情報処理安全確保支援士試験 問題PDF

暗号・PKI 第1巻

Q0001

暗号・PKI
タグ：AES
用語：AESの確認ポイント1：共通鍵を用いる代表的なブロック暗号

次の説明に最も合う用語はどれか。共通鍵を用いる代表的なブロック暗号

A. RSA
B. Diffie-Hellman鍵共有
C. AES
D. 公開鍵証明書

答え・解説

Q0001 正答：C. AES

解説：AESは、共通鍵を用いる代表的なブロック暗号。ほかの選択肢は目的又は適用場面が異なる。

Q0002

暗号・PKI
タグ：AES
用語：AESの確認ポイント2：共通鍵を用いる代表的なブロック暗号

AESの説明として最も適切なものはどれか。

A. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
B. 盗聴可能な通信路上で共通の秘密値を合意する方式
C. 公開鍵と主体の対応を認証局が署名して保証する電子文書
D. 共通鍵を用いる代表的なブロック暗号

答え・解説

Q0002 正答：D. 共通鍵を用いる代表的なブロック暗号

解説：AESの要点は「共通鍵を用いる代表的なブロック暗号」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

暗号・PKI
タグ：AES
用語：AESの確認ポイント3：共通鍵を用いる代表的なブロック暗号

用語と説明の組合せとして適切なものはどれか。論点は「AES」である。

A. AES：共通鍵を用いる代表的なブロック暗号
B. RSA：共通鍵を用いる代表的なブロック暗号
C. Diffie-Hellman鍵共有：共通鍵を用いる代表的なブロック暗号
D. 公開鍵証明書：共通鍵を用いる代表的なブロック暗号

答え・解説

Q0003 正答：A. AES：共通鍵を用いる代表的なブロック暗号

解説：正しい組合せは「AES：共通鍵を用いる代表的なブロック暗号」。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

暗号・PKI
タグ：AES
用語：AESの確認ポイント4：共通鍵を用いる代表的なブロック暗号

「AES」は、共通鍵を用いる代表的なブロック暗号。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。AESは共通鍵を用いる代表的なブロック暗号。実務では対象、目的、前提条件を併せて確認する。

Q0005

暗号・PKI
タグ：AES
用語：AESの確認ポイント5：共通鍵を用いる代表的なブロック暗号

組織が「共通鍵を用いる代表的なブロック暗号」ために採用すべき概念又は仕組みはどれか。

A. RSA
B. Diffie-Hellman鍵共有
C. AES
D. 公開鍵証明書

答え・解説

Q0005 正答：C. AES

解説：この目的に対応するのはAESである。共通鍵を用いる代表的なブロック暗号という機能・考え方を持つためである。

Q0006

暗号・PKI
タグ：AES
用語：AESの確認ポイント6：共通鍵を用いる代表的なブロック暗号

「AES」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. 公開鍵と主体の対応を認証局が署名して保証する電子文書
B. 盗聴可能な通信路上で共通の秘密値を合意する方式
C. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
D. 共通鍵を用いる代表的なブロック暗号

答え・解説

Q0006 正答：D. 共通鍵を用いる代表的なブロック暗号

解説：AESは共通鍵を用いる代表的なブロック暗号。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

暗号・PKI
タグ：AES
用語：AESの確認ポイント7：共通鍵を用いる代表的なブロック暗号

「AES」は、大整数の素因数分解の困難性を利用する公開鍵暗号方式。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述はRSAの説明である。AESは共通鍵を用いる代表的なブロック暗号。

Q0008

暗号・PKI
タグ：AES
用語：AESの確認ポイント8：共通鍵を用いる代表的なブロック暗号

次の状況で中心となる論点はどれか。「共通鍵を用いる代表的なブロック暗号」ことが求められている。

A. Diffie-Hellman鍵共有
B. AES
C. 公開鍵証明書
D. RSA

答え・解説

Q0008 正答：B. AES

解説：中心となる論点はAES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

暗号・PKI
タグ：AES
用語：AESの確認ポイント9：共通鍵を用いる代表的なブロック暗号

「共通鍵を用いる代表的なブロック暗号」という特徴を持つものを選べ。

A. 公開鍵証明書
B. Diffie-Hellman鍵共有
C. AES
D. RSA

答え・解説

Q0009 正答：C. AES

解説：AESが該当する。定義は共通鍵を用いる代表的なブロック暗号であり、他の候補とは機能が異なる。

Q0010

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント1：大整数の素因数分解の困難性を利用する公開鍵暗号方式

次の説明に最も合う用語はどれか。大整数の素因数分解の困難性を利用する公開鍵暗号方式

A. 楕円曲線暗号
B. SHA-256
C. OCSP
D. RSA

答え・解説

Q0010 正答：D. RSA

解説：RSAは、大整数の素因数分解の困難性を利用する公開鍵暗号方式。ほかの選択肢は目的又は適用場面が異なる。

Q0011

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント2：大整数の素因数分解の困難性を利用する公開鍵暗号方式

