Q0001

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント1：クラウド資源への主体、役割、権限、認証を管理する仕組み

次の説明に最も合う用語はどれか。クラウド資源への主体、役割、権限、認証を管理する仕組み

A. CSPM
B. クラウドIAM
C. Kubernetes RBAC
D. SBOM

答え・解説

Q0001 正答：B. クラウドIAM

解説：クラウドIAMは、クラウド資源への主体、役割、権限、認証を管理する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0002

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント2：クラウド資源への主体、役割、権限、認証を管理する仕組み

クラウドIAMの説明として最も適切なものはどれか。

A. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み
B. 役割とバインディングに基づきAPI操作権限を制御する仕組み
C. クラウド資源への主体、役割、権限、認証を管理する仕組み
D. ソフトウェアを構成する部品と依存関係を一覧化したもの

答え・解説

Q0002 正答：C. クラウド資源への主体、役割、権限、認証を管理する仕組み

解説：クラウドIAMの要点は「クラウド資源への主体、役割、権限、認証を管理する仕組み」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。

Q0003

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント3：クラウド資源への主体、役割、権限、認証を管理する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「クラウドIAM」である。

A. CSPM：クラウド資源への主体、役割、権限、認証を管理する仕組み
B. Kubernetes RBAC：クラウド資源への主体、役割、権限、認証を管理する仕組み
C. SBOM：クラウド資源への主体、役割、権限、認証を管理する仕組み
D. クラウドIAM：クラウド資源への主体、役割、権限、認証を管理する仕組み

答え・解説

Q0003 正答：D. クラウドIAM：クラウド資源への主体、役割、権限、認証を管理する仕組み

解説：正しい組合せは「クラウドIAM：クラウド資源への主体、役割、権限、認証を管理する仕組み」。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。

Q0004

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント4：クラウド資源への主体、役割、権限、認証を管理する仕組み

「クラウドIAM」は、クラウド資源への主体、役割、権限、認証を管理する仕組み。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。クラウドIAMはクラウド資源への主体、役割、権限、認証を管理する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0005

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント5：クラウド資源への主体、役割、権限、認証を管理する仕組み

組織が「クラウド資源への主体、役割、権限、認証を管理する仕組み」ために採用すべき概念又は仕組みはどれか。

A. CSPM
B. クラウドIAM
C. Kubernetes RBAC
D. SBOM

答え・解説

Q0005 正答：B. クラウドIAM
解説：この目的に対応するのはクラウドIAMである。クラウド資源への主体、役割、権限、認証を管理する仕組みという機能・考え方を持つためである。

Q0006

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント6：クラウド資源への主体、役割、権限、認証を管理する仕組み

「クラウドIAM」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. ソフトウェアを構成する部品と依存関係を一覧化したもの
B. 役割とバインディングに基づきAPI操作権限を制御する仕組み
C. クラウド資源への主体、役割、権限、認証を管理する仕組み
D. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

答え・解説

Q0006 正答：C. クラウド資源への主体、役割、権限、認証を管理する仕組み
解説：クラウドIAMはクラウド資源への主体、役割、権限、認証を管理する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント7：クラウド資源への主体、役割、権限、認証を管理する仕組み

「クラウドIAM」は、クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述はCSPMの説明である。クラウドIAMはクラウド資源への主体、役割、権限、認証を管理する仕組み。

Q0008

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント8：クラウド資源への主体、役割、権限、認証を管理する仕組み

次の状況で中心となる論点はどれか。「クラウド資源への主体、役割、権限、認証を管理する仕組み」ことが求められている。

A. クラウドIAM
B. Kubernetes RBAC
C. SBOM
D. CSPM

答え・解説

Q0008 正答：A. クラウドIAM

解説：中心となる論点はクラウドIAM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

クラウド・エンドポイント
タグ：クラウドIAM
用語：クラウドIAMの確認ポイント9：クラウド資源への主体、役割、権限、認証を管理する仕組み

「クラウド資源への主体、役割、権限、認証を管理する仕組み」という特徴を持つものを選べ。

A. SBOM
B. クラウドIAM
C. Kubernetes RBAC
D. CSPM

答え・解説

Q0009 正答：B. クラウドIAM
解説：クラウドIAMが該当する。定義はクラウド資源への主体、役割、権限、認証を管理する仕組みであり、他の候補とは機能が異なる。

Q0010

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント1：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

次の説明に最も合う用語はどれか。クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

A. コンテナイメージ署名
B. シークレット管理
C. CSPM
D. 脆弱性パッチ管理

答え・解説

Q0010 正答：C. CSPM
解説：CSPMは、クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0011

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント2：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

CSPMの説明として最も適切なものはどれか。

A. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
B. 鍵やパスワードを安全に保管・配布・更新する仕組み
C. 修正情報の収集、評価、検証、適用、確認を管理する活動
D. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

答え・解説

Q0011 正答：D. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

解説：CSPMの要点は「クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み」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。

Q0012

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント3：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「CSPM」である。

A. CSPM：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み
B. コンテナイメージ署名：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み
C. シークレット管理：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み
D. 脆弱性パッチ管理：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

