国事業「デジタル活用支援推進事業」標準教材を元に愛知県が編集

スマートフォンを安全に使うためのポイントを知りましょう

1

令和８年３月

本講座では、スマートフォンを安全に利用するために、安全なパスワードを作り、確実にパスワードを利用する方法と、
不安になった際にどこに相談したら良いのかなどを学習します。

なお、スマートフォンにはアンドロイドとiPhoneの２種類の端末がありますが、スマートフォンを安全に扱う上で内容に違いはありませんので、ご安心ください。

【補足説明】
講師の皆様は、この講座では、安全なパスワードの作り方や不安になったときの対処方法をお伝えしていますが、どのような方法もスマートフォンの安全性が100%保証されるものでないことはお伝えください。

また、パスワードの作り方や詐欺の種類等、講座に書かれている以上のことを聞かれた場合は、ご自身の知識で回答せず、適宜、

適切な相談窓口をご案内ください。

教材の中には、パスワードを作成する演習が含まれていますが、受講者の方の作成するパスワードはとても重要な情報ですので、絶対に見ないようにしてください。

また、他の受講者の方にも見られないようにご配慮ください。

目　次

第1章では、そもそもスマートフォンとは何か、スマートフォンの中にはどのようなデータが入っているのかを改めて確認します。

第2章では、パスワードにはどのような種類があり、どのように考えれば安全にスマートフォンを利用できるのか、学びます。

第3章では、スマートフォンに入っている大事なデータが奪われる、怪しげなメールや通知を使ったネット詐欺の事例や手口をご紹介します。

第4章では、万が一、ネット詐欺に引っかかったり、不安に駆られたりした場合の相談窓口等をご紹介します。

最後に、適切なパスワードの作成を演習形式で実施します。

目　次

第1章では、そもそもスマートフォンとは何か、スマートフォンの中にはどのようなデータが入っているのかを改めて確認します。

第2章では、パスワードにはどのような種類があり、どのように考えれば安全にスマートフォンを利用できるのか、学びます。

第3章では、スマートフォンに入っている大事なデータが奪われる、怪しげなメールや通知を使ったネット詐欺の事例や手口をご紹介します。

第4章では、万が一、ネット詐欺に引っかかったり、不安に駆られたりした場合の相談窓口等をご紹介します。

最後に、適切なパスワードの作成を演習形式で実施します。

1

スマートフォンは危険なもの?

4

基本的に、スマートフォンは利用者を保護するため、安全性を重視した作りになっています。

しかし、使い方によっては、詐欺などの危険にさらされてしまう一面も持っています。

なぜ、危険な一面があるのか、また、安全な利用方法を学ぶことがいかに重要なのかについて、スマートフォンの特徴から見ていきましょう。

【補足説明】
講師の皆様は、「スマートフォンは基本的な安全はもともと保たれているが、それだけでは不十分で、自分で使いながら、より安全性を高めていく、
パスワードなどの管理・活用法が求められている」ことを強調してください。

特に、この章は逆説的なタイトルになっているので、受講者の方が必要以上に不安を感じているようでしたら、丁寧にフォローしてください。

1-A　スマートフォンとは

スマートフォンとはパソコンのような機能を併せ持った携帯電話機の総称です。
従来の電話機よりも多機能かつ高機能なため「smart（賢い）」＋「phone（電話）」を合わせて「スマートフォン」と呼ばれています。従来の携帯電話とは異なり、アプリケーションと呼ばれるソフトを取り込むことでインターネット閲覧、ショッピング、読書、映画視聴等、様々な機能を追加し、利用者の好みに応じて機能を拡張することができます。

上記の他にも様々なアプリが存在します

5

スマートフォンとはパソコンのような機能を併せ持った携帯電話機の総称です。

従来の電話機よりも多機能かつ高機能なため「smart（賢い）」＋「phone（電話）」を合わせて「スマートフォン」と呼ばれています。

従来の携帯電話とは異なり、アプリケーションと呼ばれるソフトを取り込むことでインターネット閲覧、ショッピング、読書、
映画視聴等、様々な機能を追加し、利用者の好みに応じて機能を拡張することができます。

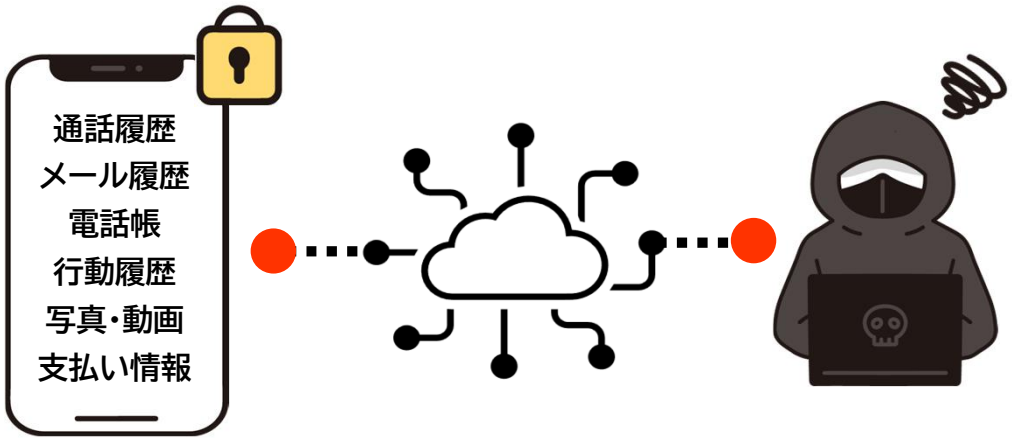
アプリには、様々な種類のものがあり、例として、他者と交流するコミュニケーション系のアプリ、映画やテレビ、ラジオ、音楽が楽しめる娯楽系のアプリ、
株価や天気予報などがわかる実利系のアプリ、交通機関用の電子マネーや決済に使えるお財布系のアプリ、カードゲームや将棋、
囲碁などを楽しめるゲーム系のアプリ、登山やジョギング、ショッピングなどの趣味のためのアプリまで、多種多様なものが揃っていま

す。

これらのアプリをスマートフォンに取り込み、使いこなすことでスマートフォンをより便利に使っていただけるようになりますが、
アプリの多くが、インターネットを通して利用する仕組みになっていることから利用時には注意が必要です。

1-B スマートフォンに入っている大量の情報

スマートフォンの中には大量の個人情報が格納されますので、適切な方法でインターネットを介した被害から身を守りましょう。



スマートフォンに保存された情報は適切に守ることが必要です。
正しく使うことができればスマートフォンは危険なものではありません。

6

なぜ、インターネットを介して利用するサービスには注意が必要なのでしょうか。

それは、スマートフォンの中には、通話やメールの履歴、電話帳、自分で撮影した写真や動画、
どこを訪れたかという位置情報や支払い履歴など、膨大な個人情報が詰まっているためです。

インターネットに接続されたスマートフォンから、これらの個人情報が漏れてしまうと、
プライバシーの侵害を受けたり、身に覚えのない請求を受けたりと、思いもよらない被害を受ける可能性があります。

これらの被害から自分自身を守り、スマートフォンを、安全かつ、便利な機能を併せ持つ、その名の通り「賢い電話」として
役立てるため、スマートフォンに保存される個人情報をしっかりと保護し、適切に守る必要があるのです。

2

パスワードを使った安全な管理をしましょう

7

スマートフォンに詰まった、膨大な個人情報を守るのが、パスワードの存在です。

ここでは、パスワードの重要性と、その作り方、使い方を学びましょう。

2-A　パスワードの重要性について

「パスワード」を適切に設定することでスマートフォンを利用したり、インターネット上の様々なサービスを利用する際、第三者の不正利用を防ぐことができます

上記以外にも様々な情報がパスワードによって守られています

8

スマートフォンを使いこなすほど、非常に多くの重要な情報が蓄積されていくことになります。

そのスマートフォン自体や、インターネット上の様々なサービスを利用する際に、第三者の不正利用を防ぐ役割を果たしているものが「パスワード」です。

例えば、銀行のキャッシュカードやクレジットカードの場合、4ケタの暗証番号を入力して使いますが、同じように、スマートフォンを起動する際や、スマートフォンに入っているアプリでさまざまなサービスを利用する時にも不正利用でないことを証明するためにパスワードが必要になります。

2-A　パスワードの重要性について

パスワードは自分の財産を守る「鍵」です

家や財産を守る鍵の役割＝パスワード

鍵（＝パスワード）を盗まれてしまうと、第三者が家（＝機器やサービス）に侵入し、情報を盗むことができてしまいます。パスワードは人の目に触れないところで保管し、大切に扱いましょう。

9

これらの重要な情報を守るパスワードは、自分の財産を守る「家の鍵」や「金庫の鍵」と同じものと言えます。

今後、スマートフォンがお財布代わりになる電子マネーが本格的に普及したり、その他便利なサービスが増えることで、まさにスマートフォンは「わが家の財産」が詰めこまれた状態になります。

