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

はじめに

お客様に安心・信頼して取引を続けていただく

個人情報を活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

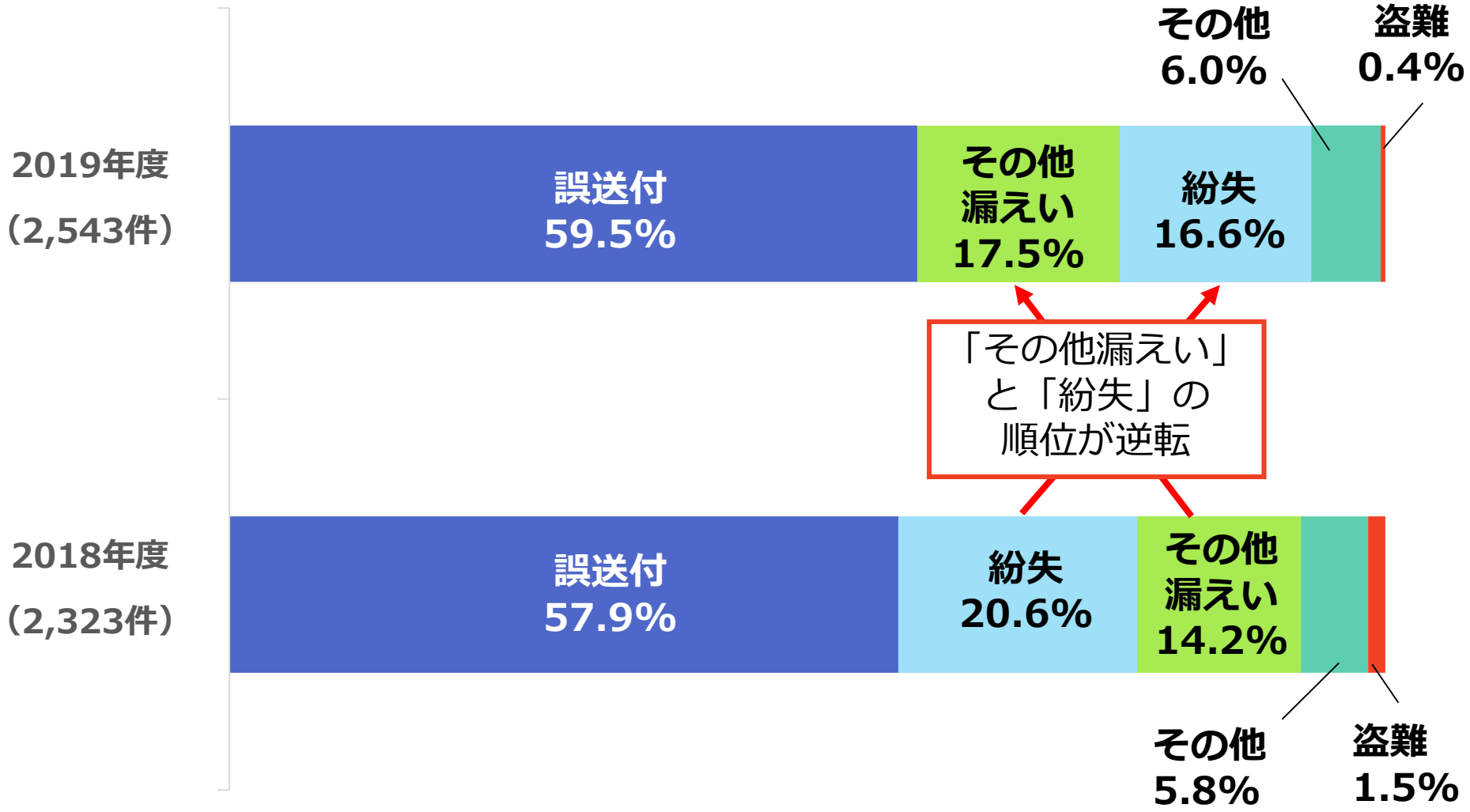
- 個人情報の取扱いに関する事故の傾向
  - JIPDEC公表の統計資料
    2019年度「個人情報の取扱いにおける事故報告集計結果」より

