NIKKEI BUSINESS DAILY FORUM
日経産業新聞
フォーラム2012

増加と巧妙化の一途をたどるサイバー攻撃、標的型攻撃に備えるための情報セキュリティセミナー

脅威の状態見極め対策を

日経産業新聞フォーラム2012「増加と巧妙化の一途をたどるサイバー攻撃、標的型攻撃に備えるための情報セキュリティセミナー」（主催・日本経済新聞社、後援・経済産業省、協賛・フォティーンフォティ技術研究所、フォーティネットジャパン／SCSK、F5ネットワークスジャパン、パロアルトネットワークス）が、7月26日開催された。サイバー攻撃や標的型攻撃から企業の情報システムを保護する具体策について、情報セキュリティー分野のエキスパートによる講演が行われた。本特集では講演概要を紹介する。

基調講演

高度化するサイバー攻撃手法の動向とその対策

慶応義塾大学
環境情報学部教授
武田圭史氏

動的セキュリティーが必須

2000年ごろから、日本のインターネットセキュリティーへの取り組みが実質的に始まった。その当時と比べ、現在起きている状況は、新しいセキュリティーへの脅威のステップに当たるのではないかと考える。

1999年にホワイトハウスのウェブサイトが改ざんされた。当時、ウェブサイトは公開している情報で、改ざんされても再度アップロードすればよいと考え、セキュリティーの脅威として認識されていなかった。だが、このころから政府機関のセキュリティー対策が進展し、日本でもセキュリティー対策企業が立ち上がっている。

コードレッドという世界的に広がる大規模ワーム、ニムダなどが登場した後、レベルの高い攻撃が起きている。ボットネットのように、感染したパソコンなどから大量のパケットを目標のサービスに送信するという分散型サービス妨害も登場した。

10年代になると目的が明確になり、それまで想定されていたサイバー脅威が現実的なものになってきた。10年にはイランのウラン濃縮施設を狙ったスタック・スネット・ワームが登場。これは何らかの政治的な目的を持った組織が開発したといわれている。

さらに、ウィキリークスによる米国の外交関係データ流出、アノニマスによる情報の自由を制限する勢力に対する攻撃などが起きている。

セキュリティー対策としては、脅威の状態に応じた動的セキュリティーが必要である。例えば、アノニマスであれば、ウェブ改ざん、サービス妨害が行われている。サービス妨害であれば、一時的に代替のサーバーを用意、容量の大きいホスティングサービスを利用、サービス妨害対策ソリューション利用など、状況に応じた対策を行う。

情報共有を進めることも攻撃に対しては有効だが難しい面もあり、効果的な仕組みを考えていく必要がある。米国ではセキュリティー人材が軍事産業で雇用され、ノウハウが蓄積されているが、日本でもサイバー攻撃に対抗できる人材を育成する必要があるのではないだろうか。

特別講演

サイバーセキュリティに関する課題と取組について

経済産業省　商務情報政策局
情報セキュリティ政策室長
上村昌博氏

官民連携の施策を強化

内閣情報セキュリティセンター（NISC）は、セキュリティー基本戦略や国際戦略の作成など、政府としてのセキュリティー総合対策を行っている。情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療機関、水道、物流など10分野を重要インフラと位置づけ、政府としての保護施策を関係省庁と協力しながら行っている。

政府の情報セキュリティー戦略は、国民の安全・安心、国の安全保障、そして経済活動に資することがコンセプトである。「情報セキュリティ2012」の施策では、標的型攻撃に対する官民連携での対策強化が挙げられる。

IT（情報技術）の安全確保は産業の基盤であり、産業発展に不可欠である。日本のIT産業全体の市場規模が約17兆円、そのうちセキュリティー産業が約7300億円であり、さらに拡大していく必要がある。

官民連携による情報共有のため、経産省ではサイバー情報共有イニシアティブ（J-CSIP）を立ち上げた。情報共有のハブになる情報処理推進機構（IPA）と参加者の間で秘密保持契約を結び、標的型メールの情報を共有している。

制御システムでは、重要インフラであるセキュリティー強化を図っていく。現在、「IEC62443」が制御システム系では一番カバー率が高いので、これをベースに国際基準にしていく作業を進めている。基準を作成し、実際の認証を国内でも行う。認証した結果が海外でも通用すれば、産業政策上有利である。

実際に制御システムに攻撃があった場合、JPCERTは