名前: 日付: 得点:

個人情報の盗難防止と資産セキュリティガイド

認証情報の漏えい、MFA、ダークウェブの監視、クレジットフリーズの通知、ソーシャルエンジニアリング

個人情報の盗難防止の学習概要

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、個人情報の盗難の防止と軽減について学びます。認証情報の漏えい、多要素認証、ダークウェブの監視、クレジットフリーズのアラート、ソーシャルエンジニアリング対策を取り上げます。

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/identity-theft/

あなたのID保護 学習ロードマップ

- ダークウェブのフォーラムでの認証情報の露出リスクを理解する。
- 多要素認証 (MFA) と、クレジットフリーズの通知を導入する。
- 標的型ソーシャルエンジニアリング詐欺に対する、企業のセキュリティ防御を設計します。

個人情報の盗難ガイドの説明

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ID保護に応用しましょう。 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。

個人情報の盗難防止と資産のセキュリティ（導入）

個人情報の盗難は、漏えいした認証情報や弱いログインを悪用して、個人や企業のアカウントを乗っ取ります。MFA、クレジットフリーズ、ダークウェブスキャナー、SPF/DKIM/DMARC の枠組みを導入することは、デジタルなりすましに対する重要な防御となります。

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. ID窃盗犯がログイン認証情報を盗むのに使う主な手口は何ですか?
   - A. 偽のメール通知を送り、ユーザーをだまして偽装されたポータルでパスワードを入力させる
   - B. ユーザーの会社のオフィス付近でラジオ放送を聞くこと
   - C. ユーザーのローカルサーバーストレージドライブをデフラグすること
   - D. 外部ネットワークのバックアップ構成を切断すること

2. 認証情報の漏えいに対して最も強力な防御となるセキュリティ対策はどれですか?
   - A. ハードウェアキーを使った多要素認証
   - B. ブラウザー既定の形式を使って長いパスワードを作成すること
   - C. メールのユーザー名を6か月ごとに変更すること
   - D. 保存された Cookie のトラッキングブラウザー履歴を削除すること

3. クレジットフリーズ(信用情報の凍結)に当たるものは何ですか?
   - A. 泥棒が無断でローンを組めないよう、信用情報をロックする
   - B. データベースから銀行口座の取引履歴を削除すること
   - C. スキャナーのクレジットカード磁気ストライプ読み取り機能を無効にすること
   - D. ローカルデータベースのハードドライブを保存時に暗号化すること

4. ダークウェブ監視が役に立つのはなぜですか?
   - A. 漏えいした認証情報が不正なデータベースに現れた場合に、ユーザーに警告する
   - B. 仮想サンドボックス内で動作中のマルウェアが実行されるのを防ぐ
   - C. 仮想ネットワーク上のブラウザーのルーティング速度を高速化する
   - D. バックエンドデータベースへの SQL インジェクションによるアクセスの試みをブロックする

5. ソーシャルエンジニアリングとはどういう意味ですか?
   - A. 人を操って、機密の認証情報を自発的に明かさせる
   - B. 企業のサーバーポートをスキャンして、悪用可能なセキュリティ上の脆弱性を探すこと
   - C. システムデータベースファイルをオフラインのハードドライブにバックアップすること
   - D. ネットワークパケットを 3 つの暗号化されたオニオンノード経由でルーティングすること

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. 個人情報の盗難が影響するのはオンラインのデジタルアカウントだけで、郵便物には影響しません。

◯ 正しい ◯ 誤り

7 質問 7

7. すべての個人アカウントでMFAを徹底すると、ほとんどのクレデンシャルスタッフィングのボット攻撃をブロックできます。

◯ 正しい ◯ 誤り

8 質問 8

8. クレジットフリーズは信用照会をブロックしますが、自分の銀行口座にもアクセスできなくなります。

◯ 正しい ◯ 誤り

9 質問 9

9. パスワードマネージャーは、なりすましドメインでのパスワードの自動入力を拒否することで、フィッシングからユーザーを守ります。

◯ 正しい ◯ 誤り

10 質問 10

10. フィッシングメールは、感情的で素早い反応を引き出すために、緊急性を強調する表現をよく使います。

◯ 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. 個人情報の窃盗犯は、個人のパスワードやユーザーの _____ を狙います。

