情報セキュリティ白書

Information Security White Paper

2015

サイバーセキュリティ新時代：あらゆる変化へ柔軟な対応を

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

序章

2014年度の情報セキュリティの概況 ～10の主な出来事～

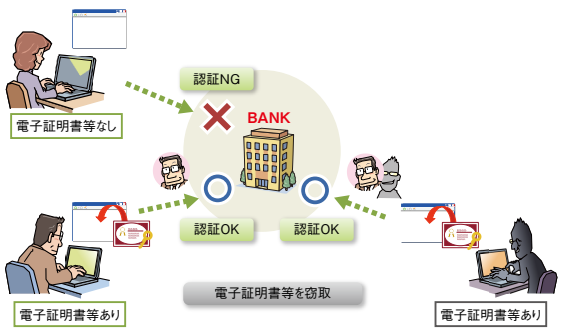
2014 年度に情報セキュリティの分野で起きた出来事について、技術面のみならず制度等を含め、社会への影響を総合的に考慮して情報セキュリティの専門家が 10 項目を選定した。10 の主な出来事として概説する。各タイトルのかっこ内には、詳細を記載した第I部の項番号を示す。

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

2014 年の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、過去最大であった 2013 年の 2 倍を超える約 29 億 1,000 万円を記録した。警察庁によると、被害件数も過去最悪となり、個人の口座に留まらず、振り込み上限額が大きい法人名義口座でも被害が拡大した。

従来の手口であるフィッシングやログイン情報を窃取するウイルスのほか、新しい手口のウイルスが登場した。このウイルスが表示する画面に、送金に必要な ID 等の情報を入力すると、それらが即座にウイルスによって悪用され、リアルタイムに第三者の口座への不正送金が行われる。ハードウェアトークンが生成するワンタイムパスワードを使っていても、不正送金を防げない。

法人向けインターネットバンキングを狙った攻撃として、電子証明書（公開鍵証明書）及び対となっている秘密鍵を窃取して不正送金を行う、新しい手口による被害が発生した。電子証明書等は正当な端末であることを示す役割を担うため、これらを窃取されると、攻撃者の端末がインターネットバンキングの「正当な端末」として認識され、不正送金が行われてしまう。

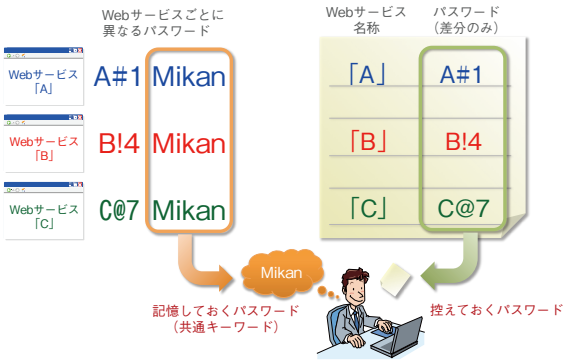


止まらないパスワードリスト攻撃による不正ログイン（1.2.4）（1.3.7）

2014 年度も不正アクセスによる情報漏えいの被害が多発した。中でもパスワードリスト攻撃が用いられたとされる事例が目立った。パスワードリスト攻撃とは、不正に入手した ID とパスワードの組み合わせのリストとツール等を用いて、Web サービスへ不正ログインを試みる手口である。

複数の Web サービスで、ポイントを不正利用されるといった金銭的被害が発生した。そのほか、不正ログインの成功率が高いパスワードリストを作成し、高値で売却することが目的と考えられる攻撃も発生した。

利用者が実施すべきパスワードリスト攻撃への対策は、パスワードを使い回さないことである。しかし、複数のパスワードを覚えることは難しいため、ID とパスワードの一覧表を利用する等、利用者が導入しやすい安全な管理方法が勧められている。



内部不正による被害が相次ぎ表面化（1.2.8）（2.1.2）（3.1）

組織の内部者による犯行が相次いで報道された。

2014 年 7 月、株式会社ベネッセコーポレーションのグループ会社が業務を委託した企業の元社員が、顧客情報を漏えいさせたとして不正競争防止法違反の容疑で逮捕された。漏えいした顧客情報は、国内史上最悪の約 3,504 万件に上った。2015 年 1 月には、株式会社エディオンの子会社の元役員が、販売戦略に関する営業

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

2014年度は、OpenSSLやGNU bashといったインターネットの基盤ともいえるソフトウェアの脆弱性が複数公開され、それを悪用したインシデントも発生した。また、政府機関や企業が保有する個人情報や機密情報を狙った高度な攻撃が発生し、大量の個人情報の漏えいや多大な経済的損失が生じるといった被害が確認された。

経済的な利得を目的とするサイバー攻撃は日々巧妙化し、銀行の顧客口座を狙った不正送金に留まらず、銀行そのものをターゲットとする攻撃による被害も発生している。更に、パソコン内のデータを暗号化し、データの復旧を条件に金銭を要求するランサムウェアによる被害も継続している。

インターネット利用の前提となるソフトウェアにも脆弱性が存在する可能性を認識し、普段からリスクの分析を行い、サイバー攻撃への総合的な対処体制の構築が求められている。

本章では、2014年度に起きた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 2014年度に観測されたインシデント状況

世界で発生した情報セキュリティインシデントを概観すると、標的型攻撃による情報漏えい、金銭を狙ったランサムウェアやインターネットバンキングへの攻撃、POS（Point-of-Sales）端末の決済情報を窃取する攻撃等により、様々な被害が確認されている。

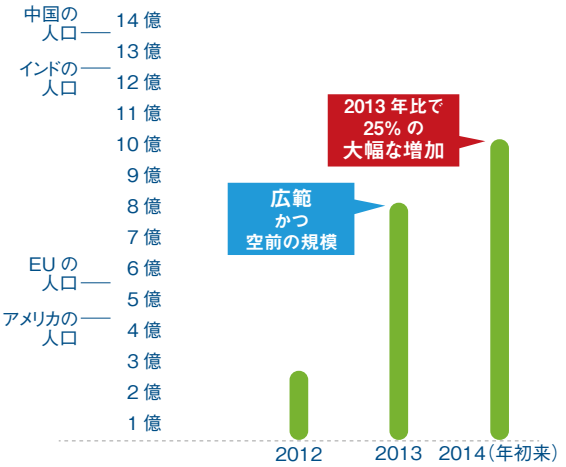
1.1.1 世界における情報セキュリティインシデント状況

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等を参照し概説する。

- 株式会社シマンテック（以下、シマンテック社）：INTERNET SECURITY THREAT REPORT 2015, Volume 20[※1]
- 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四半期レポート：2015年第1四半期[※2]
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：国内標的型サイバー攻撃分析レポート 2015年版[※3]、2014年年間セキュリティラウンドアップ[※4]
- ソフォス株式会社（以下、ソフォス社）：The "Dirty Dozen" SPAMPIONSHIP[※5]

(1) 情報漏えいインシデントの状況

シマンテック社によると、2014年に世界で発生したデータ侵害の件数は、2013年の253件から312件へと23%増加した。2012年の156件と比較すると2倍となっている。漏えいした個人情報は3億4,800万件と、前年比で37%減少したものの、1件あたりの平均は約110万件にも及ぶ。一方、日本IBM社によると、2013年比25%増の10億件を超える個人情報の漏えいがあったと推定されている（図1-1-1）。世界のインターネット人口は30億人[※6]と言われていることから、重複を無視す



■図1-1-1　総漏えい記録件数（推定人口規模との比較）
（出典）日本IBM社「IBM X-Force 脅威に対するインテリジェンス四半期レポート2015年第1四半期」