個人情報管理の重要性

2021年11月15日

JIPDEC

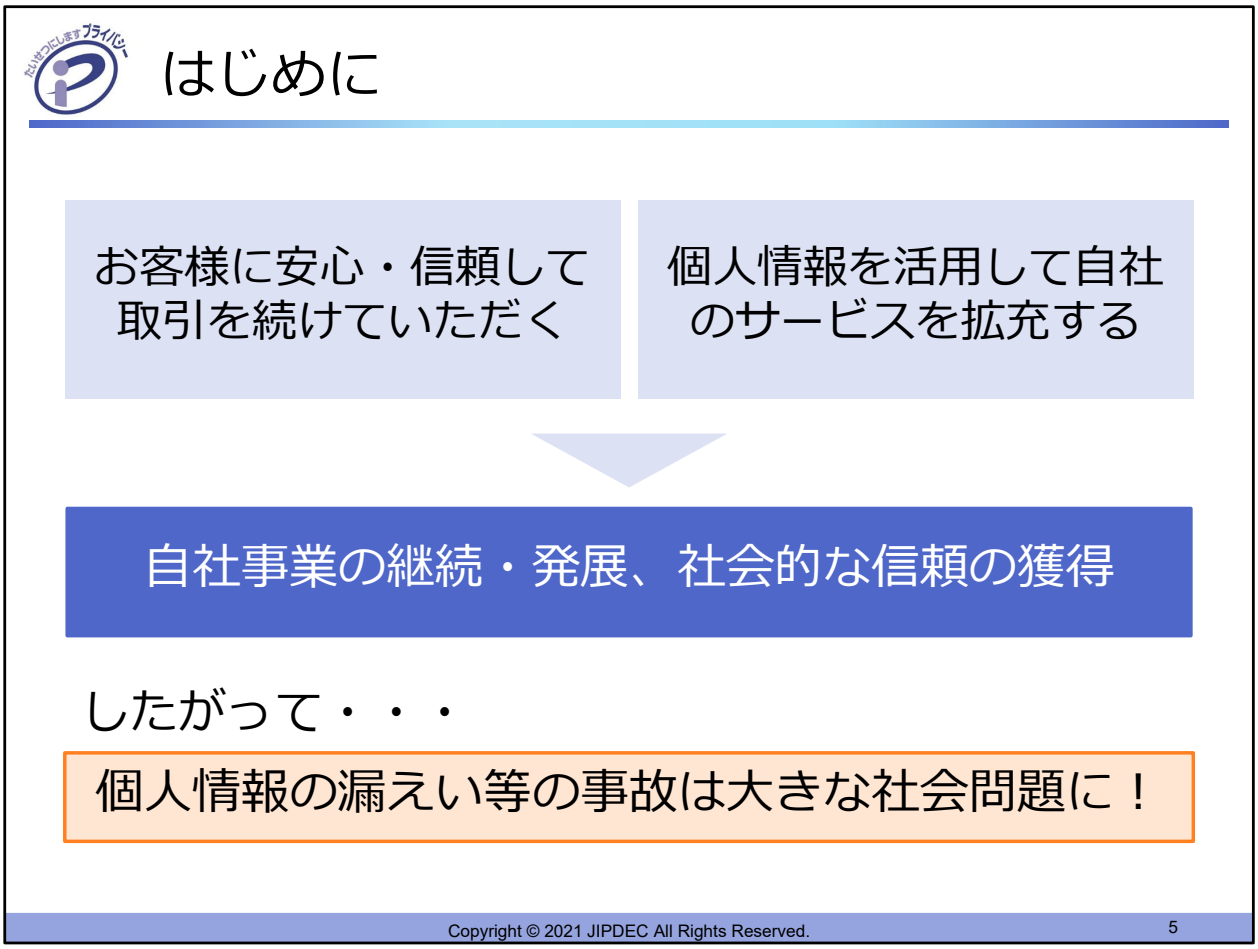
一般財団法人日本情報経済社会推進協会
プライバシーマーク推進センター

目次

1. 個人情報の管理はなぜ必要？

●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



●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

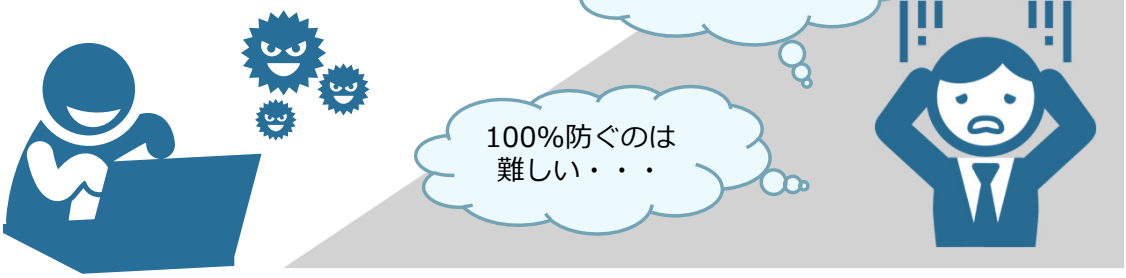
したがって、個人情報漏えい等の事故は、お客様等の関係者を巻き込んでの大きな社会問題になります。

