サイバーセキュリティ最前線

# 巨大インフラを震撼させたランサムウェア これからのサイバー防御策をどうするか

**5月9日、アメリカで最大の石油移送パイプラインを運営するColonial Pipelineがランサムウェア（身代金要求型のウイルス）によるサイバー攻撃の影響で操業を停止したと発表し、世界に衝撃を与えた。ビジネスやライフラインに大きな影響をおよぼすサイバー攻撃に、一体どう対処していけばよいのだろうか。**

## 急増するランサムウェア被害

経済産業省が警鐘を鳴らすサイバー攻撃のひとつとして、本誌2月号でも取り上げた「ランサムウェア」。これは英語の「RANSOM」（身代金）に由来するマルウェアで、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。だが経済産業省も注意喚起している通り、近年では「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」している。

長年にわたり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）によれば、米国の石油パイプラインのランサムウェアによる被害事例は「エンドポイントに入ったマルウェアがウイルス対策製品などの機能を停止させ、検知をかわしてさらに複数のパソコンに影響をおよぼし、最終的に重要データにたどり着いたとみる研究者もいる」という。つまり、1台のパソコンのデータだけが暗号化されたのではないということなのだ。その結果、「1日1億ガロン（3億8000万リットル）の燃料を輸送し、東海岸で使われる燃料の45パーセントをまかなっている」重要インフラの停止につながったのだ。

## これからのサイバー防御策

これほどまでに深刻な被害をもたらすランサムウェアによるサイバー攻撃は、これまでも日本でたびたび起こっている。経済産業省によれば、日本でのランサムウェアの被害額はなんと世界2位とのこと。「サイバーの世界での脅迫は効率がよいことから、ランサムウェアによる攻撃の手口もより巧妙となり、その種類も増えている」とブロード。しかも、このランサムウェアは「OSやOffice製品などの通常の機能を悪用して動作するため、従来のセキュリティ手法である判別・検知の成功率は下がる一方だ」という。

では、今後も増えつづけるランサムウェアに対して、どのような対策をとればよいのか。その点について、ブロードでは同社が日本総代理店を務める米国発のセキュリティ製品「HP SCE（旧Bromium）」の使用をすすめている。これは「1台のパソコン内にもう1台の仮想マシンを用意することで、マルウェアがどのような挙動を起こそうともパソコン本体や保存されたファイルに影響を与えない」というスグレモノ。ランサムウェアを含むマルウェアの新種や亜種が見つかるたびに、それを検知する仕組みを更新する必要があった従来の検知型の製品とは一線を画す新システムだ。

そのほか、同社では「システムを使用するたびにパスワードを自動変更し、事前に許可された操作だけを実行する特権管理製品」の使用もすすめているという。曰く、こうしたセキュリティソフトがあれば「万が一の侵害発生時にも影響を受けにくくなるし、マルウェアに侵害されたネットワーク上の機器からの伝搬を防ぐのにも有効。HP SCEと併用することで、石油パイプラインのような事例（前出）も阻止できるようになる」とのこと。ますます増加、複雑化の一途をたどるサイバー攻撃への防御策には、こうした専門家の知見とノウハウが必須ではないか。