、例6-16「ユーザーの権利プロファイル内のセキュリティー属性を持つコマンドの一覧表示」を参照してください。
- **Console User 権利プロファイル** – ワークステーション所有者の場合、コンピュータの前に着席しているユーザーが、承認、コマンド、およびアクションにアクセスできるようにします。
- **All 権利プロファイル** – 役割に対して、セキュリティー属性を持たないコマンドにアクセスできるようにします。このプロファイルは、限られた権限を持つユーザーに適している場合があります。
- **Stop 権利プロファイル** – それ以降のプロファイルの評価を停止する特殊な権利プロファイルです。このプロファイルは、`policy.conf` ファイル内の `AUTHS_GRANTED`、`PROFS_GRANTED`、および `CONSOLE_USER` 変数の評価を中止します。このプロファイルを使用すると、役割とユーザーに制限付きプロファイルシェルを提供できます。

注記 - Stop プロファイルは、特権の割り当てに間接的な影響を及ぼします。Stop プロファイルのあとにリストされた権利プロファイルは評価されません。したがって、そのようなプロファイル内に特権が指定されているコマンドは有効ではありません。例3-25「明示的に割り当てられた権利への管理者の制限」を参照してください。

それぞれの権利プロファイルには、関連するヘルプファイルが用意されています。ヘルプファイルは、HTML 形式で、カスタマイズが可能です。ヘルプファイルは、`/usr/lib/help/profiles/locale/C` ディレクトリにあります。

権利プロファイルの内容の表示

権利プロファイルの内容を 3 つのビューで表示できます。

- `getent` コマンドを使用すると、システム上のすべての権利プロファイルの内容を表示できます。出力例については、第6章「Oracle Solaris の権利の一覧表示」を参照してください。
- `profiles -p "`*Profile Name*`" info` コマンドを使用すると、特定の権利プロファイルの内容を表示できます。
- `profiles -l` *account-name* コマンドを使用すると、特定のユーザーまたは役割に割り当てられている権利プロファイルの内容を表示できます。

詳細は、第6章「Oracle Solaris の権利の一覧表示」および `getent`(1M) と `profiles`(1) のマニュアルページを参照してください。

承認のリファレンス

*承認*は、役割またはユーザーに付与できる個別の権利です。準拠したアプリケーションによって承認が確認されてから、ユーザーはアプリケーションまたはアプリケーションの特定の操作へのアクセス権を取得します。

承認はユーザーレベルであり、したがって拡張可能です。承認を必要とするプログラムを作成し、承認をシステムに追加し、これらの承認の権利プロファイルを作成して、その権利プロファイルを、プログラムの使用が許可されているユーザーまたは役割に割り当てることができます。

承認の命名規則

承認には、内部で使用される名前があります。たとえば `solaris.system.date` は承認の名前です。また、承認にはグラフィカルユーザーインタフェース (GUI) に表示される短い説明もあります。たとえば、`Set Date & Time` は `solaris.system.date` 承認の説明です。

慣例上、承認名はインターネット名とは逆の順序になり、サプライヤ、被認証者領域、任意の下位領域、および承認の機能で構成されます。承認名の区切り文字はドット (.) です。たとえば、`com.xyzcorp.device.access` のように指定します。この規則の例外として、インターネット名の代わりに接頭辞 `solaris` を使用する、Oracle からの承認があります。システム管理者は、

承認を階層方式で適用することができます。ワイルドカード (*) は、ドットの右側の任意の文字列を表すことができます。

承認の使用方法の例として、Network Link Security 権利プロファイルには `solaris.network.link.security` 承認のみが含まれるのに対して、Network Security 権利プロファイルには補助プロファイルとしての Network Link Security プロファイルに加え、`solaris.network.*` および `solaris.smf.manage.ssh` 承認が含まれます。

承認での委託権限

接尾辞が `delegate` の承認が許可されたユーザーまたは役割は、割り当てられている承認のうち同じ接頭辞で始まるものを、ほかのユーザーに委任できます。

`solaris auth.delegate` 承認では、ユーザーまたは役割が、これらの委任ユーザーまたは役割が割り当てられている任意の承認をほかのユーザーに委任できます。たとえば、`solaris auth.delegate` と `solaris.network.wifi.wep` の承認を持つ役割は、`solaris.network.wifi.wep` 承認をほかのユーザーまたは役割に委任できます。

権利データベース

次のデータベースには、Oracle Solaris の権利のデータが格納されます。

- **拡張ユーザー属性のデータベース** (`user_attr`) – ユーザーと役割を、ほかのキーワードの中でも承認、特権、権利プロファイルに関連付けます。
- **権利プロファイル属性のデータベース** (`prof_attr`) – 権利プロファイルを定義し、そのプロファイルに割り当てられている承認、特権、およびキーワードを一覧表示し、関連するヘルプファイルを識別します
- **承認属性のデータベース** (`auth_attr`) – 承認とその属性を定義し、関連するヘルプファイルを指定します
- **実行属性のデータベース** (`exec_attr`) – 特定の権利プロファイルに割り当てられたセキュリティー属性を持つコマンドを識別します

`policy.conf` データベースには、すべてのユーザーに適用される承認、特権、および権利プロファイルが含まれます。詳細については、126 ページの「`policy.conf` ファイル」を参照してください。

権利データベースおよびネームサービス

権利データベースのネームサービススコープは、ネームサービススイッチ svc:/system/name-service/switch の SMF サービスで定義されます。このサービス内での権利データベースのプロパティーは、auth_attr、password、および prof_attr です。password プロパティーは、passwd および user_attr データベースに対するネームサービスの優先順位を設定します。prof_attr プロパティーは、prof_attr および exec_attr データベースに対するネームサービスの優先順位を設定します。

次の出力では、auth_attr、password、および prof_attr エントリは一覧表示されていません。したがって、権利データベースは files ネームサービスを使用しています。

```
# svccfg -s name-service/switch listprop config
config                          application
config/value_authorization      astring       solaris.smf.value.name-service.switch
config/default                  astring       files
config/host                     astring       "files ldap dns"
config/printer                  astring       "user files ldap"
```

user_attr データベース

user_attr データベースには、ユーザーと役割の情報が格納されます。これらの情報は、passwd および shadow データベースによって利用されます。*attr* フィールドにはセキュリティー属性が含まれ、*qualifier* フィールドには、セキュリティー属性の効果を 1 つのシステムまたはシステムのグループに限定または制限する属性が含まれています。

attr フィールドのセキュリティー属性は、roleadd、rolemod、useradd、usermod、および profiles コマンドを使用して設定できます。ローカルに設定するか、または LDAP ネーミングスコープ内で設定できます。

- ユーザーの場合、roles キーワードで 1 つ以上の定義された役割を割り当てます。
- 役割の場合、roleauth キーワードの値を user にすると、その役割は役割のパスワードではなくユーザーのパスワードを使用して認証できるようになります。デフォルトでは、この値は role です。
- ユーザーまたは役割の場合、次の属性を設定できます。
  - access_times キーワード – 指定されているアプリケーションとサービスにアクセスできる日と時間を指定します。詳細は、getaccess_times(3C) のマニュアルページを参照してください。

