

Oracle® Solaris 11 セキュリティーガイド ライン

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション（人的傷害を発生させる可能性があるアプリケーションを含む）への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する場合、安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したこと起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはOracle Corporationおよびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

Intel, Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD, Opteron, AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

はじめに	7
1 Oracle Solaris セキュリティーの概要	11
Oracle Solaris セキュリティーの保護	11
Oracle Solaris セキュリティーのテクノロジー	12
アドレス空間レイアウトのランダム化	12
監査サービス	13
BART ファイルの検証	13
暗号化サービス	14
ファイルアクセス権とアクセス制御エントリ	14
パケットフィルタリング	15
パスワードとパスワード制約	16
プラグイン可能認証モジュール	17
Oracle Solaris の特権	17
リモートアクセス	18
役割に基づくアクセス制御	19
サービス管理機能	20
Oracle Solaris ZFS ファイルシステム	20
Oracle Solaris ゾーン	21
Trusted Extensions	21
Oracle Solaris 11 セキュリティーのデフォルト値	22
システムアクセスの制限とモニター	22
カーネル、ファイル、およびデスクトップの適切な配置	23
追加セキュリティ機能の適切な配置	24
Oracle Solaris 11 セキュリティーの評価	24
サイトのセキュリティポリシーと運用	25

2 Oracle Solaris セキュリティーの構成	27
Oracle Solaris OS のインストール	27
システムのセキュリティー保護	28
▼ パッケージの検証方法	28
▼ 不要なサービスを無効にする方法	29
▼ ユーザーから電源管理機能を削除する方法	30
▼ バナーファイルにセキュリティーメッセージを配置する方法	30
▼ 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する方法	31
ユーザーのセキュリティー保護	34
▼ より強力なパスワード制約を設定する方法	35
▼ 標準ユーザーに対してアカウントロックを設定する方法	36
▼ 標準ユーザーに対してより制限された <code>umask</code> 値を設定する方法	37
▼ ログイン/ログアウトに加えて重要なイベントを監査する方法	38
▼ リアルタイムで <code>lo</code> イベントをモニターする方法	39
▼ ユーザーから不要な基本特権を削除する方法	40
カーネルのセキュリティー保護	41
ネットワークの構成	41
▼ <code>ssh</code> ユーザーにセキュリティーメッセージを表示する方法	43
▼ TCP ラッパーの使用方法	43
ファイルシステムおよびファイルの保護	44
▼ <code>tmpfs</code> ファイルシステムのサイズを制限する方法	45
ファイルの保護と変更	47
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	47
重要なアプリケーションを含むゾーンの作成	47
ゾーンのリソースの管理	48
IPsec および IKE の構成	48
IP フィルタの構成	48
Kerberos の構成	49
レガシーサービスへの SMF の追加	49
システムの BART スナップショットの作成	49
マルチレベル(ラベル付き)セキュリティーの追加	50
Trusted Extensions の構成	50
ラベル付き IPsec の構成	50

3 Oracle Solaris セキュリティーのモニタリングと保守	51
BART を使用したファイル整合性の検証	51
監査サービスの使用	52
audit_syslog 監査概要のモニタリング	53
監査ログのレビューとアーカイブ	53
不正なファイルの検索	53
A Oracle Solaris の文献目録	55
Oracle Solaris の参照資料	55

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 セキュリティガイドラインは、次のタスクを行うセキュリティ管理者およびその他の管理者を対象としています。

- セキュリティ要件の分析
- ソフトウェアへのサイトのセキュリティポリシーの実装
- 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の適切な基盤、およびサイトのセキュリティ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

次の表では、このドキュメントで使用される表記上の規則について説明します。

表 P-1 表記上の規則

字体	説明	例
<code>AaBbCc123</code>	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。	<code>.login</code> ファイルを編集します。 <code>ls -a</code> を使用してすべてのファイルを表示します。 <code>machine_name% you have mail.</code>
<code>AaBbCc123</code>	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。	<code>machine_name%su</code> <code>Password:</code>
<i><code>aabbcc123</code></i>	プレースホルダ: 実際に使用する特定の名称または値で置き換えます。	ファイルを削除するには、 <code>rm filename</code> と入力します。
<i><code>AaBbCc123</code></i>	書名、新しい単語、および強調する単語を示します。	『ユーザーズガイド』の第6章を参照してください。 キャッシュは、ローカルに格納されるコピーです。 ファイルを保存しないでください。 注: いくつかの強調された項目は、オンラインでは太字で表示されます。

