テクニカルホワイトペーパー

HP Sure Start

ファームウェアの侵入検知と修復の自動化

HP Sure Start は、IT 管理者の介入なしに、またユーザーの生産性を中断することなく、BIOS の攻撃や破損を自動的に検出、停止、リカバリできます。 PC の電源がオンになるたびに、HP Sure Start は自動的に BIOS コードの整合性を検証し、PC が悪意のある攻撃から保護されるようにします。 PC が動作すると、実行時侵入検知は常にメモリを監視します。攻撃の場合、PC は 1 分以内に隔離された BIOS の「ゴールデンコピー」を使用して自己修復することができます。

目次

BIOS 保護はなぜ重要か？

世界がより深く結びつくにつれて、サイバー攻撃はより高い頻度と複雑さで、クライアントデバイスのファームウェアとハードウェアを狙っています。かつてはファームウェアを攻撃するためのツールやテクニックは理論的であり国家規模でのみ利用できると考えられていました。現在はこのようなツールや手法は存在するだけでなく、インターネットから容易に利用できるようになっています。

デバイスファームウェア（または BIOS）は、攻撃者が侵害を成功させる可能性のある潜在的な属性を持つため魅力的なターゲットです。:

- 永続性: ファームウェアは回路基板上の不揮発性メモリに存在し、ハードドライブを消去するだけでは削除できません。
- 制御: ファームウェアは、OS ドメインの外で最高特権レベルで実行され、OS に依存しないマルウェアを可能にします。
- ステルス性: ファームウェアは、オペレーティングシステムおよびシステムソフトウェアが完全にアクセスできないメモリ領域を占有します。アンチウイルスでスキャンすることはできないため、決して検出されない可能性があります。
- 回復の難しさ: これらのすべての側面は、システムボードの交換を含むサービスイベントに頼ることなく、この種の感染から回復することを非常に困難にします。

この種の攻撃からデバイスを保護する理想的なソリューションは、ハードウェアから「サイバー復元力」の原則を使用して設計されています。これらの原則は、不可能ではないにしても、すべての可能な攻撃を予見し予防することは極めて困難であることを認めています。理想的なソリューションは、ファームウェアの強化された保護を提供するだけでなく、成功した攻撃を検出し、それから復旧するハードウェアによって実行される機能も含みます。

HP Sure Start は優れたファームウェア保護機能を提供します

HP Sure Start は、HP PC の高度なファームウェア保護と復元力を提供する、HP 独自の画期的なアプローチです。 HP エンドポイントセキュリティコントローラ（HP ESC）を介したハードウェア強制を使用して、業界標準をはるかに超える BIOS の保護を提供し、システムが HP 純正 HP BIOS のみをブートするようにします。さらに、HP Sure Start が BIOS、ファームウェア、または実行時システム管理モード（SMM）BIOS コードの改ざんを検出した場合、保護されたバックアップコピーを使用して回復することができます。

HP Sure Start の概要

- HP コアプラットフォームファームウェアの真正性と改ざん防止—HP エンドポイントセキュリティコントローラーのハードウェア強制によるシステム起動は、正規の改ざんされていない HP ファームウェアと HP BIOS のみがロードされます。
- ファームウェアの健全性監視とコンプライアンス—隔離された HP エンドポイントセキュリティコントローラーによるファームウェアの健康関連イベントのログは、プラットフォームのファームウェアの状態と阻止された攻撃を示す可能性のある異常を提示します。
- 自己回復—HP エンドポイントセキュリティコントローラーと隔離された HP BIOS と HP ファームウェアの HP バックアップコピーを使用した HP BIOS と HP ファームウェアの破損からの自動修復。
- BIOS 設定保護—HP エンドポイントセキュリティコントローラーによる保護を BIOS コードに拡張。すべてのユーザーまたは管理者が設定した BIOS 設定の HP ESC バックアップおよび整合性チェックを含む。
- ランタイム侵入検知—OS が稼動している間、ランタイムメモリ（SMM）の重要な BIOS コードの継続的な監視。
- セキュアブートキー保護—標準 UEFI BIOS 実装に対して、OS のセキュアブート機能の整合性に不可欠な BIOS に格納されたデータベースとキーの保護が大幅に強化されました。

- ストレージ保護—HP Sure Start は、強力な暗号方式を使用して、BIOS 設定、ユーザー資格情報、およびその他の設定を HP Endpoint Security Controller ハードウェアに保存して、完全性保護、改ざん検出、およびそのデータに対する機密保護を提供します。
- Intel ® マネジメントエンジンファームウェア保護—Intel マネジメントエンジンファームウェアの保護と回復。
- 管理性—管理者は、Microsoft ® System Center Configuration Manager（SCCM）用の Manageability Integration Kit（MIK）プラグインを使用して HP Sure Start の機能を管理できます。

HP Sure Start の各世代で追加された機能の概要については、付録 A（13 ページ）を参照してください。

サードパーティーによるセキュリティ証明

HP Sure Start で使用される HP Endpoint Security Controller ハードウェアは、サードパーティーのセキュリティ評価を受け、認定されたファームウェアのみがターゲット PC 上で起動できるハードウェア強制を提供することが認定されています。[1]

前述のようにセキュリティソリューションが動作することの保証は、セキュリティ製品に関連する購入決定の重要な部分です。HP のエンドポイントセキュリティコントローラの内部動作は、公開されている基準、方法論、およびプロセスごとに主張されていることを検証するために、独立した認定ラボで検証およびテストするために公開されています。

サイバーレジリエンスデザイン

HP Sure Start は、業界標準のアプローチを超えて強化された BIOS 保護を提供するだけでなく、破損または破壊的な攻撃の場合でも BIOS 回復を保証する比類のないプラットフォームのサイバーレジリエンスを提供するようにハードウェアから設計されています。HP Sure Start を搭載した HP のビジネス PC は、サイバーレジリエンスプラットフォームの要件を公式化するための主要な公共部門の取り組みの 1 つである、ホストプロセッサブートファームウェアのための「Draft National Institute of Standards and Technology (NIST) Platform Firmware Resiliency guidelines (Special Publication 800-193)」を上回ります。

