

個人情報保護研修テキスト 2025 年

～個人情報等保護の重要性、漏えい等防止、法令違反等のリスクについて～ 2025 年 8 月
株式会社シグマスタッフ コンプライアンス事務局

個人情報とは？

「個人情報」とは、個人に関する情報であつて、氏名、生年月日その他の記述等「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でき個人を識別できる場合も含む)と個人識別符号です。

＜個人情報に該当する例＞

- ◆「氏名」、「生年月日」、「性別」、「住所」、「家族構成」、「学歴」、「職歴」、「身長・体重」、「血液型」など。
- ◆ 文字情報だけでなく、映像、写真、音声等電子データ(本人が特定できる場合)も対象になります。
(防犯カメラに記録された写真・動画、メールアドレス※など)

※個人を特定できるメールアドレスの例：meguro_taro@*****.co.jp

- ◆ 個人の商品や役務の購買・貸出履歴、視聴履歴、位置情報等 -----
- ◆ 個人の生体情報をデータ化したもの
(指紋認証データ、顔認証データ、虹彩、声紋、歩き方、遺伝子データ等)
- ◆ 個人に提供される符号・番号等
(旅券(パスポート)番号、運転免許証番号、基礎年金番号、マイナンバー、健康保険証被保険者証の番号記号、介護保険被保険者証の番号など)

これらは個人識別符号といい、2017年5月施行の改正個人情報保護法で個人情報に追加された内容です

※2025 年 6 月に予定されていた改正個人情報保護法(こどもの個人情報、生体データなどの規定追加等)は審議されなかったため、2025 年秋以降の成立になる予定です。

※マイナンバーは個人情報で個人情報保護法に基づく取扱義務がありますが、マイナンバー法に基づき、取扱範囲・目的等、他の個人情報とは異なる取扱い等の制限があるので注意が必要です。

※就業先の入退室管理システム等で使用するセキュリティカードや入館証は、カードごとに個別 ID を付与し、社内では ID ごとの使用者氏名を管理し、参照すれば本人を特定できるので、これらも個人情報です。

※携帯電話・スマートフォン機器内にある連絡先情報、送受信したメールメッセージ、人物を撮影した写真・動画、アプリの使用履歴等の情報は個人情報になります。使用時のパスワード認証や紛失等起きた場合の使用停止、位置情報確認等の対策を検討ください。

要配慮個人情報とは？

個人の不当な差別、偏見、不利益につながりかねない影響を考慮して、個人情報保護法で取扱いに特別な配慮が求められている個人情報です。

＜要配慮個人情報の例＞

- 人種、●信条(宗教、政治的見解等) ●社会的身分(被差別地域出身、非嫡出子(婚外子)など)、●病歴
- 犯罪の経歴(前科)、犯罪の被害に遭った事実 ●心身の機能の障害、●健康診断等結果(健康診断結果、検査結果(HBs(肝炎)、HCV 結果等)、●医師による保健指導等(通院歴、診療記録・薬剤服用歴、お薬手帳等)、●刑事事件の捜索・勾留・逮捕・公訴等(本人が被疑者・被告人)

◆「要配慮個人情報」の取扱いの原則は「取得、利用、提供を行わない」(禁止)です。

◆ 業務上必要があり、かつ本人の同意を得て取得する場合は、適切な保管場所・管理方法を決め業務従事者を任命する等、その取扱いには十分な配慮を求めています。

＜要配慮個人情報に該当する例＞

※健康診断結果報告書、ストレスチェック結果(個票)、医師との面接指導結果、障害者手帳等、遺伝子検査等。

※医療機関や薬局で、診療や調剤に関する情報は、概ね全て要配慮個人情報に該当します。病院等を受診したという事実、薬局等で調剤を受けたという事実(領収書や明細書)も要配慮個人情報です。

＜医療機関における要配慮個人情報の例＞

診療録、処方せん、手術記録、看護記録、検査所見記録、エックス線写真、紹介状(診療情報提供書)、患者に係る診療経過の要約、調剤録、領収書・明細書など。

＜要配慮個人情報には該当しない例(個人情報ではある)＞

※要配慮個人情報の範囲・内容は、個人情報保護法で定められており、個人情報同様、個人情報保護法等法令改正によって変更になる可能性がある。以下は現在、要配慮個人情報には該当しない。

・国籍、肌の色 ・自分で計測した体重・体脂肪率、体温、血圧等 ・「本籍地」情報

個人番号（マイナンバー）とは？

個人番号（マイナンバー）は、国民一人ひとりに付与される12桁の番号で原則として変更されません。 マイナンバーは個人情報でもあります。マイナンバー法でマイナンバーの利用目的・対象業務が決まっており、たとえ本人の同意を得たとしても法律で定めた利用目的を超えて利用することはできません。当初は3つの分野（社会保障、税、災害対策）の行政手続で利用されていましたが、その後のマイナンバー法改正により 2018年からは金融分野（預貯金口座）、医療等分野（特定健康診査情報の管理等）、2021年10月からはマイナンバーカードが健康保険証の代りに医療機関・薬局等で利用（マイナ保険証）できるようになり、2025年3月からはマイナ免許証（マイナンバーカードのICチップ内に運転免許証情報をデータとして収容しマイナンバーカードと運転免許証を一体化）が始まりました。

