名前: 日付: 得点:

フィッシング攻撃とソーシャルエンジニアリング

スピアフィッシング、ホエーリング詐欺、SPF/DKIM/DMARC プロトコル、送信者のなりすまし、従業員のセキュリティ研修。

フィッシング攻撃の学習概要

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、フィッシング攻撃とソーシャルエンジニアリングについて学びます。スピアフィッシング、ホエーリング、ドメインのなりすまし、SPF/DKIM/DMARCプロトコル、リンクの安全性、従業員の意識向上トレーニングを取り上げます。

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/phishing-attacks/

あなたのフィッシング対策 学習ロードマップ

- よくあるフィッシング、ビッシング、サポート偽装ポップアップ詐欺を見分ける。
- 帯域外での取引確認の手順を導入する。
- なりすましドメインをブロックするため、SPF、DKIM、DMARC のルールを設定してください。

フィッシング攻撃ガイドの手順

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。学んだ知識をメール認証に応用しましょう。 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。

フィッシング攻撃とソーシャルエンジニアリング（導入）

フィッシング攻撃は、標的型メッセージ、ホエーリング詐欺、ドメインのなりすましを使ってユーザーのログイン認証情報を収集します。企業システムを守るには、帯域外の承認手順に加えて、ゲートウェイに SPF、DKIM、DMARC のルールを導入する必要があります。

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. スピアフィッシングとは何ですか?
   - A. 特定の個人や組織に合わせて作り込まれた標的型フィッシングメール
   - B. ランダムな数百万のアドレスに送られる大量の一括メール
   - C. ウェブサーバーにトラフィックを大量に送りつけるネットワーク攻撃
   - D. ユーザーレコードを狙ったデータベース抽出の手法

2. 2. なりすましを防ぐため、DNSで許可された送信元IPアドレスをドメインが一覧で公開できるようにするプロトコルはどれですか？
   - A. SPF
   - B. DKIM
   - C. DMARC
   - D. HTTPS

3. 3. ホエーリング攻撃とは何ですか?
   - A. 著名な企業幹部を特に狙ったフィッシングキャンペーン
   - B. データベースのバックアップを狙うSQLインジェクション攻撃
   - C. ローカルエリアネットワークのルーター機器の物理的な盗難
   - D. 自動化されたクレデンシャルスタッフィングによる総当たりスキャン

4. 4. DKIMは何をしますか?
   - A. 送信者の真正性を確認するために、メールに暗号署名を付加する
   - B. ファイアウォールで受信ネットワークパケットのトラフィックをブロックする
   - C. 保存時にデータベースのストレージボリュームを暗号化する
   - D. メールの添付ファイルをスキャンして、シグネチャ型のマルウェアを検出する

5. 5. DMARCの役割は何ですか?
   - A. SPF/DKIMのチェックに失敗した場合の扱いを、受信側メールサーバーに指示する
   - B. 事前計算されたレインボーテーブルを使ってシステムパスワードを復号すること
   - C. 配信前にメールの添付ファイルを圧縮すること
   - D. ネットワークルーティングのアクセス権限を設定すること

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. スピアフィッシングは、無作為の数百万のアドレスに送信される一般的な大量メールに依存しています。

○ 正しい　○ 誤り

7 質問 7

7. DMARCポリシーは、許可されていないなりすましメッセージを拒否するようメールサーバーに指示できます。

○ 正しい　○ 誤り

8 質問 8

8. SPF の検証は、メール本文の暗号署名を検証することで機能する。

○ 正しい　○ 誤り

9 質問 9

9. ホエーリング攻撃は、データベースファイルにアクセスするために、下位の企業管理者を狙います。

○ 正しい　○ 誤り

10 質問 10

10. 支払い依頼を別の経路で確認することは、送金詐欺の防止に役立ちます。

○ 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. 個人情報を使って特定の従業員を狙うのは、 _____ フィッシングです。

