名前: 日付: 得点:

VPN の設定方法 ワークシート

Windows、macOS、Android、iOS、Linux、ルーターでの VPN の設定

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

- 市販の VPN アプリと、ネイティブクライアントの設定を比較してください。
- 家全体を守るため、ルーターに VPN 接続を設定してください。
- OVPN や WireGuard の鍵などの設定ファイルを設定・管理すること。
- トンネル通信のために、ルーターの特定のポートを開放して保護します。
- DNSリークチェックと接続テストで、クライアントの設定を確認します。

設定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VPNクライアントの設定とテストに応用しましょう。 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。

VPNの設定(はじめに)

VPN を手動で設定すると、暗号鍵とネットワークルーティングを完全に管理できます。モバイルデバイスにネイティブクライアントを設定する場合でも、ルーターに VPN トンネルを直接インストールする場合でも、DNS リークを防ぎ、すべてのネットワーク通信を保護するには、適切な設定が重要です。

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. モバイルデバイスにVPNを設定する最も簡単な方法は何ですか？
   - A. アプリストアから公式のVPNアプリをダウンロードする
   - B. オペレーティングシステムのカーネルファイルを手動で編集する
   - C. デバイスのハードウェアにカスタムファームウェアを書き込む
   - D. USBでスマートフォンをデスクトップコンピューターに接続する

2. 2. ルーターに直接VPNをインストールする利点は何ですか?
   - A. ローカルのすべてのデバイスの接続速度を上げる
   - B. 接続されたすべてのネットワークデバイスを自動的に保護する
   - C. ローカルの ISP の契約料を支払う必要がなくなる
   - D. ハードウェアルーターが完全に不要になる

3. 3. 「ネイティブ」VPN設定とは何を指しますか?
   - A. OSに組み込まれた標準設定を使って接続を設定する
   - B. VPNを地元でのみ使う
   - C. 自国内のサーバーにのみ接続すること
   - D. アセンブリ言語でカスタムプロトコルを書くこと

4. 4. OpenVPNを手動で外部設定するために必要なものは何ですか?
   - A. サーバー接続用のカスタムロゴをデザインする
   - B. 証明書キーを含む.ovpnプロファイルをインポートすること
   - C. 自宅ルーターの物理的な設置場所を変更すること
   - D. オペレーティングシステムのファイアウォールを完全に無効にすること

5. 5. 管理者が設定でスプリットトンネリングを使うのはなぜですか?
   - A. すべてのインターネット通信を完全にブロックするため
   - B. 安全な特定のアプリが、セキュアトンネルを迂回できるようにするため
   - C. 物理ルーターを 2 台の別々のユニットに分けるため
   - D. 管理上の監視のために暗号化を無効にするため

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. ルーターの VPN の設定は、技術的なスキルが不要な簡単な作業です。

○ 正しい ○ 誤り

7 質問 7

7. WindowsとmacOSには、IKEv2とL2TPに対応したネイティブクライアントがあります。

○ 正しい ○ 誤り

8 質問 8

8. WireGuard を設定するには、公開鍵と秘密鍵を生成する必要があります。

○ 正しい ○ 誤り

9 質問 9

9. VPNトンネルは、ローカルネットワークのプリンターと印刷ジョブを保護します。

○ 正しい ○ 誤り

10 質問 10

10. VPNアプリを実行できないスマートロックを保護するには、ルーターレベルのVPN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. ゲートウェイである _____ にVPNを導入すると、スマートテレビやゲーム機が保護されます。

