テクニカルホワイトペーパー

HP Sure Run

HP PC のハードウェア強制されたアプリケーション永続性

HP Sure Run は、ハードウェア強制アプリケーション永続化ソリューションで、OS の実行中にポリシー適用ハードウェアとの通信を維持する機能を備えています。OS 内の HP Sure Run エージェントが攻撃または削除された場合でも、重要なサービスおよびアプリケーションの存在を継続的に監視します。 HP Sure Run はハードウェアレベル（OS より下）で HP エンドポイントセキュリティコントローラーと相互作用し、OS の完全性を保ちます。一部の HP 製品 [1] に追加費用なしで含まれています。

目次

重要な OS のサービスと設定に対するマルウェアの影響

組織は、PC を安全かつ安定に保つために、ソフトウェアセキュリティプロセスを導入しています。例えば、既知のマルウェアから保護するために、ウィルス対策ソフトを使用しています。HP Device Access Manager は、許可されたユーザーだけが外部デバイスにデータをコピーできるように、USB ポートを保護し、マルウェアによるファイルのコピーの脅威を最小限に抑えます。 Windows ® OS では、暗号化サービスが機密データの保護に役立ちます。

これらの重要なサービスやアプリケーションを強制終了することで、マルウェアは発見されずに企業に深く侵入することが出来るようになります。例えば、H1N1 マルウェアファミリは、4 種類の Microsoft ® Windows セキュリティサービス（Windows ファイアウォール、Windows セキュリティセンター、Windows Defender、および Windows Update サービス）を強制終了しようとします。

これらのタイプの攻撃を防ぐために、組織は、OS 内の重要なサービス、アプリケーション、設定を確実に維持し、適切に設定する必要があります。多くの企業は、最新の OS やサードパーティのソフトウェアソリューション内のプロセスを利用して、PC アプリケーションを保護しています。ただし、これらはソフトウェアのみのソリューションであるため、マルウェアによる削除の対象とすることもできます。 理想的なソリューションは、マルウェアが削除または無効にすることができないように、オペレーティングシステムの外部から必要なポリシーを監視して強制することです。

HP Sure Run は重要なプロセスを保護します

HP Sure Run を搭載した HP ビジネス PC は、起動時ごとに Windows に直接エージェントをインストールし、OS の実行中にポリシー適用ハードウェアとの通信を維持する機能を備え、ハードウェア強制アプリケーションの永続性を提供します。HP Sure Run は、既存の HP Endpoint Security Controller ハードウェアをベースとして、オペレーティングシステムの望ましい状態を継続的に維持します。これには、常に実行する必要があるアプリケーション、特定の状態に留まるべきポリシー設定、または常に存在しなければならない特定の機能が含まれます。

HP エンドポイントセキュリティコントローラは、起動時および実行時に PC のファームウェアを保護するために HP Sure Start が構築されている回路基板上のハードウェアコンポーネントです。HP Sure Run は、このような（HP Sure Start のような）保護機能を OS の中に拡張しています。このプロセスでは、最も重要なプロセスやアプリケーション（Windows セキュリティセンターなど）を保護し、マルウェアがシャットダウンしようとすると自動的に再起動します。OS 自体の HP Sure Run エージェントが攻撃された場合、HP エンドポイントセキュリティコントローラーはこの状態を検出し、設定されたポリシーアクションを実行します。

HP Sure Run は、脅威を検出したり、設定やアプリケーションを修復したりすると、Windows アクションセンターでユーザーと管理者に警告します。これらのアラートは、プロセスが一時停止または終了したこと、ストレージドライブ上でプロセスファイルが削除されたこと、重要なレジストリ設定が変更されたことなどをカバーします。

HP Sure Run は、第 8 世代の Intel ® または AMD ® プロセッサーを搭載した HP Elite 製品で追加料金なしでご利用いただけます。

動作の仕組み

HP Sure Run には、HP エンドポイントセキュリティコントローラーによってプラットフォームのハードウェアに格納されているポリシーを強制適用するための OS エージェント [2] が含まれています。
HP Sure Run エージェントのコピーも、HP Endpoint Security Controller によってプラットフォームハードウェアに格納されていて、ファームウェアによって自動的にオペレーティングシステムに直接インストールすることができます。
HP Sure Run エージェントは、HP エンドポイントセキュリティコントローラハードウェアとの安全な通信リンクを持っています。このリンクは、ポリシーパッケージを取得し、ステータスを HP エンドポイントセキュリティコントローラに通知するために使用されます。

HP Sure Run エージェントは、監視するように構成されたアプリケーション、プロセス、ポリシー設定、および OS 機能を監視します。保護される項目は、HP セキュリティ製品、HP プロセス、サードパーティ製プロセス、

