個人情報保護委員会
Personal Information Protection Commission

個人情報の適正な取扱いのための研修資料

令和５年２月

個人情報保護委員会事務局

監視・監督室

（令和5年5月　豊島区政策経営部区民相談課抜粋編集）

報告３

目次

はじめに

本研修資料は、個人情報の取扱いに従事する職員、保護担当者、保護管理者及び総括保護管理者を対象とした個人情報保護委員会が作成した研修資料を基に作成したもので、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置に関する内容を中心に作成されています。

区民相談課で作成した「個人情報保護事務の手引き」（以下、「手引き」という。）と本研修資料等をよく理解することで、より適正に保有個人情報が取り扱われることが期待されています。

第１章
個人情報保護法の基礎

なぜ、個人情報の適正な取扱いの確保が必要か？

個人情報保護法の第一の目的
個人の権利利益の保護
＝国民・住民の権利利益を守ること

例えば個人情報が本人の知らないところで使われていると…

秘密にしたい個人情報の拡散
→人格的権利利益の侵害

個人情報が詐欺に使われた
→財産的権利利益の侵害

国民・住民の信頼の確保
↓
行政運営・業務運営の円滑化

例えば公的機関から個人情報が漏えいすると…

長による謝罪会見の実施等
国民・住民への説明が必要

不信感をもった国民・住民が
非協力的に

支える

重要

個人情報の適正な取扱いの確保の為の取り組み

（職員一人一人）
個人の権利利益を侵害するリスクを認識し、抑制

（組織全体の）
リスク管理

なぜ、個人情報の適正な取扱いの確保が必要か？

＜国民・住民の方々の権利利益の保護＞

国民・住民の方々の個人情報の適正な取扱いを確保し、**個人の権利利益を保護することが個人情報保護法の第一の目的**となります。例えば、国民・住民の方々が他人に知られたくない機微性の高い情報が漏えい等すれば、プライバシー侵害や差別を誘発する可能性があります（**人格的な権利利益の保護**）。 また、国民・住民の方々の連絡先が漏えい等すれば詐欺の端緒となってしまうこともあり得ます （**財産的な権利利益の保護**）。

＜円滑な行政運営の確保＞

参考資料の中で紹介する漏えい等の事例では、報道で大きく取り上げられ、会見で首長が謝罪する事態となったものもあります。個人情報及びプライバシーに関する国民の意識が高まっている中、公的機関である国の行政機関や地方公共団体等において重大な漏えい等事案が発生した場合、当該事例を出すまでもなく、**当該公的機関の信頼を大きく損なうことになり、円滑な行政運営にも支障**が生じます。

他方、**個人情報を取り扱う部署・職員は広範囲に及ぶ**ことから、漏えい等により個人の権利利益を侵害するリスクはあらゆる所に存在します。その大きなリスクをすべての職員が認識し、リスクを抑え、コントロールするために緊張感を持って取り組んでいただく必要があります。**一つの部署の一人の職員が起こした漏えい等が国民・住民の権利利益や組織全体に影響を与えます。一人一人がリスクを管理することが、結果として、組織全体のリスク管理に大きく繋がります。幹部や制度所管部署、取扱部署や現地事務所等、更には委託先・再委託先に至るまで、あらゆる部署・職層の職員一人一人まで浸透を図ることが重要**です。

公的機関には、様々な部署があり、個人情報の適正な取扱いの確保の取組みは、所管する部署以外の職員から見ると、忙しい通常業務に加えて、一見、負担が増えるものでもあり、事務処理の効率性を損なうようにも見えます。また、個人情報の適正な取扱いの確保と並行して、個人情報の利活用についても進めていく必要があります。

それでも、**国民・住民の権利利益の保護のため、個人情報の適正な取扱い確保し、それぞれの業務を進めていただくことを期待します**。

（職員一人一人）
個人の権利利益を侵害する
リスクを認識し、抑制

→

（組織全体の）
リスク管理

- **国民・住民の方々の権利利益の保護**
- **円滑な行政運営、国民・住民からの信頼の確保**

「個人情報保護法」とは

- **「個人情報」の適正な取扱い**に関し、**個人情報の有用性**に配慮しつつ、「プライバシー」を含む**個人の権利利益を保護**することを目的とする法律。
- **我が国の個人情報保護制度の「基本法」**として基本理念、基本方針の策定や国等の責務等を定めるほか、**民間事業者や行政機関等の個人情報の取扱いに関する「一般法」**として**民間部門及び公的部門における必要最小限の規律**を定める。
- また、**個人情報保護委員会の設置根拠**や**民間部門及び公的部門に対する監視・監督権限**についても定める。

「個人情報保護法」とは

構成

第１章　総則	**第５章　行政機関等の義務等**
第２章　国及び地方公共団体の責務等	第６章　個人情報保護委員会
第３章　個人情報の保護に関する施策等	第７章　雑則
第４章　個人情報取扱事業者等の義務等	第８章　罰則

- 国の行政機関、独立行政法人等、地方公共団体の機関及び地方独立行政法人は、原則として**法第５章の規律が適用される**ことから、その職員は法第５章の各規定に基づき個人情報を取り扱う必要がある。

行政機関等が取り扱う個人情報の重要性

国や地方公共団体は民間事業者と異なり、法令等により本人の意思にかかわらず個人情報等を取り扱う権限を有し、また、その業務の性質上多くの国民や住民の情報を取り扱うことがあり得る。
透明性や信頼性の確保の観点からも、適正に個人情報が取り扱われることが重要。

- 地方公共団体の業務の例

住民基本台帳、印鑑登録、住登外管理、戸籍、就学、選挙人名簿管理、
固定資産税、個人住民税、法人住民税、軽自動車税、収滞納管理
国民健康保険、国民年金、介護保険、後期高齢者医療、健康管理
児童手当、生活保護、障害者福祉、財務会計、人事給与、文書管理、こども子育て支援

総務省「地域情報プラットフォーム　標準レイアウト仕様」より引用

- 国の業務の例

各種国家試験、雇用保険、厚生年金、恩給、所得税、相続税　　等

「行政機関等」とは

- **<u>法第５章の規律は以下の「行政機関等」に適用される</u>。職員は、法第５章の各規定に従って個人情報を取り扱う必要がある。**
- **議会には原則として個人情報保護法の適用はない。**

● 「行政機関等」は、次に掲げる機関をいう。（法第２条第11項）

1. 行政機関（法第２条第８項）
2. 独立行政法人等（法第２条第９項・第11項第３号）
   ただし、法別表第２に掲げる法人を除く。
3. 地方公共団体の機関（法第２条第11項第２号）
   ただし、議会を除く。
4. 地方独立行政法人（法第２条第10項・第11項第４号）
   ただし、試験研究等を主たる目的とするもの又は大学等の設置及び管理若しくは病院事業の経営を目的とするものを除く。

公的部門（第５章）の規律の適用対象

	個人情報等の取扱い等に関する規律	個人情報ファイル簿に関する規律	開示・訂正・利用停止等に関する規律	匿名加工情報に関する規律
国の行政機関	公的部門の規律（法第５章第２節）	公的部門の規律（法第５章第３節）	公的部門の規律（法第５章第４節）	公的部門の規律（法第５章第５節）
独立行政法人等	公的部門の規律（法第５章第２節）	公的部門の規律（法第５章第３節）（第75条のみ）		
別表第二に掲げる法人等　※1	民間部門の規律（法第４章）※2			
地方公共団体の機関	公的部門の規律（法第５章第２節）			
病院、診療所、及び大学の運営の業務	民間部門の規律（法第４章）※2			
地方独立行政法人	公的部門の規律（法第５章第２節）			
試験研究等を主たる目的とするもの、大学等の設置・管理及び病院事業の経営を目的とするもの	民間部門の規律（法第４章）※2			

