Hewlett Packard Enterprise

HPE Trusted Platform Module 2.0 Gen10 Plus オプション

インストール手順

部品番号: P17485-191
発行: 2019 年年 12 月
版数: 1

概要

このガイドに記載された手順に従って、 HPE TPM 2.0 Gen10 Plus キット をサポートされているサーバーに取り付け、有効にしてください。このオプションは、Gen10 および以前のサーバーではサポートされません。

この手順には、次の 3 つの項があります。

1. Trusted Platform Module ボードの取り付け
2. Trusted Platform Module の有効化
3. リカバリキー/パスワードの保管

HPE TPM 2.0 の取り付けは、特定のオペレーティングシステムサポート（Microsoft® Windows Server® 2012 R2 以降など）でサポートされます。オペレーティングシステムのサポートについて詳しくは、Hewlett Packard Enterprise の Web サイト（**http://www.hpe.com/info/qs**）で製品の QuickSpecs を参照してください。Microsoft® Windows®の BitLocker ドライブ暗号化機能について詳しくは、Microsoft の Web サイト（**http://www.microsoft.com**）を参照してください。

注意: TPM が元のサーバーから取り外され、別のサーバーで電源が投入されると、TPM に格納されたデータ（キーを含む）は消去されます。

重要: UEFI ブートモードでは、サポートされている HPE TPM 2.0 Gen10 Plus キット で TPM 2.0（デフォルト）または TPM 1.2 として動作するようにサーバーを構成できます。レガシーブートモードでは、構成を TPM 1.2 と TPM 2.0 に切り替え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。

キットの内容

- TPM ボード
- TPM カバー
- リベット（2）
- 本ドキュメント

HPE Trusted Platform Module 2.0 ガイドライン

注意: 必ず、このガイドに記載されているガイドラインに従ってください。ガイドラインに従わないと、ハードウェアが損傷したり、データアクセスが中断したりする場合があります。

Hewlett Packard Enterprise 特別な注意事項 : このシステムで TPM 機能を有効にする前に、TPM の用途が関連する地域の法律、規定および政策に準拠することを保証し、該当する場合、承認または免許を取得しなければなりません。

TPM の操作や使用から発生する上記の要件に違反する準拠問題については、全面的にお客様単独の責任になります。Hewlett Packard Enterprise は、この問題について責任を負いません。

慧与特别提醒：在您启用系统中的TPM功能前，请务必确认您对TPM的使用遵守当地相关法律、法规及政策，并已事先获得所需的一切批准及许可（如适用），因您未获得相应的操作/使用许可而导致的违规问题，皆由您自行承担全部责任，与慧与无涉。

TPM の取り付けまたは交換の際には、次のガイドラインに従ってください。

- 取り付けた TPM を取り外さないでください。一度取り付けると、TPM は永続的にシステムボードの一部となります。
- ハードウェアの取り付けや交換の際に、Hewlett Packard Enterprise のサービス窓口で TPM または暗号化テクノロジーを有効にすることはできません。セキュリティ上の理由から、これらの機能を有効にできるのはユーザーだけです。
- サービス交換のためにシステムボードを返送する際は、システムボードから TPM を取り外さないでください。要求があれば、Hewlett Packard Enterprise サービスまたはサービス窓口は、TPM をスペアのシステムボードとともに提供します。
- 取り付けられた TPM のカバーをシステムボードから取り外そうとすると、TPM のカバー、TPM、およびシステムボードが損傷する可能性があります。
- TPM が元のサーバーから取り外され、別のサーバーで電源が投入されると、TPM に格納されたすべてのデータ（キーを含む）は消去されます。
- BitLocker を使用する際は、常に、リカバリキー/パスワードを保管してください。システムの保全性が侵害された可能性を BitLocker が検出した後にリカバリモードに入るには、リカバリキー/パスワードが必要です。
- Hewlett Packard Enterprise は、TPM の不適切な使用によって発生したデータアクセスのブロックについては、責任を負いかねます。操作手順については、オペレーティングシステムに付属の暗号化テクノロジー機能のドキュメントまたは TPM のドキュメントを参照してください。

