名前: 日付: 得点:

# オンライン詐欺とソーシャルエンジニアリング 保護ガイド

メールのフィッシング、なりすましドメイン、ビッシング、サポート詐欺、別経路での確認、BEC

## オンライン詐欺の学習概要

**保護済み**
データ暗号化
256 ビット AES 標準

**準拠**
世界標準
GDPR と CCPA の枠組み

**ゼロトラスト**
アクセスポリシー
多要素認証

**ようこそ！** このアクティビティ資料では、オンライン詐欺対策について学びます。偽のフィッシングサイト、ソーシャルエンジニアリングの手口、サポート詐欺、送金詐欺の経路、支払いの確認方法を取り上げます。

ワークシートのチェックポイント

- [ ] パート 1-4: サイバーセキュリティと脅威の防止を習得します。
- [ ] パート 5-7: クロスワードと単語探しのパズルを解きます。
- [ ] パート 8-9: ケーススタディと暗号チャレンジを解きます。
- [ ] パート 10: 基礎と応用の FAQ ページを確認します。
- [ ] パート 11: 実世界の興味深い事実10選を調べます。
- [ ] ボーナス: すばやく考えよう チャレンジ

VPN.com のサイバーセキュリティガイドを開く

URL: https://www.vpn.com/cybersecurity/online-scams/

# あなたのオンライン詐欺対策 学習ロードマップ

- サポート詐欺とタイポスクワッティングのドメインによくある兆候を見分ける。
- なりすましに対抗するため、メール認証プロトコル (SPF、DKIM、DMARC) を導入する。
- 企業の電信詐欺を防ぐため、別経路での取引確認を確立します。

### オンライン詐欺ガイドの手順

多肢選択問題と正誤問題に答え、語群を使って穴埋め文を完成させ、定義を結び付け、クロスワードと単語探しパズルを解いてください。学んだ知識をオンライン詐欺対策に応用しましょう。 最後にボーナス活動「すばやく考えよう」に取り組みましょう。

### オンライン詐欺とソーシャルエンジニアリング対策（導入）

オンライン詐欺は、フィッシング、サポートを装うポップアップ、ビッシング、送金詐欺などを通じて人間の行動につけ込みます。帯域外での取引確認と SPF/DKIM/DMARC のドメインルールを徹底すると、ゲートウェイでソーシャルエンジニアリングの手口を防ぎやすくなります。

**各チェックポイントをよく読んで、正しいものを選ぶか書いてください。**

## チェックポイント 1: 多肢選択チャレンジ

1. 1. サポート詐欺の主な兆候は何ですか?
   - A. システムが感染したと主張し、電話番号へかけるよう要求するポップアップ
   - B. 公式レジストリからダウンロードされた自動セキュリティ更新
   - C. 企業ドメインで認証情報の入力を拒否するパスワードマネージャー
   - D. 外付けドライブ構成で実行されるバックグラウンドのファイルバックアップ

2. 2. 銀行の情報を盗むために、偽の送信者ドメインを使う手口はどれですか?
   - A. メールフィッシング
   - B. ポートスキャン
   - C. メモリインジェクション
   - D. 暗号的消去

3. 3. 振込詐欺に当たるものは何ですか?
   - A. ソーシャルエンジニアリングを使い、被害者をだまして偽の企業口座に送金させる
   - B. ランサムウェアのペイロードを使ってシステムデータベースを暗号化すること
   - C. SQL インジェクションのコマンドでデータベースに問い合わせること
   - D. システムファイルをオフラインのストレージディスクにバックアップすること

4. 4. 詐欺師が偽のショッピングサイトを作るのはなぜですか?
   - A. 買い手のクレジットカード情報と決済の認証情報を盗むため
   - B. サンドボックス化されたマルウェア分析用のデータベーステーブルをホストするため
   - C. オンライン注文の配送を早めるため
   - D. 新しいウェブサイトのデザインを無料でテストするため

5. 5. ビッシングとはどういう意味ですか?
   - A. 電話網を通じて認証情報を盗む、音声によるフィッシング詐欺
   - B. ローカルネットワークをスキャンして保護されていないシステムデバイスを探すこと
   - C. 不正アクセスの後にシステムデータベースを復元すること
   - D. 信頼できないコードを安全な仮想コンテナ内で実行すること

