名前: _____ 日付: _____ 得点: _____

パスワード漏えいと認証情報のセキュリティ

クレデンシャルスタッフィング、データ侵害、ハッシュアルゴリズム、多要素認証、パスワードセキュリティ。

パスワード漏えいの学習概要

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、パスワード漏えいと認証情報のセキュリティについて学びます。クレデンシャルスタッフィング、データ侵害、ハッシュアルゴリズム、多要素認証、パスワードマネージャーを取り上げます。

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/passwords-leak/

あなたのパスワードセキュリティ 学習ロードマップ

- ダークウェブのフォーラムでの認証情報の露出リスクを理解する。
- 多要素認証 (MFA) と、漏えいした認証情報の監視を導入する。
- 標的型ソーシャルエンジニアリング詐欺に対する、企業のセキュリティ防御を設計します。

パスワード漏えいガイドの手順

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。学んだ知識を認証情報の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。

パスワード漏えいと認証情報のセキュリティ（導入）

パスワード漏えいにより、ユーザーの認証情報が公開ウェブやダークウェブのサイトにさらされます。パスワードマネージャーによる固有のパスワード、漏えいしたパスワードのスクリーニング、多要素認証（MFA）は認証情報スタッフィングのリスクを減らし、ソルト付きで低速なパスワードハッシュ化は、パスワードデータベースが盗まれた場合の被害を抑えます。

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. クレデンシャルスタッフィングとは何ですか?
   - A. 自動化を使い、流出したユーザー名とパスワードの組み合わせを複数のサイトで試す
   - B. ローカルのデータベースストレージファイルを暗号化すること
   - C. ネットワークトラフィックのリクエストでウェブサーバーを過負荷にすること
   - D. キーボード入力を密かに監視すること

2. 2. OWASPが現在、パスワードの保存に最初に推奨しているアルゴリズムはどれですか？
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. 3. 多要素認証（MFA）は、パスワード漏えいのリスクをどのように軽減しますか？
   - A. 追加の認証要素を必要とするため、盗まれたパスワードだけでは不十分になる
   - B. パスワードを1時間ごとに自動的に変更する
   - C. 送信中のユーザー名を暗号化する
   - D. 不正なリクエストを信用情報機関に通知する

4. 4. データ侵害ダンプとは何ですか?
   - A. オンラインで公開された、またはハッカーフォーラムで売買される、流出したユーザー認証情報の集まり
   - B. データベースファイルのバックアップコピーを外部に保管したもの
   - C. ウェブサーバーログの一時的なキャッシュ
   - D. ユーザーのパスワードをリセットするために使う管理ツール

5. 5. パスワードマネージャーの役割は何ですか?
   - A. すべてのアカウントに固有の強力なパスワードを生成して保存する
   - B. パスワード漏えいがないかネットワークトラフィックを監視すること
   - C. ゲートウェイで自動化されたブルートフォース攻撃をブロックすること
   - D. データベースのストレージブロックをスキャンして、暗号化されていないパスワードを探すこと

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. 複数のアカウントでパスワードを使い回すと、クレデンシャルスタッフィングのリスクが高まります。

○ 正しい　○ 誤り

7 質問 7

7. SHA-1 は、現代のパスワード保存に推奨されるハッシュ関数である。

○ 正しい　○ 誤り

8 質問 8

8. パスワードの複雑さだけを徹底すれば(MFAなしでも)、クレデンシャルスタッフィングを完全に止められます。

○ 正しい　○ 誤り

9 質問 9

9. ダークウェブ監視ツールは、侵害された企業の認証情報がないかインターネットをスキャンします。

○ 正しい　○ 誤り

10 質問 10

10. ソルト付きハッシュは、ハッシュ化の前にパスワードに固有のランダムなデータを加え、レインボーテーブル攻撃を無効にします。

○ 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. 多数のウェブアプリケーションで、漏えいした認証情報を試すことは、クレデンシャル _____ です。

