

Q0001

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント1：企画・設計段階から安全性を組み込む開発の考え方

次の説明に最も合う用語はどれか。企画・設計段階から安全性を組み込む開発の考え方

- A. セキュリティバイデザイン
- B. セキュアコーディング
- C. 変更管理
- D. 委託先管理

答え・解説

Q0001 正答：A. セキュリティバイデザイン

解説：セキュリティバイデザインは、企画・設計段階から安全性を組み込む開発の考え方。ほかの選択肢は目的又は適用場面が異なる。

Q0002

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント2：企画・設計段階から安全性を組み込む開発の考え方

セキュリティバイデザインの説明として最も適切なものはどれか。

- A. 脆弱性を作り込まないように安全な実装規則に従ってプログラムをすること
- B. 企画・設計段階から安全性を組み込む開発の考え方
- C. システム変更を申請、評価、承認、実施、記録する管理プロセス
- D. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

答え・解説

Q0002 正答：B. 企画・設計段階から安全性を組み込む開発の考え方

解説：セキュリティバイデザインの要点は「企画・設計段階から安全性を組み込む開発の考え方」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。

Q0003

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント3：企画・設計段階から安全性を組み込む開発の考え方

用語と説明の組合せとして適切なものはどれか。論点は「セキュリティバイデザイン」である。

- A. セキュアコーディング：企画・設計段階から安全性を組み込む開発の考え方
- B. 変更管理：企画・設計段階から安全性を組み込む開発の考え方
- C. セキュリティバイデザイン：企画・設計段階から安全性を組み込む開発の考え方
- D. 委託先管理：企画・設計段階から安全性を組み込む開発の考え方

答え・解説

Q0003 正答：C. セキュリティバイデザイン：企画・設計段階から安全性を組み込む開発の考え方

解説：正しい組合せは「セキュリティバイデザイン：企画・設計段階から安全性を組み込む開発の考え方」。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。

Q0004

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント4：企画・設計段階から安全性を組み込む開発の考え方

「セキュリティバイデザイン」は、企画・設計段階から安全性を組み込む開発の考え方。

- A. ○
- B. ×

答え・解説

Q0004 正答：○

解説：正しい。セキュリティバイデザインは企画・設計段階から安全性を組み込む開発の考え方。実務では対象、目的、前提条件を併せて確認する。

Q0005

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント5：企画・設計段階から安全性を組み込む開発の考え方

組織が「企画・設計段階から安全性を組み込む開発の考え方」ために採用すべき概念又は仕組みはどれか。

- A. セキュリティバイデザイン
- B. セキュアコーディング
- C. 変更管理
- D. 委託先管理

答え・解説

Q0005 正答：A. セキュリティバイデザイン

解説：この目的に対応するのはセキュリティバイデザインである。企画・設計段階から安全性を組み込む開発の考え方という機能・考え方を持つためである。

Q0006

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント6：企画・設計段階から安全性を組み込む開発の考え方

「セキュリティバイデザイン」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. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- B. 企画・設計段階から安全性を組み込む開発の考え方
- C. システム変更を申請、評価、承認、実施、記録する管理プロセス
- D. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムをすること

答え・解説

Q0006 正答：B. 企画・設計段階から安全性を組み込む開発の考え方

解説：セキュリティバイデザインは企画・設計段階から安全性を組み込む開発の考え方。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント7：企画・設計段階から安全性を組み込む開発の考え方

「セキュリティバイデザイン」は、脆弱性を作り込まないよう安全な実装規則に従ってプログラムをすること。

- A. ○
- B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述はセキュアコーディングの説明である。セキュリティバイデザインは企画・設計段階から安全性を組み込む開発の考え方。

Q0008

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント8：企画・設計段階から安全性を組み込む開発の考え方

次の状況で中心となる論点はどれか。「企画・設計段階から安全性を組み込む開発の考え方」ことが求められている。

- A. 変更管理
- B. 委託先管理
- C. セキュアコーディング
- D. セキュリティバイデザイン

答え・解説

Q0008 正答：D. セキュリティバイデザイン

解説：中心となる論点はセキュリティバイデザインである。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。

