個人情報管理の重要性

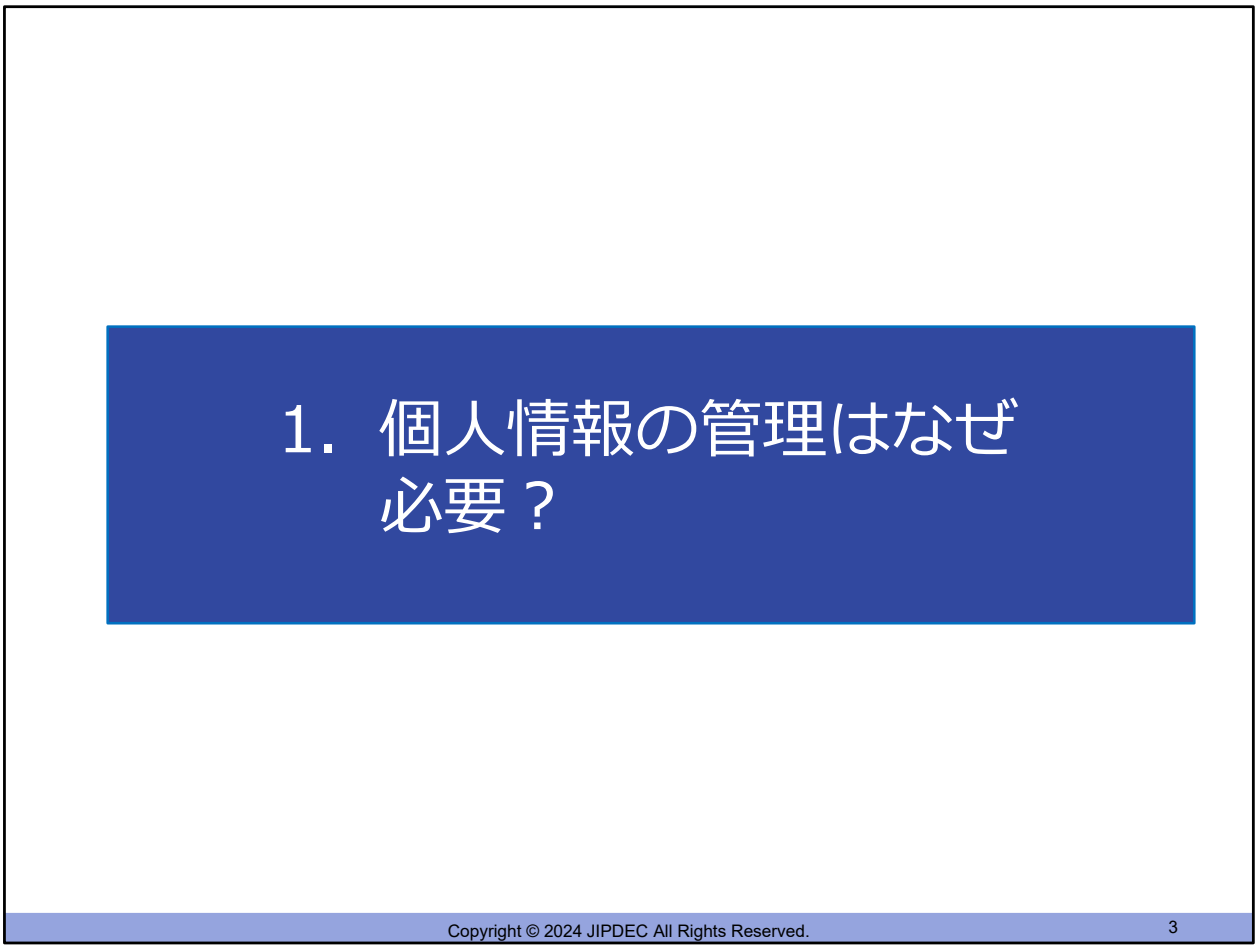
2024年11月12日

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

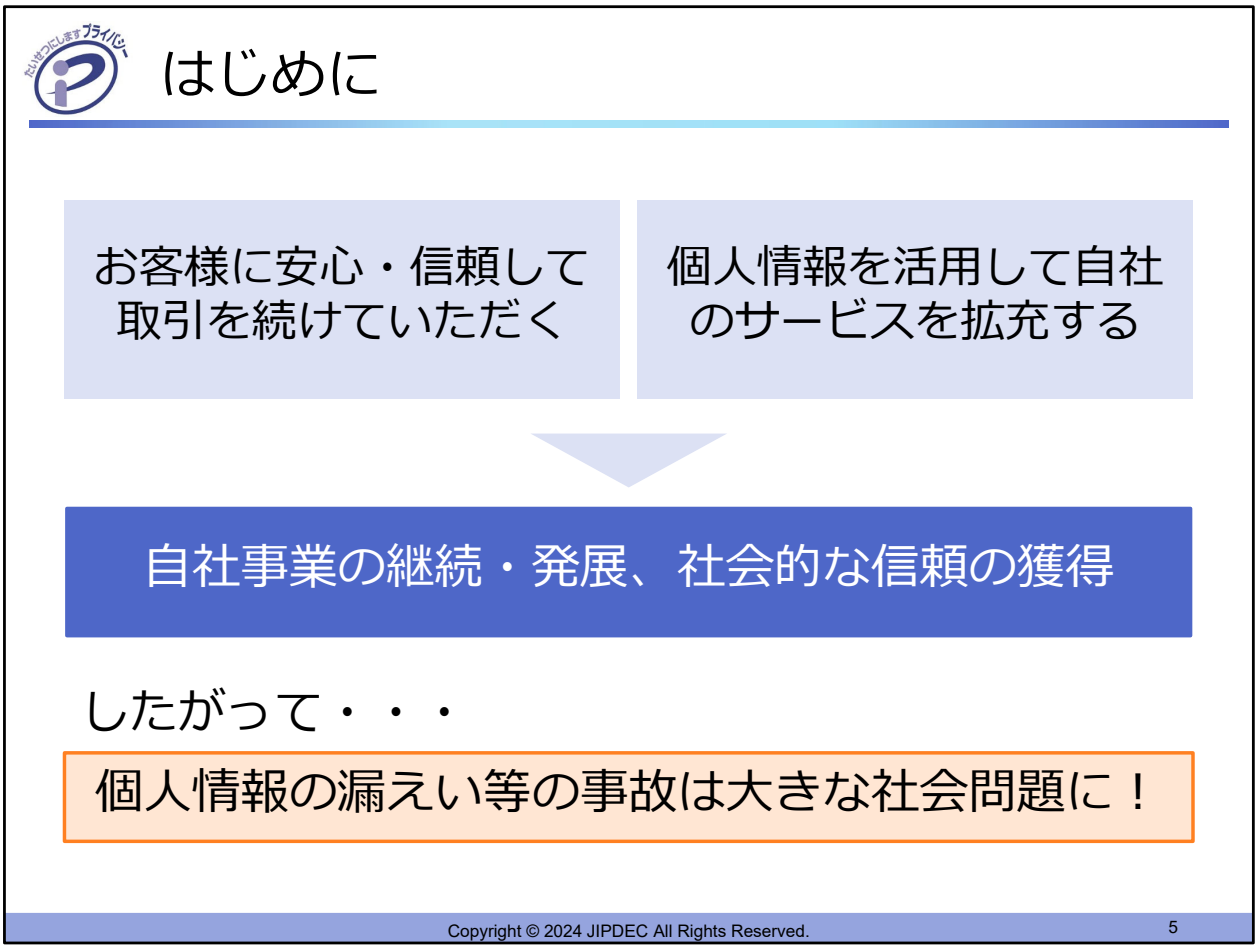
Copyright © 2024 JIPDEC All Rights Reserved.



●第１部の内容は、事業者・従業者として理解しておきたい、個人情報管理の重要性についての説明です。

はじめに

Copyright © 2024 JIPDEC All Rights Reserved.



●事業において、なぜ、個人情報の保護・管理が必要なのかを考えます。

個人情報を保護・管理する目的は、主に以下の2点。

・お客様（消費者・取引先）からお預かりした個人情報を適切に取り扱い、お客様の権利利益を守る

・お預かりした個人情報を利用目的の範囲内で有効に活用して、サービスの拡充など事業展開にいかす

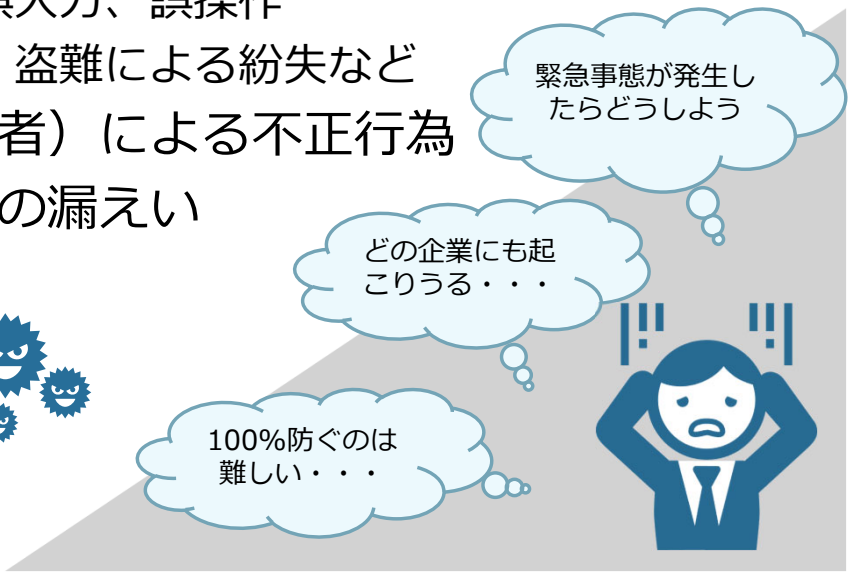
したがって、個人情報漏えい等の事故は、お客様等の関係者を巻き込んでの大きな社会問題になります。

では、万が一、個人情報に関する事故を起こしてしまうと、どのような影響があるのかを確認していきます。

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

など



Copyright © 2024 JIPDEC All Rights Reserved.

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
  2023年度「個人情報の取扱いにおける事故報告集計結果」より

Copyright © 2024 JIPDEC All Rights Reserved.