※1　独立行政法人労働者健康安全機構については、病院の運営の業務に限る。
※2　保有個人データに関する事項の公表等（第32条）並びに開示、訂正等及び利用停止等（第33条～第39条）に関する規定及び民間の事業者である匿名加工情報取扱事業者等の義務（第4節）に関する規定は適用されない。また、法令に基づき行う業務であって政令で定めるものを行う場合における個人情報の取扱いについては、民間部門の規律に加えて、行政機関等に対する規律が準用される。
注）別表第二に掲げる法人と、試験研究等を主たる目的とする地方独立行政法人並びに大学等の設置・管理及び病院事業の経営を目的とする地方独立行政法人は「行政機関等」には含まれないが、上記のとおり一部公的部門の規律が適用される。

「個人情報」とは（法第２条第１項関係）

○「個人情報」とは、**生存する個人に関する情報**であって、次の各号のいずれかに該当するものをいう。

一　**当該情報に含まれる氏名、生年月日その他の記述等**（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。以下同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）**により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）**

二　**個人識別符号が含まれるもの**

○「他の情報と容易に照合することができ」るとは、行政機関等の実態に即して個々の事例ごとに判断されるべきであるが、**通常の事務や業務における一般的な方法で、他の情報と容易に照合することができる状態**をいい、例えば、他の行政機関等や事業者への照会を要する場合等であって照合が困難な状態は、一般に、容易に照合することができない状態であると考えられる。

（例）

氏名
山田 太郎

顔写真

住所
（氏名と組み合わせた場合）
東京都●●区▲▲町
山田太郎

生年月日
（氏名と組み合わせた場合）
1980年●月▲日
山田太郎

「個人情報」とは（法第２条第１項関係）

○個人情報に該当するか否かは、行政機関等の実態に即して個々の事例ごとに判断する必要がある。

○以下の情報は、個人情報に該当すると考えられる。

【個人情報に該当する事例】 手引き 1-2-2-1 (P14)

事例1）本人の氏名
事例2）生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報
事例3）防犯カメラに記録された情報等本人が判別できる映像情報
事例4）本人の氏名が含まれる等の理由により、特定の個人を識別できる音声録音情報
事例5）特定の個人を識別することができるメールアドレス（kojin_ichiro@example.com 等のようにメールアドレスだけの情報の場合であっても、example 社に所属するコジンイチロウのメールアドレスであることが分かるような場合等）
事例6）個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できる場合は、その時点で個人情報に該当する。）
事例7）官報、電話帳、職員録、法定開示書類（有価証券報告書等）、新聞、ホームページ、SNS（ソーシャル・ネットワーク・サービス）等で公にされている特定の個人を識別できる情報

○「個人情報」の範囲に**死者に関する情報は含まれない**。ただし、死者に関する情報が、同時に、遺族等の生存する個人を識別することができる場合に限り、当該生存する個人を本人とする個人情報に該当する。

「個人識別符号」とは（法第２条第２項関係）

○「個人識別符号」は以下①②のいずれかに該当するものであり、政令で定めるものをいう。

① **身体的特徴等を電子計算機の用に供するために変換した符号**
② **対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号**

○「個人識別符号」に該当するものは、**その情報単体でも個人情報に該当する。**

（参考）個人識別符号に関する政令・規則の内容 手引き 1-2-2-2 (P15)

① 身体の一部の特徴を電子計算機の用に供するために変換した符号
➔ ＤＮＡ、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋

② サービス利用や書類において対象者ごとに割り振られる符号 ⇒公的な番号
➔ 旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険者・被保険者番号等

（例）

など

「要配慮個人情報」とは（法第２条第３項関係）

- 「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他**本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報**をいう。

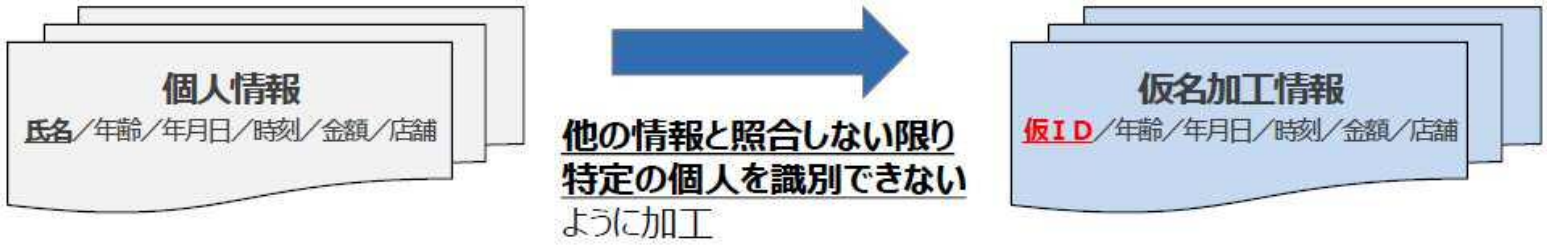
1. **人種：** 人種、世系又は民族的若しくは種族的出身を広く意味する。
2. **信条：** 個人の基本的なものの見方、考え方を意味し、思想と信仰の双方を含む。
3. **社会的身分**：ある個人にその境遇として固着していて、一生の間、自らの力によって容易にそれから脱し得ないような地位
4. **病歴：** 病気に罹患した経歴
5. **犯罪の経歴：** 前科、すなわち有罪の判決を受けこれが確定した事実
6. **犯罪により害を被った事実：** 犯罪の被害を受けた事実
7. **その他政令で定めるもの：** 施行令・施行令に委任された施行規則で規定
   - 身体障害、知的障害、精神障害（発達障害を含む。）その他の**個人情報保護委員会規則で定める心身の機能の障害があること**
   - 本人に対して**医師その他医療に関連する職務に従事する者（以下「医師等」という。）により行われた疾病の予防及び早期発見のための健康診断その他の検査（以下「健康診断等」という。）の結果**
   - 健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して**医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと**
   - 本人を被疑者又は被告人として、**逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと**
   - 本人を少年法第3条第1項に規定する少年又はその疑いのある者として、**調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと**

「仮名加工情報」とは（法第２条第５項関係）

○次に掲げる個人情報の区分に応じて当該各号に定める措置を講じて**他の情報と照合しない限り特定の個人を識別することができない**ように個人情報を加工して得られる個人に関する情報をいう。

○なお、仮名加工情報の作成については法第41条に定める規制を受けることから、同条の適用を受けない行政機関等において自ら仮名加工情報を作成することは基本的に想定されておらず、作成を委託等した第三者（民間事業者）から提供を受けて取り扱う場合が想定される。

- 法第２条第１項第１号に該当する個人情報
  - 当該個人情報に含まれる**記述等の一部を削除すること**（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
- 個人識別符号を含む個人情報
  - 当該個人情報に含まれる**個人識別符号の全部を削除すること**（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。



「匿名加工情報」とは（法第２条第６項関係）

○以下に掲げる個人情報の区分に応じて当該各号に定める措置を講じて**特定の個人を識別することができない**ように個人情報を加工して得られる個人に関する情報であって、**当該個人情報を復元することができないようにしたもの**をいう。

○なお、匿名加工情報の作成については法第43条に定める規制を受けることから、行政機関等が自ら作成することは想定しておらず、作成を委託等した第三者（民間事業者）から提供を受けて取り扱う場合が想定される。ただし、行政機関等が自ら作成することができる類似の制度として、行政機関等匿名加工情報（法第60条第3項）があり、これについては法第107条以下の定めに従って作成する必要があることに留意する。

- 法第２条第１項第１号に該当する個人情報
  - 当該個人情報に含まれる**記述等の一部を削除すること**（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
- 個人識別符号を含む個人情報
  - 当該個人情報に含まれる**個人識別符号の全部を削除すること**（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

