2017 年 6 月 5 日

平成 28 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28年度（平成28年4月1日～平成29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、事故の傾向と主な注意点について取りまとめた。

1. 事故報告の概要

平成 28 年度の事故報告件数及び事業者数は 171 件（64 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、①「電子メールの誤送信」が 36 件（21.1%）、次いで、②「発送物の誤送付・誤封入」が 31 件（18.1%）、③「従業者による書類・携帯電話・パソコンの紛失」が 30 件（17.5%）、④「委託先事業者による事故」が 29 件（17.0%）、⑤「FAX の誤送信」が 13 件（7.6%）であった。

平成 28 年度は、報告件数のトップ 5 が、全報告件数の 81.3%を占める結果となった。

2. 内容別に見た事故の概要と防止のための注意点

(1) 電子メールの誤送信による事故について

電子メールの誤送信は 36 件（21.1%）報告されている。報告の内容は、「Bcc で送るべきところを誤って 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、関係のない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」という事案が主であるが、「採用活動で学生 1 名のみに連絡するところ、誤って学生800名分のメールアドレスを登録したメーリングリストへ送信してしまった」という、より深刻な事案もあった。

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。

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 25 年度 (n=45 社)		平成 26 年度 (n=50 社)		平成 27 年度 (n=54 社)		**平成 28 年度 (n=64 社)**	
	件数	割合	件数	割合	件数	割合	件数	割合
①電子メールの誤送信	37	25.9%	32	21.0%	32	20.8%	**36**	**21.1%**
②発送物の誤送付・誤封入	15	10.5%	33	21.7%	24	15.6%	**31**	**18.1%**
③紛失（書類・携帯電話・パソコンなど）	26	18.2%	38	25.0%	40	26.0%	**30**	**17.5%**
④委託先事業者による事故	20	14.0%	15	9.9%	28	18.2%	**29**	**17.0%**
⑤FAX の誤送信	16	11.1%	12	7.9%	11	7.1%	**13**	**7.6%**
小　計	114	79.7%	130	85.5%	135	87.7%	**139**	**81.3%**
盗難（空き巣・車上荒らし・置き引き・強盗）	6	4.2%	5	3.3%	5	3.2%	10	5.8%
プログラムミス	4	2.8%	4	2.6%	6	3.8%	9	5.2%
データベース等への誤入力・誤処理	1	0.7%	2	1.3%	2	1.3%	5	2.9%
不正アクセス	5	3.5%	5	3.3%	1	0.7%	2	1.2%
誤廃棄・誤消去	0	0%	0	0%	3	1.9%	1	0.6%
目的外利用・提供	0	0%	0	0%	0	0%	1	0.6%
宅配便・郵便による紛失	7	4.9%	2	1.3%	0	0%	1	0.6%
従業者等による不正持出・不正利用	0	0%	1	0.7%	1	0.7%	1	0.6%
なりすまし	0	0%	0	0%	1	0.7%	1	0.6%
フィッシング	0	0%	0	0%	0	0%	1	0.6%
その他	6	4.2%	3	2.0%	0	0%	0	0%
合　計	143	100%	152	100%	154	100%	**171**	**100%**

(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・誤封入は 31 件(18.1%)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」「地方税決定通知書」「高額療養費支給申請書」「個人番号申告書」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おり、対応を誤ると大きな事故に発展する可能性がある。

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に加えて、なにか良いツールがあれば積極的に活用するなど、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) 紛失(書類・携帯電話・パソコン)による事故について

個人情報の紛失は 30 件(17.5%)の報告があった。1 件の紛失事案に複数の媒体の紛失が含まれているものもある。

書類の紛失は 16 件あった。紛失の経緯は、「受託した役所の受付業務で出産育児一時金等申請書を紛失した」「顧客から預かった自動振替口座登録依頼書が保管していたはずのキャビネット内になかった」「鞄に入れていた顧客の名刺が気付かないうちに紛失していた」などである。

