名前: 日付: 得点:

Surfshark のセキュリティ

CleanWeb広告ブロック、MultiHopの動的ルーティング、Nexus SDNアーキテクチャ、RAMのみのサーバー群、Camouflageモードなど、Surfsharkのセキュリティ機能を調べます。

Surfshark セキュリティ 学習の概要

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、Surfsharkのセキュリティアーキテクチャについて学びます。RAM専用のサーバーハードウェア、Nexus SDNによる動的なIPローテーション、CleanWeb広告ブロッカー、MultiHopルーティングを取り上げます。

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/surfshark/security/

あなたのSurfsharkセキュリティ 学習ロードマップ

- Surfshark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。

Surfshark セキュリティガイドの指示

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RAMのみのインフラ、Nexus SDN、CleanWeb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。

RAM 専用サーバー群、Nexus SDN、CleanWeb アーキテクチャ（導入）

Surfshark は、すべて RAM 専用のサーバー群、IP Rotator を備えた Nexus のソフトウェア定義ネットワーク、CleanWeb 広告ブロック、Dynamic MultiHop の暗号化経路によって、ユーザーのプライバシーを守っています。

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. 1. Surfsharkに統合された広告・マルウェアブロッカーの名前は何ですか?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. 2. Surfsharkはすべてのサーバーでどのハードウェアアーキテクチャを使っていますか?
   - A) ハードディスクドライブ
   - B) 100% RAMのみ
   - C) 光学ストレージ
   - D) 磁気テープ

3. 3. トラフィックを2つの異なるVPNサーバー経由で送る機能は何ですか?
   - A) バイパサー
   - B) MultiHop（ダブルVPN）
   - C) Nexusネットワーク
   - D) 固定 IP

4. 4. VPNトラフィックを通常のウェブデータに見せかける難読化機能はどれですか?
   - A) キルスイッチ
   - B) カモフラージュモード
   - C) CleanWeb 2.0
   - D) スプリットトンネル

5. 5. Surfshark Bypasserツールの働きは何ですか?
   - A) Speed Booster
   - B) スプリットトンネリング
   - C) パスワードマネージャー
   - D) DNS リゾルバー

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. RAM 専用サーバーは、サーバーの再起動時にすべての運用データを直ちに消去します。

○ 正しい ○ 誤り

7 質問 7

7. カモフラージュモードは、VPN を使っていることを ISP に検出されにくくします。

○ 正しい ○ 誤り

8 質問 8

8. CleanWeb 2.0 はブラウザー拡張機能の中で動作し、Cookie 同意ポップアップをブロックします。

○ 正しい ○ 誤り

9 質問 9

9. Surfshark は、一時的な接続のタイムスタンプと帯域の使用ログを保持しています。

○ 正しい ○ 誤り

10 質問 10

10. Nexusネットワークは、接続を切らずに、ユーザーのIPアドレスを定期的にローテーションします。

○ 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. 煩わしいウェブ広告、追跡スクリプト、フィッシングリンクは、 _____ のフィルターによってブロックされます。

