名前: 日付: 得点:

# WireGuardとOpenVPNの比較 ワークシート

WireGuard と OpenVPN のプロトコル、コードベースの規模、速度、暗号標準の比較

## VPN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、仮想プライベートネットワーク (VPN) の基本原則について学びます。暗号化トンネルがデータをどう守るか、ネットワークプロトコルがどう動くか、プライバシーのリークをどう見つけて軽減するかを取り上げます。

**ワークシートのチェックポイント**

- [ ] **パート 1-4: VPN の概念とプロトコルを習得します。**
- [ ] **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 VPN ガイドを開く**

URL: https://www.vpn.com/vpn/

# あなたのVPN 学習ロードマップ

- プロトコルのコードベースの複雑さと監査のしやすさを比較してください。
- カーネル空間内で実行することによる性能向上を分析してください。
- OpenSSL の暗号と WireGuard の最新の暗号技術を比較してください。
- ピア同士のハンドシェイク用に、公開鍵と秘密鍵のペアを設定します。
- VPN の通信を TCP と UDP のファイアウォールポート経由にすること。

### プロトコル比較ワークシートの手順

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。学んだ知識を最新プロトコルの監査に応用しましょう。 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。

### WireGuardとOpenVPNの比較（導入）

VPN プロトコルを選ぶには、速度と設定オプションのバランスを考える必要があります。OpenVPN は数十年にわたって標準であり、TCP/UDP の柔軟な設定が可能です。WireGuard はカーネル空間で直接動作する現代的な代替手段で、コードはわずか 4,000 行です。プロトコルの違いを理解することは、安全なネットワークを最適化するうえで重要です。

**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. 1. WireGuardプロトコルのコードベースの大きさは、おおよそどのくらいですか?
   - A. 約70,000行
   - B. 100,000行超
   - C. 1,000 行未満
   - D. 約 4,000 行

2. 2. WireGuard は、オペレーティングシステムのどの領域で動作しますか?
   - A. ユーザー空間
   - B. カーネル空間
   - C. アプリケーション空間
   - D. 仮想空間

3. 3. OpenVPNが主に依存している暗号ライブラリはどれですか？
   - A. ChaCha20-Poly1305
   - B. OpenSSL暗号ライブラリ
   - C. Noiseプロトコルフレームワーク
   - D. 平文のDESエンコード

4. 4. OpenVPNと比べたときの、WireGuardの主なパフォーマンス上の利点は何ですか?
   - A. 接続のハンドシェイクが速くなり、レイテンシが下がる
   - B. パブリックIPアドレスの必要性を回避すること
   - C. レガシーなダイヤルアップへの標準搭載のネイティブサポート
   - D. モバイルデバイスでバッテリーの負荷がゼロ

5. 5. WireGuard は、ピアの接続をどのように認証しますか?
   - A. 標準のユーザーパスワードを交換することによって
   - B. ドメイン登録証明書を検証することで
   - C. 静的な公開鍵と秘密鍵のペアを使うことで
   - D. ハードウェアのシリアル番号を確認することで

## チェックポイント 2: 正しい・誤りチャレンジ

**6 質問 6**

6. WireGuardのコンパクトなコードベースにより、監査が大幅にしやすくなっています。

○ 正しい ○ 誤り

**7 質問 7**

7. OpenVPN はカーネル空間で動作するため、一般に WireGuard より高速です。

○ 正しい ○ 誤り

**8 質問 8**

8. OpenVPN は柔軟に設定でき、UDP と TCP の両方のプロトコルに対応しています。

○ 正しい ○ 誤り

**9 質問 9**

9. WireGuardは、パケットの高速な暗号化のためにChaCha20などの最新の暗号を使います。

○ 正しい ○ 誤り

**10 質問 10**

10. WireGuardは、認証に複雑な認証局のセットアップが必要です。

○ 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. 最新の _____ プロトコルは、OSのカーネル内で直接動作します。
2. 従来型の _____ プロトコルは、OpenSSLの暗号ライブラリに依存しています。
3. _____ でコードを実行すると、コンテキストスイッチのオーバーヘッドが減ります。
4. OpenVPNは _____ で動作し、仮想インターフェース経由でパケットを中継します。
5. WireGuardは、接続相手を識別するために公開鍵と秘密鍵の _____ を使います。
6. コードベースが小さいと、ソフトウェアのセキュリティの _____ が高まります。

