名前: 日付: 得点:

VPN の選び方 ワークシート

VPNプロバイダー、セキュリティ標準、監査、ログポリシーの評価

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

- プライバシーの観点から、プロバイダーの管轄権とゼロログポリシーを評価します。
- WireGuard や OpenVPN などのトンネリングプロトコルを速度の面で比較してください。
- キルスイッチやRAM専用サーバーノードなどのセキュリティ機能を分析してください。
- 選ぶ際に、独立したセキュリティ監査と料金プランを見分ける。
- 速度とジオブロック解除のニーズに基づいて、サーバーロケーションを選んでください。

選択ワークシートの指示

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。学んだ知識を安全なVPNインフラの選び方に応用しましょう。 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 の選び方（導入）

適切な VPN を選ぶには、宣伝文句にとらわれずに見る必要があります。信頼できるプロバイダーには、実証されたノーログポリシー、安全な暗号化プロトコル、オープンソースのクライアントが必要です。セキュリティ機能、管轄、速度性能を評価することで、デジタル保護のニーズに合った VPN を選べます。

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 1. 安全なVPNプロバイダーを選ぶときの重要な要素は何ですか?

- A. サーバーのある国の数
- B. 独立して監査されたノーログポリシー
- C. 月額料金が最も低いプラン
- D. 派手な広告スポンサーシップ

2 2. 速度と監査のしやすさのバランスが最も優れたVPNプロトコルはどれですか?

- A. PPTP(旧式)
- B. L2TP/IPSec
- C. OpenVPN over TCP のみ
- D. WireGuard

3 3. 機密性の高い活動に無料VPNを使うべきでないのはなぜですか?

- A. 米国では禁止されている
- B. 多くの場合、あなたのウェブ閲覧履歴を販売している
- C. 基本的なウェブ閲覧に対応していない
- D. 接続に特別なハードウェアが必要である

4 4. プロバイダーの本拠地の法的管轄は何を決めますか?

- A. サーバー接続の速度
- B. 対応デバイスの種類
- C. データ保持と捜索令状に関する現地の法律
- D. クライアントアプリのビジュアルテーマ

5 5. VPNクライアントの「キルスイッチ」機能の主な目的は何ですか?

- A. VPN接続が切れた場合にインターネットアクセスをブロックするため
- B. デバイスにインストールされているすべてのアプリを削除するため
- C. サーバー接続の速度を 2 倍にするため
- D. アイドル時にオペレーティングシステムを再起動するため

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. VPNは、マルウェアのダウンロードやウイルスファイルからデバイスを守ります。

○ 正しい ○ 誤り

7 質問 7

7. Deloitte などの企業による独立監査は、ゼロログの主張を検証しています。

○ 正しい ○ 誤り

8 質問 8

8. プロバイダーの所在国の法律は、ユーザーデータのプライバシーに影響しません。

○ 正しい ○ 誤り

9 質問 9

9. WireGuardのコンパクトなコードベースは、OpenVPNより監査しやすくなっています。

○ 正しい ○ 誤り

10 質問 10

10. 無料 VPN は、サーバー費用をまかなうために、広告を販売したりユーザーを追跡したりすることがよくあります。

○ 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. 独立して検証された _____ ポリシーは、VPN事業者がオンライン履歴を記録しないことを約束します。

