HP WOLF SECURITY

BLURRED LINES AND BLINDSPOTS

曖昧になる境界とセキュリティの死角

HP WOLF SECURITY

エグゼクティブサマリーと主な調査結果

新型コロナウイルス感染症のパンデミックがビジネスにもたらしたさまざまな影響のうち、最も大きな変化は、世界中で何億人もの人が在宅勤務を余儀なくされたことでした。2020年前半のわずか数週間で、在宅勤務は、従業員の都合で時々利用するものから、多くの企業にとって事業継続のための唯一の方法へと変わりました。

これは非常に大きな変化でした。本レポートのためにHPが委託してYouGovが世界のオフィスワーカーを対象に実施した調査では、82%の回答者がパンデミック発生から在宅勤務の時間が増えたと回答しています。在宅勤務が経済にも個人にもメリットがあるものとして見直されるきっかけとなりました。働き方が恒久的に変わる可能性があり、企業は競争力を維持するためにこうした変化に適応する必要があります。実際の調査では、世界のオフィスワーカーの23%がパンデミック終息後も主に在宅勤務で働き、16%が在宅勤務とオフィス勤務半々で働くことを期待していることが明らかになりました。

しかしながら、いかに現在の環境が既存のセキュリティに対する脅威を増幅させているのかを理解することなく、企業が在宅勤務を導入するのは危険です。機密の財務情報など、自宅からアクセスされる企業データは大幅に増加し、より多くの情報がリスクにさらされています。それと同時に、従来のネットワーク境界を越えて企業ネットワークにアクセスする際に使用されるエンドポイントの数は、個人所有か会社支給に関わらず急増しています。

本レポートは、セキュリティ部門にかかる負担を含めて、リモートワーカーを守るための境界防御のセキュリティモデルには限界があることを浮き彫りにしています。ノートPC、デスクトップPC、プリンターといったエンドポイントデバイスは攻撃に対して無防備な状態にあることが多く、被害が出るまでセキュリティインシデントに気づけない危険性を高めています。このような盲点によって、多くの企業が打撃を受ける可能性があります。

「HP Wolf Security」[1]は、ニューノーマルに対応し、ハードウェア、ソフトウェア、サービスを統合したHPの新しいポートフォリオです。このHP Wolf Securityレポートでは、セキュリティに関する目下の課題について多面的な見解を提供します。パンデミックにより在宅勤務に移行した8,443人のオフィスワーカーを対象にYouGovが実施したグローバルオンライン調査と、1,100人のIT部門の意思決定者（ITDM）対象のグローバル調査の結果を統合し、それぞれの立場から状況を整理しました。また、「HP Sure Click仮想マシン（VM）」から収集した実際の脅威テレメトリーによりセキュリティに関するリスクを明らかにし、世界的な大手アナリスト企業であるKuppingerColeによる分析によって、さらに充実させました。

HP Wolf Securityレポートは、さまざまな視点から課題を検討し、以下の点について考察します。

01 **「新たなオフィス」の登場による変化：**
リモートワークへの移行が加速する中、防御の最前線としてエンドポイントがいかに重要かに着目します。

02 **パンデミックがユーザーの考え方や行動に及ぼした影響：**
従業員はオフィスにいる時よりも多くのリスクを負っています。それにより、意図せずセキュリティ侵害のリスクを高めていることを提示します。

03 **新たなリスクの出現がサイバーセキュリティの防御者に与えるプレッシャー：**
IoTデバイスをはじめ、増加を続けるエンドポイントは、企業のネットワークに侵入する足掛かりを探している攻撃者に対してより多くのアタック・サーフェスを提供することを説明します。

04 **今日の脅威を防御するために「HP Wolf Security」などの新しいタイプのエンドポイントセキュリティ・サービスが必要な理由：**
ゼロトラストの原則に従うことによって、企業がどのようにアタック・サーフェスを縮小してリスクを減らし、負担が増しているIT部門を支援できるかを実証します。

91%

91%のIT部門の意思決定者（ITDM）が、エンドポイントセキュリティはネットワークセキュリティと同じくらい重要になったと考えています。また、2年前よりもエンドポイントセキュリティに費やす時間が増えたと回答しています。

76%

76%のオフィスワーカーが、在宅勤務によりプライベートと仕事の境界が曖昧になっていると回答しています。また、半数が仕事用デバイスを個人のデバイスと見なすようになっており、46%が仕事用ノートPCを日々の雑用に使用していると認めています。