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等

など



●プライバシーマーク付与事業者の皆さまへ

具体的な事故の事例について、付与事業者専用サイトのコンテンツもご参照ください。

付与事業者専用サイトは、プライバシーマーク付与事業者が閲覧できるサイトです。

「個人情報の取扱いに関する事故を発生させないために」

https://member.privacymark.jp/

■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

●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。

★2020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。

プライバシーマーク制度＞制度の案内＞参考情報

https://privacymark.jp/system/reference/pdf/2020JikoHoukoku_211005.pdf

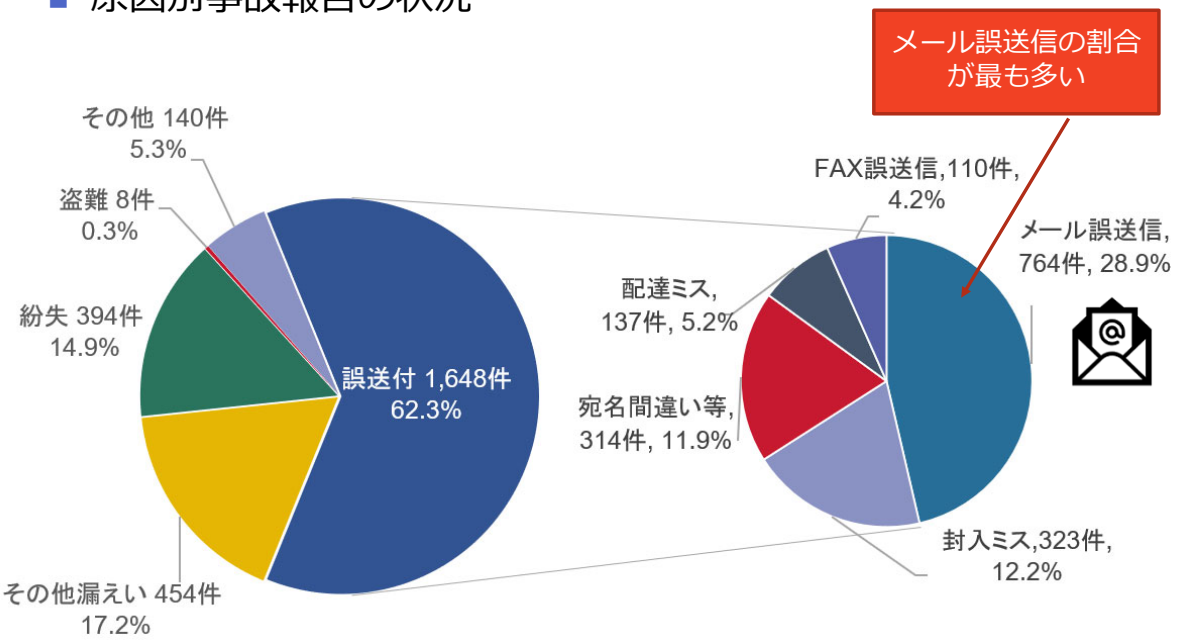
2020年度の事故報告概要

- 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。

●2020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」

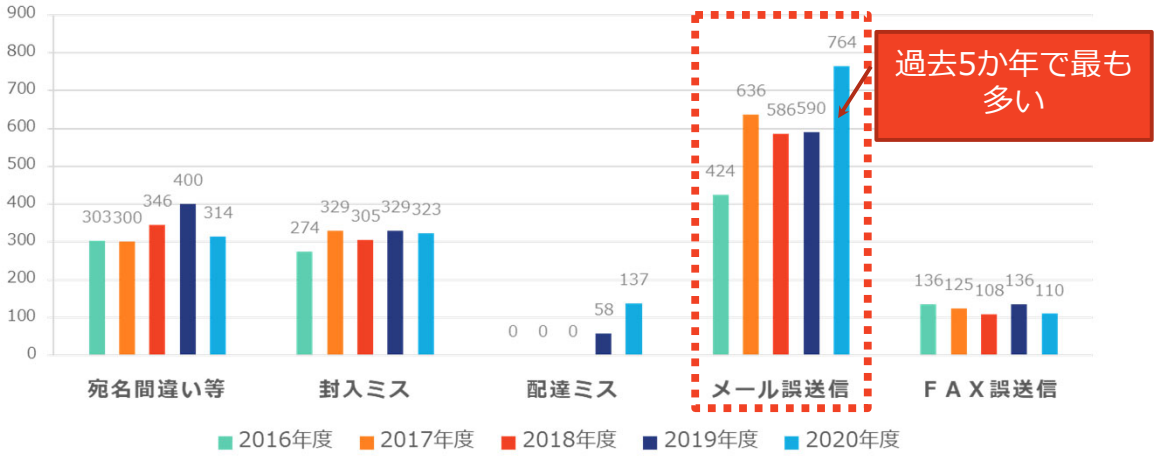
●2020年度の原因別事故報告の状況

2020年度の事故の発生原因別では、「誤送付」が一番多く、次いで「その他漏えい」、そして「紛失」の順となっています。（昨年度と傾向は同じ）

「誤送付」の内訳では、「メール誤送信」の764件が一番多く、事故報告全体の中でも報告件数が最も多いです。

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」

●原因別事故報告件数のうち「誤送付」の内訳推移

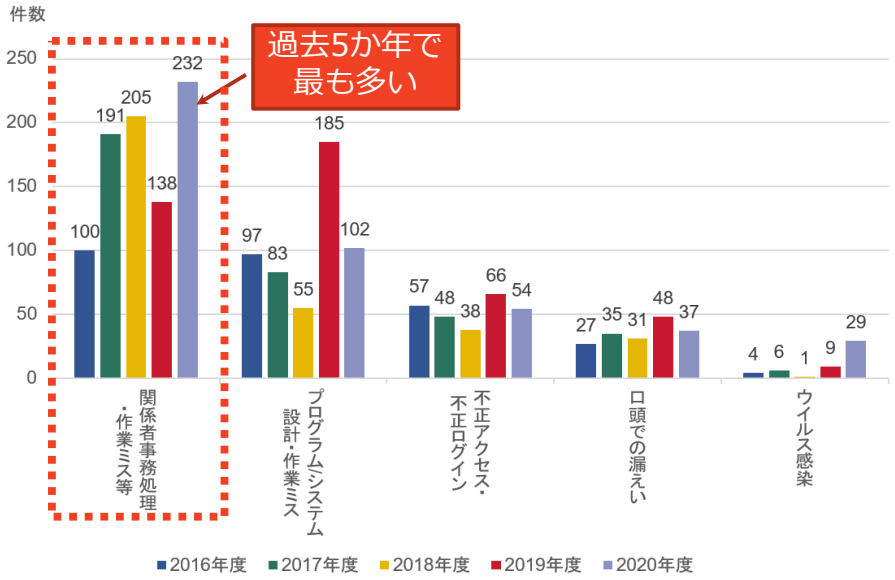
「宛名間違い等」「封入ミス」等、紙媒体による事故報告は減少しました。新型コロナウイルス感染症対策のためのテレワーク実施等により減少したものと推測されます。

一方で、メッセージングサービス等の新たなコミュニケーションツールによる事故も報告されるなど、通信手段・連絡手段の変化により、事故報告の内容も変化が見られます。

★メール誤送信に関する再発防止策例については
以下の公表資料もご参照ください。
⇒お役立ちツール＞社内教育用参考資料
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/system/reference/index.html#tools

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）



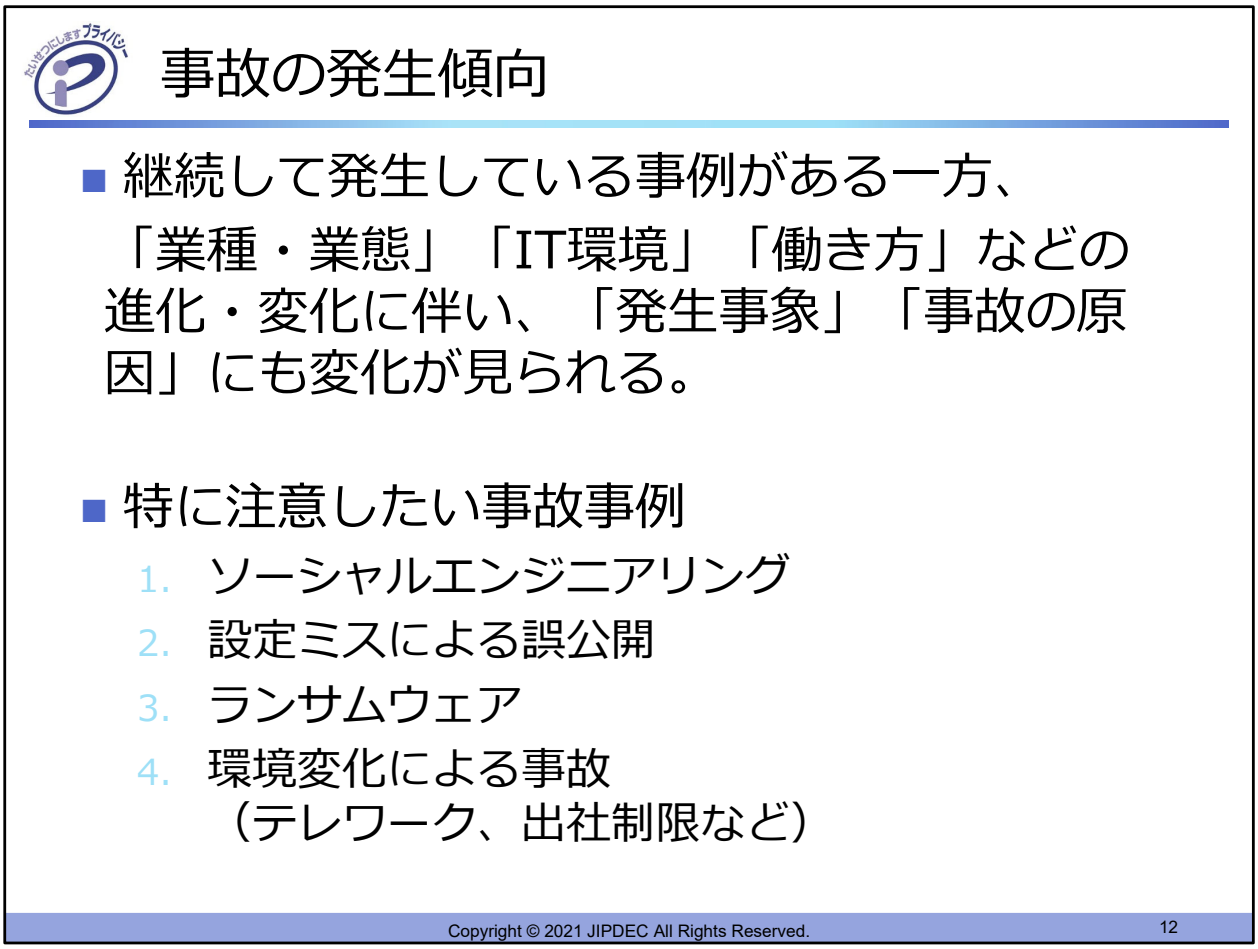
新型コロナウイルス感染症対策などで、いつもと異なる業務環境や手順による作業ミスや事故が発生。

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」

●原因別事故報告件数のうち「その他漏えい」の内訳件数

前年度と比較すると、「その他漏えい」のうち「関係者事務処理・作業ミス等」が大幅に増加しました。

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、作業手順で業務を行うことにより、作業ミスや事故が発生しやすい状況にあったといえます。