HP Sure Start-サポートモデル

HP は 2014 年に Sure Start を発表しました。その後、HP は Sure Start を強化し、Sure Start を含む製品の数を拡大しました。HP Sure Start は、タブレット、ノートブック、デスクトップ、オールインワン（AIO）など 2018 Elite 製品ラインナップ全体に提供されています。HP Sure Start Gen4 は、8 世代の Intel または AMD ® プロセッサを搭載した HP Elite および HP Pro 600 製品で使用できます。

アーキテクチャの概要と機能

HP Sure Start は 2 つの主要なアーキテクチャコンポーネントから構成されています:

- HP Sure Start ファームウェアを実行する HP エンドポイントセキュリティコントローラー
- HP エンドポイントセキュリティコントローラーのハードウェアおよびファームウェアと連携して動作する HP Sure Start BIOS

ファームウェア完全性検証—HP Sure Start のコア

HP エンドポイントセキュリティコントローラ（HP ESC）は、システムの電源投入時にファームウェアを実行し、システムが起動する前にアクティブになった最初のデバイスです。HP ESC のアクティビティには、システムの電源ボタンの監視、電源ボタンの押下時のホスト CPU 実行の開始順序の制御などが含まれますが、これに限定されません。

プラットフォームに電源が最初に供給されると（システムの電源がオンになる前に）、HP ESC はコードをロードして実行する前に、HP 独自のファームウェアが本物の HP コードであることを検証します。HP ESC ハードウェアは、業界標準の強力な暗号方式を使用して整合性の検証を実行します。この方法では、内部永続読み出し専用メモリに含まれる 2048 ビットの HP RSA 公開鍵を使用します。したがって、HP ESC は、ファームウェアと HP BIOS が実行される前にそのファームウェアを検証するために使用される、プラットフォーム用の組み込みのハードウェアベースの信頼ルート（RoT）です。このハードウェアの信頼ルートは、展開方法に関係なく、ファー

ムウェアの置換攻撃から保護し、HP プラットフォームのセキュリティが構築される基盤として機能します。

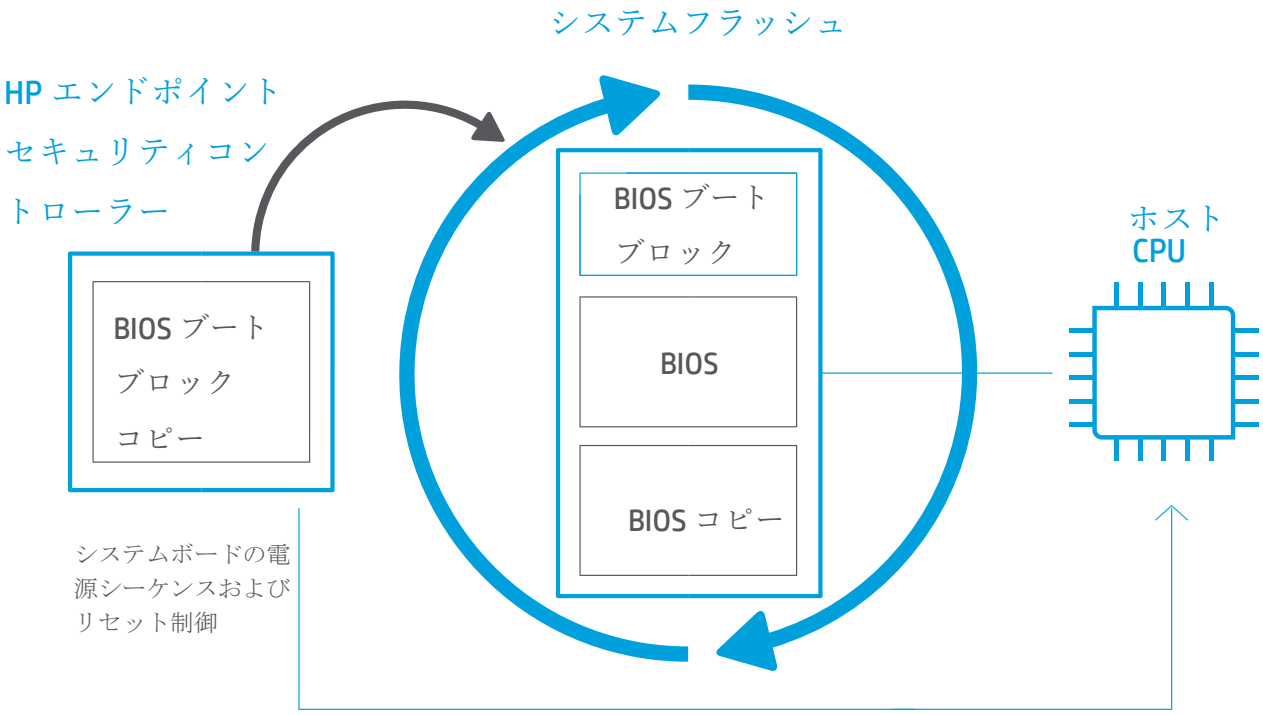

図 1 完全性検証プロセス

図 1 は、ファームウェアの完全性検証プロセスを示しています。 HP ESC が認証され、HP Sure Start ファームウェアの実行を開始すると、そのファームウェアは同じ強力な暗号操作を使用して、システムフラッシュ BIOS ブートブロックの整合性を検証します。単一ビットが無効な場合、HP ESC は、システムフラッシュの内容を、HP ESC 専用の不揮発性メモリ（NVM）に格納されている HP BIOS ブートブロックのコピーに置き換えます。

HP Sure Start の設計は、HP ESC とホスト CPU の両方で動作するすべてのファームウェアと BIOS コードが、HP がデバイスに搭載されることを意図したコードであることを保証します。

注記：システムフラッシュブートブロックの整合性チェック、および HP ESC によって実行される必要なリカバリは、ホスト CPU がオフのときに行われます。したがって、ユーザーの視点から見ると、システムがまだオフであるとき、スリープモードにあるとき、または休止状態にあるときに、全体の動作が行われる

システムフラッシュ BIOS ブートブロックは、HP BIOS の基礎となります。 HP ESC ハードウェアは、BIOS ブートブロックがリセット後に CPU が実行する最初のコードであることを保証します。 HP ESC は、BIOS ブートブロックに本物の HP コードが含まれていると判断すると、通常どおりにシステムをブートすることができます。