答え・解説

Q0012 正答：A. CSPM：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

解説：正しい組合せは「CSPM：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み」。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。

Q0013

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント4：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

「CSPM」は、クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み。

A. ○
B. ×

答え・解説

Q0013 正答：○

解説：正しい。CSPMはクラウド設定を継続評価し危険な構成や規制違反を検出する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0014

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント5：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

組織が「クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み」ために採用すべき概念又は仕組みはどれか。

A. コンテナイメージ署名
B. シークレット管理
C. CSPM
D. 脆弱性パッチ管理

答え・解説

Q0014 正答：C. CSPM

解説：この目的に対応するのはCSPMである。クラウド設定を継続評価し危険な構成や規制違反を検出する仕組みという機能・考え方を持つためである。

Q0015

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント6：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

「CSPM」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. 修正情報の収集、評価、検証、適用、確認を管理する活動
B. 鍵やパスワードを安全に保管・配布・更新する仕組み
C. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
D. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

答え・解説

Q0015 正答：D. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

解説：CSPMはクラウド設定を継続評価し危険な構成や規制違反を検出する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0016

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント7：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

「CSPM」は、イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述はコンテナイメージ署名の説明である。CSPMはクラウド設定を継続評価し危険な構成や規制違反を検出する仕組み。

Q0017

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント8：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

次の状況で中心となる論点はどれか。「クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み」ことが求められている。

A. シークレット管理
B. CSPM
C. 脆弱性パッチ管理
D. コンテナイメージ署名

答え・解説

Q0017 正答：B. CSPM

解説：中心となる論点はCSPM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。

Q0018

クラウド・エンドポイント
タグ：CSPM
用語：CSPMの確認ポイント9：クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

「クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み」という特徴を持つものを選べ。

A. 脆弱性パッチ管理
B. シークレット管理
C. CSPM
D. コンテナイメージ署名

答え・解説

Q0018 正答：C. CSPM

解説：CSPMが該当する。定義はクラウド設定を継続評価し危険な構成や規制違反を検出する仕組みであり、他の候補とは機能が異なる。

Q0019

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント1：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

次の説明に最も合う用語はどれか。イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

A. Kubernetes RBAC
B. EDR
C. イミュータブルバックアップ
D. コンテナイメージ署名

答え・解説

Q0019 正答：D. コンテナイメージ署名

解説：コンテナイメージ署名は、イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0020

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント2：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

コンテナイメージ署名の説明として最も適切なものはどれか。

A. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
B. 役割とバインディングに基づきAPI操作権限を制御する仕組み
C. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
D. 通常操作では変更・削除できない状態で保持するバックアップ

答え・解説

Q0020 正答：A. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

解説：コンテナイメージ署名の要点は「イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み」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。

Q0021

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント3：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「コンテナイメージ署名」である。

A. Kubernetes RBAC：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
B. コンテナイメージ署名：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
C. EDR：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
D. イミュータブルバックアップ：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

答え・解説

Q0021 正答：B. コンテナイメージ署名：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

解説：正しい組合せは「コンテナイメージ署名：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み」。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。

Q0022

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント4：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

「コンテナイメージ署名」は、イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。コンテナイメージ署名はイメージの作成元と改ざんの有無を検証するため署名を付与する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0023

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント5：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

組織が「イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み」ために採用すべき概念又は仕組みはどれか。

A. Kubernetes RBAC
B. EDR
C. イミュータブルバックアップ
D. コンテナイメージ署名

答え・解説

Q0023 正答：D. コンテナイメージ署名

解説：この目的に対応するのはコンテナイメージ署名である。イメージの作成元と改ざんの有無を検証するため署名を付与する仕組みという機能・考え方を持つためである。

Q0024

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント6：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

「コンテナイメージ署名」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. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
B. 通常操作では変更・削除できない状態で保持するバックアップ
C. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
D. 役割とバインディングに基づきAPI操作権限を制御する仕組み

答え・解説

Q0024 正答：A. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

解説：コンテナイメージ署名はイメージの作成元と改ざんの有無を検証するため署名を付与する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0025

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント7：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

「コンテナイメージ署名」は、役割とバインディングに基づきAPI操作権限を制御する仕組み。

A. ○
B. ×

答え・解説

Q0025 正答：×

解説：誤り。記述はKubernetes RBACの説明である。コンテナイメージ署名はイメージの作成元と改ざんの有無を検証するため署名を付与する仕組み。

Q0026

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント8：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

次の状況で中心となる論点はどれか。「イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み」ことが求められている。

A. EDR
B. イミュータブルバックアップ
C. コンテナイメージ署名
D. Kubernetes RBAC

答え・解説

Q0026 正答：C. コンテナイメージ署名

解説：中心となる論点はコンテナイメージ署名である。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。

Q0027

クラウド・エンドポイント
タグ：コンテナイメージ署名
用語：コンテナイメージ署名の確認ポイント9：イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み

「イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み」という特徴を持つものを選べ。

A. イミュータブルバックアップ
B. EDR
C. Kubernetes RBAC
D. コンテナイメージ署名

答え・解説

Q0027 正答：D. コンテナイメージ署名

解説：コンテナイメージ署名が該当する。定義はイメージの作成元と改ざんの有無を検証するため署名を付与する仕組みであり、他の候補とは機能が異なる。

Q0028

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント1：役割とバインディングに基づきAPI操作権限を制御する仕組み

次の説明に最も合う用語はどれか。役割とバインディングに基づきAPI操作権限を制御する仕組み

A. Kubernetes RBAC
B. シークレット管理
C. アプリケーション許可リスト
D. クラウドIAM

答え・解説

Q0028 正答：A. Kubernetes RBAC

解説：Kubernetes RBACは、役割とバインディングに基づきAPI操作権限を制御する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0029

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント2：役割とバインディングに基づきAPI操作権限を制御する仕組み

Kubernetes RBACの説明として最も適切なものはどれか。

A. 鍵やパスワードを安全に保管・配布・更新する仕組み
B. 役割とバインディングに基づきAPI操作権限を制御する仕組み
C. 承認済みプログラムだけの実行を認める制御
D. クラウド資源への主体、役割、権限、認証を管理する仕組み

答え・解説

Q0029 正答：B. 役割とバインディングに基づきAPI操作権限を制御する仕組み

解説：Kubernetes RBACの要点は「役割とバインディングに基づきAPI操作権限を制御する仕組み」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。

Q0030

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント3：役割とバインディングに基づきAPI操作権限を制御する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「Kubernetes RBAC」である。

A. シークレット管理：役割とバインディングに基づきAPI操作権限を制御する仕組み
B. アプリケーション許可リスト：役割とバインディングに基づきAPI操作権限を制御する仕組み
C. Kubernetes RBAC：役割とバインディングに基づきAPI操作権限を制御する仕組み
D. クラウドIAM：役割とバインディングに基づきAPI操作権限を制御する仕組み

答え・解説

Q0030 正答：C. Kubernetes RBAC：役割とバインディングに基づきAPI操作権限を制御する仕組み

解説：正しい組合せは「Kubernetes RBAC：役割とバインディングに基づきAPI操作権限を制御する仕組み」。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。

Q0031

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント4：役割とバインディングに基づきAPI操作権限を制御する仕組み

「Kubernetes RBAC」は、役割とバインディングに基づきAPI操作権限を制御する仕組み。

A. ○
B. ×

答え・解説

Q0031 正答：○

解説：正しい。Kubernetes RBACは役割とバインディングに基づきAPI操作権限を制御する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0032

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント5：役割とバインディングに基づきAPI操作権限を制御する仕組み

組織が「役割とバインディングに基づきAPI操作権限を制御する仕組み」ために採用すべき概念又は仕組みはどれか。

A. Kubernetes RBAC
B. シークレット管理
C. アプリケーション許可リスト
D. クラウドIAM

答え・解説

Q0032 正答：A. Kubernetes RBAC

解説：この目的に対応するのはKubernetes RBACである。役割とバインディングに基づきAPI操作権限を制御する仕組みという機能・考え方を持つためである。

Q0033

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント6：役割とバインディングに基づきAPI操作権限を制御する仕組み

「Kubernetes RBAC」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. クラウド資源への主体、役割、権限、認証を管理する仕組み
B. 役割とバインディングに基づきAPI操作権限を制御する仕組み
C. 承認済みプログラムだけの実行を認める制御
D. 鍵やパスワードを安全に保管・配布・更新する仕組み

答え・解説

Q0033 正答：B. 役割とバインディングに基づきAPI操作権限を制御する仕組み
解説：Kubernetes RBACは役割とバインディングに基づきAPI操作権限を制御する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0034

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント7：役割とバインディングに基づきAPI操作権限を制御する仕組み

「Kubernetes RBAC」は、鍵やパスワードを安全に保管・配布・更新する仕組み。

A. ○
B. ×

答え・解説

Q0034 正答：×
解説：誤り。記述はシークレット管理の説明である。Kubernetes RBACは役割とバインディングに基づきAPI操作権限を制御する仕組み。

Q0035

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント8：役割とバインディングに基づきAPI操作権限を制御する仕組み

次の状況で中心となる論点はどれか。「役割とバインディングに基づきAPI操作権限を制御する仕組み」ことが求められている。

A. アプリケーション許可リスト
B. クラウドIAM
C. シークレット管理
D. Kubernetes RBAC

答え・解説

Q0035 正答：D. Kubernetes RBAC

解説：中心となる論点はKubernetes RBAC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。

Q0036

クラウド・エンドポイント
タグ：Kubernetes RBAC
用語：Kubernetes RBACの確認ポイント9：役割とバインディングに基づきAPI操作権限を制御する仕組み

「役割とバインディングに基づきAPI操作権限を制御する仕組み」という特徴を持つものを選べ。

A. Kubernetes RBAC
B. クラウドIAM
C. アプリケーション許可リスト
D. シークレット管理

答え・解説

Q0036 正答：A. Kubernetes RBAC

解説：Kubernetes RBACが該当する。定義は役割とバインディングに基づきAPI操作権限を制御する仕組みであり、他の候補とは機能が異なる。

Q0037

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント1：鍵やパスワードを安全に保管・配布・更新する仕組み