2. 最新の _____ プロトコルは、高速でコードベースが非常に小さいのが特長です。

3. VPN接続が突然切れたときにすべての通信を停止する安全機能は _____ です。

4. 事業者の法的な _____ を評価すると、監視に関する条約の対象になるかどうかが分かります。

5. サーバーに _____ のディスクを採用すると、再起動後にユーザーデータが残りません。

6. ゼロ知識を謳うポリシーの検証には、信頼できる企業による第三者のセキュリティ _____ が必要です。

用語バンク

RAM専用　WireGuard　キルスイッチ　ゼロナレッジ　ノーログ　ファイブアイズ　監査　管轄

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

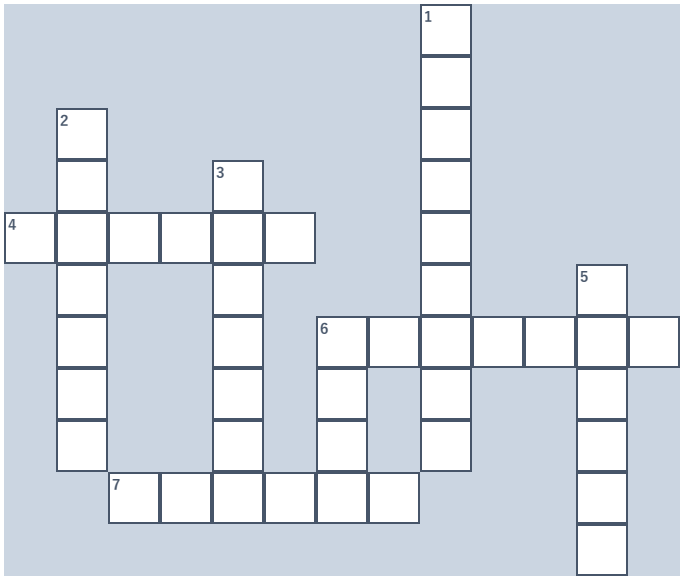
定義マッチング

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	ブラウザーデータを記録して販売することで収益化していることが多い、リスクの高い接続サービス。
2. 監査済みログ	B	安全なトンネルが切断された場合に、インターネットへのルーティングをブロックする安全機構。
3. 管轄	C	米国、英国、カナダ、オーストラリア、ニュージーランドの間の国際的な情報共有同盟。
4. キルスイッチ	D	揮発性メモリー上で動作するため、データがディスクに保存されないハードウェアインフラ。
5. ファイブ・アイズ	E	VPNプロバイダーの法的義務を定める地理的な地域。
6. 無料 VPN	F	約 4,000 行の監査しやすいコードを使った、最新の高速プロトコル。
7. RAM専用サーバー	G	WireGuardよりもコードベースがはるかに大きい、成熟していて広く監査されているオープンソースのプロトコル。
8. OpenVPN	H	独立した第三者のサイバーセキュリティ企業によって検証されたプライバシーに関する主張。

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

4. 約4,000行の監査しやすいコードで構成された、高速な最新プロトコル (6)

6. 独立した第三者のサイバーセキュリティ企業によって検証されたプライバシーの主張 (7)

7. 安全なトンネルが切断されたときにインターネット通信を遮断する安全機能 (6)

タテのカギ

1. 揮発性メモリのみで動作し、データの保存を防ぐハードウェア基盤 (9)

2. 米国・英国・カナダ・オーストラリア・ニュージーランドによる国際的な情報共有同盟 (7)

3. ソースコードが公開され、誰でも検証できる方式 (7)

5. サービス提供者がユーザーのデータを一切把握できないようにする仕組み (6)

6. VPN事業者の法的義務を定める地理的な地域 (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

4 ヨコ: 約4,000行の監査しやすいコードで構成された、高速な最新プロトコル (6 文字):

6 ヨコ: 独立した第三者のサイバーセキュリティ企業によって検証されたプライバシーの主張 (7 文字):

7 ヨコ: 安全なトンネルが切断されたときにインターネット通信を遮断する安全機能 (6 文字):

タテのカギ

1 タテ: 揮発性メモリのみで動作し、データの保存を防ぐハードウェア基盤 (9 文字):

2 タテ: 米国・英国・カナダ・オーストラリア・ニュージーランドによる国際的な情報共有同盟 (7 文字):

3 タテ: ソースコードが公開され、誰でも検証できる方式 (7 文字):

5 タテ: サービス提供者がユーザーのデータを一切把握できないようにする仕組み (6 文字):

6 タテ: VPN事業者の法的義務を定める地理的な地域 (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。

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

用語リスト

ワイヤガード　カンサズミログ　カンカツ　フアイブアイズ　キルスイツチ　ゼロナレツジ　ラムセンヨウサーバ　オープンソース

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. カンサズミログ
C. カンカツ
D. フアイブアイズ
E. キルスイツチ
F. ゼロナレツジ
G. ラムセンヨウサーバ
H. オープンソース

