情報セキュリティマネジメント試験 問題PDF

Q0001

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント1：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

次の説明に最も合う用語はどれか。情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

A. 情報セキュリティ事象
B. 情報セキュリティインシデント
C. 封じ込め
D. RTO

答え・解説

Q0001 正答：A. 情報セキュリティ事象

解説：情報セキュリティ事象は、情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事。ほかの選択肢は目的又は適用場面が異なる。

Q0002

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント2：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

情報セキュリティ事象の説明として最も適切なものはどれか。

A. 事業運営を損なう可能性がある単独又は一連の望ましくない事象
B. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
C. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
D. 災害や障害の発生後、業務を復旧させるまでの目標時間

答え・解説

Q0002 正答：B. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

解説：情報セキュリティ事象の要点は「情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0003

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント3：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

用語と説明の組合せとして適切なものはどれか。論点は「情報セキュリティ事象」である。

A. 情報セキュリティインシデント：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
B. 封じ込め：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
C. 情報セキュリティ事象：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
D. RTO：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

答え・解説

Q0003 正答：C. 情報セキュリティ事象：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

解説：正しい組合せは「情報セキュリティ事象：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0004

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント4：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

「情報セキュリティ事象」は、情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。情報セキュリティ事象は情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事。実務では対象、目的、前提条件を併せて確認する。

Q0005

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント5：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

組織が「情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事」ために採用すべき概念又は仕組みはどれか。

A. 情報セキュリティ事象
B. 情報セキュリティインシデント
C. 封じ込め
D. RTO

答え・解説

Q0005 正答：A. 情報セキュリティ事象

解説：この目的に対応するのは情報セキュリティ事象である。情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事という機能・考え方を持つためである。

Q0006

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント6：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

「情報セキュリティ事象」について、誤解を避けるための説明として最も適切なものはどれか。

A. 災害や障害の発生後、業務を復旧させるまでの目標時間
B. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
C. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
D. 事業運営を損なう可能性がある単独又は一連の望ましくない事象

答え・解説

Q0006 正答：B. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

解説：情報セキュリティ事象は情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント7：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

「情報セキュリティ事象」は、事業運営を損なう可能性がある単独又は一連の望ましくない事象。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述は情報セキュリティインシデントの説明である。情報セキュリティ事象は情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事。

Q0008

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント8：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

次の状況で中心となる論点はどれか。「情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事」ことが求められている。

A. 封じ込め
B. RTO
C. 情報セキュリティインシデント
D. 情報セキュリティ事象

答え・解説

Q0008 正答：D. 情報セキュリティ事象

解説：中心となる論点は情報セキュリティ事象である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0009

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント9：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

情報セキュリティ事象を選定するときは、「情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0009 正答：○
解説：正しい。情報セキュリティ事象の選定・運用では、情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事という目的との適合を確認する。

Q0010

インシデント対応・事業継続
タグ：情報セキュリティ事象
用語：情報セキュリティ事象の確認ポイント10：情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

情報セキュリティ事象は、情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0010 正答：×
解説：誤り。情報セキュリティ事象はまさに情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事という意味を持つ。

Q0011

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント1：事業運営を損なう可能性がある単独又は一連の望ましくない事象

次の説明に最も合う用語はどれか。事業運営を損なう可能性がある単独又は一連の望ましくない事象

A. トリアージ
B. 情報セキュリティインシデント
C. 根絶
D. RPO

答え・解説

Q0011 正答：B. 情報セキュリティインシデント

解説：情報セキュリティインシデントは、事業運営を損なう可能性がある単独又は一連の望ましくない事象。ほかの選択肢は目的又は適用場面が異なる。

Q0012

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント2：事業運営を損なう可能性がある単独又は一連の望ましくない事象

情報セキュリティインシデントの説明として最も適切なものはどれか。

A. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
C. 事業運営を損なう可能性がある単独又は一連の望ましくない事象
D. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

答え・解説

Q0012 正答：C. 事業運営を損なう可能性がある単独又は一連の望ましくない事象

解説：情報セキュリティインシデントの要点は「事業運営を損なう可能性がある単独又は一連の望ましくない事象」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0013

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント3：事業運営を損なう可能性がある単独又は一連の望ましくない事象

用語と説明の組合せとして適切なものはどれか。論点は「情報セキュリティインシデント」である。

A. トリアージ：事業運営を損なう可能性がある単独又は一連の望ましくない事象
B. 根絶：事業運営を損なう可能性がある単独又は一連の望ましくない事象
C. RPO：事業運営を損なう可能性がある単独又は一連の望ましくない事象
D. 情報セキュリティインシデント：事業運営を損なう可能性がある単独又は一連の望ましくない事象

答え・解説

Q0013 正答：D. 情報セキュリティインシデント：事業運営を損なう可能性がある単独又は一連の望ましくない事象

解説：正しい組合せは「情報セキュリティインシデント：事業運営を損なう可能性がある単独又は一連の望ましくない事象」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0014

