

Oracle® Server X5-4 セキュリティーガイド
セキュリティガイド

ORACLE®

Part No: E64498-01
2015 年 6 月

Part No: E64498-01

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

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.

このソフトウェアまた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。このソフトウェアまたはハードウェアは、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。このソフトウェアまた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。このソフトウェアまた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、Oracle Corporation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はオラクル およびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

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。適用されるお客様とOracle Corporationとの間の契約に別段の定めがある場合を除いて、Oracle Corporation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。適用されるお客様とOracle Corporationとの間の契約に定めがある場合を除いて、Oracle Corporation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。

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

基本的なセキュリティ	7
サーバー構成および管理ツールの使用	9
Oracle System Assistant のセキュリティ	9
Oracle ILOM のセキュリティ	10
Oracle Hardware Management Pack のセキュリティ	11
セキュアな環境の計画	13
オペレーティングシステムのセキュリティガイドライン	13
ネットワークポートとネットワークスイッチ	14
VLAN のセキュリティ	15
Infiniband のセキュリティ	15
ハードウェアの物理的なセキュリティ	15
ソフトウェアのセキュリティ	16
セキュアな環境の保守	17
ハードウェアの電源制御	17
アセットの追跡	17
ソフトウェアおよびファームウェアの更新	18
ネットワークのセキュリティ	18
データの保護とセキュリティ	19
ログの保守	19

基本的なセキュリティ

このドキュメントでは、Oracle サーバー、サーバーネットワークインタフェース、および接続されているネットワークスイッチを保護する際に役立つ一般的なセキュリティガイドラインを示します。

注記 - 使用しているシステムおよび特定環境に関するその他のセキュリティ要件については、組織の IT セキュリティ責任者に確認してください。

このセクションでは、すべてのハードウェアおよびソフトウェアを使用する際に準拠すべき4つの基本的なセキュリティ原則(アクセス、認証、承認、およびアカウントリング)について説明します。

■ アクセス

アクセスとは、ハードウェアへの物理的なアクセス、またはソフトウェアへの物理的、または仮想的なアクセスのことを指します。

- ハードウェアやデータを侵入から保護するには、物理的な制御とソフトウェアの制御を行います。
- ソフトウェアに付属のドキュメントを参照して、ソフトウェアで使用可能なセキュリティ機能を有効にしてください。
- サーバーと関連装置は、アクセスが制限された鍵の掛かった部屋に設置してください。
- 鍵付きのドアがあるラックに装置を設置する場合は、ラック内のコンポーネントを保守する必要があるとき以外はドアの鍵は掛けたままにしてください。
- アクセスをコネクタまたはポートに制限すると、SSH 接続よりも強力なアクセスを提供できます。システムコントローラ、配電盤(PDU)、ネットワークスイッチなどのデバイスには、コネクタおよびポートが搭載されています。
- 特にホットプラグまたはホットスワップのデバイスは簡単に取り外すことができるため、これらのデバイスへのアクセスを制限してください。
- 予備の現場交換可能ユニット(FRU)および顧客交換可能ユニット(CRU)は、鍵の掛かったキャビネットに保管してください。鍵の掛かったキャビネットへのアクセスは、承認された人だけに制限してください。

■ 認証

認証とは、ハードウェアまたはソフトウェアのユーザーが本人であることを保証することを指します。

-
- ユーザーが本人であることを保証するには、プラットフォームのオペレーティングシステムにパスワードシステムなどの認証機能を設定します。
 - 担当者がコンピュータ室に入室する際に、従業員バッジを適切に付けていることを確認してください。
 - ユーザーアカウントの場合、必要に応じてアクセス制御リストを使用し、延長セッションにタイムアウトを設定し、ユーザーに権限レベルを設定します。

- **承認**

承認とは、ハードウェアやソフトウェアを操作する担当者に課せられた制限のことを指します。

- トレーニングを受けて使用を認定されたハードウェアとソフトウェアの操作のみを担当者に許可します。
- 読み取り/書き込み/実行のアクセス権を設定して、コマンド、ディスク領域、デバイス、およびアプリケーションへのユーザーアクセスを制御します。

