Oracle® ILOM セキュリティーガイドファームウェア Release 3.0、3.1 および 3.2

Part No: E40359-04
2015 年 10 月

ORACLE

Part No: E40359-04

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

このドキュメントの使用法

- **概要** — Oracle ILOM セキュリティータスクのガイドラインに関する Web および CLI 情報を提供します。このガイドは、Oracle ILOM ドキュメントライブラリのその他のガイドと一緒に使用してください。
- **対象読者** — システムハードウェアの管理経験がある技術者、システム管理者、および Oracle 認定サービスプロバイダ。
- **必要な知識** — Oracle サーバーの構成および管理経験。

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/goto/ilom/docs で入手できます。

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 からお寄せください。

各 Oracle ILOM ファームウェアリリースのセキュリティー機能

Oracle ILOM のセキュリティー機能を利用できるファームウェアリリースは、次の表で確認できます。

ファームウェアバージョン利用可能状況	セキュリティー機能	詳細の参照先
すべて	認証および承認	■ 24 ページの「Oracle ILOM ユーザーアクセスのセキュリティー保護」
すべて	専用のセキュア管理接続	■ 15 ページの「物理管理接続のセキュリティー保護」 ■ 53 ページの「セキュアな管理接続の維持」
すべて	暗号化された事前構成ネットワークポート	■ 19 ページの「事前構成済みのサービスとネットワークポート」
すべて	IPMI 2.0 セキュア管理	■ 49 ページの「最大限のセキュリティーを得るための IPMI 管理アクセスの構成」
すべて	Secure Shell 鍵暗号化構成	■ 45 ページの「サーバー側鍵を使用して SSH 接続を暗号化する」 ■ 46 ページの「自動 CLI 認証用としてユーザーアカウントに SSH 鍵を追加する」
すべて	SNMP 3.0 セキュア管理	■ 47 ページの「最大限のセキュリティーを得るための SNMP 管理アクセスの構成」
すべて	SSL プロトコルと証明書	■ 39 ページの「カスタム SSL 証明書と非公開鍵を Oracle ILOM にアップロードする」 ■ 38 ページの「OpenSSL を使用して SSL 証明書および非公開鍵を入手する」 ■ 40 ページの「もっとも強力な SSL および TLS 暗号化プロパティーを有効にする」
すべて	リモートコンソール暗号化とセキュアプロトコル	■ 56 ページの「リモート KVMS のセキュアな使用法」
3.0.4 以降	KVMS ホストロック構成	■ 33 ページの「KVMS セッションの終了時にホストアクセスをロックする」
3.0.4 以降	セッションタイムアウトの構成	■ 42 ページの「非アクティブの Web セッションに対するタイムアウト間隔を設定する」 ■ 44 ページの「非アクティブの CLI セッションのタイムアウト間隔を設定する」
3.0.12 以降	ローカルホスト相互接続認証済セッション	■ 54 ページの「推奨される認証済みホスト相互接続アクセス」

ファームウェアバージョン利用可能状況	セキュリティー機能	詳細の参照先
3.0.8 以降	ログインバナーの構成	35 ページの「ログインバナーを使用してシステムアクセスをセキュリティー保護する (3.0.8 以降)」
3.0.8 - 3.1.2	WS-Management セキュアアクセス	■ 52 ページの「最大限のセキュリティーを得るための WS-Management アクセスの構成」
3.1.0 以降	監査ログの分離	■ 62 ページの「監査イベントのモニタリングによる不正アクセスの検出」
3.1.0 以降	物理的セキュリティープレゼンスチェック	■ 60 ページの「root アカウントのデフォルトパスワードをリセットする際の物理的セキュリティープレゼンス」
3.2.4 以降	IPMI 1.5 構成可能プロパティー	■ 49 ページの「最大限のセキュリティーを得るための IPMI 管理アクセスの構成」
3.2.4 以降	TLS プロトコルバージョン 1.1 および 1.2	■ 40 ページの「もっとも強力な SSL および TLS 暗号化プロパティーを有効にする」
3.2.4 以降	KVMS セッション数	■ 34 ページの「リモートシステムコンソールプラスで表示できる KVMS セッションを制限する (3.2.4 以降)」
3.2.4 以降	FIPS 準拠暗号化のサポート	■ 16 ページの「配備時に FIPS モードを構成するかどうかの選択」 ■ 18 ページの「FIPS モードが有効の時にサポートされない機能」 ■ 59 ページの「ユーザーアクセスをセキュリティー保護するための配備後の考慮事項」
3.2.5 以降	SSH サーバーの状態および弱い暗号	■ 43 ページの「SSH サーバーの状態および弱い暗号の管理 (3.2.5 以降) 」
3.2.5 以降	ローカルユーザーアカウントのパスワードポリシー	■ 29 ページの「すべてのローカルユーザーのパスワードポリシー制限を設定する (3.2.5 以降)」

その他のセキュリティー情報

Oracle ILOM のセキュリティー保護の詳細は、このガイドの次のセクションを参照してください。

- 「Oracle ILOM セキュリティーベストプラクティスのチェックリスト」
- 「Oracle ILOM のための配備時のセキュリティーベストプラクティス 」
- 「Oracle ILOM のための配備後のセキュリティーベストプラクティス」

Oracle ILOM セキュリティーベストプラクティスのチェックリスト

Oracle Integrated Lights Out Manager (ILOM) は全 Oracle サーバーと大半のレガシー Sun サーバーにプリインストールされているサービスプロセッサ (SP) です。システム管理者は Oracle ILOM のユーザーインタフェースを使用して、リモートサーバー管理タスクやリアルタイムのサーバー健全性モニタリング操作を実行できます。

使用環境が Oracle ILOM のセキュリティーベストプラクティスに準拠するよう、システム管理者は次のチェックリストに記載されている推奨のセキュリティータスクについて検討する必要があります。

- 11 ページの「サーバー配備のセキュリティーチェックリスト」
- 12 ページの「サーバー配備後のセキュリティーチェックリスト」

関連情報

- 「Oracle ILOM のための配備時のセキュリティーベストプラクティス 」。
- 「Oracle ILOM のための配備後のセキュリティーベストプラクティス」
- 9 ページの各 Oracle ILOM ファームウェアリリースのセキュリティー機能

サーバー配備のセキュリティーチェックリスト

新しいサーバーの配備を計画するときにどの Oracle ILOM セキュリティープラクティスが最適である可能性があるかを判定するために、システム管理者は、次の表1「チェックリスト - サーバー配備時の Oracle ILOM セキュリティーの構成 」で推奨されているセキュリティータスクの一覧を参照するようにしてください。

表 1 チェックリスト - サーバー配備時の Oracle ILOM セキュリティーの構成

✓	セキュリティータスク	対象ファームウェアバージョン	詳細の参照先
	Oracle ILOM へのセキュアな専用管理接続を確立します。	すべてのファームウェアバージョン	■ 15 ページの「物理管理接続のセキュリティー保護」

✓	セキュリティータスク	対象ファームウェアバージョン	詳細の参照先
	FIPS 140-2 セキュリティーへの準拠が配備時または配備後に必要であるかどうか、または一切必要ないのかを判断します。	ファームウェアバージョン 3.2.4 以降	■ 16 ページの「配備時に FIPS モードを構成するかどうかの選択」 ■ 18 ページの「FIPS モードが有効の時にサポートされない機能」
	すべてのローカルユーザーアカウントのパスワードポリシーを設定する	ファームウェアバージョン 3.2.5 以降	■ 29 ページの「すべてのローカルユーザーのパスワードポリシー制限を設定する (3.2.5 以降)」
	事前構成された管理者 root アカウントに提供されるデフォルトのパスワードを変更する。	すべてのファームウェアバージョン	■ 24 ページの「共有ユーザーアカウントの作成の回避」 ■ 30 ページの「初回ログイン時に root アカウントのデフォルトのパスワードを変更する」
	事前構成の Oracle ILOM サービスとそのために開かれるネットワークポートが使用環境に適しているかどうかを判断します。	すべてのファームウェアバージョン	■ 19 ページの「サービスおよび開いているネットワークポートのセキュリティー保護」
	Oracle ILOM へのユーザーアクセスを構成する。	すべてのファームウェアバージョン	■ 24 ページの「Oracle ILOM ユーザーアクセスのセキュリティー保護」 ■ 32 ページの「役割ベースの権限を持つローカルユーザーアカウントを作成する」
	リモート KVMS セッションの終了時にホストオペレーティングシステムへのアクセスをロックするべきかどうかを決定する。	ファームウェアバージョン 3.0.4 以降	■ 33 ページの「KVMS セッションの終了時にホストアクセスをロックする」
	SP から起動したリモート KVMS セッションをほかの SP ユーザーが表示することに対し制限を設けるかどうかを決定します。	ファームウェアバージョン 3.2.4 以降	■ 34 ページの「リモートシステムコンソールプラスで表示できる KVMS セッションを制限する (3.2.4 以降)」
	ユーザーログイン時またはユーザーログイン直後にセキュリティーバナーメッセージを表示するかどうかを決定します。	ファームウェアバージョン 3.0.8 以降	■ 35 ページの「ログインバナーを使用してシステムアクセスをセキュリティー保護する (3.0.8 以降)」
	すべての Oracle ILOM ユーザーインタフェースに最大限のセキュリティープロパティーが設定されていることを確認します。	すべてのファームウェアバージョン	■ 36 ページの「最大限のセキュリティーを得るための Oracle ILOM インタフェースの構成」

サーバー配備後のセキュリティーチェックリスト

環境内の既存のサーバーを維持するにはどの Oracle ILOM セキュリティープラクティスが最適であるかを判定するために、システム管理者は、次の表2「チェックリスト - サーバー配備後の Oracle ILOM セキュリティーの維持 」で推奨されているセキュリティータスクの一覧を参照するようにしてください。

表 2 チェックリスト - サーバー配備後の Oracle ILOM セキュリティーの維持

✓	セキュリティータスク	対象ファームウェアバージョン	詳細の参照先
	Oracle ILOM へのセキュアな管理接続を維持します	すべてのファームウェアバージョン	■ 53 ページの「認証されていないホスト KCS デバイスアクセスの回避」 ■ 54 ページの「推奨される認証済みホスト相互接続アクセス」

✓	セキュリティータスク	対象ファームウェアバージョン	詳細の参照先
			■ 55 ページの「チャネルのセキュリティー保護のための IPMI 2.0 暗号化の使用」
	リモート KVMS セッションとシリアルのテキストベースのセッションが Oracle ILOM からセキュアに起動されることを確認します。	すべてのファームウェアバージョン	■ 57 ページの「KVMS リモート通信と暗号化」 ■ 57 ページの「リモート KVMS 共有アクセスから保護する」 ■ 58 ページの「ホストシリアルコンソールの共有アクセスに対する保護」
	Oracle ILOM へのユーザーアクセスを維持および追跡します。	すべてのファームウェアバージョン	■ 59 ページの「ユーザーアクセスをセキュリティー保護するための配備後の考慮事項」
	事前構成の Admin `root` アカウントのパスワードを失念した際のパスワードリセットに必要なセキュリティーアクション。	ファームウェアバージョン 3.1 以降	■ 60 ページの「`root` アカウントのデフォルトパスワードをリセットする際の物理的セキュリティープレゼンス」
	サーバー配備後 Oracle ILOM の FIPS 140-2 準拠モードを変更する場合に必要なセキュリティーアクション。	ファームウェアバージョン 3.2.4 以降	■ 63 ページの「配備後に FIPS モードを変更する」 ■ 18 ページの「FIPS モードが有効の時にサポートされない機能」
	サーバー上のソフトウェアおよびファームウェアが最新であることを確認します。	すべてのファームウェアリリース	■ 65 ページの「最新ソフトウェアおよびファームウェアのアップデート」

Oracle ILOM のための配備時のセキュリティーベストプラクティス

サーバー配備時に最適な Oracle ILOM セキュリティープラクティスを判断するには、次のトピックを使用します。

- 15 ページの「物理管理接続のセキュリティー保護」
- 16 ページの「配備時に FIPS モードを構成するかどうかの選択」
- 19 ページの「サービスおよび開いているネットワークポートのセキュリティー保護」
- 24 ページの「Oracle ILOM ユーザーアクセスのセキュリティー保護」
- 36 ページの「最大限のセキュリティーを得るための Oracle ILOM インタフェースの構成」

関連情報

- 「Oracle ILOM セキュリティーベストプラクティスのチェックリスト」。
- 「Oracle ILOM のための配備後のセキュリティーベストプラクティス」
- 9 ページの各 Oracle ILOM ファームウェアリリースのセキュリティー機能

物理管理接続のセキュリティー保護

Oracle ILOM は、Oracle サーバーの保守およびモニターのために専用の管理チャネルを使用する帯域外 (OOB) 管理ツールです。帯域内管理ツールを使用するサーバーとは異なり、Oracle サーバーには組み込みのリモート管理機能が付属しており、システム管理者はサービスプロセッサ上で別個の専用ネットワークコネクタを使用して Oracle ILOM へのセキュアなアクセスを取得できます。Oracle ILOM の管理機能は、Oracle サーバーをモニターおよび管理するための特定の機能をシステム管理者に提供しますが、Oracle ILOM は、汎用の計算エンジンとして設計されておらず、またセキュリティー保護されていない信頼できないネットワーク接続からアクセスするようには設計されていません。

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を使用するか、専用のネットワーク管理ポートを使用するか、標準のデータネットワークポートを使用するかに関係なく、サーバーまたはシャーシモニタリングモジュール (CMM) 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 への物理管理接続を確立する際の詳細なガイドラインについては、次の表を参照してください。

Oracle ILOM への物理ポート管理接続	サポートされている Oracle ハードウェア	管理接続のセキュリティーガイドライン
専用接続	■ サーバー (ポート: NET MGT) ■ CMM (ポート: NET MGT)	サービスプロセッサ (SP) を一般的なデータネットワークトラフィックと分けるために、専用の内部ネットワークを使用します。 Oracle ILOM への専用ネットワーク管理接続の確立については、次を参照してください ■ 専用のネットワーク管理接続、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
ローカル接続	■ サーバー (ポート: SER MGT) ■ CMM (ポート: SER MGT)	ローカルシリアル管理接続を使用して、物理サーバーまたは CMM から直接 Oracle ILOM にアクセスします。 Oracle ILOM へのローカルシリアル管理接続の確立については、次を参照してください。 ■ Oracle ILOM へのローカルシリアルネットワーク管理接続、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
サイドバンド接続	サーバー (ポート: NET0、NET1、NET2、NET3)	2 つの別個のネットワーク接続の必要をなくすことで、ケーブル管理とネットワーク構成を簡素化する必要がある場合は、共有 Ethernet データネットワークを使用してサービスプロセッサ SP にアクセスします。 Oracle ILOM へのサイドバンド管理接続の確立については、次を参照してください ■ サイドバンド管理接続、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』 **注記 -** サイドバンド管理は、ほとんどの Oracle サーバーでサポートされています。

