デバイスライフサイクルの保護：工場からユーザーの手元、将来の再デプロイまで

ライフサイクルを通したデバイスセキュリティへのアプローチが、デバイスのサイバーリスク緩和、コスト削減、効率向上を実現する

サプライヤーの選定

オンボーディングと設定

継続的な管理

監視と修復

再利用と廃棄

目次

エグゼクティブサマリー

PCあるいはプリンターを購入することは、長期的なコミットメントをすることです。こうした機器類は企業で長年使用され、今や多くの企業が環境、社会、ガバナンス（ESG）の目標達成のために耐用年数をさらに伸ばすことを検討しています。そのため、調達チームにとっては適切なデバイスの選択は重要かつ、しばしば困難な作業です。十分な情報を基に判断するためには、さまざまな要素を考慮する必要があります。コスト、性能、信頼性、レジリエンスのすべてのバランスを慎重に検討しなければなりません。

しかし、コスト削減などの短期的な利益を追求すると、デバイスのライフサイクルが進むにつれて、総所有コスト（TCO）やリソース消費量、リスクの増大など、会社にしっぺ返しが来ることも多くなります。ITインフラストラクチャにサイバー脅威に対するレジリエンスが求められることを考えれば、PCやプリンターなどのハードウェアやファームウェアのセキュリティ、つまりプラットフォームセキュリティが必要不可欠であるにもかかわらず、見過ごされがちです。

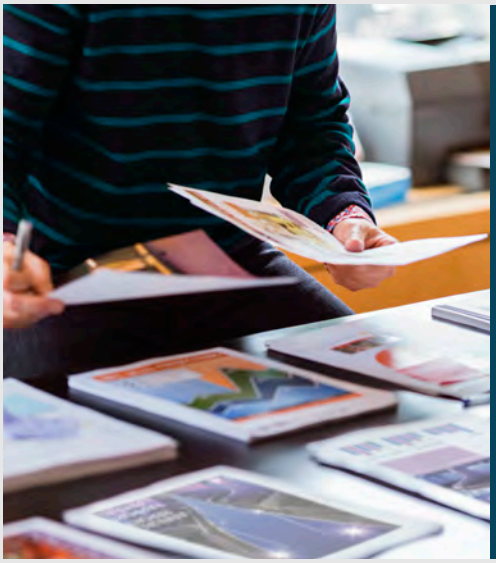
その理由の1つとして、ベンダーのプラットフォームのセキュリティに関する宣伝文句を評価することが難しいことが挙げられます。しかし、選択を誤ると広範囲に影響を及ぼし、その先何年も組織のセキュリティ体制を弱体化させることになりかねません。このレポートでは、ITおよびセキュリティの意思決定者（ITSDM）が直面するプラットフォームセキュリティの課題に焦点を当て、デバイスのライフサイクルの5つの段階ごとに、強力なプラットフォームセキュリティを実現するための方法を提案しています。

米国、カナダ、英国、日本、ドイツ、フランスで、従業員1,000人以上の企業のITおよびセキュリティの意思決定者（ITSDM）803人、および場所にとらわれない働き方を行う従業員6,055人のを対象に調査を行った結果、以下のことがわかりました。

- 下層レベルへの攻撃の脅威が増加：回答者の 81% がハードウェアやファームウェアのセキュリティを優先事項にすべきと答えており、35% が自社もしくは他社において、サプライチェーンを狙って悪意のあるハードウェアやファームウェアをデバイスに侵入させようとする国家の脅威アクターの影響を受けていることを知っていると回答しています。
- 依然としてデバイスの調達の際にセキュリティが見落とされがち：回答者の60%が、デバイスの調達にセキュリティが考慮されていないことが自社のリスクを高めていることを認めており、48%が、調達チームはまるで「子羊のように従順」にベンダーの言うことを鵜呑みにすると回答しています。
- 時間のかかる手作業がミスを招く：62%が、ハードウェアやファームウェアレベルで誤った設定のデバイスによる時限爆弾に直面していると回答し、57%がファームウェアに関してFOMU（アップデートに対する不安）に悩まされています。
- ツールや知識の欠如がチームに敗北感を与えている：79%がハードウェアやファームウェアのセキュリティについて理解を深める必要があると回答している一方、60%はハードウェアやファームウェアによる攻撃を検知し緩和することは「不可能」だとして、敗北を受け入れています。
- デバイスを安全に廃棄できないことはESGの取り組みに悪影響を及ぼす：回答者の 68% が、電子廃棄物を削減することでより広範なESG 目標の達成が容易になるとする一方で、59% が、データセキュリティ上の懸念から、デバイスの再利用は困難だと回答しています。

調査結果は、デバイスのライフサイクルのあらゆる段階でエンドツーエンドのプラットフォームセキュリティを管理するためには、包括的なアプローチが必要であることが明確に示されました。これによってリスク緩和、コスト削減、効率向上、生産性改善を実現し、同時にユーザーやITチームのエクスペリエンスも向上します。

ITリーダーはデバイスのライフサイクルの各段階で、こうしたセキュリティギャップに対処することで、プラットフォームのセキュリティ体制を成熟させていくことができます：

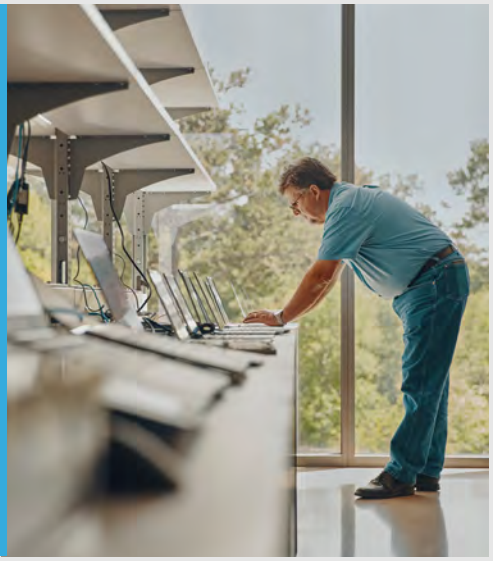


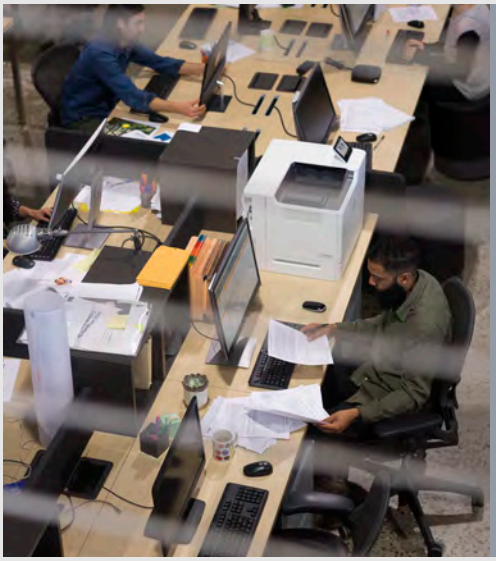
サプライヤーの選定

まず、調達、IT、セキュリティの各部門が連携した取り組みとして、デバイスのセキュリティ要件の定義、ベンダーの回答の検証、サプライヤーの監査を見直すことから始めましょう。今回の調査では、デバイス調達時の共通課題として、ステークホルダー間のコミュニケーション不足が浮き彫りになりました。緊密に連携することで、組織としてエンドポイント要件を見落とすリスクを削減し、セキュリティを強化してITにおける摩擦を低減します。セキュリティ要件を定義する際には、例えばデバイスの安全な廃棄まで考慮するなど、あらゆる状況を網羅した要件になるよう、ライフサイクルを念頭に置いて社内のすべてのデバイスを確認するよう、チームに働きかけてください。

オンボーディングと設定

多くのITリーダーは、工場からデバイスを受け取るまでのサイバー脅威はわからないと言っています。しかし、輸送中のデバイスの改ざんのような攻撃を検知し、緩和するためのソリューションは存在します。ハードウェアとファームウェアの安全な設定を制御するベンダーのファクトリーサービスと合わせて、こうしたライフサイクルの初期段階でデバイスを保護するための機能も評価することをお勧めします。納入後については、デバイスとユーザーの安全なゼロタッチオンボーディングと、レガシーなBIOSパスワードに依存しない安全なファームウェア設定管理を可能にするソリューションについてチェックします。これらの機能を組み合わせることで、ハードウェアとファームウェアのリスクを低減しながら、オンボーディングをよりシームレスかつ安全に行うことができます。



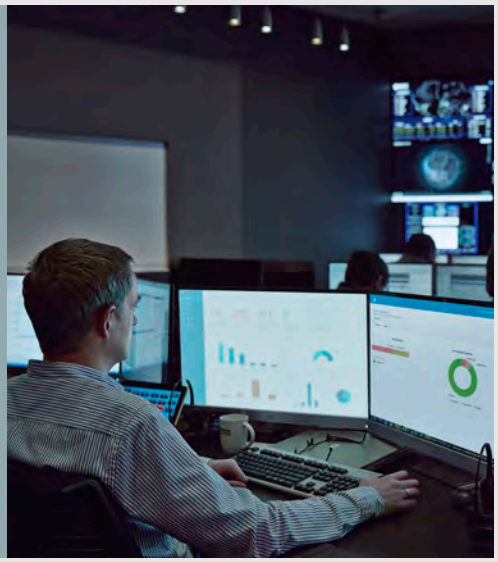


継続的な管理

デバイスセキュリティの可視性や制御性を向上させるには、保有するすべての機器のハードウェアとファームウェア構成をプロアクティブに管理する必要があります。組織のITポリシーを確実に遵守できるよう、IT部門がリモートでデバイス設定を監視したりアップデートしたりするために役立つツールを特定します。さらに、ファームウェアアップデートを迅速に展開して、自社のハードウェアやファームウェアのアタックサーフェス（攻撃対象領域）を減らせるようにし、攻撃者が脆弱性を悪用する機会を最小限に抑えるようにします。