次の説明に最も合う用語はどれか。鍵やパスワードを安全に保管・配布・更新する仕組み

A. EDR
B. シークレット管理
C. SBOM
D. CSPM

答え・解説

Q0037 正答：B. シークレット管理

解説：シークレット管理は、鍵やパスワードを安全に保管・配布・更新する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0038

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント2：鍵やパスワードを安全に保管・配布・更新する仕組み

シークレット管理の説明として最も適切なものはどれか。

A. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
B. ソフトウェアを構成する部品と依存関係を一覧化したもの
C. 鍵やパスワードを安全に保管・配布・更新する仕組み
D. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み

答え・解説

Q0038 正答：C. 鍵やパスワードを安全に保管・配布・更新する仕組み

解説：シークレット管理の要点は「鍵やパスワードを安全に保管・配布・更新する仕組み」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。

Q0039

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント3：鍵やパスワードを安全に保管・配布・更新する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「シークレット管理」である。

A. EDR：鍵やパスワードを安全に保管・配布・更新する仕組み
B. SBOM：鍵やパスワードを安全に保管・配布・更新する仕組み
C. CSPM：鍵やパスワードを安全に保管・配布・更新する仕組み
D. シークレット管理：鍵やパスワードを安全に保管・配布・更新する仕組み

答え・解説

Q0039 正答：D. シークレット管理：鍵やパスワードを安全に保管・配布・更新する仕組み

解説：正しい組合せは「シークレット管理：鍵やパスワードを安全に保管・配布・更新する仕組み」。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。

Q0040

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント4：鍵やパスワードを安全に保管・配布・更新する仕組み

「シークレット管理」は、鍵やパスワードを安全に保管・配布・更新する仕組み。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。シークレット管理は鍵やパスワードを安全に保管・配布・更新する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0041

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント5：鍵やパスワードを安全に保管・配布・更新する仕組み

組織が「鍵やパスワードを安全に保管・配布・更新する仕組み」ために採用すべき概念又は仕組みはどれか。

A. EDR
B. シークレット管理
C. SBOM
D. CSPM

答え・解説

Q0041 正答：B. シークレット管理
解説：この目的に対応するのはシークレット管理である。鍵やパスワードを安全に保管・配布・更新する仕組みという機能・考え方を持つためである。

Q0042

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント6：鍵やパスワードを安全に保管・配布・更新する仕組み

「シークレット管理」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. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み
B. ソフトウェアを構成する部品と依存関係を一覧化したもの
C. 鍵やパスワードを安全に保管・配布・更新する仕組み
D. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

答え・解説

Q0042 正答：C. 鍵やパスワードを安全に保管・配布・更新する仕組み
解説：シークレット管理は鍵やパスワードを安全に保管・配布・更新する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0043

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント7：鍵やパスワードを安全に保管・配布・更新する仕組み

「シークレット管理」は、端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述はEDRの説明である。シークレット管理は鍵やパスワードを安全に保管・配布・更新する仕組み。

Q0044

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント8：鍵やパスワードを安全に保管・配布・更新する仕組み

次の状況で中心となる論点はどれか。「鍵やパスワードを安全に保管・配布・更新する仕組み」ことが求められている。

A. シークレット管理
B. SBOM
C. CSPM
D. EDR

答え・解説

Q0044 正答：A. シークレット管理

解説：中心となる論点はシークレット管理である。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。

Q0045

クラウド・エンドポイント
タグ：シークレット管理
用語：シークレット管理の確認ポイント9：鍵やパスワードを安全に保管・配布・更新する仕組み

「鍵やパスワードを安全に保管・配布・更新する仕組み」という特徴を持つものを選べ。

A. CSPM
B. シークレット管理
C. SBOM
D. EDR

答え・解説

Q0045 正答：B. シークレット管理

解説：シークレット管理が該当する。定義は鍵やパスワードを安全に保管・配布・更新する仕組みであり、他の候補とは機能が異なる。

Q0046

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント1：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

次の説明に最も合う用語はどれか。端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

A. アプリケーション許可リスト
B. 脆弱性パッチ管理
C. EDR
D. コンテナイメージ署名

答え・解説

Q0046 正答：C. EDR

解説：EDRは、端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0047

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント2：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

EDRの説明として最も適切なものはどれか。

A. 承認済みプログラムだけの実行を認める制御
B. 修正情報の収集、評価、検証、適用、確認を管理する活動
C. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
D. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

答え・解説

Q0047 正答：D. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

解説：EDRの要点は「端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み」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。

Q0048

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント3：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

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：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
B. アプリケーション許可リスト：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
C. 脆弱性パッチ管理：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
D. コンテナイメージ署名：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

答え・解説

Q0048 正答：A. EDR：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

解説：正しい組合せは「EDR：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み」。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。

Q0049

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント4：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
「EDR」は、端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み。

A. ○
B. ×

答え・解説

Q0049 正答：○
解説：正しい。EDRは端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0050

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント5：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
組織が「端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み」ために採用すべき概念又は仕組みはどれか。

