

名前: _____

日付: _____

得点: _____

ProtonVPN のセキュリティ

Secure Coreサーバー、NetShield DNSフィルタリング、スイスのプライバシー管轄、監査済みのオープンソースアプリ、Stealthプロトコルを含む、ProtonVPNのセキュリティアーキテクチャを分析してください。

ProtonVPN セキュリティの学習概要

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、Proton VPNのセキュリティアーキテクチャについて学びます。Secure Coreのバンカーサーバー、NetShieldのDNSブロック、スイスのプライバシー法、Stealth難読化を取り上げます。

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](https://www.vpn.com/vpn/protonvpn/security/)URL: <https://www.vpn.com/vpn/protonvpn/security/>

あなたのProtonVPNセキュリティ 学習ロードマップ

- ProtonVPNセキュリティの技術的なアーキテクチャと設定ルール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。
- カスタム料金、トライアル、性能の特徴を標準モデルと比較してください。

ProtonVPN セキュリティガイドの手順

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Secure Coreのダブルホップルーティングとスイスのプライバシーガバナンスに応用しましょう。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。

Secure Core の二重ホップ構造とスイスのプライバシー法域

Proton VPN は、スイス、アイスランド、スウェーデンにある Proton 所有の Secure Core サーバー、オープンソースで監査済みのアプリ、ディープパケットインスペクションを回避するよう設計された Stealth 難読化プロトコルによって、ユーザーの通信を保護します。

(はじめに)

Proton VPN は、スイス、アイスランド、スウェーデンにある Proton 所有の Secure Core サーバー、オープンソースで監査済みのアプリ、ディープパケットインスペクションを回避するよう設計された Stealth 難読化プロトコルによって、ユーザーの通信を保護します。

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. ProtonのSecure Coreサーバーは、どのような施設に置かれていますか？

- ☐ A) パブリッククラウドの仮想マシン
- ☐ B) 高セキュリティの施設
- ☐ C) 公共のデータセンター
- ☐ D) 共有ラック

2 2. 厳しい政府の検閲を回避するのに役立つプロトコルはどれですか？

- ☐ A) PPTP
- ☐ B) ステルスプロトコル
- ☐ C) OpenVPN UDP
- ☐ D) IKEv2

3 3. Proton VPNのNetShield機能の働きは何ですか？

- ☐ A) Speed Booster
- ☐ B) DNS広告・マルウェアブロック
- ☐ C) クラウドストレージ
- ☐ D) ポート転送

4 4. Proton AGは、どの国のプライバシー法のもとで運営されていますか。

- ☐ A) 米国
- ☐ B) 英国
- ☐ C) スイス
- ☐ D) パナマ

5 5. Proton VPN のクライアントアプリは、専門家によってどのように検証されていますか？

- ☐ A) 秘密のコード
- ☐ B) オープンソース監査
- ☐ C) プロプライエタリライセンス
- ☐ D) 政府による審査

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. Secure Coreは、出口の前に、プライバシーに配慮した国を経由して通信を送ります。

☐ 正しい ☐ 誤り

7 質問 7

7. スイスは、14 Eyes 情報監視同盟の加盟国です。

☐ 正しい ☐ 誤り

8 質問 8

8. NetShield は、広告や悪意のあるドメインを DNS レベルで直接ブロックします。

☐ 正しい ☐ 誤り

9 質問 9

9. Proton VPN のアプリは 100% オープンソースで、公開監査を受けています。

☐ 正しい ☐ 誤り

10 質問 10

10. Stealthプロトコルは、難読化をせずに標準的なWireGuardヘッダーを使います。

☐ 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. Proton所有のサーバーを経由するマルチホップのルーティングは、 _____ アーキテクチャと呼ばれます。
2. ディープパケットインスペクションやネットワークのファイアウォールを回避するには、 _____ モードを有効にします。
3. マルウェアのドメイン、トラッカー、広告スクリプトは、 _____ のDNSによってフィルタリングされます。
4. Protonは、 _____ のもとではユーザーの活動ログを保持する義務はないとしています。
5. VPNトンネルが予期せず切れると、インターネット通信は _____ のガードによってブロックされます。
6. アプリは _____ のコードなので、独立したセキュリティ研究者がクライアントの完全性を検証できます。

