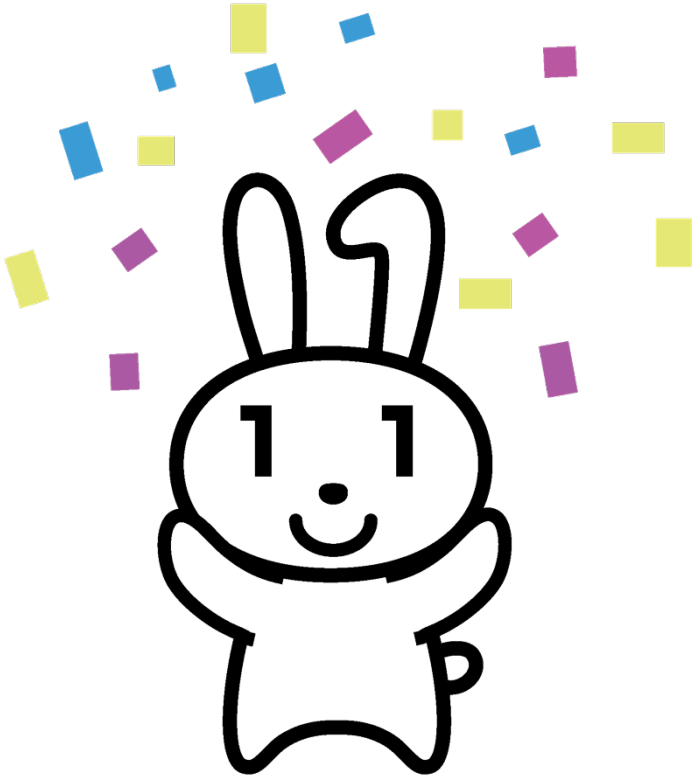
資料１－２

特定個人情報の取扱いに関する留意点について

個人情報保護委員会事務局　平成29年1月

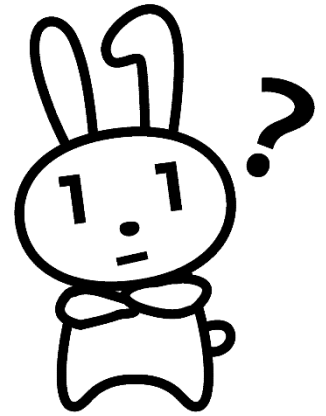
目次



はじめに

平成
25年　5月　「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」（**番号法**）　制定
26年　1月　特定個人情報保護委員会　設置
27年　9月　改正個人情報保護法　公布
27年10月　マイナンバー通知開始
28年　1月　マイナンバーの利用開始　マイナンバーカードの交付
　　個人情報保護委員会に改組

突然ですが、この数字何かわかりますか？



①26年　7月	2895万件
②27年　5月	125万件
③28年12月	42万件

（注）公表、報道ベース

④27年度	83件
⑤28年度（上半期）	66件

答え

（個人情報）

①26年　7月　　2895万件⇒　民間企業

②27年　5月　　125万件⇒　独立行政法人等

③28年12月　　42万件⇒　民間企業

⇒漏えいするなどした個人情報の件数

（特定個人情報）

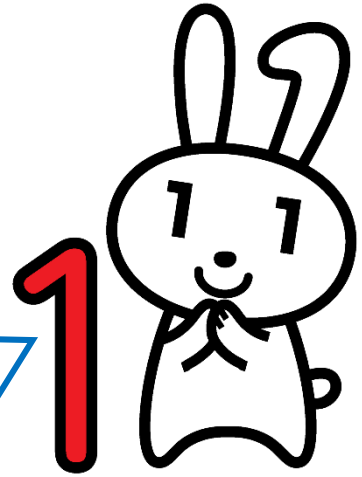
④27年度　　83件（重大な事態2件）

⑤28年度（上半期）　66件（重大な事態2件）

⇒個人情報保護委員会に報告された漏えい事案等の件数

漏えいしてしまうと、
信用が失墜し、市民の不安を招くだけでなく
①謝罪
②コールセンターの設置
③マスコミ対応
④訴訟？システムの利用停止？
など様々な対応を求められ、多大なコストを強いられることになります。

