（平成 19 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 20 年 6 月 10 日

平成 19 年度中に当協会及び各指定機関（平成 19 年度末現在 15 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を報告する。また、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 19 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 913 社 1,489 件で、平成 18 年度の 439 社 708 件に比較して、報告事業者数、報告件数共に約 2 倍に増加している。

報告の内訳は、当協会への認定事業者からの報告が 718 社 1,250 件（前年 384 社 651 件）、指定機関への認定事業者からの報告が 195 社 239 件（同 55 社 57 件）である。事故報告の増加は、認定事業者数そのものの増加が主な要因と推測するが、指定機関の増加に伴い、各指定機関への報告も増加している。

なお、平成 19 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 17～19 年度）

認定機関	日本情報処理開発協会		指定機関			合計	
	事業者数	事故件数	機関数	事業者数	事故件数	事業者数	事故件数
19 年度	718 社	1,250 件	15	195 社	239 件	913 件	1,489 件
18 年度	384 社	651 件	11	55 社	57 件	439 社	708 件
17 年度	128 社	144 件	7	40 社	46 件	168 社	190 件

表２　年度別認定事業者数（平成 10～19 年度）

年度	10	11	12	13	14	15	16	17	18	19
認定数	58	71	96	120	172	286	553	2,395	3,798	2,259
累計	58	129	225	345	517	803	1,356	3,751	7,549	9,808

２．当協会に直接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 19 年度の 1 年間に、当協会で直接報告を受け付けた、事業者（プライバシーマーク認定事業者、審査中事業者、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、806 社より 1,829 件であった。うち認定事業者からの報告は前述のように 718 社 1,250 件で、審査中事業者は 72 社 339 件、申請検討中事業者は 16 社 240 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 1,829 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、704 件（38.5%）が発生している状況であり、前年度（44.3%）より委託先等における事故の割合は減少している。

しかしながら、この委託先等での事故のうち、郵便事業株式会社（旧日本郵政公社）および宅配便事業者等への配送業務の委託については、紛失・誤配達等の事故は相変わらず多く発生している。これらに関しては、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、委託元の事業者に対して【処分なし】の措置を行っている。

表３　事業者区分別事故報告件数（平成 19 年度）

事業者区分	報告事業者数	報告件数	（内、委託先等）
認　定	718	1,250	306
審査中	72	339	250
申請検討中	16	240	148
合　計	806	1,829	704(38.5%)

(*)　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 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
審査中	146	439	224
申請検討中	49	186	110
合　計	579	1,276	565(44.3%)

(*)　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 1,829 件のうち、紛失・漏えいが 1,774 件で、全体の 97.0%を占めている。紛失・漏えいを原因別に分類すると、書簡等郵送物の誤配達や FAX 送信ミス,メールの誤送信による『誤配達』が 990 件と最も多く全体の 54.1%を占めている。次いで『紛失』430 件（全体の 23.5%）、誤交付、データ管理ミス等による『その他漏えい』が 151 件（同 8.3%）である。

また、郵送物の封入ミスによる『誤送付』は、94 件（同 5.1%）、空巣・置き引き、車上荒らし等による『盗難』は 70 件（同 3.9%）、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 2.1%）である。

事故の原因について平成 18 年度と比較すると、書簡等郵送物と FAX の誤配達による情報の漏えいが大幅に増加している（36.7%→48.5%）。一方、『紛失』による漏えいと封入ミスによる『誤送付』については前年度より減少している。

なお、漏えい・紛失以外の事故「その他」55 件（全体の 3.0%）の内訳は、個人情報の目的外利用・提供、不正取得、データの破壊･改ざん等に関係するものであり、具体的に社内の内部犯罪・不正行為として報告があった内容も多くなっている。

表５　事業者区分別・事故原因別件数（平成 19 年度）　（単位：件数）

事業者区分	漏えい								漏えい計	紛失	漏えい＋紛失計	その他	合計
	誤配達			誤送付	盗　難		ｳｨﾙｽ感染	その他漏えい					
	書簡等	FAX	メール	封入ﾐｽ	車上荒らし	置き引き等							
認定	345	225	89	88	24	34	33	117	955	256	1211	39	1250
審査中	187	13	10	6	2	5	4	11	238	94	332	7	339
申請検討中	105	13	3	0	1	4	2	23	151	80	231	9	240
合計	637	251	102	94	27	43	39	151	1344	430	1774	55	1829
（割合　%）	34.8%	13.7%	5.6%	5.1%	1.5%	2.4%	2.1%	8.3%	73.5	23.5%	97.0%	3.0%	100.0%