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。

発生件数別の傾向（１）

- 原因別事故報告の状況

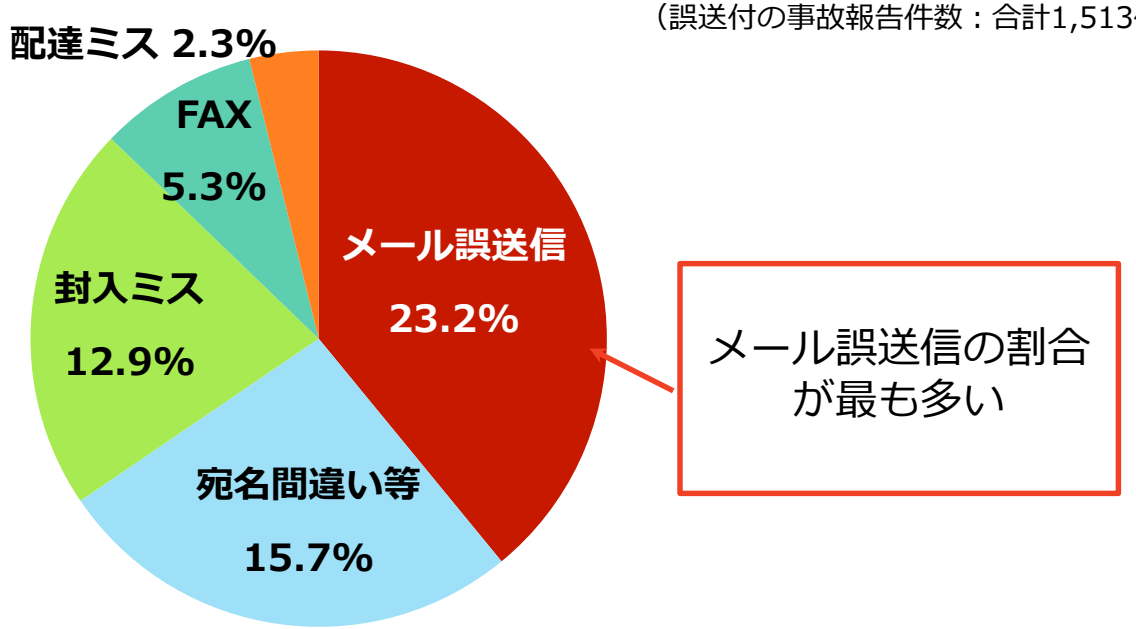


出典：（2019年度）「個人情報の取扱いにおける事故報告集計結果」

発生件数別の傾向（２）

- 2019年度原因別事故報告の状況　誤送付の内訳

（誤送付の事故報告件数：合計1,513件）



2019年度メール誤送信の特徴

- 添付ファイルの間違い
- 添付ファイルに本来送付すべきではない情報を含めて送信
- 本来使用すべき電子メール配信ツールや、電子メール誤送信防止ツールを使わず、本来とは異なった手段で送信

出典：（2019年度）「個人情報の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)とプログラム/システム設計・作業ミスの事故事例

内容	関係者事務処理・作業ミス	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	口頭での漏えい	システムのバグ	ウイルス感染	合計
2018年度	205	50	38	31	5	1	330
2019年度	138	160	66	48	25	9	446

約3倍増加

出典：（2019年度）「個人情報の取扱いにおける事故報告集計結果」

プログラム/システム設計・作業ミスの事故事例

- ウェブシステム上の公開・表示設定を誤り、利用者の個人情報が外部から閲覧できる状態となった。
- ウェブサービスにおいて、アクセス権の設定間違いで、契約者Ａが契約者Ｂの契約情報を参照可能な状態となった。

発生件数別の傾向（４）

- 原因別事故報告件数のうち「その他」の内訳（件数）と誤廃棄の事故事例

内容	目的外利用	誤廃棄	分類できない内容	消失・破壊	同意のない第三者提供	不正取得	内部不正行為	評価対象外	合計
2018年度	41	24	10	8	6	4	1	40	134
2019年度	47	66	3	9	12	2	8	5	153

