名前: 日付: 得点:

企業向けVPN

ゼロトラストネットワークアクセス、専用ゲートウェイノード、一元化された企業の管理者向け制御を導入すること。

企業向けVPNネットワーク 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、企業のVPNネットワークについて学びます。ゼロトラストアーキテクチャ、専用の固定IPゲートウェイ、管理者コンソール、プロビジョニング、サイト間IPsecトンネルを取り上げます。

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/best-vpn-for-business/enterprise/

あなたの企業VPNネットワーク 学習ロードマップ

- ゼロトラストネットワークアクセス (ZTNA) の枠組みを導入する。
- ホワイトリストフィルター用に、専用サーバーのゲートウェイ IP アドレスを設定してください。
- 一元化された企業向けの管理パネルとユーザーのシート一覧を管理する。
- ネットワークアクセスログとユーザーの接続履歴を監査します。
- シングルサインオン (SSO) と多要素認証のルールを設定してください。
- 拠点間の IPsec トンネルを設定します。

企業向けVPNネットワーク手順

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とサイト間IPsec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専用ゲートウェイ（入門）

企業向けVPNは、ゼロトラストネットワークアクセス(ZTNA)フレームワークへの移行と、専用の固定IPゲートウェイのホワイトリスト化によって、社内の資産を守ります。IT管理者は、集中管理コンソールを使って、拠点間IPsecトンネルとシングルサインオン(SSO)の連携を調整します。

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. 従来の企業向けVPNに代わりつつあるセキュリティモデルは何ですか?
   - A) ゼロトラスト
   - B) マルチホップ
   - C) ピアツーピア
   - D) 単一のゲートウェイ

2. データベースへのアクセスを会社のサーバーのみに制限するために必要な機能は何ですか?
   - A) 専用IP
   - B) 動的ルーティング
   - C) スプリットトンネル
   - D) DNS プロキシ

3. 企業の拠点間トンネルの標準となっているプロトコルはどれですか?
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. 管理者が従業員のシート数を管理できる中央ツールは何ですか?
   - A) 管理コンソール
   - B) レジストリキー
   - C) ルーターのファームウェア
   - D) システムログ

5. OktaやMicrosoft Entra IDでのログインを可能にする認証規格はどれですか？
   - A) シングルサインオン
   - B) 共有シークレット
   - C) EPP認証
   - D) WEPキー

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. ゼロトラストネットワークアクセスは、機器への信頼を継続的に検証した後にのみ、ネットワークへの接続を許可します。

○ 正しい ○ 誤り

7 質問 7

7. 専用IPゲートウェイは、従業員のトラフィックを、不特定多数の一般ユーザーのトラフィックと同じ経路で送ります。

○ 正しい ○ 誤り

8 質問 8

8. 一元管理型の管理者コンソールにより、IT 管理者は従業員個々のライセンス枠を即座に取り消せます。

○ 正しい ○ 誤り

9 質問 9

9. IPsec は軽量なプロトコルで、拠点間のネットワークトンネルには対応していません。

○ 正しい ○ 誤り

10 質問 10

10. シングルサインオンは、会社の ID プロバイダーを使った、安全な従業員認証を可能にします。

○ 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. 最新のセキュリティアーキテクチャでは、従来型のトンネルが _____ アクセスに置き換えられています。