Q0009

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント9：企画・設計段階から安全性を組み込む開発の考え方

セキュリティバイデザインを選定するときは、「企画・設計段階から安全性を組み込む開発の考え方」という本来の目的に合うかを確認する。

A. ○

B. ×

答え・解説

Q0009 正答：○

解説：正しい。セキュリティバイデザインの選定・運用では、企画・設計段階から安全性を組み込む開発の考え方という目的との適合を確認する。

Q0010

安全な開発・運用

タグ：セキュリティバイデザイン

用語：セキュリティバイデザインの確認ポイント10：企画・設計段階から安全性を組み込む開発の考え方

セキュリティバイデザインは、企画・設計段階から安全性を組み込む開発の考え方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。セキュリティバイデザインはまさに企画・設計段階から安全性を組み込む開発の考え方という意味を持つ。

Q0011

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント1：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作成すること

次の説明に最も合う用語はどれか。脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作成すること

- A. 入力値検証
- B. セキュアコーディング
- C. 構成管理
- D. 脆弱性管理

答え・解説

Q0011 正答：B. セキュアコーディング

解説：セキュアコーディングは、脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作成すること。ほかの選択肢は目的又は適用場面が異なる。

Q0012

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント2：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作成すること

セキュアコーディングの説明として最も適切なものはどれか。

- A. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策
- B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- C. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作成すること
- D. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

答え・解説

Q0012 正答：C. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作成すること

解説：セキュアコーディングの要点は「脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作成すること」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

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント3：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること

用語と説明の組合せとして適切なものはどれか。論点は「セキュアコーディング」である。

- A. 入力値検証：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること
- B. 構成管理：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること
- C. 脆弱性管理：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること
- D. セキュアコーディング：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること

答え・解説

Q0013 正答：D. セキュアコーディング：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること

解説：正しい組合せは「セキュアコーディング：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること」。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

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント4：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること

「セキュアコーディング」は、脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること。

- A. ○
- B. ×

答え・解説

Q0014 正答：○

解説：正しい。セキュアコーディングは脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること。実務では対象、目的、前提条件を併せて確認する。

Q0015

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント5：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを
作ること

組織が「脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること」のために採用すべき概念又は仕組みはどれか。

- A. 入力値検証
- B. セキュアコーディング
- C. 構成管理
- D. 脆弱性管理

答え・解説

Q0015 正答：B. セキュアコーディング

解説：この目的に対応するのはセキュアコーディングである。脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ることという機能・考え方を持つためである。

Q0016

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント6：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを
作ること

「セキュアコーディング」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. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- C. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること
- D. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策

答え・解説

Q0016 正答：C. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムを
作ること

解説：セキュアコーディングは脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること。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

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント7：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを
作成すること

「セキュアコーディング」は、外部から受け取るデータの型、長さ、範囲、形式を確認する対策。

- A. ○
- B. ×

答え・解説

Q0017 正答：×

解説：誤り。記述は入力値検証の説明である。セキュアコーディングは脆弱性を作り込まないよう安全な実装規則に従ってプログラムをすること。

Q0018

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント8：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを
作成すること

次の状況で中心となる論点はどれか。「脆弱性を作り込まないよう安全な実装規則に従ってプログラムをすること」ことが求められている。

- A. セキュアコーディング
- B. 構成管理
- C. 脆弱性管理
- D. 入力値検証

答え・解説

Q0018 正答：A. セキュアコーディング

解説：中心となる論点はセキュアコーディングである。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

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント9：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること

セキュアコーディング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。セキュアコーディングは脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ることという概念であり、対象・目的・前提条件の確認が必要である。

Q0020

安全な開発・運用

タグ：セキュアコーディング

用語：セキュアコーディングの確認ポイント10：脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること

セキュアコーディングと他の類似概念を区別する際は、「脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ること」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。セキュアコーディングの定義は脆弱性を作り込まないよう安全な実装規則に従ってプログラムを作ることであり、類似概念との区別に使える。

Q0021

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント1：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

次の説明に最も合う用語はどれか。外部から受け取るデータの型、長さ、範囲、形式を確認する対策

- A. 変更管理
- B. ログ管理
- C. 入力値検証
- D. 職務分掌

答え・解説

Q0021 正答：C. 入力値検証

解説：入力値検証は、外部から受け取るデータの型、長さ、範囲、形式を確認する対策。ほかの選択肢は目的又は適用場面が異なる。

Q0022

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント2：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

入力値検証の説明として最も適切なものはどれか。

- A. システム変更を申請、評価、承認、実施、記録する管理プロセス
- B. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- C. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- D. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策

答え・解説

Q0022 正答：D. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策

解説：入力値検証の要点は「外部から受け取るデータの型、長さ、範囲、形式を確認する対策」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