●最新の事故の傾向について、JIPDECが公表している個人情報の取扱いにおける事故報告の統計資料からご紹介します。

★2023年度「個人情報の取扱いにおける事故報告集計結果」から要点をピックアップしています。

詳細については公表資料をご参照ください。

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

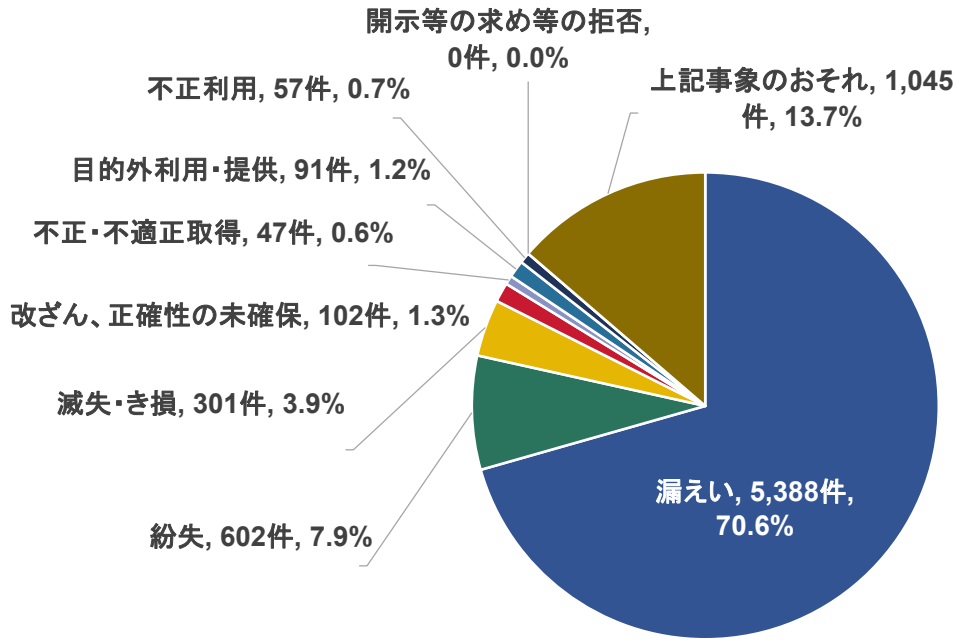
2023年度の事故報告概要

- 発生件数別の傾向
  - 報告事業者数（1,952社）、報告件数（9,208件）ともに2022年度から約1.3倍増加。
  - 速報の事故報告件数（3,005件）は2022年度から約1.6倍増加。
  - 発生事象別では「漏えい」（5,388件：70.6%）が最も多く、次に「紛失」（602件：7.9%）の順。前年度と傾向は同じ 。
  - 事象分類別では「誤配達・誤交付」（2,703件：36.2%）が最も多く、続いて「誤送信」（2,138件：28.7%）の順。前年度と比較すると「誤配達・誤交付」の割合は減少したが、「誤送信」、「不正アクセス」、「マルウェア・ウイルス」 は増加。
  - 原因別では「作業・操作ミス」（3,824件）が最も多く、2022年度から約1.6倍に増加。

Copyright © 2024 JIPDEC All Rights Reserved.

●2023年度中にJIPDECと各審査機関に報告があったプライバシーマーク付与事業者の個人情報の取扱いにおける事故についての概要です。

発生事象別の傾向



「漏えい」が一番多く、次いで「紛失」、そして「滅失・き損」の順。

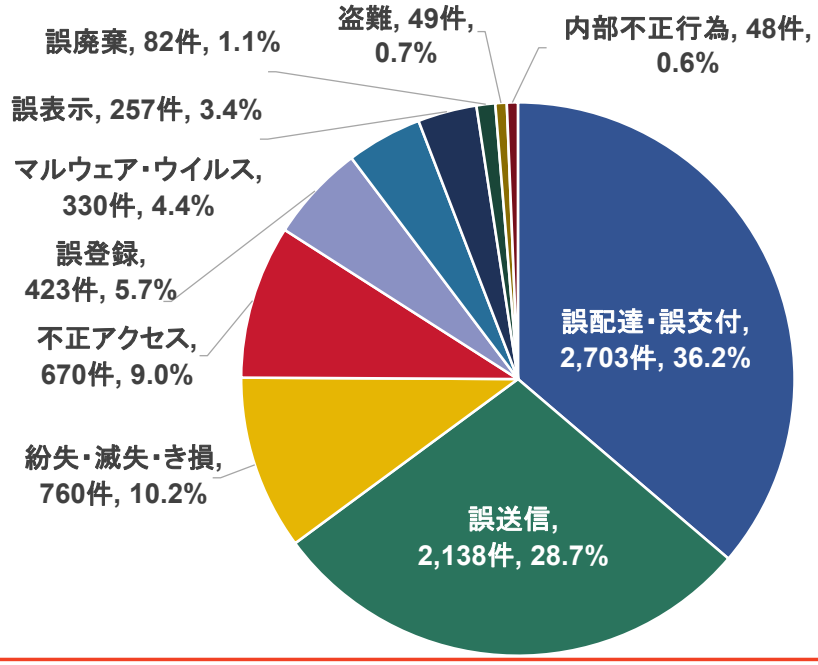
出典：（2023年度）「個人情報の取扱いにおける事故報告集計結果」

Copyright © 2024 JIPDEC All Rights Reserved.

●2023年度の発生事象別の傾向

2023年度の事故の発生事象別では、「漏えい」が一番多く、次いで「紛失」、そして「滅失・き損」の順となっています。（2022年度と傾向は同じ）

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。

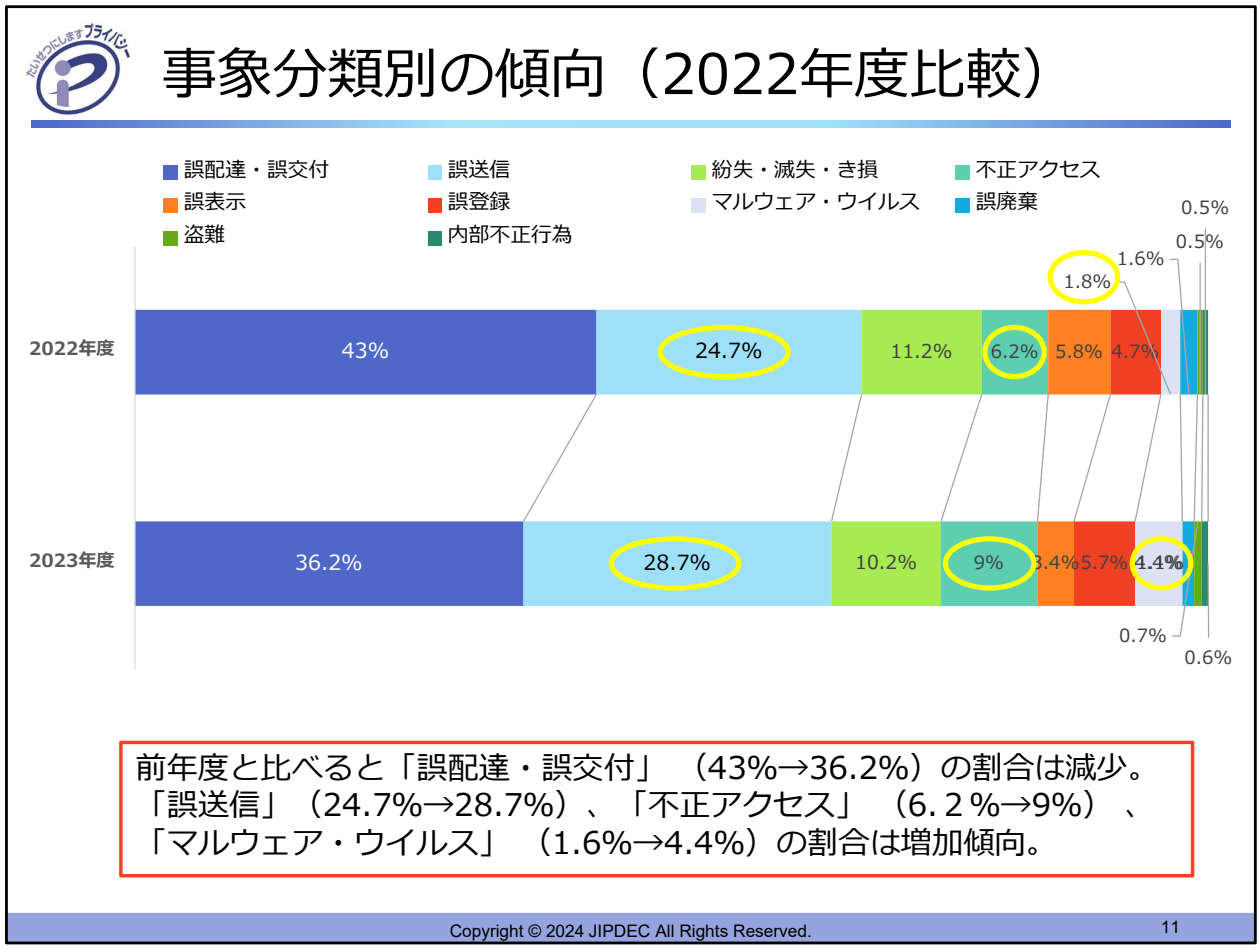
出典：（2023年度）「個人情報の取扱いにおける事故報告集計結果」

Copyright © 2024 JIPDEC All Rights Reserved.

