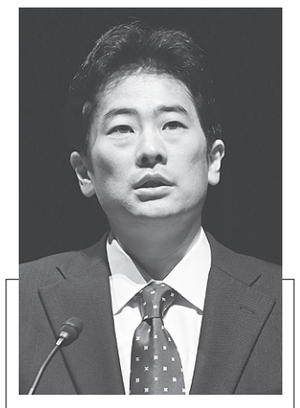
NIKKEI BUSINESS DAILY FORUM
日経産業新聞
フォーラム2013

クラウド時代のサイバー攻撃、標的型攻撃対策を考える

特定の企業や組織を狙ったサイバー攻撃の被害は増加の一途をたどっている。一度の攻撃で社会的信用や競争力を失ってしまうリスクは、企業にとって大きな脅威だ。しかもＩＴ（情報技術）の著しい進展によって、ネットワークに潜む脅威は複雑化かつ巧妙化している。先ごろ開催された日経産業新聞フォーラム２０１３「クラウド時代のサイバー攻撃、標的型攻撃対策を考える～経営・マネジメント層に求められるセキュリティ戦略とは～」では、標的型攻撃の最新事情とともに、今後企業や組織が取るべきセキュリティー戦略について紹介された。

基調講演 サイバースペースにおける安全保障問題



慶應義塾大学大学院
政策・メディア研究科教授
土屋 大洋氏

多様化するサイバー攻撃
国家レベルの防衛確保を

サイバー攻撃を大別すると3つの型がある。1つはＤＤｏＳ（分散型サービス拒否）攻撃だが、それよりもっと深刻なのがＡＰＴあるいは標的型電子メール攻撃と呼ばれるものだ。カスタマイズされたウイルスが仕込まれた添付ファイルをうっかり開いてしまい、当事者が知らないうちに情報を抜き取られるということが今は日常的に起きている。

３つ目は、サイバー攻撃と通常兵器の組み合わせだ。２００８年にはイスラエルがシリアの防空レーダー網を不能化してから核施設を空爆したといわれる。さらに10年には米国とイスラエルがイランの核施設の遠心分離器制御システムに対するサイバー攻撃を行ったともいわれる。

ここで注目すべきは重要インフラの制御システムへの攻撃だ。イランの核施設はインターネットにつながっていないにもかかわらず、異常動作を起こさせるウイルスが送り込まれた。作り込みの独自のシステムであっても、もはや安全とはいえない。しかも経済産業省の調査によれば、日本の工場や水道、発電所などの37％がネットワークにつながっているという。そこに脆弱性があれば、サイバー攻撃を受ける可能性は高くなる。

サイバー空間をめぐる国家レベルの問題を議論すべく、英国のヘイグ外相の呼びかけで国際会議が開催された。国連でも安全保障を担当する第1委員会の政府専門家会合で国家のＩＴ利用に関する規範について話し合われている。主な争点は2つある。既存の国際法をサイバー空間にも適用すべきかどうかと、信頼醸成措置をサイバー空間に持ち込めるかどうかだ。

日本も創設を予定している日本版ＮＳＣ（国家安全保障会議）と内閣官房情報セキュリティセンターが密接に協力して司令塔機能を強化するとともに、国際的な規範の確立に貢献していく必要がある。通信の秘密に配慮しながら、国家レベルのサイバー攻撃を防衛し、サイバー空間の衛生をどのように確保するかが問われている。

国際的な規範の確立と防衛を

プレゼン① 新たな現実のためのセキュリティ ～セキュリティ専門家が語る新たな時代にとるべき脅威対策とは～

ヒューレット・パッカードカンパニー
HPエンタープライズ・セキュリティ・プロダクツ セキュリティ ストラテジスト／エバンジェリスト
ペリー・ペイン氏

新たな脅威に情報可視化で対応

今、企業や政府機関は、国家が主導するスパイ活動や組織化された犯罪グループによって絶えずサイバー攻撃にさらされている。この数年で攻撃はより高度で、洗練されたものになった。闇市場ではリサーチや侵入、マッピングなどの専門家がパスワードやアクセスポイントなどの情報を売買し合っている。犯罪グループは特定のスキルを身につけ、互いに協力して数千億ドルもの取引を行っている。

また、従業員や取引先など、ネットワークに接続できる人たちによる脅威も忘れてはならない。カーネギーメロン大学の研究によると、サイバー犯罪の23％は社内で始まるという。

我々はこうした現実にどう立ち向かえばいいのか。偉大な軍略家である孫子は「敵を知り、己を知れば、百戦危うからず」と言ったが、この言葉は現代においても通用する。社内外の新たな脅威に対応して、考え方と戦略を変えなくてはいけない。

求められているのは、ＩＤＳ／ＩＰＳ（侵入検知／防御システム）やアプリケーション・モニタリング・システムなどを全て統合することで一元的にデータを収集して分析し、自動的に対応するセキュリティー・インテリジェント・システムである。

このシステムの特徴は完全な可視化だ。送られてくる様々な情報の相関関係をリアルタイムに分析することで、ネットワーク上で何が起きているかを可視化し、怪しい行動パターンを検知すると同時に、自動的に対応する。新たな脅威は次々と出てくる。適用するインテリジェンスを1日に何度も更新することによって、システムそのものがインテリジェントなものになっていくのも特徴の一つだ。

今年、米国のポネモン研究所が世界の２００を超える企業を調査したところ、費用対効果の面でもセキュリティー・インテリジェント・システムが最も優れていることがわかった。単なるツールの寄せ集めでは、もはや現在の脅威には対応できない。

