ネットワークを保護

HPの高い安全性を確保する大判プリント

ファイアウォールだけではハッカーからの攻撃に耐えることはできません。デバイス、データ、ドキュメント、ネットワークを保護するには、HPの優れた保護機能が必要です。

目次

プリンターの
セキュリティ上の脅威

見えないリスクを認識する

多くのIT部門は個々のコンピューターに対して厳しいセキュリティ対策を講じていますが、プリンターやスキャナーはセキュリティ対策の対象から外れ、無防備な状態になっていることが少なくありません。セキュリティ対策が講じられていないデバイスが存在する場合、ネットワーク全体がサイバーセキュリティ攻撃にさらされる可能性があります。

潜在的なコストを把握する

プリンターやスキャナーのセキュリティが原因で機密情報や個人情報が危険にさらされている場合、個人情報窃盗、ビジネス情報の盗難、ブランドイメージの低下、訴訟、業務の停滞などのさまざまな問題を引き起こす可能性があります。また、法規制に適合していないために、多額の罰金が課されることもあります。

HPのソリューション

HPの大判プリンターに内蔵されたセキュリティ機能により、お客様のネットワークを保護します。HPでは、デバイス、データ、ドキュメント、ネットワークの保護の自動化に役立つ幅広いソリューションを提供しています。

デバイス、データ、ドキュメント、ネットワークの保護

ネットワークに接続したプリンター環境下では、重大なセキュリティギャップとなるポイントがいくつか存在します。これらの脆弱性を理解しておくと、リスク対策を簡単に行うことができます。

ネットワークに接続したプリンター環境下の脆弱性ポイント

デバイスに対する脅威

コントロールパネル
ユーザーによってデバイスの設定や機能が悪用される可能性があります。

デフォルトパスワード
プリンターは、シンプルなデフォルトパスワードが設定された状態で工場から出荷されます。このようなパスワードは簡単に突破される可能性があります。

BIOSとファームウェア
ファームウェアが侵害されると、デバイスやネットワークが攻撃を受ける可能性があります。

データに対する脅威

保管中のデータ
プリンターに保管された重要な機密情報ががリスクにさらされる可能性があります。

スキャンデータ
セキュリティ対策が講じられていない多機能プリンターでは、スキャンデータをどこにでも送信できてしまいます。

送信中のデータ
デバイス間での送信中にデータが盗まれる可能性があります。

ドキュメントに対する脅威

排紙トレイ
排紙トレイに放置されたままの文章・資料は取違や持ち去られる危険があります。

ポートとプロトコル
セキュリティ保護されていないポート（USBまたはネットワーク）やプロトコル（FTPまたはTelnet）によってデバイスを危険にさらします。

管理
検出されないセキュリティギャップによりデータが危険にさらされます。

デバイスの保護

HP Secure Boot

BIOSは、起動時に重要なハードウェアコンポーネントをロードし、ファームウェアを起動するのに使用される一連の指示です。BIOSを書き換えたりマルウェアなどを仕込んだ形跡があれば起動を中止します。正しいオリジナルのBIOS使用時のみ起動可能です。

Whitelisting

予めHPが承認しているソフトウェアのリストを照合しプリントを実行します。HPの電子署名されたソフトウェアのみプリンター上で動作可能です。

HP Connection Inspector

HP Connection Inspectorにより、ネットワーク接続をチェックして、疑わしいリクエストやマルウェアによる妨害を防止します。プリンターがセキュリティ被害を受けた場合は、自動的にシステムの再起動が行われます。

HP Trusted Platform Module（ TPM ）

セキュリティチップ（ TPM ）搭載で耐タンパー性を強化し、プリンター内蔵のHDDは自己暗号化されたデータを保存します。

デバイスの保護

固有の管理者パスワード

すべてのプリンターに固有の管理者パスワードがデフォルトで設定されているため、セットアップを行わなくてもプリンターは常にパスワードで保護された状態になっています。

LDAP/Kerberosユーザー認証

これらのプロトコルを使うと、企業のディレクトリを使ってプリンターユーザーを認証し、許可されたオプションや情報以外にユーザーがアクセスできないようにすることができます。

HPスマートカードソリューション

プリンターでユーザーに2要素認証を要求することで、機密情報を保護し、プリンターへのアクセスを制御できます。

Role Based Access Control（ RBAC ）

プリンターの設定に関わる機能にアクセスできるアカウントを制限します。企業はユーザーレベルに合わせた異なるアクセス制限を実行可能です。
3つのアクセスレベル:Admin/Guest/User

