Oracle® Solaris 11 セキュリティーと強化ガイドライン

Part No: E62714
2016 年 11 月

Part No: E62714

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。

目次

表目次

このドキュメントの使用方法

- **概要** - Oracle Solaris のセキュリティー機能の概要と、それらの機能を使用して、インストールされたシステムとそのアプリケーションを強化および保護するためのガイドラインを示します。
- **対象読者** - Oracle Solaris 11 システム上のセキュリティーを開発、配備、または評価するシステム管理者、セキュリティー管理者、アプリケーション開発者、および監査者。
- **必要な知識** – サイトのセキュリティー要件。

製品ドキュメントライブラリ

この製品および関連製品のドキュメントとリソースは `http://www.oracle.com/pls/topic/lookup?ctx=E62101-01` で入手可能です。

フィードバック

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

♦ ♦ ♦ 第 1 章

1 Oracle Solaris セキュリティーについて

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。

Oracle Solaris 11.3 セキュリティーの新機能

このセクションでは、既存のお客様のために、このリリースに含まれる重要なセキュリティーの新機能について説明します。

- Oracle Solaris は、GRUB メニューのパスワードを保護します。詳細は、『Oracle Solaris 11.3 システムのブートとシャットダウン』 の 「GRUB メニューのパスワード保護」を参照してください。
- TPM が SP/SPP ボード上に存在する SPARC マルチドメインシリーズサーバーでは、TPM はスペアボードにフェイルオーバーできます。詳細は、『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「TPM フェイルオーバーオプション」を参照してください。
- 検証済みブートを使用すると、カーネルゾーンのブートプロセスをセキュリティー保護できます。検証済みブートは、Oracle Solaris カーネルモジュールを実行前にセキュアにロードすることで、破損したカーネルゾーンモジュール、悪意のあるプログラム、および未承認のサードパーティーカーネルモジュールのインストールからカーネルゾーンを保護します。詳細は、『Oracle Solaris カーネルゾーンの作成と使用』 の 「ベリファイドブートを使用した Oracle Solaris カーネルゾーンのセキュリティー保護」を参照してください。
- SPARC および x86 プラットフォーム上のゾーンのライブ移行を暗号化できます。セキュアなライブ移行と呼ばれる、暗号化されたライブ移行がデフォルトです。詳細は、『Oracle Solaris カーネルゾーンの作成と使用』 の 「セキュアなライブ移行について」を参照してください。
- デスクトップセッションに最初にログインすると、ダイアログボックスによって最終ログインの時間と場所が通知されます。承認されていないログインが発生していた場合、この通知は適切なセキュリティー対策であり、さまざまなセキュリティーポリシーによって一般的に必要とされています。詳細は、`pam_unix_session(5)` のマニュアルページを参照してください。
- 暗号化されたパスワード、または `pwhash` コマンドを使用してパスワードハッシュを作成できます。その後、自動インストール (AI) での初期のブートシーケンス中にパスワードを指定できます。また、`-p` オプションを使用して `passwd` コマンドにハッシュを渡すこともできます。Unresolved link to " pwhash1" および `passwd(1)` のマニュアルページと、『Oracle Solaris 11.3 システムのインストール』 の 「root アカウントとユーザーアカウントの構成」を参照してください。
- 変数値を使用してコーディングされたコンプライアンス規則を使用すると、サイトのセキュリティー要件を満たす正確な値をチェックする規則を含むテーラリングを作成できます。『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』 の 「コンプライアンス規則内の変数の代替値の選択」および `compliance-tailor(1M)` のマニュアルページを参照してください。
- コンプライアンス評価が定期的に実行されるようにスケジュールできます。この機能は、デフォルトでは無効になっています。『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』 の 「評価の定期的な実行」および `compliance(1M)` のマニュアルページを参照してください。

- 実行可能ファイルのスタック破損からの保護は、これまでの `/etc/system` ファイルに設定された `no_exec_userstack` システム変数に代わり、Oracle Solaris のセキュリティー拡張機能になりました。`nxstack` セキュリティー拡張機能は、デフォルトで設定されます。さらに、`nxheap` セキュリティー拡張機能は、ヒープの破損から保護します。詳細は、『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「悪影響からのプロセスヒープと実行可能スタックの保護」を参照してください。
- 暗号化フレームワークには、Camellia アルゴリズムが含まれるようになりました。Camellia がサポートするメカニズムを表示するには、`cryptoadm list -m | grep camellia` コマンドを実行します。SPARC T4 シリーズサーバーでは、このアルゴリズムのためのハードウェアアクセラレーションを提供します。
- カーネル SSL プロキシは SSLv3 をサポートしますが、デフォルトでは無効になっています。『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 「SSL カーネルプロキシ は Web サーバー通信を暗号化する」を参照してください。
- パケットフィルタは、ポリシーベースのルーティング (PBR) をサポートしています。詳細は、『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 「パケットフィルタ規則のオプションのアクション」にある `route-to` の説明を参照してください。
- 別個の中央署名サービスといった外部メカニズムを使用してプロバイダを署名するために、`elfsign` ユーティリティーを使用できます。詳細は、『Oracle Solaris 11.3 での暗号化と証明書の管理』 の 「外部署名のための Elfsign サポート」および `elfsign(1)` のマニュアルページを参照してください。
- `pktool gencsr` コマンドでは、標準の PKCS #10: Certification Request Syntax Specification (`http://www.ietf.org/rfc/rfc2986.txt`) に従わない認証局用の証明書を作成できるようになりました。`pktool(1)` のマニュアルページを参照してください。
- Oracle Solaris は、Secure Shell の `openssh` 実装を提供しています。この OpenSSH 実装は、OpenSSH 6.5p1 および追加機能に基づいて構築されています。デフォルトは引き続き `sunssh` 実装です。2 つの実装間を切り替えるには、`pkg mediator` コマンドを使用します。詳細は、『Oracle Solaris 11.3 での Secure Shell アクセスの管理』 の 第 1 章, 「Secure Shell の使用」を参照してください。
- IPsec および IKEv2 への移行に役立つように、Oracle Solaris では `pass` アクションと `ike_version` オプションが提供されています。`pass` アクションを使用すると、サーバーが IPsec クライアントおよび IPsec 以外のクライアントをサポートでき、`ike_version` オプションを使用すると、IPsec のポリシールールが使用する必要がある IKE プロトコルのバージョンを指定できます。このオプションを使用すると、ネットワークで 2 つのバージョンの IKE プロトコルが実行可能となり、サポートできるシステムでのみ新しい IKE プロトコルが必要となります。詳細および例へのリンクについては、『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 「Oracle Solaris 11.3 のネットワークセキュリティーの新機能」を参照してください。

- Oracle Solaris は、追加のファイアウォールオプションである OpenBSD Packet Filter を提供しています。詳細は、『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 4 章,「Oracle Solaris での OpenBSD パケットフィルタファイアウォール」を参照してください。
- 既存のベンチマークのバージョンまたはテーラリングを作成できます。テーラリングは、評価からエラーや誤検出を取り除くことで、特定システムのセキュリティー状況を正確に評価できます。詳細は、『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』および `compliance(1M)` と `compliance-tailor(1M)` のマニュアルページを参照してください。
- Oracle Solaris には、システムを、共通脆弱性 (CVE) を修復する最新のクリティカルパッチアップデートに更新できるようにするための `pkg:/support/critical-patch-update/solaris-11-cpu` パッケージが用意されています。『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』 の 「Oracle Solaris での CVE アップデートの管理」および『Oracle Solaris 11.3 ソフトウェアの追加と更新』 の 「サポート更新の適用」を参照してください。
- `dax_access` 特権により、Oracle Database 12c に対し、SPARC M7 シリーズおよび SPARC T7 シリーズサーバーの DAX コプロセッサでのデータ分析が高速化されます。この特権が与えられたデータベースは、クエリー処理の部分をサーバーハードウェアにオフロードできます。

インストール後の Oracle Solaris 11 セキュリティー

Oracle Solaris は、「デフォルトでのセキュリティー強化」(SBD) でインストールされます。このセキュリティー状況では、さまざまなセキュリティー機能の中でも特に、侵入からのシステムの保護と、ログイン試行のモニタリングが行われます。

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。インストール時には、初期ユーザーと `root` アカウントのパスワードは同一です。

- ログイン後、初期ユーザーは `root` 役割になって、システムを引き続き構成できます。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なったり、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 – ユーザーパスワードは、少なくとも 6 文字にし、少なくとも 2 つの英文字と 1 つの非英文字を使用する必要があります。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。

