（平成 27 年度）「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」

一般財団法人日本情報経済社会推進協会（JIPDEC）
プライバシーマーク推進センター
平成 28 年 8 月 22 日

平成 27 年度中に当協会(JIPDEC)及び審査機関（平成 27 年度末現在 18 機関）に報告があったプライバシーマーク付与事業者（以下、付与事業者）の個人情報の取扱いにおける事故についての概要を報告する。

平成 27 年度の事故報告内容は、事故の原因及び、盗難・紛失の媒体において、ほぼ前年度と同様の傾向にある。付与事業者各位においては、引き続き個人情報の取扱いに関する事故の再発防止に活用して頂きたい。

平成 27 年度の報告件数

① 796 付与事業者より 1,947 件の事故報告があり、前年度の 768 付与事業者 1,646 件より、事業者数、事故報告件数共に増加した。特に報告件数は 20%弱の増加となっている。
② 平成 27 年度末時点の付与事業者数（下記1．の「参考：有効付与事業者数の推移」を参照）に占める事故報告事業者の割合は 5.4%であり、平成 26 年度（5.5%）、平成 25 年度（5.4%）とほとんど差異はない。

報告内容の概要

① 事故の原因は、「紛失」（22.2%）が最も多く、次いで「メール誤送信」「封入ミス」「宛名間違い等」の順に割合が多い。前年度に比べ、「紛失」「宛名間違い等」の割合は減少したが、「メール誤送信」「封入ミス」は増加した。
② 事故の原因の『その他』では、「目的外利用」が前年度より大幅に増加（11 件⇒22 件）したが、「内部不正行為」は前年度より若干減少した。
③ 盗難・紛失の媒体について、スマホを含む携帯電話やノートPC・タブレット端末は、平成 25 年度から件数・割合共に増加し、特に、ノートPC・タブレット端末の増加が目立っている。一方、平成 25 年度には過半数を占めていた書類の割合（52.6%）が、平成 26 年度に減少（48.3%）し、平成 27 年度は更に減少（46.9%）した。

1. 事故報告(*)のあった付与事業者数と事故報告件数(平成 23～27 年度)

年　度	23 年度	24 年度	25 年度	26 年度	27 年度
付与事業者数	682	620	736	768	796
事故報告件数	1,434	1,447	1,627	1,646	1,947

(*) 配送物の中に個人情報が含まれていても、配送委託先のミスが原因で事故(配送ミス・紛失等)が発生した場合は、欠格性(欠格レベル)の評価(PMK510)において不可抗力によるものとし、「措置なし」の評価を行っている。当該理由により、措置なしと評価した付与事業者数と事故報告件数は含めていない。

参考:有効付与事業者数の推移(平成 23～27 年度の各年度末時点)

年　度	23 年度	24 年度	25 年度	26 年度	27 年度
付与事業者数	12,564	13,075	13,591	14,044	14,755

2. 付与事業者から報告のあった原因別事故報告件数と割合(平成 25～27 年度)

原因		漏えい							盗難・紛失			その他(※4)	合計
		誤送付(※2)					ウィルス感染	その他漏えい(※3)	盗難		紛失		
		宛名間違い等	配達ミス	封入ミス	FAX	メール			車上荒し	置き引き等			
平成 25 年度	報告件数	270	2	243	126	274	2	194	4	28	404	80	1,627
	割合(%)	16.6	0.1	14.9	7.8	16.9	0.1	11.9	0.3	1.7	24.8	4.9	100.0
平成 26 年度	報告件数(※1)	282	1	275	126	305	1	114	8	40	416	80	1,648
	割合(%)	17.1	0.1	16.7	7.6	18.5	0.1	6.9	0.5	2.4	25.2	4.9	100.0
平成 27 年度	報告件数(※1)	311	5	334	157	409	6	135	13	29	435	121	1,955
	割合(%)	15.9	0.3	17.1	8.0	20.9	0.3	6.9	0.7	1.5	22.2	6.2	100.0

※1 :報告件数について

1 件の事故報告について、複数の原因が存在する場合があることから、平成 26 年度及び平成 27 年度においては、事故報告件数と原因別事故報告件数の合計は一致しない。

※2 :「誤送付」の分類について

- 「宛名間違い等」は、誤送付の原因となる配送に関係する事務処理上のミス(宛名書き間違い、誤登録・誤入力等)及び渡し間違い等である。
- 「配達ミス」は、付与事業者自らが配達した際の間違い等である。

