資料3

個人情報保護法　いわゆる３年ごと見直し規定に基づく検討
（実効性のある監視･監督の在り方②）

令和６年５月15日
個人情報保護委員会事務局

※　本資料における外国法令等の日本語訳は仮訳である。

漏えい等報告及び本人通知の在り方①

1．漏えい等報告及び本人通知に係る現行の規律

漏えい等報告に係る現行の規律

- 漏えい等報告は、規則第7条各号に該当する事態について、速報及び確報に分けて行うこととされている。
- 漏えい等報告の**趣旨は、委員会が事態を早急に把握し、必要な措置を講ずることができるようにすること**にある。
- 委員会は、漏えい等報告を受けた内容を踏まえ、関係する法令やガイドラインの説明を行いつつ、報告事項の記載について不明点等を確認し、個人情報取扱事業者に対し、本人通知を履行させ、再発防止に向けた安全管理措置義務に係る指導等を行っている。特に、速報を受領した段階においては、事案の規模や概要を把握して、事案の軽重を踏まえて今後の調査方針や権限行使の方向性について検討し、また、必要に応じて漏えい等事態が発生して間もない段階で個人情報取扱事業者として対応すべきことを助言し、個人情報取扱事業者における調査の一般的な手法やセキュリティに関する情報提供等を実施している。さらに、不正アクセス事案の場合、個人情報取扱事業者に対し、警察など関係機関への連絡を行うこと等も助言している。

○ 個人情報保護法（抜粋）

第二十六条（漏えい等の報告等）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。

○ 個人情報保護法施行規則（抜粋）

第七条（個人の権利利益を害するおそれが大きいもの）

法第二十六条第一項本文の個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

一　要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第一項において同じ。）の漏えい、滅失若しくは毀損（以下この条及び次条第一項において「漏えい等」という。）が発生し、又は発生したおそれがある事態

二　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

三　不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）の漏えい等が発生し、又は発生したおそれがある事態

四　個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

第八条（個人情報保護委員会への報告）

個人情報取扱事業者は、法第二十六条第一項本文の規定による報告をする場合には、前条各号に定める事態を知った後、速やかに、当該事態に関する次に掲げる事項（報告をしようとする時点において把握しているものに限る。次条において同じ。）を報告しなければならない。

○ 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）（抜粋）

３－５－３－１（※２）

報告対象事態における「おそれ」については、その時点で判明している事実関係に基づいて個別の事案ごとに蓋然性を考慮して判断することになる。漏えい等が発生したおそれについては、その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合がこれに該当する。

漏えい等報告及び本人通知の在り方②

１．漏えい等報告及び本人通知に係る現行の規律

本人通知に係る現行の規律

- 委員会への報告を要する事態が生じた場合には、本人への通知も行う必要がある。
- 本人への通知の**趣旨は、通知を受けた本人が漏えい等の事態を認識することで、その権利利益を保護するための措置を講じられるようにすること**にある。
- 本人通知は原則として本人に直接知らせる必要があるが、「本人への通知が困難な場合」には事案の公表を含む代替措置をとることが可能。

○　個人情報保護法（抜粋）

第二十六条（漏えい等の報告等）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

２　前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

○　個人情報保護法施行規則（抜粋）

第十条（本人に対する通知）

個人情報取扱事業者は、法第二十六条第二項本文の規定による通知をする場合には、第七条各号に定める事態を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、第八条第一項第一号、第二号、第四号、第五号及び第九号に定める事項を通知しなければならない。

○　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）　（抜粋）

３－５－４－２

「当該事態の状況に応じて速やかに」とは、速やかに通知を行うことを求めるものであるが、具体的に通知を行う時点は、個別の事案において、その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断する。

３－５－４－４

「本人への通知」とは、本人に直接知らしめることをいい、事業の性質及び個人データの取扱状況に応じ、通知すべき内容が本人に認識される合理的かつ適切な方法によらなければならない･･･。