2. メッセージを正規のものに見せかけるためにメールヘッダーを偽造することは、送信者の _____ です。

3. 許可されたメールサーバーのIPアドレスを列挙したDNSレコードは _____ です。

4. 送信者を検証するための電子署名の標準は _____ です。

5. SPFやDKIMの検証に失敗したメールを拒否するポリシーを定めるには、 _____ を使います。

6. 経営幹部を狙うフィッシングキャンペーンは _____ と呼ばれます。

用語バンク

DKIM　DMARC　SPF　スピア　スプーフィング　ビッシング　フィッシング　ホエーリング

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

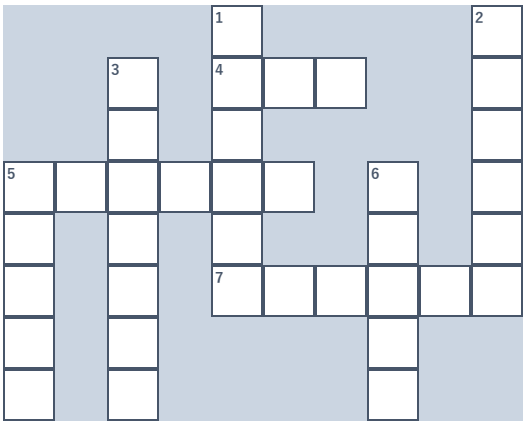
定義マッチング

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. スピア	A	音声による詐欺電話。
	2. なりすまし	B	C レベルの経営幹部を狙います。
	3. SPF	C	ポリシー拒否の指示。
	4. DKIM	D	DNSで認可された送信元IP。
	5. DMARC	E	ソーシャルエンジニアリングのメール。
	6. ホエーリング	F	個人宛てにカスタマイズされたメール。
	7. フィッシング	G	送信者のメールアドレスの偽装。
	8. ビッシング	H	メールにおける暗号署名。

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

4. 個人に合わせて作られた標的型のメール (3)

5. 認証に失敗したメールを拒否するよう指示するポリシー (6)

7. ソーシャルエンジニアリングを使ったメール (6)

タテのカギ

1. DNSで許可された送信元のIPアドレス (6)

2. 経営幹部を狙う攻撃 (6)

3. 送信者のメールアドレスを偽造すること (7)

5. メールに付けられる暗号による署名 (5)

6. 音声通話を使った詐欺 (5)

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

4 ヨコ: 個人に合わせて作られた標的型のメール (3 文字):

5 ヨコ: 認証に失敗したメールを拒否するよう指示するポリシー (6 文字):

7 ヨコ: ソーシャルエンジニアリングを使ったメール (6 文字):

タテのカギ

1 タテ: DNSで許可された送信元のIPアドレス (6 文字):

2 タテ: 経営幹部を狙う攻撃 (6 文字):

3 タテ: 送信者のメールアドレスを偽造すること (7 文字):

5 タテ: メールに付けられる暗号による署名 (5 文字):

6 タテ: 音声通話を使った詐欺 (5 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。

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

用語リスト

スピア　スプーフイング　エスピーエフ　デイーキム　デイーマーク　ホエーリング　フイツシング　ビツシング

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	定義とマッチ欄
A. スピア	1. 送信者のメールアドレスを偽造すること。
B. スプーフイング	2. 個人に合わせて作られた標的型のメール。
C. エスピーエフ	3. 音声通話を使った詐欺。
D. デイーキム	4. DNSで許可された送信元のIPアドレス。
E. デイーマーク	5. ソーシャルエンジニアリングを使ったメール。
F. ホエーリング	6. 認証に失敗したメールを拒否するよう指示するポリシー。
G. フイツシング	7. メールに付けられる暗号による署名。
H. ビツシング	8. 経営幹部を狙う攻撃。

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. ピアス
2. フエピエース
3. デーマクーイ
4. グシツンフイ
5. イグフースンプ
6. キデームイ
7. ンホリグーエ
8. グビシンツ