約2倍増加

出典：（2019年度）「個人情報の取扱いにおける事故報告集計結果」

誤廃棄の事故事例

- 顧客のミスで不要な書面を受領したため返送するはずが、本来取扱わない書面のため管理手順が定められておらず、誤って廃棄した。

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。
- 従業者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。

事故発生原因別の傾向

- 事故発生原因別の傾向

事故発生原因	概要	割合
手順等の不備・不注意・その他	定められた規程や手順の問題、規程や手順が整備されていない取扱い、従業者の不注意・見落とし、その他原因不明	63%
規程・手順の不遵守	定められた規程・手順を意図して守らなかった、省略した等	23%
システム等の設定・構築ミス	アクセス権限等の設定ミス、システムの不具合等	8%
マルウェア感染・不正アクセス	サーバー、PC等への不正アクセス、マルウェア感染	3%
不可抗力	顧客本人のミス、予見が困難な自然災害等	2%
従業者の不正	従業者・担当者が不正の意図をもって行った個人情報の取扱い	1%
不正・不法行為	盗難・強盗、組織的に行われた不正行為等	1%

事故発生原因として多かったこの2つに対して、どのような再発防止策が考えられるでしょうか。

出典：（2019年度）「個人情報の取扱いにおける事故報告集計結果」

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かを見直す。
- 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。

- 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・・・。

個人情報の取扱いに関する事故の影響

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】」

個人情報の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

従業者は

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

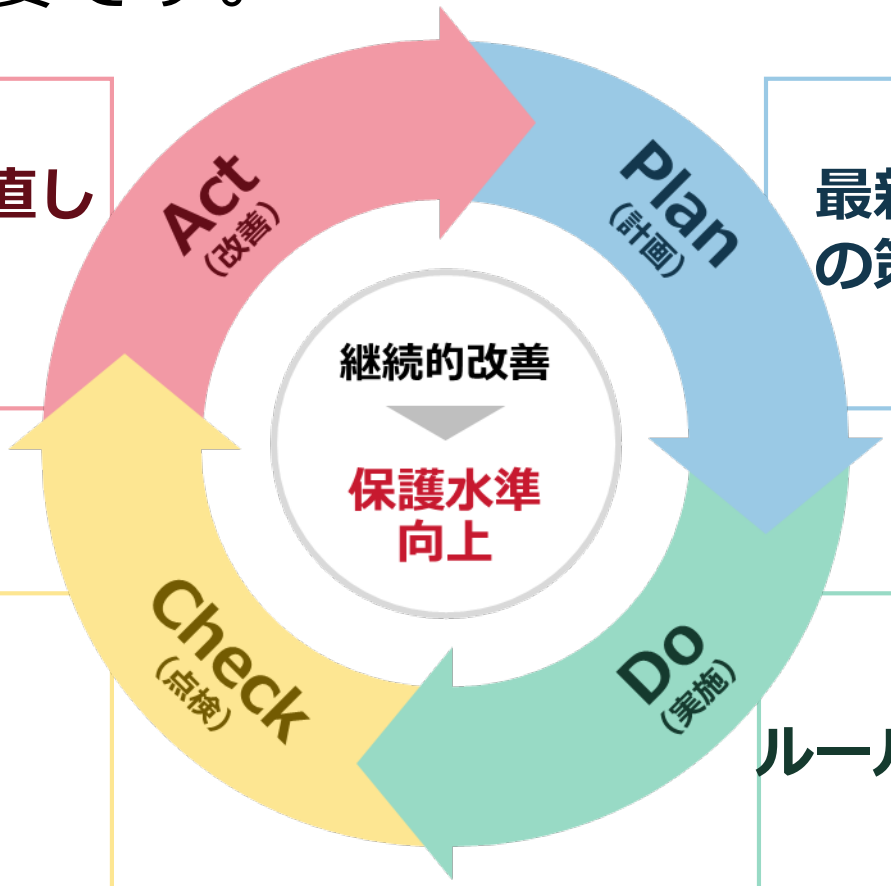
従業者は

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。

リスク対策の見直し
ルールの見直し



最新のリスク対策の策定

運用状況の確認、対策の有効性のレビュー

ルールに従った運用

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

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）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

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