個人情報保護マネジメントシステム社内教育テキスト

個人情報管理の重要性

SOHRIN UNITED WORKS

株式会社エスユーワークス

目次

1. 個人情報の管理はなぜ必要？

はじめに

はじめに

- 個人情報を保護・管理する目的

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

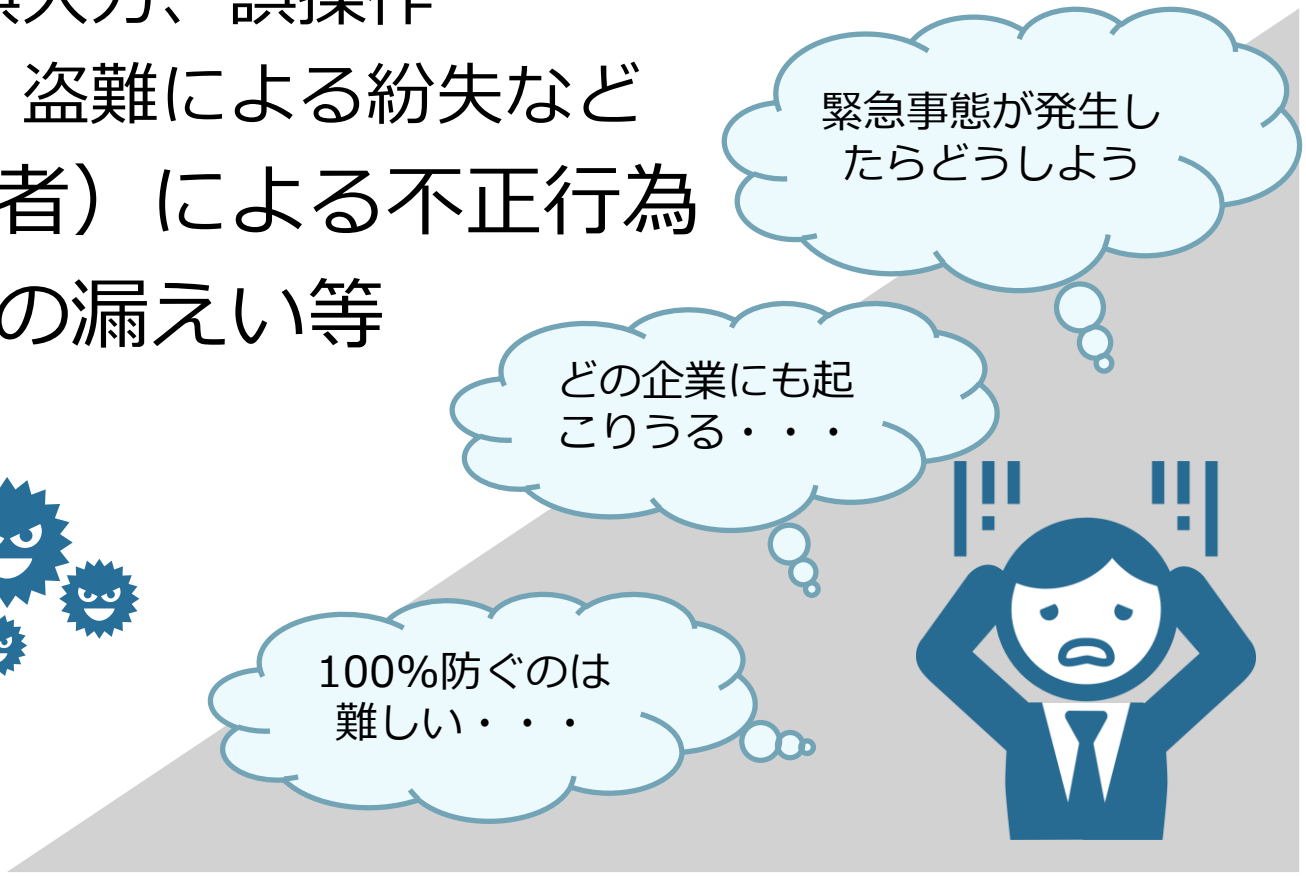
したがって・・・

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



- 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
    2020年度「個人情報の取扱いにおける事故報告集計結果」より

