Hewlett Packard Enterprise

HPE Gen10およびGen10 Plusセキュリティリファレンスガイド

部品番号: 30-2905B658-001-ja-JP
発行: 2021年10月
版数: 1

HPE Gen10およびGen10 Plusセキュリティリファレンスガイド

摘要
このドキュメントでは、Hewlett Packard Enterprise Gen10およびGen10 Plusサーバーおよびコンピューティングモジュールによってサポートされているセキュリティ機能について説明します。このドキュメントは、HPEサーバーおよびコンピューティングモジュールの安全な構成と運用を行う担当者を対象としています。

部品番号: 30-2905B658-001-ja-JP
発行: 2021年10月
版数: 1

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。

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

AMDは、Advanced Micro Devices, Incの商標です。

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。

改訂履歴

部品番号	発行日	版数	変更の概要
30-2905B658-001-ja-JP	2021年10月	1	新しいドキュメント構造と部品番号 Gen10 Plus情報を追加しました
882428-195	2019年2月		新しいiLO機能に応じてアップデートしました

目次

HPEGen10およびGen10Plusプラットフォームのセキュリティ機能

Hewlett Packard Enterpriseのセキュリティ機能は、Gen10およびGen10 Plusプラットフォームと関連ハードウェア環境のハードウェアとファームウェアのセキュリティを継続的に強化することにより、セキュリティの課題に対応するように設計されています。セキュリティ機能により、セキュリティのチェーン内のすべてのリンクで効果的な保護を提供します。ProLiant、BladeSystem c-Class、Apollo、およびSynergyなどのHPE Gen10およびGen10 Plusプラットフォーム全体に、強化されたセキュリティ機能が含まれています。

ライセンスされた機能

iLO（Standard）は、追加コストまたはライセンスなしでHPEサーバーに事前設定されています。セキュリティと生産性を向上させる一部の機能には、iLO Advancedライセンスが必要です。iLO Webインターフェイス、コマンドライン、およびスクリプトツールを介して管理できる機能に加えて、iLO Advancedライセンスにより、サーバー構成ロックやSmartアレイセキュア暗号化などの機能が有効になります。詳しくは、iLOライセンスガイド（https://www.hpe.com/support/iLOLicenseGuide-en）を参照してください。

サプライチェーンのセキュリティ

Hewlett Packard Enterpriseサーバーのセキュリティはサプライチェーンから始まり、製品ライフサイクル全体に及びます。

詳しくは

HPE Trusted Supply Chain
サーバー構成ロック
シャーシ侵入検知デバイス
プラットフォーム証明書
HPEプラットフォーム証明書検証ツール

HPE Trusted Supply Chain

HPE Trusted Supply Chainは、安全な施設において高いセキュリティ標準で構築されたサポートされているサーバーによって、サイバー攻撃者に対する最初の防衛線を提供します。HPE Trusted Supply Chainは、セキュリティ、プロセス、および人員を組み合わせて、サーバーが展開される前であっても、最も機密性の高いアプリケーションやデータを保護します。

HPE Trusted Supply Chainサーバーには、以下の特性があります。

米国が生産国

準拠要件と共に、最も厳しい生産国である米国の安全なHewlett Packard Enterprise施設で構築された各サーバーは、悪意のあるマイクロコードや偽造部品がないことが検査および検証され、ライフサイクル全体を通じてサイバーエクスプロイトからサーバーを保護します。

強化されたセキュリティが組み込まれている

HPE Trusted Supply Chainは、比類のないサプライチェーンの可視性と標準への準拠によって、厳選したHPE製品に組み込まれた保護を強化し、現在および新たに発生するサイバー脅威に対して包括的な軽減プランを提供します。

信頼できる認証

HPE Trusted Supply Chainは、最も厳しい調達、検査、およびトレーサビリティの標準に準拠した製品製造プロセスを管理する、製品ビルドを担当するHPE従業員による保護を提供します。

一意のラベリング

HPE Trusted Supply Chain製品には、HPE ProLiant DL380Tなど、サーバーモデル名にTが含まれます。Trusted Supply Chainステッカーが製品ハードウェアに貼られます。

詳しくは、HPE Trusted Supply Chain**プレスリリース**をご覧ください。

詳しくは

デフォルトのHPE Trusted Supply Chainサーバーの構成

デフォルトのHPE Trusted Supply Chainサーバーの構成

HPE Trusted Supply Chainサーバーは、次のデフォルト構成で出荷されます。

iLOセキュリティ状態 高セキュリティ

「高セキュリティ」セキュリティ状態を使用するように、iLOを構成すると、サイバー攻撃者の攻撃対象領域が減少し、侵害されたコードやマルウェアをサーバーファームウェアに入り込ませることがさらに困難になります。このセキュリティ状態はホストをロックダウンし、ユーザーがサーバーにログインできる前に暗号化による特定の認証を必要とします。

UEFIセキュアブート機能：有効

Hewlett Packard Enterpriseに工場でOSをロードするように求めるお客様の場合、UEFIセキュアブートを有効にすると、Silicon Root of TrustがOSに接続されます。業界で認められた機能であるUEFIファームウェアをブートローダーに取り付けることにより、正規の認証済みOSが確実に初期化されます。

ウイルス対策ソフトウェアは実際にOSで実行されますが、OSが完全に実行されるまで、ハッカーや侵入を検出できません。一部の巧妙な悪意のあるアクターは、ウイルス対策ツールが起動する機会を得る前にOSの侵害を試みます。UEFIセキュアブート機能は、このシナリオに対する保護を提供します。

お客様が自分でOSをロードすることを選択した場合は、HPE Trusted Supply Chainサーバーがエンドユーザーの場所に納入されたときに、この機能を構成できます。

HPEサーバー構成ロック：有効

この機能は、サポートされているHPE Trusted Supply Chainサーバーファームウェア、ハードウェアコンポーネント、およびオプションの暗号化測定値またはイメージを取得します。それはサーバー構成のデジタルフィンガープリントを作成します。いずれかのファームウェア、ハードウェア、またはオプションが変更されている場合、起動時にアラートが表示されます。

工場でこの機能を有効にすると、どれだけわずかなものでも、サーバー構成に対するすべての改ざんや侵害を本質的に防ぎます。この機能は、Hewlett Packard Enterpriseによって作成されたパスワードを使用して、工場でサーバー構成をロックダウンします。パスワードはお客様に安全に送信され、お客様はそれが到着したときにサーバーのロックを解除します。

リセラーやパートナーなどを通じて、追加の構成手順を実行する必要があるお客様の場合は、パスワードを使用して、ロックを解除し、サーバーをエンドユーザーの場所に出荷する前に再ロックすることができます。

HPEシャーシ侵入検知デバイス：有効

このメカニズムは、HPE Trusted Supply Chainサーバーを物理的な侵入から保護します。サーバー構成ロックによる保護を補完および強化するシャーシ侵入検知デバイスは、サーバーシャーシの上部が取り外された場合にアラートを登録します。サーバーの電源がオフの場合でも、iLOファームウェアにイベントを記録します。サイバー攻撃者や無許可の者がサーバーシャーシを開いた場合、お客様は誰かがサーバーを改ざんした可能性があることがわかります。

詳しくは

Silicon Root of Trust
サーバー構成ロック
シャーシ侵入検知デバイス
セキュアブート
iLOセキュリティ状態

サーバー構成ロック

サーバー構成ロックは、サーバー構成の改ざんや侵害からサーバーを保護します。この機能は、サーバーの輸送中に有効にすることも、常に使用して構成の変更を監視することもできます。

HPE Trusted Supply Chainサーバーは、この機能が有効になっている状態で出荷され、サーバーは輸送中状態に設定されています。HPEはサーバー構成ロックパスワードを作成し、それが安全にお客様に送信されます。初回起動時に、お客様はパスワードを入力して、輸送中ステータスを無効にします。現在のところ、機能構成を無効化または変更できます。

サーバー構成ロックは、サーバー構成のデジタルフィンガープリントを作成します。デジタルフィンガープリントは、サーバーTPM 2.0（サポートされている場合）またはサーバーの不揮発性メモリに安全に保存されたログファイルです。

サーバー構成ロックはサーバーの次を監視します。

- DIMMの変更
- CPUの変更
- PCIeデバイスの変更
- セキュリティ構成の変更
- システムのファームウェアリビジョン
- サーバー構成ロックのパスワード認証の失敗

POST中に構成の変更が検出された場合、管理者はサーバー構成ロックパスワードを入力して、問題を確認し、起動プロセスを続行する必要があります。構成の変更は、インテグレーテッドマネジメントログ（IML）に記録されます。検出された問題の数は、UEFIシステムユーティリティのサーバー構成ロック検出ログで取得できます。

サーバー構成ロックは、UEFIシステムユーティリティで、またはiLO RESTful APIを使用して構成できます。

重要:
サーバー構成ロックを使用する場合、パスワードを安全に記録してください。設計上、このセキュリティ機能では、パスワードを紛失したり忘れたりした場合に、パスワードのバイパスまたはリセットができません。

輸送中ステータスを無効にする手順を含む構成手順については、次のWebサイトのHPEProLiant Gen10、Gen10 Plusサーバー、およびHPE Synergy用サーバー構成ロックユーザーガイドを参照してください。（https://www.hpe.com/info/server-config-lock-UG-en）を確認してください。

詳しくは

デフォルトのHPE Trusted Supply Chainサーバーの構成

シャーシ侵入検知デバイス

サポートされているGen10およびGen10 Plus製品は、シャーシ侵入検知デバイスで利用できます。シャーシ侵入検知デバイスは、シャーシへの物理的な侵入を検知します。iLOは、アクセスパネルが開いたり閉じたりしたときにイベントをログに記録します。シャーシ侵入監視とiLOのレポートは、サーバー電源の状態に関係なく、サーバーが接続されている限り行われます。

さまざまなアラートメカニズム（リモートSysLog、SNMP、またはアラートメール）を構成して、シャーシ侵入イベントが発生したときに通知させることができます。

この機能に対するサーバーのサポートを確認するには、次のWebサイトでサーバーのQuickSpecsドキュメントを確認してください。https://www.hpe.com/info/qs。

プラットフォーム証明書

サポートされているHewlett Packard Enterpriseサーバーで、HPE iLOは**Trusted Computing Group**（TCG）準拠のプラットフォーム証明書によってプロビジョニングできます。プラットフォーム証明書は、ハードウェアシャーシまたは構成の署名付きマニフェストとして機能する属性証明書です。プラットフォーム証明書は、HPEの注文に製品番号（SKU）P42104-B21を含めると作成されます。

プラットフォーム証明書は、サプライチェーンの改ざんを検出するために使用されます。お客様がサーバーを受け取ったら、プラットフォーム証明書検証ツール（PCVT）を使用して、サーバーの状態をプラットフォーム証明書と比較できます。

iLOでは、証明書をアップデートまたは削除することはできません。証明書は、次のiLO RESTful API GETコマンドを使用して表示できます。

```
/redfish/v1/Managers/1/SecurityService/PlatformCert/Certificates/1
```

詳しくは

高度なBIOSおよびプラットフォームセキュリティオプション
HPEプラットフォーム証明書検証ツール

HPEプラットフォーム証明書検証ツール

Trusted Computing Group（TCG）準拠のプラットフォーム証明書でプロビジョニングされたサーバーでは、構成を検証するためのHPEプラットフォーム証明書検証ツール（PCVT）を使用できます。

PCVTを実行すると、サーバーの状態をプラットフォーム証明書に保存されている情報と個別に比較できます。

- コンポーネントの測定値が参照値と一致する場合、この結果は、サーバーがHewlett Packard Enterpriseの工場を出発してから構成が変更されていないことを示しています。
- 測定値が参照値と一致しない場合、この結果は、サーバーがHPEの工場を出発してから構成が変更されたことを示しています。変更が検出された場合、その変更は予想され承認されているかどうか、またはサプライチェーンの改ざんが行われたかどうかを判断するための調査が必要です。

次のWebサイトで、HPE PCVTとHPEプラットフォーム証明書検証ツールユーザーガイドをダウンロードできます。https://github.com/HewlettPackard/PCVT。

