令和6年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【初学者等向け研修】
Aコース
～情報セキュリティの重要性～

一般社団法人ソフトウェア協会

目的

- 本研修は、医療機関等の中でセキュリティの基礎知識を身に付けたい人に、セキュリティに興味を持ってもらえるような気付きを与えることを目的としています。

- 皆さんにとって身近なセキュリティをはじめ、一般的なセキュリティ脅威についても興味を持っていただけるよう、噛み砕いて説明していきます。

- 本研修を通して、セキュリティを他人事ではなく自分事と捉え、セキュリティ事故を未然に防げるようセキュリティへの意識を持ち、対策に取り組む必要があることを理解していただければと思います。

①情報セキュリティとは？

情報セキュリティという言葉は知っていますか？

情報セキュリティとは・・・

組織が保有する大切な情報を安全に守ることです。

情報セキュリティとサイバーセキュリティの違い

	情報セキュリティ	サイバーセキュリティ
対象	紙や電子など、保存された媒体を問わないあらゆる情報	電子化された情報
アプローチ	情報の扱い方そのものについて考える	サイバー攻撃の脅威となる存在への技術的な対処法を考える
含まれるもの	会話内容や紛失などの人為的な行為も含む	デジタル形式で発生するデータのみ

セキュリティが守られていないとどんなことが起こるのか？

情報の漏えい

システムの障害

↓

業務への影響

システムの停止により診療や手術が行えず、業務に大きな影響を及ぼす可能性があります

組織の損害

患者情報の漏えいによる信用の低下、事故対応にかかる多額の費用等、組織に大きな損害を及ぼす可能性があります

情報セキュリティは、皆さん自身や組織にとって必要不可欠です
どのように皆さんの生活にも関係しているかを説明していきます

用語解説

ハードウェア

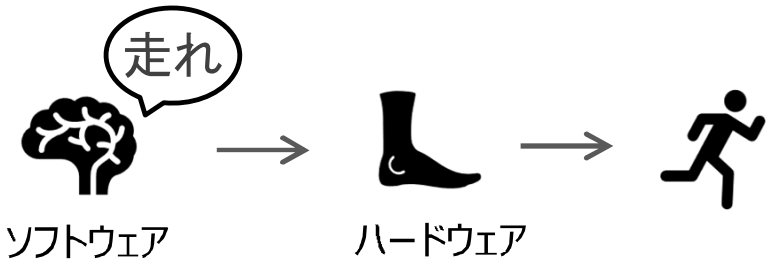
・目に見える物理的なもの

・人間に例えると、身体そのもの

ソフトウェア

・ハードウェアを動かすための機能

・人間に例えると、脳や神経、思考など



脆弱性

・ソフトウェアの弱点

・設計ミスや不具合が原因

マルウェア

・Malisious(悪意のある)＋Software(ソフトウェア)

・悪影響なソフトウェアの総称

②身近な情報セキュリティ

身近な情報セキュリティについて意識したことがありますか？

皆さんの身近な情報セキュリティには、以下のようなものがあります

スマートフォン　インターネットサービス　ごみ捨て

スマートフォンとは、携帯電話とパソコンの機能を合わせた情報端末です

インターネットサービスとは、私たちがPCやスマートフォンを使って、世界中の情報にアクセスしたり、他のユーザーとコミュニケーションを取ったりできるようにするためのサービスの総称です

セキュリティ対策をしていないとどうなる？

マルウェアに感染

不審なサイトやメールを開いたり、OSやアプリの脆弱性を狙われてマルウェアに感染

不正なアクセス

パスワードを盗まれてサイトに不正アクセスされ、情報が漏えい

詐欺被害

怪しいサイトと気づかずにアクセスし、個人情報を入力してしまい詐欺被害に遭う

さまざまなリスクがあります

日常的に皆さんが行っているごみ捨てにも、
実はセキュリティの危険性が潜んでいます

・郵便物（宛名が書かれた封筒や宅配便の送り状　等）
・書類（医療機関の診断書　等）
・メディア（写真や動画を保存したCDやDVD　等）
・電子機器（PCやスマートフォン）

そのまま捨てていませんか？

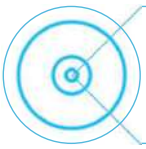
廃棄する前にすべき対策があります

郵便物や書類を廃棄する際は、以下のような対策を実施しましょう！

シュレッダーで細かく切断

個人情報部分を切り取る

データが保存されたCDやDVDを廃棄する際は、以下の方法でデータを消去してから廃棄しましょう！



データを上書きし、元データを削除する

物理的に破壊し、復元を困難にする

専門業者にデータの消去を依頼する

PCやスマートフォンなどの電子機器を安全に廃棄するために、以下の対応を実施しましょう

データを完全に消去できる専用ソフトを使用する

PCやスマートフォンを初期化する

ハードディスクを物理的破壊する

専門業者に依頼する

身近に利用しているモノ、行っているコトの中にも、実は危険が潜んでいます。
意識していないと、セキュリティ事故に巻き込まれる危険性があるため、普段から**セキュリティへの意識をもつこと**が大切です！

