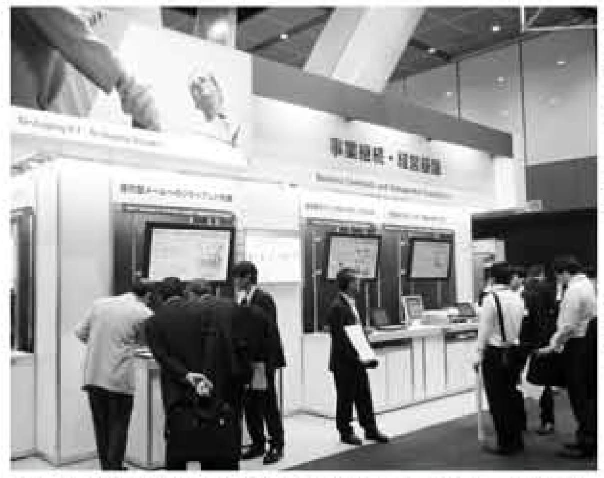
深刻化する標的型攻撃

ユーザーの意識向上が鍵

明確な犯罪意識 何重もの巧妙な罠で

特定の企業や団体を狙った標的型攻撃／サイバー攻撃が脅威を増している。日を追って攻撃は巧妙化しており、政府機関からインフラ企業、一般企業に至るまでウイルス感染したという報告が後を絶たない。関連省庁では予算が盛り込まれ、政府内でも省庁横断の対策機関が設立されるなどの動きが見られる。これらはやっかいなことに、対策ソフトを入れておけば安心というようなものでないため、個々人の意識が重要になってくる。そこで今、改めて標的型／サイバー攻撃の本質や現状、どのような対処を行うべきかについて解説していく。



市場には標的型攻撃対策向けのＩＴ製品が続々と登場している

「標的型攻撃」といわれるサイバー攻撃が注目され出したのは、日本を含む世界のインフラ産業がねらわれたことが明らかになってからだが、その後言葉がひとり歩きし、従来のフィッシングなどまでを含めて標的型と呼ぶベンダーも出始めている。

ここで改めて、世界的に深刻な問題を投げかけている標的型攻撃と従来型攻撃の違いを明らかにし、標的型攻撃とは何かを明確にしてみる。

従来のフィッシングなどが、主に金銭の搾取などを目的としているのに対し、標的型攻撃は、情報の搾取が目的となっている。前者を「詐欺師」と例えるなら、後者は「産業スパイ」となる。

相手を特定した攻撃

標的型攻撃は、従来の無差別的な攻撃とは一線を画しており、その名の通り、相手を特定して攻撃することが特徴となっている。相手が分かっているため、より巧妙な罠を何重にもしかけて、攻撃してくる。

ただし、「標的型でターゲットにされるのは、個人ではない」と情報処理推進機構（IPA）セキュリティセンターの大森雅司研究員はいう。無論、攻撃そのものは個人のPCをねらって行われる場合が多いが、実際のターゲットは、その企業全体となる。

犯人は、その企業から盗みたい情報があり、その方法として、もっともアプローチし易い個人のPCがねらわれることになる。そのため、「複数の職員がねらわれることもある」という。

そして、世界的な傾向から、犯人は「特定の業界全体を一斉に攻撃する場合が多い」という。その場合、軍需産業やエネルギー産業など業界全体をターゲットに、世界情勢を左右しかねない重要情報を盗むことが、犯人の目的だ。

代表的なメール攻撃

具体的な方法としては、メールを使ったものが代表的だ。例えば、ターゲットが普段メールでやり取りをしている相手に対して、いつもの体裁でメールを送りつける。メール文中にWebサイトへの誘いなど、ウイルスを実行させるための地雷が仕込まれている。

手の込んだ手口になると、ターゲットの周辺で防御の甘い人物を割り出し、そこから間接的にターゲットの情報を得る。そして、実際の上司や顧客を装い、心理的に指定のサイトに行かざるをえない状況を作り出して、実行までこぎつける。

これらの巧妙な手口に関しては、対策ソフトやファイアウォールを使って防ぐことは、もはや不可能となっている。

IPAの大森研究員は、「入口で防ぐことのできる攻撃は限られてくるので、一度システムに侵入されてしまうことは、あらかじめ想定せざるを得ない。その場合、大事なのは、とにかく情報漏えいを防ぐこと」と指摘する。暗号化などの技術的な対策のほかに、「簡単に社内の情報が外にでないようなシステム設計」にすることも重要だという。

さらに、大森研究員が懸念するのが、セキュリティ人材の欠乏だ。各企業にセキュリティの専門化が不足しているのは無論のことだが、ベンダーについても例外ではない。

今後新たなスタイルの脅威が次々と登場してくることは避けられないので、「ログ解析の技術に加えて、システムの基礎が身に付いていて、新たな脅威に対しても応用の利くようなセキュリティ技術者の育成が必要となってくる」としている。

