練馬区
委託事業者等向け情報セキュリティ教材

令和６年３月版

企画部　情報政策課

はじめに

- 委託事業者等の皆様は、受託業務の遂行にあたり、区と同等以上の情報セキュリティ対策を実施する必要があります。
- 本研修教材は、「特記事項」が添付された契約等において、皆様に遵守していただく情報セキュリティ対策（主に特記事項の内容）をまとめたものです。
- 本教材は、**主に委託事業者を想定して作成しています**。
  指定管理者や派遣契約、リース会社においては、適宜文言を置き換えてご活用ください。

用語の定義

- 本教材で使用する用語の定義を以下に示します。

委託事業者等	委託事業者および指定管理者
区	練馬区
情報	委託契約の受託者が、委託者から受託した業務を履行するにあたり、委託契約で取り扱う情報
特記事項	情報の取扱いルールについて記載し、契約等に際し仕様書に添付する以下の書類 • 情報の保護および管理に関する特記事項 • 指定管理における情報の保護および管理に関する特記事項 • 労働者派遣契約における情報の保護および管理に関する特記事項 • メンテナンスリースにおける情報の保護および管理に関する特記事項 • ファイナンスリースにおける情報の保護および管理に関する特記事項 • 特定個人情報の保護および管理に関する特記事項（４種類）

特記事項とは

「特記事項」について、基本的な内容を以下にまとめます。

- **特記事項とは**
  委託事業者等が、個人情報をはじめとする区の情報を取り扱う業務に関して**共通に遵守すべき基本的な事項を規定したもの**です。

- **特記事項の目的**
  契約等における**個人情報の保護、および一定の情報セキュリティ水準を確保**することを目的としています。
  契約書に特記事項を添付することで、区が求める個人情報の保護および情報セキュリティレベルを明らかにしています。

- **記載内容の概要**
  対象は当該契約で取り扱う情報（区の情報）であり、個人情報だけではありません。
  情報の取扱いルールとして、「受託業務の従事者へのセキュリティ教育実施・報告の義務」や「情報の管理における義務」などを規定しています。

本教材が対象とする契約等について

- 本教材は、**特記事項**が添付されている契約等を対象にしています。そのうち、**「特定個人情報の保護および管理に関する特記事項」**が添付されている契約等は、本教材と併せて、**「練馬区委託事業者等向け情報セキュリティ教材（特定個人情報の取扱いについて）」**（以下「特定個人情報の教材」という。）も活用し、研修を実施してください。

- 特定個人情報（マイナンバーを含む個人情報）を取り扱う場合は、**より厳重なルールが決められています**。「特定個人情報の教材」で確認してください。

特

「特定個人情報の教材」を確認する必要があるページは、右上に左図のような表記をしています。
※カッコ書きのページ番号は、参照する特定個人情報の教材のページ番号を示しています。

教材の利用イメージ

※ 特定個人情報を取り扱う契約等

本教材　特(P.３)

○○に係る遵守事項

1　×××をすること。
2　△△△をすること。
3　■■■をしないこと。

- 5 -

「特」表記があるページ（項目）は「特定個人情報の教材」を併せて確認する。

特定個人情報の教材　委(P.5)

○○に係る遵守事項

A　◇◇◇をすること。
B　◎◎◎をしないこと。

- 3 -

左のイメージ図の場合、１～３の３項目とA・Bの２項目の合計５項目を遵守する必要があります。

本教材の目的

- 区では、委託業務における情報セキュリティを確保し、情報漏えい等の事故を防止するため、契約書に**「特記事項」**を添付しています。

- 本教材は、受託者および受託業務の従事者に対し、それぞれの立場から「特記事項」の内容を正しく理解し、遵守していただくことを目的としています。

- 本教材の構成／主な想定対象

本教材の構成	主な想定対象		
	受託者	管理責任者	従事者
第１章 契約の前提となる事項	○	―	―
第２章 契約締結時に実施すべき事項	○	―	―
第３章 履行中に実施すべき事項	○	○	○
第４章 契約終了時に実施すべき事項	○	―	―
第５章 再委託について	―	○	○

第３章は管理責任者を含めた従事者の遵守事項も記載しているため、情報セキュリティ教育に使用してください。
また、巻末の復習テストを適宜活用してください。

情報セキュリティ事故等とは

■ 「情報セキュリティ事故等」とは、以下のような事象またはそれらのおそれ・兆候を言います。

情報漏えい

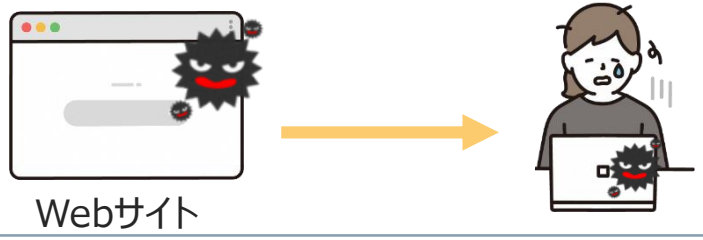
例：区民の個人情報を、送信先を誤ってメールする。

不正アクセス

例：他人のID・パスワードを使って、権限の無いシステムにログインする。

ウイルス感染

例：パソコンがウィルスに感染する。



情報資産の紛失・盗難

例：自転車のカゴに入れておいた書類が盗まれる。

情報資産の所在不明

例：情報機器の管理が不十分で所在不明になる。

その他、特記事項や関係法令等への違反

例：私物のパソコンやスマートフォンを業務で利用する。

委託事業者等における情報漏えいの事例

【倉敷市】申込フォームでミス、個人情報が流出(令和６年２月)

- 岡山県倉敷市は、3月に開催を予定しているサイクリングイベントの申込フォームにおいて、**申込者の個人情報が閲覧できる状態となる不具合**があったことを明らかにした。
- 業務委託先における**フォームの設定ミスが原因**で、**32人分の氏名、住所、電話番号などが流出**した。同日申込フォームを停止するとともに削除。同市や委託先事業者では参加申込者に対して経緯を説明し、謝罪した。
- 同市では、申込フォームの設定を行う場合に複数人によるチェックを行い、動作確認の徹底を図ることで再発防止を図るとしている。

（出典：https://www.security-next.com/153370）

「特記事項」は、このような事故や情報の不適切な取扱いの発生を未然に防止するために、**①契約締結当初、②履行中、③契約終了時**の各段階で、受託事業者等が情報を適切に管理することを目的としています。

第１章　契約の前提となる事項

対象：受託者

本章は、受託者が区の業務を受託する前提として
守るべき事項を記載しています。

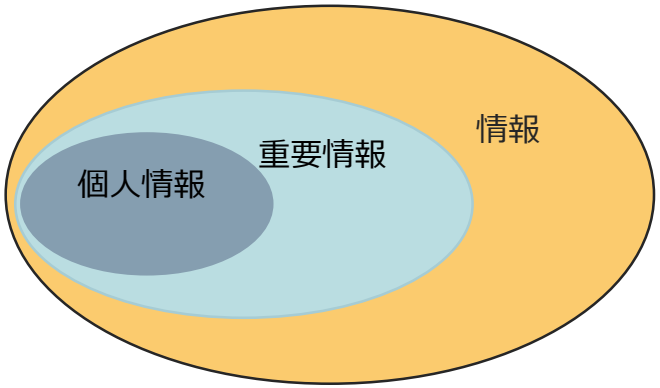
契約の前提となる事項（１／２）

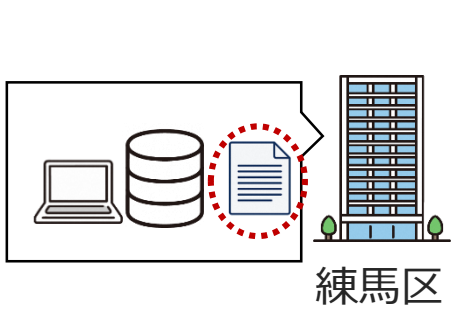
特(P.7,P.８)

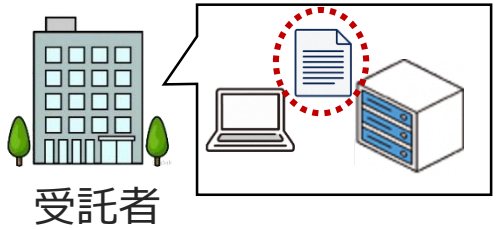
ａ．重要情報とは

個人情報や**その情報が脅威にさらされることにより区政運営に重大な影響を及ぼす情報**をいいます。
受託業務を遂行するにあたっては、**どのような重要情報をどのように扱うのかを特定**した上で、特記事項に基づき重要情報を厳重に取り扱う必要があります。

重要情報とその取扱いの例







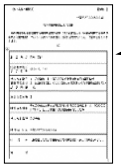
区の情報システムを使用する。
例：住民情報システム

受け取った情報を自社内で取り扱う。
例：自社のパソコン、サーバ

区民の個人情報を含むファイル
（例：名簿、連絡先一覧表）

・氏名
・住所
・電話番号
・・・

申請書・届出書



・申請者
・申請内容
・承認者
・・・

公開前の計画書　等

・件名
・目的
・実施期間
・・・

契約の前提となる事項（２／２）

特(P.9)

b．個人情報等の重要情報を守るために

個人情報とは、**生存する個人に関する情報であって、**以下のいずれかに該当するものをいいます。

①**当該情報に含まれる氏名、生年月日その他の記述等（個人識別符号（※）を除く。）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。）

②**個人識別符号が含まれるもの**　【個人情報の保護に関する法律第２条】

※ その情報単体から特定の個人を識別することができるものとして政令で定められた文字、番号、記号その他の符号のこと。

区は、特記事項の記載内容と同等以上の情報セキュリティ対策を実施している（実施することができる）事業者にのみ、区の業務を委託することができます。**そのため、区では個人情報を取り扱う契約について、契約締結前に「安全管理体制確認書」を提出（※）することを求めています。**

また、業務を受託しようとする事業者は、情報を保護し、適切に管理するために、自社における個人情報保護方針や、情報セキュリティに関する規程、運用マニュアルといった情報管理ルールを定め、**従事者に周知・徹底する必要があります。**

※ 提出にあたり、件名、契約期間、受託事業者名等が契約書の記載と一致していることをチェックしてください。

区の情報を取り扱う受託者は、特記事項と同等以上の情報セキュリティレベルを維持する必要がある。

第２章　契約締結当初に実施すべき事項

対象：受託者

本章は、受託者が契約締結当初に実施すべき事項を記載しています。

契約締結当初に実施すべき事項（１／３）

特(P.11)

a．管理体制の確立

情報セキュリティ事故等を防止するためには、適切な情報の管理が必須であり、受託業務における**体制を明確にする**ことが大前提です。

そのため、受託者は**個人情報を取り扱う契約の場合、**情報の管理に責任を持つ**「管理責任者」を任命**し、また、受託業務に従事する**「従事者」を特定**して体制を明確にし、区に**書面で報告する**必要があります。

報告内容に変更があった場合は、**速やかに再報告（再提出）する**必要があります。

しなければならないこと

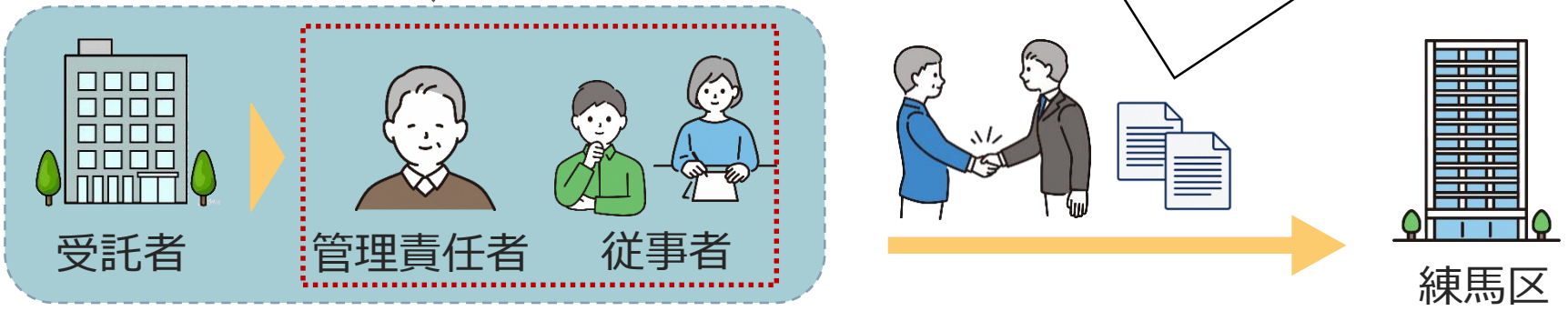
管理責任者を任命し、従事者を特定

管理責任者は原則として従事者から選任

※　書面の参考様式は、区から提示します。

個人情報を取り扱う契約の場合

- 管理責任者について、「情報の管理責任者　選任届」を**書面で提出する**。
- 従事者について、「受託業務従事者報告書」を**書面で提出する**。
- 提出にあたり、会社名、契約件名等が**契約書と一致しているかチェックする**。



契約締結当初に実施すべき事項（２／３）

b．情報セキュリティ教育

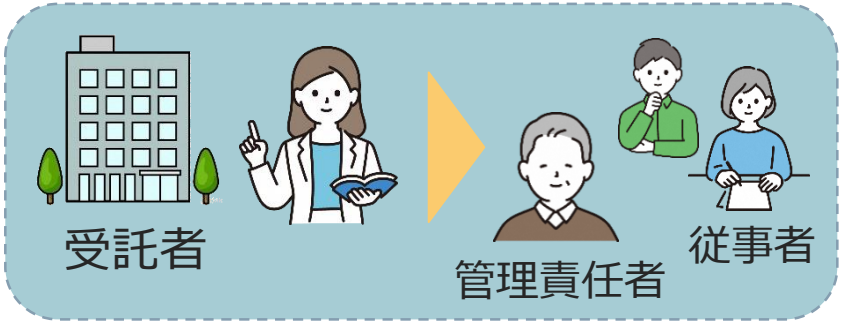
受託者は特記事項の内容を周知徹底するために、**個人情報を取り扱う契約の場合は、管理責任者も含めた従事者に対する情報セキュリティ教育**を実施して、その結果を区に**書面で報告する**必要があります。

