NEC

iLO５
ユーザーズガイド

NEC NX7700xシリーズサーバ

2022年 1月 Rev 3.00

本書の内容は、将来予告なしに変更されることがあります。製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、脱落に対して、責任を負いかねますのでご了承ください。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、その保有、使用、または複製には、弊社から使用許諾を得る必要があります。FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェアドキュメンテーション、および商業用製品の技術データ（Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items）は、ベンダー標準の商業用使用許諾のもとで、米国政府に使用許諾が付与されます。

他社の Web サイトへのリンクは、弊社の Web サイトの外に移動します。弊社は、弊社の Web サイト以外にある情報を管理する権限を持たず、また責任を負いません。

商標

Intel® およびインテルは、インテルコーポレーションまたはその子会社のアメリカ合衆国およびその他の国における商標または登録商標です。

Java は、Oracle および/またはその関連会社の登録商標です。

Linux® は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft®および Windows® は、米国および/またはその他の国における Microsoft Corporation の登録商標または商標です。

Red Hat® は、米国およびその他の国における Red Hat, Inc.の商標または登録商標です。

SD は SD-3C の米国およびその他の国における商標または登録商標です。

VMware® は、VMware, Inc.の米国および各国での登録商標または商標です。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に掲載されている製品情報には、日本国内で販売されていないものも含まれている場合があります。

目次

1. はじめに

iLO の概要

iLO は、NX7700x サーバのマザーボードに内蔵されているリモートサーバー管理プロセッサーです。iLO では、リモートからサーバーを監視および制御できます。iLO マネージメントは、サーバーをリモートから構成、更新、監視、および修復する複数の方法を提供する強力なツールです。

iLO マネージメントは、iLO ライセンスに依り使用可能な機能が変わります。NX7700x サーバには、サーバー管理者の生産性を最大化させるために、iLO(Advanced)ライセンスが標準でインストールされています。

iLO の主な機能

- **サーバーの状態監視** - iLO はサーバー内部の温度を監視して冷却ファンを制御し、適切なサーバーの冷却を行います。さらにインストールされたファームウェアとソフトウェアのバージョン、本機に搭載された冷却ファン、メモリ、ネットワーク、プロセッサー、電源ユニット、ストレージ、デバイスなどのステータスも監視します。
- **Agentless management** - iLOファームウェアのRESTful APIやSNMPを利用し、ホストOS上のメモリやプロセッサーのリソースを使わずに管理できます。すべての重要な内部サブシステムの監視に加えて、iLOは、ホストOSがインストールされていない場合でも、ESMPRO/ServerManagerのような管理ソフトウェアに直接SNMP通報を送信できます。
- **インテグレーテッドマネージメントログ（IML）** - サーバーで発生したイベントを記録しています。SNMP 通報、Email アラート、およびリモート Syslog での通知を設定することができます。
- **Active Health System(AHS)ログ** - AHS ログは NX7700x サーバのハードウェア問題を調査する為に必要となる基礎的な情報(シリアル番号、構成情報、ファームウェア/BIOS 情報等)、iLO イベントログ(IEL)、IML、詳細ログなどを含むバイナリー・ファイルです。サポートを要する場合は、AHS ログファイルを NEC に送付、または保守員が採取することがあります。
- **iLO 連携管理** - iLO 連携機能を使用すると、管理ソフトウェアを利用せずに一度に複数のサーバーを検出および管理することができます。
- **統合リモートコンソール（IRC）** - サーバーとのネットワーク接続があれば、リモートコンソールにより、世界中どこからでも高速、安全にサーバーにアクセスして表示または管理できます。
- **仮想メディア** - リモートから高性能な仮想メディアデバイスをサーバーにマウントできます。
- **仮想電源制御** - リモートから安全に管理対象サーバーの電源状態を制御できます。
- **デプロイメントとプロビジョニング** - iLO Advancedを使用すれば、利用可能なサーバー群に対しての状態参照、ファームウェアアップデート、電力やライセンス設定ができるほか、選択されたサーバーに対して、サーバーが実行中かオフラインかにかかわらず、リモート制御できます。
- **消費電力と電力設定** - サーバーの消費電力を監視し、サポートされているサーバーの消費電力上限を設定します。

- **ユーザーアカウント** - ローカルまたはディレクトリサービスのユーザーアカウントを使用して、iLO にログインできます。
- **Kerberos サポート** - Kerberos 認証を設定できます。ログイン画面に**[Zero Sign In]**ボタンが追加されます。
- **iLO インターフェースコントロール** - セキュリティを強化するために、選択した iLO インターフェース機能を有効または無効にできます。
- **ファームウェア管理** - コンポーネントを iLO リポジトリへの保存、リポジトリからのインストール実施、インストールキューの登録、管理などができます。
- **iLO サービスポート** - サポートされている USB Ethernet アダプターを使用して、iLO サービスポートにクライアントを接続し、サーバーに直接アクセスします。また、USB キーを接続して、Active Health System ログをダウンロードすることもできます。
- **IPMI** - iLO ファームウェアは、IPMI バージョン 2.0 仕様に準拠したサーバー管理を提供します。
- **iLO RESTful API および RESTful インターフェースツール（iLOrest）** - iLO 5 は、Redfish API 準拠の iLO RESTful API をサポートしています。
- **iLO Backup & Restore** - 事前にバックアップしたiLO設定を故障によるマザーボード交換時などにリストアできます。
- **Intelligent System Tuning**[1] - Intelligent System Tuningサーバーは、サーバーのパフォーマンスを向上させるいくつかの機能から構成されています。Jitter Smoothing(CPU安定化機能)は、クロック周波数の変動が少なく安定した性能を発揮できるクロック周波数を検知して固定化させることで、定格周波数より高い処理の遅延やばらつきを排除します。さらにCore Boosting(コアブースト機能)モードを使用することで、クロック周波数の変動を緩和し、全体的の最大スループットを向上させます。Workload Matching(ワークロード最適設定機能)は、ワークロード毎の最適設定を構成したプロファイルを用意し、サーバー内部リソースを自動的に調整し、デフォルト設定よりも最大のパフォーマンスを向上させます。
- **Performance Monitoring**[2] - Innovation Engine のサポートによってサーバーでサポートされたセンサーから収集したパフォーマンスデータを表示します。収集したデータに基づいてアラートを構成できます。
- **仮想NIC**[3] - ホストオペレーティングシステムからiLO に安全にアクセスします。
- **ファームウェアの検証とリカバリ**[4] - 正式なファームウェアにはデジタル署名がされており、ファームウェアアップデート時にファームウェアが改ざんされたものかどうかを検証します。もし不正なファームウェアを検知した場合には、アップデート適用を実行せず終了させます。スケジュール済みまたはオンデマンドでファームウェアの検証スキャンを実行して、問題が検出されたときに実装するリカバリ操作を設定します[5]。
- **安全なリカバリ** - 電源の作動時に iLO ファームウェアを検証します。ファームウェアが無効

1 iLO 5 Firmware Version 1.40 Feb 05 2019 以降

2 iLO 5 Firmware Version 1.40 Feb 05 2019 以降

3 iLO 5 Firmware Version 1.40 Feb 05 2019 以降

4 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

5 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

な場合、 iLO ファームウェアは自動的にフラッシュされます（iLO Standard ライセンス）。サーバーの起動時に、システム ROM を検証します。有効なシステム ROM が検出されないと、サー バーは起動できません。リカバリオプション[6]には、アクティブおよび冗長ROM のスワッピングや、ファームウェアの検証スキャンとリカバリアクションの起動などがあります。スケジュール済みのファームウェア検証スキャンと自動リカバリを行うには、iLO Advanced ライセンスが必要です。

- **ワークロードパフォーマンスアドバイザー**[7] - 選択されたサーバーワークロード特性を表示します。監視対象データに基づき、推奨のパフォーマンスチューニング設定を表示したり、構成したりできます。
- **セキュリティダッシュボード**[8] - 重要なセキュリティ機能のステータスを表示したり、潜在的なリスクがあるかどうか設定を評価したりします。リスクが検知されたら、詳細情報とシステムセキュリティを向上させる方法についてのアドバイスを見ることができます。
- **セキュリティ状態** - ご使用の環境に合ったセキュリティ状態を設定します。iLO は、本番環境（デフォルト）のセキュリティ状態や、高セキュリティ、FIPS、CNSA[9] などのより高いセキュリティ状態をサポートします。

  リカバリオプション[10]には、アクティブおよび冗長ROM のスワッピングや、ファームウェアの検証スキャンとリカバリアクションの起動などがあります。スケジュール済みのファームウェア検証スキャンと自動リカバリを行うには、iLO Advanced ライセンスが必要です。

注記： IPMI には IPMI 仕様におけるパスワードハッシュを取得される脆弱性(CVE-2013-4786)問題が含まれています。

脆弱性概要

IPMI の仕様は、RMCP+ Authenticated Key-Exchange Protocol (RAKP) 認証をサポートしているため、パスワードハッシュを取得される、およびオフラインパスワード推測攻撃を実行される脆弱性が存在します。

解決方法

この問題に対する解決策はありません。IPMI2.0仕様の認証プロセスは、クライアント認証に先がけてサーバーが要求されたユーザーのパスワードのSHA1、MD5ハッシュをクライアントに送るのを規定しています。BMCは、要求されたユーザーカウントのパスワードハッシュを返しますが、このパスワードハッシュは、オフラインパスワード推測攻撃で壊すことができます。この機能は、IPMI2.0仕様の重要な部分でIPMI2.0仕様から逸脱せずこの問題を解決することはできません。そのためこのリスクを軽減させるため以下を行うことを推奨します。

6 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

7 iLO 5 Firmware Version 1.40 Feb 05 2019 以降

8 iLO 5 Firmware Version 1.40 Feb 05 2019 以降

9 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

10 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

- IPMI を使用しない場合、IPMI over LAN を無効化してください。iLO Web インターフェースの**[Security]**-**[Access Settings]**ページで**[IPMI/DCMI over LAN]**を無効化することができます。デフォルトは無効化です。
- 最新の iLO ファームウェアを適用してください。
- システム、ネットワーク上のパスワード管理において最善な方策をとってください。強固なパスワードを使用してください。
- IPMI を使用する場合、iLO 管理インターフェースへのアクセスを制限し、個別のマネージメント LAN/VLAN、アクセス制御リスト(ACL)または VPN を使用してください。

△**注意:**

- サーバーの再起動中は、iLO のリセットを実行しないようにしてください。Web インターフェースの**[Information]**-**[Overview]**ページの UUID、UUID（論理）の表示において、不正な値が表示される場合があります。
- 本体装置に iLO ファームウェア 1.40 Feb 05, 2019 以降が適用されている場合、Web インターフェースへログインした後に右上部の iLO セキュリティ(盾マーク)、及び**[Information]**-**[Security Dashboard]**のステータスがリスク状態として表示されます。お客様のセキュリティポリシーに応じてセキュリティ対処をお願いします。推奨値等の詳細に関しては、「セキュリティダッシュボード詳細」を参照してください。
- iLO の SNTP の設定が行われていない場合、iLO のリセットを行うと iLO の時刻(**[Information]**-**[Overview]**-**[Status]**-**[iLO Date/Time]**、**[Information]**-**[iLO Event Log]**-**[Last Update]**)がずれてしまう場合があります。Web インターフェースで SNTP 設定をして頂くことを推奨します。
- ファイバーチャネルアダプターが実装されている本体装置に iLO ファームウェア 1.40 Feb 05, 2019 が適用されて、iLO Web インターフェースの言語に日本語が選択されている場合、**[System Information]**-**[Network]**で表示されるファイバーチャネルアダプターのポートのステータスに”ダウン”ではなく”下へ”が表示される場合があります。これは FC カードのポートの接続状態が”ダウン”状態であることを示します。
- iLO の拡張ライセンスがインストールされている本体装置に iLO ファームウェア 1.40 Feb 05, 2019 以降が適用されている場合、iLO Web インターフェースの**[Access Settings]**-**[Update Service]**-**[Downgrade Policy]**からダウングレードポリシーの設定が可能となります。本設定に[Permanently disallow downgrades]を設定すると、iLO に対して永続的な変更が行われます。永遠にダウングレードを禁止するように設定した後は、iLO インターフェースや各種ユーティリティからこの設定の変更を行うことができなくなります。iLO を出荷時のデフォルト設定に設定しても、この値はリセットされません。本設定に[Permanently disallow downgrades]を設定しないでください。

ROM ベースの構成ユーティリティ（BMC 構成ユーティリティ）

システムユーティリティ内の BMC 構成ユーティリティを使用して、ネットワークパラメーター、グローバル設定(BMC 機能、BMC 構成ユーティリティ、BMC Web インターフェース等の有効/無

効、シリアル CLI 設定等の BMC、BMC 構成ユーティリティに関わる設定)、およびユーザーアカウントを構成できます。
BMC 構成ユーティリティは、初期の iLO セットアップのためにご使用いただくもので、継続的な iLO 管理のためのものではありません。これらのユーティリティはサーバーが起動するときに起動でき、リモートコンソールを使用してリモートから実行できます。

ユーザーが ROM ベースの構成ユーティリティにアクセスするときにログインを必要とするよう iLO を構成することができます。またはすべてのユーザーに対してユーティリティを無効にすることができます。これらの設定は、iLO アクセスオプションで構成できます。BMC 構成ユーティリティを無効にすると、iLO セキュリティを無効にするようシステムメンテナンススイッチが設定されないかぎり、ホストからの再構成を防止します。詳細については、本体装置のメンテナンスガイドを参照ください。

詳細情報

iLO アクセスの設定

iLO RESTful API

iLO には、Redfish 1.0 準拠である iLO RESTful API が含まれています。iLO RESTful API は、サーバー管理ツールから使用することで、iLO 経由でサーバーの構成、インベントリ、および監視を実行できる管理インターフェースです。RESTful インターフェースツール（iLOrest）などの REST/Redfish クライアントは、HTTPS 操作を iLO Web サーバーに送信して JSON 形式のデータを GET および PATCH を行い、UEFI BIOS 設定などのサポートされる iLO とサーバーの設定を構成します。

サポートされている HTTPS 操作の例としては、GET、PUT、POST、PATCH、および DELETE などがあります。

iLO Standard ライセンスで有効になる iLO のすべての機能には、RESTful インターフェースツールを使用してアクセスできます。iLO Scale-Out、iLO Essentials、iLO Advanced ライセンスによって有効になる機能にアクセスするには、ライセンスをインストールする必要があります。詳しくは、「iLO ライセンス」を参照してください。

RESTful インターフェースツール

RESTful インターフェースツール（iLOrest）は、サーバー管理タスクを自動化するためのスクリプトツールです。 iLO RESTful API を活用した一連の簡略化されたコマンドを提供します。

このツールは、リモートで使用するためにコンピューターにインストールすることも、Windows または Linux オペレーティングシステムを搭載したサーバーにローカルにインストールすることもできます。 RESTful インターフェースツールは、自動化時間を短縮するために、インタラクティブモード、スクリプト可能モード、ファイルベースモードを提供します。

iLO スクリプティングとコマンドライン

iLO コマンドラインツールを使用して、複数のサーバーを設定したり、デプロイメントプロセスに標準設定を組み込んだり、サーバーやサブシステムを制御することができます。

iLO スクリプティング/コマンドラインガイドには、コマンドラインインターフェースまたはスクリプティングインターフェースを通じて iLO を使用するために利用できる構文およびツールに関する説明が記載されています。

2. iLO セットアップ

iLO をセットアップするための準備

iLO マネージメントプロセッサーをセットアップする前に、ネットワークとセキュリティの処理方法を決める必要があります。以下の質問に回答していくと、iLO の設定方法が明らかになります。

手順

1. iLO はどのようにネットワークに接続しますか？
2. 共有ネットワークポート構成で NIC チーミングを使用できますか？
3. iLO はどのように IP アドレスを取得しますか？
4. 必要なアクセスセキュリティと、必要なユーザーアカウントと特権は何ですか？
5. iLO の設定にはどのようなツールを使用しますか？

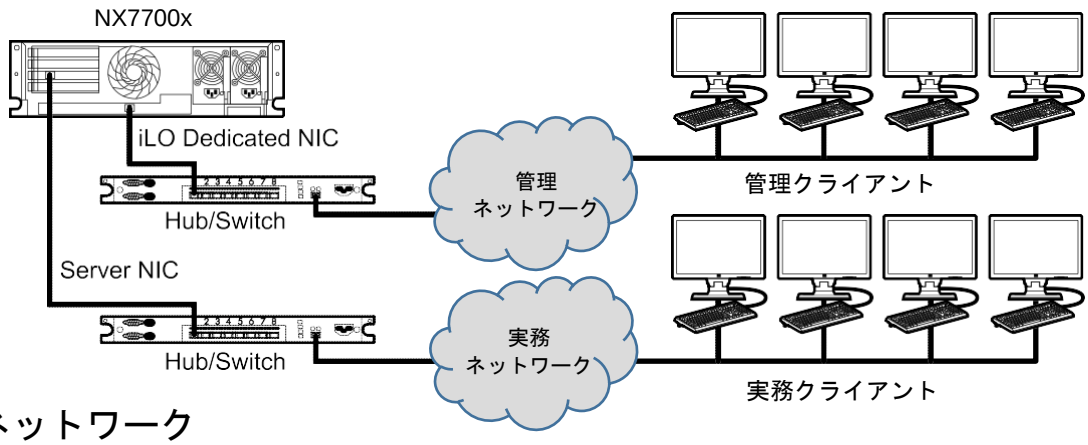
iLO のネットワーク接続の選択

通常、iLO は専用管理ネットワークまたは企業ネットワーク上の共有接続を通してネットワークに接続されます。

専用管理ネットワーク

この設定では、独立したネットワークに iLO ポートを配置します。管理ネットワークが独立しているため、性能が向上し、どのコンピューターをネットワークに接続するかを物理的に制御できるので、セキュリティが強化されます。また、企業ネットワーク内のハードウェアに障害が発生した場合には、サーバーへの冗長接続が提供されます。この構成では、企業ネットワークから直接 iLO にアクセスすることはできません。専用の管理ネットワークは、iLO の優先ネットワーク構成です。

図 1 専用ネットワーク接続例

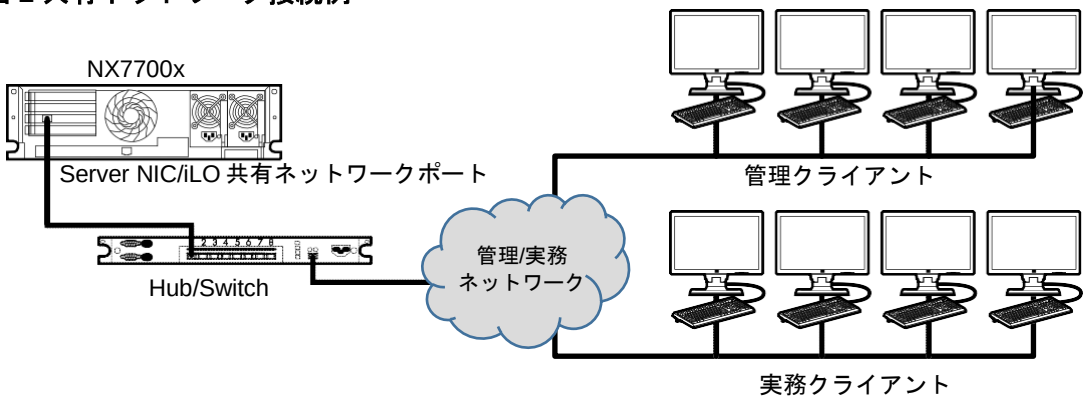


共有ネットワーク

この構成では、NIC と iLO ポートの両方が同一ネットワークに接続されています。iLO では、このタイプの接続を共有ネットワークポート構成と呼びます。この接続により、ネットワーク上のどこからでも iLO にアクセスできるため、iLO をサポートするために必要なネットワークハードウェアとインフラストラクチャの量が削減されます。
この構成にはいくつかの欠点があります。

- 共有ネットワーク接続では、トラフィックによって iLO パフォーマンスが低下する場合があります。
- サーバーのブート中および OS の NIC ドライバーのロード/アンロード中に、ネットワークから iLO にアクセスできない期間（2〜8 秒）があります。

図 2 共有ネットワーク接続例



iLO 共有ネットワークポート構成時の NIC チーミング

OS の NIC チーミングは、サーバーNIC のパフォーマンスと信頼性を向上させるために使用できる機能です。チーミングのメンバーに iLO の共有ネットワークポートを含むことはできますが、iLO の通信は共有ネットワークポートとして設定したポートのみでおこないます。従って、iLO の通信としては、OS の NIC チーミング機能による恩恵は受けることはできません。また、受信はすべて iLO の共有ネットワークポートで行われる必要があります。

NIC チーミングの制約

iLO が共有ネットワークポートを使用するように設定されている場合に NIC チーミングモードを選択すると、iLO のネットワーク通信は、次の条件でブロックされます。

- 選択した NIC チーミングモードによっては、iLO が接続されているスイッチによって、iLO が共有するように設定されているサーバーの NIC/ポートからのトラフィックが無視されます。
- 選択した NIC チーミングモードによっては、iLO を宛先とするすべてのトラフィックが、iLO が共有するように設定されている NIC/ポート以外の NIC/ポートに送信されます。
- iLO とサーバーは同じスイッチポート上で送受信するため、選択した NIC チーミングモードによっては、スイッチが同じスイッチポート上の 2 つの異なる MAC アドレスを使用してトラフィックに耐えられるようにする必要があります。LACP（802.3ad）の一部の実装では、同じリンク上の複数の MAC アドレスが許容されません。

NIC チーミングモード

NIC チーミングを使用するようにサーバーを構成する場合は、次のガイドラインに従ってください。

ネットワークフォールトトレランス

サーバーは、プライマリーアダプターで送受信します。チームの他の NIC（セカンダリーアダプター）は、サーバートラフィックを送信せず、受信トラフィックを無視します。このモードでは、iLO 共有ネットワークポートが正しく機能します。

iLO が優先プライマリーアダプターとして使用する NIC/ポートを選択します。

送信ロード バランシング

サーバーは複数のアダプターを送信しますが、1 次アダプターのみを受信します。このモードでは、iLO 共有ネットワークポートが正しく機能します。

iLO が優先プライマリーアダプターとして使用する NIC/ポートを選択します。

スイッチ アシスト ロード バランシング

このモードでは、プライマリーアダプターとセカンダリーアダプターの概念はありません。すべてのアダプターは、データの送受信で等しいと見なされます。このモードが iLO 共有ネットワークポート構成で最も問題となるのは、iLO 向けのトラフィックをサーバーNIC/ポートの 1 つのみしか受信できないためです。スイッチアシストロードバランシングに関する制約を判断するには、スイッチベンダーのマニュアルを参照してください。

iLO の IP アドレス取得方法

iLO がネットワークに接続されてから iLO へのアクセスを可能にするには、動的プロセスまたは静的プロセスを使用して iLO マネージメントプロセッサーが IP アドレスとサブネットマスクを取得する必要があります。

- **動的 IP アドレス**は、デフォルトで設定されます。iLO は、DNS または DHCP サーバーから IP アドレスとサブネットマスクを取得します。この方法が最も簡単です。

  DHCP を使用する場合：

- iLO 管理ポートは、DHCP サーバーに接続されているネットワークに接続される必要があります。本体装置に電源を入れる前に、iLO がネットワークに接続されている必要があります。iLO は、電源が投入された直後に DHCP 要求を送信します。 iLO が最初に起動したときに DHCP 要求に応答しないと、90 秒間隔で要求が再発行されます。
- DHCP サーバーは、DNS と WINS 名前解決を提供するように構成する必要があります。
- **静的 IP アドレス**は、ネットワークで DNS または DHCP サーバーを使用できない場合に使用されます。静的 IP アドレスは、システムユーティリティ内の BMC 構成ユーティリティを使用して構成できます。

  静的 IP アドレスの使用を予定する場合は、iLO セットアッププロセスを開始する前に IP アドレスが必要です。

iLO のアクセスセキュリティ

次の方法で iLO へのアクセスを管理できます。

- **ローカルアカウント** - iLO には、最大 12 のアカウントを格納できます。これは、研究所や中小企業のような小規模環境に最適です。ローカルアカウントを使用したログインセキュリティは、iLO のアクセス設定とユーザー権限によって管理されます。
- **ディレクトリサービス** - iLO に最大 6 つのディレクトリグループを設定できます。ディレクトリを使用して、iLO のアクセスを認証します。この構成により、無制限のユーザー数が可能になり、エンタープライズ内の iLO デバイスの数に合わせて簡単に拡張できます。ディレクトリサービスを使用する予定の場合は、少なくとも 1 つのローカル管理者アカウントでのアクセスを有効にすることを検討してください。ディレクトリは、iLO デバイスとユーザーの集中管理でき、強力なパスワードポリシーを実施できます。

詳細情報

iLO セキュリティの設定

iLO のユーザーアカウント

ディレクトリの認証と認可

iLO の設定ツール

iLO は、設定と操作用にさまざまなインターフェースをサポートしています。このガイドでは、次のインターフェースについて説明します。

- **iLO の Web インターフェース**は、Web ブラウザーを使用してネットワーク上の iLO に接続できる場合に使用します。また、iLO マネージメントプロセッサーの設定を変更する場合も、この方法を使用できます。

- システム環境が DHCP、DNS、または WINS を使用しない場合は、システムユーティリティ内の **BMC 構成ユーティリティ**を使用して iLO の Web インターフェースへのアクセスに必要な最低限のネットワーク設定を行います。

このガイドでは説明しませんが、その他に以下の設定オプションがあります。

- **iLO RESTful API** - サーバー管理ツールから使用することで、iLO 経由でサポート対象サーバーの構成、インベントリ、および監視を実行できる管理インターフェースです。
- **スクリプティング・コマンドライン** - スクリプティング・コマンドラインを使用すると、複数の iLO マネージメントプロセッサーの高度なセットアップを行うことができます。ネットワーク経由での設定、初期展開の際の設定、展開済みのホストからの設定などさまざまな設定が可能です。

  以下の方法を使用できます。

  - **SMASH CLP** - SSH または物理シリアルポートからコマンドラインにアクセスできるときに使用できるコマンドラインプロトコルです。詳しくは、help コマンドを参照してください。

詳細情報

BMC 構成ユーティリティを使用した iLO のセットアップ

iLO の Web インターフェースを使用した iLO のセットアップ

初期セットアップ手順

iLO は、デフォルト設定のままでも、ほとんどの機能を使用できます。ただし iLO では、複数の企業環境のために柔軟なカスタム設定が可能です。この章では、初期の iLO セットアップ手順について説明します。

1. iLO をネットワークに接続します。
2. 動的 IP アドレスを使用しない場合は、BMC 構成ユーティリティを使用して静的 IP アドレスを設定します。
3. ローカルアカウント機能を使用する場合は、BMC 構成ユーティリティを使用してユーザーアカウントを設定します。
4. iLO 5 にタイムゾーンを設定します。iLO 5 で正しい時刻を表示するためにタイムゾーンの設定が必要になります。
5. オプション：iLO ライセンスをインストールします。
6. 必要な場合、iLO ドライバーをインストールします。

詳細情報

iLO ドライバー

iLO のタイムゾーンを設定

iLO をネットワークへ接続

共有ネットワークまたは専用の管理ネットワークを使用して iLO をネットワークに接続します。

- **専用管理ネットワーク**では、独立したネットワークに iLO ポートを配置します。図 1 を参照してください。
- **共有ネットワーク**では、サーバーNIC と iLO 共有ネットワークポートの両方をネットワークに接続します。図 2 を参照してください。

詳細情報

iLO のネットワーク接続の選択

BMC 構成ユーティリティを使用した iLO のセットアップ

初めて iLO をセットアップする場合と、DHCP、DNS、または WINS を使用しない環境に iLO のネットワークパラメーターを構成する場合は、システムユーティリティ内の BMC 構成ユーティリティを使用することをおすすめします。BMC 構成ユーティリティを使用して iLO Web インターフェースへアクセスするために必要な最低限の設定を行った後に、iLO Web インターフェースへアクセスしてください。

BMC 構成ユーティリティを使用した静的 IP アドレスの設定

この手順は、静的 IP アドレスを使用する場合にのみ必要です。動的 IP アドレスを使用する場合は、DHCP サーバーによって iLO の IP アドレスが自動的に割り当てられます。

インストールを簡単にするために、iLO では DNS または DHCP を使用することをおすすめします。

手順

1. サーバーを再起動するかまたは電源を入れます。
2. サーバーの POST 画面で **F9** キーを押して、システムユーティリティを起動します。
3. **[システム構成]**画面で上向きまたは下向きの矢印キーおよび **Enter** キーを使用して**[システム構成]**→**[BMC 構成ユーティリティ]**→**[ネットワークオプション]**に移動します。
4. DHCP を無効にします。
   a. **[DHCP 有効]**で**[オフ]**を選択します。
5. IP アドレス、サブネットマスク、およびゲートウェイの IP アドレスを入力します。
   a. **[IP アドレス]**を入力します。
   b. **[サブネットマスク]** を入力します。
   c. **[ゲートウェイ IP アドレス]**を入力します。
6. **F10** キーを押して、変更を保存します。

   BMC 構成ユーティリティによって、保留中の構成変更をすべて保存するか確認するメッセージが表示されます。
7. **Y** キーを押して変更を保存し、終了します。

   BMC 構成ユーティリティから、変更を反映するために iLO をリセットする必要があることが通知されます。

重要: 本書では iLO の再起動という意味で iLO のリセットという用語を使用することがあります。

8. **Enter** キーを押します。

   iLO がリセットされ、iLO セッションが自動的に終了します。約 30 秒で再接続することができます。
9. 通常の起動プロセスを再開します。

   a. iLO リモートコンソールを起動します。

      BMC 構成ユーティリティは、前のセッションから開いたままになっています。

   b. **ESC** キーを数回押して、**[システム構成]**ページに移動します。

   c. **ESC** キーを押して、システムユーティリティを終了し、通常の起動プロセスを再開します。

BMC 構成ユーティリティを使用したローカルユーザーアカウントの管理

ユーザーアカウントの追加

1. サーバーを再起動するかまたは電源を入れます。
2. サーバーの POST 画面で **F9** キーを押して、システムユーティリティを起動します。
3. **[システムユーティリティ]**画面で、**[システム構成]**→**[BMC 構成ユーティリティ]**→**[ユーザー管理]**→**[ユーザーの追加]**の順に選択し、**[Enter]** キーを押します。
4. 次の権限のいずれかを選択し、**[Enter]** キーを押します。
   - **[ユーザーアカウント管理]**
   - **[リモートコンソールアクセス]**
   - **[仮想電源およびリセット]**
   - **[仮想メディア]**
   - **[設定の構成]**
   - **[ホスト BIOS]**
   - **[ホスト NIC]**
   - **[ホストストレージ]**
5. 各オプションで、次の設定のいずれかを選択し、**[Enter]** キーをもう一度押します。
   - **[はい]**（デフォルト） - このユーザーの権限を有効にします。
   - **[いいえ]** - このユーザーの権限を無効にします。
6. 次のオプションから選択し、**[Enter]** キーを押します。
   - **[新しいユーザー名]**
   - **[ログイン名]**

- **[パスワード]**と **[パスワードの確認]**

7. 新しいユーザーの各オプションの設定を完了し、**[Enter]** キーを押します。
8. 必要な数のユーザーアカウントを作成し、**F10** キーを押します。
9. メインメニューが表示されるまで、**Esc** キーを押します。
10. メインメニューで **[終了して起動を再開]**を選択し、**Enter** キーを押します。
11. 要求の確認を求めるメッセージが表示されたら、**Enter** キーを押してユーティリティを終了し、起動プロセスを再開します。

詳細情報

iLO ユーザー権限
ユーザーアカウントオプション

ユーザーアカウントの編集または削除

1. オプション：サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーの POST 画面で **F9** キーを押して、システムユーティリティを起動します。
4. **[システムユーティリティ]**画面で、**[システム構成]**→**[BMC 構成ユーティリティ]**→**[ユーザー管理]**→**[ユーザーの編集/削除]**を選択し、**[Enter]** キーを押します。
5. 編集または削除するユーザー名の **[Action]** メニューを選択し、**Enter** キーを押します。
6. 次のいずれかを選択し、**Enter** キーを押します。
   - **[変更なし]** - メインメニューに戻ります。
   - **[削除]** - このユーザーを削除します。
   - **[編集]** - ユーザーを編集します。
7. 手順 6 での選択内容に応じて、次のいずれかの操作を行います。
   - **[変更なし]**を選択した場合、それ以上の処置は必要ありません。
   - **[削除]**を選択した場合は、このページで変更を保存するときに削除するユーザー名にマークが付けられます。
   - **[編集]**を選択した場合は、ログイン名、パスワード、またはユーザーのアクセス権を更新します。
8. 必要な数のユーザーアカウントを更新し、**F10** キーを押します。
9. メインメニューが表示されるまで、**Esc** キーを押します。
10. メインメニューで **[終了して起動を再開]**を選択し、**Enter** キーを押します。
11. 要求の確認を求めるメッセージが表示されたら、**Enter** キーを押してユーティリティを終了し、起動プロセスを再開します。

詳細情報

iLO ユーザー権限
ユーザーアカウントオプション
パスワードに関するガイドライン

iLO の Web インターフェースを使用した iLO のセットアップ

Web ブラウザーを使用してネットワーク上の iLO に接続できる場合、iLO Web インターフェースを使用して iLO を構成できます。また、iLO マネージメントプロセッサーの設定を変更する場合も、この方法を使用できます。

サポートされているブラウザーを使用して、デフォルトの DNS 名、ユーザー名、およびパスワードを入力して、リモートのネットワーククライアントから iLO にアクセスします。DNS 名およびデフォルトのユーザーアカウント認証情報については、「iLO に初めてログインする方法」を参照してください。

iLO に初めてログインする方法

iLO ファームウェアは、デフォルトのユーザー名、パスワード、および DNS 名が事前に設定されています。デフォルトのユーザー情報は、iLO マネージメントプロセッサーを搭載するサーバーに取り付けられているシリアルラベルプルタブに記載されています。これらの記載内容を使用し、Web ブラウザーを使用して、ネットワーククライアントからリモートで iLO にアクセスしてください。

デフォルトの値は次のとおりです。

- **ユーザー名** - Administrator
- **パスワード** - 無作為に選んだ英数字 8 文字による文字列
- **DNS 名** - BMC**XXXXXXXXXXXX**（12 個の **X** は、サーバーのシリアル番号）

正しくないユーザー名やパスワードを入力したり、ログインに失敗したりすると、iLO はセキュリティ遅延時間を課します。ログインセキュリティについて詳しくは、「ログインセキュリティ」を参照してください。

重要: ネットワークを介して制御できる機器において、その制御用パスワードを初期値のまま運用しますと、悪意のある第三者による不正アクセスを許すリスクが発生します。不正アクセスにより機器が乗っ取られますと、情報漏えいのみならず、可用性や完全性を阻害してシステムに被害を生じさせたり、ボットネットによるサイバー攻撃の足場に悪用されたりする可能性があります。

当製品の初期パスワードは、あくまでも保守運用における初期設定のために設けられています。**初期設定時に必ずパスワード変更を行ってください。**もし初期パスワードのまま運用して不正アクセスの被害が発生した場合、**当社は一切の責任を負うことができません。**

なお、パスワード変更を行っても、強度の低いもの（桁数の少ないもの）や容易に考えられるもの（“123456789”, “abcdefg”, “password”, “Administrator” など）では不正アクセスの防止が困難です。**強度の強いパスワード（8 文字以上で大文字/小文字/数字混在のもの**を推奨）に変更頂きますようお願い致します。

手順については、「iLO のユーザーアカウント」を参照してください。

iLO を工場出荷時のデフォルト設定にリセットした場合は、リセット後にデフォルトの iLO アカウント情報を使用してログインします。

iLO ライセンス機能の有効化

NX7700x サーバには、サーバー管理者の生産性を最大化させるために、iLO(Advanced)ライセンスが標準でインストールされています。

詳細情報

iLO ライセンス

iLO ドライバー

iLO 用のドライバーとして iLO 5 チャネルインターフェースドライバーが用意されています。iLO は、内蔵のオペレーティングシステムを実行する独立したマイクロプロセッサーです。このアーキテクチャーでは、ホストのオペレーティングシステムとは関係なく、iLO のほとんどの機能を使用できます。iLO 5 チャネルインターフェースドライバーは、Agentless Management Service などのソフトウェアやオンラインROMフラッシュコンポーネントとiLOの通信を可能にします。

EXPRESSBUILDER および StarterPack を使用してインストールを行うと自動的に適用されます。詳細については、各種 OS のインストレーションガイドをご確認ください。

iLO タイムゾーン設定

iLO のタイムゾーンを設定します。Configure iLO Settings 権限を持ったユーザーで iLO の Web インターフェースにログインしてください。iLO 専用ネットワークポートを使用している場合、**[iLO Dedicated Network Port]→[SNTP]**ページを開いてください。iLO 共有ネットワークポートを使用している場合は、**[iLO Shared Network Port] →[SNTP]**ページを開いてください。

SNTP サーバーをお使いで iLO の時刻を SNTP サーバーと同期させる場合は、SNTP サーバーの設定を行ってください。

SNTP サーバーとの時刻同期機能をお使いにならない場合は、**[Use DHCPv4 Supplied Time Settings]**と**[Use DHCPv6 Supplied Time Settings]**を**[無効]**に、**[Primary Time Server]**と**[Secondary Time Server]**を空白にしてください。また、次のページの記載を参照し、**[Time Zone]**の設定を行ってください。

[Time Zone]は、**[Use DHCPv4 Supplied Time Settings]**と**[Use DHCPv6 Supplied Time Settings]**とが**[無効]**な場合にのみ設定可能です。

注意： iLO が正しい時刻を表示するために、SNTP サーバーとの時刻同期を行わない場合でもタイムゾーンの設定が必要になります。

手順(iLO 5 Firmware Version 1.30 May 31 2018 以降の場合)

1. iLO Web インターフェースの**[iLO Dedicated Network Port]→[SNTP]**ページにおいて、**[Use DHCPv4 Supplied Time Settings]**と**[Use DHCPv6 Supplied Time Settings]**を**[無効]**にしてください。
2. BIOS/プラットフォーム構成(RBSU)で**[Time Format]**に**[Local Time]**を設定している場合、[**Local Time]**に対応するタイムゾーンを**[Time Zone]**に設定してください。

   日本の場合、**[Asia/Tokyo(GMT+09:00:00:00)]/[Osaka, Sapporo, Tokyo, Seoul, Yakutsk (GMT+09:00:00:00)]**[11]**)**を選択し、**[Apply]**をクリックしてください。

   BIOS/プラットフォーム構成(RBSU)で**[Time Format]**に**[Coordinated Universal Time (UTC)]**を設定している場合、**[Time Zone]**に BIOS/プラットフォーム構成(RBSU)で設定されている**[Time Zone]**と同じ設定にしてください。

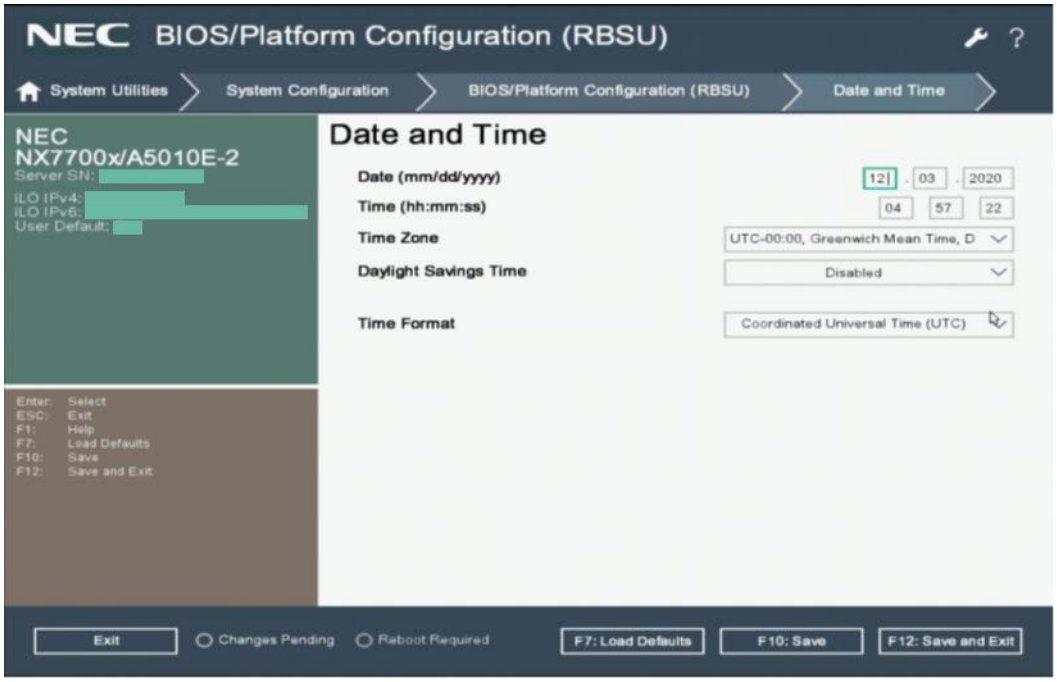
   RBSU の[Time Zone] が"UTC+09:00, Osaka, Sapporo, Tokyo, Seoul, Yakutsk"の場合、iLO の**[Time Zone]** には**[Asia/Tokyo(GMT+09:00:00:00)]/[Osaka, Sapporo, Tokyo, Seoul, Yakutsk (GMT+09:00:00:00)]**[12]**)**を選択し、**[Apply]**をクリックしてください。

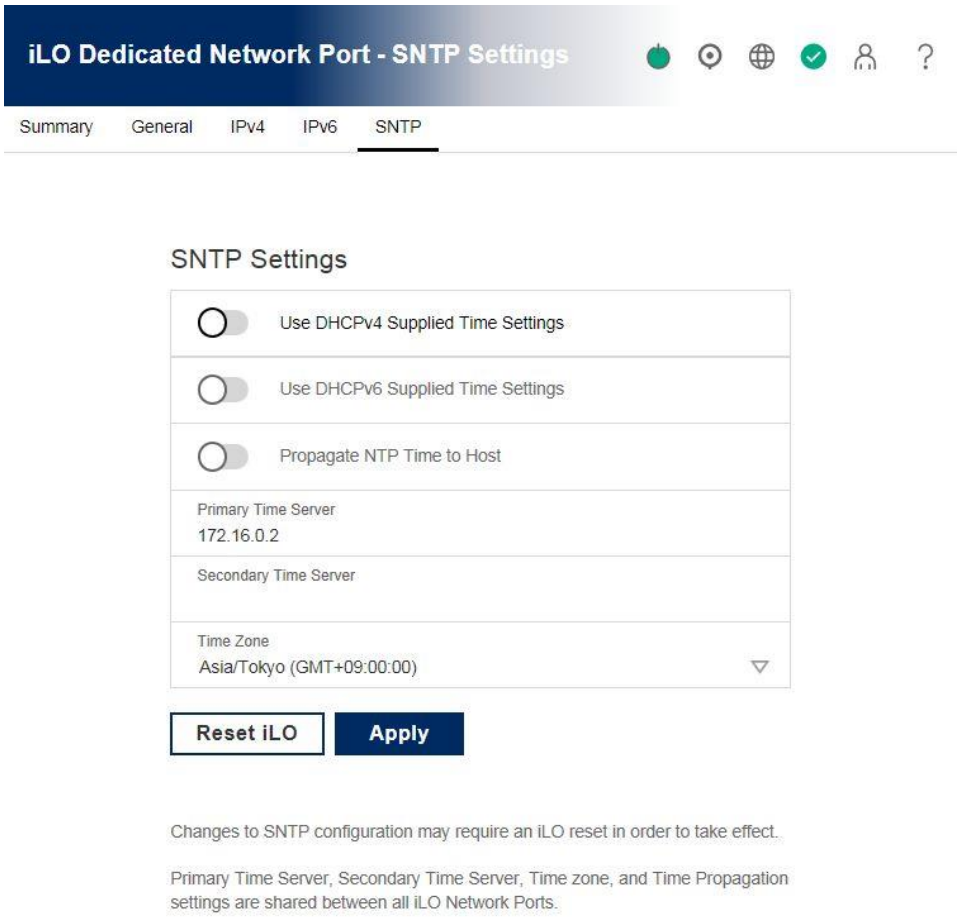
3. **[Reset iLO]**をクリックして、iLO を再起動します。

11 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

12 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

BIOS/プラットフォーム構成(RBSU)で**[Time Format]**に**[Coordinated Universal Time (UTC)]**を設定している場合

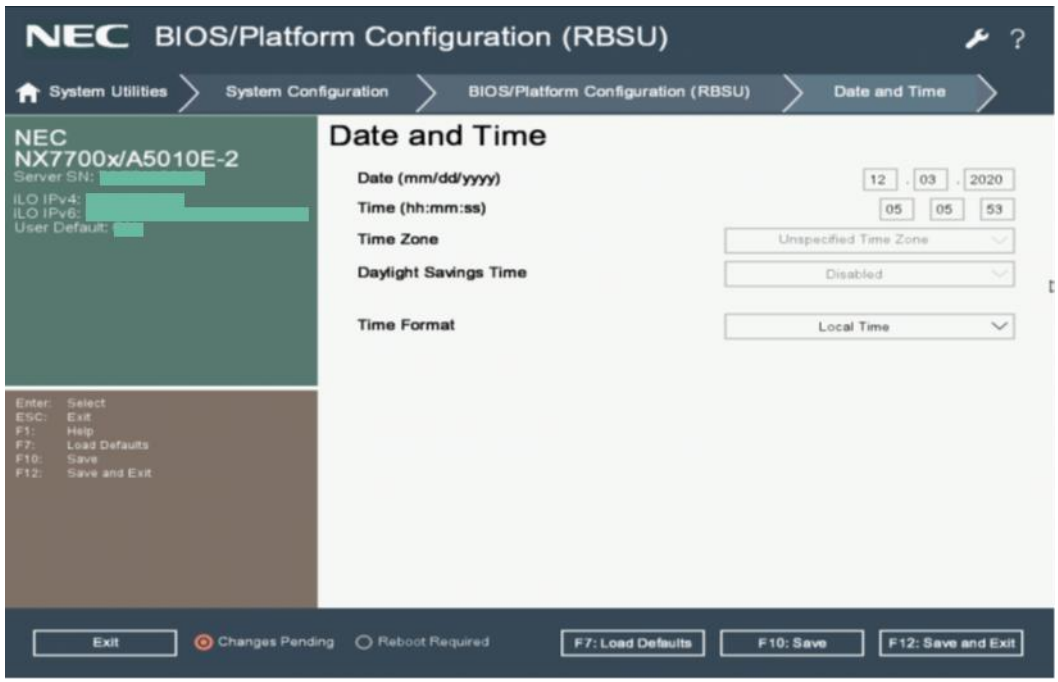




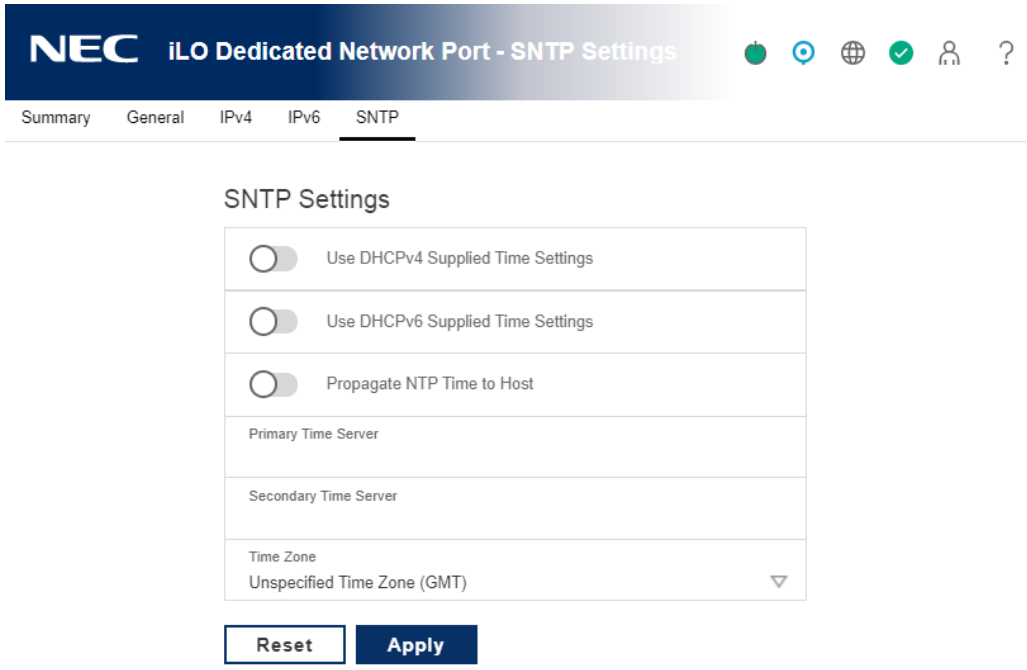
手順(iLO 5 Firmware Version 1.20 Feb 02 2018 以前の場合)

BIOS/プラットフォーム構成(RBSU)で**[Time Format]**に**[Local Time]**を設定している場合、**[Time Zone]**に**[Unspecified Time Zone (GMT)]**を設定してください。

BIOS/プラットフォーム構成(RBSU)



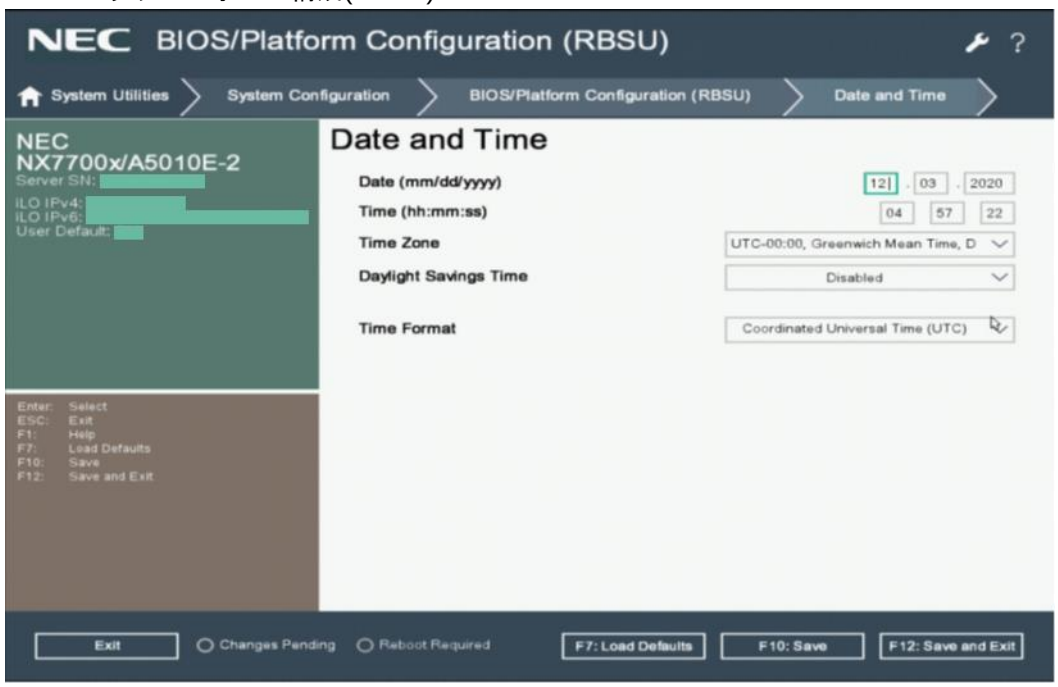
iLO Web インターフェース



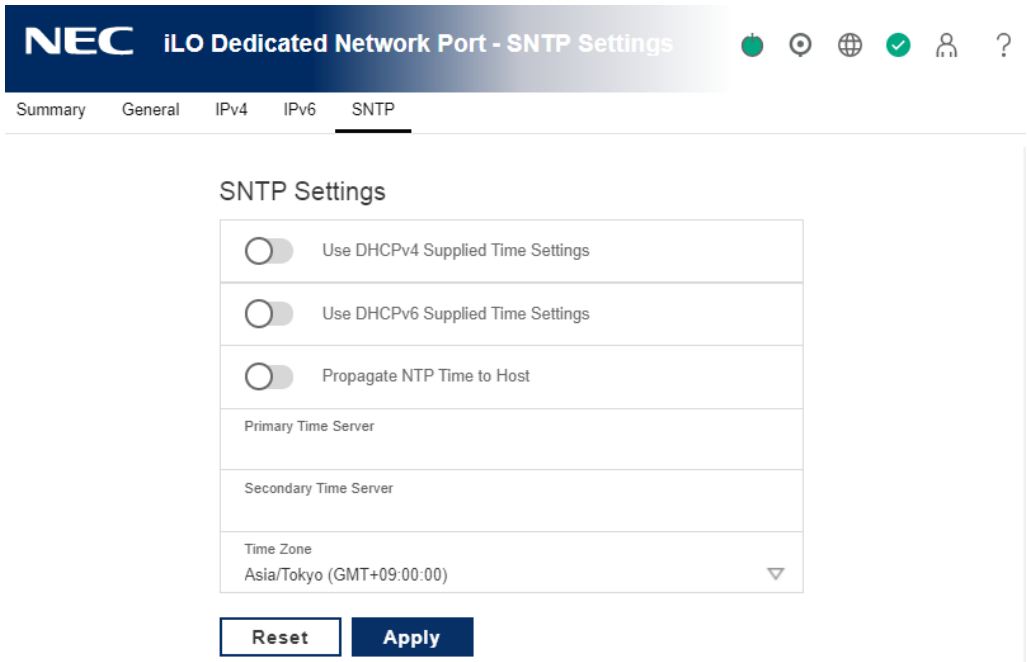
手順(iLO 5 Firmware Version 1.20 Feb 02 2018 以前の場合)

BIOS/プラットフォーム構成(RBSU)で**[Time Format]**に**[Coordinated Universal Time (UTC)]**を設定している場合、**[Time Zone]**に BIOS/プラットフォーム構成(RBSU)で設定したものと同じタイムゾーンを設定してください。

BIOS/プラットフォーム構成(RBSU)



iLO Web インターフェース



設定完了後、**[Apply]**を押し、続けて**[Reset]**を押してください。iLO の再起動が実行されます。iLO が再起動し、Web インターフェースにアクセスできるようになるまでしばらくお待ちください。

詳細情報

SNTP の設定
iLO Web インターフェースの使用

3. iLO Web インターフェースの使用

iLO の Web インターフェース

iLO Webインターフェースを使用してiLOを管理できます。また、リモートコンソール、SMASH CLP、またはiLO RESTful APIを使用することもできます。

ブラウザーのサポート

iLO Web インターフェースでは、以下の要件を満たすブラウザーが必要です。

- **JavaScript** - iLO の Web インターフェースは、クライアント側 JavaScript を頻繁に使用します。
- **Cookies** - 一部の機能が正常に動作するために、Cookie を有効にする必要があります。
- **ポップアップウィンドウ** - 一部の機能が正常に動作するために、ポップアップウィンドウを有効にする必要があります。ポップアップブロックが無効になっていることを確認してください。
- **TLS** - iLO の Web インターフェースにアクセスするには、ブラウザーで TLS 1.0 以降を有効にする必要があります。

iLO 5 がサポートするブラウザーは、以下のブラウザーの最新版になります。

［推奨ブラウザー］

- Microsoft Edge
- Mozilla Firefox
- Google Chrome mobile and desktop

［レガシーブラウザー］

- Microsoft Internet Explorer 11

> 注: Microsoft Edge 42 ブラウザー使用時にセキュリティ証明書のエラー警告が表示される場合、"詳細"をクリックし、"この Web ページの閲覧を続ける"をクリックしてください。信頼済みでない証明書の警告ポップアップを表示させなくするには、信頼済み証明書をインストールしてください。

iLO Web インターフェースへのログイン

1. **https://<iLO** ホスト名または **IP** アドレス**>** を入力します。

   iLO の Web インターフェースのアクセスには HTTPS を使用する必要があります（HTTPS は SSL 暗号セッションで交換される HTTP です）。

   iLO ログインページが開きます。 ログインセキュリティバナーが設定されている場合、バナーテキストは NOTICE セクションに表示されます。

2. 次のいずれかを実行します。

   - ログインページで、ディレクトリまたはローカルユーザーアカウント名とパスワードを入力して、**[Log In]**をクリックします。

- **[Zero Sign In]**ボタンをクリックします。

  iLO が Kerberos ネットワーク認証用に設定されている場合は、**[Log In]**ボタンの下に**[Zero Sign In]**ボタンが表示されます。**[Zero Sign In]**ボタンをクリックすると、ユーザー名とパスワードを入力しなくても、iLO にログインできます。

ログインのセキュリティとログインの問題について詳しくは、「ログインセキュリティ」および「ログインと iLO アクセスの問題」を参照してください。

ログインの 1 回目の失敗に対して、iLO ファームウェアはログインの遅延を課します。ログインの遅延設定について詳しくは、「iLO アクセスの設定」を参照してください。

ブラウザーインスタンスと iLO の間での Cookie の共有

iLO にアクセスし、ログインすると、1 つのセッション Cookie が、ブラウザーのアドレスバーで同じ iLO URL を開いているすべてのブラウザーウィンドウで共有されます。この結果、開いているすべてのブラウザーウィンドウが 1 つのユーザーセッションを共有します。1 つのウィンドウでログアウトすると、開いているすべてのウィンドウでユーザーセッションが終了します。新しいウィンドウで別のユーザーとしてログインすると、他のウィンドウ内のセッションが置き換えられます。

これは、ブラウザーの標準的な動作です。iLO は、同一クライアント上の同じブラウザー内の 2 つの異なるブラウザーウィンドウから複数のユーザーがログインすることをサポートしません。

共有インスタンス

iLO の Web インターフェースが別のブラウザーウィンドウまたはタブ（ヘルプファイルなど）を開く場合、このウィンドウは、iLO への同じ接続とセッション Cookie を共有します。

iLO の Web インターフェースにログインしているときに、手動で新しいブラウザーウィンドウを開くと、元のブラウザーウィンドウの複製インスタンスが開きます。アドレスバーのドメイン名が元のブラウザーセッションと一致する場合、新しいインスタンスは元のブラウザーウィンドウとセッション Cookie を共有します。

Cookie の順序

ログイン時に、ログインページは、ウィンドウを iLO ファームウェアの適切なセッションにリンクさせるブラウザーセッション Cookie を作成します。ファームウェアは、ブラウザーログインを、**[Information]**→**[Session List]**ページの**[Current Session]**セクションに示される個別のセッションとして追跡します。

たとえば、User1 がログインすると、Web サーバーは、上部の  アイコンをクリックした時に User1 でログインしていることを示し、左側ナビゲーションペインの項目を示し、右下のウィンドウにページデータを示す初期フレームビューを表示します。User1 が各リンクをクリックすると、ページデータがアップデートされます。

User1 がログインしているときに、User2 が同じクライアントでブラウザーウィンドウを開いてログインすると、元の User1 セッションで作成された Cookie は、2 番目のログインによって上書きされます。User2 が異なるユーザーアカウントである場合、異なる現在のフレームが作成され、新しいセッションが許可されます。2 番目のセッションは、**[Information]**→**[Session List]**ページの**[Current Session]**セクションに、User2 として表示されます。

2 番目のログインによって、User1 のログイン時に作成された Cookie が上書きされ、事実上、最初のセッションが親ブラウザーから切り離されています。この動作は、User1 のブラウザーが、

[Logout]ボタンをクリックせずに閉じられた場合と同じです。親ブラウザーから切り離された User1 のセッションは、タイムアウトしたときに再要求されます。

ブラウザーのページ全体が強制的に更新されない限り、現在のユーザーのフレームは更新されないので、User1 は、ブラウザーウィンドウを使用して操作を続けることができます。ただし、ブラウザーは、すぐに判別できない場合でも、すでに User2 のセッション Cookie 設定を使用して動作しています。

User1 がこのモード（User2 がログインしてセッション Cookie をリセットしたために User1 と User2 が同じプロセスを共有）で操作を続ける場合、以下の状態になることがあります。

- User1 のセッションは、User2 に割り当てられている権限を使用して継続的に動作します。
- User1 が操作しても User2 のセッションは中断されませんが、User1 のセッションはタイムアウトになる場合があります。
- どちらかのウィンドウがログアウトすると、両方のセッションが終了します。ログアウトしなかったほうのウィンドウでのその次の動作によって、ユーザーは、タイムアウトまたは早期タイムアウトが発生したかのように、ログインページに転送されることがあります。
- 2番目のセッション（User2）から**[Logout]**をクリックすると、次の警告メッセージが表示されます。

  Logging out: unknown page to display before redirecting the user to the login page.
- User2 が、ログアウトした後に User3 としてログインしなおすと、User1 は、User3 のセッションを共有します。
- User1 がログインしているときに User2 がログインする場合、User1 は、URL を変更してインデックスページに転送することができます。これにより、User1 は、ログインせずに iLO にアクセスしているかのような状態になります。

これらの動作は、複製ウィンドウが開いている限り継続されます。すべての動作は、最後のセッション Cookie セットを使用して、同じユーザーに帰属させられます。

現在のセッション Cookie の表示

ログイン後に URL ナビゲーションバーに次のように入力すると、ブラウザーに現在のセッション Cookie が表示されます。

javascript:alert(document.cookie)

表示される最初のフィールドにセッション ID が示されます。異なるブラウザーウィンドウでセッション ID が同じである場合、これらのウィンドウは同じ iLO セッションを共有しています。

F5 キーを押すか、**[表示]→[最新の情報に更新]**の順に選択するか、**[表示の更新]**ボタンをクリックすることによって、ブラウザーの表示を更新して、ユーザーの本当の ID を表示することができます。

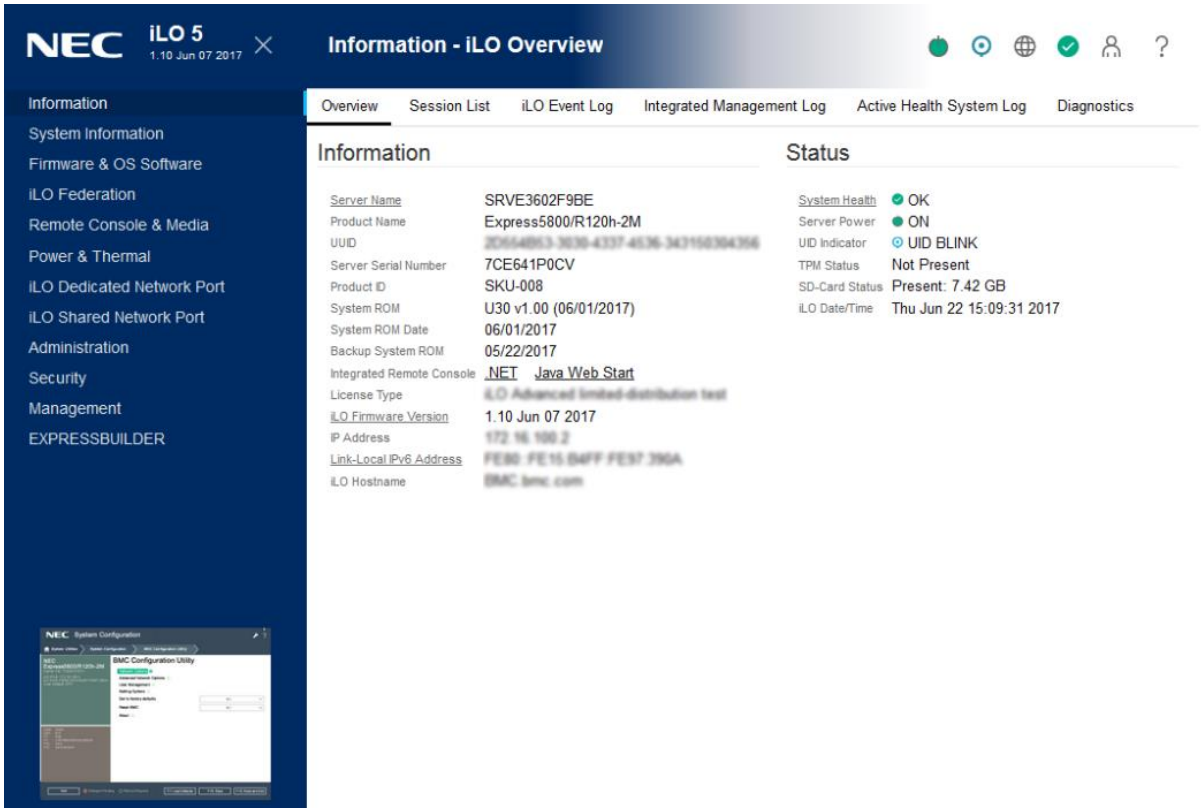
Cookie に関連する問題を回避するためのベストプラクティス

- ブラウザーのアイコンまたはショートカットをダブルクリックして、ログインごとに新しいブラウザーを起動します。
- ブラウザーウィンドウを閉じる前に、**サインアウト**ボタンをクリックして iLO セッションを閉じます。

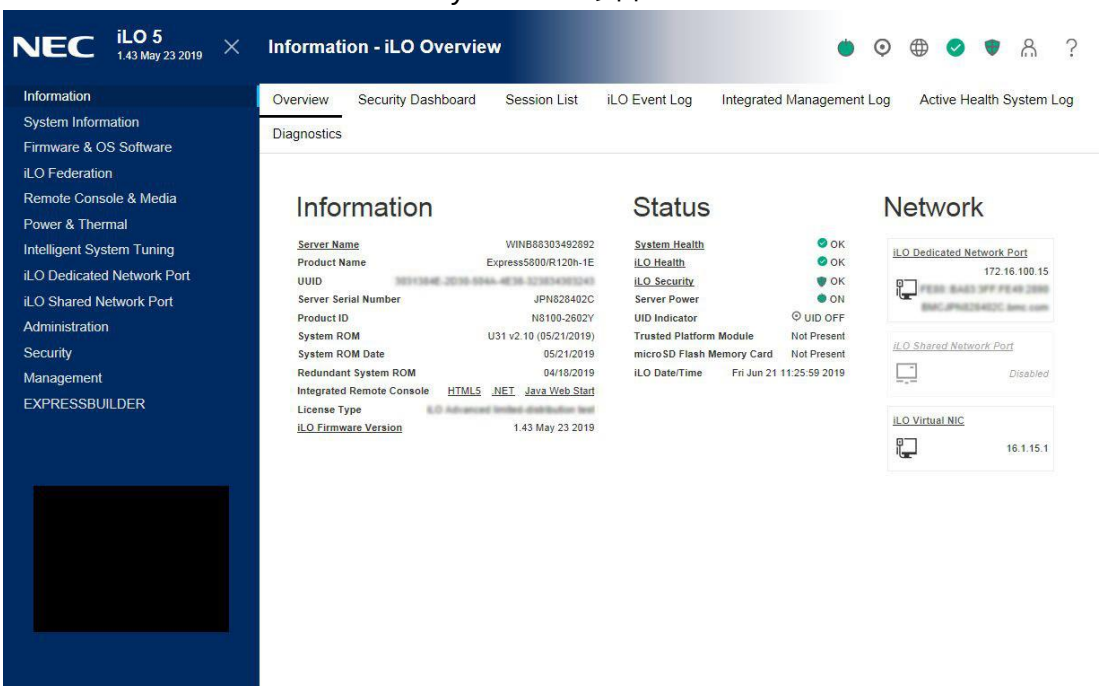
Web インターフェース

iLO の Web インターフェースは、類似の作業をグループ化しており、容易なナビゲーションとワークフローを提供します。インターフェースの編成は、このページの左側にあるナビゲーションペインに示されます。

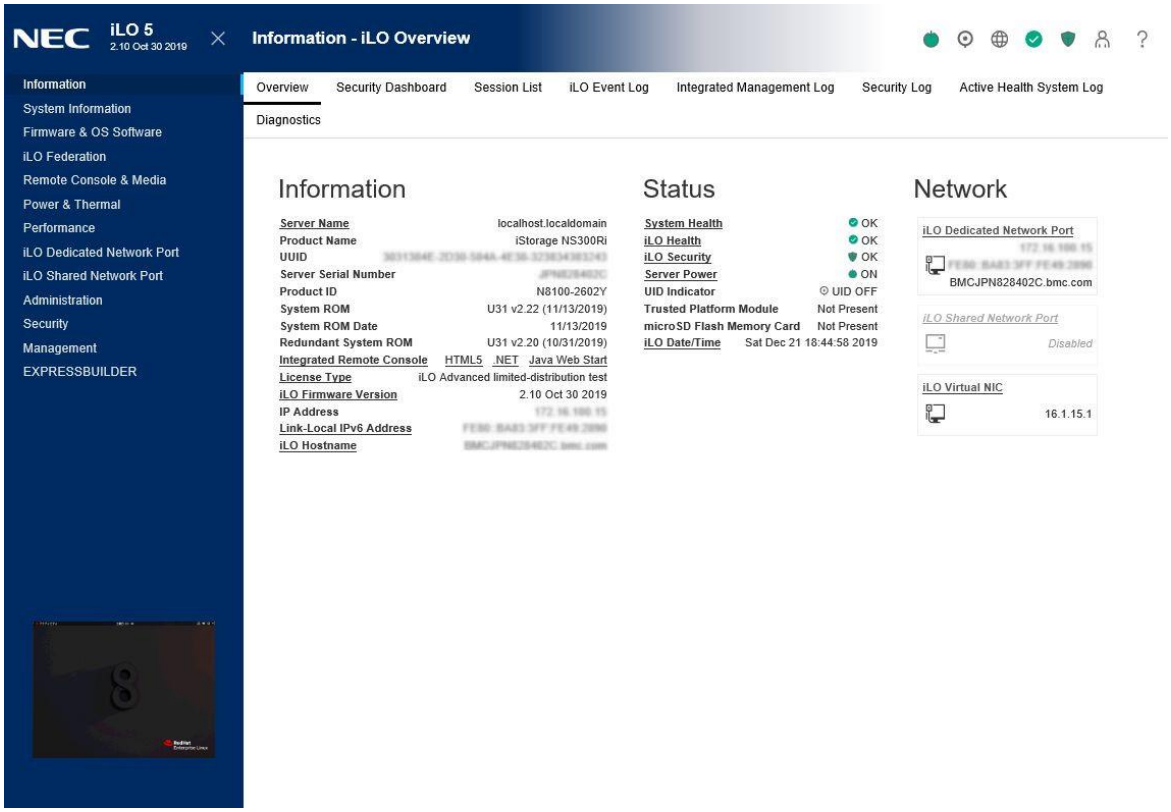
- iLO 5 Firmware Version 1.40 Feb 05 2019 以前



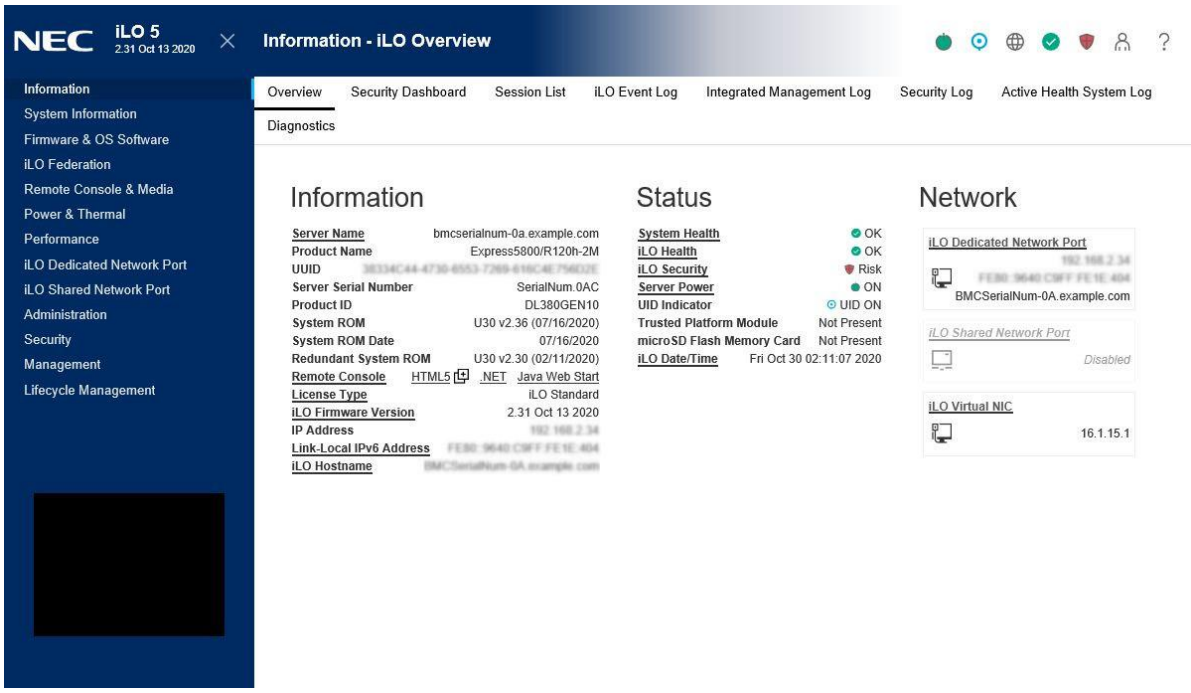
- iLO 5 Firmware Version 1.43 May 23 2019 以降



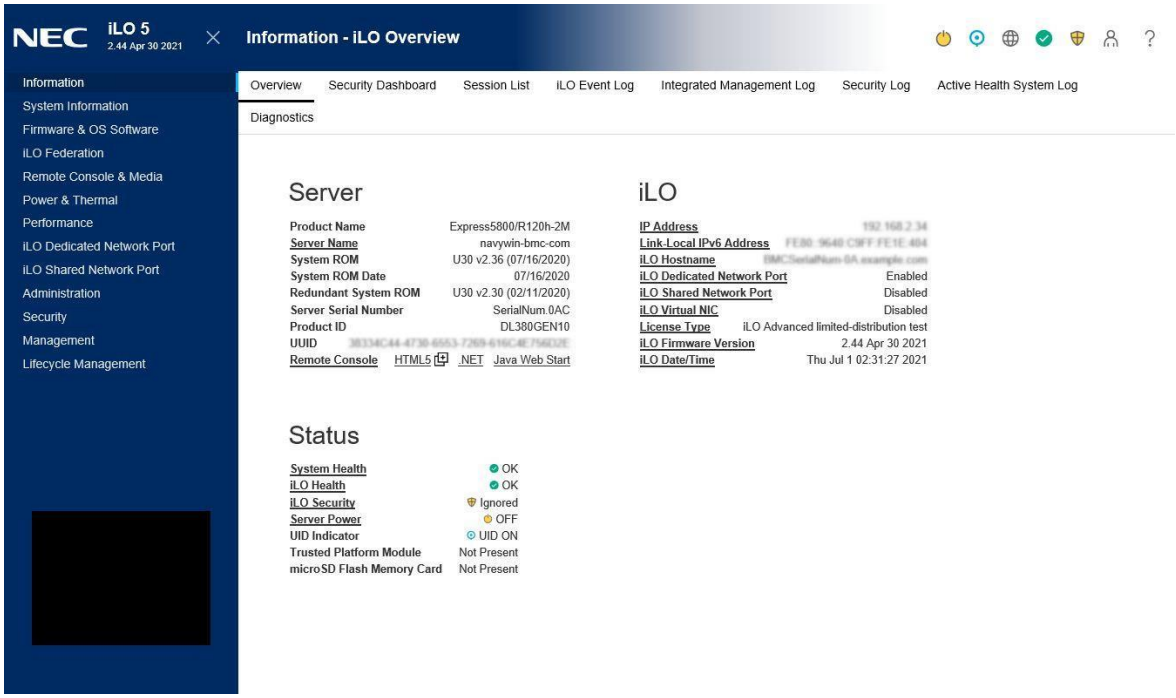
- iLO 5 Firmware Version 2.10 Oct 30 2019 以降



- iLO 5 Firmware Version 2.31 Oct 13 2020



- iLO 5 Firmware Version 2.44 Apr 30 2021 以降



iLO の Web インターフェースを使用する場合、以下の点に注意してください。

- 各メニューをクリックして表示されたページには、タブメニューがあります。タブメニュー項目をクリックして、対応する iLO Web インターフェースページを表示します。
- また、iLO のすべてのページについて操作方法の説明が用意されており、iLO のヘルプページから参照できます。ページ固有のヘルプにアクセスするには、そのページの右上にある「?」アイコンをクリックします。

iLO 制御の使用

iLO の Web インターフェースにログインすると、ブラウザーウィンドウの右上にある制御を任意の iLO ページから使用できます。

- **Power アイコン** - 仮想電源制御機能にアクセスするには、このメニューを使用します。
- **UID アイコン** - UID ランプをオン/オフにするには、このボタンを使用します。
- **言語アイコン** - このメニューを使用して、言語を選択するか、**[Administration]**→**[Language]**ページに移動します。このページでは、言語パックのインストールと、他の言語関連設定を行うことができます。このオプションは、言語パックがインストールされている場合のみ使用できます。
- **iLO セキュリティ** - セキュリティダッシュボードページの包括的な結果を示します。表示される値は、**[OK]**、**[Ignored]**、および**[Risk]**です。クリックすると、**[Security Dashboard]**ページに移動します。

- **ヘルスアイコン** - サーバーのファン、温度センサー、および他の監視対象サブシステムの全体的なヘルスステータスを表示するには、このアイコンを使用します。アイコンはヘルスステータスによって変化します。アイコンをクリックすると、監視対象コンポーネントのステータスが表示されます。AMS 以外のコンポーネントでは、コンポーネントを選択すると、コンポーネントのステータスに関する詳細が表示されます。
- **ユーザーアイコン** -このアイコンをクリックすると、次の操作を実行できます。
  - 現在の Web インターフェースセッションからログアウトするには、ユーザーアイコンをクリックし、**[Logout]**を選択します。
  - アクティブなセッションを表示するには、ユーザーアイコンをクリックし、**[Sessions]**を選択します。
  - ユーザーアカウントを表示または変更するには、ユーザーアイコンをクリックし、**[Settings]**を選択します。
- **ヘルプアイコン** -このアイコンをクリックすると、現在のページのオンラインヘルプが表示されます。
- **省略アイコン** - ブラウザーウィンドウが小さすぎてフルページを表示できない場合に表示されることがあります。

iLO ナビゲーションペイン

iLO には、各ページからアクセス可能で縮小可能なナビゲーションペインがあります。

- ナビゲーションペインの表示と非表示を切り替えるには、iLO Web インターフェースの左上隅にあるアイコンをクリックします。

- ナビゲーションペインを非表示にするには、X アイコンをクリックします。
- ナビゲーションペインには、リモートコンソールのサムネイルが表示されます。リモートコンソールを起動するには、サムネイルをクリックし、メニューからコンソールオプションを選択します。
- モニター付きサーバーの場合は、ナビゲーションペインのリモートコンソールのサムネイルをクリックし、スリープモードになっているモニターを起動するために**[Wake-Up Monitor]**を選択します。

ログインページからの言語の変更

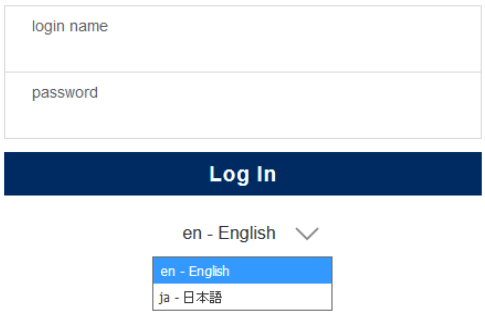
現在、言語パックが iLO にインストールされている場合は、iLO セッション用の言語を選択するために、ログイン画面で**言語**メニューが使用できます。この選択は、今後の Web インターフェースを表示するために、ブラウザーの Cookie に保存されます。

前提条件

言語パックがインストールされている。

手順

1. iLO のログインページに移動します。
2. 言語メニューから言語を選択します。



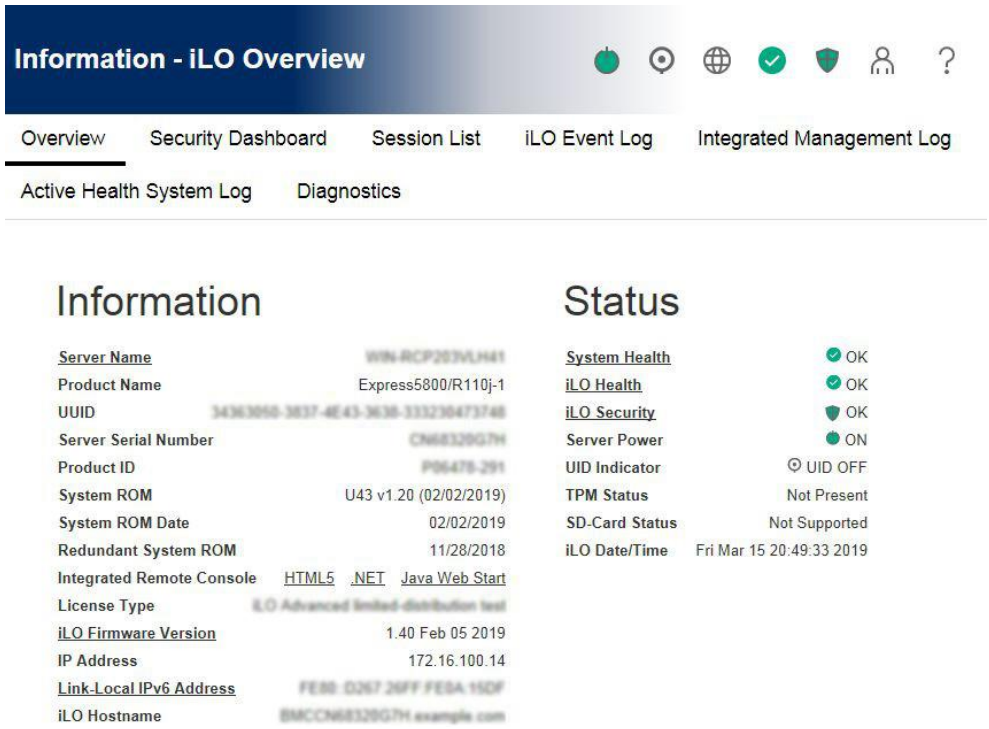
4. iLO の情報とログの表示

iLO の概要情報の表示

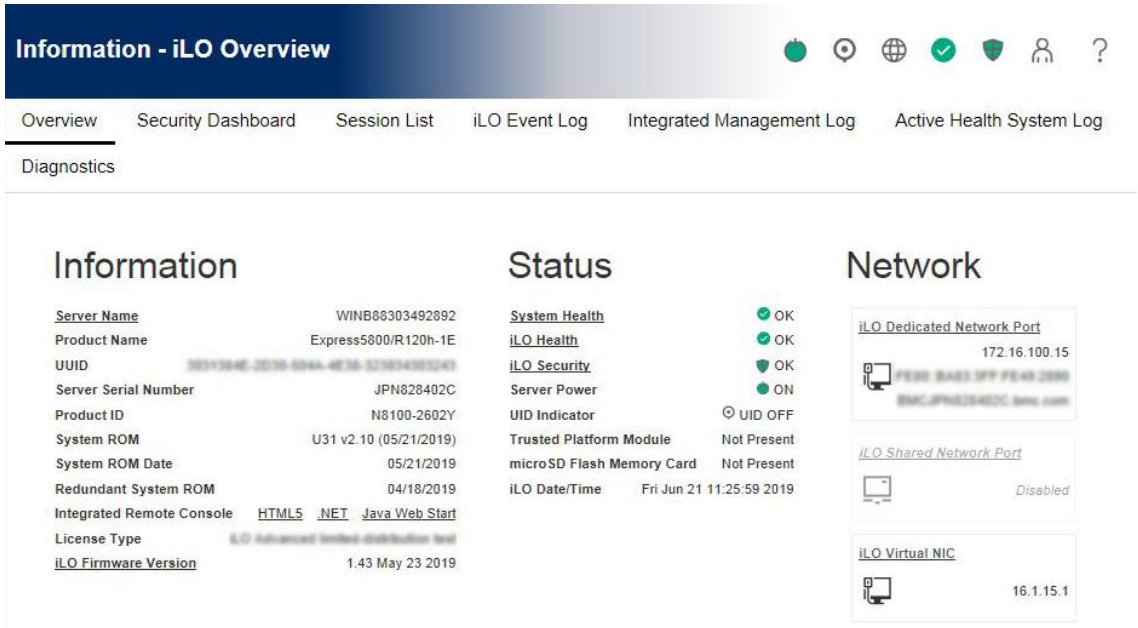
[Information]→[Overview]ページに移動します。

iLO Overview ページは、サーバーと iLO サブシステムに関する概要を表示し、一般に使用される機能へリンクします。

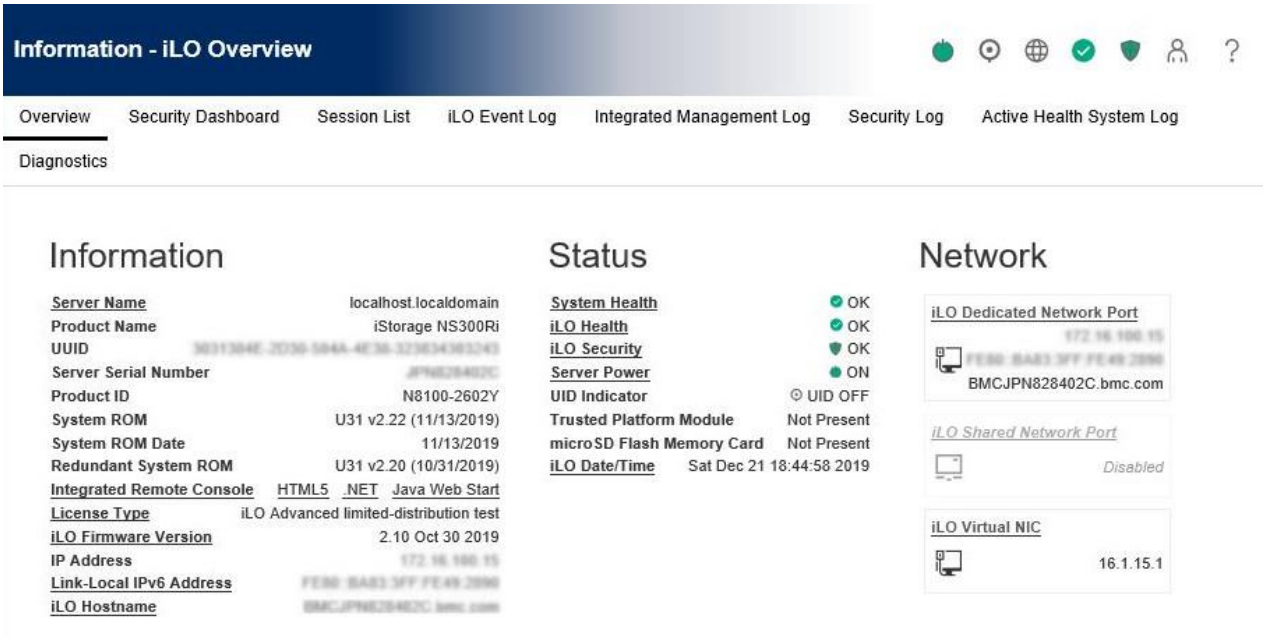
- iLO 5 Firmware Version 1.40 Feb 05 2019 以前



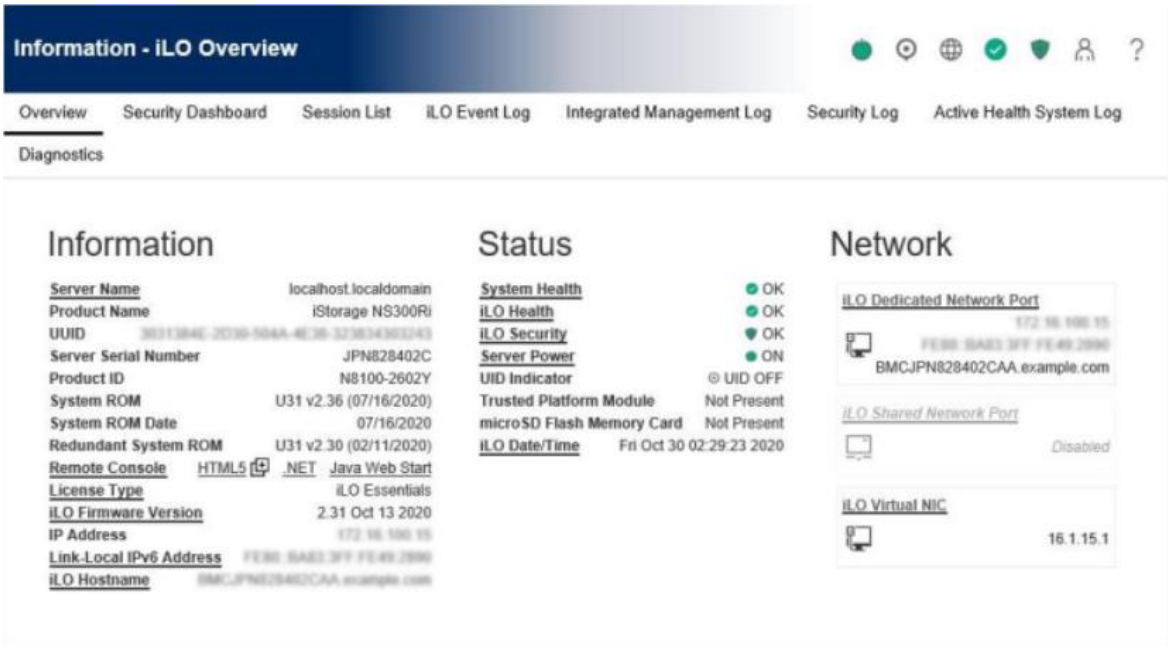
- iLO 5 Firmware Version 1.43 May 23 2019 以降



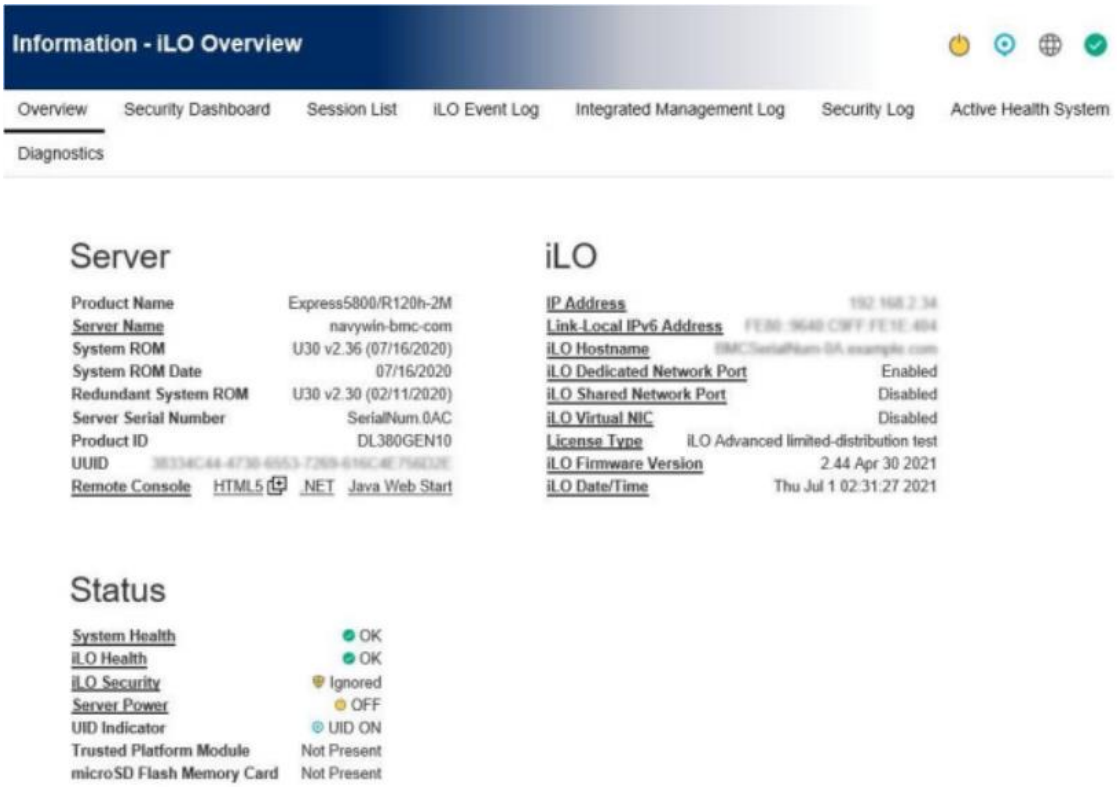
- iLO 5 Firmware Version 2.10 Oct 30 2019 以降



- iLO 5 Firmware Version 2.31 Oct 13 2020 以降



- iLO 5 Firmware Version 2.44 Apr 30 2021 以降



システム情報の詳細

- **[Server Name]** - ホストオペレーティングシステムで定義されたサーバー名。**[Server Name]** リンクをクリックすると**[Access Settings]**ページに移動します。
- **[Product Name]** - この iLO プロセッサーが搭載されているシステムの製品名。
- **[UUID]** - ソフトウェアがこのホストを一意に識別するために使用する UUID（Universally Unique Identifier）。この値は、システムの製造時に割り当てられます。
- **[UUID (Logical)]** - ホストアプリケーションから提示されるシステム UUID。**[UUID (Logical)]** の値が設定されていないと、この項目は表示されません。
- **[Server Serial Number]** - システムの製造時に割り当てられるサーバーシリアル番号。POST 実行時にシステムユーティリティを使用すると、この値を変更できます。
- **[Serial Number (Logical)]** - ホストアプリケーションに提示されるシステムシリアル番号。**[Serial Number (Logical)]**の値が設定されていないと、この項目は表示されません。
- **[Product ID]** - この値は、同じシリアル番号を持つ異なるシステムを区別します。製品 ID は、システムの製造時に割り当てられます。POST 実行時にシステムユーティリティを使用すると、この値を変更できます。
- **[System ROM]** - アクティブなシステム ROM のバージョン。
- **[System ROM Date]** - アクティブなシステム ROM の日付。
- **[Backup System ROM/Redundant Backup System ROM]** - バックアップシステム ROM の日付。バックアップシステム ROM は、システム ROM の更新に失敗した場合や、システム

ROM がロールバックされる場合に使用されます。この値は、システムがバックアップシステム ROM をサポートする場合のみ表示されます。

- **[Integrated Remote Console]** - サーバーコンソールとのリモートアウトバンド通信用に.NET IRC、Java IRC アプリケーション、または HTML5 IRC を起動するためのリンクを提供します。

  HTML5 IRC で⊞をクリックすると、新しいウィンドウでコンソールを開きます。

  Java IRC を使用するときは次の点に留意してください。

  - Windows または Linux と Oracle JRE の環境の場合は、**[Java Web Start]**リンクを使用します。
  - Linux と OpenJDK JRE の環境の場合は、**[Remote Console & Media]**ページにて**[Applet]**リンクを使用します。

- **[License Type]** - 適用済みの iLO ファームウェアライセンス。
- **[iLO Firmware Version]** - インストールされている iLO ファームウェアのバージョンと日付。**[iLO Firmware Version]**リンクをクリックし、**[Firmware & OS Software]**ページに移動します。
- **[IP Address]** - iLO サブシステムのネットワーク IPv4 アドレス。
- **[Link-Local IPv6 Address]** - iLOサブシステムのSLAACリンクローカルアドレス**[Link-Local IPv6 Address]**リンクをクリックして、**[iLO Dedicated Network Port]→[Summary]**ページに移動します。この値は、iLO 専用ネットワークポート構成についてのみ表示されます。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。デフォルトのホスト名は[BMC]+システムのシリアル番号および現在のドメイン名です。この値はネットワーク名に使用され、一意である必要があります。

システムステータスの詳細

- **[System Health]** - サーバーヘルスインジケーター。この値は、全体的なステータスや冗長性（障害処理能力）など、監視対象サブシステムの状態を要約します。起動時にいずれかのサブシステムが冗長でなくても、システムヘルスステータスはデグレードしません。**[System Health]**リンクをクリックし、**[System Information]→[Summary]**ページに移動します。
- **[iLO Health]** - iLO ヘルスステータス。iLO 診断セルフテストを組み合わせた結果に基づいています。表示される値は、**[OK]**または**[Degraded]**です。診断ページに移動するには、**[iLO Health]**リンクをクリックします。
- **[iLO Security]** –iLO のセキュリティ状態。セキュリティダッシュボードページからの結合した結果に基づいています。表示される値は、**[OK]**、**[Ignored]**、および**[Risk]**です。セキュリティダッシュボードページに移動するには、**[iLO Security]**リンクをクリックします。
- **[Server Power]** - サーバー電力の状態（**[ON]**または**[OFF]**）。
- **[UID Indicator]** - UID ランプ の状態。UID ランプを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**[UID ON]**、**[UID OFF]**、および**[UID BLINK]**があります。

サーバーシャーシにある UID スイッチまたは iLO Web インターフェースの上部にある UID 制御アイコンを使用すると、UID ランプの状態を**[UID ON]**または **[UID OFF]**に変更することができます。

UID ランプが点滅しているとき、**[UID Indicator]**にはステータスが **[UID BLINK]**と表示されます。UID ランプの点滅が停止すると、ステータスは前回の値（**[UID ON]**または **[UID OFF]**）に戻ります。UID ランプが点滅している間に新しい状態を選択すると、UID ランプが点滅を停止したときに新しい状態が有効になります。

iLO サービスポートを使用中は、[**UID BLINK (Service Port Busy)**]、[**UID BLINK (Service Port Error)**]、および[**UID BLINK (Service Port Finished)**]を表示します。

△ 注意**:** ホストでリモートコンソールのアクセスやファームウェアの更新のような重要な操作が進行中であると UID ランプは自動的に点滅します。UID ランプの点滅中は、絶対にサーバーの電源を切らないでください。

- **[TPM Status]**または **[TM Status]** - TPM または TM ソケットまたはモジュールのステータス。
- **[Module Type]** - TPM または TM の種類と仕様のバージョン。指定できる値は、**[TPM 1.2]**、**[TPM 2.0]**、**[TM 1.0]**、**[TPM Module 2.0 (Intel PTT)]**、**[Not Specified]**、および**[Not Supported]**です。この値は、サーバーに TPM または TM が存在する場合に表示されます。
- **[SD-Card Status]** - 内蔵 SD カードの現在のステータス。SD カードが存在する場合、SD カードのブロック数が表示されます。
- **[iLO Date/Time]** - iLO サブシステムが持つ日時。

※ iLO 5 Firmware Version 2.44 Apr 30 2021 以降

- **[Platform RAS Policy]** - 構成されたプラットフォームの耐障害性及び保守性(RAS)ポリシー。保守性(RAS)ポリシーには以下があります。
  - Firmware First (デフォルト) - BIOS は、メモリ等の訂正可能障害を監視し、訂正されたエラーに対してアクションが必要な場合、イベントを IML ログに記録します。この構成では、OS は、訂正されたエラーの監視および OS のシステムログへの記録を行いません。
  - OS First - 訂正済みエラーは OS に通知され、OS が OS のシステムログへの記録等を制御します。

△注記：訂正可能障害(エラー)は、当然起こるものと予想されます。訂正可能障害(エラー)イベントが IML ログに記録されていない限り、アクションを実行する必要はありません。

この設定は、System Utilities の「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options」にて設定できます。
デフォルト設定を使用することをお勧めします。

ネットワークの詳細[13]

- **[Active network interface name]** - アクティブな iLO ネットワークインターフェース（iLO 専用ネットワークポートまたは iLO 共有ネットワークポート）の名前。**[Active network interface name]**のリンクをクリックすると、各 iLO ネットワークインターフェースの**[Network Summary]**ページに移動します。
- **[IP Address]** - 現在使用中の IPv4 アドレス。IPv4 アドレスが設定されていない場合、表示されません。
- **[Link-Local IPv6 Address]** - SLAAC リンクローカルアドレス。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。この値はネットワーク名に使用され、一意である必要があります。

iLO Virtual NIC[14]

iLO Virtual NIC セクションでは、仮想 NIC に接続するための IP アドレスが表示されます。

[iLO Virtual NIC]のリンクをクリックすると、**[Access Settings]**ページに移動します。**[Virtual NIC]**が**[Disabled]**に設定されている場合は、本セクションは表示されません。

セキュリティダッシュボードの使用[15]

セキュリティダッシュボードページには、重要なセキュリティ機能のステータス、システムの全体セキュリティステータス、セキュリティ状態およびサーバー構成ロック機能の現在の構成が表示されます。ダッシュボードを使用して、構成の潜在的なリスクについて評価します。リスクが検知されたら、詳細情報とシステムセキュリティを向上させる方法についてのアドバイスを見ることができます。

前提条件
iLO の設定を構成権限

手順

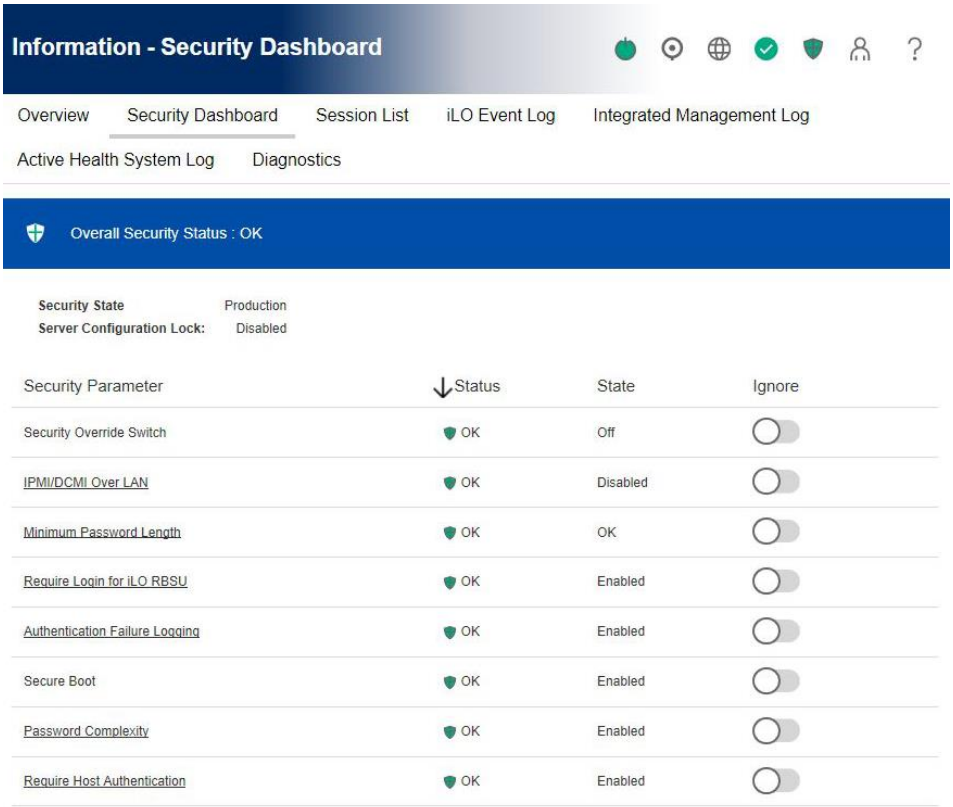
1. ナビゲーションツリーで**[Information]**をクリックして、セキュリティダッシュボードタブをクリックします。

13 iLO 5 Firmware Version 1.43 May 23 2019 以降

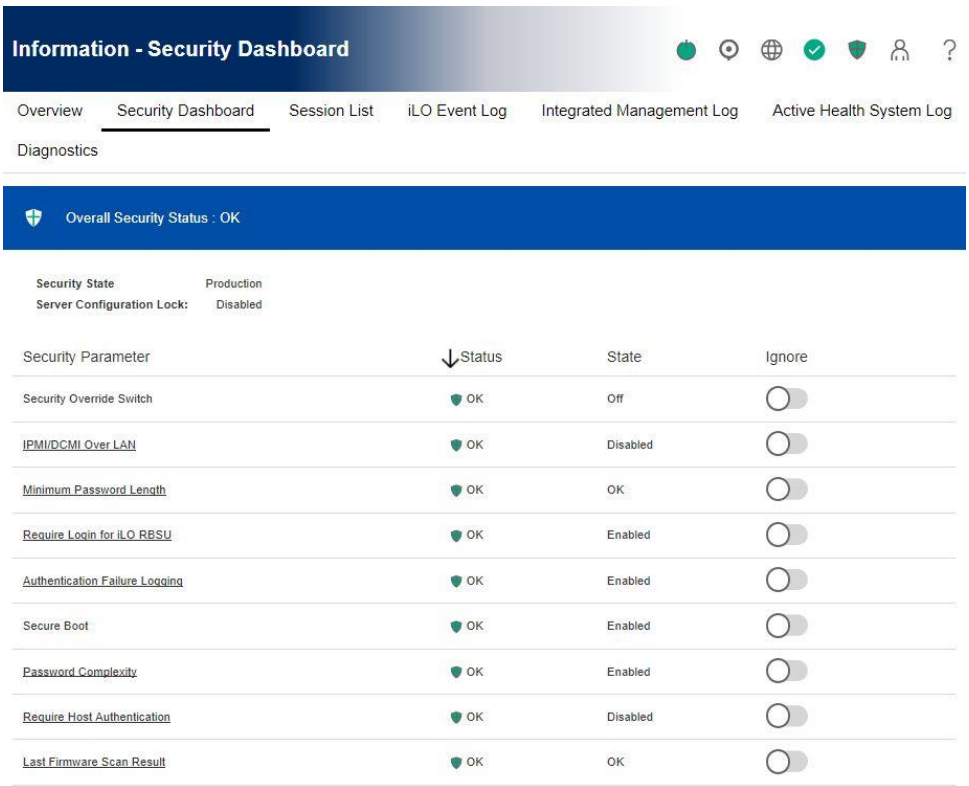
14 iLO 5 Firmware Version 1.43 May 23 2019 以降

15 iLO 5 Firmware Version 1.40 Feb 05 2019 以降

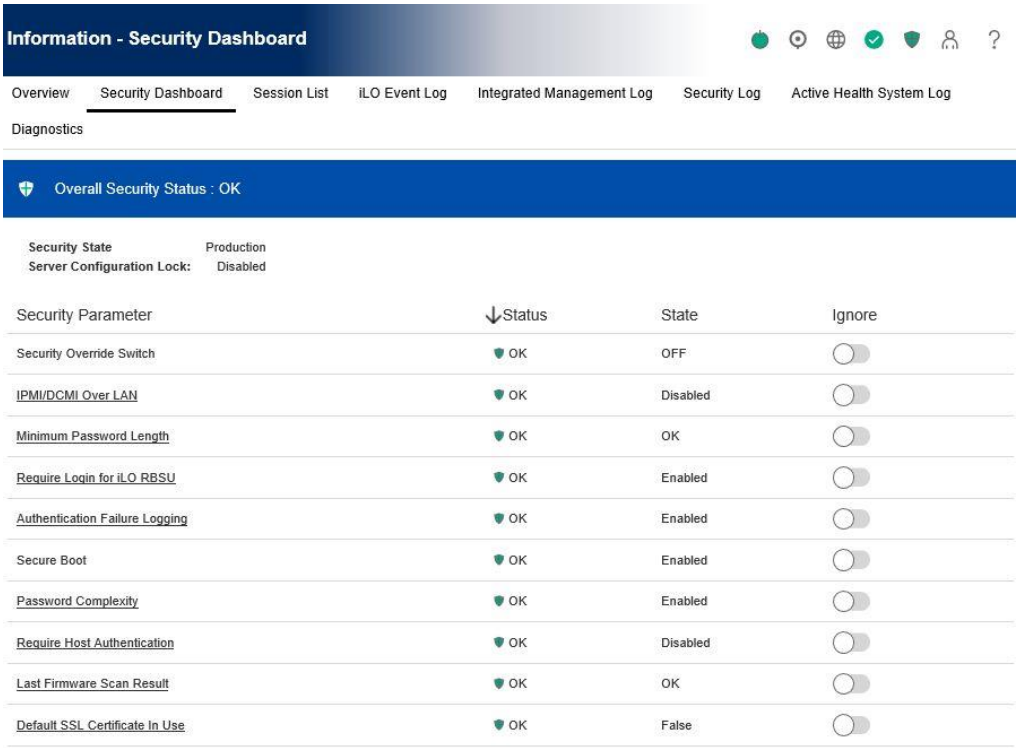
- iLO 5 Firmware Version 1.40 Feb 05 2019



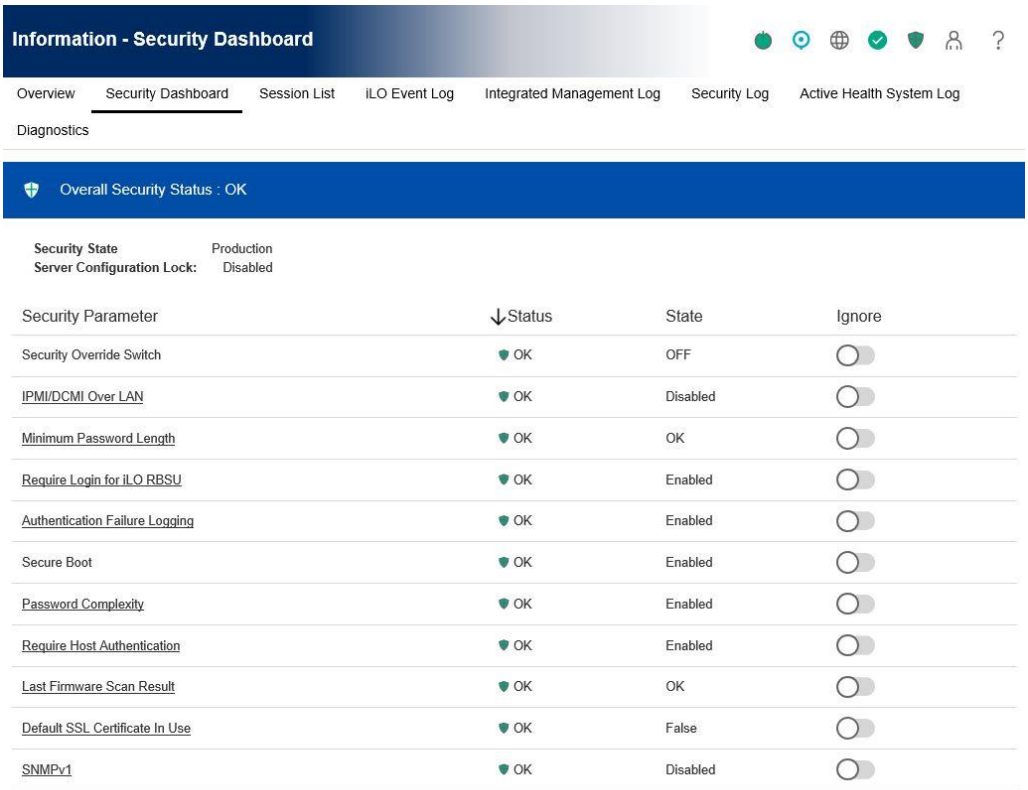
- iLO 5 Firmware Version 1.43 May 23 2019 以降



- iLO 5 Firmware Version 2.10 Oct 30 2019 以降



- iLO 5 Firmware Version 2.31 Oct 13 2020 以降



2. オプション：テーブルの列でソートするには、見出し列をクリックします。

   ソート順を昇順または降順に変更するには、見出し列をもう一度クリックするか、見出し列の横にある矢印アイコンをクリックします。

3. セキュリティダッシュボード表で検出されたリスクについて確認します。

   セキュリティ機能にリスクステータスが付いて表示されている場合は、ステータスの値をクリックすると詳細情報が表示されます。詳細情報には、リスクと可能な解決策についての情報が含まれています(説明、及び推奨されるアクションの内容は英語表記)。

4. オプション：**[Ignore]**オプションをセキュリティ機能に構成します。

   - **[Ignore]**オプションは、デフォルトでは**[Disabled]**になっています。
   - **[Ignore]**オプションをセキュリティ機能に対して有効にすると、iLO が全体セキュリティステータスを判定するときその機能のステータスは無視されます。セキュリティ機能のステータスを無視に変更しても、セキュリティダッシュボード表のステータス値は変わりません。

セキュリティ機能を**[Ignore]**に変更すると、iLO が全体セキュリティステータスを再表示します。

セキュリティダッシュボード詳細

全体セキュリティステータス

- **[OK]** - iLO が監視対象のセキュリティ機能に関連したセキュリティリスクをは検出されませんでした。
- **[Risk]** - iLO が監視対象のセキュリティ機能に関連する潜在的なセキュリティリスクを一つ以上検出しました。
- **[Ignore]** - iLO が監視対象のセキュリティ機能に関連する潜在的なセキュリティリスクを 1 つ以上検出しました。影響を受けるすべての機能が全体セキュリティステータスから除外されるよう設定されています。

  このステータスは、概要ページと iLO のコントロールにも表示されます。

セキュリティ状態

構成されているセキュリティ状態を表示します。表示される値は、以下の通りです。

- Production
- High Security
- FIPS

詳しくは、「iLO セキュリティ状態」を参照してください。

サーバー構成ロック

構成されるサーバー構成ロックの設定状態を示します。SysROM v2.30 以降でサポートされています。

セキュリティダッシュボード表

- **[Security Parameter] -** セキュリティ機能をテストします。監視対象のセキュリティ機能の名前。iLO Web インターフェースで構成できる機能については、この列のリンクをクリックして関連する web インターフェースページに移動してください。
- **[Status] -** 監視対象のセキュリティ機能のセキュリティステータス。
  - [**OK**] - iLO がこの機能に関連したセキュリティリスクを検出しませんでした。
  - [**Risk**] - iLO がこの機能に関連した潜在的なセキュリティリスクを検出しました。
- **[State]** - 監視対象のセキュリティ機能の現在の状態。表示される値は、以下のとおりです。
  - **[Enabled]** - 機能は有効です。
  - **[Disabled]** - 機能は無効です。
  - **[Insufficient]** - 機能は有効ですが、推奨される構成は使用されていません。
  - **[Off]** - 機能はオフに設定されています。
  - **[On]** - 機能はオンに設定されています。
  - **[OK]** - 機能は iLO のセキュリティ推奨事項に準拠しています。
  - **[Failed]** - 機能は障害を報告しました。
  - **[Repaired]** - 機能は、修正された障害を報告しました。
  - **[True]** - 機能は使用中です。
  - **[False]** - 機能は使用されていません。
- **[Ignore]** −この列に表示されるトグルスイッチを使って、セキュリティ機能を無視するよう設定できます。**[Ignore]**に設定すると、監視対象のセキュリティ機能は全体セキュリティステータス値に含まれません。

  セキュリティ機能を**[Ignore]**に設定しても、セキュリティダッシュボード表のステータスは変わりません。

> △**参考:**
> [BIOS/Platform Configuration (RBSU)]-[Sever Security]-[Server Configuration Lock]において、[Enabled]を設定してください。

リスク詳細

セキュリティダッシュボードページでセキュリティ機能のリスク詳細を表示すると、以下の情報が利用可能です。

- **[Enabled]** - セキュリティ機能がリスクステータスになっている理由の説明。
- **[Recommended Action]** - 推奨される解決策。

  [Ignore]オプションが有効になっている場合、この値は表示されません。

- **[Ignored]** - 無視オプションが有効になった日時。
- **[Ignored by]** - 無視オプションを有効にしたユーザーの名前。

セキュリティリスク状態の原因

以下のセキュリティ機能がセキュリティダッシュボードページで監視されます。サーバーでサポートされない機能は表示されません。

[Default SSL Certificate In Use][16]

iLO のデフォルト自己署名証明書が使用中です。信頼済みの証明書を**[Security] - [SSL Certificate] - [Customize Certificate]**ページで構成することをお勧めします。

[IPMI/DCMI over LAN]

IPMI/DCMI over LAN 機能が有効になっています。これにより、サーバーは既知の IPMI に関するセキュリティ脆弱性にさらされます。詳細は、「iLO の主な機能」を参照してください。
IPMI/DCMI over LAN を**[Disabled]**にすることをお勧めします。
詳しくは、iLO アクセス設定を参照してください。

[Password Complexity]

iLO は、パスワードの複雑さのガイドラインを適用するように構成されていません。これにより、サーバーは辞書攻撃に対して脆弱になります。
この機能を有効にすることをお勧めします。
詳しくは、iLO アクセス設定を参照してください。

[Security Override Switch]

サーバーのセキュリティオーバーライドスイッチ（システムメンテナンススイッチとも呼ばれる）が有効になっています。セキュリティオーバーライドスイッチを有効にすると、ログイン認証が不要なため、この構成は 1 つのリスクです。
この機能を**[Disabled]**にすることをお勧めします。
詳しくは、装置のユーザーガイドを参照してください。

[Minimum Password Length]

最小パスワード長が推奨の長さよりも短くなっています。これにより、サーバーは辞書攻撃に対して脆弱になります。
この値を 8(デフォルト)以上に設定することをお勧めします。
詳しくは、iLO アクセス設定を参照してください。

[Require Login for iLO RBSU]

iLO は、UEFI システムユーティリティの BMC 構成ユーティリティへのアクセスにログイン認証情報を要求するよう構成されていません。この構成では、システムブート中に iLO 構成への認証なしのアクセスが許可されます。
この機能を有効にすることをお勧めします。
詳しくは、iLO アクセス設定を参照してください。

[Authentication Failure Logging]

iLO は、iLO への認証の失敗を記録するように構成されていません。
この機能を有効にすることをお勧めします。
詳しくは、iLO アクセス設定を参照してください。

16 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

[Secure Boot]

UEFI セキュアブートオプションが**[Disabled]**になっています。この構成では、UEFI システムファームウェアは、信頼された署名がブートローダー、オプション ROM ファームウェア、およびシステムソフトウェアの実行ファイルにあるかどうかの検証をスキップします。これにより、電源オン時に iLO によって確立された信頼チェーンが壊れます。
この機能を有効にすることをお勧めします。
詳しくは、UEFI システムユーティリティのドキュメントを参照してください。

> △**参考:**
> [RBSU]-[Sever Security]-[Attempt Secure Boot]において、[Enabed]を設定してください。

[Require Host Authentication]

iLO は、RESTful API 経由での iLO へのアクセス時にログイン認証情報を要求するよう構成されていません。この構成では、RESTful API 経由での iLO への認証なしのアクセスが許可されます。
詳しくは、iLO アクセス設定を参照してください。

[SNMPv1]

SNMPv1 は有効になっています。この構成は、iLO での SNMPv1 要求の受信および SNMPv1 アラートの送信を許可します。SNMPv1 を有効にすると、攻撃に対するシステムの脆弱性が増加します。
SNMP 設定ページでこの機能を無効にすることをお勧めします。

[Last Firmware Scan Result][17]

> △**注記:**iLO5 ファームウェア 1.43 および 1.45 をご使用の場合、**[Last Firmware Scan Result]** がハイパーリンク表示されますが、本ハイパーリンクのクリックは行わないでください。誤ってクリックしてしまうと、各メニューおよびタブ間の移動ができなくなります。もし、誤ってクリックを行ってしまった場合は、以下のいずれかの方法で復旧させてください。
> ・ブラウザーのリロードボタンをクリックする。
> ・iLO Web インターフェースのログアウトを行い、再度ログインを行う。

最新のファームウェア検証テストが失敗しました。ファームウェアコンポーネントが壊れているか、その整合性が損なわれています。
影響のあるファームウェアコンポーネントを、検証済みのイメージにアップデートすることをお勧めします。NX7700xシリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。。

iLO セッションの管理

前提条件

ユーザーアカウント管理権限

手順

17 iLO 5 Firmware Version 1.43 May 23 2019 以降

1. [**Information**]ページに移動し、[**Session List**]タブをクリックします。セッションリストページには、アクティブな BMC セッションに関する情報が表示されます。

2.オプション：1 つまたは複数のセッションを切断するには、切断する各セッションの左にあるチェックボックスにチェックしてから、**[Disconnect Session]**をクリックします。

セッションリストの詳細

BMC は、Current Session および Session List テーブルに次の詳細を表示します。

- **[User]** - BMC ユーザーアカウント名。
- **[IP]** - iLO へのログインに使用されたコンピューターの IP アドレス。
- **[Login Time]** - BMC セッションが開始した日時。
- **[Access Time]** - BMC がセッションで最後にアクティブになった日時。
- **[Expires]** - セッションが自動的に終了する日時。
- **[Source]** - セッションソース（リモートコンソール、Web インターフェース、ROM ベースのセットアップユーティリティ、iLO RESTful API、または SSH など）。
- **[権限アイコン]**（Current Session のみ） - 現在のユーザーアカウントに割り当てられている特権。

iLO イベントログ（IEL）

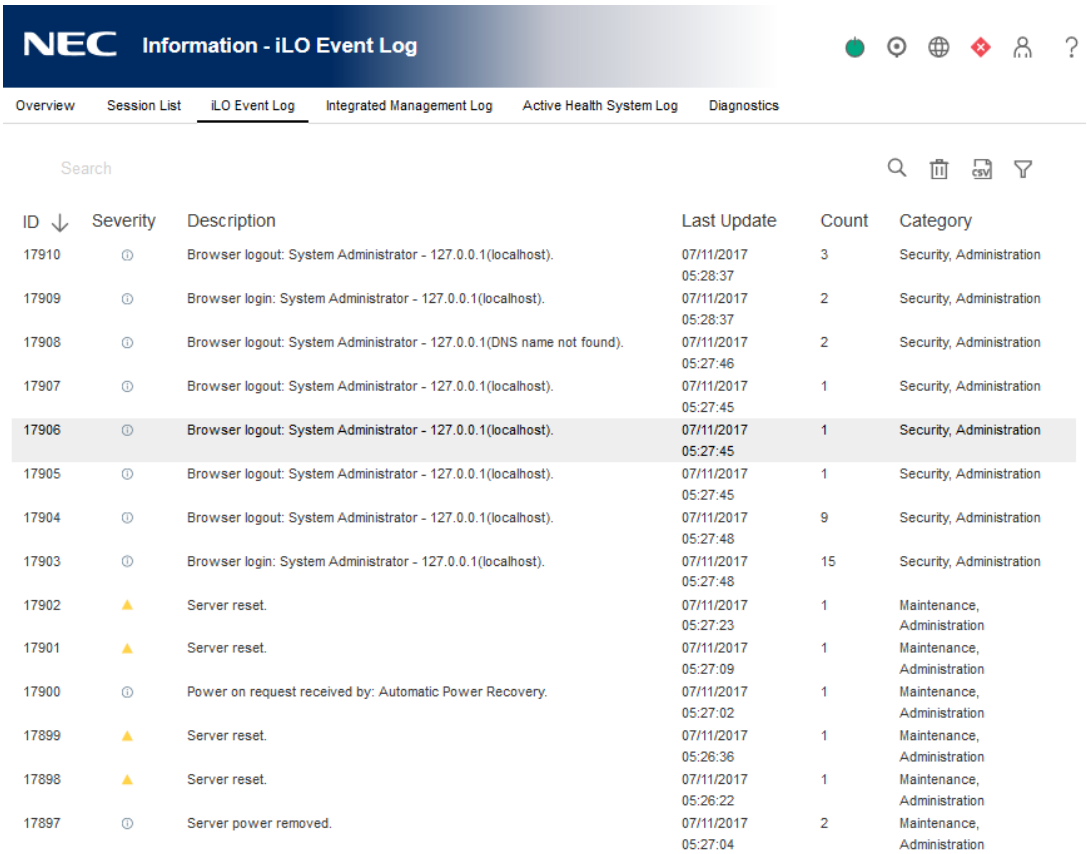
iLO イベントログは、iLO が記録した重要なイベントが表示されます。

記録されるイベントには、サーバーの電源障害やサーバーリセットのような主要なサーバーイベントと不正なログイン試行のような iLO イベントが含まれます。また、他にブラウザーおよびリモートコンソールへのログイン成功や失敗、仮想電源および電源の再投入イベント、ログのクリア、ならびにユーザーの作成や削除のような設定変更も含まれます。

iLO により、パスワードの安全な暗号化、すべてのログインのトラッキング、およびログインに失敗したときのすべての記録の管理が可能となります。**[Authentication Failure Logging]**設定により、認証失敗のログ記録条件を設定できます。イベントログは、DHCP 環境での監査機能を向上させるために記録したエントリーごとにクライアント名を取得し、アカウント名、コンピューター名、および IP アドレスを記録します。認証失敗ログの構成については、「iLO アクセスの設定」を参照してください。

iLO イベントログの表示

1. **[Information]→[iLO Event Log]**ページに移動します。
2. オプション：イベントログフィルターを使用してログの表示をカスタマイズします。
3. オプション：イベント詳細ペインを表示するには、イベントをクリックします。



ID	Severity	Description	Last Update	Count	Category
17910	ⓘ	Browser logout: System Administrator - 127.0.0.1(localhost).	07/11/2017 05:28:37	3	Security, Administration
17909	ⓘ	Browser login: System Administrator - 127.0.0.1(localhost).	07/11/2017 05:28:37	2	Security, Administration
17908	ⓘ	Browser logout: System Administrator - 127.0.0.1(DNS name not found).	07/11/2017 05:27:46	2	Security, Administration
17907	ⓘ	Browser logout: System Administrator - 127.0.0.1(localhost).	07/11/2017 05:27:45	1	Security, Administration
17906	ⓘ	Browser logout: System Administrator - 127.0.0.1(localhost).	07/11/2017 05:27:45	1	Security, Administration
17905	ⓘ	Browser logout: System Administrator - 127.0.0.1(localhost).	07/11/2017 05:27:45	1	Security, Administration
17904	ⓘ	Browser logout: System Administrator - 127.0.0.1(localhost).	07/11/2017 05:27:48	9	Security, Administration
17903	ⓘ	Browser login: System Administrator - 127.0.0.1(localhost).	07/11/2017 05:27:48	15	Security, Administration
17902	▲	Server reset.	07/11/2017 05:27:23	1	Maintenance, Administration
17901	▲	Server reset.	07/11/2017 05:27:09	1	Maintenance, Administration
17900	ⓘ	Power on request received by: Automatic Power Recovery.	07/11/2017 05:27:02	1	Maintenance, Administration
17899	▲	Server reset.	07/11/2017 05:26:36	1	Maintenance, Administration
17898	▲	Server reset.	07/11/2017 05:26:22	1	Maintenance, Administration
17897	ⓘ	Server power removed.	07/11/2017 05:27:04	2	Maintenance, Administration

iLO イベントログの詳細

- **[ID]** - イベントの ID 番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、イベントログは ID でソートされ、最新のイベントが先頭になります。

- **[Severity]** - 検出されたイベントの重要度。

- **[Description]** - この説明によって、記録されるイベントのコンポーネントと詳細な特性が特定されます。

  iLO ファームウェアが前のバージョンにロールバックされると、より新しいファームウェアによって記録されたイベントについて、「不明なイベントタイプ」という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアに更新するか、イベントログをクリアすることによって解決できます。
- **[Last Update]** - このタイプの最新のイベントの発生日時。この値は、iLO ファームウェアによって保存される日時に基づいています。

  イベントが更新された日時を iLO ファームウェアが認識しなかった場合は、[NOT SET]と表示されます。
- **[Count]** - このイベントが発生した回数（サポートされている場合）。

  通常、重要なイベントは発生するたびにイベントログエントリーを生成します。これらのイベントが 1 つイベントログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは 1 つのイベントログエントリーにまとめられ、**[Count]**および**[Last Update]**値が更新されます。各イベントタイプは特定の間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。
- **[Category]** - このイベントのカテゴリー。

iLO イベントログのアイコン

iLO は、以下のアイコンを使用してイベント深刻度を示します。

- **[Critical]** - イベントはサービスの停止（またはサービスの停止が予期されること）レベルであることを示しています。すぐに対処する必要があります。
- **[Caution]** - イベントは重要レベルであることを示していますが、性能の低下を示してはいません。
- **[Informational]** - イベントは情報レベルであることを示しています。
- **[Unknown]** - イベント深刻度を判断できませんでした。

iLO イベントログペインの詳細

- **[Initial Update]** -このタイプの最初のイベントの発生日時。この値は、iLO ファームウェアによって保存される日時に基づいています。イベントが最初に発生した日時を iLO ファームウェアが認識しなかった場合は、[NOT SET] と表示されます。
- **[Event Class]** - イベントクラスのユニークな識別子で、16 進数で表示します。
- **[Event Code]** -イベントのユニークな識別子で、16 進数で表示します。
- **[Recommended Action]** - 障害の推奨アクションの簡単な説明。

iLO イベントログビューのカスタマイズ

イベントのソート

列の見出し文字（**ID**、**Severity**、**Description**、**Last Update**、**Count** および **Category**）をクリックすると、その列でイベントログがソートされます。
表示の昇順または降順に変更するには、見出し文字を再度クリックします。

イベントのフィルター

イベントログのフィルタリングするために、  をクリックします。

- 重要度でフィルタリングするには、**[Severity]**メニューから重要度を選択します。
- イベントカテゴリでフィルタリングするには、**[Category]**メニューでカテゴリーを選択します。

- イベントの表示日時を変更するには、**[Time]**メニューで値を選択します。 次の中から選択してください：
  - **[Show Default]** - UTC 時刻で表示します。
  - **[Show Local Time]** - iLO Web インターフェースに接続しているクライアント時刻で表示します。
  - **[Show ISO Time]** - UTC 時刻を ISO 8601 フォーマットで表示します。

  iLO 5 Firmware Version 1.10 Jun 07 2017 では、SNTP 設定を行わない場合やタイムサーバーと時刻同期できる環境で利用されない場合には、以下に示す時刻が表示されます。

  - **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）
  - **[Show Local Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）に、さらに iLO へ接続したクライアントの環境のタイムゾーンを加味した時刻

  iLO 5 Firmware Version 1.15 Aug 17 2017、および Version 1.20 Feb 02 2018 では、以下に示す時刻が表示されます。

  - **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）
  - **[Show Local Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）に、さらに iLO へ接続したクライアントの環境のタイムゾーンを加味した時刻

  iLO 5 Firmware Version 1.30 May 31 2018 以降では、以下に示す時刻が表示されます。

  - **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
    - UTC 時刻
  - **[Show Local Time]**を選択時に以下を表示。
    - ローカル時刻

- 最後の更新日でフィルタリングするには、**[Last Update]**メニューで値を選択します。

  注記:**[Show Default]**で表示される時刻に基づいてフィルターが掛かります。

- フィルターをデフォルト値に戻すには、**[Reset filter]**をクリックします。

イベントの検索

日付、イベント ID、または説明テキストに基づいてイベントを検索するには、🔍をクリックし、検索ボックスにテキストを入力します。

CSV ファイルへの iLO イベントログの保存

イベントログを CSV ファイルにエクスポートします。

1. **[Information]**→**[iLO Event Log]**ページに移動します。
2. CSV アイコンをクリックします。

3. **CSV Output** ウィンドウで、**[Save]**をクリックしてから、ブラウザーのプロンプトに従ってファイルを保存または開きます。

iLO イベントログのクリア

iLO 設定権限を持つユーザーは、イベントログに記録されているすべての情報をクリアできます。

1. **[Information]**→**[iLO Event Log]**ページに移動します。
2. 🗑をクリックします。
3. 要求を確認するメッセージが表示されたら、**[OK]**をクリックします。

   以前に記録されたすべてのログはクリアされ、以下のイベントが記録されます。

   Event log cleared by: <ユーザー名>.

