Q0001

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント1：組織が目的達成のために受け入れる意思のあるリスクの種類と量

次の説明に最も合う用語はどれか。組織が目的達成のために受け入れる意思のあるリスクの種類と量

A. リスク登録簿
B. リスクアペタイト
C. セキュリティメトリクス
D. NIST CSF

答え・解説

Q0001 正答：B. リスクアペタイト

解説：リスクアペタイトは、組織が目的達成のために受け入れる意思のあるリスクの種類と量。ほかの選択肢は目的又は適用場面が異なる。

Q0002

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント2：組織が目的達成のために受け入れる意思のあるリスクの種類と量

リスクアペタイトの説明として最も適切なものはどれか。

A. 特定したリスク、所有者、評価、対応、期限などを記録する台帳
B. 管理策の実施状況や有効性を測定する指標
C. 組織が目的達成のために受け入れる意思のあるリスクの種類と量
D. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

答え・解説

Q0002 正答：C. 組織が目的達成のために受け入れる意思のあるリスクの種類と量

解説：リスクアペタイトの要点は「組織が目的達成のために受け入れる意思のあるリスクの種類と量」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

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント3：組織が目的達成のために受け入れる意思のあるリスクの種類と量

用語と説明の組合せとして適切なものはどれか。論点は「リスクアペタイト」である。

A. リスク登録簿：組織が目的達成のために受け入れる意思のあるリスクの種類と量
B. セキュリティメトリクス：組織が目的達成のために受け入れる意思のあるリスクの種類と量
C. NIST CSF：組織が目的達成のために受け入れる意思のあるリスクの種類と量
D. リスクアペタイト：組織が目的達成のために受け入れる意思のあるリスクの種類と量

答え・解説

Q0003 正答：D. リスクアペタイト：組織が目的達成のために受け入れる意思のあるリスクの種類と量

解説：正しい組合せは「リスクアペタイト：組織が目的達成のために受け入れる意思のあるリスクの種類と量」。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

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント4：組織が目的達成のために受け入れる意思のあるリスクの種類と量

「リスクアペタイト」は、組織が目的達成のために受け入れる意思のあるリスクの種類と量。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。リスクアペタイトは組織が目的達成のために受け入れる意思のあるリスクの種類と量。実務では対象、目的、前提条件を併せて確認する。

Q0005

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント5：組織が目的達成のために受け入れる意思のあるリスクの種類と量

組織が「組織が目的達成のために受け入れる意思のあるリスクの種類と量」ために採用すべき概念又は仕組みはどれか。

A. リスク登録簿
B. リスクアペタイト
C. セキュリティメトリクス
D. NIST CSF

答え・解説

Q0005 正答：B. リスクアペタイト

解説：この目的に対応するのはリスクアペタイトである。組織が目的達成のために受け入れる意思のあるリスクの種類と量という機能・考え方を持つためである。

Q0006

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント6：組織が目的達成のために受け入れる意思のあるリスクの種類と量

「リスクアペタイト」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. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
B. 管理策の実施状況や有効性を測定する指標
C. 組織が目的達成のために受け入れる意思のあるリスクの種類と量
D. 特定したリスク、所有者、評価、対応、期限などを記録する台帳

答え・解説

Q0006 正答：C. 組織が目的達成のために受け入れる意思のあるリスクの種類と量

解説：リスクアペタイトは組織が目的達成のために受け入れる意思のあるリスクの種類と量。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

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント7：組織が目的達成のために受け入れる意思のあるリスクの種類と量

「リスクアペタイト」は、特定したリスク、所有者、評価、対応、期限などを記録する台帳。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述はリスク登録簿の説明である。リスクアペタイトは組織が目的達成のために受け入れる意思のあるリスクの種類と量。

Q0008

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント8：組織が目的達成のために受け入れる意思のあるリスクの種類と量

次の状況で中心となる論点はどれか。「組織が目的達成のために受け入れる意思のあるリスクの種類と量」ことが求められている。

A. リスクアペタイト
B. セキュリティメトリクス
C. NIST CSF
D. リスク登録簿

答え・解説

Q0008 正答：A. リスクアペタイト

解説：中心となる論点はリスクアペタイトである。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。

Q0009

ガバナンス・リスク
タグ：リスクアペタイト
用語：リスクアペタイトの確認ポイント9：組織が目的達成のために受け入れる意思のあるリスクの種類と量

「組織が目的達成のために受け入れる意思のあるリスクの種類と量」という特徴を持つものを選べ。

A. NIST CSF
B. リスクアペタイト
C. セキュリティメトリクス
D. リスク登録簿

答え・解説

Q0009 正答：B. リスクアペタイト

解説：リスクアペタイトが該当する。定義は組織が目的達成のために受け入れる意思のあるリスクの種類と量であり、他の候補とは機能が異なる。

Q0010

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント1：特定したリスク、所有者、評価、対応、期限などを記録する台帳

