Hewlett Packard Enterprise

HPE Integrated Lights-Out セキュリティテクノロジーの概要

摘要

HPE Integrated Lights-Out（iLO）は、データセンターでサーバーをリモート管理するための標準として広く受け入れられています。データセンターの管理にはあらゆる面でセキュリティ上の重要な懸念（リモート管理を含む）があるため、本書では、不正アクセスのリスクを防ぐために iLO が使用するファームウェアおよびハードウェア上の方式について説明します。さらに、iLO とそのホストシステムにアクセスポイントを提供するユーティリティおよびサービスについて説明します。また、iLO のセキュリティパラメーターおよび iLO 接続オプションの構成に関する推奨事項を提示します。すべての機能とユーティリティがすべての iLO に使用できるわけではありません。

部品番号: P01962-195
発行: 2020 年 2 月
版数: 1

目次

ご注意

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。Hewlett Packard Enterprise 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、Hewlett Packard Enterprise 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、Hewlett Packard Enterprise の Web サイトの外に移動します。 Hewlett Packard Enterprise は、Hewlett Packard Enterprise の Web サイト以外の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

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。

Java®および Oracle®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。

Intel®、インテル、およびインテル®Xeon®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。

すべてのサードパーティのマークは、それぞれの所有者に帰属します。

HPE iLO セキュリティ

HPE iLO は、サーバーに組み込まれた自律型管理プロセッサーです。これにより、サーバーのセットアップが簡素化され、サーバーのヘルス監視が行われ、電力と温度の最適化が可能になり、リモートサーバーの管理が容易になります。このような幅広い範囲の制御は、サーバーの OS、さらにはサーバーのハードウェアの状態に依存しません。iLO は、その強力な機能を不正ユーザーから保護するように設計されています。

重要: データセンターの管理者は、施設の物理面のセキュリティに対して責任を負っています。サーバーに物理的にアクセスできる人は誰でも、 システムメンテナンススイッチを使用して、iLO の構成を変更できる可能性があります。サーバーシャーシ内へのアクセス権限を持つユーザーはスーパーユーザーまたは管理者であるものとします。

iLO を使用すると、懸念なしにご使用のサーバーを展開できます。強力な認証、高度に構成可能で強力な承認プロセスを持つユーザー権限、およびデータ、キーストローク、およびセキュリティキーの暗号化を使用します。ハードウェア設計では、キーと、パスワードの機密情報を保護し、すべてのサーバートラフィックから iLO の管理トラフィックを分離できます。

FIPS 認証と Common Criteria 認定

HPE iLO 5 v1.11 は以下を取得しています。

- HPE iLO 5 v1.11 の暗号モジュールは、FIPS 140.2 レベル 1 で検証済みです。**https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3122** で NIST Cryptographic Module Validation 認定を参照してください。
- HPE iLO 5 v1.11 は Common Criteria 認定に合格しており、EAL 2+（ALC_FLR.2）への適合に対して Common Criteria 認定が授与されました。**https://www.cse-cst.gc.ca/en/node/2112/html/28448** で認定レポートを参照してください。

ファームウェアベースの保護

iLO では、不正アクセスやフラッシングから保護を行うファームウェアベースのメカニズムを使用しています。

不正アクセスの防止

iLO ポータルを介したアクセスには、認証、認可、データ整合性、およびセキュリティキーを含むマルチレイヤーのセキュリティプロセスが関与しています。iLO ファームウェアはプライベートキーを使用してデジタル署名されており、不正なファームウェアは実行できません。

認証

ネットワーク接続の反対側にいるユーザーを判断します。認証は、ローカルで、またはディレクトリサービスを介して実行できます。サポートされる認証方法には、ローカルアカウント、Kerberos 認証、ディレクトリ統合、SSO、およびスマートカードが含まれます。

許可

アクションを実行しようとするユーザーが、そのアクションを実行する権限を持っているかどうかを判断します。ローカルアカウントを使用して個別の iLO ユーザーを定義し、そのサーバーアクセス権限を変えることができます。ディレクトリサービスを使用して、数千ものユーザーとシステム管理ロールをサポートしているスケーラブルな中央データベースで、ネットワークのユーザーアカウントとセキュリティポリシーを維持します。

データ整合性

受信したコマンドまたはデータが変更されていないことを検証します。iLO は、デジタル署名と、iOS および Android で使用可能な信頼済みのリモートコンソールおよび iLO モバイルアプリケーションを使用します。

セキュリティキー

機密データおよびトランザクションの機密保持を管理します。iLO は、Web ページの TLS による暗号化、およびリモートコンソールと仮想シリアルポートデータの AES による暗号化を介してプライバシーを保護します。最高の暗号化方式（AES など）のみの使用を許可するように iLO を構成できます。iLO はセキュリティのレイヤーと業界標準方式を使用して、サーバーに安全にアクセスします。高暗号化モードが使用されていない場合、iLO はより強度の弱いキーまたはアルゴリズムをネゴシエートすることがあります。

フラッシングの防止

フラッシングは永続的なサービス拒否（PDOS）攻撃です。理論的に、PDOS 攻撃はネットワークベースのファームウェアのアップデート中に脆弱性を利用する場合があります。PDOS 攻撃を受けてインストールされた不正なファームウェアは、許可されていないサーバーアクセスや、恒久的なハードウェアの損傷を引き起こす可能性があります。

iLO では、以下の保護を備えています。

承認されたファームウェアアップデート

iLO ファームウェアイメージは、4096 ビットのプライベートキーでデジタル署名されています。ブートブロックは、iLO がリセットされるたびにデジタル署名を確認します。iLO は、ファームウェアアップデートの実行を許可する前にデジタル署名を確認します。リモートのフラッシングには、オプションの Two-Factor 認証を含むログイン認証と承認が必要です。

暗号化されていないポート

iLO では、ポート暗号化ステータスを明確に定義しています。暗号化されていないポート（IPMI など）へのアクセスを無効にできます。iLO にアクセスするには、パスワードを無効にする場合を除き、パスワードが必要です。

認証と監査証跡

iLO では、すべてのインターフェイスでの認証の失敗と成功のログが作成されます。SSH キー認証により、ブルートフォースアタックの成功の可能性をかなり低くすることができます。保護を強化するため、iLO 5 では 2048 ビットの RSA キーを使用します。CNSA セキュリティ状態を使用している場合、iLO では、ECDSA 384 ビットキーが必要です。

失敗したログインの遅延

iLO では、すべてのログインアクティビティをキャプチャしています。ブルートフォースアタックおよびディクショナリアタックを妨げるため、失敗するログイン試行中にタイミングを漸進的に遅延します。

重要なセキュリティパラメーターのアクセスと変更の制限

iLO では、ユーザーアカウント、ログの変更、証明書などのセキュリティパラメーターの変更を記録しています。この機能により、情報への潜在的な不正アクセスをトレースできます。

日次のファームウェアフラッシュ制限

iLO およびサーバーハードウェアを執拗なフラッシュ攻撃から保護するために、iLO では、サポートされている各ファームウェアタイプをフラッシュできる 1 日あたりの回数を制限しています。制限は 20 回です。これには、ファームウェアフラッシュアクティビティの成功と失敗の両方が含まれます。ファームウェアフラッシュカウントは 24 時間ごとに、またはファームウェアのアップデートに成功してから 24 時間後にリセットされます。ファームウェアフラッシュ制限は、どのアプリケーションまたはインターフェイスから開始されたファームウェアアップデートにも適用されます。

ファームウェアフラッシュカウントは不揮発性メモリに保存されます。フラッシュ制限を超えた場合、ファームウェアをフラッシュできず、後で再試行する必要があることがソフトウェアから通知されます。

ハードウェアベースの保護

iLO サブシステムには、独立した命令キャッシュとデータキャッシュを搭載した 32 ビットの iLO RISC プロセッサーコア、メモリコントローラー、SDRAM、NVRAM、管理 ROM、および NIC が組み込まれています。iLO サブシステムには、システムヘルスモニタリング、コンソールリダイレクション、ホスト/ファイアウォールブリッジ、サーバー NIC、仮想メディアなどの他の構成要素も含まれます。**図 1: iLO プロセッサーブロック図**で示すように、iLO は、システムの電源投入機能（サーバーの電源が入っているときにのみ使用可能）と補助電源投入機能（サーバーに電源が供給されている間は使用可能）から構成されます。

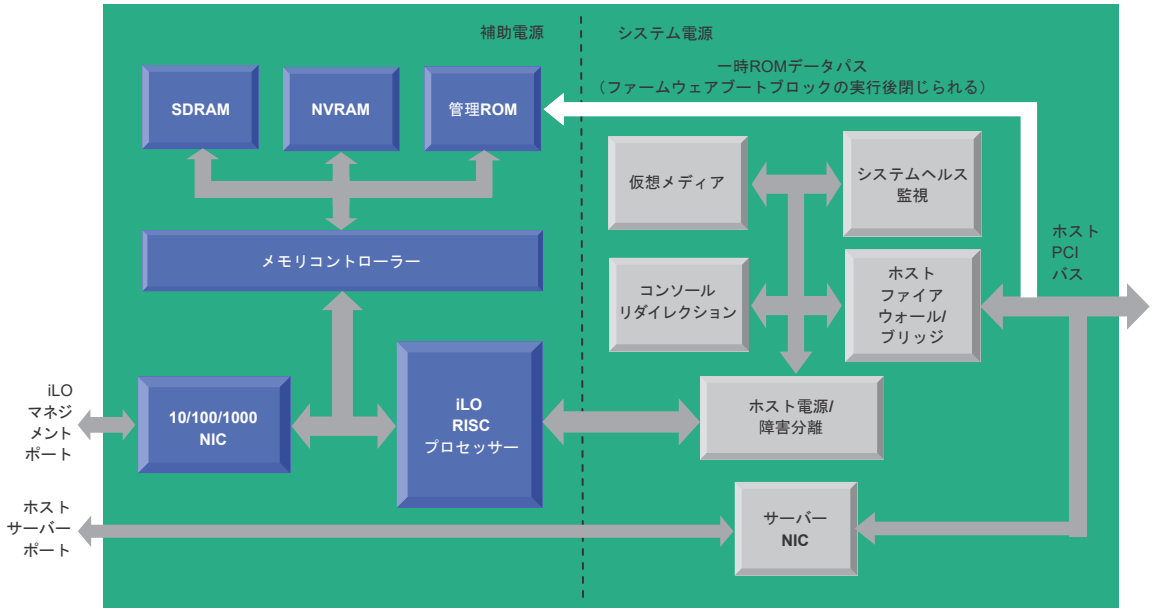


図 1: iLO プロセッサーブロック図

保護された管理 ROM

iLO ファームウェアイメージの署名チェックは 2 種類あります。

- iLO フラッシュデバイスにプログラムされる前の新しいイメージの検証。
- iLO 起動時のファームウェアイメージの整合性チェック。

イメージの検証

イメージ全体が SHA512 でハッシュされ、Hewlett Packard Enterprise の RSA 4096 ビットプライベートキーを使用して署名されます。この署名ブロックは、ファームウェアのバイナリイメージの先頭に追加されます。

ファームウェアのアップデートを実行する場合、ハッシュは Hewlett Packard Enterprise のパブリックキーを使用して現在実行中の iLO ファームウェアによって復号化されます。このハッシュはイメージ全体のハッシュと比較されます。一致している場合、ファームウェアのアップデートは続行可能です。署名ブロックは破棄されます。

Silicon Root of Trust

iLO 5 チップセットは Silicon Root of Trust の機能を実行し、チップ製造施設でシリコンハードウェアに組み込まれる暗号化されたハッシュが含まれています。この機能により、ブートプロセスを破壊する可能性のあるマルウェア、ウイルス、または侵害されたコードを入り込ませることが事実上不可能になります。iLO ファー

ムウェアが起動するたびにファームウェアの整合性をチェックするのではなく、iLO チップセットシリコンに永続的に格納されている暗号化ハッシュに一致するかどうかに基づいて、iLO 5 ハードウェアが iLO ファームウェアを実行するかどうかを決定します。

Silicon Root of Trust は、かつてないレベルのハードウェアセキュリティを実現します。

Silicon Root of Trust には次のような特徴があります。

- シリコンチップハードウェア自体に直接組み込まれています。
- 事実上、変更不可能です。
- ファームウェアをサプライチェーンから認証可能です。
- 安全な起動プロセスを実現します。

ファームウェアイメージが壊れて起動しない場合は、iLO が自動的にシステムリカバリセットのバックアップイメージから復旧します。iLO ファームウェアイメージの各要素（カーネルなど）も署名されています。これらの整合性署名は、フラッシュプロセス中に破棄されません。

保護された PCI バス

iLO は、メモリとファームウェアに保存されたキーとデータを保護し、PCI バス経由のキーへの直接アクセスを許可しません。

ネットワークポートとマネジメントポート

iLO のファイアウォールおよびブリッジロジックによって、iLO マネジメントポートとサーバーの Ethernet ポートとの間の接続ができません。共有ネットワークポート（SNP）を使用しても、iLO は自身の 10/100/1000 Ethernet ポートとサーバーの Ethernet ポートとの間のトラフィックをブリッジできません。このため、サーバーネットワークでの攻撃が iLO を危険にさらすことはありません。その逆も同様です。

詳しくは

iLO ネットワーク接続オプション

共有ネットワークポート

共有ネットワークポート（SNP）では、iLO マネジメントトラフィックは、もう 1 つ別のポートを専用で iLO マネジメントトラフィックに割り当てるのではなく、サーバー NIC 上でのサイドバンド接続を可能にします。iLO のトラフィックはサーバーの OS トラフィックとポートを共有しますが、iLO とサーバー NIC の両方で、独自の MAC と IP アドレスを持ちます。この構成により、他のデバイスは確実に iLO のアドレスを個別に指定できます。この機能は、管理および本番の両方のトラフィックを処理するために 1 つのネットワークインフラストラクチャを設置して維持する場合に利点があります。

ご使用のサーバーが SNP をサポートしているかどうかを確認するには、サーバーのドキュメントを参照してください。Hewlett Packard Enterprise では、HPE BladeSystem サーバーブレードまたは Synergy コンピュートモジュールでの SNP をサポートしていません。

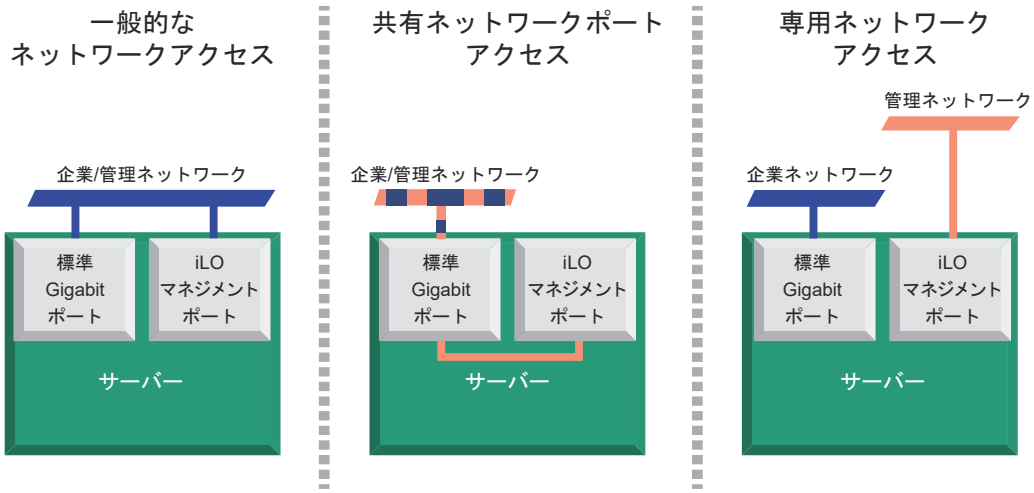


図 2: 共有および専用のネットワークのトラフィックパス

仮想 LAN

共有ネットワークポート

仮想 LAN（VLAN）タグを実装すると、iLO 共有ネットワークポート（SNP）セキュリティが強化されます。VLAN タグを有効にすると、iLO SNP は仮想 LAN の一部になります。VLAN は、ネットワークトラフィックをセグメントに分離する論理ネットワークです。作成したルールに従って、あるセグメントのトラフィックは別のセグメントに入らないため、セキュリティが向上します。物理的に同じ LAN に接続されている場合でも、同じ 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。SNP NIC は、Ethernet フレームで VLAN ID を調べて、その ID の設定値と比較します。それらが一致する場合、SNP は VLAN タグのフレームを除去し、それを iLO に転送します。それらが一致しない場合、SNP はフレームをサーバーに転送します。SNP NIC は、すべての送信 Ethernet フレームに VLAN タグを挿入します。

iLO 専用ネットワークポート

VLAN タグは、iLO 5 1.43 以降の iLO 専用ネットワークポートでサポートされています。VLAN タグ機能を使用して、適切に構成されたデバイスと未構成のデバイスを区別できます。VLAN タグ機能を使用すると、未構成のデバイスが物理的に接続されている場合でも、それらをネットワークから遠ざけることができます。

システムメンテナンススイッチ

Hewlett Packard Enterprise サーバーには、サーバーセキュリティのさまざまな側面を制御する、ハードウェアのシステムメンテナンススイッチがあります。

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。

システムメンテナンススイッチの使用について詳しくは、サーバーメンテナンスおよびサービスガイドを参照してください。

iLO セキュリティ（位置 1）

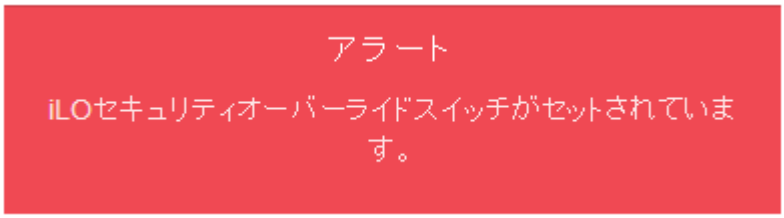
システムメンテナンススイッチの iLO セキュリティ設定により、管理者は、サーバーのシステムボードを物理的に制御して、緊急時にアクセスすることができます。

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。

iLO セキュリティを無効にすると、次の影響があります。

- iLO が本番環境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、すべてのセキュリティ認証確認が無効になります。
- iLO が、高セキュリティ、FIPS、または CNSA の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：
  - ホストシステムから実行される iLO RESTful API および RIBCL コマンドに対してユーザー名とパスワードの制限が適用されます。
  - 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によって、iLO へのログインに関するパスワード要件は無効になりません。

  ホストサーバーがリセットされると、UEFI システムユーティリティソフトウェアが実行されます。
- iLO のネットワーク構成が工場出荷時のデフォルト設定にリセットされます。工場出荷時のデフォルトネットワークインターフェイスがネットワークに接続されている場合、iLO はネットワーク上で利用可能です。この変更は、iLO セキュリティが無効に設定され、iLO 機能が無効になった場合でも行われます。
- iLO Web インターフェイスページに、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。
- SNMP アラートの送信先が構成されている場合、iLO が iLO セキュリティ構成の変更後に起動するとアラートが送信される。
- システムリカバリ権限が必要なアクションは実行できません。

  iLO にログインすると、既存のアカウントと一致するユーザー名とパスワードを入力した場合でも、匿名アカウントが使用される。

電源オンパスワードの制御（位置 5）

このスイッチは、コールドブートを実行するたびにサーバーがパスワードを要求するかどうかを制御します。オフ（デフォルト）の場合、システムの電源が切断されていてコールドブートを実行するたびに、電源投入時パスワードが必要です。オンの場合、電源投入時パスワードは無効です。UEFI システムユーティリティでパスワードを設定します。

デフォルトのリストア（位置 6）

スイッチがオンの位置にある場合（デフォルトはオフ）、すべての製造時デフォルト設定がリストアされます。ただし、UEFI でセキュアブートを有効にした場合、以下の項目は工場出荷時のデフォルト設定にリセットされません。

- セキュアブートは無効にならず、有効のままとなります。
- ブートモードがレガシーに設定されている場合でも、ブートモードは UEFI ブートモードのままとなります。
- セキュアブートデータベースはそのデフォルトの状態にリストアされません。
- iSCSI Software Initiator の構成設定はデフォルト設定にリストアされません。

システムメンテナンススイッチの仕様について詳しくは、ご使用のサーバーのハードウェアガイドを参照してください。

iLO セキュリティを無効にする理由

次の状況で、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すべてのユーザーアカウントがロックアウトされた。
- 不適切な設定により、ネットワーク上に iLO が表示されず、ROM ベースの構成ユーティリティが無効になっている。
- iLO に、iLO の NIC がオフになっているか、iLO ネットワーク構成が正しくないため、ネットワーク経由で到達できない。UEFI システムユーティリティを使用して構成を修正することが不可能であるか、または不便である。

  iLO セキュリティを無効にすると、iLO のネットワーク構成が工場出荷時のデフォルト設定にリセットされます。
  - ほとんどのサーバーでは、このアクションによって DHCP および iLO 専用ネットワークポートが有効になります。
  - iLO 専用ネットワークポートがオプションのアドオンカードであるサーバーでは、このアクションによって DHCP および共有ネットワークポートが有効になります。
- ユーザー名が 1 つだけ設定され、パスワードを忘れた。
- バッテリ駆動の SRAM メモリデバイスに保存されている構成情報を消去します。

  iLO を起動すると、バッテリ駆動の SRAM メモリデバイスに保存されている構成情報が不揮発性フラッシュメモリ（NAND）にバックアップされます。SRAM が削除されると、構成が自動的にリストアされます。iLO セキュリティを無効にすると、SRAM データが自動的にリストアされません。

Trusted Platform Module および Trusted Module

Trusted Platform Module および Trusted Module 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。iLO 概要ページに以下の **TPM ステータス**または **TM ステータス**情報が表示されます。

- **未サポート** — TPM または TM はサポートされていません。
- **存在しません** — TPM または TM は取り付けられていません。
- **装着: 有効** — TPM が取り付けられていて、有効になっています。

TPM または TM のモジュールがサーバーに取り付けられている場合は、**モジュールタイプ**が表示に追加されています。モジュールタイプは、TPM が取り付けられているかサポートされているかを示すステータス、またはサポートされているモジュールのバージョンを示すステータスのいずれかを表示します。

