名前: 日付: 得点:

ウイルス対策ソフトとエンドポイント保護ガイド

シグネチャ検出、ヒューリスティック、動作監視、サンドボックス、アップデート

ウイルス対策ソフトの学習の概要

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、ウイルス対策ソフトとエンドポイント保護について学びます。シグネチャデータベース、ヒューリスティックスキャナー、挙動の監視、サンドボックス化された仮想ファイル、誤検知の軽減を取り上げます。

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/antivirus/

あなたのウイルス対策戦略 学習ロードマップ

- シグネチャベースとヒューリスティックベースのマルウェア検出の違いを説明します。
- 振る舞い監視とサンドボックス隔離のプロトコルを理解する。
- リアルタイムスキャンがシステムのパフォーマンスとエンドポイントに与える影響を評価します。
- デジタル証明書の検証を使って、誤検出による分類を減らす。
- 企業のエンドポイント全体での、毎日の定義ファイル更新の配布を管理する。

ウイルス対策ガイドの手順

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。学んだ知識をエンドポイントのウイルス対策セキュリティに応用しましょう。 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。

ウイルス対策とシグネチャスキャン(はじめに)

ウイルス対策ソフトは、マルウェアを特定、隔離、削除することでエンドポイントを保護します。最新のシステムは、シグネチャデータベース（既知の脅威のハッシュと照合）、ヒューリスティック（ファイル構造の分析）、動作監視を組み合わせて、ゼロデイ攻撃を検出します。

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. シグネチャベース検出の限界は何ですか?
   - A. 未知のマルウェアや改変されたマルウェアは識別できない
   - B. 誤検知が多く発生する
   - C. 高い CPU 処理能力が必要になる
   - D. インターネットに接続しているときにのみ動作する

2. 2. ヒューリスティックスキャナーは、新しいマルウェアの亜種をどのように検知しますか?
   - A. 不審なパターンやコード構造を特定することによって
   - B. ファイルのハッシュを脅威のデータベースと照合することで
   - C. 署名のない実行ファイルをすべて自動的に削除することで
   - D. すべてのファイルをパブリッククラウドのフォルダーにアップロードすることで

3. 3. ウイルス対策のサンドボックス実行の目的は何ですか?
   - A. 安全な仮想の保管庫でファイルを隔離して分析する
   - B. ローカルファイルシステムのバックアップ転送の高速化
   - C. ローカルのオペレーティングシステムのセキュリティパッチを更新すること
   - D. 保存容量を節約するために大きな文書ファイルを圧縮すること

4. 4. 脅威となる動作をリアルタイムで検出する検出方法はどれですか?
   - A. ソフトウェアの動作を監視する行動分析
   - B. 夜間に実行される過去ログの検査
   - C. 動作の遅いアプリを報告するユーザーの手動対応
   - D. インストール済みプログラムを毎週手動で確認すること

5. 5. スキャナーにとって、定義ファイルを定期的に更新することが重要なのはなぜですか?
   - A. シグネチャエンジンのデータベースに脅威の識別子を供給するため
   - B. 動作中にCPUのクロック速度を上げるため
   - C. グローバル DNS ネームサーバーのキャッシュ時間を変更するため
   - D. ウェブブラウザーの Cookie 設定を承認するため

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. シグネチャ検出は、ファイルの暗号学的ハッシュをデータベースのリストと照合します。

○ 正しい ○ 誤り

7 質問(正誤) 7

7. ヒューリスティックスキャナーは、安全なファイルに対して誤検知のアラートを出すことがあります。

○ 正しい ○ 誤り

8 質問(正誤) 8

8. サンドボックスは、マルウェアがネットワークファイルに制限なくアクセスできるようにします。

○ 正しい ○ 誤り

9 質問(正誤) 9

9. 行動スキャンは、ファイルが悪意のある動作を示したときにブロックします。

○ 正しい ○ 誤り

10 質問(正誤) 10

10. 標準的なウイルス対策ソフトは、ゼロデイ攻撃をすべて完全に防ぎます。

○ 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. 従来型のスキャナーは、既知のマルウェアを見つけるために _____ の照合に頼っています。