●2023年度の事象分類別の傾向

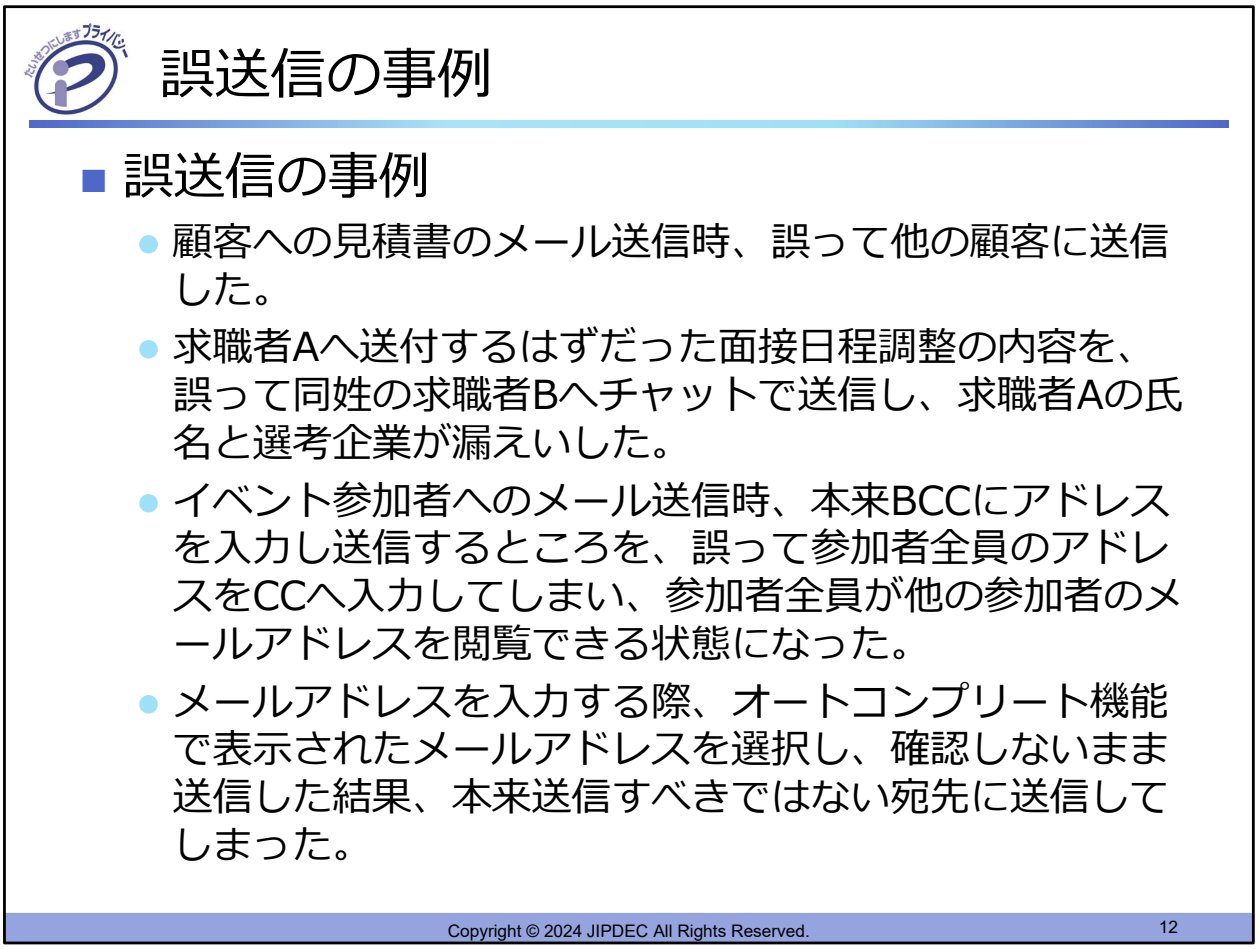
2023年度の事故の発生事象別では、「誤配達・誤交付」が一番多く、次いで「誤送信」、そして「紛失・滅失・き損」の順となっています。

（2022年度と傾向は同じ）



●事象分類別に関する2023年度と2022年度の比較

前年度と比べると、「誤配達・誤交付」の割合は減少しました。一方で、「誤送信」、「不正アクセス」、「マルウェア・ウイルス」の割合はそれぞれ増加しています。



●誤送信の事例

事象分類別の傾向で2022年度より増加した誤送信の事故事例をみていきます。

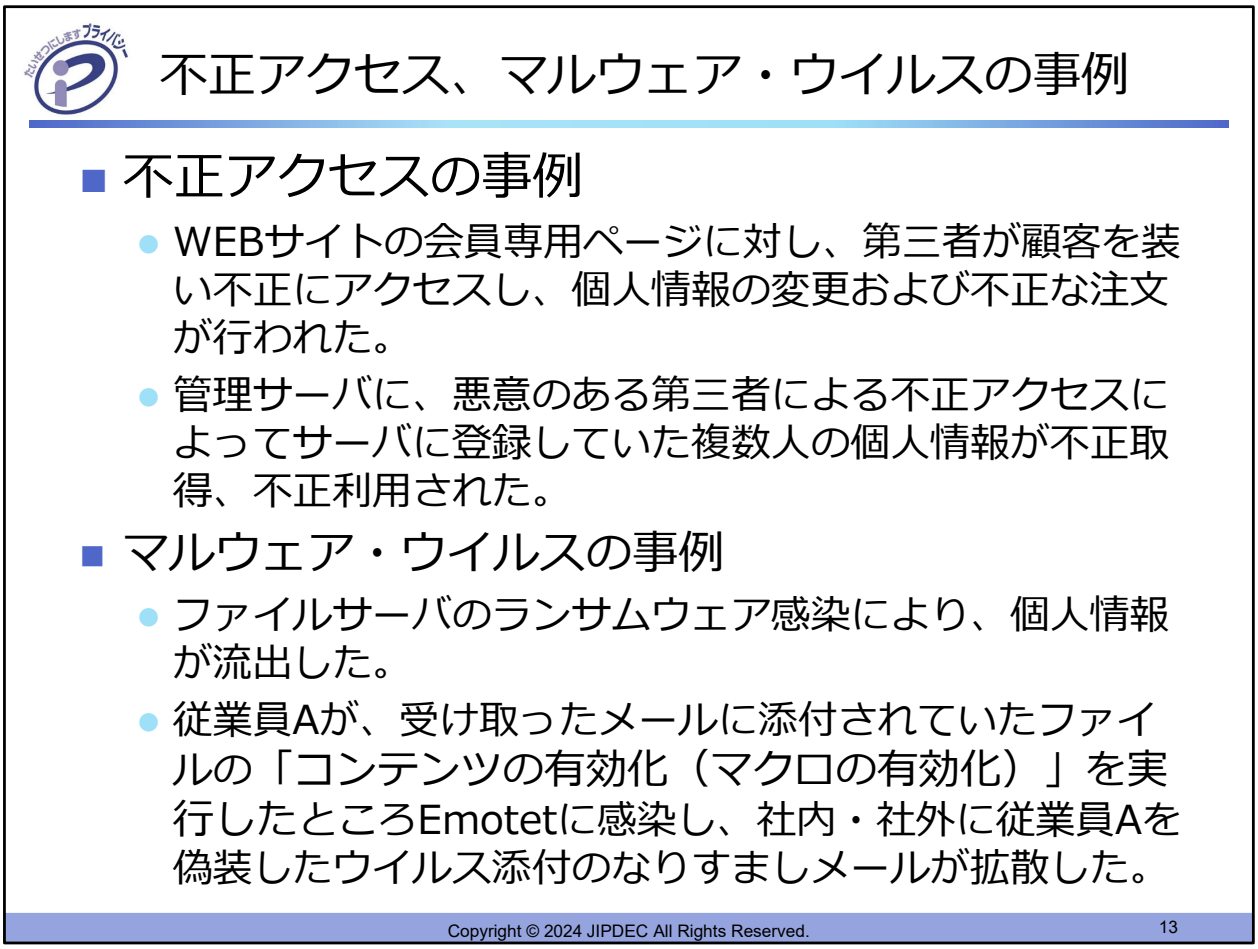
＜参考資料＞

誤送信のうち、メール誤送信に関するその他の事例や対策については、JIPDECプライバシーマーク推進センターが公表する社内教育用資料

「メール誤送信を防ごう」をご覧ください。

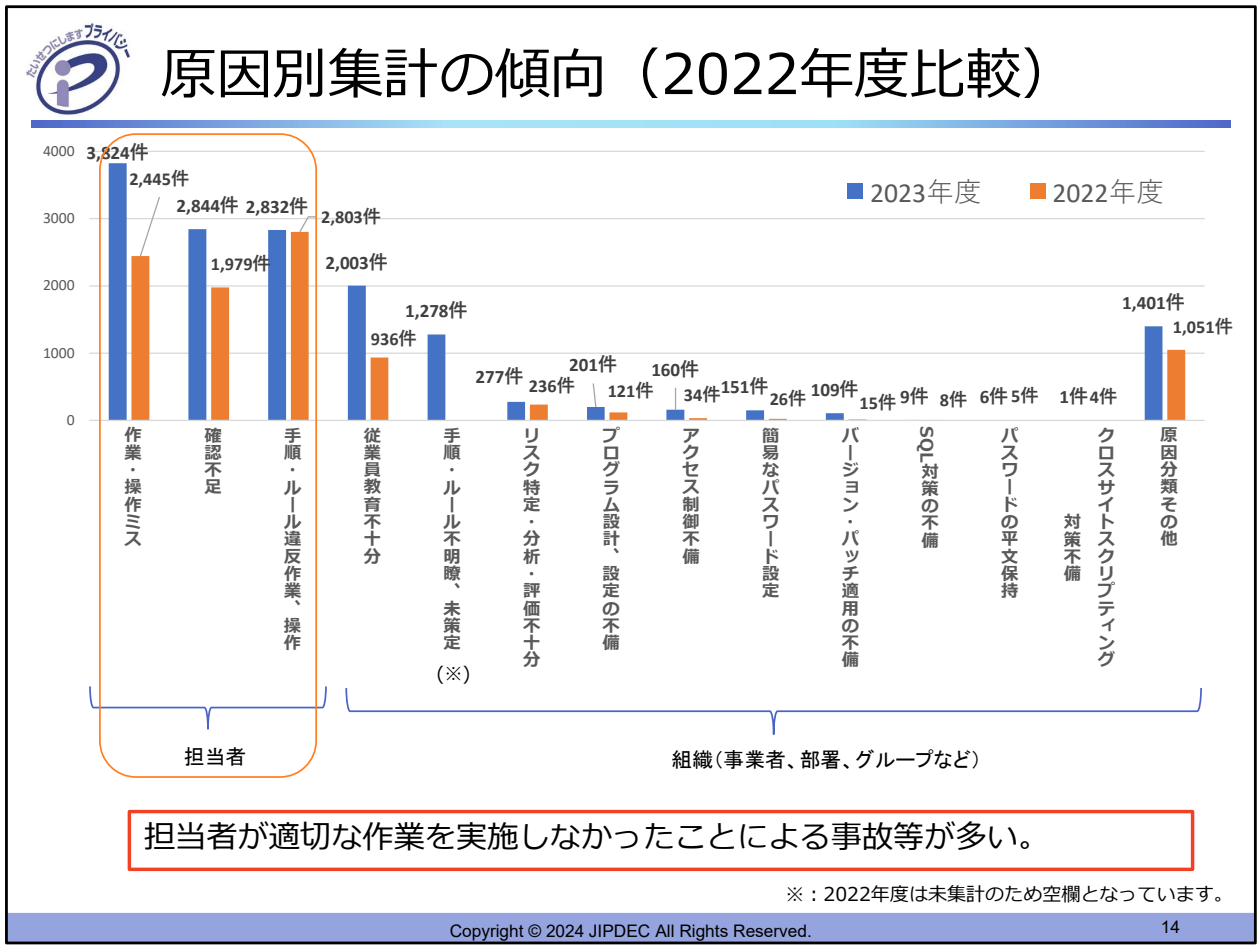
基本編：個人情報の取扱いに関する事故を起こさないために「メール誤送信を防ごう」

https://privacymark.jp/guideline/wakaru/index.html



●不正アクセス、マルウェア・ウイルスの事例

事象分類別の傾向で2022年度より増加した不正アクセス、マルウェア・ウイルスの事故事例をみていきます。



●2023年度の原因別集計の傾向（2022年度との比較）

2022年度の件数は9,663件でしたが、2023年度は15,096件となり、約1.6倍に増加しています。

2022年度、2023年度共に、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多く発生しています。

- 個人情報の取扱いに関する事故の影響

Copyright © 2024 JIPDEC All Rights Reserved.

