個人情報保護ハンドブック
＜JISQ15001＞

2026年度個人情報保護研修用資料（本社・大阪）

株式会社テンダーラビングケアサービス

個人情報とは…

個人に関する情報であって、当該情報に含まれる氏名、生年月日、
その他の記述などによって特定の個人を識別できるもの

たとえば・・・

◆「生年月日」だけの情報＝同じ日に生まれた人がたくさんいて特定できない
⇒個人情報とはいえない

◆「生年月日＋住所」の情報＝特定される可能性が高い⇒個人情報となる可能性大
（※双子の場合等、特定できないこともある）

◆「生年月日＋住所＋氏名」の情報　＝ 完全に特定される ⇒ 個人情報

基本的な個人情報

□氏名

□性別 □生年月日 □住所 □電話番号 □メールアドレス □会社名 □顧客番号

重要な個人情報

経歴・成績	経済的属性	心身情報	生活事項
□学業・学歴	□所得・収入	□体格・体力	□家族状況
□職業・職歴	□資産状況	□運動能力	□親族・続柄
□地位	□取引状況	□写真・肖像	□婚姻
□資格	□口座番号等		□居住状況
□成績・評価			□意見・要望
□賞罰			□趣味・嗜好

特定の機微な個人情報

□思想、信条および宗教
□人種、民族、門地、本籍地、身体・精神障害、犯罪歴
□労働者の団結権、団体交渉、その他団体行動の行為に関する事項
□集団示威行為への参加、請願権の行使、その他政治的権利の行使に関する事項
□保健医療および性生活に関する事項

個人情報管理の重要性

1．個人情報の管理はなぜ必要？
- はじめに
- 個人情報の取扱いに関する事故の傾向
- 個人情報の取扱いに関する事故の影響
- 個人情報を適切に取り扱うために

2．当社の個人情報取扱いルールについて
- 個人情報保護方針
- 個人情報保護の体制
- 個人情報保護に関する規程
- 緊急事態への対応

3．まとめ

１．個人情報の管理はなぜ必要？

はじめに

はじめに

お客様に安心・信頼して取引を続けていただく

個人情報を活用して自社のサービスを拡充する

自社事業の継続・発展、社会的な信頼の獲得

したがって・・・

個人情報の漏えい等の事故は大きな社会問題に！

頻発する個人情報の漏えい等の事故

- 巧妙化、高度化するサイバー攻撃
- ヒューマンエラーによる事故
  - ✓データの誤入力、誤送信、誤操作
  - ✓置き忘れ、盗難による紛失など
- 内部（関係者）による不正行為
- 委託先からの漏えい等

