情報セキュリティマネジメント試験 問題PDF

Q0001

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント1：許可された者だけが情報へアクセスできる状態を保つ性質

次の説明に最も合う用語はどれか。許可された者だけが情報へアクセスできる状態を保つ性質

A. 完全性
B. 機密性
C. 真正性
D. 脆弱性

答え・解説

Q0001 正答：B. 機密性

解説：機密性は、許可された者だけが情報へアクセスできる状態を保つ性質。ほかの選択肢は目的又は適用場面が異なる。

Q0002

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント2：許可された者だけが情報へアクセスできる状態を保つ性質

機密性の説明として最も適切なものはどれか。

A. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質
B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質
C. 許可された者だけが情報へアクセスできる状態を保つ性質
D. 脅威によって悪用され得る情報資産や管理策の弱点

答え・解説

Q0002 正答：C. 許可された者だけが情報へアクセスできる状態を保つ性質

解説：機密性の要点は「許可された者だけが情報へアクセスできる状態を保つ性質」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。

情報セキュリティマネジメント試験 問題PDF

Q0003

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント3：許可された者だけが情報へアクセスできる状態を保つ性質

用語と説明の組合せとして適切なものはどれか。論点は「機密性」である。

A. 完全性：許可された者だけが情報へアクセスできる状態を保つ性質
B. 真正性：許可された者だけが情報へアクセスできる状態を保つ性質
C. 脆弱性：許可された者だけが情報へアクセスできる状態を保つ性質
D. 機密性：許可された者だけが情報へアクセスできる状態を保つ性質

答え・解説

Q0003 正答：D. 機密性：許可された者だけが情報へアクセスできる状態を保つ性質

解説：正しい組合せは「機密性：許可された者だけが情報へアクセスできる状態を保つ性質」。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

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント4：許可された者だけが情報へアクセスできる状態を保つ性質

「機密性」は、許可された者だけが情報へアクセスできる状態を保つ性質。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。機密性は許可された者だけが情報へアクセスできる状態を保つ性質。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

Q0005

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント5：許可された者だけが情報へアクセスできる状態を保つ性質

組織が「許可された者だけが情報へアクセスできる状態を保つ性質」ために採用すべき概念又は仕組みはどれか。

A. 完全性
B. 機密性
C. 真正性
D. 脆弱性

答え・解説

Q0005 正答：B. 機密性
解説：この目的に対応するのは機密性である。許可された者だけが情報へアクセスできる状態を保つ性質という機能・考え方を持つためである。

Q0006

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント6：許可された者だけが情報へアクセスできる状態を保つ性質

「機密性」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. 脅威によって悪用され得る情報資産や管理策の弱点
B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質
C. 許可された者だけが情報へアクセスできる状態を保つ性質
D. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質

答え・解説

Q0006 正答：C. 許可された者だけが情報へアクセスできる状態を保つ性質
解説：機密性は許可された者だけが情報へアクセスできる状態を保つ性質。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報セキュリティマネジメント試験 問題PDF

Q0007

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント7：許可された者だけが情報へアクセスできる状態を保つ性質
「機密性」は、情報や処理方法が正確かつ完全であり、不正に変更されていない性質。

A. ○
B. ×

答え・解説

Q0007 正答：×
解説：誤り。記述は完全性の説明である。機密性は許可された者だけが情報へアクセスできる状態を保つ性質。

Q0008

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント8：許可された者だけが情報へアクセスできる状態を保つ性質
次の状況で中心となる論点はどれか。「許可された者だけが情報へアクセスできる状態を保つ性質」ことが求められている。

A. 機密性
B. 真正性
C. 脆弱性
D. 完全性

答え・解説

Q0008 正答：A. 機密性
解説：中心となる論点は機密性である。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

Q0009

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント9：許可された者だけが情報へアクセスできる状態を保つ性質

機密性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

Q0009 正答：×

解説：誤り。機密性は許可された者だけが情報へアクセスできる状態を保つ性質という概念であり、対象・目的・前提条件の確認が必要である。

Q0010

セキュリティ基礎・脅威
タグ：機密性
用語：機密性の確認ポイント10：許可された者だけが情報へアクセスできる状態を保つ性質

機密性と他の類似概念を区別する際は、「許可された者だけが情報へアクセスできる状態を保つ性質」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0010 正答：○

解説：正しい。機密性の定義は許可された者だけが情報へアクセスできる状態を保つ性質であり、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

Q0011

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント1：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

次の説明に最も合う用語はどれか。情報や処理方法が正確かつ完全であり、不正に変更されていない性質

A. 可用性
B. 責任追跡性
C. 完全性
D. 情報セキュリティリスク

答え・解説

Q0011 正答：C. 完全性

解説：完全性は、情報や処理方法が正確かつ完全であり、不正に変更されていない性質。ほかの選択肢は目的又は適用場面が異なる。

Q0012

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント2：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

