名前: 日付: 得点:

ゼロトラストアーキテクチャとセキュリティ

継続的な検証、ネットワークのマイクロセグメンテーション、ID・アクセス管理、最小権限、ポスチャチェック。

ゼロトラストセキュリティ学習概要

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、ゼロトラストのアーキテクチャとセキュリティについて学びます。継続的な検証、ネットワークのマイクロセグメンテーション、ID・アクセス管理 (IAM)、最小権限、セッション監査を取り上げます。

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/zero-trust-cyber-security/

あなたのゼロトラスト戦略 学習ロードマップ

- 継続的な検証という中核の原則を理解する。
- ネットワークのマイクロセグメンテーションと、最小権限のアクセスを導入する。
- デバイスのポスチャチェックと、アクティブなセッションの監査を設定してください。

ゼロトラスト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。学んだ知識をゼロトラストアーキテクチャに応用しましょう。 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。

ゼロトラストアーキテクチャとセキュリティ（入門）

ゼロトラストセキュリティは、従来のネットワーク境界モデルを、「決して信頼せず、常に検証する」という厳格なポリシーに置き換えます。マイクロセグメンテーション、IDおよびアクセス管理 (IAM)、最小権限、セキュリティ状態のチェックを導入すると、脅威の横方向の移動を阻止できます。

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. ゼロトラストセキュリティの中心となる原則は何ですか?

- A. 決して信頼せず、発信元にかかわらずすべてのアクセスリクエストを常に検証する
- B. 企業ファイアウォール内のトラフィックはすべて安全だと想定すること
- C. 速度向上のためにデータベースファイルを暗号化せずに保存すること
- D. SPF レコードだけでメール認証を実施すること

2 2. ネットワークのマイクロセグメンテーションとは何ですか?

- A. ネットワークを小さな隔離ゾーンに分割し、横方向の移動を封じ込める
- B. データ転送中にネットワークカードを暗号化すること
- C. すべてのローカルサーバーを1つのパブリックIPアドレスに接続すること
- D. ブラウザーセッションでのユーザーのキー入力を監視すること

3 3. 最小権限の原則とは何ですか?

- A. ユーザーのアクセス権限を、業務に必要なものだけに制限する
- B. 既定ですべてのユーザーにすべてのシステム権限を与えること
- C. 企業のデータベースサーバーへの匿名ログインを許可すること
- D. 公衆 Wi-Fi ルーターをパスワードなしで設定すること

4 4. ID・アクセス管理(IAM)とは何ですか?

- A. デジタルIDを管理し、システム権限を制御するフレームワーク
- B. ローカルのファイルディレクトリをスキャンするウイルス対策ユーティリティ
- C. エアギャップメディアを使ったバックアップ保管システム
- D. なりすましドメインを拒否するメールゲートウェイのプロトコル

5 5. 継続的認証とはどういう意味ですか?

- A. 有効なセッション中に、ユーザーの身元とデバイスの状態を繰り返し検証する
- B. マスターパスワードを10分ごとに変更すること
- C. 複数のアルゴリズムでデータベースのレコードをハッシュ化すること
- D. TLS 鍵を使って通信中のネットワークパケットを暗号化すること

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. ゼロトラストは、企業のファイアウォールの内側にあるすべての通信は安全だと想定します。

○ 正しい ○ 誤り

7 質問 7

7. マイクロセグメンテーションは、攻撃者が内部サーバー間を横方向に移動する能力を制限します。

○ 正しい ○ 誤り

8 質問 8

8. 最小権限では、デフォルトですべてのデータベースファイルへのアクセスが許可されます。

○ 正しい ○ 誤り

9 質問 9

9. 継続的な検証では、ログインセッションの全体を通じて、デバイスの健全性と認証情報を検証します。

○ 正しい ○ 誤り

10 質問 10

10. ゼロトラストを導入すると、企業のログイン情報が侵害された場合の影響を抑えられます。

○ 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. すべてのアクセスポイントで認証情報を求めることは、継続的な _____ です。

