

個人情報保護研修テキスト

2022年7月

株式会社フリースタイル

1. なぜ個人情報の保護が必要なのか？

個人情報保護は、何が基準になるのか？

フリースタイルでは、個人情報保護するために、
次の2つを遵守します

1. 個人情報保護に関する法律（個人情報保護法）
2. JIS Q 15001 : 2017（個人情報保護に関するJIS規格）

【法令等の改正内容】

a. 法令関連

個人情報保護に関する法律が改正され、2022年4月から施行されています。

<https://elaws.e-gov.go.jp/document?lawid=415AC0000000057>

b. 2022年4月の改正個人情報保護法の施行により、Pマークの審査基準も大幅に見直しがされます。

旧審査基準：JIS Q 15001 : 2017 の附属書 A の要求事項を満たしていること

新審査基準：JIS Q 15001 : 2017 の附属書 A および本文の要求事項を満たしていること

c. 参考資料

1) プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針(JIPDEC 2022.4.28)

<https://privacymark.jp/system/guideline/outline.html>

2) 構築・運用指針と(現行)審査基準との対照表(JIPDEC 2022.2.14)

https://privacymark.jp/system/guideline/pdf/pm_shishin_taisyo20220428.pdf

個人情報保護の目的について

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



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！

2. 個人情報の事故を起こしてしまうと

個人情報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

- 取引の減少
- 経営状況の悪化

最悪の場合、
事業終了も・・・



3. 法令他

<令和4年>

4月1日

「個人情報の保護に関する法律等の一部を改正する法律」施行

「デジタル社会の形成を図るための関係法律の整備に関する法律」施行

（令和2年改正法による改正後の個人情報保護法の全面施行及び令和3年改正法による改正後の個人情報保護法（行政機関・独立行政法人等に係る部分）の施行）

「個人情報保護法」とは

「個人情報保護法」とは

平成29年5月30日から、すべての事業者に「個人情報保護法」が適用されています！



個人情報保護法とは？

- ✓ 個人の権利・利益の保護と個人情報の有用性(社会生活やビジネス等への活用)とのバランスを図るための法律
- ✓ 民間事業者の個人情報の取扱いについて規定
- ✓ 従来は、取り扱う個人情報の数が5,000人分以下の事業者には適用されていませんでしたが、平成29年5月30日からは、すべての事業者に適用されています



出典: 個人情報保護委員会 「はじめての個人情報保護法」より

フリースタイルが守るべき4つのルール

事業者が守るべき4つのルール

① 取得・利用

- 利用目的を特定して、その範囲内で利用する。
- 利用目的を通知又は公表する。



勝手に使わない!

② 保 管

- 漏えい等が生じないように、安全に管理する。
- 従業者・委託先にも安全管理を徹底する。(持ち運ぶ場合も要注意)



なくさない! 漏らさない!

③ 提 供

- 第三者に提供する場合は、あらかじめ本人から同意を得る。
- 第三者に提供した場合・第三者から提供を受けた場合は、一定事項を記録する。



勝手に人に渡さない!

④ 開示請求等への対応

- 本人から開示等の請求があった場合はこれに対応する。
- 苦情等に適切・迅速に対応する。



お問合わせに対応!

(※) ②～④は個人情報をデータベース化(特定の個人を検索できるようにまとめたもの)した場合にかかるルールです。
なお、これらの個人情報データベース等を構成する個人情報を、「個人データ」といいます。

出典: 個人情報保護委員会 「はじめての個人情報保護法」より

令和2年改正個人情報保護法の概要

1. 個人の権利の在り方

- ・ 利用停止・消去等の個人の請求権について、一部の法違反の場合に加えて、個人の権利又は正当な利益が害されるおそれがある場合にも拡充する。
- ・ 保有個人データの開示方法（現行、原則、書面の交付）について、電磁的記録の提供を含め、本人が指示できるようにする。
- ・ 個人データの授受に関する第三者提供記録について、本人が開示請求できるようにする。
- ・ 6ヶ月以内に消去する短期保存データについて、保有個人データに含めることとし、開示、利用停止等の対象とする。
- ・ オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外とする。

（※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

2. 事業者の守るべき責務の在り方

- ・ 漏えい等が発生し、個人の権利利益を害するおそれ大きい場合（※）に、委員会への報告及び本人への通知を義務化する。
（※）一定の類型（要配慮個人情報、不正アクセス、財産的被害）、一定数以上の個人データの漏えい等
- ・ 違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する。

3. 事業者による自主的な取組を促す仕組みの在り方

- ・ 認定団体制度について、現行制度（※）に加え、企業の特定分野(部門)を対象とする団体を認定できるようにする。

（※）現行の認定団体は、対象事業者の全ての分野（部門）を対象とする。

4. データ利活用の在り方

- ・ 氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和する。
- ・ 提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける。

5. ペナルティの在り方

- ・ 委員会による命令違反・委員会に対する虚偽報告等の法定刑を引き上げる。
- ・ 命令違反等の罰金について、法人と個人の資力格差等を勘案して、法人に対しては行為者よりも罰金刑の最高額を引き上げる(法人重科)。

6. 法の域外適用・越境移転の在り方

- ・ 日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収・命令の対象とする。
- ・ 外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等を求める。