など

１．個人情報の管理はなぜ必要？

個人情報の取扱いに関する事故の傾向

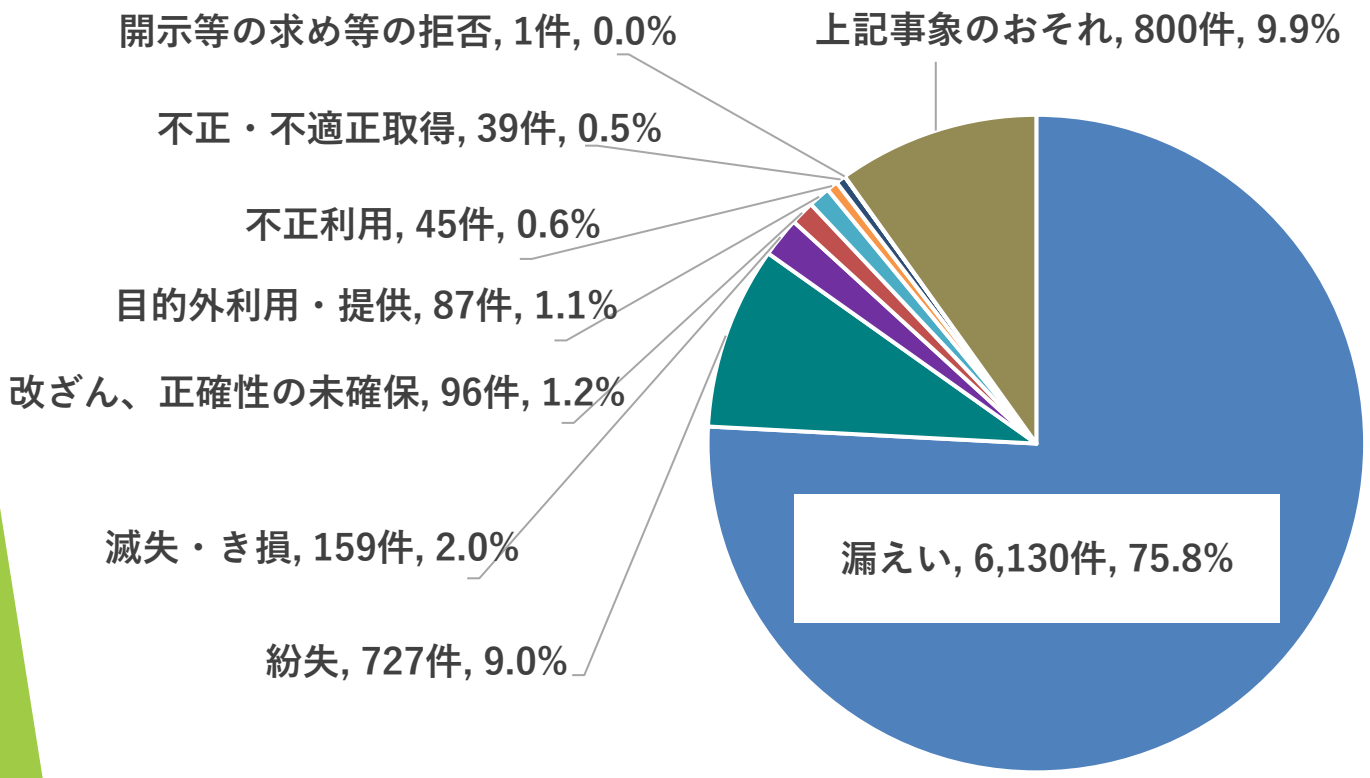
個人情報の取扱いに関する事故の傾向

- JIPDEC公表の統計資料
  2024年度「個人情報の取扱いにおける事故報告集計結果」より

トップページ＞審査基準・指針＞お役立ち情報・ツール
https://privacymark.jp/guideline/wakaru/index.html

※JIPDEC（一般財団法人日本情報経済社会推進協会）
　当社プライバシーマークの認証機関

発生事象別の傾向

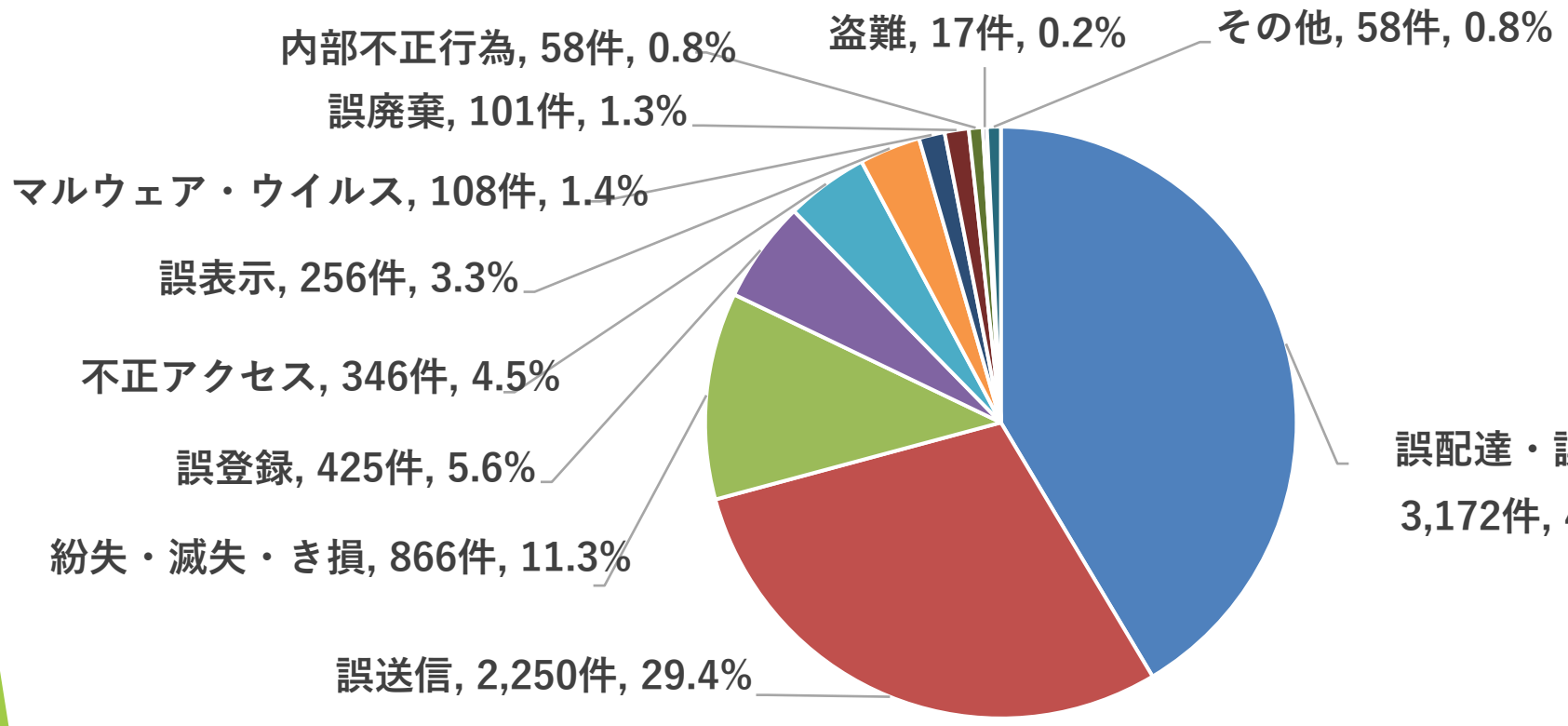


「漏えい」「紛失」が
全体の
約85%

「漏えい」が一番多く、次いで「紛失」、そして「滅失・き損」の順。
全体の約85%を「漏えい」「紛失」が占める。

出典：（2024年度）「個人情報の取扱いにおける事故報告集計結果」

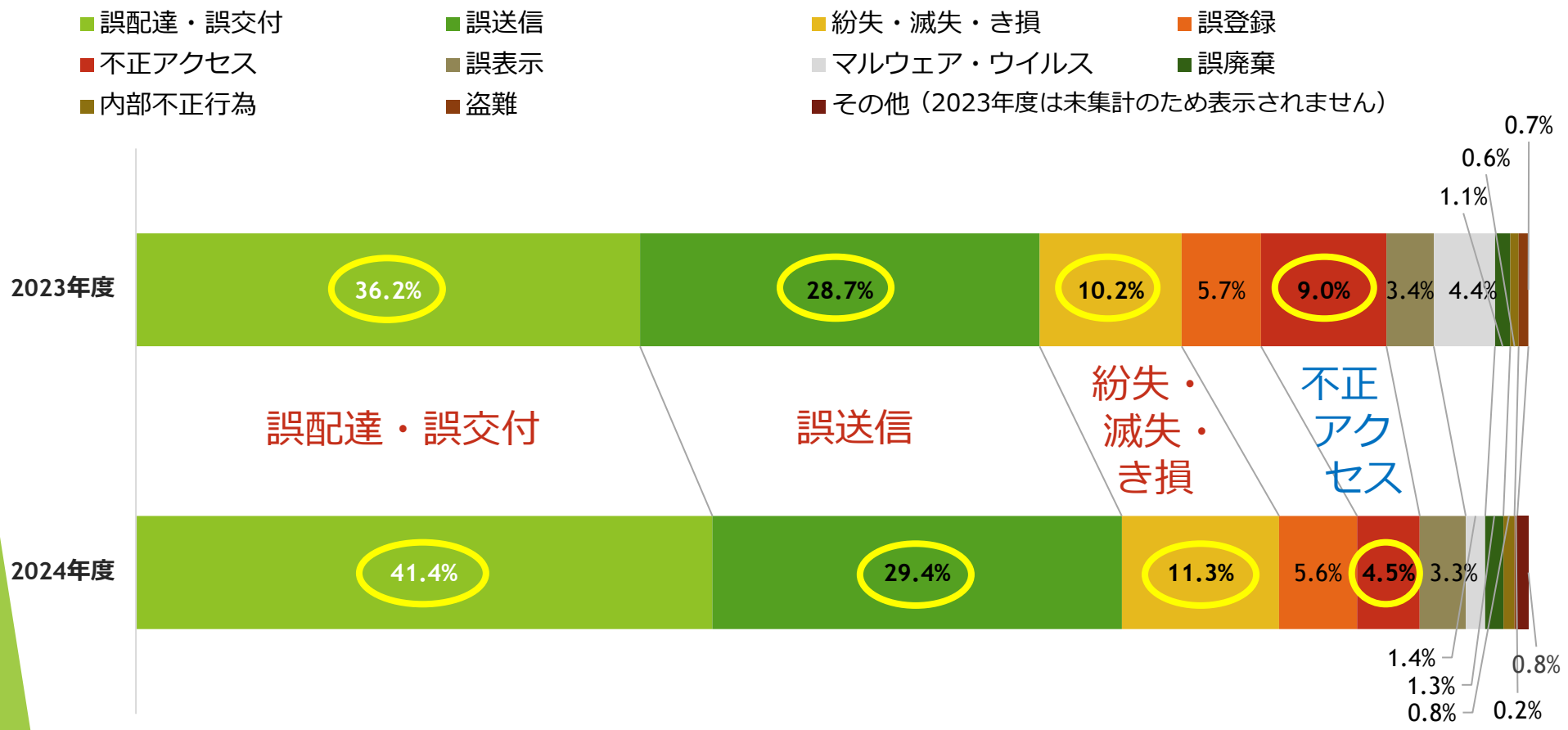
事象分類別の傾向



「誤配達・誤交付」が一番多く、次いで「誤送信」、そして「紛失・滅失・き損」の順。

出典：（2024年度）「個人情報の取扱いにおける事故報告集計結果」

事象分類別の傾向（前年度比較）



前年度と比べると「誤配達・誤交付」（ 36.2 %→41.4%）「誤送信」（28.7%→29.4%）、「紛失・滅失・き損」（10.２%→11.3%）の割合は増加傾向。
「不正アクセス」（9.0%→4.5%）の割合は減少。

