情報セキュリティマネジメント試験 問題PDF

Q0001

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント1：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

次の説明に最も合う用語はどれか。端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

A. DLP
B. MDM
C. EDR
D. 責任共有モデル

答え・解説

Q0001 正答：C. EDR

解説：EDRは、端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0002

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント2：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

EDRの説明として最も適切なものはどれか。

A. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
B. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
C. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
D. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

答え・解説

Q0002 正答：D. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

解説：EDRの要点は「端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み」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

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント3：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「EDR」である。

A. EDR：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
B. DLP：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
C. MDM：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
D. 責任共有モデル：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

答え・解説

Q0003 正答：A. EDR：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

解説：正しい組合せは「EDR：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み」。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

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント4：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

「EDR」は、端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。EDRは端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0005

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント5：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

組織が「端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み」ために採用すべき概念又は仕組みはどれか。

A. DLP
B. MDM
C. EDR
D. 責任共有モデル

答え・解説

Q0005 正答：C. EDR

解説：この目的に対応するのはEDRである。端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組みという機能・考え方を持つためである。

Q0006

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント6：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

「EDR」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. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
B. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
C. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
D. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

答え・解説

Q0006 正答：D. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

解説：EDRは端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み。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

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント7：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
「EDR」は、機密情報を識別し、持出しや外部送信を監視・制御する仕組み。

A. ○
B. ×

答え・解説

Q0007 正答：×
解説：誤り。記述はDLPの説明である。EDRは端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み。

Q0008

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント8：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
次の状況で中心となる論点はどれか。「端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み」ことが求められている。

A. MDM
B. EDR
C. 責任共有モデル
D. DLP

答え・解説

Q0008 正答：B. EDR
解説：中心となる論点はEDR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

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント9：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

EDRを選定するときは、「端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み」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。EDRの選定・運用では、端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組みという目的との適合を確認する。

Q0010

端末・クラウド・監視
タグ：EDR
用語：EDRの確認ポイント10：端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

EDRは、端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み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。EDRはまさに端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組みという意味を持つ。

Q0011

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント1：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

次の説明に最も合う用語はどれか。機密情報を識別し、持出しや外部送信を監視・制御する仕組み

A. SIEM
B. 最小権限の原則
C. ゼロトラスト
D. DLP

答え・解説

Q0011 正答：D. DLP

解説：DLPは、機密情報を識別し、持出しや外部送信を監視・制御する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0012

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント2：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

DLPの説明として最も適切なものはどれか。

A. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
B. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み
C. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則
D. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

答え・解説

Q0012 正答：A. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み

解説：DLPの要点は「機密情報を識別し、持出しや外部送信を監視・制御する仕組み」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

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント3：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「DLP」である。

A. SIEM：機密情報を識別し、持出しや外部送信を監視・制御する仕組み
B. DLP：機密情報を識別し、持出しや外部送信を監視・制御する仕組み
C. 最小権限の原則：機密情報を識別し、持出しや外部送信を監視・制御する仕組み
D. ゼロトラスト：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

答え・解説

Q0013 正答：B. DLP：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

解説：正しい組合せは「DLP：機密情報を識別し、持出しや外部送信を監視・制御する仕組み」。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

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント4：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

「DLP」は、機密情報を識別し、持出しや外部送信を監視・制御する仕組み。

A. ○
B. ×

答え・解説

Q0014 正答：○

解説：正しい。DLPは機密情報を識別し、持出しや外部送信を監視・制御する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0015

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント5：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

組織が「機密情報を識別し、持出しや外部送信を監視・制御する仕組み」ために採用すべき概念又は仕組みはどれか。

A. SIEM
B. 最小権限の原則
C. ゼロトラスト
D. DLP

答え・解説

Q0015 正答：D. DLP

解説：この目的に対応するのはDLPである。機密情報を識別し、持出しや外部送信を監視・制御する仕組みという機能・考え方を持つためである。

Q0016

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント6：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

