

Integrated Lights Out Manager (ILOM) 3.0 入門ガイド





Integrated Lights Out Manager (ILOM) 3.0 入門ガイド

Copyright 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

本書には、富士通株式会社により提供および修正された技術情報が含まれています。

Sun Microsystems, Inc. および富士通株式会社は、それぞれ本書に記述されている製品および技術に関する知的所有権を所有または管理しています。これらの製品、技術、および本書は、著作権法、特許権などの知的所有権に関する法律および国際条約により保護されています。これらの製品、技術、および本書に対して Sun Microsystems, Inc. および富士通株式会社が有する知的所有権には、<http://www.sun.com/patents> に掲載されているひとつまたは複数の米国特許、および米国ならびにその他の国におけるひとつまたは複数の特許または出願中の特許が含まれています。

本書およびそれに付属する製品および技術は、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。富士通株式会社と Sun Microsystems, Inc. およびそのライセンサーの書面による事前の許可なく、このような製品または技術および本書のいかなる部分も、いかなる方法によっても複製することが禁じられます。本書の提供は、明示的であるか黙示的であるかを問わず、本製品またはそれに付随する技術に関するいかなる権利またはライセンスを付与するものでもありません。本書は、富士通株式会社または Sun Microsystems, Inc. の一部、あるいはそのいずれかの関連会社のいかなる種類の義務を含むものでも示すものでもありません。

本書および本書に記述されている製品および技術には、ソフトウェアおよびフォント技術を含む第三者の知的財産が含まれている場合があります。これらの知的財産は、著作権法により保護されているか、または提供者から富士通株式会社および / または Sun Microsystems, Inc. ヘラライセンスが付与されているか、あるいはその両方です。

GPL または LGPL が適用されたソースコードの複製は、GPL または LGPL の規約に従い、該当する場合に、一般ユーザーからの申し込みに応じて入手可能です。富士通株式会社または Sun Microsystems, Inc. にお問い合わせください。

この配布には、第三者が開発した構成要素が含まれている可能性があります。

本製品の一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

Sun, Sun Microsystems, Sun のロゴ, Java, Netra, Solaris, Sun StorEdge, docs.sun.com, OpenBoot, SunVTS, SunSolve, CoolThreads, J2EE および Sun Fire は、米国およびその他の国における Sun Microsystems, Inc. の商標または登録商標です。

富士通および富士通のロゴマークは、富士通株式会社の登録商標です。

すべての SPARC 商標は、SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における登録商標です。SPARC 商標が付いた製品は、Sun Microsystems, Inc. が開発したアーキテクチャーに基づくものです。

SPARC64 は、Fujitsu Microelectronics, Inc. および富士通株式会社が SPARC International, Inc. のライセンスを受けて使用している同社の商標です。

SSH は、米国およびその他の特定の管轄区域における SSH Communications Security の登録商標です。

OPEN LOOK および Sun™ Graphical User Interface は、Sun Microsystems, Inc. が自社のユーザーおよびライセンス実施権者向けに開発しました。Sun Microsystems, Inc. は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザーインタフェースの概念の研究開発における Xerox 社の先駆者としての成果を認めるものです。Sun Microsystems, Inc. は Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは、OPEN LOOK GUI を実装しているかまたは Sun の書面によるライセンス契約を満たす Sun Microsystems, Inc. のライセンス実施権者にも適用されます。

United States Government Rights - Commercial use. U.S. Government users are subject to the standard government user license agreements of Sun Microsystems, Inc. and Fujitsu Limited and the applicable provisions of the FAR and its supplements.

免責条項：本書または本書に記述されている製品や技術に関して富士通株式会社、Sun Microsystems, Inc. またはそのいずれかの関連会社が行う保証は、製品または技術の提供に適用されるライセンス契約で明示的に規定されている保証に限り、このような契約で明示的に規定された保証を除き、富士通株式会社、Sun Microsystems, Inc. およびそのいずれかの関連会社は、製品、技術、または本書に関して、明示、黙示を問わず、いかなる種類の保証も行いません。これらの製品、技術、または本書は、現状のまま提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も、かかる免責が法的に無効とされた場合を除き、行われたいものとします。このような契約で明示的に規定されていないかぎり、富士通株式会社、Sun Microsystems, Inc. またはそのいずれかの関連会社は、いかなる法理論のもとで第三者に対しても、その収益の損失、有用性またはデータに関する損失、あるいは業務の中断について、あるいは間接的損害、特別損害、付随的損害、または結果的損害について、そのような損害の可能性が示唆されていた場合であっても、適用される法律が許容する範囲内で、いかなる責任も負いません。

本書は、「現状のまま」提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も、かかる免責が法的に無効とされた場合を除き、行われたいものとします。

原典:	Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide Manual Code: C120-E576-01EN
-----	-----------------------------------------------------------------------------------------------

目次

はじめに	v
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
root アカウントの使用	2
Web インタフェースまたは CLI の使用	3
初期 ILOM セットアップの計画	4
ILOM への接続	6
▼ DHCP を使用した SP ネットワークの設定	6
▼ BIOS を使用した SP ネットワークの設定	7
▼ シリアル接続を使用した静的ネットワーク設定	7
▼ IPMItool を使用したネットワークの設定	8
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
▼ root ユーザーアカウントを使用した ILOM 3.0 へのログイン	10
作業を開始する前に	10
▼ ユーザーアカウントの追加と権限の割り当て	11
▼ IActive Directory 用の LOM の設定	13
▼ LDAP サーバの設定	19
▼ LDAP 用の ILOM の設定	20