不正アクセス、マルウェア・ウイルスの事例

不正アクセスの事例

情報システム課の指示どおり
PCなどを利用すること

- WEBサイトの会員専用ページに対し、第三者が顧客を装い不正にアクセスし、個人情報の変更および不正な注文が行われた。
- 管理サーバに、悪意のある第三者による不正アクセスによってサーバに登録していた複数人の個人情報が不正取得、不正利用された。

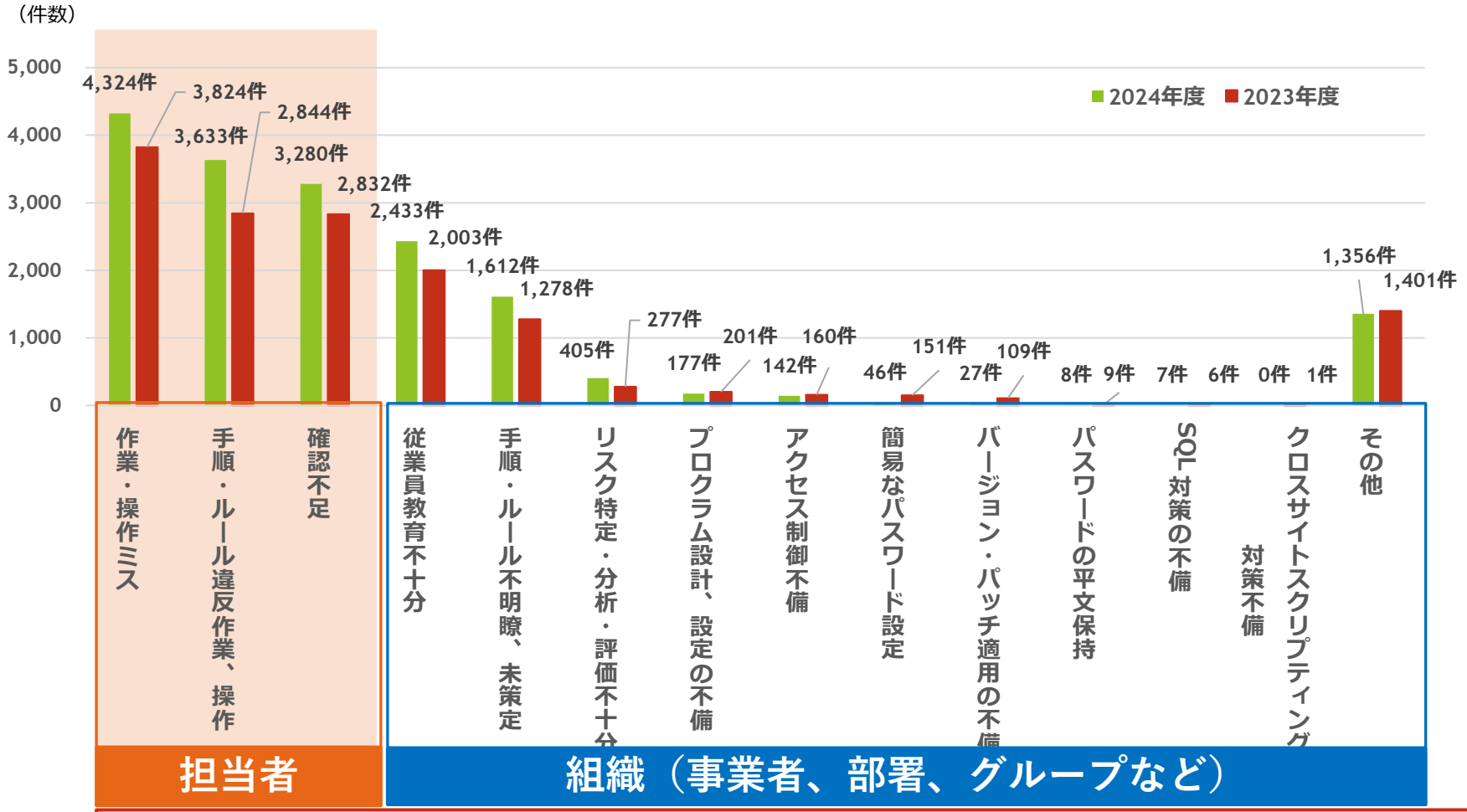
マルウェア・ウイルスの事例

- ファイルサーバのランサムウェア感染により、個人情報が流出した。
- 従業員Aが、受け取ったメールに添付されていたファイルの「コンテンツの有効化（マクロの有効化）」を実行したところEmotet（エモテット）に感染し、社内・社外に従業員Aを偽装したウイルス添付のなりすましメールが拡散した。

誤送信の事例

動画を視聴👉click

原因別集計の傾向（前年度比較）



担当者が適切な作業を実施しなかったことによる事故等が増加傾向。

日常業務での心遣い
～作業・操作ミス（誤送信・誤送付など）を防ぐために～

- 作業は集中して行いましょう！
  - ✓ 操作ミスによる重大な事故を防ぐため、上司に呼ばれても「少々お待ちください」と断ることは、プロ意識の高い適切な判断です。※断り方は角を立てず
  - ✓ あらかじめ上司に「集中が必要な操作中は、安全のためにお声がけいただいてもすぐに対応できないことがあります」と共有しておくと、よりスムーズです。※朝礼時に作業を共有
- 声をかける時の作業状況をよく見てあげましょう！
  - ✓ メールを書いているなどの状況の時は、「終わったら声をかけてね」など、作業者がミスを起こしにくい、職場環境をみんなで作りましょう。
  - ✓ 可能であれば、声かけ前に状況を把握すると良いでしょう。

１．個人情報の管理はなぜ必要？

個人情報の取扱いに関する事故の影響

個人情報の事故を起こしてしまうと・・・

- お客様は・・・
  - ✓ もうこの会社を利用するのはやめよう。
  - ✓ 信頼して預けたのに、悪用されたらどうしよう。
  - ✓ 私の情報も漏えいしたかもしれない。心配・・・。
- 取引先は・・・
  - ✓ 今後、継続的な取引は見直した方がいいだろうか？
  - ✓ 取引への対応が遅れて困る。
- 自社は・・・
  - ✓ 問合せが殺到、大変だ。
  - ✓ 原因は何？影響は？何をすれば？
  - ✓ これまで築いてきた信頼は・・・。
  - ✓ 苦情の対応に苦慮・・・。

個人情報の取扱いに関する事故の影響

社会的な信用の失墜

- 顧客や取引先の信用を失う
- 企業ブランドのイメージダウン

経済的な損失

- 再発防止策への投資
- 本人への補償
- 業務の停止（営業機会の損失）
- 信用回復のための投資

事業継続へのダメージ

- 株価の下落
- 取引の減少
- 経営状況の悪化

最悪の場合、
事業終了も・・・

個人情報の取扱いに関する事故の影響(まとめ)