# チェックポイント 2: 正しい・誤りチャレンジ

### 6 質問 6

6. フィッシング詐欺はエンドユーザーだけを狙い、経営幹部を狙うホエーリングの標的にはなりません。

◯ 正しい ◯ 誤り

### 7 質問 7

7. なりすましのドメインは、信頼できるブランドに似せるために、わずかなタイプミス (amaz0n.com など) を使うことがよくあります。

◯ 正しい ◯ 誤り

### 8 質問 8

8. サポート詐欺は、電話をかけてきた相手にリモートアクセスを許可すれば解決できます。

◯ 正しい ◯ 誤り

### 9 質問 9

9. ソーシャルエンジニアリングは、恐怖や緊急性といった人間の心理を悪用して、セキュリティのルールを回避します。

◯ 正しい ◯ 誤り

### 10 質問 10

10. 送金依頼は、常に別の連絡手段(アウトオブバンド)で確認する必要があります。

◯ 正しい ◯ 誤り

## チェックポイント 3: 重要用語の穴埋め

以下の各文を読み、空欄にワードバンクから正しい用語を入れてください。

1. 利用者をだます不正なメールは _____ と呼ばれます。
2. 信頼できるブランドを装ったウェブアドレスは、 _____ されたものです。
3. 銀行口座の情報を狙う音声通話の詐欺は _____ と呼ばれます。
4. ウイルス除去の代金を要求するポップアップは、サポート _____ です。
5. 支払い依頼を確かめるには、別経路での _____ が必要です。
6. 企業の取引を泥棒の口座へ振り向けるのは、 _____ 詐欺です。

**用語バンク**

スミッシング　ビッシング　フィッシング　ホエーリング　確認　偽装　詐欺　送金

**ここに答えを書いてください:**

1. 
2. 
3. 
4. 
5. 
6. 

# チェックポイント 4: セキュリティの概念マッチング

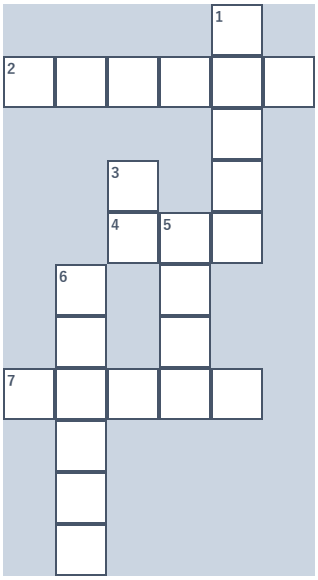
**定義マッチング**

左の各用語を、入力欄に対応する文字（A〜H）を入力して、右の正しい定義と組み合わせてください。

| | | | |
|---|---|---|---|
| ☐ | 1. フィッシング | A | 銀行取引を犯罪者の口座へ不正に振り向けること。 |
| ☐ | 2. なりすまし済み | B | 被害者から金銭やログイン情報を盗むために仕組まれた詐欺の手口。 |
| ☐ | 3. ビッシング | C | モバイルアカウントの認証情報を盗むために、詐欺のテキストメッセージを送ること。 |
| ☐ | 4. 詐欺 | D | 認証情報とアカウントの詳細を盗むために仕組まれた不正な音声通話。 |
| ☐ | 5. 検証 | E | C レベルの経営幹部から認証情報を盗むことを狙った、標的型フィッシング攻撃。 |
| ☐ | 6. 有線 | F | 正規に見せかけた、偽装されたメール送信者またはウェブサイトのアドレス。 |
| ☐ | 7. ホエーリング | G | ログイン情報とパスワードを盗むために仕組まれた不正なメールキャンペーン。 |
| ☐ | 8. スミッシング | H | 信頼できる別の連絡手段を使って支払い情報を確認すること。 |