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント4：事業運営を損なう可能性がある単独又は一連の望ましくない事象

「情報セキュリティインシデント」は、事業運営を損なう可能性がある単独又は一連の望ましくない事象。

A. ○
B. ×

答え・解説

Q0014 正答：○

解説：正しい。情報セキュリティインシデントは事業運営を損なう可能性がある単独又は一連の望ましくない事象。実務では対象、目的、前提条件を併せて確認する。

Q0015

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント5：事業運営を損なう可能性がある単独又は一連の望ましくない事象

組織が「事業運営を損なう可能性がある単独又は一連の望ましくない事象」ために採用すべき概念又は仕組みはどれか。

A. トリアージ
B. 情報セキュリティインシデント
C. 根絶
D. RPO

答え・解説

Q0015 正答：B. 情報セキュリティインシデント
解説：この目的に対応するのは情報セキュリティインシデントである。事業運営を損なう可能性がある単独又は一連の望ましくない事象という機能・考え方を持つためである。

Q0016

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント6：事業運営を損なう可能性がある単独又は一連の望ましくない事象

「情報セキュリティインシデント」について、誤解を避けるための説明として最も適切なものはどれか。

A. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
C. 事業運営を損なう可能性がある単独又は一連の望ましくない事象
D. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

答え・解説

Q0016 正答：C. 事業運営を損なう可能性がある単独又は一連の望ましくない事象
解説：情報セキュリティインシデントは事業運営を損なう可能性がある単独又は一連の望ましくない事象。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0017

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント7：事業運営を損なう可能性がある単独又は一連の望ましくない事象

「情報セキュリティインシデント」は、受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業。

A. ○
B. ×

答え・解説

Q0017 正答：×

解説：誤り。記述はトリアージの説明である。情報セキュリティインシデントは事業運営を損なう可能性がある単独又は一連の望ましくない事象。

Q0018

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント8：事業運営を損なう可能性がある単独又は一連の望ましくない事象

次の状況で中心となる論点はどれか。「事業運営を損なう可能性がある単独又は一連の望ましくない事象」ことが求められている。

A. 情報セキュリティインシデント
B. 根絶
C. RPO
D. トリアージ

答え・解説

Q0018 正答：A. 情報セキュリティインシデント

解説：中心となる論点は情報セキュリティインシデントである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0019

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント9：事業運営を損なう可能性がある単独又は一連の望ましくない事象

情報セキュリティインシデントは名称だけで判断できるため、対象や目的を確認する必要はない。

A. ○
B. ×

答え・解説

Q0019 正答：×

解説：誤り。情報セキュリティインシデントは事業運営を損なう可能性がある単独又は一連の望ましくない事象という概念であり、対象・目的・前提条件の確認が必要である。

Q0020

インシデント対応・事業継続
タグ：情報セキュリティインシデント
用語：情報セキュリティインシデントの確認ポイント10：事業運営を損なう可能性がある単独又は一連の望ましくない事象

情報セキュリティインシデントと他の類似概念を区別する際は、「事業運営を損なう可能性がある単独又は一連の望ましくない事象」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0020 正答：○

解説：正しい。情報セキュリティインシデントの定義は事業運営を損なう可能性がある単独又は一連の望ましくない事象であり、類似概念との区別に使える。

Q0021

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント1：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

次の説明に最も合う用語はどれか。受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

A. 封じ込め
B. 復旧
C. トリアージ
D. 事業継続計画

答え・解説

Q0021 正答：C. トリアージ

解説：トリアージは、受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業。ほかの選択肢は目的又は適用場面が異なる。

Q0022

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント2：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

トリアージの説明として最も適切なものはどれか。

A. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
B. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
C. 重大な中断時にも重要業務を継続又は早期復旧するための計画
D. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

答え・解説

Q0022 正答：D. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

解説：トリアージの要点は「受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0023

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント3：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

用語と説明の組合せとして適切なものはどれか。論点は「トリアージ」である。

A. トリアージ：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
B. 封じ込め：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
C. 復旧：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
D. 事業継続計画：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

答え・解説

Q0023 正答：A. トリアージ：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

解説：正しい組合せは「トリアージ：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0024

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント4：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

「トリアージ」は、受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業。

A. ○
B. ×

答え・解説

Q0024 正答：○

解説：正しい。トリアージは受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業。実務では対象、目的、前提条件を併せて確認する。

Q0025

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント5：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

組織が「受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業」ために採用すべき概念又は仕組みはどれか。

A. 封じ込め
B. 復旧
C. トリアージ
D. 事業継続計画

答え・解説

Q0025 正答：C. トリアージ

解説：この目的に対応するのはトリアージである。受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業という機能・考え方を持つためである。

Q0026

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント6：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