RSAの説明として最も適切なものはどれか。

A. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
B. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
C. 256ビットのハッシュ値を生成するSHA-2系列の関数
D. 証明書の失効状態をオンラインで照会するプロトコル

答え・解説

Q0011 正答：A. 大整数の素因数分解の困難性を利用する公開鍵暗号方式

解説：RSAの要点は「大整数の素因数分解の困難性を利用する公開鍵暗号方式」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。

Q0012

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント3：大整数の素因数分解の困難性を利用する公開鍵暗号方式

用語と説明の組合せとして適切なものはどれか。論点は「RSA」である。

A. 楕円曲線暗号：大整数の素因数分解の困難性を利用する公開鍵暗号方式
B. RSA：大整数の素因数分解の困難性を利用する公開鍵暗号方式
C. SHA-256：大整数の素因数分解の困難性を利用する公開鍵暗号方式
D. OCSP：大整数の素因数分解の困難性を利用する公開鍵暗号方式

答え・解説

Q0012 正答：B. RSA：大整数の素因数分解の困難性を利用する公開鍵暗号方式

解説：正しい組合せは「RSA：大整数の素因数分解の困難性を利用する公開鍵暗号方式」。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。

Q0013

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント4：大整数の素因数分解の困難性を利用する公開鍵暗号方式

「RSA」は、大整数の素因数分解の困難性を利用する公開鍵暗号方式。

A. ○
B. ×

答え・解説

Q0013 正答：○

解説：正しい。RSAは大整数の素因数分解の困難性を利用する公開鍵暗号方式。実務では対象、目的、前提条件を併せて確認する。

Q0014

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント5：大整数の素因数分解の困難性を利用する公開鍵暗号方式

組織が「大整数の素因数分解の困難性を利用する公開鍵暗号方式」ために採用すべき概念又は仕組みはどれか。

A. 楕円曲線暗号
B. SHA-256
C. OCSP
D. RSA

答え・解説

Q0014 正答：D. RSA

解説：この目的に対応するのはRSAである。大整数の素因数分解の困難性を利用する公開鍵暗号方式という機能・考え方を持つためである。

Q0015

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント6：大整数の素因数分解の困難性を利用する公開鍵暗号方式

「RSA」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. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
B. 証明書の失効状態をオンラインで照会するプロトコル
C. 256ビットのハッシュ値を生成するSHA-2系列の関数
D. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

答え・解説

Q0015 正答：A. 大整数の素因数分解の困難性を利用する公開鍵暗号方式

解説：RSAは大整数の素因数分解の困難性を利用する公開鍵暗号方式。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0016

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント7：大整数の素因数分解の困難性を利用する公開鍵暗号方式

「RSA」は、楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述は楕円曲線暗号の説明である。RSAは大整数の素因数分解の困難性を利用する公開鍵暗号方式。

Q0017

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント8：大整数の素因数分解の困難性を利用する公開鍵暗号方式

次の状況で中心となる論点はどれか。「大整数の素因数分解の困難性を利用する公開鍵暗号方式」ことが求められている。

A. SHA-256
B. OCSP
C. RSA
D. 楕円曲線暗号

答え・解説

Q0017 正答：C. RSA

解説：中心となる論点はRSA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

暗号・PKI
タグ：RSA
用語：RSAの確認ポイント9：大整数の素因数分解の困難性を利用する公開鍵暗号方式

「大整数の素因数分解の困難性を利用する公開鍵暗号方式」という特徴を持つものを選べ。

A. OCSP
B. SHA-256
C. 楕円曲線暗号
D. RSA

答え・解説

Q0018 正答：D. RSA

解説：RSAが該当する。定義は大整数の素因数分解の困難性を利用する公開鍵暗号方式であり、他の候補とは機能が異なる。

Q0019

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント1：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

次の説明に最も合う用語はどれか。楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

A. 楕円曲線暗号
B. Diffie-Hellman鍵共有
C. HMAC
D. 前方秘匿性

答え・解説

Q0019 正答：A. 楕円曲線暗号

解説：楕円曲線暗号は、楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号。ほかの選択肢は目的又は適用場面が異なる。

Q0020

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント2：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

楕円曲線暗号の説明として最も適切なものはどれか。

A. 盗聴可能な通信路上で共通の秘密値を合意する方式
B. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
C. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
D. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

答え・解説

Q0020 正答：B. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

解説：楕円曲線暗号の要点は「楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号」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

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント3：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

用語と説明の組合せとして適切なものはどれか。論点は「楕円曲線暗号」である。

A. Diffie-Hellman鍵共有：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
B. HMAC：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
C. 楕円曲線暗号：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
D. 前方秘匿性：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