非常に大きな損失が発生

- 本人へのお詫びや補償以外にも、社会的説明責任を果たすには様々な対応が必要

影響の長期化

- 被害規模の拡大
- 漏えいした情報の回収が困難
- 一度失った信頼の回復が困難

一瞬の事故が大きな問題に。
では、どうしたら・・・？

１．個人情報の管理はなぜ必要？

個人情報を適切に取り扱うために

～個人情報取扱いルールの運用～

ルールを定め、理解し守ること

事故を起こさない（未然防止）

事故を起こさないための体制・対策のルール化

従業者は

定められたルールを理解し、守る

事故が発生した場合の影響を最小限に抑える

早期発見、緊急時対応のルール化や対策の実施

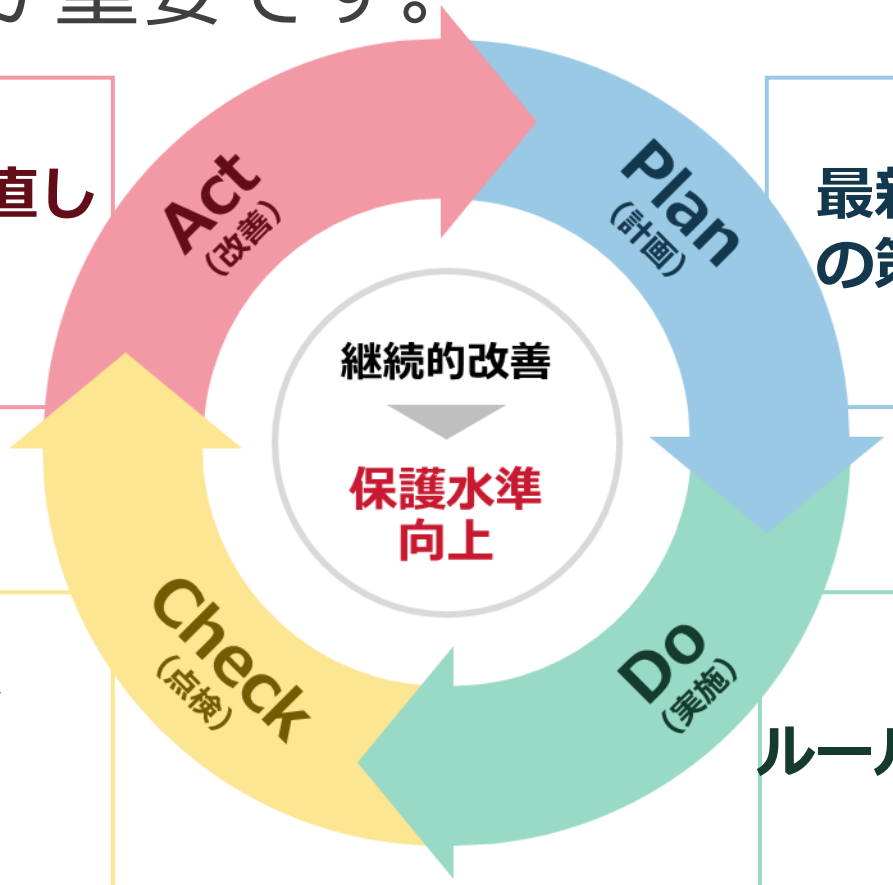
従業者は

事故発覚・発見時にルールに従って行動する

個人情報保護リスク対策の見直し

- 個人情報の取扱いのPDCAサイクル
  ルールは適宜見直し、必要に応じて改善することが重要です。

リスク対策の見直し
ルールの見直し



最新のリスク対策の策定

運用状況の確認、対策の有効性のレビュー

従業者は

ルールに従った運用

万が一事故を起こしてしまったら

- 重要なことは迅速な対応と再発防止の徹底

迅速な対応

- 緊急時対応のルールに従い迅速かつ適切な対応

→ 早期の信頼回復

再発防止の徹底

- 適正な改善策、再発防止策の策定と実施を徹底

→ 保護水準のさらなる向上

２．当社の個人情報取扱いルールについて

個人情報保護方針

https://www.tenderlove.co.jp/privacy/

認証番号：10862123
更新回数：(08)

2024/12更新完了（**2年**おき）
2026/10中旬ごろ　更新審査

個人情報保護方針

制定日：平成20年4月1日
改定日：令和6年11月1日
株式会社テンダーラビングケアサービス
代表取締役 柚上 尚満

株式会社テンダーラビングケアサービスは、「人と人のふれあいのあるぬくもりのある社会の構築に供する」ことを目的として、福祉サービスに関する事業を行っています。当社が事業活動を行う上で、個人情報を適切に取り扱うことは社会的責務であると考えており、当社では、この責務を全うするために、以下の取り組みを実施します。

1. 個人情報の取得、利用及び提供について

当社の全ての事業で取り扱う個人情報及び従業員の個人情報について、適切な取得、利用及び提供を行い、特定した利用目的の達成に必要な範囲を超えて個人情報を取り扱うことはありません。また、そのための措置を講ずることとします。
尚、利用目的を超えて個人情報の取り扱いを行う場合には、あらかじめご本人の同意を得ます。

2. 個人情報に関する法令や指針、規範について

個人情報に関する法令・国が定める指針その他の規範を守ります。

3. 個人情報の安全管理について

個人情報への不正アクセスや、個人情報の漏えい、紛失、破壊、改ざん等に対して、合理的な防止並びに是正措置を行います。

4. 個人情報に関する苦情及び相談について

個人情報に関する苦情及び相談には、速やかに対処します。

5. 個人情報保護の取り組み（個人情報保護マネジメントシステム）について

個人情報の保護を適切に行うため、継続的にその取り組みを見直し、改善します。

個人情報保護の体制

株式会社テンダーラビングケアサービス　個人情報保護体制図

更新日:2026/3/25

バクラク稟議
14563

選任者

主担：
補佐：

深澤

主担：萩原
補佐：池田(哲)

柏木

大森

部門長

栗本

各部門情報管理者
人材営業部：根岸
人事・総務：萩原

LS：山口譲
業務：浦野

G：山崎
PR：深浦

施設：大森/梅澤
施設営業：松尾

～役割～

個人情報保護管理者：PMS運用責任者。緊急時対応時、個人情報の漏洩や不正利用が発生した場合の対応を指揮する。

事務局：PMS運用担当者。個人情報保護委員会や認証機関のJIPDECとの事務手続き。Pマークに関する問い合わせは事務局まで。

※PMS（個人情報保護マネジメントシステム）

個人情報保護の体制

個人情報保護体制上の役割	責任
トップマネジメント	当社PMSの最高責任者として、管理責任者、監査責任者を指名し、PMSを実施させる。
個人情報保護管理者	当社PMSの統括責任者として、PMSの構築、維持および個人情報取扱いの管理全般について責任を負う。
個人情報保護監査責任者	全部門の監査を計画、実行し、代表者に報告する。
苦情相談窓口責任者	保有個人データに関する問合せや各種依頼への対応、及び個人情報取扱についての苦情相談等に対応する。
情報システム管理者	情報システムに関して、PMSを維持するための安全管理対策を実施する。 システム導入時に、導入プロジェクトに参画。セキュリティ面での管理監督を行う。
特定個人情報等事務取扱責任者	個人番号を含む個人情報の取扱いについて、特定個人情報取扱いの管理全般について責任を負う。
特定個人情報等事務取扱担当者	個人番号を含む個人情報の取扱いについて。特定個人情報等事務取扱責任者の指示を受けて適切な取得、利用、保管を実施する。