次の説明に最も合う用語はどれか。特定したリスク、所有者、評価、対応、期限などを記録する台帳

A. 脅威モデリング
B. サプライチェーンリスク
C. リスク登録簿
D. ゼロトラストアーキテクチャ

答え・解説

Q0010 正答：C. リスク登録簿

解説：リスク登録簿は、特定したリスク、所有者、評価、対応、期限などを記録する台帳。ほかの選択肢は目的又は適用場面が異なる。

Q0011

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント2：特定したリスク、所有者、評価、対応、期限などを記録する台帳

リスク登録簿の説明として最も適切なものはどれか。

A. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
B. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
C. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
D. 特定したリスク、所有者、評価、対応、期限などを記録する台帳

答え・解説

Q0011 正答：D. 特定したリスク、所有者、評価、対応、期限などを記録する台帳

解説：リスク登録簿の要点は「特定したリスク、所有者、評価、対応、期限などを記録する台帳」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

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント3：特定したリスク、所有者、評価、対応、期限などを記録する台帳

用語と説明の組合せとして適切なものはどれか。論点は「リスク登録簿」である。

A. リスク登録簿：特定したリスク、所有者、評価、対応、期限などを記録する台帳
B. 脅威モデリング：特定したリスク、所有者、評価、対応、期限などを記録する台帳
C. サプライチェーンリスク：特定したリスク、所有者、評価、対応、期限などを記録する台帳
D. ゼロトラストアーキテクチャ：特定したリスク、所有者、評価、対応、期限などを記録する台帳

答え・解説

Q0012 正答：A. リスク登録簿：特定したリスク、所有者、評価、対応、期限などを記録する台帳

解説：正しい組合せは「リスク登録簿：特定したリスク、所有者、評価、対応、期限などを記録する台帳」。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

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント4：特定したリスク、所有者、評価、対応、期限などを記録する台帳
「リスク登録簿」は、特定したリスク、所有者、評価、対応、期限などを記録する台帳。

A. ○
B. ×

答え・解説

Q0013 正答：○
解説：正しい。リスク登録簿は特定したリスク、所有者、評価、対応、期限などを記録する台帳。実務では対象、目的、前提条件を併せて確認する。

Q0014

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント5：特定したリスク、所有者、評価、対応、期限などを記録する台帳
組織が「特定したリスク、所有者、評価、対応、期限などを記録する台帳」ために採用すべき概念又は仕組みはどれか。

A. 脅威モデリング
B. サプライチェーンリスク
C. リスク登録簿
D. ゼロトラストアーキテクチャ

答え・解説

Q0014 正答：C. リスク登録簿
解説：この目的に対応するのはリスク登録簿である。特定したリスク、所有者、評価、対応、期限などを記録する台帳という機能・考え方を持つためである。

Q0015

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント6：特定したリスク、所有者、評価、対応、期限などを記録する台帳

「リスク登録簿」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. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
B. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
C. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
D. 特定したリスク、所有者、評価、対応、期限などを記録する台帳

答え・解説

Q0015 正答：D. 特定したリスク、所有者、評価、対応、期限などを記録する台帳

解説：リスク登録簿は特定したリスク、所有者、評価、対応、期限などを記録する台帳。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

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント7：特定したリスク、所有者、評価、対応、期限などを記録する台帳

「リスク登録簿」は、資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述は脅威モデリングの説明である。リスク登録簿は特定したリスク、所有者、評価、対応、期限などを記録する台帳。

Q0017

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント8：特定したリスク、所有者、評価、対応、期限などを記録する台帳

次の状況で中心となる論点はどれか。「特定したリスク、所有者、評価、対応、期限などを記録する台帳」ことが求められている。

A. サプライチェーンリスク
B. リスク登録簿
C. ゼロトラストアーキテクチャ
D. 脅威モデリング

答え・解説

Q0017 正答：B. リスク登録簿

解説：中心となる論点はリスク登録簿である。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

ガバナンス・リスク
タグ：リスク登録簿
用語：リスク登録簿の確認ポイント9：特定したリスク、所有者、評価、対応、期限などを記録する台帳

「特定したリスク、所有者、評価、対応、期限などを記録する台帳」という特徴を持つものを選べ。

A. ゼロトラストアーキテクチャ
B. サプライチェーンリスク
C. リスク登録簿
D. 脅威モデリング

答え・解説

Q0018 正答：C. リスク登録簿

解説：リスク登録簿が該当する。定義は特定したリスク、所有者、評価、対応、期限などを記録する台帳であり、他の候補とは機能が異なる。

Q0019

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント1：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

