名前: 日付: 得点:

データ保護と企業ストレージ セキュリティガイド

データマスキング、トークン化、保存時と転送時の暗号化、オフラインバックアップ

データ保護の学習概要

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、データ保護の基準と管理策について学びます。ディスク全体の暗号化、安全なアクセス制御、ハードウェアのバックアップ、クラウドのセキュリティ態勢、データマスキング技術を取り上げます。

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/data-protection/

あなたのデータ保護戦略 学習ロードマップ

- データマスキングとトークン化の技術の違いを説明します。
- ストレージドライブの保存時の暗号化と、TLS による転送時の暗号化を導入する。
- ランサムウェア対策として、オフラインでネットワークから隔離されたバックアップシステムを設計します。

データ保護ガイドの手順

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。学んだ知識をデータ保護に応用しましょう。 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。

データ保護と企業ストレージのセキュリティ（導入）

データ保護は、マスキング、トークン化、保存時のデータベース暗号化、安全な転送プロトコルによって、企業のデータ資産を守ります。ネットワークから隔離したバックアップを設計することで、実際に侵入が起きた場合でも重要なデータベースを復元しやすくなります。

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. データマスキングの主な目的は何ですか?
   - A. プライバシーを守るために、機微な識別子を架空だが現実的な文字に置き換える
   - B. 物理サーバーのストレージ容量を節約するために、大きなデータベースファイルを圧縮すること
   - C. アーカイブ用バックアップシステムから古い顧客連絡先メールを削除すること
   - D. データベースサーバーのパブリック IP アドレスをインターネットのスキャンから隠すこと

2. 2. データベースサーバーのハードドライブに保存されたファイルを暗号化する仕組みはどれですか?
   - A. 保存データのフルディスク暗号化
   - B. 通信中のTLSセッションハンドシェイクプロトコル
   - C. 動的DNSのネームサーバー転送ルール
   - D. ハードウェアキーを使った多要素認証

3. 3. 転送中のデータに当たるものは何ですか?
   - A. ネットワークのルーターやスイッチを移動するデータパケット
   - B. コールドバックアップドライブに保存されたデータベーストランザクションログ
   - C. 隔離されたクラウド保管庫に保存されたアーカイブ済みユーザーファイル
   - D. ローカルのデスクトップストレージにある静的なシステム設定ファイル

4. 4. ランサムウェア対策として、定期的なオフラインバックアップが重要なのはなぜですか?
   - A. 身代金を払わずにファイルを復元できる、クリーンなオフラインコピーを提供する
   - B. ハッカーが開いているポートの設定をスキャンするのを防ぐ
   - C. ローカルネットワークの伝送帯域幅の速度を上げる
   - D. ブラウザーでの Cookie 同意オプトインのログを自動化する

5. 5. データのトークン化は何をしますか?
   - A. 機微なカード番号を、機微でないランダムなトークンに置き換える
   - B. 複数の安全なオニオンノードを経由してウェブトラフィックをルーティングする
   - C. システムディレクトリをスキャンして、シグネチャ型のマルウェアを検出する
   - D. データベース管理者のログインセッション時間を監査する

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. データマスキングは、本番環境のデータベースレコードを恒久的に変更します。

○ 正しい ○ 誤り

7 質問 7

7. ランサムウェアの拡散を防ぐため、オフサイトのバックアップは社内のメインネットワークから隔離する必要があります。

○ 正しい ○ 誤り

8 質問 8

8. SSL/TLS 証明書は、物理メディアに保存されている保存時のデータを暗号化することで、データベースを保護する。

○ 正しい ○ 誤り

9 質問 9

9. ゼロトラストネットワークアクセス (ZTNA) は、データベースへのアクセスを許可する前に、すべてのユーザーの身元を検証します。

○ 正しい ○ 誤り

10 質問 10

10. 保管庫方式のトークン化では、元のカード番号の値を、安全な中央のトークン保管庫に保存します。

○ 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. 個人名を現実的な代替の値に置き換えることを、データ _____ と呼びます。

