

個人情報保護定期教育

〈個人情報保護マネジメントシステム教材〉

株式会社イカイコントラクト

2023年10月～12月

AGENDA

- ▶ はじめに
- ▶ 個人情報とは
- ▶ 個人情報保護教育の4つの目的
 - 1)個人情報保護方針
 - 2)個人情報保護の重要性
 - 3)個人情報保護における自分の役割と責任
 - 4)個人情報保護に違反した際に予想される結果
- ▶ 通常業務で実施すること
 - 1) PC・情報機器の使用ルール
 - 2) 保管・廃棄のルール
 - 3) クリアデスク・クリアスクリーン
 - 4) 緊急時の対応
 - 5) テレワーク時のイレギュラーオペレーションとリスク要因による注意
- ▶ 株式会社イカイコントラクト 個人情報保護体制
- ▶ 理解度テスト

はじめに



当社は個人情報について適切な取り扱いが行われている事業者として、
2022年2月1日にプライバシーマークの付与認定を受けています。

- ▶ **個人情報は本人の生活や社会的地位、評価に大きな影響を及ぼすもので、厳重な取り扱いが必要です！**
- ▶ 個人情報は紙や電子データ、あるいは伝聞の形でやり取りをされ、様々な方法で利用、保管されています。**情報は一度外部へ流出すると回収は不可能に近い性質のものであり、不正な漏えいは取り返しのつかない事態に発展する恐れがあります。**
- ▶ 本教育を通じて、個人情報の意識を持つことが、結果的に組織や自身の保護につながることを認識してください。

個人情報とは①

個人情報の定義（JISQ15001:2017）

個人に関する情報であって、当該情報に含まれる氏名、生年月日、性別、住所など特定の個人を識別できる情報、または個人別に付けられた番号、記号その他の符号、画像もしくは音声によって当該個人情報を識別できるもの（当該個人情報だけでは識別できないが、その他の情報と容易に照合することができ、それによって当該個人情報を識別できるものを含む）

例えば・・・

その情報のみで特定可能なもの
名前、クレジットカード情報、顔の画像、音声データ、銀行口座番号

※該当しない例

「東京都在住、モデル、25歳の女性」
といった、組み合わせても個人を特定できない情報。

他の情報と組み合わせることで特定可能なもの

国籍、人種、本籍、生い立ち、出身、家族構成、続柄、家族の身分事項、家族の職業、本人及び家族の勤務先、職種、地位、学歴、職歴、結婚歴、離婚歴、妊娠経験、出産回数、学業成績記録、犯罪歴（前科）、賞罰、病歴、手術歴、身長、体重、血液型、血圧、身体機能、言語、地方なまり、性癖、趣味、嗜好、特技、志望、資産、所得、支払い税額、取引銀行、営業顧客取引先、土地建物、住居の構造や大きさ、信仰、宗教、支持政党、所属する政党その他の団体名、友人関係

※下線を引いたもの（要配慮個人情報）：

特定の機微な個人情報としてJISQ15001において原則収集を禁止している
特定の個人情報

個人情報とは②（これも個人情報）

入室監視カメラの録画映像



- 例えば、社員名簿に写真が登録されていて照合すれば特定できる場合

留守番電話に架かって来た録音音声



- 個人の特定が可能な場合で録音した情報

番号だけの情報



- 預金番号、クレジットカード番号、社員番号、保険証番号などは、当該企業では容易に照合して特定可能

電話帳の情報



- 住所、氏名、電話番号が公開されている情報

個人情報とは③（業務上の個人情報）

当社での個人情報の取り扱い例

- ▶ 従業員情報（人事労務管理・業務管理等）
- ▶ システム運用に伴う個人情報（お取引先システムなど）
- ▶ 取引先情報（担当者名刺・業務上の連絡、受発注業務）

等…

個人情報は業務内で取り扱うこともあり身近に存在しています。
個人情報について知り、また適切な運用をすることで
重大な事故を防ぎ、安心した取引を行うことができます。

