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】
メールとパスワード管理コース

誰でも実践できるメールセキュリティとパスワード管理

2025年9月18日
一般社団法人ソフトウェア協会

目次

目的

■ **日常的に利用するメールやパスワードに潜むリスクを知り、正しい利用方法を身に付けることで、情報漏えいやサイバー攻撃を未然に防ぐことができるようになること**

- 安全なパスワードの作成および管理方法を理解し、実践できるようになること
- メール誤送信が及ぼすリスクを理解し、防ぐための対策を実践できるようになること
- 不審メールの特徴や見分け方を学び、被害に遭わない判断力を身に付けること
- フィッシング詐欺の手口やその影響を理解し、対策を実践できるようになること

認証とパスワード管理について

認証とは？

認証とは、**「その人が本当に本人かどうか確かめる仕組み」**です。

業務では・・・

PCにログインしたり、
電子カルテを開いたり…

プライベートでは・・・

スマートフォンを開いたり、
アプリにログインしたり…

普段から**認証**を利用していると思います。

認証の要素

本人かどうかを確かめるために使う情報や手段の種類のことを、**認証の要素**と言い、認証の要素は、大きく３つに分類されます。

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

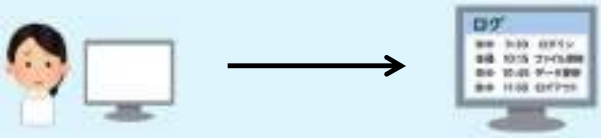
指紋

なぜ「認証」が必要なのか？

- なりすまし防止のため
- 責任の所在を明確にするため
- 大切な情報・サービスを守るため
- 安心してサービスを利用するため

認証は、アクセスしようとしている人が本当に登録された本人かどうかを確認するために必要です。これにより、**なりすましによる不正アクセスを防ぐ**ことができます。

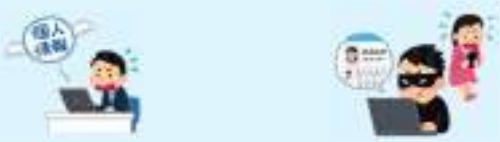
認証を行うことで「誰が、いつ、何をしたか」を記録できるため、トラブルが発生した際に**利用履歴を追跡して原因を調べる**ことができます。



なぜ「認証」が必要なのか？

- なりすまし防止のため
- 責任の所在を明確にするため
- 大切な情報・サービスを守るため
- 安心してサービスを利用するため

認証によって、個人情報や機密情報を正当な利用者だけが扱えるようにし、**大切な情報の漏えいや、サービスの不正利用を防ぐ**ことができます。



認証の仕組みが整っていることで、自身のアカウントや情報が守られているという**信頼感を持ち、安心してサービスを利用する**ことができます。

パスワードの適切な扱い

皆さんが日常的に使っている認証の中でも、最もよく使われているものが、「**パスワード**」です。パスワードは身近な認証方法ですが、実は最も破られやすく狙われやすいもののため、**どのように扱うのか**が大切です。

弱いパスワードの危険性

安全なパスワードの設定

認証の強化

３つの側面からパスワードの安全な利用方法を学びましょう。

弱いパスワードの危険性

【シナリオ】パスワード漏えいによる不正アクセス

弱いパスワードの設定により、どのような被害に遭ってしまうのかを見てみましょう。

1.
看護師の田中さんは、業務中に電子カルテにログインしました。パスワードは名前と誕生日です。

2.
攻撃者は、攻撃ツールを使いパスワードを推測し、田中さんのアカウントに不正アクセスしました。

3.
後日、田中さんは、夜中に身に覚えのないログイン履歴が残っていることに気が付きました。

4.
システム部門が異常なアクセスを検知し、患者情報が外部に流出した可能性が発覚しました。

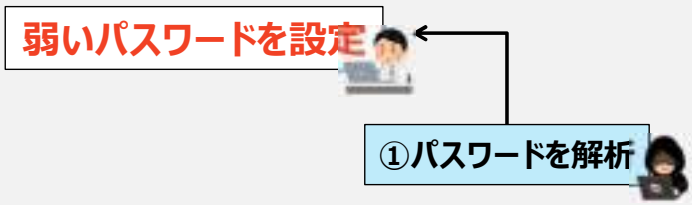
弱いパスワードを使う危険性

弱いパスワードを使うことで、どのような危険があるのでしょうか。

①パスワードを解析

攻撃者が専用ツール等を利用し、**膨大なパスワードを自動的に試すことで、短時間でパスワードが解析されてしまう**危険があります。

イメージ図

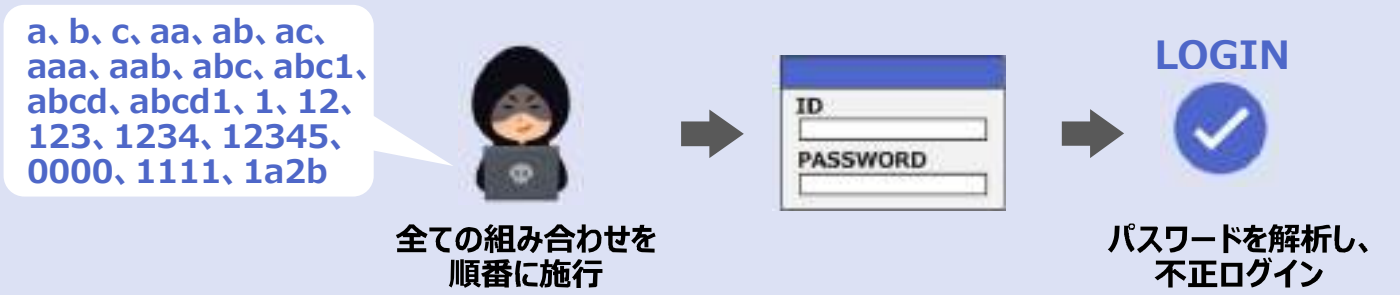


主なパスワード解析方法

パスワードの主な解析方法とその仕組みをご紹介します。

■ ブルートフォース攻撃（総当たり攻撃）

ブルートフォース攻撃とは、**パスワードを構成できるすべての文字の組み合わせ**（例：a、aa、aab　等）を試していく攻撃手法です。1 秒間に何千～何百万通りの速さで機械的にすべて総当たりするため、短く単純なパスワードは数分で解析されてしまいます。



主なパスワード解析方法

パスワードの主な解析方法とその仕組みをご紹介します。

■ 辞書攻撃

辞書攻撃（Dictionary Attack）とは、事前に用意した**パスワードとしてよく使われる単語やフレーズを集めたリスト**に従って、順番に試していく攻撃手法です。リストには何百万もの単語やフレーズがまとめられていて、攻撃ツールを利用すると一瞬で試行できてしまいます。

