名前: 日付: 得点:

IP アドレスを隠す方法 ワークシート

IP アドレスの隠蔽、位置情報のマスキング、プロキシ、Tor、DNS/WebRTC 漏えいの防止

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

- IPアドレスがどのように機能し、どのように位置情報が漏れるかを説明します。
- ネットワークアドレスを隠す手段として、プロキシ、Tor、VPN を比較してください。
- DNS と WebRTC の漏えいを検出して防ぐ方法を見分ける。
- Webサイトが公開IPを通じてユーザーをどのように追跡するかを理解する。
- IP保護のためのマルチホップルーティングと暗号化トンネルを評価します。

IP 保護ワークシートの説明

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IPアドレスの隠蔽と漏えいの防止に応用しましょう。 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。

IP を隠す(導入)

IPアドレスは、あなたの物理的な所在地やネットワークの利用傾向を明らかにするデジタルの住所です。IPを隠すことは、オンラインの追跡、ターゲットのプロファイリング、位置情報によるブロックに対する最初の防御線です。アドレスを安全に隠す方法を理解すると、オンラインのプライバシーを守るのに役立ちます。

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. デバイスのパブリックIPアドレスから、訪問したウェブサイトには何がわかりますか？

- A. ユーザーのクレジットカード番号
- B. おおよその所在地とISPの名前
- C. ローカルのファイルディレクトリ全体
- D. キーボードの言語設定

2. IPを隠し、システム全体のすべてのトラフィックを暗号化する方法はどれですか?

- A. 標準的なウェブプロキシ
- B. ブラウザーのCookieを消去すること
- C. 仮想プライベートネットワーク（VPN）
- D. ネイティブのファイアウォールを無効にすること

3. 無料のウェブプロキシを使う場合の、プライバシー面での大きな制限は何ですか?

- A. 公共ネットワーク上のデータ通信を暗号化しない
- B. 外部のオペレーティングシステムをインストールする必要がある
- C. 米国では完全に違法である
- D. 専用の電話回線接続が必要になる

4. 4. Torネットワークは、どのようにして利用者に高い匿名性を提供しますか？

- A. 接続速度を高速化する
- B. ボランティアが運営する3つのリレーを経由して通信を送る
- C. 利用者の名前を世界的なデータベースに登録する
- D. アクセスを政府機関のみに制限する

5. 5. DNSリークとは何ですか?

- A. 間違ったアドレスにメールを送ってしまうエラー
- B. DNSクエリがVPNトンネルを迂回してISPに送られるとき
- C. ローカルルーターの電源装置のハードウェア障害
- D. ローカルネットワークアダプターのドライバーの更新

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. プロキシサーバーは、VPNと同じようにバックグラウンドのOS通信を暗号化します。

○ 正しい ○ 誤り

7 質問 7

7. Torのルーティングは非常に安全ですが、ネットワークの閲覧速度が低下します。

○ 正しい ○ 誤り

8 質問 8

8. WebRTCリークにより、VPNセッション中でも実際のIPが露出する可能性があります。

○ 正しい ○ 誤り

9 質問 9

9. VPNをオンにして漏えいがなければ、ISPはあなたがどのウェブサイトを訪問しているか見ることができません。

○ 正しい ○ 誤り

10 質問 10

10. IP アドレスを隠すと、ブラウザーフィンガープリントによる追跡を防げます。

○ 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. VPNトンネルを迂回して、閲覧したドメインへの問い合わせが露出する問題は _____ と呼ばれます。