- access_tz キーワード – access_times エントリの時間を解釈するときに使用する時間帯を指定します。詳細は、pam_unix_account(5) のマニュアルページを参照してください。
- audit_flags キーワード – 監査マスクを変更します。詳細は、audit_flags(5) のマニュアルページを参照してください。
- auths キーワード – 承認を割り当てます。詳細は、auths(1) のマニュアルページを参照してください。
- auth_profiles キーワード – 認証権利プロファイルを割り当てます。詳細は、profiles(1) のマニュアルページを参照してください。
- defaultpriv キーワード – デフォルトの特権の基本セットに特権を追加するか、または特権を削除します。
- limitpriv キーワード – デフォルトの特権の制限セットに特権を追加するか、または特権を削除します。

  defaultpriv および limitpriv 特権は、ユーザーの初期プロセスに割り当てられているため常に有効です。詳細は、privileges(5) のマニュアルページと 28 ページの「特権の実装方法」を参照してください。
- idlecmd キーワード – idletime に達したあとでユーザーをログアウトし、画面をロックします。
- idletime キーワード – キーボードアクティビティーが行われなかったあとでシステムが使用可能である時間を設定します。idlecmd の値を指定するときには idletime を設定します。
- lock_after_retries キーワード –値が yes の場合、再試行回数が /etc/default/login ファイルで許可されている回数を超えると、システムはロックされます。詳細は、login(1) のマニュアルページを参照してください。
- profilesキーワード – 権利プロファイルを割り当てます。詳細は、profiles(1) のマニュアルページを参照してください。
- project キーワード - デフォルトのプロジェクトを追加します。詳細は、project(4) のマニュアルページを参照してください。

注記 - access_times および access_tz 属性は PAM 属性であるため、認証中に検査されます。したがって、ユーザーまたは役割に直接割り当てるか、または認証権利プロファイルに含める必要があります。これらは通常の権利プロファイルでは無視されます。

修飾属性は、LDAP ネーミングスコープ内のユーザーと役割に対してのみ設定できます。これらの修飾子により、権利プロファイルなどのユーザーと役割の属性割り当てが 1 つまたは複数のシステムに限定されます。例については、useradd(1M) および user_attr(4) のマニュアルページを参照してください。

修飾子は host と netgroup です。

- host 修飾子 – ユーザーまたは役割が指定されたアクションを実行できるシステムを識別します。
- netgroup 修飾子 – ユーザーまたは役割が指定されたアクションを実行できるシステムを一覧表示します。host 割り当ては、netgroup よりも優先されます。

詳細は、user_attr(4) のマニュアルページを参照してください。このデータベースの内容を表示するには、getent user_attr コマンドを使用します。詳細は、getent(1M) のマニュアルページと 第6章「Oracle Solaris の権利の一覧表示」を参照してください。

auth_attr データベース

auth_attr データベースには、承認定義が格納されます。承認は、ユーザー、役割、権利プロファイルに割り当てることができます。承認を権利プロファイルに配置してから、その権利プロファイルを役割またはユーザーに割り当てる方法が推奨されます。

このデータベースの内容を表示するには、getent auth_attr コマンドを使用します。詳細は、getent(1M) のマニュアルページと 第6章「Oracle Solaris の権利の一覧表示」を参照してください。

prof_attr データベース

prof_attr データベースには、権利プロファイルに割り当てる名前、説明、ヘルプファイルの場所、特権、および承認が格納されます。権利プロファイルに割り当てられたコマンドとセキュリティー属性は、exec_attr データベースに格納されます。詳細については、126 ページの「exec_attr データベース」を参照してください。

詳細は、prof_attr(4) のマニュアルページを参照してください。このデータベースの内容を表示するには、getent exec_attr コマンドを使用します。詳細は、getent(1M) のマニュアルページと 第6章「Oracle Solaris の権利の一覧表示」を参照してください。

exec_attr データベース

exec_attr データベースでは、成功するためにセキュリティー属性を必要とするコマンドが定義されます。このコマンドは、権利プロファイルの一部です。セキュリティー属性を指定したコマンドは、プロファイルが割り当てられている役割またはユーザーが実行できます。

詳細は、exec_attr(4) のマニュアルページを参照してください。このデータベースの内容を表示するには、getent コマンドを使用します。詳細は、getent(1M) のマニュアルページと 第6章「Oracle Solaris の権利の一覧表示」を参照してください。

policy.conf ファイル

/etc/security/policy.conf ファイルは、特定の権利プロファイル、特定の承認、および特定の特権をすべてのユーザーに付与する方法を定義します。ファイル内の関連するエントリは、*key=value* のペアから構成されます。

- AUTHS_GRANTED=*authorizations* – 1 つまたは複数の承認を示します。
- AUTH_PROFS_GRANTED=*rights profiles* – 1 つまたは複数の認証権利プロファイルを示します。
- PROFS_GRANTED=*rights profiles* – 1 つまたは複数の未認証の権利プロファイルを示します。
- CONSOLE_USER=Console User – Console User 権利プロファイルを示します。このプロファイルは、便利な承認セットとともにコンソールユーザーに提供されます。このプロファイルはカスタマイズできます。
- PRIV_DEFAULT=*privileges* – 1 つまたは複数の特権を示します。
- PRIV_LIMIT=*privileges* – すべての特権を示します。

次の例では、policy.conf データベースの権利値をいくつか示します。

```
##
AUTHS_GRANTED=
AUTH_PROFS_GRANTED=
CONSOLE_USER=Console User
PROFS_GRANTED=Basic Solaris User
#PRIV_DEFAULT=basic
#PRIV_LIMIT=all
```

権利管理コマンド

このセクションには、権利の管理に使用するコマンドのリストを示します。承認を使用してアクセス権を制御できるコマンドの表も含まれています。

承認、権利プロファイル、および役割を管理するコマンド

次の表に示すコマンドは、ユーザープロセスに対する権利を取得および設定します。

表 8-1 権利管理コマンド

コマンド	説明
auths(1)	ユーザーの承認を表示します。新しい承認を作成します。
getent(1M)	権利データベースの内容を一覧表示します。
nscd(1M)	権利データベースをキャッシュする場合に有用なネームサービスキャッシュデーモン。svcadm コマンドを使用してデーモンを再起動します。
pam_roles(5)	PAM 用の役割アカウント管理モジュール。役割を引き受けるための承認を確認します。
pam_unix_account(5)	PAM 用 の UNIX アカウント管理モジュール。時間制約や非アクティブな状態などのアカウントの制限を調べます。
pfbash(1)	権利を評価できるプロファイルシェルプロセスの作成に使用されます。
pfedit(1M)	管理ファイルの編集に使用します。
pfexec(1)	セキュリティー属性を持つコマンドの実行に使用されます。
policy.conf(4)	システムセキュリティーポリシーの構成ファイル。与えられている承認、与えられている特権、およびその他のセキュリティー情報を一覧表示します。
profiles(1)	指定したユーザーの権利プロファイルを表示します。権利プロファイルを作成または変更します。
roles(1)	指定されたユーザーが引き受けられる役割を表示します。
roleadd(1M)	役割をローカルシステムまたは LDAP ネットワークに追加します。
roleadd(1M)	役割をローカルシステムまたは LDAP ネットワークに追加します。
rolemod(1M)	ローカルシステムまたは LDAP ネットワーク上で役割のプロパティーを変更します。
userattr(1)	ユーザーまたは役割アカウントに割り当てられている特定の権利の値を表示します。
useradd(1M)	ユーザーアカウントをシステムまたは LDAP ネットワークに追加します。ユーザーのアカウントに役割を割り当てるには、-R オプションを使用します。

