

情報セキュリティ研修

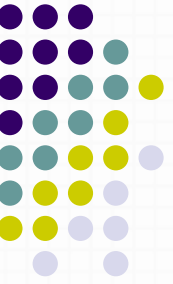
東京都福祉局指導監査部



研修の内容

- 研修の目的
- 情報セキュリティ知識・理解度チェック & 解答・解説
- 業務上取り扱う具体的な「個人情報」「機密情報」
- 近年の情報漏えいの傾向
- 情報漏えいがあった場合の影響
- 誰にでもできる！具体的な漏えい対策
- 明日から実践すること

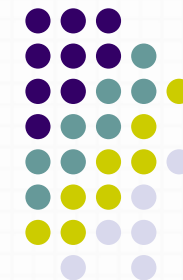




研修の目的

今後、各事業者にてDXに取り組んでいく中で、
これまで以上に必要になってくる
「情報セキュリティリテラシー」を身につける

情報セキュリティ知識・理解度チェック



	問題内容	○ or ×
問1	特定の個人を識別できない氏名だけの情報であっても、それは個人情報である	×
問2	免許証番号の情報だけでも個人情報に該当する	○
問3	要配慮個人情報とは、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に、その取扱いに配慮を要する個人情報であり、病歴は含まれない	×
問4	個人情報取扱事業者は、不正の手段により個人情報を取得してはならない。かつ、本人から直接、書面に記載された個人情報を取得する場合、あらかじめ本人に利用目的を明示する必要がある	○
問5	個人情報保護委員会への報告には速報と確報の2種類があり、速報は漏えい等が発生したのを知った時点から1週間以内、確報は2か月以内に報告しなくてはならない	×
問6	情報セキュリティとは、正当な権利をもつ個人や組織が、情報や情報システムを意図どおりに制御できることであり、機密性のみが担保されている必要がある	×
問7	入退管理技術の一つで、何らかの方法で忍び込んだ不審者が隠れないように、普段使わない会議室などのドアを開けておくことをクリアデスクポリシーという	×
問8	機密性の高い情報が必要なくなった場合、いつまでもデスクトップやフォルダーに置いておかず、デスクトップ内にあるゴミ箱に入れることで、情報は抹消される	×
問9	Gmailの送信ボタンを押したあとはすぐに相手方にメールが送信されるので、送信前に、送信先や添付資料に間違いがないか、必ずダブルチェックを行うなどメール誤送信の対策を行う必要がある	×
問10	外出先でパソコンを業務上使用する際、投影されて機密性の高い情報を背後から画面で見られたとしても、写真など具体的にデータが取られたわけではないので、情報漏えいとまでは言えない	×



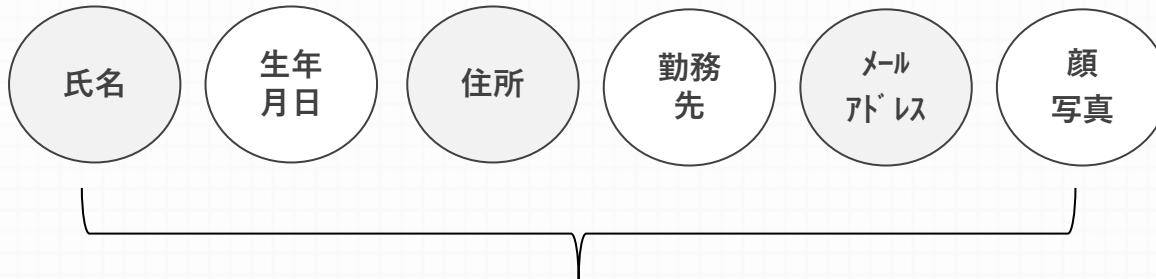
問1：『個人情報』とは？



「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等に記載され、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により特定の個人を識別することができるものをいう

【個人情報保護法・第2条第1項】

■個人情報



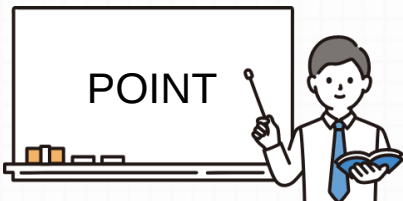
これらの組み合わせにより、特定の個人を識別できるもの



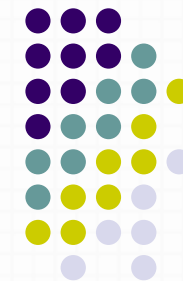
死亡者



音声・画像・
パソコン内データ



氏名のみでも、特定の個人を識別できる場合は「個人情報」に該当するので注意（例：珍しい名字）



問2：『個人識別符号』とは？



「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう

1. 身体的特徴等を電子計算機の用に供するために変換した符号
2. 対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号

