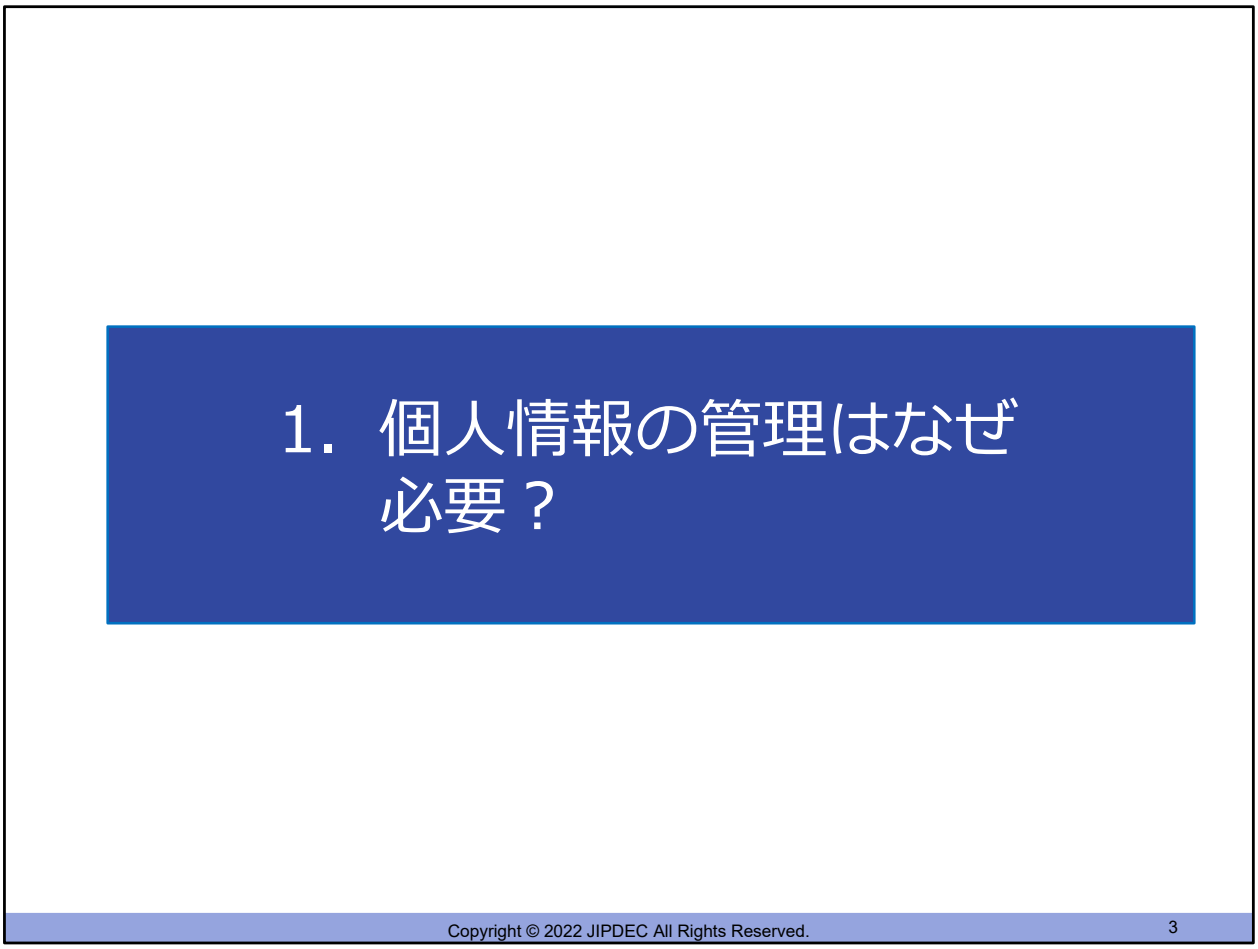
個人情報管理の重要性

2022年12月12日

JIPDEC

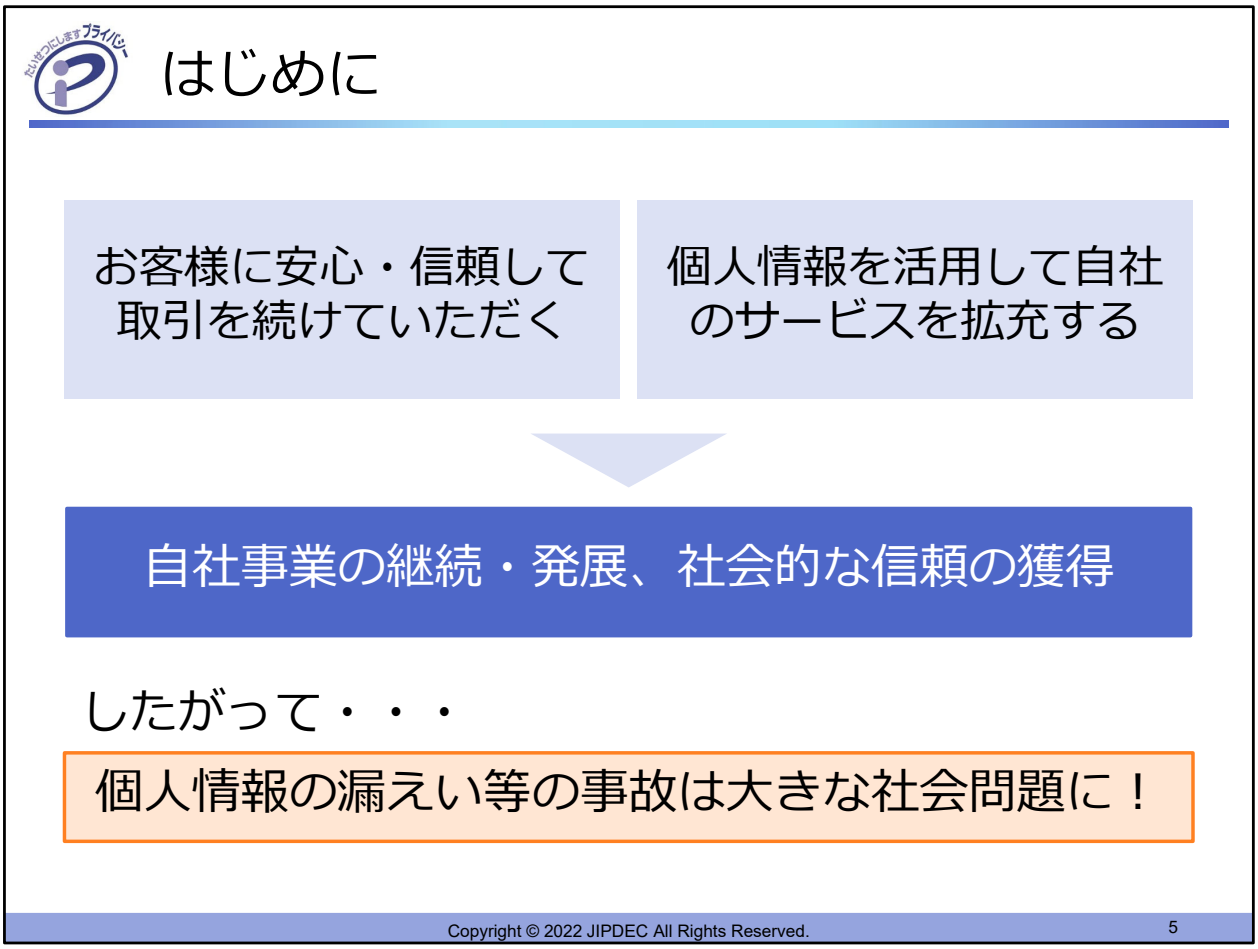
一般財団法人日本情報経済社会推進協会
プライバシーマーク推進センター

目次



●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

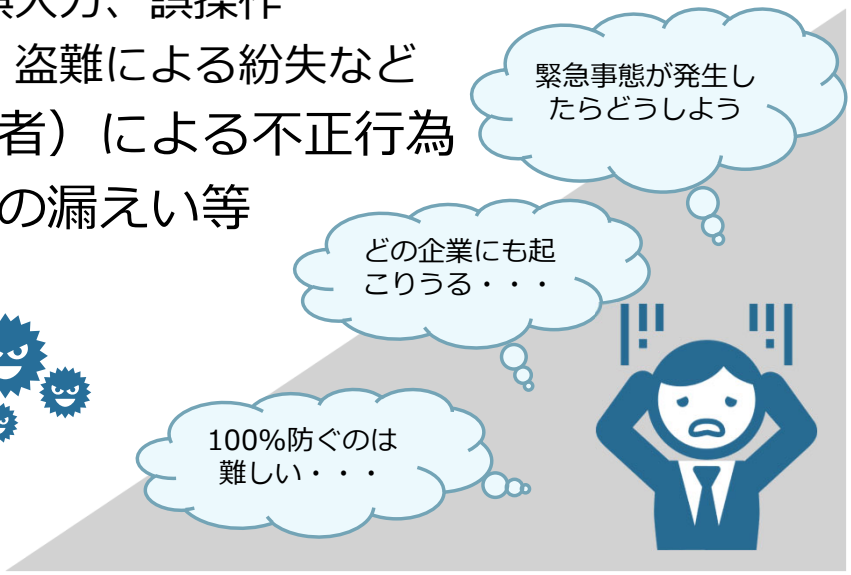
したがって、個人情報漏えい等の事故は、お客様等の関係者を巻き込んでの大きな社会問題になります。

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



■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
  2021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。

