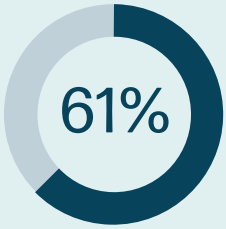
新しい時代：ハイブリッドワーカーのためのセキュリティ

HP WOLF SECURITY レポート

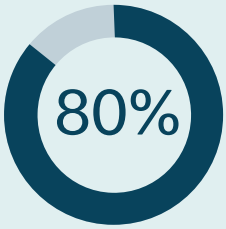
エグゼクティブサマリー

多くの組織がハイブリッドワークの青写真を描いた今、これまでの歩みを振り返り、課題を評価し、その先にあるチャンスに対処するときが来ました。

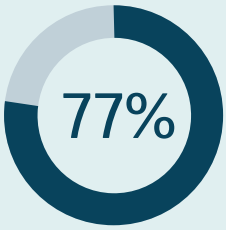
米国、英国、フランス、ドイツ、日本のITリーダー984人への調査結果に基づく。



が来年はハイブリッド従業員の保護がさらに難しくなると回答しています。[i]



がハイブリッドワーカーに対応するために、サイバーセキュリティ戦略全体に変更を加えています。[i]



がハイブリッド従業員のエンドポイント数が増加するにつれて、サイバー攻撃が加速することを認めています。[i]

本レポートでは、データに基づいてITリーダーが次に何をすべきかを議論しています。このレポートがハイブリッドワーカーの新たな要求を理解し、断固とした行動を起こすために役立つことを願っています。

より良いハイブリッドセキュリティに向けて

セクション01

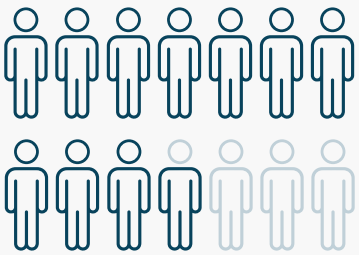
ハイブリッド従業員のセキュリティ向上は、社内と社外のリスクを十分に理解することから始まります。圧倒的に多いのは、オフィス外ワーカーとそのデバイスに関するものです。

本調査の回答者は、自社のセキュリティ体制にギャップがあることを認識しています。実際、ITリーダーは、常時オフィスにいる従業員（73%）と比較して、ハイブリッド従業員（82%）に対してギャップを感じているようです。[i]

調査では、ITリーダーが共通して取り組むべきと考えている2つの大きな課題が浮かび上がりました。

1. デバイスとソフトウェアの急増

77%

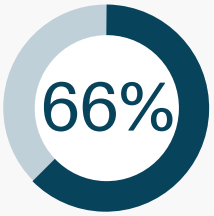


がエンドポイントの数が増えるにつれ、サイバー攻撃が加速するという事に同意しています。[i]

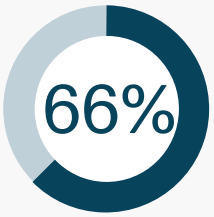
7 in 10

がハイブリッドワークでは、従業員が仕事用のデバイスを紛失したり、盗まれたりするリスクが高まるという事に同意しています。[i]

2. 企業ネットワークの外で働く従業員



が最大のサイバーセキュリティの弱点は、ハイブリッド従業員が危険にさらされる可能性という事に同意しています。[i]



がハイブリッド従業員の行動に合わせて脅威検知対策（EDRやSIEMツールなど）をアップデートすることは容易ではないと回答しています。[i]

リーダーは、まだすべての答えを持っていないにしても、デバイスとユーザーの働く場所に関するハイブリッドワークの現実を受け入れています。エンドポイントが攻撃に対して脆弱であること、企業ネットワークの外にいるハイブリッドワーカーが攻撃者による侵入の弱点となり得ることを知っています。

「ハイブリッドワーカーにリスクと責任について教育することは重要ですが、エンドポイントセキュリティに関しても同様です。マイクロ仮想化のような技術は、その良い例です。これにより、リンクや添付ファイルを開くといった潜在的にリスクのある作業を他のシステムから分離し、攻撃者が重要なデータにアクセスできないようにします」