「DLP」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. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
B. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方
C. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則
D. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み

答え・解説

Q0016 正答：A. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み

解説：DLPは機密情報を識別し、持出しや外部送信を監視・制御する仕組み。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

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント7：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

「DLP」は、複数機器のログを集約・相関分析して異常の検知を支援する仕組み。

A. ○
B. ×

答え・解説

Q0017 正答：×

解説：誤り。記述はSIEMの説明である。DLPは機密情報を識別し、持出しや外部送信を監視・制御する仕組み。

Q0018

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント8：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

次の状況で中心となる論点はどれか。「機密情報を識別し、持出しや外部送信を監視・制御する仕組み」ことが求められている。

A. 最小権限の原則
B. ゼロトラスト
C. DLP
D. SIEM

答え・解説

Q0018 正答：C. DLP

解説：中心となる論点はDLP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。

情報セキュリティマネジメント試験 問題PDF

Q0019

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント9：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

DLP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。DLPは機密情報を識別し、持出しや外部送信を監視・制御する仕組みという概念であり、対象・目的・前提条件の確認が必要である。

Q0020

端末・クラウド・監視
タグ：DLP
用語：DLPの確認ポイント10：機密情報を識別し、持出しや外部送信を監視・制御する仕組み

DLPと他の類似概念を区別する際は、「機密情報を識別し、持出しや外部送信を監視・制御する仕組み」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。DLPの定義は機密情報を識別し、持出しや外部送信を監視・制御する仕組みであり、類似概念との区別に使える。

情報セキュリティマネジメント試験 問題PDF

Q0021

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント1：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

次の説明に最も合う用語はどれか。複数機器のログを集約・相関分析して異常の検知を支援する仕組み

A. SIEM
B. MDM
C. パッチ管理
D. サイバーハイジーン

答え・解説

Q0021 正答：A. SIEM

解説：SIEMは、複数機器のログを集約・相関分析して異常の検知を支援する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0022

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント2：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

SIEMの説明として最も適切なものはどれか。

A. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
B. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み
C. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
D. 更新、認証、バックアップなど基本的な安全習慣を継続する取組

答え・解説

Q0022 正答：B. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み

解説：SIEMの要点は「複数機器のログを集約・相関分析して異常の検知を支援する仕組み」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

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント3：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「SIEM」である。

A. MDM：複数機器のログを集約・相関分析して異常の検知を支援する仕組み
B. パッチ管理：複数機器のログを集約・相関分析して異常の検知を支援する仕組み
C. SIEM：複数機器のログを集約・相関分析して異常の検知を支援する仕組み
D. サイバーハイジーン：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

答え・解説

Q0023 正答：C. SIEM：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

解説：正しい組合せは「SIEM：複数機器のログを集約・相関分析して異常の検知を支援する仕組み」。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

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント4：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

「SIEM」は、複数機器のログを集約・相関分析して異常の検知を支援する仕組み。

A. ○
B. ×

答え・解説

Q0024 正答：○

解説：正しい。SIEMは複数機器のログを集約・相関分析して異常の検知を支援する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0025

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント5：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

組織が「複数機器のログを集約・相関分析して異常の検知を支援する仕組み」ために採用すべき概念又は仕組みはどれか。

A. SIEM
B. MDM
C. パッチ管理
D. サイバーハイジーン

答え・解説

Q0025 正答：A. SIEM

解説：この目的に対応するのはSIEMである。複数機器のログを集約・相関分析して異常の検知を支援する仕組みという機能・考え方を持つためである。

Q0026

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント6：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

「SIEM」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. 更新、認証、バックアップなど基本的な安全習慣を継続する取組
B. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み
C. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
D. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

答え・解説

Q0026 正答：B. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み

解説：SIEMは複数機器のログを集約・相関分析して異常の検知を支援する仕組み。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

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント7：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