## チェックポイント 5: クロスワードパズル

有効な白いマスに文字を入力して、クロスワードパズルを解いてください。数字は下のカギに対応しています。




### ヨコのカギ

**2. 経営幹部の認証情報を盗むことを狙った標的型のフィッシング攻撃 (6)**

**4. 正規に見せかけた、なりすましのメール送信元やウェブサイトのアドレス (3)**

**7. 認証情報や口座の詳細を盗むための不正な音声通話 (5)**

### タテのカギ

**1. ログイン情報や口座の詳細を確かめて、本人かどうかを判断すること (5)**

**3. 被害者から金銭やログイン情報を盗むための不正な計画 (2)**

**5. 銀行取引を犯罪者の口座へ不正に振り向けること (4)**

**6. ログイン情報やパスワードを盗むために仕組まれた不正なメールの攻撃 (6)**

# チェックポイント 5 代替活動: アクセシブルなクロスワードのヒント

スクリーンリーダーやキーボードを使うユーザーは、下の入力欄にクロスワードの答えを直接入力できます。

## ヨコのカギ

**2 ヨコ: 経営幹部の認証情報を盗むことを狙った標的型のフィッシング攻撃 (6 文字):**

**4 ヨコ: 正規に見せかけた、なりすましのメール送信元やウェブサイトのアドレス (3 文字):**

**7 ヨコ: 認証情報や口座の詳細を盗むための不正な音声通話 (5 文字):**

## タテのカギ

**1 タテ: ログイン情報や口座の詳細を確かめて、本人かどうかを判断すること (5 文字):**

**3 タテ: 被害者から金銭やログイン情報を盗むための不正な計画 (2 文字):**

**5 タテ: 銀行取引を犯罪者の口座へ不正に振り向けること (4 文字):**

**6 タテ: ログイン情報やパスワードを盗むために仕組まれた不正なメールの攻撃 (6 文字):**

## チェックポイント 6: 隠れた単語さがし

下のグリッドに隠れている8つの重要な用語を見つけてください。単語は横、縦、斜めに並んでいます。

ウ ソ ビ ス ト ブ ジ ピ ザ サ ミ ル リ ヘ ツ
ロ ウ ミ エ ズ コ ウ グ ソ フ ル ト ー コ シ
ウ ヨ ヤ ト ヌ ザ ヤ セ ヨ ウ セ ロ ヒ サ オ
ゲ シ ポ イ ツ ハ ゾ ネ ヌ ポ キ ラ ゲ バ ウ
ン ン ヒ シ ヒ フ ベ メ ペ ロ ボ ン タ レ ミ
ク ニ グ ヌ チ イ ユ ビ ガ メ ロ サ ギ ボ ワ
ラ キ ゼ ゴ ザ ツ ス ホ ツ ノ オ ア オ キ ル
パ ホ ヒ パ ヘ シ ボ ズ フ シ サ ン メ ハ コ
ン ヌ ヤ モ ヘ ン ワ レ テ モ ン モ ン ギ ゲ
ニ ズ ジ ツ カ グ ゴ ワ ラ ニ グ グ カ バ コ
ク ホ エ ー リ ン グ ザ ペ ダ キ ポ バ タ ギ
カ フ ト ー コ モ サ ガ ベ レ カ ゾ エ ソ ア
ー ユ コ ヘ イ サ ラ サ ソ テ ヌ コ ウ ギ ン
メ ス ヌ グ ポ ゴ ソ ガ ド セ イ イ ガ リ ヤ
レ ズ ボ ワ ヒ グ ゼ ゲ ケ ヤ プ オ タ グ ベ

**用語リスト**

フイツシング　ギソウ　ビツシング　サギ　カクニン　ソウキン　ホエーリング　ニンショウ

# チェックポイント 6 代替活動: アクセシブルな用語マッチング

ワードサーチの 8 つの用語を、空欄に文字（A〜H）を書いて、正しい定義と組み合わせてください。

| 用語 |
| --- |
| A. フイツシング |
| B. ギソウ |
| C. ビツシング |
| D. サギ |
| E. カクニン |
| F. ソウキン |
| G. ホエーリング |
| H. ニンシヨウ |

