問題発生カードの解説

問題発生カード	ア　本物のメール！？
	取り引きのある銀行から「【重要】口座利用の確認について」という件名のメールが届いた。件名に【重要】と記載があったので急いで手続きをしないといけないと考え、メールの中にある「ご利用確認はこちら」というリンクを押してインターネットバンキングにログインし、利用状況を確認した。 １問目　この後どんなことが起こるでしょうか？ ２問目　どうすれば防ぐことができたでしょうか？
回答例	１問目　○IDやパスワードが盗まれ、口座を乗っ取られる ○不正送金される ○個人情報を悪用される ○さらにフィッシングメールが増える ２問目　○メール内のリンクは押さず、公式サイトや公式アプリからログインして確認する ○メールの差出人やURLが本物かどうか確認する ○銀行に対して確認する
解説	このケースは、銀行を騙る「フィッシングメール」の典型的な手口です。 「【重要】」「【至急】」などの強い言葉で利用者を焦らせ、メール内のリンクを押させるのが特徴です。 リンク先には、本物の銀行サイトに似せた偽サイトが用意されており、そこで入力したIDやパスワードが攻撃者に盗まれます。 盗まれた情報を不正利用され、不正ログイン、不正送金、口座の乗っ取りが発生する恐れがあります。 また、フィッシングメールは銀行だけではありません。 公的機関や市役所、証券会社やクレジットカード会社、又は業者、大手通販サイトなど様々な組織を装って届きます。「普段利用している会社からだから大丈夫」「公的機関からだから大丈夫」という思い込みは危険です。 公式サイトや公式アプリを参考にしながら、届いたメールが本物かどうか判断しましょう。 安易にメール内のリンクは押さないということも大切です。

問題発生カード	# イ　パスワードの大切さ
	ネットゲームでなかなかクリアできないステージがあり、ゲーム内で仲良くなった人から、「代わりにクリアしてあげるからあなたのIDとパスワードを教えて」と言われた。 どうしてもそのステージをクリアしたかったのでIDとパスワードを教えた。 １問目　この後どんなことが起こるでしょうか？ ２問目　どうすれば防ぐことができたでしょうか？
回答例	１問目　〇アカウントを乗っ取られる ○ゲーム内のアイテムや通貨が盗まれる ○登録しているクレジットカードを不正利用される ２問目　○どんな相手でもIDとパスワードは教えない ○ゲームの攻略は公式サポート等を利用する
解説	オンラインゲームのIDとパスワードを他人に教えてしまうと、他人があなたのゲームにログインし、乗っ取られる可能性があります。 ゲーム内で仲良くなった相手にIDやパスワードを渡すと、相手はアカウントを自由に操作できるようになるため、アイテムやゲーム内の通貨を盗まれるかもしれません。 また、パスワードを変更されてログインできなくなる可能性もあります。 さらに、アカウントを削除されたり、売買されてしまう可能性もあります。 オンラインゲームだけではありません。 ＳＮＳやその他ログインが必要なサイトなどでも同じです。 パスワードはあなたの情報を守る大切な鍵です。 どんなに甘い誘いを受けても、人に教えてはいけません。 逆に他人のID・パスワードを勝手に使ってログインしたり、他人のパスワードを勝手に別の人に教えたりすることは、不正アクセス禁止法違反に抵触することがあります。

問題発生カード	## ウ　返金手続きのはずが‥
	通販サイトで気になる商品を購入した。 後日、欠品のため電子マネーで返金手続きをするというお知らせが届き、サイト管理者の指示通りにコード決済アプリを操作した。 １問目　この後どんなことが起こるでしょうか？ ２問目　インターネットで買い物をする際、注意すべきことはなんでしょうか？
回答例	１問目　〇　返金を受けられない ○　さらに、電子マネーをだまし取られる ２問目　○　ECサイトが詐欺サイトではないか ○　返金手続きでチャットアプリに誘導されないか ○　「○○Payで返金する」と言われていないか
解説	SNS上には詐欺サイトが多数存在します。「極端に値段が安い」や、「どのお店でも在庫切れで手に入らない人気商品が多数販売されている」などの怪しいサイトには注意しましょう。 そのようなサイトで商品を購入してしまい、「商品が届かなかった」という相談が多数寄せられています。 また、「商品が届かなかったから、サイト事業者へ問い合わせたところ、チャットアプリ等へ誘導され、『○○Pay（コード決済アプリ）で返金します』と言われ、コード決済アプリを操作したところ、お金を送金してしまった」という返金詐欺の被害も多数寄せられています。 コード決済アプリで返金を受ける際、基本的に受ける側はアプリを操作する必要はありません。 「○○Payで返金します」と言われたら詐欺を疑いましょう。