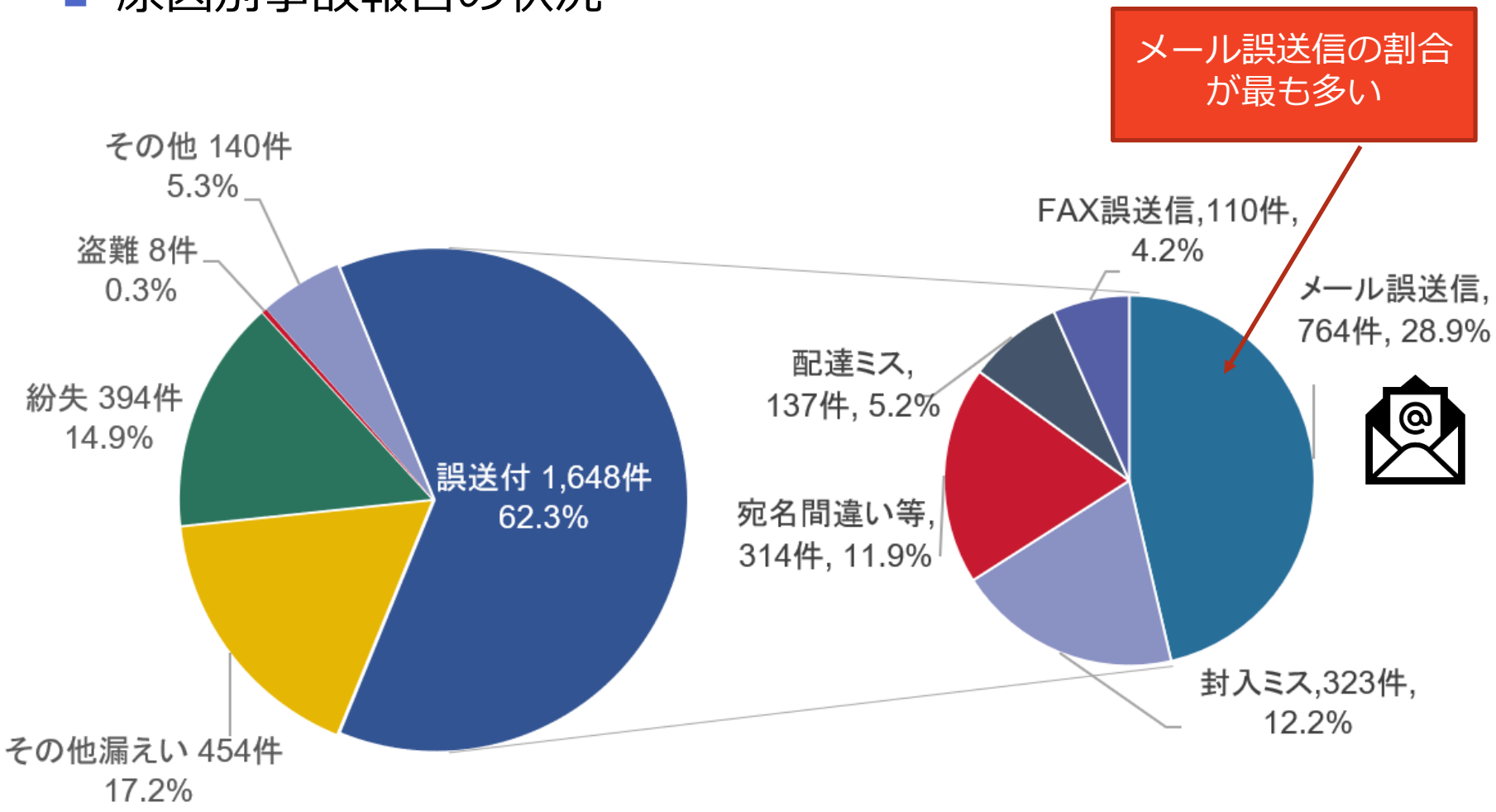
2020年度の事故報告概要

- 発生件数別の傾向
  - 「誤送付」（1,648件：62.3%）が最も多く、次に「その他漏えい」（454件：17.2%）の順。
  - 「誤送付」のうち、「メール誤送信」（764件：28.9%）が最も多く、昨年度より大きく増加。
  - 「その他漏えい」のうち、「関係者事務処理・作業ミス等」（232件）が過去5か年で最も多い。

- 2020年度の報告傾向
  - 新型コロナウイルス感染症対策を含め、「テレワーク実施」や「新たなコミュニケーションツールの利用」などの業務環境の変化による影響が見られる。

