Hewlett Packard Enterprise

HPE ProLiant Gen10 サーバー、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およびシェルリリースノート（2019 年 12 月）

部品番号: 881333-199
発行: 2019 年 12 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。

Intel®、インテル、Itanium®、Pentium®、Intel Inside®、および Intel Inside ロゴは、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。

UEFI®は UEFI Forum, Inc.の登録商標です。

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

リリースノート

説明

HPE ProLiant Gen10 サーバー、ProLiant Gen10 Plus、および HPE Synergy コンピュートモジュールには、システム ROM に内蔵された UEFI（Unified Extensible Firmware Interface）システムユーティリティが組み込まれています。

HPE ProLiant Gen10 サーバー、ProLiant Gen10 Plus、および HPE Synergy モジュールは、UEFI 仕様のバージョン 2.7（**http://www.uefi.org/specifications** で入手可能）および UEFI クラス 2 のシステムファームウェアに適合しています。

UEFI システムユーティリティを使用すると、次のような広範な構成作業を実行できます。

- システムデバイスと取り付けられているオプションの構成
- システム機能の有効化および無効化
- システム情報の表示
- プライマリブートコントローラーまたはパーティションの選択
- メモリオプションの構成
- 内蔵 UEFI シェルや Intelligent Provisioning のような他のプリブート環境の起動

詳しくは、以下を参照してください。

- **重要な UEFI 要件**（Hewlett Packard Enterprise の Web サイト：**https://www.hpe.com/info/UEFI/docs**）
- UEFI の仕様（**http://www.uefi.org/specifications**）

バージョン

- インテル Xeon スケーラブルパフォーマンスシリーズプロセッサーで構成される HPE ProLiant、Synergy、および Apollo Gen10 サーバー：2.17
- AMD EPYC プロセッサーで構成される HPE ProLiant Gen10 サーバー：1.40
- AMD EPYC プロセッサーで構成される HPE ProLiant Gen10 Plus サーバー：1.10（初期リリース）

旧バージョン情報

- インテル Xeon スケーラブルパフォーマンスシリーズプロセッサーで構成される HPE ProLiant、Synergy、および Apollo サーバー：2.16
- AMD EPYC プロセッサーで構成される HPE ProLiant サーバー：1.34

製品モデル

このリリースは、すべての ProLiant Gen10 サーバー（HPE ProLiant MicroServer Gen10 は除く）、ProLiant Gen10 Plus、および HPE Synergy コンピュートモジュールに適用されます。

オペレーティングシステム

オペレーティングシステムおよび仮想化ソフトウェアのサポートについては、**http://www.hpe.com/servers/ossupport** の OS サポートサイトを参照してください。

セキュアブートは、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 および Linux の最新バージョンを実行するシステムで使用できます。

言語

このリリースでサポートされる言語は、英語、日本語、および簡体字中国語です。

ファームウェアまたはシステム ROM のアップデート

- インテル：推奨事項 — Hewlett Packard Enterprise では、可能な限り速やかにこのバージョンのファームウェアに更新することをお勧めしています。
- AMD: 推奨事項 — Hewlett Packard Enterprise では、可能な限り速やかにこのバージョンのファームウェアに更新することをお勧めしています。

インストール手順については、次のドキュメントを参照してください。

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

部品番号：881334-198

版数：1

ブート方法の作成

ブート方法の作成について詳しくは、**https://www.hpe.com/info/UEFI/docs** にある 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。

機能強化

このリリースの UEFI 機能強化は、以下のとおりです。

- Gen10 Plus サーバーのサポート
- HPE One button セキュア消去のサポート。このオプションは、HPE Intelligent Provisioning アプリケーションから、または HPE RESTful API を介して起動し、システムを安全にデフォルト構成に復元することができます。このオプションは、iLO ファームウェア 1.40 以降、および Intelligent Provisioning 3.30 以降も必要です。
- セキュア設定ロック機能を追加しました。この機能を有効にすると、システムハードウェア、セキュリティ設定、またはファームウェアのリビジョンの変更を検出して、悪意のあるまたは意図しないサーバーの変更から保護することができます。この保護は、工場から顧客サイトへの移行中、ある顧客サイトから別の顧客サイトへの移行中のシステムに対して有効にすることも、展開されたサーバーで有効のままにすることもできます。この機能を有効にして構成するために、サーバーセキュリティオプションの新しい BIOS/プラットフォーム構成（RBSU）サーバー構成ロックメニューが使用可能です。

- システムのデフォルトオプションに新しい BIOS/プラットフォーム構成（RBSU）バックアップおよび復元設定メニュー。このオプションは、現在の BIOS 構成を USB ストレージデバイスにバックアップ（保存）して別のサーバーに移行するために使用できます。
- 最新の GPU アダプターをサポートするためにシステムのサーマルロジックを修正しました。
- システムユーティリティのための言語翻訳（英語以外のモード）をアップデートしました。
- 最新の BIOS/プラットフォーム構成オプションに対応するように RESTful API HPE BIOS 属性レジストリリソースをアップデートしました。
- RBSU 検索オプション

