（平成 18 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」

財団法人日本情報処理開発協会
プライバシーマーク推進センター
平成 19 年 6 月 11 日

平成 18 年度中に当協会及び各指定機関（平成 18 年度末現在 11）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ので公表する。

１．プライバシーマーク認定事業者の事故について

平成 18 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報告は 439 社 708 件で、平成 17 年度の 168 社 190 件に比較して、事業者数が約 2.6 倍に増加している。

報告の内訳は､当協会による認定事業者からの報告が 384 社 651 件(前年 128 社 144 件)、指定機関による認定事業者からの報告が 55 社 57 件（同 40 社 46 件）である。事故報告の増加は、プライバシーマーク認定事業者に対する事故報告の義務化と、認定事業者数そのものの増加に伴うものが主な要因と推測する。

なお、平成 18 年度中に「プライバシーマーク制度設置及び運営要領」の第 8 条の欠格条項に該当する事故と判断し、認定を取消したプライバシーマーク認定事業者はない。

表１　認定事業者の事故報告件数（平成 17～18 年度）

認定機関	日本情報処理開発協会		11 指定機関		合計	
	事業者数	事故件数	事業者数	事故件数	事業者数	事故件数
H18 年度	384 社	651 件	55 社	57 件	439 社	708 件
H17 年度	128 社	144 件	40 社	46 件	168 社	190 件

表２　年度別認定事業者数（平成 10～18 年度）

年度	10	11	12	13	14	15	16	17	18
認定数	58	71	96	120	172	286	553	2,395	3,798
累計	58	129	225	345	517	803	1,356	3,751	7,549

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 18 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、579 社より 1,276 件であった。うち認定事業者からの報告は前述のように 384 社 651 件で、申請中事業者は 146 社 439 件、申請検討中事業者は 49 社 186 件であった。

なお、事故等は自社内だけではなく、報告された 1,276 件のうち、委託先、代理店、子会社、協力会社、提携先等において、565 件（44.3%）が発生している。この委託先等での事故発生件数は、日本郵政公社 259 件と宅配便業者 72 件を合わせると、全体の 58.6%を占めているが、日本郵政公社及び宅配便業者による紛失･誤配事故等に関しては、欠格性判断の運用ルールにおいて、一定の条件が満たされている場合に限り、当該事業者に対して【処分なし】の判断を行っている。

表３　事業者区分別事故報告件数（平成 18 年度）

事業者区分	報告事業者数	報告件数	（内、委託先等）
認定	384	651	231
申請中	146	439	224
申請検討中	49	186	110
合計	579	1,276	565

(*)　委託先等：　委託先、代理店、子会社、協力会社、提携先等

表４　事業者区分別事故報告件数（平成 17 年度）

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：　委託先、代理店、子会社、協力会社、提携先等

２．２　事故の原因等

事故等の報告があった 1,276 件のうち、紛失・漏えいが 1,239 件で、全体の 97.1%を占めている。紛失・漏えいを原因別に分類すると、書簡・FAX 等の誤配（誤封入、印刷ミス等）による情報漏えいが 686 件と最も多く、全体の 53.8%を占めている。次いで紛失が 341 件（全体の 26.7%）、盗難によるものが 100 件（同 7.8%）である。

また、メール配信ミスによる漏えいは 73 件（同 5.7%）、ファイル交換ソフト（Winny、Share 等）のウィルス感染による漏えい（流出）は 39 件（同 3.1%）である。

事故の原因について平成 17 年度と比較すると、書簡・FAX 等の誤配による情報漏えいが大幅に増加し（37.2%→53.8%）、事故報告件数の過半数を占めている。次いで、ウィルス感染による漏えいの増加（1.4%→3.1%）が顕著である。一方、紛失による漏えい、

車上荒らし等の盗難による漏えいは減少している。

なお、紛失・漏えい以外の事故 37 件（同 2.9%）の内訳は、個人情報の目的外利用・提供、データの破壊･改ざん、従業員等の不正な持ち出し等に関係するものである。

表５　事業者区分別・事故原因別件数（平成 18 年度）　（単位：件数）

事業者区分	紛失・漏えい							その他	合計
	誤　配		盗　難		ｳｨﾙｽ感染	紛失	計		
	書簡・FAX 等	メール	車上荒らし	置き引き等					
認定	363	42	17	36	28	145	631	20	651
申請中	195	23	12	23	7	167	427	12	439
申請検討中	128	8	4	8	4	29	181	5	186
合計	686	73	33	67	39	341	1,239	37	1,276
（割合　%）	53.8%	5.7%	2.6%	5.2%	3.1%	26.7%	97.1%	2.9%	100.0%

表６　事業者区分別・事故原因別件数（平成 17 年度）　（単位：件数）

事業者区分	紛失・漏えい							その他	合計
	誤　配		盗　難		ｳｨﾙｽ感染	紛失	計		
	書簡・FAX 等	メール	車上荒らし	置き引き等					
認定	55	18	9	17	3	40	142	2	144
申請中	74	18	14	20	5	67	198	10	208
申請検討中	77	8	10	14	0	83	192	10	202
合計	206	44	33	51	8	190	532	22	554
（割合　%）	37.2%	7.9%	6.0%	9.2%	1.4%	34.3%	96.0%	4.0%	100.0%