「トリアージ」について、誤解を避けるための説明として最も適切なものはどれか。

A. 重大な中断時にも重要業務を継続又は早期復旧するための計画
B. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
C. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
D. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

答え・解説

Q0026 正答：D. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

解説：トリアージは受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0027

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント7：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
「トリアージ」は、感染拡大や不正アクセスの継続を止めるため対象を隔離する対応。
A. ○
B. ×

答え・解説

Q0027 正答：×
解説：誤り。記述は封じ込めの説明である。トリアージは受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業。

Q0028

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント8：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
次の状況で中心となる論点はどれか。「受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業」ことが求められている。
A. 復旧
B. トリアージ
C. 事業継続計画
D. 封じ込め

答え・解説

Q0028 正答：B. トリアージ
解説：中心となる論点はトリアージである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0029

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント9：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

トリアージを選定するときは、「受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0029 正答：○

解説：正しい。トリアージの選定・運用では、受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業という目的との適合を確認する。

Q0030

インシデント対応・事業継続
タグ：トリアージ
用語：トリアージの確認ポイント10：受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

トリアージは、受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0030 正答：×

解説：誤り。トリアージはまさに受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業という意味を持つ。

Q0031

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント1：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
次の説明に最も合う用語はどれか。感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

A. 根絶
B. CSIRT
C. 情報セキュリティ事象
D. 封じ込め

答え・解説

Q0031 正答：D. 封じ込め
解説：封じ込めは、感染拡大や不正アクセスの継続を止めるため対象を隔離する対応。ほかの選択肢は目的又は適用場面が異なる。

Q0032

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント2：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
封じ込めの説明として最も適切なものはどれか。

A. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
C. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム
D. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

答え・解説

Q0032 正答：A. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
解説：封じ込めの要点は「感染拡大や不正アクセスの継続を止めるため対象を隔離する対応」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0033

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント3：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

用語と説明の組合せとして適切なものはどれか。論点は「封じ込め」である。

A. 根絶：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
B. 封じ込め：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
C. CSIRT：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
D. 情報セキュリティ事象：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

答え・解説

Q0033 正答：B. 封じ込め：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

解説：正しい組合せは「封じ込め：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0034

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント4：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

「封じ込め」は、感染拡大や不正アクセスの継続を止めるため対象を隔離する対応。

A. ○
B. ×

答え・解説

Q0034 正答：○

解説：正しい。封じ込めは感染拡大や不正アクセスの継続を止めるため対象を隔離する対応。実務では対象、目的、前提条件を併せて確認する。

Q0035

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント5：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

組織が「感染拡大や不正アクセスの継続を止めるため対象を隔離する対応」ために採用すべき概念又は仕組みはどれか。

A. 根絶
B. CSIRT
C. 情報セキュリティ事象
D. 封じ込め

答え・解説

Q0035 正答：D. 封じ込め
解説：この目的に対応するのは封じ込めである。感染拡大や不正アクセスの継続を止めるため対象を隔離する対応という機能・考え方を持つためである。

Q0036

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント6：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

「封じ込め」について、誤解を避けるための説明として最も適切なものはどれか。

A. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
B. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
C. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム
D. マルウェア、侵入経路、不要アカウントなど原因を除去する対応

答え・解説

Q0036 正答：A. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
解説：封じ込めは感染拡大や不正アクセスの継続を止めるため対象を隔離する対応。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0037

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント7：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

「封じ込め」は、マルウェア、侵入経路、不要アカウントなど原因を除去する対応。

A. ○
B. ×

答え・解説

Q0037 正答：×

解説：誤り。記述は根絶の説明である。封じ込めは感染拡大や不正アクセスの継続を止めるため対象を隔離する対応。

Q0038

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント8：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

次の状況で中心となる論点はどれか。「感染拡大や不正アクセスの継続を止めるため対象を隔離する対応」ことが求められている。

A. CSIRT
B. 情報セキュリティ事象
C. 封じ込め
D. 根絶

答え・解説

Q0038 正答：C. 封じ込め

解説：中心となる論点は封じ込めである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0039

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント9：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

封じ込めは名称だけで判断できるため、対象や目的を確認する必要はない。

A. ○
B. ×

答え・解説

Q0039 正答：×

解説：誤り。封じ込めは感染拡大や不正アクセスの継続を止めるため対象を隔離する対応という概念であり、対象・目的・前提条件の確認が必要である。

Q0040

インシデント対応・事業継続
タグ：封じ込め
用語：封じ込めの確認ポイント10：感染拡大や不正アクセスの継続を止めるため対象を隔離する対応

封じ込めと他の類似概念を区別する際は、「感染拡大や不正アクセスの継続を止めるため対象を隔離する対応」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。封じ込めの定義は感染拡大や不正アクセスの継続を止めるため対象を隔離する対応であり、類似概念との区別に使える。

Q0041

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント1：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