制限されたネットワークアクセス – インストール後、システムはネットワーク経由での侵入から保護されます。初期ユーザーによるリモートログインは、Secure Shell プロトコルで認証および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。Secure Shell 鍵は、`AES128` アルゴリズムによってラップされます。暗号化と認証を適用することで、ユーザーは傍受、改変、スプーフィングを受けることなくリモートシステムに到達できます。

記録されたログイン試行 – 監査サービスは、すべての `login/logout` イベント (ログイン、ログアウト、ユーザーの切り替え、Secure Shell セッションの起動と停止、画面のロック)、およびユーザーに起因しないすべての (失敗した) ログインに対して有効になっています。`root` 役割はログインできないため、`root` の役目を果たしているユーザーの名前が監査証跡に記録されます。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したあとは、カーネル、ファイルシステム、システムファイル、およびデスクトップアプリケーションがファイルアクセス権、特権、およびユーザー権利によって保護されます。ユーザー権利は、役割によるアクセス制御 (RBAC) とも呼ばれます。

カーネル保護 – 多くのデーモンおよび管理コマンドには、正常に実行できるための特権のみが割り当てられます。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` は `022` であるため、ユーザーが新しいファイルまたはディレクトリを作成すると、そのユーザーだけに変更が許可されます。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。デフォルトの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。

システムファイル - システム構成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、または特定のファイルシステムを編集する権利を割り当てられたユーザーだけが、システムファイルを変更できます。

デスクトップアプレット - デスクトップアプレットは権利管理によって保護されます。したがって、管理アクション (印刷マネージャーでのリモートプリンタの追加など) は、印刷の管理者権限を持っているユーザーおよび役割に制限されます。

Oracle Hardware Management Package

Oracle Hardware Management Package は、Oracle サーバーの構成、管理、およびモニタリングに使用する一連のユーティリティーを提供します。この Oracle ハードウェア用の付加価値ツールセットは、いつでも使用できます。特定のハードウェアに関する情報を ILOM に自動的に配信して、ILOM によるシステムハードウェアの表示を完成させることができます。これらのユーティリティーとセキュリティーについては、システム管理と診断のドキュメント (`http://www.oracle.com/goto/ohmp/docs`)を参照してください。

Oracle Solaris 構成可能セキュリティー

Oracle Solaris セキュリティーのデフォルト値によって提供される強固な基盤に加えて、Oracle Solaris システムのセキュリティー状況は高度に構成可能であり、幅広いセキュリティー要件に対応します。

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。

データの保護

Oracle Solaris は、インストール、使用、およびアーカイブによるブートからデータを保護します。

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、デフォルトのファイルシステムである ZFS では、個別のファイルシステムオブジェクトまたはファイルシステムオブジェクトのグループへのアクセスをより詳細に制御するアクセス制御リスト (ACL) がサポートされます。

詳細については、次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 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 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。
- セキュリティーに関連する ZFS ファイル属性については、『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 の 「ファイル属性を使用して ZFS ファイルにセキュリティーを追加する」およびマニュアルページを参照してください。
- ZFS ファイルの保護の概要と例については、『Oracle Solaris 11.3 での ZFS ファイルシステムの管理』 の 第 9 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。
- ZFS ファイルに対する ACL の設定手順については、`chmod(1)` のマニュアルページを参照してください。

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。KMF は、さまざまな公開鍵インフラストラクチャー (PKI) 用の異なるストレージメカニズム、管理ユーティリティー、およびプログラミングインタフェースに対する統合インタフェースを提供します。

暗号化フレームワークは、暗号化要求を処理するアルゴリズムと PKCS #11 ライブラリの共通の格納場所を提供します。PKCS #11 ライブラリは、RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) 標準に従って実装されます。標準ユーザーは、ファイルの暗号化と復号化などの暗号化サービスを使用できます。

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)`、`digest(1)`、`encrypt(1)`、`mac(1)`、`pktool(1)`、`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 11.3 での暗号化と証明書の管理』 の 第 1 章, 「暗号化フレームワーク」および『Oracle Solaris 11.3 での暗号化と証明書の管理』 の 第 4 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の例については、『Oracle Solaris 11.3 での暗号化と証明書の管理』 の 第 3 章, 「暗号化フレームワーク」およびマニュアルページを参照してください。
- 暗号化フレームワークの FIPS 140-2 プロバイダを有効にするには、『Oracle Solaris 11.3 での暗号化と証明書の管理』 の 「FIPS 140 が有効になったブート環境を作成する方法」を参照してください。

Oracle Solaris ZFS ファイルシステム

ZFS は、Oracle Solaris 11 のデフォルトの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 のアクセス権と ACL によってファイルが保護され、データセット全体を作成時に暗号化できます。Oracle Solaris の権利管理では、ZFS データセットの委任管理がサポートされます。つまり、制限された特権のセットを割り当てられたユーザーが ZFS データセットを管理できます。

詳細については、次を参照してください。

- 『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「ユーザー権管理」
- 『Oracle Solaris 11.3 での ZFS ファイルシステムの管理』 の 第 1 章, 「Oracle Solaris ZFS ファイルシステムの概要」
- 『Oracle Solaris 11.3 での ZFS ファイルシステムの管理』 の 「Oracle Solaris ZFS 機能」
- 『Oracle Solaris 11.3 での ZFS ファイルシステムの管理』 の 第 7 章, 「Oracle Solaris ZFS ファイルシステムの管理」
- 『Oracle Solaris 11.3 での Secure Shell アクセスの管理』 の 「Secure Shell を使用して ZFS をリモートで管理する方法」

- 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。

アプリケーションの保護と分離

アプリケーションは、マルウェアや悪意のあるユーザーのエントリポイントになる可能性があります。Oracle Solaris では、特権を使用し、アプリケーションをゾーン内に封じ込めることで、これらの脅威を軽減します。アプリケーションは、そのアプリケーションが必要とする特権でしか実行できないため、悪意のあるユーザーはシステムのほかの部分にアクセスするための root 特権を得られません。ゾーンにより、攻撃の範囲を制限できます。非大域ゾーン内のアプリケーションに対する攻撃は、そのゾーンのプロセスにのみ影響し、ゾーンのホストシステムには影響しません。

アドレス空間レイアウトのランダム化 (ASLR)、nxheap、および nxstack などのセキュリティー拡張機能は、侵入者が実行可能ファイルやヒープを損なうことを困難にします。詳細は、23 ページの「セキュリティー拡張機能」を参照してください。
また、サービス管理機能 (SMF) は、管理者がアプリケーションの開始、停止、および使用を制限できるようにすることで、アプリケーションを保護します。

Oracle Solaris の特権

特権は、プロセスに対する細かく設定された個別の権利で、カーネルで適用されます。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、プロセス、ユーザー、または役割に対して付与できます。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。

特権の使用は、プロセス権管理とも呼ばれます。特権を使用すると、組織は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指定 (制限) できます。
詳細については、次を参照してください。

- 『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「プロセス権管理」
- 『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。

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に対してモニタリングまたは影響したり、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。

保護を追加するため、不変大域ゾーンと呼ばれる物理的な大域ゾーン、および Oracle Solaris カーネルゾーンと呼ばれる仮想的な大域ゾーンを読み取り専用にできます。不変大域ゾーンはカーネルゾーンよりやや強力ですが、どちらもシステムのハードウェアや構成を永続的に変更できません。読み取り専用ゾーンは、書き込みを許可するゾーンよりブート速度とセキュリティーが向上します。

不変大域ゾーンには、保守のためにトラステッドコンピューティングベース (TCB) と呼ばれる特別なプロセスのセットが定義されています。これは、トラステッドパスと呼ばれる保護されたログインを介して構成できます。詳細は、『Oracle Solaris ゾーンの作成と使用』 の 第 11 章,「不変ゾーンの構成と管理」を参照してください。ゾーン構成のリソースについては、『Oracle Solaris ゾーンの紹介』を参照してください。`mwac(5)` および `tpd(5)` のマニュアルページも参照してください。

Oracle Solaris カーネルゾーンは、準拠するシステムを配備するのに役立ちます。たとえば、準拠するシステムを構成し、統合アーカイブを作成し、そのイメージをカーネルゾーンとして配備できます。詳細は、`solaris-kz(5)` のマニュアルページ、『Oracle Solaris カーネルゾーンの作成と使用』、『Oracle Solaris 11 仮想環境の紹介』 の 「Oracle Solaris ゾーンの概要」、および『Oracle Solaris 11.3 でのシステム復旧とクローン』を参照してください。