答え・解説

Q0021 正答：C. 楕円曲線暗号：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

解説：正しい組合せは「楕円曲線暗号：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号」。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

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント4：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

「楕円曲線暗号」は、楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。楕円曲線暗号は楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号。実務では対象、目的、前提条件を併せて確認する。

Q0023

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント5：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

組織が「楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号」ために採用すべき概念又は仕組みはどれか。

A. 楕円曲線暗号
B. Diffie-Hellman鍵共有
C. HMAC
D. 前方秘匿性

答え・解説

Q0023 正答：A. 楕円曲線暗号

解説：この目的に対応するのは楕円曲線暗号である。楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号という機能・考え方を持つためである。

Q0024

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント6：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

「楕円曲線暗号」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. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
B. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
C. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
D. 盗聴可能な通信路上で共通の秘密値を合意する方式

答え・解説

Q0024 正答：B. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

解説：楕円曲線暗号は楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号。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

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント7：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

「楕円曲線暗号」は、盗聴可能な通信路上で共通の秘密値を合意する方式。

A. ○
B. ×

答え・解説

Q0025 正答：×

解説：誤り。記述はDiffie-Hellman鍵共有の説明である。楕円曲線暗号は楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号。

Q0026

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント8：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

次の状況で中心となる論点はどれか。「楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号」ことが求められている。

A. HMAC
B. 前方秘匿性
C. Diffie-Hellman鍵共有
D. 楕円曲線暗号

答え・解説

Q0026 正答：D. 楕円曲線暗号

解説：中心となる論点は楕円曲線暗号である。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。

Q0027

暗号・PKI
タグ：楕円曲線暗号
用語：楕円曲線暗号の確認ポイント9：楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

「楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号」という特徴を持つものを選べ。

A. 楕円曲線暗号
B. 前方秘匿性
C. HMAC
D. Diffie-Hellman鍵共有

答え・解説

Q0027 正答：A. 楕円曲線暗号

解説：楕円曲線暗号が該当する。定義は楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号であり、他の候補とは機能が異なる。

Q0028

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント1：盗聴可能な通信路上で共通の秘密値を合意する方式

次の説明に最も合う用語はどれか。盗聴可能な通信路上で共通の秘密値を合意する方式

A. SHA-256
B. Diffie-Hellman鍵共有
C. デジタル署名
D. AES

答え・解説

Q0028 正答：B. Diffie-Hellman鍵共有

解説：Diffie-Hellman鍵共有は、盗聴可能な通信路上で共通の秘密値を合意する方式。ほかの選択肢は目的又は適用場面が異なる。

Q0029

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント2：盗聴可能な通信路上で共通の秘密値を合意する方式

Diffie-Hellman鍵共有の説明として最も適切なものはどれか。

A. 256ビットのハッシュ値を生成するSHA-2系列の関数
B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
C. 盗聴可能な通信路上で共通の秘密値を合意する方式
D. 共通鍵を用いる代表的なブロック暗号

答え・解説

Q0029 正答：C. 盗聴可能な通信路上で共通の秘密値を合意する方式

解説：Diffie-Hellman鍵共有の要点は「盗聴可能な通信路上で共通の秘密値を合意する方式」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。

Q0030

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント3：盗聴可能な通信路上で共通の秘密値を合意する方式

用語と説明の組合せとして適切なものはどれか。論点は「Diffie-Hellman鍵共有」である。

A. SHA-256：盗聴可能な通信路上で共通の秘密値を合意する方式
B. デジタル署名：盗聴可能な通信路上で共通の秘密値を合意する方式
C. AES：盗聴可能な通信路上で共通の秘密値を合意する方式
D. Diffie-Hellman鍵共有：盗聴可能な通信路上で共通の秘密値を合意する方式

答え・解説

Q0030 正答：D. Diffie-Hellman鍵共有：盗聴可能な通信路上で共通の秘密値を合意する方式

解説：正しい組合せは「Diffie-Hellman鍵共有：盗聴可能な通信路上で共通の秘密値を合意する方式」。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。

Q0031

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント4：盗聴可能な通信路上で共通の秘密値を合意する方式

「Diffie-Hellman鍵共有」は、盗聴可能な通信路上で共通の秘密値を合意する方式。

A. ○
B. ×

答え・解説

Q0031 正答：○

解説：正しい。Diffie-Hellman鍵共有は盗聴可能な通信路上で共通の秘密値を合意する方式。実務では対象、目的、前提条件を併せて確認する。

Q0032

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント5：盗聴可能な通信路上で共通の秘密値を合意する方式

組織が「盗聴可能な通信路上で共通の秘密値を合意する方式」ために採用すべき概念又は仕組みはどれか。

A. SHA-256
B. Diffie-Hellman鍵共有
C. デジタル署名
D. AES

答え・解説

Q0032 正答：B. Diffie-Hellman鍵共有

解説：この目的に対応するのはDiffie-Hellman鍵共有である。盗聴可能な通信路上で共通の秘密値を合意する方式という機能・考え方を持つためである。

Q0033

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント6：盗聴可能な通信路上で共通の秘密値を合意する方式

「Diffie-Hellman鍵共有」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. 共通鍵を用いる代表的なブロック暗号
B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
C. 盗聴可能な通信路上で共通の秘密値を合意する方式
D. 256ビットのハッシュ値を生成するSHA-2系列の関数

