

「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則の一部を改正する規則（案）」に関する意見
募集結果

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
1	規則案第2条	第2条で追加された、漏えい等の「おそれ」とは、具体的にどういった事案か。 【匿名】	本規則案第2条の「発生したおそれ」の具体例等については、ガイドライン等でお示しすることを検討してまいりますが、「発生したおそれ」とは漏えい等が疑われるものの確証がない場合をいい、個別の事例に即して判断することになります。
2	規則案第2条	2条2号各号 個人データ漏えい等の基準では、規則案6条の2第2号「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」とされ、「財産的被害」だけが特出しされているが、特定個人情報の漏えい等にはそれはない理由は何か。 【匿名】	特定個人情報は、利用範囲が「税・社会保障・災害対策」に限定されており、これまで当委員会に「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」のある事案と同様の事案は報告されておられません。また、マイナンバー利用の前提となる提供行為の際には本人確認が必要である等の保護措置が施されています。そのため、特定個人情報においては、「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」は想定しておられません。 なお、本規則案第2条第2号において、特定個人情報の不正の目的をもった利用等が生じたおそれがある事態には、報告いただく必要があります。
3	規則案第2条第1号	規則案2条1号 報告対象の特定個人情報のうち「高度な暗号化その他の個人情報利益を保護するために必要な措置を講じたもの」を除く規定となって	本規則案第2条第1号の「高度な暗号化その他の個人情報の権利利益を保護するために必要な措置を講じたもの」については、ガイドライン等でお示しすることを

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>いるが、この規定の仕方は、ある（ロー）データに暗号化処理を行ったものを通信するイメージで書かれているが、データには暗号化せずに通信を暗号化したものは、措置を講じたものとして対象外という趣旨か。</p> <p>【匿名】</p>	<p>検討してまいります。</p>
4	規則案第 2 条第 2 号	<p>2 条 2 号</p> <p>「発生し、又は発生したおそれ」とは、アクシデント（事態が起きたこと、又は起きているかもしれないこと）を指し、インシデント（事態が起きかねなかったこと）を含まない趣旨か。</p> <p>【匿名】</p>	<p>本規則案第 2 条の「発生し、又は発生したおそれ」については、ガイドライン等でお示しすることを検討してまいります。が、「発生したおそれ」とは漏えい等が疑われるものの確証がない場合をいい、個別の事例に則して判断することになります。</p>
5	規則案第 2 条及び規則案第 2 条第 4 号	<p>（該当箇所）</p> <p>規則（案）の第 2 条及び第 5 条</p> <p>（意見）</p> <p>グローバル・プライバシー・アライアンス（以下「GPA」といいます。）を代理して、今回、改正番号法（以下「改正法」といいます。）に関する貴委員会の規則案について、意見を提出いたします。</p> <p>GPA は、航空宇宙、通信、コンピュータ及びコンピュータソフトウェア、消費者製品、電子取引、金融サービス、物流、製薬、専門サービス、並びに旅行/観光セクターといった様々なグローバル企業で</p>	<p>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ことから、おそれがある場合も対象としており、一般的に現状の案で御理解いただけるものと考えます。</p> <p>また、利用範囲に制限のない個人情報と比べ、特定個人情報は利用範囲が「税・社会保障・災害対策」に限定されており、特定個人情報を取り扱う場面・量とも限られております。</p>

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>構成されています。GPA は、消費者の信頼向上と情報の自由な流れの確保に向けた、責任あるグローバルプライバシー慣行の推進に取り組んでいます。GPA 会員は、自らのプライバシーに関する義務を極めて真摯に受け止めています。本書に記載される意見は、GPA 会員の意見を総じて代表するものです。本書で示す全体的な姿勢は全会員が支持するものですが、個別の論点の中には全会員には該当しないものがある場合があります。</p> <p>概要</p> <p>改正番号法第 29 条の 4 及び規則案第 2 条により、個人番号利用事務等実施者は、個人の権利利益を害するおそれ大きいものとして定められる、以下の事態が発生し、又は発生したおそれがある場合には、貴委員会への報告が義務付けられます（ただし、高度な暗号化等の措置を講じたものを除きます）。</p> <ul style="list-style-type: none"> • 次に掲げる特定個人情報の漏えい等： <ul style="list-style-type: none"> ○ 情報提供ネットワークシステム及びこれに接続された電子計算機に記録された特定個人情報 ○ 個人番号利用事務実施者が個人番号利用事務を処理するために使用する情報システムにおいて管理される特定個人情報 ○ 行政機関、地方公共団体、独立行政法人等及び地方独立行政法人が個人番号関係事務を処理するために使用する情報システム並びに行政機関、地方公共団体、独立行政法人等及び地方独立行政法人から個人番号関係事務の全部又は一部の委託を受けた者が当該個人番 	<p>このため、本規則案第 2 条第 4 号で定める報告基準を個人情報の保護に関する法律施行規則案第 6 条の 2 第 4 号にあわせると、従来報告されていたような事案の把握ができなくなるなど、当委員会の適正な監視監督業務に支障が出る懸念があることから、一般的に現状の案で御理解いただけるものと考えます。</p>

