【講師原稿】

次にスマートフォンについて説明します。「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。

【講師原稿】

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。

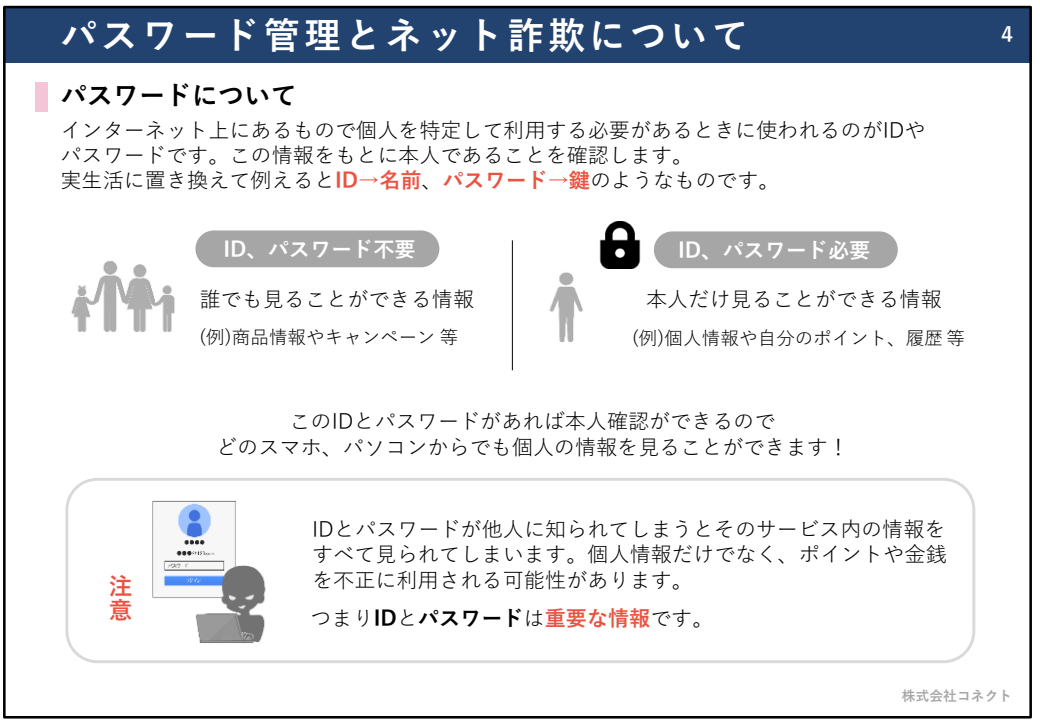
ですから、スマートフォンに保存された、これらの個人情報にはしっかりと鍵をかけ、適切に守らなければいけません。

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。

【講師原稿】
皆さんはパスワードって聞いたことありますか？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。

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。

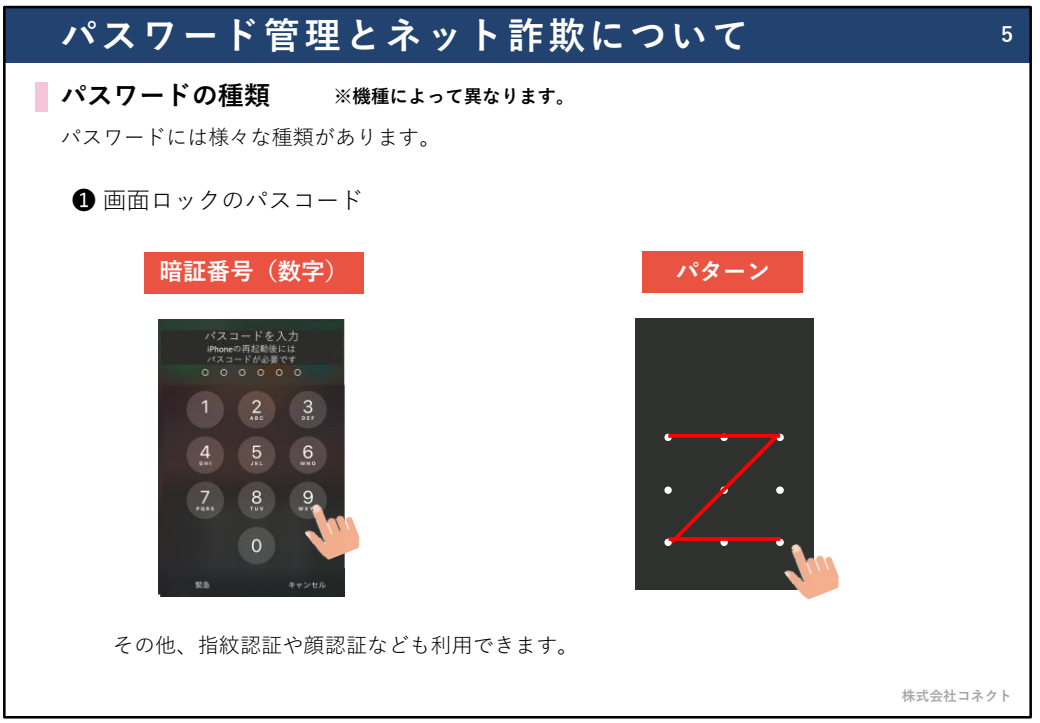
【講師原稿】
これらの重要な情報を守るパスワードは、自分の財産を守る「家の鍵」や「金庫の鍵」と同じです。
今後、スマートフォンがお財布代わりになる電子マネーの本格的な普及や、その他便利なサービスが増えてくると、まさにスマートフォンには「わが家の財産」が詰めこまれた状態になります。
その大切な鍵、すなわち、パスワードが盗まれてしまうと、他人が家（機器やスマートフォン）に侵入して、「わが家の財産」が勝手に盗み取られる可能性があります。
これからスマートフォンがさらに便利になれば、パスワードの重要性はますます高まります。パスワードは外に漏れないように、今まで以上にしっかり管理する必要があります。