個人情報保護教育の4つの目的

1

個人情報保護方針

2

個人情報保護の重要性および利点を理解する

3

個人情報保護における自分の役割および責任を理解する

4

個人情報保護に違反した際に予想される結果を理解する

個人情報保護教育の4つの目的①

1

個人情報保護方針

個人情報保護の重要性および利点を理解する

個人情報保護における自分の役割および責任を理解する

個人情報保護に違反した際に予想される結果を理解する

①個人情報保護方針

個人情報保護方針

- 必要な公表事項
 - a)取得、利用及び提供
 - b)法令、指針の準拠
 - c)漏洩、滅失等是正
 - d)苦情相談への対応
 - e)PMS継続的改善
 - f)トップマネジメント氏名
 - g)制定日、最終改正日
 - h)問合せ先

※当社の「個人情報保護方針（＝プライバシーポリシー）（右記イメージ）」は、ホームページに公表しています。

URL)
<https://ikai-con.co.jp/privacy/>

QRコード



株式会社イカイコントラクト 個人情報保護方針

株式会社イカイコントラクトは、総合人材サービス事業を営む企業として、個人情報の重要性和多数の個人情報を取り扱う責任の重大性を深く認識し、以下のように個人情報を適正に取り扱うことにより、社会の信頼に応えていきます。

1. 個人情報の保護に関する法令等の遵守
当社は、個人情報の保護に関する法令、国が定める指針その他の規範を遵守します。
2. 個人情報の取得・利用及び提供
当社は、個人情報を取得・利用する場合には、利用目的を明確にし、その利用目的達成のために必要な範囲内において、適法かつ公正な手段によって取得し利用します。また、本人の同意を得ることなく、目的外の利用、第三者への提供は行いません。また、目的外の利用をおこなわないための措置を講じます。
3. 個人情報に対する安全管理措置
当社は、個人情報への不正アクセス、個人情報の漏洩・紛失・棄損等のリスクに対し、万全の安全対策及び是正措置を講じます。従業者や委託先に対しても適切な監督を行います。
4. 個人情報に関する請求、苦情・相談等への対応
当社は、本人からの個人情報の開示・訂正・削除等の請求、個人情報の取扱いに関する苦情・相談等に対し、専用の窓口を設け、適切かつ迅速に対応します。
5. 個人情報の保護の継続的改善
当社は、個人情報に関して一層適切な取扱いをするため、個人情報の保護に関する規程類や管理体制を定期的に見直し、継続的に改善を行います。

平成 29 年 4 月 1 日 制定

令和 2 年 4 月 1 日 最終改訂

代表取締役 伊海 剛志

【当個人情報保護方針についてのお問い合わせ先】

個人情報相談窓口にお問い合わせ下さい。

〒426-0031 静岡県藤枝市築地 1-6-33

株式会社イカイコントラクト 個人情報相談窓口

E-mail: kanri_con@ikaigp.co.jp

TEL: 054-645-1806、FAX: 054-645-1807

個人情報保護教育の4つの目的②



個人情報保護方針



個人情報保護の重要性および利点を理解する



個人情報保護における自分の役割および責任を理解する



個人情報保護に違反した際に予想される結果を理解する

個人情報保護の重要性および利点①

個人情報保護の重要性およびPマーク取得による利点

1. 個人情報の漏えい等事故のリスクの認識と低減
2. 第三者機関から認証されるため、取引先から信頼を得ることができる
3. Pマークを取得した取引先とスムーズに契約が結べる
4. 仕事の受注増加が見込める
5. 社内の個人情報取扱への注意喚起・個人情報保護への意識向上につながる

👉 委託先も同様の管理が必要。

個人情報保護の重要性および利点②

「個人情報保護規程」を確実に運用することのメリット

1. 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
2. 万一、個人情報漏えい事故が発生した場合、その状況を論理的に、かつ、可能な限り正確に説明することができる
3. 万一、個人情報漏えい事故を起こしても、会社の致命傷になることを避けられる

👉 リスクマネジメントとは、主にリスクアセスメントとリスク対応とから成る。例えば個人情報を取得するなどライフサイクル毎に、どんなリスクがあるか、そのリスクに対して、どう対応するか、などです。※ライフサイクル（局面）は、取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄のこと。

個人情報保護教育の4つの目的③



個人情報保護方針



個人情報保護の重要性および利点を理解する



個人情報保護における自分の役割および責任を理解する



個人情報保護に違反した際に予想される結果を理解する

個人情報保護における自分の役割および責任

**経営判断
(リスクを軽減する)**

リスクと投資の
バランスを取る



ルールの作成

- ルールを教育で
周知



人的投資

- 担当者を置く



物的投資

- 鍵付きのロッ
カーを購入



リスクを減じるには
投資が必要。
ただ、いくら投資して
もリスクは“ゼロ”に
なりません。

※会社の状況に合わせたリスク管理が重要である。

個人情報保護教育の4つの目的④



個人情報保護方針



個人情報保護の重要性および利点を理解する



個人情報保護における自分の役割および責任を理解する



4

個人情報保護に違反した際に予想される結果を理解する

個人情報保護に違反した際に予想される結果

■会社（事業者）

- ▶ 法令違反の場合、主務大臣の指導、勧告の対象になる
- ▶ プライバシーマーク企業にあってはマークの停止・はく奪
- ▶ 個人情報の漏えい等事故のリスクが高まる
- ▶ 取引先、消費者の信頼を失う
- ▶ 多額の損害賠償
- ▶ 問合せ対応、二次被害拡大防止等のコスト
- ▶ 事業継続の危機

■当事者本人（個人）

- ▶ 解雇を含む懲戒の対象になる
- ▶ 被害者及び会社から損害賠償を請求される
- ▶ 社会的信用を失う
- ▶ 刑事罰を科される可能性もある



個人情報保護マネジメント
システムに則った
運用が必須!!

通常業務で実施すること

1) PC・情報機器の使用ルール

2) 保管・廃棄のルール

3) クリアデスク・クリアスクリーン

4) 緊急時の対応

5) テレワーク時のイレギュラーオペレーションとリスク要因による注意

1) PC・情報機器の使用、持出・持込ルール

PC・情報機器の利用

- ▶ ■ PC等のパスワードは、他人に教えたり他人に見える箇所に保管しないこと！
 - PCなど、会社支給端末のパスワードは、使用者個人が管理する必要があります。
- ▶ ■ 離席中のPC画面に注意！！長時間離席する場合にはロック画面にする
 - 初期設定で、画面操作がない場合には指定時間（10分を想定）でロック画面になるように設定してください。
設定時間の設定解除および設定変更は**厳禁**です！（ただし、設定時間を短くするのは可）
- ▶ ■ 個人情報を含むファイルを外部へ送信する時は、ファイルにパスワードを設定する
- ▶ ■ 盗難を防ぐ為、ノートPCは事務所に置いて帰る場合、施錠できる場所に保管する
- ▶ 在宅勤務等社外での利用時は外部に見られない様に対応、盗難されない様十分に気を付けること。
 - 盗難・紛失など起きた場合は直ぐに上司、または管理部まで連絡を！！
- ▶ ■ 会社が選定したソフトウェア以外に会社の承認を得ず、無許可でソフトウェアをインストールしないで下さい。
 - ▶ 業務上利用必要なソフトがある場合には個人情報保護管理者(=代表)までご相談ください。
- ▶ ※個人のPCなどを会社に持ち込むことは禁止です。業務上どうしても必要な場合は、個人情報保護管理者の許可を受けてください。また、個人で持ち込んだPCを社内LANにつなぐことは厳禁です。

2) 保管・廃棄のルール

資料の保管・廃棄

- ▶ 個人情報が含まれている紙の資料は、**シュレッダー** により廃棄すること。
 - シュレッダー・溶解のために書類を一時的に保管する場合は、必ず紛失・盗難のおそれのない場所においてください。
- ▶ 個人情報が含まれている資料を保管する場合は、必ず施錠できる場所に保管して帰宅時には必ず施錠すること。
 - 名刺なども、置いたままにせず、鍵のかかる引き出しへ！
- ▶ 個人情報が含まれるPCの廃棄
 - P Cの廃棄は**個人情報保護管理者**で行います。
社内で不要になったPCがある場合には連絡を。
- ▶ 保管する期間が分からない場合は、**個人情報保護管理者**に確認して下さい。

