名前: _____ 日付: _____ 得点: _____

サイバーセキュリティの基礎とオンライン脅威予防

サイバーセキュリティの脅威、ネットワークファイアウォール、多要素認証、セキュリティフレームワーク

サイバーセキュリティの基礎の学習概要

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、サイバーセキュリティの基礎とオンライン脅威の防止の基本原則について学びます。マルウェアの脅威、多要素認証、ネットワークファイアウォール、インシデント対応の枠組みを取り上げます。

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/

あなたのサイバーセキュリティ基礎 学習ロードマップ

- マルウェア、フィッシング、企業ネットワークへの侵入のよくある経路を見分ける。
- MFA、ファイアウォール、エンドポイント防御を含む、標準的なサイバーセキュリティ対策を導入する。
- データ侵害の影響を軽減するためのインシデント対応手順を評価します。
- NISTガイドラインに基づく、組織のリスク要因とセキュリティの整合性を分析してください。
- 自動化されたクレデンシャルスタッフィングを抑えるため、セキュリティ衛生のための対策を設定してください。

サイバーセキュリティガイドの手順

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。学んだ知識を脅威の防止に応用しましょう。 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。

サイバーセキュリティの基礎と脅威の防止（導入）

サイバーセキュリティは、ネットワーク、システム、データを不正なデジタル攻撃から守ります。強固なセキュリティ習慣を身につけること、ファイアウォールを設定すること、多要素認証を必須にすること、従業員に脅威の見分け方を教育することは、企業のネットワーク防御に欠かせない要素です。

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. フィッシング攻撃の主な目的は何ですか?
   - A. 認証情報と機微なユーザーデータを盗む
   - B. ウェブサイトの検索エンジンでの可視性を高めること
   - C. ネットワーク帯域幅の容量を増やすこと
   - D. バックアップ用データセンターのレプリケーションを管理すること

2. 2. アカウントを最も強力に保護する仕組みはどれですか?
   - A. ハードウェアキーを使った多要素認証
   - B. 30日ごとに更新される複雑なパスワード
   - C. アカウントへのログインを営業時間内に制限すること
   - D. アカウントのユーザー名を公開ディレクトリから隠すこと

3. 3. ランサムウェア感染のペイロードは何によって定義されますか?
   - A. システムファイルを暗号化し、支払いを要求する
   - B. キー入力をリモートサーバーにひそかに記録すること
   - C. ブラウザーに不正な広告を挿入すること
   - D. ローカルの CPU リソースを使って暗号資産をマイニングすること

4. 4. ゼロデイ攻撃は、セキュリティ対策にどのような影響を与えますか?
   - A. パッチ未適用の未知の脆弱性を狙う
   - B. 企業のファイアウォールを自動的に無効にする
   - C. システムを強制的にハードリブートさせる
   - D. 対処に費用が一切かからない

5. 5. 企業のセキュリティ管理を統括するフレームワークはどれですか?
   - A. NISTサイバーセキュリティフレームワークのガイドライン
   - B. W3C HTML5ドキュメントスキーマ仕様
   - C. プリンタードライバーのインストールマニュアル
   - D. IETF のルーティングプロトコル定義

チェックポイント 2: 正しい・誤りチャレンジ

6 **質問(正誤) 6**

6. フィッシング攻撃は個人のメールアカウントだけを狙います。

○ 正しい　○ 誤り

7 **質問(正誤) 7**

7. 多要素認証は、クレデンシャルスタッフィング攻撃の防止に役立ちます。

○ 正しい　○ 誤り

8 **質問(正誤) 8**

8. ファイアウォールはネットワーク通信を検査し、許可されていないポートへのアクセスを遮断します。

○ 正しい　○ 誤り

9 **質問(正誤) 9**

9. ゼロデイ攻撃への対処には、標準的なウイルス対策の定義ファイルの更新が必要である。

○ 正しい　○ 誤り

10 **質問(正誤) 10**

10. ハニーポットは、サイバー犯罪者をおびき寄せるために使われるおとりのサーバーです。

○ 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. ネットワーク管理者は、受信トラフィックをフィルタリングするために _____ を導入します。