コマンド例のシェルプロンプト

Oracle Solaris OS に含まれるシェルで使用する、UNIX 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。コマンド例では、シェルプロンプトはコマンドが標準ユーザーまたは特権ユーザーのどちらによって実行されるべきかを示しています。

表 P-2 シェルプロンプト

シェル	プロンプト
Bash シェル、Korn シェル、および Bourne シェル	<code>\$</code>
Bash シェル、Korn シェル、および Bourne シェルのスーパーユーザー	<code>#</code>

表 P-2 シェルプロンプト (続き)

シェル	プロンプト
Cシェル	machine_name%
Cシェルのスーパーユーザー	machine_name#

Oracle Solaris セキュリティーの概要

Oracle Solaris 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 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。

- 11 ページの「Oracle Solaris セキュリティーの保護」
- 12 ページの「Oracle Solaris セキュリティーのテクノロジー」
- 22 ページの「Oracle Solaris 11 セキュリティーのデフォルト値」
- 24 ページの「Oracle Solaris 11 セキュリティーの評価」
- 25 ページの「サイトのセキュリティーポリシーと運用」

Oracle Solaris 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 リソース管理および 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。
- メモリーの保護 - ユーザーランドプロセスのためにアドレス空間レイアウトがランダム化されます。
- 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ン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 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。

アドレス空間レイアウトのランダム化

アドレス空間レイアウトのランダム化 (ASLR) では、ある特定のバイナリで使用されるアドレスをランダム化します。ASLR は、ある一定のメモリー範囲の正確な場所の把握に基づいた特定の種類の攻撃を防ぐことができ、その企てによって実行可能ファイルが停止する可能性が高い場合に検出できます。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「アドレス空間レイアウトのランダム化」を参照してください。

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 11.1 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、38 ページの「ログイン/ログアウトに加えて重要なイベントを監査する方法」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 11.1 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。
- 監査タスクについては、『Oracle Solaris 11.1 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。

BART ファイルの検証

Oracle Solaris の BART 機能を使用すると、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うことで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、49 ページの「システムの BART スナップショットの作成」、51 ページの「BART を使用したファイル整合性の検証」、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 11.1 の管理: セキュリティーサービス』の第 6 章「BART を使用したファイル整合性の検証(タスク)」を参照してください。
- BART の使用例については、『Oracle Solaris 11.1 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 11.1 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 11.1 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 11.1 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 11.1 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 11.1 の管理: ZFS ファイルシステム』の第 7 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 11.1 でのネットワークのセキュリティー保護』の第 4 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 11.1 でのネットワークのセキュリティー保護』の第 5 章「IP フィルタ (タスク)」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、便利なモニタリング機能です。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る可能性があるネットワークサービスには、proftpd 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せん。

詳細については、次を参照してください。

- TCP ラッパーについては、『Oracle Solaris 11.1 ネットワークの構成と管理』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 11.1 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 11.1 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) が含まれていません。

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 11.1 の管理: セキュリティーサービス』の第 14 章「プラグイン可能認証モジュールの使用」
- `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、タスク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 11.1 の管理: セキュリティーサービス』の「特権(概要)」
- 『Oracle Solaris 11.1 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)` が含まれていません。

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 (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 11.1 でのネットワークのセキュリティ保護』の第 6 章「IP セキュリティアーキテクチャー (概要)」
- 『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の第 7 章「IPsec の構成 (タスク)」
- 『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の第 9 章「インターネット鍵交換 (概要)」
- 『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の第 10 章「IKE の構成 (タスク)」
- 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送信できます。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送信したり、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り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 11.1 の管理: セキュリティサービス』の第 15 章「Secure Shell の使用」
- 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、ネットワーク経路でのセキュリティ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ーを提供します。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 11.1 の管理: セキュリティサービス』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タスク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 11.1 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、およびリフレッシュ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 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」
- 『Oracle Solaris 11.1 でのサービスと障害の管理』の第 2 章「サービスの管理 (タスク)」
- 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 によってファイルを保護し、作成時にデータセット全体を暗号化できます。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 11.1 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 11.1 の管理: ZFS ファイルシステム』の「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 11.1 の管理: ZFS ファイルシステム』の第 5 章「Oracle Solaris ZFS ファイルシステムの管理」

- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「Secure Shell を使用して ZFS をリモートで管理する方法」
- 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リソースを共有できます。

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モニタリングまたは適用したり、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せん。Oracle Solaris 11 では、読み取り専用のゾーンルートを構成できます。

詳細については、次を参照してください。

- 『Oracle Solaris 11.1 の管理: Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理』の「読み取り専用ゾーンの構成」
- 『Oracle Solaris 11.1 の管理: 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 zoncfg(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 ユーザーズガイド](#)』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、ログイン試行をモニターします。

システムアクセスの制限とモニター

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、2 文字以上の英字と 1 文字以上の英字以外の文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、その他のタスク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モニター」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。

Oracle Solaris 11 セキュリティーの評価

Oracle Solaris 11 は現在 Canadian Common Criteria Scheme に従って Evaluation Assurance Level 4 (EAL4) で評価中であり、欠陥を修正することで拡張されます (EAL4+)。EAL4+ は、商用ソフトウェアで獲得できる最高レベルの評価です。EAL4 は、Common Criteria Recognition Arrangement (CCRA) のもとで 26 か国によって互いに認められている最高レベルの評価でもあります。

この評価は、Operating System Protection Profile (OS PP) に基づいて行われており、次の 4 つのオプションの拡張パッケージが含まれています。

- Advanced Management (AM)
- Extended Identification and Authentication (EIA)
- Labeled Security (LS)
- Virtualization (VIRT)

注 – 評価中であることは、セキュリティー認証が得られることを保証するものではありません。

評価については、次を参照してください。

- Oracle Security Evaluations (<http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html>)
- The Common Criteria Recognition Arrangement (<http://www.commoncriteriaportal.org/ccra/>)

- Products in Evaluation (<http://www.cse-cst.gc.ca/its-sti/services/cc/oe-pece-eng.html>)
- Operating System Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf)

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。プログラムの開発中またはサードパーティー製プログラムのインストール中である場合は、それらのプログラムをセキュアに開発およびインストール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。

- 『Oracle Solaris 11 セキュリティーサービス開発ガイド』の付録A「開発者のためのセキュアコーディングガイドライン」
- 『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)

Oracle Solaris 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。

- 27 ページの「Oracle Solaris OS のインストール」
- 28 ページの「システムのセキュリティー保護」
- 34 ページの「ユーザーのセキュリティー保護」
- 41 ページの「カーネルのセキュリティー保護」
- 41 ページの「ネットワークの構成」
- 44 ページの「ファイルシステムおよびファイルの保護」
- 47 ページの「ファイルの保護と変更」
- 47 ページの「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」
- 49 ページの「システムの BART スナップショットの作成」
- 50 ページの「マルチレベル (ラベル付き) セキュリティーの追加」

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、次のように、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の両方によって、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、デスクトップサーバーに `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 11.1 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 11.1 システムのインストール』
- 『Oracle Solaris 11.1 カスタムインストールイメージの作成』
- 『Oracle Solaris 11.1 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

次のタスク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 OS がインストールされ、root 役割にな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。	28 ページの「パッケージの検証方法」
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 11.1 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。	29 ページの「不要なサービスを無効にする方法」
4. 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。	30 ページの「ユーザーから電源管理機能を削除する方法」
5. 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モニターされていることを通知します。	30 ページの「バナーファイルにセキュリティーメッセージを配置する方法」 31 ページの「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する方法」

▼ パッケージの検証方法

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 役割になる必要があります。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 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。

▼ 不要なサービスを無効にする方法

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 役割になる必要があります。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 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 11.1 でのサービスと障害の管理』の第 1 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。

▼ ユーザーから電源管理機能を削除する方法

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 役割になる必要があります。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 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 11.1 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 詳細は、『Oracle Solaris 11.1 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。

▼ バナーファイルにセキュリティーメッセージを配置する方法

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セキュリティーメッセージを2つのバナーファイル内に作成します。これらのバナーファイルの内容は、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。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。