| 定義とマッチ欄 |
| --- |
| 1. 正規に見せかけた、なりすましのメール送信元やウェブサイトのアドレス。 |
| 2. 信頼できる別の連絡手段で支払いの詳細を確かめること。 |
| 3. 銀行取引を犯罪者の口座へ不正に振り向けること。 |
| 4. ログイン情報や口座の詳細を確かめて、本人かどうかを判断すること。 |
| 5. 経営幹部の認証情報を盗むことを狙った標的型のフィッシング攻撃。 |
| 6. 認証情報や口座の詳細を盗むための不正な音声通話。 |
| 7. ログイン情報やパスワードを盗むために仕組まれた不正なメールの攻撃。 |
| 8. 被害者から金銭やログイン情報を盗むための不正な計画。 |

## チェックポイント 7: 並べ替え単語チャレンジ

下の文字を並べ替えて、サイバーセキュリティの重要な概念と用語を見つけましょう。答えは用意された入力欄に書いてください。

1. ツフシングイ
2. ビグンシツ
3. ンカニク
4. グリーンホエ
5. ウソギ
6. ギサ
7. キソンウ
8. ウニシヨン

# ボーナス活動: すばやく考えよう

それぞれのカテゴリーで答えを 3 つ書きましょう。最初にリストを埋めた人の勝ちです。

| | | | | |
|---|---|---|---|---|
| 1 | ハッキングされるおそれのあるデバイス | | | |
| 2 | 詐欺師がよく使うフレーズ | | | |
| 3 | 詐欺師が要求する支払い方法 | | | |
| 4 | オンライン詐欺の種類 | | | |
| 5 | 話がうますぎるオファー | | | |
| 6 | 詐欺を報告できる場所 | | | |
| 7 | サイバーセキュリティに関連する言葉 | | | |
| 8 | 詐欺について注意を促せる人 | | | |
| 9 | バックアップするもの | | | |
| 10 | メールの危険なサイン | | | |
| 11 | コンピューターが感染しているサイン | | | |
| 12 | オンラインショップを確認する方法 | | | |
| 13 | アカウントを守る方法 | | | |
| 14 | 詐欺に遭ったときにすること | | | |
| 15 | データが漏えいした後にすること | | | |

# チェックポイント 8: サイバーセキュリティのケーススタディ

学んだ概念を応用して、以下の実際のシナリオを解いてみましょう。

## ケーススタディ 1: 企業を狙う送金詐欺の防止



**シナリオ:** 経理部門が、なりすましのベンダーのアドレスから、今後の請求書の送金先を新しい口座番号にするよう求める緊急のメールを受け取ります。

**ディスカッションの問い:** 送金詐欺の確認ポリシーを概説し、メール認証による防御策を示せますか？

## ケーススタディ 2: 経営幹部を狙うホエーリング型フィッシング事件



**シナリオ:** 経営幹部が、安全な取締役会の資料があると称するフィッシングリンクをクリックし、偽のポータルに自分の主要な社内認証情報を入力してしまいました。

**ディスカッションの問い:** インシデント対応の手順を詳しく説明し、経営幹部のログインを監査する方法を説明できますか？

## チェックポイント 9: 暗号を解読しよう

サイバーセキュリティの専門家は、ネットワーク資産をオンラインの脅威アクターから守ります。下の文字と数字の対応表を使い、対応する文字を空欄に書いて、メッセージを解読してください。

**文字から数字への暗号鍵**

ア=1 イ=2 ウ=3 エ=4 オ=5 カ=6 キ=7 ク=8 ケ=9 コ=10 サ=11 シ=12

ス=13 セ=14 ソ=15 タ=16 チ=17 ツ=18 テ=19 ト=20 ナ=21 ニ=22 ヌ=23 ネ=24

ノ=25 ハ=26 ヒ=27 フ=28 ヘ=29 ホ=30 マ=31 ミ=32 ム=33 メ=34 モ=35 ヤ=36

ユ=37 ヨ=38 ラ=39 リ=40 ル=41 レ=42 ロ=43 ワ=44 ヲ=45 ン=46 ガ=47 ギ=48

グ=49 ゲ=50 ゴ=51 ザ=52 ジ=53 ズ=54 ゼ=55 ゾ=56 ダ=57 ヂ=58 ヅ=59 デ=60

ド=61 バ=62 ビ=63 ブ=64 ベ=65 ボ=66 パ=67 ピ=68 プ=69 ペ=70 ポ=71 ー=72

| 28 | 2 | 18 | 12 | 46 | 49 | 45 |  | 6 | 8 | 22 | 46 | 12 | 19 |  | 32 | 23 | 8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | |

**解読したメッセージ:**

ヒント: 各数字は、上の暗号鍵のカタカナ 1 文字を表します。

# チェックポイント 10: サイバーセキュリティ FAQ – 基礎 (パート A)

オンラインの脅威への対策に関するよくある質問と回答を確認しましょう。

### Q1: オンライン詐欺とは何ですか?

デジタルチャネルを使い、被害者をだましてお金を送らせたり、個人の認証情報を渡させたりする詐欺の手口。

### Q2: メールのフィッシングの主な兆候は何ですか?

緊急性(アカウント停止など)を装い、公式ドメインと一致しないリンクへ誘導するメッセージ。

### Q3: タイポスクワッティングとは何ですか?

人気ブランドのよくあるタイプミスのドメイン (amaz0n.com など) を登録して、偽のフィッシングサイトを運営すること。

### Q4: サポート詐欺とは何ですか?

PCがウイルスに感染したと主張し、電話番号へかけさせて、偽のクリーンアップソフトやリモートアクセスサービスの代金を払わせようとするポップアップ。 [1]

### Q5: ビッシングとは何ですか?

音声電話を使って、被害者に銀行口座やログインの情報を教えるよう仕向けるフィッシング攻撃。

# チェックポイント 10: サイバーセキュリティ FAQ – 基礎 (パート B)

オンラインの脅威への対策に関するよくある質問と回答を確認しましょう。

### Q6: 電信詐欺とはどういう意味ですか?

取引先や経営幹部になりすまして、支払い取引を詐欺用の口座に誘導すること。

### Q7: ホエーリングとは何ですか?

C-levelの企業幹部のような価値の高いターゲットを直接狙う、きわめて標的を絞ったスピアフィッシング。

### Q8: スミッシングとは何ですか?

モバイルデバイスに送られる詐欺のテキストメッセージで、偽のポータルや配送状況の更新へのリンクを促すもの。

### Q9: 帯域外の確認が重要なのはなぜですか?

侵害されたメールのやり取りを避けて、別の通信手段(電話など)で取引の詳細を確認します。

### Q10: 偽のエスクロー詐欺はどのような仕組みですか?

詐欺師は偽のエスクローサイトを作り、資金は安全に保管されると主張して、買い手が振り込んだ代金を盗みます。

# チェックポイント 10: セキュリティ FAQ – 応用 (パート C)

セキュリティフレームワーク、マルウェア分析、データコンプライアンスについて、高度な技術的側面を探ります。

### Q1: 詐欺師は BEC（ビジネスメール詐欺）をどのように使って送金詐欺を実行しますか?

正規の従業員のメールアカウントを乗っ取り、請求書のやり取りを監視して、詐欺用の銀行口座を記載した更新済みの請求先情報を送ります。

### Q2: オンライン詐欺における IDN ホモグラフ攻撃のリスクは何ですか?

通常の文字と見分けがつかないASCII以外の文字(キリル文字の' a 'など)を使い、本物のブランドをまねた偽のドメインを登録すること。

### Q3: 詐欺の検出でメールヘッダーの確認が重要なのはなぜですか?

実際の送信元サーバーの IP と SPF/DKIM の検証状況を明らかにし、送信者のドメインが偽造されているかどうかを示します。

### Q4: サポート詐欺師はリモートデスクトップソフトをどう悪用しますか?

AnyDeskやTeamViewerなどのユーティリティを使って被害者のデバイスに接続し、マルウェアを仕込んで、保存されたパスワードを盗みます。

### Q5: 前払い手数料詐欺の目的は何ですか?

存在しない高額の報酬と引き換えに、先に手数料を支払うよう被害者をだますこと。

# チェックポイント 10: セキュリティ FAQ – 応用 (パート D)

セキュリティフレームワーク、マルウェア分析、データコンプライアンスについて、高度な技術的側面を探ります。