③よくある脅威とその対策・対応

情報セキュリティ10大脅威

IPAが毎年発表する、社会的影響が特に大きかったと考えられる情報セキュリティの事案をまとめたものです。

IPA（独立行政法人情報処理推進機構）とは、
経済産業省のIT政策実施機関です。

「個人」向け脅威（五十音順）	「組織」向け脅威（五十音順）
インターネット上のサービスからの個人情報の窃取	サプライチェーンの弱点を悪用した攻撃
インターネット上のサービスへの不正ログイン	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
クレジットカード情報の不正利用	脆弱性対策情報の公開に伴う悪用増加
スマホ決済の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃
偽警告によるインターネット詐欺	内部不正による情報漏えい等の被害
ネット上の誹謗・中傷・デマ	標的型攻撃による機密情報の窃取
フィッシングによる個人情報等の詐取	ビジネスメール詐欺による金銭被害
不正アプリによるスマートフォン利用者への被害	犯罪のビジネス化（アンダーグラウンドサービス）
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	不注意による情報漏えい等の被害
ワンクリック請求等の不当請求による金銭被害	ランサムウェアによる被害

出典：IPA
https://www.ipa.go.jp/security/10threats/10threats2024.html

「個人」向け脅威（五十音順）	「組織」向け脅威（五十音順）
インターネット上のサービスからの個人情報の窃取	サプライチェーンの弱点を悪用した攻撃
インターネット上のサービスへの不正ログイン	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
クレジットカード情報の不正利用	脆弱性対策情報の公開に伴う悪用増加
スマホ決済の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃
偽警告によるインターネット詐欺	内部不正による情報漏えい等の被害
ネット上の誹謗・中傷・デマ	標的型攻撃による機密情報の窃取
フィッシングによる個人情報等の詐取	ビジネスメール詐欺による金銭被害
不正アプリによるスマートフォン利用者への被害	犯罪のビジネス化（アンダーグラウンドサービス）
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	不注意による情報漏えい等の被害
ワンクリック請求等の不当請求による金銭被害	ランサムウェアによる被害

出典：IPA
https://www.ipa.go.jp/security/10threats/10threats2024.html

1．偽警告によるインターネット詐欺（サポート詐欺）

サポート詐欺とは

サポート詐欺とは、インターネットを利用中に、「ウイルスに感染しました」「パソコンが壊れています」といった警告画面が表示され、利用者が焦って表示されている電話番号に電話をしてしまうと、サポートの名目で金銭を騙し取られる詐欺のことです。

警告画面のイメージ例

被害に遭うとどうなる？

金銭的な損失

高額なサポート料金の請求や、不正決済の被害を受ける可能性があります。

情報機器の機能不全

PCやスマートフォンが遠隔操作により利用できなかったり、データを削除される可能性があります。

個人情報の漏えい

口座情報やクレジットカード情報等、個人情報が盗まれる可能性があります。

サポート詐欺の被害イメージ

焦らせて電話をするように誘導

1 PCを操作

2 警告画面が表示される

不安を煽る内容になっている

3 焦って動揺する

4 記載された番号に電話してしまう

5 電話の指示で、遠隔操作ソフトをインストール

6 攻撃者が遠隔でPCを操作

7 高額なサポート料金を請求

なぜ警告画面が表示されてしまうのか

1 **不審な広告のクリック**

ウェブサイトの広告枠にある不審な広告をクリックすると、詐欺広告が表示されることがあります。

2 **不審なウェブサイトへのアクセス**

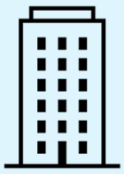
悪意のあるウェブサイトにアクセスすることで、詐欺広告に誘導されることがあります。

3 **ブラウザの偽通知**

ブラウザの通知機能を悪用した偽通知をクリックすることで、警告画面が表示されることがあります。

セキュリティ対策において、組織と個人ではそれぞれの役割があります

組織



経営者や管理者などが
組織単位でできること

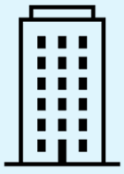
個人

個人単位でできること

組織の中で個人ができる（ご家庭でもできる）対策を紹介します

セキュリティ対策において、組織と個人ではそれぞれの役割があります

組織



経営者や管理者などが
組織単位でできること

個人

個人単位でできること

組織の中で個人ができる（ご家庭でもできる）対策を紹介します

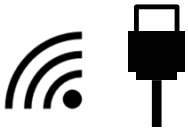
被害に遭わないために

不審なウェブサイトに注意する	• 少しでも怪しいと感じたら開かない
ウイルス対策ソフトを導入する	• パソコンやスマートフォンにセキュリティソフトを導入しウイルス感染を防ぐ
冷静に判断する	• 焦って電話をしない！不審に思ったらすぐに誰かに相談する

