トピックス

CSIRTと多層防御で企業を守る
―「企業における情報セキュリティ実態調査」の結果から―

NRIセキュアテクノロジーズでは毎年「企業における情報セキュリティ実態調査」を実施している。本稿では、2014年の調査でCSIRT（Computer Security Incident Response Team）または類似機能を持つ企業が4割を超えた背景、今後の情報セキュリティに必要な考え方について解説する。

NRIセキュアテクノロジーズ コンサルティング事業本部
ストラテジーコンサルティング部 セキュリティコンサルタント
高木（たかぎ） 大輔（だいすけ）
専門は情報セキュリティに関する調査・コンサルティング

高まる一方の危機感

2014年の4月に、Internet ExplorerやOpenSSL（オープンソースの暗号通信ライブラリー）などの深刻なぜい弱性が立て続けに見つかって大騒ぎになった。前者は、細工が施されたWebサイトにアクセスするとマルウェアに感染したりするもの、後者は、サーバーのメモリー上の情報（ID・パスワード、クレジットカード情報など）を読み取られたりするものである。修正プログラムが配布されて深刻な危険は回避されたが、それ以降もソフトウェアのぜい弱性や、それを突いた攻撃がたびたび報じられている。

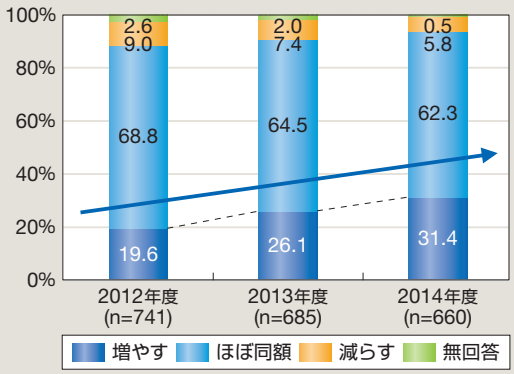
2014年に目立ったのはリスト型アカウントハッキングである。ユーザーが複数のWebサイトのサービスで同じIDとパスワードを使っていることを悪用し、セキュリティの弱いサイトから盗み取ったIDとパスワードで別のサービスへの不正ログインを試みるものである。Webサイトの改ざんや、メールによるフィッシング（偽の情報を送信してIDとパスワードを盗み取る）によって、インターネットバンキングの口座から不正に金銭を振り込ませるものも多かった。このほか、個人情報を扱う企業の内部の人間が不正に情報を持ち出す行為も後を絶たない。

情報漏えいは企業の信用を失墜させるだけでなく、訴訟に発展して企業に大きな損失をもたらす恐れも大きい。情報セキュリティへの危機感はこのところ増すばかりだが、2014年は被害の報告が多かったこともあり、それが特に目立った年であった。

CSIRTへの期待

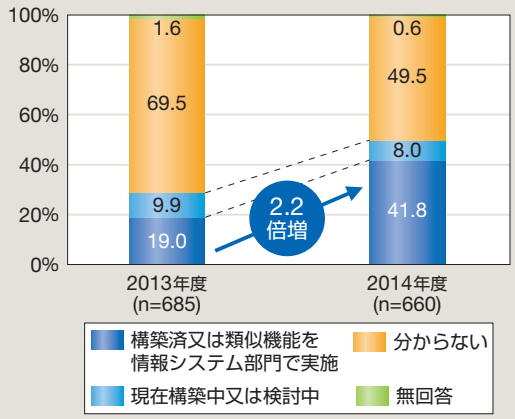
危機感の高まりを反映して、情報セキュリティ対策の予算を増やす企業の割合は増え続けている（図1参照）。しかし、この予算でセキュリティ人材を適切に配置できているわけではなく、「人材が不足している」と回答した企業は過去3年間、毎年8割を超えている。人材が不足している原因として、適切なキャリアパスが用意されていないこと、モチベーションを与える仕組みがないことのほか、ますます巧妙化する攻撃に対してスキル

図1　企業の情報セキュリティ予算の増減動向



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」（2014年8月～10月）

図2　急増するCSIRTの構築率



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」（2014年8月～10月）

が追い付いていないという問題があると筆者は考えている。

こうした問題をカバーするため、また攻撃や対策の情報を油断なくキャッチするために、部署横断的にチームを組んで、また他企業などとも連携して情報セキュリティに当たることが必要になっている。この仕組みがCSIRTである。

CSIRTにはさまざまなタイプがあるが、基本的には社内で各種の情報セキュリティ対策や事故対応を行う専門チームである。しかしそれだけでなく、他社のCSIRT、公的機関、外部の委託先、一般生活者などとの間で情報を共有したりするなどの連携を行うことが求められる。2014年度の調査では、CSIRTまたは類似の機能を持つ企業の割合が前年度の2.2倍となり、4割を超える結果となった（図2参照）。

多層防御の考え方が重要

情報セキュリティについて、今後CIOやCISO（最高情報セキュリティ責任者）、担当者には以下のような姿勢が必要になる。

①感度よく情報を収集し連携させる

スマートデバイスやクラウドサービスなどの新しい技術やサービスが生まれるスピードが速まると同時に、それらが持っているぜい弱性や外部の脅威が明らかになるスピードも格段に速くなっている。情報セキュリティに携わる者は、こうした情報をいち早くキャッチし、CSIRTを通じて社内だけでなく業界横断的に情報連携することが重要である。

②情報セキュリティに完璧はないと考える

サイバー攻撃の高度化によって、それらを100%防御することは不可能になってきた。これまでの取り組みのように「何かが起きないために防御する」ことだけでなく、「何かが起きた後のことをあらかじめ決めておく」ことが重要になる。

このように、何かが起きることを前提に、情報収集→防御→検知→対処といった一連のプロセス全てにおいて対策を行い、総合的にリスクを低減する「多層防御」の考え方が最も大切である。そのような「多層防御」の情報セキュリティ対策の中核を担うのがCSIRTなのである。