2. 企業ネットワークを細かなゾーンに分割することは、マイクロ _____ です。

3. デジタルIDとアクセス制御を設定するには、 _____ システムを使います。

4. ユーザーの権限を制限するには、 _____ の原則を使います。

5. 接続したデバイスの健全性を評価することは、デバイスの _____ をスキャンすることです。

6. アクティブなセッションを記録して確認することは、セキュリティ _____ です。

用語バンク

IAM　アクセス　セグメンテーション　ポスチャ　監査　境界　検証　最小権限

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

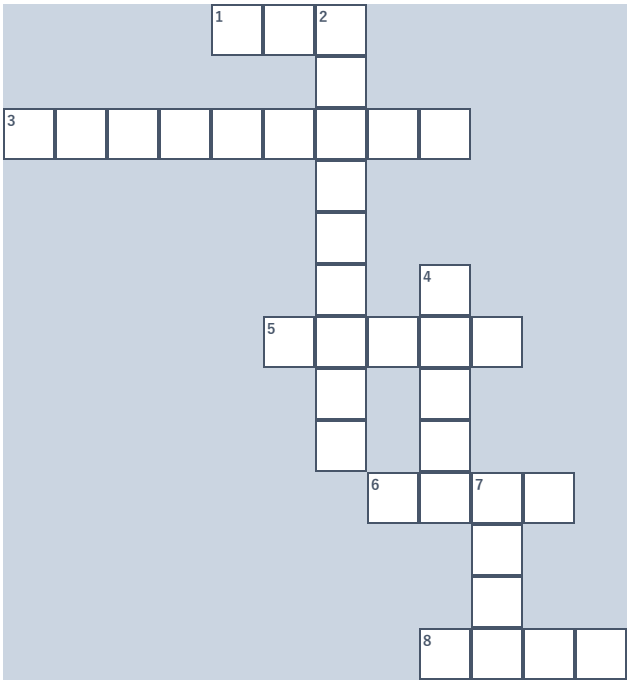
定義マッチング

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. 検証	**A**	ユーザーの認証情報へのアクセスを管理すること。
	2. セグメンテーション	**B**	最小アクセス権の原則。
	3. IAM	**C**	ネットワークパケットの通信を経路制御すること。
	4. 権限	**D**	外部ネットワークの境界による保護。
	5. ポスチャ	**E**	記録されたアクセスセッションを確認すること。
	6. 監査	**F**	内部ネットワークゾーンの分割。
	7. ファイアウォール	**G**	常にユーザーの認証情報を確認する。
	8. ルーター	**H**	デバイスの健全性の状態を評価すること。

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

1. 記録されたアクセスセッションを見直すこと (3)
3. 内部ネットワークをゾーンに分けること (9)
5. ユーザーの認証情報を常に確認すること (5)
6. ユーザーの認証情報とアクセスを管理すること (4)
8. デバイスの健全性の状態を評価すること (4)

タテのカギ

2. 必要最小限のアクセス権だけを与える原則 (9)
4. 外部ネットワークとの間に設けられる防御の線 (5)
7. ユーザーがシステムや資源に接続して利用すること (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

1 ヨコ: 記録されたアクセスセッションを見直すこと (3 文字):

3 ヨコ: 内部ネットワークをゾーンに分けること (9 文字):

5 ヨコ: ユーザーの認証情報を常に確認すること (5 文字):

6 ヨコ: ユーザーの認証情報とアクセスを管理すること (4 文字):

8 ヨコ: デバイスの健全性の状態を評価すること (4 文字):

タテのカギ

2 タテ: 必要最小限のアクセス権だけを与える原則 (9 文字):

4 タテ: 外部ネットワークとの間に設けられる防御の線 (5 文字):

7 タテ: ユーザーがシステムや資源に接続して利用すること (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。

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

用語リスト

ケンシヨウ　セグメンテーシヨン　アイアム　サイシヨウケンゲン　ポスチヤ　カンサ
アクセス　キヨウカイ

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. ケンショウ
B. セグメンテーションヨン
C. アイアム
D. サイショウケンゲン
E. ポスチヤ
F. カンサ
G. アクセス
H. キヨウカイ

定義とマッチ欄
1. ユーザーがシステムや資源に接続して利用すること。
2. 記録されたアクセスセッションを見直すこと。
3. 必要最小限のアクセス権だけを与える原則。
4. 内部ネットワークをゾーンに分けること。
5. 外部ネットワークとの間に設けられる防御の線。
6. デバイスの健全性の状態を評価すること。
7. ユーザーの認証情報とアクセスを管理すること。
8. ユーザーの認証情報を常に確認すること。