用語バンク

AES

NetShield

Secure Core

WireGuard

オープンソース

キルスイッチ

スイス法

ステルス

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

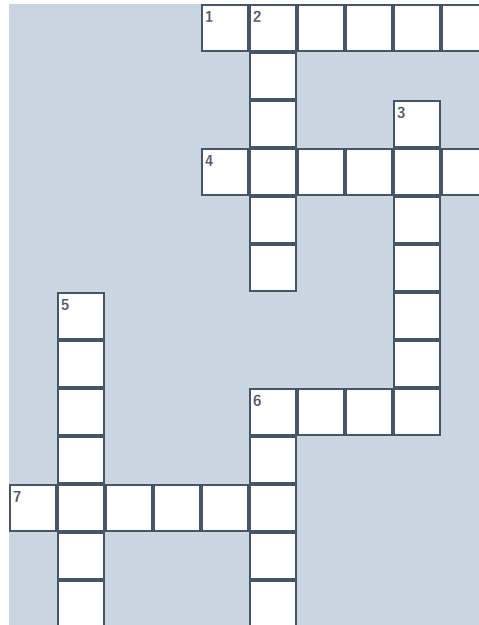
定義マッチング

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。

- | | | |
|-----------------------------------|---|--|
| <input type="text"/> 1. セキュアコア | A | 一般に公開され、独立した監査を受けているクライアントアプリのソフトウェア。 |
| <input type="text"/> 2. ステルス | B | VPN のデータパケットを暗号化する、共通鍵暗号の標準規格。 |
| <input type="text"/> 3. ネットシールド | C | 14 Eyes の法域の外にある、スイスの厳格なプライバシー関連法令。 |
| <input type="text"/> 4. スイス法 | D | 標準的なHTTPSウェブ通信に偽装された、難読化トンネリングプロトコル。 |
| <input type="text"/> 5. キルスイッチ | E | 強力な暗号化と高速な通信を提供する、最新の軽量プロトコル。 |
| <input type="text"/> 6. オープンソース | F | 広告、テレメトリートラッカー、マルウェアをブロックするDNSベースのフィルター。 |
| <input type="text"/> 7. WireGuard | G | Proton所有の最初の中継サーバーを経由して通信を送る、マルチホップの設計。 |
| <input type="text"/> 8. AES-GCM | H | 接続が切れている間、ネットワーク伝送を停止する安全対策。 |

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. Proton所有の最初の中継サーバー経由で通信を送る、マルチホップ型の設計 (6)
4. 堅牢な暗号と高速な通信を提供する、軽量で最新のプロトコル (6)
6. 通常のHTTPSのウェブ通信に偽装した、難読化されたトンネリングプロトコル (4)
7. カプセル化されたVPNのデータパケットをすべて守る、軍用水準の共通鍵暗号 (6)

タテのカギ

2. 接続が切れたときにネットワークの送信を止める安全策 (6)
3. 一般に公開され、独立した監査を受けているクライアントアプリのソフトウェア (7)
5. 広告、テレメトリのトラッカー、マルウェアをブロックするDNSベースのフィルター (7)
6. 14アイズの管轄の外にある、スイスの厳格なプライバシー関連の法令 (5)

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: Proton所有の最初の中継サーバー経由で通信を送る、マルチホップ型の設計 (6 文字):

4 ヨコ: 堅牢な暗号と高速な通信を提供する、軽量で最新のプロトコル (6 文字):

6 ヨコ: 通常のHTTPSのウェブ通信に偽装した、難読化されたトンネリングプロトコル (4 文字):

7 ヨコ: カプセル化されたVPNのデータパケットをすべて守る、軍用水準の共通鍵暗号 (6 文字):

タテのカギ

2 タテ: 接続が切れたときにネットワークの送信を止める安全策 (6 文字):

3 タテ: 一般に公開され、独立した監査を受けているクライアントアプリのソフトウェア (7 文字):

5 タテ: 広告、テレメトリのトラッカー、マルウェアをブロックするDNSベースのフィルター (7 文字):

