名前: 日付: 得点:

Mullvad セキュリティ

ディスクレスのRAM専用サーバー、監査済みのゼロログポリシー、ローカルでの鍵生成、WireGuard暗号化、量子耐性トンネル構成を含む、Mullvad VPNのセキュリティアーキテクチャを分析してください。

Mullvad セキュリティ 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、Mullvadのセキュリティアーキテクチャについて学びます。ディスクレスのRAMのみのサーバー、監査済みのノーログポリシー、ローカルでの鍵生成、量子コンピューター耐性のあるトンネルを取り上げます。

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/mullvad/security/

あなたのMullvadセキュリティ 学習ロードマップ

- Mullvadセキュリティの技術的なアーキテクチャと設定ルール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。
- カスタム料金、トライアル、性能の特徴を標準モデルと比較してください。

Mullvad セキュリティガイド 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Mullvadのプライバシー重視のサーバー制御に応用しましょう。 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。

匿名性重視のインフラとRAMプランの評価(入門)

Mullvad は、パスワード付きの標準的なアカウントを使わず、ランダムに生成された 16 桁のコードに依存しています。インフラはディスクレスの RAM のみのノード、ローカルで生成される WireGuard 鍵、監査済みのデータ非保持ポリシーで構成されています。

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. Mullvadのアプリでデフォルトとなっているトンネリングプロトコルはどれですか?

- A) OpenVPN
- B) WireGuard
- C) IKEv2
- D) PPTP

2. Mullvadで新しいアカウントを作成するには何が必要ですか？

- A) 何も必要ありません
- B) メールアドレス
- C) 電話番号
- D) 身分証明書

3. 量子コンピューターから守る暗号トンネルはどれですか?

- A) AES-256-GCM
- B) Quantum WireGuard
- C) RSA-4096
- D) SOCKS5 プロキシ

4. WebRTCリークの危険を防ぐセキュリティの仕組みは何ですか?

- A) ブラウザー拡張機能
- B) ネットワークキルスイッチ
- C) WebRTCをVPNインターフェース経由でルーティングすること
- D) スプリットトンネリング

5. 複数のノードを経由してトラフィックを送るマルチホップ機能はどれですか?

- A) 二重NAT
- B) WireGuardマルチホップ
- C) Chameleonプロトコル
- D) Bypasser

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. Mullvad では、アカウントの生成時にメールアドレスが必要です。

◯ 正しい ◯ 誤り

7 質問 7

7. SOCKS5 プロキシは、Mullvad のトンネル内で構成できます。

◯ 正しい ◯ 誤り

8 質問 8

8. Mullvad は、自社のサーバーハードウェアをすべて所有し、運用しています。

◯ 正しい ◯ 誤り

9 質問 9

9. Network Kill Switchは、デフォルトで常に有効です。

◯ 正しい ◯ 誤り

10 質問 10

10. 郵送した現金での支払いは、まったく返金できません。

◯ 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. Mullvadは、主な高速セキュアトンネルプロトコルとして _____ に依存しています。

2. 2つのサーバー拠点を経由してデータを送ることは、 _____ 構成と呼ばれます。

3. ディスク上のログを防ぐため、Mullvadは _____ の専用ノードを導入しています。

4. トンネルが切れるとシステムの通信は、内蔵の _____ フェイルセーフによって遮断されます。

5. 監査報告書により、Mullvadが厳格で検証済みの _____ 構造を維持していることが確認されています。

6. アプリ内部のルーティングは、独自の _____ 設定で分離できます。

7. ポストクォンタム暗号のアルゴリズムは、 _____ トンネルの内側でデータを保護します。

8. 専用のネームサーバーが世界中に配置され、危険な _____ の脅威をブロックします。

用語バンク

DNSリーク　RAM専用　SOCKS5　WireGuard　キルスイッチ　キルスイツチ　ノーログ　マルチホップ　マルチホツプ　量子

ここに答えを書いてください:

1.
2.
3.
4.
5.
6.
7.
8.

