IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2010

情報セキュリティ白書

広まる脅威・多様化する攻撃：求められる新たな情報セキュリティ対策

Information Security White paper

独立行政法人 情報処理推進機構

序章

2009年度の情報セキュリティの概況（トピックス10）

この1年間に情報セキュリティの分野で何が起きたのだろうか? 2009年度に起きた注目すべき10の出来事を取り上げて概説する。

1 大手企業のWebサイトが悪意あるサイトに書き換えられるガンブラー型攻撃が頻発

ガンブラー型攻撃は、ウイルス感染を広げるための今年注目された手口の代表である。Webサイトや Webアプリケーションの脆弱性等を組み合わせた攻撃であり、これまでよりも手口が巧妙化かつ複雑化している。

アクセスの多い大手企業の Webサイトが改ざんされ、それら Webサイトから悪意あるサイトに誘導されることで、多くの利用者がウイルスに感染した。更に、そのウイルスが ID・パスワードを窃取する機能を有していたことから、Webサイト管理者がウイルス感染すると新たな Webサイトが改ざんされ、悪意あるサイトに誘導する Webサイトが増加することで大きな被害となった。

被害状況としては、2009年5～6月にかけて世界的に猛威を振るい、その後いったん終息したと思われたが、11月頃から再び広がった。被害にあったサイトは、2009年11月末時点において、日本だけで3,000件以上、海外を含めると70,000件を越えた。被害 Webサイト数と同数の管理者がウイルス感染したと考えたとしても、一般利用者のウイルス感染被害はその何倍にもなると推測される。

利用者は普段利用する Webサイトが改ざんされていると、知らぬ間に悪意あるサイトに誘導され、その悪意あるサイトでウイルス感染してしまうため、感染を防ぐことや感染に気付くことが困難であった。

（⇒ 1.1.2 セキュリティインシデントの動向）

2 クラウドコンピューティングへの期待と同時に情報セキュリティについての議論も高まる

クラウドコンピューティングは、これまでのようにIT環境を自社に構築するのではなく、クラウドサービス事業者が提供するサービスや機能をネットワークを介して利用するモデルである。しかし、新しいモデルは、新たなものを提供すると同時に、新たな情報セキュリティ上の課題も抱えることになる。

クラウドコンピューティングは、適用技術や運用等の様々な要素に関連した課題が存在する。例えば、仮想マシン間でデータを混在させない隔離技術の開発、オペレータのアクセス管理と特権管理、データセンターの立地国の法制度、サービスの継続性の確保等が指摘されている。これらの対応策について世界各国での研究が進められており、成果の報告がなされている。

今後とも情報セキュリティに対する課題との調和を形成しつつ、ITの利活用の浸透と高度化が進むことが望まれる。

（⇒4.10 クラウド・コンピューティングの情報セキュリティ）

3 国際的なサイバー攻撃が頻発する中、各国が国家レベルでの対応に動き出す

2009年7月、韓国や米国の政府機関、金融機関等の Webサイトを標的に大規模な DDoS（分散型サービス妨害）攻撃が行われた。韓国の国家情報院によると、「朝鮮人民軍が中国の偽装拠点から攻撃プログラムを発信している可能性がある」と伝えている。しかし、未だ犯人や発信源の特定に至ったとの報道は確認できていない。このような脅威が高まる中、各国は国家レベルでのサイバーセキュリティへの対応に動き出している。

米国では、オバマ政権が発足当初からサイバーセキュリティを最優先事項とし、2009年6月にサイバー軍発足を決定し、2010年10月から本格稼働の予定である。また2009年11月に、米国とロシアがサイバー問題に関して、両国の法執行機関間の協力と情報共有の推進、サイバー兵器の廃絶をうたう国際条約について協議を行ったと報道されている。

韓国は、2010年1月、サイバー戦を指揮するサイバー司令部を国防情報本部の下に新設し、サイバー作戦の施行や訓練、研究開発を行うことを発表した。2012年までに、数百人規模の独立部隊を構成するとともに、企業の情報保護を目的にサイバー保安官3,000人を育成する予定である。