被害に遭ってしまったとき

ネットワークから切断する

感染の拡大を防ぐため、該当端末をネットワークから切断しましょう。



被害時の状況を記録する

いつ、どんな操作をしていたか、どんなファイルを開いたか等、今後の調査のために詳細を記録しておきましょう。
※画面のスクリーンショットを撮影しておくと良いです

被害を報告する

個人の場合は、警察やカード会社などの関連組織に相談しましょう。
組織の場合は、速やかに上司や（いる場合は）システム担当者に状況を報告しましょう。

※組織で決められた対応がある場合は、そちらに従い対応してください

被害に遭わないよう気を付けていても、いざ警告画面が出ると焦ってしまう

参考

実際にサポート詐欺の警告画面の閉じ方を体験できるサイトがあります

IPA　警告画面体験サイト

https://www.ipa.go.jp/security/anshin/measures/fakealert.html

2. フィッシング

フィッシングとは

インターネットを利用してパスワードやクレジットカード番号等の個人情報を盗み出す詐欺のことです。

配達に伺いましたが、お客様が不在でした。荷物はこちらに保管しています。http://t.co/dBwikOcaX

被害に遭うとどうなる？

個人情報の漏えい

クレジットカード情報、銀行口座情報、住所等の個人情報が漏えいし、悪用される可能性があります。

金銭的被害

クレジットカードで不正に買い物されたり、銀行口座から不正に引き出されたりする可能性があります。

なりすまし被害

本人になりすまして金銭を騙し取ったり、周囲に迷惑をかける可能性があります。

フィッシング攻撃の流れ

偽のメールやSMS

信頼できる企業（銀行やクレジットカード会社など）を装い、偽のメールやSMSを送信

偽のウェブサイト

偽のメールやSMSに含まれるリンクをクリックさせ、本物そっくりの偽ウェブサイトに誘導

個人情報の入力

偽のウェブサイトで、ID、PW、クレジットカード番号など、個人情報を入力させる

情報窃取

入力された個人情報を不正に利用

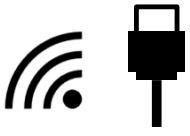
被害に遭わないために

不審なメールに注意する	• 知らない差出人からのメールは、安易に開かない
リンクをクリックしない	• 少しでも怪しいメールに記載されたリンクはクリックしない
パスワードを適切に管理する	• 複数のサービスで同じパスワードを使わない
認証方法を強化する	• 認証方法を強化することでアカウントへの不正アクセスを防ぐ

