平成 17 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

財団法人日本情報処理開発協会
プライバシーマーク事務局
平成 18 年 7 月 10 日

プライバシーマーク認定事業者から個人情報の取扱いにおける事故等の報告が、当協会プライバシーマーク事務局及び各指定機関に寄せられている。また、プライバシーマーク申請中事業者及びプライバシーマーク申請検討中事業者からも、「プライバシーマーク制度設置及び運営要領（10 情報開･セ第 126 号)」（以下「運営要領」という。）第 8 条の欠格条項に該当する事故等であるかとの問合せがある。

これに対し、当協会では個人情報の取扱いにおける事故等に係る欠格性を判断する基準を設定し、事故を起こした認定事業者には、事故の内容、経緯、原因、情報主体への対応、影響、再発防止策等につき詳細な報告を求めるとともに、設定された基準を参考に、当協会又は各指定機関から勧告、要請、注意等の措置を行う運用を行ってきた。

以下は、平成 17 年度中に当協会及び各指定機関に報告があったプライバシーマーク認定事業者等の個人情報の取扱いにおける事故等についての概要と、事業者への注意喚起を目的として、当協会に直接報告された事例にみる傾向と問題点・注意点を取りまとめたものである。

１．プライバシーマーク認定事業者の事故について

平成 17 年度の 1 年間に、当協会及び各指定機関で受け付けた、プライバシーマーク認定事業者の個人情報の取扱いにおける事故等の報告は 168 社（190 件）で、その内訳は、当協会による認定事業者からの報告が 128 社（144 件)、指定機関による認定事業者からの報告が 40 社（46 件）である。

なお、平成 16 年度中の認定事業者による事故報告は 51 社（53 件）であり、プライバシーマーク制度がスタートした平成 10 年度から平成 17 年度までに報告された、プライバシーマーク認定事業者の事故等の報告件数は、累計で 278 社（302 件）である。

ちなみに平成 17 年度、16 年度ともに「運営要領第 8 条の欠格条項に該当する事故」と判断し認定を取消した事業者はない。

２．当協会に報告があった事故報告について

２．１　事業者区分別の事故報告件数

平成 17 年度の 1 年間に、当協会で受け付けた、事業者（プライバシーマーク認定事業者、申請中事業者、申請検討中事業者）からの個人情報の取扱いにおける事故等の報告は、382 社より 554 件であった。うち認定事業者からの報告は前述のように 128 社（144 件）で、申請中事業者は 168 社（208 件)、申請検討中事業者は 86 社（202 件）であった。

なお、事故等は自社内だけではなく、委託先、代理店、子会社、協力会社、提携先等においても、554 件のうち 103 件（18.6%）が発生している。

表１　事業者区分別事故報告件数

事業者区分	報告事業者数	報告件数	（内、委託先等）
認定	128	144	32
申請中	168	208	48
申請検討中	86	202	23
合計	382	554	103

(*)　委託先等：　外部委託先、再委託先、代理店、子会社、協力会社、提携先等

２．２　事故の内容等

事故等の報告があった 554 件のうち、紛失・漏えいが 532 件で、全体の 96%を占めている。紛失・漏えいを原因別に分類すると、誤配送等（誤配送、誤封入、誤送付、印刷ミス等）の結果の漏えいが 396 件と最も多く、全体の 71.5%である。次に、盗難によるものが 84 件（同 15.2%）、うち車上荒らしによる盗難が 33 件（同 6.0%）である。また、メール配信ミスによる漏えいは 44 件（同 7.9%）、また、ファイル交換ソフト、ウィニー等を悪用したウィルス感染による漏えい（流出）は 8 件（同 1.4%）である。

なお、紛失・漏えい以外の事故 22 件（同 4.0%）の内訳は、個人情報の目的外利用・提供、不正アクセス、システム障害によるデータの破壊等である。

表２　事業者区分別・事故内容別件数

（単位：件数）

事業者区分	紛失・漏えい							その他	合計
	誤配送等	メール配信ミス	盗　難			ｳｨﾙｽ感染	計		
			車上荒らし	置き引き等	計				
認定	95	18	9	17	26	3	142	2	144
申請中	141	18	14	20	34	5	198	10	208
申請検討中	160	8	10	14	24	0	192	10	202
計	396	44	33	51	84	8	532	22	554
（割合）	71.5%	7.9%	6.0%	9.2%	15.2%	1.4%	96.0%	4.0%	100.0%