2. ブラウザベースの _____ 通信APIは、本来のIPアドレスをうっかり漏らすことがあります。

3. _____ はブラウザの通信を転送しますが、パケットのペイロードは暗号化しません。

4. 多層暗号化を行う _____ は、高いレベルの匿名性を提供します。

5. あなたの公開 _____ は通信事業者から割り当てられ、おおよその地域を明らかにします。

6. 地域ごとの動画配信の制限を回避するには、位置情報の _____ を行います。

用語バンク

DNSリーク　IPアドレス　Torネットワーク　WebRTC　ウェブプロキシ　マスキング　暗号化トンネル　追跡

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

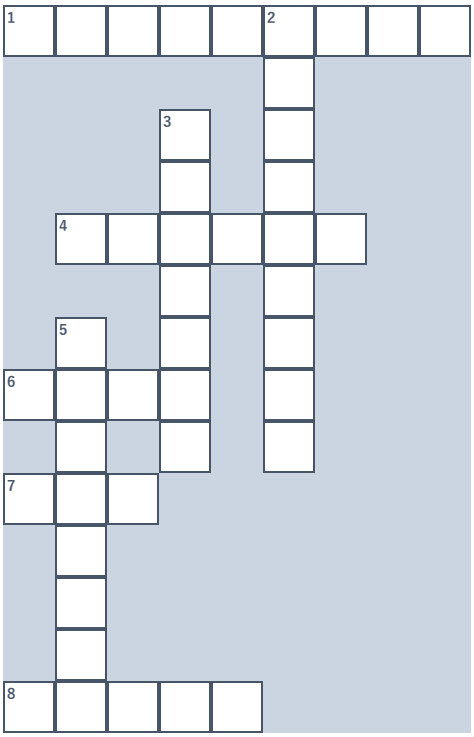
定義マッチング

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. IP アドレス	A	デバイスのすべての通信を暗号化し、VPNサーバー経由で送ります。
2. VPN トンネル	B	3 つのボランティアのサーバーを経由してデータを送り、各段階で層ごとに暗号化します。
3. Tor ネットワーク	C	ジオブロックを回避するために、別の国のサーバーを経由して接続すること。
4. ウェブプロキシ	D	インターネット上のデバイスインターフェースを識別する固有の数値ラベル。
5. DNS リーク	E	システムレベルの暗号化なしに、アプリケーション層でブラウザーの通信を転送すること。
6. WebRTC API	F	通信事業者による、暗号化されていないインターネット通信の接続先の記録。
7. 位置情報の隠蔽	G	VPN トンネルの外で名前解決されるクエリで、閲覧したドメインが ISP に露出します。
8. ISPによる追跡	H	音声/動画用のブラウザー機能で、トンネルを迂回して実際のIPアドレスを露出させる可能性があるもの。

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

1. デバイスの全通信を暗号化し、VPNサーバー経由で送る仕組み (9)

4. 特定の地域からのアクセスを制限する仕組み (6)

6. 暗号化されていない通信の宛先を通信事業者が記録すること (4)

7. VPNトンネルの外で名前解決が行われ、訪問したドメインがISPに知られてしまうこと (3)

8. 別の国のサーバーを経由して接続し、地域制限を回避すること (5)

タテのカギ

2. 3つのボランティアサーバーを経由させ、各段階で層ごとに暗号化する通信経路 (9)

3. システム全体を暗号化せず、アプリケーション層でブラウザの通信を転送するもの (7)

5. インターネット上でデバイスのインターフェースを識別する固有の数値ラベル (8)

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

1 ヨコ: デバイスの全通信を暗号化し、VPNサーバー経由で送る仕組み (9 文字):

4 ヨコ: 特定の地域からのアクセスを制限する仕組み (6 文字):

6 ヨコ: 暗号化されていない通信の宛先を通信事業者が記録すること (4 文字):

7 ヨコ: VPNトンネルの外で名前解決が行われ、訪問したドメインがISPに知られてしまうこと (3 文字):

8 ヨコ: 別の国のサーバーを経由して接続し、地域制限を回避すること (5 文字):

タテのカギ

2 タテ: 3つのボランティアサーバーを経由させ、各段階で層ごとに暗号化する通信経路 (9 文字):

3 タテ: システム全体を暗号化せず、アプリケーション層でブラウザの通信を転送するもの (7 文字):

5 タテ: インターネット上でデバイスのインターフェースを識別する固有の数値ラベル (8 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	ジ	ロ	ボ	ワ	ラ	キ	ゼ	ゴ
ザ	ス	ホ	ノ	オ	ア	オ	オ	キ	ル	マ	パ	ホ	ヒ	パ
ヘ	ボ	キ	ズ	フ	サ	ン	ブ	メ	ハ	ス	コ	ヌ	ヤ	モ
ク	ヘ	セ	ワ	レ	テ	モ	ロ	モ	ン	キ	ギ	ゲ	ズ	ジ
ー	ツ	イ	カ	ゴ	ア	ワ	ツ	ラ	ニ	ン	グ	カ	ア	バ
ワ	コ	ツ	ザ	ペ	ン	ダ	ク	キ	ポ	グ	バ	タ	イ	フ
ト	ト	ー	コ	モ	ゴ	サ	ガ	ウ	ベ	レ	カ	ゾ	ピ	エ
ツ	ア	ー	ユ	コ	ウ	ヘ	イ	エ	サ	ラ	サ	ソ	ー	テ
ネ	ヌ	コ	ギ	ン	カ	メ	ス	ブ	ヌ	グ	ポ	ゴ	ア	ソ
ア	ガ	ド	セ	イ	ト	リ	イ	プ	ガ	リ	ヤ	レ	ド	ズ
ー	ボ	ワ	ヒ	グ	ン	ー	ゼ	ロ	ゲ	ケ	ヤ	プ	レ	オ
ト	タ	グ	ベ	ブ	ネ	ク	ノ	キ	イ	ギ	ー	ピ	ス	ピ
マ	ツ	ヌ	メ	ガ	ル	ヒ	ム	シ	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