●事故の発生傾向

事故の発生傾向としては、継続して発生している事例がある一方で、「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」にも変化が見られます。

今回、特に注意したい事故事例として以下の4点を挙げています。

- ソーシャルエンジニアリング
- 設定ミスによる誤公開
- ランサムウェア
- 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１：ソーシャルエンジニアリング

付与事業者において事故発生件数が増加しています。
古典的な手法ではありますが、特定の個人や集団を狙っており、注意が必要です。

具体的な取り扱いの場面を想定したルールの策定が必要です。
そして、従業者の皆さんはそのルール・手順を確認し遵守しましょう。

★ソーシャルエンジニアリングに関する再発防止策例については
以下の公表資料もご参照ください。
⇒お役立ちツール＞社内教育用参考資料＞
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『日常業務の中で注意すべきこと』
https://privacymark.jp/system/reference/index.html#tools

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２：設定ミスによる誤公開

近年、テレワークを導入する事業者の増加し、業務の電子化、ペーパレス化が進んでいます。それに伴い個人情報の取り扱いに関する手順の策定・ルールの見直しが必要な時期となっています。

紙媒体から電子媒体への変化だけではなく、インターネット上を介した個人情報の取り扱いも増加しており、新たなリスクへの対応も必要となってきます。

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３：ランサムウェア

不正アクセスのターゲットとなるのは大企業だけと思いがちですが、ランサムウェアに関しては中小企業での被害も多く、業種業態や規模の大小に関わらず、事故報告が増えており、全ての企業にとっての脅威となっています。

2021年2月には警視庁から注意喚起もされています。

⇒
https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/ransomware.html

また、ランサムウェアによる被害は、IPAの「情報セキュリティ10大脅威2021」でも組織の項目で1位となっています。

⇒　https://www.ipa.go.jp/security/vuln/10threats2021.html

ランサムウェアは常に攻撃手法や身代金の要求パターンを変更しており、進化を続けています。

今後、対応策も変わっていく可能性はありますが、現在のビジネスシーンにおいては各種サーバやパソコンを使わないという選択肢はなく、常に情報セキュリティに関する情報収集をして、対策をしていくしかありません。

ランサムウェアによる個人情報漏えい事故は、どの企業にも起こりうることです。他人事と思わず、自分事として対応していって欲しいと思います。

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：環境変化による事故

2020年度は、新型コロナウイルス感染症の拡大により、急遽テレワークが導入され、「業務内容」「業務のやり方」「業務環境」などの変更（イレギュラーオペレーション）を余儀なくされる状況となり、多かれ少なかれ、（業務上の）混乱が生じたことと思われます。

こうしたことが原因で個人情報に係る事故が発生した事例もありますが、再発防止を図ることで、思いもよらない状況になった時でも事故を発生させずに業務を行うことができる体制へと強化を図るきっかけとしていただければと思います。

★テレワーク実施時に注意をしなければならない点については、
以下の公表資料もご参照ください。
⇒お役立ちツール＞社内教育用参考資料＞
　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『テレワーク時に注意すべきこと』
　https://privacymark.jp/system/reference/index.html#tools

・総務省「テレワークセキュリティガイドライン（第5版）」
　https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