３．問題点・注意点

① 初歩的ミスの再発防止について

- 個人情報の集合体（リスト・名簿等の紙媒体、電子データが入った磁気媒体等）については、かなり徹底した管理が行われている状況ではあるが、伝票、伝票の控え、申込書類等、個別の個人情報が記載された書面についてのリスク認識が甘く、事故を繰り返すことが多い。
- 誤配送、誤封入、誤送付、印刷ミス等の結果の漏えいについては、確認の行為が重要であるが、ルールの周知・徹底だけではなく、発生原因を究明した上での根本的な対応策、個人情報の重みを認識した対応・措置を取ることが必要である。１件は初歩的なミスであっても、再発防止のためには、人的な問題やシステムでの対応等、事業の代表者の責任において対処すべき問題でもあることの認識が重要である。
- また、事故が発生した場合の本人への影響、経済的損失、社会的な信用失墜等を考えた対応・措置が出来ているかを検証することが重要である。

② 盗難への対応

- 置き引き、引ったくり、空巣、事務所荒らし、車上荒らし等による盗難については、盗難に遭遇しうることを意識した対応・措置が取られているか、また、遭遇した際の対応のルールが周知、徹底されているかが重要である。

③ ノートＰＣの安全対策

- ノートＰＣの紛失・盗難による個人情報の漏えいが多く報告されている。個人情報の社外への持ち出しのリスクの認識、個人情報をノートＰＣ等で社外に持ち出す場合のノートＰＣ本体のセキュリティ対策、格納されている個人情報に対するセキュリティ対策、移動時の安全対策等、総合的な対策を講じることが重要である。

④ 外部委託先の管理について

- 外部委託先での事故は、原則として、委託元が全責任を負うことを認識すること、事故が発生した場合の経済的損失より、社会的な信用等の失墜が大きいことを認識した管理が重要である。
- 委託先の選定とあわせ、『委託先管理』をルール化し、具体的な指導等を実施すること。

⑤ 事故発生時の対応

- 事故などが発生した場合、事故により被害を受けると思われる本人が必ず存在していること、本人にとっては重要な個人情報であること、個人情報の重みの認識は、個人差があること等を認識した対応処理を行なうことが重要である。
- 初期対応の失敗から、事故対応ではなく苦情対応へと発展することを認識すること。

⑥ 従業員教育について

- 個人情報の目的外利用・提供、不正アクセス、従業員による個人情報の不正持ち出し等の事故は、従業員教育を実施していても、防止することの難しい問題である。しかし、個人情報保護についての教育の成果が具体的に上がるように、教育の内容及び実施方法等については、定期的に評価を行い、見直しを行うことが重要である。

⑦ 日常の点検・確認

- ルールは整備されているが、ルール通り実施（運用）しているかを、日常的、継続的に点検・確認し、その結果を踏まえた注意喚起を行い、改善に結びつけることが重要である。