2. 物理的なストレージブロックを暗号化すると、データベース資産が _____ に保護されます。

3. TLSプロトコルは、 _____ のアクティブなデータパケットを暗号化します。

4. ロールベースの権限は、どのユーザーがデータベースに _____ できるかを制限します。

5. 侵害後にクリーンな社内ファイルを復元するには、安全なオフラインの _____ が必要です。

6. クラウド設定の監査は、組織のセキュリティ _____ を評価します。

用語バンク

アクセス　バックアップ　ポスチャ　マスキング　最小化　侵害　転送中　保存時

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

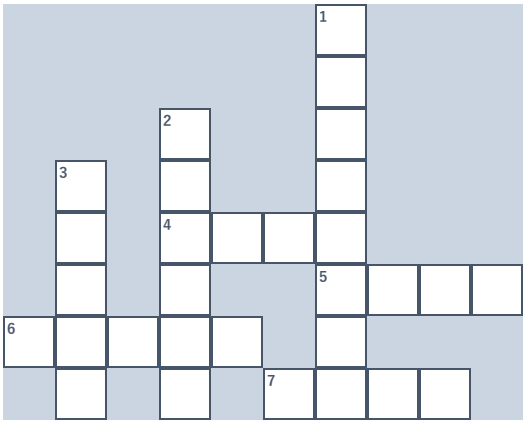
定義マッチング

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. 暗号化	A	システム障害時に復元できるよう、データの安全なオフサイトコピーを作成すること。
2. バックアップ	B	平文を読めない暗号文に変換し、傍受されたデータが秘密のままになるようにすること。
3. 最小化	C	組織のクラウド全体のセキュリティ状態と防御体制。
4. アクセス	D	個人情報を管理するための GDPR や CCPA などの規制基準を満たすこと。
5. ポスチャ	E	保護されたデータが、許可なくアクセスまたは開示されるセキュリティインシデント。
6. 侵害	F	データベースの読み取りと書き込みの権限を、認証されたユーザーロールに限定すること。
7. コンプライアンス	G	個人の身元を保護するために、データベースのフィールド内の機密性の高い文字を置き換えること。
8. マスキング	H	個人データの収集を、運用に必要な最小限にとどめること。

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

4. 保護されたデータが無許可でアクセスまたは開示されたセキュリティインシデント (4)

5. データベースの読み書きの権限を、認証されたユーザーの役割に限ること (4)

6. 平文を読めない暗号文に変換し、傍受されたデータの秘密を保つこと (5)

7. 組織のクラウドが持つセキュリティ状態と防御体制の総体 (4)

タテのカギ

1. GDPRやCCPAなどの規制基準を満たし、個人情報を管理すること (8)

2. 事業運営に必要なごく最小限に個人データの収集を限ること (6)

3. 個人の特定を防ぐために、データベース項目内の機密性の高い文字を置き換えること (5)

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

4 ヨコ: 保護されたデータが無許可でアクセスまたは開示されたセキュリティインシデント (4 文字):

5 ヨコ: データベースの読み書きの権限を、認証されたユーザーの役割に限ること (4 文字):

6 ヨコ: 平文を読めない暗号文に変換し、傍受されたデータの秘密を保つこと (5 文字):

7 ヨコ: 組織のクラウドが持つセキュリティ状態と防御体制の総体 (4 文字):

タテのカギ

1 タテ: GDPRやCCPAなどの規制基準を満たし、個人情報を管理すること (8 文字):

2 タテ: 事業運営に必要なごく最小限に個人データの収集を限ること (6 文字):

3 タテ: 個人の特定を防ぐために、データベース項目内の機密性の高い文字を置き換えること (5 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。

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

用語リスト

アンゴウカ　バツクアツプ　サイシヨウカ　アクセス　ポスチヤ　シンガイ
コンプライアンス　マスキング

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
A. アンゴウカ
B. バツクアツプ
C. サイシヨウカ
D. アクセス
E. ポスチヤ
F. シンガイ
G. コンプライアンス
H. マスキング

定義とマッチ欄
1. 保護されたデータが無許可でアクセスまたは開示されたセキュリティインシデント。
2. 個人の特定を防ぐために、データベース項目内の機密性の高い文字を置き換えること。
3. データベースの読み書きの権限を、認証されたユーザーの役割に限ること。
4. 組織のクラウドが持つセキュリティ状態と防御体制の総体。
5. GDPRやCCPAなどの規制基準を満たし、個人情報を管理すること。
6. 事業運営に必要なごく最小限に個人データの収集を限ること。
7. 平文を読めない暗号文に変換し、傍受されたデータの秘密を保つこと。
8. システム障害に備えて復元できるよう、データの安全なオフサイトコピーを作成すること。

