

Sun Server X3-2 (旧 Sun Fire X4170 M3)

セキュリティーガイド

Copyright © 2013, 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了ことに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

1. Sun Server X3-2 セキュリティーガイド	5
システムの概要	5
セキュリティーの原則	6
サーバー構成および管理ツールの使用	7
Oracle System Assistant のセキュリティー	7
Oracle ILOM のセキュリティー	8
Oracle Hardware Management Pack のセキュリティー	9
セキュアな環境の計画	10
Oracle オペレーティングシステムのガイドライン	10
ネットワークポートとネットワークスイッチ	10
VLAN のセキュリティー	11
Infiniband のセキュリティー	11
ハードウェアの物理的なセキュリティー	12
ソフトウェアのセキュリティー	12
セキュアな環境の保守	13
ハードウェアの電源制御	13
アセットの追跡	13
ソフトウェアおよびファームウェアの更新	13
ネットワークアクセス	14
データ保護とセキュリティー	14
ログの保守	15

1

・・・ 第 1 章

Sun Server X3-2 セキュリティーガイド

このドキュメントでは、Oracle Sun Server X3-2、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ーガイドラインを示します。



注記

Sun Server X3-2 は以前は Sun Fire X4170 M3 サーバーという名前でした。この以前の名前がまだソフトウェアに表示されている場合があります。新しい製品名は、システム機能の変更を示すものではありません。

この章は、次のセクションで構成されています：

- ・ [5 ページの「システムの概要」](#)
- ・ [6 ページの「セキュリティーの原則」](#)
- ・ [7 ページの「サーバー構成および管理ツールの使用」](#)
- ・ [10 ページの「セキュアな環境の計画」](#)
- ・ [13 ページの「セキュアな環境の保守」](#)

システムの概要

Sun Server X3-2 は、エンタープライズクラスの 1 ラックユニット (1U) サーバーです。次のコンポーネントがサポートされています：

- ・ 最大 2 基の Intel プロセッサ。次の機能を備えたプロセッサがサポートされています：
 - ・ 2.4 GHz、4 コア、80W
 - ・ 2.5 GHz、6 コア、95W
 - ・ 2.2 GHz、8 コア、95W
 - ・ 2.9 GHz、8 コア、135W
- ・ プロセッサ当たり最大 8 基の DIMM で、デュアルプロセッサシステムでは最大 16 基の DDR3 DIMM および最大 512G バイトのメモリー。8B バイト、16G バイト、および 32G バイトのサイズの DIMM がサポートされています。



注記

シングルプロセッサシステムでは、最大 8 基の DIMM で最大 256G バイトがサポートされています。

- デュアルプロセッサシステムでは 4 基の PCIe Gen3 スロット、3 基の外部スロットと 1 基の内部。外部スロットである PCIe スロット 1 は、シングルプロセッサシステムでは機能しません。
- ストレージドライブ構成には、ハードディスクドライブ (HDD) とソリッドステートディスク (SSD) ドライブの両方を含めることができます。サポートされるストレージドライブ構成は次のとおりです：
 - ホットプラグ対応 3.5 インチ SAS HDD (4 台まで)
 - ホットプラグ対応 2.5 インチ SAS/SATA HDD/SSD (4 台まで) と DVD
 - ホットプラグ対応 2.5 インチ SAS/SATA HDD/SSD (8 台まで)
- 2 台のホットプラグ可能な冗長電源装置。
- ローカルおよびリモート管理をセキュリティ保護する AST2300 チップをベースとしたオンボードの Oracle Integrated Lights Out Manager (Oracle ILOM) サービスプロセッサ (SP)。
- インストール済みの USB フラッシュドライブに組み込まれている Oracle System Assistant サーバー設定ツール。

セキュリティの原則

基本的なセキュリティの原則として、アクセス、認証、承認、およびアカウントिंगの 4 つがあります。

• 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、これらのデバイスに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は、承認された人だけがアクセスするよう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。

- ・ アカウンティング

アカウンティングとは、ログインアクティビティの監視およびハードウェア目録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監視するには、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監視してください。
- ・ 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。カード、モジュール、およびマザーボードには、Oracle パーツ番号が電子的に記録されています。
- ・ 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、次のセキュリティガイドラインに従ってください。

- ・ [7 ページの「Oracle System Assistant のセキュリティ」](#)
- ・ [8 ページの「Oracle ILOM のセキュリティ」](#)
- ・ [9 ページの「Oracle Hardware Management Pack のセキュリティ」](#)

Oracle System Assistant のセキュリティ

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、以下で『*Sun Server X3-2 管理ガイド*』を参照してください:

