エンドポイントがセキュリティリスクにさらされる5つの理由

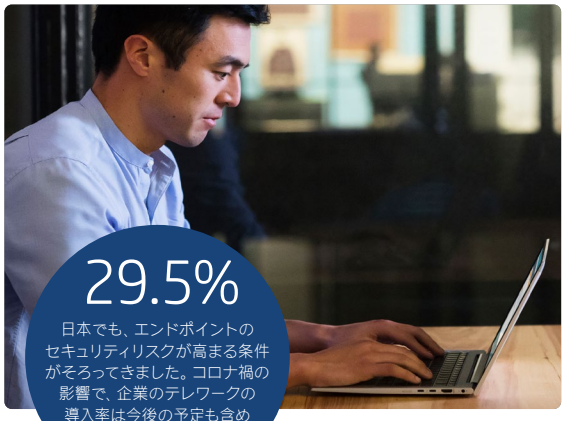
サイバーセキュリティの脅威は日々進化し、組織はエンドポイントのセキュリティの脆弱性に常に対応し続けなければいけません。

混乱の原因に対抗する

現代のサイバーセキュリティはデバイス保護を複雑なタスクにしてしまい、組織は十分な防御策がないままに脅威にさらされています。日本ではサイバー攻撃が著しく増えています。過去2年間で経済犯罪・不正の被害に遭ったと申告した組織の36%がサイバー犯罪を受けており、多種ある経済犯罪被害の中で1位（2018年比15ポイント増）となりました（出典1）。

ターゲットとしてのエンドポイント

サイバー攻撃はエンドポイントを対象にしており、その傾向はますます高まっています。2018年にPonemonがグローバル企業のITおよびITセキュリティの専門家に対して調査を行った結果、約2/3の回答がエンドポイントから重大なセキュリティインシデントが始まっていると報告しています。これは前年比で17%増となります（出典2）。年を追うごとにサイバー攻撃のレベルが高まり、対策が複雑になる一方、エンドポイントのセキュリティ対策がおろそかになっているのが現状と言えます。以下に、エンドポイントが貴社に脆弱性をもたらす5つの理由を示します。



29.5%

日本でも、エンドポイントのセキュリティリスクが高まる条件がそろってきました。コロナ禍の影響で、企業のテレワークの導入率は今後の予定も含め29.5%に上ります（出典3）

01.

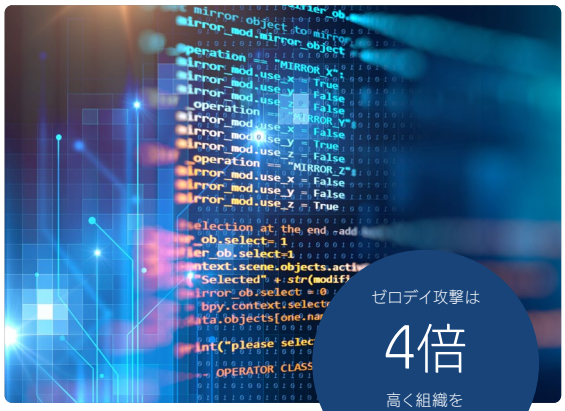
仕事の場は分散しつつある

オフィスに縛られていた従業員が、今や自宅やカフェ、移動先でリモートワークすることが一般的になりつつあります。東京都では、すでにテレワークを導入している企業や現在検討中の企業を合わせると、テレワークの導入率は45.6%（出典4）に上る一方、ランサムウェアによる業務の停止、情報漏洩によるセキュリティインシデントも急激に増加しています。テレワークの普及に伴い、社内ネットワーク外へのデバイスの持ち出し、VPNを利用した組織ネットワークへの接続、パブリックWifiへの接続が増加し、それらの脆弱性を突いたサイバー攻撃のリスクがますます高まっています。

02.

従業員は脅威を見逃す恐れがある

成功したサイバー攻撃のほとんどは人の弱点を突くものです。Ponemonによれば、中小企業におけるデータ漏洩やランサムウェア攻撃の大半は人為的ミスによるものです(出典5)。従業員が気づかないうちにサイバー攻撃を許す発端となる可能性は、非常に高いと言ってよいでしょう。



03.