詳細については、次を参照してください。

- 『Oracle Solaris ゾーンの作成と使用』 の 「読み取り専用ゾーンの構成」
- 『Oracle Solaris ゾーンの紹介』
- 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。

セキュリティー拡張機能

Oracle Solaris のセキュリティー拡張機能は、スタックやヒープを侵害から保護するためのカーネルレベルのフラグです。アドレス空間レイアウトのランダム化 (ASLR) は、特定のプログラムによって使用されるアドレスをランダム化します。nxheap および nxstack セキュリティー拡張機能は、悪意のあるコードによる実行可能ファイルのスタックやヒープの破損を防止します。詳細は、『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「アドレス空間レイアウトのランダム化」および『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「悪影響からのプロセスヒープと実行可能スタックの保護」を参照してください。アプリケーションをコンパイルするときにこれらのセキュリティー拡張機能を使用する方法については、34 ページの「セキュアに実行されるアプリケーションの記述」のリンクを参照してください。

サービス管理機能

サービスは、永続的に実行されるアプリケーションです。サービスは、実行中のアプリケーション、デバイスのソフトウェア状態、その他の一連のサービスのいずれかを表現できます。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、権利管理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 11.3 でのシステムサービスの管理』
- 『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「特定の特権を Apache HTTP サーバー に割り当てる方法」
- 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。

Java Cryptography Extension

Java には、Java アプリケーションの開発者用に Java Cryptography Extension (JCE) が用意されています。詳細は、Java SE セキュリティー (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html)を参照してください。

ユーザーの保護と追加の権利の割り当て

16 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。これらの権利は構成可能です。ユーザーの基本的な権利を拒否したり、権利を増やしたりできます。

Oracle Solaris は、パスワードに対する柔軟な複雑性の要件、異なるサイト要件に応じて構成可能な認証、および権利プロファイル、承認、特権を使用して管理者権限を信頼できるユーザーに制限および配布するユーザー権利管理によって、ユーザーを保護します。さらに、役割と呼ばれる特殊な共有アカウントによって、ユーザーがその役割を引き受けたときに、該当する管理者権限だけがそのユーザーに割り当てられます。ARMOR (Authorization Rules Managed On RBAC) パッケージは、事前定義された役割を提供します。

パスワードとパスワード制約

強力なユーザーパスワードは、ブルートフォースの推測を伴う攻撃を防止するために役立ちます。Oracle Solaris は、業界標準とサイト要件に合ったユーザーパスワードを構成するために使用できるいくつかの機能を提供します。

詳細については、次を参照してください。

- 『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「ログイン制御の管理」
- 『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「ログインとパスワードのセキュリティー」
- 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、管理者は認証を要求するサービスを変更せずに、アカウント、資格、セッション、およびパスワードの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 `ssh` などのシステムエントリサービスは、新規にインストールされたシステムのすべてのエントリポイントをセキュリティー保護するために PAM フレームワークを使用します。PAM 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。

Oracle Solaris は、ほとんどのサイトポリシーに対応するさまざまな PAM モジュールと構成のセットを提供します。詳細については、次を参照してください。

- 『Oracle Solaris 11.3 での Kerberos およびその他の認証サービスの管理』 の 第 1 章, 「プラグイン可能認証モジュールの使用」
- 『Oracle Solaris 11 セキュリティーサービス開発ガイド』 の 「PAM サービスを使用するアプリケーションの記述」
- `pam.conf(4)` のマニュアルページ

ユーザー権利管理

Oracle Solaris のユーザー権利は、最小特権のセキュリティー原則に準拠します。組織は、組織固有のニーズと要件に従って、ユーザーまたは役割に管理者権限を選択的に付与できます。また、必要に応じてユーザーに対する権利を拒否することもできます。権利は、プロセスに対する特権と、ユーザーまたは SMF メソッドに対する承認として実装されます。権利プロファイルは、特権と承認を集めて関連する権利のバンドルを作成するための便利な方法を提供します。

詳細については、次を参照してください。

- 『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』
- 選択したマニュアルページには、`auths(1)`、`privileges(5)`、`profiles(1)`、`rbac(5)`、`roleadd(1M)`、`roles(1)`、および `user_attr(4)` が含まれています。

ネットワーク通信のセキュリティー保護

ネットワーク通信は、ファイアウォール、ネットワークアプリケーションに対する TCP ラッパー、暗号化および認証されたリモート接続などの機能によって保護できます。

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、OpenBSD Packet Filter、IP フィルタ機能、および TCP ラッパーがあります。

OpenBSD Packet Filter ファイアウォール

Oracle Solaris の OpenBSD Packet Filter (PF) 機能は、インバウンドパケットを収集してシステムの出入りを評価します。PF はステートフルパケットインスペクションを提供します。これは、IP アドレスおよびポート番号でパケットを照合できるほか、受信ネットワークインタフェースでも照合できます。

PF は、OpenBSD Packet Filter バージョン 5.5 をベースにして、排他 IP インスタンスのゾーンなどの Oracle Solaris コンポーネントと連携するように強化されています。Oracle Solaris 11.3 では、PF と IP フィルタの両方をパケットのフィルタリングに使用できます。

詳細については、次を参照してください。

- 概要については、『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』の 第 4 章,「Oracle Solaris での OpenBSD パケットフィルタファイアウォール」を参照してください。
- PF の使用例については、『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 5 章,「パケットフィルタファイアウォールの構成」とマニュアルページを参照してください。

IP フィルタファイアウォール

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。

- IP フィルタの概要については、『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 6 章,「Oracle Solaris での IP フィルタファイアウォール」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 11.3 でのネットワークのセキュリティー保護』 の 第 7 章,「IP フィルタファイアウォールの構成」と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。

- 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。

TCP ラッパー

TCP ラッパーは、インターネットサービスに対するアクセス制御を提供します。さまざまなインターネット (inetd) サービスが有効になっている場合、tcpd デーモン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 と照合します。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 syslog に記録します。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されます。実行可能ファイルと 1 対 1 のマッピングを持つネットワークサービス (proftpd や rpcbind など) が、TCP ラッパーの候補です。

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。

TCP ラッパーについては、次を参照してください。

- 52 ページの「TCP ラッパーの使用方法」
- 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。
- 選択したマニュアルページには、tcpd(1M) および inetd(1M) 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、システムとネットワークが損害を受ける可能性があります。Oracle Solaris は、ネットワーク転送に対する徹底的な防御を提供します。防御機能には、データ転送の暗号化と認証のチェック、ログイン認証、および不要なリモートサービスの無効化が含まれます。

IPsec と IKE

IP セキュリティー (IPsec) は、IP パケットの認証、IP パケットの暗号化、またはその両方を行うことによって、ネットワーク転送を保護します。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 およびその自動鍵交換プロトコル (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によって中央のキーストアが提供されます。メタスロットを使用するように IKE を構成すると、組織は鍵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と呼ばれるソフトウェアキーストアを選択できます。Oracle Solaris は、IKE Version 2 (IKEv2) プロトコルおよび IKEv1 プロトコルをサポートします。

IPsec と IKE は、構成を必要とするため、インストールしてもデフォルトでは有効になりません。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 11.3 でのネットワークのセキュリティー保護』 の 第 8 章, 「IP セキュリティーアーキテクチャーについて」
- 『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 9 章, 「IPsec の構成」
- 『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 「IPsec と FIPS 140-2」
- 『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 10 章, 「インターネット鍵交換について」
- 『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 11 章, 「IKEv2 の構成」
- 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

デフォルトでは、Oracle Solaris の Secure Shell 機能は、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。ほかのすべてのネットワークサービスは、無効または待機専用モードになっています。

現在の Oracle Solaris リリースには、Secure Shell のデフォルト `sunssh` 実装と、OpenSSH 6.5p1 および追加機能の上に構築された Secure Shell の新しい `openssh` 実装の両方が含まれています。

Secure Shell では、システム間に暗号化された通信チャネルが作成されます。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。

詳細については、次を参照してください。

- 『Oracle Solaris 11.3 での Secure Shell アクセスの管理』 の 第 1 章, 「Secure Shell の使用」
- 『Oracle Solaris 11.3 での Secure Shell アクセスの管理』 の 「Secure Shell と FIPS 140」
- 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。

注記 - これらのマニュアルページをオンラインで表示すると、システムで有効な Secure Shell の実装についての説明が表示されます。

Kerberos サービス

Oracle Solaris の Kerberos 機能を使用すると、システムごとに異なるオペレーティングシステムが実行され、Kerberos サービスが実行され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とセキュアなトランザクションが可能です。AI を使用して Kerberos クライアントをインストールすると、そのクライアントは最初のブート時に Kerberos システムになります。

