

Oracle® Integrated Lights Out Manager (ILOM) 3.0

入門ガイド



Part No. 820-7382-11
2010 年 11 月、Revision A

Copyright © 2008, 2010, 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。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 RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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したこと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 と 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。

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。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。UNIX は X/Open Company, Ltd. からライセンスされている登録商標です。

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。



リサイクル
してください



Adobe PostScript

目次

このマニュアルの使用方法	vii
ILOM の使用を開始する	1
このガイドについて	2
ILOM の使用開始プロセス	2
ILOM へのシステムの接続	5
接続の要件	5
Web インタフェースまたは CLI の使用	6
root アカウントの使用	7
1. Web インタフェースを使用した ILOM の初期セットアップ手順	9
Web インタフェースを使用した ILOM への初回ログイン	10
▼ root ユーザーアカウントを使用して ILOM にログインする	10
IPv4 と IPv6 のネットワーク環境の設定	12
▼ Web インタフェースを使用して IPv4 と IPv6 の設定を構成する	12
ユーザーアカウントの追加またはディレクトリサービスの設定	15
▼ ユーザーアカウントを追加して権限を割り当てる	16
▼ Active Directory 用の ILOM の設定	18
▼ LDAP サーバーを設定する	23
▼ LDAP 用の ILOM の設定	24
▼ LDAP/SSL 用に ILOM を設定する	26

- ▼ LDAP/SSL テーブルを編集する 29
- ▼ RADIUS 用の ILOM の設定 30
- ▼ 新しいユーザーアカウントを使用して ILOM にログインする 31
- ▼ ILOM からログアウトする 32

次の手順 32

2. ILOM CLI を使用した ILOM の初期セットアップ手順 33

CLI を使用した ILOM への初回ログイン 34

- ▼ root ユーザーアカウントを使用して ILOM にログインする 34

IPv4 と IPv6 のネットワーク環境の設定 35

- ▼ CLI を使用して IPv4 と IPv6 の設定を構成する 35

ユーザーアカウントの追加またはディレクトリサービスの設定 40

- ▼ ユーザーアカウントを追加して権限を割り当てる 40

- ▼ Active Directory 用の ILOM の設定 41

- ▼ LDAP 用に ILOM を設定する 45

- ▼ LDAP/SSL 用に ILOM を設定する 45

- ▼ RADIUS 用の ILOM の設定 49

- ▼ 新しいユーザーアカウントを使用して ILOM にログインする 50

- ▼ ILOM からログアウトする 51

次の手順 51

3. ILOM ファームウェア 53

ILOM バージョン情報の識別 54

- ▼ Web インタフェースを使用して ILOM のバージョンを識別する 54

- ▼ CLI を使用して ILOM のバージョンを識別する 54

ILOM ファームウェアの最新バージョンへの更新 55

インストールを開始する前に 55

- ▼ Web インタフェースを使用して ILOM ファームウェアを更新する 56

- ▼ CLI を使用して ILOM ファームウェアを更新する 58

このマニュアルの使用法

この入門ガイドでは、使用しているシステムで Oracle Integrated Lights Out Manager (ILOM) 3.0 ファームウェアにはじめてアクセスするために必要な手順を実行する方法を説明します。

説明する手順には、ILOM へのログイン、ネットワーク接続、ユーザーアカウントの作成、ディレクトリサービスの設定、ファームウェアのアップグレードなどが含まれます。このガイドは、技術者、システム管理者、承認サービスプロバイダ、およびシステムハードウェアの管理の経験を持つユーザーを対象にしています。

このガイドに記載されている情報を十分に理解するには、このガイドとともに、Oracle Integrated Lights Out Manager (ILOM) 3.0 のその他のガイドを使用してください。ILOM 3.0 の各種ガイドについては、[viii ページの「関連ドキュメント」](#)を参照してください。

ここでは、次のトピックについて説明します。

- [viii ページの「関連ドキュメント」](#)
- [ix ページの「マニュアル、サポート、およびトレーニング」](#)
- [ix ページの「ILOM 3.0 のバージョン番号」](#)
- [x ページの「ドキュメントのフィードバック」](#)

関連ドキュメント

次の表に、ILOM 3.0 の各種ガイドのリストを示します。これらのガイドには、次の URL からオンラインでアクセスし、ダウンロードすることができます。

<http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic>

注 – ILOM 3.0 の各種ガイドは、これまで Sun Integrated Lights Out Manager (ILOM) ガイドと呼ばれていました。

タイトル	コンテンツ	パーツ番号	形式
『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』	ILOM の特長と機能に関する説明	820-7370	PDF HTML
『Oracle Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』	ネットワーク接続、初回の ILOM へのログイン、およびユーザーアカウントやディレクトリサービスの設定の説明と手順	820-7382	PDF HTML
『Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』	ILOM Web インタフェースを使用して ILOM 機能にアクセスするための説明と手順	820-7373	PDF HTML
『Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』	ILOM CLI を使用して ILOM 機能にアクセスするための説明と手順	820-7376	PDF HTML
『Oracle Integrated Lights Out Manager (ILOM) 3.0 管理プロトコルリファレンスガイド』	SNMP、IPMI、または WS-Man と CIM を使用して ILOM 機能にアクセスするための説明と手順	820-7379	PDF HTML
『Oracle Integrated Lights Out Manager (ILOM) 3.0 機能更新およびリリースノート』	ILOM 3.0 の新しい機能および既知の問題と回避方法についての最新の情報	821-0647	PDF HTML
『Oracle Integrated Lights Out Manager (ILOM) CMM 管理ガイド – Sun Blade 6000/Sun Blade 6048 モジュールシステム』	CMM 固有の ILOM 機能にアクセスするための説明と手順	821-3083	PDF HTML

ILOM 3.0 の各種マニュアルに加えて、関連する ILOM 補足マニュアルやプラットフォームの管理マニュアルにも、使用しているサーバープラットフォームに固有の ILOM の機能やタスクが記載されています。ILOM 3.0 の各種マニュアルとともに、使用しているサーバープラットフォームに付属している ILOM 補足マニュアルやプラットフォームの管理マニュアルを使用してください。

これらのドキュメントの一部については、この表の上に記載されている Web サイトで翻訳版が入手可能です。英語版は頻繁に改訂されており、翻訳版よりも最新の情報が記載されています。

マニュアル、サポート、およびトレーニング

次の Web サイトでは追加リソースが提供されています。

- マニュアル <http://docs.sun.com>
- サポート <http://www.sun.com/support/>
- トレーニング <http://www.sun.com/training/>

ILOM 3.0 のバージョン番号

ILOM 3.0 では、システムで動作している ILOM のバージョンを識別しやすいように、新しいバージョン番号方式を採用しています。この番号方式では、5 つのフィールドがある文字列を使用しています。たとえば、a.b.c.d.e となります。

- a - ILOM のメジャーバージョンを示します。
- b - ILOM のマイナーバージョンを示します。
- c - ILOM の更新バージョンを示します。
- d - ILOM のマイクロバージョンを示します。マイクロバージョンは、プラットフォームまたはプラットフォームのグループ単位で管理されます。詳細は、使用しているプラットフォームの製品ノートを参照してください。
- e - ILOM のナノバージョンを示します。ナノバージョンは、マイクロバージョンの増分反復です。

たとえば、ILOM 3.1.2.1.a の意味は、次のとおりです。

- ILOM 3 は、ILOM のメジャーバージョンです。
- ILOM 3.1 は、ILOM3 のマイナーバージョンです。
- ILOM 3.1.2 は、ILOM 3.1 の 2 番目の更新バージョンです。
- ILOM 3.1.2.1 は、ILOM 3.1.2 のマイクロバージョンです。
- ILOM 3.1.2.1.a は、ILOM 3.1.2.1 のナノバージョンです。

ドキュメントのフィードバック

このドキュメントに関するコメントは、次のサイトで「Feedback [+]」リンクをクリックしてお送りください。

<http://docs.sun.com>

ご意見をお寄せいただく際には、下記のタイトルとパーツ番号を記載してください。

『Oracle Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』、part number 820-7382-11。

第1章

ILOM の使用を開始する

項目	
説明	リンク
このガイドの使用法を確認します	<ul style="list-style-type: none">• 2 ページの「このガイドについて」
ILOM の使用を開始するためのプロセスと準備すべき事柄を確認し、インタフェースを選択し、ILOM のセットアップについて計画します	<ul style="list-style-type: none">• 2 ページの「ILOM の使用開始プロセス」• 5 ページの「ILOM へのシステムの接続」
ILOM への接続の要件を確認します	<ul style="list-style-type: none">• 5 ページの「ILOM へのシステムの接続」• 6 ページの「Web インタフェースまたは CLI の使用」• 7 ページの「root アカウントの使用」

このガイドについて

『Oracle ILOM 3.0 入門ガイド』では ILOM のセットアップと設定のための簡単な手順を紹介します。これにより、ホストシステムに電源を投入する前でも ILOM を使用できるようになります。

ILOM を使用すると、使用している Oracle Sun サーバプラットフォームを、オペレーティングシステムのリソースを使うことなく遠隔から監視および管理できます。ILOM では、ブラウザベースの Web インタフェース、コマンド行インタフェース、SNMP インタフェース、IPMI インタフェースなど、豊富な機能を備えたインタフェースが用意されています。これらのインタフェースは、業界標準に基づいており、直感的な操作が可能です。

この使用開始手順では、システムを ILOM に接続する方法と、ILOM に必要な初期設定について説明します。また、ILOM ファームウェアのバージョンの確認と更新の手順についても説明します。ILOM の特徴と機能についての詳細な情報は、ILOM 3.0 マニュアルセットに含まれるほかのマニュアルで説明されています。これらのドキュメントの一覧は、[viii ページの「関連ドキュメント」](#)を参照してください。

ILOM の使用開始プロセス

ILOM のデフォルトの構成および設定を使用して、ILOM の多くの機能にアクセスできますが、それぞれの環境で一部の ILOM 設定をカスタマイズして使用することもできます。ILOM の初期セットアップを開始する前に、ILOM へのアクセス方法を決定し、使用しているシステムおよびデータセンター環境に合わせた ILOM の設定方法を決めてください。

表 1-1 では、ILOM をはじめて使う場合に考慮すべきタスクについて説明します。次の手順では、各タスクについて詳しく説明します。

表 1-1 ILOM の初期セットアップおよび設定タスク

タスク	考慮すべき情報	参照する手順
ILOM へのログインの前提条件として必要な情報		
システムを ILOM に接続し、ILOM Web インタフェースと CLI のいずれかの使用を選択した後、事前設定された root ユーザーアカウントについて確認します	<p>ILOM には、Ethernet 接続またはシリアル接続を使用して接続できます。</p> <p>ILOM 3.0.12 以降のリリースでは、IPv4 と IPv6 のデュアルスタックネットワーク環境を使用できます。</p> <p>ILOM の初回セットアップは、Web インタフェースまたはコマンド行インタフェース (CLI) のどちらを使っても行うことができます。</p> <p>初回ログインには、事前設定された root ユーザーアカウントを使用します。</p>	<p>5 ページの「ILOM へのシステムの接続」</p> <p>6 ページの「Web インタフェースまたは CLI の使用」</p> <p>7 ページの「root アカウントの使用」</p> <p>使用しているプラットフォームのドキュメントも参照してください。</p>
ILOM への最初のログイン		
root ユーザーアカウントを使用した ILOM へのログイン	<p>Oracle Sun サーバプラットフォームに電源を投入すると、ILOM は自動的に起動します。ILOM では、root ユーザーアカウントおよびそのパスワードが事前構成されています。最初のログインとアカウントのセットアップには、この特別なアカウントを使用できます。</p> <p>root アカウントを使用してログインするには、次のユーザー名とパスワードを使用します。</p> <ul style="list-style-type: none"> ユーザー名: root パスワード: changeme 	<p>10 ページの「Web インタフェースを使用した ILOM への初回ログイン」</p> <p>34 ページの「CLI を使用した ILOM への初回ログイン」</p>
ネットワークアクセスについての ILOM の設定		
IPv4 または IPv6 ネットワークの設定	<p>提供されているデュアルスタックの IPv4 (DHCPv4) および IPv6 (ステートレス) のデフォルト設定をそのまま使用することも、ILOM Web インタフェースまたはコマンド行インタフェース (CLI) を使用して設定を変更することもできます。</p> <p>また、使用するネットワークで IPv4 のみがサポートされている場合は、ホストオペレーティングシステムから BIOS ユーティリティまたは IPMItool を使って IPv4 のデフォルト設定を変更できます。</p>	<p>12 ページの「IPv4 と IPv6 のネットワーク環境の設定」(web)</p> <p>35 ページの「IPv4 と IPv6 のネットワーク環境の設定」(CLI)</p>

