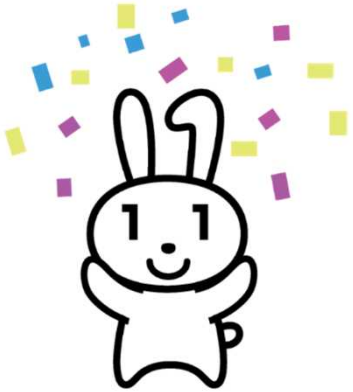



特定個人情報の適正な取扱いのための各種研修資料



個人情報保護委員会事務局　令和7年4月

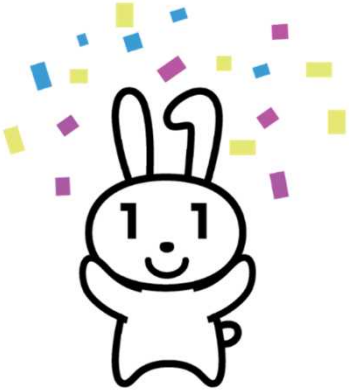
目次

はじめに

本研修資料は、特定個人情報等を取り扱う事務取扱担当者、保護責任者及び特定個人情報ファイルを取り扱う事務に従事する者を対象としており、特定個人情報等の漏えい、滅失、毀損の防止等のための安全管理措置に関する内容を中心に作成されています。

各機関で作成している業務マニュアルと本研修資料をよく理解することで、各機関においてより適切に特定個人情報等が取り扱われることを期待しています。

第１章　　事務取扱担当者研修



第１節
マイナンバー制度の概要

第１節では、マイナンバー制度とはどのような制度なのかを学んでいきましょう。

１－１　マイナンバー制度

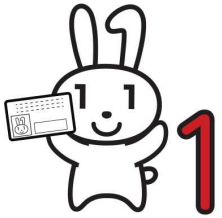
マイナンバー制度は、マイナンバー法に基づく制度です。

○マイナンバー法

・正式な法律名称は「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」で、「マイナンバー法」や「番号法」の略称を使用
・マイナンバー法では、マイナンバー（個人番号）や特定個人情報が適正に取り扱われるよう、利用範囲や取得・提供等の制限、監視・監督、罰則等について規定

○マイナンバーと特定個人情報

・マイナンバーは、住民票を有する全ての人に付番され、通知される12桁の番号
・マイナンバーは、個人情報に該当
・特定個人情報は、マイナンバーを含む個人情報



１－２　マイナンバー制度の目的

マイナンバー制度の目的は、「公平・公正な社会の実現」「行政の効率化」「国民の利便性の向上」です。

公平・公正な社会の実現

所得や他の行政サービスの受給状況が把握しやすくなり、負担を不当に免れることや給付を不正に受けることを防止し、本当に困っている方にきめ細やかな支援を行える。

行政の効率化

行政機関等で、様々な情報の照合、転記、入力等に要している時間や労力の削減ができる。

国民の利便性の向上

行政手続の簡素化により、従来の行政手続で必要だった添付書類等が削減され、国民の負担が軽減される。
行政機関等が持っている自分の情報を確認したり、行政機関等から様々なサービスのお知らせを受け取れる。

１－３　マイナンバーの利用範囲

マイナンバーの利用は、社会保障・税・災害対策その他の行政分野に及びます。

【利用範囲の例】

社会保障	
年金	年金の資格取得・確認 など
労働	雇用保険等の資格取得・確認など
福祉 医療 その他	医療保険等の保険料徴収等の医療保険者における手続、福祉分野の給付、生活保護の実施など

税
国民が税務当局に提出する確定申告書、届出書、調書等に記載

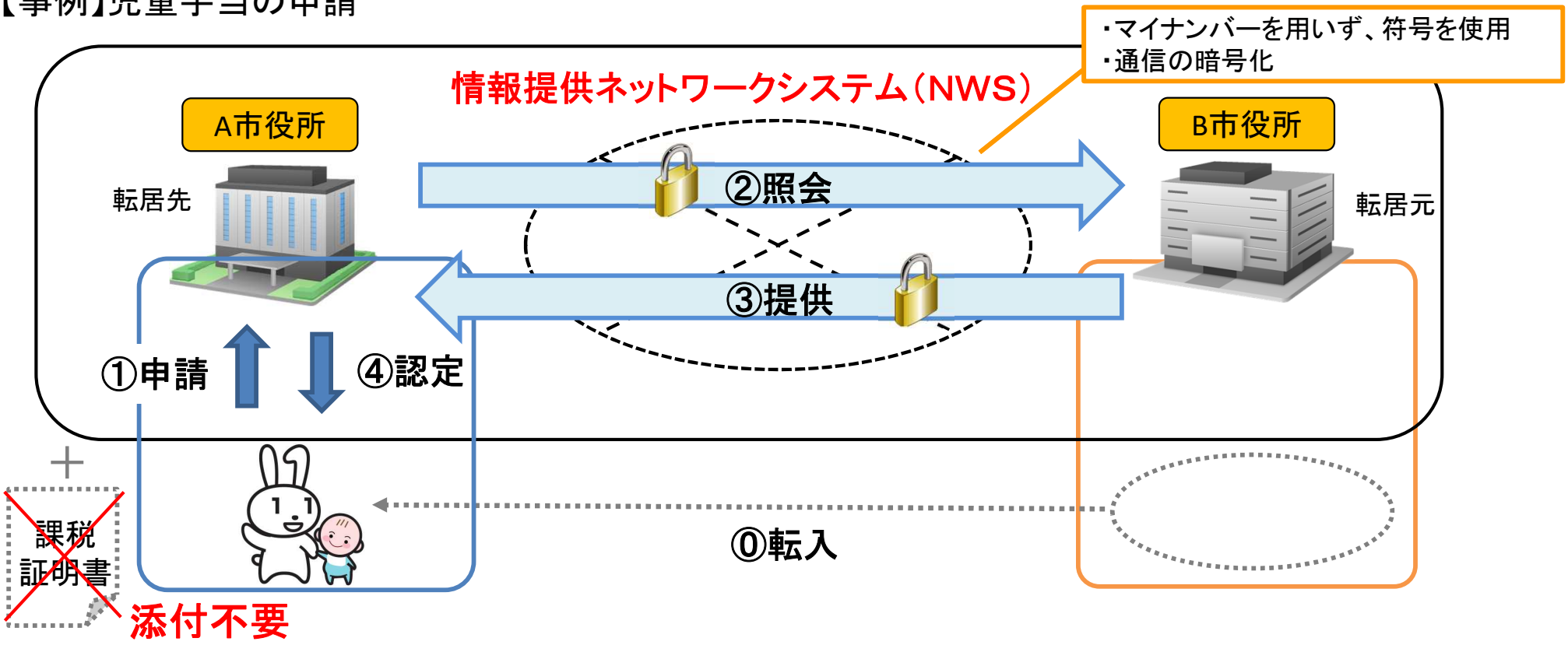
災害対策
被災者生活再建支援金の支給事務、被災者台帳の作成事務 など

上記のほか、社会保障、地方税、防災に関する事務その他の事務であって地方公共団体が条例で定める事務（独自利用事務）に利用

１－４　マイナンバー制度における「情報連携」

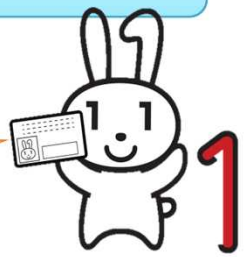
「情報連携」とは、各種手続の際に住民が行政機関等に提出する書類を省略可能とするため、異なる行政機関等の間で専用のネットワークシステムを用いた個人情報のやり取りを行うことです。

【事例】児童手当の申請



１－５　マイナンバーカード

マイナンバーカードは、マイナンバーが記載されたカードで、公的な身分証明書として利用されるほか、様々な用途に利用が可能です。市区町村等に申請すると交付されます。



マイナンバーカードの特徴

マイナンバーカード

顔写真※付きのプラスチック製カードで、マイナンバーを裏面に記載。

ICチップ内に電子的に個人を認証する機能（電子証明書）を搭載。

※　当該申請の日において本人の年齢が一定の年齢に満たない場合を除きます。（法第２条第７項）

マイナンバーカード（カード代替電磁的記録（注）を含む）の利活用

（注）法第2条第8項に規定されるカード代替電磁的記録を指します。

本人確認の公的な身分証明書として

コンビニなどで住民票などの各種証明書取得のために

健康保険証等との一体化により、他のサービスのカードとして

※ マイナンバーカードの詳しい内容については、以下のマイナンバーカード総合サイトホームページを参考にしてください。　（https://www.kojinbango-card.go.jp/）

１－６　マイナポータル

マイナポータルは、政府（デジタル庁）が運営するオンラインサービスで、行政機関等への各種申請などが可能となる国民一人一人に用意されたポータルサイトです。

マイナポータルでできること

手続の検索・電子申請
行政機関の手続の検索・申請

わたしの情報
所得・個人住民税の情報などの確認

お知らせ
行政機関等からあなたへのお知らせ

やりとり履歴
「わたしの情報」が行政機関間でやりとりされた履歴

もっとつながる
e-Taxなど、外部サイトとの連携

マイナポータルの利用には、マイナンバーカード、登録した利用者証明用電子証明書パスワード（4桁）、ICカードが読み取れるICカードリーダーやスマートフォン等が必要です。

※マイナポータルの詳しい内容については、以下のマイナポータルホームページを参考にしてください。
（https://myna.go.jp/）

第２節
マイナンバー制度の安全対策

第１節では、マイナンバー制度について、様々なメリットがあることを学びました。
しかし、メリットがある一方、マイナンバーの利用のリスクについて懸念を抱く国民も少なくありません。
第２節では、国民が抱く懸念を理解し、マイナンバーを安心して利用するための安全対策について学びましょう。

第２節　マイナンバー制度の安全対策

２－１　マイナンバーにおける安心・安全の確保

マイナンバー制度では、漏えいや不正利用等を防ぐため、「制度面における保護措置」と「システム面における保護措置」を設けています。

マイナンバー制度に対する国民の懸念

- マイナンバーを用いた個人情報の追跡・名寄せ・突合が行われ、集積・集約された**個人情報が外部に漏えい**するのではないかといった懸念
- マイナンバーの不正利用等（例：他人のマイナンバーを用いた**なりすまし**）により財産その他の被害を負うのではないかといった懸念
- 国家により個人の様々な個人情報がマイナンバーをキーに名寄せ・突合されて**一元管理**されるのではないかといった懸念

対 応

「制度面における保護措置」 ＋ 「システム面における保護措置」

２－２　制度面における保護措置（概要）

特定個人情報の漏えい、滅失、毀損などを防ぐために、制度面においても各種の保護措置が設けられています。

制度面における保護措置

① 本人確認措置（マイナンバーの確認・身元（実存）の確認）
② 特定個人情報の利用、提供、収集・保管、特定個人情報ファイルの作成の制限
③ 委託先の監督・再委託の許諾手続
④ 安全管理措置の実施
⑤ 個人情報保護委員会による監視・監督
⑥ 特定個人情報保護評価
⑦ 罰則の強化
⑧ マイナポータルによる情報提供等記録の確認

※下線の項目は、次ページ以降で内容を説明しています

２－３　制度面における保護措置（本人確認措置）

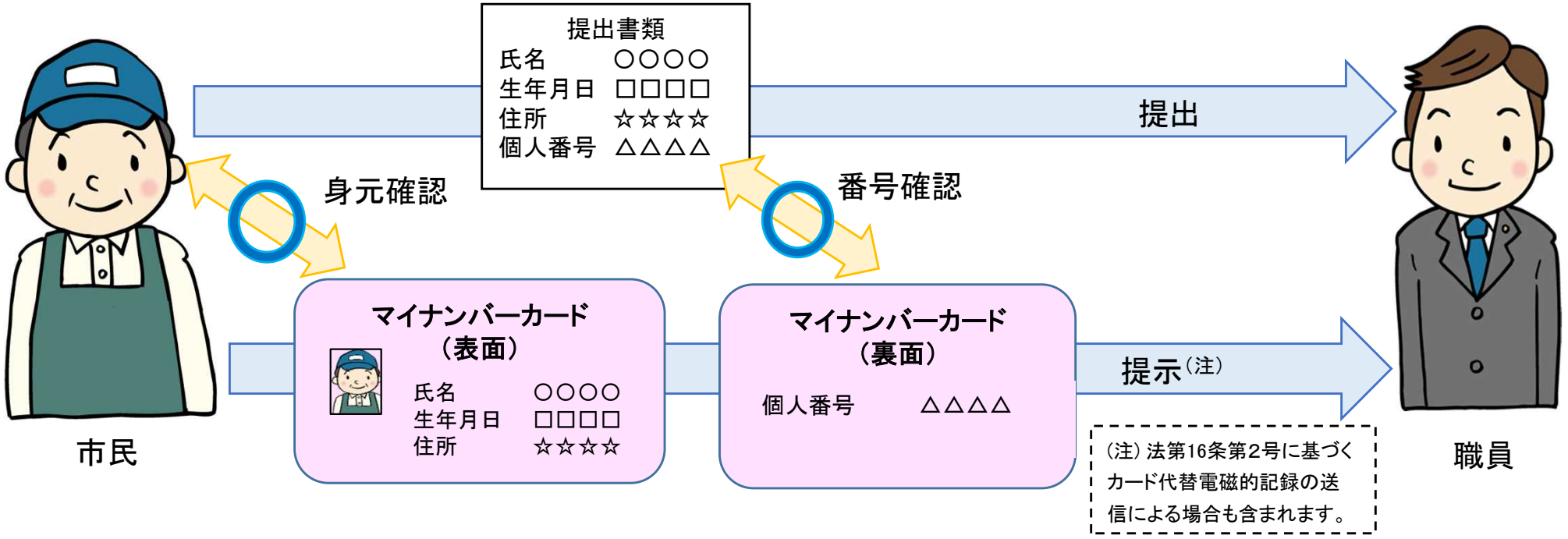
マイナンバーの提供を受ける際には、他人によるなりすましを防止するため、提供されたマイナンバーカード（カード代替電磁的記録(注)を含む）が本人のものであることを確認しなければならないこととなっています。

（注）法第2条第8項に規定されるカード代替電磁的記録を指します。

本人確認

①提供されたマイナンバーカード（カード代替電磁的記録を含む）が正しいか（番号確認）

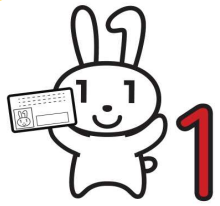
②手続を行っている者が番号の正しい持ち主であるか（身元確認）



２－３　制度面における保護措置（本人確認措置）

主な本人確認書類の例

マイナンバーカードの場合は、１枚で番号確認と身元確認が可能です



※通知カードは令和２年５月25日に廃止され、マイナンバーの通知は個人番号通知書を送付する方法により行われています。
通知カードに記載された氏名、住所等が住民票に記載されている事項と一致しているときは、引き続きマイナンバーを証明する書類として使用できます。

