名前: 日付: 得点:

ビジネスにおすすめのVPN

ビジネス向けVPNのセキュリティ、拡張性、集中管理の実機レビュー。

ビジネス向けおすすめ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、ビジネスVPNとリモートアクセス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、IPsecのサイト間トンネル、SASEフレームワーク、多要素ログイン、エンドポイントのセキュリティチェックを取り上げます。

ワークシートのチェックポイント

- [ ] **パート 1-4: 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/

あなたのビジネスVPN 学習ロードマップ

- 主要なビジネス向け VPN プロバイダーと、そのチーム向けの機能を見分ける。
- 消費者向けVPNのプライバシーと、ビジネス向け管理コントロールの違いを分析してください。
- リモートアクセスVPNと拠点間の企業向けトンネルの違いを説明します。

ビジネスVPNガイドの指示

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。学んだ知識を企業のリモートアクセス構成に応用しましょう。 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。

企業のリモートアクセスと安全なエッジ(入門)

企業のリモートアクセスを保護するには、従来の境界型 VPN モデルから、ゼロトラストアーキテクチャへ移行する必要があります。強力な多要素認証 (MFA) と Secure Access Service Edge (SASE) のフレームワークを適用することで、侵害されたエンドポイントから重要な資産を守ります。

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. オフィスのネットワーク全体を相互に接続する、ビジネス向けVPNの種類はどれですか?
   - A. サイト間VPN
   - B. リモートアクセスVPN
   - C. コンシューマー向けVPN
   - D. スマート DNS

2. 2. ビジネスチームに総合的に最適な選択肢として紹介されているのはどれですか?
   - A. NordLayer
   - B. Surfshark
   - C. Proton VPN
   - D. Private Internet Access

3. 3. 専用の固定IPアドレスは、企業チームにとって何を防ぎますか?
   - A. IPアドレスのブラックリスト登録
   - B. ルーターの速度が低下する
   - C. データ圧縮
   - D. クライアントの更新

4. 4. 専用インフラに最適として紹介されているプロバイダーはどれですか?
   - A. Proton VPN
   - B. NordLayer
   - C. Surfshark
   - D. Private Internet Access

5. 5. ユーザーを管理する一元化された管理者ダッシュボードを提供する機能は何ですか?
   - A. 管理者向けコントロール
   - B. ポートフォワーディング
   - C. ルーターのエミュレーション
   - D. スプリットトンネリング

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. リモートアクセス VPN を使うと、個々の従業員がどこからでも接続できます。

○ 正しい ○ 誤り

7 質問 7

7. 個人向け VPN は、1 つの管理パネルで組織全体を保護する。

○ 正しい ○ 誤り

8 質問 8

8. 専用IPアドレスは、会社のトラフィックを公共のトラフィックから分離します。

○ 正しい ○ 誤り

9 質問 9

9. Private Internet Access は、大企業に最適として紹介されています。

○ 正しい ○ 誤り

10 質問 10

10. SASE は、WAN のルーティングとクラウド提供のセキュリティフレームワークを統合します。

○ 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. ビジネスチーム向けの総合1位のプロバイダーは _____ です。
2. 複数の企業拠点を相互に接続するには _____ を使います。
3. アドレスのブラックリスト入りを避けるため、チームは _____ を導入します。
4. 管理者は、中央の _____ を使ってデバイスの権限を管理します。
5. チームの成長に合わせて席数を動的に追加できることを _____ といいます。
6. 規制やデータ監査の基準を満たすには _____ が必要です。

