

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 (10 点:(1)5 点, (2)5 点)

- (1) 画面 B
- (2) HTTP 通信で暗号化されずに送信されたクッキーからセッション ID を盗聴できるから

設問 2 (15 点:(1)5 点, (2)5 点, (3)5 点)

- (1) a : %0d%0a%0d%0a
- (2) b : ウ
- (3) c : 入力された検索文字列に改行コードが含まれていればエラーを応答

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

- (1) d : 17
e : 27 (d と e は順不同)
- (2) f : 01234
- (3) 利用者 K のログイン後のセッション ID と攻撃者 J のセッション ID が同一だから
- (4) g : セッション ID を破棄し、新たにセッション ID を生成し返信する

問 2 (配点 50 点)

設問 1 (18 点:(1)6 点, (2)4 点×3)

- (1) FW のログで宛先 IP アドレスが一致する許可した通信を確認する。
- (2) a : FW
b : プロキシサーバ
c : MAC アドレス

設問 2 (14 点:(1)7 点, (2)7 点)

- (1) 外部にある C&C サーバの名前解決を行えず FW にパケットが到達しないから
- (2) C&C サーバの FQDN をプロキシサーバのブラックリストに登録し通信を遮断する。

設問 3 (18 点:(1)6 点, (2)6 点, (3)6 点)

- (1) ファイル配信サーバから他の PC やサーバへのマルウェアの感染
- (2) V さんの利用者 ID を無効化する。
- (3) 3 台のサーバ上のログとログ管理サーバ上の保存ログを照合する。

問 3 (配点 50 点)

設問 1 (7 点)

候補となるパスワードのハッシュ値一覧テーブルを用意し、ファイルに保存されているハッシュ値と比較してパスワードを推測する。

設問 2 (18 点:(1)6 点, (2)6 点, (3)6 点)

(1) a: 32

(2) b: 単位時間当たりの同一 IP アドレスからのログイン失敗数

(3) c: 複数の異なる IP アドレス

設問 3 (18 点:6 点×3)

d : 10^6

e : 200

f : 80^8

設問 4 (7 点)

他のサイトで窃取した利用者 ID とパスワードを使用して, Z サイトへの不正ログインを試行する。

【午 後 II】

問 1 (配点 100 点)

設問 1 (16 点:(1)4 点, (2)4 点×2, (3)4 点)

- (1) a : DNSSEC
- (2) b : オープン
c : エンベロープ
- (3) d : n-sha.co.jp

設問 2 (4 点)

e : 送信者メールアドレス

設問 3 (8 点)

サーバ管理者登録ホワイトリストに N 社の指定ソフトウェアのベンダサイトの URL を登録する。

設問 4 (32 点:(1)8 点, (2)8 点, (3)8 点, (4)8 点)

- (1) 初期設定用ネットワークに接続し, W 社から駆除ツールをダウンロードして, PC に適用する。
- (2) 部分一致方式で server.example.net を登録する。
- (3) 営業部広報グループ全員の PC のマルウェア X の感染を調査し, 原因となったメールを開かずに削除するよう指示した。
- (4) スキャン不能の場合, 結果を通知する設定にする。

設問 5 (16 点:8 点×2)

- ① PC のウイルス定義ファイル更新時刻を管理者が参照し, 更新遅延の PC にダウンロードと更新を動作指示する。
- ② PC のフルスキャン実行結果を管理者が参照し, 実行していない PC にフルスキャンの実行を動作指示する。

設問 6 (24 点:(1)8 点×2, (2)8 点)

- (1) (連絡用メールアドレス) 標的とする第三者のメールアドレス
(お問合せ内容) ウイルスがダウンロードされる URL
- (2) f : httphttp://

問 2 (配点 100 点)

設問 1 (8 点)

a : 事務用 PC から事務系 LAN に接続している転送用 PC にマルウェアが感染し, 製造系 LAN に接続を切り替えた転送用 PC から製造装置にマルウェアが感染する。

設問 2 (18 点:(1)4 点×3, (2)6 点)

- (1) b : ログアウト
c : 強度が高い
d : 知られないように
- (2) e : K サーバの利用を停止し, セキュリティパッチなどの適用を行う

設問 3 (16 点:8 点×2)

- f : 情報共有系 LAN と製造系 LAN は同一 LAN 上ではないため, 感染を防止できる。
- g : マルウェアによって SAN ストレージヘファイルが書き込まれても, 単方向レプリケーションのため製造装置への感染を防止できる。

設問 4 (58 点:(1)8 点×2, (2)4 点×5, (3)8 点, (4)7 点×2)

- (1) ① 接続端末に固定の IP アドレスを割り当てるのが義務付けられておらず, 接続端末を特定できないから
- ② プロキシサーバや NAT, NAPT を利用しているとアクセス元 IP アドレスから接続端末を特定できないから
- (2) h : K 工場
i : K 工場
j : J 社本社
k : K 工場
l : J 社本社
- (3) 証明書による協力会社の接続端末の認証を行うのは K 工場の K サーバだから
- (4) ① 証明書の公開鍵とのペアである秘密鍵が漏えい, 紛失した場合
- ② 証明書に記載されている事項に変更が生じた場合

以上