



# プリント環境の保護： サイバーレジリエンスに向けた プロアクティブなライフサイクルアプローチ

プリントセキュリティ：長期にわたり影響を及ぼす調達時の意思決定



プリンターは数年単位での更新を前提とした長期的な投資対象でありながら、セキュリティは後回しにされがちです。しかし、印刷分野の適切なパートナーを選定することで、コスト効率、信頼性、パフォーマンスの向上に加え、サイバーレジリエンスの強化にもつながります。

プリンターはしばしば「無害な機器」と見なされがちですが、実際にはPCと同様にハードドライブや通信機能を備えた高度なネットワーク接続型デバイスです。しかし、通常サイバー脅威対策のためにエンドポイントセキュリティのレイヤーが組み込まれているPCとは異なり、多くのプリンターのエンドポイント保護は限定的なものであり、まったく対策されていない場合もあります。そのため、企業が脅威を検知して迅速に対応することが困難になっています。

企業のセキュリティ戦略においては、プリンターのハードウェアとファームウェアにより提供されるセキュリティ、すなわち「プリンタープラットフォームのセキュリティ」が見過ごされがちです。

プリント環境の保護にライフサイクル全体で取り組むことは、長期的な企業レジリエンス確保につながります。あらゆる段階において適切なセキュリティ対策を講じることで、組織の防御力を強化し、プリントインフラストラクチャを信頼できるITエコシステムの一部として維持することができます。本レポートでは、強固なプラットフォームセキュリティを実現するための主な課題と有効な戦略について詳しく解説しています。

「プリンタープラットフォームのセキュリティを基盤から組み込み、プロアクティブに管理することで、データの窃取、プリントジョブの妨害、ランサムウェア、ゼロデイ攻撃、中間者攻撃などのリスクを軽減できます」

# サプライヤーの選択とオンボーディング：工場で製造からユーザーの手元に届くまで、プリント環境を保護



プリンターのライフサイクルは工場から始まりますが、調達プロセスにおいてサプライチェーンのセキュリティは後回しにされがちです。初期段階からプリンターのセキュリティ要件を組み込むことで、将来的な攻撃への耐性を高めることができます。しかし、プリンターの調達時に、調達、セキュリティ、ITの各部門が連携してセキュリティ基準を策定していると回答したITおよびセキュリティの意思決定者（ITSDM）は、わずか38%にとどまっています。さらに60%が、このような連携不足が組織にリスクをもたらしていると危惧しています。

## 38%

プリンター購入の際に、調達、セキュリティ、ITの各部門が連携してセキュリティ基準を策定していると回答したITおよびセキュリティの意思決定者（ITSDM）は、38%にとどまっています。

## 60%

さらに60%が、このような連携不足が組織を危険にさらすと危惧しています。

IT部門とセキュリティ部門は、本来調達における重要なステークホルダーであるにもかかわらず、多くの場合、ベンダーのセキュリティ対策を評価する機会から外されています。プリンターの提案依頼書を評価するプロセスにおいて、多くの組織が以下の重要な対応を実施していない実態が明らかになっています。

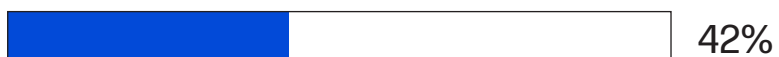
ベンダー宛のセキュリティ関連の質問事項をIT部門およびセキュリティ部門に提出し、事前にレビューを受けていない



ベンダーのセキュリティ対策を検証するために、ベンダーに技術情報の提出を求めている



ベンダーに対し、IT部門とセキュリティ部門への回答提出を要求していない





また、プリンターが納品された時点で完全性を確認することが難しいという課題もあります。工場内や輸送中にプリンターへの改ざんの有無を確認できないと回答したITSDMは過半数（51%）にのぼります。ITSDMは平均して4年間にわたりこれらのデバイスの監視を行うことから、導入初日からプラットフォームセキュリティを統合することで、長期的な信頼性、効率性、レジリエンスを確保することができます。