- ▼ LDAP/SSL の用の ILOM の設定 21
- ▼ LDAP/SSL テーブルの編集 25
- ▼ RADIUS の用の ILOM の設定 26
- ▼ ユーザーとして ILOM へのログイン 27
 - 作業を開始する前に 27
- ▼ ILOM からのログアウト 28
- CLI を使用した ILOM の初期セットアップ手順 28
 - ▼ root ユーザーアカウントを使用した ILOM 3.0 へのログイン 29
 - ▼ ユーザーアカウントの追加と権限の割り当て 29
 - ▼ Active Directory の用の ILOM の設定 30
 - ▼ LDAP サーバの設定 34
 - ▼ LDAP 用の ILOM の設定 34
 - ▼ LDAP/SSL の用の ILOM の設定 35
 - ▼ RADIUS の用の ILOM の設定 38
 - ▼ ユーザーとして ILOM へのログイン 39
 - ▼ ILOM からのログアウト 40
- ILOM バージョン情報の識別 40
 - ▼ Web インタフェースを使用した ILOM バージョンの識別 40
 - ▼ CLI を使用した ILOM バージョンの識別 40
- ILOM ファームウェアの最新バージョンへの更新 41
 - 作業を開始する前に 41
 - ▼ 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 41
 - ▼ CLI を使用して ILOM ファームウェアを更新する 43
- 次の手順 44

はじめに

『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』では、システムではじめて ILOM にアクセスするために必要な手順を実行する方法について説明します。説明する手順には、ILOM ネットワークの接続、ログイン、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。

本書は、ネットワークングの概念および基本的なシステム管理プロトコルについての知識があるシステム管理者を対象にしています。

注 – 本書の説明は、ILOM をサポートするサーバに限定されます。「すべてのサーバプラットフォーム」という説明は、ILOM をサポートしている富士通製のすべてのサーバを指します。使用するサーバによっては、ILOM の一部の機能がサポートされていないことがあります。ILOM の補足マニュアルと各サーバのプロダクトノートを事前に確認してください。

安全な使用のために

このマニュアルには当製品を安全に使用していただくための重要な情報が記載されています。当製品を使用する前に、このマニュアルを熟読してください。また、このマニュアルは大切に保管してください。

富士通は、使用者および周囲の方の身体や財産に被害を及ぼすことなく安全に使っていただくために細心の注意を払っています。本製品を使用する際は、マニュアルの説明に従ってください。

関連マニュアル

本書で説明されている情報を完全に理解するには、本書を次の表に示すマニュアルと一緒に使用することをお勧めします。SPARC Enterprise シリーズのすべてのマニュアルの最新版は、次の Web サイトから入手できます。

グローバルサイト

<http://www.fujitsu.com/sparcenterprise/manual/>

日本語サイト

<http://primeserver.fujitsu.com/sparcenterprise/manual/>

まず、『ILOM 3.0 概念ガイド』を読み、ILOM の特徴と機能を理解してください。ILOM がサポートしている新しいシステムをセットアップするには、『ILOM 3.0 入門ガイド』を参照してください。ここでは、ネットワークに接続する手順、ILOM への初回ログイン手順、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手順が記載されています。その後、その他の ILOM タスクを実行するために使用する ILOM インタフェースを決定してください。インタフェースが決定したら、選択したインタフェース用の ILOM 3.0 手順ガイドを参照してください。

次の表に、ILOM 3.0 に関する各種マニュアルを示します。

タイトル	説明	コード
Integrated Lights Out Manager (ILOM) 3.0 概念ガイド	ILOM の特徴および機能に関する情報	C120-E573
Integrated Lights Out Manager (ILOM) 3.0 入門ガイド	ネットワーク接続、ILOM への初回ログイン、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に関する情報および手順	C120-E576
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情報および手順	C120-E574
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情報および手順	C120-E575
Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド	SNMP または IPMI 管理ホストを使用して ILOM 機能にアクセスするための情報および手順	C120-E579

ILOM 3.0 の各種マニュアルに加えて、関連する ILOM 補足マニュアルに、使用しているサーバプラットフォームに固有の ILOM 機能およびタスクが記載されています。ILOM 3.0 の各種マニュアルと、使用しているサーバプラットフォームに付属の ILOM 補足マニュアルと一緒に使用してください。

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体系が採用されています。この番号体系では、たとえば、a.b.c.d.e のように、5 つのフィールドを持つ文字列が使用されます。

- a – ILOM のメジャーバージョンを表します。
- b – ILOM のマイナーバージョンを表します。
- c – ILOM の更新バージョンを表します。
- d – ILOM のマイクロバージョンを表します。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グループごとに管理されます。詳細については、使用しているプラットフォームのプロダクトノートを参照してください。
- e – ILOM のナノバージョンを表します。ナノバージョンは、マイクロバージョンの増分イテレーションです。

たとえば、ILOM 3.1.2.1.a は、次のような意味になります。

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

製品識別情報

製品識別情報により、システムは、それ自体を登録し、その識別情報に関連付けられたサービス契約に基づいて特定の自動サービスを使用できるようになります。製品識別情報を使用すると、システムを特定することができます。また、システムに関するサービスを依頼する際には、保守担当者に製品識別情報を提供する必要があります。製品識別情報には、次の情報が含まれます。

- `product_name`: 製品の販売名。
- `product_part_number`: 製品が固有のシリアル番号を持つように製造時に割り当てられるネームスペース。同じ製品パーツ番号が複数の製品に割り当てられることはありません。「602-3098-01」などです。
- `product_serial_number`: 製造時に製品の各インスタンスに割り当てられる固有の識別情報。「0615AM0654A」などです。
- `product_manufacturer`: 製品の製造元。「FUJITSU」などです。