また、HP ESC は、システムがオフになるか、休止状態またはスリープモードに入るたびに、システムフラッシュブートブロックコードの整合性をチェックします。これらの各状態で CPU の電源がオフになり、CPU は BIOS ブートブロックコードを再実行して再開する必要があるため、改ざんをチェックするたびに BIOS ブートブロックの整合性を再確認することが重要です。

さらに、HP インテルモデルの場合、HP Sure Start は定期的（15 分おき）にシステムの稼動中にシステムフラッシュ BIOS ブートブロックの整合性をチェックします。[2]

マシン固有データの完全性

HP ESC と BIOS は連携して、各マシンに固有の出荷時設定の重要な変数を、特定のプラットフォームの存続期間にわたって一定に保つことを意図した高度な保護を提供します。工場では、この変数データのバックアップコピーが HP ESC 不揮発性メモリストアに保存されます。バックアップは、HP Sure Start BIOS コンポーネントで読み取り専用で使用できるようになり、すべての起動時にデータの整合性チェックを実行します。工場出荷時設定に比べて共有フラッシュの設定が変更されている場合、HP Sure Start BIOS コンポーネントは、HP ESC が提供するバックアップコピーからシステムフラッシュ内のデータを自動的に復元します。

ディスクリプタ領域

HP インテルモデルの場合、HP Sure Start はシステムフラッシュのディスクリプタ領域を保護します。 Intel アーキテクチャ特有のディスクリプタ領域には、リセット時に Intel Core ロジックによってサンプリングされ、その後、Core ロジックを構成するために使用される重要な構成パラメータが含まれています。ディスクリプタ領域には、BIOS 領域がフラッシュ内のどこに存在するかを判断するために Intel Core ロジックによって使用されるシステムフラッシュのパーティション情報も含まれているため、CPU がリセットから実行するコードを取得する場所も含まれます。 HP Sure Start は、この領域の整合性を監視し、改ざんや破損が発生した場合に、意図した構成に回復します。

ネットワークコントローラ保護

さらに、HP インテルモデルの場合、HP Sure Start は、システムフラッシュに含まれるネットワークコントローラ（NIC）の設定を保護します。 HP のお客様の中には、出荷時に設定された NIC 設定に正当な変更が必要なユースケースがあります。したがって、HP Sure Start はデフォルトで NIC 設定の変更を防止しません。代わりに、HP Sure Start は、有効にすると、NIC の設定が変更されたことをユーザーに警告する機能を提供します。さらに、HP Sure Start は NIC 設定を工場出荷時の値に復元する方法を提供します。保護された設定には、MAC アドレス、PXE（Pre-boot Execution Environment）設定、および RPL（Remote Initial Program Load）が含まれます。この復元は、HP ESC によって保護された読み取り専用バックアップコピーによって実現されています。

BIOS 設定保護

前述のとおり、HP Sure Start は、HP BIOS コードの整合性と信頼性を検証します。このコードは HP によって作成された後は静的なので、デジタル署名を使用してコードの両方の属性を確認することができます。ただし、BIOS 設定のダイナミックでユーザー設定可能な性質により、これらの設定を保護するための追加の課題が生じます。デジタル署名は HP によって生成されず、HP Sure Start ESC ハードウェアによって使用されて、これらの設定を確認することはできません。

HP Sure Start BIOS 設定保護は、HP ESC ハードウェアを使用して、ユーザーが希望するすべての BIOS 設定の保全性をバックアップしてチェックするようにシステムを設定する機能を提供します。

この機能がプラットフォームで有効になっている場合、BIOS で使用されるすべてのポリシー設定が後でバックアップされ、各ブート時に整合性チェックが実行されて、BIOS ポリシー設定のいずれも変更されていないことを確認します。変更が検出された場合、システムは HP Sure Start 保護記憶域からのバックアップを使用して、ユーザー定義の設定に自動的に戻ります。

HP Sure Start BIOS 設定保護機能は、BIOS 設定を変更しようとすると HP Sure Start ESC ハードウェアにイベントを生成します。イベントは HP Sure Start 監査ログに記録され、ローカルユーザーは起動時に BIOS から通知を受け取ります。

HP Sure Start ストレージ保護

HP ESC ハードウェアをベースにしたストレージの保護は、HP Sure Start で保護されている BIOS /ファームウェアのデータと設定を最高レベルで保護します。 HP Sure Start ストレージ保護、攻撃者がシステムを逆アセンブルし、回路基板上の不揮発性ストレージデバイスに直接接続する物理的な攻撃シナリオであっても機密性、整合性、改ざん検出を提供するように設計されています。

データ完全性

ファームウェアによる不揮発性メモリに格納され、さまざまな機能の状態を制御するために使用される動的データの完全性は、プラットフォーム全体のセキュリティ姿勢にとって重要です。動的データには、デバイスのエンドユーザーまたは管理者が変更できるすべての BIOS 設定が含まれます。例には、セキュアブート機能、BIOS 管理者パスワードと関連ポリシー、トラステッドプラットフォームモジュールの状態制御、HP Sure Start のポリシー設定などのブートオプションが含まれます（ただしこれに限定されません）。

これらの設定の不正な変更を防ぐための既存のアクセス制限をバイパスする攻撃が成功すると、プラットフォームのセキュリティが壊れる可能性があります。たとえば、攻撃者がセキュアブート状態を不正に変更して検出されずに無効にするシナリオを考えてみましょう。このシナリオでは、プラットフォームは、OS が起動する前に、ユーザーに知られずに攻撃者のルートキットを起動します。

業界標準の UEFI（Unified Extensible Firmware Interface）BIOS は、これらの変数に対する不正な変更を防止するアクセス制限を実装しており、HP はこれを他の PC 業界と同様に実装しています。ただし、HP Sure Start は、これらのメカニズムの違反がプラットフォームに与えるリスクを考慮すると、ベースラインの業界標準よりも強力な二次防御を提供します。

ファームウェアが使用する BIOS 設定およびその他の動的データは、HP Sure Start によって保護されている状態を制御するためにホスト CPU 上で実行されるソフトウェアに直接アクセスできない HP Endpoint Security Controller の独立した不揮発性メモリに格納されます。

