令和7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】
はじめての情報セキュリティコース

情報セキュリティの重要性

2025年10月23日
一般社団法人ソフトウェア協会

目次

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場合の影響

セキュリティが守られていないと、どのようなことが起こるのでしょうか？

情報の漏えい

システムの障害

↓

業務への影響

組織の損害

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なものです。

用語解説（1/2）

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

ソフトウェア　　ハードウェア

用語解説（2/2）

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

※ 一般的にコンピュータウイルスと呼ばれるもの

2．身近な情報セキュリティ

身近なセキュリティ

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

- 携帯電話とパソコンの機能を併せ持った情報端末
- 連絡先や写真、メール、ウェブサイトの閲覧履歴などの情報が入っている

身近なセキュリティ

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

- PCやスマートフォンで世界中の情報にアクセスしたり、コミュニケーションをとったりするためのサービスの総称
- 例：チャットサービスや決済サービス

身近なセキュリティ

セキュリティ対策をしていないとどうなるでしょうか？

マルウェアに感染	不正なアクセス	詐欺被害
不審なサイトやメールを開く、OSやアプリの脆弱性を狙われる等によりマルウェアに感染	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	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の被害に

さまざまなリスクがあります。

身近なセキュリティ

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

日常的に行っているごみ捨てにもセキュリティの危険性が・・・

身近なセキュリティ

郵便物

書類

メディア

電子機器

廃棄する前にすべき対策があります。

身近なセキュリティ

廃棄する前にすべき対策

- シュレッダー等を利用し、細かく切断する
- 個人情報部分を切り取る

- シュレッダー等を利用し、細かく切断する
- 個人情報部分を切り取る

身近なセキュリティ

廃棄する前にすべき対策

- 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

- データを完全に消去できる専用ソフトを利用する
- ハードディスクを物理的に破壊する
- 初期化し、SIMカード等を抜き取る
- 専門業者に依頼する

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。

情報セキュリティ10大脅威

「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	**機密情報等を狙った標的型攻撃**
インターネット上のサービスへの不正ログイン	サプライチェーンや委託先を狙った攻撃
クレジットカード情報の不正利用	システムの脆弱性を突いた攻撃
スマホ決済の不正利用	地政学的リスクに起因するサイバー攻撃
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**
ネット上の誹謗・中傷・デマ	ビジネスメール詐欺
フィッシングによる個人情報等の詐取	不注意による情報漏えい等
不正アプリによるスマートフォン利用者への被害	分散型サービス妨害攻撃（DDoS攻撃）
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**ランサム攻撃による被害**
ワンクリック請求等の不当請求による金銭被害	リモートワーク等の環境や仕組みを狙った攻撃

