名前: 日付: 得点:

プロキシと VPN の比較 ワークシート

プロキシサーバーと仮想プライベートネットワーク、暗号化の違い、アプリ単位とシステム全体のルーティングの比較

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

- アプリ単位のプロキシと、システム全体の VPN 暗号化を比較してください。
- 基本的な HTTP プロキシと比べた SOCKS5 の機能を見分ける。
- ブラウザーベースのプロキシが、バックグラウンドのアプリを無防備なままにする仕組みを分析してください。
- ISPがプロキシトンネル上の暗号化されていない通信をどのように記録するかを理解する。
- 速度とセキュリティのニーズに応じて、適切なルーティングツールを選んでください。

プロキシ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。学んだ知識をプロキシとVPNの比較に応用しましょう。 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。

プロキシと VPN の比較（導入）

プロキシと VPN は、デジタルプライバシーにおいて異なる役割を果たします。プロキシサーバーはアプリケーション層のリダイレクトとして機能し、データを暗号化せずに、特定のプログラムの IP アドレスを隠します。VPN はネットワークレベルで動作し、暗号化によってシステム全体の通信を保護します。適切なツールは、セキュリティ要件によって決まります。

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. 標準的なHTTPプロキシは、OSI参照モデルのどの層で動作しますか？

- A. 物理層
- B. ネットワーク層
- C. アプリケーション層
- D. データリンク層

2. 標準的なHTTPプロキシと比べたときの、SOCKS5の主なプロトコル上の利点は何ですか?

- A. ペイロードの完全な暗号化を強制する
- B. あらゆるTCP/UDPトラフィックのルーティングに対応している
- C. DNS リークの影響を受けない
- D. カーネル空間で直接動作する

3. VPNが一般にプロキシサーバーより安全なのはなぜですか?

- A. より高速なリモートハードウェア上で動作する
- B. システム全体のネットワークトラフィックをすべて暗号化する
- C. ローカルのルーティングテーブルを必要としない
- D. ネットワークの遅延を完全になくす

4. デフォルトでは暗号化せずにトラフィックをリダイレクトするプロキシの種類はどれですか?

- A. 基本的なHTTPプロキシ
- B. 暗号化されたHTTPSプロキシ
- C. 安全なWireGuardクライアント
- D. 難読化された VPN サーバー

5. ブラウザーのプロキシを使うと、バックグラウンドのアプリのトラフィックはどうなりますか?

- A. 自動的に暗号化される
- B. プロキシサーバーによってブロックされる
- C. プロキシトンネル経由でルーティングされる
- D. プロキシを迂回して IP を露出させる

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. SOCKS5プロキシは、サーバーを通るすべてのパケットのペイロードを暗号化します。

○ 正しい ○ 誤り

7 質問 7

7. VPNはネットワーク層で動作し、システム全体の通信を保護します。

○ 正しい ○ 誤り

8 質問 8

8. プロキシは深いパケット暗号化を行うため、一般に VPN より高速です。

○ 正しい ○ 誤り

9 質問 9

9. プロキシを設定するには、特定のアプリの中でトラフィックのリダイレクトを設定する必要があります。

○ 正しい ○ 誤り

10 質問 10

10. プロキシを使っても、ローカルISPによる追跡からデータ通信を守ることはできません。

○ 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. アプリケーション層の _____ は、他のアプリを保護せずに特定のブラウザ通信を転送します。