表 1-1 ILOM の初期セットアップおよび設定タスク (続き)

タスク	考慮すべき情報	参照する手順
ローカルユーザーアカウントの作成またはディレクトリサービスの使用		
注 - ローカルユーザーアカウントの作成とディレクトリサービスの設定のうちどちらかを選ぶことができます。		
ローカルユーザーアカウントの追加と役割の割り当て	ILOM へのログイン後、最大 10 個のローカルユーザーアカウントを作成して設定できます。	15 ページの「ユーザーアカウントの追加またはディレクトリサービスの設定」(web) 40 ページの「ユーザーアカウントの追加またはディレクトリサービスの設定」(CLI)
Active Directory 用の ILOM の設定	Active Directory を使用するには、主サーバー、ポート番号、および証明書モードのような基本的なデータや、代替サーバー、イベントレベル、および重要度レベルのような省略可能データを入力する必要があります。	18 ページの「Active Directory 用の ILOM の設定」(web) 41 ページの「Active Directory 用の ILOM の設定」(CLI)
LDAP 用の ILOM の設定	ILOM は、LDAP を使用して、LDAP クライアントとして認証を実行できます。LDAP 認証を使用するには、ILOM が認証に使用するかバインドできる LDAP サーバー上にユーザーアカウントを作成する必要があります。それにより、クライアントは LDAP サーバーの適切なディレクトリを検索する権限を持ちます。	23 ページの「LDAP サーバーを設定する」(web) 45 ページの「LDAP 用に ILOM を設定する」(CLI)
LDAP/SSL 用に ILOM を設定する	SSL (Secure Socket Layer) を使用した LDAP を設定するには、主サーバー、ポート番号、および証明書モードのような基本的なデータや、代替サーバー、イベントレベル、および重要度レベルのような省略可能データを入力する必要があります。	26 ページの「LDAP/SSL 用に ILOM を設定する」(web) 45 ページの「LDAP/SSL 用に ILOM を設定する」(CLI)
RADIUS 用の ILOM の設定	RADIUS 認証を使用するには、最初に、RADIUS サーバーの IP アドレスとポート番号、および RADIUS サーバーへのアクセスに使用する共有シークレットを設定する必要があります。	30 ページの「RADIUS 用の ILOM の設定」(web) 49 ページの「RADIUS 用の ILOM の設定」(CLI)
管理者ユーザーアカウントを使用した ILOM へのログインとログアウト		
ローカルの管理者ユーザーアカウントを使用した ILOM へのログイン	ローカルユーザーアカウントの作成またはディレクトリサービスの設定が完了したら、ローカルの管理者ユーザーアカウントを使用して ILOM にログインします。	31 ページの「新しいユーザーアカウントを使用して ILOM にログインする」(web) 50 ページの「新しいユーザーアカウントを使用して ILOM にログインする」(CLI)

表 1-1 ILOM の初期セットアップおよび設定タスク (続き)

タスク	考慮すべき情報	参照する手順
ILOM からのログアウト	構成の設定が保持されている際、ILOM セッションからログアウトできます。	32 ページの「ILOM からログアウトする」(web) 51 ページの「ILOM からログアウトする」(CLI)
ILOM のバージョン識別とファームウェアのアップグレード		
ILOM バージョンの識別	サービスプロセッサまたはシャーシ監視モジュール上で実行されている ILOM のバージョンを簡単に識別できます。	54 ページの「ILOM バージョン情報の識別」
ILOM ファームウェアのアップグレード	ILOM のファームウェアを簡単に最新バージョンに更新できます。	55 ページの「ILOM ファームウェアの最新バージョンへの更新」

ILOM へのシステムの接続

ネットワーク接続がない場合は、シリアルポート経由で ILOM にログインできます。また、ネットワーク管理ポートを使用してネットワーク経由でシステムを ILOM に接続することもできます。

使用しているネットワークインフラストラクチャーでファイアウォールが使われている場合や一般的なサービス用に標準でないポートが使われている場合は、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』で説明しているデフォルトのネットワークポート割り当てを確認してください。

接続の要件

ILOM 3.0.12 では、IPv4 と IPv6 のデュアルスタックネットワーク環境の構成をサポートするために、新しいネットワーク構成の設定が ILOM Web インタフェースと CLI に追加されています。IPv4 と IPv6 のデュアルスタックネットワークについては、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

ILOM へのログインとネットワーク設定の構成の手順を実行する前に、次の要件を満たしていることを確認してください。

- データセンター環境で動作するように ILOM をサーバーにセットアップする方法を計画すること。『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』で、ILOM との通信の確立に関する節を参照してください。

- ネットワーク接続を使用しないでシリアルポート経由で ILOM に接続するか、ネットワーク経由で ILOM にログインすること。シリアル直接接続を使用してログインするには、ワークステーション、端末、または端末エミュレータと、サーバーの SER MGT ポート (Sun Blade モジュラーシステムシャーシを使用している場合はシャーシ監視モジュール (CMM) ポート) にシリアルケーブルを接続します。ネットワーク接続を使用してログインする場合は、サーバーまたは CMM の NET MGT ポートに Ethernet ケーブルを接続します。詳細については、使用しているプラットフォームのドキュメントを参照してください。
- ネットワーク設定を構成する方法を決定すること。ILOM 3.0.12 では、新しいデュアルスタックの IPv4 と IPv6 の設定が用意されており、IPv4 と IPv6 のネットワーク環境で ILOM を完全に動作させることができます。ILOM 3.0.12 より前は、IPv4 用のネットワーク構成の設定が提供されていました。IPv4 と IPv6 のデュアルスタックネットワーク設定、IPv4 用の DHCP 設定、または IPv6 用のステートレス設定のいずれかを使用できます。デフォルトで、ILOM は、DHCP を使用してネットワーク設定を取得しようとします。
- IPv4 ネットワーク環境用のネットワークアドレスが ILOM で受け付けられたこと、また、IPv6 ネットワーク環境用の DNS 名とホスト名が ILOM で受け付けられたことを確認してください。

Web インタフェースまたは CLI の使用

ILOM の機能には、SNMP インタフェースや IPMI インタフェースに加えて、Web インタフェースまたはコマンド行インタフェース (command-line interface、CLI) のいずれかを使用してアクセスすることができます。Web インタフェースまたは CLI では、ILOM のすべてのタスクを実行することができます。

このガイドでは、使用開始のための手順は 2 つの章に分かれています。第 2 章では、Web インタフェースを使用して初期セットアップおよび設定タスクを実行する方法について説明します。第 3 章では、CLI を使用して同じタスクを実行する方法について説明します。セットアップと設定を開始する前に、いずれかのインタフェースを選択し、それぞれのインタフェースに対応する手順に従ってください。

root アカウントの使用

ILOM 3.0 では、root ユーザーアカウントが事前構成されています。はじめて ILOM にログインするときは、root アカウントを使用します。この root ユーザーアカウントについては、ILOM 2.x から ILOM 3.0 への移行で変更はありません。同じ方法で、root ユーザーアカウントを使用してログインできます。

root ユーザーアカウントは持続的であり、root アカウントを削除しないかぎり、すべてのインタフェース (Web インタフェース、CLI、SSH、シリアルコンソール、および IPMI) で使用できます。root アカウントでは、ILOM のすべての機能やコマンドに対して組み込み型の管理権限 (読み取りおよび書き込み) が提供されます。

root アカウントを使用して ILOM にログインするには、次のユーザー名とパスワードを使用します。

- ユーザー名: **root**
- パスワード: **changeme**

システムへの承認されていないアクセスを防止するために、システムに搭載された各サービスプロセッサ (SP) またはシャーシ監視モジュール (CMM) で、root のパスワード (changeme) を変更する必要があります。あるいは、root アカウントを削除して、システムアクセスのセキュリティを保護することもできます。ただし、root アカウントを削除する前に、新しいユーザーアカウントを設定するか、ディレクトリサービスを設定して、ILOM にログインできるようにする必要があります。

ILOM にログインするための新しいユーザーアカウントやディレクトリサービスを設定する前に root アカウントを削除した場合は、代替手段として、事前設定された別のアカウントである default ユーザーアカウントを使用してログインし、root アカウントを再作成できます。default ユーザーアカウントの詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

第2章

Web インタフェースを使用した ILOM の初期セットアップ手順

項目	
説明	リンク
ILOM への最初のログイン	• 10 ページの「Web インタフェースを使用した ILOM への初回ログイン」
ネットワーク環境の設定	• 12 ページの「IPv4 と IPv6 のネットワーク環境の設定」
ユーザーアカウントの追加またはディレクトリサービスの設定	• 15 ページの「ユーザーアカウントの追加またはディレクトリサービスの設定」
それ以降の ILOM 設定の各ステップに関する情報の確認	• 32 ページの「次の手順」

Web インタフェースを使用した ILOM への初回ログイン

ILOM Web インタフェースへの初回ログインを実行するには、デフォルトの root ユーザーアカウントとそのアカウントのデフォルトのパスワードである `changeme` を使用します。

▼ root ユーザーアカウントを使用して ILOM にログインする

root ユーザーアカウントを使用して ILOM への初回ログインを実行するには、Web ブラウザを開いて次の操作を行います。

1. Web ブラウザに `http://system_ipaddress` と入力します。

ILOM がデュアルスタックネットワーク環境で動作している場合は、IPv4 または IPv6 のいずれかのアドレス形式を使用して `system_ipaddress` を入力できます。

例:

IPv4 の場合 - `http://10.8.183.106`

または

IPv6 の場合 - `http://[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

Web インタフェースのログインページが表示されます。

デュアルスタック環境での IP アドレスの入力の詳細、および接続の問題の診断については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。



2. 次のように、root ユーザーアカウントのユーザー名とパスワードを入力します。

ユーザー名: **root**

パスワード: **changeme**

3. 「Log In」をクリックします。

Web インタフェースの「Version」ページが表示されます。

これで、ネットワーク設定を構成して ILOM のすべての機能にアクセスする準備ができました。ILOM の特徴および ILOM の機能にアクセスするための手順については、ILOM 3.0 マニュアルセットに含まれるほかのマニュアルを参照してください。ILOM 3.0 マニュアルセットには、次の URL からアクセスできます。

<http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic>

IPv4 と IPv6 のネットワーク環境の設定

次に示す Web インタフェースの手順では、ILOM 3.0.12 以降のバージョンを IPv4 と IPv6 のデュアルスタックネットワーク環境で動作するように設定する方法を説明します。IPv4 と IPv6 のネットワーク環境での ILOM の設定の詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

