HP WOLF SECURITY

OUT OF SIGHT & OUT OF MIND REPORT

目の届かないところで軽視されるセキュリティ

HP WOLF SECURITY

エグゼクティブサマリー

近年、職場ではハイブリッドな働き方の波が到来しています。デジタルトランスフォーメーションと職場の変革が加速し、働き方は一変しました。従業員は今後ますます分散化し、IT部門とセキュリティ部門は従業員のIT環境を把握することが難しくなっていくでしょう。また、米国では2027年までに全労働人口の50%がフリーランスで占められる状況に達することが予想されています。このような状況から、IT部門によるITエコシステムの展開、管理、保護がかつてないほど困難になっています。

これは組織にとっての新たな現実で、変化に適応し、進化していくほかなくなっています。

大規模な変革には調整期間が必要です。しかし、これほどの変化が急激に進む場合には、解決が難しい問題が伴うことも往々にしてあります。多くの組織は、こうした大規模な働き方の変化に対応する準備ができていませんでした。ユーザーにセキュアなデバイスを提供することから脅威のトリアージまで、ITセキュリティのサポートをリモートで提供する際の時間と複雑さが大きな課題となっています。

サイバー犯罪者は、この混乱をいち早く利用しています。彼らは分散する従業員を頻繁に標的にし、より多くのデバイスを危険にさらし、より多くのアラートを引き起こしています。さらに犯罪者は、組織の可視性が低下しているという、身を潜めるのに好都合な状況を悪用しています。さらに、企業が後れを取らないよう苦戦している状況にも乗じています。

本レポート「HP Wolf Security: Out of Sight & Out of Mind ~ 目の届かないところで軽視されるセキュリティ」では、新型コロナウイルス感染症のパンデミック期間中に在宅勤務に移行したオフィスワーカー8,443人を対象にYouGovがオンラインで実施したグローバル調査と、IT部門の意思決定者（ITDM）1,100人を対象に実施したグローバル調査からデータを収集しました。本レポートは、最近の働き方の変革がどのようにユーザーの行動に変化をもたらし、ITセキュリティの管理に影響を及ぼしているかを検証しています。

今回のHP Wolf Securityレポートでは、以下の点について考察します。

- **新たなシャドーIT：**
  在宅勤務が増えてから、ユーザーはIT部門を蚊帳の外に置くようになっています。セキュリティを考慮せずに、未承認のIT機器を購入して設置し、使用しています。また、有害かもしれないリンクをクリックしても、IT部門に報告していません。

- **攻撃者の侵入：**
  攻撃者の侵入リスクが高まっています。IT部門によると、従業員が悪意のある添付ファイルを開くことが増えており、その結果として侵害されたデバイスの再インストール率が上昇しています。これは氷山の一角にすぎず、気づかないうちに侵害されたデバイスは報告されている数よりも多い可能性があります。

- **差し迫った事態：**
  これらの問題が相まって、ITのセットアップやサポートのコストが増加し、複雑化しています。脅威のトリアージから、新規の従業員へのセキュアなデバイスの準備や設定、再インストールやパッチの適用まで、ITセキュリティはますます複雑さを増す傾向にあります。それによって、企業内の情報セキュリティ対策がかつてないほど困難になっています。

「HP WOLF SECURITY」の視点：

HP INC.
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
イアン・プラット（IAN PRATT）

「本レポートで、企業が現在直面している厳しい現実が浮き彫りになりました。脅威アクターは、ますます巧みにエンドポイントの防御をすり抜けています。ユーザーは自律的に行動し、IT部門が把握していないツールを導入しています。また、従業員は何を信頼してよいのか分からなくなっています。

これらの課題の多くはパンデミックが発生するずっと前から存在していましたが、ハイブリッドな働き方の急増による行動の構造的な変化によって、問題が深刻化しています。もうこれまでと同様の対応を続けることはできません。ITとセキュリティの進化が求められています。既知と未知の脅威から保護するだけでなく、サイバーセキュリティ部門とユーザーの負担を減らしつつリモートでの働き方が可能になる、新しいセキュリティアーキテクチャが必要です。」