**用語バンク**

OpenVPN　WireGuard　カーネル空間　キーペア　コンパクト　ユーザー空間　ライブラリ　監査性

**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: ネットワークの概念マッチング

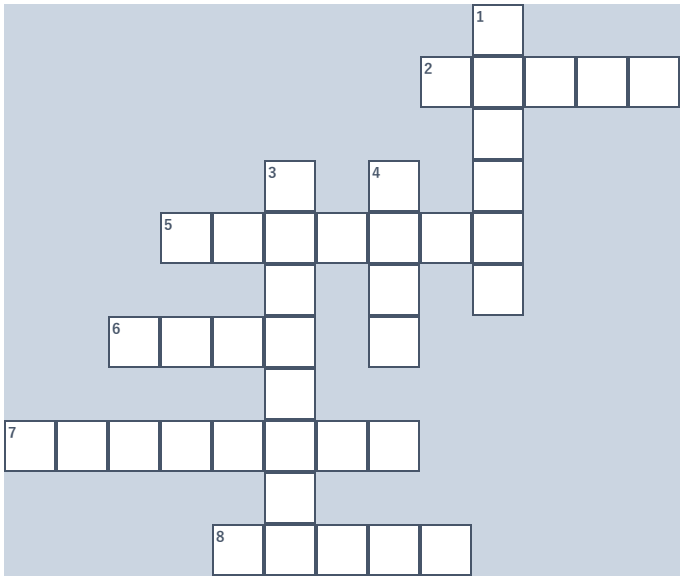
**定義マッチング**

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 | OpenVPNが動作する実行領域で、コンテキストスイッチのオーバーヘッドが生じます。 |
| | 2. OpenVPN | B | WireGuardのコードベースが小さく、監査がはるかに容易であること。 |
| | 3. カーネル空間 | C | OpenVPN が暗号アルゴリズムのために利用する暗号ライブラリ。 |
| | 4. ユーザー空間 | D | OpenVPNがサポートするトランスポートプロトコル。WireGuard自体はUDPのみで動作します。 |
| | 5. 4,000 行 | E | WireGuard が速度のために動作するオペレーティングシステムの実行領域。 |
| | 6. OpenSSL | F | WireGuardがピア接続を検証するために使う、非対称トークン。 |
| | 7. キーペア | G | 高速性と簡単なコード監査を目指して設計された、最新の VPN プロトコル。 |
| | 8. TCP/UDP | H | 大規模で複雑な設定コードベースを持つ、堅牢な従来型のプロトコル。 |