30%

30%の従業員が仕事用デバイスを他者に使用させたことがあり、85%のITDMはそうした行動が自社のセキュリティ侵害のリスクを高めていることを懸念していると回答しています。

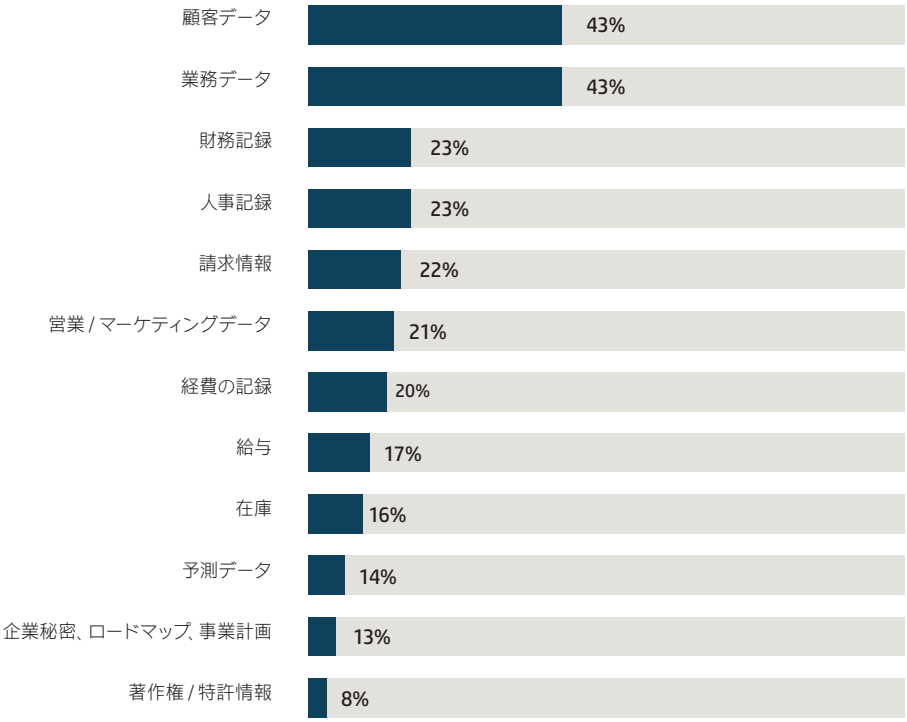
54%

54%のITDMが、過去1年の間にフィッシング攻撃が増加したと回答し、45%が不正アクセスされたプリンターが攻撃ポイントとして利用された形跡があったと回答しています。

1
新たなオフィス

パンデミックが在宅勤務や自宅とオフィスの両方で働くハイブリッドワークのトレンドを作ったわけではありませんが、このような働き方を加速させたことは間違いありません。10年はかかったかもしれないリモートワークやモバイルワークへの移行が、数カ月で進みました。これにより、従業員がリモート環境から会社のデータにアクセスする必要性が必然的に高まっています。本レポートでは、調査対象のオフィスワーカーの71%が、パンデミック前と比較して、より多くの企業データへ、より頻繁に自宅からアクセスしていることが明らかになりました。よくアクセスしているデータの種類は以下のとおりです。

従業員の71%が、パンデミック前と比較して、より多くの企業データへ、より頻繁に自宅からアクセスしていると回答。



「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）**

「企業のネットワーク、アプリケーション、データへのアクセスを従来の方法で保護することはもはや適切ではありません。境界防御は時代遅れになっています。過去数年にわたって従業員の分散化が進み、SaaSの導入が増加しています。つまり、重要なデータは企業のファイアウォールの外にあるのです。企業はゼロトラストの概念を活用して、未知の脅威からの防御に着手すべき時代になりました。ただし、それをユーザーに負担をかけずに行う必要があります。」

サイバー犯罪者は躊躇なく混乱に乗じます。パンデミックでも同様に、企業の防御が普段よりも脆弱であることに気づくと、次から次へとサイバー攻撃を仕掛けてきました。世界経済フォーラム（WEF）のデータによると、2020年2月から4月にかけて、世界中でサイバー攻撃件数が238%増加しました。

分散した従業員は企業のファイアウォールによって保護されておらず、多くの従業員が安全ではない接続を使用して重要なデータにアクセスしているため、このような攻撃を防ぐことはますます難しくなっています。ITDMを対象にした調査では、回答者の89%が、従業員がVPNなどの安全な接続を使用していないことを懸念しています。

