（平成 28 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 29 年 8 月 28 日

平成 28 年度中に当協会(JIPDEC)及び審査機関（平成 28 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 28 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を示している。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 28 年度の報告件数

① 843 付与事業者より 2,044 件の事故報告があり、前年度の 796 付与事業者 1,947 件より、事業者数、事故報告件数共に増加した。
② 平成 28 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%であった。

報告内容の概要

① 事故の原因は、「メール誤送信」（20.7%）が最も多く、次いで「紛失」「宛名間違い等」の順に割合が多い。前年度に比べ、「メール誤送信」「紛失」「宛名間違い等」のいずれも割合は減少した。
② 事故の原因の「その他漏えい」は、前年度に比べ割合が大幅に増加（6.9%⇒13.8%）し、特に、『プログラム/システム設計・作業ミス』による漏えい、『不正アクセス・不正ログイン』による漏えいの報告件数が 2 倍強に増加している。
③ 盗難・紛失の媒体については、書類、スマホを含む携帯電話、ノートPC・モバイル端末の順に件数・割合共に多く、この傾向は平成 25 年度から変化はない。平成 28 年度については、前年度に比べ書類の割合が若干増加し、スマホを含む携帯電話がやや減少している。

1. 事故報告(*)のあった付与事業者数と事故報告件数(平成 24～28 年度)

年　度	24 年度	25 年度	26 年度	27 年度	28 年度
付与事業者数	620	736	768	796	843
事故報告件数	1,447	1,627	1,646	1,947	2,044

(*) 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 24～28 年度の各年度末時点)

年　度	24 年度	25 年度	26 年度	27 年度	28 年度
付与事業者数	13,075	13,591	14,044	14,755	15,297

＜コメント＞

843 付与事業者より 2,044 件の事故報告があり、前年度の 796 付与事業者 1,947 件より、事業者数、事故報告件数共に増加した。
これは付与事業者数が増加したことに加え、より個人情報の取扱いに係る事故の報告の意義を理解し真摯に対応している事業者が増えてきていることが背景にあるものと考えられる。

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 26～28 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
平成28年度	報告件数	303	0	274	136	424	4	281	9	37	409	167	2,044
	割合(%)	14.8	0.0	13.4	6.7	20.7	0.2	13.8	0.4	1.8	20.0	8.2	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、配送を業とする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・作業ミス』『不正アクセス・不正ログイン』による漏えい、『口頭での漏えい』及び『◆その他（事務処理・作業ミス等）』のヒューマンエラーと考えられるもの等が含まれる。

平成 26～28 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
平成28年度	報告件数	89	8	57	27	100	281

・「その他漏えい」の『◆その他』には、付与事業者の関係者等が関与した漏えいも含まれる。

＜コメント＞

- 「その他漏えい」は、前年度に比べ割合が大幅に増加し、特に、『プログラム/システム設計・作業ミス』による漏えい、『不正アクセス・不正ログイン』による漏えいの報告件数が 2 倍強に増加している。
- 「◆その他」は、付与事業者の関係者等が関与した漏えいも含まれるが、事務処理・作業ミス等人為的なミスによる漏えい事故が大幅に増加したことが読み取れる。

※4 :「その他」の内容について

平成 26～28 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
平成28年度	報告件数	3	23	6	7	27	6	95	167

・「その他」の『★左記に分類できない内容』には、付与事業者より提出された事故報告書の内容が、「評価対象外」となった報告件数も含まれる。

３．事故に対する主な注意事項等

（1）IT （Information Technology） 関連の事故について

『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などを指し、事業におけるIT利用の増加・高度化に伴い、IT関連事故の件数の増加、内容の複雑化が見られる。

平成28年度の事故報告：「その他漏えい」の内訳においても、『IT関連事故』（『プログラム/システム設計・作業ミス』『不正アクセス・不正ログイン』による漏えい）は、前年度より大幅に増加している。

IT関連事故の特徴としては以下の 3 つのケースが挙げられ、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。

（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。

＜その1：システムプログラム上の問題による事故に関して＞

- システムプログラム上の問題による事故としては、「公開・表示設定間違い」「アクセス権設定間違い」「想定外の処理」等がある。「想定外の処理」等の場合に、例えば『ウェブサイトなどで、本来は公開対象ではない個人情報が公開された』『プログラムの不具合等により、想定したアクセス設定とは異なる設定となり、本来、該当の個人情報を閲覧できないはずの人が閲覧できてしまった』『設計・設定時には想定していなかったシステム上の処理が行われたことにより、個人情報が漏えいした』等が発生しており、人為的なミスが原因となっているケースが数多く見受けられる。