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	フィッシングメールのサイン			
3	コンピューターが感染しているサイン			
4	偽の緊急性を生み出す言葉			
5	送信者を確認する方法			
6	ITのサポートを頼める人			
7	バックアップするもの			
8	知っている魚や海の生き物			
9	詐欺師がなりすます企業			
10	今日から始められる安全な習慣			
11	偽のリンクをクリックした後にすること			
12	データが漏えいした後にすること			
13	フィッシングが起こるチャネル			
14	メールで決して送ってはいけないもの			
15	アカウントを守る方法			

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: 経営幹部を狙うホエーリング攻撃への対処



シナリオ: 最高財務責任者（CFO）が、CEOを名乗る高度にパーソナライズされたメールを受け取ります。機密のドメイン購入を完了するために、50,000ドルをすばやく送金するよう求める内容です。

ディスカッションの問い: ブランドのなりすましのリスクを分析し、SPF/DKIM/DMARCと認証の制御について詳しく説明できますか？

ケーススタディ 2: SPF/DKIM/DMARC ゲートウェイポリシーの導入



シナリオ: ある企業が、送信するマーケティングメールが頻繁にスパムとして判定され、ハッカーが同社のブランドドメインを積極的になりすましているため、セキュリティ監査に不合格になっています。

ディスカッションの問い: メールの真正性を検証するための技術的・管理的な制御を策定できますか？

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

34	72	41	60		15	72	12	36	41	4	46	53	22	1	40	46	49	45

32	36	64	41

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: フィッシングとは何ですか?

フィッシングは、犯罪者が不正なメッセージを送り、ユーザーをだまして機密データを共有させるソーシャルエンジニアリング攻撃です。

Q2: フィッシングとスピアフィッシングの違いは何ですか?

フィッシングは一般的な内容で広範なグループを狙い、スピアフィッシングはカスタマイズした詳細情報を使って特定の被害者を狙います。

Q3: ホエーリングとは何ですか?

ホエーリングは、管理権限を持つ著名な経営幹部を標的にした、高度に絞り込まれたフィッシング攻撃です。

Q4: メールのなりすましとは何ですか?

メールのなりすましとは、送信者アドレスを偽ったメールを作成し、受信者にその送信元を信頼させようとすることです。

Q5: SPF はなりすましをどう防ぎますか?

許可された送信元 IP アドレスの一覧を DNS で公開し、受信サーバーがメールの送信元を検証できるようにします。 [1]

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: DKIM とは何ですか?

DomainKeys Identified Mailは、メールヘッダーに暗号署名を追加し、ドメインが責任を負っていることと、メッセージが改ざんされていないことを証明します。

Q7: DMARC は何の略ですか?

Domain-based Message Authentication, Reporting, and Conformance。 [2]

Q8: DMARC ポリシーとは何ですか?

SPF/DKIMに失敗したメッセージをメールサーバーがどう扱うか(none、quarantine、reject)を指示するポリシー。 [2]

Q9: ビッシングとは何ですか?

ボイスフィッシング。攻撃者が不正な電話を使って、管理情報や金融情報を聞き出します。

Q10: リンクスキャナーはどのように役立ちますか?

受信したメールのリンクをスキャンして書き換え、クリックした時点で、リンク先のWebページの安全性を確認します。

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: ホモグラフ攻撃はどのような仕組みですか?

攻撃者は、正規のドメイン名に見た目が似た非ASCIIのUnicode文字を使ってドメイン名を登録し、本物のように見せかけます。

Q2: ピュニコード表記とは何ですか?

DNSで扱えるように、Unicodeのドメイン名を「xn--」で始まるASCII互換の文字列に変換するエンコーディング。

Q3: 'p=reject' が最も安全な DMARC の状態なのはなぜですか?

SMTP セッション中に DMARC(整合した SPF/DKIM)に失敗したメールを拒否するよう受信サーバーに求め、直接のなりすましを防ぎます。 [2]

Q4: 攻撃者はどのように SPF ルールを回避しますか?

