FORRESTER®

# ハイブリッド環境における エンドポ イントセキュリティ

FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER（HPの委託による調査）2023年9月

# 目次




**プロジェクトチーム:**

Sanny Mok
シニアマーケット・インパクトコンサルタント

Tarun Avasthy
シニアコンサルタント



**調査協力:**

Forrester セキュリティおよびリスク調査グループ


**FORRESTER CONSULTINGについて**

Forresterは組織のリーダーが主要な成果を上げる取り組みの一環として、独自の客観的調査に基づくコンサルティングを提供しています。Forrester の経験豊富なコンサルタントは、顧客志向のリサーチに基づいて、持続的な効果をもたらす独自のエンゲージメントモデルを駆使しながら、リーダーの優先課題に取り組みます。詳細については、forrester.com/consulting をご覧ください。

## エグゼクティブサマリー

進化するデジタル環境において、エンドポイントライフサイクル管理が注目を浴びています。それに伴い、資産管理、ユーザー体験の保証、リスク管理という3つの包括的なビジネス課題が浮かび上がっています。リーダーがリモートワークを推進する中で、デバイス戦略の必要性が明らかになっています。例えば、正確な資産データベースの維持が重要な懸念事項となっています。特に、EUにおけるネットワーク情報システムのセキュリティに関する指令 (NIS2) の改訂案では、資産管理が義務化されています。

デジタル化への移行を進める中で、常時接続されたPCフリート管理の概念は希望の光となるものです。このアプローチは、紛失したデバイスの管理だけでなく、資産管理の改善にも役立ちます。堅牢なデータ保護を保証し、生産性を向上させ、厳格なコンプライアンスを徹底するほか、デバイスのライフサイクルにおいて、サステナビリティへの取り組みにも貢献しています。こうしたリアルタイム戦略を活用することで、企業は安全なライフサイクルを維持すること、すなわち継続的な監視と厳格なエンドポイント防御を重視したフレームワークを強化することができます。

2023年3月、HPの依頼により、Forrester Consultingは分散した拠点におけるエンドポイント管理の現在と今後のアプローチについて評価しました。ハイブリッドワークでは、紛失したノートパソコンや退職した従業員など、ノートパソコンや他のデバイスの効率的な管理を維持することは困難です。Forresterは、500人以上の従業員を抱える企業における312人のITおよびセキュリティの意思決定者を対象にオンライン調査を実施し、資産管理とデータセキュリティプロセスの不備が従業員体験 (EX)、業務効率、およびリスク管理に与える影響について調べました。

## 主な調査結果

**進化するデジタルワークスペース。**リモートやハイブリッドモデルの増加に伴い、分散型のワーク環境で生産性とセキュリティのバランスを取るために、エンドポイントを強化する対策が緊急に求められています。

**ファームウェア管理におけるアプローチの不備。**多くの組織において、重要なファームウェアのアップデートを見落とし、セキュリティリスクや効率の低下を招いているといった懸念すべき傾向が見られます。そのため、対策を取ることが急務です。

**位置確認、ロック、消去ソリューションの多面的な利点。**位置確認、ロック、消去は単なるセキュリティツールに留まらず、データ保護、業務効率、および規制遵守を強化する包括的なソリューションです。このツールを採用する組織は、サイバー脅威に対する強固な防御、従業員の生産性向上、NIS 2を含むコンプライアンスへの効率的なアプローチが期待できます。

**常時接続されたエンドポイント管理が包括的なITレジリエンスの要。**常時接続されたエンドポイント管理アプローチを活用することで、組織は迅速に脅威に対処し、資産の監視を向上させ、サステナブルなデバイスの運用を推進し、ITの柔軟性を強化し、コンプライアンス対策を補強することができます。

## リモートおよびハイブリッドワークモデルへの移行

今日の動的なデジタル環境では、ビジネスは大規模な変革を遂げ、リモートおよびハイブリッドなワークモデルへと移行しています。組織でこの新しい枠組みが定着していく中で、IT専門家たちは特にノートパソコンなどのエンドポイントを効率的に管理し、セキュリティを確保するという重要な課題に直面しています（図1参照）。

- **多数派となったハイブリッドワーク。**従来のオフィス環境からの大きな移行が明らかになりました。[1] Forrester Researchの2021年度データでは、46%のインフラストラクチャ系意思決定者が労働力の半数以上が常にリモートで作業していると述べています。[2] 変化をもたらした原因はコロナ禍によるものです。現在、各企業にはハイブリッドワークを成功させるための絶好の機会かつ緊急のニーズがあります。本調査では、回答者の72%は職場でハイブリッドワークモデルを採用しており、常に労働力のかなりの割合がリモートであると述べています。このため、IT専門家は従来のオフィス環境外にあるエンドポイントのセキュリティを確保しなければならないという課題に直面しています。また、それによって資産管理やデータセキュリティにおけるプロセスの複雑化とリスクが増しています。
- **今も続くオンプレミスのワークモデル。**リモートワークの傾向が強まっていますが、回答者の21%は組織が完全オンプレミスであると述べています。興味深いことに、回答者はこの数字が翌年1年間で27%に増加すると予想しています。そのため、ITリーダーは従来の作業環境と新たな環境の要求をバランスする必要が生じ、エンドポイント管理のタスクに複雑性が加わります。
- **完全リモートワークはわずかに増加。**現在、回答者のうちわずか7%が組織は完全にリモートワークモデルであると述べていますが、これは今後1年間で若干増加し、9%になる見込みです。回答者は、これが今後の1年間で若干増加し、9%にな