用語バンク

NordLayer　ゲートウェイ　コンプライアンス　サイト間　ダッシュボード　拡張性　拠点間接続　固定IP

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

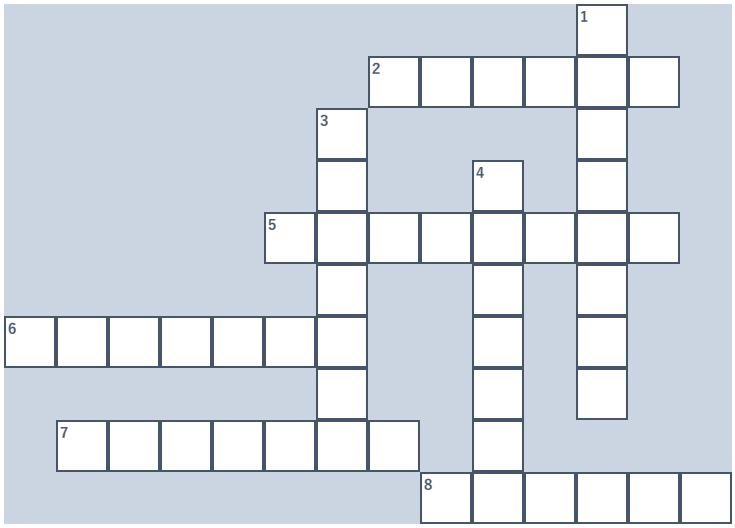
定義マッチング

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. NordLayer	A	席数を柔軟に増やせる、チームの拡大。
☐	2. サイト間	B	ビジネス向けの総合おすすめ。
☐	3. 固定 IP	C	スプリットトンネリングによる通信制御。
☐	4. ダッシュボード	D	規制当局による標準的な監査。
☐	5. 拡張性	E	認証用のリモート入口ノード。
☐	6. コンプライアンス	F	ブラックリストに載っていない専用アドレス。
☐	7. ルーティング	G	オフィスネットワーク間を接続するトンネル。
☐	8. ゲートウェイ	H	中央の管理者用コントロールコンソール。

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. スプリットトンネリングでの通信制御 (6)

5. オフィスのネットワーク同士を結ぶトンネル (8)

6. チームの規模に合わせて席数を柔軟に増やせること (7)

7. 管理者向けの中央管理コンソール (7)

8. 認証を行うリモート接続の入口ノード (6)

タテのカギ

1. 規制や監査の基準を満たすこと (8)

3. ブラックリストに載っていない専用アドレス (7)

4. 総合的に最も優れたビジネス向けの選択肢 (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

2 ヨコ: スプリットトンネリングでの通信制御 (6 文字):

5 ヨコ: オフィスのネットワーク同士を結ぶトンネル (8 文字):

6 ヨコ: チームの規模に合わせて席数を柔軟に増やせること (7 文字):

7 ヨコ: 管理者向けの中央管理コンソール (7 文字):

8 ヨコ: 認証を行うリモート接続の入口ノード (6 文字):

タテのカギ

1 タテ: 規制や監査の基準を満たすこと (8 文字):

3 タテ: ブラックリストに載っていない専用アドレス (7 文字):

4 タテ: 総合的に最も優れたビジネス向けの選択肢 (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。

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

用語リスト

ノードレイヤー　サイトツーサイト　コテイアイピー　ダツシユボード　カクチヨウセイ
コンプライアンス　ルーテイング　ゲートウエイ

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. ノードレイヤー
B. サイトツーサイト
C. コテイアイピー
D. ダツシユボード
E. カクチヨウセイ
F. コンプライアンス
G. ルーテイング
H. ゲートウエイ

定義とマッチ欄
1. スプリットトンネリングでの通信制御。
2. 管理者向けの中央管理コンソール。
3. 認証を行うリモート接続の入口ノード。
4. ブラックリストに載っていない専用アドレス。
5. 規制や監査の基準を満たすこと。
6. オフィスのネットワーク同士を結ぶトンネル。
7. 総合的に最も優れたビジネス向けの選択肢。
8. チームの規模に合わせて席数を柔軟に増やせること。

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、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. レヤノイードー
2. コイーピイアテ
3. ヨカウイチセク
4. グイテンルー
5. ーサイトツサイト
6. ーシボダユドツ
7. コスイアンンラプ
8. トイゲエウー