答え・解説

Q0033 正答：C. 盗聴可能な通信路上で共通の秘密値を合意する方式

解説：Diffie-Hellman鍵共有は盗聴可能な通信路上で共通の秘密値を合意する方式。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0034

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント7：盗聴可能な通信路上で共通の秘密値を合意する方式

「Diffie-Hellman鍵共有」は、256ビットのハッシュ値を生成するSHA-2系列の関数。

A. ○
B. ×

答え・解説

Q0034 正答：×

解説：誤り。記述はSHA-256の説明である。Diffie-Hellman鍵共有は盗聴可能な通信路上で共通の秘密値を合意する方式。

Q0035

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント8：盗聴可能な通信路上で共通の秘密値を合意する方式

次の状況で中心となる論点はどれか。「盗聴可能な通信路上で共通の秘密値を合意する方式」ことが求められている。

A. Diffie-Hellman鍵共有
B. デジタル署名
C. AES
D. SHA-256

答え・解説

Q0035 正答：A. Diffie-Hellman鍵共有

解説：中心となる論点はDiffie-Hellman鍵共有である。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

暗号・PKI
タグ：Diffie-Hellman鍵共有
用語：Diffie-Hellman鍵共有の確認ポイント9：盗聴可能な通信路上で共通の秘密値を合意する方式

「盗聴可能な通信路上で共通の秘密値を合意する方式」という特徴を持つものを選べ。

A. AES
B. Diffie-Hellman鍵共有
C. デジタル署名
D. SHA-256

答え・解説

Q0036 正答：B. Diffie-Hellman鍵共有

解説：Diffie-Hellman鍵共有が該当する。定義は盗聴可能な通信路上で共通の秘密値を合意する方式であり、他の候補とは機能が異なる。

Q0037

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント1：256ビットのハッシュ値を生成するSHA-2系列の関数

次の説明に最も合う用語はどれか。256ビットのハッシュ値を生成するSHA-2系列の関数

A. HMAC
B. 公開鍵証明書
C. SHA-256
D. RSA

答え・解説

Q0037 正答：C. SHA-256

解説：SHA-256は、256ビットのハッシュ値を生成するSHA-2系列の関数。ほかの選択肢は目的又は適用場面が異なる。

Q0038

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント2：256ビットのハッシュ値を生成するSHA-2系列の関数

SHA-256の説明として最も適切なものはどれか。

A. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
B. 公開鍵と主体の対応を認証局が署名して保証する電子文書
C. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
D. 256ビットのハッシュ値を生成するSHA-2系列の関数

答え・解説

Q0038 正答：D. 256ビットのハッシュ値を生成するSHA-2系列の関数

解説：SHA-256の要点は「256ビットのハッシュ値を生成するSHA-2系列の関数」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。

Q0039

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント3：256ビットのハッシュ値を生成するSHA-2系列の関数

用語と説明の組合せとして適切なものはどれか。論点は「SHA-256」である。

A. SHA-256：256ビットのハッシュ値を生成するSHA-2系列の関数
B. HMAC：256ビットのハッシュ値を生成するSHA-2系列の関数
C. 公開鍵証明書：256ビットのハッシュ値を生成するSHA-2系列の関数
D. RSA：256ビットのハッシュ値を生成するSHA-2系列の関数

答え・解説

Q0039 正答：A. SHA-256：256ビットのハッシュ値を生成するSHA-2系列の関数

解説：正しい組合せは「SHA-256：256ビットのハッシュ値を生成するSHA-2系列の関数」。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。

Q0040

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント4：256ビットのハッシュ値を生成するSHA-2系列の関数

「SHA-256」は、256ビットのハッシュ値を生成するSHA-2系列の関数。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。SHA-256は256ビットのハッシュ値を生成するSHA-2系列の関数。実務では対象、目的、前提条件を併せて確認する。

Q0041

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント5：256ビットのハッシュ値を生成するSHA-2系列の関数

組織が「256ビットのハッシュ値を生成するSHA-2系列の関数」ために採用すべき概念又は仕組みはどれか。

A. HMAC
B. 公開鍵証明書
C. SHA-256
D. RSA

答え・解説

Q0041 正答：C. SHA-256

解説：この目的に対応するのはSHA-256である。256ビットのハッシュ値を生成するSHA-2系列の関数という機能・考え方を持つためである。

Q0042

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント6：256ビットのハッシュ値を生成するSHA-2系列の関数