マイナンバーは、マイナンバー法に基づき、不正な取得や売買、目的外利用等を行った **当事者に対して罰則**があります。（正当な理由なく個人番号を提供した場合4年以下の拘禁又は200万円以下の罰金）

営業秘密（秘密情報）とは？

営業秘密とは、秘密として管理されている事業活動に有用な技術上又は営業上の情報で、企業の競争力・利益の源泉とされる重要な経営資源です。不正競争防止法により保護されています。（不正競争防止法第2条）

＜営業秘密の例＞ ・勤務先等の事業計画 ・顧客情報、取引先情報 ・商品情報、生産・技術等
※社内業務手順書・マニュアル・企画書・提案書、会議配布資料等も含まれます。

営業秘密の漏えいや盗用があると、自社製品の優位性が失われ、企業業績に深刻な影響が出る場合があります。
社内の出来事や人事内部情報などの営業機密をSNS等で投稿することは漏えい行為で罰則の対象になります。

情報の適切な取扱い（安全管理対策）

情報の不適切な取扱いや管理の不備等は、漏えい・紛失等につながり個人情報保護法違反（事業者の義務とされる安全管理措置違反）となります。注意すべき主な事項は以下のとおりです。

不適切な取扱い（規則・守秘義務の違反）			業務上許可された目的以外の用途での複製や印刷	
業務上知り得た情報・写真等の私的なSNS投稿	私物のパソコン・記録媒体等（使用禁止）	許可・権限のない情報資産へのアクセス	業務上許可された目的以外の用途での複製や印刷	重要情報を含む印刷物・文書をそのままゴミ箱に捨てる
				

【対策1】

- ・従事する業務で決められた規則・許可された手順等に従って業務を遂行してください。勝手に解釈して規則・手順を変えたり、省略してはいけません。
- ・個人所有（私物）のパソコンや記録媒体等を業務で使用してはいけません。会社から貸与又は許可を得た機器を使用してください。

情報漏えい（メール誤送信）	情報漏えい（書類誤発送）
メール誤送信（宛先間違い、添付データ間違いなど） 	宛先の間違い 封入書類の間違い 

＜メール誤送信と書類誤発送、情報漏えいの代表的な原因＞

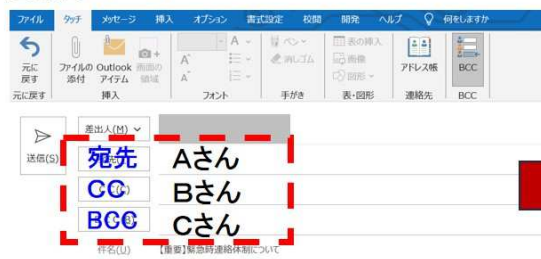
「メール誤送信」は主要な漏えい事故の一つです。他に「誤送付（宛名間違い）」、「誤送付（封入ミス）」などの「書類等誤発送」などがあります。漏えい等は複数の原因がありますが、それぞれに適切な対策を確実に講じることによって、漏えい等の発生を低減することができます。

【対策2】 ★メール誤送信の防止のために

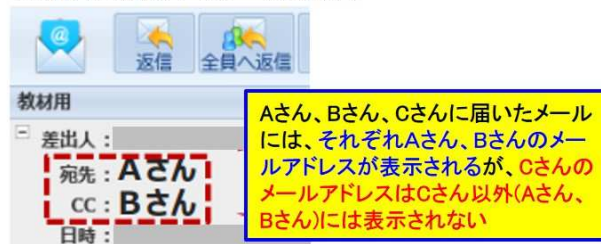
メール誤送信には、主に 3 つの類型 (①宛名間違い、②添付文書(データファイル)の間違い、③送信方法(BCC と TO/CC 等)の間違い)があります。送信時の目視確認・チェックを確実に行うようにしましょう。

※BCC 送信は、不特定多数へ送信する際に利用する方法で、**BCC 送信した場合、本人以外のメールアドレスは表示されません。**(下記図参照)

送信者のメール



受信者には以下のメールが届く



【対策3】 ★書類等誤発送の防止のために

書類等誤発送には、主に 2 つの類型 (①宛名間違い、②封入書類間違い)があります。窓あき封筒の利用や宛名書き・封入時のダブルチェックを可能な限り行うようにしましょう。

【対策4】

- ・ **公共交通機関の利用や移動途中の飲食・トレイ等**で、かばんや情報機器の置忘れが起きやすいです。業務上必要な情報の持出しや機器の使用は必要最小限にし、置き忘れや紛失等起こさないよう留意ください。
- ・ **自動車や自転車の移動中**も、車内等に置いたカバン等をから離れないよう注意ください。