その大切な鍵、すなわち、パスワードが盗まれてしまうと、他人が家（機器やスマートフォン）に侵入して、「財産」とも言える情報が勝手に盗み取られる可能性があります。

そのため、パスワードは外に漏れないように、しっかりと管理する必要があります。

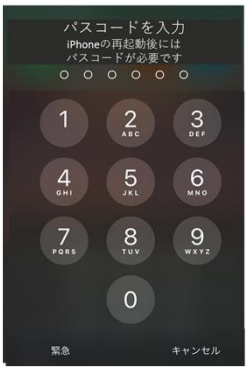
2-B　パスワードの種類

※機種によって機能が異なります

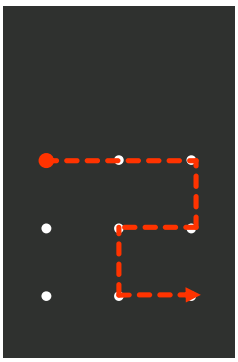
パスワードには様々な種類があります。

❶ 画面ロックのパスコード

暗証番号（数字）



パターン



※その他、指紋認証や顔認証なども利用できます。

10

次にパスワードの種類についてご説明します。

パスワードには様々な種類がありますが、もっともイメージしやすいのは、スマートフォンの画面ロックを解除する際のパスワード（パスコードともいいます）ではないでしょうか。

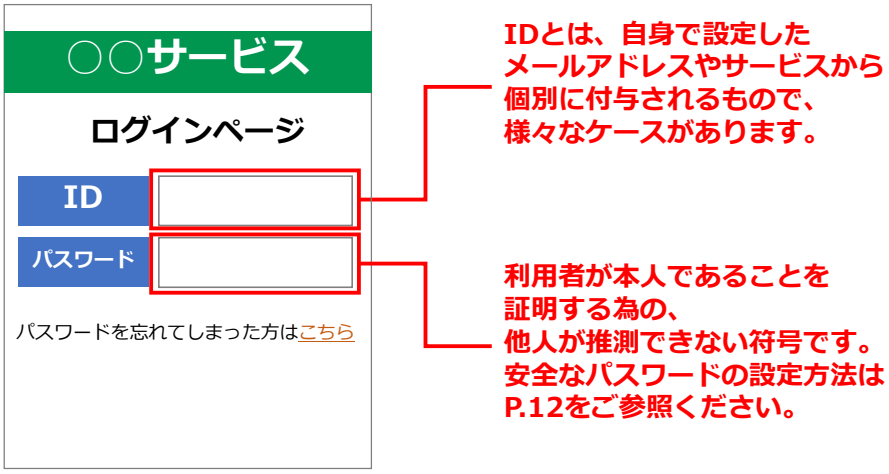
4ケタから6ケタの数字を設定して入力するものや、任意の図形パターンを指でなぞるタイプのものがあります。

最近では、パスワードを入力する代わりに、持ち主の顔や指紋を認証して、スマートフォンを起動させる機能を持ったスマートフォンも普及しています。

2-B　パスワードの種類

パスワードには様々な種類があります。

❷ アプリやサービス利用時のパスワード



11

もうひとつの種類は、IDとパスワードを入力するタイプのものです。

IDとは、利用者を識別するユーザー名のことで、名前に近いイメージと考えましょう。

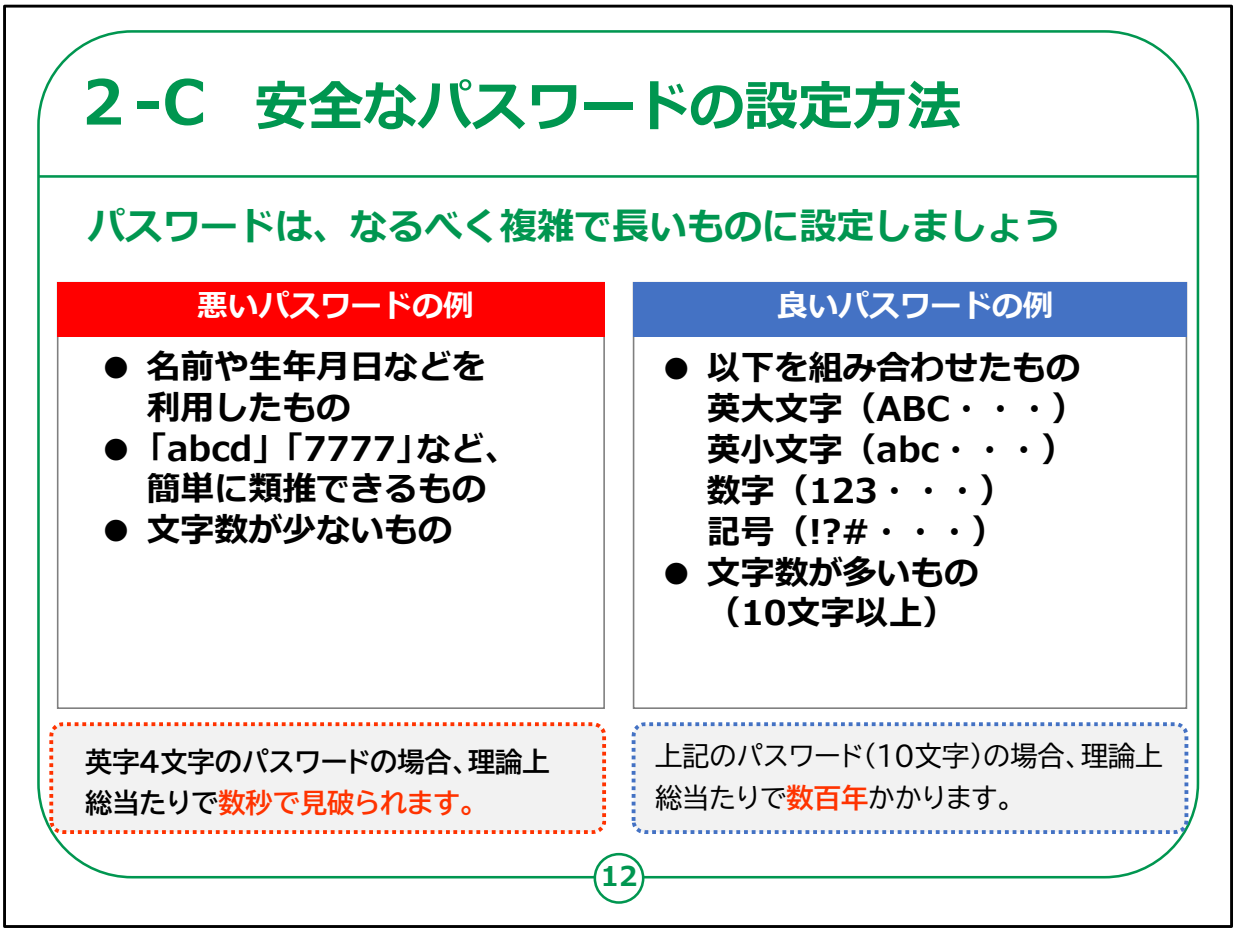
IDには、大きく分けて自分で設定できるケースや利用するサービスを提供する事業者から付与されるケースと、
自分のメールアドレスをIDの代わりにするケースがあります。

そのIDと合致する、パスワードを入れることで、本人確認がなされたことになり、サービスの利用が許可される仕組みです。

これらのパスワードがIDとセットで盗まれると、他人がご自身になりすまして、通販サイトで買い物をしたり、さまざまなサービスを自由に受けることが可能になってしまいます。

パスワードは、最初にご説明した通り「家の鍵」と同様に、とても大事なものです。

IDとともに、大切に保管しましょう。



ここからは、どのようにパスワードを作れば、より安全かをご説明します。

パスワードは他人から推測されにくく、より複雑なものが、安全です。

自分の名前や生年月日を利用したり、簡単に推測できる文字の羅列を使ったり、または入力するのが面倒だからと、少ない文字数でパスワードを作った場合、簡単に見破られてしまうリスクが高まるため、注意しましょう。

パスワードを見破る手段には「総当たり攻撃」といわれるものがあります。

これはすべての文字列の組み合わせを、次から次へとコンピュータで自動で試し、合致するパスワードを発見する手口です。

たとえば、英字4文字だけのパスワードは、この総当たり攻撃に遭うと、数秒で見破られるそうです。

ところが、英大文字、英小文字、数字、記号を組み合わせた、10文字のパスワードになると、理論上、解明するまでに数百年かかると言われています。

これなら、簡単に見破られることは無くなります。

安全なパスワードは、英大文字、英小文字、数字、記号を組み合わせた、10文字以上と、心がけてください。

【補足説明】
講師の皆様は、受講者の関心に応じて、パスワードを見破る攻撃の種類についても補足してください。

パスワードが漏れるケースは、「総当たり攻撃」以外に、WEBサービス会社などが保管している、IDやパスワードなどの個人データが流出して使われる「リスト型攻撃」などもあります。

