HP TamperLock ユーザー ガイド

概要

HP TamperLock は、攻撃者がお使いの PC のケースを開いて、悪意を持ってハードウェアを変更することを防ぎます。

初版：2020 年 9 月

製品番号：M11669-291

目次

1 概要

HP TamperLock は、攻撃者がお使いの PC のケースを開いて、悪意を持ってハードウェアを変更することを防ぎます。HP TamperLock には、ケースが開かれたかどうかを検出するセンサーと、ケースが開かれた場合に実行する操作を設定するためのポリシー コントロールが備わっています。

HP TamperLock のポリシーには、オプションとして、有効な BIOS 管理者の証明情報が入力されるまで BIOS レベルでのシステム起動をブロックする機能、HP Trusted Platform Module（TPM）をクリアしてすべてのユーザー キー（例：リモートで保存されている BitLocker 回復キーでのみローカル ドライブに保存されているデータにアクセスできるようにする BitLocker のキー）を削除する機能、およびカバー取り外し時にシステムの電源をただちにオフにする機能があります。カバー開放イベントおよび履歴はプラットフォーム ハードウェアに保存され、リモート管理者が調べることができます。

HP TamperLock のポリシーの変更を、HP Endpoint Security Controller ハードウェアに根差した保護されたストレージによって防止しています。保護されたストレージには、HP TamperLock 設定に関連するフラッシュ メモリに保存されている BIOS およびファームウェアのデータおよび設定に対する、物理的な攻撃保護機能があります。この機能は HP TamperLock をサポートするシステムに常駐し、無効にすることはできません。

2 操作

HP TamperLock 機能は不正アクセスが発生した場合にシステムをロックするように設定されており、カバーが不正に開けられたとき、システムの電源状態に関係なくカバーが開いたことが検出されます。具体的には、HP TamperLock が HP の推奨する設定になっている場合、以下のすべてのシステム電源状態でカバー開放イベントが検出されます。

- **[システム電源オン]**（オペレーティング システム（OS）が実行中）
- **[システム電源オフ]**（OS がシャットダウンされている、または OS が休止状態）
- **[システムがスリープ状態]**

重要：このドキュメントに記載されている最適な結果を得るには、HP の推奨する設定（表 4-1）で HP TamperLock を設定してください。

また、HP TamperLock カバー開放センサーは、カバーが取り外されると、内部バッテリおよびリアルタイム クロック（RTC）コイン セルを含めて、すべての電源が取り外されている状態でもトリガーされます。

注記：RTC の電源が失われると、HP TamperLock のカバー開放センサーが自動的にトリガーされます。したがって、電源を 2 年以上接続せずに保管されていたシステムでは、カバーが取り外されていなくても、HP TamperLock カバー開放センサーがトリガーされます。

システムの電源がオンになっているとき、またはスリープ状態のときに HP TamperLock によってカバーが開いたことが検出された場合、システムは直ちに電源オフになり、保存されていないデータは失われます。カバーが開いたことが検出された時点で TPM の状態をクリアするオプションのポリシーが**[Enabled]**（有効）に設定されている場合、BIOS によって TPM がクリアされます。カバーが開いたことが検出された後、BIOS によって OS は起動されず、ローカル ユーザーは、BIOS administrator password（BIOS 管理者パスワード）または（[Sure Admin]モードで）1 回限りの PIN（個人識別番号）を入力して、システムのロックを解除し通常どおり起動するよう求められます。

HP TamperLock の状態は、関連する BIOS 設定のクエリ、または[HP Notifications]ソフトウェアがインストールされている場合は Windows®イベント ビューアーで確認できます。

3 シーケンス

ここでは、HP TamperLock の手順を説明します。

1. HP TamperLock によって、シャーシ カバーが開いたことが検出されます。
2. システムの電源がオンまたはスリープ状態になっている場合、HP TamperLock によって強制的にシャットダウンされます。キャンセルのオプションはありません。
3. カバー開放イベントによって、システム ハードウェアがロックされた状態になります。
4. カバーを元の位置に戻すと、システムの電源を再度オンにできます。システムの電源が次回オンになると、以下のイベントが発生します。
    1. TPM をクリアするポリシーが有効になっている場合は、BIOS によって TPM がクリアされます。
    2. ローカル ユーザーにカバーが開いていることが通知されます。
    3. BIOS 管理者の証明情報が要求されます。
        - 証明情報が入力された場合、システムが正常に起動します。
        - 証明情報が入力されない場合、OS は起動されません。
5. [HP Notifications]ソフトウェアがインストールされている場合、監査ログ エントリが Windows イベント ログと同期されます。

4 ポリシー設定

HP Client Management ツールを使用すると、HP TamperLock ポリシーを BIOS 設定として表示および設定できます。関連する設定によって、HP TamperLock の機能の有効化およびカバーの取り外し時に実行される操作が制御されます。