主な統計データ

在宅勤務者を対象としたYouGovの調査で、以下のことが明らかになりました。

68%	在宅勤務のためにデバイスを購入した人の68%が、セキュリティは重要な検討事項ではなかったと回答しています。
43%	購入したデスクトップPCやノートPCの確認やインストールをIT部門にしてもらわなかったと回答しています。
49%	18歳から24歳の回答者の49%が、在宅勤務を始めてから悪意のあるメールをクリックする回数が増えたと回答しています。
70%	疑わしいリンクをクリックした回答者の70%が、IT部門に報告していませんでした。

ITDMを対象としたTolunaの調査で、以下のことが明らかになりました。

74%	**74%**が、悪意のあるリンクをクリックしたり添付ファイルを開いたりする従業員が増加したと回答しています。
79%	**79%**が、再インストール率が上昇したと回答しています。
77%	**77%**が、アラートのトリアージに要する時間が増加していると回答しています。
62%	エンドポイントに関連するアラートの**62%**が誤検知です。

新たなシャドーITは、ユーザーがIT部門から見えなくなるにつれて出現

世界中の従業員のうち70%がパンデミック後も柔軟な働き方を継続できる選択肢を希望しており、10社中9社の企業が今後もリモートワークとオフィス勤務を組み合わせる予定であることが調査結果で示されています。それに伴い、仕事の様相が変化しています。従業員はホームオフィスを整え、一日の内、さまざまな時間に仕事をできる働き方に移行しています。また、近くに意見を聞ける同僚がいない孤立した環境で仕事をしています。そうした状況がユーザーの行動の変化につながっており、IT部門とセキュリティ部門に新たな課題を生んでいます。

「シャドーIT」とは一般に、IT部門以外の部門（財務部門やマーケティング部門など）がIT部門の範囲外でソフトウェアを導入することを指します。クラウド、特にSaaS（Software-as-a-Service）の普及により、今ではどの部門も事業部の予算内で新しいソフトウェアをダウンロードして使用できるため、IT部門をすり抜けられるのです。この傾向はセキュリティ部門とIT部門にとって多くの悩みの種となっており、何が使用されているのか、また、そのサービスがデータセキュリティ、コンプライアンス、ガバナンスにどのような影響を及ぼし得るのかを把握しにくくなっています。

当社の調査で、「シャドーIT」がこれまで以上に広がっていることが明らかになりました。IT部門に確認もなく、個人がIT機器を購入し、それらのデバイスを使用して自社のネットワークに接続することが増えています。オフィスワーカーの45%が過去1年間で在宅勤務のために個人用のIT機器を購入しており、そのうち29%がデスクトップPCやノートPCを、16%がプリンターを購入していました（図1）。

図1：在宅勤務のためにIT機器を購入したオフィスワーカーの国別割合

	全体	カナダ	メキシコ	米国	ドイツ	英国	日本	オーストラリア
デスクトップPCまたはノートPC	29%	35%	45%	31%	21%	14%	20%	34%
プリンターまたは複合機	16%	19%	27%	17%	14%	8%	9%	18%
インターネットルーター	15%	16%	22%	18%	11%	4%	9%	19%
タブレット、iPad	11%	13%	19%	12%	10%	5%	6%	13%

新しいデバイスを購入したオフィスワーカーのうち、セキュリティを重視したと回答しているのはわずか32%です。この割合は、英国では16%に低下します（図2）。コストと機能がより重要と考えられており、機能を重視したと回答した割合は69%、コストを重視したと回答した割合は51%でした。さらに、購入したデスクトップPCやノートPCについては43%が、購入したプリンターについては50%が、IT部門に確認やインストールをしてもらっていませんでした（図3）。こういったデバイスが企業ネットワークへの不正アクセスの裏口として悪用される可能性を考えれば、これは憂慮すべき傾向です。

図2：オフィスワーカーが在宅勤務用に新たなデバイスを購入する際に重視した点

	全体	カナダ	メキシコ	米国	ドイツ	英国	日本	オーストラリア
コスト	51%	52%	47%	51%	45%	54%	52%	54%
機能	69%	64%	77%	70%	80%	62%	43%	69%
セキュリティ	32%	32%	33%	32%	33%	16%	37%	34%