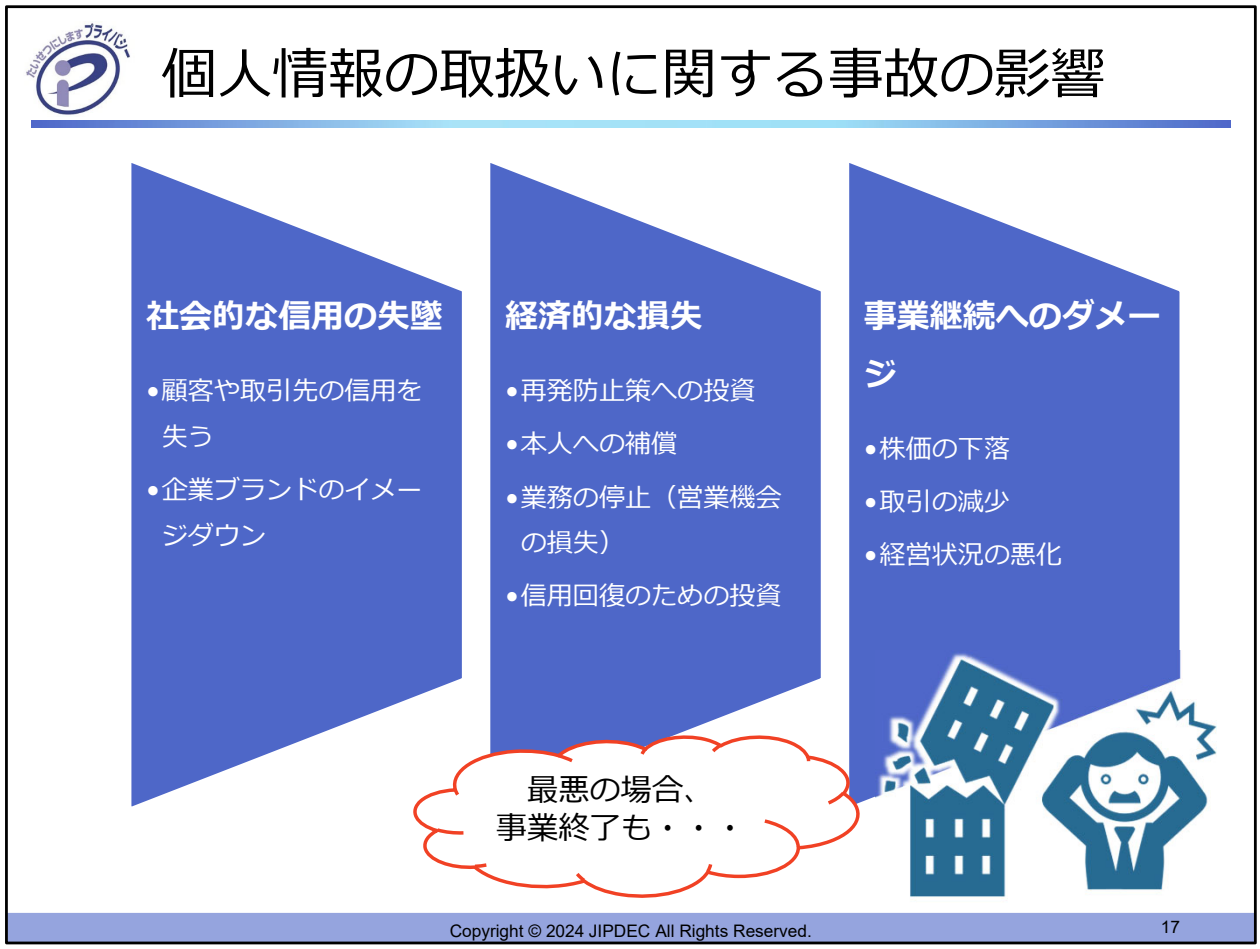
個人情報の事故を起こしてしまうと・・・

- 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・・・。

Copyright © 2024 JIPDEC All Rights Reserved.

●万が一、自社において個人情報に関する事故を起こしてしまった際の関係者（自社も含む）の思いは。

・事故の対象となったお客様
・事故の対象とはなっていないが、自社と取引のあるお客様



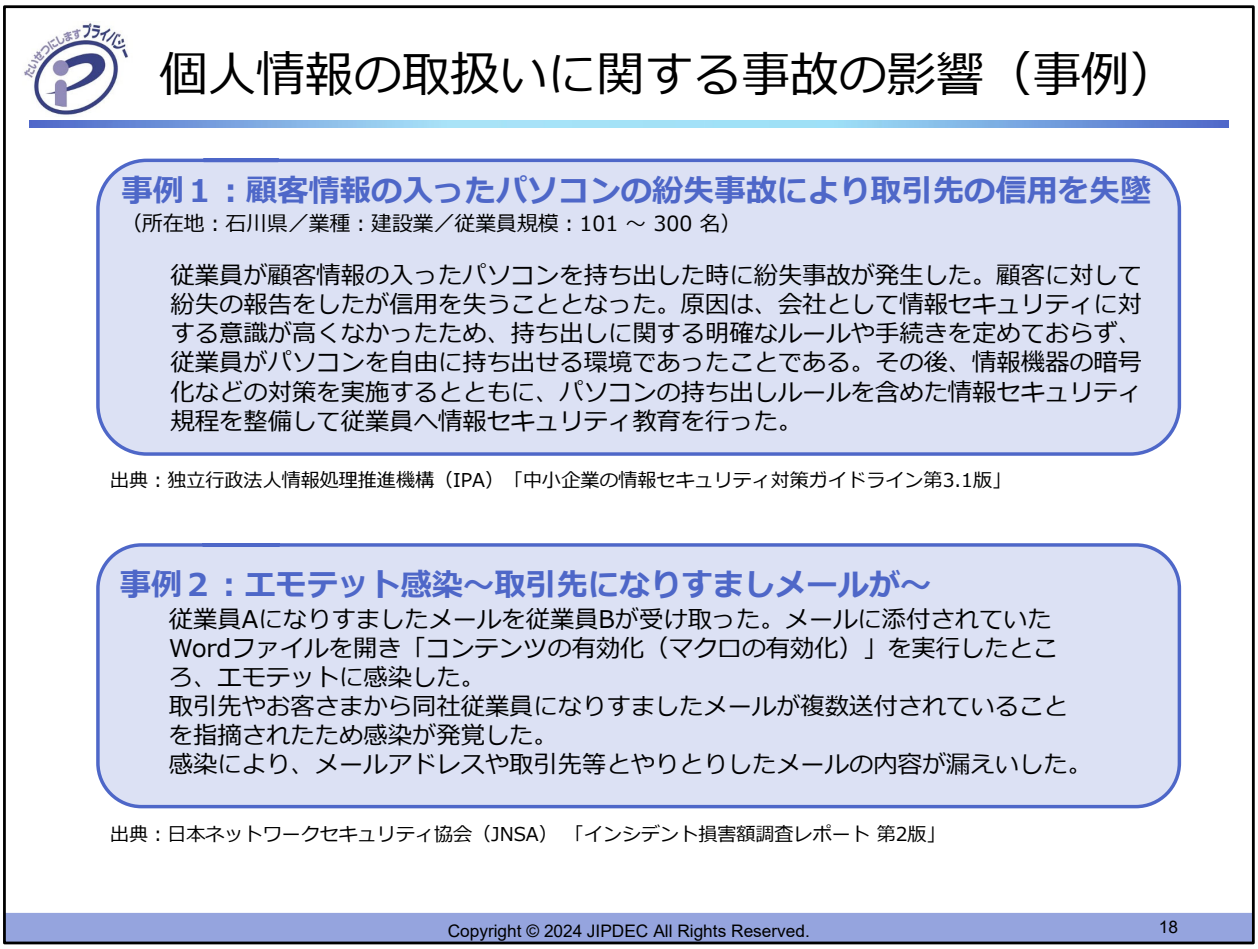
●個人情報の取扱いに関する事故の影響

①社会的な信用の失墜=顧客や取引先の信用はもちろん、業界全体の信用が失われる場合もあります。またこれまで培ってきた自社のブランドイメージも低下するなどの影響があります。

②経済的な損失=現状把握・被害拡大防止のために業務停止となれば、当然その間の売上は失われます。さらに再発防止のための投資、ご本人への謝罪・補償なども必要となる場合もあります。

③事業継続へのダメージ＝被害の規模が大きく事故への対応に時間がかかった場合、結果的に事業経営に大きく影響を及ぼす可能性があります。

⇒個人情報の事故が事業経営に及ぼす影響は非常に大きい



個人情報の取扱いに関する事故の影響（事例）

事例１：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」

事例２：エモテット感染～取引先になりすましメールが～

従業員Aになりすましたメールを従業員Bが受け取った。メールに添付されていたWordファイルを開き「コンテンツの有効化（マクロの有効化）」を実行したところ、エモテットに感染した。
取引先やお客さまから同社従業員になりすましたメールが複数送付されていることを指摘されたため感染が発覚した。
感染により、メールアドレスや取引先等とやりとりしたメールの内容が漏えいした。

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 第2版」

Copyright © 2024 JIPDEC All Rights Reserved.