２－４　制度面における保護措置（利用、提供、収集・保管の制限）

マイナンバーや特定個人情報は、自由に利用、提供、収集・保管はできません。
マイナンバー法において制限が設けられています。

利用の制限

マイナンバーは、マイナンバー法があらかじめ限定的に定めた事務以外で利用することはできません。

利用できる事務

行政機関等がマイナンバーを利用するのは、個人番号利用事務※1、個人番号関係事務※2、マイナンバー法第19条第13号から第17号までに基づき特定個人情報の提供を受けた目的を達成するために必要な限度で利用する事務に限られます。

また、マイナンバーの例外的な利用は、①金融機関が激甚災害時等に金銭の支払を行う場合、②人の生命、身体又は財産の保護のために必要がある場合に限られています。

※１　マイナンバー法別表の各項の上欄に掲げる行政機関等が利用することができる同表の当該各項の下欄に掲げる事務、準法定事務(注)及びマイナンバー法第９条第２項に基づいて条例で規定した事務
（注）マイナンバー法別表の各項の下欄に掲げる事務に準ずる事務として主務省令で定めるもの

※２　職員等の社会保障及び税等に関する手続書類の作成事務

２－４　制度面における保護措置（利用、提供、収集・保管の制限）

提供、収集・保管の制限

○　個人番号利用事務及び個人番号関係事務（個人番号利用事務等）を処理するために必要がある場合に限って、本人等にマイナンバーの提供を求めることができます。

○　マイナンバー法第19条各号に定められている場合※を除き、
・マイナンバーの提供を求めること
・特定個人情報を提供、収集・保管すること
は禁止されています。

○　個人番号利用事務等を処理する必要がなくなった場合で、文書管理に関する規程等によって定められている保存期間を経過したときには、マイナンバーをできるだけ速やかに廃棄又は削除しなければなりません。

※　マイナンバー法第19条各号に定められている場合については、次ページを参照

２－４　制度面における保護措置（利用、提供、収集・保管の制限）

＜参考＞
【マイナンバー法第19条各号】

第１号	個人番号利用事務実施者※1からの提供
第２号	個人番号関係事務実施者※2からの提供
第３号	本人又は代理人からの提供
第４号	使用者等から他の使用者等に対する従業者等に関する特定個人情報の提供
第５号	地方公共団体情報システム機構によるマイナンバーの提供
第６号	委託、合併に伴う提供
第７号	住民基本台帳法上の規定に基づく提供
第８号	情報提供ネットワークシステムによる提供
第９号	情報提供ネットワークシステムによる提供（条例事務関係情報連携）
第10号	国税・地方税法令に基づく国税連携及び地方税連携による提供
第11号	地方公共団体の他の機関に対する提供
第12号	株式等振替制度による提供
第13号	個人情報保護委員会への提供
第14号	総務大臣への提供
第15号	各議院審査等その他公益上の必要があるときの提供
第16号	人の生命、身体又は財産の保護のための提供
第17号	個人情報保護委員会規則に基づく提供

※１　個人番号利用事務実施者とは、個人番号利用事務を処理する者及び個人番号利用事務の全部又は一部の委託を受けた者
※２　個人番号関係事務実施者とは、個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託を受けた者

２－５　制度面における保護措置（委託／再委託）

個人番号利用事務等を委託する場合、委託先に対して必要かつ適切な監督を行う必要があります。

委託先の監督

委託者（行政機関等）は、委託先において、マイナンバー法に基づき個人番号利用事務等を行う委託者が果たすべき安全管理措置と同等の措置が講じられるように、必要かつ適切な監督を行う必要があります。

委託者
（行政機関等）

必要かつ適切な監督

個人番号利用事務等を委託

委託先
（民間事業者）

２－５　制度面における保護措置（委託／再委託）

委託先に対する「必要かつ適切な監督」のポイントは次の3つです。

＜①選定＞

委託先の適切な選定

委託先において、委託者が果たすべき安全管理措置と同等の措置が講じられるか確認

＜③契約後＞

委託先における取扱状況の把握

委託先から報告、委託先への実地の監査等により、特定個人情報の取扱状況を把握

＜②契約時＞

委託先に安全管理措置を遵守させるための必要な契約の締結

（契約に盛り込む必要がある内容）

- 秘密保持義務
- 委託する業務の遂行に必要な範囲を超える事業所内からの特定個人情報の持ち出しの禁止
- 特定個人情報の目的外利用の禁止
- 再委託における条件
- 漏えい等事案が発生した場合の委託先の責任
- 委託契約終了後の特定個人情報の返却又は廃棄
- 特定個人情報を取り扱う従業者の明確化
- 従業者に対する監督・教育
- 契約内容の遵守状況について報告を求める規定
- 必要があると認めるときに実地調査等を行うことができる規定

２－５　制度面における保護措置（委託／再委託）

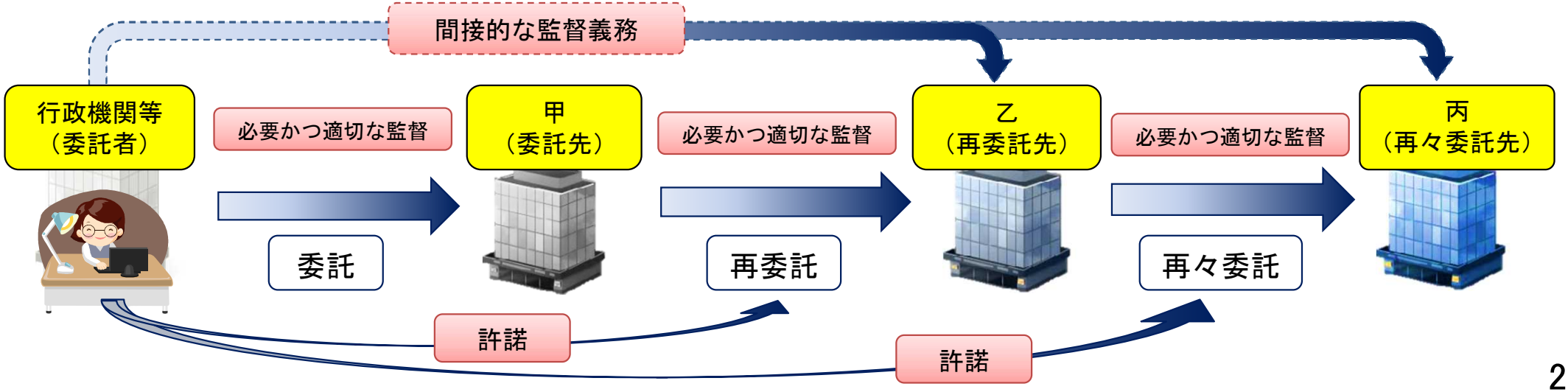
委託者の許諾なしに、委託先が再委託を行うことは禁止されています。

再委託の許諾手続

委託先が再委託する場合は、最初の委託者（行政機関等）の許諾を得た場合に限り、再委託をすることができます。再々委託以降も、最初の委託者の許諾が必要です。

再委託先の監督

最初の委託者は、再委託先等に対しても、委託先を通じて間接的な監督義務を負います。



２－６　制度面における保護措置（安全管理措置）

個人番号利用事務等実施者は、個人番号の漏えい、滅失、毀損の防止、その他個人番号の適切な管理のために、安全管理措置を講じなければなりません。

安全管理措置

講ずべき安全管理措置の内容は、**「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」（ガイドライン）の別添1**に示されています。

また、ガイドライン以外にも、次のものを遵守することを前提として、安全管理措置について検討する必要があります。

- マイナンバー法
- 個人情報保護法等関係法令
- 個人情報保護条例
- 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）
- 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）
- 特定個人情報保護評価書
- 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等に準拠した各府省庁等における情報セキュリティポリシー
- 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において策定した情報セキュリティポリシー
- 接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置等
- 個人番号と個人情報を紐付ける登録事務（以下「個人番号登録事務」という。）を実施する行政機関等は、デジタル庁が策定した「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」及び各制度の所管省庁等が策定した個人番号登録事務に係るガイドライン等

２－６　制度面における保護措置（安全管理措置）

ガイドライン（別添１）２で示す講ずべき安全管理措置の内容

A　基本方針の策定

B　取扱規程等の見直し等

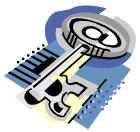
C　組織的安全管理措置

a　組織体制の整備
b　取扱規程等に基づく運用
c　取扱状況を確認する手段の整備
d　漏えい等事案に対応する体制等の整備
e　取扱状況の把握及び安全管理措置の見直し

D　人的安全管理措置

a　事務取扱担当者の監督
b　事務取扱担当者等の教育
c　法令・内部規程違反等に対する厳正な対処

E　物理的安全管理措置



a　特定個人情報等を取り扱う区域の管理
b　機器及び電子媒体等の盗難等の防止
c　電子媒体等の取扱いにおける漏えい等の防止
d　個人番号の削除、機器及び電子媒体等の廃棄