★2021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。

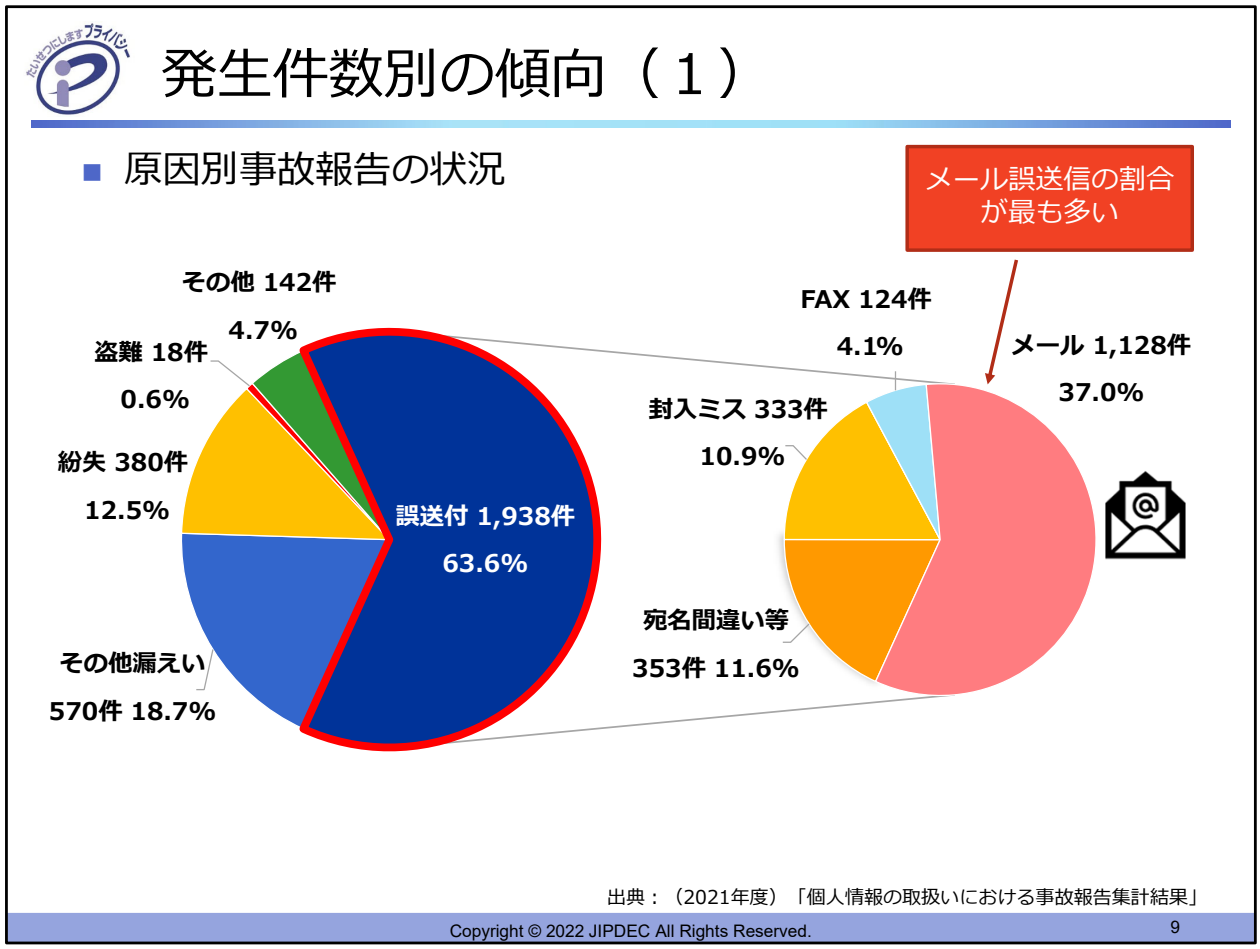
プライバシーマーク制度＞制度の案内＞参考情報

https://privacymark.jp/system/reference/pdf/2021JikoHoukoku_221007.pdf

2021年度の事故報告概要

- 発生件数別の傾向
  - 報告事業者数（1,045社）、報告件数（3,048件）ともに2020年度から増加。
  - 「誤送付」（1,938件：63.6%）が最も多く、次に「その他漏えい」（570件：18.7%）の順。
  - 「誤送付」のうち、「メール誤送信」（1,128件：37.0%）が最も多く、2020年度から約1.5倍に大きく増加。
  - 「その他漏えい」のうち、「プログラム/システム設計・作業ミス 」、「不正アクセス・不正ログイン」は2020年度から約２倍に大きく増加。
- 2021年度の報告傾向
  - 2020年度に続き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」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。

●2021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。



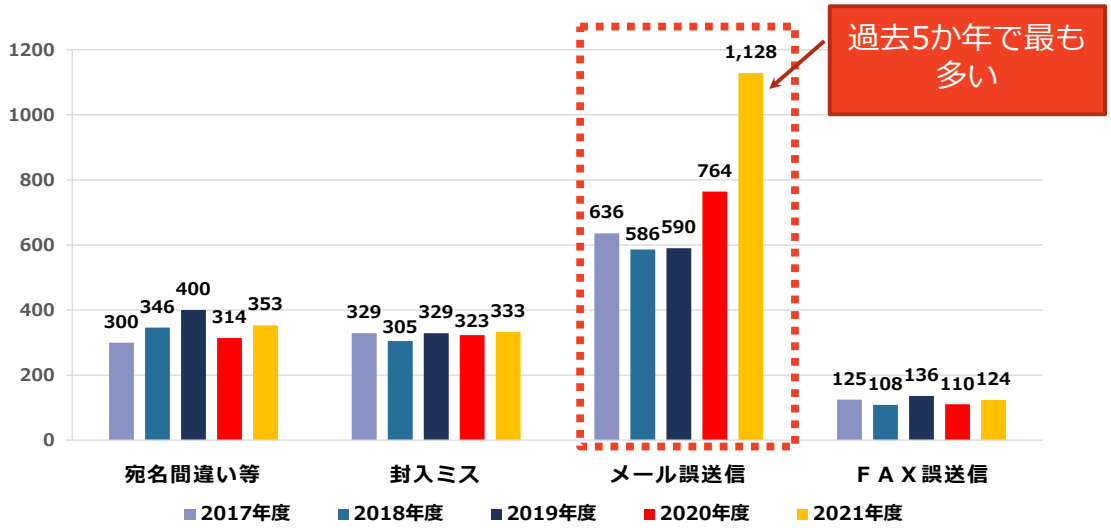
●2021年度の原因別事故報告の状況

2021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。（2020年度と傾向は同じ）

「誤送付」の内訳では、「メール誤送信」の1,128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、メッセージアプリ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。

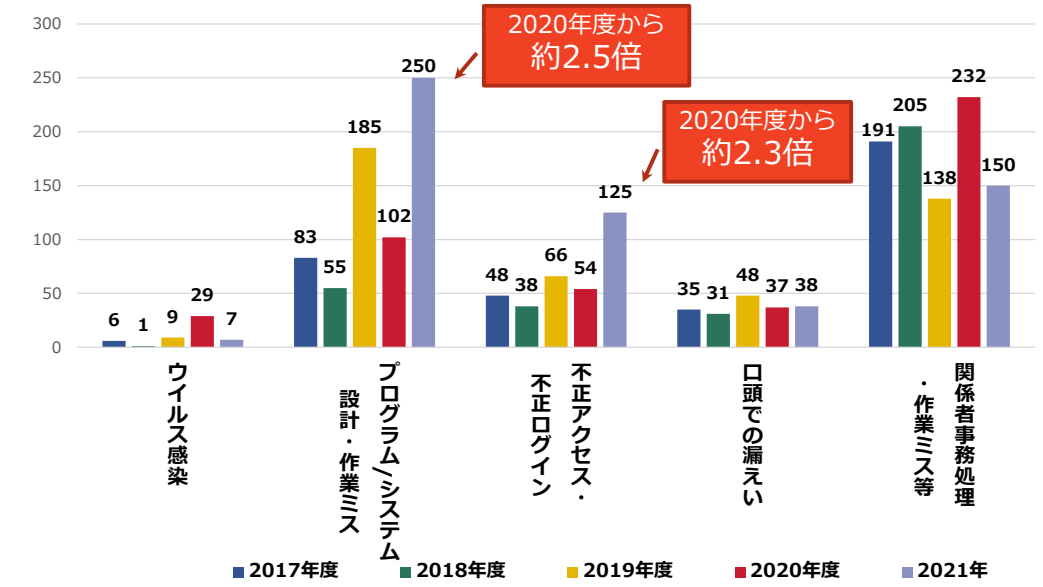
出典：（2021年度）「個人情報の取扱いにおける事故報告集計結果」

●原因別事故報告件数のうち「誤送付」の内訳推移

メール誤送信は過去５か年で最も多く、中にはメッセージアプリ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・連絡手段の変化が見られます。

発生件数別の傾向（３）

■ 「その他漏えい」の内訳推移



「プログラム/システム設計・作業ミス」と「不正アクセス・不正ログイン」はそれぞれ2020年度から大幅に増加した。

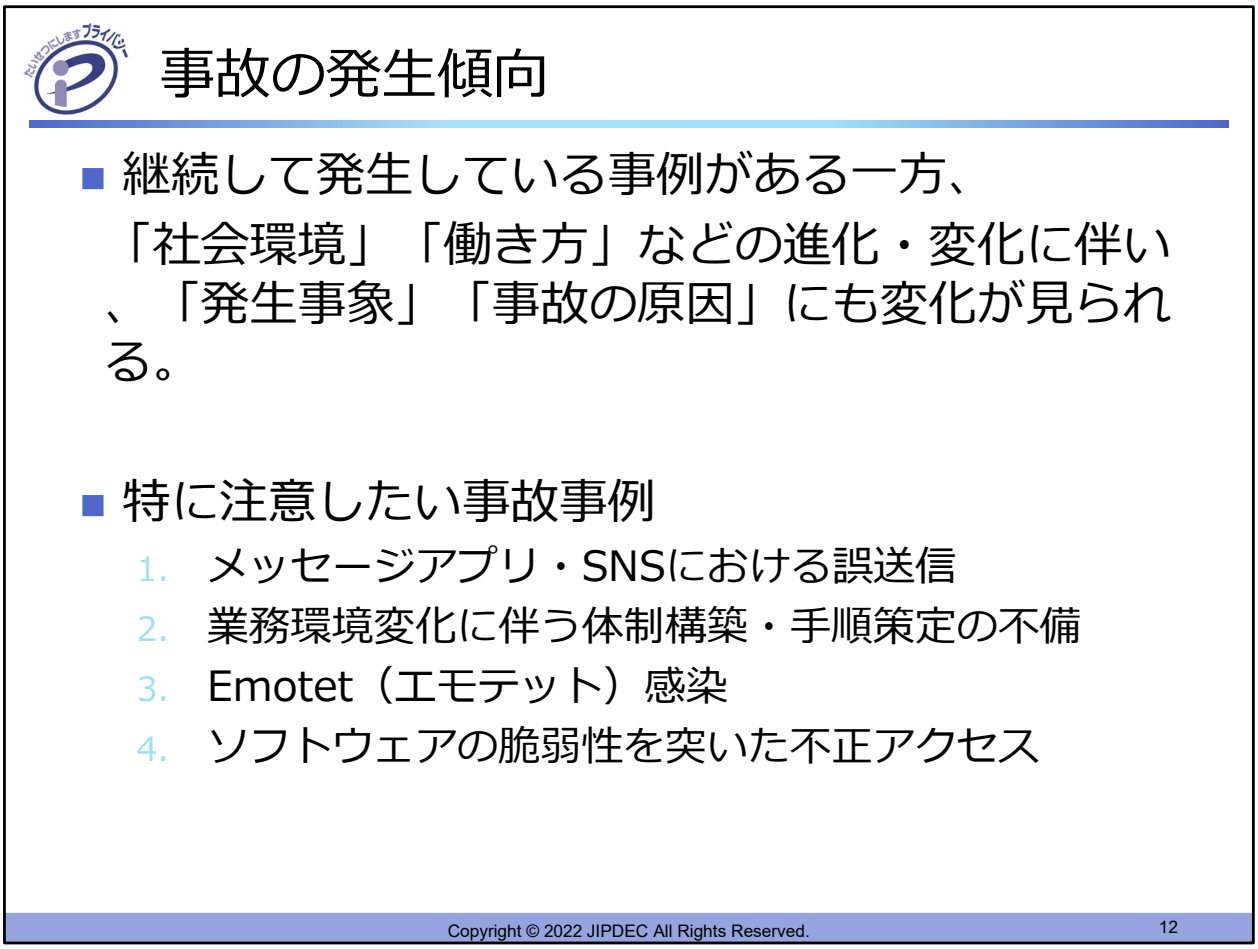
出典：（2021年度）「個人情報の取扱いにおける事故報告集計結果」

●原因別事故報告件数のうち「その他漏えい」の内訳件数

2020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」は減少したものの、「プログラム/システム設計・作業ミス（システムのバグを含む）」と「不正アクセス・不正ログイン」はそれぞれ昨年度から大幅に増加しました。

「プログラム/システム設計・作業ミス」が増加した背景には、新しいシステム導入の増加やテレワーク等により、いつもと異なる作業環境や手順の中で作業ミスが発生していること、