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント3：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

用語と説明の組合せとして適切なものはどれか。論点は「入力値検証」である。

- A. 入力値検証：外部から受け取るデータの型、長さ、範囲、形式を確認する対策
- B. 変更管理：外部から受け取るデータの型、長さ、範囲、形式を確認する対策
- C. ログ管理：外部から受け取るデータの型、長さ、範囲、形式を確認する対策
- D. 職務分掌：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

答え・解説

Q0023 正答：A. 入力値検証：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

解説：正しい組合せは「入力値検証：外部から受け取るデータの型、長さ、範囲、形式を確認する対策」。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

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント4：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

「入力値検証」は、外部から受け取るデータの型、長さ、範囲、形式を確認する対策。

- A. ○
- B. ×

答え・解説

Q0024 正答：○

解説：正しい。入力値検証は外部から受け取るデータの型、長さ、範囲、形式を確認する対策。実務では対象、目的、前提条件を併せて確認する。

Q0025

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント5：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

組織が「外部から受け取るデータの型、長さ、範囲、形式を確認する対策」ために採用すべき概念又は仕組みはどれか。

- A. 変更管理
- B. ログ管理
- C. 入力値検証
- D. 職務分掌

答え・解説

Q0025 正答：C. 入力値検証

解説：この目的に対応するのは入力値検証である。外部から受け取るデータの型、長さ、範囲、形式を確認する対策という機能・考え方を持つためである。

Q0026

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント6：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

「入力値検証」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. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- B. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- C. システム変更を申請、評価、承認、実施、記録する管理プロセス
- D. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策

答え・解説

Q0026 正答：D. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策

解説：入力値検証は外部から受け取るデータの型、長さ、範囲、形式を確認する対策。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

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント7：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

「入力値検証」は、システム変更を申請、評価、承認、実施、記録する管理プロセス。

- A. ○
- B. ×

答え・解説

Q0027 正答：×

解説：誤り。記述は変更管理の説明である。入力値検証は外部から受け取るデータの型、長さ、範囲、形式を確認する対策。

Q0028

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント8：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

次の状況で中心となる論点はどれか。「外部から受け取るデータの型、長さ、範囲、形式を確認する対策」ことが求められている。

- A. ログ管理
- B. 入力値検証
- C. 職務分掌
- D. 変更管理

答え・解説

Q0028 正答：B. 入力値検証

解説：中心となる論点は入力値検証である。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

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント9：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

入力値検証を選定するときは、「外部から受け取るデータの型、長さ、範囲、形式を確認する対策」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。入力値検証の選定・運用では、外部から受け取るデータの型、長さ、範囲、形式を確認する対策という目的との適合を確認する。

Q0030

安全な開発・運用

タグ：入力値検証

用語：入力値検証の確認ポイント10：外部から受け取るデータの型、長さ、範囲、形式を確認する対策

入力値検証は、外部から受け取るデータの型、長さ、範囲、形式を確認する対策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。入力値検証はまさに外部から受け取るデータの型、長さ、範囲、形式を確認する対策という意味を持つ。

Q0031

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント1：システム変更を申請、評価、承認、実施、記録する管理プロセス

次の説明に最も合う用語はどれか。システム変更を申請、評価、承認、実施、記録する管理プロセス

- A. 構成管理
- B. アクセス権レビュー
- C. セキュリティバイデザイン
- D. 変更管理

答え・解説

Q0031 正答：D. 変更管理

解説：変更管理は、システム変更を申請、評価、承認、実施、記録する管理プロセス。ほかの選択肢は目的又は適用場面が異なる。

Q0032

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント2：システム変更を申請、評価、承認、実施、記録する管理プロセス

変更管理の説明として最も適切なものはどれか。

- A. システム変更を申請、評価、承認、実施、記録する管理プロセス
- B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- C. 付与済み権限が現在の職務に必要なかを定期的に確認する活動
- D. 企画・設計段階から安全性を組み込む開発の考え方

答え・解説

Q0032 正答：A. システム変更を申請、評価、承認、実施、記録する管理プロセス

解説：変更管理の要点は「システム変更を申請、評価、承認、実施、記録する管理プロセス」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

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント3：システム変更を申請、評価、承認、実施、記録する管理プロセス

