テクニカル ホワイトペーパー

HP Sure Start Gen3

第 7 世代インテル®Core™プロセッサ搭載
HP Elite 製品で利用可能
2017 年 1 月

目次

1 HP Sure Start Gen3

1.1 背景

HP は、クライアントデバイスのコンピューティングスタックのすべての層でセキュリティを実現することを目的とした、クライアントセキュリティの全体像を把握しています。 我々の焦点は、OS やクラウドベースのセキュリティソリューションだけではなく、「OS の下」に位置するデバイスのファームウェアとハードウェアのセキュリティも重要だと考えています。

我々の世界がより深く接続されるにつれて、サイバー攻撃は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ターゲットにして、その頻度や巧妙さが増しています。 デバイスファームウェアはハードウェア上で最初に実行され、OS を安全に起動する役割を担うため、ファームウェアを信頼できないとなるとクライアントデバイスの OS すらも信頼はできません。

すべての可能性のある攻撃を予見することは不可能なことではないとはいえ、それを行うことは非常に困難です。そのため、HP はクライアントデバイスに「サイバー回復能力」をもたせるべく、侵入された攻撃を検出しそこから回復する機能を設計に取り入れています。

HP Sure Start は、HP 独自の革新的なアプローチにより、強制力をもつハードウェアを使用して純正 HP BIOS のみでのブートするようにし、クライアントデバイスに高度な「OS の下」での保護を提供します。 さらに、HP Sure Start が HP BIOS の改ざんを検出すると、保護されたバックアップコピーを使用して純正 HP BIOS にリカバリすることが可能です。

1.2 HP Sure Start Gen3 概要

HP Sure Start Gen3(第 3 世代の HP Sure Start)には、以前の世代の HP Sure Start と同一のベースラインの機能に加えて、HP Sure Start の高度な保護、攻撃の検出、および HP システムファームウェアのリカバリを大幅に向上させる新機能が含まれています。[1] クライアントデバイスに追加される主な機能には、次の 2 つがあります：

- ランタイム侵入検知
- BIOS 設定保護

さらに、HP は Microsoft System Center Configuration Manager（SCCM）のプラグインを含む Manageability Integration Kit（MIK）の提供を開始し、既存の SCCM インフラストラクチャを使用して、既存および新しい HP Sure Start Gen3 機能を管理するための簡単なメカニズムを IT 管理者に提供します。このホワイトペーパーでの焦点は、MIK によって実現されるターンキーのリモート管理機能ではなく、上記 2 つの新しいクライアントデバイス機能になります。

1.3 ランタイム侵入検知(Runtime Intrusion Detection, RTID)

1.3.1 コンテキスト

HP Sure Start Gen3 ランタイム侵入検知機能が、Gen3 よりも前の HP Sure Start で提供されているベースラインの機能とどのように異なるのかを理解するために、**図 1** に示すベースラインの内容を確認することが有効です。この図は、これまでの HP Sure Start によって提供される内容の概要を示しています。このベースライン機能の焦点は、（起動時に）ホスト CPU が置換または変更されたファームウェアコードの実行を開始しないということを保証することです。 したがって、HP Sure Start は、OS を安全に起動するために必要なクライアントデバイスのハードウェアを安全に動作させる HP 純正の HP ファームウェアのみを起動するという保証を提供します。

HP Sure Start with Dynamic Protection の場合でも、起動時にホスト CPU によって実行されるシステムフラッシュの BIOS コードを監視することに重点が置かれていることに注意してください。[2] これは、システムが OS にブートされた後、電源管理やその他の重要なサービスを提供するためにメイン（DRAM）メモリに常駐する BIOS コードとは重要な違いになります。次に、その違いをより詳細に説明します。