注記 - セキュリティー攻撃から防御するには、**ユーザー**は、インターネットなどの**パブリックネットワークに Oracle ILOM SP を決して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。

配備時に FIPS モードを構成するかどうかの選択

Oracle ILOM ファームウェアリリース 3.2.4 の時点では、Oracle ILOM の CLI および Web インタフェースには、FIPS (Federal Information Processing Standards) レベル 1 準拠のための構成可能なモードが用意されています。このモードが有効になっていると、Oracle は、システムの機密データまたは重要なデータを保護するために、FIPS 140-2 セキュリティー標準に準拠した暗号化アルゴリズムを使用します。

ファームウェア 3.2.4 以降のサーバーを配備しているシステム管理者は、ほかの Oracle ILOM プロパティーを構成する前に FIPS モードを構成するかどうかを決定するようにしてください。デフォルトでは、Oracle ILOM の FIPS 準拠モードは無効の状態で出荷されます。

FIPS 準拠モードを変更すると、すべての構成データが出荷時のデフォルト値にリセットされます。

配備時に (Oracle ILOM プロパティーを構成する前に) FIPS モード準拠を有効にするには、17 ページの「配備時に FIPS モードを有効にする」を参照してください。Oracle ILOM でユーザー定義の構成プロパティーがすでに設定されているときに FIPS プロパティーを変更する必要がある場合は、63 ページの「FIPS モードを変更するための配備後のアクション」を参照してください。

▼ 配備時に FIPS モードを有効にする

注記 - Oracle ILOM の FIPS 準拠モードは、「State」および「Status」プロパティーによって表されます。「State」プロパティーは Oracle ILOM で構成されているモードを表し、「Status」プロパティーは Oracle ILOM の動作モードを表します。FIPS の「State」プロパティーが変更された場合、その変更は、次回の Oracle ILOM のリブートまで動作モード (FIPS の「Status」プロパティー) に影響を与えません。

始める前に

- FIPS の「State」および「Status」プロパティーは、デフォルトでは無効の状態で出荷されます。
- FIPS が有効になっている (構成され、動作可能になっている) と、Oracle ILOM の一部の機能がサポートされません。FIPS が有効になっているときにサポートされない機能の一覧については、表3「FIPS モードが有効の時にサポートされない Oracle ILOM 機能」を参照してください。
- FIPS の「State」プロパティーを変更するには、Admin (a) の役割が必要です。
- FIPS 準拠のための構成可能なプロパティーは、ファームウェア 3.2.4 以降の Oracle LOM で使用できます。ファームウェアリリース 3.2.4 より前では、Oracle ILOM は FIPS 準拠のための構成可能なプロパティーを提供していません。
- Oracle ILOM で FIPS モードの「State」および「Status」プロパティーを変更すると、ユーザー定義のすべての構成設定が出荷時のデフォルトにリセットされます。

1. **Oracle ILOM Web インタフェースで「ILOM Administration」->「Management Access」->「FIPS」をクリックします。**
2. **「FIPS」ページで、次を実行します。**
   a. **「FIPS State」チェックボックスにチェックマークを付け、構成済み FIPS プロパティーを有効にします。**
   b. **「Save」をクリックして変更を適用します。**

その他の構成の詳細は、FIPS Web ページで「`More details....`」リンクをクリックします。

3. **Oracle ILOM で FIPS 動作モードのステータスを変更するには、次の手順を実行して Oracle ILOM をリブートします。**

   a. **Web インタフェースで、「ILOM Administration」->「Maintenance」->「SP Reset」をクリックします。**

   b. **「SP Reset」ページで、「SP Reset」ボタンをクリックします。**

   Oracle ILOM をリブートすると、次のようになります。

   - 最後に構成した FIPS State (有効) がシステムに適用されます。
   - 以前から Oracle ILOM に構成されていたユーザー定義構成設定が工場出荷時のデフォルト値にリセットされます。
   - FIPS Status プロパティーが更新され、現在 Oracle ILOM で有効になっている動作状態が反映されます。

     FIPS Status メッセージの完全なリストと説明については、「FIPS」ページで「`More details`」リンクをクリックしてください。
   - FIPS シールドアイコンが Web インタフェースの上部に表示されます。
   - サポートされていない FIPS 機能はすべて、CLI および Web インタフェースで無効になるか表示されなくなります。

     サポートされない FIPS 機能の完全なリストと説明については、「FIPS」ページで「`More details`」リンクをクリックしてください。

関連情報

- 18 ページの「FIPS モードが有効の時にサポートされない機能」
- 63 ページの「FIPS モードを変更するための配備後のアクション」
- FIPS モードプロパティーの構成、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』。

FIPS モードが有効の時にサポートされない機能

Oracle ILOM で FIPS 準拠を有効にすると、FIPS 140-2 に準拠しない次の Oracle ILOM 機能がサポートされなくなります。

表 3 FIPS モードが有効の時にサポートされない Oracle ILOM 機能

サポートされない FIPS モード機能	説明
IPMI 1.5	FIPS モードが有効でシステムで実行されている場合、IPMI 1.5 構成プロパティーが Oracle ILOM の CLI および Web インタフェースから削除されます。IPMI 2.0 サービスは Oracle ILOM で自動的に有効になります。IPMI 2.0 は FIPS 準拠モードと非準拠モードの両方をサポートしています。
Oracle ILOM システムリモートコンソールのファームウェア互換性	Oracle ILOM を FIPS モードにすると、古いファームウェアバージョンの Oracle ILOM リモートシステムコンソールが新しい Oracle ILOM リモートシステムコンソールファームウェアバージョンと互換しなくなります。

サポートされない FIPS モード機能	説明
	たとえば、Oracle ILOM リモートシステムコンソールクライアントファームウェアバージョン 3.2.4 は Oracle ILOM リモートシステムコンソールファームウェアバージョン 3.2.3 以前との下位互換性があります。ただし Oracle ILOM リモートシステムコンソールクライアントファームウェアバージョン 3.2.2 以前には、Oracle ILOM リモートシステムコンソールファームウェアバージョン 3.2.4 以降との上位互換性がありません。 **注記 -** このファームウェア互換性制限は Oracle ILOM リモートシステムコンソールプラスには適用されません。Oracle ILOM リモートシステムコンソールプラスは、SPARC T5 以降のシステムや Oracle サーバー x4-4、x4-8 およびそれ以降のシステムなど、比較的新しいサービスプロセッサシステムで提供されます。Oracle ILOM リモートシステムコンソールは SPARC T3 および T4、Sun サーバー x4-2/2L/2B 以前のシステムなど、比較的古いサービスプロセッサシステムで提供されます。
Lightweight Directory Access Protocol (LDAP)	FIPS モードが有効でシステムで実行されている場合、Oracle ILOM の LDAP 構成プロパティーが Oracle ILOM の CLI および Web インタフェースから自動的に削除されます。 **注記 -** 次のリモート認証サービスは FIPS 準拠モードと非準拠モードの両方でサポートされます: Active Directory および LDAP/SSL。
Remote Authentication Dial-In User Service (RADIUS)	FIPS モードが有効でシステムで実行されている場合、Oracle ILOM の RADIUS 構成プロパティーが Oracle ILOM の CLI および Web インタフェースから自動的に削除されます。 **注記 -** 次のリモート認証サービスは FIPS 準拠モードと非準拠モードの両方でサポートされます: Active Directory および LDAP/SSL。
Simple Network Management Protocol (SNMP) DES および MD5	FIPS モードが有効でシステムで実行されている場合、DES プライバシプロトコルおよび MD5 認証プロトコルの SNMP 構成プロパティーが Oracle ILOM の CLI または Web インタフェースでサポートされなくなります。

サービスおよび開いているネットワークポートのセキュリティー保護

サービスとそのネットワークポートを Oracle ILOM で正しく構成するには、次のトピックを参照してください。

- 19 ページの「事前構成済みのサービスとネットワークポート」
- 20 ページの「不要なサービスと開いているポートの管理」
- 21 ページの「サービスとネットワークポートの構成」

事前構成済みのサービスとネットワークポート

Oracle ILOM では、事前構成によって、大半のサービスがデフォルトで有効になっています。これにより、Oracle ILOM の配備は簡単でわかりやすくなっています。ただし、サーバー上の開いているサービスネットワークポートはすべて、悪意のあるユーザーからの攻撃ポイントとなる可能性があります。このため、Oracle ILOM の初期設定とそれぞれの目的を理解して、配備したシステムに本当に必要なサービスを選択することが重要になります。最善のセキュリティーを実現するために、必要な Oracle ILOM サービスだけを有効にしてください。

次の表に、Oracle ILOM のデフォルトで有効になっているサービスの一覧を示します。

表 4 デフォルトで有効になるサービスとポート

サービス	ポート
HTTPS への HTTP リダイレクション	80
HTTPS	443
IPMI	623
Oracle ILOM リモートコンソールのリモート KVMS	5120、5121、5122、5123、5555、5556、7578、7579
Oracle ILOM リモートコンソールプラスのリモート KVMS	5120、5555
サービスタグ	6481
SNMP	161
シングルサインオン	11626
SSH	22

次の表に、Oracle ILOM のデフォルトで無効になっているサービスの一覧を示します。

表 5 デフォルトで無効になるサービスとポート

サービス	ポート
HTTP	80

不要なサービスと開いているポートの管理

すべての Oracle ILOM サービスはオプションで無効にでき、それにより、それらのサービス用に開かれている各ネットワークポートが閉じられます。大半のサービスはデフォルトで有効になっていますが、一部の機能を無効にしたり、デフォルトの設定を変更したりして、Oracle ILOM 環境をよりセキュアにすることができます。Oracle ILOM サービスはどれも無効にできますが、無効にすると機能が失われます。一般には、配備された環境で絶対に必要なサービスだけを有効にします。機能が失われることと、有効なネットワークサービスの数を減らすことによるセキュリティー上の利点とを、比較検討する必要があります。

次の表は、各サービスを有効化または無効化した場合の影響について説明しています。

表 6 サービスを無効にした場合

サービス	説明	有効または無効にした結果
HTTP	Oracle ILOM Web インタフェースにアクセスするための非暗号化プロトコル	このサービスを有効にすると暗号化 HTTP (HTTPS) よりも高いパフォーマンスが得られます。ただし、このプロトコルを使用すると、機密情報が暗号化されずにインターネット経由で送信されることになります。
HTTPS	Oracle ILOM Web インタフェースにアクセスするための暗号化プロトコル	このサービスを有効にすると、Web ブラウザと Oracle ILOM 間でセキュアな通信が可能となります。ただし、このサービスでは、Oracle ILOM 上でネットワークポートを開いておく必要があるため、サービス拒否などの攻撃に対する脆弱性が増します。

サービス	説明	有効または無効にした結果
サービスタグ	サーバーを識別し、サービス要求を容易にするための Oracle の発見プロトコル	このサービスを無効にすると、Oracle Enterprise Manager Ops Center が Oracle ILOM を発見できなくなり、その他の Oracle の自動サービスソリューションへの統合もできなくなります。 サービスタグの状態は Oracle ILOM CLI からでしか構成できません。たとえば、サービスタグの状態プロパティーを変更するには次のように入力します。 `set /SP/services/servicetag state=`*enabled*|*disabled*
IPMI	標準の管理プロトコル	このサービスを無効にすると、Oracle Enterprise Manager Ops Center、およびサードパーティー製ソフトウェアへの接続を提供する一部の Oracle 管理コネクタによってシステムを管理できなくなることがあります。
SNMP	Oracle ILOM の健全性のモニタリングおよびトラップ通知受信のモニタリングを行うための標準の管理プロトコル	このサービスを無効にすると、Oracle Enterprise Manager Ops Center、およびサードパーティー製ソフトウェアへの接続を提供する一部の Oracle 管理コネクタによってシステムを管理できなくなることがあります。
KVMS	リモートのキーボード、ビデオ、マウス、およびストレージを提供するためのプロトコルセット	このサービスを無効にすると、ホストコンソールとリモートストレージ機能が使用不可になり、Oracle ILOM リモートシステムコンソール (または Oracle ILOM リモートシステムコンソールプラス) と CLI ストレージリダイレクションアプリケーションを使用できなくなります。
SSH	リモートシェルにアクセスするためのセキュアなプロトコル。	このサービスを無効にすると、ネットワーク経由でのコマンド行アクセスが禁止され、Oracle Enterprise Manager Ops Center が Oracle ILOM を発見できなくなることがあります。
SSO	ユーザーによるユーザー名とパスワードの入力回数を減らすシングルサインオン機能	このサービスを無効にすると、パスワードを再入力せずに KVMS を起動することができなくなり、パスワードを再入力せずにシャーシモニタリングモジュール (CMM) からブレード SP にドリルダウンすることが許可されます。

個々のネットワークサービスの有効化および無効化の詳細は、次のトピック21 ページの「サービスとネットワークポートの構成」を参照してください。

サービスとネットワークポートの構成

管理サービスおよびそのサービスで使用する各ネットワークポートを Oracle ILOM で構成する方法の詳細は、次の手順を参照してください。

- 22 ページの「プロトコル管理サービスの状態とポートを変更する」
- 23 ページの「KVMS サービスの状態とポートを変更する」
- 23 ページの「シングルサインオンサービスの状態とポートを変更する」

各サービスとそれに対応するネットワークポートは、Oracle ILOM のコマンド行インタフェース (CLI) または Web インタフェースを使用して無効または有効にできます。このセクションの手順は、すべての Oracle ILOM ファームウェアリリースに対応する Web ベースのナビゲーション手順を示しています。CLI の手順について、または構成プロパティーの詳細は、各手順のあとの「関連情報」セクションに記載されている適切なドキュメントを参照してください。

▼ プロトコル管理サービスの状態とポートを変更する

始める前に

- 次の表を参照して、どのプロトコルサービスとネットワークポートが Oracle ILOM でデフォルトで有効または無効になるかを確認してください。
  - 表4「デフォルトで有効になるサービスとポート」 デフォルトで有効になるサービスとポート
  - 表5「デフォルトで無効になるサービスとポート」 デフォルトで無効になるサービスとポート
- Oracle ILOM でプロトコルサービスの「State」プロパティーを変更するには、Admin (a) の役割が必要です。

ネットワークサービスの「State」プロパティーを変更するには、次の手順に従います。

1. **Oracle ILOM Web インタフェースで、「Management Access」サービスに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「Configuration」->「System Management Access」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」をクリックします。**

2. **該当する「Management Access」->次に示すサービスタブをクリックします。**

Management Access ->	説明
Web Server	「Web Server」ページを使用してサービスの状態と HTTP および HTTPS プロトコル管理アクセスのポート割り当てを管理します。
IPMI	「IPMI」ページを使用して、サービスの状態と IPMI プロトコル管理アクセスのポートプロパティーを管理します。
SNMP	「SNMP」ページを使用して、サービスの状態と SNMP 管理アクセスのポートプロパティーを管理します。
SSH	「SSH」ページを使用して、セキュアシェル管理アクセスのサービス状態プロパティーを管理します。

