資料１

改正法に関連する政令・規則等の整備に向けた論点について
（漏えい等報告及び本人通知）

令和２年10月30日

１．改正法における漏えい等報告・本人通知の概要

- 漏えい等が発生し、**個人の権利利益を害するおそれが大きい場合**に、**委員会への報告・本人への通知を義務化**（改正法第22条の２）。

- 対象となる事態、委員会への報告・本人への通知の方法等については、委員会規則で定めることとしている。

改正後の個人情報の保護に関する法律（平成15年法律第57号）

（漏えい等の報告等）

第22条の２　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。

2．検討すべき主な論点

- 漏えい等報告の趣旨は、**委員会が事態を早急に把握し、必要な措置を講じることができるようにすること**にある。

- 本人通知の趣旨は、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。

▶ こうした制度趣旨も踏まえ、以下の事項を検討する必要があるのでないか。

① 漏えい等報告・本人通知の対象となる事態

② 報告の時間的制限・報告事項

③ 本人通知の時間的制限・通知事項

④ 委託先から委託元への通知方法

⑤ その他

①漏えい等報告・本人通知の対象となる事態

（１）基本的考え方

- 改正法において「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」を漏えい等報告・本人通知の対象としている。

- 現行の告示に基づいて委員会に報告された事案についてみると、**漏えい等の対象となった本人の数だけで重大性を判断できるものではない**。

- 制度改正大綱の意見募集においても、**形式的に漏えいされた個人データの数だけを考慮するのではなく、個人の権利利益に対する実質的な影響を考慮すべき**との意見があった。

- 漏えい等報告を義務化している諸外国の個人情報保護法制においても、その要否を判断するにあたって、様々な要素を考慮している。例えば、GDPRにおいては、個人データ侵害のリスクを評価するにあたって、侵害の種類、個人データの性質・機微性及び量等複数の要素を考慮するとされている。

①漏えい等報告・本人通知の対象となる事態

（１）基本的考え方

- 一方で、事業者が委員会への報告及び本人通知の要否を判断できるよう、**基準として明確かつ簡便である必要がある。**

▶ したがって、様々な考慮要素の中から、まずは個人の権利利益に対する影響が大きいと考えられる、**漏えい等した個人データの性質・内容、漏えい等の態様、漏えい等の事態の規模等**を考慮した上で、対象となる事態を定めるものとしてはどうか。

①漏えい等報告・本人通知の対象となる事態

（参考）「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱」に関する意見募集結果（抜粋）

【意見】「一定以上の漏洩」「一定の類型」の要件をガイドライン等で具体的にして頂きたい。

【理由】大規模な個人データ漏えい、要配慮個人情報の漏えい等、迅速な対応が求められる事案がある一方、事業者がそういった事案に該当するかを判断するのは難しく、ガイドライン等で事例や規模の目安などを示していただきたい。【一般財団法人　日本情報経済社会推進協会】

報告・本人通知の基準を設定するにあたっては、これらの義務化が個人の権利利益の保護を図ることにあることに鑑みて、形式的に漏えいされた個人データの数だけを考慮するのではなく、実質的に、個人の権利利益に重大な侵害を与える可能性があるかどうか、すなわち、漏えいされた個人データの種類、漏えいの状況（アクセス可能であった人の数や期間）、漏えいにより生じる可能性のある損害の性質、漏えい後の是正措置（限られた相手にメールで誤送信した個人データが削除されたことを確認できたことなど）なども考慮した基準にすべきである（つまり、一定の形式的基準及び実質的基準をすべて満たす場合のみに報告及び／又は本人通知を義務付けべきである）と考えます。【一般社団法人　国際銀行協会】