「SHA-256」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. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
B. 公開鍵と主体の対応を認証局が署名して保証する電子文書
C. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
D. 256ビットのハッシュ値を生成するSHA-2系列の関数

答え・解説

Q0042 正答：D. 256ビットのハッシュ値を生成するSHA-2系列の関数

解説：SHA-256は256ビットのハッシュ値を生成するSHA-2系列の関数。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0043

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント7：256ビットのハッシュ値を生成するSHA-2系列の関数

「SHA-256」は、秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述はHMACの説明である。SHA-256は256ビットのハッシュ値を生成するSHA-2系列の関数。

Q0044

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント8：256ビットのハッシュ値を生成するSHA-2系列の関数

次の状況で中心となる論点はどれか。「256ビットのハッシュ値を生成するSHA-2系列の関数」ことが求められている。

A. 公開鍵証明書
B. SHA-256
C. RSA
D. HMAC

答え・解説

Q0044 正答：B. SHA-256

解説：中心となる論点はSHA-256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。

情報処理安全確保支援士試験 問題PDF

Q0045

暗号・PKI
タグ：SHA-256
用語：SHA-256の確認ポイント9：256ビットのハッシュ値を生成するSHA-2系列の関数

「256ビットのハッシュ値を生成するSHA-2系列の関数」という特徴を持つものを選べ。

A. RSA
B. 公開鍵証明書
C. SHA-256
D. HMAC

答え・解説

Q0045 正答：C. SHA-256

解説：SHA-256が該当する。定義は256ビットのハッシュ値を生成するSHA-2系列の関数であり、他の候補とは機能が異なる。

Q0046

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント1：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

次の説明に最も合う用語はどれか。秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

A. デジタル署名
B. OCSP
C. 楕円曲線暗号
D. HMAC

答え・解説

Q0046 正答：D. HMAC

解説：HMACは、秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式。ほかの選択肢は目的又は適用場面が異なる。

Q0047

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント2：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

HMACの説明として最も適切なものはどれか。

A. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
C. 証明書の失効状態をオンラインで照会するプロトコル
D. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号

答え・解説

Q0047 正答：A. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

解説：HMACの要点は「秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式」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

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント3：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

用語と説明の組合せとして適切なものはどれか。論点は「HMAC」である。

A. デジタル署名：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
B. HMAC：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
C. OCSP：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
D. 楕円曲線暗号：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

答え・解説

Q0048 正答：B. HMAC：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

解説：正しい組合せは「HMAC：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式」。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

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント4：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

「HMAC」は、秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式。

A. ○
B. ×

答え・解説

Q0049 正答：○

解説：正しい。HMACは秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式。実務では対象、目的、前提条件を併せて確認する。

Q0050

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント5：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

組織が「秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式」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. OCSP
C. 楕円曲線暗号
D. HMAC

答え・解説

Q0050 正答：D. HMAC

解説：この目的に対応するのはHMACである。秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式という機能・考え方を持つためである。

Q0051

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント6：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

「HMAC」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. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
B. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
C. 証明書の失効状態をオンラインで照会するプロトコル
D. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

答え・解説

Q0051 正答：A. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

解説：HMACは秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式。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

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント7：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

「HMAC」は、秘密鍵で署名し公開鍵で真正性と完全性を検証する技術。

A. ○
B. ×

答え・解説

Q0052 正答：×

解説：誤り。記述はデジタル署名の説明である。HMACは秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式。

Q0053

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント8：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

次の状況で中心となる論点はどれか。「秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式」ことが求められている。

A. OCSP
B. 楕円曲線暗号
C. HMAC
D. デジタル署名

答え・解説

Q0053 正答：C. HMAC

解説：中心となる論点はHMAC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

暗号・PKI
タグ：HMAC
用語：HMACの確認ポイント9：秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式

「秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式」という特徴を持つものを選べ。

A. 楕円曲線暗号
B. OCSP
C. デジタル署名
D. HMAC

答え・解説

Q0054 正答：D. HMAC

解説：HMACが該当する。定義は秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式であり、他の候補とは機能が異なる。

Q0055

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント1：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

次の説明に最も合う用語はどれか。秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

A. デジタル署名
B. 公開鍵証明書
C. 前方秘匿性
D. Diffie-Hellman鍵共有

答え・解説

Q0055 正答：A. デジタル署名

解説：デジタル署名は、秘密鍵で署名し公開鍵で真正性と完全性を検証する技術。ほかの選択肢は目的又は適用場面が異なる。

Q0056

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント2：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