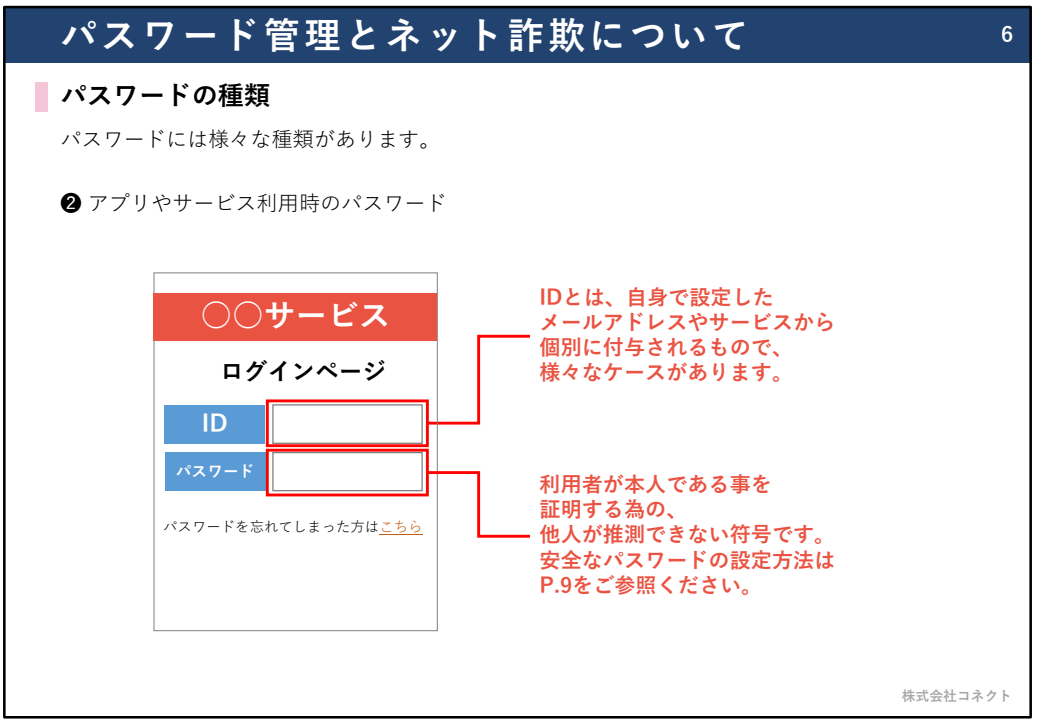
【講師原稿】
ここでは「パスワードの役割」についてお話しします。
スマホやインターネットを使うとき、本人だけが利用できるようにするために必要なのが「ID」と「パスワード」です。
例えば実生活に置き換えると、IDは「名前」、パスワードは「鍵」のようなものです。名前だけなら誰でも知ることができますが、
鍵がないと家の中には入れませんよね。同じように、IDとパスワードをそろえて入力することで、
本人確認ができ、スマホやパソコンから自分の情報にアクセスできる仕組みになっています。

逆に、もしこのパスワードが他人に知られてしまうと大変です。住所や履歴といった個人情報だけでなく、
ポイントやお金まで不正に利用される危険があります。つまり、パスワードは「自分を守る大切な情報」なんです。

誰でも見られる情報（商品の広告やキャンペーン）にはパスワードは不要ですが、自分だけが見られる情報には必ずIDとパスワードが必要になります。
この違いを理解し、しっかりとパスワードを守る意識を持ちましょう。