発生件数別の傾向（１）

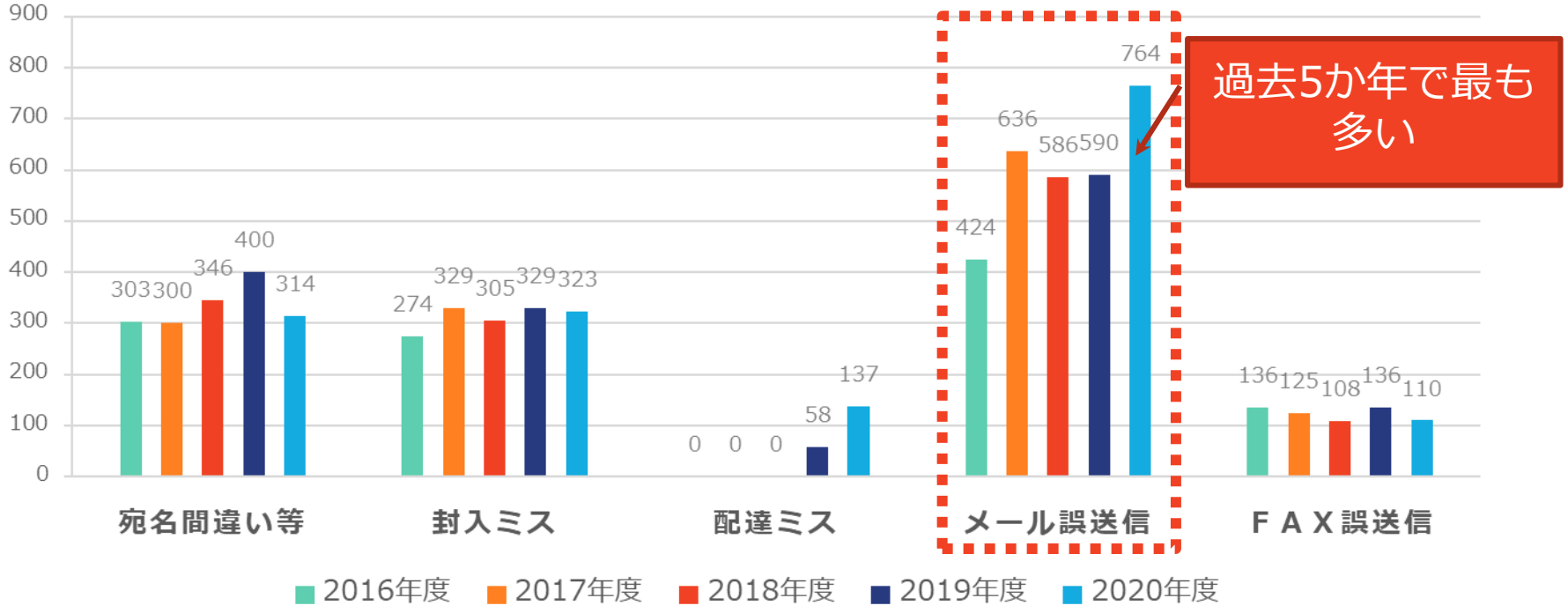
- 原因別事故報告の状況



出典：（2020年度）「個人情報の取扱いにおける事故報告集計結果」

発生件数別の傾向（２）

- 「誤送付」の内訳推移

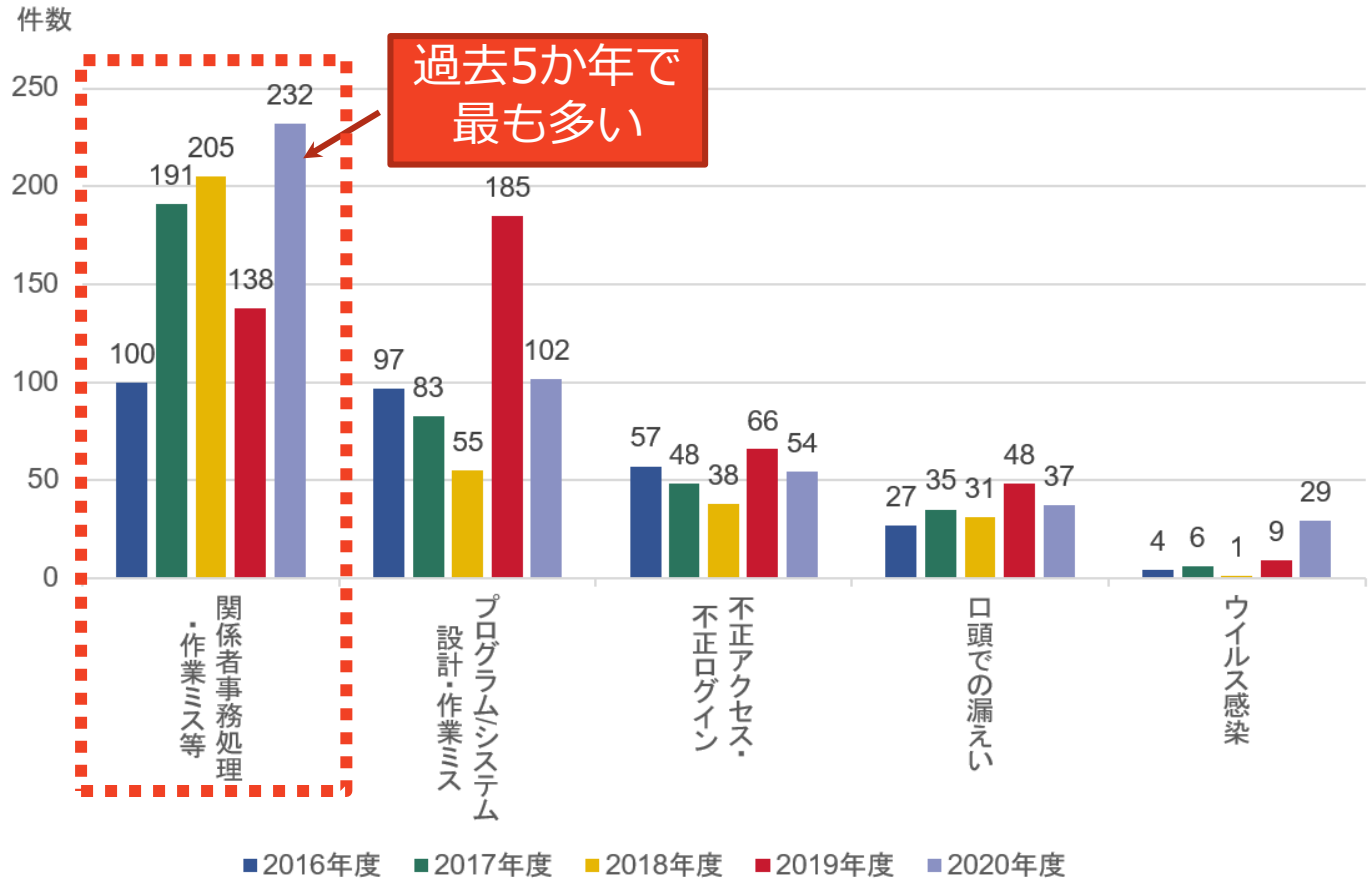


テレワークの実施、メッセージングサービスなど新たなコミュニケーションツールの利用などにより、メール誤送信は増加。
業務環境や手順が変化したときには、注意が必要。

出典：（2020年度）「個人情報の取扱いにおける事故報告集計結果」

発生件数別の傾向（３）

- 原因別事故報告件数のうち「その他漏えい」の内訳（件数）



新型コロナウイルス感染症対策などで、いつもと異なる業務環境や手順による作業ミスや事故が発生。

出典：（2020年度）「個人情報の取扱いにおける事故報告集計結果」

事故の発生傾向

- 継続して発生している事例がある一方、
  「業種・業態」「IT環境」「働き方」などの進化・変化に伴い、「発生事象」「事故の原因」にも変化が見られる。

- 特に注意したい事故事例
  1. ソーシャルエンジニアリング
  2. 設定ミスによる誤公開
  3. ランサムウェア
  4. 環境変化による事故
     （テレワーク、出社制限など）

特に注意したい事故事例（１）

1. ソーシャルエンジニアリング

情報通信技術を使用せず、人間の心理的な隙や行動のミスを利用して、個人情報等の情報を盗み出す事象。

◆ 事例

支払い督促の電話をした際に、電話を受けた債務者の家族を

債務者本人と誤認し、ローン商品名や金額を伝えてしまった。

本人確認手続きのルールや手順を遵守しましょう。
本人への影響について十分理解したうえで、自己判断で提供することがないようにしましょう。

特に注意したい事故事例（２）

2. 設定ミスによる誤公開

◆事例

インターネット上の無償で使用できるサービスを利用してセミナー参加申込Webサイトを運用していたが、作業者のシステム設定ミスにより、申込者が他の申込者の個人情報を閲覧できる状態となっていた。