「不正アクセス・不正ログイン」が増加した背景には、2021年に開催された東京オリンピック・パラリンピックを目標とした攻撃が要因にあると考えられます。



●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、「社会環境」「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。

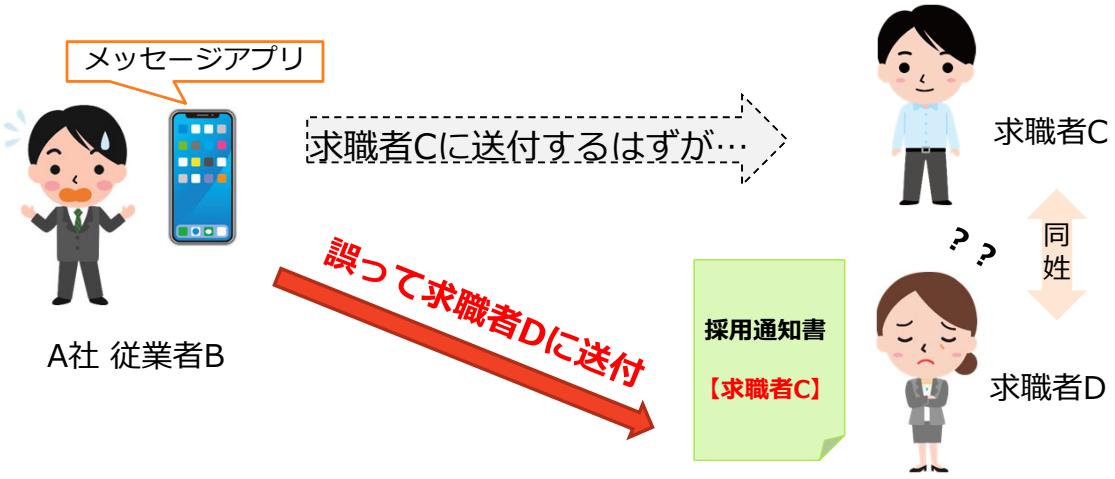
1. メッセージアプリ・SNSにおける誤送信
2. 業務環境変化に伴う体制構築・手順策定の不備
3. Emotet（エモテット）感染
4. ソフトウェアの脆弱性を突いた不正アクセス

次からはそれぞれ事例をもとに確認していきます。

特に注意したい事故事例（１）

1. メッセージアプリ・SNSにおける誤送信

A社は、採用活動において、求職者との連絡および電子ファイルのやり取りにスマートフォン用メッセージアプリの利用を始めた。
求職者Cへ採用通知を送信する際、操作に不慣れな担当者Bが誤って同じ姓の求職者Dに採用通知を送信してしまった。



●特に注意したい事故事例１：メッセージアプリ・SNSにおける誤送信

1990年代以前の電子的な連絡や情報伝達の方法は、電話やFAX、電子メールでのやり取りが中心でしたが、2000年代以降はメッセージアプリやSNS（ソーシャルネットワーキングサービス）でのコミュニケーションが生活に広く浸透しました。

その利用範囲はビジネスシーンにも広がり、組織内外を問わず様々な場面で利用されていますが、その急速な普及に伴い、事業者における事故件数も増加しています。

特に注意したい事故事例（１）

発生原因

- 担当者の送信先の選択ミス（氏名の姓のみで判断してしまった）。

＜その他の要因＞

- 新ツール利用開始後間もない時期
  - ルールの理解度や日々の利用による習熟度が上がらないとミスを起こしやすい。
- リスクに対する認識
  - メッセージアプリの利用は近年急速に普及。業務で取扱う情報の重要度を考慮せず、プライベートでの利用に近い感覚で利用してしまう恐れがある。

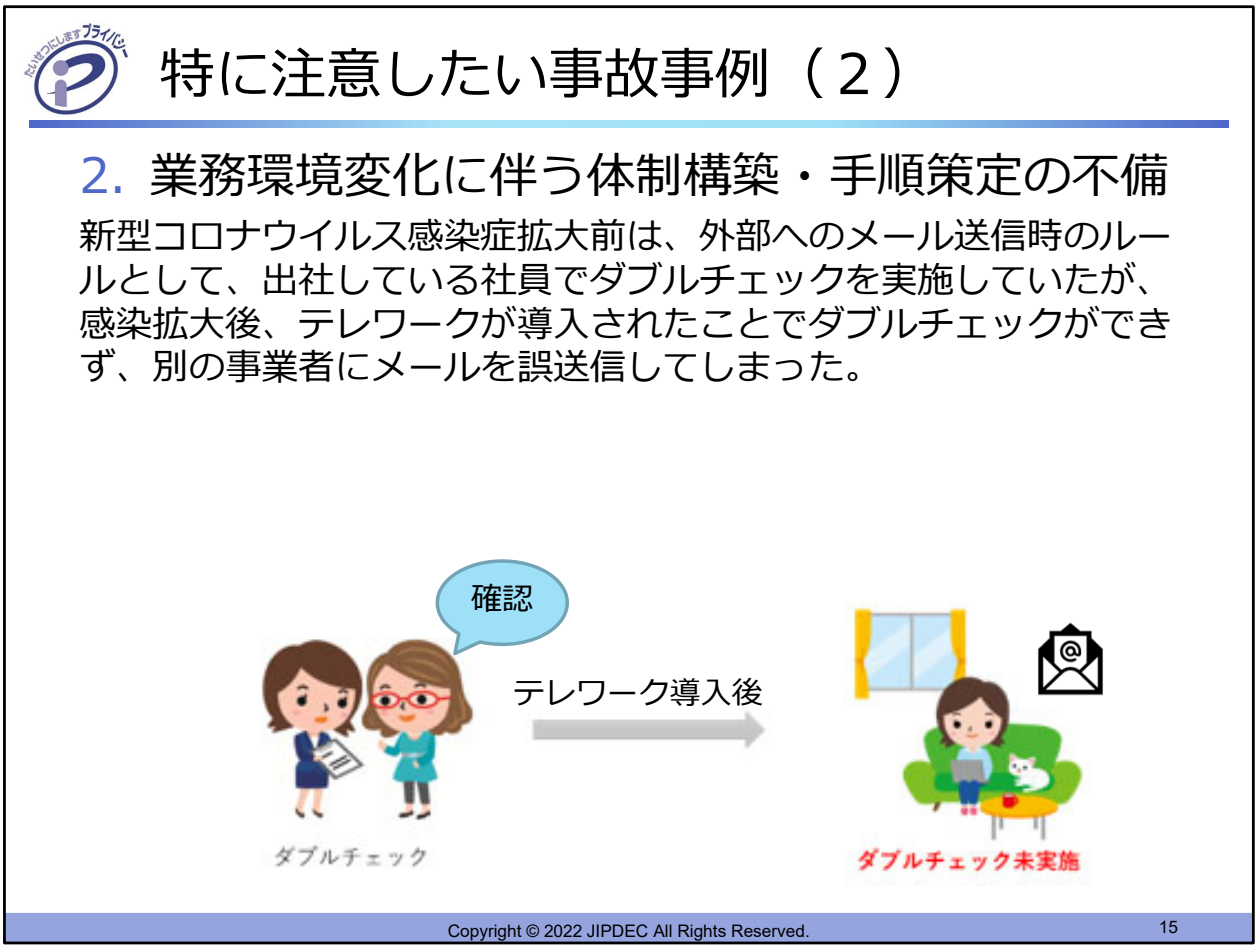
注意すべきこと

- 新たなツールを利用する際、業務手順が変更になった際は必ず社内のルールや手順を確認し、遵守しましょう。
- 業務においてメッセージアプリを利用する際は、取扱う情報の重要度を認識し、十分に留意した上で利用するようにしましょう。

●特に注意したい事故事例１：メッセージアプリ・SNSにおける誤送信

新たなツールの利用に伴い、社内ルールや業務手順が変更になることがあります。
従業員の皆さんは、最新のルールや手順書を確認し遵守しましょう。

★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



●特に注意したい事故事例２：業務環境変化に伴う体制構築・手順策定の不備

新型コロナウイルス感染症拡大や働き方改革、DXなどの影響により、近年、テレワークを導入する事業者が増加し、業務の電子化、ペーパレス化が進んでいます。
それに伴い、個人情報を取り扱う業務環境や作業内容・手順が変更になっていることが考えられます。

特に注意したい事故事例（２）

発生原因

- 担当者の送信先の選択ミス。

＜その他の要因＞

- 業務環境の変化
  - 新型コロナウイルス感染症の影響により、出社人数が制限されたオフィスや店舗で、複数人での送信前のダブルチェックが難しくなった。
- 手順策定の不備
  - 業務変化に伴うルールの整備が不十分であった。

注意すべきこと

- 業務環境が変わり、ルールや作業手順が変更になっていることがあります。テレワークをする際は必ず最新の社内ルールや手順書を確認し、遵守しましょう。
- 業務環境が変化しても、日々の業務において「事故防止の意識」をもちましょう。

●特に注意したい事故事例２：業務環境変化に伴う体制構築・手順策定の不備

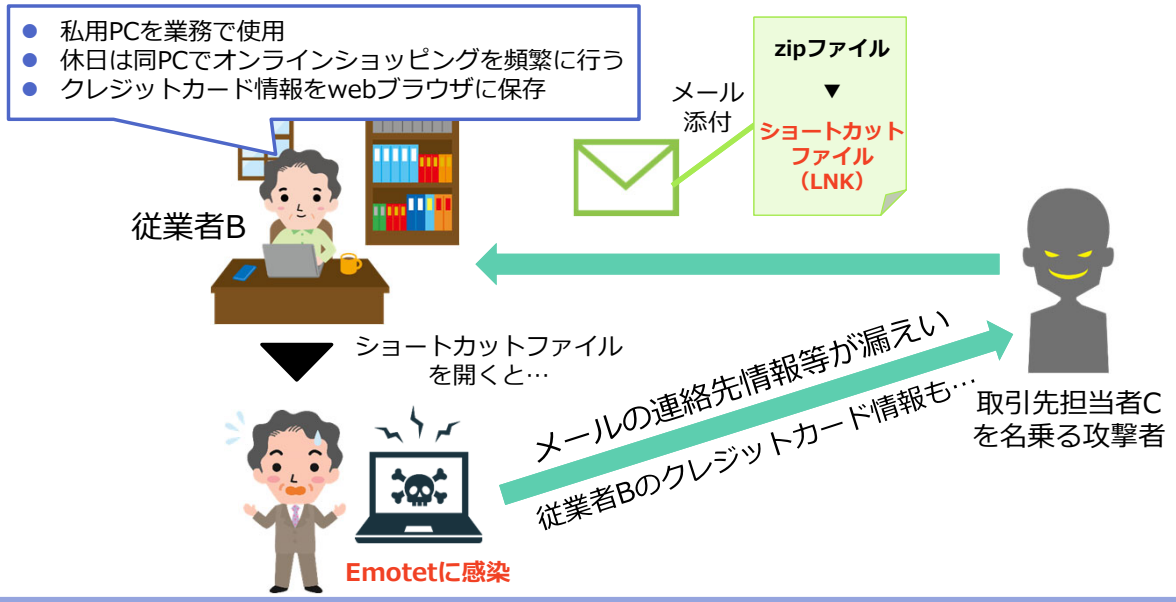
★テレワーク実施時に注意をしなければならない点については、
以下の公表資料もご参照ください。
⇒お役立ちツール＞社内教育用参考資料＞
　基本編：個人情報の取扱いに関する事故を起こさないために『テレワーク時に注意すべきこと』
　https://privacymark.jp/system/reference/index.html#tools

