HP WOLF SECURITY

REBELLIONS & REJECTIONS REPORT

IT部門と従業員の確執

HP WOLF SECURITY

エグゼクティブサマリーと主な調査結果

世界的なパンデミックによって、企業はオフィスを基本とする働き方から、ダイナミックでハイブリッドな働き方を標準とするモデルへの迅速な移行を余儀なくされました。この新しい働き方は、短期的な傾向ではありません。「HP Wolf Security Blurred Lines & Blindspots～曖昧になる境界とセキュリティの死角」レポート(https://jp.ext.hp.com/content/dam/jp-ext-hp-com/jp/ja/ec/lib/info/newsroom/2021_hp_wolf_security_blurred_lines_report.pdf)によると、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くことを期待しており、16%が在宅勤務とオフィス勤務の半々で働くことを期待しています。

パンデミックによって、数日で変わらざるを得なかった企業は、デジタル技術をフル活用することにより、それを実現しました。しかしながら、デジタルイノベーションにはセキュリティが不可欠であるということは忘れられがちです。セキュリティ部門は、ビジネスを可能にするという極めて重要な役割であるにもかかわらず、新たな制限を課せられて抵抗する従業員から拒否されているように感じています。

従業員が在宅勤務を余儀なくさせられるという混乱の中、サイバー犯罪が拡大し、その猛攻撃の痕跡がさまざまな地域で確認されました。大手アナリスト企業KuppingerColeの分析によると、2020年には世界中でインターネットに接続されたエンドポイントは、1分間に1.5回の攻撃を受けました。

不運にも、サイバー犯罪の革新性と創造性が増したこの期間は、企業が流動的であり、事業継続のために迅速に行動しなければならなかった時期と重なっていました。このことは、サイバー犯罪の増加、セキュリティの可視性の低下、IT部門の管理範囲を超えた場所で働く分散された従業員の増加といった問題が入り混じった状況をもたらしました。

セキュリティ部門のリーダーにとって、この迷路から抜け出すことは大きな課題となるでしょう。そして、それは自部門だけでは達成できません。従業員は、仕事で毎日使用する技術に対し、新たな期待を抱いており、ワークフローを妨げないシームレスな体験を求めています。物事が速やかに進むことを期待し、邪魔されることを拒みます。特に若年層です。その結果、サイバーセキュリティ部門は、セキュリティの境界がなくなっていく職場を守ろうと苦戦し、その努力が無視されると燃え尽き、落胆します。したがって、従業員とサイバーセキュリティ部門のギャップを埋めることが、今後の働き方を守る上で重要なのです。

セキュリティ部門のリーダーシップは、かつてないほど重要です。また、サイバーセキュリティが役員会の議題で最優先事項となっている今、最高情報セキュリティ責任者 (CISO) の役割が変化しつつあります。最も成功を収めるCISOは、幅広いスキルを活用してリスクをコミュニケーションし、理解を得て効果的に管理できる人でしょう。これを実現する鍵は、前向きなセキュリティ文化を組織に根付かせ、それを全員が受け入れることです。セキュリティのプロセスを、ユーザビリティと事業継続性を念頭に置いて策定し、その一方でサイバーセキュリティ部門には最も高度なセキュリティツールを導入して可視化を向上させ、リモート環境下での管理を可能にします。サイバーセキュリティ部門を、セキュリティの強制的な執行者ではなくパートナーとして位置付けられるようにします。

2回目となる今回のHP Wolf Securityレポートでは、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のオンライン調査データと、1,100人のIT部門の意思決定者を対象に実施したグローバル調査データに、大手アナリスト企業KuppingerColeによる分析結果を収集しました。本レポートは、従業員とセキュリティ部門の関係性に焦点を当て、変化の必要性を浮き彫りにしています。

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。

- **従業員との軋轢：**
  調査結果では、多くの従業員がセキュリティポリシーについて理解不足であることが示されています。多くの人が、セキュリティを業務の妨げと見なしており、在宅勤務中にセキュリティの技術や制御をすり抜けようとしていました。このことは特に、18歳から24歳の次世代の従業員に当てはまり、無視できない傾向です。