【個人情報保護法・第2条第2項】

■ 「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

DNA

顔

指紋

声紋

歩行
態様

虹彩

■ 「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

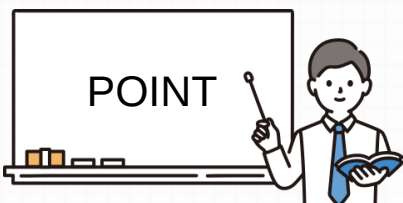
年金
番号

免許証
番号

住民票
コード

旅券
番号

被保険
者番号



「個人識別符号」は特定の個人を識別できるため、
その情報“単体”でも、個人情報に該当する



問3：『要配慮個人情報』とは？

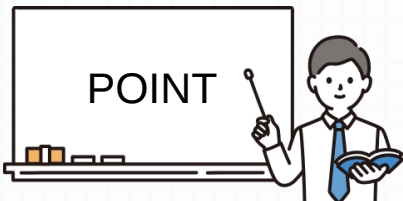
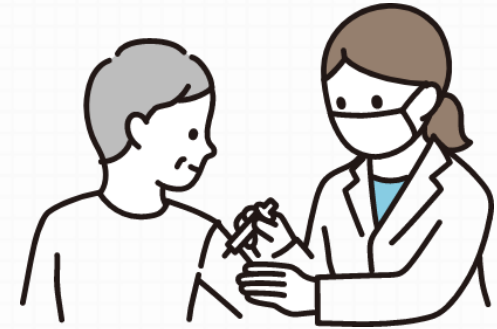


「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報という

【個人情報保護法・第2条第3項】

■『要配慮個人情報』に該当するもの

- ①人種 ②信条 ③社会的身分 ④病歴
- ⑤犯罪の経歴 ⑥犯罪により害を被った事実
- ⑦身体障害・知的障害・精神障害等があること
- ⑧健康診断その他の検査の結果
- ⑨保健指導、診療・調剤情報
- ⑩本人を被疑者又は被告人として、逮捕、搜索等の刑事事件に関する手続が行われたこと
- ⑪本人を非行少年又はその疑いのある者として、保護処分等の少年の保護事件に関する手続が行われたこと



取得するときは、原則、“事前”に
本人の同意を得る必要のある情報である



問4：個人情報の取得・利用



個人情報取扱事業者は、偽り、その他『不正の手段』により個人情報を取得してはならない

【個人情報保護法・第20条】

個人情報を取得した場合は、あらかじめその『利用目的』を公表している場合を除き、速やかにその利用目的を本人に通知し、又は公表しなければならない

【個人情報保護法・第21条】

■不正な取得手段例



窃盗、脅迫



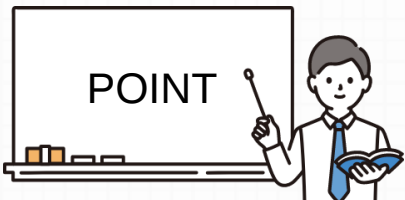
十分な判断能力のない子供からの取得

■利用目的の通知・公表

本人から直接書面に記載された個人情報を取得する場合、あらかじめ本人に利用目的を明示する必要あり

利用目的の通知や公表は、速やかであれば“事後”でもかまわない

人の生命等の保護のために緊急の必要がある場合は通知、公表義務はない



子どもが利用目的を理解できない場合、親の同意がなければ、不正な手段による個人情報の取得となる。同意を得る必要がある具体的な年齢の目安は社会通念上、12歳～15歳までの年齢以下とされている



問5：個人データの漏えい



個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって、個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるものが生じたときは、（中略）当該事態が生じた旨を個人情報保護委員会に報告しなければならない

【個人情報保護法・第26条第1項】

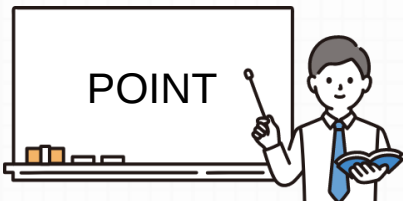
2020年の改正法（2022年全面施行）によって、個人情報取扱事業者は、個人データの漏えい等又はそのおそれがある場合で、以下のいずれかのような個人の権利利益を害するおそれ大きい場合は、個人情報保護委員会への報告及び本人への通知が「義務」となった。