●個人情報の取扱いに関する事故の影響（事例）

【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」

https://www.ipa.go.jp/security/guide/sme/about.html

・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 第2版」

https://www.jnsa.org/result/incidentdamage/202402.html

●事例については、最近の事故などを紹介し、より具体的に説明することによって、より理解を促すことができます。

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。

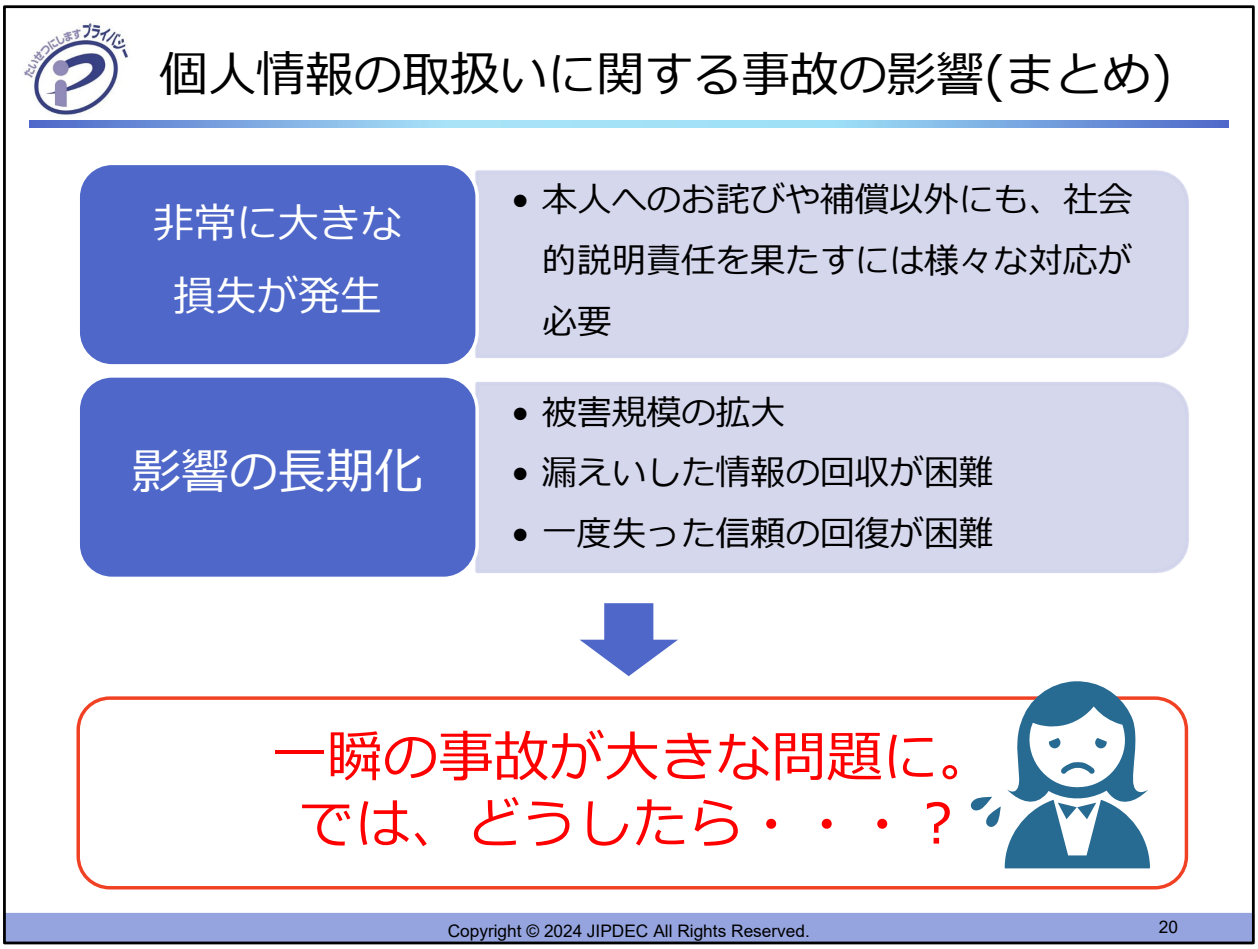
Copyright © 2024 JIPDEC All Rights Reserved.