また、区が特記事項の遵守に必要な教育を実施する時は、管理責任者および従事者に教育を受けさせる必要があります。

管理責任者および従事者に変更があった場合は、**速やかに教育を実施し、再報告（再提出）する**必要があります。

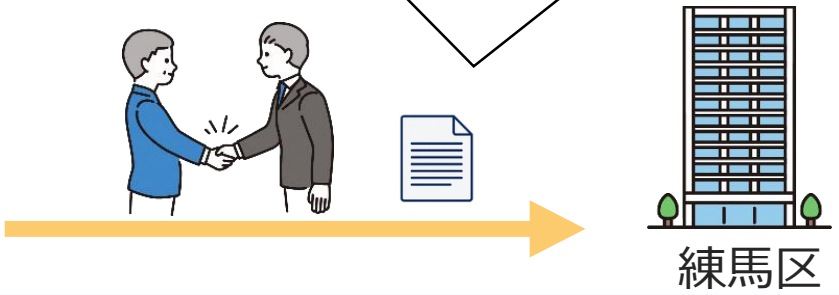
しなければならないこと

管理責任者および従事者に対し、**情報セキュリティ教育を実施**



※ 書面の参考様式は、区から提示します。

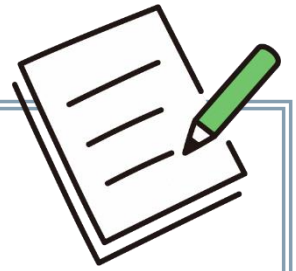
個人情報を取り扱う契約の場合	教育の実施状況について、「情報セキュリティ教育実施結果報告書」を**書面で提出する**。その際は、会社名、受託業務件名が**契約書と一致しているかチェックする**。



契約締結当初に提出する書類について

- 個人情報を取り扱う契約等では、契約締結の際に以下の書類を提出する必要があります。提出にあたり、以下の項目をチェックしてください。

提出する書類とチェック内容



情報の管理責任者選任届

- □ 件名、契約期間、受託事業者名等は契約書の記載と一致していますか？
- □ 管理責任者の役職と氏名は記載されていますか？

受託業務従事者報告書

- □ 会社名、契約件名は契約書の記載と一致していますか？
- □ 管理責任者氏名は「情報の管理責任者選任届」の氏名と一致していますか？
- □ 従事者氏名は実際に業務している者と一致していますか？

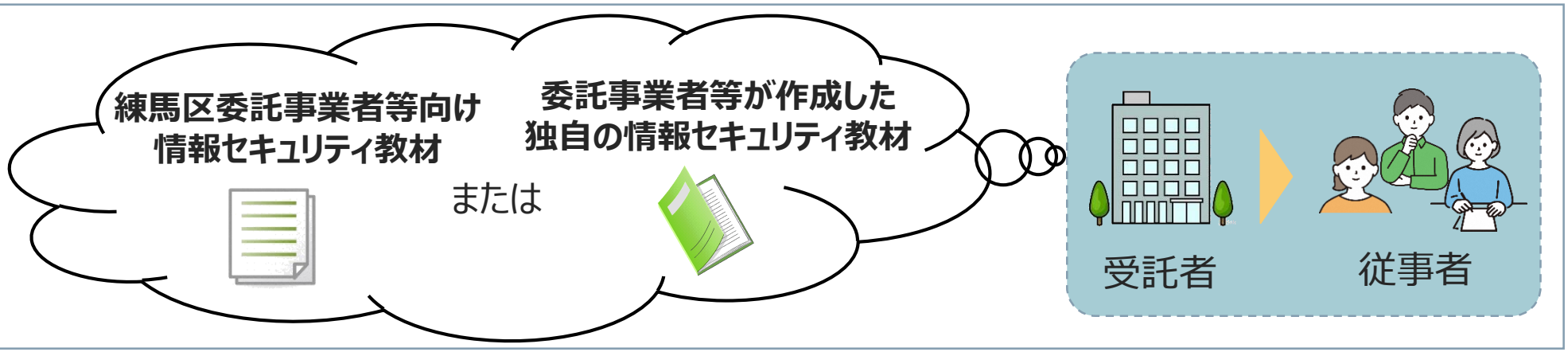
情報セキュリティ教育実施結果報告書

- □ 会社名、受託業務件名は契約書の記載と一致していますか？
- □ 管理責任者氏名は「情報の管理責任者選任届」の氏名と一致していますか？
- □ 参加人数及び配付人数の合計は、「受託業務従事者報告書」の従事者数と一致していますか？

※ 特定個人情報を取り扱う契約等では、上記に追加して提出する書類があります。「特定個人情報の教材」で確認してください。

情報セキュリティ監査では、ここを指摘しました！

従事者の情報セキュリティ教育結果報告書を提出していない事業者がいました。



個人情報を取り扱う契約では、
従事者の**全員に**情報セキュリティ教育を実施し、
区に**書面で報告**してください。

- 情報セキュリティに関する知識と意識が十分でないまま受託業務に従事していた場合、情報セキュリティ事故等の発生リスクが高まります。
- **契約期間中に追加となった従事者に対しても**、速やかに教育を実施して、区に書面で報告してください。

契約締結当初に実施すべき事項（３／３）

c．緊急時対応の手順化

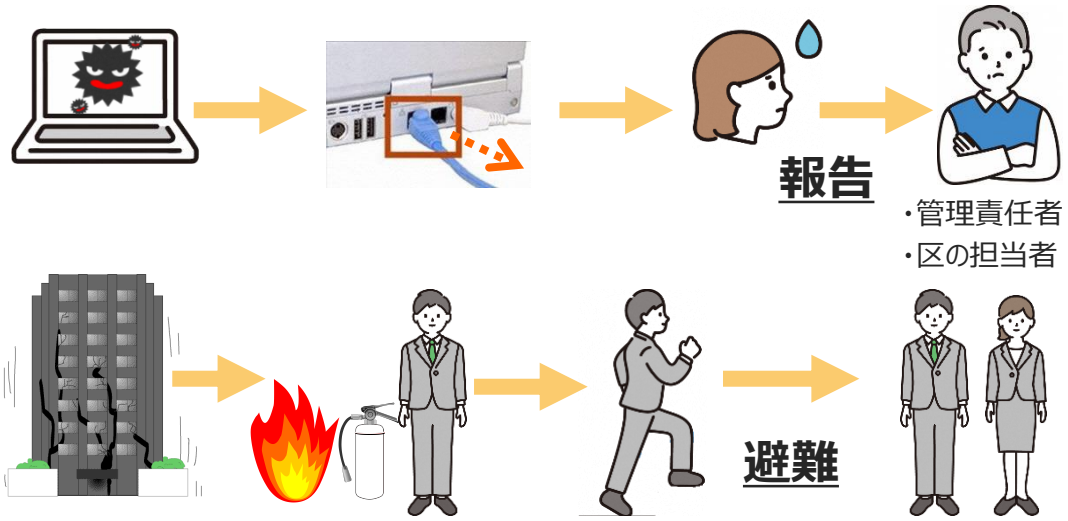
情報セキュリティ事故や災害等発生時に備えた緊急時対応手順を策定し、**管理責任者を含めた従事者に周知する**必要があります。これは、事故や災害等によって情報が脅威にさらされても、可能な限り早く対応して影響を最小限に抑えられるようにするためです。

また、緊急時対応手順の実効性を高めるために、**定期的な確認または訓練を実施する**必要があります。

遵守事項のイメージ

- 管理責任者を含めた従事者に対し、緊急時対応手順を周知

- 緊急時対応手順に基づき迅速に対応



第３章　履行中に遵守すべき事項

対象：受託者、管理責任者、従事者

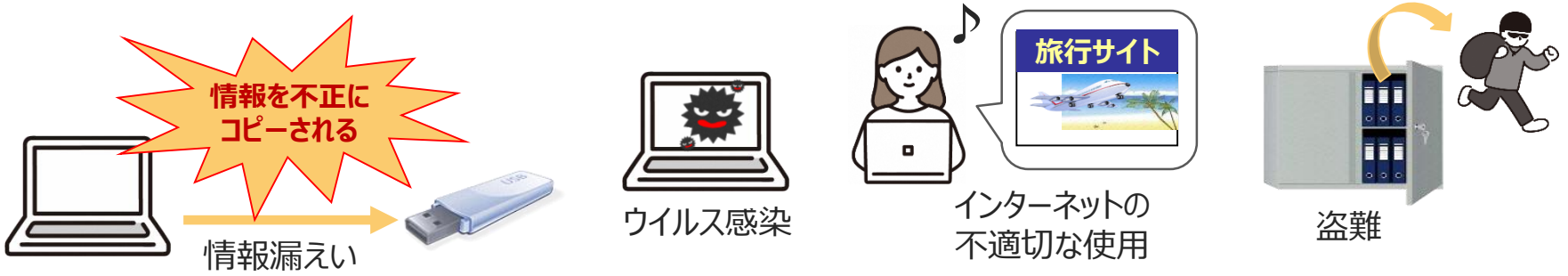
本章は、受託業務に従事する方が業務を遂行する際に
守っていただきたいことを記載しています。
管理責任者を含めた従事者向け研修資料として適宜
活用してください（教材の最後に復習テストもあります）。

履行中に遵守すべき情報セキュリティルールの重要性

情報セキュリティルールの重要性

- 皆さんは、業務の中で多くの情報（印刷した帳票、電子データおよび電子データを格納した記録媒体等）を取り扱っています。その中には、区民の情報をはじめとする重要な情報が含まれている可能性があるため、**情報セキュリティルールに従い作業することが重要**になります。それにより、重大な情報セキュリティ事故等が起きにくくなります。

➢ 情報セキュリティ事故等とは…



- 情報セキュリティ事故等の発生を防ぐため、区の業務に従事する皆さんに守っていただきたい、情報セキュリティ上の**16のルール**について取り上げます。

履行中に遵守すべき事項（１／16）

（１）守秘義務等

【情報を取り扱う際の遵守事項】

１）**個人の権利利益を侵害することのないよう**、情報を適正に取り扱う。

２）個人情報を収集する時は、受託業務の履行を達成するために**必要な範囲内で、適法かつ公正な手段により行う**。

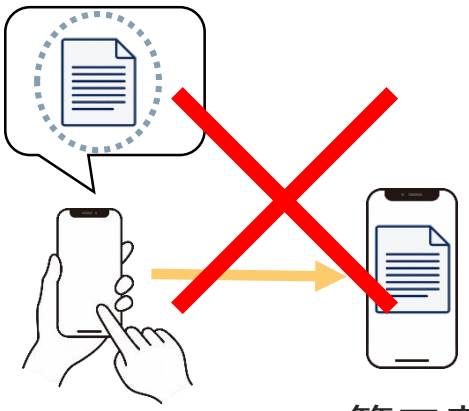
３）受託業務の履行にあたり、知り得た情報を**第三者に漏らさない**。

４）情報を**第三者に提供しない**。

５）情報を**他の用途に使用しない**（ソーシャルメディアへの発信を含む）。

遵守事項のイメージ

● 情報を漏らさない・提供しない



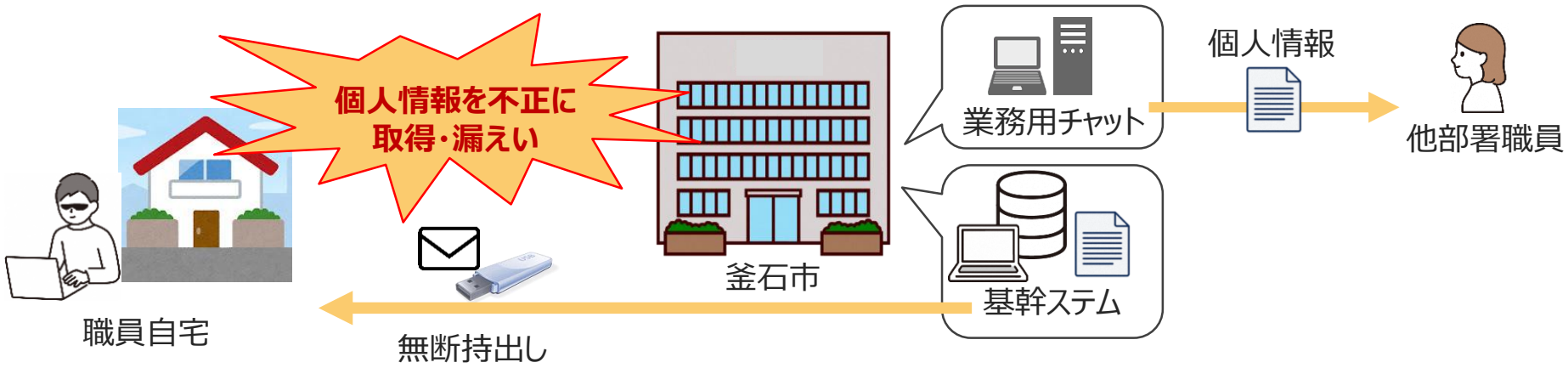
● 情報を他の用途に使用しない

例えば、こんな事故が起きています。

【釜石市】全住民の個人情報を無断持ち出し（令和５年３月）

- 釜石市は、職員3名（係長1名、主査2名）が**市民全員分（約32,000人）の住基情報（住所、氏名、生年月日、性別、収入額等）、624人分のマイナンバー情報を自宅に持ち帰るなどして不正に取得して漏えいさせていた**ことを調査委員会報告書として令和5年3月に公表した。
- 同市によれば、**市民の個人情報が記載されたエクセルファイルを電子メールに添付し、複数回にわたり自宅パソコンのメールアドレスに送信**していた。また、**私物のUSBメモリにも住基データを入れて自宅に持ち帰っていた**。
- 当該職員は、勤務時間中に、業務で用いるチャット機能を私的に繰り返し利用しており、業務上知り得た市民の情報を他部署職員に漏えいしていた。**市の外部に漏らさなければ、市職員間で個人情報のやり取りをすることは問題ないという誤った認識**を持っていた。