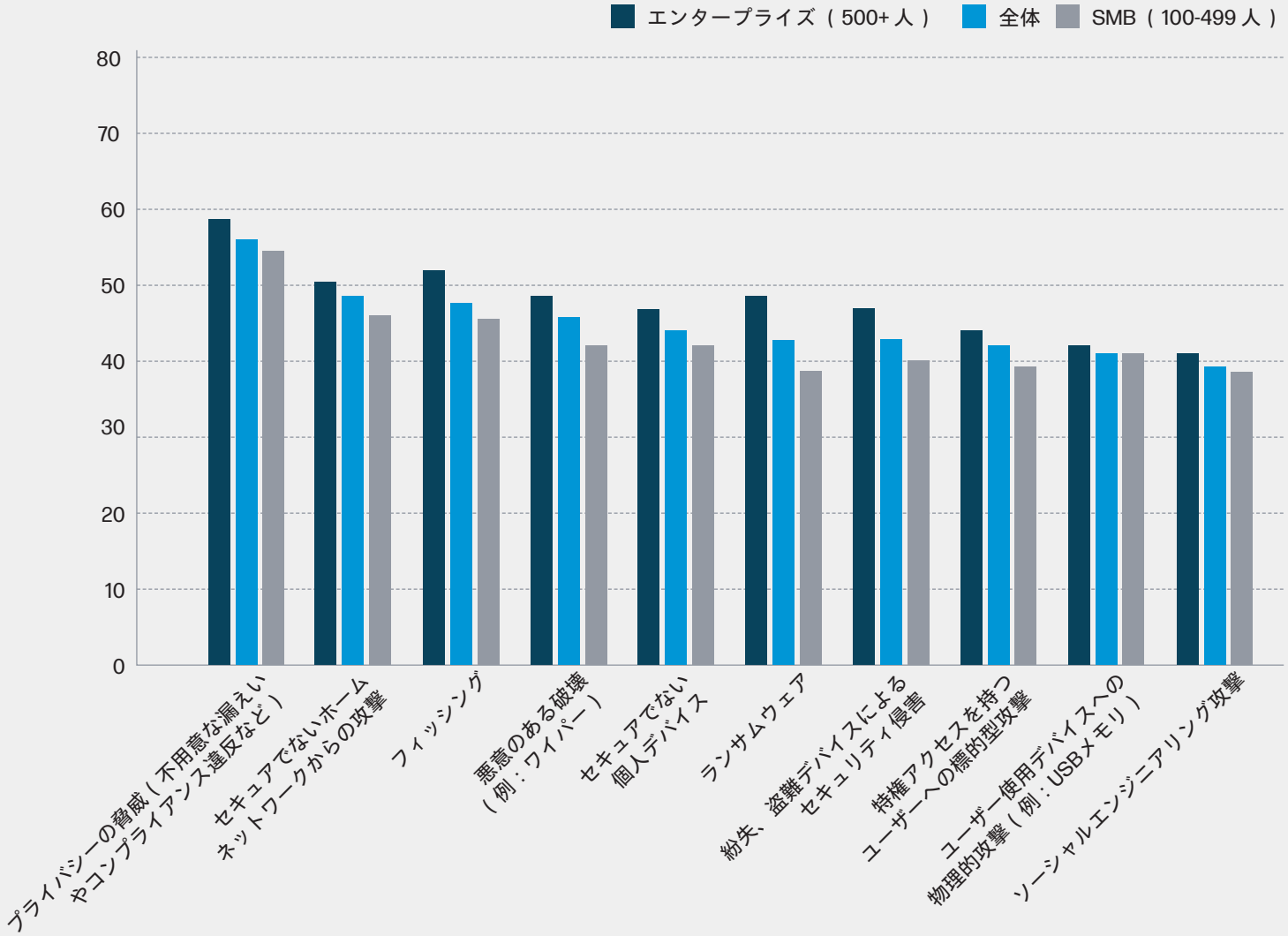
Dr. イアン・プラット（Ian Pratt）
HPパーソナルシステムズ事業セキュリティ部門
グローバル責任者、HP Inc

多様な脅威、
共通した一つのターゲット

リーダーは組織の課題を認識すると同時に、外部からの幅広いセキュリティの脅威を認識しています。そして最も差し迫った脅威のほとんどが、何らかの形で従業員のデバイスをターゲットにしています。

セキュリティ全体について考え、懸念材料として最も多く選ばれた脅威は以下の通りでした。上位10個のうち9個がエンドポイントに関連するものです。

回答者が現在懸念しているセキュリティ脅威上位10[i]



エンドポイントの重要性

ITリーダーが現在のエンドポイントの脅威を継続的な、そしてまさに今増大しているリスクとみなしていることは明らかです。リーダーが現在懸念しているエンドポイントに焦点を当てた脅威と同じものが、今後12ヶ月間にハイブリッドワーカーにとって増加すると予想される脅威の中でも上位にランクされています。最も多く挙げられているのは、フィッシング（33%）、ランサムウェア（28%）、従業員のセキュアでないホームネットワーク経由の攻撃（27%）です。[i]

