Oracle® Solaris 11 セキュリティーガイドライン

Part No: E25817
2012 年 3 月

ORACLE

120411@25097

目次

はじめに

このガイドは、Oracle Solaris オペレーティングシステム (Oracle Solaris OS) のセキュリティーガイドラインを示しています。最初に、このガイドではエンタープライズ OS が対処する必要があるセキュリティー問題について説明します。次に、Oracle Solaris OS のデフォルトのセキュリティー機能について説明します。最後に、システムを強化し、Oracle Solaris セキュリティー機能を使用してデータやアプリケーションを保護する際に実行する特定のステップについて説明します。このガイドの推奨事項は、サイトのセキュリティーポリシーに合わせて調整できます。

対象読者

Oracle Solaris 11 セキュリティーガイドライン は、次の作業を行うセキュリティー管理者およびその他の管理者を対象としています。

- セキュリティー要件の分析
- ソフトウェアへのサイトのセキュリティーポリシーの実装
- Oracle Solaris OS のインストールと構成
- システムおよびネットワークセキュリティーの保守

このガイドを使用するには、UNIX 管理の一般知識、ソフトウェアセキュリティーの適切な基盤、およびサイトのセキュリティーポリシーの知識が必要です。

Oracle サポートへのアクセス

Oracle のお客様は、My Oracle Support を通じて電子的なサポートを利用することができます。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。

表記上の規則

このマニュアルでは、次のような字体や記号を特別な意味を持つものとして使用します。

表 P–1 表記上の規則

字体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 system%
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	system% **su** password:
AaBbCc123	変数を示します。実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、rm *filename* と入力します。
『 』	参照する書名を示します。	『コードマネージャ・ユーザーズガイド』を参照してください。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第 5 章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	sun% **grep '^#define ** **XV_VERSION_STRING'**

Oracle Solaris OS に含まれるシェルで使用する、UNIX のデフォルトのシステムプロンプトとスーパーユーザープロンプトを次に示します。コマンド例に示されるデフォルトのシステムプロンプトは、Oracle Solaris のリリースによって異なります。

- C シェル

  machine_name% **command y|n** [*filename*]

- C シェルのスーパーユーザー

  machine_name# **command y|n** [*filename*]

- Bash シェル、Korn シェル、および Bourne シェル

  $ **command y|n** [*filename*]

- Bash シェル、Korn シェル、および Bourne シェルのスーパーユーザー

```
# command y|n [filename]
```

[ ] は省略可能な項目を示します。上記の例は、*filename* は省略してもよいことを示しています。

| は区切り文字 (セパレータ) です。この文字で分割されている引数のうち 1 つだけを指定します。

キーボードのキー名は英文で、頭文字を大文字で示します (例: Shift キーを押します)。ただし、キーボードによっては Enter キーが Return キーの動作をします。

ダッシュ (-) は 2 つのキーを同時に押すことを示します。たとえば、Ctrl-D は Control キーを押したまま D キーを押すことを意味します。

◆ ◆ ◆ 第 1 章

1 Oracle Solaris 11 セキュリティーの概要

Oracle Solaris 11 は、実証済みのセキュリティー機能を提供する、堅牢かつ最高級のエンタープライズオペレーティングシステムです。Oracle Solaris 11 では、ユーザーによるファイルアクセス、システムデータベースの保護、およびシステムリソースの使用の方法を制御する、洗練されたネットワーク規模のセキュリティーシステムを使って、あらゆる層のセキュリティー要件に対応します。従来のオペレーティングシステムにはセキュリティーに関する固有の脆弱性が含まれていることがありますが、Oracle Solaris 11 ではその柔軟性によって、エンタープライズサーバーからデスクトップクライアントに至るまで、さまざまなセキュリティー目標を満たすことができます。Oracle Solaris 11 は完全にテスト済みであり、Oracle のさまざまな SPARC および x86 ベースのシステム、およびサードパーティーベンダーのその他のハードウェアプラットフォームでサポートされています。

Oracle Solaris 11 セキュリティーの保護

Oracle Solaris は、ディスク上および転送中のデータを保護することによって、会社のデータおよびアプリケーションの強固な基盤を提供します。Oracle Solaris リソースマネージャー (資源管理とも呼ばれる) および Oracle Solaris ゾーンには、アプリケーションを分離して誤用から保護する機能があります。Oracle Solaris の特権および役割に基づくアクセス制御 (RBAC) 機能によって実装された最小特権とともに、この封じ込めによって、侵入者や標準ユーザーの動作によるセキュリティーリスクが軽減されます。IP セキュリティー (IPsec) などの認証および暗号化済みのプロトコルでは、インターネット間の仮想プライベートネットワーク (VPN)、および安全なデータ配布のための LAN または WAN 内のトンネルが提供されます。さらに、Oracle Solaris の監査機能によって、重要なアクティビティーのレコードが保持されます。

Oracle Solaris 11 セキュリティーサービスは、システムおよびネットワークに保護層を提供することによって徹底的な防御を行います。Oracle Solaris は、ユーティリティーで実行可能な特権動作をカーネルユーティリティー内で制限することによって、カーネルを保護します。デフォルトのネットワーク構成では、システム上およびケーブル間でデータ保護を行います。IPsec、Oracle Solaris の IP フィルタ機能、および Kerberos を使用すると、追加の保護が可能です。

Oracle Solaris セキュリティーサービスには、次の機能があります。

- カーネルの保護 - ファイルアクセス権および特権によってカーネルデーモンおよびデバイスが保護されます。
- ログインの保護 - ログインにパスワードが必要です。パスワードは強固に暗号化されています。初期状態では、リモートログインが Oracle Solaris の Secure Shell 機能を使用した暗号化および認証済みのチャネルに制限されています。`root` アカウントは直接ログインできません。
- データの保護 – ファイルアクセス権によってディスク上のデータが保護されます。追加の保護層を構成できます。たとえば、アクセス制御リスト (ACL) を使用したり、データをゾーンに配置したり、ファイルを暗号化したり、Oracle Solaris ZFS データセットを暗号化したり、読み取り専用の ZFS データセットを作成したり、 `setuid` プログラムおよび実行可能ファイルを実行できないようにファイルシステムをマウントしたりできます。

Oracle Solaris 11 セキュリティーのテクノロジー

Oracle Solaris のセキュリティー機能は、サイトのセキュリティーポリシーを実装するように構成できます。

次のセクションでは、Oracle Solaris のセキュリティー機能について簡単に紹介します。このガイドおよびこれらの機能を実証するその他の Oracle Solaris システム管理ガイドには、より詳細な説明および手順への参照が記載されています。

監査サービス

監査とは、システムリソースの使用状況に関するデータを収集することです。監査データは、セキュリティーに関連するシステムイベントの記録を提供します。このデータは、システムで発生する動作に対する責任の割り当てに使用できます。

監査は、セキュリティーの評価、検証、および認証機関に対する基本的な要件です。監査は、疑わしい侵入者に対する抑止力にもなります。

詳細については、次を参照してください。

- 監査関連のマニュアルページの一覧については、『Oracle Solaris の管理: セキュリティーサービス』の第 29 章「監査 (参照)」を参照してください。
- ガイドラインについては、35 ページの「ログイン/ログアウトに加えて重要なイベントの監査」およびマニュアルページを参照してください。
- 監査の概要については、『Oracle Solaris の管理: セキュリティーサービス』の第 26 章「監査 (概要)」を参照してください。
- 監査作業については、『Oracle Solaris の管理: セキュリティーサービス』の第 28 章「監査の管理 (タスク)」を参照してください。

Basic Audit Reporting Tool

Oracle Solaris の基本監査報告機能 (BART) を使用すると、一定期間にわたってシステムのファイルレベルチェックを行い、システムを包括的に検証できます。BART マニフェストを作成すると、配備されたシステムにインストールされたソフトウェアスタックのコンポーネントに関する情報を、簡単かつ確実に収集できます。

BART は、1 つのシステム上またはシステムのネットワーク上で整合性管理を行う際に役立つツールです。

詳細については、次を参照してください。

- 選択したマニュアルページには、`bart(1M)`、`bart_rules(4)`、および `bart_manifest(4)` が含まれています。
- ガイドラインについては、50 ページの「システムの BART スナップショットの作成」、53 ページの「基本監査報告機能 (BART) の使用」、およびマニュアルページを参照してください。
- BART の概要については、『Oracle Solaris の管理: セキュリティーサービス』の第 6 章「基本監査報告機能の使用方法 (タスク)」を参照してください。
- BART の使用例については、『Oracle Solaris の管理: セキュリティーサービス』の「BART の使用方法 (タスク)」およびマニュアルページを参照してください。

暗号化サービス

Oracle Solaris の暗号化フレームワーク機能および Oracle Solaris の鍵管理フレームワーク (KMF) 機能では、暗号化サービスおよび鍵管理のための中央リポジトリが提供されます。ハードウェア、ソフトウェア、およびエンドユーザーは、最適化されたアルゴリズムにシームレスにアクセスできます。各種公開鍵インフラストラクチャー (PKI) のためのさまざまなストレージメカニズム、管理ユーティリティー、およびプログラムインタフェースでは、KMF インタフェースを導入するときに、統合されたインタフェースを使用できます。

暗号化フレームワークは、各コマンド、ユーザーレベルのプログラミングインタフェース、カーネルプログラミングインタフェース、およびユーザーレベルとカーネルレベルのフレームワークを使用して、暗号化サービスをユーザーおよびアプリケーションに提供します。暗号化フレームワークは、これらの暗号化サービスをエンドユーザーに対してシームレスな方法で、アプリケーションおよびカーネルモジュールに提供します。また、直接的な暗号化サービス (ファイルの暗号化や復号化など) もエンドユーザーに提供します。

KMF は、公開鍵オブジェクト (X.509 証明書や公開と非公開鍵のペアなど) を中央で管理するためのツールおよびプログラミングインタフェースを提供します。これらのオブジェクトの格納形式としては、さまざまなものが使えます。また、KMF では、アプリケーションによる X.509 証明書の使用方法を定義したポリシーを管理するためのツールも提供されます。KMF では、サードパーティーのプラグインがサポートされています。