要配慮個人情報が含まれる個人データ等

不正に利用されることにより財産的被害が生じるおそれがある個人データ等

不正な目的をもって行われたおそれがある個人データ等

個人データに係る本人の数が1,000人を超える漏えい等



報告には、速報と確報の2種類がある。『速報』は、漏えい等が発生したのを知った時点から概ね3～5日以内、『確報』は30日以内に報告しなくてはならない



問6：情報セキュリティとは？

「情報セキュリティ」とは、正当な権利をもつ個人や組織が、情報や情報システムを意図どおりに制御できることです。尚、情報セキュリティの3要素は下記のとおりです。

許可された者だけが情報を使用できるようにすること



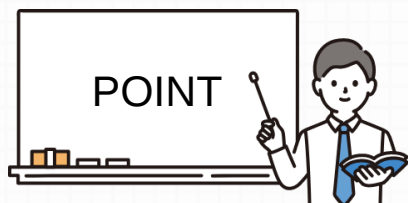
機密性

情報や情報の処理方法が、正確で完全であるようにすること

完全性

可用性

許可されている者が、必要なときに情報や関連する情報資産にアクセスできること



情報セキュリティは上記3つの要素すべてを満たしていることが重要であり、一つも欠けることのないように留意すること

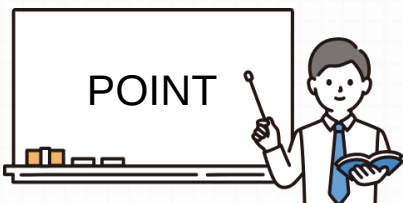
問7：オープンドアポリシー・クリアデスクポリシー



入退管理技術の一つとして、何らかの方法で忍び込んだ不審者が隠れないよう、未使用の会議室などのドアを開けておくことを「オープンドアポリシー」といいます。



自分の席の机の上に情報を記録したものを放置したまま席を離れないことを「クリアデスクポリシー」といいます。



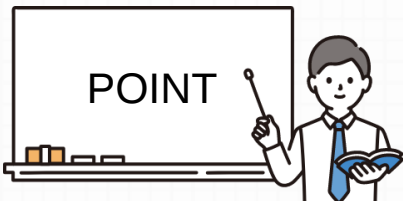
離席時のパソコンにスクリーンロックをかける、ノートパソコンのスクリーン部分を軽く閉じる、機密情報が記載された資料は裏返しにするなどがある



問8：データ消去方法

「ごみ箱を空にする」でデータを削除しても、仮想的に使用する論理アドレスを消去したにすぎないため、物理的に削除する必要があります。データそのものはハードディスク上に物理的に存在するため、復元が可能なので漏えいする危険性があります。

よって、データを消去する場合は、完全にデータを消去するソフトを使用するか、物理的にハードディスクを破壊することが望ましいです。

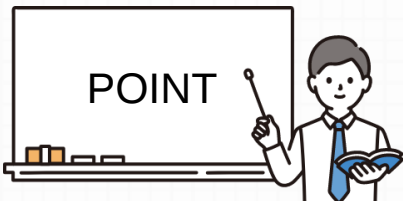


データの最終的な消去方法に関しては、自組織の規程・ルールに沿って行うこと。
独自の判断で行うことのないように留意する



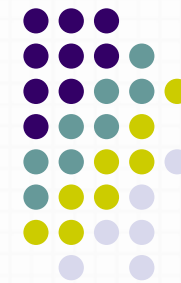
問9：メール誤送信直後の対応

Gmailには、送信ボタンを押したあとも、設定しておいた秒数の間はメールが送信されないという保留の機能があります。5～30秒の間に送信を保留する時間（送信を取り消しできる時間）を設定できますので、使いやすい秒数を設定してください。

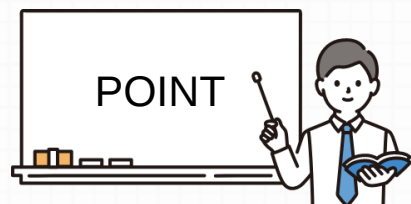
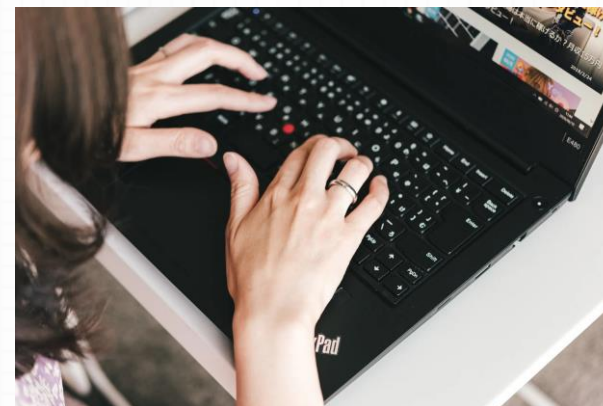


