会社のコンピュータシステムは強固 で安全ですか

サイバー攻撃などの被害を受けると、業務上深刻な問題へと発展することがあります。
そのため、コンピュータシステムの防衛力向上は、いま重要な経営課題となっています。
今号では、サイバー攻撃などの種類や被害内容を考察しながら、対処法を紹介します。

AMAROK JAPAN事務局長
関西大学社会安全学部教授
亀井克之 かめい･かつゆき

1962年生まれ。90年大阪外国語大学大学院修士課程フランス語学専攻修了。97年フランス政府給費留学生としてエクス･マルセイユ第三大学IAE(企業経営研究院)に入学し、DEA(経営学)取得。2002年大阪市立大学より博士(商学)の学位取得。関西大学総合情報学部教授を経て、10年同大学社会安全学部教授に。日本リスクマネジメント学会副理事長、日仏経営学会常任理事など兼務。著書に『新版 フランス企業の経営戦略とリスクマネジメント』『現代リスクマネジメントの基礎理論と事例』(ともに法律文化社)など。

マルウェア（悪意のあるプログラム）は、不特定多数のIPアドレスに対して通信を行い、その応答を待つことで探索（スキャン活動）し、次なる攻撃先を見つけ出していきます。現在、それに該当すると思われる通信数が急増しており、（国研）情報通信研究機構の統計では、一つのIPアドレスに届くパケット数が１年間で46万9,104（2016年）に上り、15年の倍以上になっているという結果が出ています。皆さんのパソコンも同じぐらいスキャンされている可能性があるといわれると、驚かれる方も多いのではないでしょうか。

一方、企業が実際にウイルス感染やサイバー攻撃を受けた状況に目を向けると、（独）情報処理推進機構（IPA）の「企業のCISOやCSIRTに関する実態調査2017－調査報告書－」では、ウイルス感染の被害が「発生した」が26.1％、「攻撃はあったが被害は発生していない」が25.8％。サイバー攻撃に関しては、被害が「発生した」は11.1％、「攻撃はあったが被害は発生していない」のが24.2％となっています。企業が認識したものとしては「ウイルス感染」が51.9％、「サイバー攻撃」が35.3％となります。

ICT（情報通信技術）の活用は、企業の収益向上に欠かせないものになっていますので、現在、サイバー攻撃などは避けることができないリスクであるといえるでしょう。実際、被害が発生すると、機密性が高い企業情報や顧客データの流失、コンピュータシステムの障害による業務の遅滞や停止など、深刻な問題へと発展し、企業の社会的信用の損失も招くことになるのです。

脆弱性を突くサイバー攻撃

問題を引き起こす脅威はさまざまなところに潜んでいます。例えばメールであれば、一方的に大量の迷惑メールを送り付け、ネットワーク遅延やウイルス感染などを生じさせるスパムメールや、金融機関を装い、金銭などを搾取するフィッシングメールなどが挙げられます。これら以外にも、不正なプログラムが仕込まれているWebサイトを閲覧しただけでウイルスなどに感染したり、リンクをクリックした人の情報が盗まれるといったケースも発生しています。

また、外部からサイバー攻撃されることもあり、脆弱性のあるサーバであれば、乗っ取りやサイト内容の改ざんなどといった被害が生じます。先述したIPAの報告書では、攻撃手法として「脆弱性（セキュリティパッチの未適用）を突かれたことによる不正アクセス」が51.7％と最も多く、「ID・パスワードをだまし取られてユーザになりすまされたことによる不正アクセス」が34.8％と次に多くなっていますので注意が必要です。

主な被害の種類

- 情報漏えい
- データなどの改ざん･破壊
- サービス機能の低下･停止
- ウイルス感染
- 踏み台（不正アクセスを行う際に利用されるなど）
- なりすまし（本人のふりをした行為をされる）
- 遠隔操作などでコンピュータを不正使用される

など

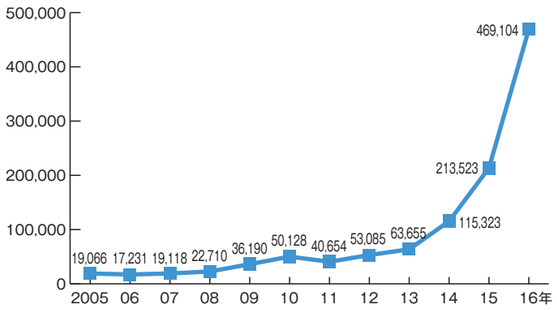
事後対策も万全にする

これらの被害を避けるためには、ウイルス対策用ソフトウェアの導入はもちろん、ＯＳを最新のバージョンに更新したり、脆弱性を修正するプログラムを適用（パッチあて）するなど、事前対策が必要になります。また、不審なメールや添付ファイルなどは開かない、会社から指定されたソフトウェア以外はダウンロードしないといった組織的な対策も重要です。

しかし、いくら事前対策を行っても100％安全が保証されるわけではありませんので、発生した時の対処法を準備しておくことも必要です。例えば、不正アクセスを検知するシステムを導入したり、被害を受けた場合は拡大を防ぐためネットワークへの接続を遮断し、ウイルスであればそれを駆除して、システムの初期化や、アプリケーションやデータの再インストールを実施するなどです。さらに、被害にあったことを速やかに報告する連絡経路を設定しておくことや、データなどが破損した場合に備え、常にバックアップを取っておくことも有効です。

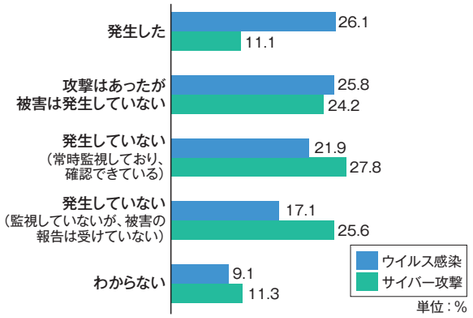
サイバー攻撃などへの対策は、いま重要な経営課題になっていますので、経営者自らが率先し、強固で安全なコンピュータシステムを構築されることが肝心であるといえるでしょう。

1IPアドレスあたりに届く年間の総観測パケット数の推移



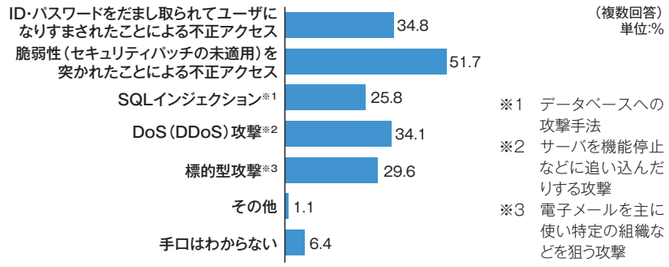
出所:「NICTER観測レポート2016」、(国研)情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティ研究室

ウイルス感染・サイバー攻撃による被害の発生状況



出所:「企業のCISOやCSIRTに関する実態調査2017－調査報告書－」、(独)情報処理推進機構(IPA)

サイバー攻撃の手法



出所:「企業のCISOやCSIRTに関する実態調査2017－調査報告書－」、(独)情報処理推進機構(IPA)