漏えい等報告及び本人通知の在り方③

1．漏えい等報告及び本人通知に係る現行の規律

漏えい等報告及び本人通知の報告対象・通知対象

- 委員会への漏えい等報告については、①概要、②漏えい等が発生し、又は発生したおそれがある個人データの項目（規則第７条第３号に定める事態については、同号に規定する個人情報を含む。以下同じ。）、③漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数、④原因、⑤二次被害又はそのおそれの有無及びその内容、⑥本人への対応の実施状況、⑦公表の実施状況、⑧再発防止のための措置、⑨その他参考となる事項を報告する必要がある。
- ただし、**速報時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる**。
- 本人へ通知すべき事項は、上記漏えい等報告における報告事項のうち、①概要、②漏えい等が発生し、又は発生したおそれがある個人データの項目、④原因、⑤二次被害又はそのおそれの有無及びその内容、⑨その他参考となる事項に限られる。

○ 個人情報保護法施行規則（抜粋）

第八条（個人情報保護委員会への報告）

個人情報取扱事業者は、法第二十六条第一項本文の規定による報告をする場合には、前条各号に定める事態を知った後、速やかに、当該事態に関する次に掲げる事項（報告をしようとする時点において把握しているものに限る。次条において同じ。）を報告しなければならない。

一　概要
二　漏えい等が発生し、又は発生したおそれがある個人データ（前条第三号に定める事態については、同号に規定する個人情報を含む。次号において同じ。）の項目
三　漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
四　原因
五　二次被害又はそのおそれの有無及びその内容
六　本人への対応の実施状況
七　公表の実施状況
八　再発防止のための措置
九　その他参考となる事項

２　前項の場合において、個人情報取扱事業者は、当該事態を知った日から三十日以内（当該事態が前条第三号に定めるものである場合にあっては、六十日以内）に、当該事態に関する前項各号に定める事項を報告しなければならない。

第十条（本人に対する通知）

個人情報取扱事業者は、法第二十六条第二項本文の規定による通知をする場合には、第七条各号に定める事態を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、第八条第一項第一号、第二号、第四号、第五号及び第九号に定める事項を通知しなければならない。

○ 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）（抜粋）

３－５－３－３

「速やか」の日数の目安については、個別の事案によるものの、個人情報取扱事業者が当該事態を知った時点から概ね３～５日以内である。

漏えい等報告及び本人通知の在り方④

1．漏えい等報告及び本人通知に係る現行の規律

「漏えい」と第三者提供の関係

- 個人情報保護法施行規則で定める事態が生じたときは、委員会に対する報告及び本人通知を行う必要がある。

- 他方、**現行法上、「個人データ」が違法に第三者に提供された場合、委員会に対する報告及び本人通知を行う義務は存在しない**。

○ 個人情報保護法（抜粋）

第二十六条（漏えい等の報告等）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

第二十七条（第三者提供の制限）

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

○ 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） （抜粋）

２－17

「提供」とは…個人データ等…を、自己以外の者が利用可能な状態に置くことをいう。個人データ等が、物理的に提供されていない場合であっても、ネットワーク等を利用することにより、個人データ等を利用できる状態にあれば（利用する権限が与えられていれば）、「提供」に当たる。

３－５－１－２

個人データの「漏えい」とは、個人データが外部に流出することをいう。（略）

また、個人情報取扱事業者が自らの意図に基づき個人データを第三者に提供する場合（※）は、漏えいに該当しない。

（※）個人情報取扱事業者は、個人データの第三者への提供に当たり、原則としてあらかじめ本人の同意を取得する必要がある。

漏えい等報告及び本人通知の在り方⑤

2．個人情報取扱事業者等における漏えい等報告の現状ー漏えい等報告の件数の推移

- 令和２年改正法の施行により、令和４年度から漏えい等報告が義務化されたこともあり、漏えい等報告の件数は増加している。同一の事業者において繰り返し漏えい等が発生している事例も存在する。