「SIEM」は、スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み。

A. ○
B. ×

答え・解説

Q0027 正答：×

解説：誤り。記述はMDMの説明である。SIEMは複数機器のログを集約・相関分析して異常の検知を支援する仕組み。

Q0028

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント8：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

次の状況で中心となる論点はどれか。「複数機器のログを集約・相関分析して異常の検知を支援する仕組み」ことが求められている。

A. パッチ管理
B. サイバーハイジーン
C. MDM
D. SIEM

答え・解説

Q0028 正答：D. SIEM

解説：中心となる論点はSIEM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

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント9：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

SIEMを選定するときは、「複数機器のログを集約・相関分析して異常の検知を支援する仕組み」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。SIEMの選定・運用では、複数機器のログを集約・相関分析して異常の検知を支援する仕組みという目的との適合を確認する。

Q0030

端末・クラウド・監視
タグ：SIEM
用語：SIEMの確認ポイント10：複数機器のログを集約・相関分析して異常の検知を支援する仕組み

SIEMは、複数機器のログを集約・相関分析して異常の検知を支援する仕組み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。SIEMはまさに複数機器のログを集約・相関分析して異常の検知を支援する仕組みという意味を持つ。

Q0031

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント1：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

次の説明に最も合う用語はどれか。スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

A. 最小権限の原則
B. MDM
C. 3-2-1バックアップ
D. EDR

答え・解説

Q0031 正答：B. MDM

解説：MDMは、スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0032

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント2：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

MDMの説明として最も適切なものはどれか。

A. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則
B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
C. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
D. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

答え・解説

Q0032 正答：C. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

解説：MDMの要点は「スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み」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

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント3：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「MDM」である。

A. 最小権限の原則：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
B. 3-2-1バックアップ：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
C. EDR：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
D. MDM：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

答え・解説

Q0033 正答：D. MDM：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

解説：正しい組合せは「MDM：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み」。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

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント4：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

「MDM」は、スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み。

A. ○
B. ×

答え・解説

Q0034 正答：○

解説：正しい。MDMはスマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0035

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント5：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

組織が「スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み」ために採用すべき概念又は仕組みはどれか。

A. 最小権限の原則
B. MDM
C. 3-2-1バックアップ
D. EDR

答え・解説

Q0035 正答：B. MDM

解説：この目的に対応するのはMDMである。スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組みという機能・考え方を持つためである。

Q0036

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント6：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

「MDM」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. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
C. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
D. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

答え・解説

Q0036 正答：C. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

解説：MDMはスマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み。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

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント7：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

「MDM」は、業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則。

A. ○
B. ×

答え・解説

Q0037 正答：×

解説：誤り。記述は最小権限の原則の説明である。MDMはスマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み。

Q0038

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント8：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

次の状況で中心となる論点はどれか。「スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み」ことが求められている。

A. MDM
B. 3-2-1バックアップ
C. EDR
D. 最小権限の原則

答え・解説

Q0038 正答：A. MDM

解説：中心となる論点はMDM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。

情報セキュリティマネジメント試験 問題PDF

Q0039

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント9：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

MDM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。MDMはスマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組みという概念であり、対象・目的・前提条件の確認が必要である。

Q0040

端末・クラウド・監視
タグ：MDM
用語：MDMの確認ポイント10：スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

MDMと他の類似概念を区別する際は、「スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み」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。MDMの定義はスマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組みであり、類似概念との区別に使える。

情報セキュリティマネジメント試験 問題PDF

Q0041

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント1：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

次の説明に最も合う用語はどれか。業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

A. パッチ管理
B. 責任共有モデル
C. 最小権限の原則
D. DLP

答え・解説

Q0041 正答：C. 最小権限の原則

解説：最小権限の原則は、業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則。ほかの選択肢は目的又は適用場面が異なる。

Q0042

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント2：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

最小権限の原則の説明として最も適切なものはどれか。

A. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
B. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
C. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
D. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