セキュリティイベントログ

より詳細に可視化することで、悪意のあるセキュリティ上の脅威をすばやく検知できます。セキュリティログでは、各オブジェクトで設定された監査ポリシーの条件に従って各イベントを記録します。

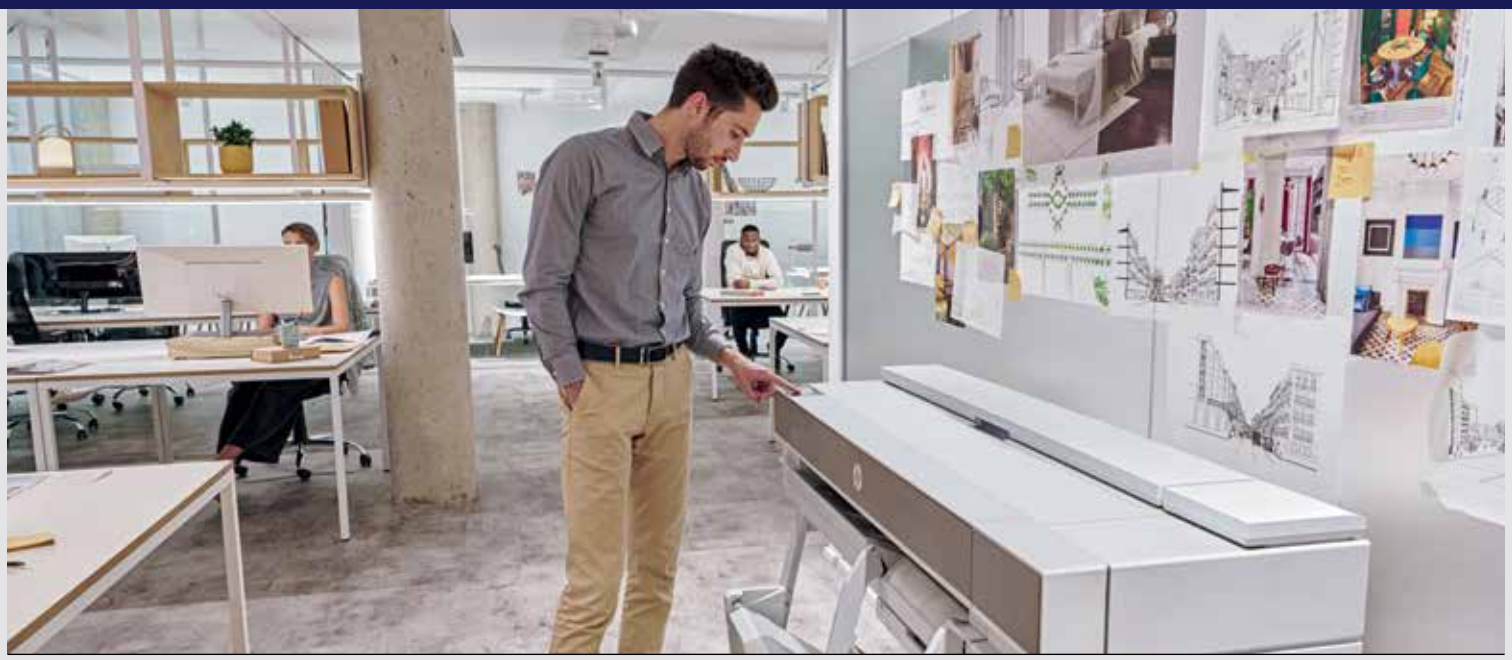
ランタイム侵入検知

ランタイム侵入検知では、カーネルメモリを継続的に監視し、破損や不正変更を検知します。検知されると、デバイスを再起動して良好な状態に戻すことでデバイスの自己修復が行われます。

HP Sure Start

HP Sure Startは、包括的なファームウェア/ソフトウェア設定を備えた高度なハードウェア強化型ソリューションで、BIOSのデジタル署名の検証を行います。

データの保護



保存時

ハードディスクの自己暗号化

内蔵された自己暗号化機能により、ハードドライブに保存された重要なビジネス情報を保護します。

セキュアなファイル消去

ハードディスクからファイルが削除された後に、プリンター内にデータは一切残りません。

セキュアなディスク消去

プリンターのハードディスクの情報はすべて消去され、重要なデータを復元することはできなくなります。

送信時

暗号化通信

標準的な暗号化プロトコル（802.1xまたはIPSec）でネットワーク暗号化規格を使用し、ドライバーまたは送信者からのプリント時にネットワーク上で送信されたデータを保護します。