### Q6: 詐欺師はソーシャルメディアのプロファイリングを標的型フィッシングにどう利用しますか?

企業の組織構造や従業員の名前を集め、説得力のある標的型フィッシングメールを作成します。

### Q7: 偽のネットショップが大幅な割引を提示するのはなぜですか?

買い手をだましてクレジットカードの詳細を入力させ、カード不正のフォーラムで再利用や転売をするために認証情報を盗むため。

### Q8: DMARC レコードはフィッシング詐欺をどう防ぎますか?

DMARCを使うと、ドメイン所有者は、SPFとDKIMの整合性チェックに失敗したメールを隔離または拒否するよう受信側に求めることができ、直接的ななりすましを防げます。 [5]

### Q9: 認証情報収集ポータルの脅威とは何ですか?

Microsoft 365 や Google ワークスペースにそっくりに作られた偽のランディングページで、入力された認証情報を盗みます。

### Q10: セキュリティチームは、詐欺ドメインをどのように報告し、無効化しますか?

詐欺の証拠を、レジストラの不正報告用メール、ホスティングプロバイダー、Google Safe Browsingのレジストリに提出することによって。

# パート 11: 実世界のサイバーセキュリティの事実10選と洞察

セキュリティ侵害、防御の仕組み、コンプライアンス基準に関する実際の事実を確認しましょう。

**1. セキュリティの洞察**

2025年、フィッシングとなりすましは FBI の IC3 に最も多く報告された犯罪の種類で、191,561件の届け出がありました。 [2]

**2. セキュリティの洞察**

ビジネスメール詐欺（BEC）は、2025年にFBIのIC3へ報告された損失が$3 billionを超えました。 [2]

**3. セキュリティの洞察**

タイポスクワットされたドメインは、本物のブランド名と1、2文字しか違わないため、ざっと見ただけでは見落とされることがあります。

**4. セキュリティの洞察**

2025年に FBI の IC3 に報告された、テクニカルサポート詐欺による被害額は 21 億ドルを超えました。 [2]

**5. セキュリティの洞察**

ホモグラフ攻撃は、ブラウザーがピュニコードの表記を表示しない限り、ブラウザーのアドレスバーでは同一に見えます。

**6. セキュリティの洞察**

SMS のテキスト詐欺 (スミッシング) は、リンク付きの短く緊急性のあるメッセージを使い、被害者が詐欺に気づくための手がかりをほとんど与えません。

**7. セキュリティの豆知識**

ホエーリング攻撃は、高額の送金を承認する権限を持つため、経営幹部のメールを狙います。

**8. セキュリティの豆知識**

既知の保存済みの電話番号に電話して支払い先の変更を確認することは、BEC(ビジネスメール詐欺)による送金詐欺への重要な防御策です。

**9. セキュリティの豆知識**

偽のエスクローサイトは、オンラインマーケットプレイスでよくある詐欺です。安全な決済サービスに見えますが、買い手の電信送金をだまし取ります。

**10. セキュリティの洞察**

Google セーフブラウジングは、フィッシングやマルウェアの疑いがあるとして警告対象にしたサイトを開く前に、ユーザーに警告します。

# 技術参考資料と出典

この学習ガイドとインタラクティブなパズルは、世界のNIST、OWASP、およびデータプライバシー・コンプライアンスの標準をもとに作成されています。

## 学術・業界の参考資料

[1] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.
https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).
https://www.rfc-editor.org/rfc/rfc7489.html