出典：個人情報保護委員会「個人情報保護法 令和2年改正及び令和3年改正案について」より

令和4年4月1日以降のチェックポイント

**令和4年4月1日
改正個人情報保護法対応
チェックポイント**

まずはここから！
万が一に備え
漏えい等報告・
本人通知の手順
を整備しましょう

まずはここから！
個人データを
外国の第三者へ
提供しているか
確認しましょう

まずはここから！
安全管理措置
を公表する等
本人の知り得る状態
に置きましょう

保有個人データを
棚卸し、開示請求等
に備えましょう

個人情報を
不適正に利用
していないか
確認しましょう

個人関連情報の
利用状況や提供先を
確認しましょう

改正内容を確認し、プライバシーポリシーの改訂等が必要な場合は対応しましょう

個人情報保護委員会

個人情報保護委員会
Personal Information Protection Commission
<https://www.ppc.go.jp/>

出典：個人情報保護委員会

4. 個人情報とは

個人に関する情報（１）

「個人情報」とは

個人情報

生存する個人に関する情報で、
特定の個人を識別することができるもの

（例）「氏名」、「生年月日と氏名の組合せ」、「顔写真」等

（※その情報単体でも個人情報に該当することとした「個人識別符号」も個人情報に該当します。）

顧客情報だけでなく、従業員情報や取引先の名刺といったものも個人情報です。



「個人識別符号」とは？

☑ 以下①②のいずれかに該当するものであり、政令・規則で個別に指定されています

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

⇒DNA、顔認証データ、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋

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(公的な番号)

⇒旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー等

出典：個人情報保護委員会「はじめての個人情報保護法」より

個人に関する情報（２）

個人情報

生存する特定の個人を識別できる情報

- ・ 個人識別符号が含まれるもの
- ・ 他の情報と容易に照合でき、その結果特定の個人を識別できる情報も含む

例）従業員情報、免許証番号、指紋認証データ等

要配慮個人情報

- ・ 不当な差別、偏見その他の不利益が生じないように取扱いに配慮を要する情報として、法律・政令に定められた情報

例）人種、信条、社会的身分、病歴、
犯罪の経歴、犯罪被害の事実等

個人データ

「個人情報」のうち、紙媒体、電子媒体を問わず、特定の個人情報を検索できるように体系的に構成したもの
（箱ファイル管理、データベース管理等）

保有個人データ

「個人データ」のうち、開示、訂正、消去等の権限を有するもの

個人に関する情報（３）

個人関連情報

個人情報

仮名加工情報

（令和２年改正で追加）

他の情報と照合しない限り特定の個人を識別することができないように加工された個人に関する情報

- a. 個人情報に含まれる記述等の一部を削除（変換を含む）すること
- b. 個人識別符号の全部を削除（変換を含む）すること

（対照表と照合すれば本人が分かる程度まで加工されたもの）

個人情報である仮名加工情報

個人情報ではない仮名加工情報

個人関連情報

生存する個人に関する情報であって、個人情報、仮名加工情報、匿名加工情報のいずれにも該当しないもの

匿名加工情報

特定の個人を識別することができず、加工元の個人情報を復元することができないように加工された個人に関する情報
（本人が一切分からない程度まで加工されたもの）

フリースタイルでは、取り扱いはない

個人に関する情報（４）

（参考）個人情報・仮名加工情報・匿名加工情報の対比（イメージ）

	個人情報※１	仮名加工情報※２	匿名加工情報※２
適正な加工 （必要な加工のレベル）	—	<ul style="list-style-type: none"> 他の情報と照合しない限り特定の個人を識別することができない 対照表と照合すれば本人が分かる程度まで加工 	<ul style="list-style-type: none"> 特定の個人を識別することができず、復元することができない 本人が一切分からない程度まで加工
利用目的の制限等 〔利用目的の特定、制限、 通知・公表等〕	○	○ ・利用目的の変更は可能 ・本人を識別しない、内部での分析 ・利用であることが条件	× （規制なし）
利用する必要がなくな ったときの消去	○ （努力義務）	○ （努力義務）	× （規制なし）
安全管理措置	○	○	○ （努力義務）
漏えい等報告等	○ （改正法で義務化）	× （対象外）	× （対象外）
第三者提供時の 同意取得	○	— （原則第三者提供禁止）	× （同意不要）
開示・利用停止等 の請求対応	○	× （対象外）	× （対象外）
識別行為の禁止	—	○	○

※１：個人データ、保有個人データに係る規定を含む。 ※２：仮名加工情報データベース等、匿名加工情報データベース等を構成するものに限る。

出典：厚生労働省「（参考）個人情報保護法 令和2年改正及び令和3年改正について」

5. フリースタイルでの 個人情報の取扱いについて

個人情報保護方針（内部向け、外部向け）

株式会社フリースタイル(以下、「当社」)は、以下のとおり個人情報保護方針を定め、個人情報保護の社内規程及び体制を確立し、全従業員に個人情報保護の重要性の認識と取組みを徹底させることにより、当社が行う全ての業務上で使用する個人情報について、以下の方針に従って、これを実行し維持することを宣言いたします。

