個人情報を適切に管理するために

JIS Q 15001(PMS)教育テキスト

CONTENTS

PMSの定義

PMS=Personal information protection Management Systemの略。個人情報保護マジメントシステムのこと。

企業や組織の中での個人情報の取り扱いルールを決めたり、所有している個人情報のリスク評価をし、それらが適切に守られているか、きちんと認識されているかを確認し、改善を行う仕組みのこと。

PMSが整備されていることが、
JIS Q 15001＝Pマーク（個人情報保護の国内規格）の条件。

高セキュリティが要求される事業を営む当社として、
セキュリティの国際基準、国内基準をクリアしていくことを目指す

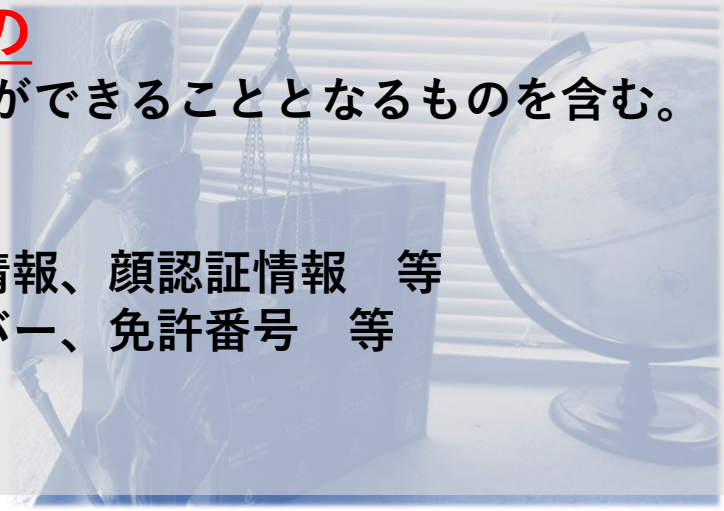
CONTENTS

個人情報の定義とは？

Pマークにおける個人情報の定義

生存する個人に関する情報であり、以下のいずれかに該当するものを指します。

① 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（《②の個人識別符号を除く。》を指します。）により**特定の個人を識別することができるもの**
※他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。



② 個人識別符号が含まれるもの
1. 身体の一部の特徴を電子計算機のために変換した符号：例　指紋・静脈認証情報、顔認証情報　等
2. サービス利用や書類において対象者ごとに割り振られる符号：例　マイナンバー、免許番号　等