被害に遭ってしまったとき

ネットワークから切断する

感染の拡大を防ぐため、該当端末をネットワークから切断しましょう。



被害時の状況を記録する

いつ、どんな操作をしていたか、どんなファイルを開いたか等、今後の調査のために詳細を記録しておきましょう。
※画面のスクリーンショットを撮影しておくと良いです

被害を報告する

個人の場合は、警察やカード会社などの関連組織に相談しましょう。
組織の場合は、速やかに上司や（いる場合は）システム担当者に状況を報告しましょう。

※組織で決められた対応がある場合は、そちらに従い対応してください

3．ランサムウェア

ランサムウェアとは

大切なデータやデバイスを勝手に暗号化し、復号の代わりに「身代金」を要求するマルウェアの一種です。

被害に遭うとどうなる？

- ファイルなどのデータが暗号化される
- データが利用できず業務が停止する
- 身代金を要求される
- データが漏えいする可能性がある

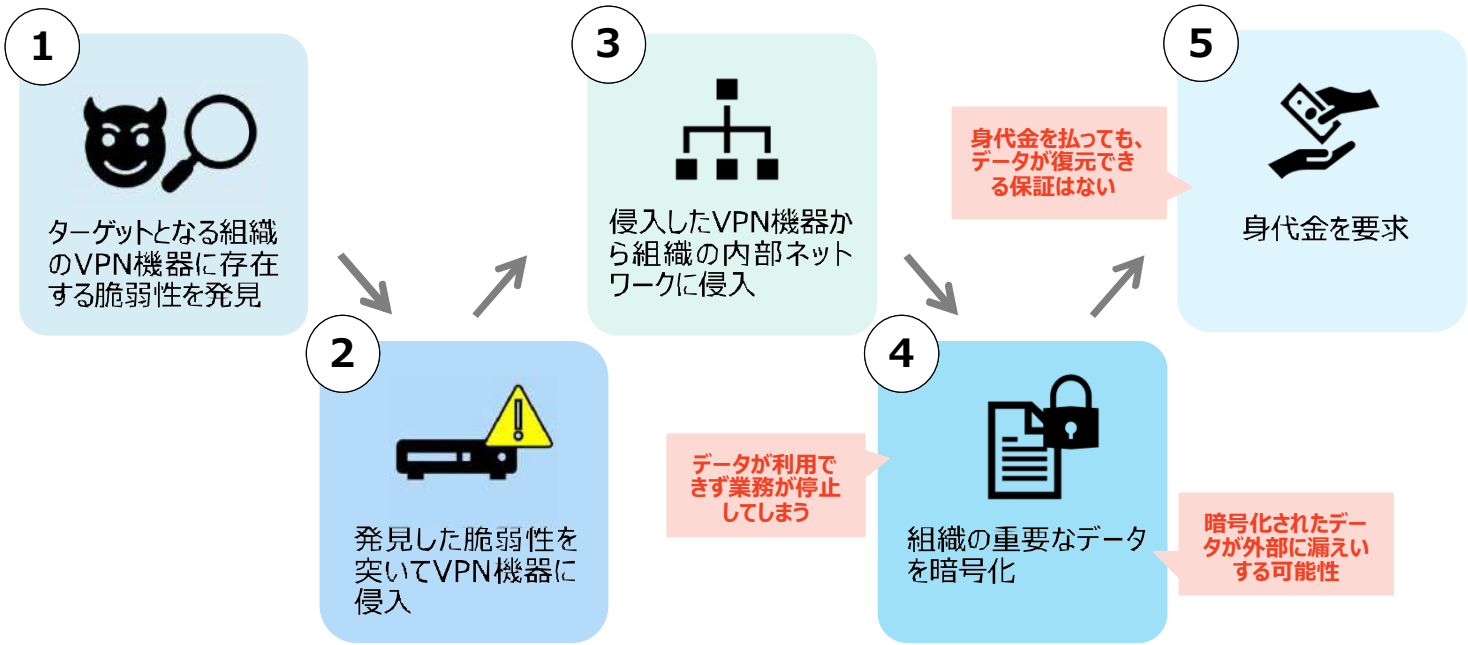
感染経路

- VPN機器からの侵入
  VPN（Virtual Private Network）とは、インターネットの通信を安全かつプライベートにするためのネットワーク

- リモートデスクトップからの侵入
  リモートデスクトップとは、離れた場所にあるPCの画面を、インターネット経由で操作できる技術のこと

- 不審メールやその添付ファイルから侵入

ランサムウェア攻撃のイメージ（VPN機器からの侵入パターン）



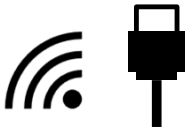
被害に遭わないために

不審なメールを開かない	• 不審なメールは開かず、添付ファイルも実行しない
パスワードを適切に管理する	• パスワードが漏えいしないよう、強固なパスワード管理を行う
ソフトウェアを最新の状態に保つ	• （自身で管理できる環境の場合）OSやソフトウェアのアップデートをこまめに行う
バックアップを取る	• 自身で作成したデータについて、重要なデータがある場合はコピーを取りサーバに保存するなど、自身で管理する

被害に遭ってしまったとき

ネットワークから切断する

感染の拡大を防ぐため、該当端末をネットワークから切断しましょう。



被害時の状況を記録する

いつ、どんな操作をしていたか、どんなファイルを開いたか等、今後の調査のために詳細を記録しておきましょう。
※画面のスクリーンショットを撮影しておくと良いです

被害を報告する

個人の場合は、警察に相談しましょう。
組織の場合は、速やかに上司や（いる場合は）システム担当者に状況を報告しましょう。

※組織で決められた対応がある場合は、そちらに従い対応してください

4．内部不正

内部不正とは

組織の内部にいる職員や関係者が、故意または過失により、組織の利益に反する行為を行うことです。
情報セキュリティに関わる内部不正には次のようなものがあります。

情報漏えい

患者情報、職員情報など、組織の機密情報を外部に漏らしてしまう行為です。

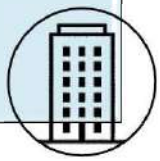
不正アクセス

組織の情報システムに不正にアクセスし、データを改ざんしたり、削除する行為です。

内部不正が起こるとどうなる？

- 患者情報や研究情報の流出により、想定外の対応費用や損害賠償につながる可能性があります。

経済的な損失

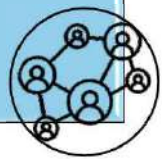


- 内部不正の発覚により職員の士気が低下したり、不正行為が蔓延してしまう可能性があります。

職員への影響

- 内部不正の発覚により患者からの信用を失う可能性があります。

信頼の低下



内部不正が起こりやすい環境

高圧的な職場環境

職員が上司に意見を言いづらい雰囲気

過度なプレッシャー

不可能な業務目標の設定

不公平な報酬体系

自分の貢献度に対して正当な報酬を得られない

情報共有不足な組織

情報が共有されないことによる不安感

参考

内部不正を防ぐために（組織ができる対策）

環境づくり	• 内部不正が起こりにくい環境づくりを心掛ける
職員への教育	• 内部不正の危険性について職員に周知したり、倫理観の向上を図るための研修を実施する
アクセス権限の管理	• 職員には必要最低限のアクセス権限を与え、定期的にアクセス権限の見直しを行う
監視システムの導入	• 情報システムへのアクセスログを記録・確認し、不正なアクセスがないかチェックする

意図しない内部不正に注意！

意図しない内部不正とは、職員が故意に不正行為をしようと考えていなくても、誤った操作や判断によって情報漏えい等を引き起こしてしまうことです。

患者の個人情報をむやみに閲覧/公開しない、家族や友人にも口外しない
注意しましょう！

5．標的型攻撃

標的型攻撃とは

特定の組織や個人を事前に選定し、その組織や個人の持つ機密情報などを盗み出すことを目的とした攻撃です。標的型攻撃には次のような種類があります。

標的型メール

標的となる組織の取引先や職員になりすまして業務に関連した内容のメールを送信し、メールに添付されたファイルを開封したり、リンクをクリックすると、マルウェアに感染する

