名前: 日付: 得点:

VPN.com VPNガイド ワークシート

ネットワークプロトコル、トンネリング、セキュリティ制御の実践演習。

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

- データトンネリングとカプセル化の概念を説明します。
- 標準的なプロトコルの設定と帯域幅の要件を見分ける。
- インターネットのルーティングにおける、ファイアウォールと地域ブロックの役割を分析してください。
- ISPが暗号化されていない閲覧をどのように追跡するか、そしてVPNがそれをどう防ぐかを理解する。
- サーバーの所在地と管轄権が運用面でどこまで及ぶかの境界を区別します。

VPNガイドの手順

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。学んだ知識をケーススタディのセクションにある実際のシナリオに応用しましょう。 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とは?（導入）

仮想プライベートネットワークは、単なるプライバシーの切り替えスイッチではありません。インターネット通信をリモートサーバー経由で送る暗号化トンネルです。これによりIPアドレスが隠れ、ISPがオンラインでの行動のログを作成するのを防ぎ、公共ネットワーク上のデータを守ります。デジタルセキュリティを保つには、用語を理解することが欠かせません。

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. VPNプロトコルとは何ですか?
   - A. ケーブルをつなぐために使うハードウェア機器。
   - B. データの暗号化と送信方法を定めたルールの集まり。
   - C. 広告をブロックするブラウザープラグイン。
   - D. インターネットサービスプロバイダー企業。

2. 2. VPN の接続が遅く感じられる場合、最も可能性の高い原因は何ですか?
   - A. VPNサーバーが遠すぎるか、過負荷になっている。
   - B. モニターの解像度が高すぎる。
   - C. ウェブブラウザーの Cookie を無効にしている。
   - D. キーボードの配列が正しく設定されていない。

3. 3. 公共Wi-Fiに接続するとき、VPNの利用が強く推奨されるのはなぜですか?
   - A. Wi-Fi接続が無料になる。
   - B. ルーターの電波の届く範囲が広がる。
   - C. トラフィックを暗号化し、同じネットワーク上のハッカーを防ぐ。
   - D. 迷惑メールを自動的に削除する。

4. 4. ジオブロックを説明しているのは、次のうちどれですか?
   - A. サーバーまでの物理的な距離を測るツール。
   - B. 場所に基づいてサイトへのアクセスをブロックする制限。
   - C. ローカルでのファイル圧縮用プロトコル。
   - D. バックアップの保存の仕組み。

5. 5. VPNを使用すると、インターネットサービスプロバイダー(ISP)には何が見えますか?
   - A. 検索キーワードと、閲覧したウェブページの内容。
   - B. VPNに接続していることは分かるが、トラフィックの詳細は分からない。
   - C. 一切の情報が見えない。オンラインであることさえわからない。
   - D. ローカルのハードドライブにあるファイルと写真。

チェックポイント 2: 正しい・誤りチャレンジ

6 位置情報のマスキング

6. VPNはデバイスの公開IPアドレスを隠すため、第三者のウェブサイトが物理的な所在地を簡単に特定できなくなります。

○ 正しい ○ 誤り

7 VPNが速度に与える影響

7. VPN接続を有効にすると、VPNなしの接続と比べて、基本のインターネット速度が二倍になります。

○ 正しい ○ 誤り

8 公共 Wi-Fi でのスニッフィング

8. VPN なしで保護されていない公衆 Wi-Fi ネットワークを使うと、同じネットワーク上の他のユーザーが、暗号化されていないあなたの通信を傍受できる可能性があります。

○ 正しい ○ 誤り

9 ファイアウォールと遮断された接続

9. ネットワーク管理者は、外向きの VPN 接続トンネルを検出して遮断するようにファイアウォールを設定できます。

○ 正しい ○ 誤り

10 厳格なノーログポリシー

10. 厳格な「ノーログ」ポリシーとは、VPNプロバイダーがあなたの検索クエリと閲覧したリンクを少なくとも30日間保存することを法的に義務づけられているという意味です。

○ 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. 通信を守るため、VPNはデータパケットを別のプロトコルで包みます。この処理は _____ と呼ばれます。