詳しくは

プラットフォーム証明書

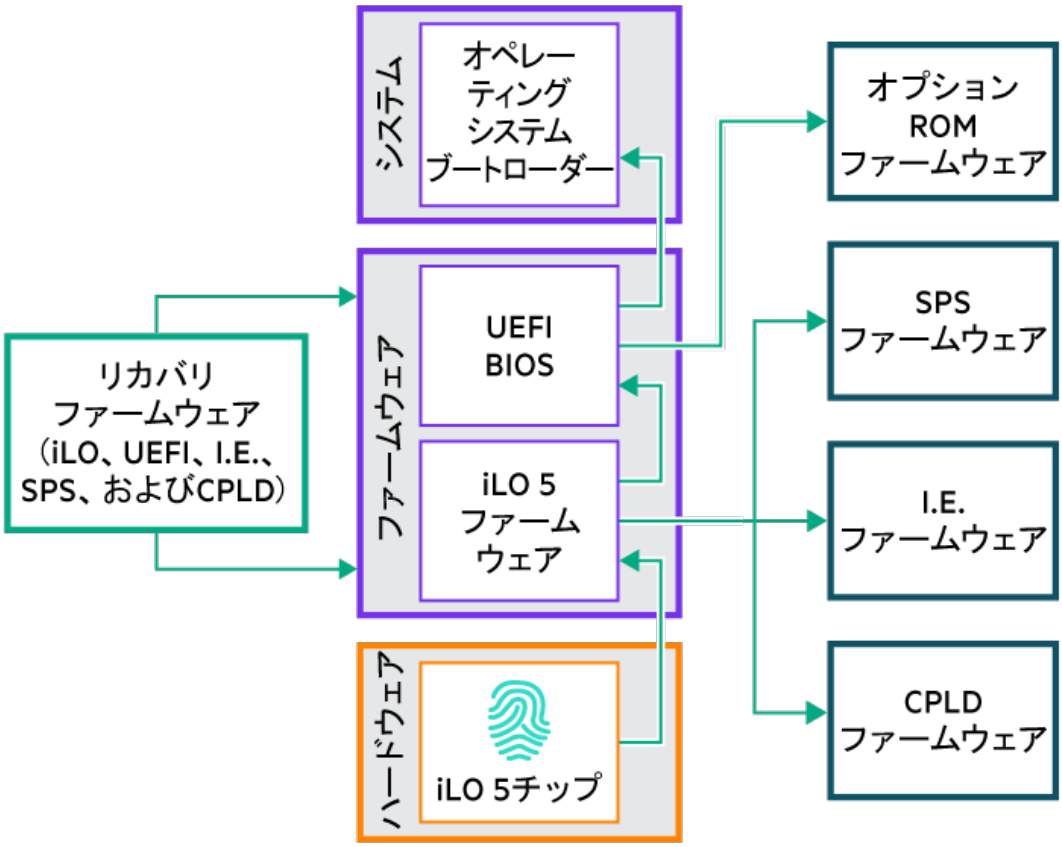
ゼロトラストセキュリティ

ゼロトラスト環境では、ハードウェア、ファームウェア、ハイパーバイザー、OS、およびアプリケーションを保護するために、サーバーのライフサイクル全体を通じてセキュリティが監視されます。

詳しくは

Silicon Root of Trust
サーバーID
Trusted Platform Module
不正アクセスの防止
永続的なサービス拒否攻撃からの保護
システムROMおよびiLOファームウェアのiLOファイアウォール
iLOとサーバーブレードまたはコンピューティングモジュール間の通信

Silicon Root of Trust



iLO 5チップは、Silicon Root of Trustとして機能します。Silicon Root of Trustにより、サーバー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ファームウェアのデジタルフィンガープリントが工場でiLO 5チップに埋め込まれます。起動時に、iLO 5チップはiLOファームウェアの整合性を検証し、実行が許可されているかどうかを判断します。この判断は、iLOファームウェアがデジタルフィンガープリントと一致しているかどうかに基づきます。iLOファームウェアが検証に失敗すると、システムは自動的にシステムリカバリセットからiLOファームウェアを復元します。

iLOファームウェアが実行されると、UEFI BIOS（システムROM）、CPLD（System Programmable Logic）、Innovation Engine、およびServer Platform Services（SPS）ファームウェアが検証されます。

アクティブなシステムROMの検証に失敗し、冗長化システムROMが有効である場合は、冗長化システムROMがアクティブになります。アクティブシステムROMと冗長化システムROMの両方が無効であり、iLO Advancedライセンスがインストールされている場合は、ファームウェア検証スキャンが開始されます。構成されているファームウェア検証の設定に応じて、システムリカバリセット内のコンポーネントを使用した修復が開始されるか、または障害のログが記録され、手動で修復を完了する必要があります。システムROMが検証されない場合、サーバーは起動しません。

CPLD（System Programmable Logic）、Innovation Engine、またはServer Platform Services（SPS）ファームウェアが検証に失敗した場合、iLO Advancedライセンスがインストールされていれば、システムがそれらをシステムリカバリセットから自動的に復元します。ライセンスがインストールされていない場合は、失敗がログに記録され、手動で修復を完了する必要があります。

ファームウェアの検証アクティビティおよびリカバリアクションについてIMLをチェックします。

ファームウェアが検証され、サーバーの電源がオンになると、セキュアブート機能がブートプロセス中に追加のコンポーネントを検証します。

詳しくは

システムリカバリセット
セキュアブート
ファームウェア検証

セキュアブート

セキュアブートはBIOSに実装されているため、特別なハードウェアが必要ありません。セキュアブートにより、ブートプロセス中に起動した各コンポーネントにデジタル記号が付けられ、この署名がUEFI BIOSに内蔵された一連の信頼済みの証明書と照合されて検証されます。セキュアブートは、次のコンポーネントのソフトウェアIDを検証します。

- PCIeカードからロードされたUEFIドライバー
- 大容量ストレージデバイスからロードされたUEFIドライバー
- プリブートUEFIシェルアプリケーション
- OS UEFIブートローダー

セキュアブートが有効になっている場合：

- ブートプロセス中、ブートローダーを持つオペレーティングシステムとファームウェアコンポーネントは、実行するために適切なデジタルシグネチャーを持っている必要があります。
- オペレーティングシステムは、起動するためには、セキュアブートをサポートし、認証済みキーの1つで署名されたEFIブートローダーを持っている必要があります。サポートされるオペレーティングシステムについて詳しくは、https://www.hpe.com/servers/ossupportを参照してください。

直接接続された管理コンソールまたはiLOリモートコンソールを使用して、UEFI BIOSに埋め込まれた証明書をカスタマイズできます。詳しくは、HPE ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用UEFIシステムユーティリティユーザーガイドを参照してください。

サーバーID

サーバーID（DevID）は、ネットワーク全体でサーバーを一意に識別するための方法を提供します。それはIEEE 802.1AR DevID標準に基づいています。DevIDはサーバーに一意にバインドされているため、サーバーは、通信デバイスを認証、プロビジョニング、および権限付与するさまざまな業界標準およびプロトコルでそのIDを証明できます。

iLOは、工場出荷時にプロビジョニングされたサーバーID（iLO IDevID）およびユーザー定義のサーバーID（iLO LDevID）をサポートしています。また、工場出荷時にプロビジョニングされたシステム証明書（システムIDevIDおよびシステムIAK）も保存します。この機能のサポートを確認するには、製品のQuickSpecsドキュメント（https://www.hpe.com/info/qs）を参照してください。

サーバーID機能について詳しくは、HPE iLO 5ユーザーガイドとIEEE 802.1Xベースのサーバーオンボーディングの有効化テクニカルペーパーを参照してください。

> **注記:**
> iLO IDevID、iLO LDevID、システムIDevID、およびシステムIAKは、iLOセキュリティ状態の移行および工場出荷時設定へのリセット後でも保持されます。

iLO IDevID

iLOは、工場でサーバーIDを使用してプロビジョニングできます。工場出荷時にプロビジョニングされたサーバーIDはiLO IDevIDと呼ばれます。HPEサーバーは、802.1X認証用のIDevIDを使用して、顧客ネットワークに安全にオンボーディングできます。iLO IDevIDは生涯有効であり、不変です。

HPEの工場にIDevIDでサーバーをプロビジョニングするように指示するには、SKU P41905-B21（TPM 2.0モジュールがない場合）またはP42104-B21（TPM 2.0モジュールがある場合）を注文に含めます。

iLO LDevID

IDevIDは、iLO LDevIDと呼ばれるユーザー定義のサーバーIDで補完できます。iLO LDevIDは、サーバーが使用される管理ドメインで一意のものです。HPEサーバーは、802.1X認証用のLDevIDを使用して、顧客ネットワークに安全にオンボーディングできます。iLO LDevIDは、iLO IDevIDを持たないサーバーで使用できます。

LDevIDは、ローカルネットワーク管理者による登録（認証情報の認証および認可）を容易にするのに役立ちます。iLOは、工場外でのLDevIDのインポート、表示、および削除をサポートします。

システムIDevID証明書

iLOは、サーバーホストIDを使用してプロビジョニングでき、オペレーティングシステムで使用できます。この工場出荷時にプロビジョニングされたIDは システムIDevIDと呼ばれます。その対応する秘密キーはTPMに保存されます。システムIDevIDは、IDevIDのTPM 2.0インプリメンテーションに関するTrusted Computing Group（TCG）提案に従います。システムIDevIDを取得するには、SKU P42104-B21を注文してください。

iLOでは、システムIDevID証明書をアップデートまたは削除することはできません。証明書は、次のiLO RESTful API GETコマンドを使用して表示できます。

```
/redfish/v1/Managers/1/SecurityService/SystemIDevID/Certificates/1
```

システムIAK証明書

iLOは、システム初期認証キー（IAK）証明書を使用してプロビジョニングできます。この機能はシステムIDevIDに似ていますが、TPMベースの認証に使用されます。対応する秘密キーはTPMに保存されます。システムIAKは、IDevIDのTPM 2.0インプリメンテーションに関するTCG提案に由来しています。システムIAK証明書を取得するには、SKU P42104-B21を注文してください。

iLOでは、システムIAK証明書をアップデートまたは削除することはできません。証明書は、次のiLO RESTful API GETコマンドを使用して表示できます。

```
/redfish/v1/Managers/1/SecurityService/SystemIAK/Certificates/1
```

詳しくは

802.1XおよびiLO
DevIDおよびシステムIAKのOne-buttonセキュア消去

802.1XおよびiLO

IEEE 802.1Xは、ポートベースのネットワークアクセス制御のメカニズムです。ネットワークへのアクセスを規制し、未識別および未許可のネットワークアクセスから保護します。

802.1Xは、認証プロセス中のメッセージ交換に拡張認証プロトコル（EAP）を使用します。EAP-トランスポート層セキュリティ（EAP-TLS）は、認証に証明書またはスマートカードを使用するEAPタイプです。

HPE iLO 5は、802.1Xアクセス制御ネットワークへのオンボーディングのためのEAP-TLS認証をサポートします。工場出荷時にプロビジョニングされたサーバーID（iLO IDevID）を使用して、HPEサーバーは、802.1X認証用に、ゼロタッチ（無人自律操作）で安全にオンボードしてIDを確立できます。iLOは、802.1X認証用にユーザーがプロビジョニングしたサーバーID（iLO LDevID）もサポートしています。iLO IDevIDとiLO LDevIDの両方がシステムに存在する場合、iLO LDevIDがEAP-TLS認証に使用されます。

802.1X認証のデフォルト設定は有効です。システムにiLO IDevIDまたはiLO LDevIDがない場合、iLO 5はEAP-TLS認証を開始したり、認証要求に応答したりしません。

詳しくは

サーバーID

Trusted Platform Module

Trusted Platform Module（TPM）は、プラットフォームの認証に使用される仕掛けを安全に格納するコンピューターチップです。これらの仕掛けには、パスワード、証明書、暗号鍵などが含まれます。また、TPMを使用すると、プラットフォームの測定値を格納してプラットフォームの信頼性を保証することができます。