答え・解説

Q0042 正答：D. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

解説：最小権限の原則の要点は「業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則」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

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント3：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

用語と説明の組合せとして適切なものはどれか。論点は「最小権限の原則」である。

A. 最小権限の原則：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則
B. パッチ管理：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則
C. 責任共有モデル：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則
D. DLP：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

答え・解説

Q0043 正答：A. 最小権限の原則：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

解説：正しい組合せは「最小権限の原則：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則」。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

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント4：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

「最小権限の原則」は、業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則。

A. ○
B. ×

答え・解説

Q0044 正答：○

解説：正しい。最小権限の原則は業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則。実務では対象、目的、前提条件を併せて確認する。

情報セキュリティマネジメント試験 問題PDF

Q0045

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント5：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

組織が「業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則」ために採用すべき概念又は仕組みはどれか。

A. パッチ管理
B. 責任共有モデル
C. 最小権限の原則
D. DLP

答え・解説

Q0045 正答：C. 最小権限の原則

解説：この目的に対応するのは最小権限の原則である。業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則という機能・考え方を持つためである。

Q0046

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント6：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

「最小権限の原則」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. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
B. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
C. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
D. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

答え・解説

Q0046 正答：D. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

解説：最小権限の原則は業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則。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

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント7：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

「最小権限の原則」は、脆弱性修正プログラムの評価、適用、確認を計画的に行う管理。

A. ○
B. ×

答え・解説

Q0047 正答：×

解説：誤り。記述はパッチ管理の説明である。最小権限の原則は業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則。

Q0048

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント8：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

次の状況で中心となる論点はどれか。「業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則」ことが求められている。

A. 責任共有モデル
B. 最小権限の原則
C. DLP
D. パッチ管理

答え・解説

Q0048 正答：B. 最小権限の原則

解説：中心となる論点は最小権限の原則である。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

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント9：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

最小権限の原則を選定するときは、「業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則」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。最小権限の原則の選定・運用では、業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則という目的との適合を確認する。

Q0050

端末・クラウド・監視
タグ：最小権限の原則
用語：最小権限の原則の確認ポイント10：業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

最小権限の原則は、業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則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。最小権限の原則はまさに業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則という意味を持つ。

Q0051

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント1：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

次の説明に最も合う用語はどれか。脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

A. 3-2-1バックアップ
B. ゼロトラスト
C. SIEM
D. パッチ管理

答え・解説

Q0051 正答：D. パッチ管理

解説：パッチ管理は、脆弱性修正プログラムの評価、適用、確認を計画的に行う管理。ほかの選択肢は目的又は適用場面が異なる。

Q0052

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント2：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

パッチ管理の説明として最も適切なものはどれか。

A. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
C. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方
D. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み

答え・解説

Q0052 正答：A. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

解説：パッチ管理の要点は「脆弱性修正プログラムの評価、適用、確認を計画的に行う管理」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

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント3：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

用語と説明の組合せとして適切なものはどれか。論点は「パッチ管理」である。

A. 3-2-1バックアップ：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
B. パッチ管理：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
C. ゼロトラスト：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
D. SIEM：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

答え・解説

Q0053 正答：B. パッチ管理：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

解説：正しい組合せは「パッチ管理：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理」。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

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント4：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

「パッチ管理」は、脆弱性修正プログラムの評価、適用、確認を計画的に行う管理。

A. ○
B. ×

答え・解説

Q0054 正答：○

解説：正しい。パッチ管理は脆弱性修正プログラムの評価、適用、確認を計画的に行う管理。実務では対象、目的、前提条件を併せて確認する。

Q0055

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント5：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

組織が「脆弱性修正プログラムの評価、適用、確認を計画的に行う管理」ために採用すべき概念又は仕組みはどれか。

A. 3-2-1バックアップ
B. ゼロトラスト
C. SIEM
D. パッチ管理

答え・解説

Q0055 正答：D. パッチ管理

解説：この目的に対応するのはパッチ管理である。脆弱性修正プログラムの評価、適用、確認を計画的に行う管理という機能・考え方を持つためである。

Q0056

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント6：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