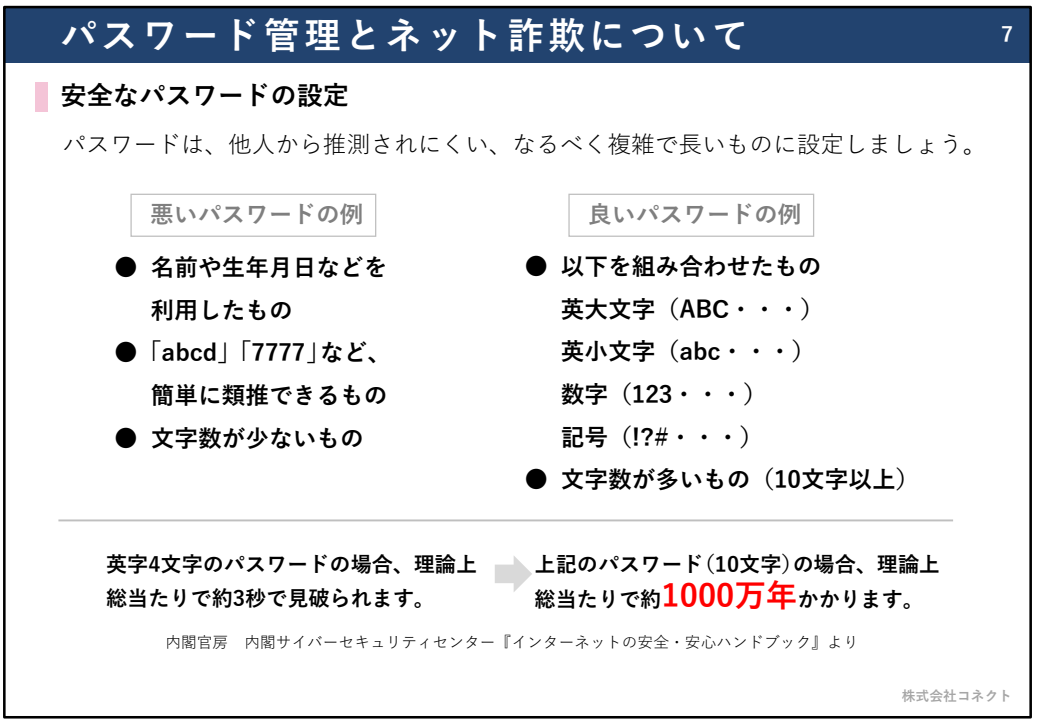


【講師原稿】
パスワードには様々な種類があります。
もっともイメージしやすいのは、スマートフォンの画面ロックを解除する際のパスワード（パスコードともいいます）ではないでしょうか。
4ケタから6ケタの数字を設定して入力するものや、任意の図形パターンを指でなぞるタイプのものがあります。
これらのパスワードも、他人に知られれば、自分のスマートフォンを人に勝手に使われるきっかけになりますので、十分注意が必要です。
最近では、パスワードを入力する代わりに、持ち主の顔や指紋を認証して、スマートフォンを起動させるタイプのものもあります。



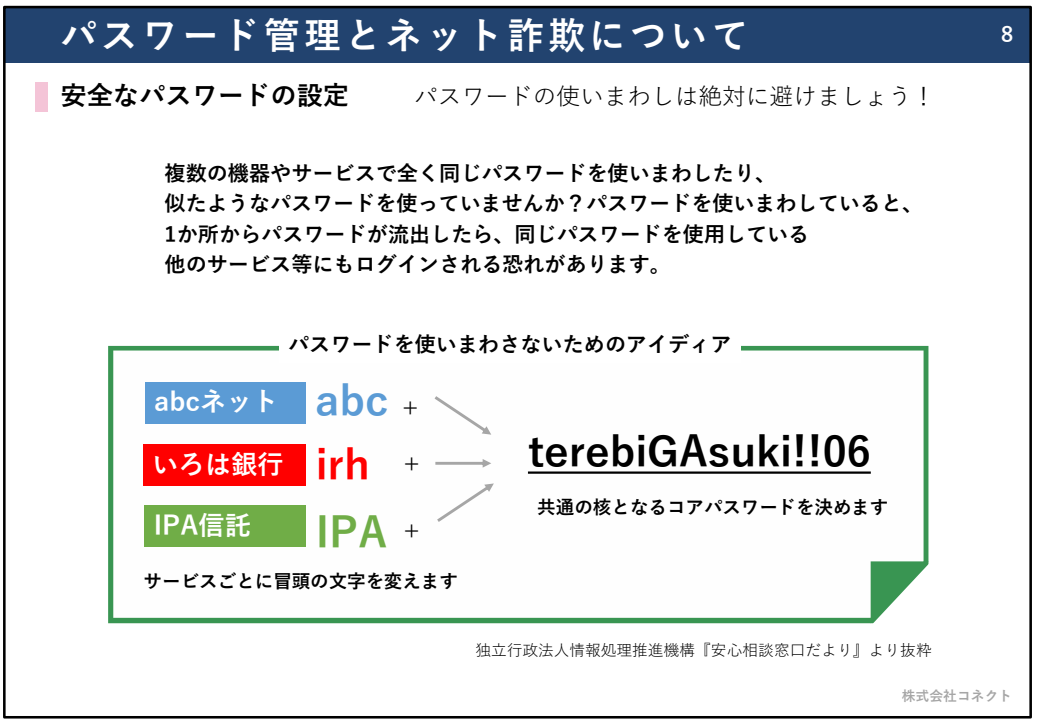
【講師原稿】
もう1つのパスワードのタイプは、さまざまなアプリを利用する際に必要になるものです。その際には、このような画面が出てきて、IDとパスワードを入力する必要があります。IDとは、利用者を識別するユーザー名のことで、名前に近いイメージです。
IDには、自分で設定できるケースや利用するサービスを提供する事業者から付与されるケース、自分のメールアドレスをIDの代わりにするケース等があります。次にそのIDと合致する、パスワードを入れることで、本人確認がなされたことになり、サービスの提供が許可される仕組みです。
このように、インターネット上のサービスを利用する際に、IDとパスワードを使って本人を確認することを「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。



【講師原稿】
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に作れば、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、解明するまでに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。

