平成 27 年 6 月 1 日

平成 26 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26年度（平成26年4月1日～平成27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以下のとおり取りまとめた。

１．事故報告の概要

平成 26 年度の事故報告件数及び事業者数は 152 件（50 社）である。前年度は 143 件（45 社）であったので、若干であるが報告件数、事業者数共に増えている。

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、「従業者によるパソコン・携帯電話・書類等の紛失」が 38 件（25.0%）、次いで、「発送物の誤送付・誤封入」が 33 件（21.7%）、「電子メールの誤送信」が 32 件（21.0%）、「委託先事業者による事故」が 15 件（9.9%）、「FAX の誤送信」が 12 件（7.9%）であり、上位五つの事故が全体の 85.5%を占めている。

報告内容はヒューマンエラーに起因する軽微なものがほとんどであるが、その一方で、平成 20 年度から平成 24 年度まで報告実績のなかったシステムの脆弱性を狙った不正アクセスの事案が、平成 25 年度と同様に 5 件報告されている。

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 23 年度 (n=59 社)		平成 24 年度 (n=59 社)		平成 25 年度 (n=45 社)		平成 26 年度 (n=50 社)	
	件数	割合	件数	割合	件数	割合	件数	割合
紛失（パソコン・携帯電話・書類など）	57	35.6%	31	22.5%	26	18.2%	38	25.0%
発送物の誤送付・誤封入	12	7.5%	12	8.7%	15	10.5%	33	21.7%
電子メールの誤送信	34	21.3%	35	25.4%	37	25.9%	32	21.0%
委託先事業者による事故	27	16.9%	21	15.2%	20	14.0%	15	9.9%
FAX の誤送信	14	8.8%	15	10.9%	16	11.1%	12	7.9%
小計	**144**	**90.1%**	**114**	**82.6%**	**114**	**79.7%**	**130**	**85.5 %**
盗難（空き巣・車上荒らし・置き引き）	2	1.3%	5	3.6%	6	4.2%	5	3.3%
不正アクセス	0	0%	0	0%	5	3.5%	5	3.3%
プログラムミス	3	1.9%	3	2.2%	4	2.8%	4	2.6%
宅配便・郵便による紛失	8	5.0%	3	2.2%	7	4.9%	2	1.3%
データベース等への誤入力・誤処理	0	0%	4	2.9%	1	0.7%	2	1.3%
従業者による不正持ち出し・不正利用	1	0.6%	0	0%	0	0%	1	0.7%
ファイル交換ソフト（Winny など）	1	0.6%	0	0%	0	0%	0	0%
その他	1	0.6%	9	6.5%	6	4.2%	3	2.0%
合計	**160**	**100%**	**138**	**100%**	**143**	**100%**	**152**	**100%**

２．内容別に見た事故の概要と防止のための注意点

（１）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 38 件（25.0%）で、前年度までは減少傾向にあったが、再び増加に転じた。

38 件の紛失事故のうち、書類の紛失が 18 件と約半数近くを占めている。紛失の経緯は「自転車で取引先を回っている最中に顧客の名刺が入った名刺入れを落とした」「誤って廃棄した可能性もあるが確かではない」「帰宅途中で書類が入ったカバンごとなくした」などである。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。なかには紛失した顧客の名刺を拾った第三者から見返りに金銭を要求されたという事案もあった。

携帯電話の紛失は 15 件報告されており、前年度の 10 件から増加している。なかでも帰宅途中の飲食店や電車の中での紛失又は旅行先での紛失が目立つ。社給の携帯電話を緊急時などの連絡用として常に携行していることから紛失し易いものであるが、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を利用しているので、二次被害につながった例はない。また、ノートパソコン及び記憶媒体の紛失が 5 件報告されているが、ハードディスクや記憶媒体への暗号化措置、シンクライアント化などの対策が講じられており、いずれも二次被害の発生には至っていない。

プライバシーマーク付与事業者は、概して、ノートパソコンや携帯電話などの携行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蓋然性は極めて低い。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は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。

