

【午 後 I】

問 1 （配点 50 点）

設問 1 （1）3 点，（2）2 点×2

- (1) a : hidden
(2) b : なし c : あり

設問 2 （1）3 点，（2）3 点×2

- (1) サニタイジング（HTML エンコード）
(2) d : < e : <

設問 3 （1）3 点×4，（2）10 点

- (1) f : 32 g : 14 h : 32 i : 79
(2) 共通かぎの可変部分と暗号化された利用者 ID 部分の組合せから，共通鍵の固定部分が解読可能だから

設問 4 6 点×2

- ① セッション ID のビット長は十分に長くする
② 乱数などを用いて推測しにくいものとする

問 2 （配点 50 点）

設問 1 4 点×4

a : イ b : ク c : カ d : ウ

設問 2 （1）8 点，（2）8 点

- (1) 参照時の履歴として参照日時と参照者を特定できる情報を残す必要があるから
(2) 従業員ごとにアクセス権を設定することは，業務効率を著しく損なうから

設問 3 機能 10 点，条件 8 点

機能：登録されたハッシュ値と，設計開発文書から新たに生成したハッシュ値とを比較する機能

条件：承認者の秘密鍵を使ってハッシュ値を暗号化したものを登録する

問3 (配点 50 点)

設問1 3点×2

a: 認証局 (CA, Certificate Authority)

b: 改ざん

設問2 5点×2

次のうち二つ

- ・ 認証局の公開鍵
- ・ 公開鍵証明書の有効期限
- ・ 公開鍵証明書の失効情報 (証明書失効リスト, CRL)

設問3 2点×4

c: L

d: LN=5

e: XX

f: R

設問4 (1)3点, (2)5点, (3)脅威4点, 範囲5点, (4)用途5点, 情報4点

- (1) 辞書攻撃
- (2) MWがICカードを認証する
- (3) 脅威: PINの盗聴
範囲: MWとICカード間の通信範囲
- (4) 用途: MWとICカード間のセキュアメッセージ化
情報: 共有している暗号化鍵

問4 (配点 50 点)

設問1 3点×2

a: 盗聴

b: SV

設問2 (1)5点, (2)6点, (3)7点×2

- (1) CRLで証明書失効の有無確認
- (2) SVの秘密鍵を持たなければ乱数を復号できないから
- (3) (ア): SVに偽装した不正なサーバにアクセスしている可能性があるから
(イ): SVの証明書の有効性や真正性を確保せずに接続してしまうから

設問3 (1)3点, (2)8点×2

- (1) 4
- (2) ① CLからの接続要求を横取りしてSVになりすまし, 攻撃者の公開鍵をCLに送信する
② 中間者攻撃によって, SVの公開鍵を盗聴し攻撃者の公開鍵にすりかえてCLに送信する

【午後Ⅱ】

問1 (配点 200 点)

設問1 (1)6点×3, (2)19点, (3)13点

- (1) a: 職務分離 b: 列 c: 行
- (2) プログラムやデータベースの更新権限を持つシステム管理者とデータベースの参照権限しか持たない業務 AP の利用者を明確に分離する
- (3) 業務 AP の利用者がアクセス権限を持つカテゴリのデータで構成された利用者ビューを設計する

設問2 (1)6点×4, (2)6点×3

- (1) d: 任意 e: 機密ラベル f: 社外秘 g: 強制
- (2) ① 取扱レベル
② カテゴリ
③ 権限クラス

設問3 (1)6点×5, (2)理由9点, 問題19点, (3)16点×2, (4)問題9点, 解決策9点

- (1) h: クラス4 i: B 製品開発 j: クラス5
k: クラス3 l: F 製品開発
- (2) 理由: 一つの事業部や本社管理部が, 複数のプロジェクトに参与しているから
問題: 各利用者は, 同じ事業部や本社管理部のものであれば, 自分が担当しないプロジェクトの情報資産にもアクセスすることができる
- (3) 処理①: オペレータが B 製品開発プロジェクトの“製品仕様書”のデータを管理文書サーバから機密情報管理サーバへ移動する
処理②: システム管理者が機密情報管理サーバの“製品仕様書”の取扱レベルの設定を“取扱注”から“社外秘”に変更する
- (4) 問題: Q 氏の権限クラスでは取扱レベルが極秘の情報資産にアクセスできない
解決策: Q 氏の権限クラスを一時的にクラス5に変更し, レビュー後に元に戻す

問2 (配点 200 点)

設問1 (1)7点×2, (2)10点

- (1) ① SMTP によるメールの転送経路
② POP によるメールの受信経路
- (2) パスワードでメールの送信者を認証する Web のメールサーバ

設問2 (1)5点×10, (2)8点, (3)15点

- (1) a: デジタル署名 b: 送信者
c: 暗号化 d: 秘密鍵
e: 公開鍵 f: データ符号化 (Base64)
g: 6 h: 24
i: 3 j: 1.3

この解答例の著作権は TAC(株)のものであり、無断転載・転用を禁じます。

Copyright by TAC Co.,Ltd.2006

- (2) ヘッダ部の記述内容は暗号化されないから
- (3) メールに付与されたデジタル署名を J 社の調達担当者の公開鍵で復号して検証する

設問 3 (1) 10 点, (2) 13 点 × 2, (3) 20 点

- (1) J 社で開発担当者のパスワードの更新を確実に実施できる点
- (2) 自社に割り当てられないディレクトリをアクセスする方法 : 文字列 “../” をファイル名に含めて親ディレクトリを指定する
任意のファイルをアクセスする方法 : ナル文字 “%x00” をファイル名に含めて, その後ろの文字列を無視させる
- (3) ダウンロードされるファイルのファイル名に利用可能な 40 文字以外の文字が含まれる場合はサーバ側でエラーにする機能

設問 4 (1) 10 点, (2) 10 点, (3) 確認すべきこと 8 点, 目的 19 点

- (1) ファイルが暗号化されておらず転送時に漏えいする恐れがあるから
- (2) 調達ファイルを取得する開発担当者が事前に定まっていないから
- (3) 確認すべきこと : Web ページの URL が J 社のものかどうか
目的 : 偽装された Web ページにアクセスして認証情報やダウンロード情報を誤って漏えいさせることを防ぐため

以上