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。

●特に注意したい事故事例４：環境変化による事故（つづき）

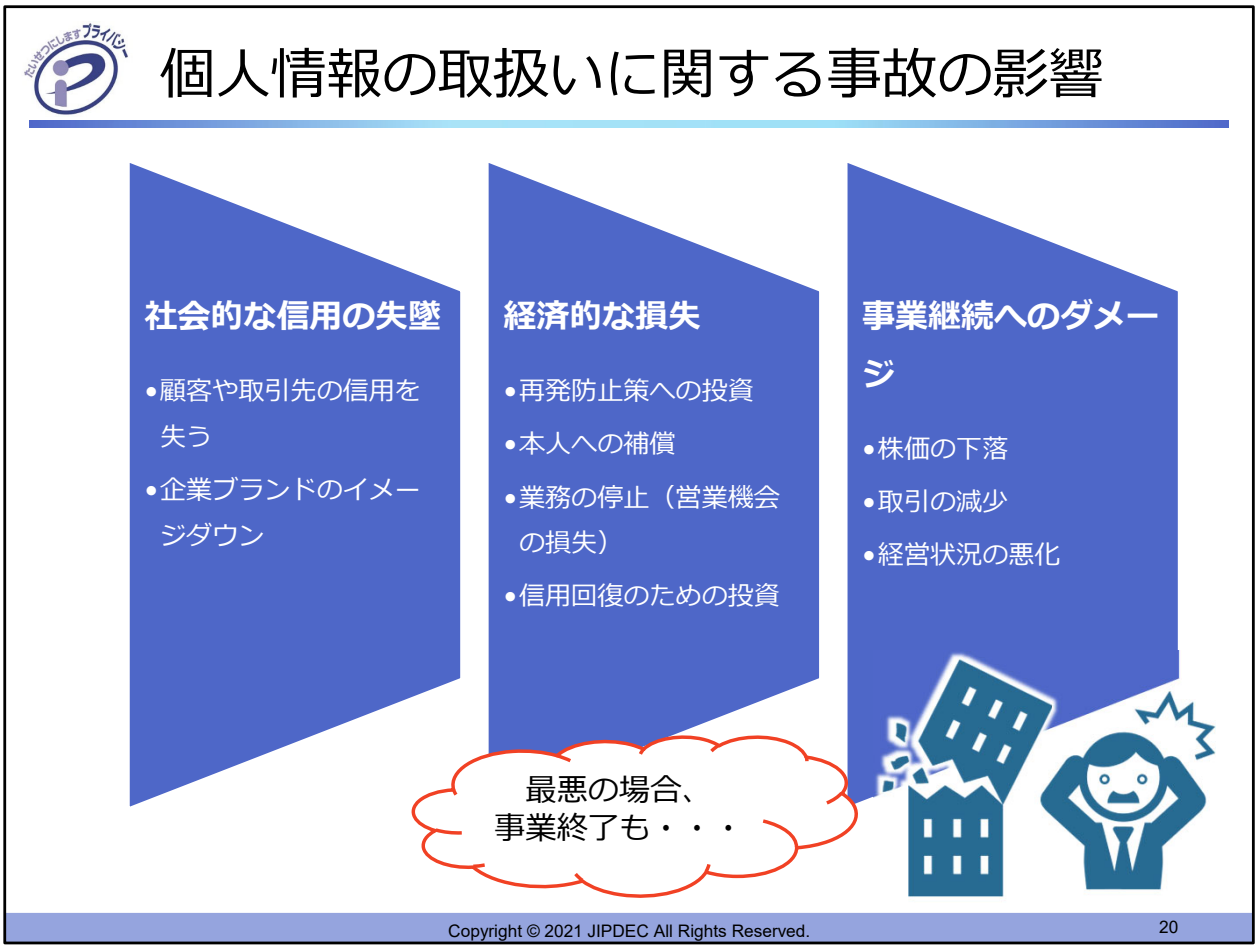
- 個人情報の取扱いに関する事故の影響

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・・・。

●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



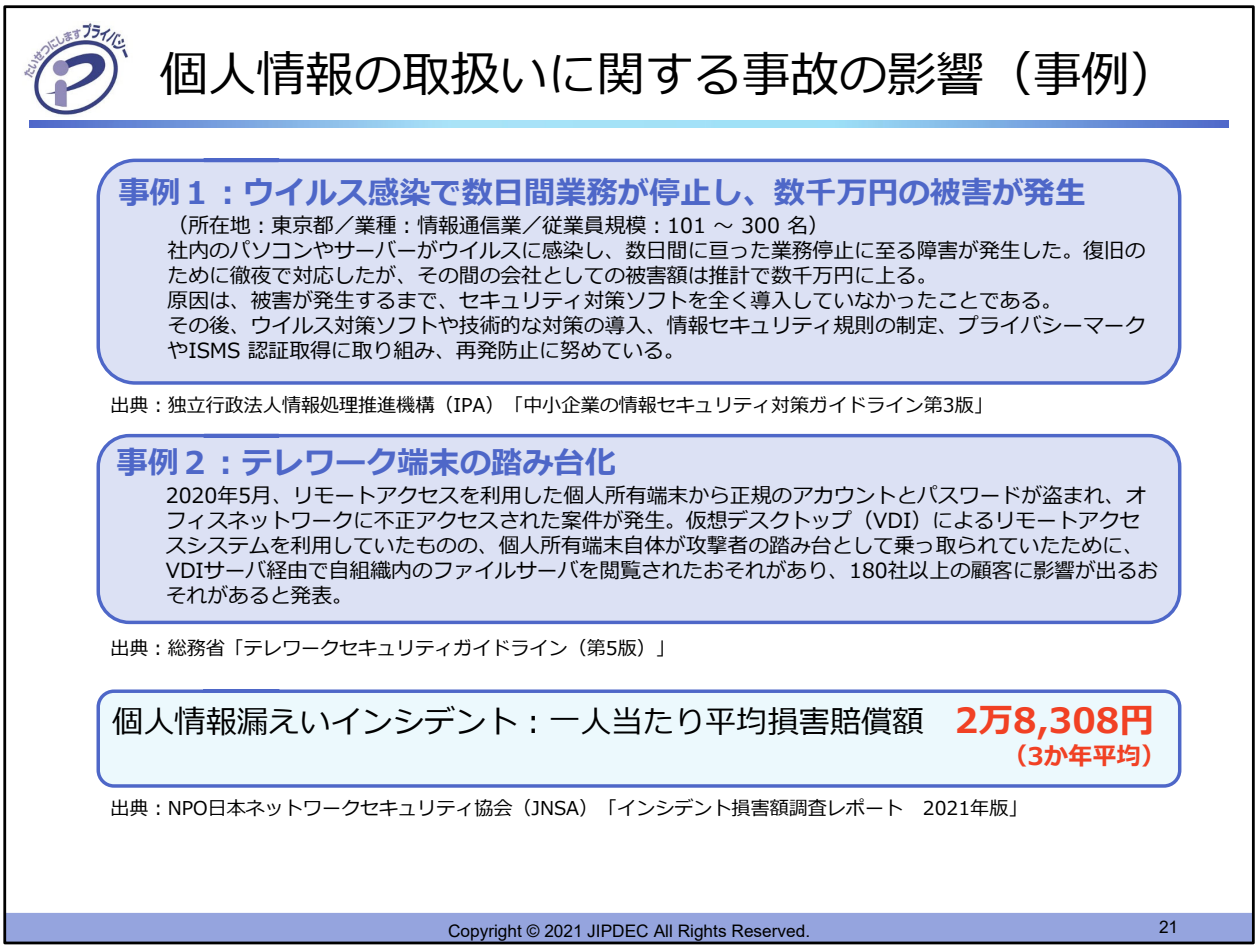
●個人情報の取扱いに関する事故の影響

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）

【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」

https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

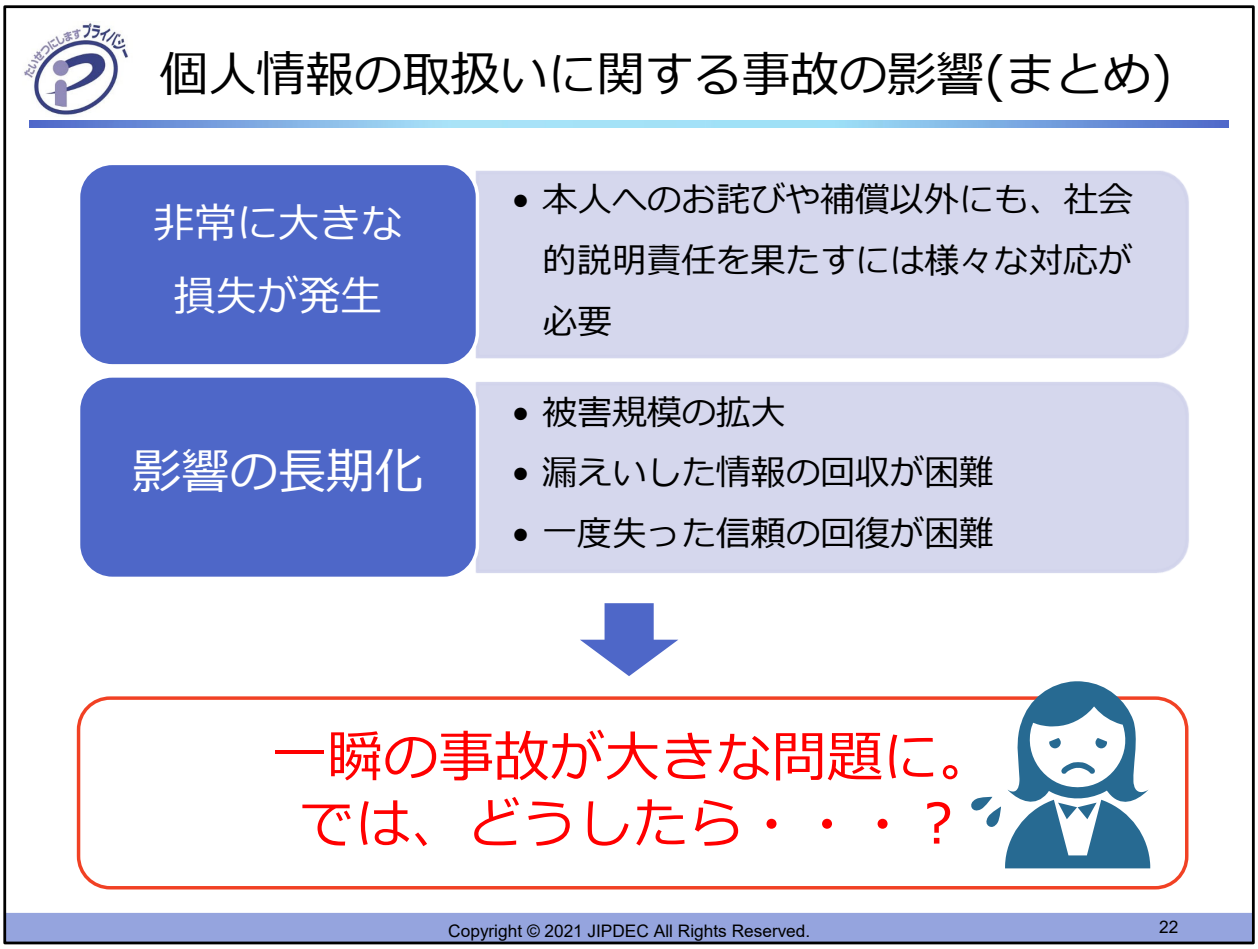
・総務省「テレワークセキュリティガイドライン（第5版）」

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework

・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」

https://www.jnsa.org/result/2021.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。

