名前: 日付: 得点:

ランサムウェア攻撃とビジネス復旧

ペイロードの実行、ファイルの暗号化、オフラインバックアップ、封じ込め手順、災害復旧。

ランサムウェア攻撃の学習概要

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、ランサムウェア攻撃と事業の復旧について学びます。ペイロードの実行、ファイルの暗号化、オフラインバックアップ、脅威の封じ込め、暗号資産での支払い、災害復旧計画を取り上げます。

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/ransomware-attack/

あなたのランサムウェアからの復旧 学習ロードマップ

- トロイの木馬、ランサムウェア、スパイウェアのペイロードの違いを説明します。
- 安全なサンドボックス環境内で、悪意のあるファイルを分析してください。
- ネットワークの迅速な隔離と封じ込めの手順を策定する。

ランサムウェア攻撃ガイドの手順

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。学んだ知識をランサムウェアからの復旧に応用しましょう。 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。

ランサムウェア攻撃と災害復旧(導入)

ランサムウェアのペイロードは、システムのストレージを暗号的にロックし、復号鍵と引き換えに暗号資産での支払いを要求します。この脅威を軽減するには、ネットワークの分離ルール、サンドボックスでのマルウェア分析、堅牢なエアギャップのコールドバックアップが有効です。

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. ランサムウェア攻撃の主なメカニズムは何ですか?

- A. システムへのアクセスを拒否するための、ユーザーファイルの暗号化
- B. フォームフィールドに悪意のあるSQLコマンドを注入すること
- C. 公衆 Wi-Fi 接続でネットワークパケットを盗聴すること
- D. SPF 検証を回避するためにメールヘッダーを偽造すること

2 2. オフライン(コールド)バックアップとは何ですか?

- A. マルウェアの拡散から守るため、ネットワークから切り離された保管用コピー
- B. プライマリウェブサーバーのハードドライブに保管されたバックアップ
- C. システムレジストリ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

3 3. ランサムウェア攻撃の際、セキュリティチームは感染したシステムをどのように隔離すべきですか?

- A. すぐにネットワークケーブルを抜き、ワイヤレスインターフェースを無効にする
- B. ウイルス対策シグネチャデータベースをアップグレードする
- C. プライマリ DNS サーバーをシャットダウンする
- D. 侵害されたファイルの拡張子を変更する

4 4. セキュリティ機関がランサムウェアの要求に応じないよう勧めるのはなぜですか?

- A. 資金を支払うと攻撃者を助長し、復号鍵が届く保証もない
- B. 企業の保険契約をすべて自動的に無効にする
- C. すべての顧客に自動的にメールで通知する
- D. 残りのシステムバックアップファイルを破損させる

5 5. 災害復旧計画(DRP)とは何ですか?

- A. システムが侵害された後に、業務とデータを復旧するための体系的なプロセス
- B. 受信ネットワークポートを割り当てるファイアウォール設定
- C. ユーザーの管理権限を一覧にしたデータベーススキーマ
- D. なりすましドメインを拒否するメール認証プロトコル

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. ランサムウェアのペイロードは、ネットワークに接続されたオンラインバックアップに簡単に拡散することがあります。

○ 正しい ○ 誤り

7 質問 7

7. 暗号資産による身代金を支払えば、ファイルが確実に復号されることが保証されます。

○ 正しい ○ 誤り

8 質問 8

8. 感染したシステムをネットワークから切断すると、ランサムウェアが隣接するシステムに広がるのを防ぐのに役立ちます。

○ 正しい ○ 誤り

9 質問 9

9. ランサムウェアが、システムストレージの暗号化に共通鍵暗号を使うことは決してありません。

○ 正しい ○ 誤り

10 質問 10

10. データ復元の手順を定期的にテストすることは、災害復旧の重要な要素です。

○ 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. ローカルファイルへのアクセスを拒むには、暗号による _____ を使います。
2. システム上で実行される悪意のあるコードは _____ です。
3. 切り離されたオフサイトの保管コピーは、安全な _____ にあたります。
4. マルウェアの拡散を止めるには、エンドポイントのネットワーク _____ が必要です。
5. サイバー犯罪者が要求する暗号資産での支払いは _____ です。
6. 業務用データファイルを元に戻すことは、災害 _____ にあたります。