サイバー攻撃被害状況

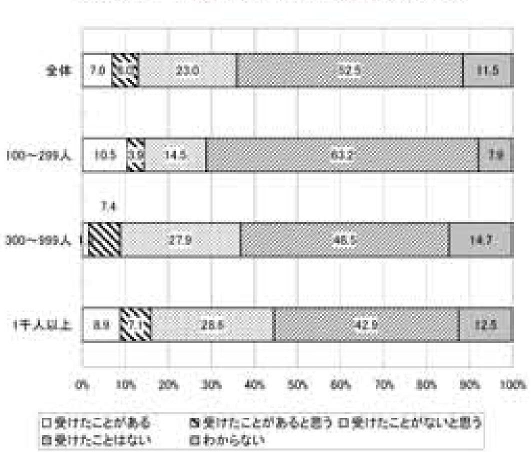
ＡＩＵが経営者対象に調査

ＡＩＵ保険が、昨年末に経営者の情報漏洩リスクに対する意識調査を実施した。従業員数100名以上、資本金5千万円以上の200社の取締役以上を対象に行ったもので、そのなかでサイバー攻撃に関する意識調査も実施している。

調査によると、過去にサイバー攻撃（不正アクセス・ウイルス感染など）を受けたことが「ある」企業は7・0%、「あると思う」企業は6・0%で、サイバー攻撃を受けたことを認識している企業は、合計で13・0%という結果となった。

「あらゆるサイバー攻撃について対策を取っている」企業は8・5%で、「ある程度対策を取っている」企業が55・0%だった。一方で、「あまり対策を取っていない」企業が21・5%あり、「まったく対策を取っていない」企業も6・5%存在しているという状況だ。

サイバー攻撃を受けた経験の有無



大企業は人材確保

具体的な対策として一番多かったものは、「セキュリティポリシーおよび対策の定期的な更新」で、70・9%の企業が実施している。そのほかには、「定期的なサーバー・モニタリング調査」が40・9%のほか、「従業員教育の徹底」が39・4%、「保険への加入」が18・9%だった。「セキュリティ専門人材の採用」は14・2%だったが、1千人以上の企業では23・8%と高くなっており、大企業ほどセキュリティ人材の必要性を認識していることがわかる。

企業がサイバー攻撃の標的として最も意識しているものは、「顧客情報（住所・電話番号・口座・カードなど）の盗取」が42・5%で、「機密情報（マーケティング・開発情報など）の盗取」が27・0%、「特許・知的財産の盗取」が10・0%との順となっている。

自社が実際にサイバー攻撃に遭遇した場合の被害総額の推測値は、平均で1億2303万円となった。価格帯では「1千万円から5千万円未満」が最も割合が高かった。

検疫アプライアンス

ユーザーの対策意識促す

日立電線ネットワークス

日立電線ネットワークスは、検疫ネットワークアプライアンス「QuOLA@Adapter（クオラ・アダプター）」を販売しており、昨年12月に最新版をリリースしている。

元々同社は、ネットワークインテグレーターとして、親会社である日立電線の製品や他社製品を使ってネットワークセキュリティ分野でサービスを展開してきた。その経験をもって、2007年に独自製品を開発している。

モバイルに対応

クオラ・アダプターは、クライアントレスで端末のブラウザーベースで稼働し、幅広いプラットフォームに対応しており、ウインドウズ、Mac、Linuxのほか、新版からはアンドロイド端末にも対応している。

機能面では、ネットワーク接続時およびネットワーク内の端末の起動時に、OS、セキュリティベンダーなどから提供されるパッチのチェックをはじめ、ウイルス対策ソフトがインストールされているか、禁止／必須ソフトインストールされていないかのチェックなど検疫を行い、チェックに引っかかった場合は事前の設定に準じて接続の遮断あるいは警告を行う。

同製品では、検疫している状況をあえて端末の画面で表示し、NGの場合は「何月何日までにこの番号のパッチをあててください」といった警告を出す。これにはユーザーの情報セキュリティ意識を啓もうするという意図があり、ユーザーの対策意識が重要となる標的型攻撃対策に適した機能となっている。

高速でチェック

ただしその際に、検疫に何分もかかっていたのでは生産性やモチベーションの低下をもたらすが、同製品では「5秒から10秒程度で実施する」（システムエンジニアリング本部プロジェクトマネージメント部第一SEグループ田中宗マネージャー）としている。

機能面以外にも、専門の要員が、OSベンダーやセキュリティベンダーがリリースするパッチを一元管理し、安定性や整合性を確認した上で1日に数回、まとめて情報を提供するサービスを提供する。これにより、担当者の負担を減らす。

これまでに、大学や病院、企業など約50件の導入実績を持つ。日立電線のスイッチ製品のほか、丸紅情報システムなどグループ外のパートナー製品との連携展開もあり、今後も製品と販売面でパートナー連携を模索していく。