トピックス

ネットワーク分離による標的型攻撃対策
―仮想ブラウザー導入による効果と留意事項―

標的型攻撃への対策方法の1つとして、業務端末のインターネット環境からの分離が政府や省庁、IPA（独立行政法人情報処理機構）から推奨されている。本稿ではその手法の1つである仮想ブラウザー方式によるネットワーク分離の効果と導入時の検討ポイントについて解説する。

NRIデータiテック OA基盤事業部 次長
松浦（まつうら） 充宏（みつひろ）
専門はITインフラの設計、構築、運用、サポート

巧妙化する標的型攻撃の手口

企業や団体が標的型攻撃のターゲットとなり、情報漏えいが発生する事例は後を絶たない。その要因の1つとなっているのが、標的型攻撃の巧妙化である。一般的な標的型攻撃の手口は、以下の通りである。

①攻撃対象とする企業や組織に対し、マルウェアを添付したメールを送信する。
②受信者がマルウェアを実行すると、受信者のPCが感染し、そのPCを踏み台として社内ネットワークから機密情報を盗み出す。

これだけ見ると、「怪しいメールは開かなければいいのではないか」と考えるところだが、近年巧妙化しているのが、攻撃メールの送付手口である。攻撃者が攻撃対象の内部事情を把握したうえで、関係者を装った内容のメールを送信したり、差出人のメールアドレスを偽装したりするため、受信者が何の違和感もなくマルウェアを含む添付ファイルを実行してしまう可能性が高い。また、これらのマルウェアは攻撃対象ごとに作成される場合もあるため、ウイルス対策ソフトを導入していたとしても防ぐ事は非常に困難である。

そのため、仮に標的型攻撃を受け、PCが感染するような事態が発生してもその被害を極小化するための対策が重要となってくる。

標的型攻撃対策としてのネットワーク分離の考え方

巧妙化・高度化する標的型攻撃への防御策やサイバーセキュリティ戦略として、2015年以降、IPA（独立行政法人情報処理機構）や政府、総務省、経済産業省が、機密情報を扱う業務用ネットワークと、インターネットに接続する外部ネットワークを分離する対策を推奨している。ネットワークを分離する事により、仮に攻撃を受けたとしても、乗っ取られたPCのネットワーク内には機密情報が存在しないため、情報漏えいが発生するリスクを格段に減少させる効果がある。

このネットワークの分離という考えは、目新しいものではない。これまでにも金融機関をはじめとして事例は多く存在するが、物理的にネットワークを分離するには多額の投資

や運用コストが発生する。そこで注目されているのが、仮想化技術を利用し、実際にはネットワークを接続したまま論理的にネットワークを分離する方法である。仮想ブラウザー方式のインターネット分離は、その1つである。

仮想ブラウザー方式のネットワーク分離

仮想ブラウザーによるネットワーク分離の仕組みは、以下の通りである（図1参照）。

①ファイアウォールで遮断されたネットワーク上にインターネット接続用のブラウザーを配信するサーバー環境を構築する。

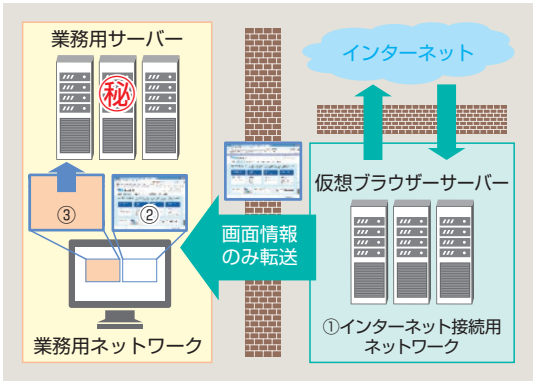
②インターネット接続用のブラウザーはサーバー上の仮想ブラウザーを利用し、画面情報のみをユーザーのPCへ転送する。

③業務用ネットワークで使用するローカルブラウザーは外部へはアクセスしない。

物理的ネットワーク分離と比較した場合、仮想ブラウザー方式の優位性は主に2つある。1つ目はユーザーの利便性向上である。物理的ネットワーク分離では2台のPCを使い分ける必要があるが、仮想ブラウザー方式では1台のPCのデスクトップ上で業務用ブラウザーとインターネット接続用ブラウザーを使い分ける事が可能である。

2つ目は投資コストの削減である。仮想ブラウザー環境をオンプレミスで導入する場合は、専用ソフトウェアを調達する必要があるが、最近では仮想ブラウザーの機能に絞った低価格のライセンス形態を提供するソフトウェアベンダーも出てきており、物理的ネットワーク分離と比較しても投資コストを抑える事が可能である。また仮想ブラウザー環境をクラウドサービスとして提供するベンダーも増えており、選択肢も広がっている。

図1　仮想ブラウザーの利用イメージ例



仮想ブラウザー導入時のポイント

仮想ブラウザーの導入に当たっては、考慮すべき点もいくつかある。ユーザーのインターネット利用目的の要件を満たせるか、また業務効率が極端に低下しないかなどを十分に精査しなければならない。例えば、インターネットでファイルをダウンロードする要件が存在する場合は、ファイルをセキュアにPCへ受け渡すための仕組みも検討する必要がある。

また、仮想ブラウザー方式でのインターネット分離は、標的型攻撃のダメージを最小限にとどめる事を前提とした対策手法のため、徹底した通信ログの監視を行い、悪意を持った第三者の侵入を早期に検知するためのセキュリティ運用も重要である。

仮想ブラウザーを導入する選択肢は数多く存在するが、そこにゴールを置くのではなく、ユーザビリティや導入後の運用を踏まえたフィージビリティ検証を十分に行ったうえで導入を進める事がポイントとなる。 ■