2. データベースへのアクセスを制限するため、企業は _____ ゲートウェイアドレスを設定します。

3. 支社は、拠点間の _____ トンネルで安全に接続されます。

4. IT管理者は、一元化された _____ 内で従業員のユーザーライセンスを割り当てます。

5. Oktaとの連携により、従業員は企業の _____ で認証できます。

6. ログインを保護するため、企業向けポータルでは _____ が必須とされています。

用語バンク

IPsec　ゲートウェイ　シングルサインオン　ゼロトラスト　プロビジョニング
管理コンソール　専用IP　多要素認証

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: 重要概念のマッチング

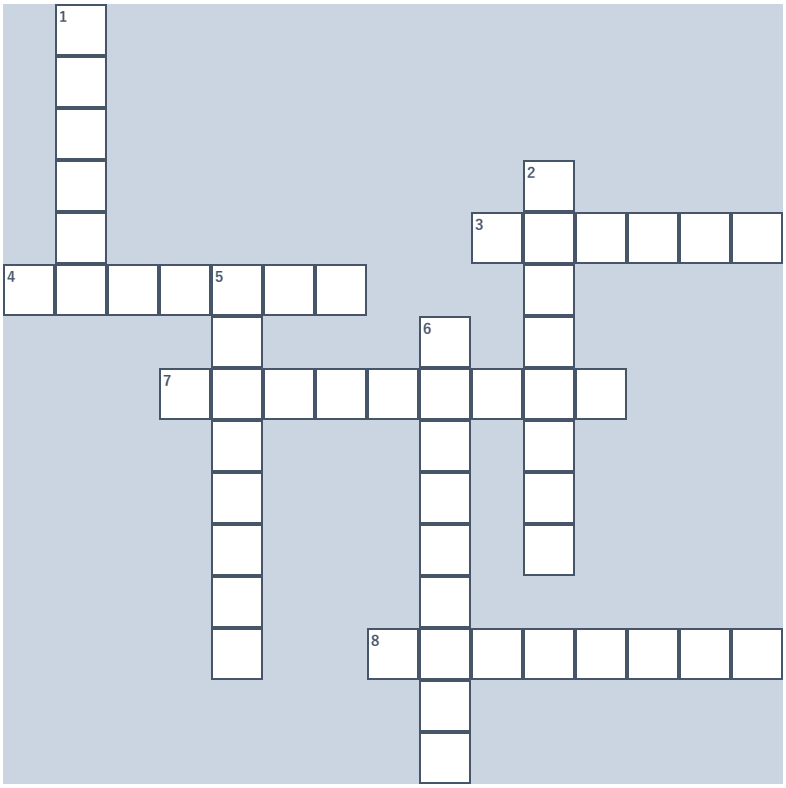
定義マッチング

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. ゼロトラスト	A	従業員のVPNアクセスライセンスの割り当て。
	2. 専用IP	B	OktaとEntra IDのID連携。
	3. IPSEC	C	追加のトークンを必要とするログインセキュリティ。
	4. 管理コンソール	D	固定のホワイトリストのゲートウェイアドレス。
	5. シングルサインオン	E	拠点間トンネルの標準規格。
	6. 多要素	F	ネットワークの入口となるルーティングノード。
	7. ゲートウェイ	G	IT 管理者向けの中央席管理ポータル。
	8. プロビジョニング	H	継続的に信頼を検証するフレームワーク。

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

3. 信頼性を継続的に検証する枠組み (6)

4. 拠点間トンネルの標準規格 (7)

7. 追加のトークンを必要とするログインのセキュリティ (9)

8. IT管理者が席(ライセンス)を一元管理するポータル (8)

タテのカギ

1. ネットワークの入口となる経路制御ノード (6)

2. 従業員にVPNアクセスのライセンスを割り当てること (8)

5. ホワイトリスト登録用の固定ゲートウェイアドレス (8)

6. OktaやEntra IDとのID連携 (9)

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: 信頼性を継続的に検証する枠組み (6 文字):

4 ヨコ: 拠点間トンネルの標準規格 (7 文字):

7 ヨコ: 追加のトークンを必要とするログインのセキュリティ (9 文字):

8 ヨコ: IT管理者が席(ライセンス)を一元管理するポータル (8 文字):

タテのカギ

1 タテ: ネットワークの入口となる経路制御ノード (6 文字):

2 タテ: 従業員にVPNアクセスのライセンスを割り当てること (8 文字):

5 タテ: ホワイトリスト登録用の固定ゲートウェイアドレス (8 文字):