注記: すべてのプロセッサーですべての機能が使用できるわけではありません。

バックアップおよびリストア設定の変更

バックアップファイルには、シリアル番号と製品 ID 情報が含まれます。バックアップからリストアする場合、この情報をシステムに適用するかどうかを求められます。バックアップを使用して新しいシステムをセットアップする場合は、シリアル番号と製品 ID のリストアを省略できます。

デバイス暗号化設定を変更するには、**システム構成** > **BIOS/プラットフォーム構成（RBSU）** > **サーバーセキュリティ** > **デバイス暗号化オプション** > **デバイス暗号化移行オプション**にアクセスします。

手順

1. **システムユーティリティ**画面で、**システム構成** > **BIOS/プラットフォーム構成（RBSU）** > **システムデフォルトオプション** > **バックアップおよびリストア設定**を選択します。
2. 次のいずれかを実行します。
   a. **バックアップ**を選択します。
   b. **リストア**を選択します。
3. 手順に従って、バックアップファイルがある場所に移動するか、バックアップファイルを作成する場所に移動します。

   注記: バックアップをリストアする場合、バックアップファイルは`.json`か`.zip`ファイルである必要があります。
4. **操作を開始**をクリックします。

修正点

本リリースでは、以下の項目が修正されました。

- インテルプロセッサー：
  - さまざまなセキュリティ脆弱性に対する緩和策を提供する UEFI EDK2 サポートの最新版が含まれています。次の脆弱性は、このシステム ROM リリースで対応済です。CVE-2018-3613 CVE-2017-5731、CVE-2017-5732、CVE-2017-5733、CVE-2017-5734、CVE-2017-5735、CVE-2018-3630、CVE-2018-12178、CVE-2018-12179、CVE-2018-12180、CVE-2018-12181、

CVE-2018-12182、および CVE-2018-12183。これらのセキュリティ脆弱性は、HPE サーバーに固有のものではありません。

- 特定のプロセッサー（i3、Pentium、または Celeron）が BIOS/プラットフォーム構成（RBSU）で SGX のサポートを誤って表示していました。SGX 対応の i3、Pentium、または Celeron プロセッサーを使用しているお客様は、ML30 Gen10 1.20_01_28_2019 以降の BIOS バージョンにアップデートする前に、SGX で保護されたデータをすべてバックアップする必要があります。そうしないと、SGX で保護されたデータにアクセスできなくなります。この問題は HPE サーバーに固有のものではありません。
- 特定の PCIe オプションカードが正しくトレインされず、POST 中にシステムがハングアップすることがあります。この問題は HPE サーバーに固有のものではありません。
- システムがレガシーブートモードに構成されているときに SD カードが内部 SD スロットに取り付けられていると、システムが HPE 8GB デュアル microSD フラッシュ USB ドライブから正しく起動しない場合があります。この問題は、UEFI ブートモードのシステムには影響しません。
- システムが UEFI ブートモードに構成されている場合、システムリセット後に特定のサードパーティ製 USB ドライブキーが正しく機能しないことがあります。
- HPE CN1000E-T アダプターがレガシーブートモードで正しく起動しない場合があります。この問題は、UEFI ブートモードで構成されているシステムには影響しません。
- HPE RESTful API を通じてステージングされたファームウェアアップデートが、次回の起動時に正しく実行されず、iLO ファームウェアインストールキューに例外としてマークされることがあります。
- iLO リモートコンソールの次のリセット時に起動オプションとメディア - 仮想メディア設定を設定した後に、iLO 仮想メディアが正しく起動しないことがあります。
- System Utilities Embedded Applications または UEFI Shell の AHS Download アプリケーションが、iLO ファームウェア 1.30 以降で正しく機能しないことがあります。
- UEFI シェルの `sysconfig` コマンドがオプションの設定に失敗したり、応答しなくなったりすることがあります。
- オプションの SATA DVD ドライブがロック解除されず、オペレーティングシステムの再起動後にメディアを取り出すことができない場合があります。
- SATA M.2 ドライブを取り付けたままレガシーブートモードで起動すると、システムが起動中に応答しなくなり、レッドスクリーン（RSOD）が発生する場合があります。この問題は、UEFI ブートモードのシステムには影響しません。
- HP AF611A KVM などの USB KVM がシステムの再起動後に正しく機能しないことがあります。

