名前: 日付: 得点:

VPNとは ワークシート

ネットワークプロトコル、トンネリング、セキュリティ制御の実践演習。

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

- データトンネリングとカプセル化の概念を説明します。
- 標準的なプロトコルの設定と暗号化の方式を見分ける。
- 仮想プライベートネットワークにおける、サーバーとIPマスキングの役割を分析してください。
- ISPが閲覧をどのように追跡するか、そしてVPNがそれをどう防ぐかを理解する。
- 仮想ネットワークトポロジーが運用面でどこまで及ぶかの境界を区別します。

VPNとは 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。学んだ知識をケーススタディのセクションにある実際のシナリオに応用しましょう。 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。

VPNとは?（導入）

仮想プライベートネットワークは、単なるプライバシーの切り替えスイッチではありません。インターネット通信をリモートサーバー経由で送る暗号化トンネルです。これによりIPアドレスが隠れ、ISPがオンラインでの行動のログを作成するのを防ぎ、公共ネットワーク上のデータを守ります。デジタルセキュリティを保つには、用語を理解することが欠かせません。

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. 仮想プライベートネットワーク(VPN)の主な機能は何ですか?

- A. インターネットブラウザーの描画速度を上げるため
- B. データパケットを暗号化し、パブリックIPを隠すため
- C. ウェブサイトの Cookie データベースをローカルに保存するため
- D. 物理的なコンピューターのハードウェアを置き換えるため

2 2. VPNにおけるネットワークトンネリングとは何ですか?

- A. 重複したネットワークログファイルを削除する
- B. ローカルのデータベースストレージファイルをインストールすること
- C. ほかのローカルコンピューターとファイルを共有すること
- D. あるネットワークパケットを別の安全なパケットの内部にカプセル化すること

3 3. VPN通信の保護に広く使われている暗号化規格はどれですか？

- A. 旧式のDES暗号化
- B. 最新のAES-256規格
- C. 平文のbase64エンコード
- D. 標準的なrot13暗号

4 4. VPNは、ネットワークトラフィックのどの部分を暗号化しますか?

- A. ローカルデバイスのネットワーク印刷ジョブのみ
- B. 物理的なイーサネットケーブルの配線経路
- C. ネットワークパケットのデータペイロード部分全体
- D. ウェブブラウザーの検索履歴だけ

5 5. ネットワークで「暗号化」という用語は何を意味しますか?

- A. 平文データを読めない暗号文に変換する
- B. 古い通信記録を削除すること
- C. ローカルの帯域幅の速度制限を引き上げること
- D. データベースのアクセスキーを公開で共有すること

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. VPNは通信を暗号化し、公共Wi-Fiでのローカルな盗聴を防ぎます。

○ 正しい ○ 誤り

7 質問 7

7. VPNは、ルーター機器のハードウェア構成を物理的に変更します。

○ 正しい ○ 誤り

8 質問 8

8. トンネリングプロトコルは、データパケットを暗号化されたトランスポート層で包みます。

○ 正しい ○ 誤り

9 質問 9

9. 共通鍵暗号は、通信の暗号化と復号に同じ鍵を使います。

○ 正しい ○ 誤り

10 質問 10

10. VPNを使えば、インターネット接続は停電によるオフラインの状態に対して物理的に影響を受けなくなります。

○ 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. 通信を守るため、VPNはデータパケットを別のプロトコルで包みます。この処理は _____ と呼ばれます。