A. アプリケーション許可リスト
B. 脆弱性パッチ管理
C. EDR
D. コンテナイメージ署名

答え・解説

Q0050 正答：C. EDR
解説：この目的に対応するのはEDRである。端末テレメトリを用いて侵害を検知・調査・封じ込める仕組みという機能・考え方を持つためである。

Q0051

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント6：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

「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. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
B. 修正情報の収集、評価、検証、適用、確認を管理する活動
C. 承認済みプログラムだけの実行を認める制御
D. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

答え・解説

Q0051 正答：D. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

解説：EDRは端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0052

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント7：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

「EDR」は、承認済みプログラムだけの実行を認める制御。

A. ○
B. ×

答え・解説

Q0052 正答：×

解説：誤り。記述はアプリケーション許可リストの説明である。EDRは端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み。

Q0053

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント8：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

次の状況で中心となる論点はどれか。「端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み」ことが求められている。

A. 脆弱性パッチ管理
B. EDR
C. コンテナイメージ署名
D. アプリケーション許可リスト

答え・解説

Q0053 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。

Q0054

クラウド・エンドポイント
タグ：EDR
用語：EDRの確認ポイント9：端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

「端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み」という特徴を持つものを選べ。

A. コンテナイメージ署名
B. 脆弱性パッチ管理
C. EDR
D. アプリケーション許可リスト

答え・解説

Q0054 正答：C. EDR

解説：EDRが該当する。定義は端末テレメトリを用いて侵害を検知・調査・封じ込める仕組みであり、他の候補とは機能が異なる。

Q0055

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント1：承認済みプログラムだけの実行を認める制御

次の説明に最も合う用語はどれか。承認済みプログラムだけの実行を認める制御

A. SBOM
B. イミュータブルバックアップ
C. Kubernetes RBAC
D. アプリケーション許可リスト

答え・解説

Q0055 正答：D. アプリケーション許可リスト

解説：アプリケーション許可リストは、承認済みプログラムだけの実行を認める制御。ほかの選択肢は目的又は適用場面が異なる。

Q0056

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント2：承認済みプログラムだけの実行を認める制御

アプリケーション許可リストの説明として最も適切なものはどれか。

A. 承認済みプログラムだけの実行を認める制御
B. ソフトウェアを構成する部品と依存関係を一覧化したもの
C. 通常操作では変更・削除できない状態で保持するバックアップ
D. 役割とバインディングに基づきAPI操作権限を制御する仕組み

答え・解説

Q0056 正答：A. 承認済みプログラムだけの実行を認める制御

解説：アプリケーション許可リストの要点は「承認済みプログラムだけの実行を認める制御」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。

Q0057

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント3：承認済みプログラムだけの実行を認める制御

用語と説明の組合せとして適切なものはどれか。論点は「アプリケーション許可リスト」である。

A. SBOM：承認済みプログラムだけの実行を認める制御
B. アプリケーション許可リスト：承認済みプログラムだけの実行を認める制御
C. イミュータブルバックアップ：承認済みプログラムだけの実行を認める制御
D. Kubernetes RBAC：承認済みプログラムだけの実行を認める制御

答え・解説

Q0057 正答：B. アプリケーション許可リスト：承認済みプログラムだけの実行を認める制御

解説：正しい組合せは「アプリケーション許可リスト：承認済みプログラムだけの実行を認める制御」。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。

Q0058

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント4：承認済みプログラムだけの実行を認める制御

「アプリケーション許可リスト」は、承認済みプログラムだけの実行を認める制御。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。アプリケーション許可リストは承認済みプログラムだけの実行を認める制御。実務では対象、目的、前提条件を併せて確認する。

Q0059

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント5：承認済みプログラムだけの実行を認める制御

組織が「承認済みプログラムだけの実行を認める制御」ために採用すべき概念又は仕組みはどれか。

A. SBOM
B. イミュータブルバックアップ
C. Kubernetes RBAC
D. アプリケーション許可リスト

答え・解説

Q0059 正答：D. アプリケーション許可リスト
解説：この目的に対応するのはアプリケーション許可リストである。承認済みプログラムだけの実行を認める制御という機能・考え方を持つためである。

Q0060

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント6：承認済みプログラムだけの実行を認める制御

「アプリケーション許可リスト」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. 承認済みプログラムだけの実行を認める制御
B. 役割とバインディングに基づきAPI操作権限を制御する仕組み
C. 通常操作では変更・削除できない状態で保持するバックアップ
D. ソフトウェアを構成する部品と依存関係を一覧化したもの

答え・解説

Q0060 正答：A. 承認済みプログラムだけの実行を認める制御
解説：アプリケーション許可リストは承認済みプログラムだけの実行を認める制御。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0061

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント7：承認済みプログラムだけの実行を認める制御

「アプリケーション許可リスト」は、ソフトウェアを構成する部品と依存関係を一覧化したもの。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述はSBOMの説明である。アプリケーション許可リストは承認済みプログラムだけの実行を認める制御。