表 4-1 TamperLock のポリシー設定

設定	説明	初期設定	HP 推奨
カバー開放センサー	• **Disabled**（無効）：カバーが取り外されたとき、何も実行しません • **Notify the user**（ユーザーに通知）：カバーが開くと、次回の起動時に警告メッセージが表示されます • **Administrator password**（管理者の証明情報）:この設定を選ぶと、カバーが開いた後に起動を続行する際、管理者パスワードまたは（[HP Sure Admin]が有効になっている場合）1 回限りの PIN（個人識別番号）の入力を求められます。この設定を有効にするには、パスワードを設定するか、またはローカル アクセス キーを設定して[HP Sure Admin]の拡張 BIOS 認証モードを有効にする必要があります • **Administrator Password**(管理者パスワード)：管理者の証明情報と同じように動作します（この設定名は、カバー開放センサーをサポートしていた以前の設定管理ソフトウェアとの互換性を維持するために存在します)	Disabled	Administrator Credential または Administrator Password
Power off upon cover opening（カバーが開いた時点で電源オフ）	カバー開放センサーが[Disabled]に設定されていない場合のみ使用できます **Disabled**：カバーが取り外された時点でシステムの電源がオンまたスリープ状態になっている場合、その状態のままになります **Enabled**（有効）：カバーが取り外された時点でシステムの電源がオンまたスリープ状態（S3 またはモダン スタンバイ）になっている場合、システムの電源が直ちにオフになります	Disabled	Enabled
Clear TPM on boot after cover opening（カバーが開いた後の起動時に TPM をクリア）	カバー開放センサーが無効になっていない場合のみ使用できます • **Disabled**：カバーが取り外されても、TPM 状態に変化は生じません • **Enabled**：カバーが取り外された後、次回の起動時に TPM がクリアされま	Disabled	お客様の要件によって異なります

表 4-1 TamperLock のポリシー設定 (続き)

設定	説明	初期設定	HP 推奨
	す。TPM のすべてのカスタマー キーがクリアされます **注記：**この設定は、リモート バックアップから手動復元が可能な場合、または復元を希望しない場合のみ有効にします。BitLocker が有効になっている場合、BitLocker 回復キーを使用せずにドライブの暗号化を解除することはできません		
Pre-boot DMA protection（起動前の DMA 保護）	**Thunderbolt Only**（Thunderbolt のみ）：BIOS 起動前の環境において、Thunderbolt に接続されている PCIe デバイスに対して、Input-Output Memory Management Unit（IOMMU）ハードウェアベースの DMA 保護を有効にします **All PCIe devices**（すべての PCIe デバイス）：BIOS 起動前の環境において、すべての内蔵および外付け PCI 接続デバイスに対して、Input-Output Memory Management Unit（IOMMU）ハードウェアベースの DMA 保護を有効にします	Thunderbolt Only	All PCI-Devices
DMA Protection（DMA の保護）	**Disabled**：BIOS で Input-Output Memory Management Unit（IOMMU）ハードウェアが設定されず、DMA 保護をサポートしているオペレーティング システムは使用することができません **Enabled**：BIOS で Input-Output Memory Management Unit（IOMMU）ハードウェアが設定され、DMA 保護をサポートしているオペレーティング システムが使用することができます	Enabled	Enabled

5 状態

既存の BIOS 設定管理ツールを使用して BIOS 設定を調べ、HP TamperLock の状態を確認できます。この設定を解除する唯一の方法は、BIOS administrator password（BIOS 管理者パスワード）または BIOS 管理者の証明情報（[Sure Admin]モードの場合）を入力することです。

表 5-1

設定	説明
Last cover opening and count（最後にカバーが開いた日時および回数）	カバー開放センサーが[Disabled]（無効）に設定されていない場合、この設定によって、最後にカバーが取り外された日時と、BIOS 管理者による最後のクリア以降にカバーが取り外され確認された回数がレポートされます。エントリ形式は MM/DD/YYYY HH: MM: SS.X 回です。システム要因（コンピューターの電源がオフになっているなど）によっては、カバーが連続して開いた場合は回数が増えません。リアルタイム クロックの電源が失われた後など、値を判定できない場合は、日付と時刻がすべて 0 としてレポートされます

イベント監査ログ

[HP Notifications]ソフトウェアがインストールされている場合、Windows イベント ビューアーの[HP Sure Start]フォルダーで以下のイベント ログを確認できます。

表 5-2 監査ログ

ソース ID	イベント ID	イベント	イベント ログのタイプ
0x8A	0x1E	HP TamperLock：カバーが開いたことが検出されました	警告
	0x1F	HP TamperLock：カバーが開いたことを伝える BIOS POST 通知をユーザーが確認しました	情報
	0x20	HP TamperLock：HP TamperLock の現在のポリシー設定に基づき、カバーが開いたことによって TPM がクリアされました	情報