

平成 26 年 8 月 29 日

平成 25 年度「個人情報の取扱いにおける事故報告」の傾向と注意点

一般社団法人 情報サービス産業協会
審査業務部

情報サービス事業者における個人情報保護の一層の充実に資するため、当協会ではプライバシーマークの付与適格性審査に合格した事業者から平成25年度（平成25年4月1日～平成26年3月31日）に提出された「個人情報の取扱いにおける事故報告」をもとに、事故の傾向と注意点について取りまとめたので、以下のとおり報告する。

1. 事故報告の概要

事故報告の件数及び事業者数は 143 件（45 社）である。前年度の 138 件（59 社）に比べて報告件数はほぼ横ばいであるが、事業者数は前年度比 76.3%と大きく減少している。

表-1 に個人情報関連事故の内容別件数と割合を示した。これによると、「電子メールの誤送信」が 37 件（25.9%）と、この 4 年間で最も多く、次いで、「従業員によるパソコン・携帯電話・書類等の紛失」が 26 件（18.2%）、「委託先事業者による事故」が 20 件（14.0%）、「FAX の誤送信」が 16 件（11.1%）、「発送物の誤送付・誤封入」が 15 件（10.5%）であり、上位 5 件で全体の 79.7%を占めている。

報告内容は例年同様に軽微な事案が多く、殆どがヒューマンエラーによるものである。

平成 25 年度の事故の特筆すべき点は、従来報告の無かったパスワードリスト攻撃をはじめとする不正アクセス攻撃が増加傾向にあり、IDやパスワードに加えてクレジットカード情報など金銭的な 2 次被害が懸念される漏えい事故が発生していることである。独立行政法人情報処理推進機構などから公表されているセキュリティに関する最新情報を収集し、攻撃を受ける前に適宜に対策を講ずる必要がある。

表-1 個人情報関連事故の内容別件数と割合

事故の内容	平成 22 年度 (n=84 社)		平成 23 年度 (n=59 社)		平成 24 年度 (n=59 社)		平成 25 年度 (n=45 社)	
	件数	割合	件数	割合	件数	割合	件数	割合
電子メールの誤送信	28	17.1%	34	21.3%	35	25.4%	37	25.9%
紛失 (パソコン・携帯電話・書類など)	62	37.8%	57	35.6%	31	22.5%	26	18.2%
委託先事業者による事故	31	18.9%	27	16.9%	21	15.2%	20	14.0%
FAX の誤送信	7	4.3%	14	8.8%	15	10.9%	16	11.1%
発送物の誤送付・誤封入	15	9.1%	12	7.5%	12	8.7%	15	10.5%

小計	143	87.2%	144	90.1%	114	82.6%	114	79.7%
----	-----	-------	-----	-------	-----	-------	-----	-------

宅配便・郵便による紛失	4	2.4%	8	5.0%	3	2.2%	7	4.9%
盗難 (空き巣・車上荒らし・置き引き)	5	3.0%	2	1.3%	5	3.6%	6	4.2%
不正アクセス	0	0%	0	0%	0	0%	5	3.5%
プログラムミス	4	2.4%	3	1.9%	3	2.2%	4	2.8%
データベース等への誤入力・誤処理	2	1.2%	0	0%	4	2.9%	1	0.7%
ファイル交換ソフト (Winny など)	2	1.2%	1	0.6%	0	0%	0	0%
従業員による不正持ち出し・不正利用	2	1.2%	1	0.6%	0	0%	0	0%
その他	2	1.2%	1	0.6%	9	6.5%	6	4.2%
合計	164	100%	160	100%	138	100%	143	100%

2. 内容別に見た事故の概要と防止のための注意点

(1) 電子メール及びFAXの誤送信による事故について

電子メールの誤送信による事故は37件で全体の25.9%を占めており、発生件数、全体に占める割合は前年度とほぼ同じである。

事故内容は、「メールの宛先を誤って送信した、本来送信すべき宛先のほかCCに関係のない第三者を加えてしまった(29件)」等関係の無い第三者にメールを送ってしまったという事案が顕著である。オートコンプリート機能を利用する際に、よく似たアドレスを選択してしまったり、過去に使用したメールを使い回して送る際に送り先の修正を忘れてたり、テンプレートの選択ミスなどが誤送信の原因となっている。

一方、FAXの誤送信による事故は16件で全体の11.1%を占めており、報告件数は前年度とほぼ同数である。誤送信の原因は、顧客から送信先を電話で聞いた際に聞き間違えた、ゼロ発信するべきところゼロを付け忘れた、短縮ダイヤルの登録ミスなどが原因となっている。

