

「事業者における特定個人情報の漏えい事案等が発生した場合の対応についての一部を改正する件（告示案）」に関する意見募集の結果について（案）

平成29年 月 日  
個人情報保護委員会事務局

個人情報保護委員会においては、本年2月22日（水）から3月23日（木）まで「事業者における特定個人情報の漏えい事案等が発生した場合の対応についての一部を改正する件（告示案）」につきまして、広く国民の皆様からの御意見を募集しました。

その結果、この意見募集に対して2の個人から延べ4件の御意見が寄せられ、これら御意見に対する当委員会の考え方について、別紙のとおり取りまとめました。

また、お寄せいただいた御意見を踏まえ、本日、「事業者における特定個人情報の漏えい事案等が発生した場合の対応についての一部を改正する件」を定め、平成29年5月30日から施行することとなりましたのでお知らせします。

御意見をお寄せいただいた皆様に感謝申し上げますとともに、引き続き、当委員会の活動に御理解と御協力をいただきますようお願い申し上げます。

「事業者における特定個人情報の漏えい事案等が発生した場合の対応についての一部を改正する件（告示案）」  
に関する意見募集の結果について

No.	寄せられた御意見等	御意見等に対する考え方
1	<p>個人情報保護委員会への報告を要しない場合について 対象事業者を個人情報取扱事業者以外の事業者から従業員の数が100人以下の事業者に変更するとは従業員が100人以下の事業者でも1件でも個人情報を保有する場合例外なく個人情報取扱事業者に該当するか 従業員が100人以下の事業者が顧客から4000件の個人情報を保有し漏洩した場合に4000件の個人情報の漏えい事故の報告を個人情報保護委員会に報告義務はない 新個人情報保護法の法令が適用され懲罰が適用されるのか 個人情報保護委員会への報告義務ないのに新個人情報保護法上の義務は発生するのか よろしくをお願いします</p>	<p>個人情報保護法の改正により、個人情報データベース等を事業の用に供している者は全て個人情報取扱事業者となります。 なお、前提として、本告示は、事業者における特定個人情報の漏えい事案等が発生した場合の対応について定めたものであり、個人番号を含まない個人情報が漏えい等した場合は、「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）等に従い、対応することになります。 また、個人情報保護委員会への報告を要しない場合について、本告示においては、従業員の数が100人以下の事業者に限定していますが、「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」においては、従業員の数にかかわらず全ての個人情報取扱事業者を対象としており、対象範囲が異なっております。 さらに、例示として記載された事案の「個人情報」が特定個人情報を指すという前提であれば、番号法第28条の4及び「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」（平成27年特定個人情報保護委員会規則第5号）に定める「重大な事態」（以下「重大事態」という。）に該当しますので、事業者は当委員会に報告する義務を負っています。なお、規則及び告示に基づく報告を行わなかった場合、その行為のみに対する直接的な罰則はありませんが、番号法所定の罰則規定に該当する事情が生じた場合、罰則を科せられる可能性があります。</p>

No.	寄せられた御意見等	御意見等に対する考え方
2	<p>&gt;2. (2). 本文</p> <p>つまり、連絡等をしていない場合は報告がなされ、外部に漏洩していると判断される場合は報告がなされ、事実関係の調査が不十分に行なえない場合や何らかの事情で再発防止策を決定していない場合は報告がなされ、重大事態である場合は報告がなされる、という事になると思われるのであるが、しかしこれだけでは不適切なのではないかと当方は考える。</p> <p>後に記す 2. (2). O2 についての内容についての懸念もあるが、これでは従業員の数が 100 人以下である、いわゆる名簿会社や、ソーシャルゲーム等を運営する会社等が定義から漏れてしまう事になってしまう事になるので（これらの会社は通常、数万から数百万といった数の個人情報を取得し事業の用に供しているのである。）、従前と同様の、いわゆる「5000 人要件」も併せ行なっていただきたいと考える。</p> <p>（でない、はっきり言うと、以前の方がまだましな定義であると考え。数多くあるこのような会社における問題事態が報告を要しないとなる事は国家として問題なレベルでの悪影響を国民に及ぼす事必至である。5000 人より多い個人情報を保有する会社については、やはり従前と同様に、報告を要する対象としておくべきであると考え。）”</p>	<p>番号法上、事業者が特定個人情報等を取り扱えるのは個人番号利用事務又は個人番号関係事務の場合だけであり、名簿会社やソーシャルゲーム等を運営する会社等であれば、通常、従業員及びその家族の特定個人情報等以外の者の特定個人情報等を取り扱うことは番号法上できないことから、現状の案のとおりとします。</p>
3	<p>&gt;2. (2). O2</p> <p>この「実質的に外部に漏えいしていないと判断される場合」については注意を要すると考える。</p> <p>近年（2013 年以降）では、量子コンピュータが実用化されていると言って良い状況であると思われるのであるが（多量の量子コンピュータが商用含めて既に用いられているし、1 台で使用可能な量子ビットも増大している。2048Qbit の量子コンピュータが商用に供されている今日現在において、これによる解読を行なわれる事は現実的危機である。）、この状況下では、「暗号化されたデータの漏洩」は「実質的に外部に漏洩していないと判断される場合」に含まれないと考えられるものである（この事については国全体で意識を変えていただきたい。少し前に、「ハードディスクを暗号化していれば、盗まれてもそのまま廃棄しても平気」などという事を言う不届き者がいたが、それらの者は他国作業員もしくはその息がかかった者である可能性が大きい。量子コンピュータの存在を見ない振りしようとする行政職員も同様である。）。現状、国や社会一般は、（作られた風潮によって）暗号化されたデータであれば漏洩しても実質的に漏洩していないと見なしているのであるが、その定義は通用しないと見ていただきたい。</p> <p>よって、この定義については、通知等で、多くの場合が実質的に外部に漏洩した事になると示す事によって、認識を改めていただきたいと思う。”</p>	<p>「外部に漏えいしていないと判断される場合」については、一時的に不特定多数の者が閲覧することができる状態にあったが、直ぐに回収等を行ったため、第三者に閲覧されなかったことが確認できた場合等も想定しており、今回、その趣旨がより明確になるよう、「実質的に」という文言を追加しております。</p>

No.	寄せられた御意見等	御意見等に対する考え方
4	<p>&gt;2. (2). ○3  有期の期限設定があるのが望ましいのではないかと思われる（永遠に調査中、などという口実によって報告を行なうべき事態であるにも関わらずこれを行なわない事している場合。30日以内、といったあたりであると適切であると考え。）。</p> <p>また、再発防止策についての定義についても記述が必要であると考え（「起きないようにします」という文言だけでは当然駄目である。）。また、1と合わせてその連絡等を行なわせるようにすべきであると考え。”</p>	<p>事案の内容等により、再発防止策の決定に要する期間、再発防止策の内容は異なるものと考えられるため、一律に期間、定義を定めておりません。</p> <p>なお、重大事態の場合は、事業者は、再発防止策の決定の有無にかかわらず、事案が発覚した時点で、直ちにその旨を報告するよう努めることとしております。また、再発防止策について、適切な対応がなされないことが確認された場合は、指導等を行うこととなります。</p> <p>以上のことから、現状の案のとおりとします。</p>

※ 個人情報保護法：個人情報の保護に関する法律（平成15年法律第57号）

※ 番号法：行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）