定義とマッチ欄
1. 安全なトンネルが切断されたときにインターネット通信を遮断する安全機能。
2. 約4,000行の監査しやすいコードで構成された、高速な最新プロトコル。
3. ソースコードが公開され、誰でも検証できる方式。
4. サービス提供者がユーザーのデータを一切把握できないようにする仕組み。
5. 米国・英国・カナダ・オーストラリア・ニュージーランドによる国際的な情報共有同盟。
6. 揮発性メモリのみで動作し、データの保存を防ぐハードウェア基盤。
7. VPN事業者の法的義務を定める地理的な地域。
8. 独立した第三者のサイバーセキュリティ企業によって検証されたプライバシーの主張。

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. カカツン
3. キスイチツル
4. ヨバーンサウラムセ
5. ミグズサカロン
6. イイアフブズア
7. ツゼレジナロ
8. ーンスオーソプ

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が隠せるもの			
2	価格よりも大事なこと			
3	VPNのレビューが読める場所			
4	VPNでは守れないもの			
5	VPNの営業担当者への質問			
6	インターネットプロバイダーが見られるもの			
7	VPNを選ぶときのチェックリストの項目			
8	VPNを使う場所			
9	VPNプロバイダーの危険なサイン			
10	プライバシーに関連する言葉			
11	最初に試すこと			
12	優れたVPNプロバイダーが約束すること			
13	旅行中にVPNを使う理由			
14	VPNを使えるデバイス			
15	VPNに関する誤解			

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

選び方ガイドのトレーニングを完了するために、安全なインフラの選び方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

1	46	55	46	21		12	13	19	33	20		42	71	72	20	45

27	6	8	13	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: なぜ VPN を使うべきですか?

VPNはデジタルプライバシーを守り、カフェや空港などの公共Wi-Fiでの接続を保護します。また、ISPが暗号化された通信の種類を識別できない場合には、通信内容に応じた速度制限を減らせる可能性があり、地域制限を回避して世界中のコンテンツにアクセスでき、リモートワークのリソースを守る助けにもなります。

Q3: VPN を使えば、オンラインで完全に匿名になれますか?

いいえ。VPN は IP アドレスを隠してトラフィックを暗号化しますが、ブラウザーのクッキー、ログイン中のアカウント（Google や Facebook など）、ブラウザーのフィンガープリント、あるいは VPN プロバイダーがデータを記録している場合には、追跡される可能性があります。

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: どのように収益を得ていますか?

ビジネスモデルを確認してください。サブスクリプション、フリーミアム、データ販売はいずれも VPN をどこまで信頼できるかに影響し、データを一切収集しないサービスはデータを販売できません。まずプライバシーポリシーを読んでください。 [1]

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: 「ノーログ」ポリシーとは何ですか?

ノーログポリシーは、プロバイダーが保持しないとしている活動データや接続データを説明するものです。正確な範囲は異なるため、読者はポリシーと独立監査の結果を確認してください。

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: ダブル VPN またはマルチホップルーティングとは何ですか?

マルチホップは、トラフィックを 2 台以上の VPN サーバーに順番に経由させます。これにより暗号化の層がもう 1 つ加わり、一方のサーバーが侵害されても、2 番目のホップから本当の IP アドレスを隠しておくのに役立ちます。

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: RAM 専用サーバーとは何で、なぜ重要ですか?

従来型のサーバーはデータをハードドライブに書き込むため、押収されたり侵害されたりする可能性があります。RAMのみ(ディスクレス)のサーバーは、完全に揮発性メモリ(RAM)上で動作します。サーバーを再起動または電源オフにすると、メモリ内のデータは消去されます。

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 トラフィックのパケットを通常の HTTPS ウェブトラフィック（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: 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: 5/9/14 Eyes 同盟とは何で、なぜ気にする必要がありますか?