Q0062

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント8：承認済みプログラムだけの実行を認める制御

次の状況で中心となる論点はどれか。「承認済みプログラムだけの実行を認める制御」ことが求められている。

A. イミュータブルバックアップ
B. Kubernetes RBAC
C. アプリケーション許可リスト
D. SBOM

答え・解説

Q0062 正答：C. アプリケーション許可リスト

解説：中心となる論点はアプリケーション許可リストである。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。

Q0063

クラウド・エンドポイント
タグ：アプリケーション許可リスト
用語：アプリケーション許可リストの確認ポイント9：承認済みプログラムだけの実行を認める制御

「承認済みプログラムだけの実行を認める制御」という特徴を持つものを選べ。

A. Kubernetes RBAC
B. イミュータブルバックアップ
C. SBOM
D. アプリケーション許可リスト

答え・解説

Q0063 正答：D. アプリケーション許可リスト

解説：アプリケーション許可リストが該当する。定義は承認済みプログラムだけの実行を認める制御であり、他の候補とは機能が異なる。

Q0064

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント1：ソフトウェアを構成する部品と依存関係を一覧化したもの

次の説明に最も合う用語はどれか。ソフトウェアを構成する部品と依存関係を一覧化したもの

A. SBOM
B. 脆弱性パッチ管理
C. クラウドIAM
D. シークレット管理

答え・解説

Q0064 正答：A. SBOM

解説：SBOMは、ソフトウェアを構成する部品と依存関係を一覧化したもの。ほかの選択肢は目的又は適用場面が異なる。

Q0065

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント2：ソフトウェアを構成する部品と依存関係を一覧化したもの

SBOMの説明として最も適切なものはどれか。

A. 修正情報の収集、評価、検証、適用、確認を管理する活動
B. ソフトウェアを構成する部品と依存関係を一覧化したもの
C. クラウド資源への主体、役割、権限、認証を管理する仕組み
D. 鍵やパスワードを安全に保管・配布・更新する仕組み

答え・解説

Q0065 正答：B. ソフトウェアを構成する部品と依存関係を一覧化したもの

解説：SBOMの要点は「ソフトウェアを構成する部品と依存関係を一覧化したもの」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。

Q0066

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント3：ソフトウェアを構成する部品と依存関係を一覧化したもの

用語と説明の組合せとして適切なものはどれか。論点は「SBOM」である。

A. 脆弱性パッチ管理：ソフトウェアを構成する部品と依存関係を一覧化したもの
B. クラウドIAM：ソフトウェアを構成する部品と依存関係を一覧化したもの
C. SBOM：ソフトウェアを構成する部品と依存関係を一覧化したもの
D. シークレット管理：ソフトウェアを構成する部品と依存関係を一覧化したもの

答え・解説

Q0066 正答：C. SBOM：ソフトウェアを構成する部品と依存関係を一覧化したもの

解説：正しい組合せは「SBOM：ソフトウェアを構成する部品と依存関係を一覧化したもの」。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。

Q0067

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント4：ソフトウェアを構成する部品と依存関係を一覧化したもの

「SBOM」は、ソフトウェアを構成する部品と依存関係を一覧化したもの。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。SBOMはソフトウェアを構成する部品と依存関係を一覧化したもの。実務では対象、目的、前提条件を併せて確認する。

Q0068

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント5：ソフトウェアを構成する部品と依存関係を一覧化したもの

組織が「ソフトウェアを構成する部品と依存関係を一覧化したもの」ために採用すべき概念又は仕組みはどれか。

A. SBOM
B. 脆弱性パッチ管理
C. クラウドIAM
D. シークレット管理

答え・解説

Q0068 正答：A. SBOM

解説：この目的に対応するのはSBOMである。ソフトウェアを構成する部品と依存関係を一覧化したものという機能・考え方を持つためである。

Q0069

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント6：ソフトウェアを構成する部品と依存関係を一覧化したもの

「SBOM」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. 鍵やパスワードを安全に保管・配布・更新する仕組み
B. ソフトウェアを構成する部品と依存関係を一覧化したもの
C. クラウド資源への主体、役割、権限、認証を管理する仕組み
D. 修正情報の収集、評価、検証、適用、確認を管理する活動

答え・解説

Q0069 正答：B. ソフトウェアを構成する部品と依存関係を一覧化したもの

解説：SBOMはソフトウェアを構成する部品と依存関係を一覧化したもの。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0070

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント7：ソフトウェアを構成する部品と依存関係を一覧化したもの

「SBOM」は、修正情報の収集、評価、検証、適用、確認を管理する活動。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述は脆弱性パッチ管理の説明である。SBOMはソフトウェアを構成する部品と依存関係を一覧化したもの。

Q0071

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント8：ソフトウェアを構成する部品と依存関係を一覧化したもの

次の状況で中心となる論点はどれか。「ソフトウェアを構成する部品と依存関係を一覧化したもの」ことが求められている。

A. クラウドIAM
B. シークレット管理
C. 脆弱性パッチ管理
D. SBOM

答え・解説

Q0071 正答：D. SBOM

解説：中心となる論点はSBOM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。

Q0072

クラウド・エンドポイント
タグ：SBOM
用語：SBOMの確認ポイント9：ソフトウェアを構成する部品と依存関係を一覧化したもの

「ソフトウェアを構成する部品と依存関係を一覧化したもの」という特徴を持つものを選べ。

A. SBOM
B. シークレット管理
C. クラウドIAM
D. 脆弱性パッチ管理

答え・解説

Q0072 正答：A. SBOM

解説：SBOMが該当する。定義はソフトウェアを構成する部品と依存関係を一覧化したものであり、他の候補とは機能が異なる。

Q0073

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント1：修正情報の収集、評価、検証、適用、確認を管理する活動

