名前: 日付: 得点:

ダークウェブとディープウェブ: セキュリティと違い

検索エンジンのインデックス登録、ディープウェブのデータベース、Tor のオニオンルーティング、ネットワークの匿名性とリスク

ダークウェブとディープウェブの学習概要

保護済み
データ暗号化
256 ビット AES 標準

準拠
世界標準
GDPR と CCPA の枠組み

ゼロトラスト
アクセスポリシー
多要素認証

ようこそ！ このアクティビティ資料では、ディープウェブとダークウェブの違いについて学びます。インデックスされていないデータベース、Torブラウザーのオニオンルーティング、.onion の暗号ドメイン、匿名性に伴うセキュリティリスクを取り上げます。

ワークシートのチェックポイント

- [ ] パート 1-4: サイバーセキュリティと脅威の防止を習得します。
- [ ] 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 のサイバーセキュリティガイドを開く

URL: https://www.vpn.com/cybersecurity/dark-web-vs-deep-web/

あなたのディープウェブ・ダークウェブ戦略 学習ロードマップ

- ディープウェブ（インデックスされていないデータベース）とダークウェブ（オニオンサービス）を比較してください。
- オニオンルーティングがネットワーク通信をどのように暗号化し中継するかを理解する。
- 未確認のTorネットワークのサイトにアクセスするセキュリティ上のリスクを評価します。
- 脅威インテリジェンスのクロール用に、セキュアなゲートウェイとサンドボックスのポリシーを展開します。
- オニオンサービスドメインの暗号アドレス形式を分析してください。

ディープウェブとダークウェブ ガイド手順

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。学んだ知識をディープウェブとダークウェブのプライバシーに応用しましょう。 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。

ディープウェブのデータベースとダークウェブのオニオンルーティング(入門)

ディープウェブは、プライベートなメールや企業の銀行ポータルのように、パスワードやログインの背後にあるインデックスされていないページで構成されています。ダークウェブはディープウェブの一部で、意図的に隠されており、匿名でアクセスするには特殊なブラウザー(Torなど)とonionネットワークが必要です。

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. ディープウェブとサーフェスウェブの違いは何ですか?

- A. ディープウェブのページは、公開の検索エンジンにインデックスされていない
- B. ディープウェブのトラフィックは違法で、法執行機関に監視されている
- C. ディープウェブのサイトにアクセスするには、Torのような専用ブラウザーが必要
- D. ディープウェブのページは、サーフェスウェブのページより常に速く読み込まれる

2 2. ダークウェブにはどのようにアクセスしますか?

- A. オニオンルーティングネットワークを利用する専用ブラウザーを通じて
- B. 一般的なルーターでカスタムDNS設定を構成することで
- C. 招待制の非公開のサーフェスウェブ検索コンソールを通じて
- D. 標準的な広告ブロックのブラウザー拡張機能をインストールすることで

3 3. ディープウェブの最大部分を占める構造はどれですか?

- A. パスワードで保護されたユーザーデータベースと非公開のアカウント
- B. 違法な物品を取引する、違法なブラックマーケットのフォーラム
- C. 暗号化されていないピアツーピアのファイル共有プロトコル
- D. 公開された検索エンジンのキャッシュデータベース

4 4. オニオンルーティングはネットワークトラフィックに何をしますか?

- A. パケットを暗号化し、複数のリレー経由で送る
- B. ISPのノードを迂回することでダウンロード速度が上がる
- C. デバイスのハードウェアシリアル番号を IP レコードに対応付ける
- D. クリックのたびにウェブブラウザーの Cookie を削除する

5 5. Torネットワークだけで使われるドメインのサフィックスはどれですか?

- A. 暗号化された.onionトップレベル拡張子
- B. 標準的な従来型の.com商用拡張子
- C. Web3 の分散型 .eth ブロックチェーン拡張子
- D. 国コードの .ai テクノロジー拡張子