●個人情報の取扱いに関する事故の影響（被害額）

【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～」

https://www.jnsa.org/result/incidentdamage/202407.html

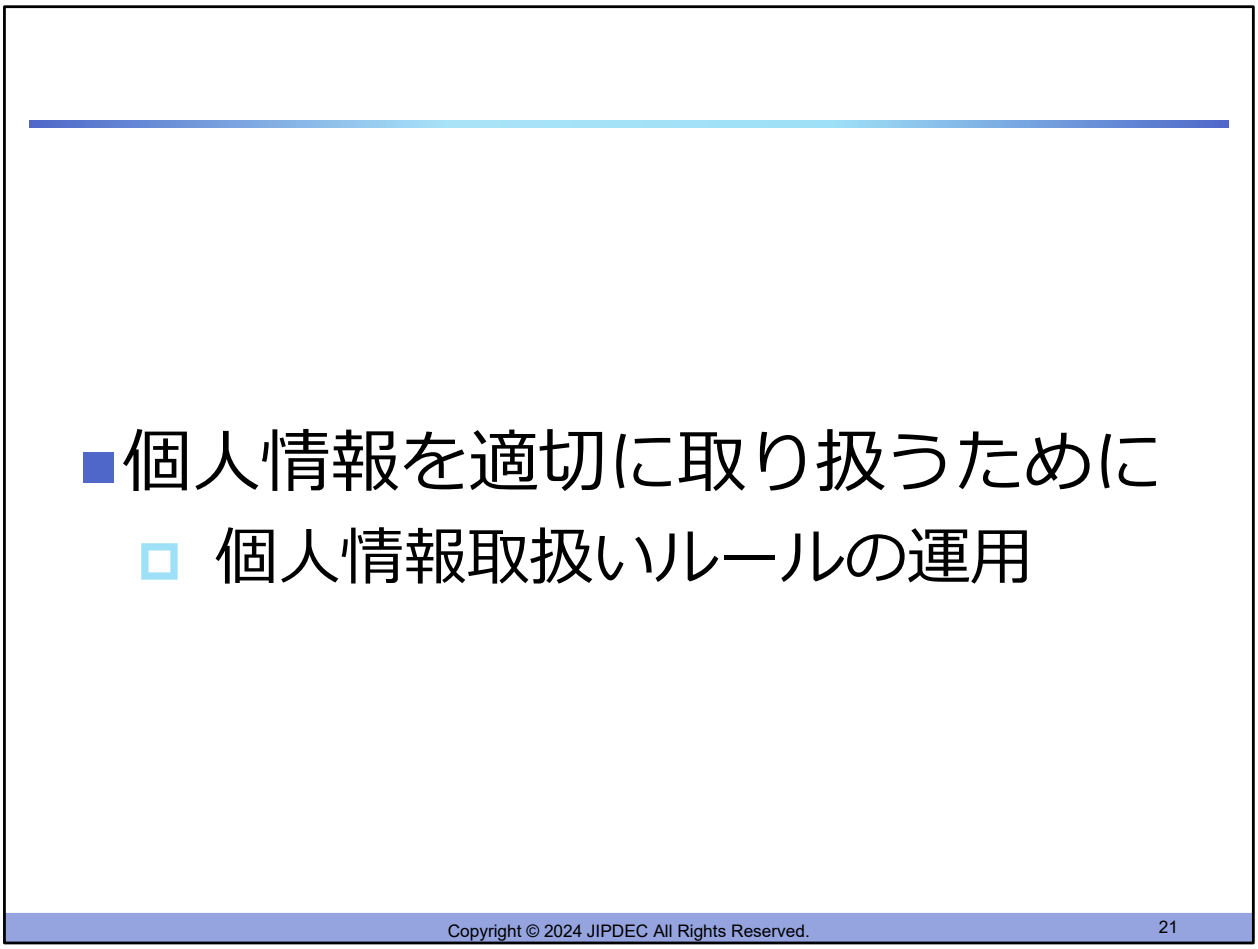


●個人情報の取扱いに関する事故の影響は、金銭的な負担のほか、社会的な信用の失墜など非常に大きな損失が生じます。

近年多くなっているインターネットを介した漏えいでは、情報の拡散が速く、回収も困難であり一度発生させた場合は影響が長期化する可能性が大きくなります。

このように、一瞬の事故が大きな問題につながっています。

こうした事態を発生させないために、事業者は、またそこで働く従業者はどうしたらよいかを考えていきます。

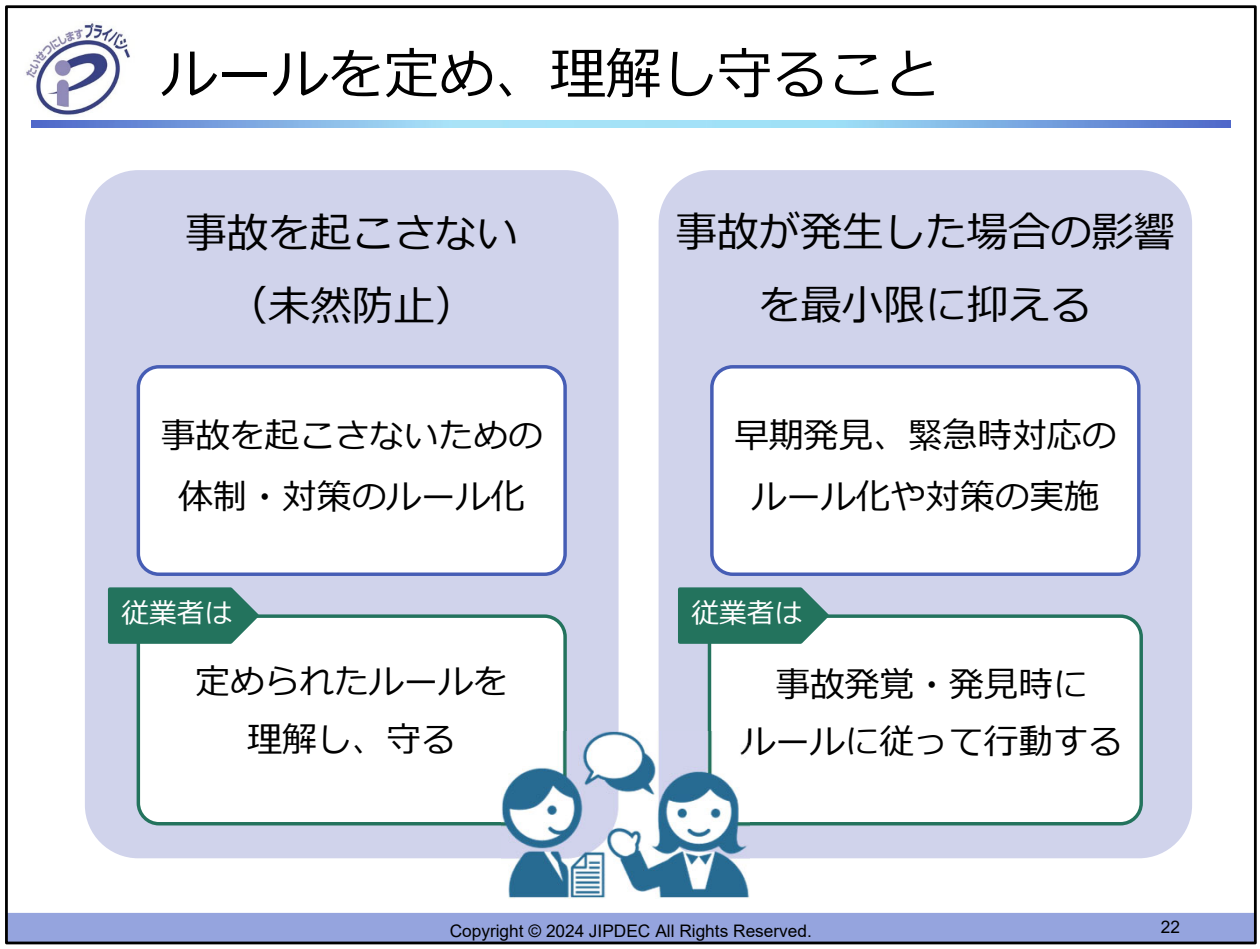


●事業者は、個人情報の取扱いに関するルールを定め運用することで、事故というリスクに備えます。

一度事故を起こしてしまうとその対応を対策には非常に大きなコストと時間がかかります。

そこで重要となるのは以下の点です。

・事業者がルールを定め、それを従業者全員が理解して守ること
・事業者がリスク対策を見直し、改善すること



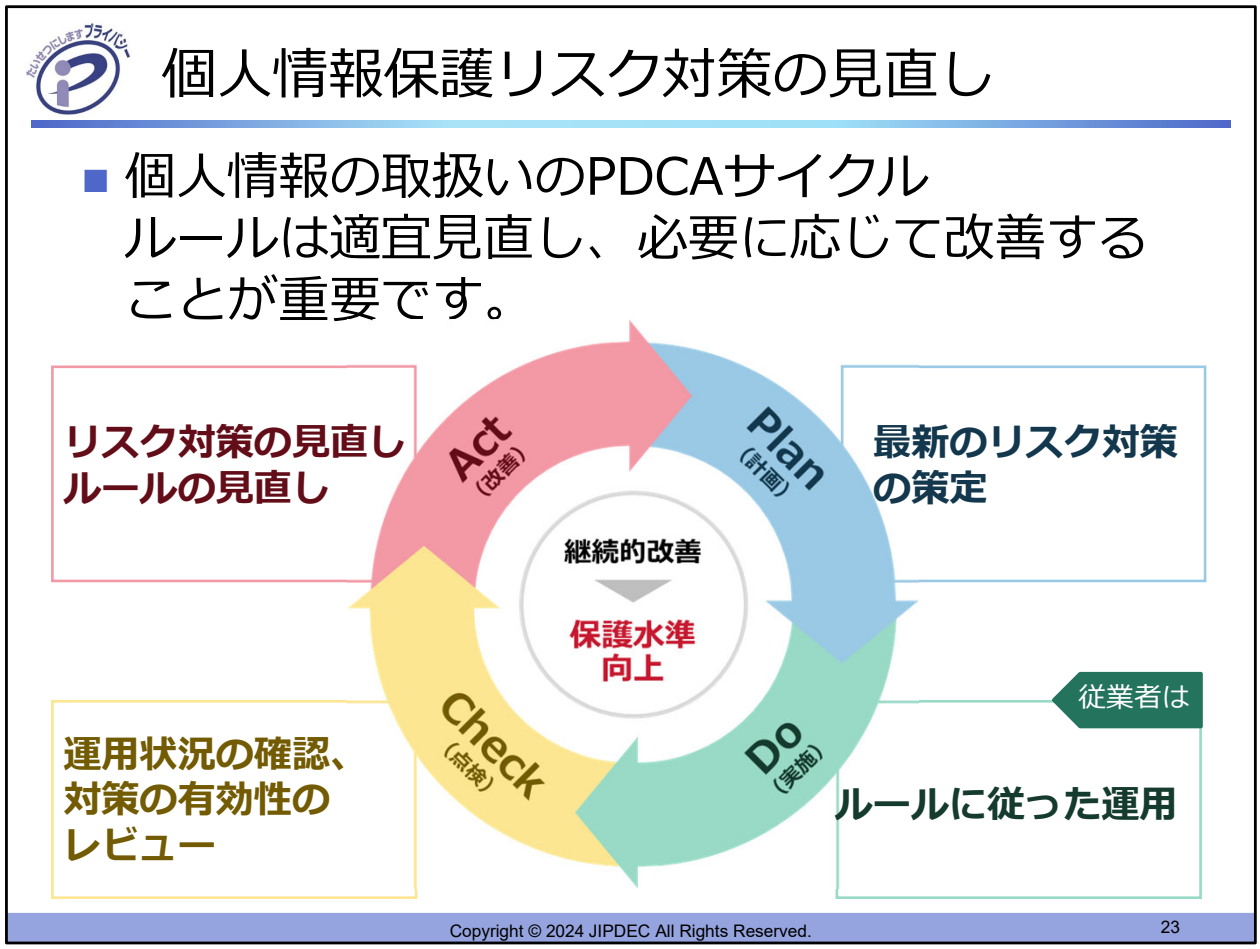
●事業者は、個人情報の取扱いに関するルールを定め運用することで、事故というリスクに備えます。

事故を起こさないために、また万が一発生した場合の影響を最小限に抑えるために

まずは、

- 事故を起こさないための体制、仕組みを作る
- 起きた場合の影響を最小限に抑えるためのルールを作成する

⇒そして「従業者全員」が、ルールを理解し、守り運用していくことが第一です。

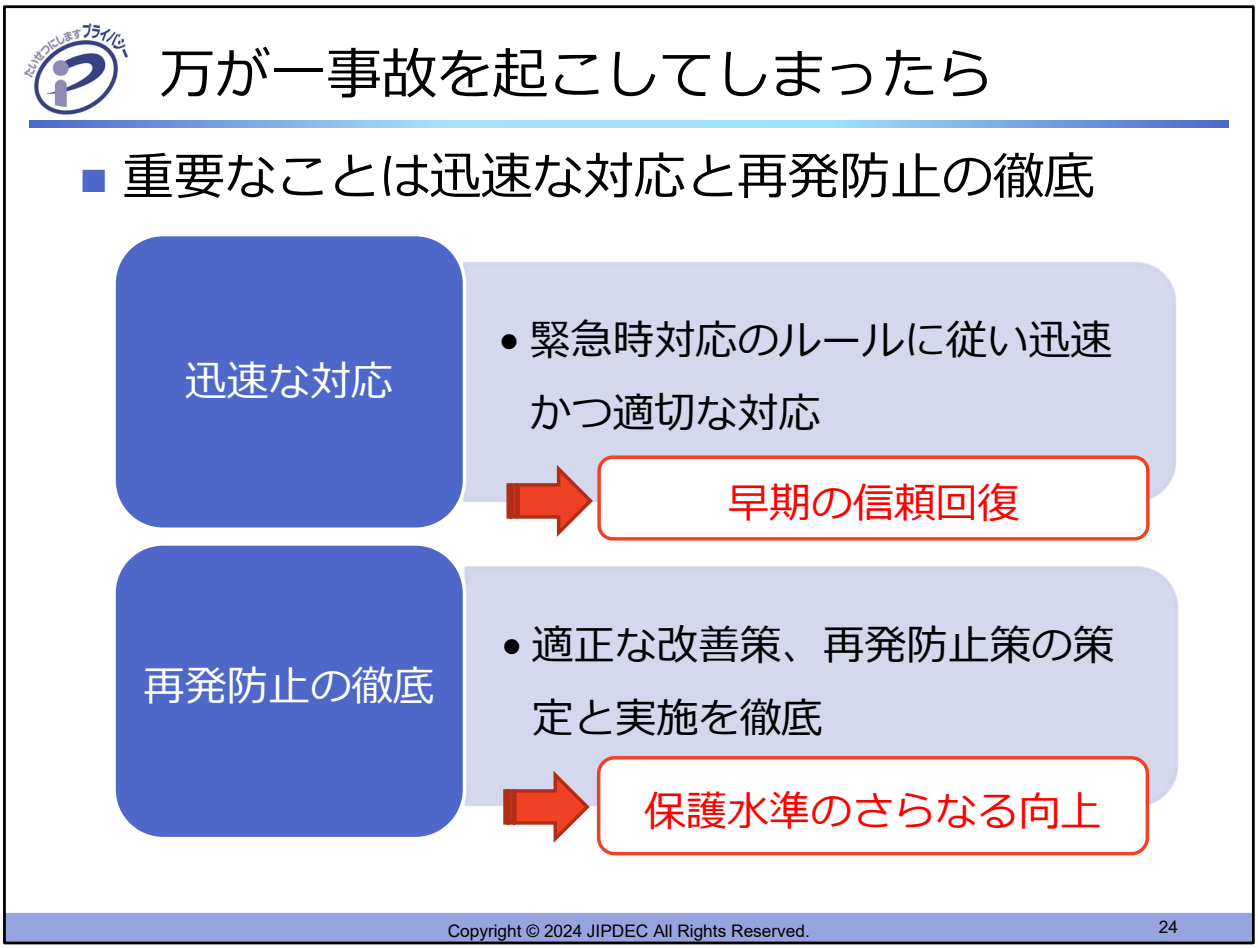


●プライバシーマーク制度では、個人情報の取扱いについてルールを定め、PDCAサイクルに沿った運用を実施することを求めています。
（この研修もDo「実施」に当たります。）

★ここで示しているのは、個々の業務における個人情報の取扱いについてのPDCAサイクルです。
　事業者としての個人情報マネジメントシステムのPDCAサイクルの中で、個々の業務におけるPDCAサイクルも含まれます。

