

平成 18 年度 春期 テクニカルエンジニア（情報セキュリティ） 午後 解答例

この解答例は、独立行政法人 情報処理推進機構 情報処理技術者試験センターが公表しているものです。著作権は、同センターにありますので、その点ご注意ください。

問 1

設問 1

- (1) a - HIDDEN
(2) b - なし c - あり

設問 2

- (1) サニタイジング処理
(2) d - < e - <

設問 3

- (1) f - 32 g - 14 h - 32 i - 80
(2) 共通鍵の長さが実質的に 128 ビットから 120 ビットとなり，共通鍵が解析されやすくなるから

- 設問 4 ・疑似乱数を用いて生成すること
 ・十分な長さの文字列とすること

* -----*

問 2

設問 1

- a - イ b - ク c - カ d - ウ

設問 2

- (1) ・失敗時のログだけでは，参照，更新日時と参照，更新者を特定できないから
 ・失敗時のログだけでは，参照，更新の履歴を要求する規程を満たさないから
(2) 設計開発文書ごとのアクセス制御は，業務効率を著しく損なうから

設問 3

- 機能... ・設計開発文書のハッシュ値の確認の依頼を受けると，その正当性を回答する機能
 ・設計開発文書のハッシュ値を利用して，設計開発文書の改ざんを検知する機能
条件...ハッシュ値の登録者を設計開発文書の承認者に限定すること

* ----- *

問 3

設問 1

a - 認証局 又は CA

b - 改ざん 又は 変更

設問 2

- ・ 証明書失効リスト
- ・ 認証局の公開鍵証明書
- ・ 検証時の時刻

設問 3

c - W

d - LN = 5

e - XX

f - RW

注：c, d は順不同

設問 4

- (1) 辞書攻撃
- (2) IC カードの認証
 - ・ 不正な IC カードの拒否
- (3) 脅威...PIN の盗聴
 - 範囲...・ MW と IC カード間
 - ・ PC と IC カード間
- (4) 用途...IC カードのロック状態の解除
 - 情報...・ 管理者 PIN
 - ・ 管理者パスワード
 - ・ 人事総務部 PIN

* ----- *

問 4

設問 1

a - 盗聴

b - SV 又は サーバ

設問 2

- (1) 失効情報の確認
 - ・ 証明書の失効確認
- (2) SV だけが乱数を正しく復号できることについて、適切に記述していること
- (3) (ア) 認証に成功したサーバが SV であるとは限らないから
 - ・ 意図した URL のサーバに接続していない可能性があるから(イ) 送られてきた証明書の所有者が SV であるとは限らないから
 - ・ 接続しているサーバがアドレス詐称している可能性があるから

設問 3

- (1) 4
- (2) 中間者攻撃を用い、SV から送られる SV の公開鍵を自分のものにすり替える。
 - ・ アドレス詐称を行い、偽のサーバを構築する。

注：この解答例に関するメールでのご質問には、応じかねます。あしからずご了承ください。