チェックポイント 2: 正しい・誤りチャレンジ

6 質問(正誤) 6

6. ディープウェブとダークウェブは、同じネットワーク領域を指しています。

○ 正しい ○ 誤り

7 質問(正誤) 7

7. 企業のイントラネットポータルは、ディープウェブの一部です。

○ 正しい ○ 誤り

8 質問(正誤) 8

8. オニオンルーティングは、すべての中継ノードでデータパケットを完全に復号します。

○ 正しい ○ 誤り

9 質問(正誤) 9

9. ダークウェブにアクセスすると、デバイスがマルウェアの高いリスクにさらされます。

○ 正しい ○ 誤り

10 質問(正誤) 10

10. 標準的なWeb検索エンジンは、オニオンサイトをクロールしてインデックスに登録します。

○ 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. 非公開の銀行ポータルは、インデックスされていない _____ に存在します。
2. 専用のTorノードは、隠れた _____ サービスを運営します。
3. Torのウェブサイトは、暗号技術に基づく _____ というトップレベルの拡張子を使います。
4. 暗号化された多層構造の通信経路の設定は、オニオン _____ と呼ばれます。
5. 表層の検索エンジンは、公開されていて _____ されているページを巡回します。
6. オニオンネットワークは、ユーザーの _____ を保つためにクライアントのIPを暗号化します。

用語バンク

インデックス化　エントリーノード　オニオン　サーフェスウェブ　ダークウェブ
ディープウェブ　ルーティング　匿名性

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: セキュリティの概念マッチング

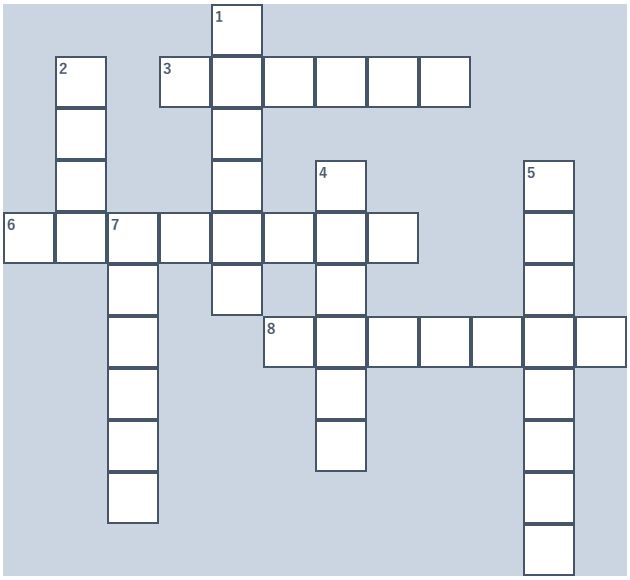
定義マッチング

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. ディープウェブの領域	A	特殊なブラウザーからしかアクセスできない、暗号化されたネットワークセグメント。
	2. ダークウェブポータル	B	データを層ごとに暗号化し、三つのノードを経由して中継すること。
	3. Onion 拡張子	C	インデックスされていないシステム記録を保管する、安全なバックエンドストレージ。
	4. Tor ルーティング	D	Tor ネットワークで使われる、暗号的なトップレベルドメインの接尾辞。
	5. インデックス済みのページ	E	Torネットワークにアクセスするために使う入口ノード。
	6. ユーザーの匿名性	F	収集されて Google で検索できる、サーフェスウェブのコンテンツ。
	7. プライベートデータベース	G	クライアントの公開 IP アドレスをサーバーから隠し続けること。
	8. 入口ゲートウェイ	H	非公開のログイン、メール、データベースのレコードなど、インデックスされていないWebコンテンツ。

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. 専用のブラウザからしかアクセスできない、暗号化されたネットワーク領域 (6)

6. Torネットワークにアクセスするための入口となるノード (8)

8. 非公開のログイン画面、メール、データベースの記録など、インデックスされていないウェブコンテンツ (7)

タテのカギ

1. インデックスされていないシステムの記録を保管する、安全なバックエンドのストレージ (6)

2. Torネットワークで使われる、暗号技術ベースのトップレベルドメインの接尾辞 (4)

4. データを多層に暗号化し、3つのノードを経由して中継すること (6)

5. Googleで検索可能な形でまとめられた、表層ウェブのコンテンツ (8)

7. クライアントの公開IPアドレスをサーバーから隠しておくこと (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

3 ヨコ: 専用のブラウザからしかアクセスできない、暗号化されたネットワーク領域 (6 文字):

6 ヨコ: Torネットワークにアクセスするための入口となるノード (8 文字):

8 ヨコ: 非公開のログイン画面、メール、データベースの記録など、インデックスされていないウェブコンテンツ (7 文字):