**58%**

の回答者が、自社の評判を維持し、未知の脅威からデータや情報を保護するためのエンドポイントセキュリティに資金を投じると述べています。

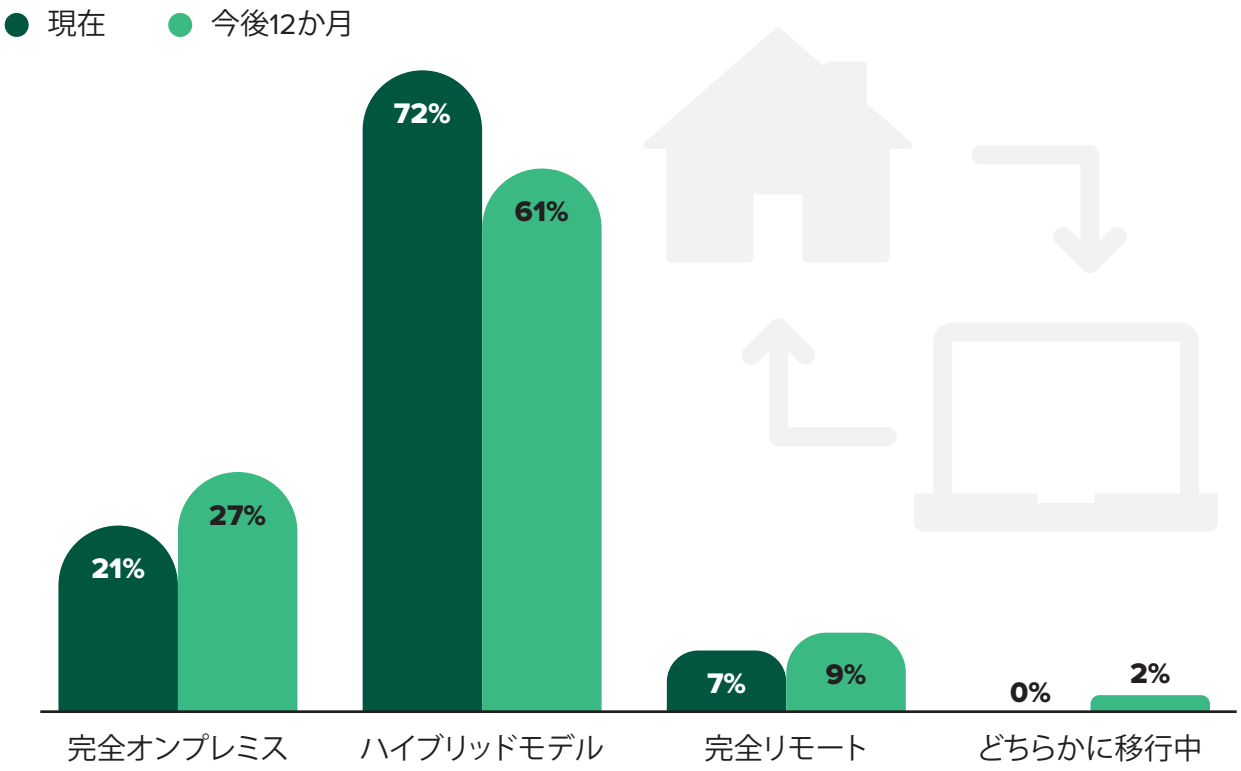
ると予測しています。控えめな上昇ではありますが、従来とは違ったモデルが容認されてきたことを示しています。これに伴い、仕事の環境において信頼できるエンドポイント管理の対策が必要になります。

**79%**

の回答者（北米企業）が、ハイブリッドモデルを採用していると答え、そのうち58%が今後1年間もこのモデルを継続する予定だと述べています。APACでは、74%がハイブリッドモデルを採用していると回答し、そのうち45%が今後もこのモデルを継続する予定だと答えました。

**図 1**

**「自組織のリモートワークの実施状況について、現在と12か月後のそれぞれに、最もよく当てはまるものを選んでください」**




調査対象：500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
出典：HP委託によるForrester Consulting調査（2023年9月）

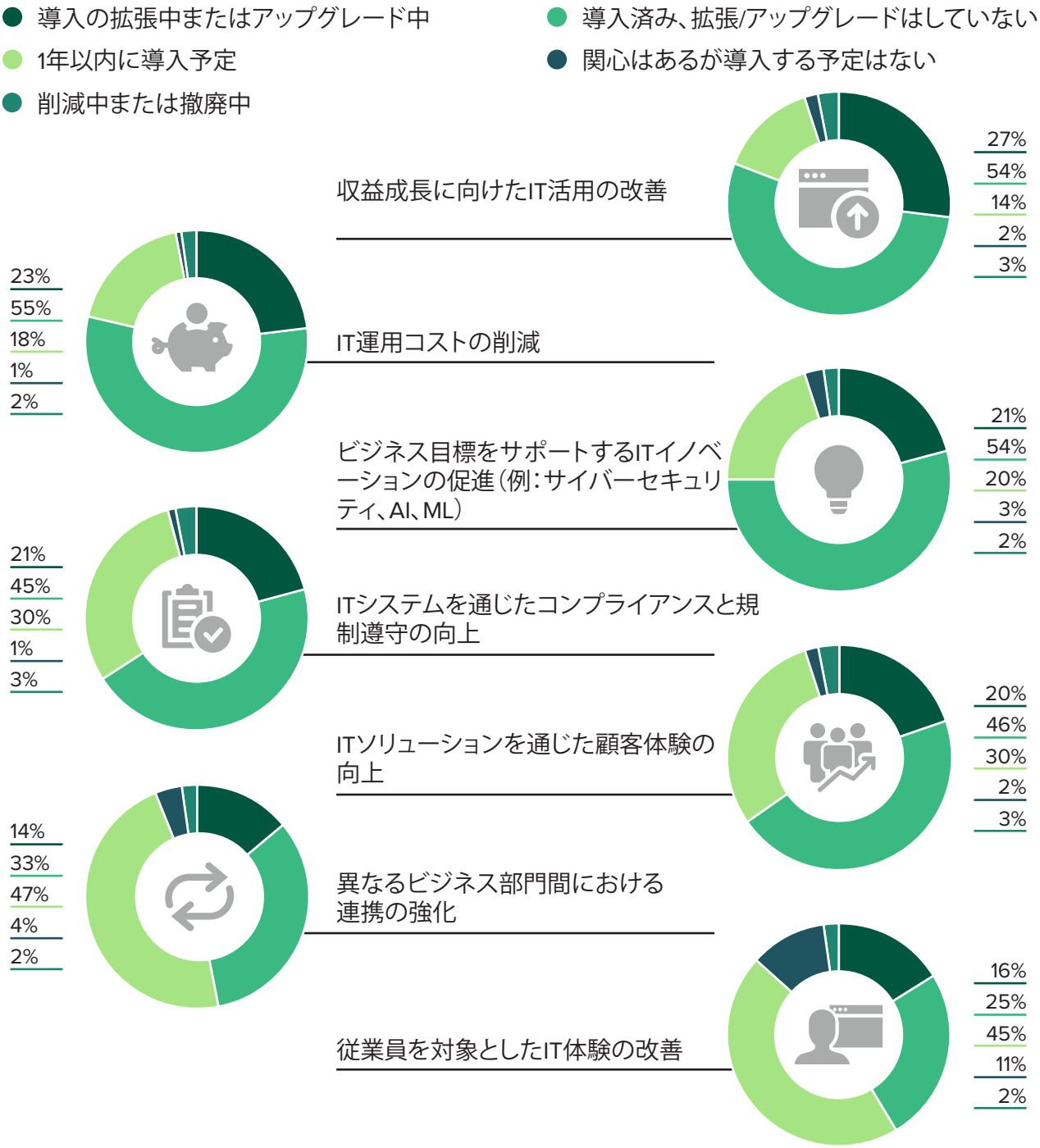
## ITの優先事項としての成長・革新・コラボレーションの重視

仕事の進化に伴い、ITリーダーの優先事項も変化しています。組織の今後の焦点と投資を決定づける戦略的なイニシアチブが重要であり、収益成長、運用コスト削減、革新、コラボレーションが最優先事項として重視されています（図2を参照）。