表６　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	漏えい								漏えい計	紛失	漏えい＋紛失計	その他	合計
	誤配達			誤送付	盗　難		ｳｨﾙｽ感染	その他漏えい					
	書簡等	FAX	メール	封入ﾐｽ	車上荒らし	置き引き等							
認定	185	34	42	86	17	36	28	58	486	145	631	20	651
審査中	113	38	23	19	12	23	7	25	260	167	427	12	439
申請検討中	90	9	8	7	4	8	4	22	152	29	181	5	186
合計	388	81	73	112	33	67	39	105	898	341	1239	37	1276
（割合　%）	30.4%	6.3%	5.7%	8.8%	2.6%	5.3%	3.1%	8.2%	70.4	26.7%	97.1%	2.9%	100.0%

３.各指定機関に報告があった事故報告について

各指定機関に報告があった認定事業者からの報告は 195 社 239 件であり、『紛失』が 91 件と最も多く（全体の 38.1%）、次いで書簡等郵送物の誤配達や FAX 送信ミス、メールの誤送信による『誤配達』が 64 件と多い（同 26.8%）。また、ファイル交換ソフトのウィルス感染による漏えいも目立っている（同 9.6%）。

４．問題点・注意点

4.1 事故内容に関する注意事項

① 誤操作等による事故について

- 宛名記載ミスや誤封入による郵送物の誤送付、メールや FAX の操作ミスによる誤送信、個人情報記載書類を渡す相手を間違える等の誤交付や誤返却等の事故は、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。
- 事故報告書により「ダブルチェックを行う」等の再発防止策が講じられていることを確認するが、実際には同種事故が発生している状況もある。事故発生の事実を事業者内で情報共有し、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させたうえで慎重に業務を進めることの教育が重要である。

② メールの誤送信について

- メールアドレスの漏えいや、メール添付文書の間違い（添付ミス）等、メール配信に伴う事故も多い。
- 本来 BCC で送信すべきところ TO や CC で送信する等のミスにより、メールアドレスが漏えいした場合等においては、BCC 以外では送れない等システム的に（メールソフトでの対応）対応が可能であるが、添付ミスの場合には一度に多くの個人情報が漏えいすることが少なくない。添付ミスにおいては、確認以外に対処方法は考えられないが、確認行為が実際に確実に行なわれているかを検証することが重要である。ルールとして規定した場合でもそれが実際に実行されているかの確認が必要と考える。なお、添付ファイルについては、パスワードや暗号化等の安全対策措置が重要である。

③ 盗難等の事故について

- 車上荒らしや置き引き、空巣、引ったくり等の盗難による個人情報漏えいの事故は、不可抗力的な場合もあるものの、個人情報を取扱う担当者の認識の問題によるところも大きい。
- 結果的に個人情報の漏えいに繋がる場合に、担当者の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見受けられる。
- 個人情報を社外に持ち出すことに対し、持ち出すことの必要性の確認、持ち出す場合にはそのリスクを十分に認識した上での対応策（持ち出す媒体毎の注意点等）をルール化し、従業者にルールの徹底を図る等の教育を継続的に行い、意識付けを行うことが必要である。

④ ファイル交換ソフト：「Winny」「Share」等への対策

- 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の問題は、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・徹底された状況と考えられ、報告全体に占める割合は、前年度に比べ減少している状況であるが、報告件数は特に減少していない。
- 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。
- また、ファイル交換ソフトについては全社的な一斉点検、定期的な点検を行うこと、さらに、無許可のソフトをインストールすることが出来ない等の技術的措置を講じる等対応を行なうことが必要である。

