特集 情報セキュリティ最前線

巻頭言

多様化・高度化する脅威に企業はどう取り組むべきか

機密情報の窃取、情報の大量流出、社会インフラを狙った攻撃など、次々と報道されるサイバー攻撃。情報セキュリティを取り巻く環境が変化する中、企業は対策コストの増大や技術的な課題を抱えている。多様化・複雑化する脅威によって増大する情報セキュリティのリスクに、企業の経営者は、そして現場はどう取り組むべきか。独立行政法人 情報処理推進機構（IPA）は『10大脅威 変化・増大する脅威！』を毎年発行するなど、日本におけるウイルス・不正アクセスや脆弱性への対策推進、およびユーザー・ベンダーの対策意識向上に取り組んでいる。今回はIPAのセキュリティセンター 情報セキュリティ技術ラボラトリー長の小林偉昭氏、および研究員の大森雅司氏にお話を伺った。

独立行政法人
情報処理推進機構（IPA）
技術本部 セキュリティセンター
情報セキュリティ技術ラボラトリー

●ラボラトリー長
小林偉昭 氏
Kobayashi Hideaki

●研究員 CISSP
大森雅司 氏
Omori Masashi

インターネットが諜報活動・抗議活動の場へ 今後は重要インフラへの攻撃拡大も

「情報セキュリティ」という考え方が出てきたのは、コンピュータウイルスが登場した1980～1990年代です。それから2000年代に入り、ウイルスがPCだけでなくサーバ上でもさまざまな不正アクセスを行うようになりました。当初の攻撃の目的は、愉快犯的な、自らの技術力を顕示・誇示することでしたが、2005年頃から、金銭を目的にした攻撃に変わってきました。当然その背景には、インターネットが経済活動の場となり、金銭に関わる情報のやり取りが増えてきたことがあります。

また最近になって、攻撃者像の多様化も進んでいます。従来の個人のハッカーに加えて、集団で攻撃するサイバーギャングや、機密情報を狙う産業スパイ・国家スパイも登場してきました。その一方では、「Anonymous（アノニマス）」に代表されるような、自らの政治的理念や宗教的理念に対立する組織を攻撃するハクティビスト※1も登場してきました。これまで現実世界で行われていたデモや抗議活動がサイバー空間に移り、Webサイトを攻撃したり、情報を窃取してインターネット上に公開したりすることで、自分達の主義・主張を示すようになっているのです。

今後は、スマートフォンや情報家電など、ネットワークにつながる機器の爆発的増加を背景に、これまで情報セキュリティをあまり意識していなかった家電や装置などの組み込み製品、および制御システムへの攻撃の拡大が懸念されます。情報家電を踏み台としたWebサイト攻撃や、製造工場や重要インフラの制御システムへの攻撃など、すでに多くの事例が報告されています。

日本でも加速化する情報共有の枠組み

大企業には、「CSIRT（シーサート）（Computer Security Incident Response Team）」と呼ばれる、情報セキュリティ上の問題が発生した際の対策を行う専任部隊を置いているところがあります。そして、各社のCSIRTが他社のCSIRTと情報を共有しあうための国際的な連合体として、「FIRST（ファースト）（Forum of Incident Response and Security Teams）」が設立されています。このFIRSTには、日本からも40社近い企業が参加し、そこで得られる情報や実践ノウハウを、自社や顧客のセキュリティ対策に反映しています。

しかしながら、こうしたCSIRTをすべての企業が持つのは困難です。そこで、重要なインフラを狙う攻撃への事前対策として、2011年経済産業省主管の下、重工業9社をメンバーとした「サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））」が発足しました。IPAは、J-CSIPにおける企業と企業、企業と政府の間の“情報ハブ”となり、各社から標的型攻撃の情報を収集・分析し、機密情報を匿名化したうえでメンバー間の共有を推進しています。こうしたイニシアティブは、電力やガス、石油、化学など、他の業界への

展開も予定されています。

また、攻撃対象が情報システムのみに限定されないことを示したStuxnet(スタックスネット)※2によるイラン核施設のウラン濃縮一時停止を受け、2012年には、「制御システムセキュリティセンター(CSSC)」が設立されました。重要インフラを支える制御システムの情報セキュリティを目的としたCSSCでは、2013年度より、宮城県多賀城市のセキュリティ検証施設(テストベッド)で、経営者や技術者向けの教育が始まる予定です。