- **アカウントティング**

アカウントティングとは、ログインアクティビティのモニターおよびハードウェアインベントリの保守で使用されるソフトウェアおよびハードウェアの機能のことを指します。

- ユーザーログインをモニターするには、システムログを使用します。特にシステム管理者アカウントとサービスアカウントは強力なコマンドにアクセスできるため、これらのアカウントをモニターしてください。
- すべてのハードウェアのシリアル番号を記録しておいてください。システムアセットを追跡するには、コンポーネントのシリアル番号を使用します。Oracleのパーツ番号は、カード、モジュール、およびマザーボードに電子的に記録されており、インベントリの目的に使用できます。
- コンポーネントを検出および追跡するには、コンピュータハードウェアのすべての主要品目 (FRU など) にセキュリティーマークを付けます。専用の紫外線ペンまたはエンボスラベルを使用してください。

サーバー構成および管理ツールの使用

ソフトウェアおよびファームウェアのツールを使用してサーバーを構成および管理するときは、次のセキュリティーガイドラインに従ってください。

- 9 ページの「Oracle System Assistant のセキュリティー」
- 10 ページの「Oracle ILOM のセキュリティー」
- 11 ページの「Oracle Hardware Management Pack のセキュリティー」

Oracle System Assistant のセキュリティー

Oracle System Assistant は、サーバーハードウェアをローカルまたはリモートで構成および更新したり、サポートされているオペレーティングシステムをインストールしたりする際に役立つインストール済みのツールです。Oracle System Assistant を使用方法については、次の場所にある『Oracle X5 シリーズサーバー管理ガイド』を参照してください。

<http://www.oracle.com/goto/x86AdminDiag/docs>

次の情報は、Oracle System Assistant に関するセキュリティー問題を理解する際に役立ちます。

- **Oracle System Assistant にはブート可能なルート環境が含まれます。**

Oracle System Assistant は、設置済みの内蔵 USB フラッシュドライブで実行されるアプリケーションです。ブート可能な Linux ルート環境上に構築されます。Oracle System Assistant には、基盤となるルートシェルにアクセスする機能も用意されています。システムに物理的にアクセスするユーザーや、Oracle ILOM 経由でシステムにリモート KVM (キーボード、ビデオ、マウス、およびストレージ) アクセスするユーザーは、Oracle System Assistant およびルートシェルにアクセスできます。

ルート環境を使用すると、システム構成およびポリシーを変更したり、その他のディスク上のデータにアクセスしたりできます。サーバーへの物理的なアクセスを保護し、Oracle ILOM ユーザーに対する管理者権限およびコンソール権限を慎重に割り当てることをお勧めします。
- **Oracle System Assistant では、オペレーティングシステムにアクセス可能な USB ストレージデバイスがマウントされます。**

Oracle System Assistant はブート可能な環境であることに加えて、インストール後にホストオペレーティングシステムにアクセス可能な USB ストレージデバイス (フラッシュドライブ) としてマウントされます。これは、保守および再構成のためにツールやドライバにアクセスする際に役立ちます。Oracle System Assistant の USB ストレージデバイスは、読み取りと書き込みの両方が可能であり、ウイルスによって攻撃される可能性があります。

定期的なウイルススキャンや整合性チェックなど、ディスクを保護するときと同じ方法を Oracle System Assistant のストレージデバイスにも適用することをお勧めします。

■ **Oracle System Assistant は無効にできません。**

Oracle System Assistant は、サーバーの設定、ファームウェアの更新と構成、およびホストオペレーティングシステムのインストールの際に役立つ便利なツールです。ただし、前述のセキュリティーによる影響が受け入れられない場合や、ツールが必要ない場合は、Oracle System Assistant を無効にできます。Oracle System Assistant を無効にすると、USB ストレージデバイスがホストオペレーティングシステムにアクセスできなくなります。さらに、Oracle System Assistant のブートもできなくなります。

Oracle System Assistant はツール自体または BIOS から無効にできます。Oracle System Assistant を無効にしたら、BIOS 設定ユーティリティーからしか再度有効にすることはできません。承認されたユーザーのみが Oracle System Assistant を再度有効にできるように、BIOS 設定をパスワードで保護することをお勧めします。Oracle System Assistant を無効にして再度有効にする方法の詳細については、『Oracle X4 シリーズサーバー管理ガイド』を参照してください。

<http://www.oracle.com/goto/x86AdminDiag/docs>

Oracle ILOM のセキュリティー

このサーバー、その他の Oracle x86 ベースのサーバー、および一部の Oracle SPARC ベースのサーバーにインストール済みの Oracle Integrated Lights Out Manager (Oracle ILOM) 管理ファームウェアを使用すると、システムコンポーネントを積極的にセキュリティー保護、管理、およびモニターできます。