次の説明に最も合う用語はどれか。資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

A. セキュリティメトリクス
B. 第三者リスク管理
C. セキュリティ例外管理
D. 脅威モデリング

答え・解説

Q0019 正答：D. 脅威モデリング

解説：脅威モデリングは、資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0020

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント2：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

脅威モデリングの説明として最も適切なものはどれか。

A. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
B. 管理策の実施状況や有効性を測定する指標
C. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動
D. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

答え・解説

Q0020 正答：A. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

解説：脅威モデリングの要点は「資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動」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。

Q0021

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント3：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

用語と説明の組合せとして適切なものはどれか。論点は「脅威モデリング」である。

A. セキュリティメトリクス：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
B. 脅威モデリング：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
C. 第三者リスク管理：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
D. セキュリティ例外管理：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

答え・解説

Q0021 正答：B. 脅威モデリング：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

解説：正しい組合せは「脅威モデリング：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動」。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。

Q0022

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント4：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

「脅威モデリング」は、資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。脅威モデリングは資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動。実務では対象、目的、前提条件を併せて確認する。

Q0023

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント5：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

組織が「資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動」ために採用すべき概念又は仕組みはどれか。

A. セキュリティメトリクス
B. 第三者リスク管理
C. セキュリティ例外管理
D. 脅威モデリング

答え・解説

Q0023 正答：D. 脅威モデリング

解説：この目的に対応するのは脅威モデリングである。資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動という機能・考え方を持つためである。

Q0024

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント6：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

「脅威モデリング」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. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
B. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
C. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動
D. 管理策の実施状況や有効性を測定する指標

答え・解説

Q0024 正答：A. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動

解説：脅威モデリングは資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0025

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント7：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
「脅威モデリング」は、管理策の実施状況や有効性を測定する指標。

A. ○
B. ×

答え・解説

Q0025 正答：×
解説：誤り。記述はセキュリティメトリクスの説明である。脅威モデリングは資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動。

Q0026

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント8：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
次の状況で中心となる論点はどれか。「資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動」ことが求められている。

A. 第三者リスク管理
B. セキュリティ例外管理
C. 脅威モデリング
D. セキュリティメトリクス

答え・解説

Q0026 正答：C. 脅威モデリング
解説：中心となる論点は脅威モデリングである。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。

Q0027

ガバナンス・リスク
タグ：脅威モデリング
用語：脅威モデリングの確認ポイント9：資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
「資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動」という特徴を持つものを選べ。

A. セキュリティ例外管理
B. 第三者リスク管理
C. セキュリティメトリクス
D. 脅威モデリング

答え・解説

Q0027 正答：D. 脅威モデリング
解説：脅威モデリングが該当する。定義は資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動であり、他の候補とは機能が異なる。

Q0028

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント1：管理策の実施状況や有効性を測定する指標
次の説明に最も合う用語はどれか。管理策の実施状況や有効性を測定する指標

A. セキュリティメトリクス
B. サプライチェーンリスク
C. ISO/IEC 27001
D. リスクアペタイト

答え・解説

Q0028 正答：A. セキュリティメトリクス
解説：セキュリティメトリクスは、管理策の実施状況や有効性を測定する指標。ほかの選択肢は目的又は適用場面が異なる。

Q0029

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント2：管理策の実施状況や有効性を測定する指標

セキュリティメトリクスの説明として最も適切なものはどれか。

A. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
B. 管理策の実施状況や有効性を測定する指標
C. ISMSの要求事項を定める国際規格
D. 組織が目的達成のために受け入れる意思のあるリスクの種類と量

答え・解説

Q0029 正答：B. 管理策の実施状況や有効性を測定する指標

解説：セキュリティメトリクスの要点は「管理策の実施状況や有効性を測定する指標」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

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント3：管理策の実施状況や有効性を測定する指標

用語と説明の組合せとして適切なものはどれか。論点は「セキュリティメトリクス」である。

A. サプライチェーンリスク：管理策の実施状況や有効性を測定する指標
B. ISO/IEC 27001：管理策の実施状況や有効性を測定する指標
C. セキュリティメトリクス：管理策の実施状況や有効性を測定する指標
D. リスクアペタイト：管理策の実施状況や有効性を測定する指標