【基本方針】

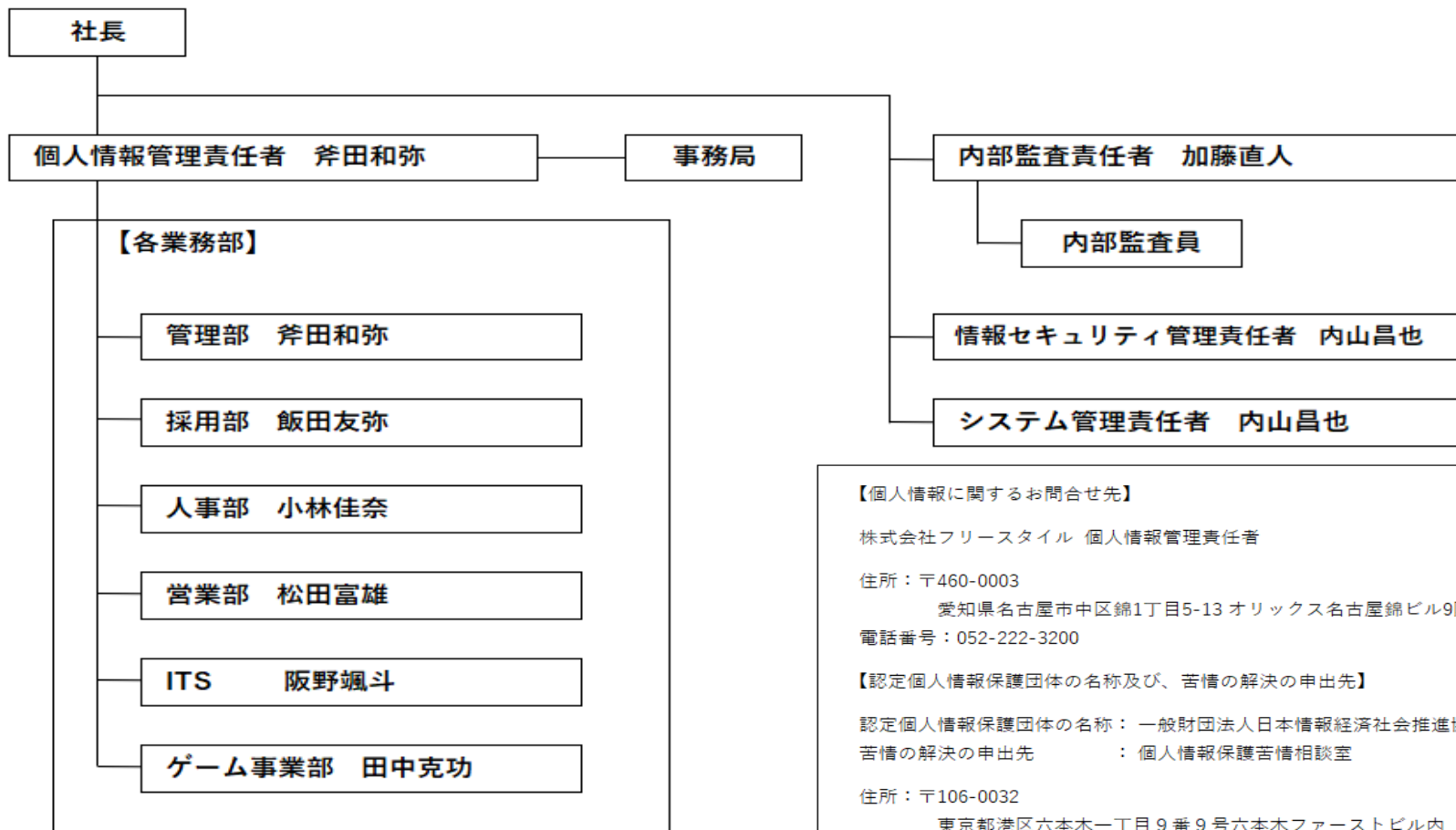
1. 当社は、当社の行う事業で取扱う個人情報及び雇用等において、取扱う個人情報の特定された利用目的の範囲の中で個人情報の適切な取得・利用を行い、利用目的の達成に必要な範囲を超えた個人情報の取扱い(目的外利用)を行わないこと及びそのための措置を講じます。
2. 当社は個人情報の取扱いに関する法令、国が定める指針及びその他の規範を遵守します。
3. 当社は個人情報への不正アクセス、個人情報の漏えい、滅失又はき損の防止を行い、不適切な事項については是正を行うなどの内部規程を定め、個人情報を保護します。
4. 当社は個人情報の取扱いに関する苦情及び相談対応への内部規程を定め、苦情及び相談に対応します。
5. 当社は個人情報保護マネジメントシステム(PMS)の継続的改善を行います。

株式会社フリースタイル 代表取締役 青野 豪淑

個人情報保護の社内体制

2022年4月8日

個人情報保護推進体制



【個人情報に関するお問合せ先】

株式会社フリースタイル 個人情報管理責任者

住所：〒460-0003

愛知県名古屋市中区錦1丁目5-13 オリックス名古屋錦ビル9階

電話番号：052-222-3200

【認定個人情報保護団体の名称及び、苦情の解決の申出先】

認定個人情報保護団体の名称：一般財団法人日本情報経済社会推進協会

苦情の解決の申出先：個人情報保護苦情相談室

住所：〒106-0032

東京都港区六本木一丁目9番9号六本木ファーストビル内

電話番号：03-5860-7565 0120-700-779

※当社の商品・サービスに関する問合せ先ではございません。

個人情報保護推進体制の役割

個人情報保護推進体制では、
PMS(個人情報保護マネジメントシステム)の構築と
運用、および継続的な改善を行います。

【プライバシーマーク（Pマーク）の取得について】

PMS が、
「JIS Q 15001 : 2017」の本文と附属書Aを満たしている場合、
JIPDEC（または 認定個人情報保護団体）による PMS の審査後、
P マークの取得、および P マークが使用できるようになります