このPDCAサイクルを継続的にまわしていき、改善していくことで個人情報の保護水準を向上していきます。

⇒見直されたルールが、適時、従業者に周知され、最新のルールに従って個人情報を取り扱うことが重要です。

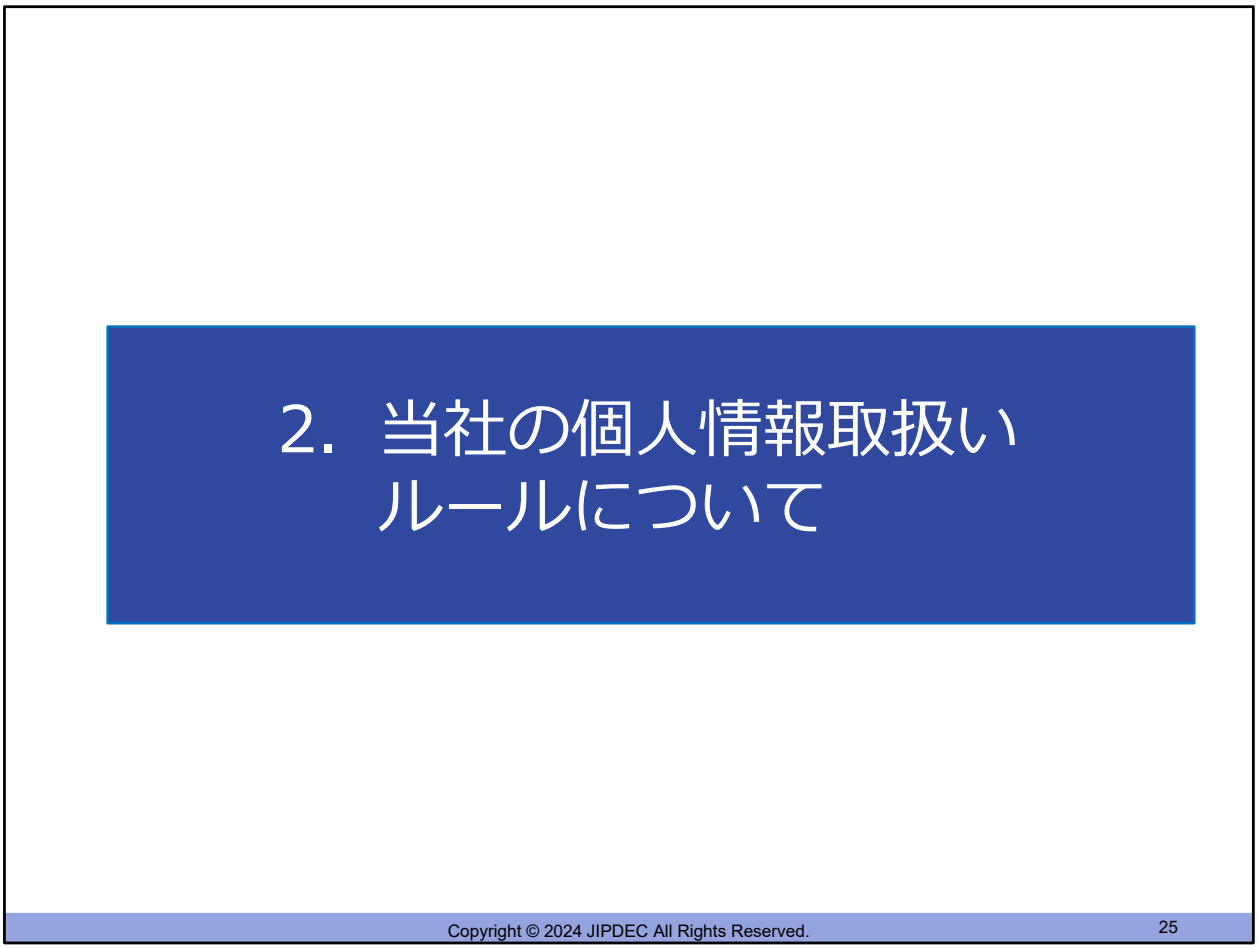


●最後に、万が一事故を起こしてしまったら。

緊急事態への対応ルールに従い、迅速に対応することが重要です。

適正な改善策の策定と実施、および再発防止を徹底することにより、早期の解決、信頼回復につながります

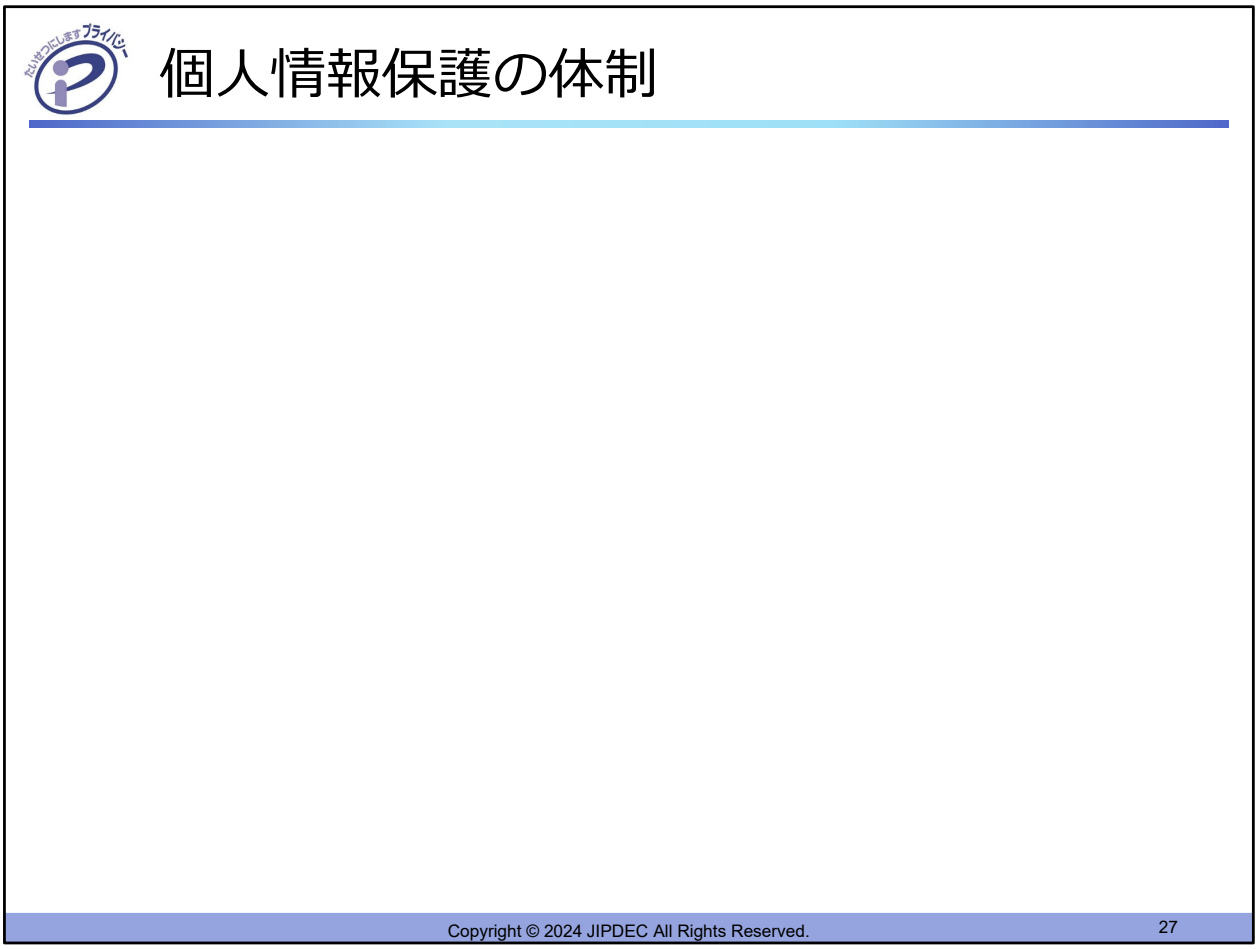
●自社の緊急事態への対応ルールについて、次の第2部で周知しましょう。



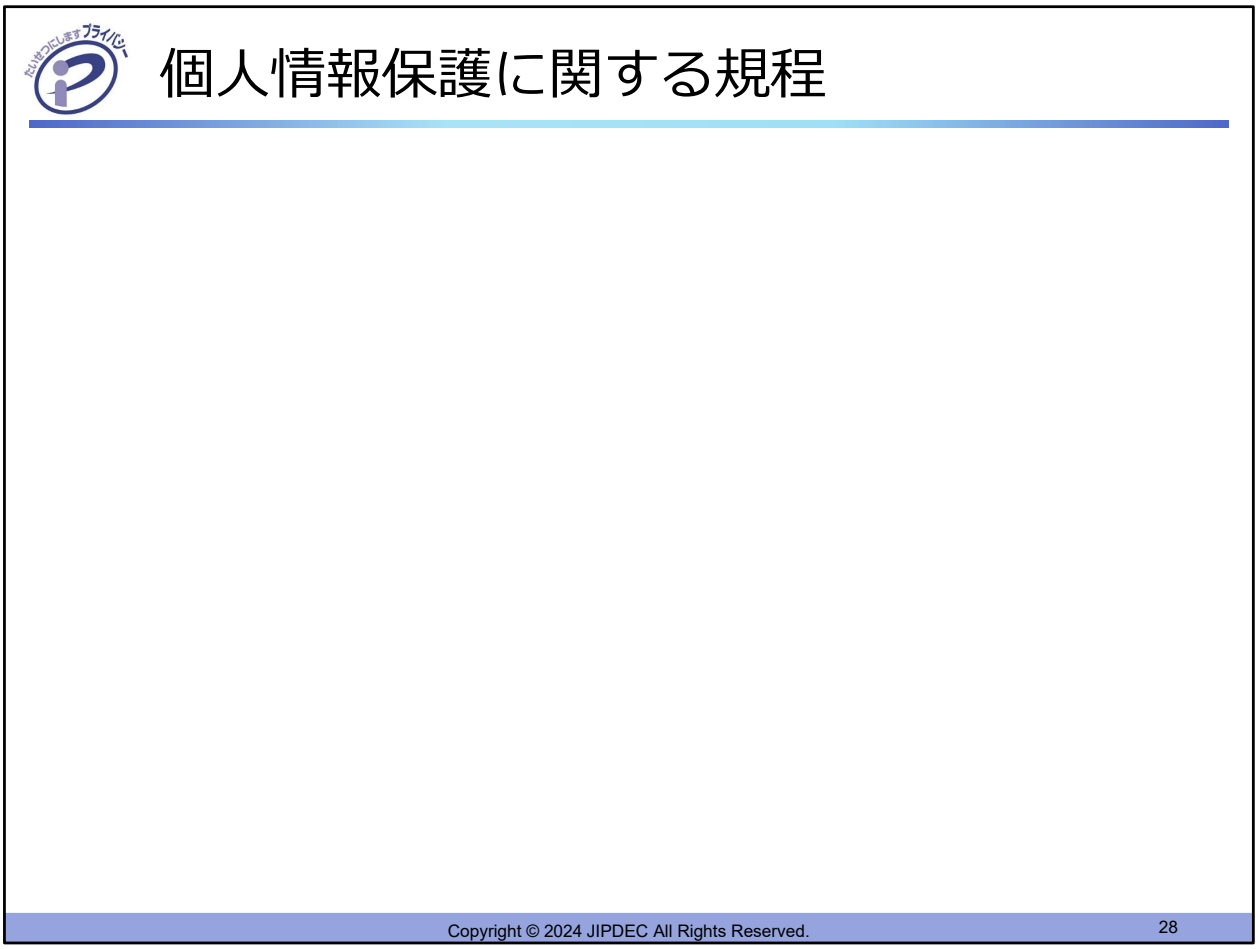
●第2部は、自社における個人情報取扱いに関する規程、ルールを追記してご利用ください。

