Q1 サイバー防犯訓練

PC で調べものをしている最中、突然画面上に「パソコンをロックした。24 時間以内に 20 万円を支払うように。」という表示が！一体どうするのがよい？

A 大変だ！すぐにお金を払おう！

B まずは相手と連絡をとろう

C パソコンをネットワークから切り離そう

Q1 サイバー防犯訓練

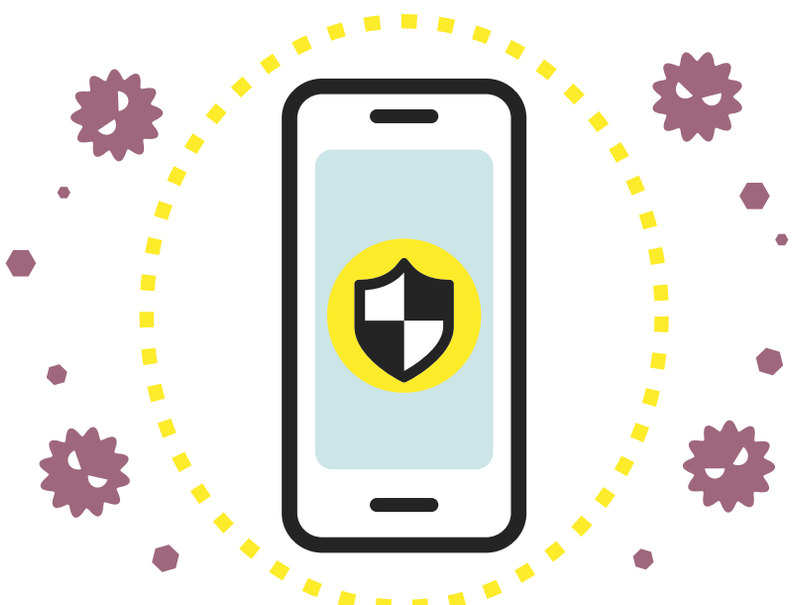
正解： C

解説

ファイルを暗号化したり、問題文のように端末を操作できなくして金銭を要求する悪質なソフトウェアを「ランサムウェア」といいます。ランサムウェアに感染した場合は、相手の要求に応じてはいけません。すぐに端末をネットワークから切り離し、セキュリティソフトでランサムウェアを除去するなどの対策を行いましょう。

Q2 サイバー防犯訓練

次のうち、セキュリティソフトがやってくれることとして、間違っているのはどれ？



A 危険な WEB サイトをブロックする

B 嫌いな人からのメールをブロックする

C メールの危険な添付ファイルを検知する

Q2 サイバー防犯訓練

正解： B

解説

通常、セキュリティソフトはパソコンやスマホの電源をオンにすると自動的に起動し、常時ウイルス感染やオンライン詐欺などから守ってくれます。新型のウイルスにも対応できるように、OS やセキュリティソフトは常に最新にアップデートしましょう。

Q3 サイバー防犯訓練

悪質なプログラムの一種である「ランサムウェア」。その説明として最も適切なのは次のうちどれ？

A パソコンのカメラを勝手に起動するプログラム

B パソコン内部の情報を暗号化し、身代金を要求するプログラム

C 勝手に迷惑メールを送信するプログラム

Q3 サイバー防犯訓練

正解： B

解説

「ランサムウェア」とは、パソコンやスマホに格納された情報を暗号化してアクセスできなくし、その復元と引き換えに金銭を要求する危険なプログラムです。感染を防ぐために、不審なメールや添付ファイルは開かないようにしましょう。また、万が一感染してしまった場合、金銭を支払っても情報が復元されるとは限りません。このような金銭の要求には応じないようにしましょう。

Q4 サイバー防犯訓練

メールなどを通じて感染を広げるコンピュータウイルス「Emotet」。「Emotet」に感染しないために気を付けるべきことは、次のうちどれ？

A メールのリンクは不用意にクリックしない！

B 普段使うメールアドレスは一つに絞る！

C スマホではなくパソコンからメールを開く！

Q4 サイバー防犯訓練

正解： A

解説

「Emotet」は、過去にあなたがメールのやり取りをしたことがある相手からのメールを装って届きます。添付ファイルを開いたり、不正な URL をクリックしたりすることで、コンピュータウイルスに感染してしまいます。正しい送信者からのメールであるかどうか確認をして、身に覚えのない添付ファイルや URL は開かないようにしましょう。必要に応じて送信者に問い合わせるなど、十分な対策をとることが大切です。

Q5 サイバー防犯訓練

コンピュータウイルス感染などが原因でパソコンに作られる「バックドア」。あなたのパソコンに「バックドア」が設置された場合、コンピュータが遠隔操作される危険性がある？それともない？

A 危険性があるので十分に気をつけよう！

B そんなわけあるか！大丈夫！

Q5 サイバー防犯訓練

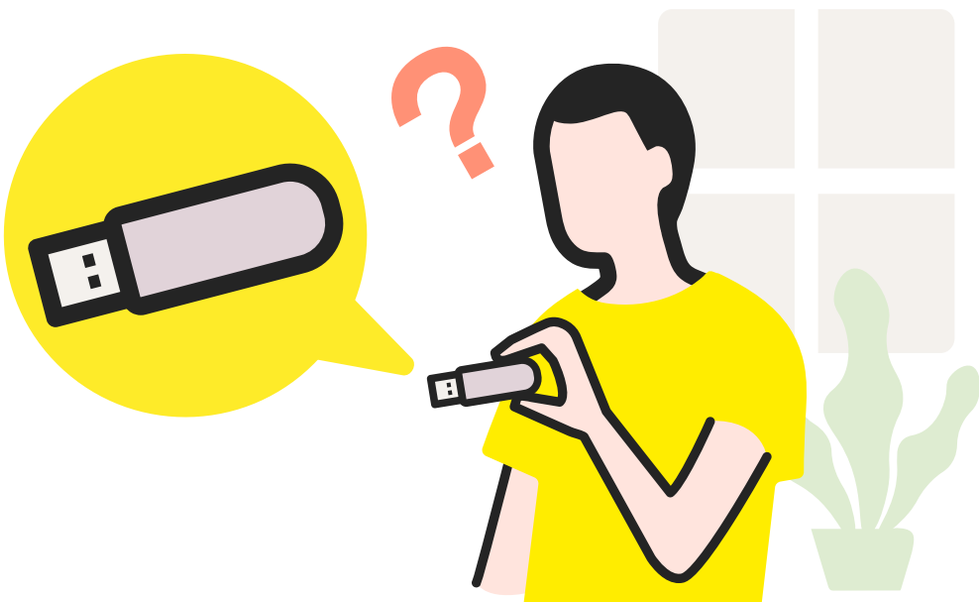
正解： A

解説

「バックドア」とは、外部からコンピュータへ侵入しやすくするためのプログラムで、「裏口」という意味があります。このプログラムが実行されてしまうと、正規の利用者認証やセキュリティ対策などを回避して、遠隔操作されてしまう危険性があります。「バックドア」はウイルスに感染した際に設けられることがあるため、ウイルス対策は必ず行いましょう。