一般的なネットワークから切り離すには、サービスプロセッサ (SP) 専用の内部ネットワークを使用します。Oracle ILOM は、サーバーの制御機能やモニタリング機能をシステム管理者に提供します。これらの機能には、管理者に認められた管理レベルに応じて、サーバーの電源を切る機能、ユーザーアカウントを作成する機能、リモートストレージデバイスをマウントする機能などがあります。したがって、Oracle ILOM のもっとも信頼性が高くセキュアな環境を維持するために、サーバー上の専用のネットワーク管理ポートまたはサイドバンド管理ポートは常に、内部の信頼できるネットワークや専用のセキュアな管理/プライベートネットワークに接続している必要があります。

デフォルトの管理者アカウント (root) の使用は、初期の Oracle ILOM ログインに限定してください。このデフォルトの管理者アカウントは、初期のサーバーインストールを支援するためにのみ提供されています。したがって、最大限セキュアな環境にするため、このデフォルトの管理者パスワード (changeme) をシステムの初期設定の一部として変更する必要があります。デフォルトの管理者アカウントのパスワードを変更することに加え、一意のパスワードと割り当てられた承認レベルを持つ新しいユーザーアカウントを、新規 Oracle ILOM ユーザーごとに確立すべきです。

パスワードの設定、ユーザーの管理、およびセキュリティー関連機能 (Secure Shell (SSH)、Secure Socket Layer (SSL)、RADIUS 認証など) の適用の詳細については、Oracle ILOM のドキュメントを参照してください。Oracle ILOM に固有のセキュリティーガイドラインについては、使用している Oracle ILOM リリース用の Oracle ILOM ドキュメントライブラリに含まれる『Oracle Integrated Lights Out Manager (ILOM) セキュリティーガイド』を参照してください。Oracle ILOM のドキュメントは次の場所で検索できます。

<http://www.oracle.com/goto/ILOM/docs>

Oracle Hardware Management Pack のセキュリティー

Oracle Hardware Management Pack は使用しているサーバー、および多くの x86 ベースのサーバーと一部の SPARC ベースのサーバーで利用できます。Oracle Hardware Management Pack には、サーバーを管理するための 2 つのコンポーネント (SNMP モニタリングエージェントと、クロスオペレーティングシステムのコマンド行インタフェースツール (CLI ツール) のファミリ) が用意されています。

Hardware Management Agent SNMP Plugins を使用すると、SNMP を使用してデータセンター内の Oracle サーバーおよびサーバーモジュールをモニターでき、2 つの管理ポイント (ホストと Oracle ILOM) に接続する必要がないという利点が得られます。この機能により、複数のサーバーおよびサーバーモジュールのモニターに単一の IP アドレス (ホストの IP アドレス) を使用できます。SNMP Plugins は、Oracle サーバーのホストオペレーティングシステム上で実行します。

Oracle Server CLI ツールを使用すると、Oracle サーバーを構成できます。CLI ツールは、Oracle Solaris、Oracle Linux、Oracle VM、その他の Linux バリエーション、および Microsoft Windows オペレーティングシステムで動作します。

これらの機能の詳細については、Oracle Hardware Management Pack のドキュメントを参照してください。Oracle Hardware Management Pack に固有のセキュリティーガイドラインについては、Oracle Hardware Management Pack のドキュメントライブラリに含まれる『Oracle Hardware Management Pack (HMP) セキュリティーガイド』を参照してください。Oracle Hardware Management Pack のドキュメントは次の場所で検索できます。

<http://www.oracle.com/goto/OHMP/docs>

セキュアな環境の計画

サーバーおよび関連装置を設置して構成するときは、実行前および実行時に次の点に注意してください。

次のトピックで構成されています。

- 13 ページの「オペレーティングシステムのセキュリティーガイドライン」
- 14 ページの「ネットワークポートとネットワークスイッチ」
- 15 ページの「VLAN のセキュリティー」
- 15 ページの「Infiniband のセキュリティー」
- 15 ページの「ハードウェアの物理的なセキュリティー」
- 16 ページの「ソフトウェアのセキュリティー」

オペレーティングシステムのセキュリティーガイドライン

次の詳細については、Oracle オペレーティングシステム (OS) のドキュメントを参照してください。

- システムの構成時にセキュリティー機能を使用する方法
- システムにアプリケーションやユーザーを追加する場合のセキュアな運用方法
- ネットワークベースのアプリケーションを保護する方法

