平成 23 年 5 月 25 日

平成 22 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対策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認定を受けた事業者から平成22年度内に提出された「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纏めたので、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 164 件（84 社）であり、前年度の 129 件（67 社）に比べて件数、事業者数とも増加している。報告内容は、例年同様に軽微な事案がほとんどであるが、プライバシーマーク付与認定の一時停止処分を受ける結果となった誤入力・誤処理に起因する個人情報漏えい事故も含まれている。

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 62 件（37.8%）と過去 4 年間を通して最も多く、次いで委託先事業者による事故が 31 件（18.9%）、同報メール（複数の宛先に同一内容を一斉に送信するメール）を中心とする電子メールの誤送信が 28 件（17.1%）、発送物の誤送付・誤封入 15 件(9.1%)などが報告されており、毎年、事故の内容別件数の上位を占める「紛失」「委託先による事故」「電子メールの誤送信」「発送物の誤送付・誤封入」の報告件数が、全体の 82.9%を占める結果となっている。

事故原因は、ほとんどがヒューマンエラーに起因したものであり、過去のデータと比較してほとんど傾向は変わらないが、委託先事業者による事故（事故内容の内訳は、表－２を参照）が件数、比率ともに増加していることが顕著である。

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 19 年度 (n=88 社)		平成 20 年度 (n=73 社)		平成 21 年度 (n=67 社)		平成 22 年度 (n=84 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）	45	31.9%	52	43.7%	48	37.2%	62	37.8%
委託先事業者による事故	19	13.5%	19	16.0%	20	15.5%	31	18.9%
電子メールの誤送信	25	17.7%	21	17.6%	20	15.5%	28	17.1%
発送物の誤送付（誤封入）	16	11.3%	10	8.4%	15	11.6%	15	9.1%
小計	**105**	**74.5%**	**102**	**85.7%**	**103**	**79.8%**	**136**	**82.9%**
FAX の誤送信	2	1.4%	3	2.5%	4	3.1%	7	4.3%
盗難（空き巣・車上荒らし・置き引き）	10	7.1%	2	1.7%	4	3.1%	5	3.0%
宅配便・郵便による紛失	3	2.1%	5	4.2%	8	6.2%	4	2.4%
プログラムミス	8	5.7%	3	2.5%	2	1.6%	4	2.4%
ファイル交換ソフト（Winny など）	10	7.1%	1	0.8%	3	2.3%	2	1.2%
データベース等への誤入力・誤処理	0	0%	0	0%	4	3.1%	2	1.2%
従業者による不正持ち出し・不正利用	0	0%	1	0.8%	1	0.8%	2	1.2%
外部からの不正アクセス	1	0.7%	0	0%	0	0%	0	0%
その他	2	1.4%	2	1.7%	0	0%	2	1.2%
合計	**141**	**100%**	**119**	**100%**	**129**	**100%**	**164**	**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依然として高い割合を占めている。平成 22 年度に報告された 62 件の紛失事故のうち、携帯電話の紛

失が 41 件で全体の 66%を占めている。緊急時などの連絡用として常に携行していることから事故の発生率が高くなっているが、ほとんどの事業者では暗証番号ロックや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を使用しているため、実際に情報漏えい事故に繋がった事案はない。また、ノートパソコンの紛失について平成 22 年度の報告件数は 3 件のみで、ハードディスクへの暗号化措置などによりいずれも二次被害には至っていない。

プライバシーマーク事業者は、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されていることによって二次被害の防止に繋がっている。しかしながら、セキュリティ本来の目的は安全管理措置に頼ることではなく、ノートパソコンや携帯電話などの紛失自体を未然に防ぐことであり、そのためには事業者の仕組み作りと携行者一人ひとりの心構えが重要になる。

（2）委託先事業者による事故について

個人情報の取扱いに関連する事故は、自社のみならず委託先からも生じており、平成 22 年度は 31 件の報告があり、全体における比率は 18.9%、と前年の 20 件（15.5%）に比べて件数、比率とも増加している。

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 19 年度	平成 20 年度	平成 21 年度	平成 22 年度
誤送付	4	7	9	11
紛失	3	5	8	10
メール誤送信	5	2	0	4
Winny	6	3	1	3
宅配便による誤送付	0	0	1	1
誤入力・誤処理	0	0	0	1
不正利用	0	1	1	1
FAX 誤送信	0	0	0	0
盗難	1	0	0	0
プログラムミス	0	1	0	0
合計（件）	19	19	20	31

表－２によると、事故内容は、「書類の誤送付」「書類の紛失」「メール誤送信」といったヒューマンエラーに起因する事故がほとんどであるが、そのほか「自宅 PC から Winny による業務情報の流出」や「不正利用」に起因する事故も報告されている。これらの主たる原因についての報告では、「委託先における個人情報の取扱い状況を把握していなかった」「委託先の調査を定期的に実施していなかった」「定期的な業務報告を受けていなかった」といった管理の不徹底さが顕著である。

