

経済産業省が警鐘を鳴らす 最新のサイバー攻撃への対応を

2020年12月18日、経済産業省が昨今のサイバー攻撃の状況を踏まえた注意喚起を公表した。そこで、今号ではその内容を確認するとともに、有効な対策を講じてみたい。

攻撃パターンの多様化により 急拡大中のサイバーリスク

の標的が拡大してきている」と分析する。

経済産業省が公表したサイバー攻撃に関する注意喚起では①中小企業を巻き込んだサプライチェーン上での攻撃、パターンの急激な拡がり②大企業・中小企業等を問わないランサムウェアによる被害の急増③機微性の高い情報の窃取等を目的としたと考えられる海外拠点を経由した攻撃の深刻化が指摘されている。

まず①について、長年にわたってセキュリティシステムの提案をしている株式会社ブロード（東京都千代田区）は「昨今は中小企業もグローバルなサプライチェーンの一端を担うことが増えており、それにとまってサイバー攻撃のリスクが急速に高まっている。また、従来は著名企業データの流出などの被害が中心だったが、最近では取引先や委託先、社外要員などを通じて、そ

の標的が拡大してきている」と分析する。

②についてはランサムウェアがキーワードとなる。英語の「Ransom」（身代金）に由来するマルウェアの一種で、もともとはユーザーのパソコンに暗号化（圧縮ファイルにパスワードをかけてしまうような状態）を施して使用できないようにし、それを解除するパスワードの代償として金銭を要求するという手口が一般的だった。しかし、今回の注意喚起によると「暗号化する前にあらかじめデータを窃取しておき、身代金を支払わなければならないデータを公開するなどと脅迫する、いわゆる『二重の脅迫』を行うランサムウェアの被害が国内でも急増」しており日本におけるランサムウェアの被害額はもはや世界2位に達してしまっているという。

③に関しては、①のサプライチェーンと似ているところもあるが、今回の注意喚起はとくに海外拠点でのセキュリティ対策や管理を問題視している。この点について、経済産業省は「重要情報に係わるシステム分離、脆弱性対策の迅速なアップデート適用、振る舞い検知など最新の対策導入」を提案しているが、はたしてそれは企業や組織にとって現実的な対策なのだろうか。その点について、前出のブロードは「つねに全体を最新の状態に維持するには膨大なコストと時間がかかり、現実的ではない。また、これらの対策に投資してきた企業においても、あらたなマルウェアによる侵害が起きつつづけている」としている。

「Bromium」の導入が 万全のセキュリティ対策に

こうしたなかで注目されているのが、ブロードが日本総代理店を務めている米国発のセキュリティ製品「Bromium（ブロミ

ウム（現HP S C E）」だ。

この製品の特徴は仮想技術を用いて、パソコン本体から隔離された仮想環境でウェブサイトを閲覧したり、文書ファイルを安全に開いたりできること。そのため「いかにランサムウェアやマルウェアが攻撃してきても、パソコン本体にはまったく影響がない」という。また、同様に「進化型のランサムウェアがパソコン上のデータを外部に送信しようとしても、仮想パソコンには盗られるデータが入っていないので安心だ」という。

ブロミウムにはこのほかにもパソコンごと導入できる、一般的なセキュリティソフトのようにアップデートしなくてもセキュリティレベルを維持できるといった利点があるので、中小企業もスムーズに導入することができるといえる。これを機にブロミウムを軸にしたセキュリティ環境を構築してはどうだろうか。

もう無駄な時間と費用は「0」にしましょう



おかげさまで Bromium は
HP Sure Click Enterprise に進化しました

エンドポイントのサイバー対策に関する費用や専門家は、もう必要ありません。
100%* 防御し、レポートします。是非ブロードにお問い合わせください。

*2013年以降、Bromiumは推計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。(Bromium社調べ)

詳細は [BROAD Security Square] で ... <https://bs-square.jp/columbus>

株式会社ブロード

〒100-0014 東京都千代田区永田町1-11-30 サウスビル永田町7F
TEL: 03-6205-7463 (代表)