サポートされている Oracle オペレーティングシステムに関するセキュリティーガイドドキュメントは、OS のドキュメントライブラリに含まれています。Oracle OS に関するセキュリティーガイドドキュメントを検索するには、Oracle OS のドキュメントライブラリに移動します。

オペレーティングシステム	リンク
Oracle Solaris OS	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Oracle Linux OS	http://linux.oracle.com
Oracle VM OS	http://www.oracle.com/technetwork/documentation/vm-096300.html

Red Hat Enterprise Linux、SUSE Linux Enterprise Server、Windows、VMware ESXi など、ほかのベンダーのオペレーティングシステムについては、ベンダーのドキュメントを参照してください。

ネットワークポートとネットワークスイッチ

提供されるポートセキュリティー機能のレベルはスイッチによって異なります。次を実行する方法については、スイッチのドキュメントを参照してください。

- スイッチへのローカルアクセスとリモートアクセスには、認証、承認、アカウントリング機能を使用してください。
- デフォルトで複数のユーザーアカウントとパスワードを持っている可能性のあるネットワークスイッチで、すべてのパスワードを変更してください。
- スイッチの管理は、帯域外で(データトラフィックと切り離して)行なってください。帯域外管理を実現できない場合は、帯域内管理用に専用の仮想ローカルエリアネットワーク (VLAN) 番号を用意してください。
- 侵入検知システム (IDS) のアクセスには、ネットワークスイッチのポートのミラー化機能を使用してください。
- スイッチの構成ファイルはオフラインで管理し、承認された管理者しかアクセスできないようにしてください。構成ファイルには各設定の説明がコメントとして含まれているはずです。
- MAC アドレスに基づいてアクセスを制限するには、ポートセキュリティーを実装してください。自動ランキングはすべてのポートで無効にしてください。
- スイッチに次のようなポートセキュリティー機能がある場合は、これらの機能を使用してください。
 - **MAC Locking** では、接続された 1 つ以上のデバイスのメディアアクセス制御 (MAC) アドレスがスイッチの物理ポートに関連付けられます。スイッチのポートを特定の MAC アドレスに固定すると、スーパーユーザーによるバックドアの作成を防ぎ、不正アクセスポイントを利用したネットワークへのアクセスを防止できます。
 - **MAC Lockout** では、指定した MAC アドレスからのスイッチへの接続を無効にします。
 - **MAC Learning** では、ネットワークスイッチが現在の接続に基づいてセキュリティーを設定できるように、各スイッチポートの直接接続に関する情報を使用します。

VLAN のセキュリティー

仮想ローカルエリアネットワーク (VLAN) を設定する場合は、VLAN ではネットワーク上の帯域幅が共有され、追加のセキュリティー対策が必要であることを忘れないでください。

- 機密性のあるシステムのクラスタをその他のネットワークと切り離すように、VLAN を定義してください。これにより、それらのクライアントやサーバーに格納された情報にアクセスされる可能性が少なくなります。
- トランクポートには、一意のネイティブ VLAN 番号を割り当ててください。
- VLAN でのトランク経由のトランスポートは、どうしても必要な場合だけにしてください。
- VLAN Trunking Protocol (VTP) は、可能な場合は無効にしてください。そうでない場合は、VTP に対して管理ドメイン、パスワード、およびプルーニングを設定します。その後、VTP を透過モードに設定してください。

Infiniband のセキュリティー

Infiniband ホストをセキュアな状態にしてください。Infiniband ファブリックのセキュリティーは、もっともセキュリティーが低い Infiniband ホストに依存します。

- パーティションを分割しても Infiniband ファブリックを保護する効果はありません。パーティション分割は、ホストの仮想マシン間で Infiniband のトラフィックを分散させる機能です。
- 可能な場合は、静的 VLAN 構成を使用してください。
- スイッチの未使用のポートは無効にし、未使用の VLAN 番号を割り当ててください。

ハードウェアの物理的なセキュリティー

物理的なハードウェアのセキュリティー保護は非常にシンプルで、ハードウェアへのアクセスを制限すること、およびシリアル番号を記録することです。

- **アクセスを制限する**
 - サーバーと関連装置は、アクセスが制限された鍵の掛かった部屋に設置してください。
 - 鍵付きのドアがあるラックに装置を設置する場合は、ラック内のコンポーネントを保守する必要があるとき以外はドアの鍵は掛けたままにしてください。装置を保守したあとはドアに鍵を掛けてください。

