平成１９年度　秋期　情報セキュリティアドミニストレータ　午後Ｉ　解答例

問１

出題趣旨：

IPsec-VPN の設定を通して，IPsec に関する知識だけでなく，セキュリティの基礎技術である暗号やセキュリティプロトコルについての知識を問う。特に，様々な VPN から適切な方式を選択する判断力及び適切に IPsec-VPN を運用する能力を総合的に問う。

設問１　a　ア　　b　カ　　c　オ　　d　エ　　e　キ

設問２　ア　意図しない相手との通信
　　イ　データの破壊

設問３　FWR1 と FWR2 で，フェーズ 1 の暗号スイートが，少なくとも一つは同じになるように設定を変更することについて，適切に記述していること（解答の要点を示す）

設問４（1）U 研究室とデモルームのいずれにおいても，ユーザ認証といった，VPN に関する PC 上での操作をせずに VPN を利用できることについて，適切に記述していること（解答の要点を示す）
（2）公開鍵証明書 IKE 方式と比較したときのメリット：
・公開鍵証明書の発行や失効などの管理が必要ないこと
・TTP から公開鍵証明書を購入しなくてもよいこと
手動鍵管理方式と比較したときのメリット：
暗号鍵がセッションごとに更新(生成)されないという安全性の懸念がないこと

講評：

問 1 では，暗号技術と VPN に関する基本的な知識について出題した。全体として，正答率は高かった。

設問 1 b，c は，正答率が低く，IKE と DH の役割といった，IPsec や通信セキュリティの基本知識が不足していると推察された。情報セキュリティアドミニストレータとして，基本的な知識は身に付けておいてほしい。

設問 4(1)は，利用者の観点から解答することを求めたが，この趣旨を違えた解答が散見された。問題文のケースでの IPsec VPN は，利用者への負担が最も少なく，ほかの方式で想定される操作が必要でないものがあることを指摘してほしかった。一方，(2)は，運用管理の観点から解答することを求めており，問題文から論理的に分析する技術的な問題であるが，正答率は低かった。与えられた技術的情報を，状況に応じて，論理的に分析することを心掛けてほしい。

問２

出題趣旨：

情報セキュリティマネジメントの重要な要素の一つである，情報のライフサイクル管理を取り上げ，抑止，予防，検知，回復の観点から実施すべき情報セキュリティ対策を問う。併せてリスク対応を取り上げ，そのうちのリスク回避について，正しい考え方を問う。

設問１　a　ア　　b　ケ　　c　キ　　d　カ　　e　サ

設問２　ア　USB メモリを袋に入れて封印し，未開封であることを受領時に確認する。
イ　送信履歴をチェックして，社外への誤送信の有無を確認する。
ウ　・ファックスはメモリへ受信し，係の者が印刷して届ける。
・受信したファックスの取扱者を定め，その取扱者が名あて人へ届ける。
エ　・受信したファックスの授受簿を用意し，受信履歴と照合して確認する。
・名あて人が受領したファックスと受信履歴を定期的に照合し確認する。
オ　・メールの内容を記録し，保存することをアナウンスする。
・送信済メールの内容を定期的に確認することをあらかじめ周知する。

設問３　(1) ⑨と⑩
(2) 暗号化した添付ファイルの内容を確認できない。

設問４　・本社と各営業所にスキャナを設置して紙文書を電子化し，更に暗号化してからメールで送受信する。
・紙文書を電子化し，本社と各営業所間を VPN 接続してファイル共有サーバで受け渡す。

講評：
問 2 では，電子メール，ファックス，USB メモリなどを例にとり，情報の身近な取扱いに潜むリスクについて出題した。全体として，正答率は高かった。
設問 2 では，想定されるリスクに対する情報セキュリティ対策を，抑止，予防，検知の各視点から解答することを求めたが，それらの視点を混同している解答が見受けられた。情報セキュリティ対策を検討する際には，各視点の意味を理解した上で，それらを組み合わせる対策検討が効果的であることを理解してほしい。
設問 4 は，正答率が高く，ほぼ題意は理解されているようだが，リスク回避策ではなく，リスク移転策を記述した解答が散見された。リスク対応の選択肢である，リスク回避，リスク低減，リスク移転などの考え方について，十分に理解してほしい。