2. サーバーが _____ のメモリで動作するため、ユーザーの操作は法的調査の痕跡を残しません。

3. 暗号化された2つのサーバーホップを経由させるのは、 _____ のトンネルです。

4. インターネットプロバイダーからVPNの利用を隠すには、 _____ モードを有効にします。

5. 銀行アプリをVPNトンネルの対象外にするのは、 _____ の設定で管理します。

6. サーバー群をつなぐ次世代のSDNアーキテクチャは、 _____ システムです。

用語バンク

Bypasser　CleanWeb　Nexus　RAM専用　カモフラージュ　キルスイッチ　マルチホップ　ローテーション

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

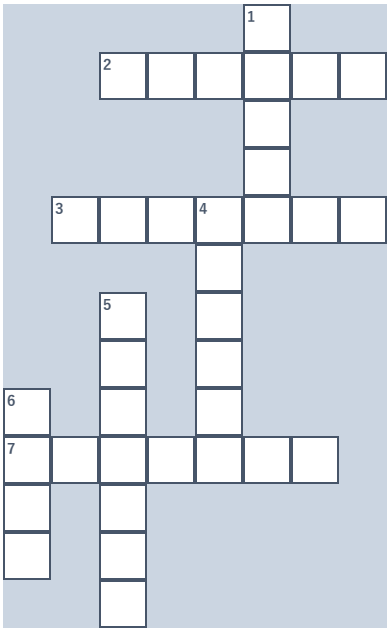
定義マッチング

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. クリーンウエブ	A	VPNが切れたときにネットワーク通信をブロックする自動の安全機能。
	2. RAM専用	B	選択したアプリが VPN を迂回できるようにする、スプリットトンネリング機能。
	3. マルチホップ	C	広告、マルウェア、Cookie同意バナーをブロックする高度なフィルター。
	4. カモフラージュ	D	電源を入れ直すたびにすべてのデータが消去される揮発性メモリのサーバーハードウェア。
	5. Bypasser	E	トンネルを中断せずに、外部IPアドレスを定期的に変更する機能。
	6. キルスイッチ	F	VPN の特徴を隠して通常の HTTPS トラフィックに似せる難読化技術。
	7. Nexus ネット	G	2つの別々のサーバーノードを経由して通信を暗号化する、ダブルVPNのルーティング機能。
	8. ローテーション	H	すべてのサーバーを1つの統合されたメッシュにつなぐ、独自のソフトウェア定義ネットワーク。

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. VPNが切れたときに、ネットワーク通信を自動で遮断する安全機能 (6)

3. VPNの特徴を隠して通常のHTTPS通信に見せかける難読化技術 (7)

7. 広告、マルウェア、クッキー同意バナーをブロックする高度なフィルター (7)

タテのカギ

1. 選んだアプリをVPNの対象から外せる、スプリットトンネリングの機能 (5)

4. 電源を入れ直すたびにデータがすべて消える、揮発性メモリのサーバーハードウェア (6)

5. トンネルを中断せずに、外向きのIPアドレスを定期的に変える機能 (7)

6. すべてのサーバーを一つのメッシュに結ぶ、独自のソフトウェア定義ネットワーク (4)

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: VPNが切れたときに、ネットワーク通信を自動で遮断する安全機能 (6 文字):

3 ヨコ: VPNの特徴を隠して通常のHTTPS通信に見せかける難読化技術 (7 文字):

7 ヨコ: 広告、マルウェア、クッキー同意バナーをブロックする高度なフィルター (7 文字):

タテのカギ

1 タテ: 選んだアプリをVPNの対象から外せる、スプリットトンネリングの機能 (5 文字):

4 タテ: 電源を入れ直すたびにデータがすべて消える、揮発性メモリのサーバーハードウェア (6 文字):

5 タテ: トンネルを中断せずに、外向きのIPアドレスを定期的に変える機能 (7 文字):

6 タテ: すべてのサーバーを一つのメッシュに結ぶ、独自のソフトウェア定義ネットワーク (4 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。

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

用語リスト

クリーンウエブ　ラムセンヨウ　マルチホツプ　カモフラージユ　バイパサー　キルスイツチ　ネクサス　ローテーシヨン

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. クリーンウエブ
B. ラムセンヨウ
C. マルチホツプ
D. カモフラージユ
E. バイパサー
F. キルスイツチ
G. ネクサス
H. ローテーシヨン

定義とマッチ欄
1. VPNの特徴を隠して通常のHTTPS通信に見せかける難読化技術。
2. VPNが切れたときに、ネットワーク通信を自動で遮断する安全機能。
3. 広告、マルウェア、クッキー同意バナーをブロックする高度なフィルター。
4. 選んだアプリをVPNの対象から外せる、スプリットトンネリングの機能。
5. 電源を入れ直すたびにデータがすべて消える、揮発性メモリのサーバーハードウェア。
6. トンネルを中断せずに、外向きのIPアドレスを定期的に変える機能。
7. 2つの別々のサーバーノードを経由して通信を暗号化する、二重VPNのルーティング機能。
8. すべてのサーバーを一つのメッシュに結ぶ、独自のソフトウェア定義ネットワーク。

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. ンエクウブーリ
2. プマチツホル
3. パバーサイ
4. スサネク
5. ンセウラヨム
6. ジフーカラユモ
7. ツキイチスル
8. ーーンロヨシテ

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	Surfsharkのセキュリティ機能			
2	VPN接続が遅いときのサイン			
3	知っているVPNのプロトコル			
4	暗号化が守るもの			
5	公共のWi-Fiにある脅威			
6	プライバシー保護の法律が強いことで知られる国			
7	強力なパスワードを作る方法			
8	Surfsharkをインストールするデバイス			
9	Surfsharkのカスタマーサポートへの質問			
10	セキュリティを高めるためにオンにする設定			
11	Surfsharkがネットワークから隠せるもの			
12	VPNの漏えいの種類			
13	VPNが決して保存してはいけないデータ			
14	優れたVPNアプリを表す言葉			
15	監査で確認できること			