問題発生カード	エ　闇バイト…？
	副業の広告をクリックすると、メールが届いた。 「自分の口座に入金されたお金を指定された別の口座に移し替えるだけで報酬金がもらえる」という簡単な仕事だったので、その仕事を始めた。 １問目　この後、どんなことが起こるでしょうか？ ２問目　気をつけるべきポイントはなんでしょうか？
回答例	１問目　〇　犯罪に加担してしまう ○　口座が凍結されて使えなくなる ○　個人情報をもとに脅される ２問目　○　「簡単に稼げる」という言葉は疑う ○　個人情報を安易に送信しない
解説	問題の「自分の口座に入金されたお金を、指定された別の口座に移し替える」という仕事は、犯罪で得たお金を移動させる役割である可能性が高く、犯罪に加担することになってしまいます。 このような副業は「簡単」「すぐ稼げる」「ホワイトバイト」などという言葉で人を引きつけますが、いわゆる闇バイトであり、正規の仕事ではありません。 一度でも関わってしまうと、犯人グループから抜けられなくなったり、警察から事情を聞かれたり、口座が凍結されてしまうことがあります。 「知らなかった」「騙された」という理由でも責任を問われる場合があります。 簡単に稼げる仕事はありません。

問題発生カード	# オ　その情報、本物？
	地震があり、SNSを見ていると救助を求める投稿を見つけた。自分は救助に行けないが困っている人を助けたいと考え、その投稿を拡散したが、後日、拡散した情報は偽情報だったと判明した。 １問目　偽情報を拡散したときどんなことが起こるでしょうか？ ２問目　確認すべきポイントはなんでしょうか？
回答例	１問目　〇　偽情報が広がり混乱を招く ○　本当に困っている人や救助活動の妨げになる ○　偽情報を流したとして信用を失う ２問目　○　情報の出所（信頼できる機関か） ○　矛盾や不自然な点はないか
解説	災害時や事件などのニュースはSNSで情報がすぐに広がります。 しかし、中には偽情報が含まれています。 善意で拡散しても、それが偽情報だと、混乱を招いたり、本当に困っている人の救助の妨げになる可能性があります。 偽情報を流したことで信頼を失ってしまわないように、情報を見つけたときは ・　公的機関などの信頼できる情報か ・　複数の情報源があるか ・　不自然な点はないか 等を確認するようにしましょう。

問題発生カード	# カ　ウイルス感染！？
	パソコンでインターネットを閲覧中、いきなり大音量で警告音が鳴り響きウイルスに感染したと警告メッセージが出た。画面上にサポートセンターの電話番号が表示されていたので電話をかけた。 １問目　この後、どんなことが起こるでしょうか？ ２問目　警告メッセージが表示された場合にとるべき行動はなんでしょうか？
回答例	１問目　〇　遠隔操作される ○　個人情報が盗まれる ○　インターネットバンキングで不正送金される ○　盗撮や盗聴をされる ○　高額請求される ２問目　○　電話をかけない ○　画面を閉じる ○　セキュリティソフトでウイルススキャンする
解説	ウイルスに感染したという警告画面は、テクニカルサポート詐欺という詐欺です。 慌てて電話をかけたり、リンクをクリックすると ・　高額請求される ・　個人情報やパスワードを盗まれる ・　端末に不正プログラムを入れられる というような被害につながります。 正しい行動は「落ち着いて対応すること」です。 公式のセキュリティソフトやOSのサポート等で確認し、怪しい指示には従わないようにしましょう。