2. ストリーミング中にダウンロード速度が遅いなら、ネットワークの _____ が限られていることが原因かもしれません。

3. 特定の国でしか利用できない配信サービスは、世界のユーザーを制限するために _____ を使っています。

4. 暗号化や接続のパラメーターを定める接続ルールは、VPN _____ と呼ばれます。

5. お使いのコンピューターは、ネットワークの通信を監視して安全でない接続を遮断するローカルの _____ を使います。

6. VPNに接続すると、公開IPを隠すために通信が遠隔の _____ 経由になります。

用語バンク

ISP　サーバー　ジオブロック　トンネリング　ファイアウォール　プライバシー　プロトコル　帯域幅

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

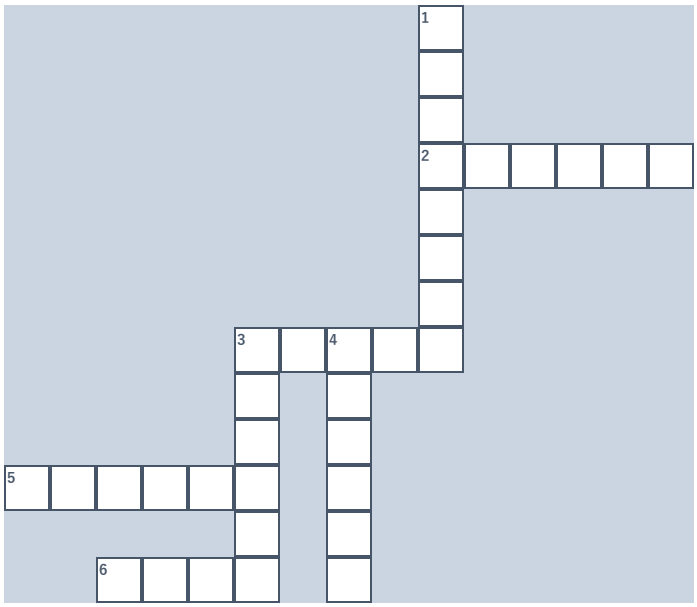
定義マッチング

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. トンネリング	A	ネットワーク上でデータをどのように伝送するかを決めるルールの集まり。
2. プロトコル	B	接続を通じて転送できるデータの最大速度。
3. 帯域幅	C	物理的な所在地に基づいてウェブアクセスを妨げる制限。
4. サーバー	D	無許可の通信を監視してブロックするセキュリティシステム。
5. ジオブロック	E	通信を経由させてIPアドレスを隠すリモートコンピューター。
6. ファイアウォール	F	追跡や公的な監視を受けていない状態。
7. プライバシー	G	あなたの通信を運び、暗号化されていない活動を見ることができるインターネットサービスプロバイダー。
8. ISP	H	安全に転送するために、データパケットを別のパケットの中に包むこと。

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. インターネットサービスプロバイダー。暗号化されていなければ通信を記録する (6)

3. データをネットワーク上でどう送るかを決める規則の集まり (5)

5. 接続を通じてデータを転送できる最大の速度 (6)

6. 通信を中継し、IPアドレスを隠す遠隔のコンピューター (4)

タテのカギ

1. 許可されていない通信を監視して遮断するセキュリティシステム (8)

3. 追跡や公的な監視を受けない状態 (6)

4. 安全に送るために、データパケットを別のパケットで包むこと (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

2 ヨコ: インターネットサービスプロバイダー。暗号化されていなければ通信を記録する (6 文字):

3 ヨコ: データをネットワーク上でどう送るかを決める規則の集まり (5 文字):

5 ヨコ: 接続を通じてデータを転送できる最大の速度 (6 文字):

6 ヨコ: 通信を中継し、IPアドレスを隠す遠隔のコンピューター (4 文字):

タテのカギ

1 タテ: 許可されていない通信を監視して遮断するセキュリティシステム (8 文字):

3 タテ: 追跡や公的な監視を受けない状態 (6 文字):

4 タテ: 安全に送るために、データパケットを別のパケットで包むこと (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。

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

トンネリング　プロトコル　タイイキハバ　サーバー　ジオブロツク　フアイアウオール
プライバシー　アイエスピー

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. トンネリング
B. プロトコル
C. タイイキハバ
D. サーバー
E. ジオブロツク
F. フアイアウオール
G. プライバシー
H. アイエスピー