2. ファイルのコードパターンを分析する方法は、 _____ スキャンと呼ばれます。

3. アンチウイルスツールは、疑わしいファイルを _____ 環境に隔離します。

4. リアルタイム監視は、プログラムの _____ を見て不審な動きを探します。

5. スキャナーは、新しい脅威を認識するため、データベースの _____ を毎日ダウンロードします。

6. 安全なプログラムがマルウェアと判定されると、 _____ の警告が出ます。

用語バンク

アンチウイルス　サンドボックス　シグネチャ　ヒューリスティック　隔離　誤検出　更新　振る舞い

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

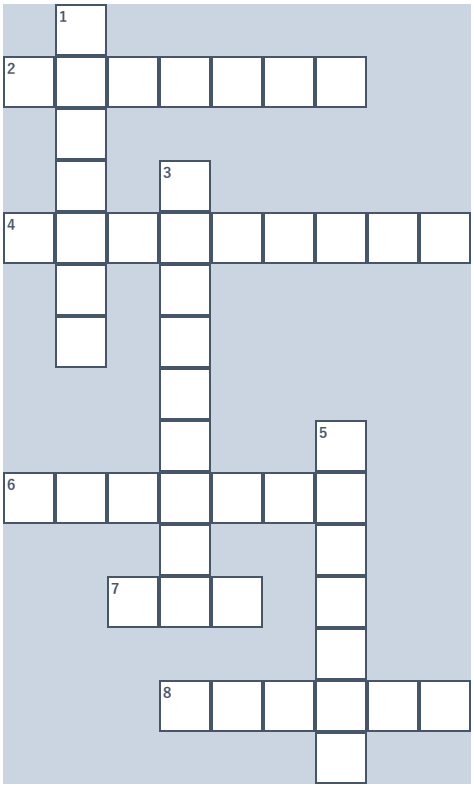
定義マッチング

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. ハッシュ署名	A	疑わしいファイルを隔離して、ローカルシステムへの露出を防ぐこと。
	2. コードヒューリスティック	B	エンドポイントをスキャンし、エクスプロイトから保護するソフトウェア群。
	3. ファイルサンドボックス	C	実行中のソフトウェアの動作を監視して、悪意のある動作パターンを見つけること。
	4. 振る舞いスキャン	D	既知の脅威を識別するために使われる、固有の暗号的なデータベースの指紋。
	5. 毎日の更新	E	信頼できないコードを安全に実行する、安全な仮想テスト環境。
	6. 誤検知	F	脅威データベースに情報を供給する、定期的な定義ファイルのダウンロード。
	7. 脅威の隔離	G	疑わしいコード構成を持つファイルを検出する、ルールベースの分析。
	8. ウイルス対策ツール	H	安全なソフトウェアをマルウェアと誤って分類するセキュリティ警告。

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. エクスプロイトからエンドポイントをスキャンして保護するソフトウェア群 (7)

4. 既知の脅威を識別するために使う、暗号学的な固有のデータベース上の痕跡 (9)

6. 実行中のソフトウェアの動作を監視し、悪意のある動きのパターンを探すこと (7)

7. 疑わしいファイルを閉じ込めて、ローカルシステムへの影響を防ぐこと (3)

8. 安全なソフトウェアを誤ってマルウェアと判定するセキュリティ警告 (6)

タテのカギ

1. 信頼できないコードを安全に実行できる、隔離された仮想のテスト環境 (7)

3. 疑わしいコード構造を持つファイルを、ルールに基づく分析で検出する方法 (9)

5. 脅威データベースに反映させる定義ファイルを定期的にダウンロードすること (7)

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 タテのカギ

ヨコのカギ

2 ヨコ: エクスプロイトからエンドポイントをスキャンして保護するソフトウェア群 (7 文字):

4 ヨコ: 既知の脅威を識別するために使う、暗号学的な固有のデータベース上の痕跡 (9 文字):

6 ヨコ: 実行中のソフトウェアの動作を監視し、悪意のある動きのパターンを探すこと (7 文字):