2. OpenVPNを手動で設定するには、OVPN形式の _____ のインポートが必要です。

3. OS内蔵の設定では、システムの _____ クライアント設定を使用します。

4. WireGuardの認証は、暗号の公開鍵と秘密鍵の _____ に基づいています。

5. 使いやすいインストールは、プロバイダー公式の _____ によって実現できます。

6. VPNの _____ サーバーを経由して問い合わせることで、名前解決の追跡による漏えいを防げます。

用語バンク

DNS　VPNアプリ　キーペア　スプリットトンネル　ネイティブ　ルーター　接続ログ　設定ファイル

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

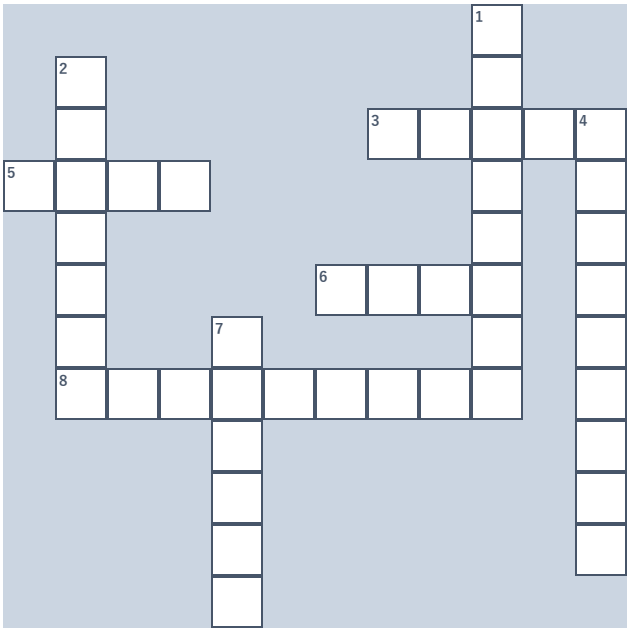
定義マッチング

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. VPN アプリ	A	ローカルネットワーク上のすべてのスマート家電を保護するゲートウェイレベルの暗号化。
2. ルーター VPN	B	ワンクリックで簡単にセットアップできるよう、サブスクリプションサービスが提供するソフトウェアパッケージ。
3. ネイティブクライアント	C	エラー出力とクライアントのステータスログを確認して、失敗したセットアップをデバッグすること。
4. .ovpn プロファイル	D	トラフィックの経路を区別して、特定のアプリが暗号化トンネルを迂回できるようにすること。
5. 鍵ペア	E	アプリをインストールせずに、OS 標準の設定内で通信を保護すること。
6. スプリットトンネリング	F	ドメイン検索のリークを防ぐためのネットワークリゾルバーのアドレス設定。
7. DNSサーバーの設定	G	WireGuard のハンドシェイクを確立するために必要な暗号トークン（公開鍵/秘密鍵）。
8. 接続ログ	H	サーバー、ポート設定、証明書キーを含む OpenVPN のファイル形式。

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. アプリをインストールせず、OS標準の設定の中で通信を保護すること (5)

5. ローカルネットワーク上のすべてのスマート家電を保護する、ゲートウェイ段階の暗号化 (4)

6. WireGuardのハンドシェイクを確立するために必要な、暗号の公開鍵と秘密鍵 (4)

8. 通信経路を分け、特定のアプリだけを暗号化トンネルの外に通すこと (9)

タテのカギ

1. サーバー、ポート設定、証明書キーを含むOpenVPNのファイル形式 (8)

2. ドメインの名前解決での漏えいを防ぐために、リゾルバーのアドレスを設定すること (7)

4. 契約サービスが提供する、ワンクリックで簡単に設定できるソフトウェア (9)

7. 失敗した設定をデバッグするために、エラー出力やクライアントの状態ログを確認すること (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

3 ヨコ: アプリをインストールせず、OS標準の設定の中で通信を保護すること (5 文字):

5 ヨコ: ローカルネットワーク上のすべてのスマート家電を保護する、ゲートウェイ段階の暗号化 (4 文字):

6 ヨコ: WireGuardのハンドシェイクを確立するために必要な、暗号の公開鍵と秘密鍵 (4 文字):

8 ヨコ: 通信経路を分け、特定のアプリだけを暗号化トンネルの外に通すこと (9 文字):

タテのカギ

1 タテ: サーバー、ポート設定、証明書キーを含むOpenVPNのファイル形式 (8 文字):

2 タテ: ドメインの名前解決での漏えいを防ぐために、リゾルバーのアドレスを設定すること (7 文字):

4 タテ: 契約サービスが提供する、ワンクリックで簡単に設定できるソフトウェア (9 文字):

