



個人情報管理の重要性

2020年12月23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

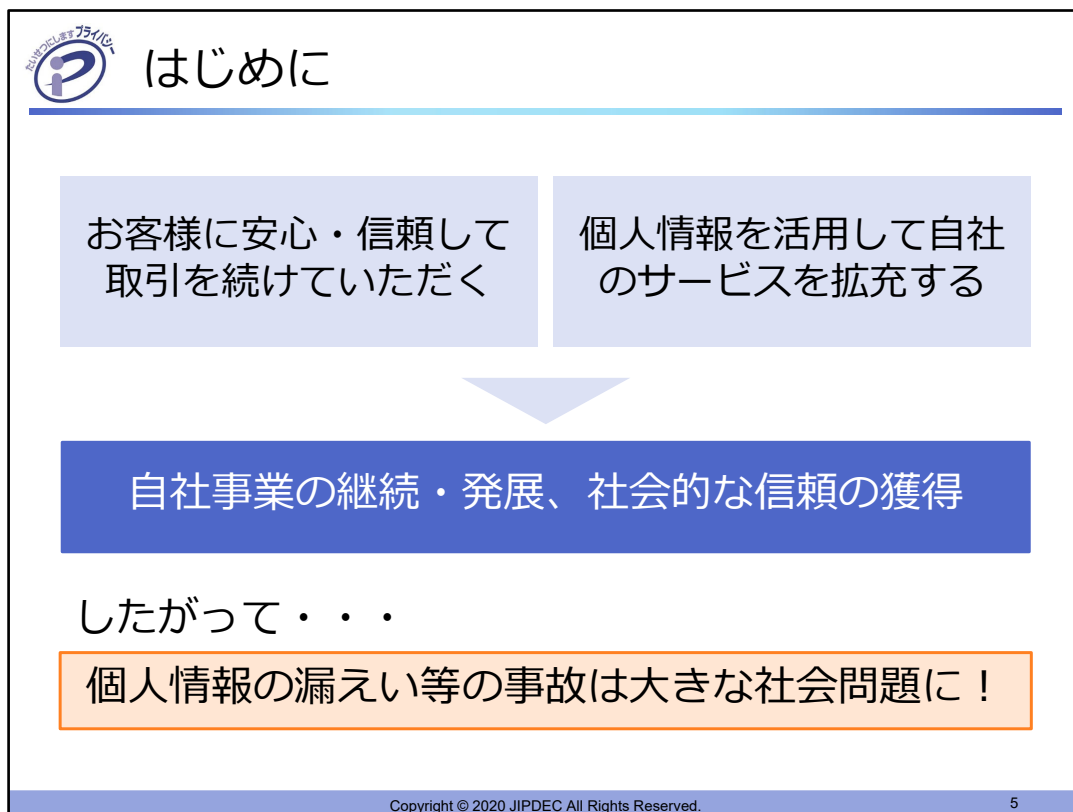
1. 個人情報の管理はなぜ必要？

Copyright © 2020 JIPDEC All Rights Reserved.

3

●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。

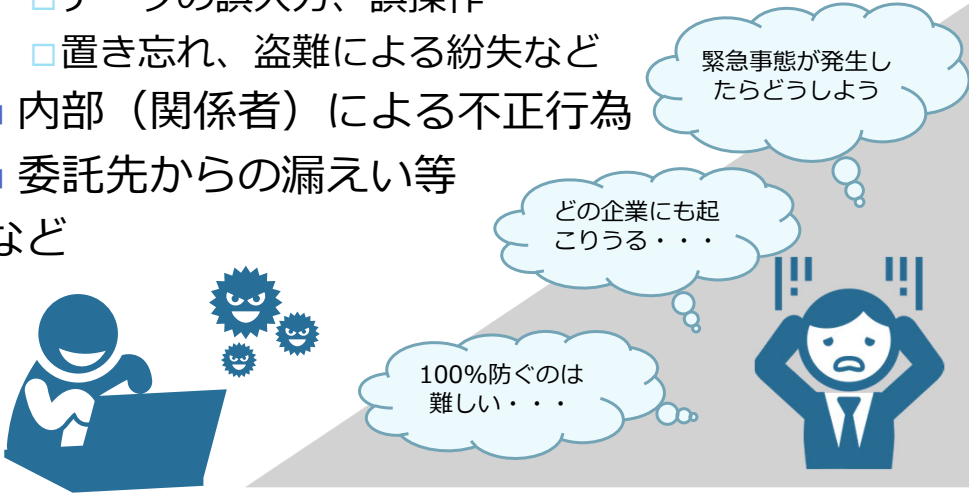
- ・お客様（消費者・取引先）からお預かりした個人情報を適切に取り扱い、お客様の権利利益を守る
- ・お預かりした個人情報を利用目的の範囲内で有効に活用して、サービスの拡充など事業展開にいかす

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



Copyright © 2020 JIPDEC All Rights Reserved. 6

● 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

2019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 © 2020 JIPDEC All Rights Reserved.

7

●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。

★2019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/2019JikoHoukoku_201109.pdf