3. **「Management Access」->サービスページで State プロパティーを変更し、「Save」をクリックして変更を適用します。**
   プロトコルサービスの State プロパティーを無効にすると対応するプロトコルサービスネットワークポートが閉じるため、Oracle ILOM でそのプロトコルサービスを使用できなくなります。

関連情報

- 「管理サービスおよびネットワークのデフォルトのプロパティー」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』

- 「管理サービスおよびネットワークのデフォルトのプロパティー」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「ネットワーク設定の構成」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「ネットワーク設定の構成」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

▼ KVMS サービスの状態とポートを変更する

始める前に

- KVMS サービスの「State」プロパティーは、Oracle ILOM でデフォルトで有効になっています。KVMS サービスに関連付けられた開いているネットワークポートの一覧については、表4「デフォルトで有効になるサービスとポート」を参照してください。
- Oracle ILOM で KVMS の「State」プロパティーを変更するには、Admin (a) の役割が必要です。

1. **Oracle ILOM Web インタフェースで、「KVMS」タブに移動します。**

   たとえば:

   - **3.0.x Web インタフェースで、「Remote Control」->「KVMS」をクリックします。**
   - **3.1 以降の Web インタフェースで、「Remote Console」->「KVMS」をクリックします。**

2. **「KVMS」タブで KVMS State プロパティーを変更し、「Save」をクリックして変更を適用します。**

   State プロパティーを変更すると開いていた KVMS サービスネットワークポートが閉じるため、a) リモートホストコンソールと、b) Oracle ILOM リモートコンソールおよび Oracle ILOM リモートストレージ CLI、または Oracle ILOM リモートコンソールプラスを使用できなくなります。

関連情報

- 「ローカルクライアントの KVMS 設定の構成」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「ローカルクライアントの KVMS 設定の構成」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「初期セットアップタスク」、『*Oracle ILOM 3.0 リモートリダイレクションコンソール - Web および CLI ガイド*』

▼ シングルサインオンサービスの状態とポートを変更する

始める前に

- シングルサインオン (SSO) サービスの「State」プロパティーとそれに対応するネットワークポート (1126) は、Oracle ILOM でデフォルトで有効になっています。
- Oracle ILOM で SSO サービスの「State」プロパティーを変更するには、Admin (a) の役割が必要です。

1. **Oracle ILOM Web インタフェースで、「User Account」タブに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「User Management」->「User Account」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「User Account」をクリックします。**

2. **「User Account」ページで SSO State プロパティーを変更し、「Save」をクリックして変更を適用します。**
   Oracle ILOM で SSO State プロパティーを無効にすると、a) 開いていた SSO ネットワークポートが閉じ、b) KVMS コンソールの起動時にユーザーはパスワードの再入力を求められ、c) CMM ユーザーはパスワードを再入力しなくてもブレードサーバー SP に移動できます。

関連情報

- 「シングルサインオンサービス」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「シングルサインオンサービス」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「シングルサインオンの構成」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「シングルサインオンを設定する」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

Oracle ILOM ユーザーアクセスのセキュリティー保護

Oracle ILOM でユーザーアクセスをセキュリティー保護するには、次のトピックを参照してください。

共有ユーザーアカウントの作成の回避

共有アカウントの作成を回避することで、セキュアな環境を維持します。共有アカウントとは、特定のユーザーアカウントパスワードを共有するユーザーアカウントのことです。共有アカウントを作

成するのではなく、Oracle ILOM に対するアクセス権を持つ各ユーザーに一意なパスワードを作成するのが、ユーザーアカウントの適切な処理方法です。各ユーザーアカウントとパスワードの組み合わせを知っているのは 1 人のユーザーだけであるようにしてください。

注記 - Oracle ILOM でサポートされるローカルユーザーアカウントは 10 個までです。より多くのユーザーに Oracle ILOM に対するアクセス権を与える必要がある場合は、LDAP や Active Directory などのディレクトリサービスを構成することにより、集中管理されたデータベースを使用してより多くのアカウントをサポートできます。詳細は、28 ページの「リモート認証サービスとセキュリティープロファイル」を参照してください。

一意のパスワードを付与して個々のユーザーアカウントを作成した後、システム管理者は事前構成の管理者 `root` アカウントに一意のパスワードが割り当てられていることを確認する必要があります。そうしないと、一意のパスワードが設定されていない事前構成の管理者 `root` アカウントは共有アカウントと見なされます。許可されていないユーザーによる事前構成の管理者 `root` アカウントの使用を防ぐため、事前構成の `root` アカウントのパスワードを変更するか、Oracle ILOM からアカウントを削除する必要があります。事前構成の管理者 `root` アカウントの詳細は、30 ページの「初回ログイン時に `root` アカウントのデフォルトのパスワードを変更する」を参照してください。

一意のパスワードを持つセキュアなアカウントを作成する方法の詳細は、26 ページの「ユーザーアカウントとパスワードの管理のセキュリティーガイドライン」を参照してください。

ユーザーアカウント構成の詳細は、29 ページの「最大限のセキュリティーを確保するためのユーザーアクセスの構成」を参照してください。

役割ベースの権限の割り当て

すべての Oracle ILOM ユーザーアカウントには、一連の役割ベースの権限が与えられます。これらの役割ベースの権限により、Oracle ILOM 内の個々の機能に対するアクセス権を与えることができます。たとえば、システムをモニターできるが構成の変更は一切できないようなユーザーアカウントを構成できます。あるいは、大部分の構成オプションの変更は許可するが、ユーザーアカウントの作成と変更は許可しないようにすることもできます。さらには、サーバーの処理能力を制御できるユーザーやリモートコンソールにアクセスできるユーザーを制限することも可能です。各権限レベルを理解し、それらを組織内のユーザーに適切に割り当てることが重要です。

次の表は、Oracle ILOM の各ユーザーアカウントに割り当てることができる権限の一覧を示しています。

表 7 ユーザーアカウント権限の説明

役割	説明
`Admin (a)`	ユーザーはすべての Oracle ILOM 構成オプションを変更できますが、ユーザー管理など、ほかの権限によって明示的に承認されている構成オプションは除きます。

役割	説明
User Management (u)	ユーザーは、ユーザーの追加と削除、ユーザーパスワードの変更、認証サービスの構成を実行できます。この役割を与えられたユーザーは、すべての権限を持つ別のユーザーアカウントを作成できるので、この役割はすべてのユーザーの役割の中で最高レベルの権限を持ちます。
Console (c)	ユーザーはホストコンソールにリモートからアクセスできます。このリモートからのコンソールへのアクセス権により、ユーザーは、BIOS または OpenBoot PROM (OBP) にアクセスできる可能性があり、それにより、ブート動作を変更して、システムにアクセスできるようになります。
Reset and Host Control (r)	ユーザーは、ホストの処理能力の制御や Oracle ILOM のリセットを実行できます。
Read-only (o)	ユーザーは、Oracle ILOM ユーザーインタフェースへの読み取り専用アクセス権を与えられます。このアクセス権はすべてのユーザーに付与されており、ログや環境情報を参照したり、構成設定を表示したりできます。

ローカルユーザーアカウントの作成と役割ベースの権限の割り当ての詳細は、32 ページの「役割ベースの権限を持つローカルユーザーアカウントを作成する」を参照してください。

ユーザーアカウントとパスワードの管理のセキュリティーガイドライン

Oracle ILOM ユーザーアカウントおよびパスワードの管理時には、次のセキュリティーガイドラインを考慮してください。

- 26 ページの「ユーザーアカウントの管理のガイドライン」
- 27 ページの「パスワード管理のガイドライン」

ユーザーアカウントの管理のガイドライン

ユーザーアカウントの管理のガイドライン	説明
ユーザーアカウントの共有を決して推奨しないでください	常に Oracle ILOM ユーザーごとに別個のアカウントを作成するべきです。 Oracle ILOM は、最大 10 個のローカルユーザーアカウントをサポートします。比較的大きいサイトを管理していて、10 個を超えるユーザーアカウントが必要な場合は、LDAP や Active Directory などのサードパーティーのユーザー認証サービスの使用を検討するべきです。 外部の認証サービスを使用した Oracle ILOM でのユーザー認証の実装に関する詳細は、28 ページの「リモート認証サービスとセキュリティープロファイル」を参照してください。
ローカルユーザーアカウントに準拠した名前を選択します	ローカル Oracle ILOM ユーザーアカウントのユーザー名の選択時に、ユーザー名は: ■ 4 - 16 文字の長さにします (最初の文字は文字である必要があります)。 ■ 組織内で一意である必要があります ■ スペース、ピリオド (.)、またはコロン (:) を含めません
ローカルユーザーアカウントに準拠したパスワードを選択します	ローカル Oracle ILOM ユーザーアカウントのパスワードの選択時に、パスワードは: ■ 必ず長さが最大 16 文字の強力なパスワードにします

ユーザーアカウントの管理のガイドライン	説明
	■ 強力で複雑なパスワードを作成するには、小文字と大文字を混在させ、1 つまたは 2 つの特殊文字を含めます ■ スペース、ピリオド (.)、またはコロン (:) を含めません ■ 会社のパスワード管理ポリシーに準拠します Oracle ILOM でのパスワード管理の詳細は、26 ページの「ユーザーアカウントとパスワードの管理のセキュリティーガイドライン」を参照してください。
担当業務に基づいてユーザーアカウント権限を制限します (*最小権限の原則*)	最小権限の原則とは、適切なセキュリティー対策を実施するために、ユーザーにはその業務を遂行するために必要な最小限の権限だけを与えることです。とりわけ組織のライフサイクルの初期の段階で、責任、役割などを必要以上に与えてしまうと、システムの乱用を許してしまう可能性があります。ユーザー最小権限の原則を定期的に確認して、各ユーザーの現在の職務責任に対する妥当性を判断します。 Oracle ILOM には、ユーザーごとに権限を管理する機能が用意されています。各ユーザーアカウントに対して、担当業務に基づく適切なユーザーの役割の権限を割り当ててください。 役割ベースの権限を持つユーザーアカウントの作成方法の詳細は、32 ページの「役割ベースの権限を持つローカルユーザーアカウントを作成する」を参照してください。

パスワード管理のガイドライン

パスワード管理のガイドライン	説明
初回ログインの直後にデフォルトの `root` パスワード (`changeme`) を変更する	Oracle ILOM への初回のログインとアクセスを有効にするために、システムにはローカル管理者 `root` アカウントが用意されています。セキュアな環境を構築するには、Oracle ILOM への初回ログインのあとに、用意されている管理者パスワード (`changeme`) を変更する必要があります。 管理者 `root` アカウントへの不正なアクセスを取得すると、ユーザーには Oracle ILOM のすべての機能への無制限のアクセスが与えられます。そのため、強力でセキュアなパスワードを指定することが不可欠となります。
Oracle ILOM アカウントのすべてのパスワードを定期的に変更する	悪意のあるアクティビティーを防止し、パスワードが現在のパスワードポリシーに確実に準拠しているようにするには、すべての Oracle ILOM パスワードを定期的に変更するべきです。
強力で複雑なパスワードを作成するための一般的なルールを適用します	強力で複雑なパスワードを作成するための次の一般的なルールを適用します。 ■ 長さが 16 文字より短いパスワードを作成しません。 ■ 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ません。 ■ 簡単に推測できるパスワードを選択しません。 ■ 12345 など、連続した数字文字列を含むパスワードを作成しません。 ■ 単純な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でください。 ■ ユーザーに同じパスワードの複数のシステム間での再利用を許可しないでください。 ■ ユーザーに古いパスワードの再利用を許可しないでください。 ■ 最大限のセキュリティーを確保するため、CLI では次の構文を使用して、新しいパスワードエントリを常にマスクするようにしてください。 **`set [`***SP|CMM***`]/users/root password=`**[*do not type password, press Enter*] または **`set [`***SP|CMM***`]/users/newuser password=`**[*do not type password, press Enter*] CLI は、パスワードをビューからマスクした状態で新しいパスワード値の入力を求めます。

パスワード管理のガイドライン	説明
ローカルユーザーのパスワードポリシー制限を設定する (ファームウェア 3.2.5 以降で使用可能)	すべてのローカルユーザーアカウントのパスワードポリシーを適用します。詳細は、29 ページの「すべてのローカルユーザーのパスワードポリシー制限を設定する (3.2.5 以降)」を参照してください。
パスワード管理ポリシーについて IT セキュリティー責任者に問い合わせる	IT セキュリティー責任者に問い合わせて、会社のパスワード管理要件およびポリシーが満たされていることを確認します。

リモート認証サービスとセキュリティープロファイル

Oracle ILOM は、外部の集中管理されたユーザーストアを使用するように構成できるので、Oracle ILOM の各インスタンス上にローカルユーザーを構成する必要はありません。これにより、ユーザー証明書の一元的な作成と変更、およびユーザーによる多数の異なるシステムへのアクセスが可能になり、利便性がさらに向上します。

認証サービスを選択および構成する前に、これらのサービスがどのように動作し、それぞれをどのように構成する必要があるかを理解してください。サポートされている各サービスは、認証だけでなく、Oracle ILOM ユーザー権限を特定のリモートユーザーに割り当てる方法を定義した承認ルールを構成する機能も備えています。適切なユーザーの役割または権限を割り当ててください。

次の表に、Oracle ILOM でサポートされているユーザー認証サービスを示します。

表 8 リモート認証サービスとセキュリティープロファイル

サービス名	セキュリティープロファイル	情報
Active Directory	高	■ このサービスはデフォルトでセキュアになっています。 ■ 厳密な証明書モードを使用するには、証明書サーバーが必要になりますが、それによりセキュリティーがさらに強化されます。
Lightweight Directory Access Protocol/Secure Socket Layer (LDAP/SSL)	高	■ このサービスはデフォルトでセキュアになっています。 ■ 厳密な証明書モードを使用するには、証明書サーバーが必要になりますが、それによりセキュリティーがさらに強化されます。
Legacy LDAP	低	■ このサービスは、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。
Remote Authentication Dial In User Service (RADIUS)	低	■ このサービスは、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。

高いセキュリティープロファイルを持つサービスは、証明書、および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できます。セキュリティープロファイルの低いサービスはデフォルトで無効になっています。これらの低いセキュリティープロファイルは、セキュリティーレベルが低いことによる制限を理解して受け入れる場合にのみ、有効にしてください。

リモート認証サービスの構成の詳細は、次に示す適切な Oracle ILOM ドキュメントを参照してください。

- 「ユーザーアカウントの設定および管理」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「ユーザーアカウントの設定および管理」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「ユーザーアカウントの管理」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「ユーザーアカウントを管理する」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