次の説明に最も合う用語はどれか。マルウェア、侵入経路、不要アカウントなど原因を除去する対応

A. 根絶
B. 復旧
C. RTO
D. 情報セキュリティインシデント

答え・解説

Q0041 正答：A. 根絶
解説：根絶は、マルウェア、侵入経路、不要アカウントなど原因を除去する対応。ほかの選択肢は目的又は適用場面が異なる。

Q0042

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント2：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

根絶の説明として最も適切なものはどれか。

A. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
C. 災害や障害の発生後、業務を復旧させるまでの目標時間
D. 事業運営を損なう可能性がある単独又は一連の望ましくない事象

答え・解説

Q0042 正答：B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
解説：根絶の要点は「マルウェア、侵入経路、不要アカウントなど原因を除去する対応」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0043

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント3：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

用語と説明の組合せとして適切なものはどれか。論点は「根絶」である。

A. 復旧：マルウェア、侵入経路、不要アカウントなど原因を除去する対応
B. RTO：マルウェア、侵入経路、不要アカウントなど原因を除去する対応
C. 根絶：マルウェア、侵入経路、不要アカウントなど原因を除去する対応
D. 情報セキュリティインシデント：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

答え・解説

Q0043 正答：C. 根絶：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

解説：正しい組合せは「根絶：マルウェア、侵入経路、不要アカウントなど原因を除去する対応」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0044

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント4：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

「根絶」は、マルウェア、侵入経路、不要アカウントなど原因を除去する対応。

A. ○
B. ×

答え・解説

Q0044 正答：○

解説：正しい。根絶はマルウェア、侵入経路、不要アカウントなど原因を除去する対応。実務では対象、目的、前提条件を併せて確認する。

Q0045

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント5：マルウェア、侵入経路、不要アカウントなど原因を除去する対応
組織が「マルウェア、侵入経路、不要アカウントなど原因を除去する対応」ために採用すべき概念又は仕組みはどれか。

A. 根絶
B. 復旧
C. RTO
D. 情報セキュリティインシデント

答え・解説

Q0045 正答：A. 根絶
解説：この目的に対応するのは根絶である。マルウェア、侵入経路、不要アカウントなど原因を除去する対応という機能・考え方を持つためである。

Q0046

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント6：マルウェア、侵入経路、不要アカウントなど原因を除去する対応
「根絶」について、誤解を避けるための説明として最も適切なものはどれか。

A. 事業運営を損なう可能性がある単独又は一連の望ましくない事象
B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
C. 災害や障害の発生後、業務を復旧させるまでの目標時間
D. 安全を確認しながらシステムや業務を正常な状態へ戻す対応

答え・解説

Q0046 正答：B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
解説：根絶はマルウェア、侵入経路、不要アカウントなど原因を除去する対応。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0047

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント7：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

「根絶」は、安全を確認しながらシステムや業務を正常な状態へ戻す対応。

A. ○
B. ×

答え・解説

Q0047 正答：×

解説：誤り。記述は復旧の説明である。根絶はマルウェア、侵入経路、不要アカウントなど原因を除去する対応。

Q0048

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント8：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

次の状況で中心となる論点はどれか。「マルウェア、侵入経路、不要アカウントなど原因を除去する対応」ことが求められている。

A. RTO
B. 情報セキュリティインシデント
C. 復旧
D. 根絶

答え・解説

Q0048 正答：D. 根絶

解説：中心となる論点は根絶である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0049

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント9：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

根絶を選定するときは、「マルウェア、侵入経路、不要アカウントなど原因を除去する対応」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0049 正答：○

解説：正しい。根絶の選定・運用では、マルウェア、侵入経路、不要アカウントなど原因を除去する対応という目的との適合を確認する。

Q0050

インシデント対応・事業継続
タグ：根絶
用語：根絶の確認ポイント10：マルウェア、侵入経路、不要アカウントなど原因を除去する対応

根絶は、マルウェア、侵入経路、不要アカウントなど原因を除去する対応という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0050 正答：×

解説：誤り。根絶はまさにマルウェア、侵入経路、不要アカウントなど原因を除去する対応という意味を持つ。

Q0051

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント1：安全を確認しながらシステムや業務を正常な状態へ戻す対応

次の説明に最も合う用語はどれか。安全を確認しながらシステムや業務を正常な状態へ戻す対応

A. CSIRT
B. 復旧
C. RPO
D. トリアージ

答え・解説

Q0051 正答：B. 復旧
解説：復旧は、安全を確認しながらシステムや業務を正常な状態へ戻す対応。ほかの選択肢は目的又は適用場面が異なる。

Q0052

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント2：安全を確認しながらシステムや業務を正常な状態へ戻す対応

復旧の説明として最も適切なものはどれか。

A. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム
B. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
C. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
D. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業

答え・解説

Q0052 正答：C. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
解説：復旧の要点は「安全を確認しながらシステムや業務を正常な状態へ戻す対応」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0053

