サイバーセキュリティ最前線

# 拡大する「EMOTET」関連の被害「HP SCE」による抜本的な対策を

**別種のマルウェアをインターネット経由でダウンロードさせたり、一般的なウイルス対策ソフトで検知しづらくしたりする機能を持つ「EMOTET（エモテット）」というマルウェアが、国内外で猛威を振るっている。そこで、今号ではその最新動向とともに抜本的な対策につながる「HP SCE（旧Bromium）」について紹介したい。**

## イタチごっこがつづくサイバーセキュリティ業界

最先端のマルウェア「EMOTET（エモテット）」に関して、さまざまな動きが取り沙汰されている。たとえば2月19日、警察庁と総務省はエモテットに感染したパソコンの利用者への注意喚起をはじめることを発表。それによると、海外の捜査当局より日本国内でエモテットに感染した機器のIPアドレスが2万6000件ほど情報提供され、警察庁と総務省では2月下旬からこれらの情報をインターネットサービスプロバイダー（ISP）に提供することに。ISPは機器の利用者を特定して注意喚起を行い、感染した機器からエモテットを駆除するように指導するそうだ。

他方、海外ではつぎのような報道があった。1月27日にユーロポール（欧州刑事警察機構）が8カ国の治安当局などとの合同捜査を実施した結果、エモテットのコントロールサーバーを摘発することに成功したというのだ。しかし、これで安心というわけにはいかない。長年、セキュリティシステムの提案をしている㈱ブロード（東京都千代田区）によると「サイバーセキュリティ業界ではつねにイタチごっこがつづいており、脅威がひとつ摘まれてもすぐにあらたな脅威があらわれる」と。そして「ハッキングに使われるツールやマルウェアなどのプログラムは、悪意を持つ行為者らの間で流通・売買されており、今回報じられたエモテットも特定のグループのものとはかぎらない」とも。

そもそも、こうしたマルウェアの多くはメールやウェブサイトを使用した手口で拡散されていく。企業や組織のネットワーク内にマルウェアを送り込むうえで、もっとも一般的に解放されている経路だからだ。そこで、一部の大手企業などではITセキュリティの啓発活動の一環として「標的型攻撃訓練」を実施し、偽装メールを使った抜き打ち検査などを行っているという。だが、「これまでにこの訓練で100点を取れたという話を耳にしたことはない。もっとも、社員一人ひとりがつねに正しい判断ができるわけではないので、より抜本的な課題解決法を模索すべきではないか」とブロードは指摘する。

## 抜本的な対策の手段として「HP SCE（旧Bromium）」を導入

では、いかなる手段が抜本的な対策となり得るのだろうか。その候補としてあげられるのが「HP SCE（旧Bromium）」の活用だ。仮想技術を用いたこの製品であれば、「PC本体から隔離された仮想環境でウェブサイトの閲覧や文書ファイルを安全に開けるため、引っ掛けメールの口上やマルウェアの種類にかかわらず『すべてを隔離する』ことができる」という。従来のセキュリティツールはウェブサイトや文書ファイルの良し悪しを判定することに重きを置いてきたためイタチごっこになっていたが、検知・判定に頼らないHP SCEであれば恒常的な対策として活用することができるというわけだ。もちろん、先述の標的型攻撃訓練などをわざわざ実施する必要もなくなる。

サイバーセキュリティを脅かすエモテットの動向に注視しつつ、ユーザーにはこういった抜本的な対策にもシッカリと目を向けてほしいものだ。