IT部門の知らないところで、
個人がデバイスを購入し
企業ネットワークに接続しています。

HPの視点：

HP INC.
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
イアン・プラット（IAN PRATT）

「悪意のあるものをクリックしても気づかないユーザーが多いため、実際の件数は調査で明らかになった数字よりはるかに多い可能性があります。長期戦でラテラルムーブ（横展開）を行い、価値の高いインフラに侵入する方がもうかるため、脅威アクターは必ずしも不正アクセスを知らせてくるとは限りません。したがって、エンドポイントが侵害された場合は、攻撃者が実行できることを制限することが不可欠です。脅威を封じ込めれば、有害な影響を緩和できます。」

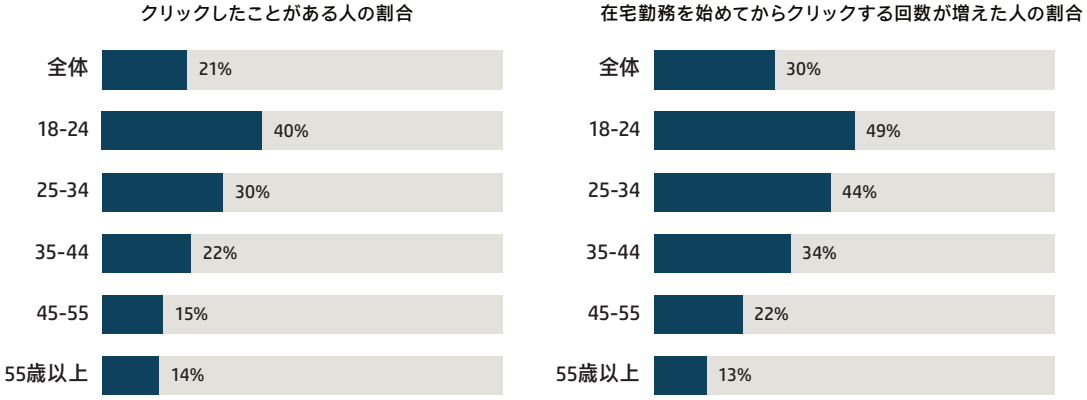
HP INC.
最高情報セキュリティ責任者
（CISO）
ジョアンナ・バーキー
（JOANNA BURKEY）

「分散化が進む中、クリックする前に何かおかしくないかと健全性を確認する普段の繋がりが減っています。教育は役に立つという程度でしかありません。従業員がインシデントを報告しやすく奨励する必要はありますが、自己報告のみに頼ることはできません。適切なレベルの可視性を実現できる多層型のセキュリティを確立することが重要です。」

図3：在宅勤務用の新たな機器を購入したオフィスワーカーのうち、IT部門により確認やインストールが行われたと回答した割合

また、調査結果は、従業員の警戒心が薄れている、またはクリックしても安全かどうか判断するのが難しくなっていることも示しています。オフィスワーカーの21%が、在宅勤務を始めてから悪意のあるリンクをクリックしたことがあると回答しており、そのうち30%が在宅勤務を始めてからそのようなことが増えたと回答しています（図4）。この割合は18歳から24歳の回答者で大幅に増加し、40%が悪意のあるメールをクリックしており、49%が在宅勤務を始めてからクリックした回数が増えています。これらは悪意のあるものをクリックしたと自覚している従業員だけの割合であり、多くはそのことに気づいていないため、実際の割合はさらに高い可能性があります。