答え・解説

Q0030 正答：C. セキュリティメトリクス：管理策の実施状況や有効性を測定する指標

解説：正しい組合せは「セキュリティメトリクス：管理策の実施状況や有効性を測定する指標」。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

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント4：管理策の実施状況や有効性を測定する指標
「セキュリティメトリクス」は、管理策の実施状況や有効性を測定する指標。

A. ○
B. ×

答え・解説

Q0031 正答：○
解説：正しい。セキュリティメトリクスは管理策の実施状況や有効性を測定する指標。実務では対象、目的、前提条件を併せて確認する。

Q0032

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント5：管理策の実施状況や有効性を測定する指標
組織が「管理策の実施状況や有効性を測定する指標」ために採用すべき概念又は仕組みはどれか。

A. セキュリティメトリクス
B. サプライチェーンリスク
C. ISO/IEC 27001
D. リスクアペタイト

答え・解説

Q0032 正答：A. セキュリティメトリクス
解説：この目的に対応するのはセキュリティメトリクスである。管理策の実施状況や有効性を測定する指標という機能・考え方を持つためである。

Q0033

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント6：管理策の実施状況や有効性を測定する指標

「セキュリティメトリクス」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. 組織が目的達成のために受け入れる意思のあるリスクの種類と量
B. 管理策の実施状況や有効性を測定する指標
C. ISMSの要求事項を定める国際規格
D. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

答え・解説

Q0033 正答：B. 管理策の実施状況や有効性を測定する指標

解説：セキュリティメトリクスは管理策の実施状況や有効性を測定する指標。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

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント7：管理策の実施状況や有効性を測定する指標

「セキュリティメトリクス」は、委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク。

A. ○
B. ×

答え・解説

Q0034 正答：×

解説：誤り。記述はサプライチェーンリスクの説明である。セキュリティメトリクスは管理策の実施状況や有効性を測定する指標。

Q0035

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント8：管理策の実施状況や有効性を測定する指標

次の状況で中心となる論点はどれか。「管理策の実施状況や有効性を測定する指標」ことが求められている。

A. ISO/IEC 27001
B. リスクアペタイト
C. サプライチェーンリスク
D. セキュリティメトリクス

答え・解説

Q0035 正答：D. セキュリティメトリクス

解説：中心となる論点はセキュリティメトリクスである。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

ガバナンス・リスク
タグ：セキュリティメトリクス
用語：セキュリティメトリクスの確認ポイント9：管理策の実施状況や有効性を測定する指標

「管理策の実施状況や有効性を測定する指標」という特徴を持つものを選べ。

A. セキュリティメトリクス
B. リスクアペタイト
C. ISO/IEC 27001
D. サプライチェーンリスク

答え・解説

Q0036 正答：A. セキュリティメトリクス

解説：セキュリティメトリクスが該当する。定義は管理策の実施状況や有効性を測定する指標であり、他の候補とは機能が異なる。

Q0037

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント1：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

次の説明に最も合う用語はどれか。委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

A. 第三者リスク管理
B. サプライチェーンリスク
C. NIST CSF
D. リスク登録簿

答え・解説

Q0037 正答：B. サプライチェーンリスク

解説：サプライチェーンリスクは、委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク。ほかの選択肢は目的又は適用場面が異なる。

Q0038

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント2：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

サプライチェーンリスクの説明として最も適切なものはどれか。

A. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動
B. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
C. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
D. 特定したリスク、所有者、評価、対応、期限などを記録する台帳

答え・解説

Q0038 正答：C. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

解説：サプライチェーンリスクの要点は「委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク」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

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント3：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

用語と説明の組合せとして適切なものはどれか。論点は「サプライチェーンリスク」である。

A. 第三者リスク管理：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
B. NIST CSF：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
C. リスク登録簿：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
D. サプライチェーンリスク：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

答え・解説

Q0039 正答：D. サプライチェーンリスク：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

解説：正しい組合せは「サプライチェーンリスク：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク」。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

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント4：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

「サプライチェーンリスク」は、委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。サプライチェーンリスクは委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク。実務では対象、目的、前提条件を併せて確認する。

Q0041

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント5：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