2. OWASPが今も認めている、処理が遅く適応型のパスワードハッシュアルゴリズムは _____ です。

3. 機密のデータベースファイルがインターネット上に露出することは、データ _____ です。

4. ハッシュ化の前にパスワードへランダムな値を加えることは、 _____ と呼ばれます。

5. ユーザーの認証情報を保管する安全なローカルデータベースは、パスワード _____ です。

6. ログインに二段階目の確認を加えるには、 _____ を使います。

用語バンク

bcrypt　スタッフィング　ソルティング　フィッシング　マネージャー　レインボーテーブル　侵害　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: セキュリティの概念マッチング

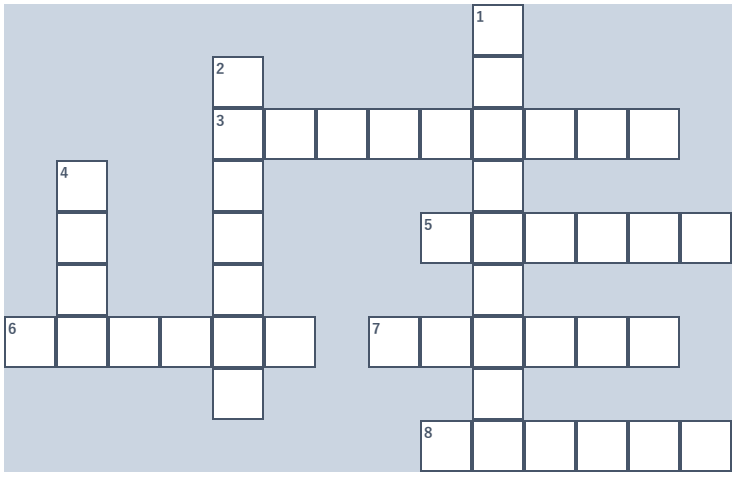
定義マッチング

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. スタッフィング	A	パスワードハッシュを事前に計算した表。
☐	2. bcrypt	B	多要素ログインの確認。
☐	3. 侵害	C	認証情報の保管ツール。
☐	4. ソルティング	D	データベースの不正な露出。
☐	5. マネージャー	E	ログイン情報を盗むソーシャルエンジニアリング。
☐	6. MFA	F	漏えいした認証情報を試すこと。
☐	7. レインボーテーブル	G	パスワードハッシュにランダムなソルトを加える。
☐	8. フィッシング	H	低速なパスワードハッシュアルゴリズム。

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. 複数の要素によるログイン確認 (9)

5. 処理が遅いパスワードのハッシュアルゴリズム (6)

6. ログイン情報を盗むためのソーシャルエンジニアリング (6)

7. 認証情報を保管するためのツール (6)

8. パスワードのハッシュに、ランダムな値を加えること (6)

タテのカギ

1. パスワードのハッシュをあらかじめ計算して並べた表 (9)

2. 漏えいした認証情報を次々に試すこと (7)

4. データベースが許可なく外部にさらされること (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

3 ヨコ: 複数の要素によるログイン確認 (9 文字):

5 ヨコ: 処理が遅いパスワードのハッシュアルゴリズム (6 文字):

6 ヨコ: ログイン情報を盗むためのソーシャルエンジニアリング (6 文字):

7 ヨコ: 認証情報を保管するためのツール (6 文字):

8 ヨコ: パスワードのハッシュに、ランダムな値を加えること (6 文字):

タテのカギ

1 タテ: パスワードのハッシュをあらかじめ計算して並べた表 (9 文字):

2 タテ: 漏えいした認証情報を次々に試すこと (7 文字):

4 タテ: データベースが許可なく外部にさらされること (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。

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

用語リスト

スタツフイング　ビークリプト　シンガイ　ソルテイング　マネージヤー
タヨウソニンシヨウ　レインボーテーブル　フイツシング

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. スタツフイング
B. ビークリプト
C. シンガイ
D. ソルテイング
E. マネージヤー
F. タヨウソニンシヨウ
G. レインボーテーブル
H. フイツシング

