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5年９月

みなさん、こんにちは。

本講座では、スマートフォンを安全に使う方法を学んでいきたいと思います。

よろしくお願いします。

スマートフォンを安全に利用するために、この講座では、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についてお伝えします。

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。

講座の中には、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

2

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か?

3

基本的に、スマートフォンはとても安全にできています。

しかし、使い方によっては、詐欺を誘発する危ないツールになるのも、スマートフォンです。

なぜ、危険なツールになるのか、安全に利用する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「smart（賢い）+phone（電話）」で賢い電話を指します。

**電話やメールだけでなく、アプリケーションを入れることで、
インターネットや写真、買い物や読書等、様々な機能を追加することができます。**

4

「スマートフォン」を日本語に訳すと、「賢い電話」という意味になります。

以前の携帯電話は、主に通話やメールの機能が中心でした。

しかし、スマートフォンでは、最初から搭載されている基本機能に加え、アプリケーションと呼ばれる様々な働きをする機能を追加することで、自分好みの電話を作ることができます。

アプリには、たとえば、他者と交流するコミュニケーション系のアプリから、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、交通系のカードや電子マネーなどが使えるお財布系のアプリ、テレビゲーム・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。

これらのアプリのほとんどが、インターネットを通して利用する仕組みになっています。

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情報が入っており、常にインターネットを介して外に出て行っている可能性があります。

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。

5

アプリを利用する際には、氏名や住所、年齢、メールアドレスなどを登録しなければ使えないものもたくさんあります。

有料のアプリになると、その上、クレジットカードや銀行の口座情報などの登録も必要になります。

これらに加えて、もともと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など、膨大な個人情報が詰まっています。

インターネットといつも繋がっている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、プライバシーが他人に知られてしまったり、お金がいつの間にか抜き取られてしまうなど、さまざまな被害を受ける可能性があります。

ですから、スマートフォンに保存された、これらの個人情報にはしっかりと鍵をかけ、適切に守らなければいけません。

それさえ怠らなければ、スマートフォンは、安全、かつ、便利な機能を併せ持つ、その名の通り「賢い電話」として役立つはずです。

2

パスワードを使った安全な管理をしましょう

6

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

スマートフォン等を利用する際やネットの様々なサービスを利用するときに、自分だけが利用でき、他人が利用できないようにする役割を果たしているのが「パスワード」です。

7

スマートフォンには非常に多くの重要な情報が保管されています。

スマートフォンを利用する際やネットの様々なサービスを利用するときに、自分だけが利用でき、他人が利用できないようにする役割を果たしているのが「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ケタの秘密のパスワードを入力して使います。

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、自分を証明する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

パスワードとは、いわば自分の財産を守る「家の鍵」や「金庫の鍵」です。

**大切な鍵（＝パスワード）を盗まれてしまうと、
他人が家（＝機器やサービス）に侵入する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する等、大切に扱いましょう。**

8

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」と同じです。

今後、スマートフォンがお財布代わりになる電子マネーの本格的な普及や、その他便利なサービスが増えてくると、まさにスマートフォンには「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、「わが家の財産」が勝手に盗み取られる可能性があります。