主なパスワード解析方法

パスワードの主な解析方法とその仕組みをご紹介します。

■ クレデンシャルスタッフィング

クレデンシャルスタッフィングとは、**過去に別のサービスから流出したIDとパスワードの組み合わせをそのまま再利用し、ログインを試みる**攻撃手法です。攻撃者は、漏えいした認証情報を大量に保有しており、それを使って様々なサービスに自動でログインを試す専用ツールを使用します。

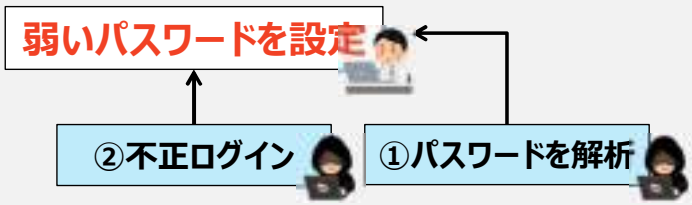
弱いパスワードを使う危険性

弱いパスワードを使うことで、どのような危険があるのでしょうか。

②不正ログイン

①で解析したパスワードを使って、**システムやアカウントに不正ログインされてしまう**可能性があります。

イメージ図



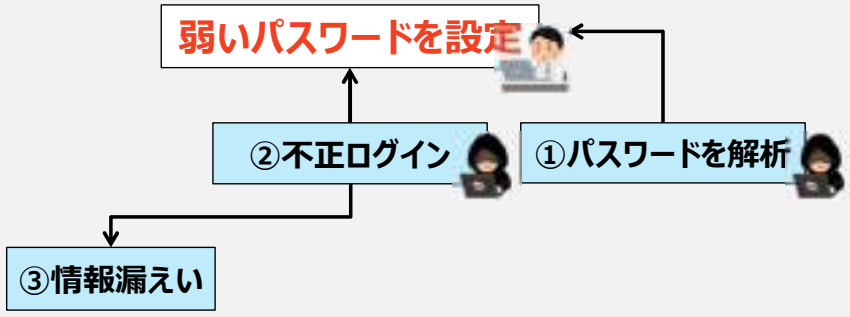
弱いパスワードを使う危険性

弱いパスワードを使うことで、どのような危険があるのでしょうか。

③情報漏えい

不正ログインされたシステム等に、**患者情報や機密情報といった重要な情報が保管されている場合、その情報が漏えい**してしまいます。

イメージ図



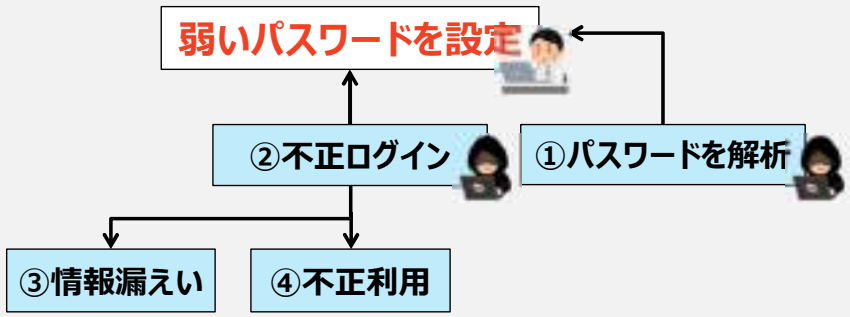
弱いパスワードを使う危険性

弱いパスワードを使うことで、どのような危険があるのでしょうか。

④不正利用

アカウントに不正ログインされると、その人になりすまし、例えばオンラインショッピングやSNS投稿等、**サービスを不正利用される**可能性があります。

イメージ図



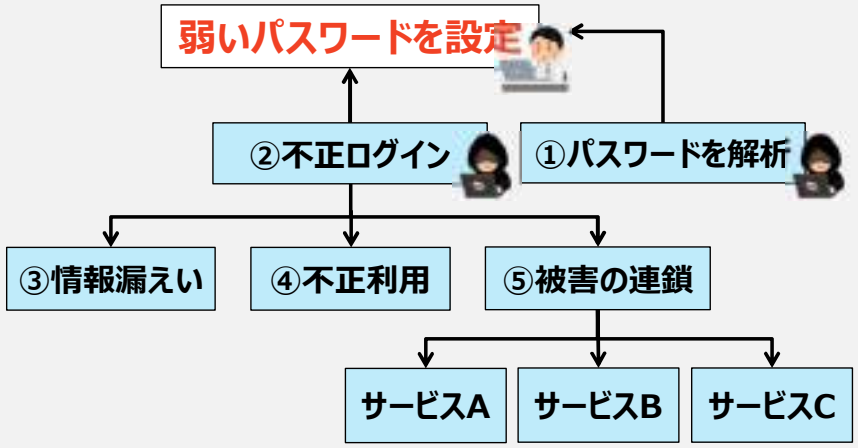
弱いパスワードを使う危険性

弱いパスワードを使うことで、どのような危険があるのでしょうか。

⑤被害の連鎖

もし複数のサービスで同じパスワードを設定していた場合、**１つ破られると次々と他のサービスにも不正ログインされ、被害が連鎖する**可能性があります。

イメージ図



“弱いパスワード”とは？

下記のようなパスワードは**“弱いパスワード”**です。利用しないようにしましょう。

- **連番や単純な数字 ・・・123456、0000**
- **単語そのまま ・・・password、login**
- **名前や生年月日 ・・・hanako、19950401**
- **キーボードの配列 ・・・qazwsx、qwerty**
- **名前＋数字 ・・・sato123、taro918**
- **短いパスワード ・・・abc01、pw01**

⚠ 使い回しにも注意！

パスワードを複数のサービスで使い回ししている場合、**1つのサービスでパスワードが漏れてしまうと、同じパスワードを使っている他のサービスにも不正アクセスされるおそれがある**ため、パスワードの使い回しはしないようにしましょう。

安全なパスワードの設定

安全なパスワードとは？

安全なパスワードを設定するためには、３つのポイントを意識しましょう。

１．長さを確保する

パスワードの文字数が増えると解読が困難になります。長ければ長いほど安全になるため、出来るだけ長く設定しましょう。

２．適度に複雑化する（文字種は制限しない）

大文字・小文字・数字・記号といった文字種は強制せず、予測されないある程度の複雑性を持たせたパスワードを設定することで、安全性を確保できます。（前頁の弱いパスワードは避けましょう。）

３．使い回しをしない

パスワードを使い回すと漏えいのリスクが高まり、漏えい時の被害が拡大してしまうため、各サービスに異なるパスワードを設定しましょう。

パスフレーズとは？

安全なパスワードを作成するには、「**パスフレーズ**」を活用できます。パスフレーズとは、複数の単語を組み合わせて作成するパスワードのことです。

パスフレーズの**メリット**は？

- 好きな言葉の組み合わせや文章を利用するため覚えやすく、**文字数も自然と長くなる**
- 辞書にある単語やよくある組み合わせと違い、意味のある文章は予測が難しく、**複雑性を持たせることができる**