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。また、事故による経済的損失より、本人に及ぼす影響、社会的信用の失墜が大きいことを認識しなければならない。

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提供していないか」などを精査する必要がある。また、委託業務によって再委託、再々委託が生じる場合には、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。

最近では、プライバシーマーク認定事業者であることを委託先の前提条件としている事業者が増えているが、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心せず、委託業務の実態に見合った管理を心掛けることが、事故を防ぐための重要な要素である。

（3）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による事故は 28 件で全体の 17.1%を占めており、平成 19 年度からの発生比率は、ほぼ横ばいとなっている。

事故内容は、「メールの宛先を誤って送信した（13 件）」のほか、「同報メールの際に宛先が見える形（本来 Bcc で送信すべきところ To や Cc で送信する）で送信した（11 件）」ために、メールアドレスを漏えいする事案が依然として顕著である。

これらの対策としての基本は、メール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り、そのためには、事業者が教育などを通じてメール送信前の確認行為を義務付け、定期的にチェック機能を働かせる（運用の確認をする）ことであるが、そのほか「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、徹底した社内ルールや便利ツールを併用することで、より未然防止に効果的である。

なお、万が一添付ファイルの送信先を誤った場合に備えて、暗号化やパスワード保護等

の安全管理措置を講じることが二次被害防止策として有効である。

（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・誤封入による事故は 15 件（9.1%）で、発生件数は、前年度横ばいである。誤送付された発送物のなかには、例年同様に、地方税通知書、不採用となった応募者の履歴書、口座振替情報、契約書類、給与明細書、保険金支払い明細書など、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かかわ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もあり、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、作業にあたっての導入教育を義務付けるなどして、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心理的に負担の掛からない作業方法への転換を図ることなどが重要である。

（5）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、FAX の誤送信が 7 件（4.3%）、盗難（空き巣・車上荒らし・置き引き）が 5 件（3.0%）、宅配便・郵便による紛失、プログラムミスが各 4 件（2.4%）、Winny などファイル交換ソフトによる事故、データベース等への誤入力・誤処理、従業者による不正持ち出し・不正利用、その他が各 2 件（1.2%）報告されている。

従業者による不正持ち出し・不正利用やファイル交換ソフトによる事故などの内部犯罪・内部不正行為の割合は、ここ数年非常に低くなっている。過去にこれらに起因した情報漏えい事故により二次被害が生じ、業界の社会的信用失墜に繋がった事案があったことなどから、事業者が「性善説」から「性悪説」に基づくセキュリティ管理方針への転換を図り、従業者への啓発教育は言うまでもなく、「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」「従業者の自宅 PC のチェック」など、積極的な対応に取り組んでいることが功を奏してい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 22 年度の報告をもとに、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

述べてきたが、委託先から生じた事故を含め、傾向としては、単純なヒューマンエラーに起因した事故が顕著である。

プライバシーマーク事業者は、事業の用に供する個人情報を特定し、その取扱いの局面毎のリスクを洗い出し、対策を立て、残存リスクを洗い出す作業を行っているが、残存リスクの代表的なものが、このヒューマンエラーである。

ヒューマンエラー対策として、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、各事案が幸いにも二次被害に繋がるような大きな事故ではないために、特に究極の対応策が採られないまま、その都度是正処置が繰り返されている。

事業者では、教育などの機会を通じて従業者を作業方法に従わせることが一般的だと思われるが、これとは逆に、作業を構成する人間以外の要素である機器、文書、手順等の作業方法を従業者に合わせて（人間の記憶、知覚、判断、動作の機能を確実に行えるよう容易なものに）改善するエラープルーフ化対策がある。

これは、「ヒューマンエラーは、人間の意識レベルが下がったときに起こりやすいが、人間の意識レベルが下がることは避けられず、それを不注意だということで片付けてしまうと再発防止に繋がらない」という安全人間工学に基づく概念であり、ヒューマンエラー個々の発生率は概して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り、発生したものにいくら対策を施しても、同じ事象が別の人によって再び発生することから、是正処置（発生した事故の再発防止）よりも、むしろ予防処置（未然防止）に重点が置かれている。

「ポカヨケ」とも呼ばれ、注意力が下がって「ポカ」をすることは人間として避けられないことである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すことが事故を未然に防ぐために最も効果的だというものである。トヨタ生産方式をはじめ製造業分野における基本概念であり、また、事故が発生したら取り返しのつかない事態が想定される医療現場などでも採用されている概念であるが、情報サービス事業者にとっても十分参考になるはずである。

以上