これからスマートフォンがさらに便利になれば、パスワードの重要性はますます高まります。

パスワードは外に漏れないように、今まで以上にしっかり管理する必要があります。

2-B　パスワードの種類

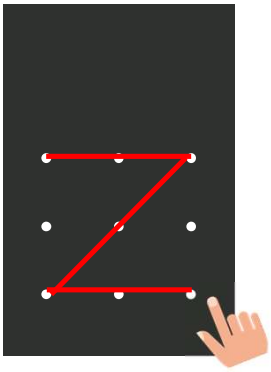
パスワードには様々な種類があります。

❶ 画面ロックのパスコード

※機種によって異なります。

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。

9

パスワードには様々な種類があります。

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。

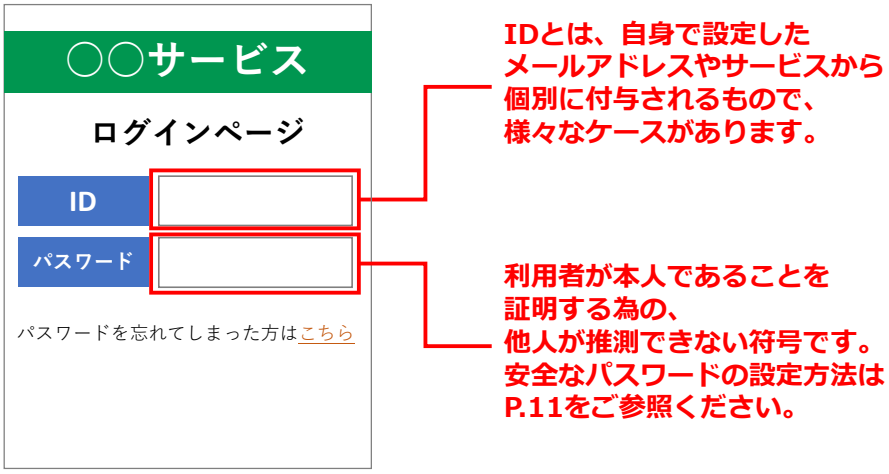
4ケタから6ケタの数字を設定して入力するものや、任意の図形パターンを指でなぞるタイプのものがあります。

これらのパスワードも、他人に知られれば、自分のスマートフォンを人に勝手に使われるきっかけになりますので、十分注意が必要です。

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タイプのものもあります。

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



10

もう1つのパスワードのタイプは、さまざまなアプリを利用する際に必要になるものです。

その際には、このような画面が出てきて、IDとパスワードを入力する必要があります。

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です。

IDには、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、自分のメールアドレスをIDの代わりにするケース等があります。

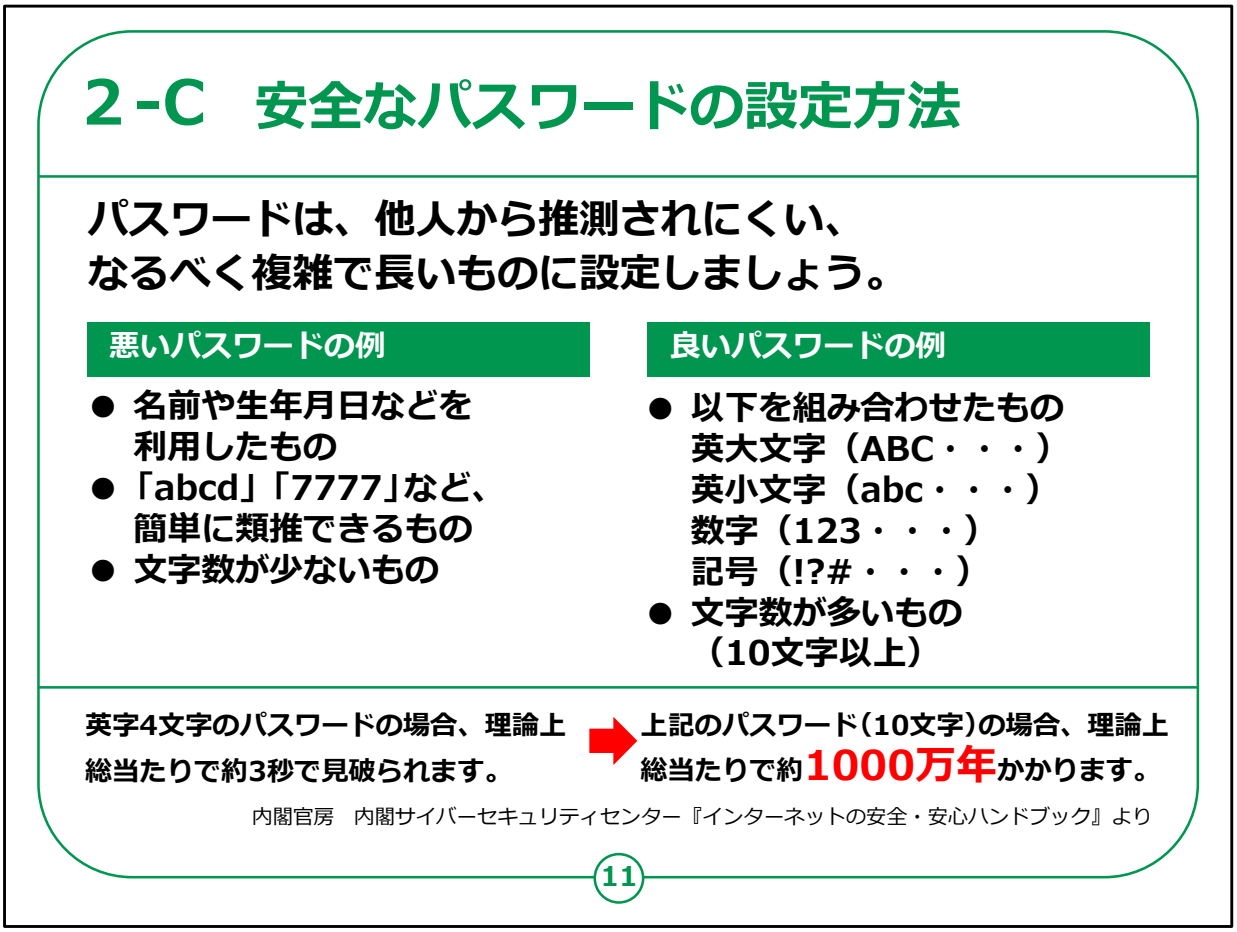
次にそのIDと合致する、パスワードを入れることで、本人確認がなされたことになり、サービスの提供が許可される仕組みです。