用語バンク

コールドバックアップ　ペイロード　暗号化　隔離　感染　災害　身代金　復旧

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

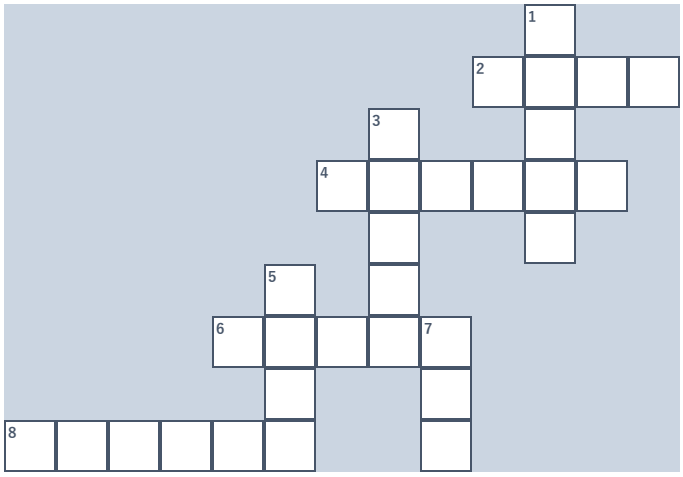
定義マッチング

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	感染したネットワークシステムの切り離し。
	2. ペイロード	B	無害を装った悪意のあるファイル。
	3. コールドバックアップ	C	ファイルを暗号技術でロックすること。
	4. 隔離	D	システムの大規模な障害イベント。
	5. 身代金	E	悪意のあるソフトウェアの実行。
	6. 復旧	F	切り離されたオフラインのコピー。
	7. 災害	G	バックアップからデータベースを復元すること。
	8. トロイの木馬	H	暗号鍵の支払い要求。

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. システムに大きな障害が起きる事態 (4)

4. 感染したシステムを切り離す対象となる通信網 (6)

6. ファイルを暗号で使えなくすること (5)

8. 暗号鍵と引き換えに支払いを求める要求 (6)

タテのカギ

1. 悪意のあるソフトウェアの実行部分 (5)

3. バックアップからデータベースを元に戻すこと (5)

5. マルウェアに侵され、ネットワーク上で被害が広がった状態 (4)

7. 感染したネットワークシステムを切り離すこと (3)

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: システムに大きな障害が起きる事態 (4 文字):

4 ヨコ: 感染したシステムを切り離す対象となる通信網 (6 文字):

6 ヨコ: ファイルを暗号で使えなくすること (5 文字):

8 ヨコ: 暗号鍵と引き換えに支払いを求める要求 (6 文字):

タテのカギ

1 タテ: 悪意のあるソフトウェアの実行部分 (5 文字):

3 タテ: バックアップからデータベースを元に戻すこと (5 文字):

5 タテ: マルウェアに侵され、ネットワーク上で被害が広がった状態 (4 文字):

7 タテ: 感染したネットワークシステムを切り離すこと (3 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。

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

用語リスト

アンゴウカ　ペイロード　カンセン　カクリ　ミノシロキン　フツキユウ　サイガイ　ネツトワーク

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. ペイロード
C. カンセン
D. カクリ
E. ミノシロキン
F. フツキユウ
G. サイガイ
H. ネットワーク

定義とマッチ欄
1. マルウェアに侵され、ネットワーク上で被害が広がった状態。
2. 感染したシステムを切り離す対象となる通信網。
3. ファイルを暗号で使えなくすること。
4. 暗号鍵と引き換えに支払いを求める要求。
5. 感染したネットワークシステムを切り離すこと。
6. システムに大きな障害が起きる事態。
7. 悪意のあるソフトウェアの実行部分。
8. バックアップからデータベースを元に戻すこと。

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. カセンン
3. ミシロンキノ
4. イガサイ
5. ロドペーイ
6. クリカ
7. ユウフキツ
8. トクネーワツ