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 サービスでは、強力なユーザー認証とともに、整合性とプライバシが提供されます。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 11.3 システムのインストール』 の 「AI を使用して Kerberos クライアントを構成する方法」『Oracle Solaris 11.3 での Kerberos およびその他の認証サービスの管理』
- 『Oracle Solaris 11.3 での Kerberos およびその他の認証サービスの管理』
- 『Oracle Solaris 11.3 での Kerberos およびその他の認証サービスの管理』 の 「FIPS 140-2 アルゴリズムと Kerberos 暗号化タイプ」
- 選択したマニュアルページには、`kadmin(1M)`、`kdcmgr(1M)`、`kerberos(5)`、`kinit(1)`、および `krb5.conf(4)` が含まれています。

システムセキュリティーの維持

Oracle Solaris は、システムのセキュリティーを維持するために次の機能を提供します。

- 検証済みブート - ブートプロセスをセキュリティー保護します。検証済みブートは、デフォルトでは無効になっています。
- リポジトリの検証 – ローカル IPS リポジトリファイルが有効であることを確認します。
- パッケージの検証 – インストール済みパッケージが有効であることを確認します。
- 監査サービス - システムのアクセスと使用を監査します。監査機能はデフォルトで有効になります。
- ファイルの整合性の検証 - BART マニフェストによってシステム上のあらゆるファイルをリストできます。また、マニフェストの比較によってファイルの整合性が維持されていることを検証します。
- コンプライアンスレポート - Oracle Solaris は、システムの評価に使用する複数のセキュリティーベンチマークを提供します。これらの評価によって、システムのセキュリティー状況の評価に役立つレポートが生成されます。
- ログファイル - SMF は、あらゆるサービスに対してログファイルを提供します。サービスのログファイルを見つけるには、`svcs -L` *service* コマンドを実行します。`syslog` ユーティリティーは、システムサービスに対するログの名前指定と構成を行う中央ファイルを提供し、オプションで管理者に重大なイベントを通知できます。その他の機能 (監査など) でも、独自のログが作成されます。たとえば、`pkg history` コマンドを使用してパッケージサマリー情報を表示できます。

検証済みブート

検証済みブートは、システムのブートプロセスをセキュリティー保護し、承認されていないカーネルモジュールやトロイの木馬アプリケーションのインストールなどの脅威からシステムを保護する Oracle Solaris 機能です。デフォルトでは、検証済みブートは無効になっています。

詳細は、Unresolved link to " Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護 の ベリファイドブートの使用"および『Oracle Solaris カーネルゾーンの作成と使用』 の 「ベリファイドブートを使用した Oracle Solaris カーネルゾーンのセキュリティー保護」を参照してください。

パッケージの整合性の検証

パッケージの整合性は、インストールの前とあとに検証できます。ローカル IPS リポジトリを使用している場合は、`pkgrepo verify` コマンドを実行して、そのリポジトリが破損していないことを検証できます。`ignore` 以外のすべての署名ポリシーでは、このコマンドは、署名付きパッケージが正しく署名されていることを検証します。

パッケージをインストールまたは更新したあと、`pkg verify` コマンドを実行して、たとえば、システム上のパッケージが正しくない所有権またはハッシュを含むファイルをインストールしなかったことを確認できます。`ignore` 以外のすべての署名ポリシーでは、このコマンドは、署名付きパッケージが正しく署名されていることを検証します。

詳細については、次を参照してください。

- 『Oracle Solaris 11.3 ソフトウェアの追加と更新』 の 「パッケージの署名のプロパティー」
- 『Oracle Solaris 11.3 パッケージリポジトリのコピーと作成』
- `pkg(1)` のマニュアルページ
- 61 ページの「システムセキュリティーの保守とモニタリング」
- 39 ページの「パッケージの検証方法」

監査サービス

Oracle Solaris は、システムのアクセスと使用に関するデータを収集する監査サービスを提供します。監査データによって、セキュリティー関連のシステムイベントに関する、信頼性の高いタイムスタンプ付きのログが提供されます。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、コンプライアンス、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。

- 監査に関するマニュアルページの一覧については、『Oracle Solaris 11.3 での監査の管理』 の 第 7 章, 「監査の参照情報」を参照してください。
- ガイドラインについては、48 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 11.3 での監査の管理』 の 第 1 章, 「Oracle Solaris での監査について」を参照してください。
- 監査タスクについては、『Oracle Solaris 11.3 での監査の管理』 の 第 3 章, 「監査サービスの管理」を参照してください。

ファイルの整合性の検証

BART とは、暗号化強度ハッシュ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。BART を使用すると、システムのファイルレベルのチェックを一定期間にわたって実行することによって、システムを包括的に検証できます。31 ページの「パッケージの整合性の検証」の説明に従ってファイルが正しくインストールされていることを確認したあと、BART を使用して、ファイルの変更を簡単かつ確実に追跡できます。

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。システムのファイルを、システムの元のファイルやほかのシステムのファイルと比較できます。レポートには、システムにパッチが適用されていないこと、侵入者が承認されていないファイルをインストールしたこと、または侵入者がシステムファイル (`root` が所有するファイルなど) のアクセス権や内容を変更したことが示される可能性があります。

詳細については、次を参照してください。

- 概要および例については、『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 の 第 2 章, 「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。
- 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。

セキュリティー標準に対するコンプライアンス

`compliance assess` コマンドは、システムのセキュリティー状況のスナップショットを提供します。評価のレポートには、業界のセキュリティーベンチマークを満たすために必要な具体的なシステムの変更点が示されます。さらに、これらのベンチマークからテーラリングを作成できます。テーラリングとは、セキュリティーベンチマークおよびプロファイルに基づいたカスタマイズされた評価です。詳細は、『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』および `compliance(1M)` のマニュアルページを参照してください。

ログファイル

Oracle Solaris のサービス管理機能 (SMF) は、サービスのステータスをサービス単位でログに記録します。監査や Secure Shell など、多くのサービスは独自のログを書き込みます。`syslog` または `rsyslog` デーモンは、管理者に多くのサービスの重大な状態を通知および警告できる集中管理されたログを書き込みます。たとえば、`syslog` に

要約された監査レコードを書き込むように監査を構成できます。syslogd(1M) および syslog.conf(4) のマニュアルページを参照してください。

ラベル付きセキュリティー

Oracle Solaris のラベル付きセキュリティーは、Trusted Extensions 機能によって提供されます。

Oracle Solaris の Trusted Extensions 機能

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。

Trusted Extensions の実装は、互換性を最大限に確保し、オーバーヘッドを最小限に抑えながら、高度な保証を提供できるという点で独自性があります。Trusted Extensions は、35 ページの「Oracle Solaris 11 の Common Criteria EAL4+ 認定」の一部です。

Trusted Extensions は、Common Criteria の Labeled Security Package (LSP) の要件を満たしています。35 ページの「Oracle Solaris 11 の Common Criteria EAL4+ 認定」を参照してください。

詳細については、次を参照してください。

- Trusted Extensions の構成と保守の詳細については、『Trusted Extensions 構成と管理』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)、labeladm(1M)、および labeld(1M) が含まれています。

ラベル付きファイルシステム

デフォルトでは、ある 1 つのラベルが付けられたゾーン内のファイルシステムには、その同じラベルが割り当てられます。マルチレベルの ZFS データセットを作成し、

それを Trusted Extensions システムにマウントし、適切なアクセス権を使用してそのデータセット内のファイルをアップグレードおよびダウングレードできます。詳細は、『Trusted Extensions 構成と管理』 の 「ファイルのラベル変更に使用されるマルチレベルのデータセット」を参照してください。

ラベル付きネットワーク通信

Trusted Extensions は、ネットワーク通信にラベルを付けます。送信元ネットワークのエンドポイントに関連付けられたラベルと受信先ネットワークのエンドポイントに関連付けられたラベルの比較に基づいて、データフローが制限されます。ゲートウェイと中間ホップにもラベルを付けて、通信のラベルで情報が通過できるようにする必要があります。NFS とマルチレベルの ZFS データセットによって、ネットワークに追加機能が提供されます。

詳細については、次を参照してください。

- 『Trusted Extensions 構成と管理』 の 「Trusted Extensions でのネットワークインタフェースの構成」
- 『Trusted Extensions 構成と管理』 の 第 15 章, 「トラステッドネットワーク」
- 『Trusted Extensions 構成と管理』 の 第 16 章, 「Trusted Extensions でのネットワークの管理」