7 ヨコ: 疑わしいファイルを閉じ込めて、ローカルシステムへの影響を防ぐこと (3 文字):

8 ヨコ: 安全なソフトウェアを誤ってマルウェアと判定するセキュリティ警告 (6 文字):

タテのカギ

1 タテ: 信頼できないコードを安全に実行できる、隔離された仮想のテスト環境 (7 文字):

3 タテ: 疑わしいコード構造を持つファイルを、ルールに基づく分析で検出する方法 (9 文字):

5 タテ: 脅威データベースに反映させる定義ファイルを定期的にダウンロードすること (7 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。

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

用語リスト

ハツシユシグネチヤ　ヒユーリステイツク　サンドボツクス　フルマイケンチ　ニチジコウシン
ゴケンシユツ　カクリ　アンチウイルス

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
A. ハツシユシグネチヤ
B. ヒユーリステイツク
C. サンドボツクス
D. フルマイケンチ
E. ニチジコウシン
F. ゴケンシユツ
G. カクリ
H. アンチウイルス

定義とマッチ欄
1. 実行中のソフトウェアの動作を監視し、悪意のある動きのパターンを探すこと。
2. エクスプロイトからエンドポイントをスキャンして保護するソフトウェア群。
3. 脅威データベースに反映させる定義ファイルを定期的にダウンロードすること。
4. 疑わしいコード構造を持つファイルを、ルールに基づく分析で検出する方法。
5. 疑わしいファイルを閉じ込めて、ローカルシステムへの影響を防ぐこと。
6. 既知の脅威を識別するために使う、暗号学的な固有のデータベース上の痕跡。
7. 信頼できないコードを安全に実行できる、隔離された仮想のテスト環境。
8. 安全なソフトウェアを誤ってマルウェアと判定するセキュリティ警告。

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. グシユツハネチヤシ
2. サドスクツボン
3. コニウンジシチ
4. クリカ
5. イスユクテリヒツー
6. ンマケフイチル
7. ユゴシツンケ
8. ンウスアルイチ

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	ソフトウェアを更新する理由			
2	ITのサポートを頼める人			
3	アンチウイルスが何かを検出したときにすること			
4	コンピューターウイルスのサイン			
5	隔離されるもの			
6	ウイルスが隠れる場所			
7	決して共有してはいけない情報			
8	悪意のあるソフトウェアの種類			
9	知っているセキュリティツール			
10	アンチウイルスがスキャンするもの			
11	バックアップするもの			
12	ハッキングされるおそれのあるデバイス			
13	知っているアンチウイルスソフト			
14	誤検知の理由			
15	今日から始められる安全な習慣			

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: シグネチャ型スキャンとヒューリスティックスキャン



シナリオ: 従業員が、別のチームが社内で開発したカスタムユーティリティをダウンロードします。シグネチャ型スキャナーは問題なしと判定しますが、ヒューリスティック型スキャナーは不審だとして警告します。

ディスカッションの問い: なぜこうなったのか、またファイルが安全かどうかをどのように確認できるかを説明できますか？

ケーススタディ 2: 誤検知への対応



シナリオ: ソフトウェア開発者が自分のアプリケーションをコンパイルします。システムのアンチウイルスは、新しい実行ファイルをマルウェアとして警告し、隔離します。

ディスカッションの問い: ホワイトリスト登録のリスクを概説し、正しい解決の手順を説明できますか？

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

27	37	72	40	13	19	2	18	8	60		31	41	3	4	1	45

32	18	9	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: 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: ウイルス対策ソフトは、マルウェアをどのように識別しますか?

データベースのシグネチャ照合、ヒューリスティックなコード構造の分析、リアルタイムの挙動監視によって、マルウェアを特定します。

Q2: シグネチャベースの検出とは何ですか?

ファイルの暗号ハッシュを、既知のマルウェアの脅威のデータベースのリストと照合する、スキャン方法です。

Q3: ヒューリスティックスキャナーとは何ですか?

ヒューリスティックは、ファイルの構造とコードの命令を分析し、マルウェアの亜種に共通する疑わしいパターンを検知します。

Q4: ファイルが隔離されるとはどういう意味ですか?

