# 問題発生カード

回答できたらボーナス 100pt

【Q1】取引先の課長から「現在私は休暇中なのですが、弊社側の振込先口座が変更になったので、至急お金を振り込んでください」というメールが来た。その課長のいつものアドレスじゃなかったけれども、納品代 10 万円分だったので、出張中の当社の課長には相談せずすぐに対応した。

[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。

# 問題発生カード

回答できたらボーナス 100pt

【Q2】宿泊業を営んでいる弊社のフロント宛に、1 ヶ月後に宿泊する予定だというお客様から、「私は特定の洗剤に対するアレルギーがあります。詳しくはこちらのサイトをご確認ください。」というメールと URL が送られてきた。情報を得るためにこの URL を開いて確認した。

[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。

# Q1 解説

これは、**ビジネスメール詐欺(BEC)**の例です。課長を名乗るアドレスは偽物です。先方のメールの指示通りにお金を振り込んだ場合は、その後課長を名乗るアドレスから「入金がない。振込先が間違っているのではないか」などの連絡が追加で届き、さらに金銭を要求されることがあります。時代の変化でこれまでの支払いの常識が異なるケースもあり、だまされやすいのです。

『セキュリティ五箇条』では、**【一】、【四】、【五】**に当てはまります。メールの内容が不審な場合は、電話など別の手段を利用して確認するとともに、上司・同僚にも報告・相談をしましょう。また、このような被害事例も組織内で共有しておくと安心できます。

# Q2 解説

これは、**ホテルを狙った標的型攻撃**の例です。指示されたURLを開くとホテル側のPCがマルウェアに感染し、ホテル予約サイトで利用するログイン情報が盗まれます。次に、その情報を使って、犯人がホテルになりすまし、予約サイトの利用者に偽サイトへの誘導メッセージを送ります。その偽サイトを利用して、クレジットカード情報を盗み出します。

『セキュリティ五箇条』では、**【一】、【二】、【四】、【五】**に当てはまります。被害事例を組織内で共有し、組織として相談体制を作ることに加え、OSやアプリを常にアップデートしておき、ウィルス感染にも備えましょう。

# 問題発生カード

回答できたらボーナス 100pt

【Q３】SNS のダイレクトメッセージで知り合いから「アンバサダーに立候補したので投票して」と連絡が来たので「いいよ」と返信した。携帯電話番号を聞かれたので送信したら、ショートメッセージで“投票リンク”が送られた。それを SNS ダイレクトメッセージに貼り付けてと指示されたので、その通りにした。

[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。

# 問題発生カード

回答できたらボーナス 100pt

【Q４】「【重要】カード利用に関するお知らせ」というタイトルのメールで、カード会社からカードの不正検知システムにより決済が停止しているので、カードの利用確認を行なっていると連絡があり、次の URL をクリックするように言われた。問題なさそうだったのでクリックした。 https://www.creditcard.co.jp/e-navi/

[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。

# Q３解説

これは、**SNS アカウントの不正アクセス**に遭遇する攻撃の例です。ショートメッセージに送られた URL は、SNS のあなたのアカウントに対する正規のパスワードリセット専用リンク先です。この URL を相手に送ると、あなたの SNS アカウントのパスワードが強制的に変更され、不正アクセス被害に遭います。ダイレクトメッセージを送ってきた相手も別人のなりすましだと思われます。

『セキュリティ五箇条』では、**【一】、【四】、【五】**に当てはまります。このような被害事例も組織内で共有し、急な抽選や投票のような連絡は常に疑い、確認するように心がけましょう。

# Q４解説

これは、**クレジットカード会社からの連絡を装ったフィッシング詐欺攻撃**の例です。URL も正式なカード会社からのように見せかけた偽物です。リンクを押すと、クレジットカード会社の偽サイトに誘導され、ID やパスワード、クレジットカード番号などの情報を入力するよう求められます。また不正なアプリをインストールするように要求するものもあります。

『セキュリティ五箇条』では、**【一】、【三】、【四】、【五】**に当てはまります。リンクをクリックする前に、その会社が本当にそのような案内を出しているかを直接調べるようにしましょう。また、パスワードの使いまわしは厳禁ですよ！！