- **部門を超えたコラボレーションの増加。**注目すべき点は、回答者の47%が今後12か月以内に、社内のあらゆるビジネスユニット間のコラボレーションを強化する計画だと述べていることです。この関心の高まりと共に、異なる場所に分散するチーム間で効果的なコラボレーションを促進できるようにするためのセキュアなITフレームワークの需要も増加しています。ITの貢献が単に生産性やセキュリティの強化にとどまらず、部門を超えた連携で相乗効果を発揮するためにも不可欠となります。
- **デジタル体験への関心の高まり。**従業員向けのデジタル体験は変革の段階を迎えています。この分野での措置を講じているが将来的な拡大計画はないと述べたのは、回答者のうちわずか25%でした。これに対し、45%が来年に向けて従業員のデジタル体験を改善するための準備を進めていると答えています。こうした大きな変化は、デジタル体験が最大限に活用されていないことを示しています。16%の回答者が、現在のデジタルワークスペースを拡大またはアップグレードしている過程にあると述べており、デジタル体験の向上に関心を示しています。
- **収益成長とコスト削減の2つの使命。**これは依然として、ビジネスの目標に掲げられています。回答者の54%が、収益を増やすためにITイニシアチブを実施し、積極的な対策を講じていると答えています。回答者の27%が、既存のIT導入を拡張するか、改善する過程にあると述べました。これは、ITがサポートサービスとしてだけでなく、ビジネス拡大の要としての二重の役割を果たしていることを示しています。同時に、コスト削減は回答者の組織にとって引き続きITの優先事項であり、23%がコスト削減の取り組みを強化しており、驚くべきことに55%が既にコスト削減戦略を展開しています。

**図 2**

## 「今後12か月間で以下のイニシアチブのうち、あなたの組織でITの上位優先事項になるものはどれですか?」




調査対象:500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
注:割合は四捨五入しているため合計が100%にならない場合があります。
出典:HP委託によるForrester Consulting調査(2023年9月)

- **イノベーションは必要不可欠。**ITイノベーションは、サイバーセキュリティ、人工知能、機械学習(ML) などの領域を含んでおり、多くの企業にとって既に焦点となっています（54%が自社が関連するイニシアチブを既に展開していると回答）。約21%の企業は、既存のシステムの改善や更新を検討していると答えています。ハイブリッドモデルとリモートワークの拡大に伴い、先端のIT革新が必要とされています。これは、広範な労働力のために、安全で、柔軟性に優れた、効果的なデジタルワークスペースを創る上で重要な役割を果たします。

デジタル体験の改善を優先する企業は、APACは38%、EMEAは31%、北米は21%でした。

## 事後対応型になるデバイスライフサイクル管理

デバイスのライフサイクルを管理することは、単なる日常業務とは異なり、組織の業務レジリエンスを維持するために重要なタスクです。ファームウェア、オペレーティングシステム (OS)、およびアプリケーション全体で一貫した更新とメンテナンスを確実に行う包括的なエンドポイント管理戦略は、任意ではなく必須です。特に、ハイブリッドワークやリモートワークモデルを採用する中で、ますます重要性を増しています。このような戦略は、ITおよびセキュリティの業務効率を達成する上で重要です（図3を参照）。

- **ファームウェアの更新が著しく不十分。**現在のファームウェア更新のアプローチは、事後対応型であるうえ、リスクが伴います。パッチ管理はエンドポイントの健全性を保つ上で重要です。ただし、企業がエンドポイントセキュリティプラットフォームにおいて、完全な可視性とコントロールを持っている場合にのみ有用です。[3] 残念ながら、多くの企業が調整不足のために効果的にパッチを適用することに苦心しています。驚くべきことに、回答者の約42%が、自身の組織がファームウェアの更新を年に1回しか行っていないと述べており、15%は更新の頻度は半年ごとと回答しました。こうした更新頻度の低さは、通常の業務を妨げる互換性の問題からセキュリティの脆弱性まで、多くのトラブルを引き起こす可能性があります。さらに注視すべき調査結果は、回答者の12%が、自身の組織がセキュリティやシステムの安定性に差し迫った脅威を感じた時にのみファームウェアの更新に頼ると述べたことです。注意を欠くこのような態度は単にリスクがあるだけでなく、潜在的なサイバー攻撃を明らかに呼び寄せることになります。
- **デバイスのライフサイクル終了後に必要となる消去。**デバイスのライフサイクル終了時には課題が待っています。回答者の約35%が、自身の組織がデータを消去した後、デバイスをリサイクルをするための社内プロセスを実施していると指摘しています。このプロセスはセキュリティに配慮されているように見えますが、手作業の手順が多く、労力を要するうえに非効率です。徹底的にデータを消去し、廃棄時にデータ漏洩を防ぐことは困難です。このような煩雑で非効率な手作業、労働集約的なプロセスは、リモートやハイブリッド従業員のデバイスを扱う場合、さらに困難になります。

- **外部委託される廃棄プロセス。**内部でのトラブルを回避するために、回答者の約17%が、自身の組織がデバイスの廃棄プロセスを外部の専門家に委託していると述べています。その理由は社内のリソース不足によるものや、外部の専門家によって安心を確保できることにあります。ただし、これらの第三者サービスに、組織のデータセキュリティプロトコルに適合し、世界的な環境基準を満たすことを義務付ける必要があります。また、追加費用の負担もあります。外部委託への傾向は、組織が内部の手作業プロセスの非効率性や複雑さを認識し、より効率的なソリューションを求めていることの表れです。

APACでは、中小企業(SMB) の回答者の48%がデバイスをリサイクルする前にデータを社内で消去しています。一方、その割合はEMEAでは28%、北米では35%です。

**図3**

**「以下のうち、あなたの組織がファームウェア (BIOS) の更新を行う頻度はどの程度ですか?」**


**「ライフサイクルが終了したデバイスをどう管理していますか?」**

**35%** データを内部で消去し、デバイスをリサイクルに出す

**18%** ハードドライブを物理的に破壊し、残りのデバイスを売却/寄付する

**17%** データを内部で消去し、デバイスをリサイクルに出す

**17%** 第三者サービスにプロセスを委託する

**13%** ハードドライブを物理的に破壊し、残りのデバイスをリサイクルに出す

調査対象:500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
注:割合は四捨五入しているため合計が100%にならない場合があります。
出典:HP委託によるForrester Consulting調査(2023年9月)