- **妥協、リスク、拒否：**
  サイバーセキュリティ部門は、データ漏えいに繋がる可能性がある問題を警告しても聞いてもらえないと感じていることも、データに示されています。サイバーセキュリティ部門は、コンプライアンスの低下、可視性の低下、サイバーリスクの高まりが見られる中で、事業継続のために、セキュリティを妥協せざるを得ないプレッシャーを与えられています。

- **社内の懸け橋としてのCISOの役割：**
  こうした状況に介入しなければ、軋轢とリスクが高まる可能性があります。セキュリティ部門のリーダーは今、ダイナミックで柔軟で安全な働き方確保のために基盤固めを行う責務があります。また、CISOは、成功に導くためにサイバーセキュリティ部門と従業員の間のぎくしゃくした関係をパートナーシップに変えるという前向きな役割も担っています。CISOはこれまで以上に、交渉や、コミュニケーション、人材管理のスキルが必要になるでしょう。

「HP WOLF SECURITY」の視点：

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

「従来型の境界型防御による職場環境は、パンデミック終息後に向け分散型労働というハイブリッドモデルに移行しています。避けられない事態に抵抗するよりも、変化を受け入れ対応する企業がトップに立つでしょう。これは痛みを伴わずには実現できないプロセスであり、強力なリーダーシップとコミュニケーションが必要です。サイバーセキュリティ部門は、新しいハイブリッドな職場環境において、目的に合ったセキュリティの導入を優先する必要があります。その一方で従業員は、会社のセキュリティに対して責任を持つ必要があります。」

主な統計データ

オフィスワーカーの視点

無関心

39%	18歳から24歳までのオフィスワーカーの**39%**が、自社のデータセキュリティポリシーについてよく理解していませんでした。
36%	オフィスワーカーの**36%**が、自宅のネットワークを保護する方法について研修を受けていました。
54%	18歳から24歳までのオフィスワーカーの**54%**が、組織がデータ漏えいにさらされることよりも業務の期日に間に合うかどうかを気にしています。

フラストレーション

48%	18歳から24歳までのオフィスワーカーの**48%**が、セキュリティポリシーを業務の妨げだと考えていました。
37%	オフィスワーカーの**37%**が、セキュリティポリシーや技術の制限が厳し過ぎると回答しています。
48%	オフィスワーカーの**48%**が、セキュリティ対策によって多くの時間が無駄になっていると回答しています。

回避

31%	18歳から24歳までのオフィスワーカーの**31%**が、セキュリティを回避しようとしていました。

主な統計データ

IT部門の視点

妥協

76%	IT部門の**76%**が、パンデミック中は事業の継続を優先してセキュリティが後回しになっていたと回答しています。
91%	IT部門の**91%**が、事業の継続のためにセキュリティを妥協しなければならないというプレッシャーを感じていました。
83%	IT部門の**83%**が、在宅勤務がネットワークの侵害を招く「時限爆弾」につながっていると考えています。

制限

91%	IT部門の**91%**が、在宅勤務の増加に伴いセキュリティポリシーを更新しました。
78%	IT部門の**78%**が、Webサイトやアプリケーションへのアクセスを制限しました。

落胆

80%	その結果、IT部門の**80%**が従業員からの抵抗に遭っていました。
80%	IT部門の**80%**が、ITセキュリティは報われない仕事になってきたと回答しています。
69%	IT部門の**69%**が、従業員に制限を課すことで自分たちが悪者であるかのような気分にさせられていると回答しています。

無関心とフラストレーションが抵抗の原因なのか？

全世界でのリモートワークへの移行は、エグゼクティブから現場まであらゆる人に影響を及ぼし、誰もが適応しなければなりませんでした。ストレスは多いものの、全般的に見ると、人々が危機に対してしっかり団結していることは注目に値します。

その一方で、混乱と変化は緊張をもたらし、軋轢を悪化させる可能性があります。オフィスワーカーを対象に実施したYouGovのグローバル調査から、3つの問題が浮かび上がりました。

- 1つ目は、在宅勤務者がサイバーセキュリティを自分には関係の無いことと感じており、無関心であること。これは、コミュニケーションとトレーニング不足が原因の可能性があります。
- 2つ目は、リモートワークのリスクを管理する上で役立つセキュリティポリシーとツールが、従業員の生産性に及ぼしている悪影響と、それによって生じている軋轢です。
- 3つ目は最も懸念すべき内容で、従業員は業務を片付けるために、サイバーセキュリティ部門の管轄外でセキュリティを回避しているという事実です。