## 解答: チェックポイント 1 – 多肢選択

**1 問題 1** 正解: A

### 指導メモ

サポート詐欺の主な兆候は何ですか? → システムが感染したと主張し、電話番号へかけるよう要求するポップアップ

**2 問題 2** 正解: A

### 指導メモ

銀行の情報を盗むために、偽の送信者ドメインを使う手口はどれですか? → メールフィッシング

**3 問題 3** 正解: A

### 指導メモ

振込詐欺に当たるものは何ですか? → ソーシャルエンジニアリングを使い、被害者をだまして偽の企業口座に送金させる

**4 問題 4** 正解: A

### 指導メモ

詐欺師が偽のショッピングサイトを作るのはなぜですか? → 買い手のクレジットカード情報と決済の認証情報を盗むため

**5 問題 5** 正解: A

### 指導メモ

ビッシングとはどういう意味ですか? → 電話網を通じて認証情報を盗む、音声によるフィッシング詐欺

## 解答: チェックポイント 2 – 正誤問題

### 6 問題 6

正解: 誤り

#### 指導メモ

誤り: フィッシングは経営幹部も標的にします。ホエーリングは、上級幹部を狙ったフィッシングです。

### 7 問題 7

正解: 正しい

#### 指導メモ

なりすましのドメインは、信頼できるブランドに似せるために、わずかなタイプミス (amaz0n.com など) を使うことがよくあります。

### 8 問題 8

正解: 誤り

#### 指導メモ

誤り: サポート詐欺の犯人にリモートアクセスを許すと、マルウェアを仕込まれ、データを盗まれる可能性があります。

### 9 問題 9

正解: 正しい

#### 指導メモ

ソーシャルエンジニアリングは、恐怖や緊急性といった人間の心理を悪用して、セキュリティのルールを回避します。

### 10 問題 10

正解: 正しい

#### 指導メモ

送金依頼は、常に別の連絡手段(アウトオブバンド)で確認する必要があります。

# 用語解答と採点基準

**教師用採点基準: 正しい組み合わせ 1 つにつき 1 点(合計 8 点)、文脈の用語 1 つにつき 1 点(合計 6 点)を与えてください。**

## チェックポイント 4: 解答 – 概念マッチング

| | | | |
|---|---|---|---|
| G 1. フィッシング | F 2. なりすまし済み | D 3. ビッシング | B 4. 詐欺 |
| H 5. 検証 | A 6. 有線 | E 7. ホエーリング | C 8. スミッシング |

## チェックポイント 3: 解答 – 重要用語

| | | | |
|---|---|---|---|
| 1 フィッシング | 2 偽装 | 3 ビッシング | 4 詐欺 |
| 5 確認 | 6 送金 | | |

## チェックポイント 6 代替活動: 解答 – 用語マッチング

| | | | |
|---|---|---|---|
| 1 B – ギゾウ | 2 E – カクニン | 3 F – ソウキン | 4 H – ニンシヨウ |
| 5 G – ホエーリング | 6 C – ビツシング | 7 A – フイツシング | 8 D – サギ |

### 指導者向けディスカッションメモ

**重要用語:**
生徒がフィッシング、なりすまし済み、ビッシングを自分の言葉で説明し、それぞれの例を挙げられるか確認してください。

**ケーススタディ:**
生徒には、意見ではなくワークシートの事実を根拠に提案するよう促してください。

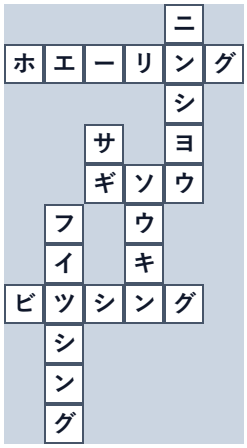
**情報源の評価:**
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