- **TPM 1.2**
- **TPM 2.0**
- **TM 1.0**
- **未指定**
- **未サポート**

IT インフラストラクチャセキュリティの留意事項

iLO ネットワーク接続オプション

iLO は、専用の管理ネットワークまたは本番環境ネットワークの共有接続を使用してネットワークに接続できます。

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。ネットワークが独立しているため、性能が向上し、どのワークステーション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、本番環境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、サーバーへの冗長アクセスが提供されます。この構成では、本番環境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。専用管理ネットワークは、優先される iLO ネットワーク構成です。

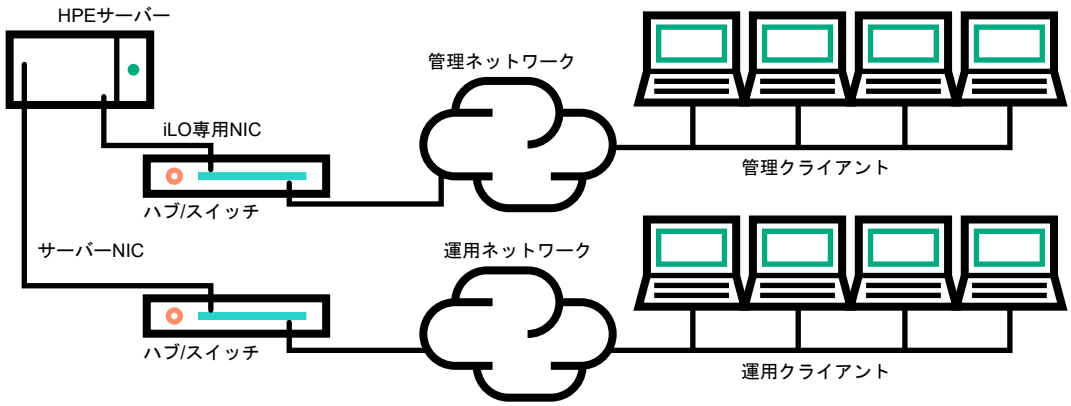


図 3: 専用管理ネットワーク

本番環境ネットワーク

この設定では、NIC と iLO ポートの両方を本番環境ネットワークに接続します。iLO で、このタイプの接続は、共有ネットワークポート構成と呼ばれます。特定の Hewlett Packard Enterprise 内蔵 NIC とアドオンカードが、この機能を提供します。この接続により、ネットワークのどこからでも iLO にアクセスできます。共有ネットワークポート構成を使用すると、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やインフラストラクチャの量が減ります。

この設定の使用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 のパフォーマンスが低下することがあります。
- サーバーのブートプロセス時およびオペレーティングシステム NIC ドライバーのロードおよびアンロード時に、短時間（2〜8 秒）、ネットワークから iLO にアクセスできません。この短い時間の経過後に、iLO の通信がリストアされ、iLO がネットワークトラフィックに応答します。

  このようなシチュエーションが起きた場合は、リモートコンソールと、接続されている iLO 仮想メディアデバイスが切断されることがあります。

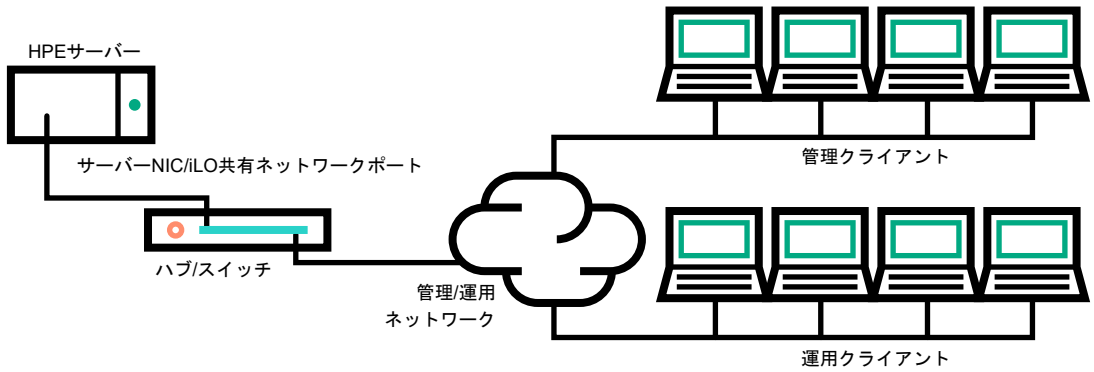


図 4: 共有ネットワーク接続

詳しくは

ネットワークポートとマネジメントポート

iLO とサーバーブレードまたは Synergy コンピュートモジュール間の通信

ProLiant c-Class サーバーブレード

HPE BladeSystem アーキテクチャーでは、単一のエンクロージャーで複数のサーバーを保持します。独立した電源サブシステムは、そのエンクロージャー内のすべてのサーバーに電源を供給します。ProLiant c-Class サーバーブレードでは、iLO を使用してアラートおよび管理情報をサーバーブレードインフラストラクチャ全体に送信します。

ProLiant c-Class サーバーのコンポーネント間には厳密な通信階層があります。Onboard Administrator（OA）の管理モジュールは、各サーバーブレード上の iLO プロセッサーと通信します。iLO プロセッサーまたは OA モジュールからサーバー NIC への接続はありません。iLO プロセッサーは、インフラストラクチャ内にある他のサーバーブレードの存在に関する情報、およびサーバーブレードを起動するために必要な電流が電源サブシステムから供給できるかどうかに関する情報を保持しているだけです。BladeSystem エンクロージャーの背面にある 2 つのポートから、サーバーブレード上の iLO ネットワーク接続にアクセスできます。

Synergy コンピュートモジュール

HPE Synergy 12000 フレームでは、単一のエンクロージャーで複数のサーバーを保持します。独立した電源サブシステムは、そのエンクロージャー内のすべてのサーバーに電源を供給します。iLO は、ハードウェアインフラストラクチャ全体にアラートと管理情報を送信します。

システムのコンポーネント間には厳密な通信階層があります。フレームリンクモジュールは、 各 Synergy コンピュートモジュールの iLO プロセッサーと通信します。iLO プロセッサーまたはフレームリンクモジュールからサーバー NIC への接続はありません。iLO プロセッサーは、インフラストラクチャ内にある他のコンピューティングモジュールの存在に関する情報、およびコンピューティングモジュールを起動するために十分な電流が電源サブシステムから供給できるかどうかに関する情報を保持しているだけです。エンクロージャーの背面にある 2 つのポートから、Synergy コンピュートモジュール上の iLO ネットワーク接続にアクセスできます。

セキュリティ監査

多くの企業には、定期的なセキュリティ監査を義務付けるポリシーがあります。iLO には、iLO の構成および操作で発生したイベントに関連する、日付および時刻のスタンプが付いた情報を含むイベントログがあります。iLO Web インターフェイスでログにアクセスできます。iLO RESTful API を使用すると、自動化テストを

セットアップしたり、日付/時刻ごとに、およびセキュリティイベントに関する情報にアクセスできる認証済みユーザーごとにログを解析する抽出プロセスをセットアップしたりできます。

セキュリティ脆弱性スキャナーと iLO

セキュリティ脆弱性スキャナーは、調査および対処が必要な脆弱性を調査するためにサーバー環境で使用されます。iLO チームは、iLO ファームウェアのリリースごとに、弊社の品質研究所でセキュリティ脆弱性スキャナーを使用します。セキュリティ脆弱性スキャナーの使用に関連する、既知の問題とベストプラクティスがあります。組織のビジネス要件によって脆弱性スキャンが必要とされる場合は、iLO のセキュリティ状態を高セキュリティ以上に設定することがセキュリティのベストプラクティスであることを覚えておいてください。

本番環境に展開する前に、ラボ環境で新しいバージョンのセキュリティ脆弱性スキャナーをテストすることがベストプラクティスです。定義により、セキュリティ脆弱性スキャナーは既知または疑いのある脆弱性のインターフェイスを調査します。実際には、スキャナーはテスト対象のインターフェイスのハッキングを試みています。この操作は、スキャン対象のシステムの安定性に悪影響を与える可能性があります。このため、小規模な範囲から始めて、さらに広い範囲、そして本番環境へと移すことが賢明です。

ほとんどのセキュリティ脆弱性スキャナーが特定する既知の問題がいくつかあります。これらの項目については、以下のセクションで説明しており、修復の推奨事項を含んでいます。示されている問題の多くは、iLO のセキュリティ状態を高セキュリティまたはそれ以上に設定することによって解決されます。

X.509 証明書のサブジェクト CN がエンティティ名と一致しない

デフォルトの自己署名の SSL 証明書を、認証機関（CA）によって署名された証明書と置き換えてください。iLO が工場から出荷される時点では、お客様の情報とサーバーの DNS 名/IP アドレスは不明です。そのため、iLO はデフォルトの自己署名証明書を使用します。

iLO ファームウェアは、CA から署名済み証明書を要求するために使用できる証明書署名リクエスト（CSR）を作成する機能を提供します。その後、その署名済み証明書を iLO にインポートできます。

- iLO Web インターフェイスを使用してこのタスクを実行するには、**SSL 証明書の取得とインポート**または HPE iLO 5 ユーザーガイドを参照してください。
- RIBCL スクリプトを使用してこのタスクを実行するには、HPE iLO 5 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。
- RESTful インターフェイスツールおよび iLO RESTful API を使用してこのタスクを実行するには、Web サイト **https://www.hpe.com/support/restfulinterface/docs** を参照してください。

IPMI 2.0 RAKP RMCP +認証 HMAC パスワードハッシュの暴露

IPMI 仕様で要求される IPMI ハンドシェイクは、より安全でなければなりません。iLO 5 では IPMI はデフォルトで無効になっています。積極的に IPMI を使用していないお客様の場合、Hewlett Packard Enterprise では、IPMI over LAN インターフェイスを無効のままにしておくことをお勧めします。

この問題に関するセキュリティ報告は、Web サイト **http://www.hpe.com/support/iLO234-SB-CVE-2013-4786** から入手できます。

- iLO Web インターフェイスを使用して IPMI over LAN を有効または無効にするには、**iLO アクセス設定の構成**または HPE iLO 5 ユーザーガイドを参照してください。
- XML スクリプトを使用して IPMI を有効または無効にするには、HPE iLO 5 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。
- RESTful インターフェイスツールおよび iLO RESTful API を使用して IPMI を有効または無効にするには、Web サイト **https://www.hpe.com/support/restfulinterface/docs** を参照してください。

Hewlett Packard Enterprise では、IPMI over LAN 機能の代替として iLO RESTful API をお勧めします。iLO RESTful API および RESTful インターフェイスツールについて詳しくは、**http://www.hpe.com/info/redfish** または **https://www.hpe.com/support/restfulinterface/docs** を参照してください。

IPMI を使用する必要がある場合に、それを有効にすると、この問題が露見します。

TLS/SSL サーバー X.509 証明書が信頼されていない

デフォルトの自己署名の SSL 証明書を、認証機関（CA）によって署名された証明書と置き換えてください。iLO が工場から出荷される時点では、お客様の情報とサーバーの DNS 名/IP アドレスは不明です。そのため、iLO はデフォルトの自己署名証明書を使用します。

iLO ファームウェアは、CA から署名済み証明書を要求するために使用できる証明書署名リクエスト（CSR）を作成する機能を提供します。その後、その署名済み証明書を iLO にインポートできます。

- iLO Web インターフェイスを使用してこのタスクを実行するには、**SSL 証明書の取得とインポート**または HPE iLO 5 ユーザーガイドを参照してください。
- RIBCL スクリプトを使用してこのタスクを実行するには、HPE iLO 5 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。
- RESTful インターフェイスツールおよび iLO RESTful API を使用してこのタスクを実行するには、Web サイト **https://www.hpe.com/support/restfulinterface/docs** を参照してください。

IPMI 1.5 GetChannelAuth レスポンス情報の暴露

これは IPMI プロトコルの Hewlett Packard Enterprise のサポートに基づく仮想的な脆弱性です。iLO 自体は、この脆弱性の影響を受けやすくありません。この脆弱性レポートは、IPMI を無効にすることで抑止できます。

- iLO Web インターフェイスを使用して IPMI over LAN を有効または無効にするには、**iLO アクセス設定の構成**または HPE iLO 5 ユーザーガイドを参照してください。
- XML スクリプトを使用して IPMI を有効または無効にするには、HPE iLO 5 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。
- RESTful インターフェイスツールおよび iLO RESTful API を使用して IPMI を有効または無効にするには、Web サイト **https://www.hpe.com/support/restfulinterface/docs** を参照してください。

TCP シーケンス番号予測の脆弱性

iLO は TCP シーケンス番号のランダム化を使用しており、TCP シーケンス番号予測攻撃に対する抵抗性があります。iLO はこの脆弱性の影響を受けやすくありません。

IPMI 2.0 RAKP RMCP +認証ユーザー名の暴露

IPMI 仕様では、あらかじめ認証されたクライアントが構成済みのユーザー名の存在を確認できます。Hewlett Packard Enterprise では、デフォルトのユーザー名を変更することをお勧めします。

IPMI を積極的に使用していない場合、Hewlett Packard Enterprise ではインターフェイスを無効にすることをお勧めします。

- iLO Web インターフェイスを使用して IPMI over LAN を有効または無効にするには、**iLO アクセス設定の構成**または HPE iLO 5 ユーザーガイドを参照してください。
- XML スクリプトを使用して IPMI を有効または無効にするには、HPE iLO 5 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。
- RESTful インターフェイスツールおよび iLO RESTful API を使用して IPMI を有効または無効にするには、Web サイト **https://www.hpe.com/support/restfulinterface/docs** を参照してください。

脆弱な暗号化キー

この脆弱性は、iLO 5 のセキュリティ状態を**高セキュリティ**に設定することで対処できる場合があります。このアクションには、iLO がより強度の強い暗号を使用する必要があります。

この脆弱性は、デフォルトの SSL 証明書を使用している場合も報告されます。

iLO ファームウェアは、CA から署名済み証明書を要求するために使用できる証明書署名リクエスト（CSR）を作成する機能を提供します。その後、その署名済み証明書を iLO にインポートできます。

- iLO Web インターフェイスを使用してこのタスクを実行するには、**SSL 証明書の取得とインポート**または HPE iLO 5 ユーザーガイドを参照してください。
- RIBCL スクリプトを使用してこのタスクを実行するには、HPE iLO 5 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。
- RESTful インターフェイスツールおよび iLO RESTful API を使用してこのタスクを実行するには、Web サイト **https://www.hpe.com/support/restfulinterface/docs** を参照してください。

TCP タイムスタンプ応答

これは標準の TCP 動作です。この動作は、理論的にシステムの稼動時間を見積もるために使用できるため、さらなる攻撃に利用される可能性があります。CVE 脆弱性評価は 1 であり、非常に低くなっています。

Missing HTTPOnly Flag from Cookie

セキュリティスキャナーによって、脆弱性として、`Missing HTTPOnly Flag from Cookie` と報告された場合、クライアント側スクリプト攻撃（XSS）による HTTP-only Cookie へのアクセスを防ぐクライアント側防御メカニズムを示しています。HTTP-only Cookie は、すべての XSS エクスプロイトを防止するわけではないため、それらを使用することが、XSS の脆弱性を解消するための代替策にはなりません。この設定は一部のブラウザーではサポートされていないため、依存できません。ブラウザーのバージョンは、各 iLO 構成で異なります。

Hewlett Packard Enterprise では、XSS 攻撃に対する防御方法を実装しています。利用可能な最新のセキュリティの機能強化については、HPE Integrated Lights-Out 5（iLO 5）ファームウェアのダウンロードページを参照してください。さらに、デフォルトの自己署名証明書を、認証機関によって署名された証明書と置き換えてください。

iLO 5 では、他のサーバーからのトラッカー、スクリプト、HTML などの外部から提供されたコンテンツを使用しません。iLO 5 内には、管理者から提供されたものではないページコンテンツはありません。そのため、報告された脆弱性 `Missing HTTPOnly Flag from Cookie` は、実際の脆弱性ではありません。

iLO 製品をスキャンする際に、このエラーを無視するか、 `Missing HTTPOnly Flag from Cookie` のスキャンを無効にします。

iLO の機能によって使用されるポート

ネットワーク設定とポート

表 1: iLO 経由で構成可能なネットワーク設定とポートにリストされているポートを、サイトの要件またはセキュリティのイニシアチブに適合するように構成できます。これらの設定は、ホストシステムには影響しません。

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 ブラウザーの構成を変更する必要があります。これらの設定を変更すると、変更を有効にするためにリセットが必要になります。

表 1: iLO 経由で構成可能なネットワーク設定とポート

アクセス設定	説明またはデフォルト値
IPMI/DCMI over LAN	LAN 経由の iLO との IPMI/DCMI通信を許可するかどうかを指定します。 デフォルトは、無効です。
IPMI/DCMI over LAN ポート	UDP 623
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有効または無効にすることができます。 初期設定では有効になっています。
リモートコンソールポート	TCP 17990
セキュアシェル（SSH）	SSH 機能を有効または無効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。 初期設定では有効になっています。
セキュアシェル（SSH）ポート	TCP 22
SNMP	iLO が外部の SNMP 要求に応答するかどうかを指定します。 初期設定では有効になっています。
SNMP ポート	UDP 161
SNMP トラップポート	SNMP アラート用の UDP 162（送信のみ）。
仮想メディア	仮想メディアを有効にするか無効にするかを指定できます。 初期設定では有効になっています。

表は続く

アクセス設定	説明またはデフォルト値
仮想メディアポート	TCP 17988
Web サーバー	iLO Web サーバー経由のアクセスを有効または無効にすることができます。 初期設定では有効になっています。
Web サーバー非 SSL ポート（HTTP）	TCP 80
Web サーバー SSL ポート（HTTPS）	TCP 443

その他のポート

セキュリティ管理者は、**表 2: iLO が使用するその他のポート**にリストされているポートを知っておく必要がある場合があります。これらのポートは、サードパーティの送信サービス用です。

表 2: iLO が使用するその他のポート

ポート	プロトコル	タイトルの設定	iLO 内のロケーション
88	TCP、UDP	Kerberos KDC サーバーポート	**セキュリティ** > **ディレクトリ**
636	TCP	ディレクトリサーバー LDAP ポート	
25	TCP	SMTP	**管理** > **アラートメール**
514	UDP	syslog	**管理** > **リモート Syslog**
53	UDP	DNS	なし
1900	UDP	SSDP	なし
67	UDP	DHCP	なし
68	UDP	DHCP	なし

詳しくは

iLO アクセス設定の構成

HPE iLO 5 のセキュリティに関する推奨事項

iLO は、強力な権限付与、認証、および暗号化によって、ネットワーク化された環境に本来備わっている多くのセキュリティリスクを最小限に抑えます。**セキュリティガイドライン**に従うことで、攻撃の可能性をさらに減らすことができます。

セキュリティガイドライン

iLO をセットアップして使用する場合は、セキュリティを最大化するために、次のガイドラインを考慮してください。

- 専用の管理ネットワーク上に iLO を構成します。Hewlett Packard Enterprise では、データネットワークとは別のプライベート管理ネットワークを確立することをお勧めします。管理ネットワークは、管理者のみがアクセスできるように構成します。

  共有ネットワークに iLO デバイスを接続する場合、iLO デバイスを個々のサーバーと考え、それらのデバイスをセキュリティおよびネットワークの監査対象に含まれるようにします。

- iLO は、インターネットに直接接続しないでください。iLO プロセッサーは、運用管理ツールであり、インターネットのゲートウェイではありません。ファイアウォール保護を提供する企業 VPN を使用してインターネットに接続します。

  > **重要:** iLO がインターネットに直接接続されている場合、iLO ユーザーアカウントのパスワードをすぐに変更してください。

- 認証機関（CA）によって署名された SSL 証明書をインストールして、デフォルトの自己署名証明書を置き換えてください。

  SSL 証明書情報ページでこのタスクを実行できます。

- LDAP などの外部サービスの証明書をインストールします。

- デフォルトのユーザーアカウントを含め、ユーザーアカウントのパスワードを変更します。サーバーの管理者パスワードと同じガイドラインに従って iLO 管理パスワードを変更してください。

  このタスクは、**ユーザー管理**ページからも実行できます。

  > **重要:** ユーザーアカウントを作成および更新する場合、iLO ユーザーアカウントの**パスワードに関するガイドライン**に従います。

- すべての権限を持つユーザーアカウントを作成する代わりに、権限の数が少ないアカウントを複数作成します。

- iLO およびサーバーファームウェアを常に最新の状態に保持します。

- できれば Two-Factor 認証の認証サービス（Active Directory や OpenLDAP など）を使用します。この機能により、ネットワーク全体で同じログインプロセスを使用して認証および承認を行うことができます。同時に複数の iLO デバイスを制御する方法を提供します。ディレクトリは、時刻と位置に基づく非常に特殊なロールおよび権限で、iLO へのロールベースのアクセスを提供します。

- Two-Factor 認証を実装します。この機能により、さらにセキュリティが強化されます。特に、リモートで、またはローカルネットワークの外で接続できる場合に有効です。

- SNMP トラフィックを保護します。管理パスワードと同じガイドラインに従ってコミュニティストリングをリセットします。また、特定の送信元と送信先のアドレスのみを受け入れるようにファイアウォールまたはルーターを設定します。必要ない場合は、サーバーで SNMP を無効にします。

- 使用しないポートおよびプロトコル（**SNMP** や **IPMI/DCMI over LAN** など）を無効にします。

アクセス設定ページでこのタスクを実行できます。

- 使用しない機能（リモートコンソールなど）を無効にします。

  アクセス設定ページでこのタスクを実行できます。

- リモートコンソールに HTTPS を使用します。

  このオプションを構成するには、**リモートコンソール&メディア**ページの**セキュリティ**タブで **IRC は iLO 内の信頼された証明書を要求します**を有効にします。

- サーバー OS コンソールを自動的にロックするようにリモートコンソールを構成します。

  このオプションを構成するには、**リモートコンソール&メディア**ページの**セキュリティ**タブにある、**リモートコンソールのコンピューターロック**設定を構成します。

- **暗号化設定**ページで、より高いセキュリティ状態を構成してください。
- UEFI システムユーティリティで iLO 5 構成ユーティリティを無効にするか、ユーザーがアクセスする場合にログイン認証情報を要求するように iLO を構成します。