詳細については、次を参照してください。

- 選択したマニュアルページには、`cryptoadm(1M)`、`encrypt(1)`、`mac(1)`、`pktool(1)`、および `kmfcfg(1)` が含まれています。
- 暗号化サービスの概要については、『Oracle Solaris の管理: セキュリティーサービス』の第 11 章「暗号化フレームワーク (概要)」および『Oracle Solaris の管理: セキュリティーサービス』の第 13 章「鍵管理フレームワーク」を参照してください。
- 暗号化フレームワークの使用例については、『Oracle Solaris の管理: セキュリティーサービス』の第 12 章「暗号化フレームワーク (タスク)」およびマニュアルページを参照してください。

ファイルアクセス権とアクセス制御エントリ

ファイルシステムのオブジェクトを保護する防御の第一線は、すべてのファイルシステムオブジェクトに割り当てられたデフォルトの UNIX アクセス権です。UNIX アクセス権では、一意のアクセス権をオブジェクトの所有者、オブジェクトに割り当てられたグループ、および他の任意のユーザーに割り当てることがサポートされています。さらに、ZFS ではアクセス制御リスト (ACL) がサポートされています。これはアクセス制御エントリ (ACE) とも呼ばれ、ファイルシステムオブジェクトの個人またはグループへのアクセスをより細かく制御します。

詳細については、次を参照してください。

- ZFS ファイルに ACL を設定する手順については、`chmod(1)` のマニュアルページを参照してください。
- ファイルアクセス権の概要については、『Oracle Solaris の管理: セキュリティーサービス』の「UNIX アクセス権によるファイル保護」を参照してください。

- ZFS ファイルの保護の概要および例については、『Oracle Solaris の管理: ZFS ファイルシステム』の第 8 章「ACL および属性を使用した Oracle Solaris ZFS ファイルの保護」およびマニュアルページを参照してください。

パケットフィルタリング

パケットのフィルタリングは、ネットワークベースの攻撃に対する基本的な保護を提供します。Oracle Solaris には、IP フィルタ機能および TCP ラッパーがあります。

IP フィルタ

Oracle Solaris の IP フィルタ機能は、ネットワークベースの攻撃を防ぐファイアウォールを作成します。

特に、IP フィルタはステートフルパケットフィルタリング機能を提供し、IP アドレスまたはネットワーク、ポート、プロトコル、ネットワークインタフェース、およびトラフィックリダイレクションでパケットをフィルタリングできます。また、ステートレスパケットフィルタリングと、アドレスプールの作成および管理を行う機能もあります。さらに、IP フィルタには、ネットワークアドレス変換 (NAT) およびポートアドレス変換 (PAT) を実行する機能もあります。

詳細については、次を参照してください。

- 選択したマニュアルページには、`ipfilter(5)`、`ipf(1M)`、`ipnat(1M)`、`svc.ipfd(1M)`、および `ipf(4)` が含まれています。
- IP フィルタの概要については、『Oracle Solaris の管理: IP サービス』の第 20 章「Oracle Solaris の IP フィルタ (概要)」を参照してください。
- IP フィルタの使用例については、『Oracle Solaris の管理: IP サービス』の第 21 章「IP フィルタ (手順)」およびマニュアルページを参照してください。
- IP フィルタポリシー言語の構文の詳細および例については、`ipnat(4)` のマニュアルページを参照してください。

TCP ラッパー

TCP ラッパーは、特定のネットワークサービスを要求するホストのアドレスを ACL と突き合わせて検査することによるアクセス制御の実装方法を提供します。要求は、状況に応じて、許可されたり拒否されたりします。また、TCP ラッパーはネットワークサービスへのホスト要求のログを記録します。これは、便利な監視機能です。Oracle Solaris の Secure Shell および `sendmail` 機能は、TCP ラッパーを使用するように構成できます。アクセス制御下に置かれたネットワークサービスには、`ftpd` および `rpcbind` が含まれています。

TCP ラッパーでは、組織がセキュリティーポリシーをグローバルにだけでなく、サービスごとに指定することもできる多機能な構成ポリシー言語がサポートさ

れています。サービスへの追加アクセスは、ホスト名、IPv4 または IPv6、ネットグループ名、ネットワーク、および DNS ドメインに基づいて許可または制限できます。

詳細については、次を参照してください。

- TCP ラッパーの詳細については、『Oracle Solaris の管理: IP サービス』の「TCP ラッパーを使って TCP サービスのアクセスを制御する方法」を参照してください。
- TCP ラッパーのアクセス制御言語の構文の詳細および例については、`hosts_access`(4) のマニュアルページを参照してください。

パスワードとパスワード制約

強固なユーザーパスワードは、総当たりの推測などの攻撃に対して防御する際に役立ちます。

Oracle Solaris には、強固なユーザーパスワードを推進する際に使用できる数多くの機能があります。パスワードの長さ、内容、変更の頻度、および変更の要件を設定したり、パスワード履歴を保持したりできます。避けるべきパスワードのパスワードディクショナリが提供されます。複数のパスワードアルゴリズムが利用可能です。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の「ログイン制御の管理」
- 『Oracle Solaris の管理: セキュリティーサービス』の「ログインとパスワードの保護 (タスク)」
- 選択したマニュアルページには、`passwd`(1) および `crypt.conf`(4) が含まれています。

プラグイン可能認証モジュール

プラグイン可能認証モジュール (PAM) フレームワークを使用すると、アカウント、資格、セッション、およびパスワードに対するユーザー認証要件を調整および構成できます。

PAM フレームワークを使用すると、組織がアカウント、セッション、およびパスワード管理機能に加えて、ユーザー認証エクスペリエンスもカスタマイズできます。`login` や `ftp` などのシステムエントリサービスは、PAM フレームワークを使用して、システムのすべてのエントリポイントがセキュリティー保護されていることを確認します。このアーキテクチャーでは、フィールド内の認証モジュールを交換または変更することによって、PAM フレームワークを使用するシステムサービスを変更せずに、新たに見つかった弱点からシステムをセキュリティー保護できます。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の第 15 章「PAM の使用」
- pam.conf(4) のマニュアルページ

Oracle Solaris の特権

特権は、カーネルで強制されるプロセス上の適切に調整された個別の権限です。Oracle Solaris では、file_read のような基本特権から proc_clock_highres のようなより特化した特権まで、80 以上の特権が定義されています。特権はコマンド、ユーザー、役割、またはシステムに付与できます。多くの Oracle Solaris コマンドおよびデーモンは、作業を実行するために必要な特権でしか実行されません。特権の使用は、プロセス権管理とも呼ばれます。

特権対応のプログラムによって、侵入者がプログラム自体で使用される特権以外の特権を取得することを回避できます。さらに、特権を使用すると、組織がシステムで実行されるサービスおよびプロセスに付与される特権を制限することもできます。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の「特権 (概要)」
- 『Oracle Solaris の管理: セキュリティーサービス』の「特権の使用 (タスク)」
- 『Oracle Solaris 11 セキュリティーサービス開発ガイド』の第 2 章「特権付きアプリケーションの開発」
- 選択したマニュアルページには、ppriv(1) および privileges(5) が含まれています。

リモートアクセス

リモートアクセス攻撃によって、システムおよびネットワークが損害を受ける可能性があります。ネットワークアクセスをセキュリティー保護することは、現在のインターネット環境で必要であり、WAN および LAN 環境でも役立ちます。

IPsec と IKE

IP セキュリティー (IPsec) は、パケットの認証またはパケットの暗号化 (あるいはその両方) を行うことによって、IP パケットを保護します。Oracle Solaris では、IPv4 と IPv6 の両方の IPsec がサポートされています。IPsec はアプリケーション層によく実装されるため、インターネットアプリケーションはコードを変更する必要なく IPsec を利用できます。

IPsec およびそのキー変換プロトコル (IKE) では、暗号化フレームワークのアルゴリズムが使用されます。さらに、暗号化フレームワークは、メタスロットを使用するアプリケーションに softtoken キーストアを提供します。メタスロットを使用するように IKE を構成すると、組織はキーを格納する場所として、ディスク、接続したハードウェアキーストア、またはソフトトークンキーストアを選択できます。

正しく管理すれば、IPsec は、ネットワークトラフィックの保護に有効なツールとなります。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: IP サービス』の第 14 章「IP セキュリティーアーキテクチャー (概要)」
- 『Oracle Solaris の管理: IP サービス』の第 15 章「IPsec の構成 (タスク)」
- 『Oracle Solaris の管理: IP サービス』の第 17 章「インターネット鍵交換 (概要)」
- 『Oracle Solaris の管理: IP サービス』の第 18 章「IKE の構成 (手順)」
- 選択したマニュアルページには、`ipsecconf(1M)` および `in.iked(1M)` が含まれています。

Secure Shell

Oracle Solaris の Secure Shell 機能を使用すると、ユーザーまたはサービスが、暗号化された通信チャネル経由で、リモートシステム間でファイルにアクセスしたりファイルを転送できます。Secure Shell では、すべてのネットワークトラフィックが暗号化されます。また、Secure Shell は、認証および暗号化されたネットワークリンク経由で、ローカルシステムとリモートシステム間で X ウィンドウシステムトラフィックを転送したり、各ポート番号に接続したりできるオンデマンド仮想プライベートネットワーク (VPN) としても使用できます。

したがって、Secure Shell では、不審な侵入者が傍受された通信を読み取ったり、敵対者がシステムになりすましたりすることが回避されます。デフォルトでは、Secure Shell は新たにインストールされたシステムで唯一のアクティブなリモートアクセスメカニズムです。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の第 17 章「Secure Shell の使用 (タスク)」
- 選択したマニュアルページには、`ssh(1)`、`sshd(1M)`、`sshd_config(4)`、および `ssh_config(4)` が含まれています。