タテのカギ

1 タテ: インデックスされていないシステムの記録を保管する、安全なバックエンドのストレージ (6 文字):

2 タテ: Torネットワークで使われる、暗号技術ベースのトップレベルドメインの接尾辞 (4 文字):

4 タテ: データを多層に暗号化し、3つのノードを経由して中継すること (6 文字):

5 タテ: Googleで検索可能な形でまとめられた、表層ウェブのコンテンツ (8 文字):

7 タテ: クライアントの公開IPアドレスをサーバーから隠しておくこと (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。

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

デイープウエブ　ダークウエブ　オニオン　ルーテイング　サーフエスウエブ　トクメイセイ
データベース　エントリーノード

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. デイープウエブ
B. ダークウエブ
C. オニオン
D. ルーテイング
E. サーフエスウエブ
F. トクメイセイ
G. データベース
H. エントリーノード

定義とマッチ欄
1. クライアントの公開IPアドレスをサーバーから隠しておくこと。
2. インデックスされていないシステムの記録を保管する、安全なバックエンドのストレージ。
3. データを多層に暗号化し、3つのノードを経由して中継すること。
4. 非公開のログイン画面、メール、データベースの記録など、インデックスされていないウェブコンテンツ。
5. 専用のブラウザからしかアクセスできない、暗号化されたネットワーク領域。
6. Torネットワークで使われる、暗号技術ベースのトップレベルドメインの接尾辞。
7. Torネットワークにアクセスするための入口となるノード。
8. Googleで検索可能な形でまとめられた、表層ウェブのコンテンツ。

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、サイバーセキュリティ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. プエデウブーイ
2. オオンニ
3. エーサスウブエフ
4. スベターデー
5. ウクブダエー
6. ンイルテグー
7. セトイイメク
8. リンードエーノト

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	ダークウェブに近づかない理由			
2	検索エンジンが見つけられないもの			
3	ハッキングされるおそれのあるデバイス			
4	Torを使う合法的な理由			
5	ソフトウェアを更新する理由			
6	メールの危険なサイン			
7	ダークウェブで違法に売られているもの			
8	ITのサポートを頼める人			
9	今日から始められる安全な習慣			
10	データが漏えいした後にすること			
11	ディープウェブに属するもの			
12	ログインして使うサイト			
13	匿名性に関連する言葉			
14	決して共有してはいけない情報			
15	「水面下」にあるもの			

チェックポイント 8: サイバーセキュリティのケーススタディ

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: データ漏えいの特定



シナリオ: 企業のセキュリティ監査により、機密性の高い顧客データベースのレコードが、オニオンマーケットプレイスで取引されていることが判明します。このデータはGoogleにインデックスされていません。

ディスカッションの問い: どのウェブの領域が関係しているのか、またこの漏えいがどのように起きたのかを説明できますか？

ケーススタディ 2: 匿名性とマルウェアのリスク



シナリオ: アナリストが、Torのウェブサイトで脅威インテリジェンスのフィードを確認したいと考えています。Torブラウザーをダウンロードして、そのサイトにアクセスします。

ディスカッションの問い: 匿名性のメリットを評価し、マルウェアへの対策手順を示せますか？

チェックポイント 9: 暗号を解読しよう

サイバーセキュリティの専門家は、ネットワーク資産をオンラインの脅威アクターから守ります。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

5	22	5	46	60		20	8	34	2	14	2	45		16	35	18

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: サイバーセキュリティ FAQ – 基礎 (パート A)

オンラインの脅威への対策に関するよくある質問と回答を確認しましょう。

Q1: ディープウェブとは何ですか?

ディープウェブは、オンラインバンキング、メールのデータベース、有料会員向けジャーナルなど、検索エンジンがインデックスできないすべてのWebページで構成されています。

Q2: ダークウェブとは何ですか?

ダークウェブはディープウェブの小さな一部で、意図的に隠されており、onionネットワークを使う特殊なブラウザーからのみアクセスできます。

Q3: 検索エンジンはどのようにページをインデックスしますか?

検索エンジンは自動プログラム(スパイダー)を実行して公開リンクをたどり、ロボットディレクティブでクロールがブロックされていないページをインデックスします。

Q4: オンラインバンキングがディープウェブの一部と見なされるのはなぜですか?