定義とマッチ欄
1. ログイン情報を盗むためのソーシャルエンジニアリング。
2. データベースが許可なく外部にさらされること。
3. 処理が遅いパスワードのハッシュアルゴリズム。
4. パスワードのハッシュをあらかじめ計算して並べた表。
5. 漏えいした認証情報を次々に試すこと。
6. パスワードのハッシュに、ランダムな値を加えること。
7. 認証情報を保管するためのツール。
8. 複数の要素によるログイン確認。

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. フンスイグツタ
2. シガイン
3. マージーヤネ
4. ールブボーテレイン
5. リクトビプー
6. ンイソテグル
7. ンタヨウシソヨニウ
8. ツグフンシイ

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	今日から始められる安全な習慣			
2	強力なパスワードのルール			
3	知っているパスワードマネージャー			
4	知っているセキュリティツール			
5	メールの危険なサイン			
6	長いパスフレーズに使える楽しい言葉			
7	パスワードなしでログインする方法			
8	決して共有してはいけない情報			
9	ソフトウェアを更新する理由			
10	パスワードが漏えいしたときにすること			
11	MFAが必要なアカウント			
12	パスワードを決して保存してはいけない場所			
13	コンピューターが感染しているサイン			
14	人がよく使う悪いパスワード			
15	バックアップするもの			

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: 企業の認証情報漏えいへの対処



シナリオ: ダークウェブ監視サービスが、企業のシステム管理者のパスワードを含むデータベースのダンプがオンラインで公開されたと、ある組織に警告します。

ディスカッションの問い: 認証情報の漏えいのリスクを分析し、管理者によるリセットの戦略を提案できますか？

ケーススタディ 2: パスワードのハッシュ化標準の導入



シナリオ: 企業のデータベースが現在、暗号学的なソルトなしの旧式のMD5ハッシュでユーザーのパスワードを保存しており、すばやく抽出される危険があります。

ディスカッションの問い: データベースのハッシュアルゴリズムをアップグレードするための移行戦略を設計できますか？

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

43	3	4	2	12	16		67	13	44	72	61	45		22	46	12	38	3	60

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: パスワード漏えいとは何ですか?

パスワード漏えいは、データ侵害やサーバーの設定ミスによって、ユーザーのログイン認証情報が露出することです。

Q2: ハッカーは、漏えいしたパスワードをどのように見つけますか?

ハッカーは、ダークウェブのフォーラム、公開データベースのダンプ、侵害データが公開されるペーストサイトをスキャンしています [8]。

Q3: パスワードの使い回しは危険ですか?

はい、1つのサイトが侵害されると、ハッカーが同じ認証情報を何千もの他のプラットフォームで試せるためです [3]。

Q4: 暗号のソルトとは何ですか?

ソルトは、ハッシュ化の前にパスワードに加えられるランダムなデータで、事前計算された表を使う攻撃を無効にします [2]。

Q5: MD5 が時代遅れなのはなぜですか?

MD5 は高速で時代遅れの汎用ハッシュなので、特にソルトのないハッシュでは、攻撃者がパスワードの推測を極めて素早く試せます [2]。

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: パスワードマネージャーはユーザーをどう守りますか?

サイトごとに複雑で一意な認証情報を自動生成し、人が記憶する際のミスや使い回しを減らします。

Q7: ブルートフォース攻撃とは何ですか?

正しいパスワードが見つかるまで、考えられるすべての文字の組み合わせを体系的に試す攻撃 [4]。

Q8: アカウントロックアウトはどう役立ちますか?

ロックアウトやレート制限は、オンラインでの繰り返しの推測を遅らせ、監視や MFA と組み合わせることで総当たり攻撃のリスクを減らします [4]。

Q9: マスターパスワードは安全ですか?

エントロピーの高いパスフレーズで、他のWebシステムで使い回さなければ、安全です。

Q10: パスワードは定期的に変更すべきですか?

NIST は、定期的な変更を強制せず、漏えいの証拠があったときに変更し、長さ、ブロックリスト、MFA を優先するよう述べています [1]。

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: Argon2 は bcrypt とどう違いますか?