2.個人情報とは？

個人情報の具体例

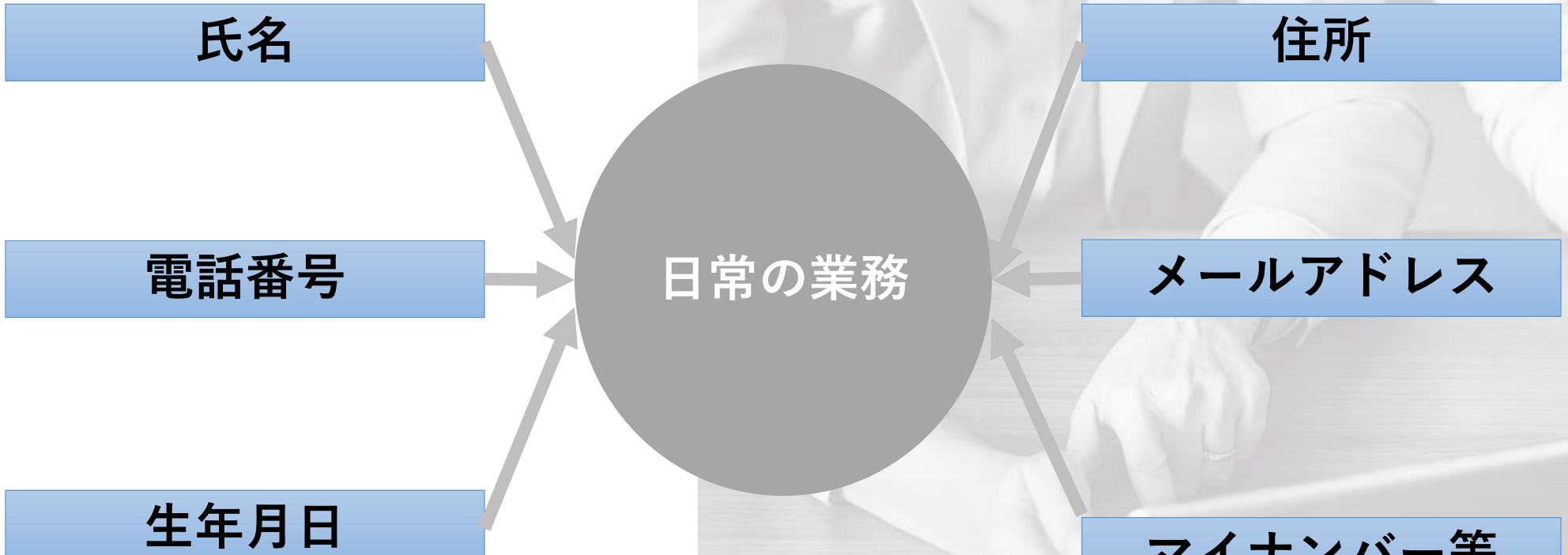
組織にとって“大事なモノ”とは？

- 業務を行う従業員に関する情報
- 営業情報
  （顧客情報、著者情報、新製品情報等）
- 経営・財務・人事情報
- 技術情報
- 情報端末（PC,FAX等）
- 個人情報