6 タテ: OktaやEntra IDとのID連携 (9 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 ロ ト ボ タ レ ミ プ ク グ ヌ チ ユ ガ メ
ロ ボ ス ワ ラ キ ゼ ロ ゴ ザ ア ス ホ ノ オ
ア オ ラ キ ル パ ホ ビ ヒ パ イ ヘ ボ ズ フ
ウ サ ト ン メ ハ コ ジ ヌ ヤ ピ モ ヘ ワ レ
ヨ テ ロ モ モ シ ン ヨ ギ ゲ ー ズ ジ セ ツ
シ カ ゼ ゴ ワ ン ラ ニ ニ グ セ カ バ ン コ
ン ザ ペ ダ キ グ ポ ン カ バ ツ タ フ ヨ ト
ニ ー コ モ サ ル ガ グ ン ベ ク レ カ ウ ゾ
ソ エ ア ー ユ サ コ ヘ リ イ サ ラ イ ア サ
ウ ソ テ ヌ コ イ ギ ン コ メ ス エ ヌ イ グ
ヨ ポ ゴ ソ ガ ン ド セ ン イ ウ イ ガ ピ リ
タ ヤ レ ズ ボ オ ワ ヒ ソ ト グ ゼ ゲ ー ケ
ヤ プ オ タ グ ン ベ ブ ー ノ イ ギ ー ピ ピ
マ ツ ヌ メ ガ ヒ ム ゲ ル ミ ジ リ ト ロ ン
テ ー ウ ラ デ チ ダ カ プ グ プ オ ト ミ ー

用語リスト

ゼロトラスト　センヨウアイピー　アイピーセツク　カンリコンソール　シングルサインオン
タヨウソニンショウ　ゲートウエイ　プロビジョニング

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	定義とマッチ欄
A. ゼロトラスト	1. ホワイトリスト登録用の固定ゲートウェイアドレス。
B. センヨウアイピー	2. ネットワークの入口となる経路制御ノード。
C. アイピーセツク	3. 従業員にVPNアクセスのライセンスを割り当てること。
D. カンリコンソール	4. 追加のトークンを必要とするログインのセキュリティ。
E. シングルサインオン	5. 拠点間トンネルの標準規格。
F. タヨウソニンシヨウ	6. 信頼性を継続的に検証する枠組み。
G. ゲートウエイ	7. OktaやEntra IDとのID連携。
H. プロビジヨニング	8. IT管理者が席(ライセンス)を一元管理するポータル。

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、このワークシートの重要な概念を見つけましょう。答えは用意された入力欄に書いてください。

1. トゼラストロ
2. アピクツセーイ
3. シイサンンンルオグ
4. イウトエゲー
5. アインーウセピヨ
6. ールコソカンンリ
7. ンタヨウシソヨニウ
8. ジロヨグプンニビ

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	会社が毎日使うツール			
2	VPNが隠せるもの			
3	IT部門の役割			
4	ゼロトラストを表す言葉			
5	安全にログインする方法			
6	従業員にVPNを提供する理由			
7	セキュリティ侵害の後にすること			
8	旅行中にVPNを使う理由			
9	安全なリモートワークのルール			
10	会社が守らなければならないデータ			
11	ビデオ会議の妨げになるもの			
12	VPNを使えるデバイス			
13	知っているオフィスソフト			
14	従業員が働く場所			
15	従業員が持っているかもしれないデバイス			

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: ゼロトラストへの移行

👷

シナリオ: ある企業が、ネットワーク内にいる人を信頼するのではなく、デバイスのコンプライアンス証明書、ファイアウォールの状態、ユーザーの所在地を継続的に検証して、社内サーバーを保護したいと考えています。

ディスカッションの問い: ITセキュリティ責任者は、これを実現するために、どのフレームワークを導入するべきですか？

ケーススタディ 2: ゲートウェイの制限

👷

シナリオ: ある企業が、機密性の高い財務データベースをクラウド上でホストしています。管理パネルへの公開インターネットからのアクセスはすべてブロックし、検証済みの社内エンドポイントからのログインのみを許可したいと考えています。

ディスカッションの問い: データベース管理者は、クラウドのファイアウォールでどのようなネットワーク設定を行うべきですか？

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

55	43	20	39	13	20	26		13	65	19	25		7	7	45

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: 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: エンタープライズ VPN とは何ですか?