2. 攻撃者は、システムのパッチを回避するためにゼロデイの _____ を使います。

3. 攻撃者は、従業員を狙った _____ キャンペーンを行うために、なりすましメールを送ります。

4. ランサムウェアは、ユーザーのデータをロックする破壊的な形態の _____ です。

5. 強固な _____ を確立することで、認証情報の盗難リスクを軽減できます。

6. 機密性の高い通信を保護するために、ユーザーは _____ プロトコルを使います。

用語バンク

エクスプロイト　サイバーハイジーン　ゼロデイ　ハニーポット　ファイアウォール
フィッシング　マルウェア　暗号化

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

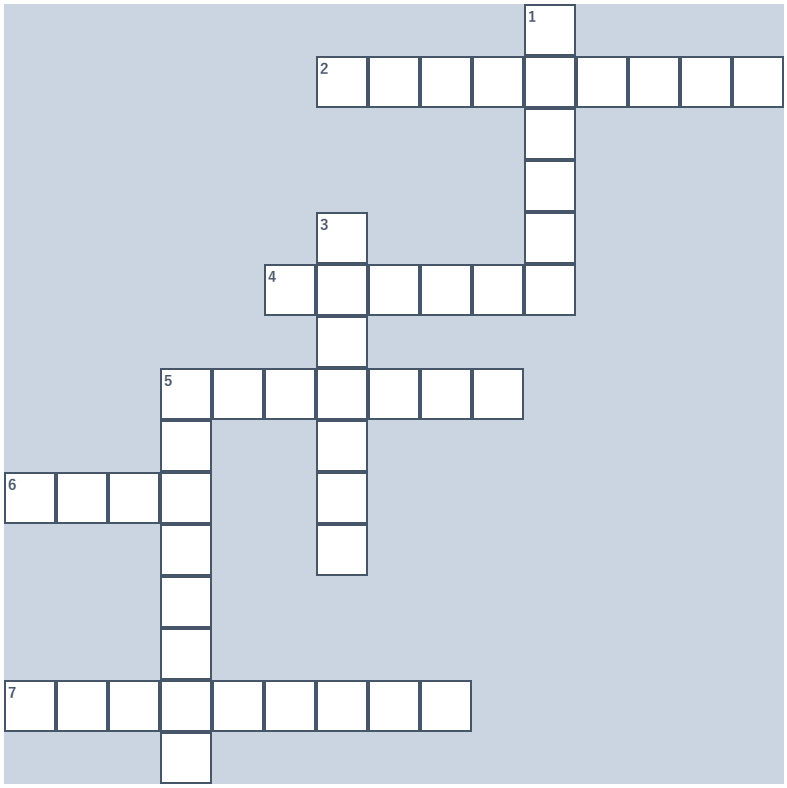
定義マッチング

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. ランサムウェアの脅威	A	NIST のような、サイバーリスクを管理するために使われる体系的なガイドライン。
2. 多要素認証	B	セキュリティ侵害に対処し、被害を軽減するための体系的な計画。
3. ゼロデイ攻撃	C	セキュリティルールに基づいてトラフィックをフィルタリングするネットワークの障壁。
4. おとりのハニーポット	D	データを暗号化し、復号と引き換えに金銭の支払いを要求するマルウェア。
5. 侵入防止ファイアウォール	E	ベンダーの修正パッチが公開される前に狙われる脆弱性攻撃。
6. インシデント対応	F	認証情報と認証キーを管理するためのベストプラクティス。
7. パスワード衛生	G	2つ以上の認証要素を求めるセキュリティ検証。
8. セキュリティフレームワーク	H	悪意ある攻撃者をおびき寄せて分析するために設置されたおとりのシステム。

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. 2つ以上の認証要素を求めるセキュリティ検証 (9)

4. セキュリティ侵害に対処し、被害を軽減するための体系的な計画 (6)

5. サイバーリスクの管理に使われる、NISTのような体系的なガイドライン (7)

6. ベンダーが修正パッチを公開する前に狙われる、脆弱性の悪用 (4)

7. 認証情報や認証キーを管理するためのベストプラクティス (9)

タテのカギ

1. 悪意ある攻撃者をおびき寄せて分析するために設置する、おとりのシステム (6)

3. データを暗号化し、復号と引き換えに金銭の支払いを要求するマルウェア (7)

5. セキュリティ規則に基づいて通信をフィルタリングする、ネットワーク上の防壁 (8)

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: 2つ以上の認証要素を求めるセキュリティ検証 (9 文字):