携帯電話の紛失は 14 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かなり顕著であるが、幸い「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。

ノートパソコンの紛失は、「飲食後電車内で居眠りをし、鞄ごとなくなっていた」という事案 1 件が報告されているが、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、二次被害は生じていない。

プライバシーマーク付与事業者の場合は、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、万が一紛失を契機に二次被害につながった場合は、被害が大きくなることも懸念される。そのため、携行者である従業

者一人ひとりの心構えは勿論のことであるが、事業者としての管理態勢も堅固にしておかなければならない。

一方、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、偶然悪意の第三者の手に渡った場合などは二次被害につながる可能性があるため、紛失しないよう特に注意が必要である。過去には、顧客の名刺を入れた自分の名刺入れを落とした際に、拾った第三者から、引き替えに金銭を要求されたという例もあった。

(4) 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、表－2のとおり、29 件(17.0%)報告されている。事故の内容は、多い順に「誤送付」「メール誤送信」「紛失」「FAX 誤送信」「目的外利用・提供」「誤入力・誤処理」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 25 年度	平成 26 年度	平成 27 年度	**平成 28 年度**
誤送付	12	8	17	**13**
メール誤送信	2	0	3	**7**
紛失	0	4	4	**4**
FAX 誤送信	4	0	2	**2**
目的外利用・提供	0	0	0	**2**
誤入力・誤処理	0	1	2	**1**
プログラムミス	1	1	0	0
宅配便業者の誤送付	0	1	0	0
不正利用	1	0	0	0
合計(件)	20	15	28	**29**

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必要である。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。

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事案が依然として多く見られる。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ので、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鑑みて事業者の選定及び管理を心掛けることが重要である。

(5) FAX の誤送信について

FAXの誤送信は13件(7.6%)報告されている。誤送信の経緯は、「FAX番号を誤った」「ゼロ発信である手順を誤った」「機械操作を誤り、関係のない第三者にも送信した」「社内で FAX 送信を依頼した際、誤った FAX 番号を伝えてしまった」などである。

FAX の誤送信は厄介なもので、うっかり番号を誤り、個人情報に限らず大切な情報が関係のない第三者へ送られても、誤送信先からの指摘がないと、なかなか気が付きにくい性質がある。

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」また、「送信する際には必ず複数で相互に確認しながら送信する」などが考えられるが、いずれの対策を取るにしても、送信者自身が正しい宛先(番号)へ送信することを念頭に置いていることが基本である。

(6) その他の事故について

その他の事故として、「盗難」が 10 件(5.8%)、「プログラムミス」が 9 件(5.2%)、「データベース等への誤入力・誤処理」が 5 件(2.9%)、「不正アクセス」が 2 件(1.2%)、そして、「誤廃棄・誤消去」「目的外利用」「宅配便・郵便による紛失」、「従業者等による不正持出・不正利用」「なりすまし」「フィッシング」がそれぞれ 1 件(0.6%)ずつ報告されている。以下に主な例を紹介する。

a) 盗難

「盗難」に関する報告は、「夜間帰宅途中に待ち伏せされて採用応募者情報、健康診断書等の入った鞄を奪われた」「鞄を電車の網棚に乗せて網棚を背に携帯電話の操作をしていた束の間に置き引きされた」「上着に入れていた顧客情報の入った財布を抜き取られ、後に財

布は戻ったが顧客情報は抜かれていた」などであった。

b) 不正アクセス

「不正アクセス」に関する報告は、「OS コマンドインジェクションの脆弱性を突かれてデータベースサーバ内の個人情報を盗まれた」「E コマースサイトに対し、悪意の第三者が外部で取得したと思われる顧客会員の ID・パスワードを利用して 2000 名分のログインを成功させ、会員情報を閲覧し、一部改ざんした」というものであった。