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

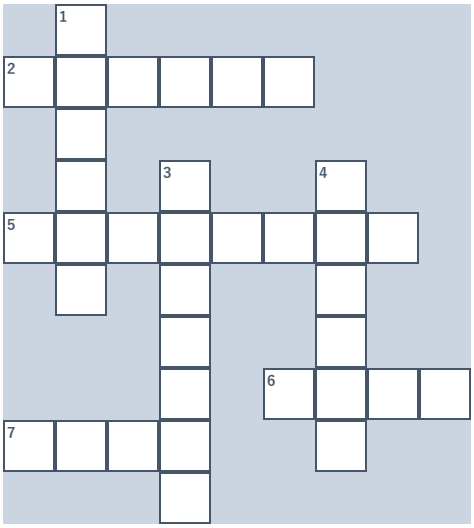
定義マッチング

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. WireGuard	A	VPNが切れたときに通信を遮断する安全機能。
	2. マルチホップ	B	軽量で高性能な安全なトンネリングプロトコル。
	3. RAM専用	C	クライアントアプリケーションを隔離するために使われる内部プロキシプロトコル。
	4. キルスイッチ	D	入口と出口のサーバーノードを経由して通信すること。
	5. ノーログ	E	量子攻撃に耐えるよう設計された暗号化の仕組み。
	6. ソックスファイブ	F	VPNトンネルの外でのDNSクエリの宛先の露出。
	7. ポストリヨウシ	G	再起動時にデータを一切保持しない揮発性メモリのサーバーハードウェア。
	8. DNSリーク	H	独立した監査で検証された、データを一切保持しない基準です。

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. VPNが切れたときに通信を遮断する安全機能 (6)

5. クライアントアプリを隔離するために使われる内部のプロキシプロトコル (8)

6. 外部の監査で検証された、データを一切保持しない基準 (4)

7. データを第三者に読み取れなくするための仕組み (4)

タテのカギ

1. 入口と出口のサーバーノードを経由して通信を送ること (6)

3. 次世代の計算機による攻撃に耐えるよう設計された暗号の仕組み (7)

4. 軽量で高性能な、安全なトンネリングプロトコル (6)

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: VPNが切れたときに通信を遮断する安全機能 (6 文字):

5 ヨコ: クライアントアプリを隔離するために使われる内部のプロキシプロトコル (8 文字):

6 ヨコ: 外部の監査で検証された、データを一切保持しない基準 (4 文字):

7 ヨコ: データを第三者に読み取れなくするための仕組み (4 文字):

タテのカギ

1 タテ: 入口と出口のサーバーノードを経由して通信を送ること (6 文字):

3 タテ: 次世代の計算機による攻撃に耐えるよう設計された暗号の仕組み (7 文字):

4 タテ: 軽量で高性能な、安全なトンネリングプロトコル (6 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。

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

用語リスト

ワイヤガード　マルチホップ　ラムセンヨウ　キルスイッチ　ノーログ　ソックスファイブ
ポストリョウシ　アンゴウ

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. ワイヤガード
B. マルチホップ
C. ラムセンヨウ
D. キルスイッチ
E. ノーログ
F. ソックスファイブ
G. ポストリョウシ
H. アンゴウ

定義とマッチ欄
1. クライアントアプリを隔離するために使われる内部のプロキシプロトコル。
2. 次世代の計算機による攻撃に耐えるよう設計された暗号の仕組み。
3. 軽量で高性能な、安全なトンネリングプロトコル。
4. 再起動してもデータが残らない揮発性メモリのサーバーハードウェア。
5. VPNが切れたときに通信を遮断する安全機能。
6. 入口と出口のサーバーノードを経由して通信を送ること。
7. データを第三者に読み取れなくするための仕組み。
8. 外部の監査で検証された、データを一切保持しない基準。

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. ヤワガードイ
2. ウラセヨンム
3. グノロー
4. シスヨリウポト
5. ホチプマツル
6. ツイキスチル
7. ソブフアイツスク
8. アウゴン