などが対象。

2.個人情報とは？

⚠ あなたの仕事にも、個人情報が含まれている



CONTENTS

3．個人情報保護方針とは

簡単に言うと、
「個人情報を守っていくために会社でどういったことを
していくかを示したもの」

個人情報保護方針は、当社ホームページに掲載しており
いつでも見ることができます

個人情報保護方針の内容
a)目的外利用の禁止
b)法令等の順守
c)個人情報の事故に対する是正処置
d)苦情相談対応
e)個人情報保護の継続的改善

CONTENTS

４．個人情報取扱いによるリスク

個人情報の管理はなぜ必要なのか？

個人情報を有効に活用して事業の拡大に活かす

お客様に安心・信頼して取引を続けていただく

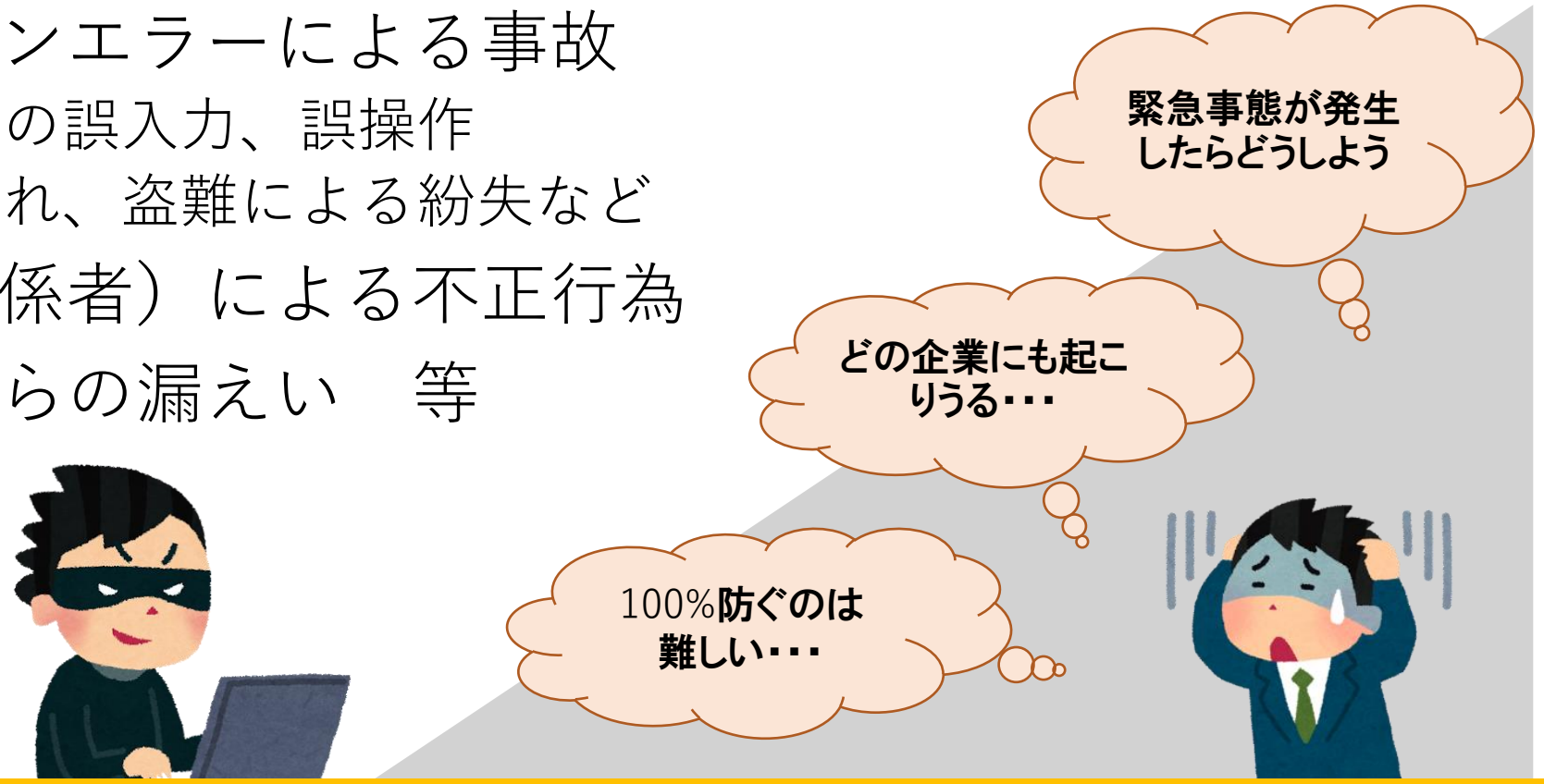
自社事業の継続・発展、社会的な信頼の獲得

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