## 課題として残るリモートエンドポイントの管理

リモートワークやハイブリッドワークモデルへの移行によって、エンドポイントの管理がますます複雑になりました。包括的な資産データベースの維持から、サステナブルなデバイスライフサイクルの管理、エンドポイントセキュリティの強化、コンプライアンスの確保まで、組織はあらゆる課題に直面しています（図4を参照）。

**44%**

の大企業の回答者が、効率的なツールやシステムの不足により、紛失や盗難にあったデバイスを見つける能力が限られていると述べました。

- **複雑化する資産の追跡。**注目すべきは、回答者の62%が、組織が正確かつ常に更新された資産データベースを維持するのに苦労していると述べており、この課題は切実な問題として広く認識されています。この問題は、効率的な意思決定を妨げるだけでなく、リソースの配分やセキュリティポリシーの適合にも障害をもたらします。特に、労働力が異なる場所に分散する状況では、その影響が顕著になります。
- **デバイスのライフサイクル管理とサステナビリティ。**およそ55%の回答者が、サステナビリティを考慮したデバイスのライフサイクル管理を監督するのは困難を極めると指摘しました。環境への影響を最小限に抑えながら実施するため、デバイスの調達から最終的な廃棄やリサイクルに至るまで、全体のプロセスが労力を要する取り組みとなっています。
- **脆弱なエンドポイントのセキュリティ確保。**回答者の50%が、自身の組織のエンドポイントセキュリティソリューションが不十分だと考えています。デバイスを保護する堅牢なセキュリティや包括的な機能の不足を挙げており、ますますデジタル化し分散した作業環境において、ITセキュリティソリューションの重要性が強調されていました。

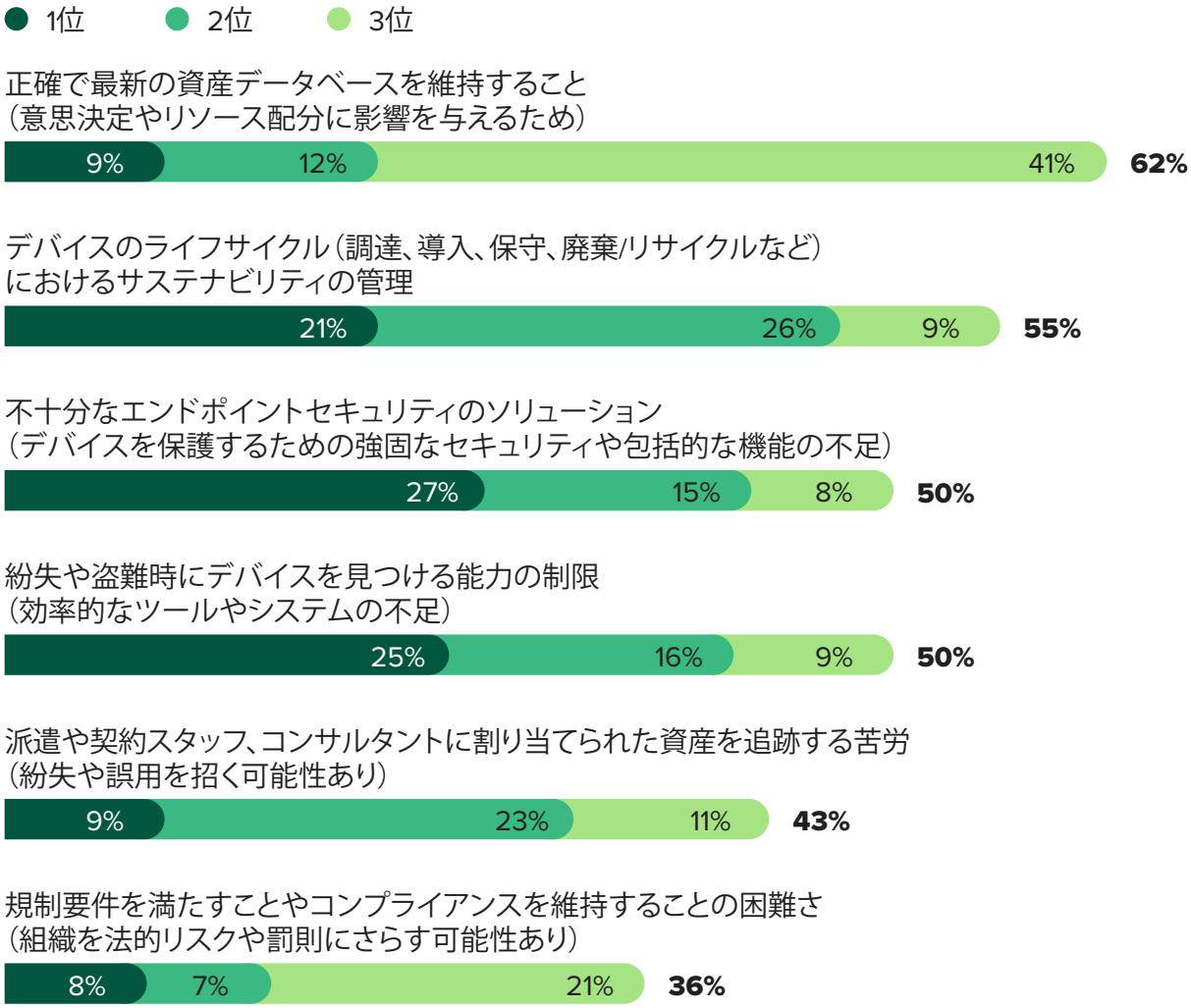
**67%**

の回答者が、リモートのエンドポイントとの安全な通信を確保することが一番の懸念事項だと考えています。

さらに、これらの課題と絡み合っているのは、規制要件の遵守が必要とされているということです。組織は外部からの規制に対処するだけでなく、内部の監査基準にも対応しようと努力しており、堅牢なエンドポイント管理を確保するために内部評価と外部のコンプライアンスの双方からの圧力があることを強調しています。