問３

出題趣旨：
電子文書が広く活用されるようになり，その漏えい，改ざん，破壊対策に真剣に取り組まねばならない時期にきている。電子文書はコピーや改ざんが容易なことから，紙とは異なる管理が求められる。
本問は，このような管理の実現に必要な知識と問題解決能力を問う。

設問１　a　ウ　　b　ア

設問２　・電子文書登録時にアクセス許可期間を設定できるから
・アクセス許可期間を過ぎると利用許可証が発行されないから

設問３　①②
・各電子文書ごとのアクセスを許可する者とその操作権限の見直し
・電子文書の管理単位の見直し
・電子文書の登録番号の重複調査と付け直し
・統合後の事業部の文書管理者の任命

設問 4　文書管理者が RM サーバに登録された電子文書の属性一覧を定期的に確認する。

設問 5　処理内容(A)　①②　・共通鍵の生成　　・電子文書の暗号化
通知内容(B)　①②　・登録番号　　・生成した共通鍵

講評：

問 3 では，機密に区分される電子文書の安全な管理について出題した。全体として，正答率は低かった。

設問 1 は，選択肢問題にもかかわらず，“必要の原則(need to know)”の正答率が低かった。“必要の原則”は，セキュリティマネジメントの原則の一つであり基本的な用語なので，知っておいてほしい。

設問 3 では，“公開鍵証明書の失効と再発行”とした誤った解答が目立った。問題文中の失効や再発行の条件を読めば，事業部統合時は該当しないことがすぐに分かるはずである。

設問 4 は，予想以上に正答率が低かった。“確認”は管理の基本である。不適切な権限設定によって引き起こされる問題の真の原因は，正しく設定されているかどうかの確認がなされていなかったことであることを読み取ってもらいたい。

設問 5 では，文書ごとの共通鍵の生成，文書の暗号化，生成した共通鍵の通知，通知された共通鍵による復号という一連の流れについて出題したが，(B)の通知内容として“生成した共通鍵”を答えていない解答が目立った。受験者の知識がまだ不十分であると思われる。

問４

出題趣旨：

PDCA モデルに基づく情報セキュリティマネジメントシステムの継続的改善手法は，時々刻々と変化する環境下において，組織が有効に機能し続けるための，重要な手法を提供している。

本問は，情報セキュリティアドミニストレータとして理解していなければならない，情報セキュリティの継続的改善を主題としている。本問では，設問を通じて，インシデント対応能力，改善策を立案する能力などを問う。

設問 1　a　個人を識別されない者による，アカウントの不正利用
b　パスワードを推測した者による，アカウントの不正利用

設問 2　・残存している退職者のアカウントを停止する。
・すべてのパスワードを変更し，利用者に通知する。

設問 3　(1) 調査用紙に記載された数値の根拠
(2) 社内規程遵守の不徹底の原因を究明して改善策を立案すること
(3) 効果のある対策事例を見いだして改善策に反映させること

設問 4　(1) 正社員以外のアカウント付与に時間がかかっていること
(2) 正社員以外にアカウントを付与する場合の承認者を総務部長から各部署の部長に修正すること

講評：

問 4 では，アカウント管理を例にとり，情報セキュリティの継続的改善について出題した。全体として，正答率は低かった。

設問 3(1)では，評価値の精度を確保するためには，評価値の算出方法に問題がないことが重要であ

るということを理解してほしかったが，題意を正しく理解していない解答が目立った。例えば，周知の不徹底によって評価値の算出方法がサーバ管理者ごとに異なると，評価値の精度が確保できない。定量分析の実施に当たって重要なポイントが何かということを，問題文中の背景から十分に読み取ってほしい。

設問 4(1)では，題意は理解されているが，原因としての記述になっていない解答が散見された。問題となっている事象を記述するのではなく，その原因を考察して記述してほしい。

設問 4(2)では，アカウント付与の承認者を変更することは理解しているが，承認者として選んだ役職には不適当な解答が散見された。社内規程の修正に当たっては，問題点を解決するという視点にとどまることなく，修正された規則の実効性が十分であるかということにも留意してほしい。

注：この解答例に関するメールでのご質問には、応じかねます。あしからずご了承ください。