（平成 26 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 27 年 8 月 25 日

平成 26 年度中に当協会(JIPDEC)及び審査機関（平成 26 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 26 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、おおよそ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 26 年度の報告件数

① 768 付与事業者より 1,646 件の事故報告があり、前年度の 736 付与事業者：1,627 件より、事業者数、事故報告件数共に若干増加した。
② 平成 26 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 5.5%であり、前年度（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」（25.2%）が最も多く、次いで「メール誤送信」「宛名間違い等」「封入ミス」の順に割合が多く、前年度とほぼ同様の傾向にあるが、「封入ミス」「メール誤送信」の増加が目立つ。
② 盗難・紛失の媒体について、全体的には平成 24～25 年度と同様に書類、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やノートPCは、平成 25 年度に一旦減少したが、平成 26 年度には件数・割合共に増加した。（125 件：28.1%→153 件：32.3%）一方、平成 24～25 年度に、過半数を占めていた書類の割合が若干減少し、半数を下回る割合（48.3%）であった。

1．事故報告(*)のあった付与事業者数と事故報告件数(平成 22～26 年度)

年　度	22 年度	23 年度	24 年度	25 年度	26 年度
付与事業者数	691	682	620	736	768
事故報告件数	1,590	1,434	1,447	1,627	1,646

(*) 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 22～26 年度の各年度末時点）

年 度	22 年度	23 年度	24 年度	25 年度	26 年度
付与事業者数	12,091	12,564	13,075	13,591	14,044

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 24～26 年度）

原因		漏えい							盗難・紛失			その他（※3）	合計
		誤送付（※1）					ウィルス感染	その他漏えい（※2）	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24年度	報告件数	188	3	254	108	253	2	133	17	30	379	80	1,447
	割合（%）	13.0	0.2	17.6	7.4	17.5	0.1	9.2	1.2	2.1	26.2	5.5	100.0
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	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26年度においては、1件の事故報告に複数の原因が存在したことから、事故報告件数の合計と原因別報告件数の合計は合致しない。

※1:「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。

※2:「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 24～26 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	合計
平成24年度	報告件数	72	1	11	14	35	133
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

※3:「その他」の内容について

平成 24～26 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24年度	報告件数	1	15	7	12	21	13	11	80
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

3. 事故に対する主な注意事項等

【IT 関連事故に関して】

- 『IT 関連事故』は、コンピュータシステム、情報システム、ネットワークシステムにおける、あるいは IT 機器操作における事故等を指すが、前年度より報告件数は減少したものの、内容の複雑化が見られる。

- IT関連事故の特徴として以下の様なケースが挙げられる。
  (1)被害対象の規模が大きいケースがある。
  (2)金銭的被害に結び付くケースがある。
  (3)ニュースになるような話題性のあるケースがある。　等

＜システムプログラム上の問題による IT 関連事故＞

- システムプログラム上の問題による事故の原因は、「システム等の設計不備・設計ミス」「公開・表示設定ミス」「アクセス権設定ミス」「操作ミス」「検証不備・検証ミス」等であり、『システム導入時』『システム移行時』『専任担当に任せている』『委託先に全て任せている』等の状況において発生しているとの報告がある。
- 「設計不備・設計ミス」「操作ミス」「検証不備・検証ミス」等に対し具体的な防止策を講じると共に、
  (1)手順やルールの見直し
  (2)作業実施ルールの確認・見直し
  (3)チェックルールの確認・見直し
  (4)具体的な作業手順等の工夫
  (5)従業員への注意喚起・教育
  (6)委託先の管理
  等、体制整備の視点からの事故防止策を検討することが重要である。
  また、万が一、事故が発生した場合に備え、二次被害等防止策についても見直し、確実に実行できるような従業員教育も必要である。

