平成３０年度秋期　情報処理安全確保支援士　午後Ⅱ試験　解答速報

（株）アイテック　IT 人材教育研究部　2018.10.24 発表

問１　クラウド環境におけるセキュリティ対策

【解答例】

［設問１］ GDPR

［設問２］

(1) R&D 情報は，物理的な入退室管理が行われているプロジェクトルーム内に配置されたプロジェクト専用サーバに保管すること

(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 社の工場及びデータセンタに配置すること

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

③ 同じ重要インフラ設備を製造する工場及び生産関連サーバは同一の国又は地域内の 2 か所以上に配置すること

IaaS C のサービス仕様の内容：日本国内のデータセンタは 1 か所で，被災時に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こと

(3) X 社のシステム機器の IP アドレスが，IaaS C で予約されているプライベート IP アドレスと重複した場合に，利用できないという問題

［設問３］

(1) 1 回のログオン操作によって利用可能なサーバが増える。

(2) 業務サーバ：㋑，㋒　　構成要素：㋖，㋗，㋘，㋙

［設問４］

(1) ティア 1：イ　　ティア 2：ウ　　ティア 3：ア

(2) パッチの適用や脆弱性情報の管理に関する情報セキュリティ標準に不適合となる。

(3) ① 設定値を自動で収集できる。

② 設定値を自動で変更できる。

［設問５］

(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　セキュリティインシデントへの対応

【解答例】

［設問１］

(1) a：イ　　b：エ　（順不同）

(2) c：ケ　　d：ウ　　e：コ

［設問２］

(1) f：ログを取得する機器

g：取得するログの種類

h：保存期間と廃棄方法

(2) i：フォーマット

j：正規化

(3) 通常時のトラフィック量や推移を基にして異常な状態を検出する。

［設問３］

(1) プロキシサーバのログからサイト M へのアクセスを抽出し，プロキシサーバへの送信元 IP アドレスで PC を特定する。

(2) HTTP リクエストによる活動：遠隔操作の指示の要求と指定されたファイルの送信を行う。

HTTP レスポンスによる活動：遠隔操作の指示に従って動作する。

(3) 問題：ネットワーク切断に伴ってマルウェアの活動に関する情報が消失する可能性がある。

措置：PC-A において消失する可能性のある情報を保全する。

(4) k：プロキシサーバのログを用いて，PC-A 以外の機器から IPn への通信の有無

(5) 7（回）

(6) l：ファイルハッシュ

(7) 行番号：28（行目）

役立つ情報：PC-A から IPn へ送信された HTTP リクエストのメッセージサイズ

［設問４］

(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］

課題：b

措置：インシデント対応における作業手順を規定する。

以上