iLO ファームウェアアップデート補足

本書は、Starter Pack により iLO ファームウェアをアップデートするときの注意事項などについて説明しています。アップデート操作を誤るとサーバーが起動しなくなる等の障害が起きることがありますので、本説明文を最後までよく読み誤操作のないようアップデートしてください。 また、データ書き換え中に予期せぬアクシデント（停電、雷、遮断、ノイズ等）によりサーバーが誤動作したり電源が切断されたりしますと、最悪の場合、機器が損傷し正常動作しなくなります。 このような場合お客様のご負担で修理を必要とすることがありますので十分ご注意ください。

- ファームウェアアップデート中にブラウザーのリロードボタンまたは F5 キーを押さないでください。誤ってそれらの操作をしてアップデートが完了しない状態になった場合は、iLO のリセットを行ってください。
- サーバーに TPM または TM がインストールされている場合、システム ROM(BIOS)または iLO ファームウェアをアップデートする前に、TPM または TM に関する情報を格納するソフトウェアを一時停止またはバックアップしてください。例えば、ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。ソフトウェアの停止をせずにシステム ROM(BIOS)または iLO ファームウェアのアップデートを行った場合、データへアクセスできなくなる可能性があります。TPM または TM を使用するソフトウェアを停止していない状態では、システム ROM(BIOS)または iLO ファームウェアのアップデートを開始しないようにしてください。
- 旧バージョンの iLO ファームウェア(「1.10 Jun 7, 2017」または「1.15 Aug 17, 2017」)が適用されているサーバーに本 iLO ファームウェアを適用した場合、デフォルト設定では「マネージメント」-「アラートメール」ページにおいて「SMTP セキュア接続(SSL/TLS)を有効」が有効になっているため、「SMTP 認証」を行うか、「SMTP セキュア接続(SSL/TLS)を有効」を無効にしてください。設定が旧バージョンのままの場合、アラートメールが送信されなくなります。
- 旧バージョンの iLO ファームウェア(「1.10 Jun 7, 2017」または「1.15 Aug 17, 2017」)が適用されているサーバーに本 iLO ファームウェアを適用した場合、SNMPv3 アラートを再設定してください。アップデート前に SNMPv3 アラート機能を使用していた場合は、本ファームウェア適用後に再設定してください。
- iLO ファームウェア(1.15 Aug 17, 2017)のバックアップとリストア機能を使用してバックアップしたファイルを、本 iLO ファームウェアでリストアしないようにしてください。iLO ファームウェア(1.20 Feb 02 2018)以降でバックアップしたファイルをお使いください。

  iLO ライセンスキーの紛失や HW 障害などによる設定値消失に備え、iLO ファームウェアアップデート実施後にバックアップとリストア機能を使用して iLO 設定のバックアップを行うことを推奨します。

- 本ファームウェアのアップデートとともに以下の各ファームウェアとソフトウェアをアップデートしてください。
  a) システム ROM(BIOS): Starter Pack の Standard Program Package を適用
  b) Agentless Management Service: Starter Pack の Standard Program Package を適用
  c) ESMPRO/ServerAgentService: Starter Pack のバンドルソフトウェアをインストール
  d) 装置情報収集ユーティリティ: Starter Pack のバンドルソフトウェアをインストール
  e) RESTful インターフェースツール: Starter Pack のバンドルソフトウェアをインストール
  f) ESMPRO/ServerManager: 別紙「ESMPRO アップデート補足」を参照
  g) エクスプレス通報サービス(MG)の受信情報設定ファイル: 別紙「ESMPRO アップデート補足」を参照

- IPMI は、その仕様上、パスワードハッシュを取得される脆弱性(CVE-2013-4786)が含まれています。対処方法は、iLO 5 ユーザーズガイドを参照してください。

- 本 iLO ファームウェアでサポートする HTML5 統合リモートコンソール(IRC)は、日本語キーボードの半角/全角、Alt キーの入力ができません。入力できないキーは、OS のスクリーンキーボード機能を使用してください。Alt キーは、HTML5 統合リモートコンソール(IRC)の仮想キーでも使用可能です。

- OS インストール前に本 iLO ファームウェアへのアップデートを行う場合は、OS インストレーションガイドを参照して BIOS/プラットフォーム構成(RBSU)の[Date and Time]-[Time Format]の設定を行ってから本 iLO ファームウェアへのアップデートを実施してください。

  本 iLO ファームウェアへのアップデート後、 BIOS/プラットフォーム構成(RBSU)の[Date and Time]-[Time Format]の設定に合わせて、[iLO Dedicated Network Port] または [iLO Shared Network Port]の[SNTP]-[Time Zone]にタイムゾーンを設定してください。

  ① RBSU の[Time Format]の設定が[Coordinated Universal Time (UTC)]の場合 :