- 特に、システム導入時・システム移行時において、ひとりの担当者（責任者）に全てを任せきりにしてしまうことや、システム構築委託先に全てを任せきりにしてしまうこと等については、特に注意が必要である。

- システムプログラム上の問題による事故の防止策としては、設定不備のミス防止や操作ミス防止、検証・検収不備のミス防止等の具体的な防止策の他、体制の整備として次のような対策も重要なポイントである。

  （1）手順やルールの見直し
  　① 適切な業務運営ガバナンス体制の構築　　②作業実施ルール確認・見直し
  　③ チェックルール確認・見直し 等
  （2）具体的な手順等の工夫
  　① 二重チェック体制の構築
  　② 従来のやり方にとらわれない新たな手順の導入 等
  （3）注意喚起・教育
  　① 教育方法・実施時期・教育の目的・教育内容等の見直し
  　② 事故防止のルールの見直しと見直したルールの周知徹底
  　③ 人為的ミス防止のための定期的な教育の実施 等

（4）委託先の管理

① 定期的な運用モニタリングの実施等、チェック体制の確立及び、監査実施の徹底

② 人為的ミス防止のための委託先教育の実施　等

更に万が一、事故が発生した場合に備えての二次被害等防止策の策定も重要なポイントである。

＜その2：不正行為よるIT事故に関して＞

- IT事故における不正行為には、外部からのものと内部におけるものがあるが、それぞれに「悪意によるもの」「愉快犯的なもの」「自己利益を目的としたもの」などが存在する。いずれの場合も、事業者の信頼性を失ったり経済的損失を被ったりするリスクがあるのは同様であるため、個人情報保護の重要性を事業者全体で認識し、従業員や委託先への教育を徹底させることや、社内監視体制を強化するなど、不正防止に向けた取組みが肝要である。

- 「データ保管ミス」「アクセス制御ミス」「不正持出制御ミス」等が原因で、データの不正持出・不正使用の事故（例えば、『従業員が顧客のクレジットカード情報を持出し、不正使用した』等）が発生している。また、「システムの脆弱性等」「なりすまし」により、不正アクセス・不正ログインの事故（例えば『SQLインジェクション（コンピュータ操作言語SQLを悪用し、データベースを不正に操作する攻撃方法）による不正アクセス攻撃により、メールアドレスやID・パスワードが流出した』『第三者が「実在するID・パスワード」を利用して「なりすまし」により不正行為を行った等』が発生している。

- 特に、委託契約終了時（委託先の問題）や雇用契約終了時（退職者の問題）においては、IT事故における不正行為発生のリスクが高く、また、個人情報取扱権限が集中した場合及び個人情報が放置されている状況については、より注意が必要と考える。

- 不正行為によるIT事故については、次のような具体的な再発防止策が考えられる。

（1）データの不正持出・不正使用の場合

＊ 個人情報抽出用端末の制限

＊ 退職者対応

＊ 外部への接続制限

＊ データの管理

＊ その他（例えば、複数名による作業の徹底・不正アクセス検知モニタリングの強化等）

（2）不正アクセス・不正ログインの場合

＊ システムの脆弱性等の早期発見と対応

＊ なりすましを防止するシステムへの改善

なお、内部不正行為防止については、下記の情報も参考にして頂きたい。

独立行政法人　情報処理推進機構（**IPA**）：　https://www.ipa.go.jp/
情報セキュリティに関する情報収集・提供を行っている組織で、
ウェブサイトから多くの有用な情報を得ることができます。
★「組織における内部不正防止ガイドライン」
http://www.ipa.go.jp/security/fy24/reports/insider/

（2）対面・電話等における事故に関して

本人等と対面もしくは電話にて対応する場合、時間をかけて検討する間もなく即時の対応を迫られる等、その場のやりとりの状況によってはルール通りの対応が難しく思えるケースや、親切心が仇になり、思わぬトラブルを招く結果になってしまうケースが見られる。

平成 28 年度の事故報告:「その他漏えい」の内訳においても、『口頭による漏えい』は、前年度より増加している。

- 対面・電話等における事故としては、「第三者への漏えい」「職場内での漏えい」「家族などへの漏えい」「他企業への漏えい」「本人との思い込みによる別人への漏えい」「不審な問合せ者への漏えい」があり、例えば、『業務上保管している（顧客・会員・契約者等の）連絡先を本人の同意なしに第三者に伝えた』『会員Aに対して、同姓同名の会員Bの情報を伝えた』『（本人の）自宅に電話した際、本人不在であったために家族に要件を伝えてしまった』『従業員や退職者の勤務状況等を他社に伝えた』等の事故がある。