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	ハッキングされるおそれのあるデバイス			
3	身代金を支払うべきでない理由			
4	今日から始められる安全な習慣			
5	知っているセキュリティツール			
6	アカウントを守る方法			
7	コンピューターが感染しているサイン			
8	バックアップを保管する場所			
9	絶対に失いたくないファイル			
10	ランサムウェアが広がる経路			
11	攻撃を受けてから最初の1時間にすること			
12	攻撃を受けたときに連絡する人			
13	ランサムウェアがロックできるもの			
14	サイバーセキュリティに関連する言葉			
15	よく標的にされる組織			

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: 企業でのランサムウェアのペイロードの封じ込め



シナリオ: ある企業のローカルエリアネットワークが、活動中のランサムウェアに侵害されました。 主要なファイルサーバーで、ファイル拡張子が .locked と表示され始めています。

ディスカッションの問い: 封じ込めの手順を詳しく説明し、データ復旧のプロトコルを概説できますか？

ケーススタディ 2: オフラインバックアップ構成の評価



シナリオ: ある企業が、主要なローカルネットワークがランサムウェアに完全に乗っ取られた場合でも、バックアップが侵害されるリスクを減らす、データバックアップの戦略を設計したいと考えています。

ディスカッションの問い: 安全なオフラインバックアップ保管庫システムを設計してください。

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

62	18	8	1	18	69	6	39		60	72	16	45		28	18	7	37	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: ランサムウェアとは何ですか?

ランサムウェアは、身代金が支払われるまでコンピューターシステムやファイルへのアクセスを妨げるように設計された悪意のあるソフトウェアです。

Q2: ランサムウェアはどのように拡散しますか?

メールのフィッシング添付ファイル、未修正のソフトウェアの脆弱性、侵害されたリモートアクセスシステムを経由します。 [1]

Q3: 支払いを暗号資産で求められるのはなぜですか?

ビットコインなどの暗号資産は相対的な匿名性を備えており、法執行機関が資金を追跡しにくくなります。

Q4: ウイルス対策ソフトはランサムウェアをブロックしますか?

はい、ただし、シグネチャベースのアンチウイルスは、新たに作られたゼロデイのランサムウェアのペイロードには対応できないことがあります。

Q5: エアギャップバックアップとは何ですか?

主ネットワークとの物理的・論理的な接続がなく、被害の拡大から守られているバックアップコピー。

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: 二重脅迫とは何ですか?

攻撃者がファイルを暗号化するだけでなく、機密データも盗み出し、身代金が支払われなければ公開すると脅す場合。

Q7: 復号ツールとは何ですか?

ロックされたファイルを平文に戻すために必要な暗号鍵を含むソフトウェアユーティリティ。

Q8: ランサムウェアを早期に検出するにはどうすればよいですか?

ファイルシステムを監視し、突然の大量のファイル変更や名前変更の動きを検出することによって。

Q9: 保険の役割は何ですか?

サイバー保険は復旧費用の補填に役立つことがありますが、補償の条件や身代金支払いに関するルールは契約によって異なります。

Q10: 感染したシステムは再起動すべきですか?

いいえ、再起動すると揮発性メモリの証拠が失われる可能性があります。代わりにネットワークから隔離してください。 [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: ランサムウェアは、非対称暗号をどのように使いますか?

マルウェアに埋め込まれた公開鍵を使ってファイルを暗号化するため、復号には攻撃者の秘密鍵が必要です。

Q2: なぜ共通鍵暗号も使われるのですか?

共通鍵暗号 (AES など) は高速で、巨大なデータベースを数分でロックできますが、非対称鍵が AES の鍵を保護します。

Q3: 論理セグメンテーションとは何ですか?

ネットワークを隔離されたゾーンに分割して、マルウェアがワークステーションからコアサーバーへ横方向に広がるのを防ぎます。

Q4: WORM ストレージとは何ですか?

Write-Once, Read-Many(WORM)メディアで、ランサムウェアのペイロードによるバックアップデータの編集、上書き、削除を防ぎます。

Q5: シャドウコピーとは何ですか?