特定個人情報等の取扱いには十分注意してください！！



立入検査の状況

27年度　行政機関1機関　地方公共団体1機関　2件

28年度（上半期）　行政機関3機関　地方公共団体1機関　4件

28年度検査計画　行政機関5件　地方公共団体5件

番号法

（報告及び立入検査）

第38条　委員会は、この法律の施行に必要な限度において、特定個人情報を取り扱う者その他の関係者に対し、特定個人情報の取扱いに関し、必要な報告若しくは資料の提出を求め、又はその職員に、当該特定個人情報を取り扱う者その他の関係者の事務所その他必要な場所に立ち入らせ、特定個人情報の取扱いに関し質問させ、若しくは帳簿書類その他の物件を検査させることができる。（略）

（委員会による検査等）

第28条の3　特定個人情報ファイルを保有する行政機関、独立行政法人等及び機構は、個人情報保護委員会規則で定めるところにより、定期的に、当該特定個人情報ファイルに記録された特定個人情報の取扱いの状況について委員会による検査を受けるものとする。

2　特定個人情報ファイルを保有する地方公共団体及び地方独立行政法人は、個人情報保護委員会規則で定めるところにより、定期的に、委員会に対して当該特定個人情報ファイルに記録された特定個人情報の取扱いの状況について報告するものとする。

※漏えい事案等を踏まえて、随時に検査を行うことがあります。

立入検査は、どのような観点で行うのか？

Point①　規程が適切に定められているか。

- 特定個人情報保護評価書（PIA）や特定個人情報の適正な取扱いに関するガイドラインに沿って規程が定められているか。

Point②　地方公共団体が定めた規程や、上記のPIA、ガイドラインに基づいて、実施（運用）されているか。

⇒検査に当たっては、客観的な証拠に基づいて説明できているかという観点で検査を行いますので、客観的な証拠として記録を残すことも重要です。

例：入退室の記録、廃棄の記録、アクセスログ、研修実施の記録　など

特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）より抜粋

２　講ずべき安全管理措置の内容

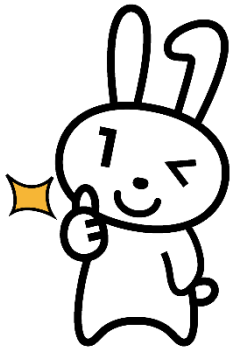
地方公共団体等は、安全管理措置を講ずるに当たり、番号法、個人情報保護条例、本ガイドライン、指針等及び地方公共団体における情報セキュリティポリシーに関するガイドライン等を参考に地方公共団体等において策定した情報セキュリティポリシー等を遵守することを前提とする。

事例1　事務の範囲及び事務取扱担当者

A事業主体は、特定個人情報の取扱いに関する規程を定め、事務分掌表に基づき、個人番号を取り扱う事務に従事する職員を事務取扱担当者として定めている。

しかしながら、総務課の非常勤職員が、特定個人情報が記載されている申請書・届出書等を含む郵便物を開封し、内容を確認して担当者に配布しているにもかかわらず、当該事務及び当該者を、特定個人情報の取扱事務及び事務取扱担当者に指定していなかった。また、市民課の臨時職員が、マイナンバーカードの申請及び交付の事務に携わっているにもかかわらず、当該事務及び当該者を、特定個人情報の取扱事務及び事務取扱担当者に指定していなかった。

Point!! 事務の範囲及び事務取扱担当者



① 規程を整備しているか。

② 個人番号を取り扱う事務の範囲を明確にしているか。

- 範囲：郵便物の開封・配布業務、マイナンバーカード交付業務なども事務の範囲に含めているか。

③ 特定個人情報等の範囲を明確にしているか。

④ 事務取扱担当者を明確にしているか。

- 対象者：非常勤職員、臨時職員、監査担当者も対象に含めているか。

Q. なぜ事務の範囲、事務の取扱担当者を明確にしなければならないのか？

A. ①他の事務や関係のない者に個人番号を利用させないようにするため、②人的安全管理措置等の安全管理措置を適切に織り込むため、③事務の責任を明確にするためなどが挙げられます。また、特定個人情報の漏えい等の事案が発生した場合、どこから、どのように漏えいしたのかなど原因を究明できないおそれがあるため、明確にする必要があります。