- SSH 接続より強力なアクセスを提供できる USB コンソールへのアクセスを制限してください。システムコントローラ、配電盤 (PDU)、ネットワークスイッチなどのデバイスは、USB 接続が可能です。
- 特にホットプラグまたはホットスワップのデバイスは簡単に取り外すことができるため、これらのデバイスへのアクセスを制限してください。
- 予備の現場交換可能ユニット (FRU) または顧客交換可能ユニット (CRU) は鍵の掛かったキャビネットに保管してください。鍵の掛かったキャビネットへのアクセスは、承認された人だけに制限してください。
- **シリアル番号を記録する**
 - すべての主要なコンピュータハードウェア項目 (FRU など) にセキュリティーのマークを付けてください。専用の紫外線ペンまたはエンボスラベルを使用してください。
 - すべてのハードウェアのシリアル番号を記録しておいてください。
 - ハードウェアのアクティベーションキーとライセンスは、システム緊急時にシステムマネージャーが簡単に取り出せるセキュアな場所に保管しておいてください。これらの印刷ドキュメントは、所有権を示す唯一の証明になる可能性があります。

ソフトウェアのセキュリティー

ハードウェアのほとんどのセキュリティーは、ソフトウェアを通じて実装されます。

- 新規システムのインストール時に、デフォルトのパスワードをすべて変更してください。ほとんどの種類の装置では、changeme のようなデフォルトのパスワードが使用されており、これらは広く知られているため、装置への承認されていないアクセスを許可してしまいます。
- デフォルトで複数のユーザーアカウントとパスワードを持っている可能性のあるネットワークスイッチで、すべてのパスワードを変更してください。
- デフォルトの管理者アカウント (root) の使用を単一の管理者ユーザーに限定してください。新規ユーザーごとに必ず新しい Oracle ILOM アカウントを作成してください。各 Oracle ILOM ユーザーアカウントには常に一意のパスワードと適切なレベルの承認特権 (オペレータや管理者など) が割り当てられるようにしてください。
- サービスプロセッサには、一般的なネットワークから分離された専用のネットワークを使用してください。
- USB コンソールへのアクセスを保護してください。システムコントローラ、配電盤 (PDU)、ネットワークスイッチなどのデバイスでは USB 接続が可能であり、SSH 接続よりも強力なアクセスを提供できます。
- ソフトウェアに付属のドキュメントを参照して、ソフトウェアで使用可能なセキュリティー機能を有効にしてください。
- MAC アドレスに基づいてアクセスを制限するには、ポートセキュリティーを実装してください。自動ランキングはすべてのポートで無効にしてください。

セキュアな環境の保守

初期インストールおよび設定が終了したら、Oracle ハードウェアおよびソフトウェアのセキュリティ機能を使用して、ハードウェアの制御およびシステムアセットの追跡を続行してください。

- [17 ページの「ハードウェアの電源制御」](#)
- [17 ページの「アセットの追跡」](#)
- [18 ページの「ソフトウェアおよびファームウェアの更新」](#)
- [18 ページの「ネットワークのセキュリティ」](#)
- [19 ページの「データの保護とセキュリティ」](#)
- [19 ページの「ログの保守」](#)

ハードウェアの電源制御

一部の Oracle システムへの電源は、ソフトウェアを使用してオンとオフを切り替えることができます。リモートから配電盤 (PDU) を有効および無効にできるシステムキャビネットもあります。これらのコマンドの承認は、一般にシステムの構成時に設定され、通常はシステム管理者とサービス担当者に制限されます。

詳細は、システムまたはキャビネットのドキュメントを参照してください。

アセットの追跡

インベントリを追跡するには、シリアル番号を使用します。Oracle のシリアル番号は、オプションのカードとシステムのマザーボード上のファームウェアに組み込まれています。これらのシリアル番号は、ローカルエリアネットワーク接続で読み取ることができます。

また、ワイヤレスの無線周波数識別 (RFID) リーダーを使用すると、より簡単にアセットを追跡できます。RFID を使用した Oracle Sun システムアセットの追跡方法に関する Oracle のホワイトペーパーを参照してください。

<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf>

ソフトウェアおよびファームウェアの更新

サーバー装置上のソフトウェアとファームウェアは、最新のバージョンに保ってください。

- 更新を定期的にチェックしてください。
- 装置には、常に最新リリースバージョンのソフトウェアやファームウェアをインストールしてください。
- ソフトウェアに必要なセキュリティパッチをすべてインストールしてください。
- ネットワークスイッチなどのデバイスや Express Module に搭載されたファームウェアには、パッチおよびファームウェア更新が必要なものもあることを覚えておいてください。