最大限のセキュリティーを確保するためのユーザーアクセスの構成

最大限のセキュリティーを確保するように Oracle ILOM のユーザーアクセスを最適に構成する方法については、次のトピックを参照してください。

- 29 ページの「すべてのローカルユーザーのパスワードポリシー制限を設定する (3.2.5 以降)」
- 30 ページの「初回ログイン時に `root` アカウントのデフォルトのパスワードを変更する」
- 32 ページの「役割ベースの権限を持つローカルユーザーアカウントを作成する」
- 33 ページの「KVMS セッションの終了時にホストアクセスをロックする」
- 34 ページの「リモートシステムコンソールプラスで表示できる KVMS セッションを制限する (3.2.4 以降)」
- 35 ページの「ログインバナーを使用してシステムアクセスをセキュリティー保護する (3.0.8 以降)」

ユーザーアクセスのプロパティーは、Oracle ILOM のコマンド行インタフェース (CLI) または Web インタフェースを使用して構成できます。このセクションの手順は、すべての Oracle ILOM ファームウェアリリースに対応する Web ベースのナビゲーション手順を示しています。CLI の手順または構成プロパティーの詳細は、各手順の最後にある「関連情報」セクションに記載されている適切なドキュメントを参照してください。

▼ すべてのローカルユーザーのパスワードポリシー制限を設定する (3.2.5 以降)

ファームウェアリリース 3.2.5 時点の Oracle ILOM は、すべてのローカルユーザーアカウントのパスワードポリシーを適用します。パスワードポリシーには、パスワードポリシー制限のデフォルトセットが標準装備されています。システム管理者は、デフォルトのプロパティーをそのまま使用するか、またはそれらを各パスワードポリシーのニーズが満たされるように変更するかのどちらかを選択できます。

注記 - パスワードポリシーのプロパティーへの変更は、ローカルユーザーアカウントの作成前に設定するようにしてください。パスワードポリシーのプロパティーがローカルユーザーアカウントの構成後に変更された場合、Oracle ILOM は自動的に 1) すべてのローカルユーザーアカウントの構成を削除し、2) システムに最初に標準装備されていたデフォルトの root アカウントを復元します。

始める前に

- パスワードポリシーのプロパティーを構成するには、Admin (a) の役割が必要です。
- パスワードポリシーは、ローカルユーザーアカウントにのみ適用されます。LDAP や Active Directory などのリモートユーザー認証サービスのアカウントには影響を与えません。
- パスワードポリシーのプロパティーへの変更を保存すると、次が実行されます。
  - すべてのローカルユーザーアカウント構成が Oracle ILOM から削除されます。
  - システムに標準装備されているデフォルトのローカルユーザーアカウント (root) が復元されます。
  - root の初回ログイン時、root ユーザーは、root アカウントのパスワードを変更するよう求められます。

すべてのローカルユーザーのパスワードポリシーを設定するには、次の Web ベースの手順を使用します。

注記 - CLI のパスワードポリシー手順については、この手順の「関連情報」セクションに記載されている Oracle ILOM 管理ガイドのリファレンスをクリックしてください。

1. **Oracle ILOM で現在のパスワードポリシー制限を表示するには、「ILOM Administration」>「User Management」>「Password Policy」をクリックします。**
2. **パスワードポリシー制限を変更するには、「Password Policy」ページにある「More Details...」リンクをクリックして詳しい手順を確認します。**
3. **変更を保存するには、「Save」をクリックします。**

関連情報

- 「Modify Password Policy Restrictions for Local Users」in『Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x』

▼ 初回ログイン時に root アカウントのデフォルトのパスワードを変更する

Oracle ILOM への初回のログインとアクセスを有効にするために、システムには事前構成された管理者 root アカウントとデフォルトのパスワード (changme) が用意されています。Oracle

ILOM への不正なアクセスを防止するために、事前構成された root アカウントに標準装備されているデフォルトのパスワード (changeme) を初回ログイン時に変更する必要があります。そうしないと、事前構成された root アカウントとデフォルトのパスワード (changeme) が共有アカウントとして機能するため、管理者アクセスがすべてのユーザーに対して有効になります。

事前構成された管理者 root アカウントに標準装備されているデフォルトのパスワード (changeme) を変更するには、次の Web ベースの手順を使用します。

注記 - 事前構成の root アカウントへのアクセス権がないユーザーが Oracle ILOM 管理者機能にアクセスする必要がある場合は、システム管理者に連絡し、管理者権限のあるユーザーアカウントを入手してください。

始める前に

- 26 ページの「ユーザーアカウントとパスワードの管理のセキュリティーガイドライン」について確認します。

  注記 - Oracle ILOM への無許可のアクセスを防ぐためには、root アカウントに強力でセキュアなパスワードを割り当てる必要があります。強力なパスワードにするには、大文字と小文字を混在させ、少なくとも 1 つの特殊文字 (% や $) を含める必要があります。

- Oracle ILOM でローカルユーザーアカウントのパスワードを変更するには User Management (u) の役割が必要です。

1. **Oracle ILOM Web インタフェースで、「User Account」ページに移動します。**

   たとえば:

   - **3.0.x Web インタフェースで、「User Management」->「User Accounts」をクリックします。**
   - **3.1 以降の Web インタフェースで、「User Management」->「User Accounts」をクリックします。**

2. **「User Account」ページで、root アカウントの「Edit」をクリックします。**

   「Edit: User Root」ダイアログが表示されます。

3. **「Edit: User Root」ダイアログで次を実行します。**

   - **「New Password」テキストボックスに一意のパスワードを入力し、「Confirm New Password」テキストボックスに同じパスワードを再入力します。**
   - **「Save」をクリックして変更を適用します。**

関連情報

- 「ローカルユーザーアカウントの構成」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「ローカルユーザーアカウントの構成」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- ユーザーアカウントの変更、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「ユーザーアカウントを変更する」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』
- 60 ページの「root アカウントのデフォルトパスワードをリセットする際の物理的セキュリティープレゼンス」

▼ 役割ベースの権限を持つローカルユーザーアカウントを作成する

始める前に Oracle ILOM では、1 つの SP またはシャーシモニタリングモジュール (CMM) に最大 10 個のローカルユーザーアカウントを作成して保存できます。Oracle ILOM ユーザーには権限のセットが割り当てられるため、ユーザーは構成されたアカウントで許可される範囲で機能を使用できます。

注記 - システム管理者はリモート認証サービスを使用して Oracle ILOM を構成することで、さらに多くのユーザーアカウントをサポートすることも可能です。リモート認証サービス構成では、ログイン、パスワード、および権限が外部ユーザーストアから導出されます。詳細は、28 ページの「リモート認証サービスとセキュリティープロファイル」を参照してください。

役割ベースのアクセス権限を持つローカルユーザーアカウントを構成するための Web ベースの手順については、次の手順を参照してください。

始める前に

- 26 ページの「ユーザーアカウントとパスワードの管理のセキュリティーガイドライン」について確認します。
- 表7「ユーザーアカウント権限の説明」の「Oracle ILOM でサポートされている Web ブラウザ」を確認してください。
- Oracle ILOM で権限を持つローカルユーザーアカウントを作成するには、User Management (u) の役割が必要です。

1. **Oracle ILOM Web インタフェースで、「User Account」ページに移動します。**

   たとえば:

   - **3.0.x Web インタフェースで、「User Management」->「User Accounts」をクリックします。**
   - **3.1 以降の Web インタフェースで、「User Management」->「User Accounts」をクリックします。**

2. **「User Account」ページで「Add」をクリックします。**
   「Add User」ダイアログが表示されます。

3. **「Add User」ダイアログで次を実行します。**

   a. **「User Name」テキストボックスでユーザー名を指定します。**

   b. **「Roles」ドロップダウンリストで、適切なユーザー役割のプロファイル (Administrator、Operator、または Advanced) を選択します。**

   c. **「New Password」テキストボックスに一意のパスワードを入力し、「Confirm New Password」テキストボックスに同じパスワードを再入力します。**

   d. **「Save」をクリックして変更を適用します。**

関連情報

- 「ユーザーアカウントの作成とユーザーの役割の割り当て」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「ユーザーアカウントの作成とユーザーの役割の割り当て」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- ユーザーアカウントの追加および役割の割り当て、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「ユーザーアカウントを追加して役割を割り当てる」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

▼ KVMS セッションの終了時にホストアクセスをロックする

リモート KVMS を使用している間、ホストコンソールは共有ネットワークリソースとみなされるため、あるユーザーがホストコンソールにログインしたあと、ホストオペレーティングシステムからログアウトせずに Oracle ILOM リモートシステムコンソール、リモートシステムコンソールプラス、または CLI ストレージリダイレクションアプリケーションを閉じた場合、同じコンソールにリモート KVMS を使って接続した 2 番目のユーザーは以前に認証済みのオペレーティングシステムセッションを使用できます。このため、Oracle ILOM では、リモート KVMS セッションが切断されるたびにホストオペレーティングシステムを自動的にロックする機能を提供しています。最大限のセキュリティーを確保するため、Oracle ILOM でこの機能を有効にするか構成してください。

KVMS セッションの終了後にリモートホストデスクトップをロックするには、次の Web ベースの手順を参照してください。ホストロック機能を有効化する方法の詳細は、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』を参照してください。

始める前に

- Oracle ILOM でホストロックモードプロパティーを変更するには Console (c) の役割が必要です。
- Oracle ILOM のホストロックモード機能を使用するにはファームウェア 3.0.4 以降が必要です。
- ホストロックモード機能はデフォルトで無効になっています。

1. **Oracle ILOM Web インタフェースで「KVMS」ページに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「Remote Console」->「KVMS」をクリックします。**
   - **3.1 以降の Web インタフェースで、「Remote Control」->「KVMS」をクリックします。**

2. **「KVMS」ページの「Host Lock Settings」セクションで、次のいずれかを実行します。**

   - **ロックモードを指定します (Windows、Custom、または Disabled)。**
   - **「Save」をクリックして変更を適用します。**

関連情報

- ホストデスクトップのロック、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- ホストデスクトップのロック、『*Oracle ILOM 3.1 構成および保守ガイド*』
- KVMS ロック、『*Oracle ILOM 3.0 リモートリダイレクションコンソール - CLI および Web ガイド*』

▼ リモートシステムコンソールプラスで表示できる KVMS セッションを制限する (3.2.4 以降)

ファームウェアリリース 3.2.4 の時点では、リモートシステムコンソールプラスのプライマリユーザーは「Maximum Client Session Count」を 1 セッションビューアに制限することによって、ビデオリダイレクションセッション中に入力された機密データが SP 上のほかのサインインセッションユーザーに表示されないようにできます。デフォルトでは、Oracle ILOM リモートシステムコンソールプラスの「Maximum Client Session Count」プロパティーは 4 セッションビューアに設定されています。

Oracle ILOM リモートシステムコンソールプラスの「Maximum Client Session Count」プロパティーを変更するには、次の Web ベースの手順を参照してください。

始める前に

- KVMS Oracle ILOM リモートシステムコンソールプラスの「Maximum Client Session Count」プロパティーは、ファームウェアリリース 3.2.4 以降で使用できます。

注記 - KVMS の「Maximum Client Session Count」プロパティーは、Oracle ILOM リモートコンソールをサポートしているシステムでは構成できません。

- Oracle ILOM リモートシステムコンソールプラスは、ファームウェアリリース 3.2.1 時点の新しくリリースされた SP システムでのみ使用できます。
- KVMS Maximum Client Session Count プロパティーを変更するには、Oracle ILOM で Console (c) の役割が必要です。
- Oracle ILOM で Maximum Client Session Count プロパティーをリセットすると、SP 上でアクティブの Oracle ILOM リモートシステムコンソールプラスのビデオセッションがすべて終了します。
- デフォルトで 1 つの SP につき最大 4 つのリモートシステムコンソールプラスビデオリダイレクションセッションを、Oracle ILOM の「Redirection」ページから起動できます。

1. **Oracle ILOM Web インタフェースで「Remote Console」->「KVMS」をクリックし、「KVMS」ページに移動します。**
2. **「KVMS」ページで Maximum Client Session Count プロパティー (指定可能な値: *4* (デフォルト)|*1*|*2*|*3*) を変更します。**
3. **「Save」をクリックして変更を適用します。**

関連情報

- 「リモートデバイスリダイレクトのプロパティー」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』

▼ ログインバナーを使用してシステムアクセスをセキュリティー保護する (3.0.8 以降)

ファームウェアリリース 3.0.8 時点の Oracle ILOM では、システム管理者は、Oracle ILOM の CLI および Web インタフェースにログインしたすべてのユーザーにバナーメッセージを表示できます。ログインバナーの使用は、リモートデバイスによる不正なシステムアクセスから保護したり、承認された正当なユーザーにシステムの受け入れ可能な使用に関連した義務をアドバイスしたりするのに役立ちます。

実装するバナーメッセージは、情報のセキュリティーポリシーに従って作成するようにしてください。作成されるメッセージに関するさらに詳細なガイドラインについては、サイト管理者またはセキュリティー責任者に問い合わせてください。

ログイン時またはログイン後にすべてのユーザーにバナーメッセージを表示するには、次の Web ベースの手順を参照してください。

始める前に

- バナーメッセージを作成するには、Admin (a) の役割が必要です。

- バナーメッセージは、Oracle ILOM ファームウェアリリース 3.0.8 以降で構成できます。
- 管理者は、バナーメッセージを「Login」ページか、またはユーザーが Oracle ILOM にログインした直後に表示されるダイアログに表示されるように構成できます。

1. **Oracle ILOM Web インタフェースで「Banner Message」ページに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「System Information」->「Banner Messages」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」->「Banner Messages」をクリックします。**

2. **「Banner Message」ページで、「*More Details...*」リンクをクリックして、バナーメッセージを構成する方法を決定します。**
   CLI の手順については、この手順の「関連情報」セクションに記載されている該当する *Oracle ILOM 管理ガイド*を参照してください。

3. **「Save」をクリックして変更を適用します。**

関連情報

- 「Management of Banner Messages at Log-In」 in『Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x』
- 「バナーメッセージの管理」、『*Oracle ILOM 構成および保守用管理者ガイド (ファームウェア 3.2.x)*』
- 「バナーメッセージの構成プロパティー」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「バナーメッセージの表示」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「バナーメッセージの表示」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

最大限のセキュリティーを得るための Oracle ILOM インタフェースの構成

最大限のセキュリティーを得るための Oracle ILOM インタフェースの構成については、次のトピックを参照してください。

- 37 ページの「最大限のセキュリティーを得るための Web インタフェースの構成」
- 43 ページの「最大限のセキュリティーを確保するように CLI を構成する」
- 47 ページの「最大限のセキュリティーを得るための SNMP 管理アクセスの構成」

- 49 ページの「最大限のセキュリティーを得るための IPMI 管理アクセスの構成」
- 52 ページの「最大限のセキュリティーを得るための WS-Management アクセスの構成」

