名前: 日付: 得点:

公共 Wi-Fi のセキュリティと暗号化

中間者攻撃、不正なアクセスポイント、パケットスニッフィング、VPN トンネル、HTTPS 暗号化。

公共 Wi-Fi セキュリティの学習概要

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、公共Wi-Fiのセキュリティについて学びます。暗号化されていないネットワーク、中間者 (MitM) 攻撃、不正アクセスポイント、パケットスニッフィング、VPNトンネル、HTTPS通信のセキュリティを取り上げます。

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/public-wifi-security/

あなたの公共Wi-Fiセキュリティ 学習ロードマップ

- パケットスニッフィングや不正アクセスポイントなど、公衆 Wi-Fi のよくあるリスクを見分ける。
- 転送中のデータを守るために、VPN の暗号化トンネルを導入する。
- リモートワーカーに対して、HTTPSと安全なウェブブラウザー設定を強制します。

公共 Wi-Fi 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。学んだ知識をリモートアクセスのセキュリティに応用しましょう。 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。

公共 Wi-Fi のセキュリティと通信保護（導入）

暗号化されていない公共のWi-Fiホットスポットでは、ネットワーク通信がパケットスニッフィングやイービルツイン偽装にさらされます。通信を安全なVPN暗号化トンネルに通し、HTTPSのみのHSTSルールを適用すると、ローカルネットワークでの傍受からセッションを守れます。

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. 中間者(MitM)攻撃とは何ですか?

- A. 共有ネットワーク上の2者間の通信を傍受して改ざんする
- B. ユーザー記録を狙うデータベース抽出手法
- C. ネットワークトラフィックのリクエストでウェブサーバーを過負荷にすること
- D. ローカルのハードドライブのストレージボリュームを消去すること

2 2. 不正アクセスポイント(イービルツイン)とは何ですか?

- A. 正規のネットワークと同じSSIDに設定された悪意のあるWi-Fiホットスポット
- B. データベースのバックアップを監視するために使われる管理ツール
- C. 安全なVPNゲートウェイ構成
- D. 許可されたメールサーバーを対応付ける DNS レコード

3 3. VPN は、公衆 Wi-Fi の通信をどのように守りますか?

- A. すべてのネットワークパケットを暗号化トンネルで包み、スニッファーに読めなくする
- B. 受信接続リクエストをすべて自動的にブロックする
- C. 物理ネットワークカードの MAC アドレスを変更する
- D. ウェブブラウザーのキャッシュされた Cookie を削除する

4 4. パケットスニッフィングとは何ですか?

- A. ハードウェアまたはソフトウェアのツールで、ネットワークパケットを取得して記録する
- B. ローカルディレクトリをスキャンして重複ファイルを探すこと
- C. ユーザーの役割に基づいてデータベースの読み取り権限を制限すること
- D. AES-256 鍵を使ってストレージドライブを暗号化すること

5 5. HTTPSの役割は何ですか?

- A. ブラウザーとウェブサーバー間のセッション通信を暗号化する
- B. ゲートウェイで受信メールメッセージをフィルタリングすること
- C. ページの読み込みを速くするために画像を圧縮すること
- D. ネットワーク接続ストレージのファイル構造を管理すること

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. 接続しているユーザーは、オープンな公衆 Wi-Fi ネットワーク上の平文データを簡単に取得できます。

◯ 正しい ◯ 誤り

7 質問 7

7. 不正アクセスポイント（イービルツイン）は、常にネットワーク管理者によって承認されている。

◯ 正しい ◯ 誤り

8 質問 8

8. VPNは、公共ネットワークでのパケットスニッフィングから通信を守る効果がありません。

◯ 正しい ◯ 誤り

9 質問 9

9. HTTPS が暗号化するのは URL のパスだけで、パケットのペイロードは平文のままです。

◯ 正しい ◯ 誤り

10 質問 10

10. WPA3セキュリティを使うWi-Fiホットスポットは、オープンでパスワードのないネットワークより強力な保護を提供します。

◯ 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. 公共Wi-Fiで個人のパスワードを盗み取ることは、通信の _____ です。
2. ローカルネットワーク上の生のパケットを解析するには、パケット _____ を使います。
3. ホテルのWi-Fiに似せた不正なホットスポットは _____ です。
4. ウェブ通信の経路を守るには、 _____ で暗号化する必要があります。
5. ネットワークの出力をすべて暗号化するには、クライアントの _____ を使います。
6. 公共のネットワークを通る暗号化された通信経路は、 _____ です。