Kerberos サービス

Oracle Solaris の Kerberos 機能を使用すると、Kerberos サービスを実行する異機種システム混在ネットワーク上でも、シングルサインオンおよびセキュリティー保護されたトランザクションが可能です。

Kerberos は、マサチューセッツ工科大学 (MIT) で開発された Kerberos V5 ネットワーク認証プロトコルに基づいています。Kerberos サービスは、ネットワーク経由でのセキュリティー保護されたトランザクションを提供するクライアントサーバーアーキテクチャーです。Kerberos サービスでは、強力なユーザー認証とともに、整合性とプライバシを提供します。Kerberos サービスを使用して、他のシステムに 1 度ログインしてアクセスしたり、コマンドを実行したり、データを交換したり、ファイルを安全に転送したりできます。さらに、このサービスを使用して、管理者がサービスおよびシステムへのアクセスを制限することもできます。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』のパート VI「Kerberos サービス」
- 選択したマニュアルページには、`kerberos(5)` および `kinit(1)` が含まれています。

役割に基づくアクセス制御

RBAC では、組織が独自のニーズおよび要件に応じて、選択的に管理者権限をユーザーまたは役割に付与できるようにすることによって、最小特権のセキュリティー原則が適用されます。

Oracle Solaris の役割に基づくアクセス制御 (RBAC) 機能は、通常は `root` 役割に制限されるような作業へのユーザーアクセスを制御します。RBAC では、プロセスやユーザーにセキュリティー属性を適用することで、管理者権限を複数の管理者に分配できます。RBAC はユーザー権限管理とも呼ばれます。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』のパート III「役割、権利プロファイル、特権」
- 選択したマニュアルページには、`rbac(5)`、`roleadd(1M)`、`profiles(1)`、および `user_attr(4)` が含まれています。

サービス管理機能

Oracle Solaris のサービス管理機能 (SMF) は、サービスを追加、削除、構成、および管理する際に使用されます。SMF は RBAC を使用して、システム上のサービス管理機能へのアクセスを制御します。特に、SMF は承認を使用して、サービスを管理するユーザーおよびそのユーザーが実行できる機能を判定します。

SMF を使用すると、組織がサービスへのアクセスを制御することに加えて、それらのサービスの起動、停止、および再表示する方法も制御できます。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: 一般的なタスク』の第 6 章「サービスの管理 (概要)」
- 『Oracle Solaris の管理: 一般的なタスク』の第 7 章「サービスの管理 (手順)」
- 選択したマニュアルページには、`svcadm(1M)`、`svcs(1)`、および `smf(5)` が含まれています。

Oracle Solaris ZFS ファイルシステム

ZFS は Oracle Solaris 11 のデフォルトファイルシステムです。基本的に、ZFS ファイルシステムでは、Oracle Solaris ファイルシステムが管理される方法が変更されています。ZFS は堅牢かつスケーラブルで、管理が容易です。ZFS でのファイルシステム作成は軽量なので、割り当ておよび予約された容量を簡単に構築できます。UNIX アクセス権と ACE 保護ファイル、および RBAC では、ZFS データセットの委任管理がサポートされています。

詳細については、次を参照してください。

- 『Oracle Solaris の管理: ZFS ファイルシステム』の第 1 章「Oracle Solaris ZFS ファイルシステム (概要)」
- 『Oracle Solaris の管理: ZFS ファイルシステム』の第 3 章「Oracle Solaris ZFS ファイルシステムと従来のファイルシステムの相違点」
- 『Oracle Solaris の管理: ZFS ファイルシステム』の第 6 章「Oracle Solaris ZFS ファイルシステムの管理」
- 選択したマニュアルページには、`zfs(1M)` および `zfs(7FS)` が含まれています。

Oracle Solaris ゾーン

Oracle Solaris ゾーンソフトウェアのパーティション分割テクノロジーを使用すると、サーバーごとに 1 つのアプリケーションという開発モデルを保持しながら、同時にハードウェア資源を共有できます。

ゾーンは仮想化されたオペレーティング環境であり、複数のアプリケーションを同じ物理ハードウェア上にある他の各アプリケーションから分離して実行できます。この分離によって、ゾーン内で実行されるプロセスが、他のゾーンで実行されるプロセスを監視または適用したり、相互のデータを表示したり、基礎となるハードウェアを操作したりすることが回避されます。ゾーンは、アプリケーションが配備されたシステムの物理属性 (物理デバイスパスやネットワークインタフェース名など) からアプリケーションを分離する抽象レイヤーも提供します。

詳細については、次を参照してください。

- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』のパート II「Oracle Solaris ゾーン」
- 選択したマニュアルページには、`brands(5)`、`zoneadm(1M)`、および `zonecfg(1M)` が含まれています。

Trusted Extensions

Oracle Solaris の Trusted Extensions 機能は、データの安全性ポリシーをデータ所有者から分離できるセキュリティー保護されたラベル作成テクノロジーがオプションで有効化された層です。Trusted Extensions では、所有権に基づいた従来の随意アクセス制御 (DAC) ポリシーと、ラベルに基づいた必須アクセス制御 (MAC) ポリシーの両方がサポートされています。Trusted Extensions 層が有効になっている場合を除いて、すべてのラベルは同じであるため、カーネルは MAC ポリシーを強制するように構成されません。ラベルに基づいた MAC ポリシーが有効になっている場合は、アクセスを要求するプロセス (サブジェクト) とデータを含むオブジェクトに関連付けられたラベルの比較に基づいて、すべてのデータフローが制限されます。その他の大部分のマルチレベルオペレーティングシステムとは異なり、Trusted Extensions にはマルチレベルデスクトップが含まれています。

Trusted Extensions は、Common Criteria Labeled Security Protection Profile (LSPP)、Role-Based Access Protection Profile (RBACPP)、および Controlled Access Protection Profile (CAPP) の要件を満たしています。ただし、Trusted Extensions の実装は、互換性を最大限にし、オーバーヘッドを最小限にしながら高保証を実現できるという点で独自性があります。

詳細については、次を参照してください。

- Trusted Extensions の構成と管理の詳細については、『Trusted Extensions 構成と管理』を参照してください。
- マルチレベルデスクトップの使用についての詳細は、『Trusted Extensions ユーザーガイド』を参照してください。
- 選択したマニュアルページには、`trusted_extensions(5)` と `labeld(1M)` が含まれています。

Oracle Solaris 11 セキュリティーのデフォルト値

インストール後に Oracle Solaris は、数あるセキュリティー機能の中でも特に、システムを侵入から保護し、ログイン試行を監視します。

システムアクセスの制限と監視

初期ユーザーおよび root 役割アカウント - 初期ユーザーアカウントはコンソールからログインできます。このアカウントには root 役割が割り当てられます。初期状態では、2 つのアカウントのパスワードが同じです。

- ログイン後に、初期ユーザーはシステムを追加構成するために root 役割を引き受けることができます。役割を引き受けると、ユーザーは root パスワードを変更するように要求されます。役割 (root 役割を含む) は直接ログインできないことに注意してください。
- 初期ユーザーには、/etc/security/policy.conf ファイルからデフォルト値が割り当てられます。デフォルト値には、基本 Solaris ユーザー権利プロファイルおよびコンソールユーザー権利プロファイルが含まれています。これらの権利プロファイルによって、ユーザーはコンソールの前に座ったときに、CD または DVD への読み取りと書き込みを行ったり、特権なしでシステムでコマンドを実行したり、システムを停止して再起動したりできます。
- 初期ユーザーアカウントには、システム管理者権利プロファイルも割り当てられています。したがって、初期ユーザーは root 役割を引き受けなくても、ソフトウェアをインストールする権限やネームサービスを管理する権限などの管理者権限を持っています。

パスワード要件 – ユーザーのパスワードは 6 文字以上の長さで、1 文字以上の英字と数字が含まれる必要があります。パスワードは、SHA256 アルゴリズムを使用してハッシュ化されます。パスワードを変更したら、root 役割を含むすべてのユーザーがパスワード要件に準拠する必要があります。

制限付きのネットワークアクセス – インストール後に、システムはネットワーク経由の侵入者から保護されます。初期ユーザーによるリモートログインは、ssh プロトコルで認証、暗号化された接続経由で許可されます。これは、受信パケットを許可する唯一のネットワークプロトコルです。ssh キーは、AES128 アルゴリズムによってラップされます。暗号化および認証を適切に行うと、ユーザーは傍受、変更、またはなりすましを受けることなくシステムに到達できます。

記録されたログイン試行 - すべてのログイン/ログアウトイベント (ログイン、ログアウト、ユーザーの切り替え、ssh セッションの起動と停止、画面のロック) およびすべての非限定的な (失敗した) ログインで、監査サービスが有効になっています。root 役割はログインできないため、root として動作するユーザーの名前は、監査証跡で追跡できません。初期ユーザーは、システム管理者権利プロファイルから付与された権限で監査ログをレビューできます。

カーネル、ファイル、およびデスクトップの適切な配置

初期ユーザーがログインすると、カーネル、ファイルシステム、およびデスクトップアプリケーションが最小特権、アクセス権、および役割に基づくアクセス制御 (RBAC) によって保護されます。

カーネルの保護 - 多くのデーモンおよび管理コマンドには、これらを正常に実行できる特権のみが割り当てられています。多くのデーモンは、`root` (`UID=0`) 特権を持たない特別な管理者アカウントから実行されるため、その他の作業を実行するためにハイジャックできません。このような特別な管理者アカウントはログインできません。デバイスは特権によって保護されます。

ファイルシステム - デフォルトでは、すべてファイルシステムが ZFS ファイルシステムです。ユーザーの `umask` が `022` であるため、ユーザーが新規ファイルまたはディレクトリを作成すると、そのユーザーのみが変更を許可されます。ユーザーグループのメンバーは、ディレクトリの読み取りと検索、およびファイルの読み取りが許可されます。ユーザーグループ外部でのログインでは、ディレクトリを一覧表示し、ファイルを読み取ることができます。ディレクトリアクセス権は `drwxr-xr-x` (`755`) です。ファイルアクセス権は `-rw-r--r--` (`644`) です。