6 タテ: 14アイズの管轄の外にある、スイスの厳格なプライバシー関連の法令 (5 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	ア	ロ	ボ	タ	レ	ミ	ク	グ	ヌ	チ	ユ	ガ	メ	ロ
ボ	コ	ウ	ワ	ラ	キ	ゼ	ゴ	ワ	ザ	ス	ホ	ノ	オ	ア
オ	ア	ホ	キ	ル	パ	ホ	ヒ	パ	イ	ヘ	ボ	ズ	フ	サ
ン	ユ	ス	ス	エ	ー	イ	ー	エ	メ	ヤ	ハ	コ	ヌ	ヤ
モ	キ	イ	ヘ	ワ	ネ	レ	テ	モ	モ	ン	ガ	ギ	ゲ	ズ
ジ	セ	ス	ツ	カ	ツ	ゴ	オ	ワ	ラ	ニ	グ	ー	カ	バ
チ	コ	ザ	ペ	ダ	ト	キ	ポ	ー	バ	タ	フ	ト	ド	ー
ツ	コ	モ	サ	ガ	シ	ベ	レ	カ	ブ	ゾ	エ	ア	ー	ユ
イ	コ	ヘ	イ	サ	ー	ラ	サ	ソ	テ	ン	ヌ	コ	ギ	ン
ス	メ	ス	ヌ	グ	ル	ポ	ゴ	ソ	ガ	ド	ソ	セ	イ	イ
ル	ガ	リ	ヤ	レ	ド	ズ	ボ	ワ	ヒ	ス	グ	ー	ゼ	ゲ
キ	ケ	ヤ	プ	オ	タ	グ	ベ	ブル	ノ	イ	ギ	ス	ー	
ピ	ピ	マ	ツ	ヌ	メ	ガ	ヒ	テ	ム	ミ	ジ	リ	ト	ロ
ン	テ	ー	ウ	ラ	デ	チ	ス	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

セキュアコア

ステルス

ネットシールド

スイスハウ

キルスイッチ

オープンソース

ワイヤガード

エーイーエス

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	定義とマッチ欄
A. セキュアコア	☐ 1. 通常のHTTPSのウェブ通信に偽装した、難読化されたトンネリングプロトコル。
B. ステルス	☐ 2. 堅牢な暗号と高速な通信を提供する、軽量で最新のプロトコル。
C. ネットシールド	☐ 3. 14アイズの管轄の外にある、スイスの厳格なプライバシー関連の法令。
D. スイスハウ	☐ 4. Proton所有の最初の中継サーバー経由で通信を送る、マルチホップ型の設計。
E. キルスイッチ	☐ 5. カプセル化されたVPNのデータパケットをすべて守る、軍用水準の共通鍵暗号。
F. オープンソース	☐ 6. 接続が切れたときにネットワークの送信を止める安全策。
G. ワイヤガード	☐ 7. 広告、テレメトリのトラッカー、マルウェアをブロックするDNSベースのフィルター。
H. エーイーエス	☐ 8. 一般に公開され、独立した監査を受けているクライアントアプリのソフトウェア。

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. ユセアコアキ

5. ススルテ

2. ネットドルーシツ

6. ホススウイ

3. キスイチツル

7. オーソスーンブ

4. ドガーワイ

8. イスエエー

ボーナス活動: すばやく考えよう

それぞれのカテゴリで答えを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	毎日オンラインでしていること			
2	プライバシー保護の法律が強いことで知られる国			
3	Proton VPNのセキュリティ機能			
4	VPNの漏えいの種類			
5	キルスイッチが役立つ場面			
6	監査で確認できること			
7	セキュリティを高めるためにオンにする設定			
8	暗号化が守るもの			
9	優れたVPNアプリを表す言葉			
10	Proton VPNを選ぶ理由			
11	VPNアプリにあるボタンやメニュー			
12	見ているストリーミングサービス			
13	公共のWi-Fiにある脅威			
14	強力なパスワードを作る方法			
15	Proton VPNのサーバーがほしい国			

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: 制限の厳しいファイアウォールの回避



シナリオ: ユーザーが、OpenVPNやWireGuardなどの標準的なVPN通信がDPIによってブロックされる国に渡航します。

ディスカッションの問い: ユーザーが国家レベルの検査を回避できるのは、Proton VPNのどのプロトコル設定ですか？

ケーススタディ 2: 高度な攻撃者からの保護



シナリオ: 金融監査人が、現地のISPの出口ノードが、高度な持続的脅威（APT）によって侵害されているのではないかと疑っています。

ディスカッションの問い: Secure Coreは、出口ノードが侵害された場合に、監査人の身元をどのように守りますか？

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 シ=46 ガ=47 ギ=48

グ=49 ゲ=50 ゴ=51 ザ=52 ジ=53 ズ=54 ゼ=55 ソ=56 ダ=57 チ=58 ツ=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