インテグレーテッドマネージメントログ（IML）

IML は、サーバーで発生したイベントの記録です。イベントは、システム ROM や AMS などのサービスによって生成します。ログに記録されるイベントには、オペレーティングシステム情報や ROM ベースの POST コードなど、システム ROM や AMS で記録されたすべてのサーバー固有のイベントがあります。
IML のエントリーが問題の診断や発生する可能性がある問題の特定に役立つ可能性があります。サービスの中断を防止するための予防的処置にも役立つ場合があります。

iLO が IML を管理するので、サーバーが稼動していない状態でもブラウザーを使用して IML を参照でき、リモートホストサーバーの問題のトラブルシューティングに役立てることができます。

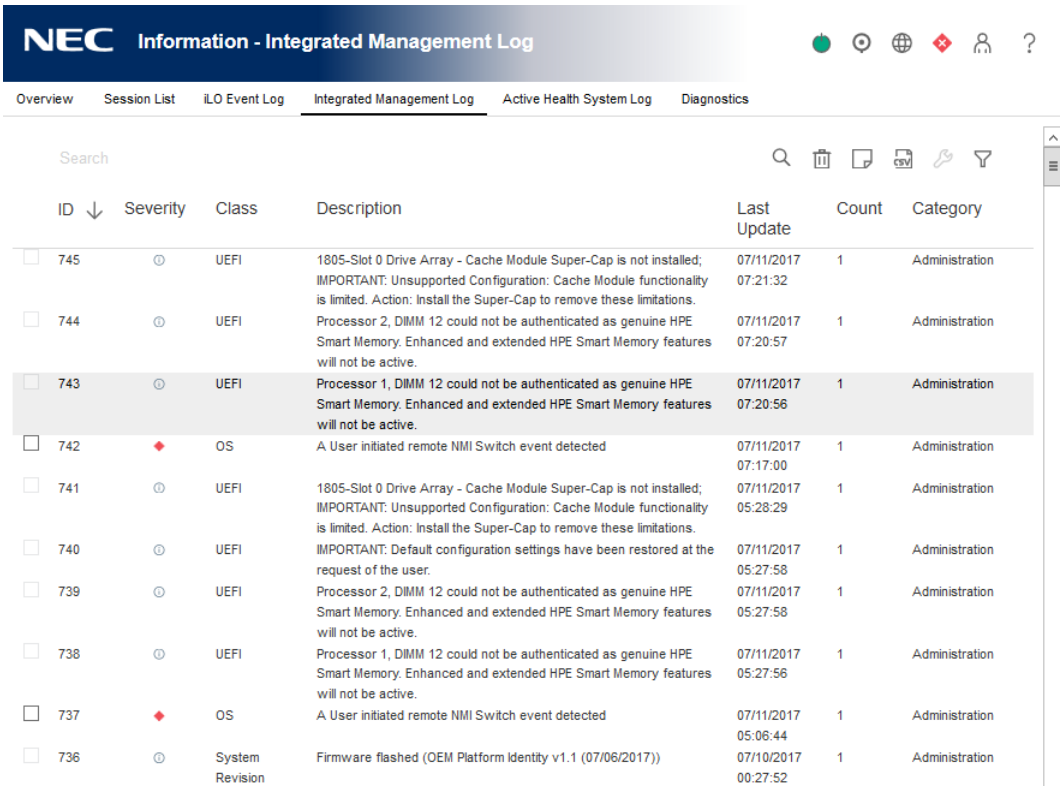
IML に記録される情報の種類の例は、次のとおりです。

- Fan inserted（ファンが取り付けられた）
- Fan removed（ファンが取り外された）
- Fan failure（ファンが故障した）
- Fan degraded（ファンの機能が低下した）
- Fan repaired（ファンが修復した）
- Fan redundancy lost（ファンの冗長性が失われた）
- Fans redundant（ファンが冗長化した）
- Power supply inserted（電源が取り付けられた）
- Power supply removed（電源が取り外された）
- Power supply failure（電源が故障した）
- Power supplies redundancy lost（電源の冗長性が失われた）
- Power supplies redundant（電源が冗長化した）
- Temperature over threshold（温度は異常）
- Temperature normal（温度は正常）
- Automatic shutdown started（自動シャットダウンが開始した）
- Automatic shutdown cancelled（自動シャットダウンが取り消された）
- Drive failure（ドライブ障害）

IML が一杯になると、新しいイベントごとにログ内の一番古いイベントが上書きされます。

IML の表示

1. **[Information]→[Integrated Management Log]**ページに移動します。
2. オプション：イベントログフィルターを使用してログの表示をカスタマイズします。
3. オプション：イベント詳細ペインを表示するには、イベントをクリックします。



ID	Severity	Class	Description	Last Update	Count	Category
745		UEFI	1805-Slot 0 Drive Array - Cache Module Super-Cap is not installed; IMPORTANT: Unsupported Configuration: Cache Module functionality is limited. Action: Install the Super-Cap to remove these limitations.	07/11/2017 07:21:32	1	Administration
744		UEFI	Processor 2, DIMM 12 could not be authenticated as genuine HPE Smart Memory. Enhanced and extended HPE Smart Memory features will not be active.	07/11/2017 07:20:57	1	Administration
743		UEFI	Processor 1, DIMM 12 could not be authenticated as genuine HPE Smart Memory. Enhanced and extended HPE Smart Memory features will not be active.	07/11/2017 07:20:56	1	Administration
742		OS	A User initiated remote NMI Switch event detected	07/11/2017 07:17:00	1	Administration
741		UEFI	1805-Slot 0 Drive Array - Cache Module Super-Cap is not installed; IMPORTANT: Unsupported Configuration: Cache Module functionality is limited. Action: Install the Super-Cap to remove these limitations.	07/11/2017 05:28:29	1	Administration
740		UEFI	IMPORTANT: Default configuration settings have been restored at the request of the user.	07/11/2017 05:27:58	1	Administration
739		UEFI	Processor 2, DIMM 12 could not be authenticated as genuine HPE Smart Memory. Enhanced and extended HPE Smart Memory features will not be active.	07/11/2017 05:27:58	1	Administration
738		UEFI	Processor 1, DIMM 12 could not be authenticated as genuine HPE Smart Memory. Enhanced and extended HPE Smart Memory features will not be active.	07/11/2017 05:27:56	1	Administration
737		OS	A User initiated remote NMI Switch event detected	07/11/2017 05:06:44	1	Administration
736		System Revision	Firmware flashed (OEM Platform Identity v1.1 (07/06/2017))	07/10/2017 00:27:52	1	Administration

IML の詳細

- Web インターフェースの左側の最初の列には、ステータスが**クリティカル**または警告の各イベントの隣にチェックボックスが表示されます。このチェックボックスを使用して、修復済みとしてマークするイベントを選択します。

  修復済みとしてマークする方法について詳しくは、「IML エントリーの修正済みへの変更」を参照してください。

- **[ID]** - イベントの ID 番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、IML は ID でソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。

- **[Severity]** - 検出されたイベントの重要度。

- **[Class]** - ネットワーク、保守、またはシステムのリビジョンなど、発生したイベントの種類を特定します。

- **[Description]** - この説明によって、記録されるイベントのコンポーネントと詳細な特性が特定されます。

  iLO ファームウェアがロールバックされると、より新しいファームウェアによって記録されたイベントについて、「不明なイベントタイプ」という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアに更新するか、ログをクリアすることによって解決できます。

  選択したイベントのトラブルシューティング情報にアクセスするには、**[Description]**列のリンクをクリックします。

- **[Last Update]** - このタイプの最新のイベントの発生日時。この値は、iLO ファームウェアによって保存される日時に基づいています。

イベントが更新された日時を iLO が認識しなかった場合は、[NOT SET]と表示されます。

- **[Count]** - このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントが発生するたびに IML エントリーを生成します。これらのイベントが 1 つイベントログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは 1 つの IML エントリーにまとめられ、**[Count]**および**[Last Update]**値が更新されます。各イベントタイプは特定の間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。

- **[Category]** - イベントのカテゴリ。例：ハードウェア、ファームウェア、管理

IML アイコン

iLO は、以下のアイコンを使用して IML イベント深刻度を示します。

- **[Critical]** - イベントはサービスの停止（またはサービスの停止が予期されること）レベルであることを示しています。すぐに対処する必要があります。
- **[Caution]** - イベントは重要レベルであることを示していますすが、性能の低下を示してはいません。
- **[Informational]** - イベントは情報レベルであることを示しています。
- **[Repaired]** - イベントは修正アクションを行いました。
- **[Unknown]** - イベント深刻度を判断できませんでした。

IML イベントペインの詳細

- **[Initial Update]** -このタイプの最初のイベントの発生日時。この値は、iLO ファームウェアによって保存される日時に基づいています。イベントが最初に発生した日時を iLO ファームウェアが認識しなかった場合は、[NOT SET]と表示されます。
- **[Event Class]** - イベントクラスのユニークな識別子で、16 進数で表示します。
- **[Event Code]** -イベントのユニークな識別子で、16 進数で表示します。
- **[Recommended Action]** - 障害の推奨アクションの簡単な説明。

IML ビューのカスタマイズ

イベントのソート

列の見出し文字（**ID**、**Severity**、**Class**、**Description**、**Last Update**、**Count** および **Category**）をクリックすると、その列でイベントログがソートされます。
表示の昇順または降順に変更するには、見出し文字を再度クリックします。

イベントのフィルター

イベントログのフィルタリングするために、をクリックします。

- 重要度でフィルタリングするには、**[Severity]**メニューから重要度を選択します。
- イベントクラスでフィルタリングするには、**[Class]**メニューでクラスを選択します。
- イベントカテゴリでフィルタリングするには、**[Category]**メニューでカテゴリーを選択します。

- イベントの表示日時を変更するには、**[Time]**メニューで値を選択します。 次の中から選択してください：
  - [Show Default] - UTC 時刻で表示します。
  - [Show Local Time] - iLO Web インターフェースに接続しているクライアント時刻で表示します。
  - [Show ISO Time] - UTC 時刻を ISO 8601 フォーマットで表示します。

  iLO 5 Firmware Version 1.10 Jun 07 2017 では、SNTP 設定を行わない場合やタイムサーバーと時刻同期できる環境で利用されない場合には、以下に示す時刻が表示されます。

  - **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）
  - **[Show Local Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）に、さらに iLO へ接続したクライアントの環境のタイムゾーンを加味した時刻

  iLO 5 Firmware Version 1.15 Aug 17 2017、および Version 1.20 Feb 02 2018 では、iLO がタイムサーバーと時刻同期しておらず、かつ BIOS/プラットフォーム構成(RBSU)で[Time Format]に[Local Time]を設定している場合に、以下に示す時刻が表示されます。

  - **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）
  - **[Show Local Time]**を選択時に以下を表示。
    - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）に、さらに iLO へ接続したクライアントの環境のタイムゾーンを加味した時刻

  iLO 5 Firmware Version 1.30 May 31 2018 以降では、以下に示す時刻が表示されます。

  - **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
    - UTC 時刻
  - **[Show Local Time]**を選択時に以下を表示。
    - ローカル時刻
- 最後の更新日でフィルタリングするには、**[Last Update]**メニューで値を選択します。

  注記:**[Show Default]**で表示される時刻に基づいてフィルターが掛かります。
- フィルターをデフォルト値に戻すには、**[Reset filter]**をクリックします。

イベントの検索

日付、イベント ID、または説明テキストに基づいてイベントを検索するには、🔍をクリックし、検索ボックスにテキストを入力します。

IML エントリーの修正済みへの変更

IML エントリーのステータスを**[Critical]**または**[Caution]**から**[Repaired]**に変更するには、この機能を使用します。

前提条件
iLO の設定を構成権限

手順

1. 問題を調べて修正します。
2. **[Information]**→**[Integrated Management Log]**ページに移動します。
3. ログエントリーを選択します。

   IML エントリーを選択するには、IML テーブルの最初の列のエントリーの横のチェックボックスをクリックします。IML エントリーの横にあるチェックボックスが表示されない場合、エントリーを修復済みとしてマークことはできません。

4. をクリックします。

iLO Web インターフェースが更新され、選択したログエントリーのステータスが**[Repaired]**に変化します。

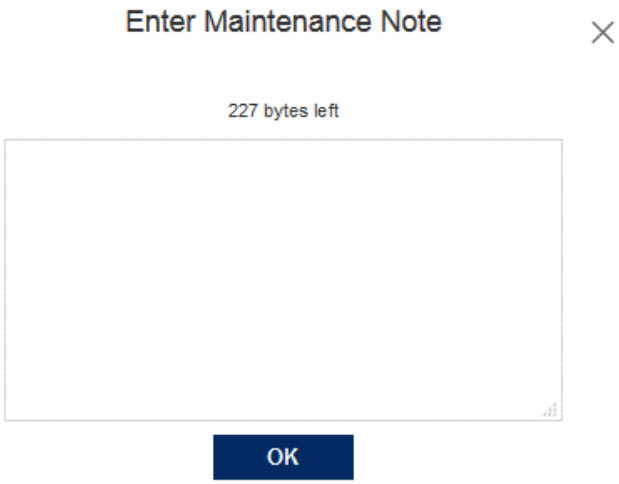
IML にメンテナンスノートを追加する

コンポーネントのアップグレード、システムのバックアップ、定期的なシステムのメンテナンス、またはソフトウェアのインストールのようなメンテナンス作業に関する情報を記録するログエントリーを作成するには、メンテナンスノート機能を使用します。

前提条件
iLO の設定を構成権限

手順

1. **[Information]**→**[Integrated Management Log]**ページに移動します。
2. をクリックします。メンテナンスノートを入力ウィンドウが開きます。



3. ログエントリーとして追加するテキストを入力し、**[OK]** をクリックします。

   入力できるテキストの最大長さは 227 バイトです。テキストを入力せずにメンテナンスノートを送信することはできません。

   Maintenance クラスの **Informational** ログエントリーが IML に追加されます。

CSV ファイルへの IML の保存

IML を CSV ファイルにエクスポートします。

1. **[Information]→[Integrated Management Log]**ページに移動します。
2. をクリックします。

3. **CSV Output** ウィンドウで、**[Save]**をクリックしてから、ブラウザーのプロンプトに従ってファイルを保存または開きます。

IML のクリア

iLO 設定構成設定権限を持つユーザーは、IML に記録されているすべての情報をクリアできます。

1. **[Information]**→**[Integrated Management Log]**ページに移動します。
2. 🗑をクリックします。
3. 要求を確認するメッセージが表示されたら、**[OK]**をクリックします。

   以前に記録されたすべてのログはクリアされ、以下のイベントが記録されます。

   IML Cleared (iLO user: <ユーザー名>)

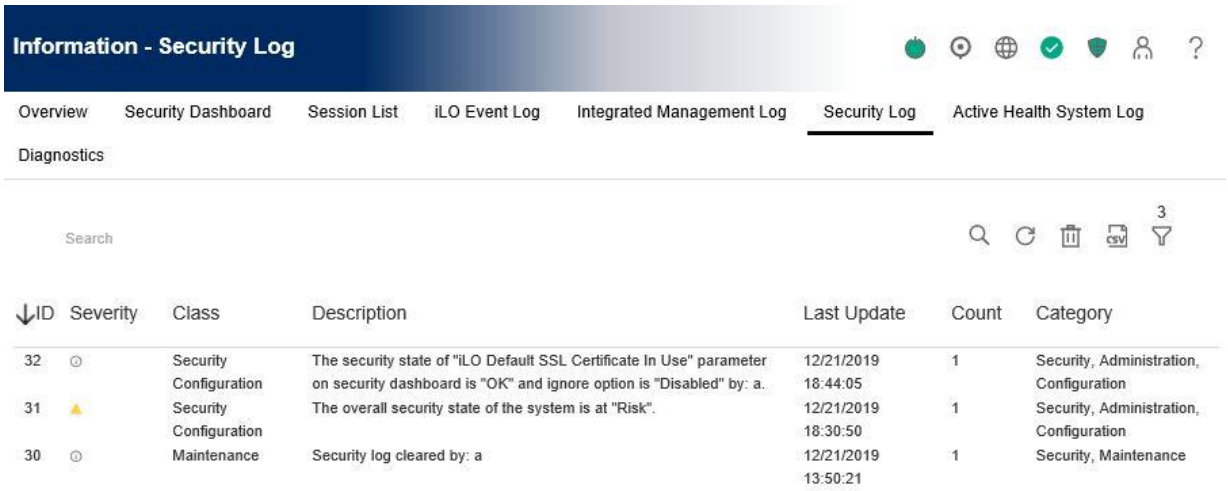
セキュリティログ[18]

セキュリティログは、iLO ファームウェアによって記録されたセキュリティイベントのレコードを提供します。

ログに記録されるイベントの例には、セキュリティ構成の変更や、セキュリティコンプライアンスの問題などがあります。ログに記録されるその他のイベントには、ハードウェアへの侵入、メンテナンス、サービス拒否攻撃などがあります。

セキュリティログは、記録されたすべてのセキュリティイベントの集中的なビューを提供します。いくつかの同じイベントは、iLO イベントログまたは IML にも含まれます。

セキュリティログがいっぱいになると、新しいイベントごとにログ内の一番古いイベントが上書きされます。



セキュリティログの表示

手順

1. **[Information]→[Security Log]**ページに移動します。
2. （オプション）ソート、検索、およびフィルター処理機能を使用して、ログのビューをカスタマイズします。
3. （オプション）イベントリストを更新するには、↻をクリックします。
4. （オプション）イベントをクリックして、イベントの詳細ペインを表示します。

セキュリティログビューのコントロール

イベントのソート

列でログテーブルをソートするには、列見出しをクリックします。

表示を昇順または降順に変更するには、列見出しをもう一度クリックするか、列の横にある矢印アイコンをクリックします。

18 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

イベントリストの更新

ログエントリーのリストを更新するには、をクリックします。

イベントの検索

日付、イベント ID、または説明テキストに基づいてイベントを検索するには、をクリックしてから、検索ボックスにテキストを入力します。

イベントフィルター

ログフィルターにアクセスするには、をクリックします。

- 深刻度でフィルタリングするには、**[Severity]**メニューで重大度レベルを選択します。
- クラスでフィルタリングするには、**[Class]**メニューでクラスを選択します。
- カテゴリでフィルタリングするには、**[Category]** メニューででカテゴリーを選択します。
- 表示されるイベントの日付と時刻を変更するには、**[Time]**メニューで値を選択します。以下から選択します。
  - **[Show Default]** - UTC 時刻で表示します。
  - **[Show Local Time]** - iLO Web インターフェースに接続しているクライアント時刻で表示します。
  - **[Show ISO Time]** - UTC 時刻を ISO 8601 フォーマットで表示します。
- 最終更新日付でフィルタリングするには、**[Last Update]**メニューで値を選択します。
- フィルターをデフォルト値に戻すには、**[Reset filter]**をクリックします。

セキュリティログの詳細

セキュリティログを表示すると、記録されたイベントの合計数がフィルターログアイコンの上に表示されます。

ログフィルターを適用すると、フィルター条件を満たすイベントの数がフィルターアイコンの下に表示されます。

イベントごとに、次の詳細が表示されます。

- **[ID]** - イベントの ID 番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、ログは ID でソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。

- **[Severity]** - 検出されたイベントの重要度。

- **[Class]** - UEFI、環境、またはシステムのリビジョンなど、発生したイベントの種類を特定します。

- **[Description]** - この説明によって、記録されるイベントのコンポーネントと詳細な特性が特定されます。

  iLO ファームウェアがロールバックされると、より新しいファームウェアによって記録されたイベントについて、「不明なイベントタイプ」という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアに更新するか、ログをクリアすることによって解決できます。

- **[Last Update]** - このタイプの最新のイベントの発生日時。この値は、iLO ファームウェアによって保存される日時に基づいています。

イベントが更新された日時をiLOが認識しなかった場合は、値がNOT SETと表示されます。

- **[Count]** - このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントは発生するたびにログエントリーを生成します。これらのイベントが1つのログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは 1 つのログエントリーにまとめられ、iLO によって回数および最終更新の値が更新されます。

  各イベントタイプは定義された間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。

- **[Category]** - イベントのカテゴリ。たとえば、セキュリティ、メンテナンス、または構成。

セキュリティログアイコン

- [Critical] - イベントはサービスの停止（またはサービスの停止が予期されること）レベルであることを示しています。すぐに対処する必要があります。
- [Caution] - イベントは重要レベルであることを示していますが、性能の低下を示してはいません。
- [Informational] - イベントは情報レベルであることを示しています。
- [Unknown] - イベント深刻度を判断できませんでした。

セキュリティログイベントペインの詳細

- **[Initial Update]** -このタイプの最初のイベントの発生日時。この値は、iLO ファームウェアによって保存される日時に基づいています。イベントが最初に発生した日時を iLO ファームウェアが認識しなかった場合は、**[NOT SET]**と表示されます。
- **[Event Class]** - イベントクラスのユニークな識別子で、16 進数で表示します。
- **[Event Code]** -イベントのユニークな識別子で、16 進数で表示します。
- **[Recommended Action]** - 障害状態に対する推奨アクションの簡単な説明。

CSV ファイルへのセキュリティログの保存

手順

1. **[Information]**→**[Security Log]**ページに移動します。
2. をクリックします。

3. **CSV Output** ウィンドウで、**[Save]**をクリックしてから、ブラウザーのプロンプトに従ってファイルを保存または開きます。

セキュリティログのクリア

前提条件

iLO の設定を構成権限

手順

1. **[Information]**→**[Security Log]**ページに移動します。
2. 🗑をクリックします。
3. 要求を確認するメッセージが表示されたら、**[OK]**をクリックします。
   以前に記録されたすべてのログはクリアされ、以下のイベントが記録されます。
   Security log Cleared by: <ユーザー名>

Active Health System

Active Health System は、サーバーハードウェアとシステム構成の変化を監視し、記録します。

Active Health System は以下の機能を提供します。

- 1,600 を超えるシステムパラメーターの継続的なヘルス監視
- すべての構成変更のロギング
- ヘルスおよびサービスの統合アラート（正確なタイムスタンプ付き）
- アプリケーションパフォーマンスに影響しないエージェントレス監視

Active Health System データの収集

Active Health System は、ユーザーの経営、財務、顧客、従業員、またはパートナーに関する情報を収集しません。

収集されるデータの例を示します。

- サーバーモデルおよびシリアル番号
- プロセッサーのモデルと速度
- ストレージの容量と速度
- メモリの容量と速度
- ファームウェア/BIOS およびドライバーのバージョンと設定

Active Health System は、サードパーティのエラーイベントログ活動（たとえば、オペレーティングシステムを介して作成し、渡した内容）からのオペレーティングシステムデータを解析したり、変更したりしません。

注記: iLO 5 Firmware Version 1.20 Feb 02 2018 以降では、ユーザー権限レベルが未設定のユーザーアカウントでは AHS ログのダウンロードができません。

Active Health System ログ

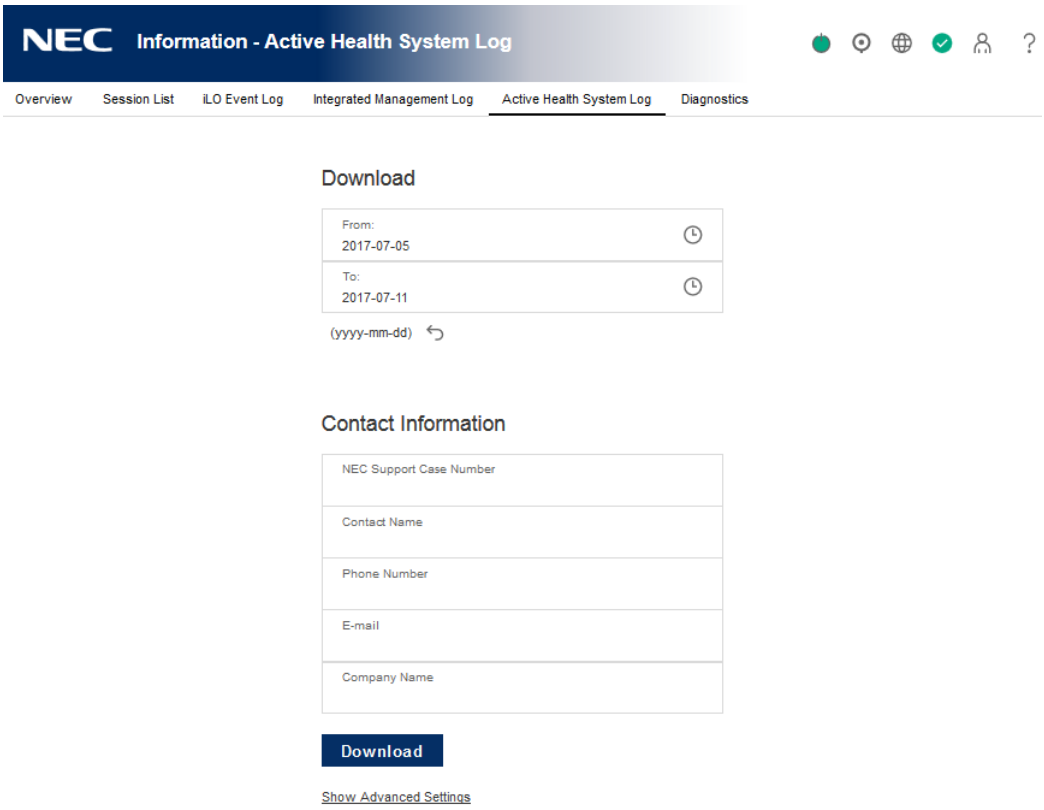
Active Health System が収集したデータは Active Health System ログに保存されます。データは安全に記録され、オペレーティングシステムから分離し、顧客データから切り離されます。
Active Health System ログがいっぱいになると、新しいデータはログ内の最も古いデータを上書きします。

Active Health System ログをダウンロードし、NEC に送信することで、お客様は、分析、技術的な解決、および品質改善のために NEC がデータを使用することに同意したものと見なされます。

日付範囲を指定した Active Health System ログのダウンロード

1. **[Information]→[Active Health System Log]**ページに移動します。

iLO サービスポートなど他の手段で Active Health System ログが使用されている場合、Active Health System ログにアクセスできません。



2. ログに含める日付の範囲を入力します。デフォルト値は 7 日です。
   a. **[From]**ボックスをクリックします。
      カレンダーが表示されます。
   b. カレンダーで範囲の開始日を選択します。
   c. **[To]**ボックスをクリックします。
      カレンダーが表示されます。
   d. カレンダーで範囲の終了日を選択します。
3. オプション：以下の情報は通常入力する必要はありません。保守員の指示があった場合に限り入力してください。
   - **[NEC Support Case Number]**
   - **[Contact Name]**
   - **[Phone Number]**
   - **[E-mail]**
   - **[Company Name]**

   この情報は、サーバーに保存されるログデータには記録されません。
4. **[Download]**をクリックします。
5. ファイルを保存します。

Active Health System ログ全体のダウンロード

Active Health System ログ全体のダウンロードには、かなり時間がかかる場合があります。技術的な問題のために Active Health System ログをアップロードする必要がある場合は、問題が発生した特定の日付範囲のログをダウンロードすることをおすすめします。

1. **[Information]→[Active Health System Log]**ページに移動します。

   iLO サービスポートなど他の手段で Active Health System ログが使用されている場合、Active Health System ログにアクセスできません。
2. **[Show Advanced Settings]**をクリックします。
3. オプション：以下の情報は通常入力する必要はありません。保守員の指示があった場合に限り入力してください。
   - **[NEC Support Case Number]**
   - **[Contact Name]**
   - **[Phone Number]**
   - **[E-mail]**
   - **[Company Name]**

   この情報は、サーバーに保存されるログデータには記録されません。
4. **[Download Entire Log]**をクリックします。
5. ファイルを保存します。

Active Health System ログのクリア

ログファイルが壊れた場合、またはログをクリアして再開する場合は、次の手順を使用して Active Health System ログを消去してください。

前提条件
iLO の設定を構成権限

手順**[Information]→[Active Health System Log]**ページに移動します。

iLO サービスポートなど他の手段で Active Health System ログが使用されている場合、Active Health System ログにアクセスできません。

1. **[Show Advanced Settings]**をクリックします。
2. **[Clear Log]**セクションまでスクロールしてから、**[Clear]**ボタンをクリックします。
3. 要求を確認するメッセージが表示されたら、**[OK]**をクリックします。

   ログがクリア中であることが iLO によって通知されます。
4. iLO をリセットします。

   一部の Active Health System データは iLO の起動中にしかログに記録されないので、Active Health System ログをクリアした後で iLO をリセットする必要があります。この手順を行うことにより、データー式が確実にログに記録されます。
5. サーバーを再起動します。

サーバーの起動時にオペレーティングシステムの名前とバージョンなど、一部の情報がログに記録されるため、Active Health System ログのクリア後にはサーバーの再起動が必要です。この手順を行うことにより、データー式が確実にログに記録されます。

詳細情報

iLO の再起動（リセット）

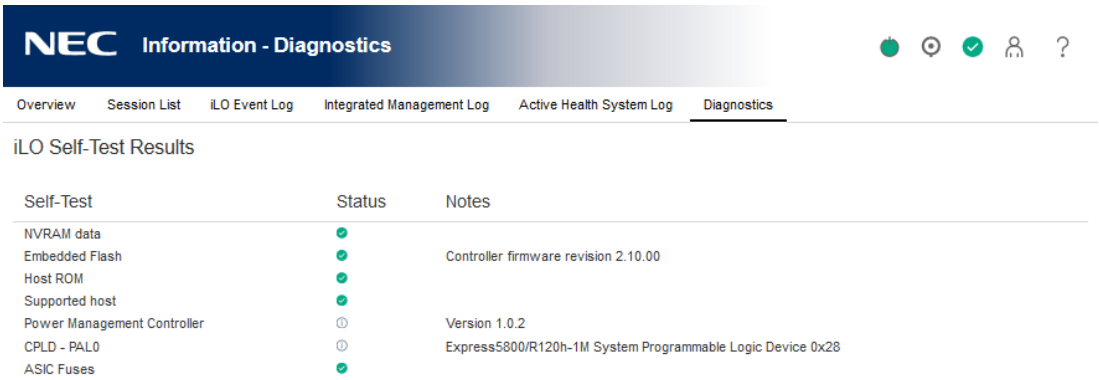
iLO 診断

診断ページには iLO セルフテストの結果が表示され、iLO のリセットおよびシステム NMI の生成を行うことができます。

iLO セルフテスト結果の表示

[iLO Self-Test Results]セクションには、iLO 診断テストの結果やテスト名、ステータス、ノートなどが表示されます。実行されるテストはシステムに依存します。すべてのテストがすべてのシステムで実行されるわけではありません。ご使用のシステムで実行されるテストを表示するには、診断ページのリストを参照してください。テストのステータスが報告されない場合、テストはリストされません。

[Information]→**[Diagnostics]**ページに移動します。



セルフテストの詳細

- **[Self-Test]** -テストされた機能。
- **[Status]** –テストの結果。
- **[Pass]** - テストは成功しました。
- **[Fail]** - テストで問題が検出されました。再起動、ファームウェアまたはソフトウェアの更新、またはサービスが必要な場合があります。
- **[Informational]** - テストされたシステムに関する補足データは、**[Notes]**の欄に記載されています。
- **[Note]** - 補足情報。いくつかのテストでは、この列には、マザーボード PAL や電源管理コントローラーなど、他のシステムプログラマブルロジックのバージョンが表示されます。

セルフテストのタイプ

- **[Cryptographic] -** セキュリティ機能をテストします。
- **[NVRAM data] -** 不揮発性の構成データ、ログ、および設定を保持するサブシステムをテストします。
- **[Embedded Flash] -** 設定、プロビジョニング、およびサービス情報を格納できるシステムの状態をテストします。
- **[Power Management Controller] -** 電力測定、電力上限、および電力管理に関連する機能をテストします。
- **[CPLD] -** サーバー内のプログラム可能なハードウェアをテストします。
- **[Host ROM] -** BIOS が管理プロセッサーと比較して古いかどうかを確認します。

- **[Supported host] -** 管理プロセッサファームウェアをチェックして、サーバーハードウェアの期限が切れているかどうかを判断します。
- **[EEPROM] -** 製造プロセス中に割り当てられた基本 iLO プロパティを格納するハードウェアをテストします。
- **[ASIC-Fuses] -** iLO チップに組み込まれていることが想定されるデータと既知のデータパターンとを比較して、チップが適切に製造され、動作設定が許容範囲を満たしていることを確認します。

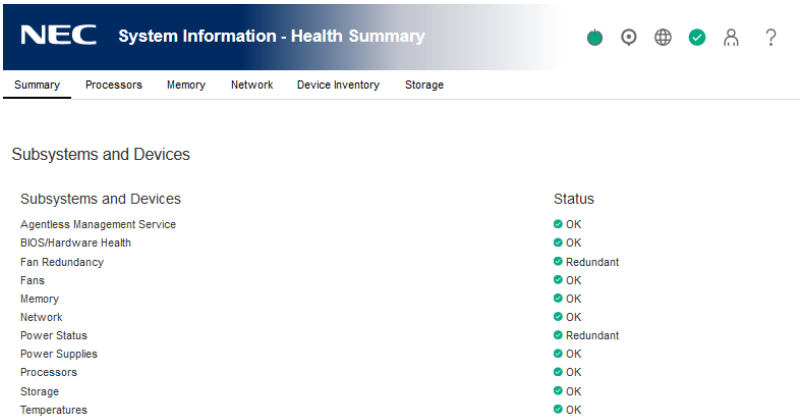
5. 装置システム情報の表示

ヘルスサマリー情報の表示

[System Information]ページに移動し、**[Summary]**タブをクリックします。

ヘルスサマリーのページには、監視対象サブシステムおよびデバイスのステータスが表示されます。このページの情報は、サーバー構成、AMS がインストールされているかどうかによって異なります。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、電源オフする前の状態です。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみ更新されます。



冗長ステータス

以下の項目に関する冗長ステータスが表示されます。

- **[Fan Redundancy]**
- **[Power Status]**

サブシステムおよびデバイスのステータス

以下の項目に関するステータス情報が表示されます。

- **[Agentless Management Service]**
- **[BIOS/Hardware Health]**
- **[Fans]**
- **[Memory]**
- **[Network]**
- **[Power Status]**
- **[Power Supplies]**
- **[Processors]**
- **[Storage]**
- **[Temperatures]**
- **[Smart Storage Battery Status]**（搭載サーバーのみ）

サブシステムおよびデバイスのステータスの値

ヘルスサマリーのページでは、次のステータスの値を使用します。

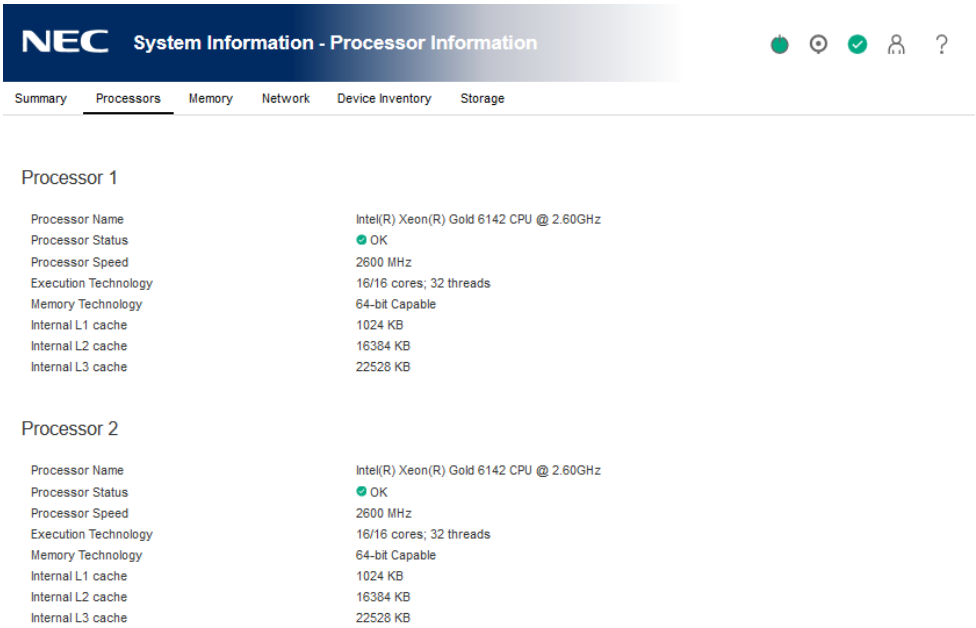
- **[Redundant]** - デバイスまたはサブシステム用のバックアップコンポーネントがあります。
- **[OK]**— デバイスまたはサブシステムは正常に動作しています。
- **[Not Redundant]** - デバイスまたはサブシステム用のバックアップコンポーネントがありません。
- **[Not Available]** - コンポーネントは利用できないか、インストールされていません。
- **[Degraded]** - デバイスまたはサブシステムの機能が低下しています。

  iLO 5 では、一致しないパワーサプライが取り付けられている場合、パワーサプライのステータスは**[Degraded]**となります。

  非冗長ファンまたは電源装置を備えたサーバーを起動する場合、システムヘルスステータスは**[OK]**と表示されます。ただし、システムの起動時に冗長ファンまたは電源装置で障害が発生すると、ファンまたは電源装置を交換するまでシステムヘルスステータスは**[Degraded]**と表示されます。
- **[Failed Redundant]** - デバイスまたはサブシステムは動作していません。
- **[Failed]** - デバイスまたはサブシステムの 1 つまたは複数のコンポーネントが動作していません。
- **[Other]** - 詳しくは、このステータスを報告するコンポーネントの**[System Information]**ページに移動してください。
- **[Link Down]** - ネットワークリンクはダウンしています。
- **[Unknown]** - iLO ファームウェアがデバイスのステータスに関するデータを受信していません。
  iLO をリセットしたときにサーバーの電源が切れていた場合、サーバーの電源が切れているとステータスを更新できないため、一部のサブシステムでは**[Unknown]**のステータスが表示されます。
- **[Not Installed]** - サブシステムまたはデバイスがインストールされていません

プロセッサー情報の表示

[System Information]ページに移動し、**[Processor]**タブをクリックします。



プロセッサー情報ページには、空いているプロセッサースロット、各スロットに取り付けられているプロセッサーの種類、プロセッサーサブシステムのサマリーが表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、電源オフする前の状態を示します。サーバーの電源が投入され、POST の実行が完了した場合にのみ、ヘルス情報が更新されます。

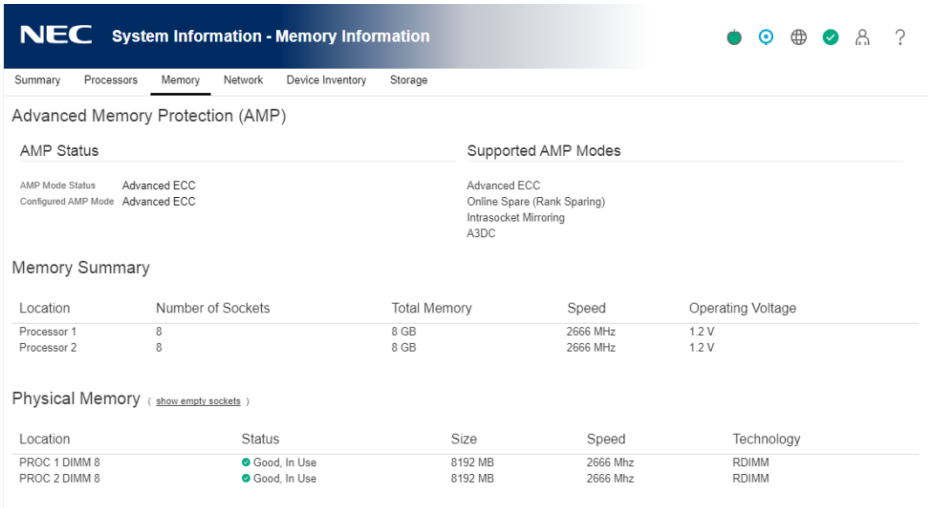
プロセッサー詳細

プロセッサーごとに、次の情報が表示されます。

- **[Processor Name]** - プロセッサーの名前。
- **[Processor Status]** - プロセッサーのヘルスステータス。
- **[Processor Speed]** - プロセッサーの速度。
- **[Execution Technology]** - プロセッサーのコアおよびスレッドに関する情報。
- **[Memory Technology]** - プロセッサーのメモリ機能。
- **[Internal L1 cache]** - L1 キャッシュサイズ。
- **[Internal L2 cache]** - L2 キャッシュサイズ。
- **[Internal L3 cache]** - L3 キャッシュサイズ。

メモリ情報の表示

1. **[System Information]**ページに移動し、**[Memory]**タブをクリックします。



2. オプション：デフォルトでは**[Memory Details]**テーブルでは空のメモリソケットは表示されません。空メモリソケットを表示するには、**[show empty sockets]**をクリックします。空メモリソケットが表示されている場合、それらを非表示にするには**[hide empty sockets]**をクリックします。

メモリ情報ページには、システムメモリの概要が表示されます。サーバーの電源が入っていない場合は、AMP データが使用できないため、POST 実行時に存在するメモリモジュールのみが表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、電源オフする前の状態を示します。サーバーの電源が投入され、POST の実行が完了した場合にのみ、ヘルス情報が更新されます。

アドバンストメモリプロテクション(AMP)の詳細

[AMP Status]セクションには、以下の情報が表示されます。

- **[AMP Mode Status]** - AMP サブシステムのステータスです。
  - **[Other/Unknown]** - システムが AMP をサポートしていない、またはマネージメントソフトウェアがステータスを判定できません。
  - **[Not Protected]** - システムは AMP をサポートしていますが、機能が無効になっています。
  - **[Protected]** - システムは AMP をサポートしています。機能は有効であり、保留になっていません。
  - **[Degraded]** - システムは保護されていましたが、AMP が保留中です。したがって、AMP は使用できません。
  - **[DIMM ECC]**（エラー訂正コード） - システムは、DIMM ECC のみによって保護されます。
  - **[Mirroring]** - システムはミラーモードの AMP で保護されています。DIMM の不具合は検出されていません。

- **[Degraded Mirroring]** - システムはミラーモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **[On-line Spare]** - システムはホットスペアモードの AMP で保護されています。DIMM の不具合は検出されていません。
- **[Degraded On-line Spare]** - システムはホットスペアモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **[RAID-XOR]** - システムは XOR メモリモードの AMP で保護されています。DIMM の不具合は検出されていません。
- **[Degraded RAID-XOR]** - システムは XOR メモリモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **[Advanced ECC]** - システムはアドバンスト ECC モードの AMP で保護されています。
- **[Degraded Advanced ECC]** - システムはアドバンスト ECC モードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **[LockStep]** - システムはロックステップモードの AMP で保護されています。
- **[Degraded LockStep]** - システムはロックステップモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **[A3DC]** - システムは、A3DC モードの AMP で保護されています。
- **[Degraded A3DC]** - システムは、A3DC モードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。

- **[Configured AMP Mode]** - 構成済みのアクティブな AMP モード。

  以下のモードがサポートされます。

  - **[None/Unknown]** - マネージメントソフトウェアが AMP フォールトトレランスを判定できない、またはシステムが AMP 用に構成されていません。
  - **[On-line Spare]** - 起動時にメモリの単一のスペアバンクが確保されています。多数の ECC エラーが発生すると、スペアメモリがアクティブになり、エラーが発生したメモリは無効になります。
  - **[Mirroring]** - システムはミラーメモリ用に構成されています。オンラインスペアメモリの場合の 1 つのメモリバンクとは異なり、ミラー化されたメモリではすべてのメモリバンクが二重化されています。多数の ECC エラーが発生すると、スペアメモリがアクティブになり、エラーが発生したメモリは無効になります。
  - **[RAID-XOR]** - システムは、XOR エンジンを使用して AMP 用に構成されています。
  - **[Advanced ECC]** - システムはアドバンスト ECC エンジンを使用して AMP 用に構成されています。
  - **[LockStep]** - システムは、ロックステップエンジンを使用して AMP 用に構成されています。
  - **[Online Spare (Rank Sparing)]** - システムは Online Spare Rank AMP 用に構成されています。

- **[Online Spare (Channel Sparing)]** - システムは Online Spare Channel AMP 用に構成されています。
- **[Intersocket Mirroring]** - システムは 2 つのプロセッサーまたはボードのメモリの間でミラー化された Intersocket AMP 用に構成されています。
- **[Intrasocket Mirroring]** - システムは 1 つのプロセッサーまたはボードのメモリの間でミラー化された Intrasocket AMP 用に構成されています。
- **[A3DC]** - システムは、A3DC エンジン用 AMP 用に構成されています。

[Supported AMP Modes]セクションには、サポートされる AMP モードが表示されます。
表示される可能性がある AMP モードは、以下のとおりです。

- **[RAID-XOR]** - システムは、XOR エンジンを使用して AMP 用に構成することができます。
- **[Dual Board Mirroring]** - システムは、デュアルメモリボード構成で、ミラー化されたアドバンストメモリ保護用に構成することができます。ミラーメモリは、同じメモリボード上のメモリまたは 2 番目のメモリボード上のメモリと交換することができます。
- **[Single Board Mirroring]** - システムは、単一のメモリボードで、ミラー化されたアドバンストメモリ保護用に構成することができます。
- **[Advanced ECC]** - システムは、アドバンスト ECC 用に構成することができます。
- **[Mirroring]** - システムは、ミラー化された AMP 用に構成することができます。
- **[On-line Spare]** - システムは、オンラインスペア AMP 用に構成することができます。
- **[LockStep]** - システムは、ロックステップ AMP 用に構成することができます。
- **[Online Spare (Rank Sparing)]** - システムは Online Spare Rank AMP 用に構成できます。
- **[Online Spare (Channel Sparing)]** - システムは Online Spare Channel AMP 用に構成できます。
- **[Intersocket Mirroring]** - システムは 2 つのプロセッサーまたはボードのメモリの間でミラー化された Intersocket AMP 用に構成できます。
- **[Intrasocket Mirroring]** - システムは 1 つのプロセッサーまたはボードのメモリの間でミラー化された Intrasocket AMP 用に構成できます。
- **[A3DC]** - システムは、A3DC AMP 用に構成することができます。
- **[None]** - このシステムは、AMP 用に構成することができません。

メモリサマリー

[Memory Summary]セクションには、本体装置に搭載され、POST 実行時に正常に動作したメモリの概要が表示されます。

- **[Location]** - メモリボード、カートリッジ、またはライザーが搭載されているスロットまたはプロセッサー。
  表示される可能性がある値は、以下のとおりです。

- **[System Board]** - 個別のメモリボードスロットはありません。すべての DIMM がマザーボードに取り付けられています。
- **[Board <Number>]** - 使用できるメモリボードスロットがあります。すべての DIMM がメモリボードに取り付けられています。
- **[Processor <Number>]** - メモリ DIMM が搭載されているプロセッサー。
- **[Riser <Number>]** - メモリ DIMM が搭載されているライザー。

- **[Number of Sockets]** - 現在のメモリモジュールソケット数。
- **[Total Memory]** - メモリの容量。これには、オペレーティングシステムが認識するメモリ、およびスペア、ミラー、または XOR 構成に使用されるメモリが含まれます
- **[Speed]** - メモリが動作する周波数。
- **[Voltage]** - メモリが動作する電圧。

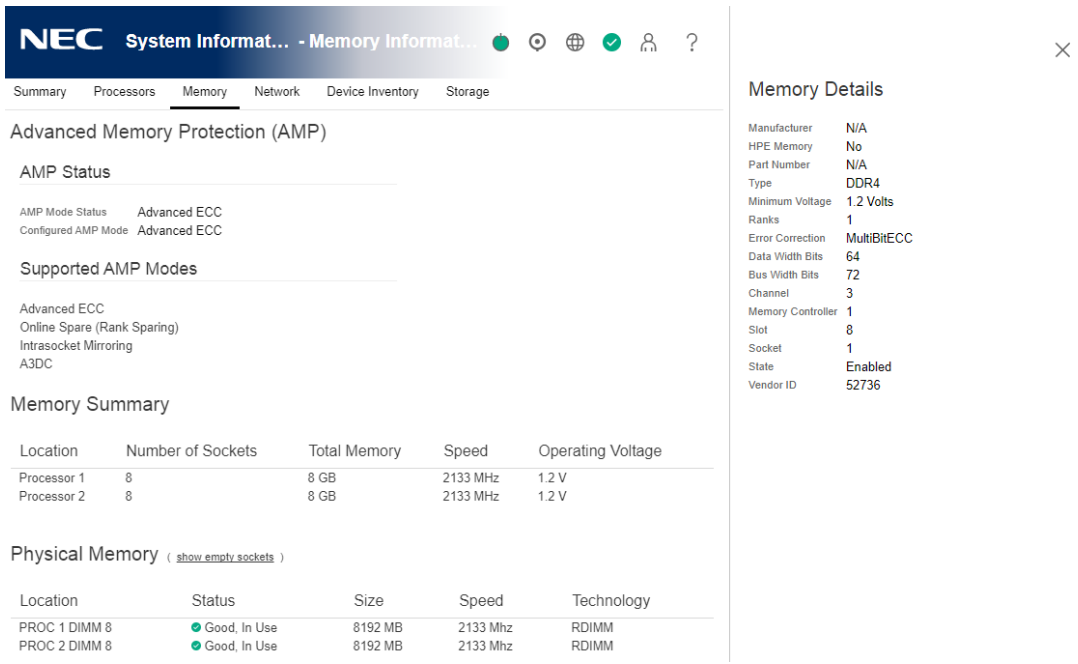
物理メモリ詳細

物理メモリセクションには、ホストに搭載され、POST 実行時に正常に動作していた、ホスト上の物理メモリモジュールが表示されます。メモリモジュールが取り付けられていない位置も示されます。各種の耐障害メモリ構成により、実際のメモリインベントリが、POST の実行時に検出されたものから変化する場合があります。システムに多数のメモリモジュールが搭載されている場合は、一部のモジュール位置しか表示されない場合があります。

- **[Location]** - メモリモジュールが搭載されているスロットまたはプロセッサー。
- **[Status]** - メモリモジュールのステータスおよびモジュールが使用中かどうか。表示される可能性がある値は、以下のとおりです。
  - **[Added But Unused]** - DIMM が追加されましたが、未使用です。
  - [Configuration Error] - DIMM に構成エラーがあります。
  - [Degraded] - DIMM ステータスが低下しています。
  - [Does] - DIMM タイプが一致していません。
  - [Expected but Missing] - DIMM が期待とおりに構成されていません。
  - [Good, In Use] - DIMM は正しく機能しており、使用中です。
  - [Good, Partially in Use] - DIMM は正しく機能しており、一部使用中です。
  - [Map Out Error] - トレーニングに失敗したため、DIMM は使用されていません。
  - [Map Out Configuration] - 構成エラーのため、DIMM は使用されていません。
  - [Not Present] - DIMM が存在しません。
  - [Not Supported] - DIMM はサポートされていません。
  - [Other] - DIMM ステータスは、標準のステータス定義のいずれにも当てはまりません。
  - [Present, Spare] - DIMM が存在し、スペアとして構成されています。
  - [Present, Unused] - DIMM が存在し、使用されていません。
  - [Unknown] - DIMM ステータスが不明です。
  - [Upgraded but Unused] - DIMM はアップグレードされましたが、使用されていません。
- **[Size]** - メモリモジュールのサイズ（MB）
- **[Speed]** - メモリモジュールの速度。
- **[Technology]** - メモリモジュールのテクノロジー。表示される可能性がある値は、以下のとおりです。

- **[Unknown]** - メモリのテクノロジーを判定できません。
- **[N/A]** - 存在しません。
- **[Synchronous]**
- **RDIMM**
- **UDIMM**
- **LRDIMM**
- **NVDIMM**
- **NVDIMM-N**
- **R-NVDIMM**
- **PMM**

メモリ詳細ペイン



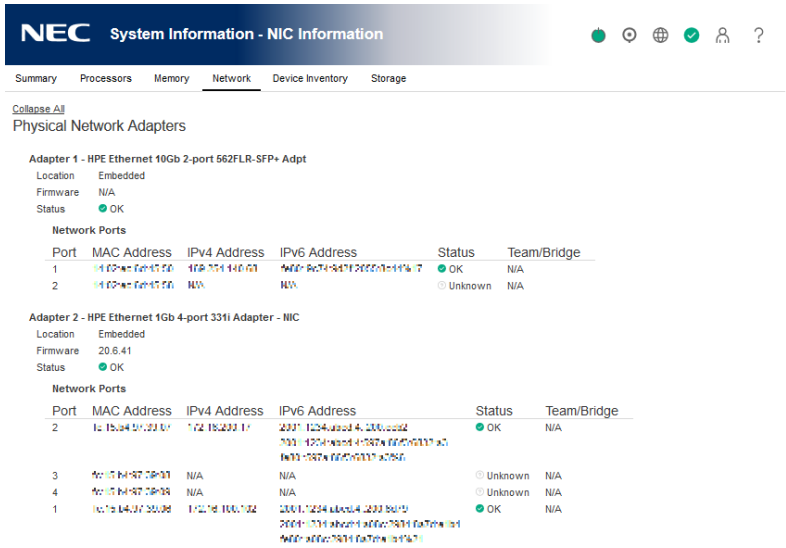
Physical Memory

- **[Manufacturer]** - メモリモジュールの製造元。
- **[Type]** - 搭載されたメモリのタイプ。表示される可能性がある値は、以下のとおりです。
  - **[Other]** - メモリのタイプを判定できません。
  - **[Board]** - メモリモジュールは（モジュール式でなく）システムボードまたはメモリ拡張ボードに固定されています。
  - **[DDR4]**
  - **[N/A]** - メモリモジュールはありません。
- **[Minimum Voltage]** - メモリモジュールが動作可能な最小電圧。
- **[Ranks]** - メモリモジュール内のランクの数。

- **[Error Correction]** - メモリモジュールが使用する誤り訂正のタイプ。
- **[Data Width Bits]** - メモリモジュールのデータ幅（ビット単位）。
- **[Bus Width Bits]** - メモリモジュールのバス幅（ビット単位）。
- **[Channel]** - メモリモジュールが接続されているチャネル番号。
- **[Memory Controller]** - メモリコントローラー番号。
- **[Memory Slot]** - メモリモジュールのスロット番号。
- **[CPU Socket]** - メモリモジュールのソケット番号。
- **[State]** - メモリの状態。
- **[Vendor ID]** - メモリベンダーID。
- **[Armed]** - NVDIMM-N の現在のバックアップ準備状態（使用できる場合）。
- **[Last Operation]** - 最後の操作のステータス。NVDIMM のみ。
- **[Media Life]** - メディアの残りの寿命の割合。NVDIMM のみ。

ネットワーク情報の表示

1. **[System Information]**ページに移動し、**[Network]**タブをクリックします。



2. オプション：このページで情報を展開するには**[Expand All]**をクリックし、情報を折りたたむには**[Collapse All]**をクリックします。

サーバーの電源が切れている場合、このページのヘルスステータス情報は、電源オフする前の状態です。サーバーの電源が投入され、POST の実行が完了した場合にのみ、ヘルス情報が更新されます。

このページのすべてのデータセットを表示するには、AMS がインストールされていて実行中であることが必要です。AMS がインストールされ、サーバー上で実行されている場合にのみ、サーバーの IP アドレス、アドインのネットワークアダプター、サーバーの NIC ステータスが表示されます。

物理ネットワークアダプター

このセクションには、サーバーの内蔵 NIC および追加された NIC に関する以下の情報が表示されます。

- **[Adapter number]** - アダプター番号（**Adapter 1**、**Adapter 2** など）の後にネットワークアダプターの名前が表示されます。
- **[Location]** - マザーボード上のアダプターの位置。
- **[Firmware]** - インストールされているアダプターのファームウェアのバージョン（該当する場合）。この値は、システム NIC（内蔵および直立型）の場合にのみ表示されます。
- **[Status]** - NIC ステータス。
  Windows サーバー：
  NIC がネットワークに接続されたことがない場合、iLO はステータスを[不明]と表示します。NIC がネットワークに接続されていたが現在は接続されていない場合、iLO はステータスを[リンクダウン]と表示します。
  Linux サーバー：

NetworkManager を使用して NIC を管理する場合、デフォルトのステータスは[アップ]であり、リンクステータスが iLO に表示されます。Linux のレガシーユーティリティを使用して NIC を管理する場合、iLO は、NIC が管理者によって設定されている場合にのみリンクステータスを表示します。NIC が設定されていない場合、iLO はステータスを[不明]と表示します。

VMware サーバー：

iLO が NIC ポートと通信できない場合、ステータスは[不明]と表示されます。NIC ドライバーが link_down のステータスを報告する場合、iLO はステータスを[ダウン]と表示します。NIC ドライバーが link_up のステータスを報告する場合、iLO はステータスを[アップ]と表示します。

- **[Port]** - 設定されているネットワークポート。この値は、システム NIC（内蔵および直立型）の場合にのみ表示されます。
- **[MAC Address]** - ポートの MAC アドレス。
- **[IPv4 Address]** - システム NIC（内蔵および直立型）の場合、サーバーの IP アドレス（使用できる場合）。
- **[IPv6 Address]** - システム NIC（内蔵および直立型）の場合、サーバーの IP アドレス（使用できる場合）。
- **[Status]** - ポートのステータス。
- **[Team/Bridge]** - ポートが NIC チーミング用に設定されている場合、論理ネットワークアダプターを形成する物理ポートの間で設定されているリンクの名前。この値は、システム NIC（内蔵および直立型）の場合にのみ表示されます。

ファイバーチャネルホストバスアダプターまたはコンバージドネットワークアダプターファイバーチャネルのホストバスアダプターまたはコンバージドネットワークアダプターに関する、次の情報が表示されます。

- **[Physical Port]** - 物理ネットワークのポート番号。
- **[WWNN]** - ポートのワールドワイドノード名。
- **[WWPN]** - ワールドワイドポート名。
- **[Status]** - ポートのステータス。

ブートの進行状況とブートターゲット

DCI 接続が使用可能な場合は、ブートの進行状況とブートターゲットに関する以下の情報が表示されます。

- **[Port]** - 設定済み仮想ポート番号。
- **[Boot Progress]** - ブートの現在のステータス。
- **[Boot Targets]**
  - [**WWPN**] - ワールドワイドポート名。
  - [**LUN ID**] - 論理ユニット番号 ID。

論理ネットワークアダプター

このセクションには、NIC チーミングを使用して 1 つの論理ネットワーク接続に 2 つ以上のポートを搭載しているネットワークアダプターに関する以下の情報が表示されます。

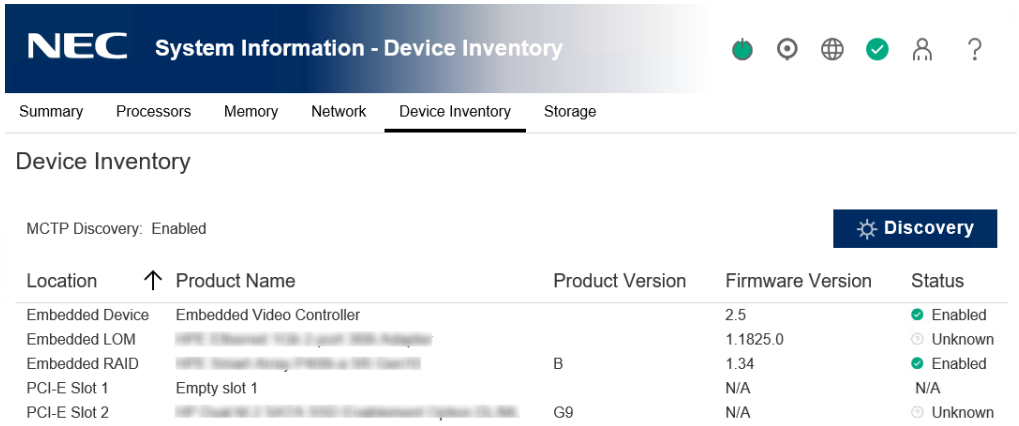
- **[Adapter number]** - アダプター番号（**Adapter 1**、**Adapter 2** など）の後に論理ネットワークアダプターを形成する物理ポートの間で設定されているリンクの名前が表示されます。
- **[MAC Address]** - 論理ネットワークアダプターの MAC アドレス。
- **[IP Address]** - 論理ネットワークアダプターの IP アドレス。
- **[Status]** - 論理ネットワークアダプターのステータス。

各論理ネットワークアダプターを形成するポートに関する、次の情報が表示されます。

- **[Members]** - 論理ネットワークアダプターを形成する各ポートに割り当てられた一連の番号。
- **[MAC Address]** - 物理アダプターポートの MAC アドレス。
- **[Status]** - 物理アダプターポートのステータス。

デバイスインベントリの表示

[System Information]ページに移動し、**[Device Inventory]**タブをクリックします。



デバイスインベントリページには、マザーボードに取り付けられたデバイスに関する情報が表示されます。このページに表示されるデバイスには、たとえば、取り付けられているアダプター、PCI デバイス、SATA コントローラー、Smart Storage バッテリーなどがあります。サーバーの電源が切れている場合、このページのヘルスステータス情報は、最後に電源が入っていた時点の情報になります。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみ更新されます。

AMS がインストールされ、サーバー上で実行されている場合にのみ、アドインネットワークアダプターのファームウェアバージョンとステータス、ネットワーク接続ストレージの詳細、および Smart Storage バッテリーのステータスが表示されます。

iLO ファームウェアがネットワークアダプターの製品名や製品番号をデバイスから直接取得できない場合、AMS からこの情報の収集を試みます。

重要: 画面右上の**[Discovery]**ボタンは使用しないでください。

デバイスインベントリの詳細

- **[Discovery]** - サーバーの MTCP 検出機能の有効・無効。本機能は使用しません。
- **[Location]** - デバイスの取り付け位置。
- **[Product Name]** - デバイスの製品名。
- **[Product Version]** - デバイスの製品バージョン。
- **[Firmware Version]** - インストールされているデバイスファームウェアバージョン。
- **[Status]** - デバイスのステータス。

デバイスステータスの値

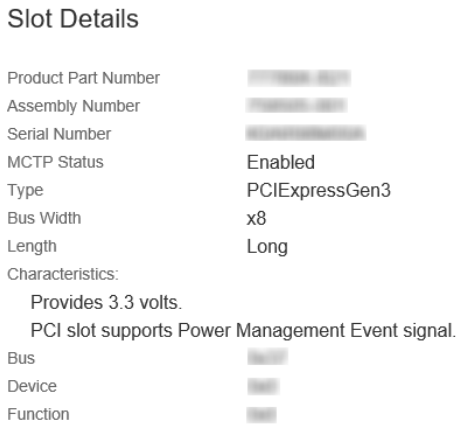
[Device Inventory]ページでは、次のステータスの値を使用します。

- **[OK]** - デバイスは正常に動作しています。
- **[Other]** - デバイスのステータスを判別できませんでした。

- **[No Supporting CPU]** - デバイスのスロットをサポートする CPU が取り付けられていません。
- **[Not Installed]** - デバイスが取り付けられていません。
- **[Link Down]** - ネットワークリンクはダウンしています。
- **[Failed]** - デバイスの 1 つまたは複数のコンポーネントが動作していません。
- **[Degraded]** - デバイスの機能が低下しています。
- **[Unknown]** - iLO ファームウェアがデバイスのステータスに関するデータを受信していません。

PCI スロットの詳細の表示

1. **[System Information]**ページに移動し、**[Device Inventory]**タブをクリックします。
2. 表示された PCI スロットをクリックします。

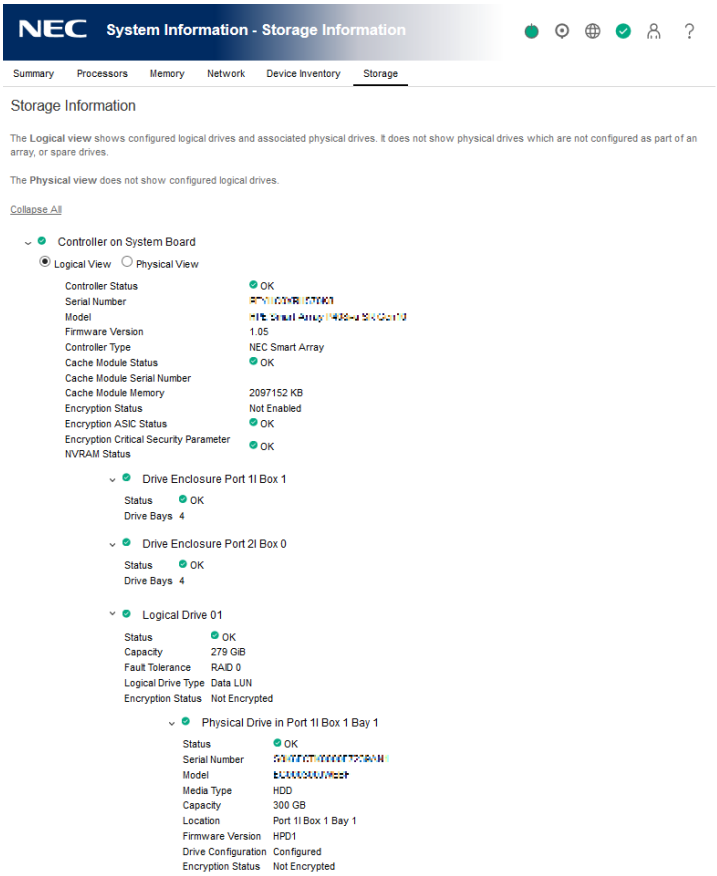


PCI スロット詳細ペイン

- **[Product Part Number]** - デバイスの製品番号。
- **[Assembly Number]** - デバイスのアセンブリー番号。
- **[Serial Number]** - デバイスのシリアル番号。
- **[MCTP Status]** - 使用しません。
- **[Type]** - PCI スロットのタイプ。
- **[Bus Width]** - PCI スロットのバス幅。
- **[Length]** - PCI スロットの長さ。
- **[Characteristics]** - PCI スロットに関する情報。たとえば、電圧やその他のサポートに関する情報です。
- **[Bus]** - BIOS によって割り当てられた PCI バス番号。
- **[Device]** - BIOS によって割り当てられた PCI デバイス番号。
- **[Function]** - BIOS によって割り当てられた PCI Function 番号。

ストレージ情報の表示

1. **[System Information]**ページに移動し、**[Storage]**タブをクリックします。



2. オプション：データを展開するには **[Expand All]**をクリックし、データを折りたたむには **[Collapse All]**をクリックします。
3. Smart アレイコントローラーのみ：表示するコントローラーに対して、次のオプションのいずれかを選択します。
   - **[Logical View]** - 設定されている論理ドライブと、関連付けられた物理ドライブを表示します。このビューには、アレイの一部またはスペアドライブとして構成されていない物理ドライブは表示されません。
   - **[Physical View]** - 物理ドライブを表示します。このビューには論理ドライブは表示されません。

サーバーの電源がオフの場合、このページのシステムの情報は、最後に電源が入っていた時点の情報になります。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみ更新されます。

このページのすべてのデータセットを表示するには、AMS がインストールされていて実行中であることが必要です。AMS がインストールされ、サーバー上で実行されている場合にのみ、SAS/SATA コントローラーの情報が表示されます。

このページに表示される情報は、ご使用のストレージ構成によって異なります。一部のストレージ構成では、各カテゴリーの情報は表示されません。

サポート対象のストレージコンポーネント

ストレージ情報ページには、以下のストレージコンポーネントに関する次の情報が表示されます。

- Smart アレイコントローラー、ドライブエンクロージャー、接続されている論理ドライブ、および論理ドライブを構成する物理ドライブ。
- 直接接続されたストレージを管理するNECおよび他社製のストレージコントローラー、および接続された物理ドライブ。
- M.2 SSD 対応キット
- 12G SAS エキスパンダー
- デュアル 8GB MicroSD EM USB キット(Windows のみ)
- NVMe ドライブ

このページには、最初に Smart アレイコントローラーが表示され、続いて他のストレージコントローラーが表示されます。

> △**注記:**
> デュアル 8GB MicroSD EM USB キットのスタータスの表示は、Windows 環境でのみサポートされます。Linux や VMware 環境では、「不明」と表示されます。

Smart アレイの詳細

iLO では、コントローラー、エンクロージャー、論理ドライブ、および物理ドライブの情報が表示されます。
iLO では、合計 256 の物理ドライブと合計 256 の論理ドライブを監視できます。

コントローラー

このセクションには、Smart アレイコントローラーごとに以下の詳細が表示されます。

- コントローラー位置 - スロット番号またはマザーボード
- 最上位のコントローラーステータス - 最上位のコントローラーステータス（コントローラーの場所の左側に表示される）は、コントローラーのハードウェアステータスと、キャッシュモジュール、エンクロージャー、物理ドライブ、論理ドライブ、およびそのコントローラーと関連付けられたスペアドライブのステータスとの組み合わせです。コントローラーハードウェアステータスが**[OK]**であり、関連付けられたいずれかのハードウェアに障害がある場合、最上位のコントローラーステータスは、障害の種類によって、**[Major]**、**[Warning]**、または**[Degraded]**に変化します。コントローラーハードウェアのステータスが**[Failed]**の場合、最上位のコントローラーステータスは**[Failed]**です。
- **[Controller Status]** - コントローラーハードウェアステータス（**[OK]**または**[Failed]**）
- **[Serial Number]** - シリアル番号
- **[Model]** - モデル
- **[Firmware Version]** - ファームウェアバージョン
- **[Controller Type]** - コントローラタイプ
- **[Cache Module Status]** - キャッシュモジュールのステータス

- **[Cache Module Serial Number]** - キャッシュモジュールのシリアル番号
- **[Cache Module Memory]** - キャッシュモジュールメモリ
- **[Encryption Status]** - コントローラーで暗号化が有効になっているかどうかを示します。

  表示される値は、以下のとおりです。
- **[Encryption ASIC Status]** - コントローラーの ASIC 暗号化自己診断が成功したか失敗したかどうかを示します。「失敗」ステータスは、コントローラーが暗号化されていないことを示します。
- **[Encryption Critical Security Parameter NVRAM Status]** - コントローラーが正常に重要なセキュリティパラメーターNVRAM を検出したかどうかを示します。「失敗」ステータスは、コントローラーが暗号化されていないことを意味します。

Smart Storage Administrator(SSA)を使用して、Smart アレイコントローラーの暗号化設定を設定できます。

ドライブエンクロージャー

このセクションには、Smart アレイコントローラーに接続されているドライブエンクロージャーに関する以下の情報が表示されます。

- **[Enclosure port and box numbers]** - エンクロージャーのポート番号とボックス番号
- **[Status]** - ステータス
- **[Drive Bays]** - ドライブベイの数
- **[Serial Number]** - シリアル番号
- **[Model]** - モデル
- **[Firmware Version]** - ファームウェアバージョン

一部のエンクロージャーでは表示されるプロパティの一部しかなく、一部のストレージ構成ではドライブエンクロージャーがありません。

論理ドライブ

[Logical View]オプションを選択すると、Smart アレイコントローラーに接続されている論理ドライブについて以下の情報が表示されます。

- **[Logical drive number]** - 論理ドライブ番号
- **[Status]** - ステータス
- **[Capacity]** - 容量
- **[Fault Tolerance]** - フォールトトレランス
- **[Logical Drive Type]** - 論理ドライブのタイプ
- **[Encryption Status]** - 暗号化ステータス

論理ドライブは、Smart Storage Administrator ソフトウェアで設定しないと、このページに表示されません。

物理ドライブ

このセクションで示される情報は、**[Logical View]**オプションと**[Physical View]**オプションのうちどちらが選択されているかによって異なります。論理ビューでは、アレイの一部として構成されている物理ドライブが表示されます。物理ビューでは、すべての物理ドライブが表示されます。

物理ドライブが**[Failed]**ステータスにある場合、このステータスは全体的なストレージのヘルスステータスには影響しません。ストレージのヘルスステータスに影響するのは、論理ドライブだけです。

Smart アレイコントローラーに接続されている物理ドライブについて、次の情報が一覧で表示されます。

- **[Physical drive port, box, and bay numbers]** - 物理ドライブのポート、ボックス、およびベイ番号。
- **[Status]** - ステータス
- **[Serial Number]** - シリアル番号
- **[Model]** - モデル
- **[Media Type]** - メディアタイプ
- **[Capacity]** - 容量
- **[Location]** - 位置
- **[Firmware Version]** - ファームウェアバージョン
- **[Drive Configuration]** - ドライブの構成
- **[Encryption Status]** - 暗号化ステータス

以下の項目は、サポートされている SSD ドライブが構成されている場合に表示されます。

- **[Power On Hours]** -ドライブの電源がオンになってる時間。
- **[Estimated Life Remaining Based on Workload to Date]** - 推定されたドライブの残り寿命。残り寿命が 100%のときは 100%の値が表示されます。残り寿命が 100%より少ないときは、推定値（日数）が表示されます。
- **[Life Remaining]** - 残っているドライブ寿命のパーセント値です。この値は、ドライブから読み取られたデータに基づきます。

ダイレクトアッタチストレージ(DAS)の詳細

iLO には以下の情報が表示されます。

- コントローラー
- 物理ドライブ

コントローラー

このセクションには、直接接続ストレージを管理する NEC および他社製のストレージコントローラーに関する以下の情報が表示されます。

- **[Controller location]** - 暗号化ステータスコントローラ位置
- **[Top-level controller status]** - 最上位のコントローラーステータス（コントローラーの場所の左側に表示される）は、コントローラーのハードウェアステータスと、エンクロージャー、物理ドライブ、およびそのコントローラーと関連付けられたスペアドライブのステータスとの組み合わせです。コントローラーハードウェアステータスが**[OK]**であり、関連付けられたいずれかのハードウェアに障害がある場合、最上位のコントローラーステータスは、障害の種類によって、**[Major]**、**[Warning]**、または**[Degraded]**に変化します。コントローラーハードウェアのステータスが**[Failed]**の場合、最上位のコントローラーステータスは**[Failed]**です。
- **[Controller Status]** - コントローラーハードウェアステータス（**[OK]**または**[Failed]**）
- **[Serial Number]** - シリアル番号
- **[Model]** - モデル
- **[Firmware Version]** - ファームウェアバージョン
- **[Controller Type]** - コントローラータイプ

物理ドライブ

このセクションでは、NEC および他社製のストレージコントローラーに接続された物理ドライブに関する情報が表示されます。

物理ドライブが**[Failed]**ステータスにある場合、このステータスは全体的なストレージのヘルスステータスには影響しません。ストレージのヘルスステータスに影響するのは、論理ドライブだけです。

- **[Physical drive location]** - 物理ドライブの位置
- **[Status]** - ステータス
- **[Serial Number]** - シリアル番号
- **[Model]** - モデル
- **[Media Type]** - メディアタイプ
- **[Capacity]** - 容量
- **[Location]** - 位置
- **[Firmware Version]** - ファームウェアバージョン
- **[Drive Configuration]** - ドライブの構成
- **[Encryption Status]** - 暗号化ステータス

以下の項目は、サポートされている SSD ドライブが構成されている場合に表示されます。

- **[Power On Hours]** -ドライブの電源がオンになってる時間。
- **[Estimated Life Remaining Based on Workload to Date]** - 推定されたドライブの残り寿命。残り寿命が 100%のときは 100%の値が表示されます。残り寿命が 100%より少ないときは、推定値（日数）が表示されます。
- **[Life Remaining]** - 残っているドライブ寿命のパーセント値です。この値は、ドライブから読み取られたデータに基づきます。

注意：実際のスマートアレイの FW バージョンが、**[System Information]-[Storage]ページ**で表示されるバージョンと異なって表示される場合がありますが、運用には影響ありません。

ドライブの電源管理

サポート対象ドライブを選択すると、物理ドライブ詳細ペインのドライブ電源ボタンセレクションに、現在のドライブの電源状態が表示されます。

表示される可能性のある値は、[ON]、[OFF]、および[Start]です。

[Drive Power Button]ボタンオプションを使用して、ドライブの電源をオンまたはオフにすることができます。

電源操作は、サポートされているドライブでのみ機能します。

前提条件

- iLO の設定を構成する権限
- 電源管理をサポートするドライブが構成されている

手順

1.ナビゲーションツリーで[System Information]をクリックし、[Storage]タブをクリックします。

2. ドライブを選択します。

   [Physical Drive Details]ペインが表示されます。

3. [Power On]または[Power Off]ボタンをクリックします。
4. 操作を確認するメッセージが表示されたら、[OK]をクリックします。

ドライブの電源ボタンオプション

- [Power On] - すぐにドライブの電源を入れます。
- [Power Off] - すぐにドライブの電源を切ります。このオプションを使用すると、強制的にシャットダウンされます。

6. ファームウェア、ソフトウェア、言語パックの管理

ファームウェアの更新

ファームウェアの更新では、新機能、改良、およびセキュリティ更新によりサーバーと iLO 機能が向上します。

以下の方法でファームウェアを更新することができます。

- **オンラインファームウェア更新** - オンライン方式を使用してファームウェアを更新する場合、サーバーオペレーティングシステムをシャットダウンせずに更新を実行できます。オンラインでのファームウェア更新は、インバンドまたはアウトバンドで実行できます。
- **インバンド** - ファームウェアは、サーバーのホストオペレーティングシステムから iLO に送信します。インバンドファームウェア更新には、iLO 5 チャネルインターフェースドライバーが必要です。ホストベースのユーティリティでは root ログイン（Linux および VMware）または管理者ログイン（Windows）が必要になるため、ホストベースのファームウェア更新では、ログイン認証情報またはユーザー権限が iLO によって確認されません。

  オンラインによるインバンドファームウェア更新方法の例として、iLO オンライン ROM フラッシュコンポーネントがあります
- **アウトオブバンド** - ファームウェアは、ネットワーク接続経由で iLO に送信します。iLO 設定権限を持つユーザーは、アウトバンド方式を使用してファームウェアを更新できます。iLO セキュリティを無効にするようにシステムメンテナンススイッチが設定されている場合、すべてのユーザーは、アウトバンド方式でファームウェアを更新できます。

  オンラインでのアウトバンドのファームウェアの更新方法の例として、iLO Web インターフェース、iLO RESTful API および SMASH CLP があります。

詳細情報

オンラインでのファームウェアの更新

オフラインでのファームウェアの更新

オンラインでのファームウェアの更新

インバンドファームウェア更新

以下のインバンドファームウェア更新方法を使用できます。

オンライン **ROM** フラッシュコンポーネント - サーバーの稼動中に実行可能ファイルを使用してファームウェアを更新します。実行可能ファイルには、インストーラーとファームウェアパッケージが含まれています。NX7700x シリーズポータルサイト (https://jpn.nec.com/nx7700x/index.html)で、iLO およびサーバーファームウェア向けオンライン ROM フラッシュコンポーネントをダウンロードすることができます。

アウトバンドファームウェア更新

以下のアウトバンドファームウェア更新方法を使用できます。

- **iLO Web** インターフェース - iLO Web インターフェースを使用してサポートされるファームウェアファイルをダウンロードし、インストールします。単一のサーバーまたは iLO 連携グループのファームウェアを更新できます。
- **SMASH CLP** - SSH ポートを通じて SMASH CLP にアクセスし、標準のコマンドを使用してファームウェア情報を表示し、ファームウェアを更新します。

  SMASH CLP について詳しくは、iLO スクリプティング/コマンドラインガイドを参照してください。
- **iLO RESTful API** - iLO RESTful API および REST クライアントを使用して、ファームウェアを更新します。

詳細情報

フラッシュファームウェア機能を使用した iLO またはサーバーファームウェアの更新
iLO 連携グループファームウェアアップデート

オフラインでのファームウェアの更新

以下のオフラインファームウェア更新方法を使用できます。

- **Starter Pack** - Starter Pack を使用してブートした後にファームウェアをインストールします。詳細は本体装置のメンテナンスガイドを参照ください。

iLO Web インターフェースからのファームウェアの表示と更新

iLO の Web インターフェースは、次のファームウェアおよびソフトウェア管理機能をサポートしています。

- インストールされているファームウェアの表示。
- インストールされているソフトウェアの表示。
- フラッシュファームウェア制御機能を使用して、ローカル管理対象サーバーのファームウェアを更新。
- グループファームウェアアップデート機能を使用して、iLO フェデレーショングループの複数のサーバーに対するファームウェアの更新。
- Smart Update 機能を使用して iLO にアクセスする。このバージョンの iLO では、次の操作がサポートされています。
- iLO リポジトリを管理し、保存されたコンポーネントをインストールキューへ追加。
- インストールセットの表示と削除とインストールキューへの追加。SUM を使用してインストールセットを構成します。
- インストールキューからコンポーネントを表示および削除。

  ベストプラクティスは、SUM を使用してインストールキューを管理することです。iLO Web インターフェースを使用して、個々のコンポーネントを追加または削除してキューを更新することができます。

ファームウェアおよび OS ソフトウェアページのすべてのタブから、フラッシュファームウェア制御および iLO リポジトリにアクセスできます。

フラッシュファームウェア機能を使用した iLO またはサーバーファームウェアの更新

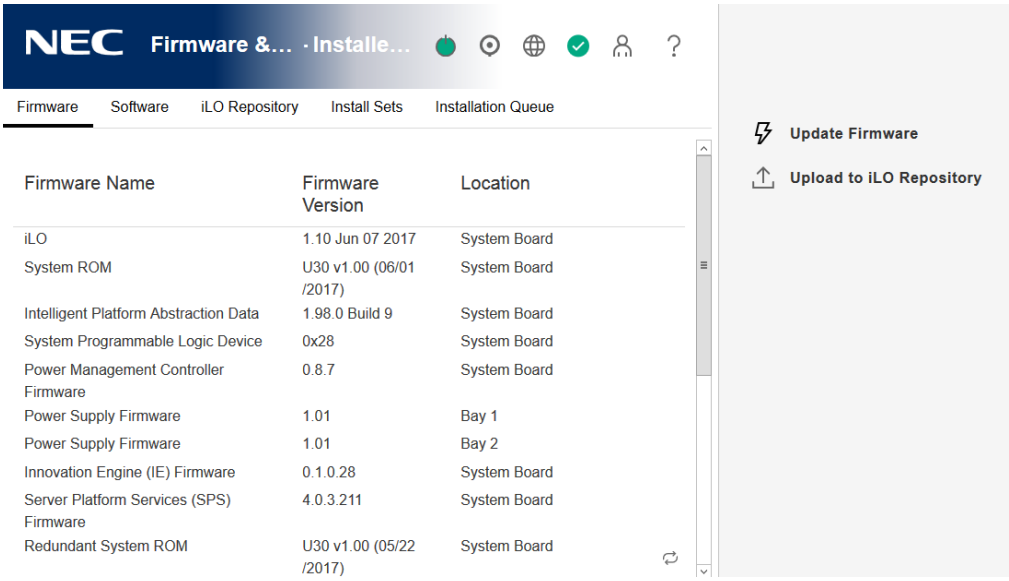
iLO Web インターフェースを使用して、任意のネットワーククライアントからファームウェアをアップデートできます。ファームウェアの更新には署名済みのファームウェアイメージファイルが必要です。また、iLO リポジトリページから登録済みのコンポーネントを更新することもできます。

前提条件

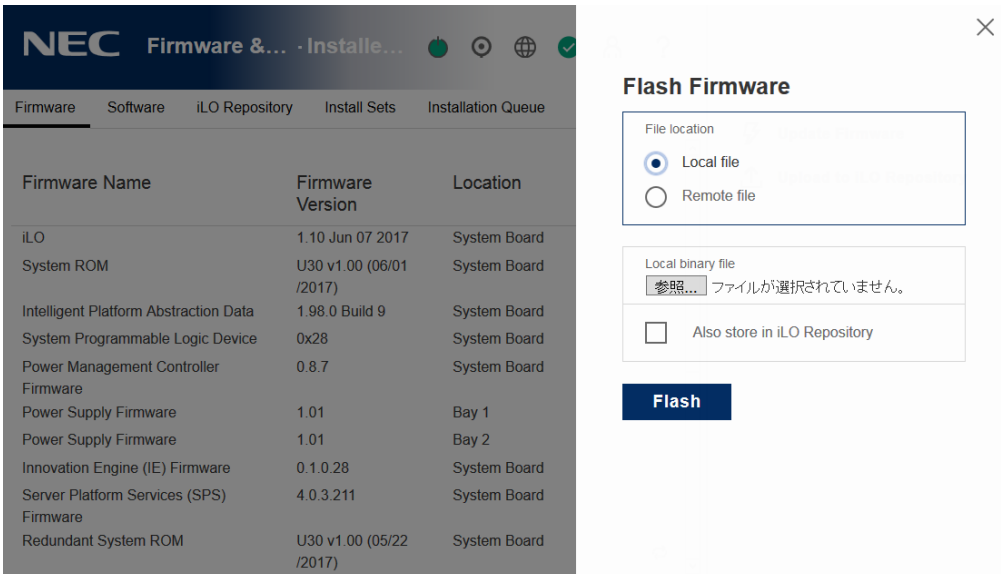
iLO の設定を構成権限

手順

1. ファームウェアイメージファイルを取得します。
2. **[Firmware & OS Software]**ページに移動し、**[Update Firmware]**をクリックします。**[Update Firmware]**オプションが表示されていない場合は、iLO Web インターフェースの右上隅にある ⋯ 省略記号アイコンをクリックし、**[Update Firmware]**をクリックします。



3. **[Local file]**または**[Remote file]**オプションを選択します。



4. 選択したオプションに応じて、次のいずれかを実行します。
   - **[Local binary file]**ボックスで、[参照]（Internet Explorer または Firefox）または[ファイルの選択]（Microsoft Edge または Chrome）をクリックし、ファームウェアコンポーネントの場所を指定します。
   - **[Remote binary file URL]** ボックスに、アクセス可能な Web サーバー上のファームウェアコンポーネントの URL を入力します。
5. オプション：更新するコンポーネントのコピーを iLO リポジトリに保存するには、**[Also store in iLO Repository]**チェックボックスをオンにします。
6. **[Flash]**をクリックし、更新プロセスを開始します。
   サーバーの設定に応じて、iLO は次のことを通知します。
   - iLO ファームウェアをアップデートすると、iLO は自動的に再起動します。
     一部の種類のサーバーファームウェアでサーバーの再起動が必要な場合がありますが、サーバーは自動的には再起動されません。
   - サーバーに TPM または TM がインストールされている場合、システム ROM または iLO ファームウェアのアップデートを開始する前に、TPM または TM に関する情報を格納するソフトウェアを一時停止またはバックアップしてください。たとえば、ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアの更新を開始する前に停止してください。これらの指示に従わなかった場合、データへのアクセスが失われる可能性があります。
7. 次のいずれかを実行します。
   - TPM または TM メッセージが表示されない場合は、**[OK]**をクリックします。
   - TPM または TM メッセージが表示された場合は、TPM または TM にデータを格納するソフトウェアが一時停止またはバックアップされていることを確認し、**[OK]**をクリックします。
     iLO ファームウェアは、ファームウェアイメージを受け取り、検証して、フラッシュします。

重要: ファームウェア更新を中断しないでください。ファームウェアの更新が中断された場合や更新に失敗した場合は、ただちに、再度、更新を試みてください。

iLO ファームウェアを更新すると、iLO が再起動し、ブラウザー接続が終了します。接続を再確立できるまでに数分かかります。

8. iLO ファームウェアの更新のみ：新しいファームウェアの使用を開始するには、ブラウザキャッシュをクリアしてから、iLO にログインします。
9. サーバーファームウェアの更新のみ：ファームウェアの種類に応じて新しいファームウェアを有効にするためにシステムリセットまたはサーバーの再起動が必要な場合は、適切な処置を行ってください。詳細については、「ファームウェアの更新が有効になるための要件」を参照してください。
10. オプション：新しいファームウェアが有効になっていることを確認するには、**[Firmware & OS Software]→[Firmware]**ページでファームウェアのバージョンを確認します。
概要ページで iLO ファームウェアバージョンを確認することもできます。

詳細情報

iLO ファームウェアの更新が失敗する

iLO ファームウェアイメージファイルの入手

サポートされるファームウェアタイプ

次のファームウェアタイプは、ファームウェアアップデートのページから更新できます。

- iLO ファームウェア
- システム ROM/BIOS
- シャーシ
- 電源管理コントローラ
- パワーマネージメントコントローラー
- システムプログラマブルロジックデバイス（CPLD）
- NVMe バックプレーンファームウェア
- 言語パック

ファームウェアの更新が有効になるための要件

- iLO ファームウェアおよび言語パック - 自動的に実行される iLO のリセットが必要です。
- システム ROM（BIOS） - サーバーの再起動が必要です。
- シャーシファームウェア（Power Management） - すぐに有効になります。
- システムプログラマブルロジックデバイス（CPLD）- サーバーの再起動が必要です。
- Power Management Controller および NVMe バックプレーンファームウェア - サーバーの再起動やシステムのリセットは必要ありません。

NVMe ファームウェアのバージョンは、次のサーバーの再起動後に iLO Web インターフェースに表示されます。

iLO ファームウェアイメージファイルの入手

iLO ファームウェアを更新する方法によっては、iLO オンライン ROM フラッシュコンポーネントに含まれる BIN ファイルが必要になります。

iLO オンライン ROM フラッシュコンポーネントファイルをダウンロードし、BIN ファイルを抽出するには、以下の手順に従ってください。

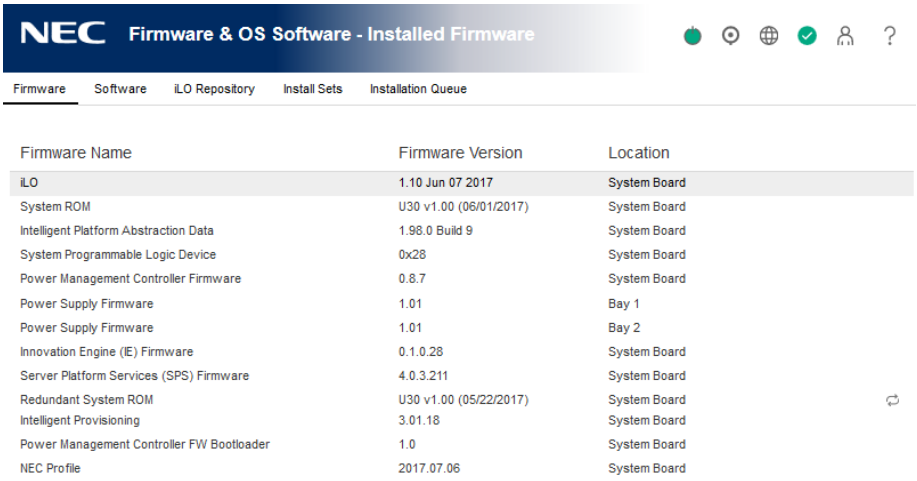
1. NX7700x シリーズポータルサイト（https://jpn.nec.com/nx7700x/index.html）に移動します。
2. 画面の指示に従って、iLO Online ROM Flash Component ファイルを見つけて、ダウンロードします。

   BIN ファイルを抽出するために、Windows または Linux のコンポーネントをダウンロードします。
3. BIN ファイルを抽出します。
   - Windows コンポーネントの場合、ダウンロードしたファイルをダブルクリックして、**[解凍]**ボタンをクリックします。ファイルを抽出する位置を選択して、**[OK]**をクリックします。
   - Linux コンポーネントの場合、ファイル形式によって異なりますが、次のいずれかのコマンドを入力します。
     - #sh ./CP00XXXX.scexe –unpack=/tmp/
     - #rpm2cpio `<firmware_file_name>.rpm` | cpio -id

     iLO ファームウェアイメージの名前は、ilo5_<yyy>.bin です。ここで、<yyy>はファームウェアバージョンを表します。

ファームウェア情報の表示

[Firmware & OS Software]ページに移動し、**[Firmware]**タブをクリックします。



ファームウェア情報ページには、さまざまなサーバーコンポーネントのファームウェア情報が表示されます。

サーバーの電源が切れている場合、このページの情報は、最後に電源が入っていた時点の情報を示します。ファームウェア情報は、サーバーの電源が入っており、POST が完了している場合にのみ更新されます。

ファームウェアの種類

ファームウェア情報ページに表示されるファームウェアタイプは、サーバーモデルおよびサーバーの構成によって変化します。

ほとんどのサーバーでは、システム ROM および iLO ファームウェアが表示されます。他の表示可能なファームウェアオプションは、次のとおりです。

- パワーマネージメントコントローラー
- サーバープラットフォームサービスファームウェア
- Smart アレイ
- Intelligent Platform Abstraction Data
- Smart Storage バッテリー
- TPM または TM ファームウェア
- SAS プログラマブルロジックデバイス
- システムプログラマブルロジックデバイス
- EXPRESSBUILDER
- ネットワークアダプター
- NVMe バックプレーンファームウェア
- Innovation Engine (IE)ファームウェア
- ドライブファームウェア

- 電源装置ファームウェア
- 内蔵ビデオコントローラー

ファームウェアの詳細

ファームウェア情報ページでは、リストされているファームウェアのタイプごとに以下の情報が表示されます。

- **[Firmware Name]** - ファームウェアの名前。
- **[Firmware Version]** - ファームウェアのバージョン。
- **[Location]** - 表示されたファームウェアを使用するコンポーネントの位置。

冗長化 ROM の入れ替え

前提条件

- 本体装置が冗長化システム ROM をサポートしている必要があります。
- 仮想電源およびリセット権限

ROM 設定の更新

1. **[Firmware & OS Software]**→**[Firmware]**ページに移動します。
2. アクティブシステム ROM とバックアップシステム ROM を交換するには、Redundant System ROM の右に表示される🔁アイコンをクリックします。

3. 要求を確認するメッセージが表示されたら、**[OK]**をクリックします。

   変更は、次のシステム再起動後に有効になります。

注意：ファームウェアアップデート中にブラウザーのリロードボタン実行もしくは F5 キー押下を実行しないでください。

iLO ファームウェアではファームウェアアップデート中にブラウザーのリロードボタン実行もしくは F5 キー押下を実行して、アップデートが完了しない状態になった場合は、ILO のリセットを行ってください。

---

iLO レポジトリ

iLO レポジトリは、マザーボードに内蔵された不揮発性フラッシュメモリ内にある安全なストレージ領域です。このフラッシュメモリは、iLO NAND と呼ばれます。Smart Update Manager（SUM）、または iLO を使用して、iLO レポジトリ内の署名済みのソフトウェアおよびファームウェアコンポーネントを管理します。

iLO、UEFI BIOS、Smart Update Manager、および他のクライアントソフトウェアでこれらのコンポーネントを取得してサポートされるサーバーに適用できます。Smart Update Manager を使用して、インストールセットに保存するコンポーネントを整理し、Smart Update Manager または iLO を使用してインストールキューを管理します。

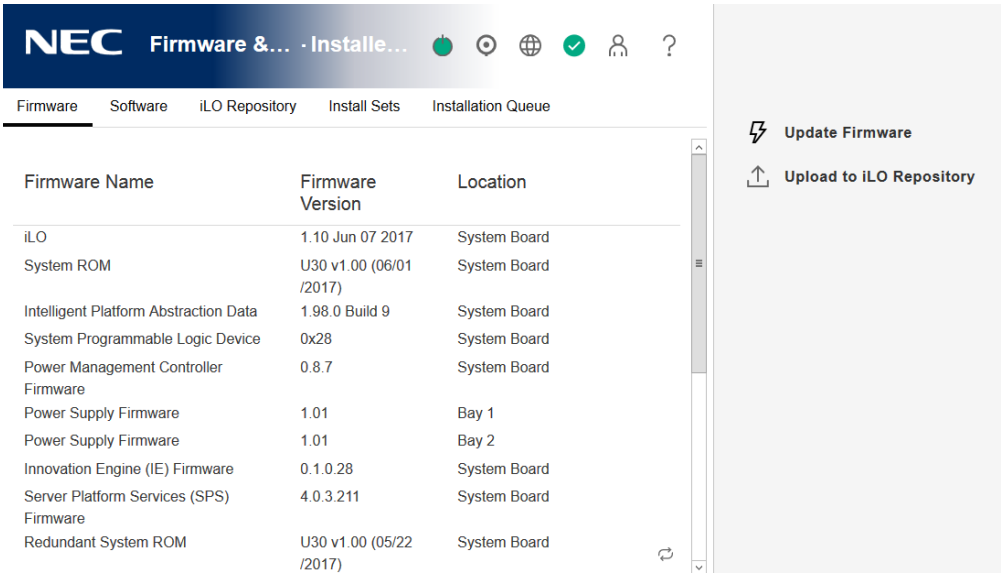
iLO レポジトリにコンポーネントの追加

前提条件

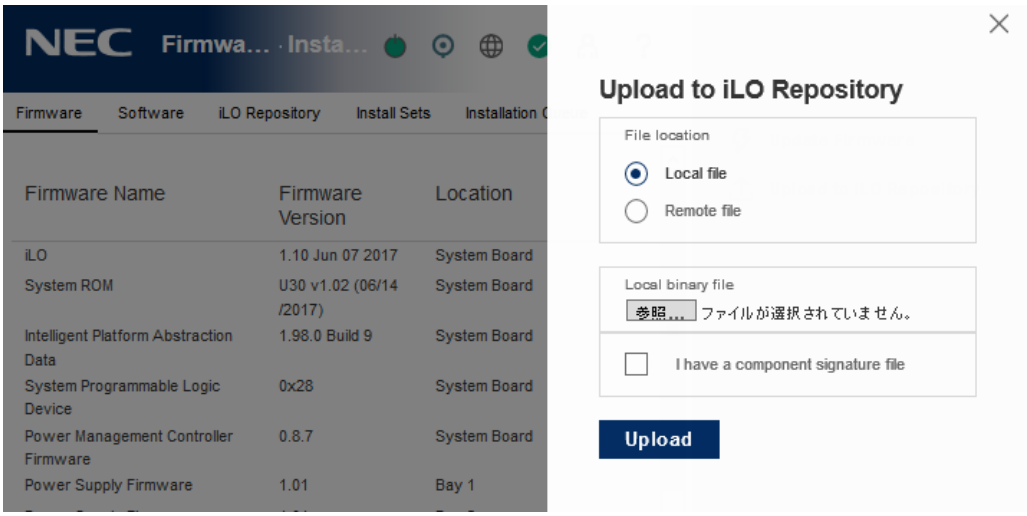
iLO の設定を構成権限

手順

1. **[Firmware & OS Software]**ページに移動し、**[Upload to iLO Repository]**をクリックします。**[Upload to iLO Repository]**オプションが表示されていない場合は、iLO Web インターフェースの右上隅にある ⋯ 省略記号アイコンをクリックし、**[Upload to iLO Repository]**をクリックします。



2. **[Local file]**または**[Remote file]**オプションを選択します。



3. 選択したオプションに応じて、次のいずれかを実行します。
   - **[Local binary file]**ボックスで、**[参照]**（Internet Explorer または Firefox）または**[ファイルの選択]**（Chrome）をクリックし、ファームウェアコンポーネントの場所を指定します。
   - **[Remote binary file URL]** ボックスに、アクセス可能な Web サーバー上のファームウェアコンポーネントの URL を入力します。
4. 複数ファイルのみで指定されたファームウェアコンポーネントの場合：［**I have a component signature file**］チェックボックスを選択します。
5. 前の手順でチェックボックスを選択した場合は、以下のいずれかを実行します。
   - ［**Local component signature file**］ボックスで、**[参照]**（Internet Explorer または Firefox）あるいは**[ファイルの選択]**（Microsoft Edge または Chrome）をクリックしてから、コンポーネント署名ファイルの場所を指定します。
   - ［**Remote component signature file URL**］ボックスに、アクセス可能な Web サーバー上のコンポーネント署名ファイルの URL を入力します。
6. ［**Upload**］をクリックします。
   既存のコンポーネントと同じ名前を持つコンポーネントをアップロードすると既存のコンポーネントが置換されることが iLO により通知されます。コンポーネントがリカバリーセットの一部である場合は保護されており、同じ名前の新しいコンポーネントをアップロードすることで置換することはできません。リカバリーセットのコンポーネントを置換するには、リカバリーセット権限を持つアカウントでログインしてから、リカバリーインストールセットを削除します。
7. ［**OK**］をクリックします。アップロードが開始されます。アップロードステータスは iLO Web インターフェースの上部に表示されます。

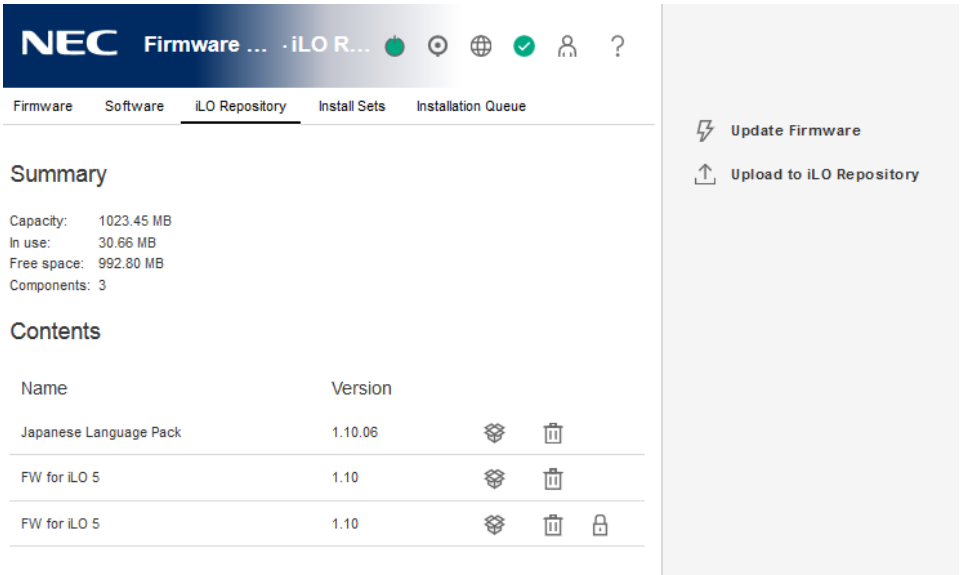
iLO レポジトリからのコンポーネントのインストール

iLO レポジトリのページからインストールキューにコンポーネントを追加できます。
コンポーネントをインストールキューに追加すると、コンポーネントはキューの末尾に追加されます。キューに入れられた他の項目が完了した後、コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときに、追加されたコンポーネントがインストールされます。アップデートを開始できるソフトウェアについては、iLO レポジトリのページとインストールキューページでコンポーネントの詳細を確認してください。
キューにすでに入れられているタスク内のコンポーネントが開始または終了を待機している場合、キューに入れられた新しいコンポーネントは無期限に遅延する場合があります。たとえば、キューに入れられたアップデートがサーバーの POST 中に UEFI BIOS によって検出されるまで待機する必要があり、サーバーが再起動されていない場合、キュー内のその後のアップデートはインストールされません。

前提条件
iLO の設定を構成権限

手順

- **[Firmware & OS Software]→[iLO Repository]**ページに移動します。



- インストールするコンポーネントの横にある、コンポーネントの  インストールアイコンをクリックします。
  iLO は、コンポーネントがインストールキューの末尾に追加されることを通知し、要求を確認するプロンプトを表示します。
- **[Yes, add to the end of the queue]**をクリックします。
  キューに入れられた既存のタスクが終了し、選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出すると、アップデートが開始されます。

iLO レポジトリからのコンポーネントの削除

前提条件

- iLO の設定を構成権限
- コンポーネントがインストールセットに含まれていない。

- コンポーネントがキュー内のタスクの一部ではない。

手順

1. **[Firmware & OS Software]**→**[iLO Repository]**ページに移動します。
2. コンポーネントの削除アイコンをクリックします。iLO によって要求を確認するように求められます。
3. **[Yes, remove]**をクリックします。

iLO レポジトリの概要とコンポーネントの詳細の表示

手順

1. **[Firmware & OS Software]**→**[iLO Repository]**ページに移動します。
2. オプション：コンポーネントの詳細な情報を表示するには、個々のコンポーネントをクリックします。

iLO レポジトリの詳細

iLO レポジトリのストレージの詳細

iLO レポジトリページの概要セクションには、iLO レポジトリのストレージの使用状況に関する以下の詳細が表示されます。

手順

1. **[Capacity]** - iLO レポジトリの総ストレージ容量
2. **[In use]** - 使用されているストレージ
3. **[Free space]** - iLO レポジトリの使用可能なストレージ
4. **[Components]** - iLO レポジトリに保存されているコンポーネントの数

iLO レポジトリの内容

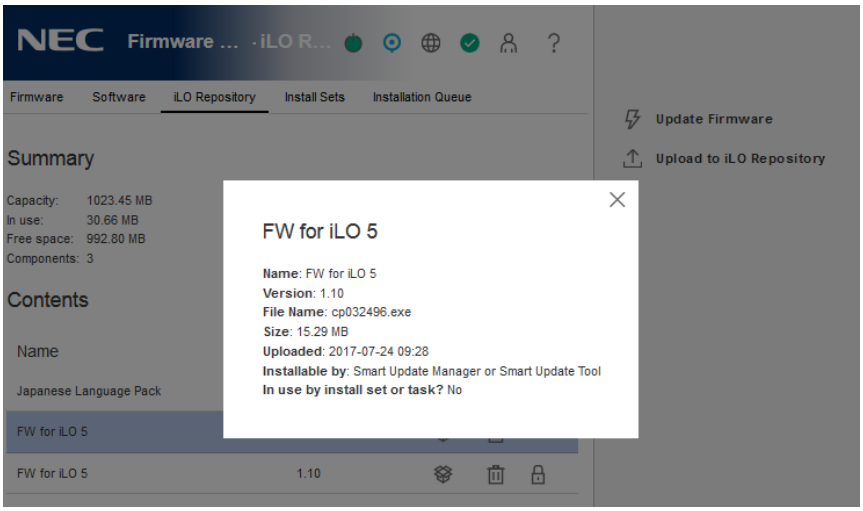
iLO レポジトリページの **Contents** セクションには、ソフトウェアコンポーネントまたは各ファームウェアに関する以下の詳細が表示されます。

手順

1. **[Name]** - コンポーネント名
2. **[Version]** - コンポーネントのバージョン

iLO レポジトリの個々のコンポーネントの詳細

個々のコンポーネントをクリックすると、以下の詳細が表示されます。



- ［**Name**］- コンポーネント名
- ［**Version**］- コンポーネントのバージョン
- ［**File Name**］- コンポーネントのファイル名
- ［**Size**］- コンポーネントのサイズ
- ［**Uploaded**］- アップロードの日時
- ［**Installable by**］- コンポーネントのアップデートを開始できるソフトウェア
- ［**In use by install set or task?**］- コンポーネントがインストールセットの一部かどうか

インストールセット

インストールセットは、1 つのコマンドで、サポートされるサーバーに適用できるコンポーネントセットです。iLO を使用して既存のインストールセットを iLO Web インターフェースに表示できます。

インストールセットのインストール

インストールセットページからインストールセットをインストールキューに追加できます。
インストールセットをインストールキューに追加すると、iLO は、インストールセット内のコンポーネントまたはコマンドごとにタスクをインストールキューの末尾に追加します。キューに入れられた他の項目が完了した後、各コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときに、インストールセットの内容がインストールされます。アップデートを開始できるソフトウェアについては、コンポーネントの詳細を確認してください。
キューにすでに入れられているタスク内のコンポーネントが開始または終了を待機している場合、キューに入れられた新しいコンポーネントは無期限に遅延する場合があります。たとえば、キューに入れられたアップデートがサーバーの POST 中に UEFI BIOS によって検出されるまで待機する必要があり、サーバーが再起動されていない場合、キュー内のその後のアップデートはインストールされません。

前提条件

- iLO の設定を構成権限
- インストールセット内のコンポーネントが別のインストールタスクの一部としてキューに入れられることはありません。

手順

1. **[Firmware & OS Software]→[Install Sets]**ページに移動します。
2. インストールセットの横にあるインストールアイコンをクリックします。
3. iLO は、インストールセットの内容がインストールキューの末尾に追加されることを通知し、要求を確認するプロンプトを表示します。
4. **[Yes, add to the end of the queue]**をクリックします。
5. キューに入れられた既存のタスクが終了し、選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出すると、アップデートが開始されます。

インストールセットの削除

前提条件

- iLO の設定を構成権限
- リカバリーセット権限

手順

1. **[Firmware & OS Software]→[Install Sets]**ページに移動します。
2. コンポーネントの削除アイコンをクリックします。
3. iLO によって要求を確認するように求められます。
4. **[Yes, remove]**をクリックします。
5. インストールセットが削除されます。

インストールセットの表示

1. **[Firmware & OS Software]→[Install Sets]**ページに移動します。

オプション：インストールセットをクリックして詳細情報を表示します。

インストールセットの詳細

インストールセットの概要の詳細

インストールセットタブには、各インストールセットに関する以下の詳細が表示されます。

- **[Name]** - インストールセットの名前。
- **[Components/Commands]** - インストールセット内のコンポーネントとコマンド。

インストールセットアイコンを使用して、インストールセットをインストールキューに追加したり、インストールセットを削除したりします。保護されたインストールセットは、ロックアイコン付きで表示されます。

個々のインストールセットの詳細

個々のインストールセットをクリックすると、以下の詳細が表示されます。

- **[Name]** - インストールセットの名前。
- **[Created]** - 作成日時。
- **[Description]** - インストールセットの説明。
- **[Component/Commands]** - インストールセット内のコンポーネントとコマンド。

- **[System Recovery Set?]** - インストールセットを編集または削除できるかどうかを示します。このステータスは、リカバリーセットで使用されていることを示します。保護されたセットは同時に 1 つのみ存在できます。

システムリカバリセット

デフォルトでは、システムリカバリセットがすべてのサーバーに付属します。リカバリーセット権限を持つユーザーアカウントのみがこのインストールセットを構成できます。
デフォルトのリカバリーセットには、以下のファームウェアコンポーネントが含まれます。

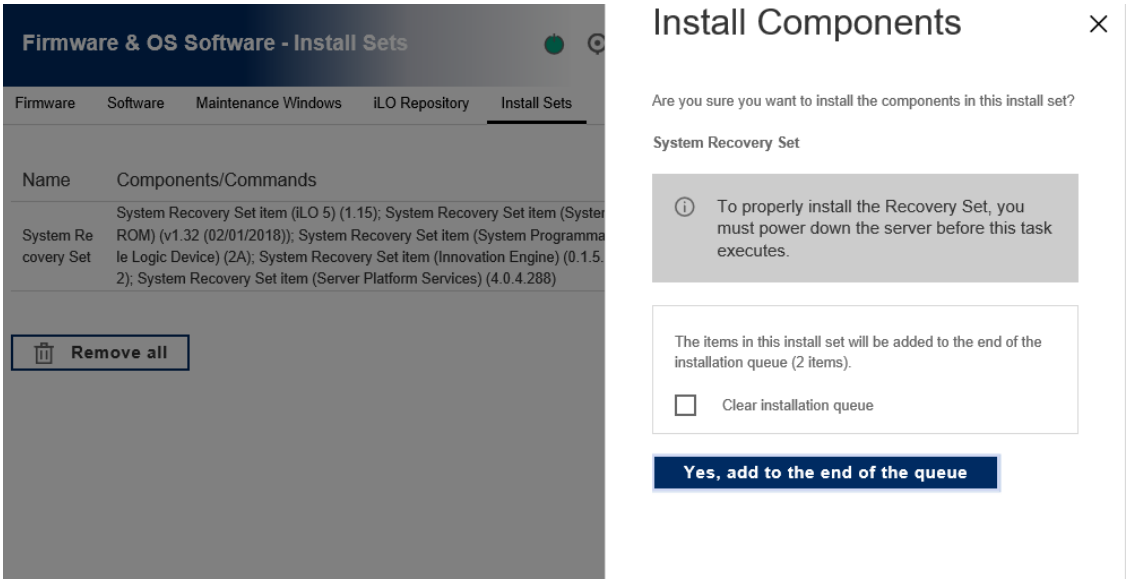
- システム ROM（BIOS）
- iLO ファームウェア
- システムプログラマブルロジックデバイス（CPLD）
- Innovation Engine
- サーバープラットフォームサービス（SPS）ファームウェア

デフォルトのリカバリーセットが削除された場合、リカバリーセット権限を持つユーザーは Smart Update Manager を使用してインストールセットを作成し、iLO RESTful API を使用してインストールセットを保護された状態に設定できます。保護されたインストールセットは同時に 1 つのみ存在できます。

手順については、Smart Update Manager ユーザーガイドを参照してください。システムリカバリセットは同時に 1 つのみ存在できます。

インストールキューのクリア

インストレーションセットがインストールキューに登録されている場合、**[Install Components]** 表示画面の**[Clear Installation queue]**でクリアすることができます。



インストールキュー

インストールキューは、順序付けされたコンポーネントとインストールセットのリストです。Smart Update Manager を使用してキューを管理します。iLO Web インターフェースから、キューに入れられたタスクを表示したり、1 つのコンポーネントをキューに追加したりできます。
コンポーネントをインストールキューに追加すると、コンポーネントはキューの末尾に追加されます。キューに入れられた他の項目が完了した後、コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときに、追加されたコンポーネントがインストールされます。アップデートを開始できるソフトウェアについては、iLO レポジトリページとインストールキューページでコンポーネントの詳細を確認してください。
キューにすでに入れられているタスク内のコンポーネントが開始または終了を待機している場合、キューに入れられた新しいコンポーネントは無期限に遅延する場合があります。たとえば、キューに入れられたアップデートがサーバーの POST 中に UEFI BIOS によって検出されるまで待機する必要があり、サーバーが再起動されていない場合、キュー内のその後のアップデートはインストールされません。

インストールキューの表示

1. **[Firmware & OS Software]→[Installation Queue]**ページに移動します。
2. オプション：詳細な情報を表示するには、個々のタスクをクリックします。

インストールキューの詳細

タスク概要の詳細

インストールキュータブには、各タスクに関する以下の詳細が表示されます。

- **[State]** - タスクのステータス。値には、以下のものがあります。
- **[In progress] -** タスクは処理されています。
- **[Expired] -** タスクの期限が切れています。このタスクがキューから削除されるまで、その後のタスクは実行されません。
- **[Exception] -** タスクを完了できませんでした。このタスクがキューから削除されるまで、その後のタスクは実行されません。
- **[Complete] -** タスクが正常に完了しました。
- **[Pending] -** コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときにタスクは実行されます。
- **[Name]** - タスク名。
- **[Starts]** - タスクの開始日時。
- **[Expires]** - タスクの有効期限（日付と時刻）。

個々のタスクの詳細

個々のタスクをクリックすると、以下の詳細が表示されます。

- **[Name]** - タスク名。
- **[State]** - タスクのステータス。
- **[Result]** - タスクの結果（ある場合）。
- **[Installable by]** - 選択したコンポーネントのアップデートを開始できるソフトウェア。
- **[Start time]** -タスクの開始日時。
- **[Expiration]** -タスクの有効期限（日付と時刻）。

インストールキューからのタスクの削除

前提条件

iLO の設定を構成権限

手順

1. **[Firmware & OS Software]**→**[Installation Queue]**ページに移動します。
2. コンポーネントの削除アイコンをクリックします。
3. iLO によって要求を確認するように求められます。
4. **[Yes, remove]**をクリックします。
5. インストールセットが削除されます。

言語パックのインストール

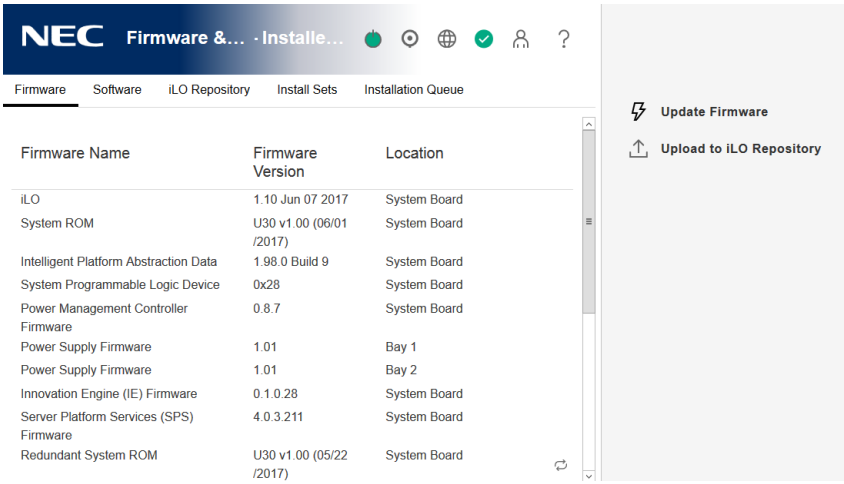
前提条件

iLO の設定を構成権限

手順

1. 次の Web サイトに移動します。https://jpn.nec.com/nx7700x/index.html
2. 画面の指示に従って、言語パックを見つけて、ダウンロードします。
3. ダウンロードしたファイルをダブルクリックして、内容を解凍します。

   言語パックのファイル名は次のような形式です。lang_< 言語 >_< バージョン >.lpk
4. **[Firmware & OS Software]**ページに移動し、[**Flash Firmware**]をクリックします。



5. **[参照]**（Internet Explorer または Firefox）または **[ファイルを選択]**（Microsoft Edge または Chrome）をクリックします。
6. 言語パックを選択し、**[開く]**をクリックします。

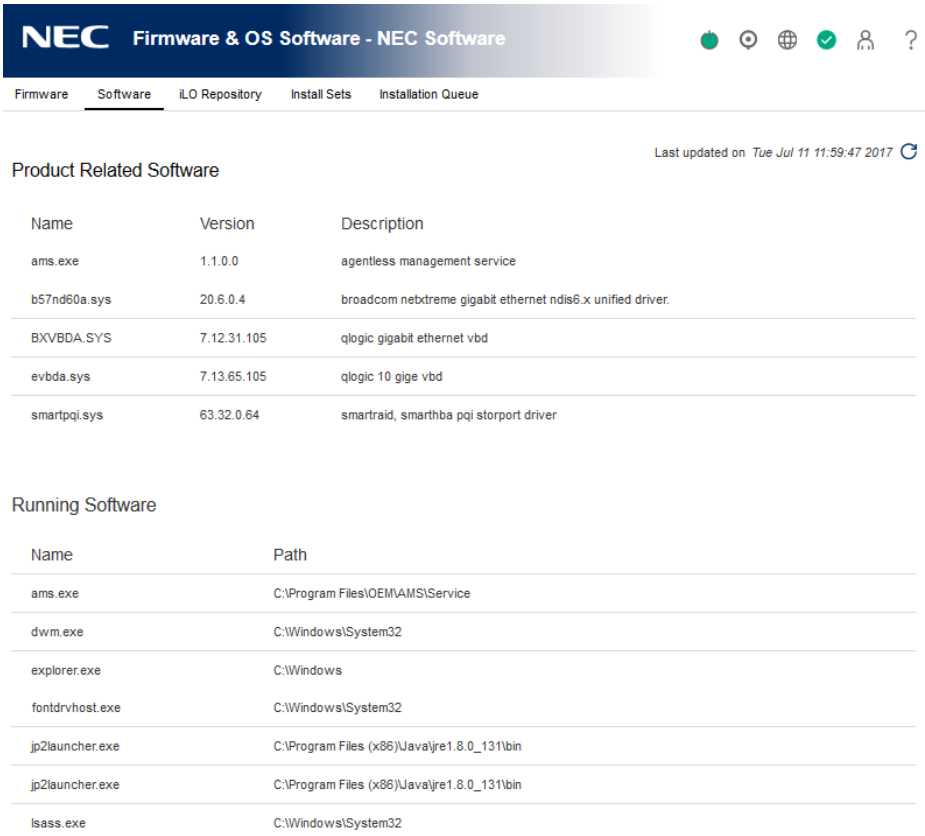
   iLO に、インストールの確認を求めるメッセージが表示されます。
7. **[OK]**をクリックします。
8. **[Flash]**をクリックします。

   iLO に言語パックがインストールされ、再起動し、ブラウザー接続が終了します。

   接続を再確立できるまでに数分かかります。

ソフトウェア情報の表示

1. **[Firmware & OS Software]**ページに移動し、**[Software]**タブをクリックします。



2. 次のいずれかを選択します。

- **[Product Related Software]** - 管理対象サーバー上のすべての製品関連ソフトウェアを表示します。これには、手動で、または StarterPack を使用して追加されたソフトウェアと NEC 推奨の他社製ソフトウェアが含まれます。
- **[Running Software]** - 管理対象サーバー上で実行されているか、実行可能であるすべてのソフトウェアを示します。
    - ✧ **[Installed Software]** - 管理対象サーバーにインストールされているすべてのソフトウェアを示します。このページのすべてのデータのセットを表示するには、AMS がインストールされている必要があります。

製品関連ソフトウェアの詳細

- **[Name]** - ソフトウェアの名前。
- **[Version]** - ソフトウェアのバージョン。

  このページに表示されるファームウェアコンポーネントのバージョンは、ローカルのオペレーティングシステムに保存されているファームウェアフラッシュコンポーネントで利用可能なファームウェアバージョンを示しています。表示されるバージョンが、サーバーで実行されているファームウェアと一致しない可能性があります。
- **[Description]** - ソフトウェアの説明。

実行中のソフトウェアの詳細

- **[Name]** - ソフトウェアの名前。
- **[Path]** - ソフトウェアのファイルパス。

インストールされたソフトウェアの詳細

- **[Name]** - インストールされた各ソフトウェアプログラムの名前が表示されます。

> △**注意:**
> OS 起動直後など AMS が起動できていないタイミングでは、iLO のファームウェア&OS ソフトウェアメニューのソフトウェアタブの情報に AMS のバージョンが表示されない場合があります。少し待ってからブラウザのリロードボタン押下もしくは F5 キー入力によりページの再読み込みを行ってしてください。

メンテナンスウィンドウ

メンテナンスウィンドウでは、インストレーションタスクを実行する時間枠を設定できます。
メンテナンスウィンドウは次のいずれかの方法で作成できます。

- メンテナンスウィンドウタブ上
- タスクをインストールキューに追加するとき

メンテナンスウィンドウの追加

前提条件
iLO の設定を構成権限

手順

1. ナビゲーションツリーで**[Firmware & OS Software]**をクリックし、**[Maintenance Windows]**をクリックします。
2. メンテナンスウィンドウの追加アイコン＋をクリックします。
   iLO に、メンテナンスウィンドウ情報を入力するよう求められます。
3. **[Name]**ボックスに名前を入力します。
4. **[Description]**ボックスに説明を入力します。
5. メンテナンスウィンドウの開始時刻と終了時刻を[**From**]および[**To**]ボックスに入力します。
   a **[From]**ボックスにある🕒をクリックします。
   カレンダーが表示されます。
   b 開始日時を選択し、完了をクリックします。
   c **[To]**ボックスにある🕒をクリックします。
   カレンダーが表示されます。
   d 終了日時を選択し、完了をクリックします。
   iLO を管理するために使用しているクライアントの現時時間に基づいて日時を入力します。
   入力した日時に相当する UTC が日時の上に表示されます。
6. **[Add]**をクリックします。
   メンテナンスウィンドウが追加されます。

メンテナンスウィンドウの編集

前提条件

iLO の設定を構成権限

手順

1. ナビゲーションツリーでファームウェア & OS ソフトウェアをクリックし、メンテナンスウィンドウをクリックします。
2. 固定モードから編集モードに変更するには、  .
   iLO に、メンテナンスウィンドウ情報を更新するよう求められます。
3. 名前ボックスでメンテナンスウィンドウ名を更新します。
4. 説明ボックスで説明を更新します。
5. 開始および終了ボックスでメンテナンスウィンドウの開始時刻と終了時刻を更新します。
   a **[From]**ボックスにある  をクリックします。
   カレンダーが表示されます。
   b 開始日時を選択し、完了をクリックします。
   c **[To]**ボックスにある  をクリックします。
   カレンダーが表示されます。
   d 終了日時を選択し、完了をクリックします。
   iLO を管理するために使用しているクライアントの現時時間に基づいて日時を入力します。
   入力した日時に相当する UTC が日時の上に表示されます。
   キュー内の既存のタスクの開始時刻よりも前の終了日時を入力した場合、iLO から、別の値を入力するよう求められます。インストールキューは、タスクの「先入れ先出し」リストです。既存のタスクの実行前に有効期限が切れるメンテナンスウィンドウを作成することはできません。
6. OK をクリックします。
   メンテナンスウィンドウが更新されます。

メンテナンスウィンドウの削除

前提条件

iLO の設定を構成権限

手順

1. ナビゲーションツリーで **[Firmware & OS Software]** をクリックし、**[Maintenance Windows]**をクリックします。
2. メンテナンスウィンドウの削除アイコン  をクリックします。
   iLO に、すべてのメンテナンスウィンドウの削除を確認するプロンプトが表示されます。
3. **[Yes, remove]**をクリックします。
   メンテナンスウィンドウが削除されます。

すべてのメンテナンスウィンドウを削除

前提条件

iLO の設定を構成権限

手順

1. ナビゲーションツリーで**[Firmware & OS Software]**をクリックし、**[Maintenance Windows]**をクリックします。
2. **[Remove all]**をクリックします。iLO に、すべてのメンテナンスウィンドウの削除を確認するプロンプトが表示されます。
3. **[Yes, remove all]**をクリックします。メンテナンスウィンドウが削除されます。

メンテナンスウィンドウの表示

手順

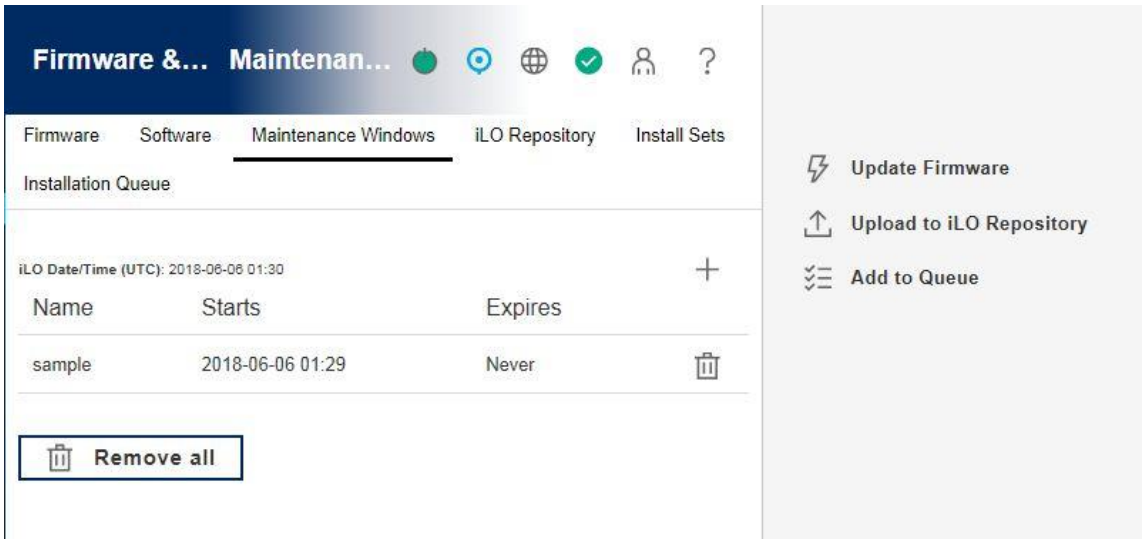
1. ナビゲーションツリーで**[Firmware & OS Software]**をクリックし、**[Maintenance Windows]**をクリックします。
2. オプション：詳細情報を表示するには、個々のメンテナンスウィンドウをクリックします。

メンテナンスウィンドウのサマリーの詳細

メンテナンスウィンドウタブに iLO の日時および構成された各メンテナンスウィンドウに関する次の詳細が表示されます。

- **[Name]** - メンテナンスウィンドウのユーザー定義名。
- **[From]** - メンテナンスウィンドウの開始時刻（UTC）。
- **[To]** - メンテナンスウィンドウの終了時刻（UTC）。

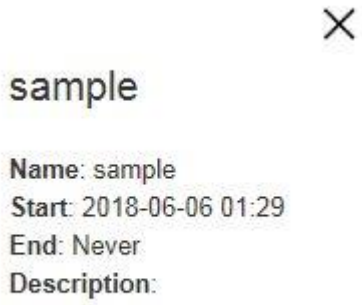
メンテナンスウィンドウは期限を過ぎてから 24 時間以内に自動的に削除されます。



各メンテナンスウィンドウの詳細

各メンテナンスウィンドウをクリックすると、以下の詳細が表示されます。

- **[Name]** - メンテナンスウィンドウのユーザー定義名。
- **[From]** - メンテナンスウィンドウの開始時刻（UTC）。
- **[To]** - メンテナンスウィンドウの終了時刻（UTC）。
- **[Description]** - メンテナンスウィンドウの説明。



オープンソースライセンス

[Open source licenses]をクリックすると、iLO で使用しているオープンソースとその権利表示を行います。

7. iLO 連携機能の設定と使用

iLO 連携機能

iLO 連携では、iLO Web インターフェースを実行している 1 つのシステムから複数のサーバーを管理できます。

iLO 連携が設定されている場合、iLO は、マルチキャスト検出での他 iLO システムの検出を行い、、ピアツーピア通信により他 iLO システムとの通信及び情報交換を行います。

iLO Web インターフェースの iLO 連携ページ上のデータがロードされると、Web インターフェースを実行する iLO システムから iLO のピア、およびそれらのピアから他のピア、選択した iLO 連携グループのすべてのデータが取得されるまでデータのリクエストが送信されます。

iLO 5 は、次の機能がサポートされています。

- グループのヘルスステータス - サーバーのヘルス情報とモデル情報を表示します。
- グループの仮想メディア - iLO 連携グループ内のサーバーからアクセスできるスクリプト方式のメディアに接続します。
- グループの電力制御 - iLO 連携グループ内のサーバーの電力情報を管理します。
- グループ消費電力上限 - iLO 連携グループ内のサーバーに対して動的な消費電力上限を設定します。
- グループファームウェアアップデート - iLO 連携グループ内のサーバーのファームウェアを更新します。
- グループ構成 - 複数の iLO システムに iLO 連携グループメンバーシップを追加します。

どのユーザーも iLO 連携ページで情報を表示できますが、グループの仮想メディア、グループの電力制御、グループ消費電力上限、グループ構成、およびグループファームウェアアップデートを使用するにはライセンスが必要です

iLO 連携の設定

iLO 連携機能を使用するための前提条件

- ネットワーク構成が、iLO 連携の要件を満たしている。
- iLO 連携グループに追加される各 iLO システムで、マルチキャストオプションが構成されている。

  デフォルトのマルチキャストオプション値を使用する場合、構成は不要です。
- iLO 連携のグループメンバーシップが構成されている。

  すべての iLO システムが、自動的に**[DEFAULT]**グループに追加されます。

iLO 連携のネットワーク要件

- iLO 5 Firmware Version 1.15 Aug 17 2017 以前で iLO 連携を使用する際には、iLO 専用のネットワークポート構成を使用する必要があります。これらのバージョンの iLO ファームウェアでは、iLO 連携機能は iLO 共有ネットワークポート構成ではサポートされていません。iLO

5 Firmware Version 1.20 Feb 02 2018 以降では、iLO 共有ネットワークポートで iLO 連携をご使用いただけます。

- オプション：iLO 連携は、IPv4 と IPv6 の両方をサポートしています。両方のオプションについて有効な構成があり、iLO システムで IPv6 ではなく IPv4 を使用する場合は、 **[iLO Dedicated Network Port]→[IPv6]** ページの **[iLO Client Applications use IPv6 first]**チェックボックスをクリアします。
- 複数の場所にある iLO システムを管理する場合は、マルチキャストトラフィックを転送するようにネットワークを設定します。
- ネットワーク内のスイッチにマルチキャストトラフィックを有効または無効にするためのオプションが含まれている場合は、有効になっていることを確認します。これは、iLO 連携が、ネットワーク上で iLO システムを検出するために必要です。
- レイヤー 3 スイッチで分断されている iLO システムの場合は、ネットワーク間で SSDP マルチキャストトラフィックを転送するためにスイッチを構成する必要があります。
- iLO システム間のマルチキャストトラフィック（UDP ポート 1900）と直接 HTTP（TCP のデフォルトポート 80）通信を許可する必要があります。
- 複数の VLAN を持つネットワークでは、VLAN 間のマルチキャストトラフィックを許可するスイッチを構成します。
    - IPv4 ネットワークの場合：スイッチの PIM を有効にし、PIM デンスモードに設定します。
    - IPv6 ネットワークの場合：スイッチを MLD スヌーピングに設定します。

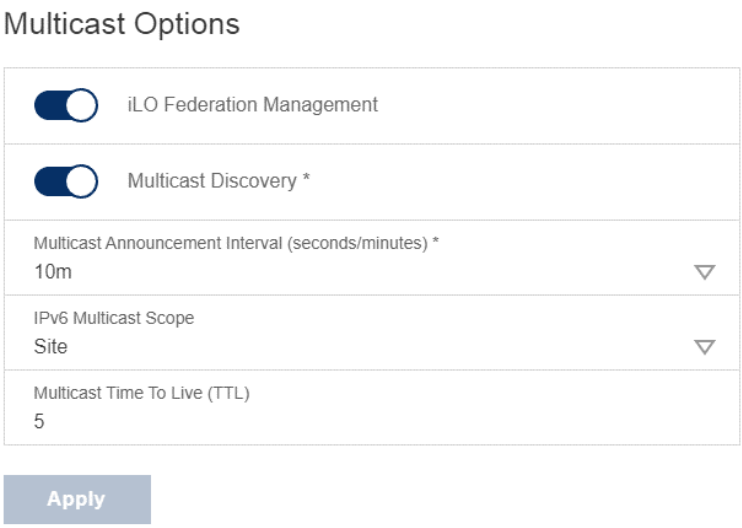
1 つの iLO システムのマルチキャストオプションを一度に構成する方法

以下の手順を使用して、iLO 連携グループに追加される各 iLO システムのマルチキャストオプションを構成します。デフォルト値を使用する場合、構成は不要です。

前提条件
iLO の設定を構成権限

手順

1. **[iLO Federation]→[Setup]**ページに移動します。



2. **[iLO Federation Management]**には、**[**有効**]**または **[**無効**]**を選択します。

   デフォルト設定は、**[**有効**]**です。**[**無効**]**を選択すると、ローカル iLO システムに対し iLO 連携機能が無効になります。

3. **[Multicast Discovery]**には、**[**有効**]**または **[**無効**]**を選択します。

   デフォルト設定は、**[**有効**]**です。**[**無効**]**を選択すると、ローカル iLO システムに対し iLO 連携機能が無効になります。

4. **[Multicast Announcement Interval (seconds/minutes)]**の値を入力します。

   この値は、iLO システムがネットワーク上で通知する頻度を設定します。各マルチキャスト通知は約 300 バイトです。30 秒 ～30 分の値を選択します。デフォルト値は 10 分です。

   [無効**]**を選択すると、ローカル iLO システムに対し iLO 連携機能が無効になります。

5. **[IPv6 Multicast Scope]**の値を選択します。

   有効な値は、**[Link]**、**[Site]**、および **[Organization]**です。デフォルト値は **[Site]**です。マルチキャスト検出が正しく機能するようにするため、**[IPv6 Multicast Scope]** に、同じグループ内のすべての iLO システムで同じ値を使用していることを確認してください。