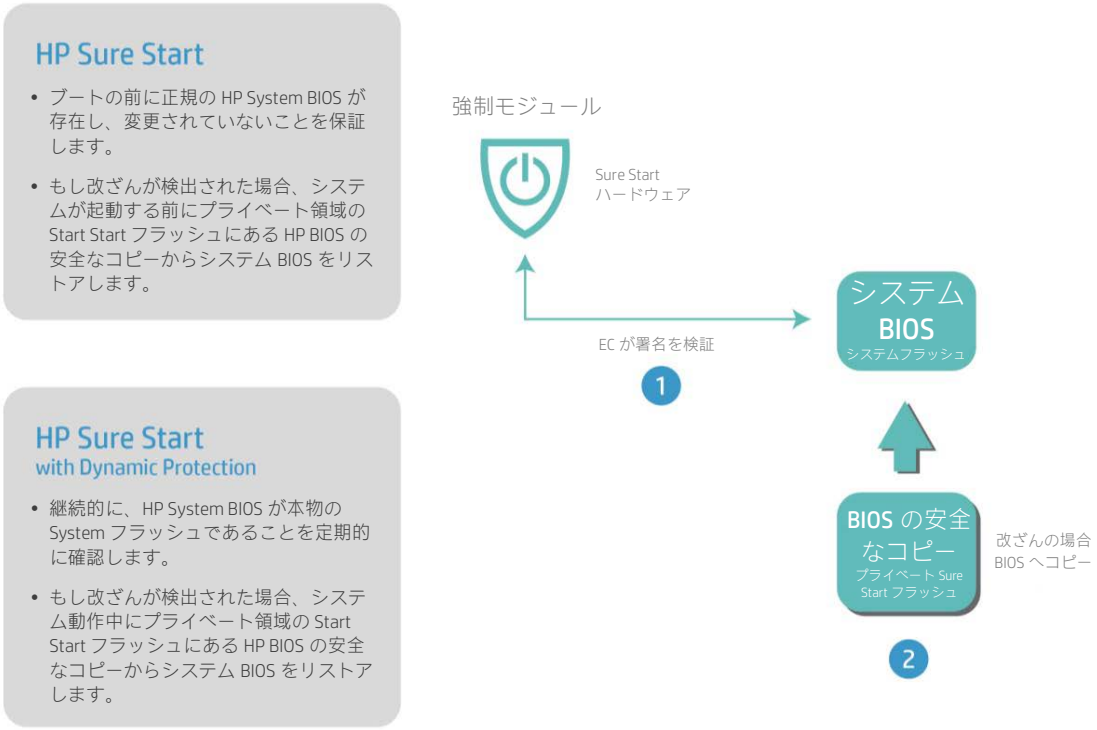

図 1 ベースライン HP Sure Start 概要（第 6 世代インテル ® Core™プロセッサ以降搭載の HP Elite 製品に適用）

1.3.2 ランタイム BIOS コード vs.スタートアップ BIOS コード

各起動時に、CPU は固定アドレスのフラッシュメモリから BIOS コードの実行を開始します。 この BIOS コードは、DRAM メモリを含むハードウェアを初期化し、すべてのルーチンをフラッシュメモリから揮発性（DRAM）メモリにコピーします。 その BIOS コードの大部分は、OS を起動する前に必要な「Pre-OS」機能を提供するために使用されます。 「Pre-OS」BIOS サポートの例には、ビデオドライバ、PXE ブートサポート、キーボードとマウスドライバ、プリブート認証、大容量ストレージ暗号化のロック解除などがあります。 これらのルーチンのほとんどは、OS が実行されるともう必要がなくなります。これらの機能は OS への受け渡し前にのみ関連するものであり、あるいは OS では別途独自のドライバがあるためです。

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。[3] このコードは、HP Sure Start のランタイム侵入検知の環境では「ランタイム」BIOS コードとも呼ばれます。

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の状態にとって重大です。 ベースラインの HP Sure Start の実装は、OS の起動時に DRAM に存在する SMM コードを含め、システムが起動するたびに***すべての***コードが HP BIOS であることを保証するところまでです。

OS の起動時に HP SMM BIOS コードの開始地点が良好であることを保証するだけでなく、さらに高度な保護へ向かうために残された機会としては、新しい保護機能を追加し、HP SMM BIOS コードを保護する既存のメカニズムをバイパスしようとするあらゆる攻撃を検出する手段を提供することによって、OS が稼働している間でも良好な状態を***保持する***ためのメカニズムを提供することです。

1.3.3 ランタイム侵入検知アーキテクチャ

図 2 は、ランタイム侵入検知（RTID）機能の実装の詳細を示しています。 RTID 機能は、プラットフォームチップセットの専用ハードウェアを使用して、ランタイム時の HP SMM BIOS に対する改ざんが試行されたかを検出します。 さらに、チップセットハードウェアは、SMM コンテキストで実行されているコードに動作制限を適用して、侵害された SMM コードを示す動作を検出して報告する機能を提供します。 これらの状態が検出されると、HP Sure Start ハードウェアに通知され、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。