OWASP は Argon2id を第一選択として挙げています。メモリハードな設定により、GPU や ASIC による解読に対して bcrypt より強い耐性があります [2]。

Q2: 鍵ストレッチングとは何ですか?

ハッシュアルゴリズムを何千回も繰り返してパスワードの検証を遅くし、解読にコストがかかるようにする技術 [2]。

Q3: レインボーテーブルはどのように機能しますか?

平文のパスワードとそのハッシュを対応付けた事前計算済みの検索テーブルで、ソルトなしのハッシュを素早く逆算するために使われます [2]。

Q4: 認証情報の使い回しとは何ですか?

ある情報漏えいで盗まれたユーザー名とパスワードの組み合わせを再利用して、他のサービスへのアクセスを試みること。特にパスワードを使い回している場合に起こります [3]。

Q5: パスワードマネージャーはハッキングされることがありますか?

はい。多くはゼロ知識暗号化を使っているため、サーバーが侵害されても暗号化された保管庫しか露出しませんが、弱いマスターパスワードはオフラインで破られる可能性があります。

チェックポイント 10: セキュリティ FAQ – 応用 (パート 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: 辞書攻撃とは何ですか?

ランダムな文字ではなく、一般的な単語、フレーズ、過去に流出したパスワードを試すブルートフォース攻撃の一種。

Q7: パスフレーズが好まれるのはなぜですか?

パスフレーズは複数のランダムな単語を使うため、人間には覚えやすく、計算上は解読に手間がかかる高いエントロピーが得られます [1]。

Q8: シングルサインオン(SSO)はパスワード漏えいにどう影響しますか?

SSO はパスワードの乱立を減らしますが、ID プロバイダーが価値の高い標的になるため、強力で、できればフィッシングに強い MFA が必要です [6]。

Q9: セッションハイジャックとは何ですか?

攻撃者が有効なセッショントークンを入手または悪用し、パスワードを再入力せずにサインイン中のユーザーになりすますこと [5]。

Q10: パスワードスプレー攻撃はどのように検出しますか?

多数のアカウントで同じ少数のパスワードが試されていないかを調べることによって。多くの場合、ロックアウトのしきい値を下回るよう、ゆっくりと試されます [7]。

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

NIST SP 800-63B は、新しいパスワードを、よくあるパスワードや漏えい済みパスワードのブロックリストと照合して確認することを求めています [1]。

2. セキュリティの洞察

2019年の「Collection #1」のダンプは、以前の多数の情報漏えいで流出したデータを、メールアドレスとパスワードの組み合わせの巨大な1つのファイルにまとめたものでした [8]。

3. セキュリティの洞察

NIST は現在、唯一の認証要素として使うパスワードを 15 文字以上にすることを求めています [1]。

4. セキュリティの洞察

ASICハードウェアは1秒間に何十億ものSHA-256ハッシュを計算できるため、生のSHAハッシュ化はユーザーのパスワードには安全ではありません [2]。

5. セキュリティの洞察

ソルトが固有であれば、まったく同じパスワードを持つ2人のユーザーでも、データベース上のハッシュは異なります [2]。

6. セキュリティの洞察

多くのパスワードマネージャーは、ユーザーのマスターパスワードから導き出した強力な暗号技術で、保管庫のデータをローカルで暗号化します。

7. セキュリティの豆知識

クレデンシャルスタッフィングが成立するのは、多くの人がEC、銀行、メールのアカウントで同じパスワードを使い回しているためです [3]。

8. セキュリティの豆知識

NIST SP 800-63B は、検証者が定期的なパスワード変更を要求してはならず、漏えいの証拠があった後にのみ変更を求めるべきだとしています [1]。

9. セキュリティの豆知識

短いパスワードに大文字1文字と記号1つを加えても、最新の自動化されたGPU辞書攻撃を防ぐことはできません [1]。

10. セキュリティの洞察

MFA は、パスワードが漏えいした後でも多くのクレデンシャルスタッフィングの試みを防げます。フィッシングに強い MFA は SMS コードより強力です [3]。

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 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