始める前に Administrator Message Edit 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、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 1 セキュリティーメッセージを `/etc/issue` ファイルに追加します。

```
$ pfedit /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.

telnet および FTP サービスの場合と同様に、認証前に、login コマンドによって `/etc/issue` の内容が表示されます。ほかのアプリケーションでこのファイルを使用できるようにする場合は、43 ページの「ssh ユーザーにセキュリティーメッセージを表示する方法」および 31 ページの「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する方法」を参照してください。

詳細は、[issue\(4\)](#) と [pfedit\(1M\)](#) のマニュアルページ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。

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

Oracle Solaris では、ユーザーの初期シェルによって `/etc/motd` ファイルの内容が表示されます。

▼ 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する方法

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。

詳細を表示するには、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ポリシーも満たしていない可能性があります。ベストプラクティスは、セキュリティ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。

始める前に ファイルを作成するには、root 役割になる必要があります。既存のファイルを変更するには、`solaris.admin.edit/path-to-existing-file` 承認が割り当てられている管理者になる必要があります。

- セキュリティメッセージをデスクトップログイン画面に配置するには、次の3つのオプションのいずれかを使用します。

ダイアログボックスを作成するオプションでは、30 ページの「[バナーファイルにセキュリティメッセージを配置する方法](#)」の手順1で作成した `/etc/issue` ファイル内のセキュリティメッセージを使用できます。

- 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。

```
# pfdedit /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メッセージを表示します。

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

システムファイルを root 以外のユーザーとして編集する方法については、`pfdedit(1M)`のマニュアルページを参照してください。

- 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メッセージを表示します。

```
$ pfdedit /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内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ー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. GNOMEToolkitのインターフェースデザイナーを使用して、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+インターフェースデザイナーが開きます。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
```

インターフェースデザイナー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)変更された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.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。

```
# pfdedit /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、次のタスク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。	35 ページの「より強力なパスワード制約を設定する方法」
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。	37 ページの「標準ユーザーに対してより制限された umask 値を設定する方法」
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。	36 ページの「標準ユーザーに対してアカウントロックを設定する方法」
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モニタリングと記録をより適切に行います。	38 ページの「ログイン/ログアウトに加えて重要なイベントを監査する方法」
監査イベントのテキスト概要を syslog ユーティリティに送信します。	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ッジをリアルタイムで提供します。	39 ページの「リアルタイムで lo イベントをモニターする方法」

タスク	説明	参照先
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、個別の管理タスクを複数の信頼できるユーザーに配布します。	『Oracle Solaris 11.1 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」 『Oracle Solaris 11.1 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 11.1 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」
表示できる GNOME デスクトップアプリケーションの数を減らします。	セキュリティーに影響を及ぼす可能性のあるデスクトップアプリケーションをユーザーが使用できないようにします。	『Oracle Solaris 11.1 デスクトップ管理者ガイド』の第 11 章「Oracle Solaris デスクトップシステムでの機能の無効化」を参照してください。
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。	40 ページの「ユーザーから不要な基本特権を削除する方法」

▼ より強力なパスワード制約を設定する方法

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ー一覧に従います。

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` 役割になる必要があります。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- `/etc/default/passwd` ファイルを編集します。

- 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モニター」](#)を参照してください。
 - `passwd(1)` のマニュアルページ

▼ 標準ユーザーに対してアカウントロックを設定する方法

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 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。

`root` 役割になる必要があります。詳細は、『[Oracle Solaris 11.1 の管理: セキュリティーサービス](#)』の「[割り当てられている管理権限を使用する方法](#)」を参照してください。

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。


```
# pftedit /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。

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

- 参照
- ユーザーおよび役割セキュリティ属性については、『Oracle Solaris 11.1 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。

▼ 標準ユーザーに対してより制限された **umask** 値を設定する方法

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` 役割になる必要があります。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 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 026` – 適度なファイル保護を提供します。
(741) – グループには `r`、他のユーザーには `x`
- `umask 027` – 厳密なファイル保護を提供します
(740) – グループには `r`、他のユーザーにはアクセス権なし
- `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 11.1 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」
- 『Oracle Solaris 11.1 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)` が含まれていません。

