平成 28 年 6 月 7 日

平成 27 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27年度（平成27年4月1日～平成28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。

１．事故報告の概要

平成 27 年度の事故報告件数及び事業者数は 154 件（54 社）であった。

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 40 件（26.0%）、次いで、「電子メールの誤送信」が 32 件（20.8%）、「委託先事業者による事故」が 28 件（18.2%）、「発送物の誤送付・誤封入」が 24 件（15.6%）、「FAX の誤送信」が 11 件（7.1%）であった。

例年報告件数の上位を占める 5 種のヒューマンエラーに関連する報告が平成 27 年度は全報告件数の 87.7%を占める結果となった。

また、その他にもヒューマンエラー関連では、「誤廃棄・誤消去」が 3 件（1.9%）、「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。これらを合算すると、平成 27 年度のヒューマンエラーに関連する事故報告件数は 140 件で、全体に占める割合は 90.9%になる。

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 40 件（26.0%）であった。1 件の紛失事故の中に複数の媒体を紛失した事案も含まれている。

携帯電話の紛失は 20 件報告されている。帰宅途中に飲食店に立ち寄り酒に酔った状態での紛失が目立つ。ただし、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、書類の紛失は17件あった。紛失の経緯は、「顧客から預かった後に自転車で搬送途中に風で飛ばされた」「書類を箱詰めにした際に誤廃棄した可能性がある」「帰宅途中で書類が入った鞄を電車の網棚に置き忘れた」などである。名刺を含む書類に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ず、二次被害につながる可能性があるため注意が必要である。

その他、ノートパソコンの紛失は4件、記憶媒体の紛失は2件報告されている。ただし、PC の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。

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24年度 (n=59社)		平成25年度 (n=45社)		平成26年度 (n=50社)		**平成27年度 (n=54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）	31	22.5%	26	18.2%	38	25.0%	**40**	**26.0%**
電子メールの誤送信	35	25.4%	37	25.9%	32	21.0%	**32**	**20.8%**
委託先事業者による事故	21	15.2%	20	14.0%	15	9.9%	**28**	**18.2%**
発送物の誤送付・誤封入	12	8.7%	15	10.5%	33	21.7%	**24**	**15.6%**
FAXの誤送信	15	10.9%	16	11.1%	12	7.9%	**11**	**7.1%**
小　計	114	82.6%	114	79.7%	130	85.5％	**135**	**87.7%**
プログラムミス	3	2.2%	4	2.8%	4	2.6%	6	3.8%
盗難（空き巣・車上荒らし・置き引き・強盗）	5	3.6%	6	4.2%	5	3.3%	5	3.2%
誤廃棄・誤消去	0	0%	0	0%	0	0%	3	1.9%
データベース等への誤入力・誤処理	4	2.9%	1	0.7%	2	1.3%	2	1.3%
不正アクセス	0	0%	5	3.5%	5	3.3%	1	0.7%
従業者による不正持出・不正利用	0	0%	0	0%	1	0.7%	1	0.7%
なりすまし	0	0%	0	0%	0	0%	1	0.7%
宅配便・郵便による紛失	3	2.2%	7	4.9%	2	1.3%	0	0%
その他	9	6.5%	6	4.2%	3	2.0%	0	0%
合　計	138	100%	143	100%	152	100%	**154**	**100%**

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、事業者としての管理体制と携行者である従業者一人ひとりの心構えが問われることになる。

（2）電子メールの誤送信による事故について

電子メールの誤送信は32件（20.8%）報告されている。報告の内容は、「Bccで送るところを誤ってCc又はToで送った」「送信すべき宛先の確認を怠り、関係のない第三者に送ってしまった」「オートコンプリート機能により、よく似た第三者のメールアドレスが宛先に自動追記され、確認ミスにより誤送信した」などの事案が顕著である一方で、「添付ファイル付きメールをBccで複数人へ送信したところ、自動暗号化の設定ミスにより、パスワードの自動送信メールでBccの宛先が送信先全員に見える状態となっていた」という受信者側からの指摘がないと発信者側では気付きにくい事案もあった。

基本的な対策としては、事業者が啓発教育を通じて電子メール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、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、ツールを正しく併用することが一層効果的である。

（3）委託先事業者による事故について

委託先事業者による事故は28件（18.2%）報告されている。事故の内容は、「誤送付」「紛失」「メール誤送信」「誤入力・誤処理」「FAX 誤送信」であり、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。