CLEAR！

長さを確保する

適度に複雑化する

パスフレーズは、安全なパスワードに必要なポイントを２つクリアできます。

パスフレーズの作成方法

どのように作成するのか、パスフレーズの作成例をご紹介します。

例１ 単語を組み合わせたタイプ

好きな季節		その季節のイベント		その季節の食べ物
Natsu	＋	Hanabi	＋	kakigori

↓

72#Hanabi#Kakigori

「Natsu」を「72」のように単語を数字に置き換えたり、単語同士を記号で繋げる等、使う文字種を増やす・複雑性を高めることでよりセキュリティが高くなります。

例２ 文章にしたタイプ

タイタニック		の		ジャック		と		ローズ
Titanic	＋		＋	Jack	＋		＋	Rose

↓

T1tan1cnoJack&Rose1912

「I」を「1」のようにローマ字を数字に置き換えたり、「and」を「＆」のように記号化する、さらに、関連する数字や記号（例ではタイタニック号の沈没した年）を付けることでよりセキュリティが高くなります。

自分だけが知っている情報や、オリジナルの文章でパスフレーズを作成しましょう。

定期的なパスワード漏えい状況のチェック

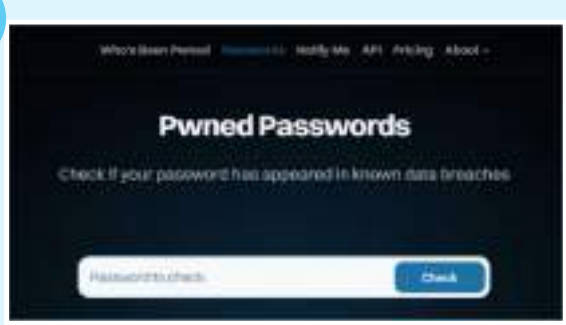
安全にパスワードを利用するためには、３つのポイントに加えて**定期的な漏えいチェック**が有効です。漏えい状況を確認するには、「**Have I Been Pwned**」というサービスがあります。

1

https://haveibeenpwned.com/

URLからサイトにアクセスし、上部にある「Passwords」をクリックします。

2



「Pwned Passwords」で、漏えい状況を確認したいパスワードを入力します。

定期的なパスワード漏えい状況のチェック

安全なパスワードを利用するためには、３つのポイントに加えて定期的な漏えいチェックが有効です。漏えい状況を確認するには、「**Have I Been Pwned**」というサービスがあります。

3

漏洩していない場合

現在漏えいしていない場合でも、**定期的に漏えい状況を確認しましょう。**（漏えいしていない＝安全なパスワードではありません。）

漏洩している場合

漏洩している場合は、**すぐに使用を止め、パスワードを変更しましょう。**（変更する際は、弱いパスワードを設定しないで下さい。）

オススメのパスワード管理方法

安全なパスワードは、長くて適度に複雑で、サービス毎に異なるパスワードでなければいけないため、覚えづらく、パスワードの管理が難しいです。そこで、おすすめの管理方法をご紹介します。

STEP 1

基本となる**コアパスワード**を決める。

72#Hanabi#Kakigori

STEP 2

サービス毎のパターンを決める。

Google	→	ggl
Amazon	→	amzn
さくら銀行	→	skr

STEP 3

コアパスワードとサービス毎のパターンを合わせてパスワードを作成する。

Google

↓

72#Hanabi#Kakigori_ggl

パスワードが覚えやすく、管理がラク！ &「使い回しをしない」をクリアできます！

認証の強化

認証の強化が必要？

パスワードによる認証は一般的ですが、最近は「**パスワードだけでは不十分**」だと言われています。その理由を見ていきましょう。

■ 簡単なパスワードが多いため

多くの人が未だに「弱いパスワード」を利用し続けてしまっているため、簡単にパスワードを解析されてしまいます。

■ 使い回しによる被害が発生するため

多くの人が同じパスワードを複数のサービスで使い回してしまっているため、１つが漏れると他のアカウントにも被害が出てしまいます。

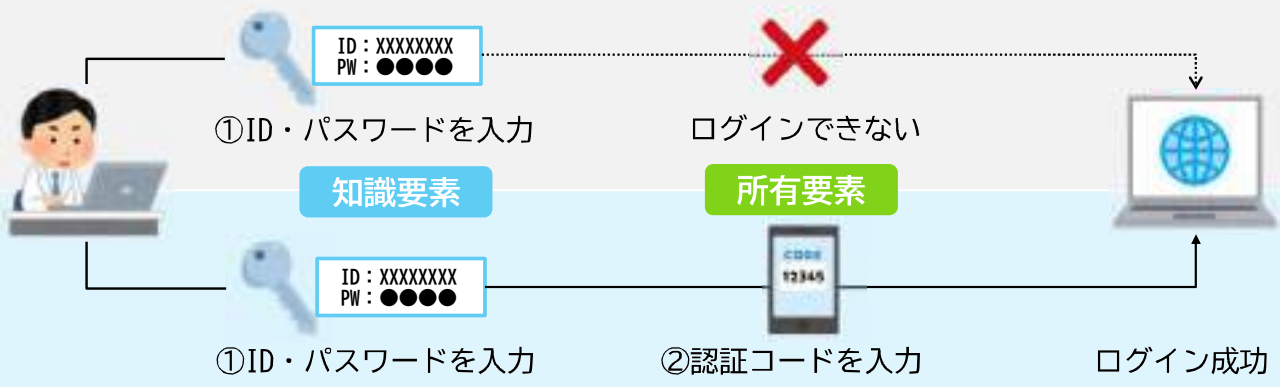
■ 攻撃手法が進化しているため

専用のソフトによる高速なパスワード自動試行によりパスワード解析が容易になったり、フィッシング詐欺等の攻撃により、複雑なパスワードでも盗まれてしまいます。

認証を強化する方法をご紹介します。

認証の強化方法を知ろう（多要素認証）

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。

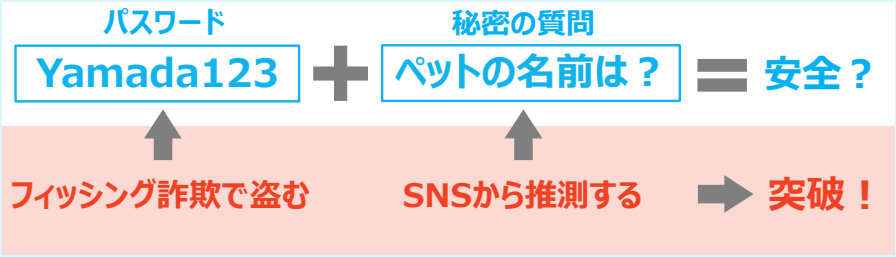


多要素認証を設定したシステムやサービスでは、ID・パスワードを入力しただけではログインできず、デバイスや本人の生体情報が必要なため、**万が一パスワードが漏えいした場合にも、不正ログインを防ぐことができる**可能性が非常に高いです。