  アクセス設定ページでこのタスクを実行できます。

- 認証エラーを記録するよう iLO を構成します。

  アクセス設定ページでこのタスクを実行できます。

- ファームウェア検証スキャンを有効にします。

  このタスクは、**ファームウェア検証**ページで実行できます。

- **セキュリティダッシュボード**ページを使用して、セキュリティリスクと推奨事項を監視します。
- **セキュリティログ**を使用して、セキュリティ関連のイベントを監視します。
- **ホスト認証が必要**機能を有効にします。

  アクセス設定ページでこのタスクを実行できます。

- **ダウングレードポリシー**を、**ダウングレードにはリカバリセットの権限が必要です**に設定します 。

  アクセス設定ページでこのタスクを実行できます。

- リカバリセットを最新の状態に保ちます。

詳しくは、**Top 10 security settings for HPE iLO 5** および **Recommended Security Settings in HPE iLO 5** のビデオをご覧ください。

詳しくは

iLO Web インターフェイスによるセキュリティの構成と監視
iLO ネットワーク接続オプション

カスタマーアドバイザリ、報告、および通知の表示

手順

1. **https://www.hpe.com/support/ilo5** にアクセスします。
2. **アラート**アイコンをクリックします。

   アドバイザリ、報告、通知などの iLO 5 に関連するすべてのアラートが表示されます。

3. （オプション）ページの左側にある**評価**ボックスで **Top Resolutions** を選択して、優先度の高い問題に関連するドキュメントのみを表示します。
4. （オプション）**アラート通知の申し込み**をクリックして、iLO 5 に対するアラートがあるときに自動的に通知されるイベントの登録ページを完成させます。

IPMI または DCMI over LAN での iLO の使用のガイドライン

iLO は、IPMI 2.0 および DCMI 業界標準プロトコルをサポートします。IPMI は、Intel が開発した業界標準プロトコルです。それは、Hewlett Packard Enterprise、IBM、Dell、Cisco、NEC、Fujitsu-Siemens、Supermicro などの 200 社を超えるベンダーによってサポートされています。IPMI について詳しくは、Intel の Web サイト **http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-home.html** を参照してください。

Data Center Management Interface（DCMI）は、IPMI で定義されているのと同じインターフェイスを使用しますが、オプションのインターフェイスは少なくなっています。DCMI 1.0 仕様では、データセンターで必要とする必須機能とインターフェイスのコアセットを規定しています。それには、IPMI 2.0 に追加された拡張機能のサブセットが含まれ、データセンターでの DCMI の機能をさらに強化させます。DCMI が IPMI と異なるのは、データセンターの管理ニーズに対応して設計されたという点です。

iLO では、業界標準の IPMI と DCMI のコマンドを LAN 経由で送信することができます。IPMI/DCMI ポートはデフォルトでは 623 に設定されていますが、変更することができます。**IPMI over LAN** オプションが有効になっている場合、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。このオプションを無効にしても、サーバー側の IPMI/DCMI アプリケーションは引き続き機能します。

IPMI/DCMI over LAN を使用する場合は、以下のガイドラインをご覧ください。

- IPMI/DCMI トラフィックをネットワークのそれ以外のトラフィックから分離します。共有 NIC 接続を使用する場合、iLO に VLAN を使用してこの分離を実行できます。ファイアウォールを使用して IPMI/管理サブネットを分離して、アクセスを認可された管理者に制限します。
- ネットワークの外からの IPMI/DCMI トラフィックを許可しません。
- iLO は、IPMI 1.5 よりも強い暗号化を使用している IPMI 2.0 をサポートしています。Hewlett Packard Enterprise では、暗号スイート 17 をお勧めします。

解決された脆弱性

2013 年 7 月、US-CERT はアラート（TA13‐207A）Risks of Using the Intelligent Platform Management Interface（IPMI）を発行しました。このアラートは、Web サイト **https://www.us-cert.gov/ncas/alerts/TA13-207A** で入手できます。

Hewlett Packard Enterprise では、次のようにこの脆弱性に対処しました。

- 暗号 0 は、認証をバイパスできるオプションです。iLO では、IPMI クライアントが暗号 0 を選択できなくすることで、この問題に対処しました。
- IPMI 仕様では、匿名ログインをサポートするためにユーザー ID 1 が使用されます。iLO は、ユーザー ID 1 を使用した匿名ログインをサポートしません。
- IPMI 仕様では、無効化されたユーザー ID は、ユーザー名とパスワードで構成されます。多くの場合、これは製造時に既知のユーザー ID とパスワードにあらかじめ構成されます。iLO は、無効化されたユーザー ID、ユーザー名およびパスワードを保持しません。iLO は、製造時に固有のパスワードであらかじめ構成された 1 つのユーザー名を持ちます。Hewlett Packard Enterprise では、お客様はこのデフォルトユーザーをすぐに再構成することをお勧めします。

- IPMI 仕様では、NULL のパスワードを許可していますが、iLO ではユーザーのパスワードの NULL 設定をサポートしていません。
- IPMI 仕様では、RAKP 認証のサポートが必要であるため、リモートでパスワードハッシュを取得して、オフラインパスワード推測攻撃を実行できます。この要件は IPMI プロトコルに含まれるため、 Hewlett Packard Enterprise では、IPMI over LAN を無効にする（使用していない場合）か、IPMI 管理サブネットを分離することをお勧めします。

iLO Web インターフェイスによるセキュリティの構成と監視

ライセンスキーのインストール

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**管理**をクリックし、**ライセンス**タブをクリックします。
2. **アクティブ化キー**ボックスにライセンスキーを入力します。

   アクティベーションキーボックスで、セグメント間でカーソルを移動するには、**Tab** キーを押す、またはボックスのセグメントの内側をクリックします。 **アクティベーションキー**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。
3. **インストール**をクリックします。

   エンドユーザー使用許諾契約を読み、合意したことを確認するプロンプトが iLO で表示されます。

   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。
4. **同意する**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。

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、サーバーのセットアップ、サーバーヘルスの監視、電力および温度制御の監視、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。

- 製品をインストールして使用するサーバーごとに 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。
- 別のサーバータイプを意味するライセンスキーを使用してサーバーにライセンスを適用することはできません。
- iLO Advanced ライセンスは Synergy コンピュートモジュールに自動的に付属します。
- ライセンスキーを無くした場合、iLO ライセンスガイドに記載されている、なくなったライセンスキーに対する手順に従います。
- 以下について詳しくは、iLO ライセンスガイドを参照してください。
  - 無料 iLO トライアルライセンスの入手
  - ライセンスキーの購入、登録、引き換え

  ライセンスガイドは次の Web サイトで入手できます。**https://www.hpe.com/support/ilo-docs**.

  詳しくは、**Licensing Options** のビデオをご覧ください。

iLO のライセンスキーを登録することの利点

- 登録により、一意の HPE サポート契約 ID（SAID）が有効になります。SAID はユーザーとユーザーが使用する製品を識別します。
- SAID を使用すると、より迅速な HPE サポートサービスが得られます。
- HPE サポートセンターにアクセスできます。
- HPE アップデートセンターでソフトウェアアップデートにアクセスできます。
- 重要な製品アラートを受信します。
- HPE ライセンスポータルを使用して 1 つの場所で HPE 製品ライセンスキーを追跡します。

セキュリティダッシュボードの使用

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

無視オプションを構成するための iLO 設定の構成権限。

手順

1. ナビゲーションツリーで**情報**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。
2. （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。
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。
4. （オプション）**無視**オプションをセキュリティ機能に構成します。

   - **無視**オプションは、デフォルトでは無効になっています。
   - **無視**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。

   セキュリティ機能の**無視**値を変更すると、iLO が**全体セキュリティステータス**を再計算します。

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検出しませんでした。
- **リスク**—iLO が 1 つ以上の監視対象セキュリティ機能に関連した潜在的セキュリティリスクを検出しました。
- **無視**—iLO が 1 つ以上の監視対象セキュリティ機能に関連した潜在的セキュリティリスクを検出しました。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。表示される値は、以下のとおりです。

- **本番稼働**
- **高セキュリティ**
- **FIPS**
- **CNSA**
- **Synergy セキュリティモード**

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。この機能は、管理者にデバイスの置き換えまたは追加、ハードウェアの取り外し、セキュアブートの変更、ファームウェアのインストールのような作業について警告します。この機能を UEFI システムユーティリティで構成したり、iLO RESTful API を使用して構成することができます。

セキュリティダッシュボードページでサーバー構成ロック情報を表示するには、環境が以下の要件を満たしている必要があります。

- インストールされているシステム ROM/BIOS ファームウェアが、サーバー構成ロック機能をサポートしている。

  Intel ベースのサーバーではバージョン 2.00 が必要で、AMD ベースのサーバーではバージョン 1.40 が必要です。
- iLO 5 1.40 以降にアップグレードした後、サーバーを再起動した。
- セキュリティ状態を本番環境から FIPS に変更した後、サーバーを再起動した。
- サーバー構成ロックを含むライセンスがインストールされている。

セキュリティダッシュボード表

- **セキュリティパラメーター**—監視対象のセキュリティ機能の名前。

  iLO Web インターフェイ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 インターフェイスページに移動してください。
- **ステータス**—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。
- **リスク**—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。

- **状態**—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。
  - **有効**—機能は有効です。
  - **無効**—機能は無効です。
  - **不十分**—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。
  - **オフ**—機能は**オフ**に設定されています。
  - **オン**—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。
  - **失敗**—機能は障害を報告しました。
  - **修正済み**—機能は、修正された障害を報告しました。
  - **真**—機能は使用中です。
  - **偽**—機能は使用されていません。
- **無視**—この列に表示されるスイッチを使って、機能を無視するよう設定できます。**無視**設定を有効にすると、監視対象の機能は**全体セキュリティステータス**値に含まれません。

  機能を無視しても、セキュリティダッシュボード表に表示される**ステータス**値は変わりません。

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。

- **説明** - 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。
- **推奨されるアクション** - 推奨される解決策。

  無視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。
- **無視** - **無視**オプションが有効になった日時。
- **以下によって無視** - **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。

アクセスパネルステータス

シャーシの侵入検知コネクターにより、アクセスパネルのステータスが**侵入**になっていることが報告されました。

この機能は、シャーシの侵入検知が構成されているサーバーでのみ使用できます。

Hewlett Packard Enterprise では、IML と iLO イベントログに記録されたイベントを監査し、監視ビデオをチェックしてサーバーへの物理的な侵入活動がないかどうかを確認することをお勧めします。

認証失敗ログ

iLO は、認証の失敗を記録するように構成されていません。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を有効にすることをお勧めします。

デフォルト SSL 証明書が使用中

iLO のデフォルト自己署名証明書が使用中です。

Hewlett Packard Enterprise では、信頼済みの証明書を **SSL 証明書カスタマイズ**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 セキュリティ脆弱性にさらされます。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を無効にすることをお勧めします。

最新のファームウェアスキャン結果

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。

Hewlett Packard Enterprise では、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。

詳しくは、iLO のユーザーガイドを参照してください。

この機能を使用するには、ライセンスをインストールする必要があります。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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

最小パスワード長

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。

Hewlett Packard Enterprise では、**アクセス設定**ページでこの値を 8（デフォルト）以上に設定することをお勧めします。

パスワードの複雑さ

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。

アクセス設定ページでこの機能を有効にできます。

ホスト認証が必要

ホスト認証が必要機能は無効になっており、iLO は高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されています。この機能が無効になっていると、ホストベースの構成ユーティリティを使用して管理プロセッサーにアクセスするときに、iLO 認証情報は必要ありません。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を有効にすることをお勧めします。

iLO RBSU へのログイン要求

iLO は、UEFI システムユーティリティの iLO 構成オプションへのアクセスにログイン認証情報を要求するようには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 構成への未認証のアクセスが許可されます。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を有効にすることをお勧めします。

セキュアブート

UEFI セキュアブートオプションが無効になっています。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。

Hewlett Packard Enterprise では、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。

セキュリティオーバーライドスイッチ

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。

Hewlett Packard Enterprise では、この機能を無効にすることをお勧めします。

詳しくは、iLO のユーザーガイドを参照してください。

セキュリティログ

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. ナビゲーションツリーで**情報**をクリックして、**セキュリティログ**タブをクリックします。
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。

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、**深刻度**リストから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、**クラス**リストから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、**カテゴリ**リストで値を選択します。
- 表示されるイベントの日付と時刻を変更するには、**時刻**メニューで値を選択します。以下から選択します。
  - **デフォルト表示** - UTC 時間を表示します。
  - **ローカル時刻表示** - iLO Web インターフェイスのクライアント時間を表示します。
  - **ISO 時刻表示** - UTC 時間を ISO 8601 形式で表示します。
- **最終更新**日付でフィルタリングするには、**最終更新**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、**フィルターのリセット**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。
- **深刻度** - 検出されたイベントの重要性。
- **クラス** - 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。
- **説明** - この説明によって、記録されたイベントの特性が提供されます。

  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。
- **最終更新** - 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た日時に基づきます。

  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。
- **回数** - 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。
- **カテゴリ** - 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

- **クリティカル** - イベントはサービスの消失（またはサービスの消失が予期されること）を示しています。すぐに対処する必要があります。
- **警告** - イベントは重大ですが、性能の低下を示してはいません。
- **情報** - イベントは背景情報を提供します。

セキュリティログイベントペインの詳細

- **初期更新** - 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た日時に基づきます。

  イベントが最初に発生した日時を iLO が認識しなかった場合は、値が `NOT SET` と表示されます。
- **イベントクラス** - イベントクラスの一意識別子。

  この値は 16 進数形式で表示されます。
- **イベントコード** - イベントクラス内のイベントの一意識別子。

  この値は 16 進数形式で表示されます。
- **推奨されるアクション** - 障害状態に対する推奨されるアクションの簡単な説明。

iLO のバックアップとリストア

自動でのバックアップとリストア

iLO の初期化プロセスが終了すると、バッテリ駆動の SRAM メモリデバイスに保存されている構成情報が不揮発性フラッシュメモリ（NAND）にバックアップされます。

SRAM が消去された、またはデータ破壊が検出された場合、 iLO はバックアップファイルから構成情報をリストアしようとします。自動リストア操作は IML に記録されます。

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すると、SRAM データは自動的にリストアされません。

自動でのバックアップとリストアのプロセスによって作成されたバックアップファイルには、ユーザーはアクセスできません。手動リストア操作を実行するために使用することはできません。

手動でのバックアップとリストア

iLO では、バッテリ駆動の SRAM メモリデバイスに保存された構成情報の手動リストアがサポートされています。この機能は、バックアップされたシステムと同じハードウェア構成を持つシステムで使用するためのものです。構成を複製して別の iLO システムに適用するものではありません。

Hewlett Packard Enterprise では、リストア操作を実行する理由が生じることは想定されていません。ただし、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。Hewlett Packard Enterprise は、iLO ファームウェアをアップデートするたびにバックアップを実行することをお勧めします。

詳しくは、**iLO Management Backup and Restore** のビデオをご覧ください。

バックアップとリストアのための iLO ファームウェア要件

- iLO 5 ファームウェアバージョン 2.10 以降では、iLO ファームウェアのバージョンが同じシステムや異なるシステムでバックアップおよびリストアのタスクが実行される、バックアップおよびリストア操作がサポートされています。
- 2.10 より前の iLO 5 ファームウェアバージョンでは、iLO ファームウェアのバージョンが同じシステムでバックアップおよびリストアのタスクが実行される、バックアップおよびリストア操作がサポートされています。

バックアップとリストアの操作中にリストアされる情報

iLO 構成には、電源、ネットワーク、セキュリティ、ライセンスキー、ユーザーデータベースなど、多くのカテゴリが含まれます。ほとんどの構成情報は、バッテリ駆動の 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。

注記: 環境変数をリストアしたときは、リストアした設定を有効にするためにサーバーのリセットが必要です。

たとえば、**パフォーマンス**設定はリストアされてもサーバーリセットが完了するまで有効になりません。

バックアップとリストアの操作中にリストアされない情報

一部の情報は、バックアップとリストアの操作中にリストアするのに適していません。リストアできない情報は iLO 構成には含まれません。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。

セキュリティログ

バックアップから、リストアが必要になったイベントまでに発生したセキュリティ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 構成を手動でリストアする理由

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。

バッテリの障害または取り外し

さまざまな構成パラメーターがバッテリ駆動の SRAM に保存されています。まれですが、バッテリ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、バッテリの交換後にバックアップファイルから iLO 構成をリストアします。

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 以外の設定を消去することが必要になることがあります。iLO を工場出荷時の設定にリセットすると、iLO の構成は消去されます。iLO 構成をすばやく復旧するには、工場出荷時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。

構成の偶発的または不適切な変更

場合によって、iLO 構成が不適切に変更され、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。

システムボードの交換

ハードウェアの問題に対処するためにシステムボードの交換が必要な場合、この機能を使用して iLO 構成を元のシステムボードから新しいシステム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。

iLO 構成のバックアップ

前提条件

- iLO の設定を構成する権限
- iLO は、本番環境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されています。iLO が高い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、構成のバックアップとリストアはサポートされていません。

手順

1. ナビゲーションツリーで**管理**をクリックし、**バックアップとリストア**をクリックします。
2. **バックアップ**をクリックします。
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、**バックアップファイルパスワード**ボックスにパスワードを入力します。

   パスワードは最大 32 文字です。
4. **ダウンロード**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 の設定を構成する権限
- ユーザーアカウント管理権限
- 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。

  本番環境または高セキュリティよりも高い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。これらのセキュリティ状態を構成せずにリストアを実行した場合、リストアされた情報はセキュリティ状態の更新時に削除されます。

手順

1. ナビゲーションツリーで**管理**をクリックし、**バックアップとリストア**をクリックします。
2. **リストア**をクリックします。
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. **アップロードおよびリストア**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. **リストア**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。

システムボード交換後の iLO 構成のリストア

システムボードを交換する場合、交換前のシステムボードから構成をリストアできます。

前提条件

- iLO の設定を構成する権限
- ユーザーアカウント管理権限
- 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。

  本番環境または高セキュリティよりも高い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。これらのセキュリティ状態を構成せずにリストアを実行した場合、リストアされた情報はセキュリティ状態の更新時に削除されます。

手順

1. システムボードを交換し、ハードウェアコンポーネントを古いシステムボードから新しいシステムボードに転送します。
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. 新しいシステム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。**

iLO ユーザーアカウント

iLO では、セキュア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を管理できます。

ユーザー指定のログイン名と高度なパスワード暗号化を使用してローカル ユーザー アカウントを最大 12 個作成することができます。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。

iLO と連携し、サポートされるアプリケーションにサービスアカウントが必要な場合は、ユーザーアカウントを追加して、このアカウントをサービスアカウントとして指定できます。また、サポートされるアプリケーションまたは iLO RESTful API を使用して、サービスアカウントを追加することもできます。

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てユーザーの認証や権限付与を行うよう iLO を構成します。

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. ナビゲーションツリーで**管理**をクリックします。

   ユーザー管理タブが表示されます。
2. **新規**をクリックします。
3. 次の詳細を入力します。

   - **ログイン名**
   - **ユーザー名**
   - **パスワード**と**パスワードの確認**
4. 次の権限のいずれかを選択します。

   - **ログイン**
   - **リモートコンソール**
   - **仮想電源およびリセット**
   - **仮想メディア**
   - **ホスト BIOS**

- **iLO 設定の構成**
- **ユーザーアカウント管理**
- **ホスト NIC 構成**
- **ホストストレージ構成**
- **リカバリセット**

使用できるすべてのユーザーの権限を選択するには、**すべてを選択**チェックボックスをクリックします。

5. （オプション）アカウントをサポートされているアプリケーションのサービスアカウントとして使用する場合は、**サービスアカウント**チェックボックスを選択します。

   サポートされているアプリケーションには、iLO Amplifier Pack や Onboard Administrator があります。

   サービスアカウントのプロパティは、最初のユーザーアカウントの作成時にのみ構成できます。既存のユーザーアカウントでこの設定を編集することはできません。

6. 新しいユーザーを保存するには、**ユーザーの追加**をクリックします。

   iLO はアカウントが追加されたことを通知します。

ローカルユーザーアカウントの編集

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーで**管理**をクリックします。

   ユーザー管理タブが表示されます。

2. ユーザーを選択し、**編集**をクリックします。
3. 必要に応じて、以下の値を**ローカルユーザーの追加/編集**ページに入力します。
   - **ログイン名**
   - **ユーザー名**
4. パスワードを変更するには、**パスワードを変更**チェックボックスをクリックし、**パスワード**と**パスワードの確認**の値を更新します。
5. 次の権限のいずれかを選択します。
   - **ログイン**
   - **リモートコンソール**
   - **仮想電源およびリセット**
   - **仮想メディア**
   - **ホスト BIOS 構成**
   - **iLO の構成**

- **ユーザーアカウント管理**
- **ホスト NIC 構成**
- **ホストストレージ構成**
- **リカバリセット**

6. 使用できるすべてのユーザーの権限を選択するには、**すべてを選択**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、**ユーザーのアップデート**をクリックします。

   iLO は、選択したアカウントが更新されたことを通知します。

iLO ユーザーアカウントオプション

- **ユーザー名**は、**ユーザー管理**ページのユーザーリストに表示されます。**ログイン名**と同じである必要はありません。ユーザー名の最大長は 39 文字です。**ユーザー名**には、印字可能な文字を使用する必要があります。わかりやすいユーザー名を割り当てると、各ログイン名の所有者を識別でき便利です。
- **ログイン名**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、**ユーザー管理**ページのユーザーリスト、**セッションリスト**ページ、ユーザーアイコンをクリックしたときに表示されるメニュー、およびログに表示されます。**ログイン名**は、**ユーザー名**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、印字可能な文字を使用する必要があります。
- **パスワード**および**パスワードの確認**では、iLO にログインするために使用するパスワードを設定および確認します。
- **サービスアカウント**は、アカウントをサービスアカウントとして指定します。サービスアカウントは、iLO で動作するサポート製品で使用されます。

