情報セキュリティ白書

Information Security White Paper

2014

もはや安全ではない：高めようリスク感度

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

序章

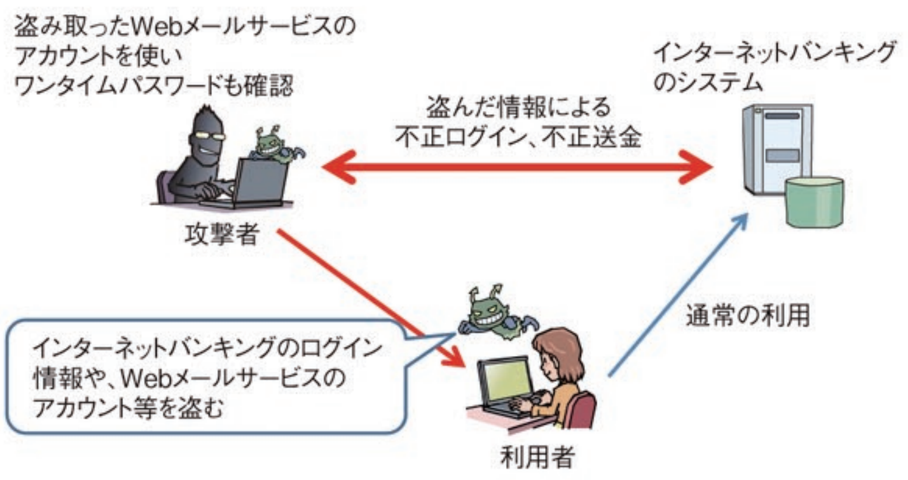
2013年度の情報セキュリティの概況 ～10の主な出来事～

2013年度に情報セキュリティの分野で起きた出来事のうち、技術のみならず制度等、社会への影響を総合的に考慮し情報セキュリティの専門家が選定した10項目について、本書の構成に沿って概説する。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。

インターネットバンキングを狙った攻撃が多発、被害額は過去最悪（1.2.1）（1.3.4）

インターネットバンキングを狙った攻撃が多発した。警察庁の調べによると、2013年は、国内のインターネットバンキングを狙った不正送金の年間被害額が過去最大の約14億600万円に上った。被害に遭った金融機関の数も過去最多の32行に上り、国内の金融機関が広く狙われた。

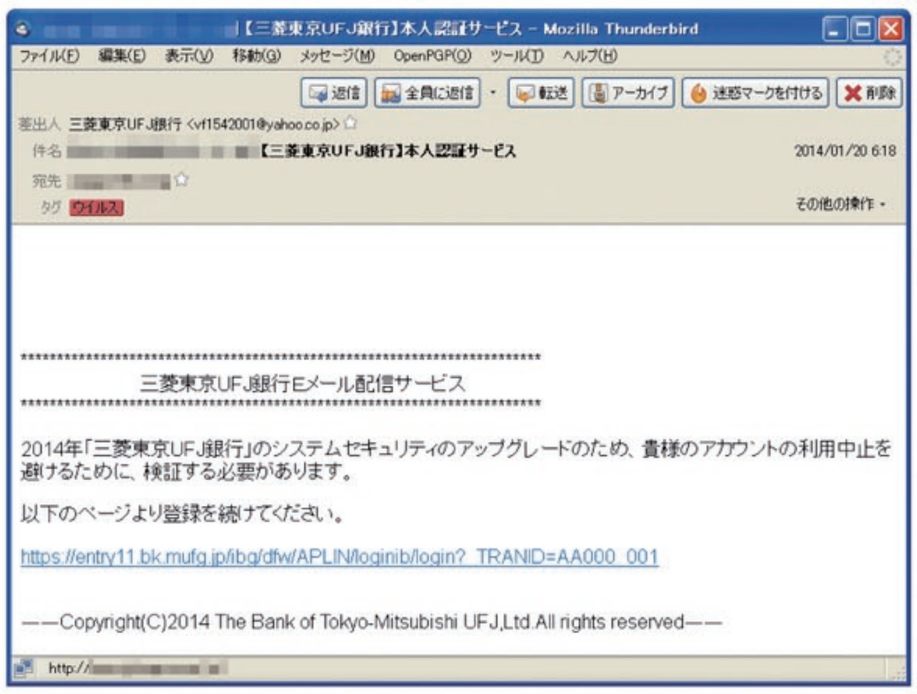
銀行をかたったフィッシングメールだけでなく、インターネットバンキングのログイン情報を窃取するウイルスが猛威を振るっている。この手口は、パソコン内のウイルスが表示する偽の画面に利用者がログイン情報を入力することで情報が盗み取られるものである。また、送金時に必要なワンタイムパスワードを盗まれたことに起因する不正送金も発生した。2013年4月には、ワンタイムパスワードをWebメールで受信している利用者のログイン情報がウイルスによって盗み取られ、その結果、Webメールに届くワンタイムパスワードも盗み見られて、不正送金されてしまう事例が確認された。2014年3月には、ハードウェアトークンで表示されたワンタイムパスワードを利用していたにもかかわらず、ウイルスによる不正送金被害が発生した。



Web改ざん被害が過去最悪、フィッシング詐欺も横行（1.2.1）（1.3.5）（1.3.6）

Webサイトの改ざんは、攻撃者がWeb閲覧者のパソコンにウイルスを感染させるための手口として利用されることから、組織や利用者に深刻な被害を及ぼす。2013年度、JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）へ寄せられたWebサイトの改ざん件数は7,726件で、2012年度の2,856件から2.7倍となり、過去最悪を記録した。特に、2013年6月以降、被害件数が急増したことを受け、9月にJPCERT/CCはIPAと共同で、Webサイト管理者及び利用者に対し注意を喚起する情報を発信した。警察庁でも、重要インフラ事業者等のWebサイトへの改ざんが多発したとして注意を呼びかけた。