Trusted Platform Module ボードの取り付け

手順

1. 次の警告に注意してください。

   警告: けが、感電、または装置の損傷を防止するために、電源コードを抜き取って、サーバーに電源が供給されないようにしてください。フロントパネルにある電源ボタンではシステムの電源を切ることはできません。AC 電源コードを抜き取るまで、電源装置の一部といくつかの内部回路はアクティブのままです。

   警告: 表面が熱くなっているため、やけどをしないように、ドライブやシステムの内部部品が十分に冷めてから手を触れてください。

2. システム ROM を更新します。

   Hewlett Packard Enterprise サポートセンターの Web サイト（**http://www.hpe.com/support/hpesc**）から、最新バージョンの ROM を見つけて、ダウンロードします。システム ROM をアップデートするには、Web サイトの指示に従ってください。

3. サーバーの電源を切ります。

   a. OS のドキュメントの指示に従って、OS をシャットダウンします。

   b. 電源ボタンを押して、サーバーをスタンバイモードにします。サーバーがスタンバイモードに入ると、システム電源 LED がオレンジ色になります。

   c. 電源コードを抜き取ります（ラックマウント型およびタワー型サーバー）。

4. 次のいずれかを実行します。

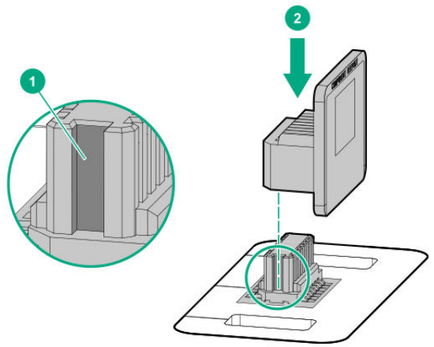
   - 必要に応じて、ラックからサーバーを取り外します。
   - サーバーまたはサーバーブレードをエンクロージャーから取り外します。

5. サーバーを平らで水平な作業台に置きます。
6. アクセスパネルを取り外します。
7. TPM コネクターにアクセスするのに妨げとなるオプション製品やケーブルがあれば、取り外します。
8. 次のアラートに注意してください。

   注意: TPM が元のサーバーから取り外され、別のサーバーで電源が投入されると、TPM に格納されたデータ（キーを含む）は消去されます。

   注意: 示された方向にのみ TPM を取り付けることが重要です。別の方向に TPM を取り付けようとすると、TPM またはシステムボードが損傷する場合があります。

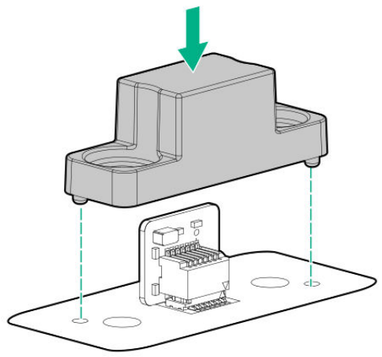
9. TPM ボードをコネクター上のキーに合わせて、TPM ボードを取り付けます。ボードを取り付けるには、TPM ボードをコネクターにしっかりと押し込みます。システムボード上の TPM コネクターの位置については、アクセスパネル上のサーバーラベルを参照してください。



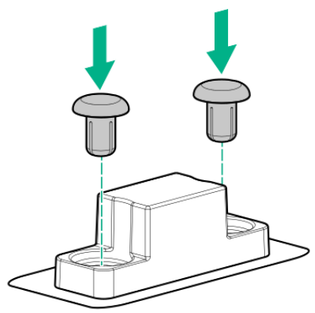
10. TPM のカバーを取り付けるには、以下の手順に従います。

    a. カバーのピンをシステムボードの開口部に合わせます。

    b. 位置決めピンが穴に固定されるまで、カバーの中央部をまっすぐ下に押し込みます。



11. TPM カバーの穴にリベットをしっかりと押し込んで、リベットを所定の位置に固定します。



12. 前の手順で TPM コネクターにアクセスするために取り外したオプション製品やケーブルがあれば、取り付けます。
13. アクセスパネルを取り付けます。
14. 次のいずれかを実行します。

    a. 必要に応じて、サーバーをラックに戻します。

    b. サーバーブレードをエンクロージャーに取り付けます。

15. サーバーの電源を入れます。

    a. 電源コードを接続します（ラックマウント型およびタワー型サーバー）。

    b. 電源ボタンを押します。

Trusted Platform Module の有効化

Trusted Platform Module を有効にするには、次のガイドラインに従ってください。

- デフォルトでは、Trusted Platform Module を取り付けた後にサーバーの電源がオンになると、Trusted Platform Module は TPM 2.0 として有効化されます。
- UEFI ブートモードでは、Trusted Platform Module を TPM 2.0（デフォルト）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、Trusted Platform Module 構成を TPM 1.2 と TPM 2.0（デフォルト）に切り替え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。