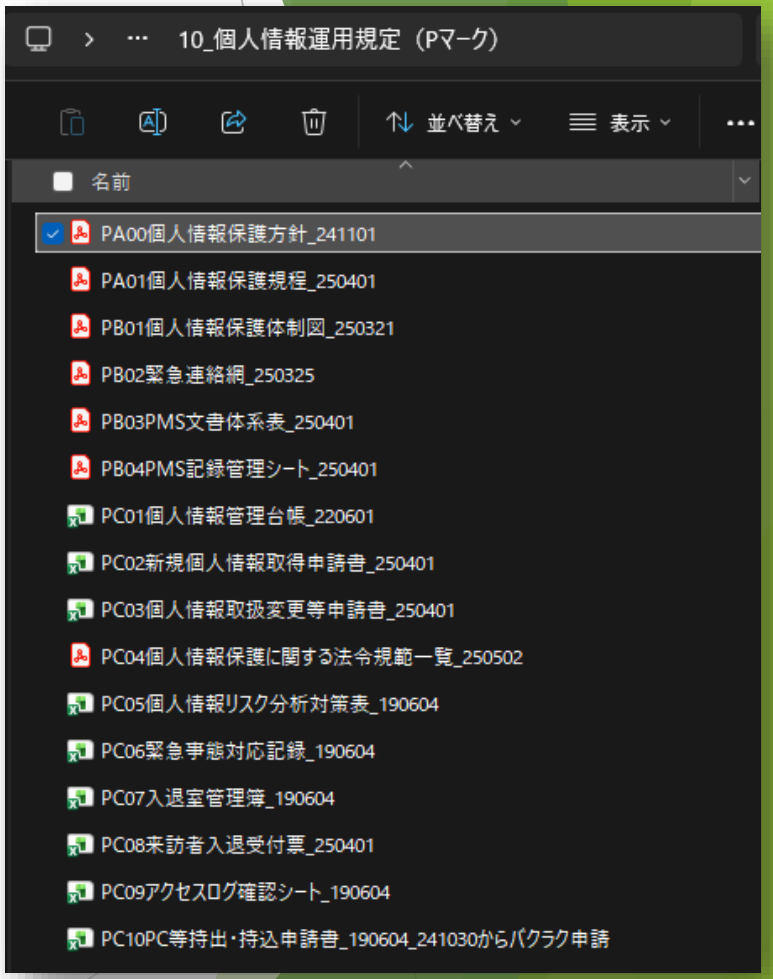
個人情報保護に関する規程

保管場所

¥¥192.168.254.13¥d¥00_全社共有¥01_規定¥01_本社・大阪支店¥10_個人情報運用規定（Pマーク）¥PA01個人情報保護規程_250401.pdf

- ✓個人情報保護方針
- ✓個人情報保護規定
- ✓個人情報取得同意文書
- ✓秘密保持契約書
- ✓個人情報開示請求書

など

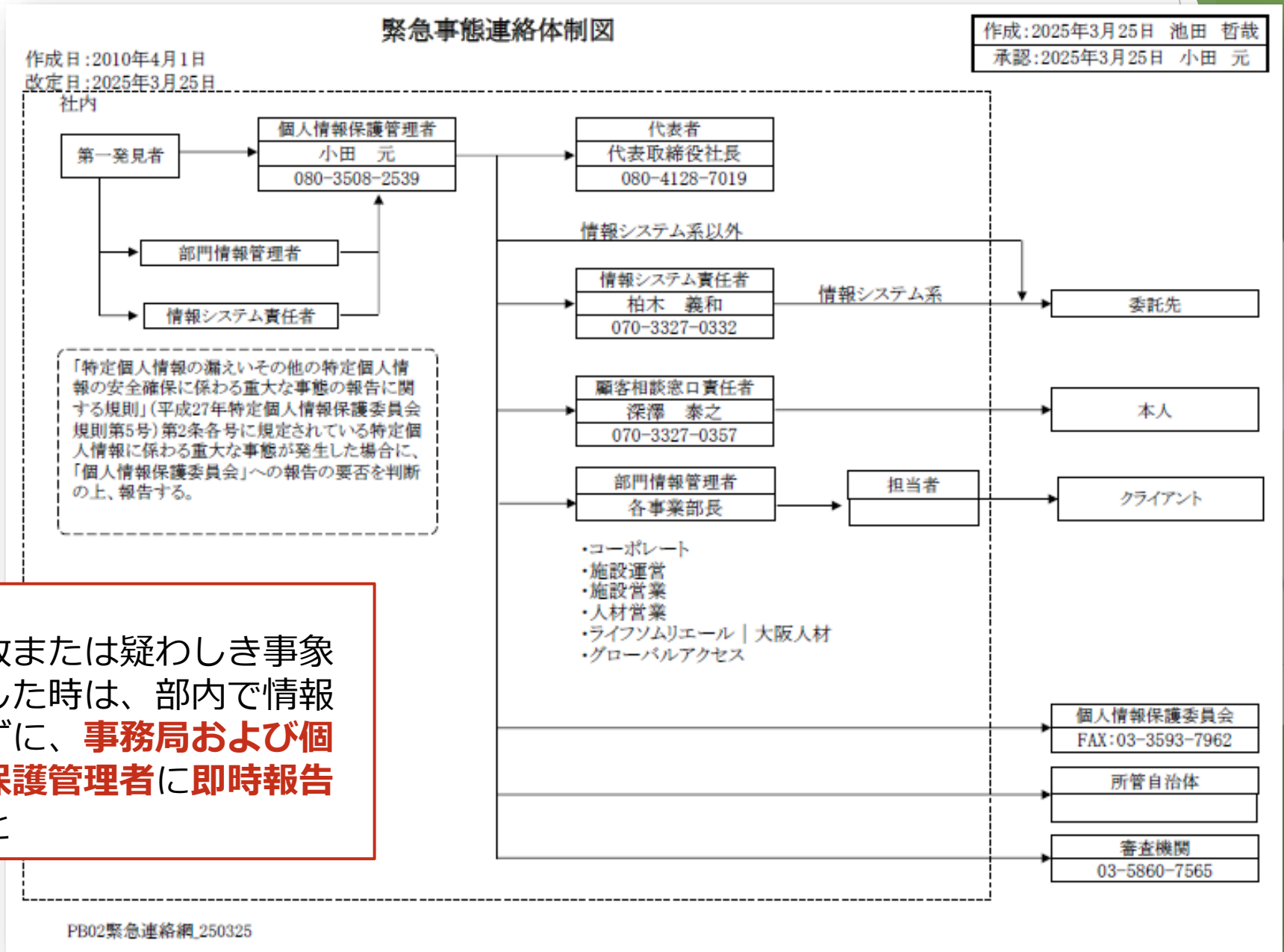


ITサービス利用の心得

～遵守するべき６つの基本ルール～

情報セキュリティの基本ルールです、しっかりと認識してください。

緊急事態への対応



緊急事態連絡体制図

作成：2025年3月25日　池田　哲哉
承認：2025年3月25日　小田　元

作成日：2010年4月1日
改定日：2025年3月25日

社内

第一発見者

個人情報保護管理者
小田　元
080-3508-2539

部門情報管理者

情報システム責任者

「特定個人情報の漏えいその他の特定個人情報の安全確保に係わる重大な事態の報告に関する規則」（平成27年特定個人情報保護委員会規則第5号）第2条各号に規定されている特定個人情報に係わる重大な事態が発生した場合に、「個人情報保護委員会」への報告の要否を判断の上、報告する。