2019年度の事故報告概要

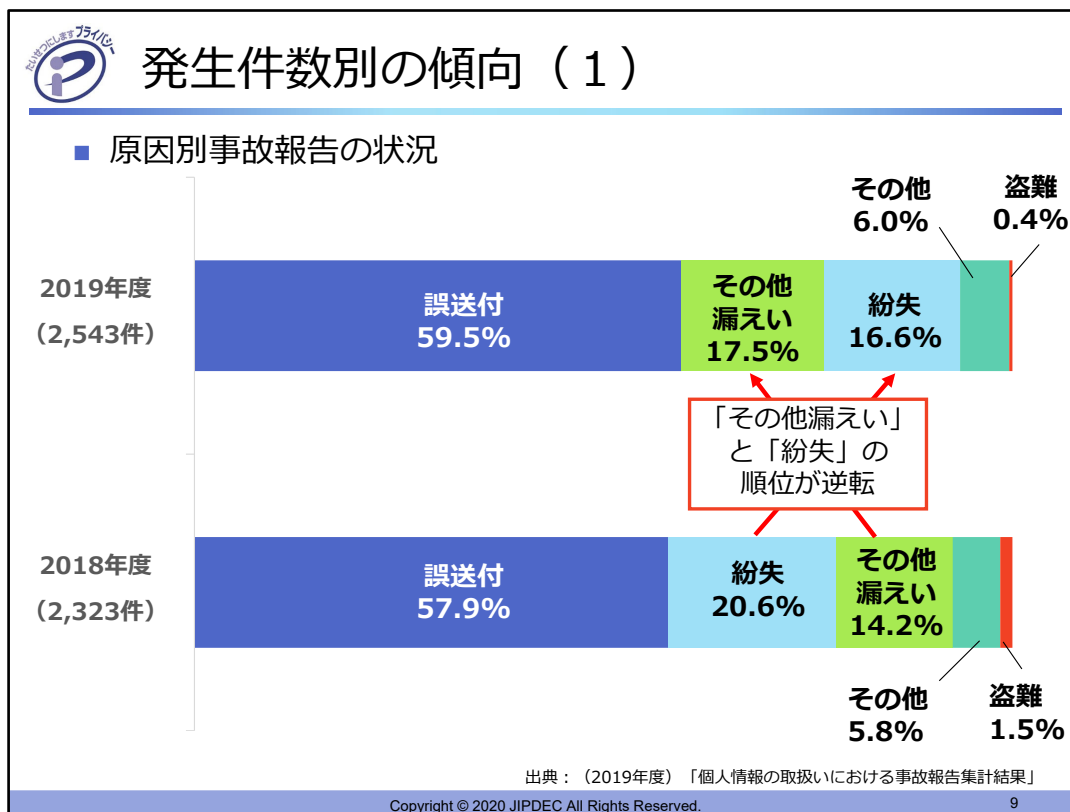
■ 発生件数別の傾向

- 「メール誤送信」 (590件:23.2%) が最も多く、次いで「その他漏えい」 (446件:17.5%) の順。
- 「その他漏えい」のうち、「プログラム/システム設計・作業ミス」が昨年度 (50件) から約3倍 (160件) に増加。
- 「誤廃棄」の件数が、昨年度 (24件) から約2倍 (66件) に増加。

■ 事故発生原因別の傾向

- 「手順等の不備・不注意・その他」 (63%) が最も多く、次いで「規程・手順の不遵守」 (23%) の順。

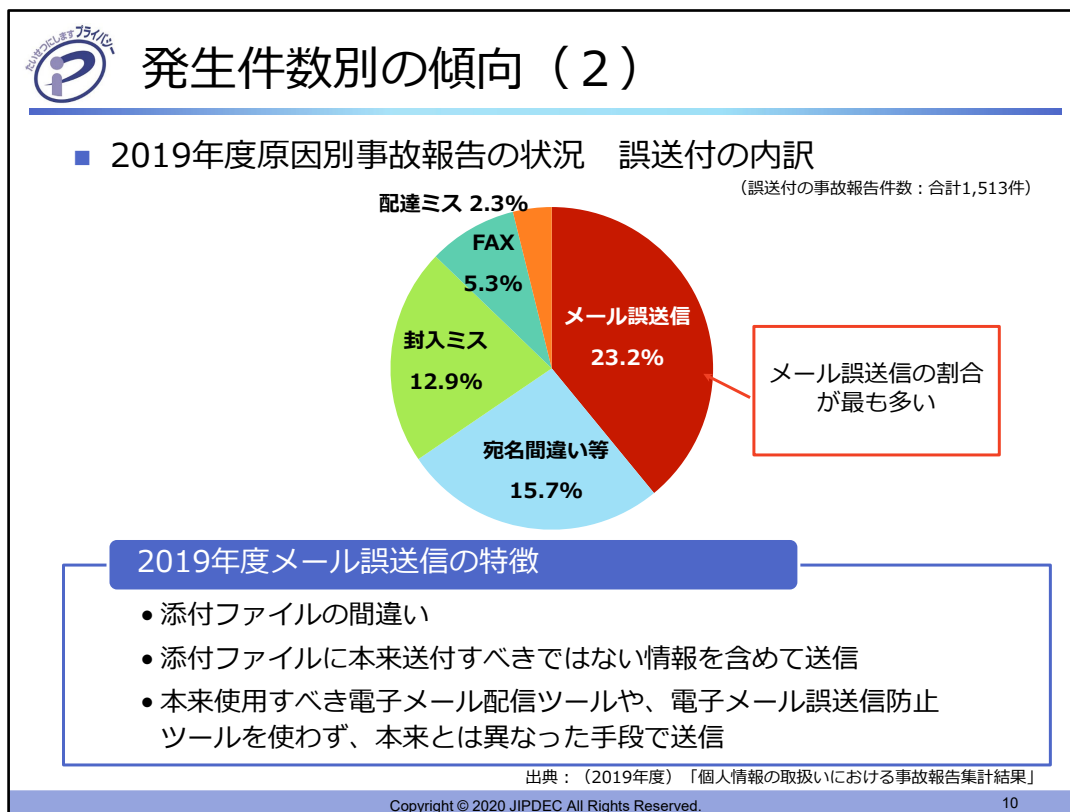
●2019度中にJIPDECと各審査機関に報告があったプライバシーマーク付与事業者の個人情報の取扱いにおける事故についての概要です。



● 2019年度の原因別事故報告の状況

2019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。

2018年度と比較すると、合計の事故報告件数が若干増加し、さらに件数別にみると「誤送付」が一番多いのは同様ですが、「その他漏えい」と「紛失」の順位が逆転する結果となりました。