用語バンク

HTTPS　VPN　WPA3　イビルツイン　スニッフィング　トンネル　ファイアウォール　傍受

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

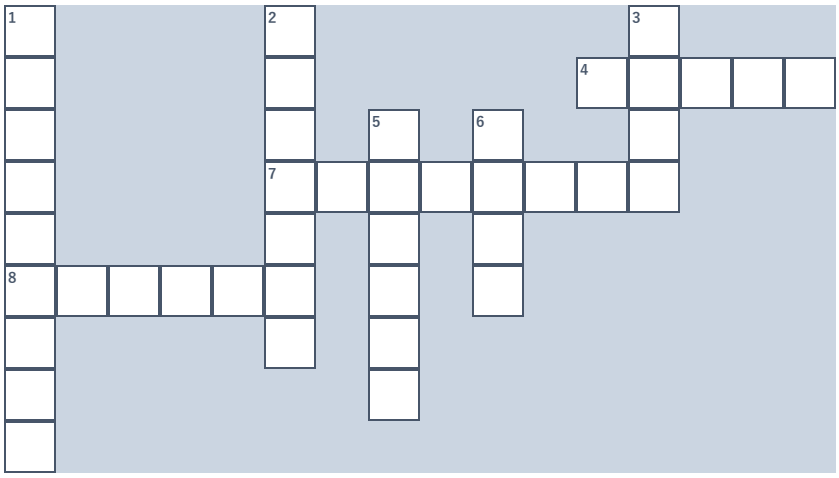
定義マッチング

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. 傍受	A	最新の Wi-Fi セキュリティ標準。
	2. スニッフィング	B	転送中の安全なデータ経路。
	3. イービルツイン	C	受信トラフィックのフィルタリング。
	4. HTTPS	D	Wi-Fi を装う不正なホットスポット。
	5. VPN	E	転送中のトラフィックを読み取ること。
	6. トンネル	F	ネットワークのデータパケットを取り込むこと。
	7. WPA3	G	暗号化された仮想プライベートネットワーク。
	8. ファイアウォール	H	安全なWeb通信。

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. ウェブ通信を守る安全な送信のしくみ (5)

7. 着信する通信を選別する仕組み (8)

8. Wi-Fiに似せた不正なホットスポット (6)

タテのカギ

1. 最新のWi-Fiの安全性に関する標準 (9)

2. ネットワークのデータパケットを捕捉すること (7)

3. 通信中のデータを通す安全な経路 (4)

5. 暗号化された仮想プライベートネットワーク (6)

6. 通信中のトラフィックを読み取ること (4)

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: ウェブ通信を守る安全な送信のしくみ (5 文字):

7 ヨコ: 着信する通信を選別する仕組み (8 文字):

8 ヨコ: Wi-Fiに似せた不正なホットスポット (6 文字):

タテのカギ

1 タテ: 最新のWi-Fiの安全性に関する標準 (9 文字):

2 タテ: ネットワークのデータパケットを捕捉すること (7 文字):

3 タテ: 通信中のデータを通す安全な経路 (4 文字):

5 タテ: 暗号化された仮想プライベートネットワーク (6 文字):

6 タテ: 通信中のトラフィックを読み取ること (4 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。

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

用語リスト

ボウジユ　スニツフイング　イビルツイン　アンゴウカ　ブイピーエヌ　トンネル
セキユリテイキカク　フアイアウオール

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. ボウジユ	1. 最新のWi-Fiの安全性に関する標準。
B. スニツフイング	2. Wi-Fiに似せた不正なホットスポット。
C. イビルツイン	3. ネットワークのデータパケットを捕捉すること。
D. アンゴウカ	4. 通信中のデータを通す安全な経路。
E. ブイピーエヌ	5. 着信する通信を選別する仕組み。
F. トンネル	6. 通信中のトラフィックを読み取ること。
G. セキユリテイキカク	7. 暗号化された仮想プライベートネットワーク。
H. フアイアウオール	8. ウェブ通信を守る安全な送信のしくみ。

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. ジボユウ
2. ンイルイツビ
3. ブピーヌエイ
4. テクカリキイセキュ
5. イグフツスンニ
6. ウアゴカン
7. ネトルン
8. アアウルフーオイ

