

2021年6月

令和2年改正個人情報保護法の施行に向けて ①個人データ漏えい等発生時の実務対応一

1. ガイドラインの一部を改正する告示(案)の公示

(1) 経緯

令和3年5月19日、令和2年改正個人情報保護法(令和2年6月12日公布、令和4年4月1日施行[一部を除く])。以下「改正個人情報法」といいます。)に関する各種ガイドラインを改正する告示(案)が公示され、パブリックコメント手続に付されました¹。最終的には、パブリックコメント手続において提出される意見を踏まえて内容が確定することにはなりますが、その草案となるガイドライン(案)の検討は、改正個人情報法対応の準備を進めていく上でも、実務上有意義といえます。

(2) 令和2年改正の概要

個人情報保護法の令和2年改正の概要は、次のとおり多岐にわたるものであり、各種ガイドラインについても大幅に改正されています²。

1	個人の権利の在り方
	<ul style="list-style-type: none"> ● 利用停止等請求権に係る要件緩和 ● 保有個人データの範囲の拡大等
2	事業者の守るべき責務の在り方
	<ul style="list-style-type: none"> ● 漏えい等の委員会への報告 ● 本人への通知等の義務化等
3	事業者による自主的な取組を促す仕組みの在り方
	<ul style="list-style-type: none"> ● 認定個人情報保護団体の認定対象の拡大
4	データ利活用に関する施策の在り方
	<ul style="list-style-type: none"> ● 仮名加工情報の創設等
5	ペナルティの在り方
	<ul style="list-style-type: none"> ● 法定刑の引き上げ
6	法の域外適用・越境移転の在り方
	<ul style="list-style-type: none"> ● 外国事業者の報告徴収・命令の対象化等

(3) 本稿のテーマ

本稿では、全ての事業者に適用の余地があり、かつ、特に実務上の影響が大きい改正点の一つである、漏えい等の報告等を行う義務について、関連する改正個人情報法及び規則の変更点とともに、個人情報保護法ガイドライン(通則編)(案)(以下「ガイドライン案」といいます。)の概要をご紹介します。

2. 漏えい等事案が発覚した場合の改正点

(1) 漏えい等報告義務等の法的義務化

個人データの漏えい等又はそのおそれのある事案(以下「漏えい等事案」といいます。)が発覚した場合、現行法上、①個人情報保護委員会(以下「個情委」といいます。)に対する報告は努力義務とされており³、②本人に対する連絡は「講ずることが望ましい」措置の一つという位置づけ⁴でした。これに対し、改正個人情報法においては、漏えい等事案のうち「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」については、①個情委に対する報告(改正個人情報法第22条の2第1項本文)及び②本人に対する通知(改正個人情報法第22条の2第2項)がいずれも法的義務とされました。

(2) 個情委への報告・本人通知が必要となる場合

個情委に対する報告及び本人に対する通知が必要となるのは、「個人データの漏えい、滅失、棄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」とされており(改正個人情報法第22条の2第1項)、具体的には、次の4種類のいずれかの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がこれに該当するとされています(改正個人情報法施行規則(以下「規則」といいます。)第6条の2第1号ないし第4号)。

【Data&Privacy/本号監修・執筆者(弁護士)】

生田 美弥子 (mikuta@kitahama.or.jp)
若井 大輔 (dwakai@kitahama.or.jp)
藤原 成和 (sfujiwara@kitahama.or.jp)
細井 南見 (mhosoi@kitahama.or.jp)

◆本ニュースレターは法的助言を目的するものではなく、個別の案件については当該案件の個別の状況に応じ、弁護士の助言を求めて頂く必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所又は当事務所のクライアントの見解ではありません。本稿の内容、テキスト等の無断転載・無断引用を禁止します。

◆本ニュースレターに関する一般的なお問合せは、下記までご連絡ください。
北浜法律事務所・外国法共同事業 ニュースレター係
(TEL: 06-6202-1088 E-mail: newsletter@kitahama.or.jp)

【大 阪】北浜法律事務所・外国法共同事業
〒541-0041 大阪市中央区北浜1-8-16 大阪証券取引所ビル
TEL 06-6202-1088 (代) / FAX 06-6202-1080

【東 京】弁護士法人北浜法律事務所東京事務所
〒100-0005 東京都千代田区丸の内1-7-12 サピアタワー14F
TEL 03-5219-5151 (代) / FAX 03-5219-5155