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. ウゴアカン
2. カサシウヨイ
3. ヤポチス
4. ランスアイコンプ
5. アクプバツツ
6. セスアク
7. ガシイン
8. グマキンス

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	バックアップするもの			
2	サイバーセキュリティに関連する言葉			
3	機密データの閲覧を許可された人			
4	データを安全に削除する方法			
5	データが保存されている場所			
6	暗号化すべきもの			
7	病院が守らなければならないデータ			
8	バックアップの種類			
9	決して共有してはいけない情報			
10	メールの危険なサイン			
11	今日から始められる安全な習慣			
12	ITのサポートを頼める人			
13	ハッキングされるおそれのあるデバイス			
14	データを守る方法			
15	データを破壊しうるもの			

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: 企業データベースの保存時暗号化のアップグレード



シナリオ: オンライン小売業者が、ディスク全体の暗号化なしで、取引データベースをクラウドストレージに保存しています。最近のコンプライアンス監査で、これがCCPAに関わる重大なデータセキュリティ上のリスクとして指摘されました。復旧アーキテクチャを設計してください。

ディスカッションの問い: CCPAのコンプライアンス上のリスクを分析し、保存データの暗号化戦略を提案できますか？

ケーススタディ 2: ランサムウェアの封じ込めとデータの復元



シナリオ: 進行中のランサムウェア攻撃が、企業のローカルネットワーク上のネットワークドライブを暗号化しています。管理者は感染を早期に検知しました。封じ込めと復旧の手順を計画してください。

ディスカッションの問い: 直ちに行うべき封じ込めの対応を詳しく説明し、安全な復元プロセスを計画できますか？

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

1	46	55	46	21		14	2	48	38	60		60	72	16	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: 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: データ保護とは何ですか?

技術的な対策により、個人や企業のデータを、不正アクセス、紛失、破損から守るプロセスです。

Q2: ディスク全体の暗号化はなぜ重要ですか?

物理ドライブ上に保存されたデータブロックを保護し、ハードドライブが物理的に盗まれても誰もデータを読めないようにします。

Q3: 保存時の暗号化と転送時の暗号化の違いは何ですか?

保存時の暗号化はドライブ上に保存されたファイルを守り、転送時の暗号化はルーターを通って移動中のネットワークパケットを守ります。

Q4: データマスキングとは何ですか?

機密性の高い詳細(クレジットカード番号など)を、架空だが本物らしいデータに置き換え、実際の記録を露出させずにテストできるようにします。

Q5: オフラインバックアップが重要なのはなぜですか?

ネットワークから隔離されたファイルのクリーンなコピーを保持し、バックアップがランサムウェアに暗号化されるのを防ぐのに役立ちます。

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 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: データトークン化ボールトとは何ですか?

ランダムなトークンと、元の機微な値(クレジットカードの主要口座番号など)を対応づける、安全で隔離されたデータベース。

Q7: ゼロトラストのデータベースアクセスとはどういう意味ですか?

ネットワーク内にいる誰も信頼せず、ログインのたびにすべてのユーザーの身元とデバイスの状態を検証することを意味します。

Q8: TLS は転送中のデータをどう守りますか?

TLS は TCP セッションのペイロードを暗号化し、公衆ネットワーク上の悪意のある者が、伝送中のパケットを盗み見たり改ざんしたりするのを防ぎます。

Q9: データベースアクセス監査とは何ですか?

不正アクセスのパターンやセキュリティ上の異常を検出するための、データベースクエリとログインの継続的な記録。

Q10: クラウドセキュリティ態勢の監査とは何ですか?

クラウド構成を分析して、開いているポート、誤設定されたアクセスルール、セキュリティコンプライアンスの不備を見つけるプロセス。

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: エンベロープ暗号化はどのような仕組みですか?

データをデータキーで暗号化し、そのデータキーをマスターキーで暗号化することで、鍵の保管とローテーションを簡素化します。

Q2: 準同型暗号とは何ですか?

暗号化されたデータを先に復号せずに、そのまま演算できる高度な暗号化方式。

Q3: データベースの列レベル暗号化が使われるのはなぜですか?