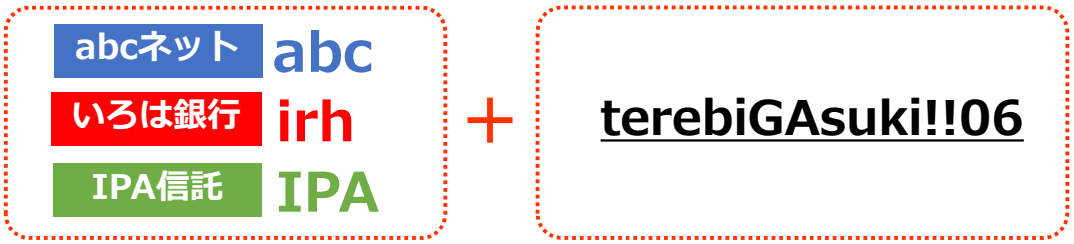
「リスト型攻撃」の場合、自分が使っているアプリなどで、情報流出が判明したら、速やかにパスワードを変更するなどの対策を取るよう、お伝えしてください。

2-C　安全なパスワードの設定方法

パスワードの使いまわしは絶対に避けましょう。

複数の機器やサービスで全く同じパスワードを使いまわしたり、似たようなパスワードを使っていないでしょうか。パスワードを使いまわしている場合、１つのサービスからパスワードが流出をきっかけに、同じパスワードを使用している他のサービス等にもログインされる恐れがあるためパスワードの使いまわしは避け、サービスごとのパスワードを必ず作るようにしてください。

パスワードを使いまわさないためのアイディア



独立行政法人情報処理推進機構『安心相談窓口だより』より抜粋

13

複雑なパスワードを作ったからといっても、同じものをいろいろなサービスで使いまわしては絶対にいけません。

これが、安全なパスワードを使うために重要なポイントです。

なぜなら、どこか1ヵ所でパスワードが流出したら、同じパスワードを使っている他のサービスにもログインされ、勝手に使われる可能性が高いからです。

とはいっても、毎回毎回、複雑なパスワードをランダムに考え出し、記憶しておくのも難しいことです。

そこで複雑な核となるコアパスワードをまず決めて、サービスごとに冒頭の文字を変えて管理する方法があります。

ここでは「て・れ・び・が・す・き」に、記号や数字を混ぜて各パスワードにしています。

このように、私的な自分の趣味や嗜好などをヒントに核となるパスワードを考えると、他人からは推測されにくいものにもなり、かつ、楽しくパスワードを作ることができます。

ここでは例として、利用するサービスの頭文字を、それぞれ核となるパスワードの冒頭につけています。これらの冒頭の文字を、末尾につけても構いません。

自分なりの法則性を決めて管理すれば、見破られる可能性は低くなり、より安全にパスワードを管理できるようになります。

【補足説明】
講師の皆様は、受講者の方から、定期的なパスワードの変更は必要かどうか質問された場合は、
利用するサービスによっては、パスワードを定期的に変更することを求められる場合がありますが、このコアパスワードのように
十分複雑なもので、複数のサービスで使いまわしをしていなければ、定期的な変更は必要ない旨をお伝えください。

ただし、そのアプリ運営会社などから情報が漏洩した場合などは、速やかにパスワードを変更する必要があることにもご留意ください。

2-C　安全なパスワードの設定方法

パスワードをノートやメモ等に書きとめて保管しましょう。

パスワードを書き留めたノートやメモ等は他の人に見られない場所で
大切に保管しましょう。なくさない限りにおいては最も安心な方法です。

abcネット
ID：～～～
パスワード：～～～～

いろは銀行
ID：～～～
パスワード：～～～～

・・・

P.39の「メモ」もご活用ください

14

利用するアプリが増えると、それぞれのIDやパスワードをどう管理するかも大きな問題です。

ノートやメモに、利用するアプリのIDやパスワード等を書き記して、保管しておくとよいでしょう。

このパスワードを管理するノートやメモは、スマートフォンとは一緒に持ち歩かないようにしましょう。

また、ノートやメモは他人から見られない場所で大切に保管するようにしてください。

最近のスマートフォンには、アプリごとにIDやパスワードを自動で記憶してくれる機能があります。

一度IDとパスワードを入力すると、次回からはスマートフォンが勝手に入力してくれて、自動的に認証を得る便利な機能です。

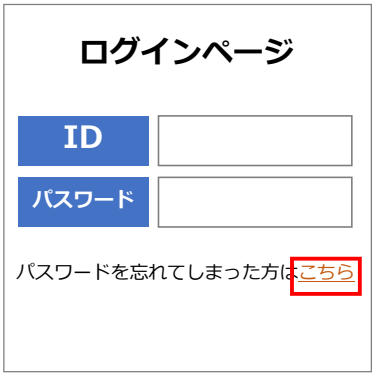
しかし、スマートフォンがインターネットと繋がっている限り、個人情報が流出する危険性が常にあります。

紙とペンで記録する方法はとても原始的な方法ですが、ネットから遮断されており、パスワードを管理するには一番確実な方法です。

2-D　パスワードを忘れた場合

パスワードを忘れた場合には、IDと登録メールアドレスがわかっていれば再設定ができます。

IDとメールアドレスが分かっていれば、パスワードを忘れても再設定できますので、パスワードを忘れないように使いまわすことはやめましょう。再設定をするためには、IDとメールアドレスが必要ですので、必ず控えておきましょう。



IDと登録メールアドレスが分かっていれば再設定できるので安心してください

15

パスワードを忘れてしまうことを懸念して同じパスワードを使いまわす方が多くなっていますが、IDとメールアドレスを忘れなければパスワードを忘れても再設定できますので、パスワードを忘れないように使いまわすことはやめましょう。

再設定をするためには、IDとメールアドレスが必要ですので、必ず控えておきましょう。

パスワードを忘れた場合は、利用するアプリやサービスのログインページに行きます。

通常、サービスのログインページには「パスワードを忘れてしまった方はこちら」のような記述がありますので、こちらをタップしてください。

新しくパスワードを設定する方法が案内されているページが表示されたり、登録しているメールアドレスにパスワードを再設定するページを案内するメールが送られてきたりします。

後者の場合は、メールからそのサイトに移動して、新たにパスワー

ドを設定すれば、ログインできるようになります。

その際は新しく設定したパスワードを必ずメモしましょう。

2-D　パスワードを忘れた場合

パスワードを自分で再設定することが難しい場合は、家族やいつも行く携帯ショップのスタッフ等、信頼できる人に相談してみましょう

ご家族・ご友人

携帯ショップ

※相談先ですべてのパスワードを再設定できるわけではありません

16

前のページでお伝えしたように、パスワードは自分で再設定することができます。

しかし、どうしても自分で再設定することが難しい場合は、信頼できる家族や友人、または携帯ショップのスタッフなどに相談してみましょう。

3

不審なメール・メッセージ・通知への対処

17

次に、IDやパスワードなど、私たちの大事なデータが奪われるリスクがある、不審なメールやメッセージの事例とその対策を見ていきましょう。

ネット詐欺にはいくつかのパターンがありますので、ここで学習する内容を知っているだけでも、かなりの確率で被害を防ぐことができるようになります

【補足説明】
講師の皆様は、ここで紹介する事例は、ネット詐欺の一部で、詐欺の種類や送られてくるメールもあくまで代表的なものであり、
他にも多くの種類がありますので、教材で挙げられている事例以外にも、少しでも不審に感じた場合は、
信頼できる人に相談するなり、第4章で紹介する専門の相談窓口へ連絡するなどの対策を取るように受講者へお伝えください。

3 -A　不審なメール･メッセージ･通知の事例

事例１： フィッシング詐欺

通販事業者等をかたる偽のメッセージに書かれているURLにアクセスすると、本物そっくりのサイトに誘導され、IDやパスワード等の重要な情報を抜き取られる手口です。

独立行政法人情報処理推進機構
『安心相談窓口だより』より抜粋

18

ネット詐欺で代表的なものが、「フィッシング詐欺」といわれるものです。ここ数年で急激に増えているネット詐欺の手口です。

これは、通販事業者等をかたる偽の事業者が一方的に送りつけたメールにURLが記載してあり、本物そっくりのサイトに誘導し、IDやパスワード、場合によってはクレジットカード番号や銀行の口座情報などを、魚釣り、すなわち、フィッシングのように釣り上げ、盗もうとするものです。

「フィッシング詐欺」でよくあるのが、教材で紹介しているような大手通販業者を装ったメールです。

これは「異常なログインが見つかり、配送先住所が変更されました」というおどすような文面で始まるメールで
「問題を解消するには、このURLをクリックしてください」と、偽のサイトに誘導し、IDとパスワードなどの個人情報を入力するように促

されるものです。

同じような手口で、宅配便業者を装って、不在通知のメールを送るものや、「あなたのカードが不正に使われた形跡があります」などと不安を煽るクレジットカード会社や銀行を装った詐欺メールも有名です。