4 ヨコ: セキュリティ侵害に対処し、被害を軽減するための体系的な計画 (6 文字):

5 ヨコ: サイバーリスクの管理に使われる、NISTのような体系的なガイドライン (7 文字):

6 ヨコ: ベンダーが修正パッチを公開する前に狙われる、脆弱性の悪用 (4 文字):

7 ヨコ: 認証情報や認証キーを管理するためのベストプラクティス (9 文字):

タテのカギ

1 タテ: 悪意ある攻撃者をおびき寄せて分析するために設置する、おとりのシステム (6 文字):

3 タテ: データを暗号化し、復号と引き換えに金銭の支払いを要求するマルウェア (7 文字):

5 タテ: セキュリティ規則に基づいて通信をフィルタリングする、ネットワーク上の防壁 (8 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。

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

用語リスト

ランサムウエア　タヨウソニンシヨウ　ゼロデイ　ハニーポツト　フアイアウオール
インシデント　サイバーハイジーン　フレームワーク

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. ランサムウエア	1. セキュリティ規則に基づいて通信をフィルタリングする、ネットワーク上の防壁。
B. タヨウソニンシヨウ	2. セキュリティ侵害に対処し、被害を軽減するための体系的な計画。
C. ゼロデイ	3. データを暗号化し、復号と引き換えに金銭の支払いを要求するマルウェア。
D. ハニーポツト	4. 2つ以上の認証要素を求めるセキュリティ検証。
E. フアイアウオール	5. 認証情報や認証キーを管理するためのベストプラクティス。
F. インシデント	6. サイバーリスクの管理に使われる、NISTのような体系的なガイドライン。
G. サイバーハイジーン	7. ベンダーが修正パッチを公開する前に狙われる、脆弱性の悪用。
H. フレームワーク	8. 悪意ある攻撃者をおびき寄せて分析するために設置する、おとりのシステム。

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. ムエラウアサン
2. ゼデイロ
3. アアフウオルーイ
4. ハンーージイサイバ
5. シニヨウンソタヨウ
6. ツポハートニ
7. ンイデトシン
8. レムクフーワー

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	サイバーセキュリティの職種			
2	ソフトウェアを更新する理由			
3	ファイアウォールがブロックできるもの			
4	メールの危険なサイン			
5	バックアップするもの			
6	よく知られたサイバー攻撃の種類			
7	ハニーポットがおびき寄せるもの			
8	決して共有してはいけない情報			
9	コンピューターが感染しているサイン			
10	ハッカーが登場する映画や番組			
11	構築できるセキュリティの層			
12	セキュリティ訓練で練習すること			
13	知っているセキュリティツール			
14	ITのサポートを頼める人			
15	「サイバー」で始まる言葉			

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: ランサムウェアからの復旧戦略



シナリオ: 企業ネットワークがランサムウェアに感染し、重要なデータベースがロックされました。攻撃者は100,000ドル相当の暗号資産の支払いを要求しています。この企業には、24時間前のオフラインバックアップがあります。

ディスカッションの問い: 支払うことのリスクを分析し、復旧戦略を評価してください。

ケーススタディ 2: クレデンシャルスタッフィングへの防御



シナリオ: オンラインサービスがクレデンシャルスタッフィング攻撃を受け、ハッカーが他のサイトから盗んだ数百万件のユーザー名とパスワードの組を試しています。

ディスカッションの問い: この攻撃の仕組みを詳しく説明し、2つの防御策を示せますか？

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		12	13	19	33	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: サイバーセキュリティの主な目的は何ですか?

主な目的は、ネットワーク、デバイス、データを、不正アクセス、攻撃、偶発的な損害から守ることです。

Q2: フィッシングとスピアフィッシングはどう違いますか?

フィッシングは無作為なユーザーを狙う広範なメールキャンペーンで、スピアフィッシングは個人データを使って特定の個人を狙います。

Q3: ネットワークファイアウォールとは何ですか?

ファイアウォールは、あらかじめ定められたセキュリティルールに基づいて、受信と送信の通信を監視・フィルタリングするネットワークセキュリティシステムです。

Q4: 多要素認証(MFA)が必要なのはなぜですか?