Trusted Platform Moduleで構成されているサーバーでは、ファームウェアおよびオペレーティングシステムは、TPMを使用して、ブートプロセスのすべてのフェーズを測定できます。

TPMサポート情報については、次のWebサイトのサーバーのQuickSpecsを参照してください。**https://www.hpe.com/info/qs**。

詳しくは

Trusted Platform Moduleオプション

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。

承認

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。

永続的なサービス拒否攻撃からの保護

理論的に、永続的なサービス拒否攻撃（PDOS）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。PDOS攻撃は、「フラッシング」と呼ばれることもあります。

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、システムBIOS、CPLD、およびInnovation Engineファームウェアなどの iLOによってフラッシュできるすべてのファームウェアタイプは、インストール前にデジタル検証されます。この検証により、物理的にアクセスできないユーザーによる侵害されたコードの挿入を防ぎます。

システムBIOS、iLOファームウェア、およびその他の重要なファームウェアタイプは、Silicon Root of Trustの一部として起動時にデジタル検証されます。この検証により、攻撃者による物理的なアクセスがあっても、ファームウェアの侵害を防ぎます。

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。

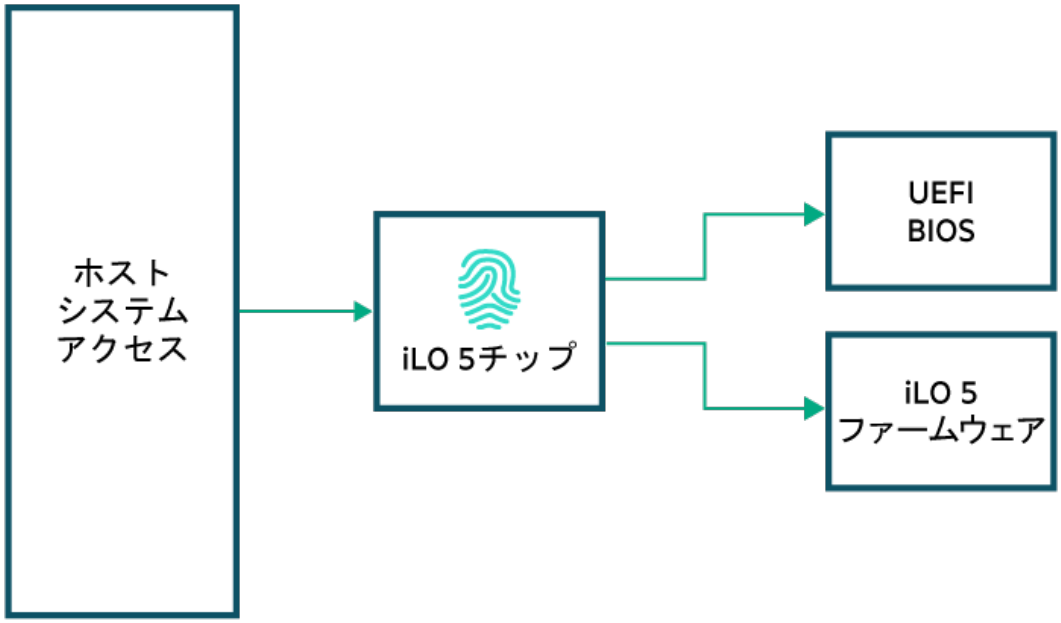
詳しくは

Silicon Root of Trust

システムROMおよびiLOファームウェアのiLOファイアウォール

HPEのサーバーとコンピューティングモジュールは**NIST800-147B、サーバーのBIOS保護ガイドライン**に準拠しています。

システムROMとiLOファームウェアは、iLOチップによって、ホストアクセスから物理的に保護されているフラッシュチップ上にあります。これらのフラッシュチップに書き込むことができるのは、iLOファームウェアだけです。この構成により、ホストシステムからの未許可アクセスが防止されます。iLOファームウェアは、BIOSフラッシュチップに書き込まれるすべてのイメージを認証します。



iLOとサーバーブレードまたはコンピューティングモジュール間の通信

HPE 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を使用して、複数のサーバーブレードを保持します。独立した電源サブシステムが、そのエンクロージャー内のすべてのサーバーブレード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サーバーブレード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。

HPE Synergyコンピューティングモジュール

HPE Synergy 12000フレームは、単一のフレームを使用して、複数のコンピューティングモジュールを保持します。独立した電源サブシステムが、フレーム内のすべてのコンピューティングモジュール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HPE Synergyコンピューティングモジュールのi LO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、フレーム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アンペア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。シャーシの背面にある2つのポートから、Synergyコンピューティングモジュール上のiLOネットワーク接続にアクセスできます。

物理的アクセスのセキュリティ

詳しくは

シャーシ侵入検知デバイス
USBセキュリティ
ラックと電源のセキュリティ
ベゼルロック
システムメンテナンススイッチ

システムメンテナンススイッチ

Hewlett Packard Enterpriseサーバーとコンピューティングモジュールには、さまざまなセキュリティ機能と構成を制御するハードウェア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、シャーシ内のシステムボード上にあります。スイッチにアクセスするには、デバイスをオフラインにし、電源を切り、アクセスカバーを取り外す必要があります。

次のシステムメンテナンススイッチはデフォルトでオフになっています。製品のセキュリティ動作を変更する場合は、これらのスイッチをオンに設定できます。システムメンテナンススイッチの設定は、アクセスパネルのラベルと製品のユーザーガイドに記載されています。

iLOセキュリティ（位置1）

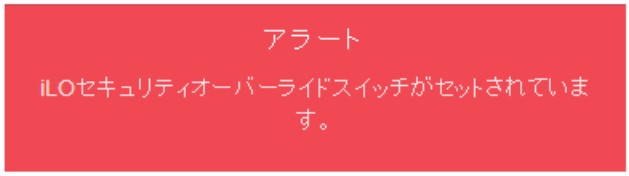
システムメンテナンススイッチのiLOセキュリティ設定により、システムボードを物理的に制御できる管理者が、緊急時にアクセスすることができます。

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。

このスイッチがオフの場合（デフォルト）、iLOは構成されている認証設定を適用します。

このスイッチを無効にすると、次のような影響があります。

- 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、すべてのログイン証明書検証が無効になります。
- 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、すべてのログイン証明書検証が適用されます。
- 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ネットワーキング、iLO Webインターフェイス、およびROMベースのシステムユーティリティは、以前に無効にされていた場合でもアクセスできます。
- システムリカバリ特権が適用されます。この特権を必要とするアクションを実行するには、特権が有効にされているユーザーアカウントで認証する必要があります。
- 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ます。



- 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ます。
- 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ます。

BIOSパスワードが無効（位置5）

スイッチがオフ（デフォルト）の場合、UEFIシステムユーティリティの管理者パスワードの設定と電源投入時パスワード設定機能を構成して使用できます。

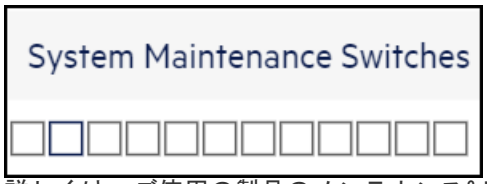
スイッチがオンになると、構成済みのBIOS管理者と電源オンパスワードが削除されます。

構成のリセット（位置6）

スイッチがオフ（デフォルト）の場合、BIOS構成が維持されます。

スイッチがオンになると、BIOSの工場出荷時のデフォルトがすべて復元されます。

システムメンテナンススイッチのステータスは、Intelligent Provisioningのシステム情報ページで表示できます。



詳しくは、ご使用の製品のメンテナンス&サービスガイドを参照してください。

詳しくは

電源投入時パスワード
管理者パスワード
iLOセキュリティを無効にする理由

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。
  - iLOネットワーク有効化モジュールのあるサーバーでは、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。
- 設定されたユーザー名は1つのみで、パスワードを忘れてしまった。
- 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たい。

  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。

詳しくは
システムメンテナンススイッチ

USBセキュリティ

UEFIシステムユーティリティ

サーバーのUSBポート設定は、UEFIシステムユーティリティのUSBオプションセクションから構成できます。

以下のリソースを構成できます。

- USBポートと内蔵デバイスの起動動作。
- 仮想メディアデバイスや内臓SDカードなどのUSBデバイスから起動する機能。
- ブートデバイスを列挙するときに、最初に検索するUSBデバイスまたはSDデバイス。
- 内蔵SDカードの可用性。

iLOサービスポート

iLOサービスポートは、サポートされているサーバーでiLOのラベルが付けられているUSBポートです。

iLOサービスポートを使用して、Active Health System Logをダウンロードするか、またはクライアントを、サポートされているイーサネットアダプターに接続して、iLOにアクセスできます。

iLOサービスポートには、次のセキュリティ特性があります。

- サービスポートを使用してサーバー内のデバイスまたはサーバー自体を起動することはできません。
- サービスポートに接続してサーバーにアクセスすることはできません。
- 接続されているデバイスにサーバーからアクセスすることはできません。

機能を無効にすることも、USBフラッシュドライブのアクセスを許可するか、資格情報を要求するか、イーサネットアダプターを使用するかどうかを選択することもできます。

詳しくは、iLOセキュリティ設定の推奨事項を参照してください。

ラックと電源のセキュリティ

Hewlett Packard Enterpriseは、物理的および電子的ロックオプションを備えたラックや、安全なケーブル保持と電源関連のダウンタイムを提供するロック電源コードなど、ラックと電源のセキュリティを強化するソリューションを提供しています。

これらのソリューションについて詳しくは、https://www.hpe.com/info/rackandpowerを参照してください。

ベゼルロック

サポートされている製品への外部アクセスに対する保護のために、ベゼルロックを取り付けることができます。注文情報については、https://www.hpe.com/info/qsの製品のQuickSpecsを参照してください。インストール手順については、製品のユーザーガイドを参照してください。

iLOサーバー管理機能

iLO Webインターフェイスでタスクを実行する方法については、オンラインヘルプを参照するか、次のWebサイトのHPE iLO 5ユーザーガイドを参照してください。https://www.hpe.com/support/ilo5-ug-ja。

iLO RESTful APIを使用して、iLO Webインターフェイス経由で利用可能なタスクの多くを実行できます。詳しくは、https://hewlettpackard.github.io/ilo-rest-api-docs/を参照してください。

詳しくは

推奨されるセキュリティ設定

iLO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。これらのオプションの構成については、次のWebサイトのHPE iLO 5ユーザーガイドを参照してください。https://www.hpe.com/support/ilo5-ug-ja。

専用管理ネットワーク

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。

インターネット接続

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。

SSL証明書

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。

信頼済みCA証明書

信頼済みCA証明書をインストールして、LDAPなどの外部サービスの証明書の検証を有効にします。

パスワード

パスワードに関するガイドラインに従います。

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。

ユーザーアカウントの権限

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。

ファームウェアアップデート

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。

認証

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。

特にリモートで、またはローカルネットワークの外部から接続する場合に、Two-Factor認証を実装して、追加のセキュリティを提供します。

SNMPトラフィックの保護

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。

ポートとプロトコルの設定

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。

.NETリモートコンソールにHTTPSを使用する

このオプションを構成するには、認証局（CA）によって署名された信頼できるSSL証明書をインストールし、IRCはiLO内の信頼済みの証明書を要求します設定を有効にします。

未使用の機能

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。

サーバーOSコンソールのロック

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。

セキュリティ状態

高セキュリティ、FIPS、CNSAなどの高いセキュリティ状態を構成します。

構成ユーティリティ

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。

認証エラーの記録

認証エラーを記録するようiLOを構成します。

ファームウェア検証

ファームウェア検証スキャンを有効にします。

セキュリティダッシュボードとセキュリティログ

セキュリティダッシュボードとセキュリティログを使用して、セキュリティリスクと推奨事項を監視します。

ホスト認証

ホスト認証が必要機能を有効にします。

ファームウェアダウングレードポリシー

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 。

リカバリセット

リカバリセットを最新の状態に保ちます。

HTTP接続

HTTP接続経由のアクセスを防ぐようにiLOを構成します。

この動作を構成するには、認証局（CA）によって署名された信頼できるSSL証明書をインストールし、IRCはiLO内の信頼済みの証明書を要求します設定を有効にします。