Trusted Platform Module（TPM 2.0）の有効化

手順

1. サーバーの起動シーケンス中、**F9** キーを押して、**システムユーティリティ**にアクセスします。
2. 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）** > **サーバーセキュリティ** > **Trusted Platform Module オプション**を選択します。
3. 次を確認します。
    - 「現在の TPM のタイプ」が **TPM 2.0** に設定されている。
    - 「現在の TPM の状態」が**装着済で有効**に設定されている。
    - 「TPM ビジビリティ」が**隠さない**に設定されている。
4. 前の手順で変更が行われた場合、**F10** キーを押して、選択した内容を保存します。
5. 前の手順で F10 キーが押された場合は、次のいずれかの操作を行います。
    - グラフィカルモードである場合、**はい**をクリックします。
    - テキストモードである場合、**Y** キーを押します。
6. **ESC** キーを押して、システムユーティリティを終了します。
7. 変更が行われて保存された場合、サーバーの再起動が要求されます。**Enter** キーを押して、再起動を確認します。

    次の操作が実行された場合、ユーザーの入力なしに、サーバーはもう一度再起動します。この再起動中に、TPM の設定が有効になります。
    - TPM 1.2 および TPM 2.0 からの変更
    - TPM バスの FIFO から CRB への変更
    - TPM の有効化または無効化
    - TPM のクリア
8. Microsoft Windows BitLocker、measured boot など、OS で TPM 機能を有効にします。

    詳しくは、**Microsoft の Web サイト**を参照してください。

Trusted Platform Module（TPM 1.2）の有効化

手順

1. サーバーの起動シーケンス中、**F9** キーを押して、**システムユーティリティ**にアクセスします。
2. 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）** > **サーバーセキュリティ** > **Trusted Platform Module オプション**を選択します。
3. 「TPM モードの切り替え操作」を **TPM 1.2** に変更します。
4. 「TPM ビジビリティ」が**隠さない**であることを確認します。
5. **F10** キーを押して、選択内容を保存します。
6. システムユーティリティで変更の保存を求めるメッセージが表示されたら、次のいずれかの操作を行います。
    - グラフィカルモードである場合、**はい**をクリックします。
    - テキストモードである場合、**Y** キーを押します。
7. **ESC** キーを押して、システムユーティリティを終了します。

    サーバーが、ユーザーの入力なしで、2 回目の再起動を実行します。この再起動中に、TPM の設定が有効になります。
8. Microsoft Windows BitLocker、measured boot など、OS で TPM 機能を有効にします。

    詳しくは、**Microsoft の Web サイト**を参照してください。

BitLocker のリカバリキー/パスワードの保管

リカバリキー/パスワードは、BitLocker のセットアップ時に生成され、BitLocker を有効にした後に保存および印刷できます。BitLocker を使用する際は、常に、リカバリキー/パスワードを保管してください。システムの保全性が侵害された可能性を BitLocker が検出した後にリカバリモードに入るには、リカバリキー/パスワードが必要です。

最大限のセキュリティを確保できるように、リカバリキー/パスワードを保管する際は、次のガイドラインに従ってください。

- リカバリキー/パスワードは必ず、複数の場所に保管してください。
- リカバリキー/パスワードのコピーは必ず、サーバーから離れた場所に保管してください。
- リカバリキー/パスワードを、暗号化されたハードディスクドライブに保存しないでください。

安全と規定準拠

安全、環境、および規制に関する情報については、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（Hewlett Packard Enterprise の Web サイト **http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts**）を参照してください。

Korean class A Notice

MSIP-REM-HPe-H-B123

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

RCM marking

ドキュメントに関するご意見、ご指摘

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。