水飲み場攻撃

標的となる組織の社員が利用する可能性が高いWebサイトを改ざんし、アクセスした際にマルウェアに感染する

ゼロデイ攻撃

まだパッチ（対策）が公開されていない未知の脆弱性を突く攻撃

狙われやすい組織の特徴

大企業
高度な研究成果や知財を保有しているため、攻撃者にとって魅力的な標的になります

重要インフラ事業者
金融、医療、交通などの社会基盤は、国家間の対立やテロ活動の一環として攻撃される可能性が非常に高くなります

政府機関
国の機密情報やインフラへの攻撃は、国家の安全保障を脅かす可能性があります

中小企業
大企業に比べてセキュリティ対策が不十分な場合が多く、比較的容易に侵入できるため狙われる可能性があります

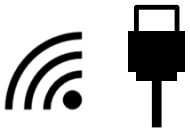
被害に遭わないために

不審なメールに注意する	• 不審なメールやウェブサイトを開かないよう注意する
不審なURLに注意する	• 不審なメールに記載されたURLをクリックしたり、添付ファイルを開かない
ソフトウェアを最新の状態に保つ	• OSやソフトウェアをアップデートし、最新の状態にする

被害に遭ってしまったとき

ネットワークから切断する

感染の拡大を防ぐため、該当端末をネットワークから切断しましょう。



被害時の状況を記録する

いつ、どんな操作をしていたか、どんなファイルを開いたか等、今後の調査のために詳細を記録しておきましょう。
※画面のスクリーンショットを撮影しておくと良いです

被害を報告する

個人の場合は、警察に相談しましょう。
組織の場合は、速やかに上司や（いる場合は）システム担当者に状況を報告しましょう。

※組織で決められた対応がある場合は、そちらに従い対応してください

個人ができる対策の中で、次の４つの対策について詳しく紹介します

- 適切なパスワード管理
- 認証方法を強化する
- 不審なメールに注意する
- ソフトウェアを最新の状態に保つ

適切なパスワード管理

認証方法を強化する

不審なメールに注意する

ソフトウェアを最新の状態に保つ

適切なパスワード管理とは

使い回しをしない

長く複雑に設定する

以前は「w4K_m&bU」のようなランダムな複雑性が求められていましたが、現在は、**長さとある程度の複雑さ（記号を含むなど）**を持ったパスワードの設定が良いとされています。

複数の単語を組み合わせて作る「**パスフレーズ**」を使用し、適切なパスワードを設定しましょう。

例　好きな食べ物 **オムライス** ＋ 好きな映画 **タイタニック** ＋ ペットのあだ名 **ナナちゃん**

↓

Omuraisu#Titanic#7chan

「12345678」や「password」のように
推測されやすいパスワードは設定しないでください！

参考：総務省「安全なパスワードの設定・管理-国民のためのサイバーセキュリティサイト」
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/06/

