TAC

平成30年度秋期　情報処理安全確保支援士試験

# 情報処理安全確保支援士　解答例

## 【午　後　Ⅰ】

問 1 （配点 50 点）

設問 1 （20 点：(1)3 点×4，(2)3 点，(3)5 点）

(1) a ： キ　b ： カ　c ： ウ　d ： ア

(2) あ ： ㋒

(3) DEP によりデータの格納された領域におけるコードの実行が妨げられるから

設問 2 （12 点：(1)4 点×2，(2)4 点）

(1) e ： canary　f ： ASLR

(2) g ： strcpy

設問 3 （18 点：(1)（行番号）3 点，（排除できない理由）5 点，(2)（問題）5 点，（開発環境）5 点）

(1) （行番号） 16 行目

（排除できない理由） ポインタ操作での書込みでライブラリ関数を使用していないから

(2) （問題） コンパイラが SSP を適用できない場合がある。

（問題の別解） コンパイラが中間言語としての検出機能を挿入できない。

（開発環境） SSP 適用可能なコンパイラをサポートしない開発環境

問 2 （配点 50 点）

設問 1 （10 点：2 点×5）

a ： ウ　b ： ス　c ： セ　d ： エ　e ： コ

設問 2 （13 点：(1)3 点，(2)5 点×2）

(1) SYN/ACK

(2) (a) 各 IP アドレスのスキャン間隔が 5 分間より大きいから

(b) 各 IP アドレス毎にスキャンは一度しか行われないから

設問 3 （12 点：(1)1 点×6，(2)2 点×3）

(1) PC101，PC133，PC277，PC301，PC321，PC340

の計 6 個の PC のホスト名を〇印で囲む。

(2) イ，オ，カ

設問 4 （15 点：(1)5 点×2，(2)5 点）

(1) ① マルウェアに感染しておらず，対策ソフトが最新の状態であること

（①の別解：マルウェア対策ソフト及びその定義ファイルが最新であること）

② 最新のセキュリティ修正プログラムが適用されていること

(2) VLAN を用いて不要な PC 同士の直接通信を制限する。

問 3 （配点 50 点）

設問 1 （6 点）

NTP サーバで時刻の同期をとる。

設問 2 （5 点）

a ： CVSS

設問 3 （8 点）

E サーバを L2SW から切り離し，待機サーバを起動して接続する。

（通販システム運用を停止し，待機サーバでサービス停止を告知する。）

設問 4 （10 点：（調査すべき機器）4 点，（調査すべき内容）6 点）

（調査すべき機器） FW1

（調査すべき内容） 外部メールサーバから内部メールサーバへの SSH 接続の有無

設問 5 （21 点：(1)5 点，(2)6 点，(3)5 点×2）

（1） b ： 攻撃 （攻撃コード，攻撃通信，アタックなど）

（2） HTTPS 通信を一旦終端して復号してから検査する機能

（3） c ： 外部 DNS サーバ

d ： CNAME

# 【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （6 点）

GDPR

設問 2 （36 点：(1)6 点，(2)6 点×3，(仕様の内容)6 点，(3)6 点）

(1) プロジェクト専用サーバは，物理的な入退室管理ができる室内に配置され，その室内の専用 PC からだけアクセスできること

(2) （満たせなくなる基本要件の具体的内容）

① 生産関連サーバは，X 社の情報セキュリティ標準への準拠のため，X 社の工場及びデータセンタに配置する。

② 生産関連サーバは，事業継続のため，バックアップを X 社の他の工場又はデータセンタに配置する。

③ 輸出管理規制への準拠のため，同じ設備を製造する生産関連サーバは同一の国内の 2 か所以上に配置する。

（IaaS C のサービス仕様の内容）

日本国内の唯一のデータセンタが被災した場合は，シンガポールのデータセンタでサービスが継続される。

(3) IaaS C であらかじめ予約されているプライベート IP アドレスを，X 社内の機器のアドレスとしても使用しており変更できない状況が生じる問題

設問 3 （12 点：(1)6 点，(2)（業務サーバ)1 点×2，(構成要素)1 点×4）

(1) シングルサインオンを用いて各サーバにログインできる。

(2) （業務サーバ） ㋑，㋒

（構成要素） ㋐，㋓，㋔，㋕

設問 4 （20 点：(1)2 点×3，(2)6 点，(3)4 点×2）

(1) ティア 1 ： イ

ティア 2 ： ウ

ティア 3 ： ア

(2) 標準ソフトウェア以外のソフトウェアの脆弱性やパッチ適用状況が管理されず放置される。

(3) ① 問題のある機器の一覧が得られる。

② 一括で機器にパッチを適用できる。

（②の別解 ： 一括で機器の設定値を変更できる。）

設問 5 （26 点：(1)（案 A)2 点×2，(案 B)2 点×3，(2)2 点×8）

(1)

| | | クライアント | 業務サーバ |
|---|---|---|---|
| 案A | ① | Ⓗ | Ⓓ |
| | ② | Ⓘ | Ⓓ |
| 案B | ① | Ⓗ | Ⓑ |
| | ② | Ⓘ | Ⓑ |
| | ③ | Ⓖ | Ⓑ |

(2) a ： カ　b ： ウ　c ： イ　d ： ア

e ： オ　f ： ク　g ： キ　h ： エ

問 2 （配点 100 点）

設問 1 （10 点：(1)2 点×2，(2)2 点×3）

（1） a ： エ　　b ： イ　（a，b は順不同）

（2） c ： ケ　　d ： ウ　　e ： コ

設問 2 （20 点：(1)3 点×3，(2)3 点×2，(3)5 点）

（1） f ： 取得対象とする機器等

g ： 取得するログの種類と項目

h ： 取得したログの保存期間

（2） i ： フォーマット　j ： 統一化

（3） ネットワークトラフィック量を通常時プロファイルと比較して異常を検知する。

設問 3 （40 点：(1)6 点，(2)（HTTP リクエスト）4 点，（HTTP レスポンス）4 点，(3)（問題）4 点，（措置）4 点，(4)4 点，(5)3 点，(6)3 点，(7)（行番号）3 点，（役立つ情報）5 点）

（1） プロキシサーバのログ等から，new3.exe をダウンロードした時刻にサイト M にアクセスした PC の IP アドレスを割り出した。

（2） （HTTP リクエストによる活動） マルウェア K が担う指令の要求とそこで指定されたファイルの送信

（HTTP レスポンスによる活動） IPn のサイトからの指令を受け取る。

（3） （問題） マルウェアが活動した痕跡情報がネットワーク切断によって失われる可能性がある。

（措置） ネットワーク切断の前に，記憶媒体等のスナップショットを採る。

（4） k ： プロキシサーバのログで IPn のサイトにアクセスした機器の記録がほかにあるか

（5） 7 回

（6） ハッシュ値

（7） （行番号） 28 行目

（役立つ情報） 当該記録の日時に宛先 IP アドレスが IPn 宛ての HTTP 通信の FW の記録

設問 4 （23 点：(1)3 点×3，(2)2 点×7）

（1） ア ： 9/4 14: 31　イ ： 9/4 14:37　ウ ： 9/5 10:41

（2） m ： タ　　n ： コ　　o ： ソ　　p ： ケ　　q ： シ　　r ： カ　　s ： オ

設問 5 （7 点：(課題)2 点，(措置)5 点）

（課題） b

（措置） インシデント対応の作業手順を明確化し，文書化する。

以上