6. **[Multicast Time To Live (TTL)]**の値を入力します。

   この値は、マルチキャスト検出が停止する前に通過できるスイッチの数を指定します。デフォルト値は、5 です。

   マルチキャスト検出が正しく機能するようにするため、**[Multicast Time To Live (TTL)]**に、同じグループ内のすべての iLO システムで同じ値を使用していることを確認してください。

7. **[Apply]**をクリックして、設定を保存します。

   ネットワークが変更され、このページで行った変更は、次のマルチキャスト通知後に有効となります。

iLO 連携グループ

ローカル iLO システムに対する iLO 連携グループメンバーシップ

ローカル iLO システムにグループメンバーシップを構成する場合、グループのメンバーがローカルの管理対象サーバーを構成するために所有する権限を指定する必要があります。

たとえば、ローカル iLO システムを **group1** に追加し、**[Virtual Power and Reset]** 権限を割り当てた場合、**group1** 内の他の iLO のユーザーはグループの電力制御機能を使用して、管理対象サーバーの電力状態を変更できます。

ローカル iLO システムが **[Virtual Power and Reset]**権限を **group1** に認めていない場合は、**group1** の他の iLO システムのユーザーはグループの電力制御機能を使用して、管理対象サーバーの電力状態を変更することはできません。

ローカル iLO システム上で、iLO セキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、**group1** 内の他の iLO システムのユーザーは、割り当てられたグループ権限とは無関係に、任意の iLO 連携機能を使用してサーバーの状態を変更できます。

ローカル iLO システムに対するグループメンバーシップは、**[iLO Federation]→[Setup]**ページで設定します。

ローカル iLO システムに対して、以下のタスクを実行できます。

- グループメンバーシップの表示。
- グループメンバーシップの追加と編集。
- グループメンバーシップの削除。

詳細情報

iLO 連携グループメンバーシップを追加する（ローカル iLO システム）

iLO 連携グループメンバーシップを編集する（ローカル iLO システム）

iLO 連携グループからのローカル iLO システムの削除

iLO システムのセットに対する iLO 連携グループメンバーシップ

複数の iLO システムに対してグループメンバーシップを追加する場合、グループのメンバーがグループの他のメンバーを構成するために所有する権限を指定する必要があります。

たとえば、**DEFAULT** グループに基づいて **group2** を構成し、**[Virtual Power and Reset]**権限を割り当てた場合、**group2** の iLO システムのユーザーはグループの電力制御機能を使用して、グループ内のすべてのサーバーの電力状態を変更できます。

[iLO Federation]→[Group Configuration]ページで、複数の iLO システムに対してグループメンバーシップを追加できます。

iLO システムのグループに対して、以下のタスクを実行できます。

- 既存のグループとメンバーは同じだが、権限が異なるグループを作成します。
- iLO 連携フィルターを使用して選択したメンバーを含むグループの作成

詳細情報

iLO 連携グループメンバーシップを追加する（複数の iLO システム）

iLO 連携グループの権限

iLO システムがグループに追加されると、グループに以下の権限を付与することができます。

- **[Login]** - グループのメンバーは iLO にログインできます。
- **[Remote Console]** - グループのメンバーは、ビデオ、キーボード、マウスの制御を含めて、ホストシステムのリモートコンソールにリモートにアクセスできます。
- **[Virtual Power and Reset]** - グループのメンバーは、ホストシステムの電源再投入やリセットを実行できます。
- **[Virtual Media]** - グループのメンバーは、ホストシステム上の仮想メディア機能を使用できます。
- **[Host BIOS]** - グループのメンバーは、システムユーティリティを使用してホスト BIOS 設定を構成できます。
- **[Configure iLO Settings]** - グループのメンバーは、セキュリティ設定を含むほとんどの iLO 設定を変更し、リモートに iLO ファームウェアを更新することができます。
- **[Administer User Accounts]** - グループのメンバーは、ユーザーがローカル iLO ユーザーアカウントを追加、編集、および削除できます。
- **[Host NIC]** - グループのメンバーは、ホストネットワークカード設定を構成できます。
- **[Host Storage]** - グループのメンバーは、ホストストレージ設定を構成できます。
- **[Recovery Set]** - グループのメンバーは、リカバリーインストールセットを管理できます。

iLO 連携グループの特性

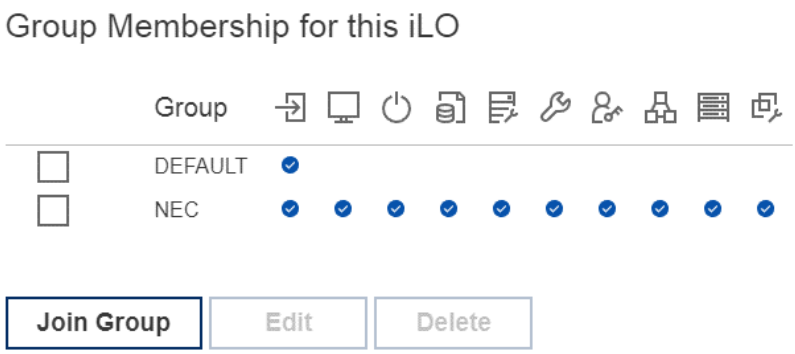
iLO 連携グループを使用すると、iLO システムは、同じグループ内の他の iLO システムへのメッセージを暗号化し署名することができます。

- すべての iLO システムは **[DEFAULT]** グループに自動的に追加され、このグループにはそれぞれのグループメンバーのログイン権限が認められています。**[DEFAULT]** グループメンバーシップは編集することも削除することもできます。
- iLO 連携グループは、一部共通することも、複数のラックおよびデータセンターにまたがることもできます。また、管理ドメインの作成に使用することもできます。
- iLO システムは最大で 10 の iLO 連携グループのメンバーとなることができます。
- グループの中にある iLO システムの数に制限はありません。
- グループメンバーシップを構成するには、iLO 設定権限が必要です。
- iLO Web インターフェースを使用して、ローカル iLO システムまたは iLO システムのグループに対してグループメンバーシップを構成することができます。
- iLO RESTful API を使用してグループメンバーシップを構成できます。
- 同じ iLO 連携グループ内の iLO システムには、同じバージョンの iLO ファームウェアをインストールしてください。

iLO 連携グループメンバーシップを表示する（ローカル iLO システム）

[iLO Federation]ページに移動します。

[Group Membership for this iLO]テーブルには、ローカル iLO システムごとに、ローカル iLO システムを含む各グループの名前とそのグループに与えられた権限が示されます。



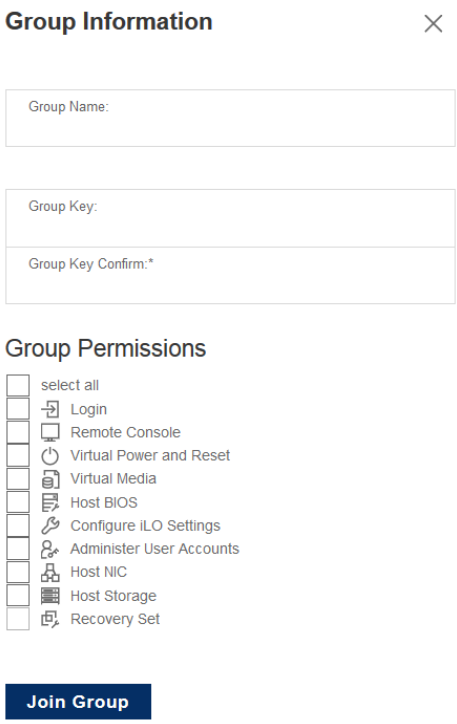
iLO 連携グループメンバーシップを追加する（ローカル iLO システム）

前提条件

iLO の設定を構成権限

手順

1. **[iLO Federation]**→**[Setup]**ページに移動します。
2. **[Join Group]**をクリックします。



3. **[Group Information]**セクションで、以下の情報を入力します。

- **[Group Name]** - グループ名は 1～31 文字で指定できます。先頭に空白文字は使用しないでください。
- **[Group Key]** - グループのパスワードは、設定されている最小パスワード長 ～31 文字で指定できます。

  記注：設定されている最小パスワード長未満の**[Group Key]**を使用しているがクループには参加できません。
- **[Group Key Confirm]** - グループのパスワードの確認。

既存のグループの名前とキーを入力すると、ローカル iLO システムがそのグループに追加されます。存在しないグループの名前とキーを入力すると、グループが作成され、ローカル iLO システムが新しいグループに追加されます。

4. **[Group Permissions]**セクションで、グループに付与する権限を入力します。

   ローカル iLO システムによりグループに付与される権限は、管理対象サーバーで、グループ内の他の iLO システムのユーザーが実行できるタスクを制御します。
5. **[Join Group]**をクリックします。

詳細情報

iLO 連携の設定
iLO 連携グループメンバーシップを追加する（複数の iLO システム）
iLO 連携グループ
アクセスオプション

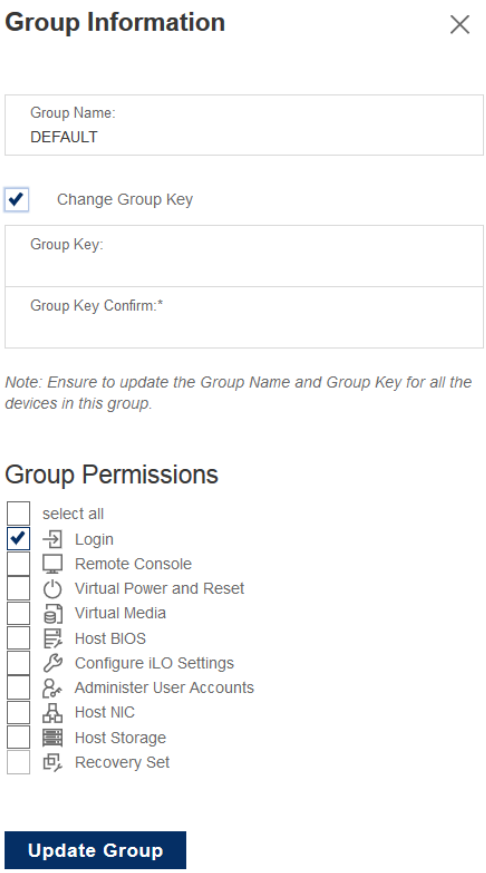
iLO 連携グループメンバーシップを編集する（ローカル iLO システム）

前提条件

iLO の設定を構成権限

手順

1. **[iLO Federation]**→**[Setup]**ページに移動します。
2. グループのメンバーシップを選択し、**[Edit]**をクリックすると編集ページが開きます。



3. グループ名を変更するには、**[Group Name]**ボックスに新しい名前を入力します。
   - グループ名は 1～31 文字で指定できます。先頭に空白文字は使用しないでください。
4. グループキーを変更するには、**[Change Group Key]**チェックボックスをクリックし、**[Group Key]**および **[Group Key Confirm]**ボックスに新しい値を入力します。
   グループキーは、設定されている最小パスワード長 ～31 文字で指定できます。
5. 更新する権限のチェックボックスをオンまたはオフにします。
   ローカル iLO システムによりグループに付与される権限は、管理対象サーバーで、グループ内の他の iLO システムのユーザーが実行できるタスクを制御します。
6. **[Update Group]**をクリックします。

詳細情報

iLO 連携の設定
iLO 連携グループ

iLO 連携グループからのローカル iLO システムの削除

前提条件

iLO の設定を構成権限

手順

1. **[iLO Federation]→[Setup]**ページに移動します。

2. 削除するグループメンバーシップの横にあるチェックボックスを選択します。
3. **[Delete]**をクリックします。
4. 要求を確認するメッセージが表示されたら、**[OK]** をクリックします。

iLO 連携グループメンバーシップを追加する（複数の iLO システム）

既存のグループに基づく、iLO 連携グループの追加

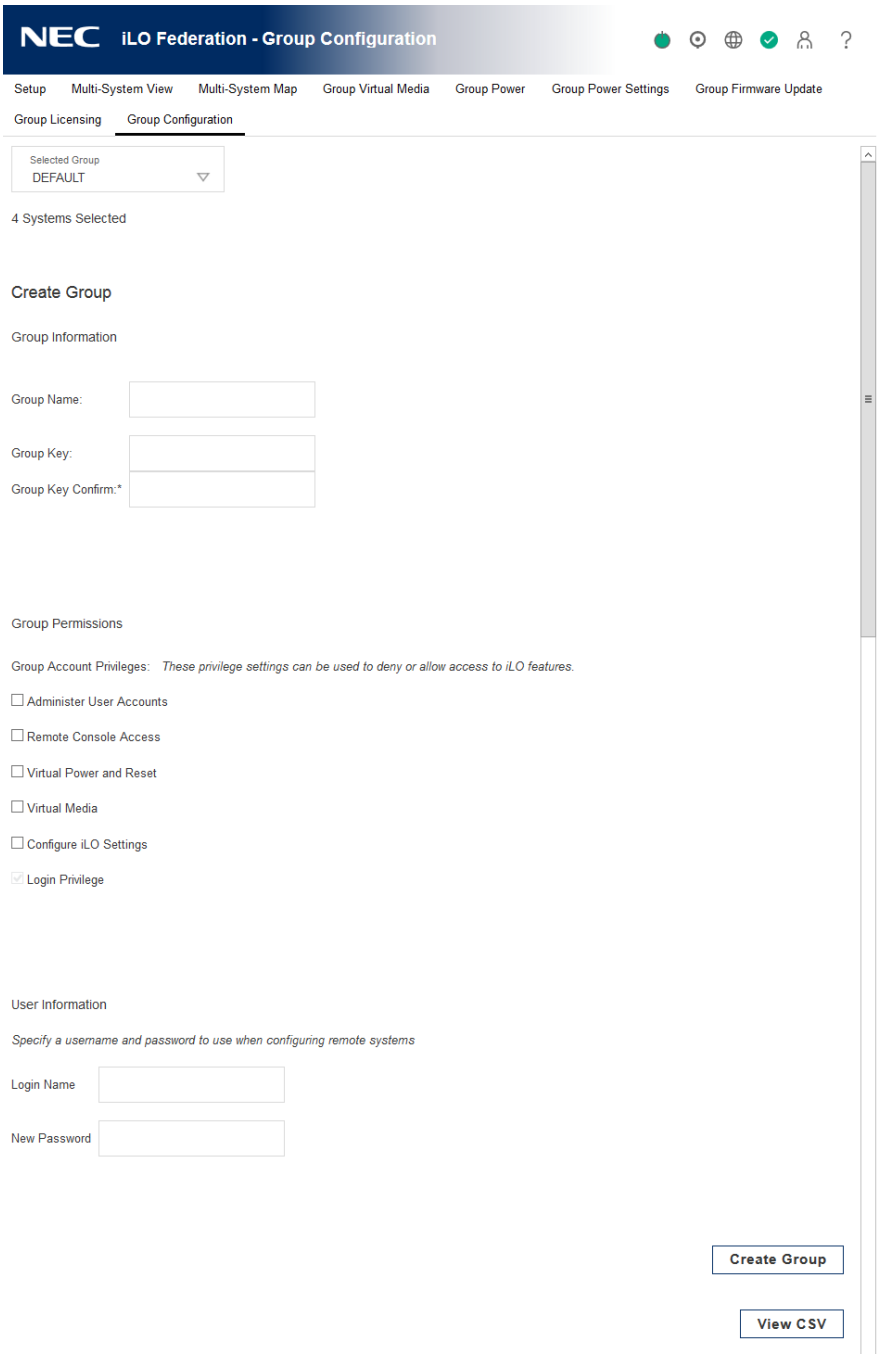
この手順を使用して、既存のグループと同じメンバーで構成される iLO 連携グループを作成します。たとえば、DEFAULT グループと同じシステムを含むが、権限を追加したグループを作成することをお勧めします。

前提条件

iLO の設定を構成権限

手順

1. **[iLO Federation]→[Group Configuration]**ページに移動します。



iLO 連携グループが存在しない場合、このページには、[There are no configured groups.]というメッセージが表示されます。**[iLO Federation]**→**[Setup]**ページを使用して、グループを作成します。

2. **[Selected Group]**メニューからグループを選択します。

   選択したグループ内のすべてのシステムが、このページで作成したグループに追加されます。

3. **[Group Information]**セクションで、次の情報を入力します。

   - **[Group Name]** - グループ名は 1～31 文字で指定できます。先頭に空白文字は使用しないでください。
   - **[Group Key]** - グループのパスワードは、3～31 文字で指定できます。
   - **[Group Key Confirm]** - グループのパスワードの確認。

既存のグループ名を入力すると、iLO から一意のグループ名の入力が求められます。

4. **[Group Permissions]**セクションで、グループに付与する権限を選択します。

   この手順では、グループのメンバーがグループの他のメンバーを構成するために所有する権限を定義します。

5. オプション：管理するリモートシステム上で、ユーザーアカウントの**[Login Name]**および**[New Password]**を入力します。

   選択したグループが、管理するリモートシステム上の iLO 設定権限を持っていない場合、この操作が必要です。

   複数のリモートシステムで認証情報を入力する必要がある場合は、ログイン名とパスワードが同じユーザーアカウントを各システムで作成できます。

6. **[Create Group]**をクリックします。

   グループの作成プロセスには数分かかります。グループは、**[**Multicast Announcement Interval (seconds/minutes)**]**に設定された時間内に検出し、構成します。

詳細情報

iLO 連携グループの権限
iLO 連携グループメンバーシップを追加する（ローカル iLO システム）
1 つの iLO システムのマルチキャストオプションを一度に構成する方法
アクセスオプション

フィルターされたサーバーのセットからのグループの作成

この手順を使用して、フィルターされたサーバーのリストから iLO 連携グループを作成します。たとえば、iLO 5 ファームウェアの特定のバージョンを備えているすべてのサーバーを含むグループを作成する場合があります。

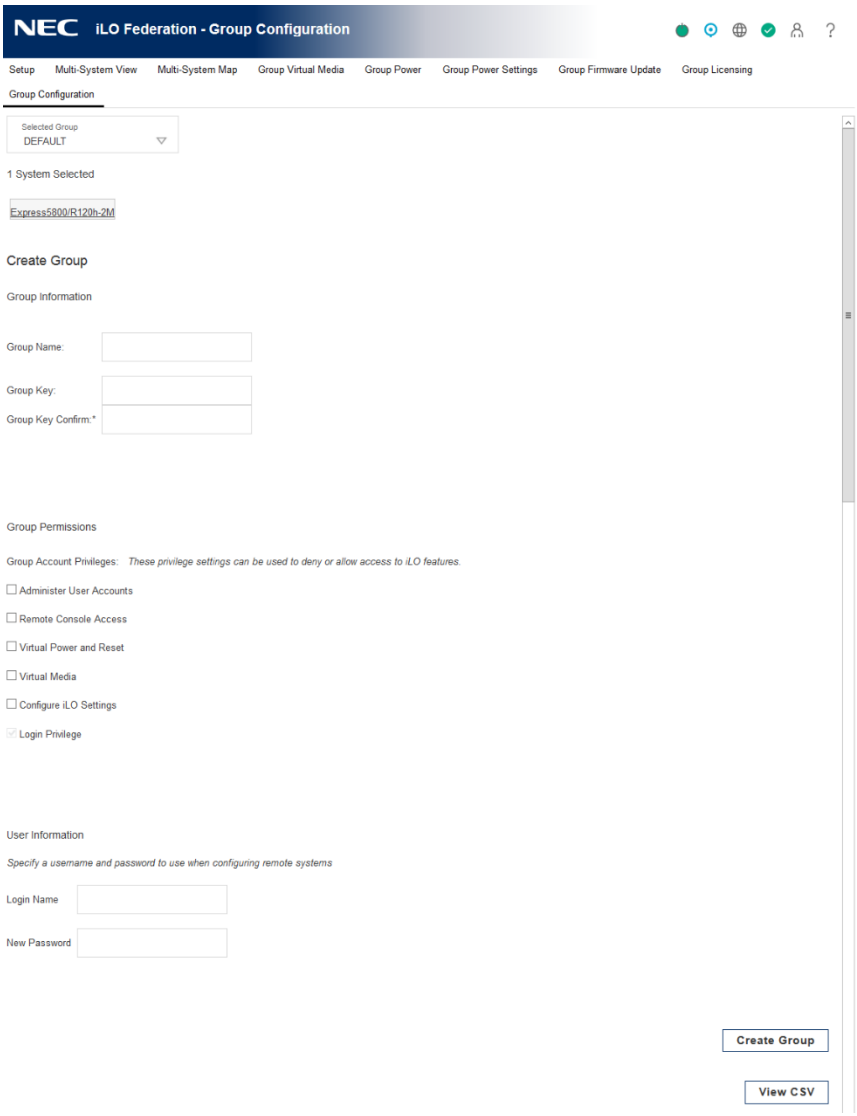
フィルターされたサーバーのリストからグループを作成すると、グループの作成時に **[**Affected Systems**]**リストに記載されているサーバーだけがグループに追加されます。グループの作成後に、フィルターの条件に適合するサーバーを構成しても、それらのサーバーはグループに追加されません。

前提条件

iLO の設定を構成権限

手順

1. **[iLO Federation]**関連のページで対象をクリックし、フィルターされたシステムのセットを作成します。
2. **[iLO Federation]**→**[Group Configuration]**ページに移動します。



iLO 連携グループが存在しない場合、[There are no configured groups.]というメッセージが表示されます。**[iLO Federation]→[Setup]**ページを使用して、グループを作成します。

3. **[Selected Group]**メニューからグループを選択します。

   選択したグループ内の、選択したフィルター条件に適合するすべてのシステムが、新しいグループに追加されます。

4. **[Group Information]**セクションで、次の情報を入力します。

   - **[Group Name]** - グループ名は 1～31 文字で指定できます。先頭に空白文字は使用しないでください。
   - **[Group Key]** - グループのパスワードは、3～31 文字で指定できます。
   - **[Group Key Confirm]** - グループのパスワードの確認。

5. **[Group Permissions]**セクションで、グループに付与する権限を選択します。

   この手順では、グループのメンバーがグループの他のメンバーを構成するために所有する権限を定義します。

6. オプション：管理するリモートシステム上で、ユーザーアカウントの **[Login Name]**および**[New Password]**を入力します。

選択したグループが、管理するリモートシステム上の iLO 設定権限を持っていない場合、この操作が必要です。

複数のリモートシステムで認証情報を入力する必要がある場合は、ログイン名とパスワードが同じユーザーアカウントを各システムで作成できます。

7. **[Create Group]**をクリックして設定を保存します。

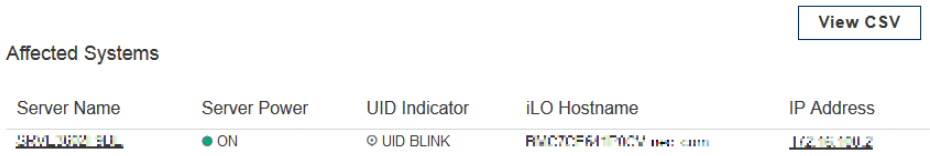
   グループの作成プロセスには数分かかります。グループは、**[Multicast Announcement Interval (seconds/minutes)]**に設定された時間内に検出し、構成します。

詳細情報

選択されたグループのリストのフィルター
iLO 連携グループメンバーシップを追加する（ローカル iLO システム）
iLO 連携グループの権限
アクセスオプション

グループメンバーシップの変更によって影響を受けるサーバー

[Group Configuration]ページの **[**Affected Systems**]**セクションには、グループメンバーシップの変更によって影響を受けるサーバーについて、次の詳細が表示されます。



- **[Server Name]** - ホストオペレーティングシステムで定義されたサーバー名。
- **[Server Power]** - サーバー電力の状態（**[ON]**または **[OFF]**）。
- **[UID Indicator]** - UID ランプの状態。UID ランプを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**[UID ON]**、**[UID OFF]**、および **[UID BLINK]**があります。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。**[iLO Hostname]** 列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。
- **[IP Address]** - iLO サブシステムのネットワーク IP アドレス。**[IP Address]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。

詳細情報

iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携機能の使用

選択されたグループのリスト

iLO 連携ページで**[Selected Group]**のリストからグループを選択した場合

- **[Group Virtual Media]**、**[Group Power]**、**[Group Firmware Update]**、**[Group Licensing]**、および **[Group Configuration]**ページでの変更の影響を受けるサーバーは、**[Affected Systems]**の表に表示されます。

- iLO 連携ページに表示される情報は、選択したグループ内のサーバーすべてに適用されます。
- iLO 連携ページで加えた変更は、選択したグループ内のサーバーすべてに適用されます。
- 選択されたグループは cookie に保存され、iLO からログアウトする場合でも、維持されます。

グループを選択した後、サーバーの情報を表示するため、またはグループ内のサーバーのサブセットに対して操作を実行するために、リスト内のサーバーをフィルター処理できます。

選択されたグループのリストのフィルター

サーバーのリストを選別する場合

- iLO 連携ページに表示される情報は、フィルター条件に適合する選択したグループ内のすべてのサーバーに適用されます。
- iLO 連携ページで加えた変更は、フィルター条件に適合する選択したグループ内のサーバーすべてに適用されます。
- フィルターの設定は cookie に保存され、iLO からログアウトする場合でも、維持されます。

選択されたグループのリストのフィルター条件

次の条件を使用して、グループ内のサーバーをフィルタリングすることができます。

- **[Health status]** - ヘルスステータスのリンクをクリックして、特定のヘルスステータスを持つサーバーを選択します。
- **[Model]** - サーバーのモデル番号リンクをクリックして、選択したモデルと一致するサーバーを選択します。
- **[Server name]** - 個々のサーバーによってフィルタリングするには、サーバー名をクリックします。
- **[Firmware Information]** - ファームウェアのバージョンまたはフラッシュステータスをクリックし、選択したファームウェアのバージョンまたはステータスに一致するサーバーを選択します。
- **[TPM** または **TM Option ROM Measuring]** - Option ROM Measuring のステータスをクリックして、選択した Option ROM Measuring のステータスに一致するサーバーを含めるか、除外します。
- **[License Usage]** - ライセンスキーに関連するエラーメッセージが表示される場合は、ライセンスキーをクリックして、そのライセンスキーを使用しているサーバーを選択します。
- **[License type]** - ライセンスタイプをクリックして、選択したライセンスタイプがインストールされているサーバーを選択します。

- **[License status]** - ライセンスステータスをクリックして、選択したステータスに一致するライセンスがインストールされているサーバーを選択します。

iLO 連携情報を CSV ファイルにエクスポートする方法

次の iLO 連携ページにて CSV ファイルにエクスポートすることができます。

- Multi-System View
- Multi-System Map
- Group Virtual Media
- Group Power
- Group Firmware Update
- Group Configuration

Group Power Settings のページは、エクスポートをサポートしていません。

手順

1. **iLO Federation** メニュー内のファイルエクスポート機能をサポートするページに移動します。
2. **[View CSV]**をクリックします。
3. **[CSV Output]**ウィンドウで、**[Save]**をクリックしてから、ブラウザーのプロンプトに従ってファイルを保存または開きます。

   リストをエクスポートする場合、CSV ファイルには iLO 連携ページに表示されているサーバーだけが含まれます。

   サーバーが複数のページにまたがってリストされている場合、CSV ファイルには iLO Web インターフェースページに現在表示されているサーバーだけが含まれます。

   クエリのエラーが発生した場合、クエリに応答しなかったシステムは、iLO Web インターフェースページおよび CSV ファイルから除外されます。

iLO 連携情報のエクスポートオプション

次の情報を **iLO** 連携ページからエクスポートできます。

- **クリティカル**または**劣化**のステータスのシステム - Multi-System View ページから、このリストをエクスポートします。
- iLO ピアのリスト - Multi-System Map ページから、このリストをエクスポートします。
- 影響するシステムリスト - 次のページでの iLO 連携操作によって影響を受けたシステムのリストをエクスポートします。
  - Group Virtual Media
  - Group Power
  - Group Firmware Update
  - Group Configuration

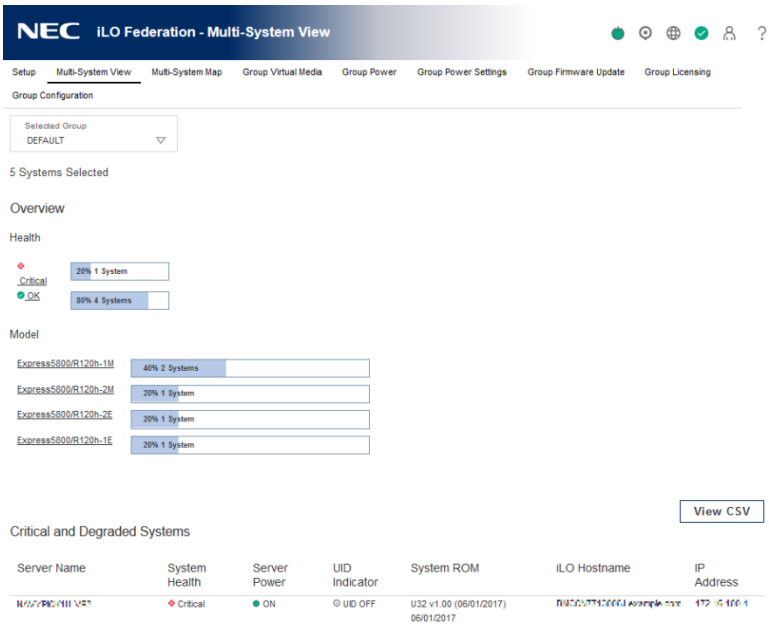
エクスポート機能は、**Group Power Settings** ページではサポートされていません。

iLO 連携マルチシステムビュー

Multi-System View ページは、iLO 連携グループ内のサーバーモデル、サーバーのヘルス、およびクリティカルおよび劣化したサーバーに関する概要を提供します。

サーバーのヘルス情報とモデル情報の表示

1. **[iLO Federation]→[Multi-System View]**ページに移動します。



2. **[Selected Group]**メニューからグループを選択します。
3. オプション：サーバーのリストをフィルタリングするには、ヘルスステータス、サーバーモデル、またはサーバー名のリンクをクリックします。

サーバーヘルスおよびモデルの詳細

- **[Health]** - 表示された各ヘルスステータスにあるサーバーの数。一覧表示された各ヘルスステータス内のサーバーの総数の割合（%）も表示されます。
- **[Model]** - モデル番号でグループ化したサーバーのリスト。各モデル番号に対するサーバー総数の割合（%）も表示されます。
- **[Critical and Degraded Systems]** - ステータスがクリティカルまたは劣化であるサーバーのリスト。

詳細情報

ヘルスサマリー情報の表示

クリティカルおよび劣化のステータスを持つサーバーの表示

1. **[iLO Federation]→[Multi-System View]**ページに移動します。
2. **[Selected Group]**メニューからグループを選択します。
3. オプション：サーバーのリストをフィルタリングするには、ヘルスステータス、サーバーモデル、またはサーバー名のリンクをクリックします。

4. **[Next]**または**[Previous]**（使用できる場合）をクリックして、クリティカルおよび劣化システムのリストのサーバーをさらに表示します。

クリティカルおよび劣化のサーバーステータスの詳細

- **[Server Name]** - ホストオペレーティングシステムで定義されたサーバー名。
- **[System Health]** - サーバーのヘルスステータス。
- **[Server Power]** - サーバーの電力ステータス（**[ON]**または**[OFF]**）。
- **[UID Indicator]** - サーバー UID ランプの状態。UID ランプを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**[UID ON]**、**[UID OFF]**、および**[UID BLINK]**があります。
- **[System ROM]** - インストールされているシステム ROM バージョン。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。**[iLO Hostname]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。
- **[IP Address]** - iLO サブシステムのネットワーク IP アドレス。**[IP Address]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。

詳細情報

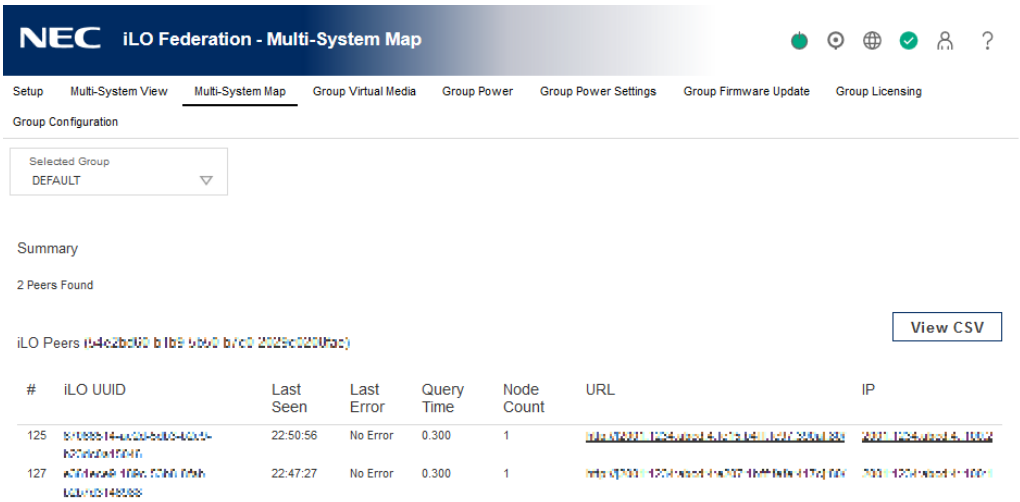
iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携マルチシステムマップの表示

Multi-System Map ページには、ローカル iLO システムのピアに関する情報が表示されます。ローカル iLO システムはマルチキャスト検出を使用してそのピアを識別します。

iLO 連携ページ上のデータがロードされると、Web インターフェースを実行する iLO システムから iLO システムのピア、およびそれらのピアから他のピア、選択した iLO 連携グループのすべてのデータが取得されるまでデータのリクエストが送信されます。

1. **[iLO Federation]→[Multi-System Map]**ページに移動します。



2. **[Selected Group]**メニューからグループを選択します。

iLO ピアの詳細

- **[#]** - ピア番号。
- **[iLO UUID]** - iLO の UPnP UUID。
- **[Last Seen]** - サーバーからの前回の通信のタイムスタンプ。
- **[Last Error]** - 表示されているピアとローカルの iLO システムの間での最新の通信エラーの説明。
- **[URL]** - 表示されているピアの iLO Web インターフェースを起動するための URL。
- **[IP]** - ピアの IP アドレス。

詳細情報

iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携グループ仮想メディア

グループ仮想メディアを使用すると、iLO 連携グループ内のサーバーからアクセスできるスクリプト方式のメディアに接続できます。

- スクリプト方式のメディアは、1.44MB のフロッピーディスクイメージ（IMG）および CD/DVD-ROM イメージ（ISO）のみをサポートします。イメージは、グループ化された iLO システムと同じネットワーク上の Web サーバーに存在する必要があります。
- 同時に 1 種類のメディアしかグループに接続できません。
- スクリプト方式のメディアの表示、接続、取り出しのほか、このメディアからの起動を行えます。スクリプト方式のメディアを使用する場合は、ディスケットや CD/DVD-ROM のディスクイメージを Web サーバーに保存し、URL を使用してそのディスクイメージに接続します。iLO では HTTP または HTTPS 形式の URL を使用できます。iLO は FTP をサポートしていません。
- 仮想メディア機能を使用する前に、仮想メディアオペレーティングシステムに関する注意事項を確認してください。

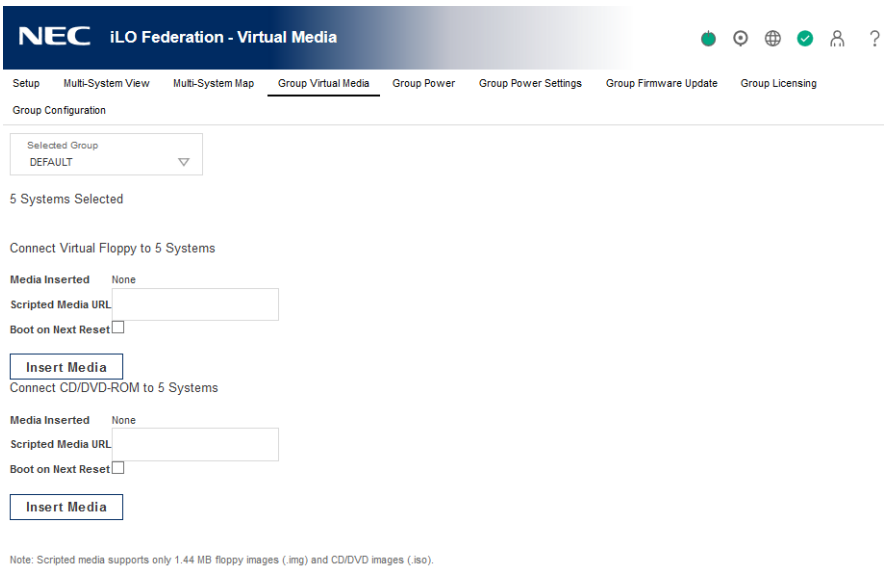
グループのスクリプト方式のメディアの接続

前提条件

- この機能をサポートする iLO ライセンスがインストールされている。
- 選択した iLO 連携グループの各メンバーが、仮想メディア権限をグループに認めている。

手順

1. **[iLO Federation]→[Group Virtual Media]**ページに移動します。



2. **[Selected Group]**メニューからグループを選択します。

   接続するスクリプト方式のメディアは、選択したグループ内のすべてのシステムで利用可能になります。

3. **[Connect Virtual Floppy]**セクション（IMG ファイル）または**[Connect CD/DVD-ROM]**セクション（ISO ファイル）の**[Scripted Media URL]** ボックスにスクリプト方式のメディアディスクイメージの URL を入力します。
4. 次のサーバー再起動時のみにこのディスクイメージからグループ内のサーバーを起動する必要がある場合は、**[Boot on Next Reset]**チェックボックスを選択します。

   ディスクイメージは 2 回目のサーバー再起動時に自動的に取り出されるので、サーバーは一度しかこのイメージから起動しません。

   このチェックボックスを選択しない場合、ディスクイメージは手動で取り出すまで接続されたまま残ります。また、サーバーは、システムブートオプションがそのように構成されている場合、以後のすべてのサーバーリセットでイメージから起動します。

   [Boot on Next Reset]チェックボックスを使用している場合に、グループ内のサーバーが POST を実行していると、POST の実行時にサーバーのブート順序を変更できないためにエラーが発生します。POST が終了するのを待ってから、再試行してください。
5. **[Insert Media]**をクリックします。

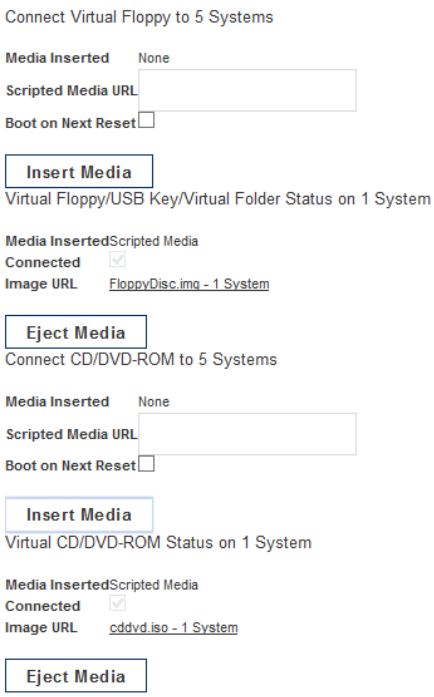
   iLO はコマンドの結果を表示します。

グループのスクリプト方式のメディアの表示

[iLO Federation]→**[Group Virtual Media]**ページに移動します。

スクリプト方式のメディアの詳細

スクリプト方式のメディアが iLO 連携グループ内のシステムに接続している場合、**[Virtual Floppy/USB Key/Virtual Folder Status]**セクションと**[Virtual CD/DVD-ROM Status]**セクションに、次の詳細が示されます。



- **[Media Inserted]** - 接続されている仮想メディアの種類。スクリプト方式のメディアが接続されている場合、**[Scripted Media]**と表示されます。
- **[Connected]** - 仮想メディアデバイスが接続されているかどうかを示します。

- **[Image URL]** - 接続されているスクリプト方式のメディアのファイル名。

スクリプト方式のメディアデバイスの取り出し

前提条件

- この機能をサポートする iLO ライセンスがインストールされている。
- 選択した iLO 連携グループの各メンバーが、仮想メディア権限をグループに認めている。

手順

1. **[iLO Federation]**→**[Group Virtual Media]**ページに移動します。
2. **[Selected Group]**メニューからグループを選択します。

   取り出すスクリプト方式のメディアデバイスは、選択したグループ内のすべてのシステムから切断されます。
3. **[Virtual Floppy/USB Key/Virtual Folder Status]**セクションまたは**[Virtual CD/DVD-ROM Status]**セクションの**[Eject Media]**をクリックします。

グループ仮想メディアの操作の影響を受けるサーバー

[Affected Systems]セクションには、**[Group Virtual Media]**ページで行った変更によって影響を受けるサーバーについて、次の詳細が表示されます。

- **[Server Name]** - ホストオペレーティングシステムで定義されたサーバー名。
- **[Server Power]** - サーバーの電力ステータス（**[ON]**または**[OFF]**）。
- **[UID Indicator]** - サーバー UID ランプの状態。UID ランプを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**[UID ON]**、**[UID OFF]**、および**[UID BLINK]**があります。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。**[iLO Hostname]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。
- **[IP Address]** - iLO サブシステムのネットワーク IP アドレス。**[IP Address]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。

[Next]または**[Previous]**（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳細情報

iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携グループ電力

グループの電力機能では、iLO Web インターフェースを実行するシステムから、複数のサーバーの電力を管理することができます。この機能を使用して、以下を行います。

- **[ON]**または**[RESET]**状態にあるサーバーのグループに対して、電源を切る、リセットする、または電源再投入を行う。
- **[OFF]**状態にあるサーバーのグループに対して電源を入れる。
- **Group Power** ページの**[Virtual Power Button]**セクションでボタンをクリックすると影響を受けるサーバーのリストを表示する。

サーバーグループの電力状態の変更

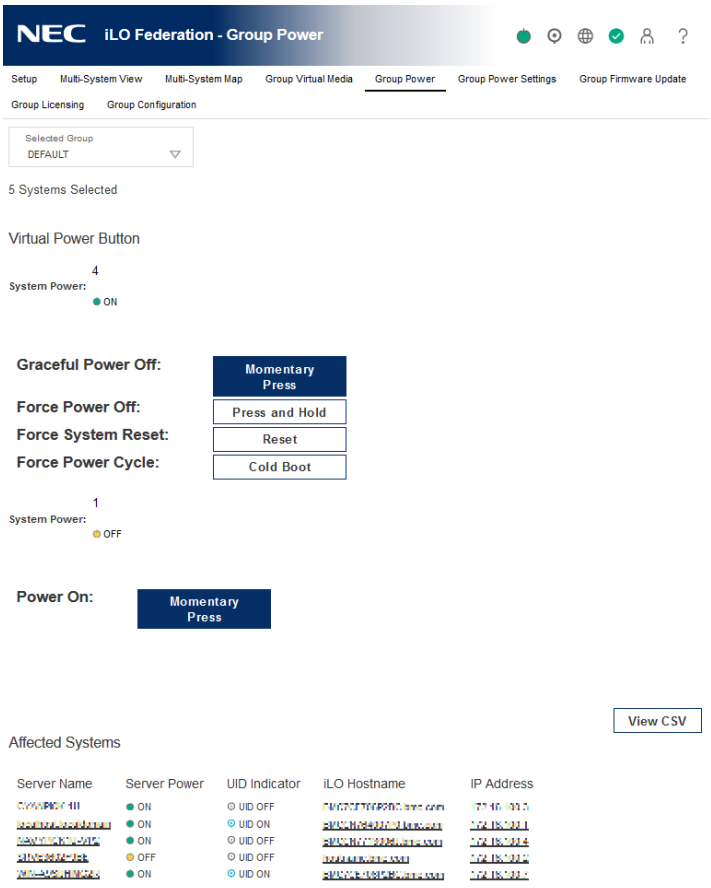
グループ電力ページの**[Virtual Power Button]**セクションには、**[ON]**、**[OFF]**、または**[RESET]**の状態にあるサーバーの総数など、グループサーバーの現在の電力状態の概要が表示されます。システム電源のサマリーは、ページが初めて開かれるときの、サーバーの電源の状態を示します。ブラウザーの更新機能を使用して、システム電源情報を更新します。

前提条件

- この機能をサポートする iLO ライセンスがインストールされている。
- 選択した iLO 連携グループの各メンバーが、仮想電源およびリセット権限をグループに認めている。

手順

1. **[iLO Federation]**→**[Group Power]**ページに移動します。



2. **[Selected Group]**メニューからグループを選択します。

   グループ化されたサーバーは電源ステータス順に表示され、各状態にあるサーバーの合計数を示すカウンターも表示されます。
3. サーバーのグループの電力状態を変更するには、次のいずれかを実行します。
   - **[ON]**または**[RESET]**状態にあるサーバーの場合は、次のいずれかのボタンをクリックします。
     - **[Momentary Press]**
     - **[Press and Hold]**
     - **[Reset]**
     - **[Cold Boot]**
   - **[OFF]**状態にあるサーバーの場合は、**[Momentary Press]**ボタンをクリックします。

     [OFF]状態にあるサーバーでは、**[Press and Hold]**、**[Reset]**、および**[Cold Boot]**オプションは使用できません。

     iLO 5 Firmware Version 1.10 Jun 07 2017 では、**[OFF]**状態にあるサーバーの場合も Graceful Power Off と表示されますが、**[Momentary Press]**ボタンをクリックすることで電源オンします。
4. 要求を確認するメッセージが表示されたら、**[OK]**をクリックします。

仮想電源ボタンの作動に対してグループ化されたサーバーが応答する間、iLO には進行状況バーが表示されます。進行状況バーには、コマンドの実行に成功したサーバーの数が示されます。**[Command Results]**セクションには、電源状態の変更に関連したエラーメッセージなど、コマンドのステータスおよび結果が表示されます。

仮想電源ボタンのオプション

- **[Momentary Press]** - 物理的な電源ボタンを押す場合と同じです。

  一部のオペレーティングシステムでは、電源ボタンを一時的に押した後、適切なシャットダウンを開始するか、またはこのイベントを無視するように設定されていることがあります。仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して適切なオペレーティングシステムシャットダウンを完了することをおすすめします。

- **[Press and Hold]** - 物理的な電源ボタンを 5 秒間押し続け、離すことと同じです。

  この操作の結果、選択したグループ内のサーバーの電源がオフになります。このオプションを使用すると、適切なオペレーティングシステムの終了に影響する場合があります。

- **[Reset]** - 選択したグループ内のサーバーを強制的にウォームブートします。
  CPU および I/O リソースがリセットされます。このオプションを使用すると、適切なオペレーティングシステムの終了に影響します。

- **[Cold Boot]** - 選択したグループ内のサーバーの電源をただちに切断します。プロセッサー、メモリ、および I/O リソースは、メインの電力が失われます。サーバーは、約 6 秒後に再起動します。このオプションを使用すると、適切なオペレーティングシステムの終了に影響します。

仮想電源ボタンによって影響を受けるサーバー

[Affected Systems]リストには、仮想電源ボタンの作動によって影響を受けるサーバーについて、次の詳細が示されます。

[Affected Systems]セクションには、**[Group Power]**ページで行った変更によって影響を受けるサーバーについて、次の詳細が表示されます。

- **[Server Name]** - ホストオペレーティングシステムで定義されたサーバー名。
- **[Server Power]** - サーバーの電力ステータス（**[ON]**または**[OFF]**）。
- **[UID Indicator]** - サーバー UID ランプの状態。UID ランプを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**[UID ON]**、**[UID OFF]**、および**[UID BLINK]**があります。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。**[iLO Hostname]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。
- **[IP Address]** - iLO サブシステムのネットワーク IP アドレス。**[IP Address]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。

[Next]または**[Previous]**（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳細情報

iLO 連携情報を CSV ファイルにエクスポートする方法

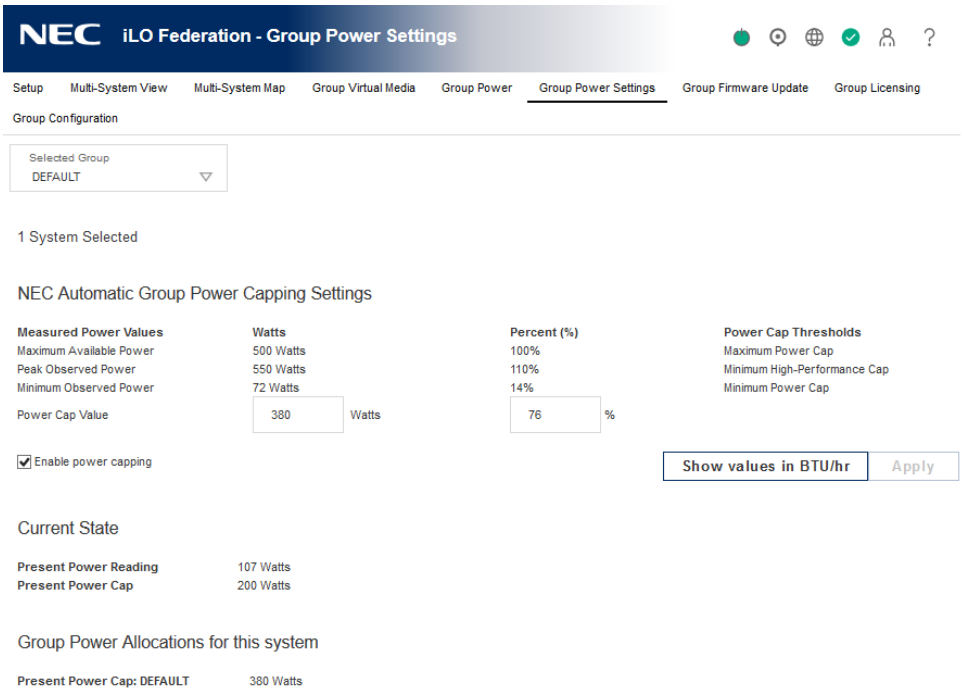
グループ消費電力上限の構成

前提条件

- この機能をサポートする iLO ライセンスがインストールされている。
- 選択した iLO 連携グループの各メンバーが、iLO 設定権限をグループに認めている。

手順

1. **[iLO Federation]→[Group Power Settings]**ページに移動します。



2. **[Selected Group]**メニューからグループを選択します。

   選択したグループ内のすべてのシステムは、このページで加えた変更の影響を受けます。
3. **[Enable power capping]**チェックボックスを選択します。
4. **[Power Cap Value]**をワット数、BTU/時、または割合（%）で入力します。

   割合（%）は、最大電力値と最小電力値の差です。消費電力上限値は、サーバーの最小電力値以下に設定できません。

   値がワット単位で表示されている場合、BTU/時単位での表示に変更するには**[Show Values in BTU/hr]**をクリックします。値が BTU/時で表示されている場合、ワット単位での表示に変更するには**[Show Values in Watts]**をクリックします。
5. **[Apply]**をクリックします。

消費電力上限の注意事項

グループ電力設定機能では、iLO Web インターフェースを実行するシステムから、複数のサーバーの消費電力上限を動的に設定することができます。

- グループ消費電力上限を設定している場合、グループ化されたサーバーは、消費電力上限を超えないように電力を節約します。電力はビジー状態のサーバーにより多く割り当てられ、アイドル状態のサーバーにはより少ない電力が割り当てられます。

- グループに対して設定した消費電力上限は、個々のサーバーの **Power Settings** ページで設定できる消費電力上限とともに動作します。
- サーバーがエンクロージャーまたは個々のサーバーレベルで構成されている消費電力上限や別の iLO 連携グループの影響を受ける場合は、他のグループの消費電力上限によりそのサーバーに割り当てられる電力が少なくなる可能性があります。
- 消費電力上限が設定されている場合、グループ化されたサーバーの平均電力測定値は、消費電力上限値以下である必要があります。
- POST 実行中、ROM は最大電力測定値と最小電力測定値を決定する 2 つの電力テストを実行します。

  消費電力上限の設定を決定するときは、**[Automatic Group Power Capping Settings]**の表の値を考慮してください。

- **[Maximum Available Power]** - グループ内のすべてのサーバーの総電源容量。これは、**[Maximum Power Cap]**のしきい値です。グループ内のサーバーはこの値を超えてはいけません。
- **[Peak Observed Power]** - グループ内のすべてのサーバーの最大電力測定値。これは、**[Minimum High-Performance Cap]**のしきい値で、現在の構成でグループ内のサーバーが使用する最大電力を表します。この値に設定されている消費電力上限は、サーバーのパフォーマンスに影響を与えません。
- **[Minimum Observed Power]** - グループ内のすべてのサーバーの最小電力測定値。これは、**[Minimum Power Cap]**のしきい値で、グループ内のサーバーが使用する最小電力を表します。この値に設定されている消費電力上限は、サーバーの電力使用量を最小化するため、その結果サーバーのパフォーマンスが低下します。

グループ消費電力上限情報の表示

前提条件

この機能をサポートする iLO ライセンスがインストールされている。

手順

1. **[iLO Federation]→[Group Power Settings]** ページに移動します。
2. **[Selected Group]**メニューからグループを選択します。
3. オプション：値がワット単位で表示されている場合、BTU/時単位での表示に変更するには**[Show Values in BTU/hr]**をクリックします。値が BTU/時で表示されている場合、ワット単位での表示に変更するには**[Show Values in Watts]**をクリックします。

消費電力上限の詳細

- **Automatic Group Power Capping Settings** セクションには、以下の詳細が表示されます。
  - **[Measured Power Values]** - 最大利用可能電力、サーバー最大電力、およびサーバー最小電力。
  - **[Power Cap Value]** - 電力消費上限値（設定されている場合）。
- **Current State** セクションには、以下の詳細が表示されます。

- **[Present Power Reading]** - 選択されたグループの現在の電力読み取り値。
- **[Present Power Cap]** - 選択したグループに割り当てられている電力の合計量。消費電力上限が設定されていない場合、この値はゼロです。

- **Group Power Allocations for this system** セクションには、ローカル iLO システムに影響を及ぼすグループ消費電力上限と、各グループ消費電力上限によってローカル iLO システムに割り当てられる電力の量。消費電力上限が設定されていない場合、割り当て電力値はゼロです。

iLO 連携グループファームウェアアップデート

グループファームウェアアップデート機能では、ファームウェア情報を表示し、1 つの iLO Web インターフェースを実行するシステムから、複数のサーバーのファームウェアを更新することができます。次のファームウェアタイプが iLO 連携でサポートされています。

- iLO ファームウェア
- システム ROM（BIOS）
- シャーシファームウェア（パワーマネージメント）
- パワーマネージメントコントローラー
- システムプログラマブルロジックデバイス（CPLD）
- NVMe バックプレーンファームウェア
- 言語パック

複数のサーバーのファームウェアの更新

前提条件

- 選択した iLO 連携グループの各メンバーが、iLO 設定権限をグループに認めている。
- この機能をサポートする iLO ライセンスがインストールされている。

手順

1. サポートされているファームウェアを NX7700x シリーズポータルサイト（https://jpn.nec.com/nx7700x/index.html）からダウンロードします。
2. ファームウェアのファイルを Web サーバーにアップロードします。
3. **[iLO Federation]→[Group Firmware Update]**ページに移動します。
4. **[Selected Group]**メニューからグループを選択します。

   このページでファームウェアアップデートを開始すると、選択したグループ内のすべてのシステムが影響を受けます。
5. 省略可能：ファームウェアのバージョン、フラッシュステータス、または**[TPM or TM Option ROM Measuring]**ステータスリンクをクリックして、影響を受けるシステムのリストをフィルタリングします。

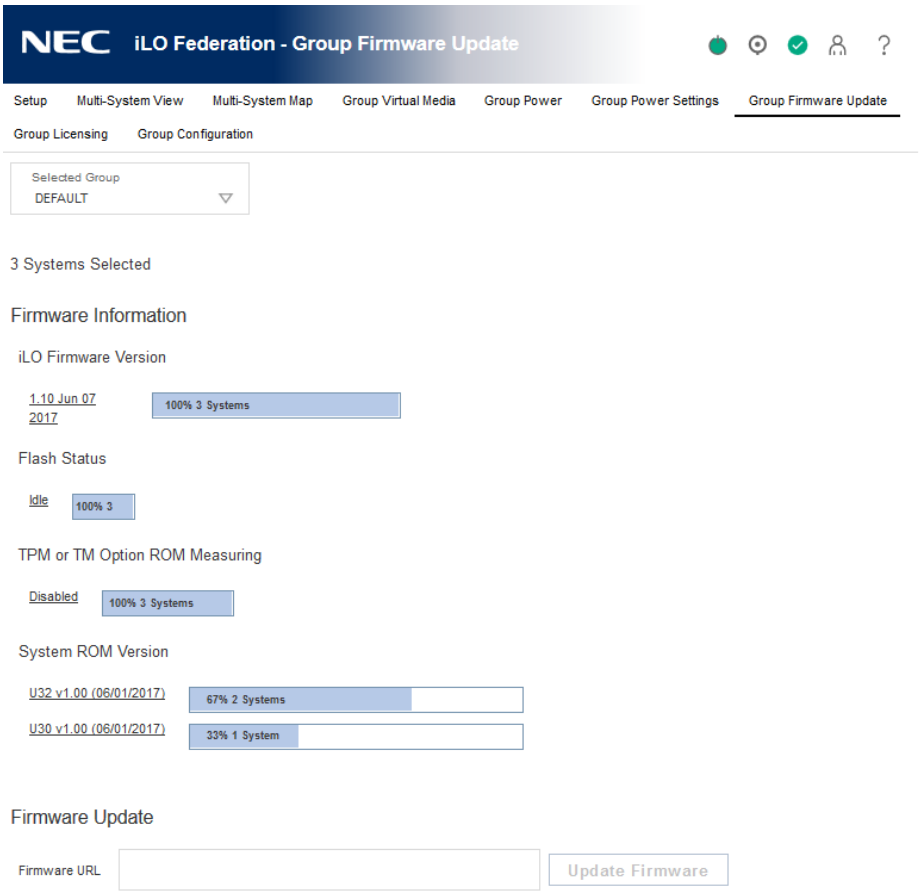
△ 注意: **[Option ROM Measuring]**を有効にしてサーバーでシステム ROM やオプション ROM のアップデートを実行すると、iLO は、更新前に更新をキャンセルし、リカバリーキーがあ

ることを確認し、BitLocker を一時停止するよう求めます。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。

6. **[Firmware Update]**セクションで、Web サーバー上のファームウェアファイルの URL を入力して、**[Firmware Update]**ボタンをクリックします。

   選択した各システムがファームウェアイメージをダウンロードし、それをフラッシュしようと試みます。

   [Flash Status]セクションが更新され、iLO はアップデートが進行中であることを通知します。更新が完了したら、**[Firmware Information]**セクションが更新されます。ファームウェアイメージがシステムに対して無効か、署名が不適切またはない場合、iLO はイメージを拒否し、**[Flash Status]**セクションに影響を受けるシステムのエラーを表示します。



   ファームウェアアップデートの種類によっては、新しいファームウェアを有効にするために、システムのリセット、iLO のリセット、またはサーバーの再起動が必要になる場合があります。

詳細情報

iLO ファームウェアイメージファイルの入手

グループファームウェア情報の表示

1. **[iLO Federation]**→**[Group Firmware Update]**ページに移動します。
2. **[Selected Group]**メニューからグループを選択します。

ファームウェアの詳細

[Firmware Information]セクションには、以下の情報が表示されます。

- サポート対象の各ファームウェアバージョンのサーバー数。リストされているファームウェアのバージョンを搭載するサーバーの総数の割合（%）も表示されます。
- グループ化されたサーバーのフラッシュステータス。リストされたフラッシュのステータスにあるサーバーの総数の割合（%）も表示されます。
- グループ化されたサーバーの**[TPM or TM Option ROM Measuring]**ステータス。表示された**Option ROM Measuring** ステータスにあるサーバーの総数の割合（%）も表示されます。

グループのファームウェアアップデートの影響を受けるサーバー

[Affected Systems]リストには、ファームウェアアップデートによって影響を受けるサーバーについて、次の詳細が示されます。

- **[Server Name]** - ホストオペレーティングシステムで定義されたサーバー名。
- **[System ROM]** - インストールされているシステム ROM（BIOS）。
- **[iLO Firmware Version]** - インストールされている iLO ファームウェアバージョン。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。**[iLO Hostname]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。
- **[IP Address]** - iLO サブシステムのネットワーク IP アドレス。**[IP Address]**列のリンクをクリックすると、サーバーの iLO Web インターフェースが開きます。

詳細情報

iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携グループライセンス

重要:　本機能は使用しないでください。

iLO 連携グループ構成機能

[iLO Federation]→**[Group Configuration]**ページの機能の使用法については、「iLO 連携グループメンバーシップを追加する（複数の iLO システム）」を参照してください。

8. iLO 統合リモートコンソール

iLO 統合リモートコンソールは、ホストサーバーのディスプレイ、キーボード、およびマウスを制御するために使用できるグラフィックリモートコンソールです。統合リモートコンソールを使用すると、リモートファイルシステムやネットワークドライブにアクセスできます。統合リモートコンソールアクセスを使用すれば、リモートのホストサーバーが再起動するときの POST ブートメッセージを確認することができ、また ROM ベースのセットアップルーチンを起動してリモートのホストサーバーのハードウェアを設定することができます。オペレーティングシステムをリモートでインストールする場合、統合リモートコンソールにより（使用許諾されている場合）、インストール作業の全体をホストサーバーの画面に表示して、制御することができます。

統合リモートコンソールのアクセスオプション

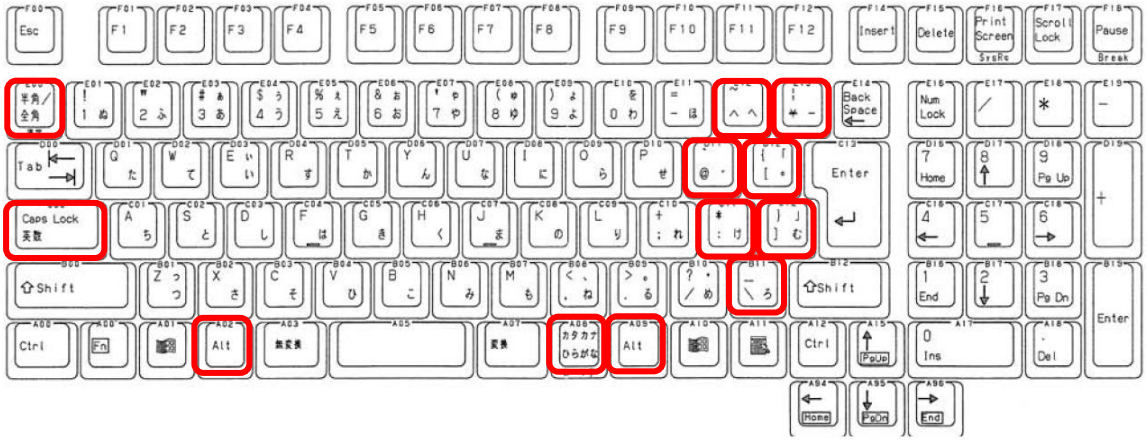
- **[.NET IRC]** - Windows ライアント上でサポートされるブラウザーを介して単一コンソールから仮想電源や仮想メディアを制御できるように、システムKVMへのアクセスを提供します。標準機能に加えて、.NET IRC は、コンソールの取得、共有コンソール、仮想フォルダー、およびスクリプト方式のメディアをサポートします。
- **[Java Web Start and Java Applet]** - システム KVM へのアクセスを提供して、仮想電源と仮想メディアの制御を可能にします。標準機能に加えて、Java IRC には iLO ディスクイメージツールとスクリプト方式のメディアが含まれます。
- **[HTML5 IRC]** - システム KVM へのアクセスを提供します。HTML5 に対応し iLO がサポートしている Web ブラウザーをご使用であれば、OS を問わずに使用可能です。HTML5 IRC は iLO 5 Firmware Version 1.20 Feb 02 2018 以降でサポートしています。

統合リモートコンソールの使用に関する情報とヒント

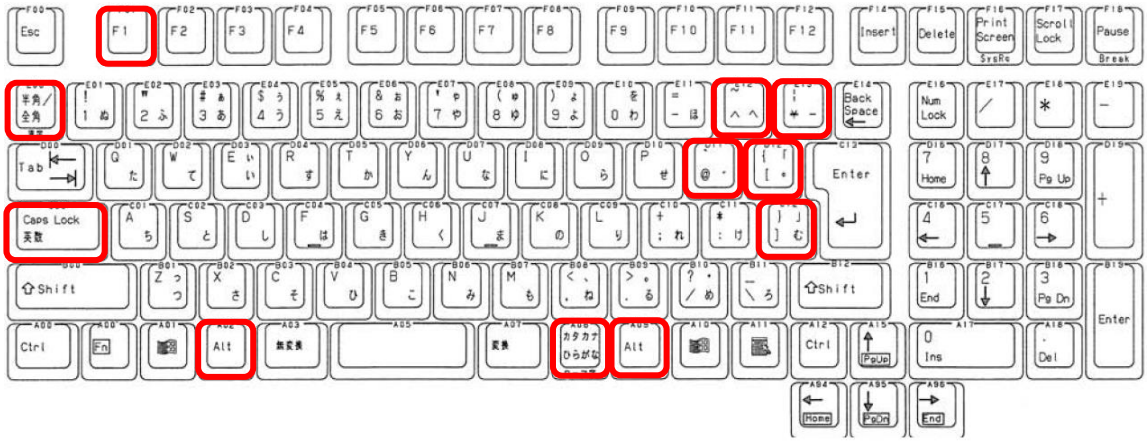
- リモートコンソール権限を持つユーザーが、.NET IRC、Java IRC および HTML5 IRC を使用できます。
- OS の起動後に統合リモートコンソールを使用するには、リモートマネージメント拡張ライセンス(Advanced)またはリモートマネージメント拡張ライセンス(Essentials)をインストールする必要があります。ライセンスがインストールされているかどうかを確認するには、**[Administration]→[Licensing]**の順に選択してください。なお、NX7700x シリーズサーバは、工場出荷時に標準でリモートマネージメント拡張ライセンス(Advanced)をインストール済みです。
- Oracle Java ランタイム環境で Windows または Linux を使用する場合、Java IRC は、iLO Web インターフェースから起動される Java Web Start アプリケーションであり、Web ブラウザーの外部にある別のウィンドウで実行されます。起動時に空白のセカンダリーウィンドウが開きます。Java IRC がロードされた後は、このウィンドウを閉じないでください。
- OpenJDK Java ランタイム環境で Linux を使用する場合、Java IRC は、iLO Web インターフェースから起動される Java アプレットであり、別のウィンドウで実行されます。
- OpenJDK での Java IRC のみ：iLO の Web インターフェースィンドウを更新するか閉じると、統合リモートコンソール接続も終了し、URL（スクリプト方式のメディアの使用）で接続されていたデバイスを除き、Java IRC で接続されていた仮想メディアデバイスにアクセスできなくなります。

- iLO プロセッサーを搭載しているサーバー上のホストオペレーティングシステムから統合リモートコンソールを実行しないでください。
- 統合リモートコンソールを通じてサーバーにログインした場合、コンソールを閉じる前にサーバーからログアウトすることをおすすめします。
- ポップアップブロッカーは.NET IRC や Java IRC アプレットの実行を妨げます。このため、統合リモートコンソールのセッションを開始する前にポップアップブロッカーを無効にする必要があります。場合によっては、**Ctrl キー**を押したまま、リモートコンソール起動ボタンをクリックすることでポップアップブロックをバイパスできることがあります。これは、Java IRC Web Start アプリケーションには適用されません。
- ブラウザーによっては、Java プラグインをサポートしないものがあります。代わりに以下の方法を使用できます。
    - Windows ユーザー：Java IRC の Java Web Start アプリケーションを使用します。
    - Oracle JRE を使用する Linux ユーザー：Java IRC の Java Web Start アプリケーションを使用します。
    - OpenJDK JRE を使用する Linux ユーザー：Java IRC アプレットを使用します。
- 統合リモートコンソールセッションがアクティブの場合、UID ランプが点滅します。
- 統合リモートコンソールの使用が完了したら、ウィンドウを閉じるか、ブラウザーの閉じるボタン（X）をクリックして終了します。
- **[Idle Connection Timeout]**では、ユーザーの操作がないまま経過し、統合リモートコンソールセッションが自動的に終了するまでの時間を指定します。仮想メディアデバイスが接続されている場合、統合リモートコンソールセッションはこの値の影響を受けません。**[Idle Connection Timeout]**について詳しくは、「iLO アクセスの設定」を参照してください。
- 統合リモートコンソールウィンドウ上にマウスが置かれている場合、コンソールウィンドウにフォーカスがあるかどうかに関係なく、コンソールはすべてのキーストロークをキャプチャします。キー入力を行う際には、統合リモートコンソールウィンドウ上にマウスポインタを置いてください。
- キー入力を正しく行うため、クライアント OS およびサーバーOS のキーボード言語を同じ設定にする必要があります。
- iLO Firmware Version 1.20 Feb 02 2018 以前が動作中の環境で Java IRC をご利用される際には、[Access Settings]ページの[Service]セクションにある[Web Server SSL Port]設定をデフォルト値にする必要があります。
- iLO 5 Firmware Version 1.20 Feb 02 2018 でサポートされる HTML5 IRC は、英語キーボード環境のみサポートしています。英語キーボードをクライアントに接続のうえ、クライアント OS、サーバーOS のキーボード言語設定、および Web ブラウザーの言語設定を英語に設定してください。設定が日本語キーボードとなっている場合、およびクライアントに日本語キーボードを接続している場合は、一部のキー入力を行うことができません（以下の図の赤で囲っている部分）。日本語環境で入力を行えないキーについては OS のスクリーンキーボード機能をご利用になり入力してください。対象となるキーはご使用の Web ブラウザーによって異なりますので、以下をご確認ください。

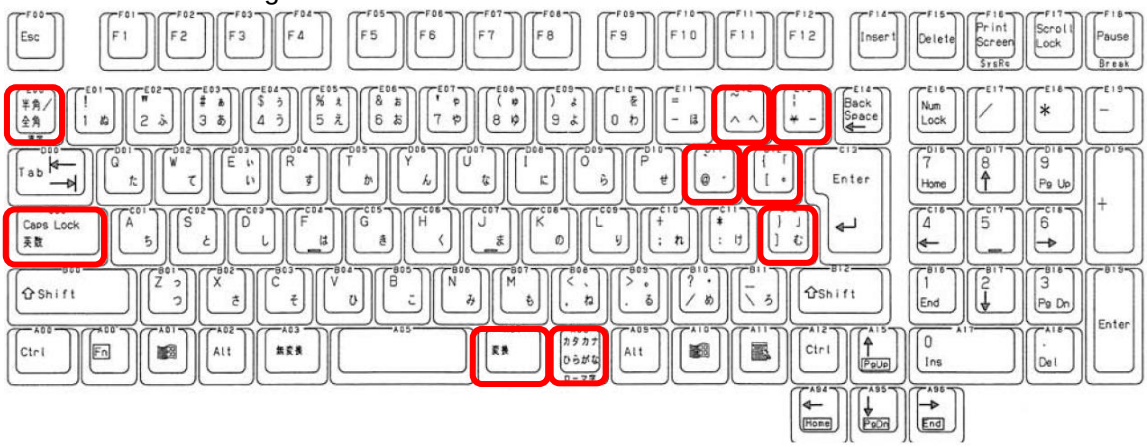
o Firefox



o Internet Explorer



o Microsoft Edge



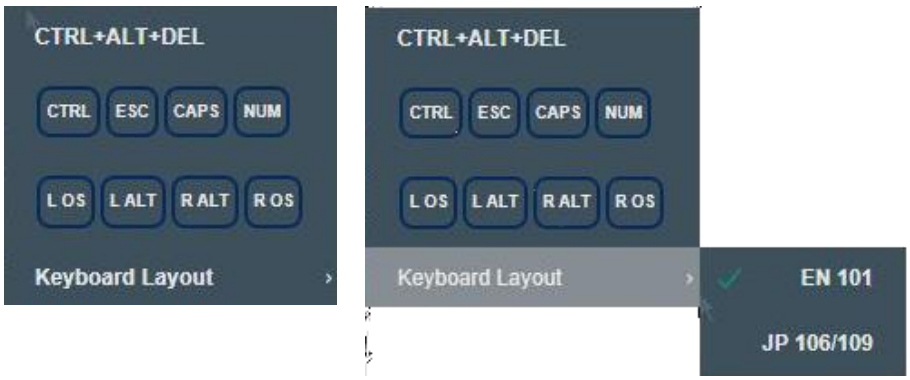
- Chrome

OS や Web ブラウザーのバージョン次第では、上記とは動作が異なる場合があります。
.NET 統合リモートコンソール(IRC)および Java 統合リモートコンソール(IRC)では、全てのキーが入力可能です。

- iLO 5 Firmware Version 1.30 May 31 2018 以降でサポートされる HTML5 IRC では、日本語キーボードの半角/全角、および Alt キーの入力を行うことができません。入力が行えないキーについては、OS のスクリーンキーボード機能をご使用になり入力してください。
  Alt キーは、HTML5 統合リモートコンソール(IRC)の仮想キーでも使用可能です。

  物理キーボードに応じて、HTML IRC のキーボードアイコン  をクリックし、**[Keyboard Layout]**から**[EN101]**または**[JP 106/109]**を選択してください。また、以下の制御キーに関しては、キーボードアイコンをクリックした際に表示される仮想キーを使用してください。

  - 物理キーボードのキーと仮想キーとの対応は次の通りです。Ctrl → CTRL、ESC → ESC、Caps Lock → CAPS、Num Lock → NUM、Windows(Left/Right) → L OS/R OS、Alt(Left/Right)→L ALT/R ALT



- IRC の動作において、推奨するネットワーク帯域は、10Mbps です。

.NET IRC 要件

ここでは、.NET IRC の使用要件を示します。

Microsoft .NET Framework

.NET IRC は、.NET Framework の次のバージョンのいずれかを必要とします。

iLO 5 Firmware Version 1.20 Feb 02 2018 以前の場合

- .NET Framework 3.5 Full（SP1 を推奨）
- .NET Framework 4.0 Full
- .NET Framework 4.5
- .NET Framework 4.6

iLO 5 Firmware Version 1.30 May 31 2018 以降の場合

- .NET Framework 4.5.1 以降

Windows 7、8、8.1、および 10 では、サポートされる.NET Framework バージョンは、OS に含まれています。.NET Framework は、Microsoft ダウンロードセンター(**http:// www.microsoft.com/download**）でも入手できます。

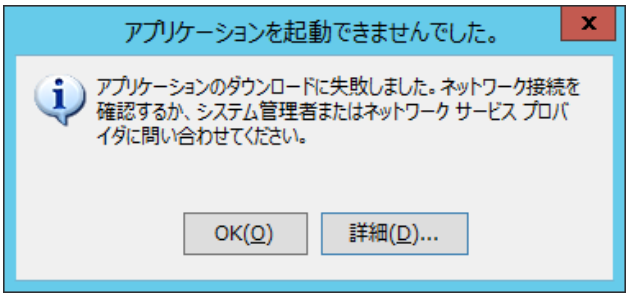
.NET Framework バージョン 3.5 および 4.0 には、2 つのデプロイメントオプション、Full および Client Profile があります。Client Profile は、Full フレームワークの一部にあたります。.NET IRC は、Full フレームワークを使用する場合にのみサポートされます。Client Profile はサポートされません。.NET Framework のバージョン 4.5 以降には、Client Profile オプションはありません。

Internet Explorer のみ：**[Remote Console & Media]→[Launch]**ページは、サポートされているバージョンの.NET Framework がインストールされているかどうかを示します。Internet Explorer がユーザーエージェント文字列を非表示にするように設定されている場合、この情報は表示されません。

Microsoft Edge ブラウザーでは、インストールされている.NET Framework のバージョンに関する情報は表示されません。

Microsoft ClickOnce

.NET IRC は、.NET Framework の一部である Microsoft ClickOnce を使用して起動します。ClickOnce は、SSL 接続からインストールされるすべてのアプリケーションが、信頼できるソースからのものであることを要求します。ブラウザーが iLO システムを信頼するように設定されていないときに**[IRC requires a trusted certificate in iLO]**の設定が有効に設定されている場合、ClickOnce に次のエラーメッセージが表示されます。



詳しくは、「統合リモートコンソールの信頼設定（.NET IRC）の設定」を参照してください。

Java ランタイム環境のダウンロード

Java IRC では最新バージョンの Java ランタイム環境を使用することをおすすめします。

1. **[Remote Console & Media]→[Launch]**ページに移動します。
2. **Java Integrated Remote Console (Java IRC)**セクションの**[the latest version of the Java™ Runtime Environment]**をクリックして次の Web サイトに移動します。このサイトから Java ソフトウェアをダウンロードできます。**http://www.java.com/ja/**

推奨されるクライアントの設定

リモートサーバーの解像度は、クライアントコンピューターの解像度以下であるのが理想的です。解像度が高くなると転送される情報量も多くなるので、全体のパフォーマンスが低下します。

最大のパフォーマンスを発揮するために、次のクライアントおよびブラウザー設定を使用してください。

- 画面のプロパティ
  - 256 色以上のオプションを選択する
  - リモートサーバーの解像度より高い画面解像度を選択する
  - Linux の画面のプロパティ - **[X Preferences]**画面で、フォントサイズを**[12]**に設定する
- マウスのプロパティ
  - [ポインターの速度] を中程度に設定する
  - [ポインターの加速度] を低に設定するか、無効にする

推奨されるサーバーの設定

すべてのサーバーで、以下の点に注意してください。

- パフォーマンスを最適にするには、サーバーの画面のプロパティで背景なし（壁紙を使用しない）を使用するように設定し、サーバーのマウスのプロパティでポインターの軌跡表示を無効に設定してください。
- クライアントの Java IRC ウィンドウにホストサーバーの画面全体を表示するには、クライアントの解像度と同じかそれより低いサーバーの表示解像度を選択してください。

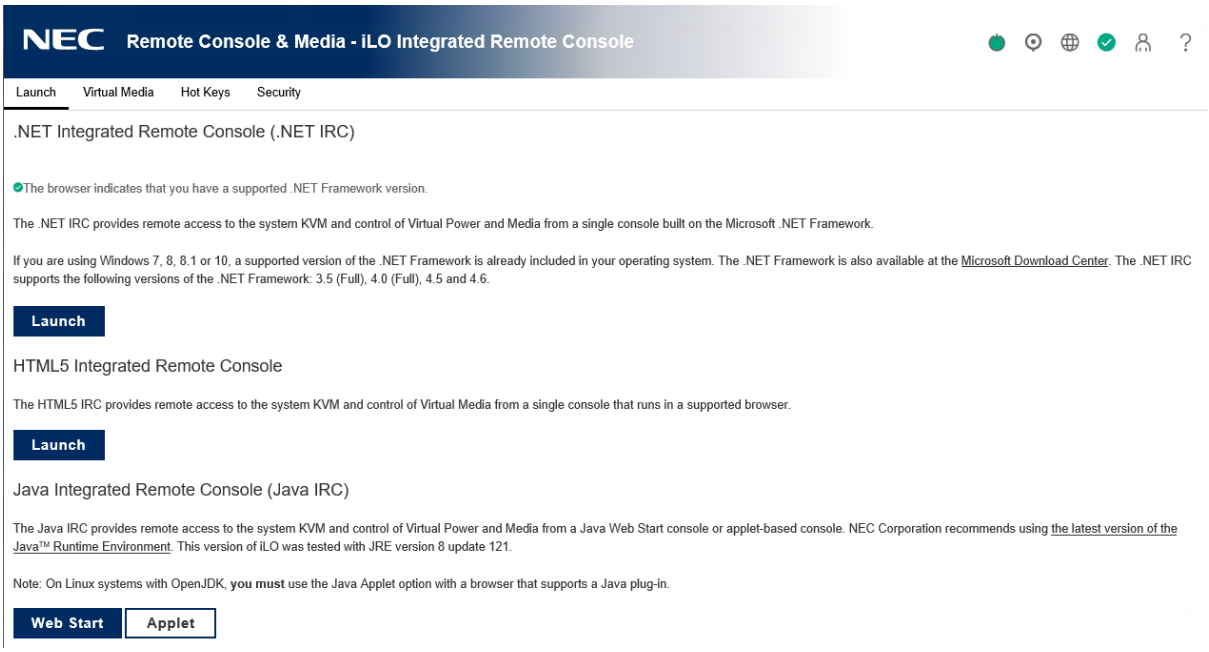
KDE の場合は、**[Control Center]**にアクセスして、**[Peripherals/Mouse]**、**[Advanced]**タブの順に選択してください。

マウスの加速を無効にするには、コマンド xset m 1 を入力します。

統合リモートコンソールの起動

.NET IRC の起動

1. **[Remote Console & Media]**→**[Launch]**ページに移動します。



2. システムが.NET IRC を使用する要件を満たしていることを確認します。
3. .NET IRC の**[Launch]**ボタンをクリックします。

[Information]→**[Overview]**ページで、[.NET]のリンクをクリックしても起動します。

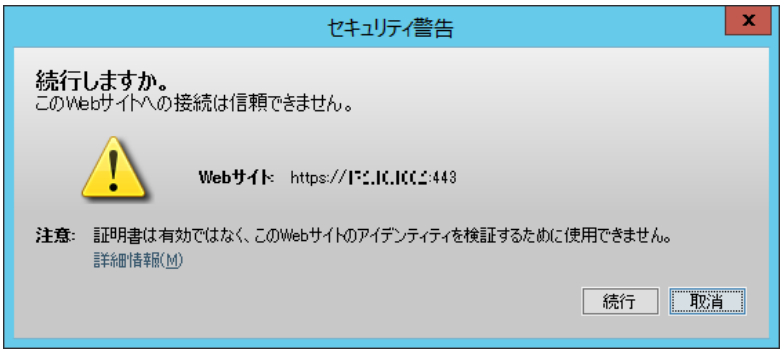
Java IRC の起動（Oracle JRE）

この手順を使用して、Windows または Linux と Oracle JRE の環境で Java IRC を起動します。

1. **[Remote Console & Media]**→**[Launch]**ページに移動します。
2. システムが Java IRC を使用する要件を満たしていることを確認します。
3. **[Web Start]**ボタンをクリックします。
   - Internet Explorer：ブラウザーが、Java IRC JNLP ファイルを開くように要求します。
   - Firefox：ブラウザーが、Java IRC JNLP ファイルを保存するように要求します。
   - Chrome：ブラウザーが Java IRC JNLP ファイルをダウンロードします。
4. JNLP ファイルを開きます。
   - Internet Explorer：ファイルを開くためのプロンプトをクリックします。
   - Firefox：ダウンロードした JNLP ファイル保存して開きます。
   - Chrome：ダウンロードした JNLP ファイルを開きます。

5. アプリケーションの実行を確認するプロンプトが表示されたら、実行をクリックします。
   実行をクリックしないと、Java IRC は起動しません。

6. セキュリティ警告ダイアログボックスが表示された場合は、続行をクリックします。
   続行をクリックしないと、Java IRC は起動しません。



[Information]→[Overview]ページで、**[Java Web Start]**のリンクをクリックしても起動します。

Java IRC の起動（OpenJDK JRE）

Linux と OpenJDK JRE の環境で Java IRC を起動するには、この手順を使用します。

1. **[Remote Console & Media]→[Launch]**ページに移動します。
2. システムが Java IRC を使用する要件を満たしていることを確認します。
3. **[Applet]**ボタンをクリックします。
4. セキュリティ警告ダイアログボックスが表示された場合は、「はい」をクリックして続行します。
   「はい」をクリックしないと、Java IRC は起動しません。

HTML5 IRC の起動

HTML5 IRC を起動するには、この手順を使用します。

- **[Remote Console & Media]→[Launch]**ページに移動します。
- HTML5 IRC の**[Launch]**ボタンをクリックします。

HTML5 IRC のコントロール

HTML5 IRC には、3 つの表示モードが用意されています。

- ウインドウモード

  1. HTML5 IRC を起動した際のデフォルトのモードです。iLO Web インターフェース上に HTML5 IRC のウィンドウが表示されます。
     - キーボードアイコンをクリックすることで、CTRL+ALT+DEL, Num Lock, Caps Lock のショートカットを送信することができます。
     - iLO 5 Firmware Version 1.30 May 31 2018 以降の場合、CD/DVD アイコンをクリックし、**[Floppy]**または**[CD/DVD]**から Virtial Media URL を選択することで、スクリプト方式の仮想メディアの接続ができます。使用する際にはイメージファイルの URL を指定してください。また、**[Floppy]**から Local *img file を選択すると、iLO が接続されている端末のディレクトリから.img ファイルを選択してイメージファイルのリダイレクションを行うことができます。**[CD/DVD]**から Local *iso file を選択すると、iLO が接続されている端末のディレクトリから.iso ファイルを選択して ISO イメージファイルのリダイレクションを行うことができます。
     - iLO 5 Firmware Version 1.20 Feb 02 2018 の場合、CD/DVD アイコンをクリックすることで、スクリプト方式の仮想メディアの接続ができます。使用する際にはイメージファイルの URL を指定してください。
     -  アイコンをクリックすることで、ドックモードに切り替わります。
     -  アイコンをクリックすることで、フルスクリーンモードに切り替わります。
     -  アイコンをクリックすることで、HTML5 IRC を終了します。
     - ウインドウを移動する場合は、ウインドウ上部をマウスでドラッグしてください。
     - ウインドウのサイズを変更する場合は、ウインドウ下部をマウスでドラッグしてください。

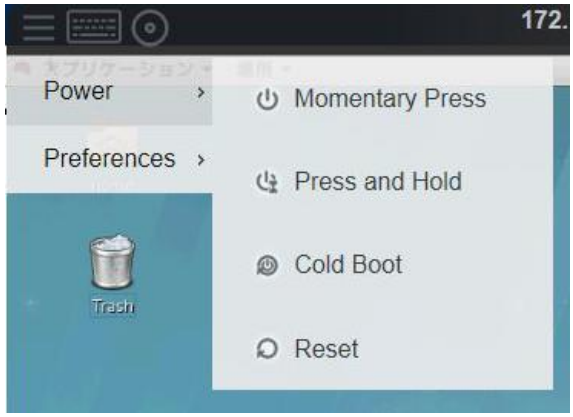
- ドックモード
  - Web インターフェース画面の左側に表示される iLO ナビゲーションペインのコンソールサムネイル部分に、HTML5 IRC が表示されます。通常のサムネイル表示と異なり画面が常時更新されますので、画面出力を確認しながら Web インターフェースの操作を行う場合に便利です。
  - キーボードアイコンをクリックすることで、CTRL+ALT+DEL, Num Lock, Caps Lock のショートカットを送信することができます。
  - iLO 5 Firmware Version 1.30 May 31 2018 以降の場合、CD/DVD アイコンをクリックし、**[Floppy]**または**[CD/DVD]**から Virtial Media URL を選択することで、スクリプト方式の仮想メディアの接続ができます。使用する際にはイメージファイルの URL を指定してください。また、**[Floppy]**から Local *img file を選択すると、iLO が接続されている端末のディレクトリから.img ファイルを選択してイメージファイルのリダイレクションを行うことができます。**[CD/DVD]**から Local *iso file を選択すると、iLO が接続されている端末のディレクトリから.iso ファイルを選択して ISO イメージファイルのリダイレクションを行うことができます。

- iLO 5 Firmware Version 1.20 Feb 02 2018 の場合、CD/DVD アイコンをクリックすることで、スクリプト方式の仮想メディアの接続ができます。使用する際にはイメージファイルの URL を指定してください。
- アイコンをクリックすることで、ドックモードに切り替わります。
- アイコンをクリックすることで、フルスクリーンモードに切り替わります。
- アイコンをクリックすることで、HTML5 IRC を終了します。

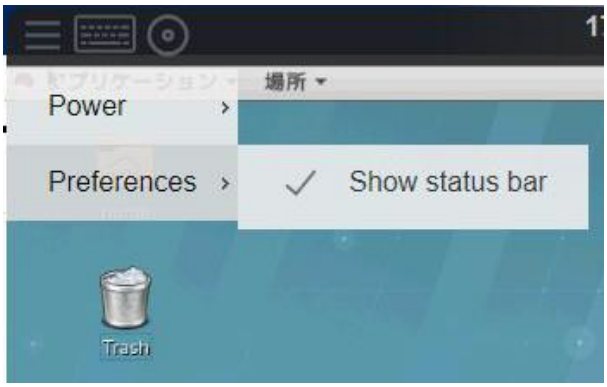
- フルスクリーンモード
  - HTML5 IRC の画面がフルスクリーン表示されます。
  - ESC キーを押すことで、フルスクリーンモードを終了します。
  - マウスポインタを画面の上端に寄せると、以下のようなメニューが上部に表示されます。

  - ピンアイコンをクリックすることで、このメニューを常時表示することができます。
  - キーボードアイコンをクリックすることで、CTRL+ALT+DEL、Num Lock、 Caps Lock のショートカットを送信することができます。
  - iLO 5 Firmware Version 1.30 May 31 2018 以降の場合、CD/DVD アイコンをクリックし、**[Floppy]**または**[CD/DVD]**から Virtial Media URL を選択することで、スクリプト方式の仮想メディアの接続ができます。使用する際にはイメージファイルの URL を指定してください。また、**[Floppy]**から Local *img file を選択すると、iLO が接続されている端末のディレクトリから.img ファイルを選択してイメージファイルのリダイレクションを行うことができます。**[CD/DVD]**から Local *iso file を選択すると、iLO が接続されている端末のディレクトリから.iso ファイルを選択して ISO イメージファイルのリダイレクションを行うことができます。
  - iLO 5 Firmware Version 1.20 Feb 02 2018 の場合、CD/DVD アイコンをクリックすることで、スクリプト方式の仮想メディアの接続ができます。使用する際にはイメージファイルの URL を指定してください。
  - アイコンをクリックすることで、フルスクリーンモードに変更する前のモードに切り替わります。
  - アイコンをクリックすることで、HTML5 IRC を終了します。

- メニュー
  - メニューアイコンから[Power]を選択するとサーバの電源制御ができます。操作できるのは以下になります。



    - **[Momentary Press]**
    - **[Press and Hold]**
    - **[Cold Boot]**
    - **[Reset]**
  - メニューアイコンから[Preferences]を選択すると、ステータスバーの表示/非表示切り替えができます。



- Remote Console status bar

  - Screen Resolution:リモートコンソールウィンドウの解像度を表示します。
  - Screen Capture:スクリーンキャプチャを作成します。
  - Encryption:リモートコンソールと iLO 間通信の暗号化タイプを表示します。
  - Health:サーバのヘルス状態を表示します。
  - Activity LED:リモートコンソールを介してローカル仮想メディアアクセス時のアクティビティインディケータを表示します。
  - Power:サーバの電源ステータス(On/Off)を表示します。

HTML5 スタンドアロンリモートコンソールの起動

最初に iLO Web インターフェースにログインせずに、HTML5 リモートコンソールにアクセスするには、この手順を使用します。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
- リモートコンソール機能がアクセス設定ページで有効になっている。

手順

1. ブラウザーウィンドウを開き、次の Web ページに移動します。https://<iLO ホスト名または IP アドレス>/irc.html

   Microsoft Internet Explorer の場合のみ：ホスト名または IPv4 アドレスを使用します。HTML5 リモートコンソールは、Microsoft Internet Explorer による IPv6 接続でサポートされていません。Microsoft WebSocket 実装では、標準以外の IPv6 リテラルアドレスが必要です。

   iLO HTML5 リモートコンソールログインページが開きます。
   - ログインセキュリティバナーが構成されている場合は、バナーテキストが通知セクションに表示されます。
   - iLO ヘルスステータスが劣化で匿名データアクセスオプションが有効な場合は、ヘルスステータスと問題の説明が iLO のログインページに表示されます。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。
2. ディレクトリまたはローカルアカウントログイン名とパスワードを入力して、ログインをクリックします。

   iLO が Kerberos ネットワーク認証用に設定されている場合は、ログインボタンの下に Zero サインインボタンが表示されます。Zero サインインボタンを使用して、ユーザー名とパスワードを入力せずにログインできます。
3. リモートコンソール機能を使用します。

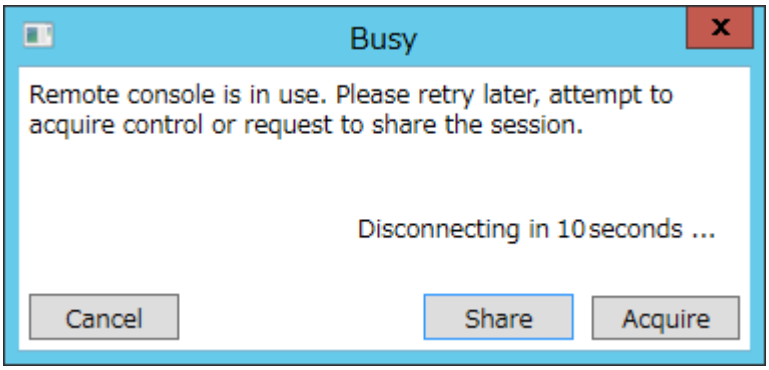
   （オプション）HTML5 リモートコンソールのオンラインヘルプを表示するには、メニューアイコンをクリックし、ヘルプを選択します。

リモートコンソールの取得

別のユーザーがリモートコンソールで作業している場合、そのユーザーからリモートコンソールを取得することができます。（HTML5 IRC を除く。）

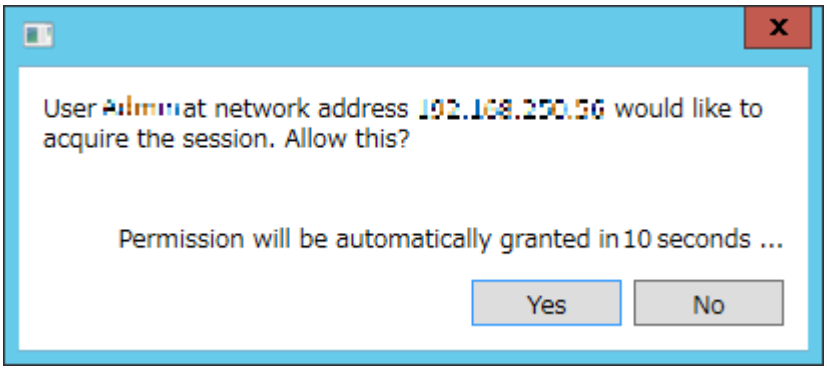
1. **[Remote Console & Media]→[Launch]**ページに移動します。
2. 使用するリモートコンソールのボタンをクリックします。

   別のユーザーがリモートコンソールで作業していることが、システムから通知されます。



3. **[Acquire]**ボタンをクリックします。

   他のユーザーは、リモートコンソールを取得する許可を承認するか拒否するように求められます。



   10 秒の間に応答がない場合、許可が付与されます。

リモートコンソールの電源スイッチの使用

電源スイッチを使用するには、.NET IRC または Java IRC の場合にはリモートコンソールの**[Power Switch]**メニューから、HTML5 IRC の場合には**[Power]**メニューから次のいずれかのオプションを選択します。

- **[Momentary Press]** - 物理的な電源ボタンを押す場合と同じです。サーバーの電源が切れている場合は、**[Momentary Press]**を押すとサーバーに電源が投入されます。

  一部のオペレーティングシステムでは、電源ボタンを一時的に押した後、適切なシャットダウンを開始するか、またはこのイベントを無視するように設定されていることがあります。仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して適切なオペレーティングシステムシャットダウンを完了することをおすすめします。
- **[Press and Hold]** - 物理的な電源ボタンを 5 秒間押し続け、離すことと同じです。

  サーバーはこの操作の結果、電源がオフになります。このオプションを使用すると、オペレーティングシステムの適切なシャットダウン機能に影響を与える可能性があります。
- **[Cold Boot]** - サーバーの電源を切断します。プロセッサー、メモリ、および I/O リソースは、メインの電力が失われます。サーバーは、約 6 秒後再起動します。このオプションを使用すると、オペレーティングシステムの適切なシャットダウン機能に影響を与えます。
- **[Reset]** - サーバーを強制的にウォームブートします。また CPU および I/O リソースはリセットされます。このオプションを使用すると、オペレーティングシステムの適切なシャットダウン機能に影響を与えます。

サーバーの電源が入っていない場合、**[Press and Hold]**、**[Cold Boot]**、および**[Reset]**は使用できません。

リモートコンソールからの iLO 仮想メディアの使用

リモートコンソールから仮想メディア機能を使用する手順については、「リモートコンソール仮想メディア」を参照してください。

共有リモートコンソール（.NET IRC 専用）

共有リモートコンソールにより、同じサーバーで複数のセッションの接続が可能です。この機能は、トレーニングやトラブルシューティングのような活動に使用できます。

通常、リモートコンソールセッションを開始する最初のユーザーがサーバーに接続し、セッションリーダーに指名されます。リモートコンソールアクセスを要求する以後のユーザーは、サテライトクライアント接続のアクセス要求を開始します。セッションリーダーのデスクトップに各アクセス要求用のダイアログボックスが表示され、要求者のユーザー名と DNS 名（使用できる場合）または IP アドレスを識別します。セッションリーダーは、アクセスを許可または拒否することができます。応答がない場合、アクセスは自動的に拒否されます。

共有リモートコンソールは、セッションリーダー指定を別のユーザーに渡したり、障害後にユーザーを再接続したりしません。障害後にユーザーアクセスを許可するには、リモートコンソールセッションを再起動する必要があります。

共有リモートコンソールセッション中、セッションリーダーはすべてのリモートコンソール機能にアクセスできますが、他のすべてのユーザーはキーボードとマウスにアクセスできるだけです。サテライトクライアントは、仮想電源や仮想メディアを制御できません。

iLO は、最初にクライアントを認証し、セッションリーダーが新しい接続を許可するかどうかを決定して共有リモートコンソールセッションを暗号化します。

共有リモートコンソールセッションへの参加

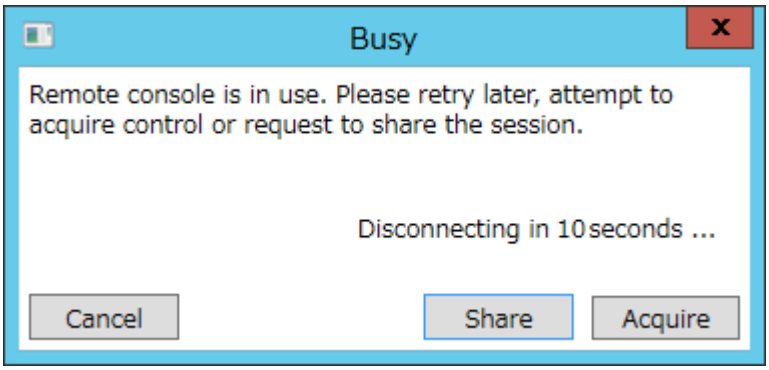
前提条件

iLO Advanced または iLO Essentials ライセンスがインストールされている。
NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

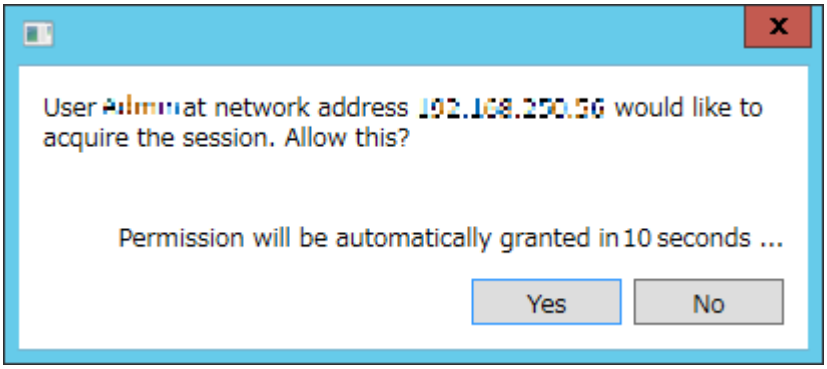
1. **[Remote Console & Media]**→**[Launch]**ページに移動します。
2. **[Launch]**をクリックして、.NET IRC を起動します。

   .NET IRC が使用中であることを通知するメッセージが表示されます。



3. **[Share]**をクリックします。

   セッションリーダーは、.NET IRC セッションへの参加のリクエストを受信します。



   セッションリーダーが**[Yes]**をクリックすると、ユーザーは.NET IRC セッションへのアクセスを許可され、キーボードやマウスを使えるようになります。

コンソールの録画（.NET IRC 専用）

コンソールの録画を使用すると、起動、および検出されたオペレーティングシステムの不具合のようなイベントのビデオストリームを記録し、再生することができます。
サーバー起動シーケンスとサーバー事前障害シーケンスは、iLO によって自動的に取得されます。
コンソールビデオの録画を手動で開始および停止することもできます。
コンソールの録画を使用する場合、以下の点に注意してください。

- コンソールの録画は.NET IRC のみでサポートされます。Java IRC と HTML5 IRC ではサポートされません。
- コンソールの録画は.NET IRC のみで使用できます。CLP や iLO RESTful API からはアクセスできません。
- サーバー起動シーケンスとサーバー事前障害シーケンスは、ファームウェアのアップデート中またはリモートコンソールの使用中には録画されません。
- サーバー起動シーケンスとサーバー事前障害シーケンスは、自動的に iLO メモリに保存されます。ファームウェアのアップデート、iLO のリセット、および電源の消失時には失われます。.NET IRC を使用すると、取得したビデオをローカルドライブに保存できます。
- サーバー起動ファイルは、サーバーの起動が検出されたときに取得を開始し、容量が一杯になったときに停止します。このファイルは、サーバーが起動するたびに上書きされます。

- サーバー事前障害シーケンスの録画は、サーバー起動ファイルの録画完了後に開始されます。障害検知時までのデータがラウンドロビンで上書き保存されます障害検出時点で自動録画は停止します。サーバー事前障害シーケンスによ録画が再生された時点で録画データは更新されますそれまでは更新されません。
- コンソール取得ツールの制御ボタンは、.NET IRC セッションウィンドウの下部にあります。

  次の再生コントロールを利用できます。

  - **[スタートにスキップ]** - ファイルの最初から再生を再開します。
  - **[一時停止]** - 再生を一時停止します。
  - **[再生]** - 現在選択されているファイルが再生されていない場合や一時停止されている場合は、再生を開始します。
  - **[録画]** - .NET IRC セッションを記録します。
  - **[プログレスバー]** - ビデオセッションの進行状況が示されます。

サーバー起動シーケンスとサーバー事前障害シーケンスの表示

前提条件

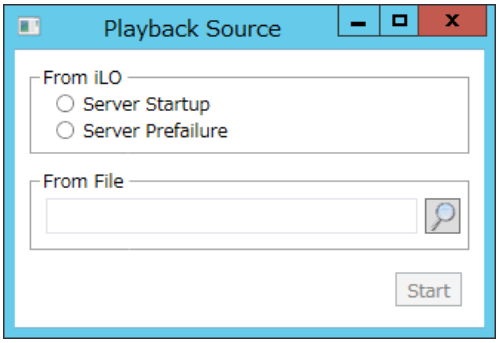
iLO Advanced ライセンスがインストールされている。

NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. .NET IRC を起動します。
2. **[再生]**ボタンをクリックします。

   再生ソースダイアログボックスが表示されます。



3. **[Server Startup]**または**[Server Prefailure]**を選択します。
4. **[Start]**をクリックします。

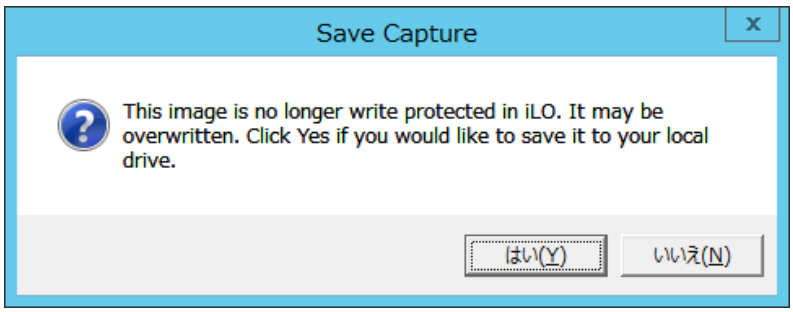
サーバー起動ビデオファイルとサーバー事前障害ビデオファイルの保存

前提条件

iLO Advanced ライセンスがインストールされている。
NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. .NET IRC を起動します。
2. **[再生]**ボタンをクリックします。
3. **[Server Startup]**または**[Server Prefailure]**を選択します。
4. **[Start]**をクリックします。
5. **[再生]**ボタンを再びクリックして、再生を停止します。
6. ローカルドライブに保存する旨の確認が表示され、**[はい]**をクリックします。



7. Save Video ダイアログボックスでファイル名、保存場所を入力し、**[保存]**をクリックします。

ビデオファイルの手動録画

前提条件

iLO Advanced ライセンスがインストールされている。
NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

コンソールの録画を使用すると、サーバー起動およびサーバー事前障害以外のシーケンスのビデオファイルを手動で取得できます。

1. .NET IRC を起動します。
2. **[録画]**ボタンをクリックします。
3. Save Video ダイアログボックスが開きます。
4. ファイル名、保存場所を入力し、**[保存]**をクリックします。
5. 録画が終了したら、もう一度**[録画]**ボタンを押して録画を停止します。

保存したビデオファイルの表示

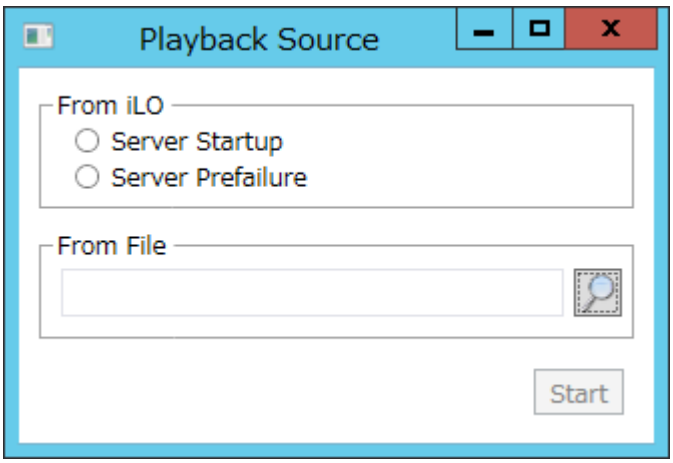
前提条件

iLO Advanced ライセンスがインストールされている。
NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. .NET IRC を起動します。
2. **[再生]**ボタンをクリックします。

   Playback Source ダイアログボックスが表示されます。



3. **[From File]**ボックスの横にある虫眼鏡アイコンをクリックします。
4. ビデオファイルに移動し、**[開く]**をクリックします。

   リモートコンソールで取得したビデオファイルは、iLO ファイルタイプ(.ilo ファイル)を使用します。
5. **[Start]**をクリックします。

リモートコンソールのホットキー

プログラムリモートコンソールホットキーのページを使用すると、リモートコンソールセッション中に使用する最大 6 つのホットキー(**Ctrl+T**、**Ctrl+U**、**Ctrl+V**、**Ctrl+W**、**Ctrl+X**、**Ctrl+Y**)を定義できます。各ホットキーは、ホットキーを押すとホストサーバーへ送信される最大 5 つのキーの組み合わせを設定できます。ホットキーは、.NET IRC、Java IRC、HTML5 IRC およびテキストベースのリモートコンソールを使用するリモートコンソールセッション中に有効です
ホットキーが設定されていない場合、たとえば、**Ctrl+V** は**[NONE]**、**[NONE]**、**[NONE]**、**[NONE]**、**[NONE]**に設定され、このホットキーは無効になります。サーバーオペレーティングシステムは、**Ctrl+V** を通常のように解釈します（この例では「貼り付け」）。別のキーの組み合わせを使用するように **Ctrl+V** を設定すると、サーバーオペレーティングシステムは iLO に設定されたキーの組み合わせを使用します（貼り付け機能がなくなります）。

例 1：**Alt+F4** をリモートサーバーに送信したいが、このキーの組み合わせを押すとブラウザーが閉じる場合は、**Alt+F4** のキーの組み合わせをリモートサーバーに送信するようにホットキー **Ctrl+X** を設定することができます。ホットキーの設定後は、リモートサーバーに **Alt+F4** を送信したいとき、リモートコンソールウィンドウで **Ctrl+X** を押します。

例 2：オルタネートグラフィック（**AltGR**）キーをリモートサーバーに送信するホットキーを作成したい場合は、キーリストの **R_ALT** を使用します。

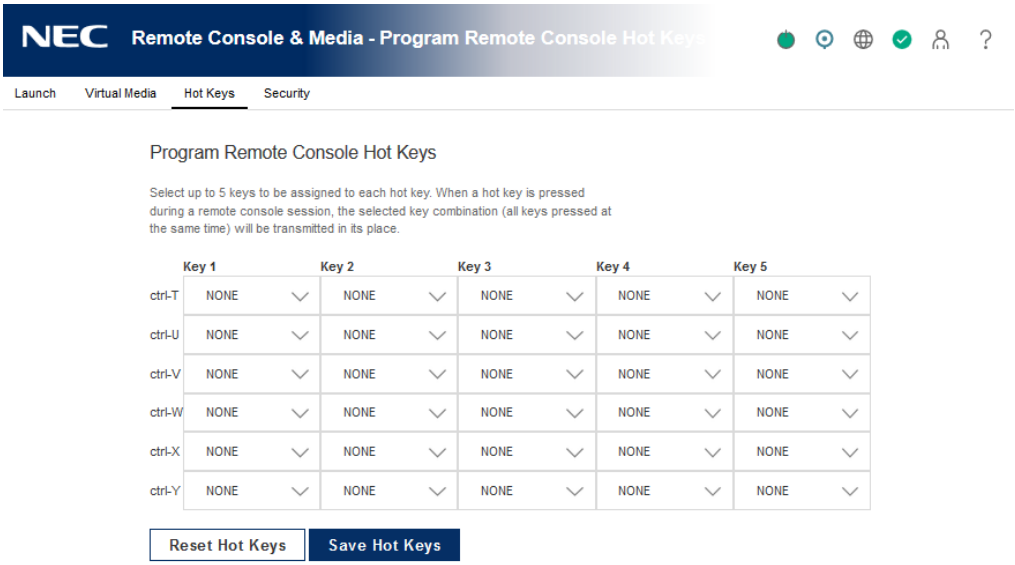
ホットキーの作成

前提条件

iLO の設定を構成権限

手順

1. **[Remote Console & Media]→[Hot Keys]**ページに移動します。



2. 作成するホットキーごとに、リモートサーバーに送信するキーの組み合わせを選択します。
表 1 はホットキーを設定するときに使用できるキーを示します。

重要: ホットキーを設定して日本語キーボードからのキーシーケンスを生成するには、日本語キーボード上の目的のキーと同じキーを送る US キーボードのキーを選択します。表 1 の括弧内のキーは US キーボードのキーに対応する日本語キーボードのキーを示します。

表 1 ホットキーの設定で使えるキー

ESC	SCRL LCK	0	f
L_ALT	SYS RQ	1	g
R_ALT	PRINT SCREEN	2	h
L_SHIFT	F1	3	i
R_SHIFT	F2	4	j
L_CTRL	F3	5	k
R_CTRL	F4	6	l
L_GUI	F5	7	m
R_GUI	F6	8	n
INS	F7	9	o
DEL	F8	;	p
HOME	F9	=（^）	q
END	F10	[（@）	r
PG UP	F11	\（]）	s
PG DN	F12	]（[）	t
ENTER	SPACE	`（半角/全角）	u
TAB	'（:）	a	v
BREAK	,	b	w
BACKSPACE	-	c	x
NUM PLUS	.	d	y
NUM MINUS	/	e	z

3. **[Save Hot keys]**をクリックします。

iLO は、ホットキーの設定が正常に更新されたことを確認します。

ホットキーのリセット

前提条件

iLO の設定を構成権限

手順

すべてのホットキー割り当てのクリアホットキーをリセットすると、現在のすべてのホットキー割り当てがクリアされます。

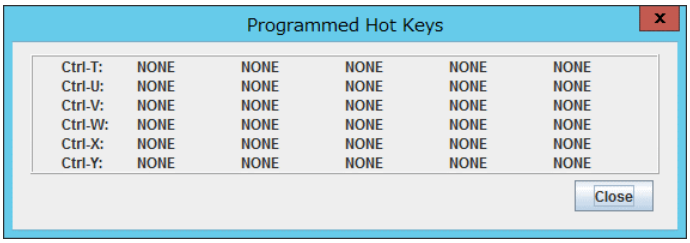
1. **[Remote Console & Media]→[Hot Keys]**ページに移動します。
2. **[Reset Hot Keys]**をクリックします。

   要求を確認するように求められます。
3. **[OK]**をクリックします。

   ホットキーがリセットされたことが iLO によって通知されます。

リモートコンソールの構成済みホットキーの表示（Java IRC のみ）

1. Java IRC を起動します。
2. **[Keyboard]→[View Hot Keys]**を選択します。



リモートコンソールセキュリティの設定

リモートコンソールのセキュリティ設定を使用して、リモートコンソールのコンピューターロック設定および統合リモートコンソールの信頼設定を制御します。

前提条件

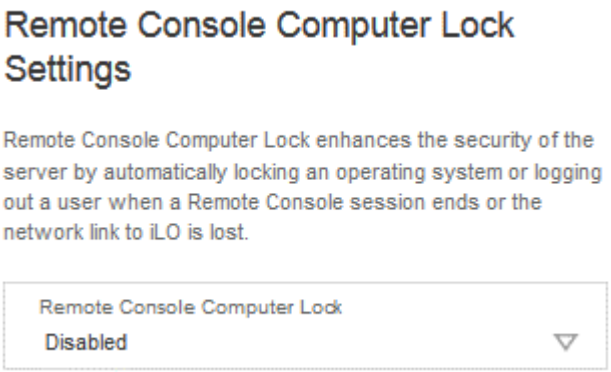
iLO の設定を構成権限

リモートコンソールのコンピューターロックの設定

リモートコンソールのコンピューターロック機能は、リモートコンソールセッションが終了したり、iLO に対するネットワークリンクが失われたりした場合に、オペレーティングシステムを自動的にロックしたり、ユーザーをログアウトさせたりすることによって、iLO で管理されるサーバーのセキュリティを向上する機能です。この機能が設定されているときにユーザーが.NET IRC 、Java IRC または HTML5 IRC の ウィンドウを開いた場合、ウィンドウを閉じるときにオペレーティングシステムがロックされます。

手順

1. **[Remote Console & Media]→[Security]**ページに移動します。



2. 以下の **[Remote Console Computer Lock]**設定から選択します。
   - **[Windows]** - Windows オペレーティングシステムを実行している管理対象サーバーをロックします。リモートコンソールセッションが終了した場合や iLO ネットワークリンクが失われた場合は、サーバーの画面がロックされます。
   - **[Custom]** - カスタムキーシーケンスを使用して管理対象サーバーをロックしたりサーバーにログインしているユーザーをログアウトさせたりできます。最大で 5 つのキーをリストから選択できます。リモートコンソールセッションが終了した場合や iLO ネットワークリンクが失われた場合は、選択されたキーシーケンスがサーバーのオペレーティングシステムに自動的に送信されます。
   - **[Disabled]**（デフォルト） - リモートコンソールのコンピューターロック機能を無効にします。リモートコンソールセッションが終了した場合や iLO ネットワークリンクが失われた場合でも、管理対象サーバー上のオペレーティングシステムはロックされません。
3. コンピューターロックのキーシーケンスを選択します。

   サポートされているキーのリストについては、「リモートコンソールの有効なコンピューターロックキー」を参照してください。
4. **[適用]**をクリックして、変更を保存します。

リモートコンソールの有効なコンピューターロックキー

リモートコンソールのコンピューターロックに使用するキーシーケンスの作成には、表 2 に記載されているキーを使用できます。

重要: ロックキーを設定して日本語キーボードからのキーシーケンスを生成するには、日本語キーボード上の目的のキーと同じキーを送る US キーボードのキーを選択します。表 2 の括弧内のキーは US キーボードのキーに対応する日本語キーボードのキーを示します

表 2 リモートコンソールのコンピューターロックキー

ESC	SCRL LCK	0	f
L_ALT	SYS RQ	1	g
R_ALT	PRINT SCREEN	2	h

L_SHIFT	F1	3	i
R_SHIFT	F2	4	j
L_CTRL	F3	5	k
R_CTRL	F4	6	l
L_GUI	F5	7	m
R_GUI	F6	8	n
INS	F7	9	o
DEL	F8	;	p
HOME	F9	=（^）	q
END	F10	[（@）	r
PG UP	F11	\（]）	s
PG DN	F12	]（[）	t
ENTER	SPACE	`（半角/全角）	u
TAB	'（:）	a	v
BREAK	,	b	w
BACKSPACE	-	c	x
NUM PLUS	.	d	y
NUM MINUS	/	e	z

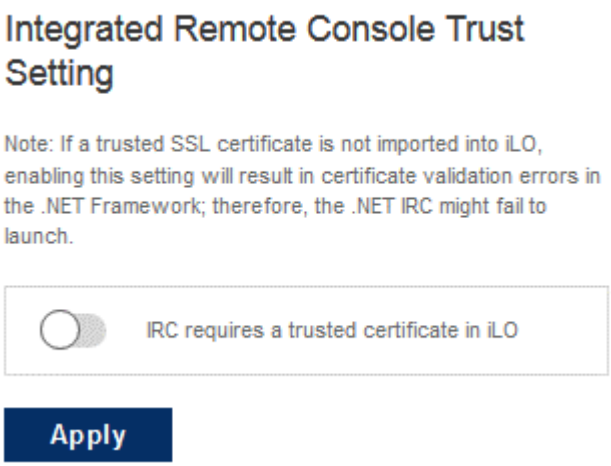
統合リモートコンソールの信頼設定（.NET IRC）の設定

.NET IRC は、Microsoft .NET Framework の一部である Microsoft ClickOnce を介して起動します。ClickOnce は、SSL 接続からインストールされるすべてのアプリケーションが信頼できるソースからのものであることを要求します。ブラウザーが iLO プロセッサーを信頼するように設定されていないときに統合リモートコンソールの信頼設定が有効に設定されている場合、ClickOnce はアプリケーションを起動できないことを通知します。

この iLO にアクセスするすべてのクライアントが.NET IRC を実行するために信頼済みの証明書を必要とするかどうかを指定するには、以下の手順に従ってください。

手順

1. **[Remote Console & Media]**→**[Security]**ページに移動します。



2. **[Integrated Remote Console Trust Setting]**セクションの**[IRC requires a trusted certificate in iLO]**トグルボタンで、いずれかを選択します。
   - **[有効]** - 信頼された SSL 証明書が iLO にインポートされている場合、.NET IRC は HTTPS 接続を使用して起動します。
   - **[無効]**（デフォルト） - .NET IRC は非 SSL 接続を使用して起動します。.NET IRC が暗号キーの交換を開始すると、SSL が使用されます。
3. **[Apply]**をクリックして、変更を保存します。

9. テキストベースのリモートコンソールの使用

iLO は、テキストベースのリモートコンソールをサポートします。サーバーからビデオ情報が取得され、ビデオメモリの内容が iLO マネージメントプロセッサーへ送信され、圧縮され、暗号化され、管理クライアントアプリケーションに転送されます。iLO は、画面フレームバッファーを使用してテキスト情報の変更を検出し、変更を暗号化し、テキストベースのクライアントアプリケーションに（画面上の位置情報とともに）文字を送信します。この方法により、標準的なテキストベースクライアントとの互換性、良好な性能、および単純さが確保されます。ただし、ASCII 以外の文字やグラフィカル情報は表示できず、表示される文字の画面上の位置の送信順序が前後にずれる場合があります。

iLO は、ビデオアダプターの DVO ポートを使用して、ビデオメモリに直接アクセスします。この方法により、iLO の性能が大幅に向上します。ただし、デジタルビデオストリームには、有用なテキストデータが含まれていません。このデータは、SSH のようなテキストベースのクライアントアプリケーションでは表示できません。

iLO 仮想シリアルポートの使用

標準ライセンスで iLO 仮想シリアルポートを使用すると、iLO からテキストベースのコンソールにアクセスできます。

iLO 仮想シリアルポートは、iLO テキストベースのリモートコンソールの一種です。iLO 仮想シリアルポートにより、サーバーのシリアルポートと双方向データフローが可能になります。リモートコンソールを使用すると、リモートサーバーシリアルポート上に物理シリアル接続が存在するかのように操作できます。

iLO 仮想シリアルポートはテキストベースのコンソールとして表示されますが、その情報はグラフィカルビデオデータを通じて描画されます。サーバーがプレオペレーティングシステム状態にあるとき、iLO は SSH クライアントを通して情報を表示するので、ライセンスのない iLO が POST 処理中にサーバーを確認して通信できるようになります。

iLO 仮想シリアルポートを使用すると、リモートユーザーは以下の操作を実行できます。

- サーバーの POST シーケンスおよびオペレーティングシステムの起動シーケンスの操作

重要: 仮想シリアルポートセッション中にシステムユーティリティを起動するには、仮想シリアルポートセッション中に、**ESC+9** キーの組み合わせを入力します

- オペレーティングシステムとのログインセッションの確立、オペレーティングシステムの操作、およびオペレーティングシステム上のアプリケーションの実行と操作
- グラフィックフォーマットで Linux を実行する iLO の場合は、サーバーのシリアルポートで getty()を設定し、iLO 仮想シリアルポートを使用して Linux オペレーティングシステムへのログインセッションを表示することができます。詳しくは、「Linux のための iLO 仮想シリアルポートの設定」を参照してください。
- iLO 仮想シリアルポートからの EMS コンソールの使用。EMS は、Windows の起動の問題とカーネルレベルの問題をデバッグする場合に便利です。詳しくは、「Windows EMS コンソールのための iLO 仮想シリアルポートの設定」を参照してください。

システムユーティリティでの iLO 仮想シリアルポートの設定

次の手順は、iLO 仮想シリアルポートを使用する前に必要な設定です。この手順は Windows システムと Linux システムの両方で必要です。

手順

1. システムユーティリティにアクセスします。
   a. オプション：サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
   b. サーバーを再起動するかまたは電源を入れます。
   c. POST 画面で **F9** キーを押して、システムユーティリティを起動します。
2. 仮想シリアルポートの COM ポートを設定します。
   a. **[システム構成]**画面で、上矢印または下矢印キーと **Enter** キーを使用して、**[BIOS/プラットフォーム構成(RBSU)]→[システムオプション]→[シリアルポートオプション]**画面に移動します。
   b. **[仮想シリアルポート]**を選択し、使用する COM ポートを選択します。
3. BIOS シリアルコンソールポートの COM ポートを設定します。
   a. **[BIOS シリアルコンソール/EMS]**を選択し、**Enter** キーを押します。
   b. **[BIOS シリアルコンソールポート]**を選択し、**[仮想シリアルポート]**を選択します。
4. BIOS シリアルコンソールボーレートを設定します。
   a. **[BIOS シリアルコンソールボーレート]**を選択します。
   b. **[115200]**を選択します。

   注記: iLO 仮想シリアルポートの現在の実装では、物理 UART は使用しません。そのため、BIOS シリアルコンソールボーレートの値は、iLO 仮想シリアルポートがシステムからのデータの送受信に使用する実際の速度には影響を与えません。

5. EMS コンソールの COM ポートを設定します。

   EMS は Windows 専用です。
   a. **[EMS コンソール]**を選択し、**Enter** を押します。
   b. 手順 2 で選択した値に一致する COM ポートを選択します。
6. **F12** キーを押します。
7. **[Yes - Save Changes]**選択し、変更を保存します。
8. **[Reboot]**をクリックします。

Linux のための iLO 仮想シリアルポートの設定

コンソールリダイレクションを使用して、Linux サーバーをリモートから管理できます。コンソールリダイレクションを使用するように Linux を設定するには、Linux ブートローダー（GRUB）を設定する必要があります。サーバーのシステム ROM が POST を完了すると、ブート可能デバイスからブートローダーアプリケーションがロードされます。シリアルインターフェース（ttyS0）をデフォルトのインターフェースに定義して、10 秒（デフォルトタイムアウト値）以

内にローカルキーボードから入力がなければ、システムは出力先をシリアルインターフェース（iLO 仮想シリアルポート）に変更します。

Red Hat Enterprise Linux 6 のための iLO 仮想シリアルポートの設定

次の例に基づいて GRUB（`/etc/grub.conf`）を設定します。

注記: ttyS0 と unit 0 は com1 用で、ttyS1 と unit 1 は com2 用です。

次の設定例では Red Hat Enterprise Linux 6 および com1 を使用しています。

```
serial --unit=0 --speed=115200
terminal --timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
title Red Hat Linux (2. 6.18-164.e15) root (hd0,2)
9
kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS0,115200
initrd /initrd-2.6.18-164.e15.img
```

com2 を選択した場合、構成の例は次のようになります。

```
serial --unit=1 --speed=115200
terminal --timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz title Red Hat
Linux (2. 6.18-164.e15) root (hd0,2)
9
kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS1,115200
initrd /initrd-2.6.18-164.e15.img
```

Linux が完全にブートすると、ログインコンソールをシリアルポートにリダイレクションできます。

- /dev/ttyS0 および/dev/ttyS1 デバイスが設定されている場合、これらのデバイスにより、iLO 仮想シリアルポートを通じてシリアル TTY セッションを取得できます。設定したシリアルポートでシェルセッションを開始するには、システムブート中に自動的にログインプロセスを開始するように/etc/inittab ファイルに次の行を追加します。

  次の例は、/dev/ttyS0 でログインコンソールを開始します。

  ```
  S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
  ```

  次の例は、dev/ttys1:でログインコンソールを開始します。

  ```
  S1:2345:respawn:/sbin/agetty 115200 ttyS1 vt100
  ```

- SSH を使用して iLO に接続し、iLO の CLP コマンド start /system1/oemNEC_vsp1 を使用して、Linux オペレーティングシステムへのログインセッションを表示します。

Red Hat Enterprise Linux 7 のための iLO 仮想シリアルポートの設定

1. テキストエディタで/etc/sysconfig/grub を開きます。

   次の設定例では `ttys0` を使用しています。

   1. GRUB_CMD_LINELINUX 行の最後に、console=ttys0 と入力します。
   2. rhgb quiet を削除します。
   3. 次のパラメーターを入力します:

   ```
   GRUB_TIMEOUT=5
   GRUB_DEFAULT=saved
   ```

```
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
console=ttyS0,115200n8"
GRUB_DISABLE_RECOVERY="true"
```

2. 次のコマンドを入力して、grub.cfg ファイルを作成します:
   ```
   grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
   ```
3. シリアルポートの getty ログインサービスを有効にします。
   例えば :
   ```
   systemctl enable serial-getty@ttyS0.service
   ```
4. シリアルポートで待つように getty を設定します。
   例えば :
   ```
   systemctl start getty@ttyS0.service
   ```
5. 設定済みのシリアルポートでシェルセッションを開始するには、/etc/inittab ファイルに次の行を追加して、システム起動時に自動的にログインプロセスを開始します。
   次の例では、/dev/ttyS0 上のログインコンソールを起動します:
   ```
   S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
   ```
6. SSH を使用して iLO に接続し、iLO の CLP コマンド start /system1/oemNEC_vsp1 を使用して、Linux オペレーティングシステムへのログインセッションを表示します。

Red Hat Enterprise Linux 8 のための iLO 仮想シリアルポートの設定

1. grub2-env コマンドを使用して、kernelopts パラメーターを確認します。
   以下に例を示します。

   # grub2-editenv list | grep kernalopts
   kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhelswap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet
2. list コマンドの結果をコピーします。
   以下に例を示します。rhgb quiet は除いてください。

   kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhelswap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
3. カーネルオプションを設定します。
   手順 2 でコピーした既存のカーネルオプションに、シリアルコンソールオプションを追加します。
   以下に例を示します。以下の設定例では、ttyS0 を使用しています。

   # grub2-editenv - set "kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhelswap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0"
4. オプション）パラメーターが正しく設定されたことを確認するには、list コマンドを再実行します。
   以下に例を記します。

   # grub2-editenv list | grep kernelopts
   kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhelswap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0
5. サーバーを再起動します。

Windows EMS コンソールのための iLO 仮想シリアルポートの設定

iLO を使用すると、Windows EMS コンソールをネットワーク経由で Web ブラウザーを介して使用できます。EMS を使用すると、ビデオ、デバイスドライバーなどオペレーティングシステム機能が原因で通常の動作や通常の修正処置が実行できない場合に、Emergency Management Services（EMS）を実行できます。
iLO で Windows EMS コンソールを使用する場合、以下の点に注意してください。

- iLO 仮想シリアルポートを使用する前に、オペレーティングシステムに Windows EMS コンソールを設定する必要があります。EMS コンソールを有効化する方法については、オペレーティングシステムのドキュメントを参照してください。EMS コンソールがオペレーティングシステムで有効になっていない場合は、iLO 仮想シリアルポートにアクセスしようとしたときに、iLO がエラーメッセージを表示します。
- Windows EMS シリアルポートは、システムユーティリティから設定する必要があります。設定では、EMS ポートを有効または無効にすることや COM ポートを選択することができます。iLO は、EMS ポートの有効/無効を自動的に検出し、COM ポートの選択を検出します。Windows EMS シリアルポートの有効化について詳しくは、「システムユーティリティでの iLO 仮想シリアルポートの設定」を参照してください。
- Windows EMS コンソールは、iLO リモートコンソールと同時に使用できます。
- SAC>プロンプトが表示されるようにするには、iLO 仮想シリアルポートを介して接続した後で、**[Enter]**キーを押す必要がある場合があります。

iLO 仮想シリアルポートを使用するために Windows を設定するには、次の手順に従ってください。

1. コマンドウィンドウを開きます。
2. 次のコマンドを入力して、起動構成データを編集します。
   bcdedit /ems on
3. 次のコマンドを入力して、EMSPORT および EMSBAUDRATE の値を構成します。
   bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200

   注記**:** EMSPORT:1 が COM1 で、EMSPORT:2 が COM2 です。
   bcdedit /?と入力して 構文のヘルプを表示します。

   ---
4. オペレーティングシステムを再起動します。

iLO 仮想シリアルポートセッションの開始

手順

1. 構成されている iLO 仮想シリアルポート設定をシステムユーティリティで確認します。
   詳しくは、「システムユーティリティでの iLO 仮想シリアルポートの設定」を参照してください。

2. Windows または Linux オペレーティングシステムが iLO 仮想シリアルポートを使用するように設定されていることを確認します。

   詳しくは、「Windows EMS コンソールのための iLO 仮想シリアルポートの設定」または「Linux のための iLO 仮想シリアルポートの設定」を参照してください。

3. SSH セッションを開始します。
   たとえば、**ssh Administrator@<iLO IP** アドレス**>**を入力するか、または putty.exe をポート 22 で接続します。
4. プロンプトが表示されたら、iLO アカウントの認証情報を入力します。
5. </>iLO->プロンプトで、**VSP** と入力し、**Enter** キーを押します。
6. （Windows システムの場合のみ） <SAC> プロンプトで **cmd** と入力して、コマンドプロンプトチャネルを作成します。
7. （Windows システムの場合のみ） **ch - si <#>** と入力して、チャネル番号で指定されたチャネルに切り替えます。
8. プロンプトが表示されたら、OS のログイン認証情報を入力します。

iLO 仮想シリアルポートログの表示

iLO 仮想シリアルポートログが有効な場合、vsp log コマンドを使用して iLO 仮想シリアルポートの動作を表示できます。

手順

1. iLO Advanced または iLO Scale-Out ライセンスがインストールされていることを確認します。
2. **[Security]**→**[Access Settings]**ページの**[Secure Shell (SSH)]**および**[Virtual Serial Port Log]**を有効にします。

   手順については、「iLO アクセスの設定」を参照してください。

3. SSH 経由で CLI に接続します。
4. **vsp** コマンドを使用して、iLO 仮想シリアルポートの動作を表示します。
5. **ESC + (**を入力して、終了します。
6. iLO 仮想シリアルポートログを表示するには、**vsp log** を入力します。

10. ホスト上での iLO 使用

仮想 NIC 機能は、iLO へセキュアなダイレクト接続が可能です。ホスト上、もしくはリモートコンソール接続を介してこの機能を使用します。

Web インターフェース、SSH、RESTful API を使用して iLO に接続します。

仮想 NIC 機能は、以下の場合に役に立ちます。

- ネットワーク構成がマネージメントネットワーク経由での接続を防止している場合に iLO にアクセスする。
- ホストまたは iLO に接続されている NIC ケーブルがない場所で iLO にアクセスできます。

仮想 NIC をサポートしているオペレーティングシステム

仮想 NIC は、以下のオペレーティングシステムでサポートされています。

- Microsoft Windows Server 2019

仮想 NIC を使用するのに必要な一般要件

- ホスト OS が仮想 NIC をサポートしている。
- USB CDC-EEM ドライバがホスト OS 上にインストールされている。
- 仮想 NIC 機能が、**[Access Settings]**ページで有効になっている。
- iLO に接続するインターフェースが**[Access Settings]**ページで有効になっている。

  例えば、iLO Web インターフェースに接続したい場合には、**[iLO Web Interface]**が有効になっている。
- ホスト OS が、iLO に接続するのに使用するポートをブロックするように構成されていない。