適切なパスワード管理とは

使い回しをしない

長く複雑に設定する

パスワードの定期変更

＋

定期的な漏えいチェック

パスワードの強度チェック「security.org」

パスワードの強度が十分かチェックしましょう

https://www.security.org/how-secure-is-my-password/

適切なパスワード管理とは

使い回しをしない

長く複雑に設定する

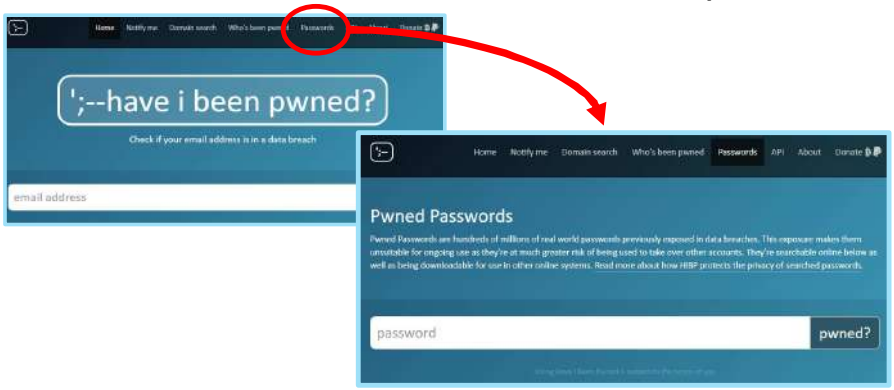
パスワードの定期変更

＋

定期的な漏えいチェック

参考

パスワードの漏えいチェック「Have I been pwned」



漏えいしていないか、チェックしてみてください

※漏えいしていた場合は、すぐに変更しましょう

https://haveibeenpwned.com/

適切なパスワード管理

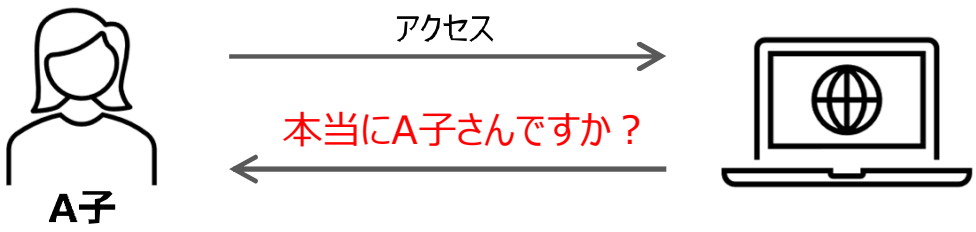
認証方法を強化する

不審なメールに注意する

ソフトウェアを最新の状態に保つ

認証とは？

コンピュータシステムやネットワークにアクセスする際に、アクセスを要求している人が正当なユーザーかどうかを判断するプロセスのことです。



認証の要素

知識要素（記憶）

- 本人だけが知っている情報（パスワード・秘密の質問　等）

所有要素（物理媒体）

- 本人だけが持っている情報（身分証・スマートフォン・ICカード　等）

生体要素（生体計測）

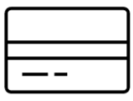
- 本人の身体的特徴（顔・指紋・虹彩　等）

パスワード認証

Webサイトにログインする際に、
IDとパスワードを入力する

知識要素

ICカード認証



電子マネー利用時やオフィス
入退室時にICカードをかざす

所有要素

生体認証

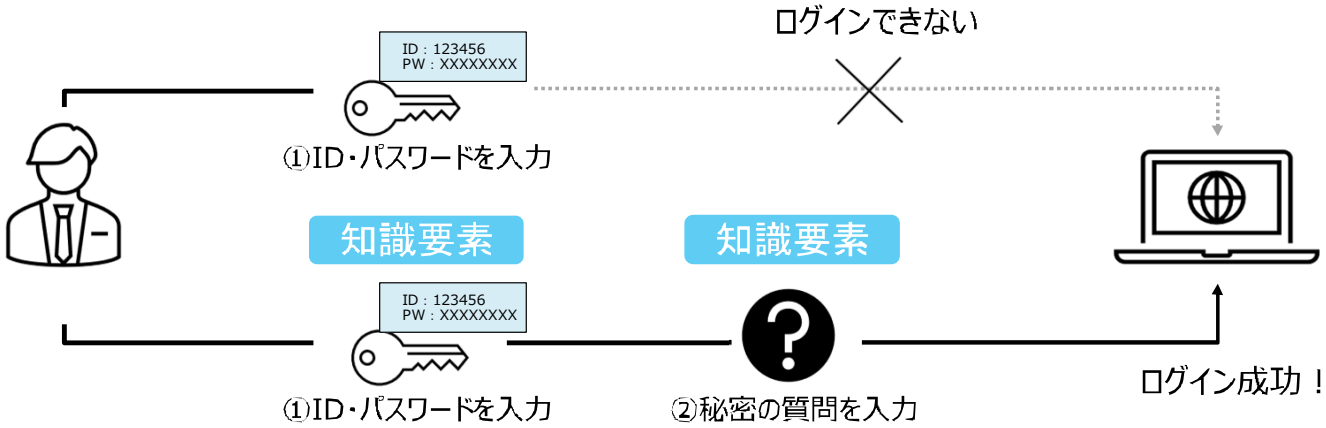
スマートフォンのロック解除時に
顔や指紋を利用する

生体要素

二段階認証と多要素認証について説明します

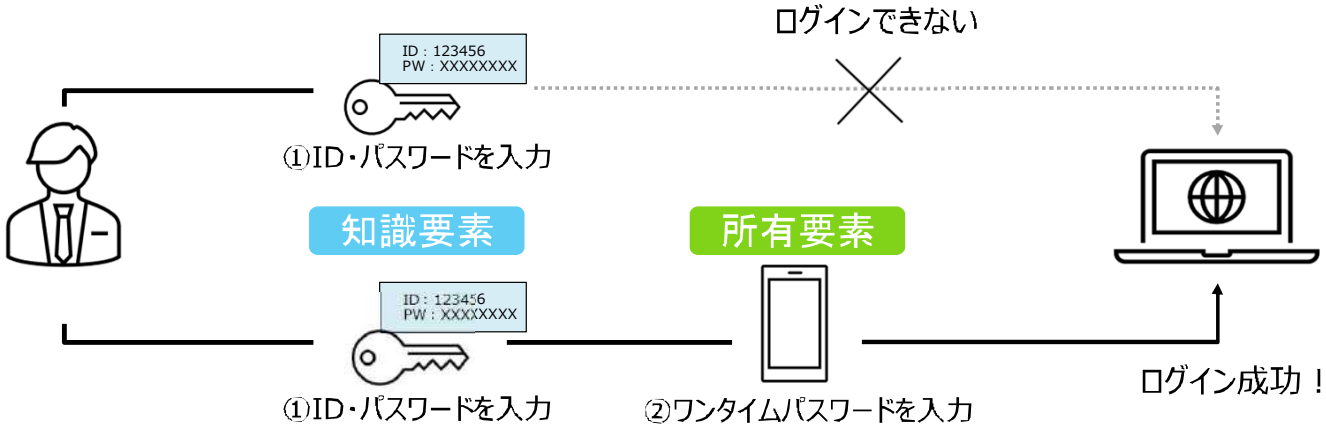
二段階認証

「二段階認証」とはインターネット上のサービスにログインする際に、認証の段階を２回に分けてアクセスする認証方法のことです。２段階の認証を行うことで、セキュリティを高めます。



多要素認証

「多要素認証」とはインターネット上のサービスにログインする際に、２種類以上の要素（多要素）を用いてアクセスする認証方法のことです。知識要素・所有要素・生体要素の３要素を組み合わせることで、セキュリティを高めます。