出典：IPA（https://www.ipa.go.jp/security/10threats/10threats2025.html）

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

被害に遭った場合の影響

サポート詐欺の被害に遭うと、どのような影響があるのでしょうか？

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。

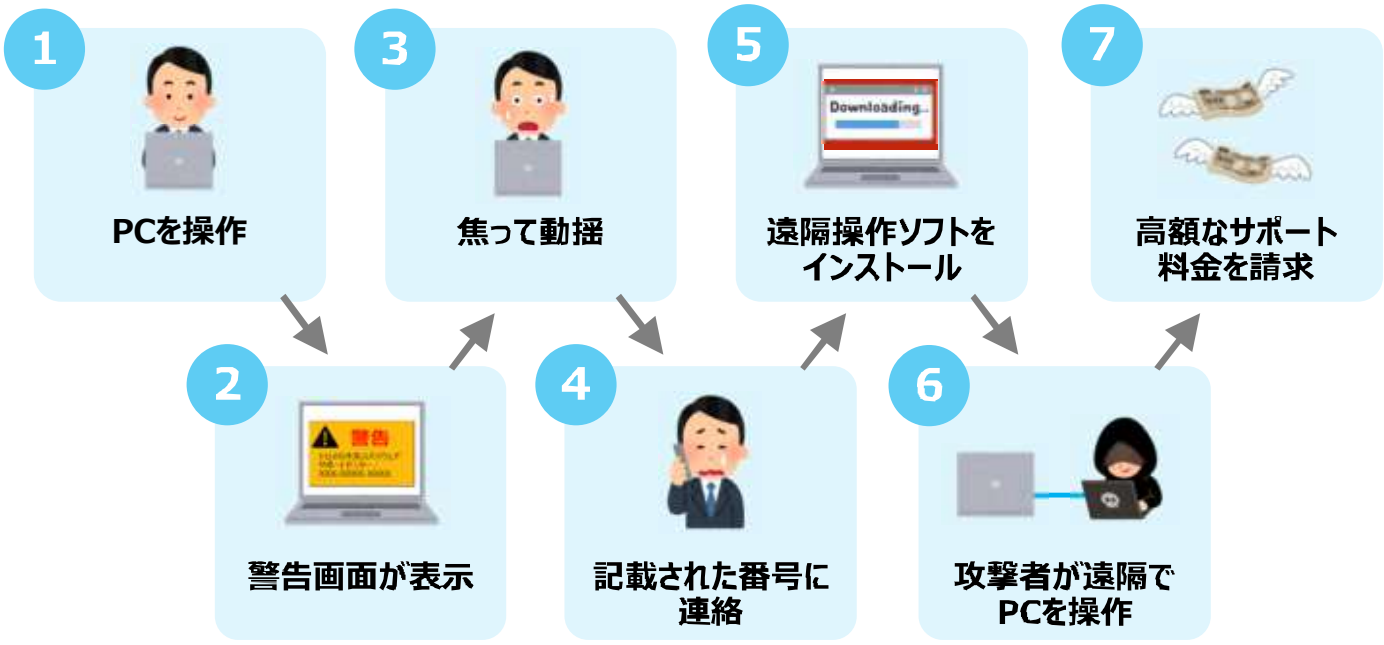
情報機器の機能不全

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



警告画面が表示される原因

なぜ警告画面が表示されてしまうのでしょうか？

- **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。
- **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。
- **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ける役割

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

サポート詐欺の被害に遭わないためにできることを紹介します。

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場合

ネットワークから切断する	被害時の状況を記録する	被害を報告する
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。	操作内容や開いたファイルを記録し、必要に応じてスクリーンショットも残しておきましょう。	個人は警察やカード会社へ、組織は上司やシステム担当者へ速やかに相談・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。

（参考）警告画面が出た場合に備えて

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

フィッシング

フィッシング詐欺とは

フィッシング詐欺とは、銀行や有名な企業を装ってメールやSMS（ショートメッセージ）、偽のWebサイトに誘導し、**パスワードやクレジットカード番号などの個人情報をだまし取る**詐欺です。