＜不正行為による IT 関連事故＞

- 『不正行為』には外部からのものと、内部におけるものがあるが、平成 26 年度の従業員等による【内部不正行為】の報告は、平成 24～25 年度に比べ件数が増加し、重大事故に発展した事例もあり、事故の原因としては特に注意を要する内容である。
- 不正行為による事故は、「データの不正持出し・不正使用」「不正アクセス・不正ログイン」等があり、原因としては、①データの保管ミス　②アクセス制御ミス　③不正持出し防御ミス　④システムの脆弱性　⑤なりすまし　等が報告されている。
  また、『委託契約終了時』『雇用契約終了時』『個人情報の取扱権限の集中』『個人情報の放置』『委託先管理の問題』等の要因もあり、注意が必要である。
- 「データの不正持出し・不正使用」「不正アクセス・不正ログイン」への対策としては、
  (1)個人情報抽出用端末の制限及び、アクセス範囲および権限者を最小限にすること
  (2)権限を持つ者の不正行為の抑制のために、入退室記録、システムへのアクセスログ等の取得と、記録の確認を定期的に行うこと
  (3)退職者のアカウントの削除等、対応を確実に行うこと
  (4)システムの脆弱性等への対応を確実に行うこと
  (5)サイトへの外部からのアクセス状況の監視を継続すること
  (6)委託先における個人情報の取扱い状況の確認及び、再委託等の状況の把握等、適切な委託先の監督を行うこと
  (7)社内においては、常時監視していることを従業員に意識させる等、内部不正行為に対するけん制の対応を検討すること
  (8)内部での報告体制を明確にしておくこと
  等が挙げられる。
- 合わせて、社会人としてのモラルや、仕事や役割に対する責任感、ルール違反を行った際に予想される結果等についても教育を行い、個人情報保護の意識を向上させることが考えられる。
- 『内部不正行為』防止については、独立行政法人情報処理推進機構（IPA）にて、「組織における内部不正防止ガイドライン」を公表しているので参考にして頂きたい。

【盗難・紛失事故について】

- 盗難事故（車上荒らし・置き引き等）の報告件数は、前年度に比べ件数・割合共に増加し（32 件：2.0%→48 件：2.9%）、特に置き引き等の件数・割合の増加が目立っている。
- 紛失事故の報告件数は、前年度に比べ件数・割合共に微増し、全報告件数に占める件数・割合は、平成 24～25 年度と同様、最も多い（416 件、25.2%）。
- 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 24～25 年度と同様に書類、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やノートPC は、平成 25 年度に一旦減少したが、平成 26 年度には件数・割合共に増加した。（125 件：28.1%→153 件：32.3%）、一方、書類は前年度に比べ件数・割合共に減少し、平成 24～25 年度に過半数を占めていた書類の割合が、半数を下回る状況であった。
- 外出時・移動中の紛失事故は、「置き忘れ」「落下」「転倒」「強風等の外的要因」等が原因となって発生し、『手荷物が多い時』『疲れている時』『飲酒・飲食時』『睡眠不足』『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。置き忘れや落下防止等に対する具体的な紛失防止策や、手順やルールの見直し等の体制の整備のほか、紛失事故の発生し易い状況を回避する等を意識した従業員の行動がポイントとなることを認識した従業員教育も重要である。
- スマホやノート PC、タブレット端末の場合、大量の個人情報の保存が可能となり、事故等が発生した場合のリスクが一層大きくなっている。紛失・盗難の件数・割合は、前年度において減少がみられたものの、件数・割合共に増加した状況から、個人情報の漏えい対策として、リモートロックや遠隔消去等機能として対応できる対策のほか、機器を使用する従業員に対する教育が最重要課題であることの認識が必要と考える。
- 盗難事故には「移動時の乗物内での盗難」「飲食店やホテルロビー等での盗難」「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』『海外出張時』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が確実に実行できることが重要である。

盗難・紛失の媒体別内訳（平成 24～26 年度）

	媒体等	書類	携帯電話 スマート フォン	ノート PC、 モバイル 機器	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24 年度	盗難(47)	25	11	2	1	0	1	8	48
	紛失(379)	199	139	23	11	1	8	8	389
	計 (426)	224	150	25	12	1	9	16	437
	割合(%)	51.3	34.3	5.7	2.7	0.2	2.1	3.7	100.0
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

(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）、社員証、入館証（ID カード）、検体等。

（※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。

【封入ミス】【ファックス誤送信】【宛名間違い等】
の事故に関する主な注意事項等については、（平成 25 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」の資料を参考にして頂きたい。

≪最近の個人情報の取扱いにおける事故について≫

＜標的型攻撃に関する情報提供＞

昨今、多くの企業、団体が標的になっている標的型攻撃とは、特定の組織内の情報（機密情報や知的財産、ユーザーアカウント情報など）を狙って行われるサイバー攻撃の一種であり、その組織の従業者宛にコンピュータウイルスが添付されたメールを送ること等によって開始される。

※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1＞

平成 17 年度～平成 25 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。