基本情報技術者試験 問題PDF

情報セキュリティ 第1巻

Q0001

情報セキュリティ
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. 真正性
C. ハイブリッド暗号
D. 機密性

答え・解説

Q0001 正答：D. 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

情報セキュリティ
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. 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. 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. 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. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

答え・解説

Q0002 正答：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

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。

Q0003

情報セキュリティ
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. 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
C. 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
D. ハイブリッド暗号：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：B. 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

情報セキュリティ
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。

Q0005

情報セキュリティ
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. 真正性
C. ハイブリッド暗号
D. 機密性

答え・解説

Q0005 正答：D. 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

情報セキュリティ
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. 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. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式
C. 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. 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：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

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。

Q0007

情報セキュリティ
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

情報セキュリティ
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. 真正性
B. ハイブリッド暗号
C. 機密性
D. 完全性

答え・解説

Q0008 正答：C. 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。

基本情報技術者試験 問題PDF

情報セキュリティ 第1巻

Q0009

情報セキュリティ
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
「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」という特徴を持つものを選べ。

A. ハイブリッド暗号
B. 真正性
C. 完全性
D. 機密性

答え・解説

Q0009 正答：D. 機密性
解説：機密性が該当する。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、他の候補とは機能が異なる。

Q0010

情報セキュリティ
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. 完全性
B. 可用性
C. 責任追跡性
D. ハッシュ関数

答え・解説

Q0010 正答：A. 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。

Q0011

情報セキュリティ
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. 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. 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. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

答え・解説

Q0011 正答：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

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。

Q0012

情報セキュリティ
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. 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
B. 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
C. 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
D. ハッシュ関数：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：C. 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。

Q0013

情報セキュリティ
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

Q0013 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。

Q0014

情報セキュリティ
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. 完全性
B. 可用性
C. 責任追跡性
D. ハッシュ関数

答え・解説

Q0014 正答：A. 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。

Q0015

情報セキュリティ
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. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
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. 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. 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

Q0015 正答：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

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。

Q0016

情報セキュリティ
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

Q0016 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。

Q0017

情報セキュリティ
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. ハッシュ関数
C. 可用性
D. 完全性

答え・解説

Q0017 正答：D. 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。

Q0018

情報セキュリティ
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

「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」という特徴を持つものを選べ。

A. 完全性
B. ハッシュ関数
C. 責任追跡性
D. 可用性

答え・解説

Q0018 正答：A. 完全性

解説：完全性が該当する。定義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り、他の候補とは機能が異なる。

Q0019

情報セキュリティ
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. 可用性
C. 共通鍵暗号方式
D. デジタル署名

答え・解説

Q0019 正答：B. 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。

Q0020

情報セキュリティ
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. 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. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
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. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

答え・解説

Q0020 正答：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

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。

Q0021

情報セキュリティ
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. 共通鍵暗号方式：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. デジタル署名：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. 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

答え・解説

Q0021 正答：D. 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。

Q0022

情報セキュリティ
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

Q0022 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。

Q0023

情報セキュリティ
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. 可用性
C. 共通鍵暗号方式
D. デジタル署名

答え・解説

Q0023 正答：B. 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。

Q0024

情報セキュリティ
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. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
B. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
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. 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

Q0024 正答：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

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。

Q0025

情報セキュリティ
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

Q0025 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。

Q0026

情報セキュリティ
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. 可用性
B. 共通鍵暗号方式
C. デジタル署名
D. 真正性

答え・解説

Q0026 正答：A. 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。

Q0027

情報セキュリティ
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

「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」という特徴を持つものを選べ。

A. デジタル署名
B. 可用性
C. 共通鍵暗号方式
D. 真正性

答え・解説

Q0027 正答：B. 可用性

解説：可用性が該当する。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、他の候補とは機能が異なる。

Q0028

情報セキュリティ
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. 責任追跡性
B. 公開鍵暗号方式
C. 真正性
D. 機密性

答え・解説

Q0028 正答：C. 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。

Q0029

情報セキュリティ
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. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
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. 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