  →RBSU の[Time Zone]と同じ値に設定してください(UTC は GMT に読み替えてください)。

  例) [Time Zone]が”UTC+09:00, Osaka, Sapporo, Tokyo, Soul, Yakutsk”の場合、[Asia/Tokyo(GMT+09:00:00:00)]を選択します。

  ② RBSU の[Time Format]の設定が [Local Time]の場合 :

  →[Local Time]に対応するタイムゾーンを設定してください。

  例) ロケールが日本の場合、”Asia/Tokyo(GMT +09:00:00)”を選択します。

- 信頼された SSL 証明書がインストールされていない状態で、Microsoft Edge 42 を使用して.NET IRC を起動すると、セキュリティアイコンがブラウザーのアドレスバーに表示され、アプリケーションのダウンロードがブロックされます。この場合、以下のいずれかを実施してください。

  - 信頼された SSL 証明書をインストールして、「リモートコンソール & メディア」-「セキュリティ」ページの「IRC は iLO 内の信頼された証明書を要求します」を有効にする。

- ブラウザーのセキュリティアイコンをクリックし、コンテンツを許可するために警告ポップアップの「すべてのコンテンツを表示」をクリックする。
- .NET IRC を使用する場合は Internet Explorer 11 を使用する。

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

- 本 iLO ファームウェアのアップデート後に.NET IRC を使用する場合は、事前に.NET Framework をバージョン 4.5.1 以降に更新してください。更新していない場合、アプリケーション起動時に例外が発生することがあります。

- Microsoft Edge 42 ブラウザー使用時、iLO Web インターフェース上にリモートコンソールのサムネイルが表示されない場合があります。サムネイルを表示させるには Internet Explorer 11 または Microsoft Edge 42 ブラウザー以外のブラウザー(Mozilla Firefox、 Google Chrome モバイルおよびデスクトップ)を使用してください。

- 本 iLO ファームウェアへ適用後、[情報]-[セキュリティダッシュボード]および右上に リスクが表示される場合があります。RBSU や iLO の設定の状態によっては iLO セキュリティのステータスに リスクが表示されますので、お客様のセキュアポリシーに応じてセキュリティの対処をお願いします。推奨値等の詳細は、iLO 5 ユーザーズガイドを参照してください。

  iLO の負荷の状態により[情報]-[セキュリティダッシュボード]の”全体セキュリティーステータス”が『リスク』であっても、iLO Web インターフェース画面の右上部の”iLO セキュリティ”アイコンが無色になる場合があります。[情報]-[セキュリティダッシュボード]の”全体セキュリティーステータス”が現在のセキュリティ状態を示します。

- 本 iLO ファームウェアへ適用後、iLO 拡張ライセンスがインストールされている場合に[アクセス設定]-[アップデートサービス]-[ダウングレードポリシー]の設定で「ダウングレードを永遠に不許可」へ設定しないでください。本設定へ変更後は、iLO に対して永続的な変更が行われるため、iLO インターフェースや各種 ユーティリティから本設定の変更を行おうとしても変更することができません。なお、本設定は BMC 構成ユーティリティの[工場出荷時のデフォルトにセット]オプションにより iLO を出荷時のデフォルト設定に設定を行った場合も、設定はリセットされず「ダウングレードを永遠に不許可」を維持します。

- [セキュリティ]-[アクセス設定]-[iLO]の [ホスト認証が必要]を[有効]に設定した場合、次に示す事象が発生します。

  - ESMPRO/ServerManager のアラートビューアに“Remote Insight/ Integrated Lights-Out 認証されないログイン試行検出“のメッセージが多数表示されます。
  - Standard Program Package (SPP)を適用するとエラーが発生します。

  また、次のサービスや機能をご利用頂けません。

- RAID 通報サービス
- iLO が収集するハードウェアに関するデバイス情報や設定情報の参照、及びイベントログ採取機能

- サーバー起動から OS の起動完了までの間(POST 実行中も含みます)は、iLO の再起動を行わないでください。また、システム ユーティリティの操作途中も、iLO の再起動を行わないでください。

  該当タイミングで iLO の再起動を行うと、期待しない動作となる場合があります。例えば、システムユーティリティの設定変更途中に iLO の再起動を行うと、直後のシステム再起動処理(Reboot)が正常に動作しない場合や、装置に記録されている Serial Number、Product ID などの設定情報を消失する場合があります。

  また、POST 実行中に iLO の再起動を行うと、[情報]-[概要]ページにおける UUID、UUID(論理)が不正な表示になる場合があります。不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

- 以下の条件を満たしている場合、iLO5 ファームウェアバージョン 1.38 以前が、システム ROM v2.00 以降で定義されている PMem 用の温度センサーをサポートしていないため、サーバーの温度が低い状態においても、ファンが高速に回転する場合があります。