7	38	3	10	21		11	72	62	72	47		37	72	52	72	25
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
				60		72	16	45		31	35	41				
				<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>				

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: Proton VPN Secure Core とは何ですか？

Secure Coreは、出口の前に、プライバシーに配慮した国の複数のサーバーを経由して通信を送ります。

Q2: Stealth プロトコルとは何ですか？

Stealth は、VPN 接続を通常の TLS/HTTPS 通信に見せかける難読化プロトコルです。

Q3: NetShield はユーザーをどう保護しますか？

NetShield は、広告、トラッカー、マルウェアのドメインを自動的にブロックする DNS ベースのツールです。

Q4: Proton VPN はスイスで法的に保護されていますか？

はい、スイスには厳格なプライバシー法があり、米国やEU/14アイズの管轄の外にあります。[4]

Q5: Proton VPN のアプリはオープンソースですか？

はい。Proton VPNのアプリはオープンソースで、公表されたセキュリティ監査を受けています。

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 (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: どの暗号が利用されていますか？

Proton VPN は、HMAC-SHA384 と RSA-4096 のハンドシェイクを組み合わせた AES-256-GCM または ChaCha20-Poly1305 を使用します。

Q7: Proton VPN にはキルスイッチがありますか？

はい、Proton VPN には、暗号化されていないリークを防ぐために、標準のキルスイッチと常時有効のキルスイッチがあります。

Q8: Proton VPN は DNS クエリを漏らすことがありますか？

いいえ、すべての DNS クエリは、Proton が所有する暗号化されたプライベート DNS サーバーを経由します。

Q9: Proton VPN は接続ログを保存しますか？

いいえ、Proton VPN は、毎年 Securitum 監査で確認された厳格なノーログポリシーを維持しています。[3]

Q10: Proton VPN は WebRTC リークに対して脆弱ですか？

いいえ、Proton のクライアントには、WebRTC の漏えいをブロックするファイアウォールルールとルーティングポリシーが組み込まれています。

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: Secure Core のデータセンターは、物理的にどこにありますか？

スイス、アイスランドの元軍事基地、スウェーデンの地下施設にあります。[1]

Q2: Proton VPN では、完全前方秘匿性はどのように機能しますか？

セッションごとに固有の一時的な暗号鍵が生成され、後から復号されることを防ぎます。

Q3: Windows/Linux の Permanent Kill Switch とは何ですか？

恒久的なキルスイッチは、VPN アプリを完全に閉じたりクラッシュしたりしても、すべてのネットワーク通信をブロックします。

Q4: Proton VPN は IPv6 ルーティングとリーク防御に対応していますか？

Proton VPN は、IPv6 の通信をトンネル経由で完全にルーティングするか、リークを防ぐために安全に無効化します。

Q5: NetShield の DNS フィルタリングは HTTPS の検査をどう扱いますか？

NetShield は、侵襲的な TLS 復号を必要とせず、純粋に DNS 解決の層で動作します。

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: Proton VPN のサードパーティーによるコード監査を行ったのは誰ですか？

SEC Consult がアプリを監査し、Securitum がアプリとノーログポリシーを監査しています。

Q7: Stealth プロトコルは OpenVPN XOR や Shadowsocks とどう違いますか？

Stealth は、難読化された TLS を使って WireGuard をトンネリングし、従来の OpenVPN ベースの難読化より高い性能を発揮します。[5]

Q8: スイス当局は Proton VPN にトラフィックの記録を強制できますか？

Proton は、スイスの法律の下では、ユーザーの活動やデータのログを保持する義務はないと述べています。

Q9: Proton VPN のサーバーは押収からどう保護されていますか？

Proton VPNのサーバーはすべて、フルディスク暗号化で保護されたベアメタルマシンです。[2]

Q10: Proton VPN はカスタム DNS サーバーの設定に対応していますか？

はい、有料の契約者は、アプリの設定でカスタムのアップストリームDNSサーバーを直接指定できます。

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

1. Proton は、Secure Core サーバーをスイス、アイスランド、スウェーデンの高セキュリティ施設に自社で所有・設置しています。[1]

2. VPN の洞察

2. Proton VPN のクライアントアプリはオープンソースで、第三者によるコード監査を繰り返し受けています。

3. VPN の洞察

3. Stealth 難読化プロトコルは、標準的な TLS トラフィックを模倣することでディープパケットインスペクションを回避します。

4. VPN の洞察

4. スイスは、5 Eyes、9 Eyes、14 Eyes という国際的な情報共有同盟の外にあります。[4]