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	ソフトウェアを更新する理由			
2	Wi-Fiに自動接続するデバイス			
3	決して共有してはいけない情報			
4	今日から始められる安全な習慣			
5	カフェで安全に過ごす方法			
6	ハッキングされるおそれのあるデバイス			
7	オープンなWi-Fiでハッカーが見られるもの			
8	偽のWi-Fiネットワークのサイン			
9	公共のWi-Fiの代わりになるもの			
10	メールの危険なサイン			
11	公共のWi-Fiでしないこと			
12	無料Wi-Fiがある場所			
13	アカウントを守る方法			
14	コンピューターが感染しているサイン			
15	怪しく見えるWi-Fi名			

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: 公衆 Wi-Fi でのパケット盗聴の封じ込め



シナリオ: 公共の空港Wi-Fiネットワークに接続しているリモートの営業幹部が、機密性の高いビジネスメールがいくつか、平文で送信した直後に漏えいしたことに気づきます。

ディスカッションの問い: 公共ネットワークのリスクを分析し、通信の暗号化による解決策を概説できますか？

ケーススタディ 2: イービルツインによる偽ホットスポットへの防御



シナリオ: 攻撃者が、正規のカフェのホットスポットに似せて「CoffeeShop_Guest」という名前の不正なワイヤレスアクセスポイントを設置し、何も知らない客のネットワーク通信を取得します。

ディスカッションの問い: 不正なアクセスポイントを検出してブロックするための確認手順を詳しく説明できますか？

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

44	2	28	1	2	45		64	2	68	72	4	23	60		1	46	51	3	6

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: なぜ公共 Wi-Fi は安全ではないのですか?

公共の Wi-Fi では通信が電波上で暗号化されないため、近くにいる他の人が保護されていないデータを傍受できます。 [2]

Q2: パケットスニッフィングとは何ですか?

パケットスニッファーは、ネットワークインターフェースを流れる生データを取得し、平文のパスワードや通信の詳細を露出させます。

Q3: イービルツインとは何ですか?

信頼できる地元のWi-Fiホットスポットの名前と設定をまねて、ハッカーが設置した不正なアクセスポイント。

Q4: VPN は私をどう守りますか?

通信を暗号化されたトンネル経由でルーティングし、閲覧活動をローカルネットワークのスニッファーから隠します。

Q5: 公共 Wi-Fi で HTTPS は私を守ってくれますか?

はい、ブラウザーとウェブサイトの間でやり取りされるデータを暗号化し、VPNはさらにもう1層の保護を加えます。

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: WPA3 とは何ですか?

最新のWi-Fi Protected Access標準で、より強力な暗号化と、オフライン辞書攻撃に対する保護を提供します。 [1]

Q7: 公共 Wi-Fi でマルウェアに感染することはありますか?

はい、攻撃者はトラフィックを傍受し、ブラウザーのセッションに悪意のあるダウンロードの表示(ドライブバイダウンロード)を挿入できます。

Q8: ファイル共有のリスクは何ですか?

ファイル共有が有効になっていると、公衆ネットワーク上の他のユーザーが、あなたのローカルフォルダーのディレクトリを読み取ったり変更したりできます。

Q9: キャプティブポータルとは何ですか?

ホテルやカフェのネットワークがインターネット接続を許可するために使うログインページで、攻撃者になりすまされることがあります。

Q10: 使っていないときは Wi-Fi をオフにすべきですか?

はい、Wi-Fiをオフにすると、信頼できないネットワークに端末が自動接続されるのを防げます。

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: 中間者攻撃は、DNS をどのように悪用しますか?

不正なルーターでDNSスプーフィングを行い、対象ブラウザーを本来のドメインではなく類似のフィッシング用ランディングページに誘導することによって。

Q2: セッションハイジャックとは何ですか?

攻撃者が公共Wi-Fi上で暗号化されていないセッションCookieをスニッフィングし、それを取り込んで認証情報によるログインを回避すること。

Q3: SSL ストリッピングとは何ですか?

攻撃者がユーザーの安全なHTTPSリクエストを暗号化されていないHTTPにダウングレードし、ログイン情報を平文で奪う中間者攻撃。

Q4: HSTS は SSL ストリッピングをどう防ぎますか?

HTTP Strict Transport Security は、ブラウザーを HTTPS 経由でのみ接続させ、暗号化されていない HTTP への切り替えを拒否します。 [3]

Q5: スプリットトンネル VPN とは何ですか?

