テレワークを割符で保護

NIST／GDPR等対応ソリューションを開発

グローバルフレンドシップ

　秘密分散技術GFI電子割符を展開するグローバルフレンドシップ（東京都渋谷区、保倉豊社長、TEL03・3466・4946、以下、GFI）は、テレワークなどのワークスタイル変化に伴うセキュリティ対策として、GFIがコロナ対応で1年以上実務利用しているテレワーク端末のセキュリティ対策内容を、「GFI Zero Sec 4 DX」として商品化。各方面で対応準拠が求められるNIST SP800-171やEUのGDPR、日本の改正個人情報保護法やISMSへの対応を検討している組織などに広く提案する。

　業種を問わず広がるテレワーク導入時の課題として、BYOD（私物の端末利用）や、一般に高度な対策を施しにくい出先や自宅などのネットワークに、見出しにくいセキュリティ上の危険が潜んでいるといった根本的な課題がある。万一、そうした環境を介して、ネットワークや端末が攻撃された場合には、端末やサーバなどから情報を窃取され大きな問題に発展する可能性がある。そうした問題への対策として、シンクライアントも検討されているが、ネットワーク品質、サーバ処理能力やサーバに情報資産が存在する課題を解決するためのセキュリティ投資の問題が浮上する。そのため、現実的なテレワークなどの運用にあたり、実務端末に対する高度、簡便で経済的なセキュリティ対策が必要となる。

　GFI電子割符は、代表的秘密分散技術で20年超の安定した動作と複数回の外部評価を持つ。同技術で生成される各分割片（割符）自体は無意味な状態になり、原本情報の推測も不能。予め定義した条件以外では復元不能で、万一の漏洩などが発生した時でも訴訟リスクをゼロ又は極小化できる特長がある。

　GFIが開発したソリューションは、同社独自の電子割符の利点を生かし、簡単かつ高レベルのセキュリティ対策を提供することで、テレワークなどの実務環境を保護する。

　GFIでは3層による多層防御を提唱しており、第1層はOS推奨のセキュリティ機能やアンチウイルスソフトなどで対応。

　第1層を突破した不正プログラム等に対し、第2層のOSプロテクト型エンドポイントセキュリティ「AppGuard」と第3層の電子割符を実装した情報資産管理アプリ「割りふってます」で、想定を超える攻撃への耐性を高める。仮に攻撃者が第2層も突破した場合でも、第3層では対象情報自体が割符化されているため情報自体が存在しないか、一部の割符しかない為、仮に攻撃者がその一部の割符を入手しても意味をなさない。

　割符はデータの種類を問わず、デジタル情報をビットレベルで分割。更に毎回異なる振り分けが行われているため、必要な数の割符が揃わない限り、原本を復元できないため、わかりやすく強固な情報管理環境を構築することが可能。原本の復元には、全ての割符が必要な通常モードに加え、一部の割符がない場合でも復元可能な閾（しきい）値分散型のBCPモード、一部の割符サイズを小さくする最小化モードなどを用意。企業や組織は最適な管理手法を選択できる。

　NIST SP800-171では侵入前の「特定」「防御」、侵入後の「検知」「対応」「復旧」などが求められている。GFIでは組織に応じた料金設定を採用することで、規模の大小に関係なく導入可能なソリューションとして展開する方針。

本商品多層防御概念図