2020年2月から4月にかけて、世界中でサイバー攻撃件数が238%増加。

他の業界よりも標的にされている業界：

2月から5月にかけて、医療業界に対する攻撃が50%急増しました。世界保健機関（WHO）は、同期間にサイバー攻撃が400%増加したことを発表しました。

2019年から2020年にかけて、教育機関に対するサイバー攻撃が33%増加しました。

2020年前半の数カ月で、ゲーム業界ではフィッシング攻撃が54%増加しました。

ITDMの91%が、2年前よりもエンドポイントセキュリティに費やす時間が増えたと回答。

その結果、境界はネットワークからエンドポイントに移行しました。ITDMを対象にした調査では、91%が在宅勤務の従業員が増えた今、エンドポイントセキュリティはネットワークセキュリティと同じくらい重要になったと考えていることが明らかになりました。また、ITDMの90%が、2020年のコロナ禍により境界が曖昧になっていく組織を防御する上で強力なエンドポイントセキュリティの重要性が高まったと認めています。また91%が、2年前よりもエンドポイントセキュリティに費やす時間が増えたと回答しています。

図1：在宅勤務の従業員が増えたためエンドポイントセキュリティはネットワークセキュリティと同じくらい重要になったと考えているITDM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
91%	91%	97%	92%	85%	91%	92%	92%

半数以上（56%）のプリンターは一般的に利用されるプリンターポートが開放されており、ハッキングされる可能性がある。

エンドポイントは常に進化し、多様化しています。KuppingerColeによると、「従業員が在宅勤務で使用しているインターネットに接続されたデバイスの多くが、企業のITインフラやネットワークの停止の一因となっています。これにはプリンターも含まれます」。自宅の環境は今や、KuppingerColeが脆弱なセキュリティ設計であると指摘するIoTデバイスなど、サイバー犯罪者が狙っているデバイスだらけです。これには、セキュリティ部門が見逃しがちなプリンターも含まれます。KuppingerColeによる2020年の調査では、プリンターの半数以上（56%）が、一般的に利用されるプリンターポートが開放されており、ハッキングされる恐れがあることが分かりました。

2

便利さとリスクのジレンマ

HPの視点:

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）

「リモート環境で働く従業員は、仕事用デバイスと個人のデバイスの境界が曖昧になり、添付ファイルを開くなどの日常的な行動が深刻な結果をもたらす可能性があります。誰がどのようにデバイスを使用しているのかについても、パンデミック前のようには可視化されておらず、IT部門やセキュリティ部門は状況を把握しにくいまま仕事をしています。」

在宅勤務への移行によって、サイバーセキュリティリスクの性質と規模が変わりました。たいていは可視化できていないためか、または過小評価しているために、多くの企業がこのことをまだ十分に理解していません。興味深い側面は、文化の変化です。オフィスで使用するデバイスは比較的管理が行き届いていますが、オフィスで使用しているデバイスを自宅に持ち込むとあらゆることが変わります。従業員は、オフィスでは決して取らないような行動を自宅で取るため、サイバーセキュリティリスクが急速に高まり、監視が容易ではなくなる可能性があります。

そうした問題は本レポートでも示されており、調査対象のオフィスワーカーの76%が、在宅勤務によって仕事場と自宅が同じ環境になったことで、プライベートと仕事の境界が曖昧になっていると回答しています。そのことが会社のデバイスの使い方にどのような影響を及ぼしているかを尋ねた質問では、50%が仕事用ノートPCを個人のデバイスと考えるようになったと認めています。

図2：新型コロナによって在宅勤務となったことでプライベートと仕事の境界が曖昧になっていると回答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
76%	78%	84%	77%	78%	79%	62%	77%

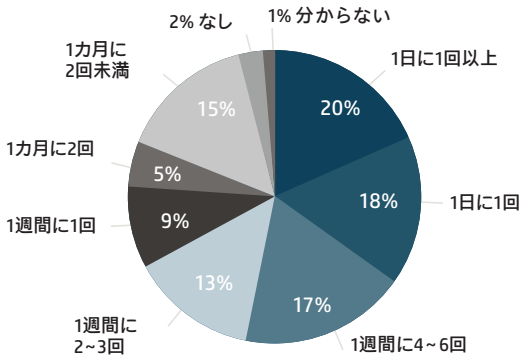
さらに重要なこととして、30%が仕事用ノートPCを、パートナーや子ども、友人などの他者に、しばしば一日一回以上、使用させていると認めています。また、デバイスを共有したことがある回答者のうち27%が、共有してはならないと分かっているものの、このような特殊な状況で「仕方なかった」と考えていると答えています。

