Hewlett Packard Enterprise

HPE Trusted Platform Module オプション

インストールの手順

部品番号: 451177-193
発行: 2018 年 4 月
版数: 3

概要

このガイドに記載された手順に従って、サポートされる HPE ProLiant G6、G7、Gen8、または Gen9 サーバーで TPM 1.2 を有効化します。システム

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. リカバリキー/パスワードの保管
3. Trusted Platform Module の有効化

TPM を有効にするには、RBSU（「ROM ベースセットアップユーティリティ」にアクセスする必要があります。ProLiant G6、G7、および Gen8 システムでは、レガシのブートモードのみからの RBSU へのアクセスがサポートされています。ProLiant Gen9 システムでは、レガシのブートモードまたは UEFI システムユーティリティからの RBSU へのアクセスがサポートされています。詳しくは、Hewlett Packard Enterprise の Web サイト(**https://support.hpe.com/hpesc/public/home/**)で入手できるドキュメントを参照してください。

TPM を取り付けるには、Microsoft® Windows® BitLocker™ ドライブ暗号化機能などのドライブ暗号化テクノロジーを使用する必要があります。BitLocker™について詳しくは、Microsoft 社の Web サイト(**http://www.microsoft.com**)を参照してください。

キットの内容

- TPM ボード
- TPM セキュリティリベット
- 本書

HPE Trusted Platform Module のガイドライン

△ **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。

Trusted Platform Module（TPM）に関する注意事項

HPE 特別な注意事項：このシステムで Trusted Platform Module（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。

For any compliance issues arising from your operation/usage of TPM which violates the above mentioned requirement, you shall bear all the liabilities wholly and solely. Hewlett Packard Enterprise は、この問題について責任を負いません。

可信任平台模块 **(Trusted Platform Module，TPM)** 声明

HPE 特别提醒：在您在系统中启用 TPM 功能前，请您务必确认，您将要对 TPM 的使用遵守相关的当地法律、法规及政策，并已获得所需的一切事先批准及许可(如适用)。
若因您未获得相应的操作/使用许可而发生的合规问题，皆由您自行承担全部责任，与 HPE 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、HPE 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、HPE 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。
- 取り付けた TPM をシステムボードから取り外そうとすると、TPM セキュリティリベットが破損または変形します。取り付けられた TPM で破損または変形したリベットを発見した場合、管理者は、システムのセキュリティが侵害されたことを考慮し、適切な措置を講じてシステムデータの保全性を確保する必要があります。
- 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を参照してください。

Trusted Platform Module ボードの取り付け

⚠ **警告:** けが、感電、または装置の損傷に対するリスクの低減のために、電源コードを抜き取って、システムに電力が供給されないようにしてください。電源オン/スタンバイボタンではシステムの電源を完全に遮断す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。

手順

1. システム ROM を更新します。

   Hewlett Packard Enterprise サポートセンターの Web サイトから、最新バージョンの ROM を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。

2. システムの電源を切ります。

   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. システムをスタンバイモードにするには、電源ボタンを押します。システムがスタンバイ電源モードに入ると、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）。

3. 以下のいずれかを実行します。

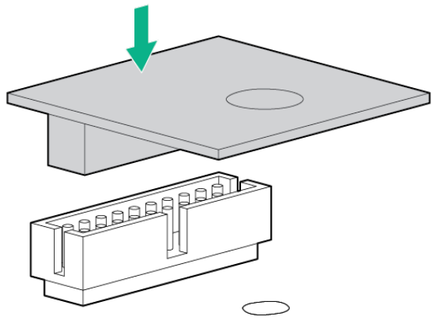
   - 必要に応じて、ラックからサーバーを取り外します。
   - サーバーまたはサーバーブレードをエンクロージャーから取り外します。

4. システムを平らで水平な面に置きます。
5. アクセスパネルを取り外します。
6. 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。

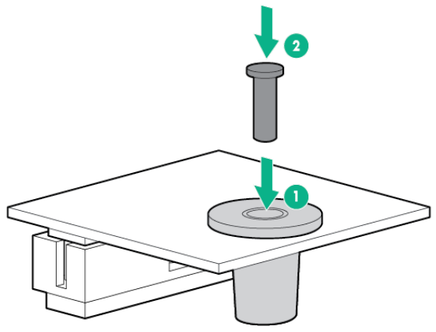
7.