  例えば、デフォルトの iLO 構成で iLO Web インターフェースに接続したい場合には、ホスト OS が 443 ポートをブロックしていないことを確認してください。
- 仮想 NIC インターフェースがチーミング、または複数のホスト NIC のいずれかとチーミング、ブリッジされていないこと。この構成では、仮想 NIC が無効あるいは不安定になります。

仮想 NIC 機能を有効にする

手順

1. ナビゲーションツリーで**[Security]**をクリックします。
2. **[Access Settings]**ページが表示されます。
3. **[iLO]**カテゴリの✎をクリックします。
4. **[Edit iLO Settings]**が開かれます。
5. **[Virtual NIC]**のチェックボックスを選択し、**[OK]**をクリックします。
   iLO が、保留中の変更を有効にするにはリセットが必要であることを通知します。
6. 変更を完了したい場合は、**[Reset iLO]**をクリックします。

iLO が要求を確認するように求めます。

7. **[Yes, Reset iLO]**をクリックします。
   接続が再確立されるまでに、数分かかることがあります。
   リセット完了後に仮想 NIC 機能が有効になり、ホスト OS 側で検出されます。
8. 仮想 NIC がホスト OS 上で有効になっていることを確認します。
   a. リモートコンソールセッションを開始するか、物理的にホストにアクセスします。
   b. ホストOSにログインします。
   c. 以下を実行してください。
      Windows の場合: ipconfig を実行して、イーサーネットアダプター イーサーネットのアダプター名を探してください。

   Linux の場合: コマンドラインから以下のように USB Ethernet の接続プロファイルの作成、USB Ethernet デバイスの有効化を行います。

   1. USB Ethernet の接続プロファイルを作成
      接続プロファイル一覧を確認し、DEVICE 列に「enp1s0f4u4」デバイスに対応する接続プロファイルが NAME 列にあるかを確認します。
      該当する接続プロファイルがない場合、接続プロファイル(vNIC)を作成します。

```
# nmcli connection
NAME    UUID                                  TYPE      DEVICE
eno1    7fd577b9-02e2-46d7-9c2b-eb62d4a11e03  ethernet  eno1
virbr0  c150df83-432d-4022-be27-81cd2fa84a96  bridge    virbr0
# nmcli connection add type ethernet con-name vNIC ifname enp1s0f4u4
接続 'vNIC' (b19fee19-cad9-4a72-97e9-cd7e69d761a4) が正常に追加されました。
# nmcli device
DEVICE      TYPE      STATE     CONNECTION
eno1        ethernet  接続済み  eno1
enp1s0f4u4  ethernet  接続済み  vNIC
virbr0      bridge    接続済み  virbr0
eno2        ethernet  切断済み  --
lo          loopback  管理無し  --
virbr0-nic  tun       管理無し  --
```

> △ **注意:**
> [Virtual NIC]が[Enabled]の状態で、StarterPack S8.10-007.01 以上から AMS をインストールすると、OS 上の USB Ethernet デバイスのプロファイル(vNIC)が作成されて自動的に接続されます。また、この時に「vNIC」という接続プロファイルが作成され、自動的に接続状態となります。そのため上記の手動での接続プロファイル作成、及びデバイスへの接続は必要ありません。

2. USB Ethernet デバイスへの接続
「enp1s0f4u4」デバイスの STATE が「切断済み」の場合、デバイスへの接続を行います。有効化後に STATE が「接続済み」になっていることを確認してください。

```
# nmcli device
DEVICE      TYPE      STATE     CONNECTION
eno1        ethernet  接続済み  eno1
virbr0      bridge    接続済み  virbr0
eno2        ethernet  切断済み  --
enp1s0f4u4  ethernet  切断済み  --
lo          loopback  管理無し  --
virbr0-nic  tun       管理無し  --
# nmcli device connect enp1s0f4u4
デバイス 'enp1s0f4u4' が 'b19fee19-cad9-4a72-97e9-cd7e69d761a4' で正常にアクティベートされました。
# nmcli device
DEVICE      TYPE      STATE     CONNECTION
eno1        ethernet  接続済み  eno1
enp1s0f4u4  ethernet  接続済み  vNIC
virbr0      bridge    接続済み  virbr0
eno2        ethernet  切断済み  --
lo          loopback  管理無し  --
virbr0-nic  tun       管理無し  --
```

3. ifconfig を実行して、以下のようなインターフェースが登録されていることを確認してください。

△ **注意:**
使用 OS が Red Hat Enterprise Linux 7.6 以上で、iLO の Virtual NIC が有効の状態で、StarterPack S8.80-002.01 以上から AMS をインストールすると、OS 上の USB Ethernet デバイスが自動的に有効化されます。また、この時に「vNIC」という接続プロファイルが作成されます。

ただし、使用 OS が Red Hat Enterprise Linux 7.6 以上の場合(Red Hat Enterprise Linux 8.0 以上を除く)で NIC カードの Bonding(チーミング)が有効化されている場合は、自動で有効化されないことがあります。その場合は上記手順で USB Ethernet デバイスを有効化してください。

※ iLO の仮想 NIC 機能を無効化する場合は、事前に「vNIC」プロファイルを削除してください。

仮想 NIC 機能を無効にする

Linux の場合、コマンドラインから以下のように USB Ethernet の接続プロファイル確認し、作成した USB Ethernet (enp1s0f4u4)に対応する接続プロファイル(vNIC)を削除します。

```
# nmcli connection
NAME    UUID                                  TYPE      DEVICE
eno1    7fd577b9-02e2-46d7-9c2b-eb62d4a11e03  ethernet  eno1
vNIC    b19fee19-cad9-4a72-97e9-cd7e69d761a4  ethernet  enp1s0f4u4
virbr0  c150df83-432d-4022-be27-81cd2fa84a96  bridge    virbr0
# nmcli connection delete vNIC
接続 'vNIC' (b19fee19-cad9-4a72-97e9-cd7e69d761a4) が正常に削除されました。
# nmcli connection
NAME    UUID                                  TYPE      DEVICE
eno1    7fd577b9-02e2-46d7-9c2b-eb62d4a11e03  ethernet  eno1
virbr0  c150df83-432d-4022-be27-81cd2fa84a96  bridge    virbr0
```

以下の手順によって、iLO の仮想 NIC 機能を無効化します。

手順

1. **ナビゲーションツリーで[Security]をクリックします。**
2. **[Access Settings]**ページが表示されます。
3. **[iLO]**カテゴリの✎をクリックします。
4. **[Edit iLO Settings]**が開かれます。
5. **[Virtual NIC]**のチェックボックスを非選択し、**[OK]**をクリックします。
   iLO が、保留中の変更を有効にするにはリセットが必要であることを通知します。
6. 変更を完了したい場合は、**[Reset iLO]**をクリックします。
   iLO が要求を確認するように求めます。
7. **[Yes, Reset iLO]**をクリックします。
   接続が再確立されるまでに、数分かかることがあります。
   ※OS 上で USB Ethernet インターフェースを無効にすることでも仮想 NIC 機能は無効になります。

仮想 NIC インターフェースを静的から DHCP に変更する（ネットワークマネージャー）

Linux ディストリビューションが DHCP の新しいネットワークインターフェースを自動的に構成しない 場合、仮想 NIC インターフェースのネットワーク構成を静的から DHCP に変更します。

手順

1. ネットワークマネージャーを開きます。
2. 仮想 NIC インターフェースを探します。
3. DHCP を使用するように仮想 NIC インターフェースを構成します。

仮想 NIC インターフェースを静的から DHCP に変更する（CLI）

Linux ディストリビューションが DHCP の新しいネットワークインターフェースを自動的に構成しない 場合、仮想 NIC インターフェースのネットワーク構成を静的から DHCP に変更します。

手順

1. /sys/bus/usb/devices 内のデバイスを特定します。 以下に例を示します。
   - cat /sys/bus/usb/devices/1-4/idVendor は値 03f0 を表示します。
   - cat /sys/bus/usb/devices/1-4/idProduct は値 2927 を表示します。
2. 仮想 NIC ネットワークインターフェース名を特定します。 以下に例を示します。

/sys/bus/usb/devices/1-4/1-4:1.0/net/usb0

3. DHCP を使用するよう仮想 NIC インターフェースを構成するネットワーク構成スクリプトを記述しま す。
   たとえば、構成スクリプトに次のエントリーを含む/etc/sysconfig/network/ifcfg-usb0 を作 成します。BOOTPROTO='dhcp'.
4. 仮想 NIC インターフェースにアクセスするか、ネットワークサービスを再起動します。

仮想 NIC を使用して iLO web インターフェースにアクセスする

前提条件

- OS 環境が、仮想 NIC 機能を使用するのに必要な要件をみたしていること。
- ブラウザーがプロキシ―サーバーを使用するようにこうせいされていないこと。

手順

1. リモートコンソールセッションを開始するか、直接ホスト OS にアクセスします。
2. ホスト OS にログインします。
3. サポートされているブラウザーを開きます。
4. アドレスバーに次の URL(https://16.1.15.1)を入力します。
5. ログインページが表示されます。
6. iLO にログインします。
   セッションは、**[Session List]**ページに IP アドレス 16.1.15.2 として表示されます。
7. サーバや、iLO 構成の参照や更新のため iLO Web インターフェースを使用します。

ホスト上の iLOREST を使用する

前提条件

- ご使用の環境が仮想 NIC 機能を使用するための一般的な前提条件を満たしていること。
- ホストサーバーオペレーティングシステムに RESTful インターフェースツールがインストールされて いること。

手順

1. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
2. ホストサーバー OS にログインします。
3. iLOREST を開始します。
4. iLO システムにログインします。
   iLOrest > login 16.1.15.1 -u iLO user name -p iLO password
   iLO のホスト名と仮想 NIC の IP アドレスがクライアントシステムの hosts ファイルにある場合は、 iLO ホスト名を使用して接続することもできます。
   （ iLOrest > login iLO hostname -u iLO user name -p iLO password ）
5. iLOREST コマンドを使用してサーバーまたは iLO 構成を表示または更新します。

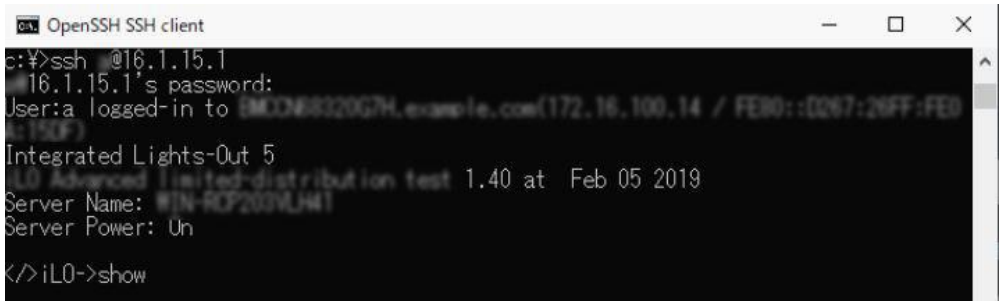
仮想 NIC を使用して SSH アクセスする

前提条件

- 環境が、仮想 NIC 機能を使用するのに必要な要件を満たしていること。
- ブラウザーがプロキシ―サーバーを使用するように構成されていないこと。

手順

1. リモートコンソールセッションを開始するか、直接ホスト OS にアクセスします。
2. ホスト OS にログインします。
3. インストールされている OS にもよりますが、コマンドプロンプトまたは PuTTY ターミナルなどでプロンプトを開きます。
4. iLO にログインします。
   ssh <iLO ユーザ名>@16.1.15.1



11. iLO 仮想メディアの使用

iLO 仮想メディアは、ネットワーク上の任意の場所にある標準のメディアからリモートホストサーバーを起動するために使用できる仮想デバイスを提供します。仮想メディアデバイスは、ホストシステムの起動時に使用できます。仮想メディアデバイスは、USB テクノロジーを使用してホストサーバーに接続します。

仮想メディアを使用する場合、以下の点に注意してください。

- 一部の形式の仮想メディアを使用するには、iLO ライセンスキーが必要です。
- この機能を使用するには、仮想メディア権限が必要です。
- 同時に 1 種類の仮想メディアしか接続できません。
- 仮想メディア機能は、最大 8TB の ISO イメージをサポートしています。ただし、ISO イメージの最大ファイルサイズは、ISO イメージが保存されているファイルシステムの 1 つのファイルサイズの制限や、サーバーの OS がサポートする SCSI コマンドなどの要因にも依存します。
- オペレーティングシステムでは、iLO の仮想ディスケット/USB キーまたは仮想 CD/DVD-ROM は、通常のドライブのように見えます。iLO を初めて使用する場合、ホストオペレーティングシステムが、新しいハードウェアの検出ウィザードを実行するよう指示する場合があります。
- 仮想デバイスが接続されてから接続を切断するまで、ホストサーバーは仮想デバイスを使用できます。仮想メディア機能の使用が終了して仮想メディアを切断するとき、ホストオペレーティングシステムからデバイスが安全に取り外されていないという警告メッセージを受け取る場合があります。デバイスを切断する前に、デバイスを停止するためのオペレーティングシステム機能を使用することにより、この警告を避けることができます。
- iLO 仮想 CD/DVD-ROM は、サポートされるオペレーティングシステムで、サーバーの起動時に使用できます。iLO 仮想 CD/DVD-ROM から起動することにより、ネットワークドライブからのオペレーティングシステムの展開、障害の発生したオペレーティングシステムのディザスタリカバリーなどの作業を実行できます。
- ホストサーバーのオペレーティングシステムが USB の大容量記憶装置または SD デバイスをサポートする場合、ホストサーバーのオペレーティングシステムをロードした後で、iLO 仮想フロッピー/USB キーを使用できます。
    - 仮想フロッピー/USB キーは、ホストサーバーのオペレーティングシステムの実行中に、デバイスドライバーのアップグレード、システム修復ディスク（ERD）の作成などの作業に使用できます。
    - サーバーの実行時に仮想フロッピー/USB キーを使用できるようにしておくと、NIC ドライバーを診断し、修復する必要がある場合に役立てることができます。
    - 仮想フロッピー/USB キーは、Web ブラウザーが動作している物理フロッピー、USB キー、または SD ドライブである場合があります。または、ローカルのハードディスクドライブまたはネットワークドライブに保存されているイメージファイルの場合もあります。

- 性能を最適化するため、高速ネットワークリンクを介してアクセスできるクライアントPC のハードディスクドライブまたはネットワークドライブに格納されているイメージファイルの使用をおすすめします。

- ホストサーバーのオペレーティングシステムが USB 大容量記憶装置をサポートする場合、ホストサーバーのオペレーティングシステムをロードした後にも、iLO 仮想 CD/DVD-ROM を使用できます。
  - 仮想 CD/DVD-ROM は、ホストサーバーのオペレーティングシステムの実行中に、デバイスドライバーのアップグレード、ソフトウェアのインストールなどの作業に使用できます。
  - サーバーの実行時に仮想 CD/DVD-ROM を使用できるようにしておくと、NIC ドライバーを診断し、修復する必要がある場合に役立てることができます。
  - 仮想 CD/DVD-ROM は、Web ブラウザーを実行しているマシン上の物理 CD/DVD-ROM ドライブである場合があります。また、仮想 CD/DVD-ROM は、ローカルのハードディスクドライブまたはネットワークドライブに保存されているイメージファイルの場合もあります。
  - 性能を最適化するため、高速ネットワークリンクを介してアクセスできるクライアントPC のハードディスクドライブまたはネットワークドライブに格納されているイメージファイルの使用をおすすめします。
- .NET IRC を使用すると、仮想フォルダーをマウントして、クライアントと管理対象サーバーの間でファイルにアクセスし、コピーすることができます。
- 仮想メディア機能を使用する前に、「仮想メディアを使用するためのオペレーティングシステム要件」にあるオペレーティングシステムに関する注意事項を確認してください。
- また、.NET IRC または Java IRC および iLO RESTful API、または SMASH CLP を使用して、仮想メディア機能にアクセスすることもできます。
- 仮想フロッピー/USB キーまたは仮想 CD/DVD-ROM 機能が有効になっている場合、通常、クライアントオペレーティングシステムからはフロッピーディスクドライブまたは CD/DVD-ROM ドライブにアクセスできません。

△ 注意: ファイルやデータが壊れることを防止するために、ローカルメディアを iLO 仮想メディアデバイスとして使用しているときは、ローカルメディアへのアクセスを試行しないでください。

仮想メディアを使用するためのオペレーティングシステム要件

ここでは、iLO 仮想メディア機能を使用する場合に注意する必要があるオペレーティングシステム要件について説明します。

オペレーティングシステムの USB 要件

仮想メディアデバイスを使用するには、オペレーティングシステムが USB 大容量記憶装置を含む USB デバイスをサポートする必要があります。詳しくは、オペレーティングシステムのドキュメントを参照してください。

システムのブート中に ROM BIOS は、オペレーティングシステムがロードされるまで USB サポートを提供します。MS-DOS は、BIOS を使用してストレージデバイスと通信しているので、DOS をブートするユーティリティディスクも仮想メディアとして機能します。

オペレーティングシステムに関する注意事項：仮想フロッピー/USB キー

- 起動プロセスおよび **DOS** セッション - 起動プロセスと DOS セッションの実行中、仮想フロッピーデバイスは標準の BIOS フロッピーディスクドライブ（A ドライブ）として表示されます。このとき、物理的に接続されたフロッピーディスクドライブがあっても使用できません。ローカル物理フロッピーディスクドライブと仮想フロッピーディスクドライブを同時に使用することはできません。
- **Windows Server 2008** 以降 - 仮想フロッピー/USB キードライブは、Windows が USB デバイスを認識した後に自動的に表示されます。仮想デバイスを、ローカル接続されたデバイスと同じように使用してください。

  Windows のインストール中にドライバーディスクとして仮想 USB キーを使用するには、USB キードライブのブート順序を変更し、USB キードライブのブート順序を最初にすることをおすすめします。
- **Red Hat Enterprise Linux** - Linux は、仮想フロッピーおよび USB キードライブの使用をサポートします。

ディスケットの交換

物理 USB ディスクドライブが搭載されているクライアントマシンで、仮想フロッピー/USB キーを使用する場合、物理 USB ディスク交換後のデバイスが認識されません。たとえば、フロッピーディスクからディレクトリリストを取得した後、ディスクを交換すると、次のディレクトリリストには、最初のフロッピー(A ドライブ)のディレクトリリストが表示されます。iLO の仮想フロッピー/USB キーの使用中にディスクを交換する必要がある場合は、必ず、物理 USB ディスクドライブ以外のディスクドライブが搭載されたクライアントマシンを使用してください。

オペレーティングシステムに関する注意事項：仮想 CD/DVD-ROM

- **MS-DOS** - 仮想 CD/DVD-ROM は、MS-DOS ではサポートされていません。
- **Windows** - 仮想 CD/DVD-ROM は、Windows がデバイスのマウントを認識した後に自動的に表示されます。これを、ローカル接続された CD/DVD-ROM ドライブと同じように使用してください。
- **Linux** - Red Hat Enterprise Linux の要件は以下のとおりです。

  1. **Red Hat Enterprise Linux**

     CD/DVD-ROM ドライブがローカル接続されているサーバーでは、/dev/cdrom1 で仮想 CD/DVD-ROM デバイスにアクセスできます。ただし、CD/DVD-ROM ドライブがローカル接続されていないサーバーは、仮想 CD/DVD-ROM は、/dev/cdrom でアクセスできる最初の CD/DVD-ROM です。

     仮想 CD/DVD-ROM は、通常の CD/DVD-ROM デバイスと同じように、次のコマンドを使用してマウントできます。

     mount /mnt/cdrom1

Linux システムで USB 仮想メディア CD/DVD-ROM をマウントする

手順

1. Web インターフェース経由で iLO にログインします。
2. .NET IRC または Java IRC を起動します。
3. **[Virtual Drives]**メニューを選択します。
4. 使用する CD/DVD-ROM を選択します。
5. 以下のコマンドを使用して、ドライブをマウントします。

   Red Hat Enterprise Linux の場合

   mount /dev/cdrom1 /mnt/cdrom1

オペレーティングシステムに関する注意事項：仮想フォルダー

- 起動プロセスおよび **DOS** セッション - 仮想フォルダーデバイスは、標準 BIOS フロッピードライブ（A ドライブ）として表示されます。このとき、物理的に接続されたフロッピードライブがあっても使用できません。ローカル物理フロッピードライブと仮想フォルダーを同時に使用することはできません。
- **Windows** - Windows が仮想 USB デバイスのマウントを認識すると、仮想フォルダーは自動的に表示されます。フォルダーは、ローカル接続されたデバイスと同じように使用できます。仮想フォルダーからは起動できません。仮想フォルダーから起動しようとすると、サーバーが起動できない場合があります。
- **Red Hat Enterprise Linux** - Linux は、FAT16 ファイルシステムフォーマットを使用する仮想フォルダー機能の使用をサポートします。

iLO の Web インターフェースからの仮想メディアの使用

仮想メディアのページでは、以下のタスクを実行できます。

- 仮想メディアポートを表示または変更する。

  [Security]→[Access Settings]ページでこの値を変更することもできます。

- ローカルに保存されたイメージファイル、フロッピーディスク、USB キー、CD/DVD-ROM、および仮想フォルダーのようなローカルメディアを表示する、または取り出す。
- スクリプト方式のメディアを表示、接続し、取り出す、またはこのメディアから起動する。スクリプト方式のメディアは、URL を使用して、Web サーバーでホストされている接続イメージを参照します。iLO は、HTTP または HTTPS の形式で URL を受け付けます。FTP はサポートされません。

仮想メディアポートの表示と変更

仮想メディアポートとは、iLO が仮想メディアを接続するために使用するポートのことです。デフォルト値は 17988 です。

前提条件

iLO の設定を構成権限

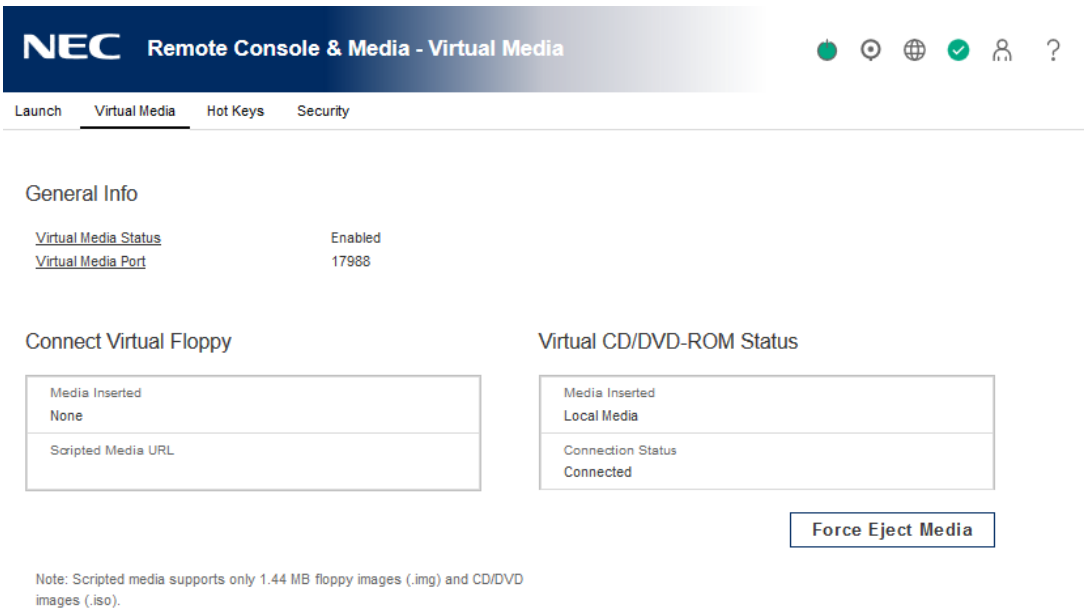
手順

1. **[Security]→[Access Settings]**ページに移動します。
2. **[Virtual Media Port]**ボックスに新しいポート番号を入力します。
3. **[Apply]**をクリックします。
4. iLO をリセットするように求められ、**[OK]**をクリックします。

ローカルメディアの表示

手順

接続されたローカルメディアデバイスを表示するには、**[Remote Console & Media]→[Virtual Media]**ページに移動します。



ローカル仮想メディアを接続すると、以下のセクションに詳細が表示されます。

- **[Virtual Floppy/USB Key/Virtual Folder Status]**
  - **[Media Inserted]** - 接続されている仮想メディアの種類。ローカルメディアが接続されている場合、**[Local Media]**と表示されます。
  - **[Connected]** - 仮想メディアデバイスが接続されているかどうかを示します。
- **[Virtual CD/DVD-ROM Status]**
  - [Media Inserted] - 接続されている仮想メディアの種類。ローカルメディアが接続されている場合、**[Local Media]**と表示されます。
  - **[Connected]** - 仮想メディアデバイスが接続されているかどうかを示します。

ローカルメディアデバイスの取り出し

手順

1. **[Remote Console & Media]→[Virtual Media]**ページに移動します。

2. **[Virtual Floppy/USB Key/Virtual Folder Status]**セクションまたは**[Virtual CD/DVD-ROM Status]**セクションにある**[Force Eject Media]**ボタンをクリックします。

スクリプト方式のメディアの接続

仮想メディアのページからスクリプト方式のメディアを接続できます。他の仮想メディアタイプを接続するには、.NET IRC または Java IRC、iLO RESTful API または CLI を使用します。

前提条件

仮想メディアのページは、1.44MB のフロッピーイメージ（IMG）および CD/DVD-ROM イメージ（ISO）の接続をサポートします。イメージは、iLO と同じネットワーク上の Web サーバーに置かれている必要があります。

手順

1. **[Remote Console & Media]**→**[Virtual Media]** ページに移動します。
2. **[Connect Virtual Floppy]**セクション（IMG ファイル）または**[Connect CD/DVD-ROM]**セクション（ISO ファイル）の**[Scripted Media URL]**ボックスにスクリプト方式のメディアの URL を入力します。
3. **CD/DVD-ROM** のみ：次のサーバー再起動時のみにこのイメージからサーバーを起動する必要がある場合は、**[Boot on Next Reset]**チェックボックスを選択します。

   イメージは 2 回目のサーバー再起動時に自動的に取り出されるので、サーバーは一度しかこのイメージから起動しません。

   このチェックボックスを選択しない場合、イメージは手動で取り出すまで接続されたまま残ります。また、サーバーは、システムブートオプションがそのように設定されている場合、以後のすべてのサーバーリセットでイメージから起動します。
4. **[Insert Media]**をクリックします。
5. オプション：接続されたイメージからただちに起動するには、サーバーを再起動します。

スクリプト方式のメディアの表示

スクリプト方式の仮想メディアが接続されている場合、**[Virtual Floppy/USB Key/Virtual Folder Status]**セクションまたは**[Virtual CD/DVD-ROM Status]**セクションに、次の詳細情報が示されます。

- **[Media Inserted]** - 接続されている仮想メディアの種類。スクリプト方式のメディアが接続されている場合、**[Scripted Media]**と表示されます。
- **[Connected]** - 仮想メディアデバイスが接続されているかどうかを示します。
- **[Image URL]** - 接続されているスクリプト方式のメディアを指し示す URL。

スクリプト方式のメディアの取り出し

手順

1. **[Remote Console & Media]**→**[Virtual Media]**ページに移動します。
2. **[Virtual Floppy/USB Key/Virtual Folder Status]**セクションまたは**[Virtual CD/DVD-ROM Status]**セクションにある**[Force Eject Media]**ボタンをクリックします。

リモートコンソール仮想メディア

ホストサーバー上の仮想メディアには、.NET IRC または Java IRC、iLO Web インターフェース、iLO RESTful API および CLP を使用してアクセスできます。このセクションでは、仮想メディア機能で.NET IRC または Java IRC を使用する方法を説明します。

仮想ドライブ

仮想ドライブ機能は、物理フロッピーディスクまたは CD/DVD-ROM、USB キードライブ、イメージファイル、URL 経由のイメージファイルの使用をサポートします。

クライアント PC での物理ドライブの使用

手順

1. .NET IRC または Java IRC を起動します。
2. **[Virtual Drive]**メニューをクリックし、クライアント PC 上のフロッピーディスク、CD/DVD-ROM、または USB キードライブのドライブ文字を選択します。
   仮想メディアの動作 LED は、仮想メディアの動作を表示します。

注記**:** Windows オペレーティングシステムバージョンの.NET IRC または Java IRC を使用する場合、物理ドライブをマウントするには Windows 管理者権限が必要です。

イメージファイルの使用

手順

1. .NET IRC または Java IRC を起動します。
2. **[Virtual Drive]**メニューをクリックし、**[Image File Removable Media]**（.img ファイル）または**[Image File CD-ROM/DVD]**（.iso ファイル）を選択します。
   .NET IRC または Java IRC に、ディスクイメージを選択するプロンプトが表示されます。
3. **[ファイル名]**テキストボックスにイメージファイルのパスまたはファイル名を入力するか、イメージファイルの位置に移動して**[開く]**をクリックします。
   仮想メディアのアクティビティ LED は、仮想メディアの動作を表示します。

URL 経由のイメージファイルの使用（IIS/Apache）

前提条件

.NET IRC または Java IRC を使用して、スクリプト方式のメディアを接続できます。スクリプト方式のメディアは、1.44MB のフロッピーディスクイメージ（.img）および CD/DVD-ROM イメージ（.iso）のみをサポートします。イメージは、iLO と同じネットワーク上の Web サーバーに置かれている必要があります。

手順

1. .NET IRC または Java IRC を起動します。
2. 使用するイメージタイプに合わせて、**[Virtual Drive]→[URL Removable Media]**（.img）または**[Virtual Drive] →[URL CD-ROM/DVD]**（.iso）を選択します。
   [Image File at URL]ダイアログボックスが開きます。

3. 仮想ドライブとしてマウントしたいイメージファイルの URL を入力して、**[Connect]**をクリックします。

   仮想メディアのアクティビティ LED は、URL でマウントされた仮想メディアのドライブの動作を表示しません。

メディアイメージの作成機能の使用（Java IRC のみ）

仮想メディアを使用するときは、物理ディスクの代わりにイメージファイルを使用すると、パフォーマンスが向上します。DD などの業界標準ツールを使用して、イメージファイルの作成や、ディスクイメージファイルから物理ディスクへのデータコピーを行うことができます。
Java IRC を使用してこれらのタスクを実行することもできます。

ディスクイメージファイルの作成

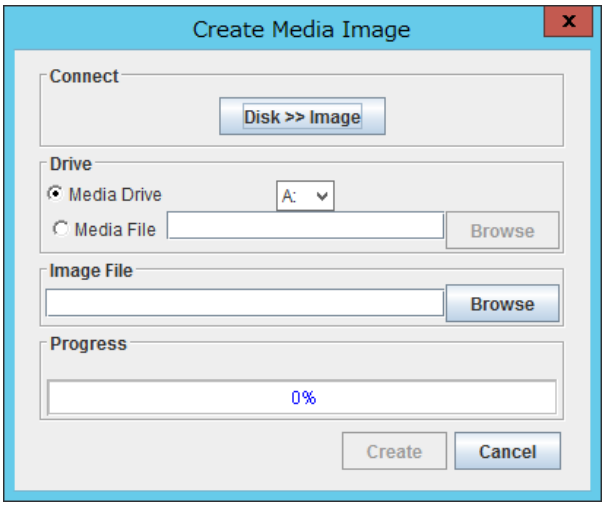
メディアイメージの作成機能では、ファイルまたは物理ディスク上のデータからディスクイメージファイルを作成することができます。

ISO-9660 ディスクイメージファイル（.img または.iso）を作成するには、以下の手順に従ってください。

手順

1. Java IRC を起動します。
2. **[Virtual Drive]→[Create Disk Image]**の順に選択します。

   [Create Media Image]ダイアログボックスが開きます。



3. **[Disk >> Image]**ボタンが表示されることを確認します。ボタンラベルが**[Image >> Disk]**の場合は、このボタンをクリックして**[Disk >> Image]**に変更します。
4. 次のいずれかを実行します。
   - ファイルを使用する場合は、**[Media File]**オプションを選択し、**[Browse]**をクリックして、使用するファイルに移動します。
   - 物理メディアを使用する場合は、**[Media Drive]**メニューで、フロッピー、USB キー、または CD-ROM のドライブ文字を選択します。
5. **[Image File]**テキストボックスに、イメージファイルのパスおよびファイル名を入力します。
6. **[Create]**をクリックします。

イメージの作成が完了すると、iLO によって通知されます。

7. **[Close]**をクリックして、**[Create Media Image]**ダイアログボックスを閉じます。
8. 指定した場所にイメージが作成されていることを確認します。

イメージファイルから物理ディスクへのデータのコピー

メディアイメージの作成機能では、ディスクイメージファイルからフロッピーディスクまたは USB キーにデータをコピーすることができます。IMG ディスクイメージファイルのみがサポートされます。CD-ROM にデータをコピーすることはできません。

ディスクイメージデータをフロッピーディスクまたは USB キーにコピーするには、以下の手順に従ってください。

手順

1. Java IRC を起動します。
2. **[Virtual Drive]**→**[Create Disk Image]**の順に選択します。
   [Create Media Image]ダイアログボックスが開きます。
3. **[Disk >> Image]**ボタンをクリックして、設定を**[Image >> Disk]**に変更します。
4. **[Media Drive]**メニューで、フロッピーまたは USB キーのドライブ文字を選択します。
5. **[Image File]**テキストボックスに、既存のイメージファイルのパスおよびファイル名を入力します。
   ディスクの作成が完了すると、iLO によって通知されます。
6. **[Close]**をクリックして**[Create Media Image]**ダイアログボックスを閉じます。
7. 指定した場所にファイルがコピーされたことを確認します。

仮想フォルダーの使用（.NET IRC 専用）

前提条件

この機能をサポートする iLO ライセンスがインストールされている。

手順

1. .NET IRC を起動します。
2. **[Virtual Drive]**→**[Folder]**の順に選択します。
3. **[**フォルダーの参照**]**ウィンドウで、使用するフォルダーを選択し、**[OK]**をクリックします。
   仮想フォルダーが、**[iLO Folder]**という名前でサーバーにマウントされます。

仮想フォルダー

仮想フォルダーを使用すると、ファイルにアクセスし、ファイルを参照し、クライアントから管理対象サーバーにファイルを転送できます。ローカルディレクトリまたはクライアント経由でアクセスできるネットワーク接続されたディレクトリのマウントとアンマウントを行うことができます。サーバーは、フォルダーまたはディレクトリの仮想イメージを作成した後で、そのイメージに USB ストレージデバイスとして接続するので、サーバーにアクセスし、iLO が生成したイメージファイルをサーバー上の任意の位置に転送できます。

この機能および他の多くの機能が、ライセンスパッケージに含まれています。

仮想フォルダーは読み取り専用であり、ここからは起動できません。マウントされたフォルダーは静的です。クライアントフォルダーに行った変更は、マウントされたフォルダーに複製されません。

12. 電力および温度機能の使用

サーバーの電源投入

iLO 5 を搭載した NX7700x サーバで AC 電源が失われた場合は、再びサーバーの電源を入れる前に約 30 秒待つ必要があります。この間に電源ボタンを押すと、電源ボタンが点滅し、要求が保留状態にあることを示します。

この遅延は、iLO ファームウェアのロード、認証、およびブートが行われているためです。iLO は、初期化の完了時に保留中の電源ボタン要求を処理します。サーバー電源が切断されていない場合、遅延はありません。30 秒の遅延は、iLO のリセット中のみ発生します。iLO が電源を管理できるようになるまで、電源ボタンは無効になります。

iLO が正常に起動しない場合、電源ボタンのウォッチドッグでは、ユーザーによる電源ボタンを使用したシステム電源の投入が許可されます。

iLO ファームウェアは管理対象電源システムをサポートするために、（たとえば、消費電力上限機能を使用して）電力しきい値を監視し、設定します。iLO が電源を管理できる前にシステムの起動を許可すると、複数のシステムで電圧低下、電圧消失、および温度過負荷が発生する場合があります。AC 電源が失われると電源管理状態が失われるので、電源管理状態を復元し、電源を投入できるように、最初に iLO を起動する必要があります。

消費電力上限機能は、「電力」ページにて「現在の電力読み取り値」に N/A 以外が表示されている場合に設定可能です。

電圧低下からの復旧

電圧低下条件は、動作中のサーバーへの電源が瞬間的に失われると発生します。電圧低下の期間およびサーバーハードウェアの構成によっては、電圧低下によりオペレーティングシステムが中断することがありますが、iLO ファームウェアは中断しません。

iLO は、電圧低下を検出し、電圧低下から復旧します。iLO が電圧低下の発生を検出すると、**[Always Power On]**が**[Always Remain Off]**に設定されていない場合、電源オン遅延の後でサーバー電源が復元されます。電圧低下の復旧後、iLO ファームウェアは、iLO イベントログに Brown-out recovery イベントを記録します。

安全なシャットダウン

iLO のプロセッサーが安全なシャットダウンを実行するには、オペレーティングシステムの協調動作が必要です。安全なシャットダウンを行うには、iLO ドライバーおよび ESMPRO/ServerAgentService または Agentless Management Service をロードする必要があります。iLO は OS のグレースフル(Graceful）シャットダウン時に iLO ドライバーを通して上記サービスと通信し、オペレーティングシステムを安全にシャットダウンするための適切な方法を実行して、データの完全性を確保します。

iLO ドライバーおよび上記サービスがロードされていない場合は、iLO は、オペレーティングシステムを適切にシャットダウンするために、物理的な電源ボタンを押す操作（iLO の**[Momentary Press]**）をエミュレートします。オペレーティングシステムの動作は、オペレーティングシステムの設定と電源ボタンを押す設定によって異なるため、事前に適切に設定することをお勧めします。

iLO ドライバーについて詳しくは、「iLO ドライバー」を参照してください。

システムユーティリティの高温シャットダウンオプションを使用して、自動シャットダウン機能を無効にできます。この構成では、物理的な損傷が発生する可能性がある極端な条件下の場合を除き、自動シャットダウンを無効にすることができます。

電力効率

iLO を使用すると、High Efficiency Mode(高効率モード)を使用して電力消費を改善できます。高効率モードは、セカンダリーパワーサプライを省電力モードに入れてシステムの電力効率を改善します。セカンダリーパワーサプライが省電力モードにある場合は、プライマリーパワーサプライがシステムにすべての DC 電力を供給します。各 AC 入力ワット数あたりの DC 出力ワット数が増えるため、パワーサプライがより効率的です。
システムがプライマリーパワーサプライの最大電力出力の 70%を超える電力を使用すると、セカンダリーパワーサプライが正常動作に戻ります（つまり、省電力モードから出ます）。消費電力がプライマリーパワーサプライの 60%未満の容量に低下すると、セカンダリーパワーサプライが省電力モードに戻ります。高効率モードを使用すると、プライマリーパワーサプライとセカンダリーパワーサプライの最大電力出力に等しい消費電力を実現し、低い消費電力レベルで改善された効率を維持することができます。

高効率モードは、電源の冗長性に影響しません。プライマリーパワーサプライに障害が発生した場合は、セカンダリーパワーサプライがただちにシステムへの DC 電力の供給を開始し、停止時間を防止します。

高効率モードは、システムユーティリティから設定する必要があります。これらの設定を iLO から変更することはできません。詳しくは、本体装置のメンテナンスガイドを参照してください。

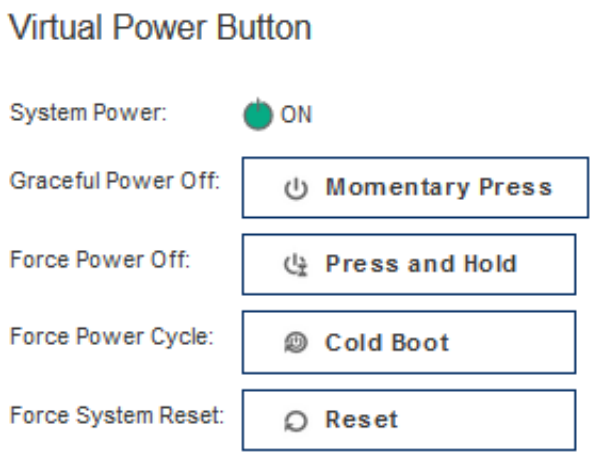
高効率モード設定は、**[Power & Thermal]**→**[Power]**ページに表示されます。

サーバー電源の管理

サーバー電源のページの**[Virtual Power Button]**セクションは、サーバーの現在の電源状態およびリモートサーバー電源制御オプションを表示します。**[System Power]**は、ページが初めて開かれるときのサーバー電源の状態を示します。サーバー電源の状態は、**[ON]**、**[OFF]**、または**[Reset]**のいずれかです。サーバー電源の現在の状態を表示するには、ブラウザーの更新機能を使用します。サーバーは、まれに**[Reset]**状態に入ることがあります。

前提条件
仮想電源およびリセット権限

手順
1. **[Power & Thermal]**→**[Server Power]**ページに移動します。



2. 次のいずれかのボタンをクリックします。
   - **[Momentary Press]**
   - **[Press and Hold]**
   - **[Cold Boot]**
   - **[Reset]**

   サーバーの電源が入っていない場合、**[Press and Hold]**、**[Cold Boot]**、および**[Reset]**は使用できません。
3. 要求を確認するメッセージが表示されたら、**[OK]** をクリックします。

仮想電源ボタンのオプション

- **[Momentary Press]** - 物理的な電源ボタンを押す場合と同じです。サーバーの電源がオフの場合、**[Momentary Press]**を押すとサーバーの電源がオンになります。

  一部のオペレーティングシステムでは、電源ボタンを一時的に押した後、適切なシャットダウンを開始するか、またはこのイベントを無視するように設定されていることがあります。仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して適切なオペレーティングシステムシャットダウンを完了することをおすすめします。
- **[Press and Hold]** - 物理的な電源ボタンを 5 秒間押し続け、離すことと同じです。

  サーバーはこの操作の結果、電源がオフになります。このオプションを使用すると、オペレーティングシステムの適切なシャットダウン機能に影響を与える可能性があります。
- **[Reset]** - サーバーを強制的にウォームブートします。CPU および I/O リソースはリセットされます。このオプションを使用すると、オペレーティングシステムの適切なシャットダウン機能に影響を与えます。
- **[Cold Boot]** - サーバーの電源を切断します。プロセッサー、メモリ、および I/O リソースは、メインの電力が失われます。サーバーは、約 6 秒後再起動します。このオプションを使用すると、オペレーティングシステムの適切なシャットダウン機能に影響を与えます。

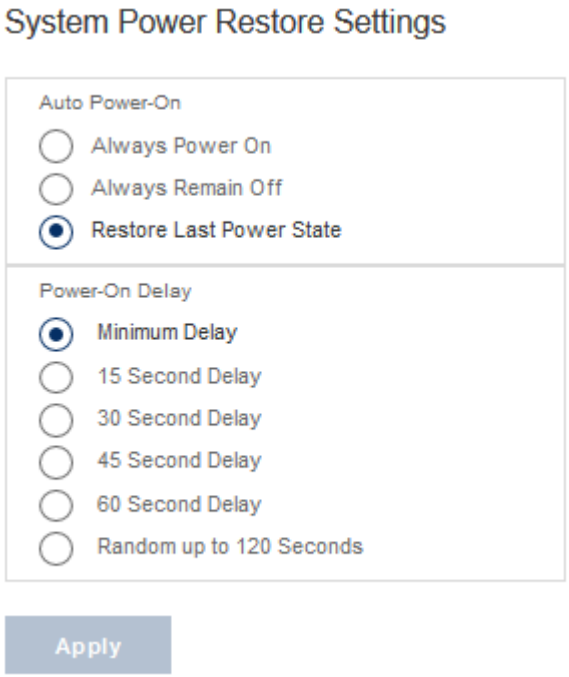
システム電源リストア設定

[System Power Restore Settings]セクションでは、電源が喪失した後のシステムの動作を制御できます。POST 実行中に、システムユーティリティを使用して、これらの設定を構成することもできます。

前提条件
iLO の設定を構成権限

手順

1. **[Power & Thermal]**→**[Server Power]**ページに移動します。



2. **[Auto Power-On]**の値を選択します。

   この設定は、たとえば、サーバーに電源ケーブルを接続した場合や電源障害の後で UPS がアクティブになった場合などの、電源の復元後の iLO の動作を制御します。
   以下のオプションを使用できます。

   - **[Always Power On]** -電源オン遅延時間が経過した後でシステムの電源オンにします。
   - **[Always Remain Off]** - サーバーは、手動でオンにされるまで電源オフのままになります。
   - **[Restore Last Power State]** - サーバーを、電源が失われたときの電源状態に戻します。サーバーがオン状態だった場合、電源がオンになります。サーバーがオフ状態だった場合、オフのままとなります。このオプションは、デフォルト設定です。

   [Auto Power-On]の変更は、次回のサーバーの再起動後に有効となります。

3. **[Power-On Delay]**の値を選択します。

この設定では、サーバーの自動電源投入を遅らせます。iLO の起動が完了した後、サーバーの電源をオンにする前の iLO の電源オン遅延時間を決定します。サポートされているサーバーでは、以下のオプションを使用できます。

- **[Minimum Delay]** - iLO の起動が完了した後に電源オンします。
- **[15 Second Delay]** - 電源投入を 15 秒遅らせます。
- **[30 Second Delay]** - 電源投入を 30 秒遅らせます。
- **[45 Second Delay]** - 電源投入を 45 秒遅らせます。
- **[60 Second Delay]** - 電源投入を 60 秒遅らせます。
- **[Random up to 120 Seconds]** - 電源投入遅延は、最大 120 秒までのランダムな値になります。

4. **[Apply]**をクリックします。

サーバー電力使用量の表示

電力メーターのページでは、最新のサーバー電力使用量を表示します。サーバーの電源がオフになると、電力履歴情報は収集されません。サーバーの電源がオフになっている期間を含むグラフを表示すると、グラフにはデータが収集されなかったことを示す空白が表示されます。

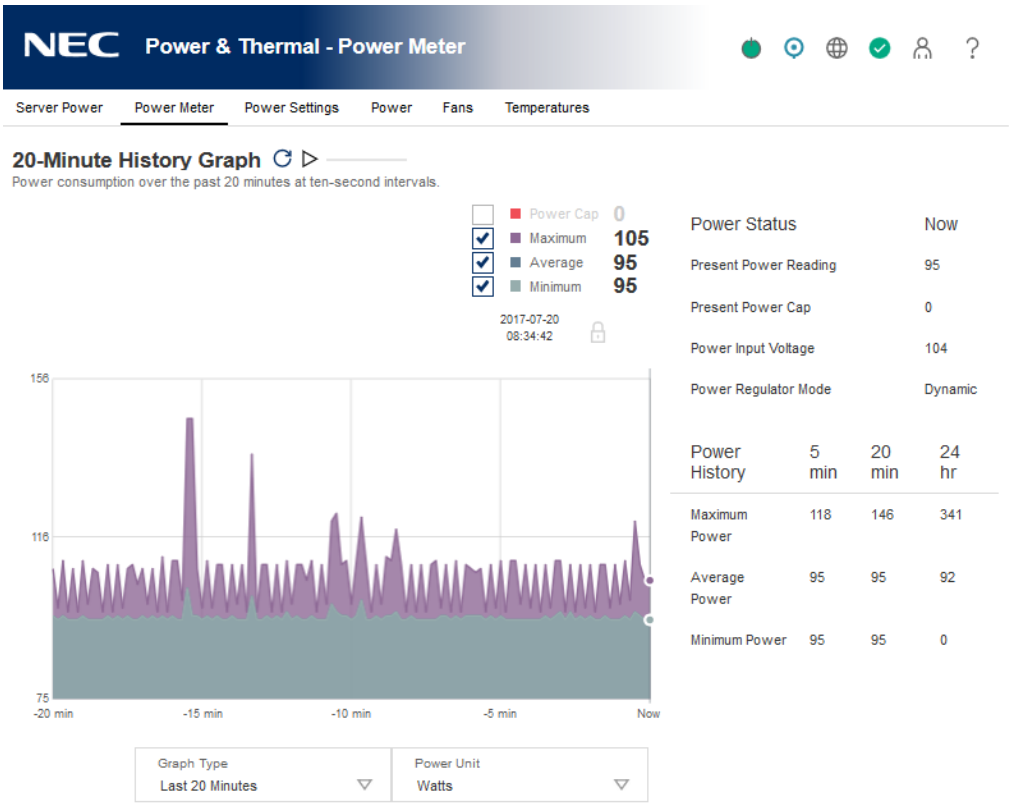
iLO がリセットされるか、サーバーの電源がオンされるとグラフデータは消去されます。また、仮想電源ボタンの**[Reset]**または**[Cold Boot]**の操作を使用してもデータが消去されます。

前提条件

この機能をサポートする iLO ライセンスがインストールされている。

手順

1. **[Power & Thermal]→[Power Meter]**ページに移動します。



2. **[Graph Type]**メニューでグラフタイプを選択します。
3. オプション：グラフの表示をカスタマイズするには、次のチェックボックスをチェックまたはクリアします。
   - **Power Cap**
   - **Maximum**
   - **Average**
   - **Minimum**
4. オプション：このページのデータを更新する方法を選択します。
   デフォルトでは、ページを開いたままにしてもページデータは更新されません。
   - すぐにページを更新するには、↻アイコンをクリックします。
   - ページを自動的に更新するには、▷アイコンをクリックします。□アイコンをクリックするか別のページに移動するまで、選択したグラフタイプに応じてページは 10 秒または 5 分間隔で更新されます。
5. オプション：電力読み取り値をワットまたは BTU/hr に変更するには、**[Power Unit]**メニューで値を選択します。
6. オプション：表示されるデータをグラフ上の特定のポイントにロックするには、目的のポイントにカーソルを移動してクリックします。カーソルのロックを解除するには、グラフをもう一度クリックするか、またはロックアイコンをクリックします。

サーバー電力使用量の表示オプション

グラフタイプ

- **[Last 20 Minutes]**- 過去 20 分間にわたるサーバーの電力使用量を示します。iLO ファームウェアは、電力使用量情報を、サーバーから 10 秒ごとに収集します。

- **[Last 24 hours]**- 過去 24 時間にわたるサーバーの電力使用量を示します。iLO ファームウェアは、電力使用量情報を、サーバーから 5 分ごとに収集します。

ヒント: 特定のポイントのその時点での電力消費を表示するには、グラフにマウスカーソルを重ねます。

グラフデータ

以下のチェックボックスを使用して、電力メーターグラフに含まれるデータをカスタマイズします。

- **[Power Cap]** - サンプル中に設定されている消費電力上限。消費電力上限データは電力メーターグラフに赤色で表示されます。
  - 消費電力上限は、長期間の平均消費電力を制限します。
  - 消費電力上限は、サーバーの再起動時に維持されないため、起動時に一時的なスパイクが発生します。
  - 消費電力上限値を、最大電力とアイドル時の電力の差の 50%未満に設定すると、サーバー内の変化によりサーバーにアクセスできなくなることがあります。消費電力上限値を 20%未満に設定することはおすすめいたしません。システム構成に対して低すぎる消費電力上限値を設定すると、システムの性能が低下する可能性があります
- **[Maximum]** - サンプル中の瞬間最高電力。iLO は、秒未満の単位でこの値を記録します。最大電力データは電力メーターグラフに紫色で表示されます。
- **[Average]** - サンプル中の電力測定値の平均。平均電力データは、電力メーターグラフに青色で表示されます。
- **[Minimum]** - ある測定期間で観測された最小値。20 分間のグラフでは、10 秒ごとの平均測定値の最小値が表示されます。24 時間のグラフでは、5 分間の平均値より低い最小値が表示されます。最小電力データは電力メーターグラフにグレーで表示されます

電力メーターグラフの更新

- すぐにページを更新するには、アイコンをクリックします。
- ページを自動的に更新するには、アイコンをクリックします。アイコンをクリックするか別のページに移動するまで、選択したグラフタイプに応じてページは 10 秒または 5 分間隔で更新されます。

電力単位の表示

電力読み取り値をワットまたは BTU/時に変更するには、電力単位リストで値を選択します。

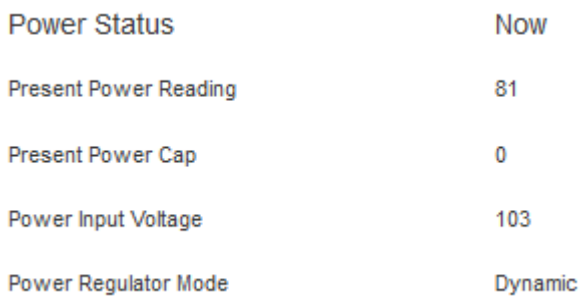
電力メーターロックアイコン

1. 自動更新が実行されていない場合、ロックアイコンをクリックするか、グラフ上の任意のポイントをクリックすると、グラフ上の特定のポイントで表示がロックされます。
2. 自動更新が実行されている場合、ロック機能を使用すると、x軸に沿った特定の履歴ポイントに対応するデータポイントが表示されます。たとえば、20 分間のグラフでは、-10 分で表示をロックすると、グラフが更新されるたびに 10 分前の値が表示されます。

現在の電源状態の表示

手順

1. **[Power & Thermal]→[Power Meter]** ページに移動します。



Power Status	Now
Present Power Reading	81
Present Power Cap	0
Power Input Voltage	103
Power Regulator Mode	Dynamic

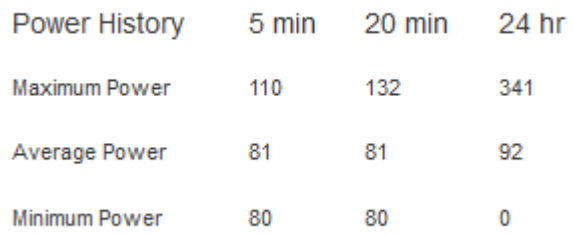
現在の電源状態の詳細

[Power Status]テーブルに表示される情報は、サーバータイプによって変化します。

- **[Present Power Reading]** - サーバーからの現在の電力読み取り値。この値は、すべてのサーバーについて表示されます。
- **[Present Power Cap]** - サーバーに対して設定されている消費電力上限。消費電力上限が設定されていない場合、この値は 0 です。
- **[Power Input Voltage]** - サーバー用に指定された入力電圧。
- **[Power Regulator Mod]** - 設定されているパワーレギュレーターモード。設定できる内容については、「電力設定」を参照してください。

サーバー電力履歴の表示

1. **[Power & Thermal]→[Power Meter]**ページに移動します。



Power History	5 min	20 min	24 hr
Maximum Power	110	132	341
Average Power	81	81	92
Minimum Power	80	80	0

電力履歴の詳細

[Power History]テーブルには、5 分、20 分、24 時間の 3 つの期間で電力読み取り値を表示します。

- **[Maximum Power]** - 指定された期限でのサーバーからの最大電力測定値。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の最大値になります。
- **[Average Power]** - 指定された期限での電力測定値の平均。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の平均になります。
- **[Minimum Power]** - 指定された期限でのサーバーからの最小電力測定値。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の最小値になります。

複数の電源装置がサーバーから同時に削除されると、**[Power History]**セクションまたは**[Power Meter]**グラフに情報が表示されない短い期間があります。この情報は、搭載されている残りの電源装置に関する情報が収集された後、再度表示されます。

電力設定

電力設定のページを使用すると、サーバーの電力管理機能を表示および制御することができます。このページに表示される電力管理機能は、サーバーの構成によって変化します。

パワーレギュレーターの設定

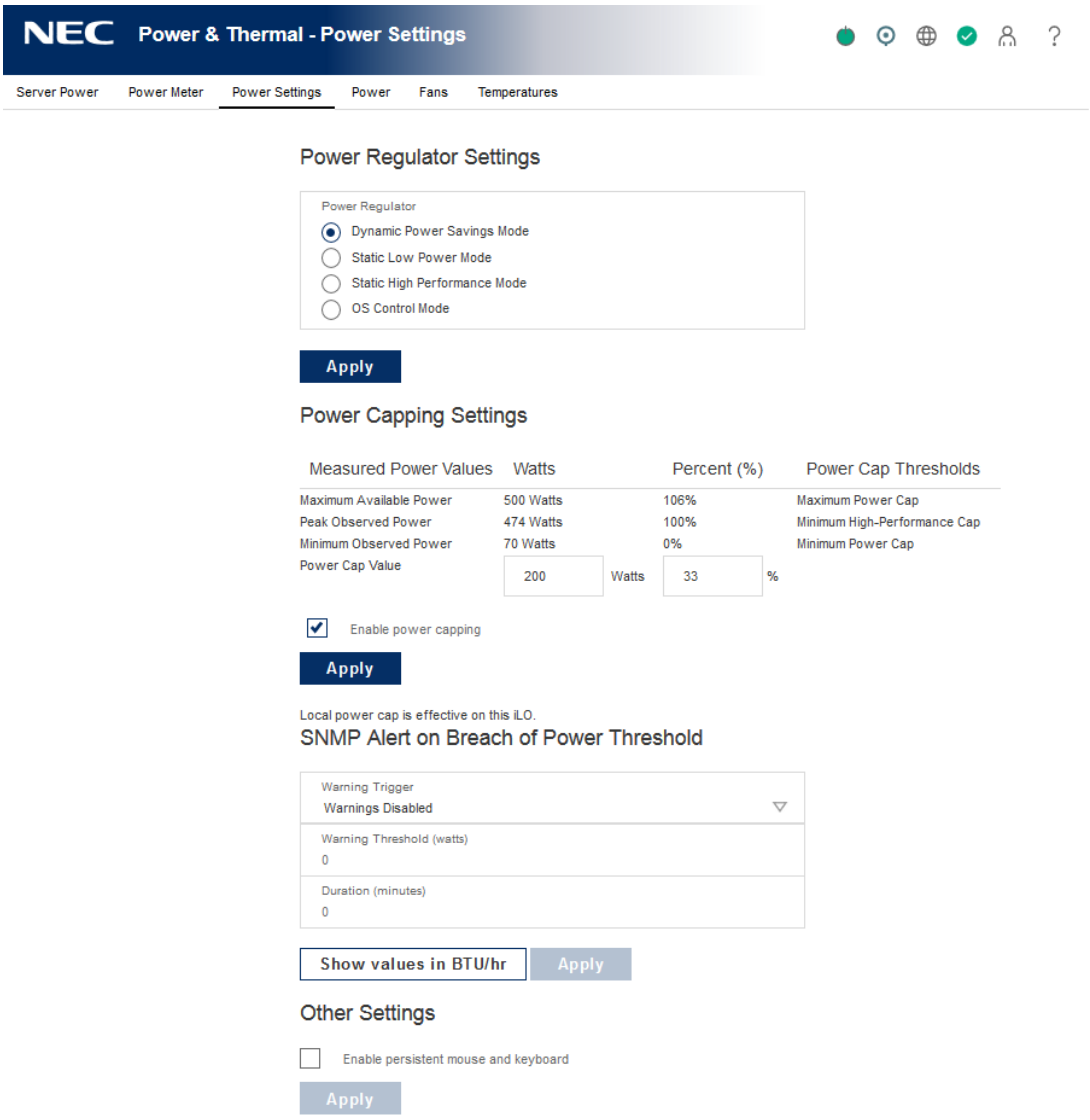
パワーレギュレーター機能を使用すると、iLO は動作条件に基づいてプロセッサーの周波数レベルと電圧レベルを動的に変更できます。これにより、パフォーマンスへの影響を最小限に抑えながら電力を節約することができます。電力設定のページを使用すると、パワーレギュレーターモードを表示または制御することができます。

前提条件

- iLO の設定を構成権限
- iLO Advanced または iLO Scale-Out ライセンスがインストールされている。
  NX7700x シリーズサーバには、iLO Advanced ライセンスが標準でインストールされています。
- サーバーが POST 実行中でない。サーバーの POST 実行中は、パワーレギュレーター設定を変更できません。

手順

1. **[Power & Thermal]**→**[Power Settings]**ページに移動します。



2. パワーレギュレーターモードを選択します。
3. **[Apply]**をクリックします。
   - **[Dynamic Power Savings Mode]**、**[Static Low Power Mode]**、および**[Static High Performance Mode]**設定の場合、iLO は、パワーレギュレーターの設定が変更されたことを通知します。
   - **[OS Control Mode]**設定の場合、iLO は、パワーレギュレーター設定の変更を完了するにはサーバーの再起動が必要であることを通知します。

   [Apply]をクリックしても設定が変化しない場合は、サーバーがブート処理中か、リブートが必要な場合があります。動作している ROM ベースのプログラムを終了し、POST を完了させてから、再試行します。
4. 再起動が必要であることが表示される場合は、サーバーを再起動します。

パワーレギュレーターモードの詳細

パワーレギュレーターを設定するときに、以下のモードから選択します。

- **[Dynamic Power Savings Mode]** - プロセッサーの利用率に基づいてプロセッサー速度と電力使用量を自動的に変化させます。このオプションにより、パフォーマンスに影響を与えず

に全体的な消費電力を減らすことができます。このオプションは、OS のサポートを必要としません。

- **[Static Low Power Mode]** - プロセッサー速度を下げ、電力使用量を減らします。
  このオプションは、システムの最大電力量を低く抑えます。
- **[Static High Performance Mode]** - OS の電力管理ポリシーに関係なく、プロセッサーは常に最大電力/パフォーマンスで動作します。
- **[OS Control Mode]** - OS が電力管理ポリシーを有効にしない場合、プロセッサーは常に最大電力/パフォーマンスで動作します。

消費電力上限の設定

前提条件

- iLO の設定を構成権限
- iLO Advanced または iLO Scale-Out ライセンスがインストールされている。
  NX7700x シリーズサーバには、iLO Advanced ライセンスが標準でインストールされています。
- 本体装置が消費電力上限をサポートしている。消費電力上限機能は、「電力」ページにて「現在の電力読み取り値」に N/A 以外が表示されている場合に設定可能です。

手順

1. **[Power & Thermal]→[Power Settings]**ページに移動します。
2. **[Power Capping Settings]**セクションで**[Enable power capping]**チェックボックスを選択します。
3. **[Power Cap Value]**をワット数、BTU/hr、または割合（%）で入力します。

   割合（%）は、最大電力値と最小電力値の差です。

   消費電力上限値は、サーバーの最小電力値以下に設定できません。
4. オプション：値がワット単位で表示されている場合、BTU/hr 単位での表示に変更するには**[Show values in BTU/hr]**をクリックします。値が BTU/hr で表示されている場合、ワット単位での表示に変更するには**[Show values in Watts]**をクリックします。
5. **[Apply]**をクリックします。

   変更が正常に終了したことが iLO によって通知されます。

消費電力上限の注意事項

- POST 実行中、ROM は最大電力測定値と最小電力測定値を決定する 2 つの電力テストを実行します。

  消費電力上限の設定を決定するときは、**[Power Capping Settings]**の表の値を検討してください。
- **[Maximum Available Power]** - サーバーのパワーサプライ容量。これは、**[Maximum Available Power]**のしきい値です。サーバーはこの値を超えてはなりません。

- **[Peak Observed Power]** - サーバーの最大電力測定値。この値は**[Minimum High-Performance Cap]**のしきい値で、現在の構成でサーバーが使用する最大電力を表します。この値に設定されている消費電力上限は、サーバーのパフォーマンスに影響を与えません。
- **[Minimum Observed Power]** - サーバーの最小電力測定値。これは、**[Minimum High-Performance Cap]**しきい値で、サーバーが使用する最小電力を表します。この値に設定されている消費電力上限は、サーバーの電力使用量を最小化するため、その結果サーバーのパフォーマンスが低下します。
- 消費電力上限を設定した場合は、サーバーの平均電力測定値が、消費電力上限以下にならなければなりません。
- 消費電力上限は、一部のサーバーではサポートされていません。詳しくは、サーバーの仕様を確認してください。消費電力上限機能は、「電力」ページにて「現在の電力読み取り値」に N/A 以外が表示されている場合に設定可能です。

SNMP アラートの設定

電力設定のページの**[SNMP Alert on Breach of Power Threshold]**セクションを使用すると、定義されたしきい値を消費電力が超えたときに SNMP アラートを送信できます。

前提条件
iLO の設定を構成権限

手順
1. **[Power & Thermal]→[Power Settings]**ページに移動します。
2. **[Warning Trigger]**リストで値を選択します。
   警告トリガーは、警告が、ピーク時消費電力に基づくか、平均消費電力に基づくか、または無効かを決定します。
3. **[Warning Trigger]**リストで、**[Peak Power Consumption]**または**[Average Power Consumption]**を選択した場合は、次を入力します。
   - **[Warning Threshold]** - 消費電力しきい値を設定します。指定期間にわたって消費電力がこの値を超える場合、SNMP アラートがトリガーされます。
   - **[Duration]** - SNMP アラートがトリガーされるまでに消費電力が警告しきい値を超えていなければならない時間を分単位で設定します。生成される SNMP アラートは、iLO がサンプリングした電源使用量のデータに基づいています。**[Duration]**の値が変更された正確な日時には基づいていません。設定可能な最大時間は 240 分で、持続時間は 5 の倍数でなければなりません。
4. **[Apply]**をクリックして設定を保存します。

マウスとキーボードの持続接続の設定

電力設定のページの**[Other Settings]**セクションを使用すると、キーボードとマウスの持続接続の機能を有効または無効にすることができます。

この機能を有効にすると、iLO 仮想キーボードとマウスが、iLO UHCI USB コントローラーに常時接続されます。この機能を無効にすると、リモートコンソールアプリケーションが開いて iLO

に接続したときにのみ、iLO 仮想キーボードおよびマウスが動的に接続されます。この機能を無効にすると、一部のサーバーでは、サーバーオペレーティングシステムがアイドル状態で仮想 USB キーボードおよびマウスが接続されていないときに、さらに 15W の電力節約が可能になります。

たとえば、24 時間当たりの電力節約は 15W×24 時間、つまり 360Wh（0.36kWh）になります。

前提条件

iLO の設定を構成権限

手順

1. **[Power & Thermal]→[Power Settings]**ページに移動します。
2. **[Enable persistent mouse and keyboard]**チェックボックスを選択またはクリアします。デフォルトでは無効になっています。
3. **[Apply]**をクリックして設定を保存します。

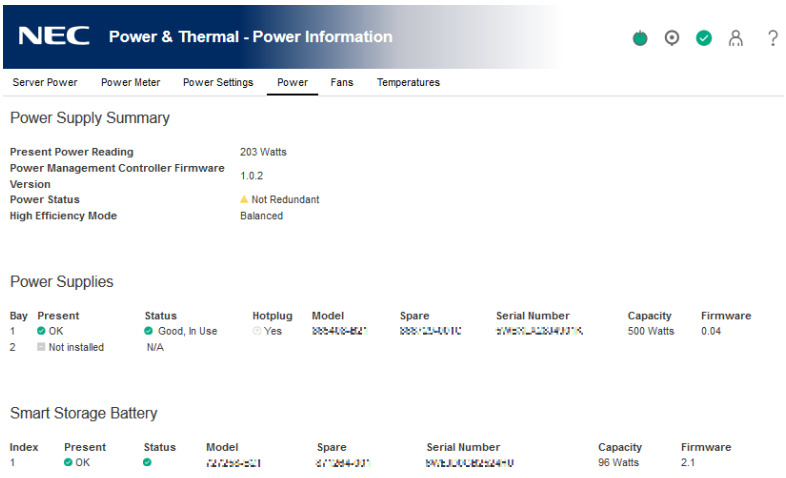
   変更が正常に終了したことが iLO によって通知されます。

電力情報の表示

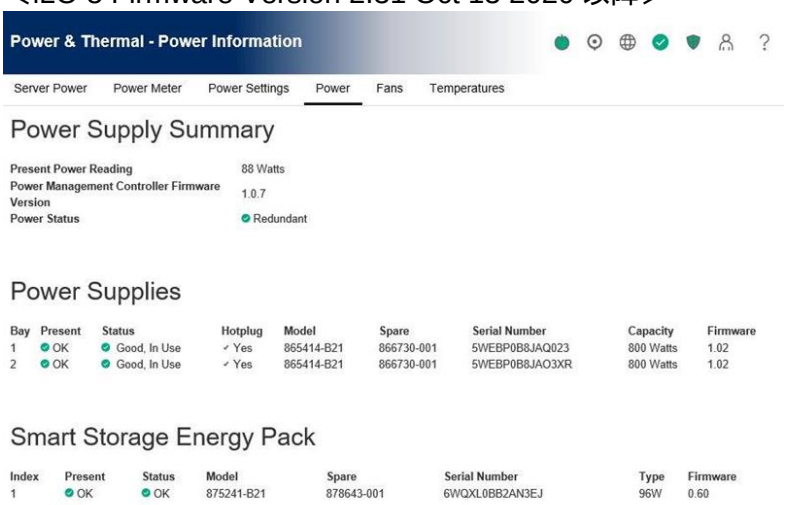
手順

[Power & Thermal]ページに移動し、**[Power]**タブをクリックします。

＜iLO 5 Firmware Version 2.18 Jun 22 2020 以前＞



＜iLO 5 Firmware Version 2.31 Oct 13 2020 以降＞



電力情報のページには、**[Power Supply Summary]**、**[Power Supplies]**、および**[Smart Storage Battery]**（搭載サーバーのみ）の各セクションが表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、電源オフする前の状態です。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみ更新されます。

電源ユニット概要の詳細

- **[Present Power Reading]** – 現在の電力読み取り値。パワーサプライスロットに電源ユニットが取り付けられている場合、サーバーからの最新の電力読み取り値が表示されます。他のパワーサプライは、このデータを提供しません。
  この値は、通常、すべてのアクティブなパワーサプライの出力の合計に等しくなりますが、個々のパワーサプライを読み取るため、多少変動する場合があります。この値はあくまで参考であり、電力メーターのページに表示される値ほど正確ではありません。詳しくは、「サーバー電力使用量の表示」を参照してください。

- **[Power Management Controller Firmware Version]** – パワーマネージメントコントローラーのファームウェアのバージョン。iLO ファームウェアがこの値を決定するには、サーバーの電源が入っている必要があります。この機能は、一部のサーバーでは使用できません。
- **[Power Status]** – サーバーに供給される電力の全体的なステータス。このセクションにはサーバー内部の電源ユニットのステータスが表示されます。
  以下の **Power Status** 値が表示されます。
  - **[Redundant]** -電源ユニットに冗長性があることを示します。
  - **[Not Redundant]** -電源ユニットの少なくとも 1 つがサーバーに電力を供給していないことを示します。このステータスの最もよくある原因は、パワーサプライへの入力電源の喪失です。
  - **[OK]** - 取り付けられている電源ユニットは正常に動作しています。
  - **[N/A]** –電源装置は一つだけ搭載されています。この構成では冗長化を適用できません。
- **[High Efficiency Mode]** – 高効率モード。冗長化パワーサプライが構成されている場合、使用される冗長化パワーサプライモード。
  値には、以下のものがあります。
  - **[N/A]** - 該当なし。
  - **[Balanced Mode]** - 取り付けられているすべてのパワーサプライに均一に電力が供給されます。
  - **[High Efficiency Mode (Auto)]** - 片方のパワーサプライには完全に電力を供給し、もう一方のパワーサプライは低い消費電力レベルでスタンバイ状態にします。**Auto** オプションではサーバーのシリアル番号に基づいて奇数の電源ユニットか偶数の電源ユニットが選ばれるため、ほぼランダムに電力が供給されます。
  - **[High Efficiency Mode (Even Supply Standby)]** - 奇数番号のパワーサプライには完全に電力を供給し、偶数番号のパワーサプライは低い消費電力レベルでスタンバイ状態にします。
  - **[High Efficiency Mode (Odd Supply Standby)]** - 偶数番号のパワーサプライには完全に電力を供給し、奇数番号のパワーサプライは低い消費電力レベルでスタンバイ状態にします。
  - **[Not Supported]** - 取り付けられているパワーサプライは高効率モードをサポートしていません。

詳細情報

電源の監視

High Efficiency Mode(高効率モード)

電源ユニットのリスト

このリストの一部の値について情報を提供しない電源ユニットもあります。電源ユニットからの情報がない場合は、**[N/A]**が表示されます。

- **[Bay]** - 電源ユニットのベイ番号。

- **[Present]** -電源ユニットが搭載されているかどうか。表示される値は、**[OK]**および**[Not Installed]**です。
- **[Status]** -電源ユニットのステータス。表示される値は、ステータスアイコン（**[OK]**、**[Degraded]**、**[Failed]**、または**[Other]**）、および詳細情報を提供するテキストを示します。値には、以下のものがあります。
  - **[Unknown]** - 不明
  - **[Good, In Use]** - 良好、使用中
  - **[Good, Standby]** - 良好、スタンバイ
  - **[General Failure]** - 一般障害
  - **[Over Voltage Failure]** - 過電圧障害
  - **[Over Current Failure]** - 過電流障害
  - **[Over Temperature Failure]** - 過熱障害
  - **[Input Voltage Lost]** - 入力電圧消失
  - **[Fan Failure]** - ファン障害
  - **[High Input A/C Warning]** - 高入力 A/C 警告
  - **[Low Input A/C Warning]** - 低入力 A/C 警告
  - **[High Output Warning]** - 高出力警告
  - **[Low Output Warning]** - 低出力警告
  - **[Inlet Temperature Warning]** - インレット温度警告
  - **[Internal Temperature Warning]** - 内部温度警告
  - **[High Vaux Warning]** - 高電圧補助電源警告
  - **[Low Vaux Warning]** - 低電圧補助電源警告
  - **[Mismatched Power Supplies]** - 電源装置の不一致
- **[Hotplug]** – パワーサプライスロットがサーバーの電源が入った状態での電源ユニットの交換をサポートするかどうか。値が **Yes** で、電源ユニットが冗長化されている場合は、サーバーの電源がオンのときにパワーサプライを取り外したり、交換したりすることができます。
- **[Model]** -電源ユニットのモデル番号。
- **[Spare]** - スペアの電源ユニットの部品番号。
- **[Serial Number]** -電源ユニットのシリアル番号。
- **[Capacity]** -電源ユニットの容量（W）。
- **[Firmware]** -搭載された電源ユニットのファームウェアバージョン。

Smart Storage バッテリーの詳細

Smart Storage バッテリーを搭載するサーバーでは、以下の詳細が表示されます。

- **[Index]** - バッテリーのインデックス番号。
- **[Present]** - バッテリーが搭載されているかどうか。表示される値は、**[OK]**および**[Not Installed]**です。
- **[Status]** - バッテリーのステータス。表示される値は、**[OK]**、**[Degraded]**、**[Failed]**または**[Other]**です。
- **[Model]** - バッテリーのモデル番号。
- **[Spare]** - スペアバッテリーの製品番号。
- **[Serial Number]** - バッテリーのシリアル番号。
- **[Capacity]** - バッテリーの容量。
- **[Firmware]** - 搭載されているバッテリーのファームウェアバージョン。

注記：**[Power & Thermal]**-**[Power]**タブの**[Smart Storage Battery]**の**[Capacity]**の表示において、96W、または 12W が表示されますが、この値はバッテリーの容量を示すものではなく、バッテリタイプを示します。

電源の監視

iLO ファームウェアは、サーバーとオペレーティングシステムの稼動時間が最大になるように、サーバーの電源ユニットを監視します。電源ユニットは低電圧などの電気条件や、不注意で AC コードが外れた場合に、影響を受ける可能性があります。このような状況によって、冗長電源が構成されている場合は冗長性を失い、冗長電源構成を使用していない場合はシステムが動作しなくなる可能性があります。電源ユニットの障害の検出（ハードウェア障害）時や、AC 電源コードの切断時には、イベントが IML に記録され、STATUS ランプに表示されます。

High Efficiency Mode(高効率モード)

高効率モードは、２個目の電源ユニットをスタンバイモードにすることにより、サーバーの電力効率を改善します。２個目の電源ユニットがスタンバイモードにある場合は、１個目の電源ユニットがシステムにすべての電力を供給します。電源ユニットの出力レベルが高いほど電源ユニットの効率が上がり（AC 入力電力当たりの DC 出力電力が増加し）、全体的な電力効率が向上します。

高効率モードは、電源の冗長性に影響しません。１個目の電源ユニットに障害が発生した場合は、２個目の電源ユニットがただちにシステムへの DC 電力の供給を開始し、システムが停止するのを防ぎます。冗長電源モードは、システムユーティリティを通じてのみ構成できます。これらの設定は iLO ファームウェアから変更することはできません。サポートされていないモードを使用するように高効率モードが構成されている場合、電源ユニット効率が低下する可能性があります。

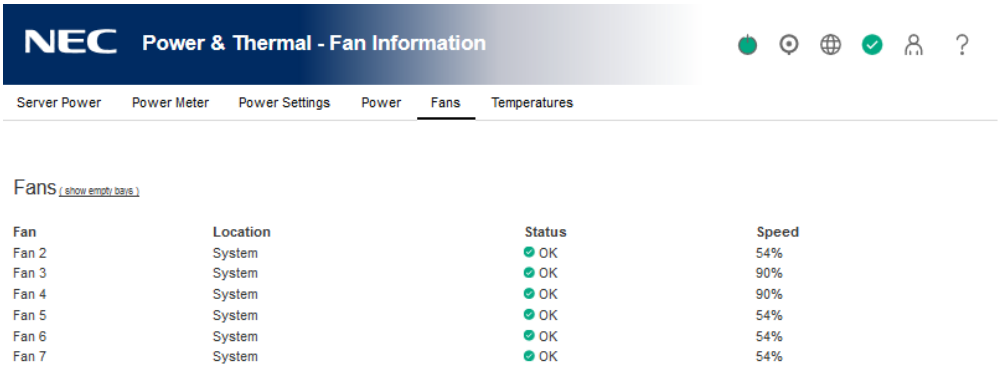
△注記:

- 本機能は、iLO 5 Firmware Version 2.18 Jun 22 2020 以前のバージョンで表示されますが、iLO 5 Firmware Version 2.31 Oct 13 2020 以降では表示されません。
- BIOS/Platform Configuration (RBSU)で、現在値の参照及び設定変更ができます。（[System Configuration] - [BIOS/Platform Configuration (RBSU)] - [Power and Performance Options] - [Advanced Power Options] に移動して、[Redundant Power Supply Mode]で設定値の参照・変更をします。）

ファン情報の表示

手順

1. **[Power & Thermal]**ページに移動し、**[Fans]**タブをクリックします。
2. オプション：冷却ファンの冗長をサポートしているサーバーでは空のファンベイは表示されません。ファンベイを表示するには、**[show empty bays]**をクリックします。空のファンベイが表示されているときにそれらを非表示にするには、**[show empty bays]**をクリックします。



ファン情報ページに表示される情報は、サーバー構成によって異なります。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、電源オフする前の状態です。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみ更新されます。

ファンの詳細

ファンごとに、次の詳細が表示されます。

- **[Fan]** - ファンの名前。
- **[Location]** - ブレード以外のサーバーの場合、サーバーシャーシ内の位置が表示されます。サーバーブレードの場合、位置が**[Virtual]**の仮想ファンが表示されます。
- **[Status]** - ファンのヘルスステータス。
  詳しくは、「サブシステムおよびデバイスのステータスの値」を参照してください。
- **[Speed]** - ファン速度（%）。

ファン

iLO ファームウェアは、ハードウェアと連携してファンの動作と速度を制御します。ファンはコンポーネントの重要な冷却機能を提供し、システムの信頼性向上と継続動作を補助します。システム全体を対象に監視した温度に対応する最小の騒音で十分な冷却機能を提供します。

ファンサブシステムの監視には、十分な構成、冗長化および非冗長化のファン構成が含まれます。1 つまたは複数のファンが故障しても、サーバーは動作を続けるのに十分な冷却機能を提供します。

ファンの動作ポリシーは、ファンの構成や冷却の必要性に応じて、サーバーごとに異なります。ファンの制御はシステムの内部温度を考慮し、温度を下げるときはファンの回転速度を上げ、十

分に下がったときはファンの回転速度を落とします。ファンの障害が発生した場合、ファンの動作ポリシーによっては、他のファンの回転速度を上げ、イベントを IML に記録し、STATUS ランプを点灯させたりします。
非冗長化構成または冗長化構成で複数のファンに障害が発生すると、システムの損傷を防ぎ、データの整合性を保証するために十分な冷却機能を提供できなくなる可能性があります。この場合、冷却ポリシー設定によって、オペレーティングシステムとサーバーの適切なシャットダウンが開始することもできます。

温度情報の表示

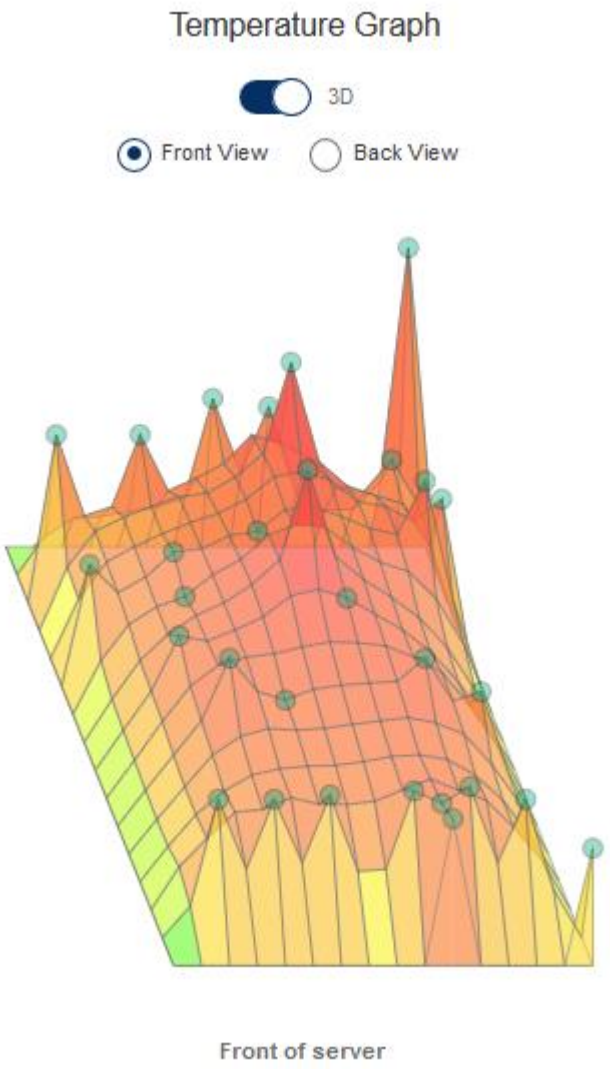
[Temperatures]ページには、温度グラフとテーブルがあります。このテーブルは、サーバーシャーシ内の温度センサーの位置、ステータス、温度、およびしきい値設定を表示します。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、電源オフする前の状態のです。サーバーの電源が投入され、POST の実行が完了した場合にのみ、ヘルス情報が更新されます。

温度グラフの表示

手順

1. **[Power & Thermal]**ページに移動し、**[Temperatures]**タブをクリックします。



2. オプション：グラフ表示をカスタマイズします。
   - **[3D]**トグルボタンを選択して、3 次元グラフを表示します。
   - **[3D]**トグルボタンをクリアして、2 次元グラフを表示します。
   - **[Front View]**または**[Back View]**を選択して、サーバーの前面または背面にあるセンサーを表示します。
3. オプション：マウスカーソルをグラフ上の円に移動すると、個々のセンサーの詳細が表示されます。
   センサーID、ステータス、および温度測定値が表示されます。

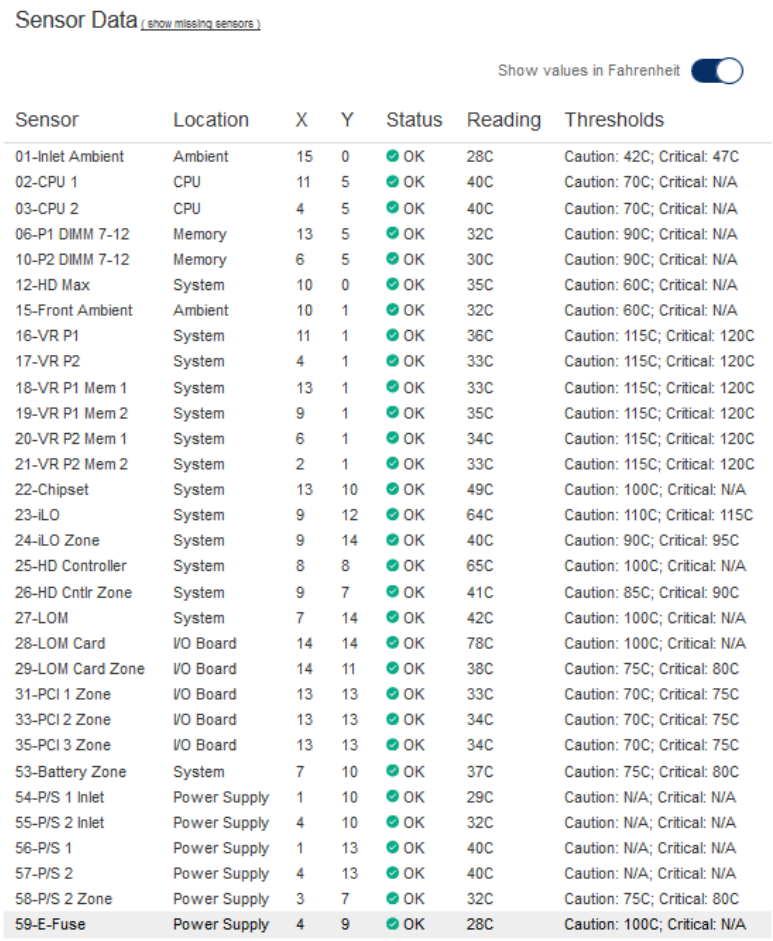
温度グラフの詳細

温度グラフを表示する場合、グラフ上の円形は、**Sensor Data** テーブルに示されるセンサーに対応します。グラフ上の色は、温度変化の程度によって緑色から赤色の範囲で示されます。緑色は温度 0°C、赤色は**クリティカル**しきい値を表します。センサーの温度が上がると、グラフの色が緑色からオレンジ色に変わり、さらに温度が上がって**クリティカル**しきい値に近づくと赤色になります。

温度センサーデータの表示

手順

1. **[Power & Thermal]**ページに移動し、**[Temperatures]**タブをクリックします。



Sensor	Location	X	Y	Status	Reading	Thresholds
01-Inlet Ambient	Ambient	15	0	OK	28C	Caution: 42C; Critical: 47C
02-CPU 1	CPU	11	5	OK	40C	Caution: 70C; Critical: N/A
03-CPU 2	CPU	4	5	OK	40C	Caution: 70C; Critical: N/A
06-P1 DIMM 7-12	Memory	13	5	OK	32C	Caution: 90C; Critical: N/A
10-P2 DIMM 7-12	Memory	6	5	OK	30C	Caution: 90C; Critical: N/A
12-HD Max	System	10	0	OK	35C	Caution: 60C; Critical: N/A
15-Front Ambient	Ambient	10	1	OK	32C	Caution: 60C; Critical: N/A
16-VR P1	System	11	1	OK	36C	Caution: 115C; Critical: 120C
17-VR P2	System	4	1	OK	33C	Caution: 115C; Critical: 120C
18-VR P1 Mem 1	System	13	1	OK	33C	Caution: 115C; Critical: 120C
19-VR P1 Mem 2	System	9	1	OK	35C	Caution: 115C; Critical: 120C
20-VR P2 Mem 1	System	6	1	OK	34C	Caution: 115C; Critical: 120C
21-VR P2 Mem 2	System	2	1	OK	33C	Caution: 115C; Critical: 120C
22-Chipset	System	13	10	OK	49C	Caution: 100C; Critical: N/A
23-iLO	System	9	12	OK	64C	Caution: 110C; Critical: 115C
24-iLO Zone	System	9	14	OK	40C	Caution: 90C; Critical: 95C
25-HD Controller	System	8	8	OK	65C	Caution: 100C; Critical: N/A
26-HD Cntlr Zone	System	9	7	OK	41C	Caution: 85C; Critical: 90C
27-LOM	System	7	14	OK	42C	Caution: 100C; Critical: N/A
28-LOM Card	I/O Board	14	14	OK	78C	Caution: 100C; Critical: N/A
29-LOM Card Zone	I/O Board	14	11	OK	38C	Caution: 75C; Critical: 80C
31-PCI 1 Zone	I/O Board	13	13	OK	33C	Caution: 70C; Critical: 75C
33-PCI 2 Zone	I/O Board	13	13	OK	34C	Caution: 70C; Critical: 75C
35-PCI 3 Zone	I/O Board	13	13	OK	34C	Caution: 70C; Critical: 75C
53-Battery Zone	System	7	10	OK	37C	Caution: 75C; Critical: 80C
54-P/S 1 Inlet	Power Supply	1	10	OK	29C	Caution: N/A; Critical: N/A
55-P/S 2 Inlet	Power Supply	4	10	OK	32C	Caution: N/A; Critical: N/A
56-P/S 1	Power Supply	1	13	OK	40C	Caution: N/A; Critical: N/A
57-P/S 2	Power Supply	4	13	OK	40C	Caution: N/A; Critical: N/A
58-P/S 2 Zone	Power Supply	3	7	OK	32C	Caution: 75C; Critical: 80C
59-E-Fuse	Power Supply	4	9	OK	28C	Caution: 100C; Critical: N/A

2. オプション：温度が摂氏単位で表示されているときは、**[Show values in Fahrenheit]**ボタンをクリックすると、温度が華氏で表示されます。温度が華氏で表示されている場合に、摂氏に表示を変更するには、**[Show values in Celsius]**ボタンをクリックします。
3. オプション：デフォルトでは、取り付けられていないセンサーは非表示です。取り付けられていないセンサーを表示するには、**[show missing sensors]**をクリックします。取り付けられていないセンサーが表示されている場合に、それらを非表示にするには、**[hide missing sensors]**をクリックします。

温度センサーの詳細

- **[Sensor]** - 温度センサーの ID。センサーの位置も示します。
- **[Location]** - 温度が測定されている領域。
  この列で Memory とは、以下の内容を指します。
  - 物理メモリ DIMM 上にある温度センサー。

- メモリ DIMM のすぐ近くにあるが DIMM 上ではない温度センサー。これらのセンサーは、追加の温度情報を提供するために、DIMM の近くの通気冷却経路をさらに下った場所に配置されています。

[Sensor]列の温度センサーの ID は、温度センサーの正確な位置を示し、DIMM またはメモリ領域に関する詳細な情報を提供します。

- **[X]** - 温度センサーの x 座標。
- **[Y]** - 温度センサーの y 座標。
- **[Status]** - 温度ステータス。
- **[Reading]** - 温度センサーによって記録された温度。温度センサーが取り付けられていない場合、**Reading** 列には **N/A** という値が表示されます。
- **[Threshold]** - 温度の警告・異常と判断するしきい値です。**Caution** と **Critical** の 2 つのしきい値が示されます。温度センサーが取り付けられていない場合、**Threshold** 列には **N/A** という値が表示されます。

温度の監視

次の温度しきい値が監視されます。

- **[Caution]** - サーバーは、温度を「警告」しきい値未満に維持するように設計されています。

  温度が警告しきい値を超えると、ファンの回転速度が最大になります。

  温度が警告しきい値を 60 秒間超えると、適切なサーバーシャットダウンが試行されます。
- **[Critical]** - 温度が制御不能になった場合または急上昇した場合、高温によってコンポーネントの障害が発生する前に、**クリティカル**温度しきい値によりサーバーを強制的にシャットダウンしてシステム障害の発生を防ぎます。

監視ポリシーはサーバーの要件によって異なります。ポリシーには通常、冷却機能を最大化するためのファンの回転速度の増加、IML の温度イベントのログ記録、STATUS ランプを使用したイベントの視覚的な表示、データの破損を防ぐためのオペレーティングシステムの適切なシャットダウンの開始が行われます。

温度超過状態の回復後は、ファンの回転速度を通常に回復、IML へのイベントの記録、STATUS ランプの正常化、シャットダウンを実行中の場合はその停止などの追加のポリシーが実施されます。

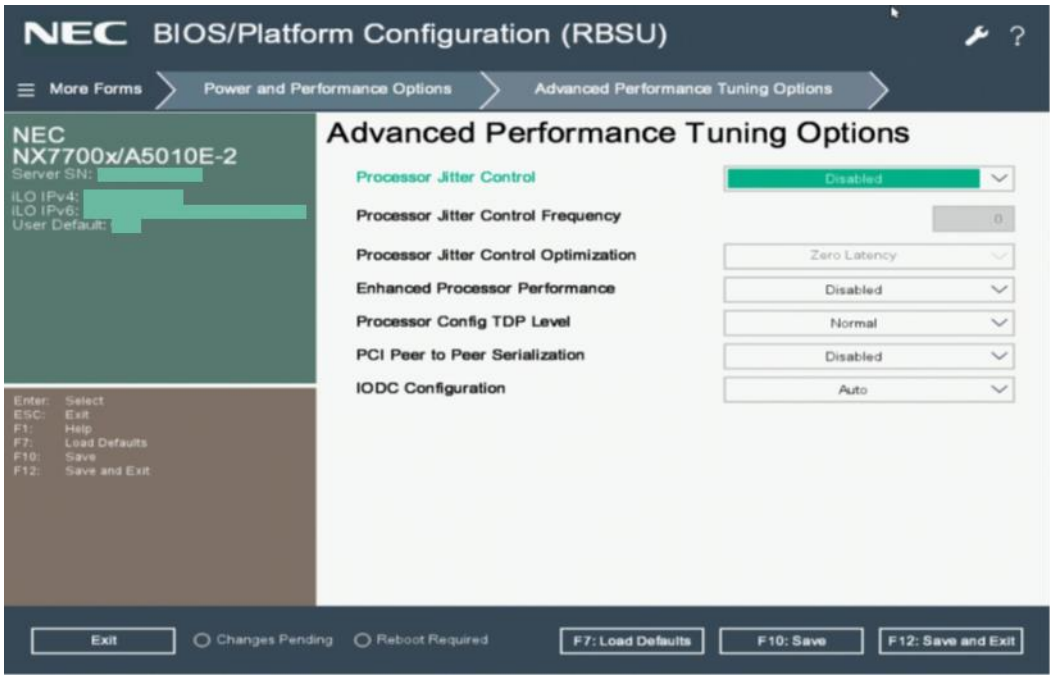
13. Intelligent System Tuning/パフォーマンス[19]

Intelligent System Tuning/パフォーマンスは、以下の機能で構成されます。本機能を使用するためには、iLO Advanced ライセンスが必要です。また、各設定はサーバーの電源がオンされてからPOST 完了後に変更可能です。

- **[Jitter Smoothing]** -周波数変動（ジッター）を最小化することで、ターボ・ブースト有効時に発生する遅延問題を解決します。
- **[Workload Matching]** - 設定済みのサーバープロファイルを使用して、アプリケーションパフォーマンスを最大化します。
- **[Core Boosting]** - アクティブコア間のパフォーマンスを高めるためにこの機能を使用します。**[Core Boosting]**を有効にすると定格周波数より高い性能動作し、処理遅延やばらつきを排除することができます。特定のインテルプロセッサーを搭載した特定のサーバーのみです。対象のサーバーに関しては、本体装置のユーザーガイドを参照してください。

[Jitter Smoothing]設定は、BIOS の System Utilities にも同じ設定があります。BIOS 側で設定変更した場合、iLO で表示される設定値も変わります。

BIOS の**[System Utilities]** - **[System Configuration]** - **[BIOS/Platform Configuration (RBSU)]** - **[Power and Peroformance Options]** - **[Advanced Performance Tuning Options]** - **[Processor Jitter Control]**からも設定可能です。



19 iLO 5 Firmware Version 2.10 Oct 30 23 2019 以降

Jitter Smoothing 設定の構成

前提条件

本機能を使用するには iLO Advanced ライセンスが必要です。
NX7700x シリーズサーバには、iLO Advanced ライセンスが標準でインストールされています。

- iLO の設定を構成権限
- パワーレギュレーターが OS コントロール以外のモードに設定されている。
- サーバーが Innovation Engine をサポートしている。Innovation Engine をサポートしていないサーバーでは、**[Intelligent System Tuning]/[Performance]**[20]ページは表示されません。Innovation Engine がサポートされているかどうかを確認するには、**[Firmware & OS Software]** - **[Firmware]**で Innovation Engine ファームウェアを検索します。
- 1.2.4 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
- 1.20 以降のバージョンのシステム ROM（BIOS）がインストールされている。プロセッサージッター制御最適化設定を使用するには、システム ROM（BIOS）1.40 以降のバージョンが必要です。
- サーバーの電源が入っており、POST が完了している。

手順

1. ナビゲーションツリーで**[Intelligent System Tuning]/[Performance]**[21]をクリックします。
2. **[Settings]**をクリックします。
3. **[Processor Jitter Control Mode]**を選択します。
4. **[Processor Jitter Control Frequency(in MHz)]**を入力します。
5. **[Processor Jitter Control Optimization]**を選択します。
6. **[Apply]**をクリックします。iLO に、変更の確認を求めるメッセージが表示されます。
7. **[Yes]**をクリックします。

Jitter Smoothing オプション

Processor Jitter Control Mode

サポートされるサーバー上のプロセッサージッター制御機能によって、プロセッサージッター（Jitter Smoothing）が軽減または削除されます。使用できる設定は、次のとおりです。

- **[Auto]** - 周波数の変化を監視し、長期的な変動を最小限に抑えるように周波数を自動的に調整します。
- **[Manual]** - プロセッサーを固定周波数で動作させ、ユーザーが低い周波数または高い周波数を静的に選択できるようにします。
- **[Disabled]** - プロセッサーのジッター制御を無効にします。

20 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

21 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

Processor Jitter Control Frequency (in MHz)

プロセッサージッター制御モードが自動または手動に設定されている場合は、この値を入力します。

- **[Auto]**に構成されている場合は、開始周波数単位を MHz で入力します。許容される最大速度を指定するには、0 を入力します。
- **[Manual]**に構成されている場合は、周波数単位を MHz で入力します。

値は 0〜10000 で入力できます。サポートされる周波数範囲はプロセッサーモデルによって異なります。通常は、1,000 MHz〜4,000 MHz の範囲内になります。

周波数が MHz 単位で入力され、システムファームウェアにより、プロセッサーで可能な最も近い周波数間隔に切り上げられます。たとえば、Intel Xeon スケーラブルプロセッサーは、100 MHz の間隔でプログラミングする周波数をサポートしています。ユーザーが 2,050 MHz と入力すると、インストールされているプロセッサーでサポートされている場合は、結果として得られる周波数は 2,100 MHz になります。

Processor Jitter Control Optimization

- [**Optimized For Throughput**] - しきい値とポーリング率は、スループットが最大になるようにプログラムされます。
- [**Optimized For Latency**] - しきい値とポーリング率は、低レイテンシになるようにプログラムされます。
- [**Zero Latency**] - しきい値とポーリング率は、ゼロレイテンシになるようにプログラムされます。

Workload Matching(ワークロードプロファイル)

サーバーのパフォーマンスを向上させるには、以下のシステム生成のワークロードプロファイルを使用します。

[General Power Efficient Compute] - 最も一般的なパフォーマンスと電源管理の設定を適用します。BIOS 設定をチューニングしないでワークロードに一致させるユーザーにお勧めします。

[General Peak Frequency Compute] - 個々のコアに可能な最大周波数を達成するパフォーマンスと電力管理設定を適用します。計算時間の短縮による恩恵を受けるワークロードにお勧めします。

[General Throughput Compute] - 最大合計持続スループットを達成するパフォーマンスと電力管理設定を適用します。NUMA（不均一メモリアクセス）の認識をサポートするように最適化されています。

[Virtualization - Power Efficient] - すべての仮想化オプションを有効にするパフォーマンスの設定を適用します。電源設定を管理して、仮想化を妨げないようにします。仮想化環境にお勧めします。

[Virtualization - Max Performance] - すべての仮想化オプションを有効にするパフォーマンスの設定を適用します。最適なパフォーマンスを実現する電源設定を無効にします。仮想化環境にお勧めします。

[Low Latency] - 速度とスループットの低減を適用し電力管理を無効にして、全体的なコンピューティング遅延を低減します。RTOS（リアルタイムオペレーティングシステム）のワークロード、または遅延の影響を受けやすい他のワークロードにお勧めします。

[Mission Critical] - 高度なメモリ RAS（信頼性、可用性、および保守性）機能を管理します。このプロファイルは、基本的なサーバーのデフォルト値を上回るサーバー信頼性とパフォーマンスの妥協点を探る顧客によって使用されるためのものです。

[Transactional Application Processing] - 最大周波数とスループットを管理します。バックエンドデータベースを必要とする OLTP（オンライントランザクション処理）アプリケーションを使用する環境を処理する場合にお勧めします。

[High Performance Compute (HPC)] - 持続する使用可能な帯域幅とプロセッサーの演算能力を最適化する電力管理を無効にします。従来の HPC 環境を実行するユーザーにお勧めします。

[Decision Support] - このプロファイルは、データマイニングや OLAP（オンライン分析処理）など、データウェアハウスに対する操作またはアクセスに焦点を合わせたエンタープライズビジネスデータベース（ビジネスインテリジェンス）のワークロードを対象にしています。

[Graphic Processing] - 電力管理と仮想化を無効にして、I/O とメモリ間の帯域幅を最適化します。GPU（グラフィックス処理ユニット）を使用するサーバーで実行するワークロードにお勧めします。

[I/O Throughput] - I/O とメモリ間のリンクに影響を与える電力管理機能を無効にします。I/O とメモリ間の最大帯域幅に依存する構成にお勧めします。

[Custom] - ワークロードのプロファイルを無効にします。特定の BIOS オプションを設定するユーザーにお勧めします。

コアブーストオプション(Core Boosting)

- **[Enabled] -** コアブーストを有効にすると、サーバーは、コアブースト対応プロセッサーの強化されたパフォーマンス機能を使用できます。有効化は、コアブーストプロセッサーがサーバーにインストール済みであることが検出されたときのデフォルト値です。
- [**Disabled**] - コアブーストを無効にすると、プロセッサーではターボ周波数プロファイルが制限され、最大電力容量が低下します。

Intelligent System Tuning/パフォーマンス[22]構成の表示

サーバーが POST 中の場合、このページの情報は、最後に電源が切れた時点の情報になります。Intelligent System Tuning 情報は、サーバーの電源が入っており、POST が完了している場合にのみ更新されます。

前提条件

22 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
- サーバーが Innovation Engine をサポートしている。Innovation Engine をサポートしていないサーバーでは、Intelligent System Tuning ページは表示されません。Innovation Engine がサポートされているかどうかを確認するには、インストール済みファームウェアページで Innovation Engine ファームウェアを検索します。
- サーバーの電源が入っており、POST が完了している。

手順

1. ナビゲーションツリーで**[Intelligent System Tuning]/[Performance]**[23]をクリックします。
2. iLO には、**[Jitter Smoothing]**、**[Workload Matching]**、および**[Core Boosting]**の各設定が表示されます。
3. **[Jitter Smoothing]**のプロセッサージッター制御周波数設定には、**[Current Jitter Control Frequency]**と**[Configured Jitter Control Frequency]**の両方が表示されます。

23 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

Intelligent System Tuning/パフォーマンス[24]のパフォーマンス監視/監視[25]

[Performance Monitoring]/[Monitoring][26]ページでは、Innovation Engine のサポートによってサーバーの以下のセンサーから収集されたパフォーマンスデータが表示されます。OS や装置構成によっては、未サポートの情報があります。

- **[CPU Utilization]**

  このセンサーは、システムに搭載されているすべてのプロセッサーの使用率を表示します。測定値は、プロセッサーの最大演算能力のパーセンテージに基づいて、プロセッサー動作時の動作速度が考慮されます。この測定値は、オペレーティングシステムが報告する値とは異なる場合があります。

- **[Memory Bus Utilization]**

  このセンサーは、メモリバスの総帯域幅の使用率を表示します。測定値は、構成時の最大メモリ帯域幅のパーセンテージに基づいています。この測定値は、オペレーティングシステムが報告する値とは異なる場合があります。

- **[I/O Bus Utilization]**

  このセンサーは、I/O バスに接続されているすべてのプロセッサー（PCI-e バス総帯域幅）の使用率を表示します。この測定値は、それらのバスの最大総帯域幅のパーセンテージに基づいています。この測定値は、I/O デバイスのビジー状態の程度を示すものではなく、デバイスが使用している PCI-e 帯域幅の量を示すものです。

- **[CPU Interconnect Utilization]**

  このセンサーは、システム内の複数のプロセッサーソケットを接続するインターコネクトの帯域幅使用率を表示します。

- **[Jitter Count]**

  このセンサーは、毎秒発生するプロセッサー周波数の変化または jitter の割合を表示します。

- **[Average CPU Frequency]**

  このセンサーは、全体の平均的なプロセッサー周波数を表示します。ゼロの値は、プロセッサーがアイドル状態であることを意味し、この値は、プロセッサーがアイドル状態でない場合のみ周波数を測定する一部のオペレーティングシステムで見られる「実行時の周波数」とは異なります。

- **[CPU Power]**

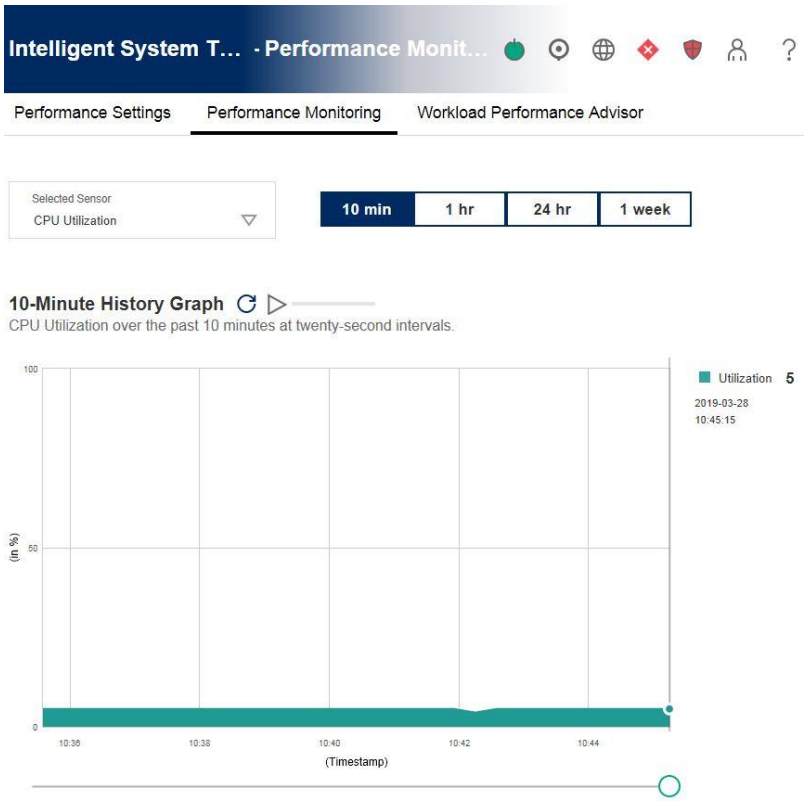
24 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

25 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

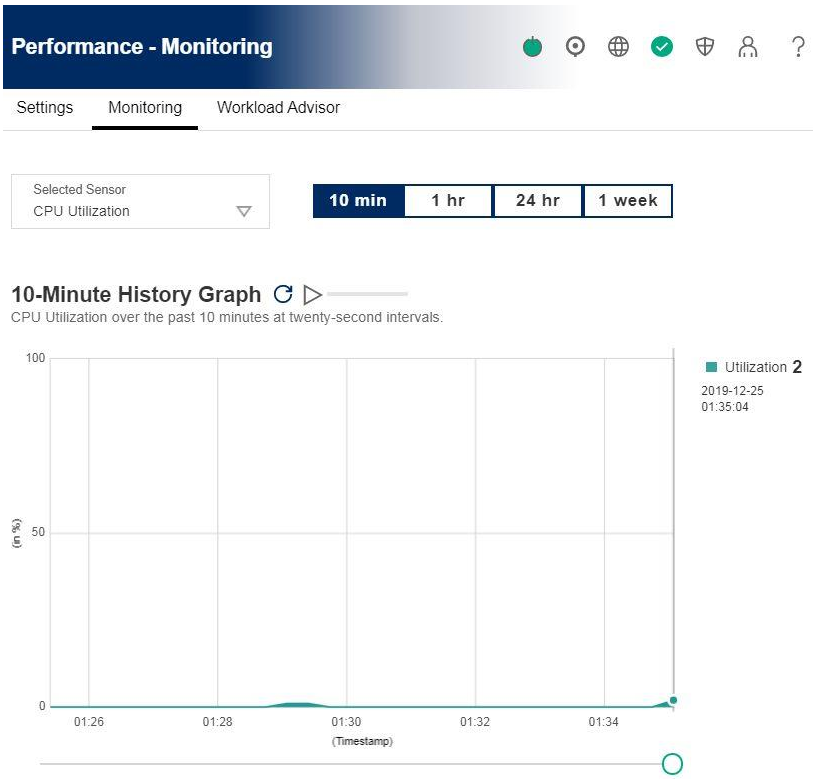
26 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

このセンサーは、プロセッサーが消費する電力を表示します。これはプロセッサー内の電力アキュムレータに基づいており、プロセッサーが電力制限の内部調整に使用する値です。

パフォーマンスデータの表示



- iLO 5 Firmware Version 2.10 Oct 30 2019 以降



パフォーマンス監視グラフに、Innovation Engine ファームウェアから収集された最新のデータが表示されます。

サーバーが電源オフまたは POST 状態のとき、メッセージが表示され、パフォーマンス測定値に 0 の値が表示されます。サーバーの電源がオンで POST が完了していると、パフォーマンスデータが更新されます。リセット後、グラフの値が 0 の場合がありますが、これはサーバーがオフまたは POST のときにデータが収集されていなかったことになります。

iLO リセット後

- 10 分および 1 時間間隔のパフォーマンスデータがクリアされます。
- 24 時間および 1 週間グラフのデータが保存され、リセットが完了した後に表示されます。
- リセットが完了した後で 24 時間および 1 週間のグラフを表示すると、毎時のデータがなくなっている場合があります。

前提条件

- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
- 2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。バージョンは、**[Firmware & OS Software]**-**[Firmware]**ページで確認できます。
- **[iLO Date/Time]**が正しく設定されている。

手順

1. ナビゲーションツリーで**[Intelligent System Tuning]**/**[Performance]**[27]をクリックし、**[Performance Monitoring]**/**[Monitoring]**[28]タブをクリックします。
2. **[Selected Sensor]**メニューでセンサーを選択します。
3. 次のいずれかでグラフ間隔を選択します。
   - 10 min
   - 1 hr
   - 24 hr
   - 1 week

   グラフには、選択した間隔でデータが表示されます。
4. オプション：グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー○ を目的のポイントに移動させます。
   スライダーを動かすと、グラフ上の選択ポイントの詳細情報がグラフの右横に表示されます。
5. オプション：**[CPU Power]**または**[Average CPU Frequency]**を選択した場合、グラフの横にある CPU リスト内のチェックボックスをオンまたはオフにします。

27 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

28 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

CPU のチェックボックスを選択すると、グラフに表示されます。CPU のチェックボックスをクリアすると、非表示になります。

6. オプション：このページでデータを更新する方法を選択します。
   デフォルトでは、ページを開いた後はページのデータは更新されません。
   - ページをただちに更新するには、↻をクリックします。.
   - ページの自動更新を開始するには、▷をクリックします。選択したグラフのタイプに応じて、ページは 10 秒または 5 分間隔で更新されます。□をクリックするか別のページに移動するまで、ページは更新されます。

パフォーマンスデータの詳細

パフォーマンスデータセクションには、次の詳細が表示されます。

- **[Sensor]** - 選択したセンサーの名前。
- **[Maximum]** - 最大測定値。単位は、選択されたセンサーの種類によって異なります。
- **[Minimum]** - 最小測定値。単位は、選択されたセンサーの種類によって異なります。

パフォーマンス監視のグラフ表示オプション

選択したセンサーのリスト

センサーのパフォーマンスデータを表示するには、**[Selected Sensor]**メニューでセンサーを選択します。

グラフタイプ

グラフタイプのオプションをクリックすると、グラフタイプが選択されます。

- **[10 min]** - 直近の 10 分間のパフォーマンスデータを表示します。iLO ファームウェアは、20 秒ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプル最大数は 30 です。
- **[1 hr]** - 直近の 1 時間のパフォーマンスデータを表示します。iLO ファームウェアは、20 秒ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプル最大数は 180 です。
- **[24 hr]** - 直近の 24 時間のパフォーマンスデータを表示します。iLO ファームウェアは、5 分ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプル最大数は 288 です。
- **[1 week]** - 先週のパフォーマンスデータを表示します。iLO ファームウェアは、30 分ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプル最大数は 336 です。

パフォーマンスグラフの更新

- ページをすぐに更新するには、↻をクリックします。.
- ページの自動更新を開始するには、▷をクリックします。.
- □をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

グラフ上に特定のデータポイントを表示

- グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー〇を目的のポイントに移動します。
  次の方法でスライダーを移動することもできます。
  - スライダートラックをクリックします。
  - スライダーアイコンをクリックし、キーボードの矢印キーを押します。

  スライダーを動かすと、グラフ上の選択ポイントの詳細がグラフの横に表示されます。

- 自動更新の実行時に、グラフの下にあるスライダー〇を動かすと、x 軸方向の特定の履歴ポイントに該当するデータポイントに焦点が当たります。

パフォーマンスアラートの構成

設定されたしきい値に達した場合に IML にイベントを登録するパフォーマンスアラート設定ができます。

[CPU Utilization] 、**[Memory Bus Utilization]**、および**[I/O Bus Utilization]**センサーにおいて、上限と下限のしきい値がサポートされます。

[CPU Interconnect Utilization] 、**[Jitter Count]**、および**[CPU Power]**センサーにおいて、上限しきい値がサポートされます。

前提条件

- iLO の設定を構成権限
- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
- 2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
  バージョンは、**[Firmware & OS Software]**-**[Firmware]**ページで確認できます。
- [**iLO Date/Time**]が正しく設定されている。

手順

1. ナビゲーションツリーで**[Intelligent System Tuning]**/**[Performance]**[29]をクリックし、**[Performance Monitoring]**/**[Monitoring]**[30]タブをクリックします。
2. パフォーマンスアラートをサポートするセンサーを選択します。
3. **[Lower Threshold]**と**[Dwell Time (in sec)]**を入力し、**[Apply]**をクリックします。
   アラートを無効にするには、**[Dwell Time (in sec)]**を 0 に設定します。

29 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

30 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

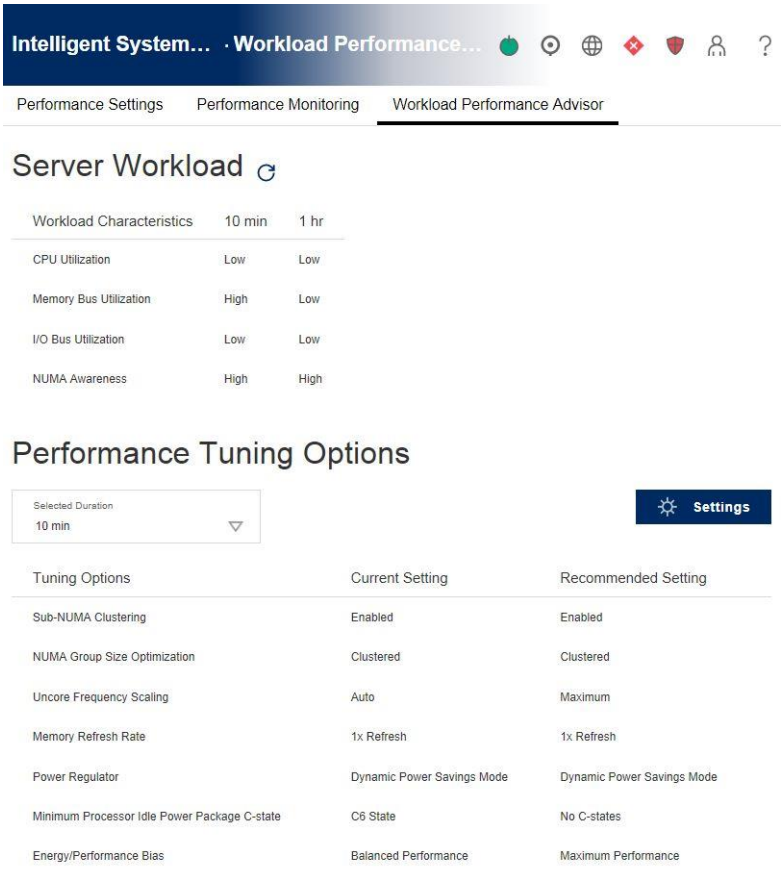
パフォーマンスアラートの設定オプション

- **[Lower Threshold]** - イベントが IML に登録される際の最小値。
  使用率のパーセンテージ(in %)を入力します。
- **[Upper Threshold]** - イベントが IML に登録される際の最大値。
  - 使用率のセンサーの場合は、選択したセンサーの使用率のパーセンテージ(in %)を入力します。
  - **[CPU Power]** センサーの場合は、値をワット単位(in Watts)で入力します。
  - **[Jitter Count]** センサーの場合は、しきい値カウント(in Count)を入力します。
- **[Dwell Time]** - 測定値がしきい値を上回ったまたは下回った滞留期間を秒数で指定します。
  指定された秒数間、しきい値を上回るまたは下回ると、イベントが IML に登録されます。
  たとえば、しきい値上限を 70%、滞留時間を 40 秒に設定した場合、センサーが 70% を超える測定値を 40 秒を超えて報告するとイベントが報告されます。
  - アラートを有効にするには、20〜64800（20 秒〜18 時間）の範囲で、滞留時間を 20 の倍数の有効な値に設定します。20 の倍数でない値を入力した場合、値は次の 20 の倍数に切り上げられます。
  - アラートを無効にするには、滞留時間を 0 に設定します。

Intelligent System Tuning/Performance[31]のワークロードパフォーマンスアドバイザー/ワークロードアドバイザー[32]

iLO は選択したサーバーワークロード特性を監視し、監視対象のデータに基づいてパフォーマンス調整の推奨設定を提供します。

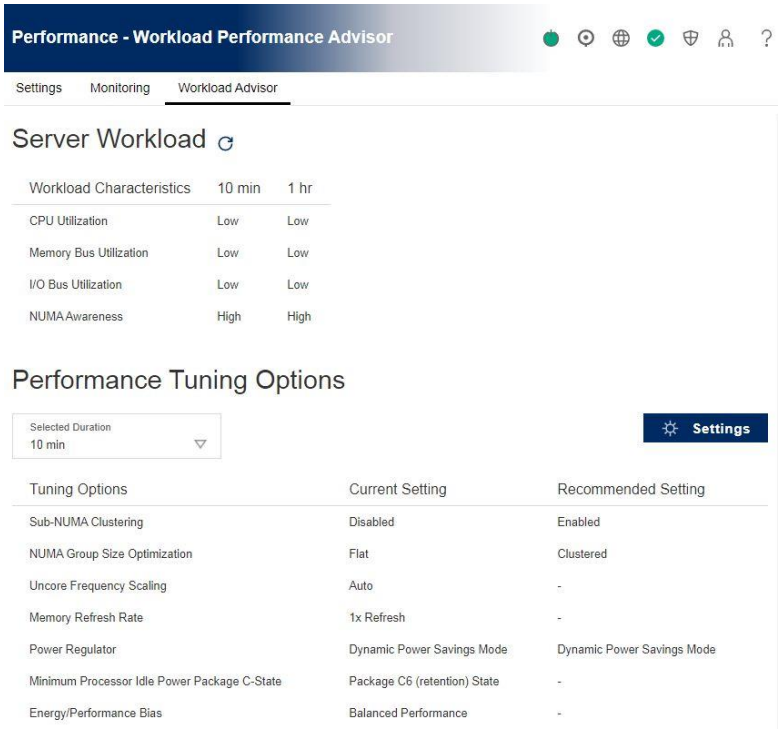
サーバーワークロード詳細の表示



31 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

32 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

- iLO 5 Firmware Version 2.10 Oct 30 2019 以降



前提条件

- ホスト BIOS 構成権限
- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
- サーバーの電源が入っており、POST が完了している。
  監視する時間間隔でサーバーの電源が入れられたことを確認します。たとえば、24 時間間隔のデータは、サーバーの電源が 24 時間入っていないと表示されません。
- 2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
  バージョンは、**[Firmware & OS Software]-[Firmware]**ページで確認できます。
- **[iLO Date/Time]**が正しく設定されている。

手順

1. ナビゲーションツリーで**[Intelligent System Tuning] [Performance]**[33]をクリックし、**[Workload Performance Advisor]/[Workload Advisor]**[34]をクリックします。
2. 詳細を**[Server Workload]**セクションで確認します。
   iLO がリセットされた場合、10 分間隔の情報はサーバーの電源が 10 分入れられた後で、1 時間間隔の情報はサーバーの電源が 1 時間入れられた後で表示されます。
3. オプション：↻をクリックして、ページを最新情報に更新します。

33 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

34 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

サーバーワークロードの詳細

ワークロード特性とは、ワークロードがシステムリソースをどのように使用しているかに関する定量的評価です。これらはパフォーマンス監視イベントから得た定量的な測定値に基づいており、チューニング決定の際に参考として役立ちます。このように観測された特性が、通常はインテリジェントなチューニング決定を行う際に必要となります。たとえば、特定の BIOS オプションがメリットをもたらすのはワークロードの**[NUMA Awareness]**が高い場合に限られます。

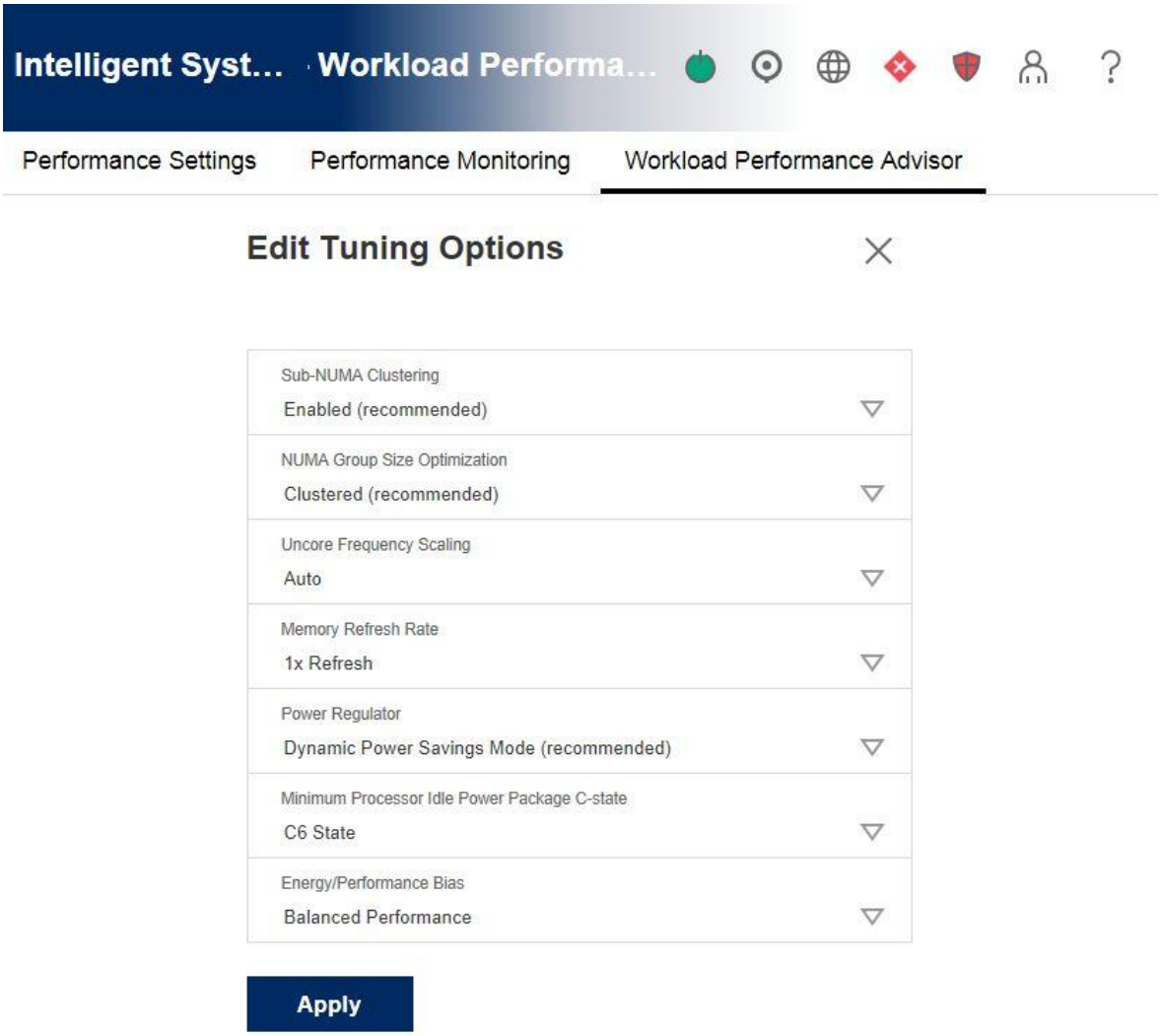
以下のワークロード特性が表示されます。

- **[CPU Utilization]** - サーバー内でのプロセッサーの使用率を示します。
- **[Memory Bus Utilization]** - サーバーで観測されるメモリトラフィック量を示します。
- **[I/O Bus Utilization]** - サーバーで観測される I/O トラフィック量を示します。
- **[NUMA Awareness]** - ワークロードがメモリおよび I/O アクセスを複数のプロセッサーにどう分散させているかを示します。NUMA 認識が高い程、I/O およびメモリトラフィックがリモートよりローカルリソースに割り当てられていることを示します。

表示される値は**[High]**、**[Medium]**、**[Low]**です。

[10 min]および**[I hr]**間隔のサーバーワークロードデータは、iLO がリセットされるとクリアされます。

パフォーマンスチューニングオプションの構成



前提条件

- ホスト BIOS 構成権限
- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
- サーバーの電源が入っており、POST が完了している。
  監視する時間間隔でサーバーの電源が入れられたことを確認します。たとえば、24 時間間隔のデータおよび推奨事項は、サーバーの電源が 24 時間入れられるまで使用できません。
- 2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
  バージョンは、**[Firmware & OS Software]**-**[Firmware]**ページで確認できます。
- **[iLO Date/Time]**が正しく設定されている。

手順

1. ナビゲーションツリーで**[Intelligent System Tuning]/[Performance]**[35]をクリックし、**[Workload Performance Advisor]/[Workload Advisor]**[36]をクリックします。
2. **[Selected Duration]**で間隔値を選択します。
   [10 min]、**[1 hr]**間隔で収集されたデータに基づいて推奨設定を確認できます。
3. 推奨設定(recommmended)を確認します。
   iLO がリセットされた場合、10 分間隔の情報はサーバーの電源が 10 分入れられた後で、1 時間間隔の情報はサーバーの電源が 1 時間入れられた後で表示されます。
4. 設定を変更するには、**[Settings]**をクリックします。
5. 必要に応じて、チューニングオプションを変更し、**[Apply]**をクリックします。
   iLO は、チューニングオプションの変更によってワークロードプロファイル設定がカスタム設定に変更されることを通知します。
6. **[Yes, apply]**をクリックします。
   iLO は設定を保存し、変更を有効にするにはサーバーの再起動が必要であることを通知します。
7. サーバーを再起動します。
   ステータスバナーの**[Reboot server]**リンクをクリックして、**[Server Power]**ページに移動できます。

パフォーマンスチューニングの設定

- **[Sub-NUMA Clustering]** - このオプションが**[Enabled]**に設定されている場合、プロセッサーコア、キャッシュ、およびメモリはこの機能によって複数の NUMA ドメインに分割されます。NUMA に対応し、最適化されているワークロードでは、この機能を有効にするとパフォーマンスが向上する可能性があります。この機能を有効にした場合、最大 1GB のシステムメモリが使用できなくなる場合があります。
- **[NUMA Group Size Optimization]** - このオプションは、NUMA のノードサイズ（論理プロセッサー数）をシステム BIOS がどう通知するかを設定します。これによりアプリケーションの使用法に応じてプロセッサーをグループ化（Kgroups）することに関し OS をサポートします。デフォルト値の**[Clustered]**は、グループが NUMA 境界に沿って最適化されるため、より良いパフォーマンスが提供されます。一部のアプリケーションは、複数のグループにまたがるプロセッサーを利用するように最適化されない場合があります。このような場合、影響を受けるアプリケーションでより多くの論理プロセッサーが使用されるように、**[Flat]**オプションを選択することが必要になることがあります。
- **[Uncore Frequency Scaling]** - このオプションは、プロセッサーの内部バス（アンコア）の周波数のスケーリングを制御します。このオプションを**[Auto]**に設定すると、プロセッサーはワークロードに基づいて周波数を動的に変更できます。**[Maximum]**または**[Minimum]**の周波数を設定すると、レイテンシおよび消費電力の調整ができます。
- **[Memory Refresh Rate]** - このオプションでは、メモリコントローラーのリフレッシュレートを調整できます。サーバーのメモリのパフォーマンスと耐障害性に影響する場合がありま

35 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

36 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

す。他のドキュメントでデフォルト値 （**[1x Refresh)]**）の変更が推奨されない限り、デフォルト値の使用をお勧めします。

- **[Power Regulator]** - このオプションを使用すると、パワーレギュレーターの設定ができます。以下の値を使用できます。
  - **[Dynamic Power Savings Mode]** - プロセッサーの利用率に基づいてプロセッサー速度と電力使用量を自動的に変化させます。このオプションにより、パフォーマンスに影響を与えずに全体的な消費電力を減らすことができます。このオプションは、OS のサポートを必要としません。
  - **[Static Low Power Mode]** - プロセッサー速度を下げ、電力使用量を減らします。このオプションは、システムの最大電力量の値を低く抑えます。パフォーマンスへの影響は、プロセッサーの使用率が高い環境では増大します。
  - **[Static High Performance Mode]** - OS の電力管理ポリシーに関係なく、プロセッサーは常に最大電力および最大パフォーマンスで動作します。
  - **[OS Control Mode]** - OS が電力管理ポリシーを有効にしない場合、プロセッサーは常に最大電力および最大パフォーマンスで動作します。

> △**注記:**
>
> - **[Workload Performance Advisor]**に表示される**[Power Regulator]**設定には、ブート時の静的構成が反映されます。システムの電源投入後の変更は反映されません。**[Workload Performance Advisor]**ページの推奨設定の変更を適用すると、この設定のブート時の構成だけが変更されます。変更を有効にするには、システムの再起動が必要です。

- **[Minimum Processor Idle Power Package C-state] -** このオプションを使用して、オペレーティングシステムが使用するプロセッサーの最小アイドル電力状態（C ステート）を選択します。C ステートを高く設定すればするほど、そのアイドル状態の消費電力は少なくなります。プロセッサーがサポートする最も低いアイドル電力状態は、**[C6 State]**です。

- **[Energy/Performance Bias] -** このオプションを使用して、プロセッサーのパフォーマンスと消費電力を最適化するように複数のプロセッサーサブシステムを構成します。以下の値を使用できます。
  - **[Maximum Performance]** - この設定は、最高のパフォーマンスと最低のレイテンシを必要とし、消費電力にこだわらない環境で使用してください。
  - **[Balanced Performance]** - この設定では、電力効率が最適化されます。ほとんどの環境でこの設定を推奨します。
  - **[Balanced Power]** - サーバー利用状況に基づいて電力効率が最適化されます。
  - **[Power Savings Mode]** - この設定は、消費電力に関する制約が厳しく、パフォーマンスの低下を容認できる環境に適しています。

14. iLO のネットワーク設定の構成

iLO ネットワーク設定

iLO は、以下のネットワーク接続オプションを提供します。

- **[iLO Dedicated Network Port]** - iLO ネットワークトラフィック専用に独立した NIC を使用します。サポートされている場合、このポートはサーバー背面の LAN コネクター（RJ-45、ラベルは **[iLO]**）を使用します。
- **[iLO Shared Network Port LOM]** - サーバーに内蔵の固定 NIC を使用します。この NIC は通常、サーバーネットワークトラフィックを処理し、共通の LAN コネクター経由で同時に iLO ネットワークトラフィックを処理するように設定できます。
- **[iLO Shared Network Port FlexibleLOM]** - サーバー上の特別なスロットに挿入するオプション NIC を使用します。この NIC は通常、サーバーネットワークトラフィックを処理し、共通の LAN コネクター経由で同時に iLO ネットワークトラフィックを処理するように設定できます。