7 タテ: 失敗した設定をデバッグするために、エラー出力やクライアントの状態ログを確認すること (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。

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

用語リスト

ブイピーエヌアプリ　ルーター　ネイテイブ　セツテイフアイル　キーペア
スプリツトトンネル　デイーエヌエス　セツゾクログ

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. ブイピーエヌアプリ
B. ルーター
C. ネイテイブ
D. セツテイフアイル
E. キーペア
F. スプリツトトンネル
G. デイーエヌエス
H. セツゾクログ

	定義とマッチ欄
	1. ドメインの名前解決での漏えいを防ぐために、リゾルバーのアドレスを設定すること。
	2. 通信経路を分け、特定のアプリだけを暗号化トンネルの外に通すこと。
	3. ローカルネットワーク上のすべてのスマート家電を保護する、ゲートウェイ段階の暗号化。
	4. WireGuardのハンドシェイクを確立するために必要な、暗号の公開鍵と秘密鍵。
	5. アプリをインストールせず、OS標準の設定の中で通信を保護すること。
	6. 失敗した設定をデバッグするために、エラー出力やクライアントの状態ログを確認すること。
	7. サーバー、ポート設定、証明書キーを含むOpenVPNのファイル形式。
	8. 契約サービスが提供する、ワンクリックで簡単に設定できるソフトウェア。

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. ヌエーイブアプリピ
2. ネブイテイ
3. アキペー
4. スイヌエエデー
5. ールター
6. イルイアセフツテ
7. トスネルンツプトリ
8. ゾグセロクツ

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	設定が終わったら確認すること			
2	VPNを使えるデバイス			
3	知っているVPNサービス			
4	旅行中にVPNを使う理由			
5	設定中に人が犯しがちなミス			
6	このワークシートで覚えておきたい言葉			
7	最初にオンにする設定			
8	優れたVPNプロバイダーが約束すること			
9	VPNを設定するときの手順			
10	VPNを使う場所			
11	偽のWi-Fiネットワークを見抜く方法			
12	VPNが隠せるもの			
13	インターネットプロバイダーが見られるもの			
14	ヘルプが見つかる場所			
15	始めるために必要なもの			

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! Coffee & Bytesに座っているよ。『Free_Wi-Fi_No_Password』という保護されていない公共ネットワークがあるんだ。学校のメールにログインして課題をアップロードしたいけど、ハッカーが心配なんだ。VPNなしでこのネットワークを使うと、どんなリスクがあるの? それと、VPNはどうやってデータを守るの?」

Alex（旅行する学生）

👱 「大変! プロジェクトのために海外を旅行中で、母国のサーバーでホストされている生物学のドキュメンタリーを見ようとしているんだ。でもサイトに『この動画は現在の場所ではご利用いただけません』と出る。どうしてブロックされるの? VPNがあれば、どうやって見られるようになるの?」

チェックポイント 9: 暗号を解読しよう

サーバー設定のトレーニングを完了するために、安全なトンネルの設定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

41 72 16 72 22 1 46 55 46 21 64 2 68 72 4 23 45

2 42 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: 始めるには何が必要ですか?

有効なVPNの契約または自分のVPNサーバー、対応する端末、そしてプロバイダーのアプリまたは手動設定に必要な情報 (サーバーアドレス、プロトコル、認証情報、鍵、証明書) が必要です。ほとんどの人は、公式アプリをインストールしてサインインし、接続をタップするだけです。

Q3: アプリなしで Windows に VPN を設定するにはどうすればよいですか?

設定 > ネットワークとインターネット > VPN を開いて VPN を追加を選び、プロバイダーのサーバー名、VPN の種類（IKEv2 や L2TP/IPsec など)、サインイン情報を入力します。その後、接続を選択します。

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: macOS をセットアップするにはどうすればよいですか?

プロバイダーの macOS アプリをインストールするか、System Settings > VPN を開いて VPN 設定を追加し、IKEv2、L2TP over IPSec、または Cisco IPSec を選んで、プロバイダーから提供されたサーバーアドレスと認証情報を入力します。

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: 無料 VPN を使えますか?