前者は、情報漏えいの他、改ざん・削除、不正なシステムの操作、ウィルス感染などの被害が起こり得る。また、これを踏み台に他サイトへ攻撃された場合は、被害者から一転して加害者になる可能性もあることから十分な対策が必要である。後者は、ユーザ側の ID・パスワードの使い回しに対する警告とも取れる事案である。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ことが推奨されているが、2015 年に IPA が行った調査では、サービス毎に異なるパスワードを設定している人は 27.3%という結果であった。こうした状況なので、悪意の第三者によるリスト型アカウントハッキングの成功率は依然として高い。

c) 従業者等による不正持出・不正利用

「従業者等による不正持出・不正利用」に関する報告は、「退職した元従業者が在職中に知り得た情報をもとに派遣スタッフにアクセスしていた」というもので、事業者への匿名の密告メールにより発覚したものであった。仮にこのことが原因で当該事業者に大きな不利益が生じた場合、元従業者や転職先事業者は不正競争防止法違反などで起訴される可能性もあるので、情報サービス事業者の社員が同業他社へ転職した場合などは、前職で知り得た情報の取扱いに十分注意する必要がある。

d) なりすまし

「なりすまし」に関する報告は、「××コールセンターの T を名乗る人物から当社の Y 専務取締役と仕事上の知り合いとのことで、Y 専務取締役から頼まれ、当社社員宛に展示会の招待状を送りたい旨電話があった際、応対した社員があらかじめ本人確認せずに社員十数名の個人情報（氏名、所属、性別）を口頭で提供してしまい、後に Y 専務取締役に確認したところ事実ではなかった」というものである。平成 27 年度に報告のあった 1 件の事案とは、被害に遭った事業者も地域も異なるが、手口はほとんど同じものである。

プライバシーマーク付与事業者として、電話、文書等で個人情報の提供依頼があった場合の対応手順（必ず相手方を確認してから提供するか否かを判断すること）を遵守していれば防げたものであるが、従業者が相手方の巧妙な話術によって冷静な判断ができなかったものと思われる。今後マイナンバー制度がより充実してくると、公的機関の職員を名乗る者が、さらに巧妙に従業者の個人番号などの提供を要求してくることも考えられる。そうした場合に備え、従業者が常に冷静な判断ができるように、日常の教育を通じて個人情報の第三者提供を行う際の手順を社内に十分に浸透させておかなければならない。

e) フィッシング

最後に「フィッシング」に関する報告であるが、「社員が取引先の請求書発行担当者を装ったメールであることに気付かずに、そこにリンクされたニセの請求書発行サイトに自身のメールアドレスとパスワードを入力してアクセスした結果、当該社員のメールアドレスから社内外数百件にフィッシングメールが発信された」というもので、危うくニセメールの受信者による負の連鎖につながるところであった。

このような被害を防ぐには、「メール内容を確認し、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」であるが、特にメールの内容が受信者の業務フローに合致している場合などは、注意を怠り無意識にアクセスしてしまう可能性がある。

主な対策として、添付ファイルがあった場合は、常にウィルスの可能性を疑う必要がある。ウィルス対策ソフトを導入し、ウィルス定義ファイルを最新に保っていれば、ウィルスの侵入阻止や侵入したウィルスの駆除ができるが、必ずしも万全ではない。少しでも不自然だと思うメールであれば、普段やり取りのある送信者からのメールであっても用心し、相手に確認を取るか、メールそのものを読まずに削除することである。一方、Web サイトの場合は、ブラウザのアドレスバーを確認して、アドレスが緑になる EV SSL を導入しているサイトであればすぐわかるが、そうでない場合は、「URL として表示されているアルファベットにおかしな点はないか」「鍵のアイコンが表示されていて SSL を導入している証明書の内容を表示できるか」などの見分け方がある。従業者がフィッシングメールを受信した際に備えて、あらかじめ注意喚起をするなど、社内のセキュリティ意識を高めておくことが重要である。

以上