代表者
代表取締役社長
080-4128-7019

情報システム系以外

情報システム責任者
柏木　義和
070-3327-0332

情報システム系

委託先

顧客相談窓口責任者
深澤　泰之
070-3327-0357

本人

部門情報管理者
各事業部長

担当者

クライアント

・コーポレート
・施設運営
・施設営業
・人材営業
・ライフソムリエール｜大阪人材
・グローバルアクセス

個人情報保護委員会
FAX：03-3593-7962

所管自治体

審査機関
03-5860-7565

PB02緊急連絡網_250325

【Point】
漏洩事故または疑わしき事象が発生した時は、部内で情報を留めずに、**事務局および個人情報保護管理者**に**即時報告**すること

3．まとめ

日常業務における心掛け①

1) オフィススペースの管理（来訪者の記録について）

- 来訪者の方を執務スペースにお迎えする場合には、入退室管理簿に記入いただくとともに面談者が面会確認の押印または署名をします。

2) 宅配便など業者との受け渡しは、執務スペースの外でおこなうこと

- 大きな荷物の受渡しであっても、執務スペース内には入れないで、執務スペース外での対応が原則です。執務室へ入れる場合は、必ず社員が同行します。

3) むやみに個人の住所、電話番号を教えないこと

- 社外からの問合せに、**本人の承諾なし**に従業員等の自宅住所や電話番号等は教えてはいけません。本人から折り返し連絡を入れる旨を、問合せ先に伝えましょう。

4)個人情報等重要な書類やメディア類は所定の場所に保管すること

- 個人情報文書やメディア類は所定の場所で施錠管理し、退社時に施錠します。自宅や出張先などへ持ち出しは、承認が必要です。

5) 各種パスワード管理は自己責任で行うこと

- 他人にわかるパスワード（名前、誕生日等）は設定してはいけません。社内においても誰にも教えてはいけません。**パソコンや机に貼って**おくのは**厳禁**です！

6) パソコンにはパスワード付スクリーンセーバーを設定すること

- 離席時、他人に覗かれないようにパスワード付スクリーンセーバーを設定しましょう。

日常業務における心掛け②

7) 機器類の持込み・持出しは許可を受けること

- 原則として、PC等の機器類の社内外への持込み・持出しは禁止です。
  機器類の持込み・持出しには、**個人情報保護管理者**の事前許可が必要です。

8) 記録媒体の持ち込み、持ち出しはしないこと

- CD-R、USBメモリ等の記憶媒体の持込み・持出しは原則禁止です。業務上必要な場合には、事前に責任者の許可を受けてください。

9) 帳票類や記録媒体の廃棄はルールどおりに行うこと

- 個人情報の入った帳票類はシュレッダー等で、記録媒体はデータの消去並びにそれ自体を物理的に破壊して処分しましょう。

10) 紛失・盗難の発生の際には、責任者へ届け出ること

- 鞄やノートパソコン等の置き忘れや盗難が発生した場合は、**遅滞なく**上司または部門の責任者を通じて個人情報保護管理者に報告しましょう。届出・連絡が遅れると、情報漏洩の被害は拡大します。

11） 予期しない個人情報の提供が発生していないか気をつけること

- 個人情報の提供には、原則として本人の同意が必要です。資料・データを社外へ提供するときは、個人情報や秘密情報を含んでいないか、　含む場合は提供が社内で承認されているかを必ず確認してください。

日常業務における心掛け③

12） 個人情報を委託する場合は、契約状況を確認すること

- 委託先で万一事故が生じた場合、**当社も責任**を問われます。委託する場合は、委託先を選定し、秘密保持契約や誓約書が交わされていることを事前に確認することが必要です。

13） 不用意に社外へ情報が渡らないよう注意すること

- **社外や社員以外の人がいる場所**で、不用意に個人情報や**営業秘密**に関することを**話してはいけません**。また社外の電子掲示板等に社内情報や個人情報の書き込みをしてはいけません。

14） 机の上や身の回りの整理整頓を徹底すること

- 「クリアデスク、クリアスクリーン」は、個人情報保護の基本です。
机上の書類放置や離席時のPC画面の消し忘れにより、重要な情報資産が持ち出されてしまう事にもなりかねません。

クリアデスク=退社時、中座時に机の上等を整理整頓しておくこと

クリアスクリーン=退社時、中座時にモニタを非表示にしておくこと
デスクトップ整理: アイコンが散らかった状態にせず、ファイルは決まったフォルダやサーバーに保存し、デスクトップはできるだけ綺麗に保つ（これも広義のクリアスクリーン）。

ヒヤリハット事例①

第三者提供_case1

学習塾で生徒同士のトラブルが発生し、生徒Aが生徒Bにケガをさせてしまった。

↓

生徒Aの保護者が、『生徒Bとその保護者に謝罪するため生徒Bの連絡先を教えてほしい』と学習塾に尋ねてきた。

↓

名簿に記載されている生徒Bとその保護者の氏名・住所・電話番号を教えてしまいそうになった。

Point

☑人の生命・身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるときなど、第三者提供制限の例外事由に該当する場合を除き、個人データ（個人情報データベース等を構成する個人情報）を第三者に提供する場合には、あらかじめ**本人の同意が必要**となります（第三者提供共通）。

☑謝罪したいというような理由であっても、本人に無断で個人データを提供してはいけません。提供する前に、生徒Bとその保護者から同意を得ましょう。

引用元：個人情報保護委員会　https://www.ppc.go.jp/files/pdf/pd_hiyari01.pdf

ヒヤリハット事例②

第三者提供_case2

会社に従業員の親を名乗る者から電話があり、至急子供（従業員）と連絡を取りたいので、携帯電話番号を教えてほしいと言われた。

⬇

従業員が営業で外出中であったため、携帯電話番号を教えてしまいそうになった。

Point

☑人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるときなど第三者提供制限の例外事由に該当する場合を除き、個人データを第三者に提供する場合には、あらかじめ**本人の同意が必要**です。

☑社会通念上、やむを得ないと思われる場合や本人の家族・親族等からの照会であっても、個人データを第三者に提供する場合には、あらかじめ本人の同意が必要であることから、まずは会社から従業員に連絡をするなどの対応が望ましいと考えられます。

☑個人データの第三者提供に当たっては、必ずしも第三者提供のたびに同意を得なければならないわけではありません。例えば、個人情報の取得時に、その時点で予測される個人データの第三者提供について、包括的に同意を得ておくことも可能です。