「個人関連情報」とは（法第２条第７項関係）

○「個人関連情報」とは、**生存する個人に関する情報**であって、**個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの**をいう。

■ **「個人に関する情報」**とは、ある個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報である。

- 「個人に関する情報」のうち、氏名、生年月日その他の記述等により特定の個人を識別することができるものは、個人情報に該当するため、個人関連情報には該当しない。

■ また、**統計情報**は、特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」に該当するものではないため、個人関連情報にも該当しない。

【個人関連情報に該当する事例（※）】

事例1）Cookie等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴

事例2）メールアドレスに結び付いた、ある個人の年齢・性別・家族構成等

事例3）ある個人の商品購買履歴・サービス利用履歴

事例4）ある個人の位置情報

事例5）ある個人の興味・関心を示す情報

（※）個人情報に該当する場合は、個人関連情報に該当しないことになる。例えば、一般的に、ある個人の位置情報それ自体のみでは個人情報には該当しないものではあるが、個人に関する位置情報が連続的に蓄積される等して特定の個人を識別することができる場合には、個人情報に該当し、個人関連情報には該当しないことになる。

「保有個人情報」とは（法第60条第１項関係）

■ 行政機関等に適用される規律の大部分においては、**「保有個人情報」**が適用対象となっている。

■ **「保有個人情報」**とは、行政機関等（法第58条第１項各号に掲げる者を含む。）の**役職員が職務上作成し、又は取得した個人情報**であって、当該行政機関等及び法別表第2に掲げる法人の**役職員が組織的に利用するもの**として、当該行政機関等及び法別表第2に掲げる法人が保有しているもののうち、**次の文書に記録されているもの**をいう（法第60条第１項）。

① **行政文書**（行政機関情報公開法第２条第２項）

② **法人文書**（独立行政法人等情報公開法第２条第２項）（同項第４号に掲げるものを含む。）

③ **地方公共団体等行政文書**（法第60条第１項）

「個人情報ファイル」とは（法第60条第２項関係）

■ 「個人情報ファイル」とは、**保有個人情報を含む情報の集合体**であって、①一定の事務の目的を達成するために特定の保有個人情報を**電子計算機を用いて検索できるように体系的に構成したもの**（電子計算機処理に係る個人情報ファイル）、又は②一定の事務の目的を達成するために氏名、生年月日、その他の記述等により**特定の保有個人情報を容易に検索することができるように体系的に構成したもの**（いわゆるマニュアル（手作業）処理に係る個人情報ファイル）をいう。

（法第60条第２項）

「個人情報」と「特定個人情報」の関係

【ポイント】
- ✓ マイナンバー（個人番号）は、個人情報に該当する。
  （※ただし、生存する方の情報である場合）
- ✓ 特定個人情報とは、マイナンバー（個人番号）を含む個人情報をいう。

- ✓ 生存する方のマイナンバー（個人番号）は、「個人情報」に該当する。
- ✓ 亡くなられた方のマイナンバー（個人番号）は、「個人情報」に該当しない。

※個人情報保護法において、「個人情報」は「生存する個人に関する情報」であることが前提となっている。

第２章
行政機関等が守るべき規律

行政機関等が守るべき規律と、「個人情報」「保有個人情報」「個人情報ファイル」の関係

【個人情報】

生存する個人に関する情報で、
特定の個人を識別することができるもの

（例：１枚の名刺）

【保有個人情報】

役職員が職務上作成・取得し、役職員が組織的に利用するものとして保有する、行政文書又は法人文書に記録されるもの

→体系的に構成（分類・整理等）され、容易に検索できる個人情報のみならず、いわゆる散在情報も含む

【個人情報ファイル】
容易に検索できるよう体系的に構成したもの（電算機又はマニュアル処理）

① 保有・取得に関するルール

- 法令の定めに従い適法に行う事務又は業務を遂行するため必要な場合に限り、保有する。
- 利用目的について、具体的かつ個別的に特定する。
- 利用目的の達成に必要な範囲を超えて保有できない。
- 直接書面に記録された個人情報を取得するときは、本人に利用目的をあらかじめ明示する。
- 偽りその他不正の手段により個人情報を取得しない。
- 違法又は不当な行為を助長し、又は誘発するおそれがある方法により利用しない。
- 苦情等に適切・迅速に対応する。

② 保管・管理に関するルール

- 過去又は現在の事実と合致するよう努める。
- 漏えい等が生じないよう、安全に管理する。
- 従業者・委託先にも安全管理を徹底する。
- 委員会規則で定める漏えい等が生じたときには、委員会に対して報告を行うとともに、本人への通知を行う。

③ 利用・提供に関するルール

- 利用目的以外のために自ら利用又は提供してはならない。
- 外国にある第三者に提供する場合は、当該提供について、参考情報を提供した上で、あらかじめ本人から同意を得る。

④ 開示請求等への対応に関するルール

- 本人から開示等の請求があった場合はこれに対応する。

⑤ 通知・公表等に関するルール

- 個人情報ファイルを保有する場合に委員会へ通知する。
- 個人情報ファイル簿を作成・公表する。

「保有」に関する規律

個人情報の保有の制限　（法第61条関係）

- 行政機関等は、個人情報を保有するに当たっては、法令（条例を含む。）の定める所掌事務又は業務を遂行するため必要な場合に限り、かつ、その利用目的をできる限り特定しなければならない。
- 行政機関等は、特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない。
- 行政機関等は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

➢ 個人情報の利用目的について、当該個人情報がどのような事務又は業務の用に供され、どのような目的に使われるかをできるだけ具体的かつ個別的に特定しなければならず、特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない。そのため、個人情報が保有される個人の範囲及び個人情報の内容は、利用目的に照らして必要最小限のものでなければならない。 手引き 2-1 (P43)

「取得」に関する規律

利用目的の明示　（法第62条関係）

- 行政機関等は、本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するときは、あらかじめ、本人に対し、その利用目的を明示しなければならない。

適正な取得　（法第64条関係）

- 行政機関の長等は、偽りその他不正の手段により個人情報を取得してはならない

- 個人情報の利用目的については、申請書等の様式にあらかじめ記載しておくことや、オンライン申請の場合に本人が送信ボタン等をクリックする前に目に留まるよう配置に留意するなど、本人が認識することができる適切な方法により明示することが重要である。手引き 2-2-2（P46）
- 一部の利用目的の明示を義務付けることが適当でない場合のため、適用除外について定めている。法第62条各号
  - ① 人の生命、身体又は財産の保護のために緊急に必要があるとき
  - ② 利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき
  - ③ 利用目的を本人に明示することにより、国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき
  - ④ 取得の状況からみて利用目的が明らかであると認められるとき

「管理」に関する規律

安全管理措置（法第66条関係）　**⇒第３章で詳細に説明する。**

- 行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

漏えい等の報告・本人通知（法第68条関係）　**⇒第４章で詳細に説明する。**

- 行政機関の長等は、保有個人情報の漏えい、滅失又は毀損その他の保有個人情報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、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。
- 上記が生じたときは、行政機関の長等は、本人に対し、当該事態が生じた旨を通知しなければならない。

➢ 漏えい等報告・通知が必要と、個人情報保護委員会規則で定めるもの。（義務化４類型）規則第43条

① 要配慮個人情報が含まれる（地方公共団体における条例要配慮個人情報に該当する場合を含む）
② 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（クレジットカード番号等）
③ 不正の目的をもって行われたおそれがある（不正アクセス、持ち出し等）
④ 本人の数が100人を超える

➢ 上記４類型に該当する場合、速やかに速報を行うことに加え、当該事態を知った日から30日以内（③の場合は60日以内）に確報を委員会（委員会ホームページの報告フォーム）に提出しなければならない。