ILOM 3.0.10 およびそれより前のバージョンの ILOM でサポートされているように、IPv4 環境で動作するように ILOM を設定する場合は、『Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』を参照してください。

デフォルトでは、ILOM は DHCPv4 を使用して IPv4 アドレスを取得し、IPv6 ステートレスを使用して IPv6 アドレスを取得しようとします。

▼ Web インタフェースを使用して IPv4 と IPv6 の設定を構成する

1. ILOM SP Web インタフェースまたは CMM ILOM Web インタフェースにログインします。
2. 「Network」タブにある IPv4 と IPv6 のネットワーク設定にナビゲートします。

例:

- サーバー SP で、「Configuration」-->「Network」をクリックします。
- CMM では次のようにします。
 - ブレード (左の区画) を選択し、次に (右の区画で) 「Configuraion」-->「Network」をクリックします。
 - 「Network Settings」テーブルで、CMM またはブレード SP のラジオボタンを選択し、「Edit」をクリックします。

注 – Web インタフェースの CMM レベルにある「Network Settings」ページでは、IPv4 と IPv6 のデュアルスタックのプロパティはサポートされていません。ただし、IPv4 専用プロパティはサポートされています。CMM の IPv6 ネットワーク設定を変更する場合は、[35 ページの「CLI を使用して IPv4 と IPv6 の設定を構成する」](#)を参照してください。

3. ネットワークの State が有効になっていることを確認します。

注 – IPv4 および IPv6 の両方に対して、ネットワークの State の設定はデフォルトで有効になります。必要に応じて、IPv6 用のネットワークの State をオプションで無効にする (チェックを外す) ことができます。ただし、ILOM を IPv4 ネットワーク環境または IPv4 と IPv6 のデュアルスタックネットワーク環境で動作させるために、IPv4 ネットワークの State は常に有効にしておく必要があります。

4. 次に示すネットワーク構成の手順で、使用しているネットワーク環境に適用するものを実行します。

- 静的 IP を手作業で構成するには、次に示す IPv4 の手順または IPv6 の手順、あるいはその両方を参照してください。
 - 静的 IPv4 アドレスを手作業で構成する手順:

手順	説明
----	----

- a. 「Static IP」のラジオボタンを有効にします。
 - b. IP アドレスのテキストボックスにデバイスの IP アドレスを入力します。
 - c. デバイスが属するネットワークのサブネットマスクを入力します。
 - d. デバイスのゲートウェイアクセスのアドレスを入力します。
-

- 静的 IPv6 アドレスを手作業で構成する手順:

手順	説明
----	----

- IP アドレスのテキストボックスにデバイスの IP アドレスを入力します。IPv6 の静的 IP とネットマスクを指定するための入力パラメータは、次のとおりです。

`<IPv6_address>/<subnet_mask_length_in_bits>`

例:

`[fec0:a:8:b7:214:4fff:feca:5f7e/64]`

注 – IPv6 では、1 つのデバイスに対する複数の IP アドレスの割り当てがサポートされます。そのため、ILOM で単一の静的 IPv6 アドレスを手作業で構成し、必要な場合はさらに、ILOM で 1 つまたは複数の IPv6 自動構成オプションを有効にできます。

- IPv4 アドレスが DHCP で自動的に割り当てられるようにするには、IPv4 DHCP のラジオボタンを選択します。
- 1 つまたは複数の IPv6 自動構成オプションを有効にするには、次に説明する適切なオプションを選択します。

IPv6 自動構成オプション	説明
Stateless (デフォルトで有効)	有効にすると、Stateless 自動構成オプションが実行され、ネットワークの IPv6 ルーターからデバイスの IPv6 ステートレスアドレスが取得されます。
DHCPv6 Stateless	有効にすると、DHCPv6 Stateless 自動構成オプションが実行され、ネットワークの DHCPv6 サーバーからデバイスの DNS 情報が取得されます。 注 - DHCPv6 Stateless 自動構成オプションは ILOM 3.0.14 で使用できます。
DHCPv6 Stateful	有効にすると、DHCPv6 Stateful 自動構成オプションが実行され、ネットワークの DHCPv6 サーバーからデバイスの IPv6 アドレスと DNS 情報が取得されます。 注 - DHCPv6 Stateful 自動構成オプションは ILOM 3.0.14 で使用できます。

注 - ILOM 3.0.14 以降では、DHCPv6 Stateless のオプションが有効になっている場合または DHCPv6 Stateful のオプションが有効になっている場合に、同時に Stateless 自動構成のオプションを有効にして動作させることができます。ただし、DHCPv6 Stateless と DHCPv6 Stateful の自動構成オプションを有効にして同時に動作させることはできません。

注 - DHCPv6 Stateful または DHCPv6 Stateless のいずれかの自動構成オプションを有効にした場合、ILOM の「Network Settings」ページで、DHCP 情報を取得するために最後に使用された、DHCPv6 サーバーの DHCP 固有 ID が識別されます。

5. 「Save」をクリックして変更を適用します。

「Save」をクリックするまでは、ネットワーク設定に対する変更はすべて、ILOM セッションで保留中であるとみなされます。

注 - デバイス (SP または CMM) の静的 IP アドレスを変更すると、デバイスとのアクティブな ILOM セッションがすべて終了します。ブラウザセッションを閉じるように促すメッセージが表示されます。新しく割り当てられた静的 IP アドレスを使用して ILOM にログインし直す必要があります。

注 – IPv6 の自動構成オプションから取得されたデバイスの IPv6 アドレスは、デバイスとのアクティブな ILOM セッションには影響しません。「Network」タブで、新しく取得された、自動構成されたアドレスを検証できます。

ILOM から IPv4 または IPv6 ネットワーク構成をテストするには、ネットワークテストツール (Ping または Ping6) を使用します。詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』を参照してください。

ユーザーアカウントの追加またはディレクトリサービスの設定

root ユーザーアカウントを使用して ILOM にログインした後、ローカルユーザーアカウントを作成するか、ディレクトリサービスを設定するかを選択できます。ILOM ユーザーアカウントとディレクトリサービスの詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

項目

説明	リンク
ユーザーアカウントを追加する方法およびユーザー役割 (権限) を割り当てる方法	<ul style="list-style-type: none">• 16 ページの「ユーザーアカウントを追加して権限を割り当てる」
Active Directory 用に ILOM を設定する方法	<ul style="list-style-type: none">• 18 ページの「Active Directory 用の ILOM の設定」
LDAP サーバーを設定する方法	<ul style="list-style-type: none">• 23 ページの「LDAP サーバーを設定する」
LDAP 用に ILOM を設定する方法	<ul style="list-style-type: none">• 24 ページの「LDAP 用の ILOM の設定」
LDAP/SSL 用に ILOM を設定する方法	<ul style="list-style-type: none">• 26 ページの「LDAP/SSL 用に ILOM を設定する」
SSL テーブルを編集する方法	<ul style="list-style-type: none">• 29 ページの「LDAP/SSL テーブルを編集する」
RADIUS 用に ILOM を設定する方法	<ul style="list-style-type: none">• 30 ページの「RADIUS 用の ILOM の設定」
新しいユーザーアカウントまたはディレクトリサービスが正常に動作していることを検証する方法	<ul style="list-style-type: none">• 31 ページの「新しいユーザーアカウントを使用して ILOM にログインする」
ILOM からログアウトする方法	<ul style="list-style-type: none">• 32 ページの「ILOM からログアウトする」

▼ ユーザーアカウントを追加して権限を割り当てる

1. ILOM Web インタフェースにログインします。
2. 「User Management」 --> 「User Accounts」 を選択します。
「User Account Settings」 ページが表示されます。
3. 「Users」 テーブルで 「Add」 をクリックします。
「Add User」 ダイアログが表示されます。

The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon and space.

User Name:

Profile:
 Admin (a) User Management (u)
 Console (c) Reset and Host Control (r)
 Read Only (o) Service (s)

New Password:

Confirm New Password:

Done 10.8.136.165

4. 次の情報を入力します。
 - a. 「User Name」 フィールドに、ユーザー名を入力します。
 - b. プロファイルを選択します。新しい ILOM 3.0 のすべてのインストールでは、「Advanced Role」を選択できます。
 - c. 適切な役割を選択します。

ユーザーアカウントの詳細な役割の説明については、次の表を参照してください。

Roles	定義	権限
a	Admin	Admin (a) 役割が割り当てられたユーザーは、ILOM 設定変数の状態を表示および変更することができます。Admin 役割が割り当てられたユーザーは、User Management、Console、および Reset and Host Control の役割を持つユーザーのタスクを除き、すべての ILOM 機能を実行できます。
u	User Management	User Management (u) 役割が割り当てられたユーザーは、ユーザーアカウントの作成および削除、ユーザーパスワードの変更、ほかのユーザーに割り当てられた役割の変更、および default ユーザーアカウントに対する物理アクセス要件の有効化または無効化を実行できます。また、この役割では、LDAP、LDAP/SSL、RADIUS、および Active Directory を設定することもできます。
c	Console	Console (c) 役割が割り当てられたユーザーは、ILOM リモートコンソールおよび SP コンソールにアクセスし、ILOM コンソール設定変数の状態を表示および変更することができます。
r	Reset and Host Control	Reset and Host Control (r) 役割が割り当てられたユーザーは、電源制御、リセット、ホットプラグ操作、コンポーネントの有効化と無効化、障害管理など、システムを操作することができます。この役割は、ILOM 2.0 のオペレータ権限を持つユーザーにほぼ対応しています。
o	Read Only	Read Only (o) 役割が割り当てられたユーザーは、ILOM 設定変数の状態を表示できますが、変更できません。また、この役割が割り当てられたユーザーは、自分のユーザーアカウントのパスワードとセッションタイムアウト設定を変更できます。
s	Service	Service (s) 役割が割り当てられたユーザーは、オンサイトサービスが必要な場合に Oracle の保守担当者を補助することができます。

d. 「New Password」フィールドにパスワードを入力します。

パスワードは、8 文字以上 16 文字以下にしてください。パスワードの大文字と小文字は区別されません。英数字のほか、セキュリティを高めるため特殊文字も使用してください。コロン以外のすべての文字を使用できます。パスワードにはスペースは使用できません。

e. 「Confirm New Password」フィールドにパスワードを再入力し、パスワードを確認します。

f. 新しいユーザーの情報を入力し終わったら、「Save」ボタンをクリックします。

「User Account Settings」ページが再表示されます。「User Account Settings」ページには、新しいユーザーアカウントとその関連情報が表示されています。

▼ Active Directory 用の ILOM の設定

1. ILOM Web インタフェースにログインします。
2. 「User Management」 --> 「Active Directory」 を選択します。
「Active Directory」 ページが表示されます。

Active Directory

Configure Active Directory settings on this page. Select default roles for all Active Directory users, either Administrator, Operator, Advanced or none (server authorization). Enter the Hostname or IP address of your server. To change the port used to communicate with your server, uncheck *Autoselect*. Enter a timeout value in seconds. Use the log detail levels to control the amount of debug information sent to the log. To load a certificate, fill in the Certificate File Upload information and click Load Certificate to complete the process.