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント3：安全を確認しながらシステムや業務を正常な状態へ戻す対応

用語と説明の組合せとして適切なものはどれか。論点は「復旧」である。

A. CSIRT：安全を確認しながらシステムや業務を正常な状態へ戻す対応
B. RPO：安全を確認しながらシステムや業務を正常な状態へ戻す対応
C. トリアージ：安全を確認しながらシステムや業務を正常な状態へ戻す対応
D. 復旧：安全を確認しながらシステムや業務を正常な状態へ戻す対応

答え・解説

Q0053 正答：D. 復旧：安全を確認しながらシステムや業務を正常な状態へ戻す対応

解説：正しい組合せは「復旧：安全を確認しながらシステムや業務を正常な状態へ戻す対応」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0054

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント4：安全を確認しながらシステムや業務を正常な状態へ戻す対応

「復旧」は、安全を確認しながらシステムや業務を正常な状態へ戻す対応。

A. ○
B. ×

答え・解説

Q0054 正答：○

解説：正しい。復旧は安全を確認しながらシステムや業務を正常な状態へ戻す対応。実務では対象、目的、前提条件を併せて確認する。

Q0055

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント5：安全を確認しながらシステムや業務を正常な状態へ戻す対応

組織が「安全を確認しながらシステムや業務を正常な状態へ戻す対応」ために採用すべき概念又は仕組みはどれか。

A. CSIRT
B. 復旧
C. RPO
D. トリアージ

答え・解説

Q0055 正答：B. 復旧
解説：この目的に対応するのは復旧である。安全を確認しながらシステムや業務を正常な状態へ戻す対応という機能・考え方を持つためである。

Q0056

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント6：安全を確認しながらシステムや業務を正常な状態へ戻す対応

「復旧」について、誤解を避けるための説明として最も適切なものはどれか。

A. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
B. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
C. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
D. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

答え・解説

Q0056 正答：C. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
解説：復旧は安全を確認しながらシステムや業務を正常な状態へ戻す対応。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0057

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント7：安全を確認しながらシステムや業務を正常な状態へ戻す対応

「復旧」は、インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム。

A. ○
B. ×

答え・解説

Q0057 正答：×

解説：誤り。記述はCSIRTの説明である。復旧は安全を確認しながらシステムや業務を正常な状態へ戻す対応。

Q0058

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント8：安全を確認しながらシステムや業務を正常な状態へ戻す対応

次の状況で中心となる論点はどれか。「安全を確認しながらシステムや業務を正常な状態へ戻す対応」ことが求められている。

A. 復旧
B. RPO
C. トリアージ
D. CSIRT

答え・解説

Q0058 正答：A. 復旧

解説：中心となる論点は復旧である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0059

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント9：安全を確認しながらシステムや業務を正常な状態へ戻す対応

復旧は名称だけで判断できるため、対象や目的を確認する必要はない。

A. ○
B. ×

答え・解説

Q0059 正答：×

解説：誤り。復旧は安全を確認しながらシステムや業務を正常な状態へ戻す対応という概念であり、対象・目的・前提条件の確認が必要である。

Q0060

インシデント対応・事業継続
タグ：復旧
用語：復旧の確認ポイント10：安全を確認しながらシステムや業務を正常な状態へ戻す対応

復旧と他の類似概念を区別する際は、「安全を確認しながらシステムや業務を正常な状態へ戻す対応」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0060 正答：○

解説：正しい。復旧の定義は安全を確認しながらシステムや業務を正常な状態へ戻す対応であり、類似概念との区別に使える。

Q0061

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント1：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

次の説明に最も合う用語はどれか。インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

A. RTO
B. 事業継続計画
C. CSIRT
D. 封じ込め

答え・解説

Q0061 正答：C. CSIRT

解説：CSIRTは、インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム。ほかの選択肢は目的又は適用場面が異なる。

Q0062

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント2：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

CSIRTの説明として最も適切なものはどれか。

A. 災害や障害の発生後、業務を復旧させるまでの目標時間
B. 重大な中断時にも重要業務を継続又は早期復旧するための計画
C. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
D. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

答え・解説

Q0062 正答：D. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

解説：CSIRTの要点は「インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0063

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント3：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

用語と説明の組合せとして適切なものはどれか。論点は「CSIRT」である。

A. CSIRT：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム
B. RTO：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム
C. 事業継続計画：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム
D. 封じ込め：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

答え・解説

Q0063 正答：A. CSIRT：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

解説：正しい組合せは「CSIRT：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0064

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント4：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

「CSIRT」は、インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム。

A. ○
B. ×

答え・解説

Q0064 正答：○

解説：正しい。CSIRTはインシデントの受付、分析、対応調整、再発防止を担う組織又はチーム。実務では対象、目的、前提条件を併せて確認する。

Q0065

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント5：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

組織が「インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム」ために採用すべき概念又は仕組みはどれか。