偽のサイトやメールの作り方は年々巧妙になっており、一見しただけでは見破ることが難しいものも数多くあります。

もっとも効果的な対策は「心当たりのないメールでは、絶対にURLを開かないこと」です。

【補足説明】
講師の皆様は、受講者の関心に応じて、フィッシング詐欺における他のメールの事例も追加でお伝えください。

通販事業者や宅配事業者、クレジットカード会社、銀行の他にも郵便局やデパート、証券会社などと称したメールで、フィッシング詐欺を企む事例も見かけられます。

3 -A　不審なメール･メッセージ･通知の事例

事例２：偽のセキュリティ警告

スマートフォンでウェブサイトを閲覧中に突然『ウイルスを検出した』などの偽のセキュリティ警告が表示され、指示に従って操作を進めると、アプリのインストールへ誘導する手口です。

独立行政法人情報処理推進機構
『安心相談窓口だより』より抜粋

19

「偽のセキュリティ警告」も、よく見られる詐欺の１つです。

スマートフォンでウェブサイトを閲覧中に、突然、「重度のウイルスで破損しています」や、「個人情報が漏えいしています」といった偽のセキュリティ警告画面が出現します。

異様な警告音を伴う場合もあります。

例えば、「ウイルスを退治するための無料のアプリをインストールしてください」などと偽り、インストールすると、セキュリティソフト等の購入を迫られ、利用料金を請求され続けたりします。

困った人をサポートするフリをして、罠にはめる、悪質な詐欺行為です。

不安を感じた場合はそのままにせず、周りの方や携帯ショップの方へ相談するようにしましょう。

3 -A　不審なメール･メッセージ･通知の事例

事例３：アカウント乗っ取り

アカウントを乗っ取った犯人が、SNSの友人や公式アカウントになりすまし、メッセージを送りつけてくる手口です。リンクから偽のログインページに誘導され、ログイン情報を要求してきます。ログイン情報を入力すると、自分のアカウントが乗っ取られます。

※実在のアイコンや色使いを真似ているので、見た目だけで気付くことは難しいです

乗っ取り被害に遭わないために｜LINEみんなの使い方ガイド https://guide.line.me/ja/cyber-bousai/ より抜粋

20

「アカウント乗っ取り」では、SNSなどで実際の友達や公式アカウントを装ったメッセージが届くことがあります。

リンクからはログイン情報を入力させる偽サイトに誘導されます。

偽サイトは実在のアイコンや色使いを真似ているため、見た目だけで気付くことは難しいです。

偽サイトではログイン時に必要な情報の入力を求められ、自分のログイン情報を入力すると、相手にその情報が伝わり、自身のアカウントへ不正ログインされるなどの被害につながる可能性があります。

教材でご紹介しているケースはあくまで一例ですが、違和感を覚えたら、実際に友人に連絡を取ってみても良いでしょう。

3-B　SNS型ロマンス詐欺とは

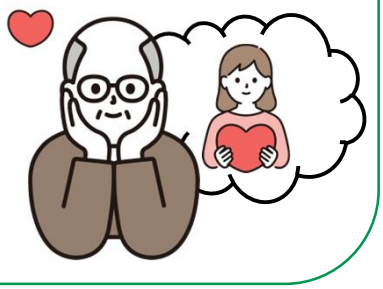
相手の好意や恋愛感情を利用した犯罪行為です

**SNSやマッチングアプリなどを通じて出会った面識の無い相手と
やりとりを続けるうちに恋愛感情や親近感を抱かせ、
金銭等をだまし取る詐欺です。**

実際に会ったことが無い相手から、「あなたと結婚するための資金が欲しい」といったような話が出たらすぐに詐欺を疑ってください。

SNS型ロマンス詐欺の特徴

その手口は様々ですが、魅力的な人物を装ってターゲットに近づき、相手の好意に付け込むという点ではどのパターンにも共通点があります。



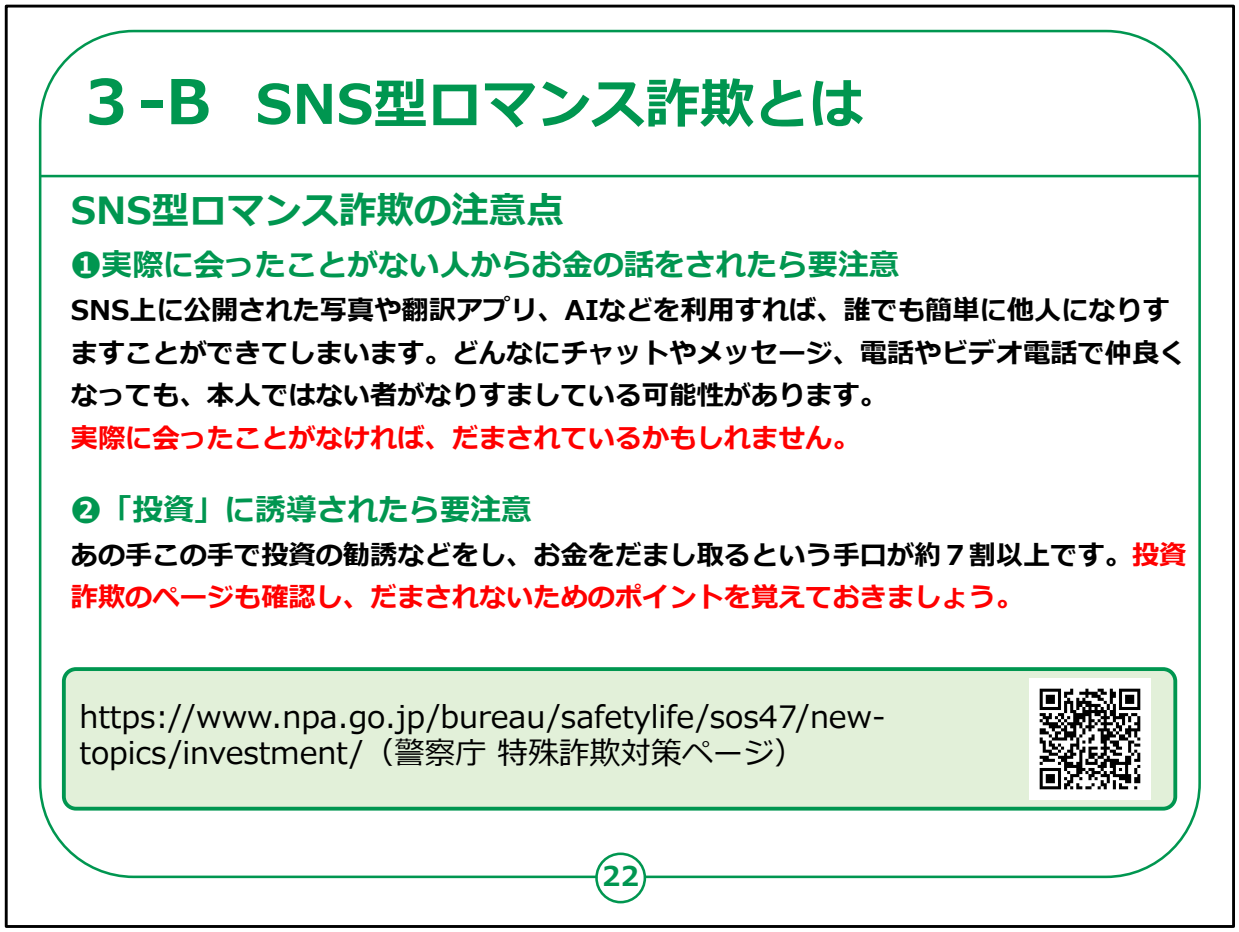
21

最初にSNS型ロマンス詐欺についてご説明します。

SNS型ロマンス詐欺は、SNSやマッチングアプリなどを通じて出会った面識の無い相手とやりとりを続けるうちに恋愛感情や親近感を抱かせ、
金銭等をだまし取る詐欺です。実際に会ったことが無い相手から「あなたと結婚するための資金が欲しい」といったような話が出たらすぐに詐欺を疑ってください。

SNS型ロマンス詐欺の手口は様々ですが、魅力的な人物を装ってターゲットに近づき、相手の好意に付け込むという点ではどのパターンにも共通点があります。

次のページからは実際の事例をもとに、SNS型ロマンス詐欺の手口と具体的な対策を学んでいきます。



SNS型ロマンス詐欺の注意点をご説明します。

それでは一つ目の注意点です。

実際に会ったことがない人からお金の話をされた場合、警戒するようにしましょう。

SNS上に公開された写真や翻訳アプリ、AIなどを利用すれば、誰でも簡単に他人になりすますことができ、本人の音声、動画を作ることができてしまいます。

どんなにチャットやメッセージ、電話やビデオ電話で仲良くなっても、本人ではない者がなりすましている可能性があります。

実際に会ったことがなければ、だまされているかもしれません。

二つ目の注意点です。

「投資」に誘導されたら要注意です。

２人の将来のために、などとあの手この手で投資の勧誘などをし、お金をだまし取るという手口が約７割以上です。

投資詐欺のページも確認し、だまされないためのポイントを覚えておきましょう。

3-C　SNS型ロマンス詐欺の具体事例

事例１：結婚を約束した相手にお金をだまし取られた

被害者：40代女性
被害額：合計約500万円

英国在住の韓国人と称する男とSNSで知り合い、一度も会わないまま結婚を約束。

「仕事で必要な金を立て替えてほしい」
「立て替えてくれないと契約違反で警察に捕まる」

などと連絡があり、女性は指定された口座に複数回入金してお金をだまし取られた。

恋愛感情や親近感を抱いていると、
相手を疑わずに振り込んでしまうことも。
会ったことのない人からお金の
振り込みを求める連絡には要注意。

出典：警察庁　特殊詐欺対策ページ

23

一つ目の事例です。

海外在住の韓国人と称する男性と結婚を約束し、その後、相手から仕事で必要なお金があり、立て替えてもらえないと刑務所に入るとの連絡があり、そのお金を振り込んでしまいだまし取られたというケースです。