デスクトップアプレット – デスクトップアプレットは RBAC によって保護されます。たとえば、初期ユーザーまたは `root` 役割のみが、パッケージマネージャーアプレットを使用して新規パッケージをインストールできます。パッケージマネージャーは、使用する権限を割り当てられていない標準ユーザーには表示されません。

追加セキュリティー機能の適切な配置

Oracle Solaris 11 は、サイトのセキュリティー要件を満たすようにシステムおよびユーザーを構成する際に使用できるセキュリティー機能を提供します。

- 役割に基づくアクセス制御 **(RBAC)** – Oracle Solaris には、数多くの承認、特権、および権利プロファイルがあります。`root` は唯一の定義された役割です。権利プロファイルは、作成された役割の基礎となります。また、一部の管理コマンドでは、RBAC 承認を正常に実行する必要があります。承認なしのユーザーは、必須の特権を持っていてもコマンドを実行できません。
- ユーザー権限 – 22 ページの「システムアクセスの制限と監視」で説明した初期ユーザーと同様に、ユーザーには特権、権利プロファイル、および承認の基本セットが `/etc/security/policy.conf` ファイルから割り当てられます。ユーザーのログイン試行は制限されていませんが、すべての失敗ログインのログが監査サービスによって記録されます。
- システムファイルの保護 – システムファイルはファイルアクセス権によって保護されます。`root` 役割のみがシステム構成ファイルを変更できます。

サイトのセキュリティーポリシーと運用

システムまたはシステムのネットワークをセキュリティー保護するには、サイトがポリシーをサポートするセキュリティー運用でセキュリティーポリシーを適切に実施する必要があります。

詳細については、次をレビューしてください。

- 『Trusted Extensions 構成と管理』の付録 A「サイトのセキュリティーポリシー」
- 『Trusted Extensions 構成と管理』の「セキュリティー要件の実施」
- Keeping Your Code Secure (`http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do`)

◆ ◆ ◆ 第 2 章

2 Oracle Solaris 11 セキュリティーの構成

この章では、システムにセキュリティーを構成するときの動作について説明します。この章では、パッケージのインストール、システム自体の構成、および各種サブシステムや IPsec などの必要な追加アプリケーションの構成について説明します。

Oracle Solaris OS のインストール

Oracle Solaris OS をインストールするときは、適切なグループパッケージをインストールするメディアを選択します。

- **Oracle Solaris Large Server –** 自動インストーラ (AI) インストールのデフォルトマニフェストおよびテキストインストーラによって、Oracle Solaris 大規模サーバー環境を提供する `group/system/solaris-large-server` グループがインストールされます。
- **Oracle Solaris Desktop –** Live Media によって、Oracle Solaris 11 デスクトップ環境を提供する `group/system/solaris-desktop` グループがインストールされます。

  集中的に使用するデスクトップシステムを作成するには、Oracle Solaris サーバーに `group/feature/multi-user-desktop` グループを追加します。詳細は、記事Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment を参照してください。

自動インストーラ (AI) を使用する自動インストールについては、『Oracle Solaris 11 システムのインストール』のパート III「インストールサーバーを使用したインストール」を参照してください。

メディアの選択についてのガイドは、次のインストールガイドを参照してください。

- 『Oracle Solaris 11 システムのインストール』
- 『カスタム Oracle Solaris 11 インストールイメージの作成』
- 『Oracle Solaris 11 ソフトウェアパッケージの追加および更新』

システムのセキュリティー保護

次の作業がもっとも多く順番に実行されています。この時点で、Oracle Solaris 11 OS がインストールされ、root 役割を引き受けることができる初期ユーザーのみがシステムにアクセスできます。

タスク	説明	参照先
1. システム上のパッケージを検証します。	インストールメディアのパッケージがインストール済みのパッケージと同じであることをチェックします。	27 ページの「パッケージの検証」
2. システム上のハードウェア設定を保護します。	ハードウェア設定を変更する際にパスワードの入力を求めることによって、ハードウェアを保護します。	『Oracle Solaris の管理: セキュリティーサービス』の「システムハードウェアへのアクセスの制御 (タスク)」
3. 不要なサービスを無効にします。	システムの必須機能の一部ではないプロセスが実行されることを回避します。	27 ページの「不要なサービスの無効化」
4. デバイス割り当てを要求します。	明示的な承認なしでリムーバブルメディアを使用することを回避します。デバイスにはマイク、USB ドライブ、および CD が含まれます。	『Oracle Solaris の管理: セキュリティーサービス』の「デバイス割り当てを有効にする方法」
5. ワークステーションの所有者がシステムの電源を切ることを回避します。	コンソールユーザーがシステムをシャットダウンしたり、保存停止したりすることを回避します。	28 ページの「ユーザーからの Power Management 機能の削除」
6. サイトのセキュリティーポリシーが反映されたログイン警告メッセージを作成します。	ユーザーおよび不審な攻撃者にシステムが監視されていることを通知します。	28 ページの「バナーファイルへのセキュリティーメッセージの配置」 29 ページの「セキュリティーメッセージのデスクトップログイン画面への配置」

▼ パッケージの検証

インストール直後に、パッケージを検証することによってインストールを検証します。

始める前に　root 役割になっている必要があります。

1. **pkg verify** コマンドを実行します。
   レコードを保存するには、コマンド出力をファイルに送信します。

   ```
   # pkg verify > /var/pkgverifylog
   ```

2. エラーがないかどうかログをレビューします。
3. エラーが見つかった場合は、メディアから再インストールするか、エラーを修正します。

参照　詳細については、pkg(1) および pkg(5) のマニュアルページを参照してください。マニュアルページには、pkg verify コマンドの使用例が記載されています。

▼ 不要なサービスの無効化

この手順を使用して、システムの目的に応じて必要がないサービスを無効にします。

始める前に　root 役割になっている必要があります。

1. オンラインサービスを一覧表示します。

   ```
   # svcs | grep network
   online         Sep_07   svc:/network/loopback:default
   ...
   online         Sep_07   svc:/network/ssh:default
   ```

2. このシステムで必要がないサービスを無効にします。
   たとえば、システムが NFS サーバーや Web サーバーではなく、サービスがオンラインである場合は、これを無効にします。

   ```
   # svcadm disable svc:/network/nfs/server:default
   # svcadm disable svc:/network/http:apache22
   ```

参照　詳細は、『Oracle Solaris の管理: 一般的なタスク』の第 6 章「サービスの管理 (概要)」および svcs(1) のマニュアルページを参照してください。

▼ ユーザーからの Power Management 機能の削除

この手順を使用して、このシステムのユーザーがシステムを保存停止したり、電源を切ったりすることを回避します。

始める前に　root 役割になっている必要があります。

1. コンソールユーザー権利プロファイルの内容をレビューします。

```
% getent prof_attr | grep Console
Console User:RO::Manage System as the Console User:
profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
Brightness,CPU Power Management,Network Autoconf User;
auths=solaris.system.shutdown;help=RtConsUser.html
```

2. ユーザーが保持する権限がコンソールユーザープロファイルに含まれる権利プロファイルを作成します。

   手順については、『Oracle Solaris の管理: セキュリティーサービス』の「権利プロファイルを作成または変更する方法」を参照してください。

3. **/etc/security/policy.conf** ファイルでコンソールユーザー権利プロファイルをコメントアウトします。

```
#CONSOLE_USER=Console User
```

4. 手順 2で作成した権利プロファイルをユーザーに割り当てます。

```
# usermod -P +new-profile username
```

参照　詳細については、『Oracle Solaris の管理: セキュリティーサービス』の「policy.conf ファイル」および policy.conf(4) と usermod(1M) のマニュアルページを参照してください。

▼ バナーファイルへのセキュリティーメッセージの配置

この手順を使用して、サイトのセキュリティーポリシーが反映された警告メッセージを作成します。これらのファイルの内容は、ローカルおよびリモートのログイン時に表示されます。

注 – この手順のサンプルメッセージは、アメリカ合衆国政府の要件を満たしておらず、ユーザーのセキュリティーポリシーも満たしていない可能性があります。

始める前に　root 役割になっている必要があります。ベストプラクティスは、セキュリティーメッセージの内容について会社の弁護士に相談することです。

1 セキュリティーメッセージを **/etc/issue** ファイルに入力します。

```
# vi /etc/issue
      ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

詳細は、issue(4) のマニュアルページを参照してください。

/etc/issue ファイルの内容が telnet プログラムのログインメッセージとして表示されます。ほかのアプリケーションでのこのファイルの使用については、39 ページの「ssh および ftp ユーザーに対するセキュリティーメッセージの表示」 および 29 ページの「セキュリティーメッセージのデスクトップログイン画面への配置」 を参照してください。

2 セキュリティーメッセージを **/etc/motd** ファイルに追加します。

```
# vi /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

▼ セキュリティーメッセージのデスクトップログイン画面への配置

ユーザーがログイン時に確認するセキュリティーメッセージを作成する方法を複数の中から選択します。

詳細は、デスクトップ上で「システム」>「ヘルプ」メニューをクリックして GNOME ヘルプブラウザを起動してください。yelp コマンドを使用することもできます。デスクトップログインスクリプトについては、gdm(1M) のマニュアルページの「GDM Login Scripts and Session Files」のセクションを参照してください。

注 – この手順のサンプルメッセージは、アメリカ合衆国政府の要件を満たしておらず、ユーザーのセキュリティーポリシーも満たしていない可能性があります。

始める前に root 役割になっている必要があります。ベストプラクティスは、セキュリティーメッセージの内容について会社の弁護士に相談することです。

- セキュリティーメッセージをデスクトップログイン画面に配置します。
  複数のオプションがあります。ダイアログボックスを作成するオプションでは、28 ページの「バナーファイルへのセキュリティーメッセージの配置」の手順 1 で作成した /etc/issue ファイルを使用できます。

  - オプション 1: ログイン時にダイアログボックスにセキュリティーメッセージを表示するデスクトップファイルを作成します。

    ```
    # vi /usr/share/gdm/autostart/LoginWindow/banner.desktop
    [Desktop Entry]
    Type=Application
    Name=Banner Dialog
    Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