Q6 サイバー防犯訓練

「会社内で USB メモリの落とし物が……持ち主に届けるために、
パソコンに接続して中身を確認しよう！」この行動は正しい？



A ○

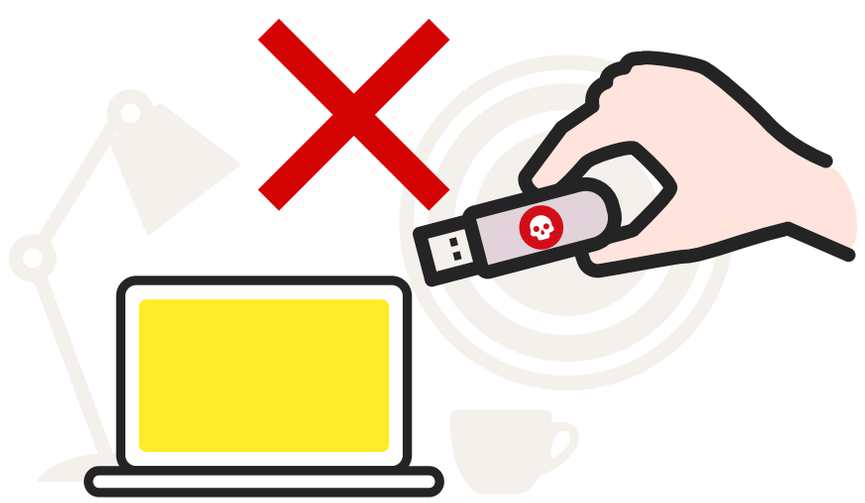
B ×

Q6 サイバー防犯訓練

正解： B

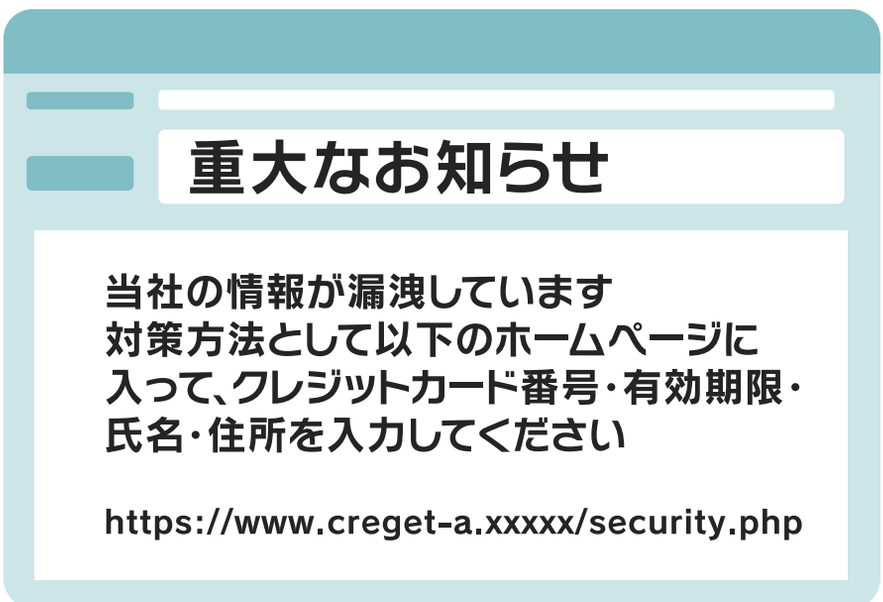
解説

出所がわからない USB メモリは、ウイルスに感染している可能性があります。ウイルスに感染した USB メモリをパソコンに差し込むと、プログラムが自動的に実行されて感染が拡大してしまいます。誰のものかわからない USB メモリは絶対に差し込まないようにしましょう！



Q7 サイバー防犯訓練

このようなメールを見たとき、すぐに考えるべきこととして正しいのは次のうちどれ？



A 個人情報がだまし取られる詐欺では！？

B 周りにも知らせるためにメールを転送しないと！

C すぐに情報登録しないと！

Q7 サイバー防犯訓練

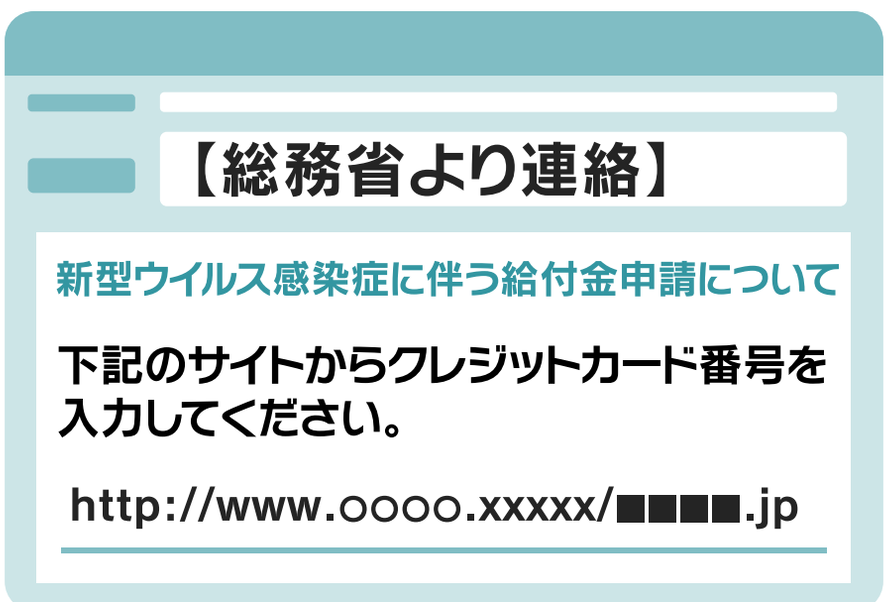
正解： A

解説

偽の電子メールから偽のウェブサイトに接続させるなどの方法で、クレジットカード番号やアカウント情報（ユーザー ID、パスワードなど）といった重要情報や個人情報を騙し取る行為のことを「フィッシング詐欺」といいます。今回の問題の場合、クレジットカード番号などを入力してしまうと、偽のメールを送った人物にカードを不正利用される可能性があります。

Q8 サイバー防犯訓練

以下のような件名のメールを受け取ったあなた。本文にはWEBサイトへのリンクと、クレジットカード番号を入力するようにという指示があります。このときに考えられることとして正しいものはどれ？



A ホラー動画を見せられるいたずらだろう

B 個人情報が盗まれる詐欺メールだろう

C 総務省からの給付金申請用の連絡だろう

Q8 サイバー防犯訓練

正解： B

解説

近年、総務省や金融庁といった行政機関のふりをして、個人情報などを盗む詐欺メールが送られる事例が多数発生しています。このようなメールが届いた際に、WEB サイトのリンクをクリックしたり個人情報を入力したりしないようにしましょう。また、迷惑メールフィルターを活用するのも効果的です。

Q9 サイバー防犯訓練

有名人から次のようなメッセージが届いたあなた。このときの正しい行動は次のうちどれ？

A 仲良くなれるチャンス！すぐに送金！

B まずはメッセージのやりとりを楽しむ！

C 送金せずに無視！

Q9 サイバー防犯訓練

正解： C

解説

サイバー犯罪者によって乗っ取られた SNS アカウントから、ダイレクトメッセージでサイトのリンクなどが拡散するケースがあります。たとえ有名人の公式アカウントからのメッセージであっても、乗っ取られている可能性があるので、不審なリンクは開かないようにしましょう。実際に、アメリカで有名人のアカウントが乗っ取られ、詐欺の被害が生じてしまった例があります。

Q10 サイバー防犯訓練

SNS で仲良くなった人から「みんな儲かってるから絶対やったほうが良いよ！」と暗号資産への投資を強く勧めるメッセージが。こんなとき、あなたならどうする？

A 怪しいので断わる

B 取引内容を十分理解したうえで契約する

C すぐに契約する

Q10 サイバー防犯訓練

正解： A

解説

SNS 上で面識がない人から DM が届き、やりとりを続けた結果、暗号資産の儲け話をされるケースがあります。その結果、詐欺サイトやアプリへ誘導され、金銭を詐取された事例があるので、「儲かるから教えてあげるよ」と提案されても冷静に判断をするようにしましょう。

Q11 サイバー防犯訓練

ある日、人気俳優から突然のダイレクトメッセージ！本当に本人なのかな……でも、せっかくのチャンスを無駄にしたくない！あなたが取るべき行動は？

A 「本人であるか？」と質問する

B 本人である証拠となる動画データを送らせる

C 相手にせず無視する

Q11 サイバー防犯訓練

正解： C

解説

サイバー犯罪者によって乗っ取られた SNS アカウントから、ダイレクトメッセージで詐欺リンクなどが拡散されるケースがあります。たとえ有名人の公式アカウントであっても、乗っ取られている可能性があるので、不審なリンクは開かないようにしましょう。動画も盗用されたものの可能性があります。実際に、アメリカで有名人のアカウントが乗っ取られ、詐欺の被害が生じてしまった例があります。

Q12 サイバー防犯訓練

WEB サイトの URL についている鍵のマーク。これは何を表している？

A 通信が暗号化されている

B 安全な WEB サイトである

C ロックされて開くことができない

Q12 サイバー防犯訓練

正解： A

解説

URL についている鍵マークは「通信が暗号化されている」という意味です。ただし、URL に鍵マークがついていても、詐欺サイトの可能性はまだあります。鍵マークをクリックすると、きちんとした証明書が登録されているかどうかも確認できるので、正規の運営会社の名前が書かれているか確認し、疑わしいときは利用をやめましょう。また、URL の文字列を工夫したり、ドメインに既存の企業名を取り込んだ偽の URL も存在するため、注意が必要です。

