資料２

個人情報保護を巡る国内外の動向
（漏えい報告の在り方関係）

平成31年１月28日

漏えい報告に係る状況について

1．実績値

○平成29年度年間実績：計 **3,338件**

〈内訳〉
- ・個人情報保護委員会に直接報告されたもの： 694件
- ・権限委任省庁経由で報告されたもの： 1,142件
- ・認定個人情報保護団体経由で報告されたもの： 1,502件

○平成30年度上半期実績（４月～９月）：計 **2,191件**

〈内訳〉
- ・個人情報保護委員会に直接報告されたもの： 596件
- ・権限委任省庁経由で報告されたもの： 670件
- ・認定個人情報保護団体経由で報告されたもの： 925件

2．傾向の分析

大規模（漏えい人数が50,000人超）漏えい事案の動向

・平成29年度： **13件**
（0.4%。全体：3,338件）

・平成30年度上半期： **14件**
（0.6%。全体：2,191件）

発生原因の傾向等

〈発生原因〉
- 平成29年度、平成30年度上半期を通じて、発生原因は、書類及び電子メールの誤送付、書類及び電子媒体の紛失が**約８割**。
- なお、大規模漏えい事案の発生原因については、インターネットを経由した不正アクセスが**約７割**。

〈1件当たりの漏えい人数〉
- 漏えい事案1件当たりの漏えい人数については、100人以下である事案が**８割以上**。

漏えい報告に係る状況について

３．主要事例

① 漏えい規模の大きい事例への対応

- 個人情報保護法（以下「法」という。）第40条に基づく立入検査等を実施して安全管理措置等の状況を確認。併せて、再発防止策の実施や個人情報の適切な取扱いを行うように法第41条に基づく指導・助言を行った。

⇒指導内容の例：不正アクセスを発生原因とする漏えい事案について、再発防止策の実施等に関し、ウェブサイトのプログラム修正を行った場合には、リリース前に、当該ウェブサイトのセキュリティチェックを行う必要があることなどについて指導を行った。

② 外国事業者の事例への対応

- 外国事業者の漏えいにより、当該事業者のサービスを利用していた国内事業者の顧客の個人データが漏えいした事案について、当該外国事業者の日本法人を通じて、サービスを利用していた国内事業者のリストの提出を求め、当該国内事業者に漏えい等報告の提出を求めた。
- 外国事業者の漏えいであって、当該事業者の協力が得られなかった事案について、海外の個人情報保護当局との執行協力として、委員会の対応状況の情報提供、漏えい等事案の発生原因や再発防止策の情報の共有依頼を行った。
- 外国事業者の漏えいについて、母国語での漏えい報告が提出されたため、日本語での詳細な報告を別途求めた。

③ 当委員会が積極的に働きかけた事例

- 漏えい等事案の報道発表を端緒として事業者に連絡を行った結果、漏えい報告が提出された。
- ソーシャルモニタリングを端緒として事業者に連絡を行った結果、漏えい報告が提出された。

④ 漏えい報告を端緒として、当委員会による行政指導等につながった事例　等

- A社：ECサイトへの不正アクセスによる漏えい事案（報告徴収、指導）
- B社：ECサイトへの不正アクセスによる漏えい事案（立入検査、指導）

参考（事業者からの個人データの漏えい等事案の状況）

（平成29年度年次報告（期間：平成29年５月30日～平成30年３月31日）を参考に作成）

①「漏えい等した人数」

（単位：件）

報告先	件数（割合）	漏えい等した人数				
		500人以下	501～5,000人	5,001～50,000人	50,001人以上	不明
個人情報保護委員会	694	600 (86.5%)	60 (8.6%)	22 (3.2%)	7 (1.0%)	5 (0.7%)
包括委任先省庁	1,142	1,105 (96.7%)	22 (1.9%)	11 (1.0%)	3 (0.3%)	1 (0.1%)
認定団体	1,502	1,420 (94.6%)	44 (2.9%)	17 (1.1%)	3 (0.2%)	18 (1.2%)
計	3,338	3,125 (93.6%)	126 (3.8%)	50 (1.5%)	13 (0.4%)	24 (0.7%)