プレゼン② マルチデバイス時代のセキュリティマネジメント戦略 ～ネットワークセキュリティの重要性～

セキュアソフト
常務執行役員
荻原 博氏

脆弱性が標的 より強固な対策を

今年3月、韓国の金融機関と放送局を狙った標的型サイバー攻撃は記憶に新しい。攻撃側は、まず放送局の外部公開サーバーのわずかな脆弱性を探し出して侵入。これを踏み台にして社内のサーバーにアクセスし、アカウントとパスワードを取得したことがわかっている。システムごとのセキュリティー対策を行っていても、脆弱性が1つでもあれば、大きな被害が引き起こされる事態になってしまう。

マルチデバイス時代になり、私たちは時間や場所を選ばずインターネットに接続できるようになったのに伴い、ソフトウエアの脆弱性も大量に発生している。こうした脆弱性対策の基本はパッチマネジメントである。しかし、ベンダーがパッチをリリースして適用するまでは、常に危険にさらされた状態が続くため、パッチマネジメントだけで対処することは不可能だ。

パッチ未適用の状態でもサイバー攻撃を防ぐにはネットワーク上の対策が不可欠となる。このような考え方をネットワークセキュリティーという。具体的には、システム管理者が許可しない通信をブロックできるファイアウオールや、パケット単位で不正通信を検出・遮断することでゼロデイ攻撃や標的型攻撃、パスワードリスト攻撃を防ぐＩＰＳが欠かせない。この両方を設置することで、ネットワークセキュリティーはより強固なものとなる。

メリットは3つある。第1は、サーバーや端末に過剰なセキュリティー対策をする必要がないため、利用者の利便性を損なわない柔軟な対策が取れること。第2は、ネットワークの出入り口でトラフィックをモニタリングするため、判断が難しい不正な通信を可視化して異常を検知できること。第3は、モニタリングしながら動的に不正な通信を防御できることである。

日本のＩＰＳ市場をリードする当社は、5月に国内のセキュリティー監視サービスのトップベンダーであるラック社と業務提携した。製品から運用まで幅広いサービスを用意して、今後もセキュリティーソリューションを強化していく考えだ。

プレゼン③ セキュリティ〝対策〟からセキュリティ〝戦略〟への転換 ～グローバル企業でのセキュリティ戦略から学ぶ～

シマンテック 執行役員
セールスエンジニアリング本部長
外村 慶氏

個々の対策から全体的な戦略へ

セキュリティーベンダーはサイバー攻撃に対して、誰にでも効く市販薬やばんそうこうのような対策で後追いをしてきたが、今問題になっているのは標的型攻撃だ。顧客の症状に応じた処方箋、つまりオーダーメードのセキュリティーを提供することが我々の課題だと考える。また企業や組織においても、個々のセキュリティー対策から、長期的かつ全体的な展望を持ったセキュリティー戦略へと転換すべきではないだろうか。

ビジネスにはＰＤＣＡという黄金のフレームワークがあるが、未知の脅威に対しては計画を立てられない。そこで、Ｐ（プラン）ではなくＣ（チェック）から始めてＣＡＰＤと回していけば、セキュリティー戦略を考えやすくなる。チェックとはリスクの可視化であり、デバイスの中を流れている通信で何が起こっているかを見えるようにすることだ。

今、企業にはファイアウオールやＩＰＳ、エンドポイントのセキュリティーソフトなどが入っていて、それぞれ「点」における可視化はされている。しかし、本当にやらなければいけないのは「線」の可視化である。点をつないで線に変換し、今起きていることをストーリーで理解すれば、実際に起こっているリスクがより明確に見えてくる。そのためには相関分析に加え、高度な分析能力が必要だ。

当社が推奨するオーダーメードの監視サービスで検知したインシデントの発生分布を見ると、43％が線で検知したものだった。これはつまり、点の監視では半分近くのリスクを見逃してしまうことを示している。

企業や組織にとってセキュリティーの問題は厄介で煩わしいものでしかない。我々がその煩わしさを肩代わりできればと考えている。

特別講演 我が国のサイバーセキュリティ政策について

総務省 情報流通行政局
情報流通振興課
情報セキュリティ対策室長
山碕 良志氏

情報通信技術（ＩＣＴ）は社会経済活動の基盤であると同時に我が国の成長力のカギである。しかし情報セキュリティー上の脅威の多様化・悪質化により、様々な被害が頻発している。インターネットを利用する人が飛躍的に増え、ネットで世界中がつながっている今、国内でいくら対策を固めても無防備な状態が起きてしまうことを意識する必要がある。安全保障の分野では、サイバー空間は陸・海・空・宇宙に次ぐ第5の戦場だと認識されている。

リスクの甚大化とグローバル化を受け、国は今年の6月、サイバー攻撃に強く、活力あるサイバー空間を構築するための「サイバーセキュリティ戦略」を策定した。ネットに対する規制を強めて情報を管理しようとする国々とは一線を画し、欧米諸国や東南アジア諸国連合（ＡＳＥＡＮ）各国などとともに情報の自由な流通を確保しつつ国際連携を推進していく方針を定めた。

総務省においては、通信事業者と協力して安心なネットワーク環境を整備するとともに、今年から官庁や企業のＬＡＮ（構内情報通信網）管理者を対象に、サイバー攻撃の実践的な防御演習をスタート。サイバー攻撃の予知・即応技術の研究開発にも取り組んでいる。またビッグデータの利用拡大に伴い、プライバシーの保護と両立するパーソナルデータの利活用に関する制度づくりも進めている。

情報セキュリティーは単なるシステムの問題ではなく、企業活動全体に関わる問題である。担当者任せにせず、トップ主導で対策に取り組んでいただきたい。

協賛　日本ヒューレット・パッカード　セキュアソフト　シマンテック