Q0029 正答：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

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。

Q0030

情報セキュリティ
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. 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
B. 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
C. 公開鍵暗号方式：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

Q0030 正答：A. 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。

Q0031

情報セキュリティ
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

Q0031 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。

Q0032

情報セキュリティ
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. 責任追跡性
B. 公開鍵暗号方式
C. 真正性
D. 機密性

答え・解説

Q0032 正答：C. 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。

Q0033

情報セキュリティ
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. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
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. 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：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

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。

Q0034

情報セキュリティ
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

Q0034 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。

Q0035

情報セキュリティ
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. 公開鍵暗号方式
B. 真正性
C. 機密性
D. 責任追跡性

答え・解説

Q0035 正答：B. 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。

Q0036

情報セキュリティ
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

「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」という特徴を持つものを選べ。

A. 機密性
B. 公開鍵暗号方式
C. 真正性
D. 責任追跡性

答え・解説

Q0036 正答：C. 真正性

解説：真正性が該当する。定義は利用者・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り、他の候補とは機能が異なる。

Q0037

情報セキュリティ
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. 共通鍵暗号方式
B. ハイブリッド暗号
C. 完全性
D. 責任追跡性

答え・解説

Q0037 正答：D. 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。

Q0038

情報セキュリティ
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. 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. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
C. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式
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

Q0038 正答：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

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。

Q0039

情報セキュリティ
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. 共通鍵暗号方式：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. 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
C. ハイブリッド暗号：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. 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

答え・解説

Q0039 正答：B. 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。

Q0040

情報セキュリティ
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

Q0040 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。

Q0041

情報セキュリティ
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. 共通鍵暗号方式
B. ハイブリッド暗号
C. 完全性
D. 責任追跡性

答え・解説

Q0041 正答：D. 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。

Q0042

情報セキュリティ
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. 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. 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. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式
D. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

答え・解説

Q0042 正答：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

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。

Q0043

情報セキュリティ
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、暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述は共通鍵暗号方式の説明である。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。

Q0044

情報セキュリティ
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. ハイブリッド暗号
B. 完全性
C. 責任追跡性
D. 共通鍵暗号方式

答え・解説

Q0044 正答：C. 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。

基本情報技術者試験 問題PDF

情報セキュリティ 第1巻

Q0045

情報セキュリティ
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

「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」という特徴を持つものを選べ。

A. 完全性
B. ハイブリッド暗号
C. 共通鍵暗号方式
D. 責任追跡性

答え・解説

Q0045 正答：D. 責任追跡性

解説：責任追跡性が該当する。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、他の候補とは機能が異なる。

Q0046

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント1：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

次の説明に最も合う用語はどれか。暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

A. 共通鍵暗号方式
B. 公開鍵暗号方式
C. ハッシュ関数
D. 可用性

答え・解説

Q0046 正答：A. 共通鍵暗号方式

解説：共通鍵暗号方式は、暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式。ほかの選択肢は目的又は適用場面が異なる。

Q0047

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント2：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

共通鍵暗号方式の説明として最も適切なものはどれか。

A. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
B. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
C. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
D. 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

Q0047 正答：B. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

解説：共通鍵暗号方式の要点は「暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式」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

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント3：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

用語と説明の組合せとして適切なものはどれか。論点は「共通鍵暗号方式」である。

A. 公開鍵暗号方式：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
B. ハッシュ関数：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
C. 共通鍵暗号方式：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
D. 可用性：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

答え・解説

Q0048 正答：C. 共通鍵暗号方式：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

解説：正しい組合せは「共通鍵暗号方式：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式」。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

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント4：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

「共通鍵暗号方式」は、暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式。

A. ○
B. ×

答え・解説

Q0049 正答：○

解説：正しい。共通鍵暗号方式は暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式。実務では対象、目的、前提条件を併せて確認する。

Q0050

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント5：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

組織が「暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式」ために採用すべき概念又は仕組みはどれか。

A. 共通鍵暗号方式
B. 公開鍵暗号方式
C. ハッシュ関数
D. 可用性

答え・解説

Q0050 正答：A. 共通鍵暗号方式

解説：この目的に対応するのは共通鍵暗号方式である。暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式という機能・考え方を持つためである。

