名前: 日付: 得点:

リモートアクセス VPN

リモート勤務者のエンドポイントの保護、多要素認証、IPsec トンネルの設定。

リモートアクセス VPN の学習概要

学習者

学生ステータス

ネットワーク防御トラック

安全

接続状況

データパケットを保護すること

有効

漏えい防止

DNSとIPv6の漏えい防止

ようこそ！ このアクティビティ資料では、リモートアクセスVPNネットワークについて学びます。クライアントからサイトへのトンネル、多要素ログイン、エンドポイントのセキュリティ状態チェック、帯域幅の上限、syslogによるセキュリティ監査を取り上げます。

ワークシートのチェックポイント

- [ ] **パート 1-4: VPN とネットワークセキュリティの設定を習得します。**
- [ ] **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 のおすすめ VPN ガイドを開く

URL: https://www.vpn.com/vpn/best-vpn-for-business/remote-access/

あなたのリモートアクセスVPN 学習ロードマップ

- ローカルネットワークのノードにアクセスする、リモート勤務者のエンドポイントを保護すること。
- リモートログインの多要素認証ポリシーを設定してください。
- クライアントからサイトへの IPsec と OpenVPN の設定を行います。
- アクセス制御違反がないか、リモート接続ログを監査します。
- ネットワークへの接続を許可する前に、デバイスの状態チェックを導入する。
- テレワークの帯域幅の詰まりを防ぐため、サーバーのスループットを最適化します。

リモートアクセス VPN 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。学んだ知識をポスチャーチェックと多要素ログインに応用しましょう。 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。

クライアント対サイトのトンネルとエンドポイントのコンプライアンス（導入）

リモートアクセス VPN は、社外の従業員のために、安全なクライアントからサイトへのトンネルを確立します。これらの接続を保護するには、多要素認証 (MFA) によるログインの適用、エンドポイントのポスチャコンプライアンスチェックの実施、中央の syslog コレクターによるログの監査が必要です。

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. リモートアクセスVPNポータルが必須にすべき認証標準は何ですか?
   - A) 多要素
   - B) 単一要素
   - C) 暗号化されていない
   - D) ローカルゲスト

2. リモートワークのクライアントとサイト間の接続を保護するための標準となっているプロトコルはどれですか?
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. 接続前にリモートのノートPCが安全かどうかを確認するチェックは何ですか?
   - A) ポスチャチェック
   - B) 速度テスト
   - C) Pingテスト
   - D) メモリ数

4. セキュリティ監査のために、リモートワーカーの接続ログはどこに保存されますか?
   - A) Syslogサーバー
   - B) レジストリキー
   - C) クライアントのメモリ
   - D) ウェブブラウザー

5. リモートワーカーの数がゲートウェイの帯域幅の容量を超えると、どんな問題が起きますか?
   - A) 帯域幅の絞り込み
   - B) DNSリーク
   - C) ハンドシェイクの通過
   - D) IP の露出

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. 多要素認証は、リモートログインを守るために、第二の検証トークンを追加します。

○ 正しい ○ 誤り

7 質問 7

7. ポスチャチェックにより、ファイアウォールが無効なリモートデバイスがプライベートサーバーにアクセスできてしまいます。

○ 正しい ○ 誤り

8 質問 8

8. リモートアクセス VPN のログは、社内ネットワークへの不正な侵入を追跡するために欠かせません。

○ 正しい ○ 誤り

9 質問 9

9. OpenVPN と IPsec は、リモートクライアントのペイロードを暗号化できない旧式のプロトコルです。

○ 正しい ○ 誤り

10 質問 10

10. ゲートウェイの帯域詰まりは、リモート通信が接続カードの容量を超えると起こります。

○ 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. 企業ポータルを保護するため、リモートログインには _____ が必須です。