監視と修復

一般的にハードウェアやファームウェアへの攻撃は検知が難しく、修復には多額のコストがかかります。しかし、ハードウェアやファームウェアに対する攻撃を予防、封じ込め、検知、修復するための機能が組み込まれたデバイスを導入することで、下層レベルへの脅威に対するレジリエンスを構築できます。特に、デバイスの盗難や紛失のリスクへの対処法として、リモートでの検索、ロック、消去機能を備えたデバイスを検討してください。次に、デバイス監査ログをプロアクティブに監視して、ハードウェアとファームウェアの変更を検証し、不正な変更を検知して漏えいのリスクや悪用の兆候を特定します。



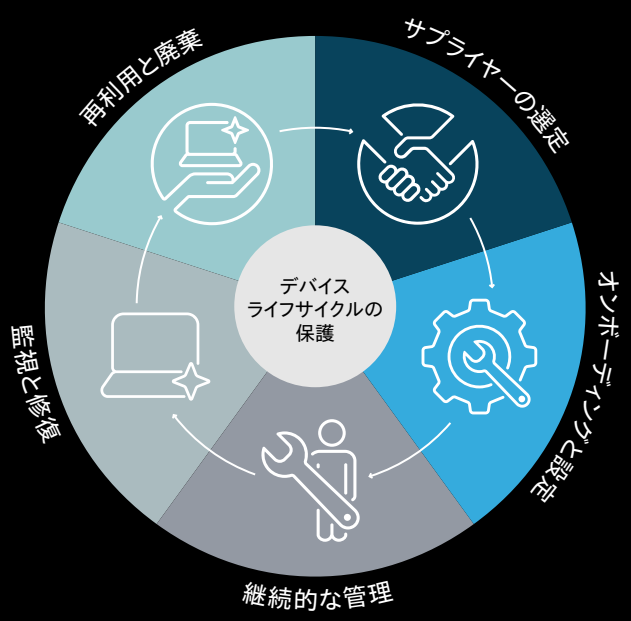
再利用と処分

安全なリサイクルや安全な廃棄に関連する運用コストを抑えるために、すべてのハードウェアおよびファームウェアの重要データを安全に消去できるデバイスを優先するようにします。デバイスを再デプロイする前に、それまでのサービス履歴を監査し、管理の連鎖（chain of custody、CoC）およびハードウェアとファームウェアの完全性を検証します。

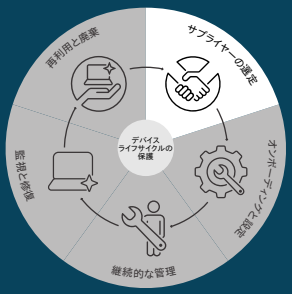
「工場から始まり、インフラ内のデバイスの寿命を通じて、ハードウェアやファームウェアに関わるサイバーリスクをデバイスのサプライチェーン全体で管理していく上で、組織は数多くの障害に直面します。攻撃者が攻撃への投資をシフトレフトするようになった現状では、こうした点を改善して最新の脅威に先回りする必要が高まっています。

これに伴って、デバイスエコシステムのライフサイクル全体を通じてハードウェアとファームウェアのセキュリティを保護、監視、管理するために、デバイスセキュリティの制御と管理のプロセスを改善することがますます求められるようになっています。」

– HP Inc. セキュリティリサーチおよび
イノベーション担当チーフテクノロジスト、
ボリス・バラシェフ（Boris Balacheff）



1. 信頼の問題—適切なサプライヤーを選定することの重要性



ソフトウェア、ハードウェア、ファームウェアのサプライチェーンに対する攻撃は、大きなダメージを与える可能性があります。今や悪名高いSunburst攻撃（SolarWinds Orion IT監視システムに悪意あるコードを挿入し、ソフトウェアを兵器化してSolarWindsの顧客に感染させる攻撃）の余波で、サプライチェーン攻撃に強いITインフラストラクチャの構築は、IT部門やビジネスリーダーだけでなく、政府にとっても優先すべき課題となっています。

2021年に発令された米国大統領令14028により、政府調達のためのソフトウェアサプライチェーンのセキュリティ要件の策定が加速し、ファームウェアもその対象範囲に含まれることが明示されました。EUでもサイバーセキュリティに関する新たな要件の導入がサプライチェーンのあらゆる段階で進んでいます。改正ネットワーク及び情報システム指令（NIS2）を皮切りに、デバイス自体を対象とする無線機器指令 第3.3条、サイバーレジリエンス法まで範囲を広げて、より安全なハードウェアとソフトウェアを確保しようとしています。他にも多くの国がこの分野に積極的に取り組んでいます。英国では新たにIoTサイバーセキュリティの規制、サイバーセキュリティおよびレジリエンス法案により、「規制範囲を拡大して、より多くのデジタルサービスとサプライチェーンを保護」しようとしています。

こうした安全なサプライチェーンの必要性に対する意識の高まりがまさに強く意識されるようになっています。ITSDMの78%が、攻撃者は工場内や輸送中にデバイスを感染させようとするため、ソフトウェアとハードウェアのサプライチェーンのセキュリティへの関心が今後高まっていくだろうと回答しています。さらに71%が、サプライチェーンを標的にしたAIが生成したマルウェアが、自社の業務にとって大きな脅威になると考えています。

このような懸念は、信頼できるサプライチェーンに依存することが組織のリスクを軽減する上でもお客様に安心を与える上でも、重要であることを改めて強調しています。そのため、最初からセキュリティ要件を考慮して、デバイスの調達プロセスに組み込む必要があります。しかし、依然としてセキュリティは後回しにされがちです。

1.1 セキュリティ、IT、調達の各部門の連携は依然として低レベル：

調達チーム、ITチーム、従業員はいずれにも、デバイスの要件について異なる優先順位があります。調達業務の難しさは、組織内のさまざまなステークホルダーから異なる要件を収集し、正しい優先順位で考慮に入れることにあります。技術的な専門知識を持つセキュリティやITの専門家は、NISTのような標準化団体のベストプラクティスに従ってガバナンスやポリシーのコンプライアンスを確保するための基準を定義し、基準を満たしているかを確認するのに最適な立場にいます。このモデルでは、IT部門がデバイスの処理能力、RAM、ストレージ容量がエンドユーザーのニーズを満たすのに十分なものになるよう、要件を設定します。セキュリティおよびリスク管理部門は、ハードウェアやファームウェアに加えてサプライヤーのセキュリティ要件まで規定し、一方、場所にとらわれない働き方を行う従業員は可搬性、物理的デザイン、ブランドの評判について、好みを提案することができます。

デバイスセキュリティの重要性を考えると、エンドポイントデバイスベンダーの選択に際してはセキュリティチームが発言権を持つことが重要です。しかし、ITSDMの半数以上（52%）は、調達部門がハードウェアやファームウェアのセキュリティに関するサプライヤーの宣伝文句を検証するために、IT部門やセキュリティ部門と協働することはほとんどないと回答しています。調達、IT、セキュリティ部門が連携して、PCやプリンターの要件を定義していると回答した企業は全体の4割以下でした。

60% | ITSDMの60%は、デバイスの調達にIT部門やセキュリティ部門が関与しないことが、企業をリスクにさらしていると回答しています。

1.2 提案依頼書（RFP）に記載されたセキュリティの宣伝文句は、検証なしに額面どおりに受け入れられる：

セキュリティやIT部門を巻き込んでベンダーからの回答を検証することで、より強固な体制でソリューションが完全に要件を満たしていることを確認できるようになります。しかし調査では、回答者の45%が、ハードウェアやファームウェアのセキュリティについての宣伝文句を検証する手段がないため、サプライヤーが真実を語っていることを信頼せざるを得ないことを認めています。セキュリティの言い分に対する信頼を確立するには、すべてのRFPで技術的説明が必要になります。

「諺にもあるように、Trust. but verify（信ぜよ、されど検証せよ）ということです。サプライヤーを信頼することはビジネスのあらゆる側面で重要ですが、自社のITインフラストラクチャのエントリーポイントとして機能するエンドポイントデバイスのセキュリティは、中でもより重要です。しかし、セキュリティ要件が確実に満たされていることを確認するために、ベンダーの宣伝文句を検証することも同じように重要です。」

– HP Inc. サプライチェーンサイバーセキュリティ担当ビジネス情報セキュリティ責任者、
マイケル・ヘイウッド（Michael Heywood）

表1：ITとセキュリティ部門は、ベンダーとの交渉に関与しない場合が多い

PC		プリンター	
41%	41%の調達部門が、ベンダーにITとセキュリティ部門へ回答を提出させていないため、必要な質問ができない	42%	42%の調達部門が、ベンダーにITとセキュリティ部門へ回答を提出させていないため、必要な質問できない
53%	53%の調達部門が、ベンダーへの質問をe-mailで提出しておらず、回答をITとセキュリティ部門でレビューできない	54%	54%の調達部門が、ベンダーの宣伝文句を裏付ける技術資料を要求していない
55%	55%の調達部門が、ベンダーの宣伝文句を裏付ける技術資料を要求していない	55%	55%の調達部門が、ベンダーへの質問をe-mailで提出しておらず、回答をITとセキュリティ部門でレビューできない
61%	61%の調達部門が、ベンダーへの質問をe-mailで提出しておらず、回答は調達部門だけでレビューしている	66%	66%の調達部門が、ベンダーへの質問をe-mailで提出しておらず、回答は調達部門だけでレビューしている