攻撃の中心が物理的オフィスからエンドユーザー（彼らがどこにいようとも）に移っていることを考えると、いかなる防御ソリューションもここ焦点を当てる必要があります。本レポートの後編では、ハイブリッドセキュリティのニーズに対応するために、企業が選択しているツールについて紹介します。

「ゼロトラストは我々のお客様にとって最もホットな話題の一つです。ある大手金融機関は、『社内ネットワークを完全になくしたい』と考えています。そのため、我々はネットワークアクセスの制限よりも、セキュリティとハイブリッドワーカーの自由を両立することが可能な新しいアーキテクチャーに焦点を当てています」

アレックス・サッチャー（Alex Thatcher）
クラウドクライアント担当ディレクター、HP Inc

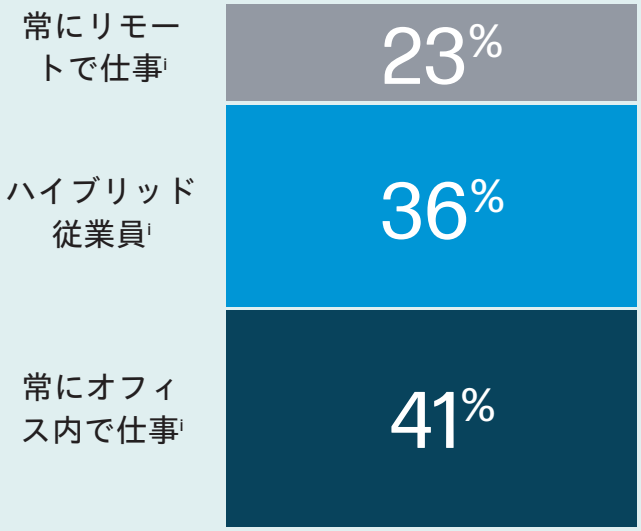
ハイブリッドワーカーを攻撃ポイントで保護する

セクション 02

ITチームはすでにハイブリッドワークフォースのサポートに成功しています。明日のハイブリッド環境に対する脅威を防御するために、どのようなテクノロジーを導入しているのでしょうか？

過去3年間で、ITチームは 生産性が高く、安全で、分散したワークフォースの実現に成功しました。ハイブリッドワークは多くの組織で定着し、社員はハイブリッドワークがもたらす可能性に熱狂しています。しかし、最も困難な仕事はまだ先にあるのかもしれません。

平均的ワークフォース比率（推定）
（PCユーザー）



85% の従業員がオフィスで働くことに満足しているが、週に2回くらいは自宅で働きたいと考えている。[ii]

67% が家でこんなに生産性が上がるとは思っていなかったと言っている。[iii]

実施された取組み

ハイブリッドワークの初期導入が成功した今、IT部門のフォーカスは増大するハイブリッドワークフォースを保護するために、より多くのリソースを割き、異なる戦術を展開することに移っています。

- 82%がハイブリッドワーカー向けのサイバーセキュリティ予算をすでに増やしていると回答。[i]
- 71%が2023年はセキュリティ予算全体が増加すると予想。[i]
- 81%がハイブリッド従業員を保護するために、異なるツールやポリシーを導入。[iv]
- 80%がハイブリッド従業員に対応するために、サイバーセキュリティ戦略全体を変更。[iv]
- 70%が侵害のリスクを最小限に抑えるために、リモートワーカーが社内ネットワークにアクセスすることを制限。[iv]

保護への投資はすでに成果を上げています。昨年と比較して、ITリーダーの77% が、ハイブリッド従業員がセキュリティの脅威から自分自身を守り、より良い仕事をしているということに同意しています。