さらに、HP ESC は、データ要素がこの不揮発性メモリストアに格納されるたびに、独自の整合性測定値を作成して付加します。完全性の測定は、HP ESC に含まれる秘密鍵に根ざす強力な暗号化アルゴリズム（SHA-256 ハッシュを利用したハッシュベースのメッセージ認証コード）に基づいています。秘密鍵は各 HP ESC に固有のものであるため、各コントローラーは同一の要素に対して一意の完全性測定値を生成します。データ要素が不揮発性メモリから読み出されると、HP ESC はそのデータ要素の完全性測定値を再計算し、データ要素に付加された完全性測定値と比較します。不揮発性メモリストア内のデータに対する許可されていない変更は、誤った比較をもたらす。このアプローチを使用すると、HP ESC は、不揮発性メモリストアに格納されているデータ要素による改ざんを検出できます。

データ機密性

プラットフォームによって保存されるデータ要素の多くは、機密性を維持することが重要です。たとえば、BIOS 管理者のパスワードハッシュ、ユーザーの資格情報、および HP Sure Run や HP Sure Recovery などのファームウェアベースの機能のために、ユーザーの代わりにファームウェアによってオプションで保存される秘密鍵が含まれます。

これらの秘密の保護は、業界標準の UEFI BIOS アプローチを使用することでは困難です。なぜなら不揮発性ストレージは通常ホストプロセッサ上で動作するソフトウェアによって読み込み可能であるからです。 HP Sure Start ストレージ保護は標準の UEFI BIOS の実装を超えてこれらの機密データを保護するためのものです。

HP Sure Start アプローチは、別個の独立したストレージに加えて HP ESC に含まれる Advanced Encryption Standard（AES）ハードウェアブロックを活用して、HP Sure Start 不揮発性メモリに格納されているすべての機密データ要素に対してこれらの要素のデータ保全性の測定に加えて AES-256 暗号化を実施します。使用される暗号化キーは各 HP ESC に固有のものでありそこから離れることはないため、個々の HP ESC コンポーネントで暗号化されたデータはその同じ HP ESC によってのみ解読できます。

セキュアブートキー保護

HP Sure Start は、業界標準の UEFI セキュアブート実装と比較して、ファームウェアによって保存される UEFI セキュアブートキーデータベースの保護を強化しています。これらの変数は、ブート時に起動される前に、OS ブートローダの整合性と信頼性を検証する UEFI セキュアブート機能を正しく動作させるために重要です。

HP Sure Start は、HP Sure Start で保護されたストレージにマスターコピーを維持して、UEFI セキュアブートキーデータベースを保護します。ランタイム中に OS によって UEFI 標準セキュアブートキーデータベースへの許可された変更は、HP Sure Start によって追跡され、HP ESC によってマスターコピーに適用されます。その後、HP

Sure Start は、HP Sure Start で保護されたストレージのマスターコピーを使用して、UEFI 標準セキュアブートキーデータベースへの不正な変更を識別して拒否します。

この機能はデフォルトで有効になっており、以下のデータベースを対象とします:

- 署名データベース (db)
- 無効化された署名データベース (dbx)
- 鍵登録鍵 (KEK)
- プラットフォーム鍵 (PEK)（ランタイム中に OS によって動的に更新される）

ランタイム侵入検知 (RTID)

各ブート時に、BIOS コードはフラッシュメモリから固定アドレスで実行を開始します。これは BIOS ブートコードと呼ばれ、OS を起動する前に必要な「Pre-OS」機能を提供します。ただし、BIOS の一部が DRAM に残っており、高度な電源管理機能、OS サービス、および OS の実行中に他の OS に依存しない機能を提供する必要があります。システム管理モード（SMM）コードと呼ばれるこの BIOS コードは、DRAM 内の OS から隠された特別な領域にあります。また、このコードを HP Sure Start のランタイム侵入検知機能のコンテキストで「ランタイム」BIOS コードと呼びます。 （SMM の詳細とその動作方法については、14 ページの付録 B を参照してください）。.

SMM コードの完全性は、クライアントデバイスのセキュリティ状態にとって重要です。 HP Sure Start は、OS 起動時に HP SMM BIOS コードが損傷していないかどうかを確認します。ランタイム侵入検出は、新しい保護機能を追加したり、そのコードへの攻撃を検出する手段を提供したりすることで、OS の実行中に SMM BIOS コードが損なわれないようにするメカニズムを提供します。

ランタイム侵入検知のアーキテクチャ

RTID 機能は、プラットフォームチップセット内の特殊なハードウェアを使用して、ランタイム HP SMM BIOS の異常を検出します。異常が検出されると、HP エンドポイントセキュリティコントローラーに通知され、CPU から独立して構成されたポリシーアクションを実行できます。