A. RTO
B. 事業継続計画
C. CSIRT
D. 封じ込め

答え・解説

Q0065 正答：C. CSIRT

解説：この目的に対応するのはCSIRTである。インシデントの受付、分析、対応調整、再発防止を担う組織又はチームという機能・考え方を持つためである。

Q0066

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント6：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

「CSIRT」について、誤解を避けるための説明として最も適切なものはどれか。

A. 感染拡大や不正アクセスの継続を止めるため対象を隔離する対応
B. 重大な中断時にも重要業務を継続又は早期復旧するための計画
C. 災害や障害の発生後、業務を復旧させるまでの目標時間
D. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

答え・解説

Q0066 正答：D. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

解説：CSIRTはインシデントの受付、分析、対応調整、再発防止を担う組織又はチーム。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0067

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント7：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

「CSIRT」は、災害や障害の発生後、業務を復旧させるまでの目標時間。

A. ○
B. ×

答え・解説

Q0067 正答：×

解説：誤り。記述はRTOの説明である。CSIRTはインシデントの受付、分析、対応調整、再発防止を担う組織又はチーム。

Q0068

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント8：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

次の状況で中心となる論点はどれか。「インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム」ことが求められている。

A. 事業継続計画
B. CSIRT
C. 封じ込め
D. RTO

答え・解説

Q0068 正答：B. CSIRT

解説：中心となる論点はCSIRTである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0069

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント9：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

CSIRTを選定するときは、「インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0069 正答：○

解説：正しい。CSIRTの選定・運用では、インシデントの受付、分析、対応調整、再発防止を担う組織又はチームという目的との適合を確認する。

Q0070

インシデント対応・事業継続
タグ：CSIRT
用語：CSIRTの確認ポイント10：インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

CSIRTは、インシデントの受付、分析、対応調整、再発防止を担う組織又はチームという説明とは無関係である。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。CSIRTはまさにインシデントの受付、分析、対応調整、再発防止を担う組織又はチームという意味を持つ。

Q0071

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント1：災害や障害の発生後、業務を復旧させるまでの目標時間

次の説明に最も合う用語はどれか。災害や障害の発生後、業務を復旧させるまでの目標時間

A. RPO
B. 情報セキュリティ事象
C. 根絶
D. RTO

答え・解説

Q0071 正答：D. RTO

解説：RTOは、災害や障害の発生後、業務を復旧させるまでの目標時間。ほかの選択肢は目的又は適用場面が異なる。

Q0072

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント2：災害や障害の発生後、業務を復旧させるまでの目標時間

RTOの説明として最も適切なものはどれか。

A. 災害や障害の発生後、業務を復旧させるまでの目標時間
B. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
C. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
D. マルウェア、侵入経路、不要アカウントなど原因を除去する対応

答え・解説

Q0072 正答：A. 災害や障害の発生後、業務を復旧させるまでの目標時間

解説：RTOの要点は「災害や障害の発生後、業務を復旧させるまでの目標時間」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0073

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント3：災害や障害の発生後、業務を復旧させるまでの目標時間
用語と説明の組合せとして適切なものはどれか。論点は「RTO」である。

A. RPO：災害や障害の発生後、業務を復旧させるまでの目標時間
B. RTO：災害や障害の発生後、業務を復旧させるまでの目標時間
C. 情報セキュリティ事象：災害や障害の発生後、業務を復旧させるまでの目標時間
D. 根絶：災害や障害の発生後、業務を復旧させるまでの目標時間

答え・解説

Q0073 正答：B. RTO：災害や障害の発生後、業務を復旧させるまでの目標時間
解説：正しい組合せは「RTO：災害や障害の発生後、業務を復旧させるまでの目標時間」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0074

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント4：災害や障害の発生後、業務を復旧させるまでの目標時間
「RTO」は、災害や障害の発生後、業務を復旧させるまでの目標時間。

A. ○
B. ×

答え・解説

Q0074 正答：○
解説：正しい。RTOは災害や障害の発生後、業務を復旧させるまでの目標時間。実務では対象、目的、前提条件を併せて確認する。

Q0075

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント5：災害や障害の発生後、業務を復旧させるまでの目標時間

組織が「災害や障害の発生後、業務を復旧させるまでの目標時間」ために採用すべき概念又は仕組みはどれか。

A. RPO
B. 情報セキュリティ事象
C. 根絶
D. RTO

答え・解説

Q0075 正答：D. RTO
解説：この目的に対応するのはRTOである。災害や障害の発生後、業務を復旧させるまでの目標時間という機能・考え方を持つためである。

Q0076

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント6：災害や障害の発生後、業務を復旧させるまでの目標時間

「RTO」について、誤解を避けるための説明として最も適切なものはどれか。

A. 災害や障害の発生後、業務を復旧させるまでの目標時間
B. マルウェア、侵入経路、不要アカウントなど原因を除去する対応
C. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
D. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