完全性の説明として最も適切なものはどれか。

A. 許可された利用者が必要なときに情報やシステムを利用できる性質
B. ある操作を誰が行ったかを記録などから追跡できる性質
C. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
D. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質

答え・解説

Q0012 正答：D. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質

解説：完全性の要点は「情報や処理方法が正確かつ完全であり、不正に変更されていない性質」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。

情報セキュリティマネジメント試験 問題PDF

Q0013

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント3：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

用語と説明の組合せとして適切なものはどれか。論点は「完全性」である。

A. 完全性：情報や処理方法が正確かつ完全であり、不正に変更されていない性質
B. 可用性：情報や処理方法が正確かつ完全であり、不正に変更されていない性質
C. 責任追跡性：情報や処理方法が正確かつ完全であり、不正に変更されていない性質
D. 情報セキュリティリスク：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

答え・解説

Q0013 正答：A. 完全性：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

解説：正しい組合せは「完全性：情報や処理方法が正確かつ完全であり、不正に変更されていない性質」。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

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント4：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

「完全性」は、情報や処理方法が正確かつ完全であり、不正に変更されていない性質。

A. ○
B. ×

答え・解説

Q0014 正答：○

解説：正しい。完全性は情報や処理方法が正確かつ完全であり、不正に変更されていない性質。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

Q0015

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント5：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

組織が「情報や処理方法が正確かつ完全であり、不正に変更されていない性質」ために採用すべき概念又は仕組みはどれか。

A. 可用性
B. 責任追跡性
C. 完全性
D. 情報セキュリティリスク

答え・解説

Q0015 正答：C. 完全性

解説：この目的に対応するのは完全性である。情報や処理方法が正確かつ完全であり、不正に変更されていない性質という機能・考え方を持つためである。

Q0016

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント6：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

「完全性」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. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
B. ある操作を誰が行ったかを記録などから追跡できる性質
C. 許可された利用者が必要なときに情報やシステムを利用できる性質
D. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質

答え・解説

Q0016 正答：D. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質

解説：完全性は情報や処理方法が正確かつ完全であり、不正に変更されていない性質。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報セキュリティマネジメント試験 問題PDF

Q0017

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント7：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

「完全性」は、許可された利用者が必要なときに情報やシステムを利用できる性質。

A. ○
B. ×

答え・解説

Q0017 正答：×

解説：誤り。記述は可用性の説明である。完全性は情報や処理方法が正確かつ完全であり、不正に変更されていない性質。

Q0018

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント8：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

次の状況で中心となる論点はどれか。「情報や処理方法が正確かつ完全であり、不正に変更されていない性質」ことが求められている。

A. 責任追跡性
B. 完全性
C. 情報セキュリティリスク
D. 可用性

答え・解説

Q0018 正答：B. 完全性

解説：中心となる論点は完全性である。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

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント9：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

完全性を選定するときは、「情報や処理方法が正確かつ完全であり、不正に変更されていない性質」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0019 正答：○

解説：正しい。完全性の選定・運用では、情報や処理方法が正確かつ完全であり、不正に変更されていない性質という目的との適合を確認する。

Q0020

セキュリティ基礎・脅威
タグ：完全性
用語：完全性の確認ポイント10：情報や処理方法が正確かつ完全であり、不正に変更されていない性質

完全性は、情報や処理方法が正確かつ完全であり、不正に変更されていない性質という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0020 正答：×

解説：誤り。完全性はまさに情報や処理方法が正確かつ完全であり、不正に変更されていない性質という意味を持つ。

情報セキュリティマネジメント試験 問題PDF

Q0021

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント1：許可された利用者が必要なときに情報やシステムを利用できる性質
次の説明に最も合う用語はどれか。許可された利用者が必要なときに情報やシステムを利用できる性質

A. 真正性
B. 否認防止
C. 標的型攻撃
D. 可用性

答え・解説

Q0021 正答：D. 可用性
解説：可用性は、許可された利用者が必要なときに情報やシステムを利用できる性質。ほかの選択肢は目的又は適用場面が異なる。

Q0022

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント2：許可された利用者が必要なときに情報やシステムを利用できる性質
可用性の説明として最も適切なものはどれか。

A. 許可された利用者が必要なときに情報やシステムを利用できる性質
B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質
C. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質
D. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

答え・解説

Q0022 正答：A. 許可された利用者が必要なときに情報やシステムを利用できる性質
解説：可用性の要点は「許可された利用者が必要なときに情報やシステムを利用できる性質」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

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント3：許可された利用者が必要なときに情報やシステムを利用できる性質

用語と説明の組合せとして適切なものはどれか。論点は「可用性」である。

A. 真正性：許可された利用者が必要なときに情報やシステムを利用できる性質
B. 可用性：許可された利用者が必要なときに情報やシステムを利用できる性質
C. 否認防止：許可された利用者が必要なときに情報やシステムを利用できる性質
D. 標的型攻撃：許可された利用者が必要なときに情報やシステムを利用できる性質