用語と説明の組合せとして適切なものはどれか。論点は「変更管理」である。

- A. 構成管理：システム変更を申請、評価、承認、実施、記録する管理プロセス
- B. 変更管理：システム変更を申請、評価、承認、実施、記録する管理プロセス
- C. アクセス権レビュー：システム変更を申請、評価、承認、実施、記録する管理プロセス
- D. セキュリティバイデザイン：システム変更を申請、評価、承認、実施、記録する管理プロセス

答え・解説

Q0033 正答：B. 変更管理：システム変更を申請、評価、承認、実施、記録する管理プロセス

解説：正しい組合せは「変更管理：システム変更を申請、評価、承認、実施、記録する管理プロセス」。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

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント4：システム変更を申請、評価、承認、実施、記録する管理プロセス

「変更管理」は、システム変更を申請、評価、承認、実施、記録する管理プロセス。

- A. ○
- B. ×

答え・解説

Q0034 正答：○

解説：正しい。変更管理はシステム変更を申請、評価、承認、実施、記録する管理プロセス。実務では対象、目的、前提条件を併せて確認する。

Q0035

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント5：システム変更を申請、評価、承認、実施、記録する管理プロセス

組織が「システム変更を申請、評価、承認、実施、記録する管理プロセス」ために採用すべき概念又は仕組みはどれか。

- A. 構成管理
- B. アクセス権レビュー
- C. セキュリティバイデザイン
- D. 変更管理

答え・解説

Q0035 正答：D. 変更管理

解説：この目的に対応するのは変更管理である。システム変更を申請、評価、承認、実施、記録する管理プロセスという機能・考え方を持つためである。

Q0036

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント6：システム変更を申請、評価、承認、実施、記録する管理プロセス

「変更管理」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. システム変更を申請、評価、承認、実施、記録する管理プロセス
- B. 企画・設計段階から安全性を組み込む開発の考え方
- C. 付与済み権限が現在の職務に必要なかを定期的に確認する活動
- D. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

答え・解説

Q0036 正答：A. システム変更を申請、評価、承認、実施、記録する管理プロセス

解説：変更管理はシステム変更を申請、評価、承認、実施、記録する管理プロセス。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

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント7：システム変更を申請、評価、承認、実施、記録する管理プロセス

「変更管理」は、機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動。

- A. ○
- B. ×

答え・解説

Q0037 正答：×

解説：誤り。記述は構成管理の説明である。変更管理はシステム変更を申請、評価、承認、実施、記録する管理プロセス。

Q0038

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント8：システム変更を申請、評価、承認、実施、記録する管理プロセス

次の状況で中心となる論点はどれか。「システム変更を申請、評価、承認、実施、記録する管理プロセス」ことが求められている。

- A. アクセス権レビュー
- B. セキュリティバイデザイン
- C. 変更管理
- D. 構成管理

答え・解説

Q0038 正答：C. 変更管理

解説：中心となる論点は変更管理である。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。

Q0039

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント9：システム変更を申請、評価、承認、実施、記録する管理プロセス

変更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

Q0039 正答：×

解説：誤り。変更管理はシステム変更を申請、評価、承認、実施、記録する管理プロセスという概念であり、対象・目的・前提条件の確認が必要である。

Q0040

安全な開発・運用

タグ：変更管理

用語：変更管理の確認ポイント10：システム変更を申請、評価、承認、実施、記録する管理プロセス

変更管理と他の類似概念を区別する際は、「システム変更を申請、評価、承認、実施、記録する管理プロセス」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。変更管理の定義はシステム変更を申請、評価、承認、実施、記録する管理プロセスであり、類似概念との区別に使える。

Q0041

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント1：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

次の説明に最も合う用語はどれか。機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

- A. 構成管理
- B. ログ管理
- C. 委託先管理
- D. セキュアコーディング

答え・解説

Q0041 正答：A. 構成管理

解説：構成管理は、機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0042

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント2：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

構成管理の説明として最も適切なものはどれか。

- A. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- C. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- D. 脆弱性を作り込まないように安全な実装規則に従ってプログラムをすること

答え・解説

Q0042 正答：B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

解説：構成管理の要点は「機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動」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。

Q0043

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント3：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

用語と説明の組合せとして適切なものはどれか。論点は「構成管理」である。

- A. ログ管理：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- B. 委託先管理：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- C. 構成管理：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- D. セキュアコーディング：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

答え・解説

Q0043 正答：C. 構成管理：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

解説：正しい組合せは「構成管理：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動」。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。

Q0044

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント4：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

「構成管理」は、機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動。

- A. ○
- B. ×

答え・解説

Q0044 正答：○

解説：正しい。構成管理は機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動。実務では対象、目的、前提条件を併せて確認する。