JIPDEC : 一般社団法人 日本情報経済社会推進協会
中部産業連盟 : 認定個人情報保護団体として、
フリースタイルの PMS の審査を行っている団体

個人情報保護に関する規程

【社内規程】

P111-3.1-A-2個人情報保護規程

緊急事態への対応（１）

従業員は、以下の事項に該当する事態が発生した場合、速やかに部門責任者へ連絡を行い、対応方法を確認する

① セキュリティ事件

PMSに対するルール違反

例）個人情報の勝手な持出し、個人情報の漏洩など

② セキュリティ事故

PMSに規定する個人情報、及び業務に関する欠陥・不具合・故障等の発生

例）ウィルス感染、ネットワーク機器の故障など

③ 情報セキュリティの弱点

PMSで定められた対策では個人情報を守れない状態

例）リスク対策実施時の考慮もれの脅威や脆弱性により
個人情報危険な状態になる恐れがある場合など

④ ソフトウェアの誤動作

使用しているソフトウェアが予期しない動きを行った場合

例）ウィルスによるソフトの誤動作、ソフトのバグなど

緊急事態への対応（２）

【関係者および関係機関への報告】[←]

部門の責任者は、以下の関係者へ報告する。[↓]

No. [←]	連絡先 [←]	レベル [←]		
		1 [←]	2 [←]	3 [←]
1 [←]	事務局 [←]	○ [←]	○ [←]	○ [←]
2 [←]	個人情報保護管理者 [←]	○ [←]	○ [←]	○ [←]
3 [←]	社長	←	○ [←]	○ [←]
4 [←]	「緊急連絡先一覧表」に登録されている関係機関 [←]	←	○ [←]	○ [←]

※○は要連絡[←]

【緊急の度合い(レベル)】[←]

- レベル 1（深刻度：低） ⇒ 部門[←]
問題の発生原因・被害の範囲とも一部門に限定される場合。[←]
- レベル 2（深刻度：中） ⇒ 会社全体[←]
セキュリティ侵害により、会社全体が被害者となる場合。[←]
- レベル 3（深刻度：高） ⇒ 本人、顧客、取引先[←]
本人や顧客、取引先等に被害を与える場合。[←]

緊急事態への対応（3）

【緊急連絡先一覧】

緊急連絡先は、
個人情報保護規程内「3.3.7 緊急事態への準備」に記載された連絡先で
次の連絡先は、その中の一部になります。

機関 [↵]	窓口 [↵]	連絡先 [↵]
中警察署（愛知県） [↵]	----- [↵]	052-241-0110 [↵]
情報処理推進機構（IPA） [↵]	----- [↵]	http://www.ipa.go.jp/index.html [↵]
JPCERT/CC [↵]	----- [↵]	http://www.jpccert.or.jp/ [↵]
個人情報保護委員会 [↵]	----- [↵]	http://www.ppc.go.jp/ [↵]
一般社団法人中部産業連盟 [↵]	Pマーク審査センター [↵]	052-931-7701 [↵]
日本情報経済社会推進協会（JIPDEC） [↵]	プライバシーマーク事務局 [↵]	03-5860-7563 [↵]
社団法人日本情報システム・ユーザー協会（JUAS） [↵]	セキュリティセンター [↵]	03-3249-4103 [↵]

罰則

個人情報情報の漏えい等に関する罰則

1. 令和2年 個人情報保護法の改正後の罰則内容（法令によるもの）

- a. 個人情報保護委員会の措置命令への違反(個人情報保護法42条2項・3項違反)
 - 個人：1年以下の懲役又は100万円以下の罰金
 - 法人：1億円以下の罰金
- b. 虚偽報告等の報告義務違反(個人情報保護法40条 1 項および同法56条の規定違反)
 - 個人：50万円以下の罰金
 - 法人：50万円以下の罰金
- c. 個人情報データベース等の不正流用
 - 個人：1年以下の懲役又は50万円以下の罰金
 - 法人：1億円以下の罰金

改正前後の法定刑の比較

表1 改正前後の法定刑の比較

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反	行為者	6 月以下	1 年以下	3 0 万円以下	100 万円以下
	法人等	-	-	3 0 万円以下	1 億円以下
個人情報データベース等の不正提供等	行為者	1 年以下	1 年以下	5 0 万円以下	5 0 万円以下
	法人等	-	-	5 0 万円以下	1 億円以下
個人情報保護委員会への虚偽報告等	行為者	-	-	3 0 万円以下	5 0 万円以下
	法人等	-	-	3 0 万円以下	5 0 万円以下

2. 就業規則の罰則内容

就業規則 第 7 章 賞罰に従う

出典:個人情報保護委員会「令和2年改正個人情報保護法について」より

6. 事故の事例

頻発する個人情報の漏えい等の事故防止が必要

- 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
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