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

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).
https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).
https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.
https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

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

クレデンシャルスタッフィングは、自動化を使って、漏えいしたユーザー名とパスワードの組を他のサイトで試す手法です [3]。

2 問題 2

正解: A

指導メモ

OWASPはまずArgon2idを推奨しており、bcryptは主に、Argon2idやscryptが使えないレガシーシステム向けです [2]。

3 問題 3

正解: A

指導メモ

MFAは追加の要素を必要とするため、盗まれたパスワードだけではアカウントのロックを解除できません [3]。

4 問題 4

正解: A

指導メモ

流出データの寄せ集めとは、2019年のCollection #1のように、漏えいした認証情報を集めたコレクションのことです [8]。

5 問題 5

正解: A

指導メモ

パスワードマネージャーは、アカウントごとに固有の強力なパスワードを生成して保存し、使い回しを防ぎます [3]。

解答: チェックポイント 2 – 正誤問題

6 問題 6

正解: 正しい

指導メモ

正しい: パスワードを使い回していると、あるサイトから漏えいした認証情報を、攻撃者が他のサイトで再利用できます [3]。

7 問題 7

正解: 誤り

指導メモ

誤り: SHA-1は高速なハッシュです。OWASPは、代わりにArgon2id、scrypt、bcrypt、PBKDF2を推奨しています [2]。

8 問題 8

正解: 誤り

指導メモ

誤り: 複雑さのルールだけでは、漏えいしたパスワードの使い回しによるスタッフィングを止められません。MFAが必要です [3]。

9 問題 9

正解: 正しい

指導メモ

正しい: 監視サービスは、流出データやダークウェブの情報源から、漏えいした認証情報を探します [8]。

10 問題 10

正解: 正しい

指導メモ

正しい: パスワードごとに固有のソルトを使うと、事前計算されたレインボーテーブルが無効になります [2]。

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

F 1. スタッフィング	H 2. bcrypt	D 3. 侵害	G 4. ソルティング
C 5. マネージャー	B 6. MFA	A 7. レインボーテーブル	E 8. フィッシング

チェックポイント 3: 解答 – 重要用語

1 スタッフィング	2 bcrypt	3 侵害	4 ソルティング
5 マネージャー	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 H – フイツシング	2 C – シンガイ	3 B – ビークリプト	4 G – レインボーテーブル
5 A – スタツフイング	6 D – ソルテイング	7 E – マネージヤー	8 F – タヨウソニンシヨウ

指導者向けディスカッションメモ

重要用語:
生徒がスタッフィング、bcrypt、侵害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。

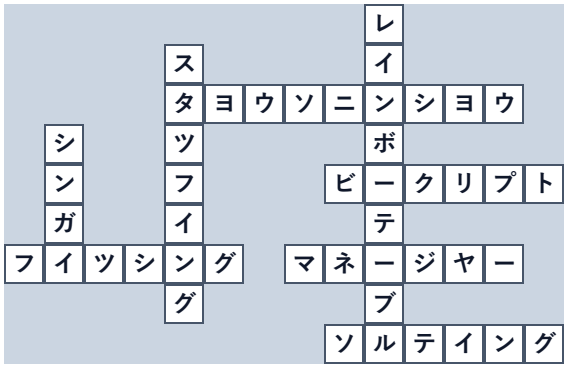
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