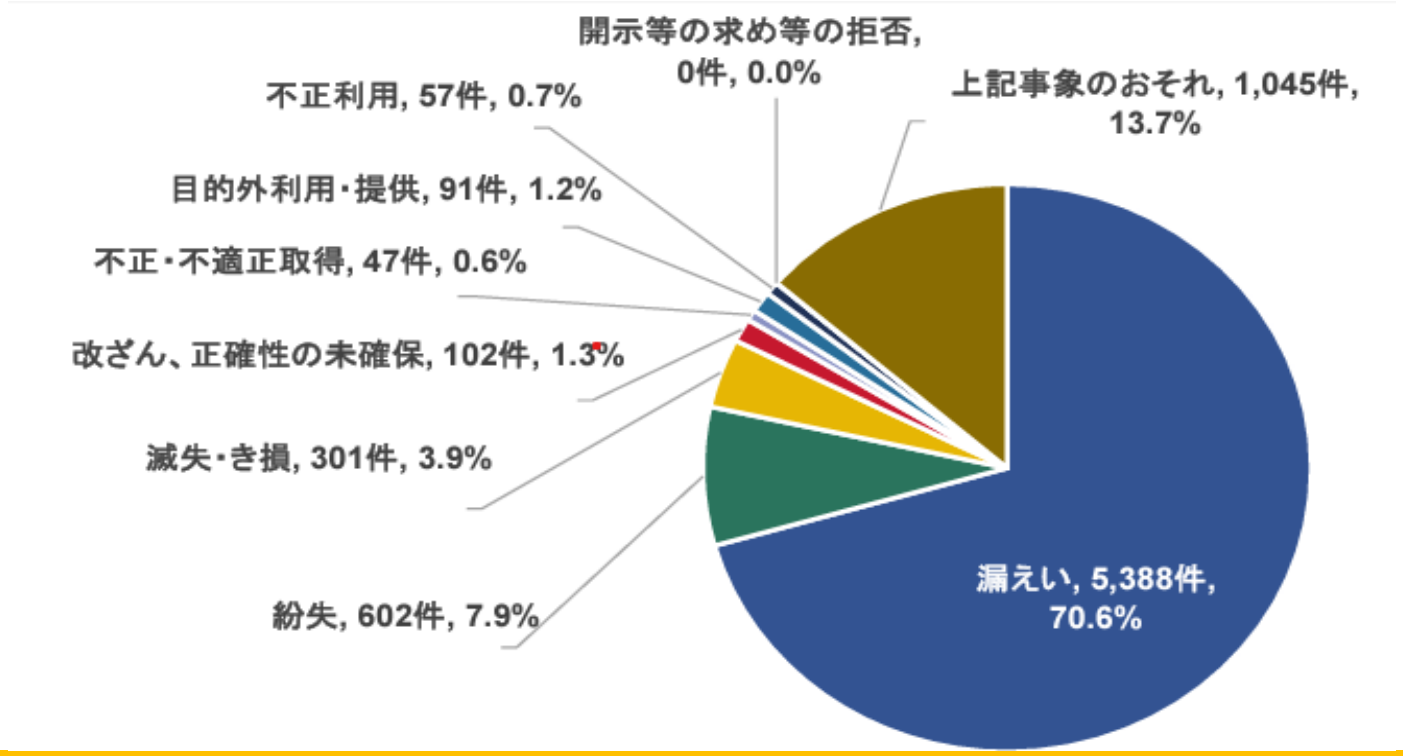
４．個人情報取扱いによるリスク

- 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年個人情報の取扱いにおける事故報告集計結果」

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」

事故事象別の統計概要

- まず発生した事象別の統計を見てみましょう。「漏えい」が最も多く、次に「紛失」事象が多い結果となりました。

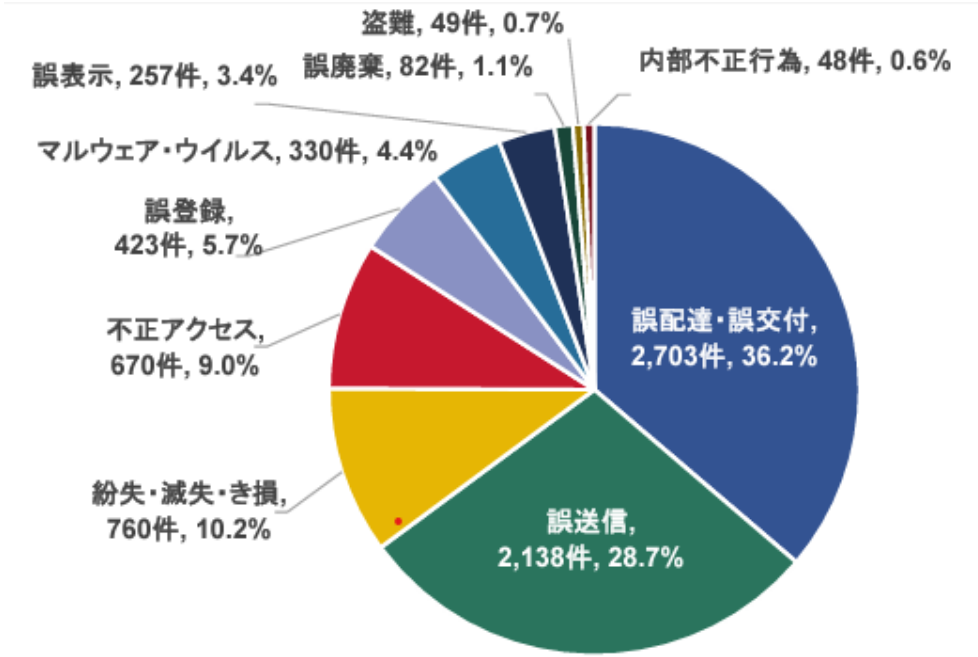


出典：（2023年度）「個人情報の取扱いにおける事故報告集計結果」

事故分類報告概要

- 次に事故分類件数が多い順に見ると、
「誤配達・誤交付」(2,703件：36.2%)が最も多く、次いで
「誤送信」(2,138件：28.7%)
「紛失・滅失・き損」(760件：10.2%)
「不正アクセス」（670件：9.0%）