●2019年度原因別事故報告の状況 「誤送付」の内訳

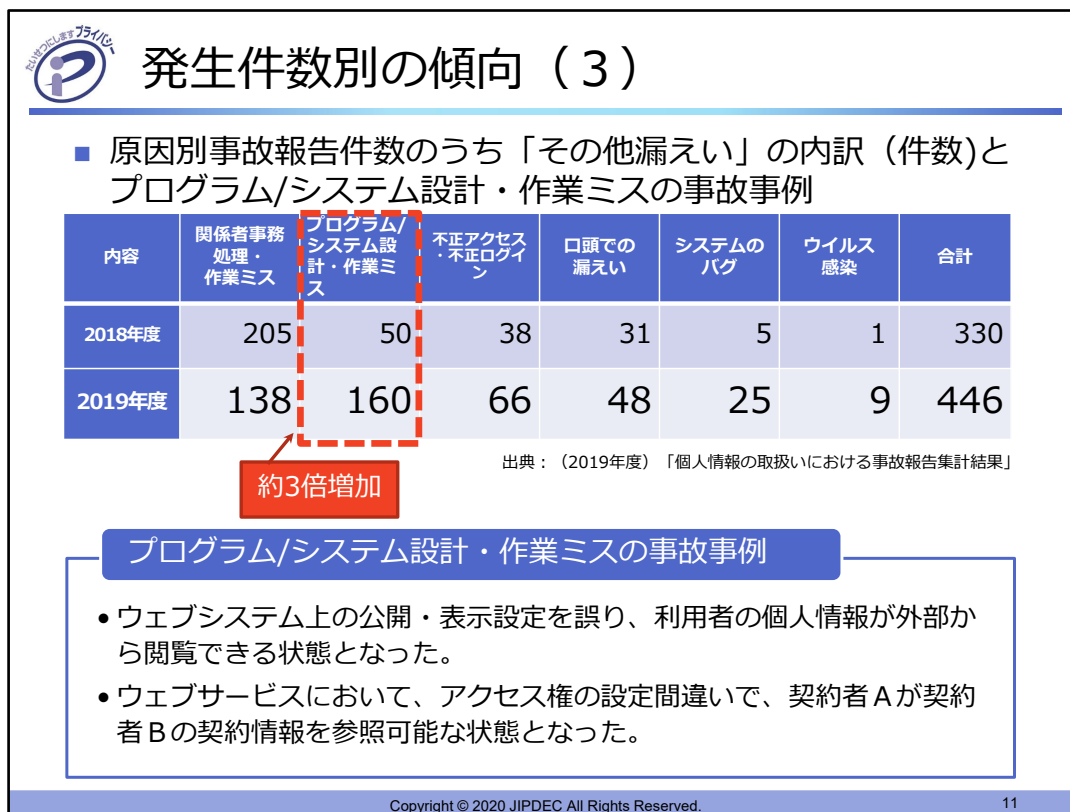
「誤送付」の内訳をみると、「メール誤送信」が最も多い結果となりました。

- ・メール誤送信
2018年度 586件（25.2%）
2019年度 590件（23.2%）

【2019年度のメール誤送信の特徴】

- ・宛名や文面の間違いだけでなく、添付ファイルの間違いや添付ファイルに本来送付すべきではない情報が含まれていた例が増加
- ・電子メール配信ツールや電子メール誤送信防止ツールなどを用いていながら、それらのツールが利用できない状況において、本来とは異なった手段で電子メールを送信したことによる誤送信

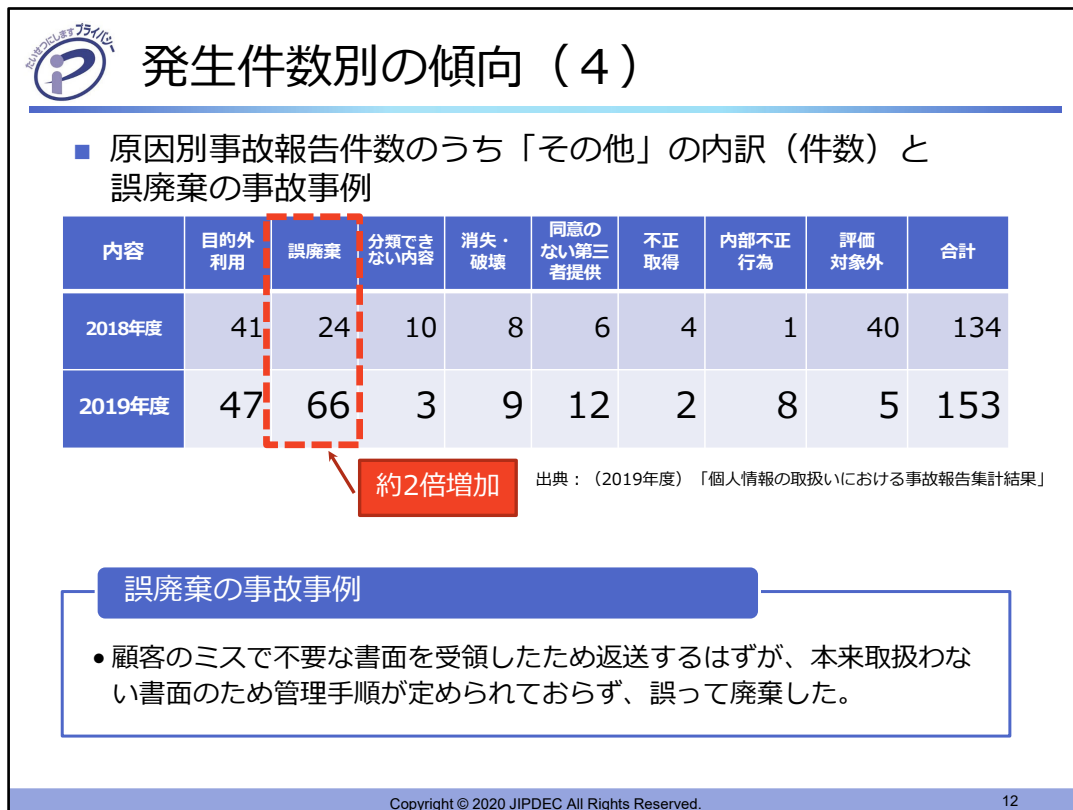
・「その他漏えい等」と「その他」の内訳を、スライド11、12にて示しています。



●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「プログラム/システム設計・作業ミス」が約3倍に増加しました。