State: Enabled

Roles: ▼
 Admin (a) User Management (u)
 Console (c) Reset and Host Control (r)
 Read Only (o) Service (s)

Address:

Port: Autoselect

Timeout:

Strict Certificate Mode: Enabled

DNS Locator Mode: Enabled

Log Detail: ▼

Certificate Information

Certificate File Status: certificate not present

Certificate File Upload

Transfer Method: ▼

Select File:

- ▼ Admin Groups
- ▼ Operator Groups
- ▼ Custom Groups
- ▼ User Domains
- ▼ Alternate Servers
- ▼ DNS Locator Queries

3. Active Directory 設定を構成します。

Active Directory の設定については、次の表を参照してください。

プロパティ (Web)	プロパティ (CLI)	デフォルト値	説明
State	state	Disabled	Enabled Disabled Active Directory クライアントを有効にするか無効にするかを指定します。
Roles	defaultRole (a u c r o s)	(なし)	Administrator Operator Advanced roles なし 認証されたすべての Active Directory ユーザーに付与されるアクセスの役割。このプロパティでは、旧バージョンの Administrator 役割や Operator 役割、または個々の役割 ID 「a」、「u」、「c」、「r」、「o」、「s」の任意の組み合わせがサポートされます。たとえば aucros と指定できます。a は Admin、u は User Management、c は Console、r は Reset and Host Control、o は Read Only、s は Service です。ここで役割を設定しない場合、役割の決定には Active Directory サーバーが使用されます。
Address	address	0.0.0.0	Active Directory サーバーの IP アドレスまたは DNS 名。DNS 名を使用する場合は、DNS が設定され機能していなければなりません。
Port	port	0	サーバーとの通信に使用するポート。または autoselect を有効にします (ポートに 0 を割り当てます)。 使用している標準以外の TCP ポートで予期しないイベントが発生した場合に使用できます。
Timeout	timeout	4	秒単位のタイムアウトの値。 個々のトランザクションが完了するまで待機する秒数です。トランザクションの数は設定に応じて異なるため、この値はすべてのトランザクションの合計時間を表すわけではありません。このプロパティは、サーバーが応答していない場合や到達不可能な場合に待機する時間を調整するために使用できます。
Strict Certificate Mode	strictcertmode	Disabled	Enabled Disabled 有効にすると、認証時にデジタル署名を利用してサーバー証明書の内容が検証されます。厳密な証明書モードを有効にするには、証明書がロードされている必要があります。
DNS Locator Mode	dnslocatormode	Disabled	Enabled Disabled 有効にすると、設定された DNS ロケータクエリーに基づき、Active Directory サーバーの検出が試みられます。
Log Detail	logdetail	なし	None High Medium Low イベントログに記録される診断項目の量を指定します。

4. 「Save」をクリックして設定を有効にします。

5. Active Directory 証明書の情報を表示します。

Active Directory の証明書の設定については、次の表を参照してください。

プロパティ (Web)	プロパティ (CLI)	表示	説明
Certificate File Status	certstatus	certificate not present	証明書の有無を示す読み取り専用の項目。
Certificate File Status	certstatus	certificate present (details)	「details」をクリックして、発行者、主題、シリアル番号、有効期限開始、有効期限終了、およびバージョンの情報を確認します。

6. 「Certificate File Upload」セクションで、証明書ファイルをアップロードする転送方法と必要なパラメータを選択します。

注 – 厳密な証明書モードを使用しない場合は、この手順は不要です。

次の表では、転送方法ごとに必要なパラメータを示します。

転送方法	必要なパラメータ
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

7. 「Load Certificate」ボタンまたは「Remove Certificate」ボタンをクリックします。

8. 「certificate present (details)」を選択した場合、証明書がロードされると、次に示す読み取り専用の詳細情報が表示されます。

アイテム	説明
issuer	証明書を発行した認証局。
subject	証明書の対象となるサーバーまたはドメイン。
valid_from	証明書の有効期限の開始日。
valid_until	証明書の有効期限の終了日。
serial_number	証明書のシリアル番号。
version	証明書のバージョン番号。

9. 「Active Directory」 ページの一番の下で、設定する設定オプションの横にあるラジオボタンをクリックします。

- Admin Groups
- Operator Groups
- Custom Groups
- User Domains
- Alternate Servers
- DNS Locator Queries

10. テーブルに必要なデータを入力します。

Admin Groups、**Operator Groups**、および **Custom Groups** のテーブルには、Microsoft Active Directory グループの名前が、識別名 (DN) 形式、単純名形式、または NT 形式で含まれます。Custom Groups では、ユーザーの役割を、実行するタスクに応じて Advanced Roles、Administrator、または Operator の権限に設定する必要があります。

User Domains は、ユーザーの認証に使われる認証ドメインです。ユーザーがログインする際に使用する名前は、このセルに表示されているドメイン名形式テンプレートの形式になります。認証の際、<USERNAME> はユーザーのログイン名に置き換えられます。原則の形式または識別名形式がサポートされます。ユーザー認証は、入力されたユーザー名と設定済みのユーザードメインに基づいて試行されます。

Alternate Servers テーブルは、認証に冗長性を提供します。証明書が指定されていない場合、トップレベルの主証明書が使用されます。代替サーバーのルールと要件は、トップレベル証明書モードと同じです。各サーバーにそれぞれの証明書状態があり、必要に応じてそれぞれの証明書コマンドで証明書を取得します。

DNS Locator Queries テーブルは、認証に使用するホストについて DNS サーバーに問い合わせるために使用されます。DNS ロケータクエリーは、DNS ロケータが有効で DNS が設定され機能している場合のみ使用します。

次の表に、Active Directory データの望ましい形式を示すためのデフォルトデータを示します。

■ Admin Groups テーブル

エン트리 1 に表示されている名前は、識別名形式を使用しています。

ID	名前
1	CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com

■ Operator Groups テーブル

エン트리 1 に表示されている名前は、識別名形式を使用しています。

ID	名前
1	CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com

■ Custom Groups テーブル

エン트리 1 に表示されている名前は、単純名形式を使用しています。

ID	名前	Roles
1	custom_group_1	Admin, User Management, Console, Reset and Host Control, Read Only (auro)

■ User Domains テーブル

エン트리 1 に表示されているドメインは、ユーザー認証を最初に試行する際に使用される原則の形式を示しています。エン트리 2 は、Active Directory が最初のエン트리での認証に失敗した場合に使用する、完全な識別名を示します。

注 – 次の例の <USERNAME> は、ユーザーのログイン名を表します。認証の際、<USERNAME> はユーザーのログイン名に置き換えられます。

ID	ドメイン
1	<USERNAME>@sales.east.oracle.com
2	CN=<USERNAME>,OU=Users,DC=sales,DC=east,DC=oracle,DC=com

■ Alternate Servers テーブル

次に示す項目は、認証に冗長性を提供します。

ID	アドレス	ポート	証明書の状態
1	10.8.168.99	0	Certificate not present
2	10.8.143.230	0	Certificate not present

■ DNS Locator Queries テーブル

DNS ロケータサービスクエリーは、DNS の名前付きのサービスを特定します。レコードには通常ポート番号が含まれますが、<PORT:636> という形式でオーバーライドできます。また、<DOMAIN> 置換マーカーを使用して、認証対象のドメイン固有のネームサービスを指定できます。

名前	ドメイン
1	_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
2	_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>

11. 「Save」をクリックして変更を有効にします。

▼ LDAP サーバーを設定する

次の手順に従って、LDAP サーバーを設定します。詳細な手順については、LDAP のマニュアルを参照してください。

1. ILOM に対して認証を行うすべてのユーザーが、「crypt」形式か、または一般的には「MD5 crypt」と呼ばれる、crypt の GNU 拡張で保存されたパスワードを使用していることを確認します。

例:

```
userPassword: {CRYPT}ajCa2He4PJhNo
```

または

```
userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
```

ILOM は、これらの 2 種類の crypt 形式で保存されたパスワードによる LDAP 認証のみをサポートしています。

2. オブジェクトクラス `posixAccount` および `shadowAccount` を追加し、このスキーマ (RFC 2307) に必要なプロパティ値を入力します。

必須プロパティ	説明
<code>uid</code>	ILOM にログインするためのユーザー名
<code>uidNumber</code>	任意の固有の数字
<code>gidNumber</code>	任意の固有の数字
<code>userPassword</code>	パスワード
<code>homeDirectory</code>	任意の値 (このプロパティは、ILOM では無視される)
<code>loginShell</code>	任意の値 (このプロパティは、ILOM では無視される)

3. LDAP サーバーを設定して、ILOM のユーザーアカウントにアクセスできるようにします。

LDAP サーバーが匿名バインドを許可するようにするか、または LDAP サーバーにプロキシユーザーを作成します。LDAP サーバーは、ILOM により認証されるすべてのユーザーアカウントに読み取り専用アクセスができます。

[24 ページの「LDAP 用の ILOM の設定」](#)を参照してください。

▼ LDAP 用の ILOM の設定

1. ILOM Web インタフェースにログインします。
2. 「User Management」 --> 「LDAP」を選択します。
「LDAP Settings」ページが表示されます。

System Information	System Monitoring	Configuration	User Management	Remote Control	Maintenance
User Accounts	Active Sessions	LDAP	LDAP/SSL	RADIUS	Active Directory

LDAP Settings

Configure ILOM access for LDAP users on this page. Select default roles for all of your LDAP users, either Administrator, Operator, or Advanced roles are available. Enter the Hostname or IP address of your LDAP server. Enter the port used to communicate with your LDAP server, the default port is 389. Enter the searchbase, or portion of your LDAP tree, where ILOM should look for LDAP user accounts (ou=sales, dn=writers). Enter the distinguished name (DN) and password for a proxy user ILOM can use to access your LDAP tree.

State: Enabled

Roles: Operator
 Admin (a) User Management (u)
 Console (c) Reset and Host Control (r)
 Read Only (o) Service (s)

Address:

Port:

Searchbase:

Bind DN:

Bind Password:

3. 次の値を入力します。

- **State** – LDAP ユーザーを認証するには、「Enabled」チェックボックスを選択します。
- **Role** – 「Administrator」または「Operator」、あるいは個々の役割 ID である「a」、「u」、「c」、「r」、「o」、および「s」の組み合わせを選択します。
- **Address** – LDAP サーバーのアドレスまたは DNS 名です。DNS 名を使用する場合は、DNS が設定され機能していなければなりません。
- **Port** – LDAP サーバーのポート番号です。
- **Searchbase** – ユーザーを検索するための LDAP サーバーの分岐を入力します。
- **Bind DN** – LDAP サーバー上の読み取り専用プロキシユーザーの識別名 (DN) を入力します。ILOM がユーザーの検索と認証を行うには、LDAP サーバーに対する読み取り専用のアクセス権が必要になります。
- **Bind Password** – 読み取り専用ユーザーのパスワードを入力します。

4. 「Save」をクリックして変更を有効にします。

5. LDAP 認証の動作を確認するには、LDAP ユーザー名とパスワードを使用して、ILOM にログインします。

注 – ILOM は、LDAP ユーザーの前にローカルユーザーを検索します。LDAP ユーザー名がローカルユーザーとして存在する場合は、ILOM は認証にローカルアカウントを使用します。

▼ LDAP/SSL 用に ILOM を設定する

LDAP/SSL は、Secure Socket Layer (SSL) テクノロジを使用して強化されたセキュリティを LDAP ユーザーに提供します。厳密な証明書モードが使われている場合は、証明書は省略可能です。

次の手順に従って、LDAP/SSL に対して ILOM を設定します。

1. ILOM Web インタフェースにログインします。
2. 「User Management」 --> 「LDAP/SSL」 を選択します。
構成の設定と LDAP/SSL テーブルがある「LDAP/SSL」ページが表示されます。

User Accounts	Active Sessions	LDAP	LDAP/SSL	RADIUS	Active Directory
---------------	-----------------	------	----------	--------	------------------

LDAP/SSL

Configure LDAP/SSL settings on this page. Select default roles for all LDAP users, either Administrator, Operator, Advanced or none (server authorization). Enter the Hostname or IP address of your server. To change the port used to communicate with your server, uncheck *Autoselect*. Enter a timeout value in seconds. Use the log detail levels to control the amount of debug information sent to the log. To load a certificate, fill in the Certificate File Upload information and click Load Certificate to complete the process.

