ニューノーマル処方箋（第3回）

その対策は効果ナシ！ セキュリティの常識を検証する

2021.02.19

サイバー攻撃の被害が深刻化し、従来のセキュリティの常識が崩れ始めています。本当に必要な対策とは何か？
情報セキュリティ大学院大学の大久保隆夫教授に聞きました。

＜目次＞

テレワークで企業のPCは危険にさらされている

サイバー攻撃による被害は、深刻化の一途をたどっています。その背景には、脅威やICT環境の変化に伴って、これまで常識とされてきた対策がもはや通用しなくなっている現実があります。

情報セキュリティ大学院大学の大久保教授は、過去に学んだセキュリティ対策を金科玉条のように守り続けているだけでは、変化し続ける脅威に適応できない時代が到来していると指摘します。

※1

などのセキュリティ製品で保護されてきた企業ネットワークから飛び出した環境で作業するようになったともいえます。その結果、“境界で守る”
（＝社内ネットワークとインターネットの間で守る）という従来のセキュリティの考え方が成り立たなくなっています」

テレワークで会社のネットワークに守られなくなったPCには、さまざまな脅威が懸念されています。大久保教授は、近年は特に「エンドポイント（従業員などエンドユーザーが利用するPC）が狙われたり、エンドポイント経由で社内ネットワークに侵入されたりして深刻な被害につながる脅威が増えています」と話します。

2016年頃に大きな話題となったランサムウエア※2
や、ここ数年の企業の情報漏えい事件でよく耳にする「標的型攻撃」も、最初の一歩はエンドポイントへの侵入がきっかけです。メールの添付ファイルを開いてしまったり、本文中のURLをクリックしたりしてジャンプした先のWebサイトから脆弱性を攻撃された結果、遠隔操作を行うマルウエアに感染し、そこから徐々に企業内に侵害を広げられてしまいます。

※1…IPS（不正侵入防止システム）は異常を通知するだけでなく、その通信をブロックする役割を担う。IDS（不正侵入検知システム）は通信を監視し異常な通信をブロックする
※2…感染した端末のデータを暗号化し、元に戻すための鍵と引き換えに金銭（主にビットコイン）を要求するマルウエア

情報セキュリティ大学院大学
情報セキュリティ研究科
教授
大久保隆夫 氏

「境界で防ぐ」という考え方は崩壊しつつある

前述のように、これまで多くの企業は、社内のネットワークとインターネットの「境界」にさまざまなセキュリティ製品を導入して脅威の侵入を防ぎ、内側を安全に保っていました。しかし、テレワークの広がりに伴ってこのセキュリティモデルは崩れ去りつつあります。

セキュリティ対策製品といえば、PCにインストールする「アンチウイルスソフト」が広く用いられ、その考えは「ウイルスの侵入を防ぎPCに感染させない」というものでした。ところがサイバー攻撃の高度化によって、近年では100%脅威を防ぐことは不可能です。

そこで現在では、“ネットワークはもはや信頼できない”という前提でセキュリティ対策を立てる「ゼロトラストセキュリティ」というアプローチに注目が集まっています。

「旧来のセキュリティモデルは、“境界でとにかく一生懸命守ろう”という発想でした。しかし、一度入り込まれてしまうと脅威を防ぐのは困難です。最近はそうではなく、『侵入されることもある』『感染する恐れはある』という前提でマネジメントや対応を考えるケースが増えています」（大久保教授）

この「ゼロトラスト」の考えで近年登場したセキュリティ対策が「EDR（Endpoint Detection and Response、エンドポイントでの検出と対応）」と呼ばれるソリューションです。

「単純に守るだけではなく、脅威の兆候を検知し、感染した場合でも速やかに対処して被害を最小限に抑える考え方が必要です。EDRであれば、それが可能になります」（大久保教授）

「PPAP」のパスワード対策はもはや意味がない… 続きを読む