★プライバシーマーク付与事業者の皆さんからご提出いただいた事故報告書より「プログラム/システム設計・作業ミス」の事例を挙げています。



●原因別事故報告件数のうち「その他」の内訳件数


前年度と比較すると、「その他」のうち「誤廃棄」が約2倍に増加しました。

★プライバシーマーク付与事業者の皆さんからご提出いただいた事故報告書より「誤廃棄」の事故事例を挙げています。

公表資料「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」の「紛失・盗難を防ごう」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

<https://privacymark.jp/system/reference/index.html#tools>



発生件数別の傾向（5）

- 原因別事故報告件数のうち「その他」の目的外利用と同意のない第三者提供の事故事例

目的外利用の事故事例

- 人材派遣会社において、システムの操作ミス・設定ミスにより、求人情報メールを誤った対象に送付した。
- 人材派遣会社において、求職者の経歴・健康情報などを本来の求人活動で用いる範囲を超えて利用・提供した。
- 従業員が顧客の情報を持ち出し、営業活動を行うなど不正に利益を得ていた。

同意のない第三者提供の事故事例

- 不動産・建物サービス会社において、居住者の情報を同意なく管理組合や管理業者等に提供した。
- 電話等で本人の関係者を騙る人物に、連絡先等を伝えた。

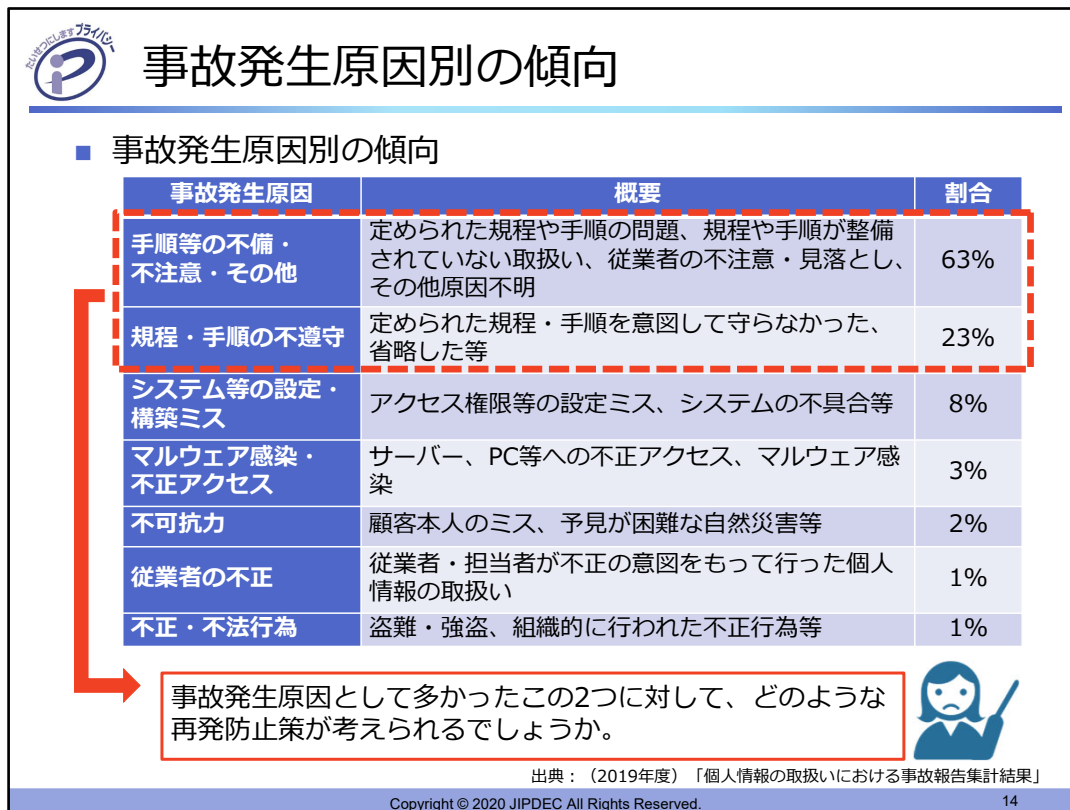
Copyright © 2020 JIPDEC All Rights Reserved. 13

★続いて、スライド12「その他」の「目的外利用」と「同意のない第三者提供」の事故事例を挙げています。

公表資料「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」の「日常業務の中で注意すべきこと」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


<https://privacymark.jp/system/reference/index.html#tools>



●事故発生原因別の傾向

事故等の発生原因を7項目の区分で分類すると、全体としては「手順等の不備・不注意・その他」が最も多く、次いで「規程・手順の不遵守」となりました。

特に手順等の不備や担当者の不注意による事故等が割合として63%と、多く発生していることは、本来想定されていなかった個人情報の取扱い、イレギュラーな状況等において多く事故が発生しているとも言えるため、事業者は、従業員に対する教育等を含め対策が求められます。

 今後の事故等への備え（再発防止策例）

不注意を防ぐ

- 業務フローや手順を改めて確認し、見直す。
- その手順が不注意を防ぐための手順として有効に機能しているかを見直す。
- イレギュラー業務が発生した場合における対応の相談先や手順を確認する。

規程・手順の不遵守を防ぐ

- 余裕がない、手間だからといって、手順を省略しない。
- 規程・手順が取扱いの実態に対して適切なのを見直す。
- 個人情報管理の重要性を認識して規程・手順のルールを守る。