アイピーアドレス　アンゴウカトンネル　トーアネツトワーク　ウエブプロキシ　リーク
ジオブロツク　マスキング　ツイセキ

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. アイピーアドレス
B. アンゴウカトンネル
C. トーアネツトワーク
D. ウエブプロキシ
E. リーク
F. ジオブロツク
G. マスキング
H. ツイセキ

定義とマッチ欄
1. システム全体を暗号化せず、アプリケーション層でブラウザの通信を転送するもの。
2. 別の国のサーバーを経由して接続し、地域制限を回避すること。
3. 特定の地域からのアクセスを制限する仕組み。
4. インターネット上でデバイスのインターフェースを識別する固有の数値ラベル。
5. 3つのボランティアサーバーを経由させ、各段階で層ごとに暗号化する通信経路。
6. 暗号化されていない通信の宛先を通信事業者が記録すること。
7. VPNトンネルの外で名前解決が行われ、訪問したドメインがISPに知られてしまうこと。
8. デバイスの全通信を暗号化し、VPNサーバー経由で送る仕組み。

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. レーアアドイスピ
2. クトーネートワツア
3. クーリ
4. キグンマス
5. ンカンルトウアネゴ
6. キブロウプシエ
7. ツジロクブオ
8. ツキセイ

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	旅行中にVPNを使う理由			
2	知っているブラウザー			
3	VPNが隠せるもの			
4	プライバシーに関連する言葉			
5	このワークシートで覚えておきたい言葉			
6	IPアドレスからウェブサイトが推測できること			
7	IPアドレスにある数字や記号			
8	VPNに関する誤解			
9	知っているVPNサービス			
10	インターネットプロバイダーが見られるもの			
11	優れたVPNプロバイダーが約束すること			
12	本当のIPが漏れる原因			
13	自分の位置情報を隠す理由			
14	IPアドレスを隠す方法			
15	VPNを使えるデバイス			

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

IPマスキングのトレーニングを完了するために、デジタルの痕跡を隠すことについてのこの秘密の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

32	4	21	2		38	3	22		1	61	42	13	45		6	8	13

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: ウェブプロキシは IP アドレスを隠しますか?

はい、ただし、プロキシを通して送ったトラフィック(通常はブラウザー)に限られます。ほとんどのウェブプロキシはデータを暗号化しないため、ISPやネットワーク事業者には、送受信している内容が見える場合があります。

Q5: IP アドレスを隠すことは合法ですか?

多くの国では合法ですが、VPN など IP アドレスを隠すためのツールを制限または禁止している国もあります。IP を隠しても違法な行為が合法になることはないため、使用する前に現地の法律を確認してください。

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: Tor は IP アドレスを隠しますか?

はい。Tor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、ウェブサイトにはエグジットリレーのアドレスが見え、どのリレーも「あなたが誰か」と「どこへ接続するか」の両方を知ることはありません。 [1]

Q7: IP アドレスから何がわかりますか?

パブリックIPからは通常、ISPと、国や都市などおおよその所在地がわかります。サイトはこれを使って、あなたの訪問を関連づけたり、地域によるブロックを適用したりすることもできます。

Q8: 隠れていることを確認するにはどうすればよいですか?

VPN に接続してから IP 確認サイトにアクセスし、DNS と WebRTC のリークテストを実行してください。表示される IP と DNS サーバーは、ISP ではなく VPN のものであるはずです。本当の IP が表示された場合は、リーク対策をオンにしてください。

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: IP アドレスを隠しても、なぜウェブサイトは私を追跡できるのですか?