  サポートされているアプリケーションには、iLO Amplifier Pack や Onboard Administrator があります。

  サービスアカウントのプロパティは、最初のユーザーアカウントの作成時にのみ構成できます。既存のユーザーアカウントでこの設定を編集することはできません。

iLO ユーザーアカウントの権限

次の権限は、ユーザーアカウントに適用されます。

- **ログイン** - iLO にログインできます。
- **リモートコンソール** - ビデオ、キーボード、マウスの制御を含めホストシステムのリモートコンソールにアクセスできます。

  この権限を持つユーザーは BIOS にアクセスできるため、ホストベースの BIOS、iLO、ストレージ、およびネットワークタスクを実行できる場合があります。
- **仮想電源およびリセット** - 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、**システムに NMI を生成**ボタンを使用してシステムを診断できます。
- **仮想メディア** - ホストシステム上の仮想メディア機能を使用できます。
- **ホスト BIOS** - UEFI 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。この権限は、アクティブなシステム ROM を冗長システム ROM で置き換えるために必要です。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- **iLO 設定の構成** - セキュリティ設定を含むほとんどの iLO 設定を構成し、iLO ファームウェアをアップデートすることができます。この権限は、ローカルユーザーアカウント管理を有効にしません。

iLO を構成したら、すべてのユーザーからこの権限を取り消して、 Web インターフェイス、iLO RESTful API、HPQLOCFG、または CLI による再構成を防止します。UEFI システムユーティリティまたは HPONCFG にアクセスできるユーザーは、引き続き 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できます。

- **ユーザーアカウント管理** - ユーザーは、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。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。この権限が割り当てられていないと、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。
- **ホスト NIC 構成** - ホスト NIC 設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- **ホストストレージ構成** - ホストストレージ設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- **リカバリセット** - ユーザーがシステムリカバリセットを管理できるようにします。

  デフォルトでは、この権限はデフォルトの管理者アカウントに割り当てられます。この権限を別のアカウントに割り当てるには、すでにこの権限を持つアカウントでログインします。

  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されている場合、この権限を使用できません。

次の権限は、CLI または RIBCL スクリプトを介して使用できません。ホスト NIC 構成、ホストストレージ、リカバリセット、ホスト BIOS 構成、およびログイン。

次の権限は、UEFI システムユーティリティの iLO 5 構成ユーティリティから使用できません。ログイン、およびリカバリセット。

パスワードに関するガイドライン

Hewlett Packard Enterprise では、ユーザーアカウントを作成および更新する場合に、以下のパスワードに関するガイドラインに従うことをお勧めします。

- パスワードを使用する場合：
  - パスワードをメモまたは記録しないでください。
  - パスワードの共有は避けてください。
  - 辞書に載っている言葉を組み合わせたパスワードを使用しないでください。
  - 推測しやすい単語を含むパスワードを使用しないでください。たとえば、会社名、製品名、ユーザー名、ログイン名などです。
  - パスワードを定期的に変更します。
  - iLO デフォルト認証情報を安全な場所に保管します。
- 強化パスワードには、少なくとも以下の 3 つの特性が必要です。
  - 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）。

  アクセス設定ページの**パスワードの複雑さ**設定を有効にした場合、ユーザーアカウントを作成または編集するときに iLO によってこれらのパスワード特性が強制されます。
- 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**ページで設定します。構成された**最小パスワード長**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。Hewlett Packard Enterprise では、8 文字以上の**最小パスワード長**を使用することをお勧めします。デフォルト値は 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、**最小パスワード長**を 8 文字未満に設定しないでください。

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。

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**上記の設定に基づく IPMI/DCMI 権限**ボックスに表示されます。

- **ユーザー** - 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。
- **オペレーター** - 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、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。
- **管理者** - 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。

詳しくは

IPMI または DCMI over LAN での iLO の使用のガイドライン

iLO アクセス設定

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 機能を無効にするには、**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 の設定を構成する権限
- **アップデートサービス**設定の変更に関する前提条件：

- iLO の設定を構成する権限
- 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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

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. アップデートしたいアクセス設定カテゴリの隣にある✎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**

   ★**編集*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を必要であることを通知します。

     設定によっては、リセットが完了する前に、設定の変更時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無効にした場合、**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。

     リセットが必要なその他の設定では、リセットを行わずに手動で構成を元の状態に戻すことができます。これらの設定の場合は、手動で変更を元に戻して、✕をクリックして、リセットメッセージを無視します。たとえば、仮想 NIC 機能を有効にした場合、保留中の変更にリセットが必要であることが、iLO から通知されます。仮想 NIC オプションを無効にリセットして手動でこの変更を元に戻すと、保留中のリセットメッセージは残され、✕をクリックして、メッセージを無視できます。

     画面またはダイアログボックスで✕をクリックすると、リセットメッセージは破棄されますが、iLO 構成が前の設定に戻されることはありません。変更を元に戻す場合は、手動で変更を元に戻す必要があります。

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、**iLO をリセット**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. **はい、iLO をリセットします**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。

詳しくは

アクセス設定クイックリファレンス
iLO の機能によって使用されるポート
iLO 5 の推奨されるセキュリティ設定

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。

- この設定が有効（デフォルト）になっている場合、iLO ネットワークを使用でき、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。
- この設定が無効になっている場合、iLO ネットワークと、オペレーティングシステムドライバーとの通信が切断されます。

  iLO 機能は、ProLiant サーバーブレードまたは Synergy コンピュートモジュールでは無効にできません。

この手順を使用して、iLO 機能の設定を変更します。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 の設定を構成する権限

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。

   アクセス設定ページが表示されます。
2. （**iLO** セクションの横）をクリックします。

   iLO 設定の編集ページが表示されます。
3. **アドバンスト設定を表示**をクリックします。
4. **iLO 機能**セクションで**無効**をクリックします。

   iLO が要求を確認するように求めます。
5. **iLO の機能の無効の確認**チェックボックスを選択します。
6. **はい、iLO の機能を無効にします**をクリックします。

   注意: このボタンをクリックした場合、iLO にはどのインターフェイスからもアクセスできなくなります。iLO の機能をリストアするには、UEFI システムユーティリティを使用できます。

   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 インターフェイスからも接続できません。
7. （オプション）**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またはシステムメンテナンススイッチを使用します。

   Hewlett Packard Enterprise では、UEFI システムユーティリティを使用してこの作業を実行することをお勧めします。

iLO 機能を有効にする方法

iLO 機能が無効になっている場合、iLO Web インターフェイスから機能を再度有効にすることはできません。UEFI システムユーティリティまたはシステムメンテナンススイッチを使用して、**iLO 機能**を再度有効にすることができます。

UEFI システムユーティリティ

Hewlett Packard Enterprise では、UEFI システムユーティリティを使用して **iLO 機能**を再度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ドキュメントを参照してください。

システムメンテナンススイッチ

iLO 機能をリストアする別の方法は、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するというものです。

iLO セキュリティを無効にすると、iLO のネットワーク構成が工場出荷時のデフォルト設定にリセットされます。工場出荷時のデフォルトネットワークインターフェイスがネットワークに接続されている場合、iLO はネットワーク上で利用可能です。この変更は iLO セキュリティをリストアした後も持続します。

△ **注意:** セキュリティを無効にし、iLO が本番環境のセキュリティ状態を使用している場合、どのユーザーも iLO にアクセスして構成を変更することができます。システムメンテナンススイッチを使用してセキュリティを無効にする場合、Hewlett Packard Enterprise では、この構成で iLO を使用する時間をできるだけ短くすることを強くお勧めします。

サーバーアクセス設定オプション

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。

サーバー名

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。

サーバーの FQDN/IP アドレス

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。

遅延前の認証の失敗時

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。

有効な値は次のとおりです。

- **毎回の失敗時でも遅延なし**—ログイン試行の最初の失敗後、ログイン遅延が発生します。
- **1 回目の失敗時では遅延なし**（デフォルト）—ログイン試行に 2 回失敗するまで、ログイン遅延は発生しません。
- **3 回目の失敗時では遅延なし**—ログイン試行に 4 回失敗するまで、ログイン遅延は発生しません。
- **5 回目の失敗時では遅延なし**—ログイン試行に 6 回失敗するまで、ログイン遅延は発生しません。

認証の失敗時の遅延時間

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。

認証失敗ログ

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。

- **有効-毎回失敗時**— 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。
- **有効-2 回の失敗ごと**— 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。
- **有効-3 回の失敗ごと**（デフォルト） — 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。
- **有効-5 回の失敗ごと**— 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。
- **無効**— ログインの失敗のログエントリーは記録されません。

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無効になります。

パスワードの複雑さ

ユーザーアカウントおよび iLO 連携グループ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）

この設定を無効（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。

ネットワークアクセス設定オプション

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無効にしたり、それらの機能で使用するポートを構成したりできます。

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、**XML を表示**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**劣化**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。

このオプションが無効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`。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

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。

この設定が無効になっていると、iLO は LAN 経由で IPMI/DCMI を無効にします。この機能が無効にされても、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。

この設定が有効になっている場合、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 が無効にされている場合、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。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

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 UDP 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有効または無効にすることができます。

このオプションを無効にすると、グラフィカルリモートコンソールと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。

リモートコンソールを無効にしても、リモートコンソールサムネイルは無効になりません。リモートコンソールサムネイルを無効にするには、**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 TCP 17990 です。

セキュアシェル（SSH）

SSH 機能を有効または無効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 TCP 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。

SNMP アクセスを無効にすると、iLO はそのまま動作を続行し、iLO Web インターフェイ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 アクセスが無効になっている場合、**SNMP 設定**ページのほとんどのボックスは使用できません。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

SNMP ポート

SNMP ポートを設定します。SNMP アクセスのデフォルト値は UDP 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 オプションが無効になっている場合、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）のデフォルト値は UDP 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。

HPE SIM 7.2 以降で SNMP v3 を使用するには、**SNMP トラップポート**の値を 50005 に変更します。

SNMP オプションが無効になっている場合、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有効または無効にすることができます。

このオプションを無効にすると、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、設定されている仮想メディアポートが検出されません。

仮想メディアポート

iLO が着信ローカル仮想メディア接続をリスンするために使用するポート。デフォルト値は TCP 17988 です。

仮想シリアルポートログ

仮想シリアルポートの記録を有効または無効にします。

この設定が有効になっている場合、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。

この設定が無効（デフォルト）になっている場合、仮想シリアルポートの動作は記録されません。

Web サーバー

iLO Web サーバー経由のアクセスを有効または無効にすることができます。

△ **注意:** この値を無効に設定した場合、iLO は、構成済みの **Web サーバー非 SSL ポート（HTTP）**または **Web サーバー SSL ポート（HTTPS）**での通信をリスンしません。

Web サーバーが無効になっている場合、次の機能は正常に動作しません。

- iLO の Web インターフェイス
- リモートコンソール
- iLO RESTful API
- RIBCL

このオプションを無効にすると、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。

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 TCP 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 TCP 443 です。

SSH クライアントによる iLO ログイン

SSH クライアントで iLO にログインすると、表示されるログインプロンプトの回数は、**認証失敗ログ**オプションの値（無効の場合は 3）に一致します。SSH クライアントはログインが失敗すると実装も遅延するため、SSH クライアント設定は、プロンプトの回数に影響を与える場合があります。

たとえば、デフォルト値（**有効-3 回目の失敗時**）で SSH 認証失敗ログを生成するには、SSH クライアントが、3 回に設定されたパスワードプロンプトで構成されている場合、連続した 3 回のログイン失敗が次のように発生します。

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 アクセス設定オプション

アクセス設定ページの **iLO** セクションでは、以下の設定を構成できます。

アイドル接続タイムアウト（分）

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 インターフェイスおよび.NET IRC および Java IRC は、アイドル時間を別々に追跡します。アイドル接続タイムアウトに達すると、アイドル状態のセッションのみが終了します。

iLO Web インターフェイスと HTML5 コンソールは、1 つの iLO セッションを共有します。アイドル接続タイムアウトに達すると、共有セッションは終了します。

有効な値は次のとおりです。

- **15**、**30**、**60**、**120** 分間 — デフォルト値は 30 分です。
- **無限** - 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。

iLO 機能

この設定については、**iLO 機能の無効化**を参照してください。

iLO RIBCL インターフェイス

iLO と通信するために RIBCL インターフェイ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。

この機能を無効にすると、HTTP/HTTPS を介した RIBCL、インバンド通信経由の RIBCL、および OA ポート経由の RIBCL は機能しません。

HPEOneView から Insight Remote Support Central Connect またはリモートサポートにサーバーを登録する場合、このオプションを有効にする必要があります。

無効の場合、RIBCL を使用しようとすると次のメッセージが表示されます。

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">

<RESPONSE
STATUS="0x00FC"
MESSAGE='RIBCL is disabled.'
/>
</RIBCL>
```

この値を変更するときは、iLO をリセットする必要があります。

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 構成オプションを有効または無効にします。

- この設定が有効（デフォルト）になっている場合、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。
- この設定が無効になっている場合、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 のプロンプトが無効になっている場合、この設定を有効にできません。

iLO Web インターフェイス

iLO と通信するために iLO Web インターフェイ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きは、iLO をリセットする必要があります。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 インターフェイ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表示を有効または無効にします。

サムネイルを無効にしても、リモートコンソール機能は無効になりません。

この設定を無効にすると、Web インターフェイ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

管理プロセッサーにアクセスするホストベースの構成ユーティリティを使用するために、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、管理者または root のホストコンテキストで、ホスト OS のコマンドラインから実行します。

- この設定を有効にすると、すべてのコマンドで有効な資格情報が必要になります。
- この設定を無効にした場合は、有効な認証情報は必要でなく、管理者権限でコマンドは実行します。

  iLO が本番環境または高セキュリティより高い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、この設定は無効にできません。

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、ユーザー認証情報が必要かどうかを決定します。

- この設定が無効（デフォルト）になっている場合、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、ログインは不要です。

  この設定が無効になっている場合でも、iLO のセキュリティ状態が本番環境または高セキュリティよりも高い場合、UEFI システムユーティリティの iLO 構成オプションにアクセスするには、ユーザー資格情報が必要です。
- この設定が有効になっている場合、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。

シリアルコマンドラインインターフェイス速度

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）

  Synergy コンピュートモジュールの場合のみ : Synergy コンソールおよび Composer CLI で、この値を 9600 に設定する必要があります。

- **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イスステータス

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。

- **有効-認証が必要**（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 ユーザー証明書が必要です。
- **有効-認証は不要** - 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。
- **無効** - 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。

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。

- この設定が有効（デフォルト）になっている場合、POST 実行中に iLO の IP アドレスが表示されます。
- この設定が無効になっている場合、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。

- この設定が有効になっている場合は、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。
- この設定が無効になっている場合は、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 秒以上押し続けると、適切な iLO の再起動またはハードウェア iLO の再起動を開始します。ハードウェア iLO の再起動中にデータの損失や NVRAM の破損が発生する可能性があります。

この機能は、Synergy コンピュートモジュールではサポートされません。

サーバーヘルスサマリー画面について詳しくは、HPE iLO 5 トラブルシューティングガイドを参照してください。

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。

- この設定が有効になっている場合（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。
- この設定が無効になっている場合、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。

この設定は、Synergy コンピュートモジュールではサポートされません。

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。

- この設定が有効になっている（デフォルト）場合は、次のことができます。
  - ホスト OS で動作している RESTful インターフェイスツールまたは別のクライアントから iLO RESTful 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 インターフェイスにアクセスする。
  - **概要**ページで仮想 NIC の IP アドレスを表示する。
- この設定が無効になっている場合、仮想 NIC を使用して iLO にアクセスすることはできません。

サービスアクセス設定オプションの更新

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。

この機能にはライセンスが必要です。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ない場合、このオプションは表示されません。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、次の web サイトにあるライセンス文書を参照してください。**https://www.hpe.com/support/ilo-docs**

以下の値から選択します。

- **ダウングレードの許可**（デフォルト）-iLO 設定の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。
- **ダウングレードにはリカバリセットの権限が必要です**-iLO 設定の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。
- **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:** この設定を構成すると 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 iLO を構成した後は、iLO のどのインターフェイ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。

SSH キーの管理

Web インターフェイスを使用した新しい SSH キーの認証

前提条件

ユーザーアカウント管理権限

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 キーまたは RSA キーを生成します。

   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、NIST P-384 曲線を使用する ECDSA 384 ビットキーが必要です。

2. `key.pub` という名前で公開キーを保存します。
3. `key.pub` ファイルの内容をコピーします。
4. ナビゲーションツリーで**セキュリティ**をクリックして、**セキュアシェルキー**タブをクリックします。
5. SSH キーを追加するユーザーアカウントの左にあるチェックボックスを選択します。

   各ユーザーアカウントに割り当てられるキーは 1 つだけです。

6. **新しいキーの認証**をクリックします。
7. **公開キー**ボックスに公開キーを貼り付けます。
8. **公開キーのインポート**をクリックします。

   認証済み SSH キーテーブルが更新され、ユーザーアカウントに関連付けられた SSH 公開キーのハッシュが表示されます。

CLI を使用した新しい SSH キーの認証

前提条件

ユーザーアカウント管理権限

手順

1. `ssh-keygen`、`puttygen.exe`、または別の SSH キーユーティリティを使用して、2,048-bit DSA または RSA SSH キーを生成します。

   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、NIST P-384 曲線を使用する ECDSA 384 ビットキーが必要です。

2. `key.pub` ファイルを生成します。
3. **アクセス設定**ページで**セキュアシェル（SSH）アクセス**が有効になっていることを確認します。
4. `putty.exe` を使用して、ポート 22 を使用した SSH セッションを開きます。

5. `/Map1/Config1` ディレクトリに変更します。
6. 次のコマンドを入力します。

   ```
   load sshkey type "oemhpe_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 を指定します。
   - `hostname` および `filename` の値は必須です。
   - `username:password` および `port` の値は省略可能です。

   CLI では、入力した値の構文は大まかにしか検証されません。よく見て、URL が正しいことを確認してください。次の例でコマンド構造を示します。

   ```
   oemhpe_loadSSHkey -source http://192.168.1.1/images/path/sshkey.pub
   ```

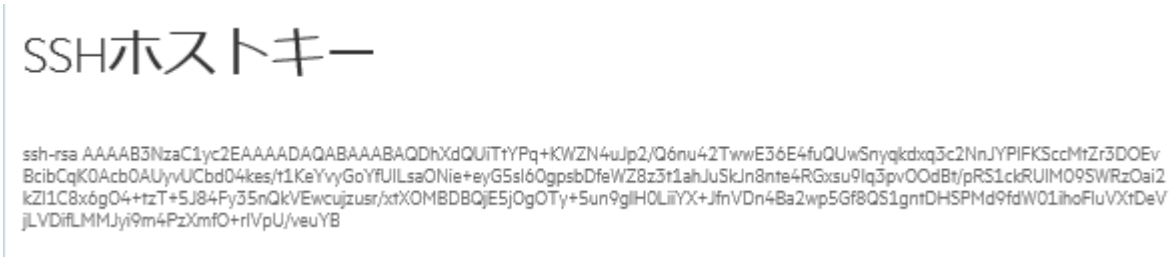
SSH ホストキーの表示

iLO によって報告される SSH ホストキーを表示するには、以下の手順に従ってください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックして、**セキュアシェルキー**タブをクリックします。

   SSH ホストキーが表示されます。

2. （オプション）ホスト名/IP アドレスと SSH ホストキーを SSH クライアント構成ファイルに追加します。

   以下に例を示します。

   - Linux の OpenSSH ユーザー：`.ssh/known_hosts` ファイルを更新します。
   - Windows の PuTTY ユーザー：Windows レジストリ（`HKEY_CURRENT_USER\SoftWare\SimonTatham\PuTTY\SshHostKeys`）を更新します。

3. （オプション）接続が安全であることを確認するには、**SSH ホストキー**の値を SSH クライアントから報告された値と比較します。

   以下に例を示します。

   ```
   Linux-client:~ # grep ilo.example.com .ssh/known_hosts
   ilo.example.com,[redacted] ssh-rsa
   AAAAB3NzaC1yc2EAAAADAQABAAABAQC9E/XDH9xPU+NdMyTu5Oylw9AN6mJlH7woMqcf79lda6DeS1D+vX1I
   Wg3GwDKFUobabQ+g2tkBrxWFzwAf51CPitsybQCK2hvLztsypb/W3p+MPZ9zU6/voCHzL2v0bAxeXuX8ack/8RA
   w0l1agB5xY6B3pjP/qaeFJb29sGqPwoaXps6g5t/YFhxIQ8is8N+LnfuTzMtQDj74rfq6pcXGnXq+ErmbkcfHn
   AdSMveT6rXPM1U+Je1B9VOVS23fUL7mfoshLnSHrJJtP7XkZ1rKf1QPKCChWLfpdmTprsaJrxDrwCNxX4+pPh
   UXqHYLTlvPA8xsqaPxPZfHxZWTZrCp
   ```

4. キーが一致しない場合は、一致しない理由を確認してから続行してください。

考えられる理由のいくつかを以下に示します。

- 手順 **1** で表示した iLO システムが、SSH クライアントで接続したシステムと同じではない。
- SSH 接続はリダイレクトされている。ネットワークが接続をリダイレクトするよう構成されているか管理者に尋ねてください。ネットワークが接続をリダイレクトするように構成されていない場合、ネットワークセキュリティが低下する可能性があります。
- iLO が出荷時のデフォルト設定にリセットされたために、アクセスしようとしているシステムの iLO SSH ホストキーが変更された。あなたは自分の SSH クライアント構成を変更していません。

SSH キー

SSH キーを iLO に追加すると、iLO ファームウェアによってキーがローカルユーザーアカウントに関連付けられます。

サポートされている SSH キーフォーマット

- RFC 4716
- OpenSSH キー形式
- レガシー iLO 形式

SSH キーの操作

- iLO Web インターフェイスおよび CLI では、サポートされている SSH キー形式がサポートされます。
- RIBCL スクリプトでは、レガシー iLO 形式のみが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、最大 1,366 バイトの長さの SSH キーをインポートすることができます。キーの長さが 1,366 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 インターフェイ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。
- iLO RESTful API を使用してパブリックキーを入力する場合は、パブリックキーとともにユーザー名が POST 本文で提供されます。
- 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。
- HPQLOCFG および RIBCL スクリプトを使用してパブリックキーを入力する場合は、パブリックキーデータに iLO ユーザー名を追加します。パブリックキーは、ユーザー名とともに格納されます。
- 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。