類似ドメイン（タイポスクワッティング）を悪用するか、正規のサードパーティ製メールサービス上の乗っ取られたアカウントを使うことによって。

Q5: ビジネスメール詐欺(BEC)とは何ですか?

攻撃者がビジネスメールアカウントを乗っ取るかなりすまして、不正な支払いを承認させる企業向け詐欺。

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: 多要素認証はフィッシングをどう阻止しますか?

よく似たランディングページだけでは盗めない、2 つ目のトークン(ハードウェアキーなど)を必要とします。

Q7: 認証情報収集用のランディングページとは何ですか?

入力されたユーザー名、パスワード、MFAトークンをリアルタイムで盗み取るよう設計された、そっくりなログインポータル。

Q8: サブドメインハイジャックとは何ですか?

攻撃者が未使用のDNSサブドメインポインタを乗っ取り、信頼できる親ドメインのもとで悪意のあるフィッシングのランディングページをホストすること。

Q9: DKIM アラインメントのチェックはどう機能しますか?

'From' ヘッダーのドメインが、DKIM ヘッダーでメッセージに暗号的に署名したドメインと一致することを検証します。

Q10: メールゲートウェイの役割は何ですか?

受信メールのフィルタリング、リンクの監査、添付ファイルのサンドボックス化、SPF/DKIM/DMARC準拠の検証。

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。 [4]

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。 [4]

3. セキュリティの洞察

ホモグラフ攻撃は、キリル文字の見た目が似た文字を使って、ブラウザー上で完全一致のブランドドメインを視覚的に複製します。

4. セキュリティの洞察

「p=reject」の場合、ドメインは受信側に対し、認証に失敗したメールを迷惑メールとして保管せず、配信時に拒否するよう求めます。 [2]

5. セキュリティの洞察

CEOを狙うホエーリング攻撃では、機密性の高い合併やドメイン購入のための緊急の支払いを求めることがよくあります。

6. セキュリティの洞察

認証情報収集ポータルは本物のログインページをコピーするため、被害者はパスワードを攻撃者のフォームにそのまま入力してしまいます。

7. セキュリティの豆知識

CISA の共同フィッシング対策ガイダンスでは、DMARC、SPF、DKIM、フィッシング耐性のある MFA に加えて、ユーザー教育を行うことが推奨されています。 [3]

8. セキュリティの豆知識

SPF の評価は、DNS を照会する項目 10 個までに制限されており、上限を超えると 'permerror' の結果が返されます。 [1]

9. セキュリティの豆知識

FIDO2ハードウェアセキュリティキーは、認証情報を遠隔から盗み取る攻撃に対して、暗号技術に裏付けられた保護を提供します。

10. セキュリティの洞察

フィッシングは、攻撃者が組織に最初に侵入する最も一般的な方法の1つであり、そのため定期的な啓発トレーニングが有効な防御策になります。

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.
https://www.rfc-editor.org/rfc/rfc7208.html

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

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

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

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

スピアフィッシングとは何ですか? → 特定の個人や組織に合わせて作り込まれた標的型フィッシングメール

2 問題 2

正解: A

指導メモ

SPFは、ドメインが許可した送信元ホストをDNSで公開し、受信側がエンベロープ送信者を確認できるようにします。

3 問題 3

正解: A

指導メモ

ホエーリング攻撃とは何ですか? → 著名な企業幹部を特に狙ったフィッシングキャンペーン

4 問題 4

正解: A

指導メモ

DKIMは何をしますか? → 送信者の真正性を確認するために、メールに暗号署名を付加する

5 問題 5

正解: A

指導メモ

DMARCの役割は何ですか? → SPF/DKIMのチェックに失敗した場合の扱いを、受信側メールサーバーに指示する

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: スピアフィッシングは、一般的な大量のフィッシングとは異なり、特定の人物に合わせて作り込まれています。