（出典：https://www.city.kamaishi.iwate.jp/docs/2023041400057/）



履行中に遵守すべき事項（２／16）

特(P.14)

（２）情報の郵送

【記録媒体（※）の郵送時の遵守事項】※ 情報システム機器のハードディスクを含む。

１）情報を格納する時は、ファイルに**パスワードを設定する等によりデータを暗号化する**。

２）重要情報を格納する時は、**中身の入れ違いがないか確認**し、**追跡可能な移送手段**を用いる。

３）情報の格納の有無に係わらず、**郵送の記録を管理簿により管理**する。

【参考】 記録媒体郵送時の取扱い

	パスワード	追跡移送	管理簿
情報	○	×	○
重要情報	○	○	○
情報なし	×	×	○

凡例 ○：要対応 ×：対応不要

【印刷物・文書の郵送時の遵守事項】

重要情報を郵送する時は、中身の入れ違いや宛先に誤りがないか確認し、**特定記録郵便または親展表示で送付**する。

遵守事項のイメージ

記録媒体の郵送

パスワード設定等により暗号化を行う

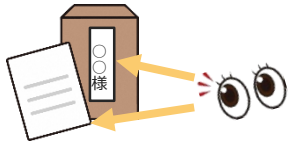
追跡可能な移送手段を用いる

○簡易書留 ○特定記録郵便

管理簿に記録する

印刷物・文書の郵送

入れ違いや宛先誤りがないか確認する



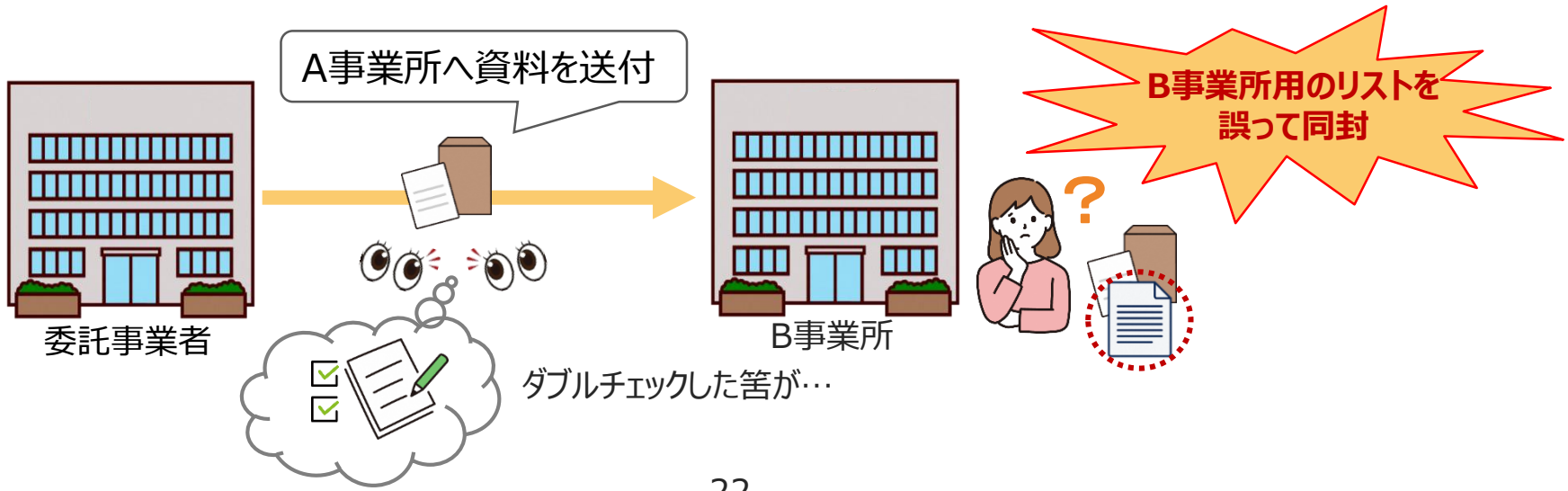
特定記録郵便または親展表示で送る

例えば、こんな事故が起きています。

【全国健康保険協会】委託業者による特定保健指導対象者リストの誤送付（令和５年10月）

- 全国健康保険協会は、大阪支部の委託業者が、**A事業所に対してB事業所の特定保健指導対象者リスト（対象者1名）を誤って同封し送付した**ことを公表した。
- 作業工程として複数人で同封物を確認することとしていたが、**ダブルチェックにおいて担当者の注意力に依存**しており、**誤りが生じることを前提としたチェック方法・体制となっていなかった**。また、封入時にチェックリストを使用していたが、**封入物の種類・枚数の確認を怠っていた**。
- 今後は、担当者の注意力に依存しないよう作業工程ごとにチェックリストにより確認し、また、作業完了時には実施責任者による確認を行うこととしている。

（出典：https://www.kyoukaikenpo.or.jp/shibu/osaka/template02/r5/r511/r51130error2/）



情報セキュリティ監査では、ここを指摘しました！

重要情報を含む文書を、特定記録郵便または親展表示で送っていない事業者がいました。

重要情報を含む文書を郵送する時は、<u>特定記録郵便</u>または<u>親展表示</u>が必要です。

さらに、<u>記録の管理</u>（送付の記録）を実施すると、事故等発生時に原因や被害状況を速やかに把握し、迅速な対応をとることができます。発送件数が多い等、都度の記録が難しい場合を除き、原則として送付の記録は残すようにしてください。

特(P.15)

（３）情報の送信（メール･FAX）

【送信時の遵守事項】
１）重要情報をメールで送信する時は、**メール本文には記載せず**添付ファイルとし、ファイルに**パスワードを設定する等によりデータの暗号化を行う**。
２）情報をメールやFAXで送信する時は、**宛先および添付ファイルを誤らないように十分注意する**。

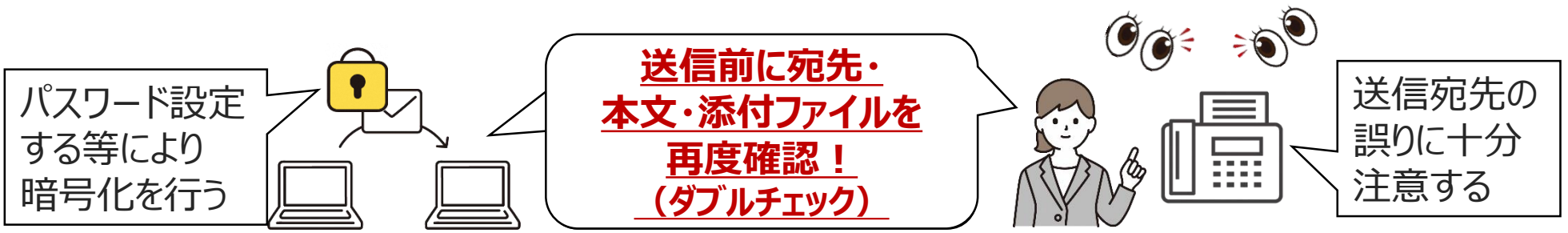
遵守事項のイメージ

メール送信

- 重要情報はメール本文に記載しない
- パスワードを設定する等により添付ファイルを暗号化する
- 送信宛先および添付するファイルに十分注意する

FAX送信

- 送信宛先、送付内容に注意する



※ パスワードはメール以外の方法で送信先に伝える手段を整備（例：あらかじめ相手先と設定するパスワードを決めておく）すると、一層有効な対策となります。
※ セキュリティが確保されたファイル送信サービスの利用も有効です（個人で契約しているサービスの利用はNG）。

履行中に遵守すべき事項（４／16）

（４）メールの利用

【メール送信時の遵守事項】
　区民等のメールアドレスも個人情報であるため、複数の区民等にメールを送る際には、TOやCCではなく、**BCCを利用して**個人情報が漏れないようにする。

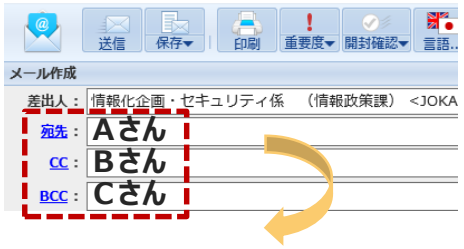
【メール受信時の遵守事項】
　不審なメール（心当たりのないメール等）は、組織内部の情報を狙った「標的型攻撃メール」の可能性があるため、添付ファイルを開く前に、メール本文や差出人等に不審な点がないかを確認する。**安全が確認できるまでは添付ファイルやメール本文のURLを開かない。**

遵守事項のイメージ

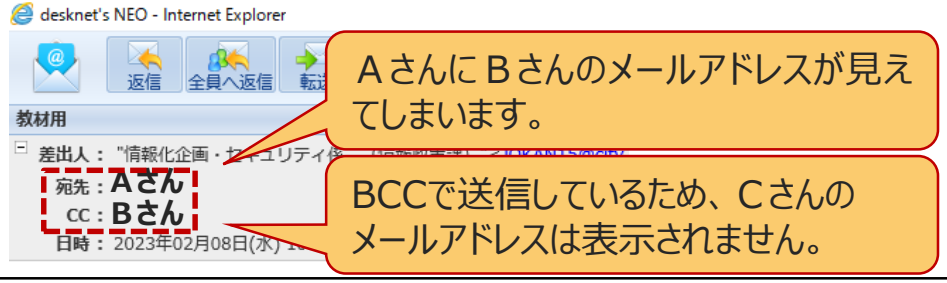
　メールを同時に複数の区民等に送信する場合は、メールアドレスを**BCCに設定**する。

宛先設定によるメールアドレスの見え方の違い
TO：送った人全員から見える
CC：送った人全員から見える
BCC：他の人から見えない

TO、CC、BCCをこのように設定すると



受信者にはこのようなメールが届きます。



履行中に遵守すべき事項（４／16）

遵守事項のイメージ（つづき）

不審なメールを受信した場合は、**正当性が確認できるまでは、添付ファイルを開いたり、メール本文のURLをクリックしない**ようにします。

不審メールの特徴例（判別のための着眼点）

□ メールの差出人
- 差出人のメールアドレスと署名（メール本文の一番下に記載されている差出人情報）のメールアドレスが異なる　等

□ 添付ファイル
- 実行形式ファイル（exe / scr / cpl等）が添付されている
- ショートカットファイルが添付されている（lnk等）　等

□ メールのテーマ、内容
- 区民からのクレームを装い、メール本文のURLや添付ファイルを開かせようとする
- 公的機関によるセキュリティの注意喚起を装い、添付ファイルを開かせようとする
- システム管理者を装い、IDやパスワードの入力を要求する
- 文法や仮名遣いがでたらめである
- 正常に表示できない文字（繁体字、簡体字）がある　等

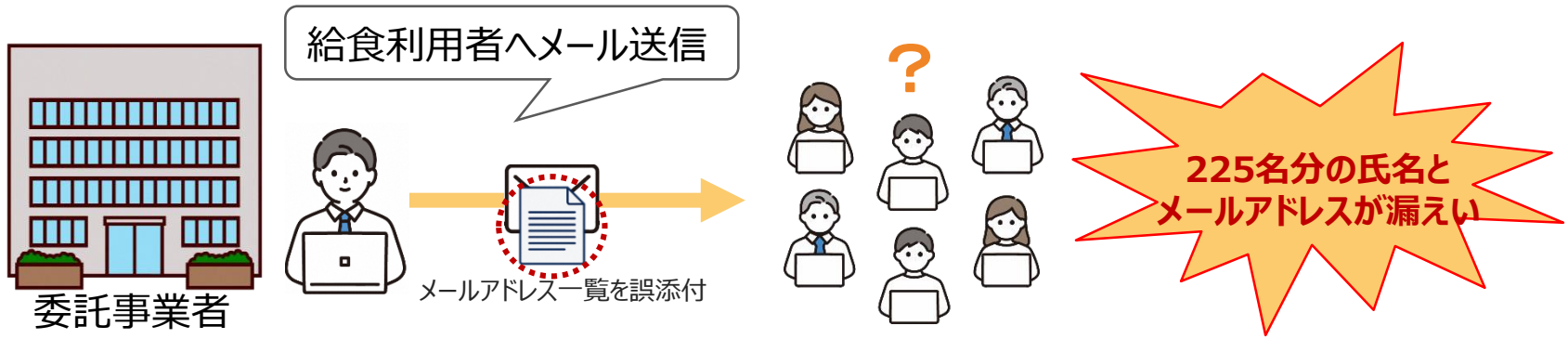
上記の特徴例に該当しない標的型攻撃メールもあります。
被害に遭わないために、**受信したメールに不審な点がないかを、注意して見極める**ように心がけてください。

例えば、こんな事故が起きています。

【横浜市】不要なファイルを添付し、メールアドレスが漏えい（令和５年７月）

- 横浜市は、同市中学校給食サポートセンター運営受託事業者から中学校１校の給食利用者225名へメールを送信した際、**添付する必要のない「送信先メールアドレス一覧（225名分）」を添付したため、225名分の氏名とメールアドレスが漏えいした**ことを発表した。
- メールを送信する際に、複数人でのチェックは行っていたものの、**その記録やチェック項目までは作成していなかったことから、ファイルが添付されていることに気付かず、そのまま送信した**とのこと。また、委託事業者は**事故発生日の夜間に市に電話**したが、業務時間外であったため連絡がつかず、**市が事故を把握したのは翌朝**であった。
- 対象となった中学校へ発生経緯等の詳細を説明するとともに、225名に対し委託事業者から謝罪のメールを送信した。同市は、個人情報の取扱いおよびその重要性を委託事業者に改めて伝えるとともに、**時間外における委託事業者との連絡体制を構築**し、事故等が発生した際の迅速な対応に繋げるとしている。