コマンド	説明
userdel(1M)	ユーザーのログインをシステムまたは LDAP ネットワークから削除します。
usermod(1M)	システム上のユーザーのアカウントプロパティーを変更します。

承認を必要とする特別なコマンド

次の表では、承認を使用して Oracle Solaris システムのコマンドオプションを制限する方法を示します。承認の詳細は、121 ページの「承認のリファレンス」を参照してください。

表 8-2 コマンドおよび関連する承認

コマンド	承認の要件
at(1)	すべてのオプションで solaris.jobs.user が必要です (at.allow ファイルおよび at.deny ファイルがない場合)
atq(1)	すべてのオプションで solaris.jobs.admin が必要です
cdrw(1)	すべてのオプションで solaris.device.cdrw が必要であり、これは policy.conf ファイルでデフォルトで付与されます。
crontab(1)	ジョブを送信するオプションの場合は solaris.jobs.user が必要です (crontab.allow および crontab.deny ファイルがない場合) ほかのユーザーの crontab ファイルを一覧表示または変更する場合は、solaris.jobs.admin が必要です
allocate(1)	デバイスを割り当てる場合は、solaris.device.allocate (または、device_allocate ファイルに指定されている別承認) が必要です ほかのユーザーにデバイスを割り当てる場合 (F オプション) は、solaris.device.revoke (または -device_allocate ファイルに指定されている別の承認) が必要です
deallocate(1)	ほかのユーザーのデバイスの割り当てを解除する場合は、solaris.device.allocate (または device_allocate ファイルに指定されている別の承認) が必要です 指定したデバイス (-F オプション) またはすべてのデバイス (-I オプション) の割り当てを強制的に解除する場合は、solaris.device.revoke (または、device_allocate に指定されている別承認) が必要です
list_devices(1)	ほかのユーザーのデバイスを一覧表示する場合 (-U オプション) は、solaris.device.revoke が必要です
roleadd(1M)	役割を作成するには、solaris.user.manage が必要です。初期パスワードを設定するには、solaris.account.activate が必要です。アカウントロックやパスワードの有効期限などのパスワードポリシーを設定するには、solaris.account.setpolicy が必要です。
roledel(1M)	パスワードを削除するには、solaris.passwd.assign 承認が必要です。

コマンド	承認の要件
rolemod(1M)	パスワードを変更するには、solaris.passwd.assign 承認が必要です。アカウントロックやパスワードの有効期限などのパスワードポリシーを変更するには、solaris.account.setpolicy が必要です。
sendmail(1M)	メールサブシステム機能にアクセスするには、solaris.mail が必要です。メールキューを表示するには、solaris.mail.mailq が必要です
useradd(1M)	ユーザーを作成するには、solaris.user.manage が必要です。初期パスワードを設定するには、solaris.account.activate が必要です。アカウントロックやパスワードの有効期限などのパスワードポリシーを設定するには、solaris.account.setpolicy が必要です。
userdel(1M)	パスワードを削除するには、solaris.passwd.assign 承認が必要です。
usermod(1M)	パスワードを変更するには、solaris.passwd.assign 承認が必要です。アカウントロックやパスワードの有効期限などのパスワードポリシーを変更するには、solaris.account.setpolicy が必要です。

特権のリファレンス

プロセスを制限する特権は、カーネル内に実装され、コマンド、ユーザー、役割、またはシステムレベルでプロセスを制限できます。

特権処理のためのコマンド

次の表に、特権の処理に使用できるコマンドのリストを示します。

表 8-3 特権処理のためのコマンド

目的	コマンド	マニュアルページ
特権失敗をデバッグします	`ppriv -eD` *failed-operation*	ppriv(1)
システム上の特権を一覧表示します	`ppriv -l`	ppriv(1)
特権とその説明を一覧表示します	`ppriv -lv` *priv*	ppriv(1)
UID、プロセス、またはポートに関する拡張特権ポリシーを一覧表示します	`ppriv -lv` *extended-policy*	ppriv(1)
プロセスの特権を検査します	`ppriv -v` *pid*	ppriv(1)
拡張特権ポリシーを UID、プロセス、またはポートに追加します	`ppriv -r` *rule*	privileges(5)
プロセス特権を設定します	`ppriv -s` *spec*	ppriv(1)

目的	コマンド	マニュアルページ
拡張特権ポリシールールを削除します	`ppriv -X` *rule*	privileges(5)
特権を権利プロファイルに割り当てます	`profiles -p` *profile-name*	profiles(1)
特権を新しい役割に割り当てます	`roleadd -K defaultpriv=`	roleadd(1M)
特権を既存の役割に追加します	`rolemod -K defaultpriv+=`	rolemod(1M)
特権を新しいユーザーに割り当てます	`useradd -K defaultpriv=`	useradd(1M)
特権を既存のユーザーに追加します	`usermod -K defaultpriv+=`	usermod(1M)
デバイスポリシーをデバイスに追加します	`add_drv -p` *policy driver*	add_drv(1M)
デバイスポリシーを設定します	`devfsadm`	devfsadm(1M)
デバイスポリシーを表示します	`getdevpolicy`	getdevpolicy(1M)
オープンデバイス上のデバイスポリシーを更新します	`update_drv -p` *policy driver*	update_drv(1M)

特権情報が含まれるファイル

`policy.conf` および `syslog.conf` ファイルには、特権に関する情報が含まれています。

- `/etc/security/policy.conf` には次の特権情報が含まれています。
  - `PRIV_DEFAULT` – システムに対する特権の継承可能セット
  - `PRIV_LIMIT` – システムに対する特権の制限セット

  詳細は、policy.conf(4) のマニュアルページを参照してください。
- `/etc/syslog.conf` は、特権デバッグに関連するデバッグメッセージのシステムログファイルです。デバッグメッセージのパスは `priv.debug` エントリに設定されています。

  詳細は、syslog.conf(4) のマニュアルページを参照してください。

監査レコードの特権アクション

特権の使用は監査することができます。プロセスで特権が使用される場合は常に、`upriv` 監査トークン内の監査トレールに特権の使用が記録されます。特権の名前がレコードに含まれる場合、テキスト形式が使用されます。次の監査イベントにより、特権の使用が記録されます。

- `AUE_SETPPRIV` **監査イベント** – 特権セットが変更されたときに監査レコードを生成します。`AUE_SETPPRIV` 監査イベントは `pm` クラスにあります。

- AUE_MODALLOCPRIV **監査イベント** – カーネルの外部から特権が追加されたときに監査レコードを生成します。AUE_MODALLOCPRIV 監査イベントは ad クラスにあります。
- AUE_MODDEVPLCY **監査イベント** – デバイスポリシーが変更されたときに監査レコードを生成します。AUE_MODDEVPLCY 監査イベントは ad クラスにあります。
- AUE_PFEXEC **監査イベント** – pfexec() が有効になっている execve() の呼び出しが行われたときに監査レコードを生成します。AUE_PFEXEC 監査イベントは、as、ex、ps、および ua 監査クラスにあります。特権の名前は、監査レコードに含まれます。