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: 学校や職場のフィルターの回避



シナリオ: 学生が、大学のキャンパスWi-Fiが、標準的なOpenVPNとWireGuardのポートをすべてブロックしていることに気づきます。

ディスカッションの問い: 学生がネットワーク管理者に検出されることなく接続できるのは、Surfsharkのどの機能ですか？

ケーススタディ 2: 高リスクなジャーナリズムの調査



シナリオ: 調査報道のジャーナリストが、企業の機密記録を調べる間、監視に対する追加の保護を必要としています。

ディスカッションの問い: Dynamic MultiHopは、単一サーバーのルーティングと比べて、どのようにして優れたプライバシーを実現しますか？

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

24	8	11	13	47		37	72	52	72	25		69	39	2	62	12	72	45

18	38	8	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 (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: Surfshark CleanWeb とは何ですか?

CleanWeb は、広告、トラッカー、マルウェア、フィッシングサイトをブロックする統合型のセキュリティ機能です。

Q2: RAM のみのサーバーとは何ですか?

RAM 専用サーバーは揮発性メモリ上で動作するため、メモリ内のデータはサーバーが再起動するたびに消去されます。

Q3: Surfshark MultiHop とは何ですか?

MultiHop（Double VPN）は、インターネット接続を 2 か所の異なるサーバーの所在地に経由させて暗号化します。

Q4: カモフラージュモードはどう機能しますか?

カモフラージュモードは VPN トラフィックを難読化するため、ISP は VPN を使っていることを判別できません。

Q5: Bypasser 機能とは何ですか?

Bypasserは、特定のアプリやウェブサイトがVPNを迂回できるようにする、Surfsharkのスプリットトンネリングツールです。

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: Surfshark にはキルスイッチがありますか?

はい、VPNが予期せず切れると、キルスイッチがインターネットから切断します。

Q7: Surfshark はどの暗号化規格を使っていますか?

Surfshark は AES-256-GCM と ChaCha20 を使用し、新しい Dausos プロトコルでは AEGIS-256X2 も使用しています。

Q8: Surfshark のノーログポリシーは監査を受けていますか?

はい、Deloitteは、2023年と再び2025年に、Surfsharkのノーログポリシーを検証しました。

Q9: Surfshark Nexus とは何ですか?

Nexus は、すべてのサーバーを統合ネットワークにつなぎ、よりスムーズなルーティングを実現する高度な SDN アーキテクチャです。

Q10: IP ローテーター機能とは何ですか?

IP Rotator は、VPN セッションを切断せずに、数分ごとに IP アドレスを自動的に変更します。

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: Dynamic MultiHop は従来のダブル VPN とどう違いますか?

Dynamic MultiHopでは、世界中の入口サーバーと出口サーバーを、好きな組み合わせにカスタマイズできます。

Q2: CleanWeb 2.0 はブラウザー拡張機能でも動作しますか?

はい、CleanWeb 2.0は、Chrome/Firefox内の動画広告、クッキー同意のポップアップ、通知バナーをブロックします。

Q3: セキュリティスイートの Alternative ID とは何ですか?

代替IDは、固有の個人用仮名、メールアドレス、電話番号のマスクを生成します。

Q4: Surfshark は DNS リークをどう防ぎますか?

Surfshark は、すべてのドメインリクエストを、各ノードにある自社のプライベート DNS サーバー経由でルーティングします。

Q5: Surfshark はモバイルで ChaCha20 暗号化に対応していますか?

はい、AndroidとiOSのWireGuardは、モバイルでの優れた効率のために、ChaCha20-Poly1305を使います。

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: Surfshark の NoBorders モードとは何ですか?

NoBorders は、制限の厳しいネットワーク環境を自動的に検出し、専用のサーバーを提供します。

Q7: Surfshark のブラウザー拡張機能のセキュリティ監査を行ったのは誰ですか?

独立系のサイバーセキュリティ企業 Cure53 は、ブラウザー拡張機能とサーバーシステムの監査を完了しました。

Q8: Surfshark は IPv6 リークをどう防ぎますか?

Surfshark は、暗号化されていない漏えいを防ぐため、IPv6 通信を安全にルーティングするか、安全に制限します。

Q9: Surfshark の法的な法域はどこにありますか?

Surfshark はオランダの法律に基づいて運営されており、厳格な欧州の GDPR プライバシー基準に従っています。

Q10: Surfshark は二要素認証（2FA）に対応していますか?