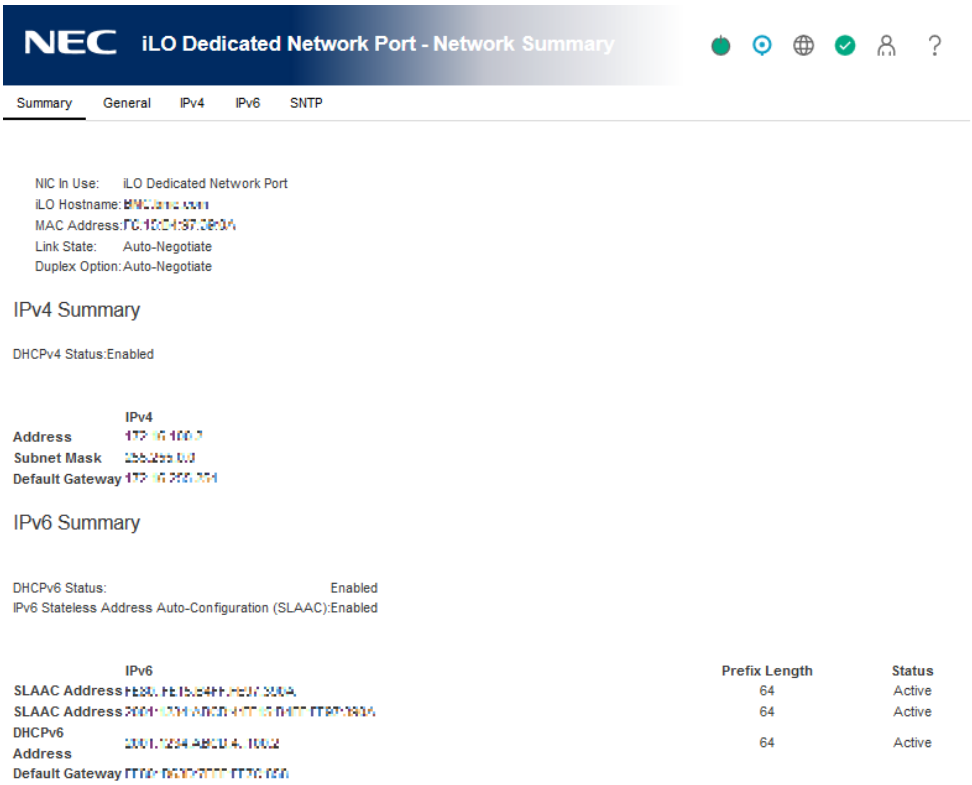
iLO Web インターフェースでネットワーク設定を表示または構成するには、ナビゲーションツリーで**[iLO Dedicated Network Port]**または**[iLO Shared Network Port]**を選択し、次のページのネットワーク設定を表示または編集します。

- **[Summary]** - ネットワーク構成の概要の表示
- **[General]** - ネットワークの全般設定
- **[IPv4]** - IPv4 の設定
- **[IPv6]** - IPv6 の設定
- **[SNTP]** - SNTP の設定

非アクティブポートオプションを選択すると、そのポートを使用するように iLO が構成されていないことを通知するメッセージが表示されます。

ネットワーク構成の概要の表示

設定されている iLO ネットワークの設定値の概要を表示するには、**[iLO Dedicated Network Port]**または**[iLO Shared Network Port]**を選択して、**[Summary]**ページに移動します。



概要の詳細

- **[NIC In Use]** - アクティブな iLO ネットワークインターフェース（iLO 専用ネットワークポートまたは共有ネットワークポート）の名前です。
- **[iLO Hostname]** - iLO サブシステムに割り当てられた完全修飾ネットワーク名（FQDN）。デフォルトで、ホスト名は **[ILO]**+ システムのシリアル番号および現在のドメイン名です。この値はネットワーク名に使用され、一意である必要があります。
- **[MAC Address]** - 選択している iLO ネットワークインターフェースの MAC アドレスです。
- **[Link State]** - 選択している iLO ネットワークインターフェースの現在のリンク速度です。デフォルト値はオートネゴシエートです。
- **[Duplex Option]** - 選択している iLO ネットワークインターフェースの現在のリンクデュプレックス設定です。デフォルト値はオートネゴシエートです。

  iLO ホスト名および NIC 設定は、**[General]**ページで設定できます。手順については、「ネットワークの全般設定」を参照してください。

IPv4 概要の詳細

- **[DHCPv4 Status]** - IPv4 で DHCP が有効かどうかを示します。
- **[Address]** - 現在使用中の IPv4 アドレス。値が 0.0.0.0 の場合、IPv4 アドレスは設定されていません。

- **[Subnet Mask]** - 現在使用中の IPv4 アドレスのサブネットマスク。値が 0.0.0.0 の場合、アドレスは設定されていません。
- **[Default Gateway]** - IPv4 プロトコルで使用されているデフォルトゲートウェイアドレス。値が 0.0.0.0 の場合、ゲートウェイは設定されていません。

IPv6 概要の詳細

- **[DHCPv6 Status]** - IPv6 で DHCP が有効かどうかを示します。表示される値は、以下のとおりです。
  - **[Enabled]** - ステートレスおよびステートフルな DHCPv6 が有効になっています。
  - **[Enabled (Stateless)]** - ステートレスな DHCPv6 のみが有効になっています。
  - **[Disabled]** - DHCPv6 が無効になっています。
- **[IPv6 Stateless Address Auto-Configuration (SLAAC)]** - IPv6 で SLAAC が有効かどうかを示します。SLAAC が無効な場合でも、iLO の SLAAC リンク-ローカルアドレスは必要なため設定されます。
- **[Address list]** - この表には、iLO に対して現在設定されている IPv6 アドレスが表示されます。表は、次の情報を提供します。
  - **[Source]** - アドレスが静的アドレスと SLAAC アドレスのどちらであるかを示します。
  - **[IPv6]** - IPv6 アドレスです。
  - **[Prefix Length]** - アドレスのプレフィックスの長さです。
  - **[Status]** - アドレスステータスです。**[Active]**（このアドレスは iLO が使用しています）、**[Pending]**（このアドレスの重複アドレス検出が進行中です）、および **[Failed]**（重複アドレス検出に失敗したため iLO はこのアドレスを使用していません）があります。

  IPv6 サポートについて詳しくは、「IPv6 の設定」を参照してください。
- **[Default Gateway]** - 現在使用されているデフォルト IPv6 ゲートウェイアドレスです。IPv6 では、iLO は使われる可能性があるデフォルトゲートウェイアドレスのリストを維持します。このリスト内のアドレスは、ルーターアドバタイズメッセージおよび IPv6 **[Static Default Gateway]**設定を元に生成されます。

  [Static Default Gateway]は、IPv6 ページで設定します。詳しくは、「IPv6 の設定」を参照してください。

ネットワークの全般設定

[iLO Dedicated Network Port]→[General]または**[iLO Shared Network Port]→[General]**ページを使用して、iLO ホスト名と NIC 設定を構成します。

iLO ホスト名とドメイン名の制限

iLO のホスト名、ドメイン名の設定をする場合、DNS/WINS など利用する場合には、それぞれの仕様に沿った設定を行う必要があります。。

- **ネームサービスの制限** - サブシステム名は DNS 名の一部として使用します。

- DNS では、英数字とハイフンが使用できます。
- ネームサービスの制限は、ドメイン名にも適用されます。

- **ネームスペースの問題** - この問題を避けるために、次のガイドラインに従ってください。
  - アンダースコア文字を使用しない。
  - サブシステム名を 15 文字までにする。
  - IP アドレスと DNS/WINS 名で iLO プロセッサーが PING コマンドで応答があることを確認する。
  - NSLOOKUP が iLO ネットワークアドレスを正しく解決し、名前空間の競合がないことを確認する。
  - DNS と WINS の両方を使用している場合は、iLO ネットワークアドレスが正しく解決されることを確認する。
  - 名前空間を変更した場合は DNS 名を更新する。
- Kerberos 認証を使用する場合は、ホスト名とドメイン名が Kerberos 使用の前提条件を満たしていることを確認します。詳しくは、「Kerberos 認証とディレクトリサービス」を参照してください。

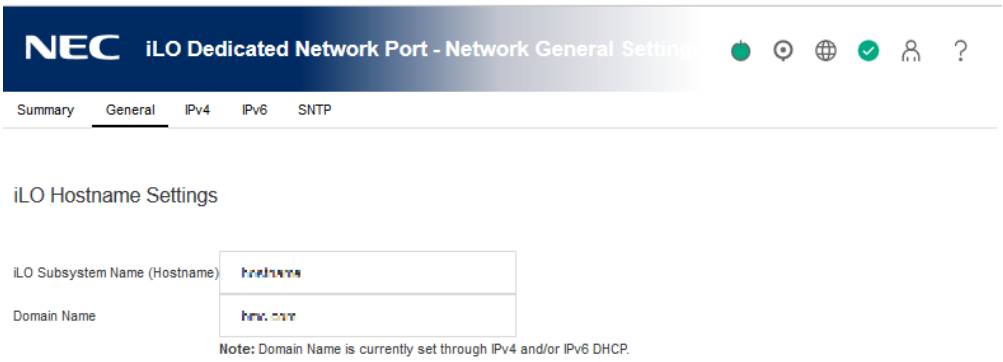
iLO ホスト名の設定

前提条件

iLO の設定を構成権限

手順

1. **[iLO Dedicated Network Port]**または**[iLO Shared Network Port]**ページに移動します。
2. **[General]**タブをクリックします。



3. **[iLO Subsystem Name (Hostname)]**を入力します。

   これは iLO サブシステムの DNS 名です（たとえば、FQDN が ilo.example.com の場合には ilo）。この名前は、DHCP と DNS が IP アドレスではなく iLO サブシステム名に接続するよう構成されている場合のみ使用されます。
4. DHCP が設定されていない場合は、**[Domain Name]**を入力します。

iLO 専用ネットワークポートが選択されている場合、静的なドメイン名を使用するには、**[Use DHCPv4 Supplied Domain Name]**および **[Use DHCPv6 Supplied Domain Name]**を無効にします。

iLO 共有ネットワークポートが選択されている場合、静的なドメイン名を使用するには、**[Use DHCPv4 Supplied Domain Name]**を無効にします。

5. **[Submit]**をクリックします。
6. **[General]**、**[IPv4]**、**[IPv6]**、および **[SNTP]** タブで iLO ネットワークの設定が完了したら、**[Reset]**をクリックして iLO プロセッサーを再起動します。

   接続を再確立できるまでに数分かかります。

[iLO Subsystem Name (Hostname)] - 最大 64 文字までの半角英数、「-」および「.」が使用できます。

[Domain Name] - 最大 49 文字 までの英数およびハイフン”-“(ただし、先頭、最後は不可)が使用できます。

詳細情報

IPv6 の設定
IPv4 の設定

iLO ネットワークポートの構成オプション

iLO サブシステムは、以下のネットワーク接続オプションを提供します。

- **[iLO Dedicated Network Port]** - iLO ネットワークトラフィック専用に独立した NIC を使用します。サポートされている場合、このポートはサーバー背面の LAN コネクター（RJ-45、ラベルは **[iLO]**）を使用します。
- **[iLO Shared Network Port LOM]** - サーバーに内蔵の固定 NIC を使用します。この NIC は通常、サーバーネットワークトラフィックを処理し、共通の LAN コネクター経由で同時に iLO ネットワークトラフィックを処理するように設定できます。
- **[iLO Shared Network Port FlexibleLOM]** - サーバー上の特別なスロットに挿入するオプション NIC を使用します。この NIC は通常、サーバーネットワークトラフィックを処理し、共通の LAN コネクター経由で同時に iLO ネットワークトラフィックを処理するように設定できます。

注記: ご使用のサーバーでサポートされる NIC については、NX7700x シリーズポータルサイト（https://jpn.nec.com/nx7700x/index.html）にある各製品のユーザーズガイドの「サポートしているボードと搭載可能スロット」章を参照してください。

---

iLO ネットワーク接続に関する注意事項

- iLO は 1 つのアクティブな NIC 接続のみをサポートしているため、一度に有効にできるのは専用ネットワークポートオプションまたは共有ネットワークポートオプションのいずれか 1 つのみです。
- デフォルトでは、iLO 共有ネットワークポートは NIC サーバーのポート 1 を使用します。サーバーの構成に応じて、この NIC は LOM または FlexibleLOM アダプターになります。ポー

ト番号は NIC 上のラベルに対応します。これは、オペレーティングシステム内の番号付けとは異なる可能性があります。

iLO ファームウェアでは、サーバーと NIC がポートの選択をサポートしている場合、別のポートを選択することができます。ポート 1 以外のポートが共有ネットワークポートの使用に選択されていて、その構成がご使用のサーバーによってサポートされていない場合、iLO は開始時にポート 1 に戻します。

- 共有ネットワークポートでの IPv6 通信は、iLO 5 Firmware Version 1.20 Feb 02 2018 以降でサポートされています。
- 専用ネットワークポートを使用しないサーバーでは、標準のハードウェア構成の場合、iLO ネットワーク接続は iLO 共有ネットワークポート接続のみを介して提供されます。これらのサーバーでは、iLO ファームウェアはデフォルトで共有ネットワークポートに設定されています。
- サーバーの補助電源に制約があるため、iLO 共有ネットワーク機能で使用される 1 Gb/s 銅線ネットワークアダプターの一部が、サーバーの電源がオフのときに 10/100 の速度でしか動作しない可能性があります。この問題を避けるために、iLO 共有ネットワークポートが接続されるスイッチをオートネゴシエーションに設定することをおすすめします。

  iLO が接続されているスイッチポートが 1 Gb/s に設定されている場合、銅線 iLO 共有ネットワークポートアダプターの一部で、サーバーの電源がオフのときに接続が切断する可能性があることに注意してください。サーバーの電源が再投入されれば、接続は復旧します。
- iLO 共有ネットワークポートを無効にした場合でも、サーバーネットワークトラフィックは NIC ポートを通過するため、オペレーティングシステムの通信には影響ありません。
- 共有ネットワークポートが有効な場合は、リンク状態やデュプレックスオプションは変更できません。共有ネットワークポート構成を使用する場合、オペレーティングシステムでこれらの設定を管理する必要があります。
- 共有ネットワークポートが有効な場合は、共有するサーバーLAN ポートと iLO は直接通信出来ません。共有するサーバーLAN ポートと iLO を通信させる場合、iLO 共有ネットワークポートを無効に設定してご使用ください。

NIC の設定

iLO 共有ネットワークポートまたは iLO 専用ネットワークポートを有効にして、関連付けられた NIC の設定を行うには、**[General]**タブの **[NIC Settings]**セクションを使用します。

NIC 設定は、以下の方法を使用しても設定できます。

- **BMC 構成ユーティリティ**
  - 詳しくは、本体装置のメンテナンスガイドを参照してください。
- **SMASH CLP**
  - SMASH CLP の CLI コマンドの詳細については、SMASH CLP 上で help コマンドを使用してご確認ください。

詳細情報

iLO ネットワークポートの構成オプション

iLO ネットワーク接続に関する注意事項

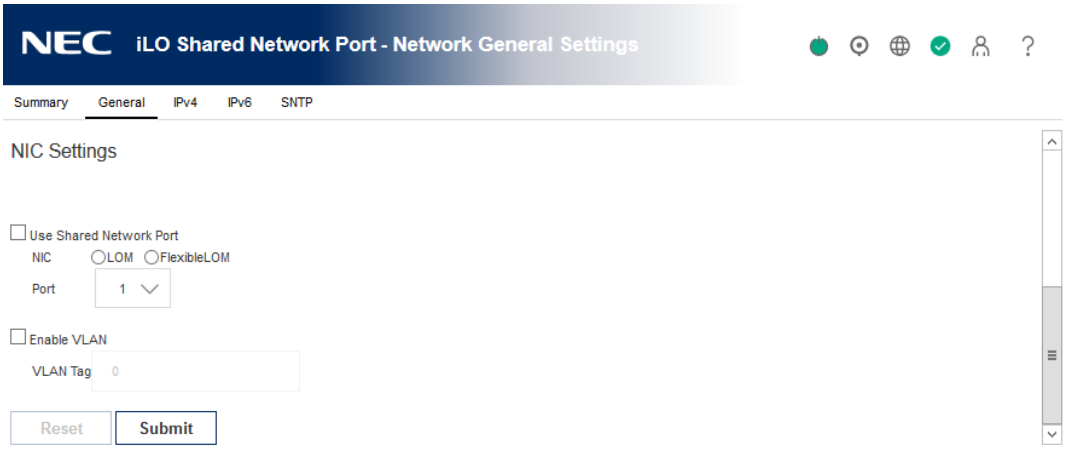
iLO Web インターフェースを介した iLO 共有ネットワークポートの有効化

前提条件

iLO の設定を構成権限

手順

1. 共有ネットワークポート LOM または FlexibleLOM ポートを LAN に接続します。
2. **[iLO Shared Network Port]**ページに移動します。
3. **[General]**タブをクリックします。



4. **[Use Shared Network Port]**チェックボックスを選択します。
5. サーバーの構成に応じて、**[LOM]** または **[FlexibleLOM]** を選択します。
6. **[Port]**メニューから値を選択します。

   1 以外のポート番号の選択は、構成がサーバーおよびネットワークアダプターの両方でサポートされている場合にのみ機能します。無効なポート番号を入力すると、ポート 1 が使用されます。
7. VLAN を使用するには、**[Enable VLAN]**チェックボックスを選択します。

   共有ネットワークポートに設定して VLAN が有効な場合、iLO 共有ネットワークポートは VLAN の一部になります。物理的に同じ LAN に接続されている場合でも、異なる VLAN タグを持つすべてのネットワークデバイスが、独立した LAN にあるかのように表示されます。
8. VLAN を有効にした場合は、**[VLAN Tag]**を入力します。相互に通信するネットワークデバイスすべてが、同じ VLAN タグを持つ必要があります。VLAN タグは、1～4094 の任意の番号です。
9. **[Submit]**をクリックして、変更を保存します。
10. **[General]**、**[IPv4]**、**[IPv6]**、および **[SNTP]** タブで iLO ネットワークの設定が完了したら、**[Reset]**をクリックして iLO を再起動します。

    接続を再確立できるまでに数分かかります。

iLO をリセットすると、共有ネットワークポートがアクティブになります。iLO との間のすべてのネットワークトラフィックが共有ネットワーク LOM または FlexibleLOM ポート経由で転送されるようになります。

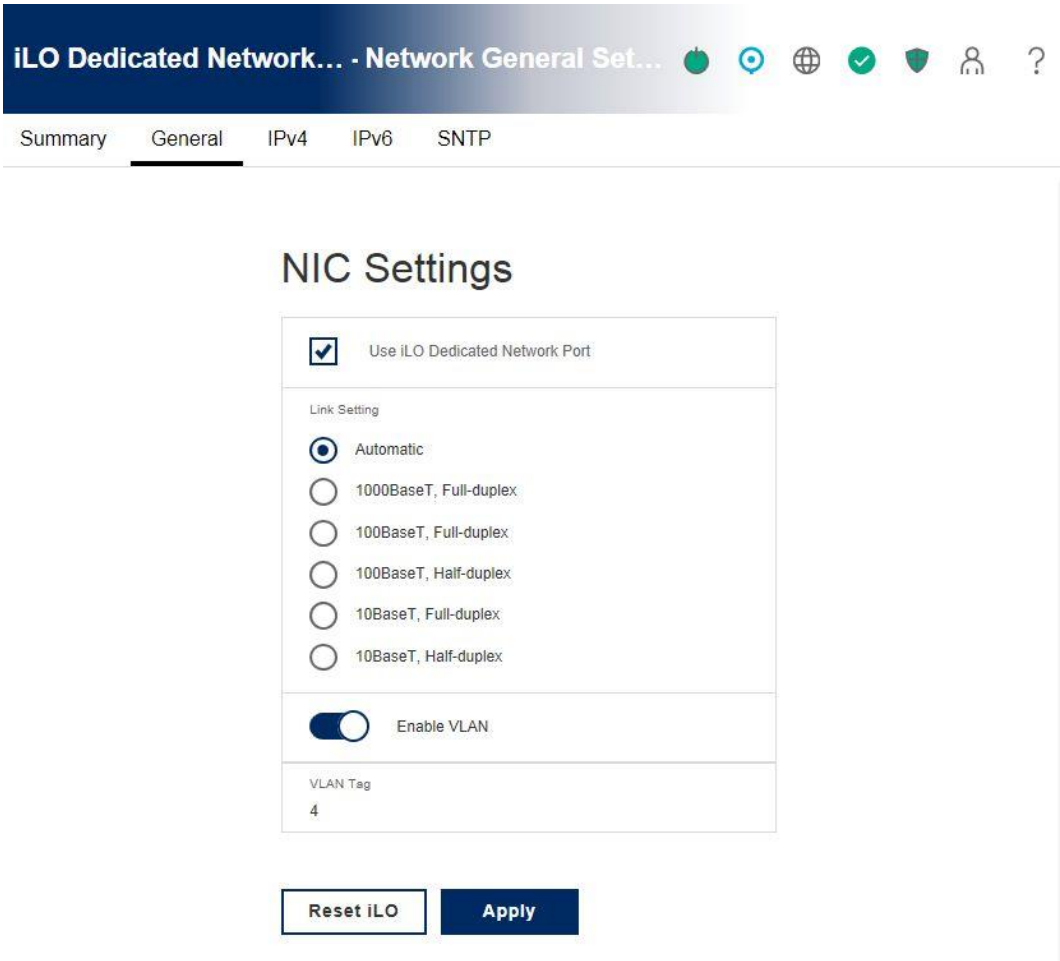
iLO Web インターフェースを介した iLO 専用ネットワークポートの有効化

前提条件

iLO の設定を構成権限

手順

1. iLO 専用ネットワークポートを、サーバーを管理する LAN に接続します。
2. **[iLO Dedicated Network Port]**ページに移動します。
3. **[General]**タブをクリックします。



4. **[Use iLO Dedicated Network Port]**チェックボックスを選択します。
5. **[Link State]**を選択します。

   リンク設定は、iLO ネットワークトランシーバーの速度とデュプレックス設定を制御します。

> 重要: **[Link State]**は、接続先(スイッチング HUB 等)の設定が Auto Negotiation 設定以外の固定設定にしている場合は、下記の場合を除き必ず接続先設定をご確認の上[Link State]に同じ設定を行ってください。接続先の設定が Auto Negotiation の場合は、Automatic に設定してください。設定が一致しない場合、正常に見えても突然通信できなくなることや通信が不安定になることがあります。

但し、接続先(スイッチング HUB 等)の設定が 100BaseT Full-duplex 設定の場合には、**[Link State]**には**[Automatic]**を設定してください。

使用できる設定は次のとおりです。

- **[Automatic]**（デフォルト） - iLO は、ネットワークに接続するときに、サポートされる最高のリンク速度とデュプレックス設定をネゴシエーションできます。
- **[1000BaseT, Full-duplex]** - 全二重を使用した 1 Gb 接続を強制します。
- **[1000BaseT, Half-duplex]** - 半二重を使用した 1 Gb 接続を強制します。

  1000BaseT, Half-duplex は標準の設定ではなく、ほとんどのスイッチがサポートしていません。この設定を使用する場合、1000BaseT, Half-duplex をサポートするようにスイッチが構成されていることを確認します。
- **[100BaseT, Full-duplex]** - 全二重を使用した 100 Mb 接続を強制します。
- **[100BaseT, Half-duplex]** - 半二重を使用した 100 Mb 接続を強制します。
- **[10BaseT, Full-duplex]** - 全二重を使用した 10 Mb 接続を強制します。
- **[10BaseT, Half-duplex]** - 半二重を使用した 10 Mb 接続を強制します。

6. VLAN を使用するには、**[Enable VLAN]**チェックボックスを選択します。

   共有ネットワークポートに設定して VLAN が有効な場合、iLO 専用ネットワークポートは VLAN の一部になります。物理的に同じ LAN に接続されている場合でも、異なる VLAN タグを持つすべてのネットワークデバイスが、独立した LAN にあるかのように表示されます。
   ※本機能は、iLO 5 Firmware Version 1.43 May 23 2019 以降でサポートされます。
7. VLAN を有効にした場合は、**[VLAN Tag]**を入力します。相互に通信するネットワークデバイスすべてが、同じ VLAN タグを持つ必要があります。VLAN タグは、1～4094 の任意の番号です。
   ※本機能は、iLO 5 Firmware Version 1.43 May 23 2019 以降でサポートされます。
8. **[Submit]**をクリックして、変更を保存します。
9. **[General]**、**[IPv4]**、**[IPv6]**、および **[SNTP]** タブで iLO ネットワークの設定が完了したら、**[Reset]**をクリックして iLO を再起動します。接続を再確立できるまでに数分かかります。

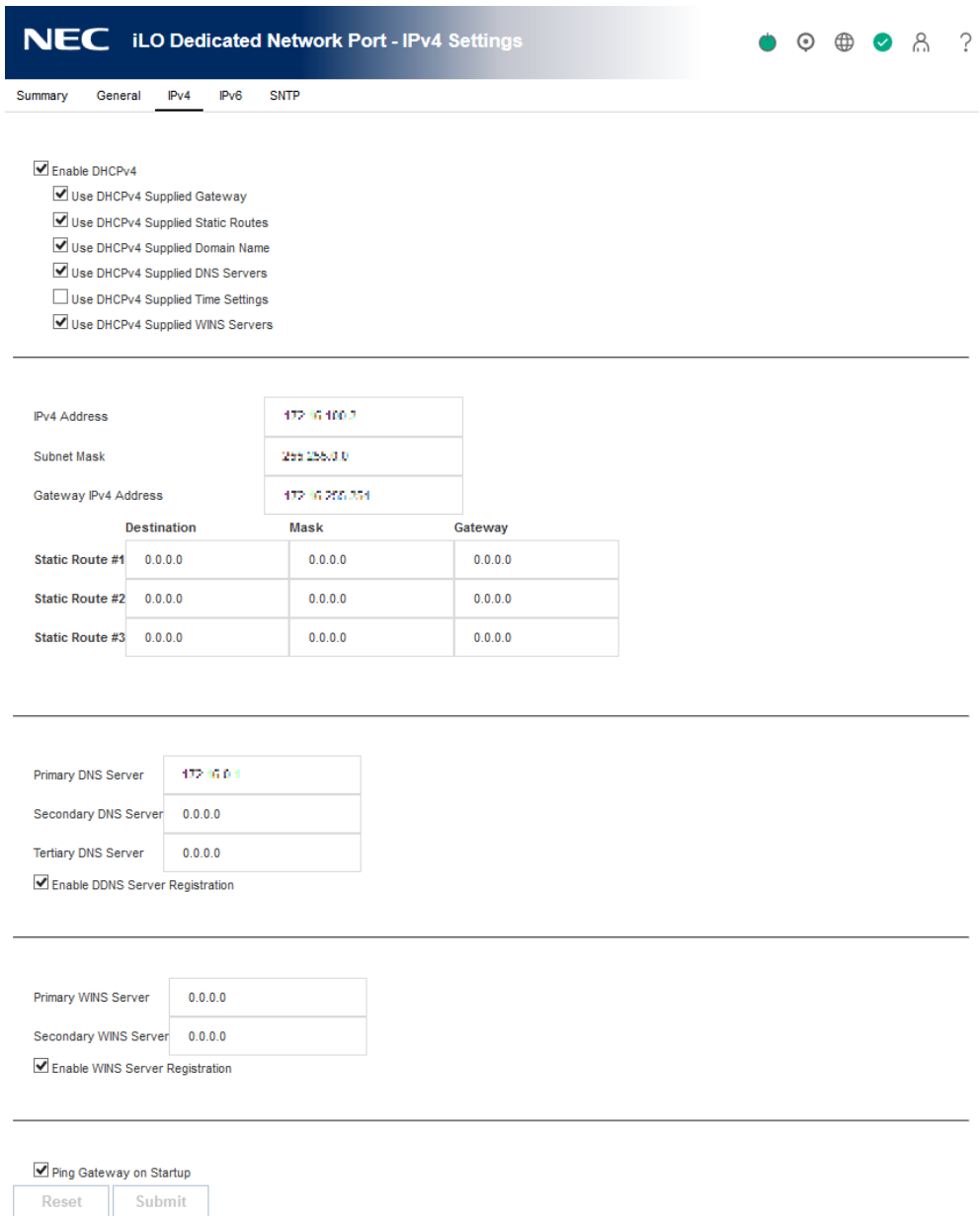
IPv4 の設定

iLO 専用ネットワークポートまたは共有ネットワークポートの**[IPv4]**ページを使用して、iLO の IPv4 を設定します。

前提条件
iLO の設定を構成権限

手順

1. **[iLO Dedicated Network Port]**または**[iLO Shared Network Port]**ページに移動します。
2. **[IPv4]**タブをクリックします。



3. 以下の設定を行います。
   - **[Enable DHCPv4]** - iLO が DHCP サーバーからの IP アドレス（およびその他の多くの設定）の取得を有効にします。

- **[Use DHCPv4 Supplied Gateway]** - iLO が、DHCP サーバーが提供するゲートウェイを使用するかどうかを指定します。DHCP を使用しない場合は、**[Gateway IPv4 Address]**ボックスにゲートウェイアドレスを入力します。
- **[Use DHCPv4 Supplied Static Routes]** - iLO が、DHCP サーバーが提供する静的経路を使用するかどうかを指定します。DHCP を使用しない場合は、**[Static Route #1]**、**[Static Route #2]**および **[Static Route #3]** ボックスに静的経路の宛先、マスク、およびゲートウェイアドレスを入力します。
- **[Use DHCPv4 Supplied Domain Name]** - iLO が、DHCP サーバーが提供するドメイン名を使用するかどうかを指定します。DHCP を使用しない場合は、**[iLO Dedicated Network Port]→[General]**または**[iLO Shared Network Port]→[General]**ページの**[Domain Name]**ボックスにドメイン名を入力します。詳しくは、「ネットワークの全般設定」を参照してください。
- **[Use DHCPv4 Supplied DNS Servers]** - iLO が、DHCP サーバーが提供する DNS サーバーリストを使用するかどうかを指定します。DNS サーバーリストを使用しない場合は、**[Primary DNS Server]**、**[Secondary DNS Server]**および **[Tertiary DNS Server]**ボックスに DNS サーバーアドレスを入力します。
- **[Use DHCPv4 Supplied Time Settings]** - iLO が、DHCPv4 が提供する NTP サービスの場所を使用するかどうかを指定します。
- **[Use DHCPv4 Supplied WINS Servers]** - iLO が、DHCP サーバーが提供する WINS サーバーリストを使用するかどうかを指定します。WINS サーバーリストを使用しない場合は、**[Primary WINS Server]**および**[Secondary WINS Server]**ボックスに WINS サーバーアドレスを入力します。

- **[IPv4 Address]** - iLO の IP アドレス。DHCP を使用する場合、iLO の IP アドレスは自動的に提供されます。DHCP を使用しない場合は、静的 IP アドレスを入力します。
- **[Subnet Mask]** - iLO IP ネットワークのサブネットマスク。DHCP を使用する場合、サブネットマスクは自動的に提供されます。DHCP を使用しない場合は、ネットワークのサブネットマスクを入力します。
- **[Gateway IPv4 Address]** - iLO のゲートウェイアドレスです。DHCP を使用する場合、iLO ゲートウェイの IP アドレスは自動的に提供されます。DHCP を使用しない場合は、iLO のゲートウェイ IP アドレスを入力します。
- **[Static Route #1]**、**[Static Route #2]**、および **[Static Route #3]** - iLO の静的経路の宛先、マスク、およびゲートウェイアドレス。**[Use DHCPv4 Supplied Static Routes]**を使用する場合、これらの値は自動的に入力されます。使用しない場合は、静的経路の値を入力します。
- **DNS** サーバー情報 - 次の情報を入力します。
  - **[Primary DNS Server]** - **[Use DHCPv4 Supplied DNS Servers]**が有効な場合、この値は自動的に入力されます。有効でない場合は、プライマリーDNS サーバーのアドレスを入力します。
  - **[Secondary DNS Server]** - **[Use DHCPv4 Supplied DNS Servers]**が有効な場合、この値は自動的に入力されます。有効でない場合は、セカンダリーDNS サーバーのアドレスを入力します。

- **[Tertiary DNS Server]** - **[Use DHCPv4 Supplied DNS Servers]**が有効な場合、この値は自動的に入力されます。有効でない場合は、ターシャリーDNS サーバーのアドレスを入力します。
- **[Enable DDNS Server Registration]** - このチェックボックスを選択またはクリアして、iLO が DNS サーバーに IPv4 アドレスと名前を登録するかどうかを指定します。

- **WINS** サーバー情報 - 次の情報を入力します。
  - **[Primary WINS Server]** - **[Use DHCPv4 Supplied WINS Servers]**が有効な場合、この値は自動的に入力されます。有効でない場合は、プライマリーWINS サーバーのアドレスを入力します。
  - **[Secondary WINS Server]** - **[Use DHCPv4 Supplied WINS Servers]**が有効な場合、この値は自動的に入力されます。有効でない場合は、セカンダリーWINS サーバーのアドレスを入力します。
  - **[Enable WINS Server Registration]** - iLO が、WINS サーバーに名前を登録するかどうかを指定します。
- **[Ping Gateway on Startup]** - iLO プロセッサーの初期化時に、ゲートウェイに 4 つの ICMP エコー要求パケットを送信します。これにより、iLO とのパケット転送を担当するルーターで、iLO 用の ARP キャッシュエントリーが最新であることを保証できます。

4. **[Submit]**をクリックして、**IPv4** の設定ページでの変更を保存します。
5. **[General]**、**[IPv4]**、**[IPv6]**、および **[SNTP]** タブで iLO ネットワークの設定が完了したら、**[Reset]**をクリックして iLO を再起動します。接続を再確立できるまでに数分かかります。

IPv6 の設定

iLO 専用ネットワークポートまたは共有ネットワークポートの **[IPv6]**ページを使用して、iLO の IPv6 を設定します。

IPv6 を使用する場合は、次に注意してください。

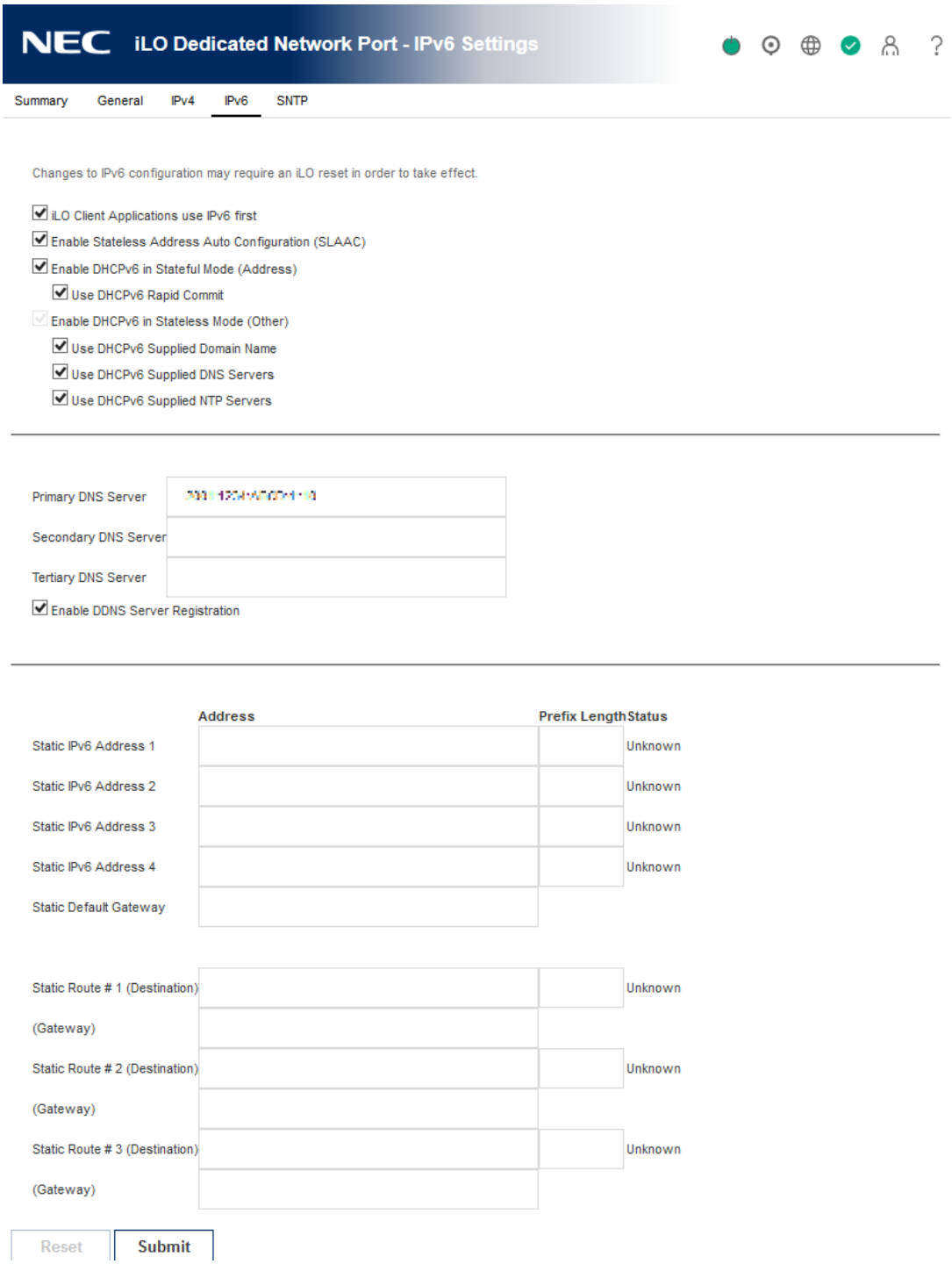
- IPv6 をサポートしている iLO の機能のリストは、「IPv6 をサポートしている iLO の機能」を参照してください。
- iLO Firmware Version 1.15 Aug 17 2017 以前では、共用ネットワークポートで IPv6 の通信を行うことができません。iLO 専用ネットワークポートをご使用ください。

前提条件

iLO の設定を構成権限

手順

1. **[iLO Dedicated Network Port]**または**[iLO Shared Network Port]**ページに移動します。
2. **[IPv6]**タブをクリックします。



3. 以下の設定を行います。
   - **[iLO Client Applications use IPv6 first]** - iLO クライアントアプリケーションで IPv4 サービスアドレスも IPv6 サービスアドレスも設定されている場合は、このオプションでクライアントアプリケーションへのアクセスの際に iLO がどちらのプロトコルを先に試すかを指定します。この設定は、FQDN を使用して NTP を設定する際にネームリゾルバーから受け取るアドレスリストにも適用されます。
     - iLO で IPv6 を先に使用する場合は、このチェックボックスを選択します。

- iLO で IPv4 を先に使用する場合は、このチェックボックスをクリアします。最初のプロトコルを使用した通信が失敗すると、iLO は自動的の 2 番目のプロトコルを試します。

- **[Enable Stateless Address Auto Configuration (SLAAC)]** - このチェックボックスを選択すると、iLO が、ルーター通知メッセージから自身の IPv6 アドレスを作成できるようになります。

注記: iLO は、このオプションが選択されていない場合でも、自身のリンク-ローカルアドレスを作成します。

- **[Enable DHCPv6 in Stateful Mode (Address)]** - このチェックボックスを選択すると、iLO が、DHCPv6 から提供される IPv6 アドレスを要求し構成できるようになります。
  - **[Use DHCPv6 Rapid Commit]** - このチェックボックスを選択すると、iLO は DHCPv6 サーバーに対し高速コミットメッセージングモードを使用するようになります。このモードは DHCPv6 ネットワークトラフィック量を減少させますが、2 台以上の DHCPv6 サーバーが応答しアドレスを提供する可能性があるネットワークで使用すると、問題を引き起こすことがあります。
- **[Enable DHCPv6 in Stateless Mode (Other)]** - このチェックボックスを選択すると、iLO は DHCPv6 サーバーから NTP および DNS サービスの場所の設定を要求できるようになります。
  - **[Use DHCPv6 Supplied Domain Name]** - このチェックボックスで、DHCPv6 サーバーが提供するドメイン名を使用するかどうかを選択します。
  - **[Use DHCPv6 Supplied DNS Servers]** - このチェックボックスを選択すると、DNS サーバーの場所に DHCPv6 サーバーによって提供された IPv6 アドレスが使用されます。この設定は、IPv4 DNS サーバーの場所オプションに加えて有効化できます。
  - **[Use DHCPv6 Supplied NTP Servers]** - このチェックボックスを選択すると、NTP サーバーの場所に DHCPv6 サーバーによって提供された IPv6 アドレスが使用されます。この設定は、IPv4 NTP サーバーの場所オプションに加えて有効化できます。

注記: **[Enable DHCPv6 in Stateful Mode (Address)]**が選択されている場合、**[Enable DHCPv6 in Stateless Mode (Other)]**がデフォルトで、必ず選択され変更できなくなります。これは、iLO と DHCPv6 サーバー間で必要な DHCPv6 ステートフルメッセージではそれが暗黙で了解されているからです。

- **[Primary DNS Server]、[Secondary DNS Server]、[Tertiary DNS Server]**

  DNS サービスの IPv6 アドレスを入力します。

  DNS サーバーの場所が IPv4 と IPv6 の両方で設定されている場合、両方のソースが使用されます。ただし、**[iLO Client Applications use IPv6 first]**構成オプションで示された優先順位に従いプライマリーソース、セカンダリーソース、ターシャリーソースの順に使用されます。
- **[Enable DDNS Server Registration]** - iLO が、DNS サーバーに IPv6 アドレスと名前を登録するかどうかを指定します。

- **[Static IPv6 Address 1]**、**[Static IPv6 Address 2]**、**[Static IPv6 Address 3]**、**[Static IPv6 Address 4]** - iLO に最大 4 つの静的 IPv6 アドレスとプリフィックス長を入力します。リンクローカルアドレスは入力しないでください。
- **[Static Default Gateway]** - ネットワーク上にルーター通知メッセージが存在しない場合に対応できるよう、デフォルト IPv6 ゲートウェイアドレスを入力します。
- **[Static Route #1]**、**[Static Route #2]**、**[Static Route #3]** - 静的 IPv6 ルートの宛先のプリフィックスとゲートウェイアドレスのペアを入力します。宛先のプレフィックス長を指定する必要があります。リンク-ローカルアドレスは宛先としては許可されませんが、ゲートウェイとしては許可されます。

4. **[Submit]**をクリックして、IPv6 の設定ページでの変更を保存します。
5. **[General]**、**[IPv4]**、**[IPv6]**、および **[SNTP]** タブで iLO ネットワークの設定が完了したら、**[Reset]**をクリックして iLO を再起動します。接続を再確立できるまでに数分かかります。

IPv6 をサポートしている iLO の機能

IPv6 プロトコルは、IPv4 アドレスプールが枯渇に向かっているという現状に対応するために、IETF によって導入されました。
IPv6 では、アドレス不足の問題を解消するために、アドレス長が 128 ビットに拡張されています。iLO はデュアルスタック実装を導入することで両方のプロトコルの同時使用に対応しています。以前に使用できた iLO のすべての機能が、IPv4 で引き続きサポートされます。

以下の機能が IPv6 の使用をサポートします。

- IPv6 静的アドレス割り当て
- IPv6 SLAAC アドレス割り当て
- IPv6 静的ルート割り当て
- IPv6 静的デフォルトゲートウェイ入力
- DHCPv6 ステートフルアドレス割り当て
- DHCPv6 ステートレス DNS、ドメイン名、および NTP 設定
- 統合リモートコンソール
- Web サーバー
- SSH サーバー
- SNTP クライアント
- DDNS クライアント
- SNMP
- アラートメール
- リモート Syslog
- WinDBG サポート
- スクリプト化可能な仮想メディア
- CLI キーインポート over IPv6 接続

- LDAP および Kerberos over IPv6 を使用した認証
- iLO 連携
- IPMI

SNTP の設定

SNTP により iLO は、外部の時刻ソースとクロックを同期させることができます。iLO の日付と時刻は、POST の実行中にシステム ROM によって同期を取ることができるため、SNTP の使用は必須ではありません。ただし、iLO で正しい時刻を表示するため、SNTP を使用しない場合であってもタイムゾーンの設定を行ってください。

iLO 5 Firmware Version 1.10 Jun 07 2017 では、SNTP 設定を行わない場合やタイムサーバーと時刻同期できる環境で利用されない場合には、iLO イベントログや IML のエントリーのログ時刻、iLO へ接続しているセッションリストの時刻などで以下に示す時刻が表示されます。SNTP 設定し、タイムサーバーと時刻同期できる環境でのご利用をお勧めします。

- Web インターフェースで iLO イベントログや IML 表示フィルターで**[Show Default]、[Show ISO Time]**を選択時に表示されるログ、セッションリストの時刻として以下を表示。
  - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）
- Web インターフェースで iLO イベントログや IML 表示フィルターで**[Show Local Time]**を選択時に表示されるログの時刻として以下を表示。
  - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）に、さらに iLO へ接続したクライアントの環境のタイムゾーンを加味した時刻

iLO 5 Firmware Version 1.15 Aug 17 2017、および Version 1.20 Feb 02 2018 では、iLO がタイムサーバーと時刻同期しておらず、かつ BIOS/プラットフォーム構成(RBSU)で[Time Format]に[Local Time]を設定している場合に、以下に示す時刻が表示されます。

- **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
  - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）
- **[Show Local Time]**を選択時に以下を表示。
  - BIOS/プラットフォーム構成(RBSU)で表示されるシステム時刻（UTC±Time Zone）に、さらに iLO へ接続したクライアントの環境のタイムゾーンを加味した時刻

iLO 5 Firmware Version 1.30 May 31 2018 以降では、以下に示す時刻が表示されます。

- **[Show Default]、[Show ISO Time]**を選択時に以下を表示。
  - UTC 時刻
- **[Show Local Time]**を選択時に以下を表示。
  - ローカル時刻

プライマリーおよびセカンダリーNTP サーバーアドレスは、手動でまたは DHCP サーバーにより設定できます。プライマリーサーバーアドレスに接続できない場合は、セカンダリーアドレスが使用されます。

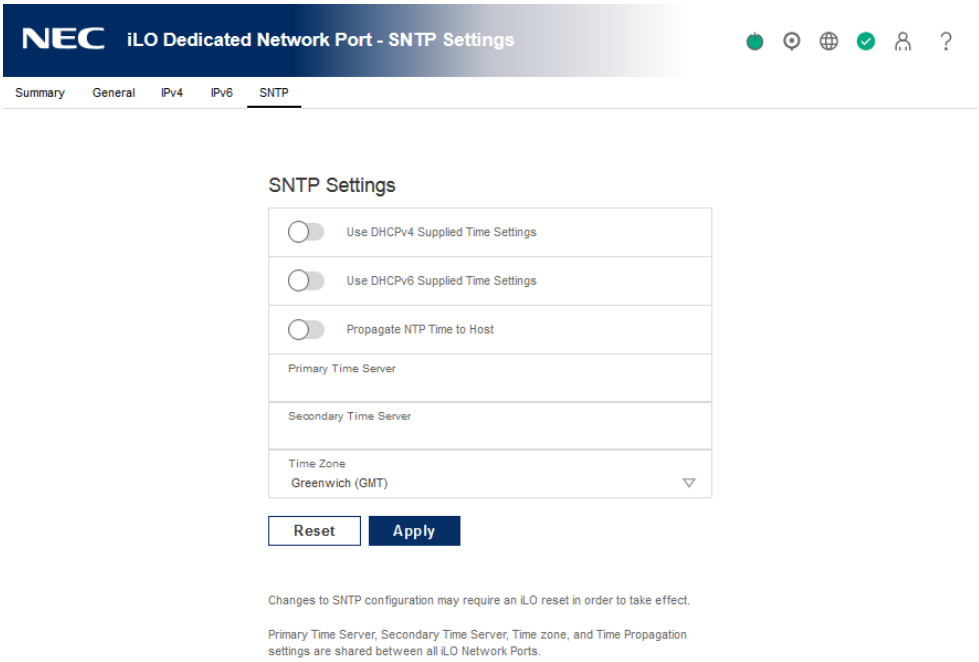
前提条件

- iLO の設定を構成権限
- 管理ネットワーク上で 1 台以上の NTP サーバーが利用可能である。
- DHCPv4 が提供する NTP サービス構成を使用する場合、**[IPv4]**タブで DHCPv4 が有効になっている。
- DHCPv6 が提供する NTP サービス構成を使用する場合、**[IPv6]** タブで DHCPv6 ステートレスモードが有効になっている。

- DHCPv6 の時間設定のみ：サーバーが iLO 専用ネットワークポートを使用するように設定されている。IPv6 は、共有ネットワークポート設定ではサポートされません。

手順

1. **[iLO Dedicated Network Port]**または**[iLO Shared Network Port]**ページに移動します。
2. **[SNTP]** タブをクリックします。



3. 次のいずれかを実行します。
   - **[Use DHCPv4 Supplied Time Settings]**のトグルボタン、**[Use DHCPv6 Supplied Time Settings]**のトグルボタン、または両方のトグルボタンを有効にして、DHCP が提供する NTP サーバーアドレスを使用します。
   - **[Primary Time Server]**ボックスおよび**[Secondary Time Server]**ボックスに、NTP サーバーアドレスを入力します。
4. **[Use DHCPv6 Supplied Time Settings]**のみを選択した場合、またはプライマリーおよびセカンダリータイムサーバーを入力した場合は、**[Time Zone]**リストからサーバータイムゾーンを選択します。
5. **[Apply]**をクリックして、**[SNTP 設定]**ページでの変更を保存します。
6. **[General]**、**[IPv4]**、**[IPv6]**、および **[SNTP]** タブで iLO ネットワークの設定が完了したら、**[Reset]**をクリックして iLO を再起動します。
   接続を再確立できるまでに数分かかります。

詳細情報

IPv4 の設定
IPv6 の設定
ネットワークの全般設定
DHCP NTP アドレスの選択

SNTP の設定
イベントログエントリーのタイムスタンプが正しくない
iLO タイムゾーン設定

SNTP 設定

- **[Use DHCPv4 Supplied Time Settings]** - DHCPv4 が提供する NTP サーバーアドレスを使用するように iLO を設定します。デフォルトは、有効です。NTP サーバーとの時刻同期機能をお使いにならない場合は、無効に設定してください。
- **[Use DHCPv6 Supplied Time Settings]** - DHCPv6 が提供する NTP サーバーアドレスを使用するように iLO を設定します。デフォルトは、有効です。NTP サーバーとの時刻同期機能をお使いにならない場合は、無効に設定してください。
- **[Propagate NTP Time to Host]** - AC ケーブルを挿した後、または iLO がデフォルト設定にリセットされた後の最初の POST を実行している間に、サーバー時間を iLO 時間と同期させるかどうかを決定します。デフォルト設定は、無効です。

  iLO 5 Firmware Version 1.15 以前では、本設定を有効にすると OS 上の時刻が不正になることがあります。デフォルト設定のままご利用ください。

  △**注意:**
  BIOS/プラットフォーム構成(RBSU)の[Time Format]に[Local Time]が設定されている場合に、本設定を有効にすると OS 上の時刻が不正になる場合がありますので、[Time Format] が[Local Time]の場合には本設定を有効にしないでください。

- **[Primary Time Server]** - 指定されたアドレスを持つプライマリータイムサーバーを使用するように iLO を設定します。サーバーのアドレスは、サーバーの FQDN、IPv4 アドレス、または IPv6 アドレスを使用して入力できます。NTP サーバーとの時刻同期機能をお使いにならない場合は、空白を設定してください。
- **[Secondary Time Server]** - 指定されたアドレスを持つセカンダリータイムサーバーを使用するように iLO を設定します。サーバーのアドレスは、サーバーの FQDN、IPv4 アドレス、または IPv6 アドレスを使用して入力できます。NTP サーバーとの時刻同期機能をお使いにならない場合は、空白を設定してください。
- **[Time Zone]** - この設定で iLO が UTC 時刻を調整して現地時間を取得し、夏時間（サマータイム）のために時間を調整する方法が決まります。iLO イベントログや IML のエントリーに正しいローカル時刻が表示されるようにするには、サーバーが存在する場所のタイムゾーンを指定し、iLO イベントログや IML 表示フィルターで**[Show Local Time]**を選択する必要があります。

  デフォルトは、**Greenwich (GMT)**です。

  iLO が調整なしで SNTP サーバーが提供する時間を使用する場合は、UTC 時間に調整を適用しないタイムゾーンを選択します。また、そのタイムゾーンに夏時間調整を適用してはなりません。この要件に適合するいくつかのタイムゾーンがあります。iLO で選択できる 1 つの例は **Greenwich (GMT)**です。このタイムゾーンを選択すると、Web インターフェースのページおよびログエントリーに、SNTP サーバーが提供する時間をそのまま表示します。

  注記: NTP サーバーは協定世界時（UTC）を使用するように構成してください。

iLO が正しい時刻を表示するために SNTP サーバーとの時刻同期を行わない場合でも、タイムゾーンの設定が必要になります。詳しくは iLO タイムゾーン設定をご覧ください。

DHCP NTP アドレスの選択

DHCP サーバーを使用して NTP サーバーアドレスを提供する場合は、**[IPv6]**タブの**[iLO Client Applications use IPv6 first]**設定によって、プライマリーおよびセカンダリータイムサーバー の値の選択を制御します。**[IPv6]** タブで **[iLO Client Applications use IPv6 first]** を選択した場合、DHCPv6 提供の NTP サービスアドレス（使用可能な場合）がプライマリー時刻サーバーに使用され、DHCPv4 提供のアドレス（使用可能な場合）がセカンダリー時刻サーバーに使用されます。

プロトコルベースの優先順位の動作を変更して、DHCPv4 をまず使用する場合は、**[iLO Client Applications use IPv6 first]**チェックボックスをクリアします。

DHCPv6 アドレスがプライマリーアドレスにもセカンダリーアドレスにも使用できない場合は、DHCPv4 アドレス（使用可能な場合）が使用されます。

詳細情報

IPv6 の設定

iLO タイムゾーン設定

iLO NIC 自動選択

iLO NIC 自動選択を使用すると、iLO が iLO 専用ネットワークポートと iLO 共有ネットワークポートを自動的に選択できるようになります。起動時に、iLO は使用可能なポートのネットワークアクティビティを検索し、ネットワークアクティビティに基づいて使用するポートを自動的に選択します。

この機能によって、ご使用の NX7700x サーバに共通の事前構成を使用することができます。たとえば複数のサーバーがある場合、一部のサーバーは iLO が iLO 専用ネットワークポートを使用して接続するデータセンターに設置されており、他のサーバーは iLO が共有ネットワークポートを使用して接続するデータセンターに設置されている場合があります。iLO NIC 自動選択を使用すると、どちらのデータセンターにもサーバーを設置できるようになり、iLO は正しいネットワークポートを選択します。

デフォルトでは、NIC 自動選択は無効です。この機能の設定については、「iLO NIC 自動選択の有効化」を参照してください。

NIC 自動選択のサポート

- この構成をサポートしているサーバー上で両方の共有ネットワークポートを検索するように設定できます。
- NIC フェイルオーバーをサポートします。有効にすると、現在の接続が切断されたときに、iLO が自動的に NIC 接続の検索を開始します。この機能を使用するには、NIC 自動選択を有効にする必要があります。

NIC 自動選択が有効になっている場合の iLO 起動時の動作

NIC 自動選択が有効な場合：

- iLO が電源に接続されると、最初に iLO 専用ネットワークポートをテストします。

- iLO がリセットされると、最後に使用した iLO ネットワークポートを最初にテストします。
- ネットワークポートのテスト時に、iLO がネットワークのアクティビティを検出した場合、そのポートを選択して使用します。約 100 秒後までにネットワークアクティビティが検出されない場合は、iLO は反対側のネットワークポートに切り替え、そのポートのテストを開始します。iLO はネットワークアクティビティが検出されるまで、iLO 専用ネットワークポートと iLO 共有ネットワークポートを交互にテストします。iLO がテストのためにネットワークポートを切り替えるたびに、iLO のリセットが発生します。

△ 注意: 物理 NIC のいずれかがセキュリティ保護されていないネットワークに接続している場合、iLO が iLO 専用ネットワークポートと iLO 共有ネットワークポートを交互に切り替えたときに不正アクセスが発生する可能性があります。必ず iLO を次のようなネットワークに接続することを強くおすすめします。

  - iLO へのアクセスに強力なパスワードを使用している。
  - セキュリティ保護されていないネットワークに iLO 専用ネットワークポートを接続しない。
  - iLO 共有ネットワークポートがセキュリティ保護されていないネットワークに接続されている場合、iLO のうち共有 NIC の部分は VLAN タギングを使用し、VLAN が安全なネットワークのみに接続されていることを確認する。

- iLO がアクティブなネットワークポートを検索するときは、サーバーの UID ランプが点灯します。検索中に iLO がリセットされた場合、UID ランプが 5 秒間点滅し、その後アクティブなポートが選択されるか、iLO がリセットされるまで継続的に点灯します。
- サーバーが iLO への LOM および FlexibleLOM 共有ネットワークポート接続の両方をサポートしている場合、iLO は構成中に選択されたオプションだけをテストします。iLO は LOM および FlexibleLOM オプションを交互にテストしません。
  共有ネットワークポートオプションの構成については、「iLO Web インターフェースを介した iLO 共有ネットワークポートの有効化」を参照してください。
- NIC 自動選択が DHCP アドレスの割り当てアクティビティを検索するよう構成されており、iLO ネットワークポートのうち 1 つだけで DHCP が有効になっている場合、iLO は DHCP 用に構成されていないポートの受信データパケットアクティビティをテストします。

iLO NIC 自動選択の有効化

NIC 自動選択はデフォルトでは無効です。NIC 自動選択を有効にするには、次の手順を使用します。

1. 両方の iLO ネットワークポートを構成します。

   NIC 自動選択機能を有効にして使用する前に、両方の iLO ネットワークポートをそれぞれのネットワーク環境に合わせて構成しなければなりません。

2. 次の方法を実行します。

   - CLI コマンド oemNEC_nicautosel を使用して、NIC 自動選択を設定します。

   SMASH CLP の CLI コマンドの詳細については、SMASH CLP 上で help コマンドを使用してご確認ください。

3. サーバーのケーブルを必要に応じて配線し、iLO をリセットします。

   NIC 自動選択の変更は、iLO がリセットされるまで有効になりません。

詳細情報

NIC フェイルオーバーの設定

NIC フェイルオーバーの設定

1. iLO NIC 自動選択を設定します。
2. 次の方法を実行します。
   - CLI コマンド oemNEC_nicfailover を使用して、NIC フェイルオーバーを設定します。

   SMASH CLP の CLI コマンドの詳細については、SMASH CLP 上で help コマンドを使用してご確認ください。

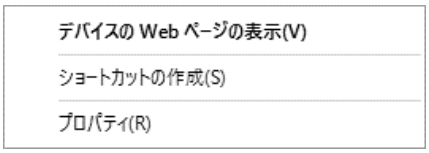
詳細情報

iLO NIC 自動選択の有効化

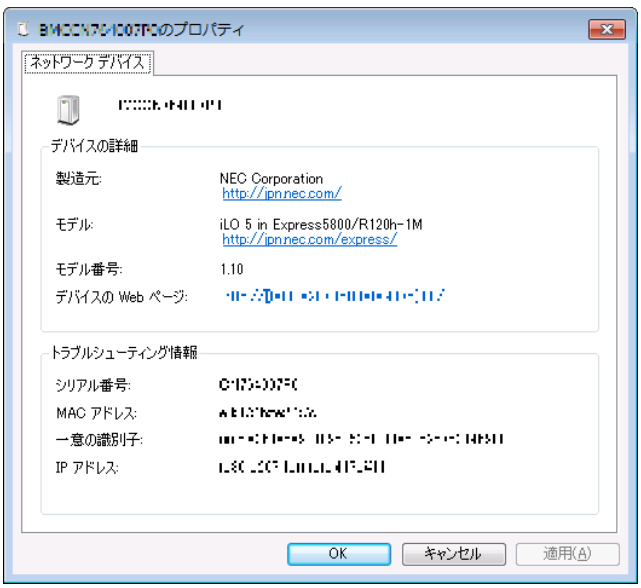
Windows ネットワークフォルダー内の iLO システムの表示

UPnP が構成されている場合、Windows システムと同じネットワーク上の iLO システムが Windows の ネットワークフォルダーに表示されます。Windows の設定によっては表示されない場合があります。

- iLO システムの Web インターフェースを起動するには、Windows の ネットワークフォルダーでシステムを右クリックし、デバイスの **Web** ページの表示を選択します。



- iLO システムのプロパティを表示するには、Windows の ネットワークフォルダーにあるアイコンを右クリックし、プロパティを選択します。Windows のバージョンや設定によっては表示されない場合があります。



プロパティウィンドウには、以下の設定があります。

- **デバイスの詳細** - iLO ソフトウェアのメーカーとバージョン情報。iLO Web インターフェースを開始するには、デバイスの **Web** ページのリンクをクリックします。
- **トラブルシューティング情報** - iLO のシリアル番号、MAC アドレス、UUID、および IP アドレス。

15. iLO 管理機能の使用

iLO のユーザーアカウント

iLO では、安全な iLO メモリにローカルで保存されているユーザーアカウントとディレクトリグループアカウントを管理できます。MMC を使用して、ディレクトリベースのユーザーアカウントを管理します。

最大 12 個のローカルユーザーアカウントを、カスタムのログイン名と高度なパスワード暗号化を使用して作成できます。権限は各ユーザーの設定を制御し、ユーザーのアクセス要件に合わせてカスタマイズできます。

13 ユーザー以上をサポートするには、ディレクトリサービスを使用した認証を行う必要があります。ディレクトリ認証を行うためには、リモートマネージメント拡張ライセンス(Advanced)またはリモートマネージメント拡張ライセンス(Scale-out)が必要です。
NX7700x シリーズサーバは、工場出荷時に標準でリモートマネージメント拡張ライセンス(Advanced)をインストール済みです。

iLO Firmware Version 1.20 Feb 02 2018 以降では、iLO のユーザーアカウントをローカルユーザーとサービスアカウントの 2 種類に区別することができます。ローカルユーザーは、通常 iLO を操作する際に使用するユーザーアカウントです。サービスアカウントは、管理用ソフトウェア（例えば、ESMPRO/ServerManager）が使用するユーザーアカウントです。iLO では、ユーザーが使用する通常のユーザーアカウントと、管理用ソフトウェアが使用するユーザーアカウントを区別して管理できます。通常のローカルユーザーと、サービスアカウントは別々に表示されます。なお、通常のユーザーアカウントとサービスアカウントは、表示が異なるだけで機能的な違いはありません。

ユーザーおよびディレクトリグループの管理には、以下の権限が必要です。

- **[Administer User Accounts]** - ユーザーの追加、変更、および削除に必要です。この権限がないと、本人の設定の表示と本人のパスワードの変更しか実行できません。
- **[Configure iLO Settings]** - ディレクトリグループの追加、変更、および削除に必要です。この権限がないと、ディレクトリグループの表示しか実行できません。

システムユーティリティ内の BMC 構成ユーティリティを使用してユーザーを管理することもできます。

ヒント：ユーザーのログイン名には、英数字と、-(ハイフン)、,(ドット)、_(アンダースコア)を使用可能です。ユーザーのユーザー名とパスワードには、英数字と記号（アスキーコード 0x20～0x7e）が使用可能です。

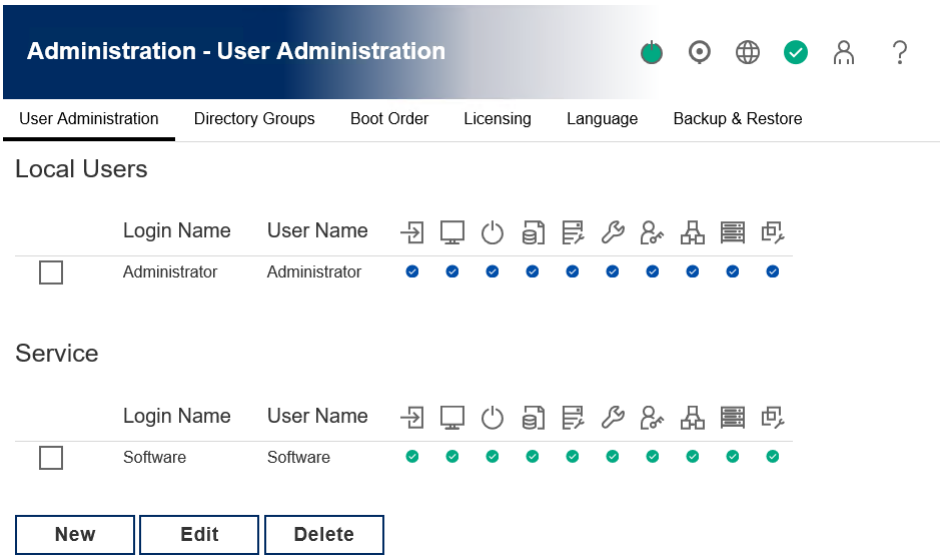
ローカルユーザーアカウントの表示

前提条件

ユーザーアカウント管理権限

手順

[Administration]→[User Administration]ページに移動します。



[Local Users]には、設定された各ユーザーのログイン名、ユーザー名、および割り当てられた権限が表示されます。権限の名前を参照するには、カーソルをアイコン上に移動します。

サービスアカウントの表示（iLO Firmware Version 1.20 Feb 02 2018 以降）

[Administration]→**[User Administration]**ページに移動します。
[Service]には、設定されたサービスアカウントのログイン名、ユーザー名、および割り当てられた権限が表示されます。

iLO ユーザー権限

次の権限は、ユーザーアカウントに適用されます。

1. **[Login]** - iLO にログインできます。
2. **[Remote Console]** - ビデオ、キーボード、マウスの制御を含めて、ホストシステムのリモートコンソールにリモートにアクセスできます。
3. **[Virtual Power and Reset]** - ホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。この権限を持つユーザーは、**[Generate NMI to System]**ボタンを使用してシステムを診断できます。
4. **[Virtual Media]** - ホストシステム上の仮想メディア機能を使用できます。
5. **[Host BIOS]** –システムユーティリティを使用してホスト BIOS 設定を構成できます。
6. **[Configure iLO Settings]** - セキュリティ設定を含むほとんどの iLO 設定を変更し、リモートに iLO ファームウェアを更新することができます。この権限では、ローカルユーザーアカウントは管理できません。

   iLO を構成したら、Web インターフェース、または CLI を使用して、すべてのユーザーからこの権限を取り消して、再構成を防止します。システムユーティリティにアクセスできるユ

ーザーは、まだ iLO を再構成することができます。ユーザーアカウント管理権限を持つユーザーのみが、この権限を有効または無効にすることができます。

7. **[Administer User Accounts]** - ユーザーがローカル iLO ユーザーアカウントを追加、編集、および削除できるようにします。この権限を持つユーザーは、すべてのユーザーの権限を変更できます。この権限がないと、本人の設定の表示と本人のパスワードの変更しか実行できません。

8. **[Host NIC]** - ホストネットワークカード設定を構成できます。

9. **[Host Storage]** - ホストストレージ設定を構成できます。

10. **[Recovery Set]** - リカバリーインストールセットを管理できます。

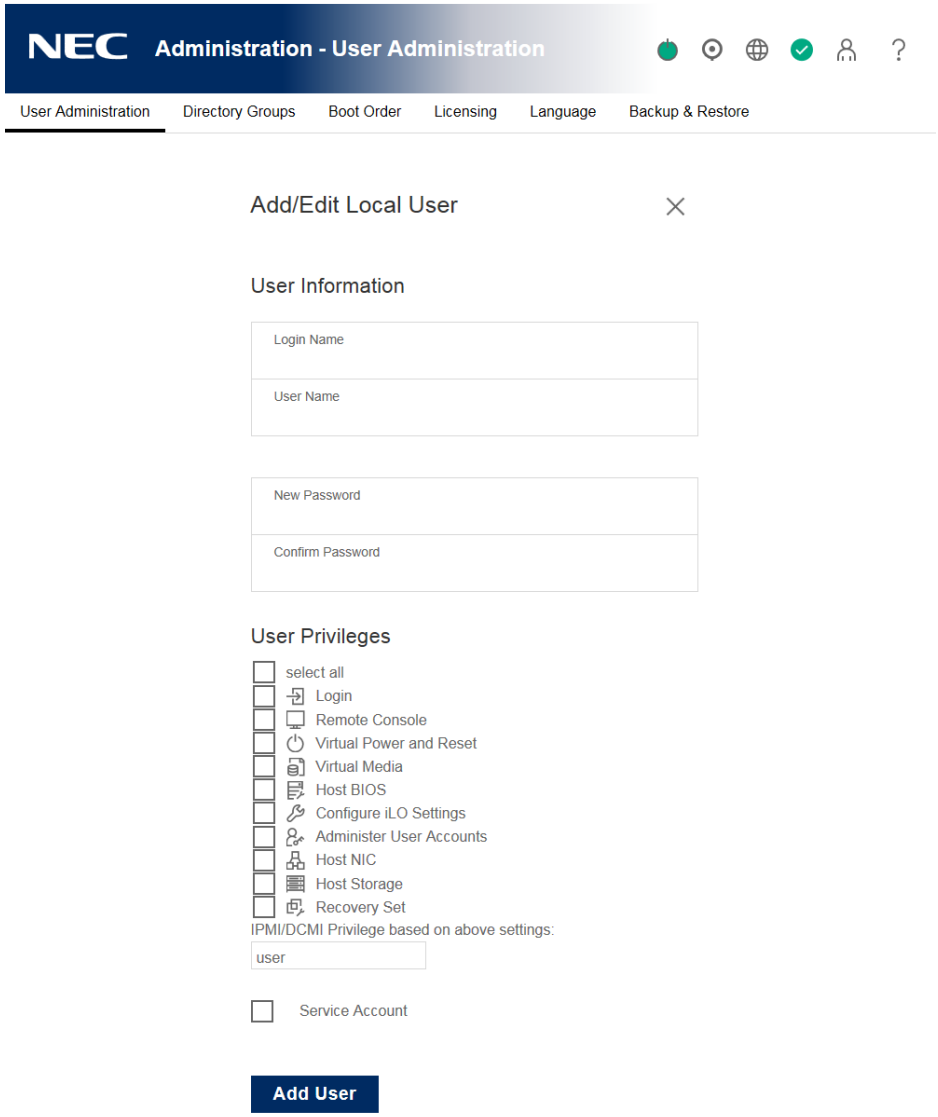
記注： **[Recovery Set]**権限は、**[Recovery Set]**を持ったユーザーからのみ権限追加を行うことができます。

ローカルユーザーアカウントの追加

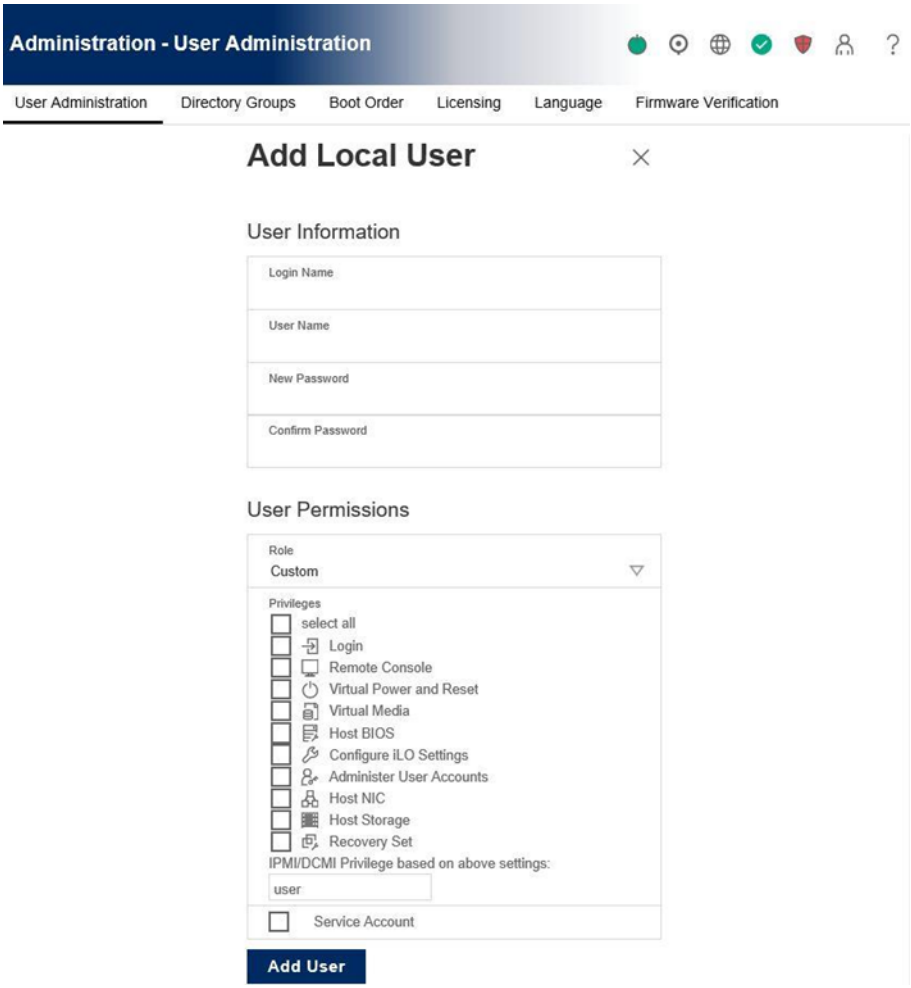
前提条件
ユーザーアカウント管理権限

手順
1. **[Administration]**→**[User Administration]**ページに移動します。
2. **[New]**をクリックして、ローカルユーザーの追加ページを開きます。

＜iLO 5 Firmware Version 2.18 Jun 22 2020 以前＞



＜iLO 5 Firmware Version 2.31 Oct 13 2020 以降＞



3. **[User Information]**セクションで次の詳細を入力します。
   - **[Login Name]**
   - **[User Name]**
   - **[New Password]**と**[Confirm Password]**
4. [User Permissions] - [Role] セッションで、事前定義されたユーザー権限セットを選択します。(iLO 5 Firmware Version 2.31 Oct 13 2020 以降の場合)
   - **[Administrator]** - 管理者は、全ての機能に対する読み取り/書き込みアクセス権を持っています。また、システムの操作、iLO をリセットしたり、ユーザーアカウントを管理したりすることができます。
   - **[Operator]** - オペレーターは、システムの操作を実行できますが、iLO をリセットしたり、ユーザーアカウントを管理することはできません。
   - **[ReadOnly]** - ユーザーは、読み取り専用アクセス権を持っています。ユーザーは、iLO の設定または書き込み及びシステムの操作は実行できません。
   - **[Custom]** - ユーザーは、上記以外のカスタム権限を持っています。カスタム権限は、[Privileges]セクションにおいて、ユーザーに与える権限を選択できます。
     手動で[Privileges]を選択する場合は、デフォルトの[Custom]を使用します。

5. [User Permissions/**User Privileges] - [Privileges]** セクションで、追加するユーザーに与える権限を選択します。

   使用できるすべてのユーザー権限を選択するには、**[select all]**チェックボックスをクリックします。
6. iLO Firmware Version 1.20 Feb 02 2018 以降の場合、 **[Service Account]**チェックボックスで追加するユーザーを通常のローカルユーザーとするかサービスアカウントとするか指定します。サービスアカウントとして登録する場合は、チェックを入れてください。
7. 新しいユーザーを保存するには、**[Add User]**をクリックします。

詳細情報

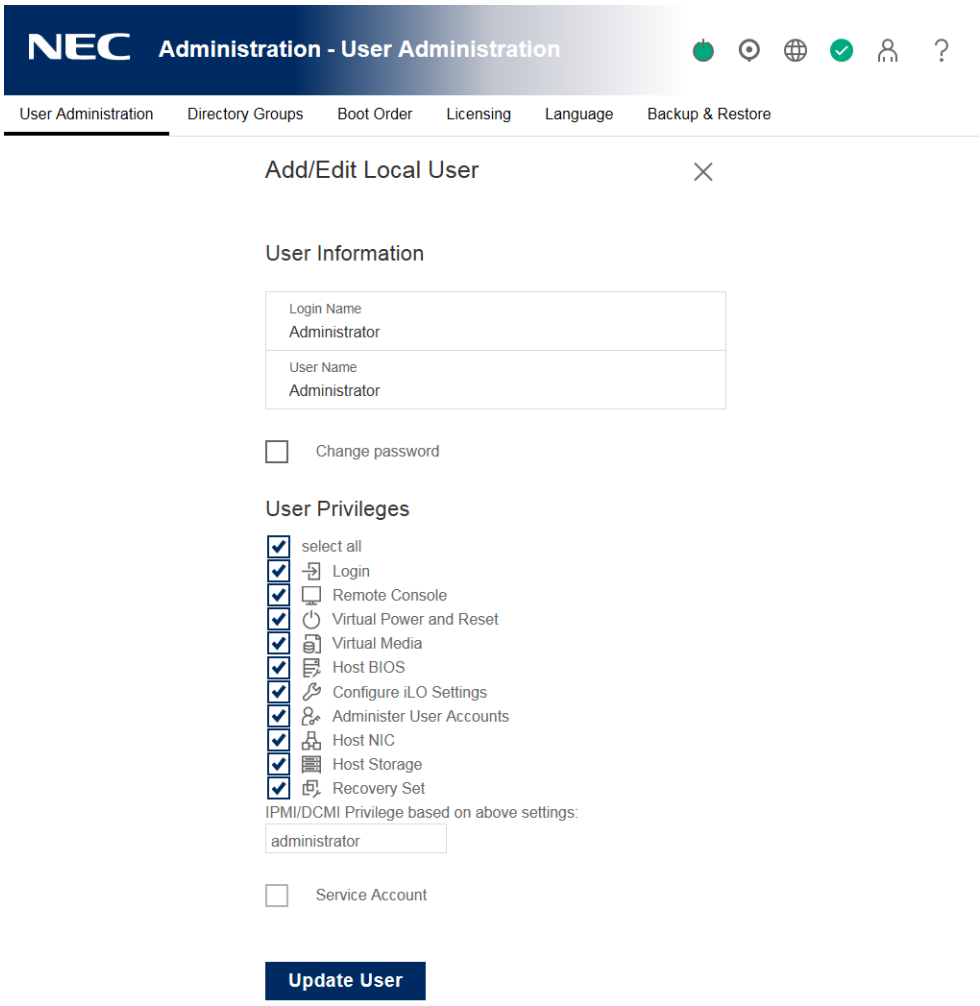
iLO ユーザー権限
ユーザーアカウントオプション
パスワードに関するガイドライン

ローカルユーザーアカウント・サービスアカウントの編集

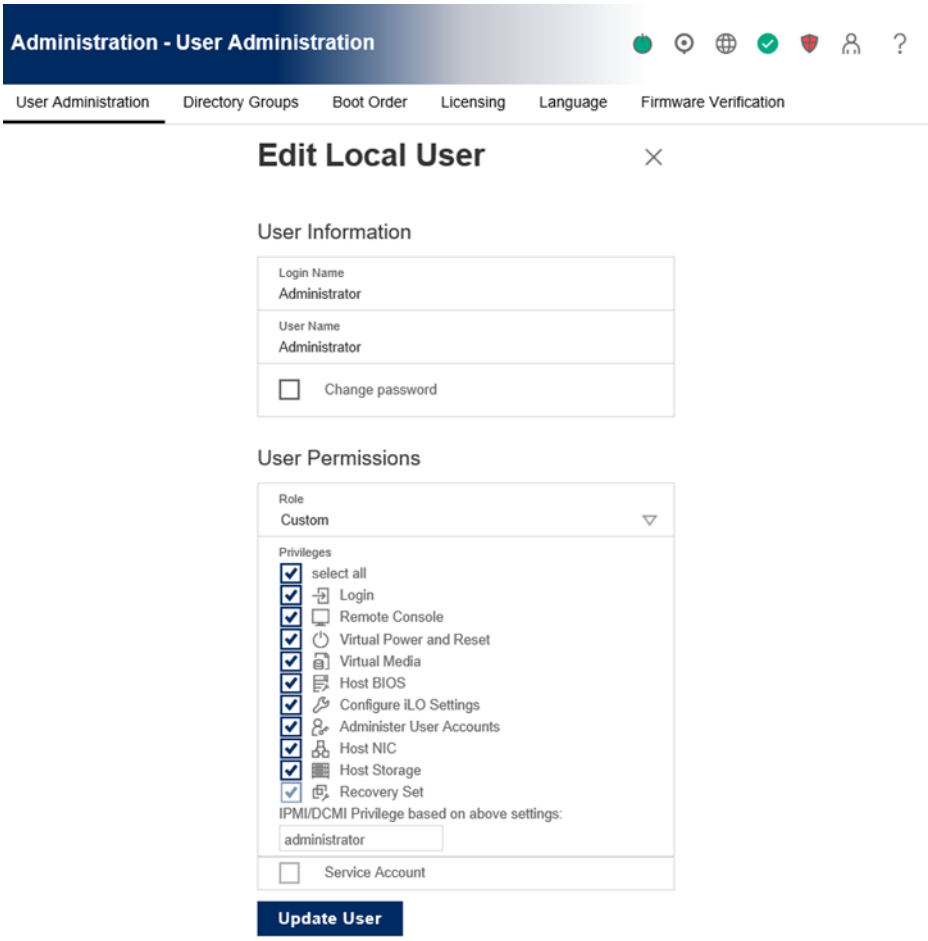
前提条件
ユーザーアカウント管理権限

手順

1. **[Administration]→[User Administration]**ページに移動します。
2. ユーザーを選択し、**[Edit]**をクリックします。
   ＜iLO 5 Firmware Version 2.18 Jun 22 2020 以前＞



＜iLO 5 Firmware Version 2.31 Oct 13 2020 以降＞



3. 必要に応じて、以下の値をローカルユーザーの編集ページに入力します。
   - **[Login Name]**
   - **[User Name]**
4. パスワードを変更するには、**[Change password]**チェックボックスをクリックし、**[New Password]**と **[Confirm Password]**の値を更新します。
5. **[User Permissions] - [Role]** セクションで、事前定義されたユーザー権限セットを選択します。
   (iLO 5 Firmware Version 2.31 Oct 13 2020 以降の場合)
   - **[Administrator]** - 管理者は、全ての機能に対する読み取り/書き込みアクセス権を持っています。また、システムの操作、iLO をリセットしたり、ユーザーアカウントを管理したりすることができます。
   - **[Operator]** - オペレーターは、システムの操作を実行できますが、iLO をリセットしたり、ユーザーアカウントを管理することはできません。
   - **[ReadOnly]** - ユーザーは、読み取り専用アクセス権を持っています。ユーザーは、iLO の設定または書き込み及びシステムの操作は実行できません。
   - **[Custom]** - ユーザーは、上記以外のカスタム権限を持っています。カスタム権限は、[Privileges]セクションにおいて、ユーザーに与える権限を選択できます。
     手動で[Privileges]を選択する場合は、デフォルトの[Custom]を使用します。

6. [User Permissions/**User Privileges] - [Privileges]** セクションで、ユーザーに与える権限を選択します。
   使用できるすべてのユーザー権限を選択するには、**[select all]**チェックボックスをクリックします。
7. ユーザーアカウントの変更を保存するには、**[Update User]**をクリックします。
   この時、**[Service Account]**は変更できません。

詳細情報
iLO ユーザー権限

ユーザーアカウントオプション
パスワードに関するガイドライン

ユーザーアカウント・サービスアカウントオプション

ユーザーアカウント・サービスアカウントを追加および編集する場合、次のオプションを使用できます。

- **[User Name]**は、**[User Administration]**ページのユーザーリストに表示されます。**[Login Name]**と同じである必要はありません。ユーザー名は、最長 39 文字です。**[User Name]**には、印字可能な文字を使用する必要があります。先頭に空白文字は使用しないでください。わかりやすいユーザー名を割り当てると、簡単に各ログイン名の所有者を特定することができます。
- **[Login Name]**は、iLO にログインするときに使用する名前です。この名前は、**[User Administration]**ページおよび **[Information]** →**[Session List]**ページのセッションリストと、ログに表示されます。**[Login Name]**は、**[User Name]**と同じである必要はありません。ログイン名の最大長は 39 文字です。ログイン名には、印刷可能な文字を使用する必要があります。先頭に空白文字は使用しないでください。
- **[New Password]**と **[Confirm Password]**で、iLO にログインするために使用するパスワードの設定と確認を行います。
- **[Service Account]**でユーザーをサービスアカウントにするか指定します。サービスアカウントとして登録する場合は、チェックを入れてください。なお、この設定はユーザー新規作成時のみ変更可能です。このオプションは、iLO Firmware Version 1.20 Feb 02 2018 以降で使用可能です。

パスワードに関するガイドライン

ユーザーアカウントを作成および編集する場合は、これらのパスワードに関するガイドラインに従うことをおすすめします。

- パスワードは
  - 書き留めたり記録したりしないでください。
  - 書き留めたり記録したりしないでください。

- パスワードを他のユーザーと共有しないでください。
- 辞書にあるような単語を使用しないでください。
- 会社名、製品名、ユーザー名、ログイン名のような推測しやすいものを避けてください。

- パスワードの強度を確保するため、少なくとも以下の 3 つの条件を満たす文字列をパスワードに設定することをおすすめします。
  - 1 文字以上の数字
  - 1 文字以上の特殊文字
  - 1 文字以上の小文字
  - 1 文字以上の大文字

> △**参考:**
> iLO 5 Firmware Version 2.55 Nov 22 2021 以降では、パスワードは 60 文字まで設定可能です。

- iLO ユーザーアカウントのパスワードの最低文字数は、アクセス設定のページで設定します。構成された**[Minimum Password Length]**値によって、パスワードの長さは最小 0 文字（パスワードなし）から最大 39 文字まで可能です。デフォルトの**[Minimum Password Length]**は、8 文字です。

ⓘ 重要: 保護されたデータセンターの外側に拡大されることのない物理的に安全な管理ネットワークがない場合は、**[Minimum Password Length]**を 8 文字未満に設定することはおすすめできません。**[Minimum Password Length]**の設定については、「iLO アクセスの設定」を参照してください。

> △**注意:**
> [Require Login for iLO RBSU]が[**Enabled**]の場合、「システムユーティリティ」起動時に管理者パスワードの入力が求められます。
> 「システムユーティリティ」で入力可能な文字は、「英数字、~!@#$%^&*()+`-={}:“|;‘<>,./\」と制限されるため、[**Require Login for iLO RBSU**]を[Enabled]する場合、パスワードに上記の文字を設定する必要があります。

IPMI/DCMI ユーザー

iLO ファームウェアは、IPMI 2.0 仕様に準拠しています。IPMI/DCMI ユーザーを追加する場合、ログイン名は最長 16 文字、パスワードは最長 20 文字です。使用できるログイン名やパスワードは IPMI の仕様に準じます。

iLO ユーザー権限を選択すると、等価な IPMI/DCMI ユーザー権限が **[IPMI/DCMI Privilege based on above settings]**ボックスに表示されます。

- **[user]** - ユーザーは読み取り専用アクセス権を持っています。ユーザーは、iLO の設定または書き込みやシステムの操作は実行できません。

IPMI ユーザー権限については、すべての権限を無効にします。オペレーターレベルを満たさない権限の任意の組み合わせは、IPMI ユーザーです。

- **[operator]** -オペレーターは、システムの操作を実行できますが、iLO を設定したり、ユーザーアカウントを管理したりすることはできません。
  IPMI オペレーター権限については、リモートコンソールアクセス、仮想電源およびリセット、および仮想メディアを有効にします。管理者レベルを満たさないオペレーター以上の権限の任意の組み合わせは、IPMI ユーザーです。
- **[administrator]** - 管理者は、すべての機能に対する読み取り/書き込みアクセス権を持っています。
  IPMI 管理者権限については、すべての権限を有効にします。

ディレクトリグループの表示

[Administration]→[Directory Groups]ページに移動します。

[Directory Groups]テーブルには、設定されたグループのグループ DN、グループ SID、および割り当てられた権限が表示されます。権限の名前を参照するには、カーソルをアイコン上に移動します。

ディレクトリグループ権限

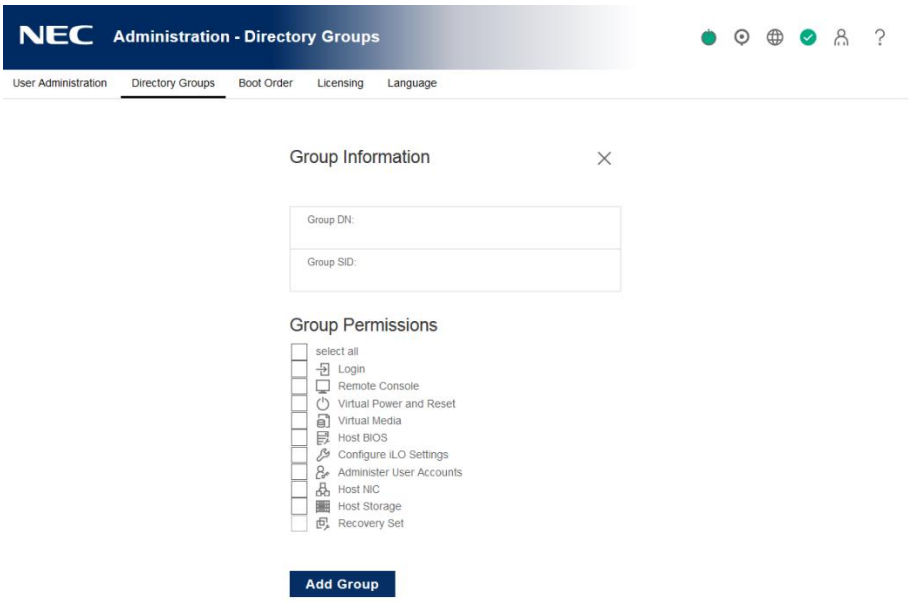
次の権限は、ディレクトリグループに適用されます。

- **[Login]** - iLO にログインできます。
- **[Remote Console]** - ビデオ、キーボード、マウスの制御を含めて、ホストシステムのリモートコンソールにリモートにアクセスできます。
- **[Virtual Power and Reset]** - ホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。この権限を持つユーザーは、**[Generate NMI to System]**ボタンを使用してシステムを診断できます。
- **[Virtual Media]** - ホストシステム上の仮想メディア機能を使用できます。
- **[Host BIOS]** - システムユーティリティを使用してホスト BIOS 設定を構成できます。
- **[Configure iLO Settings]** - セキュリティ設定を含むほとんどの iLO 設定を変更し、リモートに iLO ファームウェアを更新することができます。この権限では、ローカルユーザーアカウントは管理できません。
  iLO を構成したら、Web インターフェース、または CLI を使用して、すべてのユーザーからこの権限を取り消して、再構成を防止します。システムユーティリティにアクセスできるユーザーは、まだ iLO を再構成することができます。ユーザーアカウント管理権限を持つユーザーのみが、この権限を有効または無効にすることができます。
- **[Administer User Accounts]** - ユーザーがローカル iLO ユーザーアカウントを追加、編集、および削除できるようにします。この権限を持つユーザーは、すべてのユーザーの権限を変更できます。この権限がないと、本人の設定の表示と本人のパスワードの変更しか実行できません。
- **[Host NIC]** - ホストネットワークカード設定を構成できます。
- **[Host Storage]** - ホストストレージ設定を構成できます。
- **[Recovery Set]** - リカバリーインストールセットを管理できます。

ディレクトリグループの追加

前提条件
iLO の設定を構成権限

手順
1. **[Administration]→[Directory Groups]**ページに移動します。
2. **[New]**をクリックします。



3. **[Group Information]**セクションで、以下の詳細を提供します。
   - **[Group DN]**（セキュリティグループ DN） - このグループのメンバーには、グループに設定された権限が付与されます。ここで指定するグループは、ディレクトリに存在しなければならず、iLO にアクセスする必要があるユーザーは、このグループのメンバーでなければなりません。ディレクトリに存在する DN を入力します（たとえば、CN=Group1, OU=Managed Groups, DC=domain, DC=extension）。

     短縮された DN もサポートされます（たとえば、Group1）。短縮された DN は、一意に一致するものではありません。完全修飾の DN を使用することをおすすめします。
   - **[Group SID]**（セキュリティ ID） - Microsoft セキュリティ ID（SID）は、Kerberos および LDAP グループの権限付与に使用されます。これは Kerberos に必要です。必要な形式は、S-1-5-2039349 です。
4. **[Group Permissions]**セクションで、ディレクトリグループに与える権限を選択します。
5. 新しいディレクトリグループを保存するには、**[Add Group]**をクリックします。

詳細情報
ディレクトリグループ権限

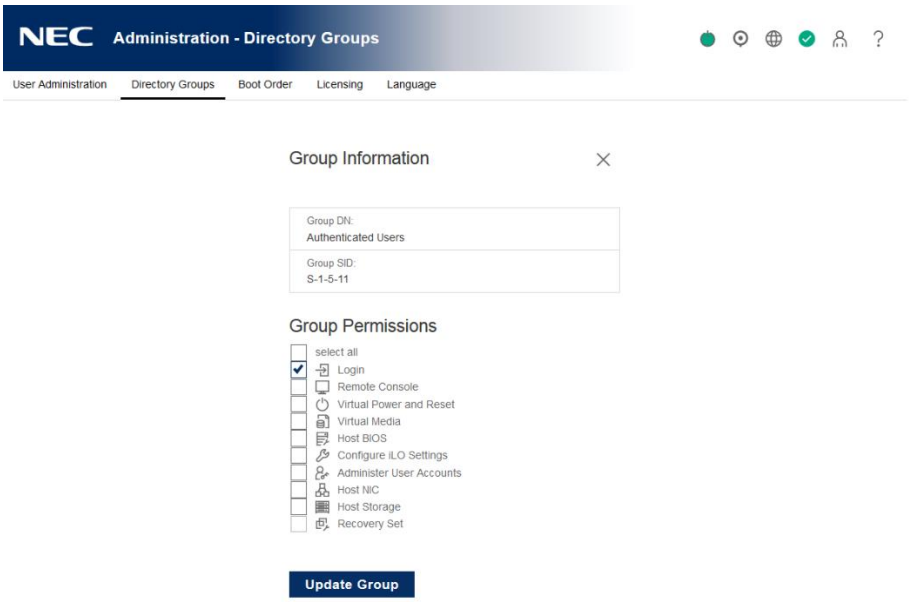
ディレクトリグループの編集

前提条件

iLO の設定を構成権限

手順

1. **[Administration]→[Directory Groups]**ページに移動します。
2. 編集したいグループを選択し、**[Edit]**をクリックします。



3. **[Group Information]**セクションで、以下の詳細を提供します。
   - **[Group DN]**（セキュリティグループ DN） - このグループのメンバーには、グループに設定された権限が付与されます。ここで指定するグループは、ディレクトリに存在しなければならず、iLO にアクセスする必要があるユーザーは、このグループのメンバーでなければなりません。ディレクトリに存在する DN を入力します（たとえば、CN=Group1, OU=Managed Groups, DC=domain, DC=extension）。

     短縮された DN もサポートされます（たとえば、Group1）。短縮された DN は、一意に一致するものではありません。完全修飾の DN を使用することをおすすめします。
   - **[Group SID]**（セキュリティ ID） - Microsoft セキュリティ ID（SID）は、Kerberos および LDAP グループの権限付与に使用されます。これは Kerberos に必要です。必要な形式は、S-1-5-2039349 です。
4. [**Group Permissions**]セクションで、ディレクトリグループに与える権限を選択します。
5. ディレクトリグループの変更を保存するには、[Update Group]をクリックします。

詳細情報

ディレクトリグループ権限

ユーザーアカウントまたはディレクトリグループの削除

前提条件

- ローカルユーザーアカウントの削除：ユーザーアカウント管理権限
- ディレクトリグループの削除：iLO の設定を構成権限

手順

1. **[Administration]→[Directory Groups]**ページに移動します。
2. 削除するユーザーまたはグループの横にあるチェックボックスを選択します。
3. **[削除]** をクリックします。

   ポップアップウィンドウが開き、次のいずれかのメッセージが表示されます。

   - ローカルユーザー：選択されたユーザーを削除しますか? 警告：少なくとも 1 つは管理者を残してください。
   - ディレクトリグループ：選択されたグループを削除しますか?
4. **[OK]** をクリックします。

ブート順序

仮想メディアのブート順序機能を使用すると、サーバーのブートオプションを設定できます。ブートモード、ブート順序またはワンタイムブートステータスの変更を行う場合、サーバーのリセットが必要になることがあります。リセットが必要な場合は iLO によって通知されます。POST の実行中はブート順序を変更できません。サーバーが POST を実行している時にサーバーのブート順序を変更しようとすると、エラーが発生します。エラーが発生した場合、POST が終了するのを待ってから、再試行してください。

サーバーブートモードの設定

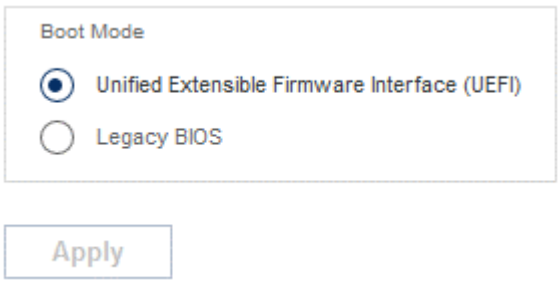
ブートモードの設定を使用して、サーバーが OS の起動ファームウェアを検索する方法を定義します。UEFI または従来のレガシーBIOS を選択することができます。

前提条件

iLO の設定を構成権限

手順

1. **[Administration]→[Boot Order]**ページに移動します。
2. **[Unified Extensible Firmware Interface (UEFI)]**または**[Legacy BIOS]**を選択します。



3. **[Apply]**をクリックします。

   iLO に、変更の確認を求めるメッセージが表示されます。この設定を変更すると、サーバーをリセットするまで、**[Boot Order]**のページで変更を追加することはできません。
4. **[OK]**をクリックして変更を確定します。
5. サーバーをリセットします。

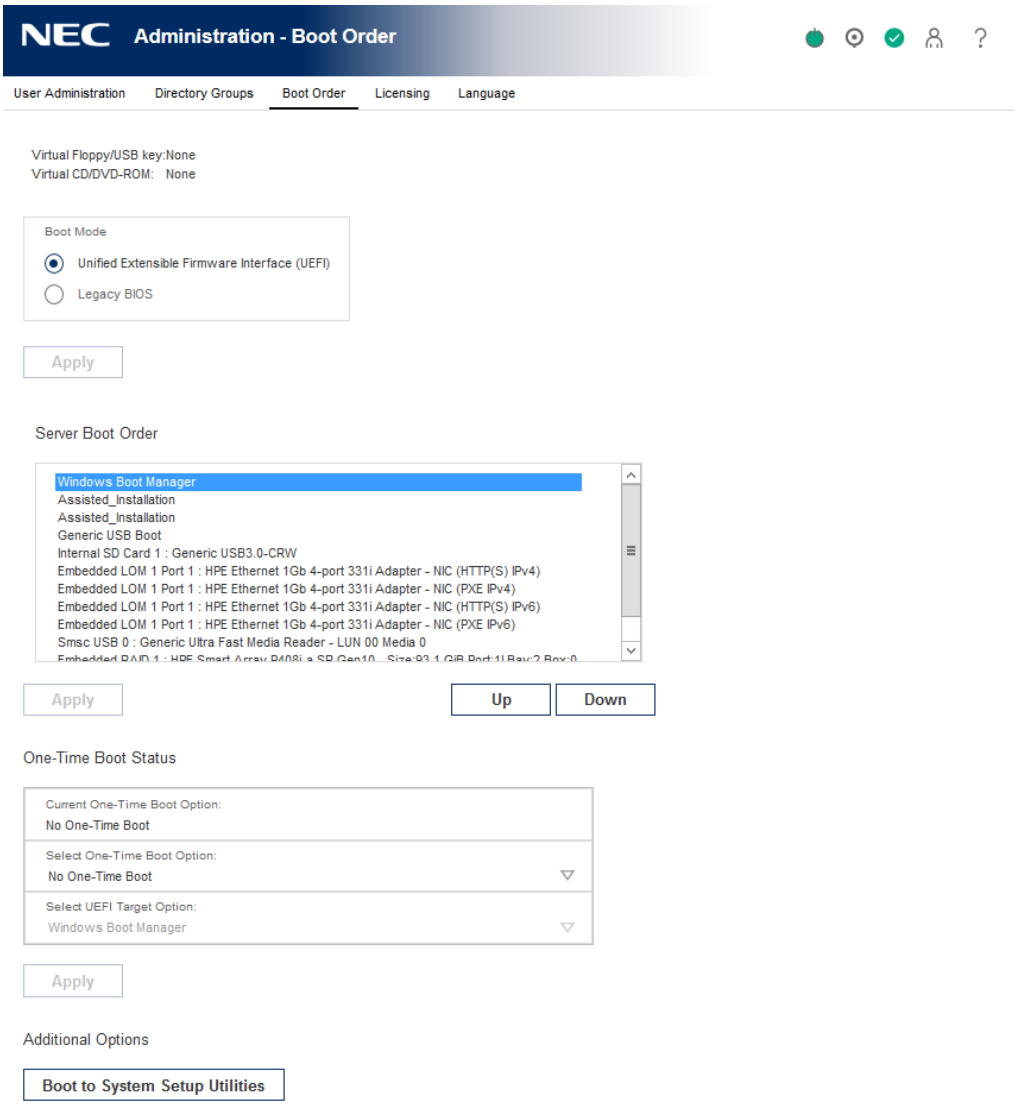
サーバーブート順序の設定

前提条件

iLO の設定を構成権限

手順

1. **[Administration]→[Boot Order]**ページに移動します。



仮想メディアが接続されると、iLO の Web インターフェースは、ページ上部の**[Virtual Floppy/USB key]**および**[Virtual CD/DVD-ROM]**テキストの横に仮想メディアタイプを表示します。

2. **[Server Boot Order]**リストでデバイスを選択し、**[Up]**または**[Down]**をクリックしてブート順序の位置を変更します。

   レガシーBIOS モードでは、以下のデバイスから選択します。

   - **CD/DVD Drive**
   - **USB Storage Drive**
   - **Hard Disk Drive**
   - **Network Device** 番号。サーバーEthernet カードおよび追加の NIC/FlexibleLOM カードはネットワークデバイス 1、2、3 などになります。

   UEFI モードでは、使用可能なブートデバイスのリストからオプションを選択します。

3. **[Apply]**をクリックします。

   iLO は、ブート順序が正常に更新されたことを確認します。

ワンタイムブートステータスの変更

ワンタイムブートステータス機能を使用して、定義済みのブート順序を変更せずに、次回のサーバーリセット時にのみ起動するメディアタイプを設定します。使用する手順は、サーバーがレガシーBIOS モードを使用するか UEFI モードを使用するかによって異なります。

前提条件

iLO の設定を構成権限

レガシーBIOS モードでのワンタイムブートステータスの変更

前提条件

iLO の設定を構成権限

手順

1. **[Administration]→[Boot Order]**ページに移動します。
2. **One-Time Boot Status セクションの[Select One-Time Boot Option:]**リストから、オプションを選択します。

以下のオプションを使用できます。

- **[No One-Time Boot]**
- **[CD/DVD Drive]**
- **[USB Storage Device]**
- **[Hard Disk Drive]**
- **[Network Device]**番号。サーバーEthernet カードはネットワークデバイス 1、追加の NIC/FlexibleLOM カードはネットワークデバイス 2、3 などになります。
- **[EXPRESSBUILDER]** - EXPRESSBUILDER が起動します。
- **[HTTP Boot]** -このオプションを選択すると、HTTP ブート機能が有効であり、ブート可能イメージの URI が ROM ベースシステムユーティリティで定義されている場合、サーバーは HTTP URI で起動します。
- **[Embedded UEFI Shell]** - このオプションを選択した場合、サーバーは、システムユーティリティから分離した組み込みシェル環境からブートします。

3. **[Apply]**をクリックします。

iLO は、ワンタイムブートオプションが正常に更新されたことを確認します。

[Current One-Time Boot Option:] の値が更新され、選択内容が示されます。

UEFI モードでのワンタイムブートステータスの変更

前提条件

iLO の設定を構成権限

手順

1. **[Administration]→[Boot Order]**ページに移動します。
2. **One-Time Boot Status セクションの[Select One-Time Boot Option:]**リストから、オプションを選択します。

   以下のオプションを使用できます。

   - **[No One-Time Boot]**
   - **[CD/DVD Drive]**
   - **[USB Storage Device]**
   - **[Hard Disk Drive]**
   - **[Network Device]** 番号。サーバー Ethernet カードはネットワークデバイス 1、追加の NIC/FlexibleLOM カードはネットワークデバイス 2、3 などになります。
   - **[EXPRESSBUILDER]** - EXPRESSBUILDER が起動します。
   - **[HTTP Boot]** -このオプションを選択すると、HTTP ブート機能が有効であり、ブート可能イメージの URI が ROM ベースシステムユーティリティで定義されている場合、サーバーは HTTP URI で起動します。
   - **[UEFITarget]** - このオプションを選択した場合、**[Select UEFI Target Option:]**リストの使用可能なブートデバイスの一覧から選択できます。
   - **[Embedded UEFI Shell]** - このオプションを選択した場合、サーバーは、システムユーティリティから分離した組み込みシェル環境からブートします。
3. **[Select One-Time Boot Option:]**リストで**[UEFI Target]**を選択した場合は、**[Select UEFI Target Option:]**リストから起動デバイスを選択します。たとえば、2 つの起動可能なパーティションを含むハードディスクドライブがある場合、このオプションを使用して、次のサーバーリセット時に使用する起動可能なパーティションを選択します。
4. **[Apply]**をクリックします。

   iLO はワンタイムブートオプションが正常に更新されたことを確認します。

   [Current One-Time Boot Option:]の値が更新され、選択内容が示されます。

追加オプションの使用

前提条件

iLO の設定を構成権限

手順

ブート順序のページの Additional Options セクションには、システムセットアップユーティリティを起動するボタンがあります。

1. **[Administration]→[Boot Order]**ページに移動します。
2. **[Boot to System Setup Utilities]**をクリックし、次回のサーバーリセットで ROM ベースのセットアップユーティリティをロードします。この機能を使用するには、仮想メディアおよび iLO の設定を構成権限。が必要です。

iLO ライセンス

iLO 標準機能はすべてのサーバーに搭載され、サーバーセットアップ、サーバーヘルスの監視、電力と温度制御の監視、およびリモートサーバー管理を簡素化します。

iLO ライセンスは、マルチユーザーコラボレーション用のグラフィカルリモートコンソール、ビデオの録画と再生のような機能や他の多くの機能を有効にします。

ライセンス情報

- 製品をインストールして使用するサーバー1 台ごとに 1 つの iLO ライセンスが必要です。ライセンスは譲渡できません。
- ライセンスキーを無くしても、再発行はできません。大切に保管してください。

ブラウザーを使用したライセンスキーのインストール

前提条件

iLO の設定を構成権限

手順

3. **[Administration]→[Licensing]**ページに移動します。
4. **[Activation Key]**ボックスにライセンスキーを入力します。

   Tab キーを押すか、**[Activation Key]**ボックスのセグメントの内側をクリックして、セグメント間を移動します。**[Activation Key]**ボックスのセグメントにデータを入力すると、カーソルは自動的に次に進みます。
5. **[Install]**をクリックします。

   エンドユーザー使用許諾契約の確認画面が表示されます。エンドユーザー使用許諾契約の詳細は、ライセンスパックオプションキットに記載されています。
6. **[OK]** をクリックします。

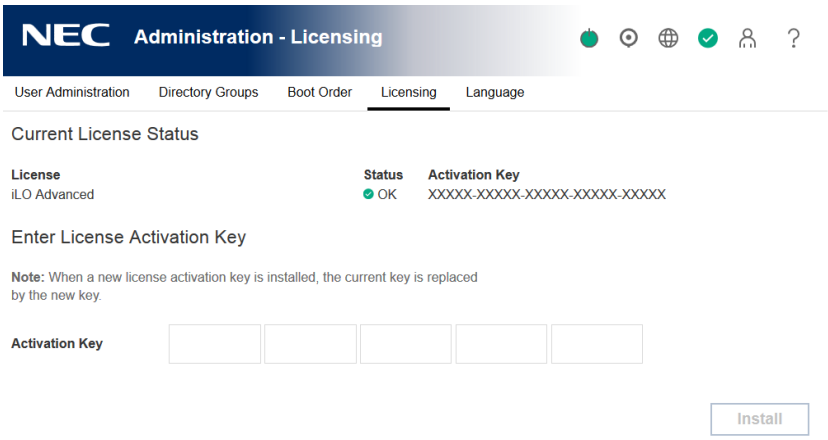
   これで、ライセンスキーは有効になります。

ライセンスのインストールに関するトラブルシューティングヒントについては、「ライセンスのインストールに失敗する」を参照してください。

ライセンス情報の表示

手順

[Administration]→[Licensing]ページに移動します。



ライセンスの詳細

- **[License]** - ライセンス名
- **[Status]** - ライセンスのステータス
- **[Activation Key]** - インストールされているキー（最後のセグメントのみ表示されます。）

言語パック

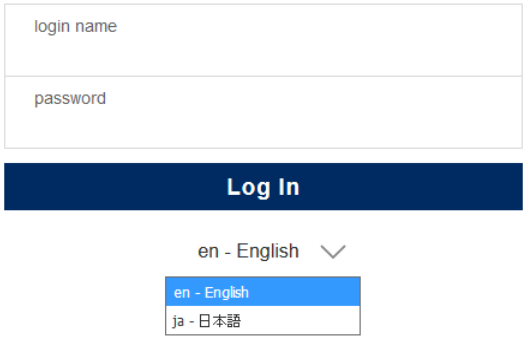
言語パックを使用すると、iLO の Web インターフェースの表示言語を英語だけでなく日本語も使用可能となります。言語パックは、iLO の Web インターフェース、.NET IRC、および Java IRC の翻訳を提供しています。
言語パックを使用する場合は、以下の点に注意してください。

- 提供されている言語パックは日本語です(装置出荷時から適用されています)。
- 言語パックはアンインストールできません。
- Java IRC および.NET IRC は、現在の iLO セッションの言語を使用します。
- Windows システムでの Java IRC のローカリゼーションサポートでは、**[地域と言語]**コントロールパネルで正しい言語を選択する必要があります。
- Linux システムでの Java IRC のローカリゼーションサポートでは、指定した言語用のフォントがインストールされ、そのフォントを JRE が使用できることを確認してください。
- インストールされている言語パックにテキスト文字列の翻訳が含まれていない場合、テキストは英語で表示されます。
- iLO ファームウェアを更新する場合は、言語パックの内容が iLO の Web インターフェースに対応するように、最新の言語パックをインストールすることを推奨いたします。言語パックのインストール手順に関しては「言語パックのインストール」の章を参照してください。

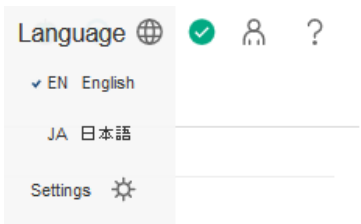
言語パックの選択

次のいずれかの方法を使用して、インストール済みの言語パックを選択します。

- ログインページに移動し、言語メニューで言語を選択します。



- ブラウザーウィンドウの右上のツールメニューで🌐をクリックし、言語を選択します。



- **[Administration]→[Language]**ページで、言語を選択します。手順については、「現在のブラウザーセッション言語の構成」を参照してください。

デフォルト言語の設定

前提条件
iLO の設定を構成権限

手順

1. **[Administration]→ [Language]**ページに移動します。
2. **[Default Language]**メニューで値を選択します。

   選択できる言語は英語です。英語以外の言語も言語パックがインストールされていれば選択できます。
3. **[Apply]**をクリックします。

   デフォルト言語が変更されたことが、iLO によって通知されます。以降の iLO Web インターフェースセッションでは、前のセッションからのブラウザーの Cookie がなく、ブラウザーまたは OS の言語をサポートしていない場合、iLO Web インターフェースに設定済みのデフォルト言語を使用します。

現在のブラウザーセッション言語の構成

手順

1. **[Administration]→ [Language]**ページに移動します。
2. **[Installed Languages]**でインストールされた言語をクリックします。現在のブラウザーセッションの iLO Web インターフェースが、選択された言語に変更されます。

   選択できる言語は英語です。英語以外の言語も言語パックがインストールされていれば選択できます。

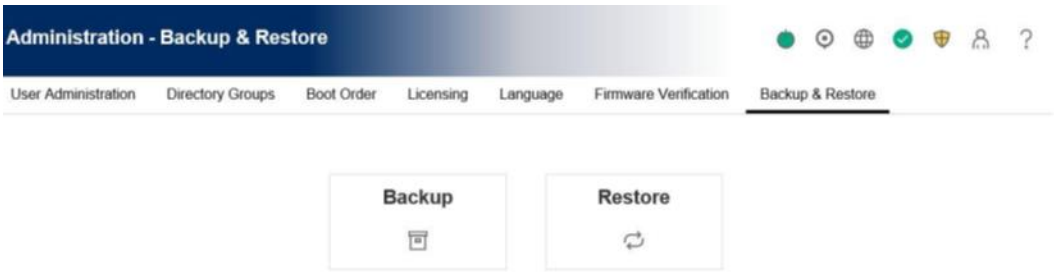
iLO がセッションの言語を決定する方法

iLO は、次のプロセスに基づいて Web インターフェースセッションの言語を決定します。

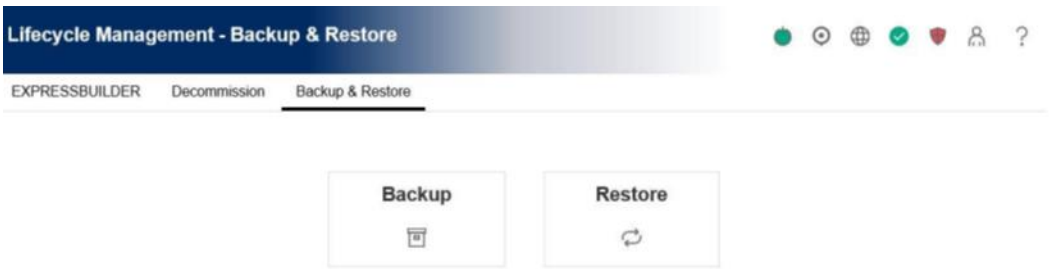
1. iLO Web インターフェースへのログインに使用するコンピューターおよびブラウザーが前回と同じで、ユーザーが Cookie を消去していない場合は、当該の iLO プロセッサーとの最後のセッションの言語設定が使用されます。
2. Cookie がない場合は、現在のブラウザーの言語が使用されます。ただし、その言語が iLO でサポートされ、必要な言語パックがインストールされていなければなりません。
3. **Internet Explorer** のみ：ブラウザーの言語がサポートされていない場合は、OS の言語が使用されます。ただし、その言語が iLO でサポートされ、必要な言語パックがインストールされていなければなりません。
4. Cookie がなく、ブラウザーの言語も OS の言語もサポートされていない場合、iLO は設定済みのデフォルト言語を使用します。詳しくは、「デフォルト言語の設定」を参照してください。

iLO バックアップとリストア

＜iLO 5 Firmware Version 2.18 Jun 22 2020 以前＞



＜iLO 5 Firmware Version 2.31 Oct 13 2020 以降＞



バックアップとリストア機能を使用すると、故障によるマザーボード交換時などに、事前にバックアップした iLO 設定をリストアできます。**この機能は、設定を複製して別の iLO システムに適用するものではありません。**バックアップしたファイルは、バックアップを行った装置にのみリストア可能です。同一機種であっても、他装置にはリストアできません。
構成のバックアップを取っておくことで、通常の動作環境に容易にすばやく戻ることができる場合があります。
あらゆるコンピューターシステムと同様に、データをバックアップして障害の影響を最小限に抑えることをお勧めします。バックアップしたファイルは装置の iLO ファームウェアをアップデートするとリストアできなくなります。iLO ファームウェアをアップデートした際には、再度バックアップを行ってください。
次のような状況では iLO 構成のリストアが必要になる場合があります。

バッテリーの障害または取り外し
さまざまな設定パラメーターがバッテリー駆動の SRAM に保存されています。まれですが、バッテリー障害が発生する場合があります。状況によっては、バッテリーの取り外しと交換が必要になる場合があります。構成情報の消失を避けるために、バッテリーの交換後にバックアップファイルから iLO 設定をリストアします。

デフォルト設定へのリセット
場合によっては、iLO を工場出荷時のデフォルト設定にリセットし、iLO 以外の他の設定を消去することが必要になることがあります。この操作では、iLO 設定が消去されます。iLO 設定をすばやく復旧するには、工場出荷時のデフォルト設定へのリセットが完了した後、バックアップファイルから構成をリストアします。

設定の偶発的または不適切な変更

iLO 設定が不適切に変更され、場合によって、重要な設定が消失することがあります。iLO を工場出荷時のデフォルト設定に設定したり、ユーザーアカウントを削除したりした場合にこのような状況が発生することがあります。元の構成を回復するには、バックアップファイルから構成をリストアします。

マザーボードの取り付け

ハードウェアの問題に対処するためにマザーボードの交換が必要な場合、この機能を使用して iLO 設定を元のマザーボードから新しいマザーボードに転送できます。

ライセンスキーの喪失

ライセンスキーが誤って置き換えられた、または iLO を工場出荷時のデフォルトの設定にリセットした場合に、インストールするキーがわからないときは、ライセンスキーと他の構成設定をバックアップファイルからリストアできます。

注記: ファームウェアバージョンをまたいだバックアップやリストア操作の可能条件は以下の通りです。×の組み合わせでは、ファームウェアバージョンをまたいだバックアップやリストア操作は行わないでください。

バックアップ	リストア	可否
iLO5 1.20	iLO5 1.20 以降	○
iLO5 1.30 以降	iLO5 1.30 以降	○
iLO5 1.30 以降	iLO5 1.20 以前	×
iLO5 1.20 未満	iLO5 1.20 以降	×

注記: iLO 5 Firmware Version 1.20 Feb 02 2018 でバックアップしたデータを iLO Firmware Version 1.30 May 31 2018 以降でリストアした場合、デフォルト設定では**[Manageement]**-**[AlertMail]**ページにおいて**[Enable SMTP Secure Connection (SSL/TLS)]**が有効になっているため**[Enable SMTP Authentication]**を有効にして SMTP 認証を行うか、**[Enable SMTP Secure Connection (SSL/TLS)]**を無効にしてください。設定が旧バージョンのままの場合、アラートメールが送信されなくなります。

リストアされる情報

iLO 設定には、電源、ネットワーク、セキュリティ、ユーザーデータベース、ライセンスキーなど、多くのカテゴリーが含まれます。ほとんどの構成情報は、バッテリー駆動の SRAM メモリデバイスに保存されており、バックアップとリストアが可能です。

リストアされない情報

情報によってはリストアの対象として適していないものがあります。リストアできない情報は iLO 設定には含まれません。その情報は iLO またはサーバーのシステム状態に関連します。
以下の情報は、バックアップまたはリストアされません。

セキュリティ状態

リストア操作によって iLO のセキュリティ状態を変更することを許可すると、セキュリティの原則が破られ、セキュリティの適用が無効になります。

インテグレーテッドマネージメントログ

バックアップから、リストアが必要になった時間またはイベントまでに発生したイベントの情報を保持するため、この情報はリストアされません。

iLO イベントログ

バックアップから、リストアが必要になった時間またはイベントまでに発生したイベントの情報を保持するため、この情報はリストアされません。

Active Health System データ

バックアップおよびリストアプロセス中に記録された情報を保持するため、この情報はリストアされません。

サーバーの状態情報

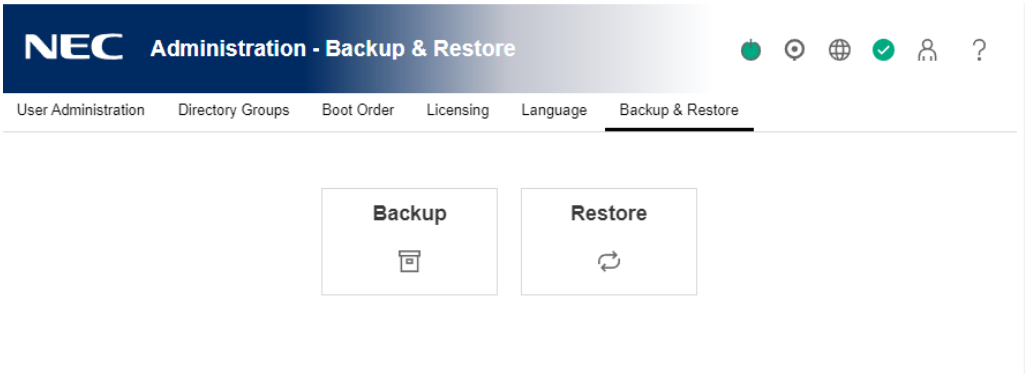
- サーバーの電源状態（オン/オフ）
- サーバーの UID LED の状態
- iLO およびサーバーのクロック設定

iLO 構成のバックアップ

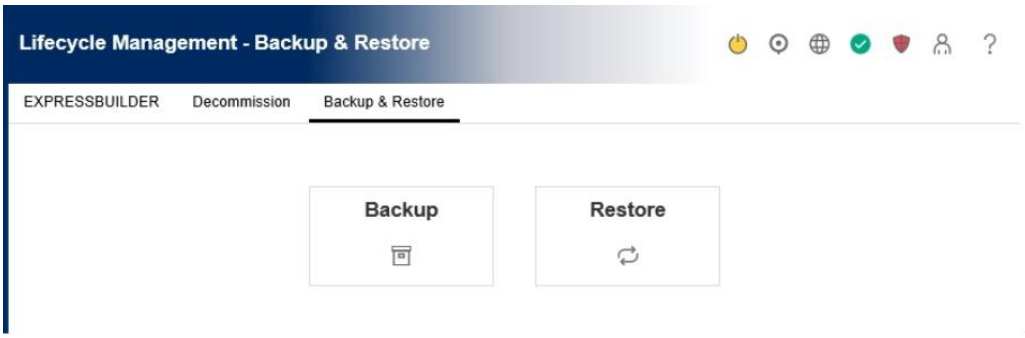
前提条件
iLO の設定を構成権限

手順
1. iLO 5 Firmware Version 2.18 以前の場合、
   ナビゲーションツリーで[**Administration**]をクリックし、[**Backup & Restore**]をクリックします。
   iLO 5 Firmware Version 2.31 以降の場合、
   ナビゲーションツリーで[Lifecycle Management]をクリックし、[**Backup & Restore**]をクリックします。

［iLO 5 Firmware Version 2.18 以前の場合］

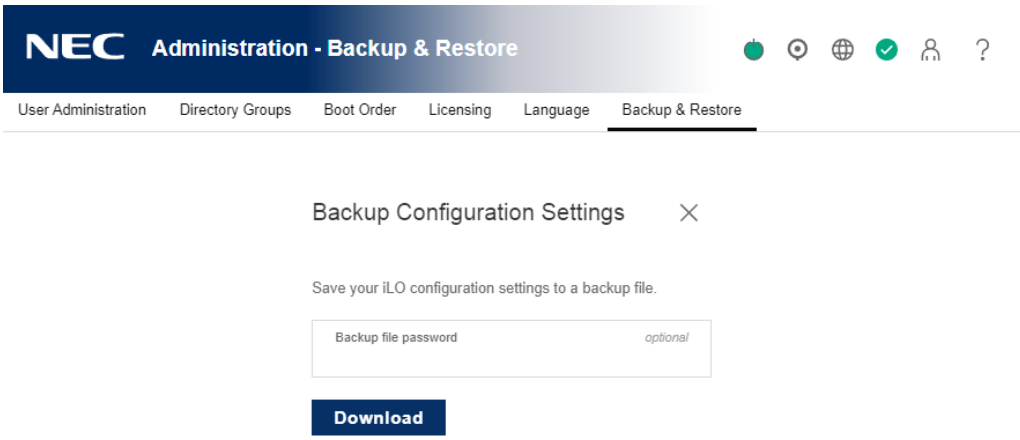


［iLO 5 Firmware Version 2.31 以降の場合］

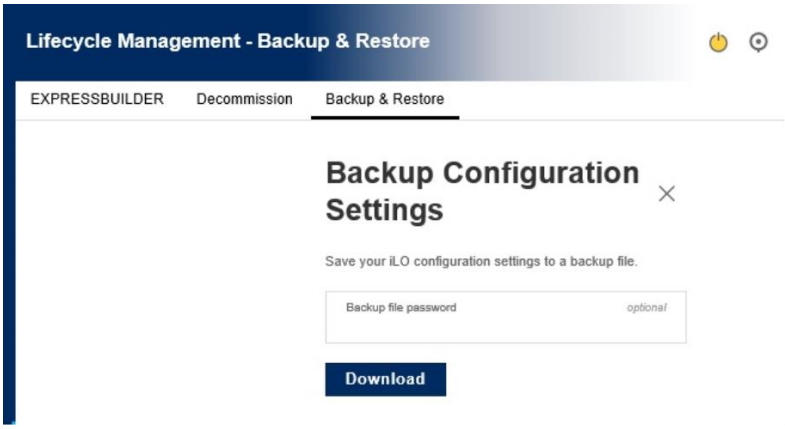


2. [**Backup**]をクリックします。

［iLO 5 Firmware Version 2.18 以前の場合］



［iLO 5 Firmware Version 2.31 以降の場合］



3. オプション：バックアップファイルをパスワード保護するには、[**Backup file password**]ボックスにパスワードを入力します。
4. [Download]をクリックします。
   ファイルがダウンロードされ、この動作がイベントログに記録されます。
   ファイル名は、次の形式を使用します。
   <**サーバーシリアル番号**>_<YYYYMMDD>_<HHMM>.bak.

iLO 構成のリストア

前提条件

- iLO の設定を構成権限
- ユーザーアカウント管理権限
- iLO バックアップファイルが存在する。
- 以前に iLO を工場出荷時のデフォルト設定にリセットした場合は、デフォルトの iLO アカウント認証情報を使用できる。
- 使用する iLO セキュリティ状態が構成されている。

> △**注意:**
> FIPS および CNSA のセキュリティ状態を構成すると、iLO は工場出荷時のデフォルト設定にリセットされます。リストア実行前にこれらのセキュリティ状態を再

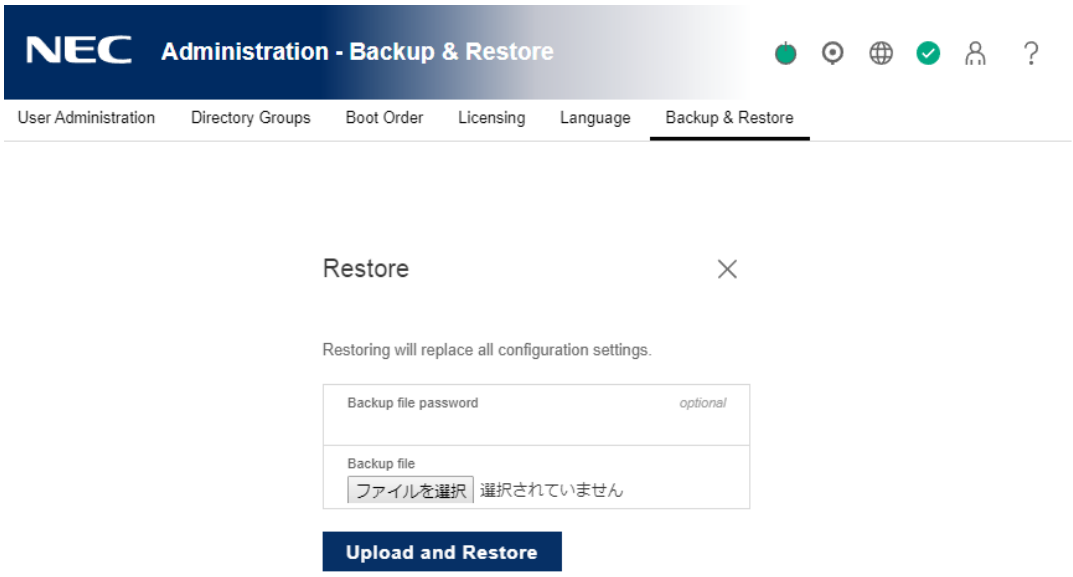
構成せずにリストアを実行した場合、復元された情報は削除されます。リストア実施前に、バックアップ時のセキュリティ状態に予め設定する必要があります。

- iLO ファームウェアのバージョンがバックアップ時から変更されていない。

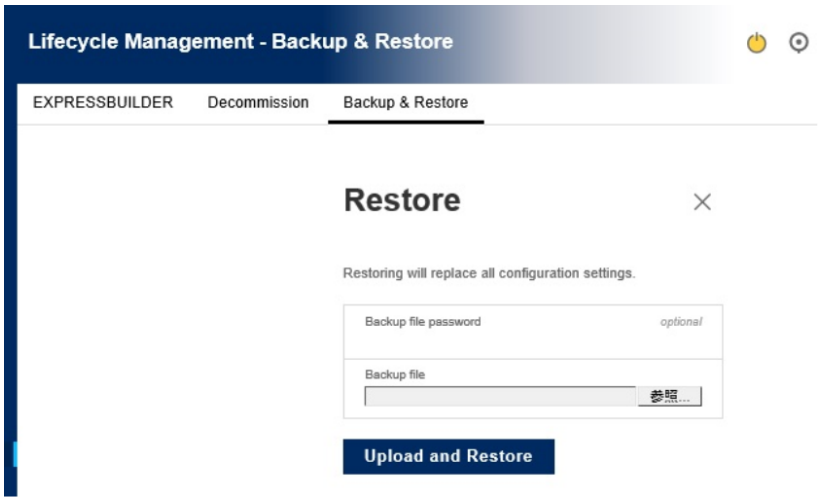
手順

1. iLO 5 Firmware Version 2.18 以前の場合、
   ナビゲーションツリーで[**Administration**]をクリックし、[**Backup file password**]をクリックします。
   iLO 5 Firmware Version 2.31 以降の場合、
   ナビゲーションツリーで[Lifecycle Management]をクリックし、[**Backup & Restore**]をクリックします。
2. [Restore]をクリックします。

［iLO 5 Firmware Version 2.18 以前の場合］



［iLO 5 Firmware Version 2.31 以降の場合］



3. 使用しているブラウザーに応じて[参照]または[ファイルを選択]をクリックし、バックアップファイルに移動します。

4. バックアップファイルがパスワードで保護されている場合、パスワードを入力します。
5. **[Upload and Restore]**をクリックします。

   iLO が要求を確認するように求めます。
6. **[Restore]**をクリックします。

   iLO が再起動され、ブラウザー接続が閉じます。接続が再確立されるまでに、数分かかることがあります。

マザーボード交換後の iLO 構成のリストア

マザーボードを交換する場合、交換前のマザーボードから構成をリストアできます。

前提条件

- iLO の設定を構成権限
- ユーザーアカウント管理権限
- iLO バックアップファイルが存在する。
- 以前に iLO を工場出荷時のデフォルト設定にリセットした場合は、デフォルトの iLO アカウント認証情報を使用できる。
- 使用する iLO セキュリティ状態が構成されている。

  △**注意:**
  FIPS および CNSA のセキュリティ状態を構成すると、iLO は工場出荷時のデフォルト設定にリセットされます。リストア実行前にこれらのセキュリティ状態を再構成せずにリストアを実行した場合、復元された情報は削除されます。リストア実施前に、バックアップ時のセキュリティ状態に予め設定する必要があります。
- 交換するマザーボードの iLO ファームウェアが、交換前のマザーボードの iLO ファームウェアと同一のバージョンである。

手順

1. マザーボードを交換し、ハードウェアコンポーネントを古いマザーボードから新しいマザーボードに移します。
2. システムの電源を入れ、すべてのコンポーネントが正常に動作していることを確認します。
3. 新しいマザーボードのデフォルトのユーザー認証情報を使用して iLO にログインします。
4. バックアップファイルから構成をリストアします。

ファームウェア検証[37]

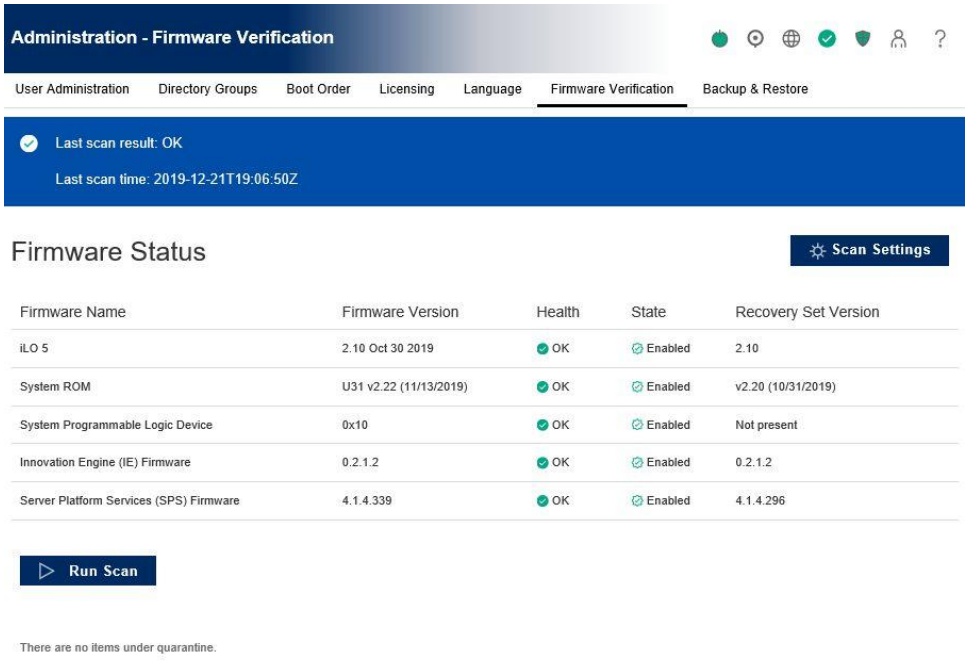
ファームウェア検証ページでは、オンデマンドスキャンを実行したり、スケジュールされたスキャンを実施できます。検出された問題に対処するために、iLO を次のように構成できます。

