プレスリリース
2015 年 1 月 15 日
独立行政法人情報処理推進機構

「2014 年度情報セキュリティ事象被害状況調査」報告書を公開

～　サイバー攻撃を受けたと認識している企業はおよそ 5 社に 1 社　～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、最新の情報セキュリティ関連の被害実態および対策の実施状況等を把握し、適切な情報セキュリティ対策の普及・啓発活動を推進するため、「2014 年度情報セキュリティ事象被害状況調査」を実施し、その報告書を 2015 年 1 月 15 日（木）から、IPA のウェブサイトで公開しました。
URL：http://www.ipa.go.jp/security/fy26/reports/isec-survey/index.html

2014 年は、IPAに寄せられた標的型サイバー攻撃 (*1) の件数が 2013 年に比べ 5.2 倍に増加したり、コンピュータウイルスの感染によるインターネットバンキングの不正送金の被害 (*2) が法人で急増したりするなど、組織が保有する機密情報や金融資産を狙ったサイバー攻撃が発生しました。また、その手口は外部から組織を狙うものに限らず、内部者による不正行為の事例も大きな問題となりました。

IPAでは、このような情報セキュリティ被害の動向や対策の実施状況を把握し、適切な対策の普及・啓発活動に役立てるため、「2014 年度情報セキュリティ事象被害状況調査 (*3)」を実施しました。調査結果のポイントおよび調査概要は以下のとおりです。

■ 調査結果のポイント

（1） サイバー攻撃 (*4) の遭遇率が 5.5 ポイント増加、ウェブサイトにおける被害が増加

サイバー攻撃の被害にあった回答は 4.2%、発見のみの回答は 15.1%であり、その合計（遭遇率）は 19.3%となり、前回の 13.8%から 5.5 ポイント増加しました（別紙①）。

ウェブサイトに関する被害が多数を占めており、具体的な内容は、「ウェブサイトのサービスの機能が低下させられた」が最も多く 22.5%、「ウェブサイトのサービスが停止させられた」被害も 13.8%となっています（別紙②）。

ウェブサイトが被害に遭う原因には、管理アカウントの窃取、ウェブサーバの脆弱性が狙われることなどがあります。

（2） 標的型攻撃メールによる被害の状況

標的型攻撃を受けたのはサイバー攻撃に遭遇した前述の 19.3%（368 社）のうち、30.4%（112 社）でした（別紙③）。そのうち被害にあった割合は 18.8%（21 社）でした（別紙④）。なおその手口を聞いたところ、「同僚や取引先、サービス事業者からのメールを装い、添付したウイルスファイルを開かせる」が最も多く 54.5%（61 社）、次に「電子メールに表示された URL 経由で攻撃用のウェブサイトに誘導される」が 40.2%（45 社）でした（別紙⑤）。このように標的型攻撃メールは、ウイルスが添付されているだけでなく、開封を促すため文面等が巧妙になっていることから注意が必要です。

(*1) IPA の標的型サイバー攻撃 特別相談窓口に寄せられた標的型攻撃メールの件数は 2013 年 1 月-12 月 97 件、2014 年 1 月-12 月 509 件

(*2) 警察庁：「平成 26 年上半期のインターネットバンキングに係る不正送金事犯の発生状況について」https://www.npa.go.jp/cyber/pdf/H260904_banking.pdf

(*3) 本調査は 1989 年度から実施しており、今回で 25 回目を数える。

(*4) 本調査ではウイルス感染に因らない、外部からの攻撃などをサイバー攻撃と定義。

(3) 電子メールでウイルスに遭遇する割合が 8.9 ポイント増加

ウイルスに遭遇（発見と感染）した割合は 2012 年度（2013 年調査）の 71.5%から 73.8%となり、2011 年度の 68.4%から年々増加傾向にあります（別紙⑥）。

侵入経路別にみると、最も多いのが「ウェブサイト閲覧」で 65.4%（前回 63.2%）、次いで「電子メール」が前回の 51.7%から 8.9 ポイント増加し 60.6%でした（別紙⑦）。

(4) クライアントパソコンへのセキュリティパッチ適用率が 7.3 ポイント向上

クライアントパソコンへのセキュリティパッチの適用状況を聞いたところ、「常に適用し、適用状況も把握」が 43.3%と、前回の 36.0%から 7.3 ポイント増加しました（別紙⑧）。

一方で、「常に適用する方針・設定だが、実際の適用状況は不明（29.7%）」と「各ユーザに適用を任せている（13.6%）」の合計は 43.3%となり（別紙⑧）、前回の 48.0%よりは減少しているものの、実際に適用を確認していない企業が依然として 4 割超存在していることがわかりました。

脆弱性が残存するパソコンをターゲットとし、ウェブサイトを閲覧しただけで感染させる攻撃が相次いでいることから、セキュリティパッチ適用が浸透しつつありますが、まだまだ十分とは言えない状況です。

(5) 内部サーバにセキュリティパッチをほとんど適用していないのは 16.8%

外部に公開しているサーバがセキュリティパッチを「ほとんど適用していない」割合は 6.3%の一方で、組織内部で利用しているサーバにセキュリティパッチを「ほとんど適用していない」が 16.8%でした（別紙⑨）。その理由の筆頭は、「パッチの適用が悪影響を及ぼすリスクを避けるため」で、74.0%でした（別紙⑩）。内部サーバは外部から直接攻撃されることはないと、現状の設定のまま変更したくない意識が働いているものと推測されます。しかし、ウイルスの侵入経路として「USB メモリ等の外部記憶媒体」が 34.5%（別紙⑦）もあることから、組織内での感染拡大を防止するためにも適切な管理が求められます。

(6) 小規模な組織では内部不正防止のための、定期的なパスワード変更の実施割合が低い

主な業務システムの一般ユーザアカウントのパスワード設定ルールについて初めて聞きました。パスワードを「システム上で、定期的な変更を必須としている」企業の割合は 53.1%でした。従業員規模で分類すると 300 人以上では 62.8%、300 人未満では 37.4%と大きな差がでました（別紙⑪）。

パスワードの強度確保に加え、定期的なパスワードの変更をシステム上で実施することは、組織内でのなりすましログインによる情報窃取等の内部不正への対策として一定の効果があります。パスワードの設定ルールの整備や管理は適切に行う必要があります。

■ 調査概要

（1） 調査対象：業種別・従業員数別に抽出した 13,000 企業
（2） 調査期間：2014 年 8 月～10 月（調査対象期間：2013 年 4 月～2014 年 3 月）
（3） 調査方法：郵送調査法
（4） 回収結果：1,913 件（有効回収率 14.7%）
（5） 主な調査項目
(A) 回答企業の概要
(B) 情報セキュリティ体制・対策の現状
(C) コンピュータウイルス・サイバー攻撃による被害状況

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター 小松／花村
Tel: 03-5978-7530 Fax: 03-5978-7546 E-mail: isec-info@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部 広報グループ 横山／白石
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp