名前: 日付: 得点:

IPVanish レビュー

米国に本社を置く IPVanish VPN、大部分が自社所有のサーバーについての技術的な分析

IPVANISH レビューの学習概要

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、IPVanishの技術レビューを行います。自社所有の物理インフラ、P2Pトレント用のSOCKS5プロキシ、WireGuardの性能、米国のデータ規制を取り上げます。

ワークシートのチェックポイント

- [ ] **パート 1-4: VPN とネットワークセキュリティの設定を習得します。**
- [ ] **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 のおすすめ VPN ガイドを開く

URL: https://www.vpn.com/vpn/ipvanish/

あなたのIPVanish 学習ロードマップ

- IPVanishレビューの技術的なアーキテクチャと暗号化標準を分析してください。
- IP、DNS、WebRTC のトラフィックが漏れないよう、クライアントの設定を構成してください。
- 独自のトンネリングプロトコルと標準的な実装を比較してください。

IPVANISH レビューの説明

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SOCKS5プロキシと自社所有のサーバーインフラに応用しましょう。 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。

自社所有のインフラと SOCKS5 P2P プロキシ（導入）

IPVanish は、物理サーバーネットワークの大部分を所有・管理しており、これがパフォーマンスとセキュリティの向上につながっている点が特徴です。高速な WireGuard プロトコルと、P2P トレントのための SOCKS5 プロキシを提供していますが、米国のファイブ・アイズの管轄下で運営されています。

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. IPVanishのクライアントアプリで、高速化のためにデフォルトとなっているオープンソースプロトコルはどれですか?

- A) WireGuard
- B) L2TP/IPSec
- C) PPTP
- D) Catapult Hydra

2. IPVanishがP2Pトレントの設定を支援するために提供するサーバープロキシの種類は何ですか?

- A) SOCKS5プロキシ
- B) HTTPプロキシ
- C) Torリレー
- D) Shadowsocks

3. 2022年に行われたIPVanish最初の独立したノーログ監査を実施した企業はどこですか？

- A) Leviathan Security Group
- B) PwC
- C) Deloitte
- D) Cure53

4. IPVanishの法人は、主にどの国の管轄下で運営されていますか。

- A) 米国
- B) スイス
- C) パナマ
- D) 英領ヴァージン諸島

5. IPVanish のプレミアムプランでは、同時にいくつのデバイスを接続できますか?

- A) 無制限
- B) 5
- C) 10
- D) 7

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. IPVanish は、物理サーバーインフラの大部分を管理し、所有しています。

○ 正しい ○ 誤り

7 質問 7

7. SOCKS5 プロキシの通信は、標準的な VPN トンネルと同様に、転送中は完全に暗号化される。

○ 正しい ○ 誤り

8 質問 8

8. IPVanishのデスクトップクライアントには、システムレベルのKill Switch機能がありません。

○ 正しい ○ 誤り

9 質問 9

9. IPVanish は、ファイブ・アイズの情報機関の加盟国である米国から運営されています。

○ 正しい ○ 誤り

10 質問 10

10. IPVanish のスプリットトンネリングでは、アプリの通信を VPN トンネルの外でルーティングできます。

○ 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. 最新の _____ プロトコルは、ルーティング性能を最適化するため初期設定になっています。

2. P2Pの通信は、実際のクライアントの位置を隠すために、高速な _____ プロキシ経由にできます。

3. 地理的に近いノードに接続すると、実際の _____ が最大になります。

4. データ漏えいを防ぐには、内蔵の _____ の制御を設定する必要があります。

5. 独立したセキュリティ監査により、同社の _____ への取り組みが認証されています。

6. 一部の競合とは異なり、IPVanishはアカウントに有効な _____ を設けていません。

用語バンク

IPアドレス　SOCKS5　WireGuard　キルスイッチ　サーバー速度　セキュリティ　デバイス制限　監査済みログ

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: VPN とネットワークの概念マッチング

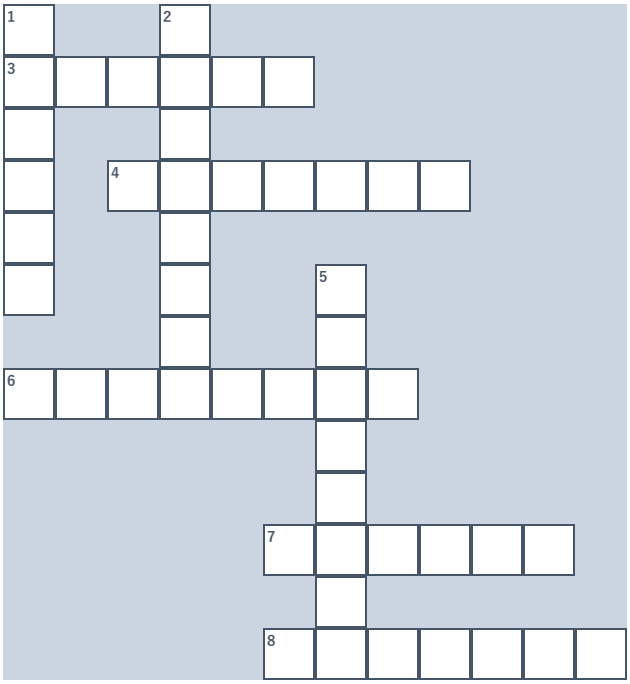
定義マッチング

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	VPNが失敗した場合にインターネットトラフィックをブロックする、フェイルセーフの仕組み。
2. SOCKS5 プロキシ	B	速度と最新の暗号技術で知られるオープンソースのプロトコル。
3. サーバー速度	C	アクティブなデバイスセッションの数を制限する制約。
4. キルスイッチ	D	アクティブな通信負荷がかかっているサーバーノードのスループット容量。
5. 監査済みログ	E	インターネット上のデバイスに割り当てられる固有のネットワーク識別子。
6. デバイス数の上限	F	暗号化トンネルシステム全体の保護態勢。
7. IP アドレス	G	ユーザーの活動が一切追跡されていないことを確認する、検証済みの記録。
8. セキュリティ	H	P2P クライアントの所在地を隠すために使われる、暗号化されていないプロキシのルーティングシステム。

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. VPNが切れたときにインターネット通信を遮断するフェイルセーフの仕組み (6)

4. 通信負荷がかかった状態でのサーバーノードのスループット容量 (7)

6. P2Pクライアントの位置を隠すために使われる、暗号化されないプロキシの中継方式 (8)

7. 速度と最新の暗号技術で知られるオープンソースのプロトコル (6)

8. ユーザーの行動が一切追跡されていないことを裏付ける、検証済みの記録 (7)

タテのカギ

1. 暗号化されたトンネルシステム全体の保護態勢 (6)

2. インターネット上でデバイスに割り当てられる固有のネットワーク識別子 (8)

5. 同時に有効にできるデバイスのセッション数に設ける上限 (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

3 ヨコ: VPNが切れたときにインターネット通信を遮断するフェイルセーフの仕組み (6 文字):

4 ヨコ: 通信負荷がかかった状態でのサーバーノードのスループット容量 (7 文字):

6 ヨコ: P2Pクライアントの位置を隠すために使われる、暗号化されないプロキシの中継方式 (8 文字):

7 ヨコ: 速度と最新の暗号技術で知られるオープンソースのプロトコル (6 文字):

8 ヨコ: ユーザーの行動が一切追跡されていないことを裏付ける、検証済みの記録 (7 文字):

タテのカギ

1 タテ: 暗号化されたトンネルシステム全体の保護態勢 (6 文字):

2 タテ: インターネット上でデバイスに割り当てられる固有のネットワーク識別子 (8 文字):

5 タテ: 同時に有効にできるデバイスのセッション数に設ける上限 (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。

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

用語リスト

ワイヤガード　ソツクスフアイブ　サーバーソクド　キルスイツチ　カンサズミログ
デバイスセイゲン　アイピーアドレス　セキユリテイ

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. ワイヤガード
B. ソツクスフアイブ
C. サーバーソクド
D. キルスイツチ
E. カンサズミログ
F. デバイスセイゲン
G. アイピーアドレス
H. セキユリテイ

定義とマッチ欄
1. P2Pクライアントの位置を隠すために使われる、暗号化されないプロキシの中継方式。
2. 暗号化されたトンネルシステム全体の保護態勢。
3. 同時に有効にできるデバイスのセッション数に設ける上限。
4. 通信負荷がかかった状態でのサーバーノードのスループット容量。
5. 速度と最新の暗号技術で知られるオープンソースのプロトコル。
6. インターネット上でデバイスに割り当てられる固有のネットワーク識別子。
7. VPNが切れたときにインターネット通信を遮断するフェイルセーフの仕組み。
8. ユーザーの行動が一切追跡されていないことを裏付ける、検証済みの記録。

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、仮想プライベートネットワーク(VPN)の重要な概念と用語を見つけましょう。答えは用意された入力欄に書いてください。

1. ヤワガードイ
2. サバドクソーー
3. ズカミグサロン
4. ーレスドアアイピ
5. フアツブスソイク
6. ツイキスチル
7. デンセイゲバスイ
8. ユイセテリキ

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	優れたVPNアプリを表す言葉			
2	IPVanishがネットワークから隠せるもの			
3	IPVanishをオンにする場所			
4	知っているVPNのプロトコル			
5	IPVanishのカスタマーサポートへの質問			
6	IPVanishのサーバーがほしい国			
7	IPVanish以外のVPNサービス			
8	キルスイッチが役立つ場面			
9	IPVanishを選ぶ理由			
10	VPN接続が遅いときのサイン			
11	毎日オンラインでしていること			
12	IPVanishをすすめたい人			
13	VPNを購入する前に確認すること			
14	このワークシートで学んだセキュリティ用語			
15	IPVanishに求める機能			

チェックポイント 8: VPN とネットワークのケーススタディ

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。

ケーススタディ 1: メディアセンターの設定



シナリオ: 顧客が、高速なスループットを維持しながら安全にストリーミングするために、IPVanishを使ってAndroidのFire TVメディアプレーヤーを保護したいと考えています。

ディスカッションの問い: リソースが限られたストリーミング用ハードウェアでは、なぜOpenVPNよりもWireGuardプロトコルのほうが好まれますか？

ケーススタディ 2: トレントネットワークのプロキシ



シナリオ: P2Pのアップローダーが、SOCKS5の設定を使って、完全なデータ暗号化のオーバーヘッドなしに、自分の所在地を隠したいと考えています。

ディスカッションの問い: SOCKS5プロキシを使う場合と、IPVanishの完全なVPNトンネルを使う場合の、セキュリティと速度のトレードオフを比較できますか？

チェックポイント 9: 暗号を解読しよう

ネットワークエンジニアは、ルーティングチャネルとクライアントトンネルを守ります。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、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

43	49	45		25	10	11	21	2		50	46	53	37	3	21		14	18	9	2

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 (VPN) とトンネリングに関する、最もよくある質問と回答を確認しましょう。

Q1: IPVanish のデフォルトのプロトコルは何ですか?

デフォルトで高速な WireGuard 経由にルーティングします。

Q2: IPVanish は自社でサーバーハードウェアを所有していますか?

はい、物理サーバーネットワークの大部分を自社で所有し、管理しています。

Q3: IPVanish の拠点はどこですか?

米国に拠点があり、米国の法律の対象となります。

Q4: 同時に何台のデバイスを接続できますか?

IPVanish は、1 つのアカウントにつき、同時接続のデバイス数に制限がありません。

Q5: 接続ログは保存されますか?

いいえ、独立した監査によって検証された、厳格なゼロログポリシーを徹底しています。 [6]

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 (VPN) とトンネリングに関する、最もよくある質問と回答を確認しましょう。

Q6: IPVanish はプロキシサービスを提供していますか?

はい、トレント用に無料のSOCKS5プロキシを提供しています。

Q7: キルスイッチは含まれていますか?

はい、キルスイッチは、Windows、macOS、Android、iOSで利用できます。

Q8: IPVanish で地域制限を回避できますか?

はい、世界中にあるサーバーネットワークにより、アクセス制限のある図書館を利用できます。

Q9: スプリットトンネリングに対応していますか?

はい、WindowsやAndroidなどでスプリットトンネリングが利用できます。

Q10: どのような暗号方式を使用していますか?

AES-256 と ChaCha20 の暗号化を使って接続を保護します。

チェックポイント 10: VPN FAQ – 応用 (パート C)

VPNトンネリングプロトコル、モバイルクライアントとの連携、企業での展開について、高度な技術的側面を探ります。

Q1: SOCKS5 プロキシはどのように設定しますか?

トレントクライアントで設定され、暗号化のオーバーヘッドなしにユーザーの IP を隠します。

Q2: サーバーハードウェアを所有すると、セキュリティはどのように向上しますか?

第三者のサーバーを借りるリスクを減らし、プロバイダーがサーバーの設定を直接管理できるようにします。

Q3: 米国の法域はプライバシーにどのような影響がありますか?

米国の法律はデータ保持を義務付けていませんが、国家安全保障書簡(NSL)や令状は認められています。

Q4: キルスイッチは IP リークをどう防ぎますか?

VPN 接続が予期せず切断された場合、すべてのインターネットアダプターを遮断します。

Q5: WireGuard にはどの暗号化が使われますか?

WireGuardは、ChaCha20の共通鍵暗号とPoly1305認証を利用します。[7]

チェックポイント 10: VPN FAQ – 応用 (パート D)

VPNトンネリングプロトコル、モバイルクライアントとの連携、企業での展開について、高度な技術的側面を探ります。

Q6: ゼロログポリシーはどのように検証されますか?

Leviathan Security Group が 2022 年に、Schellman が 2025 年に監査を行い、いずれもユーザーログは見つかりませんでした。 [3]

Q7: IPv6 の DNS クエリをどう処理しますか?

すべての DNS クエリと IPv6 クエリを、自社のプライベートネームサーバー経由で自動的にルーティングします。

Q8: IPVanish は難読化機能を提供していますか?

はい、Scramble機能がOpenVPNの通信を難読化して、ファイアウォールを回避します。

Q9: モバイルデバイスでスプリットトンネリングはどう機能しますか?

選択したアプリが VPN トンネルを回避して直接接続できるようにします。

Q10: ルーターの設定に対応していますか?

はい、OpenVPNとWireGuardの設定は、DD-WRTルーターに手動で読み込めます。 [1]

パート 11: 実世界の VPN の事実10選と洞察

VPN の暗号化の速度、プロトコルの監査、モバイル接続、企業のリモートワークに関する実際の事実を確認しましょう。

1. VPN の洞察

IPVanish は、サーバーインフラの大半を第三者から借りるのではなく、自社で所有しています。 [3]

2. VPN の洞察

IPVanish は 2012 年から運営されており、以前は J2 Global として知られた Ziff Davis が所有しています。 [2]

3. VPN の洞察

SOCKS5プロキシはクライアントの公開IPアドレスを隠しますが、データパケットは暗号化しません。

4. VPN の洞察

WireGuardはデフォルトのプロトコルで、アプリではOpenVPNとIKEv2/IPSecも利用できます。 [2]

5. VPN の洞察

標準の OpenVPN Scramble は、パケットヘッダーに XOR 難読化の層を加えて、ファイアウォールを回避します。

6. VPN の洞察

同時接続数が無制限というポリシーにより、世帯内のすべてのデバイスを同時に保護できます。 [2]

7. VPNの豆知識

Leviathan Security Group（2022年）とSchellman（2025年）による監査で、ノーログの主張が検証されました。 [3]

8. VPNの豆知識

Androidアプリは、トンネルが切断された場合にインターネットへのアクセスを防ぐ常時接続VPN設定に対応しています。

9. VPNの豆知識

OpenVPN の接続は、速度を重視するなら UDP、ファイアウォール越しの安定したルーティングを重視するなら TCP を使用できます。

10. VPN の洞察

24 時間 365 日のライブチャットサポートに加え、決まった平日の営業時間に電話サポートを提供しています。 [5]

技術参考資料と出典

この学習ガイドとインタラクティブなパズルは、世界の技術標準、仕様、規制の枠組みをもとに作成されています。

学術・業界の参考資料

[1] VPN.com. (2026). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

解答: チェックポイント 1 – 多肢選択

1 **WireGuardのデフォルト** WIREGUARD 正解: A

指導メモ

WireGuardは、ルーティング速度を最適化するようデフォルトで設定されています。出典: IPVanish Features。

2 **SOCKS5 プロキシ** SOCKS5 プロキシ 正解: A

指導メモ

SOCKS5 プロキシは、暗号化の負荷なしにクライアントの所在地を隠します。出典: IPVanish Support。

3 **問題 3** 正解: A

指導メモ

Leviathan Security Groupが2022年にIPVanish最初のノーログ監査を実施し、2025年にSchellmanが続きました。 [3]

4 **米国の管轄** アメリカ合衆国 正解: A

指導メモ

IPVanish は米国に拠点を置き、ファイブ・アイズ同盟のルールの下にあります。出典: IPVanish Review。

5 **無制限のデバイス** 無制限 正解: A

指導メモ

IPVanish では、同時接続のデバイス数に制限がありません。出典: IPVanish Support。

解答: チェックポイント 2 – 正誤問題

6 **サーバーハードウェア** OWNS NETWORK 正解: 正しい

指導メモ

IPVanish は、物理サーバーネットワークの大部分を所有し、管理しています。出典: IPVanish Support。

7 **問題 7** 正解: 誤り

指導メモ

誤り: SOCKS5プロキシはIPアドレスを隠しますが、データは暗号化しません。

8 **問題 8** 正解: 誤り

指導メモ

誤り: IPVanishには、デスクトップアプリとモバイルアプリの両方にキルスイッチが搭載されています。

9 **米国の管轄** ファイブ・アイズ 米国 正解: 正しい

指導メモ

IPVanish は米国に拠点を置き、ファイブ・アイズの監視ルールの対象となります。出典: IPVanish Review。

10 **スプリットトンネル** スプリットルート 正解: 正しい

指導メモ

スプリットトンネリングは、特定のアプリの通信を安全なトンネルの外でルーティングします。出典: IPVanish Support。

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. WireGuard	H 2. SOCKS5 プロキシ	D 3. サーバー速度	A 4. キルスイッチ
G 5. 監査済みログ	C 6. デバイス数の上限	E 7. IP アドレス	F 8. セキュリティ

チェックポイント 3: 解答 – 重要用語

1 WireGuard	2 SOCKS5	3 サーバー速度	4 キルスイッチ
5 監査済みログ	6 デバイス制限		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 B – ソツクスフアイブ	2 H – セキユリテイ	3 F – デバイスセイゲン	4 C – サーバーソクド
5 A – ワイヤガード	6 G – アイピーアドレス	7 D – キルスイツチ	8 E – 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、SOCKS5 プロキシ、サーバー速度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。

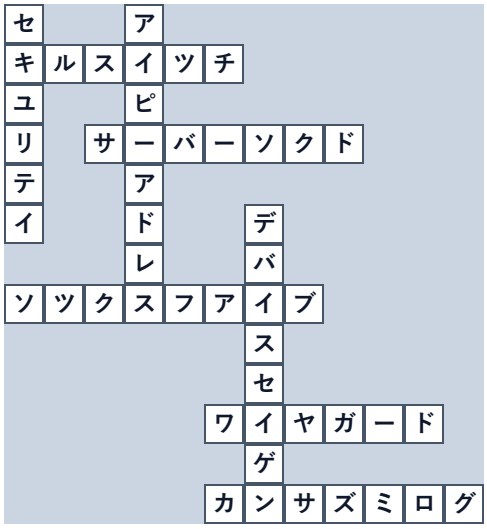
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: キルスイツチ VPNが切れたときにインターネット通信を遮断するフェイルセーフの仕組み (6 文字)

4 ヨコ: サーバーソクド 通信負荷がかかった状態でのサーバーノードのスループット容量 (7 文字)

6 ヨコ: ソツクスフアイブ P2Pクライアントの位置を隠すために使われる、暗号化されないプロキシの中継方式 (8 文字)

7 ヨコ: ワイヤガード 速度と最新の暗号技術で知られるオープンソースのプロトコル (6 文字)

8 ヨコ: カンサズミログ ユーザーの行動が一切追跡されていないことを裏付ける、検証済みの記録 (7 文字)

タテのカギ

1 タテ: セキユリテイ 暗号化されたトンネルシステム全体の保護態勢 (6 文字)

2 タテ: アイピーアドレス インターネット上でデバイスに割り当てられる固有のネットワーク識別子 (8 文字)

5 タテ: デバイスセイゲン 同時に有効にできるデバイスのセッション数に設ける上限 (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. ヤワガードイ — **ワイヤガード**
2. サバドクソーー — **サーバーソクド**
3. ズカミグサロン — **カンサズミログ**
4. ーレスドアアイピ — **アイピーアドレス**
5. ファツブスソイク — **ソツクスフアイブ**
6. ツイキスチル — **キルスイツチ**
7. デンセイゲバスイ — **デバイスセイゲン**
8. ユイセテリキ — **セキユリテイ**

秘密の暗号チャレンジ 解答

"ログヲ ノコサナイ ゲンジュウナ セッケイ"

ケーススタディの解答

A ケーススタディ 1: メディアセンターの設定

教師用解答

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:

- シナリオ分析: ある顧客が、高速なスループットを保ちながら安全にストリーミングするために、IPVanish を使って Android 搭載の Fire TV メディアプレーヤーを保護したいと考えています。
- 推奨される戦略と解決策: 採点のポイント: WireGuard はコードの規模が小さく、カーネル空間内で動作し、CPU サイクルの消費も少ないため、性能の低いハードウェアで速度を最大限に引き出せることを説明している。

B ケーススタディ 2: トレントネットワークのプロキシ

教師用解答

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:

- シナリオ分析: P2P のアップローダーが、SOCKS5 の構成を使って、完全なデータ暗号化の負荷なしに自分の所在地を隠したいと考えています。
- 推奨される戦略と解決策: 採点のポイント: SOCKS5 は通信を暗号化せずに IP アドレスを隠すため、速度は速くなるが、ISP によるパケット検査に対するプライバシー保護は全くないことを指摘している。