資料2－2

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
（案）

特定個人情報保護委員会においては、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（平成 26 年特定個人情報保護委員会告示第５号。以下「ガイドライン」という。）を平成 26 年 12 月 11 日に策定・公表した。

ガイドラインの「第３－６　特定個人情報の漏えい事案等が発生した場合の対応」において、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は、別に定めることとしていたが、事業者における特定個人情報の漏えい事案その他の「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。以下「番号法」という。）違反の事案又は番号法違反のおそれのある事案が発覚した場合の対応について、次のとおり定める。なお、ガイドラインで用いられている用語については、その例による。

１．事業者は、その取り扱う特定個人情報（委託を受けた者が取り扱うものを含む。以下同じ。）について、漏えい事案その他の番号法違反の事案又は番号法違反のおそれのある事案が発覚した場合には、次の事項について必要な措置を講ずることが望ましい。

(1) 事業者内部における報告、被害の拡大防止
　責任ある立場の者に直ちに報告するとともに、被害の拡大を防止する。

(2) 事実関係の調査、原因の究明
　事実関係を調査し、番号法違反又は番号法違反のおそれが把握できた場合には、その原因の究明を行う。

(3) 影響範囲の特定
　(2)で把握した事実関係による影響の範囲を特定する。

(4) 再発防止策の検討・実施
　(2)で究明した原因を踏まえ、再発防止策を検討し、速やかに実施する。

(5) 影響を受ける可能性のある本人への連絡等
　事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係等について、速やかに、本人へ連絡し、又は本人が容易に知り得る状態に置く。

(6) 事実関係、再発防止策等の公表
　事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係及び再発防止策等について、速やかに公表する。

２．事業者は、その取り扱う特定個人情報に関する番号法違反の事案又は番号法違反のおそれのある事案を把握した場合には、事実関係及び再発防止策等について、次のとおり報告するよう努める。

(1) 報告の方法

ア　個人番号又は特定個人情報の漏えいなど主務大臣のガイドライン等において報告対象となる事案の場合

事業者が個人情報取扱事業者（注１）に当たる場合、当該事業者は主務大臣のガイドライン等の規定に従って報告する。この場合、報告を受けた主務大臣等（注２）又は主務大臣のガイドライン等に従い主務大臣等への報告に代えて報告を受けた「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 37 条第１項に規定する認定個人情報保護団体は、特定個人情報保護委員会にその旨通知する。

なお、これらの場合、主務大臣等の求めにより個人情報取扱事業者が直接特定個人情報保護委員会へ報告しても差し支えない。

（注１）個人情報取扱事業者以外の事業者が主務大臣のガイドライン等の規定に従う場合には、当該事業者を含む。

（注２）主務大臣のガイドライン等に報告先として規定されている個人情報保護法第 51 条、「個人情報の保護に関する法律施行令」（平成 15 年政令第 507 号）第 11 条の規定により事務を処理する地方公共団体の長等を含む。

イ　個人情報取扱事業者以外の事業者又は主務大臣が明らかでない個人情報取扱事業者における個人番号又は特定個人情報の漏えいなどの事案であって、報告する主務大臣等を直ちに特定できない場合

特定個人情報保護委員会に報告する。

ウ　その他、個人番号の利用制限違反など番号法固有の規定に関する事案等の場合

特定個人情報保護委員会に報告する。

(2) 報告の時期

ア　(1)アについては、主務大臣のガイドライン等の規定に従い、(1)イ及びウについては、速やかに報告するよう努める。

イ　アにかかわらず、特定個人情報に関する重大事案（注）又はそのおそれのある事案が発覚した時点で、直ちにその旨を特定個人情報保護委員会に報告する。その後、事実関係及び再発防止策等について、(1)に従い報告する。

（注）「重大事案」とは、①情報提供等事務を実施する者の情報提供ネットワークシステムから外部に情報漏えい等があった場合（不正ア

クセス又は不正プログラムによるものを含む。)、②事案における特定個人情報の本人の数が 101 人以上である場合、③不特定多数の人が閲覧できる状態になった場合、④従業員等が不正の目的で持ち出したり利用したりした場合、⑤その他事業者において重大事案と判断される場合を指す。

(3) 特定個人情報保護委員会への報告を要しない場合

個人情報取扱事業者以外の事業者にあっては、次の全てに当てはまる場合は、特定個人情報保護委員会への報告を要しない。

①影響を受ける可能性のある本人全てに連絡した場合（本人への連絡が困難な場合には、本人が容易に知り得る状態に置くことを含む。）

②外部に漏えいしていないと判断される場合

③従業員等が不正の目的で持ち出したり利用したりした事案ではない場合

④事実関係の調査を了し、再発防止策を決定している場合

⑤事案における特定個人情報の本人の数が 100 人以下の場合