規則第44条第1項、第2項

「利用」「提供」に関する規律

利用及び提供の制限（原則）　（法第69条関係）

- 行政機関の長等は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

➢ 原則とは別に、例外的に既存の利用目的以外の目的にて個人情報の利用及び提供が認められているケース。 法第69条第1項、第2項

① 法令に基づく場合

② 本人の同意があるとき、又は本人に提供するとき

③ 行政機関等が法令の定める事務又は業務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当の理由があるとき

④ 他の行政機関、独立行政法人等、地方公共団体の機関又は地方独立行政法人に保有個人情報を提供する場合において、提供を受ける者が法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当の理由があるとき

⑤ 上記のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由があるとき

ただし、②～⑤については、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

「開示請求」に関する規律

保有個人情報の開示義務　（法第78条関係）

- 行政機関の長等は、開示請求があったときは、開示請求に係る保有個人情報に不開示情報が含まれている場合を除き、当該保有個人情報を開示しなければならない。

部分開示　（法第79条関係）

- 行政機関の長等は、開示請求に係る保有個人情報に不開示情報が含まれている場合において、不開示情報に該当する部分を容易に区分して除くことができるときは、開示請求者に対し、当該部分を除いた部分につき開示しなければならない。

裁量的開示　（法第80条関係）

- 行政機関の長等は、開示請求に係る保有個人情報に不開示情報が含まれている場合であっても、個人の権利利益を保護するため特に必要があると認めるときは、開示請求者に対し、当該保有個人情報を開示することができる

保有個人情報の存否に関する情報　（法第81条関係）

- 開示請求に対し、当該開示請求に係る保有個人情報が存在しているか否かを答えるだけで、不開示情報を開示することとなるときは、行政機関の長等は、当該保有個人情報の存否を明らかにしないで、当該開示請求を拒否することができる。

「訂正請求」に関する規律

対象となる情報　（法第90条関係）

- 訂正請求の対象となる情報は、「自己を本人とする保有個人情報」のうち、次の情報に限られる。
  ① 開示決定に基づき開示を受けた保有個人情報
  ② 開示決定に係る保有個人情報であって、法第88条第1項の他の法令の規定により開示を受けた情報

請求期限　（法第90条関係）

- 訂正請求は、保有個人情報の開示を受けた日から90日以内にしなければならない。

保有個人情報の訂正義務　（法第92条関係）

- 行政機関の長等は、訂正請求に理由があると認めるときは、当該訂正請求に係る保有個人情報の利用目的の達成に必要な範囲内で、当該訂正請求に係る保有個人情報を訂正しなければならない。

訂正の通知　（法第97条関係）

- 行政機関の長等は、訂正決定に基づく保有個人情報の訂正の実施をした場合において、提供に係る保有個人情報の内容や提供先における利用目的を勘案して個別に判断した上で必要があると認めるときは、当該保有個人情報の提供先に対し、遅滞なく、その旨を書面により通知しなければならない。

「利用停止請求」に関する規律

対象となる情報　（法第90条、98条関係）

- 利用停止請求の対象となる情報は、「自己を本人とする保有個人情報」のうち、開示決定その他法令の規定により開示を受けたものに限られる。

  ※利用停止とは、利用の停止、消去または提供の停止のことをいいます。

請求期限　（法第98条関係）

- 利用停止請求は、保有個人情報の開示を受けた日から90日以内にしなければならない。

保有個人情報の利用停止義務　（法第100条関係）

- 行政機関の長等は、利用停止請求に理由があると認めるときは、当該行政機関の長等の属する行政機関等における個人情報の適正な取扱いを確保するために必要な限度で、当該利用停止請求に係る保有個人情報の利用停止をしなければならない。

「個人情報ファイル」に関する規律

個人情報ファイル簿の作成及び公表　（法第75条関係）

- 行政機関の長等は、一定の事項を記載した帳簿である個人情報ファイル簿を作成し、公表しなければならない。
- 行政機関の長等は、個人情報ファイルの記録項目等を個人情報ファイル簿に記載し、又は個人情報ファイルを個人情報ファイル簿に掲載することにより、利用目的に係る事務又は事業の性質上、当該事務又は事業の適正な遂行に著しい支障を及ぼすおそれがあると認めるときは、その記録項目の一部若しくは事項を記載せず、又はその個人情報ファイルを個人情報ファイル簿に掲載しないことができる。

- 地方公共団体の機関、独立行政法人等及び地方独立行政法人についても、個人情報ファイル簿の作成・公表義務が課される。
- その上で、地方公共団体の機関及び地方独立行政法人においては、条例で定めるところにより、個人情報ファイル簿に加えて、個人情報の保有の状況に関する事項を記載した帳簿を作成し、公表することができる。

「個人情報ファイル」に関する規律

作成及び公表の対象外となるもの

- 次のいずれかに該当する個人情報ファイルについては、個人情報ファイル簿の作成及び公表を要しない。（法第75条第２項）

1. 国の安全、外交上の秘密その他の国の重大な利益に関する事項を記録する個人情報ファイル
2. 犯罪の捜査、租税に関する法律の規定に基づく犯則事件の調査又は公訴の提起若しくは維持のために作成し、又は取得する個人情報ファイル
3. 当該機関の職員又は職員であった者に係る個人情報ファイルであって、専らその人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項を記録するもの（当該機関が行う職員の採用試験に関する個人情報ファイルを含む。）
4. 専ら試験的な電子計算機処理の用に供するための個人情報ファイル
5. 前項の規定による通知に係る個人情報ファイルに記録されている記録情報の全部又は一部を記録した個人情報ファイルであって、その利用目的、記録項目及び記録範囲が当該通知に係るこれらの事項の範囲内のもの
6. 一年以内に消去することとなる記録情報のみを記録する個人情報ファイル
7. 資料その他の物品若しくは金銭の送付又は業務上必要な連絡のために利用する記録情報を記録した個人情報ファイルであって、送付又は連絡の相手方の氏名、住所その他の送付又は連絡に必要な事項のみを記録するもの
8. 職員が学術研究の用に供するためその発意に基づき作成し、又は取得する個人情報ファイルであって、記録情報を専ら当該学術研究の目的のために利用するもの
9. 本人の数が政令で定める数に満たない個人情報ファイル　※豊島区では作成のみ行う
10. 上記3から9までに掲げる個人情報ファイルに準ずるものとして政令で定める個人情報ファイル

第３章
講ずべき安全管理措置等について

安全管理措置について（法第66条第１項関係）

行政機関の長等が講ずべき安全管理措置

●個人情報保護法　第66条第１項

行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の**安全管理のために必要かつ適切な措置を講じなければならない。**

●個人情報の保護に関する法律についてのガイドライン（行政機関等編）

５－３－１　安全管理措置

- 求められる安全管理措置の内容は、**保有個人情報の漏えい等が生じた場合に本人が被る権利利益の侵害の大きさを考慮し**、事務又は業務の規模及び性質、保有個人情報の取扱状況（取り扱う保有個人情報の性質及び量を含む。）、保有個人情報を記録した媒体の性質等に起因する**リスクに応じて**、必要かつ適切な内容としなければならない。
- 安全管理措置の内容としては、例えば、保有個人情報にアクセスする権限を有する職員の範囲や権限の内容を業務に必要な最小限の範囲に限定する、あるいは保有個人情報が記録された媒体を保管する場所を定めた上で施錠等を行うといった対応が考えられる。
- デジタル化が進むなか、安全管理措置を適切に講じるためには、**サイバーセキュリティの確保も重要**であり、取り扱う保有個人情報の性質等に照らして適正な水準を確保する必要がある。