Q13 サイバー防犯訓練

WEB サイトなどに記載された URL を一度クリックしただけで
多額の料金を請求されてしまう「ワンクリック詐欺」。次のうち、
ワンクリック詐欺の対応としてやってはいけないことはどれ？

A 料金を請求されても無視する

B 支払い理由の確認電話をする

C 消費生活センターや警察に相談する

Q13 サイバー防犯訓練

正解： B

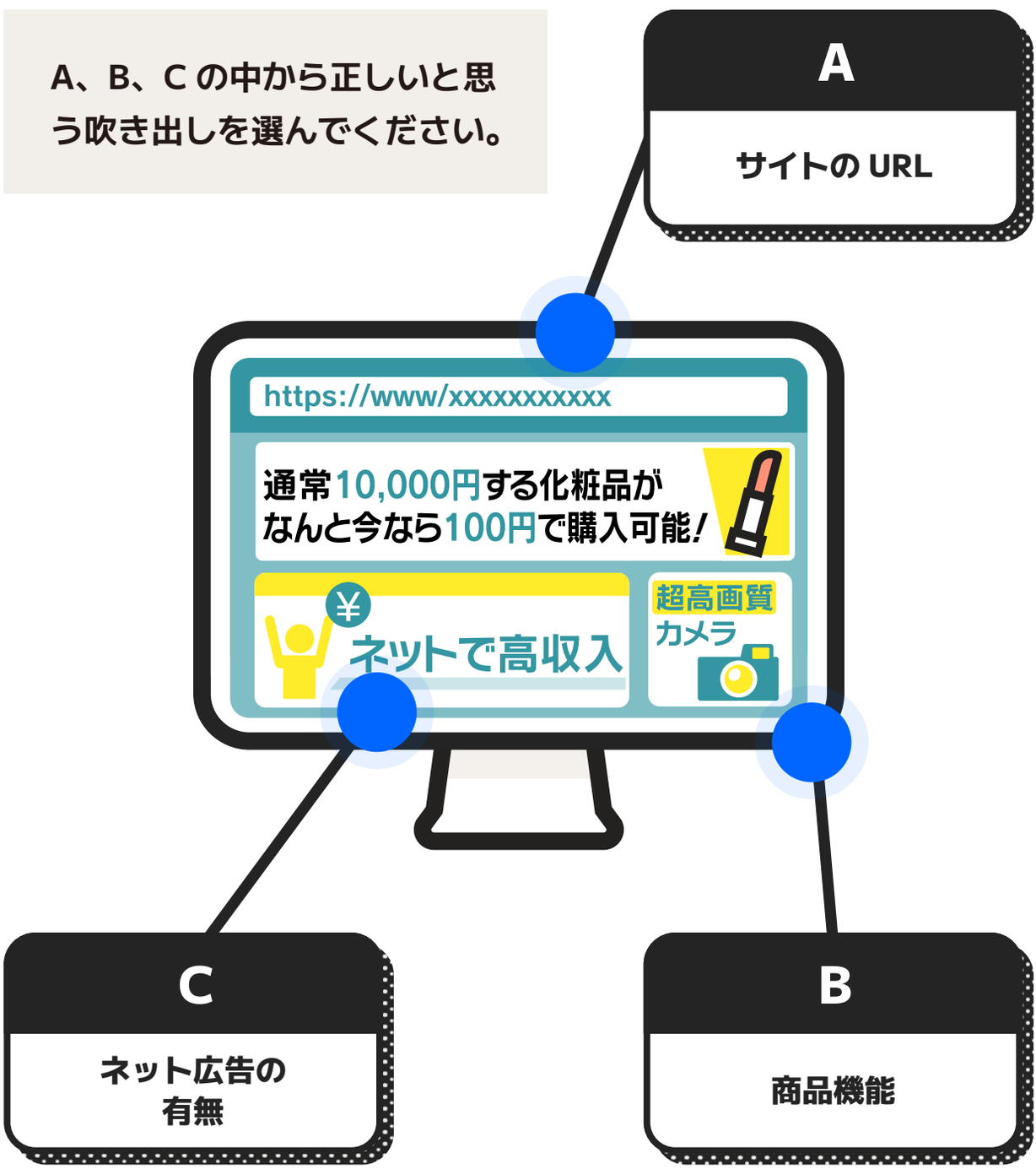
解説

相手先に電話することは、自分の個人情報を渡すことにつながるため、決して連絡をしてはいけません。「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律」では、「電子消費者契約に関する民法の特例」として消費者が契約する意志がなく申し込んだ場合における救済措置が定められています。多額の請求をされても無視するか、不安であれば消費生活センターや警察に相談しましょう。

Q14 サイバー防犯訓練

最近増えている、本物そっくりに作られた偽のショッピングサイト。サイトが偽物だと見破るポイントは、次のうちどれ？

A、B、C の中から正しいと思う吹き出しを選んでください。



Q14 サイバー防犯訓練

正解： A

解説

偽のサイトかどうかチェックする際には、「サイトの URL」「商品の価格（極端に安くないか）」「購入画面に不審な点がないか」を見るようにしましょう。目で見て確認する以外にも、セキュリティソフトを活用することも有効です。各都道府県警察などのサイトで対策が詳しく紹介されているので、一度見てみることをお勧めします。

Q15 サイバー防犯訓練

WEB サイトを見ていたら、こんな警告が！実在する企業ロゴも載っているし、一刻も早く記載された電話番号に連絡して解決した方がいい？

A ○

B ×

Q15 サイバー防犯訓練

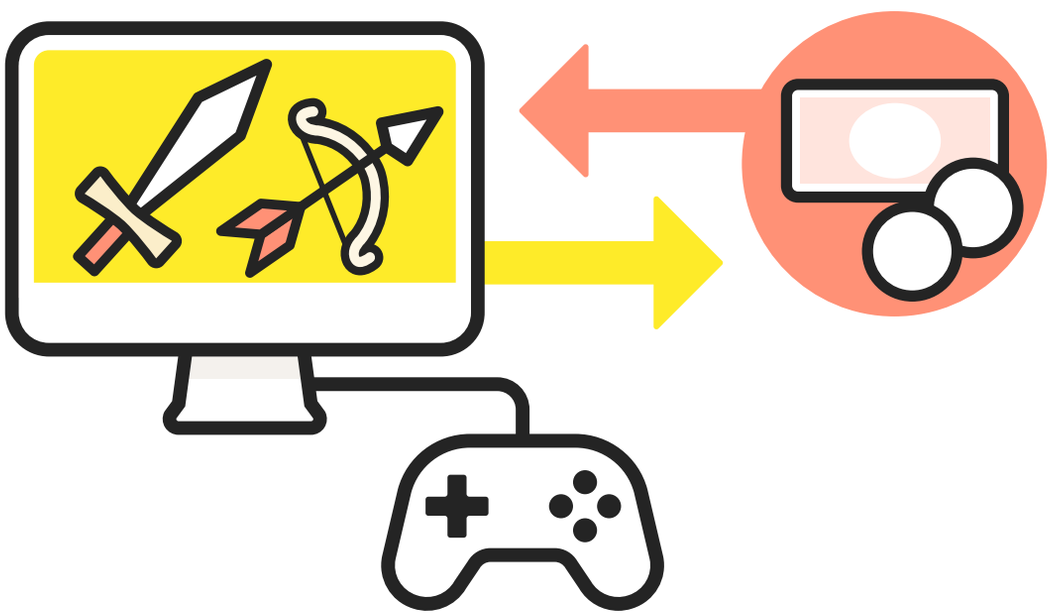
正解： B

解説

パソコンの画面上に偽の警告を表示し、偽のセキュリティ会社に電話をさせ、パソコンの修復作業やセキュリティ費用として金銭を請求するケースがあります。不審な警告表示が出た際は、ブラウザごと終了し、無視するようにしましょう。