特に若い世代の従業員の間で、セキュリティに対する意識の低さが目立ちます。安全に在宅勤務を行うためのセキュリティポリシーとガイドラインをどのくらい明確に理解しているかという質問に対し、18歳から24歳までのオフィスワーカーの39%が、セキュリティポリシーの内容を明確に把握していないか、まったく知らないと回答しています。これは、全体の世界平均（29%）よりも10%高い割合となっています。この無頓着さが、攻撃者に無数の侵入ポイントを与え、結果的にサイバーインシデントに発展する可能性があることを考えると、この数字は安心からほど遠い状況にあります。

在宅勤務を行う際、従業員は大きなセキュリティリスクに直面します。それに伴い、ホームネットワークとそれに接続されているエンドポイントへの注目が高まっています。KuppingerColeの分析によると、在宅勤務によってもたらされるITインフラとネットワークの分断は、今やグローバルリスク専門家にとって最大の懸念事項となっています。さらに、KuppingerColeが引用していた欧州連合の調査では、2020年に欧州の従業員の40%が在宅勤務環境でセキュリティに関する問題を抱えていたことが分かっています。

図1：在宅勤務を開始してからホームネットワークの保護方法について追加の研修を受け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
36%	44%	50%	38%	27%	23%	30%	42%

「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）

「従業員が自らセキュリティを回避しているという事実は、CISO（最高情報セキュリティ責任者）にとって懸念すべき点でしょう。セキュリティがあまりにも煩わしく重荷になるようであれば、従業員は抜け道を探します。このような状況からセキュリティ侵害が起こり得ます。そのため、セキュリティは目立たず、設計に組み込まれ（Secure by Design）、ユーザーが直感的に使用できるテクノロジーを用い、既存の業務パターンやフローにできる限り適合されるべきです。最終的には、セキュリティを回避した状態と同じ気軽さで安全に業務を行えるようにする必要があり、システムの中にセキュリティを初めから組み込むことでそれが可能となるのです。」

18歳から24歳までのオフィスワーカーの54%が、データ漏えいにさらされることよりも期日の方を懸念。

18歳から24歳までのオフィスワーカーの31%が、業務を片付けるために会社のセキュリティポリシーを回避しようとしたことがあると回答。

それにもかかわらず、オフィスワーカーの64%が、ホームネットワークを保護するための追加研修の機会を与えられていませんでした。これは、地域差も顕著でした。このような研修を受けた従業員は、米国で38%、カナダで44%であるのに対し、英国は23%と最も低く、日本はそれよりもわずかに高い30%となっています。さらに、安全に在宅勤務を行う上で役立つ追加の技術的リソース（セキュアなWi-Fiネットワークなど）を与えられた従業員は36%にとどまりました。

このように、サイバーセキュリティ対策への取り組み不足が、従業員の無関心さを広げる要因となっています。全体で見ると、オフィスワーカーの36%が、組織がデータ漏えいにさらされるというリスクを負うよりも、自分が期日に間に合わせることの方が重要な懸念事項であると考えています。さらに、8%がどちらを優先させるべきか分からないと回答しており、彼らの無関心さが明らかになりました。ここでも、若い世代の回答者の割合がより当惑させる結果になっています。18歳から24歳の半数以上（54%）が、データ漏えいよりも自分の期日の方が重要であると考えており、9%が分からないと回答しています。これは、セキュリティが組織の中で担っている重要な役割、または自分が、従業員として組織を攻撃から守る上で果たせる役割について、理解や関心が不足していることを示しています。

図2：セキュリティツールは役立つよりも妨げとなることが多いと思っているオフィスワーカーの年齢層別割合

全体	18～24歳	25～34歳	35～44歳	45～54歳	55歳以上
34%	48%	40%	35%	31%	23%

もうひとつの主要な調査結果は、オフィスワーカーは、セキュリティポリシーや技術が日常業務の妨げになっていると考えていることでした。平均で世界中のオフィスワーカーの3分の1以上（34%）が、セキュリティが業務の妨げになっていると回答しています。ここでも、この傾向は特に若年層の従業員に見られ、18歳から24歳では48%、25歳から34歳では40%がそのように回答しています。