表 P-1 では、ILOM で使用される共通の製品識別情報について説明します。

表 P-1 共通の製品識別情報

必要な情報	ターゲット	最小プロパティ
サーバ (ラック搭載型およびブレード) に関する基本製品情報	/SYS	<code>product_name</code> <code>product_part_number</code> <code>product_serial_number</code> <code>product_manufacturer</code>
シャーシ監視モジュール (Chassis Monitoring Module、CMM) に関する基本製品情報	/CH	<code>product_name</code> <code>product_part_number</code> <code>product_serial_number</code> <code>product_manufacturer</code>
ブレードに関する基本シャーシ情報	/SYS/MIDPLANE	<code>product_name</code> <code>product_part_number</code> <code>product_serial_number</code> <code>product_manufacturer</code>
シャーシ内でのブレードの位置	/SYS/SLOTID	<code>type</code> <code>class</code> <code>value</code>
ラック内でのシャーシの位置	/CH	<code>rack_location</code>

書体と記号について

書体または記号*	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	% su Password:
AaBbCc123	コマンド行の可変部分。実際の名前や値と置き換えてください。	rm <i>filename</i> と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	「ILOM の使用を開始する」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	% grep `^#define \ XV_VERSION_STRING`

* 使用しているブラウザにより、これらの設定と異なって表示される場合があります。

ご意見をお寄せください

本書に関するご意見、ご要望または内容に不明確な部分がありましたら、マニュアル番号、マニュアル名称、ページおよび具体的な内容を下記 URL の『お問い合わせ』から送付してください。

SPARC Enterprise マニュアルのサイト

<http://primeserver.fujitsu.com/sparcenterprise/manual/>

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」• 2 ページの「root アカウントの使用」• 3 ページの「Web インタフェースまたは CLI の使用」• 4 ページの「初期 ILOM セットアップの計画」
ILOM をネットワークに接続して IP アドレスを割り当てます。	<ul style="list-style-type: none">• 6 ページの「ILOM への接続」
ILOM の Web インタフェースを使用してログインし、ユーザーアカウントをセットアップし、ILOM を設定して、ログアウトします。	<ul style="list-style-type: none">• 9 ページの「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」
ILOM の CLI を使用してログインし、ユーザーアカウントをセットアップし、ILOM を設定して、ログアウトします。	<ul style="list-style-type: none">• 28 ページの「CLI を使用した ILOM の初期セットアップ手順」
使用している ILOM ファームウェアのバージョンを識別し、ファームウェアを更新します。	<ul style="list-style-type: none">• 40 ページの「Web インタフェースを使用した ILOM バージョンの識別」• 40 ページの「CLI を使用した ILOM バージョンの識別」• 41 ページの「ILOM ファームウェアの最新バージョンへの更新」
それ以降の ILOM 設定の各ステップに関する情報を確認します。	<ul style="list-style-type: none">• 44 ページの「次の手順」

このガイドについて

『Integrated Lights Out Manager (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、使用しているシステムを、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、ILOM の接続方法と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。これらのマニュアルの一覧は、「はじめに」の表 P-1 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。

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。

- User name: **root**
- Password: **changeme**

承認されていないアクセスからシステムを保護するために、システムに取り付けられている各サービスプロセッサ (Service Processor、SP) またはシャーシ監視モジュール (Chassis Monitoring Module、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別の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、事前構成されたもう 1 つのアカウントである default 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は、『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』を参照してください。

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 つの部分に分かれています。前半では、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。後半では、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。

初期 ILOM セットアップの計画

ここでは、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 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
ネットワークアクセスについての ILOM の設定		
ILOM への接続	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。	使用しているプラットフォームのマニュアル
ネットワークの設定	ネットワーク設定の方法は、使用しているサーバプラットフォームによって異なります。 <ul style="list-style-type: none">• DHCP を使用する – すべてのプラットフォーム• シリアルログインを使用する – すべてのプラットフォーム• BIOS を使用する – x64 ベースのサーバまたはサーバモジュール• ホスト OS 上で実行する IPMItool を使用する – x64 ベースのサーバまたはサーバモジュール• シャーシ監視モジュール (Chassis Monitoring Module, CMM) を使用する – サーバモジュール (ブレード) システムのみ	6 ページの「DHCP を使用した SP ネットワークの設定」 7 ページの「シリアル接続を使用した静的ネットワーク設定」
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	システ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。 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。 <ul style="list-style-type: none">• User name: root• Password: changeme	10 ページの「root ユーザーアカウントを使用した ILOM 3.0 へのログイン」 (web) 29 ページの「root ユーザーアカウントを使用した ILOM 3.0 へのログイン」 (CLI)
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。	11 ページの「ユーザーアカウントの追加と権限の割り当て」 (web) 29 ページの「ユーザーアカウントの追加と権限の割り当て」 (CLI)
Active Directory 用の ILOM の設定	Active Directory を使用するには、主サーバ、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、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。	13 ページの「Active Directory 用の ILOM の設定」 (web) 30 ページの「Active Directory 用の ILOM の設定」 (CLI)

表 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
LDAP 用の ILOM 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 サーバの適切なディレクトリを検索する権限を持ちます。	19 ページの「LDAP サーバの設定」 (web) 20 ページの「LDAP 用の ILOM の設定」 (web) 34 ページの「LDAP 用の ILOM の設定」 (CLI)
LDAP SSL 用の ILOM の設定	SSL (Secure Socket Layer) を使用した LDAP を設定するには、主サーバ、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、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。	21 ページの「LDAP/SSL の用の ILOM の設定」 (web) 25 ページの「LDAP/SSL テーブルの編集」 (web) 35 ページの「LDAP/SSL の用の ILOM の設定」 (CLI)
RADIUS 用の ILOM の設定	RADIUS 認証を使用するには、最初に、RADIUS サーバの IP アドレスとポート番号、および RADIUS サーバ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。	26 ページの「RADIUS の用の ILOM の設定」 (web) 38 ページの「RADIUS の用の 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。	27 ページの「ユーザーとして ILOM へのログイン」 (web) 39 ページの「ユーザーとして ILOM へのログイン」 (CLI)
ILOM からログアウトする	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。	28 ページの「ILOM からのログアウト」 (web) 40 ページの「ILOM からのログアウト」 (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。	40 ページの「Web インタフェースを使用した ILOM バージョンの識別」 40 ページの「CLI を使用した ILOM バージョンの識別」
ILOM ファームウェアの更新	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。	41 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」 43 ページの「CLI を使用して ILOM ファームウェアを更新する」