Q0051

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント6：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

「共通鍵暗号方式」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. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
C. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
D. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

答え・解説

Q0051 正答：B. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
解説：共通鍵暗号方式は暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式。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

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント7：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

「共通鍵暗号方式」は、公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式。

A. ○
B. ×

答え・解説

Q0052 正答：×
解説：誤り。記述は公開鍵暗号方式の説明である。共通鍵暗号方式は暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式。

Q0053

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント8：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

次の状況で中心となる論点はどれか。「暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式」ことが求められている。

A. ハッシュ関数
B. 可用性
C. 公開鍵暗号方式
D. 共通鍵暗号方式

答え・解説

Q0053 正答：D. 共通鍵暗号方式

解説：中心となる論点は共通鍵暗号方式である。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

情報セキュリティ
タグ：共通鍵暗号方式
用語：共通鍵暗号方式の確認ポイント9：暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

「暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式」という特徴を持つものを選べ。

A. 共通鍵暗号方式
B. 可用性
C. ハッシュ関数
D. 公開鍵暗号方式

答え・解説

Q0054 正答：A. 共通鍵暗号方式

解説：共通鍵暗号方式が該当する。定義は暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式であり、他の候補とは機能が異なる。

Q0055

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント1：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

次の説明に最も合う用語はどれか。公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

A. ハイブリッド暗号
B. 公開鍵暗号方式
C. デジタル署名
D. 真正性

答え・解説

Q0055 正答：B. 公開鍵暗号方式

解説：公開鍵暗号方式は、公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式。ほかの選択肢は目的又は適用場面が異なる。

Q0056

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント2：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

公開鍵暗号方式の説明として最も適切なものはどれか。

A. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式
B. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
C. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
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

Q0056 正答：C. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

解説：公開鍵暗号方式の要点は「公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式」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

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント3：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

用語と説明の組合せとして適切なものはどれか。論点は「公開鍵暗号方式」である。

A. ハイブリッド暗号：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
B. デジタル署名：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
C. 真正性：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
D. 公開鍵暗号方式：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

答え・解説

Q0057 正答：D. 公開鍵暗号方式：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

解説：正しい組合せは「公開鍵暗号方式：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式」。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

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント4：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

「公開鍵暗号方式」は、公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。公開鍵暗号方式は公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式。実務では対象、目的、前提条件を併せて確認する。

Q0059

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント5：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

組織が「公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式」ために採用すべき概念又は仕組みはどれか。

A. ハイブリッド暗号
B. 公開鍵暗号方式
C. デジタル署名
D. 真正性

答え・解説

Q0059 正答：B. 公開鍵暗号方式

解説：この目的に対応するのは公開鍵暗号方式である。公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式という機能・考え方を持つためである。

Q0060

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント6：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

「公開鍵暗号方式」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. 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. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
C. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
D. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

答え・解説

Q0060 正答：C. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

解説：公開鍵暗号方式は公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式。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

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント7：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

「公開鍵暗号方式」は、本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述はハイブリッド暗号の説明である。公開鍵暗号方式は公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式。

Q0062

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント8：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

次の状況で中心となる論点はどれか。「公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式」ことが求められている。

A. 公開鍵暗号方式
B. デジタル署名
C. 真正性
D. ハイブリッド暗号

答え・解説

Q0062 正答：A. 公開鍵暗号方式

解説：中心となる論点は公開鍵暗号方式である。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

情報セキュリティ
タグ：公開鍵暗号方式
用語：公開鍵暗号方式の確認ポイント9：公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

「公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式」という特徴を持つものを選べ。

A. 真正性
B. 公開鍵暗号方式
C. デジタル署名
D. ハイブリッド暗号

答え・解説

Q0063 正答：B. 公開鍵暗号方式

解説：公開鍵暗号方式が該当する。定義は公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式であり、他の候補とは機能が異なる。

Q0064

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント1：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