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/xxxxxxxxx

被害に遭った場合の影響

フィッシング詐欺の被害に遭うと、どのような影響があるのでしょうか？

個人情報の漏えい

クレジットカード情報、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。

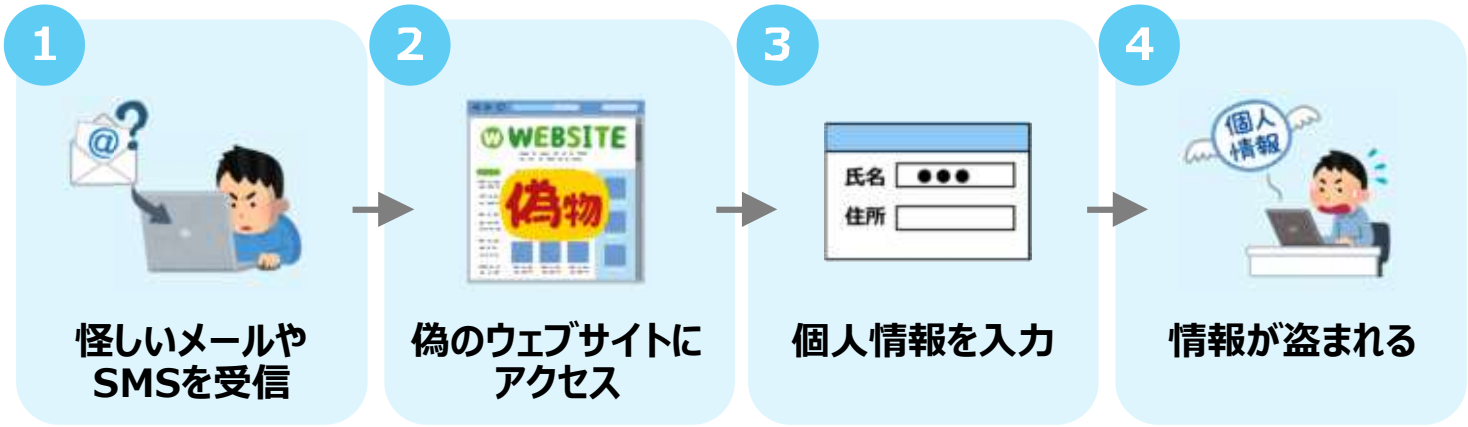
金銭的被害

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。

アカウントの乗っ取り

アカウントを乗っ取られ、本人になりすましてメッセージを送られたり、周囲に迷惑をかける可能性があります。

フィッシング詐欺の被害イメージ



被害に遭わないために

フィッシング詐欺の被害に遭わないためにできることを紹介します。

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場合

ネットワークから切断する	被害時の状況を記録する	被害を報告する
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。	操作内容や開いたファイルを記録し、必要に応じてスクリーンショットも残しておきましょう。	個人は警察やカード会社へ、組織は上司やシステム担当者へ速やかに相談・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。

ランサムウェア

ランサムウェアとは

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て利用できなくさせ、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。