2020年度の事故報告概要

■ 発生件数別の傾向

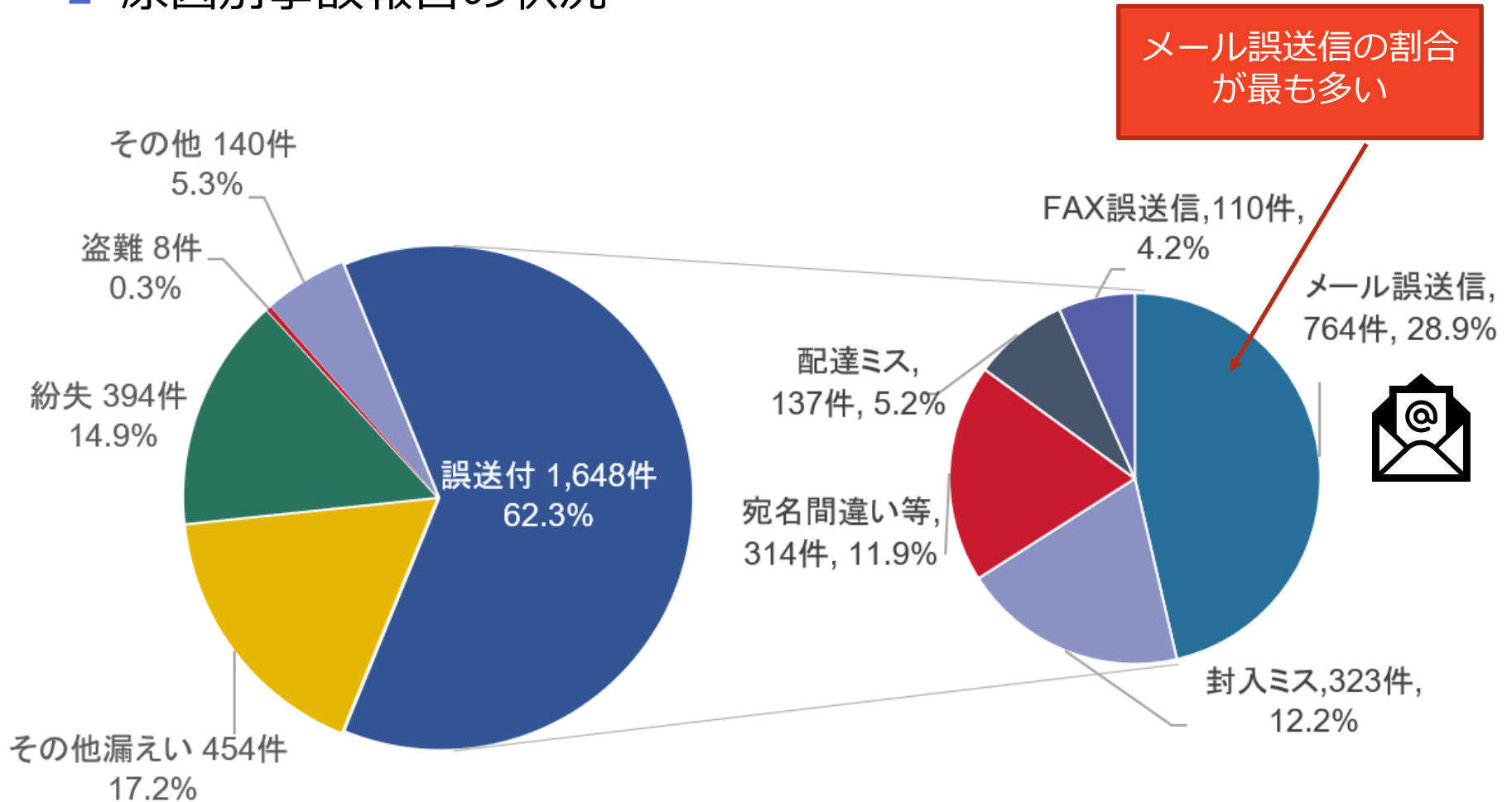
- 「誤送付」（1,648件：62.3%）が最も多く、次に「その他漏えい」（454件：17.2%）の順。
- 「誤送付」のうち、「メール誤送信」（764件：28.9%）が最も多く、昨年度より大きく増加。
- 「その他漏えい」のうち、「関係者事務処理・作業ミス等」（232件）が過去5か年で最も多い。