▼ ログイン/ログアウトに加えて重要なイベントを監査する方法

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` 役割になる必要があります。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 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は、『Oracle Solaris 11.1の管理:セキュリティサービス』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 11.1の管理:セキュリティサービス』の「監査サービスの構成(タスク)」および『Oracle Solaris 11.1の管理:セキュリティサービス』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loイベントをモニターする方法

この手順を使用して、発生時にモニター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` ファイルを変更するには、`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。詳細は、『Oracle Solaris 11.1の管理:セキュリティサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

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

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

- 2 どの `system-log` サービスインスタンスがオンラインかを決定します。

```
# svcs system-log
STATE          STIME    FMRI
disabled       13:11:55 svc:/system/system-log:rsyslog
online         13:13:27 svc:/system/system-log:default
```

ヒント - `rsyslog` サービスインスタンスがオンラインの場合は、`rsyslog.conf` ファイルを変更します。

- 3 `syslog.conf` ファイルに `audit.notice` エントリを追加します。
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
```

- 4 ログファイルを作成します。

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

- 5 **system-log** サービスの構成情報をリフレッシュします。

```
# svcadm refresh system-log:default
```

注 - rsyslog サービスがオンラインの場合は、system-log:rsyslog サービスインスタンスをリフレッシュします。

- 6 監査サービスをリフレッシュします。

リフレッシュ時に、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せん。

```
# audit -s
```

- 参照
- 監査サマリーを別のシステムに送信する場合は、『Oracle Solaris 11.1 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」に付随する例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。
 - 出力をモニターするときは、53 ページの「audit_syslog 監査概要のモニタリング」を参照してください。

▼ ユーザーから不要な基本特権を削除する方法

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 役割になる必要があります。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 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 詳細は、『Oracle Solaris 11.1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 11.1の管理:セキュリティーサービス』の「実行可能ファイルの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 11.1での一般的な問題のトラブルシューティング』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 11.1での一般的な問題のトラブルシューティング』の「コアファイルの管理(タスクマップ)」

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。

次のネットワークタスクから、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タスクを実行します。これらのネットワークタスクは、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モニターされていることを通知します。	43 ページの「ssh ユーザーにセキュリティメッセージを表示する方法」
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。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「ネットワークルーティングデーモンを無効にする方法」
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。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「ブロードキャストパケット転送を無効にする方法」
	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。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「エコーリクエストへの応答を無効にする方法」
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。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「厳密なマルチホームを設定する方法」
不完全なシステム接続の数を制御することによって、サービスの拒否 (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。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「不完全な TCP 接続の最大数を設定する方法」
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。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「中断中の TCP 接続の最大数を設定する方法」
初期の TCP 接続に対して強固な乱数を生成します。	RFC 6528 で規定されているシーケンス番号生成値に準拠します。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「初期の TCP 接続に強固な乱数を指定する方法」
ネットワークパラメータをセキュリティ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を強化します。	『Oracle Solaris 11.1 でのネットワークのセキュリティ保護』の「ネットワークパラメータをセキュアな値にリセットする方法」
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。	43 ページの「TCP ラッパーの使用方法」。

▼ ssh ユーザーにセキュリティーメッセージを表示する方法

この手順を使用して、ssh プロトコルを使用したログイン時に警告を表示します。

始める前に /etc/issue ファイルは、30 ページの「バナーファイルにセキュリティーメッセージを配置する方法」の手順 1 で作成したものです。

solaris.admin.edit/etc/ssh/sshd_config 承認といずれかの Network 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。root 役割には、これらの権利がすべて含まれています。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

- 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。

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

- b. ssh サービスをリフレッシュします。

```
# svcadm refresh ssh
```

詳細は、issue(4)、sshd_config(4)、および pfedit(1M) のマニュアルページを参照してください。

▼ TCP ラッパーの使用方法

次の手順は、Oracle Solaris で TCP ラッパーを使用する 3 つの方法を示しています。

始める前に TCP ラッパーを使用するようにプログラムを変更するには、root 役割を想定する必要があります。

- 1 TCP ラッパーで sendmail アプリケーションを保護する必要はありません。デフォルトでは、『Oracle Solaris 11.1 での sendmail サービスの管理』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、これは TCP ラッパーで保護されています。
- 2 すべての inetd サービスで TCP ラッパーを有効にする場合は、『Oracle Solaris 11.1 ネットワークの構成と管理』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。

3 TCP ラッパーで FTP ネットワークサービスを保護します。

a. `/usr/share/doc/proftpd/modules/mod_wrap.html` モジュールの説明に従います。
このモジュールは動的であるため、FTP で TCP ラッパーを使用するためにロードする必要があります。

b. 次の命令を `/etc/proftpd.conf` ファイルに追加して、モジュールをロードします。