基本セットに含まれる特権が正常に使用される場合は、監査されません。ユーザーの基本セットから削除された基本特権の使用を試みる場合、監査されます。

セキュリティー用語集

アクセス制御リスト (ACL) アクセス制御リスト (ACL) を使用すると、従来の UNIX ファイル保護よりもきめ細かな方法でファイルセキュリティーを確立できます。たとえば、特定のファイルにグループ読み取り権を設定し、そのグループ内の 1 人のメンバーだけにそのファイルへの書き込み権を与えることが可能です。

アプリケーションサーバー ネットワークアプリケーションサーバーを参照してください。

アルゴリズム 暗号化アルゴリズム。これは、入力を暗号化 (ハッシング) する既成の再帰的な計算手続きです。

暗号化アルゴリズム アルゴリズムを参照してください。

暗号化フレームワークにおけるポリシー Oracle Solaris の暗号化フレームワーク機能では、ポリシーは既存の暗号化メカニズムの無効化です。無効に設定されたメカニズムは使用できなくなります。暗号化フレームワークにおけるポリシーにより、プロバイダ (DES など) からの特定のメカニズム (`CKM_DES_CBC`など) を使用できなくなることがあります。

インスタンス 主体名の 2 番目の部分。インスタンスは、主体の主ノード指定します。サービス主体の場合、インスタンスは必ず指定する必要があります。`host/central.example.com` にあるように、インスタンスはホストの完全修飾ドメイン名です。ユーザー主体の場合、インスタンスは省略することができます。ただし、`jdoe` と `jdoe/admin` は、一意の主体です。プライマリ、主体名、サービス主体、ユーザー主体も参照してください。

オーセンティケータ オーセンティケータは、KDC にチケットを要求するときおよびサーバーにサービスを要求するときに、クライアントから渡されます。オーセンティケータには、クライアントとサーバーだけが知っているセッション鍵を使用して生成された情報が含まれます。オーセンティケータは、最新の識別として検査され、そのトランザクションが安全であることを示します。これをチケットとともに使用すると、ユーザー主体を認証できます。オーセンティケータには、ユーザーの主体名、ユーザーのホストの IP アドレス、タイムスタンプが含まれます。チケットとは異なり、オーセンティケータは一度しか使用できません。通常、サービスへのアクセスが要求されたときに使用されます。オーセンティケータは、そのクライアントとそのサーバーのセッション鍵を使用して暗号化されます。

鍵 1. 一般には、次に示す 2 種類の主要鍵のどちらか一方です。

- *対称鍵* – 復号化鍵とまったく同じ暗号化鍵。対称鍵はファイルの暗号化に使用されます。

- *非対称鍵*または*公開鍵* – Diffie-Hellman や RSA などの公開鍵アルゴリズムで使用される鍵。公開鍵には、1 人のユーザーしか知らない非公開鍵、サーバーまたは一般リソースによって使用される公開鍵、およびこれらの 2 つを組み合わせた公開鍵と非公開鍵のペアがあります。非公開鍵は、「秘密鍵」とも呼ばれます。公開鍵は、「共有鍵」や「共通鍵」とも呼ばれます。

2. キータブファイルのエントリ (主体名)。キータブファイルも参照してください。
3. Kerberos では暗号化鍵であり、次の 3 種類があります。

- 「非公開鍵」 – 主体と KDC によって共有される暗号化鍵。システムの外部に配布されます。非公開鍵も参照してください。
- 「サービス鍵」– 非公開鍵と同じ目的で使用されますが、この鍵はサーバーとサービスによって使用されます。サービス鍵も参照してください。
- 「セッション鍵」 – 一時的な暗号化鍵。2 つの主体の間で使用され、その有効期限は 1 つのログインセッションの期間に制限されます。セッション鍵も参照してください。

仮想プライベートネットワーク (VPN) 暗号化とトンネルを使用して、セキュアな通信を提供するネットワーク。公開ネットワークを通してユーザーを接続します。

関係 `kdc.conf` または `krb5.conf` ファイルに定義される構成変数または関係の 1 つ。

監査トレール すべてのホストから収集した一連の監査ファイル。

監査ファイル バイナリ形式の監査ログ。監査ファイルは、監査ファイルシステム内に個別に格納されます。

監査ポリシー どの監査イベントが記録されるかを決定する設定であり、大域の設定とユーザーごとの設定があります。大域の設定は監査サービスに適用され、一般にどのオプション情報を監査トレールに含めるかを決定します。2 つの設定 `cnt` と `ahlt` は、監査キューがいっぱいになった時点でのシステムの処理を決定します。たとえば、各監査レコードにシーケンス番号を含めるように監査ポリシーを設定できます。

キーストア キーストアは、アプリケーションによる取得のために、パスワード、パスフレーズ、証明書、およびその他の認証オブジェクトを保持します。キーストアはテクノロジ固有にすることも、複数のアプリケーションで使用される場所にすることもできます。

キータブファイル 1 つまたは複数の鍵 (主体) が含まれるキーテーブル。ホストまたはサービスとキータブファイルとの関係は、ユーザーとパスワードの関係と似ています。

基本セット ログイン時にユーザーのプロセスに割り当てられる一連の特権。変更されていないシステムの場合、各ユーザーの初期の継承可能セットはログイン時の基本セットと同じです。

機密性 プライバシを参照してください。

強化 ホストが本来抱えるセキュリティー上の脆弱性を解決するためにオペレーティングシステムのデフォルト構成を変更すること。

許可されたセット プロセスによって使用できる一連の特権。

クライアント 狭義では、`rlogin` を使用するアプリケーションなど、ユーザーの代わりにネットワークサービスを使用するプロセスを指します。サーバー自身が他のサーバーやサービスのクライアントになる場合もあります。

広義では、a) Kerberos 資格を受け取り、b) サーバーから提供されたサービスを利用するホストを指します。

広義では、サービスを使用する主体を指します。

クライアント主体 (RPCSEC_GSS API) RPCSEC_GSS で保護されたネットワークサービスを使用するクライアント (ユーザーまたはアプリケーション)。クライアント主体名は、`rpc_gss_principal_t` 構造体の形式で格納されます。

クロックスキュー Kerberos 認証システムに参加しているすべてのホスト上の内部システムクロックに許容できる最大時間。参加しているホスト間でクロックスキューを超過すると、要求が拒否されます。クロックスキューは、`krb5.conf` ファイルに指定できます。

継承可能セット プロセスが `exec` の呼び出しを通して継承できる一連の特権。

権利 すべての機能を持つスーパーユーザーの代替アカウント。ユーザー権利の管理およびプロセス権利の管理で、組織はスーパーユーザーの特権を分割して、ユーザーまたは役割に割り当てることができます。Oracle Solaris の権利は、カーネル特権、承認、または特定の UID や GID としてプロセスを実行する機能として実装されています。権利は権利プロファイルおよび役割で収集できます。

権利プロファイル プロファイルとも呼ばれます。役割またはユーザーに割り当てることができるセキュリティーオーバーライドの集合。権利プロファイルには、承認、特権、セキュリティー属性が割り当てられたコマンド、および補足プロファイルと呼ばれるその他の権利プロファイルを含めることができます。

権利ポリシー コマンドに関連付けられるセキュリティーポリシー。現在、Oracle Solaris で有効なポリシーは `solaris` です。`solaris` ポリシーでは、特権と拡張特権ポリシー、承認、および `setuid` セキュリティー属性が認識されます。