このように、インターネット上のサービスを利用する際に、IDとパスワードを使って本人を確認することを「ログイン」ということがあります。

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勝手に受けることが可能になります。

ネットワーク上の財産を守るパスワードは、「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、主にアプリやウェブサービスを利用する際に必要な家の鍵のようなパスワードをどのよう作れば、より安全かをご説明します。

第一に、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、安全なパスワードということになります。

間違っても、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らないようにしましょう。

パスワードを見破る手段に「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、たった３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1000万年以上かかると言われています。

これなら、ほぼ見破られないでしょう。

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。

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考え出すのも大変です。

そこで複雑な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コア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コア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って、かつ、楽しくパスワードを作れるのではないでしょうか。

そして、例えば、利用するサービスの頭文字を、それぞれコアパスワードの冒頭につけます。

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いです。

この講座の最後に、パスワードを作る演習の時間も設けていますので、楽しく考えてみてください。

【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.29の「メモ」もご活用ください

13

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**

14

万が一、パスワードを忘れた場合、IDと登録メールアドレスが判明していれば、パスワードを再設定することができます。

パスワードを忘れてしまったときのためにも、IDと登録メールアドレスは必ず記録しておくようにしましょう。

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。

たいてい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」のような内容が記載された場所がありますのでそこをタップします。

すると、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

15

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・通知を受け取ったときの対処

16

では、パスワードなど、私たちの大事なデータが奪われる、怪しげなメール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、これを知っているだけでも、かなりの確率で被害を避けることができると思います。

【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。

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

❶ 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。

IDやパスワードが盗まれます。

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

17

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、最後に問題を解消したいなら、「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」などとおどす、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。

これら心当たりのないメールでは、絶対にURLをタップしないようにしてください。

【補足説明】

講師の皆様は、受講者の関心に応じて、フィッシング詐欺における他のメール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

❷ 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。

利用料が請求され続ける
ことがあります。

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

「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。

3 -A　不審なメール･メッセージ･通知の事例

❸ アカウント乗っ取り

アカウントを乗っ取った犯人が、SNSの友人等になりすまし、動画を送りつけてくる手口です。動画を見ようとすると偽のログインページに誘導され、IDとパスワードを入力すると情報が抜き取られます。

IDやパスワードが盗まれます。また、さらに不審なサイトに誘導されることもあります。

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

「アカウント乗っ取り」では、Facebook（フェイスブック）のメッセンジャーのようなSNS（エスエヌエス）に、実際の友達から「このビデオはいつでしたか？」などと書いてある動画を装ったメッセージが届くことがあります。

動画を再生しようとメッセージをタップしても、動画は再生されず、IDとパスワードを入力させる偽サイトに誘導されます。

偽サイトには「動画を見るにはアカウント情報を確認する必要がある」というような内容が記載されています。

偽サイトに自分のIDとパスワードを入力すると、相手にその情報が伝わり、SNS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。