## 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. OpenVPNが暗号アルゴリズムのために頼っている暗号の部品群 (5)**

**5. OpenVPNが対応するトランスポートプロトコルの1つ。WireGuard自体はUDPのみで動作する (7)**

**6. 大きく複雑な設定のコードベースを使う、堅牢な従来型のプロトコル (4)**

**7. WireGuardが速度のために動作する、OSの実行領域 (8)**

**8. コードベースが小さく、監査がはるかに容易であること (5)**

### タテのカギ

**1. 高速かつコード監査の簡単さを重視して設計された、最新のVPNプロトコル (6)**

**3. OpenVPNが動作し、コンテキストスイッチのオーバーヘッドを生む実行領域 (8)**

**4. WireGuardが接続相手を確認するために使う非対称のトークン (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

**2 ヨコ: OpenVPNが暗号アルゴリズムのために頼っている暗号の部品群 (5 文字):**

**5 ヨコ: OpenVPNが対応するトランスポートプロトコルの1つ。WireGuard自体はUDPのみで動作する (7 文字):**

**6 ヨコ: 大きく複雑な設定のコードベースを使う、堅牢な従来型のプロトコル (4 文字):**

**7 ヨコ: WireGuardが速度のために動作する、OSの実行領域 (8 文字):**

**8 ヨコ: コードベースが小さく、監査がはるかに容易であること (5 文字):**

## タテのカギ

**1 タテ: 高速かつコード監査の簡単さを重視して設計された、最新のVPNプロトコル (6 文字):**

**3 タテ: OpenVPNが動作し、コンテキストスイッチのオーバーヘッドを生む実行領域 (8 文字):**

**4 タテ: WireGuardが接続相手を確認するために使う非対称のトークン (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。

ペ ロ ボ タ レ ミ ク コ グ ヌ チ ユ ガ メ ロ
ボ ワ ラ キ ゼ ゴ ザ ン ワ ス ホ ノ オ ア オ
キ ル ア パ ホ ヒ パ パ ヘ イ ボ ズ フ サ ン
メ ハ ペ コ ヌ ヤ モ ク ヘ ワ ヤ レ テ モ モ
ン ギ ー ゲ ズ カ ジ ト ツ カ ラ ガ ゴ ワ ラ
ー ニ キ グ カ ー バ ユ コ ザ ペ イ ー ダ キ
ピ ポ バ タ フ ネ ト ー ー コ モ サ ブ ド ガ
ー ベ レ カ ゾ ル エ ア ー ザ ユ コ ヘ ラ イ
シ サ ラ サ ソ ク テ ヌ コ ギ ー ン メ ス リ
ー ヌ グ ポ ゴ ウ ソ ガ ド セ イ ク イ ガ リ
イ ヤ レ ズ ボ カ ワ ヒ グ ゼ ー ゲ ウ ケ ヤ
テ プ オ タ グ ン ベ ブ ノ シ イ ギ ー カ ピ
ピ マ ツ ヌ メ ガ ヒ ム ガ ミ ジ リ ト ロ ン
ン テ ー ウ ラ デ チ レ 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　カーネルクウカン　ユーザークウカン　コンパクト　ライブラリ　キーペア　テイーシーピー　レガシー

# 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. カーネルクウカン |
| C. ユーザークウカン |
| D. コンパクト |
| E. ライブラリ |
| F. キーペア |
| G. テイーシーピー |
| H. レガシー |

| 定義とマッチ欄 |
| --- |
| 1. WireGuardが接続相手を確認するために使う非対称のトークン。 |
| 2. OpenVPNが動作し、コンテキストスイッチのオーバーヘッドを生む実行領域。 |
| 3. WireGuardが速度のために動作する、OSの実行領域。 |
| 4. OpenVPNが対応するトランスポートプロトコルの1つ。WireGuard自体はUDPのみで動作する。 |
| 5. 大きく複雑な設定のコードベースを使う、堅牢な従来型のプロトコル。 |
| 6. OpenVPNが暗号アルゴリズムのために頼っている暗号の部品群。 |
| 7. 高速かつコード監査の簡単さを重視して設計された、最新のVPNプロトコル。 |
| 8. コードベースが小さく、監査がはるかに容易であること。 |

## 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、VPNの重要な概念と用語を見つけましょう。答えは入力できる欄に書いてください。

1. ヤワガードイ
2. ーユンーカウクザ
3. ブラリライ
4. ーイーシピテー
5. クウーンルカカネ
6. クコパトン
7. ペキアー
8. レーシガ

# 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 | WireGuardを選ぶ理由 | | | |
| 2 | 優れたVPNプロバイダーが約束すること | | | |
| 3 | OpenVPNを選ぶ理由 | | | |
| 4 | 旅行中にVPNを使う理由 | | | |
| 5 | インターネットプロバイダーが見られるもの | | | |
| 6 | 偽のWi-Fiネットワークを見抜く方法 | | | |
| 7 | VPNに関する誤解 | | | |
| 8 | VPNを使う場所 | | | |
| 9 | 日常生活の中の速いもの | | | |
| 10 | VPNでは守れないもの | | | |
| 11 | コードを確認しやすくするもの | | | |
| 12 | VPNが隠せるもの | | | |
| 13 | WireGuardとOpenVPNの違い | | | |
| 14 | プライバシーに関連する言葉 | | | |
| 15 | 知っている暗号の名前 | | | |