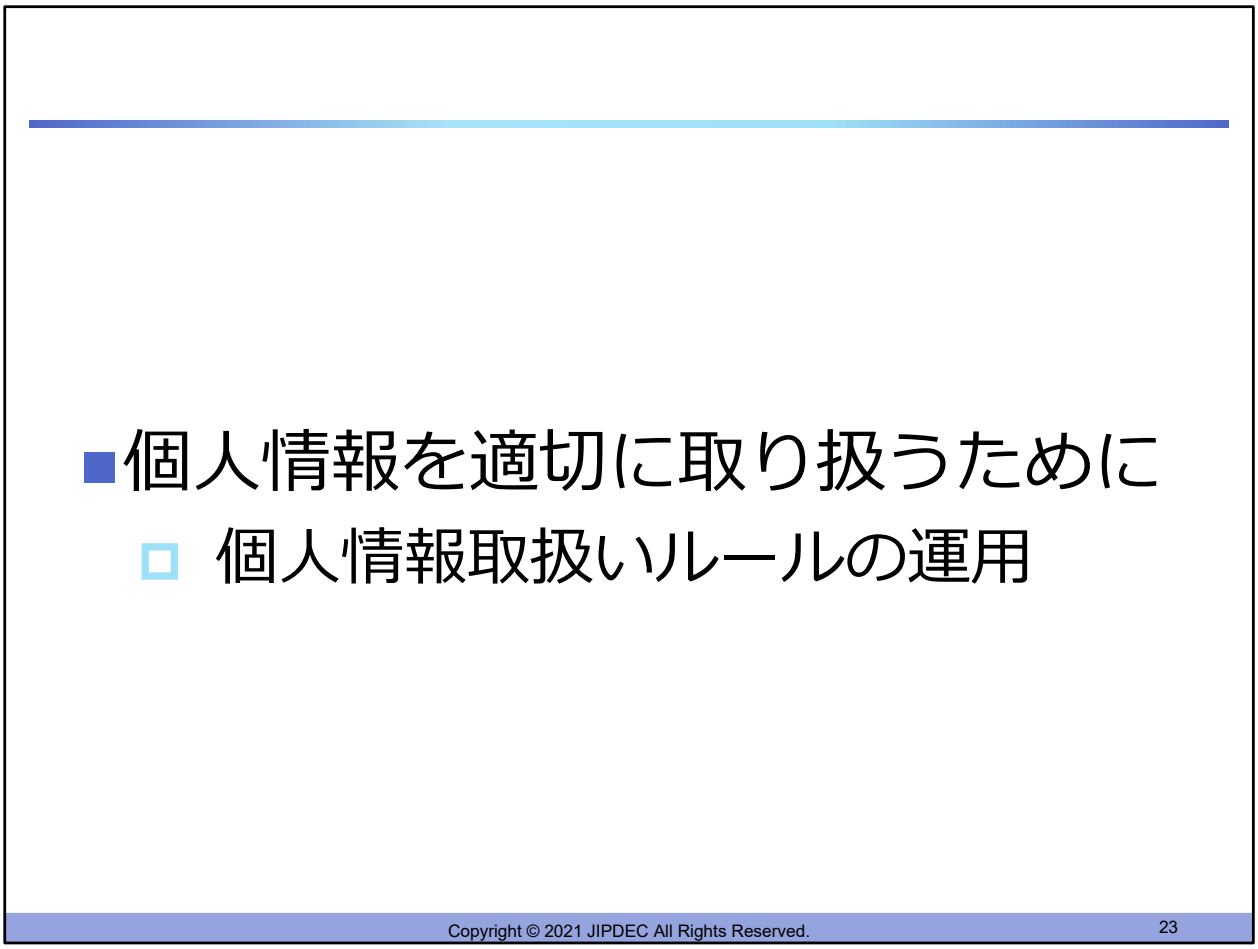


●個人情報の取扱いに関する事故の影響は、金銭的な負担のほか、社会的な信用の失墜など非常に大きな損失が生じます。

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。

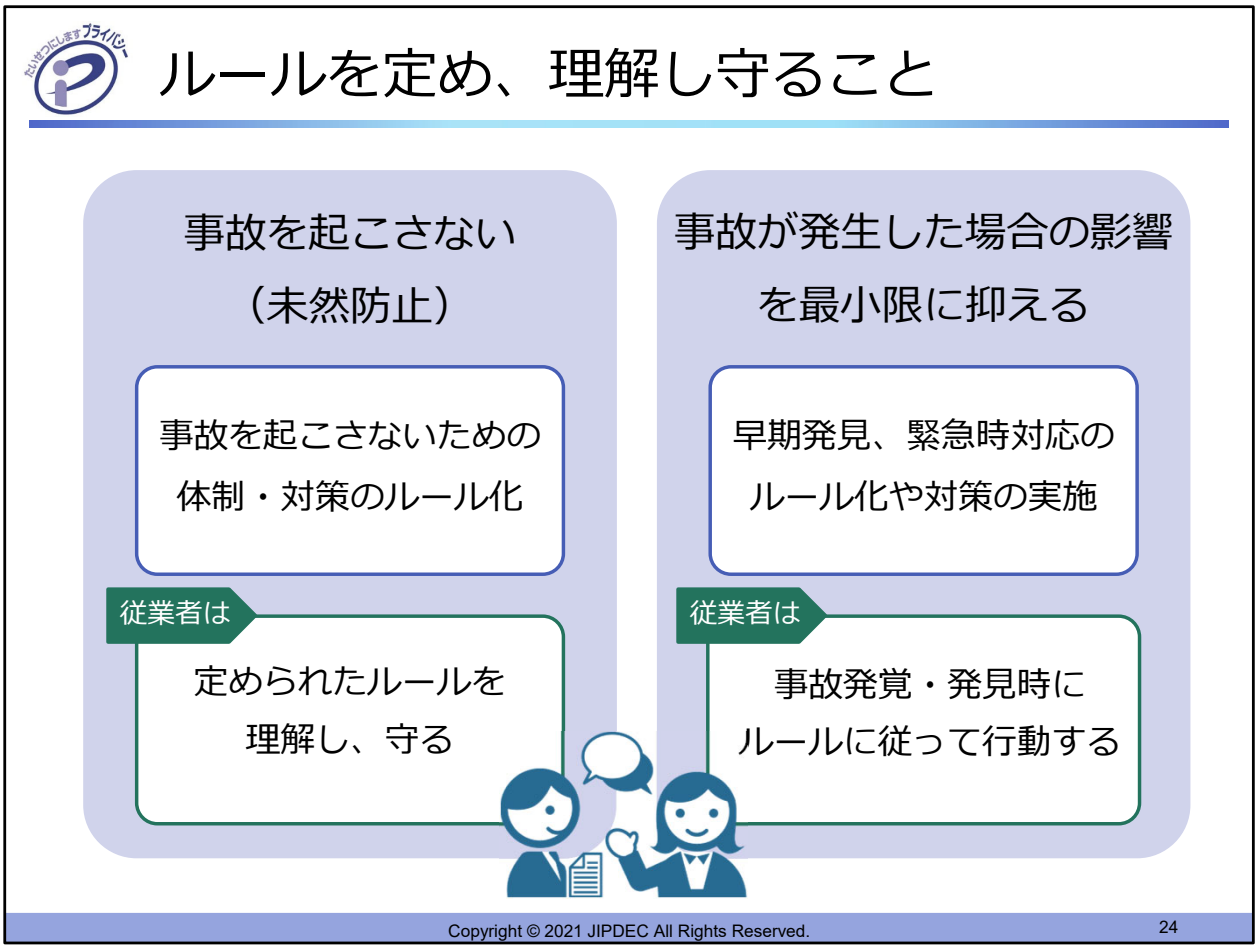


●事業者は、個人情報の取扱いに関するルールを定め運用することで、事故というリスクに備えます。

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



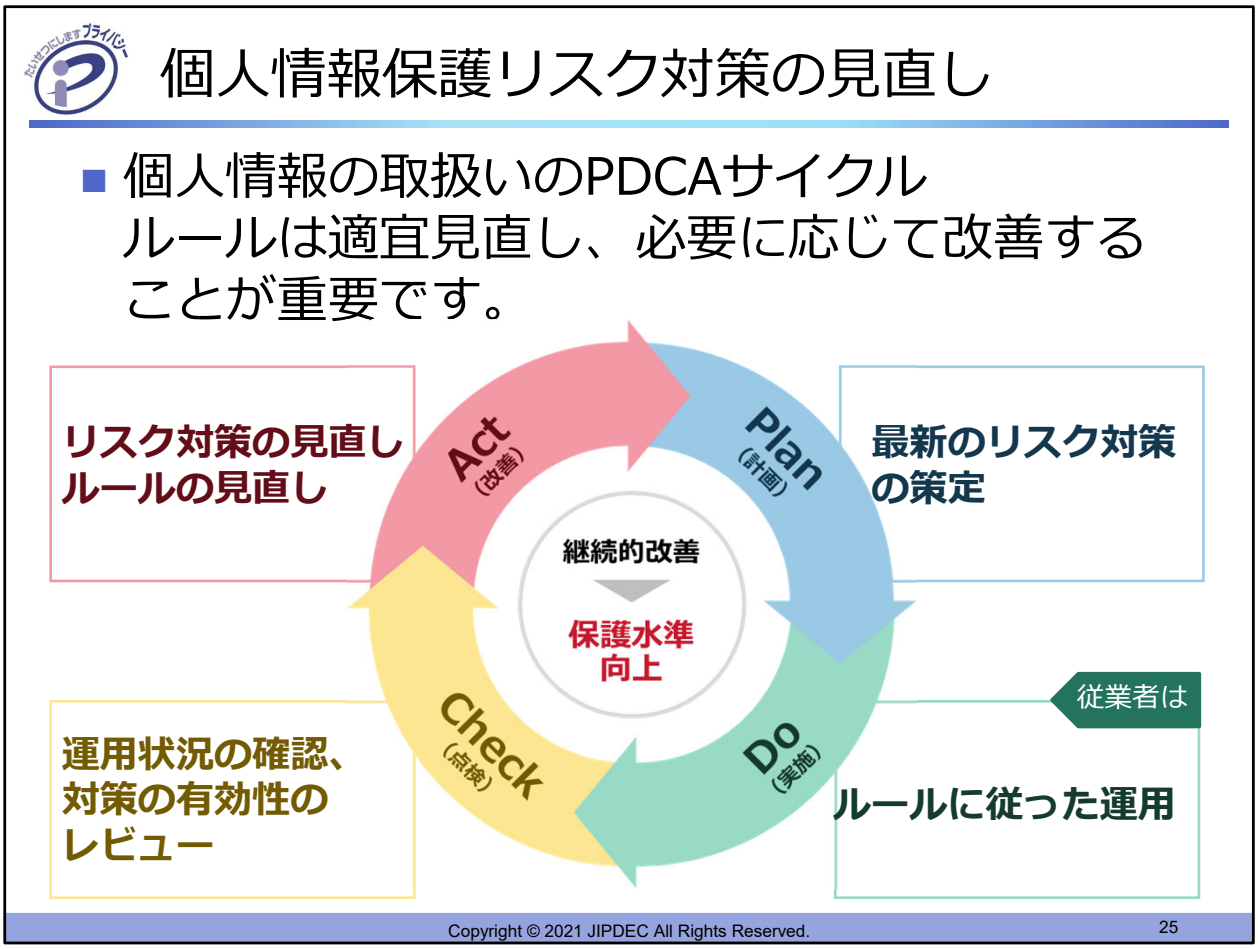
●事業者は、個人情報の取扱いに関するルールを定め運用することで、事故というリスクに備えます。