ILOM への接続

ネットワーク接続がない場合でも、シリアルポート経由で ILOM にログインできます。また、ネットワーク経由でのログインも可能です。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 (モジュラーシャーシシステムを使用している場合はシャーシ監視モジュール (Chassis Monitoring Module, CMM)) の SER MGT 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、サーバまたは CMM の NET MGT ポートに Ethernet ケーブルを接続します。次に、静的また動的設定を使用して SP のネットワークインタフェースを設定します。

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、『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。

▼ DHCP を使用した SP ネットワークの設定

ここで説明する手順は、新しいシステムをセットアップする場合や DHCP を使用するようにすでに設定されているシステムをセットアップする場合を想定しています。システムが DHCP を使用するようにセットアップされていない場合は、Web インタフェースまたは CLI を使用して DHCP オプションを設定する必要があります。詳細は、『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』または『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』を参照してください。

次の手順に従って、DHCP を使用して SP ネットワークを設定します。

1. 使用しているネットワークをサーバの Ethernet 管理ポートに接続します。

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。

サーバ上の Ethernet 管理ポートの位置については、使用しているプラットフォームのマニュアルを参照してください。
2. SP に割り当てられた IP アドレスを取得するには、次のいずれかの方法を使用します。
 - DHCP サーバログ:

詳細は、使用している DHCP サーバのマニュアルを参照してください。
 - SP のシリアルポートに接続して、次のコマンドを入力します。
-> `show /SP/network`
 - x64 ホストサーバの起動時に、BIOS で表示される IP アドレスを監視します。
 - ホスト OS で IPMItool を使用して、次のコマンドを入力します。

```
#ipmitool -I <interface> lan print 1
```

インタフェースは、Solaris システムでは、bmc と呼ばれ、Linux システムでは、open と呼ばれ、Windows 2003 Server R2 Enterprise システムでは、ms と呼ばれます。

注 – Microsoft Windows システムでは、ipmitool コマンドを使用する場合、.exe 拡張子を ipmitool コマンドに追加する必要があります。たとえば、次の例があります。

```
ipmitool.exe -I ms lan print 1
```

▼ BIOS を使用した SP ネットワークの設定

この手順では、サーバホスト側の BIOS にアクセスしており、サーバのキーボードおよび VGA ポートにキーボードおよび端末が接続されていることを前提とします。

x64 サーバやモジュラーシャーシシステムのサーバモジュール (ブレード) で、次の手順に従います。

1. システムに電源を投入し、電源投入時の自己診断テスト (Power-On Self-Test, POST) の実行時に F2 キーを押して、BIOS 設定ユーティリティを起動します。
2. BIOS のメインメニュー画面が表示されたら、「Advanced」-->「IPMI 2.0 Configuration」-->「LAN Configuration」を選択します。
3. 「LAN Configuration」画面で、「IP Assignment」の下の「DHCP」または「Static」を選択します。
 - 「DHCP」を選択すると、SP のネットワーク構成は DHCP サーバから取得されます。
 - 「Static」を選択する場合は、IP アドレス、サブネットマスク、およびデフォルトゲートウェイのフィールドに値を入力します。「Commit」を選択して変更を保存します。

▼ シリアル接続を使用した静的ネットワーク設定

次の手順に従って、シリアル接続を利用して静的ネットワーク設定を実行します。

1. サーバ SP または CMM とのシリアル接続を確立します。

端末または端末エミュレーションソフトウェアを実行する PC を、サーバまたはシャーシ監視モジュール (Chassis Monitoring Module, CMM) のシリアルポートに接続します。
2. 端末ウィンドウで、次のように設定します。
 - 8N1: 8 データビット、パリティなし、1 ストップビット
 - 9600 ボー
 - ハードウェアのフロー制御無効
 - ソフトウェアのフロー制御無効

3. Enter キーを押して、ILOM のログインプロンプトを表示します。
次のような ILOM のログインプロンプトが表示されます。
`<hostname> login:`
4. root ユーザーアカウントとパスワードを使用して ILOM CLI にログインします。
`<hostname> login: root`
`Password: changeme`
ILOM CLI のプロンプト (->) が表示されます。
5. 次のいずれかのコマンドを入力して、作業用ディレクトリを設定します。
 - サーバ SP の場合:
`-> cd /SP/network`
 - CMM の場合:
`-> cd /CMM/network`
6. 次のコマンドを使用してネットワークを設定します。
 - `set pendingipdiscovery=static`
 - `set pendingipaddress=ip_address`
 - `set pendingipnetmask=ip_netmask`
 - `set pendingipgateway=ip_gateway`
 - `set commitpending=true`

▼ IPMItool を使用したネットワークの設定

IPMItool の詳細は、次のサイトから入手可能なマニュアルページで提供されています。

<http://ipmitool.sourceforge.net/manpage.html>

次の手順に従って、IPMItool を使用してネットワークを設定します。

1. 使用する適切な静的ネットワーク設定を確認します。
2. ホスト上で IPMItool を実行し、次のコマンドを入力して静的 IP ネットワーク設定を割り当てます。

```
#ipmitool -I <interface> lan set 1 ipsrc static
#ipmitool -I <interface> lan set 1 ipaddr <ipaddress>
#ipmitool -I <interface> lan set 1 netmask <netmask>
#ipmitool -I <interface> lan set 1 defgw ipaddr <gateway>
```