次の説明に最も合う用語はどれか。修正情報の収集、評価、検証、適用、確認を管理する活動

A. イミュータブルバックアップ
B. 脆弱性パッチ管理
C. CSPM
D. EDR

答え・解説

Q0073 正答：B. 脆弱性パッチ管理

解説：脆弱性パッチ管理は、修正情報の収集、評価、検証、適用、確認を管理する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0074

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント2：修正情報の収集、評価、検証、適用、確認を管理する活動

脆弱性パッチ管理の説明として最も適切なものはどれか。

A. 通常操作では変更・削除できない状態で保持するバックアップ
B. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み
C. 修正情報の収集、評価、検証、適用、確認を管理する活動
D. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み

答え・解説

Q0074 正答：C. 修正情報の収集、評価、検証、適用、確認を管理する活動

解説：脆弱性パッチ管理の要点は「修正情報の収集、評価、検証、適用、確認を管理する活動」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。

Q0075

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント3：修正情報の収集、評価、検証、適用、確認を管理する活動

用語と説明の組合せとして適切なものはどれか。論点は「脆弱性パッチ管理」である。

A. イミュータブルバックアップ：修正情報の収集、評価、検証、適用、確認を管理する活動
B. CSPM：修正情報の収集、評価、検証、適用、確認を管理する活動
C. EDR：修正情報の収集、評価、検証、適用、確認を管理する活動
D. 脆弱性パッチ管理：修正情報の収集、評価、検証、適用、確認を管理する活動

答え・解説

Q0075 正答：D. 脆弱性パッチ管理：修正情報の収集、評価、検証、適用、確認を管理する活動

解説：正しい組合せは「脆弱性パッチ管理：修正情報の収集、評価、検証、適用、確認を管理する活動」。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。

Q0076

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント4：修正情報の収集、評価、検証、適用、確認を管理する活動

「脆弱性パッチ管理」は、修正情報の収集、評価、検証、適用、確認を管理する活動。

A. ○
B. ×

答え・解説

Q0076 正答：○

解説：正しい。脆弱性パッチ管理は修正情報の収集、評価、検証、適用、確認を管理する活動。実務では対象、目的、前提条件を併せて確認する。

Q0077

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント5：修正情報の収集、評価、検証、適用、確認を管理する活動

組織が「修正情報の収集、評価、検証、適用、確認を管理する活動」ために採用すべき概念又は仕組みはどれか。

A. イミュータブルバックアップ
B. 脆弱性パッチ管理
C. CSPM
D. EDR

答え・解説

Q0077 正答：B. 脆弱性パッチ管理
解説：この目的に対応するのは脆弱性パッチ管理である。修正情報の収集、評価、検証、適用、確認を管理する活動という機能・考え方を持つためである。

Q0078

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント6：修正情報の収集、評価、検証、適用、確認を管理する活動

「脆弱性パッチ管理」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. 端末テレメトリを用いて侵害を検知・調査・封じ込める仕組み
B. クラウド設定を継続評価し危険な構成や規制違反を検出する仕組み
C. 修正情報の収集、評価、検証、適用、確認を管理する活動
D. 通常操作では変更・削除できない状態で保持するバックアップ

答え・解説

Q0078 正答：C. 修正情報の収集、評価、検証、適用、確認を管理する活動
解説：脆弱性パッチ管理は修正情報の収集、評価、検証、適用、確認を管理する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0079

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント7：修正情報の収集、評価、検証、適用、確認を管理する活動

「脆弱性パッチ管理」は、通常操作では変更・削除できない状態で保持するバックアップ。

A. ○
B. ×

答え・解説

Q0079 正答：×

解説：誤り。記述はイミュータブルバックアップの説明である。脆弱性パッチ管理は修正情報の収集、評価、検証、適用、確認を管理する活動。

Q0080

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント8：修正情報の収集、評価、検証、適用、確認を管理する活動

次の状況で中心となる論点はどれか。「修正情報の収集、評価、検証、適用、確認を管理する活動」ことが求められている。

A. 脆弱性パッチ管理
B. CSPM
C. EDR
D. イミュータブルバックアップ

答え・解説

Q0080 正答：A. 脆弱性パッチ管理

解説：中心となる論点は脆弱性パッチ管理である。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。

Q0081

クラウド・エンドポイント
タグ：脆弱性パッチ管理
用語：脆弱性パッチ管理の確認ポイント9：修正情報の収集、評価、検証、適用、確認を管理する活動

「修正情報の収集、評価、検証、適用、確認を管理する活動」という特徴を持つものを選べ。

A. EDR
B. 脆弱性パッチ管理
C. CSPM
D. イミュータブルバックアップ

答え・解説

Q0081 正答：B. 脆弱性パッチ管理

解説：脆弱性パッチ管理が該当する。定義は修正情報の収集、評価、検証、適用、確認を管理する活動であり、他の候補とは機能が異なる。

Q0082

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント1：通常操作では変更・削除できない状態で保持するバックアップ