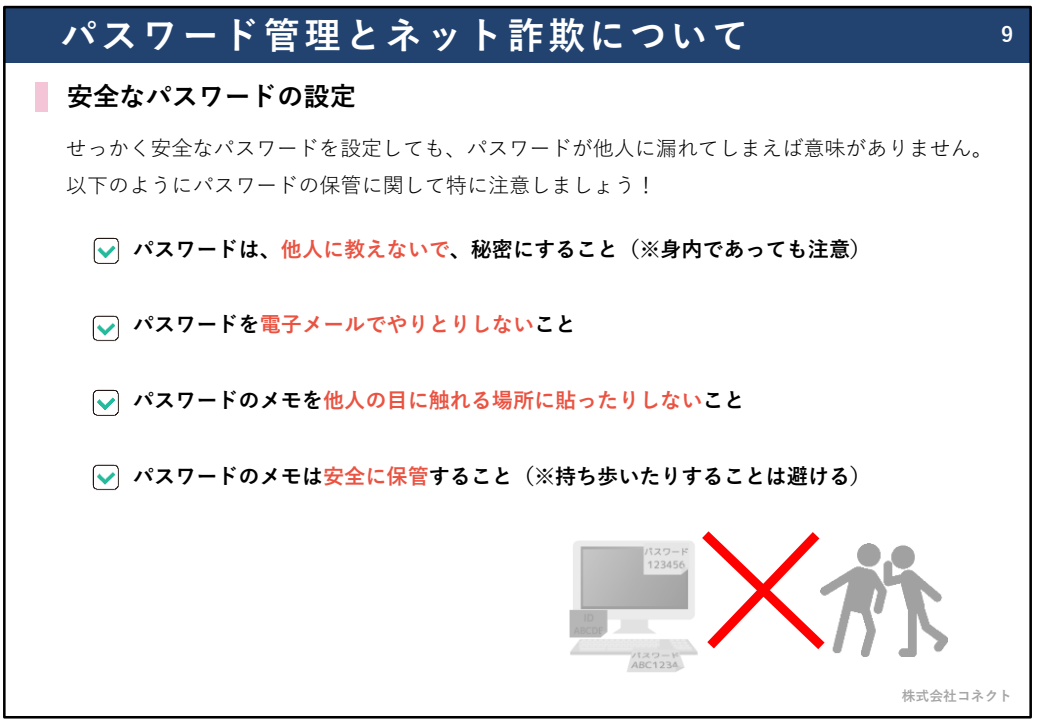
【講師向けコメント】
講師の皆様は、受講者の関心に応じて、パスワードを見破る攻撃の種類についても補足してください。パスワードが漏れるケースは、「総当たり攻撃」以外に、WEBサービス会社などが保管している、IDやパスワードなどの個人データが流出して使われる「リスト型攻撃」などもあります。
「リスト型攻撃」の場合、自分が使っているアプリなどで、情報流出が判明したら、速やかにパスワードを変更するなどの対策を取るよう、お伝えしてください。



【講師原稿】
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。

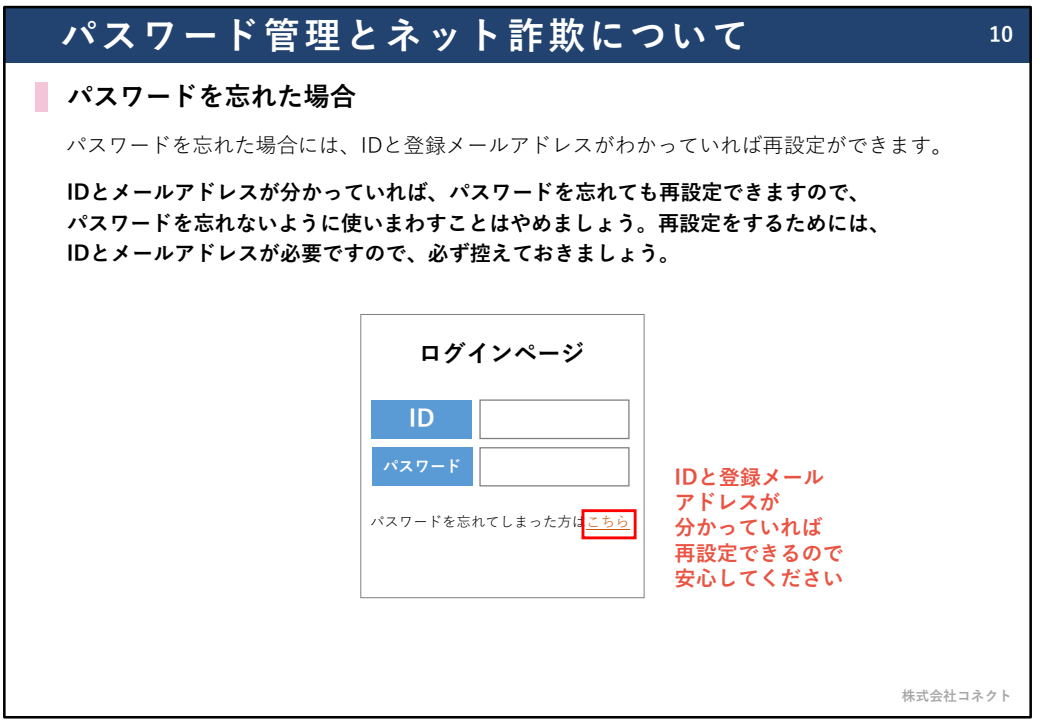
【講師向けコメント】
講師の皆様は、受講者の方から、定期的なパスワードの変更は必要かどうか質問された場合は、利用するサービスによっては、パスワードを定期的に変更することを求められる場合がありますが、このコアパスワードのように十分複雑なもので、複数のサービスで使いまわしをしていなければ、定期的な変更は必要ない旨をお伝えください。ただし、そのアプリ運営会社などから情報が漏洩した場合などは、速やかにパスワードを変更する必要があることにもご留意ください。