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	Mullvadのセキュリティ機能			
2	Mullvadのカスタマーサポートへの質問			
3	強力なパスワードを作る方法			
4	Mullvadをすすめたい人			
5	監査で確認できること			
6	プライバシー保護の法律が強いことで知られる国			
7	毎日オンラインでしていること			
8	Mullvadのサーバーがほしい国			
9	セキュリティを高めるためにオンにする設定			
10	暗号化が守るもの			
11	VPNの漏えいの種類			
12	このワークシートで学んだセキュリティ用語			
13	公共のWi-Fiにある脅威			
14	Mullvadと一緒に使うアプリ			
15	Mullvadをインストールするデバイス			

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: 量子耐性の統合



シナリオ: 金融会社が、将来の量子コンピューターによる解読に備えて、ファイル転送を保護する必要があります。

ディスカッションの問い: Mullvadのアプリで、どのようなトンネル設定を導入するべきですか？

ケーススタディ 2: ステルス調査ルーティング



シナリオ: 調査員が、接続の入口を隠すために、ネットワークを二重にルーティングしたいと考えています。

ディスカッションの問い: 複数のサーバーを経由するルーティングを実現するには、Mullvadのどの機能を有効にするべきですか？

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

1	6	3	46	20	22		67	13	44	72	61	35		34	72	41	35

28	38	3

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: Mullvad はアカウントをどのように保護しますか?

Mullvad は、パスワードもメールも不要な、生成された 16 桁のアカウント番号を使用します。 [1]

Q2: Mullvad はどのプロトコルを優先していますか?

Mullvad は、速度、シンプルさ、最新の暗号技術を理由に、WireGuard を優先しています。 [9]

Q3: Mullvad のサーバーは監査を受けていますか?

はい、第三者のセキュリティ会社が、インフラとコードの監査を定期的に行っています。

Q4: Mullvad は OpenVPN に対応していますか?

いいえ、Mullvad は 2026 年 1 月 15 日に OpenVPN を廃止しました。WireGuard のみです。 [7]

Q5: Mullvad のキルスイッチとは何ですか?

VPN が失敗した場合にインターネット通信を防ぐ、統合されたファイアウォールルールです。

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: Mullvad は IPv6 に対応していますか?

はい、Mullvadはネイティブの IPv6ルーティングとリーク保護に対応しています。

Q7: Mullvad はマルチホップを提供していますか?

はい、WireGuardのマルチホップでは、複数のサーバーロケーションを連結できます。

Q8: カスタム DNS リゾルバーを使えますか?

はい、Mullvadクライアントの設定でカスタムDNSアドレスを指定できます。

Q9: ログはどのように防がれていますか?

システム設定により、すべてのサーバーデーモンでログ記録が無効になり、キャッシュが消去されます。

Q10: Mullvad はどこで法人登録されていますか?

Mullvad はスウェーデンのヨーテボリで法人登記されており、スウェーデンの管轄下にあります。

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: 鍵のローテーションはどのような仕組みですか?

アプリはWireGuardの鍵を自動でローテーションします。CLIのデフォルトの間隔は30日です。 [3]

Q2: 耐量子トンネルとは何ですか?

WireGuardにML-KEMとClassic McElieceの鍵交換を追加し、将来の量子攻撃に耐えられるようにします。 [2]

Q3: RAM 専用ノードはどのように安全なのですか?

これらのノードはハードドライブにデータを書き込まないため、物理サーバーを盗まれても意味がありません。

Q4: SOCKS5 プロキシの機能とは何ですか?

特定のアプリの通信をトンネル内でルーティングするのに役立ち、外部ネットワークへの漏えいを防ぎます。

Q5: Mullvad は WebRTC リークから保護しますか?

はい、アプリはWebRTCのクエリを強制的にVPNインターフェース経由にして、ローカルIPを保護します。

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: Mullvad は警察の家宅捜索にどう対応しますか?

Mullvad にはユーザーデータベースのログがないため、ユーザー情報を取り出すことはできません。

Q7: スウェーデンの法域のリスクは何ですか?

スウェーデンは 14 Eyes の加盟国ですが、Mullvad のゼロログ構造により、データのリスクはなくなります。

Q8: クライアントアプリの監査はオープンソースですか?