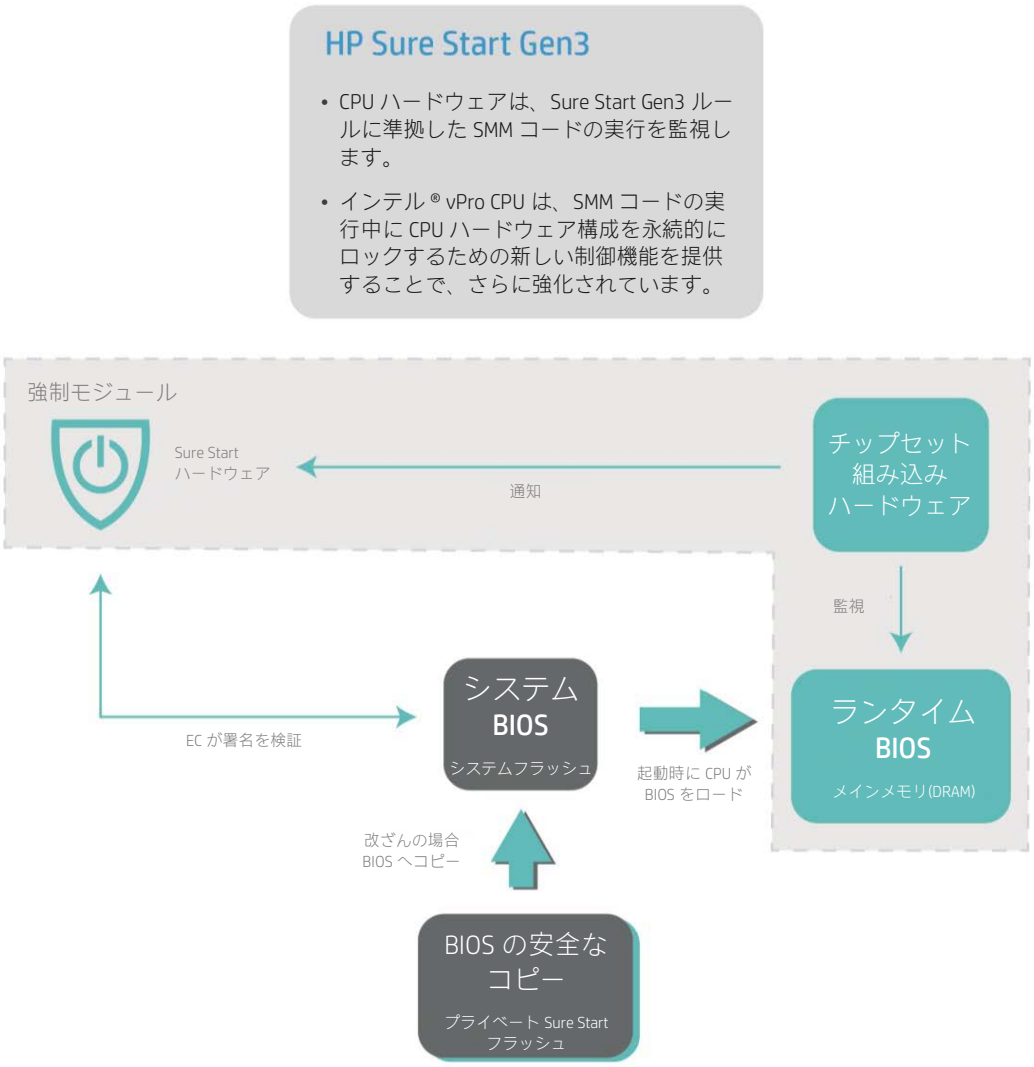

図 2 ランタイム侵入検知アーキテクチャ（第 7 世代インテル ® Core™プロセッサ以降搭載の HP Elite 製品に適用）

1.3.4 イベント

HP Sure Start RTID 機能は、HP SMM BIOS コードを改ざんする試行または SMM コードの動作異常が検出されたときに、HP Sure Start ハードウェアにイベントを生成します。 HP Sure Start ハードウェアは、BIOS セットアップにて設定されたイベントポリシーに従ってアクションを実行します。

イベントポリシーの設定にかかわらず、特定のイベントは常に HP Sure Start 監査ログに記録され、ローカルユーザーは RTID イベントの次の起動時に BIOS からの通知を受け取ります。

1.3.5 ポリシー制御

RTID 機能は、HP 工場から出荷される本機能を有するすべてのプラットフォームにてデフォルトで有効になっています。 HP Sure Start RTID を利用するために、利用者/管理者が機能を有効にしたり、別の方法で「展開」するような必要はありません！

オプションでプラットフォームの所有者/管理者が設定できる RTID 機能に関連する 2 つの BIOS ポリシーがあります：

- **エンハンスド HP ファームウェアランタイム侵入防御および検知** (有効/無効)
- **Sure Start セキュリティイベントポリシー**

1.3.5.1 エンハンスド HP ファームウェアランタイム侵入防御および検知

この BIOS ポリシー設定は、RTID 機能を有効または無効にします。 このポリシーのデフォルト設定は**有効**です。

1.3.5.2 Sure Start セキュリティイベントポリシー

この BIOS ポリシー設定は、RTID 機能が攻撃または攻撃の試行を検知したときに実行されるアクションを制御します。 このポリシーでは、次の 3 つの選択があります：