**図 4**

## 「リモートのエンドポイントに対処する際に、どのような問題に直面していますか?」



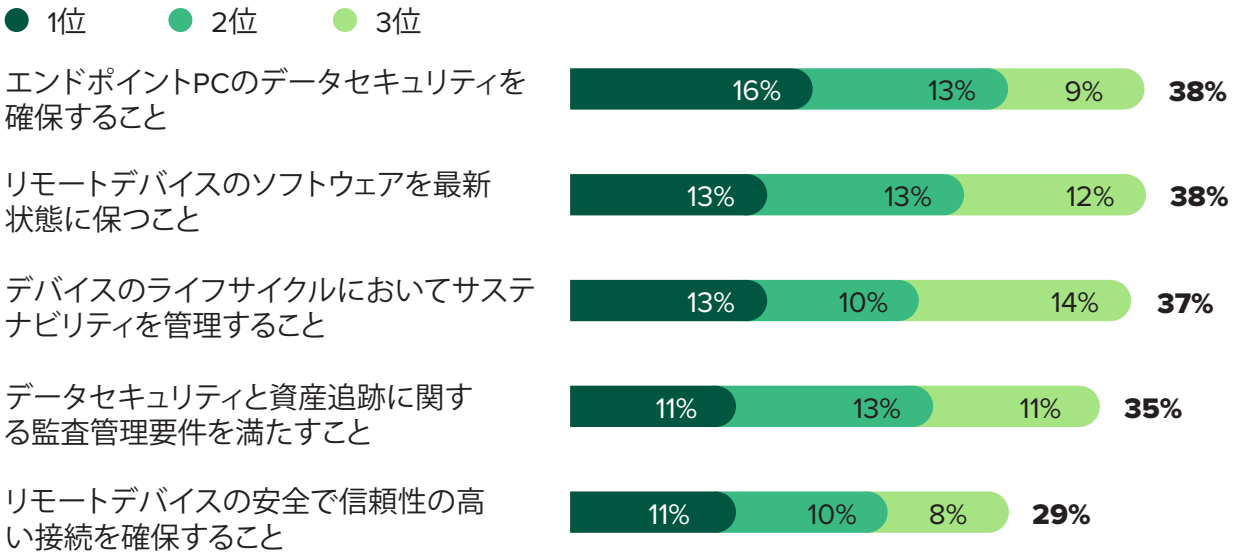

調査対象:500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
注:四捨五入のため、パーセンテージの合計は個々の数値を加算したものと一致しない場合があります。
出典:HP委託によるForrester Consulting調査(2023年9月)

## 企業が取り組むサステナブルなデバイスのライフサイクルとデータセキュリティに関する懸念

リモートエンドポイントの管理には、IT専門家が頭を抱えるさまざまな課題があります。主に深刻な課題として、サステナブルなデバイスライフサイクルの管理、リモートデバイスのソフトウェア更新の確保、そしてエンドポイントデータの保護の3つが挙げられます（図5を参照）。

**図 5**

### 「次のタスクのうち、リモートエンドポイントを管理する際に課題となるものはどれですか？」




調査対象：500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
注：上位5回答を表示
出典：HP委託によるForrester Consulting調査（2023年9月）

**エンドポイントのデータセキュリティは、回答者の55%にとって主要な懸念事項。**実際、回答者の16%がこれを一番重要な課題と位置付けています。リモートワークによって、データセキュリティへのリスクが深刻な問題となっています。デバイスが保護されていないネットワークを介して接続される場合、サイバー攻撃の脅威にさらされやすくなるためです。ノートパソコン上での適切なデータ管理を怠ると、それらのデバイスが使用されなくなった際に機密情報が侵害されたり不正アクセスのリスクにさらされる可能性があります。その結果、コンプライアンスや法的な問題を引き起こすことになります。

特定された課題とその重要性は一致しています。例えば、サステナブルなデバイスのライフサイクル管理に重点を置くことは、IT専門家が技術環境の進化に対応しつつ、サステナビリティを考慮した戦略を策定する必要性が急務となっていることを物語っています。さらに、回答者の56%が、リモートデバイス上のソフトウェアを最新の状態に保つことの重要性を強調しました。異なる作業環境における物理的な障壁だけでなく、更新のためのデバイスへのアクセスが制限される点や、しばしば優先度の低いファームウェアの更新が無視されがちであり、これが困難を増幅させていることを指摘しています。最後に、回答者の54%が資産データベースの正確性向上に向けた取り組みを重要視していると述べています。正確で最新の資産インベントリを確保することが不可欠です。特に、デバイスが各地に分散しているハイブリッドな働き方環境ではより重要となります。

## フルディスク暗号化はデータ保護の全てではなく一部

フルディスク暗号化は、単独の解決策ではなく、より広範なマルチレイヤーのセキュリティ戦略の一部と見なされています。これはデジタル化が進むリモート中心の時代におけるデータ保護の複雑さを表しています（図6を参照）。

- **フルディスク暗号化はデータ保護のための重要な対策。**半数以上の回答者(54%)が、フルディスク暗号化がエンドポイントに対して重要な保護を提供すると考えています。ただし、補足的なセキュリティ対策が必要であるとも強調しています。これは、暗号化がセキュリティの武器の中でも強力なツールである一方で、それだけに頼るべきではないことを示しています。回答者の28%がフルディスク暗号化による保護は限定的だとし、追加対策の必要性を主張しています。つまり、暗号化だけにとどまらない、より包括的なデータ保護戦略の必要性があるということです。基本的なセキュリティ機能（例：暗号化やパスワード設定など）は常に重要なエンドポイント管理機能でしたが、現在多くのベンダーは、より高度なエンドポイントセキュリティ技術を自社のポートフォリオに追加しています。[4]

> EMEA地域の中小企業の回答者の30%が、フルディスク暗号化によって十分に保護されているため追加対策が不要だと述べました。一方、北米地域の回答者のうち、同様の意見は12%にとどまりました。

- **厄介なマルウェア感染。**リモートワークの浸透に伴い、回答者の36%がマルウェア感染への懸念が中程度から大幅に増加したと報告しています。これはリモートエンドポイントが悪意のある活動の標的となり、脅威が増大している状況を示しています。
- **リモートにおける不十分なネットワークセキュリティ。**同様に、回答者の36%が、リモート地点における不十分なネットワークセキュリティに関する懸念が大幅または中程度に増加したと述べました。これはリモートワークの現実を反映しており、ネットワーク環境が社内インフラストラクチャよりも安全性が

低くなることで、データ漏洩の可能性が高まります。そのため、より効率的なエンドポイントソフトウェアの追跡と管理を実装することで、この課題に対処しています (48%)。