管轄はプロバイダーが直面しうる法的手続きに影響しますが、実際のプライバシーリスクは、プロバイダーが保持するデータ、技術的なアーキテクチャ、所有者、透明性レポート、監査履歴にも左右されます。

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: なぜ VPN を運営・支持している組織を確認するのですか?

評判は重要です。信頼する前に、その会社の所有者や経営陣を調べ、第三者による公開監査を探し、独立したセキュリティの専門家や報道が何と言っているかを確認しましょう。 [1]

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、1990年代に Microsoft が主導するグループが開発した初期の VPN プロトコルで、現在は安全でないと考えられているため、最新の VPN は WireGuard や OpenVPN を使用します。 [1]

2. 市場評価

リモートワークの需要と企業のセキュリティ需要の高まりを背景に、世界のVPN市場は急速に成長しています。

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. 厳格な監査基準

トップクラスのVPNプロバイダーは、DeloitteやKPMG、PwCなどの会計事務所にノーログの主張を確認してもらい、Cure53などのセキュリティ企業にアプリとサーバーをテストしてもらっています。 [4]

5. 5 Eyes 同盟の成り立ち

米国、英国、カナダ、オーストラリア、ニュージーランドによるファイブ・アイズ情報提携は、第二次世界大戦期の連合国間の信号情報協力から生まれました。

6. ディープパケットインスペクション

高度なファイアウォールは、ディープパケットインスペクション(DPI)を使ってネットワークパケットのメタデータを分析し、標準的なVPN接続の特徴をブロックします。

7. 企業での利用

多くの組織は、リモートで働く従業員がデータベースなどの社内システムにアクセスできるよう VPN を提供しており、VPN は職場で広く使われるセキュリティツールとなっています。

8. 分散型VPN

分散型VPN(dVPN)は、ユーザー同士が運用するノードのネットワークにトラフィックを分散し、単一の集中型プロバイダーへの依存を減らします。

9. TORとVPNの匿名性の比較

VPNは通信を1つのプロバイダー経由でトンネリングしますが、Tor(The Onion Router)は、プライバシーを最大限に高めるため、通信を3つのボランティアのリレー(ガード、ミドル、エグジット)経由で送ります。 [5]

10. データ侵害のコスト

VPN とゼロトラストのアクセスモデル（すべてのユーザーとデバイスを確認する方式）を組み合わせると、組織はデータを守り、データ侵害の被害を抑えやすくなります。

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] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

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

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

解答: VPNプロバイダー、セキュリティ基準、監査、ログポリシーの評価

1 監査済みログポリシー プロトコル

正解: B

指導メモ

独立して監査されたノーログポリシーは、プロバイダーのゼロ知識プライバシーの主張を確認するための最も現実的な方法です。派手な宣伝や自己申告では十分ではありません。出典: Deloitte Advisory、Cure53 Audit。

2 WireGuardの優位性 遅延

正解: D

指導メモ

WireGuardは、コンパクトなコードベース(約4,000行)で、カーネル空間での最新かつ高速な接続ルーティングを実現し、監査を非常に効率的にします。出典: IETF Protocol RFC、WireGuard Project。

3 問題 3

正解: B

指導メモ

無料VPNでもサーバーの費用はかかっており、FTCは、広告の配信などのために、一部のVPNアプリが利用者のデータを第三者と共有していると警告しています。

4 法的管轄 ルーティング制御

正解: C

指導メモ

管轄によって、VPN が監視法、現地のデータ保持義務、秘密の政府召喚令状の対象になるかどうかが決まります。出典: Privacy Rights Clearinghouse。

5 キルスイッチによる保護 プライバシー

正解: A

指導メモ

トンネルが切断されると、キルスイッチはシステムのネットワークアダプターのルーティングを直ちに遮断し、本当のIPやDNSの露出による漏えいを防ぎます。出典: IETF Tunnel RFC。

解答: チェックポイント 2 – 正誤問題

6 **マルウェア対策の限界** IP マスキング 正解: 誤り

指導メモ

VPNは安全な暗号化パイプラインを提供しますが、ペイロードやファイルをスキャンしません。マルウェアのブロックにはウイルス対策ソフトが必要です。出典: Deloitte Advisory。