2. データベース侵害をユーザーに警告することで、非公開のアカウント情報の _____ が判明します。

3. サインイン時に一時的なコードを求める仕組みは _____ と呼ばれます。

4. 盗まれたデータを求めてハッカーのフォーラムを調べるのは、ダークウェブの _____ です。

5. 無断の信用照会を防ぐには、信用情報の _____ が必要です。

6. 従業員にフィッシング対策の教育を行うと、能動的なセキュリティの _____ が築かれます。

用語バンク

なりすまし　フィッシング　監視　資格情報　多要素認証　凍結　防御　漏えい

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

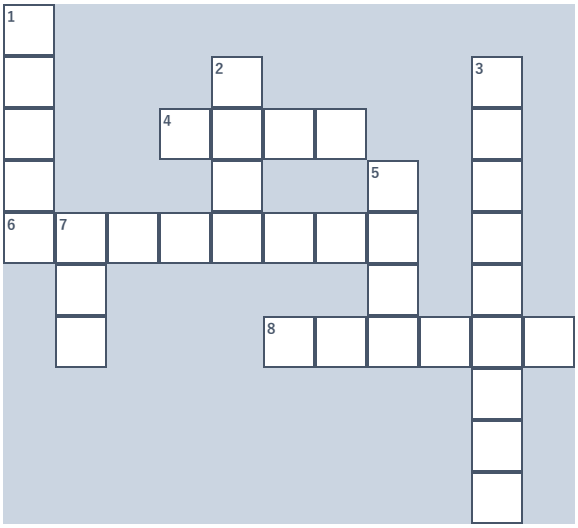
定義マッチング

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. 認証情報	A	アカウントのログインを保護する、追加の確認手順 (ハードウェアキーなど)。
	2. 漏えい	B	正当な組織に見せかけた偽のウェブサイトやメールを作成すること。
	3. MFA	C	不正なローン申請を防ぐために、信用情報へのアクセスを制限すること。
	4. 監視	D	個人ユーザーの記録を含む非公開データベースの不正な露出。
	5. フリーズ	E	個人情報の盗用から守るために使う、トレーニングと技術的な対策。
	6. 防御	F	ユーザーをだまして認証情報を渡させるために、偽のメッセージを送ること。
	7. なりすまし	G	盗まれた企業データがないか、オンラインフォーラムやハッカーのチャンネルを調べること。
	8. フィッシング	H	デジタルIDを認証するために使われる、ユーザー名、パスワード、非公開のトークン。

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. 個人のユーザー記録を含む非公開データベースが無断で外部にさらされること (4)

6. デジタル上のIDを認証するために使われるユーザー名、パスワード、非公開トークン (8)

8. 認証情報を渡させようと、だましの偽メッセージを送ること (6)

タテのカギ

1. 正規の組織を装う偽のウェブサイトやメールを作ること (5)

2. 個人情報の窃盗から守るために用いる教育と技術的な対策 (4)

3. アカウントのログインを守る、ハードウェアキーなどによる二段階目の確認手順 (9)

5. 不正なローン申請を防ぐため、信用情報へのアクセスを制限すること (4)

7. 盗まれた企業データを求めて、オンラインフォーラムやハッカーのチャンネルを調べること (3)

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: 個人のユーザー記録を含む非公開データベースが無断で外部にさらされること (4 文字):

6 ヨコ: デジタル上のIDを認証するために使われるユーザー名、パスワード、非公開トークン (8 文字):

8 ヨコ: 認証情報を渡させようと、だましの偽メッセージを送ること (6 文字):

タテのカギ

1 タテ: 正規の組織を装う偽のウェブサイトやメールを作ること (5 文字):

2 タテ: 個人情報の窃盗から守るために用いる教育と技術的な対策 (4 文字):

3 タテ: アカウントのログインを守る、ハードウェアキーなどによる二段階目の確認手順 (9 文字):

5 タテ: 不正なローン申請を防ぐため、信用情報へのアクセスを制限すること (4 文字):

7 タテ: 盗まれた企業データを求めて、オンラインフォーラムやハッカーのチャンネルを調べること (3 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。

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

用語リスト

シカクジヨウホウ　ロウエイ　タヨウソニンシヨウ　カンシ　トウケツ　ボウギヨ　ナリスマシ　フイツシング

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
A. シカクジヨウホウ
B. ロウエイ
C. タヨウソニンシヨウ
D. カンシ
E. トウケツ
F. ボウギヨ
G. ナリスマシ
H. フイツシング