デジタル署名の説明として最も適切なものはどれか。

A. 公開鍵と主体の対応を認証局が署名して保証する電子文書
B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
C. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
D. 盗聴可能な通信路上で共通の秘密値を合意する方式

答え・解説

Q0056 正答：B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

解説：デジタル署名の要点は「秘密鍵で署名し公開鍵で真正性と完全性を検証する技術」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。

Q0057

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント3：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

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. 公開鍵証明書：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
B. 前方秘匿性：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
C. デジタル署名：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
D. Diffie-Hellman鍵共有：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

答え・解説

Q0057 正答：C. デジタル署名：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

解説：正しい組合せは「デジタル署名：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術」。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。

Q0058

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント4：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

「デジタル署名」は、秘密鍵で署名し公開鍵で真正性と完全性を検証する技術。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。デジタル署名は秘密鍵で署名し公開鍵で真正性と完全性を検証する技術。実務では対象、目的、前提条件を併せて確認する。

Q0059

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント5：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

組織が「秘密鍵で署名し公開鍵で真正性と完全性を検証する技術」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. 公開鍵証明書
C. 前方秘匿性
D. Diffie-Hellman鍵共有

答え・解説

Q0059 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。秘密鍵で署名し公開鍵で真正性と完全性を検証する技術という機能・考え方を持つためである。

Q0060

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント6：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

「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. 盗聴可能な通信路上で共通の秘密値を合意する方式
B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
C. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
D. 公開鍵と主体の対応を認証局が署名して保証する電子文書

答え・解説

Q0060 正答：B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

解説：デジタル署名は秘密鍵で署名し公開鍵で真正性と完全性を検証する技術。似た用語との違いは、対象、時点、責任又は処理方法にある。

情報処理安全確保支援士試験 問題PDF

Q0061

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント7：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

「デジタル署名」は、公開鍵と主体の対応を認証局が署名して保証する電子文書。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述は公開鍵証明書の説明である。デジタル署名は秘密鍵で署名し公開鍵で真正性と完全性を検証する技術。

Q0062

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント8：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

次の状況で中心となる論点はどれか。「秘密鍵で署名し公開鍵で真正性と完全性を検証する技術」ことが求められている。

A. 前方秘匿性
B. Diffie-Hellman鍵共有
C. 公開鍵証明書
D. デジタル署名

答え・解説

Q0062 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。

Q0063

暗号・PKI
タグ：デジタル署名
用語：デジタル署名の確認ポイント9：秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

「秘密鍵で署名し公開鍵で真正性と完全性を検証する技術」という特徴を持つものを選べ。

A. デジタル署名
B. Diffie-Hellman鍵共有
C. 前方秘匿性
D. 公開鍵証明書

答え・解説

Q0063 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し公開鍵で真正性と完全性を検証する技術であり、他の候補とは機能が異なる。

Q0064

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント1：公開鍵と主体の対応を認証局が署名して保証する電子文書

次の説明に最も合う用語はどれか。公開鍵と主体の対応を認証局が署名して保証する電子文書

A. OCSP
B. 公開鍵証明書
C. AES
D. SHA-256

答え・解説

Q0064 正答：B. 公開鍵証明書

解説：公開鍵証明書は、公開鍵と主体の対応を認証局が署名して保証する電子文書。ほかの選択肢は目的又は適用場面が異なる。

Q0065

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント2：公開鍵と主体の対応を認証局が署名して保証する電子文書

公開鍵証明書の説明として最も適切なものはどれか。

A. 証明書の失効状態をオンラインで照会するプロトコル
B. 共通鍵を用いる代表的なブロック暗号
C. 公開鍵と主体の対応を認証局が署名して保証する電子文書
D. 256ビットのハッシュ値を生成するSHA-2系列の関数

答え・解説

Q0065 正答：C. 公開鍵と主体の対応を認証局が署名して保証する電子文書

解説：公開鍵証明書の要点は「公開鍵と主体の対応を認証局が署名して保証する電子文書」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

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント3：公開鍵と主体の対応を認証局が署名して保証する電子文書

用語と説明の組合せとして適切なものはどれか。論点は「公開鍵証明書」である。

A. OCSP：公開鍵と主体の対応を認証局が署名して保証する電子文書
B. AES：公開鍵と主体の対応を認証局が署名して保証する電子文書
C. SHA-256：公開鍵と主体の対応を認証局が署名して保証する電子文書
D. 公開鍵証明書：公開鍵と主体の対応を認証局が署名して保証する電子文書

答え・解説

Q0066 正答：D. 公開鍵証明書：公開鍵と主体の対応を認証局が署名して保証する電子文書

解説：正しい組合せは「公開鍵証明書：公開鍵と主体の対応を認証局が署名して保証する電子文書」。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

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント4：公開鍵と主体の対応を認証局が署名して保証する電子文書