令和元年度	令和２年度	令和３年度	令和４年度
4,520件 （内訳） 委員会直接受付分： 1,066件 （うち域外適用分：13件） 委任先省庁経由分： 1,519 件 認定団体経由分： 1,935 件	4,141件 （内訳） 委員会直接受付分： 1,027件 （うち域外適用分：８件） 委任先省庁経由分： 1,122件 認定団体経由分： 1,992件	5,846件 （内訳） 委員会直接受付分： 1,042件 （うち域外適用分：５件） 委任先省庁経由分： 2,386件 認定団体経由分： 2,418件	7,685件 （内訳） 委員会直接受付分： 4,217件 （うち域外適用分：８件） 委任先省庁経由分： 3,468件 （注）

（注）令和２年改正法が令和４年４月１日に施行されたことに伴い、認定団体を経由した漏えい等事案の報告制度は廃止された。

漏えい等報告及び本人通知の在り方⑥

2．個人情報取扱事業者等における漏えい等報告の現状ー漏えい等した人数

- 漏えい等した人数は多くの事案において1,000人以下であるものの、50,000人超という非常に大規模な個人の権利利益の侵害に繋がるケースも存在する。

（令和４年度）

件数（割合）	漏えい等した人数（注）				
	1,000人以下	1,001～10,000人	10,001～50,000人	50,001人以上	不明
7,685件（100%）	7,206件（93.8%）	245件（3.2%）	56件（0.7%）	42件（0.5%）	136件（1.8%）

（注）「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本人の数であり、人数が確定できない場合は、漏えい等した可能性のある本人を含む最大人数として報告を受けている。

- 漏えい等した人数が1,000人以下の事案が全体の93.8%（7,206件）を占めており、中でも、漏えい等した人数が１人の事案が全体の80.4%（6,175件）を占めている。また、漏えい等した人数が２～10人、11～100人及び101～1,000人の事案が、それぞれ、全体の8.2%（631件）、2.9%（220件）及び2.3%（180件）を占めている。

- 漏えい等した人数が１人の事案としては、病院や薬局における要配慮個人情報を含む書類の誤交付及び紛失や、クレジットカードの誤送付などが多い。

漏えい等報告及び本人通知の在り方⑦

2．漏えい等報告の現状ー漏えい等の原因及び報告義務該当事由

- 漏えい等の原因は、誤交付、誤送付等のいわゆるヒューマンエラーによる事案が多いものの、不正アクセスによるものも一定程度存在する。不正アクセスを原因とする事案の中には、100万人を超える個人データの漏えいのおそれが生じたものもあった。

（令和４年度）

件数（割合）	原因			
4,217件 （100%） （注）	誤交付	誤送付	誤廃棄	紛失
	2,485件 （58.9%）	801件 （19.0%）	34件 （0.8%）	207件 （4.9%）
	盗難	内部不正	不正アクセス	その他
	42件 （1.0%）	17件 （0.4%）	366件 （8.7%）	265件 （6.3%）

（注）令和４年度の漏えい等事案に関する報告（総数7,685件）のうち、直接委員会に報告されたもの（委員会直接受付分）の件数である。

- 報告義務該当事由の件数及び割合は以下のとおり。

（令和４年度）

件数（割合）	報告義務該当事由			
4,217件 （100%） （注１、２）	要配慮個人情報を含む	財産的被害が生じるおそれ	不正の目的をもって行われたおそれ	本人数1,000人超
	3,584件 （85.0%）	56件 （1.3%）	469件 （11.1%）	271件 （6.4%）

（注１）令和４年度の漏えい等事案に関する報告（総数7,685件）のうち、直接委員会に報告されたもの（委員会直接受付分）の件数である。
（注２） １つの事案で複数の報告義務要件に該当する場合には全て計上しているため、「報告義務該当事由」欄の件数は合計件数を超えることがある。同様に、「報告義務該当事由」欄の割合合計が 100%を超えることがある。

漏えい等報告及び本人通知の在り方⑧

３．EUにおけるデータ侵害通知についてー通知の件数

- GDPRは、個人データ侵害（personal data breach）が発生した場合に、原則として、各加盟国のデータ保護当局に対して通知を行うことを義務付けている。
- また、GDPRは、個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、そのデータ主体に対し、不当な遅滞なく、通知することを義務付けている。
- 各加盟国のデータ保護当局が2022年に受領した通知の件数は、例えば、以下のとおりである。
（参考： 2022年度）日本　個人情報取扱事業者等：7,685件　行政機関等：114件