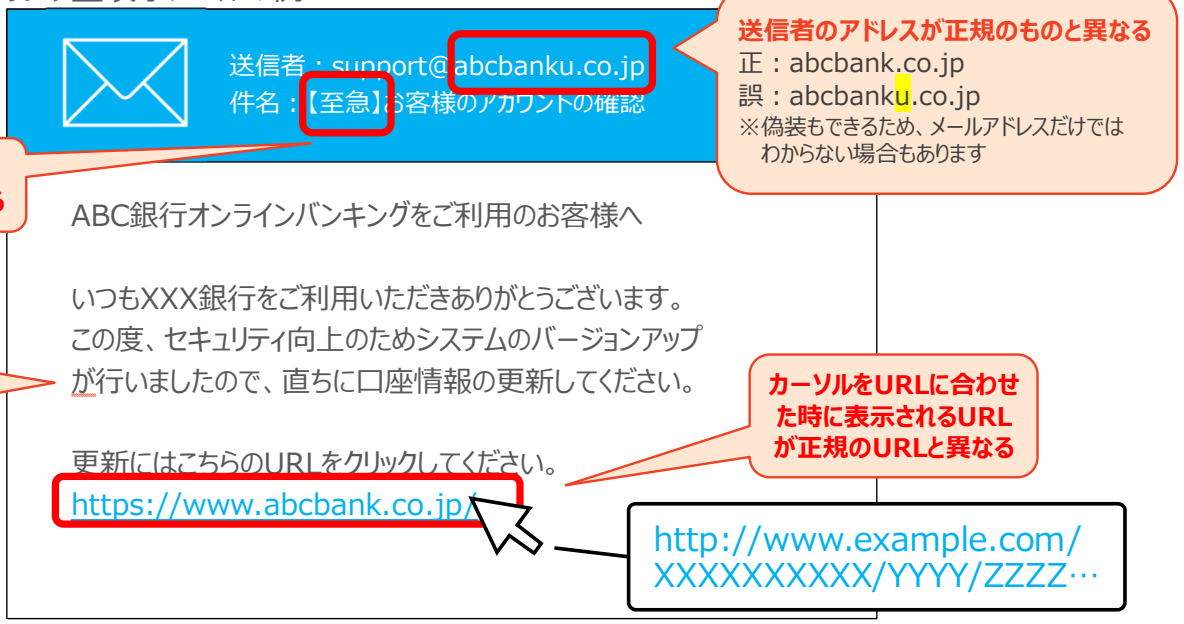
二段階認証と多要素認証の違いは？

	二段階認証	多要素認証
定義	認証を2段階で行う方式	異なる2つ以上の要素を組み合わせて認証を行う方式
要素	要素の種類を問わず2回使用する	知識要素、所有要素、生体要素のうち2つ以上
セキュリティ	セキュリティを強化	セキュリティを大幅に強化

- 適切なパスワード管理
- 認証方法を強化する
- **不審なメールに注意する**
- ソフトウェアを最新の状態に保つ

見分け方

リンク型攻撃メールの例



送信者のアドレスが正規のものと異なる
正：abcbank.co.jp
誤：abcbanku.co.jp
※偽装もできるため、メールアドレスだけでは
わからない場合もあります

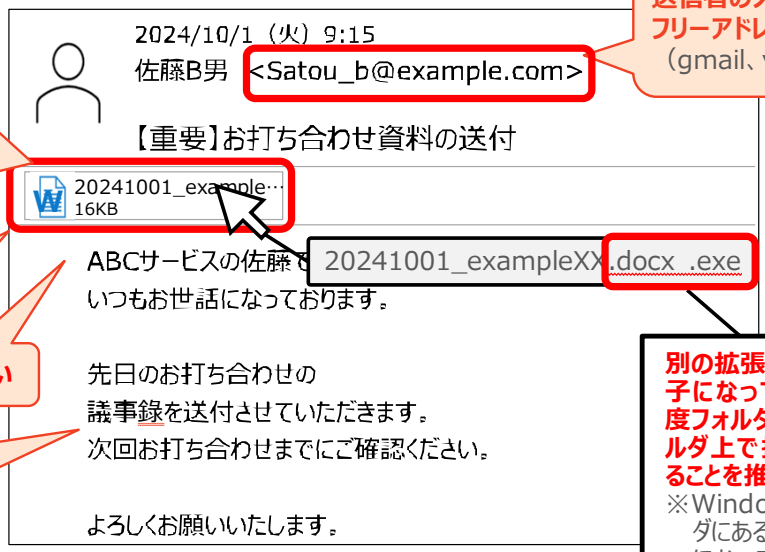
件名に【至急】など、開封を迫る言葉がある

誤字脱字が多いなど文面が不自然

カーソルをURLに合わせた時に表示されるURLが正規のURLと異なる

見分け方

添付型攻撃メールの例（やり取りしている取引先に成



送信者のメールアドレスがフリーアドレスになっている
（gmail、yahoo　など）

拡張子がexeのファイルが添付されている(ファイル名が見えない場合、カーソルを合わせて確認できます)
※拡張子とはファイルの種類を示す末尾に付けられた文字列で、「ワード：.docx」、「エクセル：.xlsx」、「パワポ：.pptx」、「実行ファイル：.exe」等があります