定義とマッチ欄
1. 認証情報を渡させようと、だましの偽メッセージを送ること。
2. デジタル上のIDを認証するために使われるユーザー名、パスワード、非公開トークン。
3. 正規の組織を装う偽のウェブサイトやメールを作ること。
4. 個人情報の窃盗から守るために用いる教育と技術的な対策。
5. 盗まれた企業データを求めて、オンラインフォーラムやハッカーのチャンネルを調べること。
6. 不正なローン申請を防ぐため、信用情報へのアクセスを制限すること。
7. 個人のユーザー記録を含む非公開データベースが無断で外部にさらされること。
8. アカウントのログインを守る、ハードウェアキーなどによる二段階目の確認手順。

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. ホジヨシウカウク
2. ウタヨソヨンシニウ
3. ツトケウ
4. スシマナリ
5. イロエウ
6. ンシカ
7. ギボヨウ
8. ツグフンシイ

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	IDが盗まれたときにすること			
2	ソーシャルメディアで共有してはいけないこと			
3	バックアップするもの			
4	財布に入っているカードや身分証			
5	守るべき書類			
6	データが漏えいした後にすること			
7	ソフトウェアを更新する理由			
8	ID窃盗犯がほしがる情報			
9	ハッキングされるおそれのあるデバイス			
10	データが漏えいしうる場所			
11	今日から始められる安全な習慣			
12	コンピューターが感染しているサイン			
13	本人であることを証明する方法			
14	ID窃盗のサイン			
15	メールの危険なサイン			

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: 経営幹部へのなりすまし対策



シナリオ: 注目度の高いC-suiteの経営幹部が、顧客をだますために個人のメールを装った、タイポスクワッティングのドメイン名の標的にされました。ブランド保護計画を設計してください。

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: ダークウェブでの企業認証情報の露出



シナリオ: ダークウェブのデータベース流出に、企業のシステム管理者のものとみられる数百件の企業の認証情報が含まれています。緩和戦略を設計してください。

ディスカッションの問い: 認証情報の整理の手順を示し、パスワードマネージャーの導入を計画できますか？

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

16	38	3	15	22	46	12	38	3	60		53	64	46	25		32	35	20	45

31	35	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: 個人情報の盗難とは何ですか?

攻撃者が個人の記録(パスワードやSSNなど)を盗み、金銭的利益のために他人になりすます犯罪。

Q2: 個人情報の盗難の最も一般的な原因は何ですか?

フィッシングは、ユーザーを偽のなりすましウェブサイトに誘導して、盗人がパスワードを入手する主要な手口の1つです。

Q3: 多要素認証(MFA)は本人の身元をどう守りますか?

MFA はログインに（ハードウェアキーなどの）第二の証明を必要とするため、パスワードを盗まれても攻撃者をブロックできます。

Q4: クレジットフリーズとは何ですか?

信用調査機関が信用情報ファイルを共有するのをブロックし、泥棒があなたの名前で新たなローンを組むのを防ぐ無料サービス。 [2]

Q5: ダークウェブ監視とは何ですか?

ハッカーフォーラムを調べて、漏えいしたメールアドレス、パスワード、個人記録を探し、データが公開された場合に知らせるソフトウェア。

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: クレデンシャルスタッフィングとはどういう意味ですか?

流出したパスワードリストを数百のウェブサイトで試し、有効なアカウントを乗っ取る自動化されたボット。

Q7: メールのなりすましが危険なのはなぜですか?

攻撃者がメールの送信者名を偽装できるため、フィッシングメッセージが信頼できる同僚から届いたように見えてしまいます。

Q8: パスワードマネージャーは ID 窃盗をどう防ぎますか?

アカウントごとに複雑で固有のパスワードを保管し、偽のフィッシングドメインでは認証情報の自動入力を拒否します。

Q9: スピアフィッシングとは何ですか?

被害者の名前や詳細に合わせて作り込み、だまされる可能性を高める、きわめて標的を絞ったフィッシング攻撃。

Q10: クレジットアラートは凍結（フリーズ）とどう違いますか?

アラートは貸し手にアカウント開設前の本人確認を促しますが、フリーズは信用情報ファイルへのアクセスを完全にブロックします。 [2]

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: SIM スワップは、どのように個人情報の盗難につながりますか?

攻撃者は通信事業者のスタッフを説得して、被害者の電話番号を新しいSIMカードに移させ、SMSベースの2FAコードを乗っ取ります。

Q2: 個人情報の盗難の防止において、DMARC はどのような役割を果たしますか?

DMARCを使うと、ドメイン所有者はなりすましメールが受信トレイに届くのを防ぎ、企業ドメインをかたる偽メールを止められます。

Q3: 合成 ID 窃盗が検出しにくいのはなぜですか?

