Hewlett Packard Enterprise

HPE ProLiant Gen10 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のリリースノート（2019 年 9 月）

部品番号: 881333-198
発行: 2019 年 9 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。

ProLiant Gen10 サーバーおよび HPE Synergy コンピュートモジュールは、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: **http://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 サーバー：2.10
- AMD EPYC プロセッサーで構成される HPE ProLiant サーバー：2.00

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：2.04
- AMD EPYC プロセッサーで構成される HPE ProLiant サーバー：1.40

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）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 の更新

- 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 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；881334-196

版数：1

ブート方法の作成

ブート方法について詳しくは、HPE ProLiant Gen10 サーバーおよび HPE Synergy 用 UEFI 展開ガイド（**http://www.hpe.com/info/UEFI/docs**）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。

- インテルプロセッサー：
  - Intel Optane DC Persistent Memory を搭載した HPE Persistent Memory をサポートします。
  - NFV ワークロード用に最適化された特定の第 2 世代 Xeon スケーラブルファミリプロセッサーでのインテルスピードセレクト - ベース周波数サポートの有効化をサポートするために、インテル Priority Based Frequency を BIOS/プラットフォーム構成（RBSU）オプションに新しく追加しました。このオプションはデフォルトでは無効になっており、プロセッサーオプションメニューにあり、NFV 最適化 SKU がインストールされている場合にのみ表示されます（SKU モデルでは N と表示されます）。サポートされているオペレーティングシステムでは、インテル Speed Select-Based Frequency 機能により、優先度の高いコアは公称基本周波数よりも高い周波数で動作し、優先度の低いコアは低速の周波数で動作します。
  - BIOS/プラットフォーム構成（RBSU）I/O ダイレクトキャッシュ（IODC）メニューが電源とパフォーマンスメニューに新しく追加されました。このオプションにより、I/O トランザクションがプロセッサーキャッシュと対話するためのポリシーを調整できます。キャッシングポリシーは、ソケット間の待ち時間にわずかな影響を与える可能性があります。最適なパフォーマンスを得るためにこのオプションをデフォルト値から変更する必要がある作業負荷は非常にまれです。
  - 単一のメモリランクが特定のメモリチャネルでしか使用できない場合に動作するための HPE フォールトトレラントメモリ（ADDDC）のサポートを追加しました。以前のバージョンのシステム ROM では、各メモリチャネルで 2 つ以上のメモリランクを使用できる必要がありました。このバージョンのシステム ROM にアップデートした後、メモリ構成がこのオプションをサポートしている場合、サーバーは自動的にシステムを HPE 高速フォールトトレラントメモリモードに構成します。
  - セキュリティの脆弱性 CVE-2019-1559 に対処するために、UEFI OpenSSL サポートをバージョン 1.0.2r に更新しました。
- AMD EPYC プロセッサーで構成される HPE ProLiant サーバー：
  - AMD EPYC 7002 プロセッサーをサポートします。

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：
  - HPE RESTful API を介して RIS 操作中に内部エラーが発生しましたというメッセージが返されると、サーバーのバックアップと復元機能が正しく動作しない場合があるという問題が解決されました。
  - 2 倍のリフレッシュレートで動作するようにメモリを設定しても、実際には 1 倍のリフレッシュレートでメモリが動作するという問題に対処しました。この問題は v2.00 のシステム ROM で発生し、以前のバージョンのシステム ROM には影響しませんでした。この問題は HPE サーバーに固有のものではありません。
  - BIOS/プラットフォーム構成（RBSU）の NVMe PCIe リソースパディングオプションが、NVMe ホットアドイベントをサポートするのに十分なリソースを適切に割り当てられない問題に対処しました。特定の構成では十分な量のリソースが予約されておらず、新しく追加されたドライブの存在を検出するために再起動が必要でした。
  - 起動不可能な（フォーマットされていない）ドライブもシステムに存在する場合に、システムが USB ドライブから起動しないという問題に対処しました。この問題は、レガシーブートモードで設定されたシステムにのみ影響します。

- AMD プロセッサー：
  - Linux オペレーティングシステムを実行している仮想マシンで AMD のセキュア暗号化機能を使用するときに暗号化テクノロジの動作を操作することによって、Secure Encryption Virtualization 暗号化キーが危