  - システム ROM バージョン：v2.00 以降

  - iLO5 ファームウェアバージョン：1.38 以前

  iLO5 ファームウェアをバージョン 1.43 以降にアップデートすることで改善できます。

改版履歴

2021/10/01 iLO ファームウェア 2.55

- システムの再起動後にアダプターの仮想化モードが維持されない場合がある件を改善。
- システムの起動中のデバイスインベントリにおいて、PCIe VDM インターフェースが有効になった後にストレージコントローラー検出を行うように処理を改善。
- iLO が複数回リセットされた場合、OS が NVMe ドライブを検出しなくなる件を改善。
- IPv6 の SLAAC 有効/無効の設定が変更された場合、IPv6 初期化中に IPv6 設定の同期が失敗する場合がある件を改善。
- iLO Web インターフェースの[システム情報]-[ストレージ]において、物理ドライブと論理ドライブのマッピング上限を最大 64 へ拡張。
- スマートアレイコントローラーにおける暗号化が有効な場合にブート時間が長くなる場合がある件と、コントローラが検出されない場合がある件を改善。
- Windows の再起動後に N8103-239(480GB OS ブート専用 SSD ボード (RAID 1))のステータスが不明になることがある件を改善。

- iLO REST ツール、Web インターフェースにおいて、20KB 以上の SSL サーバー証明書のインポートをサポート。
- パスワード認証において、64 文字のパスワードをサポート。
- NVMe M.2 ドライブのヘルス監視処理を NVMe 仕様準拠へ改善。

2021/04/30 iLO ファームウェア 2.44

- 以下の脆弱性の改善。

  CVE-2021-29201 -クロスサイトスクリプティング

  CVE-2021-29204 - クロスサイトスクリプティング

  CVE-2021-29205 - クロスサイトスクリプティング

  CVE-2021-29206 - クロスサイトスクリプティング

  CVE-2021-29207 - クロスサイトスクリプティング

  CVE-2021-29211 - クロスサイトスクリプティング

  CVE-2021-29202 - メモリ破損(バッファオーバーフロー)

  CVE-2021-29208 - DOM ベースクロスサイトスクリプティング、CRLF インジェクション

  CVE-2021-29209 - DOM ベースクロスサイトスクリプティング、CRLF インジェクション

  CVE-2021-29210 - DOM ベースクロスサイトスクリプティング、CRLF インジェクション

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2021-29201	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29202	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:L/A:L	6.4	(AV:L/AC:H/Au:M/C:C/I:C/A:C)	5.9
CVE-2021-29204	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29205	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29206	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29207	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29208	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H	7.6	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1
CVE-2021-29209	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H	7.6	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1
CVE-2021-29210	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H	7.6	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1
CVE-2021-29211	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2

2021/03/08 iLO ファームウェア 2.41

- Treck 社製 TCP/IP スタックの脆弱性(CVE-2020-27337)の改善。

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2020-27337	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	7.3	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	7.5

- iLO のローカルユーザーアカウントの”Role” (権限セット)が”ReadOnly”のアカウントで自身のパスワードを変更する場合に、エラーが発生する件を改善。
- “ホスト認証が必要”が無効の状態で、“セキュリティ設定” をデフォルトに戻す際(例：“高セキュリティ”→”本番環境”)にリセット処理が失敗する場合がある件を改善。
- iLO ファームウェア 1.47 において、VMWare ESXi 稼働中に iLO 5 Channel Interface Driver(CHIF ドライバ)の CHIF エラーを IML にログしてしまう件を改善。
- "smad[]: No response from iLO for Hello"のメッセージが、Red Hat Enterprise Linux のステムログ(SYSLOG)のシステムログにログされる件を改善。
- Linux の VSP(Virtual Serial Port)ターミナルへの 255 文字以上の文字列のコピー/ペーストができない件を改善。

- IPMI コマンドにおいて IPv6 をサポート。
- iLO Web インターフェースの[システム情報]-[メモリ]において、物理メモリ表示に DIMM シリアル番号の表示を追加。
- リモート Syslog 機能有効時、Syslog(オペレーティングシステムのシステムログ)への iLO の”セキュリティログ”のロギング機能を追加。

- RESTful API でのシリアルインターフェースの構成変更機能を追加。
- Redfish のイベントヘッダーに iLO ホスト名を追加。
- iLO Web インターフェースの[電力 & 温度]-[電力メーター]において、インターバルに"1week"を追加。
- POST 中の iLO リセットの抑止機能を追加。
- 7168 ビットより大きい LDAP CA 証明書のインポート機能を追加。
- SSH ログイン時の表示にログインセキュリティバナーの内容を追加。
- iLO Web インターフェースの[情報]-[概要]において、オペレーティングシステムのバージョン表示をサポート。
- iLO Web インターフェースの[情報]-[概要]において、プラットフォームの RAS ポリシー表示をサポート。
- Redfish の標準 Computer System スキーマのリセット、グレースフルリスタートアクションをサポート。
- iLO Web インターフェースの[電力&温度]-[温度]において、CPU パッケージ温度(実温度)を報告するように改善。
- ダイレクトアタッチストレージ(SATA ドライブ)の RESTful API によるロケーション LED 制御をサポート。
- ダイレクトアタッチストレージ(SATA ドライブ)の電源操作機能をサポート。