窃盗犯は本物の社会保障番号(SSN)と偽の名前や生年月日を組み合わせて、まったく新しい信用プロファイルを作り、基本的な不正検知アラートをすり抜けます。

Q4: データブローカーは個人の身元情報をどう悪用しますか?

データブローカーは、公的記録、ウェブ上の行動、購入履歴を収集してプロフィール資料をまとめ、それが漏えいしたり販売されたりすることがあります。

Q5: SMS ベースの MFA が脆弱と考えられているのはなぜですか?

SMS の通信は、傍受、フィッシング、通信事業者レベルの SIM スワッピング攻撃に対して脆弱です。

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: 信用情報ファイルのロックとは何ですか?

凍結に似た商用サービスで、モバイルアプリから信用情報ファイルのロックと解除をすぐに切り替えられます。

Q7: 企業のデータ侵害はどのように ID 窃盗を助長しますか?

流出したデータベースは何百万もの平文の認証情報をさらし、泥棒に標的型のなりすまし詐欺を実行するための生データを与えてしまいます。

Q8: ソーシャルメディアで共有しすぎるリスクは何ですか?

ペットの名前、出生地、母親の旧姓を公開すると、泥棒によく使われるアカウント復旧用の質問の答えを与えてしまいます。

Q9: 生体認証ログインは ID プロファイルをどう守りますか?

生体認証は、指紋や顔などの特徴にログインを結び付けます。デバイス内に保管すれば盗まれにくいですが、保存された生体データが漏えいする可能性はあります。

Q10: Red Flags Rule は個人情報の盗難にどのように対処しますか?

金融機関に対し、個人情報の盗用の兆候を検知して対応するための文書化されたプログラムの策定を求める連邦規制。

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

FTC が運営する IdentityTheft.gov では、米国の被害者が個人情報の盗難を報告し、個別の回復計画を受け取ることができます。 [1]

2. セキュリティの洞察

ハードウェアセキュリティキーは、フィッシングに強い MFA であり、CISA が推奨する最も強力な種類の MFA です。 [4]

3. セキュリティの洞察

漏えいしたパスワードはデータ侵害の一般的な入り口であり、のちの ID 詐欺の原因になります。

4. セキュリティの洞察

クレジットフリーズは連邦法により無料で、解除するまで貸し手が信用情報ファイルを照会できなくなります。 [2]

5. セキュリティの洞察

DMARCを使うと、ドメイン所有者は、チェックに失敗したなりすましメールを拒否または隔離するようメールサーバーに伝えられます。 [7]

6. セキュリティの洞察

SIM スワッピングにより、ハッカーは銀行ポータルでの SMS ベースの二要素認証を回避できます。

7. セキュリティの豆知識

合成 ID 詐欺は、本物の情報と偽の情報を混ぜ合わせるため、貸し手が見抜きにくくなります。

8. セキュリティの豆知識

多くの人が複数のオンラインアカウントで同じパスワードを使い回しているため、1 件の情報漏えいで複数のアカウントが危険にさらされる可能性があります。

9. セキュリティの豆知識

データブローカーは多数の消費者の詳細な個人情報を集めており、プライバシーのリスクが集中します。

10. セキュリティの洞察

個人情報の盗難からの回復には、請求の異議申し立てや信用情報報告書の修正など、数か月の作業が必要になることがあります。

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] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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