企業の通信だけをVPN経由にし、公共のインターネットデータは直接送る構成で、リーク経路が露出するリスクがあります。

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: WPA2 が KRACK に対して脆弱なのはなぜですか?

鍵再インストール攻撃(KRACK)は、WPA2の4ウェイハンドシェイクを悪用し、Wi-Fiパスワードなしでパケットを復号します。

Q7: クライアント分離とは何ですか?

接続されたWi-Fiデバイス同士が直接通信するのを防ぎ、ローカルでのスニッフィングをブロックするルーターのセキュリティ設定。

Q8: 攻撃者は偽の DNS サーバーをどのように利用しますか?

不正なルーターを設定してクライアントに偽のDNSサーバーを割り当て、すべてのWeb検索を傍受し書き換えます。

Q9: VPN でローカルの MAC アドレスを隠せますか?

いいえ。MAC アドレスはローカルなレイヤー 2 の識別子です。代わりに、お使いのデバイスに組み込まれた MAC のランダム化（プライベートアドレス）設定を使いましょう。

Q10: キャプティブポータルのなりすまし攻撃とは何ですか?

攻撃者が、無料Wi-Fiを装って認証情報を盗むため、不正なホットスポット上に偽の認証ポータルを設置すること。

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

リモートワーカーは、カフェ、ホテル、空港などの Wi-Fi をよく使いますが、そこではネットワークのセキュリティを自分で管理できません。

2. セキュリティの洞察

Evil Twinの不正ホットスポットは、信頼できるネットワークの名前とMACアドレスをそっくりコピーして、デバイスを混乱させることがあります。

3. セキュリティの洞察

Wireshark のようなパケットスニッフィングソフトウェアは無料で、暗号化されていない HTTP のパスワードを平文で表示できます。

4. セキュリティの洞察

WPA3セキュリティは、同時認証(SAE)を利用して、ローカルでの総当たり攻撃から保護します。

5. セキュリティの洞察

SSL ストリッピング攻撃は、ゲートウェイで最初の HTTP リダイレクトを傍受することで、基本的な HTTPS の保護を回避します。

6. セキュリティの洞察

HTTP Strict Transport Security (HSTS) のレスポンスヘッダーは、ブラウザーが暗号化されていない HTTP 接続に切り替わるのを防ぎます。 [3]

7. セキュリティの豆知識

「自動接続」をオフにすると、スマートフォンが公共の場で見た目がそっくりな不正ネットワークに接続するのを防げます。

8. セキュリティの豆知識

企業の「常時接続」VPN構成では、リモートワーカーのネットワークトラフィックをすべて、社内ファイアウォール経由にします。

9. セキュリティの豆知識

不正アクセスポイントは偽の DNS 応答を返し、標的のドメインをフィッシングサーバーに誘導することがあります。

10. セキュリティの洞察

VPNを使わないと、オープンなホットスポットにいる他のユーザーに、デバイスが接続するサイトやサーバーが見える可能性があります。

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] Wi-Fi Alliance. (n.d.). Security.
https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[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

中間者(MitM)攻撃とは何ですか? → 共有ネットワーク上の2者間の通信を傍受して改ざんする

2 問題 2

正解: A

指導メモ

不正アクセスポイント(イービルツイン)とは何ですか? → 正規のネットワークと同じSSIDに設定された悪意のあるWi-Fiホットスポット

3 問題 3

正解: A

指導メモ

VPN は、公衆 Wi-Fi の通信をどのように守りますか? → すべてのネットワークパケットを暗号化トンネルで包み、スニッファーに読めなくする

4 問題 4

正解: A

指導メモ

パケットスニッフィングとは何ですか? → ハードウェアまたはソフトウェアのツールで、ネットワークパケットを取得して記録する

5 問題 5

正解: A

指導メモ

HTTPSの役割は何ですか? → ブラウザーとウェブサーバー間のセッション通信を暗号化する

解答: チェックポイント 2 – 正誤問題

6 問題 6

正解: 正しい

指導メモ

接続しているユーザーは、オープンな公衆 Wi-Fi ネットワーク上の平文データを簡単に取得できます。

7 問題 7

正解: 誤り

指導メモ

誤り: イービルツインとは、攻撃者が本物のホットスポットに見せかけて設置した、不正なホットスポットです。

8 問題 8

正解: 誤り

指導メモ

誤り: VPNはトンネル内で通信を暗号化するため、ローカルのスニッファーは内容を読み取れません。

9 問題 9

正解: 誤り

指導メモ

誤り: HTTPSは、URLのパスやページの内容を含め、HTTPのやり取り全体を暗号化します。

10 問題 10

正解: 正しい

指導メモ

WPA3セキュリティを使うWi-Fiホットスポットは、オープンでパスワードのないネットワークより強力な保護を提供します。

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

E 1. 傍受	F 2. スニッフィング	D 3. イービルツイン	H 4. HTTPS
G 5. VPN	B 6. トンネル	A 7. WPA3	C 8. ファイアウォール