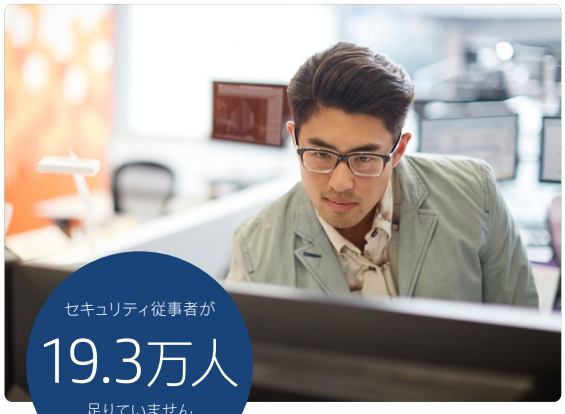
アンチウィルスソフトはもう十分ではない

エンドポイントの十分な保護のために、組織は旧来のアンチウィルスソフトについて考え直す必要があります。エンドポイント攻撃の半分以上はアンチウィルスソフトに見逃されており(出典2)、セキュリティの脆弱性の発見、対処方法の確立、そして修正プログラムが提供されるまでの間に攻撃を受けるゼロデイ攻撃も、主流になりつつあります。メールやブラウザのリンクおよびダウンロードを介してシステムに解き放たれたゼロデイ攻撃は、既知の攻撃よりも4倍高く組織を危険にさらします(出典2)。

04.

見えない脅威はより危険に

攻撃を許した組織のシステムは、数分以内に何らかのセキュリティの脅威にさらされる恐れがあります。しかし、2/3の脅威は攻撃後1か月以上経っても発見されません(出典7)。デバイスの監視を怠り脅威への対応が遅れることで、組織はさらに継続的にデータを漏洩し、やがて大きな経済的損失を被ることになります。



05.

専門知識の不足

セキュリティ脅威の増加にともない、日本では2020年にセキュリティ人材が19万3,000人不足すると総務省は見ています(出典8)。こうしたことから、今後はセキュリティ対策を人手に頼る割合を減らし、デバイス自体に脅威への対抗力を備えることが求められるようになります。

弱点を最強の防御へと変える

現在の組織にとって最新の課題とは、生産性の向上や協働、安全なリモートワーク環境を実現しながら、スムーズな運用と事業の継続性のバランスをとることといえます。

昨今のコロナ禍が原因で分散した仕事環境は、組織に対する脅威の範囲も拡大し、情報漏洩・経済的損失の危機に組織をさらしています。一方でITチームは、プライバシーやセンシティブなデータ保護の重圧が高まっているうえに、デバイスを横断的に見渡しながらリモート管理することに困難を覚えているのが現状です。

HPのデバイスとセキュリティサービスを組み合わせることによって、完全にリモートでセキュアな仕事環境に一歩近づくことができます。

HP Proactive Securityにより貴社の防御力をさらに強化します。メールの添付ファイルからのゼロデイ攻撃を防ぎ、拡散を阻止するリアルタイムの脅威隔離テクノロジーにより、すべてのエンドポイントを保護します。HPマネージドサービスを利用すれば、HPのセキュリティエキスパートがデバイスの保護状況を監視し、脅威を分析することで、貴社のITチームはより優先度の高いプロジェクトに集中することができます。

このように、HPのデバイスをHP Proactive Securityと組み合わせることで、エンドポイントを貴社の最大のリスクから最良の防護壁へと変えることができるのです。

詳しくはこちら

テクノロジーは人間の最大限の力を引き出すためにあり、いつもIT部門からその適用がはじまります。テクノロジーが日々進化する現在、ITに対するニーズも増え続けています。一方で、時間やリソース不足のなか、迅速かつ安全に解決しなければならない複雑な要件も増えています。そうした状況下でIT部門の人間は、自分たちの仕事に自主性が無く、コントロールできる要素が少ないと感じています。しかし、HPのサービスとセキュリティ、ハードウェアがそれらの問題を解消します。発生前に問題を解決するプロアクティブなデバイス監視から、統合されたクロスプラットフォームのセキュリティソリューション、適切な人材と機器の調達まで、HPはIT部門にとって本当に大切なこと——従業員の成功——を集中的に支援できるような環境を提供します。

参考文献欄：

出典 1 ：PWC「経済犯罪実態調査2020 日本分析版」, 2020年7月
出典 2 ：Ponemon Institute, 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018.
出典 3 ：総務省「令和元年 通信利用動向調査報告書（企業編）」, 2019年
出典 4 ：東京都産業労働局「多様な働き方に関する実態調査（テレワーク）結果報告書」, 2020年3月
出典 5 ：Ponemon Institute, 2018 State of Cybersecurity in Small & Medium Size Businesses, November 2018.
出典 6 ：Cofense, State of Phishing Defense 2018, 2018.
出典 7 ：Verizon, 2018 Data Breach Investigations report 11th Edition, 2018.
出典 8 ：総務省「我が国のサイバーセキュリティ人材の現状について」, 2018年12月