リモートワーカーが一元管理のもとで社内ネットワークにアクセスできるようにする、企業向けの安全なネットワークトンネル。

Q2: ゼロトラストは従来の VPN とどう違いますか?

従来のVPNはトンネル内の全員を信頼しますが、ゼロトラストはすべてのデバイスとユーザーの接続を継続的に検証します。

Q3: ビジネス向け VPN の専用 IP とは何ですか?

自社専用に確保された固定IPアドレスで、安全なクラウドデータベースへのアクセス用にホワイトリストに登録できます。

Q4: ビジネス向け VPN で SSO が重要なのはなぜですか?

シングルサインオンを使うと、従業員は会社の認証情報 (Okta や Microsoft Entra ID など) で安全にログインできます。

Q5: サイト間 VPN とは何ですか?

IPsecを使い、公共のインターネット越しに2つの物理的なオフィス(支社と本社など)を結ぶトンネル。

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: 管理コンソールの機能は何ですか?

IT管理者が従業員のシートを追加・削除し、ゲートウェイを割り当て、アクティブな接続を監視するためのダッシュボード。

Q7: MFA はビジネス向け VPN をどう守りますか?

認証アプリのトークンのような第2のコードを要求し、漏えいしたパスワードによる不正な侵入を防ぐことによって。

Q8: 従業員の接続履歴を監査できますか?

はい、企業向けVPNでは、コンプライアンス監査のために接続時刻、接続時間、割り当てられたIPが記録されます。

Q9: ZTNA とは何ですか?

ゼロトラストネットワークアクセスは、ネットワーク全体ではなく特定のアプリケーションにのみアクセスを許可するセキュリティモデルです。

Q10: ゲートウェイノードの役割は何ですか?

リモートからの通信の安全な入口として機能し、データをプライベートな社内サーバーに直接ルーティングします。

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: IPsec は、拠点間の企業通信をどのように保護しますか?

IPsec は、カプセル化セキュリティペイロード (ESP) を使ってネットワーク層で通信を暗号化し、データの機密性と完全性を確保します。

Q2: 従来の境界型セキュリティがリモートワーカーに対して機能しなくなっているのはなぜですか?

従業員が複数の場所やデバイスからデータにアクセスするため、単一のネットワークファイアウォールによる境界防御は時代遅れになっているためです。

Q3: IT 管理者は自動プロビジョニングをどのように実装しますか?

アイデンティティプロバイダー（Okta）とVPN管理コンソールの間でSCIMプロトコルをマッピングし、ユーザーディレクトリを同期することによって。

Q4: 企業環境でスプリットトンネリングを使う利点は何ですか?

ローカルの SaaS の通信(Microsoft 365 など)を VPN トンネルの外でルーティングし、企業ゲートウェイの帯域幅をプライベートなデータベースのために確保します。

Q5: デバイスポスチャチェックはエンドポイントのセキュリティをどう検証しますか?

このVPNクライアントは、接続前にデバイスをスキャンし、ファイアウォールが有効か、ウイルス対策ソフトが動作しているか、OSのパッチが最新かを確認します。

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: ビジネス向け VPN の構成において NAT トラバーサルはどのような役割を果たしますか?

NAT-T は IPsec パケットを UDP にカプセル化して、接続を切らさずに家庭用ルーターやファイアウォールを通過できるようにします。

Q7: 企業はゲートウェイの帯域幅の詰まりをどう防ぎますか?

複数のリージョンのゲートウェイノードを配置し、ロードバランサーを使って受信するユーザートラフィックを分散することによって。

Q8: 動的な許可リストより静的 IP の許可リストが好まれるのはなぜですか?

固定のホワイトリストは、許可されていない外部 IP が接続ハンドシェイクを試みるのを防ぎ、攻撃対象領域を大幅に減らします。

Q9: 企業向け VPN における証明書ベースの認証の役割は何ですか?

会社が管理するデバイスにインストールされた固有のデジタル証明書を検証し、管理されていない個人のコンピューターを遮断します。

Q10: ZTNA は横方向への移動のリスクをどのように減らしますか?