## チェックポイント 8: VPN 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。

### サラ（カフェにいる学生）

👨‍🦲 「やあ! カフェのWi-Fiにいて、VPNアプリでWireGuardかOpenVPNを選べるんだ。カフェのネットワークとスマホのテザリングの間を歩いて移動すると、ビデオ通話が途切れ続けるんだ。どっちのプロトコルを選ぶべき? それと、なぜそっちのほうが切り替えにうまく対応できるの?」

### Alex(旅行する学生)

👨‍🦲 「海外のホテルのネットワークにいるんだけど、ほとんどのVPN通信をブロックしているみたいなんだ。WireGuardがまったくつながらないのに、母国にある学校の資料にはアクセスしないといけない。何がブロックされていそうなの? OpenVPNを使うと、どうやって突破できるの?」

## チェックポイント 9: 暗号を解読しよう

プロトコル監査のトレーニングを完了するために、カーネル空間での実行についてのこの隠されたメッセージを解読しましょう。

**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

5 72 69 46 64 2 68 72 4 23 45 26 36 2 20 46 24 41 22

6 4 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の利用について、見込み客からよくある質問と回答を確認しましょう。

### Q1: VPN とは何で、どのような仕組みですか?

仮想プライベートネットワーク(VPN)は、インターネット接続を暗号化し、通信を安全なリモートサーバー経由で送ります。これにより公開IPアドレスが隠れ、VPNトンネルを通る通信について、ローカルネットワークの観察者やISPに見える情報が限られます。

### Q2: プロトコルはなぜ重要ですか?

プロトコルは、VPNがトンネルをどのように構築するか、どの暗号技術でデータを保護するか、接続と再接続がどれだけ速いかを決めます。WireGuardとOpenVPNは、ほとんどのVPNアプリが提供する2つのオープンソースプロトコルで、シンプルさ、速度、設定の自由度の間で異なるトレードオフがあります。

### Q3: どちらか一方がよりプライベートですか?

どちらのプロトコルも匿名にしてくれるわけではありません。どちらも強力な暗号でトンネルのトラフィックを暗号化します。プライバシーは主に、VPN プロバイダーが何を記録するか、そして鍵、アカウント、サーバーをどう管理するかによって決まります。

### Q4: VPN はインターネット速度を遅くしますか?

はい、わずかにあります。暗号化の処理とVPNサーバーまでの物理的な距離により、遅延とオーバーヘッドが加わります。影響の大きさは、プロバイダー、プロトコル、サーバーまでの距離、端末、ネットワークの状況によって異なります。

### Q5: 両方ともオープンソースですか?

はい。WireGuardとOpenVPNコミュニティ版はどちらもソースコードを公開しているため、独立した研究者が検証できます。WireGuardはコードが小さいため、全体の検証がはるかに早く済みます。

# 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の利用について、見込み客からよくある質問と回答を確認しましょう。

### Q6: どちらが速いですか?

WireGuardは通常より高速です。カーネル内で動作し、無駄のないChaCha20-Poly1305暗号化を使い、ハンドシェイクも素早く完了します。OpenVPNはオーバーヘッドが大きいものの、実際の速度はサーバーの負荷や距離にも左右されます。

### Q7: 両方とも TCP と UDP で動作しますか?

いいえ。OpenVPN は UDP でも TCP でも動作でき、TCP モードは UDP をブロックするネットワークで役立ちます。WireGuard はパケットを UDP でのみ送信するため、TCP のみを許可するネットワークでは失敗することがあります。 [4]

### Q8: 最適な VPN を選ぶにはどうすればよいですか?

監査済みのノーログポリシー、強力なプロトコル（WireGuard、OpenVPN）、安全なサーバーの所在地、高速な通信、RAM のみのサーバー、キルスイッチ機能、そして（5/9/14 アイズのような）情報共有同盟の外にある管轄を探しましょう。