答え・解説

Q0023 正答：B. 可用性：許可された利用者が必要なときに情報やシステムを利用できる性質

解説：正しい組合せは「可用性：許可された利用者が必要なときに情報やシステムを利用できる性質」。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

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント4：許可された利用者が必要なときに情報やシステムを利用できる性質

「可用性」は、許可された利用者が必要なときに情報やシステムを利用できる性質。

A. ○
B. ×

答え・解説

Q0024 正答：○

解説：正しい。可用性は許可された利用者が必要なときに情報やシステムを利用できる性質。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

Q0025

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント5：許可された利用者が必要なときに情報やシステムを利用できる性質

組織が「許可された利用者が必要なときに情報やシステムを利用できる性質」ために採用すべき概念又は仕組みはどれか。

A. 真正性
B. 否認防止
C. 標的型攻撃
D. 可用性

答え・解説

Q0025 正答：D. 可用性

解説：この目的に対応するのは可用性である。許可された利用者が必要なときに情報やシステムを利用できる性質という機能・考え方を持つためである。

Q0026

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント6：許可された利用者が必要なときに情報やシステムを利用できる性質

「可用性」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. 許可された利用者が必要なときに情報やシステムを利用できる性質
B. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃
C. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質
D. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

答え・解説

Q0026 正答：A. 許可された利用者が必要なときに情報やシステムを利用できる性質

解説：可用性は許可された利用者が必要なときに情報やシステムを利用できる性質。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

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント7：許可された利用者が必要なときに情報やシステムを利用できる性質

「可用性」は、利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質。

A. ○
B. ×

答え・解説

Q0027 正答：×

解説：誤り。記述は真正性の説明である。可用性は許可された利用者が必要なときに情報やシステムを利用できる性質。

Q0028

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント8：許可された利用者が必要なときに情報やシステムを利用できる性質

次の状況で中心となる論点はどれか。「許可された利用者が必要なときに情報やシステムを利用できる性質」ことが求められている。

A. 否認防止
B. 標的型攻撃
C. 可用性
D. 真正性

答え・解説

Q0028 正答：C. 可用性

解説：中心となる論点は可用性である。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

Q0029

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント9：許可された利用者が必要なときに情報やシステムを利用できる性質

可用性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

Q0029 正答：×

解説：誤り。可用性は許可された利用者が必要なときに情報やシステムを利用できる性質という概念であり、対象・目的・前提条件の確認が必要である。

Q0030

セキュリティ基礎・脅威
タグ：可用性
用語：可用性の確認ポイント10：許可された利用者が必要なときに情報やシステムを利用できる性質

可用性と他の類似概念を区別する際は、「許可された利用者が必要なときに情報やシステムを利用できる性質」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0030 正答：○

解説：正しい。可用性の定義は許可された利用者が必要なときに情報やシステムを利用できる性質であり、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

Q0031

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント1：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

次の説明に最も合う用語はどれか。利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

A. 真正性
B. 責任追跡性
C. 脅威
D. 機密性

答え・解説

Q0031 正答：A. 真正性

解説：真正性は、利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質。ほかの選択肢は目的又は適用場面が異なる。

Q0032

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント2：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

真正性の説明として最も適切なものはどれか。

A. ある操作を誰が行ったかを記録などから追跡できる性質
B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質
C. 情報資産へ損害を与える可能性がある事象又は主体
D. 許可された者だけが情報へアクセスできる状態を保つ性質

答え・解説

Q0032 正答：B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

解説：真正性の要点は「利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質」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。

情報セキュリティマネジメント試験 問題PDF

Q0033

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント3：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

用語と説明の組合せとして適切なものはどれか。論点は「真正性」である。

A. 責任追跡性：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

B. 脅威：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

C. 真正性：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

D. 機密性：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

答え・解説

Q0033 正答：C. 真正性：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

解説：正しい組合せは「真正性：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質」。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

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント4：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

「真正性」は、利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質。

A. ○

B. ×

答え・解説

Q0034 正答：○

解説：正しい。真正性は利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質。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

Q0035

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント5：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

組織が「利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質」ために採用すべき概念又は仕組みはどれか。

A. 真正性
B. 責任追跡性
C. 脅威
D. 機密性

答え・解説

Q0035 正答：A. 真正性

解説：この目的に対応するのは真正性である。利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質という機能・考え方を持つためである。

Q0036

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント6：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

「真正性」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. 許可された者だけが情報へアクセスできる状態を保つ性質
B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質
C. 情報資産へ損害を与える可能性がある事象又は主体
D. ある操作を誰が行ったかを記録などから追跡できる性質

答え・解説

Q0036 正答：B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

解説：真正性は利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質。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

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント7：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

「真正性」は、ある操作を誰が行ったかを記録などから追跡できる性質。

A. ○
B. ×

答え・解説

Q0037 正答：×

解説：誤り。記述は責任追跡性の説明である。真正性は利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質。