インタフェースは、Solaris システムでは、bmc と呼ばれ、Linux システムでは、open と呼ばれ、Windows 2003 Server R2 Enterprise システムでは、ms と呼ばれます。

注 – Microsoft Windows システムでは、ipmitool コマンドを使用する場合、.exe 拡張子を ipmitool コマンドに追加する必要があります。たとえば、次の例があります。

```
ipmitool.exe -I ms lan set 1 ipsrc static
```

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		
Step	説明	リンク
1	Web インタフェースを使用して ILOM への初回のログインを実行します。	<ul style="list-style-type: none">• 10 ページの「root ユーザーアカウントを使用した ILOM 3.0 へのログイン」
2	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択します	<ul style="list-style-type: none">• 11 ページの「ユーザーアカウントの追加と権限の割り当て」• 13 ページの「IACTive Directory 用の LOM の設定」• 19 ページの「LDAP サーバの設定」• 20 ページの「LDAP 用の ILOM の設定」• 25 ページの「LDAP/SSL テーブルの編集」• 26 ページの「RADIUS の用の ILOM の設定」
3	認証設定を確認します	<ul style="list-style-type: none">• 27 ページの「ユーザーとして ILOM へのログイン」
4	ILOM からログアウトする	<ul style="list-style-type: none">• 28 ページの「ILOM からのログアウト」

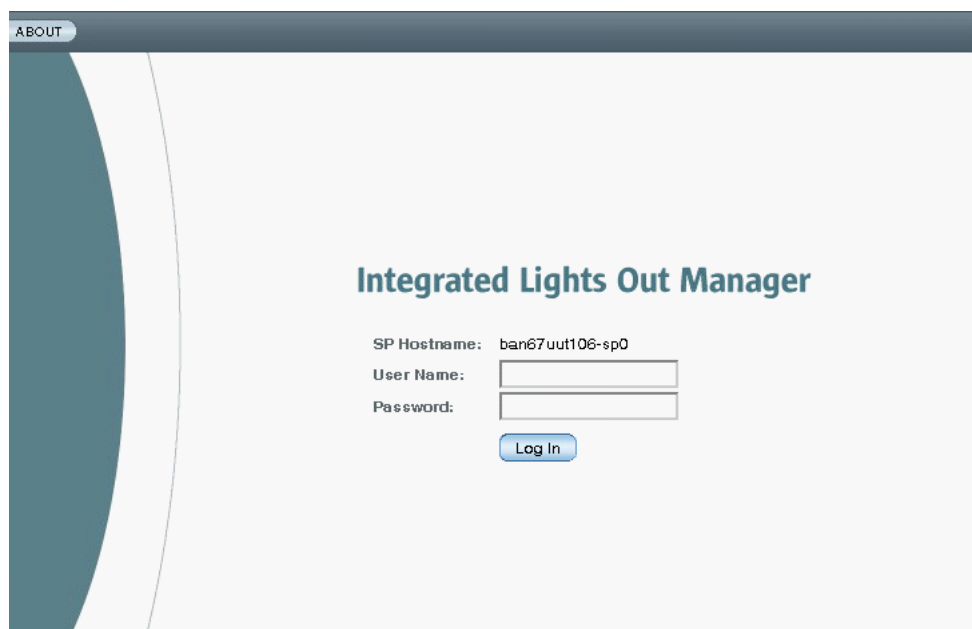
▼ root ユーザーアカウントを使用した ILOM 3.0 へのログイン

作業を開始する前に

- web ブラウザを開きます。

次の手順に従って、root ユーザーアカウントで ILOM の Web インタフェースへの初回のログインを実行します。

1. ブラウザに `http://system_ipaddress` と入力します。
Web インタフェースのログインページが表示されます。



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。
User Name: **root**
Password: **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。

▼ ユーザーアカウントの追加と権限の割り当て

作業を開始する前に

- root 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します。
- 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。

次の手順に従って、ローカルユーザーアカウントを追加し権限 (役割) を割り当てます。

1. 「User Management」 --> 「User Accounts」 を選択します。
「User Account Settings」 ページが表示されます。
2. 「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:

Roles: ▼

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

New Password:

Confirm New Password:

3. 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 Operator 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、この役割を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 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す。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が使用できます。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。

▼ IActive Directory 用の LOM の設定

作業を開始する前に

- root 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します。
- 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。

次の手順に従って、Active Directory に対して ILOM を設定します。

1. 「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 Advanced or none(server authorization). Enter the Hostname or IP address of your server. To change the communicate with your server, uncheck *Autoselect*. Enter a timeout value in seconds. Use the log detail amount of debug information sent to the log. To load a certificate, fill in the Certificate File Upload information. 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

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

2. Active Directory を設定します。

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	Description
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)	(none)	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。このプロパティには、Administrator や Operator といった従来表記の役割を使用することも、a、u、c、r、o、s といった個々の役割 ID の組み合わせを使用することもできます。For example, aucros, where a=Admin, u=User Management, c=Console, r=Reset and Host Control, o=Read Only, and s=Service. ここで役割を設定しない場合、役割の決定には Active Directory サーバが使用されます。
Address	Address	0.0.0.0	Active Directory サーバの IP アドレスまたは DNS 名。DNS 名を使用する場合は、DNS が設定されていて、機能している必要があります。
Port	port	0	Port used to communicate with the server or enable autoselect (which assigns the port to 0). 標準以外の TCP ポートが使用されているという、通常ないような場合に使用できます。
Timeout	timeout	4	秒単位のタイムアウト値。 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。トランザクション数は設定によって異なる可能性があるため、この値はすべてのトランザクションを合計した時間にはなりません。このプロパティにより、サーバが応答しない場合や到達不能な場合に待機する時間を調整することができます。
Strict Certificate Mode	strictcertmode	Disabled	Enabled Disabled 有効になっている場合、認証時にサーバの証明書の内容がデジタル署名によって検証されます。証明書がロードされていないと、「Strict Certificate Mode」を有効にすることができません。
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 サーバの検出が試みられます。
Log Detail	logdetail	none	None High Medium Low イベントログに記録する診断情報の量を指定します。