はい、アプリはオープンソース (GPL-3) で、X41 D-Secなどの企業による監査を受けています。 [6]

Q9: スプリットトンネリングはどう動作しますか?

オペレーティングシステムのルーティングテーブルを使って、特定のアプリを VPN のオーバーヘッドから除外します。

Q10: Mullvad は現金での支払いをどのように扱いますか?

現金はトークンコード付きで郵送され、手作業で付与され、封筒は裁断されます。

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

Mullvad は 2009 年にスウェーデンのヨーテボリで Amagicom AB によって設立されました。

2. VPN の洞察

アカウント番号は、アカウントへの入金とアクセスに使われる唯一の識別子です。

3. VPN の洞察

ユーザーデータベースには、名前、メールアドレス、パスワード、電話番号は保存されません。

4. VPN の洞察

WireGuardの鍵はクライアントデバイス上でローカルに生成されるため、サーバー側の侵害を防げます。

5. VPN の洞察

Cure53 による 2024 年のインフラ監査では、VPN トラフィックの匿名性を損なう欠陥は見つかりませんでした。 [5]

6. VPN の洞察

MullvadのWireGuardサーバーはすべてSOCKS5プロキシを実行しており、トンネル内からのみ到達できます。 [8]

7. VPNの豆知識

WireGuardのトラフィックは、Shadowsocks、QUIC、LWOで難読化して、ファイアウォールを通過させることができます。 [10]

8. VPNの豆知識

Mullvad は 2023 年 9 月に、RAM のみの VPN サーバーへの移行を完了しました。 [4]

9. VPNの豆知識

ML-KEM と Classic McEliece は、WireGuard 用のポスト量子事前共有鍵をネゴシエートします。 [2]

10. VPN の洞察

現金の入った封筒と、お金以外の同封物は、利用時間が付与された後に裁断されます。

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] Mullvad VPN. (n.d.). Why Mullvad VPN?
https://mullvad.net/en/why-mullvad-vpn

[2] Mullvad VPN. (n.d.). Quantum-resistant tunnels with WireGuard.
https://mullvad.net/en/help/quantum-resistant-tunnels-with-wireguard

[3] Mullvad VPN. (n.d.). CLI commands for using WireGuard.
https://mullvad.net/en/help/cli-command-wg

[4] Mullvad VPN. (2023). We have successfully completed our migration to RAM-only VPN infrastructure.
https://mullvad.net/en/blog/we-have-successfully-completed-our-migration-to-ram-only-vpn-infrastructure

[5] Mullvad VPN. (2024). Fourth Infrastructure audit completed by Cure53.
https://mullvad.net/en/blog/fourth-infrastructure-audit-completed-by-cure53

[6] Mullvad VPN. (2024). The report for the 2024 security audit of the app is now available.
https://mullvad.net/en/blog/the-report-for-the-2024-security-audit-of-the-app-is-now-available

[7] Mullvad VPN. (2024). Removing OpenVPN 15th January 2026.
https://mullvad.net/en/blog/removing-openvpn-15th-january-2026

[8] Mullvad VPN. (n.d.). SOCKS5 proxy.
https://mullvad.net/en/help/socks5-proxy

[9] Mullvad VPN. (n.d.). Why WireGuard?
https://mullvad.net/en/help/why-wireguard

[10] Mullvad VPN. (n.d.). Using Mullvad VPN in restrictive locations.
https://mullvad.net/en/help/connecting-to-mullvad-vpn-from-restrictive-locations