個人情報の取扱い・セキュリティ設定の確認は十分ですか？
新たなサービスの選定においては、必要な要件や機能を満たしているか、自社の選定基準・手順を確認して検討する必要があります。

特に注意したい事故事例（３）

3. ランサムウェア

攻撃者が身代金の獲得を目的に開発されたマルウェアのこと。感染したパソコンになんらかの制限をかけ、その制限の解除と引き換えに金銭を支払うよう要求。

感染経路は、メールとWebサイトが主体です。

- 不審な添付ファイルの開封、URLのクリックをしない
- OSやブラウザは最新状態に保ち、アンチウイルス等のセキュリティ対策ソフトを導入

常に攻撃手法を変更するなど進化続けているため、定期的な脆弱性情報の収集を行い、対策を行っていくことが重要です。

特に注意したい事故事例（４）

4. 環境変化による事故

通常と異なる状況・環境		可能性として考えられるリスク要因
テレワーク	セキュリティ環境	• 職場と比べてセキュリティ対策が不十分
	確認体制・環境	• ルールで定められたチェックを行えない
	持出資料管理	• 保管場所の確保,セキュリティ対策が不十分
	その他	• 緊張感の維持困難（気のゆるみ）
出勤制限	対応人数の不足	• 一人当たりの業務量増加 • ダブルチェック省略
	担当者以外の対応	• 該当の業務に不慣れ
	イレギュラーな業務フロー	• 本来とは異なる暫定フロー
新規ツール導入	機能や設定に関する理解	• 理解不十分なまま、使い始めた場合 • 初期設定未確認の場合
追加業務	イレギュラーオペレーションの要因に対する追加業務の発生	• 緊急事態への対応として、（通常業務に）新たな業務が追加された場合
その他	業務上のコミュニケーションの取り方の変化	• 相談したいタイミングで連絡がとれない • コミュニケーションツールが使いこなせない

特に注意したい事故事例（４）つづき

■ イレギュラーオペレーションによる事故発生防止策例

セキュリティ確保	• 業務利用PCのセキュリティ対策の確認・徹底
ミスの未然防止	• 各業務における「間違う可能性のある場面とチェックポイント」の洗出し ➢イレギュラー処理の場合こそ、チェックが重要 ・ダブルチェック、クロスチェック（※） ➢セルフチェックをせざるを得ない時のコツ ・指差し確認、声出し確認
物品・書類の管理	• クリーンデスクの徹底（職場、自宅ともに） • テレワーク時の使用機器・書類等の保管場所設定
便利な機能を正しく活用する	• 新規ツール（機器、システム等）導入時には操作や初期設定の確認を必ず行う
コミュニケーション確保	• 意識的にコミュニケーションをとる
安全確保のための柔軟性	• ルール・手順は状況と目的に合わせて、見直す • ルール・手順通りにできないからしない、のではなく、できることをする

思いもよらない状況になっても慌てないよう、日々の業務において「事故防止の意識」「ルールを確認・遵守」を徹底しましょう。

- 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（事例）

事例１：ウイルス感染で数日間業務が停止し、数千万円の被害が発生

（所在地：東京都／業種：情報通信業／従業員規模：101 ～ 300 名）
社内のパソコンやサーバーがウイルスに感染し、数日間に亘った業務停止に至る障害が発生した。復旧のために徹夜で対応したが、その間の会社としての被害額は推計で数千万円に上る。
原因は、被害が発生するまで、セキュリティ対策ソフトを全く導入していなかったことである。
その後、ウイルス対策ソフトや技術的な対策の導入、情報セキュリティ規則の制定、プライバシーマークやISMS 認証取得に取り組み、再発防止に努めている。

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版」

事例２：テレワーク端末の踏み台化

2020年5月、リモートアクセスを利用した個人所有端末から正規のアカウントとパスワードが盗まれ、オフィスネットワークに不正アクセスされた案件が発生。仮想デスクトップ（VDI）によるリモートアクセスシステムを利用していたものの、個人所有端末自体が攻撃者の踏み台として乗っ取られていたために、VDIサーバ経由で自組織内のファイルサーバを閲覧されたおそれがあり、180社以上の顧客に影響が出るおそれがあると発表。

出典：総務省「テレワークセキュリティガイドライン（第5版）」

個人情報漏えいインシデント：一人当たり平均損害賠償額　**2万8,308円**
（3か年平均）

出典：NPO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　2021年版」

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・・・？

- 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

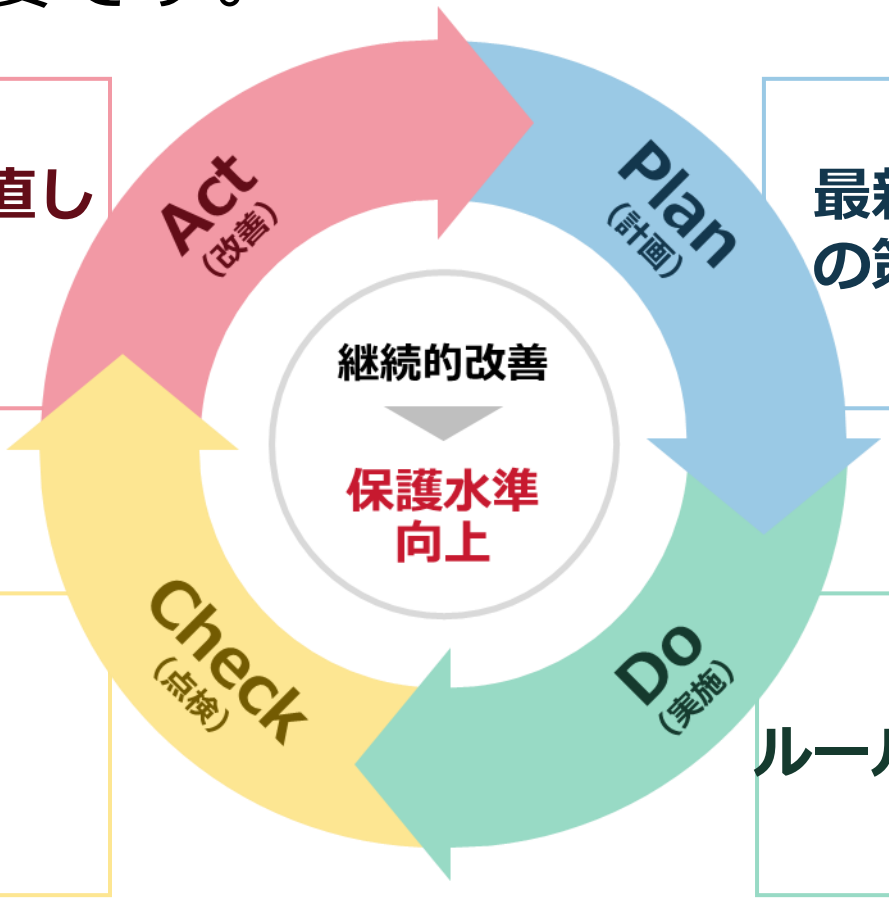
早期発見、緊急時対応のルール化や対策の実施

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

当社は、最適なICT環境を提供するソリューション事業を通じて社会に貢献することを使命とし、サービス品質の向上、お客様満足度の向上に向け努力しております。また、コンプライアンス重視、法令遵守は当然のこと、当社が個人情報を保護する事は、欠かすことの出来ない社会的責務であると考えております。そのため、全従業者に個人情報保護の重要性を認識させ、当社が定める個人情報保護目的の達成に全社一丸となって取り組みます。当社は個人情報保護の理念として、個人情報保護によって個人の権利利益の保護に取り組みます。

１．個人情報の取得・利用・提供

当社は取得する個人情報の利用目的を特定し、その利用目的を達成するために必要な範囲でのみ個人情報を取得します。当社は、個人情報を直接ご本人様から取得する場合、その利用目的や取り扱いについて、文書あるいはそれに代わる方法でご同意いただいております。（お客様のみならず、従業員、取引先様も含めて、当社が事業の用に供する全ての個人情報を対象とします。）

また、利用目的の達成に必要な範囲を超えた取り扱い（以下「目的外利用」）及び、本人の承諾を得ずに第三者に開示・提供することはいたしません。これらのことを防止する措置を、当社の個人情報保護マネジメントシステムによって確実に実施します。