となりました。

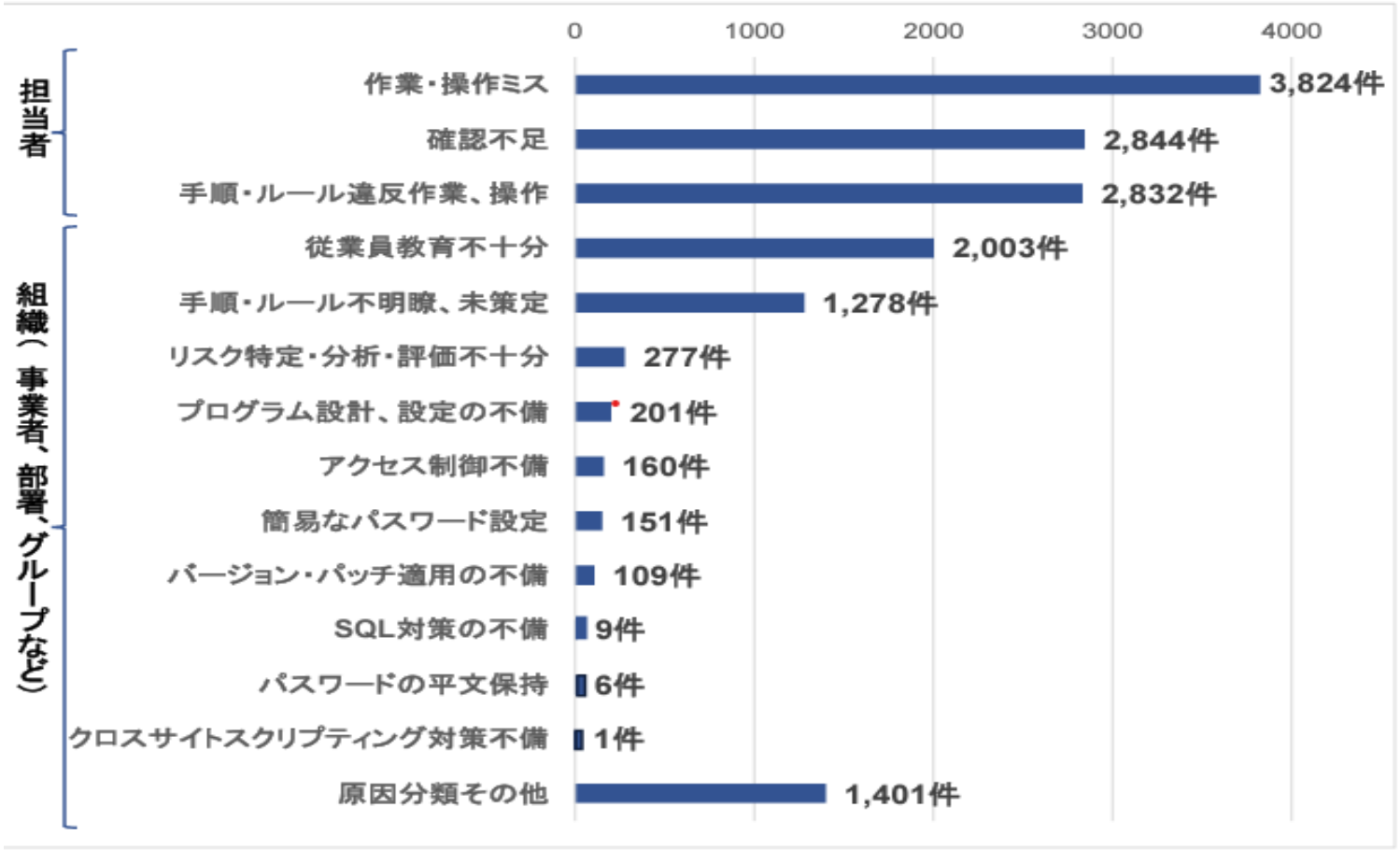


４．個人情報取扱いによるリスク

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」

原因別事故報告件数

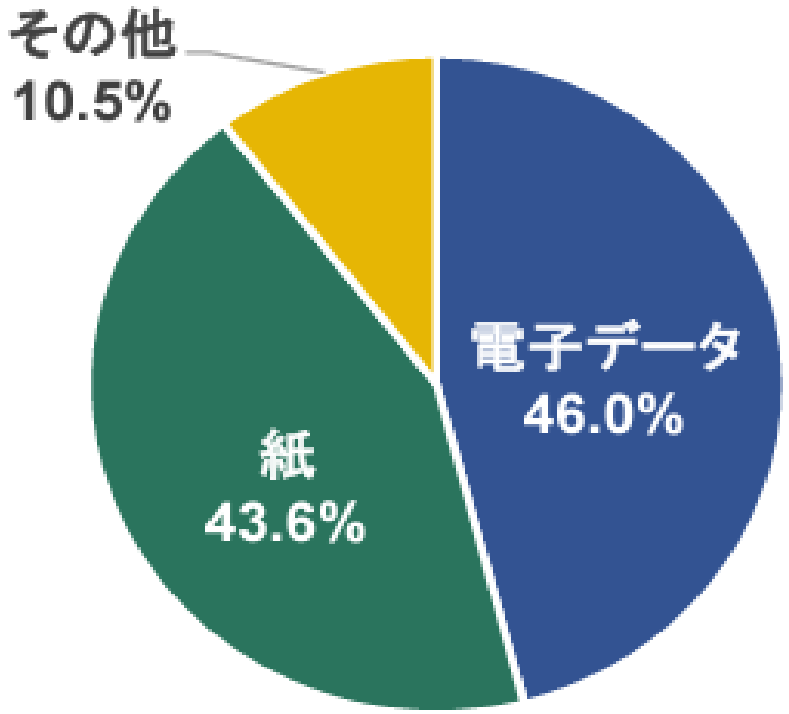
次に原因別に見てみると、「作業・操作ミス」や「確認不足」、「手順・ルール違反作業、操作」が多く見られました。以下原因別集計表になります。



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」

媒体別の事故発生割合

事故が発生した媒体別に見てみますと以下の表の通りとなります。
そこまで差異はありませんが、結果的に電子データ上回る形となりましたが、
紙媒体についてもそれなりの結果が出ている形となっています。