認証の強化方法を知ろう

例えば、「パスワードのあとに“秘密の質問”を聞かれる認証」があります。これは「知識要素と知識要素」ですが、認証が強化できているのか見てみましょう。

例



一見、二段階の認証を行っているため安全に見えます。しかし、実際はどちらも知識要素のため、**どちらも“知っていれば”簡単に破られてしまいます。**

認証について

「医療情報システムの安全管理に関するガイドライン　第6.0版」

令和9年度時点で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、**原則として二要素認証を採用する**こと。

※「二要素認証」とは、異なる2つの認証の要素を用いて本人確認する認証方法です。

「医療情報システムの安全管理に関するガイドライン」
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

2種類以上の異なる要素を用いた多要素認証を利用しましょう！

メールセキュリティについて

メールセキュリティを学ぶ

皆さんの日々の業務に欠かせない「**メール**」には、あらゆるリスクが潜んでいます。メール利用時のたった一度のミスや不注意が、患者情報の漏えいや組織全体への影響につながることもあるため、**メールセキュリティ**について学び、実践していくことが大切です。

メール誤送信	不審メール	フィッシング詐欺

今回は、特に注意すべき３つについてご紹介します。

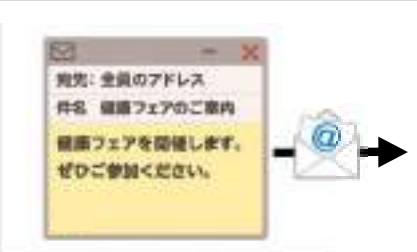
メール誤送信

【シナリオ】メール誤送信による情報漏えい

メールの誤送信により、どのような影響が出るのかを見てみましょう。

1.
事務職員の山田さんは、院内で開催する「健康フェア」というイベントの案内メールを送ろうとしています。

2.
山田さんは、BCC欄に入力したつもりが、急いでいたため、全員のアドレスをTo欄に入力して送信してしまいました。



3.
送信してから1時間後、受信者から「全員のアドレスが見えていますよ。」と、連絡が入りました。

4.
誤送信により、本来は見えないはずのメールアドレスが全員に公開され、情報が漏えいしてしまいました。

メール誤送信により情報が漏えいした場合の影響は？

- **信頼を損失する**
- **情報が回収できない**
- 更なる情報漏えいが起こる
- メールアドレスを悪用される

もしも患者の診療情報等が無関係な第三者に誤送信された場合、「本当にこの病院に情報を預けてよいのか？」と疑われ、患者や家族の信頼を失う可能性があります。

もしも知らない人のメールアドレス宛に情報を誤送信してしまった場合、一度送信したメールは取り消すことができないため、相手の手元にその情報が残り続ける可能性があります。

メール誤送信により情報が漏えいした場合の影響は？

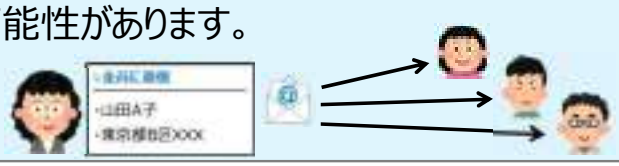
信頼を損失する

情報が回収できない

更なる情報漏えいが起こる

メールアドレスを悪用される

もしも複数人をToに設定し誤送信したメールに対し、受信者が「全員に返信」した場合、受信者がメール内に個人情報を記載し、更なる情報漏えいが発生してしまう可能性があります。



もしも誤送信によりメールアドレスが第三者に漏えいしてしまった場合、メールアドレスを詐欺師に悪用され、詐欺メールや不審な連絡が届いてしまう可能性があります。

メール誤送信のよくあるミス

宛先を間違える

似た名前の別人を選択、意図しない相手に送信してしまうことがあります。自動補完機能（入力途中で候補が表示される機能）の選択ミスが原因になることもあります。

宛先を「Cc」で一斉送信してしまう

本来「Bcc」（他の受信者にアドレスが見えない設定）に設定すべき宛先を「Cc」にしてしまうと、受信者全員に他の人のアドレスが見える状態で送信してしまいます。

添付ファイルを間違える

本来送るべきファイルとは別のファイルを添付し、場合によっては重要な情報が入ったファイルを第三者に送信してしまうことがあります。ファイル名が似ていると特に起こりやすいです。

古い送信リストを使ってしまう

異動や退職等により、送信対象が変わっていても、リストの内容を確認せずにそのまま使ってしまうことで、不要な相手に送信してしまうことがあります。

メール誤送信への対策

メール送信時に誤送信をなくすためにはどうすればよいでしょうか？

１．送信前に宛先・添付ファイルを確認する

メールを送信する前には、To・Cc・Bccの宛先が正しいか、ファイルを添付する場合は名称や内容が正しいか（誤った内容や共有すべきでない情報が含まれていないか等）を必ず目視で確認しましょう。宛先については、特に同姓や類似のアドレスには注意が必要です。

２．メール送信作業手順を見直す

メールを送信する際には、上長や同僚といった第三者にダブルチェックしてもらったうえで送信する等の手順を取ることが望ましいです。（また、万が一誤送信が発生した場合の早期発見につなげるためにも、CcやBccに上長等を入れて、確認の目を増やしましょう。）

メール誤送信への対策

メール送信時に誤送信をなくすためにはどうすればよいでしょうか？

３．ファイル共有サービスやクラウドストレージを利用する

個人情報を含むファイルをパスワードをかけずにメールに添付して送ると、情報漏えいのリスクが高まり危険です。可能な限り、OneDrive等の「クラウドストレージ」や、ギガファイル便等の「ファイル共有サービス」を利用し、安全に情報を共有しましょう。