チェックポイント 3: 解答 – 重要用語

1 傍受	2 スニッフィング	3 イビルツイン	4 HTTPS
5 VPN	6 トンネル		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 G – セキュリテイキカク	2 C – イビルツイン	3 B – スニツフイング	4 F – トンネル
5 H – フアイアウオール	6 A – ボウジユ	7 E – ブイピーエヌ	8 D – アンゴウカ

指導者向けディスカッションメモ

重要用語:
生徒が傍受、スニッフィング、イービルツイン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。

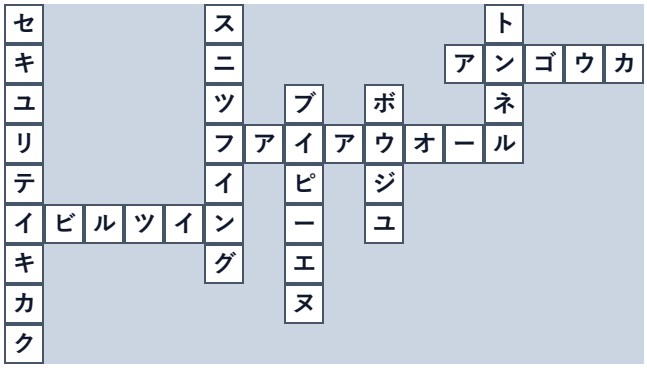
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: アンゴウカ ウェブ通信を守る安全な送信のしくみ (5 文字)

7 ヨコ: フアイアウオール 着信する通信を選別する仕組み (8 文字)

8 ヨコ: イビルツイン Wi-Fiに似せた不正なホットスポット (6 文字)

タテのカギ

1 タテ: セキュリテイキカク 最新のWi-Fiの安全性に関する標準 (9 文字)

2 タテ: スニツフイング ネットワークのデータパケットを捕捉すること (7 文字)

3 タテ: トンネル 通信中のデータを通す安全な経路 (4 文字)

5 タテ: ブイピーエヌ 暗号化された仮想プライベートネットワーク (6 文字)

6 タテ: ボウジユ 通信中のトラフィックを読み取ること (4 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. ジボユウ — **ボウジユ**
2. ンイルイツビ — **イビルツイン**
3. ブピーヌエイ — **ブイピーエヌ**
4. テクカリキイセキユ — **セキユリテイキカク**
5. イグフツスンニ — **スニツフイング**
6. ウアゴカン — **アンゴウカ**
7. ネトルン — **トンネル**
8. アアウルフーオイ — **フアイアウオール**

秘密の暗号チャレンジ 解答

"ワイファイヲ ブイピーエヌデ アンゴウカ"

ケーススタディの解答

A ケーススタディ 1: 公衆 Wi-Fi でのパケット盗聴の封じ込め 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: 空港の公共 Wi-Fi ネットワークに接続しているリモートの営業幹部が、平文で送信した機密性の高い業務メールが、送信直後にいくつか漏えいしたことに気づきます。
- 推奨される戦略と解決策: すべてのリモートワークステーションで企業向け VPN クライアントの使用を義務付けます。HTTPS のみを許可するブラウザー拡張機能を適用し、クライアントのファイアウォールで暗号化されていないプロトコル (HTTP や FTP など) をブロックします。

B ケーススタディ 2: イービルツインによる偽ホットスポットへの防御 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: 攻撃者が、正規のカフェのホットスポットを装って 'CoffeeShop_Guest' という名前の不正な無線アクセスポイントを設置し、何も知らない客のネットワークトラフィックを盗み取っています。
- 推奨される対策と解決策: アクセスポイントの BSSID MAC アドレスを監査して、ネットワークの真正性を確認します。クライアントのポスチャ検証を適用してオープンネットワークへの接続をブロックし、機密性の高い作業にはモバイルホットスポットを義務づけます。