被害に遭った場合の影響

ランサムウェアの被害に遭うと、どのような影響があるのでしょうか？

暗号化と業務の停止

ファイルが暗号化され、普段利用している業務データが開けなくなるため、業務や作業が停止してしまいます。

身代金の要求

暗号化されたファイルやシステムを元に戻すために、攻撃者からお金を要求されます。

情報漏えいのリスク

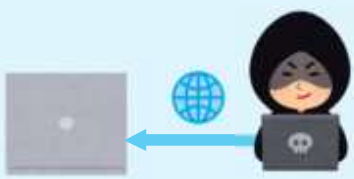
患者情報等の大切な情報が外部に漏えいし、悪用される可能性があります。

感染経路

ランサムウェアにはどのように感染するのでしょうか？

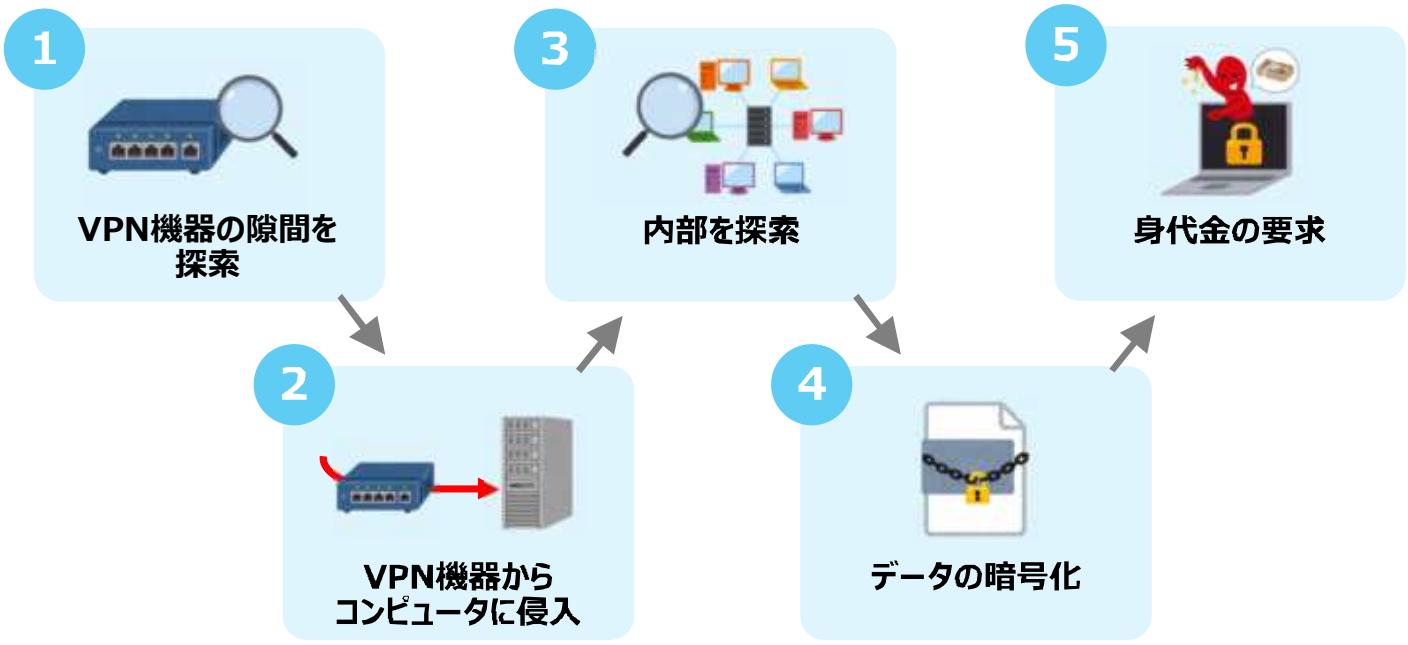
VPN機器からの侵入

リモートデスクトップからの侵入



不審メール・添付ファイルからの侵入

ランサムウェアの攻撃イメージ（VPN機器からの侵入例）



被害に遭わないために

ランサムウェア攻撃の被害に遭わないためにできることを紹介します。

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重要なものがある場合はコピーを取りサーバに保存する等、自身で管理する

被害に遭ってしまった場合

ネットワークから切断する	被害時の状況を記録する	被害を報告する
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。	操作内容や開いたファイルを記録し、必要に応じてスクリーンショットも残しておきましょう。	個人は警察へ、組織は上司やシステム担当者へ速やかに相談・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。

内部不正

内部不正とは

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。

発生した場合の影響

内部不正が起こると、どのような影響があるのでしょうか？

経済的な損失

患者情報等の流出により、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。

職員への影響

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。

信頼の低下

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。

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

内部不正を防ぐために**組織が**できることを紹介します。

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！

標的型攻撃

標的型攻撃とは

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	特定の人物や組織を狙い、取引先や同僚を装ったメールを送り、添付ファイルや偽サイトで情報を盗む攻撃です。
水飲み場攻撃	メールのやり取りなどで信頼関係を築き、改ざんした正規サイトにアクセスさせマルウェアに感染させる攻撃です。
ゼロデイ攻撃	開発者がまだ修正していない脆弱性を突き、パッチ（対策）が出る前にシステムに侵入・悪用する攻撃です。

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あります

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いため、狙われる可能性があります

被害に遭わないために

標的型攻撃の被害に遭わないためにできることを紹介します。

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場合

ネットワークから切断する	被害時の状況を記録する	被害を報告する
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。	操作内容や開いたファイルを記録し、必要に応じてスクリーンショットも残しておきましょう。	個人は警察へ、組織は上司やシステム担当者へ速やかに相談・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。

対策を学ぶ

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見てみましょう。

- **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**
- **長さを確保する**
- **適度に複雑化する**