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。

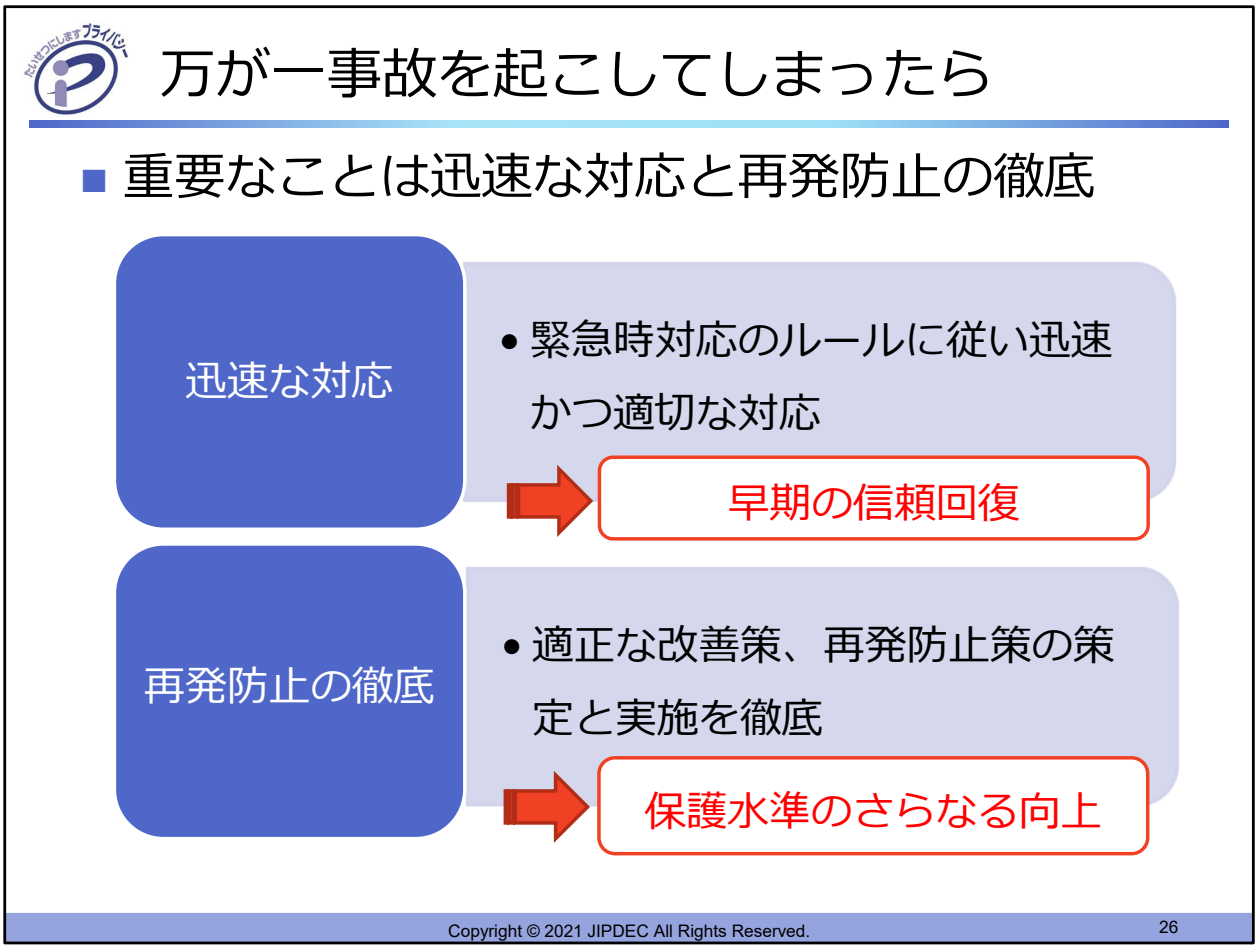


●プライバシーマーク制度では、個人情報の取扱いについてルールを定め、PDCAサイクルに沿った運用を実施することを求めています
（この研修もDo「実施」に当たります。）

★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。

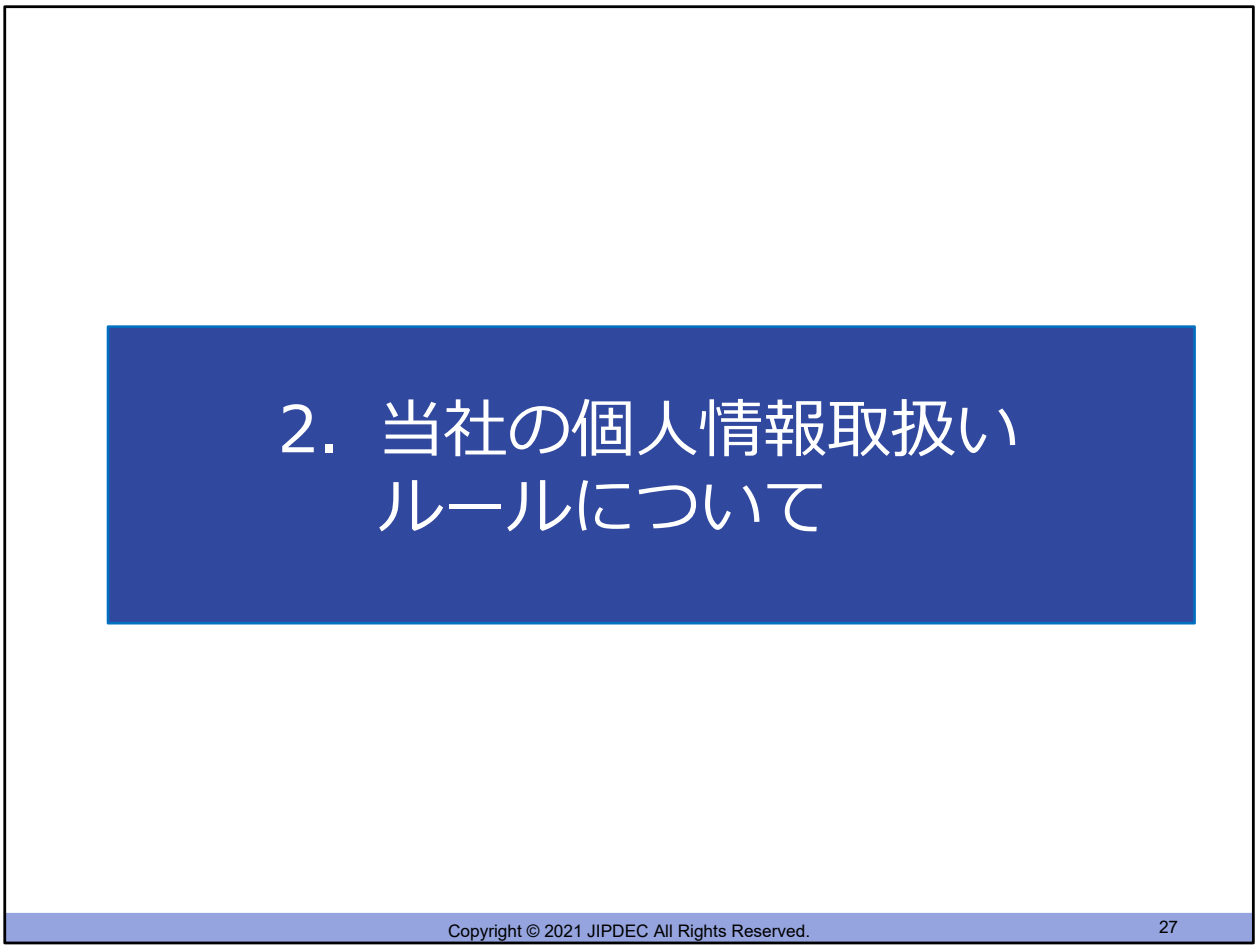


●最後に、万が一事故を起こしてしまったら。

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、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。

