ソリューション概要

HPのセキュリティとThin Client

企業のコンピューター環境は大変革を迎えています。職場の最新化に伴い、労働力と働き方が変わりつつあります。今や「在宅勤務」はカフェや空港のラウンジでも行われるようになりました。現在、従業員が自分のデスクで過ごす時間は1日のうちの55%にすぎません[1]。モバイルワーカーの増加によってデータや知的財産が失われる機会も増加しています。このことは収益と機会の喪失をもたらし、ひいては財務のひっ迫や規制違反による罰金につながるおそれがあります。そしてサイバー攻撃の頻度と巧妙さが増してきています。過去1年間にヘルスケア企業の81%がセキュリティ侵害を受け、平均で360万ドルのコストが発生しています[2]。事業継続性の維持、規制要件の遵守、セキュリティ インシデントへの対応は、現代の組織が直面するセキュリティ上の主な課題です。

HPはセキュリティ イノベーションを推進する業界のリーダーです

HPは信頼のおけるパートナーであり、お客様のデータと知的財産を保護する責任を自覚しています。HPの製品開発フレームワークの基礎となる指針は、すべての開発チームと、チームから市場に送り出されるプログラムでセキュリティ イノベーションが促進されるよう策定されています。当該分野の専門家から成るセキュリティに特化したコア チームがHPの各事業部門と意見を交換し合い、製品に最新のセキュリティ指針とベスト プラクティスが取り込まれるよう推進しています。

クラウドでアプリとデスクトップを仮想化することでセキュリティが強化されます

c06457082、2019年9月

現代の一元化されたクラウドコンピューティングモデルでは、データの処理および保存を行う場所はローカルクライアントからクラウドに移ります。これによって、ローカル クライアントを悩ませてきた従来の脅威からデータが隔離され、安全にホストされるようになります。Thin Clientはクラウドコンピューティングをサポートします。クラウドコンピューティングのエンドポイントは本質的に安全であり、インターネット、VDI、クラウドサービスに簡単に接続できます。ローカル クライアントはデータの処理および保存に必要最小限しか関与しません。

c06457082、2019年9月

HP Thin Clientは安全設計です

寒さから身を守るときと同様、セキュリティの効果を高めるにはとにかく層を重ねることです。敵が目標にたどり着くことを阻止するには階層ごとに防御壁を用意しておきます。セキュリティの専門家はこの方法を「多層防御」と呼んでいます。効果的なクラウド コンピューティング戦略の一部として、HP Thin Clientは幾重にも積み重なったハードウェアとソフトウェアの防御壁を築き、デバイス、データ、ユーザーのIDを保護します。

デバイス セキュリティで回復力、復元力、改竄防止を実現

HP Thin Clientは総合的に安全なマシンとなるよう設計されています。ハードウェアおよびソフトウェアのセキュリティ機能は以下のとおりです。

- セキュリティは安全で管理しやすいUEFI（BIOS）から始まります。すべてのモデルはUEFIセキュア ブートで起動し、ファームウェアはNIST SP800-147およびSP800-155ガイドラインに準拠しています。
- HP Mobile Thin ClientにはHP Sure Start[3]が搭載されています。これは業界をリードする技術の層で、NIST SP800-193ガイドラインを実装し、悪質な攻撃をUEFIで検出および阻止します。
- HPのポートフォリオには認定済みのTPM（Trusted Platform Module）が搭載され[9]、ハードウェアの層でID、資格情報、暗号化キーを保護します。
- AMDメモリー ガード[8]はコールド ブート攻撃の脅威を無力化する革新的な技術です。コールド ブート攻撃は揮発性のSDRAMモジュールを物理的に遮断し、再起動時にデータが消去される前に、保存されているデータにアクセスするというものです。
- 物理的な資産を盗み出そうとする昔ながらの脅威への対策が必要となることもあります。HP Thin Clientは業界標準のケーブル ロックと統合マウント ソリューション[10]をサポートし、物理的にデバイスを保護します。

データ セキュリティで一時データを保護し、データの漏洩や盗難を阻止

現代のクラウド コンピューティングはデータ セキュリティとユーザー アクセスのバランスの上に成り立っています。ユーザーは自ら進んで、または無意識のうちにセキュリティの脆弱性になり得ます。HP Thin Clientは何層にも重なった保護機能を備えているので、IT管理者と管理対象のユーザーは、ユーザー アクセスに必要なパスワード、セキュリティ トークン、USBアクセス ポートなどのツールを保護できます。