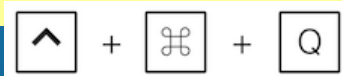
3) クリアデスク・クリアスクリーン

クリアデスク

- ▶ **机上に書類を放置しない。作業場所の整理整頓！**
 - ▶ 機密情報を扱っている作業中に席を離れる場合には、書類を裏返しにするなどして、他者に見られないようにしましょう。
- ▶ 長時間席を離れる、退社する際には、使っていた書類などを片付け（定位置に保管し必要に応じて施錠）、作業が終わっていないからと理由をつけて机の上に書類を放置しないこと。
- ▶ 印刷をした書類は速やかにプリンターから引き上げること。

クリアスクリーン

- 情報をスクリーンに残したまま離席しないこと。
- PC使用中に一時的に席を離れる時には、PC画面が表示されないようにしてから席を離れましょう。
 - ▶ スクリーンのぞき見による情報流出を防ぐ
- Windowsキー+「L」ですぐに画面ロックできます（WindowsPCの場合） + 
※Macでのショートカットキーは「control」+「command」+「Q」キーを同時に押します



4) 緊急時の対応



紛失・盗難など起きた場合には・・・

発覚した時点ですぐに所属の上長あるいは
個人情報保護管理者へ
すぐに連絡を行うこと！！

- 個人情報の流出を最低限に防ぐためには「すぐに」連絡することが重要です

紛失盗難だけでなく、個人情報の取り扱いで気になる点があれば、
遠慮せず、ためらわず

個人情報保護管理者に相談ください



5) テレワーク時のイレギュラーオペレーションとリスク要因による注意

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 (自宅、シェアオフィス等)	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 持出資料管理	・ルール・手順で定められたチェックを行えない ・職場より小さな画面での作業 ・保管場所の確保が難しい ・保管場所のセキュリティが不十分
	その他	・緊張感の維持困難 (気のゆるみ)
出勤制限 (自社・他社)	対応人数の不足	・一人当たりの業務量増加→時間的な余裕の欠如 ・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	・機能について理解不十分なまま、とりあえず使い始めた場合 ・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コンタクトが取れない ・コミュニケーションツールが使いこなせない

(参考) テレワークでの事故事例・注意事項

■ **標的型攻撃や偽サイトへの誘導**（フィッシング）、マルウェア感染などの脅威が増加しています。フィッシング（金融機関やクレジットカード会社等の企業サイトを装った偽のサイトを開設し、そこに誘導することでログインパスワードやクレジットカード番号などを入力させる）