2. ストリーミング中にダウンロード速度が遅いなら、ネットワークの _____ が限られていることが原因かもしれません。

3. 特定の国でしか利用できない配信サービスは、世界のユーザーを制限するために _____ を使っています。

4. 暗号化や接続のパラメーターを定める接続ルールは、VPN _____ と呼ばれます。

5. お使いのコンピューターは、ネットワークの通信を監視して安全でない接続を遮断するローカルの _____ を使います。

6. VPNに接続すると、公開IPを隠すために通信が遠隔の _____ 経由になります。

用語バンク

ISP　サーバー　ジオブロック　トンネリング　ファイアウォール　プライバシー　プロトコル　帯域幅

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

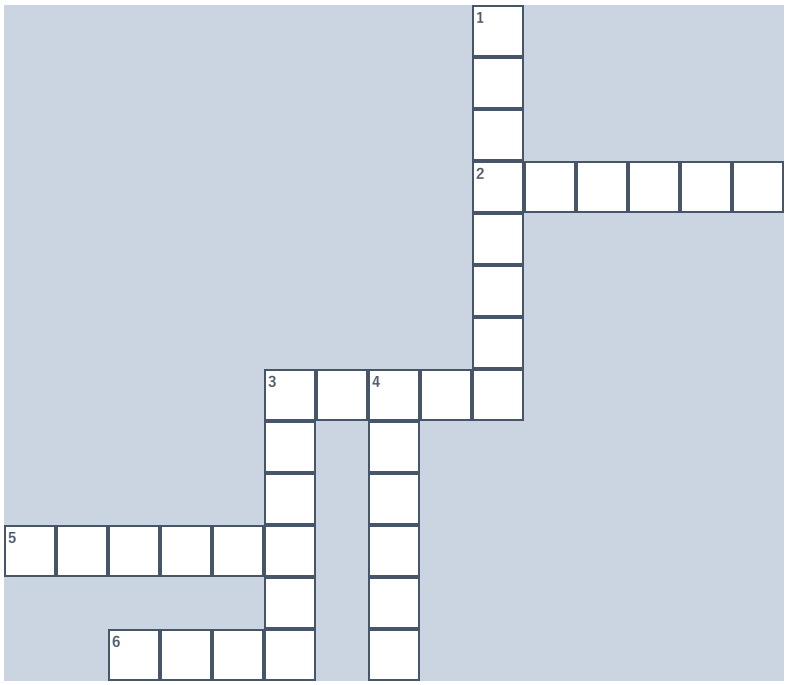
定義マッチング

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. トンネリング	A	通信を経由させてIPアドレスを隠すリモートコンピューター。
2. プロトコル	B	あなたの通信を運び、暗号化されていない活動を見ることができるインターネットサービスプロバイダー。
3. 帯域幅	C	物理的な所在地に基づいてウェブアクセスを妨げる制限。
4. サーバー	D	無許可の通信を監視してブロックするセキュリティシステム。
5. ジオブロック	E	ネットワーク上でデータをどのように伝送するかを決めるルールの集まり。
6. ファイアウォール	F	追跡や公的な監視を受けていない状態。
7. プライバシー	G	接続を通じて転送できるデータの最大速度。
8. ISP	H	安全に転送するために、データパケットを別のパケットの中に包むこと。

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. インターネットサービスプロバイダー。暗号化されていなければ通信を記録する (6)

3. データをネットワーク上でどう送るかを決める規則の集まり (5)

5. 接続を通じてデータを転送できる最大の速度 (6)

6. 通信を中継し、IPアドレスを隠す遠隔のコンピューター (4)

タテのカギ

1. 許可されていない通信を監視して遮断するセキュリティシステム (8)

3. 追跡や公的な監視を受けない状態 (6)

4. 安全に送るために、データパケットを別のパケットで包むこと (6)

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: インターネットサービスプロバイダー。暗号化されていなければ通信を記録する (6 文字):

3 ヨコ: データをネットワーク上でどう送るかを決める規則の集まり (5 文字):

5 ヨコ: 接続を通じてデータを転送できる最大の速度 (6 文字):

6 ヨコ: 通信を中継し、IPアドレスを隠す遠隔のコンピューター (4 文字):

タテのカギ

1 タテ: 許可されていない通信を監視して遮断するセキュリティシステム (8 文字):

3 タテ: 追跡や公的な監視を受けない状態 (6 文字):