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. ヨシケウン
2. アアムイ
3. ヤポチス
4. スセアク
5. シテグンーンセヨメ
6. ゲヨインケサウンシ
7. サンカ
8. イキウカヨ

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	決して共有してはいけない情報			
2	今日から始められる安全な習慣			
3	デバイスで確認されること			
4	ログに記録されるもの			
5	サイバーセキュリティに関連する言葉			
6	ゼロトラストが確認すること			
7	日常生活で身分証を見せる場所			
8	本人であることを確認する方法			
9	データが漏えいした後にすること			
10	コンピューターが感染しているサイン			
11	ソフトウェアを更新する理由			
12	会社内のアクセスレベル			
13	知っているセキュリティツール			
14	ネットワークを分割できるゾーン			
15	信頼についてのことわざ			

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: ゼロトラストネットワークアーキテクチャへの移行



シナリオ: 大企業が現在、社内ネットワークがフラットで、ローカルネットワーク上のどのデバイスからでも、すべての社内サーバーとデータベースにアクセスできる状態です。

ディスカッションの問い: 横方向の移動を制限するための、ネットワークのマイクロセグメンテーション戦略を設計できますか？

ケーススタディ 2: 最小権限のアクセス制御の導入



シナリオ: 監査ログから、一時的なデータベースユーザーや下位の従業員が、重要な会計データベースに対して、グローバルな読み取りと書き込みの権限を持っていることが判明します。

ディスカッションの問い: 最小権限の原則を徹底するために、データベースのIAM権限を監査して制限できますか？

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

55	43	20	39	13	20	60		18	24	22		9	46	12	38	3	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: 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: ゼロトラストとは何ですか?

ゼロトラストは、脅威がネットワーク境界の外にも内にも存在すると想定し、すべてのリクエストに検証を求めるセキュリティの枠組みです。 [1]

Q2: ゼロトラストの基本ルールは何ですか?

決して信頼せず、常に検証する。

Q3: マイクロセグメンテーションとは何ですか?

ネットワークを小さく安全な論理セグメントに分割して、トラフィックを制御し、侵害を封じ込めること。

Q4: 最小権限とは何ですか?

ユーザーに、特定の業務を行うために必要な最小限のアクセス権だけを与えること。 [2]

Q5: IAM は何の略ですか?

アイデンティティとアクセスの管理。

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: デバイスポスチャチェックはどう役立ちますか?

アクセスを許可する前に、デバイスにパッチが適用され、有効なウイルス対策が動作しており、安全であることを検証します。

Q7: 横展開とは何ですか?

攻撃者が、最初に侵害したノードから、より価値の高いシステムへとネットワーク内を移動していく手法。

Q8: ゼロトラストはファイアウォールに取って代わりますか?

いいえ、アイデンティティ中心のチェックと内部のセグメンテーションファイアウォールを加えることで、強化します。

Q9: 継続的認証とは何ですか?

最初のサインイン時だけでなく、ログインセッション中ずっとユーザーの本人確認を継続すること。

Q10: なぜフラットなネットワークは危険なのですか?

フラットなネットワークでは、1 つのノードが侵害されると、攻撃者はネットワーク上のあらゆるデータベースに簡単にアクセスできてしまいます。

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: ゼロトラストは、境界モデルの問題にどのように対処しますか?

時代遅れの「城と堀」モデルに代わり、防御の重点を境界のネットワークから、特定のユーザーの身元とリソースへと移します。

Q2: ポリシー決定ポイント（PDP）とは何ですか?

アクセスを許可すべきかを決めるために、認可リクエストをセキュリティルールに照らして評価するシステムコンポーネント。

Q3: ポリシー適用ポイント(PEP)とは何ですか?

PDPの判断に基づいて、接続リクエストを物理的に許可またはブロックするシステムノード(ゲートウェイやプロキシなど)。

Q4: ロールベースアクセス制御(RBAC)はゼロトラストをどう支えますか?

RBAC は権限を特定のロールにまとめることで、ユーザーが過剰な管理者権限を継承するのを防ぐのに役立ちます。

Q5: コンテキストに基づくアクセス制御とは何ですか?