2020/10/13 iLO ファームウェア 2.31

- リモート Syslog において、非構造化データ形式を RFC5424 に準拠するよう改善。
- VSP(Virtual Serial Port)経由で、NULL 文字が含まれるファイルに対して「cat」または「head」または「tail」コマンドを実行すると VSP がハングするか、NULL 文字の後にファイルをトリミングしてしまうことがある件を改善。
- iLO Web インターフェースで登録された多数のディレクトリグループに対して Kerberos 認証が構成されている場合、ディレクトリグループでのゼロ・サインオンが失敗する場合がある件を改善。
- Gratuitous ARP(Address Resolution Protocol) を使用するネットワークロードバランサーでフェイルオーバーが発生し、ゲートウェイがフェイルオーバーしたことがクライアントに通知された場合に、一部のネットワーククライアントからの通信が iLO 5 に到達できないことがある件を改善。
- I/O デバイスへの MCTP アクセス時に iLO で"device/adapter not responsive"のログが、iLO イベントログ(IEL)に登録されてしまう場合がある件を改善。
- iLO Web インターフェースの仮想ボタン押下によるシャットダウンは、iLO 拡張リセット原因に含まれるように変更。
- iLO Web インターフェースの[ライフサイクル管理]-[破棄]ページにおいて、One-button セキュア消去機能をサポート。
- iLO Web インターフェースの[管理]-[ユーザー管理]- [ローカルユーザーの追加]または [ローカルユーザーの編集]ページにおいて、ユーザーアカウント権限に事前に定義された権限セットやカスタム定義の権限セットを選択設定・変更できる"Role"(役割)を追加。
- HTML5 リモートコンソールモードにスタンドアロンモードと新規ウィンドウモードとを追加。

- iLO Web インターフェースの[電力 & 温度]-[ファン]ページにおいて最小ファン速度と温度構成の表示、[電力 & 温度]-[ファン]-[概要]-[ファン設定]ページにおいて最小ファン速度と温度構成の設定をサポート。
- RESTful での通知に自動修復とセーフモード用のアラートを追加。
- ホスト OS からの仮想 NIC 経由での iLO Web インターフェースへのアクセス時にホスト OS からの要求元として識別できるように強化。
- iLO の工場出荷時デフォルト設定へのリセット(Set to factory defaults)を実行すると、iLO Web インターフェースの[セキュリティ]-[アクセス設定]ページの仮想 NIC の設定が無効となるように変更。
- RESTful API を使用して DIMM シリアル番号の読み取り機能をサポート。

2020/6/22 iLO ファームウェア 2.18

- Ripple20 の複数の脆弱性に対応。この脆弱性は、コードの実行、サービス拒否の原因、機密情報の漏えいのためにリモートから悪用される可能性があります。

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2020-11896	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	8.2	(AV:N/AC:L/Au:N/C:N/I:P/A:C)	8.5
CVE-2020-11898	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5	(AV:N/AC:L/Au:N/C:C/I:N/A:N)	7.8
CVE-2020-11900	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	10.0	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2020-11906	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H	6.4	(AV:A/AC:H/Au:N/C:P/I:P/A:C)	5.8
CVE-2020-11907	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H	5.9	(AV:A/AC:H/Au:N/C:N/I:P/A:C)	5.3
CVE-2020-11911	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L	3.7	(AV:N/AC:H/Au:N/C:N/I:N/A:P)	2.6
CVE-2020-11912	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	3.7	(AV:N/AC:H/Au:N/C:P/I:N/A:N)	2.6
CVE-2020-11914	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	3.1	(AV:A/AC:H/Au:N/C:P/I:N/A:N)	1.8

