Oracle® Server X6-2 セキュリティーガイド

Part No: E73675-01
2016 年 4 月

Part No: E73675-01

Copyright © 2016, 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際、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に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ー 7
アクセス 7
認証 8
承認 8
アカウンティングと監査 9

サーバーの構成および管理ツールのセキュアな使用 11
Oracle ILOM のセキュリティー 11
Oracle Hardware Management Pack のセキュリティー 12

セキュアな環境の計画 15
パスワードの保護 15
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 16
ネットワークスイッチとポート 16
VLAN のセキュリティー 17
InfiniBand のセキュリティー 18

セキュアな環境の保守 19
電源制御 19
アセットの追跡 19
ソフトウェアおよびファームウェアの更新 20
ネットワークのセキュリティー 20
データの保護とセキュリティー 22
ログの保守 22

基本的なセキュリティー

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ーガイドラインを示します。

ご使用の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ー要件については、組織の IT セキュリティー責任者に確認してください。

これは、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る基本的なセキュリティー原則です。このセクションでは、4 つの基本的なセキュリティー原則について説明します。

- 7 ページの「アクセス」
- 8 ページの「認証」
- 8 ページの「承認」
- 9 ページの「アカウンティングと監査」

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。
- 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、ハードウェアやソフトウェアへの承認されていないアクセスを許可してしまいます。
- 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ー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。

- USB ポートおよび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、システムへの直接アクセスを提供できる USB 接続を備えています。物理アクセスは、ネットワークベースの攻撃の影響を受けないため、よりセキュアにコンポーネントにアクセスできます。
- ネットワーク経由でシステムを再起動する機能を制限します。
- 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

認証とはユーザーを識別する方法で、通常ユーザー名とパスワードなどの機密情報を介して行います。認証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

承認は、ユーザーが実行または使用できるタスクや権限を管理者が制御することです。担当者は自分に割り当てられたタスクおよび権限のみを実行および使用できます。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。

アカウンティングと監査

アカウンティングおよび監査は、システム上で行われたユーザーアクティビティーのレコードを保持することです。Oracle サーバーには、管理者がログインアクティビティーのモニターやハードウェアインベントリの保守に使用できるソフトウェアおよびハードウェア機能があります。

- システムログを使用して、ユーザーログインをモニターします。システム管理者アカウントおよびサービスアカウントからアクセスできるコマンドは、不正に使用されるとシステムに危害を加えたりデータ損失につながる可能性があるため、これらのアカウントは必ずモニターしてください。アクセスおよびコマンドはシステムログで注意してモニターするようにしてください。
- 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 や CRU 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。
- ハードウェアアクティベーションキーおよびライセンスは、システム管理者が (特にシステムの緊急時に) 容易にアクセスできるセキュアな場所に保持してください。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。

サーバーの構成および管理ツールのセキュアな使用

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、次のセクションのセキュリティーガイドラインに従ってください。

- 11 ページの「Oracle ILOM のセキュリティー」
- 12 ページの「Oracle Hardware Management Pack のセキュリティー」

ご使用の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ー要件については、組織の IT セキュリティー責任者に確認してください。

Oracle ILOM のセキュリティー

Oracle x86 ベースのサーバーおよび Oracle SPARC ベースのサーバーに組み込まれている 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。システム管理者に付与される承認レベルによっては、機能にはサーバーの電源切断、ユーザーアカウントの作成、リモートストレージデバイスのマウントなどの機能が含まれる可能性があります。

- **セキュアな信頼できる内部ネットワークを使用します。**

  Oracle ILOM への物理管理接続を確立する際にローカルシリアルポート、専用のネットワーク管理ポート、サイドバンド管理ポート、標準のデータネットワークポートのどれを使用する場合でも、サーバー上のこの物理ポートが常に、内部の信頼できるネットワーク、専用のセキュア管理ネットワーク、またはプライベートネットワークに接続されていることが不可欠です。

  Oracle ILOM サービスプロセッサ (SP) をインターネットなどのパブリックネットワークには絶対に接続しないでください。Oracle ILOM SP 管理トラフィックを個別の管理ネットワーク上に維持し、アクセスをシステム管理者にのみ許可するようにしてください。

- **デフォルトの管理者アカウントの使用を制限してください。**

  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。デフォルト管理者アカウントへのアクセスを取得したユーザーは、Oracle ILOM のすべての機能に対して無制限にアクセスできるようになります。さらに、Oracle ILOM の各新規ユーザーについて、一意のパスワードを持つ新しいユーザーアカウントを作成し、承認レベル (ユーザーの役割) を割り当てます。

- **シリアルポートと端末サーバーを接続する際は、そのリスクを十分に考慮してください。**

  端末デバイスが提供するユーザー認証または承認のレベルが、ネットワークを悪意ある侵入からセキュリティー保護できるレベルであるとはかぎりません。ネットワーク侵入からシステムを保護するため、サーバーに十分なアクセス制御を設定するまでは、タイプに関係なく、端末サーバーなどのネットワークリダイレクションデバイスを介して Oracle ILOM とのシリアル接続 (シリアルポート) を確立することは避けてください。