無料 VPN は、広告、機能の制限、利用状況の分析、データ上限、その他の収益化モデルに頼っている場合があります。利用する前に、プロバイダーのプライバシーポリシー、所有者、監査、ビジネスモデルを確認してください。

Q7: .ovpn ファイルはどう使いますか?

OpenVPN クライアントをインストールし、プロバイダーまたは管理者から入手した .ovpn プロファイルをインポートして、接続します。このファイルには、サーバーのアドレス、ポート、UDP か TCP かの設定が含まれ、証明書や鍵も含まれていることが多くあります。

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: スマートフォンとスマートテレビで VPN を使えますか?

はい。最近のVPNプロバイダーは、iOS、Android、macOS、Windows、Linux、スマートテレビ向けの専用アプリのほか、家庭内ネットワークのすべての機器を保護するルーター設定も提供しています。

Q10: キルスイッチとは何ですか?

キルスイッチは、VPN接続が切れたときにデバイスを自動的にインターネットから切断するセキュリティ機能です。これにより、暗号化されていないデータや本当のIPアドレスの漏えいを防ぎます。

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 を手動で設定するにはどうすればよいですか?

wg genkey と wg pubkey でキーペアを生成し、公開鍵をサーバーと共有して、自分の秘密鍵、ピアの公開鍵、許可されるIP、エンドポイントを列挙した設定を書きます。wg-quick ツールで起動します。 [2]

Q3: WebRTC リークとは何で、VPN はそれをどう防ぎますか?

WebRTCは、VPNが有効でも、実際のローカルIPアドレスとパブリックIPアドレスを明らかにする可能性があるブラウザープロトコルです。プレミアムVPNは、デスクトップ/モバイルアプリやブラウザー拡張機能でWebRTCリクエストをブロックまたは偽装します。

Q4: 自宅のルーターに VPN を安全に設定するにはどうすればよいですか?

ルーターが VPN クライアントモードに対応しているか確認し、管理ページにログインして、プロバイダーの OpenVPN または WireGuard のファイルをアップロードしてください。先にファームウェアの更新が必要なルーターもあります。設定後は、ネットワーク上のすべてのデバイスがトンネルを使います。

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: スプリットトンネリングとは何で、いつ使うべきですか?

スプリットトンネリングでは、どのアプリを暗号化された VPN トンネル経由にし、どのアプリを直接インターネットに接続するかを選べます。機密性の高い銀行アプリは VPN 経由にし、ローカルのゲームは直接接続して、VPN による遅延を避けるために使います。

Q7: 新しい VPN の設定が機能しているか確認するにはどうすればよいですか?

接続してから IP 確認サイトにアクセスしてください。VPN サーバーの IP アドレスと場所が表示されるはずです。DNS と WebRTC のリークテストを実行し、接続を一時的に切って、キルスイッチがトラフィックをブロックすることを確認してください。

Q8: 設定後に VPN が接続できない場合、何を確認すべきですか?

ログインまたは鍵、サーバーアドレスを確認し、選んだポートとプロトコルがブロックされていないか確かめてください。UDP と TCP を切り替えるか別のサーバーを試し、アプリの接続ログでエラーを確認してください。

Q9: DNS リーク保護とは何ですか?

DNSリーク防止は、ウェブサイトの検索クエリ(DNSクエリ)を、ISPのサーバーではなくVPNのプライベートで暗号化されたDNSサーバー経由で送信させます。これにより、ISPがあなたの訪問先サイトを追跡するのを防ぎます。

Q10: VPN は自動的に起動するようにすべきですか?

