

【プレスリリース】

McAfee Enterprise & FireEye

2021年11月10日

McAfee Enterprise と FireEye は、
2021年10月のSTGによる12億米ドルでのFireEyeの買収手続き完了を受け、完全統合しました。

※当資料は、米国時間2021年11月9日に米国で発表されたプレスリリースの抄訳です。

サイバー攻撃の脅威、パンデミック以降81%が増加 McAfee Enterprise & FireEye、ホリデーシーズンに標的となる危険性が高い業界に注目

ニュースハイライト：

- グローバル企業の81%がコロナ禍にサイバー脅威が増加
- 今年のホリデーシーズンは「すべてが不足」 — サプライチェーン、eコマース、旅行に対するサイバー脅威の絶好の機会に
- 79%の企業がシーズンのピーク時にサイバーセキュリティリスクによるダウンタイムを経験

McAfee Enterprise & FireEye は、「*Cybercrime in a Pandemic World: COVID-19 (コロナ禍の世界におけるサイバー犯罪: COVID-19)*」を発表しました。本レポートで、組織がサイバーセキュリティを優先的に強化する必要性が差し迫っていることを明らかにしました。今回の調査結果によると、コロナ禍において、グローバル企業の81%でサイバー脅威が増加し、79%がピーク時にサイバーインシデントによるダウンタイムを経験していました。ホリデーシーズンが近づき、サプライチェーンや物流、eコマースや小売、旅行業界では、消費者や企業の活動が活発になることが予想されるため、サイバー脅威に対して脆弱になり、企業や従業員、消費者のデータを危険にさらすこととなります。

統合企業のCEOであるブライアン・パルマ (Bryan Palma) は、次のように述べています。「特にホリデーシーズンのピーク時には、すべての企業がセキュリティを優先し、安全を維持することが不可欠です。IT担当者の94%は、組織の全体的なサイバー対応力の向上を望んでいます。企業はより多くのことをしなければならず、今日の巧妙な脅威動向に対応するためのインテリジェントなセキュリティを必要としています。」

主要産業における主要ポイント

ホリデーシーズンは、個人消費の増加に加えて、消費者ニーズの高まりに対応する業界に大きな影響を与えます。86%の組織が、2021年のホリデーシーズンには例年と同等かそれ以上の大幅な需要の増加を見込んでいます。そのため今年は、労働力、物資、配送サービスなど「あらゆるものが不足する」という状況が現実となっています。このため、組織は実用的なセキュリティ計画を用意し、脅威を効果的に抑制して対応することが急務となっています。

サプライチェーンとロジスティクス

BCIの「[Supply Chain Resilience Report 2021](#) (英語)」によると、2020年にサプライチェーンにおける混乱が20回以上あったと報告した組織は27.8%で、2019年の4.8%から増加しています。製造・物流能力や労働力の低下と、商品需要の増加が相まって、サイバー犯罪者にとっては、潜在的な弱点、脆弱なインフラを突破するための絶好の攻撃経路となっています。サプライチェーン責任者は、リスクを特定し、セキュリティ侵害やサイバー攻撃による物流への潜在的な影響を理解し、インシデントが発生した場合に迅速に対応できるような計画を準備する必要があります。

e コマースと小売

アドビの「[2021 Digital Economy Index](#) (英語)」によると、2021年のホリデーシーズンにおける世界のオンライン支出は11%増の9,100億ドルになると予想されています。店舗の閉鎖やオンラインショッピングの増加に加え、限定商品の入手可能性、配送への不安といった状況の中で、この業界はかつてないほどの脅威にさらされています。McAfee Enterpriseの「[COVID-19 ダッシュボード](#) (英語)」によると、検出されたサイバー脅威のうちの5.2%を、グローバルな小売業界が占めています。脅威には決済認証情報やクラウドストレージへの侵害、小売業への詐欺や窃盗があります。

旅行

空港、航空会社、旅行サイト、相乗りアプリなどがこれまで被害にあっており、旅行業界にとってサイバー脅威は新しいものではありません。しかし、今年の特徴は、コロナウイルスに関連した健康上の懸念や旅行制限のために、旅行業界が膠着状態に陥っていることです。[国際航空運送協会 \(IATA\)](#)によると、2020年のコロナウイルス関連の損害額は1,377億ドルで、2020年から2022年の業界全体の損害額は2,010億ドルに達すると予想されています。今後数カ月にわたって旅行需要の増加が予想される中、サイバー犯罪者たちは、労働力不足、サプライチェーンの問題、渡航禁止、ワクチン接種の義務など、新たな課題に対する旅行業界の動向を注視しており、隙あらば脆弱性を利用して利益を得ようとしています。

企業が知っておくべきこと

IT担当者はサイバー脅威が激化していることを認識していますが、今回の調査結果では、コロナ禍において、セキュリティに対して企業が効果的に優先対応していないことが明らかになりました。

- 60%がオンライン・ウェブ上の活動が増加と回答
- テクノロジーおよびセキュリティ予算を削減したと33%が回答
- 56%がサイバーインシデントによるダウンタイムに悩まされたと回答し、10万米ドル以上の損害を被った企業も
- サイバーインシデント等への対応時に十分なセキュリティチーム/SOCの人員確保がさらに困難になると76%が回答

新たな脅威への対応

サイバー犯罪に対して組織が取るべき積極的かつ実用的な方法には、セキュリティ対策や業界のサイバーセキュリティ要件の導入、従業員へのサイバーセキュリティ意識向上を目的としたトレーニングの実施、予防・対応計画の策定などがあります。さらに、企業や商業施設は、最先端且つ、ローカルおよびグローバルから集積したデータを活用した[MVISION Insights](#)のようなソリューションを活用することで、特定業界を攻撃するのはだれで、何をターゲットとするのかを特定し、脅威や攻撃キャンペーンに対する防御を最適化するための事前の対応が可能になります。

コロナ禍の世界におけるサイバー犯罪 : COVID-19 調査方法 :

McAfee Enterprise と FireEye は、本研究のための調査を世界的な独立市場調査専門会社である MSI-ACI に委託しました。2021年9月から10月にかけて、1,451人のITおよび事業部門の意思決定者にインタビューを行い、定量的な調査を実施しました。調査対象は、米国、英国、オーストラリア、フランス、ドイツ、インド、シンガポール、南アフリカ、アラブ首長国連邦です。回答者は、ITセキュリティに関与しており、従業員数500人超の組織に勤務していることを条件としました。インタビューは、マルチレベルのスクリーニングプロセスを経て、オンラインで実施されました。

McAfee Enterprise & FireEye について

McAfee Enterprise & FireEye は、2021年10月のSTGによる12億米ドルでのFireEyeの買収手続き完了を受け、完全統合しました。両社のポートフォリオと知見を有する従業員が結集し、市場をリードするセキュリティ専門企業が誕生しました。実績あるテクノロジーと他に類を見ない経験を有し、世界中の40,000を超える企業、商業施設、政府機関の顧客にサービスを提供します。革新的なテクノロジー、インテリジェンス、自動化技術を融合し、顧客が抱える極めて複雑なサイバーセキュリティの課題解決をサポートします。詳細は、www.mcafee.com/enterprise および www.fireeye.com をご覧ください。

<本情報のお問い合わせ>

McAfee Enterprise & FireEye

広報担当 戸田

Tel: 070-2680-0731

hiromi_toda@mcafee.com