1.3 監査はほとんど行われていない：

調査では、組織はPCやプリンターのセキュリティを4年近く維持することを期待していることがわかりました。そのため、サプライヤーは組織のサプライヤー向けサイバーセキュリティ要件を確実に遵守しているかどうか、その4年間に監査を受ける必要があります。しかし、57%の組織がPCサプライヤーに対して定期的な監査を行っておらず、62%がプリンターサプライヤーに対する定期的な監査を行っていません。3分の1以上（34%）の組織が、過去5年間にPCやプリンターのサプライヤーがサイバーセキュリティ監査で不適合になったことがあると回答しています。5社に1社（18%）が、監査不適合が重大であり、契約を打ち切ったと回答しています。

44% ITSDMの44%が、監査不適合後のサプライヤーのパフォーマンスレビューと契約更新にセキュリティを組み込んでいます。

1.4 メーカーのセキュリティガバナンスチェックが不十分：

調査では、多くの企業がベンダーの信頼性を把握するために必要なデューデリジェンスを怠っていることも示唆しています。ベンダー製品の製造国を確認していると回答したのは36%に過ぎないものの、49%が事業の所有構造や管轄地域の確認、57%が内部脅威を低減するために身元調査などサプライヤーの従業員のセキュリティをチェックしていました。セキュリティおよびIT部門は、ハードウェアのサプライチェーンを標的にする脅威が悪用する可能性のあるセキュリティリスクを特定する上で、重要な役割を果たします。

1.5 セキュリティの軽視は総所有コストの上昇につながる：

調達で選択したデバイスが強力なセキュリティ機能を備えていない場合、感染リスクが高まり、重大な侵害につながる可能性があります。組織はセキュリティの価値、つまり、堅牢なハードウェアとファームウェアのセキュリティ基盤、デバイスの完全性に対する信頼の確立と維持、デバイスのセキュリティをライフスパンにわたって管理するためのメカニズムなどの価値を数値化する必要があります。しかし、ITSDMの68%が、ハードウェアやファームウェアのセキュリティへの投資は、TCO（総所有コスト）において見落とされることが多く、結果としてコストのかさむセキュリティの問題や管理費用の負担、デバイスライフサイクルの後半の非効率につながると回答しています。

サプライヤー選定の提案

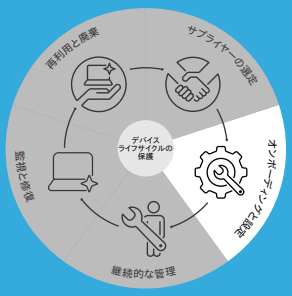
IT、セキュリティ、調達の各部門がしっかりと連携して、新規デバイスのセキュリティとレジリエンス要件を確立するようにしましょう。

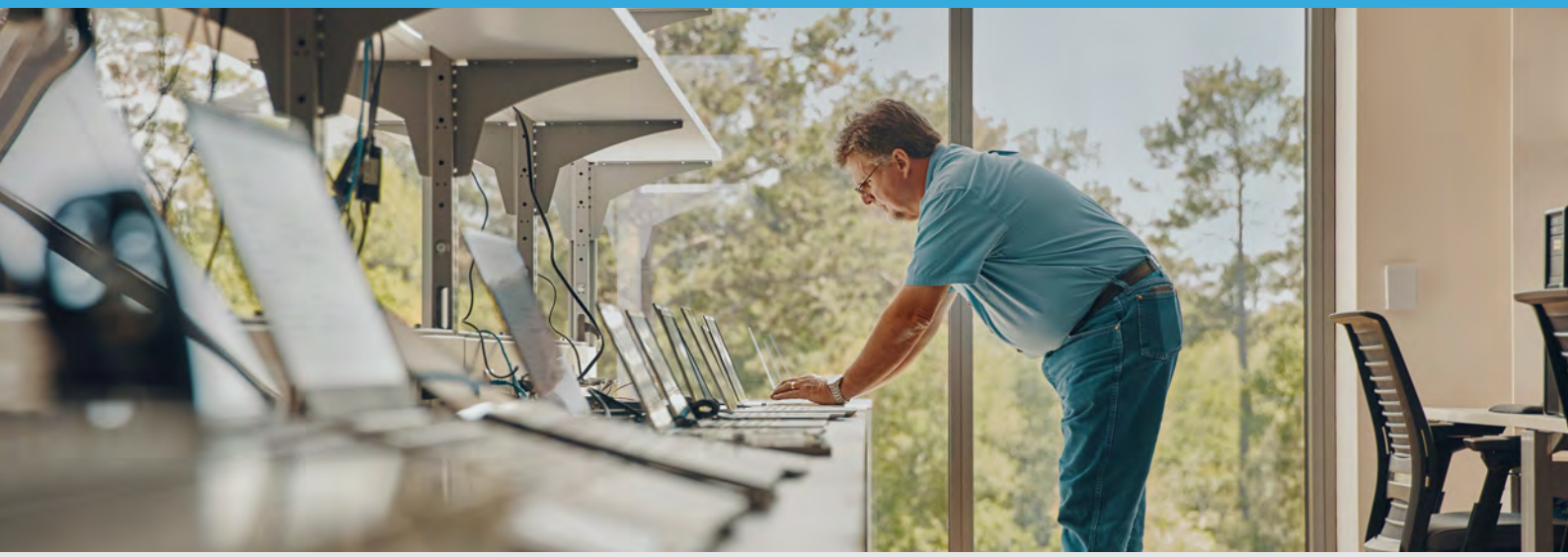
可用性の管理から、安全な運用、リカバリ、リサイクル、廃棄に至るまで、デバイスの寿命全体を通してセキュリティ要件やレジリエンス要件がどの程度、運用コストの削減に役立つかを明らかにしましょう。

ベンダーのセキュリティの宣伝文句は、技術説明や資料の提出を求めて検証。

サプライヤーの製造におけるセキュリティガバナンスの検証と監査を行ないましょう。

2. 工場から手元に届くまで—オンボーディングの過程でリスクが入り込まないようにする





デバイスは、輸送中に組織やサプライヤーの管理下を離れ、ハードウェア改ざんの潜在的リスクが生じます。攻撃者はステルス性や永続性のマルウェアをシステムファームウェアに注入したり、デバイスに悪意のあるコンポーネントを追加したりする可能性があります。そのため、デバイスのハードウェアとファームウェアが工場から到着した時点で変更されていないことを証明することが重要です。

しかし、これまではこれを証明できるようにすることが困難でした。そのため、ハードウェアとファームウェアの完全性を検証し、移動中に変更が加えられていないことを証明するプラットフォーム証明書の採用など、デバイスのセキュリティに対するより高度なアプローチのニーズが高まっています。

さらに、デバイスはシームレス（工場からエンドユーザーまで）かつセキュアに設定され、企業のインフラストラクチャに登録される必要があります。そのためには、BIOSパスワードへの依存から脱却し、最新の暗号化とハードウェアベースのセキュリティメカニズムを採用して、安全に自動化したデバイスの登録を実現する必要があります。しかし、デバイスのオンボーディングと設定に関しては、さまざまな課題が生じています：

2.1 国家主導の脅威：

ハードウェアサプライチェーンを標的にする国家レベルのグループが引き起こす脅威と、そうした攻撃に対するレジリエンスを構築する必要性に対する意識が高まっています。調査対象企業のITSDMの91%が、今後、国家主導の脅威アクターは物理的なPC、プリンターのサプライチェーンを標的に、ハードウェアやファームウェアにマルウェアもしくは悪意のあるコンポーネントを侵入させるようとすると考えています。3分の1以上（35%）が 自社もしくは他社において、サプライチェーンを狙って悪意のあるハードウェアやファームウェアをデバイスに侵入させようとする国家主導の脅威アクターの影響を受けたことを知っていると回答しています。これは、組織には、初めからそうしたサプライチェーンの脅威に対応できるように設計されたデバイスを採用する必要があることを改めて浮き彫りにしています。

63% | ITSDMの63%が、次に起こる国家主導の重大な攻撃はハードウェアサプライチェーンを侵害してマルウェアを忍び込ませるものになると考えている

2.2 ハードウェアの改ざんに対する懸念の高まり：

物理的なサプライチェーン攻撃に対する懸念が高まる中、企業はデバイスのファームウェアやハードウェアが信頼できるものであることを確認する必要があります。しかし、ITSDMの過半数（51%）は、PCやプリンターのハードウェアおよびファームウェアが輸送中に改ざんされたかどうかを確認することはできないと回答しています。プラットフォーム証明書などの製造元のアーティファクトは、デバイスに組み込まれたハードウェアやファームウェアが工場出荷後に変更されたかどうかを検証することで、輸送中のデバイスの改ざんの試みを検知するために役立ちます。