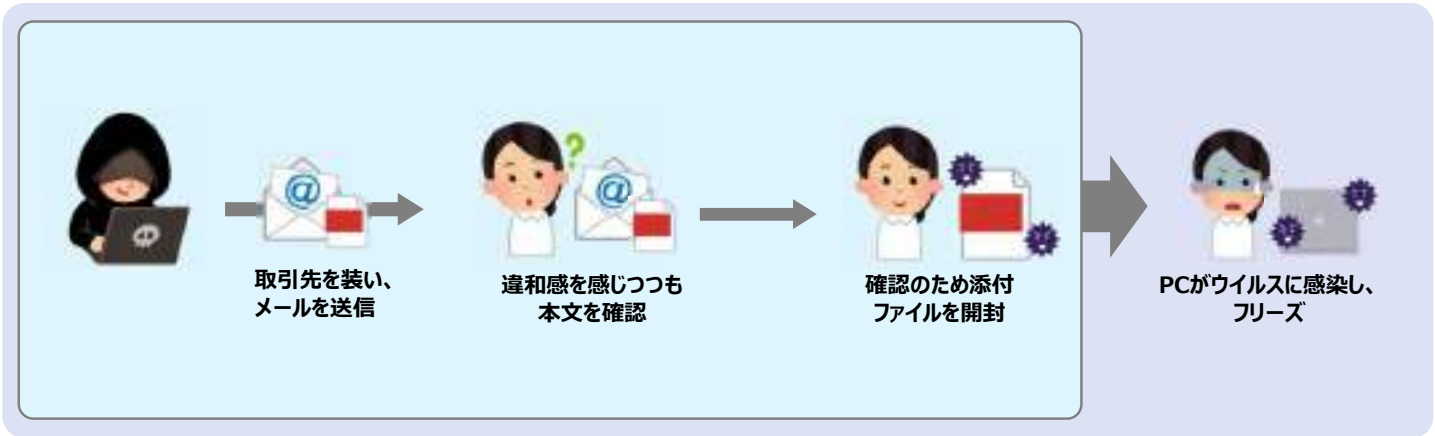
４．メールの機能を利用する

メールの送信予約機能や遅延設定が利用できる場合、利用することで、メール送信後すぐには相手に届かないようにすることも有効です。（実際に相手にメールが届くまでに猶予があり、その間にミスに気づけば送信を取り消し、誤送信を防ぐことができます。）

不審メール

不審メールとは

不審メールとは、**一見普通のメールに見えても、内容や送信元に不自然な点があり、開封や操作により被害につながる可能性のあるメール**のことです。例えば、差出人を偽装していたり、添付ファイルや本文に記載したリンクにマルウェアや詐欺につながる仕掛けが施されている場合があります。



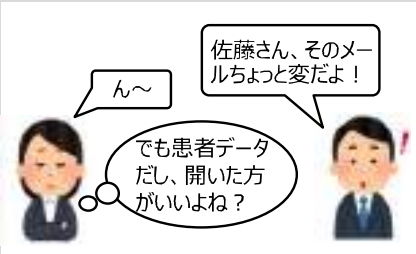
【シナリオ】不審メールの開封によるマルウェア感染

不審なメールの開封により、どのような被害を受けるのかを見てみましょう。

1.
事務職員の佐藤さんは、業務中に「患者データ確認のお願い」という見慣れないメールを受信しました。

2.
佐藤さんはメールの内容に違和感を覚えましたが、添付されているファイルを開こうとしました。

3.
近くにいた同僚の佐々木さんが、メールの不審な点に気づき、佐藤さんが開封しようとしているのを止めました。



4.
しかし佐藤さんはファイルを開いてしまい、PCがフリーズ。操作不能になってしまいました。

不審メールの主な種類

スパムメール

スパムは、不特定多数に大量に送られる広告や宣伝等のメールです。無害なものもありますが、情報収集への利用や詐欺サイトへの誘導、マルウェアが含まれることもあります。内容に心当たりがなく、関係ないリンクがある場合は開かず削除しましょう。

メッセージ例

【重要なお知らせ】あなたのアカウントが当選しました！今すぐ賞金を受け取るにはこちら👉

なりすましメール

なりすましメールは、不正サイトへの誘導や、個人情報を入力させることを目的に、知人や取引先等を装って送られてくるメールです。送信元の名前やアドレスが本物そっくりに見えるため、騙されやすいのが特徴です。不自然な文面や添付ファイル、急な依頼には注意が必要です。

メッセージ例

差出人：実際の同僚

お疲れ様です、至急お願いしたいことがあるので、対応可能でしたらこちらに返信してください。

不審メールの主な種類

フィッシングメール

フィッシングメールは、銀行や有名なサービスを装って、個人情報を盗もうとするメールです。「アカウントに問題があります」等、不安をあおる内容で偽のログインページに誘導します。正規のサイトかどうか、URLをよく確認しましょう。

メッセージ例

あなたのアカウントがロックされました。解除にはこちらからログインしてください。
ログインはこちら

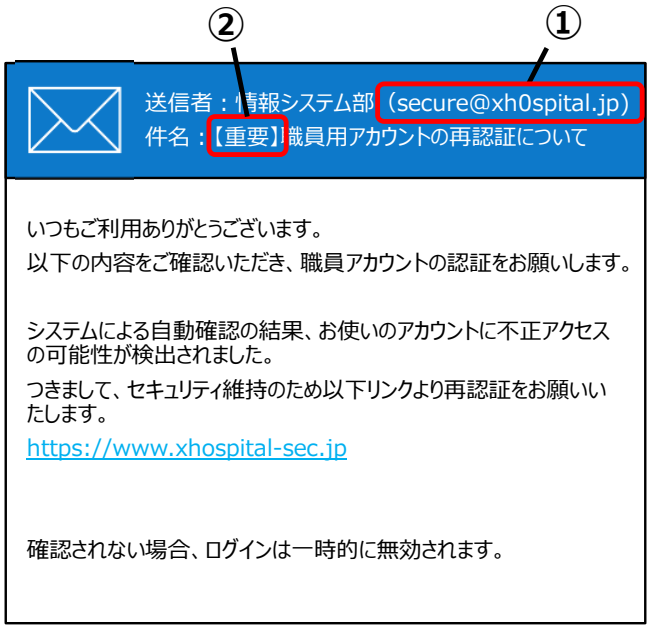
標的型攻撃メール

標的型攻撃メールは、特定の個人や企業を狙った巧妙なメールです。実在する相手や業務内容を調べたうえで送られてくるため、見た目では判断しづらい場合があります。添付ファイルやリンクのクリックでウイルスに感染する危険があります。

メッセージ例

経理担当者様
添付の請求書をご確認ください。至急ご対応お願いします。
(取引先の担当者名)