サポートされている SSH キー形式の例

RFC 4716

```
---- BEGIN SSH2 PUBLIC KEY ---- CRLF
Comment: "Administrator"CRLF
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuAlNLIivLFP3IoKZCRLF
ZtzF0VInP5x2VFVYmTvdVjSupD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCTCRLF
3wI3ldxQvPYnhTYyhPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgts8CRLF
/UAAAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAgCbnhADYXu+Mv4xuXccXWP0PcCRLF
j477YiZgos3jt/Z0ezFX6/cN/RwwZwPC1HCsMuwsVBIqi7bvn1XczFPKOt06gVWcCRLF
jFteBY3/bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHCRLF
g8ZJazhY920PpkD4hNbAAAAgDN3lba1qFVl0UlRjj21MjXgr6em9TETSOO5b7SQ8CRLF
hX/Z/axobbrHCj/2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYCRLF
aiFDLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtCRLF
STV CRLF
---- END SSH2 PUBLIC KEY ---- CRLF
```

OpenSSH キー形式

```
ssh-dss
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDIlI+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avN
Sz0DNQuU7gTPfjj/8cXyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/kDMC0d
VOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI3J61F+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5Qx
qkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpAlxAp6eDZKFvj3ZIyNjcQODeYYqOvVU45AkSkLBMGjpF
05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxDOvNWAAAAg
Ff6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80SfWSnWM3n/pekB
a9QI91H1r3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/K8YnFNwwYy2NSJyjLw
A0TSmQEOW Administrator CRLF
```

レガシー iLO 形式

iLO レガシー形式のキーは、RIBCL で必要な BEGIN および END ヘッダーで囲まれた OpenSSH キーです。

この形式は、BEGIN SSH KEY のテキストと END SSH KEY のテキストの間に 1 行で記す必要があります。

```
-----BEGIN SSH KEY----- CRLF
ssh-dss
AAAAB3NzaC1kc3MAAACBANA45qXo9cM1asav6ApuCREt1UvP7qcMbw+sTDrx91V22XvonwijdFiOM/0Vv
uzVhM9oKdGMC7sCGQrFV3zWDMJcIb5ZdYQSDt44X6bvlsQcAR0wNGBN9zHL6YsbXvNAsXN7uBM7jXwHwr
ApWVuGAI0QnwUYvN/dsE8fbEYtGZCRAAAAFQDofA47q8pIRdr6epnJXSNrwJRvaQAAAIBY7MKa2uH82I0
KKYTbNMi0o5mOqmqy+tg5s9GC+HvvYy/S7agpIdfJzqkpHF5EPhm0jKzzVxmsanO+pjju7lrE3xUxojev
lokTERSCMxLa+OVVbNcgTe0xpvc/cF6ZvsHs0UWz6gXIMCQ9Pk118VMOw/tyLp42YXOaLZzGfi5pKAAAA
IEAl7FsO7sDbPj02a5jO3qFXa762lWvu5iPRZ9cEt5WJEYwMO/ICaJVDWVOpqF9spoNb53W11pUARJg1s
s8Ruy7YBv8Z1urWWAF3fYy7R/SlQqrsRYDPLM5eBkkLO28B8C6++HjLuc+hBvj90tsqeNVhpCfO9qrjYo
mYwnDC4m1IT4= ASmith CRLF
-----END SSH KEY-----CRLF
```

CAC Smartcard 認証

Common Access Card（CAC）とは、米国防総省（DoD）の多要素認証スマートカードです。Common Access Card は、現役軍人、予備員、軍属、DoD 外政府職員、州兵、指定業者社員の標準 ID として発行されます。ID カードとして使用されるだけでなく、共通アクセスカードは官庁施設やコンピューターネットワークへアクセスする際に必要です。

各 CAC に埋め込まれているスマートカード証明書は、iLO Web インターフェイスでローカルユーザーアカウントと関連付けられなければなりません。**証明書マップ**ページのコントロールを使用して、スマートカード証明書をアップロードし、アカウントと関連付けます。

LDAP ディレクトリサポートを備えた CAC 認証ではディレクトリサービスに対して認証するサービスアカウントを使用し、ユーザーアカウントは設定されたディレクトリサーバーと同じドメイン内に存在する必要があります。さらに、ユーザーアカウントは、設定されたグループまたは拡張スキーマロールの直接メンバーでなければなりません。クロスドメイン認証とネスト化グループはサポートされません。

ツーファクター認証

連邦政府認証を満たすために必要な要件の一部がツーファクター認証です。ツーファクター認証は、CAC の二重認証です。たとえば CAC では、実際にカードを所有していてそのカードに関連付けられた PIN 番号を知っていなければならないことで、ツーファクター認証が成立します。CAC 認証に対応するためには、スマートカードが PIN を必要とするように構成されていなければなりません。

CAC Smartcard 認証設定の構成

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。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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- （オプション）LDAP サーバー CA 証明書がディレクトリ統合のためにインストールされている。
- （オプション）LDAP ディレクトリ統合がディレクトリデフォルトスキーマモードで構成されている。

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、**CAC Smartcard 認証**タブをクリックします。
2. **信頼済み CA 証明書をインストールします**。

   この証明書は、iLO に提示される証明書の検証に使用します。証明書は設定されている iLO セキュリティ状態に準拠していなければなりません。
3. 以下の**認証オプション**を設定します。

   a. **CAC Smartcard 認証**を有効にします。

   b.（オプション）**CAC 厳密モード**を有効にします。
4.（オプション）**CAC 厳密モード**の有効時にセキュリティを強化するために、Hewlett Packard Enterprise では、次の機能の 1 つ以上を有効にすることをお勧めします。

   - **ホスト認証が必要** - この設定は**アクセス設定**ページで構成できます。
   - **FIPS** セキュリティ状態 - この設定は**暗号化**ページで構成できます。
5.（オプション）ディレクトリ統合を使用している場合は、**ディレクトリユーザー証明書名マッピング**セクションでオプションを選択します。

   この設定は、ユーザー証明書のどの部分がディレクトリユーザーアカウントの識別に使用されるかを特定します。
6. **認証オプション**および**ディレクトリユーザー証明書名マッピング**設定を保存するには、**適用**ボタンをクリックします。
7.（オプション）証明書失効リスト（CRL）をインポートするには、**失効リストの URL** ボックスに URL を入力して、**適用**をクリックします。

   この手順により、以前に発行されて、失効した証明書を無効にできます。

   CRL のサイズ制限は 100 KB であり、CRL は DER フォーマットでなければなりません。

8. （オプション）オンライン証明書ステータスプロトコルを使用してユーザー証明書を確認するには、HTTP または HTTPS URL を入力して、**適用**をクリックします。
9. **スマートカード証明書をアップロードして**ローカル iLO ユーザーアカウントにマップします（iLO をローカルユーザー認証で使用する場合のみ）。

CAC スマートカード認証設定

CAC スマートカード認証

共通アクセススマートカードを使用した認証を有効または無効にします。

CAC 厳密モード

iLO への接続ごとにクライアント証明書を要求する CAC 厳密モードを有効または無効にします。このモードが有効になっている場合、iLO はユーザー名やパスワードを受け付けず、キーベースの認証方法のみが許可されます。

注記: 信頼済みの証明書がない場合、iLO にアクセスできません。iLO Web インターフェイスにアクセスしようとすると、エラーが生成されます。

ディレクトリユーザー証明書名マッピング

ディレクトリユーザー名の場合を設定すると、ユーザー証明書の部分を選択して、ご自分のディレクトリのユーザー名として使用できます。

- **証明書 SAN UPN を使用** - サブジェクト代替名（SAN）の、userPrincipalName（UPN）タイプの最初のフィールドをユーザー名として使用します。これには、ユーザー名とドメイン名がメールアドレス形式で含まれています。たとえば、`upn:testuser@domain.com` の場合、`testuser@domain.com` となります。
- **証明書件名 CN を使用** - サブジェクトの CN または CommonName の部分だけをユーザー名として使用します。たとえば、`cn = test user, ou = users, dc = domain, dc = com` という DN では、共通名は `test user` です。
- **完全な証明書の Subject DN を使用** - ディレクトリサービスでユーザーを検索するとき、完全な識別名をユーザー名として使用します。たとえば、識別名は `cn = test user, ou = users, dc = domain, dc = com` と表されます。
- **証明書 SAN RFC822 名を使用** - SAN の、rfc822Name タイプの最初のフィールドをユーザー名として使用します。これにはメールアドレスが含まれています。たとえば、`rfc822Name:testuser@domain.com` の場合、ユーザー名は `testuser@domain.com` となります。

OCSP 設定

OCSP URL 設定が有効になっている場合、認証用に入力されたユーザー証明書は、オンライン証明書ステータスプロトコルを使用して確認されます。

HTTP および HTTPS URL のみが受け付けられます。

応答が不明または失効状態の場合、認証は失敗します。

CAC Smartcard 認証用の信頼済み証明書の管理

信頼済み CA 証明書のインポート

前提条件

- iLO の設定を構成する権限
- 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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

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、**CAC Smartcard 認証**タブをクリックします。
2. **ダイレクトインポート**セクションに信頼済み CA 証明書を貼り付けます。

   証明書は、PEM でエンコードされた Base64 フォーマットでなければなりません。
3. **適用**をクリックします。

   操作が正常に実行されていないように思われる場合は、ページの上部にスクロールして、エラーメッセージが表示されていないかどうかを確認します。

証明書失効リスト（CRL）を URL からインポート

取り消された発行済み証明書を無効にするには、CRL をインポートします。

前提条件

- iLO の設定を構成する権限
- 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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

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、**CAC Smartcard 認証**タブをクリックします。
2. **失効リストのインポート**セクションに URL を入力するか貼り付けます。

   CRL のサイズ制限は 100 KB であり、CRL は DER フォーマットでなければなりません。
3. **適用**をクリックします。

   iLO が要求を確認するように求めます。
4. **はい、インポートします**をクリックします。

   CRL が**証明書失効リスト（CRL）**セクションに追加され、CRL の説明とシリアル番号が表示されます。

   操作が正常に実行されていないように思われる場合は、ページの上部にスクロールして、エラーメッセージが表示されていないかどうかを確認します。

証明書マッピング

証明書マップページには、システムのローカルユーザーと、それぞれに関連付けられた SHA-256 証明書指紋が表示されます。このページのコントロールを使用して、証明書を追加または削除します。

スマートカードまたは CAC 環境（**CAC/Smartcard** ページで構成）でスマートカードアクセスを許可するには、ローカルユーザーのスマートカード証明書が保存され、そのユーザーアカウントにマップされている必要があります。

新しいローカルユーザー証明書の承認

前提条件

- ユーザーアカウント管理権限
- 証明書が埋め込まれたスマートカードまたはその他の共通アクセスカード（CAC）を所持していること。

  証明書は設定されている iLO セキュリティ状態に準拠していなければならない。
- **CAC Smartcard 認証**が **CAC/Smartcard** タブで有効である。
- 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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックしてから、**証明書マッピング**タブをクリックします。

   iLO で、ローカルユーザーアカウントとそれぞれに関連付けられている SHA 256 証明書指紋のリストが表示されます。
2. **ログイン名**の横にあるチェックボックスをクリックして、ユーザーアカウントを選択します
3. **新しい証明書の承認**をクリックします。

   証明書インポートデータ貼り付けボックスが表示されます。
4. 選択したユーザーアカウントの証明書を PEM にエンコードされた Base64 形式でエクスポートします。
5. 証明書をテキストエディターで開きます。
6. 証明書をコピーして、**証明書**ボックスに貼り付けます。
7. **証明書のインポート**をクリックします。

SSL 証明書の管理

SSL（Secure Sockets Layer）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。SSL 証明書は、暗号化キー（サーバーの公開キー）とサーバー名をデジタル的に結合した小さなコンピューターファイルです。対応するプライベートキーを所有するサーバーのみが、ユーザーとサーバー間で認証済みの双方向通信を実現できます。

証明書は署名がないと有効になりません。認証機関（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、構成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。

重要: 自己署名証明書を使用するよりも、信頼済み証明書をインポートするほうが安全です。Hewlett Packard Enterprise では、信頼済み証明書をインポートして iLO ユーザーアカウント認証情報を保護することをお勧めします。

iLO のバックアップおよびリストア機能を使用する場合、証明書が含まれます。

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認証機関（CA）に送信できる証明書署名要求（CSR）を作成できます。

iLO は、3 KB まで（プライベートキーで使用される 1,187 バイトを含む）の 2,048 ビット SSL 証明書をサポートします。

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、CA から新しい証明書を取得するために、新しい CSR を生成する必要があります。

前提条件

iLO の設定を構成する権限

手順

1. **CA から信頼済みの証明書を取得します。**
2. **信頼済みの証明書を iLO にインポートします**。

CA からの信頼済み証明書の取得

前提条件

iLO の設定を構成する権限

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、**SSL 証明書**タブをクリックします。
2. **証明書のカスタマイズ**をクリックします。
3. 次の値を入力します。
   - **国（C）**
   - **州または県(ST)**
   - **都市または地域(L)**
   - **組織名(O)**
   - **組織ユニット(OU)**
   - **共通名(CN)**
4. （オプション）iLO IP アドレスを CSR に含めるには、**iLO の IP アドレスを含みます**チェックボックスを選択します。

   注記: 多くの認証機関（CA）では、この入力を受け入れることができません。使用中の CA でこの入力を受け入れることがわかっていない場合は、このオプションを選択しないでください。

   このオプションが有効な場合、iLO の IP アドレスが CSR サブジェクト代替名（SAN）の拡張子に含まれます。
5. **CSR の生成**をクリックします。

CSR 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。

6. 数分（最大 10 分）後に、**CSR の生成**を再度クリックします。

   CSR が表示されます。

7. CSR テキストを選択してコピーします。
8. 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。
9. 画面の指示に従って、CSR を CA に送信します。

   - 証明書の目的を選択するように求められたら、必ずサーバー証明書のオプションを選択してください。
   - CSR を CA に送信するときに、ご使用の環境でサブジェクト代替名の指定が要求される可能性があります。必要に応じて、iLO DNS 名を入力します。

   CA は証明書を生成します。証明書署名ハッシュは、CA によって決定されます。

10. 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。この値は、**概要**ページに **iLO ホスト名**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。

CSR 入力の詳細

CSR を作成するときは、次の詳細情報を入力します。

- **国（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。
- **州または県（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州または県。
- **都市または地域（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。
- **組織名（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。
- **組織ユニット（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。
- **共通名（CN）** - この iLO サブシステムの FQDN。

  FQDN は、**共通名（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、**ネットワーク共通設定**ページで**ドメイン名**を設定します。
- **iLO の IP アドレスを含みます** - CSR に iLO IP アドレスを含めるには、このチェックボックスを選択します。

注記: 多くの CA では、この入力を受け入れられません。使用中の CA でこの入力を受け入れることがわかっていない場合は、このオプションを選択しないでください。

証明書署名要求

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。iLO は、SHA-256 を使用して署名された 2048 ビット RSA キーまたは CNSA 準拠キーを生成します。生成された CSR は、新しい CSR が生成されるか、iLO が工場出荷時のデフォルト設定にリセットされるか、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。

信頼済みの証明書のインポート

前提条件

iLO の設定を構成する権限

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、**SSL 証明書**タブをクリックします。
2. **証明書のカスタマイズ**をクリックします。
3. **証明書のインポート**をクリックします。
4. **証明書のインポート**ウィンドウで、テキストボックスに証明書を貼り付けて、**インポート**をクリックします。

   iLO が要求を確認して iLO をリセットするように求めます。
5. **はい、適用およびリセット**をクリックします。

   iLO は、証明書をインポートしてからリセットします。

SSL 証明書の削除

この機能を使用して、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、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証明書を削除するよう勧められた。

前提条件

iLO 設定の構成権限

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、**SSL 証明書**タブをクリックします。
2. **削除**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するように求めます。
3. **はい、削除します**をクリックします。

   iLO がカスタム SSL 証明書を削除し、リセットしてから、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。
4. 推奨：信頼済みの証明書を取得してインポートします。

   Hewlett Packard Enterprise では、信頼済みの証明書をインポートすることをおすすめします。

iLO での Kerberos 認証

Kerberos のサポートにより、ユーザーはユーザー名とパスワードを入力する代わりに、ログインページの**Zero サインイン**ボタンをクリックして、iLO にログインすることができます。正常にログインするには、クライアントワークステーションがドメインにログインし、ユーザーが、iLO が設定されているディレクトリグループのメンバーでなければなりません。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 UPN 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。

システム管理者はユーザーサインオンの前に iLO とドメイン間の信頼関係を確立するため、(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アカウントを設定する方法については、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。

Kerberos 認証の構成

iLO で Kerberos 認証を構成するには、環境を準備してから iLO 内で Kerberos 設定を構成する必要があります。

構成の手順については、HPE iLO 5 ユーザーガイドを参照してください。

手順

1. iLO のホスト名およびドメイン名を構成します。
2. iLO ライセンスをインストールして Kerberos 認証を有効にします。
3. ドメインコントローラーで Kerberos サポートを準備します。
4. Kerberos キータブファイルを生成します。
5. ご使用の環境が Kerberos 認証の時刻要件を満たしていることを確認します。
6. iLO で Kerberos パラメーターを構成します。
7. iLO ディレクトリグループを構成します。
8. サポートされるブラウザーでシングルサインオンを設定します

iLO で使用するディレクトリ構成の選択

ディレクトリに対して iLO を構成する前に、スキーマフリー構成オプションか HPE 拡張スキーマ構成オプションかを選択します。

以下の質問について検討します。

1. **使用するディレクトリにスキーマ拡張を適用できますか。**
   - **「はい」の場合** - 質問 2 に進みます。
   - **「いいえ」の場合** - Active Directory を使用しており、お客様の会社のポリシーにより拡張を適用できません。

     「いいえ」の場合 - OpenLDAP を使用しています。HPE 拡張スキーマは、現時点では OpenLDAP でサポートされていません。

     「いいえ」の場合 - お使いの環境には、HPE 拡張スキーマとのディレクトリ統合は適しません。

     グループベースのスキーマフリーディレクトリ統合を使用します。試用版のサーバーをインストールして、HPE 拡張スキーマ構成とのディレクトリ統合の利点を検討してみるとよいでしょう。
2. **スケーラブルな設定を使用していますか。**

次の質問に回答すると、設定がスケーラブルかどうかがわかります。

- ディレクトリユーザーのグループの権限を変更する可能性がありますか。
- iLO の変更を定期的にスクリプト化するつもりですか。
- iLO 権限の制御に 6 つ以上のグループを使用しますか。

これらの質問に対する答えに応じて、次のオプションから選択します。

- **「いいえ」の場合** - スキーマフリーディレクトリ統合のインスタンスをインストールして、この方式がお使いのポリシーおよび手順の要件に合っているかどうかを検討してみましょう。必要に応じて、後で、HPE 拡張スキーマ構成を展開できます。
- **「はい」の場合** - HPE 拡張スキーマ構成を使用します。

ディレクトリ統合の利点

- **スケーラビリティ** - ディレクトリサービスを利用して、数千台の iLO プロセッサー上で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 iLO アカウントを共有することがあり、その場合、操作を実行したユーザーの特定が困難になります。
- **ロールベースの管理**（HPE 拡張スキーマ） - ロール（たとえば、事務処理、ホストのリモート制御、完全な制御）を作成して、ユーザーやユーザーグループに関連付けることができます。1 つのロールで変更が行われると、その変更は、そのロールに関連付けられたすべてのユーザーおよび iLO デバイスに適用されます。
- **集中管理**（HPE 拡張スキーマ） - MMC などオペレーティングシステム固有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** - ディレクトリでの 1 つの変更が、関連付けられた iLO プロセッサーにただちに公開されます。この機能により、このプロセスをスクリプト化する必要がなくなります。
- **認証情報の簡素化** - ディレクトリでは、iLO 用の新しい認証情報を記録せずに、既存のユーザーアカウントとパスワードを使用できます。
- **柔軟性**（HPE 拡張スキーマ） - 企業の環境に合わせて、1 台の iLO プロセッサーについて 1 ユーザーを対象に 1 つのロールを作成することも、複数の iLO プロセッサーについて複数のユーザーを対象に 1 つのロールを作成することも、ロールを組み合わせて使用することもできます。HPE 拡張スキーマ構成では、アクセスを特定の時間だけに制限したり、特定の IP アドレス範囲に制限したりすることができます。
- **互換性** - iLO ディレクトリ統合は、Active Directory および OpenLDAP をサポートします。
- **規格** - iLO ディレクトリサポートは、安全なディレクトリアクセスに関する LDAP 2.0 規格に基づいています。iLO の Kerberos サポートは LDAP v3 に基づいています。

スキーマフリーディレクトリ認証

スキーマフリーディレクトリ認証を使用すると、ユーザーおよびグループがディレクトリに存在し、グループ権限が iLO の設定に存在します。iLO はディレクトリログイン証明書を使用してディレクトリ内のユーザーオブジェクトを読み取り、ユーザーグループのメンバーシップを取得します。これらのグループは、iLO のグループ構成と比較されます。ディレクトリユーザーアカウントが、構成されている iLO ディレクトリグループのメンバーとして確認されると、iLO のログインに成功します。

スキーマフリーディレクトリ統合の利点

- ディレクトリスキーマを拡張する必要がありません。
- ディレクトリ内のユーザーについては、設定はほとんど必要ありません。設定が存在しない場合、ディレクトリは既存のユーザーおよびグループメンバーシップを使用して iLO にアクセスします。たとえば、User1 というドメイン管理者がいるとすると、このドメイン管理者のセキュリティグループの DN を iLO にコピーして、フル権限を与えます。すると、User1 は iLO にアクセスできるようになります。

スキーマフリーディレクトリ統合の欠点

グループ権限は、各 iLO システムで管理されます。この欠点は、グループ権限がほとんど変更されないため最小限に抑えられ、グループのメンバーシップを変更するタスクは、各 iLO システムでなく、ディレクトリで管理されます。Hewlett Packard Enterprise は、同時に複数の iLO システムを構成できるツールを提供しています。