（出典：https://www.city.yokohama.lg.jp/city-info/koho-kocho/press/kyoiku/2023/20230706.files/0001_20230706.pdf）



履行中に遵守すべき事項（５／16）

特(P.16)

（５）情報の持ち出し

重要情報は履行場所から持ち出してはいけません。ただし、区が必要と認めた場合はこの限りではありません。また、持ち出す場合は、以下の事項を守る必要があります。

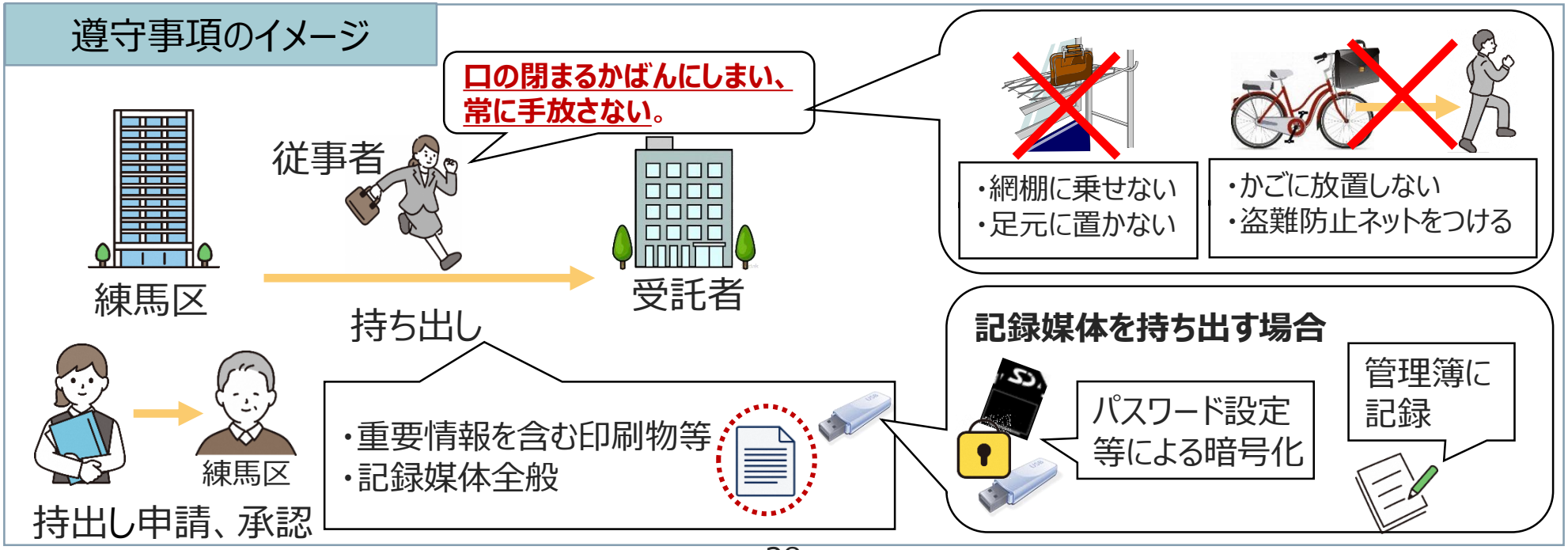
【持ち出し時の遵守事項】

１）受託業務で使用する記録媒体（携帯電話・スマートフォンを含む）、パソコン、印刷物等を持ち運びする時は、**盗難や紛失に十分注意する**。

２）記録媒体は**パスワードを設定する等によりデータの暗号化**を行う。

３）情報の格納の有無に係わらず、**記録媒体の持ち出しは、記録を管理簿により管理**する。

遵守事項のイメージ



履行中に遵守すべき事項（５／16）

持ち出し記録の管理方法（例）

記録媒体の持ち出しは、**承認～目的の作業が終了し保管場所に戻すまでを管理簿に記録**し、確実な管理を行う必要があります。

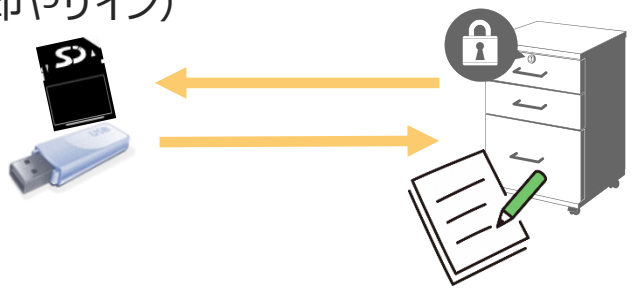
管理簿に記録・管理する項目

記録媒体別に以下を記録・管理します。

□ 記録簿の項目名

- 利用日
- 利用者
- 利用目的
- 記録媒体への格納情報（情報の内容／重要情報の有無／個人の特定（※））
- 持ち出し・送付等の種別（持出し先・送付先／送付方法）
- 練馬区（または区から承認権限を与えられた者）の承認（印やサイン）
- 受領確認日（送付先での受領日）
- 返却確認日（持ち出しの場合）
- データ消去日
- 利用終了日（保管場所への返却日）
- 返却確認（印やサイン）

（※）紛失等が発生した場合に、誰のどのような情報なのか特定できる情報



上記の記録媒体別の持ち出し記録とは別に、**記録媒体の管理も必要**です。
項目として、登録番号/媒体種類/利用目的/個人情報取扱い有無/所管部署/利用開始日/保管場所/利用終了日/終了方法/管理者承認　等を登録、管理するようにします。

履行中に遵守すべき事項（６／16）

特(P.18)

（６）情報の保管

【保管時の遵守事項】

１）重要情報を含む印刷物・文書や、情報の格納の有無に係わらず、受託業務で使用する記録媒体（携帯電話・スマートフォンを含む）を保管する際は、**施錠できるキャビネット等に保管する**。

２）情報を格納した記録媒体を保管する際は、**適切なアクセス管理を行う**。

３）記録媒体において、**不要になったデータは直ちに消去し、必ず保管場所に戻す**。

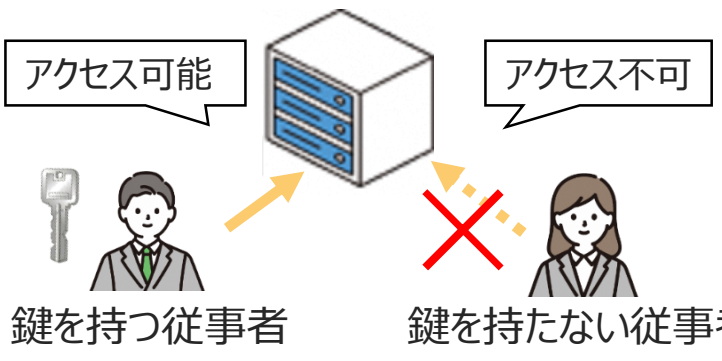
４）重要情報を、受託業務の履行以外の目的のために**複写または複製をしない**。

５）書類の受け渡しは直接手渡しで行い、決められた場所で管理し、誤廃棄や、持ち出した際の強風等による**紛失に注意する**。

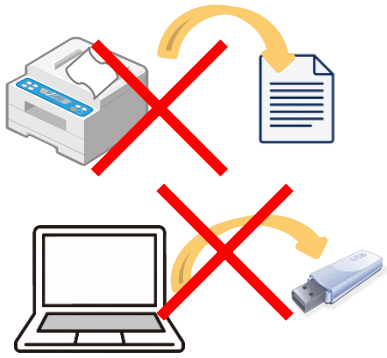
遵守事項のイメージ

● 印刷物・文書や記録媒体は施錠管理する

● 記録媒体で保管する際はアクセス管理を行う



● 履行目的以外の複写や複製は禁止

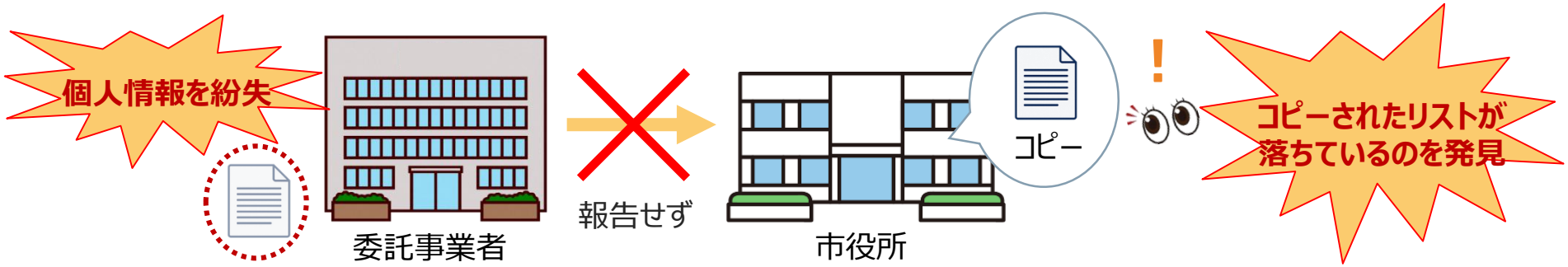


例えば、こんな事故が起きています。

【富谷市】健診委託事業者が個人情報紛失、3カ月後にコピーが発見され発覚（令和５年８月）

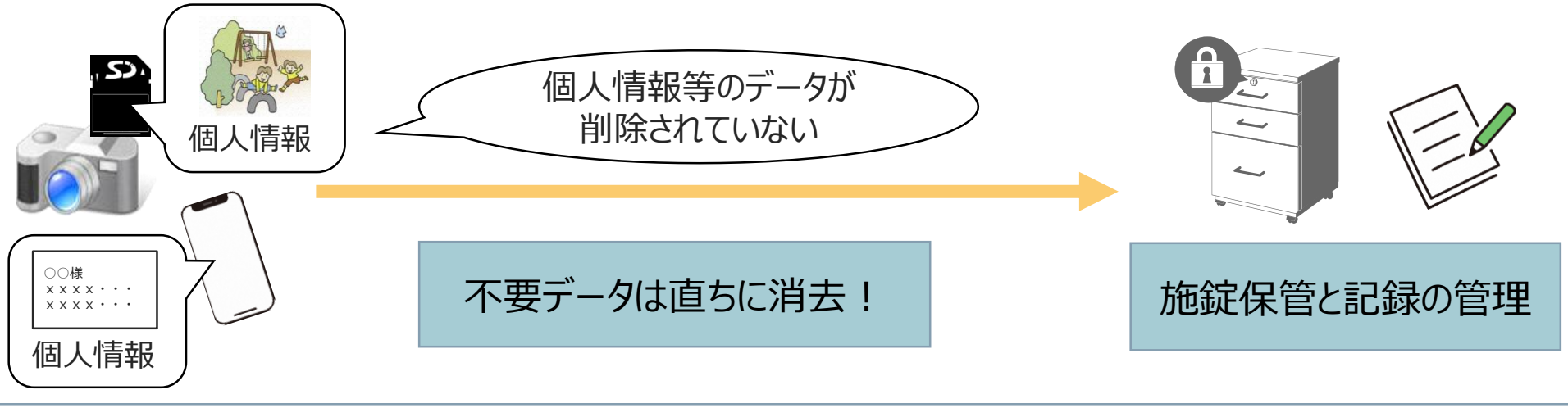
- 宮城県富谷市は、健診などの業務委託先が**健診受診票の送付リストの一部（80人分の氏名、住所、健診申込種別情報などが記載）を紛失したことを明らかにした。**
- 原本のコピーと思われるリストが市役所内に落ちているのを職員が発見、拾得したことで問題が発覚した。受託業者はコピー発見の**約３か月前に原本を紛失**していたが、同市に対する報告は行われていなかった。
- 問題のリストについて、**委託事業者の施設内より盗まれた可能性がある**として、同市では事実確認の徹底を要請。警察へ相談しており、関係者の聴取などが行われている。リストに記載されていた関係者には、委託事業者が書面で経緯の説明と謝罪を行った。

（出典： https://www.security-next.com/148660 ）



情報セキュリティ監査では、ここを指摘しました！

デジタルカメラや携帯電話の個人情報を含むデータを削除していない事業者がいました。



利用後は、**不要なデータの削除**が必要です。

デジタルカメラや携帯電話を利用した後は、必要に応じて中のデータを決められた場所に保存し、削除することが必要です。

履行中に遵守すべき事項（７／16）

特(P.19)

（７）情報の廃棄

【廃棄時の遵守事項】

１）重要情報を含む印刷物・文書を、**裏紙として再利用しない**。

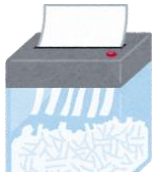
２）重要情報を含む印刷物・文書や、情報の格納の有無に係わらず、受託業務で使用した記録媒体（携帯電話・スマートフォンを含む）を廃棄する場合は、**データを復元できないよう物理的な破壊または漏えいを来さない方法での消去を行う**。