また、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。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。

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 24 年度	平成 25 年度	平成 26 年度	平成 27 年度
誤送付	5	12	8	17
紛失	9	0	4	4
メール誤送信	2	2	0	3
誤入力・誤処理	1	0	1	2
FAX 誤送信	3	4	0	2
プログラムミス	0	1	1	0
宅配便業者の誤送付	0	0	1	0
不正利用	0	1	0	0
Winny	1	0	0	0
合計（件）	21	20	15	28

なお、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重要である。

（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 24 件（15.6%）の報告があった。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」「源泉徴収票」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。

（５）FAX の誤送信による事故について

FAX の誤送信は 11 件（7.1%）報告されている。誤送信の経緯は、「FAX 番号を間違えた」

がほとんどであるが、その他「二人体制で確認作業を行ったが、結果的に二人とも確認を怠った」「ワンタッチダイヤルの選択ミス」「コールセンターによる番号の登録ミス」などであった。

誤送信対策としては、「短縮ダイヤルを使用することを義務付けし、さらに短縮ダイヤルのメンテナンス要員を任命し、定期的に登録内容のチェックをする」「送信する際には必ず複数職員で相互に確認しながら送信する」などが考えられるが、要するに、送信者は正しい宛先へ送信することを念頭に置いて送信することである。

（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、「プログラムミス」が 6 件（3.8%）、「盗難（空き巣・車上荒らし・置き引き・強盗）」が 5 件（3.2%）、「誤廃棄・誤消去」が 3 件（1.9%）、「データベース等への誤入力・誤処理」が 2 件（1.3%）、「不正アクセス」が 1 件（0.7%）、「従業者による不正持出・不正利用」が 1 件（0.7%）、「なりすまし」が 1 件（0.7%）報告されている。

「不正アクセス」に関する報告内容は、「従業者に届いたスパムメール（Flipora-Connect with Friends）に対し、誤った操作をした結果、関係する数百件のメールアドレス宛にその従業者名義のスパムメールが送信された」というものであった。これは、例えば、組織のメール機能を Google Apps で利用している場合、このサービス連携を不用意に許可すると、組織内で使用している連絡先情報等が読み取られ、自社名義の招待メールが送信されるというものである。招待メールが取引先に届いた場合、さらに同じようにサービス連携を許可してしまうことでのメールの拡散や、場合によっては自社の信用を損なう可能性も考えられる。同様の被害に遭ったと思われる事業者や大学などが実際に Web サイト上で注意喚起を行っている。

このような被害を防ぐには、「メール内容を確認し、覚えのない友達紹介などのメールには注意し、送信元、メールアドレス、本文等を確認し、安易にファイル内のリンクや添付ファイルを開かないこと」「アプリケーションが要求するアカウント連携が適切かを確認し、使用の可否を検討すること」「アプリケーションとアカウントの連携を行った場合に、アプリケーションによっては、他の外部サイトにアカウントを作成し、情報が保持される場合があるので、事前に十分な調査を行った上でアプリケーションを使用すること」など、組織内のセキュリティ意識を高めるため、従業者への注意喚起や、社内ルールの改善が必要になる。

また、「従業者による不正持出・不正利用」に関する報告内容は、「役員クラスの従業者が退職前に、採用応募者情報を自身のスマートフォンに格納して持ち出し、同業の再就職先で

利用した」というもので、不審に思った採用応募者本人からのJIPDECへの訴えにより発覚したものである。仮に個人情報を持ち出された事業者に不利益が生じていれば、刑事事件に発展する可能性のあった事案である。

最後に、「なりすまし」に関する報告であるが、「某社を名乗る人物から当社の某役員から頼まれ、当社社員宛に招待状を送りたい旨電話があった際、あらかじめ確認せずに社員十数名の個人情報を提供し、後で某役員へ確認したところ事実ではなかった」という事案であった。プライバシーマーク付与事業者として個人情報を提供する際の社内ルール（相手方を確認してから提供すること）を遵守していれば防げたはずであるが、咄嗟の判断ができなかったことによるものである。今後の対策としては、例えば、公的機関を名乗る人物が従業者の特定個人情報の提供を要求してきたときに備え、不用意に提供することがないように、教育を通じて第三者提供を行う際の社内手順を従業者に対して十分に浸透させておくべきである。

以上