2018 年 5 月 11 日

平成 29 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（以下「当該事業者」という。）から平成29年度（平成29年4月1日～平成30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。

なお、当協会が毎年度、当該事業者を対象とする事故報告について取りまとめを実施してきた『個人情報の取扱いにおける事故報告の傾向と注意点』は、今回(平成29年度分)を最終版とする。今後はJIPDECが付与事業者全体を対象とする事故報告について取りまとめを実施している『個人情報の取扱いにおける事故報告にみる傾向と注意点』を参照されたい。

1．事故報告の概要

平成 29 年度の事故報告件数及び事業者数は 108 件（56 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、「電子メールの誤送信」が 27 件（25.0%）、「発送物の誤送付・誤封入」が 26 件（24.1%）、「従業者による書類・携帯電話・パソコンの紛失」が 20 件（18.5%）、「委託先事業者による事故」が 11 件（10.1%）、その他 24 件（22.3%）であった。

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 27 件（25.0%）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」といった事案が 8 割強であるが、その他に「過去のメールを使い回し、宛先及び本文を修正し忘れて誤送信した」「添付ファイルに関係のない第三者の個人データが含まれているのを知らずに誤送信した」という事案もあった。

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 26 年度 (n=50 社)		平成 27 年度 (n=54 社)		平成 28 年度 (n=64 社)		**平成 29 年度 (n=56 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	32	21.0%	32	20.8%	36	21.1%	**27**	**25.0%**
発送物の誤送付・誤封入	33	21.7%	24	15.6%	31	18.1%	**26**	**24.1%**
紛失（書類・携帯電話・パソコンなど）	38	25.0%	40	26.0%	30	17.5%	**20**	**18.5%**
委託先事業者による事故	15	9.9%	28	18.2%	29	17.0%	**11**	**10.1%**
データベース等への誤入力・誤処理	2	1.3%	2	1.3%	5	2.9%	*7*	*6.5%*
盗難（空き巣・車上荒らし・置き引き・強盗）	5	3.3%	5	3.2%	10	5.8%	*6*	*5.5%*
FAX の誤送信	12	7.9%	11	7.1%	13	7.6%	*4*	*3.7%*
プログラムミス	4	2.6%	6	3.8%	9	5.2%	*2*	*1.9%*
不正アクセス	5	3.3%	1	0.7%	2	1.2%	*2*	*1.9%*
誤廃棄・誤消去	0	0%	3	1.9%	1	0.6%	*2*	*1.9%*
目的外利用・提供	0	0%	0	0%	1	0.6%	*1*	*0.9%*
宅配便・郵便による紛失	2	1.3%	0	0%	1	0.6%	0	0%
従業者等による不正持出・不正利用	1	0.7%	1	0.7%	1	0.6%	0	0%
なりすまし	0	0%	1	0.7%	1	0.6%	0	0%
フィッシング	0	0%	0	0%	1	0.6%	0	0%
その他	3	2.0%	0	0%	0	0%	0	0%
合　計	152	100%	154	100%	171	100%	**108**	**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 26 件（24.1%）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・パソコンなど）による事故について

個人情報の紛失は 20 件（18.5%）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 11 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 7 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、「飲食後帰宅途中の電車内で鞄ごとなくなっていた」という事案 2 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。

その他、業務で使用した顔写真入り SD カードの紛失事案 1 件が報告された。胸ポケットに入れていたところ、後に紛失したことに気付いたものであった。

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比較的行き届いており、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。

(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、11 件（10.1％）報告されている。事故の内容は、「誤送付」「紛失（書類・媒体）」「メール誤送信」「FAX 誤送信」「誤入力・誤処理」「プログラムミス」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 26 年度	平成 27 年度	平成 28 年度	平成 29 年度
誤送付	8	17	13	4
紛失	4	4	4	3
メール誤送信	0	3	7	1
FAX 誤送信	0	2	2	1
誤入力・誤処理	1	2	1	1
プログラムミス	1	0	0	1
目的外利用・提供	0	0	2	0
宅配便業者の誤送付	1	0	0	0
合計（件）	15	28	29	11