答え・解説

Q0076 正答：A. 災害や障害の発生後、業務を復旧させるまでの目標時間
解説：RTOは災害や障害の発生後、業務を復旧させるまでの目標時間。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0077

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント7：災害や障害の発生後、業務を復旧させるまでの目標時間

「RTO」は、復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点。

A. ○
B. ×

答え・解説

Q0077 正答：×

解説：誤り。記述はRPOの説明である。RTOは災害や障害の発生後、業務を復旧させるまでの目標時間。

Q0078

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント8：災害や障害の発生後、業務を復旧させるまでの目標時間

次の状況で中心となる論点はどれか。「災害や障害の発生後、業務を復旧させるまでの目標時間」ことが求められている。

A. 情報セキュリティ事象
B. 根絶
C. RTO
D. RPO

答え・解説

Q0078 正答：C. RTO

解説：中心となる論点はRTOである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0079

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント9：災害や障害の発生後、業務を復旧させるまでの目標時間

RTOは名称だけで判断できるため、対象や目的を確認する必要はない。

A. ○
B. ×

答え・解説

Q0079 正答：×

解説：誤り。RTOは災害や障害の発生後、業務を復旧させるまでの目標時間という概念であり、対象・目的・前提条件の確認が必要である。

Q0080

インシデント対応・事業継続
タグ：RTO
用語：RTOの確認ポイント10：災害や障害の発生後、業務を復旧させるまでの目標時間

RTOと他の類似概念を区別する際は、「災害や障害の発生後、業務を復旧させるまでの目標時間」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0080 正答：○

解説：正しい。RTOの定義は災害や障害の発生後、業務を復旧させるまでの目標時間であり、類似概念との区別に使える。

Q0081

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント1：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

次の説明に最も合う用語はどれか。復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

A. RPO
B. 事業継続計画
C. 情報セキュリティインシデント
D. 復旧

答え・解説

Q0081 正答：A. RPO

解説：RPOは、復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点。ほかの選択肢は目的又は適用場面が異なる。

Q0082

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント2：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

RPOの説明として最も適切なものはどれか。

A. 重大な中断時にも重要業務を継続又は早期復旧するための計画
B. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
C. 事業運営を損なう可能性がある単独又は一連の望ましくない事象
D. 安全を確認しながらシステムや業務を正常な状態へ戻す対応

答え・解説

Q0082 正答：B. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

解説：RPOの要点は「復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0083

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント3：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
用語と説明の組合せとして適切なものはどれか。論点は「RPO」である。
A. 事業継続計画：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
B. 情報セキュリティインシデント：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
C. RPO：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
D. 復旧：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

答え・解説

Q0083 正答：C. RPO：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
解説：正しい組合せは「RPO：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0084

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント4：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
「RPO」は、復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点。
A. ○
B. ×

答え・解説

Q0084 正答：○
解説：正しい。RPOは復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点。実務では対象、目的、前提条件を併せて確認する。

Q0085

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント5：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

組織が「復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点」ために採用すべき概念又は仕組みはどれか。

A. RPO
B. 事業継続計画
C. 情報セキュリティインシデント
D. 復旧

答え・解説

Q0085 正答：A. RPO

解説：この目的に対応するのはRPOである。復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点という機能・考え方を持つためである。

Q0086

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント6：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

「RPO」について、誤解を避けるための説明として最も適切なものはどれか。

A. 安全を確認しながらシステムや業務を正常な状態へ戻す対応
B. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点
C. 事業運営を損なう可能性がある単独又は一連の望ましくない事象
D. 重大な中断時にも重要業務を継続又は早期復旧するための計画

答え・解説

Q0086 正答：B. 復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

解説：RPOは復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0087

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント7：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

「RPO」は、重大な中断時にも重要業務を継続又は早期復旧するための計画。

A. ○
B. ×

答え・解説

Q0087 正答：×

解説：誤り。記述は事業継続計画の説明である。RPOは復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点。

Q0088

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント8：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

次の状況で中心となる論点はどれか。「復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点」ことが求められている。

A. 情報セキュリティインシデント
B. 復旧
C. 事業継続計画
D. RPO

答え・解説

Q0088 正答：D. RPO

解説：中心となる論点はRPOである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0089

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント9：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

RPOを選定するときは、「復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0089 正答：○

解説：正しい。RPOの選定・運用では、復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点という目的との適合を確認する。

Q0090

インシデント対応・事業継続
タグ：RPO
用語：RPOの確認ポイント10：復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点

RPOは、復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0090 正答：×

解説：誤り。RPOはまさに復旧時にどの時点までデータを戻せればよいかを示す目標復旧時点という意味を持つ。

Q0091

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント1：重大な中断時にも重要業務を継続又は早期復旧するための計画

