

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 (25 点:(1)4 点, (2)4 点, (3)4 点, (4)4 点×2, (5)5 点)

- (1) a : wana.example.jp
- (2) kensho.m-sha.co.jp
- (3) b : エ
- (4) c : https://kensho.m-sha.co.jp/Gamen2_2
d : keyword
- (5) 懸賞システムにログインしている状態

設問 2 (12 点:(1)4 点×2, (2)4 点)

- (1) e : セッション ID
f : hidden

(2) ウ

設問 3 (13 点:(1)5 点, (2)4 点, (3)4 点)

- (1) ブラウザの設定でスクリプトが無効化されていると、検査せずに入力値が渡されるから
- (2) i : Web サーバ上
- (3) j : URL

問 2 (配点 50 点)

設問 1 (10 点:5 点×2)

- a : 第三者中継
- b : 送信ドメイン

設問 2 (5 点)

- c : リフレクタ

設問 3 (24 点:(1)5 点, (2)e 5 点, 影響 8 点, (3)6 点)

- (1) d : 送信元ポート番号
- (2) e : 外部メールサーバ
(影響) U 社からの取引先宛てのメールが攻撃者のメールサーバに配送されてしまう。
- (3) ホストとの間でトンネル確立を要求する。

設問 4 (11 点:変更箇所 5 点, 変更内容 6 点)

- (変更箇所) ブラックリスト 3
- (変更内容) 複合機用メールアドレスをブラックリストに追加する。

問 3 (配点 50 点)

設問 1 (24 点:(1)6 点, (2)6 点, (3)6 点, (4)6 点)

- (1) a : S サーバ
- (2) b : 試験用 Web サーバ
- (3) c : 検証試験実施日より前の値
- (4) d : S アプリ上にサーバ認証エラー画面を表示する。

設問 2 (26 点:(1)6 点×3, (2)8 点)

- (1) e : 1, 2, 3, 4
f : 3
g : 1
- (2) S アプリの利用者が接続する公衆無線 LAN の SSID と同一の SSID を W-AP に設定する。

【午 後 II】

問 1 (配点 100 点)

設問 1 (8 点)

a : 対応すべきか否か

設問 2 (18 点:(1)8 点, (2)10 点)

(1) b : A 社 IRT に報告すべきインシデントの範囲

(2) A 社 IRT 主導による全社への影響度の判断やインシデント対応を行えるようにするため

設問 3 (20 点:(1)10 点, (2)10 点)

(1) 利用者 LAN の IT 部のセグメント上の OA 用 PC に感染させたマルウェアによって、サーバ LAN 上の各サーバの管理用ポートへの不正アクセスを行う。

(2) 一定時間内での管理画面への認証失敗回数をカウントして攻撃を検知する方法

設問 4 (20 点:(1)10 点, (2)10 点)

(1) A 社保有の情報機器の脆弱性情報の収集を漏れなく効率的に実施できる。

(2) インシデントの影響範囲を正確に把握し、対応すべき情報機器への対応指示漏れを防止できる。

設問 5 (10 点)

各部署で収集した脆弱性情報を A 社 IRT に集約して統一化する。

設問 6 (24 点:(1)6 点, (2)6 点×3)

(1) 現状評価基準

(2) c : ネットワーク

d : ローカル

e : FW1

問 2 (配点 100 点)

設問 1 (22 点:(1)8 点, (2)7 点×2)

(1) UA が DL2 ではないときは、HTTP ステータスコード 404 を返す。

(2) ① J プロキシの URL フィルタ機能

② J プロキシの RH フィルタ機能

設問 2 (6 点)

a : コード

設問 3 (24 点:(1)6 点×2, (2)6 点×2)

(1) b : ドライブバイ

c : 2k バイト未満に分割

(2) d : N コラボ

e : P 社 CRM ツール

設問 4 (6 点)

f : 見直し

設問 5 (42 点:(1)8 点, (2)7 点×2, (3)8 点, (4)項目 4 点, 変更後の案 8 点)

(1) ハードディスクの読出し時には透過的に復号されてデータにアクセスできるから

(2) ① マルウェア定義ファイルが初期化される。

② OS の修正パッチが初期化される。

(3) キーロガーや、画面の内容を取得する攻撃

(4) (項目) 3

(変更後の案) VDI サーバからの, HTTP 及び HTTPS によるアクセスだけを許可するよう設定する。

以上