MFA は重要な防御の層を加え、攻撃者が主要なパスワード認証情報を盗んだり破ったりしてもアクセスできないようにします。

Q5: コンピューターウイルスはどのように定義されますか?

ウイルスは、正常なファイルに寄生して自己複製するマルウェアで、実行されるとシステム間に広がります。

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 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: ランサムウェアはローカルデータをどうロックしますか?

ランサムウェアは暗号アルゴリズムを使ってユーザーのファイルを暗号化し、復号鍵が適用されるまで読めない状態にします。

Q7: ゼロデイ脆弱性とは何ですか?

ゼロデイは、ソフトウェアのベンダーに知られていないセキュリティ上の欠陥で、悪用される前にパッチを開発する時間がありません。

Q8: NIST フレームワークの役割は何ですか?

NISTフレームワークは、組織がサイバーセキュリティのリスクを管理し減らすのに役立つ、任意のガイドラインと標準を提供します。

Q9: セキュリティインシデント対応計画とは何ですか?

セキュリティ侵害やネットワークの侵害を検知し、封じ込め、復旧するための、文書化された一連の手順です。

Q10: ソーシャルエンジニアリングはどのようにユーザーにつけ込みますか?

ソーシャルエンジニアリングは、心理的な操作で従業員をだまし、パスワードを明かさせたり、悪意のあるファイルをダウンロードさせたりします。

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: DDoS 攻撃は、ウェブサーバーをどのように圧倒しますか?

DDoS攻撃は、乗っ取られた何百万台ものボットネットデバイスを連携させてサーバーにトラフィックを殺到させ、帯域幅とCPUの限界を使い果たさせます。

Q2: 対称暗号と非対称暗号の違いは何ですか?

共通鍵暗号は暗号化と復号に1つの鍵を使い、公開鍵暗号は公開鍵と秘密鍵のペアを使います。

Q3: ハッカーはどのように SQL インジェクション攻撃を実行しますか?

攻撃者は入力フォームに悪意のあるSQLコマンドを入力し、バックエンドのデータベースをだまして、権限のないユーザー記録を開示させます。

Q4: ネットワーク侵入における横展開とは何ですか?

攻撃者が最初のサーバーへのアクセスを悪用して、内部ネットワーク上の他の相互接続されたシステムを侵害する、手口です。

Q5: DNS スプーフィングはウェブトラフィックをどう別の場所へ誘導しますか?

DNSスプーフィングはネームサーバーのキャッシュレコードを改ざんし、正規のユーザーを本来のドメインではなく、悪意のあるそっくりなウェブサイトへ誘導します。

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: ハードウェアセキュリティトークンとは何ですか?

暗号による認証の証明を生成する物理デバイス(YubiKey など)で、リモートからのフィッシングに対して最大限の防御を提供します。

Q7: セキュリティチームはおとりのハニーポットをどう使いますか?

チームは、本番ではないおとりサーバーを設置して、侵入を早期に検知し、不正な者の攻撃パターンを分析します。

Q8: 最小権限の原則とは何ですか?

ユーザーのアクセス権を、業務上の役割を果たすために必要な最小限に制限する、セキュリティ標準です。

Q9: 中間者攻撃は接続をどう悪用しますか?

攻撃者が暗号化されていないネットワーク上の2台のデバイス間の通信を傍受して改ざんし、セッショントークンと認証情報を盗むこと。

Q10: 侵害の痕跡（IOC）とは何ですか?

IOC は、レジストリの異常な変更や不審な IP 通信など、システムが侵害されたことを示す、フォレンジック上の手がかりとなるデータです。

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

攻撃者は脆弱なサーバーを求めて常にインターネットをスキャンし、従業員の受信トレイにフィッシングメールを送ります。

2. セキュリティの洞察

フィッシングリンクのクリックなどのヒューマンエラーは、データ侵害でよくみられる要因であり、そのために研修が重要です。

3. セキュリティの洞察

データ侵害のコストには、法的な罰金、顧客離れ、調査と復旧の費用が含まれ、数百万ドルに達することもあります。

4. セキュリティの洞察

ハードウェアセキュリティキーなどのフィッシング耐性のある MFA は、最も強力な種類の MFA であり、CISA が推奨する標準です。 [2]

5. セキュリティの洞察

ランサムウェアは依然として企業ネットワークにとって大きな脅威であり、CISA は主な防御策としてオフラインの暗号化バックアップを推奨しています。 [4]

