



個人情報管理の重要性

2022年7月15日

JIPDEC

一般財団法人日本情報経済社会推進協会
プライバシーマーク推進センター



目次

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

個人情報を利用して自社
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

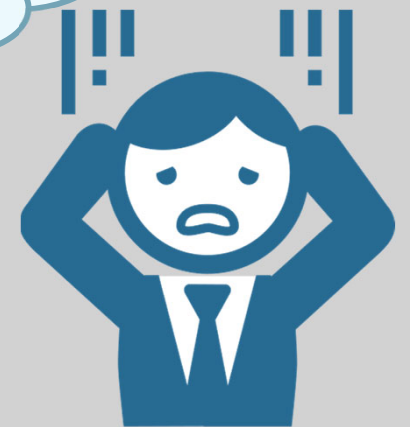
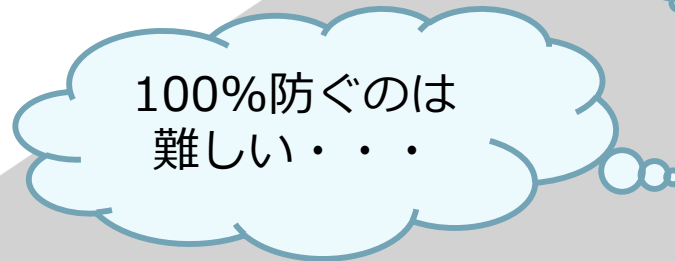
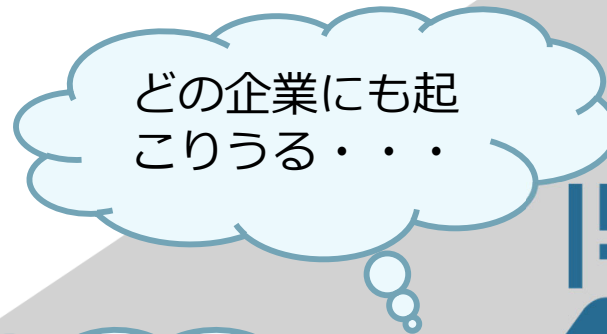
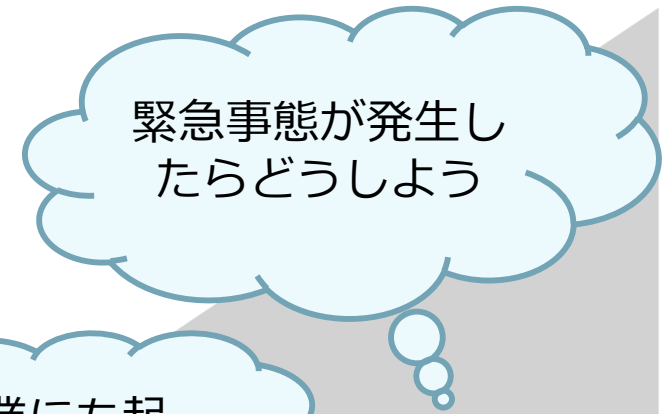
したがって・・・