■ 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。

発生件数別の傾向（１）

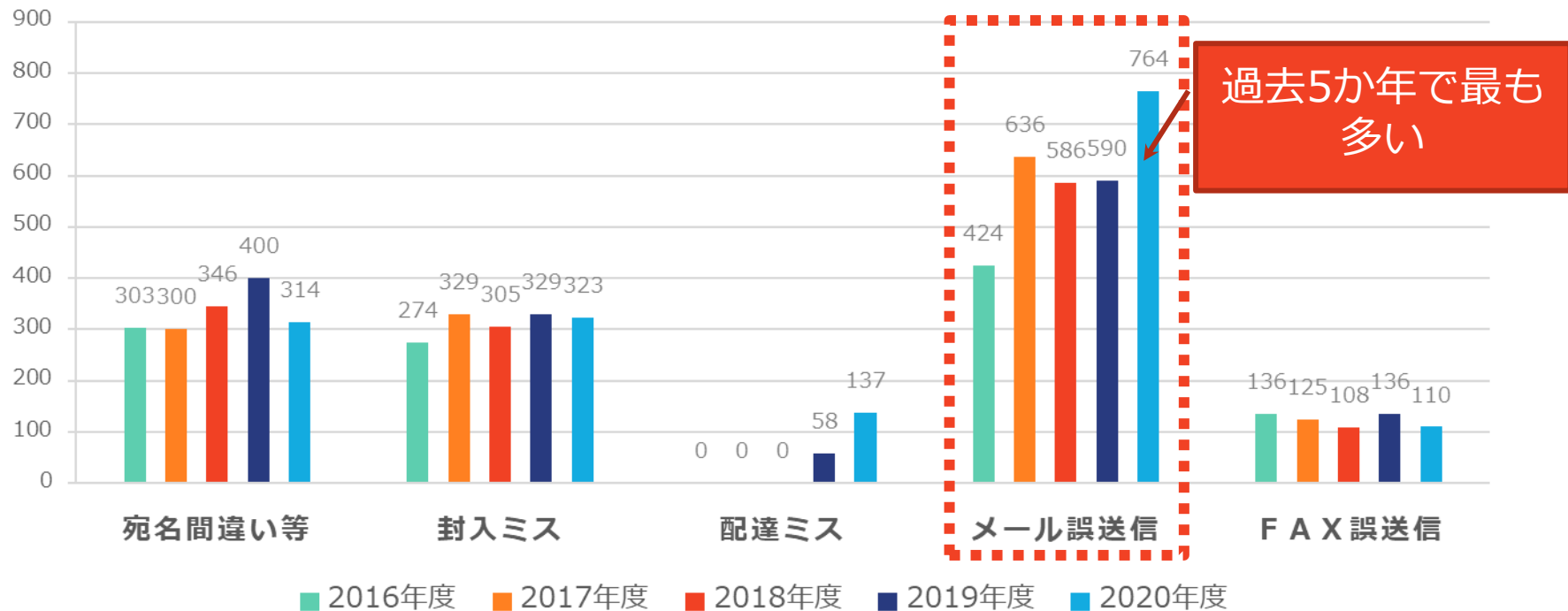
■ 原因別事故報告の状況



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」

発生件数別の傾向（２）

■ 「誤送付」の内訳推移

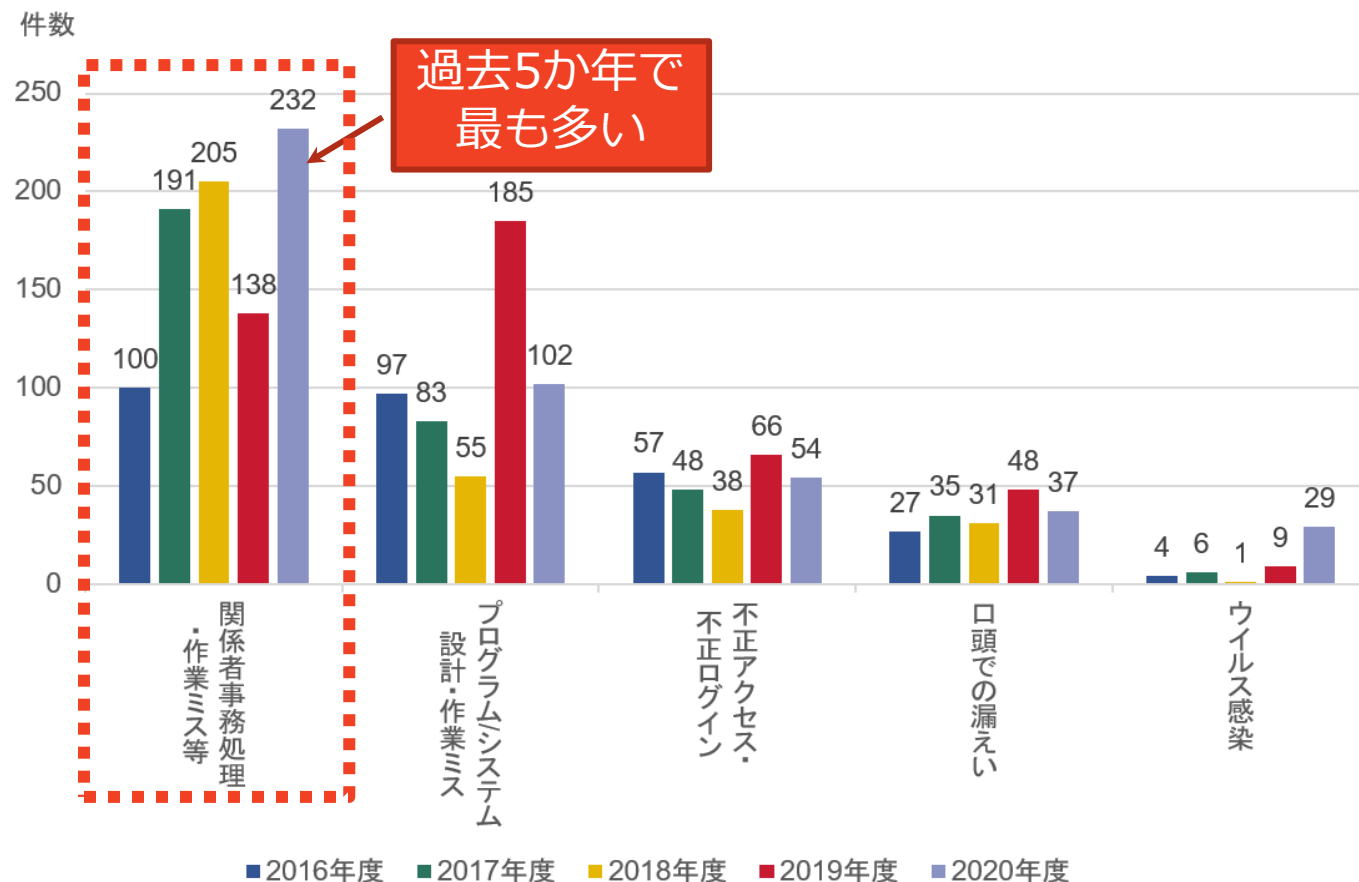


テレワークの実施、メッセージングサービスなど新たなコミュニケーションツールの利用などにより、メール誤送信は増加。
業務環境や手順が変化したときには、注意が必要。

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」

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」

事故の発生傾向

- 継続して発生している事例がある一方、
「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」にも変化が見られる。