■ **フリーWi-Fiを利用して情報が漏洩**（カフェなどで）。フリーWi-Fiは、セキュリティは高くありません。通信内容が読み取られる怖れがあります。

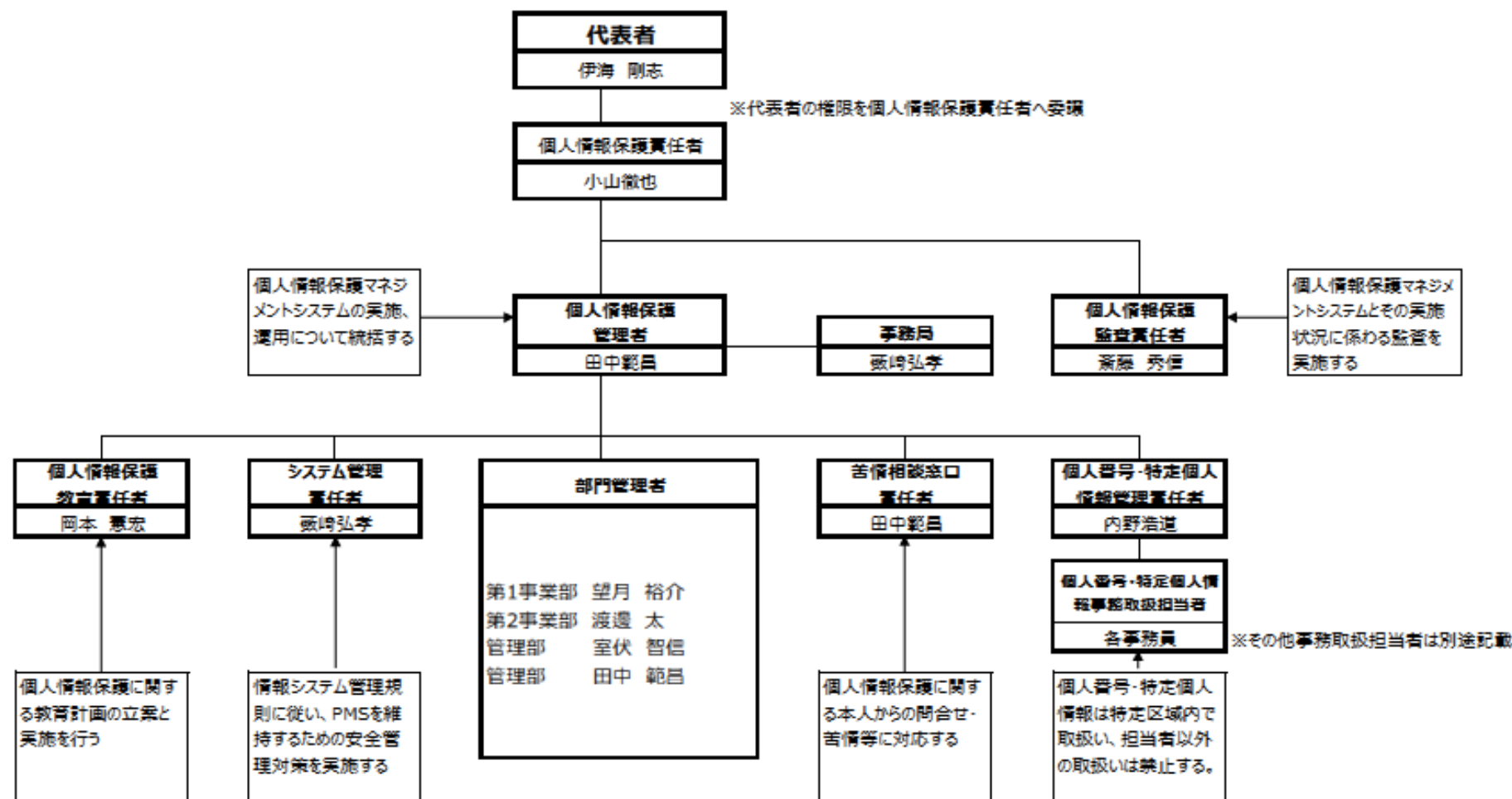
■ **会社から貸与されたパソコンがウイルスに感染**
業務外のウェブサイトを開覧したり、会社で指定されたソフト以外のフリーソフトなどをインストールをしたりすると、ウイルスに感染するリスクが増えます。

■ **自宅に持ち帰る途中でパソコンを紛失**
電車やバスを使って通勤している場合、パソコンを網棚に載せてしまい、そのまま忘れてしまったり、持ち出したパソコンを持ったまま飲みに行ったりして置き忘れ、紛失。

個人情報保護体制図

個人情報保護体制図

2023/4/7



※PMS＝個人情報保護マネジメントシステム

お疲れさまでした

私たちが扱う個人情報、
本人からお預かりしている大切な情報です。

これからも、人任せにすることなく、一人一人が当事者意識をもって、
会社全体として守っていきましょう。

それでは、ひきつづき「理解度テスト」をお受けいただき、教育責任者に回答をご提出ください。

また、2022年の**IPA公表の情報セキュリティ10大脅威（下記URL）**もご覧頂き、今後の運用面において参考にしてください。

URL) <https://www.youtube.com/watch?v=WRIJzdMA5T8>