F　技術的安全管理措置

a　アクセス制御
b　アクセス者の識別と認証
c　不正アクセス等による被害の防止等
d　情報漏えい等の防止

G　外的環境の把握

２－７　システム面における保護措置（概要）

特定個人情報の漏えい、滅失、毀損等を防ぐために、システム面においても各種の保護措置が講じられています。

システム面における保護措置

①個人情報を一元的に管理せず分散して管理

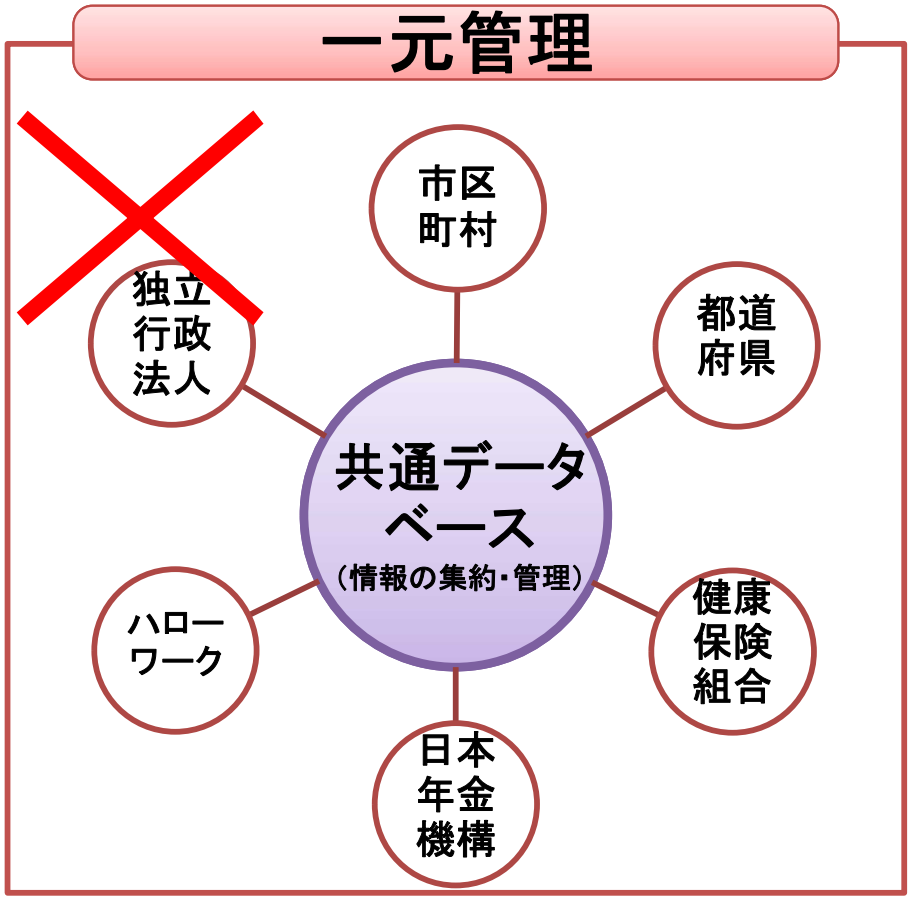
②マイナンバーを直接用いず、各機関ごと異なる符号を使用した情報連携

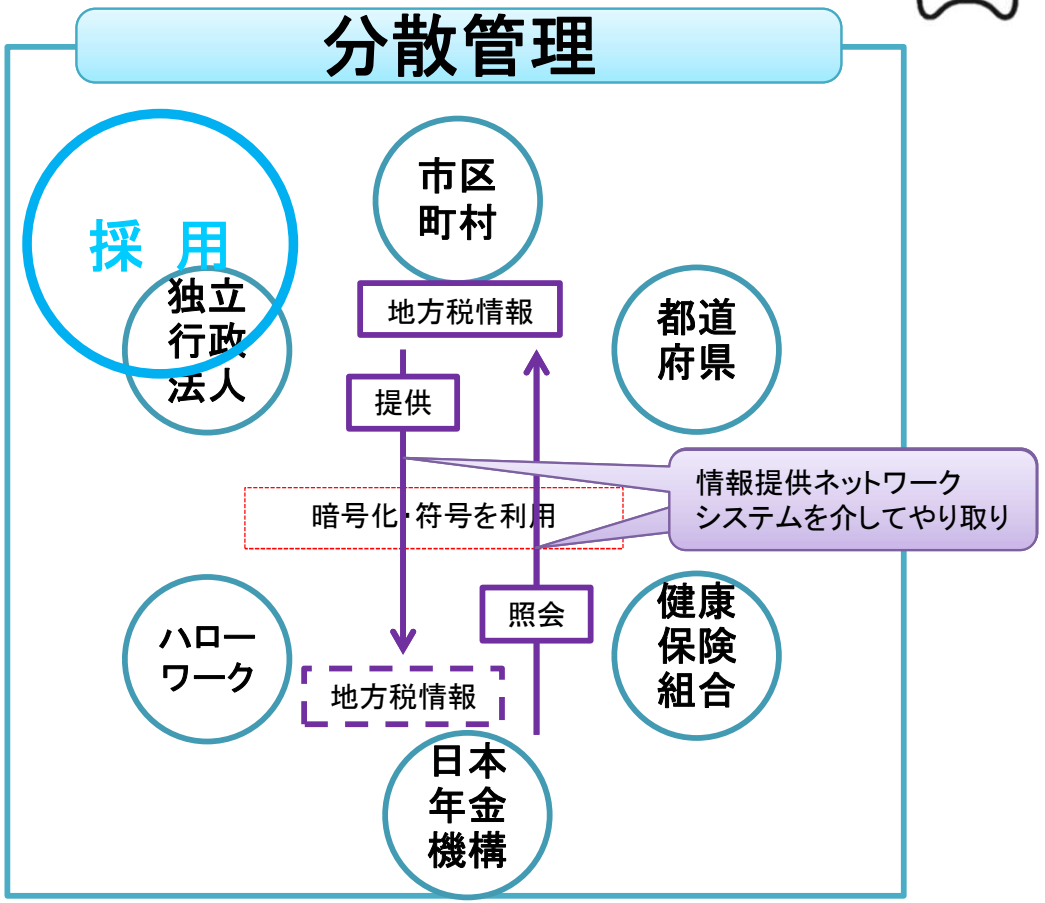
③アクセス制御により、アクセスできる人の制限・管理

④情報を通信する際の通信の暗号化

２－８　システム面における保護措置（分散管理・暗号化・符号利用）

個人情報を同一のデータベース等により一元的に管理せず、各情報の保有機関それぞれに分散して管理しています。



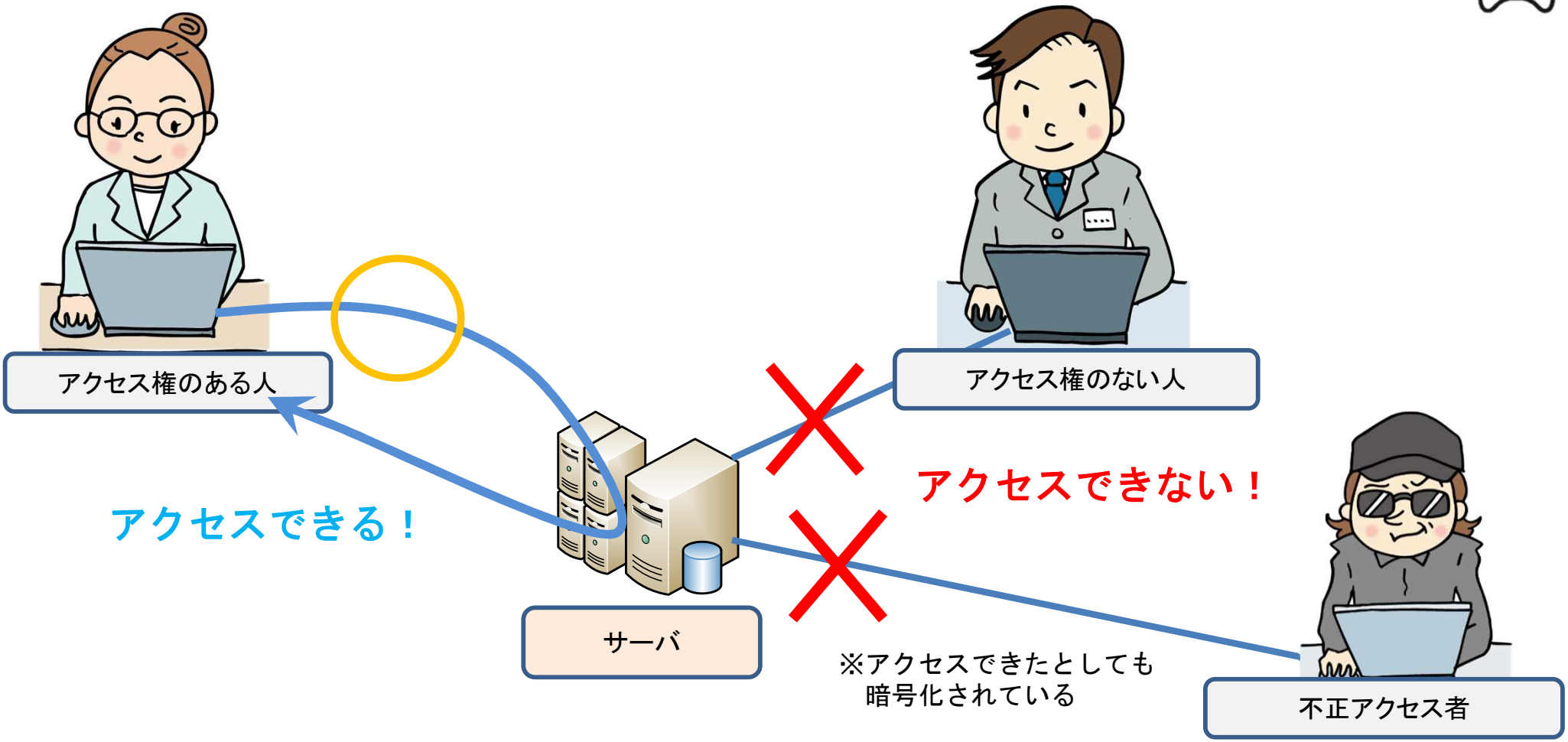


※情報提供ネットワークシステムでの符号を利用した情報連携の詳細については、以下の政府CIOポータル掲載資料を参考にしてください。

（https://cio.go.jp/sites/default/files/uploads/documents/digital/20211116_policies_posts_mynumber_security_06.pdf）

２－９　システム面における保護措置（アクセス制御・暗号化）

特定個人情報を取り扱う情報システムでは、限られた者のみにアクセス権が与えられるので、アクセス権限がない者は情報照会ができません。

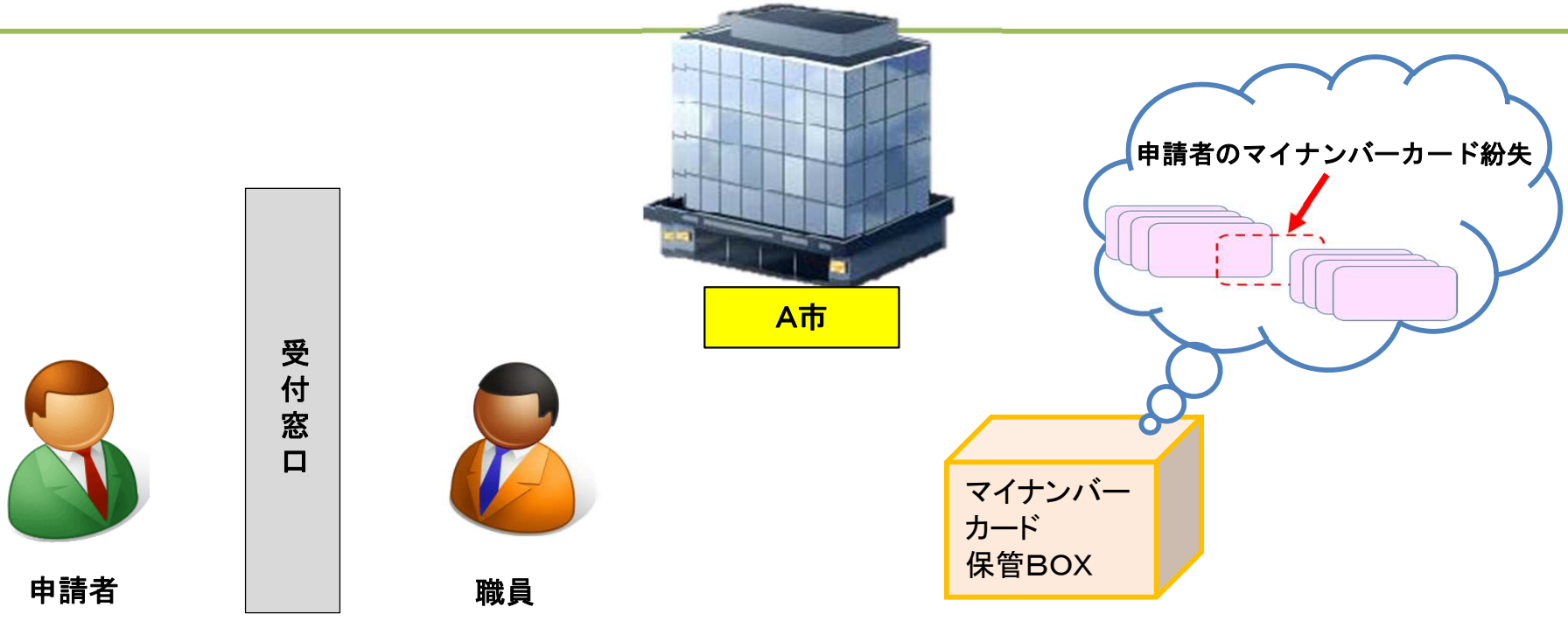


第３節
特定個人情報の適切な取扱いのポイント
～事例から学ぶ～

第2節では、マイナンバー制度の安全対策について学びました。
第3節では、第2節の内容を振り返りながら、事例を通じて、特定個人情報の適正な取扱いについて学んでいきます。
個々の事例について、自分の組織だったらどのような防止策を講じるかなど、自身のことに置き換えて、適切な安全管理措置を考えてみましょう。

事例１　マイナンバーカードの紛失

A市では、マイナンバーカード交付申請者が、カード受取のために来庁した際に、担当職員において交付前のカードを確認したところカードが見当たらず、執務室内を捜索したものの見つからず紛失が発覚した。



事例１　マイナンバーカードの紛失

防止策

紛失の直接の原因は不明ですが、マイナンバーカードの管理状況がよくなかったことが大きな要因と考えられますので、紛失が生じないような管理方法を検討する必要があります。

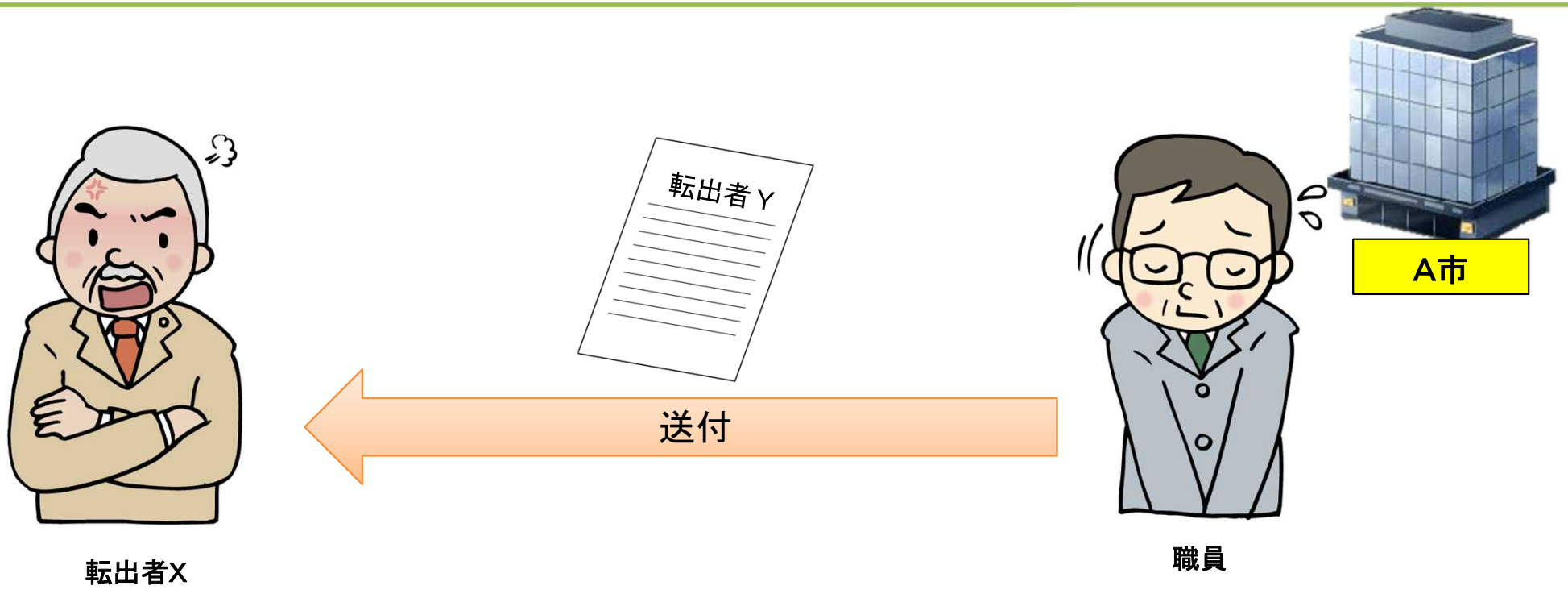
- 持出し状況の記録（持出者、持出日、目的等）を確実に残す
- 鍵付きキャビネットで保管する　　etc

特定個人情報の取扱いに関する監査を行い、管理状況を定期的に確認し、必要な場合には、管理方法の見直しを行うことも重要です。

監査は、事例1に限らず、漏えい等事案の防止のために有効です。
定期的に監査を実施して、安全管理措置の状況を確認し、必要があれば見直しをしましょう！

事例２　誤交付

A市では、郵便によりマイナンバーが記載された転出証明書を送付する際に、誤って転出者本人とは別人の証明書を送付してしまった。



事例２　誤交付

防止策

書類を封入する際のミスと考えられますので、このようなミスを防止するような対策を講じる必要があります。

- 封入する書類の中身と封筒の宛先に誤りがないか、ダブルチェックする
- 封入する際のチェック体制について、マニュアル等で整備する　　etc

同様のミスが起きないように、総括責任者や保護責任者は、事務取扱担当者に対して適切に監督を行うとともに、事務取扱担当者に特定個人情報の取扱いについての教育研修を行い、特定個人情報の保護の意識を高めることも重要です。

特定個人情報を取り扱う上で、必要な安全管理措置が生じた場合には、取扱規程等を見直しましょう。
取扱規程等に盛り込み、かつ、当該規程に基づく取扱いを徹底させることで、安全管理措置を確実に講じることができます。事例2の事案に限らず、他の事案でも同様です。