【講師原稿】
ここでは「安全なパスワードの保管と管理」についてお話しします。せっかく複雑で安全なパスワードを作っても、それを他人に知られてしまえば意味がありません。ですので、パスワードをどう守るかがとても大切です。

まず一番大事なのは「他人に教えない」ということです。家族や友人であっても、できるだけ秘密にしておきましょう。
次に、メールでやり取りをするのも危険です。送った相手以外が見てしまう可能性があるからです。

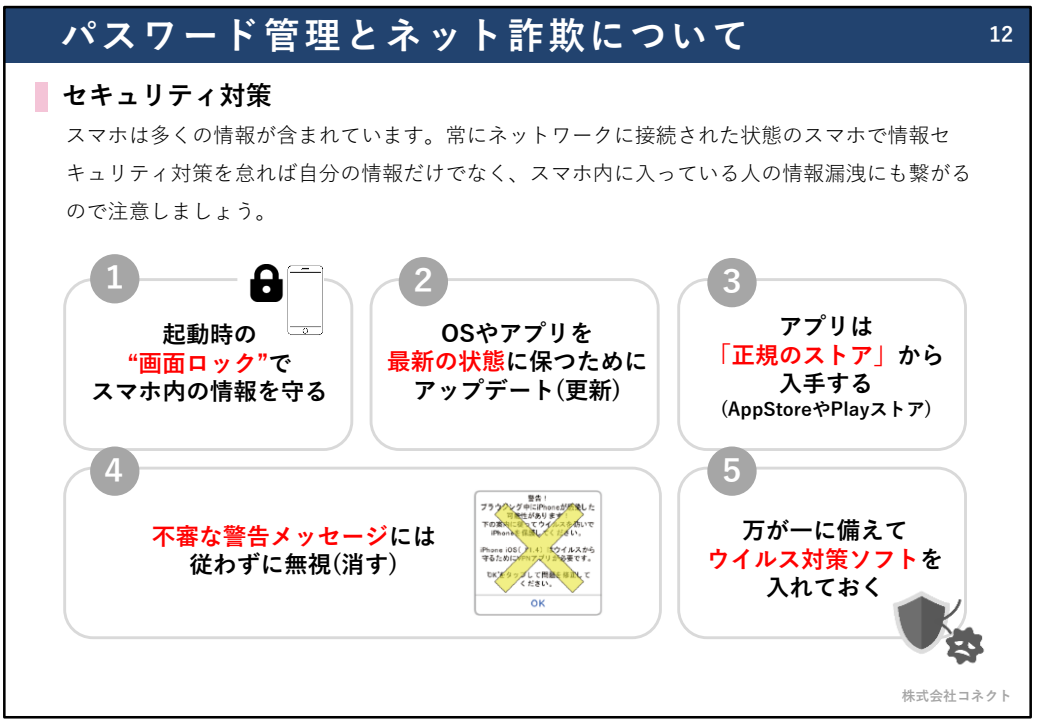
さらに、紙に書いて机の上やパソコンの画面に貼っておくのも危険です。これでは誰でも見えてしまいますよね。
どうしてもメモする場合は、人の目に触れない場所に安全に保管しましょう。
持ち歩く場合も、落としたり盗まれたりする可能性があるので注意が必要です。
まとめると「他人に教えない」「ネットでやり取りしない」「人目につくところに置かない」「安全に保管する」この4つを意識することが、パスワードを守る一番のポイントです。



【講師原稿】
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。

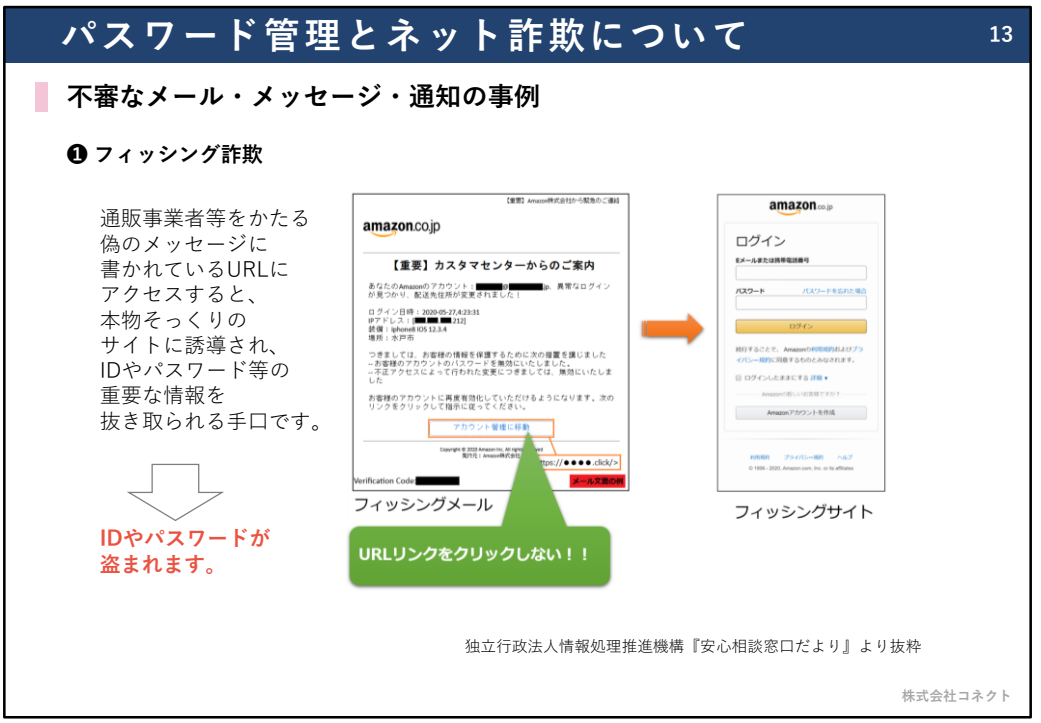
パスワードを忘れた場合は、利用するアプリやサービスのログインページに行きます。
たいていのログインページには、「パスワードを忘れてしまった方はこちら」のような内容が記載された場所がありますのでそこを押します。
すると、新しくパスワードを設定する方法が案内されているページが表示されたり、登録しているメールアドレスにパスワードを再設定するページを案内するメールが送られてきたりします。
後者の場合は、メールからそのサイトに移動して、新たにパスワードを設定すれば、ログインできるようになります。
その際は新しく設定したパスワードを必ずメモしましょう。