Copyright © 2020 JIPDEC All Rights Reserved. 15

●スライド14「事故発生原因別の傾向」において割合が多かった「担当者の不注意」、「規程・手順の不遵守」の再発防止策の一例を挙げています。

★担当者の皆様へ

事故等の発生原因を正しく特定することが適切な再発防止策の実施につながります。

★その他の発生原因に関する再発防止策例については

公表資料「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」の各編もご参照ください。

- ・「メール誤送信を防ごう」
- ・「紛失・盗難を防ごう」
- ・「日常業務の中で注意すべきこと」

⇒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

<https://privacymark.jp/system/reference/index.html#tools>

■ 個人情報の取扱いに関する事故の 影響



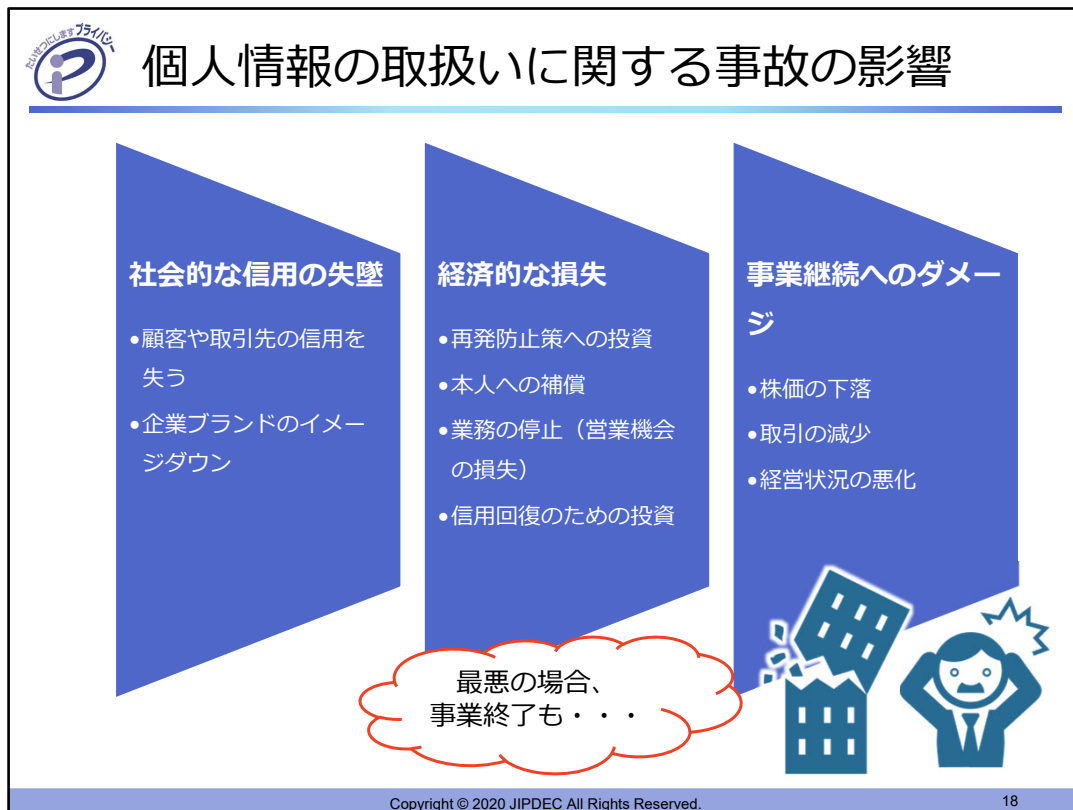
個人情報の事故を起こしてしまうと・・・

- 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：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：パブリッククラウドの設定ミス
あるプロジェクトでパブリッククラウド上に業務ファイルを保存し、外部委託先を含めた関係者で共有していたが、設定ミスでアクセス制御がかかっておらず、誰でもアクセスできる状態になっていた。
この結果、競合他社に先駆けるメリットが失われてしまい、プロジェクトの中止に至った。

出典：総務省「テレワークセキュリティガイドライン（第4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 2万9,768円

出典：NPO日本ネットワークセキュリティ協会（JNSA）「2018年情報セキュリティインシデントに関する調査報告書【速報版】」

Copyright © 2020 JIPDEC All Rights Reserved. 19

●個人情報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>

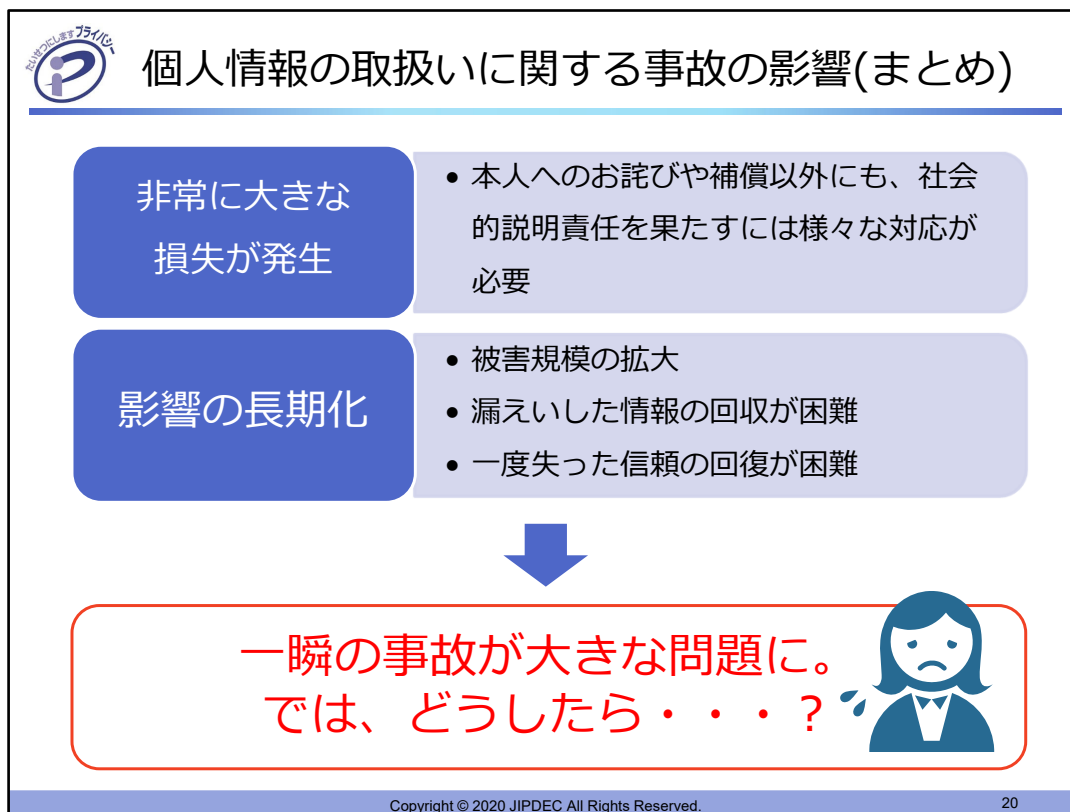
- ・総務省「テレワークセキュリティガイドライン（第4版）」

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）「2018年情報セキュリティインシデントに関する調査報告書【速報版】」