2020/2/11 iLO ファームウェア 2.14

- 以下のアクセラレーターを新規サポート。
  - Xilinx Alveo U250
  - Xilinx Alveo U50

- RESTful API 経由で Inlet Ambient センサーのユーザー定義可能な事前警告閾値を参照・設定できる機能をサポート。

2019/10/30 iLO ファームウェア 2.10

- iLO ファームウェアによってログされるセキュリティイベントの[情報]-[セキュリティログ]への追加。
- [管理]-[ファームウェア検証]にファームウェアの検証機能を追加。
- POST 実行中のファームウェア改ざん検知/リカバリを行うセキュアスタート検証に System Programing Logic Device(CPLD)の検証を行うように機能拡張。
- Intelligent System Tuning メニュー名とパフォーマンス管理機能名を変更。
- リカバリイベントのアラートを追加。
- iLO のセキュリティ設定において、セキュリティ状態に CNSA モードをサポート。
- iLO のセキュリティ設定において、高度なセキュリティ/FIPS/CNSA が設定されたサーバーでの Smart Update Manager(SUM)/Smart Update Tools(SUT)をサポート。
- UEFI システムユーティリティを使用してダイレクトアタッチストレージ(DAS)を更新するためのファームウェアのステージングをサポート。
- ドライブベイのマッピング情報のインポートおよびエクスポート機能を改善。
- 執拗なフラッシ攻撃から iLO ファームウェア、システム ROM、CPLD を保護するために日毎のアップデート可能な回数制限を追加。
- Active Health System(AHS)ログにパフォーマンスデータのログを追加するように改善。
- SSL サーバー証明書のサイズ制限を 4096 から 8096 バイトへ拡張するように改善。
- 仮想 NIC の工場出荷時のデフォルト設定を有効に変更。
- 下記のシステム診断機能をサポート。
  - セーフモードで起動 - 安全な最小構成でサーバーを起動できます。
  - インテリジェント診断モードで起動 - システムは POST 中に起動エラーを自動的に診断できます。
  - 工場デフォルト設定を復元 - すべての BIOS 構成設定を工場デフォルト値にリセットします。これにより、ブート構成、セキュアブートのセキュリティキー(セキュアブートが有効な場合)、構成された日付時刻の設定など、すべての UEFI 不揮発性変数が削除されます。
  - システムデフォルト設定の復元 - すべての BIOS 構成設定をデフォルト値にリセットしてサーバーを再起動します。このオプションは一部の UEFI 設定を保持します。
- iLO のタイムゾーンの選択肢がシステム ROM のタイムゾーンの選択肢と同じになるように改善。下位バージョン互換のため RESTful API で旧タイムゾーン選択肢または新しい選択肢のどちらも使用することができます。

- システム GPU の GPU バージョン情報が表示されない場合がある件を改善。
- 誤った消費電力情報が AHS ログ内に保存されてしまうことがある件を改善。

- Domain Name System(DNS)が利用できない場合に、サーバーが起動中に最大 3 分間無応答になることがある件を改善。

2019/10/14 iLO ファームウェア 1.47

- 最後の OS 再起動から 49.5 日以上連続稼働している状態で iLO リセット(ファームウェアアップデート含む)を実行すると、iLO 時刻が数か月以上過去に遡ってしまう可能性がある件を改善。

2019/06/27 iLO ファームウェア 1.45

- iLO ファームウェア 1.43 において iLO への RESTful API アクセスが高頻度に行われると、Web インタフェースへの HTTP/HTTPS 接続が不可となることがある件を改善。

2019/05/23 iLO ファームウェア 1.43

- iLO 専用ネットワークポート、または iLO 共有ネットワークポートとスイッチングハブの両方の通信速度が 100BASE-T フルデュプレックスに設定し接続 されている場合、稀に通信ができなくなることがある件を改善。
- RESTful インタフェースツール(ilorest)の serverlogs コマンドにオプション以外の文字列が含まれている場合においてもコマンドが成功するよう改善。
  例:ilorest -d serverlogs --selectlog=IML --clearlog rc 255
  ※下線部分：オプション以外の文字列
- iLO Web インターフェースの電力メータ表示において、ピーク電力(最大電力)の測定値が電源容量を超える場合がある件を改善。本件に伴い例えば以下のような IML エントリが記録されてしまう件を改善。
  例:Server power: %1W exceeded the redundant power capacity threshold: %2W
  ※%1: 平均電力読み取り値、%2:電力閾値(電源容量)
- iLO 専用ネットワークポート、または iLO 共有ネットワークポートのタイムゾーン設定における選択肢の "Asia/Taipei"を"Beijing, Chongqing, Hong Kong, Urumqi, Taipei, Perth"へ変更。

- iLO 専用ネットワークポートに VLAN 機能をサポート。
- iLO リセット後に SNMPv3 エンジン ID を自動生成するように機能を強化。
- iLO 負荷軽減のため RESTful API の処理を改善。
- BIOS/プラットフォーム構成(RBSU)の”Set Admin Password”にパスワードが設定されている状態で、ローカルからの RESTful API アクセス時に認証なしでログインできるよう改善。
- Red Hat Enterprise Linux 7 および VMware ESXi 6.x 環境における iLO と iLO ドライバ間のメモリ管理機能を強化。
- Express5800/R120h-2M において、オプション PCI カードを 8 枚搭載した構成で、バックアップ・リストア機能の操作を行うと、稀に処理が完了しないことがある件を改善。