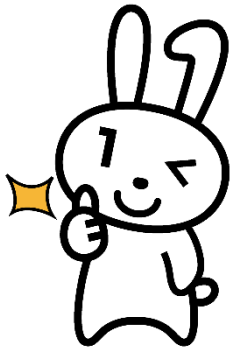
事例2　研修

A事業主体は、特定個人情報の取扱いに関する規程を定めている。そして、同規程において、責任者は所属する職員等に対して、教育研修を定期的に行うこととされている。

A事業主体は、職員500名を対象に「マイナンバー制度研修」を実施したが、500名のうち100名が出張や会議等のため欠席していた。そして、出席者は欠席者に対して、伝達研修等を実施することになっていたにもかかわらず、伝達研修等を実施せず、欠席者に対するフォローアップを実施していなかった。

また、新人職員や人事異動後の職員に対して、どのように研修を行うのかについても明確になっていなかった。

Point!! 研修



① 規程を整備しているか。（何のため、誰が、誰に）

- 目的：注意喚起（意識改革）、周知徹底、スキルの向上など
- 実施者：研修責任者、人事担当者など
- 対象者：事務取扱担当者、情報システムの管理に関する事務に従事する職員、保護責任者など

② 研修計画を立てているか。（いつ、どこで、どのように）

- 時期：例えば「定期的に」と規定している場合は、頻度、具体的な実施時期
- 方法：研修形式、実習形式、eラーニングなど

③ 出席者、欠席者の記録を取っているか。

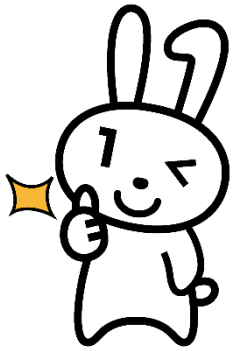
- 記録：名簿、報告書、アンケート、テストなど

④ 未受講者（欠席者、人事異動後の者、新規採用者等）への研修を実施しているか。

⑤ 未受講者に対して研修を実施した場合、記録を取っているか。

※中央で集合研修を実施し、集合研修の参加者が、支部等で伝達研修等を行うこととしている場合、適切な伝達研修等の実施の確保のために、どのような者を集合研修に参加させるかについて留意が必要です。

Point!! 研修



Q. なぜ研修をしなければならないのか？

A. 関係規程が適切に整備されているとしても、その内容が事務取扱担当者等に認知されていなければ当該規定が遵守されないことになりますので、適切な教育（研修等）を実施することが重要です。また、地方公共団体等の特徴として、他部署への人事異動により、異動後に初めて特定個人情報を取り扱う場合もありますので、研修を効果的に活用してください。

なお、研修は下記のとおり、法令において定められています。

番号法

（研修の実施）

第28条の2　行政機関の長等は、特定個人情報ファイルを保有し、又は保有しようとするときは、特定個人情報ファイルを取り扱う事務に従事する者に対して、政令で定めるところにより、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティ（サイバーセキュリティ基本法（平成26年法律第104号）第2条に規定するサイバーセキュリティをいう。第35条の2において同じ。）の確保に関する事項その他の事項に関する研修を行うものとする。

番号法　政令

（研修の実施方法）

第30条の2　法第28条の2の規定による研修の実施は、次に掲げるところによるものとする。

一　研修の計画をあらかじめ策定し、これに沿ったものとすること。

二　研修の内容は、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティの確保に関する事項として、情報システムに対する不正な活動その他のサイバーセキュリティに対する脅威及び当該脅威による被害の発生又は拡大を防止するため必要な措置に関するものを含むものとすること。

三　特定個人情報ファイルを取り扱う事務に従事する者の全てに対して、おおむね一年ごとに研修を受けさせるものとすること。

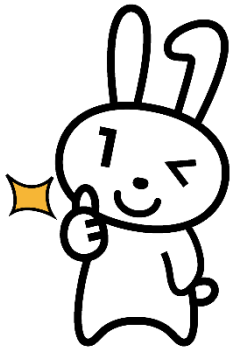
事例３　機器等の持込制限

A事業主体は、セキュリティポリシーを定めている。

しかしながら、当該セキュリティーポリシーにおいて、特定個人情報ファイルを取り扱う情報システムを管理する区域（管理区域）に持ち込む機器等の制限等の措置を講ずる規定が定められていなかった。

そして、管理区域としているサーバ室に入室する職員等は、USBメモリ等の機器を持ち込むことが可能となっており、職員等の不正による特定個人情報の漏えいリスクを抱えている状況となっていた。

