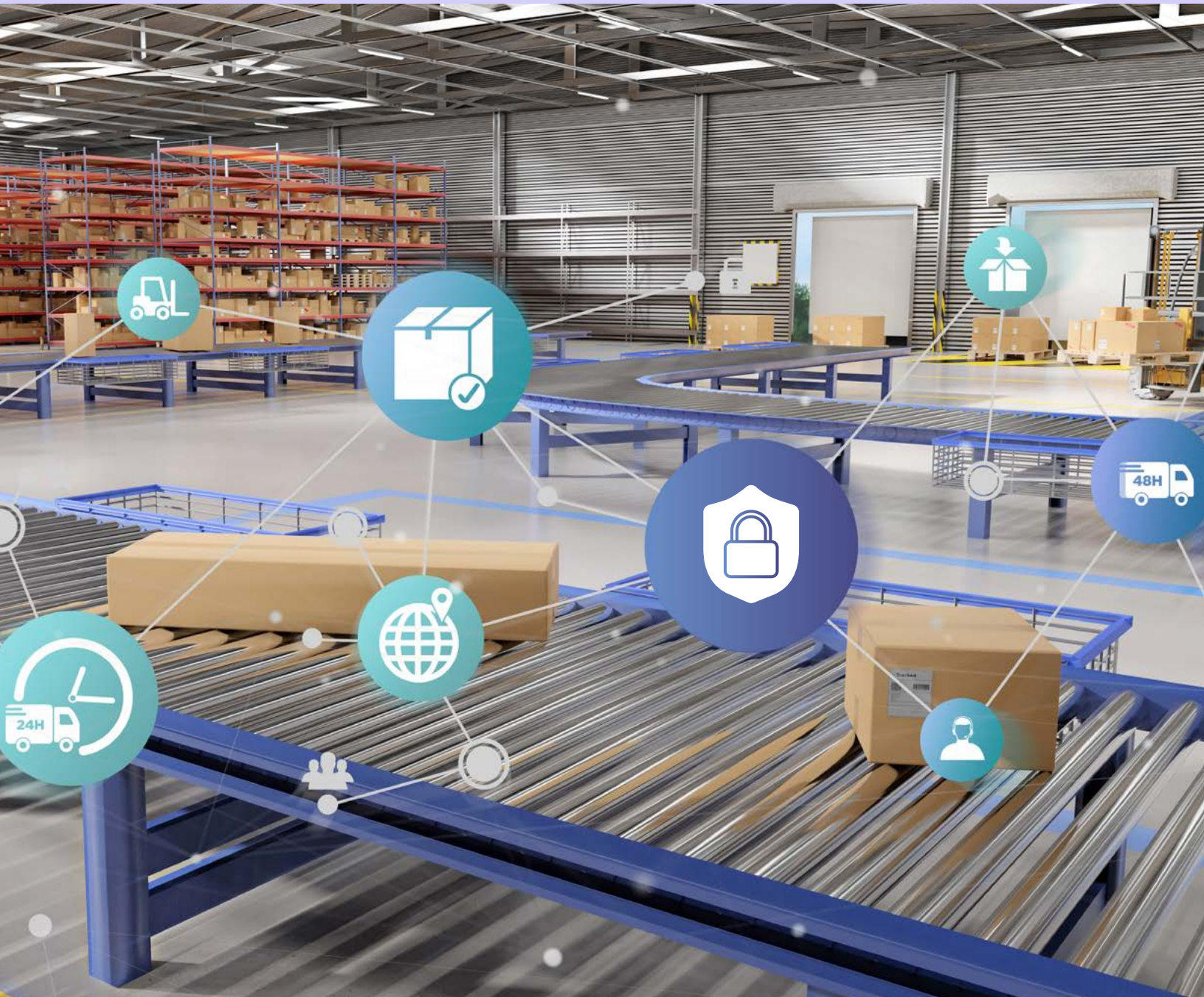
HP Inc.
サプライチェーン
セキュリティ

現代のサプライチェーンを守る

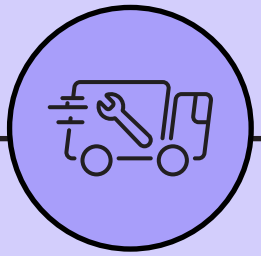


目次

HP サプライチェーン - 現代のサプライチェーンを守る

HP社内のセキュリティ

- HP セキュリティ開発ライフサイクル (SDLC)
- 情報セキュリティ
- 人的セキュリティ

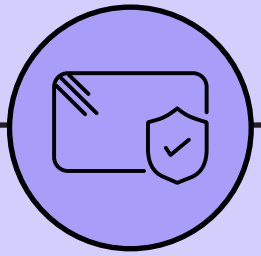


製造から配送のセキュリティ

- サプライヤーリレーション管理
- セキュアな製造環境
- 偽造防止
- 物理的セキュリティ
- 配送

サプライチェーンサービス

- イメージ&アプリケーションサービス
- ダイナミックコンフィギュレーションサービス
- カスタムシステム設定サービス
- カスタムセキュリティタグ
- HP TamperLock



製品に組み込まれたセキュリティ

- パーソナルコンピューター
- プリンター

Go to content

概要

PricewaterhouseCoopersの第25回目の年次グローバルCEO調査（PWC Emerging techs and cyber trends - HP、2022年11月15日）によると、CEOはサイバー脆弱性を将来の企業成長に対する最も重大な脅威のひとつと見なしていることが明らかになりました。調査対象となった企業の25%以上が、過去3年間に100万USドル以上のデータ侵害に対処しています。さらに、少なくとも11%のCISOとCFOが1,000万USドル以上の被害を報告しています。また、HP Wolf Security 脅威インサイトレポートでは、システム全体を制御するファームウェア攻撃から、ソフトウェアサプライチェーンのランサムウェア攻撃まで、あらゆる形態のサイバー関連攻撃の増加が報告されています。ハイブリッドワーカーと増え続ける外部脅威の環境において、エンドポイントデバイスは、私たちが保護すべきデータとリソースを守る最初の防衛線です。