Q16 サイバー防犯訓練

オンラインゲームのアイテムやキャラクターのデータを現実のお金で売買する行為は、世界的に推奨されている。正しい？間違っている？



A 正しい（世界的に推奨されている）

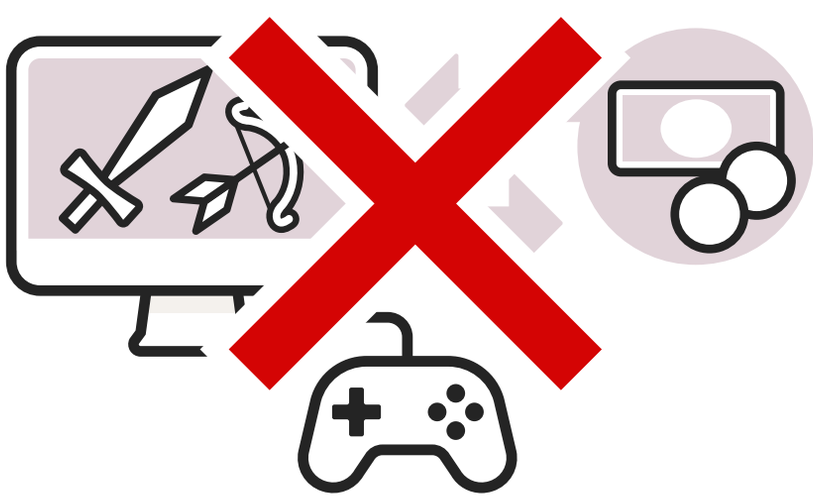
B 間違っている（ほぼ全てのゲームで禁止されている）

Q16 サイバー防犯訓練

正解： B

解説

ネット上の掲示板などを通してオンラインゲームのアイテムなどを現金で取引する行為は、ほとんど全てのゲームで禁止されています。禁止事項を破った場合は、アカウントの停止などの措置が行われます。中には、お金を払ったのにデータが送られてこないというトラブルに発展することもあるため、ルールを守り、禁止されている行為に手を出さないようにしましょう。



Q17 サイバー防犯訓練

SNS アカウントの安全なパスワードを作ろうとしているあなた。
次のうち、安全性が低くなるので避けるべき選択はどれ？

A 大文字と小文字のアルファベットに記号を混ぜる

B ペットの名前と誕生日を組み合わせる

C パスワード生成ツールを使う

Q17 サイバー防犯訓練

正解： B

解説

SNS などにペットの名前や誕生日に関する情報を投稿していた場合、犯罪者はその情報からパスワードの組み合わせを試すなどによりパスワードを特定し、アカウントを不正利用する可能性があります。パスワードは、大文字と小文字が混在したものに数字や記号を組み合わせると安全性が高まります。また、安全性の高いパスワードを生成してくれるツールを利用するという方法もあります。

Q18 サイバー防犯訓練

桁数の少ないパスワードは、簡単に破られる危険性があります。
その際の手口として、よくあるものは次のうちどれ？

A 文字列を順番にためす

B 占いで決める

C 一発勝負で試してみる

Q18 サイバー防犯訓練

正解： A

解説

あり得る文字列の組み合わせを一つずつ試すことで、いつかその数字を当てるという手法を「ブルートフォースアタック（総当たり攻撃）」といいます。例えば、４桁の数字だけのパスワードは１万通りの組み合わせがありますが、コンピューターがこれを一つずつすべて試していくのはさほど時間がかかりません。文字の種類や桁数を増やすことでブルートフォースアタックの対策を行いましょう。

Q19 サイバー防犯訓練

安全性の低い、小文字アルファベット４桁のパスワードが解読されるまでにかかる時間はどのくらい？

A　あくびの間くらい

B　カップ麺ができるくらい

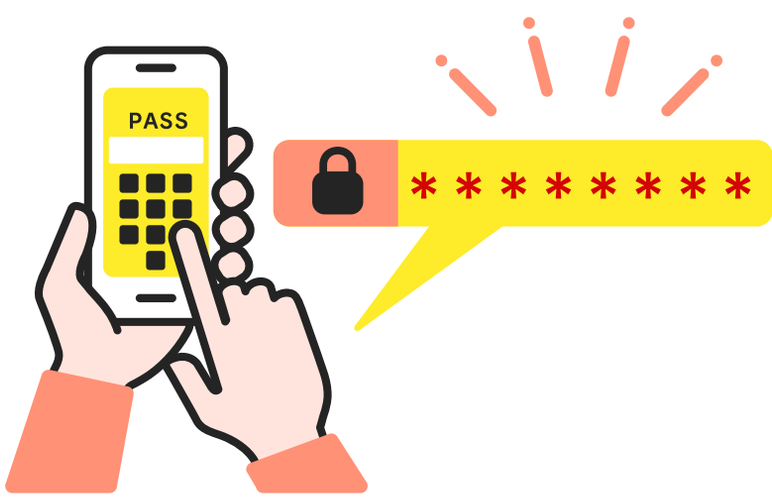
C　映画を観終わるくらい

Q19 サイバー防犯訓練

正解： A

解説

パスワードは、文字の種類が少ないほど、また桁数が少ないほど、容易に解読されてしまいます。例えば「アルファベット小文字のみ、4桁」なら、たった3秒ほどで解読されてしまう場合もあります。パスワードは、大文字と小文字が混在したものに数字や記号を組み合わせると安全性が高まります。また、安全性の高いパスワードを生成してくれるツールを利用するという方法もあります。



Q20 サイバー防犯訓練

友人から「いくつか新しいSNSアカウント作ろうと思ってるんだよね」と言われたあなた。アドバイスとして正しいものはどれ？

A パスワードは短くて覚えやすいものがいいよ

B パスワードは友達と一緒に管理するといいよ

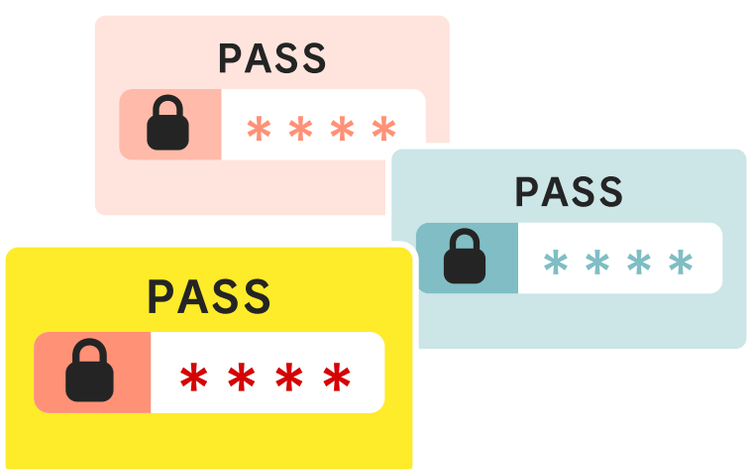
C パスワードはアカウント毎に使い分けるといいよ

Q20 サイバー防犯訓練

正解： C

解説

複数のサービスで同じ ID やパスワードを使いまわしていると、一つのサービスで情報が流出した場合、他のサービスでも被害を受けてしまう可能性があります。このような事態を防ぐためにも、パスワードは使いまわさずに別々のものを設定するようにしましょう。



Q21 サイバー防犯訓練

使っていないSNSアカウントを放置しているあなたに、友達からアドバイスが。彼はなぜこんなことを言うの？

A アカウントの多さを自慢したいから

B 放置したアカウントが乗っ取られる場合があるから

C データ通信量が減ってお得になるから

Q21 サイバー防犯訓練

正解： B

解説

アカウントを放置し続けると、アカウントが乗っ取られてしまう場合があります。たとえ自分が使っていない SNS であっても、既存のユーザーに対し勝手にダイレクトメッセージなどが送られるなど二次被害が広がるおそれがあります。最近あまり使用していないアカウントであっても、乗っ取り被害のリスクを減らすために 2 段階認証などセキュリティ設定を強化することが重要です。

Q22 サイバー防犯訓練

10 桁のパスワードをつくるとき、数字のみだと 100 億通り。
では、アルファベットの大文字と小文字・数字・記号交じりだと、
およそ何通り？

A およそ 2785 億通り

B およそ 2785 兆通り

C およそ 2785 京通り

Q22 サイバー防犯訓練

正解： C

解説

数字だけの場合、1 桁は 10 通りしかないため 10 の 10 乗で 100 億通りとなります。一方、アルファベットの大文字と小文字・数字・記号交じりだと 1 桁につき 88 通りになり、88 の 10 乗はおよそ 2785 京 97 兆 6009 億通りになります。これほど多いと機械入力でも事実上突破不可能となります。