ドキュメントの保護

プルプリント

プルプリントは、重要な情報を保護し、誰が出力したか分からないプリントジョブを減らすため、エンドツーエンドの追跡やレポートを可能にする機能です。この機能は、生産性を高め、放置されたドキュメントが意図しない人の手に渡らないようにするのに役立ちます。HP大判プリンターは、サードパーティのプルプリントソリューションにも対応しています。

暗号化されたPINプリント

PIN コードを指定したプリントが可能です。PIN コードを入力するまでプリントを待機するため、出力物の取り違えを防ぐことができます。

ネットワークの保護

セキュリティ監視/管理ソリューションにより、脆弱性を見つけ出し、データの保護、リスクの軽減、コンプライアンスの維持を実現する一元化されたポリシーベースのアプローチができます。セキュリティギャップをなくし、リスクを回避できます。

デバイスとネットワークを保護

HP Security Manager[2]を使うと、フリート全体でのセキュリティポリシーの設定、デバイス設定の修復の自動化、固有の証明書のインストールと更新を行うために必要なコストとリソースを削減できます。HP Security Manager[2]に含まれるインスタントオンセキュリティ機能では、ネットワークにデバイスを追加したときや再起動を行ったときに、新しいデバイスが自動的に設定されます。

HP Command Center（HPCC）は、オンボードされたデバイス用のセキュリティポリシーをIT管理者が作成できるクラウドソリューションです。HPCCを使うと、デバイスのセキュリティ設定を評価し、必要に応じて、あらかじめ定められた企業のセキュリティポリシーに合わせてデバイスのセキュリティ設定を修正できます。

プリントフリートセキュリティのコンプライアンス監査レポート

オンプレミスのHP Security Manager[2]とクラウドのHPCCを使用して、コンプライアンス証明レポートを作成し、プリンターへのセキュリティポリシーの適用状況と顧客データの保護状況を示すことができます。

ビジネスに悪影響をもたらす不適合デバイス

保護されていないエンドポイントがあると、サイバー犯罪の被害を受ける可能性が高まります。増大する脅威に対抗するため、世界各国の政府機関は、組織に顧客情報の保護の強化を求める厳格なセキュリティ規制を実施しています。コンプライアンス要件に対応し、セキュリティ上の脅威からビジネス情報を保護するには、HP DesignJetプリンターやHP Security Manager[2]などのデバイスやソリューションを導入することが重要です。

シンプルで卓越したセキュリティ保護機能

HP Wolf Security[3, 4]が、HP DesignJet大判プリンターで利用できるようになりました。

HP Wolf Securityは、プリントビジネスが将来の脆弱性とリスクに対処できるようにするため、ハードウェアレベルだけでなくソフトウェア全体をカバーする形で、統合型のエンドポイント保護と回復機能を提供します。

これは、ゼロトラストの原則に基づいて開発されたエンドポイントセキュリティ[3]で、常に最新の脅威に対処できるように進化を続けています。

セキュリティポスチャの強化を簡単に

HP Wolf Securityでは、卓越したセキュリティ保護だけでなく、システムによる自己防御と自己修復を行うことができます。セキュリティカバレッジを損なうことなく、システムを簡単に展開して管理できます。

HP WOLF SECURITY

ビジネスの成長を攻撃から守る

検知
ユーザーが問題に気付く前に、問題や脅威を自動的に検知できます。

保護
常に最新のサイバー脅威に対処できる強力なセキュリティでビジネスとビジネスの成長を守ります。

修復
多忙なITチームに負担をかけることなく、攻撃から自動的に回復できます。

3つの異なる保護レベル

HP Wolf Security対応のHP DesignJetプリンターには、さまざまなレベルのセキュリティ機能があらかじめ搭載されています。HP Wolf Security対応のプリンターを購入すると、お客様のニーズに適したセキュリティレベルを確保できます。

HP Wolf Essential Security
ハードウェアで強化されたセキュリティ保護基盤を提供します。

HP Wolf Pro Security
サイバー脅威に対するプロアクティブな保護を通じてビジネスを保護します。

HP Wolf Enterprise Security
常に進化を続けるセキュリティ上の脅威に対処し、同時にハイブリッドワークをサポートします。

自己修復機能の仕組み

HP Security Managerは、4ステップのセキュリティチェックサイクルを実行してデバイスのセキュリティを維持します。

動作コード（BIOS）のチェック
HP Secure Boot

HPによる署名付きの正規のコードのみがロードされるようにすることで、起動時に悪意のあるコードが実行されるのを防ぎます。

ファームウェアのチェック
Whitelisting

HPによるデジタル署名付きの正規のファームウェアのみがロードされるようにします。

プリンター設定のチェック
HP Security Manager[2]