Q0038

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント8：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

次の状況で中心となる論点はどれか。「利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質」ことが求められている。

A. 脅威
B. 機密性
C. 責任追跡性
D. 真正性

答え・解説

Q0038 正答：D. 真正性

解説：中心となる論点は真正性である。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

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント9：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

真正性を選定するときは、「利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0039 正答：○

解説：正しい。真正性の選定・運用では、利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質という目的との適合を確認する。

Q0040

セキュリティ基礎・脅威
タグ：真正性
用語：真正性の確認ポイント10：利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

真正性は、利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0040 正答：×

解説：誤り。真正性はまさに利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質という意味を持つ。

情報セキュリティマネジメント試験 問題PDF

Q0041

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント1：ある操作を誰が行ったかを記録などから追跡できる性質

次の説明に最も合う用語はどれか。ある操作を誰が行ったかを記録などから追跡できる性質

A. 否認防止
B. 責任追跡性
C. 脆弱性
D. 完全性

答え・解説

Q0041 正答：B. 責任追跡性

解説：責任追跡性は、ある操作を誰が行ったかを記録などから追跡できる性質。ほかの選択肢は目的又は適用場面が異なる。

Q0042

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント2：ある操作を誰が行ったかを記録などから追跡できる性質

責任追跡性の説明として最も適切なものはどれか。

A. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質
B. 脅威によって悪用され得る情報資産や管理策の弱点
C. ある操作を誰が行ったかを記録などから追跡できる性質
D. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質

答え・解説

Q0042 正答：C. ある操作を誰が行ったかを記録などから追跡できる性質

解説：責任追跡性の要点は「ある操作を誰が行ったかを記録などから追跡できる性質」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。

情報セキュリティマネジメント試験 問題PDF

Q0043

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント3：ある操作を誰が行ったかを記録などから追跡できる性質

用語と説明の組合せとして適切なものはどれか。論点は「責任追跡性」である。

A. 否認防止：ある操作を誰が行ったかを記録などから追跡できる性質
B. 脆弱性：ある操作を誰が行ったかを記録などから追跡できる性質
C. 完全性：ある操作を誰が行ったかを記録などから追跡できる性質
D. 責任追跡性：ある操作を誰が行ったかを記録などから追跡できる性質

答え・解説

Q0043 正答：D. 責任追跡性：ある操作を誰が行ったかを記録などから追跡できる性質

解説：正しい組合せは「責任追跡性：ある操作を誰が行ったかを記録などから追跡できる性質」。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

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント4：ある操作を誰が行ったかを記録などから追跡できる性質

「責任追跡性」は、ある操作を誰が行ったかを記録などから追跡できる性質。

A. ○
B. ×

答え・解説

Q0044 正答：○

解説：正しい。責任追跡性はある操作を誰が行ったかを記録などから追跡できる性質。実務では対象、目的、前提条件を併せて確認する。

Q0045

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント5：ある操作を誰が行ったかを記録などから追跡できる性質

組織が「ある操作を誰が行ったかを記録などから追跡できる性質」ために採用すべき概念又は仕組みはどれか。

A. 否認防止
B. 責任追跡性
C. 脆弱性
D. 完全性

答え・解説

Q0045 正答：B. 責任追跡性

解説：この目的に対応するのは責任追跡性である。ある操作を誰が行ったかを記録などから追跡できる性質という機能・考え方を持つためである。

Q0046

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント6：ある操作を誰が行ったかを記録などから追跡できる性質

「責任追跡性」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. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質
B. 脅威によって悪用され得る情報資産や管理策の弱点
C. ある操作を誰が行ったかを記録などから追跡できる性質
D. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

答え・解説

Q0046 正答：C. ある操作を誰が行ったかを記録などから追跡できる性質

解説：責任追跡性はある操作を誰が行ったかを記録などから追跡できる性質。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報セキュリティマネジメント試験 問題PDF

Q0047

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント7：ある操作を誰が行ったかを記録などから追跡できる性質

「責任追跡性」は、当事者が後から処理や送信の事実を否定できないよう証拠を残す性質。

A. ○
B. ×

答え・解説

Q0047 正答：×

解説：誤り。記述は否認防止の説明である。責任追跡性はある操作を誰が行ったかを記録などから追跡できる性質。

Q0048

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント8：ある操作を誰が行ったかを記録などから追跡できる性質

次の状況で中心となる論点はどれか。「ある操作を誰が行ったかを記録などから追跡できる性質」ことが求められている。

A. 責任追跡性
B. 脆弱性
C. 完全性
D. 否認防止

答え・解説

Q0048 正答：A. 責任追跡性

解説：中心となる論点は責任追跡性である。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

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント9：ある操作を誰が行ったかを記録などから追跡できる性質