国内でも、2010年1月に平野官房長官が会見で「サ

第1章
情報セキュリティ対策の動向と展望

1.1 利用者側の動向と展望

いまやIT（情報技術）は、重要な社会基盤となり、経済活動から日常の社会生活まで、様々な面で利用されている。しかしその一方で、ITを悪用して不正な利益をあげようと試みたり悪意を持って人や社会に大きな被害をもたらそうとしたりする行為も目立つ。本節では、これら社会の安全を脅かす、コンピュータウイルスやボット、不正アクセス行為や、企業、重要インフラ、公共領域などの情報セキュリティ対策の実態について、その動向と展望を述べる。

1.1.1 脅威の動向

利用者観点での脅威の動向として、攻撃手口やウイルス、窃取される情報の傾向を概説し、その後に世界全体の被害状況を示す。

攻撃手口は、ウイルスを仕掛けたWebサイトへ誘導し、ウイルスを感染させるWebベースの手口が多様化・巧妙化しており、増加傾向にある。企業の改ざんされたWebサイトを閲覧すると、悪意あるWebサイトに誘導させられるガンブラー型攻撃と呼ばれる手口が流行し、世界的に被害をもたらした。これまでのWebベースの手口は、スパムメール等に記載されたURLから悪意あるWebサイトへ誘導するものであったため、怪しいメールのURLをクリックしなければ悪意あるWebサイトに誘導されなかった。しかし、ガンブラー型攻撃は、改ざんされたWebサイトを閲覧するだけで、悪意あるWebサイトに誘導されるため、利用者が事前対策をとれないように巧妙化している。更にWebベースの手口は多様化しており、例えば検索エンジンの結果を上位にするSEO（Search Engine Optimization）の手法を利用して、検索結果の上位に悪意あるWebサイトを表示し、利用者にクリックさせる手口も出現している。また、Twitter等のSNSやYouTube等の動画配信サービスから、悪意あるサイトに誘導する経路も出現している。

ウイルスの種類は年々増加しており、2009年も同様に2008年よりも多くの種類が検出されている。このような状況の中、Conficker（Dowand）と呼ばれるウイルスが世界中に猛威を振るった。日本では、Conficker（Dowand）にUSBを介して感染する機能を加えた亜種が、USBメモリ感染型ウイルスとして、4～5月に大学病院や自治体において大きな被害をもたらした。

経済的利得を目的に窃取される情報は、これまでのクレジットカード情報に加えて、オンラインゲームのID・パスワード等が多くなっている。この背景には、オンラインゲームの市場が大きくなっているとともに、RMT（リアルマネートレーディング）で、オンラインゲーム内で使用する武器や防具等のアイテムをゲームの外部で現金化できることがある。犯罪者はオンラインゲームの利用者のID・パスワードを盗み、利用者のアイテムを売ることで、現金を得る。このようにクレジットカード情報に比べて、現金化しやすく、追跡されにくい点も、狙われる背景である。また、情報窃取するマルウェアを生成するツール等がブラックマーケットで販売されており、技術的な敷居が下がり、情報窃取が以前に比べて容易となっていることも関係していると考えられる。

世界における脅威の状況として、攻撃元のアドレスや、マルウェア感染率、フィッシングホスト、スパムメールの送信元について、表1-1-1に地域または国のランキングを示す。また、世界の地域別の注目すべき脅威の動向を表1-1-2に示す。

世界的にマルウェア感染率やスパムメールの送信元として割合が増加している国の傾向は、近年インターネットインフラが急速に普及しているが、それに伴うセキュリティ対策が追いついていない地域である。図1-1-1を参照すると、そのような傾向にあることが示されている。一方、セキュリティ対策が進んでいる欧州や日本はマルウェア感染率が低いことを示している。また、世界的に、オンラインゲームのID・パスワードの情報窃取の被害が発生している。