最大限のセキュリティーを得るための Web インタフェースの構成

最大限のセキュリティーを得るための Oracle ILOM Web インタフェースの最適な構成方法については、次のトピックを参照してください。

注記 - コマンド行インタフェース (CLI) または Web インタフェースを使用して、Oracle ILOM の Web 管理インタフェースプロパティーを構成できます。このセクションの手順は、すべての Oracle ILOM ファームウェアリリースに対応する Web ベースのナビゲーション手順を示しています。CLI の手順または構成プロパティーの詳細は、各手順の最後にある「関連情報」セクションに記載されている適切なドキュメントを参照してください。

- 37 ページの「信頼できる SSL 証明書および非公開鍵の使用によるセキュリティーの向上」
- 40 ページの「もっとも強力な SSL および TLS 暗号化プロパティーを有効にする」
- 42 ページの「非アクティブの Web セッションに対するタイムアウト間隔を設定する」

信頼できる SSL 証明書および非公開鍵の使用によるセキュリティーの向上

Secure Socket Layer (SSL) 証明書は、ネットワークを介した通信の暗号化とサーバーまたはクライアントの信頼性を保つために使用されます。Oracle ILOM には SSL 自己署名証明書が含まれており、これにより、HTTP over SSL プロトコルをすぐに利用できます (証明書をアップロードする必要はありません)。Oracle ILOM Web インタフェースに最初に接続すると、ユーザーは、自己署名証明書が使用されていることを通知され、その使用を受け入れるかどうかを尋ねられます。用意された証明書を使用することにより、Web ブラウザと Oracle ILOM 間の通信がすべて完全に暗号化されます。

ただし、信頼できる証明書を作成してアップロードしセキュリティーの向上を図ることも可能です。信頼できる証明書とは、その証明書が信頼できる認証局との連携によって認可されていることを意味します。既知の認証局からの信頼できる証明書を使用することで、Oracle ILOM Web サーバーの信頼性が確保されます。信頼できない (自己署名) 証明書を使用すると、中間者 (MITM) 攻撃の可能性にさらされます。

一時的な自己署名証明書または認証局署名の証明書を入手してアップロードするには、次の手順を参照してください。

- 38 ページの「OpenSSL を使用して SSL 証明書および非公開鍵を入手する」

■ 39 ページの「カスタム SSL 証明書と非公開鍵を Oracle ILOM にアップロードする」

▼ OpenSSL を使用して SSL 証明書および非公開鍵を入手する

この手順は、OpenSSL ツールキットを使用して SSL 証明書と非公開鍵を作成する方法の概略を示したものです。

注記 - Oracle ILOM では、OpenSSL を使用して SSL 証明書を生成する必要は*ありません*。この手順では、あくまでも参考として OpenSSL を使用しています。SSL 証明書はその他のツールでも生成できます。

一時的な自己署名証明書と認証局署名の証明書のどちらを使用するかは、サイト管理者またはセキュリティー責任者の決定事項です。SSL 証明書 (一時的な自己署名または認証局署名) を入手する必要がある場合は、次の例の OpenSSL コマンド行の手順に従います。

注記 - SSL 証明書の生成に関する詳しい OpenSSL 手順が必要な場合は、OpenSSL ツールキットに付属しているユーザードキュメントを参照してください。

---

1. **証明書と非公開鍵を保存するネットワーク共有ディレクトリまたはローカルディレクトリを作成します。**

2. **OpenSSL ツールキットを使用して新しい RSA 非公開鍵を作成するには、次のように入力します。**

   ```
   openssl genrsa -out <foo>.key 2048
   ```

   ここで、*<foo>* は非公開鍵の名前です。

   注記 - この非公開鍵は PEM 形式で保存される 2048 ビット RSA 鍵であるため、ASCII テキストとして読み取りが可能です。

   ---

3. **OpenSSL ツールキットを使用して証明書署名要求 (CSR) を生成するには、次のように入力します。**

   ```
   openssl req -new -key <foo>.key -out <foo>.csr
   ```

   ここで、*<foo>* は証明書署名要求の名前です。

   注記 - CSR の生成中、いくつかの情報を要求されます。

   現在の作業ディレクトリに、*<foo>*`.csr` ファイルが生成されます。

4. **SSL 証明書を生成するには、次のいずれかを実行します。**

   ■ **一時的な自己署名証明書を生成します (365 日有効)。**

自己署名 SSL 証明書は、`server.key` 非公開鍵と `server.csr` ファイルから生成されます。

OpenSSL ツールキットを使用して、次のように入力します。

```
openssl x509 -req -days 365 -in <foo>.csr
-signkey <foo>.key -out <foo>.cert
```

ここで、*<foo>* は非公開鍵 (`.key`) または証明書 (`.cert`) に割り当てる名前です。

注記 - この一時証明書では、署名認証局は不明で信頼できないという内容のエラーがクライアントブラウザに表示されます。このエラーを許容できない場合は、認証局に署名済み証明書の発行を依頼する必要があります。

- **公的に署名された証明書を認証局プロバイダから入手します。**

  証明書署名要求 (*<foo>*`.csr`) を SSL 認証局プロバイダに提出します。ほとんどの認証局プロバイダで、Web アプリケーション画面上の CSR 出力をカット & ペーストすることが必要になります。署名済証明書の入手には通常 7 営業日かかります。

5. **新しい SSL 証明書と非公開鍵を Oracle ILOM にアップロードします。**

   次の 39 ページの「カスタム SSL 証明書と非公開鍵を Oracle ILOM にアップロードする」の手順を参照してください。

▼ カスタム SSL 証明書と非公開鍵を Oracle ILOM にアップロードする

始める前に

- Oracle ILOM で Web サーバープロパティーを変更するには、Admin (a) の役割が必要です。
- 新しい (一時的な自己署名または認証局署名) HTTPS 証明書と非公開鍵を入手します。OpenSSL ツールキットの使用手順については、38 ページの「OpenSSL を使用して SSL 証明書および非公開鍵を入手する」を参照してください。
- 新しい HTTPS 証明書と非公開鍵にネットワークまたはローカルファイルシステム経由でアクセスできることを確認してください。

1. **Oracle ILOM Web インタフェースで、「SSL Certificate」ページに移動します。**

   たとえば:

   - **3.0.x Web インタフェースで、「Configuration」->「System Management Access」->「SSL Certificate」をクリックします。**

   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」->「SSL Certificate」をクリックします。**

2. 「SSL server」ページで、次を実行します。

   a. 「File Transfer Method」プロパティーで指定されているカスタム証明書ファイルをアップロードするには「Load Certificate」ボタンをクリックします。

   b. 「File Transfer Method」プロパティーで指定されているカスタム非公開鍵ファイルをアップロードするには「Load Custom Private Key」ボタンをクリックします。

   c. 「Save」をクリックして変更を適用します。

関連情報

- SSL 証明書および非公開鍵の構成プロパティー、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- SSL 証明書および非公開鍵の構成プロパティー、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「SSL 証明書のアップロード」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「SSL 証明書のアップロード」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

▼ もっとも強力な SSL および TLS 暗号化プロパティーを有効にする

Oracle ILOM は、もっとも強力な暗号を備えたもっとも強力な Secure Socket Layer 暗号化 (SSLv3 と TLS v1.0、v1.1、および v1.2) プロトコルをサポートしています。ただし、場合によっては、古い Web ブラウザの使用をサポートするために SSLv2 または弱い暗号の有効化が必要になることがあります。

セキュリティーポリシーの要件を満たすために Oracle ILOM で SSL および TLS プロパティーを設定するには、この手順を使用します。

注記 - SSL および TLSv1.0 のサポートは、ファームウェアリリース 3.1.0 の時点で使用可能になりました。TLS v1.1 および v1.2 のサポートは、ファームウェアリリース 3.2.4 時点の Oracle ILOM で使用可能になりました。

始める前に

- Oracle ILOM で Web サーバープロパティーを変更するには、Admin (a) の役割が必要です。
- Oracle ILOM での TLS プロパティーのデフォルト設定は、現在サーバーにインストールされているファームウェアバージョンに依存します。

ファームウェア	TLS のデフォルト
3.1.x、3.2.1.x、3.2.2.x、および 3.2.3.x	TLS v1.0 が有効
3.2.4 以降	TLS v1.0、v1.1、および v1.2 が有効

- 3.2.4 *より前の* Oracle ILOM ファームウェアリリースでは、SSLv3 プロパティーがデフォルトで有効になっています。

注記 - SSLv3 で検出されたセキュリティーの脆弱性のために、修正が使用可能になるまでは SSLv3 を無効にするようにしてください。詳細は、Oracle: MOS SSLv3 の脆弱性に関する記事を参照してください。

- Oracle ILOM ファームウェアリリース 3.2.4.x 以降では、デフォルトの SSLv3 設定は、サーバーモデルとインストールされている 3.2.4.x ファームウェアバージョンに依存します。

サーバーモデル	ファームウェア	SSLv3 のデフォルト
SPARC T3、T4、 T5、M5、M6	3.2.4.1	SSLv 3 は無効
X4-2	3.2.4.20 (x4-2)	SSLv3 が有効
X4-2L	3.2.4.22 (x4-2L)	詳細は、MOS SSLv3 の脆弱性に関する記事を参照してください。
X4-2B	3.2.24.24 (X4-2B)	
X4-4	3.2.4.18	SSLv3 が有効
X4-8		詳細は、MOS SSLv3 の脆弱性に関する記事を参照してください。
X5-2	3.2.4.10 (x5-2)	SSLv3 は無効
X5-2L	3.2.4.12 (x5-2L)	

- SSLv2 および「Weak Cyphers」プロパティーは、Oracle ILOM でデフォルトで無効になる

Oracle ILOM で SSL または TLS Web サーバーのセキュリティープロパティーを表示または変更するには、次の Web ベースの手順を参照してください。

1. **Oracle ILOM Web インタフェースで、「ILOM Administration」->「Management Access」->「Web Server」をクリックします。**
2. **「Web Server」ページで、SSL、TLS、または弱い暗号の Web セキュリティープロパティーを表示または変更します。**
3. **「Save」をクリックして変更を適用します。**

関連情報

- 「Web サーバーの構成プロパティー」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「Web サーバーの構成プロパティー」、『*Oracle ILOM 3.1 構成および保守ガイド*』

▼ 非アクティブの Web セッションに対するタイムアウト間隔を設定する

Oracle ILOM Web セッションのタイムアウト間隔は、Web アクセスユーザーのログアウト忘れに対するセキュリティー保護です。Web セッションタイムアウト間隔は、アクティブでない HTTP または HTTPS Web セッションが自動的にログアウトされるまでの経過時間 (分) を決定します。この機能により、Oracle ILOM に対する認証された Web セッションを確立した無人のコンピュータを、無許可のユーザーが発見する危険性を軽減できます。

HTTP および HTTPS セッションに対して設定されている Web セッションタイムアウト間隔を表示または変更するには、次の Web ベースの手順を参照してください。

始める前に

- HTTP および HTTPS 接続に対して設定されているデフォルトの Web セッションタイムアウト間隔は 15 分です。

注記 - セッションタイムアウトを短くすると、セッションの期限切れによる、ユーザー名とパスワードの再入力を求められる回数が増える場合があります。しかし、セッションタイムアウトを短くすると、無人の認証済み Web セッションがアクティブの状態に置かれる時間が短くなります。

- Web サーバープロパティーを変更するには Admin (a) の役割が必要です
- HTTP および HTTPS セッションのタイムアウト間隔プロパティーは、ファームウェアリリース 3.0.4 以降を実行しているサーバー SP の Oracle ILOM でのみ構成が可能です。

1. **「Web Server」ページに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「Configuration」->「System Management Access」->「Web Server」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」->「Web Server」をクリックします。**

2. **「Web Server」ページで、次を実行します。**

   a. **「HTTP or HTTP Session Timeout」プロパティーに移動します。**

b. **アクティブでない Web セッションが自動的にログアウトされるまでの経過時間 (分) を指定する 1 - 720 分の間の数字を入力します。**

c. **「Save」をクリックして変更を適用します。**

関連情報

- 「Web サーバーの構成プロパティー」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「Web サーバーの構成プロパティー」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「セッションタイムアウトを設定する」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

最大限のセキュリティーを確保するように CLI を構成する

最大限のセキュリティーを確保するように Oracle ILOM のコマンド行インタフェース (CLI) を最適に構成する方法については、次のトピックを参照してください。

- 43 ページの「SSH サーバーの状態および弱い暗号の管理 (3.2.5 以降) 」
- 44 ページの「非アクティブの CLI セッションのタイムアウト間隔を設定する」
- 45 ページの「サーバー側鍵を使用して SSH 接続を暗号化する」
- 46 ページの「自動 CLI 認証用としてユーザーアカウントに SSH 鍵を追加する」

CLI 管理プロパティーは、Oracle ILOM のコマンド行インタフェース (CLI) または Web インタフェースを使用して構成できます。このセクションの手順は、すべての Oracle ILOM ファームウェアリリースに対応する Web ベースのナビゲーション手順を示しています。CLI の手順または構成プロパティーの詳細は、各手順の最後にある「関連情報」セクションに記載されている適切なドキュメントを参照してください。

▼ SSH サーバーの状態および弱い暗号の管理 (3.2.5 以降)

ファームウェアリリース 3.2.5 の時点では、「SSH Server State」プロパティーと「Weak Ciphers」プロパティーは Oracle ILOM の CLI および Web インタフェースで構成できます。最大限のセキュリティーを確保するため、「SSH Server State」プロパティーは有効になっており、「Weak Ciphers」プロパティーは無効になっています。これらの SSH 管理アクセスプロパティーを変更するには、次の Web ベースの手順を参照してください。

1. **Oracle ILOM Web インタフェースで、「ILOM Administration」->「Management Access」->「SSH Server」をクリックします。**

2. **「SSH Server」ページで、「*More Details...*」リンクをクリックして詳しい手順を確認します。**

3. **「Save」をクリックして変更を適用します。**

関連情報

- 「SSH サーバーの状態および弱い暗号の管理」、『*Oracle ILOM 構成および保守用管理者ガイド (ファームウェア 3.2.x)*』

▼ 非アクティブの CLI セッションのタイムアウト間隔を設定する

Secure Shell (SSH) プロトコル経由で、またはシリアル接続を使用して Oracle ILOM に接続することによってアクセスされる Oracle ILOM CLI は、非アクティブの CLI セッションを閉じるための構成可能なセッションタイムアウト間隔をサポートしています。構成されている場合、この機能は、承認されていないユーザーが Oracle ILOM への認証された CLI セッションが存在する無人のコンピュータを見つけるリスクを軽減します。

最大限のセキュリティーを確保するため、Oracle ILOM CLI が共有コンソール上で使用されているすべての環境で CLI セッションタイムアウト間隔を構成するようにしてください。理想的には、CLI セッションタイムアウト間隔は 15 分以下に設定するようにしてください。