※3 :「その他漏えい」の内容について

「その他漏えい」には、『プログラム/システム設計ミス』『不正アクセスによる漏えい』『口頭での漏えい』及びその他『ヒューマンエラーと考えられるもの』等が含まれる。

平成 25～27 年度の「その他漏えい」の内訳は以下の通り。

内容		プログラム/システム設計・作業ミス	システムのバグ	不正アクセス・不正ログイン	口頭での漏えい	その他（事務処理・作業ミス等）	合計
平成25年度	報告件数	74	3	36	33	48	194
平成26年度	報告件数	44	4	27	17	22	114
平成27年度	報告件数	40	1	24	21	49	135

※4 :「その他」の内容について

平成 25～27 年度の「その他」の内訳は以下の通り。

内容		不正取得	目的外利用	同意のない提供	内部不正行為	誤廃棄	消失・破壊	左記に分類できない内容	合計
平成25年度	報告件数	1	20	5	7	23	4	20	80
平成26年度	報告件数	3	11	9	12	28	5	12	80
平成27年度	報告件数	1	22	7	9	28	7	47	121

3. 事故に対する主な注意事項等

（1）目的外利用等の事故について

「本人が想定していなかった目的で個人情報を使われた」との内容の事故報告は、『目的外利用』の事故として分類しているが、「手続・処理上の過失等により発生する目的外利用」と、「従業者の認識不足や不正による目的外利用」に大別できる。

平成 27 年度の「目的外利用」の事故報告件数は、全報告件数 1,947 件のうち 22 件であった。

一方、同年度に消費者相談窓口等に申出があった、「目的外利用」に関する相談件数は、全相談件数 422 件のうち 20 件であり、いずれにおいても、件数としては決して多くはないが、前年度より事故報告・相談共に増加傾向にある。

「目的外利用の結果、個人情報が漏えいした」という事例では、「漏えい」として集計するため、実際の発生件数はもう少し多くなる。また、事故報告事例と相談事例の内容が必ずしも一致しているわけではないものの、事故報告件数と相談件数を単純に比較した時に、「目的外利用」は本人からの苦情につながるリスクが高いということが推測される。

たとえ、従業者の認識不足から「行ってしまったこと」であっても、「事業者として取得した個人情報」が本人の想定外で使われたとなれば、本人は事業者に対して不信感を抱くことにもなることから、事業者の信頼性確保のためにも事故の未然防止が重要と考える。

＜手続・処理上の過失等により発生する目的外利用に関して＞

- 「大量に処理を行う時」「新規システム導入によるデータ移行時」「同姓同名が存在」等の場合に、『本人の意思に反する利用』（例えば、解約と利用停止の手続済みの元会員に連絡を入れてしまった）や、『対象を取り違えた利用』（例えば、A社・B社兼務の社員が、A社社員として名刺交換した情報をB社のDM送付に利用した）が発生し、個人情報の目的外利用となる。
- 手続・処理上の過失等により発生する目的外利用の防止策としては、手順やルールの見直しとして、①作業実施ルールの確認・見直し、②チェックルールの確認・見直しを行うことの他、従業員管理の徹底、注意喚起・教育や委託先の管理・監督（例えば、再発防止策の確認、継続的なチェック、教育状況の確認等）を行うことも重要なポイントである。
- 手続ミスや処理ミスによる目的外利用は、事故を発生させた事業者もその所属組織も「目的外利用をした」という認識を持ち難いものであるが、「うっかり発生させた」のではなく、「意図的に使用したのではないか」と本人等に思われてしまうことも少なくなく、場合によっては、漏えい事故や紛失事故よりも組織に対する不信感を与えてしまうリスクが高くなるため、十分な注意が必要である。