より詳細に尋ねると、従業員の37%が、セキュリティポリシーやセキュリティ技術の制限が厳し過ぎることが多いと考えていました。また、48%が、特に在宅勤務で必須とされているセキュリティ対策によって多くの時間が無駄になっていると考えていました。この割合は、18歳から24歳のオフィスワーカーでは64%に増加します。セキュリティで時間が無駄になると感じていた回答者のうち、82%が煩わしいセキュリティ対策で月2時間から6時間を無駄にしていると推定しており、18%が月6時間以上を無駄にしていると回答しています。

そのため、オフィスワーカーの16%が、業務をより容易に片付けるために会社のセキュリティポリシーを回避しようとしたことがあることを認めています。この割合は、18歳から24歳の従業員では31%に増加します。

妥協、リスク、拒否

デジタルトランスフォーメーションの加速は、企業や雇用だけでなく、命さえも救いました。デジタルトランスフォーメーションは、企業が生き残ることだけでなく発展を遂げることも可能にしました。また、デジタルクリエイティビティの時代を先導し、人々はパンデミックに対応した新たな体験に向けた革新的かつ斬新な方法を見いだしました。それらの多くは今後も浸透するでしょう。

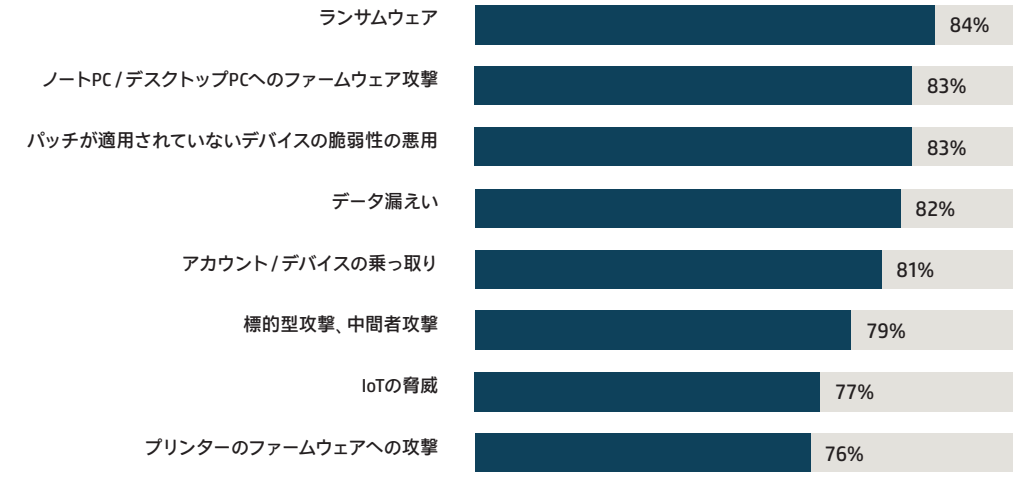
ところが、イノベーションを図っていたのは企業だけではなく、サイバー犯罪者も同様でした。IT部門を対象に実施されたTolunaの調査から、3つの問題が浮かび上がりました。

- 1つ目は、企業が直面する脅威の種類と規模に応じて、サイバーセキュリティ部門はビジネスを守るためにかつてないほど懸命に取り組んできたにもかかわらず、今では疲労困憊していることです。
- 2つ目は、サイバーセキュリティ部門は、事業継続のためにセキュリティを妥協しなければならず、多くがジレンマを感じていることです。
- 3つ目は、サイバーセキュリティ部門はビジネスを安全に保つために、自分たちの取り組みに抵抗する従業員に対処しなければならないことです。

サイバーセキュリティ部門は、ますます効率を高めているセキュリティリスクの脅威に直面しています。一方で、新しいポリシーやいっそう厳しくなる制限は従業員から拒否されています。その結果、IT部門の83%が、在宅勤務は会社のネットワークの侵害を引き起こす可能性がある「時限爆弾」になったと考えています。