HPは、設計から製造、配送に至るまで、製品ライフサイクルのすべてのステージにおいて、実績のあるセキュリティとプライバシーの原則に従い、常にお客様のサプライチェーンを安全に保つための機能と保護を提供しています。当社のサプライチェーンに組み込まれたセキュリティに加え 当社の製品には業界をリードするセキュリティ機能が組み込まれています。保護、検知、復旧は、当社のデバイスに設計段階から組み込まれ統合されています。サプライチェーンと製品のセキュリティ戦略の連携は、HPの製品サイバーセキュリティプログラムの基盤です。

HPのサプライチェーンセキュリティは、米国政府の国立標準技術研究所（NIST）800-161 Supply Chain Risk Management Practices、Open Trusted Technology Provider™ Standard（O-TTPS）、主要なサイバーセキュリティ専門家によるガイダンス、およびHP内部のリスク分析グループに基づいています。当社の「製品サイバーセキュリティ基準」は、サプライチェーンライフサイクル全体を通じて当社製品の完全性を保護するための要件を特定しています。

HP社内のセキュリティ

HP セキュリティ開発ライフサイクル (SDLC)

HPのセキュリティ開発ライフサイクル（SDLC）は、ハードウェア、ソフトウェア、ファームウェアなど、製品開発の初期計画、設計ステージからテスト、導入、保守に至るまで、あらゆるステージにセキュリティを統合しています。当社の目標は、潜在的脆弱性を特定し開発プロセスのすべてのステップで対処し、設計上安全（Secure by Design）な製品を作成することです。

製品チームは、新製品の機能や特徴を開発する際にHPのSDLCを活用し、HPのサイバーセキュリティスペシャリストは開発ライフサイクル全体を通してレビューを行います。SDLC を使用して開発された HP の製品とコンポーネントには、次のような活動が含まれます：