構成オプション

スキーマフリーのセットアップオプションは、ディレクトリ用の設定にどの方法を用いても同じです。最も柔軟でないログイン、より柔軟なログイン、または非常に柔軟なログインのディレクトリ設定を構成できます。

- **最も柔軟でないログイン** - この構成を使用すると、完全 DN とパスワードを入力して iLO にログインできます。iLO が認識するグループのメンバーでなければなりません。

  この構成を使用するには、次の設定を入力します。

  - ディレクトリサーバーの DNS 名または IP アドレスと LDAP ポート。通常、SSL 接続用の LDAP ポートは、636 です。
  - 少なくとも 1 つのグループの DN。このグループは、セキュリティグループ（例：Active Directory の場合は `CN=Administrators,CN=Builtin,DC=EXAMPLE,DC=COM`、OpenLDAP の場合は `UID=username,ou=People,dc=hpe,dc=com`）、または目的の iLO ユーザーがグループメンバーであれば、別のどのグループでもかまいません。

- **より柔軟なログイン** - この構成を使用すると、ログイン名とパスワードを入力して iLO にログインできます。iLO が認識するグループのメンバーでなければなりません。ログイン時に、ログイン名とユーザーコンテキストが結合されて、ユーザー DN になります。

  この構成を使用するには、最も柔軟でないログインの設定と少なくとも 1 つのディレクトリユーザーコンテキストを入力します。

  たとえば、ユーザーが `JOHN.SMITH` としてログインし、ユーザーコンテキスト `CN=USERS,DC=EXAMPLE,DC=COM` が構成されている場合は、iLO で `CN=JOHN.SMITH,CN=USERS,DC=EXAMPLE,DC=COM` という DN が使用されます。

- **非常に柔軟なログイン** - この構成を使用すると、完全な DN とパスワード、ディレクトリに表示される名前、NetBIOS 形式（domain/login_name）、または電子メール形式（login_name@domain）を使用して iLO にログインできます。

  この構成を使用するには、IP アドレスの代わりにディレクトリの DNS 名を入力して、iLO にディレクトリサーバーアドレスを構成します。DNS 名は、iLO およびクライアントシステムの両方から、IP アドレスに解決できなければなりません。

スキーマフリーディレクトリ統合を使用するための前提条件

手順

1. Active Directory および DNS をインストールします。
2. ルート CA をインストールして、SSL を有効にします。

iLO は、安全な SSL 接続でのみ、ディレクトリと通信します。

Active Directory での証明書サービスの使用について詳しくは、Microsoft のドキュメントを参照してください。

3. 少なくとも 1 人のユーザーのディレクトリ DN とそのユーザーが含まれているセキュリティグループの DN が、使用可能であることを確認します。

   この情報は、ディレクトリのセットアップを検証するために使用されます。

4. ディレクトリサービス認証を有効にする iLO ライセンスをインストールします。
5. iLO ネットワーク設定の IPv4 または IPv6 のページで、正しい DNS サーバーが指定されていることを確認します。

ディレクトリ統合の構成（スキーマフリー構成）

iLO でスキーマフリーディレクトリ統合を構成するには 、環境を準備してから、iLO 内で設定を構成する必要があります。

構成の手順については、HPE iLO 5 ユーザーガイドを参照してください。

手順

1. ご使用の環境がスキーマフリーのディレクトリ統合を使用するための前提条件を満たしていることを確認します。
2. iLO スキーマフリーディレクトリのパラメーターを構成します。
3. ディレクトリグループを構成します。

HPE 拡張スキーマディレクトリ認証

HPE 拡張スキーマディレクトリ認証オプションを使用すると、以下のことを行うことができます。

- 統合されたスケーラブルな共有ユーザーデータベースからユーザーを認証します。
- ディレクトリサービスを使用して、ユーザーの権限を制御（権限付与）します。
- ディレクトリサービスでは、iLO 管理プロセッサーおよび iLO ユーザーのグループレベルの管理にロールを使用します。

HPE 拡張スキーマディレクトリ統合の利点

- グループが各 iLO 上ではなく、ディレクトリ内で維持管理されます。
- 柔軟なアクセス制御 - アクセスを特定の時間だけに制限したり、特定の IP アドレス範囲に制限したりすることができます。

ディレクトリサービスのサポート

iLO ソフトウェアは、Microsoft Active Directory ユーザーとコンピュータースナップイン内で動作するように設計されており、ユーザーは、ディレクトリ経由でユーザーアカウントを管理できます。

iLO は、HPE 拡張スキーマ構成で Microsoft Active Directory をサポートします。

HPE 拡張スキーマ構成で Active Directory を設定するための前提条件

手順

1. Active Directory および DNS をインストールします。
2. ルート CA をインストールして、SSL を有効にします。

   iLO は、安全な SSL 接続でのみ、ディレクトリと通信します。

   Active Directory での証明書サービスの使用について詳しくは、Microsoft のドキュメントを参照してください。

   iLO には、ディレクトリサービスと通信するためにセキュリティ保護された接続が必要です。この接続には、Microsoft CA をインストールする必要があります。詳しくは、Microsoft Knowledge Base の Article ID 番号 321051 を参照してください。サードパーティの証明機関が SSL 経由で LDAP を有効にする方法
3. .NET Framework のバージョン 3.5 以降がインストールされていることを確認します。

   iLO LDAP コンポーネントはこのソフトウェアを必要とします。

   Windows Server Core 環境では LDAP コンポーネントを使用できません。
4. 次の Microsoft Knowledge Base の記事を参照してください。299687 MS01-036: LDAP over SSL の機能によりパスワードの変更が可能になる

ディレクトリ統合の構成（HPE 拡張スキーマ構成）

iLO で HPE 拡張スキーマを構成するには、環境を準備してから、iLO 内で設定を構成する必要があります 。

構成の手順については、HPE iLO 5 ユーザーガイドを参照してください。

手順

計画

1. HPE iLO 5 ユーザーガイドの次のセクションを確認してください。
   - ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）
   - ディレクトリサービススキーマ

インストール

2. 次のように操作します。
   a. ご使用の環境が Active Directory と HPE 拡張スキーマを構成するための前提条件を満たしていることを確認します。
   b. ディレクトリサービス認証を有効にする iLO ライセンスをインストールします。
   c. ProLiant マネジメントプロセッサー用のディレクトリサポートパッケージをダウンロードし、ご使用の環境に必要なユーティリティをインストールします。

      Schema Extender、スナップイン、および ProLiant マネジメントプロセッサー用のディレクトリサポートユーティリティをインストールすることができます。
   d. スキーマエクステンダーを使用してスキーマを拡張します。

アップデート

3. iLO の Web インターフェイスで、管理プロセッサーオブジェクトのディレクトリサーバー設定と DN を設定します。

このステップは、ProLiant 管理プロセッサーのディレクトリサポートソフトウェアを使用して実行することもできます。

ロールとオブジェクトの管理

4. HPE Active Directory スナップインを使用して、デバイスオブジェクトとロールオブジェクトを構成します。

   a. マネジメントデバイスオブジェクトとロールオブジェクトを作成します。

   b. 必要に応じて、ロールオブジェクトに権限を割り当て、役割を管理デバイスオブジェクトと関連付けます。

   c. ユーザーをロールオブジェクトに追加します。

例外の取り扱い

5. 複雑なロール関連付けについては、ディレクトリスクリプティングユーティリティの使用を検討してください。

   iLO ユーティリティは、単一のロールで簡単に使用できます。ディレクトリに複数の役割を作成することを計画している場合は、`LDIFDE` または VBScript ユーティリティのようなディレクトリスクリプティングユーティリティを使用することができます。これらのユーティリティは複雑なロールの関係を作成します。

ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）

ディレクトリ対応リモート管理により、以下の作業を実行できます。

Lights-Out Management オブジェクトの作成

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うデバイスごとに、そのデバイスを表す LOM デバイスオブジェクトを 1 つ作成する必要があります。Hewlett Packard Enterprise スナップインを使用して LOM オブジェクトを作成することができます。

Hewlett Packard Enterprise は、LOM デバイスオブジェクトに意味のある名前を付けることをおすすめします。たとえば、デバイスのネットワークアドレス、DNS 名、ホストサーバー名、シリアル番号などを使用できます。

Lights-Out マネジメントデバイスの設定

ユーザーの認証や権限付与にディレクトリサービスを使用するすべての LOM デバイスは、適切なディレクトリ設定を使用して設定する必要があります。一般に、各デバイスを、適切なディレクトリサーバーアドレス、LOM オブジェクト DN、およびユーザーコンテキストを使用して設定します。サーバーアドレスは、ローカルディレクトリサーバーの IP アドレスまたは DNS 名です。冗長性を高くするために、マルチホスト DNS 名を使用できます。

組織構造に基づいたロール

組織内の管理者は、下級管理者が上級管理者から独立して権限を割り当てなければならない階層体制に属している場合があります。このような場合、上級管理者によって割り当てられる権限を表すロールを 1 つ作成するとともに、下級管理者が独自のロールを作成して管理することを許可すると便利です。

既存のグループの使用

多くの組織では、ユーザーや管理者をグループ分けしています。多くの場合、既存のグループを使用し、そのグループを 1 つまたは複数の LOM ロールオブジェクトに関連付けると便利です。デバイスがロールオブジェクトに関連付けられている場合、管理者は、グループのメンバーを追加または削除することによって、そのロールに関連付けられた Lights-Out デバイスへのアクセスを制御します。

Microsoft Active Directory を使用する場合は、あるグループを別のグループ内に配置できます（つまり、入れ子型のグループを使用できます）。ロールオブジェクトはグループとみなされ、他のグループを直接含むこと

ができます。既存の入れ子型グループを直接ロールに追加し、適切な権限と制限を割り当ててください。新しいユーザーを、既存のグループまたはロールのいずれかに追加できます。

トラスティまたはディレクトリ権限割り当てを使用してロールのメンバーシップを拡張する場合、ユーザーは、LOM デバイスを表す LOM オブジェクトを読み出すことができる必要があります。一部の環境では、正常なユーザー認証を行うために、ロールのトラスティが、オブジェクトの読み出すトラスティでもある必要があります。

複数のロールの使用

ほとんどのデプロイメントでは、同じユーザーが、同じデバイスを管理する複数のロールに入っている必要はありません。ただし、これらの構成は、複雑な権限関係を構築する際には便利です。ユーザーが複数のロールの関係を構築すると、そのユーザーには、該当する各ロールによって割り当てられるすべての権限が付与されます。ロールは、権限を付与することしかできず、権限を取り消すことはできません。あるロールがユーザーに権限を付与する場合、そのユーザーは、その権限を付与しない別のロールに入っていても、その権限を持ちます。

一般に、ディレクトリ管理者は、最小の数の権限が割り当てられたベースロールを作成し、追加のロールを作成して権限を追加します。これらの追加権限は、特定の状況で、またはベースロールユーザーの特定のサブセットに追加されます。

たとえば、組織は、LOM デバイスまたはホストサーバーの管理者と LOM デバイスのユーザーという 2 つのタイプのユーザーを持つことがあります。この状況では、管理者のロールとユーザーのロールという 2 つのロールを作成することが有効です。両方のロールにはいくつかの同じデバイスが含まれますが、これらのロールは異なる権限を付与します。より小さなロールに包括的な権限を割り当てて、LOM 管理者をそのロールと管理者ロールに入れると便利な場合があります。

図 5: 複数の（重複する）ロールには、管理者ユーザーがユーザーロールからログイン権限を取得し、管理者ロールから高度な権限が割り当てられる例を示します。

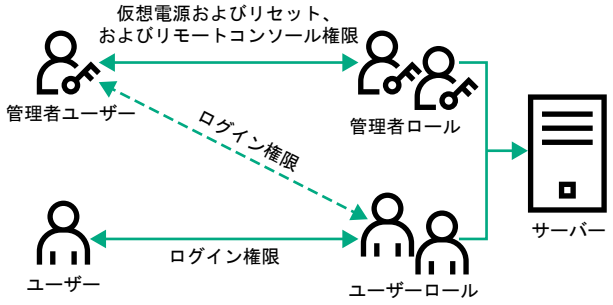


図 5: 複数の（重複する）ロール

重複するロールを使用しない場合は、**図 6: 複数の（独立した）ロール**に示すように、ログイン、仮想電源およびリセット、およびリモートコンソール権限を管理者ロールに割り当て、ログイン権限をユーザーロールに割り当てることがあります。

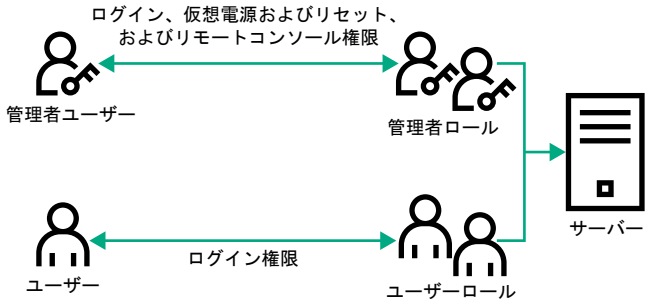


図 6: 複数の（独立した）ロール

ロールアクセス制限の適用方法

ディレクトリユーザーによる LOM デバイスへのアクセスは、2 段階の制限によって限定することができます。

- **ユーザーアクセス制限**は、ディレクトリへの認証を受けるためのユーザーアクセスを限定します。
- **ロールアクセス制限**は、1 つまたは複数のロールでの指定に基づいて LOM 権限を受けることができる認証済みユーザーの機能を限定します。

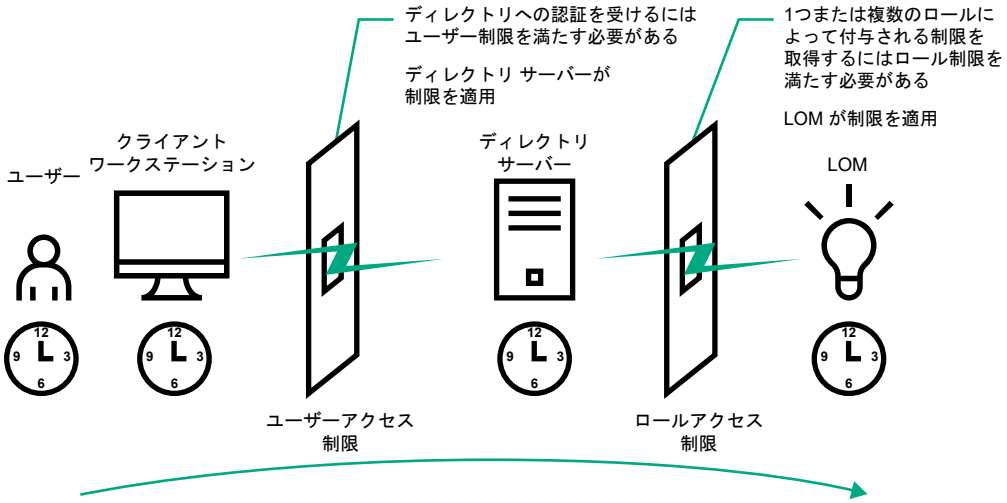


図 7: ディレクトリのログイン制限

ユーザーアクセス制限

アドレス制限

管理者は、ディレクトリユーザーアカウントにネットワークアドレス制限を設定できます。ディレクトリサーバーには、これらの制限が適用されます。

LDAP クライアント（LOM デバイスへのユーザーのログインなど）へのアドレス制限の適用について詳しくは、ディレクトリサービスのドキュメントを参照してください。

ディレクトリのユーザーに設定したネットワークアドレス制限は、ディレクトリユーザーがプロキシサーバー経由でログインする場合は、予期したとおりに適用されない場合があります。ユーザーがディレクトリユーザーとして LOM デバイスにログインする場合は、LOM デバイスが、そのユーザーとしてのディレクトリへの認証を試みます。つまり、ユーザーアカウントに設定されたアドレス制限が、LOM デバイスへのアクセス時に適用されます。プロキシサーバーが使用される場合は、認証が試みられるネットワークアドレスがクライアントワークステーションのものではなく、LOM デバイスのものになります。

IPv4 アドレス範囲制限

IP アドレス範囲制限によって、管理者は、アクセスを許可または拒否するネットワークアドレスを指定することができます。

アドレス範囲は、一般に、「最小-最大」範囲フォーマットで指定します。アドレス範囲を指定して、単一のアドレスのアクセスを許可または拒否することもできます。「最小-最大」IP アドレス範囲内のアドレスには、IP アドレス制限が適用されます。

IPv4 アドレスおよびサブネットマスク制限

IP アドレスおよびサブネットマスク制限によって、管理者は、アクセスを許可または拒否するアドレスの範囲を指定することができます。

このフォーマットは、IP アドレス範囲制限に似ていますが、ご使用のネットワーク環境によっては特有のものになる場合があります。IP アドレスおよびサブネットマスク範囲は、一般に、同じ論理ネットワーク上のアドレスを特定するサブネットアドレスおよびアドレスビットマスクによって指定します。

2 進数演算で、クライアントマシンのアドレスのビットにサブネットマスクのビットを加えたものが制限にあるサブネットアドレスと一致する場合、クライアントは制限を満たします。

DNS ベース制限

DNS ベース制限では、ネットワークネームサービスを使用して、クライアント IP アドレスに割り当てられたマシン名を検出することによって、クライアントマシンの論理名を調べます。DNS 制限には、正常に動作しているネームサーバーが必要です。ネームサービスがダウンしていたり、利用できなかったりすると、DNS 制限が満たされず、クライアントマシンは制限を満たすことができなくなります。

DNS ベース制限を使用すると、特定マシン名や、共通のドメインサフィックスを共有するマシンへのアクセスを制限できます。たとえば、**www.example.com** という DNS 制限は、**www.example.com** というドメイン名が割り当てられているホストによって満たされ、***.example.com** という DNS 制限は、**example** 社が提供元になっているすべてのマシンによって満たされます。

マルチホームホストを使用している場合があるので、DNS 制限では、あいまいさが発生する可能性があります。DNS 制限は、必ずしも単一のシステムに一対一で適用されるわけではありません。

DNS ベース制限を使用すると、セキュリティが複雑になる場合があります。ネームサービスプロトコルは、安全ではありません。ネットワークにアクセスできる悪意を持ったユーザーは、誰でも、不正な DNS サーバーをネットワークに配置して偽のアドレス制限基準を作成することができます。DNS ベースのアドレス制限を実装している場合は、組織的なセキュリティポリシーを考慮に入れてください。

ユーザーの時間制限

時間制限によって、ディレクトリへのユーザーのログイン（認証）が限定されます。通常、時間制限は、ディレクトリサーバーの時間を使用して適用されます。ディレクトリサーバーが異なるタイムゾーンにある場合または異なるタイムゾーンにあるレプリカサーバーにアクセスしている場合は、管理対象オブジェクトからのタイムゾーン情報を使用して相対的な時間を調整することができます。

ディレクトリサーバーは、ユーザーの時間制限を確認しますが、判定方法は、タイムゾーンの変化や認証メカニズムによって複雑になる場合があります。

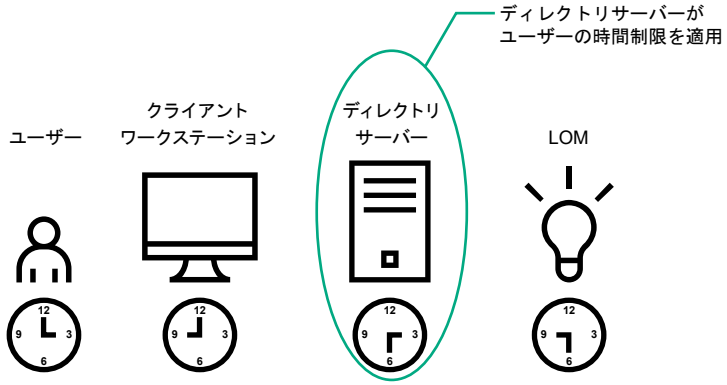


図 8: ユーザーの時間制限

ロールアクセス制限

制限によって、管理者は、ロールの範囲を限定することができます。ロールは、ロールの制限を満たすユーザーだけに権限を付与します。制限付きロールを使用することによって、ユーザーに、時間帯やクライアントのネットワークアドレスによって変化する動的権限を付与することができます。

ディレクトリが有効な場合、iLO システムへアクセス可能かどうかは、該当する iLO オブジェクトを含むロールオブジェクトへの読み取りアクセス権が、ユーザーにあるかどうかによって決まります。このユーザーには、ロールオブジェクトで許可されているメンバーも含まれますが、そのメンバーに限定されません。継承可

能な権限を親から伝達できるようにロールを設定すると、読み出し権限を持つ親のメンバーも iLO にアクセスできます。

アクセス制御リストを表示するには、**Active Directory Users and Computers** に移動し、ロールオブジェクトの**プロパティ**ページを開き、**セキュリティ**タブをクリックします。**セキュリティ**タブを表示するには、MMC で Advanced View を有効にする必要があります。

ロールベースの時間制限

管理者は、LOM ロールに時間制限を設定することができます。ユーザーには、そのユーザーがロールのメンバーであり、そのロールの時間制限を満たしている場合にのみ、そのロールに示されている LOM デバイスについて、指定された権限が付与されます。

ロールベースの時間制限は、LOM デバイスで時間が設定されている場合にのみ、機能します。LOM デバイスは、ローカルホストの時間に従って、時間制限を適用します。LOM デバイスの時計が設定されていない場合、ロールに対して時間制限が指定されていない限り、ロールベースの時間制限は適用されません。時間は、通常、ホストの起動時に設定されます。

時間設定は、SNTP を設定することで維持できます。SNTP によって、LOM デバイスでうるう年を補正することや、ホストとの時間のずれを最小限に抑えることができます。予定外の停電や LOM ファームウェアのフラッシュなどのイベントによって、LOM デバイスの時計が設定されないことがあります。また、LOM デバイスがファームウェアをフラッシュする時間の設定を保持するために、ホストの時間は正確でなければなりません。

ロールベースのアドレス制限

LOM ファームウェアでは、クライアントの IP ネットワークアドレスに基づいてロールベースのアドレス制限が適用されます。ロールのアドレス制限が満たされる場合、そのロールによって付与される権利が適用されます。