サプライヤー選択およびオンボーディングに関する推奨事項：

- IT、セキュリティ、調達各部門がしっかりと連携し、新規導入するプリンターのセキュリティおよびレジリエンス要件を明確に定義する。
- ベンダーに対して技術的な説明や資料を要求し、それらの主張の妥当性を検証する。
- 製造元/プロバイダーに、製品およびサプライチェーンプロセスに関するセキュリティ認証の提出を要求し、それらを活用する。

継続的な管理：

プラットフォームセキュリティの可視性を常に維持する



プリンターの導入後は、IT部門およびセキュリティ部門がセキュリティ設定を積極的に管理することで、組織のレジリエンスを強化できます。このような取り組みは、業界規格やサイバーセキュリティに関する規制に準拠するためにも不可欠です。ファームウェアの完全性をプリンターのセキュリティの中核に据えることで、自動的な自己修復リカバリ機能を備えた継続的な監視が可能となり、デバイスのライフサイクル全体にわたって最適な保護とパフォーマンスを維持できます。これにより、ITおよびセキュリティ部門の負担を大幅に軽減できます。

プリントセキュリティにおいてIT部門が直面する最大の課題の1つが、ファームウェアを最新の状態に保つことです。

36%

実際に、プリンターのファームウェアを速やかに更新しているITSDMは、わずか36%にとどまっています。

パッチが適用されていないプリンターは、組織全体の攻撃サーフェス（攻撃対象領域）を拡大し、ソフトウェアベースのセキュリティ対策を回避する低レベルの攻撃にさらされるリスクを高めます。その他の課題としては以下のようなものがあります。



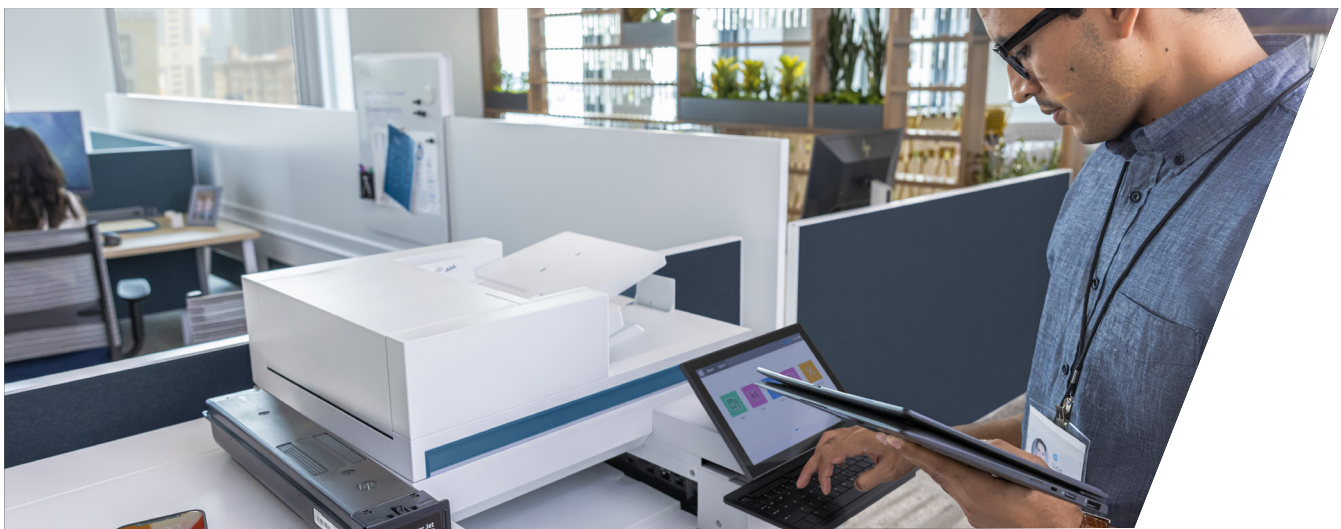
- 設定変更やテクニカルサポートを安全に実施できるよう、ファームウェア管理用のパスワードを適切に管理する。
- 物理的コンポーネントの変更を制御することで、ハードウェアの完全性を維持する。
- 適切なファームウェアのセキュリティ設定を定義し、それを常に最新の状態に保つ。