2. リモートクライアントは、標準的な _____ プロトコルでトンネルのペイロードを暗号化します。

3. 端末は、ネットワークに接続する前に、セキュリティ _____ チェックに合格する必要があります。

4. 監査可能なアクセスログは、中央の _____ サーバーに継続的に送信されます。

5. 業務時間中のトラフィック増加により、ゲートウェイの _____ が混雑することがあります。

6. 仮想アダプターのドライバーは、WindowsとmacOSでクライアントからサイトへの _____ を処理します。

用語バンク

OpenVPN　Syslog　トンネリング　ファイアウォール　ポスチャ　暗号化　多要素認証　帯域幅

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: 重要概念のマッチング

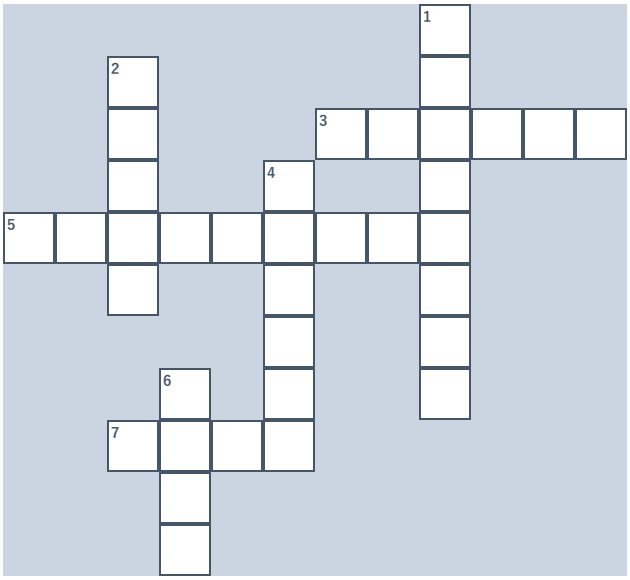
定義マッチング

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. 多要素	A	データを安全な経路にカプセル化すること。
	2. OPENVPN	B	中央のセキュリティログ収集ツール。
	3. ポスチャ	C	ネットワークのデータ容量の上限。
	4. SYSLOG	D	標準的なクライアントからサイトへのプロトコル。
	5. 帯域幅	E	リモートデバイスの状態の検証。
	6. 暗号化	F	通信フィルタリングシステムのルール。
	7. トンネリング	G	パケットの暗号によるスクランブル。
	8. ファイアウォール	H	追加のトークンを必要とするログインセキュリティ。

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

3. ネットワークのデータ容量の上限 (6)

5. 追加のトークンを必要とするログインのセキュリティ (9)

7. セキュリティログを集約する収集サーバー (4)

タテのカギ

1. 通信をフィルタリングするシステムのルール (8)

2. パケットを暗号技術で読み取れない状態にすること (5)

4. データを安全な経路に包んで送ること (6)

6. リモート端末の健全性の検証 (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

3 ヨコ: ネットワークのデータ容量の上限 (6 文字):

5 ヨコ: 追加のトークンを必要とするログインのセキュリティ (9 文字):

7 ヨコ: セキュリティログを集約する収集サーバー (4 文字):

タテのカギ

1 タテ: 通信をフィルタリングするシステムのルール (8 文字):

2 タテ: パケットを暗号技術で読み取れない状態にすること (5 文字):

4 タテ: データを安全な経路に包んで送ること (6 文字):

6 タテ: リモート端末の健全性の検証 (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。

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

タヨウソニンシヨウ　プロトコル　ポスチヤ　シスログ　タイイキハバ　アンゴウカ
トンネリング　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
A. タヨウソニンショウ
B. プロトコル
C. ポスチヤ
D. シスログ
E. タイイキハバ
F. アンゴウカ
G. トンネリング
H. フアイアウオール

定義とマッチ欄
1. セキュリティログを集約する収集サーバー。
2. 通信をフィルタリングするシステムのルール。
3. データを安全な経路に包んで送ること。
4. パケットを暗号技術で読み取れない状態にすること。
5. クライアントからサイトへの接続で標準的に使われる通信規約。
6. ネットワークのデータ容量の上限。
7. リモート端末の健全性の検証。
8. 追加のトークンを必要とするログインのセキュリティ。

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、このワークシートの重要な概念を見つけましょう。答えは用意された入力欄に書いてください。

1. ンニソヨタシヨウウ
2. ポチヤス
3. タイキバハイ
4. グリネントン
5. トルプコロ
6. ログシス
7. ウカアゴン
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	VPNに関する誤解			
2	ゼロトラストを表す言葉			
3	知っているオフィスソフト			
4	安全なリモートワークのルール			
5	インターネットプロバイダーが見られるもの			
6	知っているVPNサービス			
7	従業員が働く場所			
8	会社が毎日使うツール			
9	IT部門の役割			
10	従業員が持っているかもしれないデバイス			
11	会社が守らなければならないデータ			
12	セキュリティ侵害の後にすること			
13	ビデオ会議の妨げになるもの			
14	安全にログインする方法			
15	従業員にVPNを提供する理由			