３．問題点・注意点

① ファイル交換ソフト：「Winny」「Share」等への対策

- 平成 17 年から平成 18 年にかけて企業や公的機関等において、ファイル交換ソフトである「Winny」や「Share」等のウィルス感染による情報漏えいが相次ぎ、多くの企業等で「ファイル交換ソフトの使用禁止」や「個人 PC の持ち込み禁止」などが通達・徹底された状況にあるが、事故報告件数および報告全体に占める割合は、前年度に比べ増加している。
- 事故報告では、規程についての周知・徹底が実施されていたにも拘わらず、ルール違反や、個人の意識の問題から発生していることが多く、事業者としての対応策を根本から見直し、継続的な教育を行なうことが重要である。
- 個人情報の社外への持ち出し、持ち出した場合の個人情報の利用環境の制限、退職者の個人情報持ち出しに関する調査等がポイントとなる。

② 可搬記録媒体の紛失

- 個人情報の社外への持ち出しや授受に関連し、USB メモリー等の可搬記録媒体の紛失の事故報告も多く、紛失した際には大量の個人情報の漏えいになることを想定した管理（持ち出しについてのルール化、媒体の暗号化、授受記録等）が重要である。

③ 従業者教育

- JIS Q 15001：2006 の 3.4.5 において、従業者に個人情報保護マネジメントシステム(PMS)の運用を確実に実施できる力量を備えさせるための教育について規定されている。教育を効果的に実施することは難しいが、アンケートや小テストの実施等により、従業者の理解度を把握し、教育の内容及び実施方法等について、定期的に評価を行い見直しを行うこと、また、教育を受けたことを自覚させる仕組みを取り入れることが重要である。
- 一方、JIS Q 15001：2006 の 3.4.3.3 において、安全管理措置の遵守について、従業者に対し必要かつ適切な監督を行なうことを規定している。従業者との雇用契約時又は委託契約時に、個人情報の非開示契約の締結や、PMS に違反した場合の措置の実施等が、内部犯罪・内部不正行為の抑止にもつながることを認識し、従業員の監督を行なうことも重要である。

④ 内部犯罪・内部不正行為への対策

- 従業員の個人情報へのアクセスが可能な場合、不可能な場合の双方の状況において、従業員の不正行為による個人情報の漏えい等が発生し、一部、本人等への二次被害も発生している。
- 内部犯罪・内部不正行為への対策として、
  - ①業務内容や責任範囲に即したアクセス権の見直しを行い、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を行なった上で、定期的に記録の確認等を行なうこと
  - ③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、コミュニケーションや継続的な教育の中で自覚させ、個人情報保護の意識を向上させること

  等の運用（対応）が考えられる。

⑤ 外部委託先等の管理

- JIS Q 15001：2006 の 3.4.3.4 において、個人情報の委託先の監督について、特に委託先との契約内容が適切に遂行されていることを確認することが規定されていることから、委託先において事故が発生した場合、基本的に委託元が全責任を負うことを認識することが重要である。
- 事故が発生した場合の経済的損失より、本人に及ぼす影響や社会的な信用等の失墜が大きいことを認識した管理がポイントとなる。
- 1)委託業務に適合した委託先選定基準・判断（評価）基準であるか、2)委託業務内容に即した個人情報を預託しているか、3)継続業務においては定期的な業務のチェックを実施しているか等の『委託先管理』をルール化し、具体的な確認・指導等を実施することが重要である。