恋愛感情や親近感を抱いていると相手を疑わずお金を振り込んでしまうことがあります。

実際に会ったことが無い相手から金銭の振り込み要求があった場合は応じずに警察に相談するなどし、対処しましょう。

3-C　SNS型ロマンス詐欺の具体事例

事例2：投資名目でお金を要求され、だまし取られた

被害者：40代男性
被害額：合計約300万円

SNSで友達申請された女性に恋愛感情を抱き、その者から投資を勧められた。

「2人の将来のために投資でお金を貯めよう」
「必ず儲かる」

などと連絡があり、男性は投資用アプリから口座に振り込みを行い、約300万円をだまし取られた。

SNS型ロマンス詐欺では、2人の将来のための資産形成などと言い、投資や副業を勧めてくる場合があります。
中には偽のアプリで収益が上がっているように見せかけてくることもあります。

出典：警察庁　特殊詐欺対策ページ

24

二つ目の事例です。

こちらの事例も一つ前の事例と共通点があり、「二人の将来のため」との言い分で投資を持ちかけられ、お金を振り込んでしまい、だまし取られています。

このケースは投資アプリも利用されており、ここまでご紹介した事例よりもさらに手が込んだ内容になっています。

詐欺犯はあの手この手で相手を騙そうと試みてきます。偽の投資アプリで利益が上がっているように見せかけるケースも発生しており、その手口は年々巧妙化しているため注意が必要です。

3-D　SNS型投資詐欺とは

著名人などの名前を利用して架空投資へ誘導

インターネット上に**著名人の名前・写真を悪用した嘘の投資広告を出し、「必ず儲かる投資方法を教えます」といったメッセージを送るなどして、**SNSに誘導し、投資に関するメッセージのやりとりを重ねて被害者を信用させ、最終的に「投資金」や「手数料」などという名目で、ネットバンキングなどの手段により金銭等を振り込ませる詐欺です。

SNS型投資詐欺の特徴

一度だまされると、**詐欺と気付くまで、お金を何度も振り込んでしまうことがあります。**少しでも怪しいと感じたらすぐに警察等へ相談しましょう。

25

SNS型投資詐欺はインターネット上に著名人の名前・写真を悪用した嘘の投資広告を出し、「必ず儲かる投資方法を教えます」といったメッセージを送るなどして、
SNSに誘導し、投資に関するメッセージのやりとりを重ねて被害者を信用させ、最終的に「投資金」や「手数料」などという名目で、ネットバンキングなどの手段により金銭等を振り込ませる詐欺です。

被害者は少額でも一度だまされると、詐欺と気付くまで、お金を何度も振り込んでしまうことがあります。少しでも怪しいと感じたらすぐに警察等へ相談しましょう。

3-D　SNS型投資詐欺とは

SNS型投資詐欺の注意点

❶紹介された投資先は実在していますか？

紹介された業者が金融商品取引業者等に登録されているかを確認しましょう。無登録での金融商品取引業や暗号資産交換業は違法です。

https://www.fsa.go.jp/ordinary/chuui/highrisk.html
（金融庁からのお願い・注意喚起HP）に載っていない業者は無登録業者です！

❷「必ず儲かる」「あなただけ」といった誘い文句はありませんか？

犯罪者は、こうした言葉を巧みに操ってあなたの心に付け込んできます。「必ず儲かる」「確実に利益が出る」といった儲け話や「あなただけ特別に教える」といった誘いは、まず疑いましょう。

26

SNS型投資詐欺の注意点をご説明します。

それでは一つ目の注意点です。
投資先を紹介された場合、その業者が金融商品取引業者等に登録されているか必ず確認しましょう。

業者が掲載されていない場合、その業者は無登録業者であり、違法な話を持ち掛けられているということになります。

こちらのスライドにホームページのアドレスとQRコードを掲載しておりますので、ぜひ活用してください。

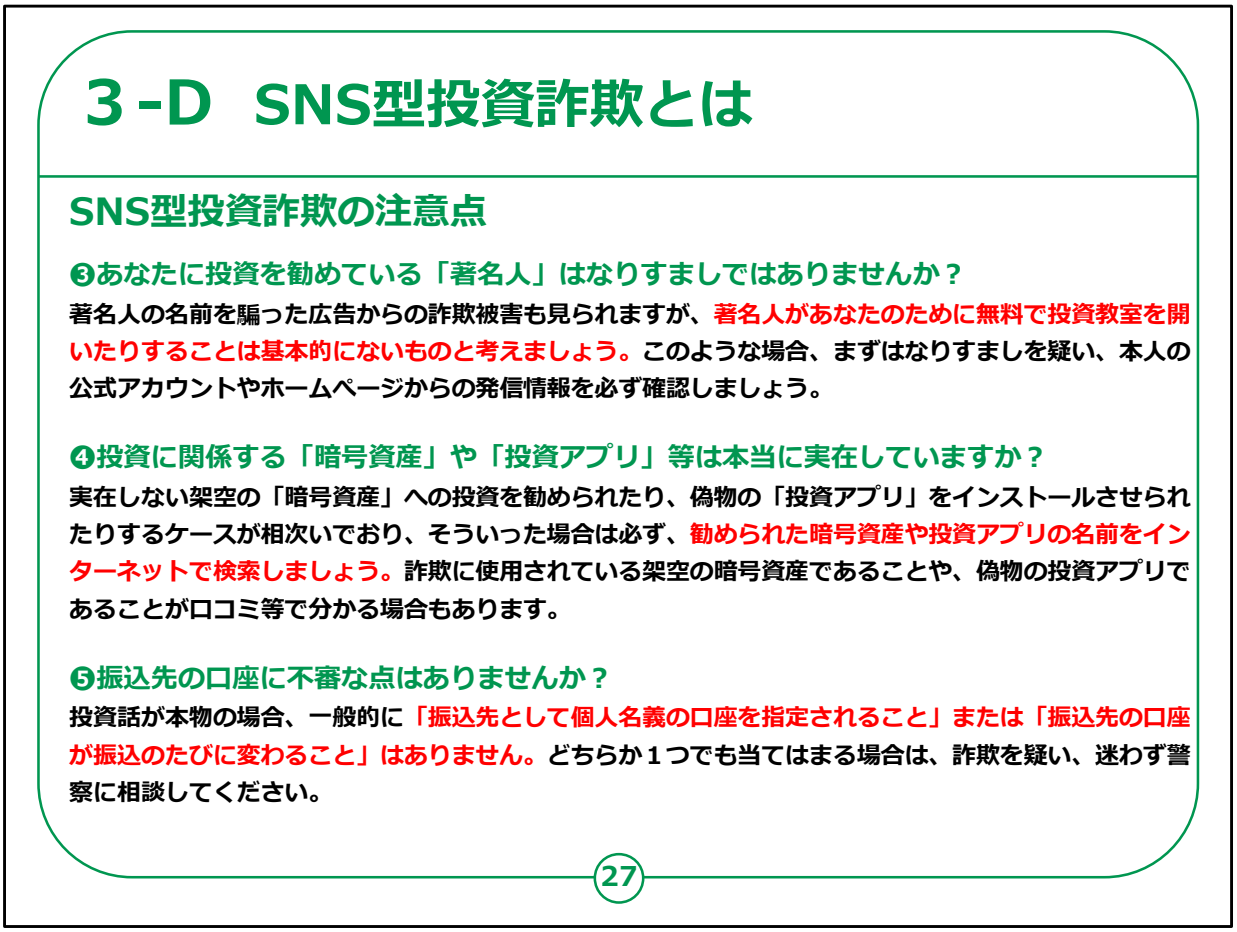
二つ目の注意点です。

「必ず儲かる」「あなただけ」といった誘い文句はなかったでしょうか。

犯罪者は、こうした言葉を巧みに操ってあなたの心に付け込んできます。

「必ず儲かる」「確実に利益が出る」といった儲け話や「あなただけ特別に教える」といった誘いは、まず詐欺を疑ってください。

そのような都合の良い儲け話が、あなただけに都合よく舞い込んでくることは無いと考えた方が良いでしょう。



三つ目の注意点です。

SNS型投資詐欺の特徴として、著名人の名前を騙った広告からの詐欺被害も見られますが、著名人があなたのために無料で投資教室を開いたりすることは基本的にないものと考えましょう。