State: Enabled

Roles: None (server authorization) ▼
 Admin (a) User Management (u)
 Console (c) Reset and Host Control (r)
 Read Only (o) Service (s)

Address:

Port: Autoselect

Timeout:

Strict Certificate Mode: Enabled

Log Detail: Trace ▼

Certificate Information

Certificate File Status: certificate present [\(details\)](#)

Certificate File Upload

Transfer Method: Browser ▼

Select File:

✚ Admin Groups ✚ Operator Groups ✚ Custom Groups
✚ User Domains ✚ Alternate Servers

3. LDAP/SSL 設定を構成します。

LDAP/SSL の設定については、次の表を参照してください。

プロパティ (Web)	プロパティ (CLI)	デフォルト値	説明
State	state	Disabled	Enabled Disabled LDAP/SSL クライアントを有効にするか無効にするかを指定します。
Roles	defaultRole (a u c r o s)	(なし)	Administrator Operator Advanced roles なし 認証されたすべての LDAP/SSL ユーザーに付与されるアクセスの役割。このプロパティでは、旧バージョンの Administrator 役割や Operator 役割、または個々の役割 ID 「a」、「u」、「c」、「r」、「o」、「s」の任意の組み合わせがサポートされます。たとえば aucros と指定できます。a は Admin、u は User Management、c は Console、r は Reset and Host Control、o は Read Only、s は Service です。ここで役割を設定しない場合、役割の決定には LDAP/SSL サーバーが使用されます。
Address	address	0.0.0.0	LDAP/SSL サーバーの IP アドレスまたは DNS 名。DNS 名を使用する場合は、DNS が設定され機能していなければなりません。
Port	port	0	サーバーとの通信に使用するポート。または autoselect を有効にします (ポートに 0 を割り当てます)。 使用している標準以外の TCP ポートで予期しないイベントが発生した場合に使用できます。
Timeout	timeout	4	秒単位のタイムアウトの値。 個々のトランザクションが完了するまで待機する秒数です。トランザクションの数は設定に応じて異なるため、この値はすべてのトランザクションの合計時間を表すわけではありません。 このプロパティは、サーバーが応答していない場合や到達不可能な場合に待機する時間を調整するために使用できます。
Strict Certificate Mode	strictcertmode	Disabled	Enabled Disabled 有効にすると、認証時にデジタル署名を利用してサーバー証明書の内容が検証されます。厳密な証明書モードを有効にするには、証明書がロードされている必要があります。
Log Detail	logdetail	なし	None High Medium Low イベントログに記録される診断項目の量を指定します。

4. 「Save」をクリックして設定を有効にします。

5. 「LDAP/SSL」ページの中央部で、LDAP/SSL の証明書情報を確認します。

LDAP/SSL 証明書の設定については、次の表を参照してください。

プロパティ (Web)	プロパティ (CLI)	Displays	説明
Certificate File Status	certstatus	certificate not present	証明書の有無を示す読み取り専用の項目。
Certificate File Status	certstatus	certificate present (details)	「details」をクリックして、発行者、主題、シリアル番号、有効期限開始、有効期限終了、およびバージョンの情報を確認します。

6. 「Certificate File Upload」セクションで、証明書ファイルをアップロードする転送方法と必要なパラメータを選択します。

注 – 厳密な証明書モードを使用しない場合は、この手順は不要です。

次の表では、転送方法ごとに必要なパラメータを示します。

転送方法	必要なパラメータ
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

7. 「Load Certificate」ボタンまたは「Remove Certificate」ボタンをクリックします。

8. 「certificate present (details)」を選択した場合、証明書がロードされると、次に示す読み取り専用の詳細情報が表示されます。

アイテム	説明
issuer	証明書を発行した認証局。
subject	証明書の対象となるサーバーまたはドメイン。
valid_from	証明書の有効期限の開始日。
valid_until	証明書の有効期限の終了日。
serial_number	証明書のシリアル番号。
version	証明書のバージョン番号。

▼ LDAP/SSL テーブルを編集する

次の手順に従って、Admin Groups、Operator Groups、Custom Groups、User Domains、または Alternate Servers についての情報を変更します。

1. ILOM Web インタフェースにログインします。
2. 「User Management」 --> 「LDAP/SSL」を選択します。
「LDAP/SSL」ページが表示されます。
3. 「LDAP/SSL」ページの最下部で、編集する情報の種類の横にあるリンクを選択します。
 - Admin Groups
 - Operator Groups
 - Custom Groups
 - User Domains
 - Alternate Servers
4. 編集するテーブルの横にあるラジオボタンを選択して、「Edit」をクリックします。
「Edit LDAP/SSL Admin Groups」ページ、「Edit LDAP/SSL Operator Groups」ページ、「Edit LDAP/SSL Custom Groups」ページ、「Edit LDAP/SSL User Domains」ページ、「Edit LDAP/SSL Alternate Servers」ページのいずれかの適切なページが表示されます。

5. 各編集ページで、変更する情報を編集します。

LDAP/SSL テーブルで追加または編集できる情報の例については、18 ページの「Active Directory 用の ILOM の設定」の手順を参照してください。Active Directory テーブルの情報は、LDAP/SSL テーブルと類似しています。

たとえば、「User Domains」テーブルで、「Name」フィールドにテキストで情報を入力します。<USERNAME> 置換マーカーを使用して、ユーザー名の場所を確保します。

```
domain=uid=<USERNAME>,OU=people,DC=sales,DC=east,DC=oracle,DC=com
```

これにより、入力した名前が ILOM に対して認証されます。

6. 「Save」をクリックして変更を有効にします。

▼ RADIUS 用の ILOM の設定

1. ILOM Web インタフェースにログインします。

2. 「User Management」 --> 「RADIUS」を選択します。

「RADIUS Settings」ページが表示されます。

System Information	System Monitoring	Configuration	User Management	Remote Control	Maintenance
User Accounts	Active Sessions	LDAP	LDAP/SSL	RADIUS	Active Directory

RADIUS Settings

Configure ILOM access for RADIUS users on this page. Select default roles for all of your RADIUS users, either Administrator, Operator or Advanced roles are available. Enter the Hostname or IP address of your RADIUS server. Enter the port used to communicate with your RADIUS server, the default port is 1812. Enter the shared secret your RADIUS server uses to authenticate users.

State: Enabled

Roles:

Admin (a) User Management (u)
 Console (c) Reset and Host Control (r)
 Read Only (o) Service (s)

Address:

Port:

Shared Secret:

3. RADIUS の設定を完了します。

プロパティ (Web)	プロパティ (CLI)	デフォルト値	説明
State	state	Disabled	Enabled Disabled RADIUS クライアントを有効にするか無効にするかを指定します。
Role	defaultrole a u c r o s	Read Only (o)	Administrator Operator Advanced Roles 認証されたすべての RADIUS ユーザーに付与されるアクセスの役割。このプロパティでは、旧バージョンの Administrator 役割や Operator 役割、または個々の役割 ID 「a」、「u」、「c」、「r」、「o」、「s」の任意の組み合わせがサポートされます。たとえば aucros と指定できます。a は Admin、u は User Management、c は Console、r は Reset and Host Control、o は Read Only、s は Service です。
Address	ipaddress	0.0.0.0	RADIUS サーバーの IP アドレスまたは DNS 名。DNS 名を使用する場合は、DNS が設定され機能していなければなりません。
Port	port	1812	RADIUS サーバーとの通信に使用するポート番号を指定します。デフォルトのポートは 1812 です。
Shared Secret	secret	(なし)	機密データを保護しクライアントとサーバーの相互認識を可能にするために使われる共有シークレットを指定します。

4. 「Save」をクリックして設定を有効にします。

▼ 新しいユーザーアカウントを使用して ILOM にログインする

root 以外のユーザーアカウントを使用して ILOM Web インタフェースにログインするには、Web ブラウザを開いて次の手順を実行します。

1. Web ブラウザに `http://system_ipaddress` と入力します。

ILOM がデュアルスタックネットワーク環境で動作している場合は、IPv4 または IPv6 のいずれかのアドレス形式を使用して `system_ipaddress` を入力できます。

例:

IPv4 の場合 - `http://10.8.183.106`

または

IPv6 の場合 - `http://[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

Web インタフェースのログインページが表示されます。

デュアルスタック環境での IP アドレスの入力の詳細、および接続の問題の診断については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

2. 次のように、ユーザーアカウントのユーザー名とパスワードを入力します。
ユーザー名: <assigned_username>
パスワード: <assigned_password>
3. 「Log In」をクリックします。
ILOM の Web インタフェースで、「Version」ページが表示されます。

▼ ILOM からログアウトする

- ILOM の Web インタフェースで、「Log Out」ボタンをクリックします。
「Log Out」ボタンは ILOM Web インタフェースの右上の端にあります。Web ブラウザの「Log Out」ボタンを使用して ILOM を終了しないでください。

次の手順

次に、使用しているシステムおよびデータセンターの環境に対して ILOM 設定のカスタマイズを続行することができます。使用している環境に合わせて ILOM を設定する前に、『Oracle Integrated Lights Out Manager 3.0 概念ガイド』を参照して、ILOM 3.0 の新しい特長と機能の概要を確認してください。ILOM の新機能の使用している環境に対する影響を知ることで、使用しているシステムやデータセンターで ILOM のすべての機能にアクセスできるように ILOM を設定するときに役に立ちます。

各ユーザーインタフェースを使用した ILOM タスクの実行方法については、『Oracle ILOM 3.0 手順ガイド』を参照してください。プラットフォーム固有の設定手順については、使用しているプラットフォームの ILOM 補足マニュアルまたはプラットフォームの管理ガイドを参照してください。

ILOM 3.0 の各種マニュアルは以下のサイトで参照できます。

<http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic>

第3章

ILOM CLI を使用した ILOM の初期 セットアップ手順

項目	
説明	リンク
ILOM への最初のログイン	• 34 ページの「CLI を使用した ILOM への初回ログイン」
ネットワーク環境の設定	• 35 ページの「IPv4 と IPv6 のネットワーク環境の設定」
ユーザーアカウントの追加またはディレクトリサービスの設定	• 40 ページの「ユーザーアカウントの追加またはディレクトリサービスの設定」
それ以降の ILOM 設定の各ステップに関する情報の確認	• 51 ページの「次の手順」

CLI を使用した ILOM への初回ログイン

ILOM CLI への初回ログインを実行するには、デフォルトの root ユーザーアカウントとそのアカウントのデフォルトのパスワードである `changeme` を使用します。ネットワーク環境をセットアップした後、割り当てられたユーザーアカウント名とパスワードを使用して管理者ユーザーアカウントを設定できます。

▼ root ユーザーアカウントを使用して ILOM にログインする

ILOM CLI にはじめてログインする際は、SSH および root ユーザーアカウントを使用します。

1. 次のように入力して、root ユーザーアカウントを使用して ILOM CLI にログインします。

```
$ ssh root@system_ipaddress
```

ILOM がデュアルスタックネットワーク環境で動作している場合は、IPv4 または IPv6 のいずれかのアドレス形式を使用して `system_ipaddress` を入力できます。

例:

IPv4 の場合 - 10.8.183.106

または

IPv6 の場合 - [fec0:a:8:b7:214:4fff:5eca:5f7e/64]

ILOM ログインプロンプトが表示されます。

デュアルスタック環境での IP アドレスの入力の詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

2. 以下のようにデフォルトのユーザー名とパスワードを入力します。

```
<hostname>: root
```

```
パスワード: changeme
```