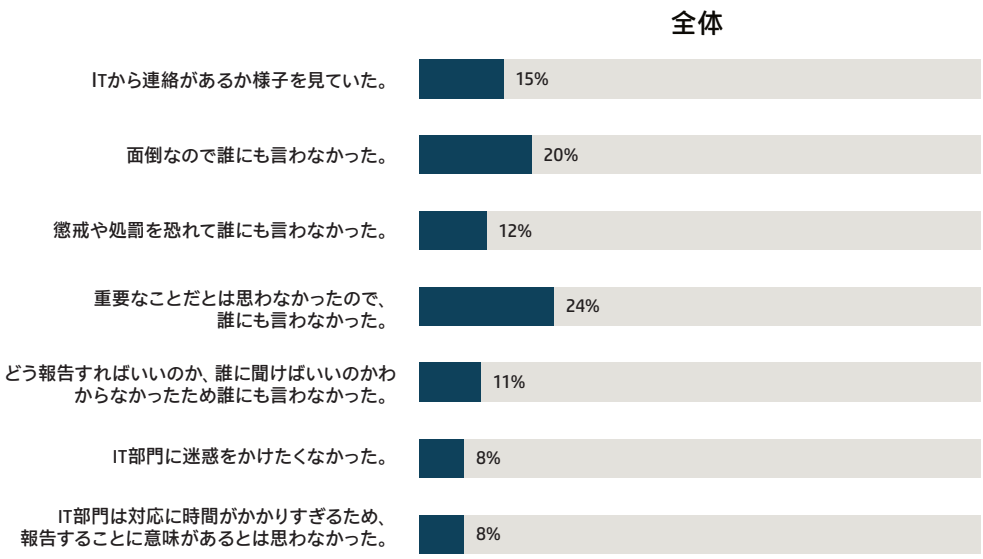
図4：在宅勤務中に悪意のあるメールをクリックしたオフィスワーカーの年齢別割合



在宅勤務中に悪意のあるものをクリックしたか、クリックしそうになったオフィスワーカーのうち、そのことをIT部門に報告したのはわずか30%でした。報告したオフィスワーカーのうち38%が、デバイスが壊れてしまったので仕方なく報告したと回答しています。また、IT部門に報告しなかった70%のうち、24%がそれを重要なことではないと考えており、20%が報告するのが面倒だった、15%がIT部門から連絡が来るかどうか様子を見ていたと回答しています。さらに、12%が懲戒を恐れて誰にも伝えていませんでした（図5）。

オフィスワーカーの35%が、
オフィスでは問題が発生すると
IT部門にすぐに相談しに行っていたが、
在宅勤務の現在はIT部門への
連絡が難しくなったと回答。

図5：悪意のあるメールをクリックした後のオフィスワーカーの対応



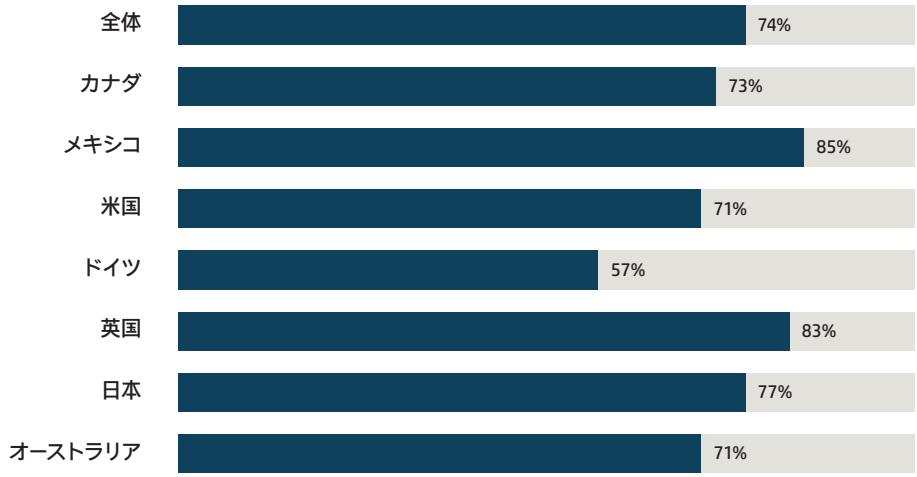
調査では、ユーザーがIT部門に報告しない潜在的な理由について、リモート環境が一因であることを示唆しています。オフィスワーカーの35%が、オフィスでは問題が発生するとIT部門にすぐに相談しに行っていたと回答しているものの、現在は在宅勤務のためIT部門に連絡しにくくなっています。また、18歳から24歳のオフィスワーカーの60%が、在宅勤務中に若干孤立していると感じており、何か問題が起こった時に自分で対処しなければならないことを心配しています。これは、オフィスワーカー全体の48%に比べて高い割合となっています。