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	優れたVPNプロバイダーが約束すること			
2	ビデオ会議の妨げになるもの			
3	安全なリモートワークのルール			
4	知っているオフィスソフト			
5	インターネットプロバイダーが見られるもの			
6	従業員にVPNを提供する理由			
7	VPNでは守れないもの			
8	従業員が働く場所			
9	会社が毎日使うツール			
10	安全にログインする方法			
11	会社が守らなければならないデータ			
12	IT部門の役割			
13	従業員が持っているかもしれないデバイス			
14	セキュリティ侵害の後にすること			
15	ゼロトラストを表す言葉			

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: 共有パブリック IP のブラックリスト登録



シナリオ: 営業チームが、コンシューマー向けのVPNを使って社内データベースにアクセスしていますが、共有の出口IPが不正検知システムのブラックリストに登録されたため、ロックアウトされています。

ディスカッションの問い: このロックアウトを解消するための、ビジネス向けVPNのインフラ構成を提案できますか？

ケーススタディ 2: 企業オフィス間の相互接続



シナリオ: ミュンヘンとボストンにオフィスを持つ企業が、公共のウェブ空間を経由せずに、社内のファイルサーバーを安全に共有する必要があります。

ディスカッションの問い: 適切なビジネス向けVPNのトポロジーを選んでください。

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	60		7	48	38	3	25		24	18	20	44	72	8	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（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: ビジネス VPN とは何ですか?

リモートスタッフやオフィスが、社内のプライベートデータに安全にアクセスできるようにする、安全なネットワーク接続。

Q2: 個人向け VPN と法人向け VPN はどう違いますか?

個人向け VPN は個人の閲覧を隠し、法人向け VPN は中央の管理者コンソールで企業システムを守ります。

Q3: サイト間 VPN とは何ですか?

ウェブ経由でオフィスのネットワーク全体を互いに結ぶトンネル。

Q4: リモートアクセス VPN とは何ですか?

個々のリモート従業員が会社のネットワークに安全に接続できるようにするトンネル。

Q5: 専用の固定 IP の利点は何ですか?

企業の通信を公開プールから分離し、共有 IP のブラックリスト登録を避けられます。

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: 小規模企業に最適なプロバイダーはどれですか?

Private Internet Access（PIA）は、小規模チームでも手頃な価格で、設定が簡単なことで知られています。

Q7: 総合1位のビジネス向け VPN はどれですか?

NordLayer は、機能と管理ツールで VPN.com から 92/100 の評価を受けました。

Q8: VPN におけるチームのスケーラビリティとは何ですか?

企業の成長に合わせて、ユーザー席数、ライセンス、ゲートウェイを動的に追加できる機能。

Q9: 一元管理が重要なのはなぜですか?

管理者は、1 つのダッシュボードでセキュリティポリシーを適用し、従業員のアクセスを取り消せます。

Q10: SASE とは何ですか?

WAN ルーティングとクラウド提供のセキュリティサービスを統合する Secure Access Service Edge。

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: スプリットトンネリングは、チームをどのように保護しますか?

プライベートな SaaS の通信は安全なトンネル内に保ちつつ、公開ウェブへのアクセスはローカルでルーティングします。

Q2: Proton VPN は法人向けに何を提供していますか?

専用サーバーインフラ、VPN.comによる評価は88/100(スイス拠点)。

Q3: どのコンプライアンス基準が VPN を求めていますか?

PCI DSS は公衆ネットワーク上での強力な暗号化を求めており、HIPAA と GDPR も保護措置として暗号化を期待しています。

Q4: ビジネス向け VPN をルーターで実行できますか?

はい、ルーターにVPNトンネルを設定すると、オフィスのすべての機器が自動的に保護されます。

Q5: 多要素認証とは何ですか?

ログインの認証に、複数の認証情報（スマートカードや SMS コードなど）を求めること。

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: 共有 IP アドレスがブロックリストに載るのはなぜですか?