6. セキュリティの洞察

NISTサイバーセキュリティフレームワーク2.0(2024年)には、統治、特定、防御、検知、対応、復旧の6つの中核機能があります。 [1]

7. セキュリティの豆知識

クレデンシャルスタッフィングのボットは、漏えいしたユーザー名とパスワードの組を、銀行や EC のログインポータルに対して大規模に試します。

8. セキュリティの豆知識

ゼロデイエクスプロイトの市場は世界中に存在し、深刻度の高い脆弱性は、修正される前に高額で売買されることがあります。

9. セキュリティの豆知識

ハニーポットのおとりシステムは、正規のユーザーがアクセスする理由がないため、侵入があるとすぐにアラートを報告します。

10. セキュリティの洞察

Transport Layer Security(TLS)はブラウザーのセッションを暗号化し、公共Wi-Fiネットワークでのパケットスニッフィングを防ぎます。

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] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

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

[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. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

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

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

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

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

解答: チェックポイント 1 – 多肢選択

1 **フィッシング攻撃** フィッシング 正解: A

指導メモ

フィッシングキャンペーンは、なりすましメールを使って認証情報や機密性の高いユーザーデータを盗もうとします。 出典: OWASP Secure Configuration.

2 **アカウント保護** MFA キー 正解: A

指導メモ

ハードウェアトークンを使った多要素認証（MFA）は、アカウントへのアクセスに対する最も強力な防御を提供します。出典: NIST Digital Identity。

3 **ランサムウェアの脅威** ランサムウェア 正解: A

指導メモ

ランサムウェアは重要なシステムとデータを暗号化し、復号鍵と引き換えに暗号資産での支払いを要求します。出典: Center for Internet Security (CIS)。

4 **ゼロデイ脆弱性** ゼロデイ 正解: A

指導メモ

ゼロデイ脅威は、ベンダーの修正プログラムが提供される前に、未修正で未知のセキュリティ上の欠陥を悪用します。出典: OWASP Secure Configuration。

5 **セキュリティフレームワーク** フレームワーク 正解: A

指導メモ

NIST などのフレームワークは、組織がサイバーリスクを管理し低減するのに役立つ体系的な指針を提供します。出典: NIST Digital Identity。

解答: チェックポイント 2 – 正誤問題

6 標的型フィッシング フィッシング

正解: 誤り

指導メモ

フィッシング攻撃は、攻撃経路を広げるために、企業ネットワークと個人アカウントの両方を狙います。 出典: OWASP Secure Configuration.

7 問題 7

正解: 正しい

指導メモ

MFAは2つ目の要素を必要とするため、盗まれたパスワードだけでは通常ログインできません。

8 通信ファイアウォール ファイアウォール

正解: 正しい

指導メモ

ファイアウォールは、特定のネットワークポートの通信を検査して遮断し、許可されていない接続を除外します。出典: Center for Internet Security (CIS)。

9 ゼロデイ対応 ゼロデイ

正解: 誤り

指導メモ

ゼロデイの脆弱性への対処には、シグネチャがまだ存在しないため、コードのパッチと WAF のフィルタリングが必要です。出典: OWASP Secure Configuration。

10 おとりのハニーポット ハニーポット

正解: 正しい

指導メモ

ハニーポットは、セキュリティチームが悪意ある攻撃者をおびき寄せ、警告を出し、調査するために使う、おとりのサーバーです。出典: Center for Internet Security (CIS)。

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

D 1. ランサムウェアの脅威	G 2. 多要素認証	E 3. ゼロデイ攻撃	H 4. おとりのハニーポット
C 5. 侵入防止ファイアウォール	B 6. インシデント対応	F 7. パスワード衛生	A 8. セキュリティフレームワーク

チェックポイント 3: 解答 – 重要用語

1 ファイアウォール	2 エクスプロイト	3 フィッシング	4 マルウェア
5 サイバーハイジーン	6 暗号化		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 E – フアイアウオール	2 F – インシデント	3 A – ランサムウエア	4 B – タヨウソニンシヨウ
5 G – サイバーハイジーン	6 H – フレームワーク	7 C – ゼロデイ	8 D – ハニーポツト

指導者向けディスカッションメモ

重要用語:
生徒がランサムウェアの脅威、多要素認証、ゼロデイ攻撃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。