組織が「委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク」ために採用すべき概念又は仕組みはどれか。

A. 第三者リスク管理
B. サプライチェーンリスク
C. NIST CSF
D. リスク登録簿

答え・解説

Q0041 正答：B. サプライチェーンリスク

解説：この目的に対応するのはサプライチェーンリスクである。委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスクという機能・考え方を持つためである。

Q0042

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント6：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

「サプライチェーンリスク」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. 特定したリスク、所有者、評価、対応、期限などを記録する台帳
B. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
C. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
D. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

答え・解説

Q0042 正答：C. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

解説：サプライチェーンリスクは委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク。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

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント7：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

「サプライチェーンリスク」は、外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述は第三者リスク管理の説明である。サプライチェーンリスクは委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク。

Q0044

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント8：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

次の状況で中心となる論点はどれか。「委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク」ことが求められている。

A. サプライチェーンリスク
B. NIST CSF
C. リスク登録簿
D. 第三者リスク管理

答え・解説

Q0044 正答：A. サプライチェーンリスク

解説：中心となる論点はサプライチェーンリスクである。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

ガバナンス・リスク
タグ：サプライチェーンリスク
用語：サプライチェーンリスクの確認ポイント9：委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

「委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク」という特徴を持つものを選べ。

A. リスク登録簿
B. サプライチェーンリスク
C. NIST CSF
D. 第三者リスク管理

答え・解説

Q0045 正答：B. サプライチェーンリスク

解説：サプライチェーンリスクが該当する。定義は委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスクであり、他の候補とは機能が異なる。

Q0046

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント1：外部事業者の選定、評価、契約、監視、終了を通じて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。外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

A. ISO/IEC 27001
B. ゼロトラストアーキテクチャ
C. 第三者リスク管理
D. 脅威モデリング

答え・解説

Q0046 正答：C. 第三者リスク管理

解説：第三者リスク管理は、外部事業者の選定、評価、契約、監視、終了を通じて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。

Q0047

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント2：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

第三者リスク管理の説明として最も適切なものはどれか。

A. ISMSの要求事項を定める国際規格
B. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
C. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
D. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

答え・解説

Q0047 正答：D. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

解説：第三者リスク管理の要点は「外部事業者の選定、評価、契約、監視、終了を通じて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。

Q0048

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント3：外部事業者の選定、評価、契約、監視、終了を通じて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「第三者リスク管理」である。

A. 第三者リスク管理：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動
B. ISO/IEC 27001：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動
C. ゼロトラストアーキテクチャ：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動
D. 脅威モデリング：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

答え・解説

Q0048 正答：A. 第三者リスク管理：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

解説：正しい組合せは「第三者リスク管理：外部事業者の選定、評価、契約、監視、終了を通じて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。

Q0049

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント4：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

「第三者リスク管理」は、外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動。

A. ○
B. ×

答え・解説

Q0049 正答：○

解説：正しい。第三者リスク管理は外部事業者の選定、評価、契約、監視、終了を通じて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。

Q0050

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント5：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

組織が「外部事業者の選定、評価、契約、監視、終了を通じて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. ISO/IEC 27001
B. ゼロトラストアーキテクチャ
C. 第三者リスク管理
D. 脅威モデリング

答え・解説

Q0050 正答：C. 第三者リスク管理

解説：この目的に対応するのは第三者リスク管理である。外部事業者の選定、評価、契約、監視、終了を通じて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。

Q0051

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント6：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

「第三者リスク管理」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. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
B. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
C. ISMSの要求事項を定める国際規格
D. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

答え・解説

Q0051 正答：D. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

解説：第三者リスク管理は外部事業者の選定、評価、契約、監視、終了を通じて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。

Q0052

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント7：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

「第三者リスク管理」は、ISMSの要求事項を定める国際規格。

A. ○
B. ×

答え・解説

Q0052 正答：×

解説：誤り。記述はISO/IEC 27001の説明である。第三者リスク管理は外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動。

Q0053

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント8：外部事業者の選定、評価、契約、監視、終了を通じて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。「外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動」ことが求められている。

A. ゼロトラストアーキテクチャ
B. 第三者リスク管理
C. 脅威モデリング
D. ISO/IEC 27001

答え・解説

Q0053 正答：B. 第三者リスク管理

解説：中心となる論点は第三者リスク管理である。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。

Q0054

ガバナンス・リスク
タグ：第三者リスク管理
用語：第三者リスク管理の確認ポイント9：外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

「外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動」という特徴を持つものを選べ。

A. 脅威モデリング
B. ゼロトラストアーキテクチャ
C. 第三者リスク管理
D. ISO/IEC 27001

答え・解説

Q0054 正答：C. 第三者リスク管理

解説：第三者リスク管理が該当する。定義は外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動であり、他の候補とは機能が異なる。