「パッチ管理」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. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
B. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み
C. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方
D. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

答え・解説

Q0056 正答：A. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

解説：パッチ管理は脆弱性修正プログラムの評価、適用、確認を計画的に行う管理。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

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント7：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

「パッチ管理」は、データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方。

A. ○
B. ×

答え・解説

Q0057 正答：×

解説：誤り。記述は3-2-1バックアップの説明である。パッチ管理は脆弱性修正プログラムの評価、適用、確認を計画的に行う管理。

Q0058

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント8：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

次の状況で中心となる論点はどれか。「脆弱性修正プログラムの評価、適用、確認を計画的に行う管理」ことが求められている。

A. ゼロトラスト
B. SIEM
C. パッチ管理
D. 3-2-1バックアップ

答え・解説

Q0058 正答：C. パッチ管理

解説：中心となる論点はパッチ管理である。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

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント9：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

パッチ管理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。パッチ管理は脆弱性修正プログラムの評価、適用、確認を計画的に行う管理という概念であり、対象・目的・前提条件の確認が必要である。

Q0060

端末・クラウド・監視
タグ：パッチ管理
用語：パッチ管理の確認ポイント10：脆弱性修正プログラムの評価、適用、確認を計画的に行う管理

パッチ管理と他の類似概念を区別する際は、「脆弱性修正プログラムの評価、適用、確認を計画的に行う管理」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。パッチ管理の定義は脆弱性修正プログラムの評価、適用、確認を計画的に行う管理であり、類似概念との区別に使える。

Q0061

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント1：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

次の説明に最も合う用語はどれか。データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

A. 3-2-1バックアップ
B. 責任共有モデル
C. サイバーハイジーン
D. MDM

答え・解説

Q0061 正答：A. 3-2-1バックアップ

解説：3-2-1バックアップは、データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方。ほかの選択肢は目的又は適用場面が異なる。

Q0062

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント2：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

3-2-1バックアップの説明として最も適切なものはどれか。

A. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
C. 更新、認証、バックアップなど基本的な安全習慣を継続する取組
D. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み

答え・解説

Q0062 正答：B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

解説：3-2-1バックアップの要点は「データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方」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

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント3：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

用語と説明の組合せとして適切なものはどれか。論点は「3-2-1バックアップ」である。

A. 責任共有モデル：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
B. サイバーハイジーン：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
C. 3-2-1バックアップ：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
D. MDM：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

答え・解説

Q0063 正答：C. 3-2-1バックアップ：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

解説：正しい組合せは「3-2-1バックアップ：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方」。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

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント4：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

「3-2-1バックアップ」は、データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方。

A. ○
B. ×

答え・解説

Q0064 正答：○

解説：正しい。3-2-1バックアップはデータを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方。実務では対象、目的、前提条件を併せて確認する。

Q0065

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント5：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

組織が「データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方」ために採用すべき概念又は仕組みはどれか。

A. 3-2-1バックアップ
B. 責任共有モデル
C. サイバーハイジーン
D. MDM

答え・解説

Q0065 正答：A. 3-2-1バックアップ

解説：この目的に対応するのは3-2-1バックアップである。データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方という機能・考え方を持つためである。

Q0066

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント6：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

「3-2-1バックアップ」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. スマートフォンなどの設定、アプリ、紛失時処置を一元管理する仕組み
B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
C. 更新、認証、バックアップなど基本的な安全習慣を継続する取組
D. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

答え・解説

Q0066 正答：B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

解説：3-2-1バックアップはデータを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方。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

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント7：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

「3-2-1バックアップ」は、クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方。

A. ○
B. ×

答え・解説

Q0067 正答：×

解説：誤り。記述は責任共有モデルの説明である。3-2-1バックアップはデータを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方。