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

■ 発生件数別の傾向

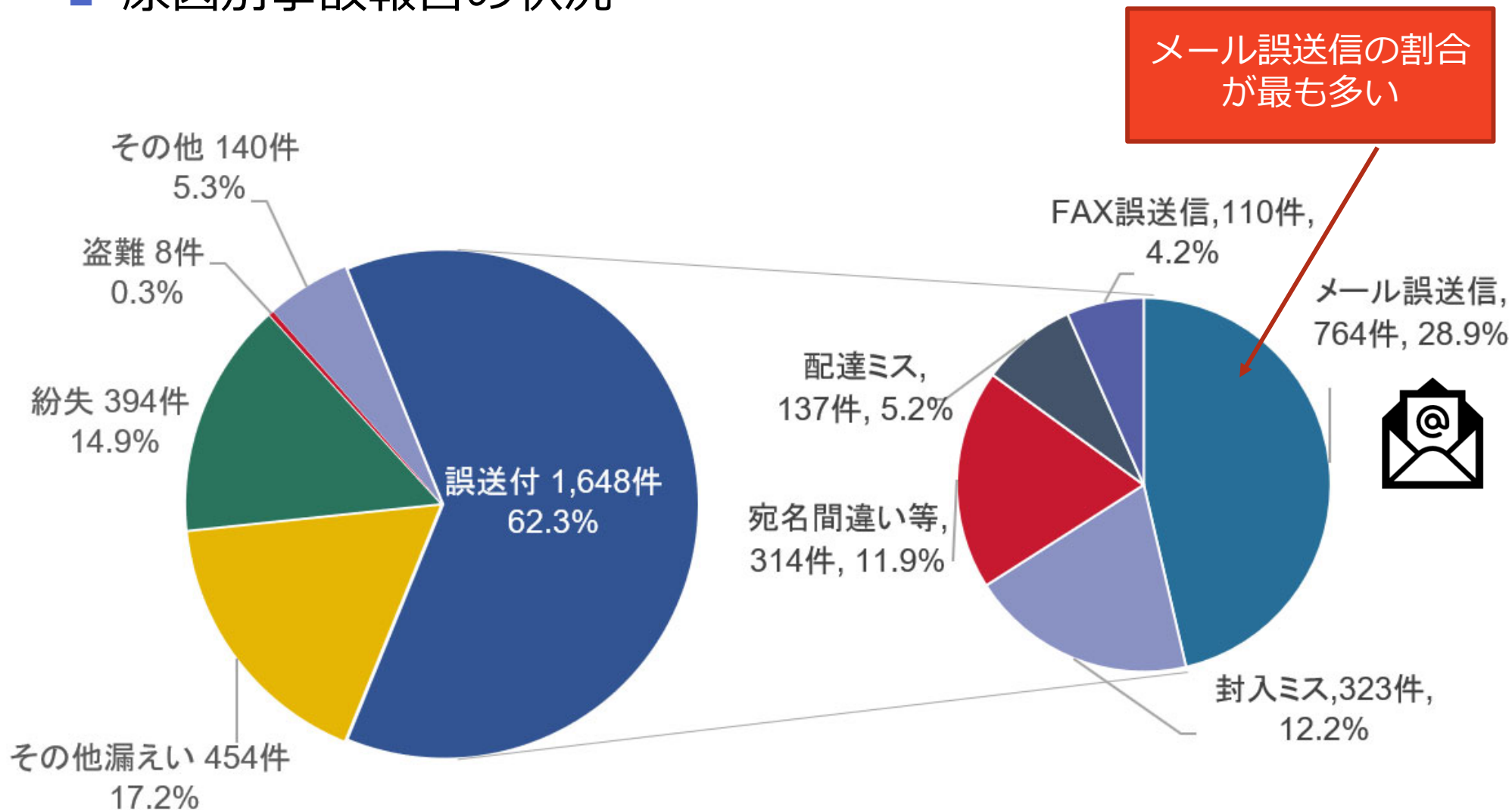
- 「誤送付」 (1,648件 : 62.3%) が最も多く、次に「その他漏えい」 (454件 : 17.2%) の順。
- 「誤送付」のうち、「メール誤送信」 (764件 : 28.9%) が最も多く、昨年度より大きく増加。
- 「その他漏えい」のうち、「関係者事務処理・作業ミス等」 (232件) が過去5か年で最も多い。