- アーキテクチャと設計の詳細なセキュリティレビュー
- アタックサーフェスの分析に基づく、新しい機能や製品の脅威分析
- Open Worldwide Application Security Project（OWASP）のセキュアコーディングプラクティスに従った、ソフトウェアの静的および動的コード分析
- 我々の脅威評価の結果を使用し、業界をリードする脆弱性評価スキャナー（例：Qualys や TenableのNessusTenable）を利用したアプリケーション侵入テスト

このプロセスを通じて、HPはセキュリティリスクを特定し緩和しています。

情報セキュリティ

HPの社内IT環境は、システムの堅牢化、ウイルスやマルウェアの保護と緩和策、強力なパスワードの強制、多要素認証、E メール添付ファイルのスキャン、システムとアプリケーションのパッチ遵守、侵入防止、ファイアウォール、堅牢な障害復旧と事業継続計画などの管理を通じて保護されています。

HPは、重要データへのアクセスを削減するために、アクセス制限やユーザーアカウント権限の限定を含むベストプラクティスを採用しています。これらのプラクティスは、機密情報へのアクセスが、割り当てられた職務を遂行するために必要な範囲でのみ許可されることを保証しています。

人的セキュリティ

セキュリティは、HPの企業文化に組み込まれています。積極的なセキュリティ文化を促進するため、当社は従業員の優れたセキュリティ行動を奨励しています。HP のセキュリティ意識向上基準には、セキュリティ意識向上トレーニング、フィッシング演習、ニュースレター、従業員を対象としたサイバーセキュリティトレーニングなどがあります。

HP のポリシーでは、国の法律および労働者評議会に従い、従業員が雇用前チェックを受けることを義務付けています。このプロセスには、セキュリティバックグラウンドチェック、身元確認、申請情報の確認が含まれます。各国の法律で許可されている限り、HP は、従業員と業務委託者が、知的財産、顧客情報、およびその他の機密データを保護するための機密保持契約に署名することを徹底しています。

HPは、HPのサプライヤーおよびパートナーが同じ高いセキュリティ基準に従うよう、注意深く努力しています。

製造から配送のセキュリティ

サプライヤーリレーション管理

HPのサプライヤー選定プロセスは、当社の調達スペシャリストがエンジニアリングチームと協力することから始まります。彼らは共に、技術的要件、国や地域のニーズ、コスト、財務の健全性、製造およびサプライチェーンの能力、品質などを考慮します。HPのドキュメント化された基準は、安全なインフラストラクチャを維持し、信頼できるサプライヤーから本物の部品を提供し、偽造品回避プログラムを維持する責任をサプライヤーに課しています。

- コンプライアンス - HP は、サプライチェーンパートナーとリセラーに対し、システムセキュリティ、グローバル取引、顧客のプライバシーに関わるすべての法的要件と規制要件に準拠することを求めています。
- 監視 – 専任の製品サプライチェーンサイバーセキュリティコンプライアンスチームが統制し、リスクの特定と是正活動を実施します。
- 基準 – HP のサプライヤー向け製品サイバーセキュリティ基準は、コンポーネントの調達、製品設計、製造、保管、および輸送に関する要件を定めています。
- 検証 – 実施状況を監視し、問題があれば特定し解決するためのプログラムとプロセスが用意されています。

コンプライアンスを確保するため、HPはサプライヤーの継続的なセキュリティレビューを実施しています。

セキュアな製造環境

製造業のセキュリティは、安全な工場環境から始まります。当社の製造施設は、システムの堅牢化、パッチ管理、ウイルス検知、マルウェアからの保護と緩和策、強力なパスワードの強制、侵入防止、ファイアウォール、堅牢な障害復旧と事業継続計画など、当社のサイバーセキュリティ基準を満たす必要があります。

さらに、HPは以下のセキュリティ対策の技術とプロセスを採用しています：

- 工場およびサプライチェーンのネットワークをセグメンテーションし分離する。
- 従業員およびパートナーにアクセスバッジを義務付ける。
- サイバーセキュリティ基準の遵守を監査し、是正活動を管理する。

PCソフトウェアイメージのセキュリティ

HPは、すべてのPCにおけるソフトウェアイメージとファームウェアのローディングとライセンスを保護しており、これは、高度なセキュリティを備えた製品を製造するというHPの戦略的目標に沿ったものです。