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>号関係事務を処理するために使用する情報システムにおいて管理される特定個人情報</p> <ul style="list-style-type: none"> • 次に掲げる事態： <ul style="list-style-type: none"> ○ 不正の目的をもって行われたおそれがある特定個人情報の漏えい等 ○ 不正の目的による特定個人情報の利用 ○ 不正の目的による特定個人情報の提供 • 個人番号利用事務実施者又は個人番号関係事務実施者の保有する特定個人情報ファイルに記録された特定個人情報の、電磁的方法による不特定多数の者による閲覧 • 次に掲げる特定個人情報に係る本人の数が百人を超える事態： <ul style="list-style-type: none"> ○ 特定個人情報の漏えい等 ○ 法第9条の規定に反する、個人番号を含む特定個人情報の利用 ○ 法第19条の規定に反する、特定個人情報の提供。 <p>以下で詳述するとおり、漏えい等が発生したおそれがある場合にまで貴委員会に報告を求めることは、改正法で定める漏えい等の報告要件をはるかに超えるものです。特筆すべきは、実際、80を超える世界各国の漏えい等報告に関する国内法のいずれも、漏えい等の疑いや可能性を行政当局に報告することを義務付けてはいないという点です。GPAとしては、行政当局への報告義務は、漏えい等が実際に発生した場合に絞るべきであると考えますが、それは漏えい等が発生したおそれがある場合にまで報告を義務付けることで過度な報</p>	

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>告が行われることになり、組織や貴委員会の貴重なリソースが奪われ、個人の権利利益を害するおそれ大きい実際のデータ漏えい等に対応する取り組みが十分に行えなくなるためです。また、漏えい等が発生したおそれがあることを個人に通知すれば、実際のリスクには関係のない数々の通知で個人を圧倒するという逆効果を招いてしまいます。結果として、不必要な恐怖と混乱を招くだけでなく、人々を鈍感にさせ、重大なリスク発生時に害から自らを守るために必要な対策を示した通知そのものが無視される事態にもなりかねません。したがって、GPAとしては、当該報告要件を、漏えい等が実際に発生した場合、又はその発生が確認できた場合に限定することを、貴委員会に強く要請します。漏えい等が発生したおそれがある場合にまで、貴委員会への報告や個人への通知を義務付けるべきではありません。</p> <p>サイバーセキュリティ攻撃の規模 企業ネットワークは日常的に、フィッシングメール、マルウェア、ボット、ランサムウェア等、さまざまな悪質なセキュリティの脅威と攻撃の対象になっています。例えば、2018年のマルウェア攻撃は8億1267万件にも上り、2019年にはモバイルをターゲットとした新たなランサムウェアのトロイの木馬が6万8000件も検出されました (Purplesec レポートをご参照ください (https://purplesec.us/resources/cyber-security-statistics/ransomware/))。</p>	

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>以下の統計データを見れば、漏えい等が発生したおそれがある場合にまで報告を義務付けた場合に、貴委員会がどれほど膨大な量の報告を受領することになるか、感覚がつかめるはずです。国際的な銀行 275 行のセキュリティ担当幹部に対する 2017 年の調査</p> <p>(https://www.computerweekly.com/news/450417135/Banks-suffer-average-of-85-attempted-serious-cyber-attacks-a-year-and-one-third-are-successful) によると、過去 12 ヶ月間にこれらの銀行は平均で 85 件の重大なサイバー対策に対する攻撃を受けており、このうち 36%は何らかのデータを盗むことに成功しています。貴委員会の規則案に従って算出した場合、貴委員会と本人は、金融セクターからだけでも 2 万 3000 件を超える報告や通知を受領していたことになり、そのうち約 1 万 5000 件は、データの盗取に至らなかったと最終的に判断された事案です。</p> <p>報告の概算数を金融セクター以外にも広げ、別の調査</p> <p>(https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf) にも目を向けてみましょう。</p> <p>11 ヶ国（オーストラリア、ブラジル、カナダ、フランス、ドイツ、イタリア、日本、シンガポール、スペイン、英国、米国）の様々なセクターの企業 355 社を対象に実施されたこの調査では、幅広い業種を代表する組織が、2018 年に、それぞれ平均で 145 件の漏えい等を経験していたことが明らかになりました。個人の権利利益を害す</p>	