「公開鍵証明書」は、公開鍵と主体の対応を認証局が署名して保証する電子文書。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。公開鍵証明書は公開鍵と主体の対応を認証局が署名して保証する電子文書。実務では対象、目的、前提条件を併せて確認する。

Q0068

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント5：公開鍵と主体の対応を認証局が署名して保証する電子文書

組織が「公開鍵と主体の対応を認証局が署名して保証する電子文書」ために採用すべき概念又は仕組みはどれか。

A. OCSP
B. 公開鍵証明書
C. AES
D. SHA-256

答え・解説

Q0068 正答：B. 公開鍵証明書

解説：この目的に対応するのは公開鍵証明書である。公開鍵と主体の対応を認証局が署名して保証する電子文書という機能・考え方を持つためである。

Q0069

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント6：公開鍵と主体の対応を認証局が署名して保証する電子文書

「公開鍵証明書」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. 256ビットのハッシュ値を生成するSHA-2系列の関数
B. 共通鍵を用いる代表的なブロック暗号
C. 公開鍵と主体の対応を認証局が署名して保証する電子文書
D. 証明書の失効状態をオンラインで照会するプロトコル

答え・解説

Q0069 正答：C. 公開鍵と主体の対応を認証局が署名して保証する電子文書

解説：公開鍵証明書は公開鍵と主体の対応を認証局が署名して保証する電子文書。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

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント7：公開鍵と主体の対応を認証局が署名して保証する電子文書

「公開鍵証明書」は、証明書の失効状態をオンラインで照会するプロトコル。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述はOCSPの説明である。公開鍵証明書は公開鍵と主体の対応を認証局が署名して保証する電子文書。

情報処理安全確保支援士試験 問題PDF

Q0071

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント8：公開鍵と主体の対応を認証局が署名して保証する電子文書

次の状況で中心となる論点はどれか。「公開鍵と主体の対応を認証局が署名して保証する電子文書」ことが求められている。

A. 公開鍵証明書
B. AES
C. SHA-256
D. OCSP

答え・解説

Q0071 正答：A. 公開鍵証明書

解説：中心となる論点は公開鍵証明書である。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

暗号・PKI
タグ：公開鍵証明書
用語：公開鍵証明書の確認ポイント9：公開鍵と主体の対応を認証局が署名して保証する電子文書

「公開鍵と主体の対応を認証局が署名して保証する電子文書」という特徴を持つものを選べ。

A. SHA-256
B. 公開鍵証明書
C. AES
D. OCSP

答え・解説

Q0072 正答：B. 公開鍵証明書

解説：公開鍵証明書が該当する。定義は公開鍵と主体の対応を認証局が署名して保証する電子文書であり、他の候補とは機能が異なる。

Q0073

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント1：証明書の失効状態をオンラインで照会するプロトコル

次の説明に最も合う用語はどれか。証明書の失効状態をオンラインで照会するプロトコル

A. 前方秘匿性
B. RSA
C. OCSP
D. HMAC

答え・解説

Q0073 正答：C. OCSP

解説：OCSPは、証明書の失効状態をオンラインで照会するプロトコル。ほかの選択肢は目的又は適用場面が異なる。

Q0074

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント2：証明書の失効状態をオンラインで照会するプロトコル

OCSPの説明として最も適切なものはどれか。

A. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
B. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
C. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
D. 証明書の失効状態をオンラインで照会するプロトコル

答え・解説

Q0074 正答：D. 証明書の失効状態をオンラインで照会するプロトコル

解説：OCSPの要点は「証明書の失効状態をオンラインで照会するプロトコル」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

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント3：証明書の失効状態をオンラインで照会するプロトコル

用語と説明の組合せとして適切なものはどれか。論点は「OCSP」である。

A. OCSP：証明書の失効状態をオンラインで照会するプロトコル
B. 前方秘匿性：証明書の失効状態をオンラインで照会するプロトコル
C. RSA：証明書の失効状態をオンラインで照会するプロトコル
D. HMAC：証明書の失効状態をオンラインで照会するプロトコル

答え・解説

Q0075 正答：A. OCSP：証明書の失効状態をオンラインで照会するプロトコル

解説：正しい組合せは「OCSP：証明書の失効状態をオンラインで照会するプロトコル」。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

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント4：証明書の失効状態をオンラインで照会するプロトコル

「OCSP」は、証明書の失効状態をオンラインで照会するプロトコル。

A. ○
B. ×

答え・解説

Q0076 正答：○

解説：正しい。OCSPは証明書の失効状態をオンラインで照会するプロトコル。実務では対象、目的、前提条件を併せて確認する。

Q0077

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント5：証明書の失効状態をオンラインで照会するプロトコル