Q0068

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント8：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

次の状況で中心となる論点はどれか。「データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方」ことが求められている。

A. サイバーハイジーン
B. MDM
C. 責任共有モデル
D. 3-2-1バックアップ

答え・解説

Q0068 正答：D. 3-2-1バックアップ

解説：中心となる論点は3-2-1バックアップである。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

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント9：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

3-2-1バックアップを選定するときは、「データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方」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。3-2-1バックアップの選定・運用では、データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方という目的との適合を確認する。

Q0070

端末・クラウド・監視
タグ：3-2-1バックアップ
用語：3-2-1バックアップの確認ポイント10：データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

3-2-1バックアップは、データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方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。3-2-1バックアップはまさにデータを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方という意味を持つ。

情報セキュリティマネジメント試験 問題PDF

Q0071

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント1：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

次の説明に最も合う用語はどれか。クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

A. ゼロトラスト
B. 責任共有モデル
C. EDR
D. 最小権限の原則

答え・解説

Q0071 正答：B. 責任共有モデル

解説：責任共有モデルは、クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方。ほかの選択肢は目的又は適用場面が異なる。

Q0072

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント2：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

責任共有モデルの説明として最も適切なものはどれか。

A. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方
B. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
C. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
D. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則

答え・解説

Q0072 正答：C. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

解説：責任共有モデルの要点は「クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方」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

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント3：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

用語と説明の組合せとして適切なものはどれか。論点は「責任共有モデル」である。

A. ゼロトラスト：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
B. EDR：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
C. 最小権限の原則：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
D. 責任共有モデル：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

答え・解説

Q0073 正答：D. 責任共有モデル：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

解説：正しい組合せは「責任共有モデル：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方」。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

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント4：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

「責任共有モデル」は、クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方。

A. ○
B. ×

答え・解説

Q0074 正答：○

解説：正しい。責任共有モデルはクラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方。実務では対象、目的、前提条件を併せて確認する。

Q0075

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント5：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

組織が「クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方」ために採用すべき概念又は仕組みはどれか。

A. ゼロトラスト
B. 責任共有モデル
C. EDR
D. 最小権限の原則

答え・解説

Q0075 正答：B. 責任共有モデル

解説：この目的に対応するのは責任共有モデルである。クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方という機能・考え方を持つためである。

Q0076

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント6：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

「責任共有モデル」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. 業務遂行に必要な最小限の権限だけを利用者やプログラムへ与える原則
B. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
C. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方
D. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

答え・解説

Q0076 正答：C. クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

解説：責任共有モデルはクラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方。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

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント7：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

「責任共有モデル」は、場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方。

A. ○
B. ×

答え・解説

Q0077 正答：×

解説：誤り。記述はゼロトラストの説明である。責任共有モデルはクラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方。

Q0078

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント8：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

次の状況で中心となる論点はどれか。「クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方」ことが求められている。

A. 責任共有モデル
B. EDR
C. 最小権限の原則
D. ゼロトラスト

答え・解説

Q0078 正答：A. 責任共有モデル

解説：中心となる論点は責任共有モデルである。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

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント9：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

責任共有モデル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。責任共有モデルはクラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方という概念であり、対象・目的・前提条件の確認が必要である。

Q0080

端末・クラウド・監視
タグ：責任共有モデル
用語：責任共有モデルの確認ポイント10：クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方

責任共有モデルと他の類似概念を区別する際は、「クラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方」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。責任共有モデルの定義はクラウド事業者と利用者がサービス形態に応じてセキュリティ責任を分担する考え方であり、類似概念との区別に使える。

情報セキュリティマネジメント試験 問題PDF

Q0081

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント1：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

次の説明に最も合う用語はどれか。場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

A. サイバーハイジーン
B. DLP
C. ゼロトラスト
D. パッチ管理

答え・解説

Q0081 正答：C. ゼロトラスト

解説：ゼロトラストは、場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方。ほかの選択肢は目的又は適用場面が異なる。