安全管理措置について（法第66条第１項関係）

●個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）

■ 安全管理のために必要かつ適切な措置

① 組織的安全管理措置
- 組織体制の整備
- 個人情報の取扱いに係る規律に従った運用
- 個人情報の取扱状況を確認する手段の整備
- 漏えい等の事案に対応する体制の整備
- 個人情報の取扱状況の把握及び安全管理措置の見直し

② 人的安全管理措置
- 従事者の教育

③ 物理的安全管理措置
- 個人情報を取り扱う区域の管理
- 機器及び電子媒体等の盗難等の防止
- 電子媒体等を持ち運ぶ場合の漏えい等の防止
- 個人情報の削除及び機器、電子媒体等の廃棄

④ 技術的安全管理措置
- アクセス制御
- アクセス者の識別と認証
- 外部からの不正アクセス等の防止
- 情報システムの使用に伴う漏えい等の防止

⑤ 外的環境の把握
- 保有個人情報が取り扱われる外国の特定
- 外国の個人情報の保護に関する制度等の把握

■ サイバーセキュリティ対策との連携

■ 委託先の監督
（クラウドサービス利用に係る安全管理措置）

具体的な安全官措置は、「手引き」107ページの2-8（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針に基づき実施することが求められています！

個人情報保護法についての事務対応ガイド（行政機関等向け）

～（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針～

・この指針は、個人情報保護法第66条第１項の規定等を踏まえ、行政機関等の保有する個人情報の安全管理のために必要かつ適切な措置として最小限を示すものであり、以下のことが挙げられている。

- ◆管理体制
- ◆教育研修
- ◆職員の責務
- ◆保有個人情報の取扱い
- ◆情報システムにおける安全の確保等
- ◆情報システム室等の安全管理
- ◆保有個人情報の提供
- ◆個人情報の取扱いの委託
- ◆サイバーセキュリティの確保
- ◆安全管理上の問題への対応
- ◆監査及び点検の実施

事務対応ガイドを基に「手引き（個人情報保護事務の手引き）」をつくりました。
よく読んで事務を行ってください。

・各行政機関等においては、この指針を参考として、個人情報の適切な管理に関する定めを整備し、個人情報の安全管理のために必要な措置を講じなければならない。

本人が被る権利利益の侵害の大きさを考慮し、リスクに応じた適切な安全管理措置を講じなければ、個人情報保護法違反と判断される可能性がありますので、事務対応ガイド指針を参考に体制の整備を図ってください。

１．組織的安全管理措置

手引き 2-8-2 (P107)

求められる措置	手法の例示
（１）組織体制の整備 ・ 組織体制の整備のため、総括保護管理者、保護管理者、保護担当者、監査責任者を設置する。	➢ 総括保護管理者、保護管理者、監査責任者の設置は、個人情報取扱規程等に規定する。 ➢ 保有個人情報を取り扱う各課室等の保護管理者は、保護担当者を指定する。特に保護担当者が人事異動や退職等で保護担当者でなくなった場合は、速やかに指定を解除する必要がある。 

組織体制の整備は、安全管理措置の運用する上で、非常に重要な事項となりますので、確実に整備することが求められます。

１．組織的安全管理措置

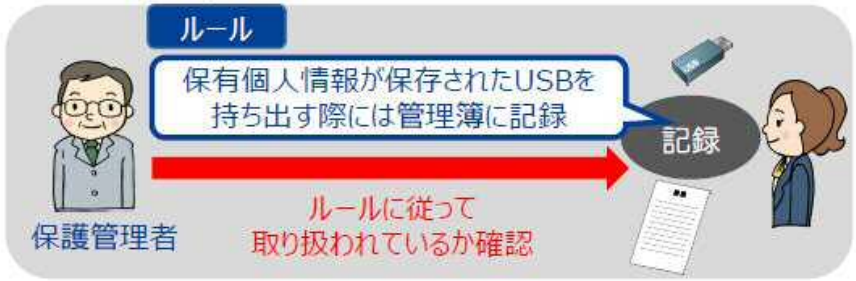
手引き 2-8-5 (1)～(3) (P109)

求められる措置	手法の例示
（２）個人情報の取扱一覧に係る規律に従った運用 ○ アクセス制限 保護管理者は、保有個人情報の秘匿性等その内容(注)に応じて、保有個人情報にアクセスする権限を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。 （注）特定の個人の識別の容易性の程度、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度を考慮する。	➢ 保護管理者は、職員のアクセス権限が業務上適切なものとなっているか、業務に必要がない権限が付与されていないか等を確認する。 ➢ 職員の異動や配置転換等によりアクセス権限が不要となった場合には、アクセス権限の削除・無効化の措置を講じる。 ➢ 職員が長期間にわたり休職している場合には、休職期間を考慮し、アクセス権限の削除・無効化の措置を講じる。

保護管理者には、アクセス権限を有する職員の異動等の状況を把握し、職員に与えられたアクセス権限を適切に管理していくことが求められます！

1．組織的安全管理措置

手引き 2-8-5(9)（P110),2-8-6(3)（P111）

求められる措置	手法の例示
（3）個人情報の取扱状況を確認する手段の整備 ① 保有個人情報の取扱状況の記録 保護管理者は、保有個人情報の秘匿性等に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱状況について記録する。	➢ 個人情報が記録された電子媒体等を外部に持ち出す場合や利用する場合は、その状況を記録することが求められる。 ➢ 要配慮個人情報を含むような秘匿性の高い媒体等を廃棄する場合には、その廃棄記録を残すことも有効である。 

個人情報の取扱いは複数の部署で行われますので、組織全体のルールの策定、台帳や取扱記録簿の様式を定め、組織全体で統一的に運用を行うことが重要です！

１．組織的安全管理措置

求められる措置	手法の例示
（３）<u>個人情報の取扱状況を確認する手段の整備</u> ② アクセス状況の記録・分析 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録を一定の期間保存し、及びアクセス記録を定期的に分析するために必要な措置を講ずる。	➢ アクセス記録（ログ）の分析を行うためのマニュアルや手順書等を定める。 ➢ ログの分析は、職員が業務には関係がない特定の人物の個人情報の閲覧やデータの書き出し等をしていないか、深夜帯や休日などの時間帯に不正なアクセスをしていないか等の観点で分析を行う。 ➢ ログ分析の頻度は、毎月または隔月といった短い頻度で実施する。

１．組織的安全管理措置

手引き 2-8-11 (P116)

求められる措置	手法の例示
（４）漏えい等事案に対応する体制の整備 ・ 漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。	➢ 漏えい等事案の発生に備え、漏えい等事案発生時の対応マニュアルや報告フロー図等を整備し、職員に周知する。 

職員は異動等により頻繁に交代しますので、定期的に対応マニュアルの周知や、インシデント時の対応訓練などを行うことが重要です！

1．組織的安全管理措置

手引き 2-8-12 (P117)

求められる措置	手法の例示
（5）取扱状況の把握及び安全管理措置の見直し ① 監査の実施 監査責任者は、定期的に監査を行い、その結果を総括保護管理者へ報告する。 ② 点検の実施 保護管理者は、保有個人情報の記録媒体や保管方法等について、定期に点検を行う。 ③ 監査等の結果を踏まえた見直し 総括保護管理者等は監査等の結果を踏まえ、必要があると認めるときは、見直しの措置を講ずる。	➢ 保有個人情報を取り扱う課室は多いことから、中期的な期間（5年程度）の監査実施計画をたて、計画的に監査を実施する。 ➢ 監査を実施する際は、監査責任者等が現場で監査事項のチェックリスト等を活用し、取扱い状況等の確認を行う。 ➢ 監査の結果、不備事項が認められた場合には、その後の改善状況をフォローアップする。 