Q23 サイバー防犯訓練

3 日前にネットで商品を購入したあなた。すると、SMS（ショートメッセージサービス）でこんな不在通知が。次のうち、あなたが取るべき行動はどれ？

A リンクを開いてすぐに中身を確認する

B 返信して詐欺メールか確かめる

C リンクは開かず、公式サイトから確認する

Q23 サイバー防犯訓練

正解： C

解説

SMS を悪用したフィッシング詐欺のことを「スミッシング」といい、今回のようなケースもその可能性が高いといえます。企業によっては、消費者に連絡をする際に使用するメールアドレスや SMS の番号を公開している場合があります。SMS が届いて確認する場合は、公式サイトでスミッシングに関する情報が公開されていないかチェックし、本物かどうか判断しましょう。

Q24 サイバー防犯訓練

SMS（ショートメッセージサービス）でこのようなメッセージと WEB サイトの URL が届いたあなた。次のうち、取るべき行動はどれ？

A すぐにリンクを開いて確認する

B リンクは使わず、公式サイトから確認する

C メールに返信して確認する

Q24 サイバー防犯訓練

正解： B

解説

SMS で送られてきた URL はすぐにタップせずに、本当に安全なリンクなのか、また似た事例の詐欺手口が存在しないかどうかを、インターネットなどで確認をしましょう。実際に利用している電力会社からの連絡かどうか心配な場合は、公式サイトからマイページにアクセスをして確認をしましょう。電力会社などの会社によっては、公式サイトで詐欺に注意するよう呼びかけていることもあります。

Q25 サイバー防犯訓練

SMS（ショートメッセージサービス）を利用した詐欺「スミッシング」。この名称は、「SMS」と何の言葉を組み合わせたもの？

A SMS＋カンニング

B SMS＋ハッキング

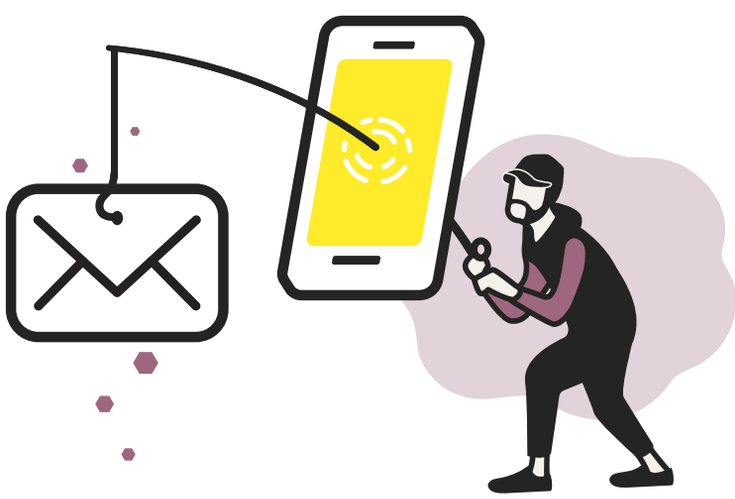
C SMS＋フィッシング

Q25 サイバー防犯訓練

正解： C

解説

SMS は「ショートメッセージサービス」の略で、携帯電話番号を宛先にしてメッセージのやりとりができるサービスのことです。最近、SMS で宅配業者などを装って個人情報やお金を盗み取ろうとする詐欺が発生しており、このような SMS を悪用したフィッシング詐欺を「スミッシング」といいます。急にメッセージが送られてきても慌てずに、まずは本物の URL かどうかやスミッシングの事例がないかどうかを調べてみましょう。



Q26 サイバー防犯訓練

送信元番号がランダムなアルファベットの羅列になっている SMS を受け取ったあなた。その原因として考えられるのは、次のうちどれ？

A スマホ利用者が増え、数字番号が足りなくなった

B フィッシング詐欺の可能性が高い

C 携帯ショップに行けばオプションで番号を変更できる

Q26 サイバー防犯訓練

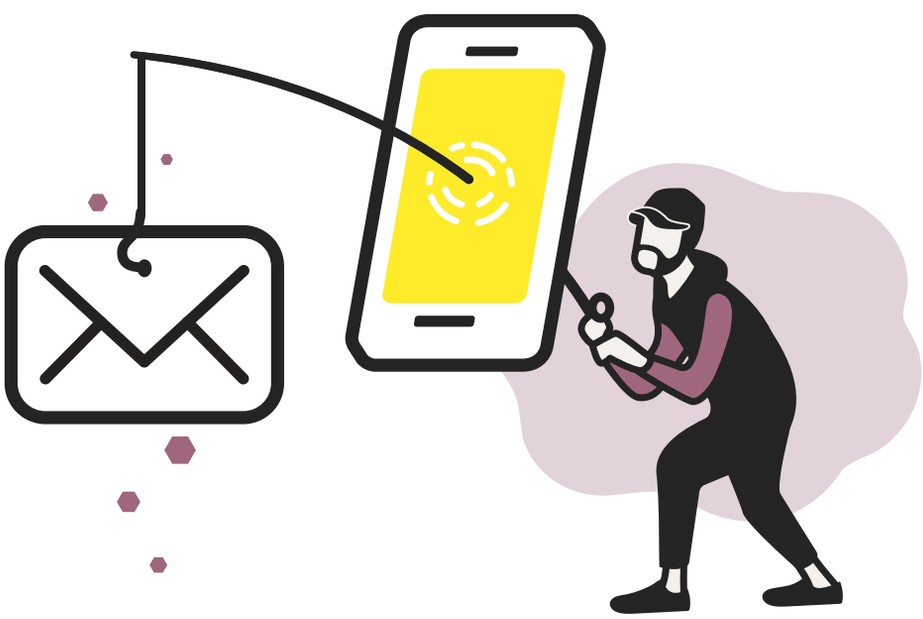
正解： B

解説

送信元がアルファベットの SMS は、国際網を経由している可能性があります。海外には利用審査や契約手続きを厳格に行わない事業者が存在しており、フィッシング詐欺に悪用されやすくなっているので、詐欺を疑う判断基準にしましょう。

Q27 サイバー防犯訓練

フィッシング詐欺と考えられるSMSを受け取ったことがある人は、全日本国民のうち約何％？



A 約37%（だいたい3人に1人）

B 約57%（だいたい2人に1人）

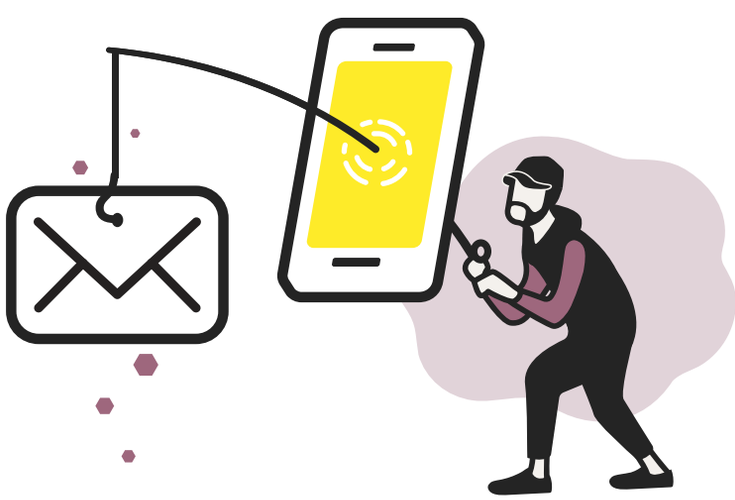
C 約77%（だいたい4人に3人）

Q27 サイバー防犯訓練

正解： B

解説

2022年にフィッシング対策協議会が発表した「SMSを用いたフィッシング詐欺についての意識調査※NTT コムオンライン調べ」のデータによると、年代・性別などの比率がほぼ均等になるように選ばれた全5275名のうち、半数以上の人が「フィッシング詐欺と考えられるSMSを受け取ったことがある」と回答しました。この結果から、SMSによるフィッシング詐欺「スミッシング」は決して珍しいものではないことがわかります。