「デバイスの安全を確保するには、まず、デバイスが意図したとおりのコンポーネントで構成されており、移動中に改ざんされていないことを確認しなければなりません。攻撃者が輸送中にデバイスを侵害すれば、比類のない可視性を得て、そのマシン上で起こることを逐一把握してコントロールできるようになります。CEOのノートPCにこんなことが起こったら、どれほど影響があるか、想像してみてください。」

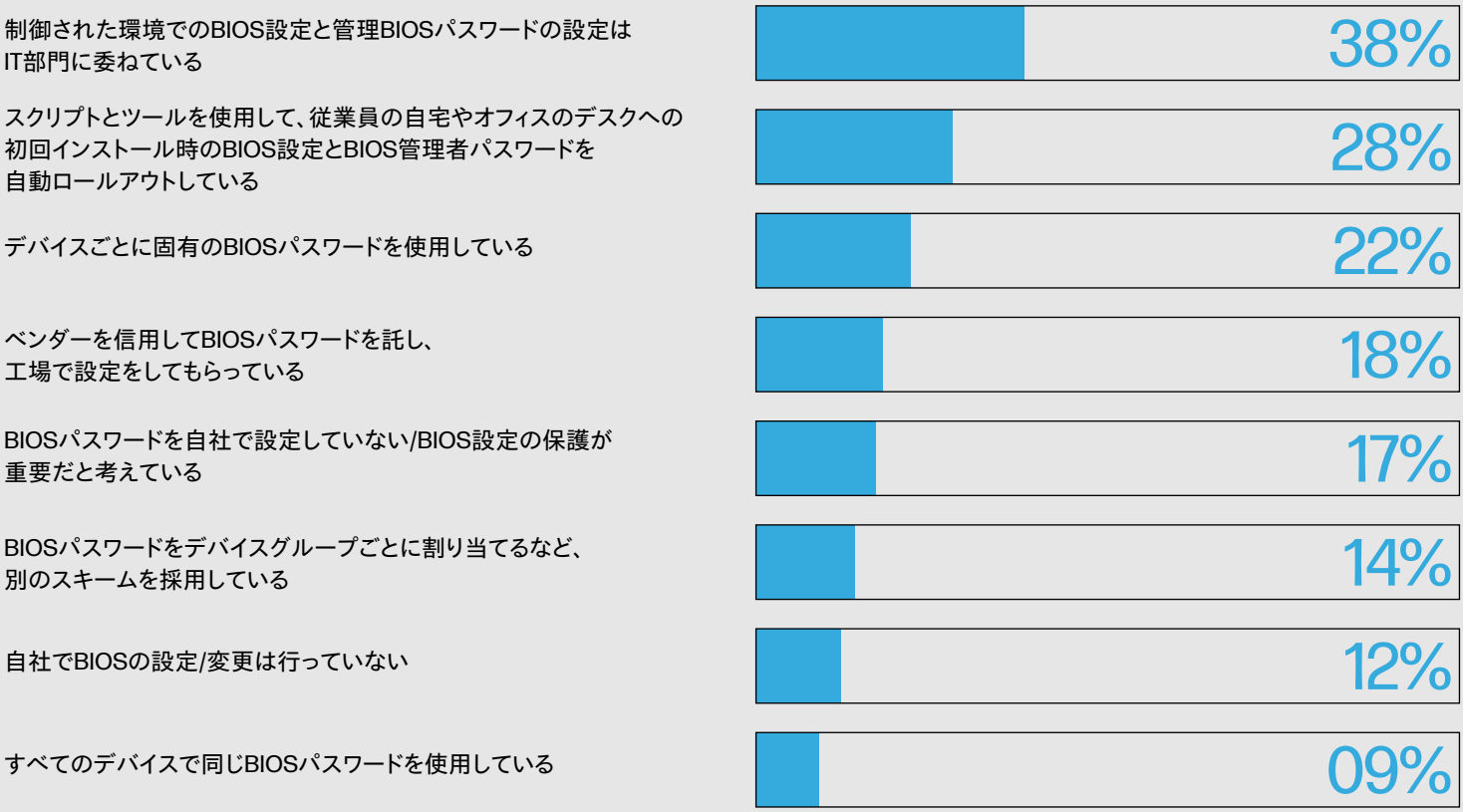
– HP Inc. HP Security Lab プリンシパル脅威研究者、アレックス・ホランド（Alex Holland）

2.3 BIOSパスワードの不適切な使用：

ITSDMの半数以上（53%）が、BIOSパスワードが共有されていたり、使いまわされていたり、強度が不十分であると回答しています。また、53%はプラットフォームのライフサイクルを通じて、BIOSパスワードを変更することがほとんどないとも答えています。強力なBIOSパスワードがないと、脅威アクターはセキュリティ機能を無効化することでシステムの設定を大幅に弱体化でき、デバイスやそこに保存されているデータが危険にさらされる可能性があります。堅牢なBIOSパスワードが、デバイスの完全性を保護し、改ざんの試みを阻止し、ファームウェア設定への不正アクセスを防止するために役立ちます。

多くのITSDM（55%）が、ファームウェア設定を保護するためにBIOSパスワードを設定したいが、複雑すぎたり、コストがかかるために設定できないと回答しています。公開鍵暗号を導入することで、より強固な保護が実現します。ITSDMの26%は、パスワードでは不十分であり、より高度な認証（公開鍵暗号など）を使用したBIOS管理をサポートするベンダーが必要と回答しています。

グラフ1：デバイスごとに固有のBIOSパスワードを使用している組織はほとんどなく、ファームウェアは危険にさらされています。以下のグラフは、BIOS設定やパスワードの安全な設定に苦労している組織の割合を示しています。



2.4 場所にとらわれない働き方（WFA）には、ゼロタッチオンボーディングが必要：

近年、従業員は常にオフィスに勤務するスタイルではなくなってきています。場所にとらわれない働き方を行う従業員の71%が、過去4年間に新しい業務用PCの支給を受けており、その半数以上（54%）がこれらのデバイスを自宅に直送していました。

しかし、こうした変化は、依然として手作業でオンボード作業や設定を行わなければならないITチームやセキュリティチームに課題を生じさせています。これはユーザーにとっても摩擦を生じさせることになります。デバイスを自宅に配送させた従業員のほぼ半数（48%）だけでなく、デバイスをオフィスで受け取っていた従業員の中でもほぼ同程度（39%）が、このプロセスが面倒であるとを訴えています。到着したデバイスの3分の1以上(37%)は依然としてオンボーディングと設定を行わなければならず、必要なソフトウェアをすべてセットアップするには平均9時間、つまりまるまる1営業日を要します。

ITやセキュリティ部門のリーダーは、ユーザーの不満を共有しており、57%がクラウド経由でデバイスをオンボードできないことに苛立ちを感じ、クラウド経由で行えるようにすることで時間も人手も無駄を抑えられると考えています。これにはOSイメージの作成と導入も含まれており、ITSDMの71%が製造元のデフォルトのイメージを使用するのではなく、OSイメージを作成していると答えています。

78% | ITSDMの78%は、セキュリティ向上のため、クラウドを通じたゼロタッチオンボーディングにハードウェアとファームウェアのセキュリティ設定を含めることを希望

34% | 場所にとらわれない働き方を行う従業員の 34% が、IT 部門からの新しいPCの入手が「必要以上に大変」と回答

オンボーディングの提案

デバイスのライフサイクル全体を通じてファームウェア構成を安全に管理し、ファームウェア設定の制御にはパスワードよりも公開鍵暗号やデジタル証明書を使用しましょう

製造元のアーティファクトを利用して、ハードウェアとファームウェアの完全性を検証することで輸送中のデバイスの改ざんを検知しましょう

ハードウェアとファームウェアの設定を安全にプロビジョニングするベンダーのファクトリーサービスを採用することで、ライフサイクルの早い段階でデバイスを保護しましょう

デバイスとユーザーの安全なゼロタッチオンボーディングを可能にするデバイスセキュリティ機能を特定し、コストを最小限に抑えて、エンドツーエンドのインフラストラクチャセキュリティを強化しましょう

3.デバイスの完全性を管理する―恐れが無為無策を促していないか？

デバイスを工場から従業員の手元に安全に届けることは、一部に過ぎません。デバイスが導入されると、ITおよびセキュリティ部門はプラットフォームのセキュリティ設定をファームウェアレベルで継続的に管理しなければなりません。実際、ITSDMの78%が、ライフサイクル全体を通じて継続的にデバイスの完全性を検証する必要があると回答しています。

デバイスインフラストラクチャと実装されるすべてのソフトウェアのセキュリティは、下層レベルのファームウェアセキュリティに依存します。そのため、ファームウェア設定のコンプライアンスは、各デバイスのライフタイムを通じて厳密に管理する必要があり、安全で堅牢なリモート構成管理のソリューションが求められます。

しかし、組織がデバイスを効果的に管理することを妨げる重要な課題があります。

3.1 アップデートに対する不安（ FOMU ）：

組織は、ドミノ効果の可能性を恐れ、BIOSやファームウェアの定期的なアップデートを実行していません。ITSDMの63%が、ノートPCのファームウェアアップデートがリリースされてもすぐに更新処理しないと回答し、プリンターでは64%と若干高くなっています。ITSDMの半数以上（ 57% ）が、ファームウェアに関してアップデートすることへの不安（ FOMU ）があるとも回答しています。4分の3（ 75% ）は、アップデートを簡単に元に戻せるなら、もっと頻繁にファームウェアのアップデートを行うと回答しています。ITSDMの80%が、AIの出現により攻撃者は不正プログラムの開発を大幅に迅速化できうるため、従来以上に素早いアップデートが重要と認識していることを考えると、これは特に重要な点です。