図3

地域	在宅勤務により仕事用ノートPCを仕事用兼個人のノートPCと見なすようになったと回答したオフィスワーカーの割合（%）	過去1年間に仕事用ノートPCまたはPCを他者に使用させたことがあると回答したオフィスワーカーの割合（%）
全体	50%	30%
カナダ	63%	37%
メキシコ	79%	55%
米国	53%	31%
ドイツ	30%	16%
英国	33%	12%
日本	35%	21%
オーストラリア	59%	34%

デバイスを共有したことがある回答者のうち27%が、共有してはならないと分かっているものの、このような特殊な状況で「仕方なかった」と考えていると回答。

図4：仕事用PCまたはノートPCを他者が使用した頻度の平均



ITDMの84%が、従業員がパンデミックの中、仕事用デバイスを私的に使用することは、自社のセキュリティ侵害のリスクを高めていると懸念。

この所有の心理が、セキュリティリスクに対する従業員の警戒の緩みを引き起こし、仕事用デバイスがさまざまな個人的用途に使用されることに繋がっています。ITDMの84%が、従業員がパンデミックの中、仕事用デバイスを私的に使用していることが自社のセキュリティ侵害のリスクを高めていると懸念しています。

ITDMは約3分の1（33%）の従業員が、仕事用PCを私的（ゲームやネットサーフィンなど）に使用していると予測していましたが、実際にはもっと多いことが分かりました。調査対象のオフィスワーカーのうち70%が、仕事用デバイスを私的に使用している、または他者に使用させていると認めています。また、46%が仕事用ノートPCを日々の雑用に使用していると認めており、25~34歳の回答者ではこの割合が61%に増加しています。さらに、調査対象となったオフィスワーカーの10人中4人が、仕事用デバイスを宿題やオンライン学習に使用しており、5~16歳の子どもを持つ親ではこの割合が57%に増加しています。

その他のリスクがある行動も容易に見つかりました。調査対象となったオフィスワーカー（またはその家族）は、以下に挙げる私的な用途に仕事用ノートPCを使用したことがあると回答しています。

- インターネットからのダウンロード: 33%
- 個人メールの添付ファイルの開封またはWebサイトへのアクセス: 55%
- 個人で使用しているソーシャルメディアサイトへのアクセス: 45%
- ビデオ通話: 58%
- ゲーム: 27%
- オンラインストリーミングサービスの視聴: 36%
- オンラインショッピング / インターネットの閲覧: 52%

個人メールの脅威

2020年、「HP Sure Click」と「HP Sure Click Enterprise」は、128人のユーザーが、会社のメールフィルタリング機能のない、個人で使用しているWebメールサービスから、マルウェア「Emotet」やランサムウェアなどの悪意のあるファイルをダウンロードするのを防ぎました。

ストリーミングサービスの脅威

KuppingerColeの分析によると、パンデミックの中、ストリーミングサービスも標的となり、2020年4月には、わずか7日間で人気のあるストリーミングサービスになりすました700以上の詐欺サイトが特定されました。Netflixユーザーを狙ったフィッシング詐欺は、2019年から60%増加しています。また、Netflixを標的としたフィッシングURLは2019年から646%、Twitchで337%、HBOで525%、YouTubeで3,064%それぞれ増加しました。

KuppingerColeの分析による裏付け

- 2020年に世界でゲームプレイ時間が36%増加しました。また、最近のゲームリリースによって、ゲームのダウンロード数は最大80%増加しました。
- 2020年1月から4月にかけて、ユーザーをフィッシングページに誘導するなど、人気があるゲーミングプラットフォームを使った悪意のあるアクターが54%増加しました。

ゲーム関連の脅威

2020年、「HP Sure Click」および「HP Sure Click Enterprise」テレメトリーで、「フォートナイト」や「Among Us」といった特に人気のあるタイトルのゲームに関連するマルウェアの増加を確認しました。