2. 堅牢な _____ は、デバイスのすべてのデータパケットをカプセル化して暗号化します。

3. アプリケーション層とトランスポート層の間に位置するのは、 _____ プロトコルです。

4. HTTPプロキシは、OSI参照モデルの _____ 層で動作します。

5. 標準的なプロキシサーバーにはペイロードの _____ がなく、データが危険にさらされます。

6. VPNは、すべてのネットワークアダプターに対して _____ の保護を提供します。

用語バンク

SOCKS5　アプリケーション　システム全体　ブラウザ拡張　プロキシ　暗号化　暗号化トンネル　第7層

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

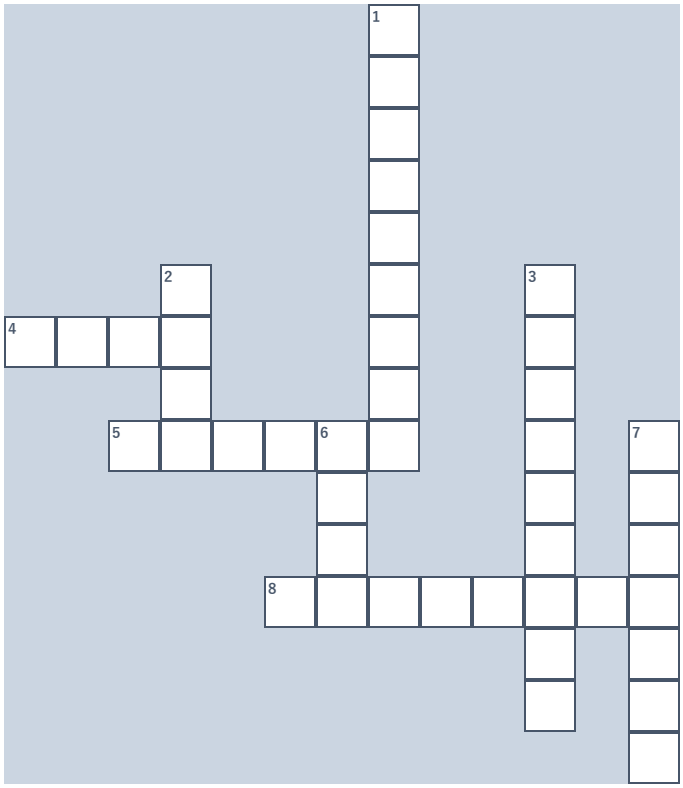
定義マッチング

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. HTTP プロキシ	A	すべてのアプリケーションの通信を暗号化する、オペレーティングシステムレベルのルーティング。
2. SOCKS5 プロキシ	B	標準的なWebプロキシプロトコルが動作するアプリケーション層。
3. VPN トンネル	C	通常のHTTPプロキシとは異なり、TCPだけでなくUDPも中継できるSOCKS5の機能。
4. システム全体の	D	ブラウザーのサンドボックス内のトラフィックだけを隠すクライアント拡張機能。
5. OSI 第 7 層	E	バックグラウンドのデバイストラフィックをすべて包む、暗号化とカプセル化。
6. UDP サポート	F	暗号化されていないプロキシのデータが、ISPから見える状態の通信。
7. ブラウザープロキシ	G	特定のウェブブラウザーのトラフィックをリダイレクトする、アプリケーション層プロキシ。
8. ISPからの可視性	H	アプリケーション層とトランスポート層の間に位置する、暗号化を行わないプロキシプロトコル。

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

4. 特定のウェブブラウザの通信を転送する、アプリケーション層の中継サーバー (4)

5. 標準的なウェブのプロキシプロトコルが動作するアプリケーション層 (6)

8. OSレベルで、すべてのアプリの通信を暗号化するルーティング (8)

タテのカギ

1. ブラウザのサンドボックス内の通信だけを隠すクライアント拡張機能 (9)

2. 暗号化されていないプロキシのデータがISPに見えてしまう通信の状態 (4)

3. バックグラウンドを含むデバイスの全通信を包み込んで暗号化する仕組み (9)

6. アプリケーション層とトランスポート層の間に位置し、暗号化を行わないプロキシのプロトコル (4)

7. プレーンなHTTPプロキシとは異なり、SOCKS5がTCPに加えて中継できるもの (7)

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: 特定のウェブブラウザの通信を転送する、アプリケーション層の中継サーバー (4 文字):

5 ヨコ: 標準的なウェブのプロキシプロトコルが動作するアプリケーション層 (6 文字):

8 ヨコ: OSレベルで、すべてのアプリの通信を暗号化するルーティング (8 文字):

タテのカギ

1 タテ: ブラウザのサンドボックス内の通信だけを隠すクライアント拡張機能 (9 文字):

2 タテ: 暗号化されていないプロキシのデータがISPに見えてしまう通信の状態 (4 文字):

3 タテ: バックグラウンドを含むデバイスの全通信を包み込んで暗号化する仕組み (9 文字):

6 タテ: アプリケーション層とトランスポート層の間に位置し、暗号化を行わないプロキシのプロトコル (4 文字):