事例２　誤交付

ガイドライン（別添１）２Db　事務取扱担当者等の教育

次表の教育研修を行うこととされています。

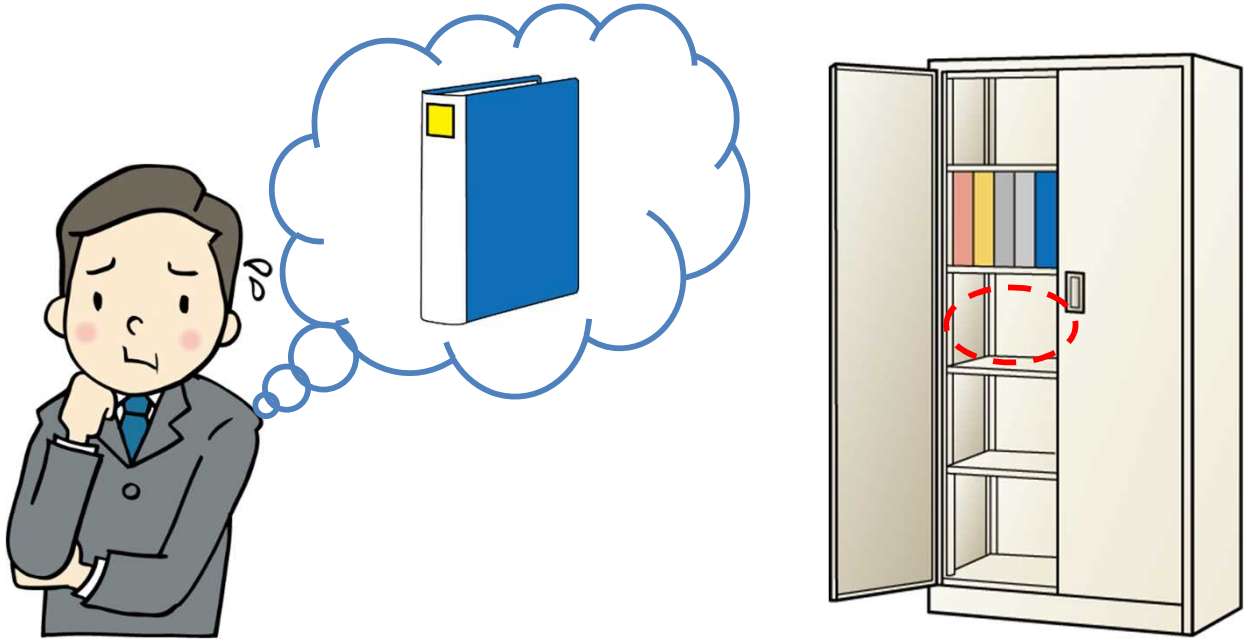
研修内容	研修対象者
特定個人情報等の適正な取扱いに関する研修	事務取扱担当者
情報システムの管理、運用及びセキュリティ対策に関する研修	特定個人情報等を取り扱う情報システムの管理者
課室等における特定個人情報等の適切な管理のために必要な研修	保護責任者
サイバーセキュリティ研修	特定個人情報ファイルを取り扱う事務に従事する者

研修対象者は、受講対象となった研修は必ず受講しましょう。
また、総括責任者等は、受講対象者の受講漏れがないように、出欠状況の確認、未受講者へのフォローアップを確実に行いましょう。

事例３　文書の誤廃棄

書棚の整理の際に、職員から提出された特定個人情報が記録された申請書等を綴った文書ファイルの紛失が発覚した。

※年度末の不要文書の廃棄作業の際に、誤廃棄したと思われる。



事例３　文書の誤廃棄

防止策

文書を誤廃棄した可能性があるということで、誤廃棄を防ぐための対策を講じる必要があります。

- 不要な文書を廃棄する際に、廃棄してはいけない書類が混入してないか、複数人でチェックする
- 必要な文書と不要な文書が混在しないように保管する　　etc

誤廃棄についても可能性にとどまり、明確には分からない状況ですので、文書の取扱状況を把握するための方法を検討する必要があります。

- 文書ファイルの管理簿を作成し、利用状況を把握する
- 文書の廃棄伺いや廃棄目録を作成し、廃棄の記録を保存する　　etc

保存期間が過ぎて不要になった書類は速やかに廃棄し、必ず廃棄の記録を残しましょう。
廃棄を外部に委託する場合には、委託先が確実に廃棄を行ったか証明書等により必ず確認しましょう。

事例４　ＵＳＢメモリの紛失

従業員等の特定個人情報が記録された年末調整用のデータが入ったUSBメモリを、持ち運ぶ際に紛失してしまった。

事例４　ＵＳＢメモリの紛失

防止策

USBメモリを持ち運んだ際に紛失したということですので、安全に持ち運ぶための運搬方法を検討する必要があります。

- 専用の鍵付きの鞄などで運搬する
- 紛失した際の漏えいを防ぐため、持ち運ぶデータの暗号化を行う　　etc

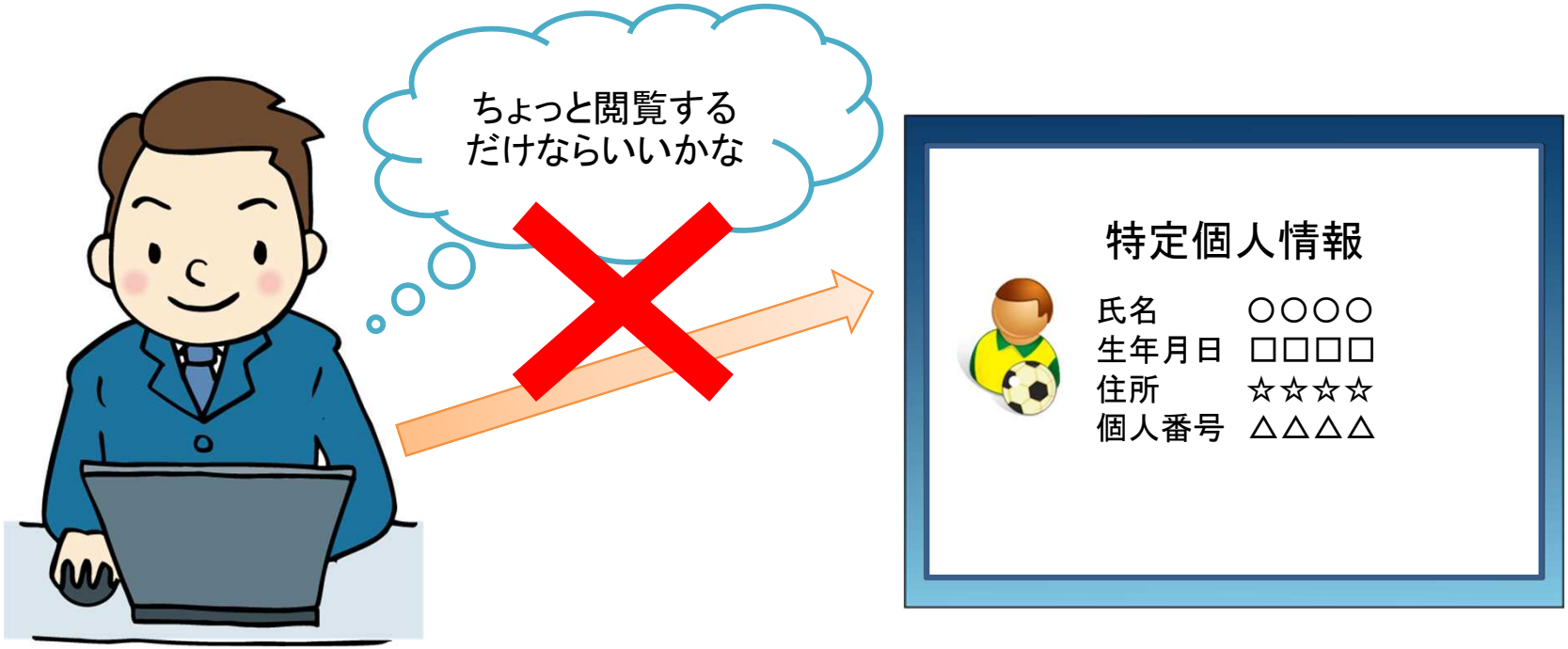
USBメモリ等の電子媒体は大量のデータを保存できることから、紛失した際の影響も甚大となります。そのため、電子媒体の利用を必要最小限に限定するような体制を検討することも重要です。

- 電子媒体を管理者が管理し、使用する際にはルールに基づき許可を申請する
- 許可された電子媒体以外を接続できないように制御する　　etc

USBメモリ等の電子媒体は膨大なデータが保存できるので、紛失した時の影響も甚大です。
許可された電子媒体以外の電子媒体の使用は制限するとともに、業務上やむを得ず電子媒体に特定個人情報を保存して持ち運ぶ必要がある場合には、紛失・盗難防止のための安全策を講じましょう！

事例５　職員による不正な利用

職員が業務に関係なくシステムを使って、有名スポーツ選手の特定個人情報を閲覧した。



事例５　職員による不正な利用

防止策

職員が不正利用をしないように、けん制するための対策などを検討する必要があります。

- システムの利用状況（ログ）を定期的に確認する
- 不正利用をした職員に対して厳正な処分を行う　　etc

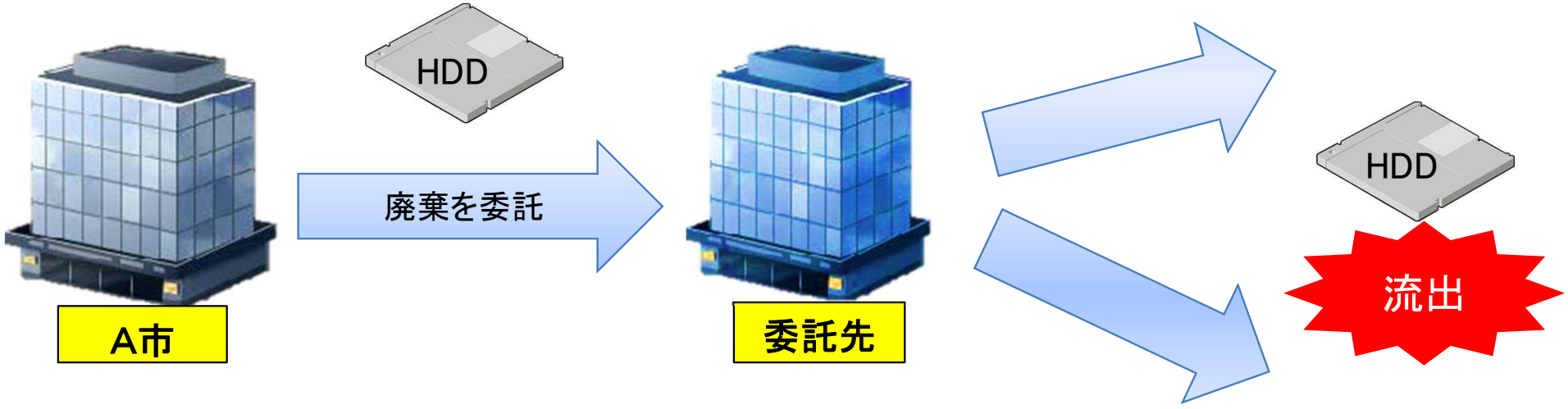
業務上必要のない職員がアクセスしないように、システムへのアクセスを防止する対策を検討する必要もあります。

- システムのアクセス権を、業務上システムの利用が必要な職員にのみ付与する
- システム上の権限を、担当する業務で必要となるものに限定し、アクセス権限を最小化する　　etc

システムを利用して特定個人情報を取り扱う事務を行っている場合には、システムのログについて定期的に分析・確認する必要があります。
また、ログの分析結果を職員に周知することで、不正行為の抑止・けん制となることも期待できます。
アクセス権の管理を適切に行うことも重要です。

事例６　ＨＤＤの流出

A市では、特定個人情報を保存したHDDのデータ削除及び廃棄を委託していたところ、当該HDDが流出していたことが、後日発覚した。



事例６　ＨＤＤの流出

防止策

電子媒体が流出すると、大量の特定個人情報等の漏えいにつながることがあります。そのため、委託先等でのデータ削除・媒体廃棄を確実に把握する必要があります。

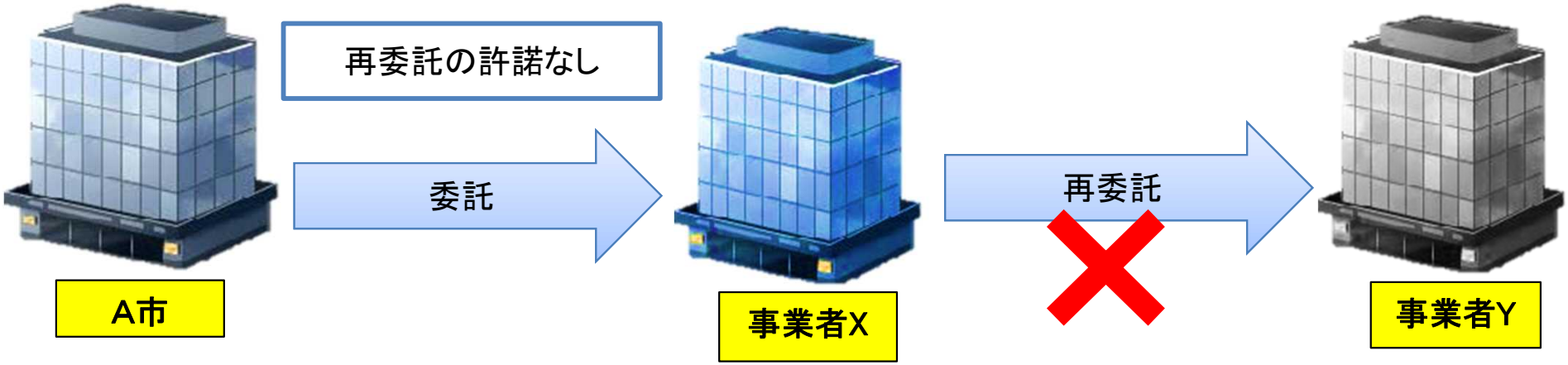
- データ削除・媒体廃棄の完了についての報告書等の証跡を求める
- 委託先でデータ削除・媒体廃棄に立会い確認する　　etc

本事例のように、データ削除・媒体廃棄の作業を委託する際は、復元不可能な状態で削除・廃棄するとともに、確実に削除・廃棄が実施された事実を証明書等により確認する必要があります。
また、自身でデータ削除・媒体廃棄をする際は、復元不可能な手段で削除・廃棄し、削除・廃棄した記録を保存する必要があります。

事例７　無許諾の再委託

A市は、事業者Xに特定個人情報の入力業務を委託していた。

事業者Xは、特定個人情報の入力業務の一部について、A市の許諾を得ずに、事業者Yに再委託していた。



事例７　無許諾の再委託

防止策

事業者Xが再委託の要件（再委託できる場合についての取決め）を把握してなかったことが要因かもしれませんので、再委託の要件を双方で認識するための検討が必要です。
また、委託先の作業状況の確認不足の可能性もあるので、確認体制も整備する必要があります。