ク	グ	一	ヌ	チ	ユ	ガ	ソ	メ	ロ	ボ	ワ	ラ	キ	ゼ
ゴ	ザ	ヤ	ス	ホ	ノ	オ	ル	ス	ア	オ	キ	ル	パ	ホ
ヒ	パ	ジ	ヘ	ボ	ズ	フ	テ	サ	タ	ン	メ	ハ	コ	ヌ
ル	ヤ	ー	モ	ヘ	ワ	レ	イ	テ	モ	ツ	モ	ン	ギ	ゲ
ブ	ズ	ネ	ジ	ツ	タ	カ	ン	ゴ	ワ	ラ	フ	ニ	グ	カ
ー	バ	マ	コ	ザ	ヨ	ペ	グ	ダ	キ	ポ	バ	イ	タ	フ
テ	ト	ー	コ	モ	ウ	サ	ガ	ビ	ベ	レ	カ	ゾ	ン	エ
ー	ア	ー	ユ	コ	ソ	ヘ	イ	ー	サ	ラ	サ	ソ	テ	グ
ボ	ヌ	コ	ギ	ン	ニ	メ	ス	ク	ヌ	グ	ポ	グ	ゴ	ソ
ン	ガ	ド	セ	イ	ン	シ	イ	リ	ガ	リ	ン	ヤ	レ	ズ
イ	ボ	ワ	ヒ	グ	シ	ン	ゼ	プ	ゲ	シ	ケ	ヤ	プ	オ
レ	タ	グ	ベ	ブ	ヨ	ガ	ノ	ト	ツ	イ	ギ	ー	ピ	ピ
マ	ツ	ヌ	メ	ガ	ウ	イ	ヒ	イ	ム	ミ	ジ	リ	ト	ロ
ン	テ	ー	ウ	ラ	デ	チ	フ	ダ	カ	プ	グ	プ	オ	ト
ミ	ー	ツ	ハ	ヨ	レ	ユ	ブ	キ	ム	ー	プ	チ	ピ	リ

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: タヨウソニンシヨウ 複数の要素によるログイン確認 (9 文字)

5 ヨコ: ビークリプト 処理が遅いパスワードのハッシュアルゴリズム (6 文字)

6 ヨコ: フイツシング ログイン情報を盗むためのソーシャルエンジニアリング (6 文字)

7 ヨコ: マネージヤー 認証情報を保管するためのツール (6 文字)

8 ヨコ: ソルテイング パスワードのハッシュに、ランダムな値を加えること (6 文字)

タテのカギ

1 タテ: レインボーテーブル パスワードのハッシュをあらかじめ計算して並べた表 (9 文字)

2 タテ: スタツフイング 漏えいした認証情報を次々に試すこと (7 文字)

4 タテ: シンガイ データベースが許可なく外部にさらされること (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. フンスイグツタ — **スタツフイング**
2. シガイン — **シンガイ**
3. マージーヤネ — **マネージヤー**
4. ールブボーテレイン — **レインボーテーブル**
5. リクトビプー — **ビークリプト**
6. ンイソテグル — **ソルテイング**
7. ンタヨウシソヨニウ — **タヨウソニンシヨウ**
8. ツグフンシイ — **フイツシング**

秘密の暗号チャレンジ 解答

"ロウエイシタ パスワードヲ ニンショウデ マモル"

ケーススタディの解答

A ケーススタディ 1: 企業の認証情報漏えいへの対処 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: ダークウェブ監視サービスが、企業のシステム管理者のパスワードを含むデータベースのダンプがオンラインで公開されたことを、ある組織に警告します。
- 推奨される戦略と解決策: 有効な管理者セッションをすべて取り消し、高エントロピーのジェネレーターで認証情報をリセットします。管理ポータルにフィッシングに強い MFA を適用し [6]、影響を受けた API キーをローテーションし、ログインログを確認して、最初の露出箇所を特定し、他の特権アカウントも確認します。

B ケーススタディ 2: パスワードのハッシュ化標準の導入 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: ある企業のデータベースは、現在、暗号学的ソルトなしの古い MD5 ハッシュでユーザーのパスワードを保存しているため、短時間で抽出されやすい状態です。
- 推奨される対策と解決策: ユーザーごとに固有のソルトを付けた Argon2id (旧システムでは bcrypt) を採用します [2]。既存の MD5 ハッシュは今すぐ新しいアルゴリズムでラップし、各ユーザーの次回ログイン時に直接再ハッシュして、長期間使われていないアカウントにはリセットを強制します。