はい。さらにSurfshark Oneでは、2FAロックが加わり、本人だけが機能の設定を変更できます。

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. Surfshark によると、4,500 台以上のサーバーネットワーク全体が、ディスクを使わない揮発性の RAM のみのハードウェアで動作しています。

2. VPN の洞察

2. ビッグフォーの Deloitte は、2023 年と 2025 年 11 月に再度、Surfshark のノーログポリシーを検証しました。

3. VPN の洞察

3. 独自の Nexus アーキテクチャは、世界中のすべてのサーバーを動的なソフトウェア定義ネットワークに接続します。

4. VPN の洞察

4. ローテーション IP は、VPN 接続を切らずに、約 5 分ごとに IP アドレスを変更します。

5. VPN の洞察

5. CleanWeb 2.0 は、煩わしい Cookie 同意ポップアップと動画広告をブラウザー上で直接ブロックします。

6. VPN の洞察

6. Dynamic MultiHop により、ユーザーは 100 か国にまたがるカスタマイズされた二重サーバー暗号化経路を作成できます。

7. VPNの豆知識

7. カモフラージュモードはVPNヘッダーの署名を取り除き、通信を通常のHTTPSと区別できなくします。

8. VPNの豆知識

8. 代替IDは使い捨ての仮名とメールマスクを生成し、データベース流出からユーザーを守ります。

9. VPNの豆知識

9. Surfsharkは、WireGuardプロトコルでAES-256-GCM対称暗号化とChaCha20を併せて適用しています。

10. VPN の洞察

10. NoBorders モードは制限されたネットワーク上で自動的に有効になり、回復力のあるトンネリングアクセスを提供します。

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

解答: チェックポイント 1 – 多肢選択

1 統合型コンテンツブロッカー 広告とマルウェアの防御 正解: B

指導メモ

CleanWeb は Surfshark に統合されたセキュリティフィルターで、広告、トラッカードメイン、フィッシングサイト、悪意のある URL スクリプトをネットワークレベルでブロックします。出典: CleanWeb Security Specs。

2 100% RAM のみのインフラ RAM アーキテクチャ 正解: B

指導メモ

Surfshark は RAM 専用サーバーを運用しているため、サーバーのメモリ上のデータは、サーバーの電源を切ったり再起動したりすると消去されます。出典: Cure53 Infrastructure Audit。

3 MultiHop 二重トンネリング マルチホップ VPN 正解: B

指導メモ

MultiHop（Double VPN）は、トラフィック相関攻撃を防ぐため、別々の国にある 2 つの異なるサーバーノードを経由してトラフィックを暗号化します。出典: Surfshark MultiHop Guide。

4 カモフラージュモードによる難読化 難読化 正解: B

指導メモ

カモフラージュモードは OpenVPN のパケットヘッダーを変更して VPN トラフィックを通常の HTTPS トラフィックに見せかけ、厳しいファイアウォールのブロックを回避します。出典: Surfshark Stealth Whitepaper。

5 Bypasserスプリットトンネリング スプリットトンネリング 正解: B

指導メモ

Bypasserは、ユーザーが特定のアプリやウェブサイトを選んで、通常のISP接続経由で直接ルーティングできる、Surfsharkのスプリットトンネリングツールです。出典: Surfshark Client Features。

解答: チェックポイント 2 – 正誤問題

6 **揮発性メモリのデータ消去** サーバーセキュリティ 正解: 正しい

指導メモ

RAM 専用サーバーは永続的なハードディスクにデータを一切保存せず、ハードウェアを再起動すると運用メモリがすべて直ちに消去されます。出典: RAM Server Architecture。

7 **カモフラージュモードによる ISP からの隠蔽** 通信の隠蔽 正解: 正しい

指導メモ

カモフラージュモードは OpenVPN プロトコルのシグネチャを取り除き、ユーザーが VPN トンネルに接続していることを ISP に検出されにくくします。出典: Deep Packet Inspection Guide。

8 **CleanWeb 2.0 ブラウザー拡張機能** ブラウザー拡張機能 正解: 正しい

指導メモ

CleanWeb 2.0 はブラウザー拡張機能の中で動作し、Cookie 同意ポップアップ、動画広告、悪意のあるリダイレクトスクリプトをリアルタイムでブロックします。出典: CleanWeb 2.0 Release Notes。

9 **接続ログの保持なし** ノーログポリシー 正解: 誤り

指導メモ

Surfshark は、独立した監査を受けた厳格なノーログポリシーを維持しており、IP アドレス、接続のタイムスタンプ、帯域のログを記録しません。出典: Deloitte No-Logs Audit。