※ 漏えい等事案には、「漏えい」のほか、「滅失」、「き損」の事案を含む。
※ 漏えい等した人数とは、漏えい等した個人情報によって識別される特定の個人の数をいう。

②「漏えい等した情報の種類」

（①のうち委員会に報告されたもの。以下⑤まで同じ。）

（単位：件）

件数（割合）		漏えい等した情報の種類					
		顧客情報		従業員情報		その他の情報	
	うち基本情報のみ		うち基本情報のみ		うち基本情報のみ		うち基本情報のみ
694	49 (7.1%)	645 (92.9%)	46 (6.6%)	49 (7.1%)	3 (0.4%)	11 (1.6%)	0 (0.0%)

※ 「基本情報」とは、氏名、生年月日、性別、住所を指す。
※ 一つの事案で複数の情報が漏えい等した場合は、全ての項目について記入。

参考（事業者からの個人データの漏えい等事案の状況）

（平成29年度年次報告（期間：平成29年５月30日～平成30年３月31日）を参考に作成）

③「漏えい等した情報の形態」

（単位：件）

件数（割合）	漏えい等した情報の形態			
	電子媒体のみ	紙媒体のみ	電子・紙媒体	その他
694	261 (37.6%)	417 (60.1%)	5 (0.7%)	11 (1.6%)

④「漏えい等元・漏えい等した者」

（単位：件）

件数（割合）	事業者					委託先				
	従業者		第三者		その他	従業者		第三者		その他
	意図的	不注意	意図的	不注意		意図的	不注意	意図的	不注意	
694	3 (0.4%)	367 (52.9%)	72 (10.4%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	236 (34.0%)	15 (2.2%)	0 (0.0%)	1 (0.1%)

⑤「漏えい等した後の改善措置状況」

（単位：件）

件数（割合）	事業者による安全管理措置			
	組織的	人的	物理的	技術的
694	239 (34.4%)	496 (71.5%)	43 (6.2%)	156 (22.5%)

件数（割合）	事業者による本人への対応		
	本人への謝罪・連絡	専用窓口の設置	商品券等の配付
694	638 (91.9%)	81 (11.7%)	13 (1.9%)

※　一つの事案で複数の安全管理措置、または対応を事業者が実施した場合は、全ての項目について記入。このため、各項目の割合の合計は100%にはならない。

※　表中の事業者による安全管理措置は、漏えい等後に事業者が講じた再発防止策を、「個人情報の保護に関する法律についてのガイドライン（通則編）」の「（別添）講ずべき安全管理措置の内容」に基づき、その再発防止策の内容に応じて分類している。

具体的な内容としては、「組織的」に社内規程の整備や監査の実施等を、「人的」に教育・研修の実施等を、「物理的」に機器及び電子媒体の盗難の防止や持ち運ぶ場合の漏えい防止等を、「技術的」にアクセス制御や外部からの不正アクセスの防止等を、それぞれ分類している。

