名前: 日付: 得点:

最も安全な VPN ガイド

高セキュリティな VPN 設計、RAM 専用の揮発性メモリサーバー、ゼロトラストのアクセスセキュリティ、プライベートな暗号化 DNS の漏えい対策、監査済みの WireGuard 設定についての技術的な分析。

最も安全な VPN ガイド 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、高度に安全なVPNの技術基準について学びます。RAMのみのサーバーハードウェア、ゼロトラストのアクセスセキュリティ、プライベートな暗号化DNSリゾルバー、監査済みのWireGuard構成を取り上げます。

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/most-secure-vpn/

あなたの最も安全なVPN 学習ロードマップ

- 最も安全なVPNガイドの技術的なアーキテクチャと暗号化標準を分析してください。
- IP、DNS、WebRTC のトラフィックが漏れないよう、クライアントの設定を構成してください。
- 独自のトンネリングプロトコルと標準的な実装を比較してください。

最も安全な VPN ガイド 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RAMのみのサーバーハードウェアとゼロトラストシステムに応用しましょう。 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。

RAM 専用インフラとゼロトラストネットワーク(導入)

本当に安全なVPNは、ゼロトラストの枠組み、ログがディスク押収で露出するのを防ぐRAM専用サーバー、プライベートな暗号化DNSリゾルバー、WireGuardのような監査済みプロトコルに支えられています。これらの対策を組み合わせることで、価値の高いデジタル資産を傍受の脅威から守ります。

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. 最新のVPNサーバーで最高レベルのセキュリティを確保するうえで根幹となるアーキテクチャはどれですか?

- A) RAM専用のサーバーインフラ
- B) ディスクベースのストレージ
- C) 動的DNSルーティング
- D) ポート転送の有効化

2. 最も安全で最新のVPN設定向けに、広く推奨されているプロトコルは何ですか?

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3. 例外なくすべての接続を継続的に検証することを求めるセキュリティフレームワークはどれですか?

- A) ゼロトラストアーキテクチャ
- B) 境界ファイアウォール
- C) 動的ルーティング
- D) 共有秘密鍵

4. VPNクライアントのDNSリーク保護の主な役割は何ですか?

- A) すべてのDNSリクエストをプライベートな暗号化リゾルバー経由にする
- B) IPパケットを難読化する
- C) DNSクエリをローカルにキャッシュする
- D) ネームサーバーを無効にする

5. マルチホップのルーティングは、VPN トンネル全体のセキュリティをどのように高めますか?

- A) 2台の別々のサーバーを直列に経由してデータを送る
- B) 圧縮速度が上がる
- C) 低セキュリティの暗号でデータを暗号化する
- D) ファイアウォールを迂回する

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. RAM 専用サーバーはログファイルを一時的なメモリに保存し、再起動すると消去されます。

○ 正しい ○ 誤り

7 質問 7

7. WireGuardは、速度のボトルネックになりにくい最新の暗号アルゴリズムを使います。

○ 正しい ○ 誤り

8 質問 8

8. VPNキルスイッチは、トンネルが切れたときにすべてのネットワーク通信をブロックして働きます。

○ 正しい ○ 誤り

9 質問 9

9. 独立した第三者による監査は、セキュリティに関する約束を検証するうえで関係ありません。

○ 正しい ○ 誤り

10 質問 10

10. ゼロトラストモデルは、社内ネットワークのすべての接続をデフォルトで安全とみなします。

○ 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. 管理者は、厳格な _____ の枠組みを導入してセキュリティを徹底します。
2. 複数の入口を経由してパケットを送るには、安全な _____ 構成が必要です。
3. 盗まれたドライブからのデータ漏えいを防ぐため、 _____ の設計を採用します。
4. ISPによる乗っ取りは、ネイティブの _____ 機能を設定することで軽減できます。
5. 接続障害のときに通信を遮断するには、 _____ の仕組みを有効にします。
6. 保存されるデータベースログを最小限にするには、完全に _____ された事業者を選びます。