Trusted Extensions マルチレベルデスクトップ

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。自分に許可されたラベルだけが表示されるようにユーザーを構成できます。各ラベルは、別個のパスワードを要求するように構成できます。

詳細は、『Trusted Extensions ユーザーズガイド』を参照してください。ユーザーを構成するには、『Trusted Extensions 構成と管理』 の 第 11 章, 「Trusted Extensions でのユーザー、権利、役割の管理」を参照してください。

セキュアに実行されるアプリケーションの記述

開発者は、Oracle Solaris でセキュアに実行されるアプリケーションを記述およびコンパイルしてください。一般的な情報については、次を参照してください。

- 『Oracle Solaris 11 セキュリティーサービス開発ガイド』

- 『Oracle Solaris 11.3 リンカーとライブラリガイド』
- ld(1) のマニュアルページの `aslr`、`nxheap`、および `nxstack` 実行時フラグ

特定の推奨事項については、次を参照してください。

- 『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,」
- 『Oracle Solaris 11 セキュリティーサービス開発ガイド』 の 付録 G, 「C 関数を使用する際のセキュリティー上の考慮事項,」
- 『Oracle Solaris 11.3 リンカーとライブラリガイド』 の 「ランタイムセキュリティー」

セキュリティー標準および評価

Oracle Solaris OS は、Common Criteria および FIPS 140-2 という 2 つのセキュリティー標準に準拠しているとの認証を受けています。

FIPS 140-2-2 レベル 1 暗号化の検証

Oracle Solaris の暗号化フレームワーク機能は、Oracle Solaris 11.3 SRU 5.6 リリースでのユーザーランドおよびカーネルの機能について FIPS 140-2-2 レベル 1 で検証されています。Oracle Solaris 11.3 上で実行される OpenSSL モジュールは、FIPS 140-2-2 でも検証されています。OpenSSL を暗号化として使用するアプリケーションはすべて、この検証済みモジュールを使用できます。詳細は、『Oracle Solaris 11.3 での FIPS 140 対応システムの使用』を参照してください。

Oracle Solaris 11 の Common Criteria EAL4+ 認定

Oracle Solaris 11 は、Canadian Common Criteria Scheme の Evaluation Assurance Level 4 (EAL4) で認定され、欠陥修正 (EAL4+) によって拡張されています。EAL4 は、Common Criteria Recognition Arrangement (CCRA) の下で 26 か国が相互に承認している最高レベルの評価です。

この認定は、Operating System Protection Profile (OSPP) を対象としており、次の拡張パッケージを含んでいます。

- Advanced Management
- Extended Identification and Authentication

- ラベル付きセキュリティー
- Virtualization

この認定については、次を参照してください。

- Oracle セキュリティー評価マトリックス (http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)
- Common Criteria Recognition Arrangement (http://www.commoncriteriaportal.org/ccra/)
- 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。

- ソフトウェアセキュリティーの重要性 (https://www.oracle.com/support/assurance/index.html)
- 『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」
- コードのセキュリティー保護に関する記事 (http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do)

♦ ♦ ♦ 第 2 章

2 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。

Oracle Solaris OS のインストール

Oracle Solaris OS をインストールするには、パッケージリポジトリからグループと呼ばれる一連のパッケージを選択します。各グループは、多目的サーバー、最小インストールシステム、デスクトップシステムなど、さまざまな用途に対応するパッケージを提供します。パッケージは署名されており、パッケージの安全な転送を確認できます。

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 Small Server -** 自動インストーラ (AI) インストールおよびテキストインストーラによって、パッケージを追加できる便利なコマンド行環境を提供する

`group/system/solaris-small-server` グループがオプションでインストールされます。

- **Oracle Solaris Minimal Server** – 自動インストーラ (AI) インストールおよびテキストインストーラによって、必要なパッケージだけを追加できる最小のコマンド行環境を提供する `group/system/solaris-minimal-server` グループがオプションで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。

  集中管理用途にデスクトップシステムを作成するには、`group/feature/multi-user-desktop` グループをデスクトップサーバーに追加します。詳細は、記事『マルチユーザー環境の Oracle Solaris デスクトップの最適化』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 11.3 システムのインストール』 の パート 3,「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。自動インストール (AI) では、インストールサーバー、指定されたクライアントシステム、指定されたインストールサービスのすべてのクライアント、およびその他の AI クライアントのインストールを、証明書と鍵によってセキュリティー保護できます。『Oracle Solaris 11.3 システムのインストール』 の 「自動インストールのセキュリティーの向上」を参照してください。

メディアを選択する指針として、次のインストレーションガイドとパッケージ内容のガイドを参照してください。

- 『Oracle Solaris 11.3 システムのインストール』
- 『Oracle Solaris 11.3 カスタムインストールイメージの作成』
- 『Oracle Solaris 11.3 ソフトウェアの追加と更新』
- 『Oracle Solaris 11.3 Package Group Lists』

初期の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 オペレーティングシステム 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。

表 1 システムのセキュリティー保護のタスクマップ

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。	パッケージが有効であることを確認します。また、署名付きパッケージの署名も確認します。	39 ページの「パッケージの検証方法」
2. 実行可能ファイルが保護されていることを確認します。	スタックやヒープを侵害から保護するセキュリティー拡張機能が有効になっていることを確認します。	『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「悪影響からのプロセスヒープと実行可能スタックの保護」

タスク	説明	参照先
3. 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。x86 システムでは、GRUB メニューへのアクセスが制御されます。SPARC システムでは、`eeprom` コマンドによってハードウェアが保護されます。	『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の 「システムハードウェアアクセスの制御」
4. 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。	41 ページの「不要なサービスを無効にする方法」
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。	41 ページの「ユーザーから電源管理機能を削除する方法」
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。	認証前および認証後のユーザーにシステムがモニターされていることを通知します。	42 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」

▼ パッケージの検証方法

パッケージの整合性の検証には、パッケージの署名の検証が含まれます。この手順では、有効かつセキュアなパッケージリポジトリが保持されていることを前提にしています。サマリーについては、62 ページの「ローカル IPS リポジトリからのセキュアなパッケージのインストールの確認」を参照してください。手順については、『Oracle Solaris 11.3 パッケージリポジトリのコピーと作成』を参照してください。

始める前に IPS リポジトリおよびパッケージを管理するには、権利を持つ管理者になる必要があります。必要な権利については、『Oracle Solaris 11.3 パッケージリポジトリのコピーと作成』 の 「リポジトリ管理の特権」を参照してください。

1. **パッケージの署名をチェックしていることを確認します。**

   a. **イメージおよびパブリッシャーの署名ポリシーを表示します。**

      この例では、管理者がデフォルトの署名ポリシーを `ignore` に明示的に変更しています。これには、すべてのマニフェストの署名を無視する効果があります。

```
$ pkg property signature-policy
PROPERTY             VALUE
signature-policy     ignore
$ pkg publisher
...
          Properties:
                    signature-policy = ignore
```

   b. **署名ポリシーが実装しようとしている値より弱い値に設定されている場合は、そのポリシーを変更します。**

使用可能なポリシーは次のとおりです。

- `verify` – 署名が含まれているすべてのマニフェストが有効に署名されていることを確認しますが、インストール済みパッケージがすべて署名されている必要はありません。
- `require-signatures` – 新しくインストールされたすべてのパッケージに、有効な署名が少なくとも 1 つ含まれている必要があります。
- `require-names` – `require-signatures` と同じ要件に従いますが、`signature-required-names` プロパティーで一覧表示される文字列が署名の信頼のチェーンを検証するためにも使用される必要があります。

次のコマンドは、イメージの署名ポリシーを `ignore` からデフォルトの `verify` に変更します。

```
$ pkg set-property signature-policy verify
```

c. (オプション) `solaris` パブリッシャーのより強力な署名ポリシーを確立し、新しいポリシーを表示します。

パブリッシャーは、そのパブリッシャーの値が明示的に変更されないかぎり、署名ポリシーをイメージから継承します。たとえば、パッケージが常に署名されるパブリッシャーには `verify` より強力なポリシーを設定することもできます。

```
$ pkg set-publisher --set-property signature-policy=require-signatures solaris
$ pkg -publisher solaris
            Publisher: solaris
...
      Catalog Updated: Feb 8, 2015  02:01:01 AM
              Enabled: Yes
           Properties:
                       signature-policy = require-signatures
```