このような場合、まずはなりすましを疑ってください。

それでもあきらめきれない場合は、本人の公式アカウントやホームページからの発信情報を必ず確認し、その情報が確かなものであるか必ず確認しましょう。

四つ目の注意点です。

実在しない架空の「暗号資産」への投資を勧められたり、偽物の「投資アプリ」をインストールさせられたりするケースが相次いでおり、そういった場合は必ず、勧められた暗号資産や投資アプリの名前をインターネットで検索しましょう。

詐欺に使用されている架空の暗号資産であることや、偽物の投資アプリであることが口コミ等で分かる場合もあります。

最後に5つ目の注意点です。

投資話が本物の場合、一般的に「振込先として個人名義の口座を指定されること」または「振込先の口座が振込のたびに変わること」はありません。

どちらか１つでも当てはまる場合は、詐欺を疑い、迷わず警察に相談してください。

もしSNSで投資を持ち掛けられた際はこの5つのポイントを思い出し、確認することで詐欺被害を回避しましょう。

次のページからは具体事例をご紹介していきます。

3-E　SNS型投資詐欺の具体事例

事例１：著名人になりすました相手とその仲間にだまし取られた

被害者：60代男性
被害額：合計約6,300万円

インターネット上で著名人が勧める広告からＳＮＳを通し著名人とそのアシスタントを自称する者と交流。

「金の投資価値が高まっています」
「必ず儲かります」

などと連絡があり、男性は投資専用サイトから指定された口座に入金。最終的に約6,300万円をだまし取られた。

著名人や投資家になりすました偽広告からSNS上でのやり取りに移行し、犯人は言葉巧みに信用を得てお金をだまし取ります。詐欺広告にはご注意ください。

出典：警察庁　特殊詐欺対策ページ

28

一つ目の事例です。

こちらはSNS広告経由で著名人を騙る相手とそのアシスタントを名乗る2人組に投資を持ち掛けられ、専用投資サイト上で運用利益が上昇しているように見せかけられ、高額をだまし取られた事例です。

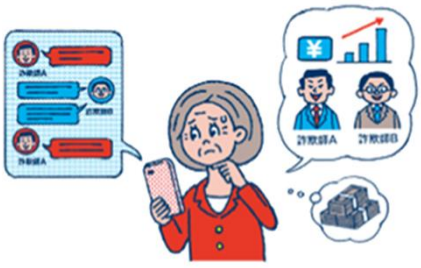
この後にもご紹介しますが、SNS型投資詐欺の事例には著名人になりすましたケースが多くなっています。

著名人を名乗る相手が現れた場合は詐欺だと認識した方が良いでしょう。

3-E　SNS型投資詐欺の具体事例

事例2：グループチャットでの偽情報を信用してしまった

被害者：60代女性
被害額：合計約2,000万円



動画配信サイトの新NISAに関する動画のURLからSNSグループチャットへの参加を招待。チャット内で投資や暗号資産の取引を誘われる。

「チャットの参加者はみな利益を得ています」

などと言われ、女性はチャット上で知り合った者から指定された口座への振り込みと暗号資産の送信により合計約2,000万円をだまし取られた。

犯人は投資用アプリやチャットから運用収益が上がっているように見せかけてきます。さらに収益を上げようと複数回振り込みを要求してくることもあります。

出典：警察庁　特殊詐欺対策ページ

29

二つ目の事例です。

こちらは新NISAに関する解説動画に記載されていたURLから詐欺グループのチャットに繋がってしまいチャットメンバーから「必ず儲かる」との甘い誘いを受け、相手が指定する口座へお金を振り込みだまし取られています。

相手はあらゆる手段で投資を魅力的に見せ、被害者からお金をだまし取ろうとします。

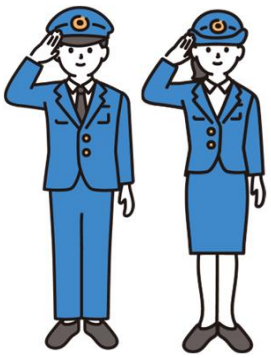
上手い投資話があっても簡単には乗らないように注意しましょう。

3 -F　SNS型詐欺のターゲットになり得る人は？

常に自分自身が被害者になり得ることを自覚する

警察庁によれば、令和6年1月から6月のわずか半年の間にSNS型ロマンス詐欺では1,498件、SNS型投資詐欺では3,570件もの被害が発生しており、いずれも50代以上の世代が60%超を占めています。

他人事ではなく、常に、自分自身が詐欺のターゲットとなり得ることを自覚し、十分に注意しながらSNSを利用しましょう。
また、詐欺の疑いがある場合は、迷わず警察に相談し詐欺被害の拡大を防ぎましょう。



出典：警察庁　特殊詐欺対策ページ

30

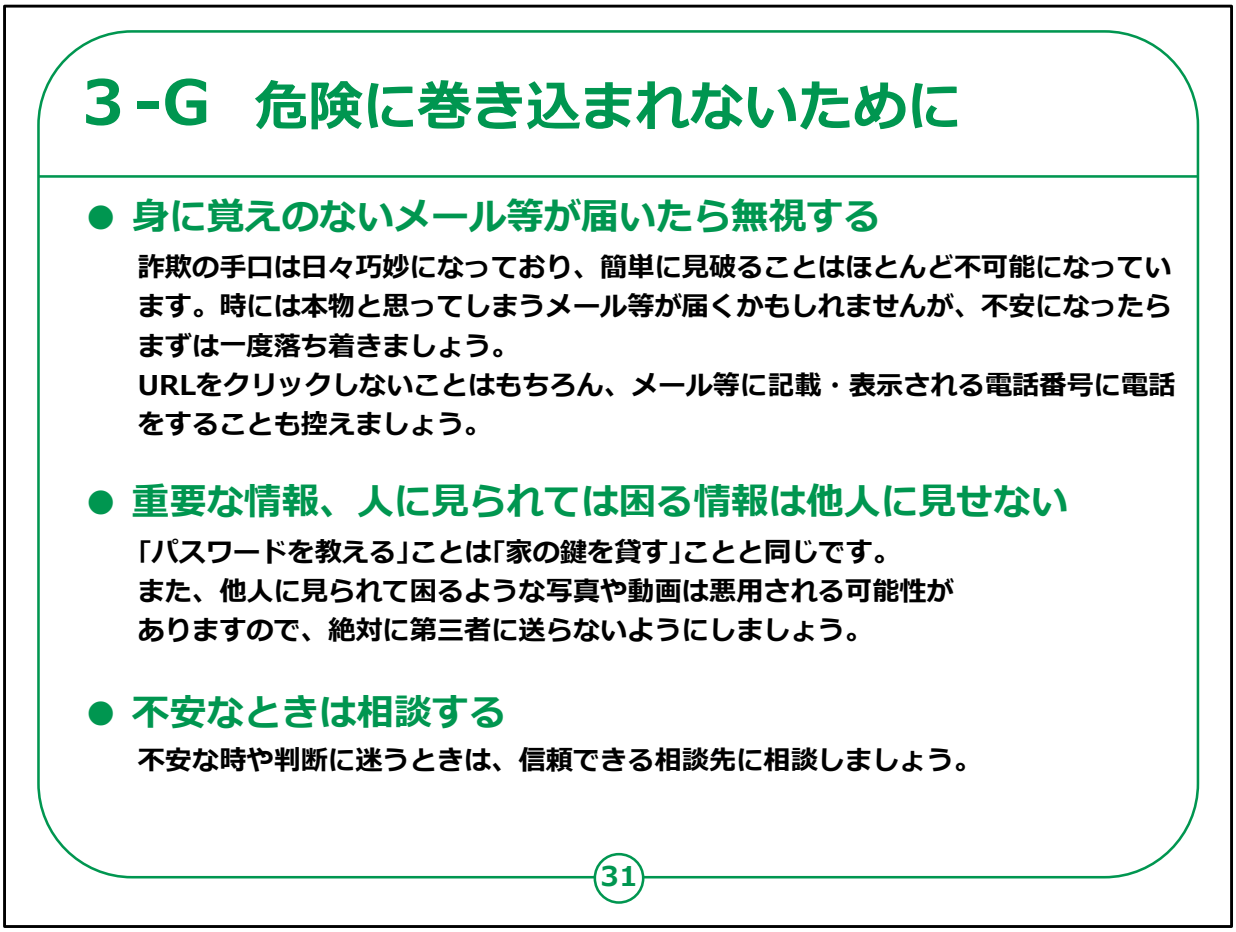
最後に、ここまでご紹介した事例に対して「自分がそんな被害にあうはずがない」と思われている方が大半だと思われますが、
警察庁によれば、令和6年1月から6月のわずか半年の間にSNS型ロマンス詐欺では1,498件、SNS型投資詐欺では3,570件もの被害が発生しています。