銀行のポータルはログイン画面とパスワードで保護されているため、公開検索エンジンが取引明細ページをインデックスすることはできません。

Q5: Tor ブラウザーのオニオンルーティングとは何ですか?

オニオンルーティングは、トラフィックを層ごとに暗号化し、複数のリレーを経由させてユーザーの IP アドレスを隠す伝送方式です。

チェックポイント 10: サイバーセキュリティ FAQ – 基礎 (パート B)

オンラインの脅威への対策に関するよくある質問と回答を確認しましょう。

Q6: ダークウェブにアクセスすることは違法ですか?

いいえ。ダークウェブへのアクセスはほとんどの国で合法ですが、違法な市場やサイバー活動への関与は禁止されています。

Q7: ダークウェブのサイトの読み込みが遅いのはなぜですか?

通信は少なくとも3つの世界各地のリレー(入口、中間、出口)を経由してルーティングおよび復号されるため、伝送の遅延が増加します。

Q8: .onion ドメインの接尾辞は何を意味しますか?

Tor ネットワークで使われる特殊なトップレベルドメインの接尾辞で、標準の DNS サーバーではなく、暗号的に生成されたアドレスを指します。

Q9: ダークウェブのリンクにはどのようなリスクがありますか?

サイトにセキュリティ審査がなく、ユーザーはマルウェア感染、フィッシングスクリプト、取引詐欺の高いリスクにさらされます。

Q10: Tor ネットワークのルーティングプロトコルは誰が作りましたか?

この技術はもともと、政府の通信を保護するために、1990年代に米国海軍研究所によって開発されました。

チェックポイント 10: セキュリティ FAQ – 応用 (パート C)

セキュリティフレームワーク、マルウェア分析、データコンプライアンスについて、高度な技術的側面を探ります。

Q1: 中間ノードは、Tor の匿名性をどのように守りますか?

各ノードは経路情報を一層ずつしか復号しないため、直前のホップと次のホップしか分からず、送信元と宛先の両方を知ることはありません。

Q2: 出口ノードの役割は何ですか?

出口ノードは暗号化の最後の層を復号し、通信を公開の接続先サーバーまたはonionサーバーへ送り出します。

Q3: Tor ブリッジゲートウェイとは何ですか?

ブリッジは、非公開のTor入口リレーで、Torブラウザーへのアクセスを制限している地域で、ISPによるブロックや検閲を回避するために使われます。

Q4: ダークウェブの関係者は暗号資産をどう悪用しますか?

攻撃者は匿名の暗号資産を使って、ダークマーケットで金融取引を行い、通常の銀行取引チェックをすり抜けます。

Q5: 一般的な検索エンジンがディープデータベースをクロールできないのはなぜですか?

クローラーは、ログイン認証情報の入力、セキュリティ CAPTCHA の解決、ディープデータベースへのアクセスに必要なバックエンドの SQL クエリスクリプトの実行ができません。

チェックポイント 10: セキュリティ FAQ – 応用 (パート D)

セキュリティフレームワーク、マルウェア分析、データコンプライアンスについて、高度な技術的側面を探ります。

Q6: Tor ネットワークのディレクトリサーバーとは何ですか?

クライアントが経路を構築するために使う、稼働中のエントリー、ミドル、出口のリレーのリストを管理する、信頼されたサーバーです。

Q7: 悪意のある攻撃者はどのように出口ノードの盗聴を行いますか?

不正な出口ノードの運営者は、暗号化されていない HTTP 通信が Tor ネットワークから出る際に傍受し、ユーザー名や Cookie を盗むことがあります。

Q8: Tor と I2P の違いは何ですか?

Torは集中型のリレーディレクトリと、公開Webにアクセスするための出口ノードを使いますが、I2Pは内部ホスティング向けの分散型ピアツーピア構造を使います。

Q9: 法執行機関はダークウェブの市場をどう追跡しますか?

捜査機関は、ブロックチェーン分析を使い、物理サーバーのホスティング環境を特定し、おとり捜査を行って、運営者を特定します。

Q10: DNS リークはクライアントの匿名性をどのように損ないますか?