責任追跡性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

Q0049 正答：×

解説：誤り。責任追跡性はある操作を誰が行ったかを記録などから追跡できる性質という概念であり、対象・目的・前提条件の確認が必要である。

Q0050

セキュリティ基礎・脅威
タグ：責任追跡性
用語：責任追跡性の確認ポイント10：ある操作を誰が行ったかを記録などから追跡できる性質

責任追跡性と他の類似概念を区別する際は、「ある操作を誰が行ったかを記録などから追跡できる性質」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0050 正答：○

解説：正しい。責任追跡性の定義はある操作を誰が行ったかを記録などから追跡できる性質であり、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

Q0051

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント1：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

次の説明に最も合う用語はどれか。当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

A. 脅威
B. 情報セキュリティリスク
C. 否認防止
D. 可用性

答え・解説

Q0051 正答：C. 否認防止

解説：否認防止は、当事者が後から処理や送信の事実を否定できないよう証拠を残す性質。ほかの選択肢は目的又は適用場面が異なる。

Q0052

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント2：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

否認防止の説明として最も適切なものはどれか。

A. 情報資産へ損害を与える可能性がある事象又は主体
B. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
C. 許可された利用者が必要なときに情報やシステムを利用できる性質
D. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

答え・解説

Q0052 正答：D. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

解説：否認防止の要点は「当事者が後から処理や送信の事実を否定できないよう証拠を残す性質」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

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント3：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

用語と説明の組合せとして適切なものはどれか。論点は「否認防止」である。

A. 否認防止：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質
B. 脅威：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質
C. 情報セキュリティリスク：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質
D. 可用性：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

答え・解説

Q0053 正答：A. 否認防止：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

解説：正しい組合せは「否認防止：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質」。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

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント4：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

「否認防止」は、当事者が後から処理や送信の事実を否定できないよう証拠を残す性質。

A. ○
B. ×

答え・解説

Q0054 正答：○

解説：正しい。否認防止は当事者が後から処理や送信の事実を否定できないよう証拠を残す性質。実務では対象、目的、前提条件を併せて確認する。

Q0055

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント5：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

組織が「当事者が後から処理や送信の事実を否定できないよう証拠を残す性質」ために採用すべき概念又は仕組みはどれか。

A. 脅威
B. 情報セキュリティリスク
C. 否認防止
D. 可用性

答え・解説

Q0055 正答：C. 否認防止

解説：この目的に対応するのは否認防止である。当事者が後から処理や送信の事実を否定できないよう証拠を残す性質という機能・考え方を持つためである。

Q0056

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント6：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

「否認防止」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. 許可された利用者が必要なときに情報やシステムを利用できる性質
B. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
C. 情報資産へ損害を与える可能性がある事象又は主体
D. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

答え・解説

Q0056 正答：D. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

解説：否認防止は当事者が後から処理や送信の事実を否定できないよう証拠を残す性質。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

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント7：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

「否認防止」は、情報資産へ損害を与える可能性がある事象又は主体。

A. ○
B. ×

答え・解説

Q0057 正答：×

解説：誤り。記述は脅威の説明である。否認防止は当事者が後から処理や送信の事実を否定できないよう証拠を残す性質。

Q0058

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント8：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

次の状況で中心となる論点はどれか。「当事者が後から処理や送信の事実を否定できないよう証拠を残す性質」ことが求められている。

A. 情報セキュリティリスク
B. 否認防止
C. 可用性
D. 脅威

答え・解説

Q0058 正答：B. 否認防止

解説：中心となる論点は否認防止である。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

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント9：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

否認防止を選定するときは、「当事者が後から処理や送信の事実を否定できないよう証拠を残す性質」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0059 正答：○

解説：正しい。否認防止の選定・運用では、当事者が後から処理や送信の事実を否定できないよう証拠を残す性質という目的との適合を確認する。

Q0060

セキュリティ基礎・脅威
タグ：否認防止
用語：否認防止の確認ポイント10：当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

否認防止は、当事者が後から処理や送信の事実を否定できないよう証拠を残す性質という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0060 正答：×

解説：誤り。否認防止はまさに当事者が後から処理や送信の事実を否定できないよう証拠を残す性質という意味を持つ。

情報セキュリティマネジメント試験 問題PDF

Q0061

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント1：情報資産へ損害を与える可能性がある事象又は主体

次の説明に最も合う用語はどれか。情報資産へ損害を与える可能性がある事象又は主体

A. 脆弱性
B. 標的型攻撃
C. 真正性
D. 脅威

答え・解説

Q0061 正答：D. 脅威

解説：脅威は、情報資産へ損害を与える可能性がある事象又は主体。ほかの選択肢は目的又は適用場面が異なる。

Q0062

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント2：情報資産へ損害を与える可能性がある事象又は主体

脅威の説明として最も適切なものはどれか。

A. 情報資産へ損害を与える可能性がある事象又は主体
B. 脅威によって悪用され得る情報資産や管理策の弱点
C. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃
D. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質