「脆弱性のパッチが適用されていない状態が続けば続くほど、悪用の機会は拡大します。これはソフトウェアだけでなくファームウェアにも言えます。攻撃者の巧妙さは高まり続けており、ソフトウェアセキュリティ対策をすり抜けようとする下層レベル攻撃にさらされる危険性を低減するには、ファームウェアパッチの適用速度と頻度に加えて、ファームウェア設定の積極的な管理が不可欠になっています。」

– HP Inc. セキュリティリサーチおよびイノベーション担当チーフテクノロジスト、ボリス・バラシェフ（ Boris Balacheff ）

81%

ITSDMの81%は、ハードウェアとファームウェアのセキュリティを優先事項にして、脅威が脆弱なデバイスを悪用できないようにしなければならないと考えています。

表2：ITSDMは、ハードウェアの完全性とファームウェア管理パスワードの管理が、チーム共通の課題と回答

PC		プリンター	
40%	ハードウェア自体の完全性管理（ハードウェアコンポーネントの変更を制御して完全性を維持）	38%	ファームウェア管理パスワードの管理による設定変更の安全な発行やテクニカルサポート
39%	設定変更の安全な実行やテクニカルサポートのためのファームウェア管理パスワードの管理	37%	最新のファームウェアの維持
39%	適切なファームウェアセキュリティ設定を定義と、最新の状態の維持	36%	ハードウェア自体の完全性管理（ハードウェアコンポーネントの変更を制御して完全性を維持）

3.2 場所にとらわれない働き方は、継続的な管理の進化を意味する：

71%のITDMが、場所にとらわれない働き方の増加によって、デバイスセキュリティの管理が一層困難になったと回答。ITおよびセキュリティ部門は、PCのハードウェアやファームウェアのセキュリティの運用管理に1カ月あたり平均4時間、プリンターに3.5時間を費やしています。さらに、ITSDMの36%が、PCに導入されたOSイメージを年に3～4回更新すると回答しています。ハイブリッドな働き方や場所にとらわれない働き方が求められる時代には、常時接続のリモート接続によってより効果的な資産管理が実現されることで、こうした課題が軽減される可能性があります。

17%

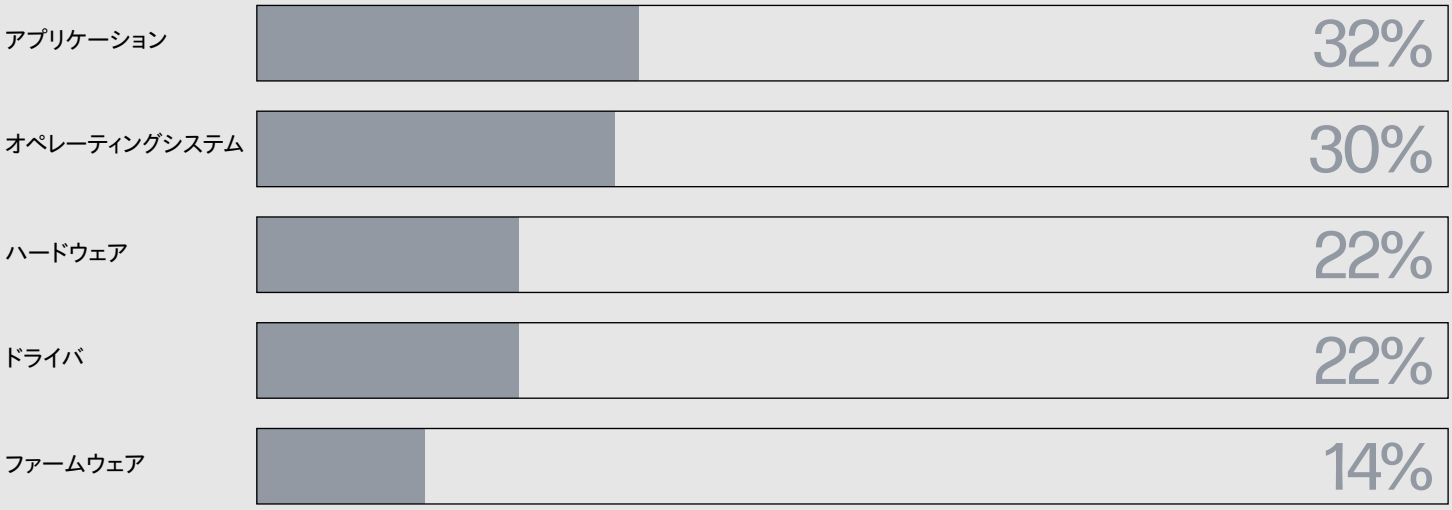
場所にとらわれない働き方を行う回答者の17%が、ソフトウェアやOSのアップデートや削除、再インストールによって自分のデバイスを修復したと答えており、20%がこのプロセスが大変で、完了までに平均5時間を要したと回答しています。

3.3 簿外修理が新たなリスクを生む：

資産管理に関する課題がPC修理に波及する可能性があります。場所にとらわれない働き方を行う従業員が職場のノートPCの修理が必要になった理由としては、パフォーマンスの問題（60%）、サイバー攻撃（35%）、物理的損傷（34%）が挙げられています。IT部門がリモートでこれらの問題を解決できたのは3分の1以下（32%）で、18%がデバイスをオフィスに持ち込む必要があったと回答しています。場所にとらわれない働き方を行う従業員の12%が、会社公認ではないサードパーティプロバイダーに業務用デバイスを修理させており、こうした行為によってデバイスのセキュリティが脅かされ、デバイスの完全性についてのIT部門の判断を誤らせることが懸念されます。業務用デバイスを修理に出してから返却または交換されるまでは、平均2.5日かかっています。

この間、ほとんどの従業員（61%）に一時的な代替デバイスが支給されています。しかし、5人に1人（21%）は、私有デバイスの使用を余儀なくされたり、仕事用に友人や家族のデバイスを借りなければならなかったりして、仕事とプライベートの境界線が曖昧になり、新たなセキュリティリスクが生じていました。

グラフ2：場所にとらわれない働き方を行う従業員から報告されたデバイスの修理の問題のうち、特に多かったのがアプリケーションとOSの問題でした。



3.4 デバイス管理のためのセントラルハブの欠如：

IT部門は、デバイス構成が最新でポリシーに準拠しているかどうかも可視化できておらず、その一因として、マルチベンダー環境ではデバイスのセキュリティが一貫して管理されていないことが挙げられます。ファームウェアやハードウェアのセキュリティを管理するツールはベンダーによって異なるため、運用管理が一層複雑になり、コストもかさむことになります。これがデバイスの管理ミスにつながり、最終的には脅威アクターに悪用される可能性があります。実際、回答者の60%が、大規模なマルチベンダーデバイスの管理に苦労していると回答しており、ITおよびセキュリティのITSDMの80%が、1つのツールでマルチベンダーデバイスのファームウェアとハードウェアのセキュリティを管理できれば、作業が大幅に楽になると回答しているのはそのためです。