加えて、リモート管理ツールの不足により、IT管理者によるプリンターのセキュリティの管理がより困難かつ時間を要する作業になっています。実際、IT管理者はハードウェアやファームウェアのセキュリティ管理に、プリンター1台あたり毎月3.5時間を費やしています。

継続的な管理に関する推奨事項：

- セキュリティ上のリスクを最小限に抑えるために、ファームウェアの更新を速やかに適用する。
- セキュリティツールを活用して、プリンターのポリシーベースの設定への準拠状況を効率的に管理する。
- SIEM（Security Information and Event Management）ツールを利用して、プリンターから生成されたイベントメッセージを監視する。このようにセキュリティイベントを継続的に監視し、文書化することで、業界の規制や標準への準拠が促進される。

## 修復：プリンター機器間のセキュリティ上の脆弱性を解消

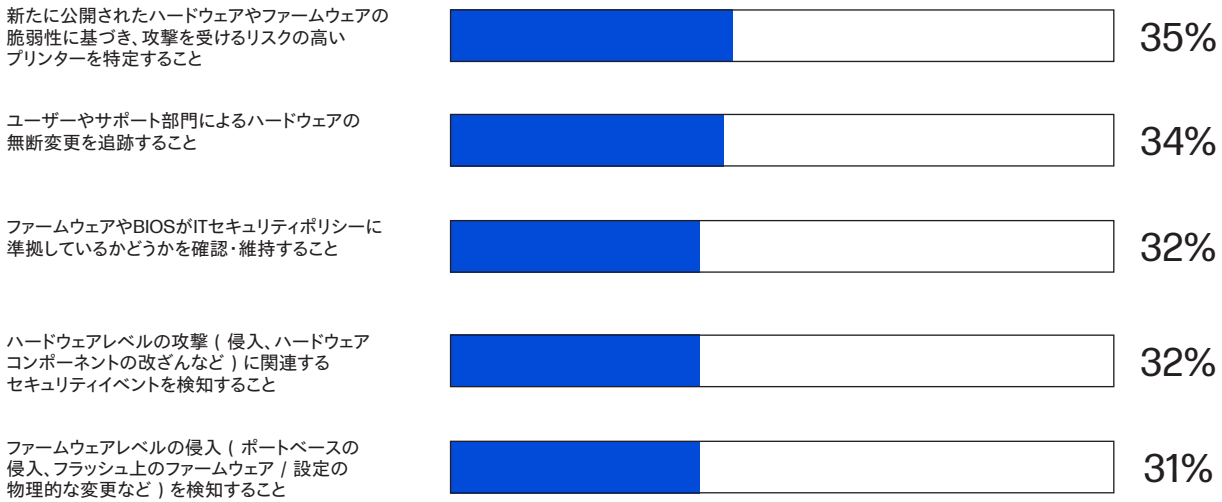


IT部門およびセキュリティ部門は、プリンターのハードウェアやファームウェアに対する潜在的な脅威を監視、対処することで、防御体制をさらに強化できます。プリントデバイスをプロアクティブに保護することで、不正アクセスを防止し、機密性の高いシステムや重要なデータを保護できます。

サイバー犯罪者は常に、組織のITインフラストラクチャに潜む脆弱性を狙っています。そのため、プリンターを含むすべての資産が保護されていることが極めて重要です。



すなわち、プリンターのハードウェアやファームウェアに対する低レベルの脅威を検知・修復することで、攻撃者に悪用される「弱点」とならないようにすることが求められます。しかし、IT部門およびセキュリティ部門は、以下のような課題に直面していると回答しています。



# 70%

サイバー脅威にとどまらず、ITSDMの70%が、人による機密企業情報の印刷や持ち出しといったオフラインの脅威に対しても懸念を強めています。

### 修復に関する推奨事項：

- ゼロデイ脅威やマルウェアを継続的に監視し、低レベルの攻撃を防止、検知、隔離し、被害を復旧するための機能を備えたプリンターを導入する。
- SIEMツールを利用してデバイス監査ログを監視することで、ファームウェアの変更を追跡し、不正な変更の検知や悪用の兆候を特定する。
- 不正アクセス、ドキュメントの盗み出し、データの流出といった脅威から機密情報を保護するために、安全な暗号化印刷とデータ損失防止（DLP）に対応したデバイスを選択する。