<https://www.jnsa.org/result/incident/2018.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員はどうしたらよいかを考えていきます。

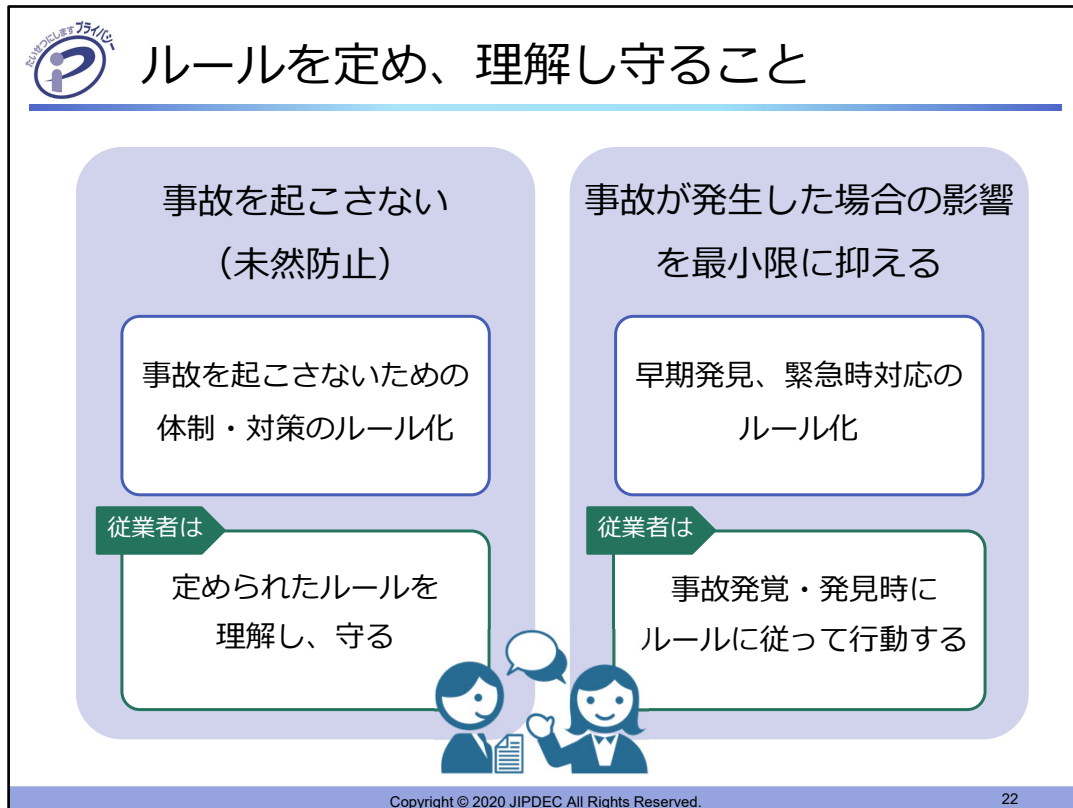
- 個人情報を適切に取り扱うために
 - 個人情報取扱いルールへの運用

●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、それを従業員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



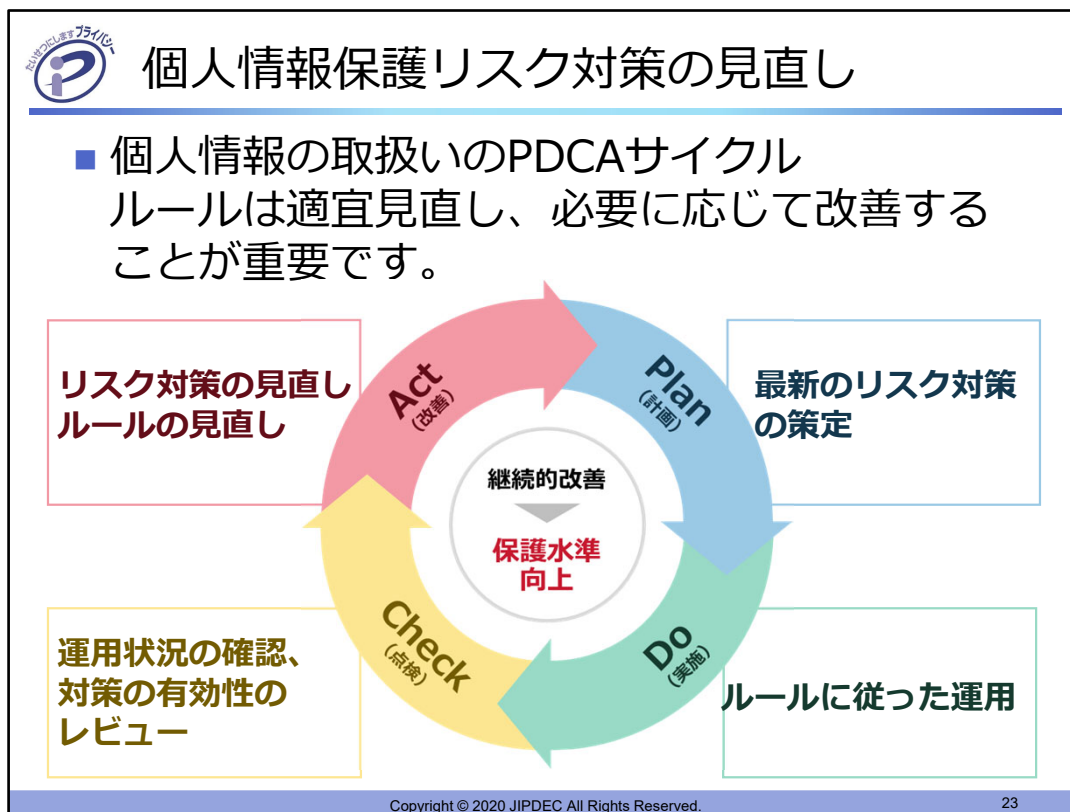
●事業者は、個人情報の取扱いに関するルールを定め運用することで、事故というリスクに備えます。