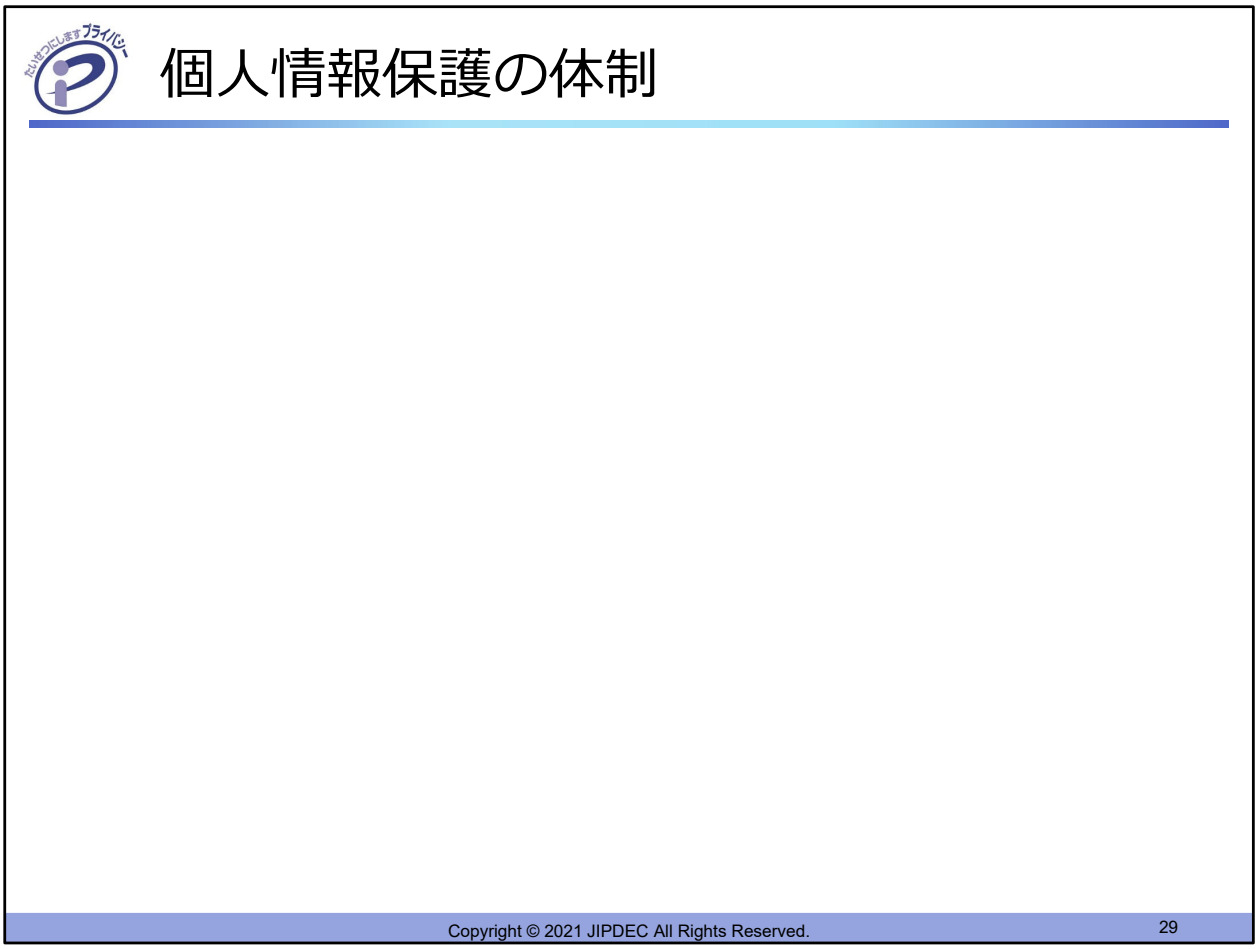
使用例：

自社が公表している個人情報保護方針の全文やWEBサイトへのリンクなどを記載します。

内容について、従業者が確認・理解することが必要です。

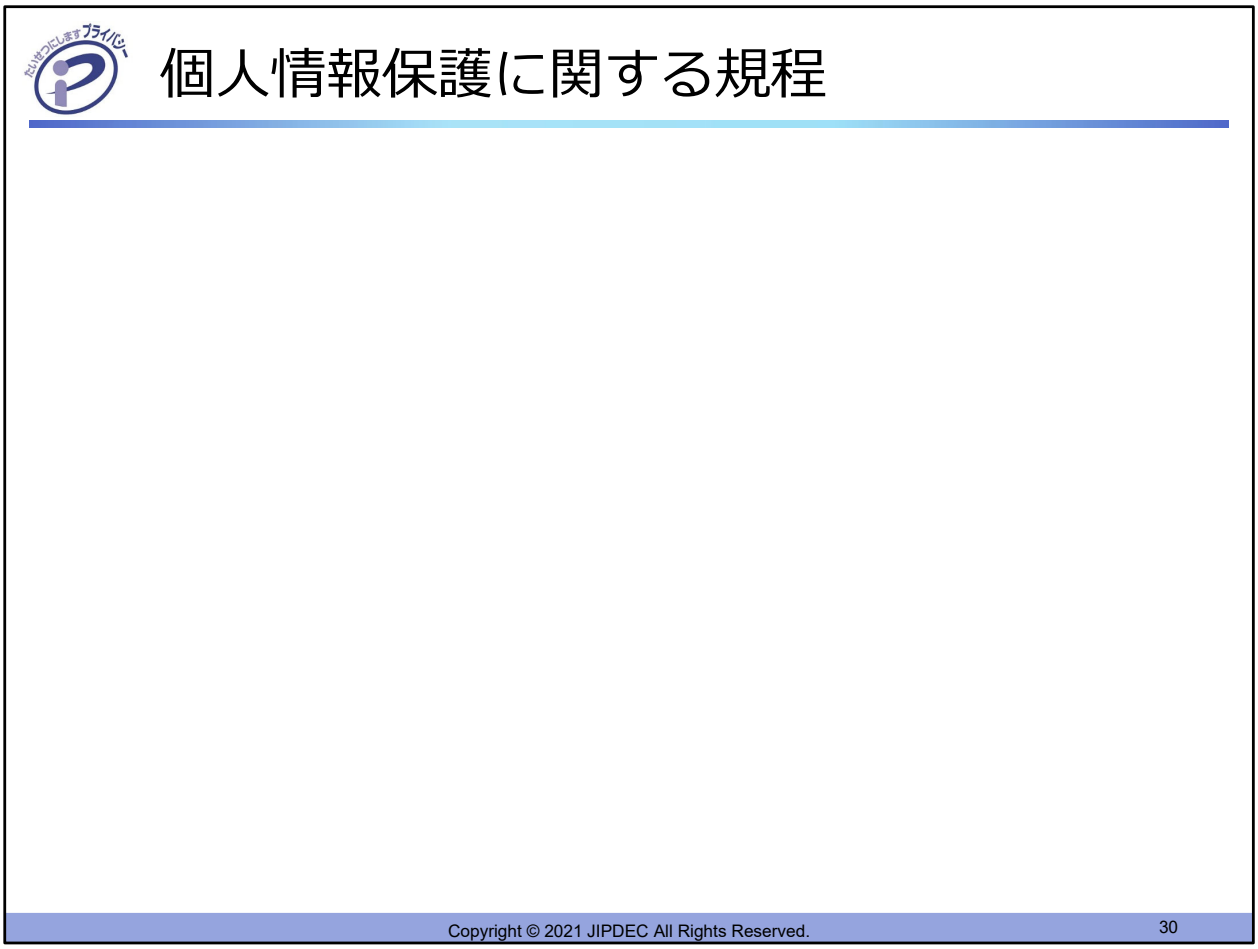
参考：

JIS Q 15001:2017では、外部向け個人情報保護方針と、内部向け個人情報保護方針について規程しています。



使用例：

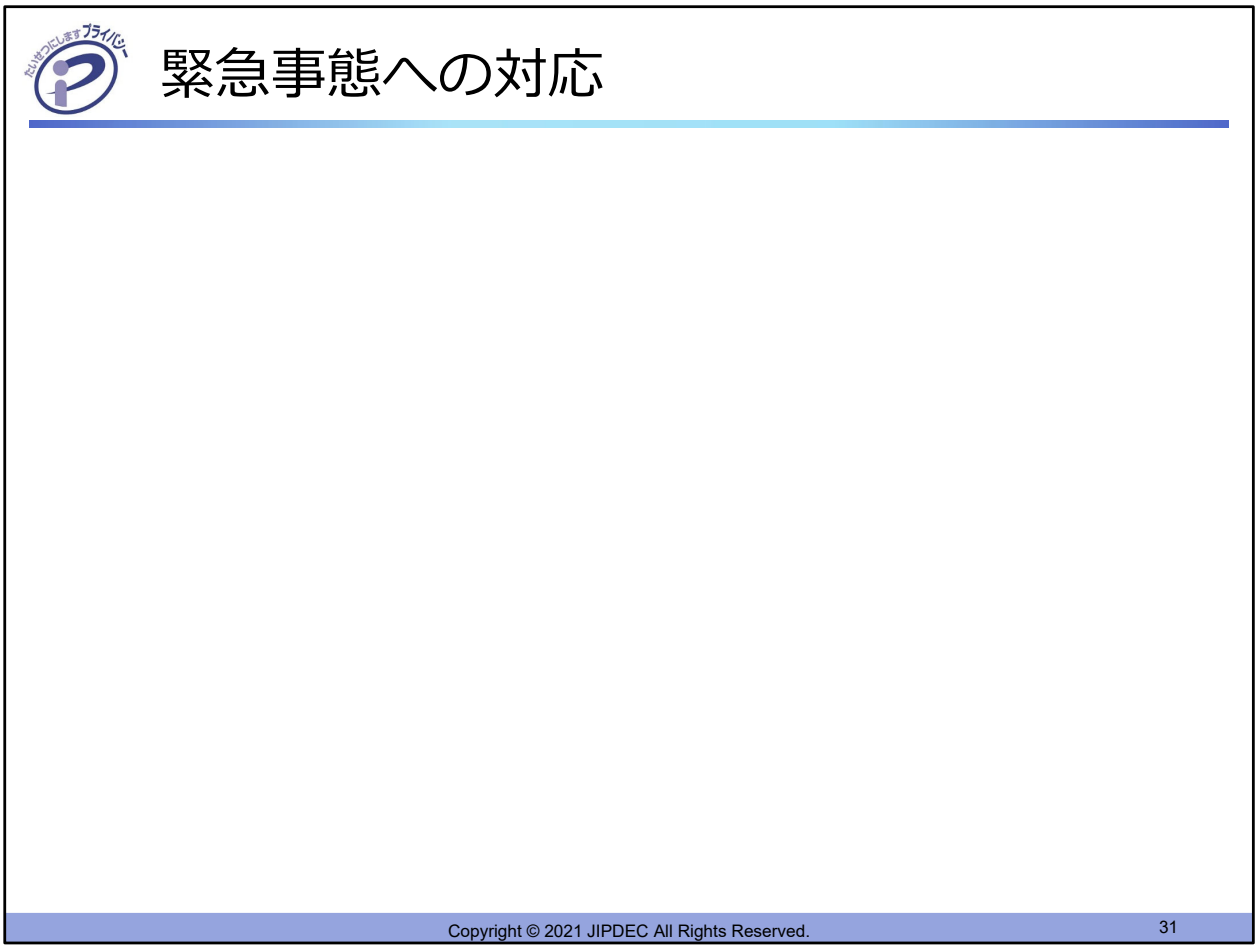
自社の個人情報保護の体制図や一覧などを記載します。



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。

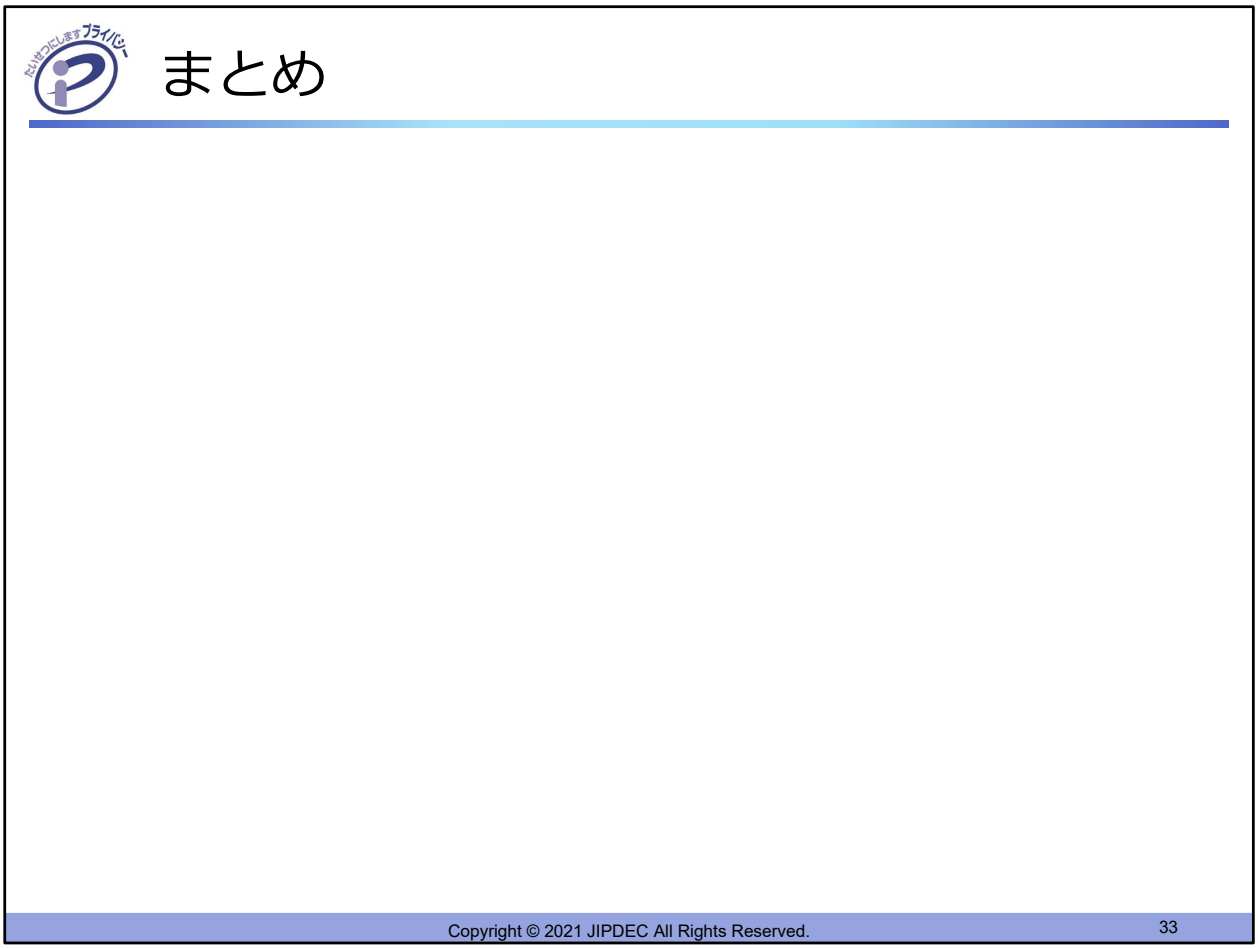
・個人情報が記載された書類等を送付する場合のルール
・メール等に添付、電子媒体で個人情報を送付する場合のルール
・個人情報を保管する場合のルール
・個人情報を削除する際のルール
・個人情報が記載された書類、PC等を持ち出す際のルール
・個人情報を委託する際のルール
など



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



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）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

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