- 被害の多かった事例として、「フォートナイト」のチートツールを装ったランサムウェア「Ryuk」（FreeHacks4Fortnite.exe）が挙げられます。「HP Sure Click Enterprise」は、ファイル共有サイトのMEGAからファイルをダウンロードして実行したユーザーを特定しました。「HP Sure Click Enterprise」は、ファイルの隔離に成功し、マルウェアによるデバイスの暗号化を防ぐことができました。

2021年2月、「HP Sure Click」は、「Gootloader」と呼ばれるステルスマルウェアのJavaScriptダウンローダーのサンプルを隔離しました。

- VirusTotalでの検知率は極めて低く、ほとんどの場合すべての検知エンジンを回避。
- 一部検体は「フォートナイト」のハックを偽装。
- アーカイブで配信。
- 最終ペイロードは「Gootkit」（バンキング型トロイの木馬）または「REvil」（ランサムウェア）。

オフィスワーカーの69%が、パンデミックが発生してから個人用ノートPCやプリンター / スキャナーを仕事に使用していると回答。

従業員が個人のデバイスを使って会社のネットワークにアクセスしている明確な傾向があることもわかりました。ITDMは、仕事関連の作業に個人のデバイスを使用している従業員の割合を半数強（53%）と予測していましたが、実際にはもっと多いことが分かりました。本レポートで、調査対象のオフィスワーカーの69%が、パンデミックが発生してから個人のノートPCやプリンター / スキャナーを仕事に使用したことがあると回答しています。過去1年間で、従業員は、これまで以上にさまざまな作業に個人のデバイスを使用しています。

- 34%が、自宅のプリンターを使用して文書をスキャンし、同僚や顧客と共有しています。
- 21%が、自宅のプリンターを使用してVPN経由で会社のネットワークにファイルを保存しています。
- 37%が、個人のPC / ノートPCを使用して仕事用のアプリケーションにアクセスしています。
- 35%が、個人のPC / ノートPCを使用して仕事の文書を保存しています
- 27%が、個人の携帯電話を使用して自宅のプリンターに仕事の文書を送信しています。
- 32%が、個人のPC / ノートPCを使用して会社の基幹ネットワークにアクセスしています。

3

脅威の激増

テクノロジーの活用が、企業をこれまで経験したことのない危険にさらしています。この問題に対する懸念は、グローバルのITDMを対象にした調査で明らかになりました。ITDMの3分の1以上（35%）が、会社のデバイスを誰がどのように使用しているか把握できないことが目下最大の課題であると回答しています。ITDMは、以下のような従業員の新たな行動が自社のリスクを高めていると懸念しています。

- 85%が、従業員が仕事用デバイスを他者（子ども、パートナー、同居人など）に使用させているため、自社のセキュリティ侵害のリスクが高まっていると懸念しています。
- 88%が、IT部門が承認していないソフトウェアを従業員が（仕事のために）ダウンロードしているため、自社のセキュリティ侵害のリスクが高まっていると懸念しています。
- 88%が、従業員がビジネスで求められるセキュリティが搭載されていない個人のデバイスを仕事に使用しているため、自社のセキュリティ侵害のリスクが高まっていると懸念しています。

「HP WOLF SECURITY」の視点：

HP INC. パーソナルシステムズ事業ソフトウェア担当グローバル責任者
ロズ・ホー（ROZ HO）

「企業が働く場所をオフィスから従業員の自宅に拡大する中、プリンターのセキュリティが死角であってはなりません。広域な企業のネットワークを感染させるためにプリンターが利用される可能性が極めて高くなっています。IT部門の意思決定者の45%が、過去1年間に不正にアクセスされたプリンターが攻撃ポイントとして利用された形跡を確認したと回答しています。企業はこの問題を認識し、プリンターを悪用した攻撃を防御するべきです。」

図5

地域	従業員が仕事用デバイスを他者に使用させているため自社のセキュリティ侵害のリスクが高まっていると考えているITDMの割合（%）	IT部門が承認していないソフトウェアを従業員が（仕事のために）ダウンロードしているため自社のセキュリティ侵害のリスクが高まっていると考えているITDMの割合（%）	従業員がビジネスで求められるセキュリティを搭載していない個人のデバイスを仕事に使用しているため自社のセキュリティ侵害のリスクが高まっていると考えているITDMの割合（%）
全体	85%	88%	88%
カナダ	91%	97%	95%
メキシコ	87%	95%	93%
米国	83%	87%	89%
ドイツ	67%	72%	71%
英国	87%	89%	87%
日本	94%	93%	93%
オーストラリア	83%	87%	89%