次の説明に最も合う用語はどれか。本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

A. ハッシュ関数
B. 機密性
C. ハイブリッド暗号
D. 責任追跡性

答え・解説

Q0064 正答：C. ハイブリッド暗号

解説：ハイブリッド暗号は、本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式。ほかの選択肢は目的又は適用場面が異なる。

Q0065

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント2：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

ハイブリッド暗号の説明として最も適切なものはどれか。

A. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
B. 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. 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. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

答え・解説

Q0065 正答：D. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

解説：ハイブリッド暗号の要点は「本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式」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

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント3：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

用語と説明の組合せとして適切なものはどれか。論点は「ハイブリッド暗号」である。

A. ハイブリッド暗号：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式
B. ハッシュ関数：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式
C. 機密性：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式
D. 責任追跡性：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

答え・解説

Q0066 正答：A. ハイブリッド暗号：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

解説：正しい組合せは「ハイブリッド暗号：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式」。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

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント4：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

「ハイブリッド暗号」は、本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。ハイブリッド暗号は本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式。実務では対象、目的、前提条件を併せて確認する。

Q0068

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント5：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

組織が「本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式」ために採用すべき概念又は仕組みはどれか。

A. ハッシュ関数
B. 機密性
C. ハイブリッド暗号
D. 責任追跡性

答え・解説

Q0068 正答：C. ハイブリッド暗号

解説：この目的に対応するのはハイブリッド暗号である。本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式という機能・考え方を持つためである。

Q0069

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント6：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

「ハイブリッド暗号」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. 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. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
D. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

答え・解説

Q0069 正答：D. 本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

解説：ハイブリッド暗号は本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式。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

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント7：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

「ハイブリッド暗号」は、入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述はハッシュ関数の説明である。ハイブリッド暗号は本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式。

基本情報技術者試験 問題PDF

情報セキュリティ 第1巻

Q0071

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント8：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

次の状況で中心となる論点はどれか。「本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式」ことが求められている。

A. 機密性
B. ハイブリッド暗号
C. 責任追跡性
D. ハッシュ関数

答え・解説

Q0071 正答：B. ハイブリッド暗号

解説：中心となる論点はハイブリッド暗号である。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

情報セキュリティ
タグ：ハイブリッド暗号
用語：ハイブリッド暗号の確認ポイント9：本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式

「本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式」という特徴を持つものを選べ。

A. 責任追跡性
B. 機密性
C. ハイブリッド暗号
D. ハッシュ関数

答え・解説

Q0072 正答：C. ハイブリッド暗号

解説：ハイブリッド暗号が該当する。定義は本文を共通鍵で暗号化し、その共通鍵を公開鍵暗号で保護する方式であり、他の候補とは機能が異なる。

Q0073

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント1：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

次の説明に最も合う用語はどれか。入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

A. デジタル署名
B. 完全性
C. 共通鍵暗号方式
D. ハッシュ関数

答え・解説

Q0073 正答：D. ハッシュ関数

解説：ハッシュ関数は、入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数。ほかの選択肢は目的又は適用場面が異なる。

Q0074

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント2：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

ハッシュ関数の説明として最も適切なものはどれか。

A. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
B. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
C. 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. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式

答え・解説

Q0074 正答：A. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

解説：ハッシュ関数の要点は「入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数」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

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント3：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

用語と説明の組合せとして適切なものはどれか。論点は「ハッシュ関数」である。

A. デジタル署名：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
B. ハッシュ関数：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
C. 完全性：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
D. 共通鍵暗号方式：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

答え・解説

Q0075 正答：B. ハッシュ関数：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

解説：正しい組合せは「ハッシュ関数：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数」。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

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント4：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

「ハッシュ関数」は、入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数。

A. ○
B. ×

答え・解説

Q0076 正答：○

解説：正しい。ハッシュ関数は入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数。実務では対象、目的、前提条件を併せて確認する。

Q0077

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント5：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

組織が「入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数」ために採用すべき概念又は仕組みはどれか。

A. デジタル署名
B. 完全性
C. 共通鍵暗号方式
D. ハッシュ関数

答え・解説

Q0077 正答：D. ハッシュ関数

解説：この目的に対応するのはハッシュ関数である。入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数という機能・考え方を持つためである。