Q0082

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント2：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

ゼロトラストの説明として最も適切なものはどれか。

A. 更新、認証、バックアップなど基本的な安全習慣を継続する取組
B. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
C. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
D. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

答え・解説

Q0082 正答：D. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

解説：ゼロトラストの要点は「場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方」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

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント3：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

用語と説明の組合せとして適切なものはどれか。論点は「ゼロトラスト」である。

A. ゼロトラスト：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方
B. サイバーハイジーン：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方
C. DLP：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方
D. パッチ管理：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

答え・解説

Q0083 正答：A. ゼロトラスト：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

解説：正しい組合せは「ゼロトラスト：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方」。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

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント4：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

「ゼロトラスト」は、場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方。

A. ○
B. ×

答え・解説

Q0084 正答：○

解説：正しい。ゼロトラストは場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方。実務では対象、目的、前提条件を併せて確認する。

Q0085

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント5：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

組織が「場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方」ために採用すべき概念又は仕組みはどれか。

A. サイバーハイジーン
B. DLP
C. ゼロトラスト
D. パッチ管理

答え・解説

Q0085 正答：C. ゼロトラスト

解説：この目的に対応するのはゼロトラストである。場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方という機能・考え方を持つためである。

Q0086

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント6：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

「ゼロトラスト」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. 脆弱性修正プログラムの評価、適用、確認を計画的に行う管理
B. 機密情報を識別し、持出しや外部送信を監視・制御する仕組み
C. 更新、認証、バックアップなど基本的な安全習慣を継続する取組
D. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

答え・解説

Q0086 正答：D. 場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

解説：ゼロトラストは場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方。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

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント7：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

「ゼロトラスト」は、更新、認証、バックアップなど基本的な安全習慣を継続する取組。

A. ○
B. ×

答え・解説

Q0087 正答：×

解説：誤り。記述はサイバーハイジーンの説明である。ゼロトラストは場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方。

Q0088

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント8：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

次の状況で中心となる論点はどれか。「場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方」ことが求められている。

A. DLP
B. ゼロトラスト
C. パッチ管理
D. サイバーハイジーン

答え・解説

Q0088 正答：B. ゼロトラスト

解説：中心となる論点はゼロトラストである。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。

Q0089

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント9：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

ゼロトラストを選定するときは、「場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方」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。ゼロトラストの選定・運用では、場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方という目的との適合を確認する。

Q0090

端末・クラウド・監視
タグ：ゼロトラスト
用語：ゼロトラストの確認ポイント10：場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方

ゼロトラストは、場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方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。ゼロトラストはまさに場所やネットワークを理由に自動的に信頼せず、継続的に確認する考え方という意味を持つ。

Q0091

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント1：更新、認証、バックアップなど基本的な安全習慣を継続する取組

次の説明に最も合う用語はどれか。更新、認証、バックアップなど基本的な安全習慣を継続する取組

A. EDR
B. SIEM
C. 3-2-1バックアップ
D. サイバーハイジーン

答え・解説

Q0091 正答：D. サイバーハイジーン

解説：サイバーハイジーンは、更新、認証、バックアップなど基本的な安全習慣を継続する取組。ほかの選択肢は目的又は適用場面が異なる。

Q0092

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント2：更新、認証、バックアップなど基本的な安全習慣を継続する取組

サイバーハイジーンの説明として最も適切なものはどれか。

A. 更新、認証、バックアップなど基本的な安全習慣を継続する取組
B. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み
C. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み
D. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方

答え・解説

Q0092 正答：A. 更新、認証、バックアップなど基本的な安全習慣を継続する取組

解説：サイバーハイジーンの要点は「更新、認証、バックアップなど基本的な安全習慣を継続する取組」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

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント3：更新、認証、バックアップなど基本的な安全習慣を継続する取組