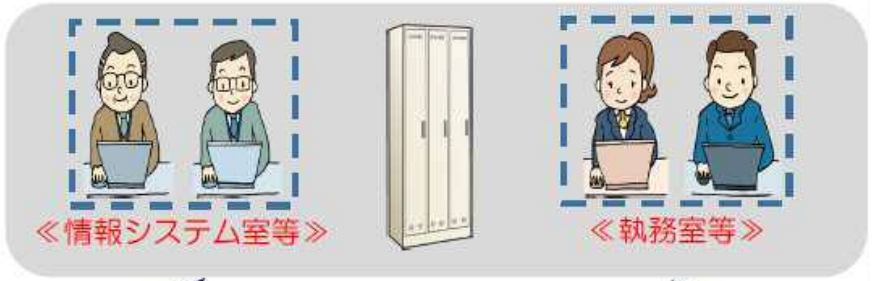
2．人的安全管理措置

手引き 2-8-3 (P108)

求められる措置	手法の例示
○**教育研修** 総括保護管理者は、以下の研修を実施する。 ① 個人情報の保護に関する研修 対象者： 保有個人情報の取り扱いに従事する職員（派遣労働者を含む） ② 情報システムの管理・運用及びセキュリティ対策に関する研修 対象者：情報システムの管理の事務に従事する職員 ③ 課室等の現場における保有個人情報の適切な管理のための研修（定期的に実施） 対象者：保護管理者及び保護担当者	➢ 研修実施計画を立て、職員に周知する。 ➢ 研修担当課や所属長が受講管理を行い、未受講者にはフォローアップを行うといった研修の実施体制を整備する。 ➢ 研修の理解度を確認するため、「まとめテスト」といった理解度を確認する手法を取り入れる。  研修用動画等を積極的に活用しましょう!!

研修の頻度は、毎年必ず行わなければいけないものではありませんが、担当者が毎年の異動等で交代することを考慮すれば、年１回実施していくことが望ましいと考えられます。

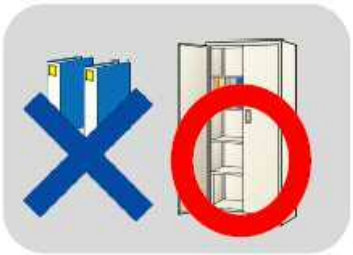
3．物理的安全管理措置

求められる措置	手法の例示
（1）入退管理 手引き 2-8-7 (1) (P113) • 保有個人情報を取り扱う基幹的なサーバー等の機器を設置する区域に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。 **（2）第三者の閲覧防止** 手引き 2-8-6 (15) (P113) • 端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。	➢ 保有個人情報を取り扱うことのできる職員以外が容易に閲覧等できないような措置を講ずる。  ≪情報システム室等≫ ≪執務室等≫ 【管理手法の例】 ➢ ICカードやナンバーキー等による入退室管理及び持ち込む機器等の制限など 【管理手法の例】 ➢ 間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施など

部外者が保有個人情報を見ることができてしまう状態にしないことが重要です。

3．物理的安全管理措置

手引き 2-8-5 (6) (P110)

求められる措置	手法の例示
（3）媒体の管理等 ① 保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行う。 ② 保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、原則として、パスワード等を使用して権限を識別する機能を設定する等のアクセス制御のために必要な措置を講ずる。	➢ 保有個人情報を取り扱う電子媒体又は保有個人情報が記載された書類等を、施錠できるキャビネットや書庫などに保管する。 ➢ 保有個人情報が記録された電子媒体を持ち運ぶ場合、パスワードの設定等の方策を講ずる。  

具体的な対応については、保護管理者が媒体に記録されている保有個人情報の秘匿性等を考慮して検討し、職員に指示してください。

3．物理的安全管理措置

手引き 2-8-6 (13) (14) (P112)

求められる措置	手法の例示
（4）端末の盗難防止等 ① 端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。 ② 保護管理者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。	➢ 保有個人情報を取り扱う端末をセキュリティワイヤー等により固定する。 ➢ 業務のため端末を外部に持ち出す際には保護管理者の承認を得ることとし、管理簿により持ち出し状況を適切に管理する。 

保護管理者が課室にある端末の状況を適切に把握し、持ち出しの承認については必要性を確認した上で行うようにしましょう。

3．物理的安全管理措置

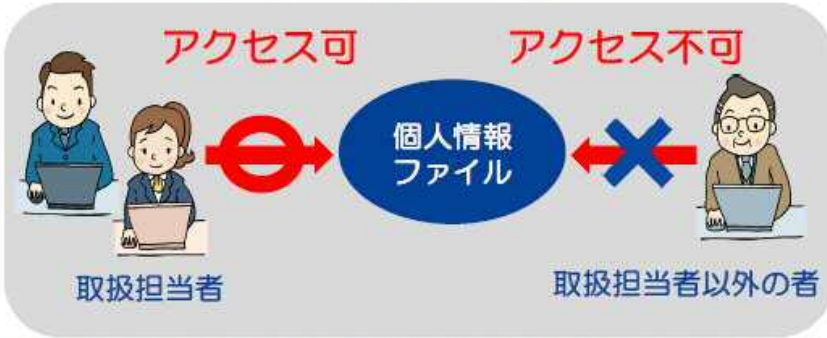
手引き 2-8-5（8）(P110)

求められる措置	手法の例示
（5）廃棄等 ① 保有個人情報又は保有個人情報が記録されている媒体が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。 ② 媒体の廃棄を委託する場合には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取るなど、委託先において廃棄等が確実に行われていることを確認する。	➢ 以下のような復元不可能な手段を採用する。 保有個人情報が記載された書類等 → ➢ 焼却、溶解、適切なシュレッダー処理等の復元不可能な手段 保有個人情報の削除、又は保有個人情報が記録された機器、電子媒体等の廃棄 → ➢ 容易に復元できない手段を採用 ➢ 専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用 ➢ 保有個人情報を削除し、又は、保有個人情報が記録された機器、電子媒体等を廃棄したことを責任ある立場の者が確認する。 

削除・廃棄の記録は適切に保存しましょう。
それらの作業を委託する場合には、委託先が確実に削除・廃棄したことについて証明書等により確認することが重要です。

4．技術的安全管理措置

手引き 2-8-6 (1) (P111)

求められる措置	手法の例示
（1）アクセス制御 • 保護管理者は、保有個人情報(※)の秘匿性等その内容に応じて、当該職員が業務を行う上で必要最小限の範囲で、アクセス制御のために必要な措置を講ずる。 (※) 情報システムで取り扱うものに限る	➢ 個人情報ファイルを取り扱うことができる情報システムの端末を限定する。 ➢ 個人情報ファイルへのアクセス権を付与すべき者を最小化する。 （1．組織的安全管理措置（2）アクセス制限も参照）  ※取扱担当者であっても業務上の目的外でのアクセスは禁止

職員に付与するアクセス権については、職員の異動や退職、長期休職者の状況を把握し、適切に管理しましょう。

４．技術的安全管理措置

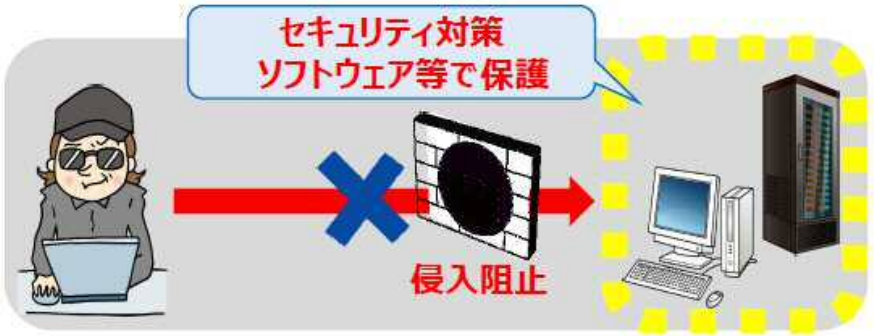
手引き 2-8-6 (1) (2) (P111)