機密性の高い特定の列(SSN など)を個別に暗号化し、管理者が一般的なテーブルの読み取り権限を得ても保護します。

Q4: データ損失防止(DLP)とは何ですか?

ネットワークの出口を監視し、機密ファイルの無断の外部送信を検出してブロックするソフトウェア。

Q5: WORM(Write Once Read Many)バックアップはランサムウェアからどう守りますか?

WORMバックアップは、設定した期間中ファイルの削除や変更を防ぎ、ランサムウェアが既存のバックアップを暗号化するのを阻止します。

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: 鍵の再利用のリスクは何ですか?

異なるデータベース間で同じ暗号鍵を再利用すると、1 つの鍵が侵害されただけですべてのデータベースが危険にさらされます。

Q7: データベースのトークン化は CCPA への準拠をどう改善しますか?

トークンは本番以外のシステムでレコードを仮名化し、侵害時の露出を抑えますが、トークン化されたデータも個人情報にあたる場合があります。

Q8: データ分類が重要なのはなぜですか?

ファイルを機密度のレベル別に分類し、組織がリスクの高いデータに最も強力な暗号化とアクセス制御を適用するのに役立ちます。

Q9: 鍵のローテーションの役割は何ですか?

暗号鍵を定期的に更新すると、1 つの鍵がいずれ破られた場合でも、露出する過去のデータの量を抑えられます。

Q10: セキュアエンクレーブは、メモリ内のデータベースクエリをどのように保護しますか?

セキュアエンクレーブは、CPU で保護されたメモリブロック内でクエリ処理を隔離し、ホスト管理者が RAM 上の平文を見られないようにします。

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

GDPR は 2018 年 5 月に施行され、世界のサイトがクッキーの同意と個人データの登録簿を管理する方法が変わりました。

2. セキュリティの洞察

GDPR違反の罰金は2000万ユーロまたは全世界売上高の4%に達することがあり、法的リスクはかなり大きくなります。[4]

3. セキュリティの洞察

CCPAは2020年1月に施行され、米国で先駆的なデジタルプライバシーの消費者の権利を確立しました。

4. セキュリティの洞察

データ最小化はデータベースの保存容量を減らし、サーバーの運用コストを抑えるとともに、侵害の影響の規模も小さくします。

5. セキュリティの洞察

暗号的消去は、過去のバックアップテープのファイルを編集するのではなく鍵を破棄することで、バックアップ削除の課題を解決します。

6. セキュリティの洞察

現在では世界のほとんどの国が、消費者のプライバシー権を守るために個人データ保護法を制定しています。

7. セキュリティの豆知識

欧州のデータプライバシー規制の定義では、あらかじめチェックが入ったオプトイン同意フォームは明確に禁止されています。

8. セキュリティの豆知識

GDPR では、可能な場合、個人データの侵害を知ってから 72 時間以内に監督機関へ報告することが求められます。 [3]

9. セキュリティの豆知識

bcrypt や Argon2 のような低速なアルゴリズムでパスワードをハッシュ化すると、盗まれたハッシュのオフラインでの解読がはるかに難しくなります。 [6]

10. セキュリティの洞察

保存データは保存されたデータベースファイルを指し、転送中のデータはネットワークルーターを実際に移動しているパケットを指します。

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. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