情報機器・記録媒体の紛失・盗難

交通機関等で置忘れ



パスワード管理の不備

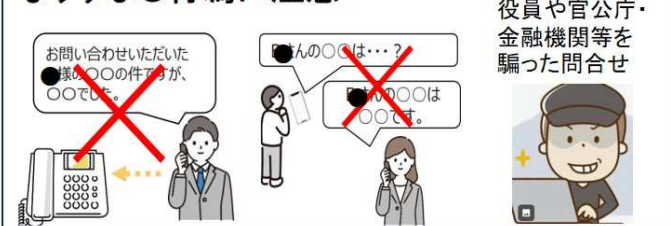


- ◆ パスワードを記載した付箋を画面に貼付け
- ◆ 業務上必要ない者に自分のパスワードを開示
- ◆ 類推されやすいパスワードに勝手に変更

【対策5】

- ・ パスワードは、**利用者本人が管理**し、他の者と共有しないこと。パソコン画面にメモ等貼ったり、他者に見られることがないようにすること。
- ・ パスワードは、名前、社員番号、生年月日等**他者から類推されるものは使用しない**こと。また、英字、数字、記号等複数を組み合わせ、一定桁数以上となるよう採番するのが望ましい。

なりすまし行為に注意



仕事の話をする場所・環境に注意



【対策6】

- ・ **別人によるなりすまし問合せの可能性**があるので、電話先が留守番電話の場合、必要最小限以上の個人情報を伝言(録音)しないこと。問合せには、本人からかけ直すよう伝え、必要以上に情報を伝えないこと。

【対策7】

- ・ **声や会話内容が第三者(家族を含む)に漏れる環境や、パソコン画面が覗き見られる場所(交通機関移動中、待合室、飲食店内等)**では、業務上やむを得ない場合を除き仕事をしない。
- ・ 第三者に聞かれる可能性があるため、**エレベータ内、洗面所・給湯所など共有スペースでの**

会話では、業務に関する情報を話さないよう注意すること。

不審なメールを開かない・クリックしない

詐欺サイトにアクセスしない・情報を入力しない

【対策 8】

- ・ 悪意のある者が、他人や大手・著名企業等を勝手に騙って偽のメールを送り付け、不正プログラムに感染したりパスワード、クレジットカード番号等重要情報を窃取、悪用される被害が多く報告されている。不自然・違和感を感じたメールは、その添付ファイルを開いたり、メール本文に記載された URL (偽サイト) にアクセスしないこと。

【対策 9】

- ・ パスワード等重要な情報を入力させ、窃取した情報を悪用する被害が報告されている。本物そっくりのサイトで、見た目では偽サイトと判別するのは難しい。メール URL で開いたサイトでは、重要な情報の入力を安易に行わないこと。

情報機器等使用条件の不徹底

セキュリティが脆弱な通信環境の利用

パスワードロック設定等利用者認証の不備

コンピュータウイルス感染

緊急時の対応

- ・ 情報漏えい発生
- ・ 不正アクセス攻撃
- ・ ウイルス感染など

- ◆ 通信を切断する (LANケーブルを外す、wifi切断)
- ◆ 該当機器・サービスの使用を中止
- ◆ システム管理者に報告、指示に従う

【対策 10】

- ・ 業務で使用する機器は、セキュリティ対策ソフト・OS 修正プログラムアップデート、パスワードロック等機器の使用条件を整えるよう留意した上で使用ください。
- ・ フリーwifi 等セキュリティが脆弱な通信ネットワークは仕事(在宅、他場所でのテレワーク含む)で使ってはいけません。
- ・ パスワードロック、顔認証など等、利用者認証を確実に行うこと。

【対策 11】

- ・ 情報漏えいの発生、不正アクセス攻撃等緊急事態が発生した場合、当該機器の通信環境を切断・周辺機器がある場合はそれを外し、当該機器・該当サービスの利用を中止する。
- ・ 緊急時連絡体制等に基づき、システム管理者等に事象の発生を報告し、指示に従う。

個人情報漏洩等の当事者になってしまった場合の責任

～ 法令に基づく罰則等、責任が問われる ～

- | | |
|---------------|-----------------------------------|
| ・ 個人情報保護法違反 | 個人情報データベース等提供罪など。 |
| ・ マイナンバー法違反 | 目的外利用、不正取得・不正利用等に刑事罰適用。 |
| ・ 不正競争防止法違反 | 会社の顧客情報を不正取得、競合会社に渡した場合など。 |
| ・ 刑法違反 | 会社の重要情報や顧客情報を勝手に持ち出す行為は、窃盗や業務上横領。 |
| ・ 不正アクセス禁止法違反 | ID・パスワード等を不正取得・不正使用等には刑事罰適用。 |



以上