3. 「Save」をクリックして設定を有効にします。

4. 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	証明書が存在するかどうかを示す読み取り専用インジケータ。
Certificate File Status	certstatus	certificate present (details)	発行者、主題、シリアル番号、有効期間の開始日、有効期間の終了日、およびバージョンについては「details」をクリックしてください。

5. 「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 – このセクションは、「Strict Certificate Mode」を使用する場合にのみ必要です

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

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

7. 「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。

issuer	証明書を発行した認証局。
subject	証明書の対象のサーバまたはドメイン。
valid_from	証明書が有効になる日。
valid_until	証明書が無効になる日。
serial_number	証明書のシリアル番号。
version	証明書のバージョン番号。

8. 「Active Directory」ページのいちばん下で、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

9. 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 (Distinguished Name、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。

代替サーバテーブルは、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 ロケータクエリーテーブルは、認証に使用するホストについて DNS サーバ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

エントリ 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=sun,DC=com
2	

■ Operator Groups テーブル

エントリ 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=sun,DC=com
2	

■ Custom Groups テーブル

エントリ 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 (aucro)

■ User Domains テーブル

エントリ 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。エントリ 2 は、Active Directory が最初のエントリ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 - 下記の例では、<USERNAME> はユーザーのログイン名を表します。認証時に、ユーザーのログイン名が <USERNAME> に置き換わります。

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

■ Alternate Servers テーブル

ID	Address	Port	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、名前付き DNS サービスを識別します。ポート ID は、通常、レコードに含まれますが、<PORT:636> 形式を使用してオーバーライドできます。また、認証されるドメイン固有の名前付きサービスは、<DOMAIN> 置換マーカーを使用して指定できます。

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

10. 「Save」をクリックして変更を有効にします。

▼ LDAP サーバの設定

次の手順に従って、LDAP サーバを設定します。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。

たとえば、次のように入力します。

```
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>	任意の固有の番号
<code>gidNumber</code>	任意の固有の番号
<code>userPassword</code>	パスワード
<code>homeDirectory</code>	任意の値 (ILOM はこのプロパティを無視します)
<code>loginShell</code>	任意の値 (ILOM はこのプロパティを無視します)

3. LDAP サーバを設定して、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 サーバにプロキシユーザーを作成します。LDAP サーバは、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。

[20 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

作業を開始する前に

- root 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します。
- 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。

次の手順に従って、LDAP 用に ILOM を設定します。

1. 「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=docs, dn=writers). Enter the distinguished name (DN) and password for a proxy user ILOM can use to access your LDAP tree.

State: Enabled

Roles: Advanced Roles ▼

Admin (a) User Management (u)

Console (c) Reset and Host Control (r)

Read Only (o) Service (s)

Address:

Port:

Searchbase:

Bind DN:

Bind Password: Change

Save

2. 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 「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 が設定されていて、機能している必要があります。
 - **Port** – LDAP サーバのポート番号です。
 - **Searchbase** – ユーザーを検索するための LDAP サーバの分岐を入力します。
 - **Bind DN** – LDAP サーバ上の読み取り専用プロキシユーザーの識別名 (Distinguished Name、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。
3. 「Save」をクリックして変更を有効にします。
4. 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、ILOM はローカルアカウントを使用して認証を行います。

▼ LDAP/SSL の用の ILOM の設定

作業を開始する前に

- root 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します。
- 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。

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。「Strict Certificate Mode」を使用する場合は、証明書は省略可能です。

次の手順に従って、LDAP/SSL の用の ILOM を設定します。

1. 「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。



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 ▾

[Save](#)

Certificate Information

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

Certificate File Upload

Transfer Method: Browser ▾

Select File: [Browse...](#)

[Load Certificate](#)

[Remove Certificate](#)

- [Admin Groups](#)
- [Operator Groups](#)
- [Custom Groups](#)
- [User Domains](#)
- [Alternate Servers](#)

2. LDAP/SSL 設定の設定

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	Description
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)	(none)	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。このプロパティには、Administrator や Operator といった従来表記の役割を使用することも、a、u、c、r、o、s といった個々の役割 ID の組み合わせを使用することもできます。For example, aucros, where a=Admin, u=User Management, c=Console, r=Reset and Host Control, o=Read Only, and s=Service. ここで役割を設定しない場合、役割の決定には LDAP/SSL サーバが使用されます。
Address	Address	0.0.0.0	LDAP/SSL サーバの IP アドレスまたは DNS 名。DNS 名を使用する場合は、DNS が設定されていて、機能している必要があります。
Port	port	0	Port used to communicate with the server or enable autoselect (which assigns the port to 0). 標準以外の TCP ポートが使用されているという、通常ないような場合に使用できます。
Timeout	timeout	4	秒単位のタイムアウト値。 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。トランザクション数は設定によって異なる可能性があるため、この値はすべてのトランザクションを合計した時間にはなりません。 このプロパティにより、サーバが応答しない場合や到達不能な場合に待機する時間を調整することができます。
Strict Certificate Mode	strictcertmode	Disabled	Enabled Disabled 有効になっている場合、認証時にサーバの証明書の内容がデジタル署名によって検証されます。証明書がロードされていないと、「Strict Certificate Mode」を有効にすることができません。
Log Detail	logdetail	none	None High Medium Low イベントログに記録する診断情報の量を指定します。

3. 「Save」をクリックして設定を有効にします。
4. 「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)	表示	Description
Certificate File Status	certstatus	certificate not present	証明書が存在するかどうかを示す読み取り専用インジケータ。
Certificate File Status	certstatus	certificate present (details)	発行者、主題、シリアル番号、有効期間の開始日、有効期間の終了日、およびバージョンについては「details」をクリックしてください。

5. 「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 – このセクションは、「Strict Certificate Mode」を使用にする場合にのみ必要です。

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

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

issuer	証明書を発行した認証局。
subject	証明書の対象のサーバまたはドメイン。
valid_from	証明書が有効になる日。
valid_until	証明書が無効になる日。
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 テーブルの編集

作業を開始する前に

- root 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します。
- 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。

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. 「User Management」 --> 「LDAP/SSL」 を選択します。
「LDAP/SSL」 ページが表示されます。
2. 「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
3. 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。
The appropriate page appears: 「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。

4. 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、13 ページの「[IActive Directory 用の LOM 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=sun,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。

5. 「Save」をクリックして変更を有効にします。

▼ RADIUS の用の ILOM の設定

作業を開始する前に

- root 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します。
- 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。

次の手順に従って、RADIUS の用の ILOM を設定します。

1. 「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: Advanced Roles ▾

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

Address:

Port:

Shared Secret:

2. 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	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。このプロパティには、Administrator や Operator といった従来表記の役割を使用することも、a、u、c、r、o、s といった個々の役割 ID の組み合わせを使用することもできます。For example, aucros, where a=Admin, u=User Management, c=Console, r=Reset and Host Control, o=Read Only, and s=Service.
Address	ipaddress	0.0.0.0	RADIUS サーバの IP アドレスまたは DNS 名。DNS 名を使用する場合は、DNS が設定されていて、機能している必要があります。
Port	port	1812	RADIUS サーバ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	(none)	機密データを保護しクライアントとサーバ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。

3. 「Save」をクリックして設定を有効にします。

▼ ユーザーとして ILOM へのログイン

作業を開始する前に

- web ブラウザを開きます。

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. ブラウザに `http://system_ipaddress` と入力します。
Web インタフェースのログインページが表示されます。
2. 設定した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。
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 からのログアウト

- 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。

通常の ILOM ユーザーとして ILOM を設定する準備ができました。ILOM の機能および 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。表 P-1 を参照してください。ILOM 3.0 マニュアルセットは以下のサイトにあります。

<http://primeserver.fujitsu.com/sparcenterprise/manual/>

CLI を使用した ILOM の初期セットアップ手順

項目		
Step	説明	リンク
1	CLI を使用して ILOM への初回のログインを実行します。	<ul style="list-style-type: none">• 29 ページの「root ユーザーアカウントを使用した ILOM 3.0 へのログイン」
2	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択します	<ul style="list-style-type: none">• 29 ページの「ユーザーアカウントの追加と権限の割り当て」• 30 ページの「Active Directory の用の ILOM の設定」• 34 ページの「LDAP サーバの設定」• 34 ページの「LDAP 用の ILOM の設定」• 35 ページの「LDAP/SSL の用の ILOM の設定」• 38 ページの「RADIUS の用の ILOM の設定」
3	認証設定を確認します	<ul style="list-style-type: none">• 39 ページの「ユーザーとして ILOM へのログイン」
4	ILOM からログアウトする	<ul style="list-style-type: none">• 40 ページの「ILOM からのログアウト」

▼ root ユーザーアカウントを使用した ILOM 3.0 へのログイン

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。

- 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
Password: changeme
```