2. パッケージのインストール後、インストールウィンドウ内のすべてのエラーメッセージに対して適切なアクションを実行します。

3. `pkg verify` コマンドを実行し、その結果をログファイルに送信します。

```
# pkg verify > /var/log/filename
```

詳細は、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。

4. エラーがないかどうかログをレビューします。

5. エラーが見つかった場合は、再インストールするか、またはエラーを修正します。

詳細は、『Oracle Solaris 11.3 ソフトウェアの追加と更新』 の 「パッケージの検証と検証エラーの修正」を参照してください。

▼ 不要なサービスを無効にする方法

この手順を使用して、このシステムでは不要な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 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **オンラインネットワーク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/http:apache22
online         Sep_07   svc:/network/nfs/server: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 サーバーでも Web サーバーでもないのに、それらのサービスがオンラインである場合は、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 11.3 でのシステムサービスの管理』 の 第 1 章, 「サービス管理機能の概要」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、システムのコンソール上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。コンソールユーザーがシステムのハードウェアを取り外すことができる場合、このソフトウェア解決方法は有効ではありません。

始める前に root 役割になる必要があります。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **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。**

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
              solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                  Network Autoconf User
 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 11.3 でのユーザーとプロセスのセキュリティー保護』 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. **ステップ 2で作成した権利プロファイルを割り当てます。**

   - 権利プロファイルを共有するユーザーの数が多い場合は、権利プロファイルにこの値を設定することがスケーラブルな解決方法になります。

     ```
     # usermod -P shared-profile username
     ```

   - また、`policy.conf` ファイルでシステムごとにプロファイルを割り当てることもできます。

     ```
     # pfedit /etc/security/policy.conf...
     #PROFS_GRANTED=Basic Solaris User
     PROFS_GRANTED=shared-profile,Basic Solaris User
     ```

参照 詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 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。`/etc/issue` ファイルは、たとえば認証前にデスクトップに表示されたり、`ssh` コマンドを使用してリモートログインしたときに表示されたりします。`/etc/motd` ファイルは、認証後に表示されます。

注記 - 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。セキュリティーメッセージの内容については、会社の弁護士に相談してください。

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 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **/etc/issue ファイルを作成し、セキュリティーメッセージを追加します。**

```
# pfedit /etc/issue
ALERT   ALERT   ALERT   ALERT   ALERT

This system is available to authorized users only.

If you are an authorized user, continue.

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

   ssh、graphical-login/gdm、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。

   詳細は、issue(4) および 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。

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、次のタスクがもっとも多く順番に実行されています。

表 2 ユーザーのセキュリティー保護のタスクマップ

タスク	説明	参照先
強固なパスワードと定期的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。	44 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。	47 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。	45 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」
すべてのユーザーに対して cusa 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。	48 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」
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 11.3 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管理」

タスク	説明	参照先
	事前定義された ARMOR 役割を使用するか、独自の役割を作成するか、または独自の役割で ARMOR を拡張できます。	『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の「ユーザーへの権利の割り当て」
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 11.3 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。	49 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と最新の業界標準を満たしていない場合に、この手順を使用します。これらの手順は、`/etc/default/passwd` ファイルの変数エントリの順序に従います。

始める前に `solaris.admin.edit/etc/default/passwd` 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。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **政府および標準化団体からの最新のパスワードセキュリティー推奨事項を確認します。**

   たとえば、National Cyber Security Centre と米国連邦取引委員会 の Web サイトにアクセスして、パスワードに関する最新の記事を検索します。

2. **`pfedit` コマンドを使用して、`/etc/default/passwd` ファイルを次のように変更します。**

   a. **パスワードを 4 か月ごとに (ただし、3 週間ごとより低い頻度で) 変更するようにユーザーに要求します。**

   ```
   ## /etc/default/passwd
   ##
   #MAXWEEKS=
   #MINWEEKS=
   MAXWEEKS=13
   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、passwd(1) のマニュアルページを参照してください。
- 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、16 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。
- https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes を確認してください。

▼ 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。

注記 - 役割は共有されるアカウントです。ロックされた 1 人のユーザーが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には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。むしろ、管理システムに異常な使用状況がないかどうかをモニターし、管理者が常に管理システムを使用できるようにしてください。

root 役割になる必要があります。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

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

属性値のスコープを選択します。

- **システム全体に設定します。**
  この保護は、システムを使用しようとするすべてのユーザーに適用されます。

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

- **ユーザーごとに設定します。**
  この保護は、このコマンドの実行対象のユーザーに対してのみ適用されます。ユーザー数が多い場合、これはスケーラブルな解決方法ではありません。

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

- **権利プロファイルを作成して割り当てます。**
  この保護は、この権利プロファイルを割り当てるすべてのユーザーまたはシステムに適用されます。

  a. **権利プロファイルを作成します。**

```
# profiles -p shared-profile -S ldap
shared-profile: set lock_after_retries=yes
...
```

  権利プロファイルの作成の詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「権利プロファイルと承認の作成」を参照してください。

  b. **権利プロファイルをユーザーまたはシステム全体に割り当てます。**
  権利プロファイルを共有するユーザーの数が多い場合は、権利プロファイルにこの値を設定することがスケーラブルな解決方法になります。

```
# usermod -P shared-profile username
```

  また、`policy.conf` ファイルでシステムごとにプロファイルを割り当てることもできます。

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

2. **RETRIES セキュリティー属性を 3 に設定します。**
   属性値のスコープを選択します。

   - **システム全体に設定します。**

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

- **ユーザーごとに設定します。**

  ```
  # usermod -K lock_after_retries=3 username
  ```

- **権利プロファイルを作成して割り当てます。**

  ステップ 1 の「権利プロファイルを作成して割り当てます」オプションに従って、lock_after_retries=3 を含む権利プロファイルを作成します。

3. **ロックされたユーザーをロック解除するには、passwd コマンドを使用します。**

   ```
   # passwd -u username
   ```

   ロックされたユーザーは、管理者の操作なしではログインできません。files と ldap の両方のネームサービスでユーザーアカウントをロック解除できます。

参照

- ユーザーおよび役割のセキュリティー属性については、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 第 8 章, 「Oracle Solaris 権利リファレンス」を参照してください。
- 選択したマニュアルページには、passwd(1)、policy.conf(4)、profiles(1)、user_attr(4)、および usermod(1M) 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

umask ユーティリティーは、ユーザーが作成したファイルのファイルアクセス権ビットを設定します。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 スケルトンファイルを編集する権限がある管理者になる必要があります。root 役割にはこれらの権限が割り当てられます。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **Oracle Solaris でユーザーシェルのデフォルトとして提供されているサンプルファイルを表示します。**

   ```
   # ls -1a /etc/skel
   .bashrc
   ```

```
.profile
local.cshrc
local.login
local.profile
```

2. **ユーザーに割り当てる `/etc/skel` ファイルに `umask` 値を設定します。**
   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。
     (`751`) – 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
     (`750`) – 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 11.3 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管理」
- 『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 の 「umask のデフォルト値」
- 選択したマニュアルページには、`useradd(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、システムアクセス、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。

注記 - 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 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **管理権利プロファイルおよび役割が割り当てられたユーザーによる特権コマンドのすべての仕様を監査します。**
   事前選択マスクに `cusa` 監査クラスを追加します。

```
# usermod -K audit_flags=cusa:no username
```

```
# rolemod -K audit_flags=cusa:no rolename
```

cusa メタクラスに含まれる監査クラスは、/etc/security/audit_class ファイルにリストされます。

2. **監査されるコマンドへの引数を記録します。**

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

3. **(オプション) 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
```

注記 - このポリシーオプションは、トラブルシューティング時に役立つことがあります。

参照

- 監査ポリシーについては、『Oracle Solaris 11.3 での監査の管理』 の 「監査ポリシー」を参照してください。
- 監査フラグの設定の例については、『Oracle Solaris 11.3 での監査の管理』 の 「監査サービスの構成」および『Oracle Solaris 11.3 での監査の管理』 の 「監査サービスのトラブルシューティング」を参照してください。
- auditconfig(1M) のマニュアルページ

▼ 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、標準ユーザーまたはゲストユーザーの基本セットから一部の基本特権を削除できます。たとえば、Sun Ray ユーザーは自分が所有していないプロセスのステータスを確認でき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 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **基本特権セットの完全な定義を一覧表示します。**

   次の 3 つの基本特権は、削除の対象になる可能性があります。

```
% ppriv -lv basic
file_link_any
 Allows a process to create hardlinks to files owned by a uid
 different from the process' effective uid.
...
proc_info
 Allows a process to examine the status of processes other
 than those it can send signals to.  Processes which cannot
```