用語バンク

DNS保護　RAM専用サーバー　キルスイッチ　ゼロトラスト　ネームサーバー　マルチホップ　暗号化　監査済み

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: VPN とネットワークの概念マッチング

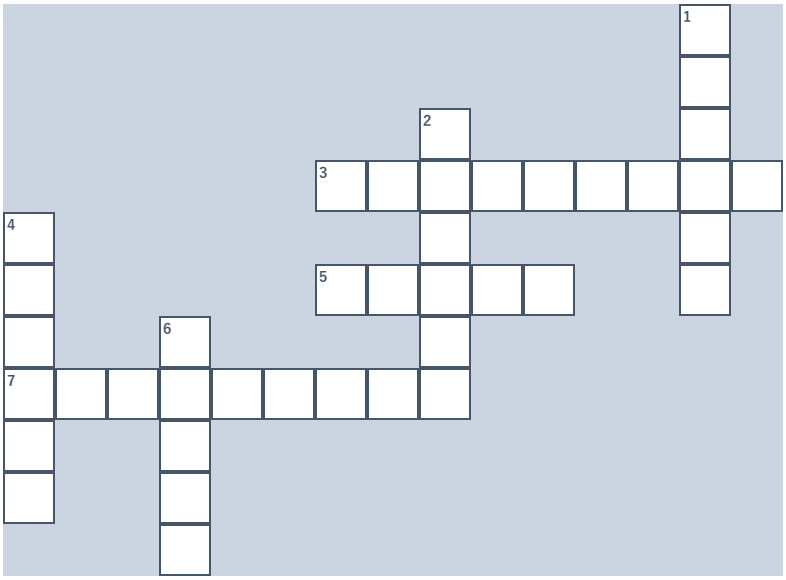
定義マッチング

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. ゼロトラスト	A	ログが保存されていないことを確認した、独立して検査された構成。
2. マルチホップ	B	通信中のデータを保護するための、データペイロードの暗号によるスクランブル。
3. RAM 専用サーバー	C	すべてのユーザーに継続的な認証を求めるセキュリティの枠組み。
4. DNS保護	D	データをどのようにまとめて送信するかを決める、一連の技術的なルール。
5. キルスイッチ	E	2 つのサーバーノードを連鎖させるカスケード型の VPN ルーティング。
6. 監査済みシステム	F	データのペイロードを保存するために揮発性メモリを利用するサーバー構成。
7. 暗号化	G	ネームサーバーの検索を守るために、プライベートDNSクエリを強制すること。
8. プロトコル	H	VPNが失敗した場合にトラフィックをブロックする、フェイルセーフの仕組み。

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. ネームサーバーの検索を守るため、非公開のDNSクエリを徹底すること (9)

5. ログが保存されていないことを確認した、独立した検査を受けた構成 (5)

7. 揮発性メモリにデータを保存するサーバーの構成 (9)

タテのカギ

1. 2つのサーバーノードを連結してつなぐ、段階式のVPNルーティング (6)

2. ドメイン名の問い合わせを受け付けるサーバー (6)

4. すべてのユーザーに継続的な認証を求めるセキュリティの枠組み (6)

6. 通信中のデータを守るため、ペイロードを暗号で読み取れなくすること (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

3 ヨコ: ネームサーバーの検索を守るため、非公開のDNSクエリを徹底すること (9 文字):

5 ヨコ: ログが保存されていないことを確認した、独立した検査を受けた構成 (5 文字):

7 ヨコ: 揮発性メモリにデータを保存するサーバーの構成 (9 文字):

タテのカギ

1 タテ: 2つのサーバーノードを連結してつなぐ、段階式のVPNルーティング (6 文字):

2 タテ: ドメイン名の問い合わせを受け付けるサーバー (6 文字):

4 タテ: すべてのユーザーに継続的な認証を求めるセキュリティの枠組み (6 文字):

6 タテ: 通信中のデータを守るため、ペイロードを暗号で読み取れなくすること (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。

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

用語リスト

ゼロトラスト　マルチホツプ　ラムセンヨウサーバ　デイーエヌエスホゴ　キルスイツチ
カンサズミ　アンゴウカ　ネームサーバ

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. ゼロトラスト
B. マルチホップ
C. ラムセンヨウサーバ
D. デイーエヌエスホゴ
E. キルスイツチ
F. カンサズミ
G. アンゴウカ
H. ネームサーバ