地理的な位置、デバイスの状態、ログイン時刻などの二次的な手がかりを使って、ログイン要求のリスクを評価すること。

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: マイクロセグメンテーションは標準の VLAN とどう違いますか?

VLANはネットワークをレイヤー2で大まかな論理セグメントに分けますが、マイクロセグメンテーションはソフトウェアのポリシーで個々のワークロードを隔離します。

Q7: ジャストインタイム(JIT)アクセスとは何ですか?

一時的に昇格した管理者権限を与え、作業が終わると自動的に取り消すこと。

Q8: ゼロトラストのフレームワークで API をどう保護しますか?

暗号署名されたOAuthトークンを要求し、すべてのAPIゲートウェイでリクエストの署名を監査することによって。

Q9: ゼロトラストネットワークアクセス(ZTNA)クライアントとは何ですか?

生のネットワークサブネットではなく、特定のアプリケーションへの安全で暗号化された外向き接続を確立するソフトウェアエージェント。

Q10: ログ監査はゼロトラストをどのように支援しますか?

継続的なログ記録により、自動化されたセキュリティ分析ツールが異常を検出し、不正なログインを直ちに停止できます。

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

ゼロトラストアーキテクチャは、従来の「城と堀」モデルを、ID中心の検証ルールに置き換えます。

2. セキュリティの洞察

ネットワークのマイクロセグメンテーションは、ワークロードを小さな保護ゾーンに隔離することで、マルウェアが到達できる範囲を狭めます。

3. セキュリティの洞察

ゼロトラストは、ネットワークセグメントではなく、資産、サービス、アカウントなどのリソースの保護に重点を置きます。 [1]

4. セキュリティの洞察

最小権限のアクセスポリシーは、中核データベースからの内部関係者によるデータ持ち出しの脅威のリスクを減らします。

5. セキュリティの洞察

デバイスの状態検証では、オペレーティングシステムのパッチレベルと、有効なアンチウイルスの状態をリアルタイムで確認します。

6. セキュリティの洞察

ゼロトラストネットワークアクセス (ZTNA) ブローカーは、企業のVPNの代わりとして、または補完として、ユーザーのアクセス範囲を制限できます。

7. セキュリティの豆知識

ジャストインタイム (JIT) の管理者権限の委任は、ドメインコントローラーでの認証情報の盗難リスクを減らします。

8. セキュリティの豆知識

継続的な検証は、ログとセッションの挙動を監査し、異常なスクリプト実行パターンを示すユーザーを停止します。

9. セキュリティの豆知識

従来の境界防御では、管理者の認証情報が漏えいすると、横方向の攻撃を防げません。

10. セキュリティの洞察

NIST Special Publication 800-207（2020 年）は、導入モデルとともに、ゼロトラストアーキテクチャの抽象的な定義を示しています。 [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

解答: チェックポイント 1 – 多肢選択

1 問題 1

正解: A

指導メモ

ゼロトラストセキュリティの中心となる原則は何ですか? → 決して信頼せず、発信元にかかわらずすべてのアクセスリクエストを常に検証する

2 問題 2

正解: A

指導メモ

ネットワークのマイクロセグメンテーションとは何ですか? → ネットワークを小さな隔離ゾーンに分割し、横方向の移動を封じ込める

3 問題 3

正解: A

指導メモ

最小権限の原則とは何ですか? → ユーザーのアクセス権限を、業務に必要なものだけに制限する

4 問題 4

正解: A

指導メモ

ID・アクセス管理(IAM)とは何ですか? → デジタルIDを管理し、システム権限を制御するフレームワーク

5 問題 5

正解: A

指導メモ

継続的認証とはどういう意味ですか? → 有効なセッション中に、ユーザーの身元とデバイスの状態を繰り返し検証する

解答: チェックポイント 2 – 正誤問題

6 問題 6

正解: 誤り

指導メモ

誤り: ゼロトラストは、ネットワークの内側か外側かにかかわらず、位置に基づく暗黙の信頼を一切与えません。

7 問題 7

正解: 正しい

指導メモ

正しい: 小さく分離されたゾーンは、侵入者がサーバー間を移動できる範囲を制限します。

8 問題 8

正解: 誤り

指導メモ

誤り: 最小権限の原則では、各役割に必要な最小限のアクセスだけを付与します。

9 問題 9

正解: 正しい

指導メモ

継続的な検証では、ログインセッションの全体を通じて、デバイスの健全性と認証情報を検証します。

10 問題 10

正解: 正しい

指導メモ

ゼロトラストを導入すると、企業のログイン情報が侵害された場合の影響を抑えられます。

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. 検証	F 2. セグメンテーション	A 3. IAM	B 4. 権限
H 5. ポスチャ	E 6. 監査	D 7. ファイアウォール	C 8. ルーター