IP を隠しても、ブラウザーフィンガープリントは防げません。トラッカーは、画面解像度、インストール済みフォント、ブラウザーの設定などの情報を組み合わせて識別子にでき、クッキーやサインイン済みのアカウントからも特定されることがあるため、プライバシー重視のブラウザーも併せて使ってください。 [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: IPv6 トラフィックで本当の IP アドレスが漏れることはありますか?

はい、VPNがIPv4しかトンネルしない場合です。その場合、端末がIPv6の通信をトンネルの外に送り、ISPが割り当てたアドレスが露出することがあります。IPv6をトンネルまたはブロックするVPNを使い、IPv6リークテストで確認してください。

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で本当の IP アドレスが露出しますか?

はい、除外したアプリについては該当します。トンネル外に送られる通信は実際のIPを使います。また、RFC 8828によると、ブラウザーが制限しない限り、WebRTCはスプリットトンネルVPNの下でもISPのアドレスを明らかにすることがあります。 [2]

Q7: 共有 IP アドレスとは何で、プライバシーにどう役立ちますか?

共有IPでは、多くのVPNユーザーが同じアドレスで同時にオンラインに表示されます。そのため、あなただけが使う専用IPに比べて、ウェブサイトが特定の1回の訪問をあなたに結び付けるのがはるかに難しくなります。

Q8: IP アドレスを隠すために VPN を使っていることは ISP に見えますか?

通常はそうです。ISPは、VPNサーバーのIPアドレスに接続していること、接続した時刻、送信したデータ量を確認できますが、訪問したWebサイトや暗号化トンネル内の内容は見えません。

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: IP を隠すにはプロキシと VPN のどちらが適していますか?

たいていはVPNのほうが優れています。VPNはデバイス上のすべてのアプリのIPアドレスを隠して通信を暗号化しますが、ウェブプロキシは通常ブラウザーだけが対象で、暗号化されないことも多いためです。

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、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。

2. フィンガープリンティング

IP を隠しても、ブラウザーフィンガープリントは防げません。画面解像度やインストール済みフォントなどの情報から、あなたを特定できる場合があります。 [3]

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。

4. WebRTC によるアドレスの露出

RFC 8828 は、ブラウザーが制限しない限り、WebRTC によって VPN の公開アドレスと、その VPN が動作している ISP のアドレスの両方が検出されうると警告しています。 [2]

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. TORサーキットの再利用

Torは同じ回線を約10分間再利用してから新しい回線を作るため、閲覧活動を結び付けにくくなります。 [1]

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。 [1]

10. プロキシと VPN トンネルの比較

ウェブプロキシは、ブラウザー通信でサイトに見えるIPアドレスを変えますが、VPNと違って通常はその通信を暗号化せず、デバイス上の他のアプリも対象にしません。 [5]

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

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

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

[5] 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

解答: IPアドレスの隠蔽、位置情報のマスキング、プロキシ、Tor、DNS/WebRTC漏えいの防止

1 問題 1

正解: B

指導メモ

デバイスのパブリックIPアドレスから、訪問したウェブサイトには何がわかりますか？ → おおよその所在地とISPの名前

2 VPNのシステム暗号化 遅延

正解: C

指導メモ

ブラウザーの通信だけをリダイレクトするプロキシとは異なり、VPNはシステム全体の暗号化トンネルを作り、バックグラウンドのアプリ、ゲーム、OSのクエリも保護します。出典: Tor Project Relays, W3C WebRTC API。

3 プロキシに暗号化がないこと Wi-Fiセキュリティ

正解: A

指導メモ

ウェブプロキシはブラウザーのトラフィックを転送するだけでパケットのペイロードを暗号化しないため、ネットワーク事業者やISPはコンテンツの通信を追跡できます。出典: IETF Proxy Vulnerabilities。

4 問題 4

正解: B

指導メモ

Torネットワークは、どのようにして利用者に高い匿名性を提供しますか？ → ボランティアが運営する3つのリレーを経由して通信を送る

5 DNSトンネルによる漏えい プライバシー

正解: B

指導メモ

DNSリークは、ドメイン名解決のリクエストがVPNトンネルを迂回してISPのリゾルバーに直接送られ、訪問したドメインの記録が露出することです。出典: DNSSEC Tunnel Testing、EFF Tracking Evasion。

解答: チェックポイント 2 – 正誤問題

6 **プロキシの制限の詳細** IP マスキング — **正解: 誤り**

指導メモ

プロキシはアプリケーション層で動作し、VPN トンネルのようなシステム全体のネットワークドライバー統合を備えていません。出典: IETF Proxy Vulnerabilities.