    ユーザーは、ログインウィンドウでの認証後にワークスペースに移動するには、このダイアログボックスを閉じる必要があります。zenity コマンドのオプションについては、zenity(1) のマニュアルページを参照してください。

  - オプション 2: ダイアログボックスにセキュリティーメッセージが表示されるように GDM 初期化スクリプトを変更します。

    /etc/gdm ディレクトリには、デスクトップログインの前、間、または直後にセキュリティーメッセージを表示するための 3 つの初期化スクリプトが含まれています。これらのスクリプトは、Oracle Solaris 10 リリースでも利用可能です。

    - ログイン画面が表示される前にセキュリティーメッセージを表示します。

      ```
      # vi /etc/gdm/Init/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

    - 認証後のログイン画面にセキュリティーメッセージを表示します。

      このスクリプトは、ユーザーのワークスペースが表示される前に実行されます。このスクリプトを作成するには、Default.sample スクリプトを変更します。

      ```
      # vi /etc/gdm/PostLogin/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

    - 認証後のユーザーの最初のワークスペースにセキュリティーメッセージを表示します。

      ```
      # vi /etc/gdm/PreSession/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

注 – このダイアログボックスは、ユーザーのワークスペース上のウィンドウの下に隠れることがあります。

- オプション 3: 入力フィールドの上にセキュリティーメッセージが表示されるようにログインウィンドウを変更します。

  メッセージに合わせてログインウィンドウが拡大されます。この方法では、/etc/issue ファイルを指定しません。GUI にテキストを入力する必要があります。

  注 – ログインウィンドウ (gdm-greeter-login-window.ui) が pkg fix コマンドと pkg update コマンドによって上書きされます。変更を保持するには、このファイルを構成ファイルディレクトリにコピーし、システムをアップグレードしたあとで、その変更を新しいファイルにマージします。詳細は、pkg(5) のマニュアルページを参照してください。

  a. ディレクトリをログインウィンドウのユーザーインタフェースに変更します。

     ```
     # cd /usr/share/gdm
     ```

  b. (省略可能) 元のログインウィンドウの UI のコピーを保存します。

     ```
     # cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
     ```

  c. GNOME Toolkit のインタフェースデザイナを使用して、ログインウィンドウにラベルを追加します。

     glade-3 プログラムによって GTK+ インタフェースデザイナが開きます。ユーザー入力フィールドの上に表示されるラベルにセキュリティーメッセージを入力します。

     ```
     # /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
     ```

     インタフェースデザイナのガイドを確認するには、GNOME ヘルプブラウザで「開発」をクリックしてください。glade-3(1) のマニュアルページは、マニュアルページの「アプリケーション」の下に表示されます。

  d. (省略可能) ログインウィンドウの GUI を変更したら、コピーを保存します。

     ```
     # cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
     ```

例 2–1 デスクトップログイン時の短い警告メッセージの作成

この例では、デスクトップファイル内の zenity コマンドへの引数として管理者が短いメッセージを入力します。管理者は、--warning オプションを使用してメッセージとともに警告アイコンも表示します。

```
# vi /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
```

```
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

ユーザーのセキュリティー保護

この時点で、root 役割を引き受けることができる初期ユーザーのみがシステムにアクセスできます。標準ユーザーがログインする前に、次の作業がもっとも多く順番に実行されています。

タスク	説明	参照先
強固なパスワードおよび頻繁なパスワード変更を要求します。	各システムでデフォルトのパスワード制約を強化します。	33 ページの「より強固なパスワード制約の設定」
標準ユーザーに対して制限されたファイルアクセス権を構成します。	標準ユーザーに対するファイルアクセス権に 022 よりも制限された値を設定します。	35 ページの「標準ユーザーに対するより制限された umask 値の設定」
標準ユーザーに対してアカウントロックを設定します。	管理で使用されていないシステムで、アカウントロックをシステム全体に設定し、ロックをアクティブにするログインの数を削減します。	34 ページの「標準ユーザーに対するアカウントロックの設定」
追加の監査クラスを事前に選択します。	システムへの潜在的な脅威の監視と記録をより適切に行います。	35 ページの「ログイン/ログアウトに加えて重要なイベントの監査」
監査イベントのテキスト概要を syslog ユーティリティーに送信します。	ログインや試みられたログインなどの重要な監査イベントのカバレージをリアルタイムで提供します。	36 ページの「リアルタイムでの lo イベントの監視」
役割を作成します。	どのユーザーもシステムを損傷できないように、個別の管理作業を複数の信頼できるユーザーに配布します。	『Oracle Solaris の管理: 一般的なタスク』の「ユーザーアカウントの設定」 『Oracle Solaris の管理: セキュリティーサービス』の「役割を作成する方法」 『Oracle Solaris の管理: セキュリティーサービス』の「役割を割り当てる方法」
許可されたアプリケーションのみをユーザーのデスクトップ上に表示します。	使用を承認されていないアプリケーションをユーザーが参照または使用することを回避します。	『Trusted Extensions 構成と管理』の「デスクトップアプリケーションにユーザーを制限する」を参照してください。

タスク	説明	参照先
ユーザーの特権を制限します。	ユーザーが必要としない基本特権を削除します。	37 ページの「ユーザーからの不要な基本特権の削除」

▼ より強固なパスワード制約の設定

デフォルトがサイトのセキュリティー要件を満たさない場合に、この手順を使用します。このステップは、`/etc/default/passwd` ファイルのエントリ一覧に従います。

始める前に　デフォルトを変更する前に、変更によってすべてのユーザーがアプリケーションおよびネットワーク上の他のシステムへの認証を行うことができることを確認します。

`root` 役割になっている必要があります。

- **`/etc/default/passwd` ファイルを編集します。**

  a. パスワードを毎月 (ただし、**3** 週間ごと以内の頻度で) 変更するようにユーザーに要求します。

  ```
  ## /etc/default/passwd
  ##
  MAXWEEKS=
  MINWEEKS=
  MAXWEEKS=4
  MINWEEKS=3
  ```

  b. **8** 文字以上のパスワードを要求します。

  ```
  #PASSLENGTH=6
  PASSLENGTH=8
  ```

  c. パスワード履歴を保持します。

  ```
  #HISTORY=0
  HISTORY=10
  ```

  d. 最後のパスワードとの最小限の相違を要求します。

  ```
  #MINDIFF=3
  MINDIFF=4
  ```

  e. **1** 文字以上の大文字を要求します。

  ```
  #MINUPPER=0
  MINUPPER=1
  ```

  f. **1** 桁以上を要求します。

  ```
  #MINDIGIT=0
  MINDIGIT=1
  ```

参照
- パスワードの作成を制約する変数の一覧については、/etc/default/passwd ファイルを参照してください。デフォルトはファイルに指定されています。
- インストール後に有効になるパスワード制約については、22 ページの「システムアクセスの制限と監視」を参照してください。
- passwd(1) のマニュアルページ

▼ 標準ユーザーに対するアカウントロックの設定

この手順を使用して、特定の数のログイン試行に失敗したあとに通常ユーザーアカウントをロックします。

注 – 役割をロック解除できるため、役割を引き受けることができるユーザーのアカウントロックを設定しないでください。

始める前に root 役割になっている必要があります。管理アクティビティーで使用されるシステムでは、この保護をシステム全体に設定しないでください。

1 **LOCK_AFTER_RETRIES** セキュリティー属性を **YES** に設定します。

- システム全体に設定します。

```
# vi /etc/security/policy.conf
...
#LOCK_AFTER_RETRIES=NO
LOCK_AFTER_RETRIES=YES
...
```

- ユーザーごとに設定します。

```
# usermod -K lock_after_retries=yes username
```

2 **RETRIES** セキュリティー属性を **3** に設定します。

```
# vi /etc/default/login
...
#RETRIES=5
RETRIES=3
...
```

参照
- ユーザーおよび役割セキュリティー属性の説明については、『Oracle Solaris の管理: セキュリティーサービス』の第 10 章「Oracle Solaris のセキュリティー属性 (参照)」を参照してください。
- 選択したマニュアルページには、policy.conf(4) および user_attr(4) が含まれています。

▼ 標準ユーザーに対するより制限された umask 値の設定

デフォルトの umask 値 022 では十分に制限されない場合は、この手順を使用して、より制限されたマスクを設定します。

始める前に　root 役割になっている必要があります。

- 各種のシェルのスケルトンディレクトリに含まれるログインプロファイルで **umask** 値を変更します。

  Oracle Solaris には、管理者がユーザーシェルのデフォルトをカスタマイズするためのディレクトリが用意されています。これらのスケルトンディレクトリには、.profile 、 .bashrc、 .kshrc などのファイルが含まれています。

  次の値のいずれかを選択します。

  - umask 027 – 適度なファイル保護を提供します。

    (740) – グループによる w、その他のユーザーによる rwx
  - umask 026 – 少し強固なファイル保護を提供します。

    (741) – グループによる w、その他のユーザーによる rw
  - umask 077 – 完全なファイル保護を提供します。

    (700) – グループや他のユーザーのアクセスを禁止します。

参照　詳細については、次を参照してください。

- 『Oracle Solaris の管理: 一般的なタスク』の「ユーザーアカウントの設定」
- 『Oracle Solaris の管理: セキュリティーサービス』の「umask のデフォルト値」
- 選択したマニュアルページには、usermod(1M) および umask(1) が含まれています。

▼ ログイン/ログアウトに加えて重要なイベントの監査

この手順を使用して、管理コマンド、システムに侵入する試み、およびサイトのセキュリティーポリシーで指定されたその他の重要なイベントを監査します。

注 – この手順の例では、セキュリティーポリシーを満たすほど十分でない場合があります。

始める前に　root 役割になっている必要があります。サイトのセキュリティーポリシーを監査に関して実装しています。

1. ユーザーおよび役割による特権コマンドのすべての使用を監査します。
   すべてのユーザーおよび役割に対して、AUE_PFEXEC 監査イベントを事前に選択したマスクに追加します。

   ```
   # usermod -K audit_flags=lo,ps:no username