ID窃盗犯がログイン認証情報を盗むのに使う主な手口は何ですか? → 偽のメール通知を送り、ユーザーをだまして偽装されたポータルでパスワードを入力させる

2 問題 2

正解: A

指導メモ

認証情報の漏えいに対して最も強力な防御となるセキュリティ対策はどれですか? → ハードウェアキーを使った多要素認証

3 問題 3

正解: A

指導メモ

クレジットフリーズ(信用情報の凍結)に当たるものは何ですか? → 泥棒が無断でローンを組めないよう、信用情報をロックする

4 問題 4

正解: A

指導メモ

ダークウェブ監視が役に立つのはなぜですか? → 漏えいした認証情報が不正なデータベースに現れた場合に、ユーザーに警告する

5 問題 5

正解: A

指導メモ

ソーシャルエンジニアリングとはどういう意味ですか? → 人を操って、機密の認証情報を自発的に明かさせる

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

個人情報の盗用は、盗まれた郵便物や書類など、オフラインでも始まることがあります。

7 問題 7

正解: 正しい

指導メモ

すべての個人アカウントでMFAを徹底すると、ほとんどのクレデンシャルスタッフィングのボット攻撃をブロックできます。

8 問題 8

正解: 誤り

指導メモ

クレジットフリーズは新たな信用照会を止めますが、既存の口座には影響しません。

9 問題 9

正解: 正しい

指導メモ

パスワードマネージャーは、なりすましドメインでのパスワードの自動入力を拒否することで、フィッシングからユーザーを守ります。

10 問題 10

正解: 正しい

指導メモ

フィッシングメールは、感情的で素早い反応を引き出すために、緊急性を強調する表現をよく使います。

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

H 1. 認証情報	D 2. 漏えい	A 3. MFA	G 4. 監視
C 5. フリーズ	E 6. 防御	B 7. なりすまし	F 8. フィッシング

チェックポイント 3: 解答 – 重要用語

1 資格情報	2 漏えい	3 多要素認証	4 監視
5 凍結	6 防御		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 H – フイツシング	2 A – シカクジヨウホウ	3 G – ナリスマシ	4 F – ボウギヨ
5 D – カンシ	6 E – トウケツ	7 B – ロウエイ	8 C – タヨウソニンシヨウ

指導者向けディスカッションメモ

重要用語:
生徒が認証情報、漏えい、MFA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。

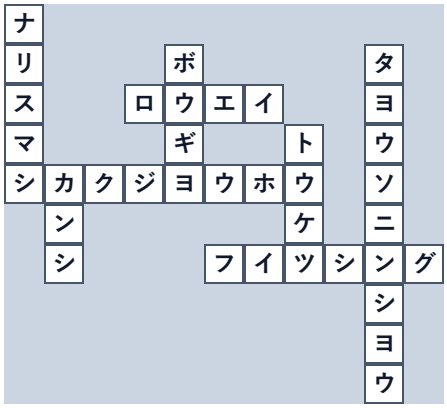
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: ロウエイ 個人のユーザー記録を含む非公開データベースが無断で外部にさらされること (4 文字)

6 ヨコ: シカクジヨウホウ デジタル上のIDを認証するために使われるユーザー名、パスワード、非公開トークン (8 文字)

8 ヨコ: フイツシング 認証情報を渡させようと、だましの偽メッセージを送ること (6 文字)

タテのカギ

1 タテ: ナリスマシ 正規の組織を装う偽のウェブサイトやメールを作ること (5 文字)

2 タテ: ボウギヨ 個人情報の窃盗から守るために用いる教育と技術的な対策 (4 文字)

3 タテ: タヨウソニンシヨウ アカウントのログインを守る、ハードウェアキーなどによる二段階目の確認手順 (9 文字)

5 タテ: トウケツ 不正なローン申請を防ぐため、信用情報へのアクセスを制限すること (4 文字)

7 タテ: カンシ 盗まれた企業データを求めて、オンラインフォーラムやハッカーのチャンネルを調べること (3 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. ホジヨシウカウク — **シカクジヨウホウ**
2. ウタヨソヨンシニウ — **タヨウソニンシヨウ**
3. ツトケウ — **トウケツ**
4. スシマナリ — **ナリスマシ**
5. イロエウ — **ロウエイ**
6. ンシカ — **カンシ**
7. ギボヨウ — **ボウギヨ**
8. ツグフンシイ — **フイツシング**

秘密の暗号チャレンジ 解答

"タヨウソニンショウデ ジブンノ ミモトヲ マモル"

ケーススタディの解答

A ケーススタディ 1: 経営幹部へのなりすまし対策

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: 著名な経営幹部が、顧客をだますために自分の個人用メールを模倣したタイポスクワッティングのドメイン名に狙われています。ブランド保護計画を立ててください。
- 推奨される戦略と解決策: 役員の名前の一般的なつづりのバリエーションをすべて登録します。ドメインのなりすましを防ぐため、メール認証プロトコル (DMARC、DKIM、SPF) を導入します。経営幹部のすべての社内ログインにハードウェア MFA を適用します。

B ケーススタディ 2: ダークウェブでの企業認証情報の露出

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: ダークウェブのデータベースのダンプに、ある企業のシステム管理者のものとみられる数百件の社内認証情報が含まれています。対策の戦略を立ててください。
- 推奨される対策と解決策: 全社でパスワードをリセットします。企業向けパスワードマネージャーの使用を義務づけます。すべてのシステムポータルで MFA を適用し、ダークウェブの継続的な自動監視アラートを設定します。