【講師原稿】
ここでは「もしパスワードを忘れてしまったらどうするか」についてお話しします。
最近はパスワードを使う機会が増えて、ついどこにメモしたかわからなくなったり、思い出せないこともありますよね。
そんなとき、まず一人で悩まないことが大切です。自分で再設定するのが難しいときは、家族やご友人など信頼できる人に相談してみてください。また、普段から利用している携帯ショップのスタッフも、相談できる心強い相手です。
ただし注意点として、すべてのパスワードを相談先で解決できるわけではありません。サービスごとに手続きの仕方が異なりますので、早めに対応することが安心につながります。
困ったときは「一人で抱え込まずに、信頼できる人に相談する」これを覚えておいてください。



【講師原稿】
スマホは多くの情報が含まれています。常にネットワークに接続された状態のスマホで情報セキュリティ対策を怠れば自分の情報だけでなく、スマホ内に入っている人の情報漏洩にも繋がるので注意しましょう。
今日からできる主な対策は５つです。

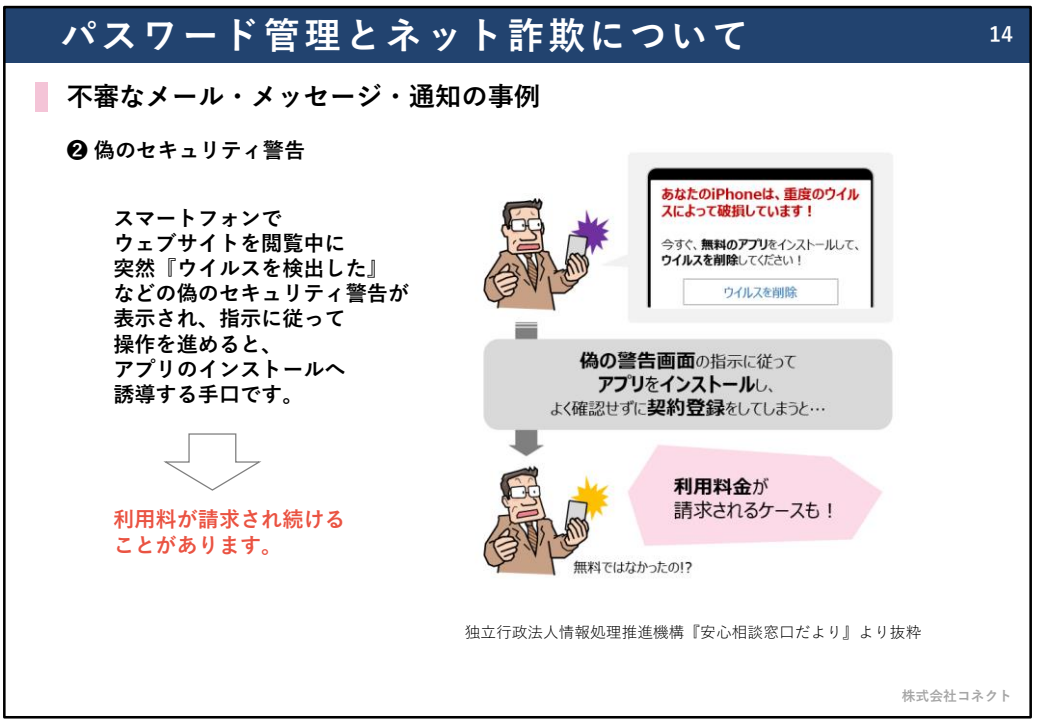
①画面ロック方法（パターン、パスコード、パスワード、生体認証）
②最新かの確認方法は割愛（時間に応じて口頭で説明）
③ブラウザから入手できるがNG、正規のストアからアプリを入手することで安全で信頼性の高いアプリを利用できるようになります。
④警告元がどこからなのかで判断する
⑤ウイルスバスターやノートンなど　500円程度の有料版がほとんど（無料版はセキュリティチェック項目が少ない）