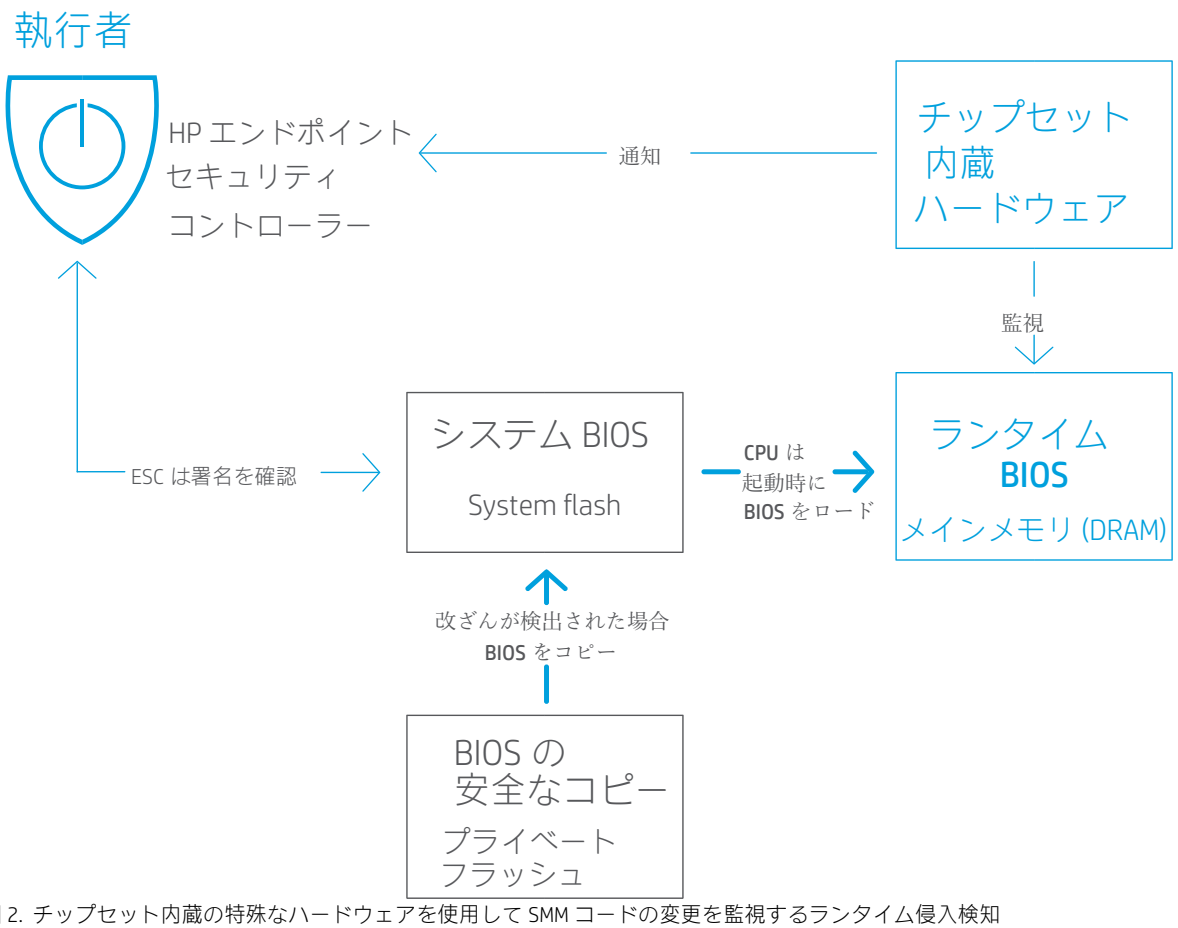

図 2. チップセット内蔵の特殊なハードウェアを使用して SMM コードの変更を監視するランタイム侵入検知

ユーザー通知、イベントログ、およびポリシー管理

HP Sure Start のエンドユーザー通知

通常の動作状態では、HP Sure Start はユーザーには見えません。デフォルト設定では、リカバリ操作は自動的に行われ、HP Sure Start が問題を特定したときにリカバリに通常必要なエンドユーザーまたは IT の操作はありません。

OS が動作している間に HP Sure Start Dynamic Protection またはランタイム侵入検知機能によって BIOS の完全性の問題が検出された場合、実行時の通知が表示されることがあります。重大なイベントが検出された場合や処置がとられた場合、HP Sure Start は、次の起動時に Windows ® の通知で警告メッセージを表示します。これらの Windows 通知を表示するには、HP Notifications ソフトウェアが必要です。

HP Sure Start のイベントログ

HP エンドポイントセキュリティコントローラは、HP Sure Start が監視するファームウェア/ BIOS コードおよびデータに関連する重要なイベントを記録します。これらのイベントは、Sure Start の不揮発性メモリストアに格納されます。これらのイベントは、HP Notifications ソフトウェアがインストールされている場合に、HP ESC から Windows イベントビューアにコピーされ、ローカルユーザーおよびお客様がお使いの管理エージェントによるこれらのイベントへのアクセスを容易にします。

次のイベントが発生すると、HP Sure Start サブシステムからすべてのイベントを収集し、Windows イベントビューアがまだ記録されていないイベントで更新されるように、HP Notifications ソフトウェアを起動します。

- Windows の 起動

- Windows のスリープやハイバネートからの復旧
- HP Sure Start Dynamic Protection のランタイムイベント通知
- HP Sure Start ランタイム侵入検知 (RTID)

HP 通知ソフトウェアは、HP Sure Start イベントを独自の「HP Sure Start」アプリケーションイベントログに取り込みます。 HP Sure Start イベントのみがこのログに含まれます。 HP Sure Start イベントへの Windows イベントビューアのパスは、システムツール/イベントビューア/アプリケーションおよびサービスログ/ HP Sure Start です。

HP Sure Start イベントに関連する Windows イベントビューアレベルのカテゴリは、下記の表で定義されています。

イベントは、HP Sure Start によって生成された順序で Windows イベントビューアに入力されます。 HP Sure Start サブシステムの最も古いイベントが最初に Windows イベントビューアに追加され、最後のイベントが最後に追加されます。

各 Windows イベントビューアエントリのタイムスタンプは、イベントが発生した時刻ではなく、そのログに追加された時刻です。各 Sure Start Windows イベントビューアエントリには、実際の発生時のタイムスタンプを含むイベントの詳細内の詳細データが含まれています。

注記：イベントは Windows イベントビューアにコピーされた後も HP エンドポイントセキュリティコントローラーの中に永続的に存在します。Windows イベントビューアがクリアされている場合、HP 通知ソフトウェアアプリケーションは、HP Sure Start イベントログを追記する際に、HP エンドポイントセキュリティコントローラー内のすべての HP Sure Start エントリで置き換えます。

HP Sure Start Windows イベントビューアイベントの種類

イベントレベル	説明
情報	通常の操作中に発生すると予想されるイベント（BIOS のアップデートなど)。
警告	予期せぬイベントが発生したが、HP Sure Start によって完全に回復されました。プラットフォームが完全に動作するために必要なユーザー/管理アクションはありません。これらのイベントは、特に複数のマシン間でこれらのイベントの傾向がある場合に、ユーザー/管理者がさらに調査したい異常な操作です。
エラー	完全に回復するために、管理者/ HP サービスがプラットフォーム上で動作する必要があるイベント。

HP Sure Start ポリシー制御

HP システム BIOS は一般的なユーザーのために HP Sure Start ポリシーを有効にして最適化します。HP Sure Start はデフォルトで有効になっているため、HP Sure Start で保護する設定を一般的なユーザーが変更する必要はありません。上級ユーザーは、システム BIOS は、（F10）BIOS セットアップのポリシー設定を使用して、HP Sure