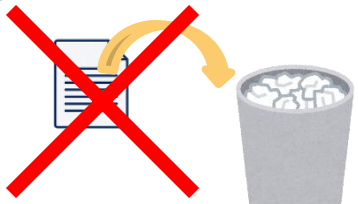
３）**記録媒体を廃棄する場合**は、その**記録を管理簿により管理する**。

遵守事項のイメージ

- 重要情報を含む印刷物や文書を処分

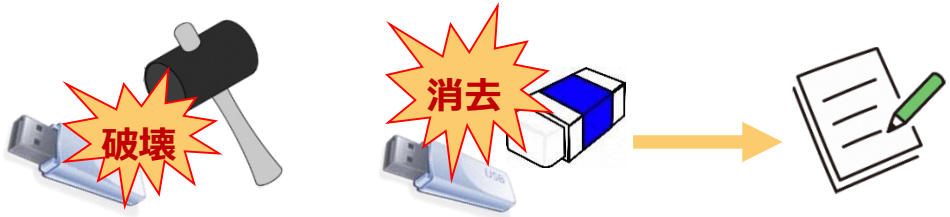
シュレッダーや溶解処理を用いて復元できないように





ゴミ箱にそのまま捨ててはいけません！

- 記録媒体（携帯電話・スマートフォンを含む）等は、物理的な破壊または漏えいを来さない方法でのデータ消去を行い、管理簿に記録



USBメモリは基盤部分を破壊するか専用ツールでデータを消去する

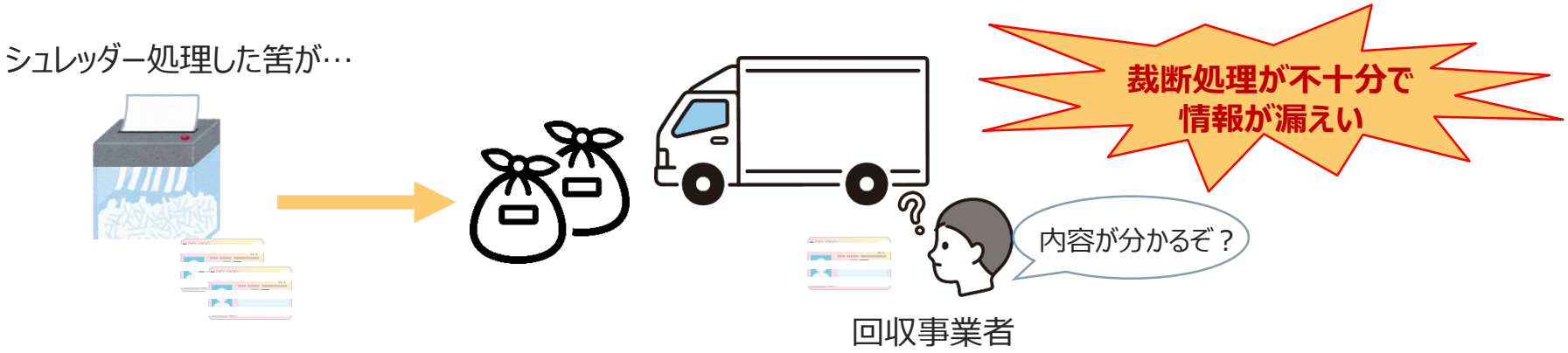
管理簿に記録

例えば、こんな事故が起きています

【台東区】廃棄処理後のマイナンバーカード等の券面情報漏えい（令和５年８月）

- 台東区は、廃棄対象のマイナンバーカードや住民基本台帳カードについて、**裁断処理が不十分**なカードが混入したごみ袋を搬出し、**カード券面情報が漏えい**したことを公表した。
- 令和５年７月、区において、廃棄対象のカードをシュレッダーで裁断処理を行い、シュレッダーにセットされているごみ袋を、廃棄場所に搬出した。ゴミ袋を回収した事業者より、裁断処理が不十分なカードが入ったごみ袋を引き取っているとの連絡を受け、事故が判明した。
- 区が当該ごみ袋を直ちに回収し、中身を確認したところ、**マイナンバーカード13件、住民基本台帳カード１件の情報が読み取れる状態**であった。
- 区は対象のカードを所持していた本人へ連絡し、謝罪と経緯説明を行った。

（出典：https://www.city.taito.lg.jp/kusei/sanka/release/press0508/press050817.html）



履行中に遵守すべき事項（８／16）

特(P.20)

（８）情報システムでの作業

情報システムで作業する場合は、以下の事項を遵守する必要があります。

【情報システムで作業する場合の遵守事項①（**受託者が情報システムを用意する場合**）】

１）IDとパスワード等による**認証を実施**※1する。情報漏えい等のリスクがあるため、必要な場合を除き**IDとパスワードは共用しない**。

２）インターネットに接続された環境で重要情報を取り扱う場合は、**標的型攻撃等の不正アクセスによる重要情報の漏えい等が生じないよう適切な措置**を講じる。

３）**ウィルス対策ソフトウェアの導入**およびウィルスパターンファイルの**最新化**を行う。

４）OS、ミドルウェア等に、定期的に**修正プログラムを適用**する。

５）許可のない記録媒体の接続やソフトウェアのインストールがされないよう、**適切な措置を講じる**※2。

６）離席時に**スクリーンセーバ等により自動でロック**する設定を行う。

※1　**IDとパスワードは、他人に知られないように管理**してください。また、パスワードは、原則として大小英字、数字、記号のうち３種類以上を組み合わせた10文字以上（最低８文字）としましょう。

※2　記録媒体やソフトウェアのインストールは可能な限り技術的な対策（制限ユーザー等）で制限してください。費用対効果等の面から難しい場合は、運用による対策が徹底されるよう、適切に管理してください。

特(P.20)

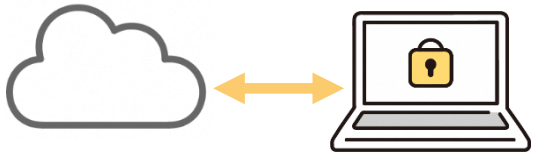
（８）情報システムでの作業（つづき）

【情報システムで作業する場合の遵守事項②（**区および受託者のシステムの共通事項**）】

１）複数の情報システムや記録媒体を使う場合、**互いに異なるパスワードを設定**する。
２）インターネットに接続された環境で重要情報を取り扱う場合は、**パスワードを設定する等によりデータを暗号化**する。
３）従事者の**私物等**、許可されていない情報システムおよび記録媒体**は使用しない**。
４）受託業務で使用する記録媒体を情報システムに接続する場合は、**ウィルスチェックを行う**。
５）情報を処理する情報システムにはWinny、Share等の**ファイル交換ソフトをインストールしない**。また、**許可されていないソフトウェアをインストールしない**。
６）区の情報システムの利用や運用保守作業等を行う時は、区の示す手順（利用マニュアル、管理マニュアル、運用設計、基本設計等）を遵守する。

遵守事項のイメージ

- インターネットに接続された環境で重要情報を取り扱う場合



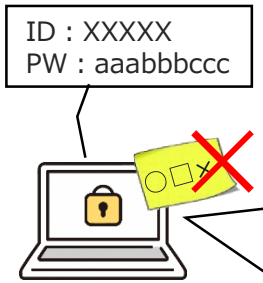
- パスワードを設定する等により暗号化
- 不要になった場合は、速やかに削除
- ファイアウォール等で、登録の無い通信先との通信を遮断

履行中に遵守すべき事項（８／16）

特(P.20)

遵守事項のイメージ（つづき）

● IDとパスワードの設定に関する留意点



- IDやパスワードは、他人に知られないように管理
- パスワード は、原則として大小英字、数字、記号のうち３種類以上を組み合わせた10文字以上（最低８文字）にする
- 複数のシステムを使用する場合、異なるパスワードを設定

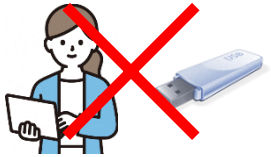
● 受託業務で使用する情報システムの設定

スクリーンセーバ

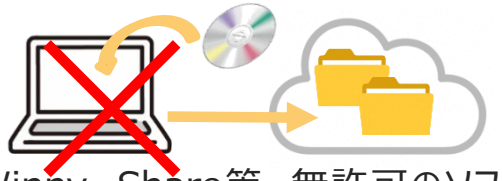
パスワードロック

- スクリーンセーバ等により自動でロックする設定
- 許可のない記録媒体の接続やソフトウェアのインストールを制限

● 使用してはいけないパソコン等



私物のパソコンや記録媒体等

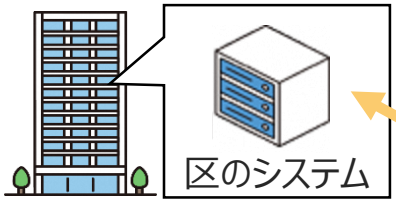


Winny、Share等、無許可のソフトがインストールされた機器

● 情報システムに行うウィルス対策

- ウィルス対策ソフトの導入
- ウィルスパターンファイルの更新
- OS等の修正プログラムの適用
- 記録媒体を情報システム機器に接続する際のウィルスチェック

● 区の情報システムの利用や運用保守作業等を行う時

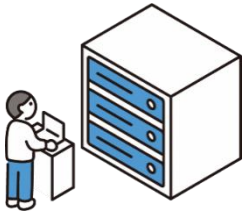


区のシステム

従事者

手順を遵守

運用保守作業者

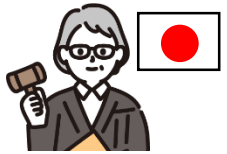


運用設計、基本設計、その他実施手順

特(P.21)

（９）外部サービスの利用

重要情報を**クラウドサービス**等の外部サービスを利用する場合は、以下の点に留意する必要があります。



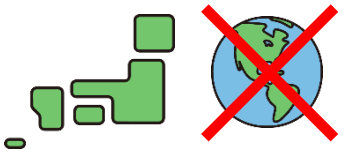
【外部サービス利用時の遵守事項】

１）**日本の法令の範囲内で運用**できるサービスであること。

２）サービス提供するリージョン（国・地域）を国内に指定でき、**データが海外に保存されない**こと。

３）次の事項を契約またはサービスレベル契約（SLA）に定められること。

- ✓ 外部サービスの**終了または変更時における事前通知などの取り決めや、情報資産の移行方法**
- ✓ **情報セキュリティ対策の履行が不十分な場合の対処**方法（改善、追完、損害賠償等）
- ✓ 外部サービス提供者が、**情報資産へ目的外のアクセスや利用を行わない**こと
- ✓ **情報セキュリティインシデント（情報セキュリティ事故およびその兆候）への対処**方法



４）情報セキュリティ対策の実施内容および管理体制について、公開資料や監査報告書、各種の認定・認証制度の適用状況から、総合的・客観的に評価し、判断可能であること。

５）次の事項を技術的に満たすこと。

- ✓ **アクセス制御**ができる
- ✓ 外部サービス内および通信経路全般に**暗号化処理**が行われる
- ✓ **各種ログの取得**機能を実装している
- ✓ 外部サービスの**利用終了時に、全ての情報が漏えいしない方法で確実に削除**される

※　上記事項を満たすとしても、従事者は**個人で契約しているクラウドサービスに、受託業務に係る情報を保存してはいけません。**

例えば、こんな事故が起きています

【杉並区】委託事業者サーバーがランサムウェア被害(令和５年６月)

- 杉並区は、同区の学童クラブ等の運営を受託している事業者の運用している一部**サーバーに格納されていたデータ（利用者のほか、職員やボランティアの個人情報を含む）が、ランサムウェアにより暗号化**されたことを公表した。
- 調査の結果、情報の漏えいの可能性は極めて低いとしたものの、被害にあった原因の特定には至らなかった。
- 同区と委託事業者は、**機器の更新、バックアップ体制の見直し、回線のIP-VPNへの変更、ウィルスソフトによる常時監視のほか、手動による検査の実施等の再発防止策**を取りまとめた。

（出典：https://www.city.suginami.tokyo.jp/news/r0508/1089625.html）

再発防止策	
ネットワークの再構築	サーバー、ファイアウォール、導入から数年経過している端末（PC）の更新
	ファイルバックアップの体制の見直し
	社内ネットワークの各事業所間を接続する回線をより閉域なIP-VPNに変更
ネットワーク保守体制の強化	保守契約更新等の機会を捉えた、定期的なセキュリティ対策の見直し
	専門業者とセキュリティ対策に関するアドバイザリー契約の締結
その他	アンチウイルスソフトによる常時監視のほか、週1回の手動による検査を実施
	サーバーや端末等のログインパスワードの定期変更および最新プログラムへ更新を徹底　等

（10）携帯電話・スマートフォンの使用

受託業務で携帯電話やスマートフォンを使用する場合は、以下の点に留意する必要があります。

【携帯電話・スマートフォン使用時の遵守事項】

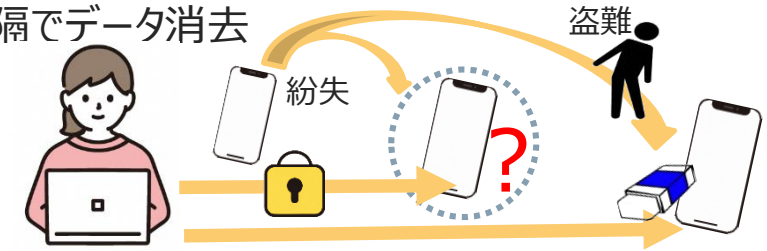
1）持ち出す場合は、肌身離さず持ち歩くなど、**紛失や盗難に十分注意**し、**持ち出しの記録を管理簿により管理**する。
2）使用後に**不要になったデータを直ちに消去**する。
3）**パスワード等のロックを設定**し、紛失や盗難時に備えて、**遠隔でのロックや遠隔データ消去のサービスを利用**する（推奨）。
4）従事者の**私物等**、許可されていない携帯電話やスマートフォンは**使用しない**。
5）LINE等、SNSの**個人アカウントで、受託業務で取り扱う情報をやり取りしない**。