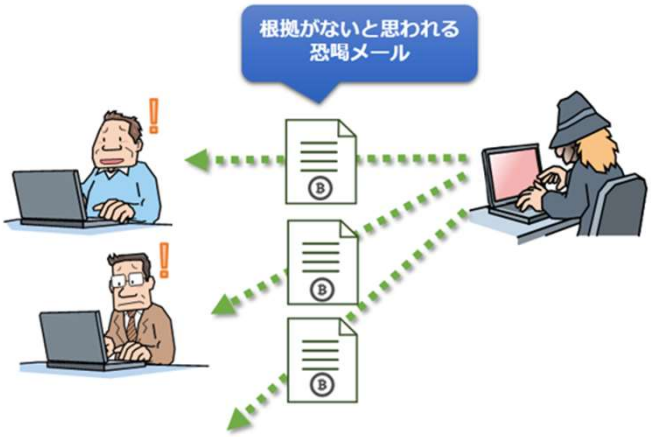
教材でご紹介しているケースはあくまで一例ですが、違和感を感じたら、実際に友人に連絡を取ってみても良いでしょう。

3 -A　不審なメール･メッセージ･通知の事例

❹ 偽セクストーション被害

「アダルトサイトを
閲覧しているあなたの姿を
パソコンについているカメラで
撮影した。家族や同僚に
ばらまかれたくなければ
仮想通貨で金銭を支払え」
といった根拠のない恐喝
メールを送りつける手口です。

**金銭を支払ってしまうと
取り戻すことができません。**



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

20

「偽セクストーション被害」とは、聞きなれない言葉かもしれませんが、このタイプの詐欺も最近増えています。

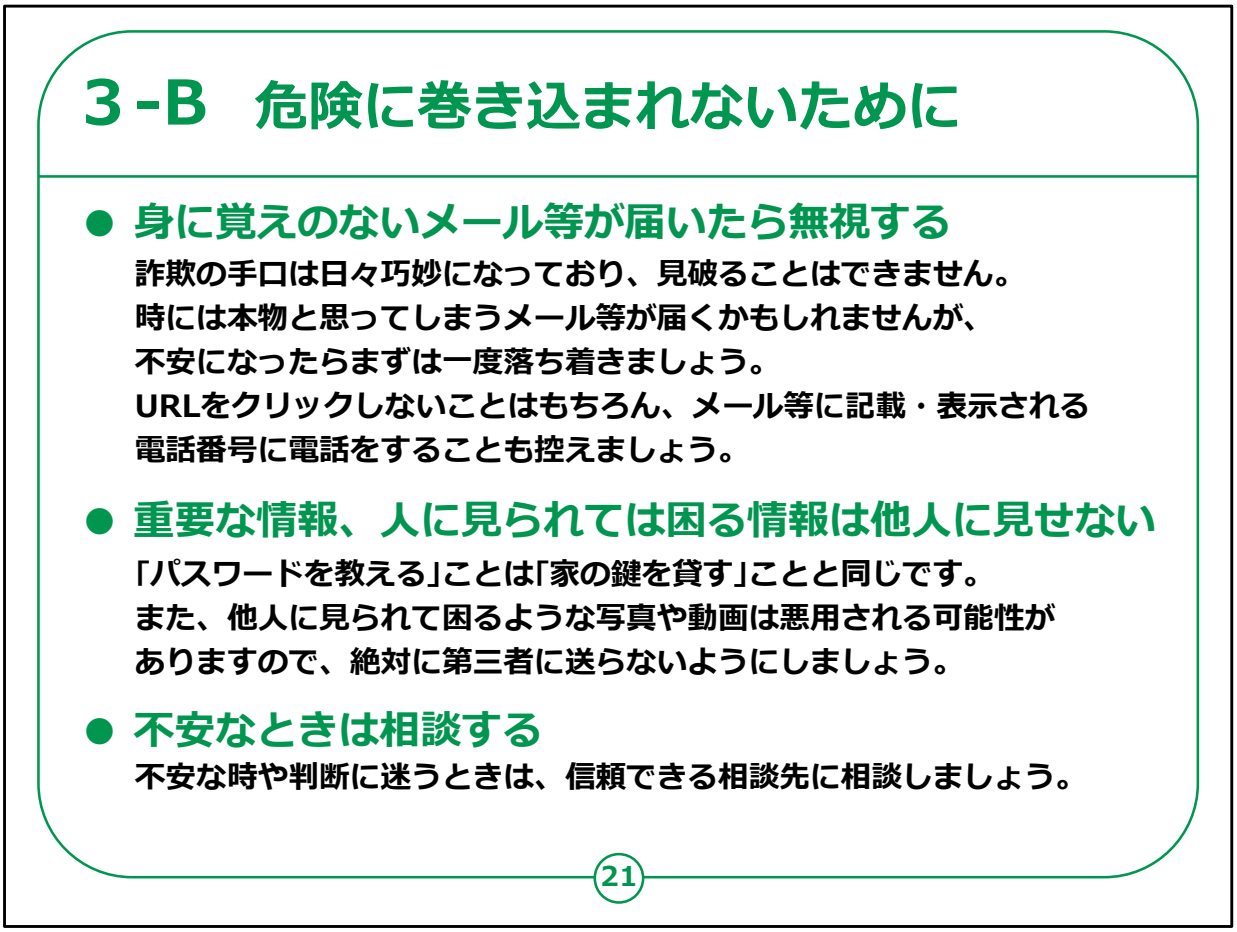
「セクストーション」とは、「sex＝性的な」と「extortion（エクストーション）＝脅迫」という英単語を組み合わせた造語です。