- 特に注意したい事事故事例
 1. ソーシャルエンジニアリング
 2. 設定ミスによる誤公開
 3. ランサムウェア
 4. 環境変化による事故
(テレワーク、出社制限など)

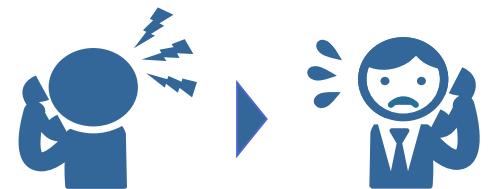
特に注意したい事故事例（１）

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（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利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（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（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） 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	<ul style="list-style-type: none">・ 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	<ul style="list-style-type: none">・ 各業務における「間違える可能性のある場面とチェックポイント」の洗出し<ul style="list-style-type: none">➢ イレギュラー処理の場合こそ、チェックが重要<ul style="list-style-type: none">・ 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<ul style="list-style-type: none">・ 指差し確認、声出し確認
物品・書類の管理	<ul style="list-style-type: none">・ 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	<ul style="list-style-type: none">・ 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	<ul style="list-style-type: none">・ 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	<ul style="list-style-type: none">・ 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に、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。

個人情報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：テレワーク端末の踏み台化

2020年5月、リモートアクセスを利用した個人所有端末から正規のアカウントとパスワードが盗まれ、オフィスネットワークに不正アクセスされた案件が発生。仮想デスクトップ（VDI）によるリモートアクセスシステムを利用していたものの、個人所有端末自体が攻撃者の踏み台として乗っ取られていたために、VDIサーバ経由で自組織内のファイルサーバを閲覧されたおそれがあり、180社以上の顧客に影響が出るおそれがあると発表。

出典：総務省「テレワークセキュリティガイドライン（第5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 **2万8,308円**
(3か年平均)

出典：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」

個人情報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・・・？



7. 事故を起こさないために行うこと

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

従業員は

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
ルール化や対策の実施

従業員は

事故発覚・発見時に
ルールに従って行動する



委託先の監督も必要になります

ウェブサイトの運営を外部委託している事業者の皆様

委託先を監督してますか？

ウェブサイト等の構築や運営にあたり、個人データの取扱いの全部又は一部を外部の業者に委託する場合は、個人データの安全管理が図られるよう委託先に対する必要かつ適切な監督を行わなければなりません。

当委員会には、不正アクセス（※1）によるECサイトや会員用ウェブサイトにおける情報漏えい事案が多く報告されており、不正アクセスに対するセキュリティ対策について、委託先に任せっきりにせず委託元の事業者も取り組む必要があります。

個人データの委託先への提供にあたり
次の事項に留意してください

1 適切な委託先の選定

委託先において、適切な安全管理措置（※2）が確実に実施されていることを事前に確認する必要があります。

2 委託契約の締結

業務の委託にあたり、個人データの取扱いに関する、必要かつ適切な安全管理措置について、委託元・委託先が双方同意した内容と共に、委託先における委託された個人データの取扱い状況を委託元が把握できる内容を契約に盛り込みましょう（※3）。

3 委託先における個人データ取扱状況の把握

委託元は委託先に対し、個人データの取扱状況について、定期的な監査等により、委託契約で盛り込んだ内容の実施状況を把握しましょう。

なお、委託先が別の業者に再委託を行い個人データを提供する場合、委託先と同様の監督が必要となります。

※1 不正アクセスに関する注意喚起についてはこちらを参考にしてください。
(https://www.ppc.go.jp/news/careful_information/)

※2 安全管理措置についてはこちらを参考にしてください。
(<https://www.ppc.go.jp/personalinfo/hiyarihatto/>)

※3 一般的な業務委託契約にはセキュリティに関する項目が含まれていないことが多いので、確認の上、セキュリティ対策を盛り込む必要があります。



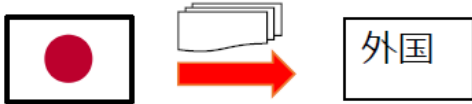
個人情報保護委員会
Personal Information Protection Commission

出典: 個人情報保護委員会

外国への提供にも注意が必要（１）

1. 外国にある第三者に個人データを提供する場合の規制の概要 （１）概要

- 令和２年個人情報保護法改正において、外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める改正が行われました。

現 行	令和４年４月以降
 <p>外国にある第三者に個人データを提供できる要件※</p> <ul style="list-style-type: none">本人の同意基準に適合する体制を整備した事業者我が国と同等の水準の個人情報保護制度を有している外国	<p>各要件に基づく移転時、それぞれ以下を義務付け</p> <div><p>本人からの<u>同意取得時</u>に、以下の情報を提供（第28条第2項）</p><ul style="list-style-type: none">・ 移転先の<u>所在国の名称</u>・ 当該<u>外国における個人情報の保護に関する制度</u>・ 移転先が講ずる<u>個人情報の保護のための措置</u></div> <div><p>1) 移転元に対し以下の必要な措置を求める</p><ul style="list-style-type: none">・ 移転先における<u>適正取扱いの実施状況等の定期的な確認</u>・ 移転先における適正取扱いに<u>問題が生じた場合の対応</u><p>+</p><p>2) <u>本人の求めに応じて</u>必要な措置等に関する情報を提供（第28条第3項）</p></div>