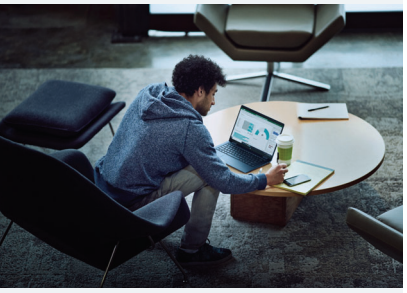
企業が現在直面している脅威の種類と深刻さについて尋ねると、IT部門の84%が、ランサムウェアを重大または極めて重大なリスクと受け止めています。その他の脅威として、PCへのファームウェア攻撃や、パッチが適用されていないデバイスの脆弱性（83%）、データ漏えい（82%）、アカウント/デバイスの乗っ取り（81%）、標的型攻撃および中間者攻撃（79%）、IoTの脅威（77%）、プリンターのファームウェアへの攻撃（76%）などが挙げられます。

図3：セキュアでない可能性があるネットワークを使用した在宅勤務が増える中、IT部門が考える攻撃方法別脅威レベル



IT部門の91%が、事業継続のためならばセキュリティを妥協しなければならないというプレッシャーを感じていると回答。

しかしながら、脅威のレベルが高まっているにもかかわらず、IT部門の76%が、パンデミック中は事業の継続が優先され、セキュリティを後回しにされたと感じています。また、同じ割合の回答者が、セキュリティを停止するように指示され、イノベーションを実現する手短な方法を構築するようプレッシャーをかけられています。さらに、ほぼ全員（91%）が、事業の継続のためならばセキュリティを妥協しなければならないというプレッシャーを感じており、そのうち50%が「相当の」プレッシャーを感じています。



「HP WOLF SECURITY」の視点：

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

「CISOは、高まり続ける攻撃の量、スピード、重大性に対処しています。CISOのチームは、ビジネスを安全に保ちつつ、可視性が減少する中で大規模なデジタルトランスフォーメーションを推進するために昼夜を問わず仕事をしなければなりません。その一方で従業員は、会社の安全を守る上での自分の役割に対して十分に理解していません。一人一人が果たすべき重要な役割を理解し、セキュリティは企業の全体責任であることを認識する必要があります。」

IT部門の69%が、ユーザーに「ノー」と言わなければならないため、悪者にされている気分になることがあると回答。

図4：パンデミック中は事業の継続が優先され、セキュリティを二の次にしなければならないことがあったと回答したIT部門の国別割合

	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
相当なプレッシャーを感じている	50%	57%	55%	43%	32%	62%	55%	48%
ある程度プレッシャーを感じている	41%	37%	41%	44%	49%	33%	38%	48%

当然ながら、このような妥協を続けることはできません。新しい社会は安全でダイナミックである必要があり、そのどちらかということはあり得ません。しかし、過去にさかのぼって誤りや手抜きを修正するのは簡単なことではありません。このような状況になってしまった今、元に戻すことは不可能です。従業員は、これまでと同じレベルの自由が継続すると期待するでしょう。

セキュリティ部門は、当然ながらリスクを軽減する方法を模索してきましたが、従業員からの抵抗に遭っています。IT部門の91%が、在宅勤務の増加に伴いセキュリティポリシーを更新しており、78%がセキュリティの理由から、Webサイトやアプリケーションへのアクセスを制限しています。しかし、Webサイトやアプリケーションへのアクセス制限をしたIT部門のうち93%が、そうした制限が生産性を下げると、従業員がフラストレーションを示したと回答しています。

さらに広く見てみると、IT部門の80%が驚くべき頻度で、在宅勤務中に課される制御を気に入らない従業員からの抵抗に遭ったと回答しています。IT部門の18%が、正当な作業が妨げられている、セキュリティポリシーやシステムによってブロックされるといった従業員からの苦情を毎日、22%が数日おき、27%が毎週受けたと回答しています。

サイバーセキュリティ部門は最終的に、負け戦をしているように感じています。IT部門の83%が、プライベートと仕事の境界が非常に曖昧になっている今、サイバーセキュリティに関する企業ポリシーを策定し強制することは不可能であると回答しています。さらに80%が、在宅勤務者は助言に耳を傾けてくれないため、ITセキュリティが報われない仕事になってきたと回答しています。