10 **Nexus の IP 動的ローテーション** Nexus ネットワーク 正解: 正しい

指導メモ

Surfshark Nexusのソフトウェア定義ネットワークは、有効なVPN接続を切らずに、数分ごとにユーザーのIPアドレスを動的にローテーションします。出典: Surfshark Nexus Architecture。

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

C 1. クリーンウエブ	D 2. RAM専用	G 3. マルチホップ	F 4. カモフラージュ
B 5. Bypasser	A 6. キルスイツチ	H 7. Nexus ネット	E 8. ローテーション

チェックポイント 3: 解答 – 重要用語

1 CleanWeb	2 RAM専用	3 マルチホップ	4 カモフラージュ
5 Bypasser	6 Nexus		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 D – カモフラージュ	2 F – キルスイツチ	3 A – クリーンウエブ	4 E – バイパサー
5 B – ラムセンヨウ	6 H – ローテーシヨン	7 C – マルチホツプ	8 G – ネクサス

指導者向けディスカッションメモ

重要用語:
生徒がクリーンウエブ、RAM専用、マルチホップ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。

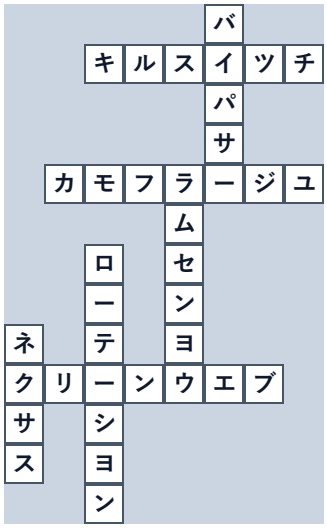
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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

2 ヨコ: キルスイツチ VPNが切れたときに、ネットワーク通信を自動で遮断する安全機能 (6 文字)

3 ヨコ: カモフラージュ VPNの特徴を隠して通常のHTTPS通信に見せかける難読化技術 (7 文字)

7 ヨコ: クリーンウエブ 広告、マルウェア、クッキー同意バナーをブロックする高度なフィルター (7 文字)

タテのカギ

1 タテ: バイパサー 選んだアプリをVPNの対象から外せる、スプリットトンネリングの機能 (5 文字)

4 タテ: ラムセンヨウ 電源を入れ直すたびにデータがすべて消える、揮発性メモリのサーバーハードウェア (6 文字)

5 タテ: ローテーション トンネルを中断せずに、外向きのIPアドレスを定期的に変える機能 (7 文字)

6 タテ: ネクサス すべてのサーバーを一つのメッシュに結ぶ、独自のソフトウェア定義ネットワーク (4 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. ンエクウブーリ — **クリーンウエブ**
2. プマチツホル — **マルチホツプ**
3. パバーサイ — **バイパサー**
4. スサネク — **ネクサス**
5. ンセウラヨム — **ラムセンヨウ**
6. ジフーカラユモ — **カモフラージユ**
7. ツキイチスル — **キルスイツチ**
8. ーーンロヨシテ — **ローテーシヨン**

秘密の暗号チャレンジ 解答

"ネクサスガ ユーザーノ プライバシーヲ ツヨクスル"

ケーススタディの解答

A ケーススタディ 1: 学校や職場のフィルターの回避

教師用解答

採点基準と解答ガイドライン

- シナリオ分析: 学生が、大学構内の Wi-Fi が、標準的な OpenVPN と WireGuard のポートをすべてブロックしていることに気づきます。
- 重点の問い: Surfshark のどの機能を使えば、学生はネットワーク管理者に検知されずに接続できますか?
- 推奨される対策と解決策: カモフラージュモード(OpenVPN)を有効にします。VPN のメタデータが隠されるため、ファイアウォールには通常の HTTPS 閲覧に見えます。

B ケーススタディ 2: 高リスクなジャーナリズムの調査

教師用解答

採点基準と解答ガイドライン

- シナリオ分析: ある調査報道ジャーナリストが、機密性の高い企業記録を調べる間、監視に対する追加の保護を必要としています。
- 重点の問い: Dynamic MultiHop は、単一サーバー経由のルーティングと比べて、どのように優れたプライバシーを実現しますか?
- 推奨される対策と解決策: ダイナミック MultiHop は、2つの国にある入口サーバーと出口サーバーを経由してトラフィックをルーティングするため、単一のサーバーでユーザーが特定されることはありません。