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「従業員全員」が、ルールを理解し、守り運用していくことが第一です。



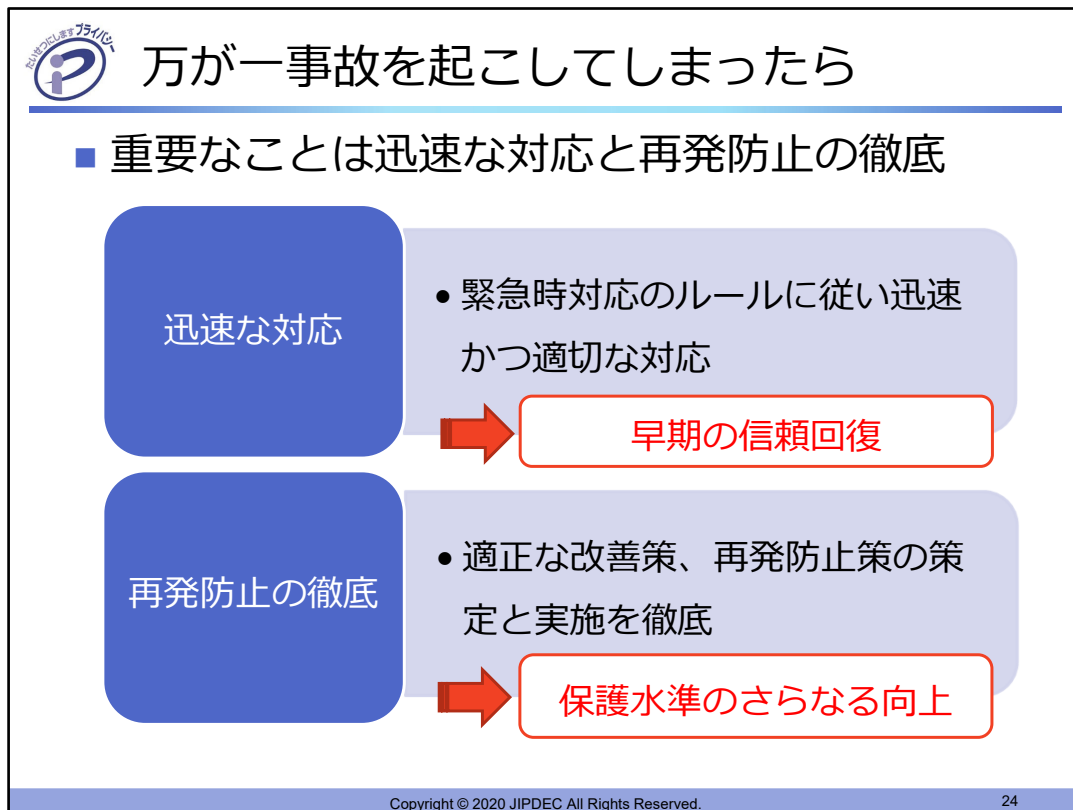
●プライバシーマーク制度では、個人情報の取扱いについてルールを定め、PDCAサイクルに沿った運用を実施することを求めています
(この研修もDo「実施」に当たります。)

★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、従業員に周知され、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、万一が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。

2. 当社の個人情報取扱い ルールについて

Copyright © 2020 JIPDEC All Rights Reserved.