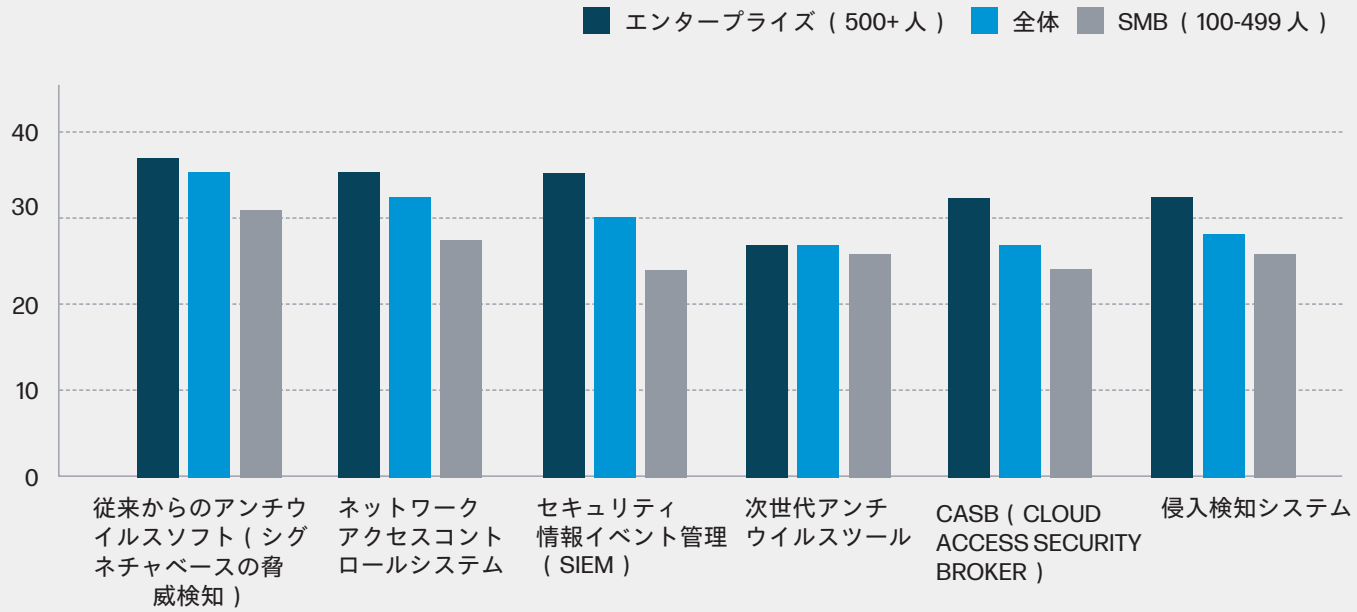
しかし、ITリーダーは認識している課題を考慮し、その多くはハイブリッド社員を保護するためにさらなる対策を取っています。

正しいツールの導入

ハイブリッドワークにおいてテクノロジーは鍵となるイネーブラーで、攻撃ベクターや防御戦術としても中心的な役割を担います。従業員の分散化が進む中、多くの攻撃が行われるエンドポイントを保護することが主要な防御戦術となります。

このことは、ITリーダーも認識しています。ITリーダーの3分の2（66%）は、ハイブリッドワーカーが危険にさらされる可能性を最大のセキュリティ上の弱点と見なしており、その多くがエンドポイントを介した潜在的な侵害の防止と修復に取り組んでいるのは不思議ではありません。

異なる規模の組織におけるサイバーセキュリティツールの利用状況[i]



ハイブリットワークを守るテクノロジー

以下のテクノロジーはセキュリティチームの間で普及し始めているものです。本調査により、ITチームはこれらの技術についてもっと深く知りたいと考えており、将来的に導入するつもりであることがわかりました。

エンドポイント

ネットワークに接続されたリモートコンピューティングデバイスで、一般的にはユーザーまたは環境とのインタラクションに使用されます。（例：PC、プリンター、スマートフォン、IoTデバイス）

EDR（ENDPOINT DETECTION AND RESPONSE）

ユーザーデバイス（PC、ノートPC、モバイルなど）のシステム動作を監視し、疑わしい行動を検知した際にアラートを発するテクノロジーです。また、EDRソリューションは脅威を封じ込め、ITチームが適切に対応するための支援を行います。

CASB（CLOUD ACCESS SECURITY BROKER）

クラウドサービスは、今日のハイブリッド組織に不可欠です。CASBは、ITチームがクラウドリソースへのアクセスを管理・制御することを容易にします。不正あるいは悪意のあるユーザーへのアクセスを制限しながら必要なサービスを提供することにより、ITチームは従業員のクラウドリソースへのアクセスを簡素化することができます。

アプリケーション隔離

アプリケーション隔離は、リスクの高いアクティビティを使い捨ての仮想コンテナ内に隔離することで、既知および未知の脅威からエンドポイントを保護します。

例えば、Eメールの添付ファイルやWebリンク、ブラウザのダウンロードに含まれる悪意のあるコンテンツに「うっかり」にアクセスしようとするユーザーを保護することに有効です。

次世代アンチウイルス

従来のアンチウイルスソフトは、シグネチャに依存して既知のマルウェアを検知し検疫していました。 次世代アンチウイルスは、AIと機械学習を使用して、エンドポイント上の正常な動作を識別して脅威を阻止します。