ILOM CLI のプロンプト (->) が表示されます。

IPv4 と IPv6 のネットワーク環境の設定

次に示す CLI の手順では、IPv4 と IPv6 のデュアルスタックネットワーク環境で動作するように ILOM を設定する方法を説明します。IPv4 と IPv6 のネットワーク環境での ILOM の設定の詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

ILOM 3.0.10 およびそれより前のバージョンの ILOM でサポートされているように、IPv4 専用ネットワーク環境で動作するように ILOM を設定する場合は、『Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』を参照してください。

デフォルトでは、ILOM は DHCPv4 を使用して IPv4 アドレスを取得し、IPv6 ステートレスを使用して IPv6 アドレスを取得しようとします。

▼ CLI を使用して IPv4 と IPv6 の設定を構成する

1. ILOM SP CLI または CMM CLI にログインします。
サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を確立します。
2. 使用しているネットワーク環境に適用するネットワーク構成の手順を実行します。
 - IPv4 ネットワーク設定を構成するには、この手順の**手順 3** から**手順 5** までを実行します。
 - IPv6 ネットワーク設定を構成するには、この手順の**手順 6** から**手順 10** までを実行します。
3. IPv4 ネットワーク構成の場合、`cd` コマンドを使用してデバイスの作業用ディレクトリである `/x/network` にナビゲートします。
例:
 - ラック搭載型サーバー SP の場合、`cd /SP/network` と入力します。
 - シャーシ CMM の場合、`cd /CMM/network` と入力します。
 - シャーシブレードサーバー SP の場合、`cd /CH/BLn/network` と入力します。
 - 複数の SP ノードタイプを持つシャーシブレードサーバーの場合、`cd /CH/BLn/NodeN/network` と入力します。
4. `show` コマンドを入力して、デバイスに構成した IPv4 ネットワーク設定を表示します。
5. DHCP または静的構成の IPv4 ネットワークを設定するには、次のいずれかを実行します。
 - DHCP IPv4 ネットワーク設定を構成するには、次のプロパティの値を設定します。

プロパティ	プロパティ値の設定	説明
state	set state=enabled	IPv4 の network state はデフォルトで enabled になります。 注 - IPv4 用に DHCP ネットワークオプションを有効にするには、state を enabled に設定する必要があります。
pendingipdiscovery	set pendingipdiscovery=dhcp	IPv4 の ipdiscovery のプロパティ値は、デフォルトで dhcp に設定されます。 注 - dhcp のデフォルトのプロパティ値が static に変更されている場合は、プロパティ値を dhcp に設定する必要があります。
commitpending=	set commitpending=true	set commitpending=true と入力して、state および ipdiscovery のプロパティ値に対して行った変更を確定します。

- 静的 IPv4 ネットワーク設定を構成するには、次のプロパティの値を設定します。

プロパティ	プロパティ値の設定	説明
state	set state=enabled	IPv4 の network state はデフォルトで enabled になります。 注 - 静的 IPv4 ネットワークオプションを有効にするには、state を enabled に設定する必要があります。
pendingipdiscovery	set pendingipdiscovery=static	静的 IPv4 ネットワーク構成を有効にするには、pendingipdiscovery のプロパティ値を static に設定する必要があります。 注 - IPv4 の ipdiscovery のプロパティ値は、デフォルトで dhcp に設定されます。
pendingipaddress pendingipnetmask pendingipgateway	set pendingipaddress= <ip_address> pendingipnetmask= <netmask> pendingipgateway= <gateway>	複数の静的ネットワーク設定を割り当てるには、各プロパティ値 (IP アドレス、ネットマスク、およびゲートウェイ) に対して、set コマンドに続けて pending コマンドを入力した後、割り当てる静的な値を入力します。
commitpending=	set commitpending=true	set commitpending=true と入力して、state、ipdiscovery、および network 設定のプロパティ値に対して行った変更を確定します。

- IPv6 ネットワーク構成の場合、`cd` コマンドを使用してデバイスの作業用ディレクトリである `/x/network/ipv6` にナビゲートします。

例:

- ラック搭載型サーバー SP の場合、`cd /SP/network/ipv6` と入力します。
- シャーシ CMM の場合、`cd /CMM/network/ipv6` と入力します。
- シャーシブレードサーバー SP の場合、`cd /CH/BLn/network/ipv6` と入力します。
- 複数の SP ノードがあるシャーシブレードサーバーの場合、`cd /CH/BLn/NodeN/network/ipv6` と入力します。

- `show` コマンドを入力して、デバイスに構成した IPv6 ネットワーク設定を表示します。

たとえば、サーバー SP デバイスの IPv6 プロパティについては、次のサンプル出力を参照してください。

```
-> show

/SP/network/ipv6
Targets:

Properties:
  state = enabled
  autoconfig = stateless
  dhcpv6_server_duid = (none)
  link_local_ipaddress = fe80::214:4fff:feca:5f7e/64
  static_ipaddress = ::/128
  ipgateway = fe80::211:5dff:febe:5000/128
  pending_static_ipaddress = ::/128
  dynamic_ipaddress_1 = fec0:a:8:b7:214:4fff:feca:5f7e/64

Commands:
  cd
  show
```

注 – ILOM 3.0.14 以降で提供されているデフォルトの IPv6 `autoconfig` プロパティ値は、`autoconfig=stateless` です。ただし、使用している CMM またはサーバーに ILOM 3.0.12 がインストールされている場合、`autoconfig` のデフォルトのプロパティ値は `autoconfig=stateless_only` と表示されます。

注 – `autoconfig` プロパティが `dhcpv6_stateful` または `dhcpv6_stateless` に設定されている場合、`dhcpv6_server_duid` の読み取り専用プロパティは、DHCP 情報を取得するために ILOM で最後に使用された、DHCPv6 サーバーの DHCP 固有 ID を識別します。

8. IPv6 の自動構成オプションを設定するには、`set` コマンドを使用して次の自動構成プロパティ値を指定します。

プロパティ	プロパティ値の設定	説明
<code>state</code>	<code>set state=enabled</code>	IPv6 ネットワークの <code>state</code> は、デフォルトで <code>enabled</code> です。IPv6 の自動構成オプションを有効にするには、この <code>state</code> を <code>enabled</code> に設定する必要があります。
<code>autoconfig</code>	<code>set autoconfig=<value></code>	このコマンドの後に続けて、設定する <code>autoconf</code> 値を指定します。 次のオプションがあります。 <ul style="list-style-type: none"> • <code>stateless</code> (ILOM 3.0.14 以降で提供されるデフォルトの設定) または <code>stateless_only</code> (ILOM 3.0.12 で提供されるデフォルト設定) IPv6 ネットワークルーターから取得した IP アドレスを自動的に割り当てます。 • <code>dhcpv6_stateless</code> DHCP サーバーから取得した DNS 情報を自動的に割り当てます。 <code>dhcpv6_stateless</code> プロパティ値は ILOM 3.0.14 で使用できます。 • <code>dhcpv6_stateful</code> DHCPv6 サーバーから取得した IPv6 アドレスを自動的に割り当てます。 <code>dhcpv6_stateful</code> プロパティ値は ILOM 3.0.14 で使用できます。 • <code>disable</code> すべての自動構成プロパティ値を無効にし、リンクローカルアドレスの読み取り専用プロパティ値を設定します。

次の情報は IPv6 の `autoconfig` オプションに関連します。

- IPv6 の `auto-config` オプションは、設定すると有効になります。変更を `/network` ターゲットに対して確定する必要はありません。
- 特定のデバイスについて取得された IPv6 `auto-config` アドレスは、そのデバイスとのアクティブな ILOM セッションに影響しません。新しく取得された、自動構成されたアドレスは、`/network/ipv6` ターゲットで確認できます。
- ILOM 3.0.14 以降では、`dhcpv6_stateless` のオプションが有効になっている場合または `dhcpv6_stateful` のオプションが有効になっている場合に、同時に `stateless auto-config` オプションを有効にして動作させることができます。ただし、`dhcpv6_stateless` と `dhcpv6_stateful` の `auto-config` オプションを有効にして同時に動作させることはできません。

9. 保留中の静的 IPv6 アドレスを設定するには、次のプロパティ値を指定します。

プロパティ	プロパティ値の設定	説明
state	set state=enabled	IPv6 ネットワークの state は、デフォルトで enabled です。静的 IP アドレスを有効にするには、state を enabled に設定する必要があります。
pendingipaddress	set pending_static_ipaddress=<ip_address>/<subnet_mask_length_in_bits>	このコマンドの後に続けて、デバイスに割り当てる静的 IPv6 アドレスおよびネットマスクのプロパティ値を入力します。 IPv6 アドレスの例: fec0:a:8:b7:214:4fff:feca:5f7e/64

10. 保留中の IPv6 静的ネットワークのパラメータを確定するには、次に示す手順を実行します。

- a. cd コマンドを使用してディレクトリをデバイスの network ターゲットに変更します。

例:

- ラック搭載型サーバーの場合、cd /SP/network と入力します。
- シャーシ CMM の場合、cd /CMM/network と入力します。
- シャーシブレードサーバー SP の場合、cd /CH/BLn/network と入力します。
- 複数のノードがあるシャーシブレードサーバー SP の場合、cd /CH/BLn/Node*n*/network と入力します。

- b. 次のコマンドを入力して、IPv6 に関して変更したプロパティ値を確定します。

```
set commitpending=true
```

注 - デバイス (SP または CMM) に新しい静的 IP アドレスを割り当てると、デバイスとのアクティブな ILOM セッションがすべて終了します。ILOM にログインし直すには、新しく割り当てられた IP アドレスを使用して新しいブラウザセッションを作成する必要があります。

ILOM から IPv4 または IPv6 ネットワーク構成をテストするには、ネットワークテストツール (Ping と Ping6) を使用します。詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』を参照してください。

ユーザーアカウントの追加またはディレクトリサービスの設定

root ユーザーアカウントを使用して ILOM にログインした後、ローカルユーザーアカウントを作成するか、ディレクトリサービスを設定するかを選択できます。ILOM ユーザーアカウントとディレクトリサービスの詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

項目

説明	リンク
ユーザーアカウントを追加する方法およびユーザー役割 (権限) を割り当てる方法	<ul style="list-style-type: none">40 ページの「ユーザーアカウントを追加して権限を割り当てる」
Active Directory 用に ILOM を設定する方法	<ul style="list-style-type: none">41 ページの「Active Directory 用の ILOM の設定」
LDAP 用に ILOM を設定する方法	<ul style="list-style-type: none">45 ページの「LDAP 用に ILOM を設定する」
LDAP/SSL 用に ILOM を設定する方法	<ul style="list-style-type: none">45 ページの「LDAP/SSL 用に ILOM を設定する」
RADIUS 用に ILOM を設定する方法	<ul style="list-style-type: none">49 ページの「RADIUS 用の ILOM の設定」
新しいユーザーアカウントまたはディレクトリサービスが正常に動作していることを検証する方法	<ul style="list-style-type: none">50 ページの「新しいユーザーアカウントを使用して ILOM にログインする」
ILOM からログアウトする方法	<ul style="list-style-type: none">51 ページの「ILOM からログアウトする」

▼ ユーザーアカウントを追加して権限を割り当てる

1. ILOM CLI にログインします。
2. ローカルユーザーアカウントを追加するには、次のようにコマンドとユーザーのパスワードを入力します。

```
-> create /SP/users/username password=password
```

例:

```
-> create /SP/users/user5
```

```
Creating user...
```

```
Enter new password: *****
```

```
Enter new password again: *****
```

```
Created /SP/users/user5
```