求められる措置	手法の例示
（２）アクセス者の識別と認証 ① アクセス制御のために、認証機能を設定する等の措置を講ずる。 ② 保護管理者はパスワード管理に関する定めを整備するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。	➢ 機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、保有個人情報を取り扱う情報システムを使用する担当職員を識別・認証する。 ➢ 情報システムのパスワードは、アクセス権限がある者に対してのみ共有し、年１～２回の頻度で定期的に変更する。 

「知識情報」「所持情報」「生体情報」といった３つの認証要素のうち、２つ以上の認証要素を組み合わせた多要素認証を取り入れることで、担当職員の識別と認証を行うことも有効です。

4．技術的安全管理措置

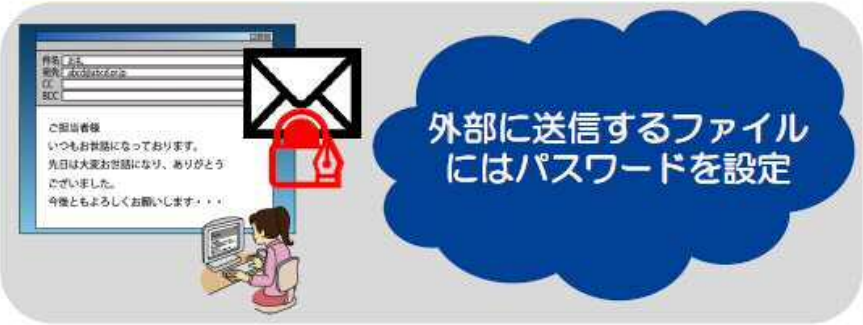
手引き 2-8-6 (5)～(8) (P111)

求められる措置	手法の例示
（3）外部からの不正アクセス等の防止 ① 保護管理者は保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォール等の設定による経路制御等の措置を講ずる。 ② 保護管理者は、不正プログラムによる保有個人情報の漏えい等の防止のため、ソフトウェア等に関する公開された脆弱性への対策等に必要な措置を講ずる。	➢ 情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ➢ 保有個人情報を取り扱う情報システムにセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。 

システムの運用保守業務を外部の事業者に委託している機関も含め、この機会にセキュリティ対策ソフトウェアの更新状況や、ファイアウォール等による通信制限状況を再確認してみましょう。

4．技術的安全管理措置

手引き 2-8-6 (10) (17) (18) (P112)

求められる措置	手法の例示
（4）情報システムの使用に伴う漏えい等の防止 ① 保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。 ② 保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。 ③ 保有個人情報に係る情報システムの設計書等の文書について外部に知られることがないよう、その保管等について必要な措置を講ずる。	➢ メール等により外部に保有個人情報が含まれるファイルを送信する場合は、当該ファイルへのパスワードを設定する。 ➢ 保有個人情報が記録されている媒体を外部に持ち出す場合には、暗号化の処理を行う。 

パスワードの秘匿に当たっては、不正に入手した者が容易に復元できないように、パスワードに用いる文字の種類や桁数等も考慮しましょう。

5．外的環境の把握

手引き 2-8-5 (10) (P110)

保有個人情報が、外国において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

？ 「保有個人情報が外国において取り扱われる場合」とは、どのようなことを指すか？

- 民間事業者が提供するクラウドサービスを利用する場合において、当該事業者が外国に所在する場合および保有個人情報が保存されるサーバが外国に所在する場合　など

民間事業者が提供するクラウドサービスを利用する場合において、クラウドサービス提供事業者が保有個人情報を取り扱わないこととなっている場合には、保有個人情報の取扱を「委託」していることにはならず委託先の監督義務等は生じませんが、行政機関等は自ら果たすべき安全管理措置の一環として、適切にクラウドサービスの選定や運用などを行う必要があります。

6．委託先の監督

手引き 2-8-9 (1) (P114)

求められる措置	手法の例示
（1）委託先の選定 ① 個人情報の適切な管理を行う能力を有しない者を委託先に選定することがないよう、必要な措置を講ずる。 ② 契約書に、所定の事項（下記参照）を明記する。 ③ 委託先における責任者・業務従事者の管理体制、業務の実施体制、個人情報の管理状況の検査等について書面で確認する。	➢ NISC（内閣サイバーセキュリティセンター）が作成する「政府機関等のサイバーセキュリティ対策のための統一基準群」を参考にして委託先の選定基準を整備する。 ➢ 契約書に明記すべき事項を網羅した契約書のひな形を作成し、関係部署に展開する。 ➢ 契約した業務を開始する前に、委託先から管理体制等の資料を提出させ、契約書に明記した事項を遵守する体制が整っていることを確認する。

【契約書に明記が必要な事項】

① 秘密保持、目的外利用の禁止
② 再委託の制限又は事前承認等
③ 個人情報の複製等の制限
④ 個人情報の安全管理措置
⑤ 個人情報の漏えい等の事案の発生時における対応
⑥ 委託終了時における個人情報の消去及び媒体の返却
⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任等
⑧ 契約内容の遵守状況についての定期的報告及び委託先における取扱状況を把握するための監査等

6．委託先の監督

手引き 2-8-9 (2) (P115)

求められる措置	手法の例示
（2）委託範囲の限定 • 保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。	➢ 委託先に引き渡すデータの中に、委託する業務と無関係の個人情報が含まれていないか事前に確認する。 ➢ 業務委託先の従業者が保有個人情報を取り扱う情報システムを使用する場合は、委託する業務に必要ない情報を閲覧することがないよう、アクセス権限を制限する。

委託先に対して業務とは無関係の個人情報を取り扱わせることは情報漏えい等のリスクもあるので、委託する情報の範囲を必要最小限にすることを徹底しましょう。

6．委託先の監督

手引き 2-8-9 (3) (P115)

求められる措置	手法の例示
（3）委託先への実地検査 • 保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも年１回以上、原則として実地検査により確認する。	➢ 委託している業務の秘匿性等を考慮し、実地検査先の優先順位を考慮して検査計画を立てた上で実地検査を実施する。 ➢ 秘匿性が高い情報を取り扱っている委託先については優先的かつ重点的に実地検査を行う。 ➢ 委託する保有個人情報の秘匿性等を検討した結果、実地検査を行わない場合であっても、報告書を提出させる等の方法で委託先の管理体制等を確認する。

原則として実地検査により委託先の管理体制等を確認しますが、実地検査の要否については委託する保有個人情報の秘匿性、情報の内容や量等の実情を考慮して検討してください。

6．委託先の監督

手引き 2-8-9 (4) (P115)

求められる措置	手法の例示
（４）再委託先の監督 • 保有個人情報の取扱いに係る業務が再委託される場合には、委託先に（１）の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが実地検査等の措置を実施する。 ※再委託先が再々委託を行う場合も同様。	➢ 委託先が再委託先を選定する際に、再委託先の管理体制等について把握した内容を委託元に報告させ、委託先が（１）の措置を適切に講じていることを確認する。 ➢ 委託先に再委託先に対する実地検査を実施させるとともに、秘匿性が高い個人情報を取り扱う業務を行っている再委託先に対しては委託元自らが実地検査を実施する。

委託元は再委託先の監督を委託先にすべて任せきりにするのではなく、委託先の監督状況を確認することで間接的に再委託先を監督することが重要です。

6．委託先の監督

手引き 2-8-9 (5) (P116)

求められる措置	手法の例示
（5）派遣労働者の監督 • 保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記する。	➢ 派遣労働者が保有個人情報を適切に取り扱うことができるよう、必要な研修を受講させる。 ➢ 研修の受講確認や情報システムのアカウント管理等において派遣労働者が確認対象から漏れないよう、業務フローを適切に構築する。