Q28 サイバー防犯訓練

iPhone ユーザーにとって便利な iCloud のカレンダー共有設定。
これを狙った悪質な犯罪手口は、次のうちどれ？

※iPhone は Apple Inc の商標です。

A iCloud 機能が利用できないようにする

B iPhone そのものを乗っ取る

C iCloud カレンダーからスパムメッセージを送る

Q28 サイバー防犯訓練

正解： C

解説

iPhone のカレンダー乗っ取りは、iCloud のカレンダー共有設定を悪用されることで起こります。スパムメッセージの送信者は、受信者を誘導し、出会い系サイトやマルチ商法に案内したり、ワンクリック詐欺に利用したりしたいと考えています。カレンダーに身に覚えのない予定が入っていても、iPhone のそのものが乗っ取られたり、ウイルスに感染しているわけではないので安心してください。落ち着いて冷静に対処しましょう。

Q29 サイバー防犯訓練

ある日、iPhone のカレンダーを見たら「iPhone が保護されていない可能性があります」と書かれた予定が追加されていました。この場合、取るべき正しい行動はどれ？

※iPhone は Apple Inc の商標です。

A 保護してもらうために詳細を見てみよう

B リンクも貼られているし、とりあえず押して確認しよう

C これは詐欺だ 速やかに削除しよう

Q29 サイバー防犯訓練

正解： C

解説

カレンダーに知らない URL が記載されていた場合、その URL をクリックすると不審な WEB サイトに飛ばされ、個人情報の入力などを求められる可能性があります。カレンダーに限らず、メールや SMS、SNS のダイレクトメッセージで送られてきた URL は安易にクリックせず、速やかに削除しましょう。

Q30 サイバー防犯訓練

iPhone のカレンダーに身に覚えのない予定がたくさん追加されていた！これ以上被害に遭わないために、避けるべき行動は？

※iPhone は Apple Inc の商標です。

13:00  あなたのデータは危険にさらされている可能性があります！

14:00  あなたの情報がオンライン上に公開されているかも・・・

15:00  警告!お使いのiphoneは深刻な損傷を受けて・・・

A カレンダーに追加された身に覚えのない予定を削除する

B カレンダーに記載されているリンクをクリックする

C カレンダーのスクリーンショットをとる

Q30 サイバー防犯訓練

正解： B

解説

カレンダーに知らない URL が記載されていた場合、その URL をクリックすると不審な WEB サイトに飛ばされ、個人情報の入力などを求められる可能性があります。カレンダーに限らず、メールや SMS、SNS のダイレクトメッセージで送られてきた URL は安易にクリックせず、速やかに削除しましょう。

Q31 サイバー防犯訓練

あなたがカフェでパソコンやスマホを使うとき、セキュリティの観点でより安心な席は次のうちどれ？

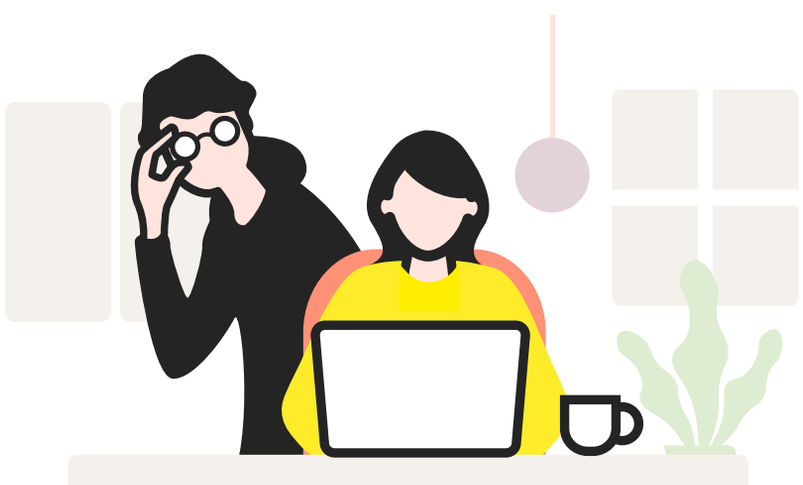
A、B、C の中から正しいと思う吹き出しを選んでください。

Q31 サイバー防犯訓練

正解： A

解説

PC やスマホを使うときは、画面を覗き見されないように注意する必要があります。背後が壁の席を選べば、後ろに回り込まれる危険性はありません。ただし、近くに窓や鏡がある場合には、画面の反射にも気をつける必要があります。覗き見を防ぐ画面フィルムなどを活用し、対策しましょう。



Q32 サイバー防犯訓練

立ち寄ったカフェでフリー Wi-Fi を見つけたあなた。セキュリティ保護がないのが少し気になったものの、短時間しか使う予定はなかったので、そのまま接続してネットショッピングを楽しみました。この行動は、セキュリティ的に正しい？間違ってる？

A 正しい（安全）

B 間違っている（危険）

Q32 サイバー防犯訓練

正解： B

解説

セキュリティ保護がされていないフリー Wi-Fi は、悪意を持った人に通信を傍受されている危険性があります。そのため、そのようなWi-Fi に接続して、カード番号や口座番号などの重要なデータをやり取りすることはリスクを伴います。モバイル通信を利用したりWi-Fi を利用したりする際は、通信内容を暗号化する VPN（仮想プライベートネットワーク）機能を使ってセキュリティを高めましょう。

Q33 サイバー防犯訓練

重要な個人情報が漏洩するおそれがあるのは、この写真（挿絵）のどこでしょう？

A 洋服のブランド

B 顔を隠す為のスタンプ

C 指紋

Q33 サイバー防犯訓練

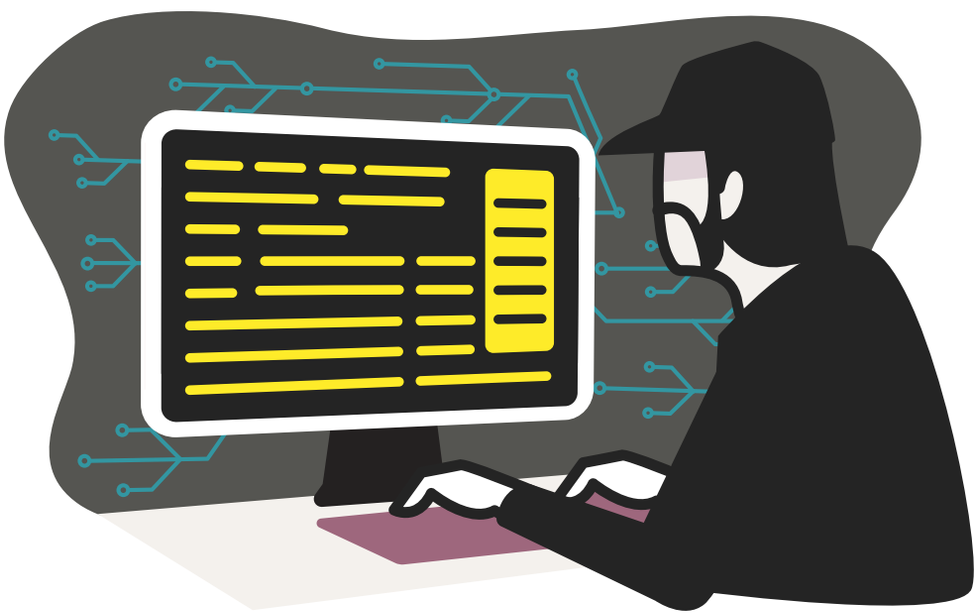
正解： C

解説

スマホのカメラ精度は年々高まっており、スマホ写真に写ったピースサインの指紋画像を解析して複製し悪用するという事例が発生しました。生体認証は、スマホやパソコンの機器のロック解除や、金融機関の認証にも活用されるものなので、悪用されると大変です。指紋認証も万全ではないので、パスワードなど他の方法と組み合わせて使うとよいでしょう。

Q34 サイバー防犯訓練

非合法な情報などが取引されるなどサイバー犯罪の温床となっている「ダークウェブ」。次のうち、「ダークウェブ」の特徴はどれ？



A 画面と文字が暗く、何が書いてあるかが読めない

B 一般的なブラウザでは検索できない

C 常に警察が監視している

Q34 サイバー防犯訓練

正解： B

解説

ダークウェブには、通常の検索エンジンで検索することができないという特徴があります。そのため、個人情報を売買する場などとして悪用されています。非常に危険なので、絶対にアクセスしないようにしましょう！