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

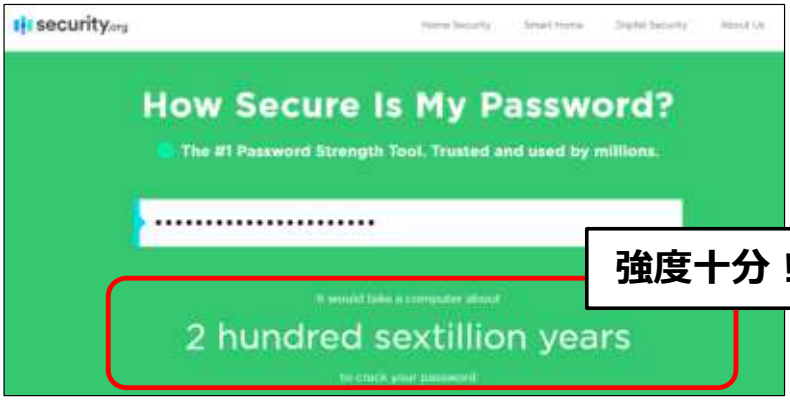
長さを確保する

適度に複雑化する

＋

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（参考）

使い回しをしない

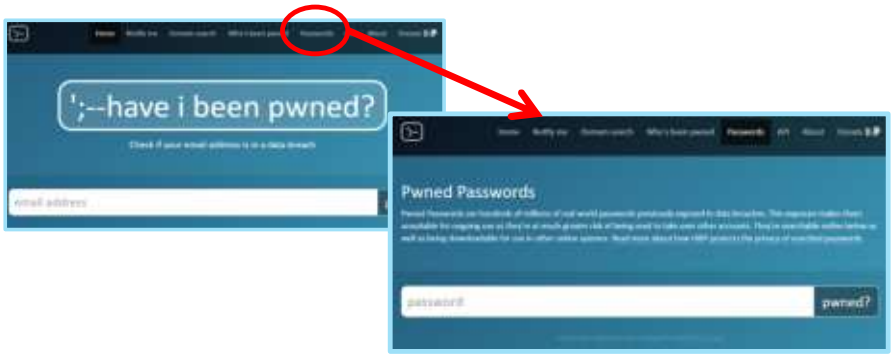
長さを確保する

適度に複雑化する

＋

定期的な漏えいチェック

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/

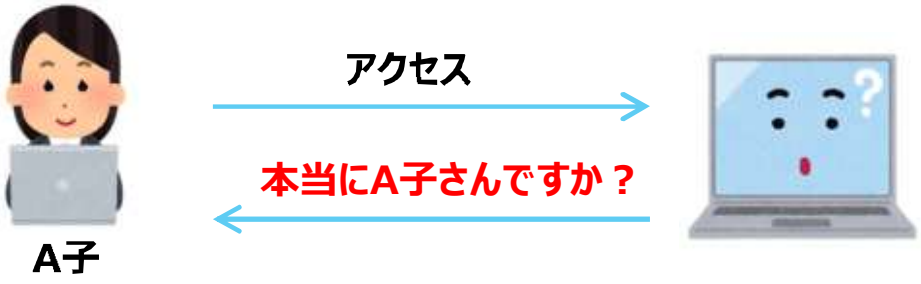
対策を学ぶ

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見てみましょう。

- 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

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本当に本人かどうかを判断する仕組み**のことです。



認証の要素

認証には大きく分けて3つの要素があります。

知識要素（記憶）

本人だけが**知っている**情報

パスワード

PINコード

所有要素（物理媒体）

本人だけが**持っている**情報

スマートフォン

マイナンバーカード

生体要素（生体計測）

本人の**身体的特徴**

顔

指紋

認証の要素

知識要素