IT部門を悩ませる脅威の拡大、高まる複雑さ、管理しにくいITセキュリティ

在宅勤務への急速な移行によって、ITセキュリティのサポートがこれまで以上に難しくなりました。この傾向は、ハイブリッドな職場環境でも継続することが予想されます。問題を悪化させているのは、脅威のレベルが上昇していることです。ユーザー自身が認めているように、クリックするべきか否かの判断が難しくなっており、デバイスの購入だけでなく潜在的な問題もIT部門を蚊帳の外に置いています。その一方で、ハッカーはより巧妙な手口でユーザーをだますようになっています。

IT部門の74%が、悪意のあるリンクをクリックしたり添付ファイルを開いたりする従業員が増加したと回答しています。この割合は、メキシコ（85%）と英国（83%）で大幅に高くなっています（図6）。オフィスワーカーのうち、悪意のあるリンクをクリックしたと自覚している割合がわずか21%であることを踏まえると、IT部門は従業員が気づいている以上にそうしたクリックを確認していることになります。

図6：悪意のあるメールや添付ファイルをクリックした従業員の数が増えたと回答したIT部門の割合



そうした背景から、侵害されたデバイスの再インストールが増加していることは当然の結果といえます。IT部門の79%が、再インストール率が上昇していると回答しています（図7）。これは、侵害されたデバイスの増加を示していますが、実際にはもっと多い可能性があります。IT部門の80%が、従業員が気づかないうちにデバイス侵害されている可能性があることを懸念しています。

図7：再インストールしたデバイスの月平均の数

	全体	カナダ	メキシコ	米国	ドイツ	英国	日本	オーストラリア
平均	61.9	67.1	56.3	67.1	57.3	61	61.7	61.3
増加	79%	79%	86%	81%	69%	86%	79%	72%

脅威の勢いが増す中、セキュリティオペレーションセンター（SOC）にはアラートが押し寄せています。回答者の推定によると、SOC部門は毎日平均4,200件のアラートを受信しており、23%は5,000～1万件のアラートを受信しています（図8）。

IT部門の80%が、従業員が気づかないうちにデバイス侵害されている可能性があることを懸念しています。

HPの視点：

HP INC.
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
イアン・プラット（IAN PRATT）

「ITの複雑さが増すにつれ、セキュリティのサポートはますます手に負えない状況になっています。HPの2021年第3四半期の脅威レポート「HP WOLF SECURITY 脅威インサイトレポート 2021年Q3」では、攻撃者は新たに見つかった脆弱性の悪用エクスプロイトに対して、すかさず行動に移していることが示されています。これは、多くの組織にとって緊急パッチの適用は複雑で時間がかかるという状況につけ込んだものです。」

HP INC.
最高情報セキュリティ責任者
（CISO）
ジョアンナ・バーキー
（JOANNA BURKEY）

「ハイブリッドな働き方がうまくいくようにするためには、IT部門とセキュリティ部門を解放し、付加価値の高いタスクに専念できるようにするための解決策を見いだす必要があります。つまり、リモートアクセスの準備や対応に何時間も費やすなど、プログラムへの組み込みや自動化が可能であるはずの日常的な手作業のタスクから、各部門を解放しなければなりません。」

エンドポイントに関するアラートの62%が誤検知のため、多くの時間が無駄になっています。

図8：SOCが受信する一日あたりのアラート数の平均

	全体	カナダ	メキシコ	米国	ドイツ	英国	日本	オーストラリア
一日2,000件未満	12%	5%	22%	11%	21%	5%	7%	13%
一日約2,000～5,000件	65%	63%	59%	64%	68%	72%	73%	58%
一日約5,000～10,000件	23%	32%	19%	25%	11%	23%	20%	29%
平均	4236.4	4710	3916.7	4367.5	3643.3	4326.7	4200	4446.7

これらの多くは対応する必要がほとんど無いファイアウォールのアラートですが、平均して14%のアラートは直接エンドポイントに関連するものです。回答者は、エンドポイントセキュリティに関するアラートのトリアージを毎週平均816件行っていると推定しています。その一方で、エンドポイントに関するアラートの62%が誤検知で有害な悪影響を及ぼさないため、多くの時間が無駄になっています。

