M&P Legal Note 2021 No.6-2

シリーズ　2020年改正個人情報保護法と実務への影響
第２回　漏えい等の報告・本人通知

2021年6月25日
松田綜合法律事務所
弁護士　森田岳人

本稿はシリーズ「2020年改正個人情報保護法と実務への影響」の第2回となります。用語については特段の指摘がない場合には、従前と同じ意味で使用します。

１　漏えい等の報告・本人通知

（１）現行法

現行法では、個人データの漏えい、滅失、毀損（以下「漏えい等」）があった場合に、個人情報取扱事業者がどのように対応すべきか、つまり、個人情報保護委員会や本人に漏えい等について報告すべきかについて、実は個人情報保護法上は何ら定められていません。
ただ、法令ではなく、個人情報保護委員会の「告示」という形で、個人データの漏えい等が生じた場合に個人情報保護委員会へ報告することや、本人へ通知することなどが定められており[1]、実務上は当該告示に則って対応することが多いです。

（２）改正法

ア　改正法による明文化、法的義務化

現行法では単なる告示に過ぎず法令上の義務ではないため、個人データの漏えい等が生じた場合に、個人情報取扱事業者が告示で求められている対応をしなくても何ら指導や処分を受けることもありません。
そのため、漏えい等がおこっても、個人情報保護委員会への報告等が行われないことも少なからずあったようです。
そこで、改正法では、個人データの漏えい等が生じた場合に、個人情報保護委員会へ報告と

[1] https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

本人への通知について明確に条文に定め、法的義務としました。また、法令及びガイドライン案[2]で、具体的にどのような場合に、どのような対応が必要なのかを、可能な限り明確化しました。

イ　対応が必要な事案

実際の個人データの漏えい等が生じた場合、その規模、情報の内容、漏えい等の方法、セキュリティの有無や程度など、事案ごとに様々な違いがあります。そのため、漏えい等が起こった場合に、全ての事案について一律に個人情報保護委員会への報告や本人への通知を求めることは、必ずしも適切ではありません。
そこで、改正法では、個人データの漏えい等のうち、「個人データの安全の確保に係る自体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」に、対応が必要としています（改正法 22 条の 2 第 1 項）。
具体的には、以下の 4 つの場面です（改正法規則 6 条の 2）。

①要配慮個人情報が含まれ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

具体例
病院における患者の診療情報や調剤情報を含む個人データを記録した USB メモリーを紛失した場合
従業員の健康診断等の結果を含む個人データが漏えいした場合
（ガイドライン案 3-5-3-1（1））

②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

具体例
EC サイトからクレジットカード番号を含む個人データが漏えいした場合
送金や決済機能のあるウェブサービスのログイン ID とパスワードの組み合わせを含む個人データが漏えいした場合
（ガイドライン案 3-5-3-1(2)）

③不正の目的をもって行われた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

[2] https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000219180

具体例
不正アクセスにより個人データが漏えいした場合
ランサムウェア等により個人データが暗号化され、復元できなくなった場合
個人データが記載又は記録された書類・媒体等が盗難された場合
従業者が顧客の個人データを不正に持ち出して第三者に提供した場合
（ガイドライン案 3-5-3-1(3)）

④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

具体例
システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が 1,000 人を超える場合

留意点が２つあります。
1 つ目は、漏えい等が発生した場合だけではなく、「おそれがある」場合も対象になりますので、対象範囲が広くなっていることです。ガイドライン案では「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確証がない場合がこれに該当する」とされており、いくつかの具体例も記載されています（ガイドライン案 3-5-3-1 の※3）。
2 つ目は、いずれの事案においても、「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」が講じられている場合には、対象から除かれることです。なお、「高度な暗号化」以外に具体的にどのような措置があればよいのかについては、法令やガイドラインには記載がありません。また、どのような暗号化であれば「高度」と言えるのかについても、明確な記載はありません。

ウ　個人情報保護委員会への報告の方法や期限

（ア）速報

個人データの漏えい等が生じた場合、個人情報取扱事業者は、速やかに以下の事項を個人情報保護委員会へ報告しなければなりません（改正法 22 条の 2 第 1 項、改正法規則 6 条の 3 第 1 項）。
なお、「速やかに」は、おおむね３～５日以内とされており、報告方法は、個人情報保護委員会のウェブサイト上の報告フォームに入力する方法で行うものとされています（ガイドライン案 3－5－3－3）。
また、以下の事項を全て報告する必要はなく、報告時点で把握しているものだけを報告すれ

ば足ります。
なお、報告先は原則として個人情報保護委員会ですが、報告受理権限が事業所管大臣に委任されている場合（改正法 44 条 1 項）には、当該事業所管大臣が報告先になります。

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
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

（イ）確報

個人データの漏えい等が生じた場合、個人情報取扱事業者は、上記（ア）の速報に加え、上記（ア）記載の事項を、原則として 30 日以内に個人情報保護委員会または事業所管大臣に報告しなければなりません（改正法 22 条の 2 第 1 項、改正法規則 6 条の 3 第 2 項）。
なお、上記イの「③不正の目的をもって行われた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」に該当する場合には、報告期限が 60 日以内となります（同）。
原則として上記（ア）記載の事項の全てを報告しなければなりませんが、合理的努力を尽くしたうえで、一部の事項が判明していないときには、後日追完することも認められています（ガイドライン案 3-5-3-4）。

（ウ）報告義務の主体

漏えい等の報告の義務を負う主体は、当該個人データを取り扱う個人情報取扱事業者です。個人データの取り扱いを委託している場合には、原則として委託元と委託先の双方が報告義務を負います。ただし、委託先が、委託元に漏えい等の事態が発生したことを速やかに通知したときは、委託先は報告義務を免除されます（改正法 22 条の 2 第 1 項但書、改正法規則 6 条の 4）。