⑥ 監査の重要性

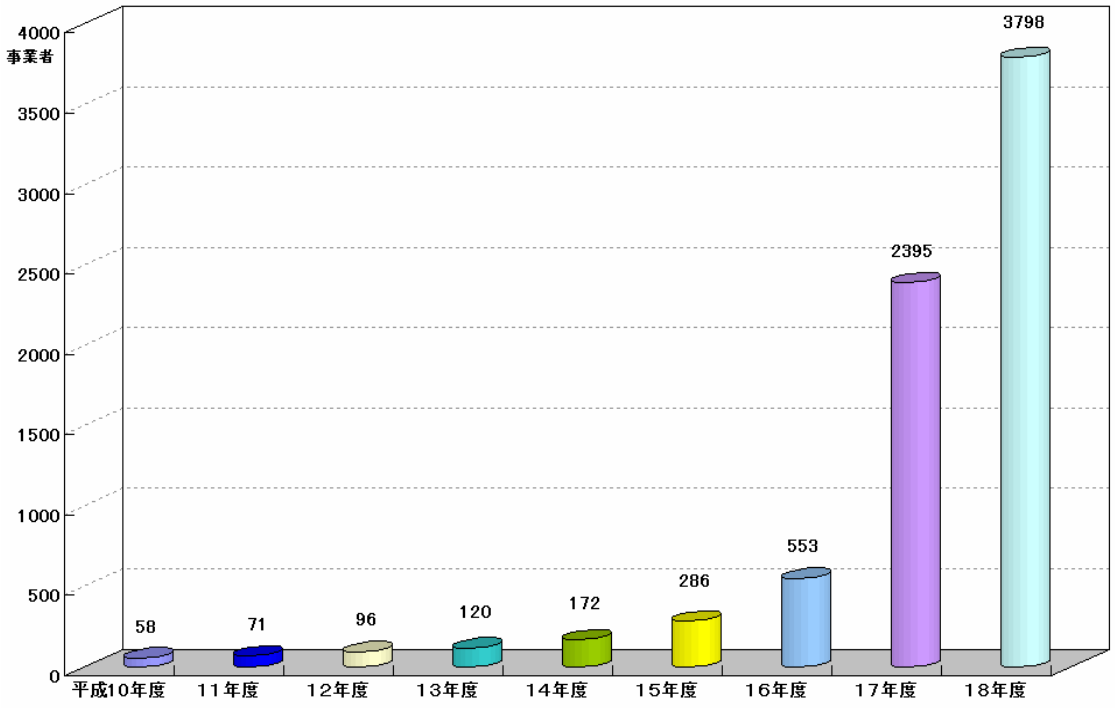
- 個人情報の取扱いにおける事故等の発生は、PMS の内容や、運用に問題があることが原因の一つと考えられる。PMS の点検（運用の確認、監査）機能が重要である。
- 監査においては、JIS 規格（JIS Q 15001）への適合状況及び、運用状況の監査がポイントとなる。
- 監査以外でも、日常業務において、PMS が適切に運用されているかを確認し、その結果を踏まえた注意喚起を行い、改善に結びつけることが重要である。

⑦ 個人情報保護体制の強化

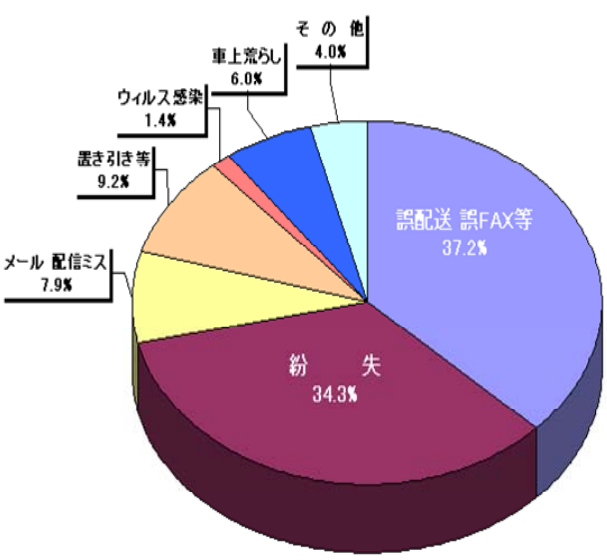
- PMS の運用において、個人情報保護体制の強化は必須である。
- 事故等が発生した場合の対応では、危機管理体制の整備、マニュアルの整備とそのマニュアルに即した迅速な行動をとることが出来る日常の訓練が重要である。

⑧ 確認行為の重要性の再認識について

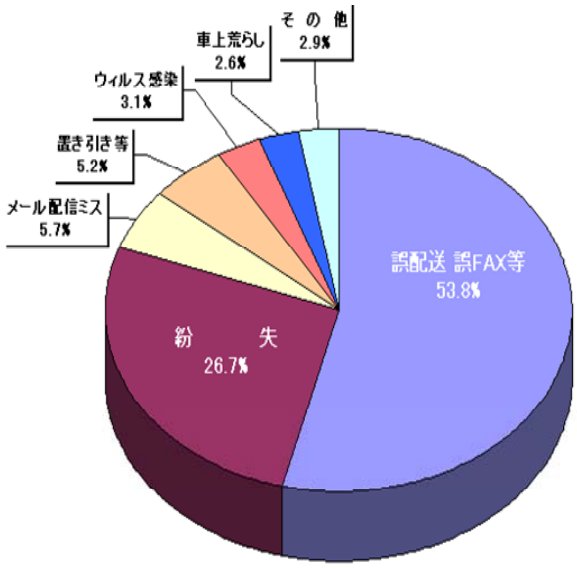
- 配送物の誤封入・誤送付、個人情報が記載された文書の FAX の誤送信、メール配信ミス等については、特に確認の行為が重要であることは認識されているが、実際には多くの事故が報告されている。「ついうっかり」「イレギュラー対応で…」「通常は行なっているが…」等、【確認ミス】の一言となるが、実際に事故が発生した場合の個人（本人）への影響を十分に認識し、ルールを厳守し慎重に業務を進めることが重要である。
- 初歩的な確認ミスが繰り返し発生する状況がある場合に、リスク認識・分析が適正に行なわれず、再発防止策が有効となっていない状況もあるので、再発防止のためには、人的な問題や PMS としての対応等、事業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。



＜図１　年度別プライバシーマーク認定事業者数（平成 10～18 年度）＞



（　平成 17 年度　）



（　平成 18 年度　）

＜ 図2　事故原因別割合 ＞