5. VPN の洞察

5. NetShield は DNS リゾルバーのレベルで動作し、ペイロードがダウンロードされる前に広告とマルウェアを防ぎます。

6. VPN の洞察

6. 完全前方秘匿性により、鍵が漏えいしても、以前に取得されたトラフィックセッションを復号できません。[7]

7. VPNの豆知識

7. Proton VPNは、サーバー構成を守るため、ベアメタルサーバーでフルディスク暗号化を利用しています。[2]

8. VPNの豆知識

8. 永続キルスイッチは、オペレーティングシステムの再起動中でも暗号化されていないデータの漏えいを防ぎます。

9. VPNの豆知識

9. Securitumは、Proton VPNのノーログポリシーを5年連続の年次監査で監査し、確認しています。[3]

10. VPN の洞察

10. Proton VPN は、CERN(欧州原子核研究機構)で出会った科学者たちによって開発されました。[4]

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] Proton VPN. (n.d.). What is Secure Core?

<https://protonvpn.com/support/secure-core-vpn>

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.

<https://protonvpn.com/blog/no-logs-audit>

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.

<https://protonvpn.com/blog/stealth-vpn-protocol>

[7] WireGuard. (n.d.). Protocol & Cryptography.

<https://www.wireguard.com/protocol/>

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.

<https://csrc.nist.gov/pubs/sp/800/38/d/final>

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.

<https://www.rfc-editor.org/rfc/rfc9076>

[2] Proton VPN. (n.d.). Proton VPN features.

<https://protonvpn.com/features>

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.

<https://protonvpn.com/features/swiss-based>

[6] GitHub. (n.d.). ProtonVPN · GitHub.

<https://github.com/ProtonVPN>

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.

<https://www.rfc-editor.org/rfc/rfc8439>

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.

<https://www.rfc-editor.org/rfc/rfc7359>

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).

<https://www.edoeb.admin.ch/en>

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

Secure Coreサーバーは、アイスランドの旧軍事基地やスウェーデンの地下データセンターなど、高セキュリティの施設に設置されています。

2 Stealth 難読化プロトコル 検閲対策

正解: B

指導メモ

Proton の Stealth プロトコルは、WireGuard 接続を標準の TLS/HTTPS トラフィックに見せかけ、ディープパケットインスペクション (DPI) のファイアウォールを回避します。出典: Proton Stealth Protocol Whitepaper. [2]

3 NetShield DNS 広告ブロッカー DNSフィルタリング

正解: B

指導メモ

NetShield は DNS レベルのフィルタリングを使って、ウェブページが読み込まれる前に、マルウェアのドメイン、スパイウェア、しつこい広告、テレメトリトラッカーをブロックします。出典: NetShield Security Specs。

4 スイスの法域 管轄

正解: C

指導メモ

Proton AG はスイスのジュネーブに本社を置き、米国や EU の 14-Eyes 監視同盟の外にある、スイスの強力なプライバシー法の恩恵を受けています。出典: Swiss Federal Data Protection Act. [2]

5 問題 5

正解: B

指導メモ

Proton VPNのアプリはすべてオープンソースで、SEC Consultと、その後はSecuritumが監査を行っています。

解答: チェックポイント 2 – 正誤問題

6 Secure Core 複数法域 ルーティングアーキテクチャ

正解: 正しい

指導メモ

Secure Coreは、宛先の国に出る前に、プライバシー保護の強い法域を経由して通信を送るため、侵害された出口サーバーへの対策に役立ちます。出典: Secure Core Architecture。

7 スイスの監視同盟 監視同盟

正解: 誤り

指導メモ

スイスは、5 Eyes、9 Eyes、14 Eyes の情報共有協定のいずれにも加盟しておらず、独立した法的主権を保っています。出典: International Surveillance Treaties。

8 問題 8

正解: 正しい

指導メモ

NetShieldはProtonのDNSサーバーを使い、既知の広告、トラッカー、マルウェアのドメインのリストと照合してドメインを確認します。

9 オープンソースクライアントの監査 セキュリティの透明性

正解: 正しい

指導メモ

Proton は、デスクトップとモバイルのアプリをオープンソースにし、第三者による監査報告書を公開しています。出典: SEC Consult Security Report.