・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（３）

3. Emotet感染

A社の従業者Bが自宅にてテレワークを実施。社内承認を受けた私用PCにて業務を行っていたところ不審なメールを開きEmotetに感染した。



●特に注意したい事故事例３：Emotet感染

特に注意したい事故事例（３）

発生原因

- 従業者が不用意に攻撃メールを閲覧し、不正ファイルを開いてしまった。

＜その他の要因＞

- 従業者への教育
  - 添付ファイルを開く上で確認すべきポイントや不審なメールを受信した際の対処方法の周知が十分に行われていなかったことが想定される。

注意すべきこと

- Emotetの攻撃手法は、主にメールです。
  - 身に覚えのないメールの添付ファイルは開かない。
  - メール本文中のURLリンクはクリックしない。
  - OSやアプリケーション、セキュリティソフトを常に最新の状態にする。
- 不審なメールへの対応ルールや、万一感染してしまった場合に備えて緊急事態への対応手順を確認しておきましょう。
- Emotetの攻撃は巧妙なため、関係各所が発出している注意喚起から攻撃の特徴を確認するなどして備えましょう。

●特に注意したい事故事例３：Emotet感染

Emotetは、情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大が試みられています。
一時は終息に向かったと思われましたが、2021年の11月頃から攻撃活動が再開し、多くの被害が発生しています。

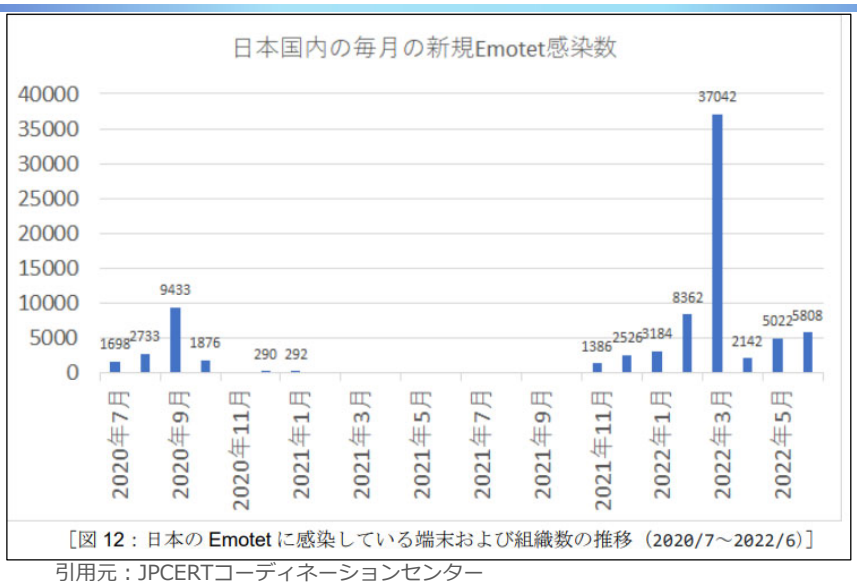
Emotet感染に関するJIPDECプライバシーマーク推進センターへの個人情報の取扱いに関する事故報告も増加しており、引き続き警戒が必要な状況です。

・JIPDEC　プライバシーマーク推進センター
【再掲_注意喚起】マルウェアEmotetの感染について
https://privacymark.jp/news/system/2020/1016.html

★Emotetへの注意喚起や情報提供が、以下のサイトで発信されていますので参考にしてください。
参考サイト：一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
「マルウェアEmotetの感染再拡大に関する注意喚起」
https://www.jpcert.or.jp/at/2022/at220006.html

参考サイト：独立行政法人情報処理推進機構（IPA）
「「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて」
https://www.ipa.go.jp/security/announce/20191202.html

（参考）Emotetの被害状況



［図 12：日本の Emotet に感染している端末および組織数の推移（2020/7～2022/6）］

引用元：JPCERTコーディネーションセンター
JPCERT/CC インシデント報告対応レポート［2022年4月1日～2022年6月30日］
https://www.jpcert.or.jp/pr/2022/IR_Report2022Q1.pdf

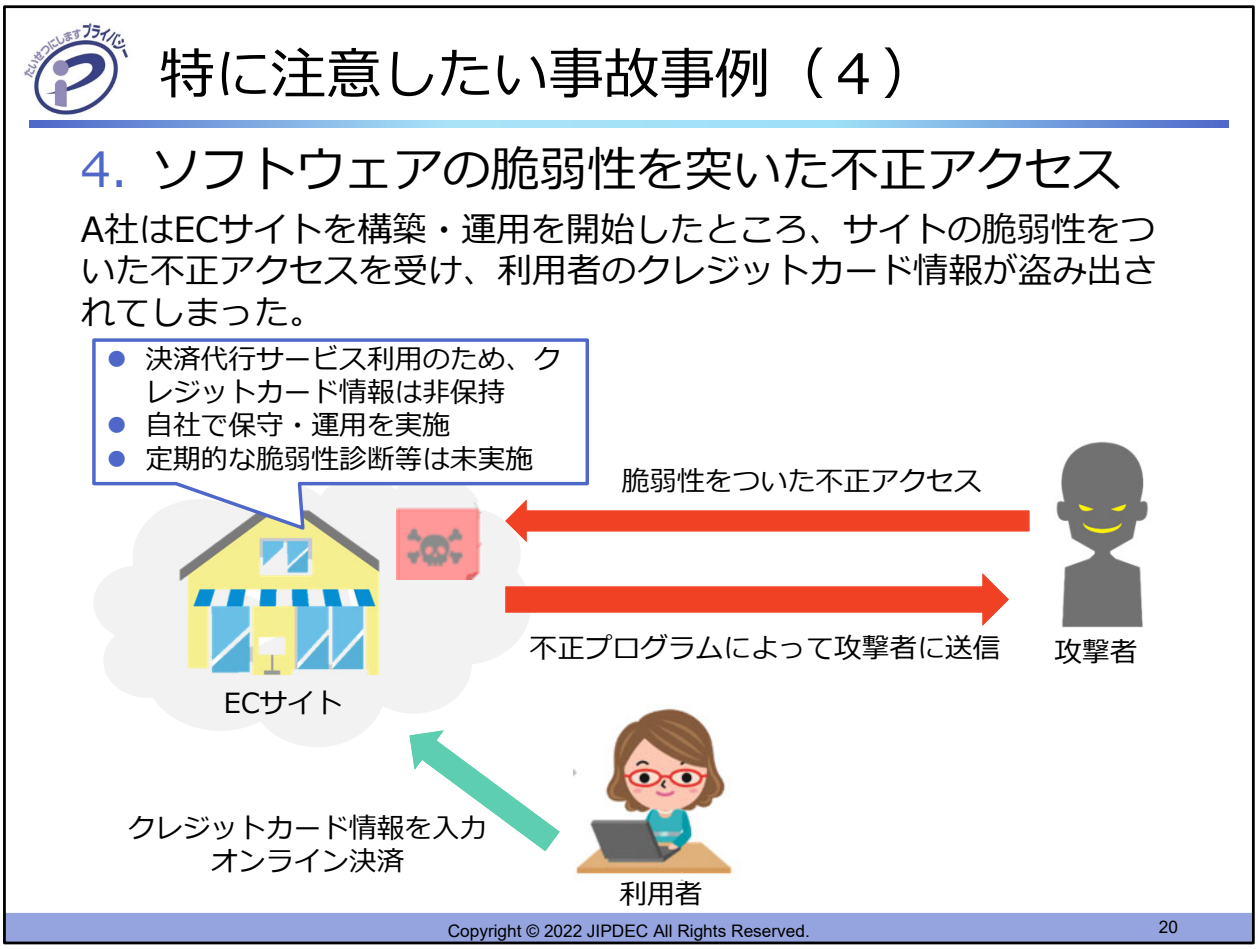
2021年11月から攻撃活動が再開し多くの被害が発生。その攻撃手法も多様化。
2022年7月中旬よりEmotetの感染に至るメールは国内では観測されていなかったが、2022年11月より再開したことが観測され、被害が発生している。

●Emotetの被害状況

2019年11月末頃から多くのメディアで取り上げられ、広く知れ渡った「Emotet」は攻撃の再開と休止を繰り返しています。

特に2021年の11月頃から再開された攻撃では、多くの被害が発生し、その攻撃手法も多様化しました。

2022年7月中旬よりEmotetの感染に至るメールは国内では観測されていませんでしたが、2022年11月より再開したことが観測されています。



●特に注意したい事故事例４：ソフトウェアの脆弱性を突いた不正アクセス

不正アクセスによる個人情報の事故報告が急増しています。

特に、クレジットカード情報など、財産的被害が発生する恐れがある情報を取り扱うECサイトにおいて事故等が多く発生している状況です。

特に注意したい事故事例（４）

発生原因

- ECサイトにおける脆弱性への対応が十分に実施されていなかった。
- 決済代行会社を利用しており自社のシステム内ではクレジットカード情報を保持しないため、クレジットカード情報の漏えいはないと安心していた。

注意すべきこと

- クレジットカード情報を狙ったwebサイトへの不正アクセスの攻撃手法は日々変化しています。
  サイトの脆弱性、セキュリティ対策を定期的に確認するようにしましょう。
  システム担当者に任せきりにするのではなく、日頃から最新の攻撃手法やセキュリティ情報の収集、知識習得に努めましょう。
- サイト構築・運用を外部委託する場合は、必要なセキュリティ対策が実施されるよう具体的に指示し、実施状況を定期的に確認しましょう。

●特に注意したい事故事例４：ソフトウェアの脆弱性を突いた不正アクセス

ECサイトを構築・運営する際は、サイトに係る脆弱性を把握し、セキュリティパッチを当てたり、ソフトウェアを更新したりすることが必要です。

事業者には、そうした脆弱性情報を収集・対応するための手順を策定し、体制を構築することが求められますが、従業者個人としても、日頃からセキュリティ情報を収集するなど、セキュリティ意識の向上に努めましょう。