定義とマッチ欄
1. VPNが切れたときに通信を遮断するフェイルセーフの仕組み。
2. ネームサーバーの検索を守るため、非公開のDNSクエリを徹底すること。
3. 2つのサーバーノードを連結してつなぐ、段階式のVPNルーティング。
4. ドメイン名の問い合わせを受け付けるサーバー。
5. 通信中のデータを守るため、ペイロードを暗号で読み取れなくすること。
6. 揮発性メモリにデータを保存するサーバーの構成。
7. ログが保存されていないことを確認した、独立した検査を受けた構成。
8. すべてのユーザーに継続的な認証を求めるセキュリティの枠組み。

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、仮想プライベートネットワーク(VPN)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. トゼラストロ
2. バラーンムウサヨセ
3. キスイチツル
4. ゴカウアン
5. ホチプマツル
6. ホエイスエデヌゴー
7. ズミカサン
8. ムバネーサー

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	毎日使う鍵やロック			
2	VPNが隠せるもの			
3	VPNを安全にするもの			
4	VPNに関する誤解			
5	旅行中にVPNを使う理由			
6	現実世界の安全な場所			
7	「保護された」を意味する言葉			
8	優れたVPNプロバイダーが約束すること			
9	プライバシーに関連する言葉			
10	監査や検査の種類			
11	このワークシートで覚えておきたい言葉			
12	ハッカーが盗みたいもの			
13	偽のWi-Fiネットワークを見抜く方法			
14	VPNを使う場所			
15	インターネットプロバイダーが見られるもの			

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: 企業インフラの強化



シナリオ: 企業向け銀行が、リモートアクセスのトポロジーを再設計しています。すべてのクライアントデバイスを安全なサーバーに結びつける、ゼロトラストアーキテクチャが必要です。

ディスカッションの問い: ゼロトラストVPNモデルにおけるネットワークのマイクロセグメンテーションの主なメリットは何ですか？

ケーススタディ 2: RAM のみのサーバーによる保護



シナリオ: セキュリティを重視するVPNプロバイダーが、物理的なサーバーの押収によってユーザーのログ履歴が露出しないよう、サーバーをアップグレードしています。

ディスカッションの問い: RAMのみのハードウェア構成は、物理的なサーバーの押収時に、フォレンジックによるデータの抽出をどのように防ぎますか？

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

53	37	3	38	3	21		12	11	46	45		1	46	55	46	22		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: VPN が「最も安全」といえる条件は何ですか?

ゼロトラスト、RAM専用サーバー、監査済みプロトコルの組み合わせ。

Q2: RAM のみのサーバーとは何ですか?

揮発性メモリ上で動作し、ディスクにログを一切保存しないように設計されたサーバー。

Q3: ゼロトラスト VPN とは何ですか?

すべてのアクセスリクエストと接続を継続的に検証するフレームワーク。

Q4: WireGuard が安全と考えられているのはなぜですか?

コードベースが小さく監査しやすく、最新の暗号を使っています。

Q5: 安全な VPN は DNS リークをどう防ぎますか?

すべてのクエリを、プライベートで暗号化されたDNSリゾルバー経由にすることによって。

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: 安全な VPN には監査が必要ですか?

はい、独立した監査により、ログを取らないという主張とコードの安全性が検証されています。

Q7: キルスイッチの役割は何ですか?

VPN 接続が切断された場合、ただちにネットワーク通信を停止します。

Q8: 安全な VPN ではどの暗号化が使われていますか?

AES-256とChaCha20は、暗号化の業界標準です。

Q9: マルチホップルーティングは安全ですか?

はい、2台以上のサーバーを連結して、トラフィック分析を防ぎます。

Q10: オフショアの管轄はどのように役立ちますか?

適用される法律を限定することはあっても、絶対的な免責は得られません。

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: RAM のみのサーバーは、データ押収のリスクをどのように防ぎますか?

RAM上で動作するため、電源プラグを抜くとメモリ内のデータは消去されるためです。

Q2: ゼロトラストは、標準的な境界型セキュリティをどのように置き換えますか?

すべてのクライアントを敵対的なものとして扱い、継続的な認証を求めます。

Q3: WireGuard のコードベースが監査しやすいのはなぜですか?

Linux 用のコードは 4,000 行未満で、一般的な VPN スタックよりはるかに小さくなっています。 [4]

Q4: DNSSEC は DNS クエリをどう保護しますか?

DNS レコードに署名し、リゾルバーが偽造または改ざんされた応答を検出できるようにします。

Q5: マルチホップはトラフィックの相関分析をどう難しくしますか?