62% | ITSDMの62%が、ハードウェアやファームウェアレベルで誤った設定をしたデバイスによる時限爆弾に直面していると回答

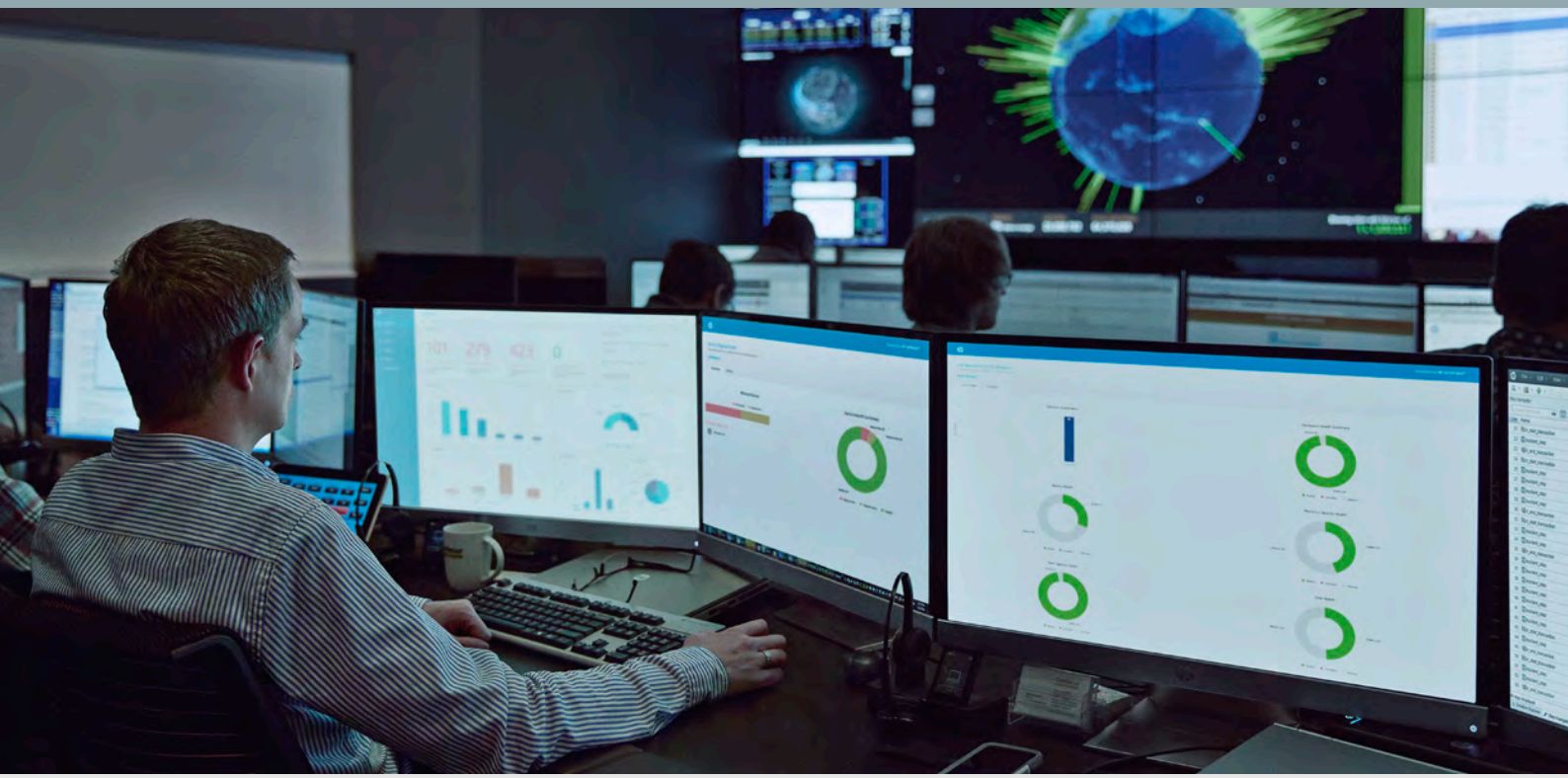
継続的な管理の提案

ファームウェアアップデートを迅速に展開して、自社のハードウェアやファームウェアのアタックサーフェスを減らし、攻撃者が脆弱性を悪用する機会を最小限に抑えるようにしましょう。

ハードウェアおよびファームウェア設定のコンプライアンス監視を全社的に導入し、ベストプラクティスや組織のITポリシーを確実に遵守できるようにしましょう。

IT部門がデバイスフリート全体を通じて、ハードウェアおよびファームウェア設定をリモートで管理できるようにする支援ツールを見つけましょう。

4. 監視と修復—
我々は負け試合を戦っているのか?



ITおよびセキュリティ部門は、脅威を継続的に監視し、セキュリティ問題を修正する必要があります。これを怠ると、脅威アクターの機密データや重要システムへのアクセスを許しかねません。しかし、PCのハードウェアとファームウェアの安全性維持に関しては、組織はいくつかの課題に直面しています。

27%	リモートでハードウェアやファームウェアレベルの脅威を緩和・修復（デバイスのロックや消去、OSソフトウェアに依存しないファームウェアの設定変更など）するためのツールがない
23%	ハードウェアおよびファームウェアの既知のセキュリティ脆弱性を、保有するすべての機器の設定にマッピングできない
22%	ハードウェアとファームウェアのセキュリティに精通し、ポリシーを主導できる人材が不足している

これらの課題は、セキュリティ部門はオペレーティングシステムのレベル同様に、ハードウェアやファームウェアのレベルでも脅威を検知し修正する能力を高めていく必要があることを明らかにしています。

ノートPCの場合、監視と修復の適用範囲を紛失あるいは盗難にあったデバイスまで広げる必要があります。これは、電源がオフまたはオフラインのデバイスにも適用できるよう、接続性やリモート管理機能を拡張することを意味します。セキュリティ部門は、ハードウェアがどのような状況に置かれていても、リモート接続して紛失や盗難、あるいはリスクのあるデバイスを見つけたり、ロックしたり、消去したりできるようにする必要があります。

組織として成熟度を高めるためには、次のような重要課題に対処しなければなりません。

4.1 AIの脅威の増大：

攻撃者がハードウェアやファームウェアのレイヤーでの侵害に成功すると、デバイスの比類なき可視性や制御性を与える可能性があり、多くの場合その方法は検知や修復が困難です。AIの急速な進化によって、このアタックサーフェスの防御が困難になり、攻撃者はこのアタックサーフェスを利用して脆弱性の特定や攻撃の開発プロセスをスピードアップしていく可能性があります。回答者の74%が、AIの民主化によって攻撃者はオペレーティングシステムより下のレベルで足掛かりを得て、複雑で巧妙な攻撃の手口が拡散することになると考えています。さらに77%が、AIによって多くの人たちが強力な機能を手にするようになり、ファームウェアやハードウェアに対する攻撃のリスクが高まると考えています。

72% | 72%が、信じられないスピードで進歩するAIによって、デバイスのセキュリティ防御がますます困難になると回答

4.2 セキュリティイベントやデバイス露出の低い可視性：

ITおよびセキュリティ部門は、セキュリティイベントをより細部まで可視化してセキュリティ体制を評価し、デバイスの使用期間中、ハードウェアやファームウェアがどのように露出した可能性があるのか把握する必要があります。しかし、ITSDMの3分の2近く（63%）は、デバイスのファームウェアやハードウェアの脆弱性や設定ミスについて、盲点がいくつもあると回答しています。さらに、57%が、ハードウェアやファームウェアの過去のセキュリティイベントの影響を分析できず、リスクのあるデバイスを見極めることができないと答えています。

79% | ITSDMの79%は、ソフトウェアセキュリティと合わせてハードウェアとファームウェアのセキュリティについても理解を深める必要があると回答

4.3 検知への高い依存度：

検知に頼ることなく、ハードウェアとファームウェアを保護することが、今後、エンドポイントデバイスセキュリティ強化の鍵になっていきます。これは極めて重要です。ITSMの60%が、ハードウェアやファームウェアへの攻撃の検知や緩和は不可能であると回答しており、情報漏洩後の修復が唯一の手段であると見なしているからです。攻撃者は捕まらないように絶えず手口を進化させており、検知メカニズムだけでシステムを脅威から守ることはできません。しかし、脅威の封じ込めのようなテクノロジーは、検知に頼ることなく脅威を安全にすることで、システムを保護します。検知メカニズムが機能しない場合でも、封じ込めを行うことで感染を防ぐことができます。ITSDMの79%が、ハードウェアやファームウェアの攻撃者の影響を抑えるためには脅威の封じ込めが重要だと考えており、さらに79%が、ハードウェアやファームウェアのセキュリティを組織のゼロトラスト管理策と統合する必要があると回答しています。

「ハードウェアやファームウェアに対する攻撃の場合、侵害後の修復は敗北戦略です。敵はこうした攻撃によってデバイスを完全に掌握し、システムの奥深くに食い込むことができます。このような脅威に対して、OSやソフトウェア層に焦点を当てた従来のセキュリティツールは無力で、検知はほぼ不可能です。先手を打つためには、最初からこれらの攻撃を未然に防いだり封じ込めたりすることが重要で、それができない企業は目に見えない、そして取り除くことができない脅威にさらされることになります」

– HP Security Lab, HP Inc. プリンシパル脅威研究者、アレックス・ホランド（Alex Holland）

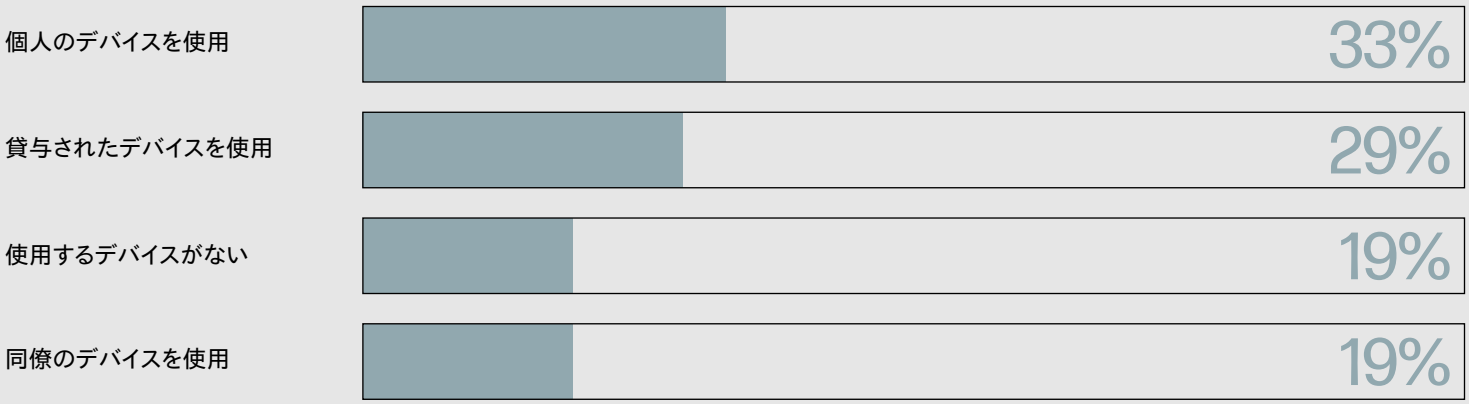
4.4 排除できないデバイスの紛失や盗難のリスク：

大企業では、昨年1年間で平均103台のPCが紛失または盗難に遭ったと推定されます。デバイスの交換にかかったコストは、デバイス1台あたり推計で平均2,273ドル（交換ハードウェア、データロス、生産性低下、ITサポートコストなど、直接および間接のコストを含む）でした。このようなデバイスの紛失や盗難の問題のために、世界中の大規模組織で生じる損失は年間86億ドル以上に上っています。