ユーザーのセッションを特定の許可されたリソースに分離し、1つのノードが侵害されてもハッカーがネットワーク内を移動できないようにすることによって。

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

ゼロトラストアーキテクチャは、ネットワークに接続しようとするすべての機器のセキュリティ状態を継続的に検証します。

2. VPN の洞察

専用IPゲートウェイを使うと、企業は固定アドレスをホワイトリスト化してクラウドデータベースを保護できます。

3. VPN の洞察

IPsec は、安全な拠点間のオフィスネットワークトンネルを設定するための業界標準プロトコルです。

4. VPN の洞察

管理コンソールでは、IT部門が従業員のVPNアクセスシートを割り当て、管理し、監査できます。

5. VPN の洞察

シングルサインオンは、VPN アクセスを Okta や Entra ID などの会社の ID プロバイダーと統合します。

6. VPN の洞察

多要素認証は、盗まれたパスワードキーによる不正な接続の試みをブロックします。

7. VPNの豆知識

スプリットトンネリングは、公開 SaaS の通信を暗号化トンネルから除外することで、社内の帯域を最適化します。

8. VPNの豆知識

デバイスの状態チェックは、企業のサーバーへのアクセスを許可する前に、ローカルのセキュリティ設定を確認します。

9. VPNの豆知識

SCIM のディレクトリ同期は、従業員の入社時と退社時のアクセス制御を自動化します。

10. VPN の洞察

ゼロトラストネットワークアクセスは、ユーザーのアクセスを許可された特定のアプリケーションに限定し、ネットワーク内での横方向の移動を防ぎます。

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] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

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

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

解答: チェックポイント 1 – 多肢選択

1 ゼロトラスト　ZTNAモデル　正解: A

指導メモ

ゼロトラストモデルは、ネットワークへの接続を許可する前に、機器のコンプライアンスを継続的に検証します。出典: NIST Zero Trust。

2 専用IP　固定 IP　正解: A

指導メモ

専用IPアドレスを使うと、ゲートウェイをホワイトリスト化して公共のトラフィックをブロックできます。出典: Dedicated IP Guide。

3 IPsec 標準　IPSEC トンネル　正解: A

指導メモ

IPsec は、支社の拠点間トンネルに使われる標準プロトコルです。出典: IPsec Tunneling。

4 IT の割り当て　管理コンソール　正解: A

指導メモ

一元管理型の管理者ダッシュボードにより、IT 管理者はシートライセンスを割り当てられます。出典: CISA Guidelines。

5 問題 5　正解: A

指導メモ

OktaやMicrosoft Entra IDでのログインを可能にする認証規格はどれですか？ → シングルサインオン

解答: チェックポイント 2 – 正誤問題

6 **ゼロトラスト** ZTNAチェック 正解: 正しい

指導メモ

ゼロトラストモデルは、ネットワークへの接続を許可する前に、機器のコンプライアンスを継続的に検証します。出典: NIST Zero Trust。

7 **問題 7** 正解: 誤り

指導メモ

専用IPは1つの企業のために確保されるため、その通信は他のユーザーの通信と混ざりません。

8 **IT の割り当て** IT 管理者席 正解: 正しい

指導メモ

一元管理型の管理者ダッシュボードにより、IT 管理者はシートライセンスを割り当てられます。出典: CISA Guidelines。

9 **IPsec 標準** サイト間 正解: 誤り

指導メモ

IPsec は、支社の拠点間トンネルに使われる標準プロトコルです。出典: IPsec Tunneling。

10 **Okta SSO リンク** SSO ログイン 正解: 正しい

指導メモ

シングルサインオンは、VPN ログインを Okta などの会社のディレクトリと統合します。出典: Okta SSO。

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. ゼロトラスト	D 2. 専用IP	E 3. IPSEC	G 4. 管理コンソール
B 5. シングルサインオン	C 6. 多要素	F 7. ゲートウェイ	A 8. プロビジョニング

