

情報セキュリティスペシャリスト 解答例

【午 後 I】

問 1 (配点 50 点)

設問 1 (21 点:(1)7 点, (2)7 点, (3)7 点)

- (1) Referer
- (2) Web ブラウザのスクリプトの実行を無効化する操作
- (3) Web サーバ側で受信したファイルの拡張子を判断する方式

設問 2 (17 点:(1)5 点×2, (2)7 点)

- (1) a: 桁あふれ
b: バッファオーバーフロー
- (2) 列数の 3 倍以上で最小の 256 の倍数に行数を掛けた値が kMaxInteger より大きい入力ファイルの場合

設問 3 (12 点:6 点×2)

- c: kMaxInteger / fhBuf.rows
- d: bytesOfRow

問 2 (配点 50 点)

設問 1 (10 点:(1)5 点, (2)5 点)

- (1) a: syslog
- (2) b: -all

設問 2 (7 点)

迷惑メール対策装置が過負荷になり、外部メールサーバに直接送られた。

設問 3 (26 点:(1)7 点, (2)7 点, (3)c 5 点, 効果 7 点)

- (1) 取引先のメールサーバの IP アドレスが変更された場合
- (2) 迷惑メールのドメイン名に対する SPF レコードを設定する行為
- (3) c: プロキシサーバ
(効果) 不正な URL へアクセスしない

設問 4 (7 点)

SMTP 通信を LB が受信し、迷惑メール対策装置に転送する。

問 3 (配点 50 点)

設問 1 (10 点:(1)5 点, (2)5 点)

- (1) フィッシングサイト
- (2) 法人利用者の使用するクライアント証明書がないとログインできないから

設問 2 (20 点:(1)5 点, (2)5 点×3)

- (1) X ネットサービスアクセス時にブラウザのアドレスバーが緑色にならない。

(2) a: 123456

b: 10000

(目的) 送金内容を書き換えたことを利用者に気付かれないようにするため

設問 3 (20 点: (1)5 点 × 2, (2)5 点, (3)5 点)

(1) c: 対策になる

d: 対策になる

(2) e: 二要素

(3) PC 用のプログラムを実行することにより, 攻撃者の意図した送金内容に対応する HMAC 値を計算されてしまう問題点

【午 後 II】

問 1 (配点 100 点)

設問 1 (6 点)

VIP 会員の PAN を含むデータを PC 内の VIP ファイルに保存し、利用している点

設問 2 (67 点:(1)5 点, (2)6 点×2, (3)6 点×4, (4)6 点, (5)5 点×4)

- (1) イ
- (2) (作業) ステータスコード確認作業
(状態) PAN が復号されずに表示される
- (3) (方式名) 方式 1
(項目番号) 3.4.1
(動作) OS へのログインに成功すると、全てのデータがアクセス時に自動的に復号される。
(内容) ディスク暗号化では、論理アクセスは OS の認証とは別に管理する。
- (4) PAN に索引が設定されているので、PAN が暗号化されずに表示されるから
- (5) a: 方式 3
b: 方式 2
c: 方式 3
d: 方式 2

設問 3 (11 点:(1)6 点, (2)5 点)

- (1) L 社本社に不正に設置された W-AP に業務端末や運用端末が自動で無線接続される。
- (2) e: IEEE802.11a

設問 4 (16 点:(1)6 点, (2)5 点×2)

- (1) 会員からの電話受付時に、本人確認を PAN ではなくお客様コードで行うことができる。
- (2) f: お客様コード, ポイント値, 最終更新日時
g: お客様コード, 会員名, 住所, 電話番号, 性別

問 2 (配点 100 点)

設問 1 (18 点:(1)6 点, (2)6 点, (3)6 点)

- (1) コンテンツへの不正アクセスの痕跡が消えてしまうから
- (2) 改ざんされた期間のログが保存されておらず、コンテンツが改ざんされた日を特定できないから
- (3) R 社の画像閲覧ソフト

設問 2 (15 点:(1)5 点, (2)5 点×2)

- (1) a: SFTP
- (2) (項目名) 送信元
(変更後の内容) E 社

設問 3 (23 点:(1)課 5 点, 内容 6 点, (2)4 点×3)

- (1) (課) 経理課
(不都合の内容) ブラウザのアドレスバーの表示で Web サイト運営者名が U 銀行であることを確認できなくなる。

- (2) b: OS ベンダの Web サーバ
- c: Q 社の Web サーバ
- d: R 社の Web サーバ (b～d は順不同)

設問 4 (15 点:5 点×3)

- e: 公開 Web サーバ
- f: インターネット
- g: すべて

設問 5 (29 点:(1)5 点, (2)6 点, (3)6 点×2, (4)6 点)

- (1) h: クライアント
- (2) CAD データを不正に外部に送信することを防止することができる。
- (3) ① PC から HTTP および HTTPS 通信によってプロキシサーバ経由で行うインターネットへの通信
- ② PC から SMTP 通信によってメールサーバ経由で行うインターネットへの通信
- (4) PC からプロキシサーバやメールサーバを経由しないインターネットへの通信

以上