   # rolemod -K audit_flags=lo,ps:no rolename
   ```

2. 監査されるコマンドへの引数を記録します。

   ```
   # auditconfig -setpolicy +argv
   ```

3. 監査されるコマンドが実行される環境を記録します。

   ```
   # auditconfig -setpolicy +arge
   ```

参照
- 監査ポリシーについての詳細については、『Oracle Solaris の管理: セキュリティーサービス』の「監査ポリシー」を参照してください。
- 監査フラグの設定例については、『Oracle Solaris の管理: セキュリティーサービス』の「監査サービスの構成 (タスク)」および『Oracle Solaris の管理: セキュリティーサービス』の「監査サービスのトラブルシューティング (タスク)」を参照してください。
- 監査を構成するときは、auditconfig(1M) のマニュアルページを参照してください。

▼ リアルタイムでの lo イベントの監視

この手順を使用して、発生時に監視するイベントについて audit_syslog プラグインをアクティブにします。

始める前に syslog.conf ファイルを監視するには、root 役割になる必要があります。その他のステップでは、監査構成権利プロファイルが割り当てられる必要があります。

1. **lo** クラスを **audit_syslog** プラグインに送信して、プラグインをアクティブにします。

   ```
   # auditconfig -setplugin audit_syslog active p_flags=lo
   ```

2. **audit.notice** エントリを **syslog.conf** ファイルに追加します。
   デフォルトエントリには、ログファイルの場所が含まれています。

   ```
   # cat /etc/syslog.conf
   ...
   audit.notice       /var/adm/auditlog
   ```

3. ログファイルを作成します。

   ```
   # touch /var/adm/auditlog
   ```

4. **syslog** サービスの構成情報を更新します。

   ```
   # svcadm refresh system/system-log
   ```

5. 監査サービスを更新します。

   更新時に、監査サービスによって変更が監査プラグインに読み込まれます。

   ```
   # audit -s
   ```

参照
- 監査概要を別のシステムに送信するときは、『Oracle Solaris の管理: セキュリティーサービス』の「syslog 監査ログの構成方法」を参照してください。
- 監査サービスでは、大量の出力が生成される可能性があります。ログの管理方法については、`logadm`(1M) のマニュアルページを参照してください。
- 出力を監視するときは、55 ページの「`audit_syslog` 監査概要の監視」を参照してください。

▼ ユーザーからの不要な基本特権の削除

特定の状況では、3 つの基本特権のうち 1 つ以上を標準ユーザーの基本セットから削除できます。

- `file_link_any` - プロセスの実効 UID と異なる UID によって所有されているファイルへのハードリンクを作成できるようにします。
- `proc_info` – シグナルを送信できるプロセス以外のプロセスのステータスを調査できるようにします。調査できないプロセスは `/proc` に表示されないため、存在していないように見えます。
- `proc_session` - プロセスのセッションの外部で信号を送信したり、プロセスを監視したりできるようにします。

始める前に　`root` 役割になっている必要があります。

1. ユーザーが所有していないファイルへのリンクを作成できないようにします。

   ```
   # usermod -K defaultpriv=basic,!file_link_any user
   ```

2. ユーザーが所有していないプロセスを調査できないようにします。

   ```
   # usermod -K defaultpriv=basic,!proc_info user
   ```

3. ユーザーが現在のセッションから 2 番目のセッション (**ssh** セッションなど) を開始できないようにします。

   ```
   # usermod -K defaultpriv=basic,!proc_session user
   ```

4. ユーザーの基本セットから 3 つの特権をすべて削除します。

   ```
   # usermod -K defaultpriv=basic,!file_link_any,!proc_info,!proc_session user
   ```

参照　詳細については、『Oracle Solaris の管理: セキュリティーサービス』の第 8 章「役割と特権の使用 (概要)」および privileges(5) のマニュアルページを参照してください。

カーネルのセキュリティー保護

この時点で、役割を引き受けることができるユーザーが作成され、役割が作成されている場合があります。root 役割のみがシステムファイルを変更できます。

タスク	説明	参照先
プログラムが実行可能スタックを悪用することを回避します。	実行可能スタックを悪用するバッファーオーバーフローの悪用を防ぐシステム変数を設定します。	『Oracle Solaris の管理: セキュリティーサービス』の「実行可能ファイルを原因とするセキュリティーへの悪影響を防止する」
機密情報を含む可能性のあるコアファイルを保護します。	コアファイル専用に制限されたアクセス権でディレクトリを作成します。	『Oracle Solaris の管理: 一般的なタスク』の「グローバルのコアファイルパスを有効にする方法」 『Oracle Solaris の管理: 一般的なタスク』の「コアファイルの管理 (作業マップ)」

ネットワークの構成

この時点で、役割を引き受けることができるユーザーが作成され、役割が作成されている場合があります。root 役割のみがシステムファイルを変更できます。

次のネットワーク作業から、サイトの要件に従って追加のセキュリティーを提供する作業を実行します。これらのネットワーク作業は、リモートログイン中のユーザーにシステムが保護されていることを通知し、IP、ARP、および TCP プロトコルを強化します。

タスク	説明	参照先
サイトのセキュリティーポリシーが反映された警告メッセージを表示します。	ユーザーおよび不審な攻撃者にシステムが監視されていることを通知します。	39 ページの「ssh および ftp ユーザーに対するセキュリティーメッセージの表示」
ネットワークルーティングデーモンを無効にします。	不審なネットワーク侵入者によるシステムへのアクセスを制限します。	40 ページの「ネットワークルーティングデーモンの無効化」

タスク	説明	参照先
ネットワークトポロジに関する情報の流布を回避します。	パケットのブロードキャストを回避します。	41 ページの「ブロードキャストパケット転送の無効化」
	ブロードキャストエコー要求およびマルチキャストエコー要求への応答を回避します。	42 ページの「エコー要求への応答の無効化」
他のドメインへのゲートウェイであるシステム (ファイアウォールや VPN ノードなど) では、厳格な転送元および転送先のマルチホーミングをオンにします。	ヘッダーにゲートウェイのアドレスが指定されていないパケットがゲートウェイ外に移動することを回避します。	42 ページの「厳格なマルチホーミングの設定」
不完全なシステム接続の数を制御することによって、DOS 攻撃を回避します。	TCP リスナーに対する不完全な TCP 接続の許容数を制限します。	43 ページの「不完全な TCP 接続の最大数の設定」
許可される受信接続の数を制御することによって、DOS 攻撃を回避します。	TCP リスナーに対する中断中の TCP 接続のデフォルト最大数を指定します。	43 ページの「中断中の TCP 接続の最大数の設定」
初期の TCP 接続に対して強固な乱数を生成します。	RFC 1948 で規定されているシーケンス番号生成値に準拠します。	44 ページの「初期の TCP 接続に対する強固な乱数の指定」
ネットワークパラメータをセキュリティー保護されたデフォルト値に戻します。	管理操作によって削減されたセキュリティーを強化します。	44 ページの「ネットワークパラメータのセキュリティー保護された値へのリセット」
アプリケーションを適切なユーザーに制限するために、TCP ラッパーをネットワークサービスに追加します。	ネットワークサービス (FTP など) へのアクセスが許可されるシステムを指定します。 デフォルトでは、『Oracle Solaris のシステム管理 (ネットワークサービス)』の「sendmail の version 8.12 からの TCP ラッパーのサポート」で説明するように、`sendmail` アプリケーションは TCP ラッパーで保護されています。	すべての `inetd` サービスで TCP ラッパーを有効にするときは、『Oracle Solaris の管理: IP サービス』の「TCP ラッパーを使って TCP サービスのアクセスを制御する方法」を参照してください。 FTP ネットワークサービスを保護する TCP ラッパーの例については、『Oracle Solaris のシステム管理 (ネットワークサービス)』の「SMF を使用して FTP サーバーを起動する方法」を参照してください。

▼ ssh および ftp ユーザーに対するセキュリティーメッセージの表示

この手順を使用して、リモートログイン時およびファイル転送時に警告を表示します。

始める前に　root 役割になっている必要があります。/etc/issue ファイルは、28 ページの「バナーファイルへのセキュリティーメッセージの配置」の手順 1 で作成したものです。

1 **ssh** を使用してログインするユーザーに対してセキュリティーメッセージを表示するには、次の手順に従います。

a. **/etc/sshd_config** ファイル内の **Banner** 設定のコメントを解除します。

```
# vi /etc/ssh/sshd_config
# Banner to be printed before authentication starts.
Banner /etc/issue
```

b. **ssh** サービスを更新します。

```
# svcadm refresh ssh
```

詳細は、issue(4) および sshd_config(4) のマニュアルページを参照してください。

2 **ftp** を使用してログインするユーザーに対してセキュリティーメッセージを表示するには、次の手順に従います。

a. **proftpd.conf** ファイルに **DisplayConnect** 設定を追加します。

```
# vi /etc/proftpd.conf
# Banner to be printed before authentication starts.
DisplayConnect /etc/issue
```

b. **ftp** サービスを再起動します。

```
# svcadm restart ftp
```

詳細は、ProFTPD (http://www.proftpd.org/) の Web サイトを参照してください。

▼ ネットワークルーティングデーモンの無効化

この手順を使用して、デフォルトルーターを指定したインストール後にネットワークルーティングを回避します。それ以外の場合は、手動でルーティングを構成したあとに、この手順を実行します。

注 – 多くのネットワーク構成の手順で、ルーティングデーモンを無効にする必要があります。したがって、より大規模な構成手順の一部として、このデーモンを無効にしておく場合があります。

始める前に　ネットワーク管理権利プロファイルが割り当てられている必要があります。

1 ルーティングデーモンが動作していることを確認します。

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

サービスが実行中でない場合は、ここで停止できます。

2 ルーティングデーモンを無効にします。

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -u ipv4-routing -d ipv6-routing
# routeadm -u
```