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

所有要素

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

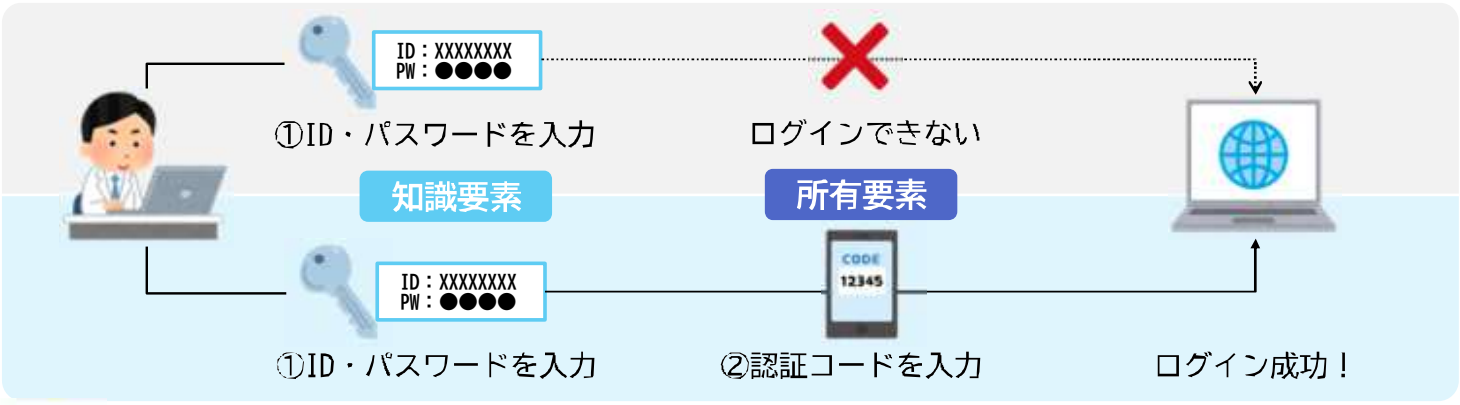
生体要素

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

多要素認証とは

認証を強化するためには、多要素認証が利用できます。多要素認証とは、ログイン時に**２種類以上の認証の要素を用いて本人確認する**認証方法のことです。



多要素認証を設定したシステムやサービスでは、ID・パスワードを入力しただけではログインできず、デバイスや本人の生体情報が必要なため、**万が一パスワードが漏えいした場合にも、不正ログインを防ぐことができる**可能性が非常に高いです。

対策を学ぶ

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見てみましょう。

適切なパスワード管理

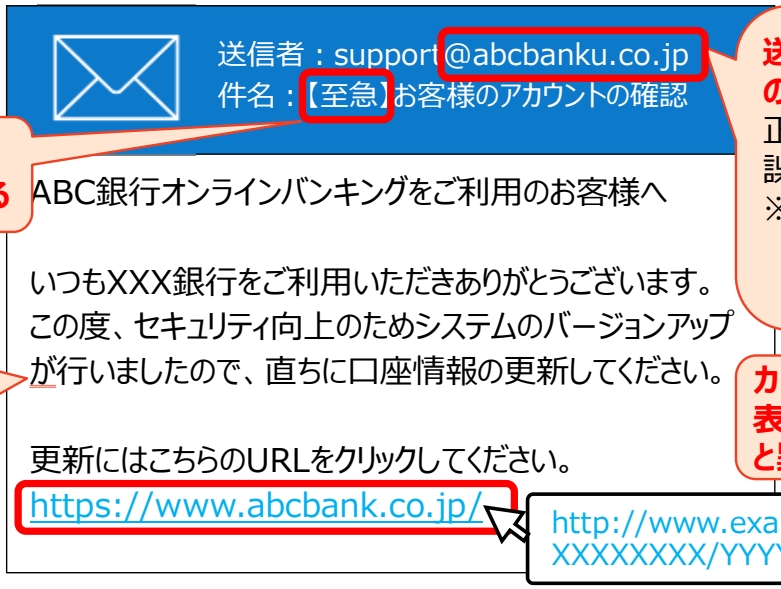
認証方法を強化する

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



件名に【至急】など、開封を迫る言葉がある

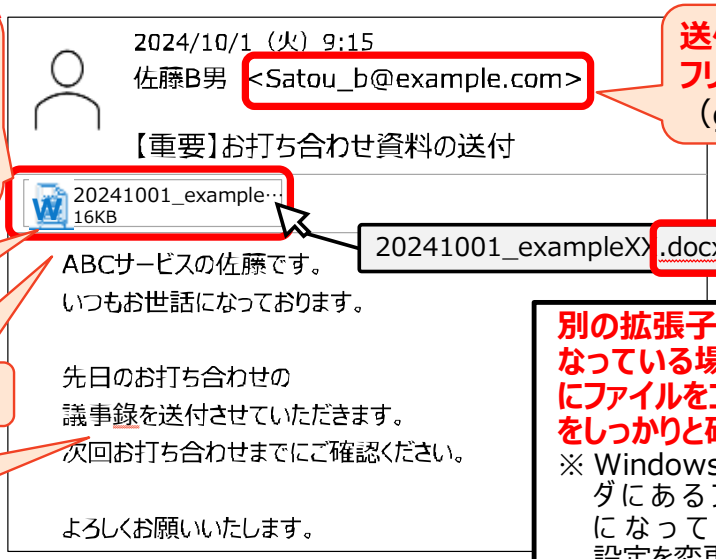
送信者のアドレスが正規のものと異なる
正：abcbank.co.jp
誤：abcbanku.co.jp
※ 偽装もできるため、メールアドレスだけではわからない場合もあります