DNSリークは、ブラウザーのDNSクエリが、暗号化されたTorネットワーク経由ではなく、ローカルISPを直接経由して送られるときに起こります。

パート 11: 実世界のサイバーセキュリティの事実10選と洞察

セキュリティ侵害、防御の仕組み、コンプライアンス基準に関する実際の事実を確認しましょう。

1. セキュリティの洞察

ほとんどのコンテンツがログインやデータベースの背後にあるため、ディープウェブは検索可能なサーフェスウェブよりはるかに大規模です。

2. セキュリティの洞察

ダークウェブはディープウェブの中の意図的に隠された小さな部分で、Torなどのツールでアクセスします。

3. セキュリティの洞察

Torのルーティングはデータパケットを3回暗号化し、各リレーノードでタマネギのように暗号化の層を1枚ずつはがしていきます。

4. セキュリティの洞察

Torは、米国海軍研究所が進めていたオニオンルーティングのプロジェクトから生まれ、そのコードはフリーソフトウェアとして公開されました。 [1]

5. セキュリティの洞察

オニオンアドレスは、公開鍵のペアから暗号的に生成された56文字の英数字の文字列です。

6. セキュリティの洞察

出口ノードは平文のトラフィックを読み取れるため、Torでも安全なセッションデータにはTLS/HTTPSが必要です。

7. セキュリティの豆知識

イントラネットのサイト、クラウドドライブ、非公開のデータベースは、ディープウェブで最大のデータ保存領域を占めています。

8. セキュリティの豆知識

DuckDuckGo のような専門の検索エンジンは、Tor ネットワークでの匿名検索を可能にするオニオンポータルを運営しています。

9. セキュリティの豆知識

毎日200万人以上のユーザーが、検閲を回避して通信のプライバシーを保つために Tor ネットワークに接続しています。

10. セキュリティの洞察

世界的な法執行作戦(Operation Bayonet など)は、ホスティング用ハードウェアを押収して、主要なダークマーケットを閉鎖させました。

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NIST、OWASP、およびデータプライバシー・コンプライアンスの標準をもとに作成されています。

学術・業界の参考資料

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

解答: チェックポイント 1 – 多肢選択

1 **検索インデックス登録** ディープウェブ 正解: A

指導メモ

ディープウェブのページはログイン画面やデータベースの背後にあり、検索スパイダーによるクロールが妨げられます。出典: IETF RFC 3986。

2 **Torへのアクセス** ダークウェブ 正解: A

指導メモ

ダークウェブは、Torなどのブラウザーからのみアクセスできる、隠されたonionサービスで構成されています。出典: IETF RFC 3986。

3 **ディープデータベース** データベース 正解: A

指導メモ

パスワードで保護されたアカウントや企業の記録が、ディープウェブの最大の部分を占めています。 出典: NIST Digital Identity.

4 **オニオンルーティング** Tor ネットワーク 正解: A

指導メモ

オニオンルーティングは、データパケットを層ごとに暗号化し、複数のノードを経由して中継することで匿名性を高めます。 出典: IETF RFC 3986.

5 **オニオンドメイン** 接尾辞 正解: A

指導メモ

暗号化された.onionドメインのサフィックスは、公開DNSを使わずにTor内部で通信をルーティングします。出典: IETF RFC 3986。

解答: チェックポイント 2 – 正誤問題

6 **ウェブセグメント** 構造 正解: 誤り

指導メモ

ディープウェブはインデックスされていないすべてのページを指し、ダークウェブはその中の小さな暗号化されたonionの一部です。出典: IETF RFC 3986。

7 **企業イントラネット** ディープウェブ 正解: 正しい

指導メモ

イントラネットのサイトはパスワードで保護されたポータルの内側にあり、インデックスされないため、ディープウェブに属します。出典: NIST Digital Identity。

8 **レイヤー暗号化** リレー 正解: 誤り

指導メモ

オニオンリレーは、ユーザーの匿名性を守るため、パケット全体ではなく1つのルーティング層だけを復号します。 出典: IETF RFC 3986.