参考サイト：JIPDEC　プライバシーマーク制度ホームページ

「【注意喚起】ECサイトにおける個人情報の漏えい（クレジットカード情報等）事故が増えています」

https://privacymark.jp/news/system/2022/1012.html

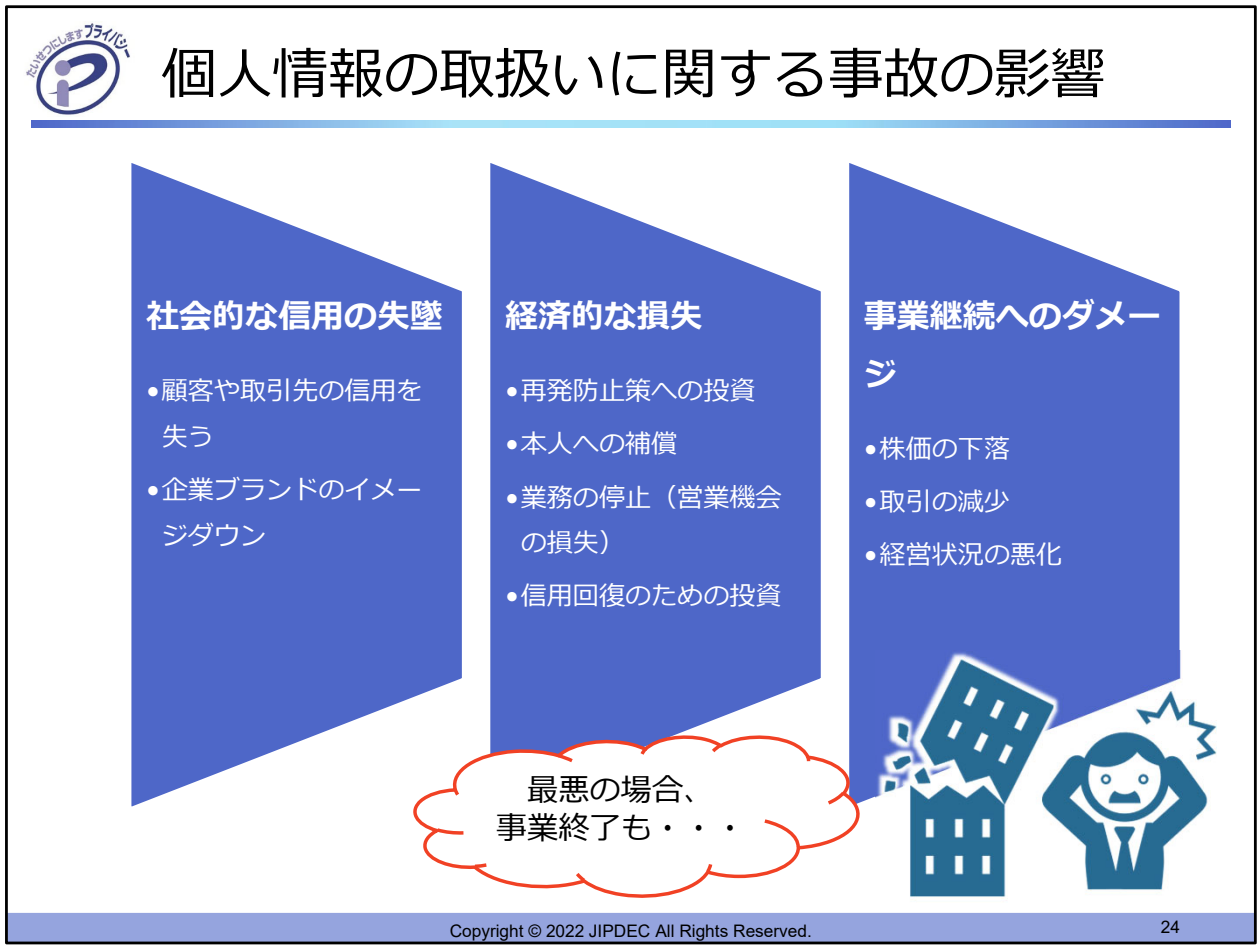
- 個人情報の取扱いに関する事故の影響

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



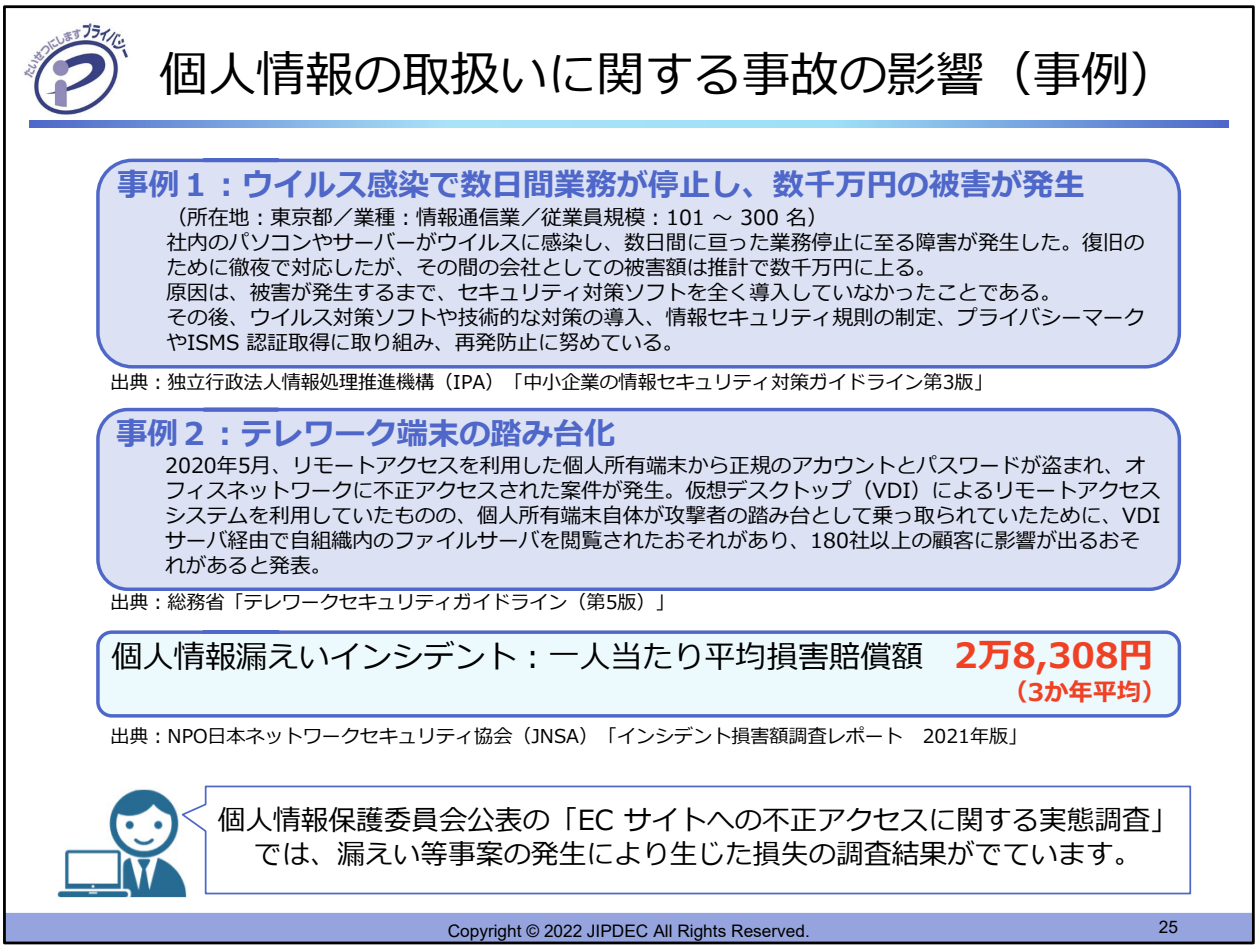
●個人情報の取扱いに関する事故の影響

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

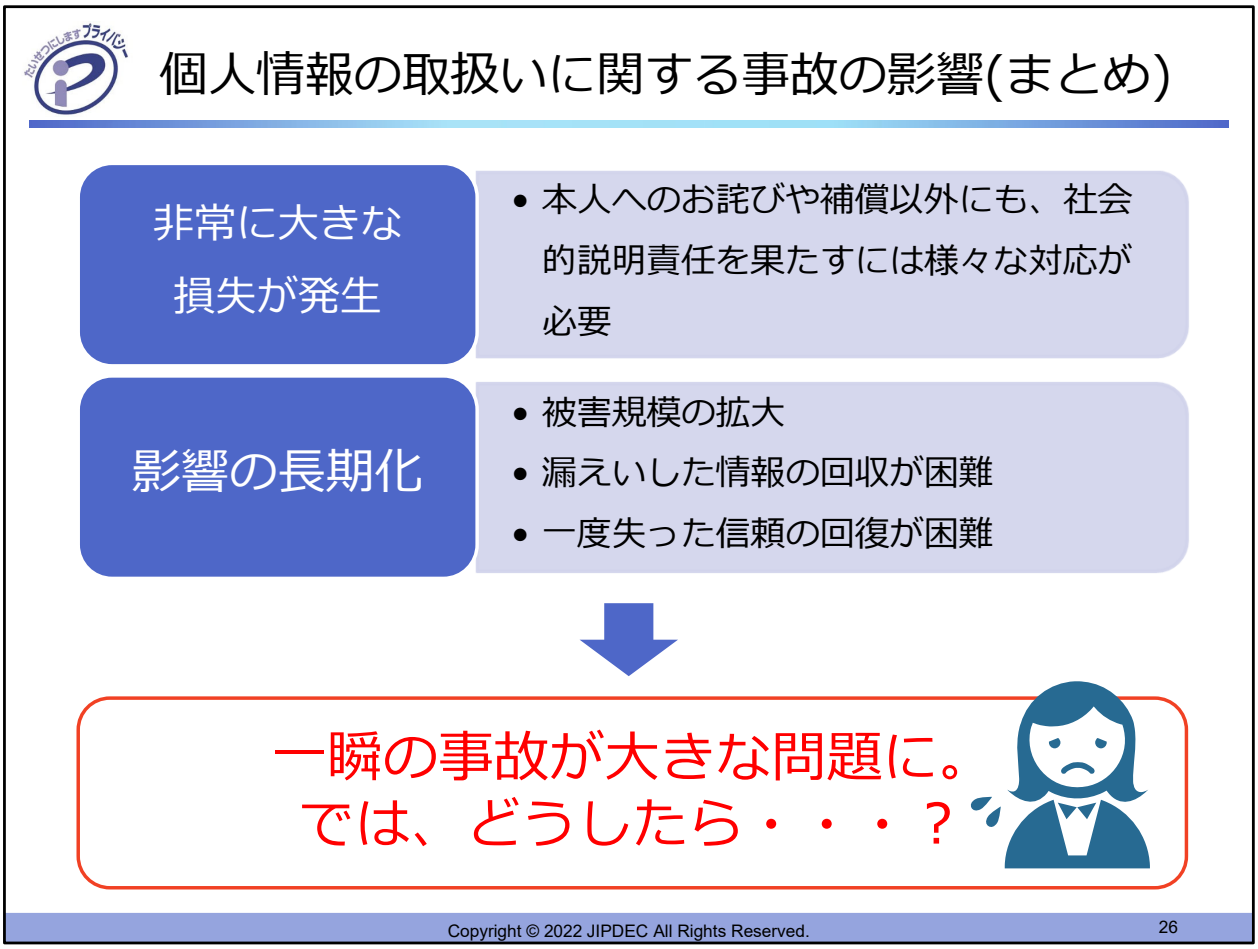
・NPO日本ネットワークセキュリティ協会（JNSA）「インシデント損害額調査レポート　2021年版」