（２）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 33 件（21.7%）の報告があり、発生件数と全体に占める割合は前年度から倍増している。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」「関係のない第三者宛の請求書」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係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。

（3）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 32 件で全体の 21.0%を占めている。発生件数、全体に占める割合は例年ほぼ横ばいである。

内容は、「Bcc で送るところを誤って CC で送った」「送信すべき宛先のほか、関係のない第三者を CC に加えてしまった」などの事案が顕著である。また、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にして、送る際に送り先の修正を忘れたり、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 12 件で全体の 7.9%である。報告件数、全体に占める割合は前年度より減少している。誤送信の経緯は、「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を間違えた」などである。

これらへの対策の基本は、事業者が啓発教育を通じて電子メール及び FAX 送信前の確認行為を義務付け、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。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全社的に禁止した上で、同報メール送信前に注意喚起メッセージを表示するソフトウェアや送信ボタン押下後に取消可能となるソフトウェアを導入するなど、社内ルールの徹底遵守に加えて、ツールを併用することが一層効果的である。FAX については、短縮ダイヤルの登録内容を適宜チェックしていなければならない。

（4）委託先事業者による事故について

平成 26 年度は 15 件の委託先事業者による事故の報告があり、全体に占める割合は 9.9%である。10 年前に本調査を開始して以来、全体に占める割合は最も低い。

事故内容は、「誤送付」「紛失」「プログラムミス」などが占めており、深刻な事案は含まれていない。これらが重大な事故に発展しないようにするための対策としては、委託先が自ら管理を徹底できるよう啓発教育等で支援するほか、委託元は「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」「委託先から定期的に業務報告を受ける」など委託先に対する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 23 年度	平成 24 年度	平成 25 年度	平成 26 年度
誤送付	10	5	12	8
紛失	4	9	0	4
プログラムミス	1	0	1	1
誤入力・誤処理	2	1	0	1
宅配便業者の誤送付	0	0	0	1
FAX 誤送信	5	3	4	0
メール誤送信	3	2	2	0
不正利用	0	0	1	0
Winny	1	1	0	0
盗難	1	0	0	0
合計（件）	**27**	**21**	**20**	**15**

管理上のポイントとして、「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付与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が多く見られる。委託先において事故が発生した場合、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ことになるため、委託先がプライバシーマーク付与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事業者の選定及び管理を心掛けることが必要である。

（5）不正アクセスについて

全体の割合から見れば僅かではあるが、ヒューマンエラーに起因するものとは別にシステムの脆弱性を狙った不正アクセスの事案が前年度と同様に 5 件（3.3%）報告されている。報告の主な内容は、「会員専用 Web サービスで使用している Open SSL の脆弱性を狙った不正アクセスにより、画面に表示される顧客情報が漏えいした」「個人情報を格納したホームページ上のデータベースが SQL インジェクション攻撃を受け、メールアドレスと暗号化されたパスワードが攻撃者に搾取された可能性がある」「親会社の Web サービスを構築・運用しているが、パスワードリスト攻撃と思われる不正アクセスにより会員情報が閲覧された可能性がある」などであり、初期対応を誤ると二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。使用ソフトウェアを最新の状態にバージョンアップすることで脆弱性対策を講じるほか、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も有効であるが、その他にも日頃から不正アクセスに備え、JPCERT/CC や独立行政法人情報処理推進機構（IPA)から公表される最新の情報セキュリティ情報や脆弱性対策情報を収集し、適切な対策を遅滞なく講じておくことが肝要である。

（6）その他の事故について

その他発生率が 5%以下の事故として、「盗難（空き巣・車上荒らし・置き引き）」が 5 件(3.3%)、「プログラムミス」が 4 件(2.6%)、「宅配便・郵便による紛失」が 2 件（1.3%）、「データベース等への誤入力・誤処理」が 2 件(1.3%)報告されている。