遵守事項のイメージ

- パスワード等のロックを設定する

- 紛失や盗難時に利用されないように、遠隔からコントロールを可能にする

・遠隔でロック
・遠隔でデータ消去



- 受託業務で取り扱う情報をSNS（LINE等）でやり取りしない

例えば、こんな事故が起きています

【港区】高齢者在宅サービスセンターで携帯電話を一時紛失（令和５年１月）

- 東京都港区は、指定管理者が運営している高齢者在宅サービスセンターにおいて、**利用者の電話番号などが登録された連絡用の携帯電話を紛失した**ことを明らかにした。
- 同区によれば、**同センターの職員が利用者の送迎中**に、送迎の連絡用として使用していた**携帯電話1台を紛失**していることに気づいたもの。
- 紛失した携帯電話には、**利用者54人の氏名と電話番号、およびヘルパー事業所の電話番号6件が保存**されていた。
- 紛失の翌日、携帯電話捜索サービスを利用して紛失場所を中心に探したところ、利用者が住むマンションの敷地内で発見された。発信や情報の消去など操作の痕跡がないことを確認した。
- 対象となる利用者とヘルパー事業者には、指定管理者が説明と謝罪を行っている。

（出典：https://www.security-next.com/142952 ）

特(P.22)

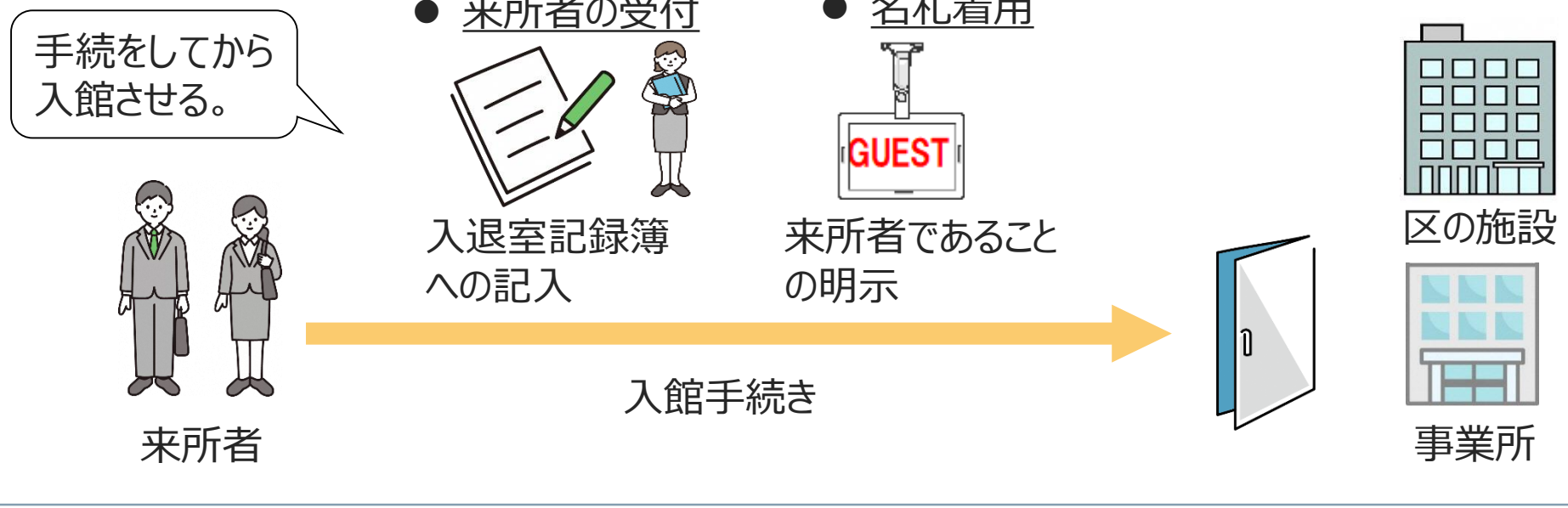
（11）施設の入退室管理

許可された者以外の入退室を防ぐとともに、情報が脅威にさらされた場合、原因を迅速に特定できるようにするため、以下の点に留意する必要があります。

【施設への入退室に関する遵守事項】

施設や事業所など、情報を取り扱う場所においては、来所者の受付や名札着用など、**入退室管理を行う**。

遵守事項のイメージ

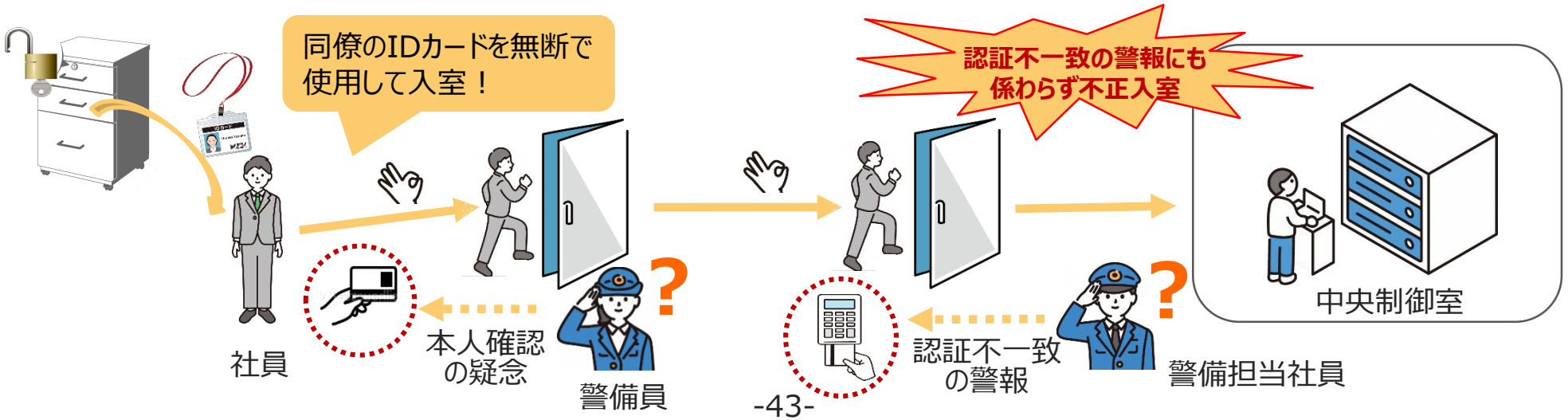


例えば、こんな事故が起きています

【柏崎刈羽原発】原発の心臓部に不正入室　ID「不一致」警報でも入室許可、社員が独断で認証情報変更も（令和３年２月）

- 東京電力柏崎刈羽原発（新潟県）で、令和２年９月に社員が**同僚のIDカードを無断使用して**中央制御室に入っていたことが判明した。
- 入室の際に、２ヶ所の出入り口でIDと**本人確認の疑念や認証情報が「不一致」という警報が出た**にもかかわらず、**警備員や警備担当社員が入室を許可**していた。
- 警備担当社員は、入域を認めた上、認証情報を不正入室した社員のものに独断で変更した。翌日、本来の持ち主が入室できず、IDの不正利用が発覚した。
- 中央制御室は原子炉を操作する設備で、危機管理上入退室が厳しく制限されているが、**ずさんな危機管理体制**が明らかになった。

（出典：https://www.tokyo-np.co.jp/article/84861）



（12）ソーシャルメディアの利用について

ソーシャルメディアで発信した情報は、瞬時に不特定多数の人々に公開されます。投稿内容によっては、区、所属する組織および自身の信用失墜につながるため、以下の点に留意する必要があります。

【ソーシャルメディア利用時の遵守事項】

1）ソーシャルメディアには、**受託業務で取り扱う情報を書き込まない。**また、**LINEやInstagram等のSNSで当該情報をやり取りしない**。

2）ソーシャルメディアにより情報を発信する必要がある場合、**インターネット上に公開して良い情報かそうでないかを正しく判断する**。

遵守事項のイメージ

- 当該契約で取り扱う情報は書き込まない

- 情報をSNS（LINE等）でやり取りしない　※ 再掲

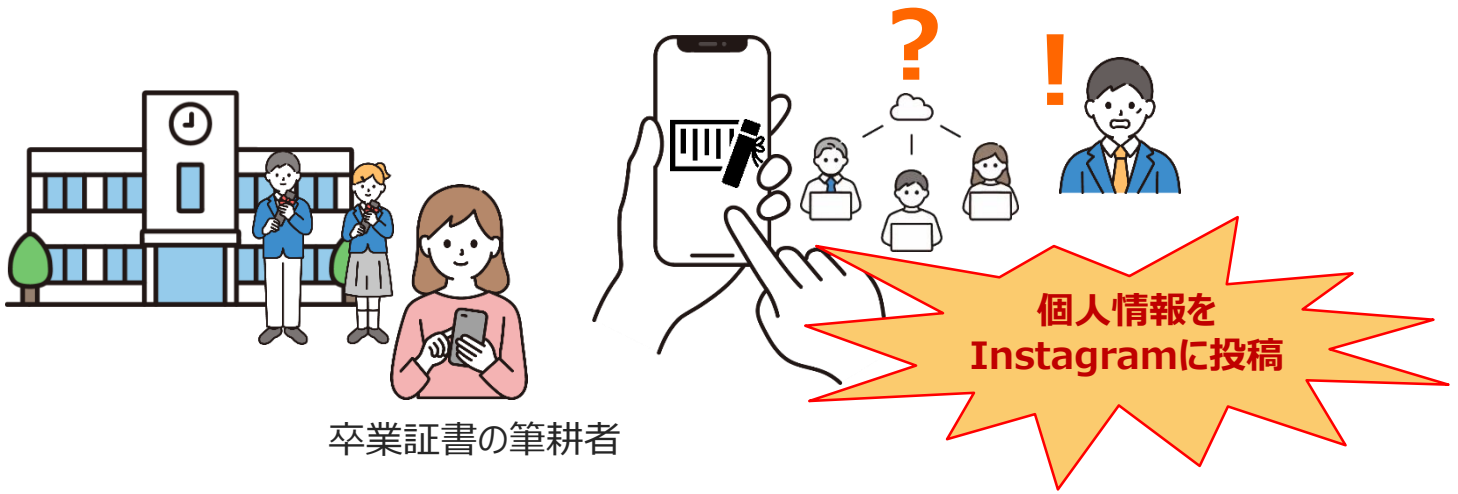
- 公開の範囲を意識して利用する

例えば、こんな事故が起きています

【東京都】卒業証書の筆耕者による生徒の個人情報の漏えい（令和６年２月）

- 東京都は、都立高等学校1校において、**卒業証書の筆耕者による生徒の個人情報の漏えい**が発生したことを公表した。
- 都によれば、同校の第三学年生徒4名に関する**卒業証書の写真（2名分の氏名・生年月日（全体）と2名分の氏名・生年月日（一部）が含まれる）**が、筆耕者名義の**Instagramに公開されていること**が、同校への匿名の電話で判明したもの。
- 同校から筆耕者に連絡し、直ちに写真は削除された。
- 当該投稿に氏名等が掲載されていた生徒と保護者には、同校管理職から説明および謝罪を行った。

（出典：https://www.kyoiku.metro.tokyo.lg.jp/press/press_release/2024/release20240207_01.html）



履行中に遵守すべき事項（13／16）

（13）Web会議の利用について

受託業務でWeb会議を利用する場合は、以下の点に留意する必要があります。

【Web会議利用時の遵守事項】

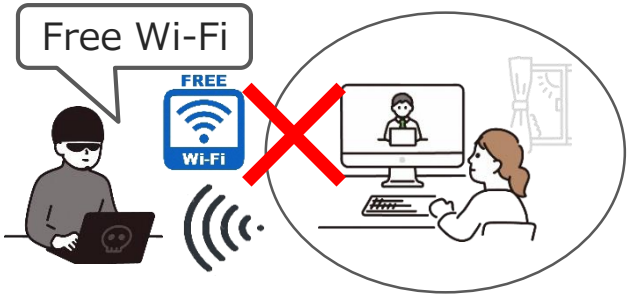
1）機密性の高い会議への利用は、**管理責任者が必要性が高いと判断した場合**に限る。
2）**重要情報が映り込まない、周囲の会話や電話等の音声が入らない場所**で利用する。
3）会議のURL、ID、パスコードなどは、**参加者のみに知らせ、使い回しをしない**。
4）全員の参加を確認後、会議をロックするなど、**第三者が参加できないように**する。
5）会議資料は原則メール等で参加者へ送付し、重要情報を含む資料は**画面共有しない**。
また、重要情報を含むファイルのアップロードはしない。
6）会議の通信では、傍受されるリスクのある**フリーWi-Fi等は利用しない**。