Windows が作成するローカルのバックアップスナップショット。ランサムウェアは通常、管理ツールを使って最初にこれらを削除します。

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: 認証情報の窃取はランサムウェアをどう可能にしますか?

攻撃者は、漏えいした管理者ログインを購入してリモートデスクトップ経由でサインインし、ネットワーク全体で手動でランサムウェアを実行します。

Q7: ドライランによる復元テストとは何ですか?

バックアップしたデータベースを隔離されたテスト環境に定期的に復元し、復元の速度とデータの整合性が災害対策の指標を満たしていることを確認すること。

Q8: エンドポイント検出(EDR)はランサムウェアをどう阻止しますか?

プロセスの動作（例: 急速な暗号化）を分析し、不正なアプリケーションをすばやく停止させることによって。

Q9: サービスとしてのランサムウェア(RaaS)モデルとは何ですか?

マルウェア開発者がランサムウェアのビルダーをアフィリエイトに貸し出し、支払いの一定割合を受け取るフランチャイズ型のモデル。

Q10: パッチ未適用の RDP は、どのようにランサムウェアを引き起こしますか?

公開されていて修正パッチが未適用のリモートデスクトッププロトコルのゲートウェイは、攻撃者によるログインへのブルートフォース攻撃と、マルウェアの手動での起動を許してしまいます。

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

ランサムウェアの攻撃者は、vssadmin.exe のようなツールを使って Windows のシャドウコピーを削除し、ローカルでの復元を阻止することがよくあります。 [1]

2. セキュリティの洞察

共通鍵の AES-256 は通常、ファイルのペイロードの暗号化に使われ、そのうえで公開鍵の RSA によってロックされます。

3. セキュリティの洞察

ランサムウェア攻撃を受けた後の復旧には数週間かかることがあるため、テスト済みのオフラインバックアップが重要です。

4. セキュリティの洞察

FBIは身代金の支払いを支持しておらず、支払ってもデータが戻ってくる保証はないと警告しています。 [2]

5. セキュリティの洞察

災害復旧計画(DRP)では、目標復旧時間(RTO)と目標復旧時点(RPO)を定めておく必要があります。

6. セキュリティの洞察

FBIは、暗号化され、変更や削除ができない不変(イミュータブル)のバックアップを推奨しています。 [3]

7. セキュリティの豆知識

ランサムウェアの開発者は、従来のシグネチャベースのウイルス対策スキャナーを回避するために、高度な難読化技術を利用します。

8. セキュリティの豆知識

ネットワークのセグメンテーションは横方向の移動を制限し、ランサムウェアが最初に感染したホストの先に広がるのを食い止めるのに役立ちます。 [3]

9. セキュリティの豆知識

リモートデスクトッププロトコル(RDP)のように、公開されていて保護が不十分なリモートサービスは、ランサムウェアの一般的な侵入口です。 [1]

10. セキュリティの洞察

CISA は、多くのランサムウェアが到達可能なバックアップを探して削除するため、暗号化したバックアップをオフラインで保管するよう助言しています。 [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] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

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

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

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

ランサムウェア攻撃の主なメカニズムは何ですか? → システムへのアクセスを拒否するための、ユーザーファイルの暗号化

2 問題 2 正解: A

指導メモ

オフライン(コールド)バックアップとは何ですか? → マルウェアの拡散から守るため、ネットワークから切り離された保管用コピー

3 問題 3 正解: A

指導メモ

ランサムウェア攻撃の際、セキュリティチームは感染したシステムをどのように隔離すべきですか? → すぐにネットワークケーブルを抜き、ワイヤレスインターフェースを無効にする