### Q9: スマートフォンで WireGuard と OpenVPN を使えますか?

はい。WireGuardはクロスプラットフォームで、Windows、macOS、Linux、iOS、Android向けのアプリがあり、OpenVPNのクライアントも同じシステム向けにあります。ほとんどのVPNアプリでどちらかを選べます。 [1]

### Q10: なぜ WireGuard はこれほど小さいのですか?

WireGuardは、多くの選択肢ではなく、最新の暗号を1つの固定セットでサポートします。Linux版の実装は4,000行未満のコードで済むため、より大規模なVPNのコードベースより監査しやすくなっています。 [3]

# チェックポイント 10: VPN FAQ – 応用（パート C）

仮想プライベートネットワークと安全なトンネリングプロトコルの、技術面と構造面を探ります。

### Q1: WireGuard、OpenVPN、IKEv2 の違いは何ですか?

WireGuardは、約4,000行のコードしかない最新の軽量プロトコルで、高速な通信と素早い接続時間を実現します。OpenVPNは、実績のある非常に安全なオープンソースプロトコルです。IKEv2は、ネットワークを切り替えたときに素早く再接続できるため、モバイルデバイスに最適です。

### Q2: WireGuard はどの暗号を使いますか?

WireGuardは、暗号化にChaCha20とPoly1305、鍵交換にCurve25519、ハッシュにBLAKE2s、ハンドシェイクにNoiseフレームワークを使います。暗号のネゴシエーションがないため、ユーザーが脆弱な選択肢を選ぶことはありません。 [2]

### Q3: OpenVPN はどの暗号とライブラリを使えますか?

OpenVPN は OpenSSL ライブラリと密接に統合されており、鍵交換に TLS を使用します。管理者は AES-256-GCM などのデータチャネル暗号を選べますが、柔軟性が高まる一方で、弱い設定が入り込む余地も生まれます。 [4]

### Q4: 各プロトコルはどのようにピアを認証しますか?

WireGuardのピアは、SSH鍵の交換に似た固定の公開鍵で互いを識別し、各鍵は許可されたトンネルIPに対応付けられます。OpenVPNは通常、X.509証明書を持つ認証局に頼り、ユーザー名とパスワードを組み合わせることも多くあります。

### Q5: 難読化は VPN のブロックをどう回避しますか?

難読化（「ステルス VPN」とも呼ばれます）は、VPN トラフィックを通常の HTTPS トラフィック（ポート 443）に見せかけます。これにより、政府や学校・職場のネットワークが VPN をブロックするために使うディープパケットインスペクション（DPI）を回避しやすくなる場合があります。

# チェックポイント 10: VPN FAQ – 応用 (パート D)

仮想プライベートネットワークと安全なトンネリングプロトコルの、技術面と構造面を探ります。

### Q6: Wi-Fi からモバイルに切り替えるとどうなりますか?

WireGuardはコネクションレスで、新しいアドレスからパケットを送り、素早いハンドシェイクの後もトンネルが継続します。OpenVPNはセッションの状態を保持するため、ネットワークが変わると再接続が必要になり、少し時間がかかる場合があります。

### Q7: 前方秘匿性(PFS)はどう機能しますか?

PFS は、セッションごとに一意の一時的な暗号鍵が生成されるようにします。将来、秘密鍵が漏えいしても、各セッションが独立した鍵を使っているため、過去や将来のセッションの復号には使えません。

### Q8: WireGuard のほうが速くても、OpenVPN は今も良い選択肢ですか?

はい。OpenVPNは成熟していて広く導入されており、UDPがブロックされるとTCPで動作し、証明書ベースの企業向け構成にも対応しています。多くのプロバイダーが両方のプロトコルを提供しているので、片方がブロックされたり遅かったりしたら切り替えられます。

### Q9: どのポートを使いますか?

OpenVPN の標準ポートは 1194 ですが、443 を含む任意の UDP または TCP ポートに変更できます。WireGuard は設定で指定した UDP ポートで待ち受け、公式例では 51820 が使われています。

### Q10: 手動での設定が簡単なのはどのプロトコルですか?

WireGuardは通常よりシンプルです。鍵のペアを生成し、公開鍵を交換して、許可するIPを列挙するだけです。OpenVPNは証明書、CA、より多くのオプションが必要ですが、.ovpnプロファイルならそれらを1つのファイルにまとめられます。