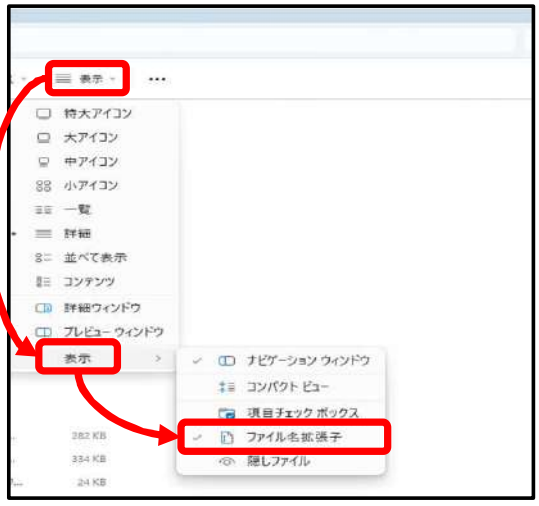
アイコンを偽装していることもある

宛名がない

日本語では使わない漢字が使われている
録 → 錄

別の拡張子に見えるよう、二重拡張子になっている場合もあるため、一度フォルダにファイルをコピーし、フォルダ上で拡張子をしっかりと確認することを推奨します。
※Windowsでは、デフォルトでフォルダにあるファイルの拡張子が非表示になっているため、表示されるよう設定を変更してください。

拡張子の表示方法



フォルダのツールバーにある「表示」をクリックし、一番下の「表示」から「ファイル名拡張子」をクリックします。

拡張子が表示されます。

参考

RLO攻撃に注意！

RLO攻撃とは、ファイルの名前を偽装して安全なファイルに見せかけることで、受信者にファイルを実行させマルウェアに感染させる攻撃です。手法としては古いですが、最近でも観測されている攻撃のため、注意してください。

RLO(Right-to-Left Override)

アラビア語など右から左に読む言語に対応するために、文字を右から左向きに書き換える文字。

ファイル名 「exampletxt.exe」

↓ eとtの間にRLOを入れると・・・

「exampleexe.txt」

拡張子を.txtに見せかけたexeファイルの完成！

不審なメールを見分けるために

- ✓ 送信元のメールアドレスをチェックする
- ✓ URLにカーソルを合わせて表示されるURLをチェックする
- ✓ 添付ファイルの拡張子をチェックする
- ✓ 本文の日本語が不自然ではないかチェックする
- ✓ 件名が開封を迫るような記載になっていないかチェックする
- ✓ 冒頭に宛名が書かれているかチェックする

適切なパスワード管理

認証方法を強化する

不審なメールに注意する

ソフトウェアを最新の状態に保つ

OSやソフトウェアのアップデートを行うと機能の追加などに加え、
セキュリティ上の問題点や不具合（脆弱性）の修正が行われます

アップデートを行わないとどうなる？

PCやスマートフォン等のソフトウェアをアップデートしましょう

④まとめ

本日紹介した脅威

サポート詐欺

フィッシング

ランサムウェア

内部不正

標的型攻撃

被害に遭わないために**今すぐできる**対策

適切なパスワード管理	・複数のサイトで同じパスワードを使っていませんか？ ・簡単なパスワードを設定していませんか？
不審なメールに注意する	・送信元の情報を確認していますか？ ・不審なメールを見分けるポイントを理解できていますか？
ソフトウェアを最新の状態に保つ	・PCやスマートフォンのOSアップデートを実施していますか？ ・アップデートが必要なものを放置していませんか？
冷静に判断する	・怪しいメールや広告を焦って開いたことはありませんか？
大切なデータはバックアップを取る	・大切なデータのコピーを別の場所に取っていますか？
＋	
認証方法を強化する	パスワードの適切な設定に加え、二段階認証や多要素認証が実装されたサービスでは、よりセキュリティを高めるため有効に設定しましょう。 **※業務で個人メールアドレス（Gmail等）を利用している場合は、組織を守るためにも有効にすべきです**

被害に遭ってしまったときの対応

ネットワークを遮断	感染が広がらないように、ネットワークから切り離しましょう
被害状況を記録	どんな画面やメッセージが表示されたかなど、被害時の状況を記録しましょう
被害を報告	個人の場合は警察やカード会社などの関連組織、組織の場合は上司やシステム担当者に報告しましょう ※個人のPCやスマートフォン、メールであっても、業務利用している場合は組織同様に上司やシステム担当者へ報告しましょう

隠さずに必ず報告！

参考

・安心相談窓口

IPAが国民のために開設している情報セキュリティに関する相談窓口

https://www.ipa.go.jp/security/anshin/about.html

参考

・インシデントかも？

厚生労働省が医療機関向けに開設している情報セキュリティに関する相談窓口

https://mhlw-training.saj.or.jp/incident/

最後に

セキュリティを他人事ではなく自分事と捉え、情報セキュリティ事故を未然に防げるようセキュリティへの意識を持ち、対策に取り組む必要があることを理解する

最後に

意識する	理解する	対策する
情報セキュリティは身近なものだという意識を持つ	意識をすると、どんなリスクがあるのかが見えてくる	リスクが見えてくると、そのリスクに対してすべき対策がわかる

× 情報セキュリティ事故を100%防ぐ

○ リスクを減らす

情報セキュリティを「**意識**」し、リスクを「**理解**」し、脅威への「**対策**」を実施してください