Q0045

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント5：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

組織が「機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動」のために採用すべき概念又は仕組みはどれか。

- A. 構成管理
- B. ログ管理
- C. 委託先管理
- D. セキュアコーディング

答え・解説

Q0045 正答：A. 構成管理

解説：この目的に対応するのは構成管理である。機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動という機能・考え方を持つためである。

Q0046

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント6：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

「構成管理」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. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムをすること
- B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- C. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- D. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

答え・解説

Q0046 正答：B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

解説：構成管理は機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0047

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント7：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

「構成管理」は、ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理。

- A. ○
- B. ×

答え・解説

Q0047 正答：×

解説：誤り。記述はログ管理の説明である。構成管理は機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動。

Q0048

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント8：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

次の状況で中心となる論点はどれか。「機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動」ことが求められている。

- A. 委託先管理
- B. セキュアコーディング
- C. ログ管理
- D. 構成管理

答え・解説

Q0048 正答：D. 構成管理

解説：中心となる論点は構成管理である。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。

Q0049

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント9：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

構成管理を選定するときは、「機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動」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。構成管理の選定・運用では、機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動という目的との適合を確認する。

Q0050

安全な開発・運用

タグ：構成管理

用語：構成管理の確認ポイント10：機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

構成管理は、機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動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。構成管理はまさに機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動という意味を持つ。

Q0051

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント1：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

次の説明に最も合う用語はどれか。ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

- A. アクセス権レビュー
- B. ログ管理
- C. 脆弱性管理
- D. 入力値検証

答え・解説

Q0051 正答：B. ログ管理

解説：ログ管理は、ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理。ほかの選択肢は目的又は適用場面が異なる。

Q0052

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント2：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

ログ管理の説明として最も適切なものはどれか。

- A. 付与済み権限が現在の職務に必要なかを定期的に確認する活動
- B. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- C. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- D. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策

答え・解説

Q0052 正答：C. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

解説：ログ管理の要点は「ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理」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

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント3：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

用語と説明の組合せとして適切なものはどれか。論点は「ログ管理」である。

- A. アクセス権レビュー：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- B. 脆弱性管理：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- C. 入力値検証：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- D. ログ管理：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

答え・解説

Q0053 正答：D. ログ管理：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

解説：正しい組合せは「ログ管理：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理」。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

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント4：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

「ログ管理」は、ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理。

- A. ○
- B. ×

答え・解説

Q0054 正答：○

解説：正しい。ログ管理はログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理。実務では対象、目的、前提条件を併せて確認する。

Q0055

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント5：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

組織が「ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理」ために採用すべき概念又は仕組みはどれか。

- A. アクセス権レビュー
- B. ログ管理
- C. 脆弱性管理
- D. 入力値検証

答え・解説

Q0055 正答：B. ログ管理

解説：この目的に対応するのはログ管理である。ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理という機能・考え方を持つためである。

Q0056

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント6：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

「ログ管理」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. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策
- B. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- C. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- D. 付与済み権限が現在の職務に必要なかを定期的に確認する活動

答え・解説

Q0056 正答：C. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

解説：ログ管理はログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理。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

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント7：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

「ログ管理」は、付与済み権限が現在の職務に必要なかを定期的に確認する活動。

- A. ○
- B. ×

答え・解説

Q0057 正答：×

解説：誤り。記述はアクセス権レビューの説明である。ログ管理はログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理。

Q0058

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント8：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

次の状況で中心となる論点はどれか。「ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理」ことが求められている。

- A. ログ管理
- B. 脆弱性管理
- C. 入力値検証
- D. アクセス権レビュー

答え・解説

Q0058 正答：A. ログ管理

解説：中心となる論点はログ管理である。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

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント9：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

ログ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。ログ管理はログの取得、時刻同期、保護、保存、分析、廃棄を適切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

安全な開発・運用

タグ：ログ管理

用語：ログ管理の確認ポイント10：ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

ログ管理と他の類似概念を区別する際は、「ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理」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。ログ管理の定義はログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理であり、類似概念との区別に使える。

Q0061

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント1：付与済み権限が現在の職務に必要なかを定期的に確認する活動

次の説明に最も合う用語はどれか。付与済み権限が現在の職務に必要なかを定期的に確認する活動

- A. 委託先管理
- B. 職務分掌
- C. アクセス権レビュー
- D. 変更管理

答え・解説

Q0061 正答：C. アクセス権レビュー

解説：アクセス権レビューは、付与済み権限が現在の職務に必要なかを定期的に確認する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0062