図5：リモートワークによるセキュリティと利便性のジレンマの複雑化

リモートワーカーの増加に伴いセキュリティポリシーを更新しているIT部門の割合	91%
現在、セキュリティのためにWebサイトやアプリケーションへのアクセスを制限しているIT部門の割合	78%
在宅勤務中に課される制御を不満に思うユーザーからの抵抗に遭っていると回答したIT部門の割合	80%
サイバーセキュリティに関する企業ポリシーの策定は報われない仕事であると回答したIT部門の割合	80%
在宅勤務者の増加は、企業ネットワークの侵害を招く「時限爆弾」となっていると回答したIT部門の割合	83%
プライベートと仕事の境界が非常に曖昧になっている今、サイバーセキュリティに関する企業ポリシーを策定し強制することは不可能であると回答したIT部門の割合	83%

その結果、ITセキュリティ部門は悪人役をさせられているように感じており、69%が悪者のような気分にさせられていると回答しています。

要約

「HP Wolf Security Rebellions & Rejections ~ IT部門と従業員の確執 ~」レポート調査結果の要約 :

- 従業員とサイバーセキュリティ部門との間に軋轢があるという考えは新しいものではありませんが、そうした課題はパンデミックによって深刻になり、関係がさらに悪化し、問題が増幅しています。
- 多くのオフィスワーカーが、自分に組織を守る役割があるとは思っておらず、また無関心です。
- 多くのユーザーがITセキュリティにいら立ちや煩わしさを感じ、抵抗しています。また、多くのユーザーがITセキュリティの境界を越えて仕事をしています。
- このことが、ビジネスを守るというプレッシャーに直面しているセキュリティ部門の仕事をつらいものにしており、その結果としてセキュリティ侵害が差し迫っていることを多くの回答者が懸念しています。
- ITセキュリティ部門は、ユーザーのために境界を設定することに関して、正当に評価されず、いら立ち、誤解されていると感じ、自分たちの役割は実行不可能で報われない仕事になってきたと考えています。

HP WOLF SECURITYの最終的な見解

目的に合ったセキュリティポリシーと制限にするための見直し

セキュリティは安全実現のためのイネーブラーです。人々はセキュリティをプライベートでは受け入れています。預金残高の確認も、オンラインでの買い物も、コミュニケーションも、安全を確保する方法がなければ何もできないことを理解しています。結局は、セキュリティを提供するガードレールが人々の安全を守っています。

ところが仕事となると、人々はセキュリティによって安全に業務を行えることよりも、業務が妨げられるということに注目しがちになります。目先のことにとらわれているように思えますが、理解もできます。新しいハイブリッドな働き方では、会社のファイアウォールによる保護がないまま業務を行うことが多いため、サイバーセキュリティ部門は従業員にさらに制限を課したくなります。しかしながら、そうしたセキュリティポリシーや制限は、ハイブリッドな働き方が標準ではなく特例だった時に策定されたものであるため、今は新しい視点で捉え直す必要があります。

成功を収めているCISOはこの点を認識しています。エンドユーザーにいっそう耳を傾け、セキュリティがエンドユーザーの業務フローや生産性にどのような影響を与えるかを理解し、組織とハイブリッドワーカーの両方のニーズに基づいてセキュリティを再評価しています。

燃え尽き症候群に陥っているサイバーセキュリティ部門へのさらなるサポート

本レポートでは、パンデミックの中、サイバー攻撃が高度化する一方で、在宅勤務の従業員の行動が把握できず、コンプライアンスへの意識の低下が進むことが組織の防御をいっそう難しくし、セキュリティ部門にとって困難な時であったことが示されています。

セキュリティ部門は、ハイブリッドな職場環境に適応し、高度なリモート管理を提供しながらもエンドユーザーによるセキュリティの回避を避けられるよう、企業のネットワーク外における新たなレベルのエンドポイント保護を模索しています。

もはやサイバーセキュリティ部門のみがビジネスのセキュリティ保護の責任を負わされるべきではありません。この責任は、全従業員が共有する必要があります。サイバーセキュリティはエンドツーエンドの規律であるということを企業が理解するまで、攻撃に対して脆弱になるだけでなく、大幅に不足しているサイバーセキュリティの人材を新たに雇用したり、雇用を維持することがますます難しくなるでしょう。