# パート 11: VPN に関する興味深い事実10選と実世界の洞察

VPN の歴史、市場、技術に関する、非常に価値のある実際の事実と知見を確認しましょう。

### 1. 最初の VPN プロトコル

PPTP（Point-to-Point Tunneling Protocol）は、Microsoft などのベンダーグループによって開発され、リモートアクセス VPN をサポートするために1999年7月に RFC 2637 として公開されました。 [6]

### 2. 2 つのトランスポート

OpenVPN はトンネルを UDP または TCP で運ぶことができ、TLS モードでは制御チャネルとデータチャネルが1つのポートを共有します。 [4]

### 3. WireGuard 革命

WireGuardは、効率を重視して設計された非常に合理化されたコードベースを持ち、従来のプロトコルよりもセキュリティ上の脆弱性を監査しやすくなっています。 [3]

### 4. 最新の暗号技術

WireGuardは、Noiseプロトコルフレームワークの中でChaCha20、Poly1305、Curve25519、BLAKE2s、SipHash24、HKDFを組み合わせており、ユーザーが選択を誤るような暗号の選択肢はありません。 [2]

### 5. OpenVPN 内部の OpenSSL

OpenVPN は OpenSSL ライブラリと密接に統合されており、鍵交換に使われる TLS をはじめ、暗号化機能の多くをそこから得ています。 [4]

### 6. ディープパケットインスペクション

ディープパケットインスペクション(DPI)は、ヘッダーだけでなくパケットの内容や通信パターンも調べ、一部のファイアウォールはこれを使って一般的なVPNプロトコルを検出しブロックします。

### 7. SSH方式のキー

WireGuardの接続は、SSH鍵の交換に似たシンプルな公開鍵の交換で設定され、認証局は必要ありません。 [1]

### 8. クロスプラットフォーム

WireGuardは最初にLinuxカーネル向けにリリースされ、現在はWindows、macOS、BSD、iOS、Androidでも利用できるため、同じプロトコルがほとんどのデバイスで使えます。 [1]

### 9. 前方秘匿性

WireGuardは、Noise_IKハンドシェイクを数分ごとに繰り返して共通のセッション鍵を更新するため、長期鍵が後で漏えいしても前方秘匿性が確保されます。 [2]

### 10. TUN/TAP インターフェース

OpenVPN は TUN/TAP 仮想ネットワークインターフェースで動作するよう設計されており、これはほとんどのプラットフォームで利用でき、トンネルのパケットを運びます。 [4]

# 技術参考資料と出典

このワークシート全体で使われている、引用された出版物、暗号仕様、公式文書の標準。

## 学術・業界の参考資料

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

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

[3] 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/

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

[5] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

# 解答: WireGuardとOpenVPNのプロトコル、コードベースの規模、速度、暗号化標準の比較

## 1 WireGuardのコードサイズ

プロトコル

正解: D

### 指導メモ

WireGuardは非常にコンパクトで、約4,000行のコードで動作します。これにより攻撃対象領域が小さく保たれ、監査もしやすくなります。出典: WireGuard Project。

## 2 カーネル空間の速度

遅延

正解: B

### 指導メモ

カーネル空間で直接実行されるため、WireGuardはコンテキストスイッチのオーバーヘッドを避けられ、高いスループットを実現できます。出典: WireGuard Project。

## 3 問題 3

正解: B

### 指導メモ

OpenVPNはOpenSSLと密接に統合されており、AES-GCMなどの暗号を提供するため、非常に柔軟に設定できる一方で、より複雑です。

## 4 プロトコルの性能

ルーティング制御

正解: A

### 指導メモ

WireGuardはミリ秒単位でハンドシェイクを確立し、ネットワークローミング(例: Wi-Fiからモバイル回線への切り替え)にも即座に反応します。出典: Microsoft Native Gateway、Apple Support。 [3]