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント2：付与済み権限が現在の職務に必要なかを定期的に確認する活動

アクセス権レビューの説明として最も適切なものはどれか。

- A. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- B. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- C. システム変更を申請、評価、承認、実施、記録する管理プロセス
- D. 付与済み権限が現在の職務に必要なかを定期的に確認する活動

答え・解説

Q0062 正答：D. 付与済み権限が現在の職務に必要なかを定期的に確認する活動

解説：アクセス権レビューの要点は「付与済み権限が現在の職務に必要なかを定期的に確認する活動」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。

Q0063

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント3：付与済み権限が現在の職務に必要なかを定期的に確認する活動

用語と説明の組合せとして適切なものはどれか。論点は「アクセス権レビュー」である。

- A. アクセス権レビュー：付与済み権限が現在の職務に必要なかを定期的に確認する活動
- B. 委託先管理：付与済み権限が現在の職務に必要なかを定期的に確認する活動
- C. 職務分掌：付与済み権限が現在の職務に必要なかを定期的に確認する活動
- D. 変更管理：付与済み権限が現在の職務に必要なかを定期的に確認する活動

答え・解説

Q0063 正答：A. アクセス権レビュー：付与済み権限が現在の職務に必要なかを定期的に確認する活動

解説：正しい組合せは「アクセス権レビュー：付与済み権限が現在の職務に必要なかを定期的に確認する活動」。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。

Q0064

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント4：付与済み権限が現在の職務に必要なかを定期的に確認する活動

「アクセス権レビュー」は、付与済み権限が現在の職務に必要なかを定期的に確認する活動。

- A. ○
- B. ×

答え・解説

Q0064 正答：○

解説：正しい。アクセス権レビューは付与済み権限が現在の職務に必要なかを定期的に確認する活動。実務では対象、目的、前提条件を併せて確認する。

Q0065

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント5：付与済み権限が現在の職務に必要なかを定期的に確認する活動

組織が「付与済み権限が現在の職務に必要なかを定期的に確認する活動」ために採用すべき概念又は仕組みはどれか。

- A. 委託先管理
- B. 職務分掌
- C. アクセス権レビュー
- D. 変更管理

答え・解説

Q0065 正答：C. アクセス権レビュー

解説：この目的に対応するのはアクセス権レビューである。付与済み権限が現在の職務に必要なかを定期的に確認する活動という機能・考え方を持つためである。

Q0066

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント6：付与済み権限が現在の職務に必要なかを定期的に確認する活動

「アクセス権レビュー」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. システム変更を申請、評価、承認、実施、記録する管理プロセス
- B. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- C. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- D. 付与済み権限が現在の職務に必要なかを定期的に確認する活動

答え・解説

Q0066 正答：D. 付与済み権限が現在の職務に必要なかを定期的に確認する活動

解説：アクセス権レビューは付与済み権限が現在の職務に必要なかを定期的に確認する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0067

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント7：付与済み権限が現在の職務に必要なかを定期的に確認する活動

「アクセス権レビュー」は、委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動。

- A. ○
- B. ×

答え・解説

Q0067 正答：×

解説：誤り。記述は委託先管理の説明である。アクセス権レビューは付与済み権限が現在の職務に必要なかを定期的に確認する活動。

Q0068

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント8：付与済み権限が現在の職務に必要なかを定期的に確認する活動

次の状況で中心となる論点はどれか。「付与済み権限が現在の職務に必要なかを定期的に確認する活動」ことが求められている。

- A. 職務分掌
- B. アクセス権レビュー
- C. 変更管理
- D. 委託先管理

答え・解説

Q0068 正答：B. アクセス権レビュー

解説：中心となる論点はアクセス権レビューである。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

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント9：付与済み権限が現在の職務に必要なかを定期的に確認する活動

アクセス権レビューを選定するときは、「付与済み権限が現在の職務に必要なかを定期的に確認する活動」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。アクセス権レビューの選定・運用では、付与済み権限が現在の職務に必要なかを定期的に確認する活動という目的との適合を確認する。

Q0070

安全な開発・運用

タグ：アクセス権レビュー

用語：アクセス権レビューの確認ポイント10：付与済み権限が現在の職務に必要なかを定期的に確認する活動

アクセス権レビューは、付与済み権限が現在の職務に必要なかを定期的に確認する活動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。アクセス権レビューはまさに付与済み権限が現在の職務に必要なかを定期的に確認する活動という意味を持つ。