7 タテ: プレーンなHTTPプロキシとは異なり、SOCKS5がTCPに加えて中継できるもの (7 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	ダ	ロ	ボ	ワ	ラ	キ	ゼ	ゴ
ザ	ス	ホ	ノ	オ	ア	オ	イ	キ	ル	プ	パ	ホ	ヒ	パ
ヘ	ボ	ス	ズ	フ	サ	ン	ナ	メ	ハ	ロ	コ	ヌ	ヤ	モ
ウ	ヘ	ク	ワ	レ	テ	モ	ナ	モ	ン	キ	ギ	ゲ	ズ	ジ
ヨ	ツ	ツ	カ	ゴ	ア	ワ	ソ	ラ	ニ	シ	グ	カ	シ	バ
チ	コ	ソ	ザ	ペ	ン	ダ	ウ	キ	ポ	バ	タ	フ	ス	ト
ク	ー	コ	モ	サ	ゴ	ガ	ベ	ユ	レ	カ	ゾ	エ	テ	ア
カ	ー	ユ	コ	ヘ	ウ	イ	サ	ー	ラ	サ	ソ	テ	ム	ヌ
ザ	コ	ギ	ン	メ	カ	ス	ヌ	デ	グ	ポ	ゴ	ソ	ゼ	ガ
ウ	ド	セ	イ	イ	ト	カ	ガ	イ	リ	ヤ	レ	ズ	ン	ボ
ラ	ワ	ヒ	グ	ゼ	ン	シ	ゲ	ー	ケ	ヤ	プ	オ	タ	タ
ブ	グ	ベ	ブ	ノ	ネ	セ	イ	ピ	ギ	ー	ピ	ピ	イ	マ
ツ	ヌ	メ	ガ	ヒ	ル	イ	ム	ー	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

プロキシ　ソツクス　アンゴウカトンネル　システムゼンタイ　ダイナナソウ
ユーデイーピー　ブラウザカクチヨウ　カシセイ

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. プロキシ
B. ソツクス
C. アンゴウカトンネル
D. システムゼンタイ
E. ダイナナソウ
F. ユーデイーピー
G. ブラウザカクチヨウ
H. カシセイ

定義とマッチ欄
1. 標準的なウェブのプロキシプロトコルが動作するアプリケーション層。
2. プレーンなHTTPプロキシとは異なり、SOCKS5がTCPに加えて中継できるもの。
3. 特定のウェブブラウザの通信を転送する、アプリケーション層の中継サーバー。
4. ブラウザのサンドボックス内の通信だけを隠すクライアント拡張機能。
5. バックグラウンドを含むデバイスの全通信を包み込んで暗号化する仕組み。
6. OSレベルで、すべてのアプリの通信を暗号化するルーティング。
7. 暗号化されていないプロキシのデータがISPに見えてしまう通信の状態。
8. アプリケーション層とトランスポート層の間に位置し、暗号化を行わないプロキシのプロトコル。

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. キプシロ
2. ルアネウントンカゴ
3. ダナナウソイ
4. カウヨザチクブラウ
5. スソクツ
6. タイムンシゼステ
7. ユピーーーイデ
8. カイセシ

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	プロキシとVPNの違い			
2	VPNがないと暗号化されないもの			
3	偽のWi-Fiネットワークを見抜く方法			
4	日常生活で仲介者がすること			
5	プロキシで十分な場面			
6	VPNを使えるデバイス			
7	知っているプロキシの種類			
8	VPNが隠せるもの			
9	VPNに関する誤解			
10	優れたVPNプロバイダーが約束すること			
11	VPNでは守れないもの			
12	このワークシートで覚えておきたい言葉			
13	旅行中にVPNを使う理由			
14	VPNがほしい場面			
15	VPNを使う場所			

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にいて、『Free_Wi-Fi_No_Password』というオープンなネットワークにつないでいるよ。学校のメールにログインしたいんだけど、友達は無料のブラウザープロキシで十分安全だって言うんだ。プロキシでログインやファイルは守られる? それともVPNが必要?」

Alex(旅行する学生)

👱 「海外にいるんだけど、母国でホストされている生物学のドキュメンタリーが『この動画は現在の場所ではご利用いただけません』と表示されるんだ。クラスメートはプロキシを使っていて、僕はVPNを持ってる。どうしてブロックされるの? どっちのツールのほうがうまくいく?」

チェックポイント 9: 暗号を解読しよう

プロキシ比較のトレーニングを完了するために、安全なトンネリング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

69	43	7	12	60		18	3	12	46	45		3	6	2	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: プロキシサーバーとは何ですか?