7 **独立監査** 速度 正解: 正しい

指導メモ

監査報告書は、サーバーソフトウェアの設定、RAMのみの構成への準拠、ログ用データベースが存在しないことを検証します。出典: Deloitte Advisory、Cure53 Audit。

8 **問題 8** 正解: 誤り

指導メモ

プロバイダーは本拠地の国の法律に従う必要があり、その中にはデータ保持の規則や、保有するデータの提出命令が含まれる場合があります。

9 **プロトコルのコードベースの規模** ファイアウォール 正解: 正しい

指導メモ

コードベースが小さいほど、攻撃対象領域が減り、セキュリティチームがプロトコルの完全性を確認しやすくなります。出典: WireGuard Project。

10 **広告収益化** ノーログ 正解: 正しい

指導メモ

無料VPNは、サブスクリプション料金がないため、収益を得るためにデータマイニング、トラフィックのプロファイリング、ブラウザーへの広告挿入に頼っています。出典: EDRi Retention Guidelines。

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

F 1. WireGuard	H 2. 監査済みログ	E 3. 管轄	B 4. キルスイッチ
C 5. ファイブ・アイズ	A 6. 無料 VPN	D 7. RAM専用サーバー	G 8. OpenVPN

チェックポイント 3: 解答 – 重要用語

1 ノーログ	2 WireGuard	3 キルスイッチ	4 管轄
5 RAM専用	6 監査		

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 A – ワイヤガード	3 H – オープンソース	4 F – ゼロナレツジ
5 D – フアイブアイズ	6 G – ラムセンヨウサーバ	7 C – カンカツ	8 B – カンサズミログ

指導者向けディスカッションメモ

重要用語:
生徒がWireGuard、監査済みログ、管轄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。

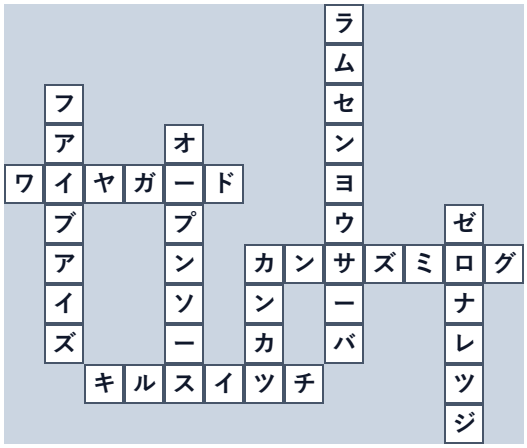
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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

4 ヨコ: ワイヤガード 約4,000行の監査しやすいコードで構成された、高速な最新プロトコル (6 文字)

6 ヨコ: カンサズミログ 独立した第三者のサイバーセキュリティ企業によって検証されたプライバシーの主張 (7 文字)

7 ヨコ: キルスイツチ 安全なトンネルが切断されたときにインターネット通信を遮断する安全機能 (6 文字)

タテのカギ

1 タテ: ラムセンヨウサーバ 揮発性メモリのみで動作し、データの保存を防ぐハードウェア基盤 (9 文字)

2 タテ: フアイブアイズ 米国・英国・カナダ・オーストラリア・ニュージーランドによる国際的な情報共有同盟 (7 文字)

3 タテ: オープンソース ソースコードが公開され、誰でも検証できる方式 (7 文字)

5 タテ: ゼロナレツジ サービス提供者がユーザーのデータを一切把握できないようにする仕組み (6 文字)

6 タテ: カンカツ VPN事業者の法的義務を定める地理的な地域 (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. カカツン — **カンカツ**
3. キスイチツル — **キルスイツチ**
4. ヨバーンサウラムセ — **ラムセンヨウサーバ**
5. ミグズサカロン — **カンサズミログ**
6. イイアフブズア — **フアイブアイズ**
7. ツゼレジナロ — **ゼロナレツジ**
8. ーンスオーソプ — **オープンソース**

秘密の暗号チャレンジ 解答

"アンゼンナ システムト レポートヲ ヒカクスル"

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。