4 問題 4 正解: A

指導メモ

セキュリティ機関がランサムウェアの要求に応じないよう勧めるのはなぜですか? → 資金を支払うと攻撃者を助長し、復号鍵が届く保証もない

5 問題 5 正解: A

指導メモ

災害復旧計画(DRP)とは何ですか? → システムが侵害された後に、業務とデータを復旧するための体系的なプロセス

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

ランサムウェアのペイロードは、ネットワークに接続されたオンラインバックアップに簡単に拡散することがあります。

7 問題 7 正解: 誤り

指導メモ

誤り: FBIは、支払ってもデータが戻ってくる保証はないと警告しています。

8 問題 8 正解: 正しい

指導メモ

正しい: CISAは、感染したホストを取り外すか、ネットワークをオフラインにして、拡散を封じ込めることを推奨しています。

9 問題 9 正解: 誤り

指導メモ

誤り: ランサムウェアは通常、AESなどの高速な共通鍵暗号でファイルを暗号化します。

10 問題 10 正解: 正しい

指導メモ

データ復元の手順を定期的にテストすることは、災害復旧の重要な要素です。

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

C 1. 暗号化	E 2. ペイロード	F 3. コールドバックアップ	A 4. 隔離
H 5. 身代金	G 6. 復旧	D 7. 災害	B 8. トロイの木馬

チェックポイント 3: 解答 – 重要用語

1 暗号化	2 ペイロード	3 コールドバックアップ	4 隔離
5 身代金	6 復旧		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 C – カンセン	2 H – ネットワーク	3 A – アンゴウカ	4 E – ミノシロキン
5 D – カクリ	6 G – サイガイ	7 B – ペイロード	8 F – フツキユウ

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、ペイロード、コールドバックアップ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。

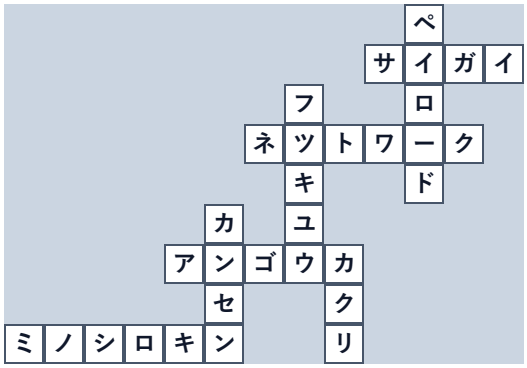
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

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

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: サイガイ システムに大きな障害が起きる事態 (4 文字)

4 ヨコ: ネツトワーク 感染したシステムを切り離す対象となる通信網 (6 文字)

6 ヨコ: アンゴウカ ファイルを暗号で使えなくすること (5 文字)

8 ヨコ: ミノシロキン 暗号鍵と引き換えに支払いを求める要求 (6 文字)

タテのカギ

1 タテ: ペイロード 悪意のあるソフトウェアの実行部分 (5 文字)

3 タテ: フツキユウ バックアップからデータベースを元に戻すこと (5 文字)

5 タテ: カンセン マルウェアに侵され、ネットワーク上で被害が広がった状態 (4 文字)

7 タテ: カクリ 感染したネットワークシステムを切り離すこと (3 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. カセンン — **カンセン**
3. ミシロンキノ — **ミノシロキン**
4. イガサイ — **サイガイ**
5. ロドペーイ — **ペイロード**
6. クリカ — **カクリ**
7. ユウフキツ — **フツキユウ**
8. トクネーワツ — **ネツトワーク**

秘密の暗号チャレンジ 解答

"バックアップカラ データヲ フッキュウスル"

ケーススタディの解答

A ケーススタディ 1: 企業でのランサムウェアのペイロードの封じ込め 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: 企業のローカルエリアネットワークが、稼働中のランサムウェアに侵害されました。主要なファイルサーバーで、ファイルの拡張子が .locked と表示され始めています。
- 推奨される対策と解決策: 影響を受けたすべてのサーバーをローカルエリアネットワークから切断します。アクティブな管理セッションを終了します。安全で書き込みロックされたオフラインバックアップシステムから、侵害されていないファイルを復元します。

B ケーススタディ 2: オフラインバックアップ構成の評価 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、メインのローカルネットワークがランサムウェアに完全に乗っ取られた場合でも、バックアップが侵害されるリスクを減らせるデータバックアップ戦略を設計したいと考えています。
- 推奨される戦略と解決策: WORM (write-once-read-many) ストレージを導入します。バックアップシステムをすべてのネットワークから切断して論理的なエアギャップを作り、毎日物理メディアのローテーションを実施します。