本来は、実際に個人のプライベートな動画や写真を交換するようにもちかけ、その後、それらをばらまくと脅迫する犯罪のことですが、実際にはそのような写真や画像は入手していないにもかかわらず、あたかも入手したかのように振る舞い、それらを家族や同僚等にばらまくなどと脅して、メールで金銭を要求する「偽セクストーション」の手口が増えています。

しかし、これはほとんどが相手を不安にさせるための攻撃者のでたらめです。

これらに類似したメールが来たら、それは偽セクストーションなのですべて無視してください。

何ら被害は発生しませんので、ご安心ください。



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。

１つ目は「身に覚えのないメールが届いたら無視する」です。

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、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をタップしたり、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「あた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。

２つ目は「重要な情報、人に見られては困る情報は他人に見せない」です。

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。

３つ目は「不安なときは相談する」です。

不安になったときや反応した方が良いメール等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。

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

22

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

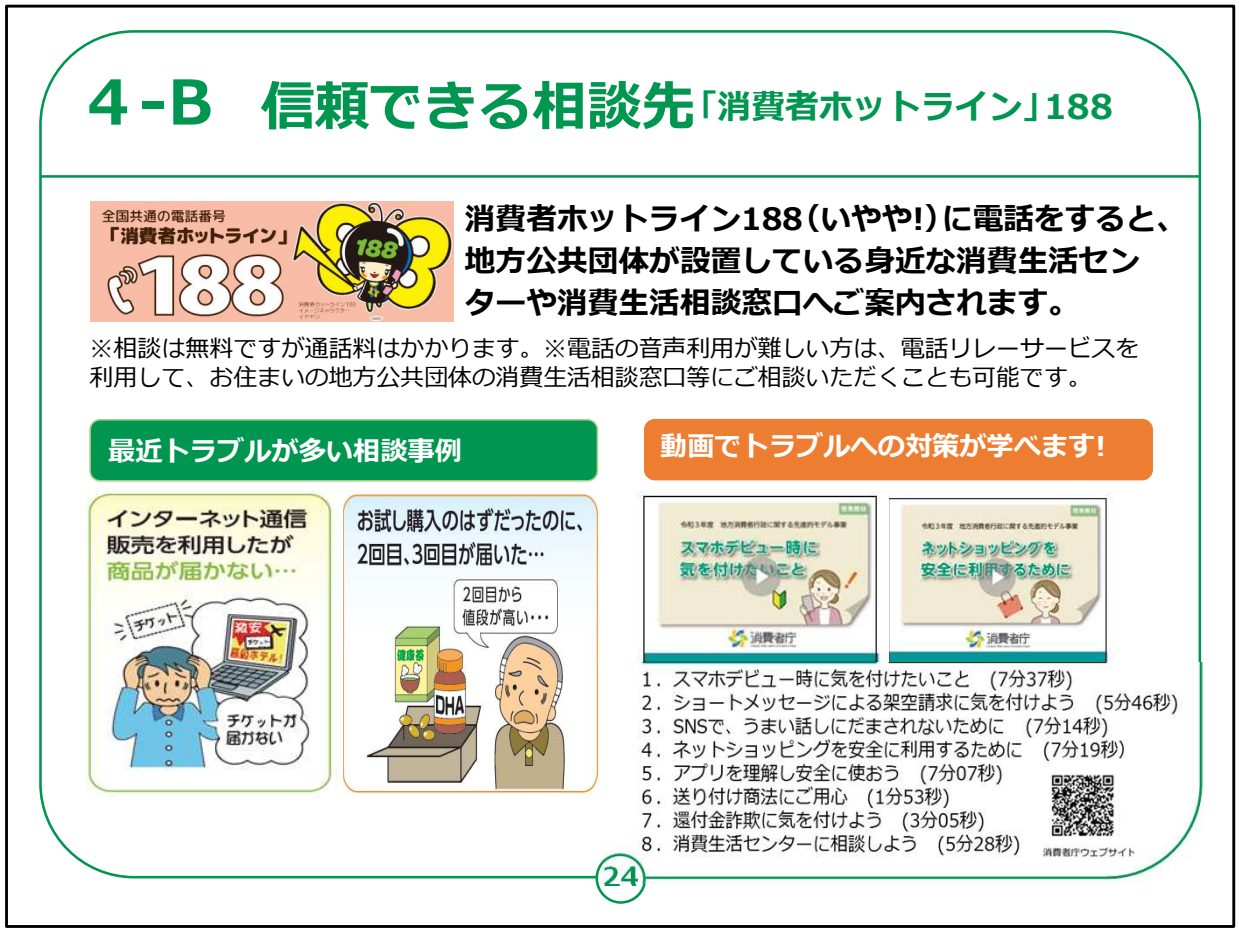
普段からインターネットの安全・安心な利用や、いざという時に
誰に相談するのかについて周囲と話しあう機会を設けると良いでしょう。