受信側と送信側のIPを異なるホスティングプロバイダーに分けることによって。

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: ファイブアイズの法域が VPN にとってリスクとなるのはなぜですか?

加盟国は情報を共有しており、法的命令を使ってユーザーデータの提供を求めることがあります。

Q7: キルスイッチはカーネルレベルでどう実装されますか?

システムのファイアウォールルール(iptables や WFP など)を使って、外向きの通信を遮断します。

Q8: VPN のハンドシェイクにおける前方秘匿性とは何ですか?

固有のセッション鍵を生成するため、過去のセッションを復号できなくなります。

Q9: 安全な VPN は WebRTC リークをどう軽減しますか?

WebRTCリクエストをブロックするか、トンネル経由にすることによって。

Q10: 独立した監査は、プライバシーコンプライアンスをどのように確保しますか?

監査人はペネトレーションテストを実施し、サーバー設定を検査します。

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

RAM 専用サーバーは起動時にオペレーティングシステムをメモリに読み込むため、再起動後はディスクに何も残りません。

2. VPN の洞察

WireGuardは、Noiseフレームワークと、Curve25519、ChaCha20、Poly1305、BLAKE2s、HKDFを使います。 [3]

3. VPN の洞察

ゼロトラストはリソースごとにアクセスを許可し、ネットワーク上の場所に基づく暗黙の信頼を与えません (NIST SP 800-207)。 [1]

4. VPN の洞察

ファイブ・アイズ情報同盟には、米国、英国、カナダ、オーストラリア、ニュージーランドが含まれます。

5. VPN の洞察

WebRTCリークは、ブラウザーがSTUNクエリを通じてクライアントの実際のパブリックIPアドレスを明らかにしたときに発生します。

6. VPN の洞察

完全前方秘匿性（PFS）は、長期鍵が漏えいしても、過去のセッション鍵が露出しないようにします。 [3]

7. VPNの豆知識

ベルリンに拠点を置くセキュリティ企業の Cure53 は、複数の VPN プロバイダーの監査結果を公開しています。

8. VPNの豆知識

DNSリークは、DNSクエリがVPNトンネルを迂回して、ローカルISPのネームサーバーに送られるときに起こります。

9. VPNの豆知識

揮発性RAMチップは、データを保持するために常に電力が必要で、電源を切ると内容が失われます。

10. VPN の洞察

企業のゼロトラストシステムは、保護されたリソースへの接続を許可する前に、デバイスの状態チェックを実施します。 [1]

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

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

解答: チェックポイント 1 – 多肢選択

1 **RAM 専用サーバー** RAM 専用 正解: A

指導メモ

RAM 専用サーバーはログをディスクに保存せず、再起動するとデータが消去されます。出典: Most Secure VPN。

2 **問題 2** 正解: A

指導メモ

WireGuardは、小規模で監査しやすいコードベースと最新の暗号を組み合わせています。

3 **ゼロトラストモデル** ゼロトラスト 正解: A

指導メモ

ゼロトラストモデルは、アクセスを許可する前に、機器のコンプライアンスを継続的に検証します。出典: Most Secure VPN。

4 **DNS保護** DNS保護 正解: A

指導メモ

DNSリーク防止は、名前解決のクエリをプライベートリゾルバー経由で送信します。出典: Most Secure VPN。

5 **マルチホップトンネル** マルチホップ 正解: A

指導メモ

マルチホップルーティングは、2 つの別々のサーバーノードを直列につなぎます。出典: Most Secure VPN。

解答: チェックポイント 2 – 正誤問題

6 **RAM 専用サーバー** RAM 専用 正解: 正しい

指導メモ

RAM 専用サーバーのハードウェアはディスクにデータを書き込まず、再起動すると消去されます。出典: Most Secure VPN。

7 **WireGuardの速度** WIREGUARD 正解: 正しい

指導メモ

WireGuardは、処理のボトルネックを避けられる最新の暗号を使います。出典: Most Secure VPN。

8 **キルスイッチ** フェイルセーフスイッチ 正解: 正しい

指導メモ

キルスイッチは、VPN接続が切れたときにすべての通信をブロックします。出典: Most Secure VPN。

9 **第三者監査** 監査は不可欠 正解: 誤り

指導メモ

企業のプライバシーに関する主張を検証するには、第三者監査が欠かせません。出典: Most Secure VPN。

10 **問題 10** 正解: 誤り

指導メモ

ゼロトラストは、ネットワーク上の位置に基づく暗黙の信頼を一切与えません。

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

C 1. ゼロトラスト	E 2. マルチホップ	F 3. RAM 専用サーバー	G 4. DNS保護
H 5. キルスイッチ	A 6. 監査済みシステム	B 7. 暗号化	D 8. プロトコル