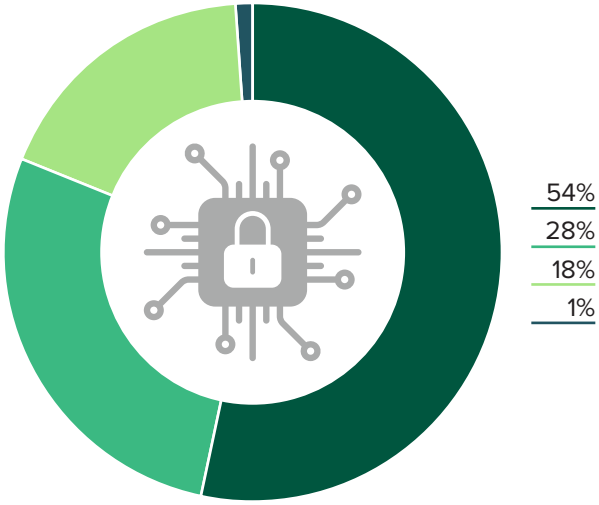
**55%**

の回答者が、デバイスのバックアップとリストアの機能があったことが、自社のノートパソコンを管理するのに役立ったと述べています。

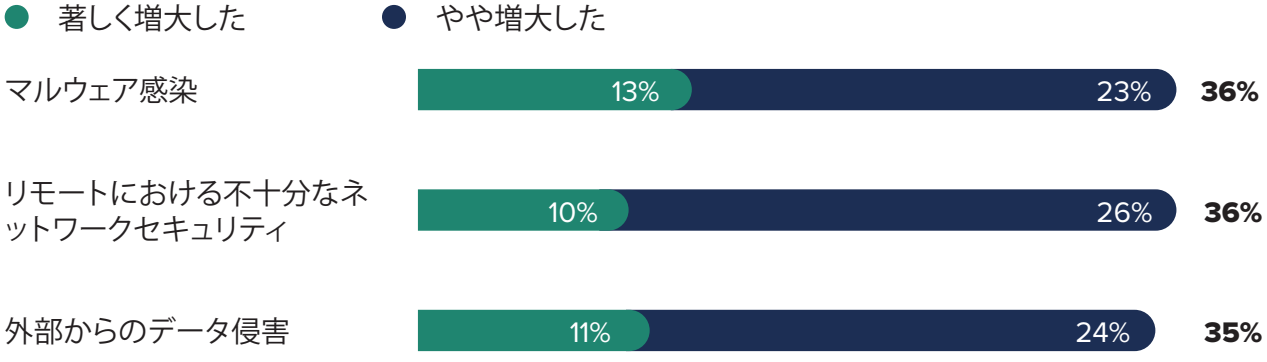
**図 6**

### 「フルディスク暗号化は、どの程度エンドポイントのデータを保護していると思いますか？」*

- 大部分は保護しているが、追加対策が必要。
- 保護は限定的なため、追加対策が必要。
- 大部分を保護しているため、追加対策は不要。
- 全く保護されていない。




### 「リモートワークによって、エンドポイントデバイス管理における以下のリスクはどう変化しましたか？」**




調査対象：500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
*注：四捨五入のため、パーセンテージの合計は個々の数値を加算したものと一致しない場合があります。
**注： 上位3回答を表示
出典：HP委託によるForrester Consulting調査（2023年9月）

## ITリーダーに新たに求められるものはエンドポイントセキュリティと効率性への投資

リモートワークの増加に伴い、エンドポイントのセキュリティと管理は、組織の業務効率とレジリエンスにおいて重要になっています。データから明らかなのは、エンドポイントセキュリティの先進的なソリューションへの投資とリモートエンドポイント管理の強化の必要性について、ITリーダーの間で意見が一致しているということです（図7を参照）。

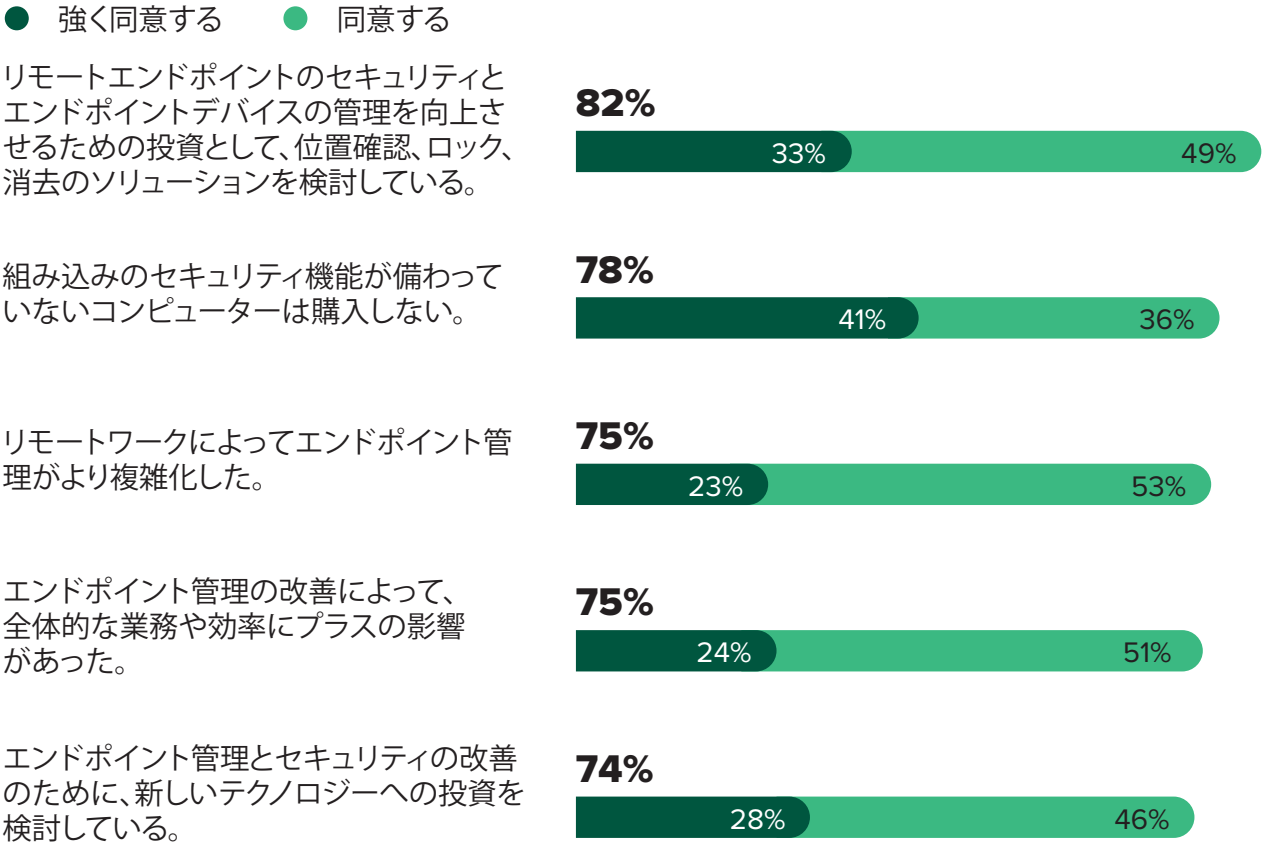
- **切り札となるのは、常時接続されたフリート管理ソリューション。**今日の世界では、リモートワークが今まで以上に普及している中、企業ネットワークに接続するデバイスであるエンドポイントのセキュリティの重要性は過小評価できません。ノートパソコンや携帯電話などのエンドポイントデバイスは、保護された組織環境の外で動作しているため、侵害のリスクが高くなります。回答者の大半 (82%) が、自身の組織ではリモートエンドポイントのセキュリティと管理を向上させるための投資として、位置確認、ロック、消去のソリューションを検討していると述べています。これは、リモートワークがもたらす複雑な課題に対処するためのソリューションが、いかに重要であるか認識されていることを示しています。
- **業務効率において二重の役割を果たすエンドポイントのセキュリティと管理。**データから明らかになったのは、回答者のうち75%が、効率的なエンドポイント管理が全体的な業務を向上させるということに「強く同意する」(24%) あるいは「同意する」(51%) と回答したことです。さらに、74%が最先端の技術を活用することで、エンドポイントの監視と保護を強化できると考えていました。簡単に言えば、効率的で安全なコンピューターシステムが、強固なセキュリティ対策の基盤となることが認識されています。
- **最初から組み込まれたセキュリティ**。回答者の77%が、新しいコンピューターを取得する際の優先事項に、堅牢なセキュリティ機能が組み込まれていることを挙げています。このデータは、多くの組織が基本的なセキュリティを調達の決定において譲れないものと考えており、ハイブリッドやリモートワークの安全な環境を作る上で不可欠であることを示しています。それ以外の