3 ルーティングデーモンが無効になっていることを確認します。

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

参照 routeadm(1M) のマニュアルページ

▼ ブロードキャストパケット転送の無効化

デフォルトでは、Oracle Solaris はブロードキャストパケットを転送します。サイトのセキュリティーポリシーでブロードキャストフラッディングの可能性を減少させる必要がある場合は、この手順を使用してデフォルトを変更します。

注 – _forward_directed_broadcasts ネットワークプロパティーを無効にすると、ブロードキャスト ping も無効になっています。

始める前に ネットワーク管理権利プロファイルが割り当てられている必要があります。

1 IP パケットに対してブロードキャストパケット転送プロパティーを 0 に設定します。

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2 現在の値を検証します。

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts rw   0         --           0         0,1
```

参照 ipadm(1M) のマニュアルページ

▼ エコー要求への応答の無効化

この手順を使用して、ネットワークトポロジに関する情報の流布を回避します。

始める前に　ネットワーク管理権利プロファイルが割り当てられている必要があります。

1 **IP** パケットに対してブロードキャストエコー要求への応答プロパティーを **0** に設定して、現在の値を検証します。

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2 **IP** パケットに対してマルチキャストエコー要求への応答プロパティーを **0** に設定して、現在の値を検証します。

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

参照　詳細は、『Oracle Solaris カーネルのチューンアップ・リファレンスマニュアル』の「_respond_to_echo_broadcast と _respond_to_echo_multicast (ipv4 または ipv6)」および `ipadm`(1M) のマニュアルページを参照してください。

▼ 厳格なマルチホーミングの設定

他のドメインへのゲートウェイであるシステム (ファイアウォールや VPN ノードなど) では、この手順を使用して厳格なマルチホーミングをオンにします。

Oracle Solaris 11 リリースでは、IPv4 および IPv6 用の新しいプロパティー `hostmodel` が導入されています。このプロパティーは、マルチホームシステム上での IP パケットの送受信動作を制御します。

始める前に　ネットワーク管理権利プロファイルが割り当てられている必要があります。

1 **IP** パケットに対して **`hostmodel`** プロパティーを **`strong`** に設定します。

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2 現在の値を検証し、指定可能な値に注意してください。

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

参照 詳細は、『Oracle Solaris カーネルのチューンアップ・リファレンスマニュアル』の「hostmodel (ipv4 または ipv6)」および ipadm(1M) のマニュアルページを参照してください。

厳格なマルチホーミングの使用についての詳細は、『Oracle Solaris の管理: IP サービス』の「トンネルモードの IPsec で VPN を保護する方法」を参照してください。

▼ 不完全な TCP 接続の最大数の設定

この手順を使用して、不完全な中断中の接続の数を制御することによってサービス拒否 (DOS) 攻撃を回避します。

始める前に ネットワーク管理権利プロファイルが割り当てられている必要があります。

1 受信接続の最大数を設定します。

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2 現在の値を検証します。

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0 rw   4096      --           128       1-4294967295
```

参照 詳細については、『Oracle Solaris カーネルのチューンアップ・リファレンスマニュアル』の「_conn_req_max_q0」および ipadm(1M) のマニュアルページを参照してください。

▼ 中断中の TCP 接続の最大数の設定

この手順を使用して、許可される受信接続の数を制御することによって DOS 攻撃を回避します。

始める前に ネットワーク管理権利プロファイルが割り当てられている必要があります。

1 受信接続の最大数を設定します。

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2 現在の値を検証します。

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q  rw   1024      --           128       1-4294967295
```

参照 詳細については、『Oracle Solaris カーネルのチューンアップ・リファレンスマニュアル』の「_conn_req_max_q」および ipadm(1M) のマニュアルページを参照してください。

▼ 初期の TCP 接続に対する強固な乱数の指定

この手順では、TCP の初期シーケンス番号生成パラメータを RFC 1948 (http://www.ietf.org/rfc/rfc1948.txt) に準拠するように設定します。

始める前に システムファイルを変更するには、root 役割になる必要があります。

- **TCP_STRONG_ISS 変数のデフォルト値を変更します。**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

▼ ネットワークパラメータのセキュリティー保護された値へのリセット

デフォルトでセキュリティー保護された多くのネットワークパラメータはチューニング可能であるため、変更可能です。サイトの条件が許す場合は、次のチューニング可能パラメータをデフォルト値に戻します。

始める前に ネットワーク管理権利プロファイルが割り当てられている必要があります。パラメータの現在値がデフォルト値よりも安全ではありません。

1 **IP パケットに対してソースパケット転送プロパティーを 0 に設定して、現在の値を検証します。**

デフォルト値で、なりすましパケットからの DOS 攻撃が回避されます。

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

詳細は、『Oracle Solaris カーネルのチューンアップ・リファレンスマニュアル』の「forwarding (ipv4 または ipv6)」を参照してください。

2 **IP パケットに対してネットマスク応答プロパティーを 0 に設定して、現在の値を検証します。**

デフォルト値で、ネットワークトポロジに関する情報の流布が回避されます。

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                        PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3 **IP パケットに対してタイムスタンプ応答プロパティーを 0 に設定して、現在の値を検証します。**

デフォルト値で、システムでの追加 CPU の要求が削除され、ネットワークに関する情報の流布が回避されます。

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp          rw   0         --           0         0,1
```

4 **IP パケットに対してブロードキャストタイムスタンプ応答プロパティーを 0 に設定して、現在の値を検証します。**

デフォルト値で、システムでの追加 CPU の要求が削除され、ネットワークに関する情報の流布が回避されます。

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast rw   0         --           0         0,1
```

5 **IP パケットに対して無視リダイレクトプロパティーを 0 に設定して、現在の値を検証します。**

デフォルト値で、システムでの追加 CPU の要求が回避されます。

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw   0         --           0         0,1
```

6 **IP ソースルーティングを回避します。**

診断目的で IP ソースルーティングが必要な場合は、このネットワークパラメータを無効にしないでください。

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes   rw   0         --           0         0,1
```

詳細は、『Oracle Solaris カーネルのチューンアップ・リファレンスマニュアル』の「_rev_src_routes」を参照してください。

7 **IP パケットに対して無視リダイレクトプロパティーを 0 に設定して、現在の値を検証します。**

デフォルト値で、システムでの追加 CPU の要求が回避されます。通常、適切に設計されたネットワークではリダイレクトは必要ありません。

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect   rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect   rw    0         --           0         0,1
```

参照 ipadm(1M) のマニュアルページ

ファイルシステムおよびファイルの保護

ZFS ファイルシステムは軽量であり、予約された容量およびディスク容量の 制限による暗号化、圧縮、および構成が可能です。

次の作業では、ZFS (Oracle Solaris のデフォルトファイルシステム) で利用可能な保護の概要を示します。詳細については、『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS の割り当て制限と予約を設定する」および zfs(1M) のマニュアルページを参照してください。

タスク	説明	参照先
ディスク容量を管理および予約することによって、DOS 攻撃を回避します。	ファイルシステム、ユーザーまたはグループ、またはプロジェクト別にディスク容量の使用を指定します。	『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS の割り当て制限と予約を設定する」
最小のディスク容量をデータセットおよびその子孫に保証します。	ファイルシステム別、ユーザーまたはグループ別、またはプロジェクト別にディスク容量を保証します。	『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS ファイルシステムに予約を設定する」
ファイルシステム上のデータを暗号化します。	データセット作成時にデータセットにアクセスするために、暗号化およびパスフレーズでデータセットを保護します。	『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS ファイルシステムの暗号化」 『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS ファイルシステムを暗号化する例」

タスク	説明	参照先
標準 UNIX ファイルのアクセス権よりも細かい粒度でファイルを保護するように ACL を指定します。	拡張されたセキュリティー属性がファイルの保護に役立つことがあります。 ACL の使用上の注意については、Hiding Within the Trees (http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf) を参照してください。	ZFS End-to-End Data Integrity (http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data)

ファイルの保護と変更

root 役割のみがシステムファイルを変更できます。

タスク	説明	参照先
標準ユーザーに対して制限されたファイルアクセス権を構成します。	標準ユーザーに対するファイルアクセス権に 022 よりも制限された値を設定します。	35 ページの「標準ユーザーに対するより制限された umask 値の設定」
不正なファイルでシステムファイルを置換することを回避します。	スクリプトまたは BART を使用して不正なファイルを検索します。	『Oracle Solaris の管理: セキュリティーサービス』の「特殊なファイルアクセス権が設定されたファイルを見つける方法」

アプリケーションおよびサービスのセキュリティー保護

アプリケーションを保護するように Oracle Solaris セキュリティー機能を構成できます。

重要なアプリケーションを含むゾーンの作成

ゾーンはプロセスを分離するコンテナです。アプリケーションおよびアプリケーションの一部に役立つコンテナです。たとえば、ゾーンを使用すると、Web サイトのデータベースをサイトの Web サーバーから分離できます。

詳細および手順については、次を参照してください。

- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の第 15 章「Oracle Solaris ゾーンの紹介」
- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の「ゾーンの機能別のサマリー」

- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の「非大域ゾーンによって提供される機能」
- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の「システムのゾーンの設定 (タスクマップ)」
- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の第 16 章「非大域ゾーンの構成 (概要)」
- Hardening Oracle Database with Oracle Solaris Security Technologies (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

ゾーンの資源の管理

ゾーンは、ゾーン資源を管理するための数多くのツールを提供します。

詳細および手順については、次を参照してください。

- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の第 14 章「リソース管理の構成例」
- 『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』のパート I「Oracle Solaris のリソース管理」

IPsec および IKE の構成

IPsec および IKE によって、IPsec と IKE を使用して合同で構成されたノードとネットワーク間での転送が保護されます。

詳細および手順については、次を参照してください。

- 『Oracle Solaris の管理: IP サービス』の第 14 章「IP セキュリティーアーキテクチャー (概要)」
- 『Oracle Solaris の管理: IP サービス』の第 17 章「インターネット鍵交換 (概要)」
- 『Oracle Solaris の管理: IP サービス』の第 15 章「IPsec の構成 (タスク)」
- 『Oracle Solaris の管理: IP サービス』の第 18 章「IKE の構成 (手順)」