引用元：個人情報保護委員会　https://www.ppc.go.jp/files/pdf/pd_hiyari01.pdf

ヒヤリハット事例③

第三者提供_case3

退職した元従業員が再就職活動を行っている同業他社の人事担当者から連絡があり、元従業員の在籍確認、勤怠状況、退職理由、健康状態等を聞かれたため、伝えそうになった。

Point

☑退職した従業者に関する在籍状況や勤務状況等が個人データになっている場合、問合せに答えることは個人データの第三者提供に該当するため、あらかじめ**本人の同意を得ている**場合や第三者提供制限の例外事由に該当する場合を除いて、第三者に提供することはできません。

☑再就職活動先企業の人事担当者が行った問合せ自体、本人の同意なく、過去の勤務先に、元従業員が再就職活動を行っているという個人データを提供することであり、個人情報保護法上問題のある行為と考えられます。

引用元:個人情報保護委員会　https://www.ppc.go.jp/files/pdf/pd_hiyari01.pdf

ヒヤリハット事例④

利用目的_case1

小売店を営んでおり、人手不足のためアルバイトを募集していたが、なかなか人が集まらなかった。

↓

店のポイントプログラムに登録している顧客をアルバイトに勧誘しようと思い、事前にその顧客の同意を得ることなく、登録された電話番号に電話をかけそうになった。

Point

☑個人情報取扱事業者は、個人情報を取り扱うに当たって、利用目的をできる限り特定しなければならず、本人の事前の同意がなければ、利用目的の達成に必要な範囲を超えて、個人情報を取り扱うことはできません。なお、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行うことはできません。

☑事例においては、顧客向けに提供されるサービスのために取得した個人情報を採用活動に利用しようとしており、一般的には、利用目的の達成に必要な範囲を超えていると判断されます。

引用元：個人情報保護委員会　https://www.ppc.go.jp/files/pdf/pd_hiyari01.pdf

ヒヤリハット事例⑤

個人情報の記載された書類を想定してください

電子媒体などの取り扱い_case1

システム上で顧客リストを管理している会社で、ある担当者が資料作りのため、システムからUSBメモリに顧客データをコピーし、作業を行っていた。

作業を終えたので、USBメモリを所定の保管場所に戻そうとしたが、保管場所の鍵を保管している担当者が離席していた。

翌日も続けて作業を行うこととしていたため、自分の机の上に置いて帰宅しそうになった。

Point

☑個人データを取り扱う機器や個人データが記録された電子媒体及び書類等は、盗難又は紛失等を防止するため、施錠できるキャビネット・書庫等に保管するなどして適切な管理を行う必要があります。

☑執務スペースが整理されていないと、電子媒体等の紛失や誤廃棄につながる可能性があります。保管場所はもちろん机の上等の整理整頓を励行しましょう。

引用元：個人情報保護委員会　https://www.ppc.go.jp/files/pdf/pd_hiyari01.pdf

個人情報の取扱いに関する事故の影響（事例）

ベネッセ個人情報流出事件__２０１４年

子供向け通信教育事業を手掛けるベネッセコーポレーションが起こした個人情報漏洩事件。

流出した顧客情報は最大で3504万件に及ぶとされる。

顧客データベース管理の委託を受けていた、情報処理系子会社シンフォームの社員による犯行とされる。

シンフォームはベネッセ個人情報流出事件の影響から、2015年3月末をもって解散。

大規模な個人情報漏洩は
資本金1億円、従業者数500名
規模の会社を解散に追いやる程
のインパクトがある。

スタッフサービスで発生した派遣登録者データの持出による漏洩__２０１７年

登録者からの問い合わせをきっかけに、元社員が登録者の個人データ1万5千件をメールで外部に送信していたことがわかった。流出した個人情報は、姓名のほか、住所・電話番号・メールアドレス・時給額・派遣先企業名などの営業情報などが含まれていた。

元社員は新会社の営業に活用するためにデータを持ち出した。

退職者の悪意による事故。
退職者のアクセス権限はすみやかに削除する。
共有ID、パスワードも迅速に変更をする。

S不動産で発生した顧客への新拠点案内メールでの誤送信__2018年

BCCで設定するべきところを宛先(TO)に記載し送信してしまったため、1875件の顧客のメールアドレスが、受信先で見られる状態で送信された。顧客からの指摘で発覚。

メールの誤送信は発生頻度が最も高い。
送信前にダブルチェックが効果的。

個人情報の取扱いに関する事故の影響（事例）

顧客情報の入ったパソコンの紛失事故により取引先の信用を失墜

（所在地：石川県／業種：建設業／従業員規模：101～300名）

従業員が顧客情報の入ったパソコンを持ち出した時に紛失事故が発生した。顧客に対して紛失の報告をしたが信用を失うこととなった。原因は、会社として情報セキュリティに対する意識が高くなかったため、持ち出しに関する明確なルールや手続きを定めておらず、従業員がパソコンを自由に持ち出せる環境であったことである。その後、情報機器の暗号化などの対策を実施するとともに、パソコンの持ち出しルールを含めた情報セキュリティ規程を整備して従業員へ情報セキュリティ教育を行った。