- **イベントログのみ**：この設定を選択すると、HP Sure Start ハードウェアは Microsoft Windows イベントビューアの「アプリケーションとサービスログ/ HP Sure Start」パスに検知イベントを記録します。[4]
- **イベントログとユーザー通知**：これはデフォルト設定です。 この設定を選択すると、HP Sure Start ハードウェアは検知イベントをログに記録します。このイベントは Microsoft Windows イベントビューアの「アプリケーションとサービスのログ/ HP Sure Start」パスで表示できます。 さらに、イベントが発生したことをユーザーに確認するメッセージが表示されます。[5]
- **イベントログとシステム電源オフ**：この設定を選択すると、HP Sure Start ハードウェアは Microsoft Windows イベントビューアの「アプリケーションとサービスのログ/ HP Sure Start」パスで検知イベントを記録します。 さらに、イベントが発生し、システムのシャットダウンを直ちに実行するかどうかをユーザーに確認するメッセージが表示されます。

1.4 BIOS 設定保護

1.4.1 コンテキスト

ベースラインの HP Sure Start では、HP BIOS コードの完全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、静的なため、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可能です。 BIOS 設定が持つダイナミックでユーザーが変更可能といった特性は、それらの設定を検証するためにデジタル署名を HP が生成することができず、HP Sure Start ハードウェアが利用できないため、これらの設定を保護するためにさらなる課題を引き起こします。

1.4.2 BIOS 設定保護 概要

HP Sure Start Gen3 BIOS 設定保護は、HP Sure Start ハードウェアを使用して、ユーザーが選択したすべての BIOS 設定のバックアップおよび整合性のチェックを実施し、システムを構成する機能を提供します。

プラットフォーム上でこの機能が有効になっている場合は、その後 BIOS で使用されるすべてのポリシー設定がバックアップされ、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。 変更が検知された場合、システムは HP Sure Start で保護された領域からのバックアップを使用して、自動的にユーザー定義どおりの設定に戻ります。

1.4.3 イベント

HP Sure Start BIOS 設定保護機能は、BIOS 設定に対して変更の試行が検知された時に HP Sure Start 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中に BIOS から通知を受け取ります。

1.4.4 ポリシー制御

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、クライアントデバイスの所有者/管理者は、まずすべての BIOS 設定を要望に沿った内容に設定する必要があります。 所有者/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もあります。

それが完了したら、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 で保護された記憶域に作成されます。 以降は、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 設定が変更可能となります。

2 付録 A

2.1 システム管理モード(SMM) 概要

システム管理モード（SMM）は、PC の高度な電源管理の機能と OS 動作中の他の OS 非依存の機能に使用される業界標準のアプローチです。 SMM の用語と実装は x86 アーキテクチャに基づくものですが、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 は起動時に BIOS によって設定されます。 SMM コードはメイン（DRAM）メモリに読み込まれ、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していない間はこの領域へのアクセスをブロックします。 ランタイム中において、SMM モードへの移行はイベント駆動型になります。 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）入力のピンをアサートします。 次の命令の境界で、マイクロプロセッサはその全体の状態をセーブして SMM に移行します。

マイクロプロセッサが SMM に入ると、ハードウェア出力のピン、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 に入っていることをチップセットハードウェアに通知します。 SMI は、SMM 自体中を除いて、どのプロセス動作モードであって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 のシグナルを認識し、後に続く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 入力を受信して SMIACT 出力をアサートした直後に、マイクロプロセッサは全体の内部状態をこの保護されたメモリ領域へ保存し始めます。

マイクロプロセッサの状態が SMRAM メモリに格納された後も、SMRAM にある特別な SMM ハンドラコード（ブート時にシステム BIOS によってその領域に置かれます）は、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、ほとんどのハードウェアおよびメモリアイソレーションのメカニズムは中断され、マイクロプロセッサはプラットフォーム内のすべてのリソースに仮想的にアクセスが可能となり、必要なタスクを実行できるようにします。 SMM コードは必要なタスクを完了すると、マイクロプロセッサを前の動作モードに戻す時間になります。この時点で、SMM コードは SMM を終了するためにシステム管理モードからの復帰（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その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）は中断した場所から実行を再開します。

1. HP Sure Start Gen3 は、第 7 世代 Intel Core プロセッサ以降を搭載した HP Elite 製品で利用可能です。
2. HP Sure Start with Dynamic Protection は、第 6 世代 Intel Core プロセッサ以降を搭載した HP Elite 製品で利用可能です。
3. SMM の詳細と動作方法については、付録 A を参照してください。
4. 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 Software がインストールされている必要があります。
5.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。