公開オブジェクト `root` ユーザーによって所有され、すべてのユーザーが読み取ることのできるファイル。たとえば、`/etc` ディレクトリ内のファイルです。

公開鍵技術のポリシー 鍵管理フレームワーク (KMF) におけるポリシーは、証明書の使用を管理します。KMF ポリシーデータベースを使えば、KMF ライブラリによって管理される鍵や証明書の使用に、制約を設けることができます。

公開鍵の暗号化 暗号化スキームの 1 つ。各ユーザーが 1 つの公開鍵と 1 つの非公開鍵を所有します。公開鍵の暗号化では、送信者は受信者の公開鍵を使用してメッセージを暗号化し、受信者は非公開

鍵を使用してそれを復号化します。Kerberos サービスは非公開鍵システムです。非公開鍵の暗号化も参照してください。

更新可能チケット 有効期限の長いチケットは、セキュリティーを低下させることがあるため、「更新可能」チケットに指定することができます。更新可能チケットには 2 つの有効期限があります。a) チケットの現在のインスタンスの有効期限と、b) 任意のチケットの最長有効期限です。クライアントがチケットの使用を継続するときは、最初の有効期限が切れる前にチケットの有効期限を更新します。たとえば、すべてのチケットの最長有効期限が 10 時間のときに、あるチケットが 1 時間だけ有効だとします。このチケットを保持するクライアントが 1 時間を超えて使用する場合は、チケットの有効期限を更新する必要があります。チケットが最長有効期限に達すると、チケットの有効期限が自動的に切れ、それ以上更新できなくなります。

コンシューマ Oracle Solaris の暗号化フレームワーク機能では、コンシューマはプロバイダが提供する暗号化サービスのユーザー。コンシューマになりえるものとして、アプリケーション、エンドユーザー、カーネル処理などが挙げられます。Kerberos、IKE、IPsec などはコンシューマの例です。プロバイダの例は、プロバイダを参照してください。

サーバー ネットワーククライアントにリソースを提供する主体。たとえば、システム `central.example.com` に `ssh` で接続する場合、そのシステムが `ssh` サービスを提供するサーバーになります。サービス主体も参照してください。

サーバー主体 (RPCSEC_GSS API) サービスを提供する主体。サーバー主体は、*service*@*host* という書式で ASCII 文字列として格納されます。クライアント主体も参照してください。

サービス 1. ネットワーククライアントに提供されるリソース。多くの場合、複数のサーバーから提供されます。たとえば、マシン `central.example.com` に `rlogin` で接続する場合、そのマシンが `rlogin` サービスを提供するサーバーになります。

2. 認証以外の保護レベルを提供するセキュリティーサービス (整合性またはプライバシ)。整合性とプライバシも参照してください。

サービス鍵 サービス主体と KDC によって共有される暗号化鍵。システムの外部に配布されます。鍵も参照してください。

サービス主体 1 つまたは複数のサービスに Kerberos 認証を提供する主体。サービス主体では、プライマリ名はサービス名 (`ftp` など) で、インスタンスはサービスを提供するシステムの完全指定ホスト名になります。ホスト主体、ユーザー主体も参照してください。

最小化 サーバーを稼働させる上で必要な最小限のオペレーティングシステムをインストールすること。サーバーの処理に直接影関係がないソフトウェアはすべて、インストールされないか、あるいはインストール後削除されます。

最少特権 指定されたプロセスにスーパーユーザー権限のサブセットのみを提供するセキュリティーモデル。最小特権モデルでは、通常のユーザーに、ファイルシステムのマウントやファイルの所有権の変更などの個人の管理タスクを実行できる十分な特権を割り当てます。これに対して、プロセスは、スーパーユーザーの完全な権限 (つまり、すべての特権) ではなく、タスクを完了するために必要な特権のみで実行されます。バッファーオーバーフローなどのプログラミングエラーによ

る損害を、保護されたシステムファイルの読み取りまたは書き込みやマシンの停止などの重要な機能にはアクセスできない root 以外のユーザーに封じ込めることができます。

最少特権の原則 最少特権を参照してください。

再認証 コンピュータ操作を実行するためにパスワードを指定する際の要件。通常、sudo 操作では再認証が必要です。認証済み権利プロファイルには、再認証が必要なコマンドを含めることができます。認証済み権利プロファイルを参照してください。

シード 乱数生成のスターター (元になる値)。この値から生成が開始されます。このスターターがランダムソースから生じる場合、このシードは「ランダムシード」と呼ばれます。

資格 チケットと照合セッション鍵を含む情報パッケージ。主体の識別情報を認証するときに使用します。チケットとセッション鍵も参照してください。

資格キャッシュ KDC から受信した資格を含むストレージ領域。通常はファイルです。

主体 1. ネットワーク通信に参加する、一意の名前を持つ「クライアントまたはユーザー」あるいは「サーバーまたはサービス」のインスタンス。Kerberos トランザクションでは、主体 (サービス主体とユーザー主体) 間、または主体と KDC の間で対話が行われます。つまり、主体とは、Kerberos がチケットを割り当てることができる一意のエンティティーのことです。主体名、サービス主体、ユーザー主体も参照してください。

2. (RPCSEC_GSS API) クライアント主体、サーバー主体を参照してください。

主体名 1. 主体の名前。書式は、*primary/instance@REALM*。インスタンス、プライマリ、レルムも参照してください。

2.(RPCSEC_GSS API) クライアント主体、サーバー主体を参照してください。

承認 1. Kerberos では、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オブジェクト、各オブジェクトに許可するアクセスの種類を決定するプロセス。

2. ユーザー権利の管理で、役割またはユーザーに割り当てる (権利プロファイルに埋め込む) ことができる一連の操作 (そうしない場合、セキュリティーポリシーによって拒否される) を実行するための権利。承認はカーネルではなく、ユーザーアプリケーションレベルで適用されます。

初期チケット 直接発行されるチケット (既存のチケット許可チケットは使用されない)。パスワードを変更するアプリケーションなどの一部のサービスでは、クライアントが非公開鍵を知っていることを確認するために、「初期」と指定されたチケットを要求することができます。初期チケットを使用した検査は、クライアントが最近認証されたことを証明するときに重要になります。チケット許可チケットの場合は、取得してから時間が経過していることがあります。

信頼できるユーザー ある程度の信頼レベルで管理タスクを実行できるように決定されたユーザー。一般に、管理者は最初に信頼できるユーザーのログインを作成してから、ユーザーの信頼および能力レベルに合致した管理者権利を割り当てます。その後、これらのユーザーはシステムの構成および保守を支援します。*特権ユーザー*とも呼ばれます。

スーパーユーザーモデル コンピュータシステムにおける典型的な UNIX セキュリティーモデル。スーパーユーザーモデルでは、管理者は絶対的なシステム制御権を持ちます。一般に、マシン管理のために 1 人のユーザーがスーパーユーザー (root) になり、すべての管理作業を行える状態となります。

スキャンエンジン 既知のウイルスがないかどうかファイルを検査する、外部ホスト上に存在するサードパーティーのアプリケーション。

スレーブ KDC マスター KDC のコピー。マスター KDC のほとんどの機能を実行できます。各レルムには通常、いくつかのスレーブ KDC (と 1 つのマスター KDC) を配置します。KDC、マスター KDCも参照してください。