7 **問題 7** — **正解: 正しい**

指導メモ

ボランティアの3つのリレーを層状の暗号化で経由させるとレイテンシーが増えるため、Torは通常、直接接続よりも低速です。

8 **問題 8** — **正解: 正しい**

指導メモ

WebRTCは、ローカルアドレスを明らかにすることがあり、VPNの構成によっては、トンネルの下にあるISPが割り当てたパブリックIPも明らかにすることがあります（RFC 8828）。

9 **問題 9** — **正解: 正しい**

指導メモ

DNSやWebRTCの漏えいがなければ、ISPが見られるのはVPNサーバーへの暗号化された通信だけで、訪問したサイトは見えません。

10 **フィンガープリンティングの限界** ノーログ — **正解: 誤り**

指導メモ

フィンガープリンティングは、画面解像度、フォント、プラグインなどのデバイス設定の指標を狙うため、IPが隠れていても見えたままです。出典: EFF Tracking Evasion。

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

D 1. IP アドレス	A 2. VPN トンネル	B 3. Tor ネットワーク	E 4. ウェブプロキシ
G 5. DNS リーク	H 6. WebRTC API	C 7. 位置情報の隠蔽	F 8. ISPによる追跡

チェックポイント 3: 解答 – 重要用語

1 DNSリーク	2 WebRTC	3 ウェブプロキシ	4 Torネットワーク
5 IPアドレス	6 マスキング		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 D – ウエブプロキシ	2 G – マスキング	3 F – ジオブロツク	4 A – アイピーアドレス
5 C – トーアネツトワーク	6 H – ツイセキ	7 E – リーク	8 B – アンゴウカトンネル

指導者向けディスカッションメモ

重要用語:
生徒がIP アドレス、VPN トンネル、Tor ネットワーク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。

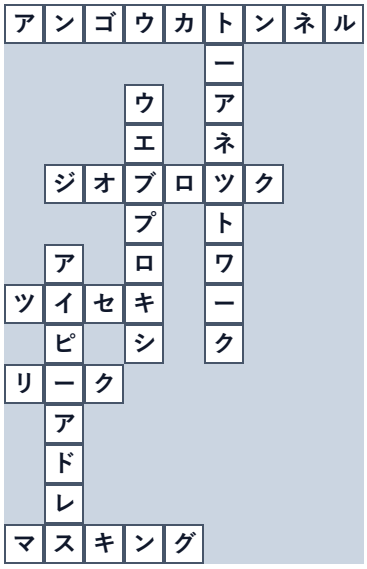
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

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

1 ヨコ: アンゴウカトンネル デバイスの全通信を暗号化し、VPNサーバー経由で送る仕組み (9 文字)

4 ヨコ: ジオブロツク 特定の地域からのアクセスを制限する仕組み (6 文字)

6 ヨコ: ツイセキ 暗号化されていない通信の宛先を通信事業者が記録すること (4 文字)

7 ヨコ: リーク VPNトンネルの外で名前解決が行われ、訪問したドメインがISPに知られてしまうこと (3 文字)

8 ヨコ: マスキング 別の国のサーバーを経由して接続し、地域制限を回避すること (5 文字)

タテのカギ

2 タテ: トーアネットワーク 3つのボランティアサーバーを経由させ、各段階で層ごとに暗号化する通信経路 (9 文字)

3 タテ: ウエブプロキシ システム全体を暗号化せず、アプリケーション層でブラウザの通信を転送するもの (7 文字)

5 タテ: アイピーアドレス インターネット上でデバイスのインターフェースを識別する固有の数値ラベル (8 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. レーアアドイスピ — アイピーアドレス
2. クトーネートワツア — トーアネツトワーク
3. クーリ — リーク
4. キグンマス — マスキング
5. ンカンルトウアネゴ — アンゴウカトンネル
6. キブロウプシエ — ウエブプロキシ
7. ツジロクブオ — ジオブロツク
8. ツキセイ — ツイセキ

秘密の暗号チャレンジ 解答

"ミエナイ ヨウニ アドレスヲ カクス"

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。