2019/02/05 iLO ファームウェア 1.40

- 電源装置のステータス変化(AC ロスト、ケーブル抜け、エラー等)が遅延する場合がある問題を改善。
- 本装置未サポートの PCI カードがインストールされた状態で、Internet Explorer 11 で iLO Web インターフェースを使用している場合、デバイスインベントリでパースエラーが表示される場合がある問題を改善。
- UID 操作の連続実行で、ごく稀にサーバーの電源がオフになる問題を改善。
- Express5800/R120h-2M に N8104-179 ネットワークカードを搭載した構成で、下記の設定項目において[Always Power On]が設定されている場合、シャットダウン後に直ぐにサーバーを起動してしまう問題を改善。
  - RBSU:[System Option s]-[Server Availability]-[Automatic Power-On]
  - iLO Web インターフェース:[Power & Thermal]-[Server Power]-[System Power Restore Settings]-[Auto Power-On]
- インストールされているすべてのモニターのビデオを表示するように"VGA ポート検出オーバーライド"機能を改善。
- 断続的なファイルのアップロードエラー問題を改善。
- FIPS モードにおける仮想メディアの問題、仮想 DVD とフロッピーの同時使用の問題を改善。
- VMWare ESXi 7 インストールドライバーと共に使用する場合の USB フロッピー問題を改善。
- ディスクドライブの過熱イベントの誤検出問題を改善。
- 本体装置に複数の NIC カードが取り付けられている構成の場合、サーバー起動時に RESTful API エラーが発生する問題を改善。
- 匿名データの XML 応答に NIC 情報が含まれない問題を改善。
- 以下のような、IPMI で NIC のリンクロストの誤検出問題を改善。
  VMware ESXi 6.0/6.5/6.7 を使用している場合、OS 起動時に vSphere Web Client の[監視]-[センサー]-[ハードウェアステータス]において NIC ポートセンサの健全状態に警告が表示される。
- POST 中にエラーコード(270/329/338)が表示される問題を改善。
- 本体装置のリセット後に、[システム情報]-[デバイスインベントリ]において RAID カード等の PCIe カードのステータスが”Unknown”と表示される場合がある問題、[ストレージ]においてストレージ情報が表示されない場合がある問題を改善。

- [ファームウェア & OS ソフトウェア]-[メンテナンスウィンドウ]にメンテナンスウィンドウの編集機能を追加。
- [セキュリティ]-[アクセス設定]-[アカウントサービス]に[パスワードの複雑さ]設定を追加。
- [セキュリティ]-[アクセス設定]-[iLO]に[外部モニターにサーバーヘルスを表示]設定を追加。
- [セキュリティ]-[アクセス設定]-[アップデートサービス]に[ダウングレードポリシー]設定を追加。
- [セキュリティ]-[アクセス設定]-[iLO]に[仮想 NIC]設定を追加。
- RESTful API と EXPRESSBUILDER にワンタッチセキュアイレース機能をサポート。
- RESTful API での LDAP/ディレクトリ設定をサポート。
- セキュリティダッシュボートをサポート。セキュリティダッシュボートは、重要なセキュリティ項目の状態や潜在リスクのため設定を評価します。

- [システム情報]-[ストレージ]において、SSD ドライブ情報(電源オン時間、見積もり余寿命、及び余寿命)の表示をサポート。
- RESTful API 経由で不揮発メモリに iLO 構成設定のコピーをバックアップ、不揮発メモリからリストアする機能を追加。
- Intelligent System Tuning に以下の新機能を追加。
  - パフォーマンス監視 - Innovation Engine によりサーバーから収集したパフォーマンスデータを参照することができます。
  - ワークロードパフォーマンスアドバイザー - サーバーのパフォーマンスを向上させるためのサーバーのチューニングの推奨事項を提供します。
- マザーボード搭載不揮発性メモリ領域(NAND)の管理機能を強化。
- 以下の脆弱性に対応。
  - リモートクロスサイトスクリプティング(XSS)(CVE-2018-7117)の脆弱性問題を改善。
  - ローカルセキュリティ制限回避(CVE-2018-7113)の脆弱性問題を改善。
  - リモートクロスサイトスクリプティング(XSS)(CVE-2019-11982)の脆弱性問題を改善。
  - SMASH-CLP におけるバッファオーバーフロー(CVE-2019-11983)の脆弱性問題を改善。

CVE-ID	V3		V2	
	Vector	Basic Score	Vector	Basic Score
CVE-2018-7113	AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L	6.4 (Medium)	(AV:L/AC:L/Au:N/C:C/I:C/A:P)	6.8 (Medium)
CVE-2018-7117	AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H	7.6(High)	(AV:A/AC:L/Au:S/C:P/I:C/A:C)	7.4(High)
CVE-2019-11982	AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H	8.3(High)	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6(High)
CVE-2019-11983	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H	7.0(High)	(AV:N/AC:M/Au:N/C:P/I:P/A:C)	8.3(High)

2018/09/11 iLO ファームウェア 1.38

- Linux または VMware 環境において、システム運用中に OS パニックまたはストールを発生させる可能性がある問題を改善。

2018/08/14 iLO ファームウェア 1.35

- 誤ったスマートアレイの異常報告(キャッシュモジュールボードのバックアップパワー異常)をする問題を改善。
- バーチャルメディアがイジェクトされた後に iLO が無応答になる問題を改善。
- VGA ポートのオーバーライド機能をサポート(検出されたビデオポートに接続されるデバイスを制御)。自動検出機能により異常なポート電圧からシステムを保護します。
- iLO RESTful API 経由での DHCP クライアント ID のオーバーライド機能をサポート。
- iLO Web インターフェースにおいて、ユーザー、グループ、セッション情報において表示対象ユーザーまたはグループでサポートされている権限レベルを示すアイコンを変更。