ウイルス対策ソフトはファイルを安全な隔離フォルダーに移動し、実行をブロックしてオペレーティングシステムを保護します。

Q5: ウイルス対策ソフトの誤検知とは何ですか?

正当で安全なソフトウェアが、スキャンアルゴリズムによって誤ってマルウェアと判定される、エラーです。

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: 動作監視はシステムをどう守りますか?

実行中のソフトウェアをリアルタイムで監視し、コードの挿入などの疑わしい変更を試みるプロセスを遮断します。

Q7: サンドボックステストが重要なのはなぜですか?

サンドボックス化は、信頼できないファイルを隔離された仮想マシンで実行し、システムを危険にさらすことなく動作を安全に観察します。

Q8: ウイルス対策の定義ファイルはどのくらいの頻度で更新すべきですか?

スキャナーは、新たに発見されたマルウェアの種類を認識するために、定義を毎日または毎時間更新する必要があります。

Q9: ウイルス対策ソフトと EDR の違いは何ですか?

ウイルス対策はファイルのスキャンに重点を置くのに対し、EDR（Endpoint Detection and Response）はネットワーク全体の脅威の追跡と封じ込めを行います。

Q10: 2つのウイルス対策プログラムを一緒に実行できますか?

いいえ。2 つのスキャナーを同時に動かすと、システムの競合が起き、性能が低下し、互いの動作を妨げることがあります。

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: ヒューリスティックルールは、脅威のすり抜けをどのように最小限に抑えますか?

ヒューリスティックは、特定のシグネチャではなく一般的な脅威のパターンを分析し、既知のマルウェアファミリーの改変された亜種を検知します。

Q2: ポリモーフィックウイルスとは何ですか?

実行のたびにファイル構造と復号ルーチンを変更するマルウェアで、シグネチャによるスキャンが効かなくなります。

Q3: サンドボックスは VM 回避をどのように検出しますか?

最新のサンドボックスはマウスのクリックやシステムの稼働時間を模倣し、仮想マシン上で動作するときに身を隠すよう作られたマルウェアをだまします。

Q4: シグネチャ更新のダウンロード形式にはどのようなものがありますか?

更新は通常、軽量な差分バイナリファイルによる増分で行われ、クライアントのネットワーク帯域幅の消費を最小限に抑えます。

Q5: エンドポイントエージェントはローカルスキャンをどう管理しますか?

エージェントは軽量なバックグラウンドチェックを行い、詳細な暗号ハッシュの照合はクラウドの脅威データベースに任せます。

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: ルートキット検出スキャンとは何ですか?

カーネルレベルのメモリーテーブルをスキャンし、ルートキットがアクティブなスレッドを隠すためにフックする OS の API を迂回します。

Q7: 動作スキャンはランサムウェアをどうブロックしますか?

ファイルを自動的に大量暗号化するループを検知し、システムのデータベースがロックされる前にホストのプロセスを終了させます。

Q8: コード署名証明書の検証とは何ですか?

スキャナーは、コードのデジタル署名を信頼できるルート認証局と照合し、ソフトウェア開発者の身元を検証します。

Q9: パッカーはスキャンエンジンにどう影響しますか?

パッカーはマルウェアのペイロードを圧縮または暗号化します。スキャナーは、シグネチャの照合を実行する前に、メモリ内でファイルを展開する必要があります。

Q10: EDR ツールはどのように隔離を自動化しますか?