非アクティブの Oracle ILOM CLI セッションに対して設定されているタイムアウト間隔プロパティーを表示または変更するには、次の Web ベースの手順を参照してください。

始める前に

- CLI プロパティーを変更するには、Admin (a) の役割が必要です。
- SSH 接続に対して設定されたデフォルトの CLI セッションタイムアウト間隔は無効になっており、0 分に設定されています。

注記 - CLI タイムアウト間隔が 0 に設定されていると、セッションがアイドル状態のままになっている時間には関係なく、Oracle ILOM は非アクティブの CLI セッションを閉じません。

- CLI セッションのタイムアウト間隔プロパティーは、ファームウェアリリース 3.0.4 以降を実行しているサーバー SP の Oracle ILOM でのみ構成が可能です。

1. **Oracle ILOM Web インタフェースで「CLI」ページに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「Configuration」->「System Management Access」->「CLI」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」->「CLI」をクリックします。**

2. **「CLI」ページで、次を実行して CLI セッションタイムアウト間隔を設定します。**

a. **「Enable」チェックボックスにチェックマークを付けます。**

b. **アクティブでないコマンド行セッションが自動的にログアウトされるまでの経過時間 (分) を指定する 1 - 1440 分の間の数字を入力します。**

c. **「Save」をクリックして変更を適用します。**

関連情報

- 「CLI セッションタイムアウトの構成プロパティー」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「CLI セッションタイムアウトの構成プロパティー」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- CLI セッションタイムアウトの設定、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』

▼ サーバー側鍵を使用して SSH 接続を暗号化する

Oracle ILOM には Secure Shell (SSH) サーバー機能が用意されており、これにより、リモートクライアントから Oracle ILOM にセキュアに接続しコマンド行インタフェースを介して Oracle ILOM を管理できます。SSH プロトコルは、サーバー側鍵を使用して管理チャネルを暗号化し、すべての通信をセキュリティー保護します。SSH クライアントは、SSH サーバーの信頼性を検証するためにも、これらの鍵を使用します。

Oracle ILOM は、出荷時のデフォルトシステムの最初のブート時に一意の SSH 鍵のセットを生成します。新しいサーバー側鍵が必要になったときのために、Oracle ILOM は手動で SSH サーバー側鍵を生成する機能をサポートしています。

SSH サーバー側暗号化鍵を表示または手動生成するには、次の Web ベースの手順を参照してください。

始める前に

- SSH サーバープロパティーを変更するには Admin (a) が必要です。

1. **Oracle ILOM Web インタフェースで「SSH Server」ページに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「System Management」->「SSH Server」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」->「SSH Server」をクリックします。**

2. **「SSH Server」ページで、生成される RSA および DSA 鍵の情報を確認するか、次を実行します。**

   a. **「Generate RSA Key」をクリックして、新しい鍵を生成します。**

   b. **「Generate DSA Key」をクリックして、新しい鍵を生成します。**

関連情報

- 「SSH サーバーの構成プロパティー」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「SSH サーバーの構成プロパティー」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「新しい SSH 鍵を生成する」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』
- 新しい SSH 鍵の生成、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』

▼ 自動 CLI 認証用としてユーザーアカウントに SSH 鍵を追加する

公開鍵を Oracle ILOM にアップロードし、カスタム生成した SSH 鍵ペア (DSA または RSA) を各ユーザーアカウントに使用できます。これは、手動操作なしで実行し、埋め込み平文パスワードを含まないスクリプトを使用する場合に有用です。ネットワーク経由の SSH 接続でリモートシステムから自動的または定期的にサービスプロセッサコマンドを実行するスクリプトを記述できます。

生成した SSH 公開鍵をアップロードし、Oracle ILOM アカウントに追加するには、次の Web ベースの手順を参照してください。

始める前に

- ssh-keygen などの SSH 接続性ツールを使用して SSH 非公開鍵と公開鍵を生成し、生成された SSH 鍵ファイルをリモート SSH システムに保存します。
- SSH 公開鍵をほかのユーザーアカウントに追加するには User Management (u) の役割が必要です。
- SSH 公開鍵を自分自身のユーザーアカウントに追加するには Read Only (o) の役割が必要です。

1. **Oracle ILOM Web インタフェースで、「User Account」ページに移動します。**

   たとえば:

   - **3.0.x Web インタフェースで、「User Management」->「User Accounts」をクリックします。**

- **3.1 以降の Web インタフェースで、「ILOM Administration」->「User Management」->「User Accounts」をクリックします。**

2. **「User Account」ページで、次を実行します。**

   a. **「SSH Keys」セクションまでスクロールダウンし、「Add」をクリックします。**

   b. **「User list」からユーザーアカウントを選択します。**

   c. **リストから転送方法を選択し、SSH 公開鍵をアップロードするのに必要な転送方法プロパティーを指定します。**

3. **「Load」をクリックして SSH 公開鍵をアップロードし、選択したユーザーアカウントに追加します。**

関連情報

- 「ローカルユーザーの SSH 鍵を使用した CLI での認証」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「ローカルユーザーの SSH 鍵を使用した CLI での認証」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「ユーザーアカウントを管理する」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』
- 「ユーザーアカウントの管理」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』

最大限のセキュリティーを得るための SNMP 管理アクセスの構成

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。Oracle ILOM では、モニタリングと管理の両方に SNMP ソリューションを提供していますが、SNMP を使用するにはまず構成する必要があります。このサービスを構成する前に、SNMP のさまざまなユーザー構成可能なオプションのセキュリティー上の影響を理解しておくことが重要です。詳細は、次の情報を参照してください。

- 47 ページの「SNMPv3 暗号化とユーザー認証を使用する」
- 49 ページの「Sun SNMP MIB でサポートされる構成可能オブジェクト」

▼ SNMPv3 暗号化とユーザー認証を使用する

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。コミュニティー文字列は平文のままネットワーク経由で送信され、個々のユー

ザー専用ではなく、通常は個人のグループ全体で共有されます。対照的に、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します。SNMPv3 のユーザーパスワードは、管理ステーション上にセキュアに格納できるように集められます。

Oracle ILOM では、SNMPv1、SNMPv2c、および SNMPv3 をすべてサポートしており、それぞれ個別に有効化または無効化できます。また、セキュリティーの追加レイヤーを提供するために、「セット」を有効化または無効化できます。この構成可能なオプションは、SNMP サービスが構成可能な SNMP MIB プロパティーの設定を許可するかどうかを指定します。「セット」を無効にすることによって、SNMP サービスを事実上モニタリング専用にすることができます。

デフォルトでは、SNMPv1 と SNMPv2c は無効になっています。SNMPv3 はデフォルトで有効になっていますが、使用する前に 1 人以上の SNMP ユーザーを作成する必要があります。事前構成された SNMPv3 ユーザーはありません。

Oracle ILOM で SNMP 管理を構成するには、次の Web ベースの手順を参照してください。

始める前に

- 最大限の SNMP セキュリティーを実現するために、SNMPv1 および SNMPv2c をモニタリングのみに使用し、これらのセキュアではないプロトコルを有効にするときは「セット」を有効にしないでください。
- SNMPv3 管理にのみ SNMP セットを有効にしてください。SNMP Set プロパティーはデフォルトで無効になっています。
- SNMPv3 セットの場合、SNMPv3 ユーザーアカウントの構成が必要になります。事前構成の SNMPv3 ユーザーアカウントは提供されません。
- SNMP サービスの State プロパティーはデフォルトで有効になっています。
- SNMP プロパティーを変更するには Admin (a) の権限が必要です。
- SNMPv3 ユーザーアカウントを追加または変更するには、User management (u) 権限が必要です。

1. **Oracle ILOM Web インタフェースで「SNMP」ページに移動します。**

   たとえば:

   - **3.0.x Web インタフェースで、「System Management Access」->「SNMP」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」->「SNMP」をクリックします。**

2. **「SNMP」ページで SNMP プロパティーを表示または変更し、「Save」をクリックして変更を適用します。**

   詳しい手順については、この手順の「関連情報」セクションに一覧されているドキュメントを参照してください。ファームウェアバージョン 3.2 以降を実行しているユーザーは、「SNMP」ページの「`More details`」リンクをクリックして詳細を参照してください。

関連情報

- 「SNMP 設定の構成」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「SNMP 設定の構成」、『*Oracle ILOM SNMP および IPMI 用プロトコル管理リファレンス (ファームウェア 3.2.x)*』
- 「SNMP 設定の構成」、『*Oracle ILOM 3.1 SNMP、IPMI、CIM、WS-Man 管理プロトコルリファレンスガイド*』
- 「SNMP 設定の構成」、『*Oracle ILOM 3.0 管理プロトコルリファレンスガイド SNMP、IPMI、WS-Man、CIM*』

Sun SNMP MIB でサポートされる構成可能オブジェクト

構成可能なオブジェクトをサポートし、「セット」が適用可能な Oracle の Sun MIB は次のとおりです。

- `SUN-HW-CTRL-MIB` – この MIB は、電源管理ポリシーなど、ハードウェアポリシーを構成するときに使用します。
- `SUN-ILOM-CONTROL-MIB` – この MIB は、ユーザーの作成やサービスの構成など、Oracle ILOM 機能を構成するときに使用します。

注記 - MIB オブジェクトは次の場合に設定できます。1) MIB オブジェクトが変更をサポートしている。2) MIB オブジェクトの `MAX-ACCESS` 要素が `read-write` に設定されている。3) セットの実行を試みるユーザーがそのことを許可されている。

最大限のセキュリティーを得るための IPMI 管理アクセスの構成

最大限のセキュリティーを得るための Oracle ILOM IPMI 管理アクセスの最適な構成方法については、次のトピックを参照してください。

- 49 ページの「拡張認証とパケット暗号化に IPMI v2.0 を使用する」
- 51 ページの「IPMI のセキュリティーガイドラインとベストプラクティス」
- 51 ページの「IPMI 2.0 認証の暗号スイートのサポート」

▼ 拡張認証とパケット暗号化に IPMI v2.0 を使用する

Oracle ILOM はリモート管理で IPMI v1.5 と v2.0 の両方がサポートされますが、Oracle サーバーを安全に管理するため、システム管理者は常に IPMI v2.0 -I lanplus インタフェースを使用する必要があります。IPMI バージョン 2.0 の時点で、-I lanplus インタフェースは、拡張された認証チェックとデータ統合チェックを提供します。

ファームウェアリリース 3.2.4 以降、Oracle ILOM には IPMI v1.5 セッションの有効化と無効化のための構成可能プロパティーが用意されています。高いセキュリティーを確保するため、デフォルトで IPMI v1.5 プロパティーは無効にされています。IPMI v1.5 プロパティーを無効にすると、Oracle ILOM へのすべての IPMI v1.5 セッション接続が拒否されます (ブロックされます)。

IPMI プロパティーサービスの State または、構成可能な IPMI v1.5 プロパティー (ファームウェアリリース 3.2.4 以降で利用可能) を表示または変更するには、次の手順を参照してください。

始める前に

- Oracle ILOM で IPMI プロパティーを変更するには Admin (a) の役割が必要です。
- IPMI サービスの State プロパティーはデフォルトで有効になっています。使用前に、IPMI 管理機能を実行できる適切な役割ベース権限 (Administrator、Operator) を持つユーザーアカウントを Oracle ILOM で構成しておく必要があります。
- Oracle ILOM ファームウェア 3.2.4 以降を実行している SP では、IPMI v2.0 管理セッションはサポートされていますが、IPMI v1.5 管理セッションはデフォルトでサポートされません。IPMI v1.5 プロパティーは Oracle ILOM で構成可能です。

注記 - Oracle ILOM で IPMI v1.5 セッションを無効にしている場合、IPMItool を使用するユーザーは IPMI 2.0 -I lanplus オプションを使用する必要があります。

- Oracle ILOM ファームウェアリリース 3.2.3 以前を実行している SP では、IPMI v2.0 および v1.5 管理セッションが Oracle ILOM でサポートされます。IPMI v1.5 プロパティーは Oracle ILOM で構成できません。

注記 - IPMI v1.5 セッションは拡張認証とパケット暗号化をサポートしていません。拡張認証と IPMI パケット暗号化を使用するには、IPMI v2.0 を使用する必要があります。

---

1. **Oracle ILOM Web インタフェースで「IPMI」ページに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「Configuration」->「System Management Access」->「IPMI」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Management Access」->「IPMI」をクリックします。**

2. **「IPMI」ページで、適切な IPMI プロパティーを表示または構成し、「Save」をクリックして変更を適用します。**

IPMI 構成の詳細な手順については、次の「関連情報」セクションに記載されている適切なドキュメントを参照してください。

関連情報

- 「IPMI を使用したサーバー管理」、『*Oracle ILOM SNMP および IPMI 用プロトコル管理リファレンス (ファームウェア 3.2.x)*』
- 「IPMI を使用したサーバー管理」、『*Oracle ILOM 3.1 SNMP、IPMI、CIM、WS-MAN プロトコル管理リファレンスガイド*』
- 「IPMI を使用したサーバー管理」、『*Oracle ILOM 3.0 管理プロトコルリファレンスガイド SNMP、IPMI、WS-MAN、CIM*』
- 51 ページの「IPMI のセキュリティーガイドラインとベストプラクティス」
- 51 ページの「IPMI 2.0 認証の暗号スイートのサポート」

IPMI のセキュリティーガイドラインとベストプラクティス

確立された IPMI システム管理セッションをセキュアなものにし、サイバー攻撃に対する脆弱性をなくすには、システム管理者は次のことを行うべきです。

- 決して IPMI Version 1.5 (`-I lan` IPMItool インタフェース) を使用して IPMI リモート管理セッションを確立しないでください。IPMItool (`-I lanplus` IPMItool インタフェース) などのコマンド行ユーティリティーを使用している場合は、明示的に IPMI バージョン 2.0 を使用するようにしてください。
- IPMI パスワードを定期的に変更します。Oracle ILOM ユーザーアカウントのライフサイクルは適切に管理してください。

  詳細は、24 ページの「Oracle ILOM ユーザーアクセスのセキュリティー保護」を参照してください。
- 外部からのネットワークアクセスを制限します。専用の Ethernet 管理チャネルを使用して、Oracle ILOM と通信します。

  詳細は、15 ページの「物理管理接続のセキュリティー保護」を参照してください。
- IT セキュリティー責任者と協力して、サーバー管理と IPMI セキュリティーに関する一連のベストプラクティスとポリシーを作成します。

IPMI 2.0 認証の暗号スイートのサポート

IPMI Version 2.0 での認証チェック、機密性チェック、および整合性チェックは、暗号スイートによってサポートされます。これらの暗号スイートは、IPMI 2.0 仕様で説明されている RMCP + 認証済み鍵交換プロトコルを使用します。

Oracle ILOM は、クライアントとサーバーとの間のセキュアな IPMI 2.0 セッションを確立するために、次の暗号スイート鍵アルゴリズムをサポートします。

