サイバーセキュリティ最前線

情報セキュリティ製品とマルウェアの長年にわたる戦いに終止符を打つ

NPO法人日本ネットワークセキュリティ協会（JNSA）の『2020年度 国内情報セキュリティ市場調査報告書』によると、サイバー攻撃の高度化や国内外における法律改正により、情報セキュリティサービスへの投資は年々増加傾向にあり、いまや1兆1201億円（2019年度）に達しているという。しかし、依然としてサイバー攻撃件数は増加の一途をたどっており、被害も拡大しつづけている。そこで、今号ではパソコンに関する情報セキュリティの変遷とその解決方法を探ってみた。

多彩な製品が誕生

パソコンに対する情報セキュリティ製品といえば、ウイルスを検知・駆除するウイルス対策ソフトがもっとも一般的だろう。その多くはパターンファイル（いわば指名手配犯リスト）の情報との照合で有害なファイルを検知・駆除するという仕組みだが、マルウェアがつぎつぎと進化していることもあり、実質、50パーセントほどしか検知できない状況になっているという。しかも、最近では「OSやアプリケーションの正常な仕組みを悪用するケースが増えており、有害なものとして判定しにくくなっている」と長年にわたってセキュリティシステムの提案を行ってきた㈱ブロード（東京都千代田区）は指摘する。

ただ、情報セキュリティサイドもこうした状況に手をこまねいていたわけではない。パソコン内部での不審な動作、たとえば無関係なプログラムの起動や外部のサーバーへの通信などを検知する手法（振る舞い検知）を取り入れたり、AIを活用した情報セキュリティの研究をすすめたりと、さまざまな手法を模索中だ。また「侵入は起こり得るもの」という発想で、侵入された後の被害を最小限にすることに重きを置いたEDR（Endpoint Detection and Response）というアプローチも注目を集めている。さらに、ウェブサーバーとの通信内容に対して、悪用される可能性がある部分を安全なものに置き換える「インターネット無害化」というタイプの製品も開発されている。しかし、いずれも精度がいまひとつだったり、ある程度の被害を前提とするものであったり、使い勝手に変化が生じたりするため、根本的な問題解決にはいたっていないのが現状だ。

「判定の境界」を乗り越える

こうしたなか、2017年頃から情報セキュリティ分野において、あらたなテーマが浮上してきた。それは「有害」「無害」といった判定がつかない「未確認」のものをどう扱うかということだ。その点について、前出のブロードは「『未確認』のものを『クロ』と判定すると正当な処理が阻害されてしまうし、かといって『シロ』にすれば未知の有害物をスルーしてしまう。まさに板挟みの状態だ」と指摘。しかも、最近は既存の情報セキュリティ対策を無効化するマルウェアまで登場しているという。「米国のパイプラインなどをターゲットにした犯行グループのマルウェアから、主要なセキュリティ製品やOSのセキュリティ機構を『オフにする』仕組みが発見された」というのだ。まさに万事休すといった感じである。

だが、判定に頼らない情報セキュリティ製品を活用すれば、こうした問題を一気に解消することができる。その代表的なものが、ブロードが取り扱っている「HP Sure Click Enterprise」だ。事実、「最先端の仮想化技術を応用したこの製品は、検知や判定に頼らず、信頼できないファイルを最初から仮想のパソコンで開くことで安全性を確保する。仮にセキュリティ機構をオフにするようなマルウェアが動作しても、パソコン本体には一切影響はない」という。情報セキュリティ製品とマルウェアは長期間、イタチごっこを繰り返してきたが、この「HP Sure Click Enterprise」を導入することで、その長い戦いに終止符を打つことができるかもしれない。