「プリンターをはじめとするIoT機器は、高性能なコンピューティングデバイスであり、攻撃者にとって企業のインフラストラクチャに侵入する足がかりとなる恰好の標的です。そのため、組織は新しいデバイスの調達時に成熟したセキュリティ要件を策定し、ライフサイクル全体にわたってそのセキュリティ設定をプロアクティブに管理することが必要です」

# 廃棄：プリンターの再利用を妨げる データセキュリティの課題を克服



プリンターを安全に廃棄することは、たとえ再利用、再導入、売却、リサイクルのいずれを選択したとしても、プリント環境のライフサイクルの重要な最終ステップとなります。ITSDMの報告によると、組織内には不要もしくは廃棄段階にあるプリンターが平均して約80台存在しており、これはセキュリティ対策と持続可能性の強化に向けた好機でもあることを示しています。

ITSDMは、プリンターの使用終了時に組織で以下の対応を実施していると回答しています。

**60%**

リサイクルする

**19%**

データを消去した上で寄付する

**17%**

データを消去した上で、社内で再配備する

**13%**

デバイスを破壊する

**13%**

売却する

しかし、データセキュリティへの懸念が大きな障壁となり、多くの組織が再利用可能なデバイスの活用に踏み切れていないのが現状です。ITSDMの86%が、プリンターの再利用、再販、リサイクルを妨げる要因としてデータセキュリティをあげており、そのうち39%がこれを「重大な」もしくは「深刻な」懸念と捉えていることがわかりました。

また、現在のサニタイズ（データ抹消処理）ソリューションに対する信頼も不十分で、35%のITSDMが、プリンター内のデータを完全かつ安全に消去できるか確信が得られないと答えています。その一方で、ITSDMの4人に1人がプリンターのストレージドライブを物理的に破壊する必要があると考えています。また、10人に1人は、データセキュリティの確保のためには、デバイス本体とストレージドライブの両方を破壊すべきだと主張しています。

### 使用終了・廃棄に関する推奨事項：

- 安全な再利用とリサイクルを実現するために、ハードウェアおよびファームウェアデータの安全な消去機能を備えたプリンターを選択する。
- 個人情報を保護し、データ漏えいを防止するために、暗号化されたストレージを使用し、廃棄時にハードディスクドライブへの複数回の上書きやソリッドステートドライブの暗号消去に対応したデバイスを導入する。

### プリントセキュリティの管理：ライフサイクル管理によるレジリエンスの強化

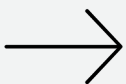
適切なアプローチとツールを選択することで、プリント環境をシームレスに保護することが可能になります。ライフサイクルを軸とした戦略により、IT部門とセキュリティ部門が導入から廃棄までの各段階で管理体制を確立できます。つまり、調達時に確固たるセキュリティ要求を設定し、運用中は可視性と制御性を維持し、使用終了時には安全かつ確実な廃棄を行うなど、ライフサイクルの初期段階から強固なセキュリティを組み込むことが求められます。

調達、IT、セキュリティの各部門が連携することで、コスト効率と業務効率に優れるだけでなく、進化する脅威に対しても高い耐性を備えたプリンターを導入することができます。管理ツールの統合や、工場出荷時点でのセキュリティプロビジョニングの強化により、管理業務が効率化されるほか、高度な監視機能により、リアルタイムでの脅威検知、対応が可能になり、被害の拡大を未然に防ぐことができます。

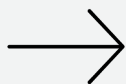
プリンターを単なるセキュリティリスクとしてみなすのではなく、デジタル資産の一部として適切に管理すべき要素と捉えることで、組織は長期的な価値、業務効率、安心感を得ることができます。これからのプリントセキュリティは、プロアクティブかつ協調的で、ライフサイクルに重点を置いたものでなければなりません。その第一歩を、今ここから始めましょう。



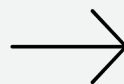
サプライヤーの選択と  
オンボーディング



継続的な管理



修復



廃棄と再利用