- 結果を記録する。
- 結果を記録し、リカバリインストールセットを使用する修復処置を開始する。

スキャン結果に応じて、情報は Active Health System ログとインテグレーテッドマネジメントログに記録されます。
次のファームウェアタイプがサポートされています。

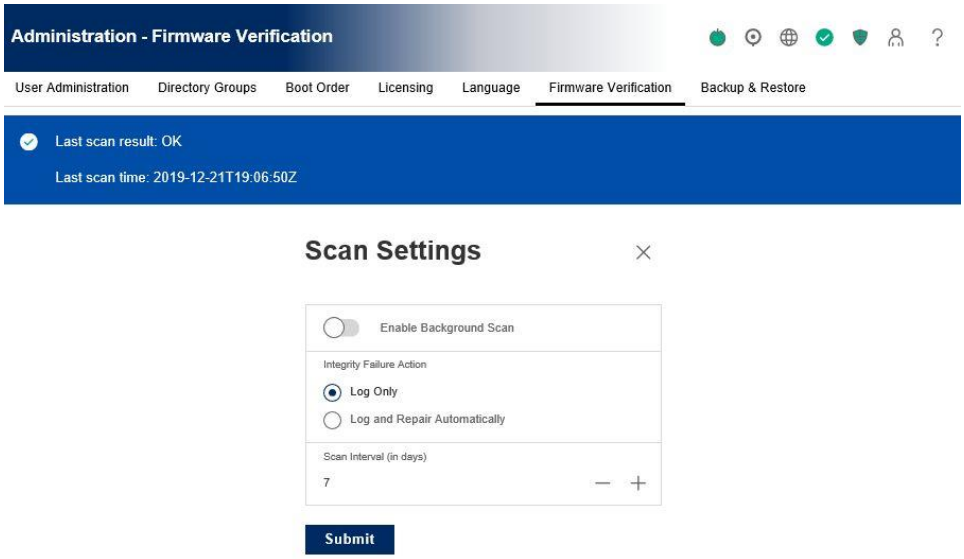
- iLO ファームウェア
- システム ROM（BIOS）
- システムプログラマブルロジックデバイス（CPLD）
- サーバープラットフォームサービス（SPS）ファームウェア（サポート対象のサーバーのみ）
- イノベーションエンジン（IE）ファームウェア

ファームウェア検証スキャンの実行中は、ファームウェアアップデートを実施したり、iLO レポジトリにファームウェアをアップロードしたりすることはできません。
無効な iLO またはシステム ROM（BIOS）のファームウェアが検出された場合は、無効なファイルが iLO レポジトリの隔離領域に保存されます。**[Quarantine]** セクションから無効なファイルをダウンロードし、バイナリファイルを分析することでその種類と発行元を調べることができます。隔離されたイメージは iLO レポジトリページに表示されず、ファームウェアアップデートで選択できません。



37 iLO 5 Firmware Version 2.10 Oct 30 2019 以降

ファームウェア検証設定の構成



前提条件

- iLO の設定を構成権限
- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. **[Administration]**ページに移動し、**[Firmware Verification]**タブをクリックします。
2. **[Scan Settings]**アイコン ⚙をクリックします。
3. **[Enable Background Scan]**を有効または無効の状態に設定します。
4. **[Integrity Failure Action]**を選択します。
5. **[Scan Interval (in days)]**(スキャン間隔)を日数で設定します。
   有効な値は 1～365 日です。
6. **[Submit]**をクリックします。

ファームウェア検証スキャンオプション

- **[Enable Background Scan]** - ファームウェア検証スキャンを有効または無効にします。有効なとき、iLO がサポート対象のインストールファームウェアでファイル破損をスキャンします。
- **[Integrity Failure Action]** - ファームウェア検証スキャン中に問題が見つかったとき iLO が実行するアクションを決定します。
  - 結果を記録するには、**[Log Only]**を選択します。
  - 結果を記録して修復アクションを開始するには、**[Log and Repair Automatically]**を選択します。

  サポート対象のファームウェアタイプについて問題が検出された場合、iLO が保護されたインストールセットで影響を受けるファームウェアタイプがあるかを調べます。デフォルトでは、このセットはリカバリセットです。ファームウェアイメージを使用可能な場合、iLO がそのファームウェアイメージをフラッシュして修復を完了します。
- **[Scan Interval (in days)]** - バックグラウンドスキャン頻度（日数）を設定します。有効な値は 1〜365 です。

詳しくはシステムリカバリセットを参照してください。

ファームウェア検証スキャンの実行

前提条件

- iLO の設定を構成権限
- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. **[Administration]** ページに移動し、**[Firmware Verification]**タブをクリックします。
2. **[Run Scan]**をクリックします。

ファームウェア検証スキャンの実行中は、ファームウェアアップデートを実施したり、iLO レポジトリにファームウェアをアップロードしたりすることはできません。
スキャン結果がページの上部に表示されます。
障害が発生した場合、ファームウェア検証ページのファームウェアの状態が障害/オフラインに変わり、システムヘルスのステータスがクリティカルに変わり、イベントが IML に記録されます。
ファームウェア検証スキャン機能がログおよび自動的に修復に構成されている場合は、障害が発生したファームウェアはフラッシュされます。成功すると、ファームウェアの状態とシステムヘルスのステータスが更新され、IML イベントは修正済みステータスに変わります。
自動修復が構成されていない場合は、手動で修復を実行する必要があります。

ファームウェアヘルスステータスの表示

前提条件

この機能をサポートするライセンスがインストールされている。
NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. **[Administration]** ページに移動し、**[Firmware Verification]**タブをクリックします。

ファームウェアヘルスステータスの詳細

サポートされる各ファームウェアタイプについて、次の情報が表示されます。

- **[Firmware Name]** - インストールされているファームウェアの名前。
- **[Firmware Version]** - ファームウェアバージョン。
- **[Health] -** ファームウェアのヘルスステータス。
- **[State] -**ファームウェアのステータス。値には、以下のものがあります。
  - **[Enabled]** - ファームウェアは検証されており、有効です。
  - **[Scanning]** - ファームウェア検証スキャンが進行中か、起動しようとします。
  - **[Flashing]** -ファームウェアアップデートが進行中です。
  - **[Failed/Offline]** - ファームウェアは検証できず、修復されませんでした。
- **[Recovery Set Version]** - システムリカバリセットのファームウェアのバージョン。

このファームウェアタイプがシステムリカバリセットにない場合や、システムリカバリセットがない場合は、**[Not present]**が表示されます。

隔離されたファームウェアの表示

前提条件

この機能をサポートするライセンスがインストールされている。
NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. **[Administration]** ページに移動し、**[Firmware Verification]**タブをクリックします。

隔離されたファームウェアファイルは、**[Quarantine]**セクションに表示されます。

隔離されたファイルがない場合は、「There are no items under quarantine（隔離中のアイテムはありません）」というメッセージが表示されます。

隔離されたファームウェアの詳細

[Quarantine]セクションには、無効なファームウェアファイルに関する以下の情報が表示されます。

- **[Name]** - 無効なファームウェアファイルの名前。
- **[Created]** - 無効なファイルの作成日。
- **[Size]** - 無効なファイルサイズ。

個々の隔離されたファイルの詳細

リストのファイルをクリックすると、以下の詳細が表示されます。

- **[Name]** - 隔離されたファイルの名前。
- **[Created]** - 無効なファイルの作成日。
- **[File Name]** - iLO レポジトリによって使用される名前。
- **[Image URI]** - 隔離されたファイルの場所。
- **[Size]** - 隔離されたファイルの作成日。
- **[Device Class]** - iLO リポジトリのリソースとファームウェアのインベントリデータの間で関係付ける際に使用可能な ID。

隔離されたファームウェアのダウンロード

iLO レポジトリの**[Quarantine]** セクションにファイルを保存するかどうか、オフライン分析のためにファイルをダウンロードすることができます。

前提条件

この機能をサポートするライセンスがインストールされている。
NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. **[Administration]** ページに移動し、**[Firmware Verification]**タブをクリックします。
2. **[Quarantine]** セクションで、ダウンロードするファイルの横にある⬇をクリックします。ステータスメッセージには、ダウンロードの進捗状況が表示されます。
3. ファイルを保存または開くには、ブラウザーの指示に従います。

隔離されたファームウェアの削除

前提条件

- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
- リカバリセット権限

手順

1. **[Administration]** ページに移動し、**[Firmware Verification]**タブをクリックします。
2. **[Quarantine]** セクションで、ダウンロードするファイルの横にある🗑をクリックします。
   iLO が要求を確認するように求めます。
3. **[Yes, remove]**をクリックします。

16. iLO のセキュリティ機能の使用

iLO セキュリティの設定

iLO には、以下のセキュリティ機能があります。

- ユーザー定義の TCP/IP ポート。
- ユーザー操作を iLO イベントログに記録。
- ログイン失敗時の遅延。
- CA が署名した X.509 証明書のサポート。
- BMC 構成ユーティリティのセキュリティ保護のサポート。
- SSL 証明書の管理を使用する暗号化通信。
- オプションの LDAP ベースディレクトリサービスのサポート。

これらのオプションの一部は、ライセンスが必要な機能です。詳しくは、「iLO ライセンス」を参照してください。

セキュリティに関する一般的なガイドライン

iLO のセキュリティに関する一般的なガイドラインは、次のとおりです。

- セキュリティを最大限に高めるには、iLO を、独立した管理ネットワーク上で設定します。詳しくは、「iLO をネットワークへ接続」を参照してください。
- iLO は、インターネットに直接接続しないでください。
- ユーザーアカウントやパスワードはデフォルト設定から変更してご使用ください。
- SSL 証明書をインストールしてご使用ください。
- 2 ファクタ認証のような認証サービスをご使用ください。
- ご使用にならない機能やプロトコルは無効にしてご使用ください。
- リモートコンソールは HTTPS で接続してご使用ください。

BMC 構成ユーティリティのセキュリティ

システムユーティリティ内の BMC 構成ユーティリティを使用すると、iLO 設定を表示したり変更したりすることができます。BMC 構成ユーティリティ、または iLO Web インターフェースを使用して BMC 構成ユーティリティのアクセス設定を構成できます。システムメンテナンススイッチで iLO セキュリティが無効に設定されている場合、構成されているアクセス設定に関係なく、すべてのユーザーが BMC 構成ユーティリティにアクセスできます。BMC 構成ユーティリティには、次のセキュリティレベルがあります。

- **[ログイン要求なし]**（デフォルト）

  POST 実行中にホストにアクセスできるユーザーであれば誰でも、BMC 構成ユーティリティを起動して、コンフィギュレーション設定の表示や変更を行えます。ホストアクセスが制限されている場合は、この設定でもかまいません。ホストアクセスが制御されない場合は、任意のユーザーが使用可能な設定メニューを使用して変更を行うことができます。

- **[ログイン要求]**（より安全）

  BMC構成ユーティリティのログインが必要な場合は、認証されたユーザーアクセス権によって使用可能な設定メニューが制御されます。

- **[無効]**（最も安全）

  BMC 構成ユーティリティが無効の場合、ユーザーアクセスは禁止されています。これにより、BMC 構成ユーティリティを使用した変更を防止します。

ログイン要求を変更するには、以下の手順に従ってください。

- iLO Web インターフェースを使用して、**[Require Login for iLO RBSU]**設定を編集します。
- BMC 構成ユーティリティを使用して、**[Require user login and configuration privilege for BMC Configuration]**設定を編集します。

BMC 構成ユーティリティを有効または無効にするには、以下の手順を使用します。

- iLO Web インターフェースを使用して、**[iLO ROM-Based Setup Utility]**設定を編集します。
- BMC 構成ユーティリティを使用して、**[BMC 構成ユーティリティ]**設定を編集します。

詳細情報

iLO アクセスの設定

システムメンテナンススイッチを使用した iLO セキュリティ

システムメンテナンススイッチの iLO セキュリティ設定により、管理者はサーバーのマザーボードを物理的に制御して緊急時にアクセスすることができます。iLO セキュリティを無効にすることにより、ユーザー ID やパスワードを使わないですべての権限を使用してログインアクセスできます。

システムメンテナンススイッチはサーバー内部にあるため、サーバーエンクロージャーを開かないとアクセスできません。システムメンテナンススイッチを操作するときは、サーバーの電源がオフであり、電源から切り離されていることを確認します。iLO セキュリティを有効または無効に設定し、サーバーの電源を投入します。

iLO セキュリティを制御するシステムメンテナンススイッチ位置は、**iLO セキュリティオーバーライドスイッチ**と呼ばれることがあります。

次の理由により iLO セキュリティを無効にしなければならないことがあります。

- ユーザーアカウント管理権限を持つすべてのユーザーアカウントがロックアウトされてしまった。
- 不適切な設定により、ネットワーク上に iLO が表示されず、BMC 構成ユーティリティが無効になっている。
- iLO NIC がオフになっていて、BMC 構成ユーティリティを実行してオンにし直すことが不可能かまたは難しい。
- ユーザー名が 1 つだけ設定され、パスワードを忘れてしまった。

システムメンテナンススイッチを使用して iLO セキュリティを無効にした場合は、以下のようになります。

- すべてのセキュリティ認証確認が無効になる。

- ホストサーバーがリセットされると、BMC 構成ユーティリティが実行される。
- iLO が無効化されず、設定に従って、ネットワーク上で表示できる。
- iLO 機能が無効にされても、サーバーの電源を切って再度投入するまで、iLO は、ユーザーをログアウトしたり無効化プロセスを実行したりしない。
- iLO Web インターフェースページに、iLO セキュリティが無効であることを示す警告メッセージが表示される。
- iLO のログに、iLO セキュリティの変更を記録するエントリーが追加される。
- システムメンテナンススイッチを使用して iLO セキュリティを有効または無効にしてから iLO を開始すると、SNMP アラート送信先が設定されている場合、SNMP アラートが送信される。

システムメンテナンススイッチを使用して iLO セキュリティを有効および無効にする方法については、ご使用のサーバーのユーザーズガイドおよびメンテナンスガイドを参照してください。

TPM と TM

Trusted Platform Module(TPM)および Trusted Module(TM)は、プラットフォームの認証に使用される仕掛けを安全に格納するコンピューターチップです。これらの仕掛けには、パスワード、証明書、暗号鍵などが含まれます。また、TPM または TM を使用すると、プラットフォームの測定値を格納してプラットフォームの信頼性を保証することができます。

サポートされているシステムでは、ROM は、TPM または TM レコードを復号化し、設定ステータスを iLO、iLO RESTful API、CLP インターフェースに渡します。

TPM または TM のステータスの表示

TPM または TM のステータスを表示するには、**[Information]→[Overview]**ページに移動します。

以下のステータス値が表示されます。

- **[Not Supported]** - TPM または TM はサポートされていません。
- **[Not Present]** - TPM または TM は取り付けられていません。
- **[Present]** - 次のいずれかのステータスを示します。
  - TPM または TM は取り付けられているが無効になっている。
  - TPM または TM が取り付けられていて、有効になっている。
  - TPM または TM が取り付けられ、有効であり、オプション ROM 計測が有効になっている。
- **[Present-Enabled]** - TPM または TM が取り付けられ、有効になっている。

ユーザーアカウントおよびアクセス

iLO は、最大 12 のローカルユーザーアカウントの設定をサポートします。以下の機能を使用して、各アカウントを管理できます。

- 権限
- ログインセキュリティ

iLO は、ディレクトリサービスを使用してユーザーの認証や権限付与を行えるように設定することができます。この構成により、iLO を使用できるユーザーの数の制限がなくなります。また、この構成は、エンタープライズ内の iLO デバイスの数に合わせて、簡単に拡張できます。ディレクトリサービスにより iLO デバイスとユーザーを集中的に管理することができ、より強力なパスワードポリシーを実施できます。iLO では、ローカルユーザー、ディレクトリユーザー、またはその両方を使用できます。

ディレクトリ認証の使用について詳しくは、「Kerberos 認証とディレクトリサービス」を参照してください。

ユーザー権限

iLO では、権限を使用して、ユーザーアカウントによる iLO 機能へのアクセスを制御することができます。ユーザーが機能を使用しようとすると、iLO は、ユーザーがその機能を使用するために適切な権限を持っていることを確認します。

ユーザーアカウントとディレクトリグループの利用可能な権限については、「iLO のユーザーアカウント」を参照してください。

ログインセキュリティ

iLO には、以下のログインセキュリティ機能があります。

- 設定したログイン失敗回数を超えると遅延時間が課せられるよう iLO を設定できます。以後、ログインに失敗するたびに、設定した秒数の遅延時間が加算されます。遅延のたびにメッセージが表示されます。これは、有効なログインが実行されるまで続きます。この機能により、ブラウザーのログインポートに対するディクショナリ攻撃が防止されます。ログイン遅延の設定は**[Security]**→**[Access Settings]**ページでできます。
- iLO では、失敗したすべてのログイン試行の詳細なログエントリーが保存されます。認証失敗ログの頻度は、**[Security]**→**[Access Settings]**ページで設定できます。

  詳しくは、「iLO アクセスの設定」を参照してください。

iLO アクセスの設定(iLO 5 Firmware Version 1.40 Feb 05 2018 以降)

アクセス設定のデフォルト値は、ほとんどの環境に適しています。アクセス設定ページで変更できる値を使用すると、特殊環境向けの iLO 外部アクセス方法をカスタマイズできます。
アクセス設定ページに入力された値は、すべての iLO ユーザーに適用されます。

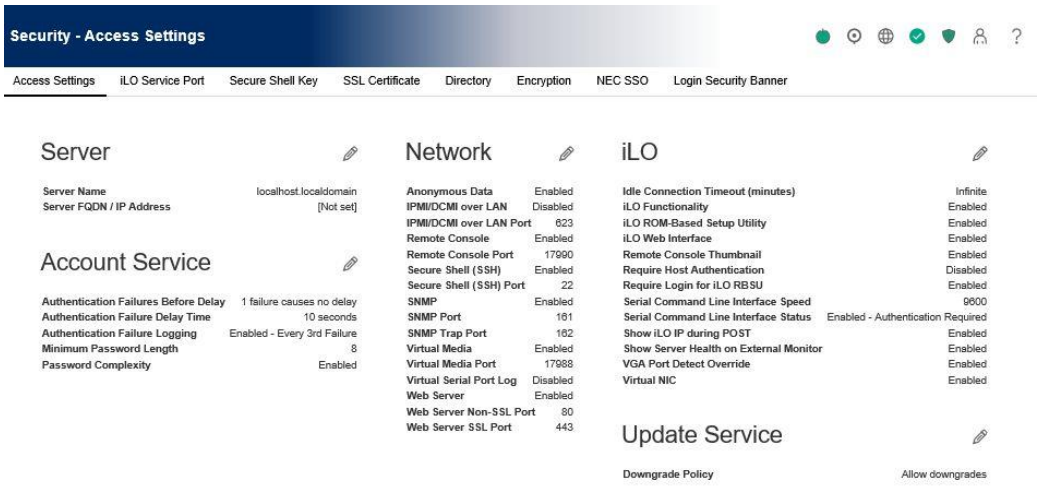
iLO アクセス設定の構成

この手順は、iLO 機能を除くすべてのアクセス設定を対象とします。iLO 機能を[Disabled]にするには、「iLO 機能の無効化」を参照してください。

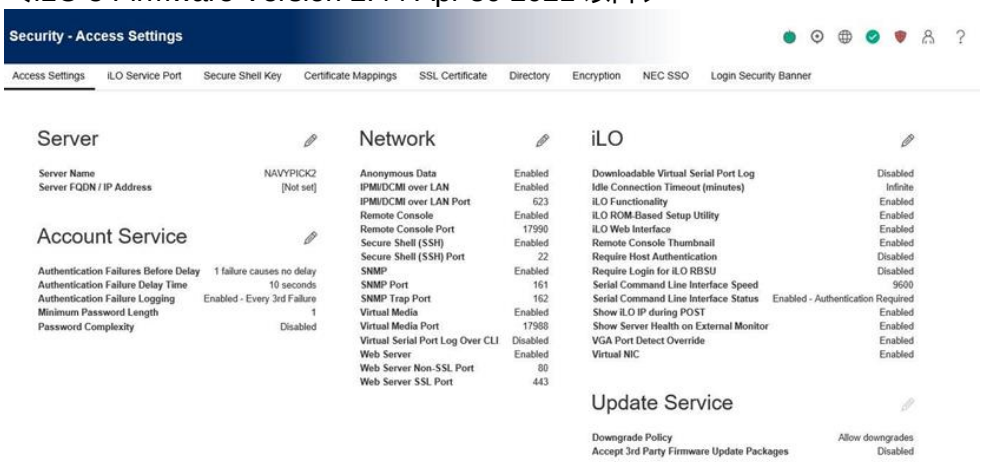
前提条件

- すべてのアクセス設定の変更に関する前提条件：
  - iLO の設定を構成権限。
- アップデートサービス設定の変更に関する前提条件：
  - iLO の設定を構成権限。
  - リカバリセット権限
  - この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、「
  - iLO ライセンスオプシ」を参照してください。

<iLO 5 Firmware Version 2.31 Oct 13 2020 以前>



＜iLO 5 Firmware Version 2.44 Apr 30 2021 以降＞



手順

1. ナビゲーションツリーでセキュリティをクリックします。
   アクセス設定ページが表示されます。
2. をクリックします。
   以下から選択します。
   - サーバー
   - アカウントサービス
   - iLO
   - アップデートサービス
   - ネットワーク

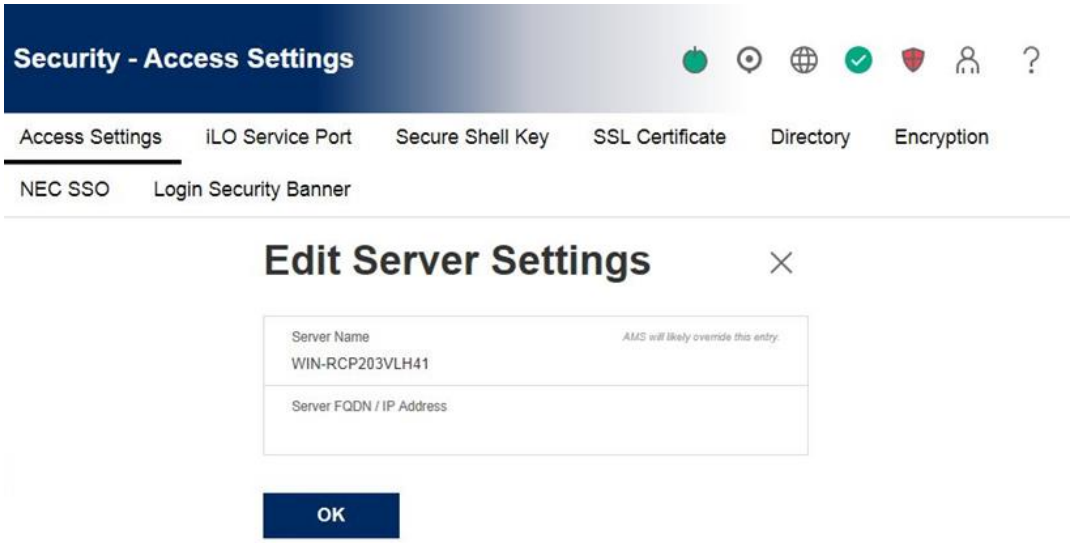
   設定タイプページが開きます。
3. 必要に応じて、設定を更新し、OK をクリックします。
   変更した設定のタイプに応じて、以下が実行される場合があります。
   - iLO が、アップデートが完了したことを通知します。
   - iLO が、保留中の変更を有効にするにはリセットが必要であることを通知します。

   ヒント:

   リセットを必要とする変更を加え、そのリセットの前に変更を元に戻した場合は、✕ をクリックして、リセットメッセージを無視します。

   場合によって、リセットが完了する前に即座に影響することがあります。たとえば、リモートコンソールを介したアクセスを**[Disabled]**にした場合、 OK をクリックするとリモートコンソールセッションを開始できません。構成の変更を完了するには、リセットが必要です。
4. オプション：2～3 の手順を繰り返して、追加のアクセス設定を更新します。
5. リセットが必要な場合、アクセス設定の更新が完了したら、**[Reset iLO]**をクリックします。
   iLO が要求を確認するように求めます。
6. **[Yes, Reset iLO]**をクリックします。
   接続が再確立されるまでに、数分かかることがあります。

サーバーアクセスの設定

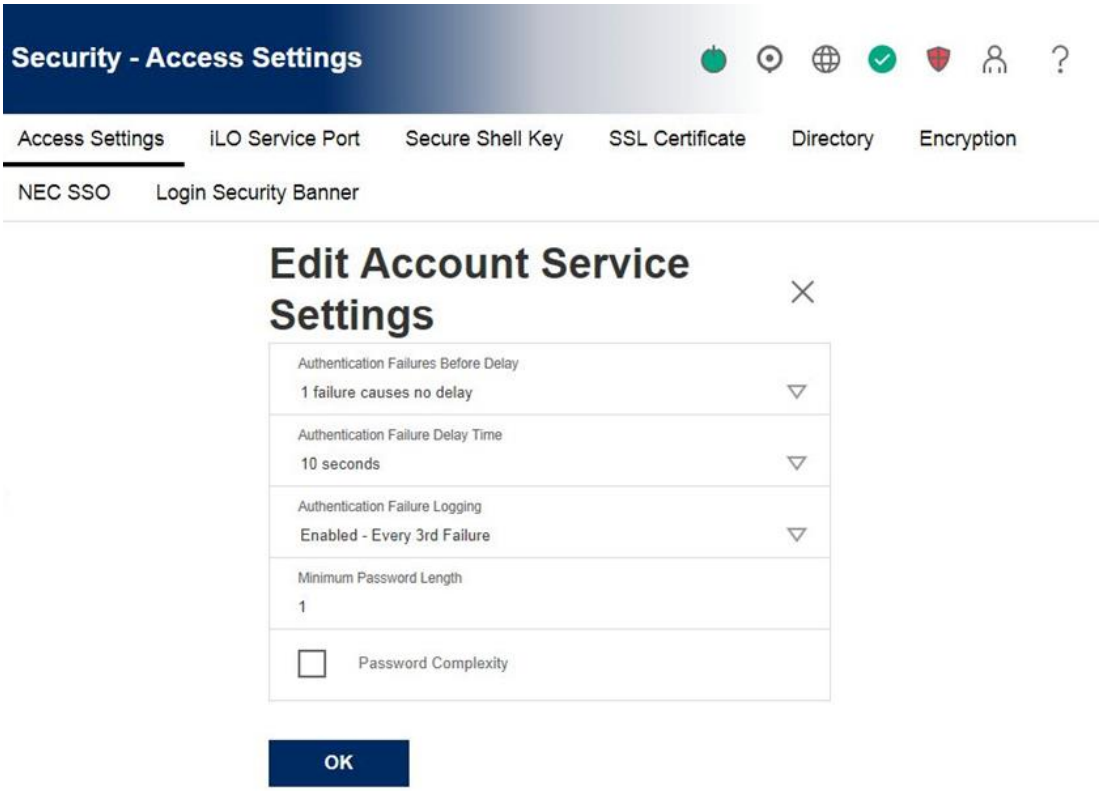


アクセス設定ページのサーバーセクションでは、以下の設定を構成できます。

- **[Server Name]** - ホストサーバー名を指定することができます。この値を手動で割り当てることができますが、オペレーティングシステムをロードするとホストソフトウェアによって上書きされることがあります。サーバー名は最大 49 バイトまで入力できます。
- **[Server FQDN / IP Address]** -サーバーの FQDN または IP アドレスを指定できます。この値を手動で割り当てることができますが、オペレーティングシステムをロードするとホストソフトウェアによって上書きされることがあります。FQDN または IP アドレスは最大 255 バイトまで入力できます。

アカウントサービスのアクセス設定オプション

アクセス設定ページのアカウントサービスセクションでは、以下の設定を構成できます。



- **[Authentication Failures Before Delay]** - iLO がログイン遅延を課すまでに許容されるログインの失敗数を設定できます。有効な値は 1、3、5 回、または各ログイン試行の失敗時です。デフォルト設定は 1 です。これは、2 度目に試したログインが失敗するまでログイン遅延は課せられないことを意味します。
- **[Authentication Failure Delay Time]** - ログインに失敗した後の iLO ログイン遅延の継続期間を構成できます。有効な値は 2、5、10、および 30 秒です。デフォルト値は 10 秒です。
- **[Authentication Failure Logging]** -認証失敗のログ記録条件を構成できます。以下の設定が有効です。
  - **[Enabled-Every Failure]** - ログインに失敗するたびに、失敗したログインログエントリーが記録されます。
  - **[Enabled-Every 2nd Failure]** - ログイン試行に 2 回失敗するごとに、ログインの失敗のログエントリーが記録されます。
  - **[Enabled-Every 3rd Failure (default)]** - ログイン試行に 3 回失敗するごとに、ログインの失敗のログエントリーが記録されます。
  - **[Enabled-Every 5th Failure]** - ログイン試行に 5 回失敗するごとに、ログインの失敗のログエントリーが記録されます。
  - **[Disabled]** - ログインの失敗のログエントリーは記録されません。

SSH クライアントでこの設定を使用する方法について詳しくは、iLO ユーザーガイドを参照ください。

最小パスワード長

ユーザーパスワードの設定または変更の際に許可される文字の最小数を指定します。指定する文字数は、0～39 文字の値でなければなりません。デフォルト値は 8 です。

パスワードの複雑さ設定を有効にした場合、iLO は、最小パスワード長を満たすパスワードを許可しないことがあります。たとえば、最小パスワード長を 1 に設定した場合、1 文字のパスワードはパスワードの複雑さ要件を満たさないため**[Disabled]**になります。

パスワードの複雑さ

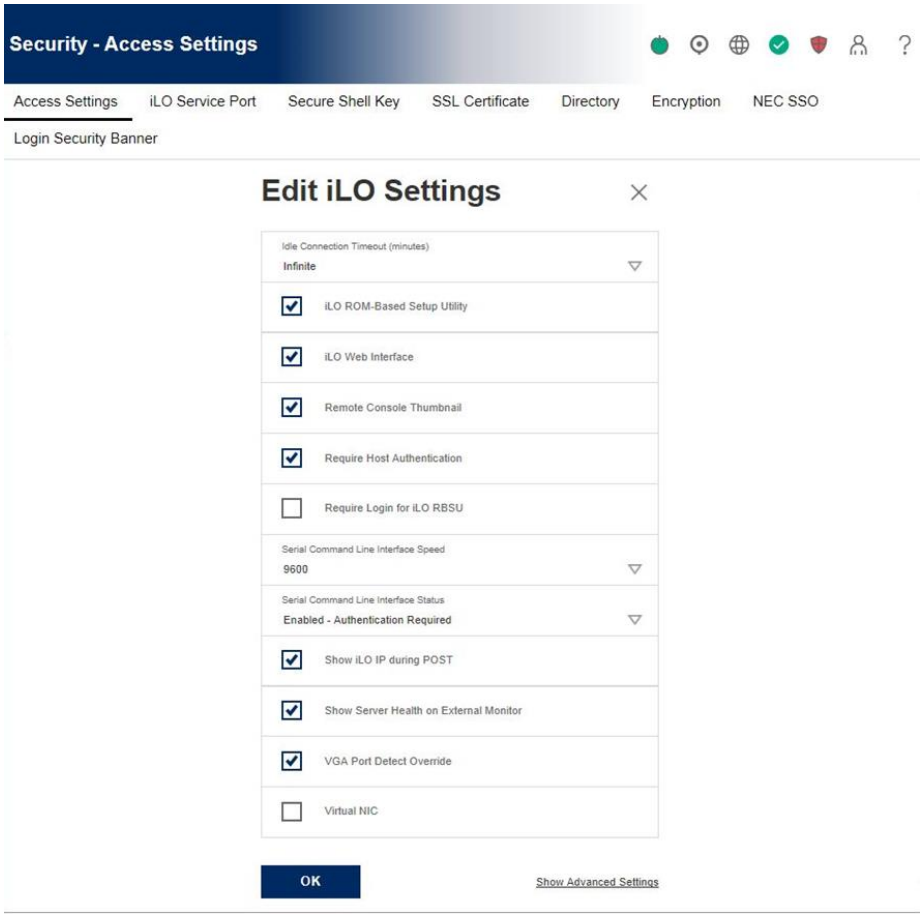
ユーザーアカウントを作成するときのパスワードの複雑さチェックの動作を制御します。
この設定を有効にすると、新しいまたは更新したユーザーアカウントパスワードには、次の特性のうちの 3 つが含まれる必要があります。

- 少なくとも 1 つの大文字 ASCII 文字
- 少なくとも 1 つの小文字 ASCII 文字
- 少なくとも 1 つの ASCII 数字
- 少なくとも 1 つの他の文字タイプ（記号、特殊文字、句読点など）。

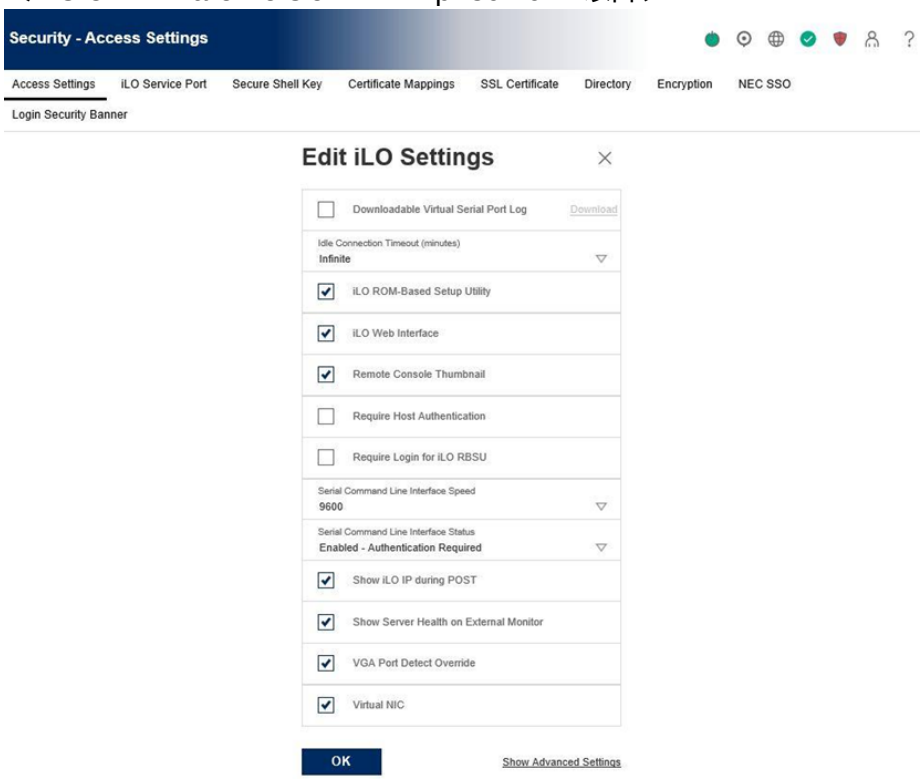
この設定を**[Disabled(デフォルト)]**にした場合、これらのパスワード特性は適用されません。

iLO アクセス設定

＜iLO 5 Firmware Version 2.31 Oct 13 2020 以前＞



＜iLO 5 Firmware Version 2.44 Apr 30 2021 以降＞



[Access Setting]ページの**[iLO]**セクションでは、以下の設定を構成できます。
[**Idle Connection Timeout (minutes)**] - iLO セッションで、ユーザーの操作がないまま経過し、自動的に終了するまでの時間を指定します。各接続は別個のセッションであるため、iLO Web インターフェースまたはリモートコンソールは、アイドル時間を別々に追跡します。仮想メディアデバイスが接続されている場合、この設定はリモートコンソールセッションに影響を与えません。
有効な値は次のとおりです。

- **[15/30/60/120]** - デフォルト値は 30 分です。
- **[Infinite]** - 非アクティブなユーザーはログアウトされません。

異なるサイトにアクセスしたりブラウザーウィンドウを閉じたりすることによって iLO からログアウトしなかった場合も、アイドル接続になります。iLO ファームウェアがサポートする接続数には制限があります。無限タイムアウトオプションを乱用すると、他のユーザーが iLO にアクセスできなくなる場合があります。アイドル接続は、期限が切れると再利用されます。
この設定は、ローカル/ディレクトリのユーザーに適用されます。ディレクトリサーバータイムアウト設定は、iLO 設定を優先的に使用する場合があります。
設定を変更しても、現在のユーザーセッションでただちに有効にならない場合がありますが、すべての新しいセッションでただちに強制設定されます。

ダウンロード可能な仮想シリアルポートログ

前提条件

- この機能をサポートするライセンスがインストールされている。
  NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。

手順

1. ナビゲーションツリーでセキュリティをクリックします。
2. アクセス設定ページが表示されます。
3. （**[iLO]** アクセス設定セクションの横にある）をクリックします。
4. **[iLO]**の編集ページが開きます。
5. [Downloadable Virtual Serial Port Log] のチェックボックスをチェックします。
6. [OK] をクリックします。

iLO 機能の無効化

iLO 機能設定は、iLO 機能が使用可能かどうかを制御します。

- **[Enabled]**(デフォルト) - iLO ネットワークを使用でき、OS 上のドライバとの通信がアクティブです。
- **[Disabled] -** iLO ネットワークと、OS 上のドライバとの通信が切断されます。

iLO 機能を再度有効にするには、UEFI システムユーティリティを使用します。詳しくは、UEFI システムユーティリティユーザーガイドを参照してください。
この手順の目的は、iLO 機能設定を変更することです。他の iLO アクセス設定を更新するには、「iLO アクセス設定の構成」を参照してください。

前提条件
iLO の設定を構成権限。

手順

1. ナビゲーションツリーでセキュリティをクリックします。
2. アクセス設定ページが表示されます。
3. （**[iLO]** アクセス設定セクションの横にある）をクリックします。
4. **[iLO]**の編集ページが開きます。
5. **[Show Advanced Settings]**を表示をクリックします。
6. **[iLO Functionality]**セクションで**[Disable]**をクリックします。
7. iLO が要求を確認するように求めます。
8. **[Confirm disabling of iLO functionality]**の確認チェックボックスを選択します。
9. **[Yes, disable iLO functionality]**をクリックします。

> △**注意:**
> **[Yes, disable iLO functionality]**をクリックした後、iLO にアクセスできなくなります。**[iLO Functionality]**を再度有効にするには、BMC 構成ユーティリティ（システムユーティリティ内）を使用して**[iLO Functionality]**を **[有効]**に設定します。詳しくは、本体装置のメンテナンスガイドを参照してください。

iLO はセッションを終了します。iLO 機能設定を再度有効にするまで、どの iLO インターフェースからも接続できません。

iLO ROM ベースセットアップユーティリティ

UEFI システムユーティリティの iLO 構成オプションを**[Enabled]**または**[Disabled]**にします。

- **[Enabled(デフォルト)]** - UEFI システムユーティリティへのアクセス時に iLO 構成オプションを使用できます。
- **[Disabled]** - UEFI システムユーティリティへのアクセス時に iLO 構成オプションを使用できません。

システム BIOS でオプション ROM のプロンプトが**[Disabled]**になっている場合、この設定を有効にできません。
このオプションは、UEFI システムユーティリティでは BMC 構成ユーティリティと呼ばれています。
この値を変更すると、iLO リセットが必要です。

iLO Web インターフェース

iLO と通信するために iLO Web インターフェースを使用できるかどうかを指定します。この設定はデフォルトで有効になっています。
この値を変更すると、iLO リセットが必要です。リセットの完了後は、UEFI システムユーティリティまたは iLO RESTful API を使用してこの設定を再度有効にするまで、Web ブラウザー経由で iLO インターフェースにアクセスすることはできません。

リモートコンソールサムネイル

iLO でリモートコンソールのサムネイルイメージのアクセシビリティを**[Enabled]**または**[Disabled]**にします。 サムネイルを**[Disabled]**にしても、リモートコンソール機能は**[Disabled]**になりません。
この設定を**[Disabled]**にすると、Web インターフェースがサムネイルの表示を中止するのに約 30 秒かかります。
この設定を有効にする場合は、ブラウザーウィンドウを更新してサムネイルを表示します。iLO からログアウトしてからログインし直して、サムネイルを表示することもできます。

ホスト認証が必要

iLOREST などのホストベースのユーティリティで iLO ユーザー認証情報が必要かどうかを決定します。これらのユーティリティは、オペレーティングシステムのコマンドラインから実行され、管理者アクセスまたはルートアクセスが可能なシステムアカウントが必要です。

- **[Enabled]** - iLO ユーザー認証情報が必要で、すべてのコマンドに権限チェックが適用されます。
- **[Disabled]** - iLO 認証情報は必要ありません。この構成では、iLOREST は iLO 管理者権限で動作します。

この設定が**[Disabled]**になっている場合、iLO 認証情報は必要ありません。この構成では、iLOREST は iLO 管理者権限で動作します。
iLO が FIPS セキュリティ状態を使用するように構成されている場合、この設定は**[Disabled]**にできません。
この設定を使用できるのは、iLO が高度なセキュリティのセキュリティ状態を使用するよう構成されている場合だけです。

iLO RBSU へのログイン要求

UEFI システムユーティリティの iLO 構成オプションにユーザーがアクセスしたときに、ユーザー認証情報プロンプトを表示するかどうかを決定します。

- **[Disabled(デフォルト)]** - EFI システムユーティリティの iLO 構成オプションにユーザーがアクセスするときに、ログインは不要です。
- **[Enabled]** - UEFI システムユーティリティの iLO 構成オプションにユーザーがアクセスするときに、ログインダイアログボックスが開きます。

FIPS セキュリティ状態が有効になっている場合、iLO は、このオプションが**[Disabled]**な場合でもユーザー認証情報プロンプトを表示します。
このオプションは、UEFI システムユーティリティでは Require user login and configuration privilege for iLO 5 Configuration と呼ばれます。

シリアルコマンドラインインターフェース速度

CLI 機能のシリアルポートの速度を変更できます。
以下の速度（ビット/秒）が有効です。

- **[9600(デフォルト)]**
- **[19200]**
- **[38400]** - UEFI システムユーティリティの iLO 構成オプションではこの値はサポートされていません。
- **[57600]**
- **[115200]**

正常に動作させるには、シリアルポート構成をパリティなし、データビット 8、ストップビット 1（N/8/1）に設定する必要があります。
この値は、UEFI システムユーティリティで構成されたシリアルポート速度と一致するように設定します。

シリアルコマンドラインインターフェースステータス

シリアルポート経由での CLI 機能のログインモデルを変更できます。以下の設定が有効です。

- **[Enabled-Authentication Required(デフォルト)]** - ホストシリアルポートに接続された端末から SMASH CLP コマンドラインにアクセスできます。有効な iLO ユーザー証明書が必要です。
- **[Enabled-No Authentication]** - ホストシリアルポートに接続された端末から SMASH CLP にアクセスできます。iLO ユーザー証明書は不要です。

- **[Disabled]** - ホストシリアルポートから SMASH CLP へのアクセスを**[Disabled]**にします。物理シリアルデバイスを使用する予定の場合は、このオプションを使用してください。

POST 中に iLO IP を表示

ホストサーバーの POST 中に iLO のネットワーク IP アドレスを表示できます。

- **[Enabled(デフォルト)]** - POST 実行中に iLO の IP アドレスが表示されます。
- **[Disabled]** - POST 実行中に iLO の IP アドレスが表示されません。

外部モニターにサーバーヘルスを表示

外部モニターでサーバーヘルスサマリー画面の表示を有効にします。

- **[Enabled(デフォルト)]** - サーバーの UID ボタンを押して放して、外部モニターにサーバーヘルスサマリー画面を表示できます。
- **[Disabled]** - サーバーの UID ボタンを押して放しても、サーバーヘルスサマリー画面は開きません。

> △**注意:**
>
> この機能を使用するには、UID ボタンを押して放します。5 秒間から 9 秒間押し続けると安全な iLO 再起動、10 秒間以上押し続けるとハードウェア iLO 再起動を行います。ハードウェア iLO 再起動によりデータの損失や NVRAM の破損が発生する可能性があります。

VGA ポート検出オーバーライド

システムのビデオポートに接続されているデバイスの検出方法を制御します。動的検出によってシステムが異常なポート電圧から保護されます。

- **[Enabled(デフォルト)]** - iLO ファームウェアは、ビデオ出力の使用を開始する前に、接続されているデバイスを検出します。
- **[Disabled]** - iLO ハードウェアは、ビデオ出力の使用を開始する前に、接続されているデバイスを検出します。

この設定は、ディスプレイ、KVM コンセントレーター、またはアクティブなドングルへのビデオ出力がない場合のトラブルシューティングで使用できます。

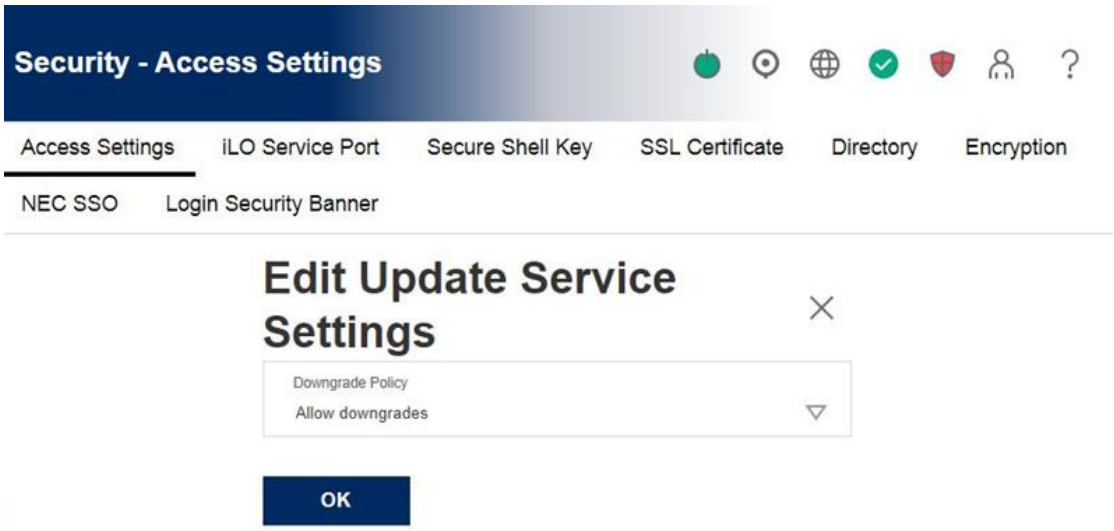
仮想 NIC

USB サブシステム経由で仮想 NIC を使用して、ホストオペレーティングシステムから iLO にアクセスできるかどうかを決定します。

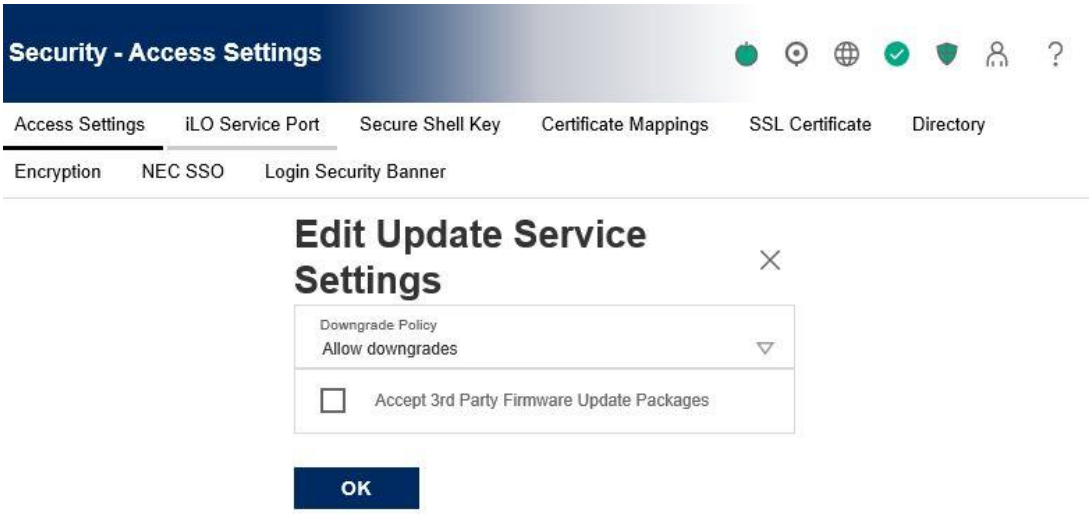
- **[Enabled]** -以下のことができます。
  - ホスト OS で動作している RESTful Interface Tool または別のクライアントから iLORESTful API コマンドを開始する。
  - ホスト OS で動作している SSH クライアントで iLO に接続する。
  - ホスト OS で動作しているサポート対象のブラウザーを使用して iLO Web インターフェースにアクセスする。
  - 概要ページに仮想 NIC のステータス情報を表示する。
- **[Disabled(デフォルト)]** -仮想 NIC を使用して iLO にアクセスすることはできません。

アップデートサービス設定

- iLO 5 Firmware Version 2.18 Jun 22 2020 以前



- iLO 5 Firmware Version 2.31 Oct 13 2020 以降



ダウングレードポリシー

iLO から更新できるファームウェアタイプをダウングレードする要求を iLO がどのようにして処理するかを指定します。
この機能には iLO Advanced ライセンスが必要です。
NX7700x シリーズサーバには、iLO Advanced ライセンスが標準でインストールされています。

以下の値から選択します。

- **[Allow downgrades (デフォルト)]** - iLO の設定を構成権限。を持つすべてのユーザーがファームウェアをダウングレードできます。
- **[Downgrade requires Recovery Set privilege]** - iLO の設定を構成権限。とリカバリセット権限を持つユーザーのみがファームウェアをダウングレードできます。
- **[Permanently disallow downgrades]** - ダウングレードを永遠に不許可-ユーザーはファームウェアをダウングレードできません。

> △**注意:**
> 本設定には変更しないでください。この設定値への変更後は、iLO のどのインターフェースやユーティリティからもこの設定の構成を変更することができな

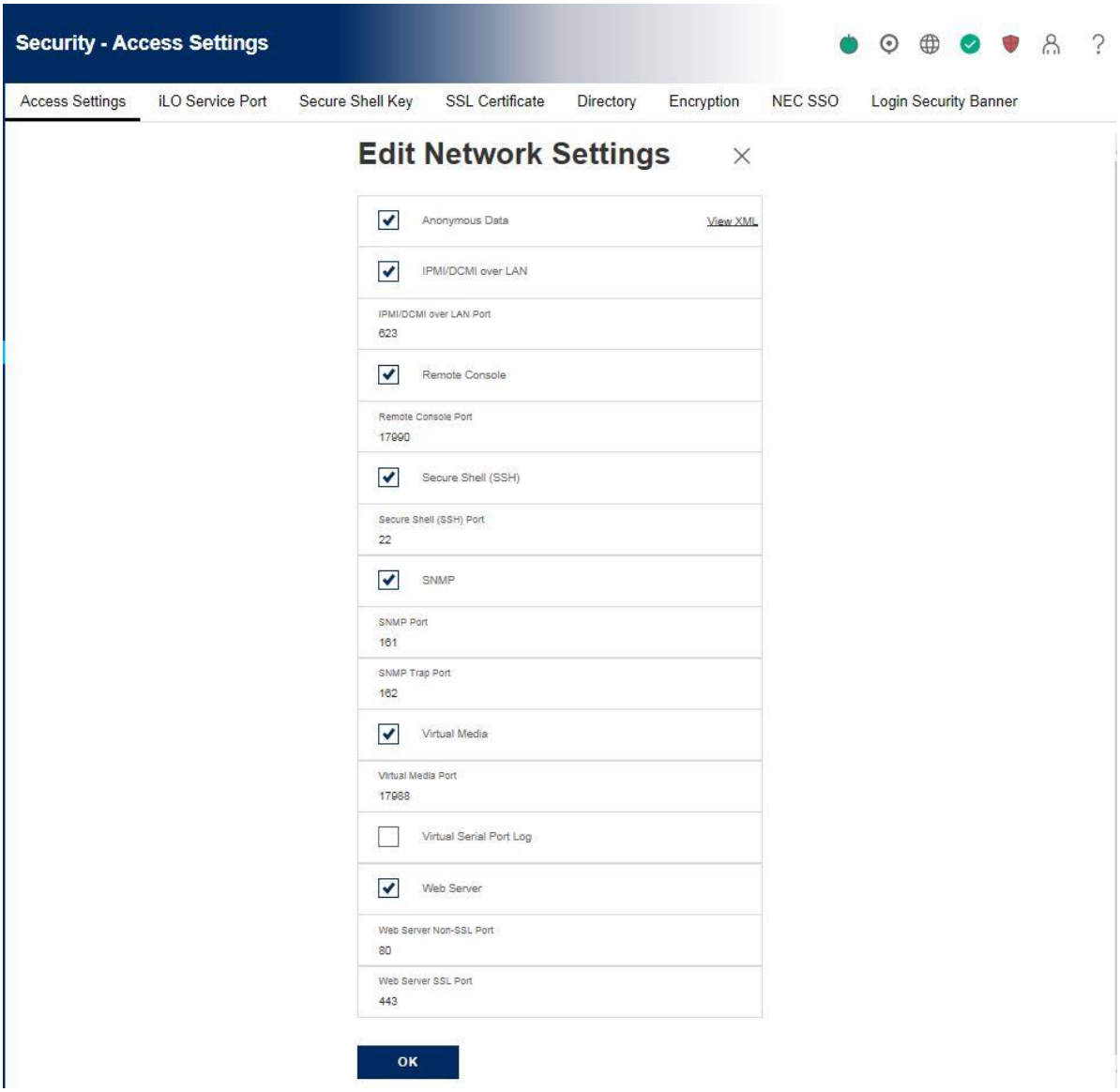
くなります。iLO を出荷時のデフォルト設定に設定しても、この値はリセットされません。

3rd パーティー ファームウェア アップデート パッケージの受け入れ

iLO が、デジタル署名されていない 3rd パーティー ファームウェアアップデートパッケージの受け入れを許可するか否かを指定します。Platform Level Data Model [38](PLDM) パッケージもサポートされます。この設定のデフォルトは”Disabled”です。

△注意:
iLO 5 Firmware Version 2.31 Oct 13 2020 以降でサポートされている機能です。

ネットワークアクセス設定



アクセス設定ページのネットワークセクションでは、iLO の機能を有効および[Disabled]にしたり、それらの機能で使用するポートを構成したりできます。

[38] OS やプラットフォーム管理サブシステムに依存することなく、デバイスアクセスを容易とすることを目的とする DMTF で標準仕様化されたプラットのデータ・モデル共通仕様。

iLO が使用する TCP/IP ポートは構成可能であり、ポート設定に関する任意のサイト要件およびセキュリティのイニシアチブに適合できます。これらの設定は、ホストシステムには影響しません。
iLO で有効なポートの値の範囲は 1〜65535 です。使用されているポートの番号を入力すると、iLO により別の値を入力するよう求められます。
通常、これらの設定を変更するには、標準の通信と SSL 通信に使用される Web ブラウザーの設定を変更する必要があります。

匿名データ

この設定は、以下を制御します。

- 基本システム情報の匿名要求への応答で iLO が提供する XML オブジェクト。
- /redfish/v1 に対する Redfish の匿名呼び出しへの応答で提供される情報。

この設定が有効になっている(デフォルト)場合は、次のようになります。

- 他のソフトウェアは、ネットワーク上の iLO システムを検出および特定できます。iLO が提供する XML 応答を表示するには、**[View XML]**をクリックします。
- /redfish/v1 に対する Redfish の匿名呼び出しには、次のような情報が含まれます。

  ```
  "ManagerFirmwareVersion": "1.40",
  "ManagerType": "iLO 5",
  "Status": {"Health": "OK"}
  ```

- iLO のヘルスステータスが**[Degraded]**の場合は、iLO のヘルスステータスと問題の説明がログインページに表示されます。iLO ヘルスステータスは、iLO 診断セルフテストを組み合わせた結果に基づいています。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

このオプションが**[Disabled]**になっている場合は、次のようになります。

- iLO は空の XML オブジェクトを使用して要求に応答します。
- iLO のバージョン情報はログインページに表示されません。
- /redfish/v1 に対する Redfish の匿名呼び出しに次の情報は含まれません。
  ManagerFirmwareVersion、ManagerType、および Status。

高セキュリティまたは FIPS のセキュリティ状態を有効にすると、この設定は自動的に**[Disabled]**になります。

IPMI/DCMI over LAN

業界標準の IPMI および DCMI コマンドを LAN 経由で送信できます。
この設定は、デフォルトでは[Disabled]になっています。

- **[Disabled]** - iLO は LAN 経由で IPMI/DCMI を**[Disabled]**にします。この機能が**[Disabled]**にされても、サーバー側の IPMI/DCMI アプリケーションは依然として機能します。
- **[Enabled]** - iLO では、クライアント側のアプリケーションを使用して LAN 経由で IPMI/DCMI コマンドを送信できます。

IPMI/DCMI over LAN が**[Disabled]**にされている場合、ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、設定されている IPMI/DCMI over LAN ポートが検出されません。
FIPS のセキュリティ状態を有効にすると、この設定は自動的に**[Disabled]**になります。

IPMI/DCMI over LAN ポート

IPMI/DCMI ポート番号を設定します。デフォルト値は 623 です。

リモートコンソール

iLO リモートコンソール経由のアクセスを**[Enabled]**または**[Disabled]**にすることができます。

- **[Disabled]** - HTML5 IRC、.NET IRC、Java IRC、スタンドアロンリモートコンソール、テキストベースのリモートコンソールが無効になります。ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、設定されているリモートコンソールポートが検出されません。
- **[Enabled]** - HTML5 IRC、.NET IRC、Java IRC、スタンドアロンリモートコンソール、テキストベースのリモートコンソールが有効になります。ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、設定されているリモートコンソールポートが検出されません。

リモートコンソールを**[Disabled]**にしても、リモートコンソールサムネイルは**[Disabled]**になりません。リモートコンソールサムネイルを**[Disabled]**にするには、iLO のアクセス設定セクションでリモートコンソールサムネイルオプションを編集します。

リモートコンソールポート

リモートコンソールポートを設定します。デフォルト値は 17990 です。

セキュアシェル（SSH）

SSH 機能を**[Enabled]**または**[Disabled]**にすることができます。
SSH は、iLO コマンドラインプロトコル（CLP）に暗号化されたアクセスを提供します。

セキュアシェル（SSH）ポート

SSH ポートを設定します。デフォルト値は 22 です。

SNMP

iLO が外部の SNMP 要求に応答するかどうかを指定します。

- **[Disabled]** - iLO はそのまま動作を続行し、iLO Web インターフェースに表示される情報は更新されます。この状態では、警告は生成されず、SNMP アクセスは許可されません。 SNMP アクセスが**[Disabled]**になっている場合、SNMP 設定ページのほとんどのボックスは使用できません。
- **[Enabled]** - SNMP アクセスは許可されます。

FIPS のセキュリティ状態を有効にすると、この設定は自動的に**[Disabled]**になります。

SNMP ポート

SNMP ポートを設定します。SNMP アクセス用の業界標準(デフォルト)の SNMP ポートは、161 です。
SNMP ポートの値をカスタマイズすると、標準以外の SNMP ポートの使用をサポートしない一部の SNMP クライアントが、iLO で正しく動作しない場合があります。
SNMP オプションが**[Disabled]**になっている場合、この値を更新することはできません。

SNMP トラップポート

SNMP トラップポートを設定します。SNMP アラート（またはトラップ）用の業界標準(デフォルト)の SNMP ポートは、162 です。
SNMP トラップポートをカスタマイズすると、標準以外の SNMP トラップポートの使用をサポートしない一部の SNMP 監視アプリケーションが、iLO で正しく動作しない場合があります。
SNMP オプションが**[Disabled]**になっている場合、この値を更新することはできません。

仮想メディア

iLO 仮想メディア機能を**[Enabled]**または**[Disabled]**にすることができます。

- **[Disabled]** - ローカルおよび URL ベースの仮想メディア機能が無効になります。ポートスキャナーを使用してセキュリティ脆弱性をスキャンするセキュリティ監査で、構成されている仮想メディアポートが検出されません。
- **[Enabled]** - ローカルおよび URL ベースの仮想メディア機能が有効になります。

仮想メディアポート

iLO が仮想メディア接続のためにリッスンするポート。デフォルト値は 17988 です。

仮想シリアルポートログ/仮想シリアルポートログ over CLI

仮想シリアルポートの記録を**[Enabled]**または**[Disabled]**にします。

- **[Disabled]** (デフォルト) -仮想シリアルポートの動作は記録されません。
- **[Enabled]** -仮想シリアルポートの動作が iLO メモリ内の 150 ページの循環バッファーに記録されます。CLI コマンド vsp log を使用して、記録された情報を表示できます。仮想シリアルポートのバッファーサイズは 128 KB です。

Web サーバー

iLO Web サーバー経由のアクセスを**[Enabled]**または**[Disabled]**にすることができます。

> △**注意:**
> この値を**[Disabled]**に設定した場合、iLO は、Web サーバー非 SSL ポートまたは Web サーバーSSL ポートでの通信をリッスンしません。Web サーバーが**[Disabled]**になっている場合、次の機能は正常に動作しません。iLO RESTful API、リモートコンソール、iLO 連携、および iLO Web インターフェース。

[Disabled] - iLO は、Web サーバー非 SSL ポートまたは Web サーバーSSL ポートでの通信をリッスンしません。Web サーバーが**[Disabled]**になっている場合、次の機能は正常に動作しません。iLORESTful API、リモートコンソール、iLO 連携、および iLO Web インターフェース。
このオプションを**[Disabled]**にすると、ポートスキャナーを使用してセキュリティ脆弱性をスキャンするセキュリティ監査で、構成されている Web サーバー非 SSL ポート（HTTP）および Web サーバーSSL ポート（HTTPS）が検出されません。
[Enabled] - iLO は、Web サーバー非 SSL ポートまたは Web サーバーSSL ポートでの通信をリッスンします。

Web サーバー非 SSL ポート（HTTP）

HTTP ポートを設定します。デフォルト値は 80 です。

Web サーバーSSL ポート（HTTPS）

HTTPS ポートを設定します。デフォルト値は 443 です。

iLO アクセスの設定(iLO 5 Firmware Version 1.38 Sep 11 2018 以前)

サービス設定、IPMI/DCMI、およびアクセスオプションを含めて、iLO アクセス設定を変更することができます。

[Security]→[Access Settings]ページに入力された値は、すべての iLO ユーザーに適用されます。

アクセス設定のデフォルト値は、ほとんどの環境に適しています。**[Access Settings]**ページで変更できる値を使用すると、特殊環境向けの iLO 外部アクセス方法をカスタマイズできます。

前提条件

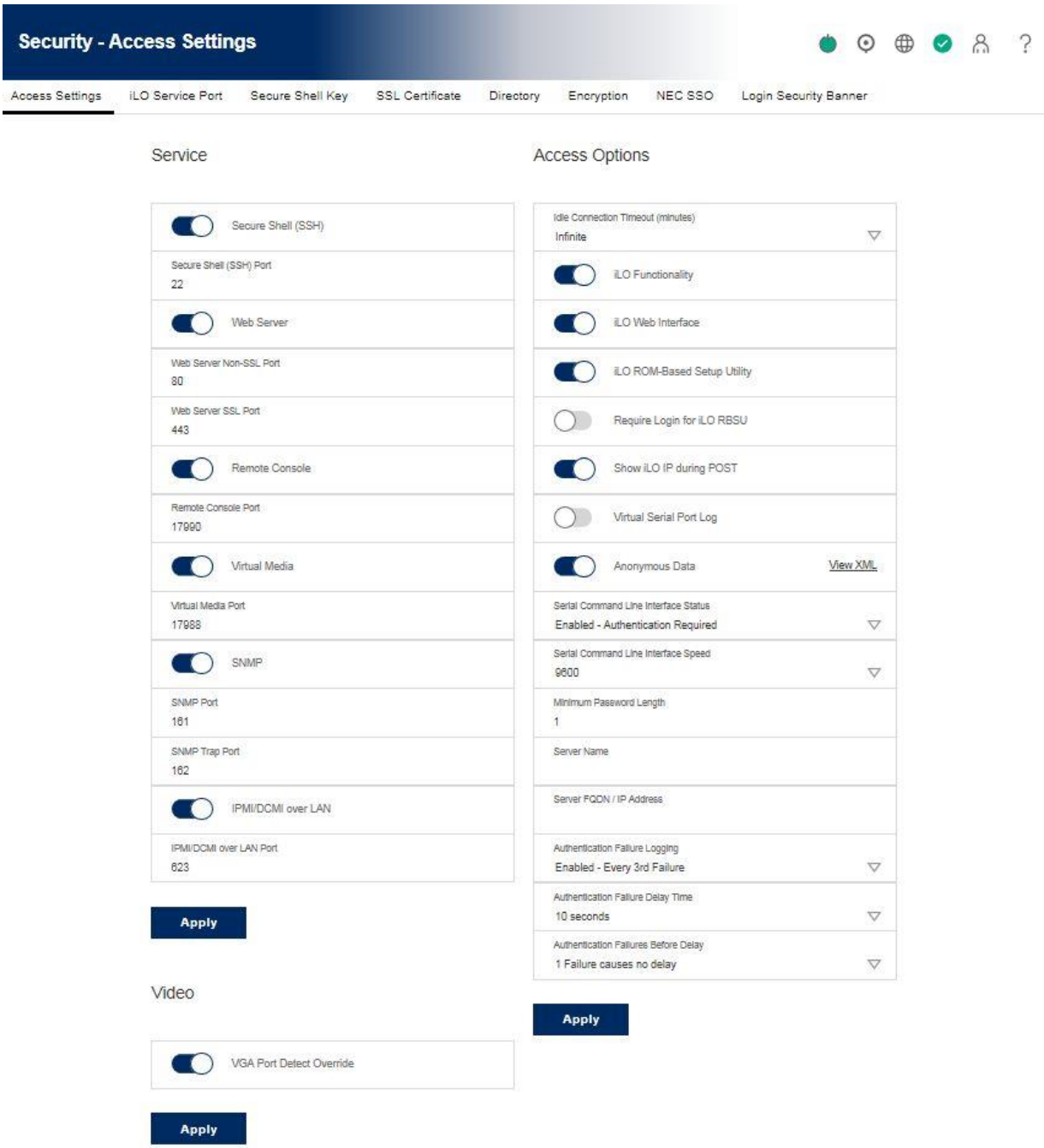
iLO の設定を構成権限

手順

iLO が使用する TCP/IP ポートは設定可能であり、ポート設定に関する任意のサイト要件およびセキュリティ構想に適合できます。これらの設定は、ホストシステムには影響しません。iLO で有効なポートの値の範囲は 1〜65535 です。

通常、これらの設定を変更するには、標準の通信と SSL 通信に使用される Web ブラウザーの設定を変更する必要があります。これらの設定を変更すると、iLO は変更を有効にするためにリセットを開始します。

1. **[Security]→[Access Settings]**ページに移動します。



必要に応じて、サービス設定を更新します。

2. **[Apply]**をクリックしてブラウザー接続を終了し、iLO を再起動します。

   接続を再確立できるまでに数分かかります。

詳細情報

サービス設定

アクセスオプションの設定

前提条件

iLO の設定を構成権限

手順

1. **[Security]→[Access Settings]**ページに移動します。
2. 必要に応じて、アクセスオプションを更新します。
3. **[Apply]**をクリックしてブラウザー接続を終了し、iLO を再起動します。

   接続を再確立できるまでに数分かかります。

   [iLO Functionality]設定を **[Disabled]**に設定した場合、**[Apply]**をクリックするとブラウザー接続が終了し、iLO ネットワークおよびオペレーティングシステムドライバーとの通信は切断されます。

詳細情報

アクセスオプション

IPMI/DCMI アクセスオプションの設定

iLO により、業界標準の IPMI および DCMI コマンドを LAN 経由で送信できるようになります。

前提条件

iLO の設定を構成権限

手順

1. **[Security]→[Access Settings]**ページに移動します。
2. **[IPMI/DCMI over LAN]** - [有効]または[無効]にします。デフォルト値は、[無効] です。
3. **[IPMI/DCMI over LAN Port]** - デフォルト値は 623 です。
4. **[Apply]**をクリックします。

サービス設定(iLO 5 Firmware Version 1.38 Sep 11 2018 以前)

[Access Settings]ページの **[Service]**セクションでは、以下の設定を構成できます。

- **[Secure Shell (SSH)]** - SSH 機能を有効または無効にすることができます。

  SSH は、暗号化された iLO CLP へのアクセスを提供します。デフォルト値は、[有効] です。
- **[Secure Shell (SSH) Port]** - デフォルト値は 22 です。
- **[Web Server]** - Web サーバー機能を有効または無効にすることができます。デフォルト値は、[有効] です。
- **[Web Server Non-SSL Port]** - デフォルト値は 80 です。iLO Firmware Version 1.20 Feb 02 2018 以前が動作中の環境で EXPRESSBUILDER をご利用される際には、この設定はデフォルト値のままお使いください。

  iLO Firmware Version 1.30 May 31 2018 以降のバージョンでは変更可能です。
- **[Web Server SSL Port]** - デフォルト値は 443 です。iLO Firmware Version 1.20 Feb 02 2018 以前が動作中の環境で Java IRC をご利用される際には、この設定はデフォルト値のままお使いください。

  iLO Firmware Version 1.30 May 31 2018 以降のバージョンでは変更可能です。
- **[Remote Console]** -リモートコンソール機能を有効または無効にすることができます。デフォルト値は、[有効] です。

- **[Remote Console Port]** - デフォルト値は 17990 です。
- **[Virtual Media]** - 仮想メディア機能を有効または無効にすることができます。デフォルト値は、[有効] です。
- **[Virtual Media Port]** - デフォルト値は 17988 です。
- **[SNMP]** - iLO が外部の SNMP 要求に応答する必要があるかどうかを指定します。デフォルト値は、[有効] です。
  [SNMP]を [無効] に設定すると、iLO の Web インターフェースに表示される情報は更新されますが、SNMP アラート（またはトラップ）は送信されず、SNMP アクセスは許可されません。また**[Management]→[SNMP Settings]**ページのほとんどのボックスが使用できなくなり、入力できなくなります。
- **[SNMP Port]** - SNMP アクセス用の業界標準（デフォルト）の SNMP ポートは、161 です。
  [SNMP Port]の値をカスタマイズすると、標準以外の SNMP ポートの使用をサポートしない一部の SNMP クライアントが、iLO で正しく動作しない場合があります。
- **[SNMP Trap Port]** - SNMP アラート（またはトラップ）用の業界標準（デフォルト）の SNMP トラップポートは、162 です。
  [SNMP Trap Port]の値をカスタマイズすると、標準以外の SNMP トラップポートの使用をサポートしないアプリケーションで、一部の SNMP 監視アプリケーションが、iLO で正しく動作しない場合があります。

Video(iLO 5 Firmware Version 1.35 Aug 14 2018 以降)

- **[**VGA Port Detect Override**]** - VGA ビデオポートの自動検出オーバライド機能を有効または無効にするかを指定します。デフォルト値は、有効(自動検出を行う)です。

アクセスオプション(iLO 5 Firmware Version 1.38 Sep 11 2018 以前)

[Access Settings]ページの **[Access Options]**セクションでは、以下の設定を構成できます。

[Idle Connection Timeout (minutes)]
この設定で指定した時間が経過してもユーザーの操作がない場合、iLO Web インターフェースセッションまたはリモートコンソールセッションは自動的に終了します。

iLO の Web インターフェースとリモートコンソールは、各接続が別のセッションであるため、アイドル時間を別々に追跡します。仮想メディアデバイスが接続されている場合、リモートコンソールセッションはこの値の影響を受けません。

以下の設定が有効です。

- **[15]**、**[30]**、**[60]**、または **[120]** 分 - デフォルト値は 30 分です。
- **[Infinite]** - ユーザーの操作がなくてもログアウトされません。

異なるサイトにアクセスしたりブラウザーを閉じたりすることによって iLO からログアウトしなかった場合も、アイドル接続になります。iLO ファームウェアがサポートする接続数には制限があります。**[Infinite]**タイムアウトオプションを乱用すると、他のユーザーが iLO にアクセスできなくなる場合があります。アイドル接続は、タイムアウトになると、再利用されます。この設定

は、ローカルユーザーとディレクトリユーザーに適用されます。ディレクトリサーバータイムアウトは、iLO 設定を優先的に使用する場合があります。

値を変更しても、現在のユーザーセッションではただちに有効にならない場合がありますが、すべての新しいセッションでただちに実施されます。

[iLO Functionality]
この設定は、iLO の機能が使用可能かどうかを指定します。

- **[有効]**（デフォルト）- iLO のネットワークが使用し、オペレーティングシステムドライバーとの通信がアクティブです。
- **[無効]** - **[iLO Functionality]** が無効になっている場合、iLO ネットワークおよびオペレーティングシステムドライバーとの通信は切断されます。

  [iLO Functionality]を再度有効にするには、BMC 構成ユーティリティ（システムユーティリティ内）を使用して**[iLO Functionality]**を **[有効]**に設定します。詳しくは、本体装置のメンテナンスガイドを参照してください。

注記:　このオプションは、システムユーティリティでは **[iLO Functionality]**または**[BMC 機能]**となっています。

[iLO Web Interface]

この設定は、iLO Web インターフェースを使用して iLO と通信できるかどうかを指定します。デフォルト値は、[有効]です。

注記:　このオプションは、システムユーティリティでは **[BMC Web Interface]** または**[BMC Web インターフェース]**となっています。

[iLO ROM-Based Setup Utility]

この設定は、BMC 構成ユーティリティを有効化または無効化します。

- **[有効]**（デフォルト）- POST 実行中に **[F9]** キーを押すとシステムユーティリティへのアクセス時に BMC 構成ユーティリティを使用できます。
- **[無効]** - POST 実行中に **[F9]** キーを押しても システムユーティリティへのアクセス時に BMC 構成ユーティリティを使用できません。

システム BIOS でオプション ROM のプロンプトが無効になっている場合、この設定を **[有効]** に設定できません。

注記:　このオプションは、システムユーティリティでは **[BMC Configuration Utility]** または［**BMC 構成ユーティリティ**］となっています。

[Require Login for iLO RBSU]

この設定は、ユーザーが BMC 構成ユーティリティにアクセスしたときにユーザー認証情報プロンプトを表示するかどうかを指定します。

- **[有効]** - BMC 構成ユーティリティにユーザーがアクセスするときにログインダイアログボックスが開きます。

- **[無効]**（デフォルト）- BMC 構成ユーティリティにユーザーがアクセスするときに、ログインは不要です。

注記:　このオプションは、システムユーティリティでは **[Require user login and configuration privilege for BMC Configuration]** または[BMC 設定のためのログインが必要]となっています。
[Require Login for iLO RBSU]を有効に設定した場合、パスワードなし（0 文字）のユーザーは BMC 構成ユーティリティに入ることはできません。

[Show iLO IP during POST]

この設定により、ホストサーバーの POST 中に iLO のネットワーク IP アドレスを表示できます。

- **[有効]**（デフォルト）- iLO の IP アドレスは、POST 実行中に表示されます。
- **[無効]** - iLO の IP アドレスは、POST 実行時に表示されません。

注記:　このオプションは、システムユーティリティでは**[Show BMC IP during POST]または[POST 中に BMC の IP アドレスを表示]**なっています。

[Virtual Serial Port Log]
この設定により、仮想シリアルポートのログ記録が有効または無効になります。

- **[有効]** - 仮想シリアルポートの動作が iLO メモリ内の 150 ページの循環バッファーに記録され、CLI コマンドの vsp log を使用して表示できます。仮想シリアルポートのバッファーサイズは 128 KB です。
- **[無効]**（デフォルト）- 仮想シリアルポートの動作は記録されません。

この機能は、ライセンスパッケージの一部です。

iLO Firmware Version 1.30 May 31 2018 以降の場合
[Anonymous Data]
iLO Firmware Version 1.20 Feb 02 2018 以前の場合
[XML Reply]
基本システム情報の匿名要求への応答で iLO が提供する XML オブジェクトを制御します。この設定が有効（デフォルト）になっている場合、ネットワーク上の iLO システムを他のソフトウェアが検出して識別することが許可されます。iLO が提供する XML 応答を表示するには、iLO Firmware Version 1.20 Feb 02 2018 以前の場合は**[View]**を、iLO Firmware Version 1.30 May 31 2018 以降の場合は**[View XML]**をクリックします。
このオプションが無効になっている場合、iLO は空の XML オブジェクトで要求に応答します。

このオプションが有効で iLO ヘルスステータスが**[Degraded]**の場合は、iLO ヘルスステータスが問題の説明とともにログインページに表示されます。iLO ヘルスステータスは、iLO 診断セルフテストを組み合わせた結果に基づいています。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

- **[有効]**（デフォルト）- 他のソフトウェアでネットワーク上の iLO システムを検出して識別することができます。iLO が提供する XML 応答を表示するには［view］をクリックします。
- **[無効] -** iLO は要求に対し空の XML オブジェクト応答をします。

[Serial Command Line Interface Status]
この設定により、シリアルポート経由で使用する CLI 機能のログイン方法を変更できます。

- **[Enabled - Authentication Required]**（デフォルト） - ホストシリアルポートに接続された端末から SMASH CLP にアクセスできます。有効な iLO ユーザー認証情報が必要です。
- **[Enabled - No Authentication]** - ホストシリアルポートに接続された端末から SMASH CLP にアクセスできます。iLO ユーザー証明書は不要です。
- **[Disabled]** - ホストシリアルポートから SMASH CLP へのアクセスを無効にします。物理シリアルデバイスを使用する予定の場合は、このオプションを使用してください。

注記:　このオプションは、システムユーティリティでは**[Serial CLI Status]**となっています。

[Serial Command Line Interface Speed]
この設定により、CLI 機能のシリアルポートの速度を変更できます。有効な速度（ビット/秒）は、

- **[9600]**（デフォルト）
- **[19200]**
- **[38400]** - この値は、BMC 構成ユーティリティでサポートされていません。
- **[57600]**
- **[115200]**

シリアルポート設定は、パリティなし、データビット 8、ストップビット 1（N/8/1）に設定されている必要があります。
このオプションで設定されたシリアルポート速度は、BMC 構成ユーティリティ（システムユーティリティ内）で構成されたシリアルポートの速度に一致する必要があります。

[Minimum Password Length]
この設定により、ユーザーパスワードの設定または変更の際に許可される文字の最小数を指定します。指定する文字数は、0～39 文字の値でなければなりません。デフォルト値は 8 です。

[Server Name]

この設定により、ホストサーバー名を指定することができます。この値は手動で割り当てることもできますが、オペレーティングシステムがロードされる際にホストソフトウェアによって上書きされる場合があります。

- サーバー名は最大 49 バイトまで入力できます。先頭に空白文字は使用しないでください。
- ブラウザーの更新を強制して新しい値を表示するには、この設定を保存して **F5** キーを押します。

[Server FQDN / IP Address]

この設定により、サーバーの FQDN または IP アドレスを指定できます。この値は手動で割り当てることもできますが、オペレーティングシステムがロードされる際にホストソフトウェアによって上書きされる場合があります。

- FQDN または IP アドレスは最大 255 バイトまで入力できます。
- ブラウザーの更新を強制して新しい値を表示するには、この設定を保存して **F5** キーを押します。

[Authentication Failure Logging]

この設定により、認証失敗のログ記録条件を設定できます。以下の設定が有効です。

- **[Enabled - Every Failure]** - ログインに失敗するたびに、失敗したログインログエントリーが記録されます。
- **[Enabled - Every 2nd Failure]** - ログインに 2 回失敗するたびに、失敗したログインログエントリーが記録されます。
- **[Enabled - Every 3rd Failure]**（デフォルト） - ログインに 3 回失敗するたびに、失敗したログインログエントリーが記録されます。
- **[Enabled - Every 5th Failure]** - ログインに 5 回失敗するたびに、失敗したログインログエントリーが記録されます。
- **[Disabled]** - 失敗したログインログエントリーは記録されません。

SSH クライアントでこの設定を使用する方法については、「SSH クライアントを使用した iLO へのログイン」を参照ください。

[Authentication Failure Delay Time]
ログイン試行が失敗した後の iLO ログイン遅延の期間を設定できます。有効な値は 2、5、10、および 30 秒です。

デフォルト値は 10 秒です。

[Authentication Failures Before Delay]
iLO がログイン遅延を課すまでに許容されるログインの失敗数を設定できます。有効な値は 1、3、5 回、または各ログイン試行の失敗時です。
デフォルト値は 1 です。これは 2 度目に試したログインが失敗するまでログイン遅延は課せられないことを意味します。

SSH クライアントを使用した iLO へのログイン

ユーザーが SSH クライアントで iLO にログインすると、iLO が表示するログイン名とパスワードのプロンプト回数は、**[Authentication Failure Logging]**オプションの値（無効の場合は 3）に一致します。プロンプトの回数は、SSH クライアントの設定に影響される場合もあります。また、SSH クライアントでは、ログイン失敗後に遅延が発生します。

たとえば、デフォルト値で SSH 認証失敗ログを生成するには（**[Enabled - Every 3rd Failure]**）の時、連続した 3 回のログイン失敗が次のように発生します（SSH クライアントのパスワードプロンプトが 3 回に設定されていると仮定します）。

1. SSH クライアントを起動し、正しくないログイン名とパスワードでログインします。パスワードプロンプトが 3 回表示されます。正しくないパスワードを 3 回入力すると、接続が終了し、最初のログイン失敗が記録されます。SSH ログイン失敗カウンターが 1 に設定されます。
2. SSH クライアントを起動し、正しくないログイン名とパスワードでログインします。パスワードプロンプトが 3 回表示されます。正しくないパスワードを 3 回入力すると、接続が終了し、2 番目のログイン失敗が記録されます。SSH ログイン失敗カウンターが 2 に設定されます。
3. SSH クライアントを起動し、正しくないログイン名とパスワードでログインします。パスワードプロンプトが 3 回表示されます。正しくないパスワードを 3 回入力すると、接続が終了し、3 番目のログイン失敗が記録されます。SSH ログイン失敗カウンターが 3 に設定されます。

iLO ファームウェアは、失敗した SSH ログインログエントリーを記録し、SSH ログイン失敗カウンターを 0 に設定します。

iLO Service Port

サービスポートは、サーバーの前面にある、iLO のラベルが付けられている USB ポートです。
サーバーに物理的にアクセスできる場合、サービスポートを使用して次のことができます。

- iLO がサポートする USB フラッシュドライブに Active Health System ログをダウンロードします。
  この機能を使用する場合、接続されている USB フラッシュドライブにホストオペレーティングシステムはアクセスできません。
- iLO がサポートする USB Ethernet アダプターにクライアント（ノートパソコンなど）を接続して、iLO Web インターフェース、リモートコンソール、CLI、または iLO RESTful API にアクセスできます。

iLO サービスポートを使用すると、次のようになります。

- 操作が iLO イベントログに記録されます。
- サービスポートのステータスを示すためにサーバーの UID ランプが点滅します。
  REST クライアントと iLO RESTful API を使用してステータスを取得することもできます。

iLO サービスポート経由での Active Health System ログのダウンロード

前提条件
[Security]→[iLO Service Port]ページの**[iLO Service Port]**および**[USB flash drives]**が有効になっている。

手順

1. command.txt という名前のテキストファイルを作成し、Active Health System ログをダウンロードするための必須の内容を記述します。
2. iLO がサポートする USB フラッシュドライブのルートディレクトリに command.txt を保存します。
3. USB フラッシュドライブを iLO サービスポート（サーバーの前面にある、iLO のラベルが付けられている USB ポート）に接続します。
   iLO にファイルシステムがマウントされ、command.txt ファイルが読み込まれて実行されます。

iLO サービスポートのステータスがビジーに変わり、UID ランプが中速で 4 回点滅してから 1 秒オフを繰り返します。
コマンドが成功した場合は、iLO サービスポートのステータスが完了に変わり、UID ランプが高速で 1 回点灯してから 3 秒オフを繰り返します。
コマンドが失敗した場合は、iLO サービスポートのステータスがエラーに変わり、UID ランプが高速で 8 回点滅してから 1 秒オフを繰り返します。エラーが発生した場合は、iLO イベントログを参照してください。
iLO からファイルシステムがマウント解除されます。

4. USB フラッシュドライブを取り外します。
   iLO サービスポートのステータスが準備完了に変わります。UID ランプは点滅を停止するか、リモートコンソールアクセスやファームウェア更新の進行中などの別の状態を示して点滅します。

iLO サービスポートを介した iLO へのクライアントの接続

前提条件

- **[Security]→[iLO Service Port]**ページの**[iLO Service Port]**および**[USB Ethernet adapters]**が有効になっている。
- クライアント NIC がサービスポート機能をサポートするように構成されている。
- サーバーに物理的にアクセスできる。

手順

1. iLO がサポートする USB Ethernet アダプターを使用して、クライアントをサービスポート（サーバーの前面にある、iLO のラベルが付けられている USB ポート）に接続します。
   クライアント NIC にリンクローカルアドレスが割り当てられます。このプロセスには、数秒かかることがあります。
2. ブラウザー、CLI、またはスクリプティングユーティリティで以下の IPv4 アドレスを使用して、iLO に接続します。
   iLO の IP アドレス：169.254.1.2
   サービスポートを介してサーバーにクライアントを接続するときは、同じ IP アドレスが使用されます。このアドレスを変更することはできません。
   サービスポートのステータスがビジーに変わり、UID が中速で 4 回点滅してから 1 秒オフを繰り返します。
3. 作業を終了したら、クライアントをサービスポートから外します。
   サービスポートのステータスが準備完了に変わります。UID は点滅を停止するか、リモートコンソールアクセスやファームウェア更新の進行中などの状態を示して点滅します。

iLO サービスポート設定の構成

前提条件
iLO の設定を構成権限

手順

1. **[Security]→[iLO Service Port]**のページに移動します。
2. 以下の設定を行います。
   - iLO Service Port
   - USB flash drives
   - Require authentication
   - USB Ethernet adapters

3. **[Apply]**をクリックします。
   更新された設定はすぐに有効になり、構成変更に関する情報が iLO イベントログに記録されます。

iLO サービスポートオプション

- **[iLO Service Port]** - iLO サービスポートを有効または無効にすることができます。デフォルト設定は、有効です。この機能を無効にすると、このページの Mass Storage Options セクションまたは Networking Options セクションの機能を構成することはできません。
  使用中の iLO サービスポートを無効にしないでください。データがコピーされているときにこのポートを無効にすると、データが破損する可能性があります。
- **[USB flash drives]** - USB フラッシュドライブを iLO サービスポートに接続して Active Health System ログをダウンロードできます。デフォルト設定は、有効です。
  iLO サービスポートを使用しているときにこの設定を無効にしないでください。データがコピーされているときに USB フラッシュドライブを無効にすると、データが破損する可能性があります。
  この設定が無効のときに USB フラッシュドライブを iLO サービスポートに挿入した場合、デバイスは無視されます。
- **[Require authentication]** - iLO サービスポートを使用して Active Health System ログをダウンロードするときに iLO ユーザー名とパスワードを command.txt ファイルに入力する必要があります。デフォルト設定は、無効です。
  iLO セキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、ユーザー認証情報は不要です。
- [**USB Ethernet adapters**] - USB Ethernet アダプターを使用してノートパソコンを iLO サービスポートに接続し、iLO Web インターフェースや統合リモートコンソールにアクセスできます。デフォルト設定は、有効です。
  この設定が無効な場合に USB Ethernet アダプターを接続してもデバイスは無視されます。

iLO サービスポートを介して接続するクライアントの設定

前提条件
iLO の設定を構成権限

手順
1. IPv4 自動構成アドレスを自動的に取得するクライアント NIC を構成します。詳しくは、オペレーティングシステムのドキュメントを参照してください。
2. 次のいずれかを実行します。
   - プロキシ例外を追加します。次のいずれかの形式を使用します。
     - Edge、Chrome、Internet Explorer：169.254.*
     - Firefox：169.254.0.0/16
   - クライアント上で Web プロキシ設定を無効にします。

   プロキシ設定について詳しくは、ブラウザーのドキュメントを参照してください。

iLO サービスポートでサポートするデバイス

USB フラッシュドライブ

iLO サービスポートは、以下の特性を持つ USB フラッシュドライブをサポートします。
- 高速 USB 2.0 準拠。

- FAT32 フォーマット（512 バイトブロックを推奨）。
- 1 つの LUN。
- 127GB までの 1 つのパーティションと、Active Health System ログをダウンロードするのに十分な空き領域。
- 有効な FAT32 パーティションテーブル。
- 読み取り保護されていない。
- ブート可能ではない。

USB Ethernet アダプター

iLO サービスポートは、ASIX Electronics Corporation の次のいずれかのチップを内蔵した USB Ethernet アダプターをサポートします。

- AX88772
- AX88772A
- AX88772B
- AX88772C

iLO サービスポート経由で Active Health System ログをダウンロードするためのサンプルテキストファイル

iLO サービスポートを使用して Active Health System ログをダウンロードする場合は、command.txt というテキストファイルを作成し、サポートされている USB デバイスにファイルを保存します。USB デバイスをサーバーに接続すると、command.txt ファイルが実行され、ログファイルがダウンロードされます。

command.txt ファイルのテンプレート

command.txt ファイルのテンプレートとして、次の例を使用します。

```
{
  "/ahsdata/" : {
    "POST" : {
      "downloadAll"     : "0",
      "from"    : "2017-08-25",
      "to"      : "2017-08-26",
      "case_no" : "ABC0123XYZ",
      "UserName"        : "my_username",
      "Password"        : "my_password"
    }
  }
}
```

command.txt ファイルのパラメーター

以下の値をカスタマイズできます。

- downloadAll - ダウンロードの範囲を制御します。日付範囲に対応するログをダウンロードするには、0 を入力します。ログ全体をダウンロードするには、1 を入力します。
  1 を入力した場合、ログファイル巨大になる可能性（5~600MB 程度）があります。
- from - 日付範囲に対応するログをダウンロードする場合の開始日。
- to - 日付範囲に対応するログをダウンロードする場合の終了日。

- case_no（オプション）- 開いている NEC サポートケースのケース番号。この値の最大長は 14 文字です。この値を入力すると、それがダウンロードしたファイルに含まれます。保守員の指示があった場合に限り入力してください。
- UserName - LO サービスポート設定で**[Require authentication]**を有効に構成されている場合は、iLO アカウントのユーザー名を入力します。**[Require authentication]**を無効にするようシステムメンテナンススイッチが設定されている場合、ユーザー名は不要です。
- Password - iLO サービスポート設定で**[Require authentication]**を有効に構成されている場合は、iLO ユーザー名のパスワードを入力します。**[Require authentication]**を無効にするようシステムメンテナンススイッチが設定されている場合、パスワードは不要です。

command.txt ファイルの要件

- ファイルは、有効な JSON 形式でなければなりません。
- オンラインの JSON フォーマッターを使用して、ファイルの構文を確認することをおすすめします。Web サイト http://www.freeformatter.com/json-formatter.html で無料のユーティリティを入手できます。
- ファイル内にコメントを含めないでください。
- ファイル内のテキストでは大文字と小文字が区別されます。
- ファイルではプレーンテキストのみサポートされます。追加の書式設定プロパティを埋め込むアプリケーションを使用してファイルを作成しないでください。

SSH キーの管理

[Secure Shell Key]ページには、各ユーザーに関連付けられた SSH パブリックキーのハッシュが表示されます。各ユーザーに割り当てられるキーは 1 つだけです。SSH キーを表示、追加、または削除するには、このページを使用します。

SSH キーを追加および削除するには、ユーザーアカウント管理権限が必要です。

SSH キー

iLO に SSH キーを追加するときは、SSH キーファイルを iLO に貼り付けます。ファイルには、ユーザーが生成したパブリックキーが含まれている必要があります。iLO ファームウェアは、選択したローカルユーザーアカウントに各キーを関連付けます。ユーザーに対して SSH キーが認証された後にそのユーザーが削除されると、SSH キーが削除されます。
次の SSH キー形式がサポートされます。

RFC 4716

```
---- BEGIN SSH2 PUBLIC KEY ---
Comment:"Administrator"
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuAlNLlivLFP3IoKZ
ZtzF0VInP5x2VFVYmTvdVjD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCT3wl
3ldxQvPYnhTYyhPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgts8/UA
AAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAgCbnhADYXu+Mv4xuXccXWP0Pcj47
7YiZgos3jt/Z0ezFX6/cN/RwwZwPC1HCsMuwsVBIqi7bvn1XczFPKOt06gVWcjFt
eBY3/bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHg8Z
JazhY920PpkD4hNbAAAAgDN3lba1qFVl0UlRjj21MjXgr6em9TETSOO5b7SQ8hX/
Z/axobbrHCj/2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYaiF
DLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtSTV
---- END SSH2 PUBLIC KEY ---
```

OpenSSH キー形式

```
ssh-dss
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDlI+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avNSz0DNQuU7gTPfjj/8c
XyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/kDMC0dVOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI
3J61F+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5QxqkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpAlxAp6eDZKFvj3ZIy
NjcQODeYYqOvVU45AkSkLBMGjpF05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxD
OvNWAAAAgFf6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80SfWSnWM3n/pekBa9Ql9lH1r
3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/K8YnFNwwYy2NSJyjLwA0TSmQEOW Administrator
```

iLO レガシー形式

BEGIN/END ヘッダーで囲まれた OpenSSH キーです。この形式は、BEGIN SSH KEY と END SSH KEY テキストの間で 1 行にする必要があります。

```
-----BEGIN SSH KEY----
ssh-dss
AAAAB3NzaC1kc3MAAACBANA45qXo9cM1asav6ApuCREt1UvP7qcMbw+sTDrx9lV22XvonwijdFiOM/0VvuzVhM9oKdGMC7sCGQr
FV3zWDMJcIb5ZdYQSDt44X6bvlsQcAR0wNGBN9zHL6YsbXvNAsXN7uBM7jXwHwrApWVuGAI0QnwUYvN/dsE8fbEYtGZCRAAAAFQ
DofA47q8pIRdr6epnJXSNrwJRvaQAAAIBY7MKa2uH82I0KKYTbNMi0o5mOqmqy+tg5s9GC+HvvYy/S7agpIdfJzqkpHF5EPhm0j
KzzVxmsanO+pjju7lrE3xUxojevlokTERSCM xLa+OVVbNcgTe0xpvc/cF6ZvsHs0UWz6gXIMCQ9Pk118VMOw/tyLp42YXOaLZzG
fi5pKAAAAIEAI7FsO7sDbPj02a5jO3qFXa762lWvu5iPRZ9cEt5WJEYwMO/ICaJVDWVOpqF9spoNb53Wl1pUARJg1ss8Ruy7YBv
8Z1urWWAF3fYy7R/SlQqrsRYDPLM5eBkkLO28B8C6++HjLuc+hBvj90tsqeNVhpCfO9qrjYomYwnDC4m1IT4= ASmith

-----END SSH KEY-----
```

SSH キーを使用する場合は、次の点に留意してください。

- これまで示したサンプル形式は、iLO Web インターフェースと CLI でサポートされています。
- 対応するプライベートキーを使用して認証される SSH 接続は、キーの所有者として認証され、同じ権限を持ちます。
- iLO ファームウェアは、1366 バイト以下の長さの SSH キーに対応できるストレージを提供します。キーが 1366 バイトを超える場合、認証に失敗することがあります。認証に失敗する場合は、SSH クライアントソフトウェアを使用して、より短いキー生成してください。
- iLO の Web インターフェースを使用してパブリックキーを入力する場合は、パブリックキーに関連付けられたユーザーを選択します。CLI を使用してパブリックキーを入力する場合は、パブリックキーが、iLO にログインするために入力したユーザーに結び付けられます。

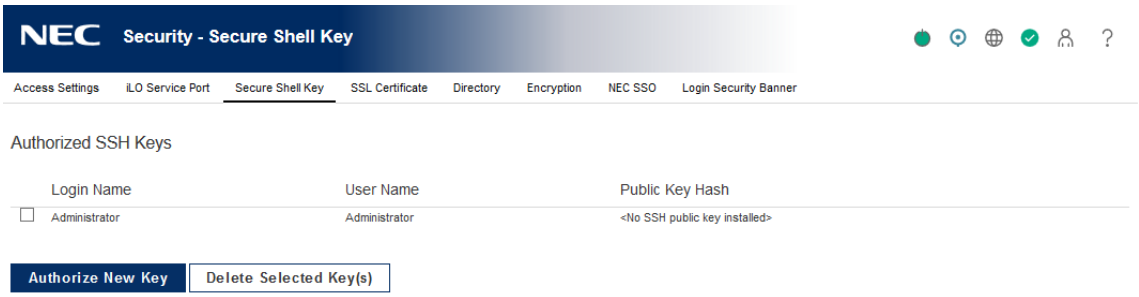
詳細情報

新しい SSH キーの認証
CLI を使用した新しい SSH キーの認証

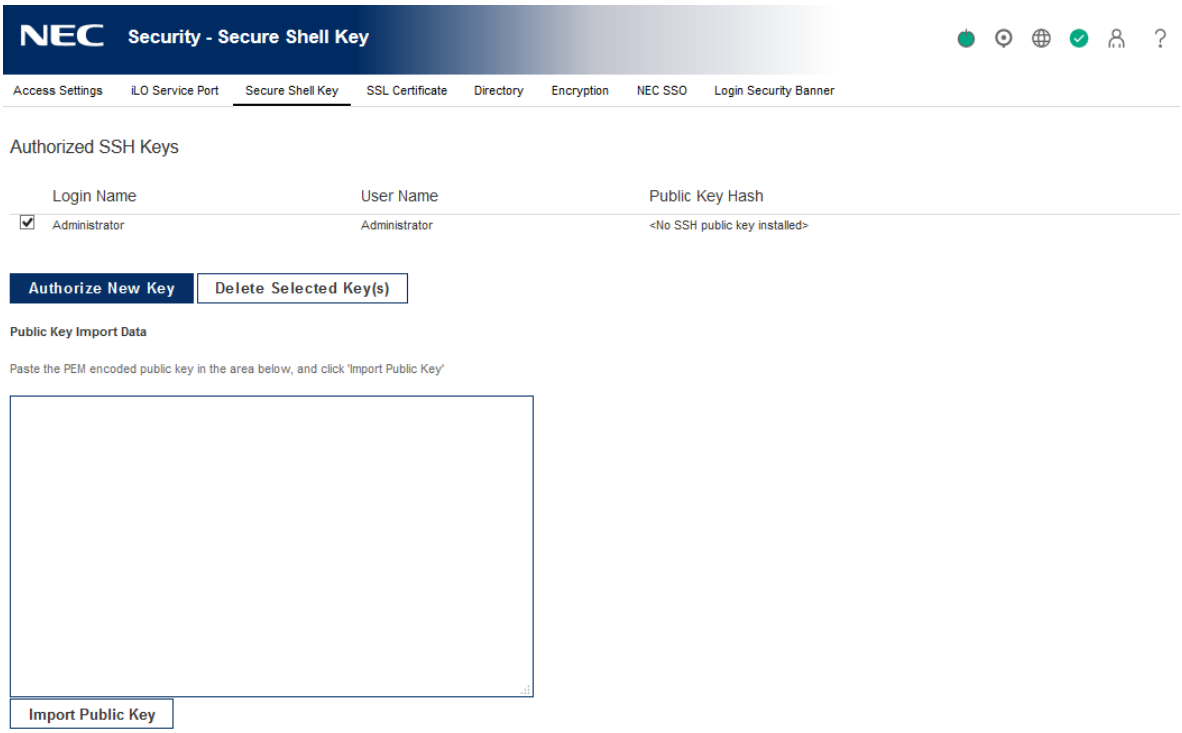
新しい SSH キーの認証

手順

1. ssh-keygen、puttygen.exe、または別の SSH キーユーティティを使用して、2,048 ビットの DSA or RSA キーを生成します。
2. key.pub ファイルを生成します。
3. **[Security]**ページに移動します。
4. **[Secure Shell Key]**タブをクリックします。



5. SSH キーを追加するユーザーの名前の左にあるチェックボックスを選択します。
6. **[Authorize New Key]**をクリックします。
7. パブリックキーをコピーして **[Public Key Import Data]**ボックスに貼り付けます。



キーは、2,048 ビットの DSA キーまたは RSA キーでなければなりません。

8. **[Import Public Key]**をクリックします。

CLI を使用した新しい SSH キーの認証

手順

1. ssh-keygen、puttygen.exe、または別の SSH キーユーティティを使用して、2,048 ビットの DSA または RSA SSH キーを生成します。
2. key.pub ファイルを生成します。
3. **[Security]→[Access Settings]**ページで **[Secure Shell (SSH)]**が有効になっていることを確認します。

   詳しくは、「iLO アクセスの設定」を参照してください。

4. ポート 22 で Putty.exe を使用して SSH セッションを開きます。
5. cd /map1/config1 ディレクトリに移動します。
6. 次のコマンドを入力します。

   oemNEC_loadSSHkey -source <protocol://username:password@hostname:port/filename>
   このコマンドを使用するときは次の点に留意してください。

   - protocol の値は必須で、HTTP または HTTPS でなければなりません。
   - hostname と filename の値は必須です。
   - username:password と port の値はオプションです。
   - oemNEC_loadSSHkey は、大文字と小文字が区別されます。

CLI では、URL の厳密な検査が行われないため、URL が正しいか確認してください。次の例でコマンド構造を示します。

```
</map1/config1>iLO-> oemNEC_loadSSHkey -source http://192.168.1.1/path/sshkey.pub
```

SSH キーの削除

手順

1. **[Security]**ページに移動します。
2. **[Secure Shell Key]**タブをクリックします。
3. SSH キーを削除するユーザーの名前の左にあるチェックボックスを選択します。
4. **[Delete Selected Key(s)]**をクリックします。

   選択した SSH キーが iLO から削除されます。SSH キーを iLO から削除すると、SSH クライアントは、iLO に対して、対応するプライベートキーを使用して認証できなくなります。

SSL 証明書の管理

SSL プロトコルは、データがネットワークを移動しているときに、他人がデータを見たり、変更したりできないようにデータを暗号化するための規格です。このプロトコルは、キーを使用してデータの暗号化と解読を実行します。一般的に、キーが長いほど、暗号強度が増えます。証明書は、SSL キーをサーバーに接続する小さいデータファイルです。証明書には、サーバーの名前とサーバーのパブリックキーが含まれています。対応するプライベートキーを持っているのはサーバーのみであり、サーバーが認証されます。
証明書は署名がないと有効になりません。CA によって署名され、その CA が信頼される場合、CA によって署名されるすべての証明書も信頼されます。自己署名証明書は、証明書の所有者がそれ自身の CA として機能する証明書です。
iLO は、SSL 接続で使用するために自己署名の電子証明書をデフォルトで作成します。この電子証明書により、設定手順を追加することなく、iLO の動作を有効にすることができます。信頼済みの証明書をインポートすると、iLO セキュリティ機能を強化できます。iLO の設定を構成権限を持つユーザーは、CA によって署名された信頼済みの証明書をカスタマイズおよびインポートできます。

SSL 証明書情報の表示

証明書情報を表示するには、**[Security]**→**[SSL Certificate]**ページに移動します。

以下の証明書詳細が表示されます。

- **[Issued To]** - 証明書の発行先の名前。
- **[Issued By]** - 証明書を発行した CA。
- **[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]** - CA によって割り当てられた証明書のシリアル番号。

SSL 証明書の取得とインポート

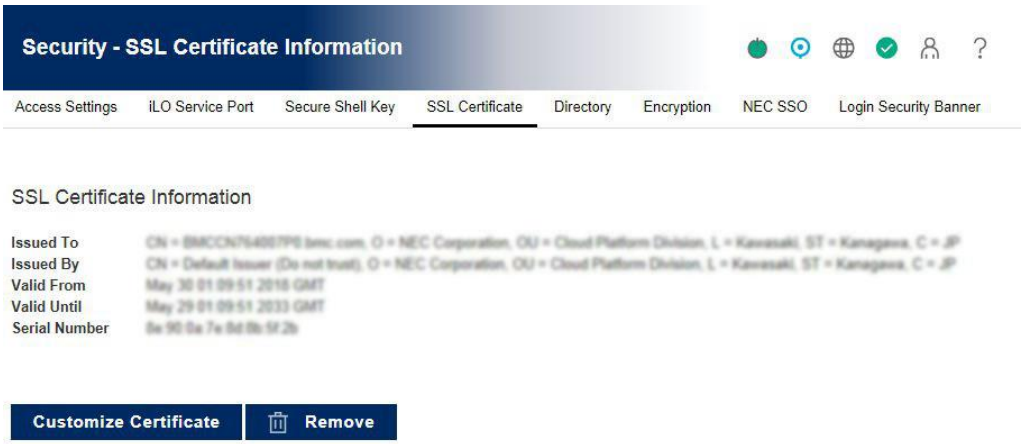
iLO では、iLO にインポートする信頼済みの SSL 証明書を取得するために証明機関に送信できる証明書署名要求を作成できます。

SSL 証明書は、対応する CSR を使用して生成されたキーがないと動作しません。iLO が工場出荷時のデフォルト設定にリセットされる場合、または前の CSR に対応する証明書がインポートされる前に別の CSR が生成される場合、証明書は動作しません。その場合には、新しい CSR を生成し、この CSR を使用して CA から新しい証明書を取得する必要があります。

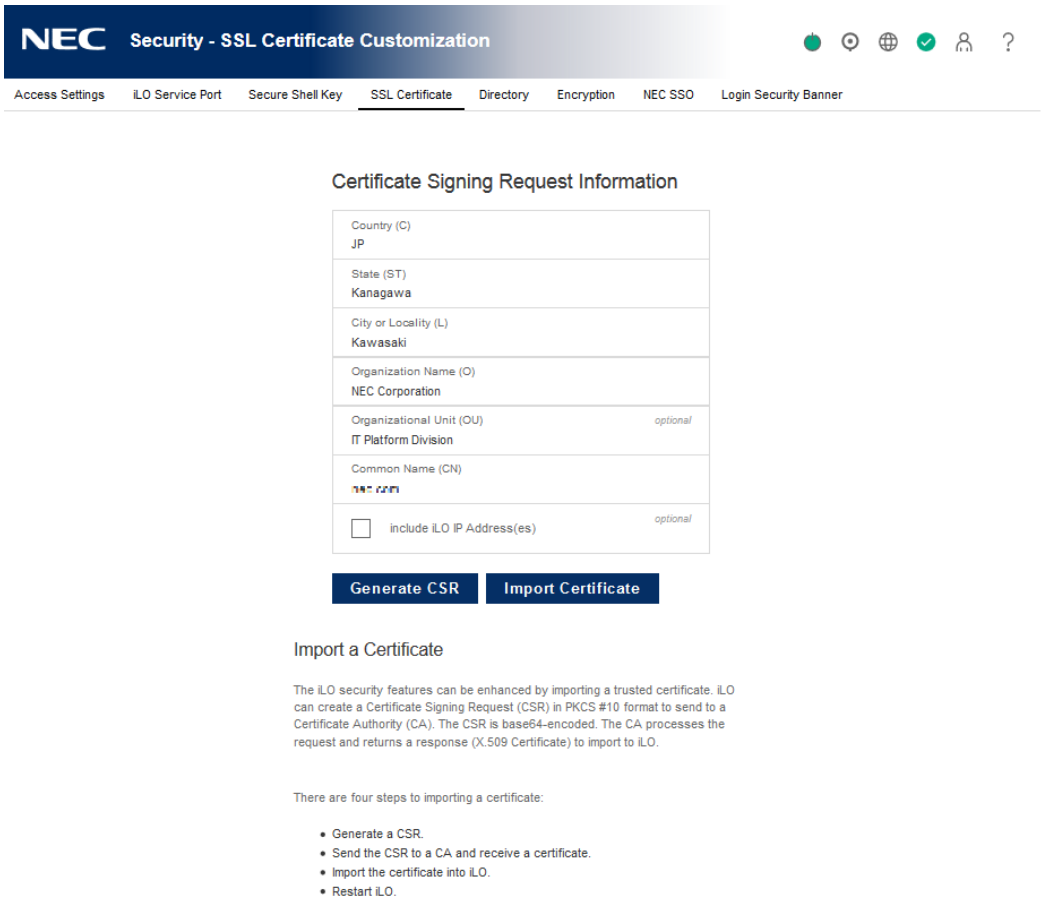
前提条件
iLO の設定を構成権限

手順(SSL 証明書の取得手順)

1. **[Security]→[SSL Certificate]**ページに移動します。



2. **[Customize Certificate]**をクリックします。



3. **[Certificate Signing Request Information]**セクションで、次のように入力します。
   - **[Country (C)]** - この iLO サブシステムを所有する会社または組織が存在する国を識別する 2 文字の国番号。2 文字の省略表記を大文字で入力します。
   - **[State (ST)]** - この iLO サブシステムを所有する会社または組織が存在する都道府県。
   - **[City or Locality (L)]** - この iLO サブシステムを所有する会社または組織が存在する市町村。
   - **[Organization Name (O)]** - この iLO サブシステムを所有する会社または組織の名前。
   - **[Organizational Unit (OU)]** - （省略可能）この iLO サブシステムを所有する会社または組織の中の単位。
   - **[Common Name (CN)]** - この iLO サブシステムの FQDN。

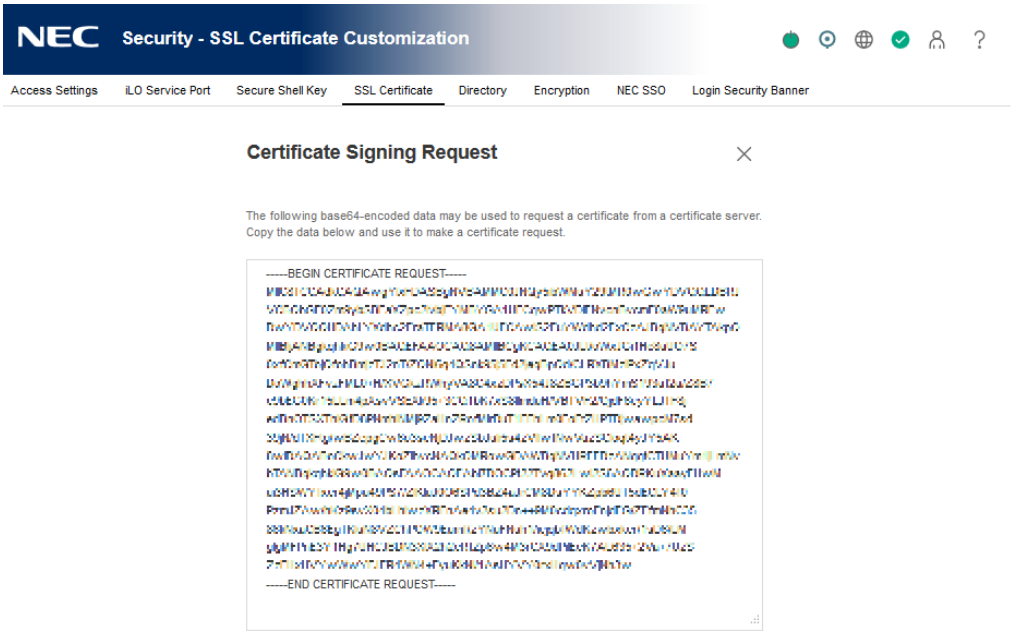
     FQDN は、**[Common Name (CN)]** ボックスに自動的に入力されます。

     iLO が CSR に FQDN を入力できるように、**[iLO Dedicated Network Port]** →**[General]** または**[iLO Shared Network Port]** →**[General]**ページで **[Domain Name]**を設定する必要があります。ネットワーク設定の構成については、「ネットワークの全般設定」を参照してください。
   - ［**include iLO IP Address(es)**］- （省略可能）CSR に iLO の IP アドレスを含める場合は、チェックボックスをオンにします。このオプションは、この値を使用できない CA があるため、デフォルトでは無効になっています。
4. **[Generate CSR]**をクリックします。

証明書を生成中であり、その処理に最大で 10 分かかる可能性があることを伝えるメッセージが表示されます。

5. 数分（最大 10 分）後に、**[Generate CSR]**を再度クリックします。

   CSR が表示されます。



   CSR には、クライアントブラウザーと iLO 間の通信を検証するパブリックキーとプライベートキーのペアが含まれています。サポートされるキーの最大サイズは 2,048 ビットです。生成された CSR は、新しい CSR が生成されるまで、iLO が工場出荷時のデフォルト設定にリセットされるまで、または証明書がインポートされるまで、メモリに保持されます。

6. CSR テキストを選択してコピーします。
7. ブラウザーウィンドウを開き、第三者認証機関に移動します。
8. 画面の指示に従って、CSR を CA に送信します。

   CSR を CA に送信する場合、ご使用の環境にサブジェクト代替名（SAN）の指定が必要となる場合があります。通常、この情報は **[追加の属性]**ボックスにあります。必要な場合、 iLO DNS の省略名と IP アドレスを **[追加の属性]**ボックスに san:dns=<IP アドレス >&dns=< サーバー名 > の構文を使用して入力します。

   CA は、PKCS #10 形式の証明書を生成します。

9. 証明書を取得したら、以下の事項を確認してください。

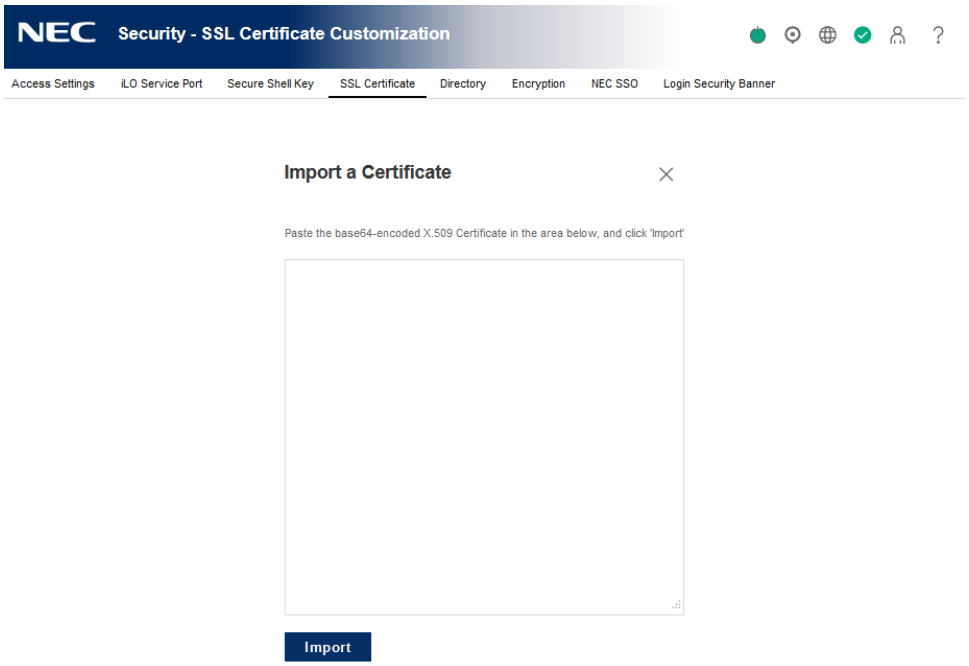
   - CN が iLO FQDN と一致している。

     これは、**[Information]**→**[Overview]**ページに **[iLO Hostname]**として表示されます。

   - 証明書が Base64 でエンコードされた X.509 証明書である。
   - 証明書に開始行と終了行が含まれている。

手順(インポート)

1. **[Security]**→**[SSL Certificate]**ページに移動します。
2. **[Customize Certificate]**、**[Import Certificate]** ボタンの順にクリックします。



3. テキストボックスに証明書を貼り付けて、**[Import]**をクリックします。

   iLO は、3 KB までのサイズ（プライベートキーで使用され、それぞれが 1,024 ビットおよび 2,048 ビット証明書に対応する 609 バイトまたは 1,187 バイトを含む）の SSL 証明書をサポートします。

4. iLO をリセットします。

   手順については、「iLO の再起動（リセット）」を参照してください。

カスタマイズされた証明書の削除

この機能を使用して、カスタム SSL 証明書を削除し、iLO 自己署名証明書を再生成します。次の理由から、カスタム証明書を削除する場合があります。

- 証明書の有効期限が切れた。
- 証明書に無効な情報が含まれている。
- 証明書に関してセキュリティ上の問題がある。
- 実績のあるサポート組織からカスタム証明書を削除するよう勧められた。

前提条件

iLO の設定を構成権限

手順

1. ナビゲーションツリーで**[Security]**をクリックし、**[SSL Certificate]**をクリックします。
2. **[Remove]**をクリックします。

   iLO が既存の証明書を削除し、iLO をリセットしてから、新しい自己署名証明書を生成することを確認メッセージが表示されます。
3. **[Yes, remove]**をクリックします。

iLO がカスタム SSL 証明書を削除し、iLO リセット後に新しい自己署名証明書を生成します。iLO で新しい証明書を生成するには数分かかる場合があります。

iLO リセット手順については、「iLO の再起動（リセット）」を参照してください。

ディレクトリの認証と認可

iLO ファームウェアは、ユーザーの認証と認可を行うために Microsoft Active Directory をサポートします。iLO は、スキーマフリーディレクトリ統合を使用して、ユーザーの認証や権限付与を行えるように設定することができます。iLO ファームウェアは、ディレクトリサービスに接続する場合に、SSL 接続を使用してディレクトリサーバーの LDAP ポートに接続します。デフォルトのセキュリティ保護されている LDAP ポートの番号は、636 です。

iLO ディレクトリサポートが有効になっている場合、ローカルに保存されているユーザーアカウント（**[Administration]→[Directory Groups]**ページに表示されます）をアクティブにすることができます。これにより、ローカルベースとディレクトリベースの両方のユーザーアクセスが可能になります。通常、iLO のディレクトリサービスに対するアクセス設定が完了した後は、ローカルユーザーアカウントを削除して問題ありません（ただし、緊急時のアクセス用アカウントは残しておくとよいでしょう）。ディレクトリサポートが有効になっている場合は、ローカルユーザーアカウントに対するアクセスを無効にしておくという運用方法もあります。

認証およびディレクトリサーバーの設定

認証およびディレクトリサーバーの設定は、ディレクトリまたは Kerberos ログインを使用するための iLO 構成プロセスの手順の 1 つです。

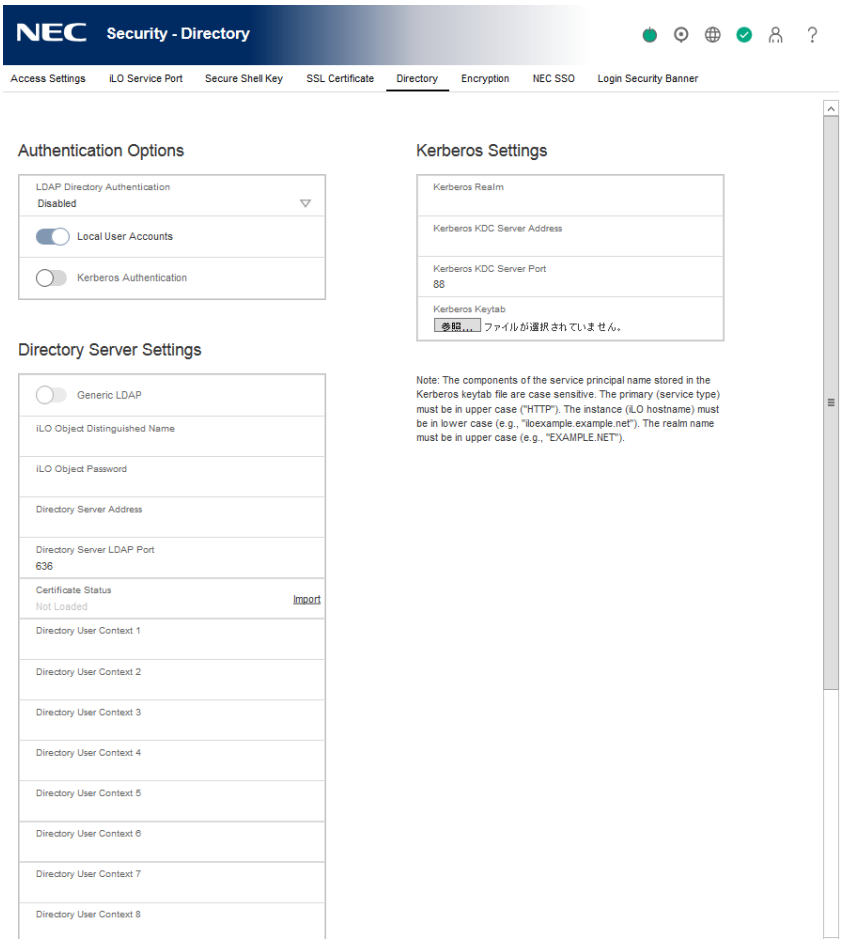
これらの機能を使用するための環境セットアップについて詳しくは、「Kerberos 認証とディレクトリサービス」を参照してください。

前提条件

- iLO の設定を構成権限
- この機能をサポートする iLO ライセンスがインストールされている。

手順

1. **[Security]→[Directory]**ページに移動します。



2. **[LDAP Directory Authentication]**を設定します。この設定は、ディレクトリ認証を有効または無効にします。ディレクトリ認証が有効で正しく設定されている場合、ユーザーはディレクトリ認証情報を使用してログインできます。

   以下のオプションの中から選択します。

   - **[Disabled]** - ディレクトリを使用してユーザー認証情報を検証しません。
   - **[Use Directory Default Schema]** - ディレクトリ内のユーザーアカウントを使用するディレクトリ認証および権限付与を選択します。
     ユーザーの認証と権限付与には、ユーザーアカウントとグループメンバーシップが使用されます。ディレクトリネットワーク情報を入力して保存したら、**[Administrator Groups]**をクリックし、ユーザーに iLO アクセスを許可するために 1 つ以上の有効なディレクトリ DN と権限を入力します。
3. **[Local User Accounts]**を設定します。この設定は、ローカルユーザーアカウントのアクセスを有効または無効にします。
   - **[有効]** - ユーザーはローカルで保存されているユーザー認証情報を使用してログインできます。このオプションを有効にして、管理者権限を持つユーザーアカウントを設定することをおすすめします。iLO がディレクトリサーバーと通信できない場合、このアカウントを使用できます。
   - **[無効]** - ユーザーアクセスは、有効なディレクトリ認証情報がある場合に限定されます。
     他のメカニズムを介してアクセスを検証するまでは、ローカルユーザーアクセスを無効にしないでください。

ローカルユーザーアカウントを使用するアクセスは、ディレクトリサポートが無効になっている場合、および iLO ライセンスが取り消された場合に有効になります。

4. **[Kerberos Authentication]**を設定します。この設定は、Kerberos ログインを有効または無効にします。Kerberos ログインが有効で、正しく設定されている場合、ログインページに**[Zero Sign In]**ボタンが表示されます。
5. **[Kerberos Authentication]**が有効にする場合は、以下を設定します。
   - **[Kerberos Realm]** - iLO プロセッサーが動作している Kerberos レルムの名前。この文字列は最大 128 文字です。レルム名は、通常、大文字に変換された DNS 名です。レルム名は、大文字と小文字が区別されます。
   - **[Kerberos KDC Server Address]** - Key Distribution Center（KDC）の IP アドレスまたは DNS 名の文字列で最大 128 文字です。各レルムには、認証サーバーおよびチケット交付サーバーを含む 1 つ上の KDC がある必要があります。これらのサーバーは、結合させることができます。
   - **[Kerberos KDC Server Port]** - KDC が使用している TCP または UDP ポート番号です。デフォルトの KDC ポートは 88 です。
   - **[Kerberos Keytab]** - サービスプリンシパル名と暗号化されたパスワードのペアが含まれているバイナリー・ファイル。Windows 環境では、キータブファイルは、ktpass ユーティリティが生成します。**[参照]**（Internet Explorer または Firefox）または **[ファイルを選択]**（Microsoft Edge または Chrome）をクリックし、画面上の指示に従ってファイルを選択します。

     Kerberos キータブファイルに格納されるサービスプリンシパル名のコンポーネントでは、大文字と小文字が区別されます。プライマリー（サービスタイプ）は、たとえば HTTP のように大文字でなければなりません。インスタンス（iLO ホスト名）は、たとえば example.example.net のように小文字でなければなりません。レルム名は、EXAMPLE.NET のように大文字でなければなりません。
6. ディレクトリサーバー設定を入力します。
   - **[Generic LDAP] -**この設定は、OpenLDAP がサポートする BIND メソッドを有効または無効にします。
   - **[Directory Server Address]** - ディレクトリサーバーのネットワーク DNS 名または IP アドレスを指します。ディレクトリサーバーアドレスは最大 127 文字です。

     ディレクトリサーバーを定義するときは、DNS ラウンドロビンを使用することをおすすめします。
   - **[Directory Server LDAP Port]** - サーバー上の安全な LDAP サービス用のポート番号を指定します。デフォルト値は 636 です。別のポートを使用するようにディレクトリサービスを設定する場合は、別の値を指定できます。
   - **[Certificate Status]** - ディレクトリサーバーの CA 証明書をロードする場合に設定します。ロードする場合には**[Import]**をクリックし、表示されたテキストボックスに証明書を貼り付け、**[Import]**ボタンをクリックします。
   - **[Directory user contexts]** - これら 1～15 のボックスを使用して、ユーザーがログイン時に完全な DN を入力する必要がないように、共通のディレクトリサブコンテキストを指定できます。ディレクトリユーザーコンテキストは最大 128 文字です。詳しくは、「ディレクトリユーザーコンテキスト」を参照してください。

7. **[Apply Settings]**をクリックします。
8. ディレクトリサーバーと iLO 間の通信をテストするには、**[Test Settings]**をクリックします。
   詳しくは、「ディレクトリテストの実行」を参照してください。
9. 省略可能：**[Administer Groups]**をクリックして、**[DirectoryGroups]**ページに移動し、ディレクトリグループを構成することができます。

ディレクトリユーザーコンテキスト

固有 DN を使用すると、ディレクトリに表示されるすべてのオブジェクトを識別できます。ただし、DN が長かったり、ユーザーが自分の DN を知らなかったり、ユーザーが異なる DN でアカウントを持っている場合があります。iLO は、DN でディレクトリサービスへの接続を試みたあと、成功するまで順番に検索コンテキストを適用します。

- 例 **1** - 検索コンテキスト ou=engineering,o=ab を入力すると、cn=user,ou=engineering,o=ab の代わりに user としてログインできます。
- 例 **2** - システムが Information Management、Services、および Training によって管理されている場合、次のような検索コンテキストを使用すると、これらの組織に所属するユーザーは、共通名を使用してログインできます。

  ディレクトリユーザーコンテキスト 1 : ou=IM,o=ab

  ディレクトリユーザーコンテキスト 2 : ou=Services,o=ab

  ディレクトリユーザーコンテキスト 3 : ou=Training,o=ab

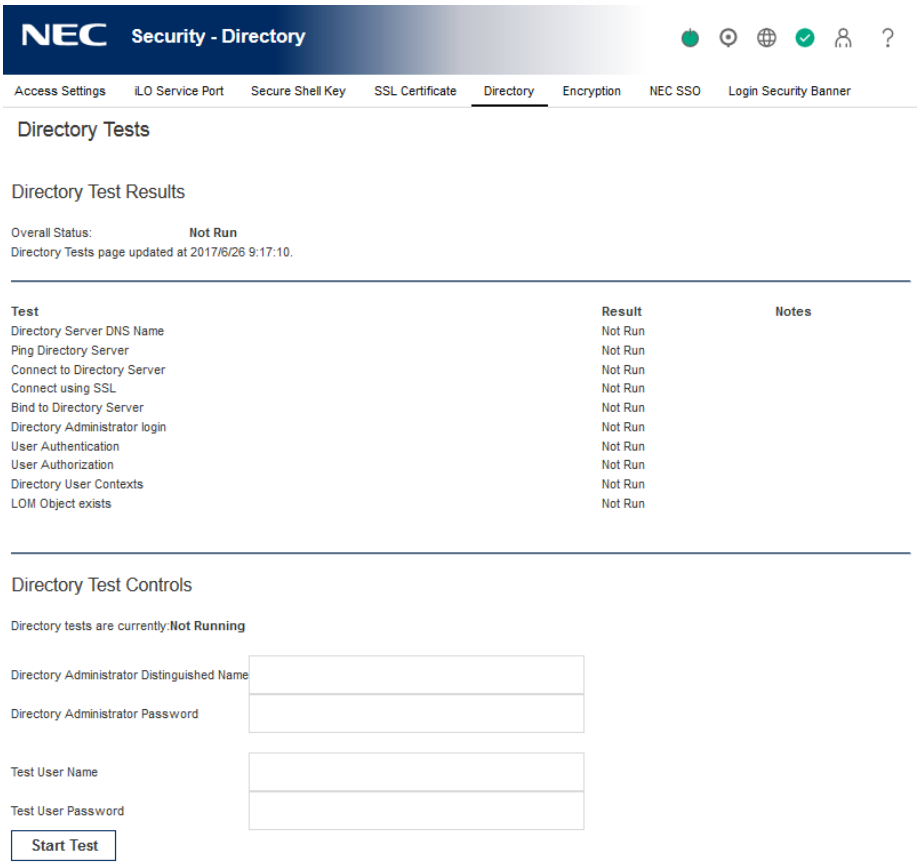
  ユーザーが IM 部門と Training 部門の両方に所属する場合は、最初に cn=user,ou=IM,o=ab としてログインが試みられます。
- 例 **3**（**Active Directory** 専用） - Microsoft Active Directory では、代替ユーザー認証情報フォーマットを使用できます。@domain.example.com という検索コンテキストによってユーザーが user としてログインできる場合、このユーザーは user@domain.example.com としてログインできます。成功したログイン試行のみが、この形式の検索コンテキストをテストできます。

ディレクトリテストの実行

[Directory Tests] を使用すると、設定が済んだディレクトリの設定を検証できます。ディレクトリテストの結果は、ディレクトリ設定が保存されるとき、またはディレクトリテストが開始されるときにリセットされます。

手順

1. **[Security]**→**[Directory]**ページの **[Test Settings]**をクリックします。



[Directory Tests]ページには、現在のディレクトリ設定の有効性を確認するために設計された一連の簡単なテストの結果が表示されます。また、このページには、テスト結果および検出された問題を示すログも表示されます。ディレクトリを正しく設定した後にこれらのテストを再実行する必要はありません。**[Directory Tests]**ページでは、ディレクトリユーザーとしてログインする必要はありません。

2. **[Directory Test Controls]**セクションで、ディレクトリ管理者の DN およびパスワードを入力します。
   - **[Directory Administrator Distinguished Name]** - iLO オブジェクト、ロール、および検索コンテキストについてディレクトリを検索します。このユーザーは、ディレクトリ読み取り権限を持っている必要があります。
   - **[Directory Administrator Password]** - ディレクトリ管理者を認証します。

   ディレクトリ内に iLO オブジェクトを作成する際に使用するものと同じ識別名とパスワードを使用することをおすすめします。これらの識別名とパスワードは、iLO によって保存されるものではなく、iLO オブジェクトとユーザー検索コンテキストを確認するために使用されます。
3. **[Directory Test Controls]**セクションで、テストユーザーの名前とパスワードを入力します。
   - **[Test User Name]** - iLO へのログインとアクセス権をテストします。ユーザー検索コンテキストを適用できるため、ユーザー名は完全修飾である必要はありません。このユーザーは、この iLO のロールに関連付けられている必要があります。
   - **[Test User Password]** - テストユーザーを認証します。

   通常、このアカウントはテスト対象の iLO プロセッサーへのアクセスに利用します。これはディレクトリ管理者アカウントでも構いませんが、スーパーユーザーアカウントではテスト

でユーザー認証を検証できません。これらのユーザー名とパスワードは、iLO によって保存されるものではありません。

4. **[Start Test]**をクリックします。

   複数のテストがバックグラウンドで開始し、最初にサーバーとの SSL 接続を確立し、ユーザー権限を評価して、ネットワーク経由でのディレクトリユーザーに対する Ping が実行されます。

テストの実行中、ページは定期的に更新されます。テストはいつでも停止でき、ページを手動で更新することもできます。

ディレクトリテスト結果

[Directory Test Results]セクションには、ディレクトリテストのステータスが最後の更新日時とともに表示されます。

- **[Overall Status]** - テストの結果の要約が示されます。
  - **[Not Run]**- テストは実行されていません。
  - **[Inconclusive]** - 結果は報告されませんでした。
  - **[Passed]** - エラーは報告されませんでした。
  - **[Problem Detected]** - 問題が報告されました。
  - **[Failed]** - 特定のサブテストが失敗しました。問題を特定するには、画面上のログをチェックします。
  - **[Warning]** - 1 つ以上のディレクトリテストが、**[Warning]**ステータスを報告しました。
- **[Test]** - 各テストの名前が示されます。