【講師原稿】
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。

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を開かないようにしてください。

【講師向けコメント】
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。



【講師原稿】

「偽のセキュリティ警告」も、よく見られる詐欺の１つです。

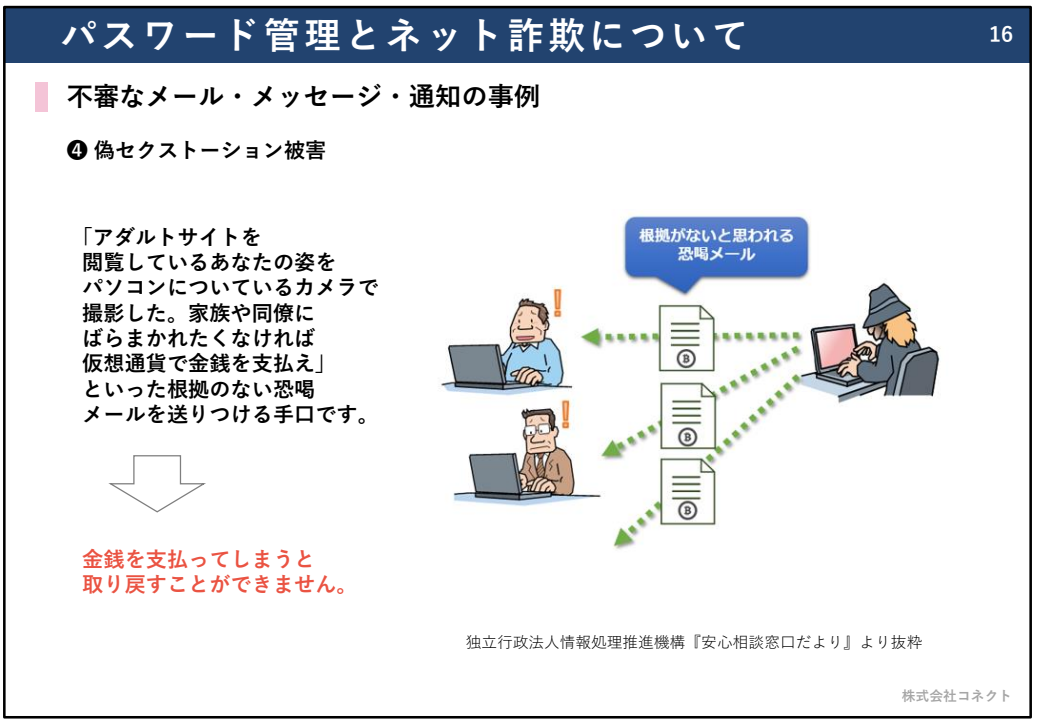
スマートフォンでウェブサイトを閲覧中に、突然、「重度のウイルスで破損しています」や、「個人情報が漏えいしています」といった偽のセキュリティ警告画面が出現します。

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。

【講師原稿】
「アカウント乗っ取り」では、Facebookのメッセンジャーのようなサービスに、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押しても、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。



【講師原稿】

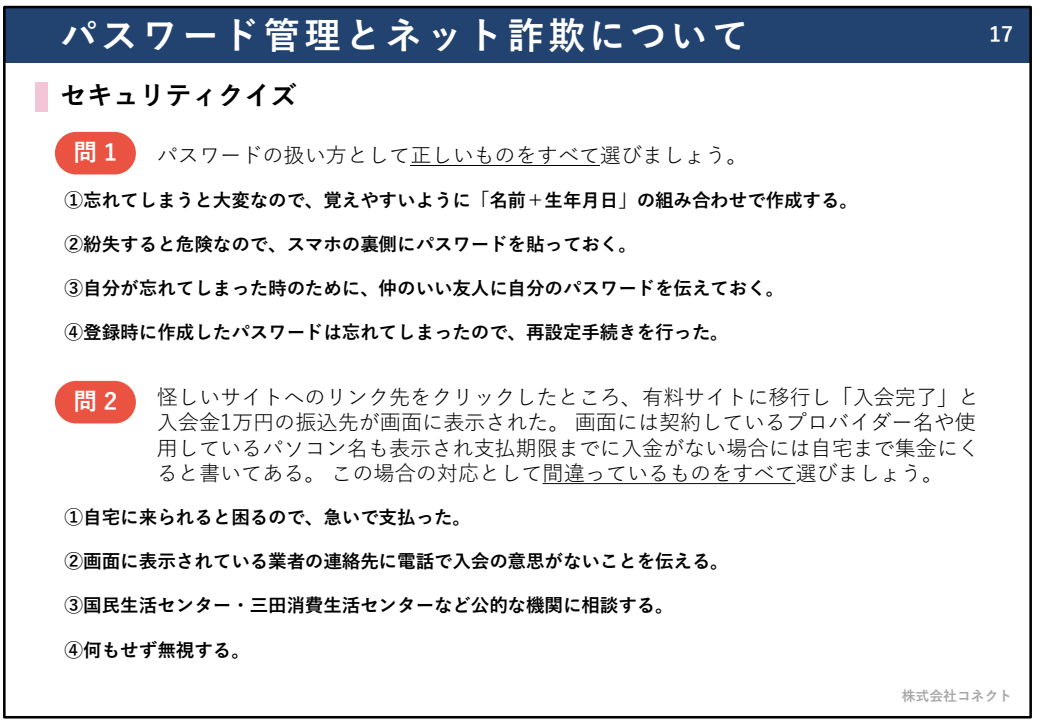
「偽セクストーション被害」とは、聞きなれない言葉かもしれませんが、このタイプの詐欺も最近増えています。