IT部門とセキュリティ部門を悩ませているのは脅威の件数だけではありません。分散型の働き方は、職場を守るためのコスト、時間、複雑さを増大させています。

IT部門の79%が、デバイスの再インストールに費やす時間が推定で47%増加し、毎回平均4時間かかっていると回答しています。また、77%がイベントのトリアージにいっそう時間がかかるようになったと回答しています。

さらに、IT部門の74%が、セキュリティポリシーやセキュリティツールによってブロックされたWebサイト、アプリケーション、文書へのアクセスに関連する問い合わせの対応に費やした時間が増えています。

ITセキュリティのサポートについても同様の傾向が見られます。

- IT部門の64%が、オペレーティングシステム（OS）とユーザー側の安全な復旧にいっそう時間と手間がかかっていると回答しています。
- 65%が、エンドポイントデバイスへのパッチ適用にいっそう時間と手間がかかっていると回答しています。
- 64%が、新たに在宅勤務に移行する人にセキュアなデバイスを準備し設定を行うことも同様であると回答しています。

セキュリティに関連するITサポートのコストが52%増加したというIT部門の推定に驚きはないでしょう。業界における深刻なスキル不足も重なり、サイバーセキュリティのプロフェッショナルの57%が、サイバーセキュリティに関する世界的なスキル不足によって自社の組織が影響を受けており、各部門は限界に達していると回答しています。

また、IT部門の83%が、パンデミックによって在宅勤務者のセキュリティ問題が生じ、ITサポートにさらなる負担がかかっていると回答しています。さらに、IT部門の77%が、IT部門が疲れ果てて担当者が退職を検討するようになるのではないかと危惧していると回答しています。

要約

「HP Wolf Security: Out of Sight & Out of Mind ~ 目の届かないところで軽視されるセキュリティ」要約

- 在宅勤務の従業員による新たなシャドーITは、IT部門が把握していないデバイスを購入しネットワークに接続しています。
- セキュアでない可能性があるデバイスが幅広い企業ネットワークに接続されていることから、シャドーITは新たなリスクをもたらしています。
- ユーザーが、有害かもしれないリンクやダウンロードしたファイルをクリックすることが増えており、潜在的な攻撃者に機会を与えています。
- 間違いをおかした場合に、ユーザーがIT部門に報告することが少なくなっています。
- IT部門とセキュリティ部門は、ユーザーが引き起こす脅威が増え、それがデバイスへの侵害の増加につながっており、自社のデータや事業がリスクにさらされていると考えています。
- 脅威の高まりに相まって、ITセキュリティのサポートの管理や提供がさらに困難になっており、それに要するコストと時間が増加しています。

「HP WOLF SECURITY」の最終的な見解

今日のハイブリッドな職場環境は流動的で、明確な境界はありません。ユーザーとエンドポイントは常に最前線に置かれています。

本来のワークフローと在宅勤務中の行動を強制的に変更しようとしている組織の努力は、徒労に終わっているといえます。セキュリティに関する教育は極めて重要ですが、それだけでは十分と言えません。

資金が豊富でますます巧妙になっている脅威アクターが、ユーザーをだますための新たな手口を編み出し、すぐそこまで迫っています。その一方で、従業員は孤立し、プレッシャーにさらされながら迅速に業務をこなしており、間違いをおかしやすくなっています。

同時に、ITセキュリティのサポートは管理がいっそう難しくなっています。パッチの適用から、トリアージ、ユーザー環境の準備に至るまで、IT部門は常に緊急の問題に対応しています。熟考したりイノベーションを図ったりする余裕はありません。

このような状況で、エンドポイントセキュリティがかつてないほど重要なものになっています。しかし、今日のデジタル化が進んだハイブリッド型の社会では、悪意のあるアクティビティの検知と防御をリアルタイムで継続することは困難です。再インストール率の激増がそのことを裏付けています。