- **暗号スイート 2** – 暗号スイート 2 は、認証と整合性の両方のアルゴリズムを使用します。

- **暗号スイート 3** – 暗号スイート 3 は、認証、機密性、および整合性の 3 つのアルゴリズムすべてを使用します。

注記 - すべての IPMI 2.0 トラフィックが確実に暗号化されるように、Oracle ILOM は、IPMI 2.0 暗号タイプ 0 (非暗号化操作モード) のサポートを実装していません。

最大限のセキュリティーを得るための WS-Management アクセスの構成

ファームウェアリリース 3.0.8 以降ファームウェア 3.1.2 まででは、Oracle ILOM には標準的な Web サービスインタフェースが用意されており、サーバーの健全性をモニターしたり、Ws-Management (Ws-Man) というプロトコルを使用してインベントリ情報を確認できます。

Oracle ILOM Ws-Man インタフェースを使用すると、ホストのピア制御や Oracle ILOM SP 自身のリセットも行えます。Ws-Man は、HTTP(S) プロトコルを利用した、SOAP (Simple Object Access Protocol) ベースのプロトコルです。Oracle ILOM Ws-Man インタフェースでは、HTTP または HTTPS のどちらかをトランスポートとして使用できます。HTTPS を使用すると、チャネルが SSL 証明書を使用して暗号化されます。SSL 証明書を使用することのセキュリティー上の利点および自己署名証明書と信頼できる証明書の違いの詳細は、37 ページの「信頼できる SSL 証明書および非公開鍵の使用によるセキュリティーの向上」を参照してください。

この Web サービスインタフェースは、SSL 証明書を使用している場合にだけ使用してください。最大限のセキュリティーを実現するために、トランスポートメカニズムとして HTTPS を使用してください。Web サーバープロパティーの構成の詳細は、37 ページの「最大限のセキュリティーを得るための Web インタフェースの構成」を参照してください。

Oracle ILOM のための配備後のセキュリティーベストプラクティス

サーバー配備後に最適な Oracle ILOM セキュリティープラクティスを判断するには、次のトピックを使用します。

関連情報

- 「Oracle ILOM のための配備時のセキュリティーベストプラクティス 」
- 「Oracle ILOM セキュリティーベストプラクティスのチェックリスト」

セキュアな管理接続の維持

Oracle ILOM へのセキュアな管理接続を維持するため、次の内容について検討します。

認証されていないホスト KCS デバイスアクセスの回避

Oracle サーバーはホストと Oracle ILOM 間でキーボードコントローラスタイル (KCS) インタフェースと呼ばれる標準の低速接続をサポートしています。サポートされているこの KCS インタフェースは、Intelligent Platform Management Interface (IPMI) Version 2.0 仕様と完全互換であり、無効にできません。

KCS デバイスアクセスはホストから Oracle ILOM を構成する際に便利ですが、物理 KCS デバイスに対するカーネルまたはドライバレベルのアクセス権を保有するオペレーティングシステムユーザーが認証なしで Oracle ILOM 設定を変更できることから、このタイプのアクセスにはセキュリティーリスクが伴います。通常、KCS デバイスにアクセスできるのは、`root` ユーザーまたは管理者ユーザーだけです。ただし、大半のオペレーティングシステムは、KCS デバイスに対するアクセス権をより広範なユーザーに与えるように構成できます。

たとえば、KCS アクセス権を持つオペレーティングシステムユーザーは次を実行できます。

- Oracle ILOM ユーザーを追加または作成する。
- ユーザーパスワードを変更する。
- ILOM 管理者として Oracle ILOM CLI にアクセスする。
- ログおよびハードウェア情報にアクセスする。

デバイスは通常、Linux または Oracle Solaris 上では `/dev/kcs0` または `/dev/bmc`、Microsoft Windows 上では `ipmidrv.sys` または `imbdrv.sys` と呼ばれています。このデバイス (Baseboard Management Controller (BMC) ドライバまたは IPMI ドライバともいう) へのアクセスは、ホストオペレーティングシステムの一部である適切なアクセス制御メカニズムを用いて慎重に管理する必要があります。

ホスト IPMI KCS デバイスを使用して Oracle ILOM 設定を構成する方法の代替として、Oracle ILOM 相互接続インタフェースを利用する方法があります。詳細は、54 ページの「推奨される認証済みホスト相互接続アクセス」を参照してください。

KCS デバイスなどのハードウェアデバイスへのアクセスを制御または保護する方法の詳細は、ホストオペレーティングシステムに付属しているドキュメントを参照してください。

推奨される認証済みホスト相互接続アクセス

KCS インタフェースに替わる高速なインタフェースとして、ホストオペレーティングシステム上で動作するクライアントは、内蔵の高速相互接続を介して Oracle ILOM と通信できます。この相互接続は、内蔵の Ethernet-over-USB 接続によって実装されており、IP スタックを実行します。Oracle ILOM にはルーティングされない IP アドレスが内部的に与えられ、ホスト上のクライアントはこのアドレスを使用して Oracle ILOM に接続できます。

ハードウェアデバイスに対する保護されたアクセスに依存している KCS インタフェースと違って、LAN 相互接続は、デフォルトでは、すべてのオペレーティングシステムユーザーが使用できます。したがって、LAN 相互接続を介して Oracle ILOM に接続するには認証が必要になりますが、これはちょうど、接続がネットワーク経由で Oracle ILOM 管理ポートに対して送られてくる場合と同じです。

また、管理ネットワーク上で公開されているサービスまたはプロトコルはすべて、LAN 相互接続を介してホストから利用できます。ホスト上の Web ブラウザを使用して Oracle ILOM Web インタフェースにアクセスしたり、Secure Shell クライアントを使用して Oracle ILOM コマンド行インタフェースに接続することができます。どのようなケースであれ、LAN 相互接続を使用するには、有効なユーザー名とパスワードを入力する必要があります。

LAN 相互接続はデフォルトでは無効になっています。LAN 相互接続が無効になっていると、Ethernet デバイスはホストオペレーティングシステムから見えなくなり、チャネルも存在しません。Oracle Hardware Management Pack を使用すると、LAN 相互接続のプロビジョニングと構成が容易になります。

セキュアな専用ホスト相互接続を介した Oracle ILOM の管理の詳細は、次のいずれかを参照してください。

- ファームウェアリリース 3.2 以降の場合、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』の「専用の相互接続 SP 管理接続」を参照してください
- ファームウェアリリース 3.1.x の場合は、『*Oracle ILOM 3.1 構成および保守ガイド*』の「専用の相互接続 SP 管理接続」を参照してください
- ファームウェアリリース 3.0.12 - 3.0.16 の場合は、*Oracle ILOM 3.0 Web 手順ガイド*のローカルホスト相互接続の構成に関する項を参照してください。

チャネルのセキュリティー保護のための IPMI 2.0 暗号化の使用

Intelligent Platform Management Interface (IPMI) Version 2.0 は、Remote Management and Control Protocol+ (RMCP+) と呼ばれる暗号化されたネットワークプロトコルをサポートしています。このプロトコルは、対称鍵ベースのチャレンジ応答メカニズムを使用してチャネルを暗号化します。このメカニズムによって、機密データが暗号化されないままネットワーク上を送信されることがなくなり、トラフィックを暗号化および復号化するにはユーザーパスワードが必要になります。すべての IPMI 2.0 トラフィックが確実に暗号化されるように、Oracle ILOM は、IPMI 2.0 暗号タイプ 0 (非暗号化) 操作モードのサポートを実装していません。

IPMItool の場合は、`-I lanplus` フラグを使用して、暗号化された RMCP+ セッションを確立する必要があることを示します。

詳細は、`ipmitool` のドキュメントを参照してください。

注記 - ファームウェアリリース 3.2.4 以降、Oracle ILOM には IPMI v1.5 用の構成可能プロパティーが用意されています。デフォルトで、IPMI 1.5 プロパティーは無効になっています。詳細は、49 ページの「拡張認証とパケット暗号化に IPMI v2.0 を使用する」を参照してください。

リモート管理のためのセキュアプロトコルの使用

Oracle ILOM は、多数のさまざまなリモート管理プロトコルをサポートしています。同じプロトコルの暗号化バージョンと非暗号化バージョンの両方がサポートされている場合もあります。セキュリティー上の理由から、可能なかぎり、利用できるプロトコルの中でもっともセキュアなもの

を使用する必要があります。サポートされている暗号化および非暗号化プロトコルの一覧は、次の表を参照してください。

表 9 サポートされているセキュアなプロトコル

カテゴリ	セキュア/暗号化	非暗号化
Web ブラウザアクセス	HTTPS	HTTP
コマンド行アクセス	SSH	未サポート
IPMI アクセス	IPMI v2.0	IPMI v1.5
プロトコルアクセス	SNMPv3	SNMPv1/v2c

セキュアで信頼されているネットワーク管理接続の確立

Oracle ILOM が組み込まれているすべての Oracle サーバーには、ネットワーク経由で Oracle ILOM に接続するために使用される専用の管理用ポートが用意されています。この専用の管理用ポートを使用して、セキュアな管理用プライベートネットワークが提供されます。一部のシステムでサポートされているサイドバンド管理では、標準のサーバーデータポート上でホストと Oracle ILOM の両方にアクセスできます。サイドバンド管理を使用すると、2 つの別個のネットワーク接続の必要がなくなるため、ケーブル管理とネットワーク構成が簡素化されます。ただし、専用の管理ポートまたはサイドバンド管理ポートが信頼できるネットワークに接続されていない場合、Oracle ILOM トラフィックが信頼できないネットワークを介して送信される可能性があることも意味します。

Oracle ILOM でもっとも信頼できるセキュアな環境を維持するには、サーバーの専用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を常に信頼できる内部ネットワークまたはセキュアな専用管理/プライベートネットワークに接続する必要があります。

セキュアなローカルシリアル管理接続の確立

サーバーにある物理シリアル管理ポートを使用すると、端末サーバーまたはダンプ端末を Oracle ILOM にローカルで接続できます。Oracle ILOM へのセキュアなローカル管理接続を維持するには、端末デバイスが内部ネットワークまたはプライベートネットワークにも接続されている場合、そのデバイスをローカルのシリアル管理ポートに接続することは避けてください。

リモート KVMS のセキュアな使用法

Oracle ILOM は、ホストサーバーのキーボード、ビデオ、マウスをリモートクライアントにリモートでリダイレクトする機能、およびリモートストレージをマウントする機能を備えています。これらの機能をまとめてリモート KVMS と呼びます。リモート KVMS を使用すると、クライアントマシン上で Oracle ILOM リモートコンソール、リモートコンソールプラス、および CLI ストレージリダイ

レクションという Java アプリケーションを実行することにより、サーバー上にホストオペレーティングシステムのグラフィカルコンソールを表示できます。

リモート KVMS セッションとシリアルのテキストベースのセッションが Oracle ILOM からセキュアに起動されるようにするには、次について検討します。

- 57 ページの「KVMS リモート通信と暗号化」
- 57 ページの「リモート KVMS 共有アクセスから保護する」
- 58 ページの「ホストシリアルコンソールの共有アクセスに対する保護」

KVMS リモート通信と暗号化

Oracle ILOM リモートシステムコンソール、リモートシステムコンソールプラス、および CLI ストレージリダイレクションの各アプリケーションは、一連のネットワークプロトコルを使用してリモートで Oracle ILOM と通信します。これらの Java アプリケーションを使用して、ホストのキーボードとマウスを制御したり、ローカルのストレージデバイス (CD ドライブや DVD ドライブなど) をリモートサーバーにマウントしたりできます。

次の表に、リモート KVMS 情報がネットワーク経由で伝送される方法を詳細に示します。

表 10 KVMS 機能と暗号化

KVMS の機能	暗号化または暗号化なし	説明
マウスリダイレクション	暗号化	マウスの座標がネットワーク経由で Oracle ILOM にセキュアに送信されます。
キーボードリダイレクション	暗号化	クライアントマシン上で入力した文字がすべて、暗号化プロトコルを使用して、Oracle ILOM に転送されます。
ビデオリダイレクション	暗号化	ビデオデータが、Java クライアントと Oracle ILOM の間で暗号化プロトコルを使用して転送されます。
ストレージリダイレクション	暗号化なし	ストレージデバイスに対するデータの読み取りと書き込みが、暗号化されずにネットワーク経由で Oracle ILOM に伝送されます。

リモート KVMS で有効になるネットワークポートの一覧については、表4「デフォルトで有効になるサービスとポート」を参照してください。

リモート KVMS 共有アクセスから保護する

リモート KVMS ビデオコンソールは、そのサーバーに接続された物理モニターに表示される内容をリダイレクトします。複数のリモートクライアントが Oracle ILOM との KVMS セッションを確立できますが、通常、1 台のサーバーにはビデオ出力が 1 つしかないため、各セッションでは同一のビデオが表示されます。

同様に、あるリモート KVMS セッションで画面に入力した内容はすべて、同じマシンに接続しているほかの KVMS ユーザーにも見えます。なにより重要なのは、あるユーザーが、Oracle ILOM リモートコンソール、リモートコンソールプラス、または CLI ストレージリダイレクションアプリケーション内のホストオペレーティングシステムに特権ユーザーとしてログインした場合、ほかのすべての KVMS ユーザーは、その認証されたセッションを共有できるという点です。したがって、リモート KVMS 機能は共有接続を許可するという点を理解しておくことが重要です。

リモート KVMS リダイレクションセッションの終了後にアイドル状態になった認証済みオペレーティングシステムセッションをセキュリティー保護するには、次を実行する必要があります。

- リモート KVMS リダイレクションセッションの終了時にホストオペレーティングシステムを自動ロックするように、Oracle ILOM を構成します。

  手順は、33 ページの「KVMS セッションの終了時にホストアクセスをロックする」を参照してください。
- ホストオペレーティングシステムでタイムアウト間隔を設定し、無人の認証済みユーザーセッションが自動的に閉じられるようにします。

  手順は、ホストオペレーティングシステムのユーザードキュメントを参照してください。

Oracle ILOM リモートシステムコンソールプラスを使用している場合で、Oracle ILOM から起動される KVMS セッションの表示可能数を制限するには、34 ページの「リモートシステムコンソールプラスで表示できる KVMS セッションを制限する (3.2.4 以降)」を参照してください。

ホストシリアルコンソールの共有アクセスに対する保護

大半のオペレーティングシステムのホストコンソールはテキストベースのシリアルコンソールを使用しても利用できます。このコンソールを使用可能にするには、Oracle ILOM CLI のコマンド行で `start /HOST/console` コマンドを実行します。グラフィカルコンソールと同様、シリアルコンソールは、すべての Oracle ILOM ユーザーに対して 1 台のみ使用可能です。したがって、これは共有リソースとみなされます。あるユーザーがシリアルコンソールからホストオペレーティングシステムにログインしたあと、ログアウトせずにコンソールリダイレクションを終了した場合、シリアルコンソールの 2 番目のユーザーは以前に認証済みのオペレーティングシステムセッションにアクセスできます。