定義とマッチ欄
1. 追跡や公的な監視を受けない状態。
2. 物理的な所在地に基づいてウェブへのアクセスを妨げる制限。
3. データをネットワーク上でどう送るかを決める規則の集まり。
4. 許可されていない通信を監視して遮断するセキュリティシステム。
5. 接続を通じてデータを転送できる最大の速度。
6. 通信を中継し、IPアドレスを隠す遠隔のコンピューター。
7. インターネットサービスプロバイダー。暗号化されていなければ通信を記録する。
8. 安全に送るために、データパケットを別のパケットで包むこと。

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. ネトリングン
2. バタイハキイ
3. ジブロクツオ
4. ーバイシプラ
5. トルプコロ
6. バーサー
7. フルウオーアアイ
8. エーアピスイ

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	「トンネル」という言葉から連想するもの			
2	VPNについて家族に教えたいこと			
3	ウェブサイトにあるトラッキングの手段			
4	VPNに関する誤解			
5	このワークシートで覚えておきたい言葉			
6	VPNを使えるデバイス			
7	VPNでは守れないもの			
8	オンラインで「訪れて」みたい国			
9	優れたVPNプロバイダーが約束すること			
10	偽のWi-Fiネットワークを見抜く方法			
11	VPNについての疑問			
12	知っているVPNサービス			
13	プライバシーに関連する言葉			
14	VPNが隠せるもの			
15	カフェでVPNを使う理由			

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

VPNは通信を暗号化して保護します。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、サイバーセキュリティの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	46	55	46	21		20	46	24	41	60		69	39	2	62	12	72	45

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: VPN を使うことは合法ですか?

VPNの使用は多くの国で合法ですが、VPNサービスを制限、規制、またはブロックしている地域もあります。使用する前に、現在のローカルの法律を確認してください。詳しくは、VPN.comの合法性に関するガイドをご覧ください。

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。 [3]

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: 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: VPN は ISP によるインターネットの速度制限を回避できますか?

場合によります。ISP が特定の通信だけを選んで遅くしている場合は VPN が役立つことがありますが、混雑、データ容量の上限、アカウント単位の速度制限、ネットワーク品質の低さを克服することはできません。

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. 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、外部の監査人(Cure53やPwCなど)を雇い、独立したコードレビューを行って、ユーザーの活動を記録していないことを検証しています。

5. 5 Eyes 同盟の成り立ち

ファイブ・アイズ同盟は、米国と英国の間で結ばれた1946年のUKUSA信号情報協定に始まり、その後カナダ、オーストラリア、ニュージーランドが加わりました。

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. 企業での利用

世界中の企業の従業員の多くが、社内データベースへのログインに安全なVPNを利用しており、重要なセキュリティ標準になっています。

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)経由で送るため、どのリレーも両端を知ることはありません。

10. データ侵害のコスト

VPNを使ったゼロトラストのセキュアアクセスモデルを採用すると、組織は知的財産を守り、データ侵害による経済的影響を軽減しやすくなります。

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。

学術文献とセキュリティ標準

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

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

技術標準の概要

- カプセル化の標準: RFC 4301は、安全なIPsec/L2TPインターネットパケットのルーティングを定義しています。
- ISP による追跡: DNS クエリを暗号化された VPN トンネル経由でルーティングすると、ローカルの ISP から DNS が見える範囲を減らせる場合があります。
- ファイアウォール制御プロトコル: 難読化されたステルスパケットは、ディープパケットフィルターを回避します。