ソフトウェアイメージは、OS、ドライバー、要求されたサードパーティ製アプリケーション、およびシステムの運用をサポートするために必要な各種ツールで構成されます。ソフトウェアイメージは、安全なチャンネルを通じて工場に送信され、安全な環境に保管されます。イメージのロードプロセスは厳重に管理されます。ソフトウェアイメージはハッシュ化され、開発からPCへのロードまで、すべての工程でチェックされます。イメージのロードプロセスはISO 27001:2013の認証を受けています。

プリンターファームウェアのローディングセキュリティ

プリンターのファームウェアは、PCのオペレーティングシステムと同様に、ハードウェア機能を調整し、コントロールパネルを実行し、ネットワークセキュリティを提供し、印刷、スキャン、Eメール送信時に利用可能な機能を決定しています。工場でインストールされたファームウェアは検証され、HPによってデジタル署名された信頼できる既知の正しいHPコードのみがデバイスにロードされます。デバイスの起動プロセス中にコード署名が検証されない場合、デバイスは安全なリカバリ状態にリブートし、有効なファームウェアアップデートを待ちます。コントロールパネルのメッセージは、特定された不正なファームウェアコードをユーザーに通知します。

Go to content

偽造防止

HPの偽造部品検知および回避システムは、国防省調達規則（DFARS）252.246-7007の基準に合致しており、当社のサプライチェーン全体で偽造部品を防止または特定し、排除するためのベストプラクティスに従っています。私たちは全ての部品サプライヤーと製造施設に対して、従業員トレーニング、サプライヤーからHP製品製造施設までの部品の追跡、電子部品の検査とテスト、偽造部品が確認された場合の排除など、偽造防止基準に準拠しているかどうかを評価します。当社の調達プロセスでは、部材がHPの承認ベンダーからのみ調達され、部品表と一致していることを確認しています。

HP は解決のために、偽造または汚染された製品に関するすべての要請について追跡調査を行います。これには、必要に応じて、調査および評価、根本原因の究明、再発防止、製造および流通チャネルからの不適合製品の排除を行う事が含まれます。HP は脅威と脆弱性を、適用される規制と業界の報告基準を満足または上回る水準で、関連する政府機関に報告します。また、顧客、パートナー、利害関係者にも報告し、各自が対応策を講じることができるようにします。

HPプラットフォーム証明書

HPプラットフォーム証明書により、IT管理者はPCとそのコンポーネントの信頼性と完全性を評価し、組織に潜在的な脅威をもたらす可能性のある不正な変更を発見することができます。この証明書を使用して、PC が正規の HP デバイスであることを確認できます。未承認の変更は、PC がサプライチェーンを通じて移動中に改ざんされたことを示す可能性があり、これは組織のセキュリティリスクとなります。IT部門にPCの完全性を認証する機能を提供することで、バックドアによるセキュリティ侵害の潜在的なリスクを低減し、リモートPCをネットワークにオンボードし接続する際の信頼性を高めることができます。

物理的セキュリティ

HP の製品や注文が製造、カスタマイズ、または履行される施設は、TAPA（Transported Asset Protection Association）、ASIS（American Society for Industrial Security）、ISO（International Organization for Standardization）、BASC（Business Alliance for Secure Commerce）等の国際的に認知された物理的セキュリティ規格に準拠していることを証明する必要があります。

HPの工場は、専任のサイトセキュリティおよび盗難防止担当者、アクセス制限、警報システム、ビデオ監視、動体検知システム、制限付き高価値ケージ、定期的な監査などの物理的セキュリティ保護を行っています。

配送

HPのパッケージングセキュリティと追跡

HPは、生産、保管、輸送、最終顧客までのすべての過程において、改ざんに対するセキュリティを提供するための技術とプロセスを備えています。輸送中の製品については、出荷を追跡・監視し、経路の逸脱や予定外の停止などの異常を確認することで、製品が意図した目的地に安全に到着するようにしています。HPは、HP TamperLockやHP Sure Adminのような追加の物理的セキュリティ機能を提供しています。