Q0055

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント1：ISMSの要求事項を定める国際規格

次の説明に最も合う用語はどれか。ISMSの要求事項を定める国際規格

A. NIST CSF
B. セキュリティ例外管理
C. セキュリティメトリクス
D. ISO/IEC 27001

答え・解説

Q0055 正答：D. ISO/IEC 27001

解説：ISO/IEC 27001は、ISMSの要求事項を定める国際規格。ほかの選択肢は目的又は適用場面が異なる。

Q0056

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント2：ISMSの要求事項を定める国際規格

ISO/IEC 27001の説明として最も適切なものはどれか。

A. ISMSの要求事項を定める国際規格
B. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
C. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
D. 管理策の実施状況や有効性を測定する指標

答え・解説

Q0056 正答：A. ISMSの要求事項を定める国際規格

解説：ISO/IEC 27001の要点は「ISMSの要求事項を定める国際規格」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

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント3：ISMSの要求事項を定める国際規格

用語と説明の組合せとして適切なものはどれか。論点は「ISO/IEC 27001」である。

A. NIST CSF：ISMSの要求事項を定める国際規格
B. ISO/IEC 27001：ISMSの要求事項を定める国際規格
C. セキュリティ例外管理：ISMSの要求事項を定める国際規格
D. セキュリティメトリクス：ISMSの要求事項を定める国際規格

答え・解説

Q0057 正答：B. ISO/IEC 27001：ISMSの要求事項を定める国際規格

解説：正しい組合せは「ISO/IEC 27001：ISMSの要求事項を定める国際規格」。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

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント4：ISMSの要求事項を定める国際規格

「ISO/IEC 27001」は、ISMSの要求事項を定める国際規格。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。ISO/IEC 27001はISMSの要求事項を定める国際規格。実務では対象、目的、前提条件を併せて確認する。

Q0059

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント5：ISMSの要求事項を定める国際規格

組織が「ISMSの要求事項を定める国際規格」ために採用すべき概念又は仕組みはどれか。

A. NIST CSF
B. セキュリティ例外管理
C. セキュリティメトリクス
D. ISO/IEC 27001

答え・解説

Q0059 正答：D. ISO/IEC 27001

解説：この目的に対応するのはISO/IEC 27001である。ISMSの要求事項を定める国際規格という機能・考え方を持つためである。

Q0060

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント6：ISMSの要求事項を定める国際規格

「ISO/IEC 27001」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. ISMSの要求事項を定める国際規格
B. 管理策の実施状況や有効性を測定する指標
C. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
D. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

答え・解説

Q0060 正答：A. ISMSの要求事項を定める国際規格

解説：ISO/IEC 27001はISMSの要求事項を定める国際規格。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

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント7：ISMSの要求事項を定める国際規格

「ISO/IEC 27001」は、識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述はNIST CSFの説明である。ISO/IEC 27001はISMSの要求事項を定める国際規格。

Q0062

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント8：ISMSの要求事項を定める国際規格

次の状況で中心となる論点はどれか。「ISMSの要求事項を定める国際規格」ことが求められている。

A. セキュリティ例外管理
B. セキュリティメトリクス
C. ISO/IEC 27001
D. NIST CSF

答え・解説

Q0062 正答：C. ISO/IEC 27001

解説：中心となる論点はISO/IEC 27001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

ガバナンス・リスク
タグ：ISO/IEC 27001
用語：ISO/IEC 27001の確認ポイント9：ISMSの要求事項を定める国際規格

「ISMSの要求事項を定める国際規格」という特徴を持つものを選べ。

A. セキュリティメトリクス
B. セキュリティ例外管理
C. NIST CSF
D. ISO/IEC 27001

答え・解説

Q0063 正答：D. ISO/IEC 27001

解説：ISO/IEC 27001が該当する。定義はISMSの要求事項を定める国際規格であり、他の候補とは機能が異なる。

Q0064

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント1：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

次の説明に最も合う用語はどれか。識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

A. NIST CSF
B. ゼロトラストアーキテクチャ
C. リスクアペタイト
D. サプライチェーンリスク

答え・解説

Q0064 正答：A. NIST CSF

解説：NIST CSFは、識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み。ほかの選択肢は目的又は適用場面が異なる。

Q0065

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント2：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