制限セット プロセスとその子プロセスでどの特権が利用できるかを示す上限。

整合性 ユーザー認証に加えて、暗号チェックサムを使用して、転送されたデータの有効性を提供するセキュリティーサービス。認証、プライバシも参照してください。

責務分離 最少特権の概念の一部。責務分離により、1 人のユーザーが、トランザクションを完了するためのすべての操作を実行または承認することが回避されます。たとえば、RBAC では、セキュリティーオーバーライドの割り当てからログインユーザーの作成を分離できます。1 つの役割がユーザーを作成します。個別の役割により、権利プロファイル、役割、特権などのセキュリティー属性を既存のユーザーに割り当てることができます。

セキュリティーサービス サービスを参照してください。

セキュリティー属性 セキュリティーポリシーをオーバーライドし、スーパーユーザー以外のユーザーによって実行されても成功する管理コマンドを有効にします。スーパーユーザーモデルでは、`setuid root` プログラムと `setgid` プログラムがセキュリティー属性です。これらの属性がコマンドで指定されると、そのコマンドがどのようなユーザーによって実行されているかにかかわらず、コマンドは正常に処理されます。特権モデルでは、セキュリティー属性として `setuid root` プログラムがカーネル特権およびその他の権利によって置き換えられます。特権モデルは、スーパーユーザーモデルと互換性があります。このため、特権モデルは `setuid` プログラムと `setgid` プログラムをセキュリティー属性として認識します。

セキュリティーフレーバ フレーバを参照してください。

セキュリティーポリシー ポリシーを参照してください。

セキュリティーメカニズム メカニズムを参照してください。

セッション鍵 認証サービスまたはチケット認可サービスによって生成される鍵。セッション鍵は、クライアントとサービス間のトランザクションのセキュリティーを保護するために生成されます。セッション鍵の有効期限は、単一のログインセッションに制限されます。鍵も参照してください。

ソフトウェアプロバイダ Oracle Solaris の暗号化フレームワーク機能では、暗号化サービスを提供するカーネルソフトウェアモジュールまたは PKCS #11 ライブラリ。プロバイダも参照してください。

ダイジェスト メッセージダイジェストを参照してください。

単一システムイメージ 単一システムイメージは、同じネームサービスを使用する一連の検査対象システムを記述するために、Oracle Solaris 監査で使用されます。これらのシステムは監査レコードを中央の監査サーバーに送信しますが、その監査サーバー上では、それらのレコードがまるで 1 つのシステムからやってきたかのように、レコードの比較を行えます。

遅延チケット 遅延チケットは、作成されても指定された時点まで有効になりません。このようなチケットは、夜遅く実行するバッチジョブなどのために効果的です。そのチケットは盗まれても、バッチジョブが実行されるまで使用できないためです。遅延チケットは、無効チケットとして発行され、a) 開始時間を過ぎて、b) クライアントが KDC による検査を要求したときに有効になります。遅延チケットは通常、チケット認可チケットの有効期限まで有効です。ただし、その遅延チケットが「更新可能」と指定されている場合、その有効期限は通常、チケット認可チケットの有効期限に設定されます。無効チケット、更新可能チケットも参照してください。

チケット ユーザーの識別情報をサーバーやサービスに安全に渡すために使用される情報パケット。チケットは、単一クライアントと特定サーバー上の特定サービスだけに有効です。チケットには、サービスの主体名、ユーザーの主体名、ユーザーのホストの IP アドレス、タイムスタンプ、チケットの有効期限を定義する値などが含まれます。チケットは、クライアントとサービスによって使用されるランダムセッション鍵を使用して作成されます。チケットは、作成されてから有効期限まで再使用できます。チケットは、最新のオーセンティケータとともに提示されなければ、クライアントの認証に使用することができません。オーセンティケータ、資格、サービス、セッション鍵も参照してください。

チケットファイル 資格キャッシュを参照してください。

デバイスの割り当て ユーザーレベルでのデバイス保護。デバイス割り当ては、一度に 1 人のユーザーだけが使用できるようにデバイスを設定する作業です。デバイスデータは、デバイスが再使用される前に消去されます。誰にデバイス割り当てを許可するかは、承認を使用して制限できます。

デバイスポリシー カーネルレベルでのデバイス保護。デバイスポリシーは、2 つの特権セットとしてデバイスに実装されます。この 1 つはデバイスに対する読み取り権を制御し、もう 1 つはデバイスに対する書き込み権を制御します。ポリシーも参照してください。

転送可能チケット チケットの 1 つ。クライアントがリモートホスト上のチケットを要求するときに使用できます。このチケットを使用すれば、リモートホスト上で完全な認証プロセスを実行する必要がありません。たとえば、ユーザー `david` がユーザー `jennifer` のマシンで転送可能チケットを取得した場合、`david` は自分のマシンにログインできます (新しいチケットを取得する必要はない、自分自身を認証できる)。プロキシ可能チケットも参照してください。

同期監査イベント 監査イベントの大半を占めます。これらのイベントは、システムのプロセスに関連付けられています。失敗したログインなど、あるプロセスに関連付けられた、ユーザーに起因しないイベントは、同期イベントです。

特権 1. 一般に、コンピュータシステム上で通常のユーザーの能力を超える操作を実行する能力または機能。スーパーユーザー特権は、スーパーユーザーに付与されているすべての権利です。特

権ユーザーまたは特権アプリケーションは、追加の権利が付与されているユーザーまたはアプリケーションです。

2. Oracle Solaris システムにおいてプロセスに対する個々の権利。特権を使用すると、root を使用するよりもきめ細かなプロセス制御が可能です。特権の定義と適用はカーネルで行われます。特権は、*プロセス特権*や*カーネル特権*とも呼ばれます。特権の詳細は、privileges(5) のマニュアルページを参照してください。

特権エスカレーション 権利 (デフォルトをオーバーライドして許可する権利を含む) を割り当てられたリソース範囲の外部のリソースへのアクセス権を取得すること。その結果、プロセスは未承認の操作を実行できます。

特権セット 一連の特権。各プロセスには、プロセスが特定の特権を使用できるかどうかを判断する 4 セットの特権があります。詳細は、制限セット、有効セット、許可されたセット、および 継承可能セットを参照してください。

基本セットも、ユーザーのログインプロセスに割り当てられる特権セットです。

特権付きアプリケーション システム制御をオーバーライドできるアプリケーション。このようなアプリケーションは、セキュリティー属性 (特定の UID、GID、承認、特権など) をチェックします。

特権モデル コンピュータシステムにおいてスーパーユーザーモデルより厳密なセキュリティーモデル。特権モデルでは、プロセスの実行に特権が必要です。システムの管理は、管理者が各自のプロセスで与えられている特権に基づいて複数の個別部分に分割できます。特権は、管理者のログインプロセスに割り当てることも、特定のコマンドだけで有効なように割り当てることも可能です。

特権ユーザー コンピュータシステム上で通常ユーザーの権利を超えた権利が割り当てられているユーザー。信頼できるユーザーも参照してください。

特権を認識する 自身のコードでの特権の使用を有効および無効にするプログラム、スクリプト、およびコマンド。本稼動環境では、たとえば、プログラムのユーザーに、その特権をプログラムに追加する権利プロファイルの使用を要求することによって、有効になった特権をプロセスに提供する必要があります。特権の詳細は、privileges(5) のマニュアルページを参照してください。