IP フィルタの構成

IP フィルタ機能はファイアウォールを提供します。

詳細および手順については、次を参照してください。

- 『Oracle Solaris の管理: IP サービス』の第 20 章「Oracle Solaris の IP フィルタ (概要)」
- 『Oracle Solaris の管理: IP サービス』の第 21 章「IP フィルタ (手順)」

Kerberos の構成

Kerberos サービスを使用してネットワークを保護できます。このクライアントサーバーアーキテクチャーでは、ネットワーク経由の転送がセキュリティー保護されます。Kerberos サービスでは、強力なユーザー認証とともに、整合性とプライバシを提供します。Kerberos サービスを使用して、他のシステムにログインしてコマンドを実行したり、データを交換したりファイルを安全に転送したりできます。さらに、このサービスを使用して、管理者がサービスおよびシステムへのアクセスを制限することもできます。Kerberos ユーザーとして、自分のアカウントに他人がアクセスするのを制限できます。

詳細および手順については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の第 20 章「Kerberos サービスの計画」
- 『Oracle Solaris の管理: セキュリティーサービス』の第 21 章「Kerberos サービスの構成 (タスク)」
- 選択したマニュアルページには、`kadmin(1M)`、`pam_krb5(5)`、および `kclient(1M)` が含まれています。

レガシーサービスへの SMF の追加

Oracle Solaris のサービス管理機能 (SMF) にアプリケーションを追加すると、アプリケーション構成を信頼できるユーザーまたは役割に制限できます。

詳細および手順については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の「RBAC プロパティーをレガシーアプリケーションに追加する方法」
- Securing MySQL using SMF - the Ultimate Manifest (`http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the`)
- 選択したマニュアルページには、`smf(5)`、`smf_security(5)`、`svcadm(1M)`、および `svccfg(1M)` が含まれています。

システムの BART スナップショットの作成

システムの構成後に、1 つ以上の BART マニフェストを作成できます。これらのマニフェストは、システムのスナップショットを提供します。その後、標準スナップショットおよび比較のスケジュールを設定できます。詳細については、53 ページの「基本監査報告機能 (BART) の使用」を参照してください。

マルチレベル (ラベル付き) セキュリティーの追加

Trusted Extensions は、必須アクセス制御 (MAC) ポリシーを強化することによって Oracle Solaris セキュリティーを拡張します。機密ラベルが自動的に、すべてのデータソース (ネットワーク、ファイルシステム、およびウィンドウ) およびデータコンシューマ (ユーザーおよびプロセス) に割り当てられます。すべてのデータへのアクセスは、データ (オブジェクト) とコンシューマ (サブジェクト) 間の関係に基づいて制限されます。階層化された機能は、ラベル対応のサービスセットで構成されます。

Trusted Extensions サービスの部分的な一覧には、次のものが含まれています。

- ラベル付きネットワーク接続
- ラベル対応ファイルシステムのマウントおよび共有
- ラベル付きデスクトップ
- ラベルの構成および変換
- ラベル対応システムの管理ツール
- ラベル対応デバイスの割り当て

`group/feature/trusted-desktop` パッケージは、マルチレベルの信頼できる Oracle Solaris デスクトップ環境を提供します。

Trusted Extensions の構成

Trusted Extensions パッケージをインストールしてから、システムを構成する必要があります。パッケージのインストール後に、ビットマップディスプレイに直接接続されたデスクトップ (ノートパソコンやワークステーションなど) をシステムで実行できます。他のシステムと通信するには、ネットワーク構成が必要です。

詳細および手順については、次を参照してください。

- 『Trusted Extensions 構成と管理』のパート I「Trusted Extensions の初期構成」
- 『Trusted Extensions 構成と管理』のパート II「Trusted Extensions の管理」

ラベル付き IPsec の構成

IPsec を使用すると、ラベル付きパケットを保護できます。

詳細および手順については、次を参照してください。

- 『Oracle Solaris の管理: IP サービス』の第 14 章「IP セキュリティーアーキテクチャー (概要)」
- 『Trusted Extensions 構成と管理』の「ラベル付き IPsec の管理」
- 『Trusted Extensions 構成と管理』の「ラベル付き IPsec の構成 (作業マップ)」

◆ ◆ ◆ 第 3 章

Oracle Solaris 11 セキュリティーの監視と保守

Oracle Solaris には、基本監査報告機能 (BART) 機能と監査サービスというセキュリティーを監視する 2 つのシステムツールが用意されています。各プログラムおよびアプリケーションで、アクセスおよび使用状況のログを作成することもできます。

基本監査報告機能 (BART) の使用

BART マニフェストは、システム上にインストールされたものを静的に記録します。インストールされたシステムへの変更およびシステム間の相違を追跡するために、長期間および複数のシステム間にわたって、BART マニフェストを比較できます。

詳細および手順については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の「基本監査報告機能 (概要)」
- 『Oracle Solaris の管理: セキュリティーサービス』の「BART の使用方法 (タスク)」
- 『Oracle Solaris の管理: セキュリティーサービス』の「BART 目録、規則ファイル、およびレポート (参照)」

インストールされたシステムへの変更を追跡する特定の手順については、『Oracle Solaris の管理: セキュリティーサービス』の「一定期間内で同一システムの目録を比較する方法」を参照してください。

監査サービスの使用

監査はシステムの使用状況を記録します。監査サービスには、監査データの分析を支援するツールが含まれています。

監査サービスについては、『Oracle Solaris の管理: セキュリティーサービス』のパート VII「Oracle Solaris での監査」で説明されています。

- 『Oracle Solaris の管理: セキュリティーサービス』の第 26 章「監査 (概要)」
- 『Oracle Solaris の管理: セキュリティーサービス』の第 27 章「監査の計画」
- 『Oracle Solaris の管理: セキュリティーサービス』の第 28 章「監査の管理 (タスク)」
- 『Oracle Solaris の管理: セキュリティーサービス』の第 29 章「監査 (参照)」

  マニュアルページの一覧およびマニュアルページへのリンクについては、『Oracle Solaris の管理: セキュリティーサービス』の「監査サービスのマニュアルページ」を参照してください。

サイトの要件を満たすには、次の監査サービス手順が役立つ場合があります。

- 監査の構成、監査のレビュー、および監査サービスの起動と停止を行うために、個別の役割を作成します。

  役割の基本として、監査構成、監査レビュー、および監査制御の権利プロファイルを使用します。

  役割を作成するときは、『Oracle Solaris の管理: セキュリティーサービス』の「役割を作成する方法」を参照してください。
- `syslog` ユーティリティーで、監査されるイベントのテキスト概要を監視します。

  `audit_syslog` プラグインをアクティブにしてから、記録されたイベントを監視します。

  『Oracle Solaris の管理: セキュリティーサービス』の「syslog 監査ログの構成方法」を参照してください。
- 監査ファイルサイズの制限

  `audit_binfile` プラグインの `p_fsize` 属性を実用的なサイズに設定します。数ある要素の中でも特に、スケジュール、ディスク容量、および `cron` ジョブ頻度のレビューを考慮してください。

  たとえば、『Oracle Solaris の管理: セキュリティーサービス』の「監査トレールのための監査領域を割り当てる方法」を参照してください。
- 個別の ZFS プール上の監査レビューファイルシステムに完全な監査ファイルを安全に転送するように、スケジュールを設定します。
- 監査レビューファイルシステム上の完全な監査ファイルをレビューします。

audit_syslog 監査概要の監視

audit_syslog プラグインを使用すると、事前に選択された監査イベントの概要を記録できます。

次のようなコマンドを実行して監査概要が生成されると、監査概要を端末ウィンドウで表示できます。

```
# tail -0f /var/adm/auditlog
```

監査ログのレビューとアーカイブ

監査レコードはテキスト形式で、または XML 形式でブラウザに表示できます。

詳細および手順については、次を参照してください。

- 『Oracle Solaris の管理: セキュリティーサービス』の「監査ログ」
- 『Oracle Solaris の管理: セキュリティーサービス』の「監査トレールのオーバーフローを防ぐ方法」
- 『Oracle Solaris の管理: セキュリティーサービス』の「ローカルシステム上の監査レコードの管理 (タスク)」

不正なファイルの検索

プログラムへの setuid および setgid アクセス権が承認なしで使用される可能性を検出できます。疑わしい実行可能ファイルによって、所有権が root または bin などのシステムアカウントではなく、通常のユーザーに与えられることがあります。

手順および例については、『Oracle Solaris の管理: セキュリティーサービス』の「特殊なファイルアクセス権が設定されたファイルを見つける方法」を参照してください。

◆ ◆ ◆ 付 録 A

Oracle Solaris の文献目録

次の参照資料には、Oracle Solaris システムで役立つセキュリティー情報について記載されています。以前のリリースの Oracle Solaris OS のセキュリティー情報には、役に立つが古くなった情報が一部含まれています。

Oracle Solaris 11 の参照資料

次の本および記事は、Oracle Solaris 11 システムでのセキュリティーについて説明しています。

- 『Oracle Solaris の管理: セキュリティーサービス』

  このセキュリティーガイドは、Oracle が Oracle Solaris 11 管理者のために発行したものです。このガイドには、Oracle Solaris のセキュリティー機能、およびシステム構成時のそれらの使用方法が説明されています。序文には、セキュリティー情報が含まれるその他の Oracle Solaris システム管理ガイドへのリンクも記載されています。

- Oracle Solaris Security: Oracle Solaris Express (`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`)

  この記事には、このリリースの 2010 年 11 月版における Oracle Solaris セキュリティー機能のスナップショットが記載されています。

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  この記事には、このリリースの 2010 年 11 月版における Oracle Solaris 機能のスナップショットが記載されています。

役に立つ Oracle Solaris 10 の参照資料については、『Oracle Solaris 10 Security Guidelines』を参照してください。