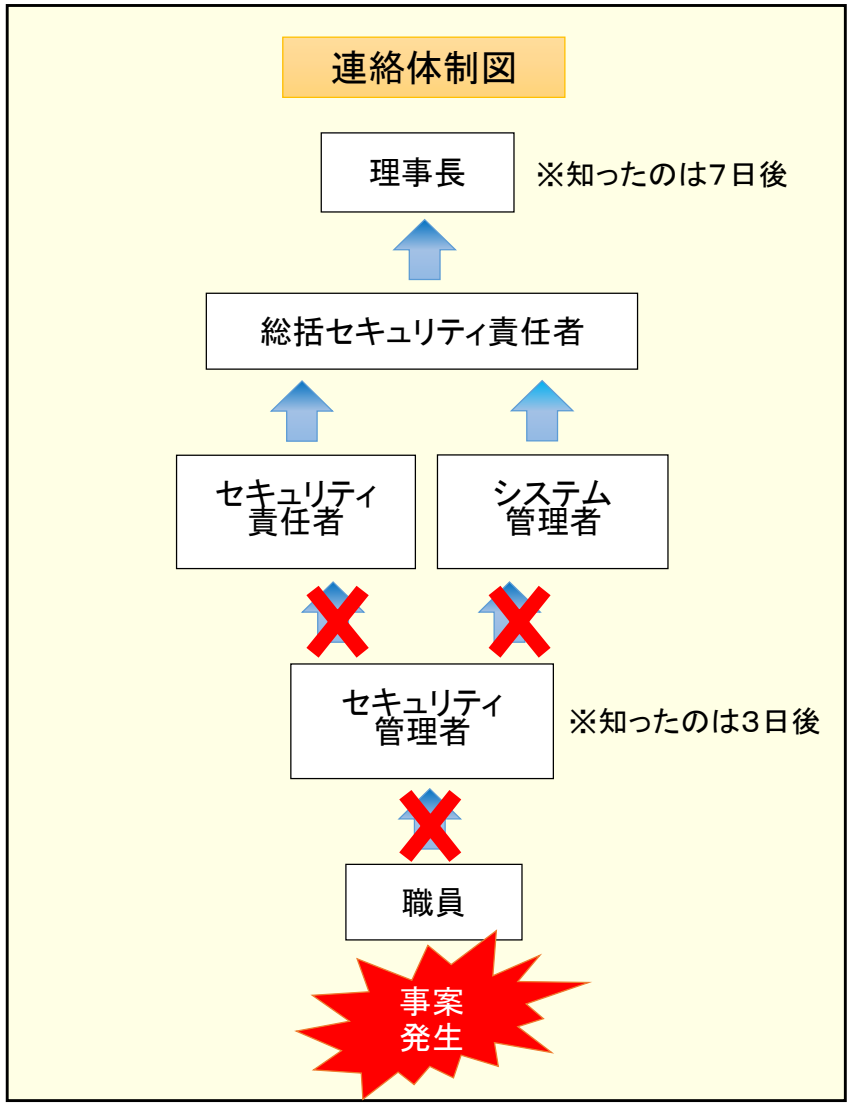
- 再委託の要件について契約書に確実に盛り込む
- 再委託を実施する際には、書面で許諾申請を受け、書面で許諾の可否を通知する
- 委託先に定期的な報告を求めることにより、作業の進捗等を確認する
- 委託先の現地確認をする　　etc

再委託を実施する際には、委託者の許諾を必ず得る必要があります。
委託者の許諾を得ない状態での特定個人情報の再委託先への提供は漏えいに該当します。

事例８　漏えい等事案が発生した際の報告体制

A機構において、漏えい等事案が発生した際の体制を整備していたが、セキュリティ管理者が不在であったため、セキュリティ管理者への報告が事案発生の３日後となった。

セキュリティ管理者に報告後、次の連絡先であるセキュリティ責任者及びシステム管理者が不在であったため、総括セキュリティ責任者と理事長への報告が事案発生の７日後になった。



事例８　漏えい等事案が発生した際の報告体制

防止策

報告先となっている職員が不在時の対応について、ルールが定められていなかったことが要因ですので、報告ルールを確立する必要があります。

- 報告先の職員が不在の場合、上位の職員へ報告するルールを定める　　etc

職員等が、報告ルールに基づいて迅速に対応できるような対策も検討する必要があります。

- 漏えい時の報告フローについて職員に周知する
- 漏えいが発生した場合を想定した訓練を実施する　　etc

漏えい等事案が発生した際には、迅速かつ適切な報告が最も重要です！
漏えい等事案が発生した際の報告先や報告方法を把握し、いざという時に迅速に対応できるようにしておきましょう。
また、特定個人情報の漏えい等が発生した場合には、個人情報保護委員会への報告が必要となりますので、報告体制が整備されているのか確認しておいてください。

第３節　特定個人情報の適正な取扱いのポイント～事例から学ぶ～

＜参考＞【マイナンバーガイドライン（行政機関等編）（別添１）2　講ずべき安全管理措置の内容】

A　基本方針の策定

特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。

B　取扱規程等の見直し等

事例2

特定個人情報等の具体的な取扱いを定めるために、取扱規程等の見直し等を行わなければならない。
特に、特定個人情報等の複製及び送信、特定個人情報等が保存されている電子媒体等の外部への送付及び持ち出し等については、責任者の指示に従い行うことを定めること等が重要である。

C　組織的安全管理措置

行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。

a　組織体制の整備

安全管理措置を講ずるための組織体制を整備する。
行政機関等は、組織体制の整備として、次に掲げる事項を含める。

- 総括責任者（行政機関等に各１名）の設置及び責任の明確化
- 保護責任者（個人番号利用事務等を実施する課室等に各１名）の設置及び責任の明確化
- 監査責任者の設置及び責任の明確化
- 事務取扱担当者及びその役割の明確化
- 事務取扱担当者が取り扱う特定個人情報等の範囲の明確化
- 特定個人情報等の取扱いにおける人的ミスの発生を防止するための確認体制の整備
- 事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制の整備
- 個人番号の漏えい、滅失又は毀損等（以下「漏えい等」という。）事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制の整備
- 特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化

事例5

b　取扱規程等に基づく運用

取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等の利用状況等を記録し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講ずるとともに、分析等を行う。

c　取扱状況を確認する手段の整備

特定個人情報ファイルの取扱状況を確認するための手段を整備する。
行政機関等は、次に掲げる項目を含めて記録する。
なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。

- 特定個人情報ファイルの名称
- 行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
- 特定個人情報ファイルの利用目的
- 特定個人情報ファイルに記録される項目及び本人として特定個人情報ファイルに記録される個人の範囲
- 特定個人情報ファイルに記録される特定個人情報等の収集方法

※　手法の例示の記載は省略しています。

第３節　特定個人情報の適正な取扱いのポイント～事例から学ぶ～

＜参考＞【マイナンバーガイドライン（行政機関等編）（別添１）2　講ずべき安全管理措置の内容】

C　組織的安全管理措置（つづき）

事例8

d　漏えい等事案に対応する体制等の整備
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及び手順等を整備する。
漏えい等事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。

事例1

e　取扱状況の把握及び安全管理措置の見直し
監査責任者は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査（外部監査及び他部署等による点検を含む。）を行い、その結果を総括責任者に報告する。
総括責任者は、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。

D　人的安全管理措置

行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。

事例2

a　事務取扱担当者の監督
総括責任者及び保護責任者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。

b　事務取扱担当者等の教育
総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。
また、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。
総括責任者は、保護責任者に対し、課室等における特定個人情報等の適切な管理のために必要な教育研修を行う。
前記教育研修については、教育研修への参加の機会を付与するとともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。
なお、サイバーセキュリティの研修については、番号法に基づき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、次に掲げるところにより、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。）の確保に関する事項その他の事項に関する研修を行う（番号法29条の2、番号法施行令第32条）。
・　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。
・　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。
・　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5

c　法令・内部規程違反等に対する厳正な対処
法令又は内部規程等に違反した職員に対し、法令又は内部規程等に基づき厳正に対処する。

※ 手法の例示の記載は省略しています。

第３節　特定個人情報の適正な取扱いのポイント～事例から学ぶ～

＜参考＞【マイナンバーガイドライン（行政機関等編）（別添１）2　講ずべき安全管理措置の内容】

E　物理的安全管理措置

行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。

a　特定個人情報等を取り扱う区域の管理

特定個人情報ファイルを取り扱う情報システム（サーバ等）を管理する区域（以下「管理区域」という。）を明確にし、物理的な安全管理措置を講ずる。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。

また、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）について、事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないよう留意する必要がある。

行政機関等は、管理区域のうち、基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合には、情報システム室等について、次の①及び②に掲げる措置を講ずる。地方公共団体等は、次の①及び②に掲げる項目を参考に、適切な措置を講ずる。

①　入退室管理

- 情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員 の立会い等の措置を講ずる。また、情報システム室等に特定個人情報等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。
- 必要があると認めるときは、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずる。
- 必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、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。

②　情報システム室等の管理

- 外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。

事例1

b　機器及び電子媒体等の盗難等の防止

管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。また、電子媒体及び書類等の庁舎内の移動等において、紛失・盗難等に留意する。

事例4

c　電子媒体等の取扱いにおける漏えい等の防止

許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。

取扱規程等の手続に基づき、特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ必要が生じた場合には、容易に個人番号が判明しないよう安全な方策を講ずる。

「持ち運ぶ」とは、特定個人情報等を管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、庁舎内での移動等であっても、特定個人情報等の紛失・盗難等に留意する必要がある。

事例3

d　個人番号の削除、機器及び電子媒体等の廃棄

特定個人情報等が記録された電子媒体及び書類等について、文書管理に関する規程等によって定められている保存期間を経過した場合には、個人番号をできるだけ速やかに復元不可能な手段で削除又は廃棄する。→ガイドライン第４－３－(4)B参照

個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。

※　手法の例示の記載は省略しています。

第３節　特定個人情報の適正な取扱いのポイント～事例から学ぶ～

＜参考＞【マイナンバーガイドライン（行政機関等編）（別添１）2　講ずべき安全管理措置の内容】

F　技術的安全管理措置

行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。

事例5

a　アクセス制御
情報システムを使用して個人番号利用事務等を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。

b　アクセス者の識別と認証
特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。

c　不正アクセス等による被害の防止等
情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。

事例4

d　漏えい等の防止
特定個人情報等をインターネット等により外部に送信する場合、通信経路における漏えい等を防止するための措置を講ずる。
特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。

G　外的環境の把握

行政機関等が、外国において特定個人情報等を取り扱う場合、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、特定個人情報等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。

※　手法の例示の記載は省略しています。

第２章　　保護責任者研修

１－１　保護責任者の役割

保護責任者は、部署内の特定個人情報の保護に関する責任者です。

保護責任者とは

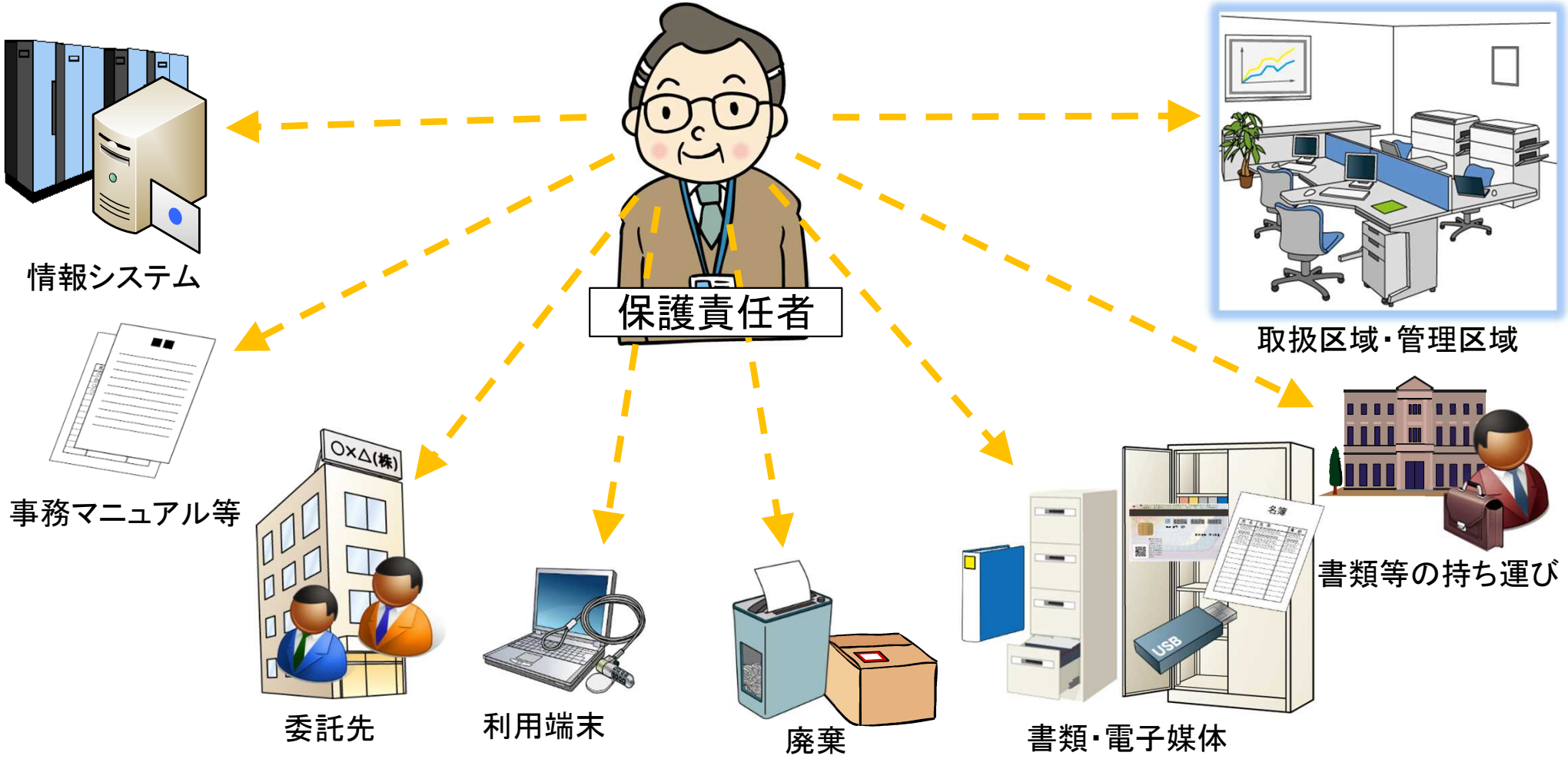
- 特定個人情報の保護のために必要な安全管理措置を講ずるための組織体制の整備として、課室等に各１名設置され、部署内の特定個人情報の保護について責任を負う。
  （マイナンバーガイドライン（行政機関等編）　別添１２Ca）