答え・解説

Q0062 正答：A. 情報資産へ損害を与える可能性がある事象又は主体

解説：脅威の要点は「情報資産へ損害を与える可能性がある事象又は主体」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。

情報セキュリティマネジメント試験 問題PDF

Q0063

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント3：情報資産へ損害を与える可能性がある事象又は主体

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」である。

A. 脆弱性：情報資産へ損害を与える可能性がある事象又は主体
B. 脅威：情報資産へ損害を与える可能性がある事象又は主体
C. 標的型攻撃：情報資産へ損害を与える可能性がある事象又は主体
D. 真正性：情報資産へ損害を与える可能性がある事象又は主体

答え・解説

Q0063 正答：B. 脅威：情報資産へ損害を与える可能性がある事象又は主体

解説：正しい組合せは「脅威：情報資産へ損害を与える可能性がある事象又は主体」。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

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント4：情報資産へ損害を与える可能性がある事象又は主体

「脅威」は、情報資産へ損害を与える可能性がある事象又は主体。

A. ○
B. ×

答え・解説

Q0064 正答：○

解説：正しい。脅威は情報資産へ損害を与える可能性がある事象又は主体。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

Q0065

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント5：情報資産へ損害を与える可能性がある事象又は主体

組織が「情報資産へ損害を与える可能性がある事象又は主体」ために採用すべき概念又は仕組みはどれか。

A. 脆弱性
B. 標的型攻撃
C. 真正性
D. 脅威

答え・解説

Q0065 正答：D. 脅威

解説：この目的に対応するのは脅威である。情報資産へ損害を与える可能性がある事象又は主体という機能・考え方を持つためである。

Q0066

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント6：情報資産へ損害を与える可能性がある事象又は主体

「脅威」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. 情報資産へ損害を与える可能性がある事象又は主体
B. 利用者・プロセス・情報などが主張どおり本物であることを確かめられる性質
C. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃
D. 脅威によって悪用され得る情報資産や管理策の弱点

答え・解説

Q0066 正答：A. 情報資産へ損害を与える可能性がある事象又は主体

解説：脅威は情報資産へ損害を与える可能性がある事象又は主体。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報セキュリティマネジメント試験 問題PDF

Q0067

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント7：情報資産へ損害を与える可能性がある事象又は主体

「脅威」は、脅威によって悪用され得る情報資産や管理策の弱点。

A. ○
B. ×

答え・解説

Q0067 正答：×

解説：誤り。記述は脆弱性の説明である。脅威は情報資産へ損害を与える可能性がある事象又は主体。

Q0068

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント8：情報資産へ損害を与える可能性がある事象又は主体

次の状況で中心となる論点はどれか。「情報資産へ損害を与える可能性がある事象又は主体」ことが求められている。

A. 標的型攻撃
B. 真正性
C. 脅威
D. 脆弱性

答え・解説

Q0068 正答：C. 脅威

解説：中心となる論点は脅威である。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

Q0069

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント9：情報資産へ損害を与える可能性がある事象又は主体

脅威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

Q0069 正答：×

解説：誤り。脅威は情報資産へ損害を与える可能性がある事象又は主体という概念であり、対象・目的・前提条件の確認が必要である。

Q0070

セキュリティ基礎・脅威
タグ：脅威
用語：脅威の確認ポイント10：情報資産へ損害を与える可能性がある事象又は主体

脅威と他の類似概念を区別する際は、「情報資産へ損害を与える可能性がある事象又は主体」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0070 正答：○

解説：正しい。脅威の定義は情報資産へ損害を与える可能性がある事象又は主体であり、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

Q0071

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント1：脅威によって悪用され得る情報資産や管理策の弱点

次の説明に最も合う用語はどれか。脅威によって悪用され得る情報資産や管理策の弱点

A. 脆弱性
B. 情報セキュリティリスク
C. 機密性
D. 責任追跡性

答え・解説

Q0071 正答：A. 脆弱性

解説：脆弱性は、脅威によって悪用され得る情報資産や管理策の弱点。ほかの選択肢は目的又は適用場面が異なる。

Q0072

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント2：脅威によって悪用され得る情報資産や管理策の弱点

脆弱性の説明として最も適切なものはどれか。

A. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
B. 脅威によって悪用され得る情報資産や管理策の弱点
C. 許可された者だけが情報へアクセスできる状態を保つ性質
D. ある操作を誰が行ったかを記録などから追跡できる性質

答え・解説

Q0072 正答：B. 脅威によって悪用され得る情報資産や管理策の弱点

解説：脆弱性の要点は「脅威によって悪用され得る情報資産や管理策の弱点」である。名称が似た概念でも、対象とする処理や目的を区別する。

情報セキュリティマネジメント試験 問題PDF

Q0073

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント3：脅威によって悪用され得る情報資産や管理策の弱点

用語と説明の組合せとして適切なものはどれか。論点は「脆弱性」である。

A. 情報セキュリティリスク：脅威によって悪用され得る情報資産や管理策の弱点
B. 機密性：脅威によって悪用され得る情報資産や管理策の弱点
C. 脆弱性：脅威によって悪用され得る情報資産や管理策の弱点
D. 責任追跡性：脅威によって悪用され得る情報資産や管理策の弱点