# パズルの解答と指導者用メモ

## ワードサーチの解答

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ウ | ソ | ビ | ス | ト | ブ | ジ | ピ | ザ | サ | ミ | ル | リ | ヘ | ツ |
| ロ | ウ | ミ | エ | ズ | コ | ウ | グ | ソ | フ | ル | ト | ー | コ | シ |
| ウ | ヨ | ヤ | ト | ヌ | ザ | ヤ | セ | ヨ | ウ | セ | ロ | ヒ | サ | オ |
| ゲ | シ | ポ | イ | ツ | ハ | ゾ | ネ | ヌ | ポ | キ | ラ | ゲ | バ | ウ |
| ン | ン | ヒ | シ | ヒ | フ | ベ | メ | ペ | ロ | ボ | ン | タ | レ | ミ |
| ク | ニ | グ | ヌ | チ | イ | ユ | ビ | ガ | メ | ロ | サ | ギ | ボ | ワ |
| ラ | キ | ゼ | ゴ | ザ | ツ | ス | ホ | ツ | ノ | オ | ア | オ | キ | ル |
| パ | ホ | ヒ | パ | ヘ | シ | ボ | ズ | フ | シ | サ | ン | メ | ハ | コ |
| ン | ヌ | ヤ | モ | ヘ | ン | ワ | レ | テ | モ | ン | モ | ン | ギ | ゲ |
| ニ | ズ | ジ | ツ | カ | グ | ゴ | ワ | ラ | ニ | グ | グ | カ | バ | コ |
| ク | ホ | エ | ー | リ | ン | グ | ザ | ペ | ダ | キ | ポ | バ | タ | ギ |
| カ | フ | ト | ー | コ | モ | サ | ガ | ベ | レ | カ | ゾ | エ | ソ | ア |
| ー | ユ | コ | ヘ | イ | サ | ラ | サ | ソ | テ | ヌ | コ | ウ | ギ | ン |
| メ | ス | ヌ | グ | ポ | ゴ | ソ | ガ | ド | セ | イ | イ | ガ | リ | ヤ |
| レ | ズ | ボ | ワ | ヒ | グ | ゼ | ゲ | ケ | ヤ | プ | オ | タ | グ | ベ |

## クロスワードの解答




## クロスワード解答の教師用ガイド

### ヨコのカギ

**2 ヨコ: ホエーリング** 経営幹部の認証情報を盗むことを狙った標的型のフィッシング攻撃 (6 文字)

**4 ヨコ: ギソウ** 正規に見せかけた、なりすましのメール送信元やウェブサイトのアドレス (3 文字)

**7 ヨコ: ビツシング** 認証情報や口座の詳細を盗むための不正な音声通話 (5 文字)

### タテのカギ

**1 タテ: ニンショウ** ログイン情報や口座の詳細を確かめて、本人かどうかを判断すること (5 文字)

**3 タテ: サギ** 被害者から金銭やログイン情報を盗むための不正な計画 (2 文字)

**5 タテ: ソウキン** 銀行取引を犯罪者の口座へ不正に振り向けること (4 文字)

**6 タテ: フイツシング** ログイン情報やパスワードを盗むために仕組まれた不正なメールの攻撃 (6 文字)

# 文字並べ替えと暗号解読の解答

単語の並べ替え活動と「秘密の暗号チャレンジ」の採点用の解答。

## 文字並べ替えの解答

1. ツフシングイ — **フイツシング**
2. ビグンシツ — **ビツシング**
3. ンカニク — **カクニン**
4. グリーンホエ — **ホエーリング**
5. ウソギ — **ギソウ**
6. ギサ — **サギ**
7. キソンウ — **ソウキン**
8. ウニシヨン — **ニンシヨウ**

### 秘密の暗号チャレンジ 解答

**"フィッシングヲ カクニンシテ ミヌク"**

# ケーススタディの解答

## A ケーススタディ 1: 企業を狙う送金詐欺の防止

教師用解答

### 採点ガイドライン

**学生の解答には、次の点を含めてください:**

- シナリオ分析: 経理部門が、なりすまされた取引先のアドレスから、今後の請求書の振込先を新しい送金先番号に変更するよう求める緊急のメールを受け取ります。
- 推奨される戦略と解決策: すべての支払いに二重承認ポリシーを適用します。あらかじめ保存した電話番号を使った別経路での確認を実施し、なりすましドメインからのメールをゲートウェイでブロックします。

## B ケーススタディ 2: 経営幹部を狙うホエーリング型フィッシング事件

教師用解答

### 採点ガイドライン

**学生の解答には、次の点を含めてください:**

- シナリオ分析: ある役員が、安全な取締役会資料があると称するフィッシングリンクをクリックし、偽のポータルに自分の主要な社内認証情報を入力してしまいました。
- 推奨される戦略と解決策: 役員のデバイスを隔離します。社内のすべてのセッショントークンと認証情報をリセットします。アクセスログでデータの持ち出しを確認し、すべてのログインにハードウェア MFA を導入します。