保護責任者の役割

- 事務取扱担当者の監督（ガイドライン別添１２Da）
  特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。　※「第１章　事務取扱担当者研修」の理解は必要です。
- 事務取扱担当者等の教育（ガイドライン別添１２Db）
  ①事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、その保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。
  ②特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に、特定個人情報等の適切な管理のため、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。
  ③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、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その他の事項に関する研修を行う。

１－２　事務取扱担当者の監督（１）

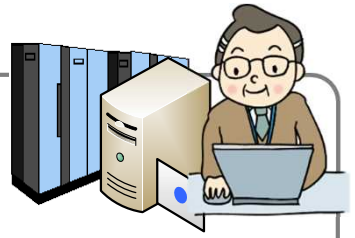
保護責任者は、部署内で特定個人情報が適切に取り扱われるよう、事務取扱担当者が行う業務を監督します。



１－２　事務取扱担当者の監督（２）

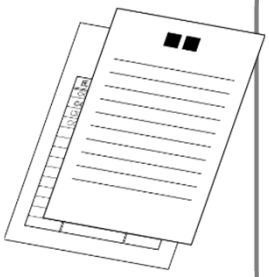
事務取扱担当者の監督に当たっては、次の事項に留意してください。

情報システム



- □ 事務取扱担当者以外に特定個人情報ファイルへのアクセス権を付与していないか
- □ 人事異動等の都度、アクセス権の追加・削除とその確認を行っているか
- □ 情報システムの業務外利用が行われていないか確認するために、ログを定期的に分析・確認しているか　　etc

事務マニュアル等



- □ 事務取扱担当者を指定し、役割を明確にしているか
- □ 人事異動や臨時職員雇用の都度、事務取扱担当者の指定が行われているか
- □ 事務マニュアルを適宜見直し、必要に応じて改訂等を行っているか
- □ 特定個人情報の漏えい等が発生した場合の報告体制を整備し、部署内へ周知しているか　　etc

１－２　事務取扱担当者の監督（３）

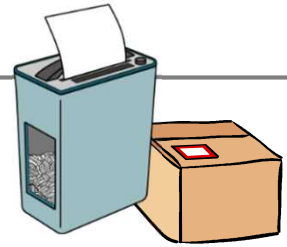
委託先

- 委託先の安全管理措置の状況を確認し、適切に選定しているか
- 再委託を許諾する場合、再委託先の安全管理措置の状況を確認しているか
- 委託期間中に委託先から契約内容の遵守状況について報告を受けているか
- 委託先が書類や電子媒体を廃棄する場合、証明書等により廃棄の事実を確認しているか　　etc

利用端末

- 端末の盗難・紛失を防止するために、セキュリティワイヤ等による固定を行っているか
- 端末を固定できない場合は、退庁時に施錠できるキャビネット等に保管しているか　　etc

廃　棄



- 保存期間を経過した個人番号の記載された書類等は、速やかに廃棄しているか
- 復元不可能な方法でデータの削除や書類・電子媒体の廃棄を行っているか
- 削除・廃棄の記録を残しているか
- 削除・廃棄を委託した場合は、証明書等により廃棄の事実を確認しているか　　etc

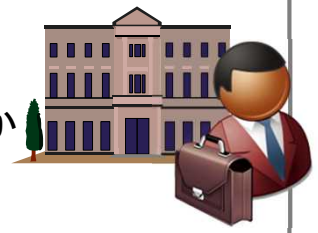
１－２　事務取扱担当者の監督（４）

書類・電子媒体

- □ 許可した電子媒体以外の使用や端末への接続を制限しているか
- □ 電子媒体を施錠できるキャビネットや書庫等に保管しているか
- □ 書類・電子媒体を持ち運ぶ場合には、記録を残しているか　　etc

書類等の持ち運び

- □ 電子媒体を持ち運ぶ場合は、データの暗号化等を行っているか
- □ 書類の場合は、封かん、目隠しシールの貼付などで特定個人情報等が容易に見えないようにしているか
- □ 庁舎内での移動であっても、紛失・盗難等が起こらないよう気をつけているか　　etc



取扱区域・管理区域

- □ 窓口等では、第三者からの閲覧を防止する措置がとられているか
- □ 事務取扱担当者以外の職員が容易に閲覧できる状況になっていないか
- □ 誤廃棄が起こらないよう保存書類と廃棄書類を分けて保管するようにしているか
- □ 管理区域は、入退室の記録、部外者が入る場合の立会い・監視設備の設置等が行われているか　etc

１－３　事務取扱担当者等の教育

保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行います。

教育研修の種類（ガイドライン（別添１）２Db）

- 事務取扱担当者への教育研修
- 情報システムの管理に関する事務に従事する職員への教育研修
- 保護責任者に対する研修※
- 特定個人情報ファイルを取り扱う事務に従事する者への研修

保護責任者の役割

研修実施期間前 ： 研修対象者を把握し、研修参加者を指名する。

研修実施期間中 ： 研修対象者を研修に参加させる。
受講状況を適宜確認し、未受講の対象者が期間内に受講するよう促す。

研修実施期間後 ： やむを得ず研修を受講できなかった職員へフォローアップを実施する。
新規採用者や他部署からの異動者への個別研修を行う。

※総括責任者が保護責任者に実施

２　総括責任者の役割

総括責任者は、特定個人情報等を取扱う部署の保護責任者と事務取扱担当者が特定個人情報を適切に取り扱っているか、監査等を通じて確認する必要があります。

監査結果に対する責任（ガイドライン別添1 2 Ce）

- 監査責任者は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査を行い、その結果を総括責任者に報告する。
- 総括責任者は、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。

組織全体の監督

- 特定個人情報等の取扱いに係る規程等が整備されているか把握する。
- インシデント発生時の報告体制を整備する。

組織全体の特定個人情報等の取扱いについて、統括的に責任を負う総括責任者との確実な連絡体制を整備することは、インシデント発生時の対応等を含め重要です。
保護責任者は、総括責任者の役割についても理解しておきましょう。

章末テスト
（第１章、第２章）

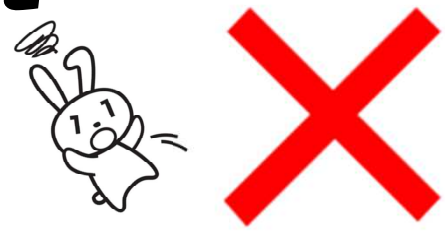
マイナンバー理解度テスト　問題１

窓口の申請手続で、マイナンバーカードの両面がコピーされたものが身分証明書の写しとして提出された。マイナンバーは申請に必要ないが、本人から提出されたものなので受け取って問題ない。

○ or ×

マイナンバー理解度テスト　問題１

こたえ



特定個人情報の利用は、マイナンバー法で限定されており、規定される以外の目的で個人番号の収集・保管、特定個人情報ファイルを作成することは禁止されています。

たとえ本人の同意があったとしても、マイナンバー法で認められる場合以外は、個人番号を利用等することはできません。

マイナンバー理解度テスト　問題２

特定個人情報が記載された文書を年度末に廃棄した。廃棄した文書は不要となったものなので、廃棄の記録は残さなくてもよい。

○ or ×

マイナンバー理解度テスト　問題２

こたえ

特定個人情報が記録された文書や電子媒体を廃棄した場合は、どのように廃棄したのか記録（いつ、誰が、何を、どのような方法で廃棄したのか）を残す必要があります。

また、廃棄作業を外部事業者に委託する場合には、委託先から廃棄証明書等を提出してもらう等により、確実に廃棄が実施されたことを確認する必要があります。

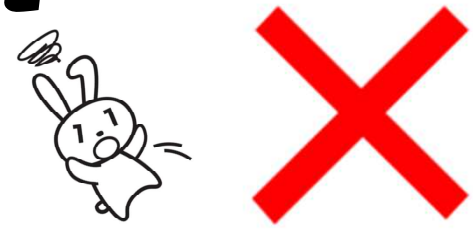
マイナンバー理解度テスト　問題３

　マイナンバーカードの交付数が急増したため、一時的に他部署の職員に交付業務を手伝ってもらうことにした。一時的な作業なので、事務取扱担当者に指定しなくてよい。

○ or ×

マイナンバー理解度テスト　問題３

こたえ



一時的な作業協力であったとしても、特定個人情報を取り扱う場合には、事務取扱担当者に指定する必要があります。
業務の繁忙期等で他部署の職員に業務の応援等を依頼する際には、指定漏れのないよう注意して下さい。

また、非常勤職員や臨時職員についても、特定個人情報を取り扱う場合には、事務取扱担当者に指定する必要がありますので、都度指定するよう留意してください。

マイナンバー理解度テスト　問題４

特定個人情報を取り扱う情報システムのログは、不正アクセスなどの問題が起きたときに確認・分析するだけでは不十分である。

○ or ×

マイナンバー理解度テスト　問題４

こたえ

○

特定個人情報を取り扱う情報システムの利用状況（ログイン・アクセス履歴）を記録したログの分析等は、定期的に実施する必要があります。

ログの分析等は、外部からの攻撃だけでなく、職員による不必要な閲覧等を防ぐ観点からも有用です。定期的に実施していることを職員に周知することにより、不正利用を牽制する効果も期待できます。

参考：特定個人情報等の利用状況のログ分析・確認について（令和４年４月　個人情報保護委員会事務局）
（https://www.ppc.go.jp/files/pdf/log_bunseki.pdf）

第３章　　サイバーセキュリティ研修

はじめに

　サイバー攻撃による情報漏えいのニュースを最近よく耳にすると思いますが、その手口は巧妙かつ悪質なものとなっており、ますます被害が拡大しています。
　そのため、マイナンバーを含む多くの個人情報を取り扱っている我々は、サイバーセキュリティについての意識を強く持ち、脅威やリスクについて十分に理解しておく必要があります。
　本章では、特に近年、組織として注意が必要なサイバーセキュリティの脅威を知ってもらうとともに、脅威への対策としてどのようなことが考えられるかを中心に学んでいきます。

情報セキュリティの　「　三大要素　」

　情報セキュリティとは、情報資産の「機密性（Confidentiality）」「完全性（Integrity）」「可用性（Availability）」（ＣＩＡ）を維持することです。
　ＣＩＡを維持することにより、保有する情報資産の正確性や信頼性が向上します。

機密性　…認められた者だけが、情報にアクセスできる状態を確保すること
完全性　…情報が破壊、改ざん又は消去されていない状態を確保すること
可用性　…認められた者が、必要な時に中断することなく情報にアクセスできる状態を確保すること

情報資産の種類	情報資産の例
①ネットワーク	通信回線、ルータ等の通信機器等
②情報システム	サーバ、パソコン、モバイル端末、汎用機、OS、ソフトウェア等
③上記①・②に関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
④電磁的記録媒体	サーバ装置、端末、ハードディスク、USBメモリ、DVD－R、磁気テープ等
⑤ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。）
⑥システム関連文書	システム設計書、プログラム仕様書、端末管理マニュアル、ネットワーク構成図等

※総務省「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（令和４年３月版）」図表10より引用（情報資産の例は一部抜粋）

サイバーセキュリティとは、上記「ＣＩＡ」の脅威となる原因に対処する考え方です。
次節では、脅威とその手口について具体的事例を紹介します。

事例１　ランサムウェアによる被害

　ランサムウェアとはウイルスの一種で、ＰＣやサーバ、スマートフォンがこのウイルスに感染すると、保存されているデータが暗号化されて利用できなくなったり、画面がロックされて端末が利用できなくなったりします。そして、それを復旧することと引き換えに金銭を要求される等の被害が発生します。
　さらに、暗号化だけではなく、重要な情報を窃取されることもあり、その情報を公開すると脅すなど、複数の脅しを組み合わせることで、ランサムウェアに感染した組織が金銭を支払わざるを得ない状況を作り出そうとします。

※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

＜攻撃手口＞

●メールから感染させる

メールの添付ファイルやメール本文中のリンクを開かせることで感染させる。

●ウェブサイトから感染させる

脆弱性等を悪用しランサムウェアをダウンロードさせるよう改ざんしたウェブサイトや攻撃者が用意したウェブサイトを閲覧させることで感染させる。

●脆弱性を悪用しネットワークから感染させる

ソフトウェアの脆弱性が未対策のままインターネットに接続されている機器に対して、その脆弱性を悪用してインターネット経由で感染させる。

●公開サーバに不正アクセスして感染させる

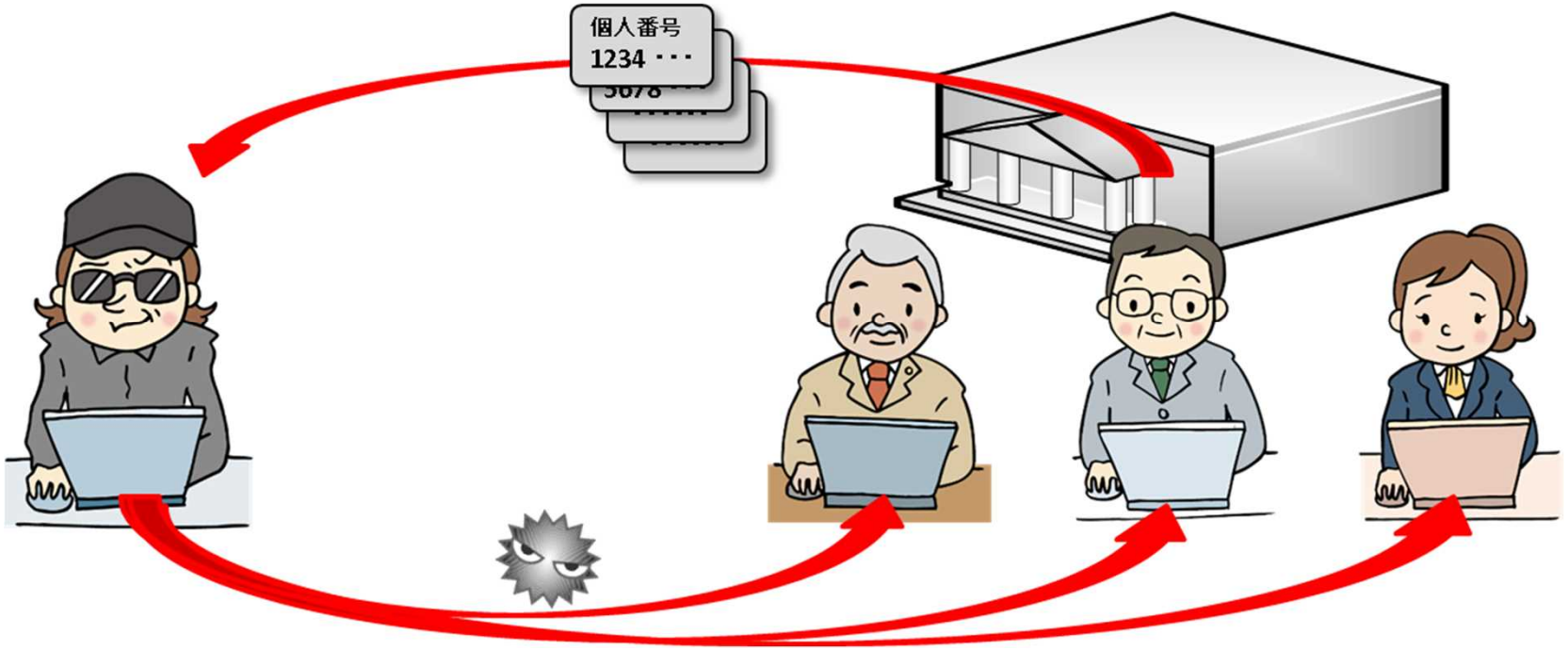
意図せず外部公開されているリモートデスクトップポートに不正ログインし感染させる。