ファイアウォールの外からのアクセスやネットワークプロキシ経由のアクセスが試みられる場合、アドレス制限は、管理が困難になる場合があります。これらの方式のアクセスが可能な場合、クライアントの見かけ上のネットワークアドレスが変更されることがあるので、アドレス制限の予期しない適用が発生する場合があります。

複数の制限およびロール

権限の適用される状況が限定されるように 1 つまたは複数のロールを制限したい場合には、多数のロールを作成すると非常に便利です。他のロールが、異なる権限を異なる制限で付与します。複数の制限とロールを使用すると、管理者は、任意の複雑な権限関係を最小限のロールで作成できます。

たとえば、組織が、LOM 管理者について、「企業ネットワーク内から LOM デバイスを使用できるが通常の業務時間外にはサーバーのリセットしかできない」というセキュリティポリシーを設定しているとします。

ディレクトリ管理者は、2 つのロールを作成してこの状況に対応しようと考えるかもしれませんが、この場合には特別の注意が必要です。必要なサーバーリセット権限を付与するロールを作成し、このロールを業務時間外に制限すると、管理者が企業ネットワークの外からサーバーをリセットできるようになる場合があり、多くの場合セキュリティポリシーに反します。

図 9: 制限およびロールの作成では、セキュリティポリシーで、一般的な使用を企業サブネット内のクライアントに制限しており、サーバーリセット操作を業務時間外に制限していることを示しています。

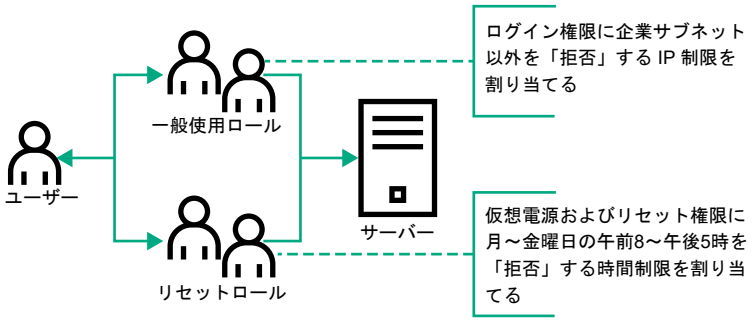


図 9: 制限およびロールの作成

また、ディレクトリ管理者は、ログイン権限を付与するロールを作成し、このロールを企業ネットワークに制限した後、サーバーリセット権限だけを付与する別のロールを作成し、これを業務時間外に制限しようと考えるかもしれません。この設定では管理が簡単になりますが、継続的な管理によって企業ネットワーク外部のアドレスからのユーザーにログイン権限を付与する別のロールが作成される場合があるため、危険性が増します。サーバーリセットロールに属する LOM 管理者がロールの時間制限を満たす場合、このロールは意図せずに、この LOM 管理者にどこからでもサーバーをリセットできる権限を付与する可能性があります。

図 9: 制限およびロールの作成に示されている設定は、企業のセキュリティ要件を満たしています。ただし、ログイン権限を付与する別のロールを追加することによって、間違って、業務時間外に企業サブネットの外からサーバーをリセットする権限を付与する可能性があります。**図 10: リセットロールと一般使用ロールの制限**で示すように、リセットロールと一般使用ロールを制限することによって、より管理しやすいソリューションを実現できます。

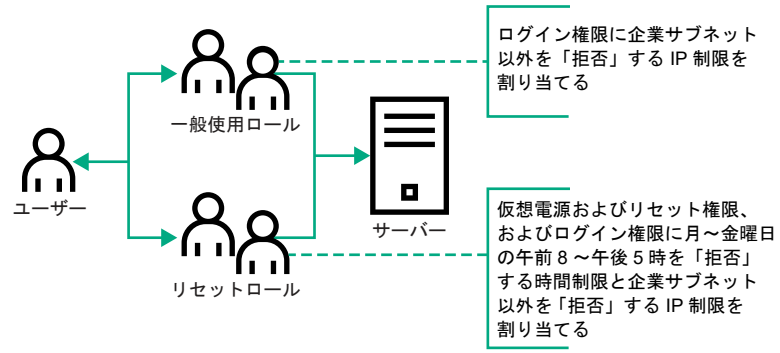


図 10: リセットロールと一般使用ロールの制限

iLO 暗号化設定

すべての Gen10 以降のサーバーに付属している HPE iLO Standard によって、お客様は次の 3 つのセキュリティ状態のいずれかでサーバーを構成することができます。iLO Advanced のライセンスでは、CNSA の最上位レベルの暗号化機能を必要とするお客様は 4 つ目のセキュリティ状態を利用できます。

セキュリティの段階が上がると、サーバーは、Web ページ、SSH、およびネットワーク通信に対してより強力な暗号化規則を適用します。各ネットワーク接続の両端が暗号化規則をサポートしている必要があることに注意してください。そうでないと通信はできず、インターフェイスによっては潜在的なセキュリティ上の脅威を制限するためにシャットダウンされます。

次のセキュリティ状態を利用できます。

- 本番環境
- 高セキュリティ

- FIPS
- CNSA

製品または「高セキュリティ」セキュリティ状態の有効化

前提条件

iLO の設定を構成する権限

手順

1. （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。
2. ナビゲーションツリーで**セキュリティ**をクリックして、**暗号化**タブをクリックします。
3. **セキュリティ状態**メニューで**本番環境**または**高セキュリティ**を選択します。
4. **適用**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。
5. 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。
6. 開いているブラウザー 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。
7. （オプション）「高セキュリティ」セキュリティ状態を有効にした場合は、**アクセス設定**ページの**匿名データ**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

この手順は、FIPS または CNSA のセキュリティ状態を構成するためのものです。iLO を FIPS 承認済み環境に構成するには、**iLO による FIPS 承認済み環境の構成**を参照してください。

前提条件

- iLO の設定を構成する権限
- 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）現在の iLO 構成をバックアップします。

   以下を使用して、この手順を実行できます。

   - **iLO Web インターフェイス**
   - RESTful インターフェイスツール

- iLO RESTful API
- HPONCFG

2. （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。
3. ナビゲーションツリーで**セキュリティ**をクリックして、**暗号化**タブをクリックします。
4. **セキュリティ状態**メニューで **FIPS** を選択して、**適用**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:** 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。

5. 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、**はい、適用およびリセット**をクリックします。

   iLO が FIPS セキュリティ状態を有効にした状態で再起動します。接続の再確立が試みられるまでに 90 秒以上かかります。

6. （オプション）CNSA セキュリティ状態を有効にします。

   a. 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。

   b. ナビゲーションツリーで**セキュリティ**をクリックして、**暗号化**タブをクリックします。

   c. **セキュリティ状態**メニューで **CNSA** を選択して、**適用**をクリックします。

      iLO が要求を確認するように求めます。

   d. CNSA 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、**はい、適用およびリセット**をクリックします。

      iLO が CNSA セキュリティ状態を有効にした状態で再起動します。接続の再確立が試みられるまでに 90 秒以上かかります。

   e. 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。

   CNSA の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 は構成された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。

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. **アクセス設定**ページで **IPMI/DCMI over LAN アクセス**、**匿名データ**、および **SNMP アクセス**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 インターフェイスは、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。

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**にあります。iLO 5 FIPS 情報にアクセスするには、検証済みモジュールの検索ページで証明書番号 3122 を入力します。

9. （オプション）iLO 構成をバックアップしている場合は、それをリストアします。

   以下を使用して、この手順を実行できます。

   - **iLO Web インターフェイス**
   - RESTful インターフェイスツール
   - iLO RESTful API
   - HPONCFG

10. （オプション）構成をリストアした場合は、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。
11. （オプション）構成をリストアした場合は、**アクセス設定**ページで **IPMI/DCMI over LAN アクセス**、**匿名データ**、および **SNMP アクセス**が無効になっていることを確認します。

    これらの設定は、構成をリストアするとリセットされる可能性があります。
12. （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（本番環境）よりも高いセキュリティ状態を有効にすると、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、交渉済み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 ユーティリティのドキュメントを参照してください。

RIBCL

- HPQLOCFG は、以下のような暗号詳細を出力表示します。

  ```
  Detecting iLO...
  Negotiated cipher: 256-bit Aes256 with 0-bit Sha384 and 384-bit 44550
  ```

- HPONCFG では、「高セキュリティ」、FIPS、または CNSA のセキュリティ状態が有効なときユーザー認証情報が必要になります。必要なユーザーの権限が割り当てられていない場合は、エラーメッセージが表示されます。

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。

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。

検証済みのセキュリティポリシードキュメントは、**NIST の Web サイト**にあります。iLO 5 FIPS 情報にアクセスするには、検証済みモジュールの検索ページで証明書番号 3122 を入力します。

FIPS セキュリティ状態の無効化

手順

1. FIPS セキュリティ状態を無効にするには（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、RIBCL スクリプト、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、すべての iLO 設定が消去されます。消去される設定は、ユーザーデータ、ライセンスデータ、構成設定、ログなどです。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 iLO 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ログに記録されません。

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 インターフェイスに表示されません。

CNSA セキュリティ状態の無効化

手順

1. CNSA セキュリティ状態を無効にするには、次のいずれかを実行します。

   - CNSA セキュリティ状態を無効にして、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 および FIPS セキュリティ状態を無効にするには、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、RIBCL スクリプト、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、すべての iLO 設定が消去されます。消去される設定は、ユーザーデータ、ライセンスデータ、構成設定、ログなどです。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 iLO 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 インターフェイスに表示されません。

iLO セキュリティ状態

本番環境（デフォルト）

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。

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、以下を経由した安全な HTTP 伝送を含め、安全なチャネル経由の AES 暗号の使用を強制します。
  - ブラウザー
  - SSH ポート
  - iLO RESTful API
  - RIBCL

  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 に接続します。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。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。
  - iLO RESTful API
  - RIBCL
- 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。
- HPQLOCFG ユーティリティは、iLO との SSL 接続をネゴシエーションした後、利用可能な最強の暗号を使用して RIBCL スクリプトをネットワーク経由で iLO に送信します。
- 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

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。

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、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 承認済みと同じではありません。FIPS 承認済みは、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。
- iLO は、以下を経由した安全な HTTP 伝送を含め、安全なチャネル経由の AES 暗号の使用を強制します。
  - ブラウザー
  - SSH ポート
  - iLO RESTful API
  - RIBCL

  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 に接続します。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。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。
  - iLO RESTful API
  - RIBCL
- 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。
- HPQLOCFG ユーティリティは、iLO との SSL 接続をネゴシエーションした後、利用可能な最強の暗号を使用して RIBCL スクリプトをネットワーク経由で iLO に送信します。
- 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

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。

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、NSA によって定義された CNSA 要件への準拠を目的とするモードで動作します。
- iLO は、米国政府機密として分類されたデータを保持するシステムの保護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
- HPE および他社製のスクリプティングツールとコマンドラインツール
- HPE および他社製の管理ツール
- アラートメール、syslog、LDAP、またはキーマネージャーサーバー
- Remote Support ソフトウェア

- HTML5 リモートコンソールを使用していることを確認してください。このコンソールでは、AES-256 ビット CNSA 準拠の暗号の使用が強制されます。

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。

Synergy セキュリティモード

サポートされるデバイスで使用される特別なセキュリティ状態。このモードを使用するデバイスのセキュリティ状態は変更できません。

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。

本番稼働

- 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

CNSA

- AEAD_AES_256_GCM および AES256-GCM 暗号
- ecdh-sha2-nistp384 キー交換
- AEAD_AES_256_GCM MAC

Synergy セキュリティモード

- AEAD_AES_256_GCM および AES256-GCM 暗号
- ecdh-sha2-nistp384 キー交換
- 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、セッション中に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、キーマネージャーサーバー、SSO サーバー、Insight Remote Support 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。

本番稼働

- 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

Synergy セキュリティモード

- 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

HPE SSO

HPE SSO を使用すると、HPE SSO 準拠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、以下の手順に従ってください。

- サポートされるバージョンの、HPE SSO に準拠したアプリケーションが必要です。
- SSO 準拠アプリケーションを信頼するように iLO を構成します。
- CAC 厳密モードが有効な場合は、信頼済み証明書をインストールします。

iLO には、HPE SSO 証明書の最小要件を決定するために HPE SSO アプリケーションのサポートが含まれます。HPE SSO 準拠アプリケーションの中には、iLO に接続したときに自動的に信頼証明書をインポートする

ものがあります。この機能を自動的に実行しないアプリケーションの場合は、HPE SSO ページを使用して SSO 設定を構成してください。

HPE SSO 用の iLO の設定

前提条件

iLO の設定を構成する権限

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、**HPE SSO** タブをクリックします。
2. **SSO 信頼モード**設定を構成します。

   Hewlett Packard Enterprise では**証明書による信頼**モードを使用することをおすすめします。
3. 各役割の iLO 権限は、**シングルサインオン設定**セクションで設定します。
4. **適用**をクリックします。
5. **証明書による信頼**または**名前による信頼**を選択した場合は、信頼済みの証明書または DNS 名を iLO に追加します。

   手順については、**信頼済みの証明書の追加**または**直接 DNS 名のインポート**を参照してください。
6. （オプション）HPE SSO 準拠アプリケーションにログインし、iLO をブラウズして、SSO 接続をテストします。

   たとえば、HPE SIM にログインし、**システム**ページに移動して iLO プロセッサーを見つけて、**詳細情報**セクションの iLO リンクをクリックします。

   SSO 信頼モードが**信頼なし**に設定されている場合、信頼できるサーバーのリストは使用されません。iLO は SSO サーバー証明書失効を強制しません。

シングルサインオン信頼モードオプション

シングルサインオン信頼モードは、HPE SSO 要求に対する iLO の応答方法に影響します。

- **信頼なし（SSO 無効）**（デフォルト） - すべての SSO 接続要求を拒否します。
- **証明書による信頼**（最も安全） - iLO に事前にインポートされている証明書と一致させて、HPE SSO 対応アプリケーションから SSO 接続を有効にします。
- **名前による信頼** - 直接インポートされた IP アドレスまたは DNS 名を一致させて、HPE SSO 準拠アプリケーションから SSO 接続を有効にします。
- **すべて信頼**（最も安全性が低い） - どの HPE SSO 対応アプリケーションから開始された SSO 接続も、すべて受け入れます。

SSO ユーザー権限

HPE SSO 準拠アプリケーションにログインする場合、HPE SSO 準拠アプリケーションの役割割り当てに基づいて認可されます。割り当てられている役割は、SSO が試みられるときに、iLO に渡されます。

SSO は**シングルサインオン設定**セクションで割り当てられた権限のみを受け入れようとします。iLO ディレクトリ設定は適用されません。

デフォルトの権限設定は以下のとおりです。

- **ユーザー** — ログインのみ
- **オペレーター** - ログイン、リモートコンソール、仮想電源およびリセット、仮想メディア、およびホスト BIOS 構成
- **管理者** - ログイン、リモートコンソール、仮想電源およびリセット、仮想メディア、ホスト BIOS 構成、iLO の設定の構成、ユーザーアカウント管理、ホスト NIC 構成、およびホストストレージ構成

信頼済みの証明書の追加

証明書レポジトリは、標準的な証明書を 5 つ保持できます。標準的な証明書が発行されない場合、証明書のサイズは一定ではありません。割り当てられた保管領域がすべて使われると、それ以上のインポートは受け付けられません。

特定の HPE SSO 対応アプリケーションから証明書を抽出する方法については、HPE SSO 対応アプリケーションのドキュメントを参照してください。

前提条件

iLO の設定を構成する権限

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、**HPE SSO** タブをクリックします。
2. **インポート**をクリックします。
3. 次のいずれかの方法を使用して、信頼済み証明書を追加します。
   - **ダイレクトインポート** - Base64 でエンコードされた証明書の X.509 データをコピーし、**ダイレクトインポート**セクションのテキストボックスに貼り付けてから、**適用**をクリックします。
   - **インダイレクトインポート** - DNS 名、IP アドレス、または証明書 URL を **URL からのインポート**セクションのテキストボックスに入力してから、**適用**をクリックします。

     iLO はネットワーク経由で HPE SSO 対応アプリケーションに接続して、証明書を取得して保存します。

直接 DNS 名のインポート

前提条件

iLO 設定の構成権限

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、**HPE SSO** タブをクリックします。
2. **インポート**をクリックします
3. **直接 DNS 名のインポート**セクションに DNS 名または IP アドレスを入力し（最大 64 文字）、**適用**をクリックします。

ログインセキュリティバナーの構成

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、メッセージとサーバー所有者の連絡先情報を入力できます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックして、**ログインセキュリティバナー**をクリックします。
2. **ログインセキュリティバナーを有効**設定を有効にします。

   iLO は、ログインセキュリティバナーに以下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、**セキュリティメッセージ**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。

   空白スペースまたは空白行をセキュリティメッセージに追加しないでください。空白スペースと空白行はバイト数にカウントされ、ログインページのセキュリティバナーには表示されません。

   ヒント: デフォルトのテキストをリストアするには、**デフォルトのメッセージを使用**をクリックします。

4. **適用**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。

リモートコンソールのコンピューターロック設定を構成する

この機能により、リモートコンソールセッションが終了したり iLO へのネットワークリンクが失われると、OS がロックされるかユーザーがログアウトされます。この機能が有効になっているときにリモートコンソールウィンドウを開いた場合、ウィンドウを閉じるときに OS がロックされます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**セキュリティ**タブをクリックします。
2. 以下の**リモートコンソールコンピューターロック**設定から選択します。**Windows**、**カスタム**、および**無効**。
3. **カスタム**を選択した場合は、コンピューターのロックキーシーケンスを選択します。
4. 変更を保存するには、**適用**をクリックします。

リモートコンソールのコンピューターロックオプション

- **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するように iLO を構成します。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、サーバーに**コンピューターロック**ダイアログボックスが自動的に表示されます。
- **カスタム** - 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するように iLO を構成します。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 OS に自動的に送信されます。
- **無効**（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り、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 OS はロックされません。

リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

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	`	u

表は続く

TAB	'	a	v
BREAK	,	b	w
BACKSPACE	-	c	x
NUM PLUS	.	d	y
NUM MINUS	/	e	z

リモートコンソールの信頼設定の構成（.NET IRC）

.NET IRC は、Microsoft .NET Framework の一部である Microsoft ClickOnce を介して起動します。ClickOnce では、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なければなりません。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この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。

Hewlett Packard Enterprise では、信頼された SSL 証明書をインストールして、**IRC は iLO 内の信頼された証明書を要求します**設定を有効にすることをおすすめします。この構成では、.NET IRC は HTTPS 接続を使用することにより起動します。**IRC は iLO 内の信頼された証明書を要求します**設定が無効の場合、.NET IRC は SSL 以外の接続を使用することで起動し、.NET IRC が暗号化キーの交換を開始した後で SSL が使用されます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**セキュリティ**タブをクリックします。
2. **IRC は iLO 内の信頼された証明書を要求します**設定の有効と無効を切り替えるには、切り替えスイッチをクリックします。
3. 変更を保存するには、**適用**をクリックします。

ファームウェア検証

ファームウェア検証機能では、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インストールしたり、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。無効なファイルをダウンロードし、その種類と発生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、フラッシュファームウェア機能を使用すると選択できません。

サポートされる管理ツールがシステムリカバリイベントをリスンするように構成されている場合は、リカバリイベントをこのページから送信できます。

ファームウェア検証設定の構成

前提条件

- iLO の設定を構成する権限
- 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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **スキャン設定**アイコン ☼ をクリックします。
3. **バックグランドスキャンを有効**を有効または無効の状態に設定します。
4. **整合性障害のアクション**を選択します。
5. **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. **送信**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

- **バックグランドスキャンを有効** - 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。
- **整合性障害のアクション** - 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、**ログのみ**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、**ログおよび自動的に修復**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。

- **スキャン間隔（日数）** - バックグランドスキャン頻度（日数）を設定します。有効な値は 1～365 です。

ファームウェア検証スキャンの実行

前提条件

- iLO の設定を構成する権限
- 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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **スキャンを実行**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インストールしたり、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。

   詳しくは、iLO のユーザーガイドを参照してください。

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。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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

管理ページに移動し、**ファームウェア検証**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。

ファームウェア名

インストールされているファームウェアの名前。

ファームウェアバージョン

ファームウェアバージョン。

ヘルス

ファームウェアのヘルスステータス。

状態

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。

- **有効** - ファームウェアは検証されており、有効です。
- **スキャニング** - 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。
- **フラッシング**—ファームウェアアップデートが進行中です。
- **障害/オフライン** - ファームウェアは検証できず、修復されませんでした。

リカバリセットバージョン

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、**未装着**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。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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

管理ページに移動し、**ファームウェア検証**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、**隔離**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`（検疫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

隔離セクションには、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。

名前

無効なファームウェアファイルの名前。

作成日

無効なファイルの作成日。

サイズ

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。

- **名前**-隔離されたファイルの名前。
- **作成日**-無効なファイルの作成日。

- **ファイル名**-iLO レポジトリによって使用される名前。
- **イメージの URI**-隔離されたファイルの場所。
- **サイズ**-無効なファイルサイズ。
- **デバイス クラス**-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 エリア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。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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **隔離**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。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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- リカバリセット権限

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **隔離**セクションで、削除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. **はい、削除**をクリックします。

フルシステムリカバリの開始

別の管理ツールを起動してフルシステムリカバリを開始するリカバリイベントを、iLO を使用して生成することができます。リカバリは、サーバーオペレーティングシステムのイメージの再構築に続き、システムリカバリセットのインストールを含めます。

△ **注意:** サーバーのイメージの再構築によって、既存のデータが失われる場合があります。

前提条件

- iLO の設定を構成する権限
- 仮想メディア権限
- 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、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- システムリカバリセットが iLO レポジトリに存在する。
- サポートされる管理ツール（iLO Amplifier Pack 1.15 以降など）がサーバーを管理するように構成されている。

手順

1. リカバリプロセスに、サーバーのシャットダウンが必要なコンポーネントが含まれている場合は、サーバーをシャットダウンします。
2. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
3. **リカバリイベントを送信**をクリックします。
4. **リカバリイベントを送信**ペインで、**はい、リカバリイベントを作成します**チェックボックスを選択して、**リカバリイベントを送信**をクリックします。