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>るおそれが大きい実際の漏えい等が発生した場合又は発生したおそれがある場合はこれらのうちの半分か三分の一程度にすぎないと仮定したとしても、組織毎に義務付けられる報告件数を対象組織の数で乗じた数字は膨大です。</p> <p>GPA の意見 貴委員会の規則案は、改正法で定める報告基準を超えて報告要件を大幅に拡大するものだと考えます。改正法第29条の4第1項は、個人の権利利益を害するおそれが大きい場合に、特に貴委員会への報告を義務付けています。セキュリティインシデントの可能性が実際のデータ漏えい等と確認されるまでは、影響を受ける本人の範囲を特定し、これらの者に対するリスクの潜在的度合いを正確に評価することは不可能です。漏えい等が発生したおそれがある場合にまで組織に報告を義務付けることは、組織によって対応方法が大幅に異なる可能性が高い理論上の取り組みとなり、有益ではないと考えられます。</p> <p>漏えい等が発生した場合に、本人に通知を求めることの主たる目的は、漏えい等発生時のなりすましや不正行為のリスクを個人が低減できるようにすることです。一方、行政当局へ報告を求めることの主な目的は、当該当局が監督機能を発揮できるようにすることにあります。例えば、持続的な又はシステム上のセキュリティの問題を特定する、問題へ対処するため必要な措置を講じる、漏えい等によ</p>	

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>り被害を被る可能性がある個人を支援するといったことがこれに当たります。こうした目的をふまえると、漏えい等が発生したおそれはあるが、まだその発生が確認できていない段階で、行政当局や個人に報告や通知を求めることは、理にかないません。サイバーセキュリティ攻撃の規模に鑑みると、漏えい等の発生のおそれに関する報告が貴委員会に殺到し、それにより組織や貴委員会の貴重なリソースが奪われ、個人の権利利益を害するおそれが大きい実際のデータ漏えい等に対する取り組みがおろそかになる可能性があります。同様に、漏えい等が発生したおそれがある場合にまで個人に通知をすれば、実際のリスクには関係のない数々の通知で個人を圧倒するという逆効果を招くことは必至です。結果として、不必要な恐怖と混乱を招くだけでなく、人々を鈍感にさせ、重大リスクの発生時に被害から自らを守るために必要な対策を示した通知そのものが無視される事態にもなりかねません。さらに、「発生したおそれ」の基準が不明確であるため、多くの企業は慎重を期すあまり過剰に報告を行う可能性があります。こうした過剰な報告により、実際の持続的な又はシステム上のセキュリティの問題の所在が希薄化されたり、特定が困難になったりすることも考えられます。</p> <p>最後に、GPA は、番号法の基準と個人情報保護法の基準との一貫性をもたせるために、漏えい等報告の基準を百人から千人に引き上げることを提言いたします。百人という基準は、漏えい等報告を求め</p>	

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>る世界各国の多くの法令で用いられる基準をはるかに下回るものです。</p> <p>【Global Privacy Alliance】</p>	
6	別記様式	<p>規則案 別記様式</p> <p>報告事項欄における「事態の概要」において、「発生事案」の種別として「漏えいのおそれ」等と記載されている。規則案6条の2等の趣旨を踏まえると、報告対象はアクシデント関連（漏えいが発生した、又は発生したおそれがある事態）であり、インシデント関連（漏えいが発生する予兆・脅威を感知した事態等）は含まれないと思われるが、この表現だと誤読される可能性があるため、様式上も「漏えいしたおそれ」等としたほうが良いのではないかと。</p> <p>また、「事務連絡者の氏名」欄における「電話」であるが、後記されている「記載要領」によれば直通番号を記載するよう指示しているが、緊急時の迅速な報告を必要とする様式という性質を踏まえれば、「電話（直通）」といった欄を設ければ誤記載が少ないと考えられる。その場合、「記載要領」において、直通番号の記載させる意図や取扱い（個人情報保護委員会が直接電話する、事業所管大臣からも直接連絡される場合がある等）を明記した方が良いのではないかと。</p> <p>なお、個人の権利利益を害する「おそれ」があつてそれが大きい場合の「おそれ」と、漏えい、滅失若しくは毀損が発生した「おそ</p>	<p>本規則案別記様式による報告は、本規則案第2条の規定を踏まえて行われるものであり、一般的に現状の案で御理解いただけるものと考えます。</p> <p>記載要領において直通電話番号である旨記載しており、一般的に現状の案で御理解いただけるものと考えます。</p> <p>本規則案第2条の「おそれ」の具体例等については、ガイドライン等でお示しすることを検討してまいります。</p>

番号	該当箇所	寄せられた御意見等	御意見等に対する考え方
		<p>れ」がある事態における「おそれ」は異なるものであるため、何の「おそれ」が生じたどの段階で、本人への通知等が求められるのか、事業者に正しく理解されるように、今後ガイドライン等において明確にされたい。</p> <p>【東京都 生活文化局広報広聴部情報公開課】</p>	
7	別記様式	<p>別記様式 記載要領 用紙の大きさは「日本産業規格 A4 とすること」とあるが、「A 列 4 番」ではないか。</p> <p>【匿名】</p>	一般的に現状の案で御理解いただけるものと考えます。

※上記意見のほか、本規則案の内容とは関係がないと考えられる御意見が1件（1名）ありました。御意見ありがとうございました。