※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

事例２　標的型攻撃による機密情報の窃取

企業や民間団体そして官公庁等、特定の組織から機密情報等を窃取することを目的とした標的型攻撃が継続して発生しています。

攻撃者は社会の変化や、働き方の変化に便乗し、状況に応じた巧みな手口で金銭や機密情報等を窃取します。



※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

＜攻撃手口＞

●メールへのファイル添付やリンクの記載

メールの添付ファイルやメール本文に記載されたリンク先にウイルスを仕込み、それらを開かせることでＰＣをウイルスに感染させる。本文や件名、添付ファイル名は業務に関連するような内容に偽装され、実在する組織の差出人名が使われる場合もある。また、複数回のメールのやりとりで油断させ、不審を抱かれにくいようにする手口が使われる。（やり取り型攻撃）

●ウェブサイトの改ざん

標的組織が頻繁に利用するウェブサイトを調査し、ウェブサイトを改ざんする。従業員がそのウェブサイトにアクセスするよう誘導することで、ＰＣがウイルスに感染する。（水飲み場型攻撃）

●不正アクセス

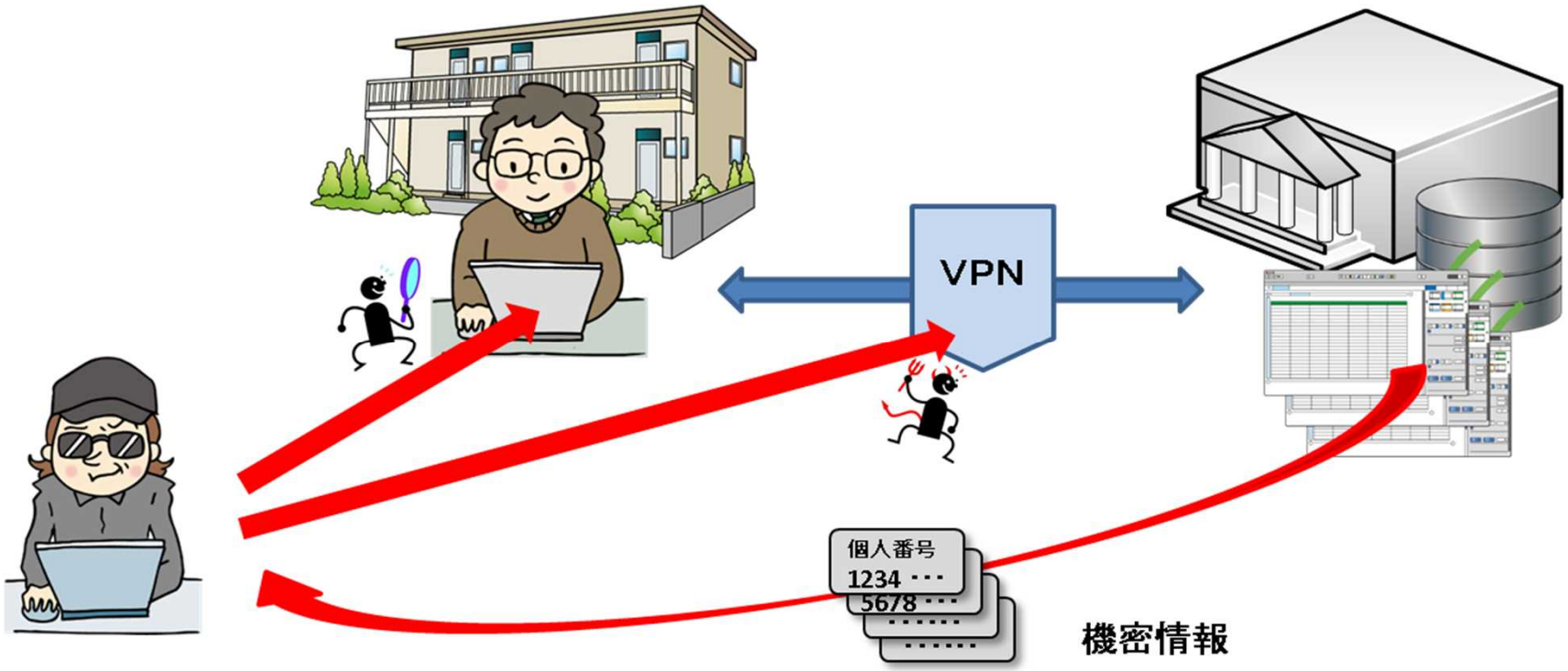
標的組織が利用するクラウドサービスやウェブサーバ、ＶＰＮ*（Virtual Private Network）等の脆弱性を悪用して不正アクセスし、認証情報等を窃取する。窃取した認証情報等を悪用して正規の経路で組織のシステムへ侵入し、ＰＣやサーバをウイルスに感染させる。

*VPNとは、一般的なインターネット回線を利用して作られる仮想のプライベートネットワークです。

※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

事例３　テレワーク等のニューノーマルな働き方を狙った攻撃

勤労形態としてテレワークが活用され、ウェブ会議サービスやＶＰＮ等の本格的な活用がされる中、それらを狙った攻撃が行われています。



※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

＜攻撃手口／発生要因＞

●テレワーク用製品の脆弱性の悪用

ＶＰＮ等のテレワーク用に導入している製品の脆弱性や設定ミス等を悪用し、社内システムに不正アクセスしたり、ＰＣ内の業務情報等を窃取したりする。また、ウェブ会議サービスの脆弱な設定を悪用し、ウェブ会議をのぞき見する。

●テレワーク移行時のまま運用している脆弱なテレワーク環境への攻撃

規則の整備やセキュリティ対策が不十分な状態で、急いでテレワークへ移行したまま運用されている脆弱なテレワーク環境を攻撃する。

●私有端末や自宅のネットワークを利用

適切なセキュリティ対策が施されていない私有端末でテレワークを行うと、ウイルスに感染したり、攻撃者にソフトウェアの脆弱性を悪用され、業務情報や認証情報を窃取されたりするおそれがある。

また、組織支給の端末を利用している場合でも、自宅やシェアオフィスのネットワーク環境に適切なセキュリティ対策が行われていないと、情報を盗聴されるおそれがある。

※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

事例４　内部不正による情報漏えい

組織に勤務する従業員や元従業員等の組織関係者による機密情報の持ち出しや悪用等の不正行為が発生しています。また、組織内における情報管理のルールを守らずに情報を持ち出し、紛失や情報漏えいにつながるケースも散見されます。

組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失により、組織に多大な損害を与えます。

また、不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがあります。

※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

＜攻撃手口＞

●アクセス権限の悪用

付与されたアクセス権限を悪用し、組織の重要情報を窃取する。必要以上に高いアクセス権限が付与されている場合、より重要度の高い情報が窃取され、被害が大きくなるおそれがある。

また、複数人で端末やアカウントを共用している場合、他人のアカウントに紐づくアクセス権限で不正アクセスされることもある。

●在職中に割り当てられたアカウントの悪用

組織の離職者が、在職中に使用していたアカウントを悪用し、組織内部の情報を窃取する。

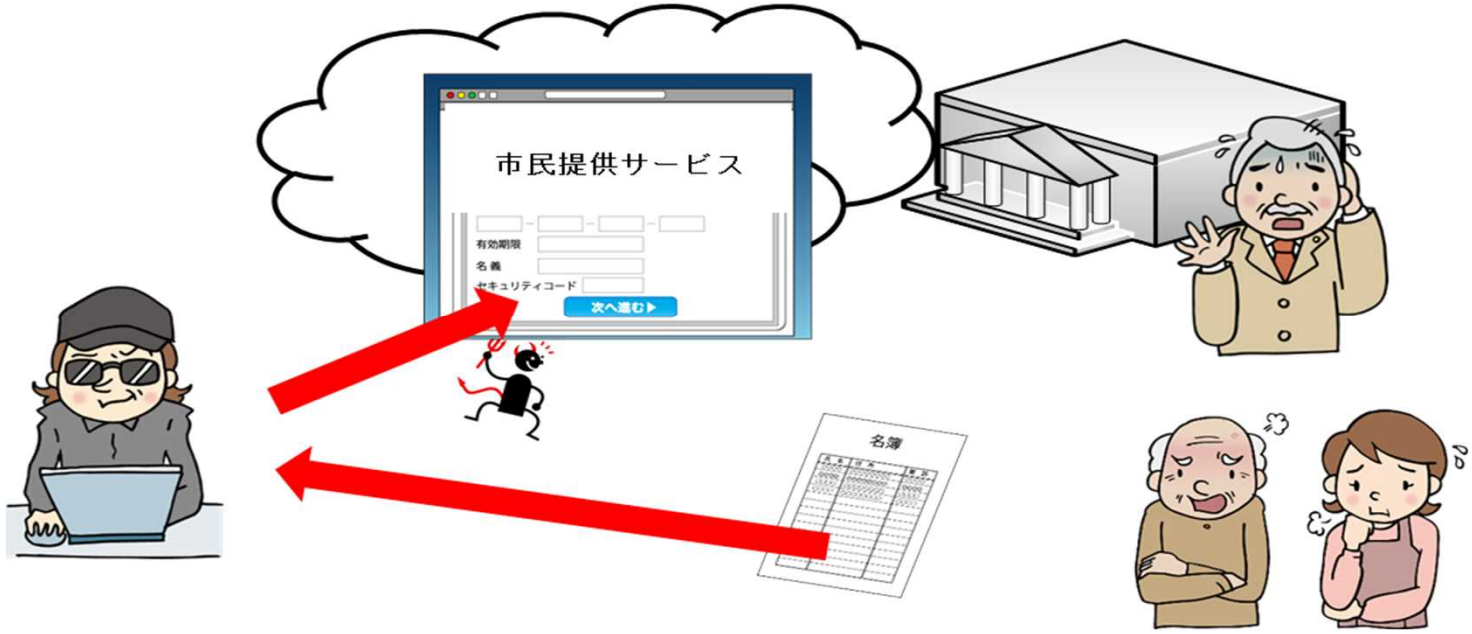
●内部情報の不正な持ち出し

組織内部の情報を、ＵＳＢメモリやＨＤＤ等の外部記憶媒体、メール、クラウドストレージ、スマホカメラ、紙媒体等を利用し、外部に不正に持ち出す。

※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

事例５　インターネット上のサービスへの不正ログイン

インターネット上のサービスへ不正ログインされ、個人情報や決済情報等の重要情報が窃取される被害が確認されています。別のサービスのアカウントと同じパスワードを使い回す利用者を狙ったパスワードリスト攻撃による不正ログインが行われています。また、不正ログインで得た情報を悪用してさらに被害を拡大させるおそれがあります。

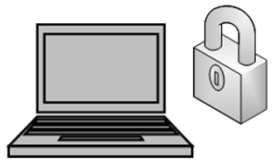


※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

＜攻撃手口＞

●パスワードリスト攻撃

　不正に入手したＩＤやパスワードのリストを使用し、自動的に入力するプログラム等を用いて、ログイン機能を持つインターネット上のサービスにログインを試みる。複数のサービスでＩＤとパスワードを使いまわしていると、１つのサービスでＩＤとパスワードが流出した場合、それら全てのサービスでログインされるおそれがある。

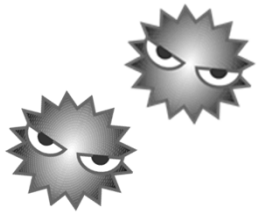


●パスワード推測攻撃

　使われやすいパスワードを推測し、そのパスワードでログインを試みる。例えば、芸能人や知人の個人情報（氏名、誕生日等）からパスワードを類推して、ログインを試みる。

●ウイルス感染

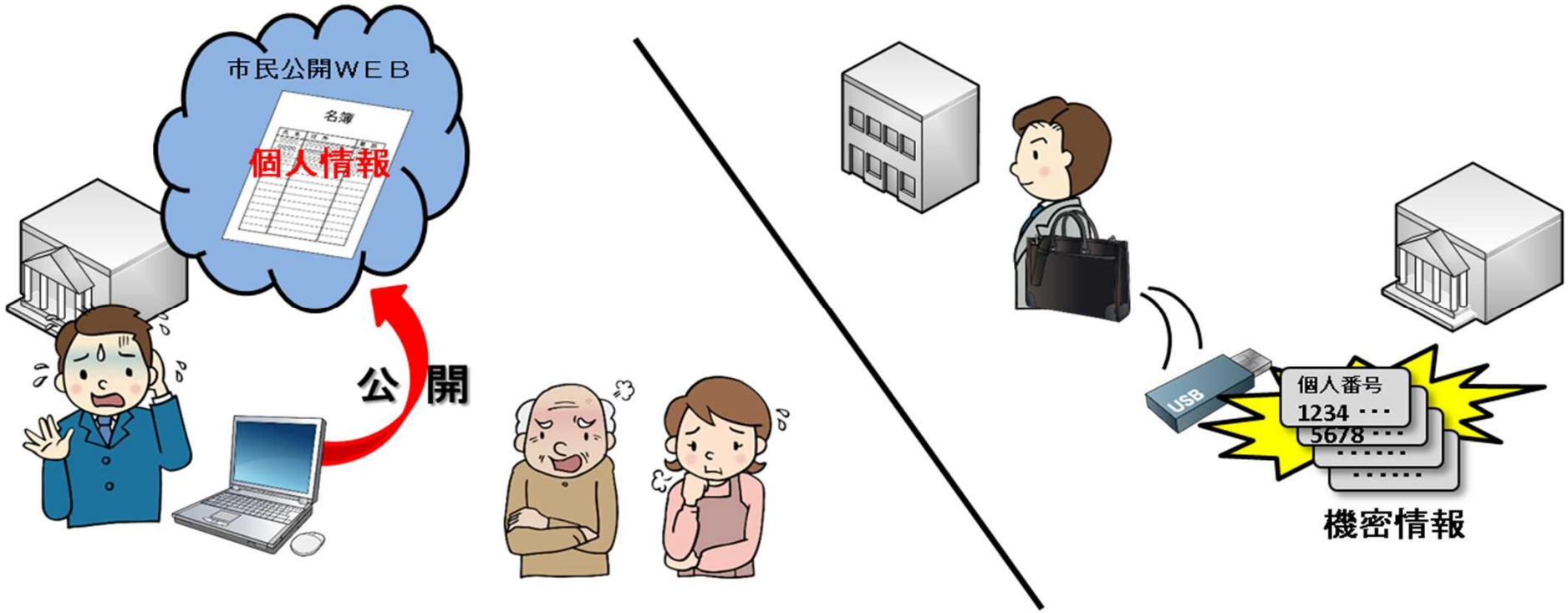
　サービスの利用者に悪意あるウェブサイトやメールに添付されたファイルを開かせることで、使用している端末をウイルスに感染させる。その後、利用者がその端末でサービスにログインすることで、その時入力したＩＤやパスワードを窃取し、その認証情報で不正ログインする。



