

アシスト

# 注目される標的型攻撃対策

## 安価な費用で強力な防御を

アシストが提供するクライアント仮想化製品「Ericom」を基盤とした標的型攻撃対策「ダブルブラウザ・ソリューション」が金融各社から注目を集めている。同製品はマルウェアに感染した場合でも情報漏えいリスクを極小化することで、その利便性の高さや安価な費用が大きな魅力となっている。同社のシステムソフトウェア事業部仮想化推進室技術部の重松俊夫部長は「標的型攻撃を防ぐことはもちろん、ユーザーの利便性も確保できる洗練されたソリューションだと自負している」と力強く語る。



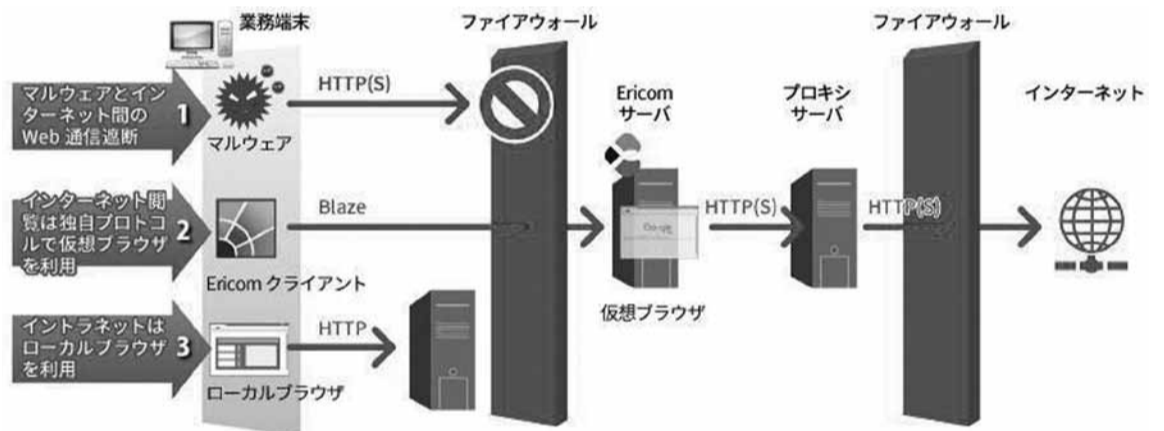
青木氏(左)と重松氏

情報処理推進機構(IIPA)が2月15日に発表した「情報セキュリティ10大脅威2016」によると、標的型攻撃による情報流出は組織にとっての10大脅威の1位に選出されている。その背景には2015年5月に発覚した日本年金機構の個人情報漏えい問題がある。厳重なセキュリティ体制を敷いていると考えられている組織からの情報流出はただで、社会に対して広く標的型攻撃の脅威を強く印象付けることとなった。こうした問題を受けて、金融庁やIPAはセキュリティソフトを複数導入する多層防御を呼び掛けているが、それでも100%の備えには至っていないのが現状だ。

情報流出の原因は、企業の業務端末がインターネットにつながっていることにある。同社はこのシビアな事実を目を付け、業務端末をインターネット端末から分離する「ダブルブラウザ・ソリューション」を開発した。

同ソリューションは、業務端末をファイアウォールでインターネットから遮断する代わりに、仮想環境上に用意したブラウザを経由してインターネットに接続できるようにする。内部

ファイアウォールは仮想ブラウザ利用のための独自プロトコル通信ポートはファイアウォールの



ダブルブラウザ・ソリューションの仕組み

外側にある仮想ブラウザを業務端末から遠隔操作することになる。こうすることで、仮にマルウェアに感染しても、ファイアウォールがマルウェアを操るC&Cサーバとの通信を遮断するため、攻撃を無効化することができる。

ユーザーの端末上にはイントラネット用のローカルブラウザと、インターネット用のブラウザの二つのショートカットアイコンが表示され、ユーザーは業務の内容に合わせてアイコンを選ぶことになる。製品名の「ダブルブラウザ」の由来はここにある。

導入に当たっては、ネットワーク回線の二重化工事や、インターネット接続用PCの追加購入が不要であるだけでなく、他社のクライアント仮想化製品に比べて約半額ともしられるEricomを使用することで、コストを安価に抑えることができる点が顧客から高く評価されている。また、

他社製品の場合、サーバーの他に、サーバーに処理を振り分けるコネクシヨンプロローカーを3000~5000ユーザーごとに1台設置する必要があるが、Ericomの場合にはサーバーで10万台まで対応できるため、システム構成がシンプルで管理しやすいというメリットもある。

その一方で、従来提供してきたWindowsベースの仮想化の場合、マイクロソフトのリモートデスクトップサービスクライアントアクセスライセンズ(RDSCAL)を取得するためにエンドユーザー一人当たり約1万5000円が加算されるため、ユーザー数が多い大規模企業にとっては高いハードルとなっていた。

そこで同社では15年10月に日本ナレッジと共同で、ライセンス料の掛からないLinux版の小規模モデルをリリース。16年2月には大規模モデルを続けてリリースし

た。Linux版に対する反響は大きく、すでに金融機関2社で導入が決定。事例公開している金融機関では2カ月で導入が完了している。利用開始の際には、利用手順書を作成して社員に公開しただけで、カットオーバー後に使い方についての問い合わせやクレームはなく、混乱も生じていないという。

さらに同社では、Windows版とLinux版のハイブリッド導入も提案している。Windows版ではセキュリティ上の品質に遜色はないが、Linux版はインターネットエクストラネットが使えないという点と、サイトの画面をPDFに加工してからの印刷ができないといった課題がある。システムソフトウェア事業部仮想化推進営業部主査の青木裕明氏は「業務に支障がないユーザーにはLinux版、業務に支障が出るユーザーにはWindows版を振り分けることで業務とコストの最適化を実現することができると展望する。重松部長は「今後もユーザーのフィードバックに基づいた改良を加えていく。それと同時に、周辺ツールと組み合わせた提案も行っていく方針だ。この仕組みを知らない方も多いため、認知度を上げていきたい」としている。