メール誤送信の事故事例と防止策例

- 事故のパターンと事例

メール宛名間違い

- アドレス帳から同姓の別人のメールアドレスを選択した
- メーラーのオートコンプリート機能により別人のメールアドレスを設定した
- コピー＆ペーストでのミス

ファイルの添付ミス

- A社に送信する際、B社用のファイルを添付した
- 添付したファイルの内容に他社分の個人情報も含まれていた

BCCとTO/CCの誤り

- 本来BCC送信すべきところをTOやCCで送信した

- 防止策例

メール送信前の確認の徹底

- メールアドレス、内容、添付ファイルの確認
- 確認のルール化、マニュアル化、ルールの教育など

添付ファイルの暗号化

- ファイルの暗号化、パスワードロック等の秘匿化など

メーラーの設定変更

- メーラーの設定を送信前に宛先、メール内容が確認できる設定に変更するなど

４．個人情報取扱いによるリスク

インターネットを介した事故事例と防止策例

- 事故のパターンと事例

作業ミス

- A社のデータを、誤ってB社のオンラインストレージにアップロードした
- Webサイト更新時、公開用フォルダに一時的に移動した個人情報が含まれるデータを削除し忘れた

ID/パスワードの漏えい

- 会員Cに対し、会員D用のID/パスワードをメールで送信した
- E社にF社用の取引先ページのID/パスワードを送信した

設定ミス

- クラウド上での作業時、取引先従業員情報の非公開設定を失念した
- Webサイトのアクセス制限設定を誤り、個人情報が掲載されたページが閲覧できる状態となった

- 防止策例

手順やルールの見直し

- 適切な業務運営やガバナンス体制の構築、
- 作業実施ルール・チェックルールの確認、見直し

など

具体的な手順等の工夫

- 二重チェック体制の構築
- 新たな手順の導入

など

注意喚起・教育

- 教育方法、実施時期、内容の見直し

など

委託先の管理

- 定期的なモニタリング、監査の実施

など

内部不正行為による事故事例と防止策例

- 事故のパターンと事例

従業者によるもの	退職者によるもの	委託先によるもの
• 人事情報を他部署の従業者が無断で持ち出した • 営業担当者が顧客になりすまし、代金の払い戻しを受けた	• 元社員が顧客データを持ち出し転職先での営業活動に利用した • 元社員が顧客名簿を持ち出し、他の事業者に転売した	• 委託先の従業者が自宅で作業するため、個人データを持ち出した • 委託先従業者が委託元の社員名簿を持ち出し社員に迷惑メールを送った

- 防止策例
  - データ管理状況の見直し
  - 端末や社内システムへの接続制限
  - 退職者に係る取扱いルール見直し（秘密保持契約締結、迅速なID削除等）
  - 注意喚起・教育

その他日常業務での事故事例と防止策例

- 事故のパターンと事例

口頭での漏えい	盗難・紛失
• 電話での本人確認が不十分だったため、本人と誤認して別人に個人情報を教えた • 誤って別人のログインID等を伝えた	• 携帯電話、スマホの紛失が増加

- 防止策例
  - **対応ルール・手順の確認・見直し**
  - 従業者への注意喚起・教育

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・・・。

４．個人情報取扱いによるリスク

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・・・

４．個人情報取扱いによるリスク

個人情報の取扱いに関する事故の影響（事例）

事例１：PayPay株式会社
スマートフォン決裁サービス「ペイペイ」 第三者からの不正アクセス

時期：2020年12月8日
内容：ブラジルからの不正アクセス。
加盟店情報(住所、連絡先、代表者名)や従業者の個人情報にアクセスされた可能性。
流出した個人情報の件数は
2,007万6,016件と見積もっている。
備考：同社発表によると、攻撃を受けた原因はサーバー更新時のアクセス権限に関わるセキュリティ設定ミスによるものです。同社では本来、加盟店の営業情報は店舗への営業に関わる従業員しかアクセスできない仕様になっていましたが、サーバー更新時に一時的に外部からのアクセスを許可した際、設定をもとに戻さず放置したことにより外部アクセスを受けたとしています。

事例２：みずほファイナンシャルグループ　顧客情報が入った記録媒体を誤廃棄

時期：2020年7月22日
内容：みずほフィナンシャルグループの子会社であるみずほ総合研究所は7月21日、約250万件の顧客情報などを記録した磁気テープ6本を紛失したと発表した。
「誤廃棄の可能性が高く、現時点では外部への情報漏えいは確認していない」という。
備考：磁気テープに記録していたのは、2018年12月7日までに取引した顧客の氏名や所属企業名、住所、メールアドレス、口座番号、同社が提供するサービスの利用実績など。内訳は、個人の情報が約240万件、企業など法人の情報が約10万7000件。みずほ銀行との共同事業である「MIZUHO membership」に関する約5万1000件の法人情報も含むという。