Point!! 機器等の持込制限



① 規程を整備しているか。

② 取扱区域（特定個人情報等を取り扱う事務を実施する区域）を定めているか。

③ 管理区域（特定個人情報ファイルを取り扱う情報システムを管理する区域）を定めているか。

④ 管理区域について、入退室管理をしているか。

⑤ 管理区域への機器等の持ち込みを制限しているか。また、機器等の範囲を適切に設定しているか。

（参考）企業の個人情報の流出

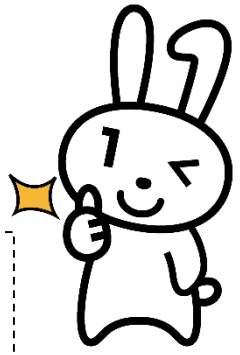
PC内のデータを外部メディアへ書き出すことについて、書き出しを制御するシステムを採用していたが、特定の新機種のスマートフォンを含む一部のメディアに対して、システムが機能しなかった。

事例４　アクセス制御

A事業主体において、システムの利用者に係るユーザー情報の登録又は変更については、システム運用管理要領に基づき、人事異動等により個人番号を取り扱う職員に変更が生じる場合には、速やかに「ユーザー情報登録・変更申請書」をアクセス権限を管理しているB課に提出し、個人番号事務権限等の付与又は削除を行うこととしている。

しかしながら、C課において、人事異動により個人番号を取り扱う事務を行わないこととなった職員の「ユーザー情報登録・変更申請書」をB課に提出していなかったことから、当該職員の個人番号事務権限が削除されていなかった。

Point!! アクセス制御



① 規程を整備しているか。

② 適切なアクセス権限を適切な者に付与しているか。

- システム、ファイルなどの使用について、対象者を限定しているか。
- 操作（印刷の設定、画面コピー、文字の加工など）の範囲を限定しているか。

③ アクセス権限について、特に権限を削除することを忘れていないか。

※人事異動等に際しては、人事異動等の手続にアクセス権限の登録、変更、削除に係る事項を盛り込むなど、人事部門とシステム部門で連携を図ることも有効です。

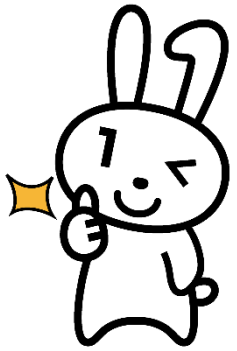
事例５　アクセスログ

A事業主体において、特定個人情報ファイルへのアクセス記録の確認については、事務処理手引に基づき、管理者は特定個人情報ファイルへのアクセス記録を定期的に確認することとし、さらに管理規程に基づき、監査責任者は、定期的にアクセス記録の確認が行われているか否かを監査することとしている。

アクセス記録の確認の頻度については、事務処理手引において定められていないことから、管理者の判断によって実施されている状況であった。そのため、確認の頻度にばらつきがある状況となっていた。

また、アクセス記録の確認方法についても、管理者が特定個人情報ファイルへのアクセス記録を画面閲覧にて確認するにとどまり、確認結果を記録していなかったことから、監査責任者はアクセス記録の確認状況を監査できない状況となっていた。

Point!! アクセスログ



① 規程を整備しているか。

※アクセスログを確認していることを周知することにより、内部へのけん制効果が働きます。

※ログの保管はできる限り行いましょう。

② 確認方法（いつ、誰が、何を）を定めているか。

- 時期：例えば「定期的に」と規定している場合は、頻度、具体的な実施時期
- 確認者：監査責任者、保護責任者、外部委託など
- 確認するログ：業務アプリケーションログなど

③ 確認記録を取っているか。

事例６－１　その他

自己点検の具体的な計画、実施方法、報告方法が定められておらず、自己点検が実施されていなかった。

監査の具体的な計画、実施方法が定められておらず、監査が実施されていなかった。

特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）より抜粋

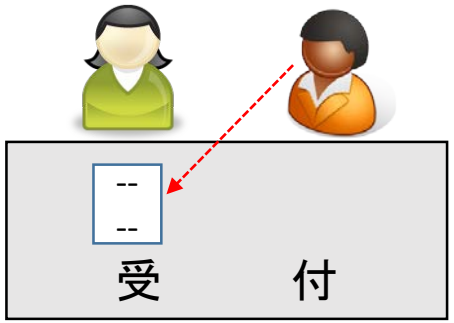
Ｃ　組織的安全管理措置

ｅ　取扱状況の把握及び安全管理措置の見直し

監査責任者（地方公共団体等においては相当する者）は、特定個人情報の管理の状況について、定期に及び必要に応じ随時に点検又は監査（外部監査を含む。）を行い、その結果を総括責任者（地方公共団体等においては相当する者。以下同じ。）に報告する。