この構成では、iLO Webインターフェイスにアクセスすると、iLOが応答ヘッダーでHTTP Strict Transport Security（HSTS）フラグを返します。これにより、ブラウザーはHTTP要求をHTTPSに自動的にリダイレクトできます。

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値を、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、iLOアクセス設定ページで構成できます。

表1: iLO経由で構成可能なネットワーク設定とポート

説明	デフォルト設定またはポート	プロトコルタイプ
IPMI/DCMI over LANポート	623	UDP
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。	無効	
リモートコンソールポート	17990	TCP
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。	有効	
セキュアシェル（SSH）ポート	22	TCP
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。	有効	
SNMPポート	161	UDP
SNMP Trap Port	SNMPアラートの場合は162（送信のみ）。	UDP
SNMP iLOが外部のSNMP要求に応答するかどうかを指定します。	有効	
仮想メディアポート	17988	TCP
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。	有効	
Webサーバー非SSLポート（HTTP）	80	TCP
WebサーバーSSLポート（HTTPS）[1]	443	TCP
Webサーバー[2] 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。	有効	

1 Direct Connect Remote Supportでは、この値を443に設定する必要があります。
2 iLO Webインターフェイス、リモートコンソール、iLO RESTful API、iLO連携、ファームウェアアップデート、およびRIBCLをサポートします。

その他の発信ポート

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

説明	既定のポート	プロトコルタイプ	iLOのWebインターフェイスの場所
DNS解決	53	UDP	該当なし
iLO連携/SSDPマルチキャスト	1900	UDP	該当なし
DHCPv4	67、68	UDP	該当なし
DHCPv6	547	UDP	該当なし
NTP	123	UDP	該当なし
WINS	42	UDP	該当なし
Kerberos KDCサーバーポート	88	TCP、UDP	セキュリティ > ディレクトリ
ディレクトリサーバーLDAP SSLポート	636	TCP	セキュリティ > ディレクトリ
アラートメールSMTPポート	25	TCP	管理 > アラートメール
Remote Syslog Port	514	UDP	管理 > リモートSyslog
キーマネージャーのポート	9000	TCP	管理 > キーマネージャー
リモートサポートのポート	7906	TCP	リモートサポート > 登録

iLOでサポートされていないポート

iLOは、表3: サポートされていないポートにリストされている一般的に使用されるポートをサポートしていません。

表3: サポートされていないポート

説明	ポート	プロトコルタイプ	注記
セキュリティ保護されていないLDAP • 接続（TCP） • コネクションレス（UDP）	389	TCP/UDP	iLOは発信LDAP接続にセキュアポート636を使用します。
グローバルカタログに対してセキュリティ保護されていないLDAP • 接続（TCP） • コネクションレス（UDP）	3268	TCP/UDP	iLOはセキュアLDAP接続を使用します。

機能、ポート、およびプロトコルのアクセス制御

iLOアクセス設定機能を使用して、未使用の機能、ポート、およびプロトコルを無効にできます。詳しくは、HPE iLO 5 ユーザーガイドのアクセス設定のドキュメントを参照してください。

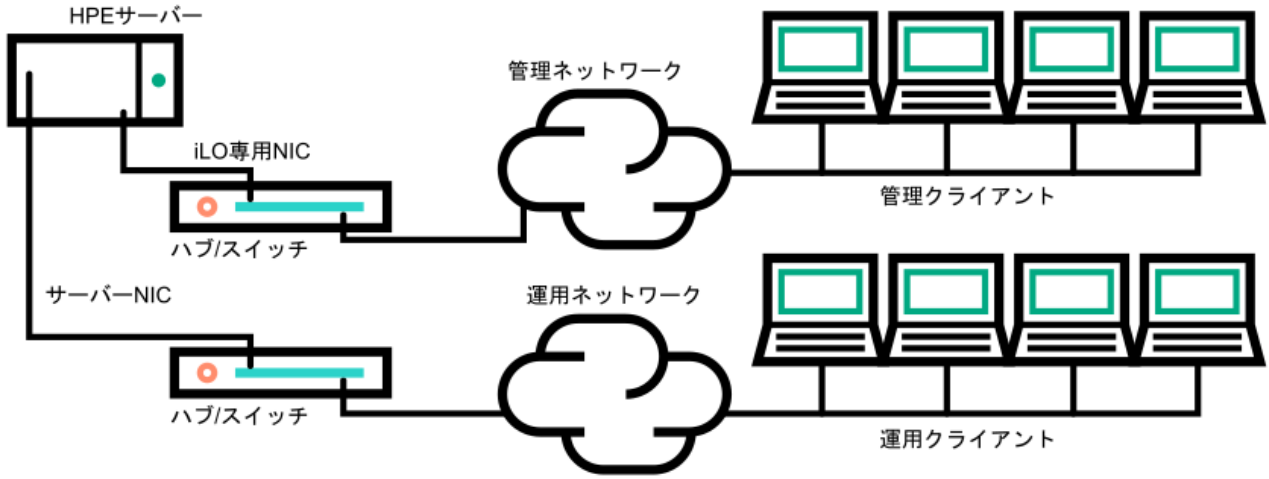
iLOネットワーク接続オプション

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1: 専用管理ネットワーク



本番環境ネットワーク

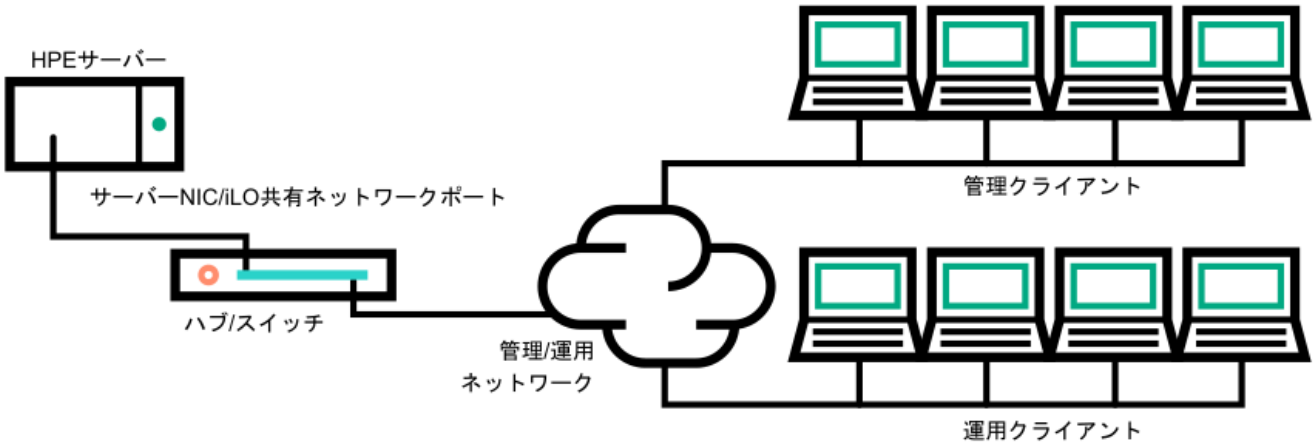
この設定では、NICとiLOポートの両方を本番環境ネットワークに接続します。iLOで、このタイプの接続は、共有ネットワークポート構成と呼ばれます。特定のHewlett Packard Enterprise内蔵NICとアドオンカードが、この機能を提供します。この接続により、ネットワークのどこからでもiLOにアクセスできます。共有ネットワークポート構成を使用すると、iLOをサポートするために必要なネットワークハードウェアやインフラストラクチャの量が減ります。

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。
- サーバーの起動時、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。
- ネットワークコントローラーのファームウェアをアップデートまたはリセットすることも、iLOが短期間、ネットワーク経由で到達不能に陥る原因となる可能性があります。
- iLO共有ネットワークポート接続は、100 Mbpsを超える速度では動作できません。iLO仮想メディアを介したデータ転送などのネットワーク集約型タスクは、iLO専用ネットワークポートを使用する構成で実行される同じタスクよりも遅くなる場合があります。

図2: 共有ネットワーク接続



iLOネットワーク有効化モジュール

一部のサーバーでは、専用管理ネットワーク（デフォルト）または共有ネットワーク接続によるリモート管理のサポートを追加するために、オプションのiLOネットワーク有効化モジュールが必要です。iLOネットワーク有効化モジュールがインストールされていない場合、iLOアクセスは、ホストベース（インバンド）のアクセス方式でのみサポートされます。サポートされているホストベースのアクセス方式の例には、iLO RESTful API、UEFIシステムユーティリティ、iLOサービスポート（利用可能な場合）、および仮想NICが含まれます。

サーバーでサポートされているネットワーク接続を確認するには、サーバーのユーザーガイドを参照してください。

詳しくは

仮想LAN
ネットワークポートとマネジメントポート

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。

詳しくは

iLOネットワーク接続オプション

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イーサーネットポートとの間の接続が妨げられます。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。

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

これらの形式の例については、iLOユーザーガイドを参照してください。

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。

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。

Two-Factor認証

連邦政府認証を満たすために必要な要件の一部がTwo-Factor認証です。Two-Factor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、Two-Factor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。

SSL証明書

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復元機能を使用する場合、証明書が含まれます。

詳しくは

iLOのバックアップとリストア
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
TLS/SSLサーバーX.509証明書が信頼されていない
脆弱な暗号化キー

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を含む200社を超えるベンダーによってサポートされています。

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。

セキュリティダッシュボード

iLOセキュリティダッシュボードには、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。

詳しくは

サーバー構成ロック
セキュリティリスク状態の原因
iLOセキュリティ状態

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へのログインが必要

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。

SNMPv1

SNMPv1は有効になっています。この構成は、iLOでのSNMPv1要求の受信およびSNMPv1アラートの送信を許可します。SNMPv1を有効にすると、攻撃に対するシステムの脆弱性が増加します。

Hewlett Packard Enterpriseでは、SNMP設定ページでこの機能を無効にすることをお勧めします。

詳しくは

セキュリティダッシュボード

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。

リモートコンソールのセキュリティ

リモートコンソールのコンピューターロック

この機能を使用すると、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たときに、自動的に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。

統合リモートコンソールの信頼設定

.NET IRCは、Microsoft .NET Frameworkの一部であるMicrosoft ClickOnceを介して起動します。ClickOnce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構成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する設定を有効にすることをお勧めします。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にされている場合、.NET IRCはSSL以外の接続を使用して起動するため、安全ではありません。この構成では、.NET IRCが暗号キーの交換を開始すると、SSLが使用されます。信頼されたSSL証明書をインストールできず、SSL以外の接続を使用したくない場合は、スタンドアロンリモートコンソール（HPLOCONS）またはHTML 5内蔵リモートコンソールを使用できます。

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

詳しくは

iLOセキュリティ状態
高いセキュリティ状態を使用する場合のiLOへの接続
SSH暗号、キー交換、およびMACのサポート
SSL暗号およびMACのサポート
FIPS認証とCommon Criteria認定

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。
- 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。

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。.NET IRCとJava IRCはCNSAに準拠していません。

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。

詳しくは

高いセキュリティ状態を使用する場合のiLOへの接続
SSH暗号、キー交換、およびMACのサポート
SSL暗号およびMACのサポート
システムメンテナンススイッチ

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。

  ホスト認証が必要のアクセス設定は、ホストベースの構成ユーティリティに次の影響を与えます。

  - 有効 – すべてのiLOセキュリティ状態のホストベースの構成ユーティリティを使用するには、有効な認証情報が必要です。
  - 無効 – iLOが製品また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設定されている場合、有効な認証情報は必要ありません。

  ホスト認証が必要の設定は、FIPSまたはCNSAセキュリティ状態が使用されている場合は無効にすることはできません。

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。

詳しくは

iLOセキュリティ状態

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、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

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

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.commoncriteriaportal.org/files/epfiles/383-4-427%20CR%20v1.0e.pdfで認定レポートを参照してください。