４．個人情報取扱いによるリスク

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・・・？

４．個人情報取扱いによるリスク

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

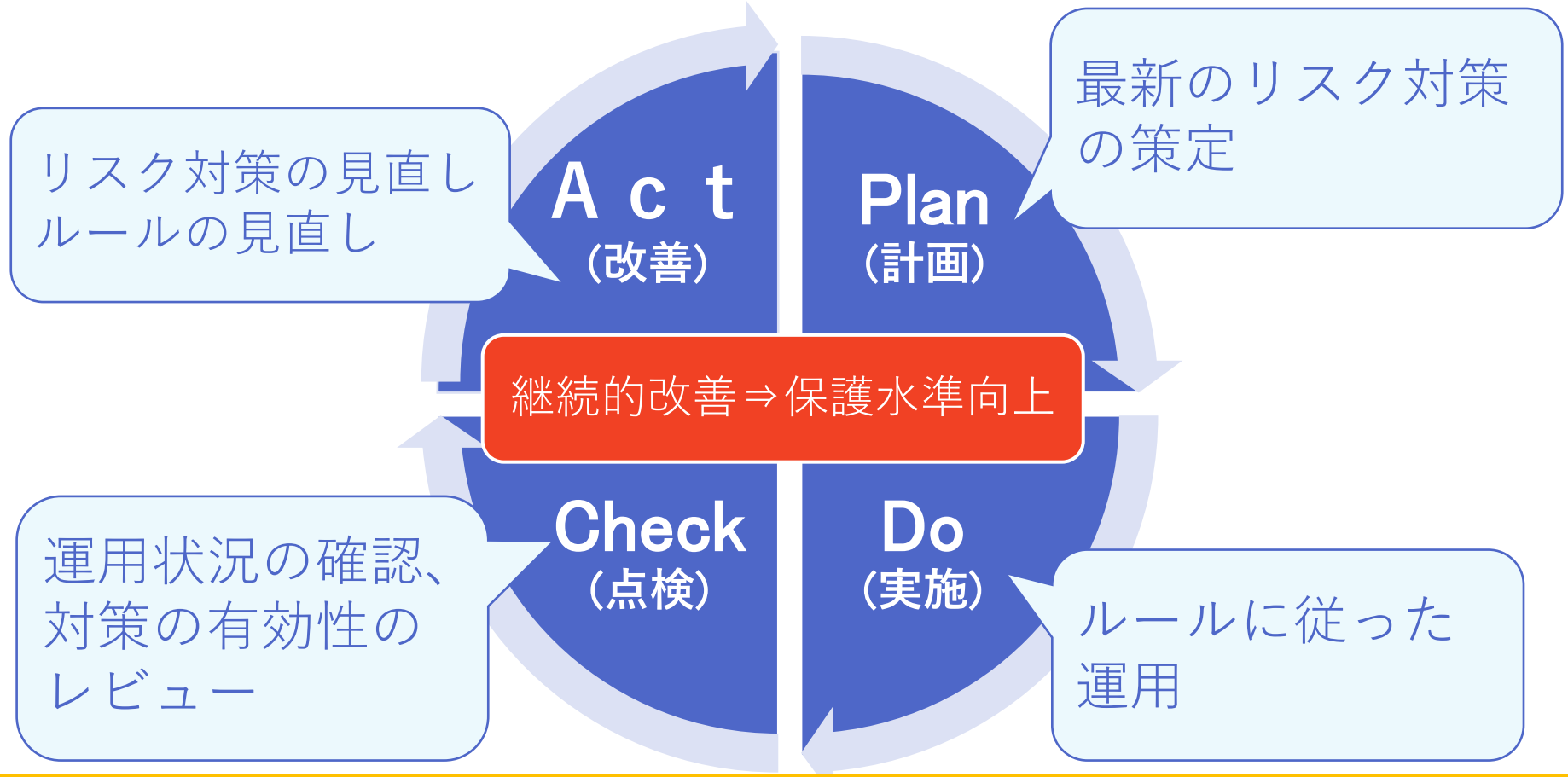
早期発見、緊急時対応のルール化

従業者は

事故発覚・発見時には、直ちに部署責任者（オンサイト就業の方は、営業担当）に第一報を行う。

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。



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**

CONTENTS

認定のメリット

直接お客様から情報を預かる企業では

お客様が安心して個人情報や機密情報等を預けていただき、信頼される。

お取引先企業から情報を預かる企業では

委託、提供先企業としての選定基準をクリアできる。
入札、見積りで排除されにくくなる。
コンプライアンス経営企業としてイメージが向上する。

どの企業にも共通したメリットは

社員の個人情報、重要資産に対する意識が高まる。
リスクマネジメントが強化され、情報漏えい等のリスクが低減する。
名刺やパンフレット、ホームページ上で認証マークが使用できる。

