情報セキュリティ白書

Information Security White Paper

2016

今そこにある脅威：意識を高め実践的な取り組みを

IPA 独立行政法人情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

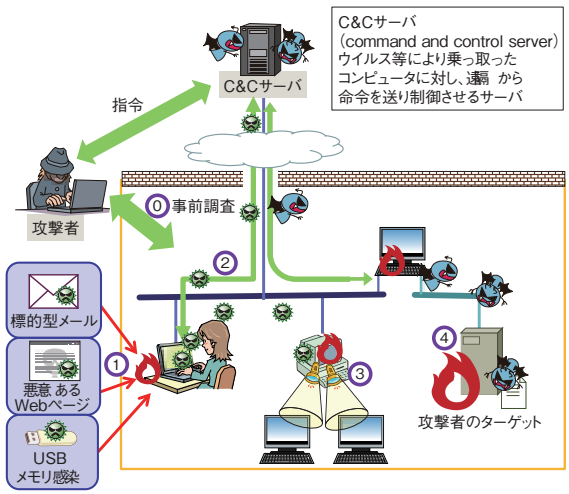
序章

2015年度の情報セキュリティの概況 ～10の主な出来事～

2015 年度に情報セキュリティの分野で起きた出来事について、技術面のみならず制度等を含め、社会への影響を総合的に考慮して選定した「10 の主な出来事」を概説する。各タイトルのかっこ内には、詳細を記載した第I部の項番号を示す。

標的型攻撃により日本年金機構から個人情報が流出（1.2.5）（1.3.2）

2015 年 6 月、日本年金機構の職員が利用する複数の端末がウイルスに感染し、約 125 万件の個人情報が漏えいしていたことが発覚した。日本年金機構によると、2015 年 5 月 8 日から複数回に分けて添付ファイル付きのメール、または外部 URL が記されたメールが送付されており、これらのメールを職員が開封、実行したことが感染の原因とされた。その後、攻撃者がウイルスを使ってネットワーク内の情報を探索し、個人情報の窃取を行ったと見られる。



2015 年 6 月前後の同時期には、類似した標的型攻撃が多く公表されている。これらには、自組織内で攻撃を検知したのではなく、外部組織からの指摘でウイルスの感染が発覚したという特徴がある。「気付けない攻撃」とされる標的型攻撃の深刻さを表す一面である。

標的型攻撃は巧妙化の一途をたどっている。基本的なセキュリティ対策のほか、防御対策を突破されても攻略されない内部対策や、インシデント発覚時の対応、対策を周知徹底するための組織の体制整備等が重要である。

インターネットバンキングの不正送金、被害額は過去最悪を更新（1.2.3）（1.3.5）

インターネットバンキングを狙った攻撃による不正送金の被害額は、過去最悪の約 30 億 7,300 万円に達した。警察庁によると、被害は都市銀行や地方銀行から、信用金庫、信用組合等に拡大している。

2014 年 12 月にインターネットバンキングを狙ったウイルス「WERDLOD」が確認され、2015 年以降も継続して検出されている。日本語で記載されたスパムメールに同ウイルスが添付されてばらまかれる等、日本国内の銀行がこのウイルスの標的となっていることが確認されている。

このウイルスに感染したパソコンからインターネットバンキングを利用すると、正規のインターネットバンキングのサーバではなく、攻撃者が用意した不正なプロキシサーバへ誘導される。この不正なプロキシサーバを経由する際に、利用者が入力した情報が窃取される。不正なプロキシサーバへの誘導は、ウイルスによってパソコンの設定を変更されてしまうことが原因であるため、ウイルス自体を削除できたとしても設定が残っていれば、利用者は被害を受け続ける可能性がある。