プロキシサーバーは、アプリケーションと接続先サーバーの間でリクエストを転送する仲介役です。ウェブサイトにはあなたのIPアドレスではなくプロキシのIPアドレスが見えますが、プロキシを使うよう設定したアプリの通信だけが転送され、基本的なプロキシはその通信を暗号化しません。

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: プロキシは VPN ですか?

いいえ。プロキシは特定のアプリのトラフィックを、通常は暗号化せずに中継します。VPN はネットワーク層で暗号化されたトンネルを作り、バックグラウンドのアプリを含むデバイスのすべてのトラフィックを運びます。

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: 無料プロキシを使えますか?

使うことはできますが、無料プロキシは運営者が不明なことが多いです。基本的なプロキシは通信を暗号化しないため、運営者は暗号化されていないページを見ることができ、書き換えることさえできます。利用する前に、誰が運営しているかを確認してください。

Q7: プロキシはログを保存しますか?

できます。プロキシは転送するすべてのリクエストを処理するため、運営者があなたの IP アドレス、訪問先のサイト、その時刻を記録する可能性があります。誰が運営しているか、プライバシーポリシーに何が書かれているかを確認してください。

Q8: プロキシで十分なのはどんなときですか?

リスクの低い作業、たとえば1つのブラウザーの見かけの場所を変えるだけなら、プロキシで足りることもあります。ネットバンキング、公共Wi-Fi、デバイス上のすべてのアプリの保護には、すべての通信を暗号化するVPNのほうが安全な選択です。

Q9: プロキシでスマートフォンのすべてのアプリを保護できますか?

いいえ。プロキシ設定に従うアプリだけがそれを使い、そのほかは直接接続します。VPN アプリは、代わりにスマートフォンのすべてのアプリを暗号化されたトンネル経由でルーティングします。

Q10: SOCKS5 プロキシとは何ですか?

RFC 1928 で定義された SOCKS5 は、アプリケーション層とトランスポート層の間に位置するプロキシプロトコルです。TCP 接続と UDP データグラムを中継でき、認証にも対応していますが、暗号化は組み込まれていません。 [1]

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: プロキシと VPN は、どのネットワーク層で動作しますか?

HTTPプロキシはアプリケーション層(レイヤー7)で動作し、ウェブリクエストを理解します。SOCKS5はアプリケーション層とトランスポート層の間に位置します。IPsecやWireGuardなどのVPNプロトコルはネットワーク層で動作するため、デバイスのすべてのIP通信を運べます。

Q2: HTTPS サイトは、プロキシ経由でも暗号化されたままですか?

はい。プロキシ経由でHTTPSのサイトを開くと、TLS暗号化がブラウザーとサイトの間でエンドツーエンドで機能するため、プロキシにはドメインが見えますがページの内容は見えません。通常のHTTPのページは読み取られます。

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: 透過型プロキシとは何で、誰が使いますか?

透過型プロキシは、ユーザーのデバイスで何も設定しなくても通信を傍受します。学校、企業、ISPがキャッシュやコンテンツフィルタリングのために使います。ユーザーは気づかないことが多く、プライバシーは得られません。

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: プロキシが VPN 接続より速く感じられることがあるのはなぜですか?

基本的なプロキシは暗号化を行わず、1つのアプリの通信しか扱わないため、処理負荷は小さくなります。VPNはデバイスのすべてのパケットを暗号化します。最新のプロトコルでは差が小さいことも多く、プロキシが提供する保護ははるかに限られています。

Q8: ウェブサイトは私がプロキシや VPN を使っていることを判別できますか?

多くの場合、はい。多くのサイトは IP アドレスを既知のプロキシや VPN サーバーのリストと照合しており、HTTP プロキシは Via や X-Forwarded-For などのヘッダーを追加することがあります。ストリーミングサービスは、どちらもブロックするのが一般的です。

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: プロキシで ISP による速度制限を止められますか?