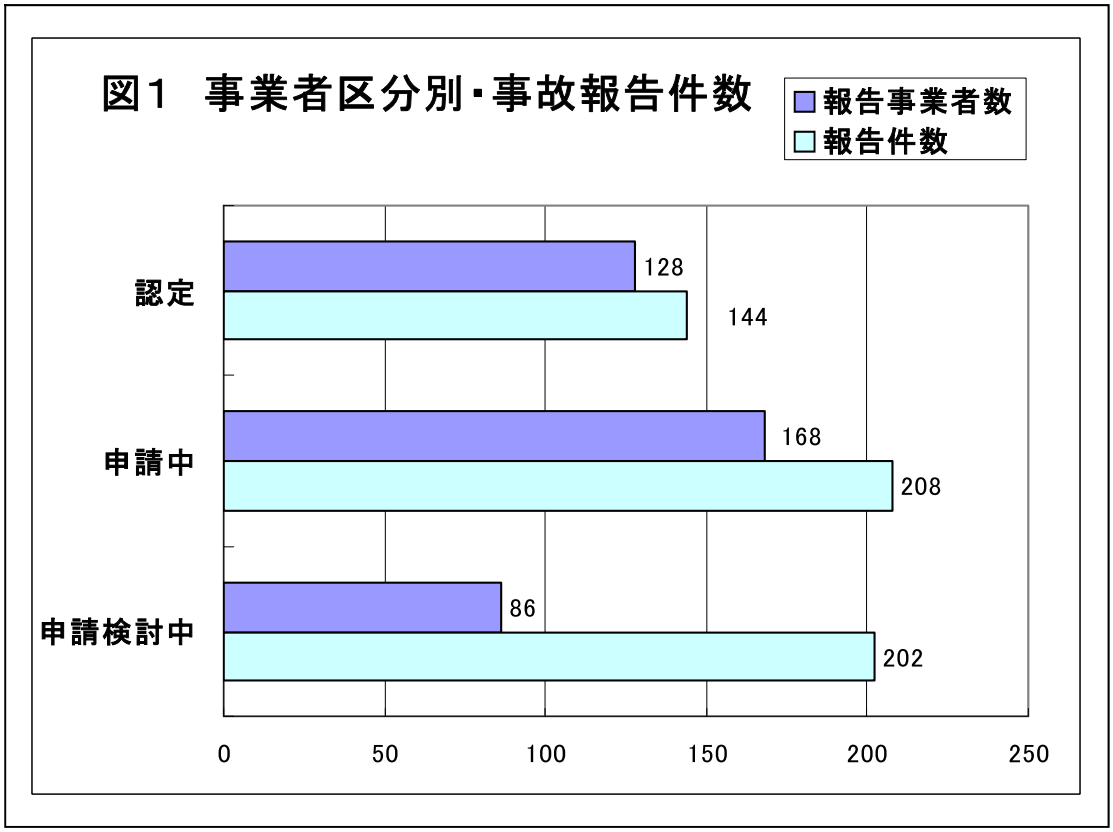
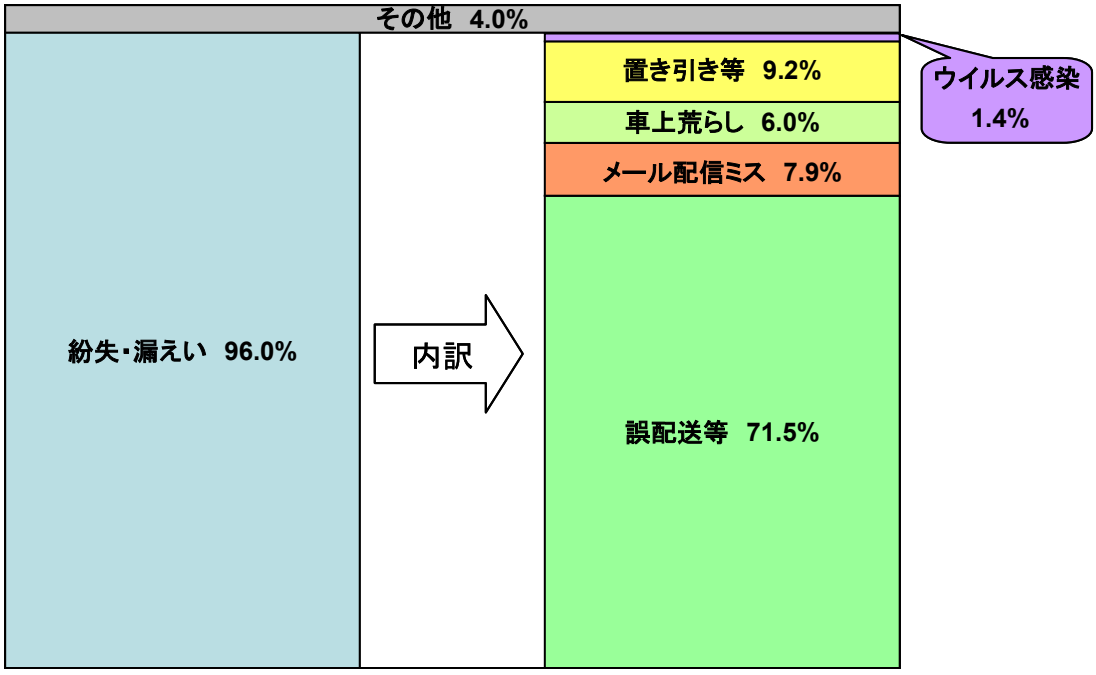


図2　事故内容件数



＊その他（個人情報の目的外利用・提供、不正アクセス、システム障害によるデータ破壊等）