  ディレクトリテストについて詳しくは、「iLO ディレクトリテストについて」を参照してください。
- **[Result]** - 特定のディレクトリ設定のステータス、または 1 つまたは複数のディレクトリ設定による動作のステータスが報告されます。これらの結果は、テストシーケンスを実行すると生成されます。テストの実行が終了したとき、テストが失敗して先に進めないとき、またはテストを停止したとき、結果は停止します。テスト結果を示します。
  - **[Passed]** - テストは正常に実行されました。複数のディレクトリサーバーがテストされた場合は、テストを実行したすべてのサーバーで成功しています。
  - **[Not Run]** - テストは実行されませんでした。
  - **[Failed]** - 1 つまたは複数のディレクトリサーバーについてテストが成功しませんでした。それらのサーバーでは、ディレクトリサポートを使用できない可能性があります。
  - **[Warning]** - テストが実行され、証明書エラーなどの警告状態を報告しました。**[Notes]**列で、警告状態を解消するために推奨される処置を確認してください。
- **[Notes]** - ディレクトリテストのさまざまな段階の結果を示します。データは、エラーの詳細と、すぐには入手できない情報（ディレクトリサーバーの証明書のサブジェクトや、どのロールの評価が成功したかなど）によって更新されます。

ディレクトリテスト制御の使用

[iLO directory tests]セクションでは、ディレクトリテストの現在の状態を表示し、テストパラメーターを調整し、テストを開始/停止し、ページの内容を更新することができます。

- **[In Progress]** - ディレクトリテストが現在バックグラウンドで実行されていることを示します。現在のテストを取り消すには、**[Stop Test]** をクリックします。最新の結果でページの内容を更新するには、**[Refresh]** をクリックします。**[Stop Test]**ボタンを使用しても、テストがただちに終了されない場合があります。
- **[Not Running]** - ディレクトリテストは最新であり、新しいパラメーターを指定してテストを再度実行できることを示します。**[Start Test]**ボタンを使用してテストを開始し、現在のテスト制御値を使用することができます。ディレクトリテストは、すでに実行中の場合には、開始できません。
- **[Stopping]** - ディレクトリテストがまだ停止できる段階に達していないことを示します。ステータスが **[Not Running]**に変わるまでは、テストを再開できません。テストが完了したかどうかを確認するには、**[Refresh]**ボタンを使用してください。

iLO ディレクトリテストについて

ディレクトリテストの説明は次のとおりです。

- **[Directory Server DNS Name]** - ディレクトリサーバーが FQDN フォーマット（directory.example.com）で定義されている場合、iLO は、名前を FQDN フォーマットから IP フォーマットに解決し、設定された DNS サーバーに問い合わせます。

  iLO が設定されたディレクトリサーバーの IP アドレスを取得した場合、テストは成功します。iLO がディレクトリサーバーの IP アドレスを取得できない場合、このテストと以後のテストすべてが失敗します。

  ディレクトリサーバーが IP アドレスで設定されている場合、iLO はこのテストを省略します。

  テストが失敗した場合は、以下を実行してください。

  1. iLO に設定されている DNS サーバーが正しいことを確認します。
  2. ディレクトリサーバーの FQDN が正しいことを確認します。
  3. トラブルシューティングツールとして、FQDN の代わりに IP アドレスを使用します。
  4. 問題がなくならない場合は、DNS サーバーの記録とネットワークルーティングをチェックします。

- **[Ping Directory Server]** - iLO は、設定されたディレクトリサーバーに対する ping を開始します。

  iLO が ping 応答を受信する場合、テストは成功します。ディレクトリサーバーが iLO に応答しない場合、テストは失敗します。

  テストが失敗する場合、iLO は以後のテストを続行します。

  テストが失敗した場合は、以下を実行してください。

  1. ディレクトリサーバーでファイアウォールが有効かどうかをチェックします。
  2. ネットワークルーティング問題をチェックします。

- **[Connect to Directory Server]** - iLO は、ディレクトリサーバーとの LDAP 接続を試みます。

  iLO が接続を開始できた場合、テストは成功します。

指定したディレクトリサーバーとの LDAP 接続を iLO が開始できなかった場合、テストは失敗します。以後のテストは、停止します。テストが失敗した場合は、以下を実行してください。

1. 設定されたディレクトリサーバーが正しいホストであることを確認します。
2. （iLO とディレクトリサーバー間のすべてのルーターやファイアウォールを考慮して）iLO がポート 636 経由でディレクトリサーバーとのクリアな通信パスを持っていることを確認します。
3. ディレクトリサーバー上のローカルファイアウォールが有効になっており、ポート 636 経由で通信できることを確認します。

- **[Connect using SSL]** - iLO は、ポート 636 経由で SSL ハンドシェークおよびディレクトリサーバーとの LDAP 通信を開始します。

  iLO とディレクトリサーバー間の SSL ハンドシェークとネゴシエーションが成功した場合、テストは成功します。

  テストが失敗する場合、ディレクトリサーバーは SSL 接続が有効になっていません。

  Microsoft Active Directory を使用する場合は、Active Directory 証明書サービスがインストールされていることを確認します。

- **[Bind to Directory Server]** - このテストは、テストボックスに指定したユーザー名との接続をバインドします。ユーザーを指定しない場合、iLO は匿名バインドを実行します。

  ディレクトリサーバーがバインドを受け付けると、テストは成功します。

  テストが失敗した場合は、以下を実行してください。

  1. ディレクトリサーバーが匿名バインドを許可することを確認します。
  2. テストボックスにユーザー名を入力した場合は、認証情報が正しいことを確認します。
  3. ユーザー名が正しいことを確認した場合は、user@domain.com、DOMAIN\username、username（Active Directory の表示名）、または userlogin のような他のユーザー名フォーマットを使用してみてください。
  4. 指定したユーザーがログインを許可され、有効であることを確認します。

- **[Directory Administrator Login]** - **[Directory Administrator Distinguished Name]** と **[Directory Administrator Password]**を指定した場合、iLO は、これらの値を使用して、管理者としてディレクトリサーバーにログインします。これらのボックスは省略可能です。

- **[UserAuthentication]** - iLO は、指定したユーザー名とパスワードでディレクトリサーバーに認証されます。

  提供したユーザー認証情報が正しい場合、テストは成功します。

  ユーザー名および/またはパスワードが正しくない場合、テストは失敗します。

  テストが失敗した場合は、以下を実行してください。

  1. ユーザー名が正しいことを確認した場合は、user@domain.com、DOMAIN\username、username（Active Directory の表示名）、または userlogin のような他のユーザー名フォーマットを使用してみてください。
  2. 指定したユーザーがログインを許可され、有効であることを確認します。
  3. 指定したユーザー名がログイン時間または IP ベースのログインに制限があるかどうかをチェックします。

- **[User Authorization]** - このテストは、指定したユーザー名が指定したディレクトリグループに属し、ディレクトリサービスの設定中に指定したディレクトリ検索コンテキストに含まれることを確認します。

  テストが失敗した場合は、以下を実行してください。

  1. 指定したユーザー名が指定したディレクトリグループに属することを確認します。
  2. 指定したユーザー名がログイン時間または IP ベースのログインに制限があるかどうかをチェックします。

- **[Directory User Contexts]** - **[Directory Administrator Distinguished Name]**を指定した場合、iLO は、指定したコンテキストを検索しようと試みます。

  iLO が管理者認証情報を使用し、ディレクトリ内のコンテナーを検索してコンテキストを見つけると、テストは成功します。

  「@」で始まるコンテキストは、ユーザーログインによってのみテストできます。

  失敗は、コンテナーが見つからなかったことを示します。

- **[LOM Object Exists]** - このテストは、**[Security]**→**[Directory]**ページで設定された**[LOM Object Distinguished Name]**を使用して、ディレクトリサーバー内の iLO オブジェクトを検索します。

  注記: このテストは、**LDAP** ディレクトリ認証が無効になっていても実行されます。

  ---

  iLO がそれ自体を表現するオブジェクトを見つけると、テストは成功します。

  テストが失敗した場合は、LOM オブジェクトの LDAP FQDN が正しいことを確認してください。

17. 暗号化の設定

製品または高度なセキュリティのセキュリティ状態の有効化

この手順を使用して、iLO がセキュリティ状態として 製品を使用するか高度なセキュリティを使用するかを設定します。FIPS を使用するように iLO を構成するには、FIPS を有効にするを参照してください。FIPS および CNSA セキュリティ状態を使用するように iLO を構成するには、FIPS および CNSA セキュリティ状態を有効にするを参照してください。

CNSA は、iLO 5 Firmware Version 2.10 Oct 30 2019 以降でサポートされます。

> 重要 : **[Security Settings]** 設定を**[HighSecurity]**、**[FIPS]**、または**[CNSA]**モードに設定すると、装置情報収集ユーティリティや ESMPRO/ServerAgentService で装置情報が取得できなくなります。装置に異常が発生した場合にエクスプレス通報サービス等で通報が行えなくなりますので、デフォルトのままご利用ください。

前提条件

iLO の設定を構成権限

手順

1. ナビゲーションツリーで**[Security]**をクリックして、**[Encription]**タブをクリックします。
2. セキュリティ状態メニューで**[Production]**または**[High Security]**を選択します。
3. **[Apply]**をクリックします。
   iLO は、新しい設定を適用するために iLO の再起動を確認するよう要求します。
4. 使用中のブラウザー接続を終了し、iLO を再起動するには、はい、適用してリセットしますをクリックします。
   接続が再確立されるまでに、数分かかることがあります。
5. 開いているブラウザ ウィンドウをすべて閉じます。
   ブラウザーセッションが開いたままになっていると、設定されたセキュリティ状態に誤った暗号が使用される場合があります。
6. オプション：高度なセキュリティセキュリティ状態を有効にした場合は、[**Access Settings**]ページの**[Anonymous Data]**が無効になっていることを確認します。

FIPS および CNSA セキュリティ状態を有効にする

この手順を使用して、iLO が FIPS および CNSA セキュリティ状態を使用するように構成します。iLO が製品または高度なセキュリティのセキュリティ状態を使用するように構成するには、製品または高度なセキュリティのセキュリティ状態の有効化を参照してください。

Common Criteria コンプライアンス、Payment Card Industry コンプライアンス、またはその他の標準には FIPS セキュリティ状態が必要になる場合があります。

FIPS または CNSA セキュリティ状態を有効にした後、ライセンスが期限切れになるか、ライセンスをダウングレードした場合、iLO は構成されてきるセキュリティ状態で引き続き動作しますが、期限切れになったまたはダウングレードしたライセンスによってアクティブ化された他のすべての機能は使用できなくなります。

前提条件

- iLOの設定を構成権限
- オプションの CNSA セキュリティ状態を有効にする予定の場合は、この機能をサポートするライセンスがインストールされていること。
- デフォルトの iLO ユーザー認証情報があること。

手順

1. オプション：iLO バックアップ機能を使用して、iLO の現在の構成をバックアップします。
   詳しくは、「iLO バックアップとリストア」を参照してください。
2. オプション：iLO バックアップ機能を使用して現在の iLO 構成を取得します。
3. オプション：必要に応じてファームウェアおよびソフトウェアのアップデートをインストールします。
4. ナビゲーションツリーで**[Security]**をクリックして、**[Encription]**タブをクリックします。
5. セキュリティ状態メニューで**[FIPS]**を選択し、**[Apply]**をクリックします。

   △ **注意：**FIPS セキュリティ状態を有効にすると iLO が工場出荷時のデフォルト設定にリセットされます。すべての iLO 設定とユーザーデータ、ほとんどの構成設定、ログが消去されます。インストール済みのライセンスキーは保持されます。
   FIPS セキュリティ状態を無効にする唯一の方法は、iLO を工場出荷時のデフォルト設定にリセットすることです。
6. FIPS セキュリティ状態を有効にする要求を確認するためには、**[Yes, appy and reset]**をクリックします。
   接続が再確立されるまでに、数分かかることがあります。
   a. オプション：CNSA セキュリティ状態を有効にします。
   b. デフォルトのユーザー認証情報を使用して iLO にログインします。
   c. ナビゲーションツリーで**[Security]**をクリックして、**[Encription]**タブをクリックします。
   d. セキュリティ状態メニューで**[CNSA]**を選択し、**[Apply]**をクリックします。
   e. iLO が要求を確認するように求めます。
   f. CNSA を有効にする要求を確認するためには、**[Yes, appy and reset]**をクリックします。
      接続が再確立されるまでに、数分かかることがあります。
   g. デフォルトの iLO 認証情報を使用して iLO に再度ログインします。
7. 信頼済みの証明書をインストールします。
   FIPS セキュリティ状態が有効な場合、デフォルトの自己署名 SSL 証明書は許可されません。それまでにインストールされていた信頼済みの証明書は、iLO が FIPS セキュリティ状態を使用するように設定されると、削除されます。
8. **[Access Settings]**ページで**[IPMI/DCMI over LAN]**、**[Anonymous Data]**、および**[SNMP]**オプションを無効にします。

   ⓘ重要: IPMI および SNMP の標準準拠実装など、一部の iLO インターフェースは、FIPS に準拠しておらず、FIPS 準拠にすることはできません。
   構成が FIPS に準拠しているかどうかを確認するには、構成を iLO FIPS 妥当性確認プロセスの一部であったセキュリティポリシードキュメントと照合してください。妥当性確認済

みのセキュリティポリシードキュメントは、NIST Web サイト[39]で入手できます。iLO FIPS 情報は Certificate #3122 の下に表示されます。

9. オプション：iLO リストアを使用して、iLO 構成を復元します。

   詳しくは、「iLO バックアップとリストア」を参照してください。

10. オプション：構成を復元した場合は、ローカル iLO ユーザーアカウントに新しいパスワードを設定します。

    オプション：構成をリストアした場合は、**[Access Settings]**ページで**[IPMI/DCMI over LAN]**、**[Anonymous Data]**、および**[SNMP]**が**[Disabled]**になっていることを確認します。

    これらの設定は、構成を復元するとリセットされる可能性があります。

11. オプション：ログインセキュリティバナーを構成して iLO ユーザーにシステムが FIPS セキュリティ状態を使用していることを知らせます。

高いセキュリティ状態を使用する場合の iLO への接続

デフォルト値よりも高いセキュリティ状態（製品）を有効にすると、iLO は、AES 暗号を使用して安全なチャネルを通じて接続することを要求します。

iLO が CNSA セキュリティ状態を使用するように構成されている場合、AES 256 GCM 暗号が必要です。

Web ブラウザー

ブラウザーが TLS 1.2 および AES 暗号をサポートするよう設定します。ブラウザーが AES 暗号を使用していない場合、iLO に接続できません。

ブラウザーが異なると、ネゴシエーション時の暗号を選択する方法も異なります。詳しくは、ブラウザーのドキュメントを参照してください。

ブラウザーの暗号設定を変更する前に、現在のブラウザーを通じて iLO からログアウトしてください。iLO にログインしている間に行った暗号設定の変更により、ブラウザーで AES 以外の暗号がそのまま使用できる場合があります。

SSH 接続

使用可能な暗号の設定については、SSH クライアントのドキュメントを参照してください。

iLO RESTful API

TLS 1.2 と AES 暗号をサポートするユーティリティを使用します。

[39] https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3122

iLO による FIPS 承認済み環境の構成

以下の手順を使用して、iLO を FIPS 検証済み環境で操作します。FIPS セキュリティ状態を iLO で使用するには、FIPS および CNSA セキュリティ状態を有効にするを参照してください。

重要なのは、FIPS 検証済みバージョンの iLO がご使用の環境に必要かどうか、あるいは iLO を FIPS セキュリティ状態を有効にして実行することで十分かどうかを判断することです。検証プロセスに時間がかかるため、FIPS 検証済みバージョンの iLO が、新機能とセキュリティ強化が加わった非検証バージョンに置き換えられている場合があります。このような状況では、FIPS 検証済みバージョンの iLO が最新バージョンよりも安全性が低くなる場合があります。

手順

FIPS 検証済みバージョンの iLO による環境をセットアップするには、iLO FIPS 承認プロセスの一部であったセキュリティポリシードキュメントの手順に従ってください。

検証済みバージョンの iLO のセキュリティポリシードキュメントは、NIST の Web サイト[40]にあります。

FIPS モードの無効化

手順

1. iLO の FIPS モードを無効にするには（たとえばサーバーを運用停止する場合）、iLO を工場出荷時のデフォルト設定に設定します。

   このタスクを実行するには、iLO RESTful API、または iLO 5 構成ユーティリティを使用します。

   △**注意：**FIPS セキュリティ状態を有効にすると iLO が工場出荷時のデフォルト設定にリセットされます。すべての iLO 設定とユーザーデータ、ほとんどの構成設定、ログが消去されます。インストール済みのライセンスキーは保持されます。FIPS セキュリティ状態を無効にする唯一の方法は、iLO を工場出荷時のデフォルト設定にリセットすることです。

2. サーバーのオペレーティングシステムを再起動します。

   工場出荷時のデフォルト設定へのリセット中に、SMBIOS レコードはクリアされます。メモリおよびネットワーク情報は、サーバーOS の再起動が完了するまで iLO Web インターフェースに表示されません。

[40] https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3122

CNSA モードの無効化

手順

1. CNSA モードを無効にするには、次のいずれかの操作を行います。

   - CNSA モードを無効にして、FIPS セキュリティ状態を引き続き使用するには、セキュリティ状態を CNSA から FIPS に変更します。
   - CNSA モードと FIPS を無効にするには、iLO を工場出荷時のデフォルト設定に設定します。このタスクを実行するには、iLO RESTful API、または iLO 5 構成ユーティリティを使用します。

   △**注意：**iLO を工場出荷時のデフォルト設定にリセットすると、iLO のユーザーデータ、ライセンスデータ、構成設定およびログを含むすべての設定が消去されます。サーバーに工場でインストールされたライセンスキーがある場合、このライセンスキーは保持されます。

   この手順によりログ内のすべてのデータが消去されるため、リセットに関するイベントは iLO イベントログおよびインテグレーテッドマネジメントログに記録されません。

2. iLO を工場出荷時のデフォルト設定にリセットした場合、サーバーのオペレーティングシステムを再起動します。

   工場出荷時のデフォルト設定へのリセット中に、SMBIOS レコードはクリアされます。メモリおよびネットワーク情報は、サーバーOS の再起動が完了するまで iLO Web インターフェースに表示されません。

iLO セキュリティ状態

Producation/本番環境(デフォルト)

このセキュリティ状態に設定されている場合、次のようになります。

- iLO は工場出荷時のデフォルトの暗号化設定を使用します。
- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にします。

High Security/高セキュリティ

iLO がこのセキュリティ状態に設定されている場合、次のようになります。

- iLO は、ブラウザー、SSH ポート、および iLO RESTful API 経由での安全な HTTP 通信において、安全なチャネルを介し AES 暗号を使用します。**[High Security]**が有効になっている場合、サポートされている暗号を使用してこの安全なチャネル経由で iLO に接続する必要があります。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。

- このセキュリティ状態を使用するように iLO が構成されている場合、ホスト OS から実行される iLO RESTful API コマンドに対してユーザー名とパスワード設定が必要になります。
- リモートコンソールデータは、AES-128 双方向暗号化を使用します。
- TLS 1.2 をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にしません。

FIPS

iLO がこのセキュリティ状態に設定されている場合：

- iLO は、FIPS 140-2 レベル 1 の要件への準拠を目的とするモードで動作します。
- FIPS は、米国政府機関および契約業者によって適用を義務付けられている一連のコンピューターセキュリティ規格です。
- FIPS のセキュリティ状態は、FIPS 認証済みと同じではありません。FIPS 認証済みとは、Cryptographic Module Validation Program を完了することにより承認を受けたソフトウェアを意味します。
- 詳しくは、iLO による FIPS 承認済み環境の構成を参照してください。
- iLO は、ブラウザー、SSH ポート、および iLO RESTful API 経由での安全な HTTP 通信において、安全なチャネルを介し AES 暗号を使用します。[High Security]が有効になっている場合、サポートされている暗号を使用してこの安全なチャネル経由で iLO に接続する必要があります。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。
- このセキュリティ状態を使用するように iLO が構成されている場合、ホスト OS から実行される iLO RESTful API コマンドに対してユーザー名とパスワード設定が必要になります。
- リモートコンソールデータは、AES-128 双方向暗号化を使用します。
- TLS 1.2 をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にしません。

CNSA

iLO がこのセキュリティ状態に設定されている場合：
CNSA セキュリティ状態（SuiteB モードとも呼ばれる）は、FIPS セキュリティ状態が有効になっている場合にのみ使用できます。
このセキュリティ状態に設定されている場合、次のようになります。

- iLO は、NSA により定義された CNSA 要件への準拠を目的とするほか、米国政府機密として分類されたデータを保持するために使用するシステムを保護することを目的とするモードで動作します。
- TLS 1.2 をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。

- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にしません。
- iLO への接続に使用するソフトウェアまたはユーティリティはすべて、CNSA に準拠している必要があります。
  以下に例を示します。
  - ファームウェアアップデートユーティリティ
  - SSH クライアント
  - スクリプティングツールとコマンドラインツール
  - 管理ツール
  - アラートメール、syslog、LDAP、またはキーマネージャーサーバー
- 準拠を確認するには、ソフトウェアのベンダーに確認するか、Wireshark などのユーティリティを使用します。

SSH 暗号、キー交換、および MAC のサポート

iLO は、安全な CLP トランザクションのために、SSH ポート経由の強化された暗号化を提供します。

設定されているセキュリティ状態に基づいて、iLO は以下をサポートします。

Production(本番環境)

- AES256-CBC、AES128-CBC、3DES-CBC、および AES256-CTR 暗号
- diffie-hellman-group14-sha1 および diffie-hellman-group1-sha1 キー交換
- hmac-sha1 または hmac-sha2-256 MAC

FIPS または High Security(高セキュリティ)

- AES256-CTR、AEAD_AES_256_GCM、および AES256-GCM 暗号
- diffie-hellman-group14-sha1 キー交換
- hmac-sha2-256 または AEAD_AES_256_GCM MAC

SSL 暗号および MAC のサポート

iLO は、分散型 IT 環境でのリモート管理用に強化されたセキュリティを提供します。SSL 暗号化により、Web ブラウザーのデータが保護されます。SSL で提供される HTTP データの暗号化により、データがネットワーク経由で転送されるときのデータの安全性が保証されます。

ブラウザーから iLO にログインすると、ブラウザーと iLO は、使用する暗号設定をネゴシエートします。ネゴシエートされた暗号は暗号化ページに表示されます。

サポートされている暗号の次の一覧は、LDAP サーバー、SSO サーバー、仮想メディアで使用される https:// URL、iLO RESTful API、CLI コマンド、iLO 連携グループのファームウェアアップデートへの接続など、すべての iLO SSL 接続に適用されます。

構成されているセキュリティ状態に基づいて、iLO は以下の暗号をサポートします。

Production(本番環境)

- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、ECDH、および SHA384 MAC（ECDHE-RSA AES256-SHA384）による 256 ビット AES
- RSA、ECDH、および SHA1 MAC（ECDHE-RSA-AES256-SHA）による 256 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA AES256-SHA256）による 256 ビット AES
- RSA、DH、および SHA1 MAC（DHE-RSA-AES256-SHA）による 256 ビット AES
- RSA および AEAD MAC（AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA および SHA256 MAC（AES256-SHA256）による 256 ビット AES
- RSA および SHA1 MAC（AES256-SHA）による 256 ビット AES
- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、ECDH、および SHA256 MAC（ECDHE-RSA-AES128-SHA256）による 128 ビット AES
- RSA、ECDH、および SHA1 MAC（ECDHE-RSA-AES128-SHA）による 128 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA-AES128-SHA256）による 128 ビット AES
- RSA、DH、および SHA1 MAC（DHE-RSA-AES128-SHA）による 128 ビット AES
- RSA および AEAD MAC（AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、および SHA256 MAC（AES128-SHA256）による 128 ビット AES
- RSA および SHA1 MAC（AES128-SHA）による 128 ビット AES
- RSA、ECDH、および SHA1 MAC（ECDHE-RSA-DES-CBC3-SHA）による 168 ビット 3DES
- RSA、DH、および SHA1 MAC（EDH-RSA-DES-CBC3-SHA）による 168 ビット 3DES
- RSA および SHA1 MAC（DES-CBC3-SHA）による 168 ビット 3DES

FIPS または高いセキュリティ

これらのセキュリティ状態には TLS 1.2 が必要です。

- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、ECDH、および SHA384 MAC（ECDHE-RSA AES256-SHA384）による 256 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA AES256-SHA256）による 256 ビット AES
- RSA および AEAD MAC（AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA および SHA256 MAC（AES256-SHA256）による 256 ビット AES
- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、ECDH、および SHA256 MAC（ECDHE-RSA-AES128-SHA256）による 128 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA-AES128-SHA256）による 128 ビット AES

- RSA および AEAD MAC（AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、および SHA256 MAC（AES128-SHA256）による 128 ビット AES

CNSA

このセキュリティ状態には TLS 1.2 が必要です。

- ECDSA、ECDH、および AEAD MAC（ECDHE-ECDSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- クライアントのみ：RSA、ECDH、および AEAD MAC（ECDHE_RSA_AES256_GCM_SHA384）による 256 ビット AES-GCM

暗号化強制設定の表示

手順

[Security]→[Encryption]ページに移動します。

iLO の現在の暗号化設定を示す **[Encryption Settings]**ページが表示されます。

- **[Current Negotiated Cipher]** - 現在のブラウザーセッションで使用されている暗号。ブラウザーから iLO にログインすると、ブラウザーと iLO は、セッション中に使用する暗号設定を交渉します。
- **[Security Settings]** - iLO の現在の暗号化設定。
  - **[Production]**（デフォルト）- この iLO システムで Production モードが有効かどうかを示します。
  - **[HighSecurity]** - この iLO システムで HighSecurity モードが有効かどうかを示します。
  - **[FIPS]** - この iLO システムで FIPS モードが有効かどうかを示します。

NEC SSO の使用

NEC SSO(シングル・サイン・オン)を使用すると、NEC SSO 対応アプリケーションから、ログイン手順を間に挟むことなく iLO に直接接続できます。この機能を使用するには、最新の ESMPRO/ServerManager が必要です。また、iLO プロセッサーを NEC SSO 対応アプリケーションを信頼するように設定する必要があります。詳しくは、ESMPRO/ServerManager の「セットアップガイド」を参照してください。

ログインセキュリティバナーの設定

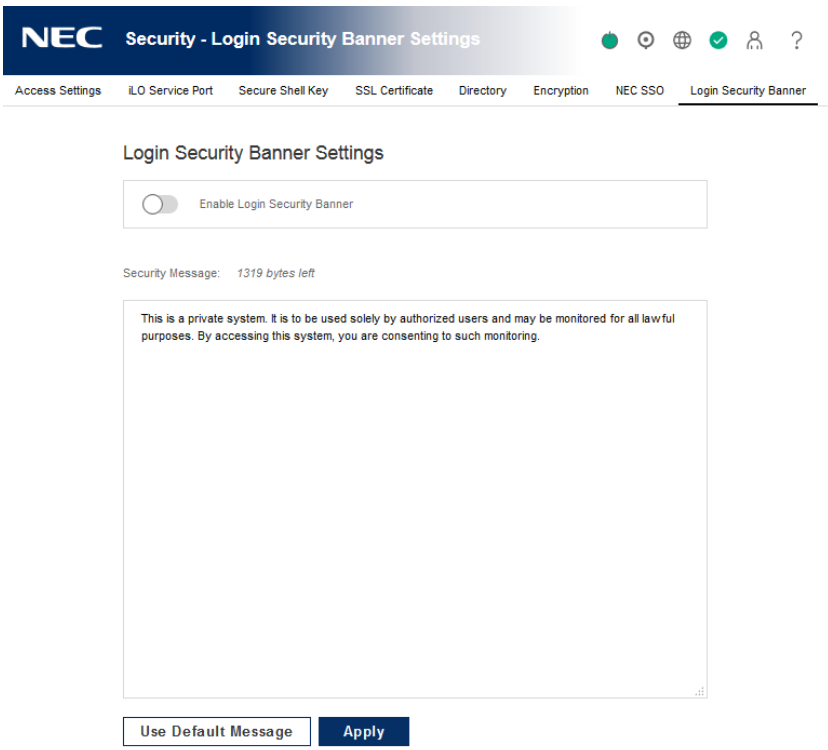
ログインセキュリティバナー機能を使用すると、iLO ログインページに表示されるセキュリティバナーを設定できます。たとえば、システムが FIPS モードに入っていることを示すメッセージを入力できます。

前提条件

iLO の設定を構成権限

手順

1. **[Security]→[Login Security Banner]**ページに移動します。



2. **[Enable Login Security Banner]**トグルボタンを有効にします。

   iLO は、ログインセキュリティバナーに次のデフォルトテキストを使用します。

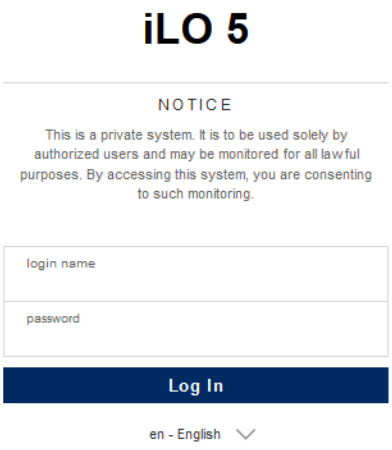
   This is a private system. It is to be used solely by authorized users and may be monitored for all lawful purposes. By accessing this system, you are consenting to such monitoring.

3. オプション：セキュリティメッセージをカスタマイズするには、**[Security Message]**テキストボックスにカスタムメッセージを入力します。

テキストボックスの上にあるバイトカウンターに、メッセージに使用できる残りのバイト数が表示されます。最大は 1,500 バイトです。

ヒント: **[Use Default Message]**をクリックして、デフォルトのテキストを復元します。

4. [Apply]をクリックします。
   次のログイン時にセキュリティメッセージが表示されます。



18. iLO マネージメント設定の構成

Agentless Management と AMS

Agentless Management は、セキュリティと安定性を強化するためにアウトバンド通信を使用します。Agentless Management では、サーバー状態監視とアラート通知機能がシステムに内蔵され、サーバーに電源コードを接続するとただちに動作を開始します。この機能は iLO ハードウェアで動作し、オペレーティングシステムやプロセッサーに依存しません。追加のオペレーティングシステムデータが、AMS のインストール時に収集されます。

AMS がインストールされていない場合：

- iLO では、**[System Information]**ページにすべてのデータは表示されません。
- iLO では、正しいサーバー名が表示されない場合があります。

表 3 Agentless Management（AMS がない場合）と（AMS がある場合）に提供する情報

コンポーネント	Agentless Management （AMS がない場合）	Agentless Management （AMS がある場合）
サーバー	• ファン • 温度 • パワーサプライ • メモリ • CPU	• ファン • 温度 • パワーサプライ • メモリ • CPU
ストレージ	• Smart アレイ • SMART ドライブ監視(Smart アレイに接続) • Smart アレイに接続されている内蔵および外付けドライブ • Smart Storage バッテリー監視(サポート対象のサーバーのみ)	• Smart アレイ • SMART ドライブ監視(Smart アレイ、Smart ホストバスアダプターおよび AHCI に接続) • Smart アレイに接続されている内蔵および外付けドライブ • Smart Storage バッテリー監視(サポート対象のサーバーのみ) • iSCSI (Windows) • NVMe ドライブ
ネットワーク	• 内蔵 NIC の MAC アドレス • 対応する NIC の物理リンク接続およびリンクアップ/リンクダウントラップ	• 独立型および内蔵 NIC の MAC アドレスおよび IP アドレス • リンクアップダウントラップ • NIC チーミングおよびブリッジ情報(Windows および Linux) • サポートされるファイバーチャネルアダプター • VLAN 情報(Windows および Linux)

その他	• iLO データ • ファームウェアインベントリ • デバイスインベントリ	• iLO データ • ファームウェアインベントリ • デバイスインベントリ • OS 情報(ホスト SNMP MIB) [1] • ドライバー/サービスインベントリ • OS ログへのイベントの追加 [2]
障害予兆アラート	• メモリ • ドライブ(物理および論理)	• メモリ • ドライブ(物理および論理)

[1] Agentless Management によって供給されるデータは、SNMP エージェントによって供給されるデータほど包括的なものではありません。

[2] Smart アレイのログ記録をサポートします。

SNMP の設定

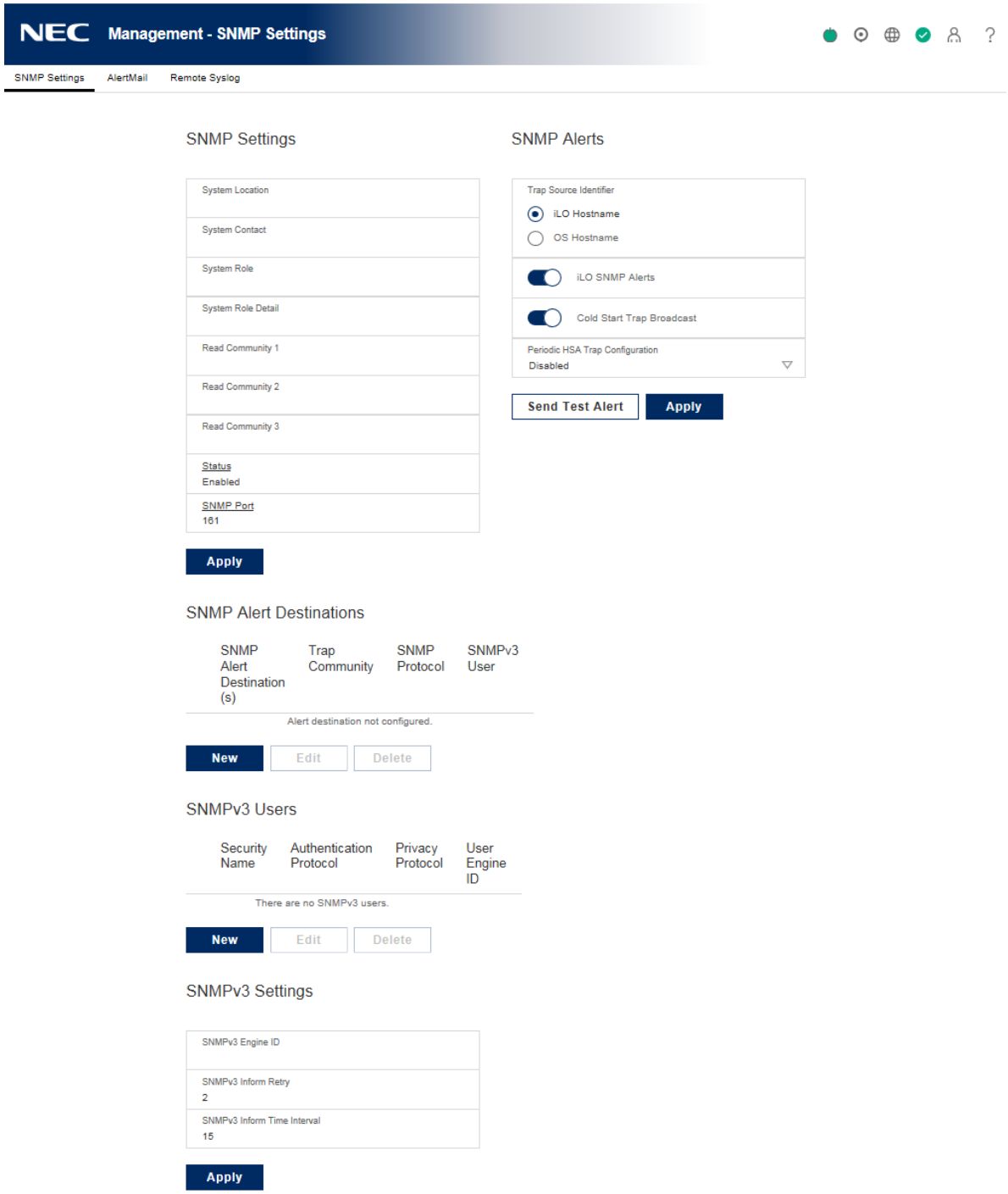
ここでは、iLO Firmware Version 1.20 Feb 02 2018 の SNMP 機能について説明します。古いバージョンの iLO Firmware を使用している場合は、iLO の Web インターフェースを開き、オンラインヘルプの記載をご確認ください。

前提条件

iLO の設定を構成権限

手順

1. **[Management]**ページに移動します。
2. **[SNMP Settings]**タブをクリックします。



3. **[SNMP Settings]**セクションで、次の値を入力します。
   - **[System Location]** - サーバーの物理的位置を指定する最大 49 文字の文字列。先頭に空白文字は使用せず、<>括弧で囲わないでください。
   - **[System Contact]** - システム管理者またはサーバーの所有者を指定する最大 49 文字の文字列。先頭に空白文字は使用せず、<>括弧で囲わないでください。文字列には、名前、Email アドレス、または電話番号を含めることができます。
   - **[System Role]** - サーバーの役割または機能を記述する最大 64 文字の文字列。先頭に空白文字は使用せず、<>括弧で囲わないでください。

- **[System Role Detail]** - サーバーが実行する場合がある具体的なタスクを記述する最大 512 文字の文字列。先頭に空白文字は使用せず、<>括弧で囲わないでください。
- **[Read Community]** - 設定されている SNMP 読み取り専用コミュニティ名(SNMP マネージャと iLO 間での Get Request 要求/応答のための認証キー)。先頭に空白文字は使用せず、<>括弧で囲わないでください。

  [Read Community]は、以下のフォーマットをサポートします。
  - コミュニティ名（たとえば、public）。
  - コミュニティ名とそれに続く IP アドレスまたは FQDN（たとえば、public192.168.0.1）。
    指定した IP アドレスまたは FQDN からの SNMP アクセスが許可されることを指定するには、このオプションを使用します。IPv4 アドレス、IPv6 アドレス、または FQDN を入力できます。
- **[SNMP Port]** - SNMP 通信に使用するポート。ここに表示されている値は読み取り専用ですが、**[Security]**→**[Access Settings]**ページで変更できます。
  [SNMP Port]リンクをクリックすると**[Security]**→**[Access Settings]**ページに移動します。詳しくは、「iLO アクセスの設定」を参照してください。

4. **[適用]**をクリックして設定を保存します。

SNMPv3 認証

SNMPv3 の次のセキュリティ機能によって、SNMP エージェントから安全にデータ収集できます。

- メッセージの整合性により、パケット送信中の改ざんを防ぎます。
- 暗号化により、パケットののぞき見を防ぎます。
- 認証により、パケットが有効なソースから送信されたものであることを確認します。デフォルトでは、SNMPv3 はユーザーベースのセキュリティモデルをサポートします。このモデルでは、セキュリティパラメーターがエージェントレベルとマネージャーレベルの両方で設定されます。エージェントとマネージャーの間でやり取りされるメッセージは、データ整合性チェックおよびデータ発信元認証で管理されます。

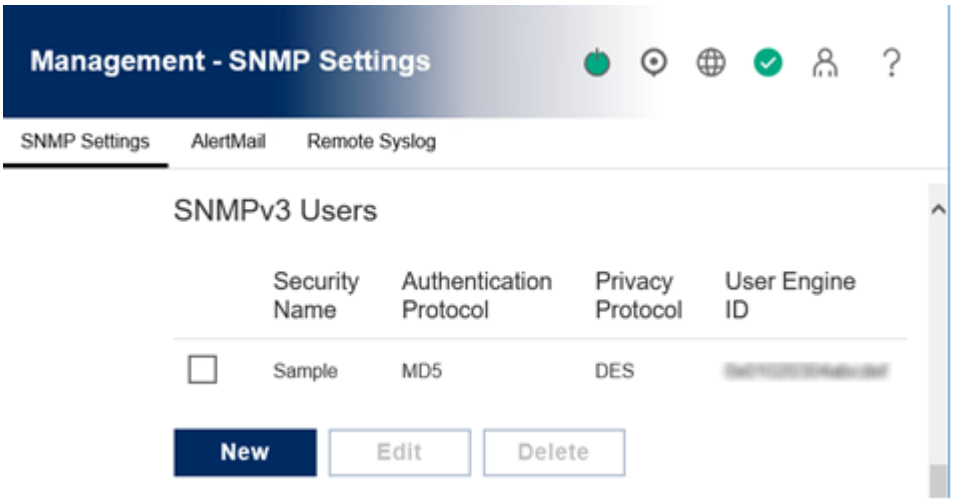
iLO は、3 つのユーザープロファイルをサポートしており、ユーザーはこのプロファイル内で SNMPv3 USM パラメーターを設定できます。

SNMPv3 ユーザーの設定

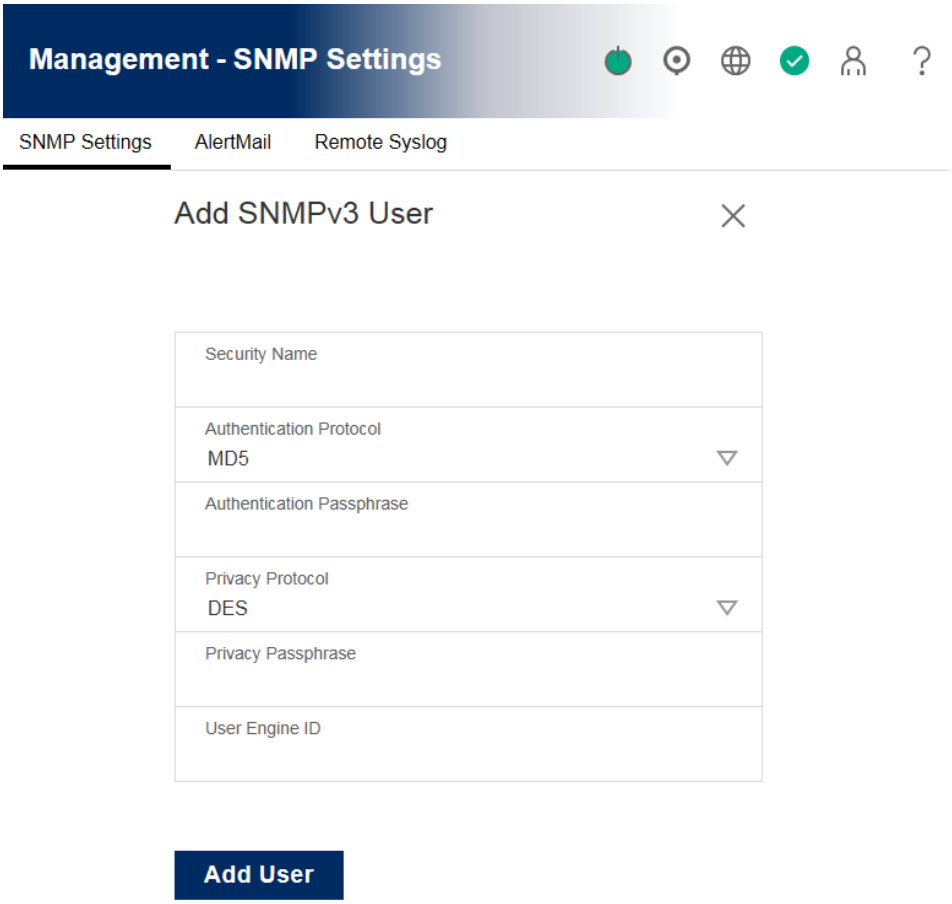
前提条件
iLO の設定を構成権限

手順

1. **[Management]**ページに移動します。
2. **[SNMP Settings]**タブをクリックし、ページをスクロールして **[SNMPv3 Users]**セクションに移動します。



3. 新規に SNMPv3 ユーザーを作成する場合は**[New]**を、既存のユーザーの設定を変更する場合はユーザープロファイルを選択して**[Edit]**をクリックします。SNMPv3 ユーザーオプションが表示されます。



4. 次の情報を入力します。

   - **[Security Name]** - ユーザープロファイルの名前。1～32 文字の範囲で英数字の文字列を入力します。
   - **[Authentication Protocol]** - 認証パスフレーズのエンコーディングに使用するメッセージダイジェストアルゴリズムを設定します。メッセージダイジェストは SNMP メッセー

ジの該当部分を対象に算出され、受信者に送信するメッセージの一部として、メッセージに含まれます。**[MD5]** または **[SHA]** を選択します。デフォルト設定は**[MD5]**です。FIPS または CNSA セキュリティ状態を使用するよう iLO を構成すると、MD5 がサポートされません。

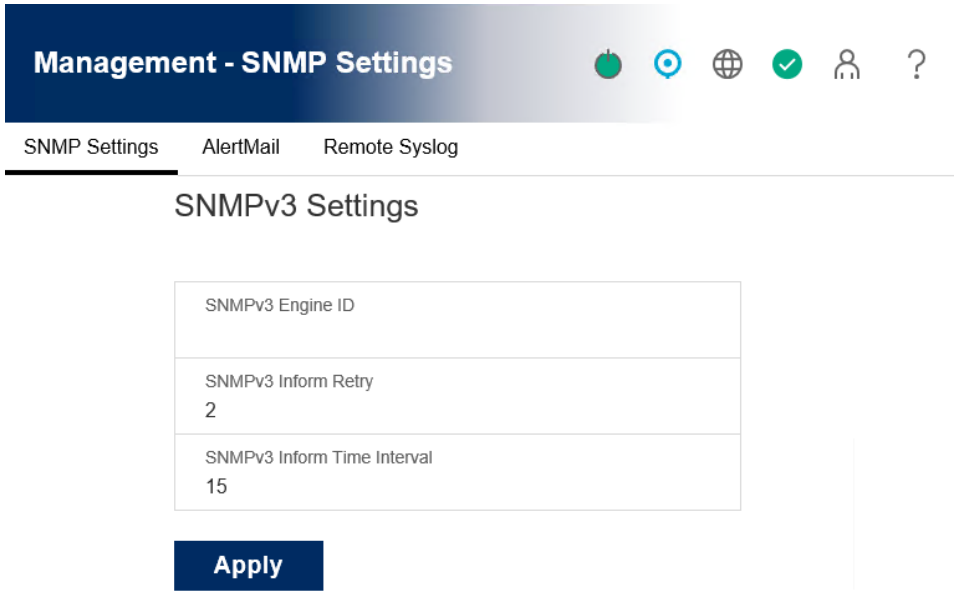
- **[Authentication Passphrase]** - 署名操作に使用するパスフレーズを設定します。8〜49 文字の範囲で値を入力します。“(ダブルクオーテーション)および空白文字は使用せず、<>括弧で囲わないでください。
  FIPS または CNSA セキュリティ状態を使用するよう iLO を構成すると、MD5 がサポートされません。
- **[Privacy Protocol]** - プライバシーパスフレーズのエンコーディングに使用する暗号化アルゴリズムを設定します。SNMP メッセージの一部は、送信前に暗号化されます。**[AES]** または **[DES]** を選択します。デフォルト設定は**[DES]**です。
- **[Privacy Passphrase]** - 暗号化操作に使用するパスフレーズを設定します。8〜49 文字の範囲で値を入力します。 “(ダブルクオーテーション)および空白文字は使用せず、<>括弧で囲わないでください。
- **[User Engine ID]** - ユーザーエンジン ID を設定します。この値は SNMPv3 Inform パケットの送信に使用されます。ユーザーエンジン ID が設定されていない場合、INFORM メッセージの送信には SNMPv3 エンジン ID が使用されます。

5. **[Add User]**または**[Update User]**をクリックして、ユーザープロファイルを保存します。
6. 変更した SNMPv3 ユーザー設定が画面に反映されない場合は、**[SNMP Settings]**ページを再読み込みしてください。

SNMPv3 の設定

前提条件
iLO の設定を構成権限

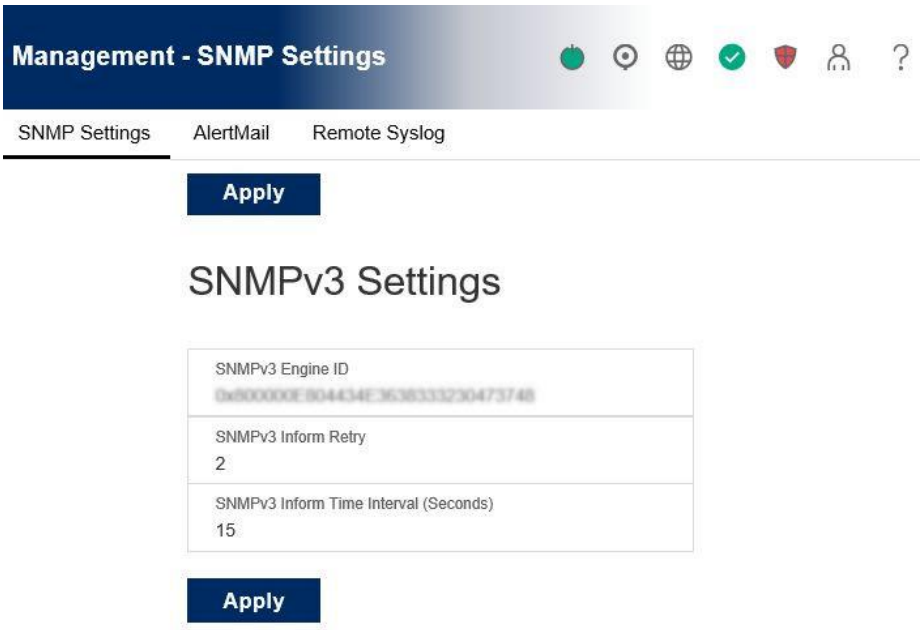
- iLO 5 Firmware Version 1.40 Feb 05 2018 以前



手順

1. **[Management]**ページに移動します。
2. **[SNMP Settings]**タブをクリックし、ページをスクロールして **[SNMPv3 Settings]**セクションに移動します。

- iLO 5 Firmware Version 1.43 May 23 2019 以降



手順

1. **[SNMPv3 Engine ID]** ボックスに値を入力します。

   この値は 6～32 文字で構成される 16 進数文字列で、文字数は先頭の 0x を除いて偶数でなければなりません（例：0x01020304abcdef）。

   iLO 5 Firmware Version 1.40 Feb 05 2018 以前ではデフォルトは空白ですが、iLO 5 Firmware Version 1.43 May 23 2019 以降では、iLO の再起動後にデフォルトの**[SNMPv3 Engine ID]**が自動生成されて設定されます。

2. **[SNMPv3 Inform Retry]** Ack を受信できなかった場合に、iLO がアラートを再送信する回数を設定します。0～5 の値を入力します。デフォルト設定は 2 です。

3. **[SNMPv3 Inform Time Interval]** アラートを再送する間隔を秒単位で設定します。5(秒)～120(秒)の値を入力します。デフォルト設定は 15（秒）です。

4. **[Apply]**をクリックします。

> △**注意:**
>
> SNMP マネージャーにより SNMPv3 プロトコルで SNMP 管理する際は SNMP エンジンを識別するためのユーニークな数値を**[SNMPv3 Engine ID]**を設定する必要があります。

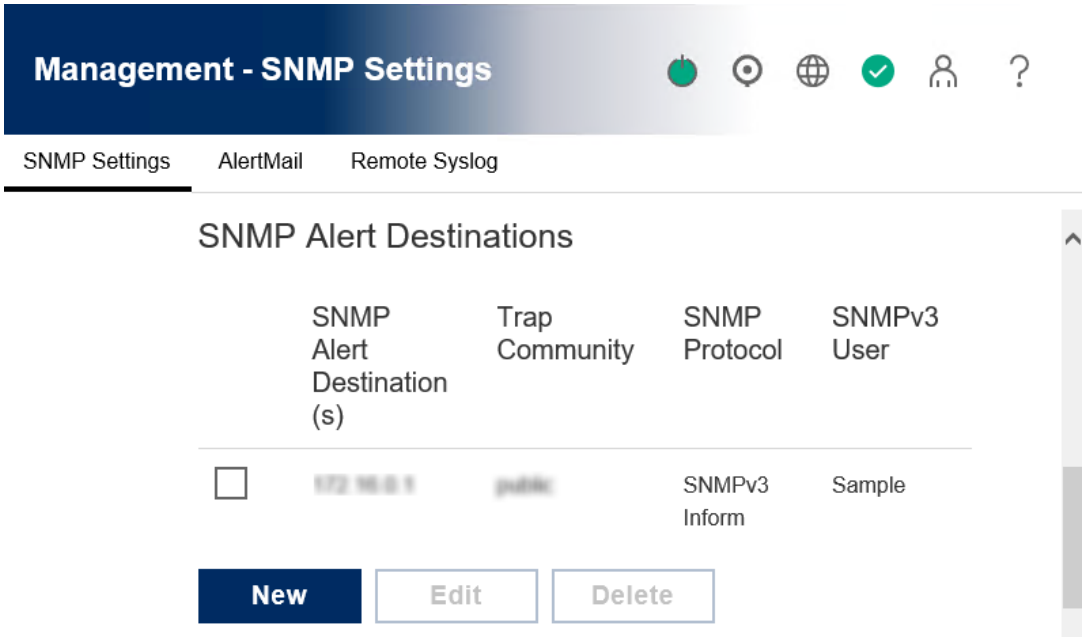
SNMP アラート送信先の設定

前提条件

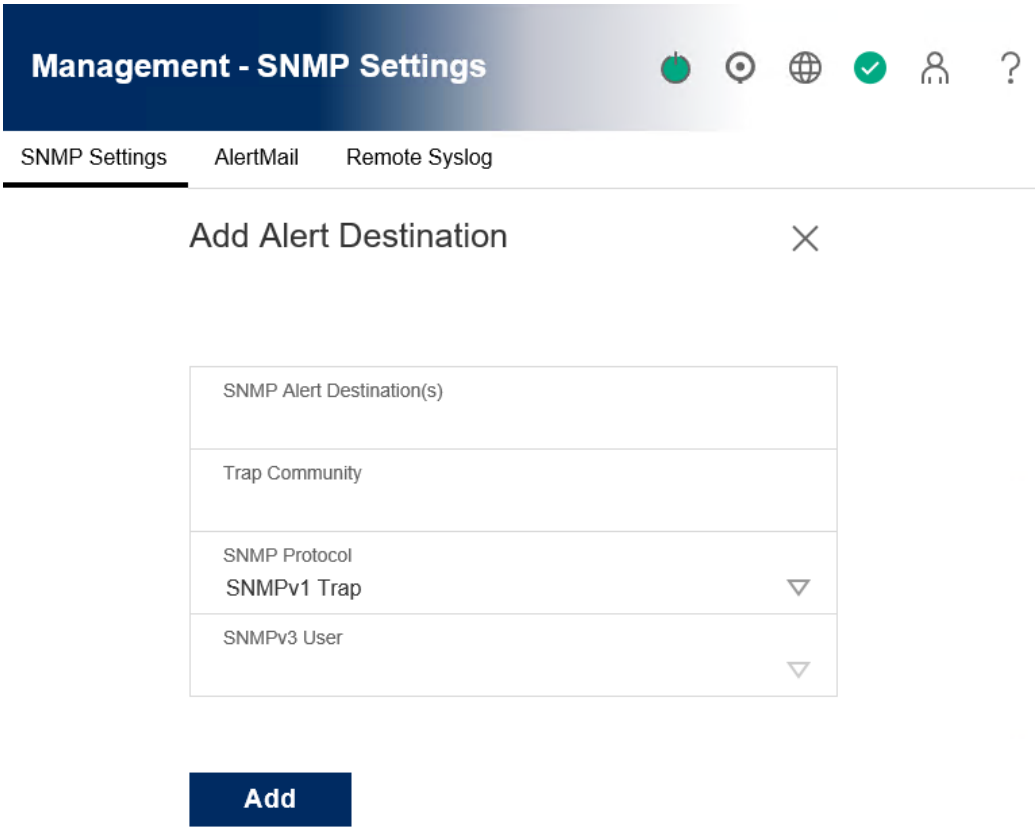
- iLO の設定を構成権限
- SNMPv3 Trap、SNMPv3 Inform を送信する場合は、事前に SNMPv3 ユーザーの設定が必要です。

手順

1. **[Management]**ページに移動します。
2. **[SNMP Settings]**タブをクリックし、ページをスクロールして **[SNMP Alert Destinations]**セクションに移動します。



3. 新規にアラート送信先を追加する場合は**[New]**を、既存の送信先を変更する場合は送信先を選択して**[Edit]**をクリックします。



4. 次の情報を入力します。
   - **[SNMP Alert Destination(s)]** - SNMP アラートの送信先アドレスを IP アドレスまたは FQDN で設定します。
   - **[Trap Community]** - SNMP Trap 用コミュニティ名(iLO から発行された SNMP を SNMP マネージャ側で受信するための認証キー)を設定します。
   - **[SNMP Protocol]** - SNMP アラートのプロトコルを設定します。**[SNMPv1 Trap]**、**[SNMPv3 Trap]**、**[SNMPv3 Inform]**から選択してください。SNMPv3 ユーザーが登録されていない場合は、**[SNMPv1 Trap]**だけが選択可能です。**[SNMPv3 Trap]**、**[SNMPv3 Inform]**を選択する場合は、事前に SNMPv3 ユーザーの登録を行ってください。デフォルト設定は**[SNMPv1 Trap]**です。
   - **[SNMPv3 User]** - SNMP アラートの送信用の SNMPv3 ユーザーを設定します。**[SNMP Protocol]**設定で**[SNMPv3 Trap]**または**[SNMPv3 Inform]**を選択した場合に設定が必要になります。登録した SNMPv3 ユーザーが選択肢として表示されます。
5. **[Add]**または**[Update]**をクリックして、送信先設定を保存します。
6. 変更した送信先設定が画面に反映されない場合は、**[SNMP Settings]**ページを再読み込みしてください。

SNMPv3 ユーザーまたは SNMP アラート送信先の削除

前提条件

SNMPv3 ユーザーまたは SNMP アラート送信先を削除するには、iLO の設定を構成権限。が必要です。

手順

1. **[Management]**ページに移動します。
2. 削除する SNMPv3 ユーザーまたは SNMP アラート送信先の横にあるチェックボックスを選択します。
3. **[Delete]** をクリックします。
   ポップアップウィンドウが開き、確認メッセージが表示されます。
4. **[Yes, delete]** をクリックします。

SNMP アラートの設定

トラップソース識別子、iLO SNMPv1 アラート、コールドスタートトラップブロードキャスト、および SNMP トラップを設定できます。

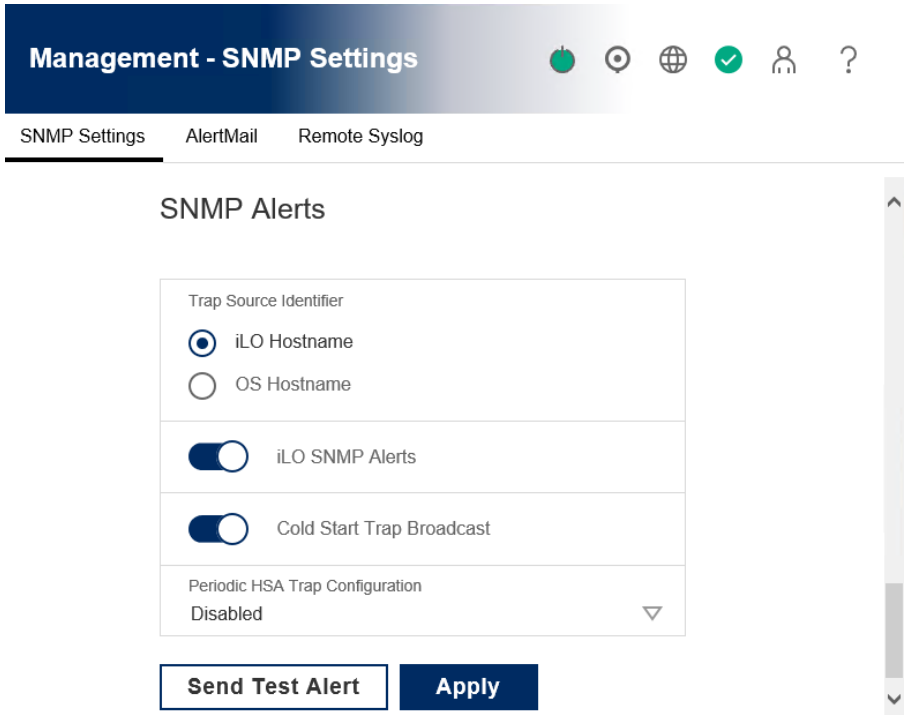
前提条件

iLO の設定を構成権限

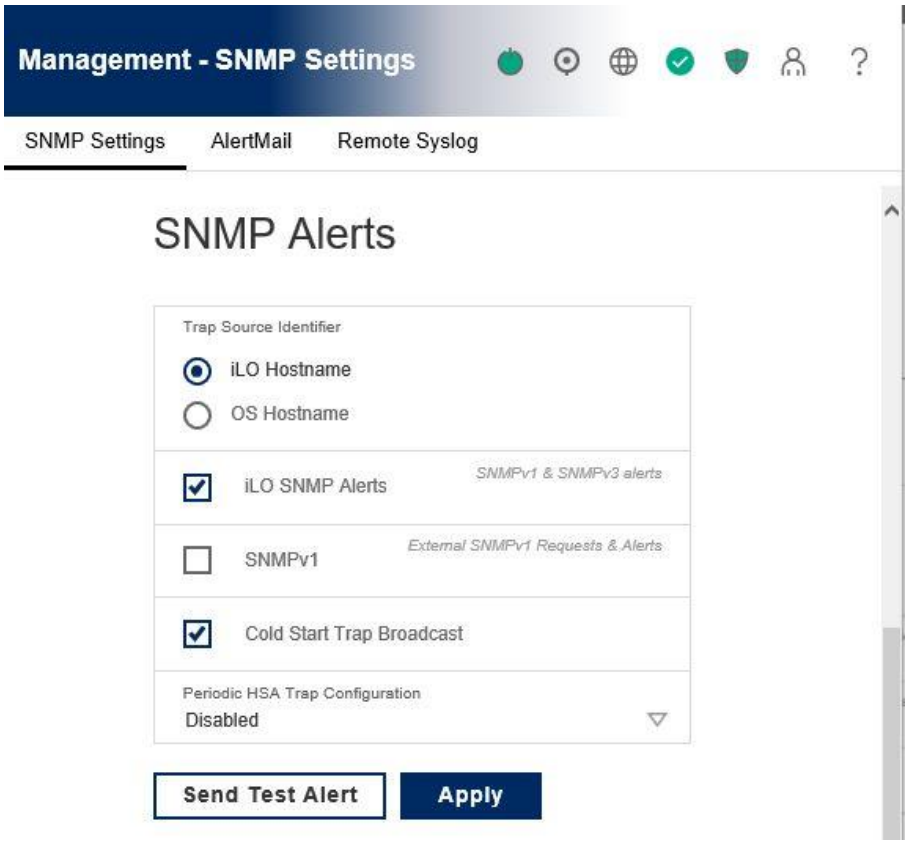
手順

1. **[Management]**ページに移動します。
2. **[SNMP Settings]**タブをクリックし、ページをスクロールして**[SNMP Alerts]**セクションに移動します。

- iLO 5 Firmware Version 2.18 Jun 22 2020 以前



- iLO 5 Firmware Version 2.31 Oct 13 2020



3. **[Trap Source Identifier]**設定に**[iLO Hostname]**または**[OS Hostname]**を選択して設定します。この設定は、iLO が SNMP トラップを生成するときに SNMP で定義された**[sysName]**変数に使用されるホスト名を決定します。デフォルト設定は、**[iLO Hostname]**です。

注記:ホスト名は OS の構成要素であり、ハードディスクドライブが新しいサーバープラットフォームに移動される場合など、サーバーに固定されているわけではありません。
ただし、iLO の**[sysName]**は、マザーボードに固定されています。

---

4. 次のアラートタイプを有効または無効にします。
   - **[iLO SNMP Alert]** - ホストオペレーティングシステムに依存せずに iLO によって検出されるアラート状態は、指定された SNMP アラート送信先（ESMPRO/ServerManager など）に送信できます。このオプションが無効になっている場合、トラップは構成された SNMP アラート送信先に送信されません。デフォルト設定は有効です。
   - **[SNMPv1]** - iLO における、外部 SNMPv1 要求の受信と、読み取りコミュニティ 1、読み取りコミュニティ 2、読み取りコミュニティ 3 の各ボックスで構成されたリモート管理システムへの SNMPv1 トラップの送信を有効にします。この設定は、デフォルトでは無効になっています。

     △**注意:**
     iLO 5 Firmware Version 2.31 Oct 13 2020 以降でサポートされている機能です。

- **[Cold Start Trap Broadcast]** - このオプションが有効になっている場合、有効なトラップ送信先が設定されていないと、コールドスタートトラップはサブネットブロードキャストアドレスにブロードキャストされます。
  次の条件のいずれかを満たす場合、コールドスタートトラップはブロードキャストされます。
  - **[SNMP Alert Destination(s)]**が設定されていない。
  - iLO が一部の**[SNMP Alert Destination(s)]**を IP アドレスに解決できなかった。

  IPv4 ホストのサブネットブロードキャストアドレスは、サブネットマスクとホスト IP アドレスのビット成分間のビット論理 OR 演算を実行することで取得されます。たとえば、サブネットマスクが 255.255.252.0 のホスト 192.168.1.1 のブロードキャストアドレスは、192.168.1.1 | 0.0.3.255 = 192.168.3.255 になります。

  デフォルト設定は有効です。

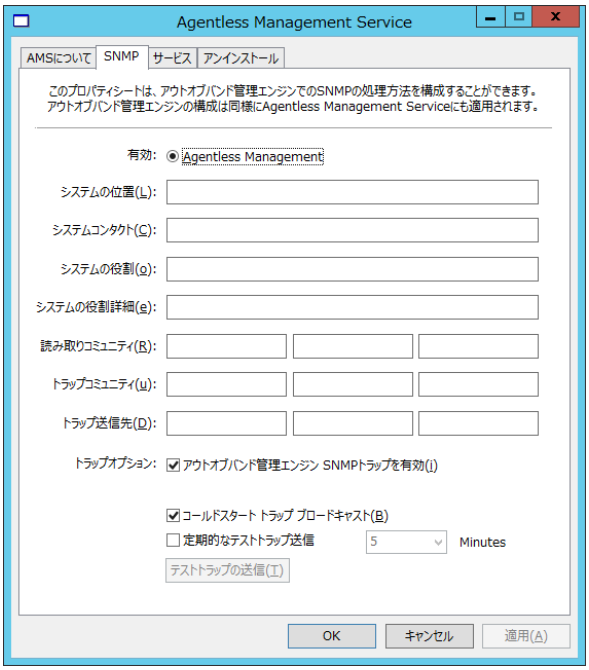
- **[Periodic HSA Trap Configuration]** - このオプションが有効になっている場合、iLO はコンポーネントが Failed または Degraded ステータスになっている間、Health Status Array (HSA) Trap を定期的に送信します。送信間隔は、毎日、毎週、毎月から選択できます。このオプションが無効になっている場合、iLO はコンポーネントのステータスが変化した時にだけ Health Status Array (HSA) Trap を送信します。**[Disabled]**、**[Daily]**、**[Weekly]**、**[Monthly]**から設定を選択してください。デフォルト設定は無効です。

5. オプション：**[Send Test Alert]**をクリックしてテストアラートを生成し、**[SNMP Alert Destination(s)**ボックス内の TCP/IP アドレスに送信します。
   iLO の設定権限を持つユーザーだけが、テストアラートを送信できます。
   アラートを生成すると確認メッセージが表示されます。ESMPRO/ServerManager のアラートビューアなどで、アラートの受信を確認します。
6. **[Apply]**をクリックして設定を保存します。

AMS コントロールパネルを使用した SNMP および SNMP アラートの設定（Windows 専用）

手順

1. コントロールパネルで Agentless Management を開きます。
2. **[SNMP]**タブをクリックします。



3. SNMP 設定を更新します。

   使用できる設定の説明については、「SNMP の設定」および「SNMP アラートの設定」を参照してください。SNMPv3 の設定は行えません。SNMPv3 をご使用になる場合は、iLO Web インターフェースから設定を行うようにしてください。

4. オプション：**[テストトラップの送信]**をクリックしてテストアラートを生成し、**[トラップ送信先]**ボックス内の TCP/IP アドレスに送信します。

   送信後、ESMPRO/ServerManager のアラートビューアなどで、アラートの受信を確認します。

5. **[適用]**をクリックして設定を保存します。

SNMP トラップ

表 4 に、iLO で生成できる SNMP トラップを示します。これらの SNMP トラップについて詳しくは、MIB 更新キットに含まれている以下のファイルを参照してください。

- cpqida.mib
- cpqhost.mib
- cpqhlth.mib
- cpqsm2.mib
- cpqide.mib
- cpqscsi.mib
- cpqnic.mib
- cpqstsys.mib
- cpqstdeq.mib

表 4 SNMP トラップ

トラップ番号	SNMP トラップ名	説明
0	Cold Start Trap	SNMP が初期化され、システムで POST が完了した、または AMS が起動しました。
4	Authentication Failure Trap	SNMP が認証失敗を検出しました。
1006	cpqSeCpuStatusChange	訂正不可能なマシンチェック例外がプロセッサーで検出されました。
1010	cpqSeUSBStorageDeviceReadErrorOccurred	接続されている USB ストレージデバイスで読み取りエラーが発生しました。
1011	cpqSeUSBStorageDeviceWriteErrorOccurred	接続されている USB ストレージデバイスで書き込みエラーが発生しました。
1012	cpqSeUSBStorageDeviceRedundancyLost	接続されている USB ストレージデバイスで書き込みエラーが発生しました。
1013	cpqSeUSBStorageDeviceRedundancyRestored	USB ストレージデバイスの冗長性が回復しました。
1014	cpqSeUSBStorageDeviceSyncFailed	USB ストレージデバイスの冗長性を回復するための同期操作に失敗しました。
2014	cpqSiIntrusionInstalled	システムイントリュージョンハードウェアがインストールされました。
2015	cpqSiIntrusionRemoved	システムイントリュージョンハードウェアが削除されました。
2016	cpqSiHoodReplaced	システムフードが交換されました。
2017	cpqSiHoodRemovedOnPowerOff	サーバーの電源が切れたときにシステムフードが取り外されました。

Table Continued

トラップ番号	SNMP トラップ名	説明
3033	cpqDa6CntlrStatusChange	Smart アレイコントローラーのステータスの変化が検出されました。
3034	cpqDa6LogDrvStatusChange	Smart アレイ論理ドライブのステータスの変化が検出されました。
3038	cpqDa6AccelStatusChange	Smart アレイキャッシュモジュールのステータスの変化が検出されました。
3039	cpqDa6AccelBadDataTrap	Smart アレイキャッシュモジュールのバックアップ電源が失われました。
3040	cpqDa6AccelBatteryFailed	Smart アレイキャッシュモジュールのバックアップ電源が故障しました。
3046	cpqDa7PhyDrvStatusChange	Smart アレイ物理ドライブのステータスの変化が検出されました。
3047	cpqDa7SpareStatusChange	Smart アレイスペアドライブのステータスの変化が検出されました。
3049	cpqDaPhyDrvSSDWearStatusChange	Smart アレイ物理ドライブの SSD 消耗ステータスの変化が検出されました。
6026	cpqHe3ThermalConfirmation	温度上昇のためにサーバーがシャットダウンされましたが、現在は稼動しています。
6027	cpqHe3PostError	1 つまたは複数の POST エラーが発生しました。
6032	cpqHe3FltTolPowerRedundancyLost	指定されたシャーシの冗長パワーサプライの冗長性が失われました。
6033	cpqHe3FltTolPowerSupplyInserted	冗長パワーサプライが取り付けられました。
6034	cpqHe3FltTolPowerSupplyRemoved	冗長パワーサプライが取り外されました。
6035	cpqHe3FltTolFanDegraded	冗長ファン状態が、[劣化]に変化しました。
6036	cpqHe3FltTolFanFailed	冗長ファン状態が、[障害]に変化しました。
6037	cpqHe3FltTolFanRedundancyLost	冗長ファンの冗長性が失われました。
6038	cpqHe3FltTolFanInserted	冗長ファンが取り付けられました。
6039	cpqHe3FltTolFanRemoved	冗長ファンが取り外されました。
6040	cpqHe3TemperatureFailed	サーバー上で温度が超過しました。
6041	cpqHe3TemperatureDegraded	温度ステータスが [劣化]に変化し、温度が正常な動作範囲にありません。システム構成によっては、このシステムがシャットダウンされる可能性があります。

Table Continued

トラップ番号	SNMP トラップ名	説明
6042	cpqHe3TemperatureOk	温度ステータスが、**[OK]** に変化しました。
6048	cpqHe4FltTolPowerSupplyOk	フォールトトレラントパワーサプライ状態が、**[OK]** にリセットされました。
6049	cpqHe4FltTolPowerSupplyDegraded	フォールトトレラントパワーサプライ状態が、**[劣化]**に変化しました。
6050	cpqHe4FltTolPowerSupplyFailed	フォールトトレラントパワーサプライ状態が、**[障害]**に変化しました。
6051	cpqHeResilientMemMirroredMemoryEngaged	アドバンストメモリプロテクションサブシステムが、メモリ障害を検出しました。ミラーメモリがアクティブになりました。
6054	cpqHe3FltTolPowerRedundancyRestore	フォールトトレラントパワーサプライの冗長性が回復しました。
6055	cpqHe3FltTolFanRedundancyRestored	フォールトトレラントパワーファンの冗長性が回復しました。
6061	cpqHeManagementProcInReset	管理プロセッサーがリセットされました。
6062	cpqHeManagementProcReady	管理プロセッサーの準備ができました。
6064	cpqHe5CorrMemReplaceMemModule	メモリエラーは訂正されましたが、メモリモジュールを交換してください。
6069	cpqHe4FltTolPowerSupplyACpowerloss	指定されたシャーシおよびベイのフォールトトレラントパワーサプライが AC 電源の消失を報告しました。
6070	cpqHeSysBatteryFailed	Smart Storage バッテリーが故障しました。
6071	cpqHeSysBatteryRemoved	Smart Storage バッテリーが取り外されました。
6072	cpqHeSysPwrAllocationNotOptimized	iLO は電力要件を決定できませんでした。 サーバーの電力割り当てが最適化されていません。
6073	cpqHeSysPwrOnDenied	ハードウェアを識別できないため、サーバーの電源を入れることができませんでした。
6074	cpqHePowerFailureError	デバイスの電源障害が検出されました。
6075	cpqHeInterlockFailureError	デバイスがマザーボードにない、または適切に取り付けられていません。

Table Continued

トラップ番号	SNMP トラップ名	説明
6077	cpqHeNvdimmRestoreError	NVDIMM の復元エラーが検出されました。
6078	cpqHeNvdimmUncorrectableMemoryError	訂正不能なメモリエラーが検出されました。
6079	cpqHeNvdimmBackupPowerError	NVDIMM のバックアップ電源エラーが発生しました。バックアップ電源を使用できません。これ以上のバッ
6080	cpqHeNvdimmNVDIMMControllerError	NVDIMM コントローラーのエラーが発生しました。OS では NVDIMM は使用されません。
6081	cpqHeNvdimmEraseError	NVDIMM を消去できませんでした。これ以上のバックアップは不可能です。
6082	cpqHeNvdimmArmingError	NVDIMM を取り付けることができませんでした。これ以上のバックアップは不可能です。
6083	cpqHeNvdimmSanitizationOK	この NVDIMM-N がサニタイズ/消去の対象として選択されました。NVDIMM に保存されているデータはすべて
6084	cpqHeNvdimmSanitizationError	この NVDIMM-N はサニタイズ/消去の対象として選択されましたが、このプロセスが正常に終了しませんでした。
6085	cpqHeNvdimmControllerFirmwareError	NVDIMM コントローラーファームウェアのエラーが発生しました。コントローラーファームウェアが壊れているため、OS で NVDIMM は使用されません。
6086	cpqHeNvdimmErrorInterleaveOn	メモリの初期化エラーまたは訂正不能エラーが発生しました。プロセッサーの NVDIMM はすべて無効です。
6087	cpqHeNvdimmInterleaveOff	メモリの初期化エラーまたは訂正不能エラーが発生しました。NVDIMM は無効になっています。
6088	cpqHeNvdimmEventNotifyError	この NVDIMM のイベント通知を設定できません。
6089	cpqHeNvdimmPersistencyLost	NVDIMM の持続性が失われました。これ以上のデータバックアップは不可能です。
6090	cpqHeNvdimmPersistencyRestored	NVDIMM の持続性が復元されました。これ以上のデータバックアップが可能です。
6091	cpqHeNvdimmLifecycleWarning	NVDIMM ライフサイクルの警告 - NVDIMM の寿命に達しました。
6092	cpqHeNvdimmLogicalNvdimmError	論理 NVDIMM のエラーが発生しました。
6093	cpqHeNvdimmConfigurationError	NVDIMM 構成エラーが発生しました。
6094	cpqHeNvdimmBatteryNotChargedwithWait	スマートバッテリは、取り付けられた NVDIMM をサポートするほど十分に充電されていません。
6095	cpqHeNvdimmBatteryNotChargedwithNoWait	スマートバッテリは、取り付けられた NVDIMM をサポートするほど十分に充電されていません。

Table Continued

トラップ番号	SNMP トラップ名	説明
6096	cpqHedimmMemoryMapChanged	訂正不能なメモリエラー-障害が発生しているメモリモジュールを判別できませんでした。
6097	cpqHeNvdimmPersistantMemoryAddressErrorPersistentMemory	アドレス範囲スクラブでエラーが検出されました。
6098	cpqHeNvdimmInitializationError	内部エラーのため、1 つまたは複数の NVDIMM を初期化できません。
6099	cpqHePwrSupplyError	システム電源装置のエラーが発生しました。
6100	cpqHePwrSupplyErrorRepaired	システム電源装置のエラーが修復されました。
6101	cpqHeBbuError	バッテリバックアップユニットのエラーが発生しました。
6102	cpqHeBbuErrorRepaired	バッテリバックアップユニットのエラーが修復されました。
6103	cpqHeNoPowerSupplyDetected	電源装置または電源バックプレーンは検出されませんでした。
6104	cpqHePowerProtectionFault	システムボードの電源保護障害が発生しました。
6105	cpqHePowerFusedegraded	電源の劣化が検出され、サーバーシステムボードを交換する必要があります。
6106	cpqHeTPMSecureEraseFailedTrusted	Platform Module のセキュア消去に失敗しました。
6107	cpqHeSPISecureEraseFailed	システムファームウェア構成のセキュア消去に失敗しました。
6108	cpqHeNvdimmSecureEraseFailed	インテル Optane DC 不揮発性メモリのセキュア消去に失敗しました。
6109	cpqHeNANDSecureEraseFailed	管理プロセッサーの内蔵メディアデバイスのセキュア消去に失敗しました。

Table Continued

トラップ番号	SNMP トラップ名	説明
8029	cpqSs6FanStatusChange	ストレージシステムのファンのステータスが変化したことを検出しました。
8030	cpqSs6TempStatusChange	ストレージシステムの温度のステータスが変化したことを検出しました。
8031	cpqSs6PwrSupplyStatusChange	ストレージシステムの電源のステータスが変化したことを検出しました。
8032	cpqSsConnectionStatusChange	ストレージエンクロージャのステータス変化したことを検出しました。
9001	cpqSm2ServerReset	サーバーの電源がリセットされました。
9003	cpqSm2UnauthorizedLoginAttempts	認証されないログイン試行回数の最大値を超えました。
9005	cpqSm2SelfTestError	iLO がセルフテストエラーを検出しました。
9012	cpqSm2SecurityOverrideEngaged	iLO が、セキュリティオーバーライドジャンパーが接続位置に切り替えられていることを検出しました
9013	cpqSm2SecurityOverrideDisengaged	iLO が、セキュリティオーバーライドジャンパーが切断位置に切り替えられていることを検出しました。
9017	cpqSm2ServerPowerOn	サーバーの電源が入りました。
9018	cpqSm2ServerPowerOff	サーバーの電源が切られました。
9019	cpqSm2ServerPowerOnFailure	サーバーの電源を入れる要求がありましたが、サーバーが障害状態にあったために電源を入れることができませんでした。
9021	cpqSm2FirmwareValidationScanFailed	ファームウェアの検証時にエラーが発生しました（iLO/IE/SPS ファームウェア）
9022	cpqSm2FirmwareValidationScanErrorRepaired	報告されたファームウェア整合性スキャンの問題は修復されました。
9023	cpqSm2FirmwareValidationAutoRepairFailed	ファームウェアのリカバリー時にエラーが発生しました。
11003	cpqHo2GenericTrap	汎用トラップ。SNMP 設定、クライアント SNMP コンソール、およびネットワークが正しく動作していることを確認します。iLO の Web インターフェースを使用すると、このアラートを生成して、SNMP コンソールでアラートが受信されることを確認できます。
11018	cpqHo2PowerThresholdTrap	電力しきい値を超えました。
11020	cpqHoMibHealthStatusArrayChangeTrap	サーバーのヘルスステータスが変化しました。
5022	cpqSasPhyDrvStatusChange	AMS が、SAS または SATA 物理ドライブのステータスが変化したことを検出しました。

Table Continued

トラップ番号	SNMP トラップ名	説明
14004	cpqIdeAtaDiskStatusChange	AMS が、ATA ディスクドライブのステータスが変化したことを検出しました。
16028	cpqFca3HostCntlrStatusChange	AMS が、ファイバーチャネルホストコントローラーのステータスが変化したことを検出しました。
18011	cpqNic3ConnectivityRestored	AMS が、ネットワークアダプターとの接続が回復したことを検出しました。
18012	cpqNic3ConnectivityLost	AMS が、論理ネットワークアダプターのステータスが[障害]に変化したことを検出しました。
18013	cpqNic3RedundancyIncreased	AMS が、接続されている論理アダプターグループ内の障害が発生していた物理アダプターが良好ステータスに復帰したことを検出しました。
18014	cpqNic3RedundancyReduced	AMS が、論理アダプターグループ内の物理アダプターが障害ステータスに変化したが、少なくとも 1 台の物理アダプターが良好な状態で残っていることを検出しました。
18015	cpqNicAllLinksDown	AMS が、論理アダプターグループ内の全ての物理アダプターが障害ステータスに変化したことを検出しました。
169001	cpqiScsiLinkUp	AMS が、iSCSI セッションの起動を検出しました。
169002	cpqiScsiLinkDown	AMS が、iSCSI セッションの切断を検出しました。

Table Continued

トラップ番号	SNMP トラップ名	説明
6077	cpqHeNvdimmRestoreError	NVDIMM の復元エラーが検出されました。
6078	cpqHeNvdimmUncorrectableMemoryError	訂正不能なメモリエラーが検出されました。
6079	cpqHeNvdimmBackupPowerError	NVDIMM のバックアップ電源エラーが発生しました。バックアップ電源を使用できません。これ以上のバックアップは不可能です。
6080	cpqHeNvdimmNVDIMMControllerError	NVDIMM コントローラーのエラーが発生しました。OS では NVDIMM は使用されません。
6081	cpqHeNvdimmEraseError	NVDIMM を消去できませんでした。これ以上のバックアップは不可能です。
6082	cpqHeNvdimmArmingError	NVDIMM を取り付けることができませんでした。これ以上のバックアップは不可能です。
6083	cpqHeNvdimmSanitizationOK	この NVDIMM-N がサニタイズ/消去の対象として選択されました。NVDIMM に保存されているデータはすべて消去されました。
6084	cpqHeNvdimmSanitizationError	この NVDIMM-N はサニタイズ/消去の対象として選択されましたが、このプロセスが正常に終了しませんでした。
6085	cpqHeNvdimmControllerFirmwareError	NVDIMM コントローラーファームウェアのエラーが発生しました。コントローラーファームウェアが壊れているため、OS で NVDIMM は使用されません。
6086	cpqHeNvdimmErrorInterleaveOn	メモリの初期化エラーまたは訂正不能エラーが発生しました。プロセッサーの NVDIMM はすべて無効です。
6087	cpqHeNvdimmInterleaveOff	メモリの初期化エラーまたは訂正不能エラーが発生しました。NVDIMM は無効になっています。
6088	cpqHeNvdimmEventNotifyError	この NVDIMM のイベント通知を設定できません。
6089	cpqHeNvdimmPersistencyLost	NVDIMM の持続性が失われました。これ以上のデータバックアップは不可能です。
6090	cpqHeNvdimmPersistencyRestored	NVDIMM の持続性が復元されました。これ以上のデータバックアップが可能です。
6091	cpqHeNvdimmLifecycleWarning	NVDIMM ライフサイクルの警告 - NVDIMM の寿命に達しました。
6092	cpqHeNvdimmLogicalNvdimmError	論理 NVDIMM のエラーが発生しました。
6093	cpqHeNvdimmConfigurationError	NVDIMM 構成エラーが発生しました。
6094	cpqHeNvdimmBatteryNotChargedwithWait	スマートバッテリは、取り付けられた NVDIMM をサポートするほど十分に充電されていません。
6095	cpqHeNvdimmBatteryNotChargedwithNoWait	スマートバッテリは、取り付けられた NVDIMM をサポートするほど十分に充電されていません。

Table Continued

トラップ番号	SNMP トラップ名	説明
6096	cpqHedimmMemoryMapChanged	訂正不能なメモリエラー-障害が発生しているメモリモジュールを判別できませんでした。
6097	cpqHeNvdimmPersistantMemoryAddressErrorPersistentMemory	アドレス範囲スクラブでエラーが検出されました。
6098	cpqHeNvdimmInitializationError	内部エラーのため、1 つまたは複数の NVDIMM を初期化できません。
6099	cpqHePwrSupplyError	システム電源装置のエラーが発生しました。
6100	cpqHePwrSupplyErrorRepaired	システム電源装置のエラーが修復されました。
6101	cpqHeBbuError	バッテリバックアップユニットのエラーが発生しました。
6102	cpqHeBbuErrorRepaired	バッテリバックアップユニットのエラーが修復されました。
6103	cpqHeNoPowerSupplyDetected	電源装置または電源バックプレーンは検出されませんでした。
6104	cpqHePowerProtectionFault	システムボードの電源保護障害が発生しました。
6105	cpqHePowerFusedegraded	電源の劣化が検出され、サーバーシステムボードを交換する必要があります。
6106	cpqHeTPMSecureEraseFailedTrusted	Platform Module のセキュア消去に失敗しました。
6107	cpqHeSPISecureEraseFailed	システムファームウェア構成のセキュア消去に失敗しました。
6108	cpqHeNvdimmSecureEraseFailed	インテル Optane DC 不揮発性メモリのセキュア消去に失敗しました。
6109	cpqHeNANDSecureEraseFailed	管理プロセッサーの内蔵メディアデバイスのセキュア消去に失敗しました。
6110	cpqHeSedPassphrasefail	デバイスの暗号化エラー。暗号化の有効化または無効化あるいはパスフレーズの変更に失敗しました。
6111	cpqHeSedUnlockfail	自己暗号化デバイスのロックを解除する不正な試行が 3 回実行されました。デバイスは次回のリブートまでロックされます。

重要: OS 上の SNMP サービスをご利用され、また AMS(Agentless Management Service)が動作している場合、いくつかのイベントは、iLO からトラップが送出されると同時に、AMS からも SNMP サービスの設定に基づき同じトラップ番号のトラップが送出されます。

同じトラップ番号のトラップが送出されますが、送出元の IP アドレスが iLO と OS で異なります。どちらか一方の Trap 情報を参照してください。

セルフテストのトラップが送信された場合、「iLO セルフテスト結果の表示」章に従いセルフテストの結果を確認してください。セルフテストのトラップが送信されても、自己修復される場合があります。セルフテストのステータスに"Pass"が表示されている場合、自己修復/回復した状態であるため問題ありません。

アラートメールの設定

iLO アラートメールを使用すると、ホストオペレーティングシステムから独立して検出されたアラート条件を、指定したメールアドレスに送信するように iLO を設定することができます。
iLO メールアラートには、主要なホストシステムイベントが含まれます。

アラートメールのサンプル

```
Subject: NEC iLO AlertMail-280: (CAUTION) System Fan Removed (Fan 4, Location System)
From: =iLO hostname < hostname.example.com@example.com>
To: mailreceiver@example.com
------------------------------------------------------------------------------------------------------------------------
---
EVENT (15-Aug-2017 00:46): System Fan Removed (Fan 4, Location System)

Integrated Management Log Severity:CAUTION



iLO URL: https://hstname.example.com
iLO IP: https://172.16.0.1
iLO Name:      hstname
iLO firmware:  1.10 Jun 07 2017

Server Model:  Express5800/R120h-2M
System ROM:    U30 06/14/2017 Server UUID:   01234567-89AB-CDEF-0123-4367890ABCDE



PLEASE DO NOT REPLY TO THIS EMAIL. For more details about NEC iLO technology, visit: jpn.nec.com/express/
```

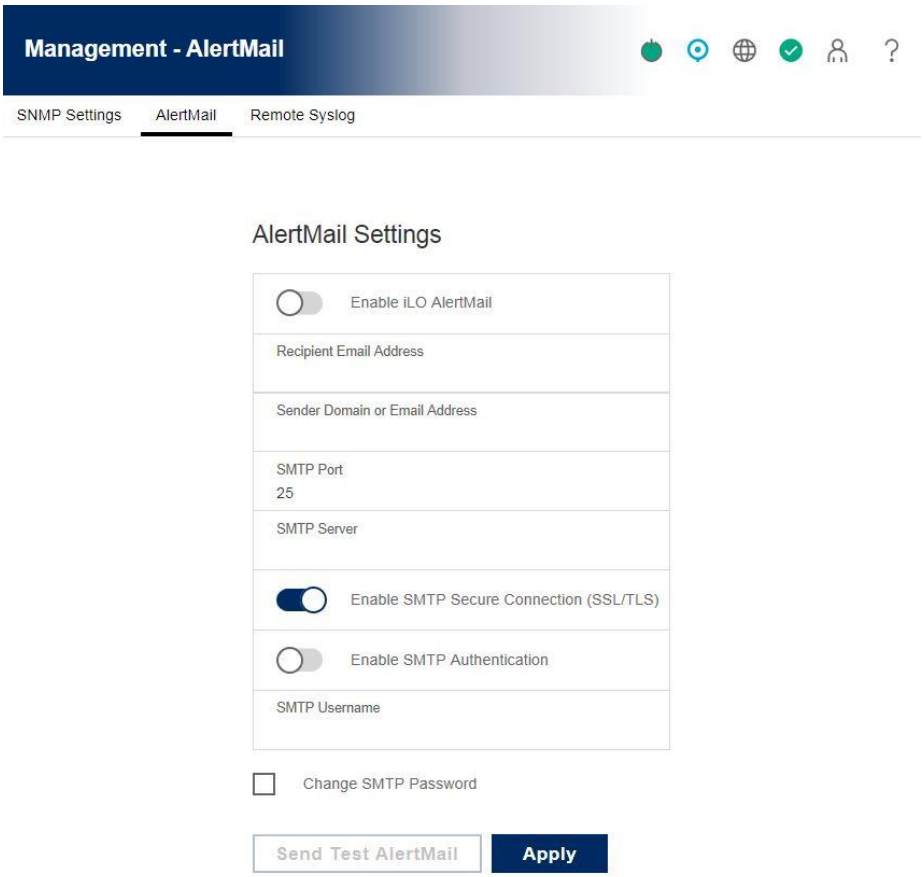
アラートメールを有効にする

前提条件

- この機能をサポートする iLO ライセンスがインストールされている必要があります。
- iLO の設定を構成権限

手順

1. **[Management]→[AlertMail]**ページに移動します。



2. **[Enable iLO AlertMail]**のトグルボタンを有効にします。
3. 次の情報を入力します。
   - **[Email Address]** - iLO メールアラートの送信先 Email アドレス。この文字列は最大 63 文字であり、標準の Email アドレス形式である必要があります。Email アドレスには、英数、+(プラス)、-(マイナス)、_(アンダースコア)、.(ピリオド)以外の文字は使用しないでください。iLO Firmware Version 1.15 Aug 17 2017 以降では、;(セミコロン)で区切ることで Email アドレスを複数指定することができます。
   - **[Sender Domain]** - 送信元 Email アドレスに設定されるドメイン名。送信元 Email アドレスは、ホスト名として iLO 名、ドメイン名として送信ドメインを使用して構成します。この文字列は最大 63 文字です。
   - **[SMTP Port]** - SMTP サーバーが非認証 SMTP 接続に使用するポート。デフォルト値は 25 です。
   - **[SMTP Server]** - SMTP サーバーまたは MSA の IP アドレスまたは DNS 名。このサーバーは、MTA と連携してメールを配信します。この文字列は最大 63 文字です。

   iLO 5 Firmware Version 1.15 Aug 17 2017 以前では、SMTP サーバーが IPv6 アドレスで稼働している場合に、DNS サーバーで SMTP サーバーの名前解決を行うことができません。IPv6 環境でアラートメールをご利用になる場合には、**[SMTP Server]**設定は SMTP サーバーの IP アドレスで指定してください。

   iLO 5 Firmware Version 1.30 May 31 2018 以降の場合は、必要に応じて 4 及び 5 の設定を行ってください。

4. セキュアな接続を介してアラートメールメッセージを送信するには、**[Enable SMTP Secure Connection (SSL/TLS)]**オプションを有効にします。
5. メールアカウントのユーザー名とパスワードで SMTP 接続を認証するには、**[Enable SMTP Authentication]**オプションを有効にします。

   [Enable SMTP Secure Connection (SSL/TLS)]および**[Enable SMTP Authentication]**が有効になっている場合：

   a. 構成されている SMTP サーバー上のメールアカウントのユーザー名を入力します。
   b. **[Change SMTP Password]**を選択します。
   c. **[New SMTP Password]**と**[Confirm SMTP Password]**にメールアカウントのユーザー名のパスワードを入力します。
6. オプション：**[Send Test AlertMail]**をクリックして、設定されたメールアドレスにテストメッセージを送信します。

   このボタンは、アラートメールが有効な場合にのみ使用できます。
7. **[Apply]**をクリックして、変更を保存します。

注記:iLO 5 Firmware Version 1.20 Feb 02 2018 以前のファームウェアから iLO Firmware Version 1.30 May 31 2018 にアップデートした場合は、デフォルト設定では**[Enable SMTP Secure Connection (SSL/TLS)]**が有効になっているため**[SMTP Authentication]**を行うか、**[Enable SMTP Secure Connection (SSL/TLS)]**を無効にしてください。設定が旧バージョンのままの場合、アラートメールが送信されなくなります。

アラートメールを無効にする

前提条件

- この機能をサポートする iLO ライセンスがインストールされている必要があります。
- iLO の設定を構成権限

手順

1. **[Management]**→**[AlertMail]**ページに移動します。
2. **[Enable iLO AlertMail]**のトグルボタンを無効にします。
3. **[Apply]**をクリックして、変更を保存します。

リモート Syslog の設定

リモート Syslog 機能を使用すると、iLO はイベント通知メッセージを Syslog サーバーに送信できます。iLO ファームウェアのリモート Syslog には、IML および iLO イベントログが含まれます。

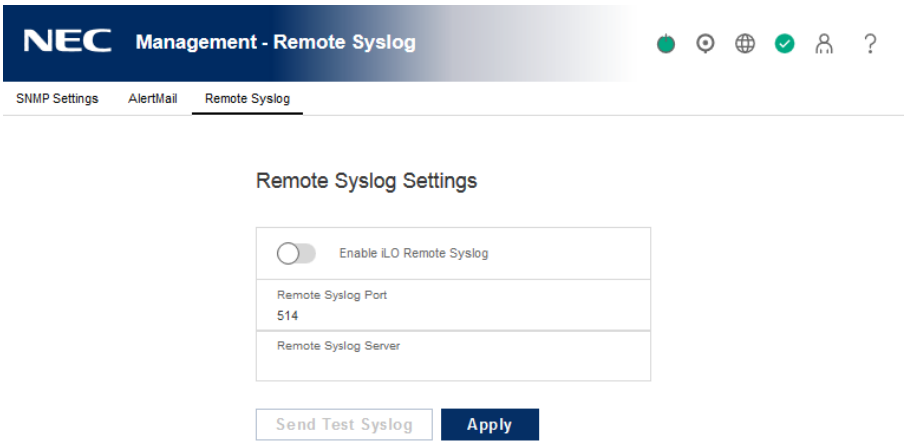
iLO リモート Syslog の有効化

前提条件

- この機能をサポートする iLO ライセンスがインストールされている必要があります。
- iLO の設定を構成権限

手順

1. **[Management]→[Remote Syslog]**ページに移動します。



2. **[Enable iLO Remote Syslog]** のトグルボタンを有効にします。
3. 次の情報を入力します。
   - **[Remote Syslog Port]** - Syslog サーバーが受信に使用するポート番号。
     デフォルト値は 514 です。
   - **[Remote Syslog Server]** - Syslog サービスを実行しているサーバーの IP アドレス、FQDN、IPv6 名、または省略名。この文字列は最大 127 文字です。

     Linux システムでは、システムイベントは「syslog」というツールによって記録されます。このツールは、すべての Linux システムにインストールする必要があります。 iLO システムの中央ログシステムとして機能するリモートシステムに Syslog サーバーを設定することができます。このように、iLO で iLO リモート Syslog 機能を有効にすると、iLO は iLO のログを Syslog サーバーに送信できます。

   iLO 5 Firmware Version 1.15 Aug 17 2017 以前では、リモート Syslog をお使いになる際、IPv6 環境の DNS サーバーで名前解決を行うことができません。IPv6 環境でリモート Syslog をご利用になる場合には、**[Remote Syslog Server]**設定はリモート **Syslog** サーバーの IP アドレスで指定してください。
4. オプション：**[Send Test Syslog]**をクリックして、設定した Syslog サーバーにテストメッセージを送信します。
   このボタンは、iLO リモート Syslog が有効な場合のみ使用できます。
5. **[Apply]**をクリックして、変更を保存します。

iLO リモート Syslog の無効化

前提条件

- この機能をサポートする iLO ライセンスがインストールされている必要があります。
- iLO の設定を構成権限

手順

1. **[Management]→[Remote Syslog]**ページに移動します。
2. **[Enable iLO Remote Syslog]**のトグルボタンを無効にします。
3. **[Apply]**をクリックして、変更を保存します。

19. ライフサイクル管理

One-button セキュア消去

サーバーを廃棄するか、または別の用途で準備する場合、One-button セキュア消去機能を使用できます。

One-button セキュア消去は、NIST Special Publication 800-88 Revision 1 の*メディアサニタイズのガイドライン*に準拠しています。

仕様について詳しくは、https://www.ipa.go.jp/files/000025355.pdf (日本語訳) を参照してください。仕様のセクション 2.4 では、サニタイズのレベルについて説明しています。付録では、メディアの最小サニタイズレベルを提示しています。

One-button セキュア消去は、ユーザーデータのパージに対する NIST SP 800-88 Revision 1 のサニタイズに関する勧告を実装しており、サーバーおよびサポートされたコンポーネントをデフォルトの状態に戻します。この機能は、サーバーの*揮発性に関する報告*ドキュメントでユーザーが行う多くのタスクを自動化します。

One-button セキュア消去アクセス方式

次の製品から One-button セキュア消去プロセスを開始できます。

- iLO 5 Firmware Version 2.31 Oct 13 2020 以降
- EXPRESSBUILDER 3.30 以降
- iLO RESTful API

iLO から One-button セキュア消去プロセスを開始するための前提条件

手順

1. 自分の iLO ユーザーアカウントにすべての iLO ユーザーアカウント権限が割り当てられていることを確認します。
2. この機能をサポートする iLO ライセンスをインストールします。
   NX7700x シリーズサーバには、この機能をサポートするライセンスが標準でインストールされています。
3. 消去するサーバーに Starter Pack Ver.S8.80-002.01 以降が適用されている。
4. 次の機能が有効になっている場合は、無効にします。
   - Server Configuration Lock/サーバ構成ロック
   - Smart アレイ暗号化
5. システムメンテナンススイッチの iLO セキュリティ設定の位置が OFF であることを確認します。
6. 消去するストレージドライブで、ネイティブのサニタイズ方式をサポートしています。

   たとえば、SATA および SAS ドライブには SANITIZE コマンドなどです。NIST 文書では、上記のデバイスタイプでデータをパージするには上記のコマンドを勧めています。これらの

コマンドを使用するほうが、ソフトウェアを使用してストレージドライブ上のデータを上書きするよりも安全です。

7. 拡張スキーマで LDAP ディレクトリ認証を使用している場合、One-button セキュア消去プロセスを開始するために、iLO にログインする別の方法があります。

   サポートされている方法には、ローカルアカウント、Kerberos 認証が含まれます。

詳しくは
ブラウザーを使用したライセンスキーのインストール
iLO ユーザー権限

iLO からの One-button セキュア消去プロセスの開始

前提条件

ご使用の環境が iLO から One-button セキュア消去プロセスを開始するための前提条件を満たしている。

手順

1. 消去しないストレージデバイスを切断またはデタッチします。

   データ損失の可能性を低減するため、消去しないドライブを切断またはデタッチすることをお勧めします。この手順には、リムーバブルドライブ、外部ストレージ、共有ストレージ、およびネイティブのサニタイズ方式をサポートしていないデバイスが含まれます。

   接続されたストレージデバイスがネイティブのサニタイズ方式をサポートしていない場合、そのストレージデバイスは One-button セキュア消去プロセス中に消去されません。インテグレーテッドマネジメントログ（IML）エントリにより、デバイスの消去の障害が報告されます。
2. （オプション）SNMP、アラートメール、または iLO RESTful API アラートを構成します。

   この手順を完了することをお勧めします。
   各コンポーネントが消去されるときにエラーが発生した場合は、各エラーについて、IML エントリーが記録されます。アラートを構成している場合、通知を受け取ります。IML は、One-button セキュア消去プロセス中に消去されます。IML が消去されると、セキュア消去レポートテーブルに高レベルのステータス情報が表示されます。
   iLO 5 Firmware Version 2.31 Oct 13 2020 以降がインストールされているサーバーの場合、セキュア消去レポートには、内蔵 NAND フラッシュと NVRAM のステータスのみが含まれます。

3. ナビゲーションツリーで[**Lifecycle Management**]をクリックし、[**Decommission**]タブをクリックします。
4. [**Erase System**]をクリックします。

   iLO が要求を確認するように求めます。

△**注意:**
この機能は、システムを廃棄する場合、または別の目的で使用する場合にのみ使用してください。このプロセスは、サーバーおよびサポートされるコンポーネントを工場出荷時の状態にリセットします。ストレージ容量によっては、サーバーとコンポーネントのセキュア消去が完了するまでに 1 日以上かかる場合があります。このプロセスはいったん開始すると、元に戻すことはできません。プロセスが完了するまで、構成の変更やシステムの電源オフに関係する iLO またはシステムとの対話は避けてください。

5. セキュア消去の確認チェックボックスをオンにして、[**Yes, permanently erase system**]をクリックします。

   サーバーが再起動し、One-button セキュア消去プロセスが開始します。
   One-button セキュア消去の進捗は、すべての iLO Web インターフェースページのバナー領域に表示されます。表示される情報には、完了率と推定の残り時間が含まれます。個々のハードウェアまたはソフトウェアコンポーネントの詳細は、セキュア消去ステータステーブルに表示されます。
   One-button セキュア消去プロセス中に、構成を変更しないでください。このプロセス中は、iLO によってファームウェアアップデートが妨げられ、iLO がリセットされます。
   One-button セキュア消去が完了すると iLO がリセットされ、ネットワーク上で使用できなくなります。
6. （オプション）システムを稼働状態に戻します。
7. （オプション）[**One-button secure erase report**]を表示、保存、または削除します。
   この手順を完了することをお勧めします。
8. （オプション）デバイスが消去プロセスに失敗した場合、またはデバイスがネイティブのサニタイズ方式をサポートしていない場合は、次のいずれかを実行します。
   - これらのデバイスを分離し、他の方式を使用してデータを削除します。
   - 組織のセキュリティポリシーに従ってデバイスを安全に廃棄します。

   この手順を完了することをお勧めします。

詳しくは
One-button セキュア消去レポートの表示
One-button セキュア消去レポートの削除
CSV ファイルへの One-button セキュア消去レポートの保存
One-button セキュア消去後にシステムを動作状態に戻す
One-button セキュア消去の FAQ
One-button セキュア消去の完了後のシステムへの影響
工場出荷時の状態に戻されるハードウェアコンポーネント
工場出荷時の状態に戻されないハードウェアコンポーネント

One-button セキュア消去ステータス値

One-button セキュア消去プロセスを開始すると、全体の進捗が iLO バナーに表示されます。個々のコンポーネントのステータスは、 セキュア消去ステータステーブルに表示されます。

- ⊖[**Idle**] - プロセスは開始されていません。
- [**Initiated**] - プロセスは開始されました。

- [In Progress] - 消去が進行中です。
- [Success] - プロセスは正常に完了しました。
- [Error] - プロセスが完了しましたが、エラーが発生しています。
- [Failed] - プロセスは失敗しました。

> △**注意:**
> セキュア消去ステータステーブル内の iLO 設定には、内蔵 NAND フラッシュと NVRAM の結果が含まれています。これらのコンポーネントのいずれかで消去の障害が発生すると、iLO 設定の全体的な障害になります。
> セキュア消去ステータステーブル内の BIOS 設定には、UEFI 構成ストアと RTC（システム日付時刻）の結果が含まれます。これらのコンポーネントのいずれかで消去の障害が発生すると、BIOS 設定の全体的な障害になります。

One-button セキュア消去後にシステムを動作状態に戻す

One-button セキュア消去プロセスでシステムが消去された後に、次の手順を使用して操作状態に戻します。

手順

1. iLO ネットワーク設定を構成します。
2. EXPRESSBUILDER リカバリイメージを使用して EXPRESSBUILDER をインストールします。

   本製品で使用する EXPRESSBUILDER は、以下 Web サイトに最新版が掲載されています。Web に掲載されている内容を確認し、最新の EXPRESSBUILDER を適用してください。
   https://www.support.nec.co.jp/
   (「NEC サポートポータル内検索」で、「EXPRESSBUILDER」を入力して検索してください。)
3. オペレーティングシステムをインストールします。
4. オプション：iLO ライセンスをインストールします。
5. BIOS 設定および環境に適用される iLO 設定を構成します。
6. （オプション）システムリカバリセットを作成します。

One-button セキュア消去レポートの表示

前提条件

- サーバーで One-button セキュア消去プロセスが完了している。
- One-button セキュア消去プロセスの完了後、iLO が IP アドレスで構成されている。

手順

1. ナビゲーションツリーで[**Lifecycle Management**]をクリックし、[**Decommision**]タブをクリックします。

サーバーで One-button セキュア消去プロセスが完了したら、 最新の消去レポートの参照ボタンが使用できます。

2. [**View Last Erase Report**]をクリックします。
   セキュア消去レポートが表示されます。
3. （オプション）テーブルの列でソートするには、列見出しをクリックします。
   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
4. （オプション）CSV ファイルへの One-button セキュア消去レポートの保存
   今後の参照用に消去レポートのコピーを保存することをお勧めします。
5. （オプション）One-button セキュア消去レポートの削除
   サーバーを廃棄するか、または別の目的で使用する前に、消去レポートを削除することをお勧めします。

One-button セキュア消去レポートの詳細

- [**Server Serial Number**] - サーバーのシリアル番号。
- [**Initiated By**] - One-button セキュア消去プロセスを開始したユーザー。

次の情報がデバイスごとにリストされます。

- [**Device Type**] - 消去されたデバイスタイプ。
  影響を受けるデバイスタイプについては、One-button セキュア消去の完了後のシステムへの影響を参照してください。
  iLO 5 Firmware Version 2.31 Oct 13 2020 以降がインストールされているサーバーの場合、セキュア消去レポートには、内蔵 NAND フラッシュと NVRAM のステータスのみが含まれます。
- [**Location**] - サーバー内のデバイスの位置。
- [**Serial Number**] - デバイスのシリアル番号。
- [**Status**] - デバイスの One-button セキュア消去ステータス。
- [**Erase Type**] - 消去操作のタイプ。実行された操作について詳しくは、One-button セキュア消去の FAQ を参照してください。
- [**Start Time**] - 特定のデバイスの One-button セキュア消去の開始時刻。
- [**End Time**] - 特定のデバイスの One-button セキュア消去の終了時間。

CSV ファイルへの One-button セキュア消去レポートの保存

One-button セキュア消去機能を使用する場合、今後の参照用に消去レポートのコピーを保存することをお勧めします。

前提条件

- サーバーで One-button セキュア消去プロセスが完了している。
- One-button セキュア消去プロセスの完了後、iLO が IP アドレスで構成されている。

手順

1. ナビゲーションツリーで[**Lifecycle Management**]をクリックし、[**Decommision**]タブをクリックします。
2. 終了ボックスにある  をクリックします。
   CSV アウトプットウィンドウが表示されます。
3. 保存をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

One-button セキュア消去レポートの削除

サーバーを廃棄または再利用する場合、iLO Web インターフェースで One-button セキュア消去レポートを使用可能なままにしたくない場合があります。

サーバーを廃棄するか、または別の目的で使用する前に、消去レポートを削除することをお勧めします。

前提条件

- iLO の設定を構成する権限
- サーバーで One-button セキュア消去プロセスが完了している。
- One-button セキュア消去プロセスの完了後、iLO が IP アドレスで構成されている。
- 後で参照するために One-button セキュア消去レポートのコピーが必要な場合に、レポートを保存している。

手順

1. ナビゲーションツリーで[**Lifecycle Management**]をクリックし、[**Decommision**]タブをクリックします。
   サーバーで One-button セキュア消去プロセスが完了したら、 最新の消去レポートの参照ボタンが使用できます。
2. [**View Last Erase Report**]をクリックします。
   セキュア消去レポートが表示されます。
3.  をクリックします。

iLO によって、レポートファイルがセキュア消去され、すぐにリセットされます。

この時点までに作成されたイベントログ、IML、セキュリティログ、および構成設定が、工場出荷時のデフォルト設定にリセットされます。iLO は、起動時に自動リストア操作を試みる場合があります。詳しくは、iLO のバックアップとリストアを参照してください。

One-button セキュア消去の完了後のシステムへの影響

One-button セキュア消去機能は、システムおよびサポートされたコンポーネントを工場出荷時の状態に戻します。システムを使用するには、再度サーバーをプロビジョニングします。

- 影響を受けたストレージドライブおよび不揮発性メモリ上にあるすべてのデータは消去され、回復可能ではありません。
  すべての RAID 設定、ディスクパーティション、および OS インストールは削除されます。
- BIOS および iLO 5 設定は工場出荷時デフォルト設定にリセットされます。
  - iLO ネットワークやその他の設定は消去され、再構成が必要となります。
  - インストールされた iLO ライセンスは削除され、ライセンスのステータスは iLO Standard に戻ります。
  - システムリカバリセットは削除され、再作成が必要となります。
  - iLO のユーザーアカウントが削除されます。プロセスが完了したら、デフォルトの工場出荷時の管理者アカウントとパスワードを使用してログインします。
  - Active Health System、インテグレーテッドマネジメントログ、セキュリティログ、および iLO イベントログは消去されます。
  - BIOS および SmartStorage Redfish API データの削除され、次回のブート時に再作成されます。
  - セキュアブートは無効になり、工場出荷時にインストールされている証明書を除き、登録された証明書は削除されます。
  - ブートオプションとユーザーが定義した BIOS のデフォルトは削除されます。
  - TPM または BIOS に格納されたパスワード、パスフレーズ、および暗号化キーは削除されます。
  - 日付、時刻、DST、およびタイムゾーンはリセットされます。
  - システムは、BIOS の最新リビジョンがフラッシュされた状態で起動されます。
- EXPRESSBUILDER は起動せず、再インストールする必要があります。

  本製品で使用する EXPRESSBUILDER は、以下 Web サイトに最新版が掲載されています。
  Web に掲載されている内容を確認し、ご使用の機種に対応した EXPRESSBUILDER のうち、最新のものを適用してください。
  https://www.support.nec.co.jp/
  (「NEC サポートポータル内検索」で、「EXPRESSBUILDER」を入力して検索してください。)

工場出荷時の状態に戻されるハードウェアコンポーネント

次のコンポーネントは、One-button セキュア消去プロセス中に、工場出荷時の状態に戻されます。

- UEFI 構成ストア
- RTC（システムの日付と時刻）
- Trusted Platform Module。トラステッドプラットフォームモジュール
- NVRAM
  - BIOS 設定 (RBSU)
  - iLO 構成設定
  - iLO イベントログ
  - インテグレーテッドマネジメントログ
  - セキュリティログ
- 内部ポートに接続された Smart アレイ SR コントローラーおよびドライブ
- Smart アレイ S100i ソフトウェア RAID
- ドライブデータ（ネイティブのサニタイズ方式をサポートするドライブの場合）
  - SATA、SAS ドライブ（SSD および HDD）
- 不揮発性メモリ

    - インテル Optane DC 不揮発性メモリ
- 内蔵フラッシュ
    - iLO RESTful API データ
    - Active Health System
    - ファームウェアレポジトリ

工場出荷時の状態に戻されないハードウェアコンポーネント

次のコンポーネントは One-button セキュア消去プロセスの影響を受けません。

- USB ドライバー
- SD カード
- iLO 仮想メディア
- PCI コントローラー上の構成
- Smart アレイ MR コントローラーおよび接続されたストレージ
- Smart アレイ SR コントローラー上の外部ポートに接続されたドライブ
- SAS HBA および接続されたドライブ
- ネイティブのサニタイズ方式をサポートしていない SATA、SAS ドライブ。
- FCoE、iSCSI ストレージ
- GPGPU
- その他の FPGA、アクセラレータ、キーまたはストレージを持つオフロードエンジン

One-button セキュア消去の FAQ

- One-button セキュア消去は USB デバイスおよび内部 SD カードをパージしますか。
  いいえ。One-button セキュア消去は USB デバイスおよび内部 SD カードをパージしません。
- HDD がパージ機能をサポートしていない場合、One-button セキュア消去はパージを試みますか。
  いいえ。One-button セキュア消去はパージ機能をサポートしていないドライブをスキップします。
- One-button セキュア消去は Smart アレイコントローラーをサポートしていますか。
  One-button セキュア消去をサポートするのは、NEC Smart アレイ SR コントローラーのみです。
- Smart アレイはパージをサポートしていないドライブを消去しますか。
  Smart アレイは、パージ操作をサポートしていないドライブをワイプ（あるパターンで上書きする）できます。One-button セキュア消去では、Smart アレイでこのセキュリティ保護されていないワイプを実行する必要はありません。EXPRESSBUILDER の[**System Erase and Reset**]機能を使用して、このようなドライブのデータをワイプします。
- One-button セキュア消去はバッテリバックアップ式キャッシュを消去しますか。
  詳しくは、次の表を参照してください。
- One-button セキュア消去は消去コマンドをどのように処理しますか。
  One-button セキュア消去がデータをパージまたは上書きする方法に関する情報については、次の表を参照してください。
- One-button セキュア消去を起動するために必要な権限は何ですか。
  One-button セキュア消去を起動するには、すべての iLO 権限が必要です。
- One-button セキュア消去はシリアル番号とプロダクト ID を削除しますか。
  いいえ、これらの項目は One-button セキュア消去によって消去されません。

- この処理はどの程度かかりますか。
  ハードウェアによって異なります。HDD のサニタイズは SSD よりも時間がかかります。

One-button セキュア消去はサポートされたドライブにどのように作用しますか。

デバイス	実施される操作	結果
NVRAM	3 パス書き込み：0x5a、0xa5、0xff	すべてのバッテリバックアップ式 iLO SRAM メモリが上書きされます。
内蔵フラッシュ（NAND）	拡張 CSD レジスタの SECURE_REMOVAL_TYPE が物理メモリ消去に設定されている eMMC 5.1（JEDEC 84-B51）セキュア消去コマンド（デバイスでサポートされている場合）。	物理メモリ内のデータが消去されます。
インテル Optane DC PMM	完全消去 + DIMM を上書き	暗号化キーが削除され、すべての物理メモリブロック内のデータ（ユーザーがアクセス可能なデータとスペアブロック内の両方のデータ）がゼロで上書きされます。すべての構成とメタデータを含む PCD 領域も上書きされます。
UEFI 構成ストア	3 パス：チップ消去（0xff）、0x00、チップ消去（0xff）	すべての物理セクターが上書きされます。
RTC	時刻を 01-01-2001 00:00:00 にリセット	日付、時刻、タイムゾーン、および DST がデフォルト設定にリセットされます。
TPM	TPM クリア + NV インデックスをクリア + プラットフォーム対象キーを削除 + PPS を変更 + EPS を変更	すべての不揮発性情報を含む、TPM のすべてのデータがクリアされます。
Smart アレイ SR コントローラー	論理ドライブを削除 + 構成のメタデータをクリア + 工場出荷時設定へのリセット + 物理ドライブのサニタイズ **注意**：One-button セキュア消去を開始する前に、Smart Storage Administrator を介して、セキュリティリセット機能を手動で実行する必要があります（Smart アレイ Secure Encryption が有効化されていた場合）。	• セキュリティリセット機能は、リモートキー管理のためにキーマネージャーに保存されているドライブキーを削除します。コントローラーおよびドライブのすべてのシークレット、キー、およびパスワードがクリアされます。この操作は、キーマネージャー上のコントローラーキーを削除しません。 • すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。すべてのコントローラー設定は工場出荷時の設定にリセットされます。 • フラッシュバックアップはクリアされ、DRAM のライトバックキャッシ

デバイス	実施される操作	結果
		ュ内のデータは電源が取り外されたときに失われます。 接続されたすべてのドライブをサニタイズする必要があります。ドライブ上で必要な操作については、以下を参照してください。
Smart アレイ S100i ソフトウェア RAID	SATA AHCI モードにリセット + 物理ドライブのサニタイズ	コントローラーは、デフォルトの SATA AHCI モードにリセットされます。すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。接続されたすべての SATA ドライブを以下のようにサニタイズする必要があります。
SATA HDD[41]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）	CRYPTO SCRAMBLE EXT コマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。
	シングルパスの ATA SANITIZE with OVERWRITE EXT オプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターがゼロで上書きされます。キャッシュ内のすべての旧データもアクセスできなくなります。
SATA SSD[42]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）	CRYPTO SCRAMBLE EXT コマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。
	シングルパスの ATA SANITIZE with BLOCK ERASE オプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロック内の旧データは元に戻すことができなくなります。キャッシュ内のすべての旧データもアクセスできなくなります。
SAS HDD[43]	シングルパスの SCSI SANITIZE with OVERWRITE EXT オプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターが上書きされます。キャッシュ内のすべてのデータもサニタイズされます。

[41] これらのドライブは、Smart アレイ SR コントローラーまたはチップセット SATA コントローラーに接続される場合があります。
[42] これらのドライブは、Smart アレイ SR コントローラーまたはチップセット SATA コントローラーに接続される場合があります。
[43] Smart アレイ SR コントローラーにのみに接続された SAS ドライブがサポートされます。

デバイス	実施される操作	結果
SAS SSD[44]	シングルパスの SCSI SANITIZE with BLOCK ERASE オプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロックがベンダー固有値に設定されます。キャッシュ内のすべてのデータもサニタイズされます。

消去プロセスが失敗するサポート済みデバイス、およびサポートされていないデバイスの消去は安全ではありません。これらのデバイスに機密データが含まれている可能性があります。消去されないデバイスを分離し、他の方法を使用してデータを削除するか、所属する組織のセキュリティポリシーに従ってデバイスを安全に破棄します。

△注記：

One-button Secure Erase プロセスの完了後に、NVRAM が正常に消去されたことにより、以下のイベントが Integrated Management Log (IML) に記録される場合があります。

「Non-Volatile Memory Corruption Detected. Configuration settings restored to defaults. if enabled, Secure Boot security settings may be lost.」

詳細は、「One-button Secure Erase プロセスの完了後、「Non-Volatile Memory Corruption Detected (不揮発性メモリの破損が検出されました)」というイベントが表示され、Integrated Management Log (IML) に記録されることがあります。」を参照してください。

[44] Smart アレイ SR コントローラーにのみに接続された SAS ドライブがサポートされます。

20. IPMI サーバーによる管理

IPMI によるサーバー管理は、サーバーを制御し、監視するための標準的な方法です。iLO ファームウェアは、以下を定義する IPMI バージョン 2.0 仕様に基づくサーバー管理を提供します。

- ファン、温度、パワーサプライなどのシステム情報の監視
- システムのリセットおよび電源オン/オフ操作などのリカバリー機能
- 温度上昇読み取りやファン障害などの異常なイベントのロギング機能
- 障害のあるハードウェアコンポーネントの特定などのインベントリ機能

IPMI 通信は、BMC と SMS に依存します。BMC は、SMS とプラットフォーム管理ハードウェアの間のインターフェースを管理します。iLO ファームウェアは BMC 機能をエミュレートし、SMS 機能が各種業界標準ツールによって提供されます。詳しくは、Intel の Web サイト http://www.intel.com/の IPMI 仕様を参照してください。

iLO ファームウェアは、SMS 通信に KCS インターフェースまたはオープンインターフェースを提供します。KCS インターフェースは、1 組の I/O マップ通信レジスタを提供します。I/O マップ SMS インターフェースのデフォルトシステムベースアドレスは、0xCA2 で、このシステムアドレスでバイトアラインされています。

KCS インターフェースは、ローカルシステムで動作する SMS ソフトウェアにアクセス可能です。互換性のある SMS ソフトウェアアプリケーションの例は、次のとおりです。

- **IPMI バージョン 2.0 Command Test Tool** - ローレベル MS-DOS コマンドラインツールです。KCS インターフェースを実装した IPMI BMC に、16 進数形式の IPMI コマンドを送信できるようにします。このツールは Intel の web サイト http://www.intel.com/からダウンロードできます。
- **IPMItool** - IPMI バージョン 1.5 および 2.0 仕様をサポートするデバイスの管理や設定するためのユーティリティです。IPMItool は、Linux 環境で使用できます。このツールは IPMItool の Web サイト http://ipmitool.sourceforge.net/index.html からダウンロードできます。
- **FreeIPMI** - IPMI バージョン 1.5 および 2.0 仕様をサポートするデバイスの管理や設定するためのユーティリティです。FreeIPMI は http://www.gnu.org/software/freeipmi/からダウンロードできます。
- **IPMIUTIL** - IPMI バージョン 1.0、1.5 および 2.0 仕様をサポートするデバイスの管理や設定するためのユーティリティです。IPMIUTIL は、次のサイトからダウンロードできます。 http://ipmiutil.sourceforge.net/

IPMI インターフェースに対する BMC をエミュレートする場合に、iLO は、IPMI バージョン 2.0 仕様にリストされている必須コマンドをすべてサポートします。SMS は、その仕様に記述された方法を使用して BMC 内で有効または無効にする IPMI 機能を決定する必要があります（たとえば、Get Device ID コマンドを使用）。

サーバーのオペレーティングシステムが動作中で iLO ヘルスドライバーが有効な場合は、KCS インターフェースを介した IPMI トラフィックがヘルスドライバーのパフォーマンスとシステム全体のヘルスに影響を与える可能性があります。KCS インターフェースを介して IPMI コマンドを実行しないでください。これはヘルスドライバーの監視に悪影響を与えることがあります。この制限には、IPMI パラメーター（たとえば、Set Watchdog Timer および Set BMC Global Enabled）

を設定または変更するあらゆるコマンドが含まれています。単にデータを返すIPMIコマンド（たとえば、Get Device ID および Get Sensor Reading）は、どれでも安全です。

Linux 環境での IPMI ツールの高度な使用方法

Linux の IPMI ツールには、IPMI 2.0 RMCP+プロトコルを使用して iLO ファームウェアと安全に通信する機能があります。これは、ipmitool lanplus プロトコル機能です。

例：iLO のイベントログを取得するには、次のように入力します。

ipmitool -I lanplus -H <iLO IP アドレス > -U < ユーザー名 > -P < パスワード> sel list

出力例：

```
1 | 03/18/2000 | 00:25:37 | Power Supply #0x03 | Presence detected | Deasserted
2 | 03/18/2000 | 02:58:55 | Power Supply #0x03 | Presence detected | Deasserted
3 | 03/18/2000 | 03:03:37 | Power Supply #0x04 | Failure detected | Asserted
4 | 03/18/2000 | 03:07:35 | Power Supply #0x04 | Failure detected | Asserted
```

21. Kerberos 認証とディレクトリサービス

この章では、Kerberos 認証、ディレクトリ認証（Active Directory）、およびディレクトリ認証（Open LDAP）を使用するように iLO を設定する方法について説明します。

ディレクトリ認証

iLO でディレクトリ認証を使用すると、以下のような利点があります。

- スケーラビリティ - ディレクトリサービスを利用して、数千のユーザーをサポートできます。
- セキュリティ - ディレクトリサービスから強力なユーザーパスワードポリシーが継承されます。ポリシーには、ユーザーパスワードの複雑度、ローテーション頻度、有効期限などがあります。
- ユーザーの責任 - 環境によっては、ユーザーが一つの iLO アカウントを共有することがあり、その場合、アクセスしたユーザーの特定が困難になります。ディレクトリ環境では多くのアカウントを作成できるため、全ユーザーに個別のアカウントを割り当てることができます。全ユーザーが自身のアカウントを使用するため、iLO にアクセスしたユーザーを特定できます。
- 集中管理 -ディレクトリサービスの管理ツールを使用して、iLO ユーザーを管理できます。
- 緊急性 - ディレクトリサーバーでのユーザーアカウント 変更が、関連付けられた iLO プロセッサーにただちに反映されます。これにより、アカウント設定変更を各 iLO に設定する必要がなくなります。
- 認証情報の簡素化 - ディレクトリに既にユーザーアカウントが登録されている場合、このユーザーアカウントとパスワードをそのまま iLO の認証に使用できます。iLO 用に新しいアカウントやパスワードを作成する必要がありません。
- 互換性 - iLO ディレクトリ認証は、Active Directory と Open LDAP をサポートします。
- 規格 - iLO ディレクトリ認証は、LDAPv2 プロトコルに基づいています。

ディレクトリ認証（Active Directory）のセットアップ

ディレクトリ統合方式を使用する場合、システムが Active Directory の前提条件に記載されているすべての前提条件を満たす必要があります。

Active Directory の前提条件

ディレクトリレベルで SSL を有効にする必要があります。SSL を有効にするためには、Active Directory にドメインの証明書をインストールします。iLO は、安全な SSL 接続でのみ、ディレクトリと通信します。
セットアップを有効にするには、少なくとも 1 人のユーザーに対するディレクトリ DN と、そのユーザーがメンバーになっているセキュリティグループの DN を持つ必要があります。

証明書サービスとは

証明書サービスは、ネットワークホストに署名済みのデジタル証明書を発行するために使用されます。証明書は、ホストとの SSL 接続を確立し、ホストが信頼されていることを確認するために使用します。

iLO が接続する各ディレクトリサービスに対し、証明書を発行する必要があります。エンタープライズ証明書サービスをインストールすると、Active Directory は、ネットワーク上のすべての Active Directory コントローラーに対して証明書を自動的に要求しインストールできます。

証明書サービスのインストール

Windows Server 2012 R2 の場合は、次の手順でインストールしてください。

1. サーバーマネージャーに移動します。
2. **[役割と機能の追加]**をクリックします。
3. **[次へ]**をクリックし、**[サーバーの役割の選択]**画面まで進みます。
4. **[Active Directory 証明書サービス]**を選択します。
5. 管理ツールのインストールを確認された場合には、**[機能の追加]**をクリックします。
6. **[次へ]**をクリックし、**[役割サービスの選択]**まで進みます。
7. 役割サービスとして**[証明機関]**のみチェックが入っていることを確認し、**[次へ]**をクリックします。
8. インストール内容を確認し、**[インストール]**をクリックします。

Windows Server 2016 の場合は、次の手順でインストールしてください。

1. サーバーマネージャーに移動します。
2. **[役割と機能の追加]**をクリックします。
3. **[役割と機能の追加ウィザード]**画面で**[次へ]**をクリックします。
4. **[インストールの種類の選択]**画面で**[役割ベースまたは機能ベースのインストール]**ラジオボタンをチェックし、**[次へ]**をクリックします。
5. **[対象サーバーの選択]**画面で、インストールするサーバーを選択し、**[次へ]**をクリックします。
6. **[サーバーの役割の選択]**画面で、[**Active Directory Federation Service**]を選択し、**[次へ]**をクリックします。
7. 役割の一覧から**[Active Directory 証明書サービス]**を選択し、**[次へ]**をクリックします。
8. **[役割と機能の追加ウィザード]**画面で管理ツールのインストールを確認された場合には、**[機能の追加]**をクリックします。
9. **[Active Directory 証明書サービス]**にチェックがついていることを確認し、**[次へ]**をクリックします。
10. **[Active Directory 証明書サービス]**のインストール設定画面まで進み、**[次へ]**をクリックし、**[役割サービスの選択]**まで進みます。
11. 役割サービスとして**[証明機関]**のみチェックが入っていることを確認し、**[次へ]**をクリックします。
12. インストール内容を確認し、**[インストール]**をクリックします。

証明書サービスの構成

Windows Server 2012 R2 の場合は、次の手順を参考に証明書サービスの構成を行ってください。この手順は設定の一例です。環境に合わせ、設定を行ってください。

1. サーバーマネージャーに移動します。
2. 右上の**[通知]**ボタン（旗アイコン）をクリックし、**[対象サーバーに Active Directory 証明書サービスを構成する]**をクリックします。
3. **[資格情報]**を確認し、**[次へ]**をクリックします。
4. **[構成する役割サービスの選択]**で**[証明機関]**にチェックを入れ、**[次へ]**をクリックします。
5. **[セットアップの種類]**で**[エンタープライズ CA]**を選択し、**[次へ]**をクリックします。
6. **[CA の種類]**で**[ルート CA]**を選択し、**[次へ]**をクリックします。
7. **[秘密キー]**で**[新しい秘密キーを作成する]**を選択し、**[次へ]**をクリックします。
8. **[CA の暗号化]**では、**[暗号化プロバイダーの選択]**に**[RSA#Microsoft Software Key Storage Provider]**を、**[この CA から発行された証明書の署名に使用するハッシュアルゴリズムを選択]**に SHA256 を選択し、**[次へ]**をクリックします。
9. **[CA の名前]**を確認し、**[次へ]**をクリックします。
10. **[有効期間]**を確認し、**[次へ]**をクリックします。
11. **[CA データベース]** を確認し、**[次へ]**をクリックします。
12. 構成内容を確認し、**[構成]**をクリックします。

Windows Server 2016 の場合は、次の手順を参考に証明書サービスの構成を行ってください。この手順は設定の一例です。環境に合わせ、設定を行ってください。

1. サーバーマネージャーを開きます。**[役割とサーバーグループ]**欄の"AD CS"をクリックします。
2. AD CS の設定画面に切り替わります。上部に"Active Directory 証明書サービスの構成が必要です"のメッセージが表示されています。右側の**[その他]**をクリックします。
3. **[すべてのサーバータスクの詳細と通知]**ダイアログが表示されます。メッセージ欄の**[操作]**列の**"対象サーバーに Active Directory 証明書サービスを構成する"**をクリックします。
4. **[AD CS の構成]**ダイアログが表示されます。**[資格情報]を**確認し、**[次へ]**をクリックします。
5. **[構成する役割サービスの選択]**画面で、**[証明機関]**チェックボックスにチェックをつけ、**[次へ]**ボタンをクリックします。
6. セットアップの種類を指定する画面で、**[スタンドアロン CA]**を選択し、**[次へ]**ボタンをクリックします。
7. CA の種類を選択します。**[ルート CA]**を選択します。
8. 秘密キーの種類を指定します。**[新しい秘密キーを作成する]**を選択します。選択後**[次へ]**ボタンをクリックします。

9. 暗号化オプションを指定します。**[暗号化プロバイダーの選択]**に**[RSA#Microsoft Software Key Storage Provider]**を、**[この CA から発行された証明書の署名に使用するハッシュアルゴリズムを選択]**に SHA256 を選択します。
10. **[CA の名前]**を確認し、**[次へ]**をクリックします。
11. **[有効期間]**を確認し、**[次へ]**をクリックします。
12. **[CA データベース]** を確認し、**[次へ]**をクリックします。
13. 構成内容を確認し、**[構成]**をクリックします。

証明書サービスの確認

iLO は SSL を使用して Active Directory と通信するため、Active Directory コントローラーで証明書を作成するかまたは証明書サービスをインストールする必要があります。組織のドメイン内のオブジェクトに対して証明書を発行することになるため、エンタープライズ CA をインストールする必要があります。

証明書サービスがインストールされていることを確認するには、**[スタート]**→**[プログラム]**→**[管理ツール]**→**[認証機関]**の順に選択します。証明書サービスがインストールされていない場合、エラーメッセージが表示されます。画面が正しく表示されれば、証明書サービスはインストールされています。そのままウィンドウを閉じてください。

自動証明書要求の設定

サーバーに対して証明書が発行されるようにするため、以下の手順に従って自動証明書要求の設定を行ってください。

1. **[スタート]**(右クリック)→**[ファイル名を指定して実行]**の順に選択し、**mmc** と入力します。
2. **[ファイル]**→**[スナップインの追加と削除]**の順に選択します。
3. スナップインを MMC に追加するには、**[グループポリシー管理エディター]** を選択し、**[追加]** をクリックします。
4. **[参照]** をクリックして、**[Default Domain Policy]** オブジェクトを選択します。**[OK]** をクリックします。
5. **[完了]** をクリックし、**[閉じる]**と **[OK]** をクリックして、残りのダイアログボックスを閉じます。
6. **[Default Domain Policy]**→**[コンピューター構成]**→**[ポリシー]**→**[Windows の設定]**→**[セキュリティの設定]**→**[公開キーのポリシー]**を展開します。
7. **[証明書の自動要求の設定]** を右クリックして、**[新規作成]**→**[証明書の自動要求]**の順に選択します。