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。

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。

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。

詳しくは
ディレクトリサービスのサポート

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。

セキュアファームウェアフラッシュアップデート

ファームウェアイメージがSHA384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。

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）
- Innovation Engine（IE）ファームウェア
- サーバープラットフォームサービス-IEフルリカバリイメージ（サポートされているサーバーのみ）

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。

破損したサーバープラットフォームサービス（SPS）記述子が検出された場合、破損したファームウェアイメージはiLOレポジトリの隔離領域に移動します。サーバープラットフォームサービス-IEフルリカバリイメージがシステムリカバリセットにあり、ファームウェア検証ページでログおよび自動的に修復が選択されている場合、リカバリが自動的に実行されます。リカバリが実行されると、イベントがIMLとセキュリティログに記録されます。破損したSPS-IE記述子の自動リカバリには、iLO Advancedライセンスが必要です。

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。

詳しくは

システムリカバリセット
サーバープラットフォームサービス記述子の検証とリカバリ

サーバープラットフォームサービス記述子の検証とリカバリ

Intel Lewisburgチップセット（PCH）を搭載した、サポートされているGen10 Plusサーバーでは、サーバーの起動時にサーバープラットフォームサービス（SPS）記述子が検証されます。記述子領域（SPIパートに存在するSPSファームウェアイメージのクリティカルセクション）は、暗号面からその整合性と所有権が検証されます。この機能はファイル記述子ゼロ検証（FDOV）と呼ばれます。検証プロセスはSPSファームウェアによって開始されます。有効な記述子が検出されない場合、フルファームウェアイメージのリカバリが開始されます。フルファームウェアイメージの自動リカバリには、iLO Advancedライセンスが必要です。

iLOでリカバリプロセスを自動的に完了するには、Gen10 Plusサーバープラットフォームサービス-IEのフルリカバリイメージが必要です。SPS記述子ファームウェアの問題が検出された時点で、リカバリイメージが構成済みシステムリカバリセットの一部である必要があります。リカバリイメージは署名付きの`.flash`イメージです。これにより、iLOでSPS-IE SPIパートの8 MBフルアップデートを実行できます。このアップデートにより、SPS-IE SPIパートが工場出荷時設定に復元されます。リカバリプロセスには、SPSソフトストラップとIEブートローダーのアップデートが含まれます。リカバリフラッシュイメージは、サーバーがS5（AUX）電源ステータスの場合にのみ使用できます。実行中またはPOST中はリカバリプロセスを完了できません。

次のWebサイトで、最新のSPS-IEフルリカバリイメージのダウンロード、またはアップデートアラートの登録を実行できます：https://www.hpe.com/support/ilo5。

詳しくは

ファームウェア検証
システムリカバリセット

システムリカバリセット

デフォルトでは、システムリカバリセットがすべてのサーバーに付属します。**リカバリセット**権限を持つユーザーアカウントは、このインストールセットを構成できます。システムリカバリセットは同時に1つのみ存在できます。

インテルサーバー用のデフォルトのシステムリカバリセットには、以下のファームウェアコンポーネントが含まれます。

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

AMDサーバー用のデフォルトのシステムリカバリセットには、以下のファームウェアコンポーネントが含まれます。

- システムROM（BIOS）
- iLOファームウェア
- システムプログラマブルロジックデバイス（CPLD）

デフォルトのシステムリカバリセットが削除されている場合

- リカバリセット権限を所有しているユーザーは、iLO RESTful APIおよびRESTfulインターフェイスツールを使用してiLOレポジトリに保存されているコンポーネントからシステムリカバリセットを作成することができます。

  詳しくは、WebサイトにあるiLOユーザーガイドを参照してください （**https://www.hpe.com/support/ilo-docs**）。
- リカバリセット権限を持つユーザーは、SUMを使用してインストールセットを作成し、iLO RESTful APIを使用してそれをシステムリカバリセットとして指定できます。

  手順については、オプションキットの**SUMドキュメントを参照**してください。

詳しくは

サーバープラットフォームサービス記述子の検証とリカバリ
ファームウェア検証

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。

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。

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。これらの問題の多くは、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。

詳しくは

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
IPMI 2.0 RAKP RMCP +認証HMACパスワードハッシュの暴露
TLS/SSLサーバーX.509証明書が信頼されていない
IPMI 1.5 GetChannelAuthレスポンス情報の暴露
TCPシーケンス番号予測の脆弱性
IPMI 2.0 RAKP RMCP +認証ユーザー名の暴露
脆弱な暗号化キー
TCPタイムスタンプ応答
Missing HTTPOnly Flag from Cookie

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、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。

詳しくは
SSL証明書

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、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。

詳しくは

機能、ポート、およびプロトコルのアクセス制御
IPMIまたはDCMI over LANでのiLOの使用のガイドライン

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、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。

詳しくは
SSL証明書

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、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。

詳しくは

機能、ポート、およびプロトコルのアクセス制御
IPMIまたはDCMI over LANでのiLOの使用のガイドライン

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、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。

詳しくは

機能、ポート、およびプロトコルのアクセス制御
IPMIまたはDCMI over LANでのiLOの使用のガイドライン

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、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。

詳しくは

SSL証明書
iLO暗号化設定

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。

詳しくは

SSL証明書

UEFIシステムユーティリティサーバー管理機能

UEFIシステムユーティリティを使用して、サーバー構成ロック機能を構成し、サーバーの設定と動作を管理し、サポートされているサードパーティソリューションを構成できます。UEFIシステムユーティリティを使用してタスクを実行する方法については、オンラインヘルプを参照するか、HPE ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用UEFIシステムユーティリティユーザーガイド（https://www.hpe.com/support/UEFIGen10-UG-en）を参照してください。

詳しくは

HPEおよびサードパーティセキュリティソリューション
サーバー構成ロック
管理者パスワード
高度なBIOSおよびプラットフォームセキュリティオプション
HTTPSブート
電源投入時パスワード
Trusted Platform Moduleオプション

電源投入時パスワード

電源投入時パスワード設定機能を有効にすると、サーバーの電源を入れたときにパスワードプロンプトが表示されます。パスワードを入力するまで、起動プロセスは続行しません。

パスワードを無効化またはクリアするには、パスワードの後にスラッシュ文字（/）を付けて入力します。

注記:
自動サーバー復旧（ASR）の再起動が行われると、電源投入時パスワードプロンプトは表示されず、サーバーは通常どおり起動します。

デフォルト設定は、**無効**です。

この機能を有効にすると、システムメンテナンススイッチを使用してパスワード要件を無効にできます。

詳しくは
システムメンテナンススイッチ

管理者パスワード

管理者パスワードの設定機能を有効にすると、UEFIシステムユーティリティまたはUEFIシェルにアクセスしようとしたときに、パスワードプロンプトが表示されます。UEFIシステムユーティリティまたはUEFIシェルに進む前にパスワードが必要です。3回のパスワード試行が許可されます。

この機能を有効にすると、システムメンテナンススイッチを使用してパスワード要件を無効にできます。

詳しくは

システムメンテナンススイッチ

HTTPSブート

UEFIシステムユーティリティでHTTPサポートとTLS（HTTPS）オプションの設定を構成して、サーバーがTLSセッションを使用してHTTPS URIで起動できるようにすることができます。このオプションは、PXEブートに代わるより安全な手段を提供します。HTTPSブートを有効にするには、HTTPSサーバーTLS証明書を登録する必要があります。

構成すると、HTTPSブートオプションが、ネットワークブートが有効になっているネットワークポートのUEFIブート順序リストに追加されます。

HTTPSサーバー証明書の管理に加えて、この機能の高度なセキュリティ設定を構成できます。オプションには、暗号スイート、証明書検証タイプ、厳密なホスト名チェック、およびTLSプロトコルバージョンが含まれます。

Trusted Platform Moduleオプション

UEFIシステムユーティリティを使用して、現在のTrusted Platform Module（TPM）構成を表示し、設定をアップデートできます。

- デフォルトでは、TPMを取り付けた後にサーバーの電源がオンになると、TPMはTPM 2.0として有効化されます。
- UEFIモードでは、TPMをTPM 2.0またはTPM 1.2として動作するように構成できます。
- レガシーブートモードでは、TPM構成をTPM 1.2とTPM 2.0間で変更することができますが、サポートされている動作はTPM 1.2のみです。

> △ **注意:**
>
> サーバーの変更や、OSでのTPMのサスペンドまたは無効化で、適切な手順に従わないと、TPMを使用しているOSですべてのデータアクセスがロックされる場合があります。システムまたはオプションファームウェアのアップデート、システムボードやハードドライブなどのハードウェアの交換、TPMのOS設定の変更を行う際は、推奨される手順に従うことが重要です。OSのインストール後にTPMモードを変更すると、データ消失などの問題の原因となることがあります。

詳しくは
Trusted Platform Module

高度なBIOSおよびプラットフォームセキュリティオプション

サーバーのセキュリティを強化するには、次の高度なオプションを検討してください。

プラットフォーム証明書サポート

Gen10 Plus製品でのプラットフォーム証明書のサポートを有効または無効にします。

iLOアカウントでのログインを許可

ユーザーがホストBIOS特権を持つiLOアカウントを使用して、ROMベースセットアップユーティリティにログインできるようにします。

バックアップROMイメージの認証

起動時の冗長ROMイメージの暗号化認証を有効にします。

ワンタイムブートメニュー（F11プロンプト）

POST中にF11プロンプトを有効または無効にします。

Intelligent Provisioning（F10プロンプト）

Intelligent Provisioningのアクセスを有効または無効にします。

UEFI変数アクセスのファームウェアコントロール

OSなどの他のソフトウェアによって特定の変数が上書きされないように、システムBIOSが制御できるようにします。

No-Executeメモリ保護

データセクションの非実行保護を有効または無効にします。

製品の廃止または再目的化

製品を廃止する場合、または別の目的で使用する場合は、One-buttonセキュア消去またはシステムの消去およびリセット機能を使用してデータを保護できます。

詳しくは

One-buttonセキュア消去
システムの消去とリセット

One-buttonセキュア消去

サーバーを運用廃止するか、または別の用途で準備する場合、One-buttonセキュア消去機能を使用できます。

One-buttonセキュア消去は、NIST Special Publication 800-88 Revision 1のメディアサニタイズのガイドラインに準拠しています。

仕様について詳しくは、**https://www.ipa.go.jp/files/000025355.pdf**(日本語訳)を参照してください。仕様のセクション2.5では、サニタイズのレベルについて説明しています。付録では、メディアの最小サニタイズレベルを提示しています。

One-buttonセキュア消去は、ユーザーデータの**パージ**に対するNIST SP 800-88 Revision 1のサニタイズに関する勧告を実装しており、サーバーおよびサポートされたコンポーネントをデフォルトの状態に戻します。この機能は、サーバーの揮発性に関する報告のドキュメントでユーザーが行う多くのタスクを自動化します。

詳しくは

One-buttonセキュア消去アクセス方式
工場出荷時の状態に戻されるハードウェアコンポーネント
工場出荷時の状態に戻されないハードウェアコンポーネント
DevIDおよびシステムIAKのOne-buttonセキュア消去
One-buttonセキュア消去のFAQ

One-buttonセキュア消去アクセス方式

次の製品からOne-buttonセキュア消去プロセスを開始できます。

- iLO 5 2.30以降
- Intelligent Provisioning 3.30以降
- iLO RESTful API

詳しくは
One-buttonセキュア消去

工場出荷時の状態に戻されるハードウェアコンポーネント

次のコンポーネントは、One-buttonセキュア消去プロセス中に、工場出荷時の状態に戻されます。

- UEFI構成ストア
- RTC（システムの日付と時刻）
- Trusted Platform Module
- NVRAM
  - BIOS設定
  - iLO構成設定
  - iLOイベントログ
  - インテグレーテッドマネジメントログ
  - セキュリティログ
- 内部ポートに接続されたHPE SmartアレイSRコントローラーおよびドライブ。たとえば、3I:1:1です。
- HPE SmartアレイS100iソフトウェアRAID
- ドライブデータ（ネイティブのサニタイズ方式をサポートするドライブの場合）
  - SATA、SASドライブ（SSDおよびHDD）
  - NVM Express
- 不揮発性メモリ
  - NVDIMM-N
  - インテルOptane DC不揮発性メモリ
- 内蔵フラッシュ
  - iLO RESTful APIデータ
  - Active Health System
  - ファームウェアレポジトリ