```
 be examined cannot be seen in /proc and appear not to exist.
proc_session
 Allows a process to send signals or trace processes outside its
 session.
...
```

2. **特権削除のスコープを選択します。**

   - **システム全体に設定します。**

     システムを使用しようとするユーザーは、これらの特権を拒否されます。この特権削除の方法は、だれでも使用可能なコンピュータに適している可能性があります。

     ```
     # pfedit /etc/security/policy.conf
     ...
     #PRIV_DEFAULT=basic
     PRIV_DEFAULT=basic,!file_link_any,!proc_info,!proc_session
     ```

   - **個別のユーザーから特権を削除します。**

     - **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
       ```

     - **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
       ```

     - **ユーザーの現在のセッションから ssh セッションを開始するなど、ユーザーが 2 つ目のセッションを開始できないようにします。**

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

     - **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
       ```

   - **権利プロファイルを作成して割り当てます。**

     この保護は、この権利プロファイルが割り当てられたユーザーまたはシステムに適用されます。

     a. **権利プロファイルを作成します。**

        ```
        # profiles -p shared-profile -S ldap
        shared-profile: set defaultpriv=basic,!file_link_any,!proc_info,!proc_session
        ...
        ```

        権利プロファイルの作成の詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「権利プロファイルと承認の作成」を参照してください。

b. 権利プロファイルをユーザーまたはシステム全体に割り当てます。

Sun Ray ユーザーやリモートユーザーなど、権利プロファイルを共有するユーザーの数が多い場合は、権利プロファイルにこの値を設定することがスケーラブルな解決方法になります。

```
# usermod -P shared-profile username
```

また、`policy.conf` ファイルでシステムごとにプロファイルを割り当てることもできます。

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

参照 詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 第 1 章, 「権利を使用したユーザーとプロセスの制御について」 および `privileges(5)` のマニュアルページを参照してください。

ネットワークの保護

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。

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、IP、ARP、および TCP プロトコルを強化します。

表 3 ネットワークの構成のタスクマップ

タスク	説明	参照先
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 11.3 でのネットワークのセキュリティー保護』 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 11.3 でのネットワークのセキュリティー保護』 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 11.3 でのネットワークのセキュリティー保護』 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 11.3 でのネットワークのセキュリティー保護』 の 「厳密なマルチホームを設定する方法」

タスク	説明	参照先
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 11.3 でのネットワークのセキュリティー保護』 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 11.3 でのネットワークのセキュリティー保護』 の 「中断中の TCP 接続の最大数を設定する方法」
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。	『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 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。	52 ページの「TCP ラッパーの使用方法」
ファイアウォールを構成します。	パケットフィルタまたは IP フィルタ機能を使用してファイアウォールを提供します。	『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 5 章, 「パケットフィルタファイアウォールの構成」 『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 7 章, 「IP フィルタファイアウォールの構成」
暗号化され認証されたネットワーク接続を構成します。	IPsec と IKE を使用すると、IPsec と IKE が一緒に構成されたノードおよびネットワーク間での転送が保護されます。	『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 9 章, 「IPsec の構成」 『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 11 章, 「IKEv2 の構成」

▼ 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。これはデフォルトで保護されます。**
2. **すべての `inetd` サービスで TCP ラッパーを有効にするには、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 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 `proftpd.conf` ファイルに追加して、モジュールをロードします。

```
# pfedit /etc/proftpd.conf
<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
```

ファイルシステムの保護

ZFS ファイルシステムは軽量であり、暗号化、圧縮、および予約された容量とディスク容量の割り当て制限による構成が可能です。

`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、54 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 11.3 での ZFS ファイルシステムの管理』 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。

表 4 ファイルシステムの保護のタスクマップ

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 11.3 での ZFS ファイルシステムの管理』 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 11.3 での ZFS ファイルシステムの管理』 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 11.3 での ZFS ファイルシステムの管理』 の 「ZFS ファイルシステムの暗号化」 『Oracle Solaris 11.3 での ZFS ファイルシステムの管理』 の 「ZFS ファイルシステムを暗号化する例」
`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。	54 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みることをお勧めします。

始める前に vfstab ファイルを編集するには、solaris.admin.edit/etc/vfstab 承認が割り当てられた管理者になる必要があります。ゾーンをリブートするには、「Maintenance and Repair」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。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 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

1. **システムのメモリー量を調べます。**

   注記 - 次の例に使用する SPARC T3 シリーズシステムは、高速な I/O のための 1 台のソリッドステートディスク (SSD) と、8 台の 279.40M バイトディスクを搭載しています。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 ≈ 3072M
```