  また、パスワードリセットや Preboot メニューなど、一部の Oracle ILOM 機能は物理シリアルポートを使用しないと使用できません。認証されていない端末サーバーを使用してシリアルポートをネットワークに接続すると、物理アクセスが不要になり、これらの機能に関連するセキュリティーが低下します。

- **Preboot メニューへのアクセスにはサーバーへの物理アクセスが必要です。**

  Oracle ILOM の Preboot メニューは強力なユーティリティーで、Oracle ILOM をデフォルト値にリセットしたり、Oracle ILOM が応答しなくなったときにファームウェアをフラッシュしたりする機能があります。Oracle ILOM がリセットされた場合、ユーザーはサーバー上のボタンを押すか (デフォルト) パスワードを入力する必要があります。この動作は Oracle ILOM 物理プレゼンスプロパティーで制御されます (`check_physical_presence= true`)。Preboot メニューへのアクセス時のセキュリティーを最大限に高めるため、Preboot メニューにアクセスするときにサーバーへの物理的なアクセスが要求されるよう、デフォルト設定 (`true`) は変更しないでください。

- **Oracle ILOM のドキュメントを参照してください。**

  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 のドキュメントライブラリに含まれる『*Oracle 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、および多くのその他の Oracle x86 ベースのサーバーと一部の Oracle 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) が備わっています。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 バリアント、および Microsoft Windows オペレーティングシステムで動作します。

- **Hardware Management Agent SNMP Plugins を使用します。**

  SNMP は、システムをモニターまたは管理するための標準のプロトコルです。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。SNMP Plugin モジュールはホストオペレーティングシステムのネイティブの SNMP エージェントを拡張して追加の Oracle MIB 機能を提供します。Oracle Hardware Management Pack 自体には SNMP エージェントは含まれていません。Linux の場合、モジュールは net-snmp エージェントに追加されます。Oracle Solaris の場合、モジュールは Oracle Solaris 管理エージェントに追加されます。Microsoft Windows の場合、このプラグインはネイティブの SNMP サービスを拡張します。Oracle Hardware Management Pack の SNMP に関連したセキュリティー設定は、プラグインによってではなく、ネイティブの SNMP エージェントまたはサービスの設定によって決まります。

  SNMPv1 と SNMPv2c は暗号化機能を備えておらず、認証の一形態としてコミュニティー文字列を使用します。よりセキュアな SNMPv3 は暗号化および個々のユーザー名とパスワードを使用してセキュアなチャネルを提供するため、このバージョンを使用することを推奨します。

- **Oracle Hardware Management Pack のドキュメントを参照してください。**

  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

システムが到着する前にセキュリティーガイドラインを作成しておくようにしてください。到着後は、組織の現行のセキュリティー要件に即するようセキュリティーガイドラインを定期的にレビューし調整するようにしてください。

次のセクションの情報は、サーバーおよび関連装置の設置および構成の実行前および実行中に使用します。

- 15 ページの「パスワードの保護」
- 16 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」
- 16 ページの「ネットワークスイッチとポート」
- 17 ページの「VLAN のセキュリティー」
- 18 ページの「InfiniBand のセキュリティー」

ご使用の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ー要件については、組織の IT セキュリティー責任者に確認してください。

パスワードの保護

不適切に選択したパスワードによって、会社のリソースへの不正アクセスが発生する可能性があるため、パスワードはセキュリティーの重要な側面です。パスワード管理のベストプラクティスを実装することで、ユーザーがパスワードの作成と保護のガイドラインセットに準拠するようになります。一般的なパスワードポリシーでは、次のことを定義します。

- パスワードの長さと強度
- パスワード期間
- 一般的なパスワードルール

強力で複雑なパスワードを作成するための次の標準的なルールを適用します。

- ユーザー名、従業員名、または家族の名前を含むパスワードを作成しない。
- 簡単に推測できるパスワードを選択しない。
- 12345 など、連続した数字文字列を含むパスワードを作成しない。
- インターネット検索で簡単に検出できる単語または文字列を含むパスワードを作成しない。

- 複数のシステム間での同じパスワードの再使用をユーザーに許可しない。
- 古いパスワードの再使用をユーザーに許可しない。

パスワードを定期的に変更する。これにより、悪意のある行為を防止し、最新のパスワードポリシーの遵守が徹底されます。

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、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ー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。

オペレーティングシステム	リンク
Oracle Solaris OS	http://www.oracle.com/technetwork/documentation/solaris-11-192991.html
Oracle Linux OS	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

Red Hat Enterprise Linux、SUSE Linux Enterprise Server、Microsoft 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。

ネットワークスイッチとポート

提供されるポートセキュリティー機能のレベルはネットワーク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、ポートのセキュリティーを実装してください。自動ト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**– 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**– 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**– ネットワークスイッチのポートごとに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、各ポートの直接接続に関する情報を収集します。