<http://www.oracle.com/pls/topic/lookup?ctx=SunServerX3-2>

次の情報は、Oracle System Assistant に関するセキュリティ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、インストール済みの内蔵 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 KVMS (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** は無効にできます

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 を無効にすることができます。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 から無効にすることができます。Oracle System Assistant を無効にしたら、BIOS 設定ユーティリティ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については、『*Sun Server X3-2 管理ガイド*』を参照してください。

Oracle ILOM のセキュリティ

Sun Server X3-2、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、および監視できます。

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、システム管理者にサーバーの制御およびモニタリング機能を提供します。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**) は、Oracle ILOM に最初にログインするとき以外は使用しないようにしてください。このデフォルトの管理者アカウントは、サーバーの初期インストール用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に、システムの初期設定の一環として、デフォルトの管理者パスワード (**changeme**) を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だけでなく、新しい Oracle ILOM ユーザーごとに、一意のパスワードと権限レベルの割り当てを設定した新しいユーザーアカウントを確立してください。

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、Oracle ILOM 3.1 のドキュメントライブラリに含まれる『*Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*』を参照してください。Oracle ILOM 3.1 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 はお使いのサーバー、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 監視エージェントと、オペレーティングシステム間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) が備わっています。

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監視でき、2 つの管理ポイント (ホストと Oracle ILOM) にアクセスする必要がなくなる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監視に単一の 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 ツールを使用して、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) Security Guide』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する装置をインストールして構成するときは、次の情報を使用してください。

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

Oracle オペレーティングシステムのガイドライン

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

- **Oracle Solaris 10 1/13** - <http://www.oracle.com/goto/Solaris10/docs>
- **Oracle Solaris 11.1** - <http://www.oracle.com/goto/Solaris11/docs>
- **Oracle Linux** - <http://www.oracle.com/technetwork/documentation/ol-1861776.html>
- **Oracle VM** - <http://www.oracle.com/technetwork/documentation/vm-096300.html>

Red Hat Enterprise Linux、SUSE Linux Enterprise Server、Windows、VMware ESXi など、ほかのベンダー製オペレーティングシステムの詳細については、各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機能のレベルはスイッチによって異なります。次の実行方法については、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、アカウンティ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witch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witch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ます。
- ・ MAC アドレスに基づいてアクセスを制限するには、ポートの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witch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switchの物理ポートに関連付けられます。スswitch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することができます。
 - ・ **MAC Lockout** では、指定した MAC アドレスからのスswitchへの接続を無効にします。
 - ・ **MAC Learning** では、ネットワークスswitch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switch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。

- ・ 機密性のある一連のシステム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。無効にできない場合は、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、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、もともと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ないことに注意してください。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。
- ・ VLAN を構成する際、可能な場合は静的 VLAN を使用してください。
- ・ スwitch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

物理的なハードウェアのセキュリティ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 接続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、これらのデバイスに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は、承認された人だけがアクセスするように制限してください。

• シリアル番号を記録する

- 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。
- 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、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が、唯一の所有権証明になる場合があります。

ソフトウェアのセキュリティ

ハードウェアのほとんどのセキュリティは、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います。このパスワードは広く知られているため、承認されていないユーザーによって装置にアクセスされる可能性があります。
- 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**) は、1 人の管理者ユーザーしか使用できないように制限してください。常に新しいユーザーごとに新しい Oracle ILOM アカウントを作成してください。それぞれの Oracle ILOM ユーザーアカウントごとに、一意のパスワードと適切なレベルの権限 (オペレータ、管理者など) が常に割り当てられていることを確認してください。
- 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 接続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する可能性があります。

- ・ 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構成が終了したら、Oracle ハードウェアおよびソフトウェアのセキュリティー機能を使用して、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。

- ・ [13 ページの「ハードウェアの電源制御」](#)
- ・ [13 ページの「アセットの追跡」](#)
- ・ [13 ページの「ソフトウェアおよびファームウェアの更新」](#)
- ・ [14 ページの「ネットワークアクセス」](#)
- ・ [14 ページの「データ保護とセキュリティー」](#)
- ・ [15 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。詳細については、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

目録を追跡するには、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や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。Oracle のホワイトペーパー『*How to Track Your Oracle Sun System Assets by Using RFID*』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。
- ・ 常に、最新の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ーパッチを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にはファームウェアも搭載され、パッチやファームウェア更新が必要な場合もあることを忘れないでください。

ネットワークアクセス

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もあります。
- 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、アカウントिंग (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。

データ保護とセキュリティ

データの保護とセキュリティ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。

- 重要なデータは、外付けハードドライブや USB ストレージデバイスなどのデバイスを使用してバックアップしてください。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削除されません。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保護してください。

- ログ記録を有効にし、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記録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情報を保存してください。
- 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。