国名	ドイツ（※1）	フランス（※2）	アイルランド（※３）	イタリア（※４）	英国（※５、６）
件数	10,614件	4,088件	5,828件	1,351件	9,146件

（※1） BfDI, Activity Report 2022（https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Taetigkeitsberichte/31TB_22.pdf?__blob=publicationFile&v=6）
（※2） CNIL, Rapport annuel 2022（https://www.cnil.fr/sites/cnil/files/2023-05/cnil_-_43e_rapport_annuel_-_2022.pdf）
（※3） DPC, Annual Report 2022（https://www.dataprotection.ie/sites/default/files/uploads/2023-03/DPC%20AR%20English_web.pdf）
（※4） GARANTE, RELAZIONE ANNUALE 2022（https://www.garanteprivacy.it/documents/10160/0/Relazione+2022+del+Garante+per+la+protezione+dei+dati+personali.pdf/125d413d-9ec3-ea46-8e01-643d585a8425?version=1.0）
（※5） 英国については、UK GDPRに基づき、2022年4月から2023年3月までの期間に行われた通知の件数。
（※6） ICO, Annual report 2022-2023（https://ico.org.uk/media/about-the-ico/documents/4025864/annual-report-2022-23.pdf）

漏えい等報告及び本人通知の在り方⑨

3．EUにおけるデータ侵害通知についてーGDPRにおけるデータ侵害通知の要件

GDPRの規律内容（抜粋）

第4条（定義）

（12） 「個人データ侵害」とは、偶発的又は違法な、破壊、喪失、改変、無権限の開示又は無権限のアクセスを導くような、送信され、記録保存され、又は、その他の取扱いが行われる個人データの安全性に対する侵害を意味する。

第33条（監督機関に対する個人データ侵害の通知）

1．個人データ侵害が発生した場合、管理者は、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがない場合を除き、不当な遅滞なく、かつ、それが実施可能なときは、その侵害に気づいた時から遅くとも72時間以内に、第55条に従って所轄監督機関に対し、その個人データ侵害を通知しなければならない。

第34条（データ主体に対する個人データ侵害の連絡）

1．個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、管理者は、そのデータ主体に対し、不当な遅滞なく、その個人データ侵害を連絡しなければならない。

（略）

3．第１項で定めるデータ主体に対する連絡は、以下の条件に合致する場合、これを要しない：

(a) 管理者が適切な技術上及び組織上の保護措置を実装しており、かつ、当該措置、特に、暗号化のような、データに対するアクセスが承認されていない者にはその個人データを識別できないようにする措置が、個人データ侵害によって害を受けた個人データに対して適用されていた場合；

(b) 管理者が、第１項で定めるデータ主体の権利及び自由に対する高いリスクが具体化しないようにすることを確保する事後的な措置を講じた場合；又は、

(c) それが過大な負担を要するような場合。そのような場合、データ主体が平等に効果的な態様で通知されるような広報又はそれに類する方法に変更される。

第83条（制裁金を科すための一般的要件）

4．以下の条項違反行為は、第２項に従い、1000 万ユーロ以下の制裁金に服するものとし、又は、事業の場合、直前の会計年度における世界全体における売上総額の2%以下の金額、若しくは、いずれか高額の方の制裁金に服するものとする：

(a) 第８条、第11条、第25条から第39条並びに第42条及び第43 条による管理者及び処理者の義務

GDPRに基づくデータ侵害通知に関するガイドライン9/2022 Version2.0の内容（抜粋）

「先に詳述したように、GDPRは、個人データ侵害が発生した場合、管理者は、不当な遅滞なく、かつ、それが実施可能なときは、その侵害に気づいた時から遅くとも72時間以内に、その侵害を通知するよう、要求している。このことは、いつ管理者が侵害を「認識」したとみなされうるかという疑問を提示しうる。EDPBは、管理者が、個人データの侵害につながるセキュリティインシデントが生じたことを合理的な程度に確信した時点で「認識」したとみなされるであろうと考えている。」（パラグラフ31）