25

- 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。

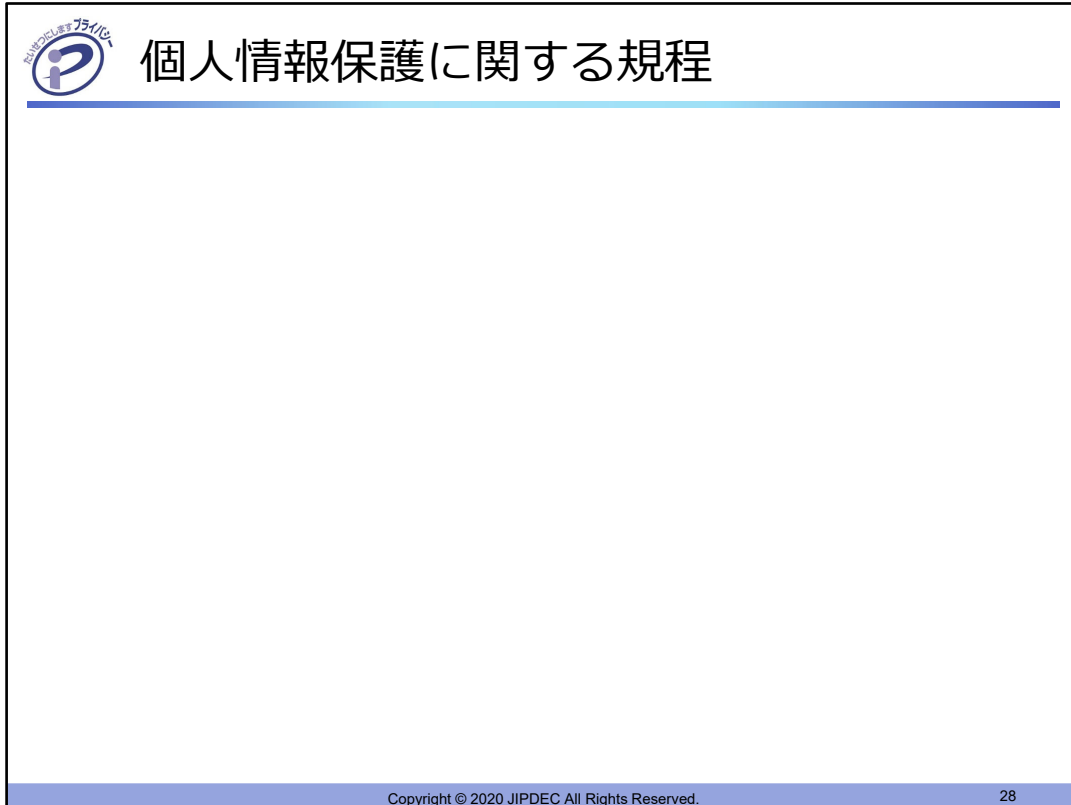
参考：

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：

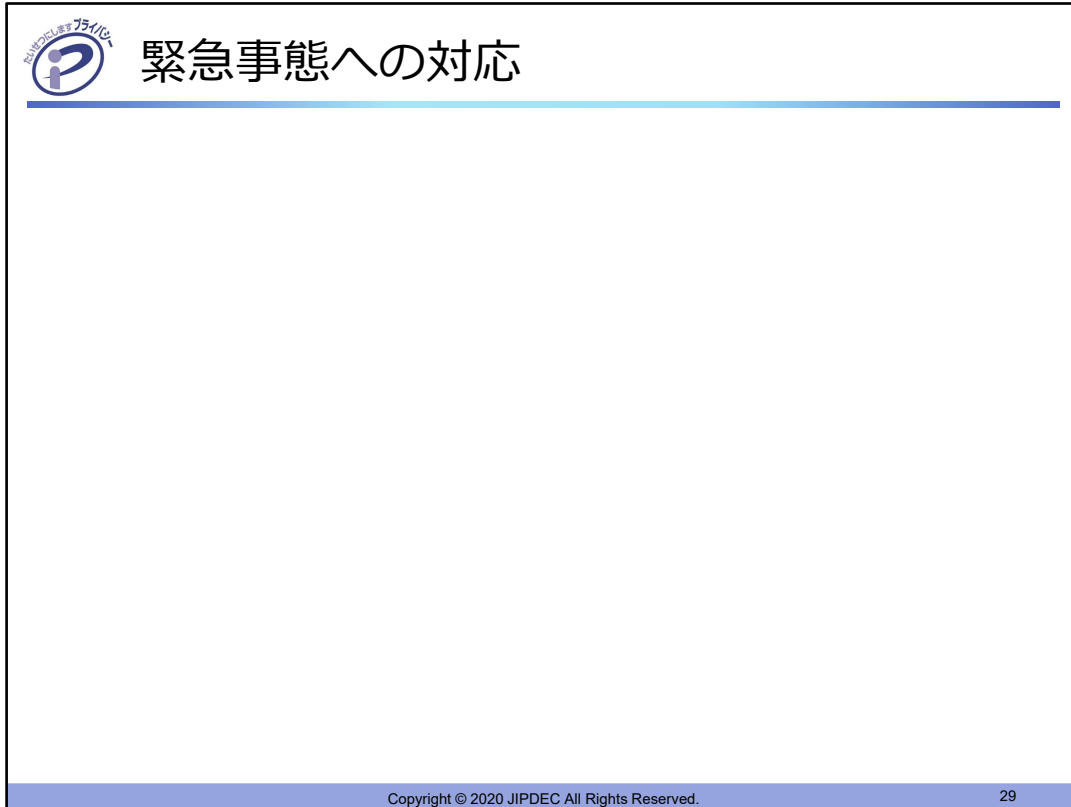
自社の個人情報保護に関する規程の体系、手順書などを記載します。

- ・ 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

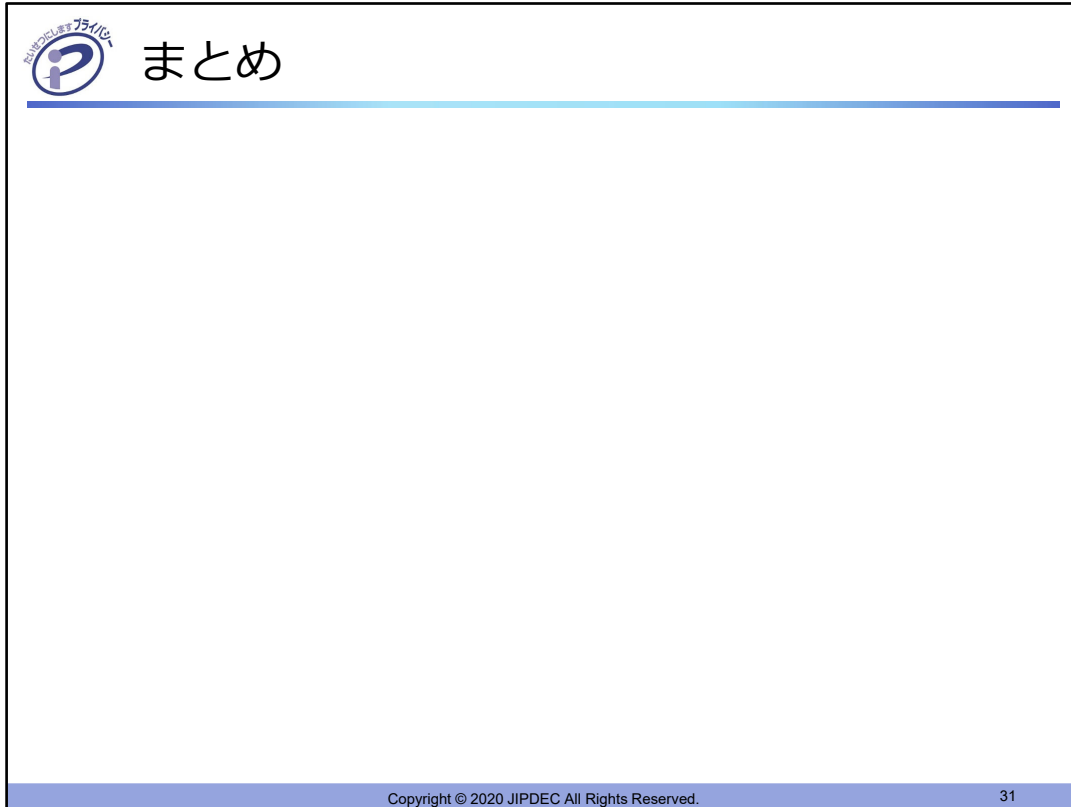


使用例：

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