チェックポイント 8: VPN とネットワークのケーススタディ

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: MFA の義務化



シナリオ: ビジネスアナリストが、リモートワーク中に会社のデータベースにログインしようとします。ユーザー名とパスワードは正しく入力しましたが、VPNポータルがアクセスをブロックし、物理トークンのコードを要求します。

ディスカッションの問い: どのセキュリティポリシーが、この二重の確認手順を強制していますか。

ケーススタディ 2: ポスチャのコンプライアンス



シナリオ: 請負業者が、個人のノートパソコンをリモートの社内ネットワークに接続します。VPNクライアントは直ちに接続を切断し、アンチウイルスの定義ファイルが古いことをユーザーに通知します。

ディスカッションの問い: この接続の試みをブロックしたのは、VPNゲートウェイのどのような専用チェックですか？

チェックポイント 9: 暗号を解読しよう

ネットワークエンジニアは、ルーティングチャネルとクライアントトンネルを守ります。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

40	35	72	20	60		7	48	38	3	25		16	46	31	18	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: VPN FAQ – 基礎 (パート A)

仮想プライベートネットワーク (VPN) とトンネリングに関する、最もよくある質問と回答を確認しましょう。

Q1: リモートアクセス VPN とは何ですか?

外出先で働く従業員が、社内のプライベートサーバーに直接接続できるようにする安全な接続方法。

Q2: クライアント対サイトはサイト間とどう違いますか?

クライアント対サイトは個々のユーザーのデバイスを接続し、サイト間接続は物理的なオフィス拠点全体を結びます。

Q3: デバイスポスチャチェックとは何ですか?

アクセスを許可する前に、リモートデバイスのセキュリティ状態(ウイルス対策、OSのパッチレベル)を確認するスキャン。

Q4: リモートアクセスに OpenVPN が使われるのはなぜですか?

強力なセキュリティプロトコル、クロスプラットフォーム対応、個々の接続を処理できる能力があるためです。

Q5: MFA はリモートアクセスをどう守りますか?

2 つ目の認証トークンを追加するため、従業員のパスワードが漏えいしたり盗まれたりしても、アクセスを防げます。

チェックポイント 10: VPN FAQ – 基礎 (パート B)

仮想プライベートネットワーク (VPN) とトンネリングに関する、最もよくある質問と回答を確認しましょう。

Q6: syslog サーバーとは何ですか?

コンプライアンス監査のために、接続イベント、ログイン、システムアラートを保存する一元的なログリポジトリ。

Q7: 帯域幅が詰まる原因は何ですか?

リモート勤務の従業員の合計帯域幅の需要が、社内ゲートウェイのインターネット速度の上限を超える場合。

Q8: 自宅のコンピューターを職場の VPN に接続できますか?

デバイスが社内のポスチャチェック監査に合格し、IT 管理者に承認されている場合のみです。

Q9: ネットワークのカプセル化とは何ですか?

安全に送信するために、転送中のデータパケットを暗号化されたプロトコルヘッダーの中に包み込むこと。

Q10: スプリットトンネリングはリモートアクセスをどのように最適化しますか?

従業員は、通常の閲覧には地元の ISP を使いつつ、業務関連のファイルは VPN 経由でルーティングできます。

チェックポイント 10: VPN FAQ – 応用（パート C）

VPNトンネリングプロトコル、モバイルクライアントとの連携、企業での展開について、高度な技術的側面を探ります。

Q1: 証明書ベースの認証は、リモートアクセスをどのように強化しますか?

接続の権限を、事前にインストールされたローカルのデジタル証明書に紐づけ、管理されていない、または許可されていないデバイスを遮断します。

Q2: リモートワークでスプリットトンネリングを使うと、どのようなセキュリティリスクがありますか?

侵害されたローカルデバイスが、外部からの脅威をプライベートネットワークへ中継できる、橋渡しの可能性が生まれます。

Q3: ポスチャチェックはレジストリ設定をどのように検査しますか?

このVPNクライアントはローカルスクリプトを実行し、レジストリのパスを調べて、企業のセキュリティソフトが動作しているかを確認します。

Q4: syslog が初期設定で UDP ポート 514 を使うのはなぜですか?