Q0071

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント1：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
次の説明に最も合う用語はどれか。委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

- A. 脆弱性管理
- B. セキュリティバイデザイン
- C. 構成管理
- D. 委託先管理

答え・解説

Q0071 正答：D. 委託先管理

解説：委託先管理は、委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0072

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント2：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
委託先管理の説明として最も適切なものはどれか。

- A. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- B. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- C. 企画・設計段階から安全性を組み込む開発の考え方
- D. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動

答え・解説

Q0072 正答：A. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

解説：委託先管理の要点は「委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動」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。

Q0073

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント3：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

用語と説明の組合せとして適切なものはどれか。論点は「委託先管理」である。

- A. 脆弱性管理：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- B. 委託先管理：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- C. セキュリティバイデザイン：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- D. 構成管理：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

答え・解説

Q0073 正答：B. 委託先管理：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

解説：正しい組合せは「委託先管理：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動」。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。

Q0074

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント4：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

「委託先管理」は、委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動。

- A. ○
- B. ×

答え・解説

Q0074 正答：○

解説：正しい。委託先管理は委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動。実務では対象、目的、前提条件を併せて確認する。

Q0075

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント5：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
組織が「委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動」ために採用すべき概念又は仕組みはどれか。

- A. 脆弱性管理
- B. セキュリティバイデザイン
- C. 構成管理
- D. 委託先管理

答え・解説

Q0075 正答：D. 委託先管理

解説：この目的に対応するのは委託先管理である。委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動という機能・考え方を持つためである。

Q0076

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント6：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
「委託先管理」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. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動
- B. 機器、ソフトウェア、設定、版などの構成項目を識別し管理する活動
- C. 企画・設計段階から安全性を組み込む開発の考え方
- D. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

答え・解説

Q0076 正答：A. 委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

解説：委託先管理は委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0077

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント7：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

「委託先管理」は、脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動。

- A. ○
- B. ×

答え・解説

Q0077 正答：×

解説：誤り。記述は脆弱性管理の説明である。委託先管理は委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動。

Q0078

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント8：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

次の状況で中心となる論点はどれか。「委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動」ことが求められている。

- A. セキュリティバイデザイン
- B. 構成管理
- C. 委託先管理
- D. 脆弱性管理

答え・解説

Q0078 正答：C. 委託先管理

解説：中心となる論点は委託先管理である。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。

Q0079

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント9：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

委託先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

Q0079 正答：×

解説：誤り。委託先管理は委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動という概念であり、対象・目的・前提条件の確認が必要である。

Q0080

安全な開発・運用

タグ：委託先管理

用語：委託先管理の確認ポイント10：委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動

委託先管理と他の類似概念を区別する際は、「委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動」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。委託先管理の定義は委託先の選定、契約、監督、終了時処置を通じて外部リスクを管理する活動であり、類似概念との区別に使える。

Q0081

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント1：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

次の説明に最も合う用語はどれか。脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

- A. 脆弱性管理
- B. 職務分掌
- C. セキュアコーディング
- D. ログ管理

答え・解説

Q0081 正答：A. 脆弱性管理

解説：脆弱性管理は、脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動。ほかの選択肢は目的又は適用場面が異なる。

Q0082

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント2：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

脆弱性管理の説明として最も適切なものはどれか。

- A. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- B. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- C. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムをすること
- D. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理

答え・解説

Q0082 正答：B. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

解説：脆弱性管理の要点は「脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動」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。

Q0083

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント3：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

用語と説明の組合せとして適切なものはどれか。論点は「脆弱性管理」である。

- A. 職務分掌：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- B. セキュアコーディング：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- C. 脆弱性管理：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- D. ログ管理：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

答え・解説

Q0083 正答：C. 脆弱性管理：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

解説：正しい組合せは「脆弱性管理：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動」。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。

Q0084

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント4：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

「脆弱性管理」は、脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動。

- A. ○
- B. ×

答え・解説

Q0084 正答：○

解説：正しい。脆弱性管理は脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動。実務では対象、目的、前提条件を併せて確認する。

Q0085

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント5：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

組織が「脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動」のために採用すべき概念又は仕組みはどれか。

- A. 脆弱性管理
- B. 職務分掌
- C. セキュアコーディング
- D. ログ管理

答え・解説

Q0085 正答：A. 脆弱性管理

解説：この目的に対応するのは脆弱性管理である。脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動という機能・考え方を持つためである。