## 5 非対称暗号

プライバシー

正解: C

### 指導メモ

WireGuardはCryptokey Routingを使い、SSHのセットアップ設定と同様に、公開鍵を許可されたトンネルIPアドレスに対応付けます。出典: WireGuard Project。

## 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

WireGuardのLinux実装は4,000行未満であるため、セキュリティチームは、OpenVPNのようなはるかに大規模なVPNのコードベースよりも、ずっと速くレビューできます。

### 7 ユーザー空間の遅延 速度

正解: 誤り

#### 指導メモ

OpenVPN はユーザー空間で動作し、カーネルの仮想インターフェースとの間でパケットを往復させるため、コンテキストスイッチのオーバーヘッドが加わります（OpenVPN DCO などのカーネルオフロードを使用する場合を除きます）。 出典: DD-WRT custom firmware.

### 8 OpenVPN の設定 スニッフィングのリスク

正解: 正しい

#### 指導メモ

OpenVPN は TCP（信頼性とファイアウォール回避のため）または UDP（速度のため）で動作でき、複雑な企業向けファイアウォールとも互換性があります。 出典: IETF Cryptographic Protocols.

### 9 現代の暗号技術 ファイアウォール

正解: 正しい

#### 指導メモ

WireGuardは、ChaCha20やPoly1305などの最新で安全なプリミティブを採用して従来の暗号を廃止しており、これらはモバイルCPUでも高速に動作します。出典: WireGuard Project。

### 10 鍵ペアによる簡素化 ノーログ

正解: 誤り

#### 指導メモ

WireGuardは証明書や複雑なCA階層を使わず、ピア同士で交換するシンプルな公開鍵と秘密鍵のペアに頼っています。出典: WireGuard Project。

# 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

| | | | |
|---|---|---|---|
| G 1. WireGuard | H 2. OpenVPN | E 3. カーネル空間 | A 4. ユーザー空間 |
| B 5. 4,000 行 | C 6. OpenSSL | F 7. キーペア | D 8. TCP/UDP |

## チェックポイント 3: 解答 – 重要用語

| | | | |
|---|---|---|---|
| 1 WireGuard | 2 OpenVPN | 3 カーネル空間 | 4 ユーザー空間 |
| 5 キーペア | 6 監査性 | | |

## チェックポイント 6 代替活動: 解答 – 用語マッチング

| | | | |
|---|---|---|---|
| 1 F – キーペア | 2 C – ユーザークウカン | 3 B – カーネルクウカン | 4 G – テイーシーピー |
| 5 H – レガシー | 6 E – ライブラリ | 7 A – ワイヤガード | 8 D – コンパクト |

### 指導者向けディスカッションメモ

**重要用語:**
生徒がWireGuard、OpenVPN、カーネル空間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。

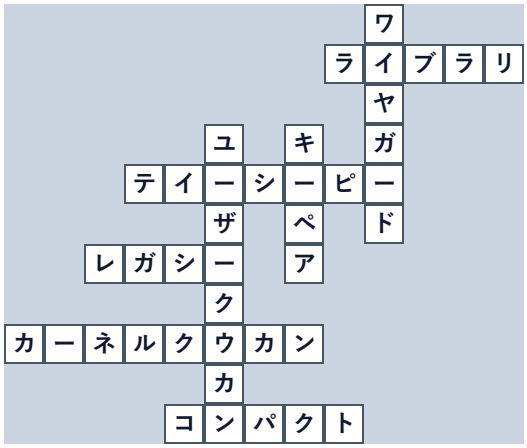
**情報源の評価:**
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