＜従業者の認識不足や不正による目的外利用に関して＞

- 従業者の認識不足や不正による目的外利用としては、『認識不足による目的外利用』（例えば、業務委託先が委託業務で預託された個人情報を用いて、自社DMを送付した）や、『個人の利益等のための不正使用』（例えば、A社元社員が、A社就業時に使用していた「個人情報」をコピーして持ち出し、自身が始めたビジネスに関するDM送付・勧誘メールに利用した）又、『プライベートにおける不正使用』（例えば、担当者が顧客と私語を交わし、しばらく後に顧客携帯電話番号宛に「好意を示す内容のメール」を送信した）等がある。
- 従業者の認識不足や不正による目的外利用の防止策としては、体制の整備として、①組織整備、②アクセス制限を行うことの他、従業員管理の徹底、注意喚起・教育や、委託先の管理・監督を行うことも重要である。
- 具体的な防止策としては、『退職者による不正使用防止』（例えば、退職時に、個人情報記録媒体等の返却・廃棄の確認を行う、退職後、速やかにアクセス制御の設定を行う）や、『不正な持出しの防止』（例えば、個人情報を端末から出力する場合の出力管理の徹底、運用担当者以外のUSBポートを物理的に封鎖する）等が考えられる。
- プライベート使用・不正使用などの目的外利用は、漏えいなどが発生した場合とは異なる種類の影響が生じることがある。場合によっては、犯罪被害発生が想定され、それに伴う不安感（場合によっては恐怖感）を本人に与えてしまうこともあるため、苦情につながるケースも少なくない。したがって、この様な類の目的外利用が発覚した際には、速やかにその行為をストップさせ、再発防止策を講じ、誠実に対象者本人への説明対応を行うことが求められる。

（2）標的型攻撃メールに関して

- 平成 23 年、大手企業や衆議院・参議院などが標的型攻撃メールを利用したサーバ攻撃を受けたことから、平成 24 年 1 月末、独立行政法人情報処理推進機構（IPA）セキュリティセンターが、「標的型攻撃メール＜危険回避＞対策のしおり」の発行・公表を通じて、企業・組織内における、さまざまな側面からの対策を促すなど、各所で注意喚起が行われた。しかしながら、

それから、4 年以上経過した今でも、規模の大小はあるものの、その攻撃及び被害は続いている。

- 標的となった事業者の従業者が、メールの添付ファイルを開いたり、メール本文中のリンク等にアクセス（リンク等をクリック）したりしなければ、被害は防げると言われているが、攻撃を仕掛けてくる側は、「あの手この手で」「手を替え品を替え」巧妙に添付ファイルを開かせたり、リンクにアクセスさせたりしようとしている。また、企業が注意喚起を行うなどの対策を熱心に行い、従業者側も、日頃から標的型攻撃メールの被害にあわないように注意していたとしても、仕事が多忙な時などに、「標的型攻撃メール」という危ない存在に関する認識が甘くなり被害に遭うというケースも想定される。場合によっては、多数の従業員宛に巧妙な（どう見ても仕事関係のメールとしか思えないような）「標的型攻撃メール」が送信されて、複数の従業者が騙されてしまうというケースもあり得る。
- これなら 100%大丈夫という策がない以上は、「標的型攻撃メールに騙されないようにする（※1）」ことと、「万が一、騙された場合にも、被害につながらないようにする（※2）」ということを念頭において、可能な限りの対策を検討する必要がある。業種、業務内容、取扱う個人情報（内容・件数）などにより、それぞれの事業者がとるべき対策の内容もレベルも異なってくると考えるが、「今の対策で十分」と過信することなく、改めて、しっかりとしたリスク認識を持ち、最新情報の収集をするところからの見直しも重要である。

（※1）「サーバではじく」「従業者が危険を察知して無視・削除するよう従業者教育を行う等」
（※2）「情報が流出しない」「悪用されない」「すぐに発見できる」

標的型攻撃の防御対策等については

■セキュリティ・システムで入口対策（攻撃の侵入を防ぐ対策）に加え、出口対策（侵入後に被害の発生を防ぐ対策）を充実させる
■従業者の心構えとセキュリティ・システムの出口対策がポイントであり、組織全体のセキュリティレベルを向上させる

等が言われているが、独立行政法人情報処理推進機構（IPA）にて、「IPA テクニカルウォッチ：標的型攻撃メールの例と見分け方」等、標的型攻撃に関する資料を公表しているので参考にして頂きたい。

【参考】 標的型サイバー攻撃対策：http://www.ipa.go.jp/security/ta/

（3）盗難・紛失事故について

- 盗難事故（車上荒し・置き引き等）の報告件数は、前年度に比べ件数・割合共に若干減少（48 件：2.9%→42 件：2.2%）し、特に置き引き等の件数・割合の減少が目立っている。
- 紛失事故の報告件数は、前年度に比べ件数は増加したものの、全報告件数に占める割合は、前年度に比べ減少（25.2%→22.2%）した状況であるが、平成 24～26 年度と同様、件数・割合共に最も多い（435 件、22.2%）。