次の説明に最も合う用語はどれか。通常操作では変更・削除できない状態で保持するバックアップ

A. クラウドIAM
B. コンテナイメージ署名
C. イミュータブルバックアップ
D. アプリケーション許可リスト

答え・解説

Q0082 正答：C. イミュータブルバックアップ

解説：イミュータブルバックアップは、通常操作では変更・削除できない状態で保持するバックアップ。ほかの選択肢は目的又は適用場面が異なる。

Q0083

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント2：通常操作では変更・削除できない状態で保持するバックアップ

イミュータブルバックアップの説明として最も適切なものはどれか。

A. クラウド資源への主体、役割、権限、認証を管理する仕組み
B. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
C. 承認済みプログラムだけの実行を認める制御
D. 通常操作では変更・削除できない状態で保持するバックアップ

答え・解説

Q0083 正答：D. 通常操作では変更・削除できない状態で保持するバックアップ

解説：イミュータブルバックアップの要点は「通常操作では変更・削除できない状態で保持するバックアップ」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。

Q0084

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント3：通常操作では変更・削除できない状態で保持するバックアップ

用語と説明の組合せとして適切なものはどれか。論点は「イミュータブルバックアップ」である。

A. イミュータブルバックアップ：通常操作では変更・削除できない状態で保持するバックアップ
B. クラウドIAM：通常操作では変更・削除できない状態で保持するバックアップ
C. コンテナイメージ署名：通常操作では変更・削除できない状態で保持するバックアップ
D. アプリケーション許可リスト：通常操作では変更・削除できない状態で保持するバックアップ

答え・解説

Q0084 正答：A. イミュータブルバックアップ：通常操作では変更・削除できない状態で保持するバックアップ

解説：正しい組合せは「イミュータブルバックアップ：通常操作では変更・削除できない状態で保持するバックアップ」。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。

Q0085

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント4：通常操作では変更・削除できない状態で保持するバックアップ
「イミュータブルバックアップ」は、通常操作では変更・削除できない状態で保持するバックアップ。

A. ○
B. ×

答え・解説

Q0085 正答：○
解説：正しい。イミュータブルバックアップは通常操作では変更・削除できない状態で保持するバックアップ。実務では対象、目的、前提条件を併せて確認する。

Q0086

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント5：通常操作では変更・削除できない状態で保持するバックアップ
組織が「通常操作では変更・削除できない状態で保持するバックアップ」ために採用すべき概念又は仕組みはどれか。

A. クラウドIAM
B. コンテナイメージ署名
C. イミュータブルバックアップ
D. アプリケーション許可リスト

答え・解説

Q0086 正答：C. イミュータブルバックアップ
解説：この目的に対応するのはイミュータブルバックアップである。通常操作では変更・削除できない状態で保持するバックアップという機能・考え方を持つためである。

Q0087

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント6：通常操作では変更・削除できない状態で保持するバックアップ

「イミュータブルバックアップ」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. 承認済みプログラムだけの実行を認める制御
B. イメージの作成元と改ざんの有無を検証するため署名を付与する仕組み
C. クラウド資源への主体、役割、権限、認証を管理する仕組み
D. 通常操作では変更・削除できない状態で保持するバックアップ

答え・解説

Q0087 正答：D. 通常操作では変更・削除できない状態で保持するバックアップ
解説：イミュータブルバックアップは通常操作では変更・削除できない状態で保持するバックアップ。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント7：通常操作では変更・削除できない状態で保持するバックアップ

「イミュータブルバックアップ」は、クラウド資源への主体、役割、権限、認証を管理する仕組み。

A. ○
B. ×

答え・解説

Q0088 正答：×
解説：誤り。記述はクラウドIAMの説明である。イミュータブルバックアップは通常操作では変更・削除できない状態で保持するバックアップ。

Q0089

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント8：通常操作では変更・削除できない状態で保持するバックアップ

次の状況で中心となる論点はどれか。「通常操作では変更・削除できない状態で保持するバックアップ」ことが求められている。

A. コンテナイメージ署名
B. イミュータブルバックアップ
C. アプリケーション許可リスト
D. クラウドIAM

答え・解説

Q0089 正答：B. イミュータブルバックアップ
解説：中心となる論点はイミュータブル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。

Q0090

クラウド・エンドポイント
タグ：イミュータブルバックアップ
用語：イミュータブルバックアップの確認ポイント9：通常操作では変更・削除できない状態で保持するバックアップ

「通常操作では変更・削除できない状態で保持するバックアップ」という特徴を持つものを選べ。

A. アプリケーション許可リスト
B. コンテナイメージ署名
C. イミュータブルバックアップ
D. クラウドIAM

答え・解説

Q0090 正答：C. イミュータブルバックアップ
解説：イミュータブルバックアップが該当する。定義は通常操作では変更・削除できない状態で保持するバックアップであり、他の候補とは機能が異なる。