これらの対策としての基本は、電子メール及びFAX送信者一人ひとりが送信前の確認行為を徹底することである。そのためには、事業者が啓発教育を通じてメール及びFAX送信前の確認行為を義務付けることであるが、さらに、電子メールについては、「オートコンプリート機能の使用を禁止する」「同報メール送信前に注意喚起メッセージを表示する」「送信ボタン押下後に取消可能となるようなソフトウェアを導入する」など、社内ルールの徹底に加えてツールを併用することが効果的である。また、FAXについては、短縮ダイヤルの登録内容を適宜チェックすることが必要である。

(2) 紛失(パソコン・携帯電話・書類など)による事故について

ノートパソコン、携帯電話、書類の置き忘れ等による個人情報の紛失事故は26件(18.2%)で、過去4年を通して減少傾向が続いている。

平成25年度に報告された26件の紛失事故のうち、書類の紛失が15件と過半数を占めている。紛失の原因は「営業中に持ち歩いていて風に飛ばされた」「シュレッダーにかけたと思われるが確証がない」「外出中にコンビニのFAXやコピー機を利用した際に原紙を置き忘れた」といった不注意に起因している。書類は携帯電話やパソコン等の電子機器と異なり、暗号化やパスワードの設定等の安全管理措置が講じられないので、特に注意が必要である。

昨年度迄過半数を占めていた携帯電話の紛失は 10 件と減少傾向にある。緊急時などの連絡用として常に携帯していることから事故が多発していたが、常時体から離さない等の再発防止策が功を奏しているものと思われる。また、紛失した場合でも「暗証番号ロック」や「指紋認証」「電話帳データの遠隔消去」などのセキュリティ機能付き携帯電話やスマートフォンが増えており、2 次被害につながった事案はない。また、ノートパソコン及び記憶媒体の紛失が 2 件報告されているが、「ハードディスクや媒体の暗号化措置」「シンクライアント化して情報を置かない」などによりいずれも二次被害の発生には至っていない。

概してプライバシーマーク付与事業者は、ノートパソコンや携帯電話などの携帯可能な端末の管理が行き届いており、情報資産の持ち出し制限やデータの暗号化措置が徹底しているため、紛失した場合でも二次被害につながる可能性は極めて低い。とはいえ、スマートフォンの利用拡大やハードディスクの高密度化等により、一旦事故が発生した場合の被害が大きくなることが予想されるため、事業者側の管理体制と携行者側である従業者一人ひとりの心構えがなお一層問われることになるであろう。

(3) 委託先事業者による事故について

委託先において事故が発生した場合は、委託元は原則として免責されることはなく、過失割合によって責任を負う可能性がある。

平成 25 年度は 20 件の委託先による事故の報告があり、全体に占める割合は 14.0%、昨年度の 21 件 (15.2%) とほぼ同じ件数で推移している。

委託先事業者における事故内容は、「誤送付」「FAX やメールの誤送信」「プログラムミス」といったヒューマンエラーに起因する事故が 19 件 (95%) を占めているが、再委託先の社員の犯罪によってキャッシュカードが偽造され、金銭的被害が発生するなど深刻な事案も 1 件報告されている。

これらの対策としては、委託先が管理を徹底出来るよう啓発教育等で支援するほか、「委託先における個人情報の取扱い状況を定期的に把握する」「定期的に業務報告を受ける」など管理を徹底することが重要である。

表-2 委託先事業者における事故の内容別件数

事故の内容	平成 22 年度	平成 23 年度	平成 24 年度	平成 25 年度
誤送付	11	10	5	12
FAX 誤送信	0	5	3	4
メール誤送信	4	3	2	2
プログラムミス	0	1	0	1
不正利用	1	0	0	1
Winny	3	1	1	0
誤入力・誤処理	1	2	1	0
盗難	0	1	0	0
紛失	10	4	9	0
宅配便業者の誤送付	1	0	0	0
合計 (件)	31	27	21	20

管理上のポイントとしては、「委託業務の実態に見合った委託先選定基準・評価基準であるか」「定期的に業務の監督・チェックを実施しているか」「必要のない個人情報まで渡していないか」などを精査する必要がある。また、再委託、再々委託の必要が生じる場合には、その再委託先、再々委託先における取扱い状況を常に把握しておくことも必要である。

