

**「2013年度 情報セキュリティ事象被害状況調査」報告書を公開**  
～ 組織内でセキュリティパッチの適用状況を確認していない割合は48% ～

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、「2013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2014年1月27日（月）から、IPAのウェブサイトで公開しました。

URL：<http://www.ipa.go.jp/security/fy25/reports/isec-survey/index.html>

近年、組織が保有する情報システムや情報資産を狙ったサイバー攻撃が巧妙になってきており、特定の企業や国家機関を狙い撃ちする標的型攻撃も発生しています。また、ウェブページが改ざんされ、そのページの利用者にウイルス感染の被害が発生するなど、情報システムを保有する組織は情報セキュリティ上の様々な危険にさらされています。

IPAでは、最新の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、「情報セキュリティ事象被害状況調査」を1989年度から毎年実施しており、今回で24回目になります。

■ 調査結果のポイント

**(1) セキュリティパッチの適用状況を確認していない割合は48%と約半数**

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は、「常に適用し、適用状況も把握」が36.0%である一方、「常に適用する方針・設定だが実際の適用状況は不明」は31.3%「各ユーザに適用を任せている」が16.7%と、実際に適用状況を確認していない割合は48%と約半数に上りました。

前回調査（2011年度）と比較すると「常に適用し、適用状況も把握」は約2ポイント、「常に適用する方針・設定だが実際の適用状況は不明」は約5ポイント上昇していますが、これはセキュリティパッチ適用の重要性は浸透したものの、実際の適用状況まで見届けることの重要性までは理解が進んでいないことを示しています。

（詳細データについては調査報告書のP63、P64を参照）

**(2) 組織内の体制整備が進展：「兼務だが担当責任者を任命」は前年から7ポイント上昇**

情報セキュリティ対策の社内体制として、「専門部署（担当者）がある」は15.7%で前回調査と同様でしたが、「兼務だが担当責任者が任命されている」は56.6%と、前回の49.6%から7ポイント上昇しました。これは「組織的には行っていない（各自の対応）」（14.8%）が前回（21.3%）より6.5ポイント減少したことも合わせ、社内体制の整備は進展していることが伺えます。

また、組織内の「役員」「正社員」「契約社員」の情報セキュリティ対策教育の実施状況を前回調査と比較すると、「特に実施していない」の割合がいずれも減少（「役員」△6.1%「正社員」△4.7%「契約社員」△2.7%）しており、組織内において対策の必要性が認識され、教育の実施率が向上していることがわかりました。

（詳細データについては調査報告書のP23、P34、P36、P37を参照）

**(3) ウェブサイト閲覧によるウイルス遭遇率が約7ポイント増加**

ウイルス遭遇率は71.5%と前回の68.4%から若干の増加となりました。ウイルスの侵入経路を

みると、最も多いのがウェブサイト閲覧で前回の56.4%から63.2%へと6.8ポイント増加し、続いて電子メール51.7%（前回52.2%）、USBメモリ等の外部記憶媒体38.0%（前回45.5%）となりました。

私物のUSBメモリ等を社内ネットワークに接続する際の運用ルールを聞いたところ、「禁止している」もしくは「届け出に応じた許可制としている」企業は67.3%となっています。一方、「禁止していない」は28.9%でした。USBメモリ経由のウイルス感染は減少傾向にありますが、未だに4割弱もあることから慎重な運用が求められます。また、ウェブサイトについてはより一層の、電子メール経由についても引き続き注意を払う必要があります。

（詳細データについては調査報告書のP50、P66、P68を参照）

#### (4) スマートデバイスに技術的な各種セキュリティ対策を行っているのはわずか3割台

スマートフォンやタブレット端末を業務に利用している企業は40.6%と前回より11.1ポイント増加しました。セキュリティ対策については、「紛失・盗難時のデータ消去」が37.5%、「セキュリティソフトの導入」が33.9%、「MDM<sup>(※1)</sup>による端末管理」が30.0%と、技術的な対策は30%台に留まり、前回調査時から進展が見られませんでした。また、「利用ルールの策定」は45.6%と運用面での対策実施率も半数以下でした。

業務で利用するスマートデバイスには企業の情報が保持されているため、技術面および運用面から、データ保護対策の実施が求められます。

（詳細データについては調査報告書のP40、P47を参照）

本年度実施した「2013年度 情報セキュリティ事象被害状況調査」の概要は下記のとおりです。

- (1) 調査対象：業種別・従業員数別に抽出した約14,000企業
- (2) 調査期間：2013年8月～10月（調査対象期間：2012年4月～2013年3月）
- (3) 調査方法：郵送調査法
- (4) 回収結果：1,881件（有効回収率13.4%）
- (5) 主な調査項目
  - (A) 回答企業の概要
  - (B) 情報セキュリティ対策の現状
  - (C) コンピュータウイルス・サイバー攻撃による被害状況

#### <訂正の内容>

該当箇所（2014年1月29日付）

サブタイトル及び「調査結果のポイント」項目番号（1）内の数値

#### 【誤】

確認していない割合は47.3%

#### 【正】

確認していない割合は48%

<p>■ 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</p> <p>■ 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</p>
--

(※1) MDM (Mobile Device Management、モバイル端末管理)：モバイル端末と社内システムとの認証、アプリケーションとの同期、外部サービスとの接続等を管理するシステム