2.　法令、国が定める指針その他の規範の遵守

当社は、個人情報に関する法令、国が定める指針その他規範を遵守いたします。

3.　個人情報の漏えい、滅失又はき損の防止及び是正について

当社は、個人情報の漏えい、滅失又はき損の防止及び是正に関して、必要かつ適切な安全対策を実施いたします。

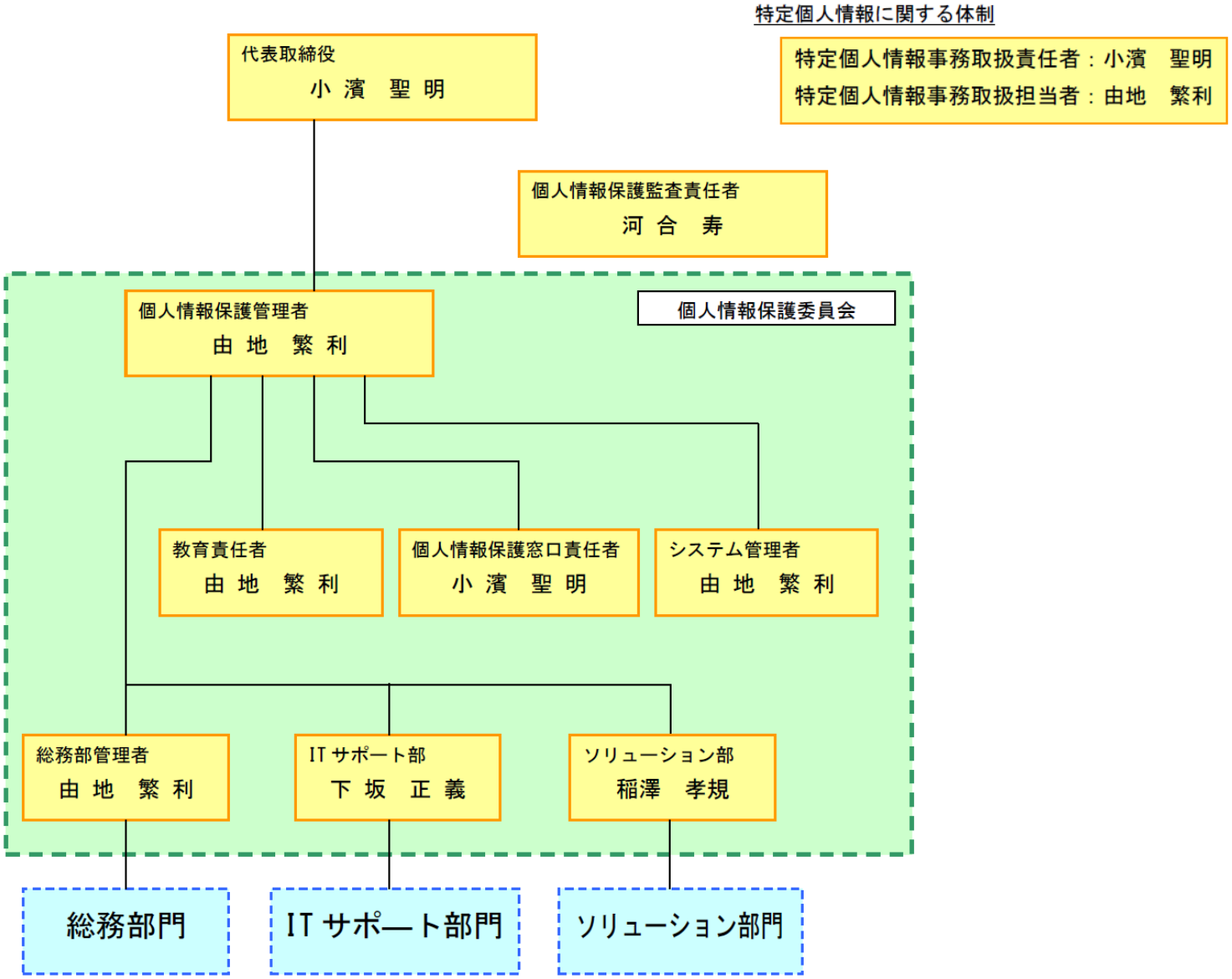
4.　個人情報に関する苦情および相談について

個人情報の取扱いに関する苦情及び相談については、迅速かつ適切に対応いたします。下記の個人情報に関するお問い合わせ窓口にご連絡下さい。

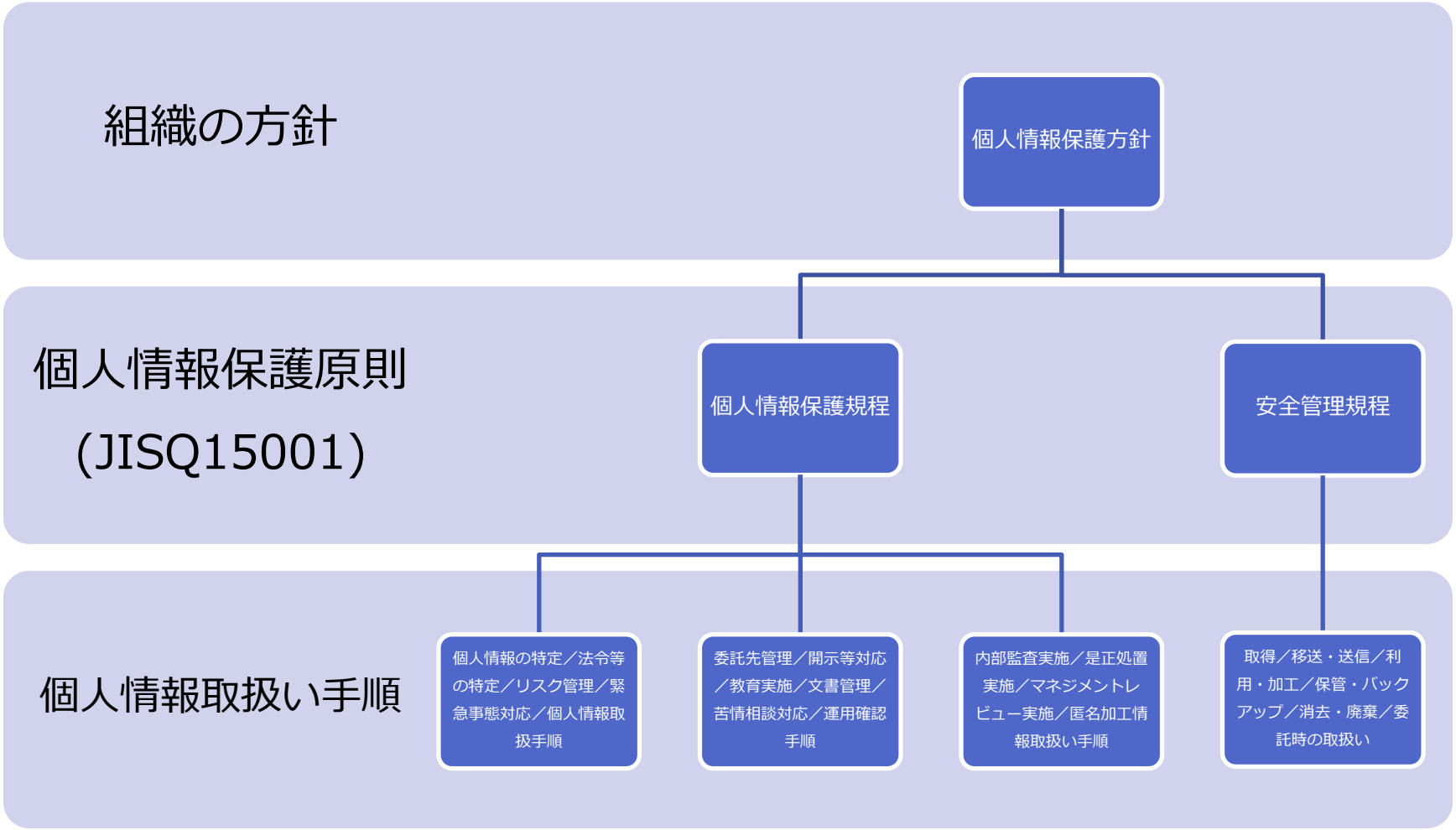
5.　個人情報保護マネジメントシステムの継続的改善

当社は、個人情報の保護と、適切な取り扱いについて、行動規範、内部規程、ルールを定めた、個人情報保護マネジメントシステムを構築し、運用します。また、定期的に実施する運用の点検、内部監査、マネジメントレビュー等により、個人情報保護マネジメントシステムを継続的に改善いたします。