問題発生カード	キ　乗っ取られている？
	SNSのフォロワーから「インフルエンサーになるために私に投票して欲しい」というメッセージが届き、携帯電話番号やメールアドレスを教えて欲しいと言われたので教えた。 その後、SMS（ショートメッセージサービス）で届いた認証コードを教えて欲しいと言われたため認証コードも送信した。 １問目　この後、どんなことが起こるでしょうか？ ２問目　どうすれば防ぐことができたでしょうか？
回答例	１問目　〇　自分のSNSアカウントが乗っ取られる ○　フォロワーに同じ詐欺メッセージが送信される ○　ログインできなくなる ２問目　○　認証コードは絶対に送らない ○　友達が乗っ取られている可能性を考える
解説	SNSで届く「投票して欲しい」「応援して欲しい」というメッセージの中には、アカウントを乗っ取ることが目的とされている詐欺があります。 電話番号やメールアドレスを教えると、SMSやメールで認証コードが送られてきます。 この認証コードは、本人であることを確認するための大切な情報です。 どんな理由があっても、人に教えてはいけません。 認証コードを他人に教えてしまうと、相手はあなたになりすましてログインでき、SNSアカウントを自由に操作できるようになります。 あなたになりすました犯人は、あなたのアカウントを使ってフォロワーに詐欺メッセージを送るなど、被害がさらに広がることになります。

問題発生カード	## ク　本当に儲かる？投資テクニック
	「絶対に儲かる投資テクニック」の広告をクリックしたところ、投資勉強グループの一員になることができた。勧められたアプリをダウンロードして投資を始めることにした。 １問目　この後、どんなことが起こるでしょうか？ ２問目　気をつけるべきポイントはなんでしょうか？
回答例	１問目　〇　投資資金すべてがなくなる ○　個人情報や口座情報が盗まれる ２問目　○　「絶対に儲かる」「簡単に稼げる」などという言葉に騙されない ○　個人情報や口座情報は容易に教えない
解説	「絶対に儲かる」などという広告は、SNS型投資詐欺です。 勉強グループに誘導され、成功報告をたくさん見かけるかもしれませんが、すべて偽物です。 投資を始めると、最初は少し儲かるかもしれませんが、それも、あなたを信頼させるための罠です。 結局、多額の投資金をだまし取られてしまいます。 お金だけではありません。 勉強グループやアプリを通じて ・　個人情報を不正利用する ・　不正な投資に誘導する など被害につながります。 絶対に儲かる投資はありません。 投資には必ずリスクがあります。

問題発生カード	# ケ　将来を約束？
	私のSNSの投稿を見た人から「気が合いそう！友達になりたい」とダイレクトメッセージが届いた。 やりとりを続けるうちに恋愛感情が生まれ、結婚の話が出るなかで、「二人の将来のために投資をしよう」と言われたので、お金を振り込んだ。 １問目　この後、どんなことが起こるでしょうか？ ２問目　気をつけるべきポイントはなんでしょうか？
回答例	１問目　〇　金銭をだまし取られる ○　相手とは連絡がつかなくなる ２問目　○　実際に会ったことがない人からお金の話をされたら詐欺を疑う ○　個人情報や口座情報は容易に教えない
解説	SNSやマッチングアプリなどを通じて知り合い、実際に会うことなくやりとりを続けることで恋愛感情や親近感を抱いてしまい、金銭をだまし取られる「SNS型ロマンス詐欺」です。 今はSNS上に公開された写真や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、あなたをだましているかもしれません。 会ったことのない相手から、 ・　2人の将来のために投資をしよう ・　必ずもうかる ・　会いたいに行きたい、二人で旅行に行きたいので飛行機代を送ってほしい などと言われたら、要注意。 お金を振り込む前に警察や家族等に相談しましょう。

問題発生カード	コ　上司からの指示！？
	社長から「SNSグループを作成してQRコードを送るように」とメールが届いた。 言われたとおりSNSでグループを作りQRコードを送ると、「当社の口座残高のスクリーンショットを送るように」「指定する口座にお金を振り分けるように」と言われたので、指示に従った。 １問目　この後どんなことが起こるでしょうか？ ２問目　どうすれば防ぐことができたでしょうか？
回答例	１問目　○不正な送金要求でお金をだまし取られる ２問目　○送信元にメール以外の方法で確認する ○メールの添付ファイルやリンク先を不用意に開かない ○ビジネスメール詐欺が発生していることを組織内外で情報共有する
解説	これは取引先や自社の経営者等になりすまして、偽の電子メールを送って送金を促す「ビジネスメール詐欺」です。 振込先は海外の銀行口座を指定されることが多く、一旦海外に送金してしまうと、回収することは非常に困難です。 このようなメールが届いたときは、送信元に電話等、メール以外の方法で確認すること、特に「送金」「至急」のメールを受理した場合は、メールに記載されている内容に不自然なところがないかよく確認しましょう。 また日ごろからウイルス対策ソフト、OSを最新の状態にする、メールの添付ファイルやリンク先を不用意に開かないなど、基本的な対策もしっかりしましょう。