EDRエージェントは、ネットワークレベルで侵害されたエンドポイントを隔離し、横方向の移動をブロックしつつ、アナリストのアクセスは許可します。

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

シグネチャデータベースは既知のマルウェアのハッシュを保存しているため、まったく新しいファイルや改変されたファイルは、定義が更新されるまで見逃されます。

2. セキュリティの洞察

ヒューリスティックエンジンは、シグネチャが存在する前に一部の新しいマルウェアの亜種を検知できますが、その代わり誤検知が増えます。

3. セキュリティの洞察

誤検知のアラートは、誤って隔離されたファイルの確認と復元に、IT部門の時間を費やさせます。

4. セキュリティの洞察

ポリモーフィック型マルウェアはコピーのたびにコードを変化させるため、防御側はシグネチャとヒューリスティックや振る舞いのチェックを組み合わせます。

6. セキュリティの洞察

マルウェアの作者は、サンドボックス環境を確認するカスタムコードを書き、実行を遅らせてタイマーをすり抜けようとします。

5. セキュリティの洞察

クラウド型のウイルス対策エンジンは、疑わしいファイルのハッシュを、大規模なオンライン脅威データベースとほぼリアルタイムで照合します。

7. セキュリティの豆知識

ベンダーは定義ファイルの更新をエンドポイントに定期的に配信し、スキャナーが新たに確認された脅威を認識できるようにします。

8. セキュリティの豆知識

ランサムウェアの動作モニターは、ファイルの暗号化やシャドウコピーの削除に関連する特定の Win32 API 呼び出しを対象にします。

9. セキュリティの豆知識

有効なコード署名は誤検知のリスクを下げられますが、マルウェアも署名される可能性があるため、署名付きファイルもスキャンされます。

10. セキュリティの洞察

ルートキットはシステムカーネルの構造を改ざんするため、検出と駆除には起動時に動作する専用のスキャナーが必要です。

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

学術・業界の参考資料

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
https://csrc.nist.gov/pubs/sp/800/83/r1/final

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

[3] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

解答: チェックポイント 1 – 多肢選択

1 **問題 1** シグネチャ 正解: A

指導メモ

シグネチャスキャンは既知のデータベースのハッシュに依存するため、未知または改変されたマルウェアは検出できません。出典: OWASP Secure Configuration。

2 **問題 2** ヒューリスティック 正解: A

指導メモ

ヒューリスティックは、コードの構造とコマンドを分析して、新種の脅威の疑わしい特徴を見つけます。出典: Center for Internet Security (CIS)。

3 **問題 3** サンドボックス化 正解: A

指導メモ

サンドボックスは、疑わしいファイルを隔離された仮想マシンで実行し、その動作を安全に観察します。出典: NIST Digital Identity。

4 **問題 4** 行動ベース 正解: A

指導メモ

振る舞いスキャンは、実行中のプログラムをリアルタイムで監視し、不正なシステム変更をブロックします。出典: Center for Internet Security (CIS)。

5 **問題 5** 更新 正解: A

指導メモ

スキャナーは、脅威の状況に合わせて、毎日の増分定義ファイルの更新をダウンロードします。出典: OWASP Secure Configuration。

解答: チェックポイント 2 – 正誤問題

6 **問題 6** シグネチャ 正解: 正しい

指導メモ

シグネチャ型のツールは暗号ハッシュを計算し、既知の脅威ハッシュのデータベースと照合します。出典: OWASP Secure Configuration。

7 **問題 7** ヒューリスティック 正解: 正しい

指導メモ

ヒューリスティックエンジンはルールベースの構造を実行するため、正当で安全なファイルを疑わしいと判定する場合があります。出典: Center for Internet Security (CIS)。

8 **問題 8** サンドボックス化 正解: 誤り

指導メモ

サンドボックスは仮想コンテナ内でコードを実行し、ネットワーク共有へのアクセスを厳密にブロックします。出典: NIST Digital Identity。

9 **問題 9** 行動ベース 正解: 正しい

指導メモ

リアルタイム監視は、不正な書き込みやファイルロックを試みる実行中のプロセスにフラグを立てます。出典: Center for Internet Security (CIS)。

10 **問題 10** 正解: 誤り

指導メモ

どのアンチウイルスもゼロデイ攻撃のすべてを防げるわけではありません。未知の脅威はシグネチャやヒューリスティックをすり抜けることがあります。

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

D 1. ハッシュ署名	G 2. コードヒューリスティック	E 3. ファイルサンドボックス	C 4. 振る舞いスキャン
F 5. 毎日の更新	H 6. 誤検知	A 7. 脅威の隔離	B 8. ウイルス対策ツール