詳しくは
One-buttonセキュア消去

工場出荷時の状態に戻されないハードウェアコンポーネント

次のコンポーネントはOne-buttonセキュア消去プロセスの影響を受けません。

- USBドライバー
- SDカード
- iLO仮想メディア
- PCIコントローラー上の構成
- HPE SmartアレイMRコントローラーおよび接続されたストレージ
- HPE SmartアレイSRコントローラー上の外部ポートに接続されたドライブ、たとえば1E:1:1です。
- SAS HBAおよび接続されたドライブ
- ネイティブのサニタイズ方式をサポートしていないSATA、SAS、およびNVM Expressドライブ。

  たとえば、Gen9以前のサーバーで使用されるほとんどのドライブです。
- FCoE、iSCSIストレージ
- GPGPU
- その他のFPGA、アクセラレータ、キーまたはストレージを持つオフロードエンジン

詳しくは
One-buttonセキュア消去

DevIDおよびシステムIAKのOne-buttonセキュア消去

iLO IDevID、iLO LDevID、システムIDevID、およびシステムIAKは、One-buttonセキュア消去プロセス中に削除されます。

Hewlett Packard Enterpriseでは、手動のiLOバックアップを実行して、iLO IDevID、iLO LDevID、システムIDevID、およびシステムIAKを失うことの影響を最小限に抑えることをお勧めします。iLOには、そのバックアップサービスにすべての証明書が含まれます。証明書は、バックアップファイルから復元できます。

詳しくは

iLOのバックアップとリストア
One-buttonセキュア消去

One-buttonセキュア消去のFAQ

One-buttonセキュア消去はUSBデバイスおよび内部SDカードをパージしますか。

いいえ。One-buttonセキュア消去はUSBデバイスおよび内部SDカードをパージしません。

HDDがパージ機能をサポートしていない場合、 One-buttonセキュア消去はパージを試みますか。

いいえ。One-buttonセキュア消去はパージ機能をサポートしていないドライブをスキップします。

One-buttonセキュア消去はSmartアレイコントローラーをサポートしていますか。

One-buttonセキュア消去をサポートするのは、HPE Smartアレイ「SR」コントローラーのみです。

Smartアレイはパージをサポートしていないドライブを消去しますか。

Smartアレイは、パージ操作をサポートしていないドライブをワイプ（あるパターンで上書きする）できます。One-buttonセキュア消去では、Smartアレイでこのセキュリティ保護されていないワイプを実行する必要はありません。Intelligent Provisioningの「システムの消去およびリセット」機能を使用して、このようなドライブのデータをワイプします。

One-buttonセキュア消去はバッテリバックアップ式キャッシュを消去しますか。

詳しくは、次の表を参照してください。

One-buttonセキュア消去は消去コマンドをどのように処理しますか。

One-buttonセキュア消去がデータをパージまたは上書きする方法に関する情報については、次の表を参照してください。

One-buttonセキュア消去を起動するために必要な権限は何ですか。

One-buttonセキュア消去を起動するには、すべてのiLO権限が必要です。

One-buttonセキュア消去はシリアル番号とプロダクトIDを削除しますか。

いいえ、これらの項目はOne-buttonセキュア消去によって消去されません。

この処理はどの程度かかりますか。

ハードウェアによって異なります。HDDのサニタイズはSSDよりも時間がかかります。

One-buttonセキュア消去はサポートされたドライブにどのように作用しますか。

デバイス	必要な操作	結果
NVRAM	3パス書き込み：0x5a、0xa5、0xff	すべてのバッテリバックアップ式iLO SRAMメモリが上書きされます。
内蔵フラッシュ（NAND）	拡張CSDレジスターのSECURE_REMOVAL_TYPEが物理メモリ消去に設定されているeMMC 5.1（JEDEC 84-B51）セキュア消去コマンド（デバイスでサポートされている場合）。	物理メモリ内のデータが消去されます。
インテルOptane DC PMM	完全消去 + DIMMを上書き	暗号化キーが削除され、すべての物理メモリブロック内のデータ（ユーザーがアクセス可能なデータとスペアブロック内の両方のデータ）がゼロで上書きされます。すべての構成とメタデータを含むPCD領域も上書きされます。
NVDIMM-N	JEDEC JESD245B工場出荷時設定	保証情報を除く、すべての物理メモリブロック内のデータが消去されます。読み取り可能なすべてレジスターはデフォルト設定にリセットされます。
UEFI構成ストア	3パス：チップ消去（0xff）、0x00、チップ消去（0xff）	すべての物理セクターが上書きされます。
RTC	時刻を01-01-2001 00:00:00にリセット	日付、時刻、タイムゾーン、およびDSTがデフォルト設定にリセットされます。
TPM	TPMクリア + NVインデックスをクリア + プラットフォーム対象キーを削除	すべての不揮発性情報を含む、TPMのすべてのデータがクリアされます。

デバイス	必要な操作	結果
HPE SmartアレイSRコントローラー	論理ドライブを削除 + 構成のメタデータをクリア + 工場出荷時設定へのリセット + 物理ドライブのサニタイズ **注記**：One-buttonセキュア消去を開始する前に、Smart Storage Administratorを介して、セキュリティリセット機能を手動で実行する必要があります（Smartアレイセキュア暗号化が有効化されていた場合）。	• セキュリティリセット機能は、リモートキー管理のためにキーマネージャーに保存されているドライブキーを削除します。コントローラーおよびドライブのすべてのシークレット、キー、およびパスワードがクリアされます。この操作は、キーマネージャー上のコントローラーキーを削除しません。 • すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。すべてのコントローラー設定は工場出荷時の設定にリセットされます。 • フラッシュバックアップはクリアされ、DRAMのライトバックキャッシュ内のデータは電源が取り外されたときに失われます。 接続されたすべてのドライブをサニタイズする必要があります。ドライブ上で必要な操作については、以下を参照してください。
HPE SmartアレイS100iおよびSR100iソフトウェアRAID	SATA AHCIモードにリセット + 物理ドライブのサニタイズ	コントローラーは、デフォルトのSATA AHCIモードにリセットされます。接続されたすべてのSATAドライブを以下のようにサニタイズする必要があります。
SATA HDD [1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）	CRYPTO SCRAMBLE EXTコマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。
	シングルパスのATA SANITIZE with OVERWRITE EXTオプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターがゼロで上書きされます。キャッシュ内のすべての旧データもアクセスできなくなります。
SATA SSD [1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）	CRYPTO SCRAMBLE EXTコマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。
	シングルパスのATA SANITIZE with BLOCK ERASEオプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロック内の旧データは元に戻すことができなくなります。キャッシュ内のすべての旧データもアクセスできなくなります。
SAS HDD [2]	シングルパスのSCSI SANITIZE with OVERWRITE EXTオプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターが上書きされます。キャッシュ内のすべてのデータもサニタイズされます。
SAS SSD [2]	シングルパスのSCSI SANITIZE with BLOCK ERASEオプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロックがベンダー固有値に設定されます。キャッシュ内のすべてのデータもサニタイズされます。

デバイス	必要な操作	結果
NVM Express	NVM Express FORMAT with Secure Erase Setting (SES) = 2 (サポートされている場合)	これは、暗号化キーを削除することで行われる暗号による消去です。
	シングルパスのNVM Express FORMAT with SES = 1	すべてのネームスペースに関連付けられているすべてのデータとメタデータは破棄されます。NVMサブシステムに存在するユーザーのすべての内容は消去されます。

1 これらのドライブは、HPE Smartアレイ「SR」コントローラーまたはチップセットSATAコントローラーに接続される場合があります。
2 HPE Smartアレイ「SR」コントローラーにのみに接続されたSASドライブがサポートされます。

消去プロセスが失敗するサポート済みデバイス、およびサポートされていないデバイスの消去は安全ではありません。これらのデバイスに機密データが含まれている可能性があります。消去されないデバイスを分離し、他の方法を使用してデータを削除するか、所属する組織のセキュリティポリシーに従ってデバイスを安全に破棄します。

詳しくは

One-buttonセキュア消去

システムの消去とリセット

システムの消去とリセットは、Intelligent Provisioningから開始されます。ハードドライブとIntelligent Provisioningの優先設定がクリアされます。

この機能を使用すると、Intelligent Provisioningによって、DoD 5220.22-Mのガイドラインを使用してドライブ上のデータが上書きされます。この標準は、データの**クリア**に関するNIST SP 800-88最小サニタイズ勧告Revision 1の記述に類似しています。この方法では、3パスプロセスでランダムパターンを適用することにより、システムに接続されているすべてのブロックデバイスがソフトウェアによって上書きされます。この方法を使用して、One-buttonセキュア消去をサポートしていないデバイスを上書きできます。システムにインストールされているストレージの量によっては、上書きプロセスが完了するまでに数時間または数日かかる場合があります。たとえば、ネイティブのサニタイズ方法をサポートしていないドライブに、このオプションを使用します。

△ **注意:**

システムの消去とリセットは、サーバーの廃止または再目的化の場合にのみ、慎重に使用してください。サーバーとiLOは、プロセスが完了するまで複数回再起動することがあります。

消去プロセスでは次が行われます。

- ドライブおよび不揮発性または永続ストレージからデータを消去します。
- iLOをリセットし、保存されているすべてのライセンスを削除します。
- BIOS設定をリセットします。
- 保存されたActive Health System（AHS）および保証データを削除します。
- 展開設定プロファイルを削除します。

他のHPEサーバー管理ツール

詳しくは

HPE InfoSight for Serversセキュリティ
HPE OneViewセキュリティ機能
iLO Amplifier Packのセキュリティ機能
Intelligent Provisioningのセキュリティ

Intelligent Provisioningのセキュリティ

Intelligent Provisioningにアクセスするには、サーバーを再起動してブートプロセス中に正しいキーを押すか、iLO 5のAlways On Intelligent Provisioning機能を使用します。

一部のiLOおよびBIOS設定は、Intelligent Provisioningから構成できます。

iLOによるIntelligent Provisioningのセキュリティ

一部のIntelligent Provisioningのセキュリティ機能はiLOのセキュリティ設定によって異なります。

- iLOは、必要な認証情報と構成可能な暗号化レベルを使用してリモートアクセスを制御します。ユーザーがAlways On Intelligent Provisioningを起動するには、iLO **ホストBIOS**および**リモートコンソール**の権限が必要です。
- Intelligent Provisioningは、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システムでサポートされていません。セキュリティ状態は、iLOの暗号化設定ページで表示し、構成できます。
- リモートコンソールを使用してAlways On Intelligent Provisioningにアクセスする場合、iLOのホスト認証が必要アクセス設定が有効にされている場合に認証情報が必要です。
- サーバーへの物理的アクセスは、組織によって設定された物理的なセキュリティメカニズムによって決まります。

Intelligent ProvisioningはTPM要件に準拠しています。

UEFIを使用したIntelligent Provisioningのセキュリティ

UEFIシステムユーティリティのアドバンストセキュリティオプションでIntelligent Provisioningアクセスを無効にできます。

iLO Amplifier Packのセキュリティ機能

iLO Amplifier Packは、iLO Advancedの機能を活用して、迅速な検出、詳細なインベントリレポート、およびファームウェアとドライバーのアップデートを可能にする、高度なサーバーインベントリとファームウェアおよびドライバーのアップデートソリューションです。iLO Amplifier Packは、ファームウェアとドライバーの大規模アップデートを目的として、サポートされている数千台のサーバーの迅速なサーバー検出およびインベントリを実行します。

サーバーアラート

iLO Amplifier Packを使用して、管理対象サーバーのアラートを表示します。電子メールまたはIFTTTアラートの構成については、iLO Amplifier Packユーザーガイドを参照してください。