4 タテ: 安全に送るために、データパケットを別のパケットで包むこと (6 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 バ ロ ボ タ レ ミ ク グ ヌ チ ユ ガ メ ロ
ボ ハ ル ワ ラ キ ゼ ゴ プ ザ ス ホ ノ オ ア
オ キ コ キ ル パ ホ ヒ パ ラ ヘ ボ ズ フ サ
ン イ ト ー ピ ス エ イ ア メ イ ハ コ ヌ ヤ
モ イ ロ ヘ ワ フ レ テ モ モ ン バ ギ ゲ ズ
ジ タ プ ツ カ ア ゴ ト ワ ラ ニ グ シ カ バ
ク コ ザ ペ ダ イ キ ポ ン バ タ フ ト ー ー
ツ コ モ サ ガ ア ベ レ カ ネ ゾ エ ア ー ユ
ロ コ ヘ イ サ ウ ラ サ ソ テ リ ヌ コ ギ ン
ブ メ ス ヌ グ オ ポ ゴ ソ ガ ド ン セ イ イ
オ ガ リ ヤ レ ー ズ ボ ワ ヒ ー グ グ ゼ ゲ
ジ ケ ヤ プ オ ル タ グ ベ バ ブ ノ イ ギ ー
ピ ピ マ ツ ヌ メ ガ ヒ ー ム ミ ジ リ ト ロ
ン テ ー ウ ラ デ チ サ 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

トンネリング　プロトコル　タイイキハバ　サーバー　ジオブロツク　フアイアウオール
プライバシー　アイエスピー

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. トンネリング
B. プロトコル
C. タイイキハバ
D. サーバー
E. ジオブロツク
F. フアイアウオール
G. プライバシー
H. アイエスピー

定義とマッチ欄
1. データをネットワーク上でどう送るかを決める規則の集まり。
2. 物理的な所在地に基づいてウェブへのアクセスを妨げる制限。
3. 許可されていない通信を監視して遮断するセキュリティシステム。
4. 追跡や公的な監視を受けない状態。
5. インターネットサービスプロバイダー。暗号化されていなければ通信を記録する。
6. 安全に送るために、データパケットを別のパケットで包むこと。
7. 通信を中継し、IPアドレスを隠す遠隔のコンピューター。
8. 接続を通じてデータを転送できる最大の速度。

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. ネトリングン
2. バタイハキイ
3. ジブロクツオ
4. ーバイシプラ
5. トルプコロ
6. バーサー
7. フルウオーアアイ
8. エーアピスイ

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	IPアドレスからわかること			
2	VPNに関する誤解			
3	インターネット上を行き交うもの			
4	優れたVPNプロバイダーが約束すること			
5	暗号化したい秘密			
6	VPNでは守れないもの			
7	偽のWi-Fiネットワークを見抜く方法			
8	プライバシーに関連する言葉			
9	VPNを使えるデバイス			
10	「接続」を押したときに起こること			
11	VPNを使う場所			
12	旅行中にVPNを使う理由			
13	現実にあるトンネルのようなもの			
14	このワークシートで覚えておきたい言葉			
15	子どもにVPNを説明するための言葉			

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

VPNは通信を暗号化して保護します。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、サイバーセキュリティの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

1	46	55	46	21		20	46	24	41	60		69	39	2	62	12	72	45

31	35	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: 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: 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: VPN を使うことは合法ですか?

VPNの使用は多くの国で合法ですが、VPNサービスを制限、規制、またはブロックしている地域もあります。使用する前に、現在のローカルの法律を確認してください。詳しくは、VPN.comの合法性に関するガイドをご覧ください。

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: 無料 VPN を使えますか?

無料 VPN は、広告、機能の制限、利用状況の分析、データ上限、その他の収益化モデルに頼っている場合があります。利用する前に、プロバイダーのプライバシーポリシー、所有者、監査、ビジネスモデルを確認してください。

Q7: 「ノーログ」ポリシーとは何ですか?

ノーログポリシーは、プロバイダーが保持しないとしている活動データや接続データを説明するものです。正確な範囲は異なるため、読者はポリシーと独立監査の結果を確認してください。

Q8: 最適な VPN を選ぶにはどうすればよいですか?

監査済みのノーログポリシー、強力なプロトコル（WireGuard、OpenVPN）、安全なサーバーの所在地、高速な通信、RAM のみのサーバー、キルスイッチ機能、そして（5/9/14 アイズのような）情報共有同盟の外にある管轄を探しましょう。

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: WireGuard、OpenVPN、IKEv2 の違いは何ですか?

