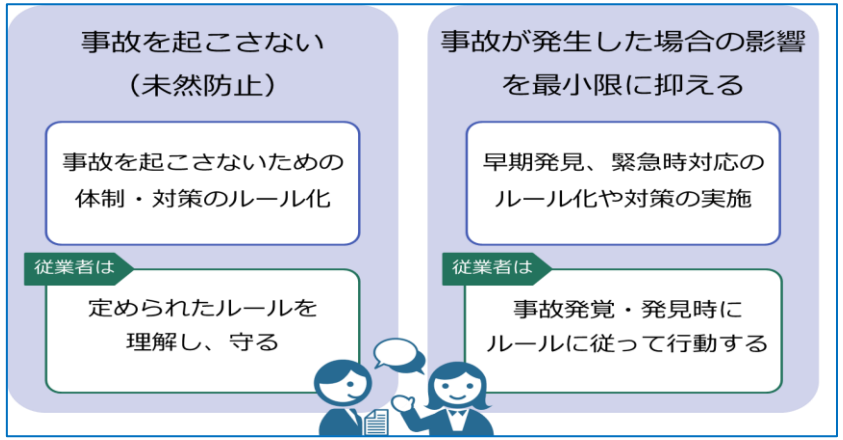
2025年度　情報セキュリティ研修

「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」の目的である「情報の安全な活用」を実現するために、個人情報の取扱いについて確認**【基本動作を徹底】**いただきたい。

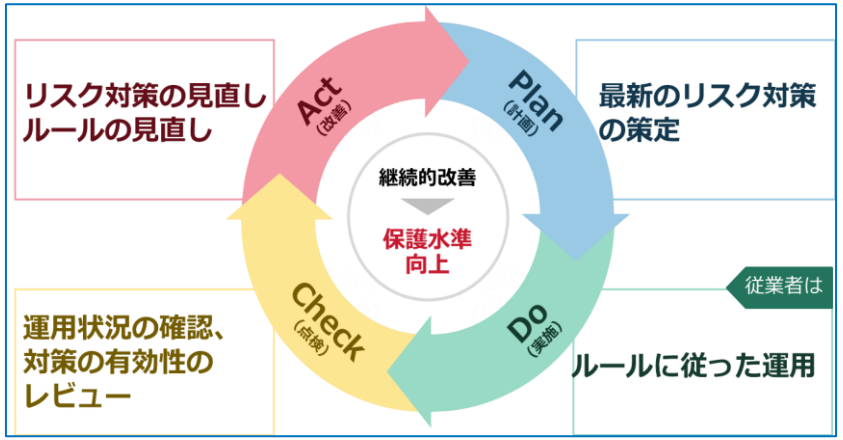
【運用ルールの遵守】

◆各業務での個人情報が、情報管理の各種規程類に即した運用か
◆従事者は、運用ルールを理解し、遵守しているか



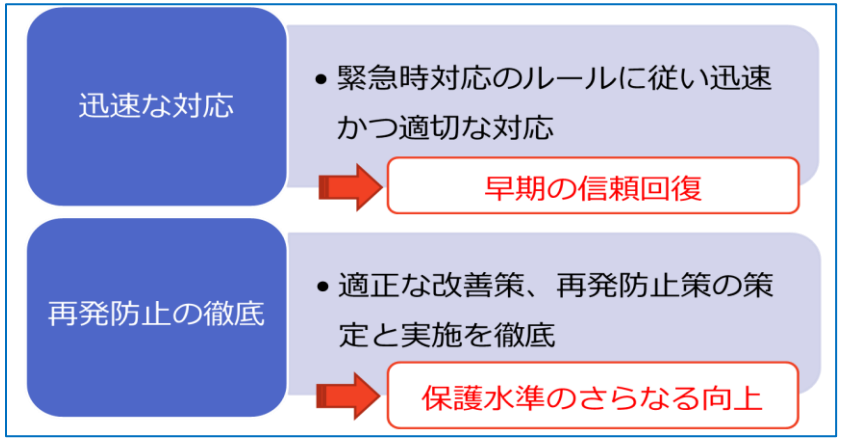
【対象情報の適正な管理・運用】

◆保有期間を終了した個人情報は、適切な方法で廃棄されているか
◆リスク対策された運用フローになっているか（情報取扱時のダブルチェック等）



【事故発生時の対応】

◆事故発生時の担当内、社内の報告先を認知しているか
◆個人情報保護委員会報告対象の事故ではないか



「要配慮個人情報」ってご存じですか？

「要配慮個人情報」とは
◆定義　：本人に対する不当な差別・偏見・その他の不利益が生じないよう、特に慎重な取扱いが必要な個人情報（個人情報保護法 第2条第3項）
◆具体例：人種・信条（宗教、思想など）、社会的身分、病歴・健康診断結果、身体・知的・精神障害に関する情報、犯罪の経歴（前科）、犯罪被害にあった事実、刑事事件や少年保護事件に関する手続き、遺伝子検査結果（ゲノム情報）
◆通常の個人情報との違い：差別や偏見の原因になりやすい情報のため、取扱いに厳しいルールがあり、漏えい時は個人情報保護委員会への報告義務がある
法令違反をした場合、行政処分や刑事罰の対象になる可能性がある