委託先を選定するにあたって、プライバシーマーク認定事業者であることをもって十分な調査をすることなく委託している例も見られるが、委託先がプライバシーマーク認定事業者であることに安堵することなく、常に委託業務の実態に見合った管理を心掛けることが、事故を未然に防ぐためには必要である。

(4) 発送物の誤送付・誤封入による事故について

発送物の誤送付・誤封入による事故については 15 件 (10.5%) の報告があり、発生件数と発生率は前年度からやや増加している。誤送付された発送物のなかには、「公共料金の口座振替依頼書」「関係の無い第三者宛の請求書の混入」など本人に与える影響の大きさが懸念される金銭やプライバシーに関する情報も含まれていることから、対応を誤ると大きな事故に発展する可能性があり、再発防止に向けた十分な対策が必要である。

再発防止策としては、作業に入る前に導入教育を義務付けるなど事故が発生した場合に生じる本人への影響及び会社の社会的信用の失墜について、あらかじめ従業者に十分に認識させておくことは言うまでもなく、発送する前には必ず複数人でチェックをするなどの検査体制の見直しを含め、個々の従業者にとって負担の掛からない作業方法へ転換することが重要である。

(5) 不正アクセスについて

特筆すべき事項として、今年度から不正アクセスに関連する事故が報告されるようになってきたことに注意する必要がある。報告された内容は、「電子商取引のサーバーが外部から不正アクセスされ、クレジットカード番号や取引内容が窃取された可能性がある」「会員向けサービスのIDとパスワードが外部からの攻撃で持ち出された」「オンラインショッピングサイトが外部からの攻撃で顧客情報が閲覧された」など、初期対応を誤ると2次被害として大規模な金銭的被害が発生する可能性がある。

脆弱性を突いた不正アクセス攻撃によってIDとパスワードが窃取されると、パスワードリスト攻撃やオンラインバンキングへの不正ログインやクレジットカード情報の悪用等に繋がり、金銭的被害に発展することが予測されるため、JPCERT/CCやJVN (Japan Vulnerability Notes)、(独)情報処理推進機構から公表される最新の情報セキュリティ情報や脆弱性情報を収集して適切な対策を遅滞なく講じる必要がある。具体的には、使用ソフトを最新の状態にバージョンアップすることで脆弱性対応を行うほか、必要に応じて侵入検知システムの導入やペネトレーションテストを受けることなどが有効である。

(6) その他の事故について

そのほか発生率が5%以下の事故として、「宅配便・郵便による紛失」が7件(4.9%)、「盗難(空き巣・車上荒らし・置き引き)」が6件(4.2%)、「プログラムミス」が4件(2.8%)、「データベース等への誤入力・誤処理」が1件(0.7%)、報告されている。

「宅配便・郵便による紛失」では、7件全てがセキュリティ便という一般の宅配便よりは安全管理を強化した特別便にも拘わらず、宅配業者が紛失や誤配送をしている。誤配送によりクレジットカードを誤って受け取った関係の無い第三者がカードの限度額一杯まで現金を引き出すなどの事件に発展した事例も報告されている。

昨年度報告の無かった「Winny などファイル交換ソフトによる事故」や「従業者による

不正持ち出し・不正利用による事故」は、本年度も全く報告されていない。これは、啓発教育は言うまでもなく、「許可の無いソフトウェアのインストール禁止」「監視ソフトの導入」「個人情報へのアクセス制限」「入退室管理の強化」「業務の自宅への持ち帰り禁止」など、事業者が従業員の管理に厳格に取り組んだ結果によるものと推測される。

3. 全般的な管理上の注意点について

平成 25 年度内に報告された事故事案をもとに、個人情報の取扱いにおける事故の傾向と注意点について述べた。傾向としては、従来と同様に委託先による事故を含め、ヒューマンエラーに起因する事故がほとんどを占めている。

事業者のセキュリティ事故対策として、啓発教育を徹底して行うこと、日常の運用の確認を励行すること、ヒヤリ・ハット事例を収集して全社的に水平展開すること、などがしばしば報告される。しかし、こうした地道な運用を継続しているにもかかわらず、ヒューマンエラーに起因する事故は繰り返し発生してしまう。

人間の意識レベルが下がることは避けられず、それを「単なる不注意」として処理してしまうとヒューマンエラーの防止にはつながらないものである。啓発教育や運用の確認は重要な事故対策であるが、これらに加えて、注意力が下がって失敗をすることは人間として避けられないという前提のもとで、作業方法を人間の特性に合わせて容易なものに見直していくことがヒューマンエラーを防止する最善策と考える。

以上