■ 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）

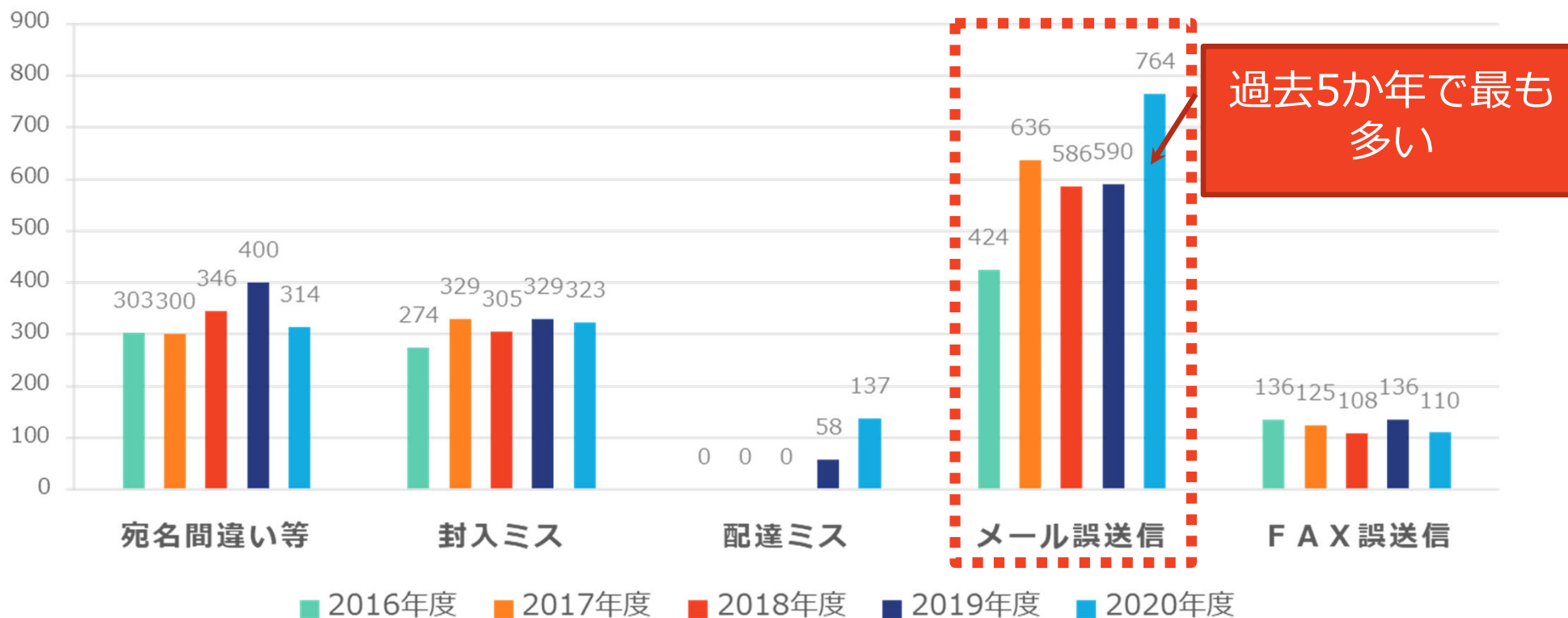
■ 原因別事故報告の状況



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



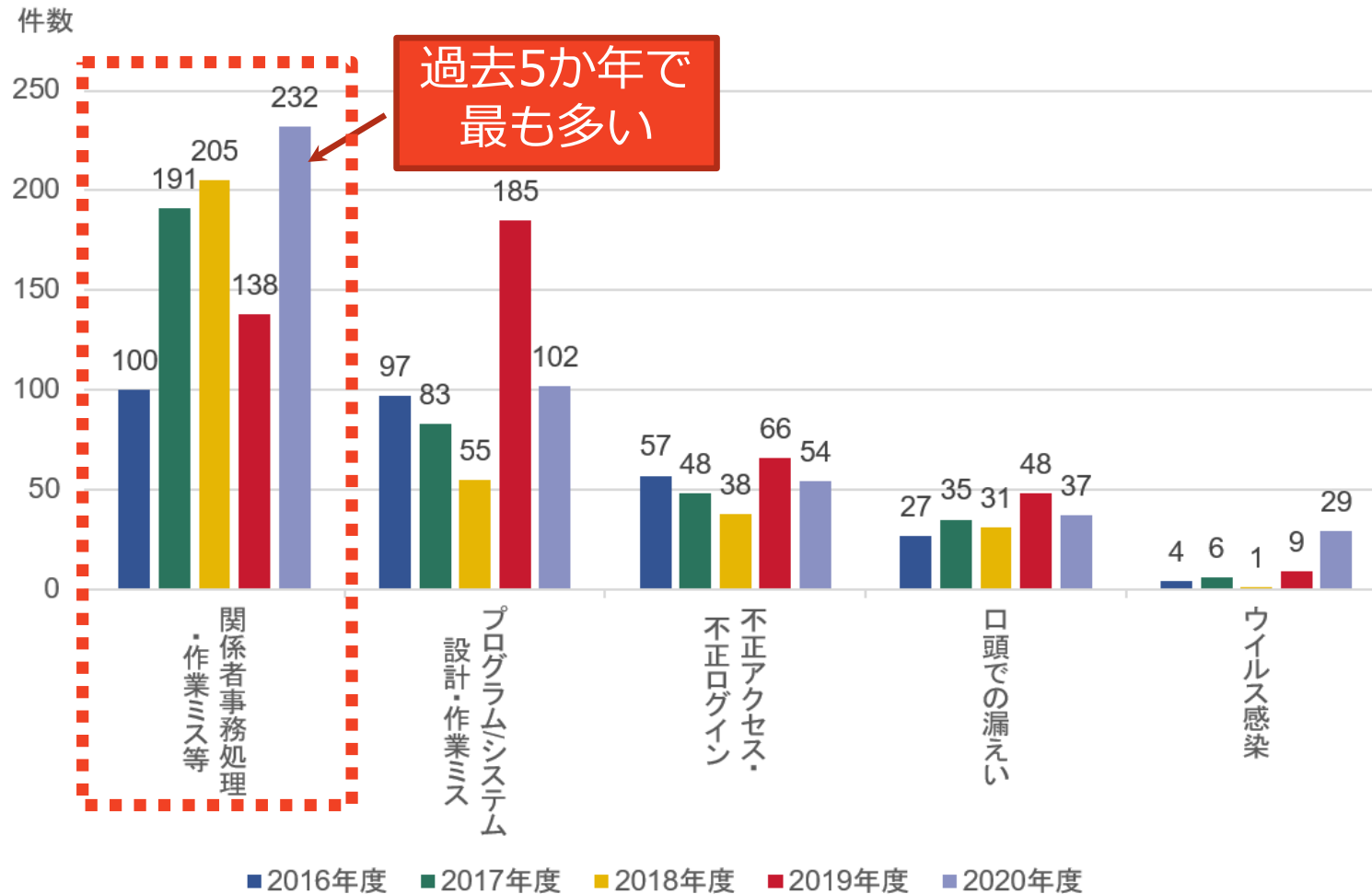
過去5か年で最も多い

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。

- 特に注意したい事件事例
 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見ることができるようになっていた。