最小限のオーバーヘッドでログを素早く送信するためですが、現在の安全な構成ではTCP上のTLSカプセル化が必須です。

Q5: 企業はゲートウェイの帯域幅のボトルネックをどう解消しますか?

ロードバランサーを導入し、リモートトラフィックをリージョンのサーバーノードに分散することによって。

チェックポイント 10: VPN FAQ – 応用 (パート D)

VPNトンネリングプロトコル、モバイルクライアントとの連携、企業での展開について、高度な技術的側面を探ります。

Q6: リモートクライアントの仮想 TAP/TUN アダプターの機能は何ですか?

それらは仮想ネットワークカードとして機能し、デバイスレベルのTCP/IP通信を暗号化されたVPNトンネルへ直接ルーティングします。

Q7: IKEv2 MOBIKE はリモートワーカーの移動をどう支えますか?

IP アドレスのバインディングを動的に更新し、ユーザーが Wi-Fi とモバイルデータの間を移動しても VPN を有効に保ちます。

Q8: スプリットトンネルとフルトンネルのルーティングの違いは何ですか?

フルルーティングはデバイスのすべてのインターネット通信を VPN 経由にしますが、スプリットルーティングは社内の宛先 IP の通信だけを送ります。

Q9: NAT デバイスはリモートの VPN 接続をどう処理しますか?

ローカルのポート範囲をパブリックゲートウェイのIPアドレスにマッピングし、戻ってくる暗号化データパケットをルーティングすることによって。

Q10: どのコンプライアンス基準がリモートアクセスの監査を義務付けていますか?

HIPAA、SOC 2、PCI DSS などの基準では、すべてのリモート接続セッションのログ記録と監視が求められます。

パート 11: 実世界の VPN の事実10選と洞察

VPN の暗号化の速度、プロトコルの監査、モバイル接続、企業のリモートワークに関する実際の事実を確認しましょう。

1. VPN の洞察

リモートアクセス VPN は、社外で働く従業員のために、安全なクライアントからサイトへのトンネルを確立します。

2. VPN の洞察

多要素認証は、リモートの業務ポータルを保護するため、コンプライアンス規則で求められています。

3. VPN の洞察

ポスチャチェックは、プライベートネットワークへのアクセスを許可する前に、ローカルクライアントのセキュリティ設定を確認します。

4. VPN の洞察

Syslog サーバーは、接続ログを集約して、不正なアクセスの試みを監査し、検出します。

5. VPN の洞察

ゲートウェイの帯域詰まりは、リモート通信の合計需要がサーバーのインターネット上限を超えると起こります。

6. VPN の洞察

仮想ネットワークアダプターは、オペレーティングシステムのネットワーククエリを、安全なプロトコルの中にカプセル化します。

7. VPNの豆知識

MOBIKE のサポートにより、リモートクライアントは VPN トンネルを切断せずにネットワークを切り替えられます。

8. VPNの豆知識

フルトンネルのルーティングは、従業員のすべてのインターネット通信を保護しますが、社内ゲートウェイの負荷が増えます。

9. VPNの豆知識

証明書認証は、VPN 接続の承認を企業が管理するハードウェアに直接結び付けます。

10. VPN の洞察

SOC 2 や PCI DSS などのフレームワークでは、リモートアクセスセッションのログ記録と監視が求められます。

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、世界の技術標準、仕様、規制の枠組みをもとに作成されています。

学術・業界の参考資料

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

解答: チェックポイント 1 – 多肢選択

1 **ログイントークン** MFA セキュリティ 正解: A

指導メモ

多要素認証は、ログインに第二の検証を義務づけます。出典: MFA Implementation。

2 **OpenVPN トンネル** クライアント対サイト 正解: A

指導メモ

OpenVPN は、クライアントとサイト間のトンネルを保護するための標準的なプロトコルです。 出典: OpenVPN Client.

3 **ポスチャ監査** デバイスチェック 正解: A

指導メモ

ポスチャチェックは、エンドポイントでファイアウォールとウイルス対策ツールが有効かどうかをスキャンします。 出典: Posture Compliance.