- AMD プロセッサー：
  - さまざまなセキュリティ脆弱性に対する緩和策を提供する UEFI EDK2 サポートの最新版が含まれています。次の脆弱性は、このシステム ROM リリースで対応済です。CVE-2018-3613 CVE-2017-5731、CVE-2017-5732、CVE-2017-5733、CVE-2017-5734、CVE-2017-5735、CVE-2018-3630、CVE-2018-12178、CVE-2018-12179、CVE-2018-12180、CVE-2018-12181、CVE-2018-12182、および CVE-2018-12183。これらのセキュリティ脆弱性は、HPE サーバーに固有のものではありません。
  - システムがレガシーブートモードに構成されているときに SD カードが内部 SD スロットに取り付けられていると、システムが HPE 8GB デュアル microSD フラッシュ USB ドライブから正しく起動しない場合があります。この問題は、UEFI ブートモードのシステムには影響しません。
  - システムが UEFI ブートモードに構成されている場合、システムリセット後に特定のサードパーティ製 USB ドライブキーが正しく機能しないことがあります。

- HPE CN1000E-T アダプターがレガシーブートモードで正しく起動しない場合があります。この問題は、UEFI ブートモードで構成されているシステムには影響しません。
- HPE RESTful API を通じてステージングされたファームウェアアップデートが、次回の起動時に正しく実行されず、iLO ファームウェアインストールキューに例外としてマークされることがあります。
- iLO リモートコンソールの次のリセット時に起動オプションとメディア - 仮想メディア設定を設定した後に、iLO 仮想メディアが正しく起動しないことがあります。
- System Utilities Embedded Applications または UEFI Shell の AHS Download アプリケーションが、iLO ファームウェア 1.30 以降で正しく機能しないことがあります。
- UEFI シェルの `sysconfig` コマンドがオプションの設定に失敗したり、応答しなくなったりすることがあります。
- オプションの SATA DVD ドライブがロック解除されず、オペレーティングシステムの再起動後にメディアを取り出すことができない場合があります。
- SATA M.2 ドライブを取り付けたままレガシーブートモードで起動すると、システムが起動中に応答しなくなり、レッドスクリーン（RSOD）が発生する場合があります。この問題は、UEFI ブートモードのシステムには影響しません。
- HP AF611A KVM などの USB KVM がシステムの再起動後に正しく機能しないことがあります。
- BIOS/プラットフォーム構成（RBSU）で無効にしても Core Performance Boost が有効のままになることがあります。

HTTP ブートが期待どおりに動作しない

症状

HTTP ブートを使用して起動するように構成されているサーバーが正しく起動できません。

原因

一般的な原因は次のとおりです。

- オペレーティングシステムが HTTP ブートをサポートしていません。
- HTTP ブートが正しく構成されていません。

アクション

1. OS のドキュメントを参照して、HTTP ブートをサポートしている OS かどうか確認してください。
2. HTTP ブートが正しく構成されていることを確認します。ブート方法の作成について詳しくは、**https://www.hpe.com/info/UEFI/docs** にある 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の Setting HTTP support を参照してください。

VMware は、インテル TXT で構成されていると、動作を停止する

症状

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）が有効で TPM 1.2 モードの Trusted Platform Module（TPM）が有効になっているシステムが構成されていると、VMware は動作を停止する可能性があります。

原因

この問題は、特定のメモリ構成でのみ見られます。

アクション

この問題について詳しくは、**https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00065453en_us** にある HPE カスタマーアドバイザリを参照してください。

関連情報

UEFI システムユーティリティおよび内蔵シェルの最新ドキュメントは **https://www.hpe.com/info/ProLiantUEFI/docs** から入手できます。入手できるドキュメントは次のとおりです。

- HPE ProLiant Gen10 サーバー、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およびシェルリリースノート
- 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
- UEFI Shell User Guide for HPE ProLiant Gen10Gen10, ProLiant Gen10 Plus Servers, and HPE Synergy
- 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およびシェルコマンドモバイルヘルプ
- UEFI Deployment Guide for HPE ProLiant Gen10, ProLiant Gen10 Plus Servers, and HPE Synergy
- UEFI Shell Quick Reference Card for HPE ProLiant Gen10, ProLiant Gen10 Plus Servers, Servers and HPE Synergy
- HPE ProLiant Gen10 サーバー、ProLiant Gen10 Plus サーバー、および HPE Synergy 用 UEFI 設定クイックリファレンスガイド
- Important UEFI Requirements for HPE ProLiant Gen10, ProLiant Gen10 Plus Servers, and HPE Synergy
- HPE ProLiant Gen10、ProLiant Gen10 Plus サーバー、および HPE Synergy 用の UEFI ワークロードベースパフォーマンスチューニングガイド

システムユーティリティ画面にある QR コードをスキャンすることによって、UEFI System Utilities and Shell Command Mobile Help for HPE ProLiant Gen10 and ProLiant Gen10 Plus Servers を利用できます。

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterprise では、お客様により良いドキュメントを提供するように努めています。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、ドキュメントフィードバック担当（**docsfeedback@hpe.com**）へお寄せください。このメールには、ドキュメントのタイトル、部品番号、版数、およびドキュメントの表紙に記載されている刊行日をご記載く

ださい。オンラインヘルプの内容に関するフィードバックの場合は、製品名、製品のバージョン、ヘルプの版数、およびご利用規約ページに記載されている刊行日もお知らせください。