認証 特定の主体の識別情報を検証するプロセス。

認証済み権利プロファイル 権利プロファイル の 1 つ。割り当てられたユーザーまたは役割は、プロファイルから操作を実行する前に、パスワードを入力する必要があります。この動作は、sudo の動作に似ています。パスワードが有効である時間の長さは構成可能です。

ネームサービススコープ 特定の役割が操作を許可されている適用範囲。つまり、NIS LDAP などの指定されたネームサービスからサービスを受ける個々のホストまたはすべてのホスト。

ネットワークアプリケーションサーバー ネットワークアプリケーションを提供するサーバー (ftp など)。レルムは、複数のネットワークアプリケーションサーバーで構成されます。

ネットワークポリシー ネットワークトラフィックを保護するためにネットワークユーティリティーで行われる設定。ネットワークセキュリティーについては、『Oracle Solaris 11.2 でのネットワークのセキュリティー保護 』を参照してください。

ハードウェアプロバイダ Oracle Solaris の暗号化フレームワーク機能では、デバイスドライバとそのハードウェアアクセラレータを指します。ハードウェアプロバイダを使用すると、コンピュータシステムから負荷の高い暗号化処理を解放され、その分 CPU リソースをほかの用途に充てることができます。プロバイダも参照してください。

パスフレーズ 非公開鍵がパスフレーズユーザーによって作成されたことを検証するために使用されるフレーズ。望ましいパスフレーズは、10 - 30 文字の長さで英数字が混在しており、単純な文や名前を避けたものです。通信の暗号化と復号化を行う非公開鍵の使用を認証するため、パスフレーズの入力を求めるメッセージが表示されます。

非公開鍵 各ユーザー (主体) に与えられ、主体のユーザーと KDC だけが知っている鍵。ユーザー主体の場合、鍵はユーザーのパスワードに基づいています。鍵も参照してください。

非公開鍵の暗号化 非公開鍵の暗号化では、送信者と受信者は同じ暗号化鍵を使用します。公開鍵の暗号化も参照してください。

非同期監査イベント 非同期イベントは、システムイベントの内の少数です。これらのイベントは、プロセスに関連付けられていないため、ブロックした後に起動できるプロセスはありません。たとえば、システムの初期ブートや PROM の開始および終了のイベントは、非同期イベントです。

秘密鍵 非公開鍵を参照してください。

プライバシ セキュリティーサービスの 1 つ。送信データを送信前に暗号化します。プライバシには、データの整合性とユーザー認証も含まれます。認証、整合性、サービスも参照してください。

プライマリ 主体名の最初の部分。インスタンス、主体名、レルムも参照してください。

フレーバ 従来は、「セキュリティーフレーバ」と「認証フレーバ」は、認証のタイプ (AUTH_UNIX、AUTH_DES、AUTH_KERB) を指すフレーバとして、同じ意味を持っていました。RPCSEC_GSS もセキュリティーフレーバですが、これは認証に加えて、整合性とプライバシのサービスも提供します。

プロキシ可能チケット クライアントに代わってクライアント操作を行うためにサービスによって使用されるチケット。このことを、サービスがクライアントのプロキシとして動作するといいます。サービスは、チケットを使用して、クライアントの識別情報を所有できます。このサービスは、プロキシ可能チケットを使用して、ほかのサービスへのサービスチケットを取得できますが、チケット認可チケットは取得できません。転送可能チケットと異なり、プロキシ可能チケットは単一の操作に対してだけ有効です。転送可能チケットも参照してください。

プロバイダ Oracle Solaris の暗号化フレームワーク機能では、コンシューマに提供される暗号化サービス。プロバイダには、PKCS #11 ライブラリ、カーネル暗号化モジュール、ハードウェアアクセラレータなどがあります。プロバイダは暗号化フレームワークに結合 (プラグイン) されるため、*プラグイン*とも呼ばれます。コンシューマの例は、コンシューマを参照してください。

プロファイルシェル 権利の管理で、役割 (またはユーザー) がコマンド行から、その役割の権利プロファイルに割り当てられた任意の特権付きアプリケーションを実行できるようにするシェル。プロファイルシェ

ルのバージョンは、システム上で使用可能なシェルのバージョン (bash の pfbash バージョンなど) に対応します。

ホスト ネットワークを通じてアクセス可能なシステム。

ホスト主体 サービス主体のインスタンスの 1 つ (プライマリ名は host)。さまざまなネットワークサービス (ftp、rcp、rlogin など) を提供するために設定します。host/central.example.com@EXAMPLE.COM はホスト主体の例です。サーバー主体も参照してください。

ポリシー 一般には、意思やアクションに影響を与えたり、これらを決定したりする計画や手続き。コンピュータシステムでは、多くの場合セキュリティーポリシーを指します。実際のサイトのセキュリティーポリシーは、処理される情報の重要度や未承認アクセスから情報を保護する手段を定義する規則セットです。たとえば、セキュリティーポリシーが、システムの監査、使用するデバイスの割り当て、6 週ごとのパスワード変更を要求する場合があります。

Oracle Solaris OS の特定の領域におけるポリシーの実装については、監査ポリシー、暗号化フレームワークにおけるポリシー、デバイスポリシー、Kerberos ポリシー、password policy、および権利ポリシーを参照してください。

マスター KDC 各レルムのメイン KDC。Kerberos 管理サーバー kadmind と、認証とチケット認可デーモン krb5kdc で構成されます。レルムごとに、1 つ以上のマスター KDC を割り当てる必要があります。また、クライアントに認証サービスを提供する複製 (スレーブ) KDC を任意の数だけ割り当てることができます。

無効チケット まだ使用可能になっていない遅延チケット。無効チケットは、有効になるまでアプリケーションサーバーから拒否されます。これを有効にするには、開始時期が過ぎたあと、TGS 要求で VALIDATE フラグをオンにしてクライアントがこのチケットを KDC に提示する必要があります。遅延チケットも参照してください。

メカニズム 1. データの認証や機密性を実現するための暗号化技術を指定するソフトウェアパッケージ。たとえば、Kerberos V5、Diffie-Hellman 公開鍵など。

2. Oracle Solaris の暗号化フレームワーク機能では、特定の目的のためのアルゴリズムの実装。たとえば、認証に適用される DES メカニズム (CKM_DES_MAC など) は、暗号化に適用されるメカニズム (CKM_DES_CBC_PAD) とは別です。

メッセージダイジェスト メッセージダイジェストは、メッセージから計算されるハッシュ値です。ハッシュ値によってメッセージはほぼ一意に識別されます。ダイジェストは、ファイルの整合性を検証するのに便利です。

メッセージ認証コード (MAC) データの整合性を保証し、データの出所を明らかにするコード。MAC は盗聴行為には対応できません。

役割 特権付きアプリケーションを実行するための特別な ID。割り当てられたユーザーだけが引き受けられます。

有効セット プロセスにおいて現在有効である一連の特権。

ユーザー主体 特定のユーザーに属する主体。ユーザー主体のプライマリ名はユーザー名であり、その省略可能なインスタンスは対応する資格の使用目的を説明するために使われる名前です (`jdoe`、`jdoe/admin` など)。「ユーザーインスタンス」とも呼ばれます。サービス主体も参照してください。