険にさらされる可能性がある問題に対処しました。次の脆弱性は、このシステム ROM リリースで対処されました。CVE-2019-9836。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。

新しい RBSU/BIOS オプション

Intel Optane DC Persistent Memory オプション：

- PMM キャッシュとして使用される DRAM：指定された PMM 構成をサポートするために、キャッシュとして使用される DRAM の量を表示します。
- 揮発性メモリとして使用される DRAM：指定された PMM 構成で揮発性メモリとして使用される DRAM の量を表示します。
- インテル Optane メモリ揮発性サイズ:指定された PMM 構成で揮発性メモリとして使用される PMM の量を表示します。
- システムの揮発性メモリサイズの合計：指定された PMM 構成でシステム内の揮発性メモリの量を表示します。
- プロセッサー 1 PMM 不揮発性サイズ：指定された PMM 構成でプロセッサー 1 の不揮発性メモリとして構成されている PMM の量を表示します。
- システムの PMM 不揮発性サイズの合計：指定された PMM 構成でシステムの不揮発性メモリとして構成されている PMM の量を表示します。
- 目標構成オプション：このオプションを使用して、PMM 目標構成を構成します。
- セキュリティオプション：このオプションを使用して、PMM セキュリティオプションを構成します。
- Security Freeze Lock：このオプションを選択して、PMM の Security Freeze Lock を有効または無効にします。
- パフォーマンスオプション：これらのオプションを使用して、PMM を備えたシステムのパフォーマンスをチューニングします。
- 不揮発性メモリインターリーブ：このオプションを使用して、新しい PMM 構成を適用するときに不揮発性メモリインターリーブを有効または無効にします。
- P コードアシスト：このオプションを使用して、P コードアシスト ADR を有効または無効にします。
- デフォルトネームスペースの適用：このオプションを使用して、PMM 構成上のデフォルトネームスペースの作成を有効または無効にします。
- ネームスペースの削除：このオプションを使用して、再起動不要でネームスペースをすぐに削除します。
- Security Freeze Lock：このオプションを選択して、PMM の Security Freeze Lock を有効または無効にします。

詳しくは、**https://support.hpe.com/hpsc/doc/public/display?docId=a00074717ja_jp** を参照してください。

AMD Rome プロセッサーオプション：

- 決定論制御：このオプションを使用して AMD 決定論制御を構成します。自動の場合、プロセッサー融合値が使用されます。
- ソケットあたりの NUMA メモリドメイン：このオプションを選択して、ソケットあたりの NUMA メモリドメインの数を構成します。
- NUMA ノードとしてのラストレベルキャッシュ（LLC）：有効にすると、LLC as NUMA ノードはプロセッサーのコアが L3 キャッシュに基づいて追加の NUMA ドメインに分割されます。
- C ステート効率モード：C ステートの変更時にコア周波数を少しずつ調整するようにシステムを構成します。

- AMD 定期的ディレクトリリンス：ディレクトリ容量をより効率的に管理するために役立つ定期的ディレクトリリンスを有効にします。
- 優先 IO バス：優先 IO デバイスのバス番号。
- 優先 IO デバイス：優先 IO デバイスのデバイス番号。
- 優先 IO 機能：優先 IO デバイスの機能番号。

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。詳しくは、HPE ProLiant Gen10 サーバーおよび HPE Synergy 用 UEFI 展開ガイド（**http://www.hpe.com/info/UEFI/docs**）の HTTP ブート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 **http://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 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

- HPE ProLiant Gen10 サーバーおよび HPE Synergy 用 UEFI シェルユーザーガイド
- HPE ProLiant Gen10 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
- HPE ProLiant Gen10 サーバーおよび HPE Synergy 用 UEFI 展開ガイド
- HPE ProLiant Gen10 サーバーおよび HPE Synergy 用 UEFI シェルクイックリファレンスカード
- HPE ProLiant Gen10 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
- HPE ProLiant Gen10 サーバーおよび HPE Synergy 用の重要 UEFI 要件
- HPE ProLiant Gen10 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、HPE ProLiant Gen10 サーバー用 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。