https://www.jnsa.org/result/2021.html

・個人情報保護委員会「EC サイトへの不正アクセスに関する実態調査」

https://www.ppc.go.jp/files/pdf/ecsite_report.pdf

●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。

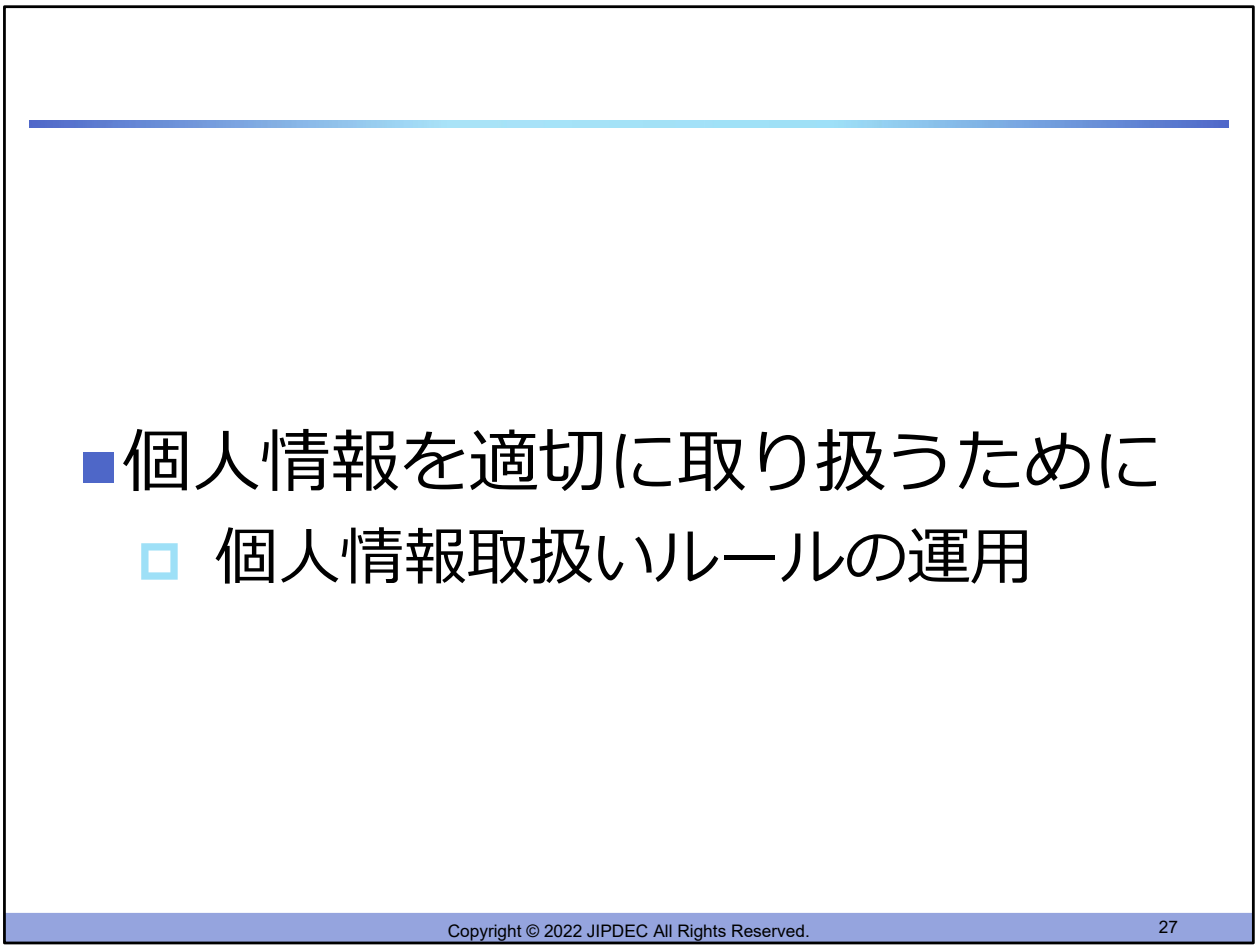


●個人情報の取扱いに関する事故の影響は、金銭的な負担のほか、社会的な信用の失墜など非常に大きな損失が生じます。

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。

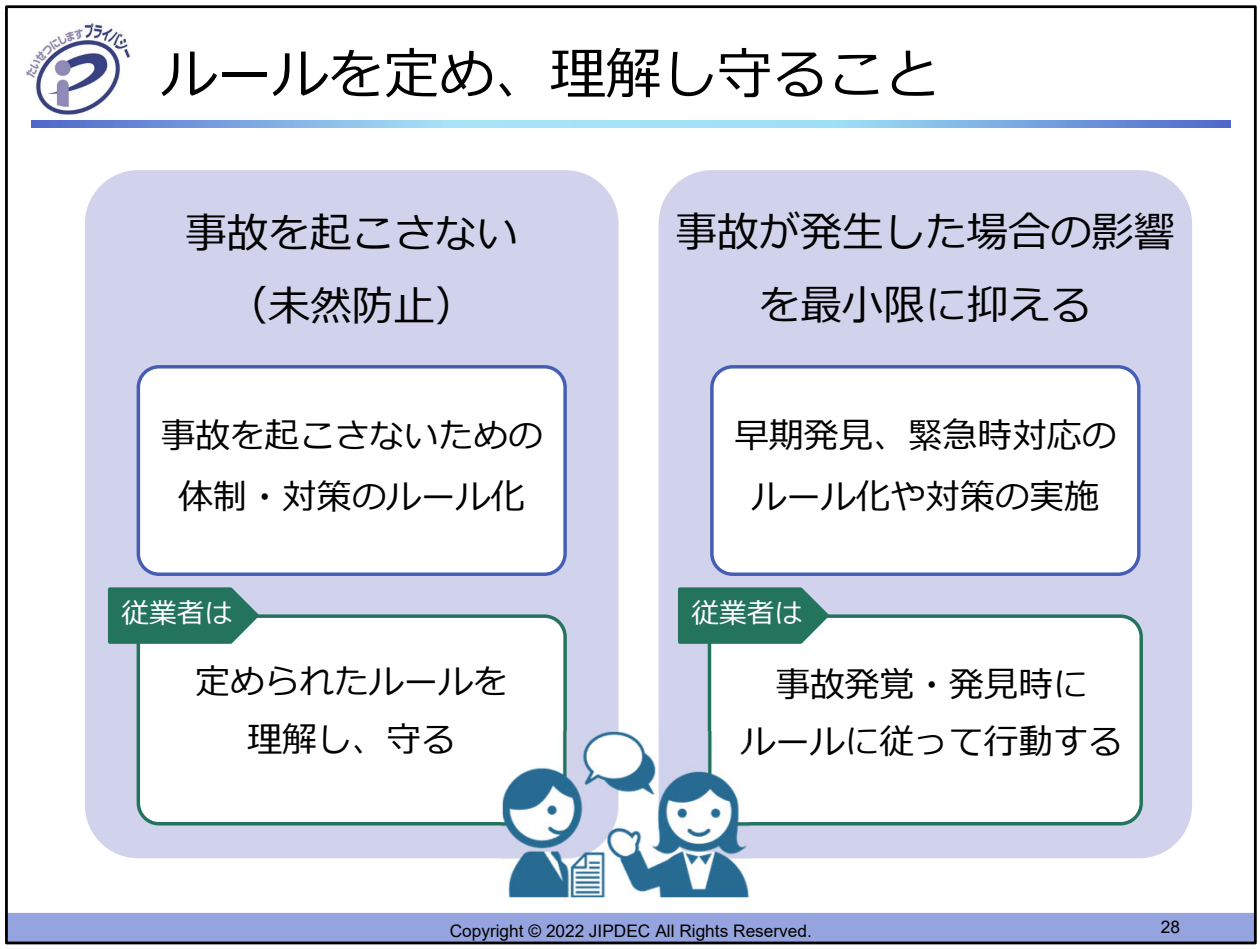


●事業者は、個人情報の取扱いに関するルールを定め運用することで、事故というリスクに備えます。

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



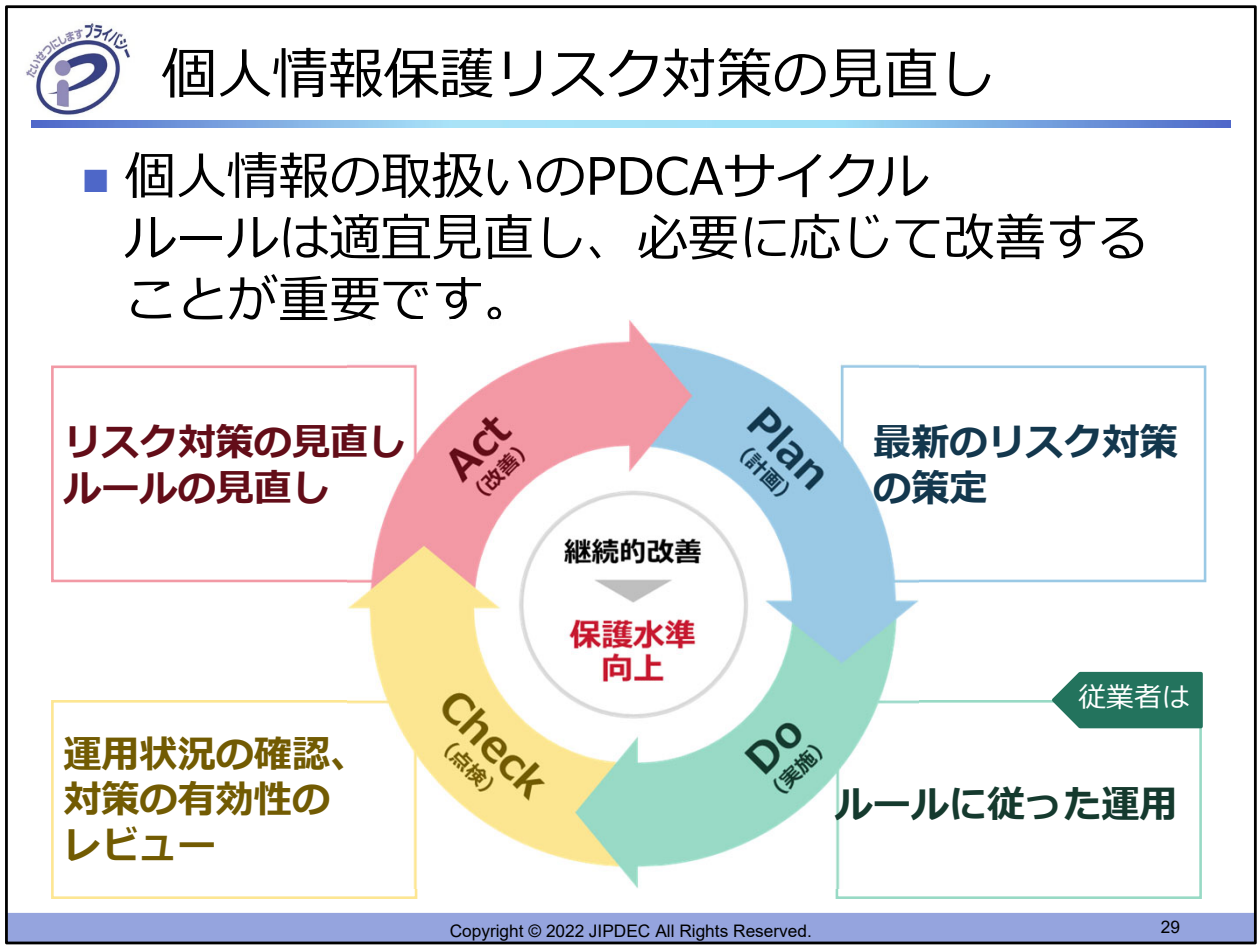
●事業者は、個人情報の取扱いに関するルールを定め運用することで、事故というリスクに備えます。