組織が「証明書の失効状態をオンラインで照会するプロトコル」ために採用すべき概念又は仕組みはどれか。

A. 前方秘匿性
B. RSA
C. OCSP
D. HMAC

答え・解説

Q0077 正答：C. OCSP

解説：この目的に対応するのはOCSPである。証明書の失効状態をオンラインで照会するプロトコルという機能・考え方を持つためである。

Q0078

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント6：証明書の失効状態をオンラインで照会するプロトコル

「OCSP」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. 秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成する方式
B. 大整数の素因数分解の困難性を利用する公開鍵暗号方式
C. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
D. 証明書の失効状態をオンラインで照会するプロトコル

答え・解説

Q0078 正答：D. 証明書の失効状態をオンラインで照会するプロトコル

解説：OCSPは証明書の失効状態をオンラインで照会するプロトコル。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

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント7：証明書の失効状態をオンラインで照会するプロトコル

「OCSP」は、長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質。

A. ○
B. ×

答え・解説

Q0079 正答：×

解説：誤り。記述は前方秘匿性の説明である。OCSPは証明書の失効状態をオンラインで照会するプロトコル。

Q0080

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント8：証明書の失効状態をオンラインで照会するプロトコル

次の状況で中心となる論点はどれか。「証明書の失効状態をオンラインで照会するプロトコル」ことが求められている。

A. RSA
B. OCSP
C. HMAC
D. 前方秘匿性

答え・解説

Q0080 正答：B. OCSP

解説：中心となる論点はOCSP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

暗号・PKI
タグ：OCSP
用語：OCSPの確認ポイント9：証明書の失効状態をオンラインで照会するプロトコル

「証明書の失効状態をオンラインで照会するプロトコル」という特徴を持つものを選べ。

A. HMAC
B. RSA
C. OCSP
D. 前方秘匿性

答え・解説

Q0081 正答：C. OCSP

解説：OCSPが該当する。定義は証明書の失効状態をオンラインで照会するプロトコルであり、他の候補とは機能が異なる。

Q0082

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント1：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

次の説明に最も合う用語はどれか。長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

A. AES
B. 楕円曲線暗号
C. デジタル署名
D. 前方秘匿性

答え・解説

Q0082 正答：D. 前方秘匿性

解説：前方秘匿性は、長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質。ほかの選択肢は目的又は適用場面が異なる。

Q0083

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント2：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

前方秘匿性の説明として最も適切なものはどれか。

A. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
B. 共通鍵を用いる代表的なブロック暗号
C. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
D. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術

答え・解説

Q0083 正答：A. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

解説：前方秘匿性の要点は「長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質」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。

Q0084

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント3：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

用語と説明の組合せとして適切なものはどれか。論点は「前方秘匿性」である。

A. AES：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
B. 前方秘匿性：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
C. 楕円曲線暗号：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
D. デジタル署名：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

答え・解説

Q0084 正答：B. 前方秘匿性：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

解説：正しい組合せは「前方秘匿性：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質」。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。

Q0085

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント4：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

「前方秘匿性」は、長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。前方秘匿性は長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質。実務では対象、目的、前提条件を併せて確認する。

Q0086

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント5：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

組織が「長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質」ために採用すべき概念又は仕組みはどれか。

A. AES
B. 楕円曲線暗号
C. デジタル署名
D. 前方秘匿性

答え・解説

Q0086 正答：D. 前方秘匿性

解説：この目的に対応するのは前方秘匿性である。長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質という機能・考え方を持つためである。

Q0087

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント6：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

「前方秘匿性」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. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質
B. 秘密鍵で署名し公開鍵で真正性と完全性を検証する技術
C. 楕円曲線上の離散対数問題を利用し短い鍵長で安全性を得る公開鍵暗号
D. 共通鍵を用いる代表的なブロック暗号

答え・解説

Q0087 正答：A. 長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

解説：前方秘匿性は長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント7：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

「前方秘匿性」は、共通鍵を用いる代表的なブロック暗号。

A. ○
B. ×

答え・解説

Q0088 正答：×

解説：誤り。記述はAESの説明である。前方秘匿性は長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質。

Q0089

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント8：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

次の状況で中心となる論点はどれか。「長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質」ことが求められている。

A. 楕円曲線暗号
B. デジタル署名
C. 前方秘匿性
D. AES

答え・解説

Q0089 正答：C. 前方秘匿性

解説：中心となる論点は前方秘匿性である。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。

Q0090

暗号・PKI
タグ：前方秘匿性
用語：前方秘匿性の確認ポイント9：長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質

「長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質」という特徴を持つものを選べ。

A. デジタル署名
B. 楕円曲線暗号
C. AES
D. 前方秘匿性

答え・解説

Q0090 正答：D. 前方秘匿性

解説：前方秘匿性が該当する。定義は長期秘密鍵が漏えいしても過去のセッション鍵が直ちに復元されない性質であり、他の候補とは機能が異なる。