ネットワークのセキュリティ

システムへのローカルアクセスとリモートアクセスをセキュリティ保護するために、次のガイドラインに従ってください。

- リモート構成を特定の IP アドレスに制限するときは、Telnet ではなく SSH を使用してください。Telnet では、ユーザー名とパスワードが平文で渡されるため、ログイン資格情報が LAN セグメントのすべてのユーザーに公開される可能性があります。SSH の強力なパスワードを設定してください。
- 簡易ネットワーク管理プロトコル (SNMP) バージョン 3 を使用して、転送をセキュリティ保護してください。古いバージョンの SNMP はセキュアではなく、認証データを暗号化されていないテキストで転送します。
- SNMP が必要な場合は、デフォルトの SNMP コミュニティ文字列を強力なコミュニティ文字列に変更してください。一部の製品では、デフォルトの SNMP コミュニティ文字列として PUBLIC が設定されています。攻撃者によってコミュニティが照会されると、完全なネットワークマップが作成され、管理情報ベース (MIB) の値が変更される可能性があります。
- システムコントローラでブラウザインタフェースを使用する場合は、使用後に必ずログアウトしてください。
- 伝送制御プロトコル (TCP) またはハイパーテキスト転送プロトコル (HTTP) などの不要なネットワークサービスを無効にしてください。必要なネットワークサービスについては、有効にしてセキュアに構成してください。
- LDAP を使用してシステムにアクセスする際は、LDAP のセキュリティ対策に従ってください。『Oracle ILOM セキュリティガイド』(<http://www.oracle.com/goto/ILOM/docs>) を参照してください。

- 無許可のアクセスを禁止することを明記したバナーを作成してください。
- 必要に応じて、アクセス制御リストを使用してください。
- 拡張セッションのタイムアウトを設定し、特権レベルを設定してください。
- スイッチへのローカルアクセスとリモートアクセスには、認証、承認、アカウントリング (AAA) 機能を使用してください。
- 可能な場合は、RADIUS および TACACS+ セキュリティープロトコルを使用してください。
 - RADIUS (Remote Authentication Dial In User Service) は、無許可のアクセスからネットワークをセキュリティー保護するクライアント/サーバープロトコルです
 - TACACS+ (Terminal Access Controller Access-Control System) は、リモートアクセスサーバーと認証サーバーとの通信を許可して、ユーザーがネットワークにアクセスできるかどうかを判定するプロトコルです。
- 侵入検知システム (IDS) のアクセスには、スイッチのポートのミラー化機能を使用してください。
- MAC アドレスに基づいてアクセスを制限するには、ポートセキュリティーを実装してください。すべてのポートで自動ランキングを無効にしてください。

データの保護とセキュリティー

データの保護レベルやセキュリティーを最大限に高めるために、次のガイドラインに従ってください。

- 外部ハードドライブや USB ストレージデバイスなどのデバイスを使って重要なデータのバックアップを取ってください。バックアップしたデータは、遠隔地のセキュアな場所に保管してください。
- データ暗号化ソフトウェアを使用して、ハードドライブ上の機密情報をセキュアな状態にしてください。
- 古いハードドライブを廃棄するときは、ドライブを物理的に破壊するか、ドライブ上のすべてのデータを完全に消去してください。ファイルが削除されたあとや、ドライブが再フォーマットされたあとでも、情報はドライブから回復できます。ファイルを削除しても、またはドライブを再フォーマットしても、ドライブ上のアドレステーブルしか除去されません。ドライブ上のすべてのデータを完全に消去するには、ディスクワイプソフトウェアを使用してください。

ログの保守

ログファイルは定期的に検査および保守してください。次の方法を使用して、ログファイルをセキュリティー保護してください。

- ログングを有効にし、専用のセキュアなログホストにシステムログを送信してください。
- ネットワークタイムプロトコル (NTP) およびタイムスタンプを使用して、正確な時間情報を含めるようにログングを構成してください。
- 可能性がある問題をログで確認し、セキュリティポリシーに従ってアーカイブしてください。
- ログファイルが適切なサイズを超えたら、定期的に回収してください。あとで参照したり、統計的に分析したりできるように、回収したファイルのコピーを保守してください。