漏えい報告の法的義務が課される対象となる事案は、重大な事案に限定されるべきであり、当該重大な事案についてガイドライン等において明確化がなされるべきと考えます。そして、この重大な事案の判断は、漏えいした個人データの数量に紐づいた閾値を設け、当該閾値を形式的に超えれば、自動的に要件を充足すべきものではなく、データ主体の権利と自由に対して生じるリスクの重大性及び当該リスクが生じる可能性を考慮することによりなされるべきです。その判断にあたっては、個人データの数量以外にも、たとえば、個人データの性質・機微性、個人の特定の容易性、個人に生じる損害の大きさ、データ主体の性質（子供等の脆弱なデータ主体）、個人データが意図不明又は悪意を持っている可能性のある者の手にある可能性があるか否か、個人にとっての結果の永続性があるか等が考慮要素に入れられるべきと考えられます。【個人】

①漏えい等報告・本人通知の対象となる事態

（参考）GDPR（一般データ保護規則）のGuidelines on Personal data breach notification under Regulation（規則に基づく個人データ侵害通知に関するガイドライン）について

- 個人データ侵害が発生した場合において、「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」侵害は、監督機関への通知を要しないこととされている（第33条第１項）。
- リスクを評価するに当たっては、以下の要素を考慮すべきであるとしている。
  - 侵害の種類
  - 個人データの性質、機微性及び量
  - 個人の特定の容易性
  - 個人にとっての結果の重大性
  - 個人の特別な特性
  - データ管理者の特別な特性
  - 影響される個人の人数
  - 一般的な点

①漏えい等報告・本人通知の対象となる事態

（２）方向性

ア　対象となる事態の類型について

- **個人データの性質**

  機微性は様々であるが、特に**要配慮個人情報**は、その取扱いによっては差別や偏見を生じるおそれがあり、漏えい等による個人の権利利益に対する影響が大きいのではないか。

- **個人データの内容**

  漏えい等によってクレジットカード番号等が不正利用される事案は、従前から大きな問題となっている。このように、**財産的被害が発生するおそれがある場合**（例：クレジットカード番号やインターネットバンキングのID・パスワード等）は、個人の権利利益に対する影響が大きいのではないか。

- **漏えい等の態様**

  過失により生じたものと故意により生じたものでは、個人の権利利益に対する影響が異なり、**故意によるもの**（例：不正アクセスや従業員による持ち出し等）は、類型的に二次被害が発生するおそれが大きいのではないか。