Oracle ILOM は、コンソールリダイレクションセッションが終了すると、ホストオペレーティングシステムにデータ転送リクエスト (DTR) 信号を送信します。多くのオペレーティングシステムは、この信号を受信すると、ユーザーを自動的にログアウトさせます。ただし、すべてのオペレーティングシステムがこの機能をサポートしているわけではありません。

- Oracle Linux 5 は、DTR 信号をサポートしており、デフォルトで有効になっています。
- Oracle Linux 6 は、DTR をサポートしていますが、手動で有効にする必要があります。
- Oracle Solaris は DTR 信号をサポートしていません。セキュリティー上のリスクを軽減するため、ユーザーはホストオペレーティングシステムでセッションタイムアウトを構成できます。

ホストシリアルリダイレクションセッションの終了後にアイドル状態になった認証済みオペレーティングシステムセッションを保護するためのガイドラインについては、次を参照してください。

- ホストオペレーティングシステムで DTR 信号機能がサポートされているかどうかを確認し、サポートされている場合は、この機能がデフォルトで有効になっているかどうかを確認します。

  DTR 信号については、使用しているホストオペレーティングシステムのユーザードキュメントを参照してください。
- ホストオペレーティングシステムでセッションタイムアウト間隔を構成します。

  ホストオペレーティングシステムでセッションタイムアウト間隔を設定する方法については、使用しているホストオペレーティングシステムのユーザードキュメントを参照してください。
- ユーザーがリモートのシリアルホストコンソールを無人の状態にして離れることがないようにするためのセキュリティーポリシーを実装します。ユーザーは、セッションが使用中でない場合、常にすべてのリモートホストコンソールセッションからログアウトするべきです。

ユーザーアクセスをセキュリティー保護するための配備後の考慮事項

セキュアなユーザーアクセスが維持されるようにするために、次の点を考慮してください。

- 59 ページの「パスワード管理の適用」
- 60 ページの「root アカウントのデフォルトパスワードをリセットする際の物理的セキュリティープレゼンス」
- 62 ページの「監査イベントのモニタリングによる不正アクセスの検出」

パスワード管理の適用

すべての Oracle ILOM パスワードは定期的に変更してください。これにより、悪意のあるアクティビティーを防ぎ、最新のパスワードポリシーに準拠した状態が保たれます。

通常はユーザー自身がパスワードを変更しますが、ユーザー管理権限を持つシステム管理者がほかのユーザーアカウントに関連付けられているパスワードを変更することも可能です。

Oracle ILOM ユーザーアカウントに関連付けられているパスワードを変更するには、次の Web ベースの手順を参照してください。

注記 - CLI の手順またはユーザー管理構成プロパティーの詳細は、次の手順にある「関連情報」セクションに記載されているドキュメントを参照してください。

▼ ローカルユーザーアカウントのパスワードを変更する

始める前に

- 26 ページの「ユーザーアカウントとパスワードの管理のセキュリティーガイドライン」について確認します。

- 自分以外のユーザーアカウントに関連付けられているパスワードまたは権限を変更するには User Management (u) の役割が必要です。
- Operator (o) の役割を持つユーザーは自分自身のアカウントのパスワードを変更できます。

1. **Oracle ILOM Web インタフェースで、「User Account」ページに移動します。**
   たとえば:
   - **3.0.x Web インタフェースで、「User Management」->「User Accounts」をクリックします。**
   - **3.1 以降の Web インタフェースで、「User Management」->「User Accounts」をクリックします。**
2. **「User Account」ページで、変更するアカウントの「Edit」をクリックします。**
   「Edit: User Name」ダイアログが表示されます。
3. **「Edit: User Name」ダイアログで次を実行します。**
   - **「New Password」テキストボックスに一意のパスワードを入力し、「Confirm New Password」テキストボックスに同じパスワードを再入力します。**
   - **「Save」をクリックして変更を適用します。**

関連情報

- 29 ページの「すべてのローカルユーザーのパスワードポリシー制限を設定する (3.2.5 以降)」
- 「ローカルユーザーアカウントの構成」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』
- 「ローカルユーザーアカウントの構成」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- ユーザーアカウントの変更、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - CLI 手順ガイド*』
- 「ユーザーアカウントを変更する」、『*Oracle Integrated Lights Out Manager (ILOM) 3.0 日常的な管理 - Web 手順ガイド*』

root アカウントのデフォルトパスワードをリセットする際の物理的セキュリティープレゼンス

Oracle ILOM の root ユーザーのパスワードをなくした場合は、パスワードをリセットできます。root パスワードをリセットするには、シリアルポート経由で Oracle ILOM に接続します。ほ

とんどの場合、Oracle ILOM シリアルポートに接続するには、システムに物理的にアクセスする必要がありますが、シリアルコンソールは端末サーバーに接続できます。端末サーバーは事実上、物理シリアルポートへのネットワークアクセスを可能にします。

端末サーバー使用時に、root パスワードをネットワーク経由でリセットできないようにするため、大半のサーバーは物理的プレゼンスチェック機能を備えています。これには、サーバーへの物理的なアクセスを証明する手段としてサーバーのボタンを押す必要があります。最大限のセキュリティーを実現するため、Oracle ILOM シリアルポートが端末サーバーに接続されているときは常に、プレゼンスチェック機能が有効になっていることを確認してください。

物理的プレゼンスチェック機能を表示または変更するには、次の Web ベースの手順を参照してください。

注記 - CLI の手順または root アカウントプロパティーの詳細は、次の手順にある「関連情報」セクションに記載されているドキュメントを参照してください。

▼ 物理的プレゼンスチェックの設定

始める前に

- Oracle ILOM の物理的プレゼンスチェックモードはデフォルトで有効になっています。
- ファームウェアバージョン 3.1 以降では、Oracle ILOM で物理的プレゼンスチェックモードを使用する必要があります。

1. **Oracle ILOM Web インタフェースで、「ILOM Administration」->「Identification」をクリックします**
2. **「Identification」ページで、「Physical Presence Check」プロパティーに移動し、次のいずれかを実行します。**

   - **「Physical Presence」チェックボックスにチェックマークを付けて有効にします。有効の場合、デフォルトの Oracle ILOM パスワードを復元するには物理システムの「Locator」ボタンを押す必要があります。**

     - または -

   - **「Physical Presence」チェックボックスのチェックマークを外して無効にします。無効の場合、デフォルトの Oracle ILOM 管理者 root パスワードは、物理システムの「Locator」ボタンを押すことなくリセットできます。**

3. **「Save」をクリックして変更を適用します。**

関連情報

- 「デバイス識別の構成プロパティー」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』。

- 「デバイス識別の構成プロパティー」、『*Oracle ILOM 3.1 構成および保守ガイド*』
- 「`root` アカウントのパスワードの復元」、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』。
- 「`root` アカウントのパスワードの復旧」、『*Oracle ILOM 3.1 構成および保守ガイド*』

監査イベントのモニタリングによる不正アクセスの検出

Oracle ILOM の監査ログには、ログインと構成変更がすべて記録されます。監査ログの各エントリでは、ユーザーとタイムスタンプがイベントに関連付けられています。監査イベントは、変更を追跡したり、Oracle ILOM に対して無許可の変更や無許可のアクセスが行われたかどうかを判別するために便利なツールです。

Oracle ILOM 監査ログのイベントを表示するには、次の Web ベースの手順を参照してください。

注記 - CLI の手順または監査ログの詳細は、次の手順にある「関連情報」セクションに記載されているドキュメントを参照してください。

▼ 監査ログを表示する

始める前に

- 監査ログはファームウェアリリース 3.1 時点の Oracle ILOM で使用可能になりました。ファームウェアリリース 3.1 より前のリリースでは、監査ログは Oracle ILOM のイベントログに捕捉されていました。
- 監査ログのエントリをクリアするには、Oracle ILOM で Admin (a) の役割権限が必要です。

1. **Web インタフェースで、「ILOM Administration」->「Logs」->「Audit」をクリックします。**
2. **「Audit log」ページで、ログエントリをフィルタするコントロールを使用するか、ログ内のイベントをクリアするコントロールを使用します。**

   ファームウェアバージョン 3.2 以降を実行しているユーザーは、「Audit」ページの「`More details`」リンクをクリックして詳細を参照してください。

関連情報

- 「Oracle ILOM のログエントリの管理」、『*Oracle ILOM システムモニタリングおよび診断用ユーザーズガイド (ファームウェアリリース 3.2.x)*』
- 「Oracle ILOM のログエントリの管理」、『*Oracle ILOM 3.1 ユーザーズガイド*』

FIPS モードを変更するための配備後のアクション

ファームウェアリリース 3.2.4 の時点では、Oracle ILOM には FIPS レベル 1 準拠のための構成可能なプロパティーが用意されています。デフォルトでは、このプロパティーは無効の状態で出荷されます。Oracle ILOM で FIPS 準拠の動作ステータスを変更すると、ユーザー定義のすべての構成プロパティーが出荷時のデフォルト設定にリセットされます。Oracle ILOM でのユーザー定義の構成設定が失われないようにするために、ほかの Oracle ILOM 設定を構成する前に FIPS 準拠を変更するようにしてください。Oracle ILOM の構成の配備後に FIPS 準拠を変更する必要がある場合は、ユーザー定義の設定が失われないようにするために、次の手順を参照してください。

注記 - Oracle は、システムの機密データまたは重要なデータを保護するために、FIPS 140-2 セキュリティー標準に準拠した暗号化アルゴリズムを使用します。

▼ 配備後に FIPS モードを変更する

ファームウェアの更新を実行するか、または Oracle ILOM でユーザー定義の構成プロパティーを指定したあとに FIPS モードの動作状態を変更する必要がある場合は、この手順を使用します。

注記 - Oracle ILOM の FIPS 準拠モードは、「State」および「Status」プロパティーによって表されます。「State」プロパティーは Oracle ILOM で構成されているモードを表し、「Status」プロパティーは Oracle ILOM の動作モードを表します。FIPS の「State」プロパティーが変更された場合、その変更は、次回の Oracle ILOM のリブートまで動作モード (FIPS の「Status」プロパティー) に影響を与えません。

始める前に

- FIPS レベル 1 準拠のための構成可能なプロパティーは、ファームウェア 3.2.4 以降の Oracle ILOM で使用できます。ファームウェアリリース 3.2.4 より前では、Oracle ILOM は FIPS レベル 1 準拠のための構成可能なプロパティーを提供していません。
- FIPS が有効になっている (構成され、動作可能になっている) と、Oracle ILOM の一部の機能がサポートされません。FIPS が有効になっているときにサポートされない機能の一覧については、18 ページの「FIPS モードが有効の時にサポートされない機能」を参照してください。
- この手順を実行するには、Admin (a) の役割が必要です。

1. **Oracle ILOM Web インタフェースで、Oracle ILOM 構成をバックアップします。**
   たとえば:

   a. **「ILOM Administration」->「Configuration Management」->「Backup/Restore」をクリックします。**

b. 「Backup/Restore」ページで「More details...」リンクをクリックし、詳細手順を確認します。

注記 - ファームウェア更新後の Oracle ILOM への再接続を簡素化するには、構成を維持するファームウェア更新オプションを有効にする必要があります。

注記 - 手順 1 の前に手順 2 を実行した場合、XML バックアップ構成ファイルを編集して、FIPS 設定を削除する必要があります。そうしないと、バックアップの Oracle ILOM XML ファイルとサーバーで実行している動作 FIPS モードの状態の間で構成の不一致が発生することになり、この状況は許可されません。

---

2. ファームウェア更新が必要な場合は、次の手順を実行します。

   a. 「ILOM Administration」->「Maintenance」->「Firmware Update」をクリックします。

   b. 「Firmware Update」ページで「More details...」リンクをクリックし、詳細手順を確認します。

3. Oracle ILOM で次のように FIPS 準拠モードを変更します。

   a. 「ILOM Administration」->「Management Access」->「FIPS」をクリックします。

   b. 「FIPS」ページで「`More details`」リンクをクリックし、次を実行するための手順を確認します。

      - FIPS State 構成を変更します。
      - SP をリセットし、システム上の FIPS 動作ステータスを更新します。

4. バックアップした Oracle ILOM 構成を次のように復元します。

   a. 「ILOM Administration」->「Configuration Management」->「Backup/Restore」をクリックします。

   b. 「Backup/Restore」ページで「`More details`」リンクをクリックし、詳細手順を確認します。

関連情報

- 16 ページの「配備時に FIPS モードを構成するかどうかの選択」
- 18 ページの「FIPS モードが有効の時にサポートされない機能」
- FIPS モードプロパティーの構成、『*Oracle ILOM 構成および保守用管理者ガイド (3.2.x)*』

最新ソフトウェアおよびファームウェアのアップデート

サーバー上のソフトウェアとファームウェアを最新のバージョンに保ちます。

- My Oracle Support に掲載される更新を定期的に確認します。
- サーバーで使用可能な最新リリースバージョンのソフトウェアまたはファームウェアを常にインストールし、バグ修正や機能拡張を利用します。
- インストールされているすべての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ます。

サーバーの Oracle ILOM ファームウェアを更新するには、次の手順を参照してください。

▼ Oracle ILOM ファームウェアを更新する

始める前に

- Oracle ILOM ファームウェアを更新するには、Oracle ILOM で Admin (a) の役割が必要です。
- すべての Oracle ILOM ユーザーにファームウェア更新のスケジュールを通知し、ファームウェア更新が完了するまですべてのクライアントセッションを閉じるように求めます。
- ファームウェア更新プロセスには数分かかり、この間はほかの Oracle ILOM タスクは実行しないようにしてください。

1. **サーバーで使用可能な最新のソフトウェア更新を My Oracle Support (MOS) Web サイトからダウンロードします。**
   必要であれば、サーバーに付属しているドキュメントを参照し、MOS からソフトウェア更新を入手する手順を確認します。

   注記 - サーバーで使用可能な最新の Oracle ILOM ファームウェアバージョンは、MOS に掲載されるサーバー用の最新ソフトウェアパッチに含まれています。

2. **ファームウェアイメージをローカルまたはネットワーク共有ドライブに保存します。**

3. **Web インタフェースで「Firmware Update」ページに移動します。**
   たとえば:

   - **3.0.x Web インタフェースで、「Maintenance」->「Firmware」をクリックします。**
   - **3.1 以降の Web インタフェースで、「ILOM Administration」->「Maintenance」->「Firmware Upgrade」をクリックします。**

4. **「Firmware Upgrade」ページで、「Enter Firmware Upgrade mode」をクリックし、プロンプトに従います。**

Oracle ILOM ファームウェア 3.2 以降を実行しているユーザーは、「Firmware Upgrade」ページで「`More details`」リンクをクリックします。