漏えい報告に係る主要な国の制度（暫定版）

	日本	米国	
		カリフォルニア州法	ニューヨーク州法
制度の有無	あり	あり	あり
制度の根拠	• 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（以下「告示」））	• データ侵害通知法（カリフォルニア州民法）Section 1798.82	• データセキュリティ侵害通知法（一般事業法第899AA条）
漏えい報告に係る義務の位置づけ	努力義務（告示２（５）及び３）	義務（1798.82. (a)）	義務（第2項）
漏えい報告の対象となる事案	• 個人情報取扱事業者が保有する個人データ等の漏えい、滅失またはき損及びその恐れ（告示１）	• 暗号化されていない個人データの流出あるいは、暗号化されているが暗号と共に流出した場合（1798.82. (a)）	• 暗号化されていない個人データの流出あるいは、暗号化されているが暗号と共に流出した場合（第1項(a)）
漏えい報告を行うべき相手方	• 影響を受ける可能性のある個人情報の本人（告示２（５）） • 個人情報保護委員会（告示３）	• 本人（カリフォルニア州在住者のみ） ⇒このほか、公表義務が存在（1798.82. (b)） • 500名以上に通知を行う場合、司法長官へ通知書提出が必要（1798.82. (f)）	• 本人（NY州在住者のみ）（第2項） • 州司法長官、州務局及び警察（第8項(a)） • 5000名を超える場合には消費者報告機関への通知も必要（第8項(b)）
漏えい報告を行うべき期限	• 対本人：「速やかに本人へ連絡し、又は本人が容易に知り得る状態に置く」ことが「望ましい」（告示２（５）） • 対個人情報保護委員会：「速やかに報告するよう努める」（告示３）	• 漏えいの発見後、速やかに通知すべき（1798.82. (a)）	• 漏洩の発見後速やかに通知すべき事を規定（第2項、第3項）
漏えい報告に係る軽減措置の概要	• 実質的に個人データ等が外部に漏えいしていないと判断される場合（高度な暗号化が施されている等） • FAXの誤送信等のうち軽微なものについては、個人情報保護委員会への報告を要しない（告示（２））	• 漏えい報告の対象となる情報を、氏名と個人番号等（社会保障番号等）の組み合わせ等に限定（1798.82. (h)） • 暗号化が施され、暗号鍵が同時に漏洩していない場合は通知義務から除外される。（第1項(a)）	• 暗号化が施され、暗号鍵が同時に漏洩していない場合は通知義務から除外される。（第1項(a)）
義務の懈怠に係る罰則	なし	• 顧客は、民事訴訟で損害賠償請求を提起することができる（1798.84(b)）	• 州司法長官は州民を代表して違反者に対して裁判所に損害賠償請求を提起できる（第6項）
漏えい報告の実績値	• 平成29年度：3,338件 • 平成30年度（上半期）：2,191件	• 2015年：178件	• 2017年：1,583件

（※１） 米国では、包括的な個人情報保護法は連邦レベルでは存在せず、分野ごとに個別法で措置されている。

漏えい報告に係る主要な国の制度（暫定版）

	EU	中国
制度の有無	あり	あり
制度の根拠	・GDPR第33条、第34条	・サイバーセキュリティ法（※２）第42条
漏えい報告に係る義務の位置づけ	義務（第33条、第34条）	義務（第42条）
漏えい報告の対象となる事案	• 個人データ侵害が発生した場合（第33条第１項、第34条第１項）	• 個人情報の漏洩、破損、紛失が発生した又は発生する恐れ（第42条）
漏えい報告を行うべき相手方	• 個人データ侵害によって権利及び自由に対する高いリスクが発生する可能性があるデータ主体（第34条第１項） • EU各国の監督機関（第33条第１項）	• 使用者 • 監督機関（第8条） ⇒法令上用語の明確な定義はされていない。
漏えい報告を行うべき期限	• 対データ主体：高いリスクを伴う個人データ侵害を認識した場合速やかに（第34条第１項） • 対当局：可能な場合には、個人データ侵害を認識した時から72時間以内。72時間を過ぎた場合はその理由を添付（第33条第１項）	• 個人情報の漏洩、破損、紛失が発生した又は発生する恐れのある場合は、直ちに救済措置を講じ、規定に従い遅滞なく使用者への告知および監督機関への報告が義務付けられている（第42条）
漏えい報告に係る軽減措置の概要	• 対データ主体：個人の権利及び自由に対する高度なリスクを発生させる恐れがない侵害 • 対EU各国の監督機関：個人の権利及び自由に対するリスクを発生させる恐れがない侵害については、報告は不要（第33条第１項、第34条第１項）	なし
義務の懈怠に係る罰則	• 報告を怠った場合には第83条に基づき何らかの制裁が適用される可能性がある（個人データ侵害通知に関するガイドライン序文）	• 関係所管機関が是正命令を行い、情状に基づき警告、違法所得の没収又は相当額以上10倍以下の制裁金を単科あるいは併科できる（第64条）
漏えい報告の実績値	• 英国：6,000以上 • ドイツ：1,000未満 ※GDPR施行後、昨年9月時点まで。ただし、英国は旧データ保護法に基づくレポートも含まれ、ドイツは報告のあった5州のみの結果。	－ （調査した限り不明）

（※２）　中国では、包括的な個人情報保護法は存在しないが、サイバーセキュリティ法においてサイバーセキュリティに関連する個人情報保護の規定を設けている。