- これらに該当しない事案であっても、**一定数以上の大規模な漏えい等**については、安全管理措置の観点から特に問題があると考えられるのではないか。

①漏えい等報告・本人通知の対象となる事態

（２）方向性

イ　大規模な漏えい等の基準について

- これまでに発生した漏えい等事案について、**件数の分布や事案の傾向等を踏まえて、**基準を検討する必要があるのではないか。

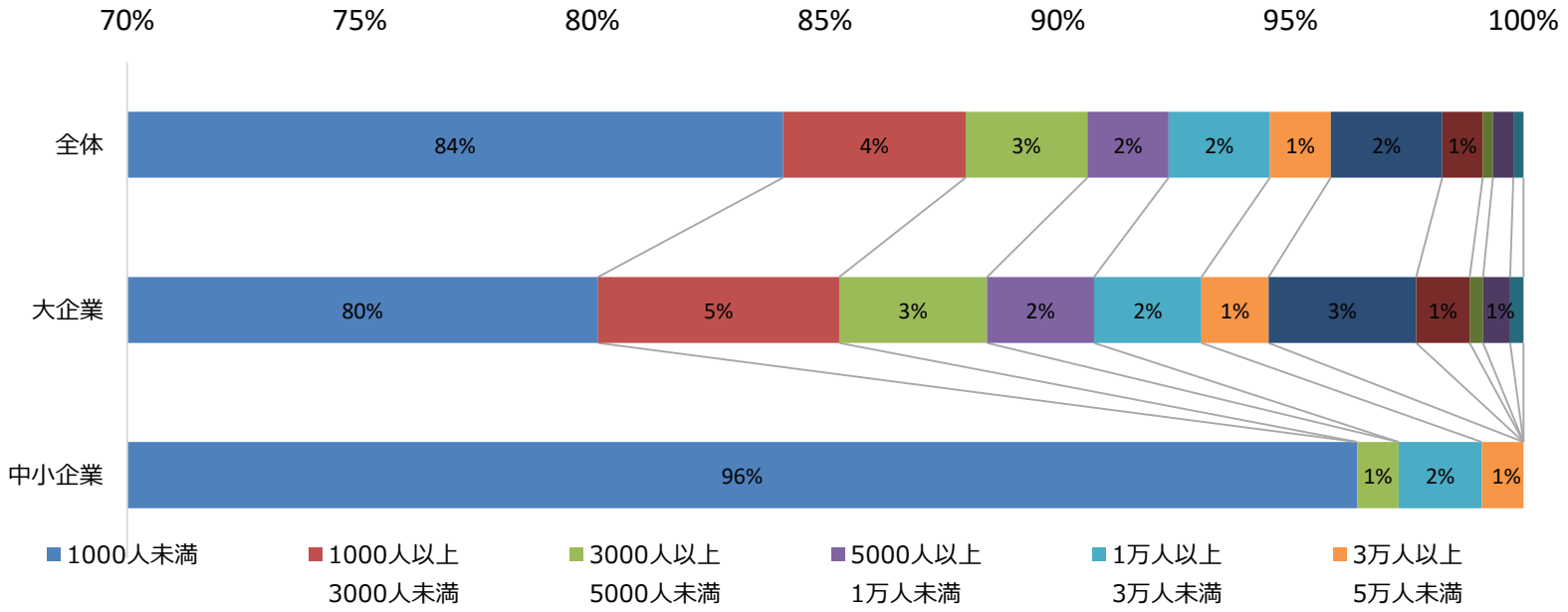
▶ 例えば、過去の漏えい等事案の件数の分布と、件数別の事案の傾向（1,000人を超える事案では、安全管理措置に大きな問題がある傾向にある）を踏まえて、**1,000人を基準とすることが考えられるのではないか。**

①漏えい等報告・本人通知の対象となる事態

（２）方向性
イ　大規模な漏えい等の基準について

（参考１）漏えい等事案の発生状況（事業者アンケート）

- 過去に漏えい等が発生した事業者464社において、漏えい等したデータに係る本人の数が最多であった事案における本人の数を集計したところ、1,000人未満が84%、1,000人以上3,000人未満が４%となった。



（出典）個人情報保護委員会「個人情報の適正な取扱いに関する実態調査（令和元年度）報告書」

①漏えい等報告・本人通知の対象となる事態

（２）方向性

イ　大規模な漏えい等の基準について

（参考２）令和元年度　漏えい等事案に関する報告の受付状況

- 委員会報告事案のうち、501人以上の事案が約15%、1,001人以上の事案が約11%、3,001人以上の事案が約７%となっている。

	個人情報保護委員会		委任先省庁		認定団体		合計	
	件数	割合	件数	割合	件数	割合	件数	割合
500人以下	901	84.5%	1,453	95.7%	1,802	93.1%	4,156	91.9%
501～1,000人	33	3.1%	14	0.9%	33	1.7%	80	1.8%
1,001～3,000人	48	4.5%	21	1.4%	23	1.2%	92	2.0%
3,001～5,000人	16	1.5%	7	0.5%	11	0.6%	34	0.8%
5,001～10,000人	18	1.7%	7	0.5%	7	0.4%	32	0.7%
10,001～30,000人	13	1.2%	8	0.5%	5	0.3%	26	0.6%
30,001～50,000人	4	0.4%	4	0.3%	1	0.1%	9	0.2%
50,001人～	22	2.1%	1	0.1%	4	0.2%	27	0.6%
不明/調査中	11	1.0%	4	0.3%	49	2.5%	64	1.4%
	1,066		1,519		1,935		4,520	

①漏えい等報告・本人通知の対象となる事態

（２）方向性
ウ　漏えい等の「おそれ」がある場合について

- **漏えい等が確定していない段階においても**、事業者が漏えい等の「おそれ」を把握した場合、事態を把握した上で、**漏えい等が発生していた場合の被害を最小限にする必要**がある。