   [証明書の自動要求のセットアップ ウィザード]が起動します。
8. **[次へ]**をクリックします。
9. **[ドメインコントローラー]**テンプレートを選択して、**[次へ]**をクリックします。
10. **[完了]**をクリックして、ウィザードを閉じます。

iLO のディレクトリ認証設定

iLO のディレクトリ認証設定は、iLO の Web インターフェースを使用してセットアップできます。これらの設定を変更できるのは、iLO の設定権限を持つユーザーのみです。iLO の設定権限を持たないユーザーは、設定値の表示だけが可能です。

前提条件
iLO の設定を構成権限

手順

1. **[Security]→[Directory]**ページに移動します。
2. **[Authentication Options]**セクションの**[LDAP Directory Authentication]**設定で、**[Use Directory Default Schema]**を選択します。
3. **[Directory Server Settings]**の**[Directory Server Address]**に Active Directory ドメインコントローラーのアドレスを設定します。IP アドレスまたは FQDN で指定することができますが、SSL 証明書の CN (Common Name)と一致させるため FQDN で指定することを推奨いたします。この場合、iLO に適切な DNS サーバーのアドレスが設定されている必要があります。
4. **[Directory Server LDAP Port]**に**[636]**を設定します。
5. **[Directory User Context 1]**に@(アットマーク)と Active Directory ドメイン名を入力します。例えばドメイン名が example.net の場合、”@example.net”と設定します。
6. **[Apply Settings]**をクリックします。この時、**[iLO Object Distinguished Name]**と**[iLO Object Password]**は空白のままにしてください。
7. 権限を設定するため、**[Administration]→[Directory Groups]**をクリックします。
8. **[New]**をクリックします。
9. 権限を付与したいユーザーが参加しているグループの名前を**[Group DN]**に設定し、**[Group Permissions]**以下で付与したい権限を設定します。設定後、**[Add Group]**をクリックします。
   [Group DN]には、グループの名前だけでなく識別名(DN)も指定可能です。識別名(DN)を指定すると、より確実にグループを一意に指定できます。例えば、Domain Users グループを設定する場合、**[Group DN]**にはグループ名”Domain Users”、または識別名(DN)”CN=Domain Users,CN=Users,DC=example,DC=net”を設定します。Active Directory グループの識別名(DN)は、ADSI エディター等で確認することができます。
   [Group SID]は空白で問題ありませんが、**[Group DN]**と組み合わせることで Active Directory のグループを絞り込むことができます。例えば、**[Group DN]**にはグループ名”Domain Users”を、**[Group SID]**には Domain Users の SID を設定することで、設定した SID を持つグループを一意に特定できます。
10. デフォルト状態では、”Administrators”グループと”Authenticated Users”グループが登録されています。必要に応じて修正、削除を行ってください。
11. ディレクトリ認証のテストを行うことができます。**[Security]→[Directory]**ページに移動し、ページ一番下にある **[Test Settings]**をクリックします。**[Test User Name]**にユーザー名を、**[Test User Password]**にパスワードを入力し、**[Start Test]**をクリックすると、ディレクトリ認証のテストが実行されます。

ユーザー名の指定方法には、次の選択肢があります。

- ユーザーログオン名@ドメイン名
- ドメイン名\ユーザーログオン名
- フルネーム（姓名・半角英数字のみ）
- 識別名(DN)

以下のようなユーザーでログインする場合の、ユーザー名指定方法の例を示します。

指定可能なユーザー名の例

- nec@example.net
- example\nec　　（\は¥キーで入力してください）
- Nippon Denki　　（姓・名の間には半角スペースを入力してください）
- CN=Nippon Denki,CN=Users,DC=example,DC=net

ディレクトリ認証（OpenLDAP）のセットアップ

OpenLDAP の前提条件

- iLO は LDAPv2 プロトコルをサポートしています。サーバー側で LDAPv2 プロトコルでの通信を許可してください。LDAPv3 プロトコルはサポートされません。
- iLO は、安全な SSL 接続を使用してサーバーと通信します。OpenLDAP サーバーで SSL 通信を有効にしてください。
- iLO はユーザーの識別に uid 属性を使用します。ユーザーには uid 属性を設定してください。
- Ldap グループの objectClass には groupOfNames を指定してください。
- グループに所属するメンバーは、Ldap グループの member 属性を使用して指定してください。1 つのグループに複数のメンバーが所属している場合、member 属性を所属ユーザーの数だけ追加してください。

iLO のディレクトリ認証設定

iLO のディレクトリ認証設定は、iLO の Web インターフェースを使用してセットアップできます。これらの設定を変更できるのは、iLO の設定権限を持つユーザーのみです。iLO の設定権限を持たないユーザーは、設定値の表示だけが可能です。

ディレクトリ認証設定

1. **[Security]→[Directory]**ページに移動します。
2. **[Authentication Options]**セクションの**[LDAP Directory Authentication]**設定で、**[Use Directory Default Schema]**を選択します。
3. **[Directory Server Settings]**の**[Generic LDAP]**を有効に変更します。
4. **[Directory Server Address]**に Ldap サーバーのアドレスを設定します。IP アドレスまたは FQDN で指定することができますが、SSL 証明書の CN (Common Name)と一致させるため FQDN で指定することを推奨いたします。この場合、iLO に適切な DNS サーバーのアドレスが設定されている必要があります。
5. **[Directory Server LDAP Port]**に”636”を設定します。
6. **[Directory User Context 1]**にユーザーが登録されている階層を指定します。iLO はここで指定された階層を検索します。複数の階層にユーザーが登録されている場合、**[Directory User Context 1]**~ **[Directory User Context 15]**まで最大 15 か所まで検索箇所を指定できます。
7. [Apply Settings]をクリックします。この時、**[iLO Object Distinguished Name]**と**[iLO Object Password]**は空白のままにしてください。
8. 権限を設定するため、**[Administration]→[Directory Groups]**をクリックします。
9. **[New]**をクリックします。
10. 権限を付与したいユーザーが参加しているグループの識別名(DN)を**[Group DN]**に設定し、**[Group Permissions]**以下で付与したい権限を設定します。設定後、**[Add Group]**をクリックします。例えば、**[Group DN]**には次のような識別名(DN)を指定します。
    ” cn=testgroup,ou=Group,dc=example,dc=net”
    [Group SID]は空白のままにしてください。
11. ディレクトリ認証のテストを行うことができます。**[Security]→[Directory]**ページに移動し、ページ一番下にある **[Test Settings]**をクリックします。**[Test User Name]**にユーザー名(UID 属性の値)を、**[Test User Password]**にパスワードを入力し、**[Start Test]**をクリックすることで、ディレクトリ認証のテストが実行されます。

ユーザー名の指定方法には、次の選択肢があります。

- ユーザー名(uid 属性の値)
- 識別名(DN)

以下のようなユーザーでログインする場合の、ユーザー名指定方法の例を示します。

 # test, People, example.net

dn: uid=test,ou=People,dc=example,dc=net

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: top

ou: People

sn: test

uid: test

cn: test

userPassword::xxxxxxxxxxxxxxxxxxxxxxxxxxxx

指定可能なユーザー名の例

1. test
2. uid=test,ou=People,dc=example,dc=net

OpenLDAP サーバー構築例（CentOS7.3 の場合）

OpenLDAP のインストール

OpenLDAP をインストールしてください。CentOS7 の場合、以下のようにして必要なパッケージをインストールすることができます。

 # yum install openldap-servers openldap-clients

OpenLDAP の初期設定

DB_CONFIG ファイルを設定します。CentOS7 の場合、デフォルトファイルが用意されていますのでこれをコピーして使用します。必要に応じて設定値を修正してください。

 # cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG

コピーした DB_CONFIG ファイルのオーナーを”ldap”に設定してください。

 # cd /var/lib/ldap
 # chown ldap:ldap DB_CONFIG

OpenLDAP を起動します。

 # systemctl start slapd

以下のコマンドを実行し、正しくデーモンが起動したことを確認してください。

 # systemctl status slapd

デーモンが正常に起動していることを確認できたら、デーモンが自動起動するように設定してください。

 # systemctl enable slapd

次に、管理用パスワードを設定します。slappasswdコマンドを使用してパスワードをハッシュ化してください。

 # slappasswd
New password: パスワードを入力します
Re-enter new password: パスワードを再度入力します
ハッシュ化されたパスワードが表示されます。

続いて、テキストエディタで以下のような rootpassword.ldif ファイルを作成します。

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: ハッシュ化されたパスワードを指定します。
先頭のハッシュ化アルゴリズムも記述してください。

以下のコマンドを実行し、管理者パスワードを設定します。

 # ldapadd -Y EXTERNAL -H ldapi:/// -f rootpassword.ldif

続いて、必要となるスキーマファイルを読み込みます。以下のようにコマンドを実行し、cosine.ldif と inetorgperson.ldif を読み込んでください。

#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
 # ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

次に、ディレクトリの設定を行います。テキストエディタで以下のような example.net.ldif ファイルを作成します。

example.net.ldif ファイル

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=example,dc=net

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=example,dc=net

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW

```

olcRootPW: ハッシュ化されたパスワードを指定します。
先頭のハッシュ化アルゴリズムも記述してください。

以下のコマンドを実行し、設定を反映します。

 # ldapmodify -Y EXTERNAL -H ldapi:/// -f example.net.ldif

続けて、テキストエディタで以下のような example.net.2.ldif ファイルを作成します。

example.net.2.ldif ファイル

```
dn: dc=example,dc=net
objectClass: top
objectClass: dcObject
objectclass: organization
o: Example
dc: example

dn: cn=Manager,dc=example,dc=net
objectClass: organizationalRole
cn: Manager
description: Manager

dn: ou=People,dc=example,dc=net
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=example,dc=net
objectClass: organizationalUnit
ou: Group
```

以下のコマンドを実行し、設定を反映します。

 # ldapadd -x -D cn=Manager,dc=example,dc=net -W -f example.net.2.ldif

OpenLDAP へのユーザー登録

ここでは、”test”ユーザーを作成します。

まず、slappasswd コマンドを使用して”test”ユーザーのパスワードをハッシュ化してください。

 # slappasswd
New password: パスワードを入力します
Re-enter new password: パスワードを再度入力します
ハッシュ化されたパスワードが表示されます。

テキストエディタで以下のような user.ldif ファイルを作成します。

user.ldif ファイル

```
dn: uid=test,ou=People,dc=example,dc=net
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
ou: People
sn: test
uid: test
cn: test
```

userPassword: ハッシュ化されたパスワードを指定します。
先頭のハッシュ化アルゴリズムも記述してください。

以下のコマンドを実行し、ユーザーを登録します。

 # ldapadd -x -D cn=Manager,dc=example,dc=net -W -f user.ldif

OpenLDAP へのグループ登録

テキストエディタで以下のような group.ldif ファイルを作成します。member 属性でグループに所属するユーザーを指定します。

group.ldif ファイル

```
dn: cn=testgroup,ou=Group,dc=example,dc=net
objectClass: groupOfNames
cn: testgroup
member: uid=test,ou=People,dc=example,dc=net
```

以下のコマンドを実行し、グループを登録します。

 # ldapadd -x -D cn=Manager,dc=example,dc=net -W -f group.ldif

OpenLDAP の SSL 通信設定

まずは証明書を作成します。/etc/pki/tls/certs ディレクトリへ移動し、以下のようにコマンドを実行して証明書を作成してください。

 # cd /etc/pki/tls/certs

 # make server.key
*umask 77 ; *
/usr/bin/openssl genrsa -aes128 2048 > server.key
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase: パスフレーズを設定してください
Verifying - Enter pass phrase: パスフレーズを再入力してください

 # openssl rsa -in server.key -out server.key
Enter pass phrase for server.key: パスフレーズを入力してください
writing RSA key

 # make server.csr
*umask 77 ; *
/usr/bin/openssl req -utf8 -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:JP
State or Province Name (full name) []:Kanagawa
Locality Name (eg, city) [Default City]:Kawasaki
Organization Name (eg, company) [Default Company Ltd]:NEC

Organizational Unit Name (eg, section) []:IT Platform Division
Common Name (eg, your name or your server's hostname) []:ldap.example.net
Email Address []:root@ldap.example.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: 何も入力せずにエンターキーを押してください
*An optional company name []:*何も入力せずにエンターキーを押してください

 # openssl x509 -in server.csr -out server.crt -req -signkey server.key
Signature ok
subject=/C=JP/ST=Kanagawa/L=Kawasaki/O=NEC/OU=IT Platform Division/CN=ldap.example.net/emailAddress=root@ldap.example.net
Getting Private key

作成した証明書とデフォルトのルート証明書を OpenLDAP の証明書ディレクトリへ格納します。

 # cp /etc/pki/tls/certs/server.key /etc/openldap/certs/
 # cp /etc/pki/tls/certs/server.crt /etc/openldap/certs/
 # cp /etc/pki/tls/certs/ca-bundle.crt /etc/openldap/certs/

作成した証明書を使い、SSL 通信を行うように設定を変更します。

テキストエディタで以下のような ssl.ldif ファイルを作成します。

ssl.ldif ファイル

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/openldap/certs/ca-bundle.crt

replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/server.crt

replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/server.key
```

以下のコマンドを実行し、設定を反映します。

 # ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl.ldif

次に、テキストエディタで/etc/sysconfig/slapd ファイルを開きます。ファイルに以下のような記載がされている行があります。

SLAPD_URLS="ldapi:/// ldap:///"

この行に以下のように”ldaps:///”を追加し、ファイルを保存してください。

SLAPD_URLS="ldapi:/// ldap:/// ldaps:///"

設定変更を反映させるため、デーモンを再起動します。

 # systemctl restart slapd

LDAPv2 プロトコルを使用してアクセスすることができるように、Ldap サーバーを設定します。
テキストエディタで以下のような ldapv2.ldif ファイルを作成します。

dn: cn=config
add: olcAllows
olcAllows: bind_v2

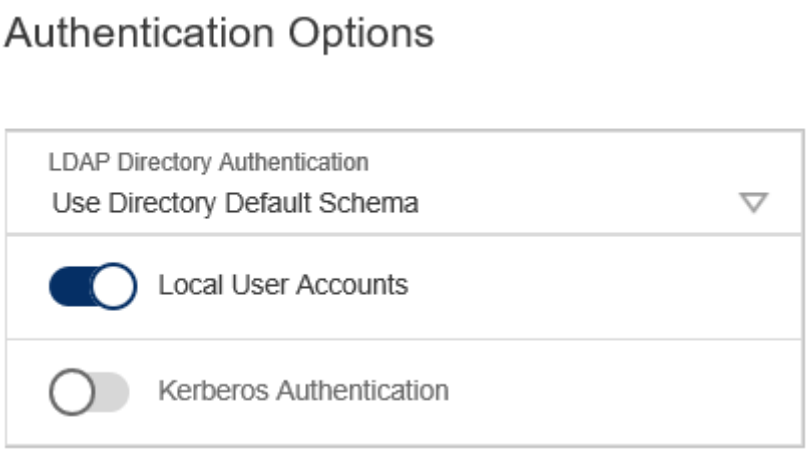
以下のコマンドを実行し、設定を反映します。

 # ldapmodify -Y EXTERNAL -H ldapi:/// -f ldapv2.ldif

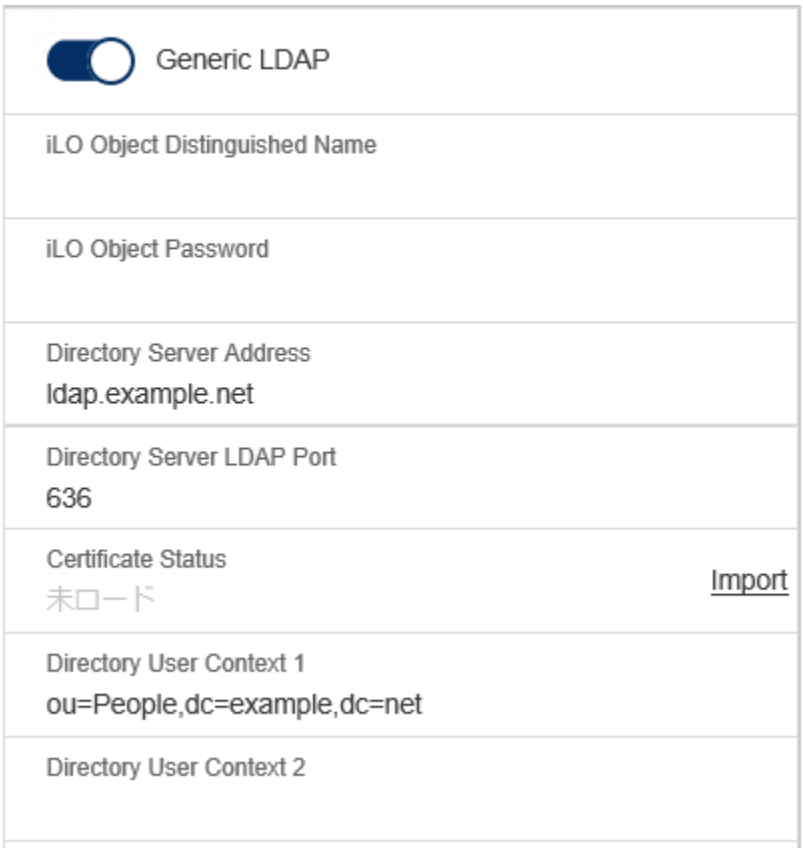
設定変更を反映させるため、デーモンを再起動します。

 # systemctl restart slapd

iLO 設定例（OpenLDAP サーバー構築例で設定したサーバーを使用する場合）



Directory Server Settings



Kerberos 認証

Kerberos がサポートされていることにより、クライアントがドメインにログインしており、ユーザーが iLO で設定されているディレクトリグループのメンバーである場合、このユーザーは、ユーザー名とパスワードを入力せずに iLO にログインできます。ワークステーションがドメインにログインしていない場合でも、ユーザーは、Kerberos ユーザー名とドメインパスワードを使用して iLO にログインできます。Kerberos サポートは、Web インターフェース、iLO RESTFul API、または SSH（SMASH CLP）によって設定できます。

iLO とドメイン間の信頼関係はユーザーサインオンの前にシステム管理者によって確立されるため、（Two-Factor 認証を含む）任意の形式の認証がサポートされます。Two-Factor 認証をサポートするようにユーザーを設定する手順については、サーバーオペレーティングシステムのドキュメントを参照してください。

前提条件

Active Directory 環境を設定し、iLO でディレクトリ認証が正常に動作することを確認してください。

正常に認証できることを確認後、iLO のホスト名とドメイン名を設定してください。

以下の点に注意してください。

- iLO ドメイン名の値は、Kerberos のレルム名に対応する必要があります。詳しくは、「レルム名」を参照してください。
- キータブの生成に使用する iLO ホスト名は、設定されている iLO ホスト名と同じである必要があります。iLO ホスト名は、大文字と小文字が区別されます。詳しくは、「キータブの生成」を参照してください。
- ドメインコントローラーと iLO の時刻が同期されている必要があります。

手順

1. **[iLO Dedicated Network Port]→[IPv4]**ページに移動します。
2. 次のチェックボックスの選択を解除して、**[Submit]**をクリックします。
   - DHCPv4 のドメイン名の使用
   - DHCPv4 の DNS サーバーの使用
3. **[IPv6]** タブをクリックします。
4. 次のチェックボックスの選択を解除して、**[Submit]**をクリックします。
   - DHCPv6 のドメイン名の使用
   - DHCPv6 の DNS サーバーの使用
5. **[General]**タブをクリックします。
6. 次の値を更新して、**[Submit]**をクリックします。
   - オプション：**[iLO Subsystem Name (Hostname)]** 値を更新します。
     iLO ホスト名では大文字と小文字が区別されます。この名前は、キータブファイルの作成時に使用されます。
   - **[Domain Name]**の値を更新します。
     この値は、Kerberos のレルム名と一致する必要があります。Kerberos のレルム名は、

通常、大文字に変換されたドメイン名です。詳しくは、「レルム名」を参照してください。

7. **[SNTP]**タブをクリックします。
8. 次の値を更新して、**[Apply]**をクリックします。
   - ドメインコントローラーが SNTP サービスを提供している場合、**[Primary Time Server]**にドメインコントローラーのアドレスを設定することを推奨いたします。ドメインコントローラーが SNTP サービスを提供していない場合、ネットワーク内に存在する SNTP サーバーのアドレスを設定してください。なお、ドメインコントローラーまたは SNTP サーバーのアドレスを手動で設定する場合は、**[Use DHCPv4 Supplied Time Settings]**および**[Use DHCPv6 Supplied Time Settings]**の設定を無効にしてください。DHCP サーバーが適切な SNTP サーバーのアドレスを配信している場合、これらの設定を有効に設定することもできます。この場合 SNTP サーバーのアドレスが自動的に設定されるため、**[Primary Time Server]**および**[Secondary Time Server]**を手動で入力する必要はありません。
   - **[Time Zone]**に適切なタイムゾーンを設定してください。**[Use DHCPv4 Supplied Time Settings]**を有効にした場合は、**[Time Zone]**で指定されたタイムゾーン設定は設定できません。DHCP サーバー側で SNTP サーバーのアドレスと UTC オフセットを配信してください。iLO は DHCP サーバーから受け取った SNTP サーバーアドレスと UTC オフセットを使用して時刻同期を行います。
9. **[Reset iLO]**をクリックして、iLO を再起動します。

ドメインコントローラーの準備

Windows Server 環境では、Kerberos はドメインコントローラーによってサポートされています。

レルム名

DNS ドメインの Kerberos レルム名は、通常、大文字に変換されたドメイン名です。

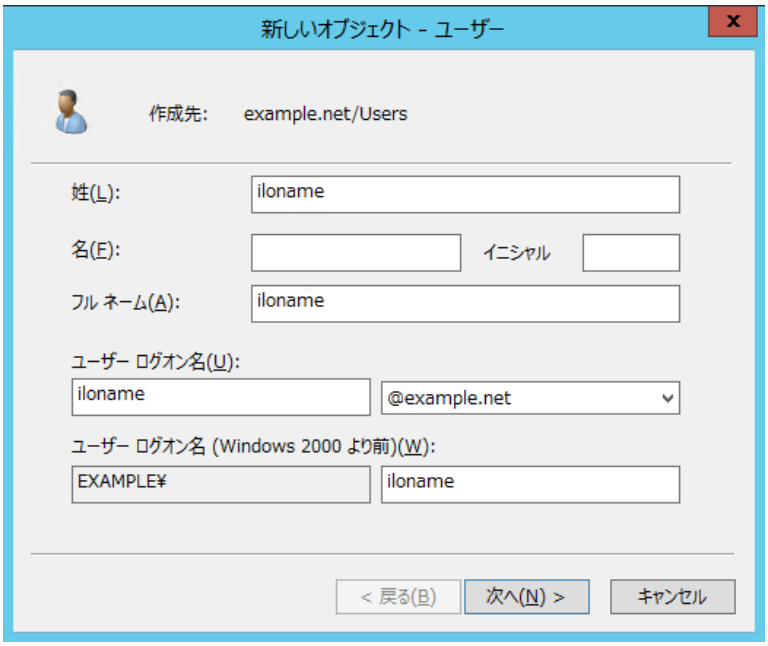
例：

- 親ドメイン名：example.net
- Kerberos レルム名：EXAMPLE.NET

iLO アカウント

各 iLO ごとにアカウントをドメインディレクトリに作成し、有効化する必要があります。Windows の場合は、**[Active Directory** ユーザーとコンピューター**]**スナップインで iLO のホスト名をユーザー名としたユーザーアカウントを作成します。以下に例を示します。

- ユーザーログオン名：iloname　（iLO ホスト名）
- ドメイン名：example.net
- パスワード：任意の文字列



ユーザーアカウント

ユーザーアカウントは、iLO にログインする各ユーザーについて、ドメインディレクトリに存在し、有効になっている必要があります。

キータブの生成

続いて、Windows 環境で iLO のキータブファイルを生成します。

キータブの生成に使用する iLO ホスト名は、設定されている iLO ホスト名と同じである必要があります。iLO ホスト名は、大文字と小文字が区別されます。

1. ktpass コマンドを使用して、キータブを生成し、共有秘密を設定します。コマンドは、大文字と小文字が区別され、特殊文字が含まれます。以下に例を示します。
   - ✧ iLO ホスト名：iloname
   - ✧ ドメイン名：example.net
   - ✧ Kerberos レルム名：EXAMPLE.NET

   ktpass -out iloname.keytab +rndPass -ptype KRB5_NT_SRV_HST -mapuser iloname@example.net -princ HTTP/iloname.example.net@EXAMPLE.NET

   出力は、次のようなものになります。

   Targeting domain controller: domaincontroller.example.net
   Successfully mapped HTTP/iloname.example.net to iloname.
   Password successfully set!
   WARNING: pType and account type do not match. This might cause problems.
   Key created.
   Output keytab to iloname.keytab:
   Keytab version: 0x502

keysize 71 HTTP/iloname.example.net@EXAMPLE.NET ptype 3
(KRB5_NT_SRV_HST) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0xfbc6266b74f09e691360d18968616948)

注記**:** ktpass には、-kvno オプションを使用しないでください。このオプションを使用すると、キータブファイルの knvo と Active Directory の kvno が同期しなくなります。
iLO で、高度なセキュリティ、FIPS、または CNSA セキュリティ状態を使用するように構成されている場合、-crypto <encryption>で AES Kerberos キータイプを使用する必要があります。

---

2. SetSPN コマンドを使用して、SPN を登録します。

   例：SetSPN -A HTTP/iloname.example.net iloname

   既に登録されている場合には、SetSPN コマンドでエラーメッセージが表示されます。この場合はエラーを無視して先に進んでください。

   例：重複する SPN が見つかりました。操作を中止します

3. SetSPN -L iloname コマンドを使用して、iLO の SPN および DN を表示します。

   HTTP/iloname.example.net サービスが表示されることを確認します。

注記**:** SetSPN コマンドでは、UPN を設定できないことに関するメッセージが表示される場合があります。これは、iLO がユーザーではなくサービスであるため、問題ありません。コンピューターオブジェクトで、パスワード変更を確認するように求められる場合があります。**[OK]** をクリックしてウィンドウを閉じ、キータブファイルの作成を続行します。

---

4. 生成したキータブ（.keytab ファイル）を手元の PC へコピーしておきます。

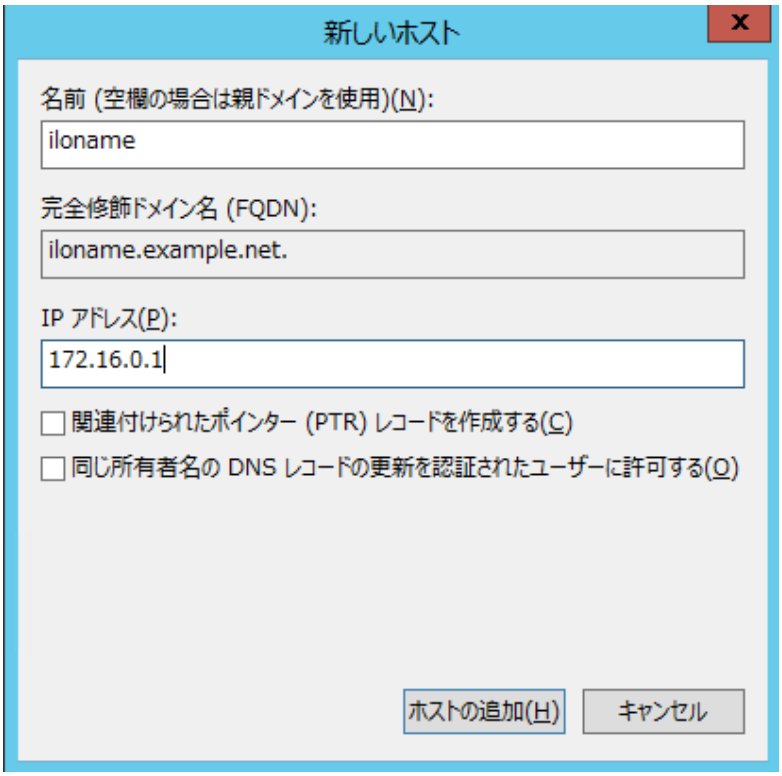
キーバージョン番号

ドメインコントローラー OS が再インストールされると、キーバージョン番号がリセットされます。この場合、ドメインコントローラーに関連付けられるデバイスに対して iLO が使用するキータブファイルを生成しなおして、再インストールする必要があります。

DNS サーバーの設定

DNS サーバーの設定を開き、iLO ホスト名が登録されているか確認します。DNS サーバーで動的更新が有効に設定されており、iLO で[Enable DDNS Server Registration]が有効に設定されている場合、iLO 起動時に iLO ホスト名が DNS サーバーに自動的に登録されます。動的更新を使用しない場合は、手動で iLO ホスト名を DNS サーバーに登録します。以下に例を示します。

- iLO ホスト名：iloname
- iLO 専用ネットワークポート：172.16.0.1



ユニバーサルおよびグローバルユーザーグループ（権限付与）

iLO で権限を設定するには、ドメインディレクトリにグループを作成する必要があります。iLO にログインするユーザーには、そのユーザーがメンバーとなっているすべてのグループの権限が全て付与されます。権限の設定には、グローバルユーザーグループおよびユニバーサルユーザーグループのみを使用できます。ドメインローカルグループは、サポートされていません。

iLO Web インターフェースを使用した Kerberos ログイン用の iLO の設定

1. ご使用の環境が、Kerberos ログインの要件を満たしていることを確認します。
2. **[Security]→[Directory]**ページに移動し、以下の Kerberos 固有パラメーターを設定します。
   - **[Kerberos Authentication]**
   - **[Kerberos Realm]**
   - **[Kerberos KDC Server Address]**
   - **[Kerberos KDC Server Port]**
   - **[Kerberos Keytab]**　（先ほど生成したキータブファイルをアップロードします）
3. **[Administration]→[Directory Groups]**ページに移動し、ディレクトリグループを設定します。各ディレクトリグループでは、DN、SID、および権限を設定します。Kerberos ログインの場合、ユーザーがメンバーになっているグループの SID が、iLO で設定されているディレクトリグループの SID と比較されます。**iLO にはディレクトリグループの SID も必ず設定してください。SID が設定されていない場合、Kerberos を使用したログインができません。**ユーザーが複数のディレクトリグループに参加している場合、ユーザーが参加しているすべてのグループの権限が全て付与されます。

   権限の設定には、グローバルグループおよびユニバーサルグループのみを使用できます。

ドメインローカルグループは、サポートされていません。

4. **[iLO Dedicated Network Port]**または**[iLO Shared Network Port]**→**[SNTP]**ページに移動します。Kerberos 認証が正常に機能するためには、iLO、KDC、およびクライアントワークステーションの間で日付と時刻が同期している必要があります。iLO の SNTP 設定を有効にして iLO がネットワークから正確な日付および時刻を取得するようにしてください。

詳細情報
前提条件
iLO のユーザーアカウント
iLO の概要情報の表示
SNTP の設定

時間要件

Kerberos で正常にログインするには、以下の日付と時間が互いに 5 分以内で設定されている必要があります。

- iLO
- Web ブラウザーを実行するクライアント PC
- 認証を実行するサーバー

SNTP を使用し、時刻同期を行ってください。iLO Web インターフェースの**[Overview]**画面に表示される**[iLO Date/Time]**が正しいことを確認してください。

サポートされるブラウザーでのシングルサインオンの設定

ユーザーが iLO にログインするには、権限が割り当てられたグループのメンバーになっている必要があります。Windows クライアントの場合、ワークステーションのロックまたはロック解除によって、iLO に使用される認証情報が更新されます。Home バージョンの Windows オペレーティングシステムは、Kerberos でのログインをサポートしていません。

Internet Explorer でのシングルサインオンの有効化

iLO に関して Active Directory が適切に設定されており、Kerberos ログインに関して iLO が適切に設定されている場合には、この手順によって、シングルサインオンによるログインが有効になります。

この手順は、Internet Explorer 11 に基づいています。

プロセスの概要：

1. 「Internet Explorer での認証の有効化」
2. 「イントラネットゾーンへの iLO ドメインの追加」
3. 「[イントラネットゾーンでのみ自動的にログオンする] 設定の有効化」
4. オプションを変更した場合は、Internet Explorer を閉じて再起動します。
5. 「シングルサインオン（Zero サインイン）設定の確認」

Internet Explorer での認証の有効化

1. **[ツール]→[インターネットオプション]**の順に選択します。
2. **[詳細設定]**タブをクリックします。
3. **[セキュリティ]**セクションまでスクロールします。
4. **[統合 Windows 認証を有効にする]**が選択されていることを確認します。
5. **[OK]** をクリックします。

イントラネットゾーンへの iLO ドメインの追加

1. **[ツール]→[インターネットオプション]**の順に選択します。
2. **[セキュリティ]**タブをクリックします。
3. **[ローカルイントラネット]**アイコンをクリックします。
4. **[サイト]**ボタンをクリックします。
5. **[詳細設定]**ボタンをクリックします。
6. **[この Web サイトをゾーンに追加する]**ボックスに、iLO のホスト名・iLO の DNS ドメイン名を入力します。ワイルドカードを使用し、*.example.net のように iLO の DNS ドメイン名のみを指定することも可能です。
7. **[追加]**をクリックします。
8. **[閉じる]**をクリックします。
9. **[OK]** をクリックして **[ローカルイントラネット]**ダイアログボックスを閉じます。
10. **[OK]** をクリックして **[インターネットオプション]**ダイアログボックスを閉じます。

[イントラネットゾーンでのみ自動的にログオンする] 設定の有効化

1. **[ツール]→[インターネットオプション]**の順に選択します。
2. **[セキュリティ]**タブをクリックします。
3. **[ローカルイントラネット]**アイコンをクリックします。
4. **[レベルのカスタマイズ]**をクリックします。
5. **[ユーザー認証]**セクションまでスクロールします。
6. **[イントラネットゾーンでのみ自動的にログオンする]**オプションが選択されていることを確認します。
7. **[OK]** をクリックして **[セキュリティ設定 - ローカルイントラネットゾーン]**ウィンドウを閉じます。
8. **[OK]** をクリックして **[インターネットオプション]**ダイアログボックスを閉じます。

Firefox でのシングルサインオンの有効化

iLO に関して Active Directory が適切に設定されており、Kerberos ログインに関して iLO が適切に設定されている場合には、以下の手順によって、シングルサインオンによるログインが有効になります。

1. ブラウザーの場所ツールバーに about:config と入力して、ドメインの設定ページを開きます。動作保証対象外になります! というメッセージが、表示された場合は、[細心の注意を払って使用する]ボタンを クリックします。
2. **[検索]**ボックスに **network.negotiate** と入力します。
3. network.negotiate-auth.trusted-uris をダブルクリックします。

4. iLO の DNS ドメイン名を入力し（たとえば、example.net）、**[OK]** をクリックします。
5. 設定をテストします。詳しくは、「シングルサインオン（Zero サインイン）設定の確認」を参照してください。

Chrome でのシングルサインオンの有効化

Chrome での設定は必要ありません。

シングルサインオン（Zero サインイン）設定の確認

1. iLO ログインページ（例：https://iloname.example.net）にアクセスします。
2. **[Zero Sign In]**ボタンをクリックします。
3. 認証情報の入力を求めるメッセージが表示される場合は、Kerberos 認証に失敗しており、システムは NTLM 認証に戻っています。**[キャンセル]**をクリックして、「サポートされるブラウザーでのシングルサインオンの設定」の手順を繰り返してください。また、iLO のディレクトリ認証設定が正しく設定されているか確認してください。

名前によるログインが動作していることの確認

iLO のコンピューターアカウントが子ドメインに含まれている場合に、Kerberos の設定パラメーター（**[Kerberos Realm]**、**[Kerberos KDC Server Address]**、**[Kerberos KDC Server Port]**）が親ドメインを参照していると、名前によるログインが正常に機能しない場合があります。

1. iLO ログインページ（例：http://iloname.example.net）にアクセスします。
2. Kerberos SPN 形式のユーザー名（例：nec@EXAMPLE.NET）を入力します。
3. 関連付けられているドメインパスワードを入力します。
4. Kerberos 認証が失敗すると、認証情報の入力が求められます。**[キャンセル]**をクリックして、ダイアログボックスを閉じます。
   設定を確認し、もう一度やり直してください。

22. iLO の再起動、工場出荷時リセット、NMI の管理

iLO の再起動（リセット）

場合によっては、iLO を再起動しなければならないことがあります。たとえば、iLO がブラウザーに応答しない場合などです。

iLO を再起動しても構成が変更されることはありませんが、iLO へのアクティブな接続がすべて終了します。

ファームウェアファイルのアップロードが進行中の場合、アップロードは強制的に終了します。ファームウェアのフラッシュが進行中の場合、このプロセスが終了するまで iLO をリセットできません。

iLO を再起動するには、次のいずれかの方法を使用します。

- iLO の Web インターフェースの**[Information]**→**[Diagnostics]**ページで、**[Reset]**をクリックします。
- BMC 構成ユーティリティを使用します。
- サポートされている NX7700x サーバで UID スイッチを使用します。
- CLI(SMASH CLP)を使用します。手順については、iLOスクリプティング/コマンドラインガイドを参照してください。
- iLO RESTful APIを使用します。詳しくは、iLOスクリプティング/コマンドラインガイドを参照してください。
- IPMI を使用します。詳しくは、iLO スクリプティング/コマンドラインガイドを参照してください。

これらのどの方法も利用できないか、予想どおりに機能しない場合は、サーバーの電源を切り、電源装置を完全に切断する必要があります。

詳細情報

iLO 診断

重要:

- POST(Power On Self Test)実行中は、iLO のリセットを行わないようにしてください。
- iLO のリセットを行うと、iLO の時刻が過去の時刻に戻ってしまう場合があります。Web インターフェースで NTP 設定をして頂くことを推奨します。

iLO のリセット（BMC 構成ユーティリティ）

前提条件

iLO の設定を構成権限

手順

1. オプション：サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーの POST 画面で **F9** キーを押して、システムユーティリティを起動します。
4. システムユーティリティの画面で、**[システム構成]**→**[BMC 構成ユーティリティ]**→**[BMC をリセット]**を選択します。
   BMC 構成ユーティリティに、**[はい]**または**[いいえ]**を選択する画面が表示されます。
5. **[はい]**を選択します。
6. リセットを確認するメッセージが表示されたら、**[OK]**をクリック、または**[Enter]**キーを押します。

   iLO がリセットされ、すべてのアクティブな接続が終了します。iLO をリモートで管理している場合は、リモートコンソールセッションが自動的に終了します。

   iLO をリセットすると、次の再起動まで BMC 構成ユーティリティを使用できなくなります。
7. ブートプロセスを再開します。
   a. オプション：iLO をリモート管理している場合は、iLO のリセットが完了するのを待ってから、iLO リモートコンソールを起動します。

      以前のセッションのシステムユーティリティがまだ開いています。
   b. 変更が保留中の確認メッセージが表示されたら**[Yes – Save Changes]**をクリックします。
   c. **[終了]**をクリックするか、メインメニューが表示されるまで、**[Esc]**キーを押します。
   d. メインメニューで、要求の確認を求めるメッセージが表示されたら、**[OK]**を選択し、**[Enter]**キーを押します。
   e. **[Reboot]**キーを押してユーティリティを終了し、通常のブートプロセスを再開します。

サーバーの UID スイッチを使用した iLO の再起動

NX7700x サーバ上の UID スイッチ（搭載装置のみ）を使用して iLO の手動再起動を開始できます。

iLO の再起動は 2 種類あります。

- 安全な **iLO** 再起動 - iLO の再起動は、iLO ファームウェアによって行われます。この機能を使用するには、UID スイッチを 5 秒間から 9 秒間押し続けます。

  UID スイッチ/ランプが青色で毎秒 4 回点滅し、安全な iLO 再起動が実行中であることを示します。

  安全な iLO 再起動を開始しても構成が変更されることはありませんが、iLO へのアクティブな接続がすべて終了します。ファームウェアファイルをアップロード中の場合は、処理は終了されます。ファームウェアのフラッシュが進行中の場合、このプロセスが終了するまで iLO を再起動できません。

- ハードウェア **iLO** 再起動 - iLO の再起動は、ハードウェアによって行われます。この機能を使用するには、UID スイッチを 10 秒間以上押し続けます。

  UID スイッチ/ランプが青色で毎秒 8 回点滅し、ハードウェア iLO 再起動が実行中であることを示します。

△ 注意: ハードウェア iLO 再起動を開始しても構成が変更されることはありませんが、iLO へのアクティブな接続がすべて終了します。ファームウェアのアップデート実行中にハードウェア iLO 再起動を開始した場合、フラッシュデバイスのデータが破損する可能性があります。

ハードウェアの iLO の再起動中にデータの損失や NVRAM の破損が発生する場合があります。

トラブルシューティングの他のオプションが使用可能な場合は、ハードウェアの再起動を開始しないでください。

UID スイッチについて詳しくは、本体装置のユーザーガイドを参照してください。

iLO の工場出荷時デフォルト設定へのリセット

場合によっては、iLO を工場出荷時のデフォルト設定にリセットする必要があることがあります。たとえば、FIPS モードを無効にすると、iLO をデフォルト設定にリセットする必要があります。システムユーティリティを使用してこのタスクを実行できます。

工場出荷時デフォルト設定への iLO のリセット（BMC 構成ユーティリティ）

△ 注意: iLO を出荷時のデフォルト設定にリセットすると、ユーザーデータ、ライセンスキー(拡張ライセンス)、構成設定、ログなど、すべての iLO 設定が消去されます。工場出荷時にライセンスキーがインストールされている場合には、ライセンスキーは保持されます。

この手順はログ内のすべてのデータを消去するため、リセットに関連するイベントは iLO イベントログと統合管理ログに記録されません。

1. サーバーを再起動するかまたは電源を入れます。
2. サーバーの POST 画面で**[F9]**キーを押して、システムユーティリティを起動します。
3. システムユーティリティ画面で、**[システム構成]**→**[BMC 構成ユーティリティ]**→**[工場出荷時のデフォルトにセット]**を選択し、**[Enter]**キーを押します。

   BMC 構成ユーティリティに、**[はい]**または**[いいえ]**を選択する画面が表示されます。
4. **[**はい**]**を選択します。
5. 要求を確認するメッセージが表示されたら、**[Enter]**キーを押します。

   iLO が工場出荷時のデフォルト設定にリセットされます。iLO をリモートで管理している場合は、リモートコンソールセッションが自動的に終了します。次にシステムを再起動するまで BMC 構成ユーティリティに再びアクセスすることはできません。
6. ブートプロセスを再開します。
   a. 変更が保留中の確認メッセージが表示されたら**[Yes – Save Changes]**をクリックします。
   b. **[終了]**をクリックするか、メインメニューが表示されるまで、**[Esc]**キーを押します。
   c. メインメニューで、要求の確認を求めるメッセージが表示されたら、**[OK]**を選択し、**[Enter]**キーを押します。
   d. **[Reboot]**キーを押してユーティリティを終了し、通常のブートプロセスを再開します。

NMI の生成

診断ページの **Non-Maskable Interrupt (NMI) Button** セクションにある **NMI** 生成機能で、オペレーティングシステムをデバッグのために停止できます。

△ 注意: 診断とデバッグのツールとしての NMI 生成機能は、主にオペレーティングシステムが使用不能になった場合に使用します。通常のサーバーの運用では、NMI 生成機能は使用しないでください。NMI ではオペレーティングシステムは適切にはシャットダウンされず、オペレーティングシステムがクラッシュします。このため、サービスとデータは失われます。**[Generate NMI to System]**ボタンは、オペレーティングシステムが正常に動作せず、調査する場合にのみに使用してください。

前提条件
仮想電源およびリセット権限

手順

1. **[Information]→[Diagnostics]**ページに移動します。
2. **[Generate NMI to System]**をクリックします。

3. NMI をシステムに生成するとデータが消失する可能性があるという警告が表示された場合は、**[OK]**をクリックして確認するか、**[キャンセル]**をクリックします。

   [OK]をクリックすると、iLO は NMI が送信されたことを確認します。

23. トラブルシューティング

この章では、iLO を使用したサーバートラブルの解決方法と iLO に関するトラブルシューティングを紹介します。

カーネルデバッグ

クライアント PC から Windows Windbg カーネルデバッガーを使用して、Windows サーバーのデバッグを実行できます。この方法では、iLO 仮想シリアルポート機能を使用します。

前提条件

PuTTY がクライアント PC にインストールされている。

PuTTY は Web サイト **http://www.putty.org/** からダウンロードできます。

手順

1. デバッグ対象である Windows サーバーの iLO Web インターフェースから、**[**Security**]**→**[**Access Settings**]**ページに移動して、**[**Serial Command Line Interface Speed**]**を設定します。
2. デバッグ対象である Windows サーバーのデバッグオプションを設定します（シリアル接続の boot.ini パラメーター）。 debugport = com2 を使用して、iLO Web インターフェースで構成された **[**Serial Command Line Interface Speed**]**と一致するようにボーレートを設定します。
3. サーバーを再起動します。
4. POST 実行中に **F9** キーを押して、UEFI システムユーティリティを開始します。
5. UEFI システムユーティリティで、次の設定を構成します。
   - EMS および BIOS シリアルコンソールを無効にします。
   - 仮想シリアルポートを COM 2 に設定します。

   UEFI システムユーティリティの使用方法については、UEFI システムユーティリティユーザーガイドを参照してください。
6. サーバーを再起動し、Windows のブートオプションの選択メニューを表示します。
7. クライアント PC から、PuTTY を使用して iLO に接続し、ログインします。

   この接続は、iLO への CLI を用いた 接続になります。
8. セッションホスト名に IP アドレスを入力し、デフォルト設定を使用して iLO に接続します。セッションが開くと、ログイン画面が表示されます（SSH キーを用いたログインをしない場合）。詳しくは、「iLO セキュリティの設定」および「SSH キーの管理」を参照してください。
9. プロンプトが表示されるまでに少し時間がかかる場合があります。
10. </>iLO-> プロンプトで、以下のコマンドを入力します。

    windbg_enable

    これにより、ポート 3002 で仮想シリアルポートへのデバッグソケットが開きます。
11. 以下のコマンドを入力して Windows デバッガーを起動します。

    windbg -k com:port=<IP-address>,ipport=3002

<IP-address> は iLO の IP アドレス、「3002」は接続するソケット（3002 は iLO の Raw シリアルデータソケット）です。

ipport パラメーターは省略可能です。デフォルトのポートは、3002 です。
必要に応じて、その他の windbg コマンドラインパラメーターを追加することができます。初期ブレークポイントのための -b パラメーターを使用することをおすすめします。

12. サーバーコンソール（または iLO リモートコンソール）上で、ブートオプションとしてデバッグモードを選択し、デバッグモードで Windows を起動します。

    これには、数分かかる場合があります。

13. ホストサーバーのデバッグを完了したら、PuTTY を使用して CLI で iLO に接続し、以下のコマンドを入力して、仮想シリアルポートへのデバッグソケットをオフにします。

    windbg_disable

注記: iLO デバッグソケットが有効になっているかぎり、Windows デバッガーへの接続の切断および再接続が可能です。

Server Health Summary の使用

サーバー電源の状態（パワーオン / パワーオフ）にかかわらず、iLO を使用することでサーバーモニターに診断情報（Server Health Summary）を表示することができます。この機能は、サーバーが起動しないとき等の問題解決に役立ち、IP アドレス等の情報を確認することができます。

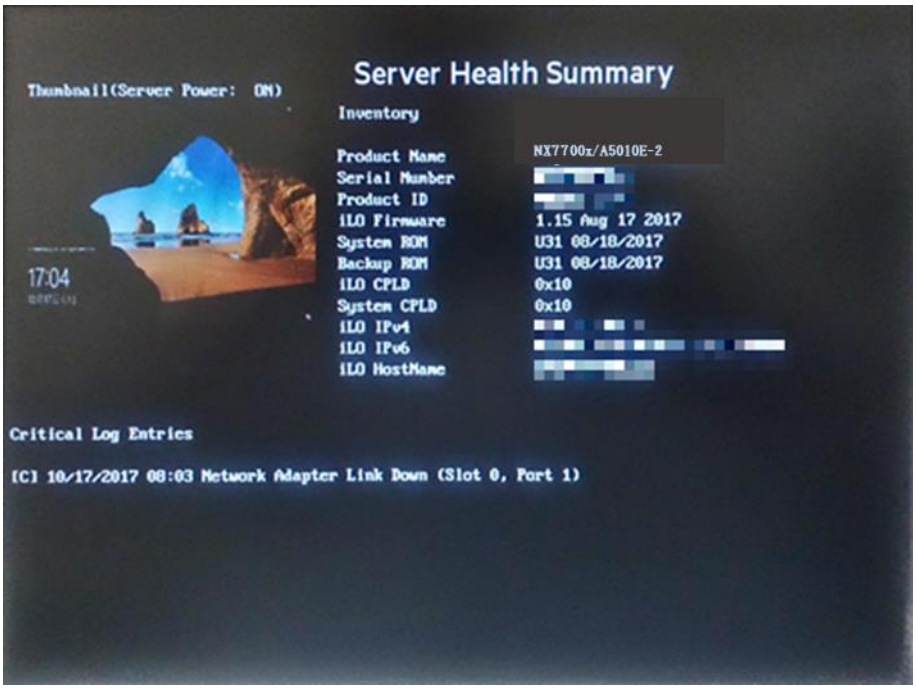
サーバーがモニターに接続されており、UID スイッチがあるサーバーで使用することができます。

1. 次のいずれかを実行します。

   - サーバー上の UID スイッチを押します。

△ 注意: この機能を使用するには、UID スイッチを押して放します。5 秒間から 9 秒間押し続けると安全な iLO 再起動、10 秒間以上押し続けるとハードウェア iLO 再起動が開始されるため、iLO の再起動が開始されないよう注意してください。ハードウェア iLO 再起動では、データの損失や NVRAM の破損が発生する場合があります。

   - iLO Web インターフェースにログインし、UID の状態を **[UID ON]**に変更します。iLO Web インターフェースィンドウの右上にある UID アイコンをクリックすることで状態を変更できます。



[Server Health Summary] 画面を閉じるには、UID の状態を **[UID OFF]**にします。iLO の再起動中は**[Server Health Summary]**は表示されません。

Server Health Summary の詳細

Server Health Summary を表示すると、以下の情報が表示されます。

- サーバーモデル名
- サーバーシリアル番号
- 製品 ID
- iLO ファームウェアのバージョン
- システム ROM のバージョン
- システム ROM (バックアップ) のバージョン
- iLO CPLD のバージョン
- システム CPLD のバージョン
- 内蔵 Smart アレイのファームウェアバージョン- サーバーの POST が正常に完了した後にのみ表示されます
- iLO の IP アドレス（IPv4 および IPv6）- これは、iLO の**[**Security**]**→**[Access Settings]**ページで **[**Show iLO IP during POST**]**が **[**有効**]**に設定されている場合のみ表示されます。
  詳しくは、「iLO アクセスの設定」を参照してください。
- iLO ホスト名
- iLO サービスポート(IP アドレス、サブネットマスク)
- クリティカルログ - IML から最新の **[**Critical**]** イベントが表示され、最新のイベントから順に表示されます。

イベントログエントリーのタイムスタンプが正しくない

症状

イベントログエントリーの日付または時刻が正しくない。

原因

NTP サーバーアドレスまたはタイムゾーンが正しく設定されていません。

操作

SNTP 設定が正しく構成されていることを確認します。

詳しくは、「SNTP の設定」および「iLO タイムゾーン設定」を参照してください。

ログインと iLO アクセスの問題

ログイン名とパスワードが受け付けられない

症状

iLO へのログインに失敗する。

解決方法 1

原因

入力されたユーザーアカウント情報が誤っています。

操作正しいログイン情報を入力します。以下の点に注意してください。

- パスワードは大文字と小文字が区別されます。
- ユーザー名は、大文字と小文字が区別されません。大文字と小文字は同一として扱われます（例：Administrator は administrator と同一として扱われます）。

解決方法 2

原因

ユーザーアカウントが無効です。

操作以下の操作を試してください。

- ユーザーアカウントが正しく設定されており、ログイン権限を持っていることを確認します。
  管理者ユーザーアカウント権限のあるユーザーにログインを依頼し、アカウントのパスワードを変更してもらいます。それでもログインが失敗する場合は、ユーザーアカウントを削除してから追加し直すようにそのユーザーに要請します。
- アカウントのパスワードが正しく入力されたことを確認します。パスワードを忘れた場合は、管理者ユーザーアカウント権限のあるユーザーがそのパスワードを再設定できます。
- スライドタグに張り付けられたラベルに記載されているデフォルトのアカウント情報を用いて、ログインを行ないます。管理者アカウントが 1 つしかなく、パスワードを忘れた場合は、次の操作を実行します。

- システムメンテナンススイッチの iLO セキュリティ設定を使用します。ログインして、新しい管理者ユーザーアカウントを作成します。詳しくは、「システムメンテナンススイッチを使用した iLO セキュリティ」を参照してください。

ディレクトリ接続が途中で終了する

症状

アクティブディレクトリセッションが途中で終了します。

原因

ネットワークエラーによって、iLO は、ディレクトリ接続が無効になったと判断することがあります。iLO がディレクトリを検出できない場合、iLO は、ディレクトリ接続を終了します。終了された接続を使用して作業の継続を試みても、ブラウザーは、ログインページに転送されます。

この問題は、以下の状況で発生する可能性があります。

- ネットワーク接続が切断された。
- ディレクトリサーバーがシャットダウンした。

操作

ログインしなおして iLO の使用を継続します。

ディレクトリサーバーを使用できない場合は、ローカルユーザーアカウントを使用してログインする必要があります。

iLO ホスト名を使用して iLO マネジメントポートにアクセスできない

症状

iLO ホスト名を使用して iLO マネジメントポートにアクセスできない。

原因

iLO ホスト名を使用して iLO マネジメントポートにアクセスできるように環境が構成されていません。

操作

iLO マネジメントポートは、WINS サーバーまたは DDNS サーバーにホスト名を動的に登録する機能があります。WINS サーバーまたは DDNS サーバーは、iLO マネジメントポートに iLO ホスト名でアクセスするために必要な名前解決を提供します。

環境が以下の要件を満たすことを確認します。

- iLO マネジメントポートの電源を入れる前に、WINS サーバーまたは DDNS サーバーが稼働している必要があります。
- iLO マネジメントポートは、WINS サーバーまたは DDNS サーバーへの有効な経路を持っている必要があります。
- iLO に WINS サーバーまたは DDNS サーバーの IP アドレスを設定する必要があります。

  これらのアドレスは DHCP を使用して、iLO に設定することができます。詳しくは、「BMC 構成ユーティリティを使用した iLO のセットアップ」または「iLO ネットワーク設定」を参照してください。

- iLO マネジメントポートにアクセスするためのクライアント PC は、iLO マネジメントポートの IP アドレスが登録された DDNS サーバーを使用するように設定しなければなりません。

WINS サーバーと動的でない DNS サーバーを使用する場合は、DNS サーバーが名前解決用に WINS サーバーを使用するように設定すると、iLO マネジメントポートへのアクセスを大幅に高速化させることができます。詳しくは、Microsoft のドキュメントを参照してください。

iLO およびサーバーのリセット後、BMC 構成ユーティリティ を使用できない

症状

iLO をリセットした直後にサーバーをリセットすると、BMC 構成ユーティリティを使用できない。

原因

サーバーが iLO ファームウェアの初期化を実行し、BMC 構成ユーティリティの起動を試みたときに、iLO ファームウェアが完全に初期化されていませんでした。

操作

サーバーをもう一度リセットしてください。

ログインページにアクセスできない

症状

iLO Web インターフェースのログインページが表示されない。

原因

ブラウザーの SSL 暗号化レベルが 128 ビット以上に設定されていません。

iLO の SSL 暗号化レベルは 128 ビット以上に設定されており、変更することはできません。ブラウザーと iLO の暗号化レベルは一致していなければなりません。

操作

ブラウザーの SSL 暗号化レベルが 128 ビット以上に設定されていることを確認します。

iLO のリセット後にログインページに戻れない

症状

iLO のリセット後に iLO ログインページが表示されない。

操作

ブラウザーのキャッシュをクリアし、ブラウザーを再起動します。

ネットワーク設定の変更後 iLO に接続できなくなった

症状

ネットワーク設定を変更した後、iLO に接続できなくなった。

原因

NIC とスイッチの設定が同じではありません。

操作

接続の両端（NIC およびスイッチ）で、リンク速度、およびデュプレックスが同じ設定であることを確認してください。

たとえば、一方の側で接続が自動選択されるように設定されている場合、もう一方の側でも同じ設定を使用してください。iLO のネットワーク設定については、「iLO ネットワーク設定」を参照してください。

ファームウェアの更新後に接続エラーが発生する

症状

ファームウェアの更新後に、Web インターフェースを使用して iLO に接続できません。

操作

ブラウザーのキャッシュをクリアして、再試行します。

NIC を用いて iLO プロセッサーに接続できない

症状

NIC 経由で iLO プロセッサーにアクセスできません。

操作以下の解決策を試してください。

- iLO の RJ-45 コネクターにある緑の LED インジケーター（リンクステータス）が点灯していることを確認します。点灯している場合、PCI NIC とネットワークハブ間の接続は問題ありません。

  緑の LED インジケーターが断続的に点滅することを確認します。断続的に点滅する場合、ネットワークトラフィックは正常です。
- システムユーティリティ内の BMC 構成ユーティリティを実行して、NIC が有効になっていることを確認し、割り当てられた IP アドレスとサブネットマスクを確認します。
- ネットワーク上の別のワークステーションから、NIC の IP アドレスに対して ping を実行して、応答があるか確認します。
- ブラウザーで、NIC の IP アドレスを URL として入力して、NIC との接続を試みます。このアドレスで、iLO のホームページを表示できます。
- iLO をリセットします。

注記: ネットワーク接続が確立した場合、DHCP サーバー要求を最大 90 秒待つ必要がある場合があります。

---

iLO の証明書のインストール後 iLO にログインできない

症状

iLO の自己署名証明書をブラウザーの証明書ストアにインストールした後、iLO にアクセスできません。

原因

iLO を工場出荷時のデフォルト設定にリセットするか、iLO ホスト名を変更すると、新しい自己署名証明書が生成されます。一部のブラウザーでは、自己署名証明書を永久的にインストールすると、新しい自己署名証明書を生成した後で iLO にログインしなおすことができないことがあります。

操作

iLO の自己署名の証明書をブラウザーの証明書ストアにインストールしないでください。証明書をインストールする場合は、CA に永久的な証明書を要求し、iLO にインポートします。手順については、「SSL 証明書の管理」を参照してください。

iLO の IP アドレスに接続できない

症状

iLO の IP アドレスを使用して iLO に接続できない。

原因

プロキシサーバーを使用するように Web ブラウザーが構成されています。

操作

プロキシサーバーを使用せずに iLO に接続するようにブラウザーを構成します。

たとえば、Internet Explorer では、次の手順を実行してください。

1. **[ツール]→[インターネットオプション]**の順に選択します。
2. **[接続]**をクリックします。
3. **[LAN の設定]**をクリックします。
4. **[プロキシサーバー]**セクションで **[詳細設定]**をクリックします。
5. **[例外]**ボックスに iLO の IP アドレスまたは DNS 名を入力します。
6. **[OK]** をクリックして、変更を保存します。

iLO 通信が失敗する

症状

iLO 通信が失敗します。

解決方法 1

原因

iLO は、設定可能な複数の TCP/IP ポートを介して通信を行います。これらのポートの 1 つ以上がファイアウォールによってブロックされています。

操作

iLO が使用するポートでの通信を許可するようにファイアウォールを設定します。iLO ポート設定の表示および変更については、「iLO アクセスの設定」を参照してください。

解決方法 2

原因

接続先(スイッチング HUB 等)と iLO の Link 設定が一致していません。

操作

Link 設定は、接続先(スイッチング HUB 等)と iLO の Link 設定を同じ設定にします。詳細については、「iLO Web インターフェースを介した iLO 専用ネットワークポートの有効化」を参照してください。接続先の設定確認方法は、スイッチベンダーのマニュアルを参照してください。

NIC チーミング設定をしたとき、iLO との通信ができない

共有ネットワークを使用する設定がされていて、共有ネットワークポートを使用した NIC チーミング設定が有効な場合は、iLO との通信ができない可能性があります。チーミングの設定によっては、iLO の共有ネットワークポートへのパケットが無視される場合や、iLO への全てのパケットが他の NIC ポートに送信される場合があります。

Kerberos アカウントによる iLO へのログインが失敗する

症状

Kerberos へのログインを試みて失敗しました。

解決方法 1

原因

クライアントにチケットがないか、チケットが無効である。

操作

Ctrl+Alt+Del キーを押してクライアント PC をロックし、新しいチケットを取得します。

解決方法 2

原因

Kerberos ログインの設定が誤っています。考えられる原因は、以下のとおりです。

- クライアント PC がログインしている Kerberos レルムが、iLO が設定されている Kerberos レルムと一致しない。
- iLO に保存されている Kerberos キータブ内のキーが、Active Directory のキーと一致しない。
- iLO が不正な KDC サーバーアドレス用に構成されている。
- クライアント PC、KDC サーバー、および iLO の間で、日時が一致しない。これらのシステム上での日時を互いの 5 分以内に設定します。

操作

ご使用の環境が、Kerberos サポートの要件を満たしていることを確認します。詳しくは、「Kerberos 認証とディレクトリサービス」を参照してください。

解決方法 3

原因ディレクトリユーザーアカウントに関わる問題があります。

- Active Directory 内の iLO 用のアカウントが存在しないか、無効になっている。

- クライアント PC にログインしているユーザーが、iLO アクセスを認可された（汎用またはグローバルな）ディレクトリグループのメンバーでない。

操作

ユーザーアカウントが存在することと、そのユーザーアカウントが iLO へのアクセス権のあるグループのメンバーであることを確認します。

解決方法 4

原因

DNS サーバーが正常に稼働していない。iLO では、Kerberos をサポートするために、稼働している DNS サーバーが必要です。

操作

DNS サーバーを修復します。

解決方法 5

原因

ブラウザーが正しく設定されていない。

操作

ブラウザーが Kerberos ログイン用に正しく設定されていることを確認します。詳しくは、「Kerberos 認証とディレクトリサービス」を参照してください。

Firefox 使用時にセキュアな接続に失敗する

症状

Firefox ESR を使用して iLO に接続しようとしたときに、次のメッセージが表示されます。

解決方法 1

操作

1. メニューボタンをクリックし、[オプション]を選択します。

2. **[詳細]**をクリックします。
3. **[証明書]**タブをクリックします。
4. **[証明書を表示]**をクリックします。

   [サーバー証明書]タブをクリックし、iLO に関係する証明書をすべて削除します。
5. **[その他]**タブをクリックし、iLO に関係する証明書をすべて削除します。
6. **[OK]** をクリックします。
7. Firefox を起動し、iLO に接続します。

注記**:** 解決方法 1 の手順は Firefox ESR 24 に基づいています。使用する手順は、インストールされている Firefox のバージョンによって異なることがあります。

解決方法 2

操作

1. Firefox アプリケーションを閉じます。
2. Firefox の AppData フォルダーに移動して、すべての Firefox ディレクトリにある *.db ファイルをすべて削除します。

   AppData フォルダーは、通常は次の場所にあります。C:\\Users\< ユーザー名 >\AppData\Local\Mozilla\Firefox\

iLO Web インターフェースで、セキュリティ証明書の警告が表示される

症状

iLO Web インターフェースに接続すると、証明書の警告が表示されます。

解決方法 1

操作

Internet Explorer を使用している場合は、以下の手順に従います。

1. **[このサイトの閲覧を続行する（推奨されません）。]** リンクをクリックします。
2. iLO にログインします。
3. 補足：今後、証明書の警告が表示されないようにするには、「SSL 証明書の管理」を参照してください。

解決方法 2

操作

Firefox を使用している場合は、以下の手順に従います。

1. **[エラー内容]**リンクをクリックしてセクションを展開し、**[例外を追加]**をクリックします。
2. **[セキュリティ例外の追加]**ダイアログボックスで、URL に **https://<iLO** ホスト名または **IP** アドレス **>** と入力します。
3. **[セキュリティ例外を承認]**をクリックします。

   セキュリティ例外が保存され、iLO ログイン画面が表示されます。

4. iLO にログインします。

解決方法 3

Chrome を使用している場合は、以下の手順に従います。

1. セキュリティ警告が表示されたら、**[詳細設定]**をクリックします。
2. **[**（**iLO** のホスト名または **IP** アドレス）にアクセスする（安全ではありません）**]**をクリックします。
3. iLO にログインします。
4. 補足：今後、証明書の警告が表示されないようにするには、「SSL 証明書の管理」を参照してください。

「Web サイトは不明な機関で認証されています」メッセージ

症状

iLO ログインページに移動すると、「Web サイトは不明な機関で認証されています」というメッセージが表示されます。

操作

1. 証明書を表示して、（にせのサーバーでなく）正しいマネジメントサーバーにアクセスしていることを確認します。
   - **[発行先]**の名前がマネジメントサーバーであることを確認します。必要と思われる手順を実行して、マネジメントサーバーの識別情報を確認します。
   - これが正しいマネジメントサーバーかどうか確信が持てない場合は、先に進まないでください。にせのサーバーにアクセスしている可能性があり、サインイン認証情報がサインインしたにせのサーバーに渡るおそれがあります。管理者に連絡してください。証明書ウィンドウを終了し、**[**いいえ**]**または **[**キャンセル**]**をクリックして接続を取り消します。
2. ステップ 1 の項目を確認した後、以下の選択肢があります。
   - このセッションのために一時的に証明書を受け入れる。
   - 永久的に証明書を受け入れる。
   - いったん中止し、管理者から提供されたファイルからブラウザーに証明書をインポートする。

詳細情報

SSL 証明書の管理

ディレクトリの問題

以下の各項では、ディレクトリの問題のトラブルシューティング手順について説明します。

ユーザーコンテキストが動作しない

解決方法：ネットワーク管理者に問い合わせてください。ユーザーオブジェクトの完全 DN が、ディレクトリ内に存在する必要があります。自分のログイン名は、最初の CN= の後に表示されます。DN の残りの部分は、ユーザーコンテキストボックスのいずれかに表示されるはずです。

ユーザーコンテキストは、大文字と小文字を区別しません。また、それ以外の文字は、空白も含めて、ユーザーコンテキストの一部です。ディレクトリユーザーコンテキストの入力については、「ディレクトリの認証と認可」を参照してください 。

ディレクトリ接続が途中で終了する

症状

アクティブディレクトリセッションが途中で終了する。

原因

ネットワークエラーによって、iLO は、ディレクトリ接続が無効になったと判断することがあります。iLO がディレクトリを検出できない場合、iLO は、ディレクトリ接続を終了します。終了された接続を使用して作業の継続を試みても、ブラウザーは、ログインページに転送されます。

この問題は、以下の状況で発生する可能性があります。

- ネットワーク接続が切断された。
- ディレクトリサーバーがシャットダウンした。

操作

ログインしなおして iLO の使用を継続します。

ディレクトリサーバーを使用できない場合は、ローカルユーザーアカウントを使用してログインする必要があります。

ディレクトリタイムアウトになった後もディレクトリユーザーがログアウトしない

解決方法：iLO の **[アイドル接続タイムアウト]**を **[無限]** に設定している場合、リモートコンソールは、定期的にファームウェアの ping を実行して、接続が存在することを確認します。 ping が発生すると、iLO ファームウェアは、ユーザー権限についてディレクトリにクエリを実行します。この定期的なクエリによりディレクトリ接続がアクティブでありつづけ、タイムアウトが防止され、ユーザーがログインしたままになります。

ktpass.exe によるキータブの生成時の問題

解決方法：ktpass.exe を使用してキータブを生成する場合は、-princ 引数を使用してプリンシパル名を指定する必要があります。

プリンシパル名では大文字と小文字が区別され、次のように入力する必要があります。

HTTP/myilo.somedomain.net@SOMEDOMAIN.NET

- コマンドの最初は大文字（HTTP）
- コマンドの中央は小文字（myilo.somedomain.net）
- コマンドの最後は大文字（@SOMEDOMAIN.NET）

ここに示されているとおりの形式ではない場合、コマンドは機能しません。

以下に、完全な ktpass.exe コマンドの例を示します。

ktpass +rndPass -ptype KRB5_NT_SRV_HST -mapuser myilo@somedomain.net
-princ HTTP/myilo.somedomain.net@SOMEDOMAIN.NET -out myilo.keytab

リモートコンソールの問題

以下の各項では、リモートコンソールの問題のトラブルシューティングについて説明します。

重要: 新しいウィンドウの自動起動を防止するポップアップブロックを有効にすると、リモートコンソールを実行できなくなります。ポップアップブロックを無効にしてから、リモートコンソールを起動してください。

Linux クライアントで Firefox を使用して Java IRC を実行すると、Java IRC に赤色の X が表示される

解決方法：Firefox ブラウザーは、Cookie を受け入れるように設定する必要があります。Firefox の設定手順については、Firefox のドキュメントを参照してください。

Java IRC が起動しない

症状 1
アプリケーションを起動し、セキュリティ警告を受け入れずに、アプリケーションを実行することを確認した場合、Java IRC が起動しません。

原因 1
セキュリティ警告を受け入れずに、アプリケーションを実行することを確認した場合、Java IRC は起動しません。

操作 1

1. **[Java** コンソール**]**ウィンドウの **[**クリア**]**ボタンをクリックします。
2. **[Java** コンソール**]**ウィンドウの **[**閉じる**]**ボタンをクリックします。
3. iLO をリセットします。
   手順については、「iLO の再起動（リセット）」を参照してください。
4. ブラウザーのキャッシュをクリアします。
5. ブラウザーを閉じて、新しいブラウザーウィンドウを開きます。
6. iLO にログインして、JAVA IRC を起動し、証明書を受け入れます。

症状 2
以下のエラーメッセージが表示され、Java IRC が起動しません。
Connection refused: connect. Your browser session may have timed out.

原因 2
iLO Firmware Version が 1.20 Feb 02 2018 以前の環境で、**[Web Server SSL Port]**設定がデフォルトから変更されています。1.20 Feb 02 2018 以前の iLO Firmware でこの設定値がデフォルトから変更されている場合、Java IRC は起動しません。

操作 2
iLO にログインして[Access Settings]ページの[Service]セクションにある[Web Server SSL Port]設定をデフォルトに戻します。

.NET IRC 起動時に例外が発生し、起動しない。

解決方法：iLO 5 Firmware Version 1.30 May 31 2018 以降のファームウェアのアップデート後に.NET IRC を使用する際は、事前に.NET Framework をバージョン 4.5.1 以降に更新してください。

Microsoft Edge 42 で.NET IRC が起動しない。

信頼された SSL 証明書がインストールされていない状態で、Microsoft Edge 42 を使用して.NET IRC を起動すると、セキュリティアイコンがブラウザーのアドレスバーに表示され、アプリケーションのダウンロードがブロックされます。

解決策：以下のいずれかを実施してください。

- 信頼された SSL 証明書をインストールして、**[**Remote Console & Media**]**-**[**Security**]**ページの**[Integrated Remote Console Trust Setting]**設定において **[IRC requires a trusted certificate in iLO]**を有効にする。
- [ブロックされたコンテンツ] メニューで [すべてのコンテンツを表示] ボタンをクリックして、現在のセッションについて信頼されていないコンテンツを承認します。すると、Microsoft Edge 42 Web ブラウザーでウィンドウが再読み込みされ、以前のバージョンの Web ブラウザーと同様に.NET Integrated Remote Console を起動できるようになります。
- Internet Explorer 11 を使用して.NET Integrated Remote Console を起動します。
- スタンドアロンの.NET コンソールアプリケーションを使用します。

リモートコンソールのマウスカーソルをリモートコンソールウィンドウの隅に移動できない

リモートコンソールウィンドウの隅にマウスカーソルを移動できないケースがあります。

解決方法：マウスカーソルを右クリックしてリモートコンソールウィンドウの外側にドラッグしてから、内側にドラッグして戻してください。

リモートコンソールのテキストウィンドウが正しく更新されない

リモートコンソールで表示したテキストウィンドウ内を高速でスクロールする場合、テキストウィンドウが正しく更新されないことがあります。この問題は、iLO のファームウェアの検出/ 表示速度よりもビデオの更新速度のほうが速いために発生します。通常、テキストウィンドウの左上隅だけが更新され、残りの部分の表示は更新されません。

解決方法：スクロールが完了した後、テキストウィンドウを更新してください。

.NET IRC 、Java IRC、HTML5 IRC でマウスやキーボードを使用できない

解決方法 **1**：.NET IRC 、Java IRC、HTML5 IRC が開いているときにマウスまたはキーボードを使用できない場合は、以下の手順に従ってください。

1. .NET IRC、 Java IRC、HTML5 IRC を閉じます。
2. **[Power & Thermal]→[Power Settings]**ページに移動します。
3. **[Enable persistent mouse and keyboard]**チェックボックスをクリアし、**[Apply]**をクリックします。
4. .NET IRC、Java IRC、HTML5 IRC を再び起動します。

解決方法 **2**（**.NET IRC** のみ）：DirectDraw をサポートしないモニターがあります。たとえば、Windows クライアントでは、一部の USB VGA デバイスドライバーは、すべてのモニターで DirectDraw を無効にする場合があります。

.NET IRC には、DirectDraw サポートが必要です。

解決方法 **3**（**Java IRC** のみ）：

1. シャットダウンして、ブラウザーを終了します。
2. Java コントロールパネルを開きます。
3. **[Java Runtime Environment** 設定**]**ダイアログボックスを表示します。
4. 次のランタイム・パラメーターを追加します。
   -Dsun.java2d.noddraw=true
5. **[OK]** をクリックして **[Java Runtime Environment** 設定**]**ウィンドウを閉じます。
6. **[**適用**]**をクリックし、**[OK]**をクリックして Java コントロールパネルを閉じます。

注記**:** **[**適用**]**をクリックする前に変更内容を表示すると、**[**ランタイム・パラメーター**]**ダイアログボックスがリセットされ、編集内容が失われることがあります。

.NET IRC がウィンドウの切り替え後に継続して文字を送信する

解決方法：.NET IRC を使用中にキーを押した状態で、誤って別のウィンドウに切り替えると、.NET IRC でキーが押されたままの状態になり、文字が継続的に表示されることがあります。これを停止させるには、.NET IRC のウィンドウをクリックし、デスクトップの前面に移動させてください。

Microsoft Edge 42 で.NET IRC がウィンドウの切り替え後に継続して文字を送信するリモートコンソールのサムネイルが表示されない

Microsoft Edge 42 ブラウザー使用時、Web インターフェース上にリモートコンソールのサムネイルが表示されない場合があります。
解決方法：サムネイルを表示させるには Internet Explore 11 もしくは Microsoft Edge 42 ブラウザー以外のブラウザー(Mozilla Firefox、 Google Chrome モバイルおよびデスクトップ)を使用してください。

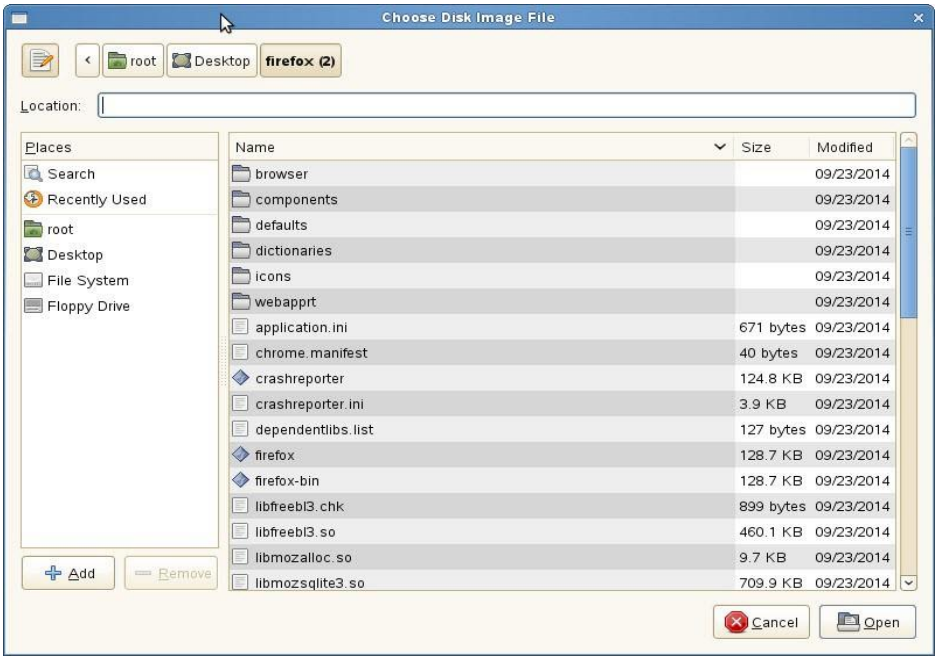
Java IRC のフロッピーディスクおよび USB キーデバイスの表示が誤っている

症状：Firefox ブラウザーを使用する場合、Java IRC が表示するフロッピーディスクドライブおよび USB キーデバイス情報が誤っている可能性があります。

操作：

1. Red Hat Enterprise Linux 6 以降がローカルクライアントシステムにインストールされていることを確認します。
2. 最新バージョンの Java をインストールし、Firefox ブラウザーで接続するように Java を設定します。
3. Firefox を使用して iLO の Web インターフェースにログインします。
4. USB キーまたはフロッピーディスクをローカルクライアントシステムに挿入します。
5. USB キーまたはフロッピーディスクにアクセスできることを確認します。
6. Java IRC セッションを開きます。
7. **[**Virtual Drives**]**→**[**Image File Removable Media**]**の順に選択します。

   [Choose Disk Image File**]**ダイアログボックスが開きます。



8. クライアントに挿入した USB キー またはフロッピーディスクのパス（/dev/disk）を入力または選択します。

   USB キーまたはフロッピーディスクを by-label でマウントすることもできます。
9. **[**Open**]** をクリックします。

iLO と Java IRC の間で Caps Lock が同期しない

Java IRC にログインすると、iLO と Java IRC の間で **Caps Lock** 設定が同期しない場合があります。

解決方法：Java IRC で**[Keyboard]**→**[CapsLock]** の順に選択して、**CapsLock** 設定を同期させます。

注記**:** IRC 上の OS の設定が日本語キーボードの場合は、IRC 上の **[Keyboard]**→**[CapsLock]**を選択すると、OS 上では CapsLock キーではなく**英数**キーと識別します。IRC 上の OS とクライアント OS の CapsLock 設定を同期させたい場合は、IME の言語バー等の言語設定を用いて同期させてください。

iLO と共有リモートコンソールの間で Num Lock が同期しない

共有リモートコンソールセッションにログインすると、iLO と一部のリモートコンソールセッションの間で **[Num Lock]** 設定が同期しない場合があります。

解決方法：リモートコンソールで**[Keyboard]→[NumLock]** の順に選択して、**[NumLock]** 設定を同期させます。

リモートコンソールセッション中に意図しないキーストロークが繰り返される

.NET IRC または Java IRC を使用しているとき、リモートコンソールセッション中に意図しないキーストロークが繰り返される場合があります。

解決方法 **1**：ネットワーク遅延を引き起こす場合がある問題を特定し、解決します。

解決方法 **2**：リモートマシンで以下の設定を調整します。

- **[Increase the typematic delay]** - この設定は、キーボードのキーを押したままにしたときに文字を繰り返す前の遅延を制御します。
- **[Decrease the typematic rate]** - この設定は、キーボードのキーを押したままにしたときに文字を繰り返す速度を制御します。

注記: 設定の正式名称は、使用している OS によって異なります。キーリピート遅延と速度の変更について詳しくは、OS のドキュメントを参照してください。

.NET IRC が再生中のとき、他セッションからの接続要求メッセージを確認できない。

解決方法：リモートコンソールのセッションリーダーがビデオデータを再生中に、別のユーザーが.NET IRC にアクセスし**[Share]**または**[Acquire]**要求をした場合、セッションリーダーは要求メッセージを確認できない場合があります。その場合、要求メッセージはタイムアウトし、新規セッションの要求を承認することになります。
セッションが切断され、再度 IRC にアクセスする必要がある場合は、他のユーザーに連絡するか、リモートコンソールの取得機能を使用して IRC の制御を取得してください。手順については、「リモートコンソールの取得」を参照してください。

リモートコンソールのキーボード LED の状態が反映されない

クライアントのキーボード LED は、リモートコンソールのキーボードロックキーの実際の状態を反映しません。リモートコンソールでキーボードオプションを使用すると、**Caps Lock**、**Num Lock**、および **Scroll Lock** キーを送ることができます。

.NET IRC が非アクティブになる

iLO .NET IRC は、稼動率が高くなると非アクティブになったり、切断されたりすることがあります。.NET IRC は非アクティブになる前に、動作が遅くなります。影響を受ける.NET IRC の症状には以下のものがあります。

- .NET IRC の画面が更新されない。
- キーボードおよびマウスの動作が記録されない。
- 共有リモートコンソール要求が登録されない。

非アクティブな.NET IRC で取得されたファイルは再生可能ですが、.NET IRC のアクティブな状態を復元することはできません。

この問題は、iLO に複数のユーザーがログインしている場合や、仮想メディアセッションが接続されて継続したコピー動作を行っている場合、または.NET IRC セッションが開いている場合に発生する可能性があります。

解決方法：.NET IRC と仮想メディアを接続しなおします。可能な場合は、同時 iLO ユーザーセッション数を減らします。必要に応じて、iLO をリセットします。

.NET IRC がサーバーに接続できない

iLO は.NET IRC セッションの確立時に「Failed to connect to server」というメッセージを表示することがあります。

iLO の.NET IRC クライアントは、iLO との接続が確立されるまで、指定された時間待ちます。この時間内に応答を受信しない場合、エラーメッセージを表示します。

このメッセージで考えられる原因は、以下のとおりです。

- ネットワークの応答が遅延している。
- 共有リモートコンソールセッションが要求されたが、セッションリーダーの受諾または拒否のメッセージ送信が遅延している。

解決方法 **1**：.NET IRC 接続を再試行します。

解決方法 **2**：可能な場合は、ネットワークの遅延を改善して、.NET IRC 接続を再試行します。

解決方法 **3**：共有リモートコンソールセッション向けの要求であった場合は、セッションリーダーに問い合わせて要求を再試行するか、リモートコンソール取得機能を使用します。詳しくは、「リモートコンソールの取得」を参照してください。

マウントされた .NET IRC 仮想ドライブの USB キーにファイルをコピーした後、ファイルが表示されない

マウントされた iLO 仮想ドライブ（Windows OS のいずれかを実行するクライアントコンピューターに接続された USB キー）にサーバーOS 上でファイルをコピーしても、クライアント PC の Windows エクスプローラーでファイルを表示できません。

Windows エクスプローラーは USB キー上のファイルのキャッシュされたコピーを維持し、ファイルが変更された場合でも iLO リモートコンソールから Windows シェルへの通知も行われません。

USB ドライブ上ではファイルは変更されていますが、ユーザーがクライアント PC のエクスプローラーウィンドウを更新すると、ファイルのキャッシュされたコピーがフラッシュされ USB キーに戻されるため、Windows エクスプローラーではファイルの変更は表示されません。

Windows クライアントからリモートコンソールを使用してマウントされた iLO 仮想メディア USB キードライブ上のファイルを変更すると、その変更のタイプとは関係なく、この問題が発生する可能性があります。

解決方法：

1. Windows クライアントコンピューターに USB キーを接続します。
2. .NET IRC を使用して、クライアントの USB キーをターゲットサーバー上の iLO 仮想メディアドライブに接続します。
3. 接続した iLO 仮想メディアドライブ上のファイルを変更（コピー、削除など）します。
4. ターゲットサーバーの iLO USB 仮想メディアドライブを安全にアンマウントして、すべてのデータが更新され仮想メディアドライブに保存されるようにします。
5. .NET IRC でクライアント USB キーの接続を切断します。

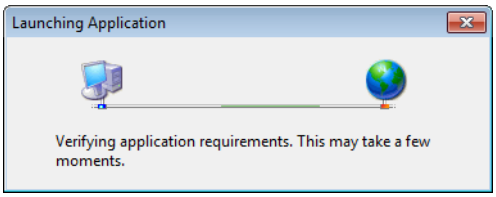
△ **注意：** USB キーの内容の更新に、Windows エクスプローラーを使用しないでください。

6. Windows の通知領域で **[ハードウェアの安全な取り外し]**アイコンをクリックして、クライアントコンピューターから USB キーを安全に取り外します。画面の指示に従います。
7. クライアントコンピューターから USB キーを取り外します。

USB キーをコンピューターに接続すると、Windows エクスプローラーでファイルの変更を確認できます。

.NET IRC はアプリケーション要件を確認するのに長い時間がかかります。

.NET IRC を iLO Web インターフェースから起動すると、**[アプリケーションの起動中]** ダイアログボックスが表示され、その画面が長い間表示されます。



解決方法：

1. Internet Explorer を起動します。
2. **[ツール]→[インターネットオプション]**の順に選択します。

   [インターネットオプション]ウィンドウが開きます。
3. **[接続]**タブをクリックし、**[LAN の設定]**ボタンをクリックします。

   [ローカルエリアネットワーク（LAN）の設定]ウィンドウが開きます。
4. **[設定を自動的に検出する]**チェックボックスの選択を解除します。
5. 必要に応じてプロキシサーバーの設定を行います。
6. すべてのブラウザーウィンドウを閉じます。

7. ブラウザーを再起動し、.NET IRC を起動します。

.NET IRC の起動失敗

.NET IRC を起動すると、**[**アプリケーションを起動できませんでした。**]** ダイアログボックスが表示されます。

解決方法：Windows コマンドプロンプトから次のコマンドを入力して、ClickOnce アプリケーションキャッシュをクリアします。
rundll32 %windir%\system32\dfshim.dll CleanOnlineAppCache

.NET IRC を共有できません

.NET IRC を共有しようとしたときに、**[**Unable to connect**]** ダイアログボックスが表示されます。

解決方法 **1**：セッションリーダーの.NET IRC クライアントと各共有.NET IRC クライアントの間に通信ルートが存在することを確認します。

解決方法 **2**：すべてのクライアントのファイアウォール設定が、リモートコンソールポート（デフォルトポートは 17990）へのインバウンド接続を許可していることを確認します。

Firefox によって.NET IRC の起動がブロックされる

症状

Mozilla Firefox で.NET IRC を起動すると、アプリケーションが起動に失敗する場合があります。

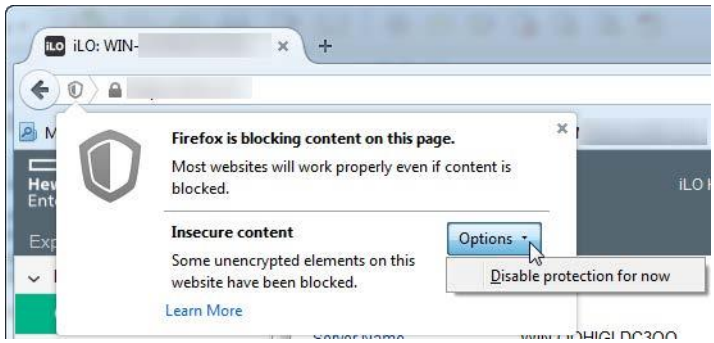
原因

iLO システムがデフォルトの iLO SSL 証明書（認証機関により署名されている信頼済み証明書ではない）を使用している場合、iLO Web インターフェースは、HTTPS ではなく HTTP を使用して、.NET IRC を起動します。iLO Web インターフェースは HTTPS を使用し、Web インターフェースは HTTP を使用して IRC を起動するため、ブラウザーに警告が表示されます。操作以下の操作を試してください。

- iLO に SSL 証明書をインポートし、**[**Remote Console & Media**]**→**[**Security**]** ページの **[**IRC requires a trusted certificate in iLO**]** 設定を有効にします。これが最も安全な解決方法です。
  証明書のインポートについて詳しくは、「SSL 証明書の管理」を参照してください。

[IRC requires a trusted certificate in iLO]設定の変更については、「統合リモートコンソールの信頼設定（.NET IRC）の設定」を参照してください。

- アドレスバーの盾アイコンをクリックし、[オプション]→[今すぐ保護を無効にする]を選択します。



警告はご使用のブラウザーのバージョンによって異なる場合があります。

- 別のブラウザーを使用します。

Google Chrome で、.NET IRC の起動ができない

症状

Google Chrome で.NET IRC を起動すると、アプリケーションが起動に失敗します。

原因

Google Chrome の以前のバージョンでは、ClickOnce をサポートする NPAPI プラグインを使用して.NET IRC を実行できました。Google Chrome バージョン 42 以降では、NPAPI ベースのプラグインがサポートされません。

操作

- 別のブラウザーを使用します。

IRC で押したキーと異なるキーが入力される

症状

IRC を使用してサーバーを操作しようとした際に、キーボード上で押したキーとは異なるキーがサーバー上の OS で入力されてしまいます。

原因

クライアント OS とサーバーOS のキーボード言語設定が不一致になっています。

または、HTML5 IRC を英語キーボード以外で操作しています。

操作

- クライアント OS とサーバーOS のキーボード言語設定を同じ値にします。
- HTML5 IRC を英語キーボード環境で実行します。

HTML5 IRC で押したキーと異なるキーが入力される

症状

HTML5 IRC を使用してサーバーを操作しようとした際に、キーボード上で押したキーとは異なるキーがサーバー上の OS で入力されてしまいます。

原因

HTML5 IRC を英語キーボード以外で操作しています。

操作

iLO Firmware Version 1.30 May 31 2018 以降の場合

- HTML5 IRC のキーボードレイアウト設定で適切なキーボード種別を選択します。
- HTML5 IRC の仮想キーもしくは OS のスクリーンキーボード機能を使用します。
- 詳細は統合リモートコンソールの使用に関する情報とヒントを参照します。

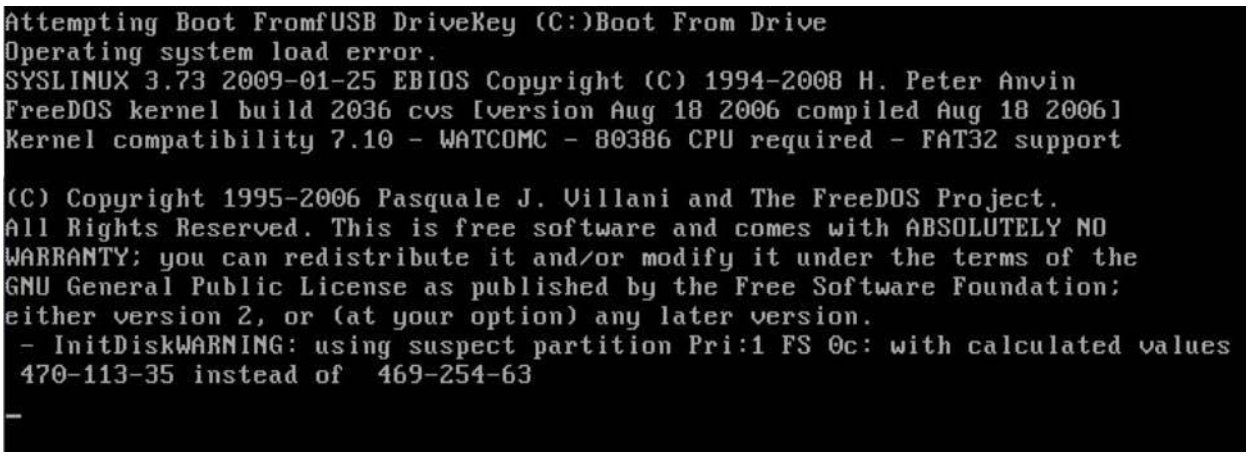
iLO 5 Firmware Version 1.20 Feb 02 2018 以前

- HTML5 IRC を英語キーボード環境で実行します。
- OS のスクリーンキーボード機能を使用します。
- 詳細は統合リモートコンソールの使用に関する情報とヒントを参照します。

マウントされている USB キーを使用して DOS をブートできない

問題：iLO リモートコンソールを使用して、マウントされている DOS ブート可能な USB キーから起動しようとすると、エラーが発生します。USB キーの容量が 2 GB 以下の場合は、次のエラーが表示されます。

USB キーの容量が 2 GB を超える場合は、次のエラーメッセージが表示され、サーバーがその時点で操作を停止します。



これは、リモートコンソールが USB キーのブートセクタにアクセスするための十分な権限を持っていないために発生します。

解決方法 **1**：Internet Explorer を右クリックし、**[**管理者として実行**]**を選択します。iLO の Web インターフェースを起動し、リモートコンソールを起動してから、USB キーからブートします。

解決方法 **2**：USB キーをサーバーに直接接続します。

仮想メディアイメージをマウントした後に HTML5 IRC が応答しなくなる

問題：Internet Explorer (IE) を使用して HTML5 IRC から仮想イメージファイルをマウントした後に、HTML5 IRC が応答しなくなる場合があります。iLO web インターフェースも応答しなくなった場合にはブラウザーのリロードボタン(F5)で再読み込みを行ってください。

解決方法 **1**：HTML5 IRC を使用して仮想メディアファイルをマウントする場合には、Internet Explorer (IE)以外のサポートブラウザーを使用してください。

iLO 共有ネットワークポートが構成された状態で、IRC の仮想メディアを使用した OS インストール時に、OS のインストレーションが失敗する場合がある

問題： iLO 共有ネットワークポートが構成された状態で、IRC の仮想メディアを使用して OS のインストールを実施した場合に、OS のインストレーションが失敗する場合があります。

解決方法 ：物理 D-ROM ドライブを接続し、OS のインストールを行ってください。

SSH の問題

以下の各項では、SSH の問題に関するトラブルシューティングについて説明します。

PuTTY の初期接続時の入力が緩慢である

PuTTY クライアントを使用して初めて iLO に接続を行う際、入力の受け付けが緩慢（約 5 秒間）になります。

解決方法：クライアントで設定オプションを変更します。[Low-level TCP connection options] の **[Disable Nagle's algorithm]** チェックボックスの選択を解除してください。

PuTTY クライアントが応答しない

共有ネットワークポート設定で PuTTY クライアントを使用すると、大量のデータが転送される場合や仮想シリアルポートまたはリモートコンソールを使用する場合に、PuTTY セッションが応答しなくなることがあります。

解決方法：PuTTY クライアントを終了して、セッションを再開してください。

NIC チーミング設定をしたとき、iLO との通信ができない

共有ネットワークを使用する設定がされていて、共有ネットワークポートを使用した NIC チーミング設定が有効な場合は、iLO との通信ができない可能性があります。

- チーミング設定により、iLO の共有ネットワークポートへのパケットが無視される場合があります。
- チーミング設定により、iLO への全てのパケットが他の NIC ポートに送信される場合があります。

iLO ファームウェア 2.10 から 2.14 において、SSH キーのインポート時に"SSH Key was not Found"または "Public Key Import Error"が表示されてインポートに失敗する。

症状

iLO ファームウェア 2.10 から 2.14 において、Web インターフェースから SSH キーのインポートを行った時に、"SSH Key was not Found"または "Public Key Import Error"が表示されてインポートに失敗します。

iLO5 Web インターフェースで[セキュリティ] - [暗号化] で [セキュリティ設定]に[本番環境]が構成されている場合、[公開キーのインポート]で[公開キー]に DSA キーが選択されて[公開キーのインポート]が行われると、以下のメッセージが表示されます。

Public Key Import Error: Invalid input.

The public key could not be imported. Verify that a correctly-formatted base64-encoded public key was used.

解決方法： 安全性の低い DSA キーを生成する代わりに、より安全な RSA キーを使用して[公開キーのインポート]を行ってください。DSA キーは、より高いセキュリティ モードでは許可されません。

iLO 連携の問題

iLO 連携ページでクエリエラーが発生する

症状

iLO 連携ページを開いたときに、iLO ピアおよび関連付けられたデータがページに表示されないことがあり、次のエラーが表示されます。

Errors occurred during query, returned data might be incomplete or inconsistent.

原因

このエラーはネットワーク通信エラー、設定の問題、または障害が発生した iLO システムによって、iLO 連携グループ内のすべてのシステムからのデータを取得できない場合に発生することがあります。

操作

以下の操作を試してください。

- 構成済みの **[Multicast Announcement Interval]**の 2 倍の時間待ってから、iLO 連携ページを更新します。iLO システムが再構成され、ローカル iLO システムと通信できない iLO ピアは、期限が切れた後でピア関係から削除されます。これによってクエリのエラーが解消するはずです。
- **[**Multi-System Map**]**ページのエラーを確認します。このページでは、iLO ピア間の通信の問題を識別することができます。
- ネットワーク内のスイッチが iLO ピア間で通信できるように構成されていることを確認します。
- iLO ピアのネットワークルート、サブネットマスク、IP アドレス、または HTTP ポートを最近変更した場合、iLO ピアがローカル iLO システムへの通信パスを持っていることを確認します。
- ファイアウォール、または iLO ネットワーク構成や HTTP ポート設定の変更によって、エラーの発生したピアとローカル iLO 間の通信がブロックされていないことを確認してください。

詳細情報

iLO 連携マルチシステムマップの表示
iLO の [Multi-System Map] ページに 502 エラーが表示される
iLO の [Multi-System Map] ページにタイムアウトエラーが表示される
iLO の [Multi-System Map] ページに 403 エラーが表示される
iLO ネットワーク設定
iLO アクセスの設定

iLO の [Multi-System Map] ページにタイムアウトエラーが表示される

症状

[Multi-System Map**]**ページに、ローカル iLO システムのピアに対するタイムエラーが表示されます。

原因

このエラーは、以下の状況で発生する可能性があります。

- ローカル iLO システムのピアに障害のあるピアがある。
- ファイアウォールによってローカル iLO システムとピア間の通信が妨害されている。
- ネットワーク構成の変更によってローカル iLO システムとピア間の通信が妨害されている。

操作

次のいずれかを試みます。

- 障害が発生したピアを削除するか修復します。
- ネットワークが iLO ピアの間で通信できることを確認します。

詳細情報

iLO 連携のネットワーク要件

iLO の [Multi-System Map] ページに 502 エラーが表示される

症状

[Multi-System Map**]**ページで 502 エラーが表示される。

原因

一覧表示されているピアがローカル iLO システムからの要求を拒否しました。

操作

ファイアウォール、または iLO ネットワーク構成や HTTP ポート設定の変更によって、エラーの発生したピアとローカル iLO システム間の通信がブロックされていないことを確認してください。

iLO の [Multi-System Map] ページに 403 エラーが表示される

症状

[Multi-System Map**]**ページで 403 禁止/認証エラーが表示されます。

原因

ローカル iLO システムのグループキーとピア iLO システムのグループキーが一致しません。

操作

選択したグループのメンバーになっているすべての iLO システムのグループキーが一致することを確認してください。

iLO ピアが iLO 連携ページに表示されない

症状

iLO ピア（ローカル iLO システムと同じグループ内のシステム）が iLO 連携ページに表示されていません。

操作

以下の操作を試してください。

- 選択したグループのメンバーになっているすべての iLO システムのグループキーが一致することを確認してください。
- マルチキャスト間隔の 2 倍の時間が経過した後、iLO 連携ページを更新します。iLO システムが再構成され、ローカル iLO システムと通信できない場合は、期限が切れた後でピア関係から削除されます。
- ネットワーク内のスイッチが iLO ピア間で通信できるように構成されていることを確認します。
- ファイアウォール、または iLO ネットワーク構成や HTTP ポート設定の変更によって、エラーの発生したピアとローカル iLO システム間の通信がブロックされていないことを確認してください。

詳細情報

iLO 連携のネットワーク要件

iLO ピアが IPv4 ネットワーク上で IPv6 アドレスで表示される

症状

IPv4 ネットワーク上の iLO ピアが iLO 連携ページに IPv6 アドレスで表示されます。

操作

ネットワークが IPv4 のみを使用するよう構成されている場合、**[iLO Dedicated Network Port]→[IPv6]** ページの **[iL**O Client Applications use IPv6 first**]** チェックボックスが選択されていないことを確認します。

詳細情報

IPv6 の設定

ファームウェア更新の問題

iLO ファームウェアの更新が失敗する

症状

iLO ファームウェアを更新できません。

解決方法 1

原因

通信またはネットワークの問題が発生しました。

操作

iLO の Web インターフェースを使用して iLO ファームウェアを更新しようとするときに iLO ファームウェアが応答しない、ファームウェアの更新が受け付けられない、または更新が成功する前に終了する場合は、次のことを確認した後、ファームウェアを再インストールしてみてください。

1. iLO に Web ブラウザー経由で接続を試みます。接続できない場合は、通信に問題があります。
2. iLO に対して ping を実行します。成功する場合、ネットワークは動作しています。

解決方法 2

操作

別のファームウェアの更新方法を試してください。

詳しくは、「ファームウェアの更新」を参照してください。

iLO ファームウェア更新エラー

症状

ファームウェアの更新中に次のエラーが表示されます。

The last attempt to update or upload firmware was not successful. Make sure you are using a valid, signed flash file and try again.

原因

iLO ファームウェアの更新で間違ったファイルを使用しました。

操作

エラーメッセージをクリアして、正しいファイルでファームウェアの更新を再び実行します。エラーをクリアしないと、正しいファイルを使用しても、同じエラーが発生する場合があります。

ライセンスのインストールに失敗する

以下の原因により、ライセンスキーのインストールに失敗する場合があります。

症状

iLO ライセンスのインストールに失敗します。

解決方法 1
原因
キーが iLO ライセンスキーではありません。

操作
iLO ライセンスキーを入手し、もう一度やり直してください。

解決方法 2
原因
正規のライセンスがすでにインストールされた状態で、評価キーが送信されました。

操作
iLO は、正規のキーがすでにインストールされている場合、評価キーのインストールできません。

解決方法 3
原因
iLO の日時設定が不適切です。

操作
iLO の日時設定を確認し、もう一度やり直してください。

解決方法 4
操作
iLO ファームウェアを更新し、もう一度やり直してください。

仮想メディアまたはグラフィックリモートコンソールにアクセスできない

解決方法：iLO の仮想メディアおよびグラフィックリモートコンソール機能は、iLO ライセンスをインストールすることによって使用できます。ライセンスがインストールされていない場合は、これらの機能を使用できないことを示すメッセージが表示されます。

iLO RESTful API の問題

OS 稼働中に HDD のホットスワップを実施した後に iLO RESTful API で取得した情報の InterfaceType が変更されない

解決方法：HDD のホットスワップ後にシステムリセットを実行して OS の再起動を行ってください。

特定の iLO ファームウェアバージョンで、iLO RESTful API を使用してログインセキュリティバナーのメッセージを変更しようとした場合に、テキストが変更されない

症状
iLO ファームウェア 1.43 あるいは 1.45 において、iLO RESTful API を使用して、「ログインセキュリティバナー」のテキストを変更した場合に、変更したテキストの内容が反映されません。この時、エラーは表示されません。本問題は、iLO ファームウェア 1.40 では発生しません。

解決方法
操作
- iLO ファームウェアを 2.18 に更新してください。

仮想 NIC 問題

iLO web インターフェースもしくは iLO RESTful API が仮想 NIC を介してアクセス出来ない

症状

iLO の Web インターフェースもしくは iLO RESTful API から仮想 NIC を介して iLO に接続する際に、接続が失敗する。

ホストからの仮想 NIC の IP アドレス(16.1.15.1)への PING が成功する。

解決方法 1

原因

必要なインターフェースもしくは機能が無効になっている。

操作

- iLO RESTful API を使用するために、**[Access Settings]**の**[Web Server]**オプションが有効になっていることを確認してください。
- iLO Web インターフェースを使用するために、**[Access Settings]**の**[Web Server]**と**[iLO Web Interface]**オプションとが有効になっていることを確認してください。

解決方法 2

原因

ホスト OS 上のファイヤーウォール設定が iLO Web Server SSL Port (HTTPS)をブロックしている。

必要なインターフェースもしくは機能が無効になっている。

操作

- ファイヤーウォールによるブロックを無効化してください。
- **[Access Settings]**の構成ポートを確認してください。デフォルトのポート番号は 443 です。

解決方法 3

原因

ブラウザーがサポートされていません。

操作

- サポートされているブラウザーを使用してください。「iLO Web インターフェースの使用」を参照してください。

解決方法 4

原因

ブラウザーがプロキシサーバを使用するように構成されています。

操作

- プロキシサーバ設定を無効にしてください。

iLO が仮想 NIC を介してアクセスされない

症状

仮想 NIC 接続を介して iLO に接続する際に、接続が失敗する。

ホストから仮想 NIC の IP アドレス(16.1.15.1)への PING が成功しない。

解決方法 1

原因

仮想 NIC 機能が無効化になっている。

仮想 NIC 機能の状態を確認して原因になっていないかを確認してください。

操作

- iLO Web インターフェースで**[Access Settings]**の**[Virtual NIC]**オプションが有効になっていることを確認してください。
- REST クライアントで Virtual NIC オプションが有効になっていることを確認してください (GET "redfish/v1/Managers/1/HostInterfaces/1")。

解決方法 2

原因

USB CDC-EEM ドライバがホスト OS 上にインストールされておらず、動作していません。

操作

- ホスト OS が仮想 NIC 機能をサポートしているかを確認してください。
- ホスト OS に USB CDC-EEM ドライバがインストールされ、動作していることを確認してください。
- ホスト OS が仮想 NIC 機能をサポートしている場合、USB CDC-EEM ドライバがインストールされていません。ドライバをインストールしてください。

解決方法 3

原因

仮想 NIC インターフェースが Linux ホスト上で DHCP を使用するように構成されていません。

ip addr や ifconfig コマンドを使用して USB イーサーネットインターフェースの IP アドレスが 16.1.15.2 となっていることを確認してください。

操作

- DHCP を使用するように仮想 NIC インターフェースを構成してください。

解決方法 4

原因

ホスト OS 上の仮想 NIC インターフェースが、他のインターフェースとチーミングされています。この構成は未サポートです。

操作

- ホスト OS 上の仮想 NIC インターフェースが、他のインターフェースとチーミングされていないことを確認してください。

Windows 環境で、デバイスマネージャの「ほかのデバイス」に「Virtual NIC」が表示される

症状

Windows のデバイスマネージャ上で「ほかのデバイス」に「Virtual NIC」が表示される。

解決方法

以下の操作で仮想 NIC 機能を無効に設定してください。

原因

- 仮想 NIC 機能は、Windows Server 2012 R2 をサポートしていないため、「Virtual NIC」デバイスにドライバーはインストールされません。
- Windows Server 2016/2019 で USB CDC-EEM ドライバがインストールされていない。

操作

1. iLO Web インターフェースのナビゲーションツリーで **[Security]** をクリックする。
2. **[Access Settings]** - **[iLO]** - **[Virtual NIC]**を**[Disabled]**にする。

その他

実際のアダプター名の代わりに「Network Controller」が表示されることがあります。

解決方法：**[System Configuration]** - **[RBSU]** - **[System Options]** - **[Boot Time Optimizations]**-**[UEFI POST Discovery Mode]** に移動して、**[Force Full Discovery]** に設定します。

iLO Web インターフェースの電力メーター表示において、ピーク電力(最大電力)の測定値が電源容量を超える場合があります。

症状

iLO 5 Firmware Version 1.40 Feb 05 2019 以前が適用されている場合に iLO の Web インターフェースの電力メータ表示において、ピーク電力(最大電力)の測定値が電源容量を超える場合があります。

これに伴い以下の IML エントリが記録されてしまいます。
Server power: %1W exceeded the redundant power capacity threshold: %2W
※%1、%2：数値代入

解決方法：iLO5 Firmware Version 1.43 May 23 2019 へアップデートしてください。

ヘルスステータス変化の検出イベントについて

ESMPRO/ServerManager から本体装置を監視対象としている場合、本体装置を再起動した場合や、iLO が管理するサブシステムの状態が変化すると、「ヘルスステータス変化の検出」のイベントが通知され、イベントの詳細に下記のような表示が行われます。

サーバーのヘルスステータスが変化しました。現在のステータスは 020402020202020202020002020204020201000000000000000000000000000 です。

このステータスは、各サブシステムのステータスを二桁の数字で表しています。
上記のステータスの場合は、各サブシステムが以下の状態であることを示しています。

ヘルスステータス	02	04	02	02	02	02	02	02	02	02	00	02	02	02	04	02	02	01	00	00	00	00	00	00	00	00	00	00	00	00	00	備考
#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	
サブシステム	システムヘルスステータス	全体	プロセッサ	メモリ	ファン	温度	電源装置	ログ	自動サーバ復旧	ドライブアレイ	SCSIデバイス	ストレージ	IDEデバイス	ファイバーチャネル	ネットワーク	MIB	BIOS/ハードウェア	バッテリ	iSCSIデバイス	-	-	-	-	-	-	-	-	-	-	-	-	-	
ステータス	OK	障害	OK	OK	OK	OK	OK	OK	OK	OK	未インストール	OK	OK	OK	障害	OK	OK	その他	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	未インストール	00 - 未インストール 01 - その他 02 - OK 03 - 劣化 04 - 障害

> △**注意:**
> iLO は、アダプターファームウェアまたは OS ソフトウェアから報告された内容に基づき通知します。インストールされていないアダプター(サブシステム)のステータス変化が検出されることがありますが、運用動作上問題はありません。

vSphere Web クライアントで VMWare ESXi 6.5/6.7 が稼働しているサーバのハードウェアのセンサーステータスが不正確に表示される場合があります。

症状

2 ポートの NIC カードが搭載されているにも関わらず、ポート 3、ポート 4 が警告表示される場合があります。本事象は vSphere web クライアントの表示問題で、システムへの影響はありません。

解決方法：ESXi バージョン毎にパッチの適用と、現在インストールされている Agentless Management Service(AMS)と iLO Channel Interface Driver の有無、バージョンを確認してから各コンポーネントのインストールまたはアップデートを行ってください。

- VMware ESXi 6.5
  パッチ:http://support.pf.nec.co.jp/View.aspx?NoClear=on&id=9010107911
  AMS :https://jpn.nec.com/nx7700x/support/dload/mn/053486-G01/index.html?
- VMware ESXi 6.7
  パッチ:http://support.pf.nec.co.jp/View.aspx?NoClear=on&id=9010108433
  AMS :https://jpn.nec.com/nx7700x/support/dload/mn/201910-01/index.html?

ゲートウェイのフェイルオーバー後に iLO へのネットワークアクセスが不可になる

症状

Gratuitous Address Resolution Protocol(GARP)を通知するゲートウェイのフェイルオーバー後に iLO へのネットワークアクセスが不通になる。

解決方法

- iLO を再起動して、ルーティングテーブルが正しく更新されるようにしてください。
- iLO 5 Firmware Version 2.31 Oct 13 2020 以降 にアップデートしてください。

原因

1. iLO5 は、使用するように構成されているゲートウェイの MAC アドレスを取得します。
2. MAC アドレスがルーティングテーブルに保存されます。
3. ゲートウェイの別の MAC アドレスが Gratuitous ARP (GARP) を介して iLO に送信されます。 ゲートウェイの IP アドレスは同じですが、MAC アドレスが変更されています。
4. iLO は引き続き古い (その時点では不正になっている) MAC アドレスを使用して、ゲートウェイとの通信を試みます。

この問題は、IPv4 ゲートウェイの MAC アドレスが変更され、新しい IPv4 アドレスが Gratuitous ARP を介して iLO に送信される場合にのみ発生します。 iLO がゲートウェイ自体に対して ARP を実行し、新しいゲートウェイから応答を受信すると、MAC アドレスは予期したとおりに更新されます。

操作

1. 「iLO の再起動（リセット）」を参照して iLO の再起動を行ってください。

Windows 上で vEthernet (Hyper-V Virtual Ethernet Adapter) が構成されている場合、iLO Web インターフェースのネットワークアダプタの IPv6 アドレス表示において、正しくない IPv6 アドレスが表示される場合があります。

症状

Windows OS 上で vEthernet(Hyper-V Virtual Ethernet Adapter)が構成されている場合、iLO　web インターフェースの[Information] - [Network] - [Physical Network Adpters]において、構成されている各[Adapter]の[Network Ports]の”IPv6 Address”において正しい IPv6 アドレスが表示されない場合があります。

解決方法

- vEthernet 構成時の IPv6 アドレスに関しては、OS 上のネッワークアダプタのプロパティにてご確認ください。
- AMS Version 2.12.0.0(Windwos)/AMS Version 2.1.0(RHEL)を適用してください。

"The iLO Health Monitoring Status of the Device / Adapter Located In Embedded Is Not Responsive" という誤った警告メッセージが iLO 5 Event Log 繰り返し記録されることがあります。

症状

iLO 5 2.31 未満の iLO5 ファームウェアが適用されている装置において、以下の誤った警告メッセージが IEL(iLO Event Log)に繰り返し記録されることがあります。

- The iLO health monitoring status of the device / adapter located in Embedded is not responsive.
- The iLO health monitoring status of the device / adapter located in Slot(n) is not responsive.

システムが正常に機能している場合は、上記の警告メッセージを無視することができます。

解決方法 1

下記を実施することで警告メッセージを停止できます。

1. iLO Web インターフェースの[システム情報]-[デバイスインベントリ]-[検出]より「MCTP 検出」のチェックを外し、「適用」をクリックしてください。確認画面では「はい」をクリックしてください。
2. 2 分間待った後、「MCTP 工場出荷時リセット」をクリックしてください。確認画面では「はい」をクリックしてください。
3. iLO Web インターフェースの[情報]-[診断]-[iLO をリセット]より「リセット」を実施してください。
4. (OS 稼働中であった場合は)OS の再起動を実施してください。

解決方法 2

- iLO 5 Firmware Version 2.31 Oct 13 2020 以降 にアップデートしてください。

iLO 5 ファームウェア v1.38 (またはそれ以前) およびシステム ROM バージョン 2.x (またはそれ以降) が適用されたサーバーを再起動した後に、システムファンが異常な高速度で回転することがある

症状

iLO5 v1.38 (またはそれ以前) およびシステム ROM バージョン 2.x (またはそれ以降) が適用された装置で、サーバーの再起動後にシステムファンが異常な高速度で回転することがあります。
この問題は、iLO 5 ファームウェア v1.38 (またはそれ以前) が、システム ROM 2.x (またはそれ以降) で定義されている DCPMM 用の温度センサーをサポートしていないため発生します。

解決方法

ファンが通常の速度で回転するようにするには、iLO 5 ファームウェア v1.43 (またはそれ以降) にアップグレードしてください。

システムの高負荷状態時に「注意」レベルの電源装置のファン障害警告イベントを IML に登録してしまう可能性があります。

症状

システムが高負荷状態時、以下の「注意レベル」の電源装置のファン障害警告イベントを IML に登録してしまう場合があるます。また該警告イベントが回復したことを示す「修復済み」イベントも登録される場合があります。

Severity - Caution
Description - System Power Supply: Fan Warning (Power Supply X) ACTION: Check the power source as well as the power supply fan.

解決方法

iLO 5 ファームウェア v2.31(またはそれ以降) にアップグレードしてください。

「Active Health System Log」のクリアが失敗する場合があります。

症状

[**Information**]-[**Active Health System Log**]-[**Show Advanced Settings**]-[**Clear Log**]において、[**Clear**]を行うと、「Active Health System ログは、他のアプリケーションによって使用されているため無効になりました」とメッセージが表示されて、 AHS のクリアが失敗する場合があります。

解決方法：

・最新の iLO ファームウェアを適用してください。
・「ハードウェア **iLO** 再起動」を行ってください。
この機能を使用するには、UID スイッチを 10 秒間以上押し続けます。

SSD の物理ドライブの容量表示が正しくない場合があります。

症状

[System Information] - [Storage] において、「Physical Drives」で表示される SSD ドライブの [Capacity]の単位 (例：223GB → 223MB) が正しくない場合があります。

解決方法

- MB を GB と読み替えてください。

BMC 構成ユーティリティからアカウントのパスワードを変更すると、「ホストストレージ構成」の権限が消失してしまう。

症状
[Administration] - [User Administration] において、[Host Storage]権限を持つユーザーアカウント作成後に、BMC 構成ユーティリティの[ユーザ管理] - [ユーザーの編集/削除] - [編集] - [パスワード] において、パスワードの変更を行うと、[Host Storage]権限が消失します。

解決方法
- iLO ファームウェア 2.44 以降を適用してください。

iLO5 と OS で異なる CPU 使用率の値が表示されることがあります。

症状
オペレーティングシステム(OS)とは異なる CPU 使用率の値が表示されることがあります。
iLO5 で表示されるハードウェア(HW)使用率の測定値は、プロセッサの実行状態の時間に対する停止状態の時間の比率に依存します。
たとえば、Linux カーネルで「idle=poll」が有効になっている状態で「top」コマンドを実行した結果、CPU アイドル状態が 99%と表示されても、iLO では CPU 使用率が 98%と表示されたりします。
この問題は、オペレーティングシステムでは、デフォルトで HALT 命令がアイドルループで使用されるために発生します。「idle=poll」が有効になっている場合は、オペレーティングシステム上はアイドル状態でも、ハードウェアはプロセッサが常にビジーであると報告します。
この動作は仕様です。

解決方法
iLO5 は設計どおりに動作しています。iLO5 では、OS とは異なる CPU 使用率の値が表示されることがあります。

One-button Secure Erase プロセスの完了後、「Non-Volatile Memory Corruption Detected (不揮発性メモリの破損が検出されました)」というイベントが表示され、Integrated Management Log (IML) に記録されることがあります。

症状
One-button Secure Erase プロセスの完了後に、NVRAM が正常に消去されたことにより、以下のイベントが Integrated Management Log (IML) に記録される場合があります。

「Non-Volatile Memory Corruption Detected. Configuration settings restored to defaults. If enabled, Secure Boot security settings may be lost.」

解決方法
One-button Secure Erase の動作や機能への影響はないため、メッセージは完全に無視することができます。

A. iLO ライセンスオプション

表 5 には、各 iLO ライセンスに含まれる機能が示されています。

表 5 iLO Standard **およびライセンス機能**

項目	オンボード機能 (Standard)	リモートマネージメント 拡張ライセンス (Advanced) 標準添付あるいは選択必須オプション
ディレクトリサービス認証（Active Directory、LDAP）	×	○
Two-Factor 認証（Kerberos サポート）	×	○
統合リモートコンソール経由での仮想メディア	Pre-OS only	○
スクリプト方式仮想メディア	×	○
統合リモートコンソール（IRC）	Pre-OS only	○
IRC 経由でのビデオの録画および再生	×	○
仮想シリアルポートの録画および再生	×	○
SSH 経由でのテキストベースのリモートコンソール	×	○
Email アラート	×	○
リモート Syslog	×	○
アドバンスド電源管理（電力グラフ、動的消費電力上限設定）	×	○
iLO 連携管理	×	○
iLO 連携検出	○	○
リモートシリアルコンソール（仮想シリアルポート）	○	○
Server Health Summary	○	○
iLO 再起動	○	○
Redfish™API	○	○
Agentless Management	○	○
サーバーの状態監視	○	○
Web ベースの GUI	○	○
仮想電源制御	○	○
SSH/SMASH CLI（シリアルコンソールリダイレクションを含む）	○	○
IPMI/DCMI（シリアルコンソールリダレクトを含む）	○	○
Intelligent System Tuning	×	○
アップデートサービス-ダウングレードポリシー設定	×	○
パフォーマンス監視	×	○
ファームウェア検証	×	○
One-button セキュア消去	×	○

B. iLO 利用ポート番号

本機能では、以下のポートを使用しますので、ファイアウォールを設置されているネットワーク環境では、ファイアウォールでの対応が必要となります。

表 6 iLO 利用ポート番号

モジュール名	iLO ポート番号	方向	プロトコル	ポート番号	用途
Secure Shell (SSH)ポート	22*1	⇔	TCP	不定*6	iLO の SMASH-CLP サーバーと SSH クライアントの通信用。
Web サーバーNon-SSL ポート	80*1	⇔	TCP	不定*6	iLO の Web サーバーへの HTTP 通信用。
NetBIOS-NS ポート	137	⇔	UDP	不定*6	マイクロソフト Windows ネットワーク(名前解決)通信用。
SNMP ポート	161*1	⇔	UDP	不定*6	SNMP マネージャーとの SNMP 通信用。
Web サーバーSSL ポート	443*1	⇔	TCP	不定*6	iLO の Web サーバーへの HTTPS 通信用。
IPMI/DCMI over LAN ポート	623*1	⇔	UDP	不定*6	外部 IPMI クライアントとの LAN 経由での IPMI 通信用。
Universal Plug and Play ポート	1900	⇔	UDP	不定*6	iLO 連携機能での相互通信用 。
Link-Local Multicast Name Resolution(LLMNR)	5355	⇔	UDP	5355	同一ローカルリンク上の外部ホストに対して名前解決を許可するための通信用。
Virtual Media ポート	17988*1	⇔	TCP	不定*6	iLO の Virtual Media サーバーと IRC クライアントとの通信用。
Remote Console ポート	17990*1	⇔	TCP	不定*6	iLO のリモートコンソールサーバと IRC クライアントとの通信用。
SMTP サーバーポート	不定*6	⇔	TCP	25*2	外部 SMTP サーバーとの通信用。
DNS サーバーポート	不定*6	⇔	UDP	53	外部 DNS サーバーとの通信用。
Kerberos KDC サーバーポート	不定*6	⇔	TCP	88*3	外部 Kerberos サーバーとの暗号化通信用。
NTP サーバーポート	不定*6	⇔	UDP	123	外部 NTP サーバーとの通信用。
SNMP Trap ポート	不定*6	⇔	UDP	162*1	外部 SNMP マネージャーとのトラップ送信用。
Web サーバーSSL ポート	不定*6	⇔	TCP	443*5	iLO の Web サーバーへの HTTPS 通信用。
Remote Syslog サーバーポート	不定*6	⇔	UDP	514*4	外部 LDAP サーバーとの通信用。
LDAP サーバーポート	不定*6	⇔	TCP	636*3	外部 Kerberos サーバーとの暗号化通信用。

*1 Security - Access Settings で変更可能

*2 Management - AlertMail で変更可能

*3 Security - Directory で変更可能

*4 Management - Remote Syslog で変更可能

*5 URL 指定時に変更可能

*6 未使用ポートを使用

用語集

3DES	トリプル DES。Data Encryption Standard 暗号化アルゴリズム
ACPI	Advanced Configuration and Power Interface
AES	Advanced Encryption Standard
AHCI	Advanced Host Controller Interface
AHS	Active Health System (AHS)は、サーバーの状態や構成を監視し、変化があったときにログとして記録します。AHS ログは、保守の場面ですばやく障害の原因を判断するために利用されます。
AMP	Advanced Memory Protection (AMP)は、搭載メモリに対してミラーリング等の制御をすることにより、強固な耐障害性を実現する技術です。
AMS	Agentless Management Service (AMS)は、OS 上で動作し、iLO が直接収集できない OS イベントなどの情報を iLO へ送信するサービスです。iLO は、このサービスを通じて取得した情報を AHS ログとして記録し、Agentless Management へ展開します。
API	Application Programming Interface。アプリケーションプログラミングインターフェース
ARP	Address Resolution Protocol
ASR	Automatic Server Recovery。自動サーバー復旧
BIOS	Basic Input/Output System。基本入出力システム
BMC	Baseboard management controller
CA	Certificate authority。認証機関
CLP	Command Line Protocol。コマンドラインプロトコル
CN	Common Name。共通名
CNSA	Commercial National Security Algorithm。米 NSA（National Security Agency：国家安全保障局）が定めた暗号スイート。
COM ポート	Communication port。通信ポート
Cookie	Web サイトが特定の設定を保持するために、ハードディスクドライブに保存するスクリプトできない小さいテキストファイルです。サイトに戻ると、システムが前に保存された設定で Cookie を開くので、サイトに設定を渡すことができます。また、Cookie は、一時的にセッションデータを保存するために使用されます。
CR	Certificate request。証明書要求
CSR	Certificate Signing Request。証明書署名要求
CSV	Comma-separated value。カンマ区切りの値
DCMI	Data Center Manageability Interface。データセンター管理インターフェース
DD	ファイル変換およびコピーに使われる Unix プログラム
DDNS	Dynamic Domain Name System。動的 DNS
DDR	Double data rate。ダブルデータレート
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman key exchange
DIMM	Dual In-line Memory Module。デュアルインラインメモリモジュール。メモリチップを保持する小型回路基板。
DLL	Dynamic-link library。ダイナミックリンクライブラリ
DMTF	Distributed Management Task Force
DN	Distinguished Name。識別名
DNS	Domain Name System。ドメインネームシステム
DSA	Digital Signature Algorithm。デジタル署名アルゴリズム
DVO	Digital Video Out

ECC	Error-correcting code
EMS	Emergency Management Services
ESMPRO/ServerAgentService	ESMPRO/ServerManager と連携し、本機の監視、および各種情報を取得するためのソフトウェアです。インストール時に、OS のサービスとして常駐させる(サービスモード)か、OS のサービスなし(非サービスモード)で動作させるか決めることができます(プリインストール時はサービスモードでインストールします)。非サービスモードで動作させると、CPU、メモリなどのリソースを削減できます。
ESMPRO/ServerManager	ネットワーク上の複数のサーバーの管理、監視を行うソフトウェアです。
EXPRESSBUILDER	本機をセットアップする機能を持つソフトウェアです。本機内に格納され、POST 時に F10 キーを押して起動します。
FAT	File Allocation Table。ファイルアロケーションテーブル
FIPS	Federal Information Processing Standard。連邦情報処理標準。
FQDN	Fully Qualified Domain Name。完全修飾ドメイン名
GMT	Greenwich Mean Time。グリニッジ標準時
GRUB	Grand Unified Bootloader
HTML5	HyperText Markup Language 5
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IIS	Internet Information Services。インターネットインフォメーションサービス
iLO	Integrated Lights-Out。標準インターフェース仕様の IPMI2.0 に準拠してハードウェアを監視するコントローラーです。本機には標準でマザーボード上に組み込まれています。本機で採用しているコントローラーは第 5 世代のため、iLO5 と呼びます。
IML	Integrated Management Log。インテグレーテッドマネージメントログ
IPMI	Intelligent Platform Management Interface
IRC	Integrated Remote Console。統合リモートコンソール
ISO	International Organization for Standardization。国際標準化機構
Java IRC	Java バージョンの統合リモートコンソール
JRE	Java Runtime Environment
JSON	JavaScript Object Notation。JavaScript オブジェクトの表記法
KCS	Keyboard Controller Style
KDC	Key Distribution Center
KDE	K Desktop Environment（Linux 用）
KVM	Keyboard, video, and mouse。キーボード、ビデオ、およびマウス
LDAP	Lightweight Directory Access Protocol
LOM	Lights-Out Management。Lights-Out マネージメント
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MIB	Management information base。管理情報ベース。ネットワーク管理プロトコルでアクセスされる管理対象オブジェクトのデータベース。SNMP MIB は、ネットワークデバイスの SNMP エージェント（ルーターなど）で SNMP 管理ステーションが照会または設定できる 1 組のパラメーターです。
MIME	Multipurpose Internet Mail Extensions
MLD	Multicast Listener Discovery。マルチキャストリスナー検出
MMC	Microsoft Management Console。Microsoft 管理コンソール
MSA	Mail Submission Agent
MTA	Mail Transfer Agent
NAND	NX7700x サーバのマザーボードに組み込まれている、非揮発性のフラッシュメモリのパーティション。NAND 型フラッシュは Active Health System データや EXPRESSBUILDER ソフトウェアなどのファイルに使用されます。
NIC	Network interface card。ネットワークインターフェースカード。ネットワーク経由のデバイス間の通信を処理するデバイス。

NMI	Non-maskable interrupt。マスク不可能割り込み
NTLM	NT LAN Manager
NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
OU	Active Directory Organizational Units。Active Directory 組織単位
PAL	Programmable Array Logic。プログラマブルアレイロジック
PIM	Protocol-Independent Multicast。プロトコル独立型マルチキャスト
PKCS	Public-Key Cryptography Standards。公開鍵暗号化標準
POST	Power on self test。電源投入時セルフテスト
PuTTY	SSH、Telnet、rlogin、およびロー TCP プロトコルのクライアントならびにシリアルコンソールクライアントとして機能できる端末エミュレーター。
RAID Report Service	RAID の状態を監視し、障害等が起きたとき、ESMPRO/ServerAgentService へ情報を送信するサービスです。
RBSU	ROM-Based Setup Utility。BMC 構成ユーティリティ。
REST	Representational State Transfer
RESTful インターフェースツール	Representational State Transfer (REST) アーキテクチャーに基づき設計された API を実装したツールです。本ツールをインストールすると、JSON 形式で記述した保守用コマンドを HTTP プロトコルで iLO へ送信できます。
RPM	RPM Package Manager
RSA	パブリックキー暗号化用のアルゴリズム
SAID	Service Agreement Identifier
SAS	Serial Attached SCSI。シリアル接続 SCSI
SATA	ディスク シリアル ATA（SATA）ディスク。ATA（IDE）インターフェースから発展したもので、物理アーキテクチャーをパラレルからシリアルに変更し、プライマリー/セカンダリー（マスター/スレーブ）からポイントツーポイントに変更します。プライマリー（マスター）とセカンダリー（スレーブ）として 2 台のドライブを接続するパラレル ATA インターフェースと異なり、SATA ドライブは個別のインターフェースに接続されます。
SD	Secure Digital
SHA	Secure Hash Algorithm。セキュアハッシュアルゴリズム
SID	Security Identifier。セキュリティ識別子
SLAAC	Stateless Address Autoconfiguration
SMASH	Systems Management Architecture for Server Hardware
SMS	System Management Software。システム管理ソフトウェア
SNMP	Simple Network Management Protocol。簡易ネットワーク管理プロトコル
SNTP	Simple Network Time Protocol。簡易ネットワークタイムプロトコル
SPN	Service Principal Name。サービスプリンシパル名
SPP	Standard Program Package (SPP)は、BIOS/FW、および OSドライバーなどを含む基本的な FW/SW をまとめたパッケージです。SPP は、Starter Pack に含まれます。
SSA	Smart Storage Administrator (SSA)は、ディスクアレイコントローラーを設定して RAID を構築するユーティリティです。Windows または Linux 上にインストールして使用するほか、本機に組み込まれた EXPRESSBUILDER から起動できます。
SSD	Solid-State Drive。ソリッドステートドライブ
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On。シングルサインオン
Starter Pack	SPP、管理用アプリケーション、および電子マニュアルを含むソフトウェアパッケージです。Starter Pack はオプション製品として購入、または Web からダウンロードし、Windows/Linux OS 上で使用します。
SUM	Software Update Manager
TLS	Transport layer security。トランスポート層セキュリティ
TM	Trusted Module

TPM	Trusted Platform Module
TPM キット	セキュリティーコントローラーを本機に増設するためのオプション製品です。
UDP	User Datagram Protocol。ユーザーデータグラムプロトコル
UEFI	Unified Extensible Firmware Interface
UHCI	Universal Host Controller Interface。ユニバーサルホストコントローラーインターフェース
UID	Unit identification。ユニット識別子
UPN	User Principal Name。ユーザープリンシパル名
UPnP	Universal Plug and Play。ユニバーサルプラグアンドプレイ
UPS	Uninterruptible Power Supply。無停電電源装置
USB	Universal serial bus。ユニバーサルシリアルバス。デバイスを接続するために使用されるシリアルバス規格。
USM	User-based Security Model
UTC	Coordinated Universal Time。協定世界時
UTP	Unshielded Twisted Pair。シールドなしツイストペア
UUID	Universally Unique Identifier。ユニバーサルー意識別子
VSP	Virtual Serial Port。仮想シリアルポート
WBEM	Web-Based Enterprise Management
WINS	Windows インターネットネームサービス
エクスプレス通報サービス	電子メールなどを使い、本機が故障したときの情報(または予防保守情報)を保守センターに通報するソフトウェアです。ESMPRO/ServerAgentService または ESMPRO/ServerAgent とともに本機にインストールします。
エクスプレス通報サービス (HTTPS)	HTTPS 経由で、本機が故障したときの情報(または予防保守情報)を保守センターに通報するソフトウェアです。ESMPRO/ServerAgentService とともに本機にインストールします。
管理 PC	ネットワーク上から本機にアクセスし、本機を管理するためのコンピューターです。Windows または Linux がインストールされた一般的なコンピューターを管理 PC にすることができます。
システムメンテナンススイッチ	本機マザーボード上の DIP スイッチで、保守の場面において、初期化、パスワード、iLO セキュリティなどの機能をオンオフするときに使用します。
システムユーティリティ	システムユーティリティは、本機内に格納され、システム情報の確認、RBSU の呼出し、およびログの採取機能などを提供します。システムユーティリティは POST 時に F9 キーを押すと起動します。
装置情報収集ユーティリティ	本機の各種情報を収集するためのソフトウェアです。保守に必要な情報をまとめて採取できます。
ターシャリー	プライマリー、セカンダリーに続く、「3 番め」を意味する単語です。
ヘクサロビュラ	ヘクスローブ、またはトルクス(「トルクス」は他社商標です)とも呼ばれるネジ規格です。サイズは小さい順から、T1 から T100 まで決められ、サイズに合わない工具を使うとネジを傷める可能性があります。6lobe と略すこともあります。

NEC NX7700x シリーズ

iLO 5 ユーザーズガイド

[GZS-001832-001-00]

2022 年 1 月

Rev 3.00

日 本 電 気 株 式 会 社

東京都港区芝五丁目 7 番 1 号

TEL（03）3454-1111 （大代表）