【福 岡】弁護士法人北浜法律事務所福岡事務所
〒812-0018 福岡市博多区住吉1-2-25
キャナルシティ・ビジネスセンタービル4F
TEL 092-263-9990 / FAX 092-263-9991

<https://www.kitahama.or.jp/>

第1類型	要配慮個人情報の漏えい等 例：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
第2類型	不正利用により財産的被害が生じるおそれがある漏えい等 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
第3類型	不正の目的をもって行われた漏えい等 例：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
第4類型	個人データの本人の数が1,000人を超える漏えい等 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

1	概要 発生日、発覚日、発生事案、発見者、規則第6条の2各号該当性、委託元及び委託先の有無、事実経過等
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 媒体や種類（顧客情報、従業員情報の別等）を含む
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 事態が発生した主体（報告者又は委託先）を含む
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

また、ガイドライン案においては、本人の数が確定できない漏えい等の場合にも、漏えい等が発生したおそれがある（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ような）個人データに係る本人の数も含めて最大1,000人を超える場合には、第4類型に該当するとされています⁵ので、漏えい等が確実なものだけでなく、漏えい等のおそれがある個人データも含めて広く事実関係を調査する必要がある点に注意が必要です。

その他、上記のいずれの類型においても、漏えい等事案が生じた個人データについて、「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個情委に対する報告及び本人に対する通知の義務は発生しないとされています。

（3）個情委に対する報告の時間的制限・報告事項

個情委に対する報告については、個情委が早急に事態を把握する必要がある一方、把握に時間を要する内容についても報告させる必要があることから、①速報及び②確報の二段階に分けて行うものとされています。具体的には、①速報については、漏えい等の事態を知った後「速やかに」（概ね3～5日以内⁶）報告するものとされ（規則第6条の3第1項柱書）、②確報については、漏えい等事案の類型に応じて30日（上記の第3類型以外）又は60日以内（上記の第3類型）以内に報告するものとされています（規則第6条の3第2項）。②確報の報告期限は、漏えい等の事態を知った日を1日目として（初日参入）、土日祝日を含む暦日ベースで算定するものとされています⁷。

報告事項は、①速報及び②確報に共通するものとして、次の9事項⁸（以下「報告事項」といいます。）を報告すべきものとされています（規則第6条の3第1項各号）。

①速報については、報告時点において把握している内容を報告すれば足り、原則として、個情委が指定する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。

②確報については、全ての報告事項を期限内に報告しなければなりません。もっとも、確報時点において、合理的努力を尽くした上で、一部の事項が判明しておらず、全ての事項を報告することができない場合には、その時点で把握している内容を報告し、判明次第、報告を追完するものとされています⁹。なお、速報時点で全ての報告事項を報告できる場合は、1回の報告で確報を兼ねることができるとされています。

（4）本人通知の時間的制限・通知事項

本人に対する通知は、漏えい等の事態を知った後、「当該事態の状況に応じて速やかに」（個別の事案ごとに、通知により本人の権利利益が保護される蓋然性や通知による弊害等を勘案して判断するものとされ、具体的な日数の目安は示されていません¹⁰。）行うものとされており、速やかに通知することでかえって本人に不利益が生じる場合もあるため、個情委への報告期限とは異なる観点から期限が設定されています。

本人に通知する事項は前記（３）の報告事項のうち、以下の５項目とされています（規則第６条の５）。

1	概要 発生日、発覚日、発生事案、発見者、規則第６条の２各号該当性、委託元及び委託先の有無、事実経過等
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 媒体や種類（顧客情報、従業員情報の別等）を含む
3	原因 事態が発生した主体（報告者又は委託先）を含む
4	二次被害又はそのおそれの有無及びその内容
5	その他参考となる事項

また、①本人通知が困難（保有個人データに連絡先が含まれていない場合等）、かつ、②本人の権利利益を保護するため必要な措置（事案の公表等）をとっている場合、本人通知が不要とされています¹¹（改正個人情報法第２２条の２第２項ただし書）。なお、本人通知の方法は、郵送や電子メールなど、合理的かつ適切な方法で行うものとされています。

（５）委託先から委託元への通知

個人データの取扱いを委託しており、委託先において漏えい等事案が生じた場合、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が、委託先は、漏えい等の事態を知った後「速やかに」（概ね３～５日以内¹²）、委託元に対し、前記（３）の報告事項について、報告時点で把握しているものを通知した場合には、①個人情報に対する報告義務及び②本人通知義務を免除されます（改正個人情報法第２２条の２第１項ただし書・規則第６条の４）。