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（個人情報保護リスクに応じた）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) その他の事故について

その他の事故として、「データベース等への誤入力・誤処理」が 5 件(2.9%)、「盗難」が 6 件(5.5%)、「FAX の誤送信」が 4 件(3.7%)、「プログラムミス」が 2 件(1.9%)、「不正アクセス」が 2 件(1.9%)、「誤廃棄・誤消去」が 2 件(1.9%)、そして「目的外利用」が 1 件(0.6%)報告されている。主な例は以下のとおりである。

“盗難”

「盗難」の報告は、「飲食後の帰宅途中に駅近くで眠り込んだ隙に鞄ごと置き引きされた」「帰宅途中の飲食店で鍵付きロッカーに入れた資料がなくなった」「帰宅途中に立ち寄った飲食店で注意を逸らした隙に鞄ごと盗まれた」などであり、夜遅く帰宅途中に立ち寄った飲食店絡みであるという点で被害に遭った状況が共通している。

盗まれた鞄の中にはノート PC や第三者の個人情報が含まれる書類などが入っており、事業者としての持出管理の徹底と、従業者を深夜まで働かせないようにする意識改革が望まれる。

“FAX 誤送信”

「FAX 誤送信」の報告は、「FAX 番号を誤り、個人宅へ誤送信した」「FAX 送信した際に、誤って関係のない第三者の書類も一緒に送信してしまった」「誤った FAX 番号を入手して誤送信した」「システムに登録されている FAX 番号の転記ミスにより誤送信した」であるが、最近ではあまり FAX を利用しなくなったためなのか、例年は 10 件以上の事故報告があったものの、今年度は 4 件のみであった。

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。

“不正アクセス”

「不正アクセス」については、「PC 一台にリモートデスクトップ接続でログインされ、ランサムウェア本体ファイルを local admin のデスクトップに保存された」という報告があった。

ランサムウェアに感染するとコンピュータのファイルが暗号化され、OS が起動しなくなり、コンピュータが使用できない被害が発生する。暗号化されたファイルの復元は困難であるため、その重要度によっては企業存続に致命的なダメージを与える可能性があり、早期復旧のためには金銭要求に応じざるを得ない状況に陥ることが考えられる。

ランサムウェアに感染しないための有効な手段として、「OS やソフトウェアの脆弱性解消」、「ウィルス対策ソフトの導入」、「添付ファイルへの注意」などがあるが、これらの対策を実施していても 100%被害を防げるとは限らない。万が一ランサムウェアに感染したことでファイルを暗号化されてしまった場合のリスクを評価し、ファイルのバックアップ態勢を強化するなど、被害を低減させるための環境づくりが重要となる。

“目的外利用”

最後に、「目的外利用」であるが、「契約終了後に消去しなければならなかった派遣スタッフ等の個人情報が含まれるデータベースを、保有期間を定めずに保有し、一部のアクセス権者が、ビジネスパートナーから技術者の紹介を受けた際に当該データベースにアクセスし、派遣スタッフ登録の有無を確認するなどして利用することがあった」というもので、このデータベースに自身の個人情報が登録されていた元派遣スタッフからの JIPDEC への実名による告発により発覚したものであった。

本件は、事業者の従業者教育や内部監査が機能していなかったことによるものであるが、仮にプライバシーマーク制度の信頼性を損なうような大きな事故に繋がっていた場合は、プライバシーマークの“取り消し”にもなり得る事案であり、そうなると事業者の存亡にも関わってくる。

従業者教育や内部監査などの PMS 活動は、事業者が JIPDEC からプライバシーマークを付与してもらうための実績作りとして実施するものではない。事業者又その代表者が世間に対して恥を晒すことのないようにするための“予防処置”と捉えて実施すべきものである。新しい JIS 規格（JISQ15001:2017）から“予防処置”の文字が消えているのは、このため（PMS 活動自体が“予防処置”だから）である。肝に銘じて取り組んでほしい。

以上