10 問題 10

正解: 誤り

指導メモ

誤り: StealthはWireGuardをTCP上の難読化されたTLSの中でトンネリングするため、通信が通常のHTTPSのように見えます。

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. セキュアコア

D 2. ステルス

F 3. ネットシールド

C 4. スイス法

H 5. キルスイッチ

A 6. オープンソース

E 7. WireGuard

B 8. AES-GCM

チェックポイント 3: 解答 – 重要用語

1 Secure Core

2 ステルス

3 NetShield

4 スイス法

5 キルスイッチ

6 オープンソース

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 B – ステルス

2 G – ワイヤガード

3 D – スイスハウ

4 A – セキュアコア

5 H – エーイーエス

6 E – キルスイッチ

7 C – ネットシールド

8 F – オープンソース

指導者向けディスカッションメモ

重要用語:

生徒がセキュアコア、ステルス、ネットシールド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:

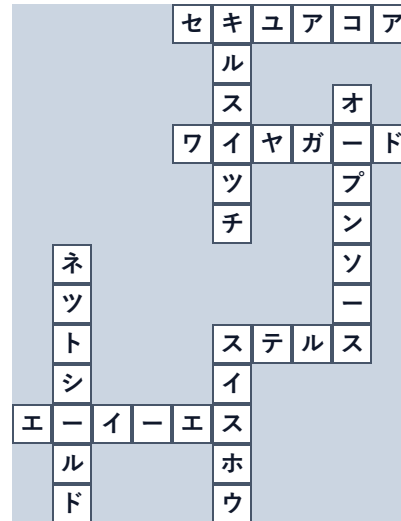
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

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: セキュアコア Proton所有の最初の中継サーバー経由で通信を送る、マルチホップ型の設計 (6文字)

4 ヨコ: ワイヤガード 堅牢な暗号と高速な通信を提供する、軽量で最新のプロトコル (6文字)

6 ヨコ: ステルス 通常のHTTPSのウェブ通信に偽装した、難読化されたトンネリングプロトコル (4文字)

7 ヨコ: エーイーエス カプセル化されたVPNのデータパケットをすべて守る、軍用水準の共通鍵暗号 (6文字)

タテのカギ

2 タテ: キルスイツチ 接続が切れたときにネットワークの送信を止める安全策 (6文字)

3 タテ: オープンソース 一般に公開され、独立した監査を受けているクライアントアプリのソフトウェア (7文字)

5 タテ: ネットシールド 広告、テレメトリのトラッカー、マルウェアをブロックするDNSベースのフィルター (7文字)

6 タテ: スイスハウ 14アイズの管轄の外にある、スイスの厳格なプライバシー関連の法令 (5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. ユセアコアキ | セキュアコア | 5. ススルテ | ステルス |
| 2. ネットドルーシツ | ネットシールド | 6. ホススウイ | スイスホウ |
| 3. キスイチツル | キルスイツチ | 7. オーソスーンプ | オープンソース |
| 4. ドガヤーワイ | ワイヤガード | 8. イスエエー | エーイーエス |

秘密の暗号チャレンジ 解答

"キョウコナ サーバーガ ユーザーノ データヲ マモル"

ケーススタディの解答

A ケーススタディ 1: 制限の厳しいファイアウォールの回避

教師用解答

採点基準と解答ガイドライン

- シナリオ分析: ユーザーが、OpenVPN や WireGuard などの標準的な VPN 通信が DPI によってブロックされる国に旅行します。
- 重点の問い: Proton VPN のどのプロトコル設定を使えば、国家レベルの検閲(検査)を回避できますか？
- 推奨される戦略と解決策: ユーザーは Stealth プロトコルを有効にするべきです。これは VPN パケットのヘッダーを通常の TLS/HTTPS のウェブ通信のように難読化し、DPI フィルターをすり抜けます。

B ケーススタディ 2: 高度な攻撃者からの保護

教師用解答

採点基準と解答ガイドライン

- シナリオ分析: 財務監査人が、自分の地元の ISP の出口ノードが、高度な持続的脅威 (APT) によって侵害されているのではないかと疑っています。
- 重点の問い: Secure Core は、出口ノードが侵害された場合に、どのように監査担当者の身元を守りますか？
- 推奨される戦略と解決策: Secure Core は通信をまずスイス、アイスランド、スウェーデンにある Proton 所有のサーバー経由で送るため、侵害された出口サーバーからユーザーの IP をたどることはできません。