- 盗難・紛失の媒体別内訳は下記の表の通りである。全体的には平成 25～26 年度と同様に書類、スマートフォン(スマホ)を含む携帯電話の紛失が多く報告されている。スマホを含む携帯電話は、平成 25 年度に一旦減少したが、平成 26 年度には件数・割合共に増加し、平成 27 年度も更に増加した。(153 件:32.3%→166 件:32.6%)、一方、書類は前年度に比べ件数は微増であったものの、割合は減少し、平成 24～25 年度に過半数を占めていた書類の割合が、半数を下回る状況(46.9%)であった。
- 外出時・移動中の紛失事故は、「置き忘れ」「落下」「転倒」等が原因となって発生し、『手荷物が多い時』『飲酒・飲食時』『何か急いでいる時』等の状況において発生しているとの報告がある。また、重要な個人情報を「どうして持っていたのか」「どうして持って行ったのか」「持っているのに、なぜそのような事(行動)をしたのか」 と疑問を持つような報告もあり、【個人情報を持っている】という認識の薄さが感じられる事故も報告されていることから、紛失事故の発生し易い状況を回避することを意識した従業員教育も重要である。
- 盗難事故には「移動時の乗物内での盗難」「飲食店等での盗難」「路上・公園等屋外での盗難」「車上荒し」等があり、『持ち物から意識が薄れる時』『持ち物から遠ざかった時』『夜間の外出』等の状況において発生しているとの報告がある。万が一、事故が発生した場合に備え、媒体別の二次被害等防止策を講ずると共に、緊急時の対応ルールを確実に実行することが重要である。

盗難・紛失の媒体別内訳(平成 25～27 年度)

	媒体等	書類	携帯電話 スマート フォン	ノート PC タブレット 端末	USB メモ リ等可搬 記録媒体	その他の 電子機器	その他の 媒体 (※1)	バッグ類 (※2)	合計
平成25年度	盗難(32)	13	12	8	0	0	7	0	40
	紛失(404)	221	113	15	15	1	40	0	405
	計 (436)	234	125	23	15	1	47	0	445
	割合(%)	52.6	28.1	5.2	3.4	0.2	10.5	0	100.0
平成26年度	盗難(48)	13	14	16	0	2	2	2	49
	紛失(416)	216	139	20	19	0	29	2	425
	計 (464)	229	153	36	19	2	31	4	474
	割合(%)	48.3	32.3	7.6	4.0	0.4	6.6	0.8	100.0
平成27年度	盗難(42)	19	19	15	0	0	5	0	58
	紛失(435)	220	147	33	14	0	38	0	452
	計 (477)	239	166	48	14	0	43	0	510
	割合(%)	46.9	32.6	9.4	2.7	0	8.4	0	100.0

(注 1) 盗難・紛失のカッコ内は事故報告件数。
(注 2) 盗難や紛失は、一つの事故で、複数媒体が関係することもあるので、合計と事故報告件数は合致しない。
(※1)その他の媒体:名刺(名刺入れ)、セキュリティカード、検体、年金手帳、健康保険証、運転免許証 等
(※2)バッグ類:個人情報の盗難・紛失の事故であるが、収納されていた媒体が不明のもの。

≪事故担当のＰ子より　一言≫

事故の未然防止と従業員教育について

事故を発生させないことが大事なのは言うまでもないことですが、万が一、事故を発生させた場合の事後対応の重要性についてもきちんと従業員の教育に盛り込んでおく必要があるかと考えます。

事故を発生させたら、どういう影響があるのか、どういう事後対応が必要となるのか、また、事後対応を疎かにした場合には、どういうリスクがあるのかといったようなことを、「個人情報保護」という観点に加えて、「真の意味での業務の効率化」「内外からの信用維持・向上」という観点からも、従業者ひとりひとりがシミュレーションしたり、ディスカッションしたりする機会を設けてみるのも、事故防止には効果的な方法の１つと言えるかと思います。

＜参考＞

平成 17 年度～平成 26 年度の「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」については、こちらを参照してください。