「宅配便・郵便による紛失」では、2 件すべてが一般の宅配便よりも安全管理を強化したセキュリティ便において発生した奇妙な事案である。2 件のうち 1 件は宅配業者が紛失し、

もう１件は宅配業者が盗難に遭っている。

なお、「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」「監視ソフトウェアの導入」「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、事業者が従業者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

ヒューマンエラー対策として、啓発教育を徹底して行う、日常の運用の確認を励行する、などをよく耳にする。しかし、このように対策を行っているにもかかわらず、ヒューマンエラーは繰り返し発生する。

ヒューマンエラーの個々の発生率は、一般に非常に低いものであるが、あらゆる作業で、あらゆる人が起こす可能性がある。発生した事象に対して、根本原因が追及されなければ、「一社員の不注意が原因であった」と簡単に処理され、事故を起こした当事者が「今後は気を付けます」と反省して完結してしまう。これでは「もぐらたたき」にすぎず、全社的なヒューマンエラーの防止にはつながらない。別の誰かがまた同じような過ちを犯し、たとえそれが軽微なものであったとしても何度も繰り返しているうちに、ある日突然重大事故に発展してしまう。

ハインリッヒの法則という労働災害の経験則がある。米国の損害保険会社で技術・調査部の副部長をしていたハーバート・ウィリアム・ハインリッヒという人物が 1929 年 11 月に、労働災害の発生確率を分析した結果を論文として発表したもので、「一件の大きな事故・災害の裏には、29 件の軽微な事故・災害、そして 300 件のヒヤリ・ハットがある」とされる。重大事故を防止するためには、事故の発生が予測されたヒヤリ・ハットの段階で対処していくことが重要である、というものである。

啓発教育を徹底して行うことや日常の運用の確認を励行することは、事業者にとって重要な事故の未然防止対策である。しかし、これらの対策に加えて、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ものであるという前提のもとで、記憶、知覚、判断、動作の機能のうち、エラーしやすいものを人間よりも確実で信頼できる機械等に置き換える、ま

た、作業方法を人間の特性に合わせて容易なものに見直す、といったことを、ヒヤリ・ハットを経験した段階から実行していくことがヒューマンエラーに起因する重大事故を防止する最善策と考える。

一方、パスワードリスト攻撃（なりすまし）による不正アクセスについては、インターネットサービスサイトを運営する事業者の努力だけで防ぐことはできない。インターネットサービスの安全な利用は、利用者が適切にパスワードを管理することが前提であり、前提が覆されている状態のままでは事業者にはなすすべがない。

IPA が 2014 年 8 月に発表した実態調査報告書によると、「金銭に関連したサービスサイトで、同一のパスワードを利用している」という回答が 25.4%あり、金銭に関連したサービスサイト以外での使い回しを合わせると、全体として、41.8%がパスワードを使い回している。また、パスワードを使い回している理由については、「(パスワードを同一にしないと) パスワードを忘れてしまうから」という回答が 64.1%、「複数のパスワードを管理するのが手間だから」が 51.3%、「ひとつのパスワードを利用していると簡単だから」が 42.2%という結果である。このように利用者は同じ ID・パスワードの組み合わせを複数のサイトで使用する傾向が強いため、パスワードリスト攻撃の成功率は高くなっている。

複数のインターネットサービスを安全に利用するには、それぞれ異なる組み合わせで ID・パスワードを設定する必要がある。とは言うものの、すべてを記憶するのは容易ではない。それならば、複数の ID・パスワードを容易に管理することができれば、それらを使い回しする必要がなくなることになる。管理方法として例えば、「第三者にわからないように紙にメモをする」「ID とパスワードを記載したリストをパスワード付電子ファイルとして保持する」などが思いつく。しかし、いずれも紛失、漏えい等のリスクに加え、人間の怠慢という究極のリスクが伴う。やはりこの場合もヒューマンエラー対策と同様に、信頼できるパスワード管理ツールを使用することが最も安全で簡単な管理方法と言えるのではないだろうか。

以上