より厳格な管理が求められる「要配慮個人情報」が、あなたの周りに存在していませんか？　もう一度、身のまわりの管理情報を見直してみましょう！

職場におけるセキュリティリスクの把握と対処について

- 2024年度は**51件の情報漏えい事故**が発生しており、年間発生件数としては**集計開始以降最多**、2025年度（第1四半期）についても、既に**7件の情報漏えい事故**が発生しております。

- 事故の未然防止に向けて各自が取り組むべきこと（**基本動作の徹底、危機意識**を持つこと）に加え、各職場において「**業務プロセスの見直しや改善**」を行うことで、**情報漏えいのリスクを軽減**させることができます。以下の内容について話し合ってみましょう。

＜職場ディスカッション内容＞

日常業務に潜んでいるセキュリティリスクを踏まえ、各職場においても同様のリスクがないかを確認し、セキュリティリスクを顕在化させないために職場で何ができるか（対処策）を議論しましょう。

※日常業務に潜んでいるセキュリティリスク（次項以降）より職場の実態に合ったものを1つ以上選定し、
具体的なケース事例【A～E】を参考に職場討議を実施してください。
※本ケース事例は発生した事例内容を参考に変更・簡素化し掲載しており実態と内容が異なる場合がございます。

■項目1　情報漏えいのケースを各職場において確認し、類似の情報漏えいリスクがないか共有を行う
（担当でどのような重要情報を扱っており、内部不正・ルール未遵守・不正アクセス等により漏えいするリスクがないか検討）

■項目2　自担当において、情報漏えいリスクへの対処策としてどのような取り組みができるか共有を行う
（情報漏えいリスクへの対処として、職場における業務改善「業務プロセス見直し等」の取り組みを検討）

日常業務に潜んでいるセキュリティリスク

お客様情報や個人情報等、各職場において取り扱うケースがあると思いますが、**情報漏えいに繋がりやすい以下のケースは特にご注意ください。**

注意を要するケース	例）潜んでいるセキュリティリスク（脅威源×脆弱性）	注意すべきポイント
ケース事例A　ケース事例B ①委託先等への業務委託実施時	委託先従業員のミス等 × 委託先管理の不備 ＝ 委託先からの漏洩 • 委託先のミスもしくはルール未遵守により、委託先へ預けたお客様情報が第3者へ流出	• 委託先へは**必要最小限の情報受け渡し**とし、不要な情報は渡さない • 委託先のお客様情報の取り扱いに関する管理責任は、**委託元企業に存在することを認識し、必要なセキュリティ対策を確認の上、契約**するとともに、**お客様情報を適切に扱っているか定期点検（実査等）**を行うこと
ケース事例C ②アカウント権限保有者の異動・退職時	内部の犯罪者 × アクセス権限管理の不備 ＝ 内部不正による漏洩 • アカウント権限の削除漏れによる会社情報への不正アクセス、情報資産の持ち出し	• 異動・退職・雇用契約終了のタイミングで、**システムの利用権限が削除**（メーリングリストやクラウドサービスのアカウントに関する現行化を含め）されていること、**貸し出した情報資産についても、全て返却済であることを確認**すること
ケース事例D ③お客様受託商材（セキュリティ装置）の設計・設定時	外部の犯罪者 × チェック管理体制の不備 ＝ 不正アクセスよる窃取 • 受託商材（セキュリティ装置）の設定不備により、お客様の情報システムへの不正アクセス、情報資産の窃取	• お客様NW環境等を踏まえた、適切な要件定義および設計を行うとともに、各フェーズ毎（提案～設計～納品）の実施項目の可視化・フロー化、**組織的なチェック、レビュー**を行うこと
ケース事例E ④社外への情報持ち出し時	内部の犯罪者 × ルール未遵守 ＝ 不正利用による漏洩 • 許可されていない個人端末を自身の判断で利用し、セキュリティ対策の不備等により会社情報が外部へ流出	• 業務上利用するお客様情報等は、**会社から許可されていない個人端末等（スマホ）で撮影**するなどして、**持ち出さないこと** 参考）プライベート利用のSNS等から誤って情報が流出することもあるため、業務に係わる情報（個人的な業務メモ含む）を個人端末に保存しないこと