4 **ログ集約ツール** SYSLOG サーバー 正解: A

指導メモ

Syslog サーバーは、セキュリティイベントのログを収集して、アクセス違反を監視します。出典: Syslog Standard。

5 **カードの限度超過** ゲートウェイの帯域詰まり 正解: A

指導メモ

ゲートウェイの帯域詰まりは、ユーザーの通信がサーバーの上限を超えると起こります。出典: Capacity Planning。

解答: チェックポイント 2 – 正誤問題

6 ログイントークン

MFA チェック

正解: 正しい

指導メモ

多要素認証は、ログインに第二の検証を義務づけます。出典: MFA Implementation。

7 問題 7

正解: 誤り

指導メモ

ポスチャーチェックは、ファイアウォールやアンチウイルスがオフのデバイスをブロックするため、そのようなデバイスは拒否されます。

8 ログ集約ツール

SYSLOG サーバー

正解: 正しい

指導メモ

Syslog サーバーは、セキュリティイベントのログを収集して、アクセス違反を監視します。出典: Syslog Standard。

9 問題 9

正解: 誤り

指導メモ

OpenVPNとIPsecは、リモートクライアントの通信を暗号化する現行のプロトコルです。

10 カードの限度超過

ゲートウェイの帯域詰まり

正解: 正しい

指導メモ

ゲートウェイの帯域詰まりは、ユーザーの通信がサーバーの上限を超えると起こります。出典: Capacity Planning。

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. 多要素	D 2. OPENVPN	E 3. ポスチャ	B 4. SYSLOG
C 5. 帯域幅	G 6. 暗号化	A 7. トンネリング	F 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 多要素認証	2 OpenVPN	3 ポスチャ	4 Syslog
5 帯域幅	6 トンネリング		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 D – シスログ	2 H – フアイアウオール	3 G – トンネリング	4 F – アンゴウカ
5 B – プロトコル	6 E – タイイキハバ	7 C – ポスチヤ	8 A – 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:
生徒が多要素、OPENVPN、ポスチャ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。

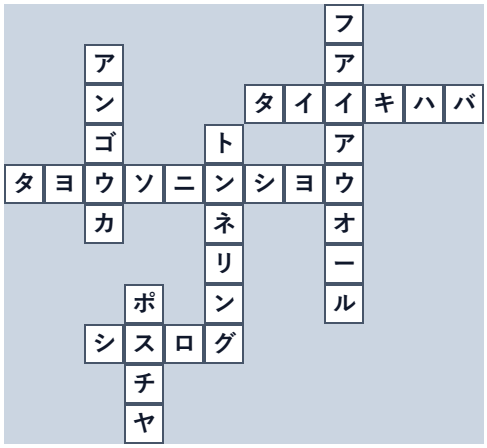
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

3 ヨコ: タイイキハバ ネットワークのデータ容量の上限 (6 文字)

5 ヨコ: タヨウソニンシヨウ 追加のトークンを必要とするログインのセキュリティ (9 文字)

7 ヨコ: シスログ セキュリティログを集約する収集サーバー (4 文字)

タテのカギ

1 タテ: フアイアウオール 通信をフィルタリングするシステムのルール (8 文字)

2 タテ: アンゴウカ パケットを暗号技術で読み取れない状態にすること (5 文字)

4 タテ: トンネリング データを安全な経路に包んで送ること (6 文字)

6 タテ: ポスチヤ リモート端末の健全性の検証 (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. ンニソヨタシヨウウ — **タヨウソニンシヨウ**
2. ポチヤス — **ポスチヤ**
3. タイキバハイ — **タイイキハバ**
4. グリネントン — **トンネリング**
5. トルプコロ — **プロトコル**
6. ログシス — **シスログ**
7. ウカアゴン — **アンゴウカ**
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

"リモートデ キギョウノ タンマツヲ マモル"

ケーススタディの解答

A ケーススタディ 1: MFA の義務化

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: ビジネスアナリストが、リモートで作業中に社内データベースにログインしようとします。正しいユーザー名とパスワードを入力しましたが、VPN ポータルはアクセスをブロックし、物理トークンのコードを要求します。
- 推奨される戦略と解決策: 社内の VPN ポータルは、リモートログインを保護するために、厳格な多要素認証 (MFA) ポリシーを適用しています。

B ケーススタディ 2: ポスチャのコンプライアンス

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: 契約社員が、自分のノートパソコンをリモートの社内ネットワークに接続します。VPN クライアントはすぐに接続を切断し、ウイルス対策の定義ファイルが古いことをユーザーに通知します。
- 推奨される戦略と解決策: リモートアクセスゲートウェイがエンドポイントのポスチャチェックを実行し、セキュリティ設定が古いためにそのデバイスをブロックしました。