HPは、TAPAの施設セキュリティ要件（FSR）および輸送追跡セキュリティ要件（TSR）に準拠しています。これらの要件には、安全な取り扱いと保管、改ざん防止包装、施錠可能なハードサイドトレーラー、ドア開閉検知機能付きGPS追跡、トラック輸送担当者の長時間の休憩のための承認された安全な駐車場などが含まれます。TAPAサプライチェーンセキュリティ基準に加え、HPはTAPA要件を上回る独自のサプライチェーンセキュリティ基準を実施し監査しています。

サプライチェーンサービス

HPでは、お客様の時間とコストを節約するために、製造工程中に工場で実行される40以上のカスタマイズサービスを提供しています。詳細については、HPのコンフィギュレーションサービスのWebサイトを参照してください。

イメージ&アプリケーションサービス

イメージ&アプリケーションサービスは、製造プロセスにおいて、お客様指定のソフトウェアイメージとアプリケーションをHP PC製品にインストールします。お客様は、すぐにインストール可能なPCソフトウェアイメージを提供するか、またはHPに構築とロードを依頼することができます。HPでは大量に配布する前に、ソフトウェアイメージを体系的にスキャン、テスト、検証します。OSリカバリドライブが組み込まれたPCを購入された場合、お客様のご希望のイメージを内蔵ドライブにロードし、迅速なイメージ復旧を可能にします。

ダイナミックコンフィギュレーションサービス

HPのダイナミックコンフィギュレーションサービスにより、お客様は安全なVPN接続を通じてHPの工場やステージングセンターにイメージング環境を拡張することができ、出荷前の新しいPCの主要なコンフィギュレーション作業を直接コントロールすることができます。この接続により、お客様はイメージ、アプリケーション、ドメイン参加、HDD暗号化、BIOS設定、ユニットの個人設定をダイレクトに管理および構成することができます。

HPプラットフォーム証明書

HPプラットフォーム証明書は、工場出荷時にデバイス構成に対応する安全な暗号化されたプラットフォーム証明書を作成するサービスで、IT 部門は、デバイスが手元に届くとすぐにそのシステムとコンポーネントの完全性を検証できます。これは、HP認証局によって署名された証明書内の暗号による検証可能なアーティファクトを提供することによって提供されます。HPプラットフォーム証明書による PC の完全性の検証は、シームレスでスケーラブルです。HPはAPI経由でそれぞれのHP プラットフォーム証明書を安全に提供するため、IT部門は複数の証明書を同時にダウンロードすることがます。また、これらのデジタル証明書をダウンロードしてPCの完全性を検証する自動化プロセスを、組織の既存の展開プロセスに統合する柔軟性を提供します。HPプラットフォーム証明書は、最新のTCG（Trusted Computing Group）標準に準拠しています。

カスタムシステム設定サービス

ファクトリーカスタムシステム設定サービスは、お客様のご要望に応じてPCのBIOSパラメータを設定します。BIOS設定のカスタマイズにより、企業環境へのPCユニットのシームレスな導入を支援し、生産性を向上させます。

カスタムセキュリティタグ

HPラベリングおよびタグサービスは、ほとんどのHPのビジネス用ノートブック、ワークステーション、シンクライアント、デスクトップ、およびリテールPOS（RPOS）ソリューションでグローバルに利用できます。HPのファクトリープロセスは、一貫して印刷されメーカー標準と顧客要件に従ってセキュアに貼付されたラベルを提供します。

HP TamperLock

HP TamperLock ソリューションは、ハードウェアによるセキュリティと、PC ケースが開けられたかどうかを検知するセンサーを組み合わせたものです。検知されたイベントに対するポリシーには、有効なBIOS認証情報が入力されるまで起動をブロックする、TPMをクリアしてBitLockerキーなどのすべてのユーザーキーを削除する、カバーが取り外されたときにシステムの電源をオフにするなどがあります。