こうした損失の主な要因は、場所にとらわれない働き方を行う従業員の行動にあります。場所にとらわれない働き方を行う従業員の5人中1人がPCを紛失したり、盗難に遭ったりしています。こうした事態が生じた場合、従業員はデータ漏洩の原因になることよりも、代わりのデバイスの代金の支払いを求められたり、ローカルで保存した文書が失われたりすることの方を心配していました。

80%の組織が、データ漏洩を防ぐためには、PCの発見、ロック、消去のための安全な常時接続が必要であると回答しています。ITSDMがデバイスの紛失や盗難による最大の影響として、最も多く挙げたのは生産性の低下（43%）であり、次いで、データ漏えい（40%）、プロジェクトの遅延（38%）の順となっています。機密データやシステムを含むデバイスの紛失や盗難は、恐喝や企業ネットワークやシステムへの不正アクセスにつながる危険性があり、最大のセキュリティリスクがデータ漏えいです。場所にとらわれない働き方を行う従業員がデバイスの紛失や盗難に気づいてからIT部門に通報するまでに、25時間の時間差がありました。IT部門は、紛失したデバイスがセキュリティリスクにならないことを確認する必要があるものの、この時間差のために、脅威アクターはデバイスの復旧や消去を試みるITチームに対して大幅に先行することができます。

グラフ3：従業員のうち、デバイスの貸与を受けているのは3分の1以下で、残りの従業員は生産性を維持するためにリスクの高い代替手段を模索している。



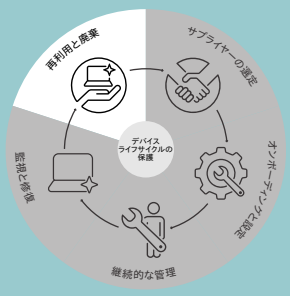
監視と修復の提案

ハードウェアおよびファームウェア攻撃を、封じ込め、検知、修復できるデバイスを導入することで、レジリエンスを向上させましょう

リモートでの検索、ロック、消去機能を備えたエンドポイントデバイスにより、デバイスの盗難や紛失のリスクに対処しましょう

デバイス監査ログを監視して、ハードウェアとファームウェアの変更を検証し、不正な変更を検知して漏えいのリスクや悪用の兆候を特定しましょう

5. セキュリティとESGのバランス— 再利用と廃棄の議論



ライフサイクルの最終段階は、デバイスが再利用、リサイクル、売却される前に確実に安全に使用停止することです。組織が持続可能性の向上を目指す中、電子廃棄物削減へのプレッシャーが次第に重視されるようになっています。

これに対して、IT部門はデバイスの再利用方法を見つけることがますます困難になっています。ITSDMの69%が、自社では簡単かつ安全に、データを完全に消去さえできれば再利用や寄付が可能なデバイスを大量に抱えていると回答しています。

しかし、データセキュリティの問題が妨げとなって再利用を進めることができず、完璧に使えるデバイスの多くが放置されたままになっています。実際、ITDMの60%は、まだ十分使えるノートPCを自社でリサイクル・再利用できていないことが、e-wasteの蔓延につながっていることを認めています。

ITSDMの過半数（68%）が、ESG（環境、社会、ガバナンス）の目標達成のためには電子廃棄物削減が容易にできなければならないが、なかなか実行に移せないでいると回答しています。デバイスに第2の生命を吹き込むには、IT部門がリモートでデバイスを確実に使用停止し、安全に再デプロイできるようにするツールが必要です。

デバイスの寿命が終わりに近づくにつれ、以下の3つの重要な課題に対処しなければなりません。

5.1 データセキュリティの懸念を解消：

持続可能性の向上に向けた圧力が高まっているものの、ITSDMの約半数（47%）が、PCを再利用、売却、リサイクルするにあたっての大きな障害はデータセキュリティの問題であると回答しており、プリンターについてはこの問題が大きな障害だと答えたのは39%でした。データのサニタイズに関する主な懸念事項は、すべての機密データが検証可能な方法でデバイスから除去されているという保証がないことです。場所にとらわれない働き方を行う従業員の41%は、雇用主の環境への影響が軽減できるという理由で、再生機器や中古機器を喜んで使用したいと考えています。しかし、ITSDMは、既存のソリューションでデバイスから消去すべきものをすべて消去できるかどうか不安を持っており、プリンター（35%）やPC（42%）の再利用に懸念を抱いています。

59% | ITSDMの59%が、データセキュリティ上の懸念からデバイスをリサイクルに出すことができず、大抵の場合、破壊・破棄していると回答

5.2 デバイスの完全なプロヴェナンス（出所、来歴）の取得：

組織がデバイスを安全に再デプロイするには、デバイスの完全性が信頼できなければなりません。しかし、68%が、デバイスの過去の使用年数やプロヴェナンス（出所、来歴）についての情報が不足している場合、再利用デバイスの購入を考え直すだろうと回答しています。デバイスを信頼できるものにするために、76%が、「サービス履歴」でデバイス寿命を通じてハードウェアに加えられた変更を確実に検証できるようにし、組織が不正な変更や悪意のあるコンポーネント、偽造部品を検知できるようにしたいと考えています。組織には、メンテナンスの全履歴に加えて、受け入れ組織が十分信頼できるデバイスのCoC（管理の連鎖）を示す能力が必要です。

5.3 デバイスの埋め立て処分の拡大：

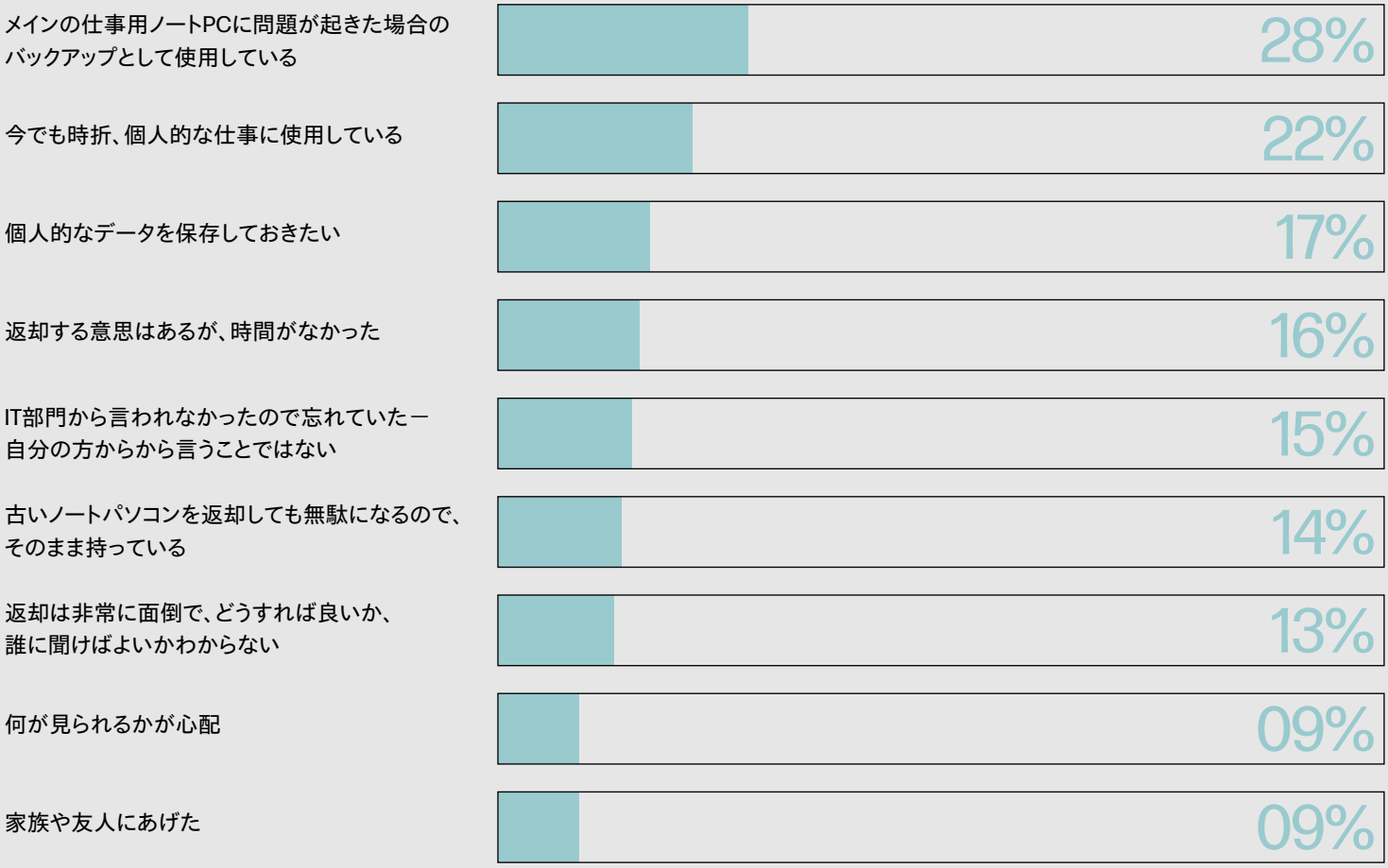
ITSDMの69%が、自社では簡単かつ安全に、データを完全に消去さえできれば再利用や寄付が可能なデバイスを大量に抱えていると回答しています。IT部門に返却されないデバイスも存在しており、場所にとらわれない働き方を行う従業員の13%が、新しい業務用ノートパソコンを支給された際に古い方をすぐに返却しておらず、7%は仕事を辞めた際にもデバイスをすぐに返却しなかったと回答しています。平均すると、場所にとらわれない働き方を行う従業員がデバイスを返却するまでの期間は8〜9週間かかっています。デバイスを返却しなければならなかった従業員のうち、70%が仕事用の古いPCを自宅やオフィスのワークスペースに保管しており、38%がそうしたデバイスを1台以上持っていると回答しています。IT部門は、古いデバイスを追跡して安全に廃棄し、機密データが残されていたり、システムにアクセスしたりできないようにする必要があります。