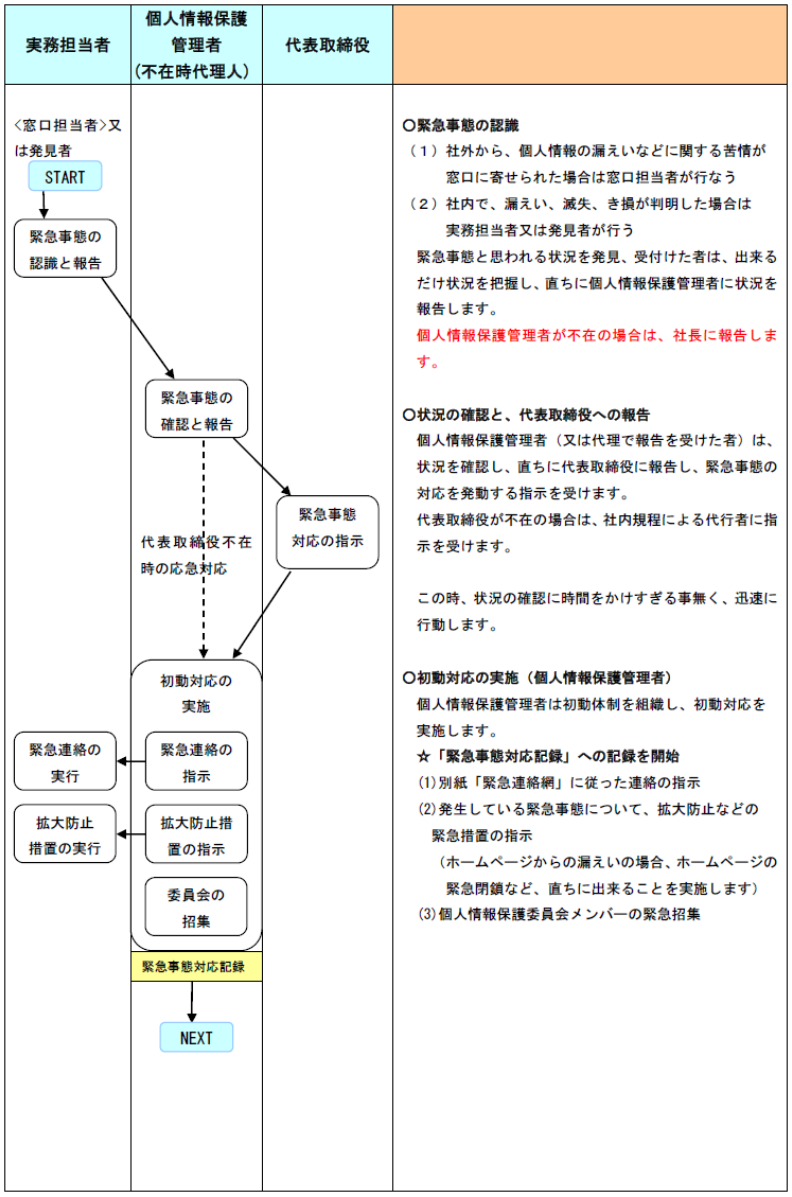
個人情報保護の体制

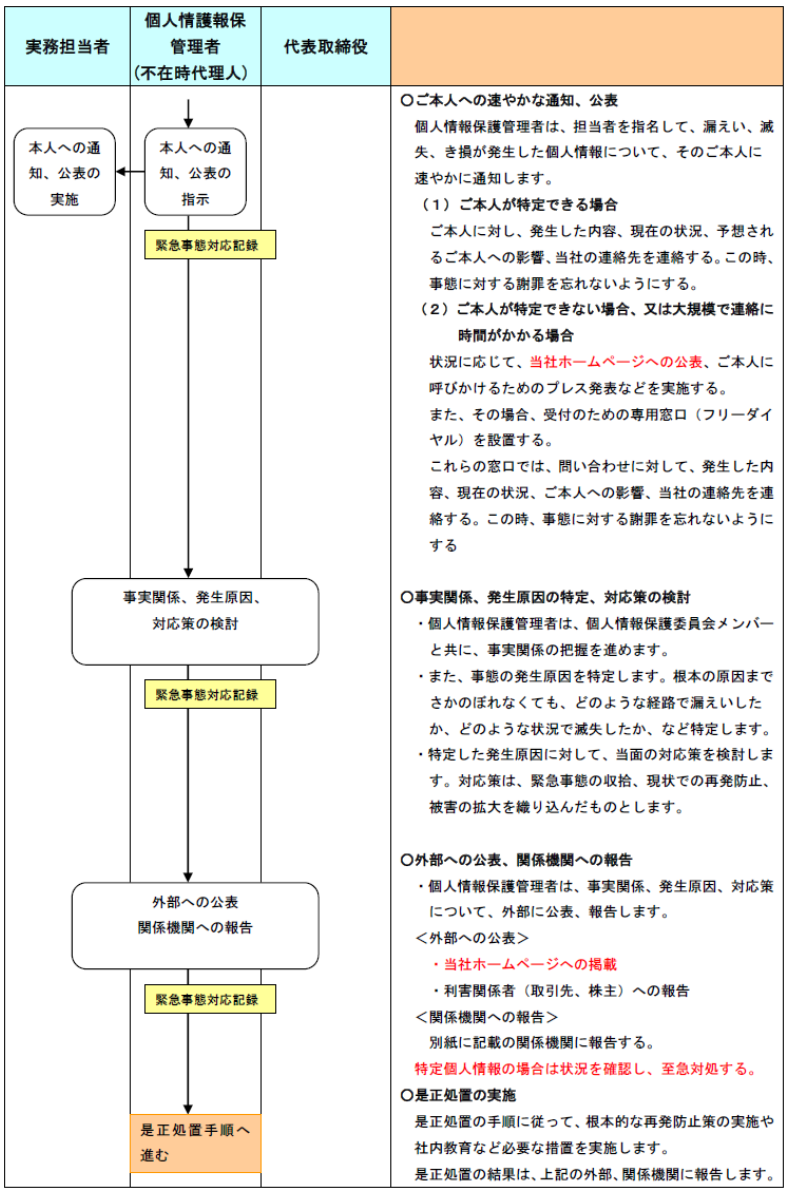

特定個人情報に関する体制
特定個人情報事務取扱責任者：小濱　聖明
特定個人情報事務取扱担当者：由地　繁利
代表取締役
小 濱　聖 明
個人情報保護監査責任者
河 合　寿
個人情報保護委員会
個人情報保護管理者
由 地　繁 利
教育責任者
由 地　繁 利
個人情報保護窓口責任者
小 濱　聖 明
システム管理者
由 地　繁 利
総務部管理者
由 地　繁 利
IT サポート部
下 坂　正 義
ソリューション部
稲澤　孝規
総務部門
IT サポート部門
ソリューション部門

