情報セキュリティ対策における課題
―2011年のセキュリティ事件を教訓に―

不正アクセス手法の高度化や多様化に伴い、情報セキュリティ対策の難しさも増している。ツールなどの技術的対策は着実に進んでいるが、情報をタイムリーに入手し、それに基づいて意思決定する人材の確保が多くの企業にとって課題となっている。本稿では、2011年に発生した情報キュリティ事件を取り上げ、進化する攻撃への対策のポイントについて解説する。

2011年の3大セキュリティ事件

近年、ニュースなどでよく耳にするように、ハッカーによる不正アクセスなどの情報セキュリティ事件が後を絶たない。2011年には以下のような事件が大きな話題になった。

(1) ネットワークサービスの個人情報漏えい

2011年4月、ソニー・コンピュータエンタテインメント（SCE）のネットワークサービス「PlayStation Network」とビデオオンデマンド・サービス「Qriocity」のサーバーが不正侵入を受けたという報道があった。アプリケーションサーバーの脆弱（ぜいじゃく）性（攻撃に利用される恐れのある仕様上の欠陥や問題点）を衝いた不正アクセスで、実に7,700万件の個人情報が漏えいした可能性があるという。

サーバーに最新のパッチ(修正プログラム)が適用されていなかったことが原因だが、大規模システムにおけるパッチマネジメントは想像以上に難しい。最新の脆弱性情報を収集する手間もさることながら、パッチ適用による不具合発生のリスクやコスト（大規模システムでは対象サーバーが数百台になることもある）を考慮した上で、パッチを適用するかどうかを総合的に判断しなければならないからである。

(2) ネットバンキングへの不正アクセス

2011年8月、全国の銀行がネットバンキングの不正利用に注意を促す文書をホームページに掲載した。6月下旬以降に不正アクセスが多発し金銭的被害も発生していることを受けての対応である。不正アクセスの多くは、ネットバンキング利用者のPCをマルウェア(コンピュータウイルスなど悪意ある不正なプログラム)に感染させてパスワードを盗み、利用者になりすましてログインするという手法によって行われていた。

近年では、不特定の企業から漏えいしたIDとパスワードのリストを用いてログインを試行しIDとパスワードの組を特定する、リスト型アカウントハッキングと呼ばれる攻撃も少なくない。こうした攻撃への対策として、同一IPアドレスからのログインの成功回数、失敗回数などをモニタリングし、不正アクセスの疑いがあるアクセスをタイムリーに遮断する運用が求められる。

(3) 防衛関連企業への標的型メール攻撃

2011年9月、三菱重工業が標的型メール攻撃を受けたことが報道された（後に社内情報

NRIセキュアテクノロジーズ
コンサルティング事業本部
上級セキュリティコンサルタント
鴨志田昭輝（かもしだあきてる）

専門は情報セキュリティに関わる調査・評価・コンサルティング・教育

NRIセキュアテクノロジーズ
コンサルティング事業本部
上級セキュリティコンサルタント
鈴木　伸（すずきしん）

専門は情報セキュリティに関するコンサルティング

が漏えいした可能性があると発表）。その後、川崎重工業やIHIなどの企業でも同様の攻撃を受けていたことが判明し、防衛関連企業が被害に遭ったことから大きな注目を浴びた。川崎重工業のケースでは、日本航空宇宙工業会（SJAC）の職員のPCがマルウェアに感染し、その職員が関連企業とやり取りしていたメールが盗まれ、それを悪用した標的型攻撃が行われたということである。

標的型攻撃は従来のセキュリティ対策で防ぐことは難しいため、マルウェア感染を検知して外部への通信を遮断する“出口対策”が重要となる。出口対策としては、セキュリティベンダーが次世代ファイアウォールと呼ぶ製品や、DLP（Data Loss PreventionまたはData Leak Prevention：データの機密性を識別してデータの流れを監視・制御するツール）と呼ばれる新しい情報漏えい対策ツールが注目されている。

セキュリティ対策は“運用”が課題

上記のような情報セキュリティ事件の発生を受けて、多くの企業でセキュリティ対策が見直されている。体制や仕組みの構築（情報セキュリティ製品の導入など）はもちろん必須だが、それに加えて適切な“運用”が重要な課題となる。運用とは、環境や脅威が変化しても重要情報を守れるように常に対策を施すことである。

しかし、その運用をどうするかに悩まされている企業が少なくない。常に最新の情報を収集して適切に対応することがいかに難しいことか、多くの企業はあらためて気が付いたといえるだろう。

中長期的な視点での対策が重要

適切な運用の基本は、脆弱性や攻撃のトレンドなどに関する一般的な情報の収集である。これらの情報は、独立行政法人情報処理推進機構（IPA）のホームページなどで収集することができるが、情報セキュリティへの脅威が深刻・複雑になるに従って、情報共有の場の必要性が増してきている。これを受けて2011年10月には、標的型攻撃などの情報共有を目的とした官民連携の「サイバー情報共有イニシアティブ」が発足している。

情報を収集したら、その情報を分析して対策の意思決定に役立てることが必要である。そのための人材確保が多くの企業で課題となっている。

2011年に発生した情報セキュリティ事件は、セキュリティ対策における運用の重要性をあらためて示した。適切な運用を行っていくために必要な情報の収集と、それを分析して意思決定する人材の確保は、多くの企業にとって共通の課題である。これらは簡単に解決できるものではない。セキュリティベンダーとの連携や人材育成などを含めて、中長期的な視点に立った情報セキュリティ対策がますます重要になっていくだろう。 ■