ILOM CLI のプロンプト (->) が表示されます。

▼ ユーザーアカウントの追加と権限の割り当て

作業を開始する前に

- root 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します。
- 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。

次の手順に従って、ローカルユーザーアカウントを追加しユーザー権限 (役割) を割り当てます。

1. 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
```

たとえば、次のように入力します。

```
-> create /SP/users/user5
Creating user...
Enter new password: *****
Enter new password again: *****
Created /SP/users/user5
```

2. 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
```

たとえば、次のように入力します。

```
-> 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、[11 ページ](#)の「ユーザーアカウントの追加と権限の割り当て」を参照してください。

▼ Active Directory の用の ILOM の設定

作業を開始する前に

- root 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します。
- 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。

Active Directory を設定して、ユーザー資格を認証しサービスプロセッサに対するアクセスレベルを認可することができます。

次の手順に従って、Active Directory に対して ILOM を設定します。

1. 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。次のように入力してください。

```
-> 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
```

2. show コマンドを使用して、テーブルにある情報を表示します。次のように入力してください。

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

n は 1 - 5 で、*name* は次のいずれかです。

- **admingroups** (Admin Groups プロパティーの場合)
- **opergroups** (Operator Groups プロパティーの場合)
- **customgroups** (Custom Groups プロパティーの場合)
- **userdomains** (User Domains プロパティーの場合)
- **alternateservers** (Alternate Servers 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 ~ 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します。

```
-> 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)
```

show コマンドを使用して、代替サーバの証明書のプロパティーを取得します。

```
-> 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)
```

3. 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。

たとえば、次のように入力します。

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

4. set コマンドを使用して、証明書をロードしたり、プロパティを変更したりします。

たとえば、次のように入力します。

- 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=sun,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=sun,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=sun,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=sun,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 – Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、または Read Only (o) のいずれかまたは個々の役割 ID の組み合わせに役割を設定できます。Administrator や Operator といった従来の表記の役割もサポートされます。