- 以下の脆弱性に対応。
  - リモートから任意のコードを実行される脆弱性(CVE-2018-7105)。

CVE-ID	V3		V2	
	Vector	Basic Score	Vector	Basic Score
CVE-2018-7105	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2(High)	(AV:N/AC:L/Au:S/C:C/I:C/A:C)	9.0(Critical)

2018/05/31 iLO ファームウェア 1.30

- バーチャルメディアで OS のインストールを行う際に、iLO 共有ネットワークポートが構成されている場合にインストールが失敗する問題を改善。
- 有効な SSH セッションを使い切ってしまう問題を改善。
- iLO5 の設定が工場出荷状態に戻ってしまう問題を改善。
- iLO Web インターフェースの"電力 & 温度"-"サーバー電源"ページの"システム電源リストア設定"-"サーバーの自動電源オン"設定で、"常に電源オン"、"最新の電源状態をリストア"が設定されている場合、サーバーのリセット後に電源オンしない問題を改善。
- iLO Web インターフェースの"システム情報"-"ストレージ"ページで表示される NVMe ドライブモデル番号が正しくない/矛盾している問題を改善。
- iLO Web インターフェースの"セキュリティ"-"アクセス設定"ページの"Web サーバー非 SSL ポート"にデフォルト以外のポート番号が設定された場合に EXPRESSBUILDER が、"Web サーバーSSL ポート"にデフォルト以外のポート番号が設定された場合には JAVA IRC が、それぞれ起動されない問題を改善。
- iLO Web インターフェースの"システム情報"-"ネットワーク"ページにおいて、Express5800/R120h-1M、R120h-2M 標準ネットワークコントローラの MAC アドレスが表示されない問題を改善。
- iLO Web インターフェースでタイムゾーンの設定がされた場合、iLO イベントログまたはインテグレーテッドマネジメントログの最終更新時刻が UTC 時間となるように対応。

- NAND 寿命延長のため 4 GB マザーボード搭載不揮発性メモリ(NAND)への書き込みアルゴリズムを改善。
- HTML5 統合リモートコンソール(IRC)のパフォーマンス向上と以下の機能を追加。
  - 統合リモートコンソール(IRC)の設定に日本語/英語キーボード選択、仮想キーを追加。
  - バーチャルメディアでローカル ISO、IMG ファイルのリダイレクションをサポート。
- 以下のファームウェア、ソフトウェアアップデート機能を改善。
  - メンテナンスウィンドウの参照、作成、削除を追加。
  - インストールセットがインストールキューに追加されている際にインストレーションキューをクリアするためのチェックボックスを新規追加。
  - インストレーションタスク完了時にリブートが必要な通知を RESTful API と Web インターフェースに追加。
  - iLO 開始時に iLO 設定情報を NAND 領域にバックアップするよう改善。
- アラートメールでセキュアメールのため SSL/TLS をサポート。
- アラートメールで外部 SMTP サーバーをサポート。
- ホストの全 NIC ダウンの SNMP トラップを追加。

- OpenSSL 1.0.2u をサポート。
- iLO Web インターフェースの"ファームウェア & OS ソフトウェア"-"ファームウェア"ページにオープンソースリストの表示機能を追加。
- iLO Web インターフェースに Intelligent System Tuning を新規サポート。iLO Web インターフェースに Jitter Smoothing 設定・参照機能を追加。Workload Matching、Core Boosting を設定するための EXPRESSBUILDER 起動を追加。
- iLO Web インターフェースの"情報"-"概要"ページに iLO ヘルスステータスを追加。
- Java IRC、.NET IRC の証明書期限の延長。
- SSL 証明書の削除機能及び iLO 自己証明書の再発行機能を追加。
- RSA-PSS 署名のサポートを追加。
- NAND 寿命延長のため Active Health System ログを改善。
- iLO Web インターフェースの"セキュリティ"-"アクセス設定"ページの"アクセスオプション"の"XML Reply"を"Anonymous Data/匿名データ"に変更。
- iLO Web インターフェースの"セキュリティ"-"暗号化"ページの"セキュリティ設定"の"製品"を"本番環境"に変更。
- iLO Web インターフェースの"電力&温度"-"電力"ページの"電力しきい値超過による SNMP アラート"の"Warning Threshold"を"警告しきい値"に変更。
- 以下の脆弱性に対応。
  - ローカル/リモートコード実行(CVE-2018-7078)の脆弱性問題を改善。
  - DoS(CVE-2018-7101)の脆弱性問題を改善。