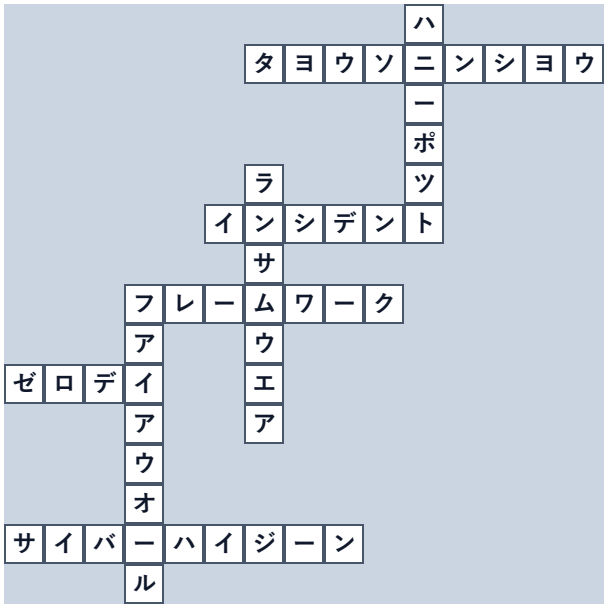
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: タヨウソニンシヨウ 2つ以上の認証要素を求めるセキュリティ検証 (9 文字)

4 ヨコ: インシデント セキュリティ侵害に対処し、被害を軽減するための体系的な計画 (6 文字)

5 ヨコ: フレームワーク サイバーリスクの管理に使われる、NISTのような体系的なガイドライン (7 文字)

6 ヨコ: ゼロデイ ベンダーが修正パッチを公開する前に狙われる、脆弱性の悪用 (4 文字)

7 ヨコ: サイバーハイジーン 認証情報や認証キーを管理するためのベストプラクティス (9 文字)

タテのカギ

1 タテ: ハニーポット 悪意ある攻撃者をおびき寄せて分析するために設置する、おとりのシステム (6 文字)

3 タテ: ランサムウエア データを暗号化し、復号と引き換えに金銭の支払いを要求するマルウェア (7 文字)

5 タテ: ファイアウオール セキュリティ規則に基づいて通信をフィルタリングする、ネットワーク上の防壁 (8 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. ムエラウアサン — **ランサムウエア**
2. ゼデイロ — **ゼロデイ**
3. アアフウオルーイ — **フアイアウオール**
4. ハンーージイサイバ — **サイバーハイジーン**
5. シニヨウンソタヨウ — **タヨウソニンシヨウ**
6. ツポハートニ — **ハニーポツト**
7. ンイデトシン — **インシデント**
8. レムクフーワー — **フレームワーク**

秘密の暗号チャレンジ 解答

"タヨウソニンショウデ システムヲ マモル"

ケーススタディの解答

A ケーススタディ 1: ランサムウェアからの復旧戦略

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: 企業のネットワークがランサムウェアに感染し、重要なデータベースがロックされました。攻撃者は 100,000 ドル相当の暗号資産の支払いを要求しています。その企業には 24 時間前のオフラインバックアップがあります。
- 推奨される戦略と解決策: 支払いのリスク: 支払ってもファイルが復号される保証はなく、その会社が支払いに応じる標的だと見なされ、犯罪活動に資金を提供することになります。復旧戦略: チームは感染したホストを隔離し、侵害されたサーバーを消去して、オフラインバックアップからデータを復元するべきです。再感染をただちに防ぐため、最初の侵入経路 (フィッシングまたはエクスプロイト) にパッチを適用する必要があります。

B ケーススタディ 2: クレデンシャルスタッフィングへの防御

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: あるオンラインサービスが、他のサイトから盗まれた数百万件のユーザー名とパスワードの組み合わせをハッカーが試す、クレデンシャルスタッフィング攻撃を受けています。
- 推奨される戦略と解決策: 仕組み: 攻撃者は、サイト間でのパスワードの使い回しを利用し、自動化されたボットでユーザーアカウントにログインします。防御策: 1. 多要素認証 (MFA) は、パスワードが正しくてもログインの試行をブロックします。2. レート制限と CAPTCHA を導入すると、ログインエンドポイントに大量の要求を送る自動化されたボットの通信をブロックできます。