製品に組み込まれたセキュリティ

パーソナルコンピューター

HP PCは設計からライフサイクルの終了までシステムを保護する、業界をリードするセキュリティ技術で作られています。

HP Endpoint Security Controller

HP PCには、ハードウェアに基づくプラットフォームのルートオブトラスト（RoT）として鍵となるセキュリティ機能を担う専用のEndpoint Security Controller（ESC）が搭載されています。このRoTは"Secure by design"アーキテクチャの一部で、以下のセクションで詳述する他の多くのセキュリティソリューションの原動力となっています。

ハードウェアに組み込まれたセキュリティ

HPのシステムには、ハードウェアベースのプラットフォームルートオブトラスト(RoT)技術を活用し、安全なシステム起動を保証するソリューション、HP Sure Startが搭載されています。HP Sure Start は、IT部門の手間なしでファームウェアへの攻撃や破損を自動的に検知、停止、復旧します。PC の電源を入れるたびに、HP Sure Start は自動的にファームウェアの完全性を検証し、悪意のある攻撃から PC を確実に保護します。PCが起動すると、ランタイム侵入検知がランタイムファームウェアを常時監視します。攻撃があった場合、PCは隔離されたファームウェアと設定の「ゴールデンコピー」を使用し数分で自己修復することができます。

運用のセキュリティ

HP Sure Runは、HP Endpoint Security Controllerによって監視されるOS上のソフトウェアエージェントで、重要なプロセス、サービス、アプリケーションの動作状況を継続的に監視し、警告を発します。HP Sure Runエージェントには、強制終了防止機能が含まれており、プロセス、サービス、アプリケーションが中断されると、自動的に再インストールします。アンチウイルスやカスタムアプリケーションなど、HP Sure Runによる監視が設定されたアプリケーションは、攻撃によって停止した場合、自動的に再起動されます。

PC設定/デバイスの改ざん防止

HP Sure Admin は、悪意のあるリモートおよびローカルの BIOS設定変更を防止するためのパスワードレス認証を提供し PCを保護します。PKIを使用し、HP Sure Adminはセットアップを HPコンフィギュレーションサービスを介して工場で行うことも、顧客自身で行うことも可能で、その後すべてのBIOS設定は暗号による安全な方法で行うことができます。ローカル管理では二要素認証が要求され、特定のPCの設定を変更する権限を持つ、事前に登録されたローカル管理者だけが変更を行うことができます。

HP TamperLock は、HP Endpoint Security Controller のハードウェアで強化されたセキュリティと、PC ケースの開放を検知して警告するセンサーを組み合わせたものです。設定イベントには有効なBIOS認証情報が入力されるまでのブートの停止、TPMをクリアしてBitLockerキーなどのすべてのユーザーキーの削除、カバーが取り外されたときにシステムの電源オフなどが含まれます。

セキュアなOS復旧

プリブートソリューションとしてシステムのハードウェアとファームウェアに組み込まれたHP Sure Recoverは、破損したOS、ドライバー、アプリケーションを最後に確認されたイメージに戻します。このソリューションは、クラウドから設定されたイメージにアクセスすることで、プリブートワイヤレスネットワーキングを使用してシームレスに復旧を行います。HP Sure Recoverでは、自動、スケジュール、ユーザー指示の3つのリカバリ方法が利用可能です。HP Sure Startと組み合わせることで、HP Sure Recoverは、OS、ドライバー、アプリケーションを含む破損したソフトウェアに起因する問題を迅速かつ簡単に自動的に修復することができます。この復旧は、HP ESCによって安全に保護された組み込みのOSリカバリードライブを使用することで、より高速に、またはネットワーク接続がない場合にオフラインで行うこともできます。

Go to content

プリンター

HPは、多層的なセキュリティ保護を保証するために、縦深型の防御アプローチを活用したサイバーレジリエンスを有するプリンターを開発しています。HPのプリンターは、新しい脅威に適応しながら、継続して脅威を検知して阻止する、常に安全な技術を中核に据えた業界最強のセキュリティを備えています。