不審メールの見分け方（リンク型攻撃メール）



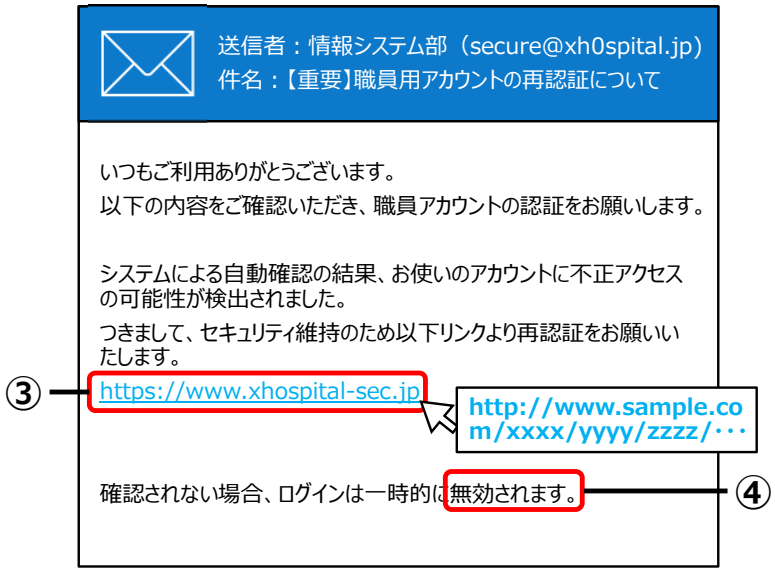
①送信者のメールアドレスがおかしい

メールアドレスをよく見ると、正規のアドレスと異なっています。
正：secure@xhospital.jp
誤：secure@xh0spital.jp
hospitalのo「オー」が0「ゼロ」になっています。

②件名に【重要】等の言葉が入っている

不審メールには、件名に【重要】や、【至急】のように、対応を急かす文言が入っている場合があります。これは受信者を焦らせるための手口のため、騙されず冷静に内容を確認することが大切です。

不審メールの見分け方（リンク型攻撃メール）



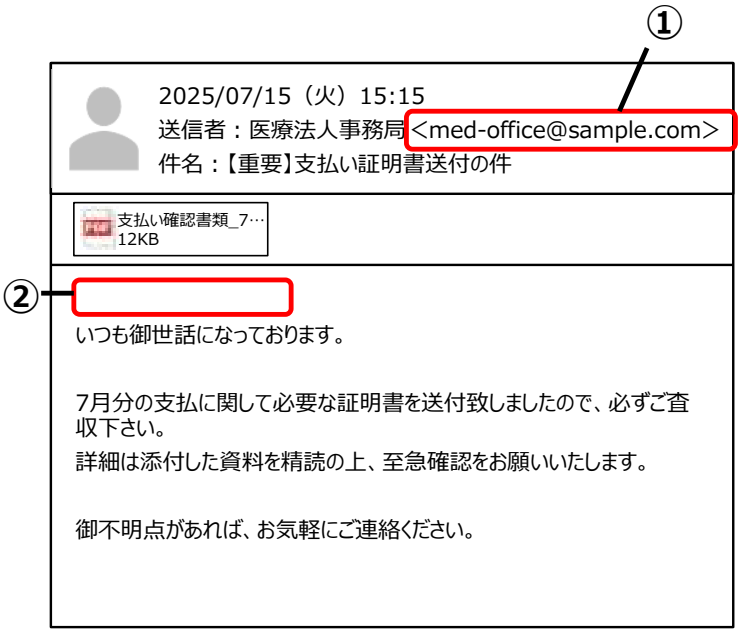
③リンクが正規のリンクではない

本文内のリンクを全文表示すると、正規のリンクとは異なるリンクが表示されています。一見本物に見えても記載するリンクは偽装できるため、カーソルをリンクに合わせて全文表示し、正しいかどうかを確認しましょう。（スマートフォンの場合は、リンクを長押しします。）

④文章が不自然

不審メールは、機械的に作成された文章により、誤字脱字や、言い回しに違和感がある場合があります。例えば、ここでは本来、「無効“に”されます」と表現されるべき文章が、「無効されます」というように誤字があります。

不審メールの見分け方（添付ファイル型攻撃メール）



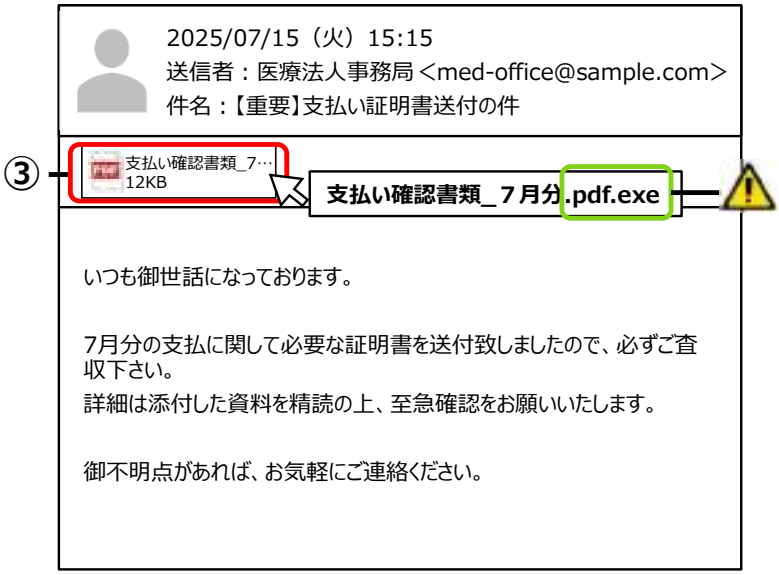
①フリーアドレスを使用している

送信者のメールアドレスが、例えばgmailやyahooといったフリーアドレスになっています。企業や医療機関等の正式な連絡でフリーメールが利用されることはほとんどないため、注意が必要です。

②宛名がない

本メールのように、宛名が記載されていないことは、不審メールの特徴の１つです。正式な連絡であれば、通常は「○○様」、「○○病院 御中」のように個別の宛名が記載されます。

不審メールの見分け方（添付ファイル型攻撃メール）



③拡張子がexeのファイルを添付している

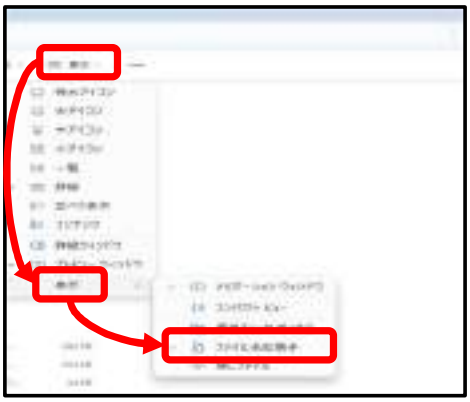
拡張子（ファイルの種類を示す末尾に付けられた文字列。「エクセル：xlsx」、「パワポ：pptx」等）が「exe」のファイルは、Windowsの実行ファイルで、開くとプログラムが動作します。exeファイルはマルウェアが仕込まれていることが多いため、開かないようにしましょう。（ファイル名がすべて見えない場合、カーソルをファイルに合わせると、全表示されます。）

一見拡張子が「pdf」に見えるよう、二重拡張子になっている場合もあります。一度該当ファイルをフォルダ上にコピーし、拡張子をしっかりと確認することを推奨します。（次ページ参照。）