保有個人情報の取扱いに際しては派遣労働者も他の職員と同様に安全管理措置を適切に実施する必要があります。派遣労働者を含む従業者全員が保有個人情報を適切に取り扱う環境を整備しましょう。

クラウドサービス利用に係る安全管理措置

手引き 2-3-1（P51）

求められる措置	解説
① 民間事業者が提供するクラウドサービス上で保有個人情報を取り扱う場合には、行政機関等は、自ら果たすべき安全管理措置の一環として、必要かつ適切な措置を講じる必要がある。 ② 外国にある事業者が提供するクラウドサービス上で保有個人情報を取り扱う場合や、国内事業者であっても外国に所在するサーバに保有個人情報が保存される場合においては、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理措置のために必要かつ適切な措置を講じなければならない。	クラウドサービスの利用が、個人情報保護法上の「提供」に該当しない場合、クラウドサービス提供事業者に対する監督義務は課されないが、自ら果たすべき安全管理措置の一環として適切な安全管理措置を講じる必要がある。 地方公共団体においてガバメントクラウドを利用する場合も同様に、ガバメントクラウドに対する監督義務は課されないが、外的環境の把握を含む必要かつ適切な安全管理措置を講ずる必要がある。

クラウドサービスの利用が「提供」に該当するかどうかは、クラウドサービスを提供する事業者において、保有個人情報を取り扱うこととなっているのかどうかが判断の基準となります。

詳しくは、情報管理課の「情報セキュリティ研修」を確認してください。

第４章
漏えい等事案が発生した場合の対応

漏えい等の定義について

手引き 2-4-1 (1)～(3) (P59)

漏えい

保有個人情報が外部に流出すること


誤交付


誤送付
（メール含む）


盗難


不正アクセス

滅　失

保有個人情報の内容が失われること


誤廃棄
※1


紛失
※2

※1　当該帳簿等が適切に廃棄されていない場合、保有個人情報の漏えいに該当する可能性がある。

※2　当該行政機関等の外部に流出した場合、保有個人情報の漏えいに該当する。

毀　損

保有個人情報の内容が意図しない形で変更されることや利用不能な状態になること


改ざん


暗号化
※3

※3　同時に保有個人情報が窃取された場合、保有個人情報の漏えいにも該当する。

漏えい等事案が発覚した際に講ずべき措置

行政機関の長等は、漏えい等事案が発覚した場合は、漏えい等事案の内容等に応じて、次の（１）から（５）に掲げる事項について必要な措置を講じなければならない。

手引き 2-8-11 (P116)

（１）　行政機関等内部における報告及び被害の拡大防止

（２）　事実関係の調査及び原因の究明

（３）　影響範囲の特定

（４）　再発防止策の検討及び実施

（５）　個人情報保護委員会への報告及び本人への通知

個人情報保護委員会への報告を行った際には、他の関係省庁・機関への通報・届出等（警察への通報や、IPA（独立行政法人情報処理推進機構）へのコンピュータウィルス・不正アクセスに関する届出等）をあわせて行う。

※第6回個人情報保護法サイバーセキュリティ連携会議及び第10回特定個人情報セキュリティ連携協議会において、関係省庁・機関の間で合意。（令和4年12月）

報告対象となる事態

手引き 2-4-1 (5) (P61)

行政機関の長等は、次の（１）から（４）に掲げる事態（おそれを含む）を知ったときは、個人情報保護委員会に報告しなければならない。※

※ 報告対象事態に該当しない漏えい等事案であっても、国民の不安を招きかねない事案については、速やかに当委員会へ情報提供を行うことが望ましい。

※ 報告対象事態における「おそれ」については、その時点で判明している事実関係に基づいて個別の事案ごとに判断することになるが、漏えい等が疑われるものの漏えい等が生じた確証がない場合がこれに該当する。

（１）要配慮個人情報（条例要配慮個人情報を含む）が含まれる保有個人情報の漏えい等

〔例〕医療機関から取得した感染症患者の診療情報を含む保有個人情報を記録した文書を紛失した場合。

（２）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保有個人情報の漏えい等

〔例〕収納業務のため取得したクレジットカード番号を含む保有個人情報が漏えいした場合。

（３）不正の目的を持って行われたおそれがある保有個人情報の漏えい等

〔例１〕不正アクセスにより保有個人情報が漏えいした
〔例２〕ランサムウェア等により保有個人情報が暗号化され復元できなくなった
〔例３〕保有個人情報が記載・記録された書類・媒体等が盗難された
〔例４〕従事者が保有個人情報を持ち出して第3者に提供した

（４）保有個人情報に係る本人の数が100人を超える漏えい等

〔例１〕情報システムの設定ミス等によりインターネット上で保有個人情報（100人を超える）の閲覧が可能な状態となった
〔例２〕ワークショップ開催に関する案内メールを参加企業に送信する際、企業の担当者氏名（100人を超える）を含む文書を誤って添付して送付した

個人情報保護委員会への報告について

手引き 2-4-1 (6)～(9) (P63)

漏えい等報告の義務を負う主体は、漏えい等が発生し、又はそのおそれがある保有個人情報を取り扱う行政機関の長等である。

※ 保有個人情報の取扱いを委託している場合、委託元と委託先の双方が保有個人情報を取り扱っていることになるため、報告対象事態に該当する場合には、原則として委託元と委託先の双方が報告する義務を負う。

※ 報告は、委員会ホームページ上に掲載する報告フォームから行う。

速　報

報告対象事態を知った後、速やか（**概ね３～５日以内**）に当該事態に関する次に掲げる事項を報告しなければならない。

①概要
②保有個人情報の項目
③保有個人情報に係る本人の数
④原因
⑤二次被害又はそのおそれの有無及びその内容
⑥本人への対応の実施状況
⑦公表の実施状況
⑧再発防止のための措置
⑨その他参考となる事項

確　報

当該事態を知った日から**30日以内**に確報を提出しなければならない。

※報告対象事態（３）に該当する場合は**60日以内**

※速報の時点で全ての事項を報告できる場合は、速報と確報を兼ねて提出することも可能

本人通知について

手引き 2-4-2（P66）

行政機関の長等は報告対象事態が生じた場合、**本人への通知を行わなければならない。**

※ 通知義務を負う主体は漏えい等が発生し、又は発生したおそれがある保有個人情報を取り扱う行政機関の長等である。

※ 保有個人情報の取扱いを委託している場合において、委託元である行政機関等と委託先の双方が保有個人情報を取り扱っていることになるため、それぞれ通知の対象事態に該当する場合には、原則として委託元と委託先の双方が通知する義務を負う。委託元及び委託先は連携するなどして、適切な方法で通知を行うことが望ましい。

時間的制限

報告対象事態の状況に応じて速やかに本人への通知を行わなければならない。

※ 具体的に通知を行う時点は、個別の事案において、その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断する。

内容

- **概要**
- **保有個人情報の項目**
- **原因**
- **二次被害又はそのおそれの有無及び内容**
- **その他参考となる事項**

方法

本人にとって分かりやすい形で通知を行うことが望ましい。

- 電子メールを送信
- 文書を郵送等で送付

本人への通知が困難である場合は、代替措置を講ずることも可能。

- 事案の公表
- 問い合わせ窓口の設置

受講いただきありがとうございました。

参考資料として、下記を用意しました。
併せてご覧ください。

・事例から学ぶ注意POINTと防止策
・保有個人情報の取扱い実務者が参考とすべきガイドライン等の紹介

PPC 個人情報保護委員会
Personal Information Protection Commission
豊島区政策経営部区民相談課行政情報グループ