# パズルの解答と指導者用メモ

## ワードサーチの解答

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ペ | ロ | ボ | タ | レ | ミ | ク | コ | グ | ヌ | チ | ユ | ガ | メ | ロ |
| ボ | ワ | ラ | キ | ゼ | ゴ | ザ | ン | ワ | ス | ホ | ノ | オ | ア | オ |
| キ | ル | ア | パ | ホ | ヒ | パ | パ | ヘ | イ | ボ | ズ | フ | サ | ン |
| メ | ハ | ペ | コ | ヌ | ヤ | モ | ク | ヘ | ワ | ヤ | レ | テ | モ | モ |
| ン | ギ | ー | ゲ | ズ | カ | ジ | ト | ツ | カ | ラ | ガ | ゴ | ワ | ラ |
| ー | ニ | キ | グ | カ | ー | バ | ユ | コ | ザ | ペ | イ | ー | ダ | キ |
| ピ | ポ | バ | タ | フ | ネ | ト | ー | ー | コ | モ | サ | ブ | ド | ガ |
| ー | ベ | レ | カ | ゾ | ル | エ | ア | ー | ザ | ユ | コ | ヘ | ラ | イ |
| シ | サ | ラ | サ | ソ | ク | テ | ヌ | コ | ギ | ー | ン | メ | ス | リ |
| ー | ヌ | グ | ポ | ゴ | ウ | ソ | ガ | ド | セ | イ | ク | イ | ガ | リ |
| イ | ヤ | レ | ズ | ボ | カ | ワ | ヒ | グ | ゼ | ー | ゲ | ウ | ケ | ヤ |
| テ | プ | オ | タ | グ | ン | ベ | ブ | ノ | シ | イ | ギ | ー | カ | ピ |
| ピ | マ | ツ | ヌ | メ | ガ | ヒ | ム | ガ | ミ | ジ | リ | ト | ロ | ン |
| ン | テ | ー | ウ | ラ | デ | チ | レ | 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: ライブラリ** OpenVPNが暗号アルゴリズムのために頼っている暗号の部品群 (5 文字)

**5 ヨコ: テイーシーピー** OpenVPNが対応するトランスポートプロトコルの1つ。WireGuard自体はUDPのみで動作する (7 文字)

**6 ヨコ: レガシー** 大きく複雑な設定のコードベースを使う、堅牢な従来型のプロトコル (4 文字)

**7 ヨコ: カーネルクウカン** WireGuardが速度のために動作する、OSの実行領域 (8 文字)

**8 ヨコ: コンパクト** コードベースが小さく、監査がはるかに容易であること (5 文字)

### タテのカギ

**1 タテ: ワイヤガード** 高速かつコード監査の簡単さを重視して設計された、最新のVPNプロトコル (6 文字)

**3 タテ: ユーザークウカン** OpenVPNが動作し、コンテキストスイッチのオーバーヘッドを生む実行領域 (8 文字)

**4 タテ: キーペア** WireGuardが接続相手を確認するために使う非対称のトークン (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. ヤワガードイ → **ワイヤガード**
2. ーユンーカウクザ → **ユーザークウカン**
3. ブラリライ → **ライブラリ**
4. ーイーシピテー → **テイーシーピー**
5. クウーンルカカネ → **カーネルクウカン**
6. クコパトン → **コンパクト**
7. ペキアー → **キーペア**
8. レーシガ → **レガシー**

**秘密の暗号チャレンジ 解答**

**"オープンブイピーエヌヌ ハヤイ トンネルニ カエル"**

# ケーススタディの解答

## A シナリオ A: プロトコルの選択

スニッフィングと暗号化 サラのジレンマ

### 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:**

- 推奨: WireGuard。軽量でコネクションレスな設計により、ネットワークが切り替わってもトンネルがすばやく回復し、ChaCha20-Poly1305 によって暗号化も高速に保たれます。
- セキュリティ: どちらのプロトコルもカフェの Wi-Fi 上での彼女の通信を暗号化するため、正しく設定されていればどちらでもログイン情報を守れます。選択が主に影響するのは速度と安定性です。

## B シナリオ B: VPN ブロックの突破

ジオブロッキングと IP Alexのジレンマ

### 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:**

- ブロックされた理由: WireGuardはUDPのみを使用しており、ホテルのファイアウォールがUDPをブロックしているか、フィルタリングやディープパケットインスペクションでWireGuardのパケットを見分けている可能性があります。
- OpenVPN が役立つ点: HTTPS が使う 443 番ポートを含め TCP 上で動作でき、ウェブ閲覧がそれに依存しているため、ホテルのファイアウォールが完全に遮断することはまれです。