リカバリ管理

サーバーシステムリストア機能は、Gen10およびGen10 PlusサーバーのiｌO 5 v2.30以降で機能し、ユーザーが作成したリカバリポリシーに従ってサーバーを復旧します。

iLOがiLO Amplifier Packによって監視されているサーバーでシステムの破損を検出すると、iLOはiLO Amplifier Packに、システムリカバリプロセスを開始して管理するようにアラートを送信します。iLO Amplifier Packは、影響を受けたシステムについてユーザーが定義したリカバリポリシーに対してイベントを照合してから、リカバリポリシーで説明されている通りにリカバリプロセスを開始します。

iLO Webインターフェイスからリカバリイベントを手動で生成するには、管理 - ファームウェア検証ページのリカバリイベントを送信をクリックします。

HPE OneViewセキュリティ機能

HPE OneViewは、単一の統合プラットフォームであり、アプライアンスとしてパッケージ化されています。HPE OneViewにより、物理インフラストラクチャのライフサイクル全体を管理するソフトウェアデファインドアプローチを実現します。

HPE OneViewには、以下のセキュリティ機能があります。

- 以下による必須のアクセス制御：
  - ローカルまたはネットワーク/LDAPアカウント
  - パスワード
  - 詳細な許可（役割とスコープ）
  - 監査ログ
  - Two-Factor認証
- 証明書を使用して認証し、信頼関係を確立します。
- HPEからの定期的なアップデートによってサポートされます。

さらに、HPE OneViewは、以下の機能とセキュリティが強化されたアプライアンスとして提供されています。

- アプライアンスは、不要なすべてのサービスを排除するためにカスタマイズされたオペレーティングシステムを使用し、攻撃対象領域を減らします。
- 機能を提供するために必要なサービスだけを実行することで、その脆弱性を最小限に抑えます。
- パスワードで保護されたOSブートローダー。
- HPE OneViewサービスで必要なポートのみへのアクセスを許可するIPファイアウォール。
- 重要なサービスは、権限があるOSユーザーとして実行されません。
- OSレベルでは、ユーザーは許可されていません。ユーザーは、RESTful API、状態変更メッセージバス（AMPQインターフェイス）、メンテナンス用のSSHやアプライアンスコンソール、またはWebインターフェイスを通じて、厳密にHPE OneViewと対話することができます。

詳しくは、http://www.hpe.com/info/OneView/docsのドキュメントを参照してください。

HPE InfoSight for Serversセキュリティ

HPE InfoSightポータルは、HPEによってホストされている安全なWebインターフェイスで、サポートされているデバイスをグラフィカルインターフェイスによって監視できます。

HPE InfoSight for Servers:

- HPE InfoSightの機械学習と予測分析を、Active Health System（AHS）およびHPE iLOのヘルスおよびパフォーマンス監視と組み合わせて、パフォーマンスを最適化し、問題を予測して防止します。
- AHSからのセンサーデータとテレメトリデータを自動的に収集および分析し、インストールベースの動作から洞察を導き出して、問題の解決とパフォーマンスの向上に関する推奨事項を提供します。

HPE InfoSightおよびセキュリティについて詳しくは、次のドキュメントを参照してください。

- **HPE InfoSight for Serversのセキュリティ**
- **HPE Nimble Storage dHCIソリューションセキュリティガイド**

HPEおよびサードパーティセキュリティソリューション

詳しくは

Microsoft Secured-coreサーバーのサポート
インテルソフトウェアガードエクステンションズ
Intelプロセッサー AES-NIサポート
インテルトラステッドエグゼキューションテクノロジー
Pensando Distributed Services Platform
暗号化とキー管理
AMDメモリ暗号化

Microsoft Secured-coreサーバーのサポート

Microsoft Secured-coreサーバーは、ハードウェア機能、ファームウェアの有効化、およびWindows Server OS機能の組み合わせを使用して、マルウェアおよびルートキットのセキュリティエクスプロイトに対して保護します。

一般に、Secured-coreサーバーは以下を提供します。

- 包括的なセキュリティ – 起動からOS保護まで機能するように設計された単一のイネーブルメントにおける一連の保護。
  - Trusted Platform Module 2.0（TPM 2.0）を使用したハードウェアの信頼のルート。
  - Dynamic Root of Trust of Measurement（DRTM）テクノロジーとDMA保護のプロセッサーサポートによって有効化されたファームウェア保護。
  - 仮想化ベースのセキュリティ（VBS）とハイパーバイザーベースのコード整合性（HVCI）。
- 将来のエクスプロイトや攻撃を防ぐように設計された予防的保守。

Secured-coreサーバーAQ（Additional Qualification）は、Windows Server2022でSecured-core機能をサポートおよび有効化するための追加の要件セットを定義しています。要件を満たすシステムは、**Windows Serverカタログ**にリストされています。

この機能は、UEFIシステムユーティリティとWindows OSの両方で構成が必要です。詳しくは、HPEProLiantサーバー、ストレージ、およびネットワークオプションを使用したMicrosoft Windows Server2022の実装**テクニカルペーパー**をご覧ください。

AMDメモリ暗号化

AMDプロセッサーを搭載したHPEサーバーは、さまざまなタイプのメモリ暗号化をサポートしています。

- セキュアメモリ暗号化（SME）- 特定のコールドブートや物理攻撃からデータを保護するのに役立つ完全なシステムメモリ暗号化。すべての物理メモリを透過的に暗号化し、ソフトウェアの介入やサポートを必要としません。メモリページは、読み取りまたは書き込み時に自動的に復号化および暗号化されます。
- 透過的SME（TSME）- SMEのより厳密なサブセットであるTSMEは、すべての物理メモリを透過的に暗号化し、ソフトウェアの介入を必要としません。メモリページは、読み取りまたは書き込み時に自動的に復号化および暗号化されます。エフェメラル暗号化キーは起動のたびに作成され、ソフトウェアからはアクセスできません。
- Secure Encrypted Virtualization（SEV）- プロセッサーだけが認識している最大509個の一意の暗号化キーの1つによって仮想マシンを保護するのに役立つAMDテクノロジーのセット。

インテルソフトウェアガードエクステンションズ

インテルソフトウェアガードエクステンションズ（SGX）は、特権マルウェアからプラットフォームを保護します。このソリューションにより、アプリケーションはデータとコードをエンクレーブと呼ばれる保護されたメモリ領域にパーティショニングできます。エンクレーブは、エンクレーブ環境の外部で実行されているコードによって読み取りや書き込みを行うことはできません。この機能により、アプリケーションは、障害が発生しているオペレーティングシステム、仮想マシンマネージャー、または別の仮想マシンから機密性の高いコードとデータを保護できます。SGXは、OSにインストールされているインテルSGXドライバーで使用されます。

この機能は、それをサポートするインテルプロセッサーを搭載したGen10 Plusサーバー上のUEFIシステムユーティリティを使用して構成できます。

インテルトラステッドエグゼキューションテクノロジー

インテルトラステッドエグゼキューションテクノロジー（TXT）は、TPMと暗号化技術を使用して、ソフトウェアおよびプラットフォームコンポーネントを測定し、誤動作や侵害されたコンポーネントの実行を防止します。それはシステム構成を変更するソフトウェアベースの攻撃から保護します。この機能は、インテルプロセッサーを搭載したサポートされているサーバーでUEFIシステムユーティリティを使用して構成できます。

サポート情報については、製品のQuickSpecsドキュメント （https://www.hpe.com/info/qs）を参照してください。

IntelプロセッサーAES-NIサポート

Intel AES-NIは、Advanced Encryption Standard（AES）アルゴリズムを改良した暗号化命令セットです。サポートされているプロセッサーでデータ暗号化と復号化を高速化します。AES-NIは、高速のデータ保護と優れたセキュリティを提供し、新しい領域での広範な暗号化を可能にします。

サポート情報については、製品のQuickSpecsドキュメント （https://www.hpe.com/info/qs）を確認してください。

Pensando Distributed Services Platform

サポートされているHewlett Packard EnterpriseサーバーのPensando Distributed Services Platform（DSP）は、ファイアウォール、マイクロセグメンテーション、テレメトリなどのソフトウェア定義サービスの強力なスイートを直接サーバーに提供します。それらのサービスを、ネットワークとサーバー間の移行が発生するサーバーエッジに移動することで、ネットワークとセキュリティのパフォーマンスを向上させます。このソリューションは、セキュリティを向上させると同時に、複数のアプライアンスを置き換え、コストと複雑さを軽減します。

詳しくは、https://www.hpe.com/solutions/Pensandoを参照してください。

暗号化とキー管理

UEFI管理暗号化

UEFI管理暗号化により、 不揮発性メモリモジュールやNVMeドライブなど、サポート対象のシステムデバイスで蓄積データの暗号化が可能になります。

自己暗号化ドライブ

Opal Storage Specificationをサポートするストレージデバイスの場合、ストレージデバイスを自己暗号化（SED）させることで、セキュリティが強化されます。自己暗号化ドライブは、保存されているデータを暗号化して、未認可ユーザーが読み取れないようにします。暗号化キーは、ローカルマスターキー（LMK）またはランダムマスターキー（RMK）を使用して保護されます。

HPE SmartアレイSR Secure Encryption

HPE SmartアレイSR Secure Encryptionは、HPEスマートアレイコントローラーまたはHPEスマートホストバスアダプターに接続されているSAS/SATAドライブ（テープドライブを除く）用のコントローラーベースの蓄積データ暗号化ソリューションです。

HPE SmartアレイSR Secure Encryptionは、HIPPAやSarbanes-Oxleyなどの機密データの規制に準拠するFIPS 140-2レベル1エンタープライズクラス暗号化ソリューションです。暗号化をサポートするコントローラーを使用する場合、暗号化はRAIDボリュームでのみサポートされます。

Secure Encryptionは、ローカルとリモートの両方のキー管理方法で利用できます。リモートキー管理モードには、iLO Advancedライセンスとサポートされているキー管理アプリケーションが必要です。

サーバーまたはコンピューティングモジュールがサポートしているコントローラーを表示するには、次のWebサイトのQuickSpecsドキュメントを参照してください。（https://www.hpe.com/info/qs）を確認してください。

HPE MegaRAID MR Gen10 Plusコントローラー

HPE MegaRAID MR Gen10 Plusコントローラーは、ドライブデータを不正なアクセスや変更から保護する自己暗号化ドライブ（SED）をサポートしています。SEDドライブがストレージシステムから取り外された場合でも、ドライブ上のデータは暗号化されているため、適切なセキュリティ認証がないとアクセスできません。

次のキー管理タイプがサポートされています。

- **パッシブ** - SEDutilなどのサードパーティのキー管理を使用してSEDを管理します。SEDの監視は、HPE MR Storage Administrator、ストレージコマンドラインインターフェイス（StorCLI）ツール、およびUEFIシステムユーティリティで利用できます。
- **ローカル** - HPE MR Storage Administrator、StorCLIツール、およびUEFIシステムユーティリティを使用して、SEDのドライブセキュリティをローカルキー管理用に有効にします。セットアップ時に、セキュリティキー識別子とセキュリティキーを指定します。起動時に、コントローラーに保存されているセキュリティキーがドライブのロックを解除します。ドライブの電源がオフになると、セキュリティが有効になっているドライブのデータ暗号化キーがロックされます。
- **リモート** - UEFIシステムユーティリティは、iLOキーマネージャー構成と連携して、リモートキーマネージャーサーバーにセキュリティキーIDとセキュリティキーを作成します。ドライブの電源がオフになると、セキュリティが有効になっているドライブのデータ暗号化キーがロックされます。起動時に、リモートキーマネージャーサーバーからセキュリティキーが取得され、ドライブのロックが解除されます。

サーバーまたはコンピューティングモジュールがサポートしているコントローラーを表示するには、次のWebサイトのQuickSpecsドキュメントを参照してください。（https://www.hpe.com/info/qs）を確認してください。

リモートキー管理

リモートキーマネージャーは、データ暗号化キーの生成、保存、操作、制御、アクセスの監査を行います。ビジネスに不可欠な機密性の高い保存データの暗号化キーへのアクセスを保護し、維持することができます。

iLOが、キーマネージャーと他の製品との間のキー交換を管理します。iLOは、キーマネージャーとの通信に、自身のMACアドレスに基づいた一意のユーザーアカウントを使用します。このアカウントを最初に作成するために、iLOは、管理者権限を持つ、キーマネージャーに以前から存在する展開ユーザーアカウントを使用します。展開ユーザーアカウントについて詳しくは、キーマネージャーのドキュメントを参照してください。