また、被害者の年代にも偏りがあり、いずれも50代以上の世代が60%超を占めています。

SNSを通じた詐欺が常に身近にあり、なおかつ自分自身が詐欺のターゲットとなり得ることを自覚し、十分に注意しながらSNSを利用しましょう。

また、詐欺の疑いがある場合は、迷わず警察に相談し詐欺被害

の拡大を防ぎましょう。



電話の「オレオレ詐欺」の手口が巧妙化したのと同様に、日々、ネットを使った詐欺も多様化、巧みに進化しています。

危険に巻き込まれないために、以下の3点を心掛けてください。

「身に覚えのないメールが届いたら無視する」

最近のメールでは、送信者名を詐称し、もっともらしい文面を装うだけでなく、接続先のサイトも本物とほとんど区別がつかないほど、そっくりに偽造するなど、簡単に見破ることはほとんど不可能になっています。

時には不安になってすぐに反応したくなることがあるかもしれませんが、不安になったときこそ、まずは落ち着くことを心がけましょう。

インターネットの詐欺に巻き込まれないための原則は、すべて無視することです。URLを開いたり、窓口に電話をして、真偽を確かめようなどとは、決してしないでください。

また「あなただけに給付金があります」といったような、うまい話の詐欺もよくありますが、これも欲を出さず、すべて無視してください。

つぎに「重要な情報、人に見られては困る情報は他人に見せない」ことを心がけてください。

パスワードは「家の鍵」のようなものであり、パスワードを他人に教えることは、「家の鍵を貸す」のと同じです。

決して他人には教えないでください。

また他人に見られて困るような写真や動画は、絶対に第三者に送らないようにしましょう。

最後に「不安なときは相談する」という選択肢を忘れないでください。

不安になったときや反応した方が良いメールなのか判断に迷う際は、一人で抱え込まずに、信頼できる相談先に相談しましょう。

デジタルリテラシーに関するご説明は以上です。

相談先については、第4章で詳しくお伝えします。

4

不安になったときの相談先

32

ネットを使った詐欺は、日々ますます巧妙化しています。

人の不安につけ込む巧みな手口で、困ったときにはひとりで抱え込まずに、周囲に相談するようにしてください。

この章では様々な相談先をご紹介します。

4-A　不安に感じることがあったら

怪しいメールを受け取ったり、不安なことがある場合は、家族やいつも行く携帯ショップのスタッフ等、信頼できる人に相談しましょう

ご家族・ご友人

携帯ショップ

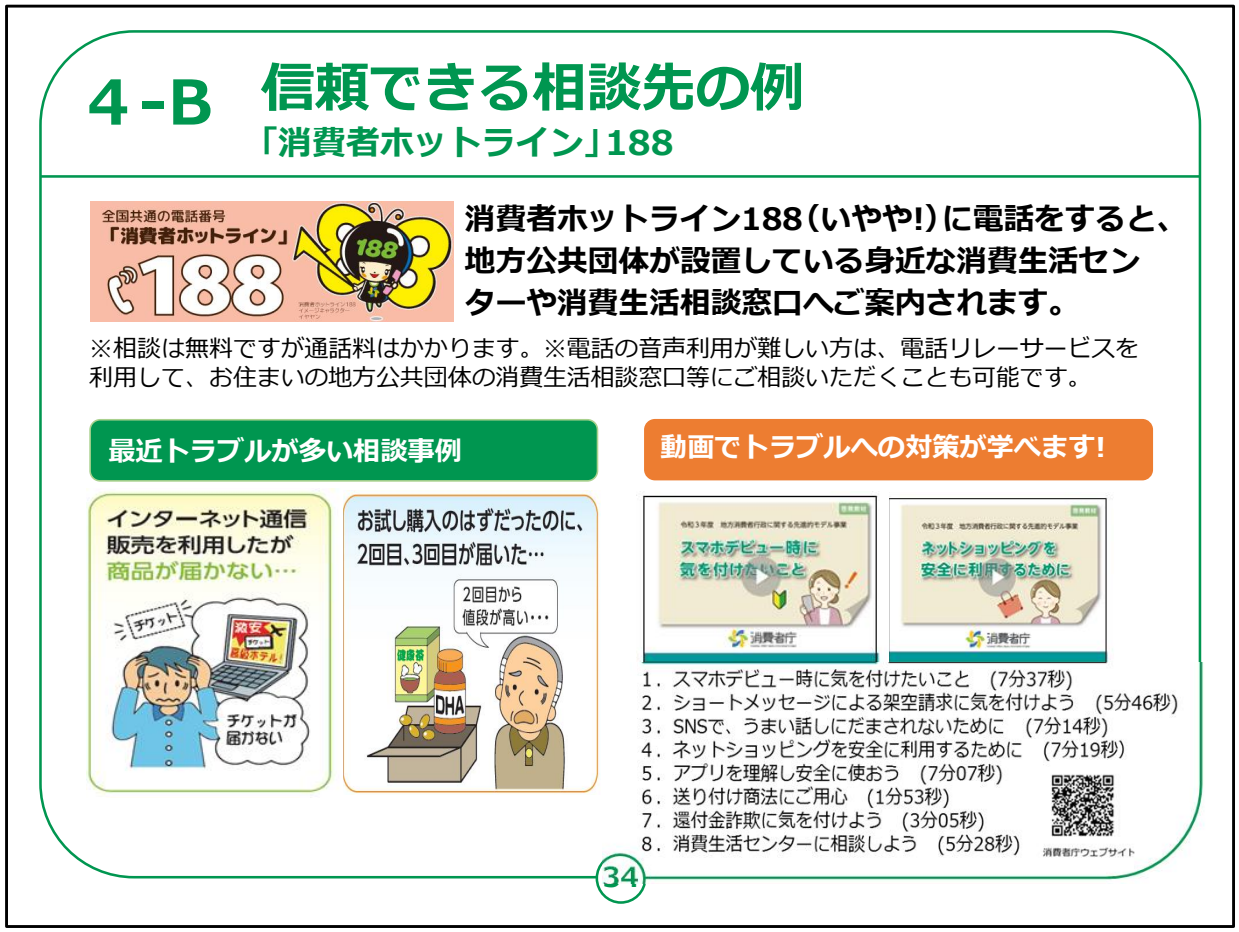
普段からインターネットの安全・安心な利用や、いざという時に誰に相談するのかについて周囲と話しあう機会を設けると良いでしょう。

33

スマートフォンを利用する中で、不安にかられたときは、1人で悩まず、まずは、家族や知人、携帯ショップのスタッフなど、信頼できる人に相談してみましょう。

また、第3章のような不審なメール等は、心の準備ができていないときに突然届きます。

慌ててしまわないように、普段から、インターネットの安全・安心な利用について学んだり、何か困ったことが起きた時には誰に相談するかについて、身近な人とも話し合っておくことが大事です。



信頼できる、公的な相談先も活用しましょう。

「消費者ホットライン188（いやや！）」に電話をすると、地方公共団体が設置している身近な消費生活センターや消費生活相談窓口へご案内されます。

局番なしの「188（いち・はち・はち）」という３ケタの電話番号で、年末年始を除いて原則毎日、ご利用いただけます。

電話の音声利用が難しい方は、手話・文字と音声を通訳する公共インフラサービスである「電話リレーサービス」を利用して、お住まいの地方公共団体の消費生活相談窓口等にご相談いただくことも可能です。

消費生活相談窓口では、「インターネットで注文したが、商品が届かない」「ネット通販でお試し購入のはずだったのに、2回目の商品が届いた」といった、最近多い通信販売や定期購入のトラブルなども相談できます。

また消費者庁では、「SNSでうまい話にだまされないために」など、
テーマごとにトラブル対策が学べる８本の動画も公開しています。

スマートフォンでも手軽に見ることができるので併せてご活用ください。

4 -B　信頼できる相談先の例

公的な相談先も活用しましょう。

情報セキュリティ安心相談窓口

IPA(独立行政法人情報処理推進機構)の運営する情報セキュリティに関する相談窓口です。電話かメールでご相談ください。

電話：03-5978-7509

受付時間 10:00～12:00｜13:30～17:00
※土日祝日・年末年始は除く

メール:anshin@ipa.go.jp
URL:https://www.ipa.go.jp/security/anshin/index.html

警察相談窓口

各都道府県警察本部のサイバー犯罪相談窓口、警察相談専用電話の「#9110」、又は、最寄の警察署にご相談ください。

都道府県警察本部のサイバー犯罪窓口一覧
https://www.npa.go.jp/bureau/cyber/soudan.html

35

経済産業省が所管する「情報処理推進機構」（IPA）にも、「情報セキュリティ安心相談窓口」があります。

電話とメールで相談を受け付けています。

また、必要に応じてURLもご参照ください。

また、警察にも相談窓口が用意されています。

警察相談専用電話「＃9110」か、各都道府県警察本部の「サイバー犯罪相談窓口」へご相談ください。

いずれも、教材にURLとQRコードを掲載しています。

4-C スマートフォンの安全な利用についての情報提供

各種ウェブサイトでスマートフォンの安全な利用についての情報提供を行っています。

①インターネットの安全・安心ハンドブック
https://security-portal.nisc.go.jp/guidance/handbook.html

②情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html

③安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html

④情報処理推進機構［IPA］X（旧：Twitter）
https://twitter.com/IPA_anshin

36

パソコンやスマートフォンで見られるウェブサイトでも、スマートフォンを安全に利用するための情報提供を行なっていますので、参考にしてください。

「内閣官房　内閣サイバーセキュリティセンター」の「インターネットの安全・安心ハンドブック」や前のページでご紹介した、情報処理推進機構（IPA）も多くの情報発信を行っています。