- 対面・電話等においては、以下のような場合に特に注意を要する。また、注意を要する対応には、復唱及びメモを取る際のミスや本人確認の際のミスも重複して発生することもあるので、慎重な対応が望まれる。

  ・相手の巧みな話術　　・家族を名乗る人物からの問合せ
  ・本人不在時の対応　　・第三者の脅し、泣き落とし
  ・権力者、権限のある人物の氏名提示　・同姓同名（契約者内、職場内）
  ・同一苗字、類似苗字　　・類似社名　等

- 再発防止策を策定し確実に実行するために、対応ルール・手順の確認・見直しを行うと共に、従業員への注意喚起・教育が重要なポイントと考える。また、対面・電話などにおける事故を起こさないためには、担当者ひとりひとりの「正しい認識」と「バランス感覚」が求められるが、それらを養うためには、具体的な事例をもとに「ロールプレイング」や「ディスカッション」を行うのも効果的かと考える。

- 対面・電話等における事故の直接の原因ではないが、個人情報の取扱いルール不整備、周知不徹底の問題も考えられるため、「個人情報取扱いに関するルール不整備・周知不徹底」「本人確認ルールの不整備・周知不徹底」「第三者提供に関するルールの不整備・周知不徹底」「本人以外への対応ルールの不整備・周知不徹底」についても注意が必要である。

（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、前年度に比べ件数は若干増加したものの割合は同一である（42 件：2.2%→46 件：2.2%）。内訳では、特に置き引き等の件数の増加が目立っている。

- 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。

- 紛失事故については、これまで事故報告の原因として報告件数・割合共に最も多い状況であったが、平成 28 年度は「メール誤送信」に次ぐ報告件数・割合となった。しかしながら全報告件数に占める割合は 20.0%と多く、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の実施等により、減少できる事故とも考えられる。

- 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 26～27 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、ノート PC,タブレット端末が多く報告されている。前年度に比べ書類の割合は若干増加しているが、あくまで割合の問題であって、書類、スマホを含む携帯電話ともに取扱いに細心の注意が必要であることは言うまでもない。

盗難・紛失の媒体別内訳（平成 26～28 年度）

媒体等		書類	携帯電話 スマホ	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26年度	報告件数 （464）	229	153	36	15	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	報告件数 （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
平成28年度	報告件数 （455）	239	151	45	10	0	45	0	490
	割合(%)	48.8	30.8	9.2	2.0	0	9.2	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、社員証　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≫

事故報告について

個人情報の取扱いにおける事故が発生した場合、緊急時対応として関係機関への報告を行うことになりますが、個人情報保護法等に基づく事故報告と、プライバシーマーク制度における事故報告には、『違い』があります。その『違い』をご確認のうえ、適切にご対応いただければと思います。

1．個人情報保護法等に基づく事故報告について

個人情報保護委員会のサイトに、関連の資料が公表されていますが、まず押さえておいていただきたいと考える資料をご紹介させていただきます。

＊個人データの漏えい等の事案が発生した場合等の対応について
（平成 29 年個人情報保護委員会告示第 1 号）
https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

＊「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ
https://www.ppc.go.jp/files/pdf/170530_faq_rouei.pdf

＊改正個人情報保護法に基づく権限の委任を行う業種等及び府省庁並びに当該業種等における漏えい等事案発生時の報告先【詳細版】
https://www.ppc.go.jp/files/pdf/170530_kengeninin_list_detail.pdf

＊事業者における特定個人情報の漏えい事案等が発生した場合の対応について
（平成 27 年特定個人情報保護委員会告示第２号）
https://www.ppc.go.jp/files/pdf/roueitaiou_jigyosha.pdf

＊特定個人情報の漏えい事案等が発生した場合の対応におけるＱ＆Ａ
https://www.ppc.go.jp/files/pdf/rouei_QA.pdf

2．プライバシーマーク制度における事故報告について

プライバシーマーク制度においては、個人情報の取扱いにおける事故が発生した場合の事故報告を義務付けていますが、その場合の「事故」の定義や、「事故報告」の対象は、個人情報保護法等に基づく事故報告よりも範囲が広くなっていますので、ご注意ください。
以下のサイトにおいて、義務付けの根拠や事故報告の目的などについてもご説明させていただいていますので、今一度、ご確認ください。

＊個人情報の取扱いに関する事故の報告について
https://privacymark.jp/privacy_mark/about/accident.html

＜参考＞
平成 17 年度～平成 27 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。