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

VPNプロトコルは、トンネルの構築とデータの暗号化に関するルールを定めたものです。他の選択肢は、ケーブル、広告ブロッカー、ISPについての説明です。

2 問題 2

正解: A

指導メモ

距離はレイテンシーを増やし、過負荷のサーバーは分け合える容量が減ります。画面解像度、Cookie、キーボードレイアウトは接続速度に影響しません。

3 問題 3

正解: C

指導メモ

オープンなネットワークでは、他の人が暗号化されていないパケットを傍受できます。VPNは通信を暗号化するため、傍受されたデータは読み取れません。

4 問題 4

正解: B

指導メモ

ジオブロッキングは、訪問者のパブリックIPアドレスを位置情報データベースと照合し、許可された地域の外からのアクセスを拒否します。

5 問題 5

正解: B

指導メモ

ISPは、暗号化されたデータをVPNサーバーに送信していることはわかりますが、どのサイトを訪問しているか、何を検索しているかはわかりません。

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

ウェブサイトにはあなたのIPアドレスではなくVPNサーバーのIPアドレスが表示されるため、おおよその所在地が相手に知られません。

7 問題 7

正解: 誤り

指導メモ

暗号化とVPNサーバーへの追加の中継により、通常は速度がわずかに低下します。VPNでベースラインの接続速度が2倍になることはありません。

8 問題 8

正解: 正しい

指導メモ

保護されていないWi-Fiでは、パケットスニッフィングツールによって、HTTPSなしで送信されたログイン情報などの暗号化されていない通信が取得されることがあります。

9 問題 9

正解: 正しい

指導メモ

管理者は、OpenVPNの1194などの既知のVPNポートをブロックしたり、ディープパケットインスペクションを使ってVPN通信を検出したりできます。

10 問題 10

正解: 誤り

指導メモ

ノーログポリシーとは、利用者の活動の記録を保持しないというプロバイダーの約束です。VPNに検索内容を30日間保存することを義務づける法律はありません。

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

H 1. トンネリング	A 2. プロトコル	B 3. 帯域幅	E 4. サーバー
C 5. ジオブロック	D 6. ファイアウォール	F 7. プライバシー	G 8. ISP

チェックポイント 3: 解答 – 重要用語

1 トンネリング	2 帯域幅	3 ジオブロック	4 プロトコル
5 ファイアウォール	6 サーバー		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 G – プライバシー	2 E – ジオブロツク	3 B – プロトコル	4 F – フアイアウオール
5 C – タイイキハバ	6 D – サーバー	7 H – アイエスピー	8 A – トンネリング

指導者向けディスカッションメモ

重要用語:
生徒がトンネリング、プロトコル、帯域幅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。

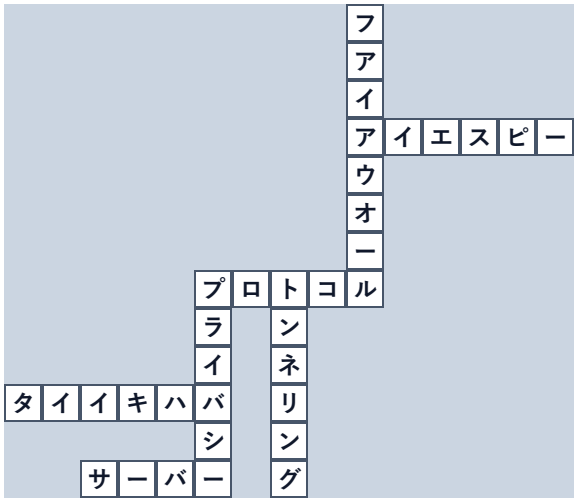
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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



ヨコのカギ

2 ヨコ: アイエスピー インターネットサービスプロバイダー。暗号化されていなければ通信を記録する (6 文字)

3 ヨコ: プロトコル データをネットワーク上でどう送るかを決める規則の集まり (5 文字)

5 ヨコ: タイイキハバ 接続を通じてデータを転送できる最大の速度 (6 文字)

6 ヨコ: サーバー 通信を中継し、IPアドレスを隠す遠隔のコンピューター (4 文字)

タテのカギ

1 タテ: ファイアウォール 許可されていない通信を監視して遮断するセキュリティシステム (8 文字)

3 タテ: プライバシー 追跡や公的な監視を受けない状態 (6 文字)

4 タテ: トンネリング 安全に送るために、データパケットを別のパケットで包むこと (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. ネトリングン — トンネリング
2. バタイハキイ — タイイキハバ
3. ジブロクツオ — ジオブロツク
4. ーバイシプラ — プライバシー
5. トルプコロ — プロトコル
6. バーサー — サーバー
7. フルウオーアアイ — フアイアウオール
8. エーアピスイ — アイエスピー

秘密の暗号チャレンジ 解答

"アンゼンナ トンネルデ プライバシーヲ マモル"

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。