そうした懸念は当然のことです。調査対象となったITDMのうち51%が、過去1年間に不正にアクセスされた個人のデバイスが自社や顧客のデータへのアクセスに利用された例を見たと回答しています。また45%が、不正にアクセスされたプリンターが攻撃ポイントとして利用された形跡が見られたと回答しています。

さらに、ITDMの54%が、過去1年間に社内でフィッシング関連の攻撃件数が増えたと回答しており、56%がWebブラウザ関連の感染が増えたと回答しています。また、51%がセキュリティパッチが適用されていないエンドポイントを使用しているユーザーの存在を過去1年間に確認したと回答しています。

図6：過去1年間にセキュリティ侵害の形跡を確認したITDMの割合

フィッシング関連の感染増加	54%
Webブラウザ関連の感染増加	56%
不正アクセスされたデバイスが、より広域な感染拡大に利用された	44%
不正アクセスされた個人のデバイスが、自社や顧客データへのアクセスに利用された	51%
セキュリティパッチが適用されていないデバイスを使用しているユーザー	51%
不正アクセスされたプリンターが攻撃ポイントとして利用された	45%

ニューノーマルへの適応

HP WOLF SECURITY レポート調査結果の要約：

- パンデミックによって、在宅勤務の従業員の増加が加速し、恒久的な変化がもたらされています。
- 在宅勤務の環境はセキュリティの観点から考えるとオフィス内と異なります。安全でないデバイスの使用、家族や友人とのデバイスの共有、仕事用デバイスを私用に使うなど、従業員はオフィスにいる時よりも多くのリスクを負っています。
- 攻撃者はその脆弱性に狙いを定め、ソーシャルエンジニアリングの悪用に特化したマルウェアキャンペーンを用いて、在宅勤務者を標的にしています。このことは、すでに負担がかかっているIT部門やセキュリティ部門の重荷となり、在宅勤務に伴う多くのリスクを見えなくしています。
- これは、境界防御セキュリティの時代から続いている、信頼に基づいた現在のエンドポイントセキュリティのアプローチの限界を浮き彫りにしました。このモデルの下で不正にアクセスされても、ほとんどの場合は重大な被害が出るまで気がつくことができません。

この大きな問題は未解決のまま残されています。どこからでも仕事ができる世界で、高まるサイバーリスクに企業をさらすことなく、将来の分散されたハイブリッドなワークフォースを築くには、どうすべきでしょうか。ゲームをダウンロードするために仕事用ノートPCを子どもに貸すことは無謀と思われるかもしれませんが、家庭と仕事を両立させようとしていることは理解でき、そのような行為をしているのは回答者だけではないことはデータからも明らかです。これは一過性のものではありません。パンデミックは企業の取り組みを後押しし、在宅勤務への移行を加速させたと同時に、人々の働き方を恒久的に変えた可能性があります。企業は、ニューノーマルにおけるリスクに対応し、労働力のモビリティとセキュリティを両立させる方法を直ちに検証する必要があります。

最終的な見解

新しいアプローチの必要性

サイバー犯罪者は、かつてないほど高度化かつ組織化し、諦めが悪くなっています。また、データの活用やデジタルトランスフォーメーションによってアタック・サーフェスが広がっています。すでに負荷がかかっているIT部門やセキュリティ部門は、最大限の努力をしているにも関わらず、後れを取らないことに苦戦しています。そうした背景から、防御の最前線としてエンドポイントセキュリティがこれまで以上に重要なものとなっています。従業員がだまされてセキュリティ対策をすり抜けられたり、警告を無視したり、単純に注意を怠っていたりしたら、それはセキュリティ対策が存在していないも同然です。セキュリティが機能しないと、システムに侵入する足掛かりを攻撃者に与え、データを引き出し、スパイ活動を行い、意のままに混乱をもたらすことを許してしまい、大きな問題につながります。これは今に始まったことではありませんが、在宅勤務の普及によってこれまでにない規模の問題に発展させます。

この問題に対する極端な措置として、技術的にロックダウンすることが挙げられます。つまり、アクセスを制限し、不必要な認証レイヤーを追加して、楽観的なポリシーでデバイスの利用を抑制することです。そうした措置は、在宅勤務では直ちに問題を引き起こし、従業員の生産性を損ない、セキュリティが邪魔だという考えを強めてしまいます。