⑤ 紛失事故について

- 社外での置忘れや、社内での所在不明による個人情報の漏えいの事故は、媒体としてノート PC、携帯電話、個人情報が記載された USB メモリー等の可搬記録媒体、個人情報記載書類の報告が多い。
- 担当者の意識の問題も重要であるが、ノート PC や USB メモリー等の可搬記録媒体を紛失した際には、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）が特に重要である。
- また、携帯電話の紛失事故も多く報告があるが、「紛失防止措置（落下防止等）」「セキュリティ措置（ロック等）」「個人情報保存（アドレス帳や受発信記録等）」の点に関して、社内ルールを見直し、教育を徹底する必要があると思われる。

⑥ システムの不具合等による漏えいについて

- 事故の原因として、「システムの不具合」「システム障害」との報告が多い。実際にシステムのバグ以外は、システムを運用する人間のミス（ヒューマンエラー）によるものがほとんどである。
- 事業者において、ヒューマンエラーの認識が薄く、システムそのものの問題と認識した場合に、システムに対する再発防止策が適正であっても問題が残り、事故の再発につながることも考えられることから、事故の原因究明に当たっては、ヒューマンエラーを認識することも必要である。
- 「WEB からの入力を行わせているサイトにおいて、アクセス時に他の人の情報が閲覧できる」との事故報告が目立つが、自社または委託先において WEB の構築を行なう場合には、事前に運用の確認を十分行なうことが重要である。また、システム障害等が発生した場合には、回復状態を十分に確認して運用を再開する等の確認の重要性を認識することが必要である。
- 最近は携帯サイトにおけるサービスも増えたが、安易にサイトが構築されたり、事前テストが不十分なままにサービスが開始されたりすることによる、事故発生が推測されるため、携帯サイトにおいても、個人情報の取扱いを十分に認識したサイトの構築、確認・チェックが重要である。

⑦ セキュリティ情報の確認と対応について

- 平成 19 年度の事故報告において、不正アクセスによる個人情報漏えいの報告が複数件あり、原因が SQL インジェクションの問題と判明した事例がある。この SQL インジェクションの問題については、経済産業省より平成 18 年 2 月 20 日に「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」として情報が発信され、当プライバシーマーク事務局においてもホームページに情報を公表した経緯がある。
- 事業者（特にシステム担当者）は、独立行政法人情報処理推進機構（IPA）や、JPCERT コーディネーションセンター」（JPCERT/CC）等が発信するセキュリティ関連情報を常に収集し、自社システムの対応状況の確認を行うとともに、委託先に対しても情報提供や対策の確認を行ない、事故の未然防止に努めることが重要である。

4.2 全般的な注意事項

① 再発防止策の実効性確認について

- 事故報告書においては、再発防止策についても報告を求めているが、実際に決定した防止策の実効性確認と検証が重要であり、その結果、改善が必要の場合には、単に現場レベルではなく、事業者の代表者の責任において速やかに対処することが必要な事項である。
- 事故対応においても、事故の真の原因究明、対応策の策定と実施、更にはその結果をチェックすることで効果の確認を行なうという PDCA のサイクルの重要性を事業者は認識すべきである

② 従業者教育

- JIS Q 15001：2006 の 3.4.5「教育」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。教育を完璧に実施することは難しいが、アンケートや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、定期的に評価を行った上で必要な見直しを行うこと、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「従業者の監督」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、従業者の監督を行なうことも重要である。

③ 内部犯罪・内部不正行為への対策

- 従業者の個人情報へのアクセス権の有無にかかわらず、従業者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。

④ 外部委託先等の管理

- JIS Q 15001：2006 の 3.4.3.4「委託先の監督」において、委託する個人情報の安全管理が図られるよう、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。従って、委託元は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。

⑤ 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。

⑥ 個人情報保護体制の強化

- プライバシーマーク認定事業者においては、個人情報保護体制の中で、事業者の代表者・個人情報保護管理者・監査責任者・教育責任者・相談窓口責任者等については、その役割、責任及び権限が規定され、個人情報保護マネジメントシステム（PMS）の運用が行われているが、PMS が実際に事業者内で適正に機能するために、個人情報保護の体制強化は必須である。
- 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。

【参考資料】

1. 財団法人日本情報処理開発協会：
   (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」(平成 19 年 6 月)
   (平成 17 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」(平成 18 年 7 月)

2. 経済産業省：
   個人情報の安全管理措置徹底に関する会員企業への周知について(依頼)（平成 19 年 7 月）

以上