Gmail以外のメールを利用している方は、自身が使っているメールに同様の機能があるかを確認すること

問10：ショルダーハック



肩越しからキー入力やディスプレイを盗み見て、機密情報やパスワードなどを収集されることを「ショルダーハック」といいます。移動中や外出先など、様々なシーンで起こりうるこのショルダーハックは、情報漏えいの一つです。



ショルダーハックの物理的な対策の一つとして、パソコン画面に「目隠しフィルター」をつけることなどが挙げられる

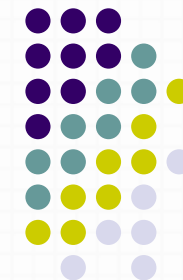


業務上取り扱う具体的な「個人情報」「機密情報」

	個人情報（例）	機密情報（例）
介護・老人ホーム 障害者支援施設	■名簿、契約書・同意書、個人情報使用同意書 ■入所（居）者・利用者の個人記録及び職種ごとの記録等 （プラン、カルテ、処方せん、介護・看護・ケース記録、日誌、申し送り記録等） ■被保険者証・受給者証 ■レセプト・給付費明細書・領収証、工賃等明細書 ■職員関係書類 （雇用・派遣契約書、履歴書、誓約書、健康診断、労災等） ■相談・苦情・事故報告・ヒヤリハット情報、虐待報告書等	■建物関係書類 （平面図、改築計画等） ■消防関係書類 （緊急連絡網、消防署への届け出書類等） ■印鑑・金品等の管理情報 （保管場所、暗証番号、管理者等） ■死亡者の情報、印影 （理事長印、契約事業者印等）
保育園・こども園 児童福祉施設	■児童名簿、児童票 ■保育日誌、保育所児童保育要録、健康診断記録 ■緊急時連絡先 ■保育の個別的な計画、アレルギー情報 ■児童の写真データ、連絡帳、個別面談記録 ■就労証明書、育了児台帳等	■建物関係書類 （平面図、改築計画等） ■消防関係書類 （緊急連絡網、消防署への届け出書類等） ■印鑑・金品等の管理情報 （保管場所、暗証番号、管理者等） ■登園時の開門扉の暗証番号 ■事故状況等の記録等

近年の情報漏えいの傾向

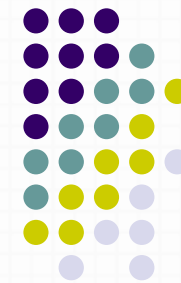
～情報セキュリティ10大脅威2024～



※出典：独立行政法人 情報処理推進機構（IPA）

順位	脅威	初選出年	10大脅威での取り扱い (2016年以降)
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

情報漏えいが起きてしまった場合の影響



組織

個人データの漏えいが発生した場合には、事業者における安全管理措置や従業者への監督が適切に行われていなかったのではないかということで責任を負う可能性があります。

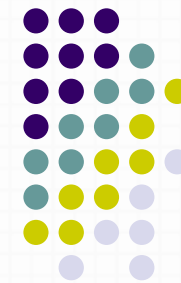


従業者

そして、その従業者が、その業務に関して取り扱った個人情報データベース等を自己若しくは第三者の不正な利益を図る目的で提供や盗用したときは、個人情報保護法第83条により刑事罰（1年以下の懲役又は50万円以下の罰金）が科される可能性があります。

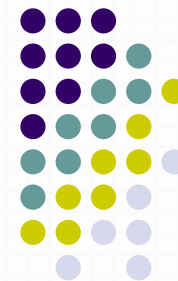


誰にでもできる！ウィルス対策



	対策
1	身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない
2	自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない
3	OSやアプリケーション、セキュリティソフトを常に最新の状態にする
4	信頼できないメールに添付されたWord文書やExcelファイルを開いた際、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない
5	メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する
6	身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する

明日から実践すること



これまでの意識

(記入例)

情報セキュリティ分野には関心が薄かった。
よって、業務上あまり意識していなかった。

研修で感じたこと

(記入例)

何が重要情報で、具体的にどのように気をつけ
ればよいか知らなかった。また、情報漏え
いが起きたときの影響を理解できた。

明日から実践すること

(記入例)

- ①自分自身及び組織全体が、業務上取り扱っている「個人情報」や「機密情報」が何であることを整理し、
明文化にする (今月中)
- ②現在使用しているOS、アプリケーション、セキュリティソフトを最新の状態にする (今週中)