通常はそうです。ほとんどのアプリは起動時や、信頼できないWi-Fiで自動的に起動して接続できるため、他のアプリがデータを送り始める前に保護されます。

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. ネイティブクライアント

WindowsとmacOSにはどちらも、IKEv2とL2TP/IPsecに対応した標準のVPNクライアントが搭載されているため、多くの接続は追加のアプリなしで設定できます。

2. 鍵の生成

WireGuardのクイックスタートでは、wg genkeyで秘密鍵を作成し、wg pubkeyでそこから公開鍵を導き出します。 [2]

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。 [1]

4. プロファイルファイル

.ovpnプロファイルにはサーバーアドレス、ポート、プロトコル、証明書がまとめられているので、1回のインポートでOpenVPN接続を設定できます。

5. 既定のポート

OpenVPN は一般にポート 1194 を使用し、WireGuard の公式例では UDP ポート 51820 が使われています。トンネルを接続するには、ファイアウォールやルーターでこれらのポートを許可する必要がある場合があります。

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)は一般的なVPNプロトコルを検出してブロックすることがあります。TCPポート443のOpenVPNや難読化モードに切り替えると役立つ場合があります。

7. ルーターの対応範囲

ルーターにVPNを設定すると、VPNアプリを動かせないゲーム機やスマートテレビも含め、その先のすべてのデバイスを、各デバイスに何もインストールせずに保護できます。

8. キープアライブ

NATやファイアウォールの内側では、WireGuardのPersistentKeepalive設定（一般的には25秒）がトンネルへの到達性を保ちます。 [2]

9. TUN/TAPドライバー

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、クライアントのインストール時に設定されます。 [3]

10. スプリットトンネリング

セットアップ中に、スプリットトンネリングを使うと、選択したアプリやアドレスをVPNから除外でき、ローカルプリンターや、VPNのIPアドレスをブロックするアプリを使うときに役立ちます。

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.). Quick Start.
https://www.wireguard.com/quickstart/

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

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

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

解答: Windows、macOS、Android、iOS、Linux、ルーターでのVPN設定

1 問題 1

正解: A

指導メモ

モバイルデバイスにVPNを設定する最も簡単な方法は何ですか？ → アプリストアから公式のVPNアプリをダウンロードする

2 ルーターゲートウェイの設定 遅延

正解: B

指導メモ

ルーターVPNはゲートウェイで通信を暗号化し、ネイティブのVPNアプリをインストールできないIoTデバイス、ゲーム機、スマート家電を守ります。出典: DD-WRT OpenVPN Clients、Linksys Router Config。 [3]

3 問題 3

正解: A

指導メモ

WindowsとmacOSにはIKEv2やL2TP/IPsecなどのプロトコル用の標準クライアントが組み込まれているため、追加のソフトウェアをインストールしなくても接続を設定できます。

4 OpenVPN プロファイルのインポート ルーティング制御

正解: B

指導メモ

手動で設定するには、接続先サーバーのポート、プロトコルのパラメーター（UDP/TCP）、暗号証明書を含む.ovpn プロファイルキーをダウンロードする必要があります。出典: DD-WRT OpenVPN Clients。

5 スプリットトンネルのルーティング プライバシー

正解: B

指導メモ

スプリットトンネリングでは、機密性の高い業務アプリを暗号化トンネル経由にし、ローカルのストリーミングやゲームは VPN のオーバーヘッドなしで直接接続させることができます。出典: IETF IKEv2 RFC。

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

ルーターでの設定では、管理ページにログインし、VPNのサポートを確認して、設定ファイルをアップロードします。

7 OS とのネイティブ統合 速度

正解: 正しい

指導メモ

主要なオペレーティングシステムはプロトコルのネイティブ統合を組み込んでおり、安全な接続設定をスムーズに行えるようにしています。出典: Microsoft Native Gateway、Apple Support Profiles。

8 WireGuardの鍵のペア設定 スニッフィングのリスク

正解: 正しい

指導メモ

WireGuardは、パスワードやCAチェーンに頼らず、非対称鍵を使って安全なP2Pハンドシェイクを確立します。出典: WireGuard CLI Specifications。

9 ローカルトラフィックのブロック ファイアウォール

正解: 誤り

指導メモ

VPNは通常、公開インターネットの通信をルーティングし、特別な設定をしない限り、ローカルネットワークのプリンターへのアクセスをブロックすることがあります。出典: Microsoft Native Gateway。