「HP WOLF SECURITY」の視点：

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

「サイバーセキュリティは、誰もが受け入れられるものにするべきです。サイバーセキュリティ部門はビジネスの安全を保つ必要がありますが、従業員も自身の役割を果たす必要があります。身体的な安全性と同じように、オフィスに階段があれば、手すりを設置して、利用者が滑ったり転んだりしないよう、おそらくタイルの代わりにカーペットを敷く必要があるでしょう。しかしそれと同時に、企業は利用者が3人で一斉に階段を駆け下りてけがをすることはないと信じています。サイバーセキュリティ部門はそのようなガードレールを提供できますが、利用者にも慎重に歩いてもらう必要があります。このハイブリッドな働き方の新しい時代を生き抜くために、全員が一丸となって会社が危険にさらされないように守る方法を私は考えています。」

協調性を向上させたセキュリティ文化の構築

CISOは、サイバーセキュリティに関する議題を役員会で優先しやすくなっており、企業戦略のあらゆる側面にサイバーセキュリティを盛り込む必要性を強調しています。今や、セキュリティを組織のDNAに組み込むために、自社のあらゆるビジネス分野と連携しなければなりません。

サイバーセキュリティ部門は、エンドユーザーとのコミュニケーションの糸口を見つける必要があります。協調性を向上させたセキュリティ文化の構築においては、明確で説得力のあるコミュニケーションと、従業員に働きかける研修や教育が鍵となります。セキュリティに関する意思決定の論理的な根拠を提示することや、一方通行の指示から脱却して新しい方針を導入する前にユーザーの意見を求めることなど、シンプルな調整によって受け止められ方が大幅に変わるでしょう。従業員全員で協調性のあるセキュリティパートナーシップを築くことによって、サイバーセキュリティは文化の礎となり始めます。

そのような懸け橋を築くために、CISOは、人材の管理やコミュニケーションなどの幅広いスキルが求められます。そうしたスキルは、多様性があり豊富な才能を持つチームから最も生まれやすく、より幅広い従業員に対して動機付けし、サイバーセキュリティとそのメリットを訴求できます。

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

本レポートで示されているとおり、従業員がユーザーフレンドリーなセキュリティツールと制限の軽減を強く求めている一方で、プレッシャーを受けているサイバーセキュリティ部門はセキュリティの負担を軽減しユーザーの行動と脅威に関する可視性を向上させる方法を見いだす必要があります。それらの両方を実現する上で、テクノロジーが重要な役割を担っています。お客様が、ハイブリッドな働き方の新しい時代にそれを実現できるようにすることが、HPの原動力です。

邪魔にならないセキュリティ技術をエンドポイントに組み込むことは、ビジネスに必要な保護を提供した上で、ユーザーに優れたセキュリティ体験を提供することに大いに役立ちます。セキュリティが追加されるのではなく内蔵されたPCやプリンターなどのエンドポイントによって、いっそうシームレスなエンドユーザー体験を提供でき、使い勝手の制限を緩くすることが可能になります。

サイバーセキュリティ部門は「HP Wolf Security」によって、ユーザーフレンドリーなツールを提供し、使い勝手の制限を緩くすることができます。また、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、ビジネス全般を保護します。

「HP Wolf Security」は、ゼロトラストの原則に基づき、セキュリティの負担の軽減に役立ちます。「HP Wolf Security」のソリューションは、ハードウェアに組み込まれたレジリエントなセキュリティによって、自己モニタリングと自己回復を徹底的に行うとともに、総合的な可視性を実現するリモートでの管理機能を提供します。これによって、サイバーセキュリティ部門は、OSの下、OS内、OS上の脅威の影響をプロアクティブに軽減し、ユーザーに対して透明性を維持することができます。

「HP Wolf Security」は、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、Webサイトへのアクセスの制限を受けることなく、あるいは従業員がメールの添付ファイルを開くことを制限することなく、内蔵された堅牢な保護機能のメリットを享受できます。ユーザーは、中断なく業務に取り組めます。ユーザーを妨害しない保護機能を提供している最新技術の例は以下のとおりです。

- **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は封じ込められた脅威と共に破棄されます。したがって、ユーザーが不適切なものをクリックしても、攻撃者はどこへも進入できず、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管理します。

- **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 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 Enterprise」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。

「HP WOLF SECURITY」について

世界で最も安全なPC[3]およびプリンター[4]のメーカーであるHPが提供する「HP Wolf Security」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 Security」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

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。

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。

[3] 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。

[4] 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。

HP WOLF SECURITY

© 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。