個人情報保護に関する規程の体系



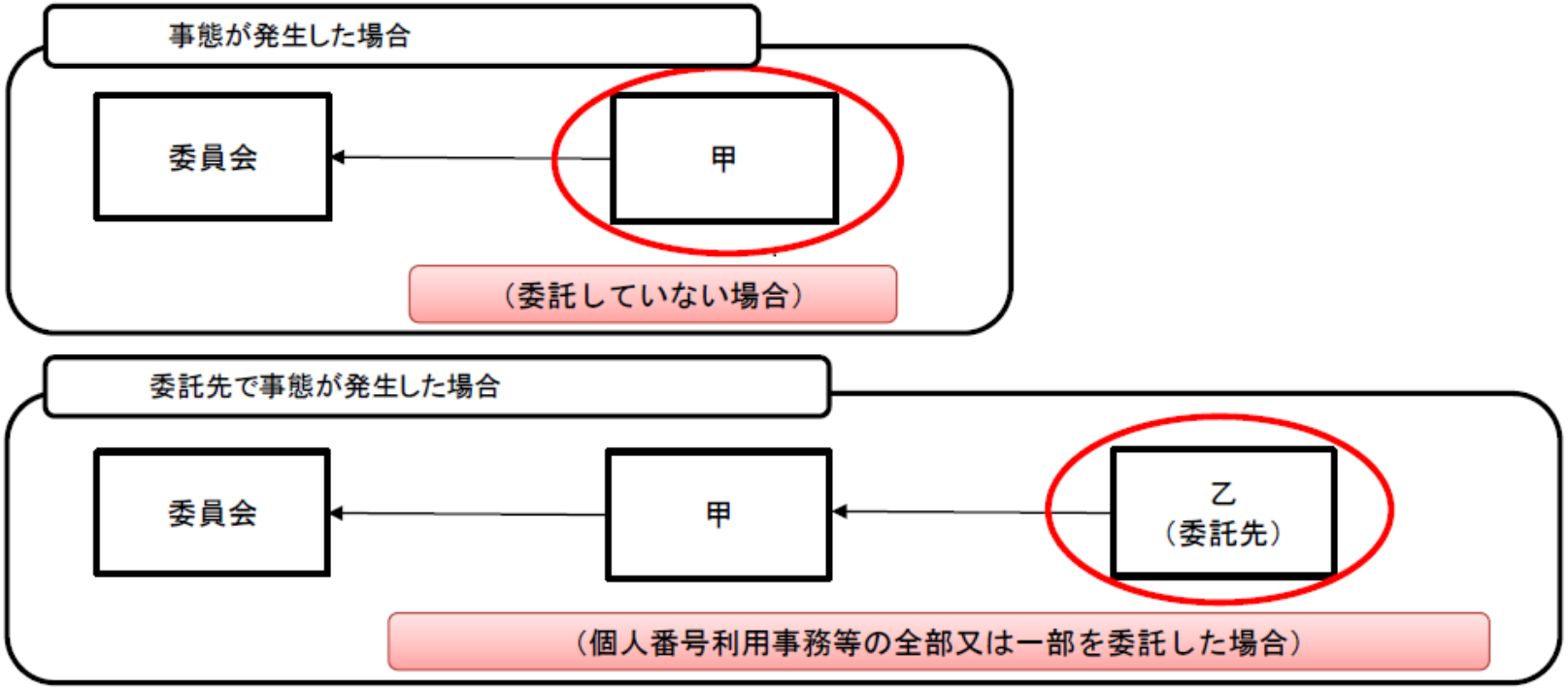
緊急事態への対応フロー





緊急事態への対応フロー (特定個人情報の事故の場合)

特定個人情報とはマイナンバーをその内容に含む個人情報をさします。



個人情報、特定個人情報に関する事故の場合は、以下の個人情報保護委員会にも通知すること。
参照先： https://www.ppc.go.jp/personalinfo/legal/leakAction/

重大事態又はそのおそれのある事案が発覚した場合には、個人情報保護委員会WEBサイトの「漏えい等の報告」ページの報告フォームから報告すること。

＜個人 情報 の事故報告＞ https://www.ppc.go.jp/legal/rouei/

＜マイナンバーを含む事故報告＞ https://roueihoukoku.ppc.go.jp/incident/?top=r2.mynumber

3．まとめ

まとめ

個人情報は会社のものではなく、
ご本人の財産であることを忘れずに、
「ご本人からお預かりしたもの」は大切に、
そして適切に取り扱うことを徹底しましょう。

当社のPMSに関して、わからないことがあれば、
個人情報保護委員会メンバーに確認して下さい。

（参考）プライバシーマーク制度における事故とは

- 「プライバシーマーク付与に関する規約」（PMK500）第5章第11条
  - “個人情報の外部への漏えいその他本人の権利利益の侵害（以下「事故等」という）”
- 「プライバシーマーク制度における欠格事項及び判断基準」（PMK510）
  - 『4.個人情報の取扱いに関する事故についての判断基準』で示す以下の事象

①漏えい	②紛失	③滅失・き損
④改ざん、正確性の未確保	⑤不正・不適正取得	⑥目的外利用・提供
⑦不正利用	⑧開示等の求め等の拒否	⑨上記①～⑧のおそれ

参考情報

- プライバシーマーク制度サイト(https://privacymark.jp/)
  - プライバシーマーク制度　運営要領
    https://privacymark.jp/system/guideline/procedure.html
  - 参考情報＞個人情報の取扱いにおける事故報告集計結果
    https://privacymark.jp/system/reference/index.html
  - 制度案内＞個人情報の取扱いに関する事故の報告について
    https://privacymark.jp/system/accident/index.html

- プライバシーマーク付与事業者専用サイト
  - https://member.privacymark.jp/

    個人情報の取扱いに関する事故を発生させないために