Start の動作をいくらか制御できます。特に明記されていない限り、これらの設定と機能は Security / BIOS Sure Start の下にあります。

注記：ポリシーは、ホスト **CPU** から直接アクセスできない **HP ESC** 不揮発性メモリに格納されます。したがって、**Sure Start** の設定が有効になるには、再起動が必要です。

以下の **HP Sure Start** の設定と機能が利用できます。

- **Verify Boot Block on Every Boot** [ブート毎にブートブロックを確認する]
- **BIOS Data Recovery Policy** [BIOS データの復元ポリシー]
- **Network Controller Configuration Restore (Intel only)** [ネットワークコントローラ構成の復元（Intel のみ）]
- **Prompt on Network Controller Configuration Change (Intel only)** [ネットワークコントローラ構成の変更時にプロンプトを表示する（Intel のみ）]
- **Dynamic Runtime Scanning of Boot Block (Intel only)** [ブートブロックの動的ランタイムスキャン（Intel のみ）]
- **HP Sure Start BIOS Setting Protection** [HP Sure Start による BIOS 設定の保護]
- **HP Sure Start Secure Boot Keys Protection** [HP Sure Start によるセキュアブートキーの保護]
- **Enhanced HP Firmware Runtime Intrusion Prevention and Detection (Intel only)** [HP ファームウェアのランタイム侵入防止および検知機能の強化（Intel のみ）]
- **HP Firmware Runtime Intrusion Detection (AMD only)** [HP ファームウェアのランタイム侵入検知（AMD のみ）]
- **HP Sure Start Security Event Policy** [HP Sure Start のセキュリティイベントポリシー]
- **HP Sure Start Security Event Boot Notification** [HP Sure Start のセキュリティイベントブート通知]
- **Lock BIOS Version** [BIOS バージョンのロック]
- **Save/Restore MBR of System Hard Drive** [システムのハードドライブの MBR の保存/復元]
- **Save/Restore GPT of System Hard Drive** [システムのハードドライブの GPT の保存/復元]
- **Boot Sector (MBR/GPT) Recovery Policy** [ブートセクター(MBR/GPT)の復元ポリシー]

Verify Boot Block on Every Boot [ブート毎にブートブロックを確認する]

HP Sure Start は、スリープ、休止状態または電源切断から再開する前に、常にシステムフラッシュ BIOS ブートブロックの整合性を確認します。[有効]に設定すると、HP Sure Start は各ウォームブート時にブートブロックの整合性も確認します（Windows 再起動）。考慮すべきトレードオフは、より速い再起動時間とより多くのセキュリティです。この機能のデフォルト設定は無効です。

BIOS Data Recovery Policy [BIOS データの復元ポリシー]

自動に設定すると、HP Sure Start は必要に応じて BIOS またはマシン固有のデータを自動的に修復します。 手動に設定すると、HP Sure Start は修復を続けるために特別なキーシーケンスが必要です。ブートブロックコードに問題が発生した場合、システムは起動を拒否し、システム LED で一瞬の点滅シーケンスが点滅します。 マシン固有のデータで問題が発生した場合は、画面にメッセージが表示されます。必要なキーシーケンス、および表示される点滅シーケンスは、システムがノートブック、デスクトップ、またはタブレットのいずれであるかによって異なります。手動モードは、修復前にシステムのフラッシュ内容に関するフォレンジックを実行できるユーザーにとって便利です。一般的なユーザーは手動モードを使用することをお勧めしません。この機能のデフォルト設定は自動です。

Network Controller Configuration Restore (Intel only) [ネットワークコントローラ構成の復元（Intel のみ）]

このコントロールは、Intel システムでのみ使用できます。これを選択すると、HP Sure Start はネットワークコントローラの設定工場出荷時のデフォルト設定に直ちに戻ります。

Prompt on Network Controller Configuration Change (Intel only) [ネットワークコントローラ構成の変更時にプロンプトを表示する（Intel のみ）]

この設定は、Intel システムでのみ使用できます。HP は、MAC アドレスを含む出荷時に定義されたネットワークコントローラ設定を提供しています。この設定が有効に設定されている場合、システムはネットワークコントローラ設定の状態を監視し、出荷時の設定状態からの変更があった場合にユーザーに確認を求めます。この機能のデフォルト設定は無効です。

Dynamic Runtime Scanning of Boot Block (Intel only) [ブートブロックの動的ランタイムスキャン（Intel のみ）]

この設定は、Intel システムでのみ使用できます。デフォルトである有効に設定されている場合、HP Sure Start は、OS の実行中に BIOS ブートブロックの整合性を定期的にチェックします。無効に設定すると、HP Sure Start は、スリープまたは休止状態からのブートまたは再開前に整合性をチェックします。

HP Sure Start BIOS Setting Protection [HP Sure Start による BIOS 設定の保護]

BIOS 設定保護ポリシーは、デフォルトで無効になっています。この機能を有効にするには、まずクライアントデバイスの所有者/管理者が、すべての BIOS ポリシーを優先設定に設定する必要があります。また、オーナー/管理者は、HP Sure Start BIOS 設定保護を使用するために BIOS セットアップ管理者パスワードを設定する必要があります。

これが完了したら、BIOS 設定保護ポリシーを「有効」に変更する必要があります。この時点で、すべての BIOS 設定のバックアップコピーが HP Sure Start 保護されたストレージに作成されます。今後は、ローカルまたはリモートで BIOS 設定を変更することはできません。各起動時に、BIOS ポリシー設定が目的の状態にあることが確認され、不一致があれば、HP Sure Start 保護されたストレージから BIOS 設定が復元されます。

BIOS 設定を変更するには、BIOS 管理者パスワードを入力する必要があります。その後、BIOS 設定の保護が無効になり、その時点で BIOS 設定を変更する事ができます。

HP Sure Start Secure Boot Keys Protection [HP Sure Start によるセキュアブートキーの保護]

この設定を出荷時のデフォルトである enable に設定すると、HP Sure Start は、起動時に起動する前に、OS ブートローダの完全性と信頼性を確認するために、BIOS が使用する安全なブートデータベースとキーの保護を強化します。 disable に設定すると、標準の UEFI セキュアブート変数保護だけが使用され、HP Sure Start サブシステムによってバックアップコピーは保持されません。