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

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

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

データマスキングの主な目的は何ですか? → プライバシーを守るために、機微な識別子を架空だが現実的な文字に置き換える

2 問題 2

正解: A

指導メモ

データベースサーバーのハードドライブに保存されたファイルを暗号化する仕組みはどれですか? → 保存データのフルディスク暗号化

3 問題 3

正解: A

指導メモ

転送中のデータに当たるものは何ですか? → ネットワークのルーターやスイッチを移動するデータパケット

4 問題 4

正解: A

指導メモ

ランサムウェア対策として、定期的なオフラインバックアップが重要なのはなぜですか? → 身代金を払わずにファイルを復元できる、クリーンなオフラインコピーを提供する

5 問題 5

正解: A

指導メモ

データのトークン化は何をしますか? → 機微なカード番号を、機微でないランダムなトークンに置き換える

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

マスキングはテスト用のコピーを変更するか、クエリ時に値を隠すものであり、本番のレコードは変更されません。

7 問題 7

正解: 正しい

指導メモ

ランサムウェアの拡散を防ぐため、オフサイトのバックアップは社内のメインネットワークから隔離する必要があります。

8 問題 8

正解: 誤り

指導メモ

TLS証明書は転送中のデータを保護します。保存中のデータには、ディスク、ファイル、データベースの暗号化が必要です。

9 問題 9

正解: 正しい

指導メモ

ゼロトラストネットワークアクセス (ZTNA) は、データベースへのアクセスを許可する前に、すべてのユーザーの身元を検証します。

10 問題 10

正解: 正しい

指導メモ

保管庫方式のトークン化は、元の値を安全なトークン保管庫に保持し、そこで各トークンを元のデータに対応づけます。

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

B 1. 暗号化	A 2. バックアップ	H 3. 最小化	F 4. アクセス
C 5. ポスチャ	E 6. 侵害	D 7. コンプライアンス	G 8. マスキング

チェックポイント 3: 解答 – 重要用語

1 マスキング	2 保存時	3 転送中	4 アクセス
5 バックアップ	6 ポスチャ		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 F – シンガイ	2 H – マスキング	3 D – アクセス	4 E – ポスチヤ
5 G – コンプライアンス	6 C – サイシヨウカ	7 A – アンゴウカ	8 B – バツクアツプ

指導者向けディスカッションメモ

重要用語:
生徒が暗号化、バックアップ、最小化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。

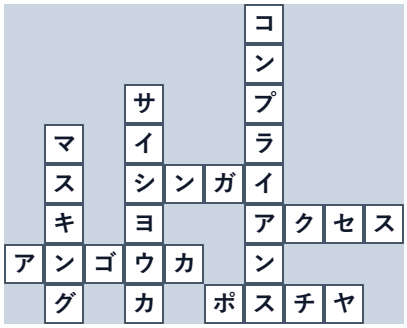
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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

4 ヨコ: シンガイ 保護されたデータが無許可でアクセスまたは開示されたセキュリティインシデント (4 文字)

5 ヨコ: アクセス データベースの読み書きの権限を、認証されたユーザーの役割に限ること (4 文字)

6 ヨコ: アンゴウカ 平文を読めない暗号文に変換し、傍受されたデータの秘密を保つこと (5 文字)

7 ヨコ: ポスチヤ 組織のクラウドが持つセキュリティ状態と防御体制の総体 (4 文字)

タテのカギ

1 タテ: コンプライアンス GDPRやCCPAなどの規制基準を満たし、個人情報を管理すること (8 文字)

2 タテ: サイショウカ 事業運営に必要なごく最小限に個人データの収集を限ること (6 文字)

3 タテ: マスキング 個人の特定を防ぐために、データベース項目内の機密性の高い文字を置き換えること (5 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. ウゴアカン — **アンゴウカ**
2. カサシウヨイ — **サイシヨウカ**
3. ヤポチス — **ポスチヤ**
4. ランスアイコンプ — **コンプライアンス**
5. アクプバツツ — **バツクアツプ**
6. セスアク — **アクセス**
7. ガシイン — **シンガイ**
8. グマキンス — **マスキング**

秘密の暗号チャレンジ 解答

"アンゼンナ セイギョデ データヲ マモル"

ケーススタディの解答

A ケーススタディ 1: 企業データベースの保存時暗号化のアップグレード

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: あるオンライン小売業者は、取引データベースをディスク全体の暗号化なしでクラウドストレージに保存しています。最近のコンプライアンス監査で、これは CCPA 上の重大なデータセキュリティリスクとして指摘されました。復旧アーキテクチャを設計してください。
- 推奨される戦略と解決策: すべてのファイルシステムで保存時の AES-256 フルディスク暗号化を実装します。自動ローテーション付きの一元的な鍵管理サービス (KMS) を使い、復号のアクセスを制御するために厳格な IAM ポリシーを適用します。

B ケーススタディ 2: ランサムウェアの封じ込めとデータの復元

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: 稼働中のランサムウェア攻撃が、企業のローカルネットワーク上のネットワークドライブを暗号化しています。管理者は感染を早期に検知しました。封じ込めと復旧の手順を計画してください。
- 推奨される戦略と解決策: 侵害されたセグメントをただちに隔離します。影響を受けたエンドポイントをフォーマットし、最新のオフラインの WORM (write-once-read-many) バックアップから復元します。システムを再接続する前にバックアップの整合性を確認します。