- 「おそれ」が生じた時点で、**委員会が報告を受け、事態を把握することができれば**、当該事業者に対して、**必要な措置を講じるよう、求めることができる**。

- また本人としても、「おそれ」が生じた時点で、**早期に事態を把握することができれば、本人として必要な措置を講じることができる**。

▶ したがって、漏えい等の**「おそれ」がある事態についても、漏えい等報告・本人通知の対象**としてはどうか。

①漏えい等報告・本人通知の対象となる事態

（２）方向性

エ　暗号化された個人データの取扱い

- **暗号化が講じられた個人データ**の漏えい等について、**「個人の権利利益を害するおそれが大きいもの」に該当するか**、検討する必要がある。

- 暗号化については、その方法にもよるが、漏えい等が発生した場合においても、**権限のない第三者が見読することを困難にする措置として有効**であり、**現行**の告示に基づく報告制度においても、**「高度な暗号化等の秘匿化」がされた個人データは報告の対象外**とされている。

- なお、改正法において、仮名加工情報である個人データは、漏えい等報告の対象外となっている。

▶ したがって、**高度な暗号化等の秘匿化がされた個人データ**については、**漏えい等報告・本人通知の対象外となる場合を認める方向**で検討してはどうか。

②報告の時間的制限・報告事項

（１）基本的考え方

- 漏えい等が発生した際の委員会への報告については、速やかに行う必要がある一方で、原因や再発防止策等、把握に時間を要する内容も報告に含める必要があるところ、これらの要請を満たす報告を一度に行うことは困難である。

▶ そこで、漏えい等の報告の期限については、**速報と確報の二段階**とした上で、それぞれ定めるものとしてはどうか。

- 速報については、事業者に漏えい等が発覚した後、速やかに報告することを求めるものであるが、**漏えい等が発覚した当初の段階では、事実関係を十分に把握できていない場合がある**ことに留意する必要がある。

- 確報については、原因や再発防止策も含めて報告を求めるものであり、事実関係の把握に時間を要することから、**一定の時間的猶予を設ける**必要がある。

②報告の時間的制限・報告事項

（２）方向性
ア　速報について

- 委員会が事態を早急に把握し、必要な措置を講じることができるようにするという漏えい等報告の趣旨からすれば、事案に関わらず一律に期限を設け、報告することを求めることも考えられるが、事業者が**事態を把握するのに要する時間については、個別具体的な事情によるところが大きい**。

▶ そこで、規則においては、明確な時間的制限を設けることなく、「速やかに」と定めた上で、**その目安をガイドラインで示してはどうか**。

- また、漏えい等が発覚した当初の段階では、事実関係を十分に把握できていないこともある。

▶ 報告内容については、現行の告示で報告内容とされている事項をもとに検討を行った上で、**速報の段階においては、その時点で把握している事項を報告対象としてはどうか**。

②報告の時間的制限・報告事項

（２）方向性
イ　確報について

- 確報においては、報告が求められる事項について基本的に全て報告をする必要がある。

- 事実関係の把握には時間を要する一方で、確報について明確な時間制限を設けない場合、事業者によって対応が分かれ、委員会が早期に事実関係を把握できない事態も想定される。

- 事実関係の把握に要する時間は、事案によって異なるものであり、不正アクセス事案等の不正の目的をもって行われた行為による漏えい等については、専門的な調査が必要となる等、他の事案に比べて時間を要する傾向にある。

▶ そこで、事実関係の把握に通常要する時間を考慮した上で、**一定の時間的制限（これまでの報告実績も踏まえ、例えば30日）を設けてはどうか**。また、漏えい等の類型も考慮し、**不正の目的をもって行われた行為による漏えい等**については、**他の事案よりも時間的猶予を認め、例えば60日としてはどうか**。

③本人通知の時間的制限、通知事項

（１）基本的考え方

- 委員会への報告を要する事態が生じた場合には、**本人に対しても通知を行う必要**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。