改善すべきエリアには、デバイスの復旧プロセスの自動化 (47%)、BIOSの更新デプロイとデバイスの位置追跡（どちらも46%）が含まれており、ノートパソコン管理の多面的なニーズを反映しています。

回答者のうち63%は、リモートエンドポイントの保護において、ハードウェアによる強制的なロックと消去のソリューションを最優先に挙げています。それに対して、定期的なソフトウェアの更新とパッチ適用は49%にとどまり、エンドポイントのバックアップソリューションは47%で使用されていますが、主要な選択肢に大きく後れを取っています。

**図7**

**「以下の記述にどの程度同意しますか？」**




調査対象：500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
注：四捨五入のため、パーセンテージの合計は個々の数値を加算したものと一致しない場合があります。
出典：HP委託によるForrester Consulting調査（2023年9月）

## 常時接続されたフリート管理は保護の強化と生産性向上を促進

今日のデジタル環境におけるデータ主導型業務の本質は、堅牢なデータ保護メカニズムの重要性を強調しています。常時接続型のフリート管理ソリューションや、位置確認・ロック・消去ソリューションの採用は、特にリモートワークやハイブリッドモデルを採用している組織にとって、多くの利点があります。これらの利点は、調査結果で明らかになっているように、データ保護、生産性、規制遵守などに大きく貢献すると期待されています（図8を参照）。

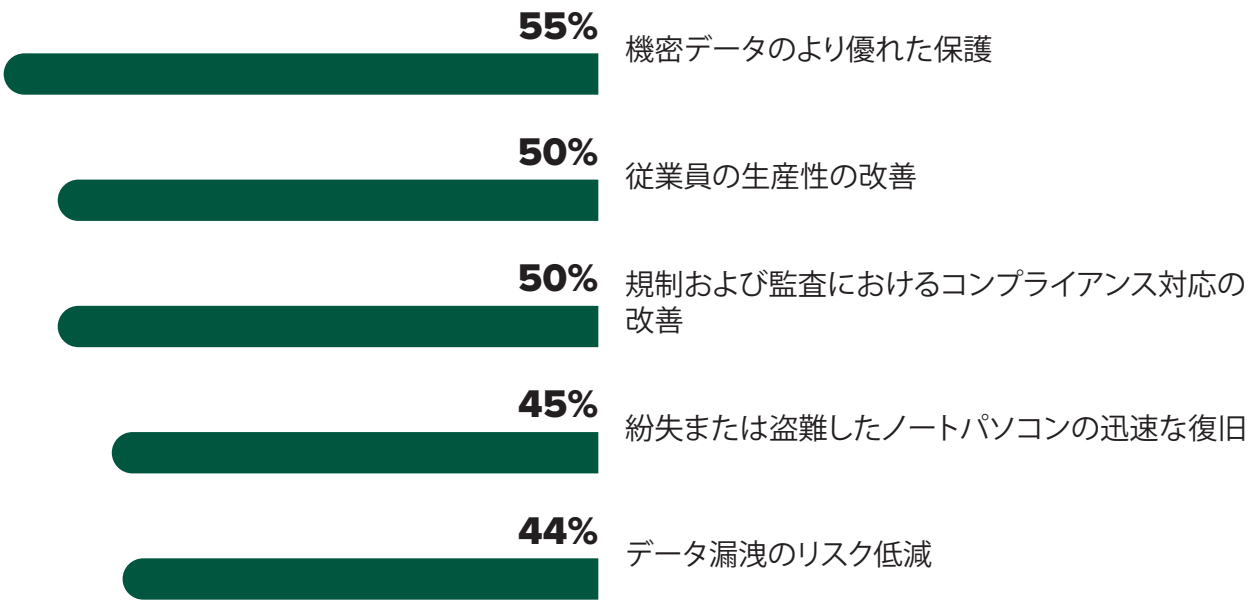
- **データ保護の強化。**55%の回答者が、位置確認・ロック・消去ソリューションの主な利点として、機密データのより優れた保護を挙げていることから、これがいかに重要であるかは明らかです。組織が自社の機密データの保護を重視しているだけでなく、既存のシステムにある潜在的な脆弱性を認識していることも示されています。
- **従業員の生産性向上。**組織は、生産性を確保しつつセキュリティを強化する最適な方法を常に模索しています。位置確認・ロック・消去ソリューションを統合することが、今日抱える課題の多くを解決する糸口であるように見受けられます。特に、回答者の50%が従業員の大幅な生産性向上につながることを期待しています。エンドポイント管理が単なるセキュリティ強化以上の役割を果たし、デバイスをスムーズに使えるようにしダウンタイムを減少させることで、ビジネスの業務効率を高めるとされています。

> ドイツの中小企業 (SMB) の回答者は、他国よりも、紛失または盗難したデバイスの位置確認・ロック・消去ソリューションの導入 (80%) や、データセキュリティや資産追跡に関連する改善された監査コントロールの導入 (50%) をより重視すると述べています。