対策の線引きに悩む大企業 リソース不足に悩む中小企業

日々多くの企業の方と話をする中で、大企業と中小企業では、情報セキュリティに対する考え方やリソースの割り当て方が異なっていると実感しています。大企業は、増え続ける情報量、増え続ける管理デバイス、手を変え品を変えやって来る攻撃に対し、セキュリティ対策をどういった切り口でどの程度行っていけばいいのか、という線引きに悩むケースが多いようです。最近では、HTTPを真似るなどしてファイアーウォールをすり抜ける攻撃や、ソーシャルエンジニアリング※3を巧みに利用した攻撃など、見えない攻撃にいくらコストを投じても効果がなかなか見えない、といった声も聞きます。

一方の中小企業は、専門家がいない・予算がない、といった理由から、セキュリティ対策を後回しにしてしまう傾向があります。しかしながら実際の被害の大部分は、システムの設定不備や、ソフトウェアの脆弱性、特に古いバージョンのソフトウェアを使い続けていることによって発生しています。「セキュリティ対策のパッチを当てる」「パスワードをきちんと管理する」など、普段の心がけで多くの攻撃を回避できるにもかかわらず、「セキュリティ対策はお金がかかる」という意識が強く、基本的な対策が進んでいないようです。

社会とのつながりの中で 自社にとっての最大リスクを捉える

例えば、SQLインジェクション※4によってデータベースを不正操作される、という事実自体は“単なる脅威”であり、その脅威によってどういう影響が出るかは、企業によって異なります。自社へのリスクがどのようなもので、自社のビジネスにとってどれほどのインパクトになるのかを把握することで、守るべきものが明確になり、対策すべき脅威の優先度が決まります。

企業の規模は関係ありません。「うちは中小だから大した被害にはならない」とは考えないでください。ウイルスに感染して工場が一日停止したら、他社も含めたサプライチェーン全体に影響があるかもしれません。自社を踏み台にして、取引先が攻撃されるかもしれません。大企業を標的としている攻撃者からすれば、取り引きがあり基本的なセキュリティ対策ができていない企業に着目し、そこから送信されるメールを介して標的のシステムに侵入していくほうが、直接大企業を攻撃するよりもはるかに簡単です。

自社が社会とどういうつながりの中で動いているかは、経営者にしか見ることができないのです。「セキュリティ対策を強化せよ」と言うだけでは、現場は何をしていいかわかりません。自社にとって最も重要なものは、顧客情報の場合もあれば、製品の設計図の場合もあります。経営者が、現場に対して事業を継続するうえで何が重要かを伝え、それを守るための対策を一緒に考えていくことから始めてください。「サービスを止められないからパッチを当てられない」「基幹業務が動かなくなるからブラウザを最新版にできない」など、さまざまな事情でセキュリティ対策が施せない環境であれば、現場は未対応の脆弱性がどこにどれだけあるかを把握し、経営者はそれを理解したうえでリスクを想定し、対策を講じることが重要です。

セキュリティ対策では、侵入を防ぐことはもちろん、万が一侵入された場合の“出口対策”も重要となります。そのためにも、自分の健康管理と同様、ネットワーク上での情報の流れやログの状況などから、システムがどういう状態にあるかを日々把握しておく。これは本当に大変な作業ですが、こうした地道な取り組みをやっていくしかありません。IPAとしても、さまざまな情報や各種ツールの提供を通じて、企業の皆様の情報セキュリティ対策をご支援させていただきます。

※1 **ハクティビスト**:ハッカーとアクティビスト(活動家)を合わせた造語
※2 **Stuxnet**:複数の未対応の脆弱性を狙った、Windows PCで感染するウイルス
※3 **ソーシャルエンジニアリング**:人間の心理的な隙や行動のミスにつけ込む攻撃手法
※4 **SQLインジェクション**:Webサイト改ざんの手口として知られ、SQLの脆弱性を悪用しデータベースを不正に操作すること

特集 情報セキュリティ最前線

contents

巻頭言・・・・・・・多様化・高度化する脅威に企業はどう取り組むべきか …… 2
傾向と対策・・・・・最新動向と事例で考察する対策の最前線 …… 4
技術解説・・・・・・知っておきたい!注目の情報セキュリティ技術 …… 8
事例・・・・・・・・㈱山梨ニューメディアセンター/トーテックアメニティ㈱ …… 10
富士通の取り組み・・ルールと技術の両輪で行う 富士通の情報セキュリティへの取り組み …… 12
講演録 ゴルフに必要な人間力 …… 有限会社大北ゴルフ練習場 ティーチングプロ 宮里 優 氏 …… 14
豊かに生きる誌上セミナー HUMAN HUMAN 積極的な人生を切り開くポジティブシンキング② …… タチリュウコンディショニングジム 立花 龍司 氏 …… 16
Family's Information ほか …… 17