Q35 サイバー防犯訓練

あなたの会社で個人情報の漏洩を防ぐルールを決めようとしています。次のうちどの案を採用するべき？

A お客さんのデータが入ったパソコンの持ち出し禁止

B お客さんのデータは必ず紙で持ち運ぶ

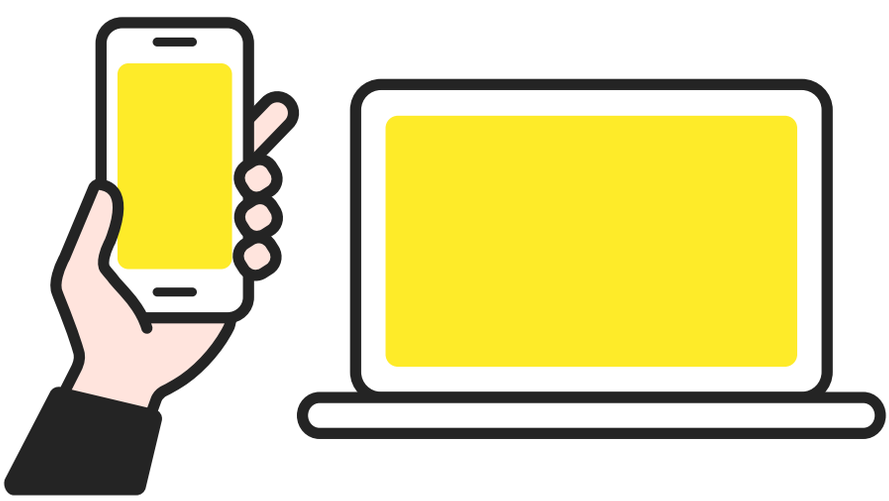
C データ紛失に備えて、複製ファイルを同じフォルダに保管

Q35 サイバー防犯訓練

正解： A

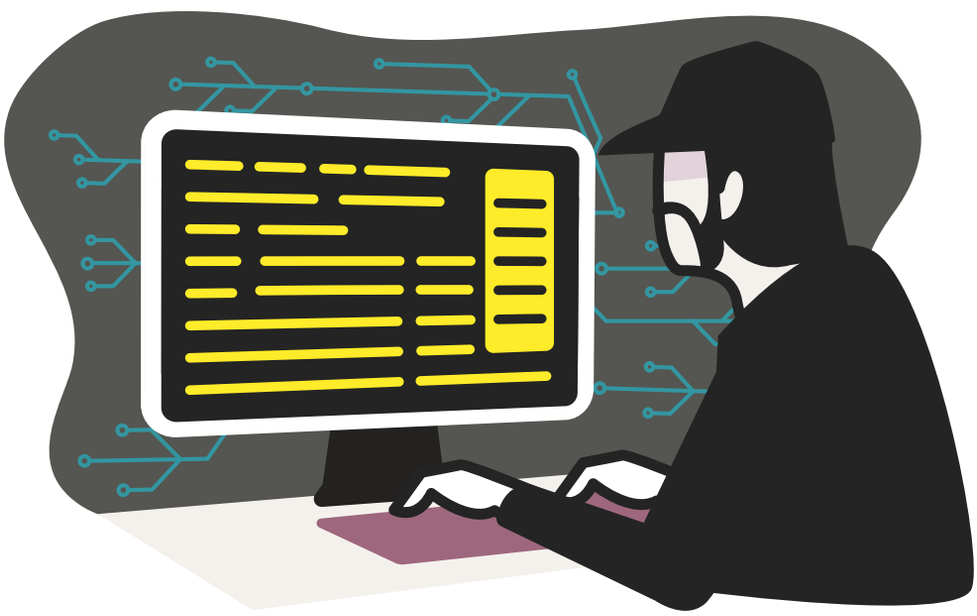
解説

業務上の個人情報漏えいの原因の一つに、人為的なミスが挙げられます。スマートフォンやノートパソコンを外部に持ち出すと、紛失や盗難による情報漏えいが発生するおそれがあります。持ち出しを禁止することが一番の情報漏えい対策となりますが、やむを得ず持ち出す場合は上長に相談するといったルールを決めることも大切です。



Q36 サイバー防犯訓練

一般の方法では閲覧できず、違法な取引の温床になっているウェブ領域を「○○ウェブ」という。○○に入る言葉は、次のうちどれ？



A ダーク

B ブラック

C ジャアク

Q36 サイバー防犯訓練

正解： A

解説

ダークウェブは、通常のブラウザでは検索することができず、情報の発信元を特定しづらいという特徴があります。そのため、個人情報を売買する場などとして悪用されています。犯罪に巻き込まれるリスクがあるため、絶対にアクセスしないようにしましょう。

Q37 サイバー防犯訓練

パソコンのログインパスワードを書いたメモ。どう処理するべき？

A 丸めてゴミ箱に捨てる

B シュレッダーにかけて処理する

C パソコンの近くに貼っておく

Q37 サイバー防犯訓練

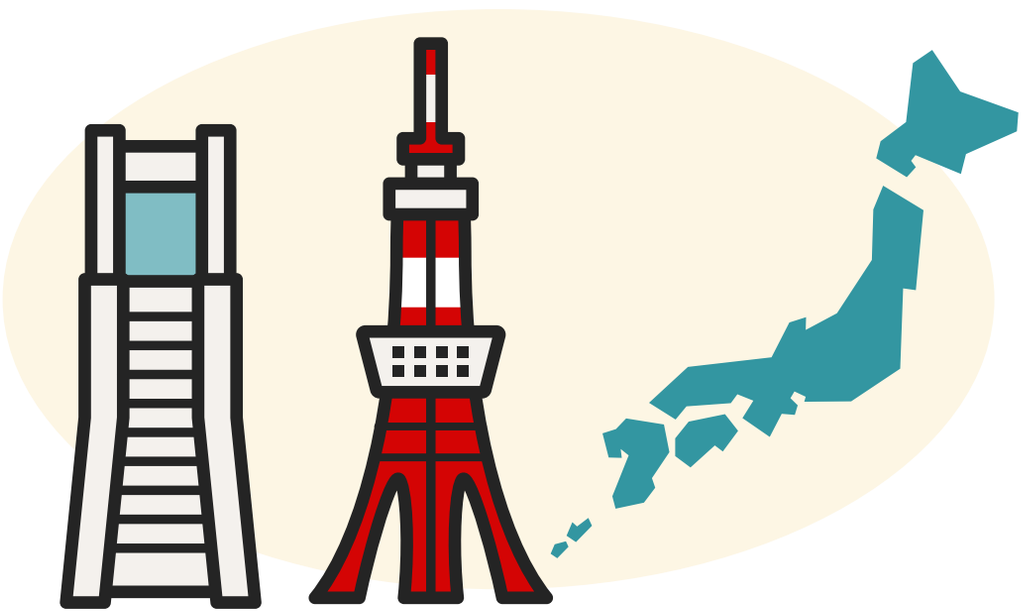
正解： B

解説

清掃員としてオフィスなどに侵入し、ごみ箱に捨てられた書類から情報を盗む「トラッシング」という手口の犯罪があります。パソコンのログインパスワードや機密情報などを記載した書類やメモは必ずシュレッダーにかけて処理し、対策しましょう。また、シュレッダーは時間をかければ復元されてしまう可能性もあるため、業者による溶解処理という選択肢もあります。

Q38 サイバー防犯訓練

[2012 年から 2021 年の 10 年間で、上場企業およびその子会社が公表した、個人情報の漏洩数] に最も近いのは次のうちどれ？



A 横浜市の人口に相当する、約 380 万人分

B 東京都の人口に相当する、約 1400 万人分

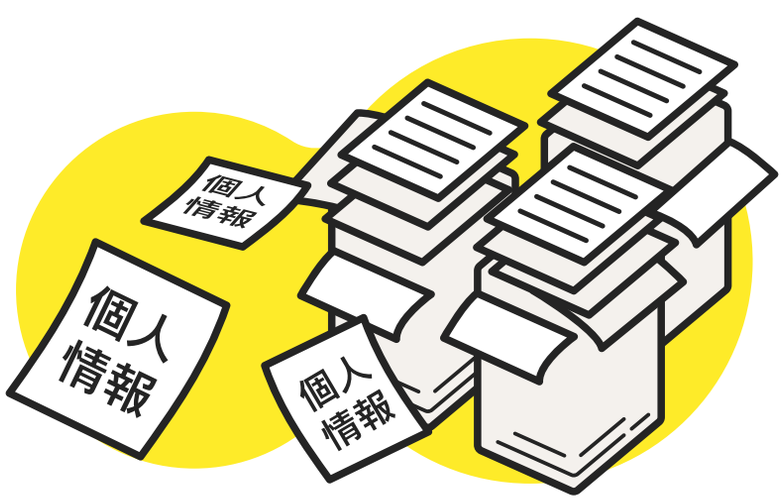
C 日本の人口に相当する約 1 億 2000 万人分

Q38 サイバー防犯訓練

正解： C

解説

総務省の統計局によると、2012 年から 2021 年での累計で、上場企業およびその子会社で個人情報の漏えい・紛失事故を公表したのは、496 社・925 件で、全上場企業の 1 割以上を占めています。漏えい・紛失した可能性のある個人情報は累計 1 億 1979 万人分に達し、これは日本の総人口 1 億 2475 万人に迫る数字です。



