



HP THIN CLIENTS

クラウドコンピューティングのための セキュリティソリューション

職場の最新化とモバイルワーカーの増加に伴い、企業のコンピューター環境は大変革を迎えています。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年間にセキュリティ侵害を受けた企業の割合。平均で360万ドルのコストが発生しています。¹

クラウドでアプリとデスクトップを仮想化して セキュリティを強化

デバイス、データ、IDの保護において、HP Thin Clientは最高レベルのセキュリティを必要とする組織にとって理想的な選択です。

デバイスセキュリティ

UEFIセキュアブートによる起動	内蔵TPMチップ	AMDメモリーガード	物理的なセキュリティ保護
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 S8000-147およびSP800-155ガイドラインに準拠しています。	ハードウェアで保護された非常にセキュアな保管場所です。ID、資格情報、暗号化キーの保護層です。	システムメモリをリアルタイムで暗号化/復号化してコールドブート攻撃から保護します。システムのパフォーマンスにはほとんど影響しません。	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 ² をサポート。物理的にデバイスを保護します。



データセキュリティ

HP ThinProでの多層型セキュリティ対策	HP Write Manager ³	HP USB Port Manager ³	モバイル用HP Sure View ⁴
読み取り専用およびロックされたファイルシステム、暗号化されたレジストリ、Linux OS、ファイアウォールのサポートによってセキュリティ層が厚くなります。	Thin Clientのローカルにデータが保存されることがないように、書き込みをオーバーレイにリダイレクトします。オーバーレイ上のデータは再起動時に消去されます。	重要なアクセスポイントに必要なデータセキュリティ層として、IT管理者はカスタムなポリシーを作成してポートを保護できます。	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、HP Mobile Thin Clientのビジュアルハッキングを防止します。



IDセキュリティ

Active Directory統合	多要素認証	柔軟なシングルサインオン	認証されたネットワークへの統合
Active Directory内でのマシンレベルのIDをサポートし、ID、探索機能、エンドポイント管理機能を提供します。	指紋認証システム、接触型および非接触型スマートカードリーダーなど ⁵ をサポートするデバイスで、多要素認証を義務付けることができます。	業界標準のSSOソリューションのサポートによってシンクライアントにすばやくログオンでき、共有する作業領域での生産性が向上します。 ⁵	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。



詳しくは、<http://jp.ext.hp.com/thin-clients/> をご覧ください

1. 出典：Technalysis Research 『Workplace of the Future: Progress, But Slowly』 2017年2月。
 2. マウントハードウェアは別売です。
 3. Windows OS搭載のThin Clientでのみご利用いただけます。
 4. 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。
 5. 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。