数千人のユーザーが共有しており、その中には悪意のある行為をする人がいるかもしれないためです。

Q7: ゲートウェイはユーザーをどう認証しますか?

アクティブディレクトリに対してクライアント証明書、パスワード、多要素コードを検証することによって。

Q8: Surfshark はチームに何を提供していますか?

VPN.comがセキュリティバンドルで最もおすすめするサービスで、84/100点、RAMのみのサーバーを採用しています。

Q9: ビジネス向け VPN の接続をどう監査しますか?

管理コンソールで接続ログ、データ使用量の指標、ログイン履歴を調べることによって。

Q10: ゼロトラストのアクセス制御とは何ですか?

すべてのデバイスを信頼できないものとみなし、セッションごとに検証を求める考え方。

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

ビジネスVPNは通信を暗号化し、公共ネットワークでのスニッフィングから社内システムを守ります。

2. VPN の洞察

サイト間 VPN は、ローカルホストを公開せずに、支社のネットワーク全体を安全につなぎます。

3. VPN の洞察

個人向け VPN は個人の閲覧を隠し、法人向け VPN は企業のリソースゲートウェイを守ります。

4. VPN の洞察

VPN.comはNordLayerに92/100点を付けており、総合的に最高のビジネス向けVPNです。

5. VPN の洞察

VPN.comはProton VPNに88/100点を付け、専用インフラに最適としています。

6. VPN の洞察

VPN.comはPrivate Internet Accessに76/100点を付け、小規模ビジネスチームに最適としています。

7. VPNの豆知識

中央の管理者用ダッシュボードにより、セキュリティ担当者はユーザーの権限とアクセスルールを管理できます。

8. VPNの豆知識

専用の固定IPアドレスがあれば、IPを共有する不正検知システムによってチームがブロックされるのを防げます。

9. VPNの豆知識

GDPR は、個人データを保護するための適切な措置として暗号化を挙げています。

10. VPN の洞察

ゼロトラストアーキテクチャは、場所や認証情報にかかわらず、すべてのリモートエンドポイントを検証します。

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 トンネルのトポロジー サイト間 正解: A

指導メモ

サイト間 VPN は、離れた支社のオフィス全体を互いに安全に接続します。出典: NIST Zero Trust。

2 問題 2 正解: A

指導メモ

VPN.comはNordLayerに100点満点中92点を付け、企業チーム向けの総合1位としています。

3 IP ホワイトリスト 専用IP 正解: A

指導メモ

専用の固定IPがあれば、共有IPのブラックリストが原因でチームが締め出されるのを防げます。出典: NIST Remote Access。

4 問題 4 正解: A

指導メモ

VPN.comはProton VPNに100点満点中88点を付け、専用インフラ向けの1位としています。

5 中央コンソール 管理者向けコントロール 正解: A

指導メモ

一元管理型のパネルにより、セキュリティ担当者はユーザーの権限とライセンス枠を管理できます。出典: NIST Remote Access。

解答: チェックポイント 2 – 正誤問題

6 **リモート接続** リモートアクセス 正解: 正しい

指導メモ

リモートアクセス VPN を使うと、個々のリモートワーカーがプライベートサーバーに接続できます。出典: NIST Remote Access。

7 **企業向けトンネル** 個人向けプランの上限 正解: 誤り

指導メモ

個人向け VPN には一元管理の管理機能がなく、組織の監査には適していません。出典: CISA Infrastructure。

8 **ゲートウェイの隔離** 専用トンネル 正解: 正しい

指導メモ

専用IPは、会社のトラフィックを公共の雑多なトラフィックから分離して、データベースを守ります。出典: NIST Zero Trust。

9 **問題 9** 正解: 誤り

指導メモ

VPN.comはPIA（100点満点中76点）を、大企業向けではなく小規模ビジネス向けの1位としています。

10 **セキュリティの統合** SASE 標準 正解: 正しい

指導メモ

SASE は、企業の WAN ルーティングと、クラウド提供のゼロトラストセキュリティを統合します。出典: Cloudflare Zero Trust。

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

B 1. NordLayer	G 2. サイト間	F 3. 固定 IP	H 4. ダッシュボード
A 5. 拡張性	D 6. コンプライアンス	C 7. ルーティング	E 8. ゲートウェイ