および Windows OS プロセスの 4 つの主要カテゴリに分類されます。Windows セキュリティセンターは、HP Sure Run で保護された重要なアプリケーションの優れた例です。

HP Sure Run エージェントは、クリティカルなサービスやアプリケーションを再起動するか、ポリシーに違反していると思われるアイテムのポリシー設定を復元するアクションも実行できます。HP Sure Run は、マルウェアによる改ざんを防止するために、孤立した HP エンドポイントセキュリティコントローラのメモリに保存されているポリシーに基づいて実行します。

OS 起動時（構成時）

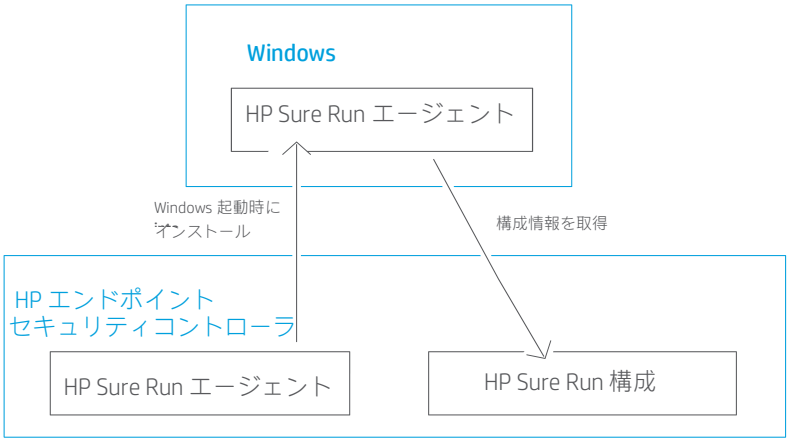

図 1. HP Sure Run を構成後の OS 起動時の動作

OS 実行中

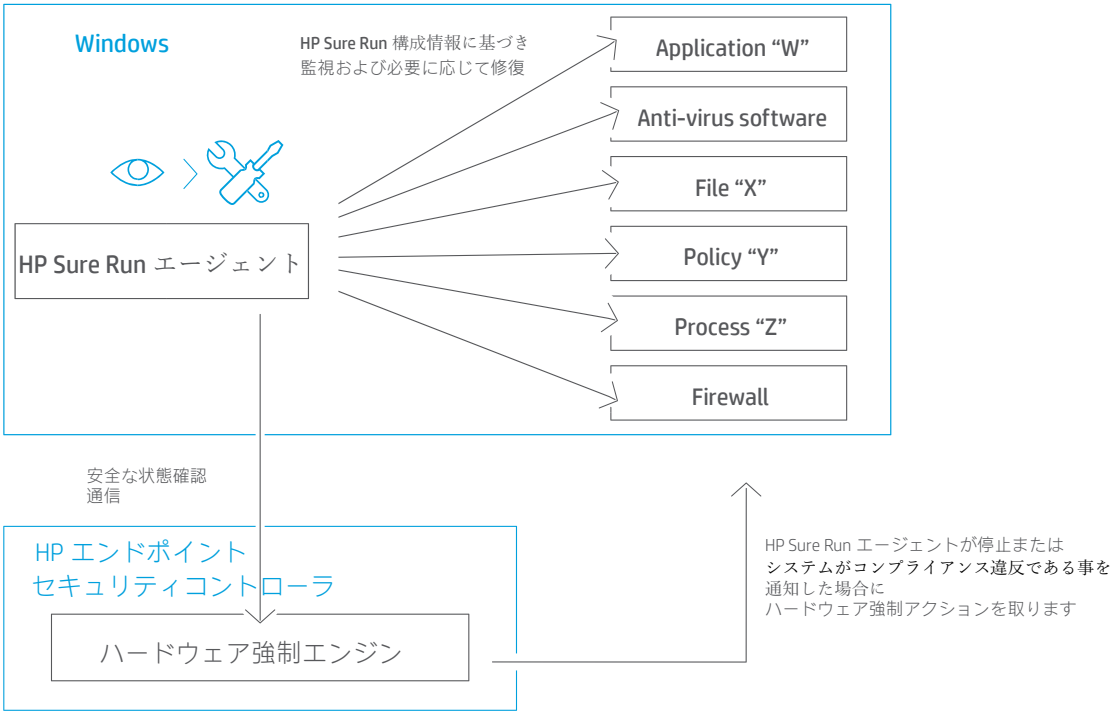

図 2. OS 実行中の HP Sure Run による監視および修復.