3. 次のコマンドを入力して、ユーザーアカウントに役割を割り当てます。

```
-> set /SP/users/username role=aucr
```

例:

```
-> set /SP/users/user5 role=aucr
```

```
Set 'role' to 'aucr'
```

ユーザーアカウントの役割の説明については、[40 ページ](#)の「ユーザーアカウントを追加して権限を割り当てる」を参照してください。

▼ Active Directory 用の ILOM の設定

1. root ユーザーアカウントを使用して、ILOM の CLI にログインします。
2. show コマンドを使用して、トップレベルのプロパティを表示します。次のように入力します。

```
-> cd /SP/clients/activedirectory
/SP/clients/activedirectory

-> show

/SP/clients/activedirectory
Targets:
  admingroups
  alternateservers
  cert
  customgroups
  dnslocatorqueries
  opergroups
  userdomains

Properties:
  address = 10.5.121.321
  defaultrole = Administrator
  dnslocatormode = enabled
  logdetail = trace
  port = 0
  state = disabled
  strictcertmode = disabled
  timeout = 4

Commands:
  cd
  set
  show
```

3. show コマンドを使用して、テーブルの情報を表示します。次のように入力します。

```
-> show /SP/clients/activedirectory/name/n
```

n は 1 ~ 5、*name* は次のいずれかです。

- **admingroups** (Admin Groups のプロパティーの場合)
- **opergroups** (Operator Groups のプロパティーの場合)
- **customgroups** (Custom Groups のプロパティーの場合)
- **userdomains** (User Domains のプロパティーの場合)
- **alternateservers** (Alternate Servers のプロパティーの場合)
- **dnslocatorqueries** (DNS Locator Queries のプロパティーの場合)
- **cert** (証明書のプロパティーの場合 - cert はテーブルではないため、*n* の値 1 から 5 は適用されません)

show コマンドを使用して、証明書のプロパティーを取得することもできます。

```
-> show /SP/clients/activedirectory/cert
```

```
/SP/clients/activedirectory/cert
```

```
Targets:
```

```
Properties:
```

```
certstatus = certificate not present  
clear_action = (none)  
issuer = (none)  
load_uri = (none)  
serial_number = (none)  
subject = (none)  
valid_from = (none)  
valid_until = (none)  
version = (none)
```

また、次の show コマンドを使用して、代替サーバーの証明書のプロパティーを取得することもできます。

```
-> show /SP/clients/activedirectory/alternateservers/1/cert
```

```
/SP/clients/activedirectory/alternateservers/1/cert
```

```
Targets:
```

```
Properties:
```

```
certstatus = certificate not present  
clear_action = (none)  
issuer = (none)  
load_uri = (none)  
serial_number = (none)  
subject = (none)  
valid_from = (none)  
valid_until = (none)  
version = (none)
```

4. set コマンドを使用して、トップレベルのプロパティを設定します。

例:

```
-> set address=10.5.121.321
Set 'address' to 10.5.121.321
->set ...etc. for defaultrole, dnslocator, logdetail, port, state,
stricmode, timeout
```

5. set コマンドを使用して、証明書をロードするかプロパティを変更します。

例:

- Active Directory 証明書をロードするには、次のように入力します。

```
-> set /SP/clients/activedirectory/cert load_uri=
tftp://10.6.143.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.143.192/sales/cert.cert'
```

- 代替サーバーの証明書をロードするには、次のように入力します。

```
-> set /SP/clients/activedirectory/alternateservers/1/cert
load_uri=tftp://10.6.143.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.143.192/sales/cert.cert'
```

- Admin Groups テーブルのプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/activedirectory/admingroups/1 name=CN=
spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=
com'
```

- Operator Groups テーブルのプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/activedirectory/opergroups/1 name=CN=
spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=
com'
```

- Custom Groups テーブルのプロパティを変更するには、次のように入力します。

注 - 役割は、Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、Read Only (o) のうちのいずれか、またはこれらの組み合わせに設定できます。旧バージョンの Administrator 役割または Operator 役割もサポートされています。

```
-> set /SP/clients/activedirectory/customgroups/1 name=CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com'
-> set /SP/clients/activedirectory/customgroups/1 roles=au
Set 'roles' to au
```

- User Domains テーブルのプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/activedirectory/userdomains/1 domain=username@sales.oracle.com
Set 'domain' to 'username@sales.oracle.com'
```

- Alternate Servers テーブルのプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/activedirectory/alternateservers/1 address=ip_address
```

- DNS Locator Queries テーブルのプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/activedirectory/dnslocatorqueries/1 service=_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
```

DNS ロケータサービスクエリーは、DNS の名前付きのサービスを特定します。レコードには通常ポート番号が含まれますが、<PORT:636> という形式でオーバーライドできます。また、<DOMAIN> 置換マーカーを使用して、認証対象のドメイン固有のネームサービスを指定できます。

名前	ドメイン
1	_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
2	_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>

▼ LDAP 用に ILOM を設定する

1. ILOM CLI にログインします。
2. `set` コマンドを使用して、プロキシユーザー名とパスワードを入力します。
例:

```
-> set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales, dc=oracle, dc=com" bindpw=password
```
3. LDAP サーバーの IP アドレスまたは DNS 名を入力します。次のように入力します。

```
-> set /SP/clients/ldap address=ldap_ipaddress|DNS_name
```
4. (省略可能) LDAP サーバーとの通信に使用するポートを割り当てます。デフォルトのポートは 389 です。次のように入力します。

```
-> set /SP/clients/ldap port=ldap_port
```
5. ユーザーとグループを含む LDAP ツリー分岐の識別名を入力します。次のように入力します。

```
-> set /SP/clients/ldap searchbase="ou=people, ou=sales, dc=oracle, dc=com"
```

これは、ユーザー認証を検索する LDAP ツリーの場所です。
6. LDAP サービスの状態を `enabled` に設定します。次のように入力します。

```
-> set /SP/clients/ldap state=enabled
```
7. LDAP 認証の動作を確認するには、LDAP ユーザー名とパスワードを使用して、ILOM にログインします。

注 - ILOM は、LDAP ユーザーの前にローカルユーザーを検索します。LDAP ユーザー名がローカルユーザーとして存在する場合は、ILOM は認証にローカルアカウントを使用します。

▼ LDAP/SSL 用に ILOM を設定する

LDAP/SSL は、Secure Socket Layer (SSL) テクノロジーを使用して強化されたセキュリティを LDAP ユーザーに提供します。厳密な証明書モードが使われている場合は、証明書は省略可能です。

次の手順に従って、LDAP/SSL に対して ILOM を設定します。

1. ILOM CLI にログインします。

2. show コマンドを使用して、トップレベルのプロパティを表示します。次のように入力します。

```
-> cd /SP/clients/ldapssl
/SP/clients/ldapssl

-> show

/SP/clients/ldapssl
  Targets:
    admingroups
    alternateservers
    cert
    customgroups
    opergroups
    userdomains

  Properties:
    address = 10.5.121.321
    defaultrole = Administrator
    logdetail = trace
    port = 0
    state = disabled
    strictcertmode = disabled
    timeout = 4

  Commands:
    cd
    set
    show
```

3. show コマンドを使用して、テーブルの情報を表示します。次のように入力します。

```
-> show /SP/clients/ldapssl/name/n
```

n は 1 ~ 5、*name* は次のいずれかです。

- **admingroups** (Admin Groups のプロパティの場合)
- **opergroups** (Operator Groups のプロパティの場合)
- **customgroups** (Custom Groups のプロパティの場合)
- **userdomains** (User Domains のプロパティの場合)
- **alternateservers** (Alternate Servers のプロパティの場合)
- **cert** (証明書のプロパティの場合 - cert はテーブルではないため、*n* の値 1 から 5 まででは適用されません)

show コマンドを使用して、証明書のプロパティを取得することもできます。

```
-> show /SP/clients/ldapssl/cert
/SP/clients/ldapssl/cert
Targets:

Properties:
  certstatus = certificate not present
  clear_action = (none)
  issuer = (none)
  load_uri = (none)
  serial_number = (none)
  subject = (none)
  valid_from = (none)
  valid_until = (none)
  version = (none)
```

また、次の show コマンドを使用して、代替サーバーの証明書のプロパティを取得することもできます。

```
-> show /SP/clients/ldapssl/alternateservers/1/cert
/SP/clients/ldapssl/alternateservers/1/cert
Targets:

Properties:
  certstatus = certificate not present
  clear_action = (none)
  issuer = (none)
  load_uri = (none)
  serial_number = (none)
  subject = (none)
  valid_from = (none)
  valid_until = (none)
  version = (none)
```

4. set コマンドを使用して、トップレベルのプロパティを設定します。

例:

```
-> set address=10.5.121.321
Set 'address' to 10.5.121.321
->set ...etc. for defaultrole, logdetail, port, state, strictmode,
timeout
```

5. set コマンドを使用して、証明書をロードするかプロパティを変更します。

例:

- LDAP/SSL 証明書をロードするには、次のように入力します。

```
-> set /SP/clients/ldapssl/cert load_uri=  
tftp://10.6.142.192/sales/cert.cert  
Set 'load_uri' to 'tftp://10.6.142.192/sales/cert.cert'
```

- 代替サーバーの証明書をロードするには、次のように入力します。

```
-> set /SP/clients/ldapssl/alternateservers/1/cert load_uri=  
tftp://10.6.142.192/sales/cert.cert  
Set 'load_uri' to 'tftp://10.6.142.192/sales/cert.cert'
```

- Admin Groups のプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/ldapssl/admingroups/1 name=CN=  
spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com  
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=  
com'
```

- Operator Groups のプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/ldapssl/opergroups/1 name=CN=spSuperOper,OU=  
Groups,DC=sales,DC=oracle,DC=com  
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=  
com'
```

- Custom Groups のプロパティを変更するには、次のように入力します。

注 – 役割は、Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、Read Only (o) のうちのいずれか、またはこれらの組み合わせに設定できます。旧バージョンの Administrator 役割または Operator 役割もサポートされています。

```
-> set /SP/clients/ldapssl/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=
com'
-> set /SP/clients/ldapssl/customgroups/1 roles=au
Set 'roles' to au
```

- User Domains のプロパティを変更するには、次のように入力します。

注 – 次の例の <USERNAME> は、ユーザーのログイン名を表します。認証の際、<USERNAME> はユーザーのログイン名に置き換えられます。

```
-> set /SP/clients/ldapssl/userdomains/1 name=<USERNAME>@uid=
<USERNAME>,OU=people,DC=oracle,DC=com
Set 'domain' to 'uid=<USERNAME>,OU=people,DC=oracle,DC=com'
```

- Alternate Servers のプロパティを変更するには、次のように入力します。

```
-> set /SP/clients/ldapssl/alternateservers/1 address=ip_address
```

▼ RADIUS 用の ILOM の設定

1. ILOM CLI にログインします。
2. RADIUS のプロパティを表示するには、次のように入力します。

```
-> show /SP/clients/radius
```

例:

```
-> show /SP/clients/radius
/SP/clients/radius
Targets:

Properties:
  address = 0.0.0.0
  defaultrole = Operator
  port = 1812
  secret = (none)
  state = disabled
```

3. `set` コマンドを使用してプロパティを変更します。

例:

```
-> set /SP/clients/radius ipaddress=1.2.3.4 port=1812 state=
enabled defaultrole=administrator secret=changeme
```

RADIUS の設定の説明については、49 ページの「RADIUS 用の ILOM の設定」を参照してください。

▼ 新しいユーザーアカウントを使用して ILOM にログインする

この手順を使用して ILOM にログインし、`root` 以外のユーザーアカウントが正常に機能しているか検証します。

次の手順に従って、`root` 以外のアカウントユーザーとして ILOM にログインします。

1. Secure Shell (SSH) セッションを使用し、ユーザー名と、サーバー SP または CMM の IP アドレスを指定して、ILOM にログインします。