【参考】拡張子の確認方法（Windows）

拡張子はフォルダ上で確認できますが、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ましょう。

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。

不審メールを開かないために注意すること

不審メールを誤って開封しないためにどのようなことに注意できるでしょうか？

1．送信元のメールアドレスをよく確認する

たとえ送信元の表示名が知っている名前でも安心せず、実際のメールアドレスが正しいかを必ず確認しましょう。例えば「病院名サポート」等の名前でも、よく見ると全く関係ないアドレスから送られていることがあります。送信元のメールアドレスは慎重に確認しましょう。

2．怪しいファイルやリンクは絶対に開かない

メールに添付されたファイルや、本文中に記載されたリンクを開くと、ウイルス感染や情報漏えいにつながるおそれがあります。「クリックしてください」や「添付ファイルをご確認ください」等と書かれていても、少しでも違和感を感じた場合は、安易に開かないようにしましょう。

不審メールを開かないために注意すること

不審メールを誤って開封しないためにどのようなことに注意できるでしょうか？

3．内容に心当たりがあるかを確認する

「支払いの催促」や「アカウントの凍結」等、焦らせるような内容で不安を煽るメールは、不審メールの典型例です。そのメールの内容が本当に自分に関係があるのか、送信者は普段からやりとりをしている相手なのかを冷静に確認しましょう。

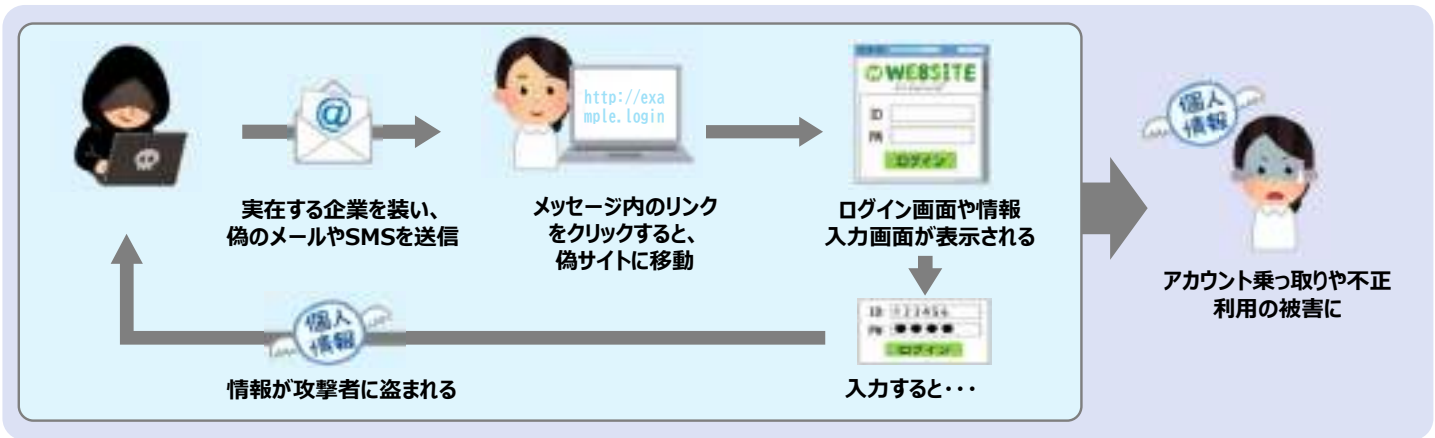
4．落ち着いて周囲の人に相談する

身に覚えのないメールや少しでも違和感のあるメールを見た際は、自分だけで判断せず、上長や情報システム部等、周囲の人に相談することが大切です。また、早めに共有することで、他の職員の被害を防ぐこともできるかもしれません。迷ったときは「相談してから」を基本にしましょう。

フィッシング詐欺

フィッシング詐欺とは

フィッシング詐欺とは、**送信者を詐称したメールやSMS（ショートメッセージ）を送信し、そこに記載されたリンクをクリックさせることで偽のウェブサイトに誘導し、IDやパスワードといったアカウント情報やクレジットカード番号を盗み出す詐欺**のことです。



【シナリオ】フィッシング詐欺による金銭被害

フィッシング詐欺により、どのような被害を受けるのかを見てみましょう。

1.
看護師の吉田さんは、休憩中に私用スマートフォンで「医療研修の受講料未払い」というメールを受け取りました。

2.
メールに記載されたリンクは、本物そっくりの支払いページで、吉田さんは迷わずクリックしました。

3.
吉田さんは、アクセスした支払いページでカード情報を入力し、受講料を無事に支払ったつもりでいました。

4.
しかし支払いページは偽物で、入力したカード情報を盗まれ、不正利用されてしまいました。

フィッシング詐欺による影響

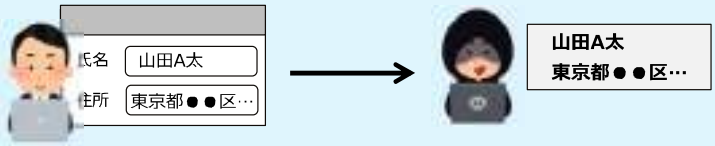
金銭的被害

個人情報の漏えい

アカウントの乗っ取り

もしも偽ウェブサイトにアクセスし、クレジットカード情報を入力してしまうと、カード情報を盗まれ、高額な買い物等、カードを不正利用される可能性があります。

もしも偽ウェブサイトで氏名や住所、電話番号といった個人情報を入力してしまうと、なりすましに利用されたり、別の詐欺の標的になる可能性があります。



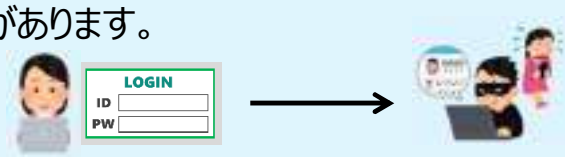
フィッシング詐欺による影響

金銭的被害

個人情報の漏えい

アカウントの乗っ取り

もしも偽ウェブサイトでLINEやメールアカウントのログイン情報を入力してしまうと、アカウントを乗っ取られ、勝手にメッセージを送られたり、知人が詐欺の被害に遭う可能性があります。



業務で利用しているメールやSNSアカウントが乗っ取られてしまった場合、**患者や職員に関する情報が漏えいする**可能性があるため、注意が必要です。

フィッシング詐欺の手口

フィッシング詐欺にはどのような手口があるのでしょうか？

メールフィッシング

銀行やクレジットカード会社、Amazon等の企業名を騙ったなりすましメールを用いた手口です。メールには、偽のウェブサイトへ誘導するリンクが添付されており、メールの内容は、「アカウントが永久停止します」や、「不正アクセスを検知しました」等、受信者の不安を煽るような内容のため、焦ってリンクをクリックしてしまう人もいます。