有効化および管理方法

HP Sure Run はデフォルトでは有効になっていません。 **HP Sure Run** によって監視される特定のアプリケーション、ポリシー、および機能の有効化と設定は、**HP** イメージにあらかじめインストールされている **HP Client Security Manager** ソフトウェアを使用して、ユーザーまたは **IT** 管理者がローカルで設定できます。また、**HP Sure Run** は、**Microsoft System Center Configuration Manager**（**SCCM**）用の **HP Management Integration Kit**（**MIK**）プラグインを使用して、安全に有効にして設定することができます。

リモート設定

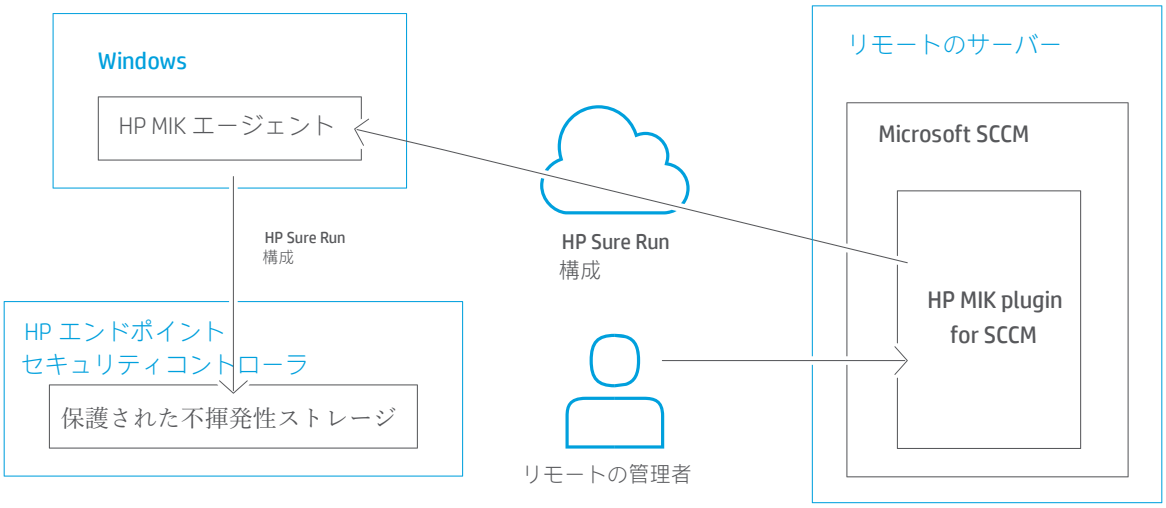

図 3. HP MIK plugin for Microsoft SCCM による HP Sure Run のリモート設定.

ローカル設定

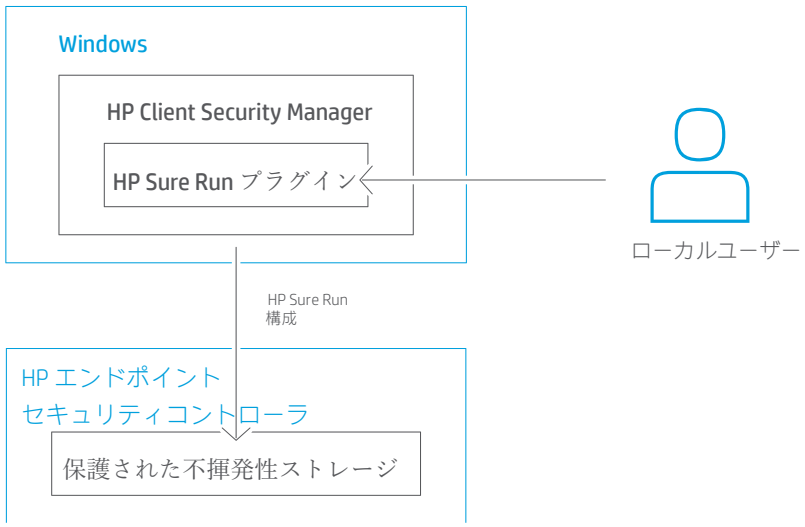

図 4. ローカルユーザーまたはシステム管理者による HP Sure Run のローカル設定.

結論

HP Sure Run によって提供されるハードウェア強制アプリケーションの永続性によって、重要なサービスおよびアプリケーションを保護します。HP Sure Run は対応する HP Elite PC でのみ利用できます。

関連情報 hp.com/go/computersecurity

[1] HP Sure Run は、Intel または AMD の第 8 世代プロセッサ搭載の HP Elite 製品で利用できます。
[2] Windows 10 RS2 以上。

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

Share with colleagues

4AA7-2200ENW, February 2018