23

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

25

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情報処理推進機構［IPA］相談窓口
https://www.ipa.go.jp/security/anshin/index.html

③情報処理推進機構［IPA］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

26

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

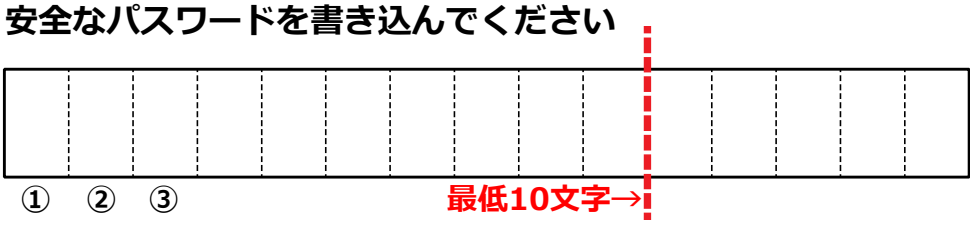
付　録
安全なパスワードの作成と保管

27

ここからは、演習を行います。

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。

28

ここでは、演習形式で、実際に安全なパスワードを作ってみます。

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。

パスワードが出来上がったら、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。

このワーク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。

【補足説明】

講師の皆様は、受講者の方がパスワードを考える時間を最低でも5分は確保できるようにしてください。

十分な時間を確保できるのであれば、講座の残り時間に応じて、少し長めに時間を設定しても構いません。

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。

メモ　アカウントの情報をメモしましょう

IDやパスワードの情報についてメモをして、
大切に保管しましょう。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。

	サービス名	ID	メールアドレス	パスワード
❶				
❷				
❸				
❹				
❺				

※IDとメールアドレスが同じ場合もあります

29

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。

用語集

用　語	意　味
アプリケーション	特定の用途や目的のために設計されたソフトウェア(機能)のこと。省略してアプリとも呼びます
アカウント	サービスを利用する際に必要な権利や個人認証情報のこと
ID	サービスの登録者や利用者を識別するために使用される文字列のこと
パスワード	サービスを利用する際に利用者本人であることを確認するための秘密の合言葉
ログイン	サービスを利用する際に、IDとパスワードを使って本人情報を確認する仕組みのこと
インストール	スマートフォン等のデジタル機器に、アプリケーション等のソフトウェアを取り込んで使えるようにすること