また、銀行やゲーム会社等を装い利用者をだますフィッシング詐欺も横行している。フィッシング対策協議会への報告件数は、2012年度はおおむね数十件で推移していたが、2014年1月には4,656件もの報告が寄せられ過去最悪を記録した。これは、フィッシングサイトへ誘導するメールが多数確認されたためである。フィッシング対策協議会では、「三菱東京UFJ銀行」「楽天銀行」「ゆうちょ銀行」等をかたり、「アカウントの確認依頼」または「ログイン画面を変更したことの通知」メールを装って



IPAに届いたフィッシングメール

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

2013年度は、政府機関や企業を狙った高度な標的型攻撃が引き続き確認され、POS端末を狙った攻撃により大量の個人情報が漏えいする被害も発生した。また、インターネットバンキングの不正送金やランサムウェアによる金銭の要求等、経済的利得を目的とした攻撃が世界中で多発した。

サイバー攻撃の手口は日々巧妙化し、従来の対策では防げない事態も起きている。サイバー空間でのリスク感度を上げ、攻撃の早期発見、被害の拡大防止が求められる。

本章では、2013年度の情報セキュリティインシデントの状況や事例、攻撃の手口について解説する。また、情報システムの脆弱性の動向及び情報セキュリティ対策の取り組みについて述べる。

1.1 2013年度に観測されたインシデント状況

世界中で国家・企業の機密情報を狙ったサイバー攻撃やWebの脆弱性を悪用した情報漏えい、ランサムウェアによる金銭被害等、様々なインシデントが発生している。

国内でも政府関係機関への標的型攻撃が依然として発生しており、情報漏えい被害も確認されている。また、Web改ざん被害やフィッシング詐欺、インターネットバンキングの不正送金被害は、それぞれ過去最悪を記録した。

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

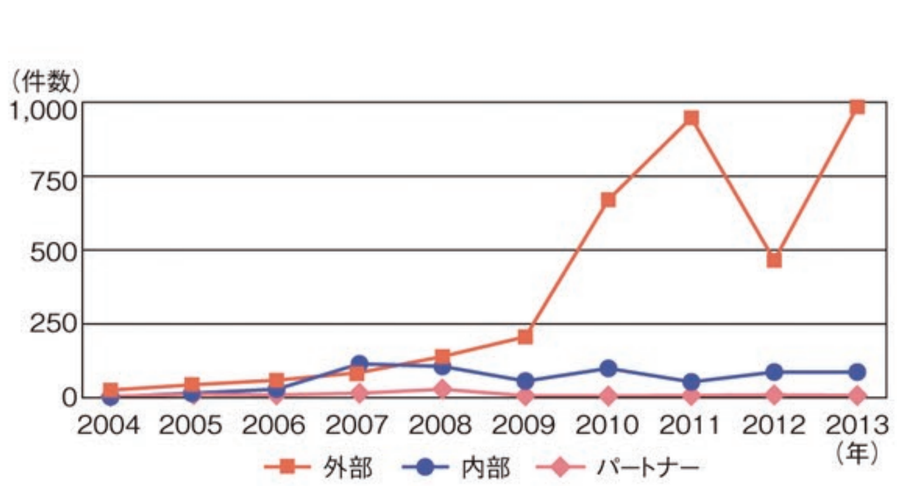
世界で発生している情報セキュリティインシデントの状況について、公開されている以下の情報セキュリティ関連の報告書を参照し概説する。

- Verizon Communications Inc.（以下、Verizon社）：2014年度データ漏洩／侵害調査報告書※1
- 株式会社シマンテック（以下、シマンテック社）：INTERNET SECURITY THREAT REPORT 2014, Volume 19※2
- Microsoft Corporation（以下、Microsoft社）：Security Intelligence Report Volume 15, 16※3
- ファイア・アイ株式会社（以下、ファイア・アイ社）：高度な攻撃に関する脅威レポート2013年版※4
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：産業制御システムへのサイバー攻撃実態調査レポート※5
- 米国国土安全保障省（Department of Homeland Security：DHS）：ICS-CERT Year in Review 2012, ICS-CERT Year in Review 2013※6
- Kaspersky Lab（以下、Kaspersky社）：カスペルスキーセキュリティ情報2013：スパムの進化※7
- ソフォス株式会社（以下、ソフォス社）：スパム送信国ワースト12※8

(1) 情報漏えいインシデントの状況

Verizon社によると、データ漏えい／侵害の事例は、外部からの攻撃によるものが圧倒的に多く、2013年は過去最悪を記録している。内部者による事例は、外部からの攻撃に比較して件数は少ないものの、2007年以降、ほぼ横ばいで推移しており、減少する兆しはない（図1-1-1）。

データ漏えい／侵害の分類を見ると、「Webアプリケーション攻撃」が35%を占め、最も多くなっている。続いて、「サイバースパイ活動」（22%）、「POSへの侵入」（14%）となっている（図1-1-2）。2013年7月、米国司法省は、Webアプリケーションへの攻撃により、世界の主要な金融機関や小売業者等から1億6,000万件のクレジットカー



■図1-1-1　脅威実行者別のデータ漏えい / 侵害事例の件数推移
（出典）Verizon社「2014年度データ漏洩／侵害調査報告書」を基にIPAが編集