```
-> set /SP/clients/activedirectory/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=sun,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.sun.com
Set 'domain' to 'username@sales.sun.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>
```

注 – DNS ロケータサービスクエリーは、名前付き DNS サービスを識別します。ポート ID は、通常、レコードに含まれますが、<PORT:636> 形式を使用してオーバーライドできます。また、認証されるドメイン固有の名前付きサービスは、<DOMAIN> 置換マーカーを使用して指定できます。

▼ LDAP サーバの設定

LDAP を使用するには、まず、LDAP サーバを設定する必要があります。Web インタフェースの節の [19 ページの「LDAP サーバの設定」](#) を参照してください。

▼ LDAP 用の ILOM の設定

作業を開始する前に

- root 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します。
- 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。

次の手順に従って、LDAP 用に ILOM を設定します。

1. 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。

たとえば、次のように入力します。

```
-> set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales, dc=sun, dc=com" bindpw=password
```

2. LDAP サーバの IP アドレスまたは DNS 名を入力します。次のように入力してください。

```
-> set /SP/clients/ldap address=ldap_ipaddress|DNS_name
```

3. (省略可能) LDAP サーバ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
```

4. 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。次のように入力してください。

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

5. LDAP サービスの状態を enabled に設定します。次のように入力してください。

```
-> set /SP/clients/ldap state=enabled
```

6. 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、ILOM はローカルアカウントを使用して認証を行います。

▼ LDAP/SSL の用の ILOM の設定

作業を開始する前に

- root 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します。
- 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。

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。「Strict Certificate Mode」を使用する場合、証明書が省略可能です。

次の手順に従って、LDAP/SSL に対して ILOM を設定します。

1. 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。次のように入力してください。

```
-> 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
```

2. show コマンドを使用して、テーブルにある情報を表示します。次のように入力してください。

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

n は 1 - 5 で、*name* は次のいずれかです。

- **admingroups** (Admin Groups のプロパティーの場合)
- **opergroups** (fOperator 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** (fUser Domains のプロパティーの場合)
- **alternateservers** (Alternate Servers 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 ~ 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します。

```
-> 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)
```

show コマンドを使用して、代替サーバの証明書のプロパティーも取得できます。

```
-> 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)
```


3. 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。
たとえば、次のように入力します。

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

4. set コマンドを使用して、証明書をロードしたり、プロパティを変更したりします。

たとえば、次のように入力します。

- 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=sun,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=sun,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=sun,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=sun,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 – Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、または Read Only (o) のいずれかまたは個々の役割ID の組み合わせに役割を設定できます。Administrator や Operator といった従来の表記の役割もサポートされます。

```
-> set /SP/clients/ldapssl/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=sun,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 – 下記の例では、<USERNAME> はユーザーのログイン名を表します。認証の際に、ユーザーのログイン名は <USERNAME> に置き換わります。

```
-> set /SP/clients/ldapssl/userdomains/1 name=<USERNAME>@uid=
<USERNAME>,OU=people,DC=sun,DC=com
Set 'domain' to 'uid=<USERNAME>,OU=people,DC=sun,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 の用の ILOM の設定

作業を開始する前に

- root 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します。
- 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。

次の手順に従って、RADIUS に対して ILOM を設定します。

1. 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
```

たとえば、次のように入力します。

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

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

2. set コマンドを使用してプロパティを変更します。

たとえば、次のように入力します。

```
-> 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、[26 ページの「RADIUS の用の ILOM の設定」](#)を参照してください。

▼ ユーザーとして ILOM へのログイン

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

たとえば、次のように入力します。

```
$ ssh username@ip_address
```

または

```
$ ssh -l username ip_address
```

パスワードの入力を求める ILOM のログインプロンプトが表示されます。

2. 設定した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て、ILOM にアクセスします。

```
<hostname>: username
```

```
Password: password
```

ILOM CLI プロンプト (->) が表示されます。

▼ ILOM からのログアウト

- コマンドプロンプトで、次のように入力します。

-> `exit`

通常の ILOM ユーザーとして、ILOM を設定する準備ができました。ILOM の機能および 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。表 P-1 を参照してください。

ILOM バージョン情報の識別

サーバ 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す。ILOM ファームウェアのバージョンを識別するには、Read Only (o) の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た ILOM バージョンの識別

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 を使用した ILOM バージョンの識別

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。たとえば、次のように入力します。

```
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

作業を開始する前に

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。詳細は、『Integrated Lights Out Manager (ILOM) 3.0 Web 手順ガイド』または『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』の「ファームウェアの更新」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にコピーします。CLI で更新する場合は、ローカルサーバ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 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 の既存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 – 「Delay BIOS upgrade」 オプションは、x64 システム上でファームウェアを ILOM 3.0 以降へ更新する場合にのみ表示されます。

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 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. ILOM Web インタフェースに再接続します。「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することを確認します。

注 – ファームウェアを更新する前に ILOM の設定を保存していない場合、ILOM に再接続するには ILOM の初期セットアップ手順を実行する必要があります。

▼ 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、IOM 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。
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_ip>/<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。
たとえば、次のように入力します。
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。システムは、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。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。システムは、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。手順 7 に進みます。
 - x64 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 アップデートの延期を確認するプロンプトが表示されます。
たとえば、次のように入力します。
Do you want to force the server off if BIOS needs to be upgraded (y/n)?

- a. BIOS アップデート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 x64 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。「いいえ」(n) と答えると、必要に応じて、SP ファームウェアの更新時に BIOS が自動的に更新されます。

- 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、ILOM サーバ SP または CMM に再接続します。

注 – ファームウェアを更新する前に ILOM の設定を保存していない場合、ILOM に再接続するには ILOM の初期セットアップ手順を実行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確認します。
CLI プロンプトで、次のように入力します。

```
-> version
```

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、『Integrated Lights Out Manager 3.0 概念ガイド』を参照して、ILOM 3.0 の新しい特徴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、『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 補足マニュアルを参照してください。

上記のマニュアルは、使用しているプラットフォームのマニュアルセットでも入手できます。次の Web サイトからアクセスしてください。

<http://primeserver.fujitsu.com/sparcenterprise/manual/>


FUJITSU