※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

事例６　不注意による情報漏えい等の被害

メールの誤送信や記録端末や記録媒体の紛失等の不注意による個人情報等の漏えいが発生しています。漏えいした情報が第三者に売買されるとさらなる悪用につながるおそれもあります。情報漏えいした組織は社会的信頼の失墜や経済的な損失につながるおそれもあり、組織はデータに対して慎重な扱いが求められます。



※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

第２節　組織における主な脅威

＜要因＞

●取扱い者の情報リテラシーの低さ

　自身の扱う情報の機密性や重要性等を理解していないために、不用意に外部へ情報漏えいしてしまう。例えば、重要情報が記載されたメールの宛先間違いや重要情報が入った端末の紛失等。また、重要情報を私的に利用して外部のサイト等に公開することで情報漏えいにつながるケースもある。

●情報を取り扱う際の本人の状況

　体調不良や多忙等、情報を取り扱う従業員が置かれた状況から注意力散漫になり、メールの誤送信等のミスによる情報漏えい事故を起こしてしまう。

●組織規程及び取扱プロセスの不備

　組織で制定している情報の取扱プロセスに不備があると情報漏えいが起きやすい。例えば、外部に情報を持ち出す際の確認手順や作業時の確認手順等に関するプロセスの不備が挙げられる。

●誤送信を想定した偽メールアドレスの存在

　組織が利用しているドメインと似たようなドメインのメールアドレスを第三者によって準備され、従業員が誤送信したタイミングで情報が漏えいする。

※独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023 解説書」を基に作成（ https://www.ipa.go.jp/security/10threats/10threats2023.html ）

第３節　脅威への対策

第２節では、**主な脅威とその攻撃手口や要因**について学びました。
第３節では、脅威に対してどのような対策を実施する必要があるのかを学びます。

サイバーセキュリティ対策の分類として、

人的・技術的・物理的

という３つ観点からの対策がありますので、順番に見ていきたいと思います。

第３節　脅威への対策

＜人的対策＞

職員のミスや不正など、人によるセキュリティリスクに対応するための対策です。
組織全体のセキュリティ対策への取組の方針や体制等を策定し運用します。

●情報セキュリティ教育

　どのようなインシデントにおいても、背景には人が関わっています。職員の作業ミスを防いだり、不正に情報を持ち出すようなモラル低下によるインシデントを引き起こさないためにも、職員の情報リテラシーや情報モラルの向上に努めることが必要です。

●マニュアル・ルールの整備

　ミスを防ぐには、確立した手順に基づいて作業を行うことが効果的です。作業手順のマニュアル化や各種ルールの明確化、決められたルール等の周知などを行うことが大切です。
　また、懲戒処分等について明確化することも、不正を防ぐという面で効果的です。

＜技術的対策＞

システムやデータ、ネットワークなどのセキュリティリスクに対して、ハードウェアやソフトウェアから対応する対策です。
ウイルス対策や暗号化のような技術を利用します。

●ツールやシステムの導入・設定

セキュリティソフトなどを導入し、守りを固めることが大切です。
次のような対策が挙げられます。

- ウイルス対策ソフトの導入・最新バージョンへの更新（ウイルス対策）
- ファイアウォールや侵入検知システムなどの設置・構築（不正アクセス対策）
- ログ監視ツールの導入（不正アクセス等の監視）
- アクセス制御（権限の管理）
- 暗号化機能付ＵＳＢメモリ等の利用（情報漏えい防止）
- バックアップを通常利用するネットワークから切り離して管理（バックアップの取得）

＜技術的対策＞ つづき

●ルール化

　ツールやシステムの導入には、それなりのコストがかかったり、現状システムへの影響を与える可能性がありますが、次のような方法も技術的対策です。

- OSやソフトウェアが最新の対策にアップデートされた状態で端末を利用
- データの取扱いに関するルールの明確化（外部記憶媒体へのデータ書き出し不可など）
- パスワードを付箋にメモして端末等に貼らない
- 実行形式ファイル（.exe）が添付されたメールの送受信禁止

＜物理的対策＞

不法侵入や破壊、紛失や災害などの物理的なセキュリティリスクに対応するための対策です。
監視カメラの設置や警備員の配置のような方法により行います。

●事務室のセキュリティ向上等

代表的な例は次のとおりです。

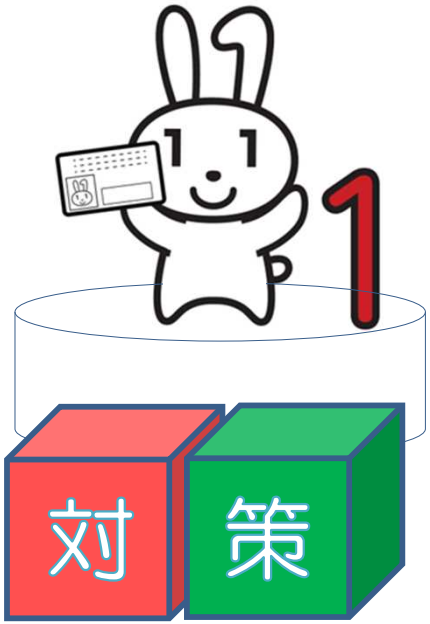
- 出入口のスマートロック・生体認証等の導入
- 監視カメラの設置
- 警備員の配置や警備システムの導入
- パーテーション等を利用し外部からののぞき見防止
- 端末の盗難防止対策（セキュリティワイヤによる施錠等）
- バックアップの遠隔地保管

＜物理的対策＞ つづき

●ルール化

何かを設置したりするだけが物理的対策ではありません。次のような仕組みも対策として考えられます。

- 入退室等の記録
- 外部作業員入室時の職員の立会い
- 部外者の識別化（職員証・入館証の明示）



●災害対策

災害などによる被害も物理的なセキュリティリスクです。

- スプリンクラーや消火器の設置
- 予備電源の準備
- 避難訓練

情報セキュリティマネジメント

　第２節の事例は、数多くある情報セキュリティの脅威の一例を紹介したものです。取り巻く環境や対応すべき脅威は、日々変化しています。
　情報セキュリティを確保するため、「**ＰＤＣＡサイクル**」を繰り返し行い、適切な対策に見直していくことが大切です 。

策定（Plan）
- ✓ 基本方針・対策基準（ポリシー）の策定
- ✓ 実施手順の策定

導入・運用（Do）
- ✓ 人的・技術的・物理的対策
- ✓ 障害時の対応策を実施

監視・見直し（Check）
- ✓ システムの監視
- ✓ ポリシーの遵守状況評価等

維持・改善（Act）
- ✓ システムの改善・対策
- ✓ ポリシーの改善

最　後　に

どんなに高いセキュリティ対策を講じても、巧妙化したサイバー攻撃に対応するためには、職員一人一人のセキュリティ意識を高めていくことが必要です。

＜事務取扱担当者、保護責任者＞

- 怪しいメールのファイルは開かない、ＵＲＬをクリックしない
- 業務で利用するＰＣのウイルス対策ソフトを最新化しましょう
- 業務上必要ない私用ＰＣの利用や資料の持ち出しはやめましょう
- 紹介しているような事例を見つけたら、すぐに上司や責任者に報告しましょう

＜情報システムに関する事務に従事する者＞

- アカウントやアクセス権の棚卸を年1回はしましょう
- 情報システムのＯＳやソフトウェアの最新化をしましょう
- 情報システムでの作業は記録やログに残しましょう
- 紹介しているような事例を見つけたら、すぐに上司や責任者に報告しましょう

どうしてセキュリティ対策が必要なのか、それぞれがよく理解することが大切です。

章末テスト
（第３章）

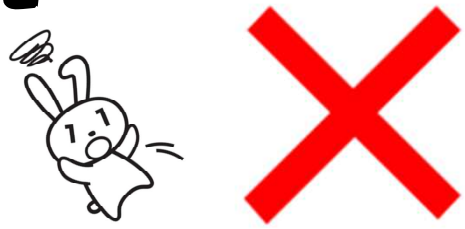
サイバーセキュリティ理解度テスト　問題１

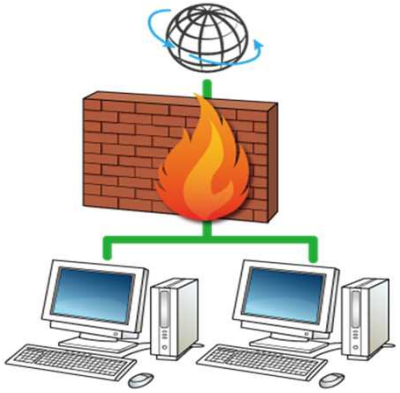
　情報システムやシステムを構成する機器にセキュリティ対策ソフトウェア等を一旦導入すれば、その後はセキュリティ対策ソフトウェア等を更新する必要はない。

○ or ×

サイバーセキュリティ理解度テスト　問題１

こたえ





セキュリティ対策ソフトウェアを最新の状態に更新することは、ウイルスを検知するために必要なことです。

また、その他のソフトウェア等についても、自動更新機能等を活用し、最新の状態にすることにより脆弱性を排除できるため、外部からの不正アクセス等に対する対策になります。

それ以外にも、情報システムのログインログやアクセスログを定期的に分析・確認することにより、外部からの不正アクセス等を検知することができるほか、内部不正の早期発見や不正の抑止につながる可能性があります。

サイバーセキュリティ理解度テスト　問題２

自宅でテレワークを行う際は、限られた空間であるため、職場よりも情報漏えいのリスクは低減されると考えられる。

○ or ×

サイバーセキュリティ理解度テスト　問題２

こたえ

自宅ならではの「情報漏えい」リスクとしては、以下のことが考えられます。

・自宅での使用のために持ち出した業務用パソコンや電子記憶媒体の紛失
・自宅で使用しているWi-Fi機器の脆弱性
・上司や周りの職員の監視がないための内部不正
・紛れ込んんだ悪意あるメールの開封（メールでのやりとりが多くなることに起因した注意不足）　など

職場の整備された環境外では、情報漏えいのリスクが高くなるということを意識しましょう。

サイバーセキュリティ理解度テスト　問題３

　システムやサービスごとに異なるパスワードを設定すると、パスワードを忘れてしまうおそれがあるため、パスワードは１つにまとめた方がよい。

○ or ×

サイバーセキュリティ理解度テスト　問題３

こたえ

パスワードは各システムや各サービスで異なるものを設定しましょう。

１つのサービスでＩＤとパスワードが流出した場合、パスワードリスト攻撃を受けて、他のシステムやサービスで不正にログインされるおそれがあります。

正規の経路でログインされた場合、そのアクセスが正規のアクセスなのか不正アクセスなのかを判断することが難しく、知らぬ間に被害が拡大してしまうおそれがあります。

また、個人情報（氏名、誕生日等）から容易に推測できるようなパスワードを設定すると、パスワード推測攻撃により、不正にログインされてしまうおそれがあります。

そのほか、１つのアカウントを複数の職員で共有しない、異動や退職等により使用しなくなったアカウントは削除するなど、アカウント管理も大切です。

最後までお付き合いいただきありがとうございました

（次ページのまとめテストに解答すれば研修終了です）

まとめテスト

所　属	氏　名

No	問題	解答 (○×)
1	マイナンバー制度では、各行政機関等が保有している個人情報を特定の機関に集約して、その集約した個人情報を各行政機関が閲覧する「一元管理」の方法を採用している。	
2	マイナポータルを利用すれば、「行政機関の手続の検索・申請」をすることができる。	
3	特定個人情報ファイルを取り扱う事務に従事する者は、サイバーセキュリティ研修を受講しなければならない。	
4	電子記憶媒体は、紛失しても買い替えればまた手に入れられるため、たとえ大量の特定個人情報を扱っていたとしても、紛失等の心配をすることなく気軽に扱ってもよい。	
5	ガイドライン別添１Ｄｂ「総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。」という記述は、組織的安全管理措置に関する記述である。	
6	特定個人情報の漏えいが発生した場合には、個人情報保護委員会への報告が必要となる。	
7	情報セキュリティとは、一般的には情報資産の機密性、完全性、可用性及び普遍性を確保することと定義されている。	
8	このウイルスに端末やサーバが感染することにより、保存されているデータが暗号化されて利用できなくなったり、画面がロックされて端末が利用できなくなったりする。そして、それを復旧することと引き換えに攻撃者から金銭を要求される等の被害が発生する。このウイルスをウェアハウスという。	
9	メールの添付ファイルやリンク先にウイルスを仕込み、それらを開かせることでＰＣをウイルスに感染させる。本文や件名等は業務に関連するような内容に偽装され、また、実在する他の組織名によって複数回やりとりすることで油断させるなど、不審を抱かれにくいようにするような手口をDos攻撃という。	
10	情報セキュリティを確保するため、「PDCAサイクル」を繰り返し行い、適切な対策に見直していくことが大切である。	

※このまとめテストの提出を受けることにより、各人が研修を実施したか確認することもできます。
解答の正解は次のページにありますので、解答を記載したあとに正解を確認しましょう。

解答

No	解答 (○×)	掲載箇所
1	×	P 25
2	○	P 10
3	○	P 32
4	×	P 36
5	×	P 46
6	○	P 44
7	×	P 68
8	×	P 69
9	×	P 72
10	○	P 87