※この他、「法令に基づく場合」等の例外要件があります。

出典：個人情報保護委員会「改正越境移転規則の施行に向けて」より

外国への提供にも注意が必要（２）

1. 外国にある第三者に個人データを提供する場合の規制の概要

（４）我が国と同等水準の個人情報保護制度を有している外国にある事業者提供する場合

「我が国と同等の水準の個人情報保護制度を有している外国」とは、現時点においては以下の国をいいます。

アイスランド	アイルランド	イタリア	英国
エストニア	オーストリア	オランダ	キプロス
ギリシャ	クロアチア	スウェーデン	スペイン
スロバキア	スロベニア	チェコ	デンマーク
ドイツ	ノルウェー	ハンガリー	フィンランド
フランス	ブルガリア	ベルギー	ポーランド
ポルトガル	マルタ	ラトビア	リトアニア
リヒテンシュタイン	ルーマニア	ルクセンブルク	50音順

※ 平成31年個人情報保護委員会告示第1号

出典：個人情報保護委員会「改正越境移転規則の施行に向けて」より

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

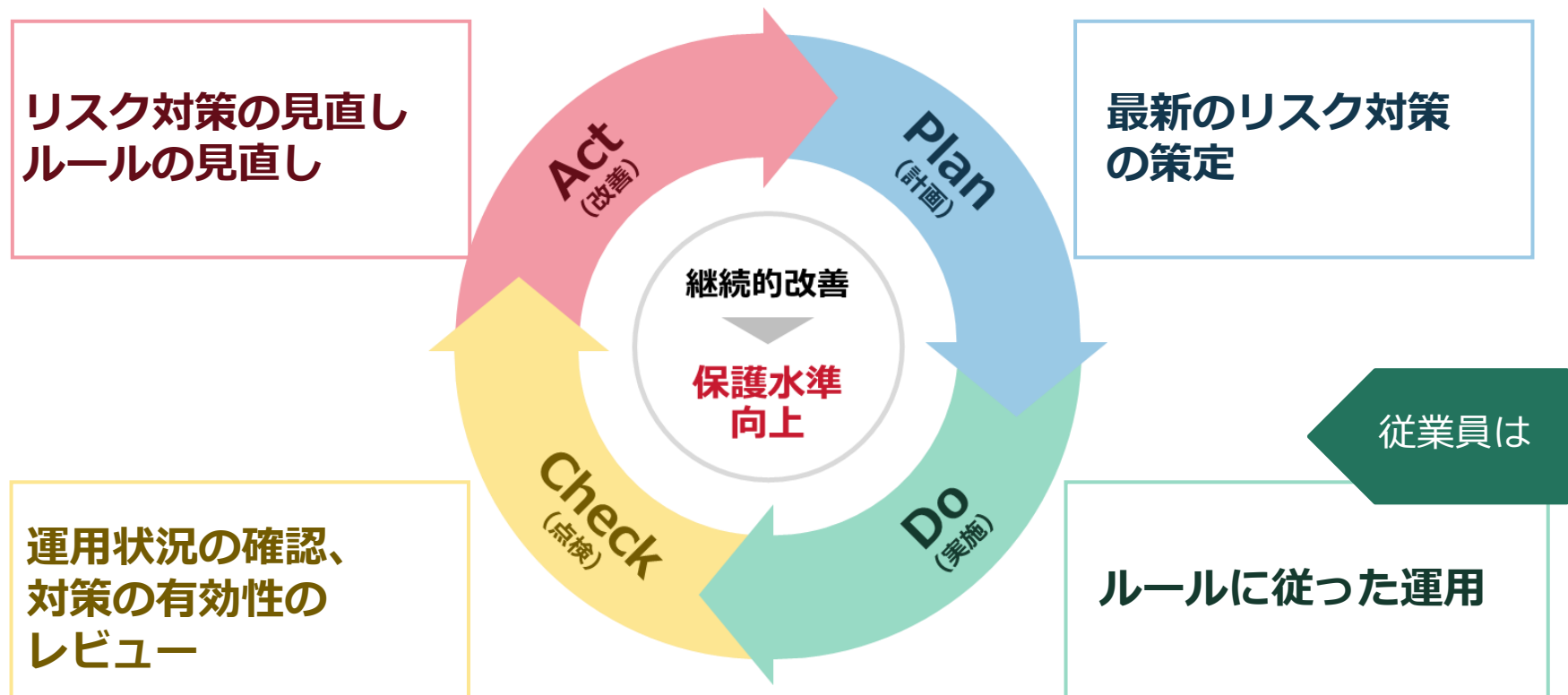
適正な改善策、再発防止策の策定と
実施を徹底



保護水準のさらなる向上

事故防止のために継続的な改善が必要

- 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



8. 2022年の研修内容

2022年 研修内容

2022年の個人情報保護、情報セキュリティ研修の内容

研修受講期間：2022年 7月 1日～2022年 7月31日

研修受講内容：研修テキストによる研修

- ・ 01 個人情報保護研修テキスト_202207
- ・ 02 情報セキュリティ研修テキスト_202207

研修修了基準：確認テストで70%以上の正解率

サイトURL：fs-security-training-documents.herokuapp.com