Q0078

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント6：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

「ハッシュ関数」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. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数
B. 暗号化と復号に同じ秘密鍵を用い、高速なデータ暗号化に適する方式
C. 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. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

答え・解説

Q0078 正答：A. 入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

解説：ハッシュ関数は入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数。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

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント7：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

「ハッシュ関数」は、秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術。

A. ○
B. ×

答え・解説

Q0079 正答：×

解説：誤り。記述はデジタル署名の説明である。ハッシュ関数は入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数。

Q0080

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント8：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

次の状況で中心となる論点はどれか。「入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数」ことが求められている。

A. 完全性
B. 共通鍵暗号方式
C. ハッシュ関数
D. デジタル署名

答え・解説

Q0080 正答：C. ハッシュ関数

解説：中心となる論点はハッシュ関数である。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。

基本情報技術者試験 問題PDF

情報セキュリティ 第1巻

Q0081

情報セキュリティ
タグ：ハッシュ関数
用語：ハッシュ関数の確認ポイント9：入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数

「入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数」という特徴を持つものを選べ。

A. 共通鍵暗号方式
B. 完全性
C. デジタル署名
D. ハッシュ関数

答え・解説

Q0081 正答：D. ハッシュ関数

解説：ハッシュ関数が該当する。定義は入力から固定長の値を生成し、改ざん検知などに用いる一方向性の関数であり、他の候補とは機能が異なる。

Q0082

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント1：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

次の説明に最も合う用語はどれか。秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

A. デジタル署名
B. 機密性
C. 可用性
D. 公開鍵暗号方式

答え・解説

Q0082 正答：A. デジタル署名

解説：デジタル署名は、秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術。ほかの選択肢は目的又は適用場面が異なる。

Q0083

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント2：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

デジタル署名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. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
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. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式

答え・解説

Q0083 正答：B. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

解説：デジタル署名の要点は「秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術」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

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント3：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

用語と説明の組合せとして適切なものはどれか。論点は「デジタル署名」である。

A. 機密性：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
B. 可用性：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
C. デジタル署名：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
D. 公開鍵暗号方式：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

答え・解説

Q0084 正答：C. デジタル署名：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

解説：正しい組合せは「デジタル署名：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術」。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

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント4：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

「デジタル署名」は、秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。デジタル署名は秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術。実務では対象、目的、前提条件を併せて確認する。

Q0086

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント5：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

組織が「秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術」ために採用すべき概念又は仕組みはどれか。

A. デジタル署名
B. 機密性
C. 可用性
D. 公開鍵暗号方式

答え・解説

Q0086 正答：A. デジタル署名

解説：この目的に対応するのはデジタル署名である。秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術という機能・考え方を持つためである。

Q0087

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント6：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

「デジタル署名」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. 公開鍵と秘密鍵の対を用い、鍵配送や署名に利用できる方式
B. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術
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. 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

Q0087 正答：B. 秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

解説：デジタル署名は秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術。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

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント7：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

「デジタル署名」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

Q0088 正答：×

解説：誤り。記述は機密性の説明である。デジタル署名は秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術。

Q0089

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント8：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

次の状況で中心となる論点はどれか。「秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術」ことが求められている。

A. 可用性
B. 公開鍵暗号方式
C. 機密性
D. デジタル署名

答え・解説

Q0089 正答：D. デジタル署名

解説：中心となる論点はデジタル署名である。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。

Q0090

情報セキュリティ
タグ：デジタル署名
用語：デジタル署名の確認ポイント9：秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術

「秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術」という特徴を持つものを選べ。

A. デジタル署名
B. 公開鍵暗号方式
C. 可用性
D. 機密性

答え・解説

Q0090 正答：A. デジタル署名

解説：デジタル署名が該当する。定義は秘密鍵で署名値を作成し、公開鍵で作成者と改ざんの有無を検証する技術であり、他の候補とは機能が異なる。