チェックポイント 3: 解答 – 重要用語

1 ゼロトラスト	2 マルチホップ	3 RAM専用サーバー	4 DNS保護
5 キルスイッチ	6 監査済み		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 E – キルスイツチ	2 D – デイーエヌエスホゴ	3 B – マルチホツプ	4 H – ネームサーバ
5 G – アンゴウカ	6 C – ラムセンヨウサーバ	7 F – カンサズミ	8 A – ゼロトラスト

指導者向けディスカッションメモ

重要用語:
生徒がゼロトラスト、マルチホップ、RAM 専用サーバー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。

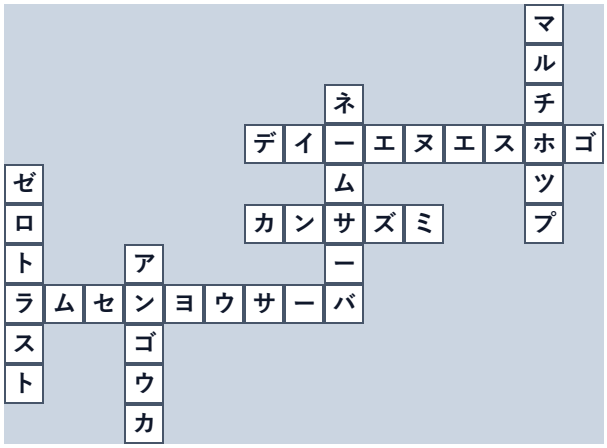
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: デイーエヌエスホゴ ネームサーバーの検索を守るため、非公開のDNSクエリを徹底すること (9 文字)

5 ヨコ: カンサズミ ログが保存されていないことを確認した、独立した検査を受けた構成 (5 文字)

7 ヨコ: ラムセンヨウサーバ 揮発性メモリにデータを保存するサーバーの構成 (9 文字)

タテのカギ

1 タテ: マルチホツプ 2つのサーバーノードを連結してつなぐ、段階式のVPNルーティング (6 文字)

2 タテ: ネームサーバ ドメイン名の問い合わせを受け付けるサーバー (6 文字)

4 タテ: ゼロトラスト すべてのユーザーに継続的な認証を求めるセキュリティの枠組み (6 文字)

6 タテ: アンゴウカ 通信中のデータを守るため、ペイロードを暗号で読み取れなくすること (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. トゼラストロ — ゼロトラスト
2. バラーンムウサヨセ — ラムセンヨウサーバ
3. キスイチツル — キルスイツチ
4. ゴカウアン — アンゴウカ
5. ホチプマツル — マルチホツプ
6. ホエイスエデヌゴー — デイーエヌエスホゴ
7. ズミカサン — カンサズミ
8. ムバネーサー — ネームサーバ

秘密の暗号チャレンジ 解答

"ジュウヨウナ シサンヲ アンゼンニ マモル"

ケーススタディの解答

A ケーススタディ 1: 企業インフラの強化 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: ある企業の銀行が、リモートアクセスのトポロジーを再設計しています。すべてのクライアントデバイスを安全なサーバーに結び付ける、ゼロトラストアーキテクチャが必要です。
- 推奨される戦略と解決策: 採点のポイント: マイクロセグメンテーションは特定のリソースへのアクセスを制限し、デバイスが侵害されても脅威が横方向に広がるのを防ぐことを説明している。

B ケーススタディ 2: RAM のみのサーバーによる保護 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: セキュリティ重視の VPN プロバイダーが、サーバーを物理的に押収されてもユーザーのログ履歴が露出しないように、サーバーをアップグレードしています。
- 推奨される戦略と解決策: 採点のポイント: RAM-Only サーバーには物理ディスクの記憶領域がなく、電源が失われると揮発性メモリ内の一時的なデータがすべて自動的に消去されることを詳しく説明している。