```
$ ssh root@system_ipaddress
```

または

```
$ ssh -l username ipaddress
```

ILOM がデュアルスタックネットワーク環境で動作している場合は、IPv4 または IPv6 のいずれかのアドレス形式を使用して `system_ipaddress` を入力できます。

例:

IPv4 の場合 – 10.8.183.106

または

IPv6 の場合 – [fec0:a:8:b7:214:4fff:5eca:5f7e/64]

ILOM ログインプロンプトが表示されます。

デュアルスタック環境での IP アドレスの入力の詳細、および接続の問題の診断については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

2. ユーザーアカウントのユーザー名とパスワードを入力します。

```
<hostname>: <assigned_username>
```

```
Password: <assigned_password>
```

ILOM CLI のプロンプト (->) が表示されます。

▼ ILOM からログアウトする

- コマンドプロンプトで、次のように入力します。

```
-> exit
```

次の手順

次に、使用しているシステムおよびデータセンターの環境に対して ILOM 設定のカスタマイズを続行することができます。使用している環境に合わせて ILOM を設定する前に、『Oracle Integrated Lights Out Manager 3.0 概念ガイド』を参照して、ILOM 3.0 の新しい特長と機能の概要を確認してください。ILOM の新機能の使用している環境に対する影響を知ること、使用しているシステムやデータセンターで ILOM のすべての機能にアクセスできるように ILOM を設定するときに役に立ちます。

各ユーザーインターフェースを使用した ILOM タスクの実行方法については、『Oracle ILOM 3.0 手順ガイド』を参照してください。プラットフォーム固有の設定手順については、使用しているプラットフォームの ILOM 補足マニュアルまたはプラットフォームの管理ガイドを参照してください。

ILOM 3.0 の各種マニュアルは以下のサイトで参照できます。

<http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic>

第4章

ILOM ファームウェア

項目	
説明	リンク
ILOM ファームウェアのバージョンの識別	• 54 ページの「ILOM バージョン情報の識別」
ILOM ファームウェアの更新	• 55 ページの「ILOM ファームウェアの最新バージョンへの更新」

ILOM バージョン情報の識別

サーバー SP 上で動作している ILOM ファームウェアのバージョンは簡単に識別できません。ILOM ファームウェアのバージョンを識別するには、Read Only (o) 役割を有効にする必要があります。

▼ Web インタフェースを使用して ILOM のバージョンを識別する

1. ILOM Web インタフェースにログインします。
2. 「System Information」 --> 「Version」 を選択します。
現在のファームウェアのバージョン情報が表示されます。

▼ CLI を使用して ILOM のバージョンを識別する

1. ILOM の CLI にログインします。
2. コマンドプロンプトで、`version` と入力します。
現在のファームウェアのバージョン情報が表示されます。例:

```
SP firmware 3.0.0.1
SP firmware build number: 38000
SP firmware date: Fri Nov 28 14:03:21 EDT 2008
SP filesystem version: 0.1.22
```

ILOM ファームウェアの最新バージョンへの更新

ILOM Web インタフェースまたは CLI を使用して ILOM ファームウェアを更新できます。次の節を参照してください。

- 56 ページの「Web インタフェースを使用して ILOM ファームウェアを更新する」
- 58 ページの「CLI を使用して ILOM ファームウェアを更新する」

インストールを開始する前に

この節の手順を実行する前に、次の要件を確認してください。

- システム上で現在動作している ILOM のバージョンを識別します。
- プラットフォームの製品 Web サイトから、使用しているサーバーまたは CMM のファームウェアイメージをダウンロードします。詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』または『Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』のファームウェアの更新に関する節を参照してください。
- サポートされているプロトコル (TFTP、FTP、HTTP、HTTPS) を使用してファームウェアイメージをサーバーにコピーします。CLI で更新する場合は、ローカルサーバーにイメージをコピーします。Web インタフェースで更新する場合は、Web ブラウザが動作しているシステムにイメージをコピーします。
- プラットフォームで必要になる場合は、サーバー SP のファームウェアを更新する前に、ホストオペレーティングシステムを停止します。
- Admin (a) 役割のアカウント権限をもつ ILOM ユーザー名とパスワードを取得します。システム上でファームウェアを更新するには、Admin (a) 権限が必要です。
- ファームウェアの更新プロセスの完了には、約 6 分かかります。この間、ほかの ILOM タスクを実行しないでください。ファームウェアの更新が完了すると、システムが再起動します。

▼ Web インタフェースを使用して ILOM ファームウェアを更新する

1. Admin (a) 役割のアカウント権限をもつユーザーとして、ILOM の Web インタフェースにログインします。
2. 「Maintenance」 --> 「Firmware Upgrade」を選択します。
「Firmware Upgrade」ページが表示されます。
3. 「Firmware Upgrade」ページで、「Enter Upgrade Mode」をクリックします。
更新プロセスが完了すると、ログインしているほかのユーザーのセッションが切断されることを示す「Upgrade Verification」ダイアログが表示されます。
4. 「Upgrade Verification」ダイアログで、「OK」をクリックして続行します。
「Firmware Upgrade」ページが表示されます。
5. 「Firmware Upgrade」ページで、次の手順を実行します。
 - a. 次のいずれかの手順を実行して、イメージの位置を指定します。
 - 「Browse」をクリックして、インストールするファームウェアイメージの位置を選択します。
 - 使用しているシステムでサポートされている場合は、「Specify URL」をクリックし、ファームウェアイメージの位置を示す URL を指定します。テキストボックスに URL を入力します。
 - b. 「Upload」ボタンをクリックして、ファイルをアップロードし検証します。
ファイルがアップロードされ検証されるまで待ちます。
「Firmware Verification」ページが表示されます。
6. 「Firmware Verification」ページで、次のいずれかのオプションを有効にします。
 - **Preserve Configuration:** ILOM の設定を保存し更新プロセスの完了後に復元する場合は、このオプションを有効にします。
 - **Delay BIOS upgrade until next server power-off:** システムが次に再起動するまで BIOS アップグレードを延期する場合は、このオプションを有効にします。

注 – BIOS についてのプロンプトは、現在 ILOM 3.x ファームウェアリリースが動作している x86 システムでのみ表示されます。このプロンプトで「はい」(y) と答えると、システムが次に再起動するまで、BIOS アップグレードが延期されます。このプロンプトで「いいえ」(n) と答えると、SP ファームウェアの更新時に、必要に応じて自動的に BIOS が更新されます。

BIOS を更新するように選択した場合、現在の BIOS 設定は自動的に上書きされ、出荷時のデフォルトの BIOS 設定が割り当てられます。

7. 「Start Upgrade」をクリックして、アップグレードプロセスを開始するか、「Exit」をクリックしてプロセスを取り消します。
「Start Upgrade」をクリックすると、アップグレードプロセスが開始され、プロセスの続行を確認するプロンプトが表示されます。
8. プロンプトで「OK」をクリックして続行します。
「Update Status」ページが表示され、更新の進捗状況が表示されます。更新の進捗状況が 100% を示すと、ファームウェアの更新は完了です。
更新が完了すると、システムが自動的に再起動します。

注 – 更新の完了後、ILOM の Web インタフェースが正しく再表示されないことがあります。ILOM の Web ページで情報が欠落している場合やエラーメッセージが表示される場合は、更新前のバージョンのキャッシュされているページが表示されている可能性があります。ブラウザのキャッシュをクリアしてブラウザを再表示してから、続行してください。

9. 手順 1 で入力したユーザー名とパスワードを使用して、ILOM Web インタフェースに再接続します。
ファームウェアの更新前に ILOM 設定を保存しなかった場合、初期 ILOM セットアップ手順を実行して ILOM に再接続する必要があります。
10. 正しいファームウェアバージョンがインストールされていることを検証します。
「System Information」 --> 「Version」を選択します。
SP または CMM のファームウェアバージョンが、インストールしたファームウェアイメージのバージョンと一致している必要があります。

▼ CLI を使用して ILOM ファームウェアを更新する

1. Admin (a) 役割のアカウント権限をもつユーザーとして、ILOM CLI にログインします。
2. ファームウェアを更新するためにネットワークに接続されていることを確認します。

例:

- サーバー SP のネットワーク接続を検証するには、次のように入力します。
-> **show /SP/network**
- CMM のネットワーク接続を検証するには、次のように入力します。
-> **show /CMM/network**

3. 次のコマンドを入力して、ILOM ファームウェアイメージをロードします。

```
-> load -source <supported_protocol>://<server_ipaddress>/<path_to_firmware_image>/<filename.xxx>
```

ファームウェア更新プロセスについての注意が表示され、続いてイメージのロードのためのメッセージプロンプトが表示されます。この注意の内容は、使用しているプラットフォームによって異なります。

4. 指定したファイルのロードについてのプロンプトで、「はい」の場合は **y**、「いいえ」の場合は **n** を入力します。

設定の保存を確認するプロンプトが表示されます。

例:

```
Do you want to preserve the configuration (y/n)?
```

5. 設定の保存についてのプロンプトで、「はい」の場合は「**y**」、「いいえ」の場合は「**n**」を入力します。

ILOM の既存の設定を保存して更新プロセスの完了後に復元する場合は、「**y**」と入力します。

注 – 設定の保存についてのプロンプトで「**n**」と入力すると、プラットフォーム固有のプロンプトが表示されます。

6. 次のいずれかの手順を実行します。

- システムに 2.x ファームウェアリリースがインストールされている場合、システムは特別なモードに入って、新しいファームウェアをロードします。その後、システムが自動的に再起動し、ファームウェアの更新が完了します。手順 7 に進みます。
- SPARC システムに 3.x ファームウェアリリースがインストールされている場合、システムは特別なモードに入って、新しいファームウェアをロードします。その後、システムが自動的に再起動し、ファームウェアの更新が完了します。手順 7 に進みます。
- x86 システムに 3.x ファームウェアリリースがインストールされている場合は、BIOS 更新の延期を確認するプロンプトが表示されます。

例:

```
Do you want to force the server off if BIOS needs to be upgraded  
(y/n)?
```

- a. BIOS 更新の延期についてのプロンプトで、「はい」の場合は y、「いいえ」の場合は n を入力します。

システムは、特別なモードに入って、新しいファームウェアをロードし、自動的に再起動してファームウェアの更新を完了します。

注 – BIOS についてのプロンプトは、現在 ILOM 3.x ファームウェアリリースが動作している x86 システムでのみ表示されます。このプロンプトで「はい」(y) と答えると、システムが次に再起動するまで、BIOS アップグレードが延期されます。このプロンプトで「いいえ」(n) と答えると、SP ファームウェアの更新時に、必要に応じて自動的に BIOS が更新されます。

BIOS を更新するように選択した場合、現在の BIOS 設定は自動的に上書きされ、出荷時のデフォルトの BIOS 設定が割り当てられます。

- b. 手順 7 に進みます。

7. 手順 1 で入力したユーザー名とパスワードを使用して、SSH 接続経由で ILOM サーバーの SP または CMM に再接続します。

ファームウェアの更新前に ILOM 設定を保存しなかった場合、初期 ILOM セットアップ手順を実行して ILOM に再接続する必要があります。

8. 正しいファームウェアバージョンがインストールされていることを検証します。CLI プロンプトで、次のように入力します。

```
-> version
```

SP または CMM のファームウェアバージョンが、インストールしたファームウェアイメージのバージョンと一致している必要があります。