組織は、IT部門にイノベーションの推進に専念してもらう必要があります。セキュリティ部門は、今後起こり得る大規模なセキュリティ侵害の防止に重点を置いてきました。しかしながら、アラートの対応に追われ、必要とはいえ日常的なタスクで身動きが取れない状況では、それに取り組むこともできません。

新たな対策が求められています。

今後の働き方を確立する上で求められる新たなセキュリティアーキテクチャのアプローチ

ハイブリッドな働き方を実現するために、セキュリティの脅威を管理する新たな方法を導入する必要があります。これには、リスクの緩和に役立つと同時に、セグメンテーションによって失敗の影響を限定的にする、セキュリティへの構造的なアプローチが求められます。

ユーザーがセキュリティの単一の障害点になるべきではありません。今後の働き方を確立する上で、1台のデバイスへの侵害が重要資産への侵害を引き起こさないように、レジリエンスを備えたセキュリティのシステムと戦略を構築する必要があります。

最小権限、強力な隔離、強制アクセス制御、強力なID管理といったゼロトラストの主要な原則を適用することによって、組織はアドレス可能なアタックサーフェス（攻撃可能領域）を削減できます。それにより、侵害を受けた場合には迅速に復旧し、ITセキュリティサポート部門への負担を減らすことができます。

このアプローチの具体例が、最も頻度の高い攻撃ベクトルから保護する隔離の活用です。OSから分離された、使い捨ての仮想マシン（VM）において、リンク、添付ファイル、ファイルのダウンロードのクリックや、有害かもしれないWebページへのアクセスなど、リスクの高いタスクを実行すると、マルウェアが無害化されます。ユーザーが悪意のある文書を起動しても、攻撃者は身動きが取れなくなります。攻撃者は行き場を失い、何も盗めません。

隔離によって、いくつかの面でIT部門とセキュリティ部門の負担が軽減されます。エンドポイントはほとんどの脅威から保護され、侵害されたデバイスの再インストールが減るだけでなく、場合によっては再インストールが不要になるほか、データやシステムの安全性が維持されます。

また、多くの脆弱性に保護のレイヤーが追加されます。これにより、各部門は時間をかけていっそう管理されたアプローチを講じることができ、緊急パッチの負担が軽減されます。IT部門とセキュリティ部門は、セキュリティ上の弱点を削減するために設定していた制限を解除することができ、ヘルプデスクにかかってくる電話を減らせます。さらに、それぞれの攻撃に関するデータがIT部門とセキュリティ部門に提供され、誤検知が解消されます。これによって、IT部門とセキュリティ部門が調査しなければならないアラートの件数を減らすことができます。

HPの視点：

HP INC.
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
イアン・プラット（IAN PRATT）

「未来をリードする技術は、設計に組み込まれた『Secure by Design』の考え方を採用し十分なインテリジェンスを備えたものになり、脅威を検知するだけでなく、その影響を封じ込めて緩和し、いつでも誰にでも起こり得るセキュリティ侵害を受けた場合に迅速に復旧できるでしょう。このような保護は、OS下やOS上に拡張し、既知と未知の脅威だけでなくゼロデイ攻撃に対する保護も提供するべきです。ハードウェアからセキュリティを構築することで、サポート部門の負担を軽減し、ユーザーが制限を受けずに業務をこなせるようになります。」

このほかにも、安全で使い捨てのVMにマルウェアを隔離することで、リスクを負わずにマルウェアを好きなだけ活動させることができます。これにより、脅威アナリストはユニークなインサイトを得られます。収集したインテリジェンスは、IT部門とセキュリティ部門が自社組織に対するAPT攻撃などの重大な脅威を追跡して捕らえる上で活用できます。そうして、これまでは弱みだったエンドポイントを、強みを結集させたインテリジェンスに変えることができます。

働き方の確立：行動の呼びかけ

ハイブリッドな働き方は、未来の働き方です。働き方の変革とデジタルトランスフォーメーションは、企業に多大なメリットをもたらしています。その一方で、環境の変化に伴うリスクを把握し、対処する必要があります。ますます分散化が進む働き方を考慮すると、強力なエンドポイントセキュリティが不可欠です。