ほとんどありません。基本的なプロキシはトラフィックを暗号化しないため、ISP はどのような種類の通信なのかを見ることができます。VPN はトラフィックの種類を隠しますが、どちらのツールも混雑やデータ上限の問題は解決しません。

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. SOCKS 標準

SOCKS プロトコルバージョン 5 は 1996 年 3 月に IETF によって RFC 1928 として公開され、今日でもブラウザーやアプリで使われる SOCKS5 プロキシの基準仕様となっています。[1]

2. シム層

RFC 1928 は SOCKS をアプリケーション層とトランスポート層の間のシム層として説明しているため、ICMP のようなネットワーク層のトラフィックを転送できません。 [1]

3. UDP リレー

SOCKS5 は UDP ASSOCIATE コマンドを追加し、プロキシが TCP 接続だけでなく UDP データグラムも中継できるようにしました。通常の HTTP プロキシにはこれができません。[1]

4. 既定の SOCKS ポート

SOCKS5 クライアントは、RFC 1928 の定義により、デフォルトで TCP ポート 1080 のプロキシサーバーに接続します。多くのプロキシサービスでは、ユーザーが別のポートを選べます。 [1]

5. HTTP の中継役

HTTP標準(RFC 9110)は、プロキシを、クライアントが選択するメッセージ転送エージェントと定義しており、リクエストをオリジンサーバーに向けて中継します。

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)はパケットの内容や通信パターンを調べます。暗号化されていないプロキシのトラフィックはすべて見えてしまいますが、VPNのトラフィックから分かることははるかに少なくなります。

7. ネットワーク層のVPN

NIST SP 800-77 に記載されている IPsec は、ネットワーク層で通信を保護するため、アプリごとの設定なしに、すべてのアプリケーションの IP パケットを保護できます。 [2]

8. ブラウザー専用の範囲

1つのブラウザーに設定したプロキシはそのブラウザーにだけ影響し、メールクライアント、ゲーム、システムアップデートは引き続きデバイスの通常の接続を使います。

9. TORとプロキシの比較

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)経由で送り、通常はローカルのSOCKSプロキシ経由で接続するため、単一のプロキシにはない層が加わります。

10. 速度とのトレードオフ

プロキシは暗号化を省略するため高速に見えることがありますが、WireGuard のような最新の VPN プロトコルはオーバーヘッドがほとんどなく、デバイスのすべての通信を保護します。

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] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

解答: プロキシサーバーと仮想プライベートネットワークの比較、暗号化の違い、アプリ単位とシステム全体のルーティング

1 プロキシの OSI 層

プロトコル

正解: C

指導メモ

標準的な HTTP/HTTPS プロキシはアプリケーション層 (レイヤー7) で動作し、特定のブラウザー通信をリダイレクトします。システム全体のネットワークルーティングはできません。出典: Tor Project Foundation。

2 問題 2

正解: B

指導メモ

SOCKS5はアプリケーション層とトランスポート層の間でTCPとUDPの通信を中継しますが、デフォルトでは暗号化を行いません。一方、HTTPプロキシはウェブのリクエストを処理します。

3 VPNのシステム暗号化

Wi-Fiセキュリティ

正解: B

指導メモ

VPNはOSのすべての通信をシステム全体でカプセル化して暗号化しますが、プロキシは設定された特定のアプリケーションの通信を転送するだけです。出典: Deloitte Advisory。

4 プロキシに暗号化がないこと

ルーティング制御

正解: A

指導メモ

HTTP プロキシは、パケットのペイロードを暗号化せずに、アプリケーション層でブラウザーの通信を転送します。つまり、ネットワーク事業者や ISP はコンテンツの通信を引き続き追跡できます。出典: IETF Proxy Vulnerabilities。

5 迂回の脆弱性

プライバシー

正解: D

指導メモ

ブラウザープロキシは、ウェブブラウザー自体にしかルールを適用しません。バックグラウンドアプリ、オペレーティングシステムの更新、メールクライアントはプロキシを迂回し、本来のIPアドレスが露出します。出典: W3C Consortium。

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

SOCKS5はアプリケーション層とトランスポート層の間で通信を中継しますが、デフォルトでは暗号化を行わないため、パケットの内容は転送中も読み取れる状態のままです。

7 ネットワーク層のトンネル 速度

正解: 正しい

指導メモ

ネットワーク層で動作することで、VPNはデバイスからの送信トラフィックをルーティングして暗号化し、システム全体のトラフィックの保護に役立ちます。出典: Deloitte Advisory。

8 プロキシの暗号化の限界 スニッフィングのリスク

正解: 誤り

指導メモ

プロキシの方が高速な場合もありますが、それは暗号化を行わないからです。暗号化がないため、データは検査されやすい状態になります。 出典: IETF Proxy Vulnerabilities.