業界で支持されることが多い代替案は、不正であることがわかっているシグネチャーやコードを探し、「検知して保護する」ことですが、自動生成されるポリモーフィック型マルウェア（機械生成のマルウェア）の急増が、そうしたアプローチを妨げています。次世代型の検知では、機械学習を利用して変異の可能性を特定することで問題への対処を試みています。しかしながら、マルウェア開発者はそれらのツールにアクセスできるため、自分のコードを自動テストし、検知を回避できるようになるまで改良を重ね、レーダーにかからないという自信を与えてしまいます。常に網の目をすり抜ける攻撃が存在します。

ゼロトラストの原則を適用

セキュリティのニーズと従業員のニーズのバランスを見直すためには、エンドポイントと在宅勤務のセキュリティに対してまったく異なるモデルが必要になります。暗黙の信頼をしないというゼロトラストの原則を基盤とし、ユーザー、デバイス、場所、セキュリティ状態といったコンテキストに基づいてリソースへのアクセスを評価する必要があります。これはデバイスだけでなく、ファームウェア、アプリケーションのセキュリティ、OSの完全性、アカウントやユーザーのアクセスデータなど、エンドポイントのさまざまな要素にも当てはまります。

分散化が進んだデジタルの世界は、必ずしも脆弱性が増した世界である必要はありません。サイバーの世界が進化し続けているように、サイバーセキュリティも進化する必要があります。近い将来のテクノロジーは、設計の段階からセキュリティを組み込み、脅威を検知するだけでなく、その影響を封じ込めて軽減させ、セキュリティ侵害が発生した場合には迅速に復旧できるほどインテリジェントになるものと予想されます。HPは、そうした動的なデジタルエコシステムをお客様が安全に活用できるようサポートするために取り組んでいます。

「HP WOLF SECURITY」—新しいタイプのエンドポイントセキュリティ[1]

そのことを念頭に置いて、HPは、セキュアな設計のPCおよびプリンター、ハードウェアで強化されたエンドポイントセキュリティソフトウェア、ならびにエンドポイントセキュリティ・サービスを統合した新しいポートフォリオとして「HP Wolf Security」を発表しました。これにより、お客様がこの困難な状況を乗り越えられるようサポートし、分散化が進むライフスタイルに関連するさまざまな新しい攻撃とリスクを防御します。「HP Wolf Security」プラットフォームは、20年を超えるセキュリティの研究とイノベーションに基づいて構築されており、包括的なエンドポイント保護とサイバーレジリエンスの実現に重点を置き、お客様に統合したポートフォリオを提供します。

「HP Wolf Security」は、ゼロトラストの原則に基づき、強化された防御、プライバシー、エンドポイントで収集したデータに基づく脅威インテリジェンスで構成される多層防御を提供し、企業を包括的に保護します。

「HP Wolf Security」は、企業が既知および未知の脅威だけでなく、ゼロデイ脆弱性さえも防御できるようにサポートします。ハードウェアで強化されたソフトウェアとセキュリティの機能に業界をリードするエンドポイントセキュリティ・サービスを組み合わせた「HP Wolf Security」は、階層型の幅広いセキュリティスタックをシームレスに統合しています。そのためお客様は、シリコンからクラウドに至るまで、また、BIOSからブラウザに至るまで、内蔵された堅牢な保護機能のメリットを享受できます。

長い間、エンドポイントは犠牲者でした。エンドポイントは、ネットワークの検知機能を使ってしか封じ込めることのできない敵に完全に負けていました。これは、重要なことだと思われていませんでしたが、脅威がエンドポイントから抜け出すと、その危険性は非常に大きくなります。脅威を食い止めるには、脅威が発生した場所、つまり侵害されたソフトウェアの特定の層で食い止めるのが正しい方法です。侵害されたエンドポイントが強力な権限を持ち続けるような攻撃を放置すべきではありません。

「HP Wolf Security」は、リモートワーク関連の脅威から企業を守り、ユーザーが常に進化する脅威に後れを取らないように新しいセキュリティ機能を提供し続けます。現在は以下の機能を提供しています。

- **ミッションクリティカルなアプリケーションをサイバー脅威から防御：**
  「HP Wolf Enterprise Security」に新しく追加された「Sure Access Enterprise」[2]は、HP独自の隔離技術により、クリティカルなアプリケーションをユーザーのPCに潜むマルウェアから完全に保護します。「HP Sure Access」は、重要なアプリケーションを保護するハードウェアで強化されたマイクロ仮想マシン（VM）を生成し、アプリケーションとホストPCの間に仮想エアギャップを形成します。アプリケーションとデータは、ホストOSと、そこに不正にアクセスした悪意のあるアクターから、安全に隔離されます。