- **コンプライアンスのサポート。**50%の回答者が、規制や監査の管理をもう1つの利点として挙げています。これは、このソリューションが、複雑な規制への遵守を進めることを可能にし、潜在的な法的・財政的影響を軽減するという極めて重要な役割を果たしていることを明らかにするものです。

**図8**

**「位置確認・ロック・消去ソリューションの使用により、どのような恩恵を受けましたか、または期待しますか?」**




調査対象:500人以上の従業員を雇用する複数業界の企業のITおよびセキュリティの意思決定者312人
注: 上位 5回答を表示
出典:HP委託によるForrester Consulting調査 (2023年9月)

## 主な推奨事項

組織はリモートやハイブリッドな働き方に移行しており、分散した環境での生産性とセキュリティを確保するために、エンドポイント管理の強化を必要としています。しかし、多くの場合、ファームウェアの更新が遅れることで、セキュリティ侵害や業務上のトラブルのリスクが生じます。資産データベースの維持は、特に規制の圧力下では困難です。それに伴い、常時接続されたエンドポイント管理戦略は、特に厳格なデータプライバシー規範がある地域で重要性を増しています。サイバー脅威が増大する中、ITリーダーはデータの安全性や業務の堅牢さを確保するための重要な投資と見なしています。本調査の結果、以下の重要な推奨事項が明らかになりました。

**リモートワークの導入には計画的な変更が必要。**

組織は2020年にリモートワークに追い込まれ、現在ではハイブリッドワークが浸透する中でエンドポイント管理やセキュリティ機能に苦戦しています。この新しいモデルに対応するためにその場しのぎの調整を行うのではなく、ITとセキュリティのための計画を立て、組織の資産を効果的に管理し保護できるよう取り組み、ベンダーと連携して計画的に対応する必要があります。適切な計画でパフォーマンスの低下を防ぐことができるのです。

**ライフサイクル管理を組み込むべき現代の資産管理。**

組織のエンドポイントやユーザーが決まった場所にいなくなった状況において、資産管理プラットフォームではエンドポイントの配布、継続的なメンテナンス、および復旧を考慮する必要があります。エンドポイントの管理における統合が重要であり、それによってエンドポイントがハードウェアからアプリケーションまで適切に管理され、最終的に廃棄される際にも組織がその過程全体を監査できることで、コンプライアンス要件を満たすことができます。

## 従業員満足度向上につながる常時接続されたエンドポイント管理プラットフォームの活用。

現代のエンドポイントのハードウェア、OS、アプリケーション、およびデータの管理には、エンドポイントがある場所やユーザーがサポートを必要とする時間を問わず、ITやセキュリティのオペレーションにアクセスできるツールが必要です。デバイスをオフィスに送り返してメンテナンスを行うことは、ユーザーの生産性やデジタル体験を低下させます。ITやセキュリティの管理者 にとって、連携していない使い勝手の悪いツールではタスクの実行が困難になります。ユーザーがニーズに時間や場所を問わず業務に対応できるよう、より効率的な管理アプローチができるベンダーの採用が不可欠です。

## 位置情報を組み込んだエンドポイントのセキュリティアプローチ。

組織のアプリケーションとデータを適切に保護するには、組織のリソースにアクセスする際に、資産（デバイス）の位置情報を把握する必要があります。普段はロサンゼルスの自宅から作業しているユーザーが、突然フロリダ州オーランドからアカウントにログインしようとしたら、貴組織のエンドポイントセキュリティのプラットフォームは異常検知しますか？これが脅威なのか、それとも単にユーザーが休暇中なのかを確認するためのツールが整っていますか？必要に応じてチームが特定のノートパソコンを見つけて遠隔で制御し、企業データが漏洩するのを防ぐことができますか？リモートワーク環境では、ユーザーや作業デバイスの特定だけでなく作業場所も特定し、アクセス方法が承認されているかどうかも確認できるセキュリティツールが必要です。

## 付録A：調査方法

本調査では、Forresterが産業を問わず、北米、欧州、中東、アフリカ、アジア太平洋地域において500人以上の従業員を雇用する企業のITおよびセキュリティの意思決定者312人を対象にオンライン調査を実施し、ノートパソコンやその他の孤立したデバイス効率的な管理と維持について調べました。本調査の目的は、資産管理とデータセキュリティの過程の不備が従業員体験(EX)、業務効率、およびリスク管理に与える影響を探ることです。参加者への質問内容として、エンドポイント管理の現状、それに伴う課題、そして将来の可能性について尋ねました。調査は2023年3月に開始し、2023年9月に終了しました。

## 付録B：調査対象者の内訳

| 国 | |
|---|---|
| 米国 | **33%** |
| 英国 | **14%** |
| オーストラリア | **14%** |
| フランス | **10%** |
| ニュージーランド | **10%** |
| ドイツ | **10%** |
| 日本 | **9%** |

| 地域 | |
|---|---|
| 欧州・中東・アフリカ | **34%** |
| 北米 | **33%** |
| アジア太平洋地域 | **33%** |

| 部門 | |
|---|---|
| IT業務担当 | **50%** |
| ITセキュリティ担当 | **50%** |

| 職責レベル | |
|---|---|
| エンドポイント管理の最終意思決定者 | **38%** |
| エンドポイント管理の意思決定チームの一員 | **32%** |
| エンドポイント管理に関連する意思決定に影響力を持つ立場 | **30%** |

| 従業員数 | |
|---|---|
| 従業員 500～999人 | **25%** |
| 従業員 1,000～4,999 人 | **29%** |
| 従業員 5,000～19,999 人 | **26%** |
| 従業員 20,000 人以上 | **20%** |

## 付録B：調査対象者の内訳（続き）

| 業界 | |
|---|---|
| 製造・材料 | **15%** |
| テクノロジー | **15%** |
| 小売 | **10%** |
| CPG（消費財） | **6%** |
| コンシューマサービス | **6%** |
| ヘルスケア | **6%** |
| 金融サービス | **6%** |
| ビジネス／プロフェッショナルサービス | **5%** |
| エネルギー／公益事業 | **5%** |
| 建設 | **4%** |
| 運輸・物流 | **3%** |
| その他 | **19%** |

| 役職 | |
|---|---|
| ディレクター (45%) | **45%** |
| マネージャー (44%) | **44%** |
| 常勤実務者 (12%) | **12%** |

注：四捨五入を用いているため、パーセントの合計が100% にならない場合があります。

## 付録C：注釈

[1] 出典：“The State Of Endpoint Security, 2022” Forrester Research, Inc. 2022年7月21日

[2] 出典：Forrester Analytics Business Technographics® Infrastructure Survey 2021年

[3] 出典：“The Future Of Endpoint Management” Forrester Research, Inc. 2022年6月6日

[4] Ibid.


FORRESTER®