```
<IfModule mod_dso.c>
    LoadModule mod_wrap.c
</IfModule>
```

c. FTP サービスを再起動します。

```
$ svcadm restart svc:/network/ftp
```

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。

`tmpfs` ファイルシステムは際限なく増大する可能性があります。サービスの拒否 (DOS) 攻撃を防ぐには、[45 ページの「tmpfs ファイルシステムのサイズを制限する方法」](#) を実行します。

次のタスクでは、`tmpfs` のサイズ制限を構成し、ZFS (Oracle Solaris のデフォルトのファイルシステム) で利用できる保護について簡単に説明します。詳細は、『[Oracle Solaris 11.1 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 11.1 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 11.1 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、暗号化およびバスマフレーズでデータセットを保護します。	『 Oracle Solaris 11.1 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 11.1 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)
tmpfs ファイルシステムのサイズを制限します。	悪意のあるユーザーが /tmp 内に大規模なファイルを作成してシステムの処理速度を低下させることを防ぎます。	45 ページの「 tmpfs ファイルシステムのサイズを制限する方法 」

▼ tmpfs ファイルシステムのサイズを制限する方法

tmpfs ファイルシステムのサイズは、デフォルトでは無制限です。そのため、tmpfs が増大して、使用可能なシステムメモリーやスワップがいっぱいになる可能性があります。/tmp ディレクトリはすべてのアプリケーションおよびユーザーによって使用されるため、使用可能なすべてのシステムメモリーが1つのアプリケーションに占有される可能性があります。同様に、悪意のある非特権ユーザーが /tmp ディレクトリ内に大規模ファイルを作成することによって、システムの処理速度が低下する可能性があります。パフォーマンスへの影響を避けるために、それぞれの tmpfs マウントのサイズを制限できます。

最良のシステムパフォーマンスを実現するために、いくつかの値を試していただくことをお勧めします。

始める前に root 役割になる必要があります。詳細は、『[Oracle Solaris 11.1 の管理: セキュリティーサービス](#)』の「[割り当てられている管理権限を使用する方法](#)」を参照してください。

- 1 システムのメモリー量を調べます。

注 - この手順の例に使用される SPARC T3 シリーズシステムには、入出力をより高速にするためのソリッドステートディスク (ssd) が1つと、279.40M バイトのディスクが8つ搭載されています。このシステムにはおよそ 500G バイトのメモリーがあります。

```
# prtconf | head
System Configuration: Oracle Corporation sun4v
Memory size: 523776 Megabytes
```

System Peripherals (Software Nodes):

```
ORCL,SPARC-T3-4
  scsi_vhci, instance #0
    disk, instance #4
    disk, instance #5
    disk, instance #6
    disk, instance #8
```

2 **tmpfs** のメモリー制限を計算します。

システムメモリーのサイズに応じて、大規模システムではおよそ 20 パーセント、小規模システムではおよそ 30 パーセントのメモリー制限を計算することをお勧めします。

したがって、小規模システムでは、乗数として **.30** を使用します。

10240M x .30 ≈ 340M

大規模システムでは、乗数として **.20** を使用します。

523776M x .20 ≈ 10475M

3 サイズ制限を使って **/etc/vfstab** ファイルにある **swap** エントリを変更します。

```
# pfedit /etc/vfstab
#device      device      mount      FS      fsck      mount mount
#to mount    to fsck    point      type     pass     at boot options
#
/devices     -          /devices   devfs    -         no      -
/proc        -          /proc      proc     -         no      -
ctfs         -          /system/contract ctfs    -         no      -
objfs        -          /system/object objfs    -         no      -
sharefs      -          /etc/dfs/sharetab sharefs  -         no      -
fd           -          /dev/fd    fd       -         no      -
swap         -          /tmp       tmpfs    -         yes     -
swap         -          tmpfs      -        yes      size=10400m
/dev/zvol/dsk/rpool/swap - -         swap     -         no      -
```

4 システムをリブートします。