チェックポイント 3: 解答 – 重要用語

1 検証	2 セグメンテーション	3 IAM	4 最小権限
5 ポスチャ	6 監査		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 G – アクセス	2 F – カンサ	3 D – サイシヨウケンゲン	4 B – セグメンテーシヨン
5 H – キヨウカイ	6 E – ポスチヤ	7 C – アイアム	8 A – ケンシヨウ

指導者向けディスカッションメモ

重要用語:
生徒が検証、セグメンテーション、IAM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。

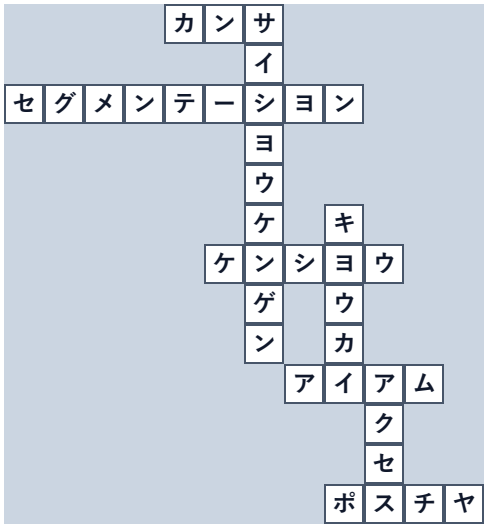
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: カンサ 記録されたアクセスセッションを見直すこと (3 文字)

3 ヨコ: セグメンテーションヨン 内部ネットワークをゾーンに分けること (9 文字)

5 ヨコ: ケンシヨウ ユーザーの認証情報を常に確認すること (5 文字)

6 ヨコ: アイアム ユーザーの認証情報とアクセスを管理すること (4 文字)

8 ヨコ: ポスチヤ デバイスの健全性の状態を評価すること (4 文字)

タテのカギ

2 タテ: サイショウケンゲン 必要最小限のアクセス権だけを与える原則 (9 文字)

4 タテ: キヨウカイ 外部ネットワークとの間に設けられる防御の線 (5 文字)

7 タテ: アクセス ユーザーがシステムや資源に接続して利用すること (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. ヨシケウン → **ケンシヨウ**
2. アアムイ → **アイアム**
3. ヤポチス → **ポスチヤ**
4. スセアク → **アクセス**
5. シテグンーンセヨメ → **セグメンテーシヨン**
6. ゲヨインケサウンシ → **サイシヨウケンゲン**
7. サンカ → **カンサ**
8. イキウカヨ → **キヨウカイ**

秘密の暗号チャレンジ 解答

"ゼロトラストデ ツネニ ケンショウスル"

ケーススタディの解答

A ケーススタディ 1: ゼロトラストネットワークアーキテクチャへの移行 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: 大企業が現在、ローカルネットワーク上のどのデバイスからでもすべての社内サーバーとデータベースにアクセスできる、フラットな社内ネットワークを使っています。
- 推奨される戦略と解決策: フラットなネットワークを、部門ごとに隔離されたゾーンに分割します。ゾーン間の通信を制御する内部ファイアウォールを設置し、すべてのアクセスに接続トークンの検証を義務付けます。

B ケーススタディ 2: 最小権限のアクセス制御の導入 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: 監査ログから、一時的なデータベースユーザーや下位の従業員が、重要な会計データベースに対する全体の読み取り権限と書き込み権限を持っていることがわかりました。
- 推奨される戦略と解決策: グローバルな管理者権限をすべて取り消します。職務に正確に合わせたロールベースアクセス制御 (RBAC) を導入し、毎週の自動化された権限レビューを確立します。