WireGuardは、約4,000行のコードしかない最新の軽量プロトコルで、高速な通信と素早い接続時間を実現します。OpenVPNは、実績のある非常に安全なオープンソースプロトコルです。IKEv2は、ネットワークを切り替えたときに素早く再接続できるため、モバイルデバイスに最適です。 [4]

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: RAM 専用サーバーとは何で、なぜ重要ですか?

従来型のサーバーはデータをハードドライブに書き込むため、押収されたり侵害されたりする可能性があります。RAMのみ(ディスクレス)のサーバーは、完全に揮発性メモリ(RAM)上で動作します。サーバーを再起動または電源オフにすると、メモリ内のデータは消去されます。

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: 前方秘匿性(PFS)はどう機能しますか?

PFS は、セッションごとに一意の一時的な暗号鍵が生成されるようにします。将来、秘密鍵が漏えいしても、各セッションが独立した鍵を使っているため、過去や将来のセッションの復号には使えません。

Q8: 5/9/14 Eyes 同盟とは何で、なぜ気にする必要がありますか?

管轄はプロバイダーが直面しうる法的手続きに影響しますが、実際のプライバシーリスクは、プロバイダーが保持するデータ、技術的なアーキテクチャ、所有者、透明性レポート、監査履歴にも左右されます。

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: VPN は ISP によるインターネットの速度制限を回避できますか?

場合によります。ISP が特定の通信だけを選んで遅くしている場合は VPN が役立つことがありますが、混雑、データ容量の上限、アカウント単位の速度制限、ネットワーク品質の低さを克服することはできません。

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. 最初の VPN プロトコル

PPTP（Point-to-Point Tunneling Protocol）は、Microsoft などのベンダーグループによって開発され、リモートアクセス VPN をサポートするために1999年7月に RFC 2637 として公開されました。 [6]

2. 市場評価

リモートワークの需要と企業のセキュリティ需要の高まりを背景に、世界のVPN市場は急速に成長しています。

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]

4. 厳格な監査基準

トップクラスのVPNプロバイダーは、外部の監査人(Cure53やPwCなど)を雇い、独立したコードレビューを行って、ユーザーの活動を記録していないことを検証しています。

5. 5 Eyes 同盟の成り立ち

ファイブ・アイズ同盟は、米国と英国の間で結ばれた1946年のUKUSA信号情報協定に始まり、その後カナダ、オーストラリア、ニュージーランドが加わりました。

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、ヘッダーだけでなくパケットの内容や通信パターンも調べ、一部のファイアウォールはこれを使って一般的なVPNプロトコルを検出しブロックします。

7. 企業での利用

世界中の企業の従業員の多くが、社内データベースへのログインに安全なVPNを利用しており、重要なセキュリティ標準になっています。

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、どのリレーも両端を知ることはありません。

10. データ侵害のコスト

VPNを使ったゼロトラストのセキュアアクセスモデルを採用すると、組織は知的財産を守り、データ侵害による経済的影響を軽減しやすくなります。

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

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

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

解答: VPNとは？ ワークシート

1 主な機能

プロトコル

正解: B

指導メモ

VPNの主な役割は、パケットのペイロードデータを守り、ユーザーの公開IPアドレスを隠す暗号化トンネルを確立することです。出典: IETF Tunnel RFC。

2 ネットワークトンネリング

遅延

正解: D

指導メモ

トンネリングプロトコルは、元のデータパケットを外側のキャリアパケットでカプセル化し、公共ネットワークを安全に通過させます。出典: IETF Tunnel RFC。

3 問題 3

正解: B

指導メモ

VPN通信の保護に広く使われている暗号化規格はどれですか？ → 最新のAES-256規格

4 暗号化されるコンポーネント

ルーティング制御

正解: C

指導メモ

VPNは、IPデータパケットのペイロード部分全体を暗号化し、伝送内容の機密性を保ちます。出典: IETF Tunnel RFC。

5 問題 5

正解: A

指導メモ

暗号化は、アルゴリズムと鍵を使って、平文を読めない暗号文に変換します。

解答: チェックポイント 2 – 正誤問題

6 **盗聴のブロック** IP マスキング 正解: 正しい

指導メモ

暗号化されたトンネルにより、ローカルWi-Fiネットワークでデータを傍受する者に、パケットのペイロードを読み取られないようにします。出典: Deloitte Advisory。