使用例：

自社の個人情報保護方針の内容、掲載先などを記載します。



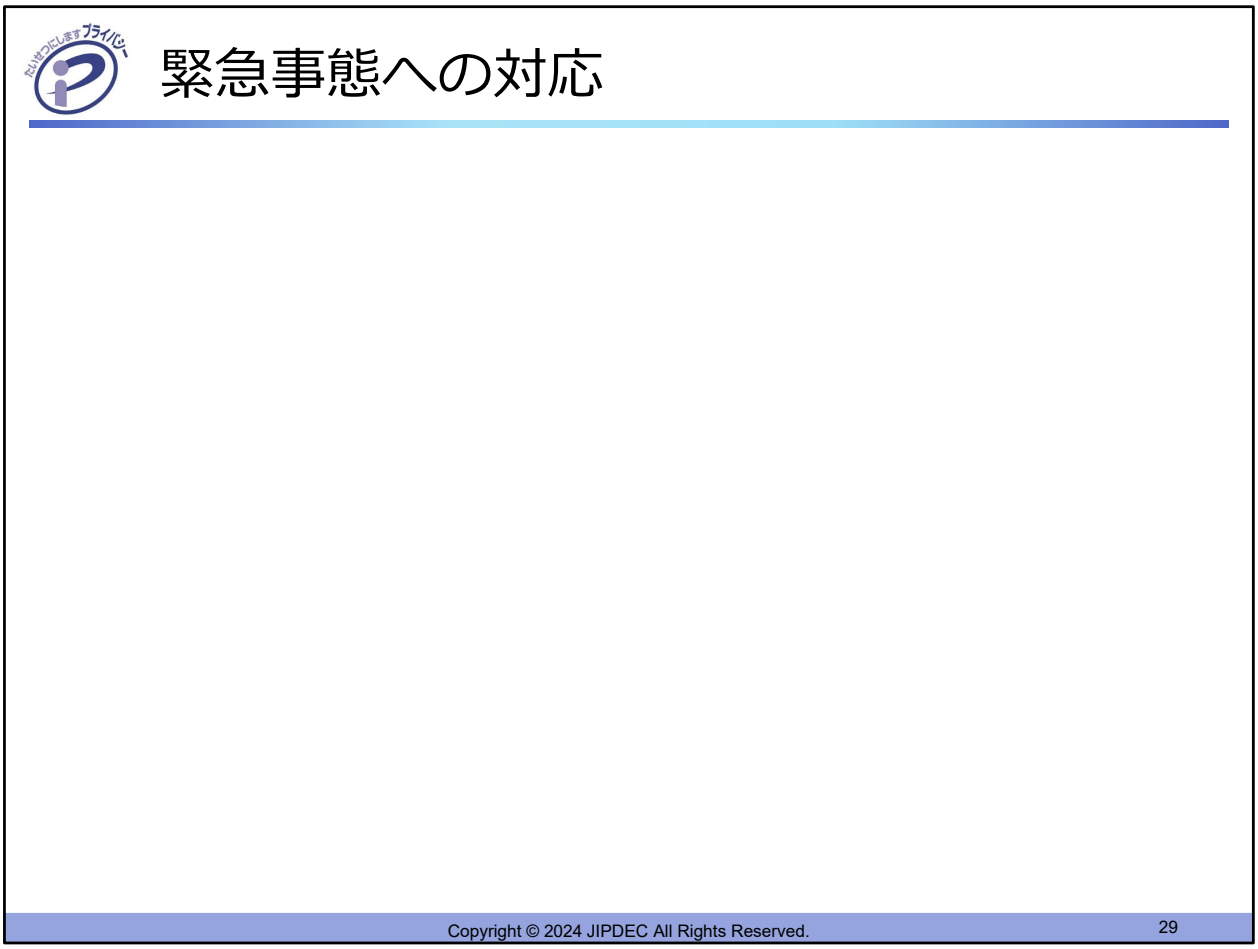
使用例：
自社の個人情報保護の体制図や一覧などを記載します。



使用例：
自社の個人情報保護に関する規程の体系、手順書などを記載します。
　・規程名
　・保管先（イントラネット、ファイルサーバーなど）

★必要に応じて、個々のルールについても記載します。

・個人情報が記載された書類等を送付する場合のルール
・メール等に添付、電子媒体で個人情報を送付する場合のルール
・個人情報を保管する場合のルール
・個人情報を削除する際のルール
・個人情報が記載された書類、PC等を持ち出す際のルール
・個人情報を委託する際のルール
など

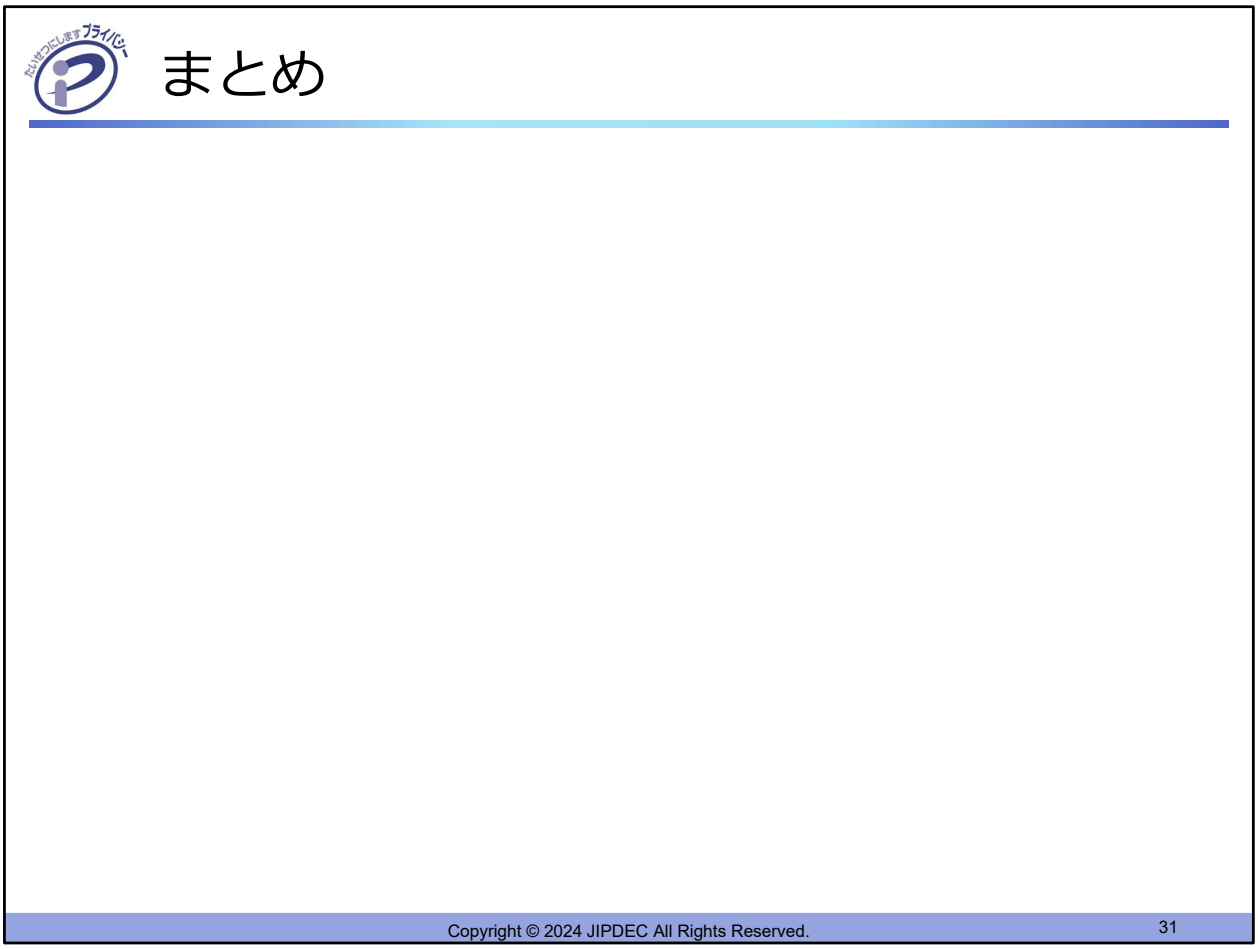


使用例：
自社における緊急事態への対応フローなどを記載します。

・事故が発生・発覚した場合の対応手順、連絡先（連絡網）は？

3．まとめ

Copyright © 2024 JIPDEC All Rights Reserved.



使用例：

・自社の規程等の閲覧・参照場所の案内
・緊急時連絡網の案内
・PMS事務局・担当からのお知らせ
・個人情報に関する相談・問合せ先（自社内）
・トップマネジメントのメッセージ

など

（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。）”

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

Copyright © 2024 JIPDEC All Rights Reserved.

●プライバシーマーク制度で定める事故の定義
プライバシーマーク制度　運営要領
https://privacymark.jp/system/about/procedure.html

事故等の報告
https://privacymark.jp/p-application/incident/index.html

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/about/procedure.html
  - 個人情報の取扱いにおける事故報告集計結果
    https://privacymark.jp/guideline/wakaru/index.html
  - 全従業員向け社内教育用資料・社内教育用動画
    基本編：個人情報の取扱いに関する事故を起こさないために
    https://privacymark.jp/guideline/wakaru/index.html
  - 事故等の報告
    https://privacymark.jp/p-application/incident/index.html

Copyright © 2024 JIPDEC All Rights Reserved.