チェックポイント 3: 解答 – 重要用語

1 シグネチャ	2 ヒューリスティック	3 サンドボックス	4 振る舞い
5 更新	6 誤検出		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 D – フルマイケンチ	2 H – アンチウイルス	3 E – ニチジコウシン	4 B – ヒユーリステイツク
5 G – カクリ	6 A – ハツシユシグネチヤ	7 C – サンドボツクス	8 F – ゴケンシユツ

指導者向けディスカッションメモ

重要用語:
生徒がハッシュ署名、コードヒューリスティック、ファイルサンドボックス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

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

クロスワードの解答

	サ					
ア	ン	チ	ウ	イ	ル	ス
	ド					
	ボ		ヒ			
ハ	ツ	シ	ユ	シ	グ	ネ	チ	ヤ
	ク		ー			
	ス		リ			
			ス			
			テ			ニ
フ	ル	マ	イ	ケ	ン	チ
			ツ			ジ
		カ	ク	リ		コ
						ウ
			ゴ	ケ	ン	シ	ユ	ツ
						ン		

ヨコのカギ

2 ヨコ: アンチウイルス エクスプロイトからエンドポイントをスキャンして保護するソフトウェア群 (7 文字)

4 ヨコ: ハツシユシグネチヤ 既知の脅威を識別するために使う、暗号学的な固有のデータベース上の痕跡 (9 文字)

6 ヨコ: フルマイケンチ 実行中のソフトウェアの動作を監視し、悪意のある動きのパターンを探すこと (7 文字)

7 ヨコ: カクリ 疑わしいファイルを閉じ込めて、ローカルシステムへの影響を防ぐこと (3 文字)

8 ヨコ: ゴケンシユツ 安全なソフトウェアを誤ってマルウェアと判定するセキュリティ警告 (6 文字)

タテのカギ

1 タテ: サンドボツクス 信頼できないコードを安全に実行できる、隔離された仮想のテスト環境 (7 文字)

3 タテ: ヒユーリステイツク 疑わしいコード構造を持つファイルを、ルールに基づく分析で検出する方法 (9 文字)

5 タテ: ニチジコウシン 脅威データベースに反映させる定義ファイルを定期的にダウンロードすること (7 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. グシユツハネチヤシ — ハツシユシグネチヤ
2. サドスクツボン — サンドボツクス
3. コニウンジシチ — ニチジコウシン
4. クリカ — カクリ
5. イスユクテリヒツー — ヒユーリステイツク
6. ンマケフイチル — フルマイケンチ
7. ユゴシツンケ — ゴケンシユツ
8. ンウスアルイチ — アンチウイルス

秘密の暗号チャレンジ 解答

"ヒューリスティックデ マルウェアヲ ミツケル"

ケーススタディの解答

A ケーススタディ 1: シグネチャ型スキャンとヒューリスティックスキャン 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: 従業員が、別のチームが社内で作成したカスタムユーティリティをダウンロードします。シグネチャスキャナーは通過させましたが、ヒューリスティックスキャナーは疑わしいと判定します。
- 推奨される戦略と解決策: 起きた理由: シグネチャスキャンはファイルのハッシュを調べますが、独自に作られたものなので脅威データベースにありません。ヒューリスティック検査は構造を分析し、疑わしい動作 (レジストリへの書き込みなど) を検出しました。検証: ファイルをサンドボックスで実行して動作を観察し、デジタル署名を確認して、ハッシュを脅威インテリジェンスポータルに提出します。

B ケーススタディ 2: 誤検知への対応 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: ソフトウェア開発者がアプリケーションをコンパイルします。システムのウイルス対策ソフトが、新しい実行ファイルをマルウェアとして検出し、隔離します。
- 推奨される戦略と解決策: ホワイトリスト登録のリスク: スキャナーを回避すると、実際に感染したコードが実行される可能性があります。解決の手順: ファイルをウイルス対策ベンダーに提出して分析してもらい、認証局を使ってコードにデジタル署名し、ウイルス対策を無効にするのではなく、特定のフォルダーの例外を一時的に設定します。