- **脅威を封じ込めて隔離しマルウェアを無害化：**
  ハードウェアで強化されたマイクロ仮想化は、ユーザーエクスペリエンスに影響を及ぼすことなく、メール、ブラウザ、ダウンロードといった最も一般的な脅威ベクトルを介してもたらされる脅威を完全に隔離します。タスクが終了すると、侵害されることなく、マイクロ仮想マシンと封じ込められた脅威を処理します。したがって、ユーザーが不適切なものをクリックしても、攻撃者はどこへも侵入できず、何も盗み出すことはできません。

- **IT部門の負荷を軽減しつつリモートのファームウェア攻撃から迅速に復旧：**
  見落としがちなプリンターとスキャナー、およびそれらの不適切な利用は、セキュリティの脅威を高めます。「HP Wolf Security」は、マルウェアによって改ざんされた場合にファームウェアをアップグレードして自己回復する能力などで、プリンター内のすべてのソフトウェアレイヤーの完全な可視化と管理を可能にし、そのような問題を解決します。デバイスがネットワークに追加されると、瞬時に機能するセキュリティが直ちに企業向けのセキュリティポリシーをデバイスに設定します。「HP Security Manager」は、対応モデル向けの200以上のセキュリティ設定を保持できます。

- **脅威テレメトリーを活用し、従来弱点とされてきたエンドポイントを情報収集のための強みに変換：**
  封じ込められた安全な環境で攻撃を完全に実行させることによってユニークな脅威データを取得し、自社のビジネスが直面している脅威に対する理解を深めることができます。クラウドベースのインテリジェンスと、エンドポイントを介して収集されたデータを活用し、脅威データの収集を強化するとともに、IoTプリントデバイスからのアラートをSIEM（Security Information and Event Management）システムに自動送信することによって、自社のビジネスのセキュリティの状態について包括的な視点を得られます。

これらはすべて、HPが最優先としている目的に結び付いています。HPは、前例のないレベルのサイバーリスクに対処する中で高まり続けるIT部門やセキュリティ部門の負荷を軽減し、ユーザーやお客様が自宅から、またはリモート環境で、安全に働き続けられるようにサポートします。詳細は、「HP Wolf Security」のWebサイトをご覧ください。

調査方法

本レポートの調査結果は、異なる4つのデータソースより作成されています。

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。対象は、パンデミック前に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。調査は2021年3月17日~25日にオンラインで実施。

02 米国、英国、メキシコ、ドイツ、オーストラリア、カナダ、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。

03 2020年3月にKuppingerColeが実施した調査レポート「The 2020 Cybersecurity Threat Landscape for Remote Workers as a Result of the COVID-19 Pandemic」。本レポートは、世界中の企業と従業員の行動や慣行に加えて、環境の変化によって生じた脆弱性に対する悪意のあるアクターの活動や動向に着目し、コロナ禍に伴い2020年に変化した労働環境の状況と分析を提示。

04 HP顧客の「HP Sure Click仮想マシン」から収集した脅威データと、HP Threat Intelligenceチームによる分析。

免責条項

[1] 「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。

[2] 「HP Sure Access Enterprise」の利用には、Windows 10 ProまたはWindows Enterpriseが必要です。HPのサービスは、ご購入時にお客様に提供または提示される、当該HPサービスに適用される使用条件に準拠します。お客様によっては該当地域の法令に従ってその他の法的権利を有することがあり、その場合には当該権利はHPサービスお取引条件またはお使いのHP製品にとともに提供されるHP限定保証条件による影響を一切受けません。システム要件の詳細は、 https://www.hpdaas.com/requirements/ja を参照してください。

HP WOLF SECURITY

© Copyright 2021 HP Development Company, L.P.
記載内容は、予告なく変更する場合があります。HP 製品およびサービスに関する保証条件は製品およびサービスとともに提供される保証書に明示された保証条件のみによるものとします。本レポートの記載内容はいかなる追加保証をも行なうものではありません。HP は本レポートの記載内容に技術上、または編集上の誤り、記載漏れがあった場合でも何ら責任を負わないものとします。