遵守事項のイメージ

- 重要情報の画面共有はしない

- 会話や電話等の音声が入らない場所で利用する

- 傍受されるリスクのある通信環境は利用しない



履行中に遵守すべき事項（14／16）

（14）テレワークについて

受託業務をテレワークで行う場合は、以下の点に留意する必要があります。

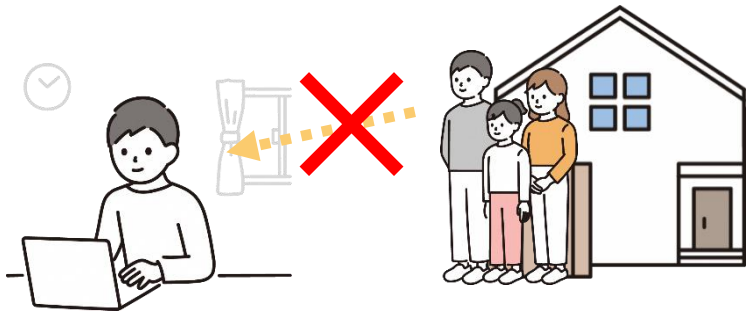
【テレワーク実施時の遵守事項】

１）**関係者以外（家族を含む）に見られない場所**で作業する。

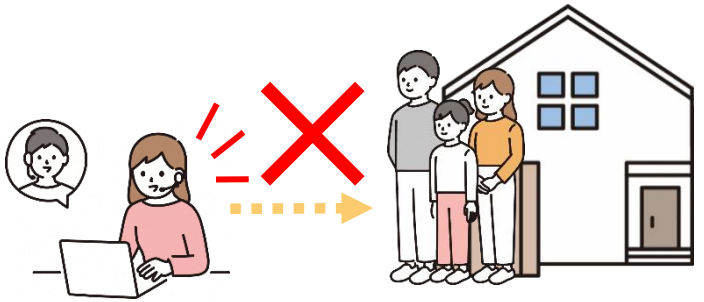
２）関係者以外（家族を含む）がいる場所で**重要情報を含む会話をしない**。

遵守事項のイメージ

- 関係者以外に見られない場所で作業する



- 関係者以外がいる場所で重要情報を含む会話をしない



履行中に遵守すべき事項（15／16）

（15）なりすまし等の防止

情報窃取の手段として、なりすましや盗み聞き等の**「ソーシャルエンジニアリング」**があります。

【ソーシャルエンジニアリング防止のための遵守事項】

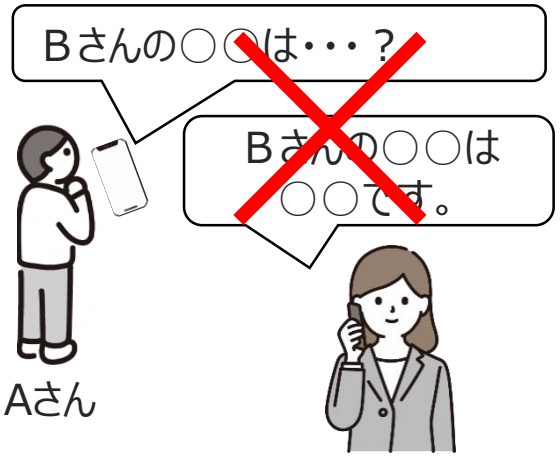
1）電話をかけた時に留守番電話であった場合、**個人情報を含む内容を録音しない**。
2）電話での問い合わせでは、こちらからかけ直すなどして、**本人以外の人に情報を伝えない**。
3）第三者がいる場所で、**個人情報を含んだ会話をしない**。

遵守事項のイメージ

● 本人以外に本人の情報を伝えない

（電話をかけた場合）

（電話を受けた場合）



● 第三者がいる場所で、個人情報を含んだ会話をしない

履行中に遵守すべき事項（16／16）

（16）事故等発生時の対応

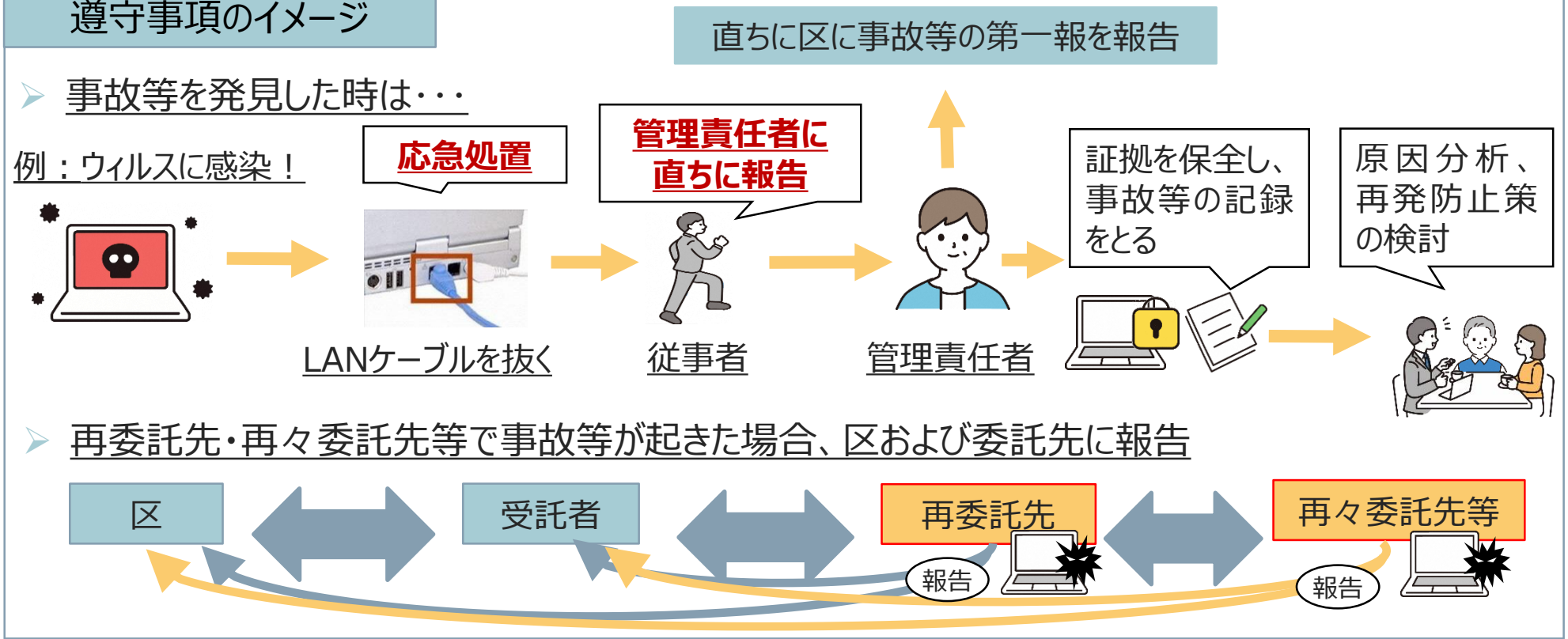
【情報セキュリティ事故等が生じた場合の遵守事項】

１）**直ちに応急処置を行う**とともに、管理責任者に報告する（管理責任者は**直ちに区に報告する**）。

２）事故等の原因を特定するため、証拠を保全しつつ**事故および対応の過程を記録する**。

３）原因を分析し、再発防止策まで含む**報告書を作成する**。

遵守事項のイメージ



第４章　契約終了時に実施すべき事項

対象：受託者

本章は、受託者が契約終了時に実施すべき事項を記載しています。

契約終了時に実施すべき事項

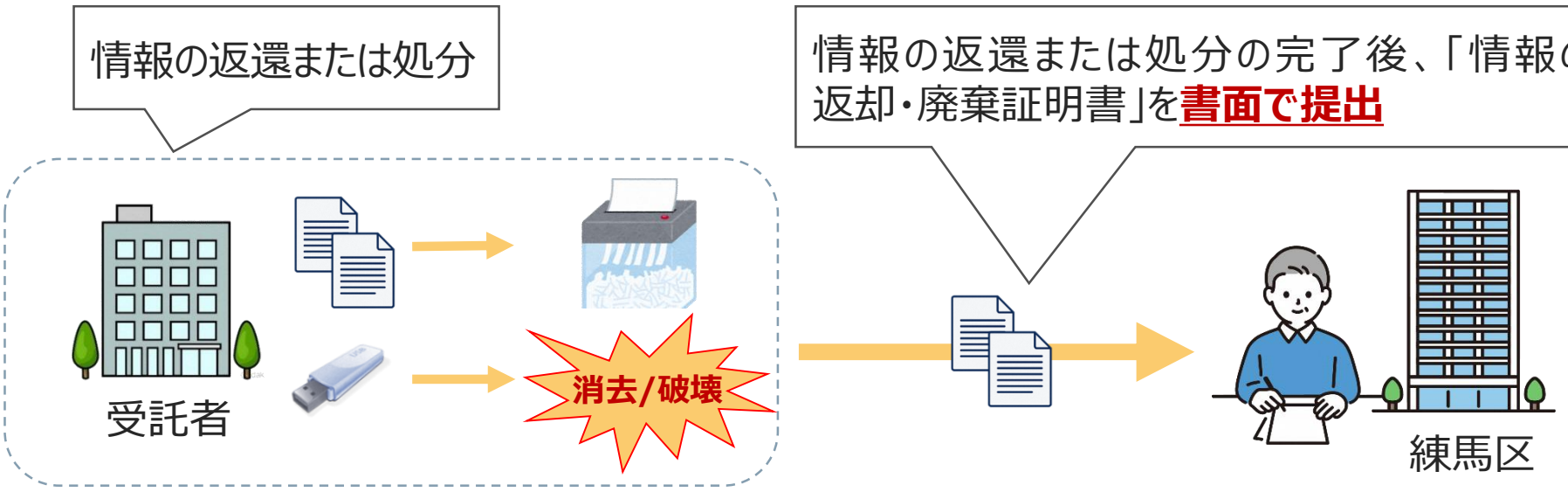
特(P.25)

a．情報の返還・処分

あらかじめ、業務の終了後に情報を返還するか処分するかを取り決める必要があります。
受託者は契約終了の際に、情報について区に**返還する**か**漏えいを来さない方法で確実に処分**して、その結果を区に**書面で報告する**必要があります。
※　契約期間中に、外部委託により処分する場合も含まれます。

しなければならないこと

※　書面の参考様式は、区から提示します。

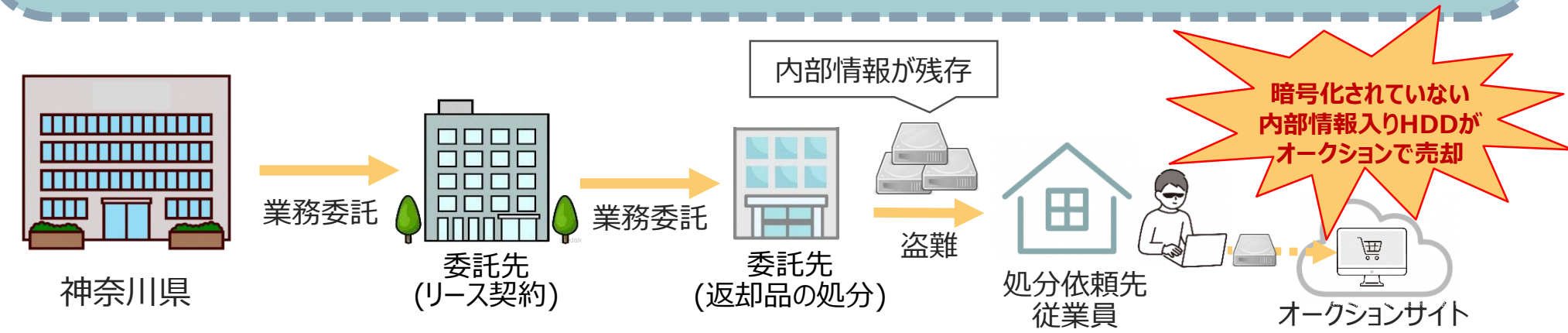


例えば、こんな事故が起きています

【神奈川県】リース返却後の内部情報入りHDDがオークションに（令和元年12月）

- 神奈川県が過去に使用したサーバのハードディスクが、**内部データが十分に消去されないまま、オークションを通じて売却されていた**ことがわかった。
- リース会社の**委託業者において、消去作業を行う前に従業員がハードディスク18台を盗み**、オークションサイトで売却していた。**落札者が同県内部情報と見られるデータを発見**し、11月26日に同県へ連絡。ハードディスクのシリアルナンバーから、返却されたサーバのハードディスクであることが判明した。
- ハードディスクについては、サーバ管理業者による簡易的なフォーマット作業の後、**リース会社にて高度な消去処理や物理的な破壊処理を行う契約**となっていた。リース会社は返却後のデータの消去処理を委託したが、県との契約に**データ消去処理を別会社に委託することについて制限する内容は盛り込まれていなかった**。
- 問題のハードディスクはいずれも**暗号化されておらず、データにアクセスできる**状態だった。
- 新たに導入されたサーバは、いずれもハードディスクが暗号化されている。旧サーバについて同県は「導入時に暗号化できる技術がなかった」と釈明した。

（出典： https://www.security-next.com/110534）



第５章　再委託について

対象：受託者

本章は、受託者が再委託や再々委託等をする場合に実施すべき事項を記載しています。

再委託について

a．再委託の制限

受託業務の再委託や再々委託等（※）（以下、「再委託等」という。）について、次の事項を遵守する必要があります。

【再委託等に関する遵守事項】

（１）やむを得ず、再委託等（再々委託等の場合は、個人情報を取り扱う場合のみ。以下同じ。）を行う場合は、**区から承認を得る（承認申請書を提出する）**。

業務内容に**特定個人情報（マイナンバー）を含む場合**、委託事業者が区の許諾を得ずに再委託等をしていることが判明した場合は、**番号法に抵触**するため、個人情報保護委員会への報告対象となります！

（２）個人情報を取り扱う再委託等の場合は、**契約締結前**に当該契約の受託予定者において、**特記事項等に規定する安全管理措置が講じられることをあらかじめ確認し、指定する書面により区に提出する**（（１）の書類と併せて提出する）。

★作成するのは、再委託等の受託予定者。提出するのは受託者。

（３）再委託等を行う場合には、**特記事項と同等以上の規定を設けて契約する**。

（４）再委託等を行う場合、当該契約の受託者（以下「再委託先等」という。）に、受託業務における**一切の義務を遵守させる**とともに、**その履行状況を監督する**。