CVE-ID	V3		V2	
	Vector	Basic Score	Vector	Basic Score
CVE-2018-7078	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2(High)	(AV:N/AC:L/Au:S/C:C/I:C/A:C)	9.0(Critical)
CVE-2018-7101	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5(High)	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	7.1(High)

2018/02/02 iLO ファームウェア 1.20

- 英語キーボード環境での HTML5 統合リモートコンソール(IRC)をサポート。
- 統合リモートコンソール(IRC)でのマウスホイールをサポート。
- iLO 共有ネットワークポート経由での IPv6 通信をサポート。
- iLO 共有ネットワークポート経由での iLO 連携機能をサポート。
- RSA-PSS アルゴリズムの SSL 証明書のインポートをサポート。
- SNMPv3 Inform アラートをサポート。
- 送信先ごとに SNMPv1 Trap・SNMPv3 Trap・SNMPv3 Inform を選択できるよう SNMP アラート機能を強化。
- SNMPv3 ユーザーごとにエンジン ID を設定できるよう SNMP アラート機能を強化。
- 登録可能な SNMP アラート送信先を最大 8 カ所に拡張。
- 登録可能な SNMPv3 ユーザーを最大 8 ユーザーに拡張。
- 定期的な HSA Trap 機能をサポート。

- iLO Web インターフェースの"ファームウェア & OS ソフトウェア"ページに、"キューに追加"ボタンを追加。
- iLO Web インターフェースの"ファームウェア & OS ソフトウェア"ページに、"すべて削除"ボタンを追加。
- iLO Web インターフェースの"ファームウェア & OS ソフトウェア"ページに、"リカバリセットをアップデート"オプションを追加。
- iLO Web インターフェースに表示される、OS にインストール済み・動作中ソフトウェア名の日本語表示をサポート（Agentless Management Service のアップデートが必要）。
- RESTful API で NVMe ドライブのプロパティをサポート
- RESTful API でデバイスインベントリをサポート。
- 管理用ソフトウェア等で使用する iLO ユーザーアカウントを区別するため、"サービスアカウント"オプションをサポート
- システム LAN ポートリンクアップ・リンクダウン時に記録される IML イベントを変更。
- アラートメール本文に正しい システム ROM（BIOS）バージョンが記載されない問題を改善。
- 同時に 2 つの仮想メディアをマウントすると、仮想メディアデバイスにアクセスできなくなることがある問題を改善。
- スクリプト仮想メディアで接続したフロッピーイメージが常に読み込み専用としてマウントされる問題を改善。
- リモート Syslog サーバーのアドレスを FQDN で設定した場合に、アラートが送信されなくなることがある問題を改善。
- SMTP サーバーを FQDN で設定し、名前解決時に IPv6 アドレスが返される場合に、アラートが送信されないことがある問題を改善。

2017/08/17　iLO ファームウェア 1.15

- iLO 設定のバックアップとリストア機能をサポート。
- SSH 鍵交換認証方式として diffie-hellman-group-exchange-sha256 をサポート。
- アラートメールの宛先でセミコロン区切りでの複数アドレス指定をサポート。

- RESTful API で Power Cycle 操作をサポート。
- RESTful API で電源装置の高効率モードの設定をサポート。
- RESTful API でキャッシュモジュールのシリアル番号の取得をサポート。
- RESTful API でログインセキュリティバナーの設定をサポート。
- RESTful API でシステムが電源投入されてからの経過時間の取得をサポート。
- RESTful API でマウスとキーボードの持続接続の設定をサポート。
- RESTful API で使用中の Cipher Suite の取得をサポート。
- AC ON 後初回の POST 時に iLO が SNTP サーバーから取得した時刻をホストに転送する機能をサポート。
- システムリセット後、iLO Web インターフェースに断続的に不正なメモリステータスが表示される場合がある問題を改善。
- iLO Web インターフェースのサーバー電源ページの応答を改善。
- Java IRC において、仮想メディアのステータスが表示されない場合がある問題を改善。
- Java IRC の使用中に、ローカルクライアントのキーボードが無効になる場合がある問題を改善。
- 最大利用可能電力が正しく表示されない場合がある問題を改善。

- IML にメンテナンスノートが含まれる場合、ログ削除に失敗する場合がある問題を改善。
- RESTful API からセキュアブートの設定を行えない場合がある問題を改善。
- RESTful API からブート順序設定を取得できない場合がある問題を改善。
- RESTful API で iLO にインストールされている SSL 証明書を削除した際に、iLO Web インターフェースがエラーする問題を改善。
- サポートされていない文字を含むグループ名が指定された場合に、iLO 連携機能で認証エラーが発生する場合がある問題を改善。
- 一部のセキュリティスキャナーにおいて、セキュアではないキャッシュマネジメントポリシーの問題が誤検出される問題を改善。
- グループキーが 1 バイトまたは 2 バイトの iLO 連携グループを作成できない問題を改善。

2017/06/07　iLO ファームウェア 1.10

- 初版。