Enhanced HP Firmware Runtime Intrusion Prevention and Detection (Intel only) [HP ファームウェアのランタイム侵入防止および検知機能の強化（Intel のみ）]と **HP Firmware Runtime Intrusion Detection (AMD only)** [HP ファームウェアのランタイム侵入検知（AMD のみ）]

RTID 機能は、HP 工場から出荷されるすべてのプラットフォームでデフォルトで有効になっています。 HP Sure Start RTID を利用するには、エンドユーザー/管理者が機能を有効にしたり、別の方法で「展開」する必要はありません。

RTID 機能は、オプションでプラットフォームの所有者/管理者が無効にするように設定できます。

HP Sure Start Security Event Policy [HP Sure Start のセキュリティイベントポリシー]

この BIOS ポリシー設定は、OS の実行中に HP Sure Start が攻撃を検出した場合や攻撃を試みた場合に実行されるアクションを制御します。このポリシーには、次の 3 つの構成が考えられます。

- **Log event only**（イベントのみを記録する）：この設定を選択すると、HP ESC は検出イベントを記録します。検出イベントは、Microsoft Windows イベントビューア [3] のアプリケーションおよびサービスログ/HP Sure Start で表示できます。
- **Log event and notify user**（イベントを記録してユーザーに通知する）：これがデフォルト設定です。この設定を選択すると、HP ESC は検出イベントを記録します。検出イベントは、Microsoft Windows イベントビューアのアプリケーションおよびサービスログ/HP Sure Start で表示できます。さらに、ユーザーは Windows 内でイベントが発生した事を知らされます [4]。
- **Log event and power off system**（イベントを記録してシステムの電源を切る）：この設定を選択すると、HP ESC はイベントを記録します。検出イベントは、Microsoft Windows イベントビューアのアプリケーションおよびサ

ービスログ/HP Sure Start で表示できます。さらに、Windows 内でイベントが発生し、システムシャットダウンが差し迫っていることをユーザーに知らせます。

HP Sure Start Security Event Boot Notification [HP Sure Start のセキュリティイベントブート通知]
この BIOS ポリシー設定は、システムの起動時に表示される HP Sure Start の警告とエラーメッセージでローカルユーザーがブートを続行する前にエラーを確認する必要があるかどうかを制御します。デフォルトの確認要求設定では、エラーメッセージが表示された状態でシステムが停止します。ローカルユーザーは、ブートを続行するにはキーを押す必要があります。15 秒後にタイムアウトに設定を変更すると、メッセージは表示されますが、メッセージが 15 秒間表示された後に自動的にブートプロセスが続行されます。

Lock BIOS Version [BIOS バージョンのロック]
（F10）BIOS セットアップでは、この機能は Main / Update System BIOS にあります。

無効に設定すると、サポートされているプロセスを使用して BIOS を更新できます。HP ESC は、システムフラッシュで有効なブートブロック更新を検出すると、ブートブロックのバックアップコピーを更新します。

有効に設定すると、すべての **HP BIOS** 更新ツールが **BIOS** の更新を拒否します。さらに、**HP Sure Start** は、不正な方法でシステムフラッシュを取り外すことによって **BIOS** バージョンの変更を試みることから **BIOS** を保護します。**HP ESC** はロックダウンされた **BIOS** のバージョンを記録します。**HP ESC** がシステムフラッシュ内の **BIOS** が変更された事を検出すると、**HP ESC** は BIOS ブートブロックをブートブロックの HP ESC コピーで上書きします。ブートブロックの HP ESC コピーは、実行して BIOS の正しいバージョンの残りの部分を回復します。この機能のデフォルト設定は無効です。

Save/Restore MBR of System Hard Drive [システムのハードドライブの MBR の保存/復元]と **Save/Restore GPT of System Hard Drive** [システムのハードドライブの GPT の保存/復元]
（F10）BIOS セットアップでは、この機能は Security / Hard Drive Utilities にあります。 HP Sure Start で検出されたプライマリドライブのパーティションタイプ（GPT または MBR）に応じて、これらの機能のうちの 1 つだけが使用できます。

有効に設定すると、HP Sure Start はプライマリドライブから MBR / GPT パーティションテーブルの保護されたバックアップコピーを保持し、各ブート時にバックアップコピーをプライマリと比較します。相違が検出された場合は、ユーザーにプロンプトが表示され、バックアップから元の状態にリカバリするか、保護されたバックアップコピーを変更内容で更新するかを選択できます。ブートセクタ（MBR / GPT）リカバリポリシーは、オプションで、HP Sure Start で検出された不一致の場合に実行されるアクションのユーザー決定を不要にするために使用できます。

無効（デフォルト）に設定すると、HP Sure Start は MBR / GPT 保護を提供しません。

Boot Sector (MBR/GPT) Recovery Policy [ブートセクター(MBR/GPT)の復元ポリシー]
ローカルユーザーコントロール（デフォルト）に設定すると、HP Sure Start が MBR / GPT パーティションテーブルの変更を検出したときに実行する処理を求めるプロンプトが表示されます。破損し場合に復元に設定すると、HP Sure Start は相違が検出された場合はいつも MBR/GPT を保存された状態に復元します。

HP Sure Start ポリシー制御のリモート管理

通常のユーザー向けに、HP Sure Start ポリシーが最適化されています。 HP Sure Start はデフォルトで有効になっているため、リモート管理者は HP Sure Start を有効にする（または展開する）必要はありません。リモート管理者が HP Sure Start のポリシー設定を変更したい場合は、他のプラットフォーム BIOS ポリシーの管理に使用される同じ WMI（Windows Management Instrumentation）API または HP BIOS 設定ユーティリティスクリプトを使用して、HP Sure Start ポリシーを管理できます。さらに、管理者は、Microsoft System Center Configuration Manager（SCCM）用の Manageability Integration Kit（MIK）プラグインを使用して、HP Sure Start の機能をリモート管理し、HP Sure Start イベントを表示できます。.