「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動画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。



正解：④
解説：ほとんどの場合、忘れてしまった場合は再設定が可能です。再設定した際には忘れないよう改めて保管しましょう
　　再設定のときには、メールアドレスや電話番号を利用するケースが多い。登録時に利用したメールアドレス/電話番号は把握しておきましょう
①推測されやすいパスワードはNG
②パスワードは他人から見られない場所に保管する&もちあるくのは避ける
③パスワードはたとえ親しい人であっても教えるべきではない
正解：①②
（解説）
見知らぬサイトからの架空請求の被害が増えています。IPアドレス等だけでは個人は特定されないので、落ち着いて対処することが必要です。無視するか、不安なら国民生活センターなど公的な機関に相談するようにしましょう。

パスワード管理とネット詐欺について

情報セキュリティクイズ

問 3

以前ネットショッピングのアマゾンを利用しました。数か月後アマゾンから「会員情報を更新してください」と偽のメールが届きました。本物のメールと比べて怪しいところはどこでしょう。

▼ 偽物

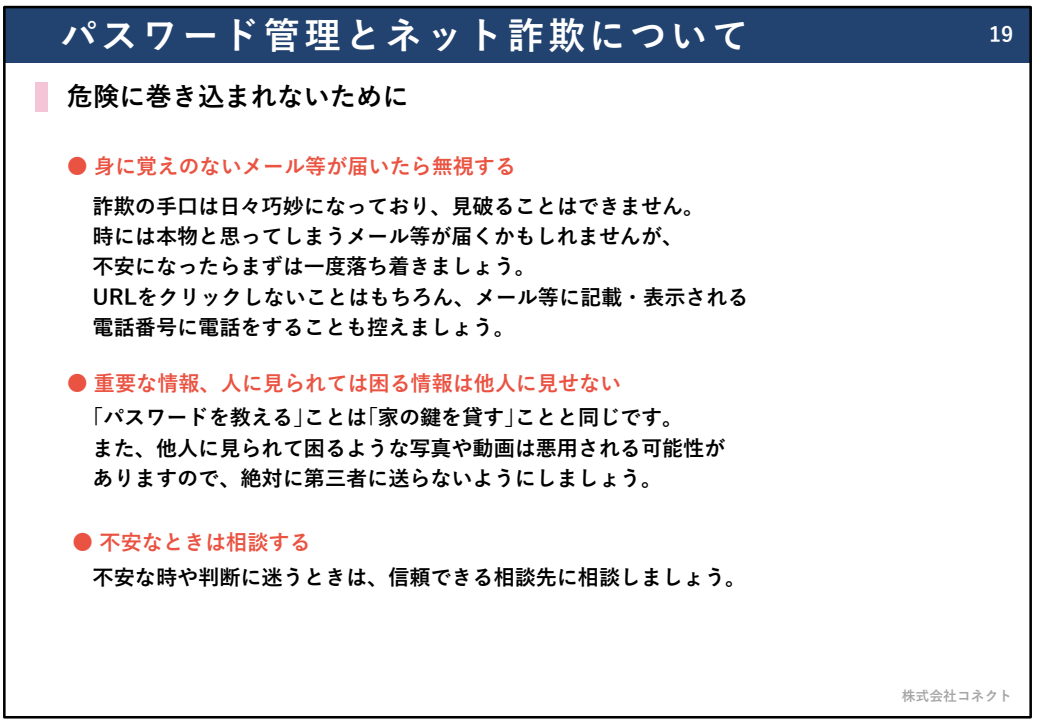
▼ 本物

※この画面はAmazonをかたる詐欺メールの例です。実際のAmazon公式メールではありません。

株式会社コネクト

正解：
・自分の名前が入っていない
・日本語がおかしい
・時間制限など緊急をあおるような文言がある

→怪しいと思ったらブラウザやアプリから変更をしましょう。



【講師原稿】

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、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。

「重要な情報、人に見られては困る情報は他人に見せない」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。

「不安なときは相談する」

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。

【講師原稿】
ここでは「困ったときに相談できる窓口」についてお話しします。
ネットやスマホのトラブルは、自分だけで解決しようとするとかえって被害が大きくなってしまうこともあります。そんなときは、専門の相談窓口にすぐ連絡しましょう。
まず、消費生活のトラブルで困ったときは「消費者ホットライン 188（いやや！）」です。身近な消費生活センターにつながります。
次に、ネットでの詐欺や有害情報については「違法・有害情報相談センター」で対応しています。Webからも受け付けができます。
そして、不安なメールや詐欺被害の相談をしたい場合は「警察相談専用電話 #9110」へ。こちらも全国共通の番号です。
困ったときに「どこに連絡すればいいのか」を知っているだけで安心につながりますので、ぜひ覚えておきましょう。

※本内容に登場する企業名・アプリ名・画面表示は、スマートフォンの
操作方法をわかりやすく紹介するための教育目的による例示です。
特定の企業・サービスを推奨・宣伝するものではありません。
商標・ロゴは各社に帰属します。

株式会社コネクト