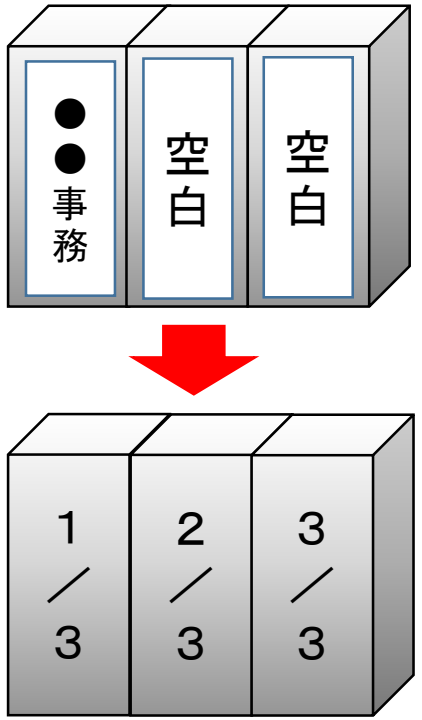
総括責任者は、点検又は監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。

事例６－２　その他



受付窓口において、つい立てがなかったり、つい立ての高さが十分でなかったりしたため、隣の申請者のマイナンバーを見ることができる状況になっていた。

特定個人情報を含む簿冊（ファイル）の管理において、簿冊を管理する記録がなく、かつ、簿冊の背表紙に番号等が振られていなかった。



事例7－1　補足（業務継続）

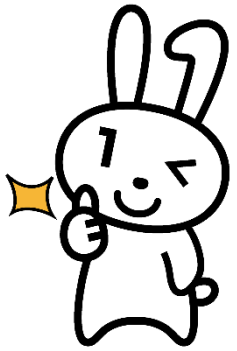
A事業主体は、統合端末に係るバックアップの取得について規程を定め、当該規程に基づいて、担当者は、サーバ室内に設置してある統合端末のバックアップを行っている。

情報資産の保管については、セキュリティ対策基準等において、特定個人情報を記録した記録媒体は、鍵のかかる書庫等に適切に保管しなければならないと規定されているため、バックアップが記録されている記録媒体は、鍵のかかるラックの中にサーバとともに保管され、「バックアップ用記録媒体管理台帳」に記載して管理されていた。

しかしながら、入退室状況を確認したところ、同サーバ室の管理区域には、外部委託業者を含む職員等が入室できることとなっていた。そして、当該ラックの施錠状況を確認したところ、前扉は施錠されていたが後扉は施錠されていなかった。

なお、サーバのバックアップが記録されている媒体を同サーバと同一の場所に保管する場合、災害や漏電、漏水等の事故により、媒体及びサーバの双方が滅失、毀損するおそれがあるため、別の場所に保管するなどの適切な対応が必要である。

Check！ 補足（業務継続）



サーバのバックアップを記録している外部記録媒体が同サーバと同一の場所に保管されており、災害等により双方に被害が及んだ際には、特定個人情報の滅失又は毀損につながるおそれがあることから、業務継続の問題について提起しています。

マイナンバーは災害時にも活用されるため、業務の継続を考えた上で、バックアップされたデータの保管場所等を検討する必要があります。

（参考）「市町村のための業務継続計画作成ガイド（内閣府（防災担当））」より抜粋

4．業務継続計画の特に重要な6要素

業務継続計画の中核となり、その策定に当たって必ず定めるべき特に重要な要素として以下の6要素がある。

(5) 重要な行政データのバックアップ

業務の遂行に必要となる重要な行政データのバックアップを確保する。

・災害時の被災者支援や住民対応にも、行政データが不可欠。

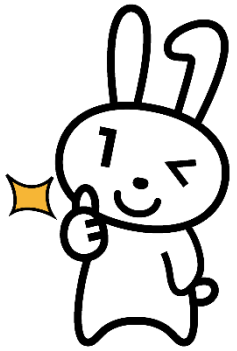
事例7－2　補足（個人情報）

A事業主体は、情報セキュリティ規程において、サーバを収納するラックを常に施錠し、その鍵を厳重に管理することとしている。

A事業主体は、特定個人情報ファイルを取り扱うシステム用のサーバと、個人情報を取り扱うサーバを、それぞれラック内に収納し、その2つのラックを並べて、施錠された部屋の中に設置していた。