ファイル整合性監視（FIM）

FIMは、組織の重要なファイル、システム、データベース、アプリケーションをスキャンし、攻撃の兆候となりうる改変が行われていないかどうかをチェックします。 予期せぬ改変を検知した場合、ITチームにアラートを発し調査をできるようにします。

セキュリティ情報イベント管理（SIEM）

SIEMソリューションにより、セキュリティチームはさまざまなソースからデータを収集し、セキュリティ上の脅威を分析することができます。また、情報やイベントの詳細なログを持つことで、セキュリティ管理（リソースの割り当て先の把握）やコンプライアンスの実証に役立てることができます。

前ページの技術の多くはすでによく知られ広く普及しているものですが、特に隔離技術は、回答者のハイブリッドワーカー防御の重要な部分を占めるものとして、調査の中で何度も話題に上っていました。

これらのツールは、デバイス、アプリケーション、特定のタスク（Eメールやワープロなど）をITインフラの他の部分から分離することによって、組織のレジリエンスを向上させます。そして、IT リーダーにとっての重要性が増しています。

現在、23%が未知の、潜在的に有害なドキュメントやリンクを扱うためにアプリケーション隔離を利用しています。また、32%は今後12ヶ月の間に隔離技術を導入する意向で、76%はハイブリッドワーク中のデバイスを保護する上で重要な役割を果たすと考えています。[i]

「見えない」ソリューションが期待に応える

調査によると、従業員はセキュリティ対策が邪魔になると拒否することがあるため、ITチームが導入する保護策は、エンドユーザーにとってできるだけ透明性の高いものであるべきです。当社の調査によると、調査対象となったオフィスワーカーの37%が、セキュリティポリシーや技術が厳格すぎると回答し、48%がセキュリティ対策は多くの時間を浪費することになると考えています。[v]

「セキュリティのより良い実践（ベストプラクティス）を従業員が理解することは重要ですが、それ以上に重要なのは、ユーザーが考える必要のない組み込まれた防御策です。セキュリティが生産性を阻害する場合、従業員はそれを回避しようとすることが分かっています。したがって、ユーザーにとって防御策の透明性が高いほど、より成功し企業の防御力はより強固になります」

ロバート・マッセ（Robert Masse）氏
HPセキュリティアドバイザリーボードメンバー、
Deloitteのパートナー

レポート寄稿者

アレックス・サッチャー（Alex Thatcher）
クラウドクライアント担当ディレクター、HP Inc

Dr. イアン・プラット（Ian Pratt）
HPパーソナルシステムズ事業セキュリティ部門グローバル責任者、HP Inc

ロバート・マッセ（Robert Masse）氏
HPセキュリティアドバイザリーボードメンバー、 Deloitteのパートナー

HP Wolf Securityについて

HP Wolf Securityはハードウェアで強化されたセキュリティとエンドポイントに特化したセキュリティサービスによるHPのポートフォリオの一部で、組織がサイバー犯罪者からPC、プリンター、そして人々を保護できるように設計されています。

HP Wolf Securityは、ハードウェアレベルから始まり、ソフトウェアやサービスに至る、包括的なエンドポイント保護とレジリエンスを提供します。https://jp.ext.hp.com/business-solution/wolf/をご覧ください。

メソドロジー

[i]HPは2022年7月から8月にかけて5つの市場（米国、英国、フランス、ドイツ、日本）において、従業員数100人から2,499人のハイブリッド組織のITリーダー984人を対象に調査を行いました。

回答者の80%はディレクタークラス以上（VPおよびC-suite）です。全員がエンドポイント、ネットワーク、クラウドあるいはプライバシー管理の意思決定者であり、組織内でサイバーセキュリティ運用チームやITのハードウェアとソフトウェアを監督しています。

ハイブリッド組織とは、オフィスで働く従業員、リモートで働く従業員、あるいはその両方が混在するさまざまな従業員を持つ組織と定義されます。

リファレンス

[ii]HP、英国と米国、エンドユーザー調査 n=200、2021年7月

[iii]HP、英国と米国、 n=537 米国と英国のエンドユーザー、2020年9月

[iv]ハイブリッドワーカーの保護に関する記述に「強くそう思う」「そう思う」と回答した人の%に基づく。

[v]HP Wolf Security (2021)「Rebellions & Rejections（IT部門と従業員の確執）」[オンライン] https://jp.ext.hp.com/blog/security/product/hp-wolf-security-rebellions-and-rejections-report/

HP Wolf Security for BusinessはWindows 10または11 Pro以上が必要で、HPのさまざまなセキュリティ機能を含み、HP Pro、Elite、RPOS、Workstation製品で利用可能です。含まれるセキュリティ機能については、製品詳細をご覧ください。