```
# reboot
```

5 サイズ制限が有効であることを確認します。

```
# mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Fri Sep 7 14:07:27 2012
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Fri ...
```

6 メモリー使用量をモニターし、サイトの要件に合わせて調整します。

df コマンドは多少役に立ちます。swap コマンドを使用すると、もっとも役立つ統計を得られます。

```
# df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap       7. 4G  44M   7.4G 1%    /tmp
```

```
# swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
7743780k available
```

詳細は、[tmpfs\(7FS\)](#)、[mount_tmpfs\(1M\)](#)、[df\(1M\)](#)、および [swap\(1M\)](#) のマニュアルページを参照してください。

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。	37 ページの「標準ユーザーに対してより制限された umask 値を設定する方法」
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 11.1 の管理: セキュリティサービス』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 ゾーンの見直し」
- 『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)」

ゾーンのリソースの管理

ゾーンは、ゾーンリソース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 11.1 の管理: 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 11.1 でのネットワークのセキュリティー保護』の第 6 章「IP セキュリティーアーキテクチャー (概要)」
- 『Oracle Solaris 11.1 でのネットワークのセキュリティー保護』の第 9 章「インターネット鍵交換 (概要)」
- 『Oracle Solaris 11.1 でのネットワークのセキュリティー保護』の第 7 章「IPsec の構成 (タスク)」
- 『Oracle Solaris 11.1 でのネットワークのセキュリティー保護』の第 10 章「IKE の構成 (タスク)」

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 11.1 でのネットワークのセキュリティー保護』の第 4 章「Oracle Solaris の IP フィルタ (概要)」
- 『Oracle Solaris 11.1 でのネットワークのセキュリティー保護』の第 5 章「IP フィルタ (タスク)」

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ーを提供します。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 11.1 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 11.1 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 11.1 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 \(http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the\)](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。詳細は、51ページの「BARTを使用したファイル整合性の検証」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せん。

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 11.1 でのネットワークのセキュリティー保護』の第 6 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 (タスクマップ)」

Oracle Solaris セキュリティーのモニタリングと保守

Oracle Solaris には、BART 機能と監査サービスというセキュリティーをモニターする 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。

- 51 ページの「BART を使用したファイル整合性の検証」
- 52 ページの「監査サービスの使用」
- 53 ページの「不正なファイルの検索」

BART を使用したファイル整合性の検証

BART とは、暗号化強度チェックサムとファイルシステムメタデータを使用して変更を報告する、規則ベースのファイル整合性の走査および報告ツールです。

詳細および手順については、次を参照してください。

- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「BART (概要)」
- 『Oracle Solaris 11.1 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 11.1 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詳細な手順については、『Oracle Solaris 11.1 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 11.1 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 11.1 の管理: セキュリティーサービス』の第 26 章「監査 (概要)」
- 『Oracle Solaris 11.1 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 11.1 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 11.1 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それらへのリンクについては、『Oracle Solaris 11.1 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。

役割を作成する場合は、『Oracle Solaris 11.1 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モニターします。

`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モニターします。

『Oracle Solaris 11.1 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。

例については、『Oracle Solaris 11.1 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 監査概要のモニタリング

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 11.1 の管理: セキュリティーサービス』の「監査ログ」
- 『Oracle Solaris 11.1 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 11.1 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 11.1 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。



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 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について説明しています。

- 『Oracle Solaris 11.1 の管理: セキュリティサービス』

このセキュリティガイドは、Oracle がシステム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。このガイドには、セキュリティ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。

- 『Security Configuration Benchmark For Solaris 11 11/11 Version 1.0.0 June 11th, 2012』

このセキュリティベンチマークは、Center for Internet Security (CIS) (<http://cisecurity.org/>) がセキュリティコミュニティのために発行したものです。このドキュメントは、Oracle Solaris OS のセキュリティ設定を推奨しています。対象読者には、開発、インストール、評価、または Oracle Solaris へのセキュリティソリューションの提供を行う、システムおよびアプリケーション管理者、セキュリティスペシャリスト、監査者、サポートエンジニア、およびインストール担当者と開発者が含まれます。ドキュメントを取得する場合は、CIS Security Benchmarks (<http://benchmarks.cisecurity.org/>) を参照してください。

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。