Q39 サイバー防犯訓練

あなたがフリー Wi-Fi に接続するとき、少しでもセキュリティを上げる方法は、次のうちどれ？

A 通信の盗聴等を防ぐために「VPN」を活用する！

B 電波状態が最も良いフリー Wi-Fi を使う！

C 一番上に表示されたフリー Wi-Fi を使う！

Q39 サイバー防犯訓練

正解： A

解説

暗号化されていない Wi-Fi であっても、VPN というサービスを使うことによって暗号化をして、通信内容の覗き見を防ぐことができます。VPN とは Virtual Private Network の略で、日本語では仮想プライベートネットワークと訳されています。暗号化をすることで擬似的な専用線を作り、そこでデータをやり取りすることで、通信内容が守られるという仕組みです。

Q40 サイバー防犯訓練

友人に勧められたアプリをダウンロードすると、「マイク」「通話履歴」「連絡先」「電話」「位置情報」の権限許可を求められました。次のうち、正しい行動はどれ？

A 必要そうではない権限を許可しない

B アプリの機能を最大化するために全て許可

C 権限許可をしても危険な事はないので全て許可

Q40 サイバー防犯訓練

正解： A

解説

アプリの中には、実際の機能では使用しない情報にまでアクセスを求めるものもあります。悪質なアプリが、必要以上に情報を取得したり、認証情報や個人情報を詐取するケースもあるため、権限を許可する必要があるか、ひとつひとつ確認するようにしましょう。権限の変更は後からでもできます。

Q41 サイバー防犯訓練

知らない人と位置情報共有アプリを使いたいあなた。そのアプリにどんな機能が確認できたら、安全に使える？

A 身分証明書の登録機能

B 怪しいユーザーに対する通告機能

C 知らない人と安全にアプリを使う方法は無い

Q41 サイバー防犯訓練

正解： C

解説

位置情報を安易に教えてしまうと、ストーカーなどの被害に遭う可能性があります。実際に位置情報が悪用された事件も発生しています。位置情報を共有するのは、家族や親しい友人に限るようにしましょう。

Q42 サイバー防犯訓練

あなたは出かけた先で入った ABC カフェで、①「abc_cafe guest」、②「ABC_Cafe Guest」の２つのフリー Wi-Fi を見つけました。①に接続したところネットが重かったため、②に接続し快適にネットを楽しみました。この行動の間違いは何？

A 最初から大文字の Wi-Fi を選ぶべきだった

B データ量の少ないネット利用をするべきだった

C どちらの Wi-Fi もお店のものだと思い接続した

Q42 サイバー防犯訓練

正解： C

解説

正規の Wi-Fi と名前を似せた「なりすまし Wi-Fi」に注意しましょう。これに接続すると、偽サイトに誘導されて個人情報を盗まれたり、通信内容を傍受されたりする危険性があります。Wi-Fi に接続する際は、ネットワーク名 (SSID) が正規のものかをよく確認しましょう。また、稀に正規の Wi-Fi と全く同じ名前の悪質な Wi-Fi が存在します。残念ながら、端末は名前が同じであれば正規の Wi-Fi と悪質な Wi-Fi を見分けることができません。公共 Wi-Fi にはこのようなリスクがあると認識し、重要な作業などを行うのは避けましょう。通信内容を暗号化する VPN アプリなどを利用し、情報を保護して Wi-Fi を利用するのも有効な手段です。

Q43 サイバー防犯訓練

スマホに表示される Wi-Fi のアクセスポイントのうち、「安全性が低い Wi-Fi」にはどのようなメッセージが表示される？

A 「安全性の低いセキュリティ」

B 「危険なネットワーク」

C 「推奨しない Wi-Fi」

Q43 サイバー防犯訓練

正解： A

解説

Wi-Fi にはいくつかのセキュリティ認証方式があり、それぞれに異なる暗号化技術が使われています。「WEP」と「WPA」の暗号化技術は、セキュリティが低いものです。「WPA3」は最もセキュリティが高く分類されています。スマホで WEP や WPA の Wi-Fi を表示するときには、自動的に「安全性の低いセキュリティ」と表示されるようになっています。これが表示された Wi-Fi は、使わないほうがより安全といえます。

Q44 サイバー防犯訓練

新しいアプリをダウンロードをしている二人のうち、どちらが正しい行動？

A 公式アプリは絶対安全！即ダウンロード！

B アプリ説明欄を読んでからダウンロード！

Q44 サイバー防犯訓練

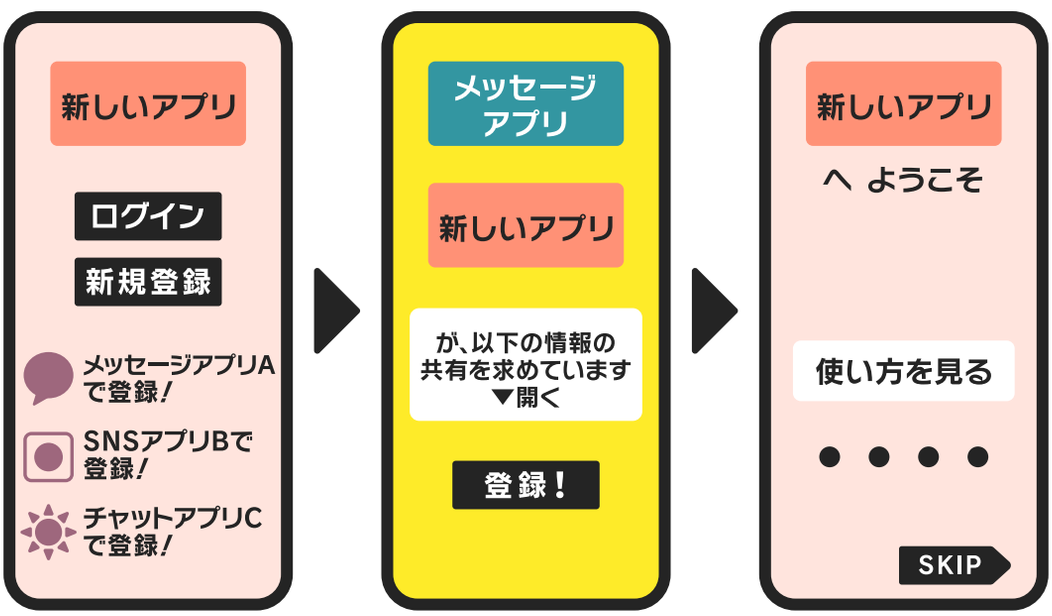
正解： B

解説

公式のアプリストアは、アプリストア以外からのダウンロードと比べれば安全性が高いですが、悪意を持った人が作成したアプリが掲載されている可能性もあります。アプリをダウンロードする前に、評価や提供者の情報、アプリの説明などをよく確認することが重要です。また、ネット検索で口コミを調べたり、セキュリティソフトでアプリの安全性を診断したりすることも有効です。アプリがアクセス権限を求めるデータについても確認するようにし、スマホ内の不要なアプリは早めにアンインストールするようにしましょう。

Q45 サイバー防犯訓練

SNS を他のアプリと連携させるとき、どこに気をつけるべき？



A 連携アプリの人気度合を確認する！

B 連携アプリがアクセスできる情報の範囲に気を付ける！

C 気を付けるところは特にない！

Q45 サイバー防犯訓練

正解： B

解説

アプリ連携をするときに、本人のプロフィール情報だけでなく、繋がっている友達のリストやその連絡先などの情報が提供されることがあります。その情報を本当に開示してもいいのかをよく確認してから連携の登録をするようにしましょう。登録の際に、アプリが参照できる情報を確認できる画面が出た場合は、チェックが入っている情報をよく確認しましょう。