10 問題 10

正解: 正しい

指導メモ

VPNアプリを実行できないスマートロックを保護するには、ルーターレベルのVPNが必要です。

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

B 1. VPN アプリ	A 2. ルーター VPN	E 3. ネイティブクライアント	H 4. .ovpn プロファイル
G 5. 鍵ペア	D 6. スプリットトンネリング	F 7. DNSサーバーの設定	C 8. 接続ログ

チェックポイント 3: 解答 – 重要用語

1 ルーター	2 設定ファイル	3 ネイティブ	4 キーペア
5 VPNアプリ	6 DNS		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 G – デイーエヌエス	2 F – スプリツトトンネル	3 B – ルーター	4 E – キーペア
5 C – ネイテイブ	6 H – セツゾクログ	7 D – セツテイフアイル	8 A – ブイピーエヌアプリ

指導者向けディスカッションメモ

重要用語:
生徒がVPN アプリ、ルーター VPN、ネイティブクライアント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。

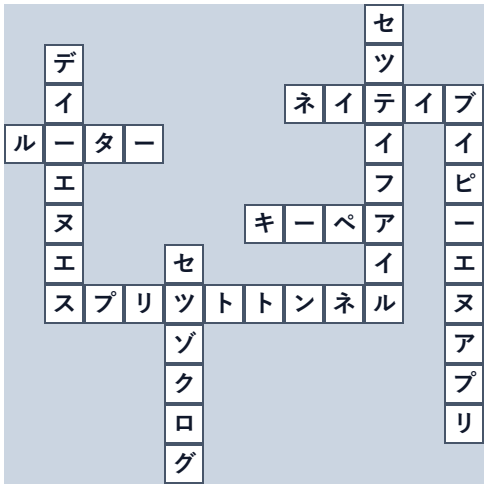
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: ネイテイブ アプリをインストールせず、OS標準の設定の中で通信を保護すること (5 文字)

5 ヨコ: ルーター ローカルネットワーク上のすべてのスマート家電を保護する、ゲートウェイ段階の暗号化 (4 文字)

6 ヨコ: キーペア WireGuardのハンドシェイクを確立するために必要な、暗号の公開鍵と秘密鍵 (4 文字)

8 ヨコ: スプリットトンネル 通信経路を分け、特定のアプリだけを暗号化トンネルの外に通すこと (9 文字)

タテのカギ

1 タテ: セツテイファイル サーバー、ポート設定、証明書キーを含むOpenVPNのファイル形式 (8 文字)

2 タテ: デイーエヌエス ドメインの名前解決での漏えいを防ぐために、リゾルバーのアドレスを設定すること (7 文字)

4 タテ: ブイピーエヌアプリ 契約サービスが提供する、ワンクリックで簡単に設定できるソフトウェア (9 文字)

7 タテ: セツゾクログ 失敗した設定をデバッグするために、エラー出力やクライアントの状態ログを確認すること (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. ヌエーイブアプリピ — ブイピーエヌアプリ
2. ネブイテイ — ネイテイブ
3. アキペー — キーペア
4. スイヌエエデー — デイーエヌエス
5. ールター — ルーター
6. イルイアセフツテ — セツテイフアイル
7. トスネルンツプトリ — スプリツトトンネル
8. ゾグセロクツ — セツゾクログ

秘密の暗号チャレンジ 解答

"ルーターニ アンゼンナ ブイピーエヌヲ イレル"

ケーススタディの解答

A シナリオ A: 公共ネットワークのセキュリティ

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:

- リスク: パケットの盗聴、データの傍受、中間者攻撃。同じカフェのネットワークにいる誰かが、彼女のログイン情報や宿題のファイルを取得するおそれがあります。
- VPNによる保護: ネットワークパケットのペイロードを暗号化し、VPNが正しく設定されていれば、傍受されたトンネル通信を、ローカルネットワーク上の受動的な盗み見から読めない状態にします。

B シナリオ B: ブロックされたリソースへのアクセス

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: 配信元はジオブロックを使っており、旅行者のローカルIPアドレスを実際の所在国に対応付け、地域ごとのライセンスに基づいてブロックします。
- VPN が役立つ点: 母国のサーバー経由で通信をルーティングすることで、本当の場所を隠します。サイトには母国の IP が見えるため、アクセスできます。