結論

HP Sure Start は次のような主な利点をもたらします。

- 中断の無い生鮮性—HP Sure Start は、攻撃や偶発的な BIOS 破損が発生した場合でも、IT/サービスイベントを待っている停止時間を排除することにより、 ビジネス継続性を維持します。
- コスト削減—HP Sure Start の自動復旧機能は、IT ヘルプデスクへのコールを削減し、生産性を向上させ、最終的にはプラットフォームのメンテナンスコストを削減します。
- 安心—HP Sure Start には、さまざまなソフトウェアおよびハードウェアプラットフォームで動作する複数のセキュリティ機能があります。

特定の HP エリート PC でのみ使用可能な業界標準のファームウェア侵入検知機能と HP Sure Start による自動修復機能により、重要な BIOS ファームウェアをマルウェアから保護します。

関連情報 hp.com/go/computersecurity

付録 A—HP Sure Start の歴史

HP は 2014 年に Sure Start を発表しました。その当時から、HP は Sure Start を拡張し、それを使用する製品の数を拡大しました。以下の表は、各世代で追加された機能の概要を示しています。

世代	リリース年	追加された機能
HP Sure Start	**2014**	• 自己修復機能を備えたファームウェアと BIOS の真正性の強制 • ファームウェアの監視とコンプライアンス
HP Sure Start with Dynamic Protection	**2015**	• Windows イベントビューア対応 • ダイナミックプロテクション (対応する Intel 製品のみ)
HP Sure Start Gen3 (select Intel products)[5] **HP Sure Start with Runtime Intrusion Detection (select AMD products)[6]**	**2017**	• ランタイム侵入検知 • BIOS 設定保護 • Microsoft SCCM 用 Manageability Integration Kit (MIK) プラグイン
HP Sure Start Gen4[7]	2018	• ストレージ保護—BIOS 設定、ユーザー資格情報、およびその他の設定を HP エンドポイントセキュリティコントローラーハードウェアに保存して、完全性保護、改ざん検出、およびそれらのデータに対する機密保護を提供する強力な暗号化方法 • セキュアブートデータベース保護—標準の UEFI BIOS 実装に対して、OS のセキュアブート機能の整合性にとって不可欠な、BIOS に格納されたデータベースとキーの保護の強化 • Intel プラットフォームでは、Intel Management Engine ファームウェアの保護と回復が強化されています • HP エンドポイントセキュリティコントローラーのサードパーティーセキュリティ証明書—HP ESC ハードウェアのコア機能が公開基準、方法論、およびプロセス[1] で要求されているように動作する事を検証するための独立した認定試験所によるテスト • HP Sure Start を搭載した HP のビジネス PC は、ホストプロセッサのブートファームウェアのためのドラフト NIST プラットフォームファームウェアレジリエンスガイドライン（SP 800-193）を上回ります。

付録 B—システム管理モード (SMM)の概要

システム管理モード（SMM）は、OS が動作している間 PC の高度な電源管理機能や他の OS に依存しない機能に使用される業界標準の方法です。 SMM の用語と実装は x86 アーキテクチャに固有ですが、多くの最新のコンピューティングアーキテクチャでは、同様のアーキテクチャ概念が使用されています。

SMM はブート時に BIOS によって設定されます。 SMM コードはメイン（DRAM）メモリに取り込まれ、BIOS はチップセット内の特別な（ロック可能な）コンフィギュレーションレジスタを使用して、マイクロプロセッサが SMM コンテキストで実行されていないときにこの領域へのアクセスをブロックします。実行時には、SMM モードへの入力はイベント駆動型です。チップセットは、多くのタイプのイベントおよびタイムアウトを認識するようにプログラムされています。このようなイベントが発生すると、チップセットハードウェアは System Management Interrupt（SMI）入力ピンをアサートします。 次の命令境界では、マイクロプロセッサはその状態全体を保存し、SMM に入ります。

マイクロプロセッサが SMM に入ると、ハードウェア出力ピン SMI Active（SMIACT）がアサートされます。このピンは、マイクロプロセッサが SMM に入っているチップセットハードウェアに通知します。 SMI は、SMM 自体の中を除いて、どのプロセス動作モードでもいつでもアサートすることができます。チップセットハードウェアは SMIACT 信号を認識し、後続のすべてのメモリサイクルを SMM 専用に予約されたメモリの保護領域（SMRAM 領域とも呼ばれます）にリダイレクトします。 SMI 入力を受信し、SMIACT 出力をアサートした直後に、マイクロプロセッサは内部状態全体をこの保護されたメモリ領域に保存し始めます。

マイクロプロセッサ状態が SMRAM メモリに格納された後、特殊な SMM ハンドラコードも SMRAM に存在し（ブート時にシステム BIOS によってそこに置かれる）、特別な SMM 動作モードで実行を開始します。このモードで動作している間は、ほとんどのハードウェアとメモリの隔離メカニズムが中断されており、マイクロプロセッサはプラットフォーム内のほぼすべてのリソースにアクセスして必要なタスクを実行できます。SMM コードが必要なタスクを完了すると、マイクロプロセッサは前の動作モードに戻します。 この時点で、SMM コードは SMM を終了するために Return from System Management Mode（RSM）命令を実行します。 RSM 命令は、マイクロプロセッサに、SMM 入力時に SMRAM に保存されたコピーから以前の内部状態データを復元させます。RSM が完了すると、マイクロプロセッサ状態全体が SMI イベントの直前の状態に復元され、以前のプログラム（OS、アプリケーション、ハイパーバイザなど）は中断したところから実行を再開します。

[1] HP Sure Start コントローラハードウェアは、CSPN 認証フレームワークごとに認定されています。
[2] HP Protect Start with Dynamic Protection は、第 6 世代の Intel Core プロセッサ以上を搭載した HP Elite 製品で使用できます。
[3] Windows イベントビューアで HP Sure Start イベントを表示するには、HP Notification ソフトウェアをインストールする必要があります。
[4] 通知を受信するには、HP Notification Software がインストールされている必要があります。
[5] HP Sure Start Gen3 は、Intel 7th 世代プロセッサ搭載の HP Elite 製品で利用できます。
[6] HP Sure Start with Runtime Intrusion Detection は AMD 第 7 世代プロセッサ搭載の HP Elite 製品で利用できます。
[7] HP Sure Start Gen4 は、第 8 世代の Intel または AMD プロセッサを搭載した HP Elite および HP Pro 600 製品で利用できます。

Sign up for updates
hp.com/go/getupdate d

Share with colleagues

4AA7-2197ENW, February 2018