出典：独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン第3.1版」

ランサムウェア感染　～高額化するランサムウェア被害～

（地域：近畿／業種：製造／従業員規模：20～999名）

利用するデータセンターのサーバー複数台がランサムウェアに感染していることが発覚。

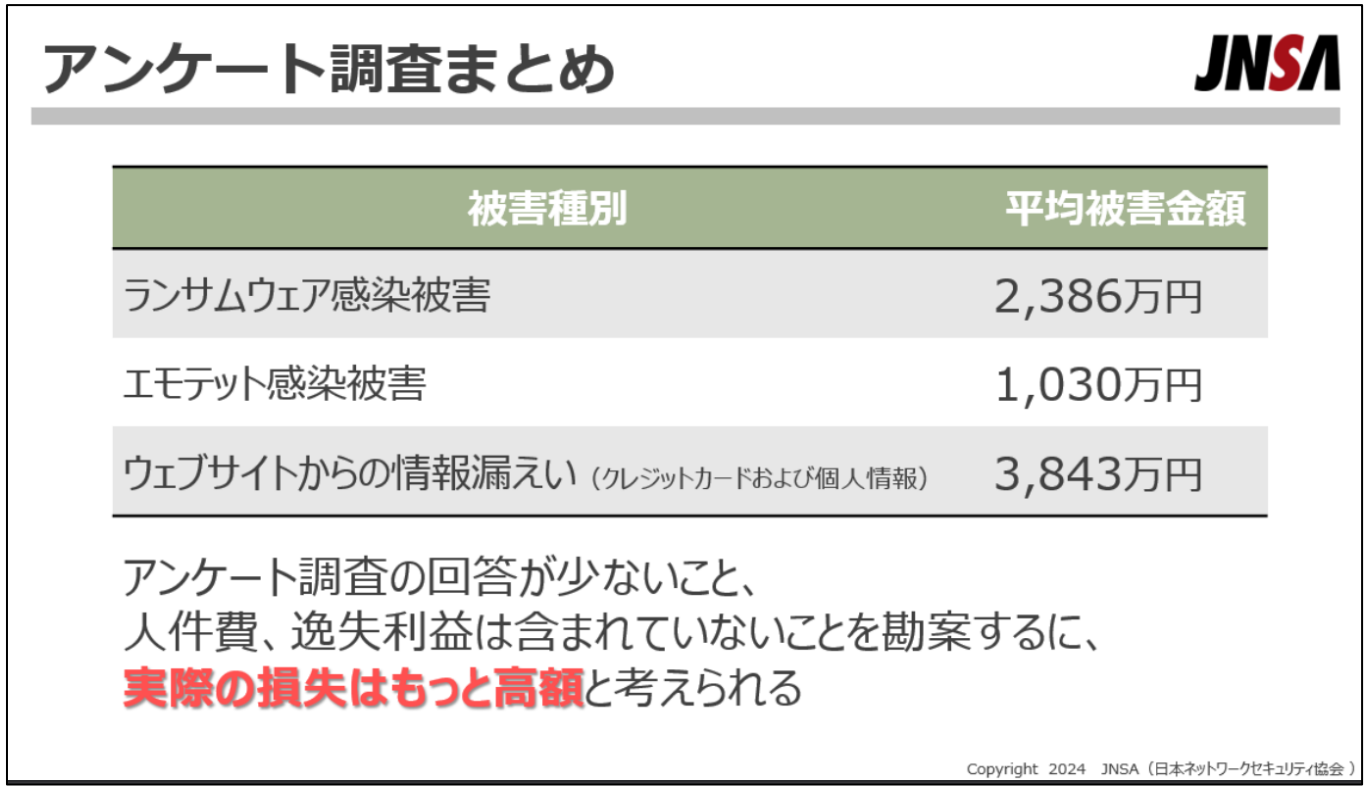
脆弱性のあるVPN機器から侵入であることが判明。

ECサイトの被害懸念はなかったものの、大事をとって一旦停止。被害がないことを後日確認。被害を受けた社内システムの復旧には２か月を要した。また、カード情報の漏えいに時間を要したため、会社全体の業務の正常化には約７か月を要した。

出典：日本ネットワークセキュリティ協会（JNSA）　「インシデント損害額調査レポート 別紙　2025年版」

個人情報の取扱いに関する事故の影響（被害額）

- サイバー攻撃の被害額



アンケート調査まとめ

JNSA

被害種別	平均被害金額
ランサムウェア感染被害	2,386万円
エモテット感染被害	1,030万円
ウェブサイトからの情報漏えい（クレジットカードおよび個人情報）	3,843万円

アンケート調査の回答が少ないこと、
人件費、逸失利益は含まれていないことを勘案するに、
実際の損失はもっと高額と考えられる

Copyright 2024 JNSA（日本ネットワークセキュリティ協会）

出典：日本ネットワークセキュリティ協会（JNSA）「サイバー攻撃を受けるとお金がかかる
～インシデント損害額調査レポートから考えるサイバー攻撃の被害額～」

サイバー攻撃を受けた場合の被害額は被害の規模や状況によって異なります。
不審なメールへの対応ルール、万が一感染してしまった際の対応手順を確認しておくことが重要です。

テンダーラビングケアサービスで発生した事故事例

当社での事故事例① 2016年 メール誤送信

先行予約(次月の予約の先行受付)のご案内(4月分)を、メール配信で希望されているお客様に送付した際、アドレスをBCCではなくCCに入れてしまった。それにより、メールアドレスがお客様相互に見えるように表示された。

発生原因:送付の際、BCCではなくCCにアドレスを入れてしまったため メール文章は汎用的な内容であり、個人の氏名などは含まれていない。　※JIPDECへの事故報告より

ポイント:ダブルチェックと配信専用ツールの導入

リスク:メールアドレス自体が個人情報であり、二次被害(迷惑メールなど)の懸念があります。管理がずさんであるという印象を与え、今後の予約や契約に影響する可能性があります。

対策:配信専用ツールの導入: BCC運用をやめ、1通ずつ自動配信されるシステム(メール配信サービス)へ切り替えるのが最も安全です。→メールワイズ導入

ダブルチェックの徹底: 複数名で「宛先欄がBCCになっているか」を送信直前に必ず目視確認します。

当社での事故事例② 2025年 メール操作ミス

・情報を一斉送信する際、誤って本来添付すべきでない顧客リストをメールに添付してしまい、メール受信した全員が当該リストに記載されている298人の氏名とメールアドレスが流出。メールを受け取った方からの指摘(返信メール)で発覚。
・個別に電話やメールでの問い合わせが9名、個人情報削除および再発防止策の提示要望あり。

※JIPDECへの事故報告より

ポイント:操作ミスと確認不足。作業者が本来添付すべきではない箇所にファイルを添付してしまった。メールワイズを使用。

リスク:メールアドレス自体が個人情報であり、二次被害(迷惑メールなど)の懸念があります。管理がずさんであるという印象を与え、今後の予約や契約に影響する可能性があります。

対策:運用マニュアルの整備。不慣れな作業者でもミスなく安定した操作ができるようにする。宛先、内容のダブルチェックの徹底なども運用に組み込む。

当社での事故事例③ 2021年 FAX誤送信

某区A保育園より、営業担当者に派遣スタッフの細菌検査結果をFAX送信するように依頼を受け送信。町田予防から、某区保育課よりFAXの件で問い合わせが入ったことを知り、確認したところ某区保育課に誤送信したことが判明。　※JIPDECへの事故報告より

ポイント：細菌検査結果という極めてデリケートな個人情報の漏洩である。自社で気づけず、外部（検査機関や行政）からの指摘で発覚した。

リスク：派遣先（園）や行政、スタッフ本人からの信用を失う。適切な管理を怠ったとして、会社としての責任を問われる。派遣契約の解除や、今後の新規取引への悪影響。

対策：FAX短縮ダイヤル登録の徹底、送信直前に「番号」と「宛先名」を必ず声出し確認する。
手法の変更: 誤送信のリスクが高いFAXから、パスワード付きメール等への切り替えを検討する。

当社での事故事例④ 2024年 誤送付

在職証明送付の送り状住所を同姓の方と誤って作成し、そのまま発送をしてしまった。
誤送付先から在職証明書は回収済み。双方に謝罪済みで、申し立て事項なし。

※社内事故報告より

ポイント：情報の性質: 氏名・住所・勤務実績を含む重要個人情報の漏洩。発生原因: 同姓の別人との取り違えによる、作成・封入時の確認不足。

リスク：プライバシー侵害: 意図しない第三者への個人情報（給与や在職状況）の露出。
信用の失墜: 従業員や取引先からの事務管理能力に対する疑念。
二次被害: 回収前のコピーや情報の書き留めによる、潜在的な拡散リスク。

対策：ダブルチェックの徹底: 作成者以外の第三者が「封入物」と「送り状・封筒」を照合する。
照合項目の複数化: 苗字だけでなく、フルネーム・住所・生年月日等の複数箇所で本人確認を行う。
指差し呼称: 封入直前に「中身の氏名」と「封筒の宛名」が一致しているか声出し確認する。

個人情報保護に関する理解度テストの受検を
お願いいたします。

QRコードもしくはURLより受検してください。

https://forms.gle/W6SVD2zv8ZoiWSiaA