これらのデバイスは、場所にとらわれない働き方を行う従業員がバックアップデバイスとして使用（28%）、個人的なタスクで使用（22%）、デバイスに個人的なデータを保存しておきたい（17%）といった理由から返却されていません。さらに 9% が、古い業務用 PCを家族にプレゼントしたことがあると回答しています。

「IT部門は、企業や個人の機密データが完全に消去されているという保証がほとんどないため、使用済みデバイスを溜め込んでいます。そのこと自体がデータセキュリティにとってリスクとなるほか、ESG目標の実現にもマイナスの影響を与えます。コンプライアンス要件を満たすには、業界標準の消去プロセスまたはメディア破壊プロセスを駆使し、データ消去証明書を発行してくれるような、評判の高いIT資産処分ベンダーを見つけることが鍵となります。」

– HP ソリューションズ オペレーションおよびポートフォリオ担当シニアバイスプレジデント、グラント・ホフマン（Grant Hoffman）

グラフ4：多くのデバイスは従業員が個人として使用するため返却されない



再利用に関する提案

安全なリサイクルや再利用、電子廃棄物の削減が行えるよう、ハードウェアやファームウェアの機密データを安全に消去できるデバイスを選びましょう。

デバイスを再デプロイする前に、それまでのサービス履歴を監査し、CoC（管理の連鎖）およびハードウェアとファームウェアの完全性を検証しましょう。

最後に—
ライフサイクルセキュリティの成功への道

ハードウェアとファームウェアのセキュリティのためには、工場出荷から廃棄まで、ライフサイクル全体を通じてデバイスのセキュリティを管理できる、新しいアプローチが必要です。しかし、3分の2以上（69%）の組織が、デバイスのハードウェアやファームウェアのセキュリティ管理の手法は、ライフサイクルのいくつかのステップに限定されており、サプライチェーンから廃棄に至るまでの間、チームがデバイスセキュリティの監視や管理ができないまま、デバイスを危険にさらすことになっています。

本レポートが示すように、IT部門とセキュリティ部門は依然として、ライフサイクルのあらゆる段階で複数のプラットフォームセキュリティギャップに直面しています。しかし、サプライヤー選定段階でのセキュリティ、IT、調達の各部門の連携を強化したり、オンボーディング前の工場の段階でより多くのセキュリティ設定を用意するなど、解決策は手近なところにあります。ハードウェアとファームウェアのセキュリティを管理し、シームレスに継続的管理を実現し、脅威の検知と対応を強化する1つのツールが必要です。最後に、IT部門にすべての機密データが除去されたことを確認する手段とサービス履歴を提供することで、IT部門はより多くのリファービッシュデバイスを導入し、ESG目標を達成することに自信が持てるでしょう。デバイスのライフサイクル全体を通じてあらゆるギャップに対処してこそ、最新の脅威に対してハードウェアとファームウェアのレイヤーを真にレジリエントにすることができます。

ライフサイクル全体でデバイスセキュリティを管理するために、以下の5つの実行可能な提案を組織に提示します。

サプライヤーの選定

デバイスのセキュリティ要件の定義、ベンダーの回答の検証、サプライヤーの監査に際しては、まずデバイスの調達を、調達、IT、セキュリティの各部門が連携した取り組みとして見直すことから始めましょう。

オンボーディングと設定

物理サプライチェーンの脆弱性領域を評価し、改ざんの脅威を排除し、ファームウェアとハードウェアのセキュリティを保護、検証するための新たな手段を検討しましょう。

継続的な管理

安全で堅牢なリモート構成管理のためのソリューションを採用し、デバイス設定を常に最新の状態に保ち、BIOSやファームウェアの定期的なアップデートを取り入れましょう。

監視と修復

プロアクティブな対応を行うために修復プロセスを進化させる、つまり悪意のあるコードの実行を封じ込める脅威封じ込め技術や、データ漏洩を予防するためにデバイスを発見、ロック、消去する安全な常時接続に方向転換していきましょう。

再利用と廃棄

ハードウェアとファームウェアの管理をさらに強化し、リモートでの安全な廃棄措置を可能にして、デバイスの安全な再利用、リサイクル、寄贈を可能にしましょう。

調査方法

本レポートの調査結果は、2つの別個のデータソースで構成されています：

1. 場所にとらわれない働き方を行う従業員のサンプル：米国、カナダ、英国、日本、ドイツ、フランスでハイブリッド型、リモート型、または場所にとらわれない働き方を行うオフィスワーカー（WFA）6,055人を対象にアンケート調査を実施しました。フィールドワークは2024年5月22日から30日にかけて実施されました。調査はCensuswide社によりオンラインで行われました。

2. ITSDMのサンプル：米国、カナダ、英国、日本、ドイツ、フランスのITおよびセキュリティ関連の意思決定者（ITSDM）803名を対象にアンケート調査を実施しました。フィールドワークは2024年2月22日から3月5日にかけて実施されました。調査はCensuswide社によりオンラインで行われました。

3. ノートPCの紛失・盗難は世界で多発しており、昨年1年間にITSDMが紛失・盗難を報告したノートPCの数は1社平均で103台、紛失・盗難事例ごとの平均コストは2,272ドル、つまり、合計で23万4,119ドルのコストとなっています。次に、このコストを、調査範囲と同地域にある大規模企業の数から推計しました。
   a. 米国 -17,834社の大規模企業（米国労働省労働統計局）
   b. カナダ - 2,868社の大規模企業（カナダ政府）
   c. 英国 - 3,900社（英国政府）
   d. 日本 - 6,557社（eStat - 政府統計）
   e. ドイツ - 4,304社（OECD）
   f. フランス -1,460社（OECD）

上記のとおり、大規模企業は合計36,923社存在します。それぞれが103台のノートPCを失うと、平均コストが2,273ドル×103で23万4,119ドルとなり、全世界のノートPCの紛失・盗難によるコストは86億4437万5837ドルとなります。

提案に関する付録

サプライヤー選定のアドバイス

IT、セキュリティ、調達の各部門がしっかりと連携して、新規デバイスのセキュリティとレジリエンス要件を確立するようにしましょう。

可用性の管理から、安全な運用、リカバリ、リサイクル、廃棄に至るまで、デバイスのライフタイム全体を通じてセキュリティ要件やレジリエンス要件がどの程度、運用コストの削減に役立つかを明らかにしましょう。

ベンダーのセキュリティクレームは、技術説明や資料の提出を求めて検証しなければなりません。

サプライヤーの製造におけるセキュリティガバナンスの検証と監査を行わなければなりません。

オンボーディングの提案

デバイスのライフサイクル全体を通じてファームウェア構成を安全に管理し、ファームウェア設定の制御にはパスワードではなく公開鍵暗号やデジタル証明書を使用することが推奨されます。

製造元のアーティファクトを利用して、ハードウェアとファームウェアの整合性を検証することで輸送中のデバイスの改ざんを検知すること

ハードウェアとファームウェアの制御を安全にプロビジョニングするベンダーのファクトリーサービスを実装することで、ライフサイクルの早い段階でデバイスを保護すること。

デバイスとユーザーの安全なゼロタッチオンボーディングを可能にするデバイスセキュリティ機能を特定し、コストを最小限に抑えて、エンドツーエンドのインフラストラクチャセキュリティを強化すること

継続的な管理の提案

ファームウェアアップデートを迅速に展開して、自社のハードウェアやファームウェアの攻撃対象領域を減らし、攻撃者が脆弱性を悪用する機会を最小限に抑えるようにします。

ITチームがデバイスフリート全体を通じて、ハードウェアおよびファームウェア設定をリモートで管理できるようにする支援ツールを見つけます。

ハードウェアおよびファームウェア構成のコンプライアンス監視を全社的に導入し、ベストプラクティスや組織のITポリシーを確実に遵守できるようにします。

提案に関する付録

監視と修復の提案

ハードウェアおよびファームウェア攻撃を防止、封じ込め、検出、回復できるデバイスを導入することで、レジリエンスを向上させること

リモートでの検索、ロック、消去が可能なデバイスにより、デバイスの盗難や紛失のリスクに対処すること

デバイス監査ログを監視して、ハードウェアとファームウェアの変更を検証し、不正な変更を検知して漏えいのリスクや悪用の兆候を特定します。

再利用のアドバイス

安全なリサイクル、セカンドライフ、電子廃棄物の削減のために、ハードウェアやファームウェアの機密データを安全に消去できるデバイスを推奨する

デバイスを再度デプロイする前に、それまでのサービス履歴を監査し、CoC（管理の連鎖）およびハードウェアとファームウェアの完全性を検証する