- HP ThinProオペレーティング システムは読み取り専用のロックされたファイル システムと暗号化されたレジストリを備えているので、ユーザーのデータが安全に保たれます。また、HP ThinProのOSには、構成可能なファイアウォールという形で統合された侵入防止システムも含まれていて、デバイス内外への通信を制御および監視できます。
- Windows 10 IoTオペレーティング システム搭載のHP Thin ClientではHP Write Managerを使用して不揮発性フラッシュ ストレージへのアクセスを制御します。データ処理は再起動のたびにデータが消去されるSDRAMで行われます。ユーザー セッションで生じた問題はその都度解決され、次回以降のセッションに持ち越されることはありません。
- USBポートと、USBポートに接続しているデバイスは、HP USB Port Manager[5]によって保護されます。IT管理者はカスタムなポリシーを作成して、この重要なアクセス ポイントに必要なデータ セキュリティの層を重ねることができます。
- ビジュアル ハッキングはリアルな脅威です。HP Sure View[6]テクノロジー搭載のHP Mobile Thin Clientをお選びください。HP Sure Viewはユーザーのみが使用できる範囲まで画面の視野角を狭めます。HP Sure Viewは製品に組み込まれていて、ボタンを押すだけでご利用いただけます。

IDセキュリティで適切な人物に適切なアクセスを

安全なエンドポイント エコシステムに不可欠な要素の1つがID保護です。認証および承認を通じて誰にどのリソースへのアクセス権が付与されているかを把握することは、デバイス、ユーザー、アプリケーションを適切に管理するうえでカギとなります。

- HP Thin Clientは認証された802.1xネットワークにシームレスに統合されます。また、Active Directory内でのマシン レベルのIDをサポートするので、IDを提供し、マシンを検出可能にして、エンドポイント管理機能を提供します。

- IT管理者は、何層にも重なった認証および身元確認機能を使用して、ユーザーの権限およびシステム リソースへのアクセス権、構成オプション、機密データを管理できます。これには指紋認証、顔認証、接触型および非接触型スマート カード、USBセキュリティ トークン、ワンタイムパスワード トークン、NFCが含まれます。[7]
- HP Thin Clientには業界標準のSSOソリューションのサポートも標準装備されています。[7]

管理ツールでデバイス管理の一元化および簡素化を促進

HPDM（HP Device Manager）は拡張性の高い一元化されたデバイス管理ツールです。ネットワーク経由で最新のセキュリティパッチや各種の更新が可能です。

HP Thin Clientは企業が直面するあらゆるセキュリティ上の課題に解決策を提供します

事業継続性を維持し、規制要件を遵守し、セキュリティ インシデントに対応するには、セキュリティがカギとなります。HP Thin Clientは、使い始めてすぐに保護機能が働くよう、セキュリティを製品設計および開発段階に不可欠な要素として構築された製品です。

詳細はこちらをご覧ください
https://jp.ext.hp.com/thin-clients/

1. 出典：Technalysis Research『Workplace of the Future: Progress, But Slowly』2017年2月
2. 『Analysis of 2018 Healthcare Data Breaches』、https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/（英語サイト）
3. HP SureStart Gen5およびBIOSphere Gen5の機能はPCプラットフォームおよび構成によって異なる場合があります。また、HP SureStart Gen5およびBIOSphere Gen5にはAMDの第8世代のプロセッサが必要です。
4. 2019年7月の時点で使用可能かつ販売中のデスクトップ シン クライアントのうち、AMDメモリー ガードによるデータ保護機能を搭載するモデルに基づきます。
5. Windows OS搭載のThin Clientでのみご利用いただけます。
6. HP Sure Viewプライバシー スクリーンはオプション機能です。ご購入時に構成に含めていただく必要があります。内蔵プライバシー スクリーンHP Sure Viewはオプション機能です。ご購入時に構成に含めていただく必要があります。また、横向き画面用の機能です。
7. 別売またはアドオン機能として提供されるオプション機能です。
8. HP t640およびt740 Thin Clientでのみご利用いただけます。
9. HP t240 Thin Clientには搭載されていません。
10. マウント ハードウェアは別売です。

c06457082、2019年9月