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。

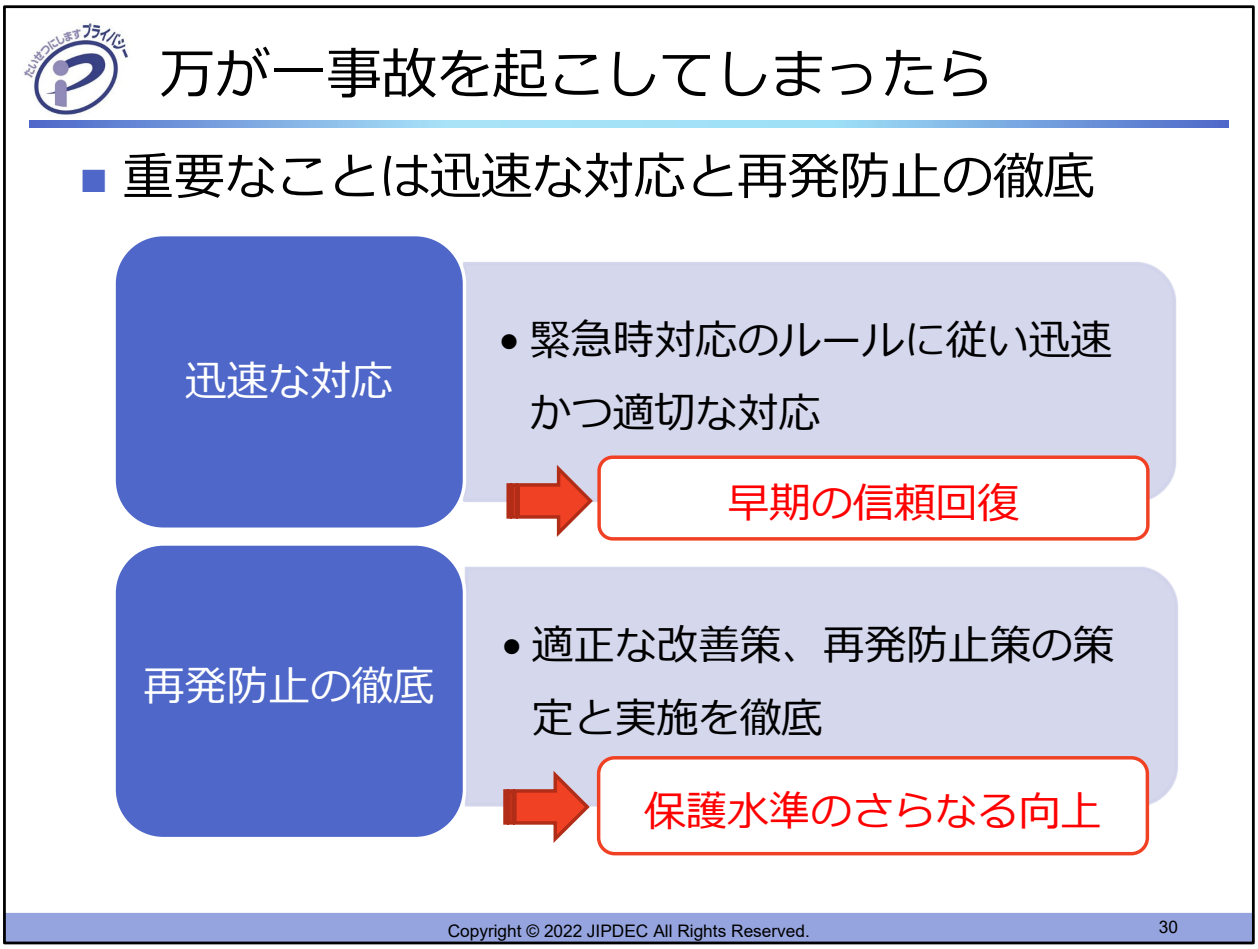


●プライバシーマーク制度では、個人情報の取扱いについてルールを定め、PDCAサイクルに沿った運用を実施することを求めています
（この研修もDo「実施」に当たります。）