チェックポイント 3: 解答 – 重要用語

1 ゼロトラスト	2 専用IP	3 IPsec	4 管理コンソール
5 シングルサインオン	6 多要素認証		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 B – センヨウアイピー	2 G – ゲートウエイ	3 H – プロビジヨニング	4 F – タヨウソニンショウ
5 C – アイピーセツク	6 A – ゼロトラスト	7 E – シングルサインオン	8 D – カンリコンソール

指導者向けディスカッションメモ

重要用語:
生徒がゼロトラスト、専用IP、IPSEC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。

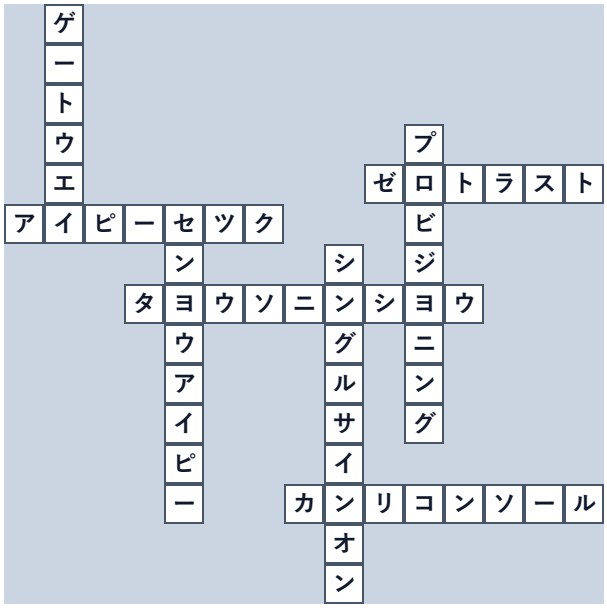
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: ゼロトラスト 信頼性を継続的に検証する枠組み (6 文字)

4 ヨコ: アイピーセツク 拠点間トンネルの標準規格 (7 文字)

7 ヨコ: タヨウソニンシヨウ 追加のトークンを必要とするログインのセキュリティ (9 文字)

8 ヨコ: カンリコンソール IT管理者が席(ライセンス)を一元管理するポータル (8 文字)

タテのカギ

1 タテ: ゲートウエイ ネットワークの入口となる経路制御ノード (6 文字)

2 タテ: プロビジヨニング 従業員にVPNアクセスのライセンスを割り当てること (8 文字)

5 タテ: センヨウアイピー ホワイトリスト登録用の固定ゲートウェイアドレス (8 文字)

6 タテ: シングルサインオン OktaやEntra IDとのID連携 (9 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. トゼラストロ — **ゼロトラスト**
2. アピクツセーイ — **アイピーセツク**
3. シイサンンンルオグ — **シングルサインオン**
4. イウトエゲー — **ゲートウエイ**
5. アインーウセピヨ — **センヨウアイピー**
6. ールコソカンンリ — **カンリコンソール**
7. ンタヨウシソヨニウ — **タヨウソニンシヨウ**
8. ジロヨグプンニビ — **プロビジヨニング**

秘密の暗号チャレンジ 解答

"ゼロトラストハ スベテノ キキヲ 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: ある企業が、ネットワーク内の誰もを信頼するのではなく、デバイスのコンプライアンス証明書、ファイアウォールの状態、ユーザーの所在地を継続的に検証して、ローカルサーバーを保護したいと考えています。
- 推奨される戦略と解決策: 部門長は、コンテキストに基づくセキュリティチェックを継続的に実施するゼロトラストネットワークアクセス (ZTNA) モデルに移行するべきです。

B ケーススタディ 2: ゲートウェイの制限

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: ある企業が、非公開の財務データベースをクラウドでホストしています。管理パネルへのすべての公開インターネットからのアクセスをブロックし、検証済みの社内エンドポイントからのログインのみを許可したいと考えています。
- 推奨される戦略と解決策: 管理者は、企業向け VPN に専用 IP ゲートウェイを設定し、この固定アドレスをクラウドデータベースのファイアウォールで許可リストに登録するべきです。