チェックポイント 3: 解答 – 重要用語

1 NordLayer	2 拠点間接続	3 固定IP	4 ダッシュボード
5 拡張性	6 コンプライアンス		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 G – ルーテイング	2 D – ダツシユボード	3 H – ゲートウエイ	4 C – コテイアイピー
5 F – コンプライアンス	6 B – サイトツーサイト	7 A – ノードレイヤー	8 E – カクチヨウセイ

指導者向けディスカッションメモ

重要用語:
生徒がNordLayer、サイト間、固定 IP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。

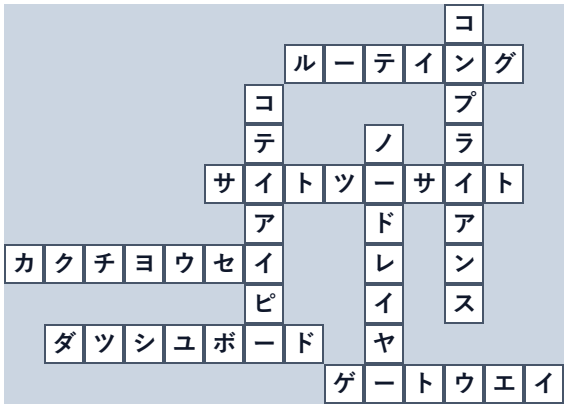
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: ルーテイング スプリットトンネリングでの通信制御 (6 文字)

5 ヨコ: サイトツーサイト オフィスのネットワーク同士を結ぶトンネル (8 文字)

6 ヨコ: カクチヨウセイ チームの規模に合わせて席数を柔軟に増やせること (7 文字)

7 ヨコ: ダツシユボード 管理者向けの中央管理コンソール (7 文字)

8 ヨコ: ゲートウエイ 認証を行うリモート接続の入口ノード (6 文字)

タテのカギ

1 タテ: コンプライアンス 規制や監査の基準を満たすこと (8 文字)

3 タテ: コテイアイピー ブラックリストに載っていない専用アドレス (7 文字)

4 タテ: ノードレイヤー 総合的に最も優れたビジネス向けの選択肢 (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. レヤノイードー → **ノードレイヤー**
2. コイーピイアテ → **コテイアイピー**
3. ヨカウイチセク → **カクチヨウセイ**
4. グイテンルー → **ルーテイング**
5. ーサイトツサイト → **サイトツーサイト**
6. ーシボダユドツ → **ダツシユボード**
7. コスイアンンラプ → **コンプライアンス**
8. トイゲエウー → **ゲートウエイ**

秘密の暗号チャレンジ 解答

"ゼロトラストデ キギョウノ ネットワークヲ マモル"

ケーススタディの解答

A ケーススタディ 1: 共有パブリック IP のブラックリスト登録 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: 営業チームが一般向けの VPN を使って社内データベースにアクセスしていますが、共有の出口 IP が不正検知システムによってブラックリストに登録されたため、ログインできなくなります。
- 推奨される対策と解決策: 公共のプールから社内トラフィックを分離するために、固定 IP アドレスと組み合わせた専用のビジネス向けサーバーを展開します。

B ケーススタディ 2: 企業オフィス間の相互接続 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: ミュンヘンとボストンにオフィスを持つ企業が、公開Webスペースを経由せずに、ローカルのファイルサーバーを安全に共有する必要があります。
- 推奨される対策と解決策: 2つの拠点ネットワークをインターネット経由で安全に相互接続するために、サイト間 VPN トンネルを構成します。