ケース事例A　委託先からの漏えい

事例内容

X県から受託している「教職員用パソコン更改業務」において、委託先であるF社が県職員情報（約4,000名程度）等を含むエクセルファイルをメール誤送信させる事象が発生した。
※誤送付先：Y市職員（5名）及び取引先であるA社従業員（3名）

F社（委託先）

従事者一覧に記載がない者が
作業に携わっており、
添付ファイルをzipにまとめる際
ファイルを誤って選択・追加

自治体（Y市）職員

F社作業者に対し
電話申告したことにより、
本事象が判明

その他明らかになったこと

「委託先選定チェックシートが適切に使用されていなかった」、「従事者が変更になったにもかかわらず、従事者一覧の更新、再提出がされていなかった」等、委託先管理上の不備が散見された。

発生要因

＜委託先＞
- セキュリティーの担保が個人任せ（チェックプロセスやルールが無い）
- 複数案件を同時に対応する場合のルールや誤送信防止の仕組みが未導入

＜委託元＞
- 委託先選定チェックシートが適切に利用されず、委託先のお客様情報取扱い従業員一覧の更新・再提出がされていない等、委託先への管理が不十分（従業者一覧に記載がない作業者が誤送信を発生）

対処・再発防止策（例）

＜委託先＞
- お客様からの受領データに対し、受領後直ちにパスワード設定を行う運用へ見直し
- 複数案件処理時に、同時にデスクトップ上にファイルを置かない運用へ見直し
- Outlookによるメール送信時の自己確認とシステムによる上長承認の2段階承認を経ないと外部へ送信できない仕様に変更

＜委託元＞
- F社に対して、当面（半年を想定）の間は、月1回の立入点検を重点的に行うこととし、再発防止策の定着状況を含め点検を実施

ポイント

- 委託先のお客様情報の取り扱いに関する管理責任は、委託元企業に存在することを認識し、必要なセキュリティ対策を確認の上、契約するとともに、お客様情報を適切に扱っているか定期点検（実査等）を行うことが必要です。

- 委託先選定チェックシート等各種チェックシート及び申請書等の運用は、お客様情報保護運用マニュアルに基づき適切に対応することを徹底いただくとともに、委託先管理が形骸化しないように、委託契約前・契約中において、委託先のお客様情報取り扱い状況を的確に確認チェックする仕組み・業務フローを予め整備しておくことが重要です。

ケース事例B　委託先からの漏えい

事例内容

X市から受託し、A社へ委託した「物価高騰支援給付金業務」において、「こども加算給付」の支給対象者あての支払通知書の裏面に、別の支給対象児童の情報を印刷し、発送した事案が発生した。（印刷内容：児童の氏名と生年月日）※ 約700世帯（児童数約1,200名）

発生要因

＜委託先＞
- 明確なプログラム設定ルールがない中、現場任せの設定となっていたことから、プログラム設定の誤りが発生
- 実データを用いた表裏テスト印刷を実施せず、納品物の内容チェックが未実施（テストデータから本データのプログラム設定に対するチェックも未実施）

＜委託元＞
- 納品前のサンプリング開封によるチェックが未実施（件数のみチェックで終了）

対処・再発防止策（例）

＜委託先＞
- 仕様に基づき、テストデータを作成し検証を実施。テスト結果を踏まえたチェック会議にて委託元に提示し承認を得るフローに見直し
- 実際の印刷条件と同一の校正紙を出力し、委託元の校了を得るフローに見直し
- プログラム作成時の動作確認テストの実施と本番印刷物とデータの整合性を確認

＜委託元＞
- 作業工程に対する委託先へのヒアリングと工程の確認を印刷開始前までに実施
- 印刷完了後に委託先と納品前チェックを実施（サンプリングチェック）

ポイント

- 委託先のお客様情報の取り扱いに関する管理責任は、委託元企業に存在することを認識し、必要なセキュリティ対策を確認の上、契約するとともに、お客様情報を適切に扱っているか定期点検（実査等）を行うことが必要です。

- 今回は、委託先の納品物について、誤りがないという前提に立ち、委託元として作業工程や作業成果物のチェックを行いませんでした。同様の事案を発生させないために、委託先の作業工程や成果物に対して、委託元が、必ず、チェック確認を行う業務フローを確立しておくことが重要です。

職場でどのような重要情報を取り扱っており、
内部不正・ルール未遵守・不正アクセス等により
情報が漏えいするリスクがないか

情報漏えいリスクへの対処として、
職場においてどのような取り組みが実践できるか、
業務フローの見直しなど含め検討してみましょう。