IT部門は、優れた可視性と管理ツールを備えたより良いエンドポイントセキュリティを今すぐ必要としています。可能であれば、IT部門はサポートの負担を軽減するために、セキュリティがハードウェアに内蔵されているデバイスをユーザーに提供すべきです。例えば、リモート復旧機能や自己回復ファームウェアは、侵害された場合にデバイスの復旧に役立ちます。これは、セキュリティにおけるサポートの役割の変革に寄与し、各部門はビジネス価値の実現に注力できるようになります。

それにより、組織は以下の体制を整えることができます:

- ビジネスイノベーションを後押しする透明性に優れたセキュリティを実現することで、確信を持って制限を解除し、従業員からのリモートアクセスの要求をより多く受け入れられます。
- アタックサーフェスを削減し、隔離によってマルウェアを無害化します。
- デバイスやOSのリモート復旧や再イメージングを可能にし、ITサポート部門の負担を軽減します。
- シームレスなユーザーエクスペリエンスを提供するために、購入時点でセキュリティが内蔵されたデバイスを使用することによって、セキュリティを損なうことなく高度なユーザーエクスペリエンスを実現します。
- 誤検知を減らして誤ったインシデントを追跡しないようにするとともに、エンドポイントから脅威インテリジェンスを収集して現実の脅威に集中することができます。
- 脅威の封じ込めと隔離を活用し、頻度の高い脅威ベクトルから保護することによって、マルウェアへの感染に伴う再インストール、エンドポイントの修復、再イメージングの必要性がなくなります。
- アプリケーションやOSの緊急パッチを避け、制御された計画的な方法で、セキュリティパッチを管理できます。

「HP WOLF SECURITY」について

世界で最も安全なPC[1]およびプリンター[2]のメーカーであるHPが提供する「HP Wolf Security」[3]は、新しいタイプのエンドポイントセキュリティです。ハードウェアにより強化されたセキュリティとエンドポイントに焦点を当てたセキュリティサービスで構成するHPのポートフォリオは、組織がPC、プリンター、従業員をサイバー犯罪者から保護できるように設計されています。「HP Wolf Se-curity」は、ハードウェアレベルからはじまり、ソフトウェアとサービスまで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。

調査方法

HP Wolf Securityレポートは、以下の調査結果に基づいて作成されています。

01 米国、英国、メキシコ、ドイツ、オーストラリア、カナダ、日本の成人8,443人を対象にYouGovが実施した調査。パンデミック前はオフィスワーカーとして働き、パンデミック後も以前と同様、またはそれ以上に在宅で仕事をしている人が対象。調査は2021年3月17日~25日にオンラインで実施。

02 英国、米国、カナダ、メキシコ、ドイツ、オーストラリア、日本のIT部門の意思決定者1,100人を対象にTolunaが実施した調査。調査は2021年3月19日~4月6日にオンラインで実施。

免責条項

[1] Windowsおよび第8世代以降のインテル® プロセッサーまたはAMD Ryzen 4000以降のプロセッサーを搭載した「HP Elite」PC、第10世代以降のインテルプロセッサーを搭載した「HP ProDesk 600 G6」、AMD Ryzen 4000または第11世代以降のインテルプロセッサーを搭載した「HP ProBook 600」。追加費用、追加インストール不要のHP独自の標準装備された包括的なセキュリティ機能に基づきます。

[2] HPの最も高度なデバイス標準装備セキュリティ機能は、HP FutureSmartファームウェア4.5以降を搭載する「HP Enterprise」および「HP Managed」デバイスで利用可能です。記載内容は、競合他社の同クラスのプリンターで2021年に発表された機能に関する米国HP Inc.のレビューに基づいています。デバイスのサイバーレジリエンスに関するNIST SP 800-193ガイドラインに従い、自動的に攻撃の検知と阻止を行い、自己修復のための再起動で復旧する統合セキュリティ機能を提供しているのはHPのみです。対応製品の一覧は、hp.com/go/PrintersThatProtectを参照してください。詳細は、hp.com/go/PrinterSecurityClaimsを参照してください。

[3] 「HP Security」は「HP Wolf Security」に名称を変更しました。セキュリティ機能はプラットフォームによって異なります。詳細は、製品データシートを参照してください。

HP WOLF SECURITY