しかしながら、個人情報を取り扱うサーバを収納したラックの背面パネルが外されており、一部機器はラック外に置かれ、機器類への接触が可能な状況であった。

Check！ 補足（個人情報）



特定個人情報のサーバではなくとも、同様の取扱いをすることとされている個人情報のサーバについても適切に取り扱う必要があります。

番号法

（指導及び助言）

第36条　委員会は、この法律の施行に必要な限度において、個人番号利用事務等実施者に対し、特定個人情報の取扱いに関し、必要な指導及び助言をすることができる。この場合において、特定個人情報の適正な取扱いを確保するために必要があると認めるときは、当該特定個人情報と共に管理されている特定個人情報以外の個人情報の取扱いに関し、併せて指導及び助言をすることができる。

漏えい事案等

漏えい事案等の報告件数

27年度	83件
28年度（上半期）	66件

多くの漏えい事案等は、個人番号が記載された書類（住民票や通知カードなど）を誤って別の者に渡したなどの誤交付によるものです。

また、ほとんどが紙媒体による漏えい事案等です。

事例①

戸籍課の受付窓口において、転出希望者Aと、転出希望者Bの２人から同時間帯に転出届が提出された。

戸籍課の職員CはAの転出証明書、職員DはBの転出証明書を処理していた。そして、職員Cと職員Dは、課内の同じプリンタから、転出証明書を出力した。

この時、職員Cは、誤ってAとB両者の転出証明書を綴じ合わせ、それをAに交付した。

そして、職員Dは、Bの転出証明書が出力されていなかったと誤認して、再度出力して、Bに転出証明書を提出した。

その後、転入先の職員が、Aの転入届けを処理する際に、別の者の転出証明書が綴じられているのを発見した。

事例②

A市において、特定個人情報を含むファイルの送信に当たり、メールを送ってきた担当者だけにメールを返信するべきところを、メール機能の「全員に返信」を選択したことにより、メールを送ってきた担当者だけではなく、他市の担当者にも特定個人情報を含むファイルを送信してしまった。

その後、他市の担当者から電話により、誤送信のメールが届いている旨の連絡があり、漏えい事案が発覚した。

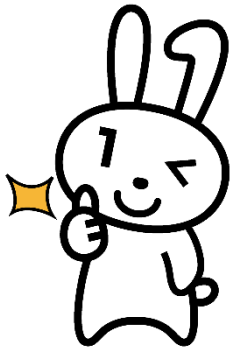
※外部の者にメールを送信する場合や、多くの者にメールを送信する場合には、メールのシステムに、一定の制限を組み込むことも有効です。

事例③

委託先の担当者が、システムに記録されていた職員の情報（特定個人情報を含む。）を誤って削除した。システムの作業ログを調査したところ、職員情報が誤って初期化されていた事が判明した。

市役所において、児童の申請書を受理し、都道府県知事へ進達を行う事務において、本来は児童の個人番号のみを記載すればよいのに、誤って保護者の個人番号が記載されたものを進達してしまった。

Point!! 漏えい事案等の報告



【報告】

独立行政法人等及び地方公共団体等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

（平成27年特定個人情報保護委員会告示第1号）

独立行政法人等及び地方公共団体等は、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ものとする。

（略）

7　個人情報保護委員会への報告

独立行政法人等及び地方公共団体等は、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、速やかに個人情報保護委員会に報告する。

（略）

また、独立行政法人等及び地方公共団体等は、重大事態に該当する事案又はそのおそれのある事案が発覚した時点で、直ちにその旨を個人情報保護委員会に報告する。

※重大事態又はそのおそれのある事案が発覚した時点で、直ちに個人情報保護委員会へ報告してください。（第一報）

最後に

漏えい事案等はいつ起こるかわかりません。

- 漏えい事案等を起こさないために、安全管理措置について、適切な規程の整備、適切な実施、さらに、規程等の見直しを行うことが重要です。
- 漏えい事案等に備えて、体制及び手順等を整備することが重要です。

※体制及び手順等を整備するに当たっては、手順等が複雑になりすぎると、現場では手順等が遵守されなくなるおそれがあるため、効率的な手順等の整備を図ることが重要です。

御清聴ありがとうございました。