7 **ハードウェアの変更** 速度 正解: 誤り

指導メモ

VPNはソフトウェアベースのネットワークトンネルであり、ゲートウェイルーターのハードウェアを物理的に変更することはありません。出典: Cure53 Audit。

8 **トンネリングされるパケット** スニッフィングのリスク 正解: 正しい

指導メモ

トンネリングは、元のネットワークパケットをトランスポートヘッダーで包んで送ることで機能します。出典: IETF Tunnel RFC。

9 **共通鍵** ファイアウォール 正解: 正しい

指導メモ

共通鍵暗号は、ネットワークストリームの暗号化と復号の両方に、共有された1つの鍵を使います。出典: WireGuard Project。

10 **電源の耐性** ノーログ 正解: 誤り

指導メモ

VPNが暗号化するのは稼働中の接続信号だけで、ローカルの停電によるサービス中断は防げません。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

H 1. トンネリング	E 2. プロトコル	G 3. 帯域幅	A 4. サーバー
C 5. ジオブロック	D 6. ファイアウォール	F 7. プライバシー	B 8. ISP

チェックポイント 3: 解答 – 重要用語

1 トンネリング	2 帯域幅	3 ジオブロック	4 プロトコル
5 ファイアウォール	6 サーバー		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 B – プロトコル	2 E – ジオブロツク	3 F – フアイアウオール	4 G – プライバシー
5 H – アイエスピー	6 A – トンネリング	7 D – サーバー	8 C – タイイキハバ

指導者向けディスカッションメモ

重要用語:
生徒がトンネリング、プロトコル、帯域幅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。

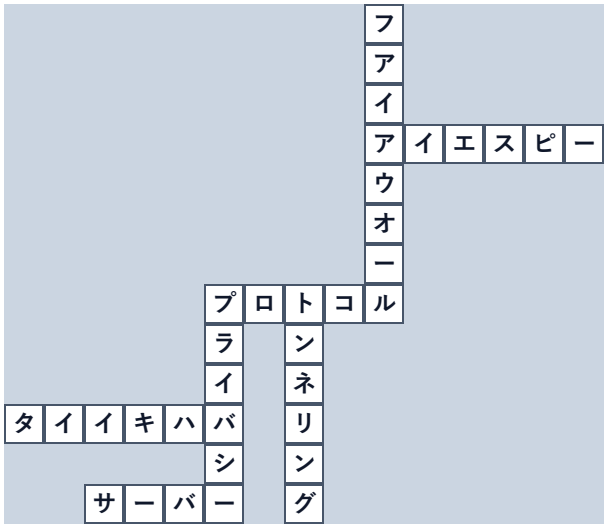
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: アイエスピー インターネットサービスプロバイダー。暗号化されていなければ通信を記録する (6 文字)

3 ヨコ: プロトコル データをネットワーク上でどう送るかを決める規則の集まり (5 文字)

5 ヨコ: タイイキハバ 接続を通じてデータを転送できる最大の速度 (6 文字)

6 ヨコ: サーバー 通信を中継し、IPアドレスを隠す遠隔のコンピューター (4 文字)

タテのカギ

1 タテ: フアイアウオール 許可されていない通信を監視して遮断するセキュリティシステム (8 文字)

3 タテ: プライバシー 追跡や公的な監視を受けない状態 (6 文字)

4 タテ: トンネリング 安全に送るために、データパケットを別のパケットで包むこと (6 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. ネトリングン — トンネリング
2. バタイハキイ — タイイキハバ
3. ジブロクツオ — ジオブロツク
4. ーバイシプラ — プライバシー
5. トルプコロ — プロトコル
6. バーサー — サーバー
7. フルウオーアアイ — フアイアウオール
8. エーアピスイ — アイエスピー

秘密の暗号チャレンジ 解答

"アンゼンナ トンネルデ プライバシーヲ マモル"

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。
- 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。