エ　本人への通知の内容及び方法

（ア）通知の時間的制限

漏えい等が生じた場合、個人情報取扱事業者は、当該事態の状況に応じて速やかに本人への

通知を行わなければなりません（改正法 22 条の 2 第 2 項、改正法規則 6 条の５）。「当該事態の状況に応じて速やかに」というのが具体的にいつまでなのかについては個別事案ごとに判断されるとされていますが、例えば以下のような事案では、時間的な猶予が認められます。

具体例
インターネット上の掲示板等に漏えいした複数の個人データがアップロードされており、個人情報取扱事業者において当該掲示板等の管理者に削除を求める等、必要な初期対応が完了しておらず、本人に通知することで、かえって被害が拡大するおそれがある場合。
漏えい等のおそれが生じたものの、事案がほとんど判明しておらず、その時点で本人に通知したとしても、本人がその権利利益を保護するための措置を講じられる見込みがなく、かえって混乱が生じるおそれがある場合。
（ガイドライン案 3-5-4-2）

（イ）通知の内容

本人へ通知すべき事項については、上記ウ（ア）の事項のうち、①、④、⑤、⑨に限られています（改正法規則 6 条の 5）。

（ウ）通知の方法

本人への通知の方法は、事業の性質及び個人データの取り扱い状況に応じ、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とされており、例えば文書による郵送や、電子メールによる送信が考えられます（ガイドライン案 3-5-4-4）。

（エ）通知の義務主体

本人への通知の義務を負う主体は、当該個人データを取り扱う個人情報取扱事業者です。個人データの取り扱いを委託している場合には、原則として委託元と委託先の双方が通知義務を負います。ただし、委託先が、委託元に漏えい等の事態が発生したことを速やかに通知したときは、委託先は報告義務を免除されます（改正法 22 条の 2 第 2 項）。

（オ）通知の例外

本人への通知を要する場合であっても、本人への通知が困難である場合には、本人の権利利益を保護するために必要な代替措置を講ずれば足ります（改正法 22 条の 2 第 2 項但書）。

本人への通知が困難な場合の具体例
保有する個人データの中に本人の連絡先が含まれていない場合

連絡先が古いために通知を行う時点で本人へ連絡できない場合
（ガイドライン案 3-5-4-5）

代替措置の具体例
事案の公表
問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにすること
（ガイドライン案 3-5-4-5）

（3）実務への影響

以上のとおり、個人データの漏えい等が生じた場合の対応が個人情報保護法上の法的義務とされ、またその適用範囲についてもガイドライン案等でかなり明確になったことから、個人情報取扱事業者は、漏えい等が生じた場合には、法やガイドラインに則った適切な対応を迅速に行う必要があります。
特に実務上は、原則 30 日、一部 60 日以内という報告期限が定められたことが大きいと思われます。
当事務所では個人データの漏えい等が生じた場合の対応について助言をすることがありますが、漏えい等のインシデントが生じた場合、事案の把握、関係部署（営業、総務、システム、広報など）との連携、個人情報保護委員会や警察との連絡、調査会社による調査など、同時に複数の対応を迫られます。関係部署の担当者には当然通常業務があるわけですが、漏えい等が生じた場合には、突然、通常業務とは別に、危機管理対応を迫られることになりますので、関係部署の担当者の業務負担は相当なものがあります。
しかも、今後は法律で期限が定められていますので、ますます時間制約が厳しい中で、同時並行で様々な対応をしなければなりません。
したがって、漏えい等が生じた後に全てを考えるのではなく、あらかじめ漏えい等に備えて、対応部署や基本的な対応方法を定めておき、いざというときに対応部署を中心に迅速な情報集約と判断ができるようにしておくべきかと思われます[3] [4]。

また、本シリーズの第 1 回でも触れましたが、改正法 22 条第 1 項が定める個人データの漏えい等が生じた場合には、本人は個人情報取扱事業者に対し、保有個人データの利用停止、

[3] CSIRT（Computer Security Incident Response Team）という、セキュリティインシデントに対応する組織内のチームをつくる動きが近年増えています。
[4] EU の一般データ保護規則（GDPR）では 72 時間以内に監督機関への通知が要求されており（33 条）、それと比較すれば、改正個人情報保護法の要求水準であればまだ時間的余裕があるとも言えます。

消去及び第三者提供停止を請求することができます（改正法 30 条 5 項）。
この利用停止等の請求がされた場合には、個人情報取扱事業者は、請求した本人の保有個人データが利用できなくなるわけですから、多数の利用停止等の請求が行われれば、今後の事業遂行に大きな影響を及ぼす可能性があります。
したがって、個人データの漏えい等のリスクを可能な限り減らすために、普段から十分な安全管理措置を実践しておくことが何よりも重要です。

（つづく）

シリーズ　2020 年改正個人情報保護法と実務への影響
第 1 回　利用停止・消去、第三者提供の停止　(本稿)
第 2 回　漏えい等報告・本人通知　（以下、次回以降）
第 3 回　不適正利用の禁止
第 4 回　認定団体制度の充実
第 5 回　公表事項等
第 6 回　仮名加工情報
第 7 回　個人関連情報
第 8 回　越境移転
第 9 回　その他

この記事に関するお問い合わせ、ご照会は以下の連絡先までご連絡ください。

弁護士　森田岳人
info@jmatsuda-law.com

松田綜合法律事務所
〒100-0004　東京都千代田区大手町二丁目 6 番 1 号　朝日生命大手町ビル 7 階
電話：03-3272-0101　FAX：03-3272-0102