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。追加のセキュリティー対策については、次のガイドラインに従ってください。

- VLAN を使用する場合は、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。

- 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。

InfiniBand のセキュリティー

InfiniBand 使用時のセキュリティーを強化するには、次のガイドラインに従ってください。

- InfiniBand ホストをセキュアな状態に維持してください。InfiniBand ファブリックのセキュリティー保護のレベルは、最低レベルの InfiniBand ホストと同じレベルにしかなりません。
- 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では、InfiniBand トラフィックがホスト上の仮想マシン間で分離されるだけです。

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。

次のセクションの情報を使用してセキュアな環境を保守してください。

- 19 ページの「電源制御」
- 19 ページの「アセットの追跡」
- 20 ページの「ソフトウェアおよびファームウェアの更新」
- 20 ページの「ネットワークのセキュリティー」
- 22 ページの「データの保護とセキュリティー」
- 22 ページの「ログの保守」

ご使用の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ー要件については、組織の IT セキュリティー責任者に確認してください。

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

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 (LAN) 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。次にある *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

セキュリティー拡張機能は新しいソフトウェアリリースとパッチによって導入されます。有効な事前パッチ管理はシステムセキュリティーの重要な部分です。セキュリティーのベストプラクティスは、最新のソフトウェアリリースおよび必要なセキュリティーパッチを使用してシステムを更新することです。

- ソフトウェアまたはファームウェア更新およびセキュリティーパッチを定期的に確認してください。
- 装置にインストールするソフトウェアやファームウェアのバージョンは、常に最新のものを使用してください。
- 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。

ソフトウェア更新およびセキュリティーパッチは、次の My Oracle Support Web サイトで検索できます。

https://support.oracle.com

ネットワークのセキュリティー

セキュリティー原則に基づいてネットワークを構成したあとは、定期的な点検と保守が必要です。

システムへのローカルおよびリモートアクセスをセキュリティー保護するには、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ローカルエリアネットワーク (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ー保護してください。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。SNMPv3 では、暗号化を使用して、セキュアなチャネルや個々のユーザー名とパスワードを提供します。

- SNMPv1 または SNMPv2 が必要な場合は、デフォルトの SNMP コミュニティー文字列を強力なコミュニティー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 コミュニティー文字列として PUBLIC が設定されています。攻撃者によってコミュニティーが照会されると、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。
- 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。伝送制御プロトコル (TCP) や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。
- LDAP を使用してシステムにアクセスする際は、LDAP のセキュリティー対策を使用してください。
- ログイン時に表示され不正アクセスの禁止を知らせるバナーメッセージを作成します。重要なポリシーやルールをユーザーに通知できます。バナーは、特定のシステムに対する特殊なアクセス制限についてユーザーに警告したり、パスワードポリシーや適切な使用法についてユーザーに注意を促す場合に使用できます。
- 必要に応じて、アクセス制御リストを使用して制限を適用してください。
- 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、アカウンティング機能を使用してください。
- これらのネットワークサービスは、証明書や、チャネルを保護するその他の形式の強力な暗号化によってセキュリティー保護されているため、きわめてセキュアな環境で使用します。
  - Active Directory
  - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer)
- これらのネットワークサービスは、悪意のあるユーザーのいないセキュアなプライベートネットワーク上で使用します。
  - RADIUS (Remote Authentication Dial In User Service)
  - TACACS+ (Terminal Access Controller Access-Control System)
- 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、ポートのセキュリティーを実装してください。自動トランキングはすべてのポートで無効にしてください。

ネットワークセキュリティーの詳細は、Oracle ILOM ドキュメントライブラリにある『*Oracle 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

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重要なデータをバックアップしてください。バックアップされたデータは、遠隔地にある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。
- ハードドライブは多くの場合、機密情報を格納するために使用されます。この情報が不正に開示されないよう保護するため、ハードドライブを再利用、廃止、または廃棄する前にサニタイズする必要があります。
  - Oracle Solaris の `format(1M)` コマンドなどのディスク抹消ツールを使用して、すべてのデータをディスクドライブから完全に消去します。または、該当し使用可能な場合は、物理消磁ツールを使用できます。
  - ハードドライブに格納されている情報の機密性が高いと、粉砕や焼却などのハードドライブの物理的な廃棄が唯一の適切なサニタイズ方法である場合があります。
  - 組織は、データ保護ポリシーを参照して、ハードドライブをサニタイズするために最適な方法を判別することを強くお勧めします。

注意 - ディスク抹消ソフトウェアは、最新のハードドライブ (特に半導体ドライブ (SSD)) では、そのデータアクセスの管理方法のために一部のデータを削除できないことがあります。

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。

- ロギングを有効にし、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ギングを構成してください。

- 異常なネットワークアクティビティーやアクセスを検出できるよう、ネットワークデバイスログのスケジュールスキャンを定期的に実行してください。
- 可能性がある問題をログで確認し、セキュリティー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、回収されたファイルのコピーを保持してください。