★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。

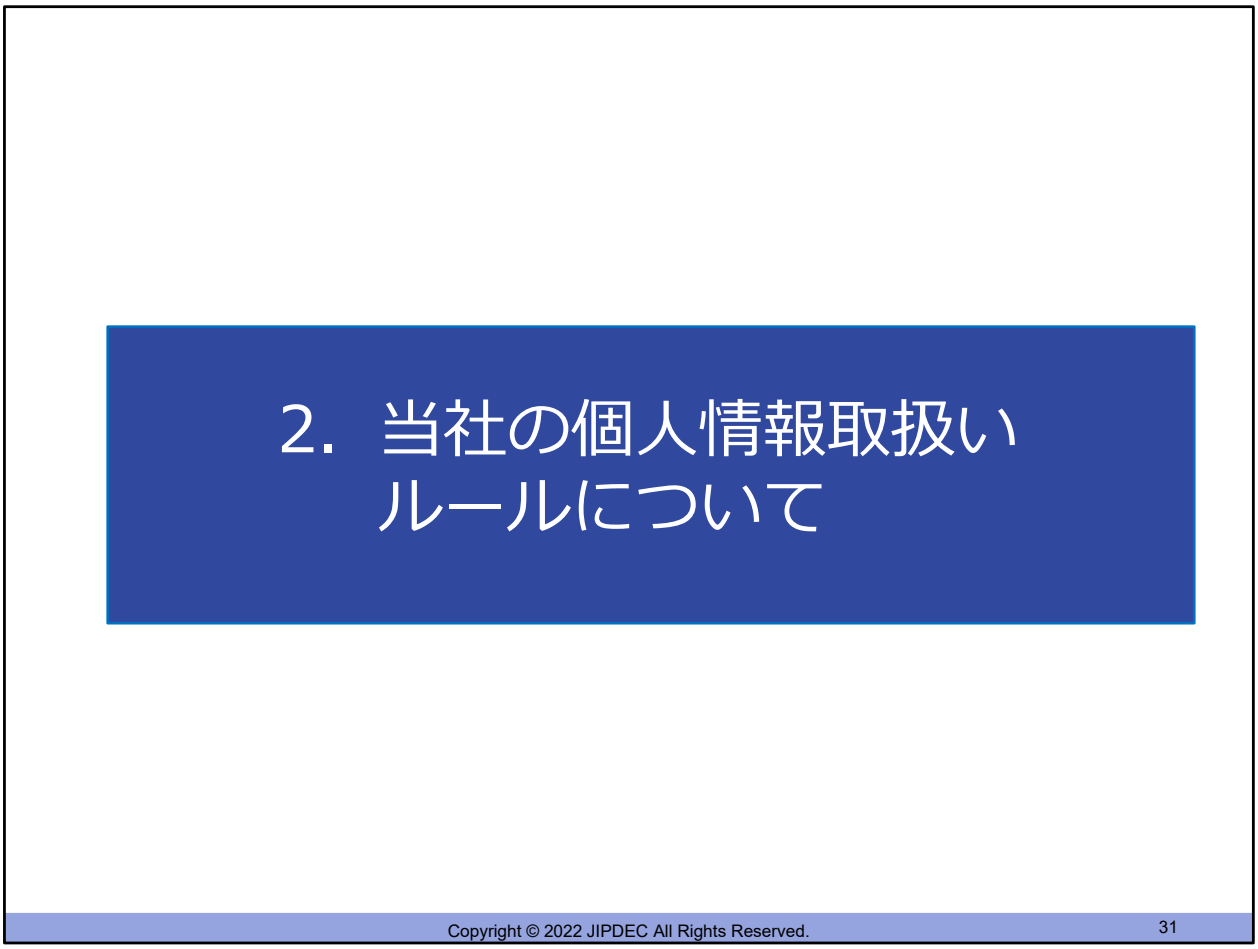


●最後に、万が一事故を起こしてしまったら。

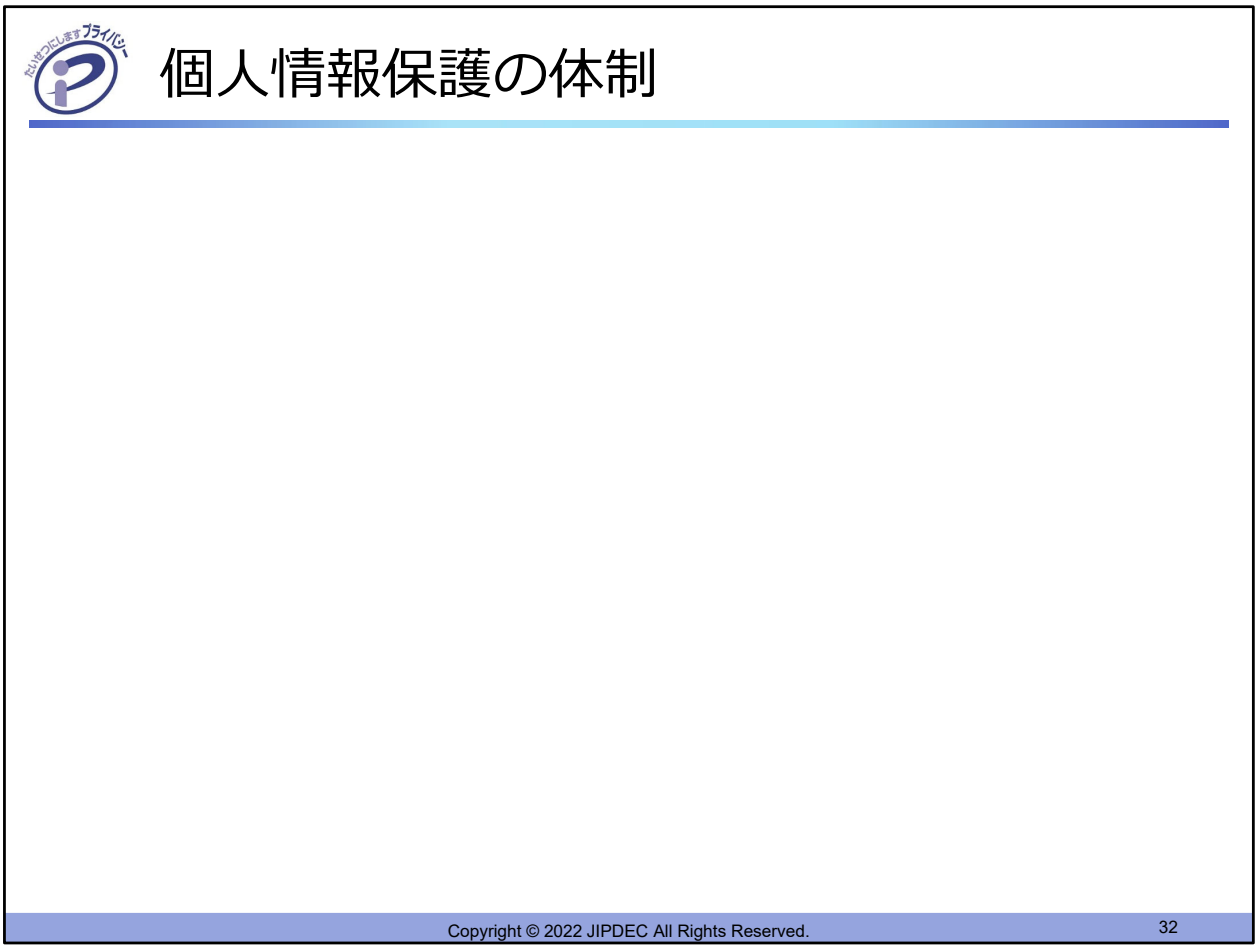
緊急事態への対応ルールに従い、迅速に対応することが重要です。

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。

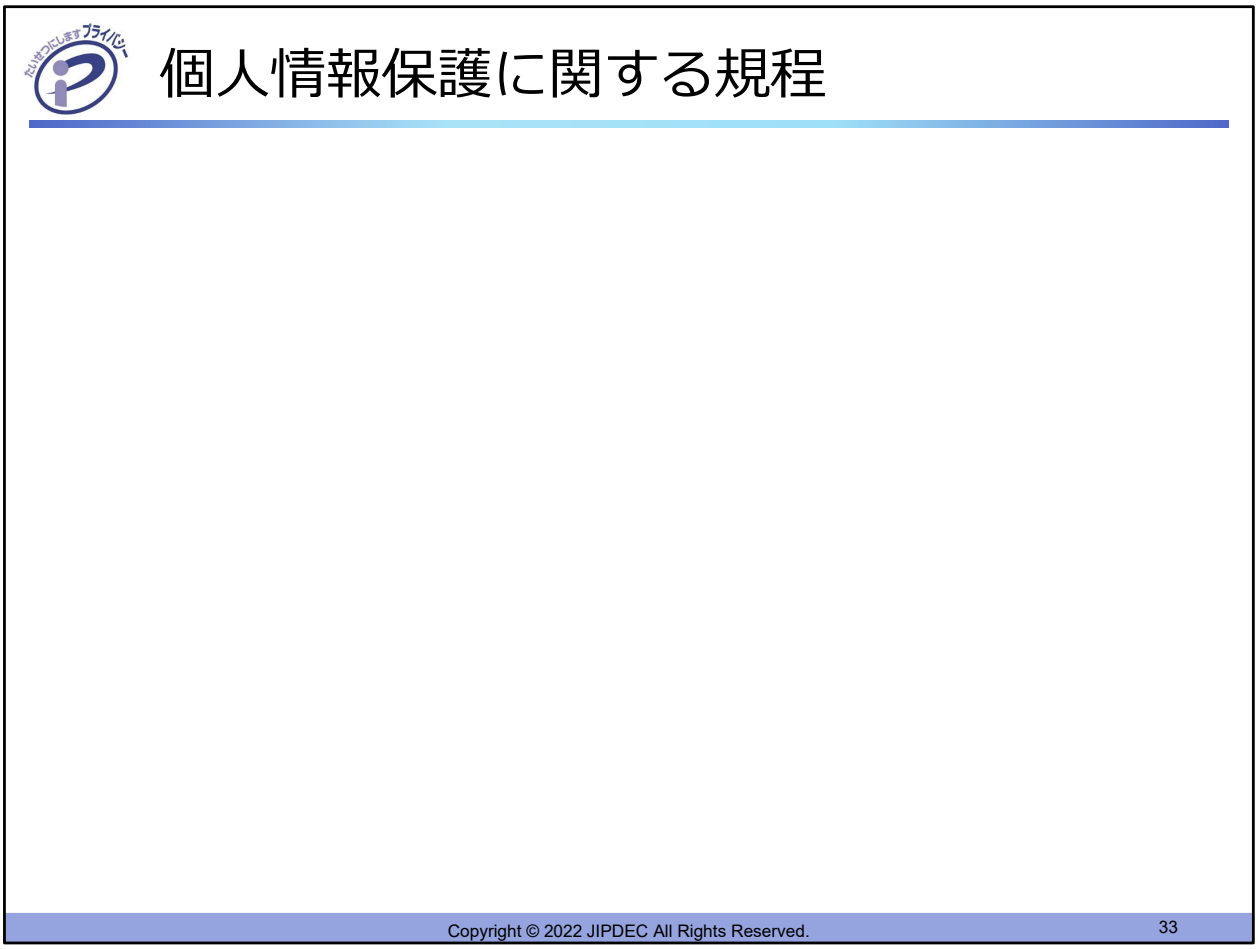


●第2部は、自社における個人情報取扱いに関する規程、ルールを追記してご利用ください。



使用例：

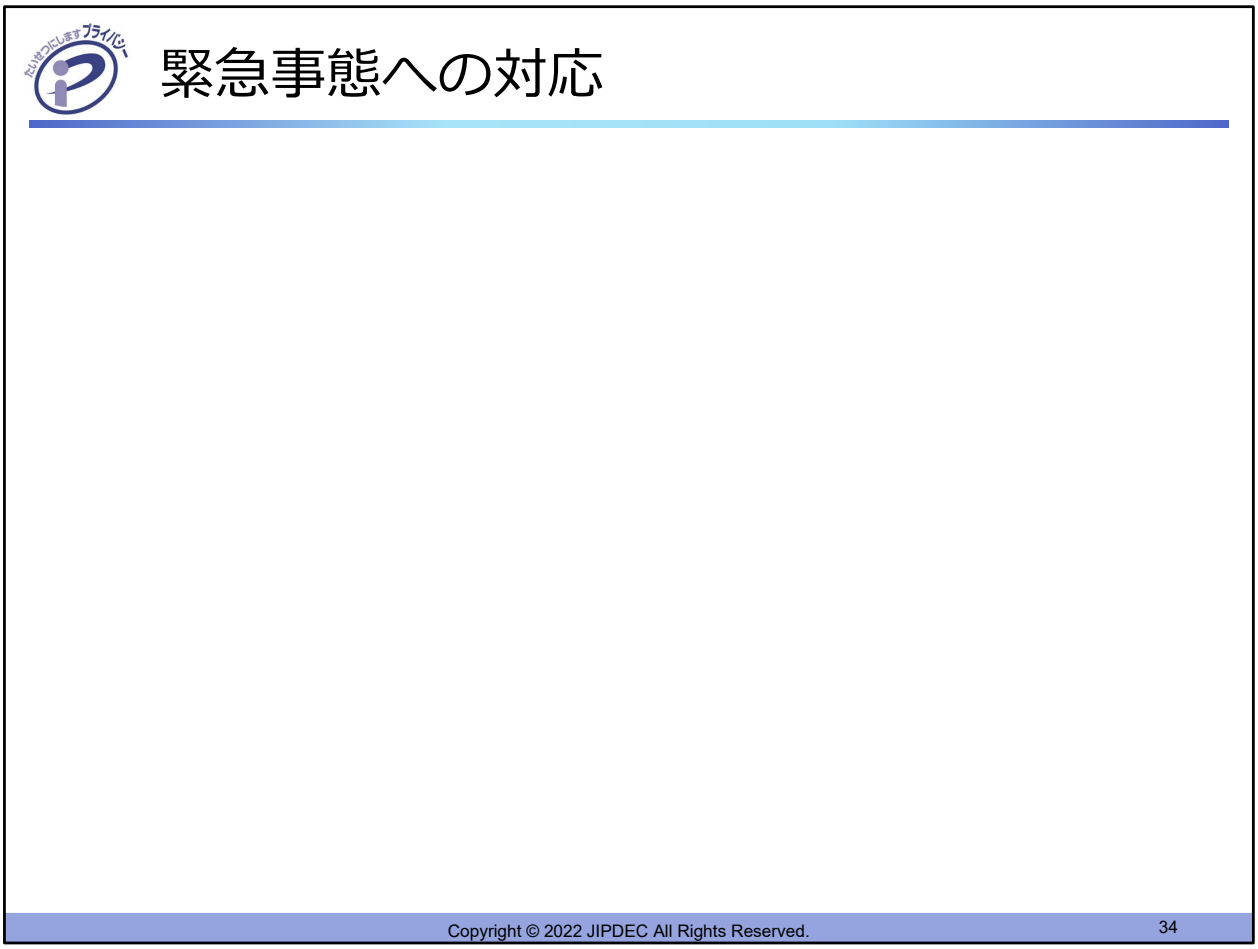
自社の個人情報保護の体制図や一覧などを記載します。



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。

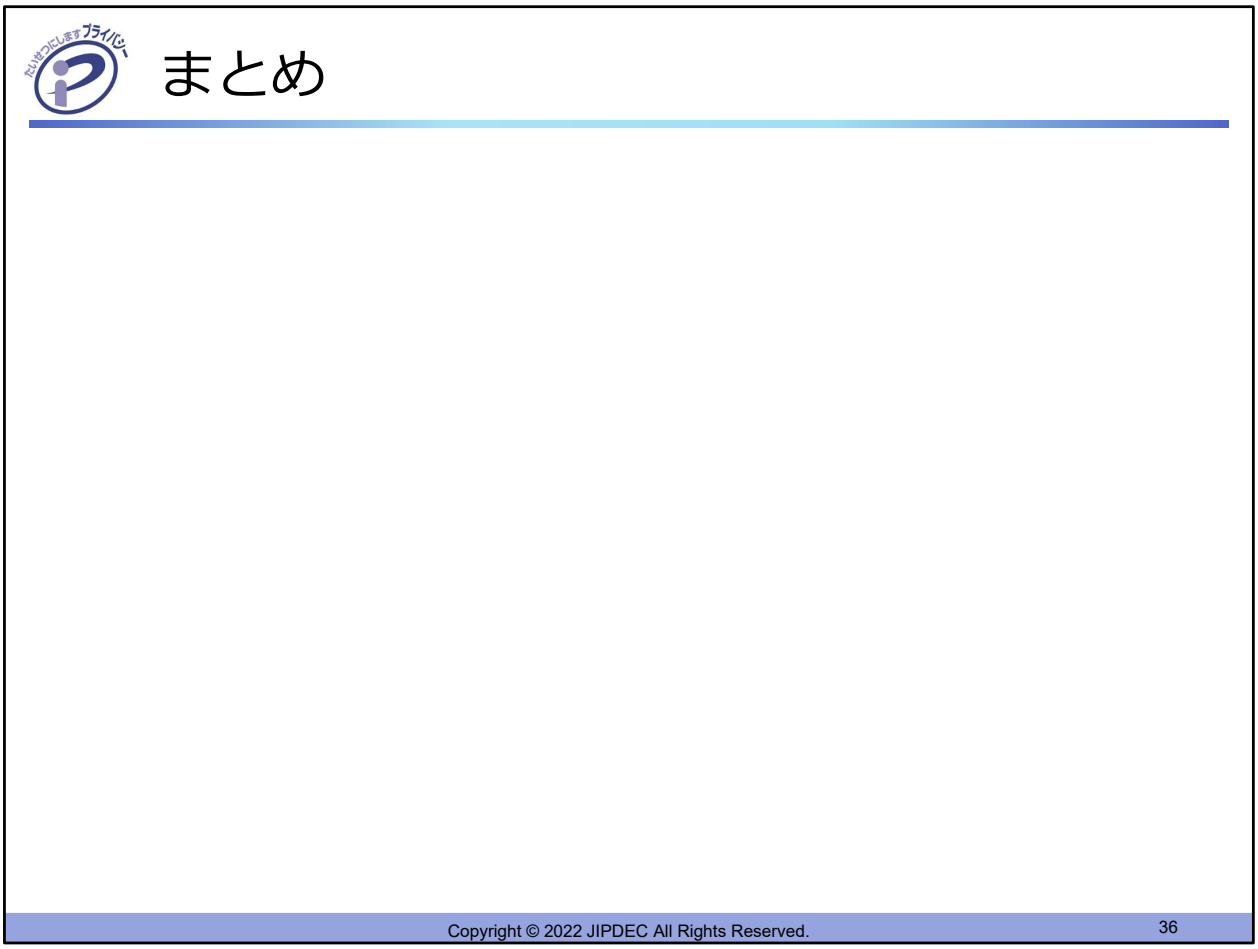
・個人情報が記載された書類等を送付する場合のルール
・メール等に添付、電子媒体で個人情報を送付する場合のルール
・個人情報を保管する場合のルール
・個人情報を削除する際のルール
・個人情報が記載された書類、PC等を持ち出す際のルール
・個人情報を委託する際のルール
など



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）
  - “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

●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