答え・解説

Q0073 正答：C. 脆弱性：脅威によって悪用され得る情報資産や管理策の弱点

解説：正しい組合せは「脆弱性：脅威によって悪用され得る情報資産や管理策の弱点」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0074

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント4：脅威によって悪用され得る情報資産や管理策の弱点

「脆弱性」は、脅威によって悪用され得る情報資産や管理策の弱点。

A. ○
B. ×

答え・解説

Q0074 正答：○

解説：正しい。脆弱性は脅威によって悪用され得る情報資産や管理策の弱点。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

Q0075

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント5：脅威によって悪用され得る情報資産や管理策の弱点

組織が「脅威によって悪用され得る情報資産や管理策の弱点」ために採用すべき概念又は仕組みはどれか。

A. 脆弱性
B. 情報セキュリティリスク
C. 機密性
D. 責任追跡性

答え・解説

Q0075 正答：A. 脆弱性

解説：この目的に対応するのは脆弱性である。脅威によって悪用され得る情報資産や管理策の弱点という機能・考え方を持つためである。

Q0076

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント6：脅威によって悪用され得る情報資産や管理策の弱点

「脆弱性」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. ある操作を誰が行ったかを記録などから追跡できる性質
B. 脅威によって悪用され得る情報資産や管理策の弱点
C. 許可された者だけが情報へアクセスできる状態を保つ性質
D. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

答え・解説

Q0076 正答：B. 脅威によって悪用され得る情報資産や管理策の弱点

解説：脆弱性は脅威によって悪用され得る情報資産や管理策の弱点。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報セキュリティマネジメント試験 問題PDF

Q0077

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント7：脅威によって悪用され得る情報資産や管理策の弱点

「脆弱性」は、脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性。

A. ○
B. ×

答え・解説

Q0077 正答：×

解説：誤り。記述は情報セキュリティリスクの説明である。脆弱性は脅威によって悪用され得る情報資産や管理策の弱点。

Q0078

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント8：脅威によって悪用され得る情報資産や管理策の弱点

次の状況で中心となる論点はどれか。「脅威によって悪用され得る情報資産や管理策の弱点」ことが求められている。

A. 機密性
B. 責任追跡性
C. 情報セキュリティリスク
D. 脆弱性

答え・解説

Q0078 正答：D. 脆弱性

解説：中心となる論点は脆弱性である。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

Q0079

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント9：脅威によって悪用され得る情報資産や管理策の弱点

脆弱性を選定するときは、「脅威によって悪用され得る情報資産や管理策の弱点」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0079 正答：○

解説：正しい。脆弱性の選定・運用では、脅威によって悪用され得る情報資産や管理策の弱点という目的との適合を確認する。

Q0080

セキュリティ基礎・脅威
タグ：脆弱性
用語：脆弱性の確認ポイント10：脅威によって悪用され得る情報資産や管理策の弱点

脆弱性は、脅威によって悪用され得る情報資産や管理策の弱点という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0080 正答：×

解説：誤り。脆弱性はまさに脅威によって悪用され得る情報資産や管理策の弱点という意味を持つ。

情報セキュリティマネジメント試験 問題PDF

Q0081

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント1：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

次の説明に最も合う用語はどれか。脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

A. 標的型攻撃
B. 情報セキュリティリスク
C. 完全性
D. 否認防止

答え・解説

Q0081 正答：B. 情報セキュリティリスク

解説：情報セキュリティリスクは、脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性。ほかの選択肢は目的又は適用場面が異なる。

Q0082

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント2：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

情報セキュリティリスクの説明として最も適切なものはどれか。

A. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃
B. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質
C. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
D. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質

答え・解説

Q0082 正答：C. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

解説：情報セキュリティリスクの要点は「脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性」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

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント3：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

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

A. 標的型攻撃：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
B. 完全性：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
C. 否認防止：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
D. 情報セキュリティリスク：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

答え・解説

Q0083 正答：D. 情報セキュリティリスク：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

解説：正しい組合せは「情報セキュリティリスク：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性」。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

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント4：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

「情報セキュリティリスク」は、脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性。

A. ○
B. ×

答え・解説

Q0084 正答：○

解説：正しい。情報セキュリティリスクは脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性。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

Q0085

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント5：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

組織が「脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性」ために採用すべき概念又は仕組みはどれか。

A. 標的型攻撃
B. 情報セキュリティリスク
C. 完全性
D. 否認防止

答え・解説

Q0085 正答：B. 情報セキュリティリスク

解説：この目的に対応するのは情報セキュリティリスクである。脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性という機能・考え方を持つためである。