Q0086

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント6：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

「脆弱性管理」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. ログの取得、時刻同期、保護、保存、分析、廃棄を適切に行う管理
- B. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動
- C. 脆弱性を作り込まないよう安全な実装規則に従ってプログラムをすること
- D. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

答え・解説

Q0086 正答：B. 脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

解説：脆弱性管理は脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0087

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント7：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

「脆弱性管理」は、一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制。

- A. ○
- B. ×

答え・解説

Q0087 正答：×

解説：誤り。記述は職務分掌の説明である。脆弱性管理は脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動。

Q0088

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント8：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

次の状況で中心となる論点はどれか。「脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動」ことが求められている。

- A. セキュアコーディング
- B. ログ管理
- C. 職務分掌
- D. 脆弱性管理

答え・解説

Q0088 正答：D. 脆弱性管理

解説：中心となる論点は脆弱性管理である。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。

Q0089

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント9：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

脆弱性管理を選定するときは、「脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動」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。脆弱性管理の選定・運用では、脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動という目的との適合を確認する。

Q0090

安全な開発・運用

タグ：脆弱性管理

用語：脆弱性管理の確認ポイント10：脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動

脆弱性管理は、脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動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。脆弱性管理はまさに脆弱性情報の収集、影響評価、優先順位付け、修正、確認を行う活動という意味を持つ。

Q0091

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント1：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

次の説明に最も合う用語はどれか。一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

- A. セキュリティバイデザイン
- B. 職務分掌
- C. 入力値検証
- D. アクセス権レビュー

答え・解説

Q0091 正答：B. 職務分掌

解説：職務分掌は、一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制。ほかの選択肢は目的又は適用場面が異なる。

Q0092

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント2：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

職務分掌の説明として最も適切なものはどれか。

- A. 企画・設計段階から安全性を組み込む開発の考え方
- B. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策
- C. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- D. 付与済み権限が現在の職務に必要なかを定期的に確認する活動

答え・解説

Q0092 正答：C. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

解説：職務分掌の要点は「一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制」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

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント3：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

用語と説明の組合せとして適切なものはどれか。論点は「職務分掌」である。

- A. セキュリティバイデザイン：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- B. 入力値検証：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- C. アクセス権レビュー：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- D. 職務分掌：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

答え・解説

Q0093 正答：D. 職務分掌：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

解説：正しい組合せは「職務分掌：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制」。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

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント4：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

「職務分掌」は、一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制。

- A. ○
- B. ×

答え・解説

Q0094 正答：○

解説：正しい。職務分掌は一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制。実務では対象、目的、前提条件を併せて確認する。

Q0095

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント5：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

組織が「一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制」のために採用すべき概念又は仕組みはどれか。

- A. セキュリティバイデザイン
- B. 職務分掌
- C. 入力値検証
- D. アクセス権レビュー

答え・解説

Q0095 正答：B. 職務分掌

解説：この目的に対応するのは職務分掌である。一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制という機能・考え方を持つためである。

Q0096

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント6：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

「職務分掌」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. 付与済み権限が現在の職務に必要なかを定期的に確認する活動
- B. 外部から受け取るデータの型、長さ、範囲、形式を確認する対策
- C. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制
- D. 企画・設計段階から安全性を組み込む開発の考え方

答え・解説

Q0096 正答：C. 一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

解説：職務分掌は一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制。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

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント7：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

「職務分掌」は、企画・設計段階から安全性を組み込む開発の考え方。

A. ○

B. ×

答え・解説

Q0097 正答：×

解説：誤り。記述はセキュリティバイデザインの説明である。職務分掌は一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制。

Q0098

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント8：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

次の状況で中心となる論点はどれか。「一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制」ことが求められている。

A. 職務分掌

B. 入力値検証

C. アクセス権レビュー

D. セキュリティバイデザイン

答え・解説

Q0098 正答：A. 職務分掌

解説：中心となる論点は職務分掌である。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

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント9：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

職務分掌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。職務分掌は一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制という概念であり、対象・目的・前提条件の確認が必要である。

Q0100

安全な開発・運用

タグ：職務分掌

用語：職務分掌の確認ポイント10：一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制

職務分掌と他の類似概念を区別する際は、「一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制」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。職務分掌の定義は一人に相反する権限を集中させず、不正や誤りを抑止・検知する統制であり、類似概念との区別に使える。