7 問題 7

正解: 正しい

指導メモ

DMARCポリシーは、許可されていないなりすましメッセージを拒否するようメールサーバーに指示できます。

8 問題 8

正解: 誤り

指導メモ

誤り: SPFは送信元IPをDNSと照合します。暗号署名を検証するのはDKIMです。

9 問題 9

正解: 誤り

指導メモ

誤り: ホエーリングは、支払いを承認でき、機密データにアクセスできる上級幹部を狙います。

10 問題 10

正解: 正しい

指導メモ

正しい: 支払い依頼を別の既知の経路で確認することは、送金詐欺の防止に役立ちます。

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

F 1. スピア	G 2. なりすまし	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. ホエーリング	E 7. フィッシング	A 8. ビッシング

チェックポイント 3: 解答 – 重要用語

1 スピア	2 スプーフィング	3 SPF	4 DKIM
5 DMARC	6 ホエーリング		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 B – スプーフイング	2 A – スピア	3 H – ビツシング	4 C – エスピーエフ
5 G – フイツシング	6 E – デイーマーク	7 D – デイーキム	8 F – ホエーリング

指導者向けディスカッションメモ

重要用語:
生徒がスピア、なりすまし、SPF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。

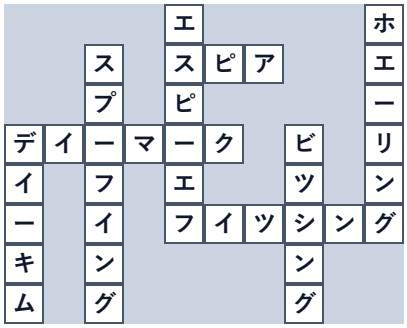
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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

4 ヨコ: スピア 個人に合わせて作られた標的型のメール (3 文字)

5 ヨコ: デイーマーク 認証に失敗したメールを拒否するよう指示するポリシー (6 文字)

7 ヨコ: フイツシング ソーシャルエンジニアリングを使ったメール (6 文字)

タテのカギ

1 タテ: エスピーエフ DNSで許可された送信元のIPアドレス (6 文字)

2 タテ: ホエーリング 経営幹部を狙う攻撃 (6 文字)

3 タテ: スプーフイング 送信者のメールアドレスを偽造すること (7 文字)

5 タテ: デイーキム メールに付けられる暗号による署名 (5 文字)

6 タテ: ビツシング 音声通話を使った詐欺 (5 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. ピアス — スピア
2. フエピエース — エスピーエフ
3. デーマクーイ — デイーマーク
4. グシツンフイ — フイツシング
5. イグフースンプ — スプーフイング
6. キデームイ — デイーキム
7. ンホリグーエ — ホエーリング
8. グビシンツ — ビツシング

秘密の暗号チャレンジ 解答

"メールデ ソーシャルエンジニアリングヲ ミヤブル"

ケーススタディの解答

A ケーススタディ 1: 経営幹部を狙うホエーリング攻撃への対処 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: 最高財務責任者 (CFO) が、CEO を名乗る非常に個人に合わせたメールを受け取ります。機密のドメイン購入を完了させるため、至急 50,000 ドルを送金するよう求める内容です。
- 推奨される対策と解決策: なりすまされた送信元ドメインをブロックするために、DMARC を 'p=reject' ポリシーで構成します。ゲートウェイに外部送信者の警告バナーを追加し、すべての金融取引について口頭による帯域外の確認を必須にします。

B ケーススタディ 2: SPF/DKIM/DMARC ゲートウェイポリシーの導入 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: ある企業は、送信するマーケティングメールが頻繁に迷惑メールと判定され、ハッカーが自社のブランドドメインを積極的になりすましているため、セキュリティ監査に不合格となっています。
- 推奨される戦略と解決策: 許可された送信元 IP を記載した SPF 用の TXT レコードを公開します。送信メールサーバーに DKIM 署名鍵を設定し、受信した DMARC の XML フィードバックレポートを分析して不正使用を特定します。