CONTENTS

規則を守ること

規則を理解し、遵守すれば、ルールに従った行動を行える。

・規則の例

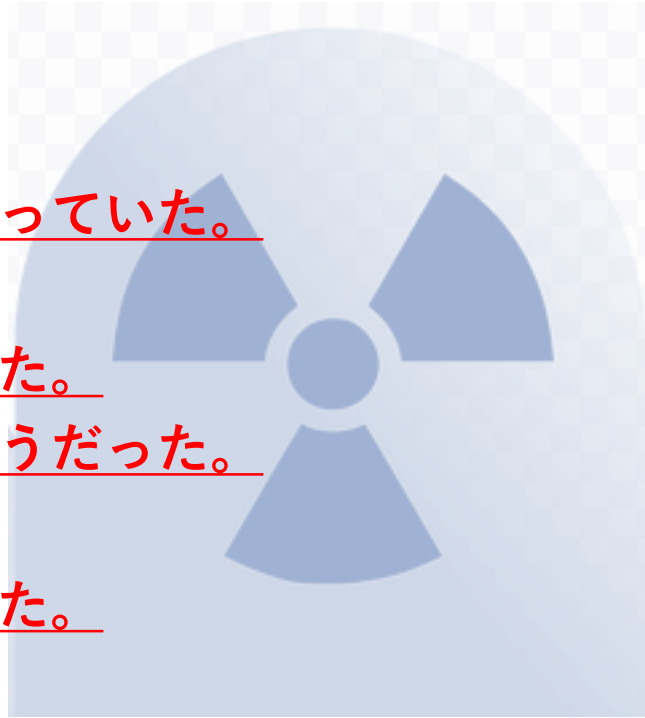
・パスワードをメモした紙をパソコンに貼り付けないようにしましょう。
・パスワードを他人に教えないようにしましょう。
・未許可のサイトへのアクセスをしないようにしましょう。
・個人情報の含まれるメールは暗号化しましょう。
・帰宅時はパソコンの電源を必ずオフにしましょう。
・許可なくノート型パソコンを社外に持ち出さないようにしましょう。
・個人情報が記載された紙はシュレッダーで廃棄しましょう。
・個人情報が記載してある物を出しっぱなしで席を離れないようにしましょう。

危ないと思ったら報告すること

事故ではないからと軽視をせず、危ないと思ったことを報告することで、本当の大きな事故を防ぐことができる。

例えば・・・

- アドレス帳から違う人のメールアドレスを選択してしまっていた。
- FAX番号を押し間違えていたが、送信前に気づいた。
- 電車を降りる時にノートパソコンを置き忘れそうになった。
- 個人情報の書かれた紙の裏を使った後、ゴミ箱に捨てそうだった。
- メールを送る時のBCC欄とCC欄を間違えていた。
- パスワードを書いたメモ紙が物を出した時に飛んでいった。



管理体制図

迷ったら、上長や管理責任者に相談を

主な活動	役割
代表者	PMSに関するリーダーシップの発揮、方針の確立、責任・役割・権限の割り当てと社内伝達、PMSのパフォーマンスの報告を受ける、マネジメントレビューの実施
個人情報保護管理者	PMSマニュアル監査、コミュニケーション、是正処置、教育、内部監査
個人情報保護監査責任者	内部監査の計画～実施・報告
システム管理者	自社のPCの初期設定やシステム面の責任を負う。
事務取扱担当者	当社規程に従い、PMS維持するための特定個人情報の管理について責任を負う。
窓口責任者	開示請求や苦情等の問合せ対応全般について責任を負う。

ノートパソコン類について

ノートPC、情報機器は**<u>所属長の許可を得て</u>**社外に持ち出す。
その場合、機器の起動パスワード設定や格納された情報（データ）へのパスワード設定/暗号化の処置を施す。

スクリーンセーバーの設定

（デスク離席時の情報漏洩を防ぐため、スクリーンセーバー設定を義務付け）

詳細は、各リンクを参照のこと。
離席して15分以内にスクリーンセーバーが表示されるよう設定。

設定方法については、下記のリンクを参照のこと。

Windows10を使用している場合
https://faq.nec-lavie.jp/qasearch/1007/app/servlet/relatedqa?QID=017754

Windows7を使用している場合
https://faq.nec-lavie.jp/qasearch/1007/app/servlet/relatedqa?QID=010717

電子記憶媒体（USB、SDカード等)の持ち出し

（社外に電子記憶媒体を持ち出す際には暗号化したものを使用すること）

業務上、個人情報を格納した電子記憶媒体は、**社外への持ち出しを原則禁止**する。
持ち出しがやむを得ない場合は、業務上必要なものに限り**所属長の許可を得て**持ち出すこととし、
搬送中は常に携帯する。

理解度テストURL

資料のご確認ありがとうございます。
下記URLより理解度テストへお進みください。

https://forms.gle/D8VQpsz7L666QSsH9