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（取引先に成りすましたメール）



拡張子がexeのファイルが添付されている
※ 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。
例：「ワード：.docx」、「エクセル：.xlsx」等

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）

アイコンを偽装していることもある

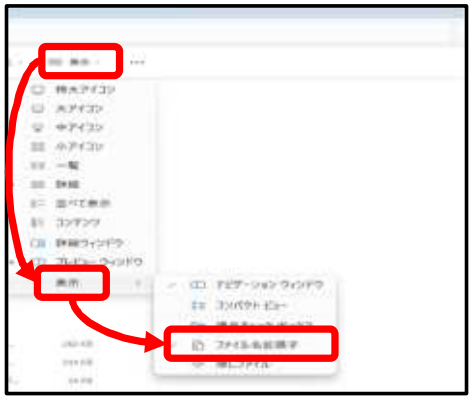
宛名がない

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。

（参考）拡張子の確認方法：Windows

任意のフォルダにファイルを保存します。



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」

↓ et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

対策を学ぶ

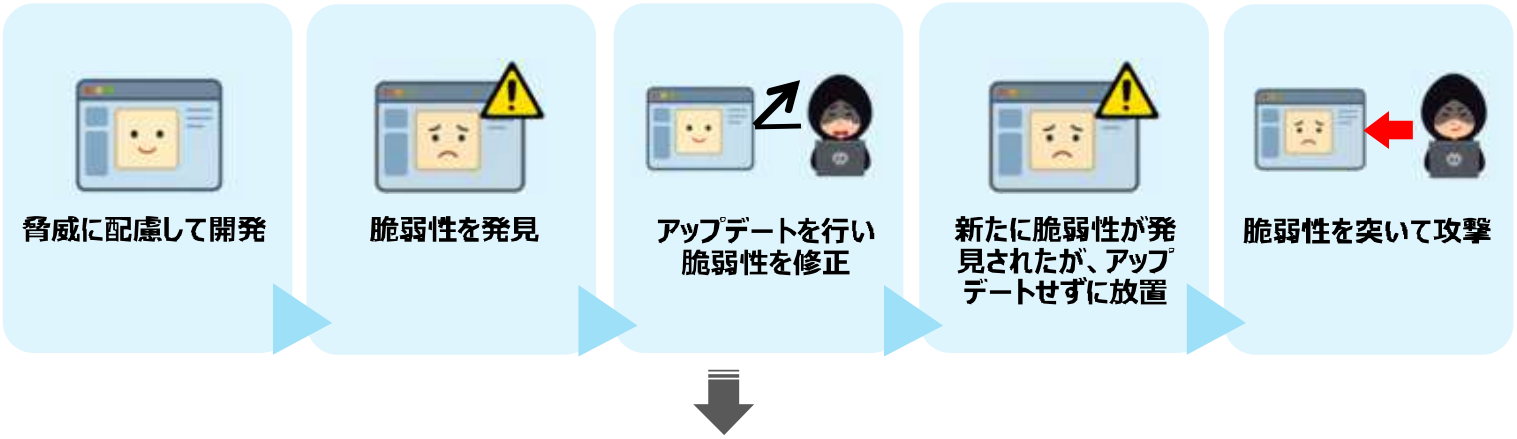
個人ができる対策の中で、次の4つの対策について詳しく見てみましょう。

- 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**

ソフトウェアの更新

ソフトウェアの更新により、**脆弱性を修正**することができます。

更新（アップデート）を行わないと・・・



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

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？

被害に遭わないために今すぐできる対策

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、多要素認証の機能を有効に設定しましょう。

※ **指示のもとで個人メールアドレス（Gmail等）を業務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場合の対応

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

隠さずに必ず報告！

- 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、指示のもと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

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/index.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://mist.mhlw.go.jp/incident/

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、どのよう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。