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Ⅱ　解答例

この解答例は、独立行政法人 情報処理推進機構　情報処理技術者試験センターが公表しているものです。著作権は、同センターにありますので、その点ご注意ください。

問１

出題趣旨：

新たな経営課題と施策を理解したうえセキュリティ対策を実施するという，企画・経営補佐的なセキュリティアドミニストレータ像が，IT の高度利用を目指すために重要となっている。

本問では，こうした背景を踏まえ，近年話題の経営改革手段を題材に，セキュリティ企画能力，セキュリティ技術基本能力，情報技術基本知識経営基本知識，及びこうした全社施策の推進能力・経験を問う。

設問１　(1)　a　盗聴　又は　改ざん　又は　漏えい
b　遮断　又は　制限　又は　ブロック
c　ウイルス定義ファイル　又は　パターンファイル　又は　シグネチャ
d　クリアデスク　又は　物品の保管管理　又は　盗難防止
e　抑止力　又は　予防効果　又は　けん制

(2) のぞき見対策　・のぞき見防止フィルタ
・プライバシフィルタ
・偏光フィルタ
置忘れ対策　・ディスクの暗号化とパスワード認証
・BIOS による起動パスワードの設定

設問２　・社員証の常時着用
・Q 社専用の ID ケースの着用

設問３　(1) 適切なユーザ属性グループを設定し，ネットワーク資源へのアクセス権を登録する。
(2) 社内ポータルシステムに不具合が起こると，基幹システムが全く利用できない。

設問４　(1)・試行対象の D 事業部は，午後出勤が多く，システム利用の集中時間がないので，全社展開時に性能が出ない。
・D 事業部は出勤時刻が不規則なのでログインが集中しないが，全社展開すると 9 時前に集中し，問題が起こる。
(2) 心配な点：誤って他部署のプリンタに出力し，他部署の人に印刷物を見られてしまう。
技術的なセキュリティ対策：
・認証機能付きのプリンタを導入する。
・近くのプリンタでしか印刷できないようネットワークで制御する。

設問５　・セキュリティ対策に関してユーザが行うべき事項についての通知を，プッシュ型で情報を通知する機能を用いて行う。
・セキュリティパッチやウイルス対策ソフトのアップデート依頼をプッシュ型で行う。
・プッシュ型で，重大なセキュリティ問題についての対応方法を通知する。

講評：

問 1 では，最近のワークスタイル改革を題材に，情報セキュリティアドミニストレータとしての知識力，状況判断力を問う出題とした。全体として，正答率は高かった。

設問 3(1)では，問題文中に示したネット型 OS の機能を理解して，設定された状況における判断を適切に記述した解答は少なかった。問題文に明記してある事項との矛盾があったり，設定と異なる状況を答えたりした誤った解答が多かった。問題文をよく読み取ってほしい。

設問 3(2)，設問 4(1)は，正答率が低かった。設問では，情報セキュリティ対策ではないが，情報システムを導入する上で必要な洞察力を問うている。情報セキュリティ対策の知識だけではなく，一般的な情報処理技術についても理解しておいてほしい。

設問 5 では，問題文中で議論してきたワンストップ型情報システムを使って，Q 社のセキュリティ上の課題を改善するための提案を求めている。経営に貢献する情報セキュリティアドミニストレータとして，適切な解答を期待したが，正答率は低かった。問題文全体を通して関連情報を集めれば，それほど難しい問題ではないので，全体を読み込んで解答してほしかった。

問２

出題趣旨：

この問題では，情報システムを統合する際のアクセス権限や認証に関する情報セキュリティの再構築の問題を背景に，一般利用者の認証とアクセス管理，及び管理業務に必要となるアクセス権限についての経験を問うこととした。また，アクセス権限を付与する考えの背景には，内部統制の強化がある。

本問では，内部統制の基本としてのアクセス管理は，情報セキュリティアドミニストレータが扱うべきものとして，基礎的な知識などを問う。

設問 1　(1) ア　R　　イ　R　　ウ　RW
(2) a　運用業務との独立性
(3) d　就業規則

設問 2　①②
・運用者が，プログラムを勝手に変更して，それを実行することを防止できる。
・保守者が，担当業務外のデータをバックアップして持ち出すことを防止できる。
・保守権限を有する開発者が，変更中のプログラムを誤って実行することを防止できる。

設問 3　(1)　B
(2) b：　リバースプロキシサーバ 2
c：　プロキシサーバ
(3) PC の画面及び操作内容をネットワーク管理サーバ 1 を経由して監視する。

設問 4　V 社の社員の行動を監視カメラで監視する。

設問 5　(1) 番号：Ⅱ.2.(2)
業務内容：Web 会員 DB とクレーム DB の一部を USB メモリで社外に持ち出していること
(2)・バックアップテープをデータセンタと本社にそれぞれ保管する。
・本社 LAN にサーバを設置して，主要 DB のバックアップデータを転送して保存する。
(3) 社員の Web 閲覧の監視の実施
(4) 新たに生じるリスク：
V 社が R 社の会員情報や機密情報を扱うことによる漏えいや改ざん

具体的な管理策：

・V 社に対して，重要度 A，B の情報の取扱いについてセキュリティポリシの管理内容を遵守するように契約に追記する。

・V 社に対して，外部による情報セキュリティ監査の受査及び結果の報告を求める。

講評：

問 2 では，システムの統合とそのシステムのデータセンタへの外部委託における情報セキュリティを主題として出題した。全体として，正答率は高く，主題とした情報セキュリティについては理解できているようであった。

設問 1 では，(2)の正答率が低かった。監査は，対象業務から独立すべきことを知っていてほしい。

設問 2 は，正答率が低かった。職務の分掌は，情報セキュリティアドミニストレータの仕事に関連するテーマであるので，理解しておいてほしい。

設問 4 は，正答率が低かった。設問では，委託先企業の担当者がサーバ室で単独で特権権限を行使して，重要な情報を媒体で不正に持ち出す場合の物理的管理策について問うている。管理策について，実際の適用場面を想定して，理解を深めてほしい。

設問 5 は，問題の背景を読み取って解答するよう工夫したが，(3)と(4)の正答率が低かった。(4)では，業務委託を想定していない解答も少なからず見られた。業務委託における情報セキュリティの問題点を理解して解答してほしかった。

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。