スミッシング

スミッシングとは、**SMS（ショートメッセージ）に偽サイトのリンクを記載して送信する手口**です。SMSは電話番号宛てにメッセージを送信するサービスのため、電話番号が漏えいしていなくても、ランダムに入力することで送信できてしまう可能性があります。また、SMSはメールよりも開封率が高いため、被害に遭う人が多い傾向にあります。

フィッシング詐欺の手口

フィッシング詐欺にはどのような手口があるのでしょうか？

ソーシャルメディアフィッシング

「Instagram」や「X」等のSNS上に偽サイトのリンクを投稿し、クリックさせることでIDやパスワードといったログイン情報を盗み出す手口です。SNSアカウントのログイン情報を窃取されてしまうと、アカウントが乗っ取られ、意図しない情報を発信されることでアカウントが凍結したり、友人にも攻撃を展開される等の可能性があるため、注意が必要です。

ボイスフィッシング（ビッシング）

音声通話を利用して個人情報や金融情報を聞き出す手口です。最近では、例えば実在する企業や金融機関の職員に成りすまして電話をかけ、「アカウントの更新が必要」等と伝え、メールアドレスを聞き出し、聞き出したメールアドレス宛にフィッシングサイトへ誘導するメールを送ることで、口座番号や暗証番号を盗み出し、不正アクセスや不正送金に悪用する巧妙な手口もあります。

フィッシング詐欺のメッセージ例

税金のお支払方法に問題があります。更新してください：https://www.exampleAbCdEf12345

【auからの重要なお知らせ】
ご利用金額が設定した金額を超えました。確認してください。https://www.sampleXXYYZZ

配達に伺いましたが、お受け取りいただけなかったため、荷物を持ち帰りました。詳細はこちらをご覧くださいhttp://t.co/dBwi●●●X

https://www.smbc-card.com/mem/service/phishing-mail_ex/index.jsp

フィッシング詐欺への対策

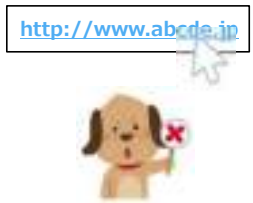
フィッシング詐欺の被害に遭わないためにはどうすればよいのでしょうか？

１．フィッシング詐欺に関する知識を身に付ける

被害に遭わないためには、フィッシング詐欺の手口や実際のメッセージの特徴等、まずはフィッシングについての基本的な知識を身に付けることが大切です。差出人は詐称できることを知っておきましょう。

２．リンクは安易にクリックしない

メールやSMS（ショートメッセージ）に記載するリンクは偽装できてしまいます。見た目だけでは偽物だと判断できないこともあるため、安易にクリックしないでください。どうしても該当のサイトにアクセスしたい場合は、公式サイトや公式アプリから接続するようにしましょう。



フィッシング詐欺への対策

フィッシング詐欺の被害に遭わないためにはどうすればよいのでしょうか？

３．むやみに情報を入力しない

最近は、本物に見えるよう作り込まれた偽サイトも多いため、普段から情報入力が必要な画面にアクセスする際には一度立ち止まり、入力して問題がないか、不審な点はないかを必ず確認するようにしましょう。

４．落ち着いて周囲の人に相談する

フィッシング詐欺のメッセージは、受信者を焦らせるような内容も多いです。焦って被害に遭わないためにも、落ち着いて家族や友人、上司等、周囲の人に相談するようにしましょう。

不審メールを開かないために注意すること

フィッシング詐欺の被害に遭わないためにはどうすればよいのでしょうか？

５．認証方法を強化する

パスワードを盗まれた場合に備え認証を強化しておくことで不正アクセスを防ぐことができます。ワンタイムパスワード（SMSや専用アプリに届く使い捨てのパスワード）等を利用し、セキュリティを高めましょう。(すべてのサイトで異なるパスワードを設定しておくことも重要です。)

６．セキュリティ対策ソフトを利用する

注意してもフィッシング詐欺を見分けることができない場合もあります。しかし、万が一偽サイトを開いてしまった場合でも、セキュリティ対策ソフトを利用することでブロックできる可能性があるため、可能な限り利用しましょう。

まとめ

まとめ（認証とパスワード管理）

- **認証は、本当に本人かどうか確かめる仕組み**
- **認証の必要性**
  - ✓ なりすましを防止するため
  - ✓ 責任の所在を明確にするため
  - ✓ 大切な情報・サービスを守るため
  - ✓ 安心してサービスを利用するため

- **弱いパスワードは簡単に解析され、不正ログインによる情報漏えい等の被害に**
- **弱いパスワード**
  - ✓ 連番・単純な数字や単語そのまま
  - ✓ 名前や生年月日
  - ✓ キーボードの配列、短いパスワード

- **安全なパスワードの条件**
  - ✓ 長さを確保する
  - ✓ 適度に複雑化する
  - ✓ 使い回しをしない
- **作成にはパスフレーズを活用**

- **パスワードだけではセキュリティが不十分のため、認証の強化が必要**
  - ✓ 多要素認証：異なる２つ以上の要素を用いて認証を行う方法で、セキュリティを高め、不正アクセスされるリスクを大幅に減らすことができます。

まとめ（メールセキュリティ）

- **メール誤送信による影響**
  - ✓ 信頼を損失する
  - ✓ 情報が回収できない
  - ✓ 更なる情報漏えいが起こる
  - ✓ メールアドレスを悪用される
- **メール誤送信への対策**
  - ✓ 送信前に宛先・添付ファイルが正しいかを確認する
  - ✓ メール送信作業の手順を見直す
  - ✓ ファイル共有サービスやクラウドストレージを利用する
  - ✓ メールの機能を利用する

- **不審メールの確認ポイント**
  - ✓ 送信元メールアドレス、件名
  - ✓ 文章の誤字脱字、言い回し
  - ✓ リンク、添付ファイルの拡張子
  - ✓ 宛名の有無　　等
- **不審メールへの対策**
  - ✓ 送信元のメールアドレスをよく確認する
  - ✓ 怪しいリンクやファイルは開かない
  - ✓ 内容に心当たりがあるか確認する
  - ✓ 落ち着いて周囲の人に相談する

- **フィッシング詐欺による影響**
  - ✓ 金銭的被害
  - ✓ 個人情報の漏えい
  - ✓ アカウントの乗っ取り
- **フィッシング詐欺への対策**
  - ✓ フィッシング詐欺に関する知識を身に付ける
  - ✓ リンクは安易にクリックしない
  - ✓ むやみに情報を入力しない
  - ✓ 落ち着いて周囲の人に相談する
  - ✓ 認証方法を強化する
  - ✓ セキュリティ対策ソフトを利用する