NIST CSFの説明として最も適切なものはどれか。

A. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
B. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
C. 組織が目的達成のために受け入れる意思のあるリスクの種類と量
D. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク

答え・解説

Q0065 正答：B. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

解説：NIST CSFの要点は「識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み」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。

Q0066

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント3：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

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

A. ゼロトラストアーキテクチャ：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
B. リスクアペタイト：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
C. NIST CSF：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
D. サプライチェーンリスク：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

答え・解説

Q0066 正答：C. NIST CSF：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

解説：正しい組合せは「NIST CSF：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み」。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。

Q0067

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント4：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
「NIST CSF」は、識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み。

A. ○
B. ×

答え・解説

Q0067 正答：○
解説：正しい。NIST CSFは識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み。実務では対象、目的、前提条件を併せて確認する。

Q0068

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント5：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
組織が「識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み」ために採用すべき概念又は仕組みはどれか。

A. NIST CSF
B. ゼロトラストアーキテクチャ
C. リスクアペタイト
D. サプライチェーンリスク

答え・解説

Q0068 正答：A. NIST CSF
解説：この目的に対応するのはNIST CSFである。識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組みという機能・考え方を持つためである。

Q0069

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント6：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

「NIST CSF」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. 委託先や部品・ソフトウェア供給経路を介して生じるセキュリティリスク
B. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み
C. 組織が目的達成のために受け入れる意思のあるリスクの種類と量
D. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

答え・解説

Q0069 正答：B. 識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

解説：NIST CSFは識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0070

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント7：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

「NIST CSF」は、暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述はゼロトラストアーキテクチャの説明である。NIST CSFは識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み。

Q0071

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント8：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

次の状況で中心となる論点はどれか。「識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み」ことが求められている。

A. リスクアペタイト
B. サプライチェーンリスク
C. ゼロトラストアーキテクチャ
D. NIST CSF

答え・解説

Q0071 正答：D. NIST CSF

解説：中心となる論点はNIST CSF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

ガバナンス・リスク
タグ：NIST CSF
用語：NIST CSFの確認ポイント9：識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み

「識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組み」という特徴を持つものを選べ。

A. NIST CSF
B. サプライチェーンリスク
C. リスクアペタイト
D. ゼロトラストアーキテクチャ

答え・解説

Q0072 正答：A. NIST CSF

解説：NIST CSFが該当する。定義は識別・防御・検知・対応・復旧などでサイバーリスク管理を整理する枠組みであり、他の候補とは機能が異なる。

Q0073

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント1：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

次の説明に最も合う用語はどれか。暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

A. セキュリティ例外管理
B. ゼロトラストアーキテクチャ
C. リスク登録簿
D. 第三者リスク管理

答え・解説

Q0073 正答：B. ゼロトラストアーキテクチャ

解説：ゼロトラストアーキテクチャは、暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計。ほかの選択肢は目的又は適用場面が異なる。

Q0074

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント2：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

ゼロトラストアーキテクチャの説明として最も適切なものはどれか。

A. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
B. 特定したリスク、所有者、評価、対応、期限などを記録する台帳
C. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
D. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動

答え・解説

Q0074 正答：C. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

解説：ゼロトラストアーキテクチャの要点は「暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計」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

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント3：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

用語と説明の組合せとして適切なものはどれか。論点は「ゼロトラストアーキテクチャ」である。

A. セキュリティ例外管理：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

B. リスク登録簿：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

C. 第三者リスク管理：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

D. ゼロトラストアーキテクチャ：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

答え・解説

Q0075 正答：D. ゼロトラストアーキテクチャ：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

解説：正しい組合せは「ゼロトラストアーキテクチャ：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計」。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

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント4：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

「ゼロトラストアーキテクチャ」は、暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計。

A. ○

B. ×

答え・解説

Q0076 正答：○

解説：正しい。ゼロトラストアーキテクチャは暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計。実務では対象、目的、前提条件を併せて確認する。

Q0077

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント5：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

組織が「暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計」ために採用すべき概念又は仕組みはどれか。

A. セキュリティ例外管理
B. ゼロトラストアーキテクチャ
C. リスク登録簿
D. 第三者リスク管理

答え・解説

Q0077 正答：B. ゼロトラストアーキテクチャ

解説：この目的に対応するのはゼロトラストアーキテクチャである。暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計という機能・考え方を持つためである。

Q0078

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント6：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

「ゼロトラストアーキテクチャ」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. 外部事業者の選定、評価、契約、監視、終了を通じてリスクを管理する活動
B. 特定したリスク、所有者、評価、対応、期限などを記録する台帳
C. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
D. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