特に新しい詐欺の手口に関しては、いち早くレポートを発表しているので、必要に応じてお役立てください。

それぞれの情報提供元については、教材にURLとQRコードを掲載しています。

スマートフォンの安全な利用についての説明は以上です。

5

付　録
安全なパスワードの作成と保管

37

ここからは、参考付録となります。

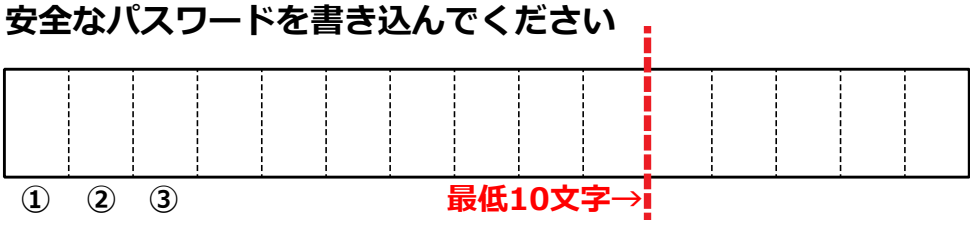
実際の演習はご自宅で行ってください。

【補足説明】
講師の皆様は、この付録部分は講座とは切り分けてください。

あくまでも個人情報を取り扱うことのないよう、十二分にお気をつけください。

演習　安全なパスワードを作ってみましょう

安全なパスワードを書き込んでください



チェック項目	チェック
既に使ったことのあるパスワードではありませんか?	☐
十分な長さになっていますか?（10文字以上）	☐
アルファベットの大文字・小文字・数字・記号が全て含まれていますか?	☐
お名前や生年月日等、容易に推測できる情報が含まれていませんか?	☐

上記が当てはまれば☑をいれてください。

38

【説明原稿】

ここでは、第2章で学んだルールを思い出して、安全なパスワードを教材に書き込んでみてください。

教材の中の四角い枠に一文字ずつ記入してください。

パスワードができ上がったら、チェック項目に従って、ご自身でチェックをしてみてください。

・既に使ったことのあるパスワードではありませんか？

もし、過去に別のサービス等で使ったパスワードを使いまわしている場合は、別のパスワードを考えてください。

・十分な長さになっていますか？

10文字以上のパスワードになっているかをご確認ください。

・アルファベットの大文字・小文字・数字・記号が全て含まれていますか？

「アルファベットの大文字はここ」「アルファベットの小文字はここ」とパスワードの近くに書き込むとわかりやすいでしょう。

・お名前や生年月日等、容易に推測できる情報が含まれていませんか？

あまりにもわかりやすいパスワードになっていないか、再度確認してみましょう。

全ての項目にチェックが入ったら、このパスワードは安全といえます。

記入を終えたシートは絶対に他人に見せないようにお気をつけください。

【講師向けコメント】
講師の皆様は、パスワードはとても大切な情報ですので、パスワードを考える際に相談に乗ったり、パスワードが安全かどうかを実際に見て確認したりしないでください。

教材のワークシートを覗き込むこともしないでください。

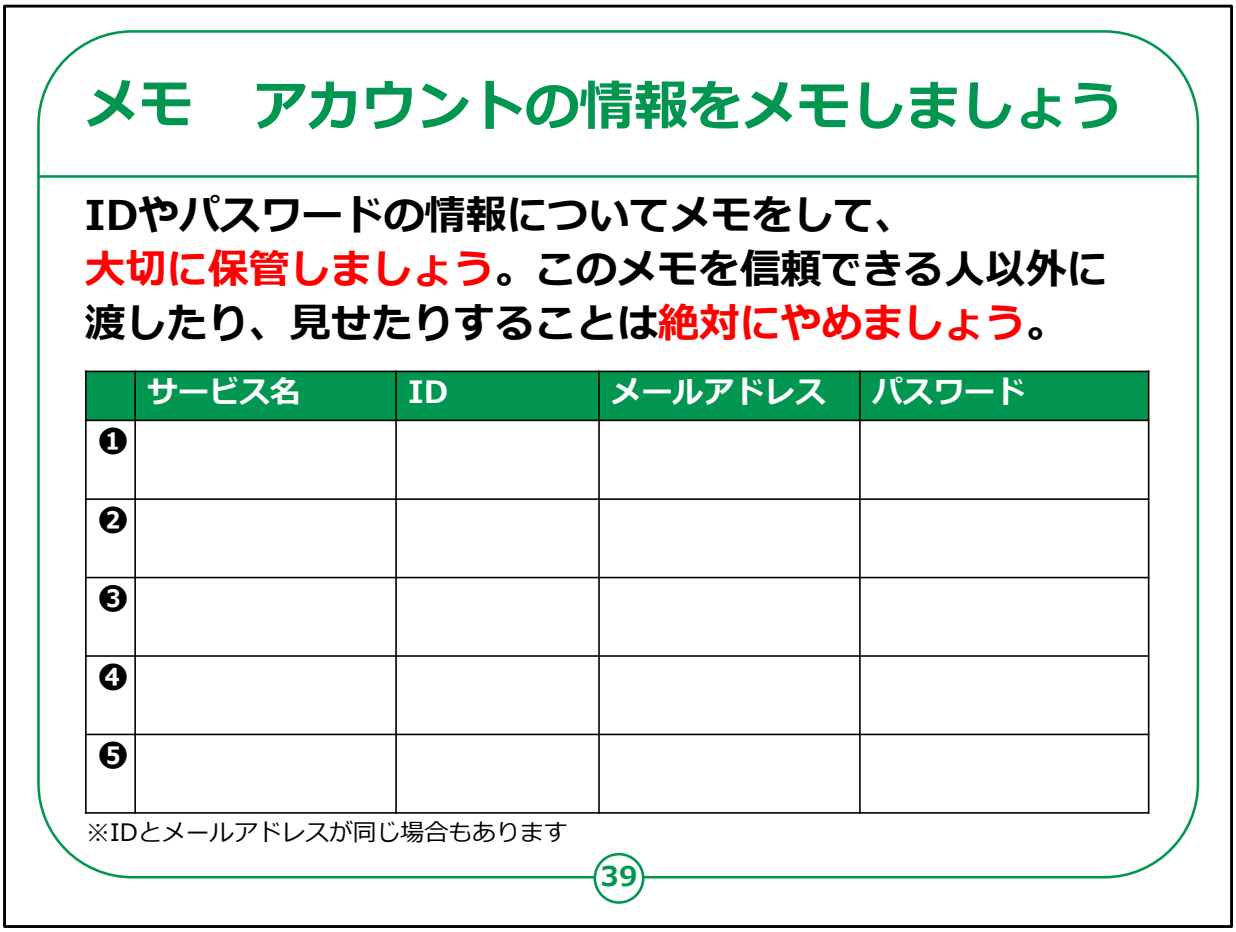
また、「チェック項目に当てはまるかどうか」、「パスワードが適切かを判断してほしい」などの確認をしないよう、またパスワードを他人に見せること自体に危険が伴うことをご説明ください。

なお、パスワードはとても大切な情報ですので、パスワードを考える際に相談に乗ったり、パスワードが安全かどうかを実際に見て確認したりしないでください。

教材のワークシートを覗き込むこともしないでください。

また、チェック項目に当てはまるかどうかの確認も、受講者自身が行うこととし、講師の皆様は、チェック項目を読み上げる等して、受講者自身で確認することを促すようにしてください。

「このパスワードが適切かを判断してほしい」と判断を求められても、パスワードを他人に見せること自体に危険が伴うことを受講者の方にご説明ください。



このページは、アカウントの情報を記録するためのメモです。

ご自宅で、ご自身が利用しているサービスの「サービス名」「ID」「登録しているメールアドレス」「パスワード」を書き出して、大切に保管しましょう。

サービスによっては「ID」と「登録しているメールアドレス」が同じ場合もあります。

また、ここに記載する情報は大切な情報ですので、このメモを信頼できる人以外に渡したり、見せたりすることは絶対にやめましょう。

【補足説明】

講師の皆様は、「メモ」の内容は自習用ですので、受講者の方が帰宅後にご自身で落ち着いて取り組むよう、お伝えください。