次の説明に最も合う用語はどれか。重大な中断時にも重要業務を継続又は早期復旧するための計画

A. 情報セキュリティ事象
B. 事業継続計画
C. トリアージ
D. CSIRT

答え・解説

Q0091 正答：B. 事業継続計画

解説：事業継続計画は、重大な中断時にも重要業務を継続又は早期復旧するための計画。ほかの選択肢は目的又は適用場面が異なる。

Q0092

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント2：重大な中断時にも重要業務を継続又は早期復旧するための計画

事業継続計画の説明として最も適切なものはどれか。

A. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事
B. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
C. 重大な中断時にも重要業務を継続又は早期復旧するための計画
D. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム

答え・解説

Q0092 正答：C. 重大な中断時にも重要業務を継続又は早期復旧するための計画

解説：事業継続計画の要点は「重大な中断時にも重要業務を継続又は早期復旧するための計画」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0093

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント3：重大な中断時にも重要業務を継続又は早期復旧するための計画

用語と説明の組合せとして適切なものはどれか。論点は「事業継続計画」である。

A. 情報セキュリティ事象：重大な中断時にも重要業務を継続又は早期復旧するための計画
B. トリアージ：重大な中断時にも重要業務を継続又は早期復旧するための計画
C. CSIRT：重大な中断時にも重要業務を継続又は早期復旧するための計画
D. 事業継続計画：重大な中断時にも重要業務を継続又は早期復旧するための計画

答え・解説

Q0093 正答：D. 事業継続計画：重大な中断時にも重要業務を継続又は早期復旧するための計画

解説：正しい組合せは「事業継続計画：重大な中断時にも重要業務を継続又は早期復旧するための計画」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0094

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント4：重大な中断時にも重要業務を継続又は早期復旧するための計画

「事業継続計画」は、重大な中断時にも重要業務を継続又は早期復旧するための計画。

A. ○
B. ×

答え・解説

Q0094 正答：○

解説：正しい。事業継続計画は重大な中断時にも重要業務を継続又は早期復旧するための計画。実務では対象、目的、前提条件を併せて確認する。

Q0095

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント5：重大な中断時にも重要業務を継続又は早期復旧するための計画

組織が「重大な中断時にも重要業務を継続又は早期復旧するための計画」ために採用すべき概念又は仕組みはどれか。

A. 情報セキュリティ事象
B. 事業継続計画
C. トリアージ
D. CSIRT

答え・解説

Q0095 正答：B. 事業継続計画

解説：この目的に対応するのは事業継続計画である。重大な中断時にも重要業務を継続又は早期復旧するための計画という機能・考え方を持つためである。

Q0096

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント6：重大な中断時にも重要業務を継続又は早期復旧するための計画

「事業継続計画」について、誤解を避けるための説明として最も適切なものはどれか。

A. インシデントの受付、分析、対応調整、再発防止を担う組織又はチーム
B. 受け付けた事象の重要度・緊急度・影響範囲を判断して対応順を決める作業
C. 重大な中断時にも重要業務を継続又は早期復旧するための計画
D. 情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事

答え・解説

Q0096 正答：C. 重大な中断時にも重要業務を継続又は早期復旧するための計画

解説：事業継続計画は重大な中断時にも重要業務を継続又は早期復旧するための計画。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0097

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント7：重大な中断時にも重要業務を継続又は早期復旧するための計画

「事業継続計画」は、情報セキュリティ方針違反や管理策不全の可能性を示す観測可能な出来事。

A. ○
B. ×

答え・解説

Q0097 正答：×

解説：誤り。記述は情報セキュリティ事象の説明である。事業継続計画は重大な中断時にも重要業務を継続又は早期復旧するための計画。

Q0098

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント8：重大な中断時にも重要業務を継続又は早期復旧するための計画

次の状況で中心となる論点はどれか。「重大な中断時にも重要業務を継続又は早期復旧するための計画」ことが求められている。

A. 事業継続計画
B. トリアージ
C. CSIRT
D. 情報セキュリティ事象

答え・解説

Q0098 正答：A. 事業継続計画

解説：中心となる論点は事業継続計画である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0099

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント9：重大な中断時にも重要業務を継続又は早期復旧するための計画

事業継続計画は名称だけで判断できるため、対象や目的を確認する必要はない。

A. ○
B. ×

答え・解説

Q0099 正答：×

解説：誤り。事業継続計画は重大な中断時にも重要業務を継続又は早期復旧するための計画という概念であり、対象・目的・前提条件の確認が必要である。

Q0100

インシデント対応・事業継続
タグ：事業継続計画
用語：事業継続計画の確認ポイント10：重大な中断時にも重要業務を継続又は早期復旧するための計画

事業継続計画と他の類似概念を区別する際は、「重大な中断時にも重要業務を継続又は早期復旧するための計画」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0100 正答：○

解説：正しい。事業継続計画の定義は重大な中断時にも重要業務を継続又は早期復旧するための計画であり、類似概念との区別に使える。