（※）再々委託等：再委託先がさらに第三者に再委託する場合（それ以降の委託を含む）

a．再委託の制限（つづき）

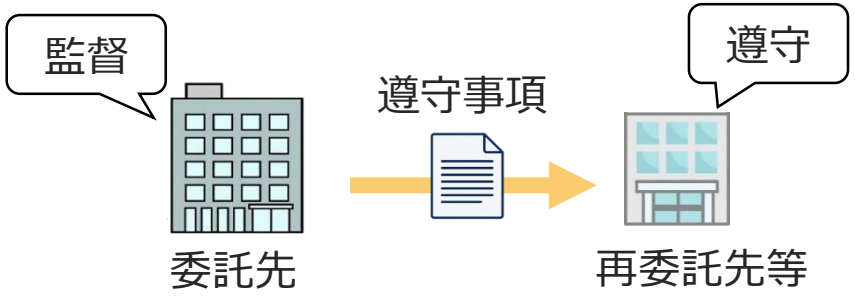
遵守事項のイメージ

- 区から承認を得る

- 個人情報を扱う場合は、「安全管理体制確認書」を提出させる

- 特記事項と同等以上の規定とする

- 受託者における一切の義務を遵守させ、履行状況を監督する

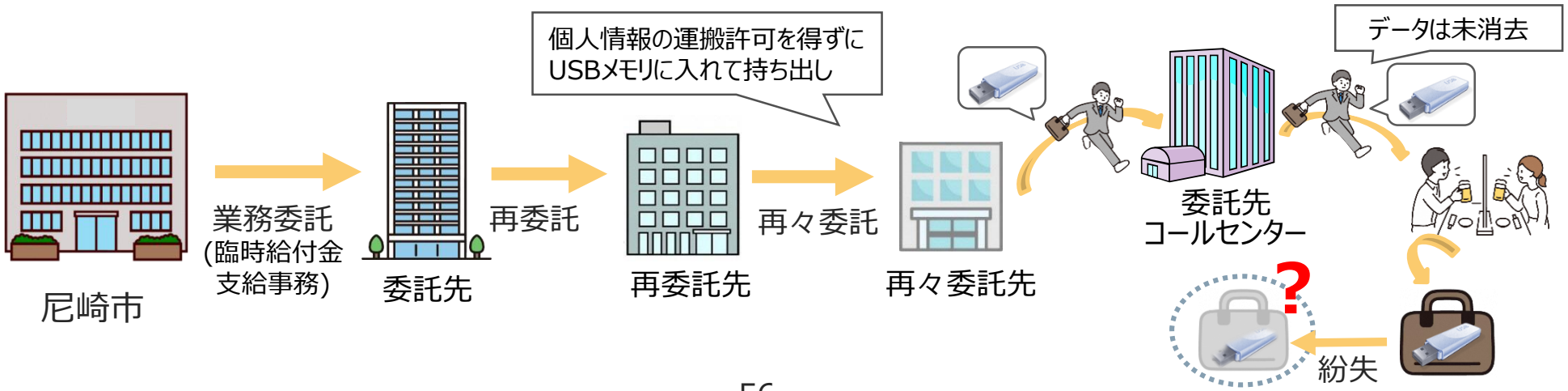


例えば、こんな事故が起きています

【尼崎市】個人情報を含むUSBメモリの紛失（令和４年６月）

- 尼崎市は、同市全住民の**個人情報を含むUSBメモリが所在不明**となっていることを明らかにした。
- 臨時給付金支給事務の**再々委託先従業員**が、全市民46万人の住民基本情報を含む個人情報約100万件が入ったUSBメモリ2つを、市の庁舎から事業者のコールセンターへ持ち出し、データを移管した後、**データを消去せずにコールセンターから持ち出し、飲酒を伴う食事の後、泥酔してカバンごと紛失**した。当該USBメモリにはパスワードが付与され、内容は暗号化されていた。
- 受託者は、委託者の事業所外でのデータ処理の許可を得ていたが、受託者の関係社員個人が記録媒体で**個人情報を運搬する具体的手法については、同市から許可を得ていなかった**。また、市は受託者に対し、持ち出す際に許可を得るべき旨を徹底していなかった。
- 加えて、受託者において、データ消去がされていない当該USBメモリを所持している作業者に対し、飲酒を伴う食事への参加を注意しない等、管理監督が適切に行われていなかった。

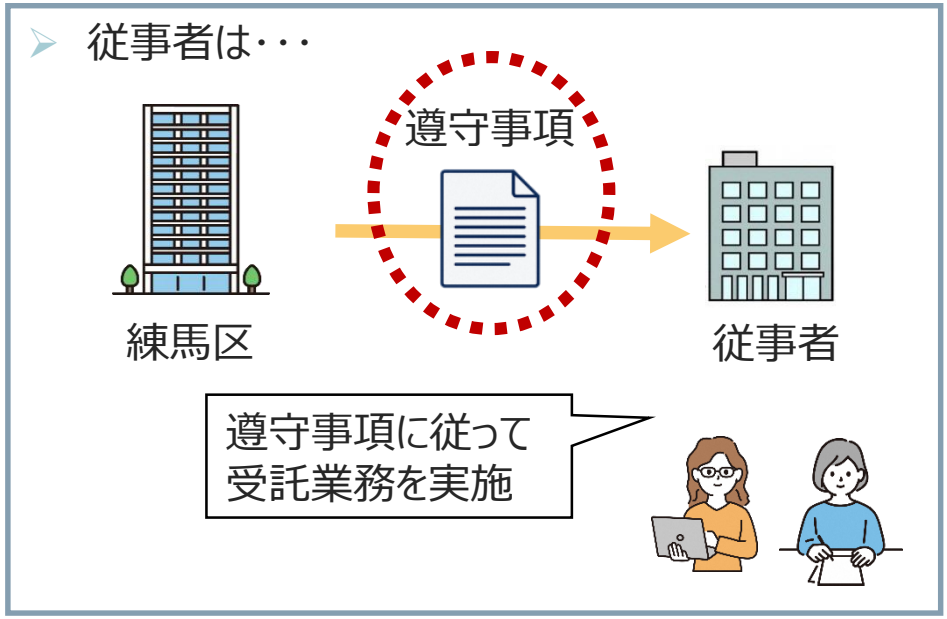
（出典： https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html）

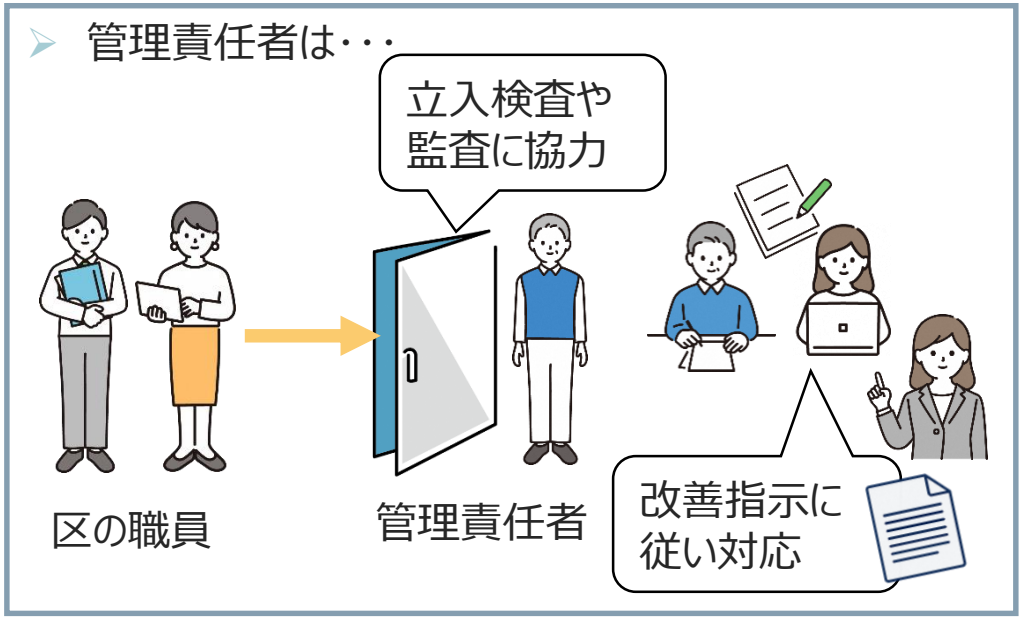


おわりに

特(P.23)

受託者およびその従事者が特記事項の内容を理解し遵守することは、情報セキュリティ事故等を防止することにつながります。
日ごろから、遵守事項や関係法令等に基づいて、情報を適切に取り扱うよう心がけてください。
なお、情報の取扱いに関して、区から受託者へ立入検査や監査を行う場合があります。その際には、ご協力ください。





復習テスト

対象：管理責任者、従事者

受託業務に従事する方が、第 3 章で学んだことの確認
および教材内容の復習を行うためのテストです。

遵守事項の復習（１）

- 今回の教材で取り上げた遵守事項について、〇か×で解答してください。

	○or✕	設問
メールの利用 (P.24、25)		Q１ 重要情報をメールで送信する時は、メール本文には記載せず添付ファイルとし、パスワード等で暗号化して送る。
		Q２ メールを送信するときは、宛先や添付ファイルに誤りがないか、自分でダブルチェックする。
		Q３ 複数人に一括でメールを送る場合、メールアドレスは「TO」ではなく「BCC」に設定する。
重要情報を含む 帳票および文書 (P.21、28、30、33)		Q４ 文書等を履行場所から持ち出す場合は、事前に練馬区の承認を得る必要がある。
		Q５ 送付する際は、宛先や封入物に誤りがないか、複数人でチェックする。
		Q６ 廃棄の際は原則としてシュレッダーや溶解処理で情報の判別を不能にするが、量が多い場合はこの限りではない。
記録の管理 （記録媒体） (P21、28、29、33)		Q７ 郵送する場合、記録媒体に情報が保存されていなければ管理簿に記録する必要はない。
		Q８ 持ち出すときは、持ち出しの承認から返却までを管理簿に記録する。

（次ページに続く）

遵守事項の復習（２）

（前ページの続き）

	○or✕	設問
私物等の利用禁止 (P.36、40)		Q９　緊急の場合は、私的に利用しているSNSで受託業務に関する情報をやり取りしてもよい。
記録媒体の 適切な利用 (P.28～30、33、36)		Q10　受託業務で使用する記録媒体を持ち出す場合、データはパスワードを設定する等により暗号化する。
		Q11　廃棄の際は、物理的な破壊または漏えいしない方法により、データが復元できない状態にして廃棄する。
受託業務で使用する パソコン等の適切な 管理 (P.35～37)		Q12　複数の情報システムを使う場合は、同じパスワードを設定する。
		Q13　情報漏えい等のリスクがあるため、必要な場合を除きID・パスワードは共用しない。
		Q14　受託業務で使用するパソコンに、許可なくソフトウェアをインストールしない。
外部サービスの利用 (P.38)		Q15　いつ・どこからでも仕事ができるよう、私的に利用しているクラウドサービスに情報を保存してもよい。
事故等発生時の対応 (P.49)		Q16　情報セキュリティ事故等が発生した時は、直ちに応急処置を行うとともに、管理責任者に報告する （管理責任者は直ちに区へ報告する）

解答（１）

- 正解は以下のとおりです。

	○or✕	設問
メールの利用 (P.24、25)	○	Q１ 重要情報をメールで送信する時は、メール本文には記載せず添付ファイルとし、パスワード等で暗号化して送る。
	✕	Q２ メールを送信するときは、宛先や添付ファイルに誤りがないか、自分でダブルチェックする。
	○	Q３ 複数人に一括でメールを送る際は、メールアドレスは「TO」ではなく「BCC」に設定する。
重要情報を含む 帳票および文書 (P.21、28、30、33)	○	Q４ 文書等を履行場所から持ち出す場合は、事前に練馬区の承認を得る必要がある。
	○	Q５ 送付する際は、宛先や封入物に誤りがないか、複数人でチェックする。
	✕	Q６ 廃棄の際は原則としてシュレッダーや溶解処理で情報の判別を不能にするが、量が多い場合はこの限りではない。
記録の管理 （記録媒体） (P.21、28、29、33)	✕	Q７ 郵送する場合、記録媒体に情報が保存されていなければ管理簿に記録する必要はない。
	○	Q８ 持ち出すときは、持ち出しの承認から返却までを管理簿に記録する。

（次ページに続く）

解答（２）

（前ページの続き）

	○or✕	設問
私物等の利用禁止 (P.36、40)	✕	Q９　緊急の場合は、私的に利用しているSNSで受託業務に関する情報をやり取りしてもよい。
記録媒体の 適切な利用 (P.28～30、33、36)	○	Q10　受託業務で使用する記録媒体を持ち出す場合、データはパスワードを設定する等により暗号化する。
	○	Q11　廃棄の際は、物理的な破壊または漏えいしない方法により、データが復元できない状態にして廃棄する。
受託業務で使用する パソコン等の適切な 管理 (P.35～37)	✕	Q12　複数の情報システムを使う場合は、同じパスワードを設定する。
	○	Q13　情報漏えい等のリスクがあるため、必要な場合を除きID・パスワードは共用しない。
	○	Q14　受託業務で使用するパソコンに、許可なくソフトウェアをインストールしない。
外部サービスの利用 (P.38)	✕	Q15　いつ・どこからでも仕事ができるよう、私的に利用しているクラウドサービスに情報を保存してもよい。
事故等発生時の対応 (P.49)	○	Q16　情報セキュリティ事故等が発生した時は、直ちに応急処置を行うとともに、管理責任者に報告する (管理責任者は直ちに区へ報告する)

［ 参考情報 ］ランサムウェア攻撃を受けた場合

情報システムで作業している際に以下の事象が確認された場合は、**ランサムウェア攻撃**(※)を受けている可能性があります。

- ✓ ネットワーク内部の複数のシステムでファイルの拡張子が変わり開封できなくなった
- ✓ 自組織から窃取されたとみられるファイルを暴露する投稿が行われた
- ✓ 攻撃者から通知が届いた

※ランサムウェア攻撃： 組織の内部ネットワークに侵入した後、情報窃取やファイルの暗号化により、身代金の要求などを行う攻撃

このような攻撃を受けた場合は、情報セキュリティ事故の対応ルールに従うとともに、インシデント対応を進める上で、以下の情報も参考としてください。

「侵入型ランサムウェア攻撃を受けたら読むFAQ」

URL： https://www.jpcert.or.jp/magazine/security/ransom-faq.html
出所： 一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)