9 アプリレベルのリダイレクト ファイアウォール

正解: 正しい

指導メモ

システム全体で動作するVPNと異なり、プロキシサーバーは、ブラウザー設定やアプリ固有のプロキシ欄で手動設定する必要があります。出典: W3C Consortium。

10 ISP による追跡のリスク ノーログ

正解: 正しい

指導メモ

標準的なHTTP/SOCKS5プロキシはペイロードデータを暗号化しないため、ローカルISPはあなたのオンライン上の行動をすべて見ることができるためです。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

G 1. HTTP プロキシ	H 2. SOCKS5 プロキシ	E 3. VPN トンネル	A 4. システム全体の
B 5. OSI 第 7 層	C 6. UDP サポート	D 7. ブラウザープロキシ	F 8. ISPからの可視性

チェックポイント 3: 解答 – 重要用語

1 プロキシ	2 暗号化トンネル	3 SOCKS5	4 アプリケーション
5 暗号化	6 システム全体		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 E – ダイナナソウ	2 F – ユーデイーピー	3 A – プロキシ	4 G – ブラウザカクチヨウ
5 C – アンゴウカトンネル	6 D – システムゼンタイ	7 H – カシセイ	8 B – ソツクス

指導者向けディスカッションメモ

重要用語:
生徒がHTTP プロキシ、SOCKS5 プロキシ、VPN トンネル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。

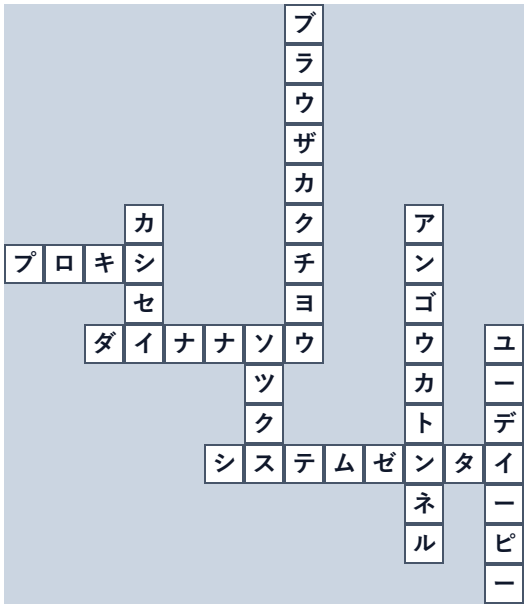
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

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

4 ヨコ: プロキシ 特定のウェブブラウザの通信を転送する、アプリケーション層の中継サーバー (4 文字)

5 ヨコ: ダイナナソウ 標準的なウェブのプロキシプロトコルが動作するアプリケーション層 (6 文字)

8 ヨコ: システムゼンタイ OSレベルで、すべてのアプリの通信を暗号化するルーティング (8 文字)

タテのカギ

1 タテ: ブラウザカクチヨウ ブラウザのサンドボックス内の通信だけを隠すクライアント拡張機能 (9 文字)

2 タテ: カシセイ 暗号化されていないプロキシのデータがISPに見えてしまう通信の状態 (4 文字)

3 タテ: アンゴウカトンネル バックグラウンドを含むデバイスの全通信を包み込んで暗号化する仕組み (9 文字)

6 タテ: ソツクス アプリケーション層とトランスポート層の間に位置し、暗号化を行わないプロキシのプロトコル (4 文字)

7 タテ: ユーディーピー プレーンなHTTPプロキシとは異なり、SOCKS5がTCPに加えて中継できるもの (7 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. キプシロ — **プロキシ**
2. ルアネウントンカゴ — **アンゴウカトンネル**
3. ダナナウソイ — **ダイナナソウ**
4. カウヨザチクブラウ — **ブラウザカクチヨウ**
5. スソクツ — **ソツクス**
6. タイムンシゼステ — **システムゼンタイ**
7. ユピーーーイデ — **ユーデイーピー**
8. カイセシ — **カシセイ**

秘密の暗号チャレンジ 解答

"プロキシデ ツウシンヲ ウカイスル"

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。
- プロキシと VPN: 基本的なブラウザープロキシは彼女の通信を暗号化しません。VPN はデバイス上のすべてを暗号化するため、傍受されたパケットは近くにいる盗聴者には読めません。

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。
- どちらが優れているか: どちらも母国のIPを得られますが、プロキシは設定したアプリのみが対象で、VPNはデバイスのすべてのトラフィックも暗号化します。