   リカバリイベントは、リカバリイベントをリスンするように構成されている管理ツールに送信されます。

   イベントが正常に送信されると、以下の情報イベントが IML に記録されます。

   `Firmware recovery is requested by Administrator.`（管理者がファームウェアリカバリを要求しています。）

フラッシュファームウェア機能を使用した iLO またはサーバーのファームウェアのアップデート

iLO Web インターフェイスを使用して、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。署名済みファイルが必要です。

前提条件

- iLO レポジトリにファームウェアをフラッシュし、コンポーネントを格納するには、iLO 設定の構成権限が必要です。
- 正常なファームウェアアップデート後、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- **リカバリセットをアップデート**機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。
- iLO 5 バージョン 2.10 以降に更新する場合、iLO 5 バージョン 1.40 以降がインストールされていること。

手順

1. サーバーファームウェアまたは iLO ファームウェアのファイルを入手します。
2. イノベーションエンジン（IE）またはサーバープラットフォームサービス（SPS）のファームウェアをアップデートする場合は、サーバーの電源を切ってから 30 秒待ちます。

3. 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、**ファームウェアアップデート**クリックします。

   ファームウェアアップデートオプションが表示されない場合は、iLO Web インターフェイスの右上隅にある省略記号アイコンをクリックし、**ファームウェアアップデート**をクリックします。

4. **ローカルファイル**または**リモートファイル**オプションを選択します。

5. 選択したオプションに応じて、以下のいずれかを実行します。

   - 使用するブラウザーに応じて、**ローカルファイル**ボックスで**参照**または**ファイルを選択**をクリックして、ファームウェアコンポーネントの場所を指定します。
   - **リモートファイル 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。

6. （オプション）コンポーネントのコピーを iLO レポジトリに保存するには、同様に、**iLO レポジトリに保存**チェックボックスを選択します。

7. （オプション）手順 **5** で選択したコンポーネントのバージョンがシステムリカバリセットに存在する場合は、**リカバリセットをアップデート**チェックボックスを選択して、選択したコンポーネントに既存のコンポーネントを置き換えます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   システムリカバリセットが存在しない場合やこの操作に必要な権限が与えられていない場合、このオプションは表示されません。

   このオプションを選択すると、システムリカバリセットが iLO レポジトリに保存されるため、**同様に、iLO レポジトリに保存**オプションが自動的に選択されます。

8. TPM または TM がサーバーにインストールされているサーバーでは、TPM または TM の情報を保存するソフトウェアを一時停止またはバックアップしてから、**TPM の上書きを確認してください**チェックボックスを選択します。

   ドライブ暗号化ソフトウェアは、TPM または TM の情報を保存するソフトウェアの例です。

   △ **注意:** ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。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。

9. **フラッシュ**をクリックして、アップデートプロセスを開始します。

   サーバーの構成に応じて、iLO によって次のことが通知されます。

   - 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。
   - 一部のサーバーファームウェアタイプではサーバーの再起動が必要になりますが、サーバーは自動的には再起動しません。

10. **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信、検証、フラッシュします。

    iLO ファームウェアをアップデートすると、iLO が再起動し、ブラウザー接続が終了します。接続が再確立されるまでに、数分かかることがあります。

11. iLO ファームウェアのアップデートのみ：新しいファームウェアを使用するには、ブラウザーのキャッシュをクリアし、iLO にログインします。

12. サーバーファームウェアのアップデートのみ : ファームウェアのタイプによって、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やサーバーの再起動が必要になる場合は、適切なアクションを実行します。
13. （オプション）新しいファームウェアがアクティブであることを確認するには、**インストールされたファームウェア**ページでファームウェア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。

サポートされるファームウェアタイプ

サーバーのプラットフォームに応じて、さまざまなファームウェアアップデートのタイプがサポートされます。一般的な例には、以下のものがあります。

- iLO
- システム ROM/BIOS
- シャーシ
- パワーマネ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）
- バックプレーン
- イノベーションエンジン（IE）
- サーバープラットフォームサービス（SPS）
- 言語パック

一部のファームウェアタイプは、組み合わせたアップデートとして提供されます。以下に例を示します。

- SAS プログラマブルロジックデバイスのアップデートは、多くの場合、SAS コントローラーのファームウェアアップデートとの組み合わせになります。
- Intelligent Platform Abstraction Data のファームウェアは、多くの場合、システム ROM/BIOS のアップデートとの組み合わせになります。

ファームウェアアップデートを有効にするための要件

アップデートを有効にするには、ファームウェアタイプに応じて、追加のアクションが必要になる場合があります。

- iLO のファームウェアまたは言語パック - これらの種類のファームウェアは、自動起動される iLO リセットの後に有効になります。
- 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（電力管理）および Edgeline シャーシコントローラーファームウェア - ただちに有効になります。
- 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。
- パワーマネジメントコントローラーおよび 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 ファームウェアバージョンは、次のサーバー再起動後に iLO Web インターフェイスに表示されます。

- イノベーションエンジン（IE）およびサーバープラットフォームサービス（SPS） - これらのファームウェアタイプでは、インストールする前にサーバーの電源を切る必要があります。サーバーに電源を入れると、変更が有効になります。

iLO ファームウェアイメージファイルの入手

iLO ファームウェアイメージファイルをダウンロードし、それを使用してグループ内の 1 つのサーバーまたは複数のサーバーをアップデートできます。

ファームウェア書き換えアップデート機能または**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 ファームウェアをアップデートするには、iLO オンラインフラッシュコンポーネントからの BIN ファイルが必要です。

手順

1. 次の Web サイトに移動します。**https://www.hpe.com/support/hpesc**
2. 画面の指示に従って iLO オンラインフラッシュコンポーネントファイルを探し、ダウンロードします。

   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、**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。
     - `#./<firmware_file_name>.scexe –unpack=/tmp/`
     - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`

   iLO ファームウェアイメージファイルの名前は、`iLO 5_<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。

サポートされるサーバーファームウェアイメージファイルの入手

手順

1. 次の Web サイトに移動します。**https://www.hpe.com/support/hpesc**
2. 画面の指示に従ってオンラインフラッシュコンポーネントファイルを探し、ダウンロードします。
3. Windows コンポーネントをダウンロードした場合：

   a. ダウンロードしたファイルをダブルクリックし、**解凍**ボタンをクリックします。

   b. 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。
4. Linux コンポーネントをダウンロードした場合：

   a. Linux コンポーネントの場合は、ファイルの形式に応じて、次のコマンドのいずれかを入力します。

- `#./<firmware_file_name>.scexe –unpack=/tmp/`
- `#rpm2cpio <firmware_file_name>.rpm | cpio -id`

b. （オプション）イノベーションエンジンまたはサーバープラットフォームサービス（SPS）のファームウェアコンポーネントを使用する場合は、`<firmware_file_name>.zip` ファイルを見つけて、バイナリファイルを抽出します。

サーバーファームウェアのファイルタイプの詳細

- システム ROM を更新する場合、署名付きのイメージまたは署名付きの ROMPAQ イメージを使用する必要があります。
  - **署名付きイメージの例**：

    http://<server.example.com:8080>/<wwwroot>/P79_1.00_10_25_2013.signed.flash
  - **署名付き ROMPAQ イメージの例**：

    http://<server.example.com>/<wwwroot>/CPQPJ0612.A48
- パワーマネジメントコントローラー、シャーシファームウェア、および NVMe バックプレーンファイルは、拡張子 `.hex` を使用します。たとえば、ファイル名は `ABCD5S95.hex` のようになります。
- システムプログラマブルロジックデバイス（CPLD）のファームウェアファイルは、ファイル拡張子 `.vme` を使用します。
- イノベーションエンジン（IE）およびサーバープラットフォームサービス（SPS）ファームウェアファイルは、ファイル拡張子 `.bin` を使用します。
- 言語パックファイルは拡張子 `.lpk` を使用します。

サポートと他のリソース

Hewlett Packard Enterprise サポートへのアクセス

- ライブアシスタンスについては、Contact Hewlett Packard Enterprise Worldwide の Web サイトにアクセスします。

  https://www.hpe.com/info/assistance

- ドキュメントとサポートサービスにアクセスするには、Hewlett Packard Enterprise サポートセンターの Web サイトにアクセスします。

  https://www.hpe.com/support/hpesc

ご用意いただく情報

- テクニカルサポートの登録番号（該当する場合）
- 製品名、モデルまたはバージョン、シリアル番号
- オペレーティングシステム名およびバージョン
- ファームウェアバージョン
- エラーメッセージ
- 製品固有のレポートおよびログ
- アドオン製品またはコンポーネント
- 他社製品またはコンポーネント

アップデートへのアクセス

- 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるソフトウェアアップデート方法を確認してください。
- 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

  Hewlett Packard Enterprise サポートセンター

  https://www.hpe.com/support/hpesc

  Hewlett Packard Enterprise サポートセンター：ソフトウェアのダウンロード

  https://www.hpe.com/support/downloads

  Software Depot

  https://www.hpe.com/support/softwaredepot

- eNewsletters およびアラートをサブスクライブするには、以下にアクセスします。

  https://www.hpe.com/support/e-updates-ja

- お客様の資格を表示、アップデート、または契約や保証をお客様のプロファイルにリンクするには、Hewlett Packard Enterprise サポートセンターの **More Information on Access to Support Materials** ページに移動します。

https://www.hpe.com/support/AccessToSupportMaterials

重要: 一部のアップデートにアクセスするには、Hewlett Packard Enterprise サポートセンターからアクセスするときに製品資格が必要になる場合があります。関連する資格を使って HPE パスポートをセットアップしておく必要があります。

リモートサポート（HPE 通報サービス）

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。リモートサポートは、インテリジェントなイベント診断を提供し、ハードウェアイベントを Hewlett Packard Enterprise に安全な方法で自動通知します。これにより、ご使用の製品のサービスレベルに基づいて、迅速かつ正確な解決が行われます。ご使用のデバイスをリモートサポートに登録することを強くおすすめします。

ご使用の製品にリモートサポートの追加詳細情報が含まれる場合は、検索を使用してその情報を見つけてください。

リモートサポートおよびプロアクティブケア情報

HPE 通報サービス

http://www.hpe.com/jp/hpalert

HPE プロアクティブケアサービス

http://www.hpe.com/services/proactivecare-ja

HPE データセンターケアサービス

http://www.hpe.com/services/datacentercare

HPE プロアクティブケアサービス：サポートされている製品のリスト

http://www.hpe.com/services/proactivecaresupportedproducts

HPE プロアクティブケアアドバンストサービス：サポートされている製品のリスト

http://www.hpe.com/services/proactivecareadvancedsupportedproducts

保証情報

ご使用の製品の保証情報を確認するには、以下のリンクを参照してください。

HPE ProLiant と IA-32 サーバーおよびオプション

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise および Cloudline サーバー

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE ストレージ製品

https://www.hpe.com/support/Storage-Warranties

HPE ネットワーク製品

https://www.hpe.com/support/Networking-Warranties

規定に関する情報

安全、環境、および規定に関する情報については、Hewlett Packard Enterprise サポートセンターからサーバー、ストレージ、電源、ネットワーク、およびラック製品の安全と準拠に関する情報を参照してください。

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

規定に関する追加情報

Hewlett Packard Enterprise は、REACH（欧州議会と欧州理事会の規則 EC No 1907/2006）のような法的な要求事項に準拠する必要に応じて、弊社製品の含有化学物質に関する情報をお客様に提供することに全力で取り組んでいます。この製品の含有化学物質情報レポートは、次を参照してください。

https://www.hpe.com/info/reach

RoHS、REACH を含む Hewlett Packard Enterprise 製品の環境と安全に関する情報と準拠のデータについては、次を参照してください。

https://www.hpe.com/info/ecodata

社内プログラム、製品のリサイクル、エネルギー効率などの Hewlett Packard Enterprise の環境に関する情報については、次を参照してください。

https://www.hpe.com/info/environment

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterprise では、お客様により良いドキュメントを提供するように努めています。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、ドキュメントフィードバック担当（**docsfeedback@hpe.com**）へお寄せください。このメールには、ドキュメントのタイトル、部品番号、版数、およびドキュメントの表紙に記載されている刊行日をご記載ください。オンラインヘルプの内容に関するフィードバックの場合は、製品名、製品のバージョン、ヘルプの版数、およびご利用規約ページに記載されている刊行日もお知らせください。

アクセス設定クイックリファレンス

表 3: デフォルトのアクセス設定は、iLO アクセス設定とそのデフォルト値のクイックリファレンスを提供します。これらの設定について詳しくは、**iLO アクセス設定**を参照してください。

表 3: デフォルトのアクセス設定

オプション	デフォルト値	説明
サーバー名	なし	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。
サーバーの FQDN/IP アドレス	なし	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。
遅延前の認証の失敗時	1 回の失敗では遅延は発生しない	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。
認証の失敗時の遅延時間	10 秒	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。
認証失敗ログ	有効 - 3 回目の失敗時	認証失敗のログ記録条件を構成できます。すべてのログインタイプがサポートされ、それぞれのログインタイプは個別に動作します。
最小パスワード長	8	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。
パスワードの複雑さ	無効	ユーザーアカウントおよび iLO 連携グループ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。
匿名データ	有効	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。
IPMI/DCMI over LAN	無効	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。
IPMI/DCMI over LAN ポート	UDP 623	IPMI/DCMI ポート番号を設定します。
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有効または無効にすることができます。

表は続く

オプション	デフォルト値	説明
リモートコンソールポート	TCP 17990	リモートコンソールポートを設定します。
セキュアシェル（SSH）	有効	SSH 機能を有効または無効にすることができます。
セキュアシェル（SSH）ポート	TCP 22	SSH ポートを設定します。
SNMP	有効	iLO が外部の SNMP 要求に応答するかどうかを指定します。
SNMP ポート	UDP 161	SNMP ポートを設定します。
SNMP トラップポート	UDP 162	SNMP トラップポートを設定します。
仮想メディア	有効	iLO 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。
仮想メディアポート	TCP 17988	iLO が着信ローカル仮想メディア接続をリスンするために使用するポート。
仮想シリアルポートログ	無効	仮想シリアルポートの記録を有効または無効にします。
Web サーバー	有効	iLO Web サーバー経由のアクセスを有効または無効にすることができます。
Web サーバー非 SSL ポート	TCP 80	HTTP ポートを設定します。
Web サーバー SSL ポート	TCP 443	HTTPS ポートを設定します。
アイドル接続タイムアウト（分）	30	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。
iLO 機能	有効	iLO 機能が利用可能かどうかを制御します。
iLO RIBCL インターフェイス	有効	iLO との通信に RIBCL コマンドを使用できるかどうかを指定します。
iLO ROM ベースセットアップユーティリティ	有効	UEFI システムユーティリティの iLO 構成オプションを有効または無効にします。
iLO Web インターフェイス	有効	iLO と通信するために iLO Web インターフェイスを使用できるかどうかを指定します。
リモートコンソールサムネイル	有効	iLO でリモートコンソールのサムネイルイメージの表示を有効または無効にします。

表は続く

オプション	デフォルト値	説明
ホスト認証が必要	有効	管理プロセッサーにアクセスするホストベースの構成ユーティリティを使用するために、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、管理者または root のホストコンテキストで、ホスト OS のコマンドラインから実行します。
iLO RBSU へのログイン要求	無効	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、ユーザー認証情報が必要かどうかを決定します。
シリアルコマンドラインインターフェイス速度	9600	CLI 機能のシリアルポートの速度を変更できます。
シリアルコマンドラインインターフェイスステータス	有効-認証が必要	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。
POST 中に iLO IP を表示	有効	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。
外部モニターにサーバーヘルスを表示	有効	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。
VGA ポート検出オーバーライド	有効	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。
仮想 NIC	有効	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。
ダウングレードポリシー	ダウングレードの許可	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。

詳しくは

iLO アクセス設定の構成
iLO 5 の推奨されるセキュリティ設定

iLO 5 の推奨されるセキュリティ設定

iLO 5 のセキュリティ関連の機能へのパスと推奨設定については、次の表を参照してください。実装するセキュリティレベルを決定するには、組織は、iLO のセキュリティ設定と、システムの使用を妨げる不必要に限定的なセキュリティ設定の導入とのバランスを見い出す必要があります。ご使用の環境のデータを保護するニーズと、許可されたユーザーがそのデータに容易にアクセスするニーズを比較検討してください。使用可能な推奨されるセキュリティ設定をすべて有効にするのは、組織にとって最適な方法ではない場合があります。

表 4: iLO 5 設定

特長または機能	iLO の Web インターフェイスページ	設定	推奨される設定値
TPM または TM のステータス	**情報 - iLO の概要**	Trusted Platform Module。トラステッドプラットフォームモジュール	読み取り専用
		モジュールタイプ	読み取り専用（TPM または TM が存在する場合のみ表示）
ローカルユーザーアカウントの制御	**管理 - ユーザー管理**	ローカルユーザーの追加、編集、および削除	最小限のアクセスのセキュリティ原則をサポートする個々のユーザー権限の設定の範囲で、最大 12 のローカルアカウント
ディレクトリグループアカウントの制御	**ディレクトリグループ**	ディレクトリグループの追加、編集、および削除	最大 6 つのディレクトリグループ、Kerberos 認証とスキーマフリーディレクトリの統合で使用されます。
iLO サーバー設定	**セキュリティ - アクセス設定**	サーバー名	この値は空白のままにして、ホスト OS で割り当てられるようにします。
		サーバーの FQDN/IP アドレス	この値は空白のままにして、ホスト OS で割り当てられるようにします。
iLO アカウントサービス設定	**セキュリティ - アクセス設定**	遅延前の認証の失敗時	1 回の失敗では遅延は発生しない
		認証の失敗時の遅延時間	10 秒
		認証失敗ログ	有効-毎回失敗時
		最小パスワード長	8
		パスワードの複雑さ	有効

表は続く

特長または機能	iLO の Web インターフェイスページ	設定	推奨される設定値
iLO ネットワーク設定	**セキュリティ - アクセス設定**	匿名データ	有効
		IPMI/DCMI over LAN	無効（ポート設定を含む）
		リモートコンソール	有効（ポート設定を含む）
		セキュアシェル（SSH）	有効（ポート設定を含む）
		SNMP	無効
		仮想メディア	有効（ポート設定を含む）
		仮想シリアルポートログ	有効
		Web サーバー	有効（非 SSL および SSL のポート設定が必要）[1]
iLO 設定	**セキュリティ - アクセス設定**	アイドル接続タイムアウト（分）	30 分間
		iLO 機能	有効
		iLO RIBCL インターフェイス	有効（ Hewlett Packard Enterprise では iLO RESTful API を使用することをお勧めします ）
		iLO ROM ベースセットアップユーティリティ	有効
		iLO Web インターフェイス	有効
		リモートコンソールサムネイル	無効
		ホスト認証が必要	有効
		iLO RBSU へのログイン要求	有効
		シリアルコマンドラインインターフェイスステータス	有効 - 認証は必要（インターフェイス速度の設定が必要）

表は続く

特長または機能	iLO の Web インターフェイスページ	設定	推奨される設定値
		POST 中に iLO IP を表示	有効
		外部モニターにサーバーヘルスを表示	有効
		VGA ポート検出オーバーライド	有効
		仮想 NIC	無効
iLO サービスポート	**セキュリティ - iLO サービスポート**	iLO サービスポート	有効
		USB フラッシュドライブ	無効
		認証が必要	有効
		USB Ethernet アダプタ	無効
セキュアシェルキーの設定	**セキュリティ - セキュアシェルキー**	キーは 2048 ビットの DSA または RSA（または CNSA セキュリティ状態では ECDSA 384 ビットキー）である必要があります。	SSH キーを使用すると、単純なパスワード認証よりもセキュリティが向上します。
証明書マッピング	**セキュリティ - 証明書マッピング**	各ローカルユーザーアカウントには関連する証明書が必要です。	証明書とともにスマートカードを使用すると、単純なパスワード認証よりもセキュリティが向上します。
スマートカード	**セキュリティ - CAC/ Smartcard**	CAC Smartcard 認証	有効（iLO Advanced のライセンスが必要）
		CAC 厳密モード	（オプション）有効
		ディレクトリユーザー証明書名マッピング	ディレクトリ統合を使用する場合、ユーザー証明書に応じて正しいオプションを選択します。
		信頼できる CA 証明書および失効リストのインポート	失効リストとともに、少なくとも 1 つの信頼できる CA 証明書をインストールする必要があります。

表は続く

特長または機能	iLO の Web インターフェイスページ	設定	推奨される設定値
		OCSP 設定	承認された OCSP プロバイダーの URL を入力して、認証のためにユーザー証明書を確認します。
SSL 証明書管理	**セキュリティ - SSL 証明書情報**	証明書のカスタマイズ	iLO ごとに信頼できる SSL 証明書をインストールします。デフォルトの自己署名証明書は安全ではありません。
ディレクトリベースの認証	**セキュリティ - ディレクトリ**	LDAP ディレクトリ認証	HPE 拡張スキーマ（Active Directory が必要）を選択するか、ディレクトリデフォルトスキーマを使用します。この機能には、iLO の外部でいくつかの構成手順が必要です。
		Local User Accounts	環境に応じて、有効または無効。
		Kerberos 認証	有効（レルム、サーバーアドレス、サーバーポート、およびキータブファイルの設定も必要）。この機能には、iLO の外部でいくつかの構成手順が必要です。
暗号化	**セキュリティ - 暗号化設定**	セキュリティ状態	高セキュリティ（最小）
HPE SSO	**セキュリティ - シングルサインオンの設定**	SSO 信頼モード	認証情報による信頼[2]（ユーザーの役割ごとに SSO 権限を選択できます）
ログインセキュリティバナー	**セキュリティ - ログインセキュリティバナー設定**	ログインセキュリティバナーを有効	有効（セキュリティメッセージの設定が必要）
ファームウェア検証	**管理 - ファームウェア検証**	スキャン設定	バックグランドスキャンを有効（整合性エラーアクションの設定が必要）

[1] 無効の場合、RIBCL、iLO RESTful API、リモートコンソール、iLO 連携、および iLO Web インターフェイスに対するアクセスは除外されます。

[2] 一部の HPE アプリケーションでは、iLO 5 のセキュリティ状態が「高セキュリティ」以上に設定されている場合は、SSO が正常に使用されない場合があります。詳しくは、アプリケーションのドキュメントを参照してください。