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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">各業務における「間違ふ可能性のある場面とチェックポイント」の洗出し<ul style="list-style-type: none">▶イレギュラー処理の場合こそ、チェックが重要<ul style="list-style-type: none">・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<ul style="list-style-type: none">・指差し確認、声出し確認
物品・書類の管理	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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。

■ 個人情報取扱いに関する事故の影響



個人情報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・・・。



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

従業員は

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

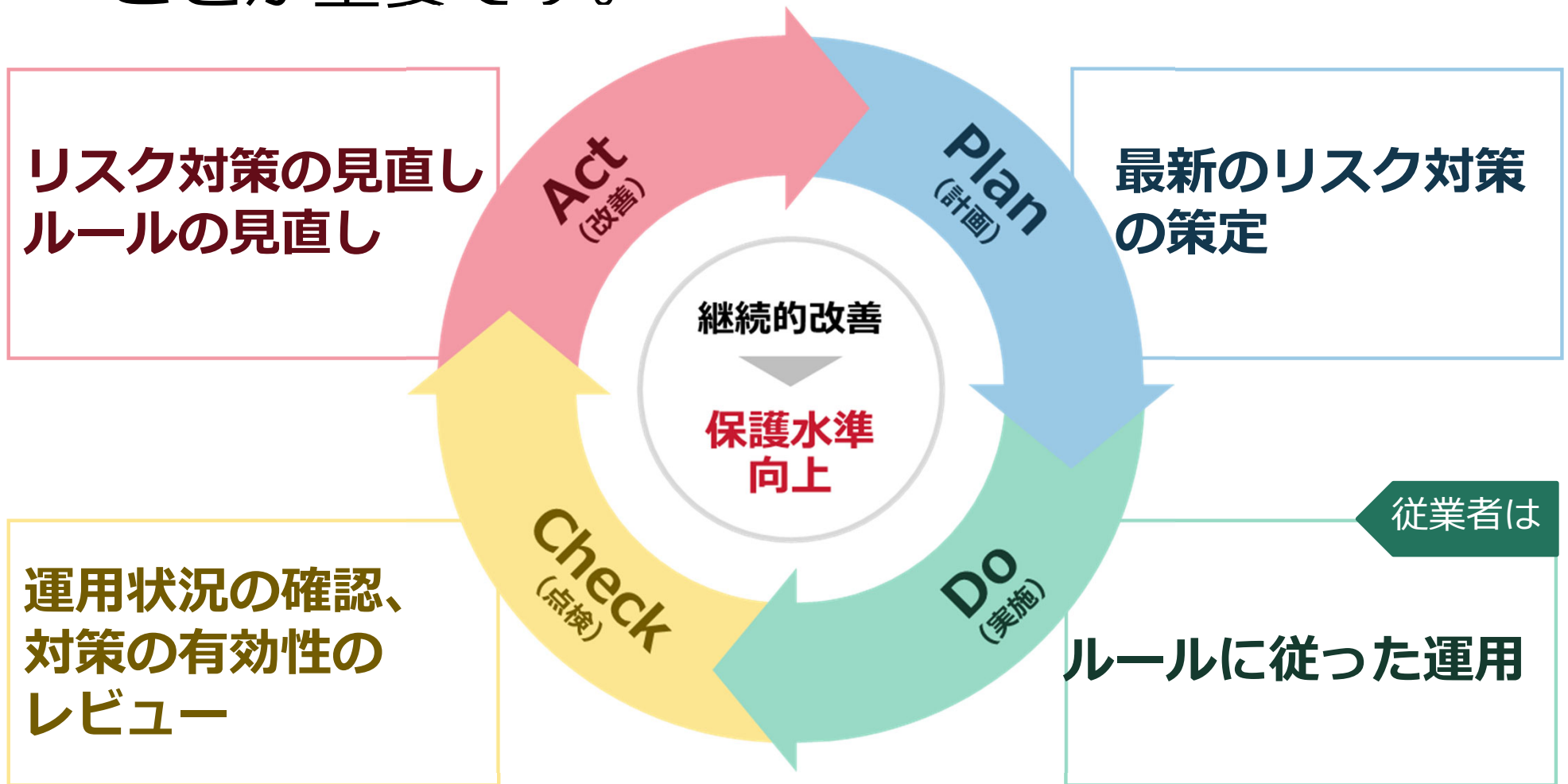
従業員は

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。



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



まとめ

(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)
 - “個人情報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）”

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>