9 **マルウェアへの接触** 脅威 正解: 正しい

指導メモ

ダークウェブのマーケットプレイスにはセキュリティフィルタリングがなく、マルウェア感染のリスクが極めて高くなります。出典: Center for Internet Security (CIS)。

10 **問題 10** 正解: 誤り

指導メモ

通常の検索エンジンのクローラーはTorを使用しないため、.onionサイトにアクセスしたりインデックスしたりすることはできません。

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. ディープウェブの領域	A 2. ダークウェブポータル	D 3. Onion 拡張子	B 4. Tor ルーティング
F 5. インデックス済みのページ	G 6. ユーザーの匿名性	C 7. プライベートデータベース	E 8. 入口ゲートウェイ

チェックポイント 3: 解答 – 重要用語

1 ディープウェブ	2 ダークウェブ	3 オニオン	4 ルーティング
5 インデックス化	6 匿名性		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 F – トクメイセイ	2 G – データベース	3 D – ルーテイング	4 A – デイープウエブ
5 B – ダークウエブ	6 C – オニオン	7 H – エントリーノード	8 E – サーフエスウエブ

指導者向けディスカッションメモ

重要用語:
生徒がディープウェブの領域、ダークウェブポータル、Onion 拡張子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。

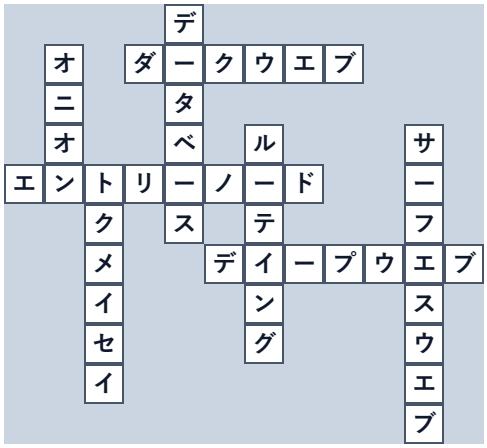
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

3 ヨコ: ダークウエブ 専用のブラウザからしかアクセスできない、暗号化されたネットワーク領域 (6 文字)

6 ヨコ: エントリーノード Torネットワークにアクセスするための入口となるノード (8 文字)

8 ヨコ: デイープウエブ 非公開のログイン画面、メール、データベースの記録など、インデックスされていないウェブコンテンツ (7 文字)

タテのカギ

1 タテ: データベース インデックスされていないシステムの記録を保管する、安全なバックエンドのストレージ (6 文字)

2 タテ: オニオン Torネットワークで使われる、暗号技術ベースのトップレベルドメインの接尾辞 (4 文字)

4 タテ: ルーテイング データを多層に暗号化し、3つのノードを経由して中継すること (6 文字)

5 タテ: サーフエスウエブ Googleで検索可能な形でまとめられた、表層ウェブのコンテンツ (8 文字)

7 タテ: トクメイセイ クライアントの公開IPアドレスをサーバーから隠しておくこと (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. プエデウブーイ — **デイープウエブ**
2. オオンニ — **オニオン**
3. エーサスウブエフ — **サーフエスウエブ**
4. スベターデー — **データベース**
5. ウクブダエー — **ダークウエブ**
6. ンイルテグー — **ルーテイング**
7. セトイイメク — **トクメイセイ**
8. リンードエーノト — **エントリーノード**

秘密の暗号チャレンジ 解答

"オニオンデ トクメイセイヲ タモツ"

ケーススタディの解答

A ケーススタディ 1: データ漏えいの特定

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: 企業のセキュリティ監査で、機密性の高い顧客データベースのレコードがオニオンマーケットプレイスで取引されていることが判明します。そのデータは Google にインデックスされていません。
- 推奨される戦略と解決策: 関係するセグメント: 非公開のデータベースはディープウェブ (インデックスされていないが安全な領域) に属します。盗まれたデータを取引するマーケットプレイスはダークウェブ (オニオンネットワーク) にあります。経緯: ハッカーはサーバーの防御を突破してディープウェブからデータベースを盗み、法執行機関の追跡を逃れるためにダークウェブに匿名で出品しました。

B ケーススタディ 2: 匿名性とマルウェアのリスク

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: アナリストが、Tor のウェブサイトで脅威インテリジェンスのフィードを確認したいと考えています。Tor ブラウザーをダウンロードして、そのサイトにアクセスします。
- 推奨される対策と解決策: メリット: Tor は3つのノードを経由してトラフィックを中継し、アナリストの社内 IP を隠します。リスクと対策: ダークウェブのリンクには評判のスクリーニングがありません。アナリストは Tor を分離された仮想マシン(VM)内で実行し、Tor の設定で JavaScript を無効にして、社内ネットワークを守るためファイルのダウンロードを避ける必要があります。