   大規模システムでは、乗数として .20 を使用します。

```
523776M x .20 ≈ 104755M
```

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
#
...
#swap       -            /tmp        tmpfs   -       yes     -
swap        -            /tmp        tmpfs   -       yes     size=104700m
/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 Tues Feb 4 14:07:27 2014
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=104700m/dev=89c0006 on Tues ...
```

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

デフォルトでは、`root` 役割のみがシステムファイルのアクセス権を変更できます。`solaris.admin.edit/`*path-to-system-file* 権限を割り当てられた役割およびユーザーは、その *system-file* を変更できます。`root` 役割のみがすべてのファイルを検索できます。

表 5 ファイルの保護と変更のタスクマップ

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。	47 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」

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。	『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 の「ファイル属性を使用して ZFS ファイルにセキュリティーを追加する」
Oracle データベースログなどの重要なファイルの削除を禁止するための ACL を指定します。	`rm` コマンドが `root` 役割で実行したときでも失敗するように、ファイルまたはディレクトリで `nounlink` プロパティーを設定します。	『Oracle Solaris 11.3 での ZFS ファイルシステムの管理』 の 「nounlink 属性による誤った削除を防止する」
システムファイルの整合性を保守します。	スクリプトまたは BART を使用して疑わしいファイルを検索します。	『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 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」

システムアクセスとシステム使用のセキュリティー保護

Oracle Solaris セキュリティー機能を構成して、システム使用を保護できます。これには、システム上およびネットワーク上のアプリケーションとサービスが含まれます。

表 6 システムアクセスとシステム使用のセキュリティー保護のタスクマップ

タスク	説明	参照先
プログラムでのヒープまたは実行可能スタックの破損を防止します。	スタックやヒープを侵害から保護するセキュリティー拡張機能が有効になっていることを確認します。	『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』 の「悪影響からのプロセスヒープと実行可能スタックの保護」
監査を構成します。	監査構成の適用範囲とファイル整合性をカスタマイズします。	62 ページの「監査サービスの使用」
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 11.3 でのシステム管理のトラブルシューティング』 の 「ファイルパスの有効化」 『Oracle Solaris 11.3 でのシステム管理のトラブルシューティング』 の 「コアファイル仕様の管理」
SSL カーネルプロキシ で Web サーバーを保護します。	Secure Sockets Layer (SSL) プロトコルを使用すると、Web サーバーの通信を暗号化および高速化できます。	『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』 の 第 3 章, 「Web サーバーと Secure Sockets Layer プロトコル」
特権と承認を使用してレガシーサービスを保護します。	アプリケーションに制限された権利を割り当てることによって、最小特権でアプリケーションを実行します。	57 ページの「SMF によるレガシーサービスの保護」
アプリケーションを含むゾーンを作成します。	ゾーンはプロセスを分離するコンテナです。アプリケーションやアプリケーションの一部分を分離できます。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。	『Oracle Solaris ゾーンの紹介』

タスク	説明	参照先
ゾーンのリソースを管理します。	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。	『Oracle Solaris 11.3 でのリソースの管理』

SMF によるレガシーサービスの保護

Oracle Solaris のサービス管理機能 (SMF) にアプリケーションを追加し、サービスを開始、リフレッシュ、および停止する権利を要求することにより、アプリケーションの構成を信頼できるユーザーまたは役割に制限できます。

`inetd` によって実行されるサービスの場合は、セキュリティー侵害を回避するために並列プロセスの数を制御してください。詳細は、『Oracle Solaris 11.3 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理』 の 「inetd ベースのサービスを実行するシステムの構成に関する推奨事項」を参照してください。

詳細および手順については、次を参照してください。

- 『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「拡張特権を使用したリソースのロックダウン」
- 選択したマニュアルページには、`smf(5)`、`smf_security(5)`、`svcadm(1M)`、`svcbundle(1M)`、および `svccfg(1M)` が含まれています。

Kerberos ネットワークの構成

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 11.3 での Kerberos およびその他の認証サービスの管理』 の 第 3 章, 「Kerberos サービスの計画」
- 『Oracle Solaris 11.3 での Kerberos およびその他の認証サービスの管理』 の 第 4 章, 「Kerberos サービスの構成」
- 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。

ラベル付きマルチレベルセキュリティーの追加

Trusted Extensions は、ラベルベースの必須アクセス制御 (MAC) ポリシーを適用することによって 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

`system/trusted` および `system/trusted/trusted-global-zone` パッケージは、マルチレベルデスクトップを必要としないヘッドレスシステムやサーバーに十分に対応します。`system/trusted/trusted-extensions` 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。`trusted-extensions` パッケージをインストールすると、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 1, 「Trusted Extensions の初期構成,」
- 『Trusted Extensions 構成と管理』 の パート 2, 「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 11.3 でのネットワークのセキュリティー保護』 の 第 8 章, 「IP セキュリティーアーキテクチャーについて」
- 『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」

♦ ♦ ♦ 第 3 章

3 Oracle Solaris セキュリティーの保守とモニタリング

初期のインストールと構成のあとに、次のアクションによってシステムのセキュリティー状況を保守およびモニターできます。

- システムを最新の CPU (クリティカルパッチアップデート) および SRU (サポートリポジトリアップデート) に更新する
- パッケージおよびファイルの整合性チェックの実行
- コンプライアンスチェックの実行
- ネットワークアクティビティーのモニタリング
- 監査レコードの定期的な確認

システムセキュリティーの保守とモニタリング

次の表に説明するタスクは、システムおよびデータのアクセスと使用、およびサイトのセキュリティー要件の順守を保守およびモニターします。

表 7 システムの保守とモニタリングのタスクマップ

タスク	説明	参照先
最新バージョンの OS を実行していることを確認します。	最新の更新およびセキュリティー修正がインストールされていることを確認します。	『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』 の 「Oracle Solaris での CVE アップデートの管理」
ローカル IPS リポジトリが有効であることを確認します。	ローカルリポジトリ内のファイルが一連のチェックに合格することを確認します。また、署名付きパッケージの署名も検証します。	62 ページの「ローカル IPS リポジトリからのセキュアなパッケージのインストールの確認」
システム上のパッケージを検証します。	更新後のパッケージがソースパッケージと同一であることを確認し、署名付きパッケージの署名を検証します。	39 ページの「パッケージの検証方法」

タスク	説明	参照先
コンプライアンステストを実行します。	セキュリティーベンチマークに対するシステムのコンプライアンスを評価します。	『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』および `compliance(1M)` のマニュアルページ
ファイルの整合性を確認します。	構成後、BART マニフェストを定期的に比較して、変更すべきファイルのみが変更されていることを確認します。	『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 の 「一定期間内で同一システムの目録を比較する方法」
疑わしいファイルを検索します。	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します。	『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』 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」
監査ログを定期的に確認します。	システムの異常なアクセスや使用を検出します。	62 ページの「監査サービスの使用」
監査ログのログインおよびログアウトイベントをリアルタイムで確認します。	違反の試みを発生後ただちに識別します。	64 ページの「リアルタイムでの監査レコードのモニタリング」

ローカル IPS リポジトリからのセキュアなパッケージのインストールの確認

有効で、かつセキュリティー保護された IPS リポジトリを保持することはパッケージのインストールにとって不可欠です。セキュアなリポジトリの作成および保守のためには、『Oracle Solaris 11.3 パッケージリポジトリのコピーと作成』 の 「ローカルの IPS パッケージリポジトリの作成および使用のベストプラクティス」に従います。これらの習慣には、次のものが含まれます。

- 署名付きパッケージの署名を検証していることの確認
- リポジトリ内のファイルが一連のチェック (パッケージが正しく署名されていることを含む) に合格することの確認
- リポジトリへのアクセスの検証

リポジトリの構成および保守の手順については、『Oracle Solaris 11.3 パッケージリポジトリのコピーと作成』を参照してください。パッケージのインストールの検証については、39 ページの「パッケージの検証方法」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 11.3 での監査の管理』で説明されています。マニュアルページとそれらへのリンクの一覧については、『Oracle Solaris 11.3 での監査の管理』 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。

多くのセキュアな環境では、次の監査サービス手順が有効です。

- 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。信頼できるユーザーに役割を割り当てます。

  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。

  役割を作成したり、定義済みの ARMOR 役割を使用したりするには、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「ユーザーへの権利の割り当て」を参照してください。
- `cusa` 監査クラスを使用して、すべての管理者を監査します。

  `cusa` 監査クラス内のイベントは、システムのセキュリティー状況に影響を与える管理アクションを対象としています。詳細は、`/etc/security/audit_class` ファイルを参照してください。手順については、48 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」を参照してください。
- 監査レコードを中央サーバーに送信します。
  - 監査リモートサーバー (ARS) と連携して動作するように監査を構成します。

    監査サービスでは、Oracle Audit Vault を使用して監査レコードを格納、確認、および分析できます。『Oracle Solaris 11.3 での監査の管理』 の 「Oracle Audit Vault and Database Firewall を使用した監査レコードの格納および分析」および『Oracle Solaris 11.3 での監査の管理』 の 「監査ファイルをリモートリポジトリに送信する方法」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。
- `syslog` ユーティリティーで、選択した監査対象イベントのテキストサマリーをモニターします。

  `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 11.3 での監査の管理』 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` 属性を有効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 11.3 での監査の管理』 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。

リアルタイムでの監査レコードのモニタリング

`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。監査のサマリーが生成されたときに、それらを端末ウィンドウに表示するには、次のようなコマンドを実行します。

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

監査ログを構成するには、『Oracle Solaris 11.3 での監査の管理』 の 「syslog 監査ログの構成方法」を参照してください。

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 11.3 での監査の管理』 の 「監査ログ」
- 『Oracle Solaris 11.3 での監査の管理』 の 「監査トレールのオーバーフローの防止」
- 『Oracle Solaris 11.3 での監査の管理』 の 「監査トレールデータの表示」

♦ ♦ ♦ 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 のセキュリティー情報には、役に立つ情報も古くなった情報も含まれています。

Oracle Technology Network にあるセキュリティーの参照資料

Oracle Technology Network Web サイト上の次の文書および記事には、Oracle Solaris 11 システム上のセキュリティーに関する説明が含まれています。

- 『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護』
- 『Oracle Solaris 11.3 でのファイルのセキュリティー保護とファイル整合性の検証』
- 『Oracle Solaris 11.3 でのネットワークのセキュリティー保護』
- 『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』
- 『Oracle Solaris 11.3 での暗号化と証明書の管理』
- 『Oracle Solaris 11.3 での監査の管理』
- 『Oracle Solaris 11.3 での Kerberos およびその他の認証サービスの管理』
- 『Oracle Solaris 11.3 での Secure Shell アクセスの管理』
- 『Oracle Solaris 11.3 セキュリティーコンプライアンスガイド』
- 『Trusted Extensions 構成と管理』
- 『Oracle Solaris 11.3 での FIPS 140 対応システムの使用』
- 『Oracle Solaris 11 セキュリティーサービス開発ガイド』

サードパーティーの刊行物における Oracle Solaris セキュリティーの参照資料

次の文書には、Oracle Solaris 11 システム上のセキュリティーに関する説明が含まれています。

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

  このセキュリティーベンチマークは、セキュリティーコミュニティーのために Center for Internet Security (CIS) によって発行されました。このドキュメントでは、Oracle Solaris オペレーティングシステム のセキュリティー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 へのセキュリティー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、セキュリティースペシャリスト、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。コピーを取得するには、メインページの「Security Benchmarks」リンクをクリックします。
- 『*Oracle Solaris 11 System Administration: The Complete Reference*』。Michael Jang、Harry Foxwell、Christine Tran、Alan Formy-Duval 著。2012 年。McGraw-Hill 社。ISBN 978007179042。

  この市販本には、Oracle Solaris のセキュリティー適用範囲が含まれています。
- 『*Oracle Solaris 11: First Look*』。Philip P.Brown 著。2013 年。Packt Publishing 社。ISBN 9781849688307。

  この市販本では、管理者を対象として Oracle Solaris とそのセキュリティーを紹介しています。
- 『*Oracle Solaris 11 System Administration*』、Bill Calkins 著。2013 年。Prentice Hall 社。ISBN 9780133007114。

  この市販本は、セキュリティー機能を含む Oracle Solaris の新機能を取り上げています。

索引

さ

N

O

P

R

S

T

U

V

Z