再起動時に、影響のあるデバイスのセキュリティ設定を検査して修正します。

継続的な監視
HP Connection Inspector

ネットワークのアウトバウンド接続を継続的に監視し、マルウェアの侵入を防ぎ、悪意のあるリクエストやマルウェアによる妨害を自動的に阻止します。

保護、検知、修復機能を備えたプリンター

HP大判プリンター

HP大判プリンターは、リスクを軽減し、コンプライアンスを強化し、ネットワークを保護できるように設計されており、内蔵された機能とアドオンソリューションを利用して、サイバー攻撃からプリンターを守ります。

HP DesignJet T850/T950

プリンターシリーズ

世界で最もA3からA1のプリントが簡単なプリンターで、多様な業務にスピーディーに対応できます。[5]

本製品の詳細はこちら：

HP DesignJet T850/T950プリンターシリーズ

HP DesignJet XL 3800

MFP

HP Wolf Enterpriseを装備した世界で最も安全な大判プリンター[6]で、ネットワークとデータを高度なセキュリティ機能で保護します。

本製品の詳細はこちら：

HP DesignJet XL 3800 MFP

HPプリンターポートフォリオ

		HP DesignJet T850/T950プリンターシリーズ	HP DesignJet XL 3800多機能プリンター
デバイス	HP Secure Boot	✓	✓
	HP Connection Inspector		✓
	Whitelisting	✓	✓
	固有の管理者パスワード	✓	✓
	TPM		✓
	ランタイム侵入検知		✓
	Sure Start		✓
	LDAP/Kerberosユーザー認証		✓
	Role Based Access Control（RBAC）		✓
	フロントパネルアクセスロック		✓
データ	セキュリティイベントログ	✓	✓
	SNMP v3互換性	✓	✓
	自己暗号化HDD		✓
	着脱式HDD		✓
	HDDなし	✓	
	IPSec互換性		✓
	TLS/SSL（g）	✓	✓
ドキュメント	セキュアなファイル消去		✓
	セキュアなディスク消去	✓(α)	✓
	802.1x互換性	✓	✓
	NTLM v2	✓	✓
	暗号化されたPINプリント		✓
	IPv4αおよびIPv6互換性	✓	✓
	CA/JD証明書	✓	✓
	ネットワークポートとプロトコルの無効化	✓	✓
フリートセキュリティ管理	HPスマートカードソリューション[1]		✓
	PINプリント	✓	✓
	HP Web JetAdmin	✓	✓
	HP Security Manager/HP Command Center	✓	✓
	SIEM統合	✓	✓

（α）セキュアなジョブ送信消去：T950

補足情報および免責事項

1. 米国政府向けNIPRNetソリューションおよび米国政府向けSIPRNetソリューションをサポートしています。

2. HP Security Managerは別途購入が必要です。詳細については、hp.com/go/securitymanagerをご覧ください

3. HP Securityは、HP Wolf Securityに名称変更しました。セキュリティ機能はプラットフォームごとに異なりますので、詳細は製品データシートをご覧ください。

4. すべてのHP DesignJetプリンターに搭載されているセキュリティレベルはさまざまです。HP Wolf Securityを搭載していると記載できるのは一部のプリンターのみです。これには、HP DesignJet XL 3800多機能プリンター、HP DesignJet T850プリンター/T850多機能プリンター、HP DesignJet T950プリンター/T950多機能プリンターが含まれます。HP Wolf Securityは、今後のHP DesignJet製品の標準機能となる予定です。

5. HP ClickとHP DesignJet T850を使用したテスト結果に基づきます。このソリューションは、主要な競合他社のプリントソリューションよりも少ない手順でプリントできます。A1とA3が混在する5ページをプリントする場合、HP Clickを使用すると3ステップで完了できるのに対し、競合A社では12ステップ、競合B社では8ステップが必要です。このテストはSogeti社により2023年4月に実施されました。詳細なテストレポートについてはお問い合わせください。

6. HPの依頼のもと、2023年2月にSogeti社が実施した、公表されているセキュリティ仕様の比較に基づきます。HP DesignJet XL 3800のセキュリティ機能と、2023年2月時点の全世界のTDP少量プリント市場シェアの大半を占めるさまざまなメーカーの競合製品を比較しています。詳細情報が必要な場合はご請求ください。

4AA8-3169JAP、2023年11月