注意: 取り付けた TPM をシステムボードから取り外そうとすると、TPM セキュリティリベットが破損または変形します。取り付けられた TPM で破損または変形したリベットを発見した場合、管理者は、システムのセキュリティが侵害されたことを考慮し、適切な措置を講じてシステムデータの保全性を確保する必要があります。

TPM ボードを取り付けます。ボードを差し込むには、コネクターを押します。システムボード上の TPM コネクターの位置については、システムアクセスパネル上のシステムラベルを参照してください。



8. TPM セキュリティリベットを取り付けます。リベットは、システムボードにしっかり押し込んでください。



9. 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。
10. アクセスパネルを取り付けます。
11. 以下のいずれかを実行します。
    - 必要に応じて、サーバーをラックに戻します。
    - サーバーブレードをエンクロージャーに取り付けます。
12. サーバーの電源を入れます。

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、システム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。

Trusted Platform Module の有効化

オペレーティング システムまたは他のアプリケーションでの Trusted Platform Module の使用方法の詳細は、オペレーティングシステムまたはアプリケーションのマニュアルを参照してください。

ProLiant G6、G7、および Gen8 システムでの Trusted Platform Module の有効化

手順

1. 電源投入シーケンスの途中でメッセージが表示されたら、**F9** キーを押して RBSU にアクセスします。
2. メインメニューから、**サーバーのセキュリティ**を選択します。
3. サーバーのセキュリティメニューから **Trusted Platform Module** を選択します。
4. Trusted Platform Module メニューから **TPM 機能**を選択します。
5. TPM 機能の設定を変更するには、**有効**を選択し、**Enter** キーを押します。
6. **Esc** キーを押して現在のメニューを終了するか、または **F10** キーを押して RBSU を終了します。
7. システムを再起動します。
8. OS で TPM を有効にします。OS 固有の手順については、OS のドキュメントを参照してください。

注意: サーバーに TPM を取り付けて有効にしている場合、システムやオプションのファームウェアの更新、システムボードの交換、ハードディスクドライブの交換、または OS アプリケーション TPM 設定の変更の際に適切な手順に従わないと、データアクセスがロックされます。

BitLocker™で使用する TPM の調整について詳しくは、Microsoft 社の Web サイト（**http://support.microsoft.com/**）を参照してください。

ProLiant Gen9 システムでの Trusted Platform Module の有効化

注意: システムに TPM を取り付けて有効にしている場合、システムやオプションのファームウェアの更新、システムボードの交換、ハードディスクドライブの交換、または OS アプリケーション TPM 設定の変更の際に適切な手順に従わないと、データアクセスがロックされます。

手順

1. システム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）** > **サーバーのセキュリティ**を選択します。
3. **Trusted Platform Module オプション**を選択し、**Enter** キーを押します。
4. TPM の動作状態を有効にするには、**有効**を選択します。
5. **隠さない**を選択して、TPM の可視性を設定します。
6. **F10** キーを押して、選択内容を保存します。
7. 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、**Y** キーを押します。
8. ESC キーを押して、システムユーティリティを終了します。システムの再起動を指示するメッセージが表示されたら **Enter** キーを押します。

   システムが、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。
9. Microsoft Windows BitLocker、メジャーブートなど、OS で TPM 機能を有効にします。

   BitLocker で使用する TPM の調整について詳しくは、Microsoft 社の Web サイト（**http://support.microsoft.com/**）を参照してください。

UEFI システムユーティリティについて詳しくは、**UEFI Information Library** の HPE ProLiant Gen9 および Synergy サーバー用 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。

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。

European Union Regulatory Notice

Products bearing the CE marking comply with applicable EU Directives:

Compliance with such directives is assessed using applicable European Harmonised Standards. The Declaration of Conformity can be found at the website **http://www.hpe.com/eu/certificates**. (Search with the product model name or its Regulatory Model Number (RMN), which may be found on the regulatory label.)

The point of contact for regulatory matters is HPE, Postfach 0001, 1122 Wien, Austria.

Korean class A notice

MSIP-REM-HPe-HSTNS-B070

A급 기기 (업무용 방송통신기기)	이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

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。