（６）漏えい等事案が発覚した場合に講ずべき措置

さらに、ガイドライン¹³においては、個人情報への報告・本人への通知のほかにも、漏えい等事案が発覚した場合に、漏えい等の内容に応じて必要な措置であって、従来は「講じることが望ましい」とされていた以下の事項¹⁴について、必要な措置を「講じなければならない」と改められています¹⁵。かかる変更は、前記（１）～（５）と異なり、全ての漏えい等事案に適用されます。

1	事業者内部における報告及び被害の拡大防止
2	事実関係の調査及び原因の究明
3	影響範囲の特定
4	再発防止策の検討及び実施

３．ガイドライン（案）を踏まえた実務対応

上記のとおり、現行法の下では、個人データの漏えい等事案が発生した場合、個人データの量、性質、本人への影響等を踏まえて、事実関係の調査・原因の究明や再発防止策の検討・実施等について講ずる措置や、個人情報に対する報告は、いずれも努力義務にとどまり、具体的な対応については、事業者の自主的な判断に委ねられていましたが、改正個人情報法の下では、一定の種類の漏えい等事案については、個人情報への報告及び本人通知が法的義務とされました。これまでも、実務上は、漏えい等の事故があった場合には、個人情報に対する報告や本人通知の要否について検討していた事業者が多かったものと思います。

しかし、令和２年改正により、全ての事業者において、これらの報告・本人通知が法的義務にあたらぬか、法令・ガイドラインに従って報告・本人通知を行う必要がないかを検討しなければならないこととなります。また、法令・ガイドラインにおいては、上記のとおり、報告・本人通知について、迅速な対応が求められていますので、個人情報に対する報告・本人通知を行うために必要なタイムラインを踏まえて、漏えい等事案の対応フローを予め見直しておくことも必要です。

なお、改正個人情報法の下では、個人情報保護法令に基づく対応のほか、改正個人情報法に基づく本人に対する通知を契機として、本人が民事上の損害賠償請求を行うことが容易になり、このような請求を受けるリスクが高まる可能性がある点にも注意が必要と考えられます¹⁶。

４．結び

改正個人情報法では、本稿でご紹介した事項のほかにも、現行法からの重要な変更点が多数あります。当事務所「個人情報 ニュースレター」では、次号以降も、改正個人情報法の主要な改正点について、ガイドライン案に対するパブリックコメント手続の結果も踏まえつつ、ご紹介する予定です。

さらに、個人情報保護法は、いわゆる３年ごと見直しが見送られており、令和２年改正では見送られた課徴金の導入等の論点もあり、今後も改正の動向が注目されます。

以上

¹ 「「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、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）」の一部を改正する告示」等に関する意見募集について」（e-Gov パブリックコメント）（<https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=240000069&Mode=0>）（令和３年６月８日に利用）

² 個人情報の保護に関する法律等の一部を改正する法律（概要）（https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf）



³ 個人情報「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）」3.

⁴ 前掲脚注 3 告示 2. (5)

⁵ ガイドライン案 3-5-3-1 (4)

⁶ ガイドライン案 3-5-3-3

⁷ ガイドライン案 3-5-3-4、同 (※2)

⁸ ガイドライン案 3-5-3-3 (1) ないし (9)

⁹ ガイドライン案 3-5-3-4

¹⁰ ガイドライン案 3-5-4-2

¹¹ ガイドライン案 3-5-4-5

¹² ガイドライン案 3-5-3-5

¹³ 個人情報保護法ガイドライン（通則編）の一部を改正する告示案においては、前掲脚注 3 告示は廃止し、個人情報保護法ガイドライン（通則編）に統合するものとされています。

¹⁴ 前掲脚注 3 告示 2. (1) ないし (4)

¹⁵ ガイドライン案 3-5-2

¹⁶ 近時の裁判例では、ベネッセ事件（最二小判平成 29 年 10 月 23 日判例タイムズ 1442 号 46 頁）において、1 人当たり最大 3,300 円の損害賠償が認められたほか（東京高判令和 2 年 3 月 25 日裁判所ウェブサイト等）、TBC 事件（東京高判平成 19 年 8 月 28 日判例タイムズ 1264 号 299 頁）では、1 人当たり 3 万 5000 円の損害賠償が認められています。また、田路至弘=松原崇弘「情報漏えいと取締役の内部統制システム構築義務」商事法務 2117 号 11 頁は、代表取締役等の役員について、内部統制システム構築義務違反を理由とする任務懈怠に基づく損害賠償責任（会社法第 423 条第 1 項）が認められる可能性も指摘しています。