- 本人への通知は、上記の制度趣旨を達成する観点から、**本人が必要とする内容を、本人にとって必要なタイミングで通知することが重要であり、委員会への報告と区別して検討すべきである**。

③本人通知の時間的制限、通知事項

（２）方向性

- 本人に対する通知は速やかに行う必要がある一方で、その具体的なタイミングは、事案によって異なる。また、事案によっては、速やかに通知することにより、かえって本人に不利益が生ずる場合もある。

▶ そこで、**本人側でも必要な措置を講じられるよう、速やかに行うこと**は確保しつつも、**事案によっては委員会への報告と同じタイミングで行うことまで求める必要はない**のではないか。

- また、通知事項・通知方法に関して、本人にとって重要なのは、漏えい等が発生したことやその概要を適切に把握・理解することである。

▶ そこで、通知事項について、**本人が事態を適切に理解するために必要な事項を規則で定め**た上で、通知方法と併せて、**本人にとってわかりやすい形となるようガイドライン等で例示**すべきではないか。

④委託先から委託元への通知方法

（１）基本的考え方

- 漏えい等の事態が発生した場合、**委託元と委託先の双方が個人データを取り扱っている**ときは、**原則として双方が報告義務を負う**ことになる。

- 他方、**委託先が委託元**である個人情報取扱事業者に**当該事態が発生した旨を通知したとき**は、委託先から**委員会への報告義務を免除**することとしている。この場合、委託元から委員会に報告を行うことになる。

- 委託元、委託先のどちらが主として漏えい報告や本人への通知を行うかについては、**個人情報の取扱状況や、委託の状況等に応じて、あらかじめ、業者間で決めておくことが適切である。**

- その上で、委員会や本人との関係では、委託元、委託先のどちらが主として漏えい報告等の対応を行ったとしても、適切な対応がなされるようにすることが必要。

④委託先から委託元への通知方法

（２）方向性

- 委託先は、委託元が漏えい等の事態を把握した上で、委員会に報告を行うことができるよう、報告に資する通知を行う必要がある。

- 加えて、委託元は、委託先の監督義務があり（法第22条）、委託先で漏えい等が発生した場合の委員会への通知体制を整備した上で、実際に発生した場合には、委託先における漏えい等の状況を適切に把握する必要もある。

▶ したがって、**委託元への通知は速やかに行う必要があり、**通知事項に関しては、**委員会に速報として報告する場合と同じ事項**を通知することが求められるのではないか。

▶ また、委託元、委託先の関係は状況によって様々であるため、**委託先が委託元に速やかに通知を行うことで、**委託先の委員会への報告義務自体は免除することとしてはどうか。

▶ なお、その場合も、委託先は、引き続き、漏えい等事案について適正に対処する必要があることは言うまでもなく、**委託先は、実態把握を行うとともに、漏えい等報告にも協力する必要がある**旨、ガイドライン等で明確化することとしてはどうか。

⑤その他

（１）改正法において漏えい等報告の対象とならない事案の取扱いについて

- 改正法における報告対象事案以外は、委員会として報告を求める対象ではない一方で、漏えい等のおそれの判断が困難な場合等に、事業者側から任意の報告ができるようにすべきではないか。

（２）認定個人情報保護団体の関与について

- 認定個人情報保護団体は、改正法における漏えい等報告の報告先となっていないが、認定個人情報保護団体の制度趣旨や、これまで対象事業者の漏えい等事案の対応・再発防止に関与してきたことを踏まえ、その関与の在り方を検討する必要がある。

- なお、この点を含め、認定個人情報保護団体の活動について、団体にとっても参考となるよう、望ましい取組の方向性等を委員会として示していくことが必要ではないか。

（３）漏えい等事案に関する国際的な情報共有への貢献

- 改正法において、漏えい等報告を義務化した理由の１つとして、国際的な制度調和が挙げられることや、諸外国のデータ保護機関間で漏えい等事案の傾向が情報共有され、執行に活用されていることを踏まえ、我が国もこうした取組により積極的に貢献すべきではないか。