以下のキーマネージャーがサポートされています。バージョンについては、HPE iLO 5ユーザーガイドを参照してください。

- Utimaco Enterprise Secure Key Manager（ESKM）
- Thales製品：

- Thales TCT KeySecure for Government G350v（旧称SafeNet AT KeySecure G350v）
- Thales KeySecure K150v（旧称SafeNet KeySecure 150v）
- Thales CipherTrust Manager 2.2.0仮想（K170v）および物理（K570）アプライアンス。

  HPEとThalesのパートナーシップについて詳しくは、ここをクリックしてください。

推奨されるセキュリティ設定

このセクションでは、パスワード、iLO、およびUEFIシステムユーティリティに関連する推奨されるセキュリティ対策について説明します。セキュリティ機能の使用については、製品のドキュメントを参照してください。

詳しくは

パスワードに関するガイドライン
iLOセキュリティ設定の推奨事項
UEFIシステムユーティリティのセキュリティ設定に関する推奨事項

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アップデートする場合に、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）。

  iLO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、iLO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適用されます。

iLOセキュリティ設定の推奨事項

Hewlett Packard Enterpriseでは、次のiLOセキュリティ設定をお勧めします。これらの設定について詳しくは、iLO 5オンラインヘルプまたはHPE iLO 5ユーザーガイドを参照してください。設定が推奨事項にリストされていない場合は、環境とセキュリティの優先順位に基づいて適切な値を判断してください。

セキュリティダッシュボード

無視オプション（デフォルト）を設定せずにすべてのセキュリティパラメーターを監視します。

リモートコンソールのセキュリティ

- リモートコンソールのコンピューターロックを有効にして、オプションで、カスタムコンピューターロックキーシーケンスを構成します。
- IRCはiLO内の信頼された証明書を要求しますを有効にして、HTTPS接続を使用して.NET IRCを起動します。

ローカルユーザーアカウントの制御

最小限のアクセスのセキュリティ原則をサポートするさまざまな個々のユーザー権限の設定で、最大12のローカルユーザーアカウントを構成します。

ディレクトリグループアカウントの制御

最大6つのディレクトリグループをKerberos認証またはスキーマフリーディレクトリの統合で使用するように構成します。

キー管理

オプションのキーマネージャーを使用して、データ暗号化キーの生成、保存、操作、制御、アクセスの監査を行います。ビジネスに不可欠な機密性の高い保存データの暗号化キーへのアクセスを保護し、維持することができます。

ファームウェア検証

バックグラウンドスキャンを有効オプションを構成し、整合性障害のアクションを選択します。

サーバーアクセスの設定

- サーバー名 - この値を空白のままにして、ホストOSによって割り当てさせます。
- サーバーFQDN/IPアドレス - この値を空白のままにして、ホストOSによって割り当てさせます。

アカウントサービスのアクセス設定

- 遅延前の認証の失敗時 - 1回目の失敗時では遅延なし（デフォルト）
- 認証の失敗時の遅延時間 - 10秒（デフォルト）
- 認証失敗ログ - 有効-毎回失敗時
- 最小パスワード長 - 8文字（デフォルト）
- パスワードの複雑さ - 有効

iLOアクセス設定

- ダウンロード可能な仮想シリアルポートログ - 無効（デフォルト）
- アイドル接続タイムアウト（分） - 30分（デフォルト）
- iLO機能 - 有効（デフォルト）
- iLO RIBCLインターフェイス - 有効（デフォルト）

  Hewlett Packard Enterpriseは、iLO RESTful APIの使用をお勧めします。
- iLO ROMベースセットアップユーティリティ - 有効（デフォルト）
- iLO Webインターフェイス - 有効（デフォルト）
- 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

  デフォルト値は、構成されたセキュリティ状態によって異なります。

  - 本番環境モード - デフォルトで無効になっています。

- 高セキュリティ – デフォルトで有効になっています。
- FIPSまたはCNSA – デフォルトで有効になっていますが、無効にすることはできません。

- 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（デフォルト）

  シリアルコマンドラインインターフェイス速度も設定する必要があります。
- POST中にiLO IPを表示 – 有効（デフォルト）
- 外部モニターにサーバーヘルスを表示 – 有効（デフォルト）
- VGAポート検出オーバーライド – 有効（デフォルト）
- **仮想NIC** – 無効

  iLOのほとんどのバージョンのデフォルト設定は無効になっています。iLO 5 v2.10では、デフォルト設定は有効になっています。iLOを工場出荷時のデフォルト設定にリセットすると、仮想NIC設定は、iLOのインストールされているバージョンのデフォルト設定に戻ります。ファームウェアのアップグレードまたはダウングレードは、この設定に影響しません。

ネットワークアクセス設定

- 匿名データ – 有効（デフォルト）
- IPMI/DCMI over LAN – 無効（デフォルト、ポート設定を含む）
- リモートコンソール – 有効（デフォルト、ポート設定を含む）
- セキュアシェル（SSH） – 有効（デフォルト、ポート設定を含む）
- SNMP – 無効（ポート設定を含む）

  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。
- 仮想メディア – 有効（デフォルト、ポート設定を含む）
- 仮想シリアルポートログover CLI – 無効（デフォルト）
- Webサーバー – 有効（デフォルト、非SSLおよびSSLポートを設定する必要があります）

  無効にすると、RIBCL、iLO RESTful API 、リモートコンソール、iLO連携、およびiLO Webインターフェイスのアクセスが削除されます。
- 802.1Xサポート – 有効

アップデートサービス設定

- ダウングレードポリシー – ダウングレードの許可（デフォルト）

  △ **注意:**

  この設定を変更する前に、HPE iLO 5ユーザーガイドでオプションを確認してください。
- サードパーティーのファームウェアアップデートパッケージの受け入れ – 無効

iLOサービスポート

- iLOサービスポート – 有効（デフォルト）
- USBフラッシュドライブ – 無効
- 認証が必要 – 有効
- USBイーサネットアダプター – 無効

セキュアシェルキー

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。

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。

スマートカードまたはCAC環境用の認定された証明書

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。

CAC/Smartcardの設定

- CAC Smartcard認証 - 有効（iLO Advanced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証明書がインストールされている必要があります。
- 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

各iLO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。

セキュリティ状態

高セキュリティ（最小）

シングルサインオン

SSO信頼モード - 証明書による信頼

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。

UEFIシステムユーティリティのセキュリティ設定に関する推奨事項

Hewlett Packard Enterpriseは、以下のUEFIシステムユーティリティ設定を推奨します。これらの設定の詳細については、UEFIシステムユーティリティオンラインヘルプまたはHPE ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用UEFIシステムユーティリティユーザーガイドを参照してください。設定が推奨事項にリストされていない場合は、環境とセキュリティの優先順位に基づいて適切な値を判断してください。

電源投入時パスワードの設定

強力なセキュリティ標準に準拠するパスワードを設定します。

管理者パスワードの設定

強力なセキュリティ標準に準拠するパスワードを設定します。

セキュアブート設定

セキュアブートの試行 - 有効

セキュアブートにはUEFIブートモードが必要です。

TLS（HTTPS）の高度なセキュリティ設定

- TLS接続で許可する暗号スイート - TLS接続で許可される暗号を選択します
- すべてのTLS接続の証明書の検証 - Peer
- ホスト名を厳密にチェック - 有効
- TLSプロトコルバージョンをサポート - 自動

プロセッサーAES-NIサポート

有効

Trusted Platform Moduleオプション

- TPM 2.0操作 - アクションなし
- TPMモード切替操作 - TPM 2.0
- TPM 2.0ビジビリティ - 隠さない
- TPM UEFIオプションROM測定 - 有効

SATAコントローラーオプション

- 内蔵SATA構成 - SATAセキュア消去をサポートするには、このオプションを「SATA AHCIサポート」に設定する必要があり、インストールされているSATAドライブがセキュア消去コマンドをサポートしている必要があります。
- SATAセキュア消去 - SATAセキュア消去機能を使用可能にするには、このオプションを有効にします。このコントロールは、セキュア消去機能を起動しません。

インテルセキュリティオプション

- インテルTXTサポート - 使用可能な場合は有効。

アドバンストセキュリティオプション

- ワンタイムブートメニュー（F11プロンプト） - 無効
- Intelligent Provisioning（F10プロンプト） - 有効
- バックアップROMイメージの認証 - 有効

iLO 5構成ユーティリティ

- iLO 5機能 - 有効
- iLO 5構成ユーティリティ - 有効
- ユーザーのログインとiLO 5構成のための構成権限が必要 - 有効
- POST中にiLO 5 IPアドレスを表示 - 有効
- ローカルユーザー - 有効
- シリアルCLIステータス - 有効

- シリアルCLI速度（ビット/秒） - 使用している環境に応じて
- iLO Webインターフェイス - 有効

セキュリティ情報のリソース

セキュリティ報告

HPEセキュリティ報告ライブラリを表示するには、次のWebサイトでセキュリティ報告ライブラリをクリックします。https://support.hpe.com/hpesc/public/home。

セキュリティの脆弱性を報告するには、HPEセキュリティ報告ライブラリWebページのセキュリティ脆弱性の報告リンクをクリックします。

製品のアラート

電子メールのアップデートにサインアップするには、次のWebサイトの製品アラートの受信登録をクリックします。https://support.hpe.com/hpesc/public/home。

サーバーセキュリティおよびインフラストラクチャセキュリティソリューション

https://www.hpe.com/us/en/solutions/infrastructure-security.html

このWebサイトは、記事、プレスリリース、ビデオ、テクニカルペーパーなど、サーバーのセキュリティに関する情報を提供します。

InfusionPointsレポート

- HPEはサプライチェーンのセキュリティをどのように先導しているか
- デバイスIDとコンポーネント認証がHPE Gen10Plusサーバーにやってくる

Ponemon Instituteレポート

Ponemon InstituteによるIT Security Gaps 2020 Global Studyの終了

Moor Insights & Strategyテクニカルペーパー

Hewlett Packard Enterpriseによる包括的なサーバー復元

Project Aurora

https://www.hpe.com/security/ProjectAurora

HPEおよびThales CipherTrustデータセキュリティプラットフォーム

Thales CipherTrust Data Security Platformを使用したHPEサーバーとストレージ

ライセンス

セキュリティ機能のライセンス要件については、HPE iLOライセンスガイド（https://www.hpe.com/support/iLOLicenseGuide-en）を参照してください。

iLOセキュリティビデオ

- HPE iLO 5の上位10のセキュリティ設定。
- HPE iLO 5の推奨されるセキュリティ設定。

HPEリソースライブラリ

https://www.hpe.com/us/en/resource-library.html

サポートと他のリソース

詳しくは

Hewlett Packard Enterpriseサポートへのアクセス
アップデートへのアクセス
リモートサポート（HPE通報サービス）
保証情報
規定に関する情報
ドキュメントに関するご意見、ご指摘

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

  マイHPEソフトウェアセンター

  https://www.hpe.com/software/hpesoftwarecenter
- 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。優れたイベント診断、Hewlett Packard Enterpriseへのハードウェアイベント通知の自動かつ安全な送信を提供します。また、お使いの製品のサービスレベルに基づいて高速かつ正確な解決方法を開始します。Hewlett Packard Enterpriseでは、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勧めします。

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。

HPE通報サービス

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

HPE Pointnext Tech Care

https://www.hpe.com/jp/ja/services/tech-care

HPE Complete Care

https://www.hpe.com/services/completecare

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。ドキュメントの改善に役立てるために、Hewlett Packard Enterpriseサポートセンターポータル（https://www.hpe.com/support/hpesc）にあるフィードバックボタンとアイコン（開いているドキュメントの下部にあります）から、エラー、提案、またはコメントを送信いただけます。すべてのドキュメント情報は、プロセスによってキャプチャーされます。