プレスリリース
2016 年 3 月 3 日
独立行政法人情報処理推進機構

「内部不正による情報セキュリティインシデント実態調査」報告書の公開

～情報持ち出し手段の最多は USB メモリ、効果的な抑止策は罰則規定・監視体制の強化～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、内部不正の発生、およびその対策の実施状況等を把握し、内部不正の防止に向けた環境整備を促すため、「内部不正による情報セキュリティインシデント実態調査」を実施し、その報告書を 2016 年 3 月 3 日（木）に公開しました。

URL：https://www.ipa.go.jp/security/fy27/reports/insider/

近年、組織内部から漏えいした情報により引き起こされるインシデントに関する報道が相次いでいます（別紙①）。例えば内部不正[*1]はその被害額が外部からの攻撃によるものよりも高額な傾向があり[*2]、組織は内部不正を未然に防ぐ必要に迫られています。しかしながら、内部不正は、職務上与えられた権限を使い行われるため、その対策は容易ではありません。

IPA では、2012 年に内部不正についてその動機や抑止・防止策を明らかにするために意識調査を実施[*3]しました。2 回目となる今回は、民間企業の従業員と内部不正を行った経験を有する者（以下、内部不正経験者）にアンケートを実施し、より実態を掘り下げる調査を目指しました。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。

（1） 内部不正の理由の約 6 割は故意が認められない“うっかり”（別紙②）

内部不正経験者に行為の理由を聞いたところ、“うっかり違反した”が 40.5%、“ルールを知らずに違反した”が 17.5%（合計 58.0%）と、全体の約 6 割は“うっかり”によるもので、故意が認められませんでした。うっかりミス等を防ぐため、管理者は扱う情報に格付けする等のルールや規則を明確にし、周知徹底することが対策として有効です。

その一方、42.0%は故意によるもので、その理由は“業務が忙しく、終わらせるために持ち出す必要があった”が 16.0%、“処遇や待遇に不満があった”が 11.0%などでした。

（2） 主たる情報の持ち出し手段は“USB メモリ”

情報の持ち出しには“USB メモリ”の利用が最多でした。組織での対策は USB メモリ等の外部記録媒体に関する利用ルールの徹底、および利用制限が有効と考えられます（別紙③）。しかしその対策状況をみると、従業員規模が 300 名未満の企業の過半数で“方針やルールはない”と回答しています（別紙④）。

上段：内部不正経験者すべて（n=200）下段：故意の内部不正経験者のみ（n=98）

	1 位		2 位		3 位	
持ち出し手段	USB メモリ	43.6%	電子メール	34.3%	パソコン	25.5%
	USB メモリ	53.0%	電子メール	28.9%	紙媒体	18.8%

[*1] 本調査では、IPA が公開している「組織における内部不正防止ガイドライン」の定義に従い、違法行為だけでなく、情報セキュリティに関する内部規程違反等の違法とまではいえない内部不正行為も含めている。

[*2] Ponemon Institute, LLC の「2015 Cost of Cyber Crime Study : Global」（提供：HP Enterprise）によると、9 種のサイバー攻撃による年間平均被害額は、内部不正が約 14.4 万ドルと最も高かった。

[*3] 2012 年 7 月 17 日発表「組織内部者の不正行為によるインシデント調査」報告書の公開
https://www.ipa.go.jp/security/fy23/reports/insider/index.html

（3）　経営者等が重要視していない対策が内部不正行為の抑止に有効

内部不正経験者と経営者・システム管理者とで、有効と考える内部不正対策の違いが顕著だったのは“罰則規定を強化する”、“監視体制を強化する”ことでした。（別紙⑤）。
なお、監視強化についての意識の差は前回調査でも同様の傾向[(*4)]が示されています。不正行為抑止のためには、監視だけでなく、監視している旨を通知することが有効です。

経営者・システム管理者は、不正行為を思い留まらせるのに有効な対策を的確に把握し、実施する必要があります。

内部不正経験者		対策	経営者・システム管理者	
順位	割合		順位	割合
4 位	25.0%	**職務上の成果物を公開した場合の罰則規定を強化する**	12 位	12.8%
5 位	23.5%	**管理者を増員する等、社内の監視体制を強化する**	11 位	13.1%

（4）　内部不正経験者の約 5 割がシステム管理者（兼務を含む）

内部不正経験者の職務を尋ねたところ、51.0%がシステム管理者（兼務を含む）でした（別紙⑥）。システム管理者は社内システムに精通し、高いアクセス権限（特権）を有することが多いため、権限の最小化・分散、および作業監視等の対策が有効です。

■アンケート調査概要

（1）　調査方法：ウェブアンケート
（2）　調査対象：業種別・従業員数別に抽出した民間企業における従業員等 3,652 名
　　内部不正経験者 200 名
（3）　調査期間：2015 年 11 月 25 日～11 月 30 日
　　本調査と同時に事前調査（内部不正の経験に関するスクリーニング）を実施
（4）　主な調査項目
A) 回答者の企業属性・個人属性および企業状況
B) 情報セキュリティインシデントの発生状況（内部不正も含む）
C) 内部不正対策の実施状況
D) 内部不正発生時の対応
E) 経営者・システム管理者と従業員の意識

■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　石綿／益子
Tel: 03-5978-7530　Fax: 03-5978-7518　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

(*4) 従業員の「内部不正への気持ちが低下する対策」の 1 位「社内システムの操作の証拠が残る」に対して、経営者・システム管理者の「現在講じている効果があると考える対策」においては、21 項目中 19 位という結果であった。