Q0086

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント6：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

「情報セキュリティリスク」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. 当事者が後から処理や送信の事実を否定できないよう証拠を残す性質
B. 情報や処理方法が正確かつ完全であり、不正に変更されていない性質
C. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性
D. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

答え・解説

Q0086 正答：C. 脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

解説：情報セキュリティリスクは脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報セキュリティマネジメント試験 問題PDF

Q0087

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント7：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

「情報セキュリティリスク」は、特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃。

A. ○
B. ×

答え・解説

Q0087 正答：×

解説：誤り。記述は標的型攻撃の説明である。情報セキュリティリスクは脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性。

Q0088

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント8：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

次の状況で中心となる論点はどれか。「脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性」ことが求められている。

A. 情報セキュリティリスク
B. 完全性
C. 否認防止
D. 標的型攻撃

答え・解説

Q0088 正答：A. 情報セキュリティリスク

解説：中心となる論点は情報セキュリティリスクである。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。

Q0089

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント9：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

情報セキュリティリスク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

Q0089 正答：×

解説：誤り。情報セキュリティリスクは脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性という概念であり、対象・目的・前提条件の確認が必要である。

Q0090

セキュリティ基礎・脅威
タグ：情報セキュリティリスク
用語：情報セキュリティリスクの確認ポイント10：脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性

情報セキュリティリスクと他の類似概念を区別する際は、「脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性」という定義を基準にするとよい。

A. ○
B. ×

答え・解説

Q0090 正答：○

解説：正しい。情報セキュリティリスクの定義は脅威が脆弱性を悪用した結果、組織へ影響が生じる可能性であり、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

Q0091

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント1：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

次の説明に最も合う用語はどれか。特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

A. 機密性
B. 可用性
C. 標的型攻撃
D. 脅威

答え・解説

Q0091 正答：C. 標的型攻撃

解説：標的型攻撃は、特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃。ほかの選択肢は目的又は適用場面が異なる。

Q0092

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント2：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

標的型攻撃の説明として最も適切なものはどれか。

A. 許可された者だけが情報へアクセスできる状態を保つ性質
B. 許可された利用者が必要なときに情報やシステムを利用できる性質
C. 情報資産へ損害を与える可能性がある事象又は主体
D. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

答え・解説

Q0092 正答：D. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

解説：標的型攻撃の要点は「特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃」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

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント3：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

用語と説明の組合せとして適切なものはどれか。論点は「標的型攻撃」である。

A. 標的型攻撃：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

B. 機密性：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

C. 可用性：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

D. 脅威：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

答え・解説

Q0093 正答：A. 標的型攻撃：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

解説：正しい組合せは「標的型攻撃：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃」。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

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント4：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

「標的型攻撃」は、特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃。

A. ○

B. ×

答え・解説

Q0094 正答：○

解説：正しい。標的型攻撃は特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃。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

Q0095

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント5：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

組織が「特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃」ために採用すべき概念又は仕組みはどれか。

A. 機密性
B. 可用性
C. 標的型攻撃
D. 脅威

答え・解説

Q0095 正答：C. 標的型攻撃

解説：この目的に対応するのは標的型攻撃である。特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃という機能・考え方を持つためである。

Q0096

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント6：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

「標的型攻撃」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. 情報資産へ損害を与える可能性がある事象又は主体
B. 許可された利用者が必要なときに情報やシステムを利用できる性質
C. 許可された者だけが情報へアクセスできる状態を保つ性質
D. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

答え・解説

Q0096 正答：D. 特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

解説：標的型攻撃は特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報セキュリティマネジメント試験 問題PDF

Q0097

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント7：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

「標的型攻撃」は、許可された者だけが情報へアクセスできる状態を保つ性質。

A. ○
B. ×

答え・解説

Q0097 正答：×

解説：誤り。記述は機密性の説明である。標的型攻撃は特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃。

Q0098

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント8：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

次の状況で中心となる論点はどれか。「特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃」ことが求められている。

A. 可用性
B. 標的型攻撃
C. 脅威
D. 機密性

答え・解説

Q0098 正答：B. 標的型攻撃

解説：中心となる論点は標的型攻撃である。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

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント9：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

標的型攻撃を選定するときは、「特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃」という本来の目的に合うかを確認する。

A. ○
B. ×

答え・解説

Q0099 正答：○

解説：正しい。標的型攻撃の選定・運用では、特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃という目的との適合を確認する。

Q0100

セキュリティ基礎・脅威
タグ：標的型攻撃
用語：標的型攻撃の確認ポイント10：特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃

標的型攻撃は、特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃という説明とは無関係である。

A. ○
B. ×

答え・解説

Q0100 正答：×

解説：誤り。標的型攻撃はまさに特定の組織や個人を狙い、偽メールなどを入口として継続的に侵入を試みる攻撃という意味を持つ。