答え・解説

Q0078 正答：C. 暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計

解説：ゼロトラストアーキテクチャは暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計。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

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント7：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
「ゼロトラストアーキテクチャ」は、標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動。

A. ○
B. ×

答え・解説

Q0079 正答：×
解説：誤り。記述はセキュリティ例外管理の説明である。ゼロトラストアーキテクチャは暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計。

Q0080

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント8：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
次の状況で中心となる論点はどれか。「暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計」ことが求められている。

A. ゼロトラストアーキテクチャ
B. リスク登録簿
C. 第三者リスク管理
D. セキュリティ例外管理

答え・解説

Q0080 正答：A. ゼロトラストアーキテクチャ
解説：中心となる論点はゼロトラストアーキテクチャである。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

ガバナンス・リスク
タグ：ゼロトラストアーキテクチャ
用語：ゼロトラストアーキテクチャの確認ポイント9：暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計
「暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計」という特徴を持つものを選べ。

A. 第三者リスク管理
B. ゼロトラストアーキテクチャ
C. リスク登録簿
D. セキュリティ例外管理

答え・解説

Q0081 正答：B. ゼロトラストアーキテクチャ
解説：ゼロトラストアーキテクチャが該当する。定義は暗黙の信頼を置かず、主体・端末・状況を継続評価してアクセスを許可する設計であり、他の候補とは機能が異なる。

Q0082

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント1：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
次の説明に最も合う用語はどれか。標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

A. リスクアペタイト
B. 脅威モデリング
C. セキュリティ例外管理
D. ISO/IEC 27001

答え・解説

Q0082 正答：C. セキュリティ例外管理
解説：セキュリティ例外管理は、標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0083

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント2：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

セキュリティ例外管理の説明として最も適切なものはどれか。

A. 組織が目的達成のために受け入れる意思のあるリスクの種類と量
B. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
C. ISMSの要求事項を定める国際規格
D. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

答え・解説

Q0083 正答：D. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

解説：セキュリティ例外管理の要点は「標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動」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。

Q0084

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント3：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

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

A. セキュリティ例外管理：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
B. リスクアペタイト：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
C. 脅威モデリング：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動
D. ISO/IEC 27001：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

答え・解説

Q0084 正答：A. セキュリティ例外管理：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

解説：正しい組合せは「セキュリティ例外管理：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動」。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。

Q0085

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント4：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

「セキュリティ例外管理」は、標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。セキュリティ例外管理は標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動。実務では対象、目的、前提条件を併せて確認する。

Q0086

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント5：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

組織が「標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動」ために採用すべき概念又は仕組みはどれか。

A. リスクアペタイト
B. 脅威モデリング
C. セキュリティ例外管理
D. ISO/IEC 27001

答え・解説

Q0086 正答：C. セキュリティ例外管理

解説：この目的に対応するのはセキュリティ例外管理である。標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動という機能・考え方を持つためである。

Q0087

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント6：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

「セキュリティ例外管理」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. ISMSの要求事項を定める国際規格
B. 資産、攻撃者、攻撃経路、対策を設計段階で体系的に分析する活動
C. 組織が目的達成のために受け入れる意思のあるリスクの種類と量
D. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

答え・解説

Q0087 正答：D. 標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

解説：セキュリティ例外管理は標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント7：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

「セキュリティ例外管理」は、組織が目的達成のために受け入れる意思のあるリスクの種類と量。

A. ○
B. ×

答え・解説

Q0088 正答：×

解説：誤り。記述はリスクアペタイトの説明である。セキュリティ例外管理は標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動。

Q0089

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント8：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

次の状況で中心となる論点はどれか。「標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動」ことが求められている。

A. 脅威モデリング
B. セキュリティ例外管理
C. ISO/IEC 27001
D. リスクアペタイト

答え・解説

Q0089 正答：B. セキュリティ例外管理

解説：中心となる論点はセキュリティ例外管理である。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。

Q0090

ガバナンス・リスク
タグ：セキュリティ例外管理
用語：セキュリティ例外管理の確認ポイント9：標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動

「標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動」という特徴を持つものを選べ。

A. ISO/IEC 27001
B. 脅威モデリング
C. セキュリティ例外管理
D. リスクアペタイト

答え・解説

Q0090 正答：C. セキュリティ例外管理

解説：セキュリティ例外管理が該当する。定義は標準管理策を適用できない場合の理由、代替策、期限、承認を管理する活動であり、他の候補とは機能が異なる。