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

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

解答: チェックポイント 1 – 多肢選択

1 問題 1

正解: B

指導メモ

Mullvadのアプリでデフォルトとなっているトンネリングプロトコルはどれですか? → WireGuard

2 問題 2

正解: A

指導メモ

「アカウントを生成」をクリックするとアカウント番号が発行され、メールアドレスなどの個人情報は求められません。

3 問題 3

正解: B

指導メモ

Mullvadの量子耐性を持つWireGuardトンネルは、ML-KEMとClassic McElieceを使って事前共有鍵を取り決めます。

4 問題 4

正解: C

指導メモ

WebRTCリークの危険を防ぐセキュリティの仕組みは何ですか? → WebRTCをVPNインターフェース経由でルーティングすること

5 問題 5

正解: B

指導メモ

複数のノードを経由してトラフィックを送るマルチホップ機能はどれですか? → WireGuardマルチホップ

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

誤り: Mullvadはメールアドレスを求めません。アカウントは生成された番号だけで識別されます。

7 問題 7

正解: 正しい

指導メモ

SOCKS5 プロキシは、Mullvad のトンネル内で構成できます。

8 問題 8

正解: 誤り

指導メモ

誤り: Mullvadは一部のサーバーを所有していますが、プロバイダーから専用サーバーを借りてもいます。

9 問題 9

正解: 正しい

指導メモ

Network Kill Switchは、デフォルトで常に有効です。

10 問題 10

正解: 正しい

指導メモ

郵送した現金での支払いは、まったく返金できません。

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

B 1. WireGuard	D 2. マルチホップ	G 3. RAM専用	A 4. キルスイツチ
H 5. ノーログ	C 6. ソツクスフアイブ	E 7. ポストリヨウシ	F 8. DNSリーク

チェックポイント 3: 解答 – 重要用語

1 WireGuard	2 マルチホップ	3 RAM専用	4 キルスイッチ
5 ノーログ	6 SOCKS5	7 量子	8 DNSリーク

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 F – ソツクスフアイブ	2 G – ポストリヨウシ	3 A – ワイヤガード	4 C – ラムセンヨウ
5 D – キルスイツチ	6 B – マルチホツプ	7 H – アンゴウ	8 E – ノーログ

指導者向けディスカッションメモ

重要用語:
生徒がWireGuard、マルチホップ、RAM専用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。

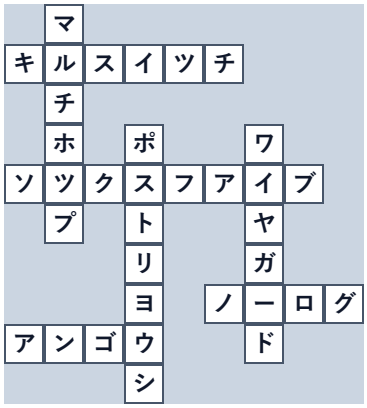
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

2 ヨコ: キルスイツチ VPNが切れたときに通信を遮断する安全機能 (6 文字)

5 ヨコ: ソツクスフアイブ クライアントアプリを隔離するために使われる内部のプロキシプロトコル (8 文字)

6 ヨコ: ノーログ 外部の監査で検証された、データを一切保持しない基準 (4 文字)

7 ヨコ: アンゴウ データを第三者に読み取れなくするための仕組み (4 文字)

タテのカギ

1 タテ: マルチホップ 入口と出口のサーバーノードを経由して通信を送ること (6 文字)

3 タテ: ポストリヨウシ 次世代の計算機による攻撃に耐えるよう設計された暗号の仕組み (7 文字)

4 タテ: ワイヤガード 軽量で高性能な、安全なトンネリングプロトコル (6 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. ヤワガードイ — **ワイヤガード**
2. ウラセヨンム — **ラムセンヨウ**
3. グノロー — **ノーログ**
4. シスヨリウポト — **ポストリヨウシ**
5. ホチプマツル — **マルチホツプ**
6. ツイキスチル — **キルスイツチ**
7. ソブファイツスク — **ソツクスファイブ**
8. アウゴン — **アンゴウ**

秘密の暗号チャレンジ 解答

"アカウントニ パスワードモ メールモ フヨウ"

ケーススタディの解答

A ケーススタディ 1: 量子耐性の統合

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: ある金融会社が、将来の量子コンピューターによる復号に備えて、ファイル転送を保護する必要があります。
- 推奨される対策と解決策: ポスト量子の事前共有鍵を使って、耐量子 WireGuard トンネルを展開します。

B ケーススタディ 2: ステルス調査ルーティング

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: ある調査員が、接続元を隠すために、ネットワークを二重に経由させたいと考えています。
- 推奨される対策と解決策: Mullvad の WireGuard マルチホップ機能を有効にして、入口ノードと出口ノードを連結します。