ハードウェアに組み込まれたセキュリティ

起動ライフサイクルの最初のステップはBIOSのロードです。このコードはルートオブトラスト（RoT）であるため、保護されていることが不可欠です。HP Sure Start 技術はBIOS コードの完全性を検証し、BIOS が侵害された場合に自己修復機能を提供します。BIOSはハッシュ化され、署名され、ブート時に検証されます。BIOSが侵害された場合、デバイスは元のイメージに戻すことができます。

起動ライフサイクルの第2ステップは、デバイスが HP 認証コードのみをロードすることを保証することです。HPは、正規の、改ざんされていない、実行可能なコードのみがHPのプリンタで実行できるようにする動的許可リスト技術を提供しています。許可リストは、ウイルス対策スキャナが既知のマルウェアのフィンガープリントを識別するために使用する拒否リストよりも効果的です。

運用のセキュリティ

HP Connection Inspectorは、HP Labsが特許を取得した技術で、プリンターがマルウェア攻撃の一歩先を行くことを支援します。この技術は、アウトバウンドネットワーク接続を検査し、何が正常かを判断し、疑わしい活動を阻止します。プリンターがネットワークの異常を検知すると、自動的に再起動を開始してHP Sure Start自己復旧プロセスを開始し、設定されている場合はセキュリティイベントをSIEMツールに自動的に送信します。

HP Memory Shieldは、プリンターに対する悪意のある攻撃を検知し、検知された場合は自動的に自己修復します。プリンタは工場出荷時のイメージにロックダウンされ、製造元で定義されていない呼び出しや操作の実行を防止します。HP Memory Shield は、ランタイム侵入検知（RTID）と呼ばれるハードウェアで保護されたソリューションを使用して、メモリーに異常がないかアクティブにスキャンします。異常が発生した場合、デバイスは再起動を実行し、潜在的なマルウェアのメモリをフラッシュし、既知の安全な状態にブートします。この際にセキュリティイベントが生成され、さまざまなセキュリティ監視ツール（SIEMツールなど）で監視することができます。KarambaのXGuard CFIは、プリンターファームウェアの実行フローを監視し、潜在的なゼロデイ攻撃の検知と防止に役立ちます。実行フローに何らかの変更があった場合、HPMemory Shieldはデバイスを停止し、安全な状態にリブートします。

インクカートリッジのセキュリティ

HPオフィスプリンターカートリッジチップは、セキュリティのために設計されています。HP純正カートリッジだけが、安全で改ざんされにくいように設計された、HP独自のファームウェアを搭載したチップを搭載しています。 HP以外のサプライ品には、信頼できないファームウェアを使用している可能性のある出所不明のチップが含まれています。

多くのオフィス用カートリッジのサプライチェーンを通したデジタル追跡が、再販業者とエンドユーザーにEnd to Endのサプライチェーン検証を提供します。HP純正カートリッジは、工場からプリンターの全行程を追跡し検証することが可能です。

独立したセキュリティの検証

HPは、Keypoint Intelligence-Buyers Lab (BLI) のSecurity Validation Testingプログラムの3つのレベルすべてを、多機能プリンター（MFP）と従来型プリンターの両方で完了した最初のプリントベンダーです。HPは、HP EnterpriseおよびManaged プリンターとMFP向けのHP FutureSmart v4+ Enterprise ファームウェアプラットフォームについて、デバイス侵入、ポリシーコンプライアンス（セキュリティ管理ソフトウェアを使用）、ファームウェアレジリエンスのテストに合格しシールを取得しました。

認証

HPのサービスおよびシステムは、実績のある業界標準の評価スキームの認証を得ています：

- ISO Information Security Management certifications: ISO/IEC 27001 and ISO/IEC 27701
- Supply Chain Security Certification ISO/IEC 20243
- Service Organization Control SOC 2 Type 2
- Secure Development Practices Assessment Certification (SD-PAC)
- Common Criteria Certification (CCC)
- Security Requirements for Cryptographic Modules (FIPS 140)

以下のリンクをクリックして、すべてのHP認証資格をご覧ください： HP certifications

4AA7-4216ENW, 2023年9月