用語と説明の組合せとして適切なものはどれか。論点は「サイバーハイジーン」である。

A. EDR：更新、認証、バックアップなど基本的な安全習慣を継続する取組
B. サイバーハイジーン：更新、認証、バックアップなど基本的な安全習慣を継続する取組
C. SIEM：更新、認証、バックアップなど基本的な安全習慣を継続する取組
D. 3-2-1バックアップ：更新、認証、バックアップなど基本的な安全習慣を継続する取組

答え・解説

Q0093 正答：B. サイバーハイジーン：更新、認証、バックアップなど基本的な安全習慣を継続する取組

解説：正しい組合せは「サイバーハイジーン：更新、認証、バックアップなど基本的な安全習慣を継続する取組」。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

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント4：更新、認証、バックアップなど基本的な安全習慣を継続する取組

「サイバーハイジーン」は、更新、認証、バックアップなど基本的な安全習慣を継続する取組。

A. ○
B. ×

答え・解説

Q0094 正答：○

解説：正しい。サイバーハイジーンは更新、認証、バックアップなど基本的な安全習慣を継続する取組。実務では対象、目的、前提条件を併せて確認する。

Q0095

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント5：更新、認証、バックアップなど基本的な安全習慣を継続する取組

組織が「更新、認証、バックアップなど基本的な安全習慣を継続する取組」ために採用すべき概念又は仕組みはどれか。

A. EDR
B. SIEM
C. 3-2-1バックアップ
D. サイバーハイジーン

答え・解説

Q0095 正答：D. サイバーハイジーン

解説：この目的に対応するのはサイバーハイジーンである。更新、認証、バックアップなど基本的な安全習慣を継続する取組という機能・考え方を持つためである。

Q0096

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント6：更新、認証、バックアップなど基本的な安全習慣を継続する取組

「サイバーハイジーン」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. 更新、認証、バックアップなど基本的な安全習慣を継続する取組
B. データを三つ保持し、二種類の媒体を使い、一つを別拠点に置く考え方
C. 複数機器のログを集約・相関分析して異常の検知を支援する仕組み
D. 端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み

答え・解説

Q0096 正答：A. 更新、認証、バックアップなど基本的な安全習慣を継続する取組

解説：サイバーハイジーンは更新、認証、バックアップなど基本的な安全習慣を継続する取組。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

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント7：更新、認証、バックアップなど基本的な安全習慣を継続する取組

「サイバーハイジーン」は、端末の挙動を継続監視し、侵害の検知・調査・対応を支援する仕組み。

A. ○
B. ×

答え・解説

Q0097 正答：×

解説：誤り。記述はEDRの説明である。サイバーハイジーンは更新、認証、バックアップなど基本的な安全習慣を継続する取組。

Q0098

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント8：更新、認証、バックアップなど基本的な安全習慣を継続する取組

次の状況で中心となる論点はどれか。「更新、認証、バックアップなど基本的な安全習慣を継続する取組」ことが求められている。

A. SIEM
B. 3-2-1バックアップ
C. サイバーハイジーン
D. EDR

答え・解説

Q0098 正答：C. サイバーハイジーン

解説：中心となる論点はサイバーハイジーンである。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

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント9：更新、認証、バックアップなど基本的な安全習慣を継続する取組

サイバーハイジーン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。サイバーハイジーンは更新、認証、バックアップなど基本的な安全習慣を継続する取組という概念であり、対象・目的・前提条件の確認が必要である。

Q0100

端末・クラウド・監視
タグ：サイバーハイジーン
用語：サイバーハイジーンの確認ポイント10：更新、認証、バックアップなど基本的な安全習慣を継続する取組

サイバーハイジーンと他の類似概念を区別する際は、「更新、認証、バックアップなど基本的な安全習慣を継続する取組」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。サイバーハイジーンの定義は更新、認証、バックアップなど基本的な安全習慣を継続する取組であり、類似概念との区別に使える。