# 問題発生カード

回答できたらボーナス 100pt

【Q5】パソコンで資料を作ろうと検索をしていたら、突然画面が変わって激しい音が鳴った。パソコンがウィルスに感染したと表示されたので、表示されたサポート番号に電話をした。


[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。


# 問題発生カード

回答できたらボーナス 100pt


【Q6】会社のホームページをデザイン会社にお願いして新しいデザインのものに変更した。その際、新着ニュースなどを当社の事務員が更新できるようにしてもらった。デザイン会社からは「定期的にシステムのアップデートをしてください」と言われたけれども、よくわからないのでやっていない。


[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。

# Q5 解説

これは、**PC サポート詐欺**に遭遇する攻撃の例です。電話をすると担当者を名乗る人物から指示があり、その通りに操作すると PC を犯人側が遠隔操作して、PC 内の個人情報などを盗みます。インターネットバンキングを経由してお金を盗むこともあります。また、電子マネーの購入を何度も要求することもあります。絶対に電話をして相手の要求に従ってはいけません。

『セキュリティ五箇条』では、**【一】、【二】、【五】**に当てはまります。このような被害事例を組織内で共有するとともに、相談先を確認しておきましょう！

近くの警察署もしくは#9110へ電話

IPA 相談窓口 03-5978-7509 へ電話

# Q6 解説

これは、**ホームページの改ざんの被害にあってしまう可能性のある行動**の例です。ホームページを更新する体制を整える際に、セキュリティに関する対策をとっておかないと簡単に犯罪者によって改ざんが実施されてしまいます。また、ホームページを動かしているサーバやアプリなどのアップデートを行わないと、不正アクセスの被害に遭いやすくなります。

『セキュリティ五箇条』では、**【一】、【二】、【三】、【五】**に当てはまります。ホームページは会社の顔です。犯罪者に攻撃されないように、セキュリティ対策はしっかりと実施しましょう。パスワードの管理や OS やシステムのアップデートも忘れずに！！

# 問題発生カード

回答できたらボーナス 100pt

【Q7】業務が長引いたので、業務用パソコンを持ったまま直帰する許可を得た。帰宅途中に友人と居酒屋で飲んだら酔ってしまい、公園のベンチで３時間ぐらい居眠りした。気づいたら鞄がなかった。慌てて辺りを探したら少し離れたところに鞄があったのでそのまま鞄を持って帰宅した。もちろん会社には報告していない。

[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。

# 問題発生カード

回答できたらボーナス 100pt

【Q8】事務職員のＡ子さんがお父さんの介護と仕事を両立したいと相談してきたので、在宅勤務を認めた。Ａ子さんが自宅のパソコンでも仕事ができるように、社内のサーバをアクセスできるサービスを使いたかったけれども予算がないと言われたので、仕方なく社内で保有する顧客名簿を USB メモリで渡した。

[問 1] このあとどうなると思いますか？

[問 2]『セキュリティ五箇条』のどれに当てはまるかを考えてみてください。

# Q7 解説

これは、**個人情報の漏えいに結びつく可能性のある行動**の例です。PC が入った鞄が見つかったから大丈夫と考えるのは早計で、すでに PC から個人情報が抜き取られたあとかもしれません。万が一、個人情報が漏えいした場合は、組織は関係部署に届出をする義務が発生します。自分のミスであっても必ず組織に報告をして、情報が保管されているかの確認を行いましょう。

『セキュリティ五箇条』では、**【一】、【二】、【三】、【五】**に当てはまります。個人情報の保管については組織のルールに従うとともに、万が一このようなミスが発生しても大丈夫なように、パスワードをつけ、暗号化するなどの措置をすることをお勧めします。

# Q8 解説

これは、**在宅勤務時のサイバー攻撃被害に結びつく可能性のある行動**の例です。在宅勤務で利用する PC のセキュリティ対策が弱いと、手渡した顧客名簿が漏えいする危険があります。

『セキュリティ五箇条』では、**【一】、【二】、【三】、【四】【五】**に当てはまります。在宅勤務の場合は通常のセキュリティ対策以上にしっかりと対策を行うことが大切です。パスワードの管理や OS やシステムのアップデートを行い、メールへの注意も必要です。

万が一、このようなミスが発生しても大丈夫なように、顧客名簿にはパスワードをつけ、暗号化するなどの措置を実施しておきましょう！