ユーザーに起因しない監査イベント 開始した人を特定できない監査イベント。AUE_BOOT イベントなど。

レルム 1. 1 つの Kerberos データベースといくつかの鍵配布センター (KDC) を配置した論理ネットワーク。

2. 主体名の 3 番目の部分。主体名が `jdoe/admin@CORP.EXAMPLE.COM` の場合、レルムは `CORP.EXAMPLE.COM` です。主体名も参照してください。

admin 主体 *username*`/admin` という形式 (`jdoe/admin` など) の名前を持つユーザー主体。通常のユーザー主体より多くの特権 (ポリシーの変更など) を持つことができます。主体名とユーザー主体も参照してください。

AES Advanced Encryption Standard。対称 128 ビットブロックのデータ暗号技術。2000 年の 10 月、米国政府は暗号化標準としてこのアルゴリズムの Rijndael 方式を採用しました。ユーザー主体の暗号化に代わる米国政府の標準として、AES が採用されています。

Blowfish 32 ビットから 448 ビットまでの可変長鍵の対称ブロックの暗号化アルゴリズム。その作成者である Bruce Schneier 氏は、鍵を頻繁に変更しないアプリケーションに効果的であると述べています。

DES Data Encryption Standard。1975 年に開発され、1981 年に ANSI X.3.92 として ANSI で標準化された対称鍵の暗号化方式。DES では 56 ビットの鍵を使用します。

Diffie-Hellman プロトコル 公開鍵暗号化としても知られています。1976 年に Diffie 氏と Hellman 氏が開発した非対称暗号鍵協定プロトコルです。このプロトコルを使用すると、セキュアでない伝達手段で、事前の秘密情報がなくても 2 人のユーザーが秘密鍵を交換できます。Diffie-Hellman は Kerberos で使用されます。

DSA デジタル署名アルゴリズム。512 ビットから 4096 ビットまでの可変長鍵の公開鍵アルゴリズム。米国政府標準である DSS は最大 1024 ビットです。DSA は入力に SHA1 を使用します。

ECDSA Elliptic Curve Digital Signature Algorithm。楕円曲線数学に基づく公開鍵アルゴリズム。ECDSA 鍵サイズは、同じ長さの署名の生成に必要な DSA 公開鍵のサイズより大幅に小さくなります。

FQDN 完全指定形式のドメイン名。`central.example.com` など (単なる `denver` は FQDN ではない)。

GSS-API Generic Security Service Application Programming Interface の略。さまざまなモジュールセキュリティーサービス (Kerberos サービスなど) をサポートするネットワーク層。GSS-

API は、セキュリティー認証、整合性、およびプライバシサービスを提供します。認証、整合性、プライバシも参照してください。

KDC 鍵配布センター (Key Distribution Center)。次の 3 つの Kerberos V5 要素で構成されるマシン。

- 主体と鍵データベース
- 認証サービス
- チケット許可サービス

レルムごとに、1 つのマスター KDC と、1 つ以上のスレーブ KDC を配置する必要があります。

Kerberos 認証サービス、Kerberos サービスが使用するプロトコル、または Kerberos サービスの実装に使用されるコード。

Oracle Solaris の Kerberos は、Kerberos V5 認証にほぼ準拠して実装されています。

「Kerberos」と「Kerberos V5」は技術的には異なりますが、Kerberos のドキュメントでは多くの場合、同じ意味で使用されます。

Kerberos (または Cerberus) は、ギリシャ神話において、ハデスの門を警護する 3 つの頭を持つどう猛な番犬のことです。

Kerberos ポリシー Kerberos サービスでのパスワードの使用方法を管理する一連の規則。ポリシーは、主体のアクセスやチケットのパラメータ (有効期限など) を制限できます。

kvno 鍵バージョン番号。特定の鍵に対して、生成順に付けられたシーケンス番号。もっとも大きい kvno が、最新の鍵を示します。

MAC 1. メッセージ認証コード (MAC)を参照してください。

2. 「ラベル付け」とも呼ばれます。政府のセキュリティー用語規定では、MAC は「Mandatory Access Control」の略です。「Top Secret」や「Confidential」というラベルは MAC の例です。MAC と対称をなすものに DAC (Discretionary Access Control) があります。UNIX アクセス権は DAC の 1 例です。

3. ハードウェアにおいては、LAN における一意のシステムアドレス。システムが Ethernet 上に存在する場合は、Ethernet アドレスが MAC に相当します。

MD5 デジタル署名などのメッセージ認証に使用する繰り返し暗号化のハッシュ関数。1991 年に Rivest 氏によって開発されました。その使用は非推奨です。

NTP Network Time Protocol (NTP)。デラウェア大学で開発されたソフトウェア。ネットワーク環境で、正確な時間またはネットワーククロックの同期化を管理します。NTP を使用して、Kerberos 環境のクロックスキューを管理できます。「クロックスキュー」も参照してください。

PAM プラグイン可能認証モジュール (Pluggable Authentication Module)。複数の認証メカニズムを使用できるフレームワーク。認証メカニズムを使用するサービスはコンパイルし直す必要がありません。PAM は、ログイン時に Kerberos セッションを初期化できます。

password policy パスワードの生成に使用できる暗号化アルゴリズム。パスワードをどれぐらいの頻度で変更すべきか、パスワードの試行を何回まで認めるかといったセキュリティー上の考慮事項など、パスワードに関連した一般的な事柄を指すこともあります。セキュリティーポリシーにはパスワードが必要です。パスワードポリシーでは、AES アルゴリズムを使用してパスワードを暗号化することを要求したり、パスワードの強度に関連したそれ以上の要件を設定したりすることもできます。

QOP 保護の品質。整合性サービスまたはプライバシサービスで使用する暗号化アルゴリズムを選択するときに使用されるパラメータの 1 つ。

RBAC Oracle Solaris のユーザー権利管理機能である、役割に基づくアクセス制御。権利を参照してください。

RBAC ポリシー 権利ポリシーを参照してください。

RSA デジタル署名と公開鍵暗号化システムを取得するための方法。その開発者である Rivest 氏、Shamir 氏、Adleman 氏によって 1978 年に最初に公開されました。

SEAM Solaris システム上の Kerberos の初期バージョンに対応する製品名。この製品は、マサチューセッツ工科大学 (MIT) で開発された Kerberos V5 テクノロジに基づいています。SEAM は、現在 Kerberos サービスと呼ばれています。引き続き、MIT バージョンとはわずかに異なります。

Secure Shell セキュリティー保護されていないネットワークを通して、セキュアなリモートログインおよびその他のセキュアなネットワークサービスを使用するための特別なプロトコル。

SHA1 セキュアなハッシュアルゴリズム。メッセージ要約を作成するために 2^{64} 文字以下の長さを入力するときに操作します。SHA1 アルゴリズムは DSA に入力されます。

stash ファイル stash ファイルには、KDC のマスター鍵を暗号化したコピーが含まれます。サーバーがリブートされると、このマスター鍵を使用して KDC が自動的に認証されてから、`kadmind` プロセスと `krb5kdc` プロセスがブートされます。stash ファイルにはマスター鍵が入っているため、このファイルやこのファイルのバックアップは安全な場所に保管する必要があります。暗号が破られると、この鍵を使用して KDC データベースのアクセスや変更が可能になります。

TGS チケット許可サービス。KDC のコンポーネントの 1 つ。チケットを発行します。

TGT チケット認可チケット。KDC によって発行されるチケット。クライアントは、このチケットを使用して、ほかのサービスのチケットを要求することができます。

索引

さ

た

な

は

ま

や

ら

わ

Q

R

S

T

U

V

W

X

Z