警視庁は、2015 年 4 月、総務省やセキュリティ事業者と連携して、ウイルス感染端末に関する情報を入手し、その利用者へ注意喚起を行った。

オンライン詐欺・脅迫被害が拡大（1.2.6）（1.2.7）（1.3.6）（1.3.7）

「ワンクリック請求」全体の相談件数は、2014 年より減少しているものの、スマートフォンにおけるワンクリック請求の相談件数は増加傾向にある。スマートフォンの被害では、ブラウザに請求画面を表示するとともにカメラのシャッター音を鳴らし、写真を撮られたと認識させることで不安を煽る手口や、電話を発信するダイアログを繰り

第1章
情報セキュリティインシデント・脆弱性の現状と対策

日々巧妙化するサイバー攻撃により、深刻な被害が絶えず発生している。2015年度は、組織的な標的型攻撃により、日本年金機構から125万件の個人情報が流出した。米国でも人事管理局から大量の個人情報が流出する等、過去に例を見ない情報セキュリティインシデントが続いた。

金銭的な被害を伴うサイバー犯罪も継続して発生している。インターネットバンキングにおける国内の不正送金被害は過去最悪となった。ソフトウェアの脆弱性は2015年度も問題となり、Adobe Flash PlayerやWordPress等が狙われた。

サイバー攻撃の脅威はすぐそこにあり、どのような組織も被害に遭う可能性がある。こうした脅威へ対処するため、政府や企業における情報共有、脆弱性への対応、体制の強化等を連携して実施することが求められる。

本章では、2015年度に発生したインシデントの状況や事例、攻撃の手口等について解説する。

1.1 2015年度に観測されたインシデント状況

情報セキュリティインシデントは世界各地で発生しており、大規模な情報漏えい事件も確認されている。2015年度も、サイバー攻撃による侵入を許すきっかけとなる脆弱性が多数発見され、Webアプリケーションや POS（Point-of-Sales）端末への攻撃等、様々な対象が狙われている現状にある。ランサムウェアによる攻撃が組織へも拡大する等、実際に業務データが暗号化され、企業活動に深刻な被害をもたらすケースも発生している。

国内においても、メールやWebサイトから巧みに侵入を試みる標的型攻撃、再び増加したマクロウイルスや継続するフィッシング詐欺等、様々な脅威がある。情報漏えいの原因は、外部からのサイバー攻撃だけでなく、組織内部の人によるケースも考慮しなければならない状況にある。

1.1.1 世界における情報セキュリティインシデント状況

世界で発生している情報セキュリティインシデントの状況について、公開されている以下の情報セキュリティ関連の報告書を参照し概説する。

- 日本アイ・ビー・エム株式会社（以下、日本IBM社）：IBM X-Force 脅威に対するインテリジェンス・レポート：2016年[※1]
- Symantec Corporation（以下、Symantec社）：INTERNET SECURITY THREAT REPORT, Volume 21[※2]
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：2015年年間セキュリティラウンドアップ[※3]
- Verizon Communications Inc.（以下、Verizon社）：2016年度データ漏洩／侵害調査報告書（2016 Data Breach Investigations Report[※4]）

(1) 情報漏えいインシデントの状況

日本IBM社によると、2015年は6億件の記録の漏えいがあったと推定されている。2014年には10億件を超えていたことから、約4割の減少となった。一方、Symantec社による調査では、2015年に発生した情報漏えいの件数は、2014年の312件から318件と、同水準での推移であった。しかし、個人情報の漏えい件数は、2014年の3億4,800万件から4億2,900万件と前年比23%の増加であった。その要因として、過去最大規模となる、1回で1億9,100万件もの情報が漏えいした事件[※5]を含め、過去最多となる9件もの大規模漏えいが報告されたとしている。

米国では、2015年6月、米国人事管理局（Office of Personnel Management：OPM）の人事データベースへの不正な侵入が発覚し、連邦政府職員・元職員400万人のデータが窃取された可能性があると発表された[※6]。調査の結果、2,150万人の個人情報への不正アクセス、560万人の指紋データの流出が確認され、政府への攻