2009 秋 情報セキュリティスペシャリスト 総合実力診断模試 講評と採点基準

2009 年 8 月 20 日 (株)アイテック 商品開発本部

■ 全体講評

得点分布が正規分布ではなく，平坦に分散している印象です。知識学習や過去問演習などの学習の進んでいる方が高得点していると推測します。合格圏に達していない受験者の方は，本試験までの残された時間を有効活用して，専門知識の定着と問題演習に取り組んでください。

平成 21 年春期の SC 試験では，問題選択によって得点結果に差がついたと思われます。今回選択しなかった問題にもチャレンジして，自分の得意/不得意分野を見極めていくことも作戦上重要です。

解答作業全体に共通する留意点を二つ書きます。まず，解答用紙の選択問題を丸で囲っていない答案がとても多かったです。本試験では採点対象外になりますので注意してください。また，「IIS」や「IE」などのように，問題文に書かれていない固有の製品名を使った解答がありました。このような解答は不正解になりますので注意してください。

■ 午後Ⅰ講評

【問1】

設問 1 は正答率が高かったです。「社内外へのウイルス感染防止」とありますので，送信元やあて先を限定するのは合理的ではありません。

設問 2（1）SSH は他の試験区分も含めて出題頻度が高くなっていますので押さえておきましょう。（2）SSH はセキュリティプロトコルですので，パスワードの保護だけではなく通信を暗号化できます。「認証できる」という解答もありましたが，認証は FTP でも可能です。(3)「DMZ の DNS サーバから不正アクセスする」や「DNS の Web サーバから不正アクセスする」のように対象サーバを限定した解答もありましたが，根拠なく解答の幅を絞り込むことは避けるべきです。解答が「攻撃」の説明になっていないものも見られました。また，IP スプーフィングの観点の「送信元 IP アドレスを DMZ のアドレスに詐称する」は，問題文の記述の範囲では合理性がありますので正解としました。ただし，ルール 8 をファイアウォールの DMZ ポートに適用するルールと見なすと，インターネットからの直接攻撃はできなくなります。

設問 3（2）下線⑤と下線⑥を逆に解答したものも目立ちました。考え方を十分理解しておきたいです。

（3）バッファオーバフロー攻撃やコマンドインジェクション攻撃が示されているにもかかわらず，「DoS 攻撃が可能」など，論点をずらしてしまう解答も目立ちますので留意してください。攻撃パケットを「正しい通信」と言い切るのも表現として違和感があります。

（4）FW との連携が前提になっているのに「IDS だけでは防御できない」といった読み違いも目立ちました。「未知の攻撃を検知できない」という解答は，FW との連携という設問の重要ポイントから離れてしまっています。

【問2】

メールセキュリティでは，特に設問 3 の SenderID や DKIM の特徴を押さえておきたいです。

設問 1 は知識問題ですので，知識力の差が得点力の差に現れます。a：はたんに「フィルタリング」という解答が目立ちました。h:の否認防止は正答率が低かったです。なりすましと否認の違いを確認しておきましょう。

設問 2（2）は問題文に直接のヒントのない知識問題です。「サーバやクライアントが対応していない状況」といった観点がありました。確かにそういう状況もあり得ますが，技術的な理由・背景がある場合は，それらを優先的に解答しなければなりません。そのためにも知識学習が必要です。（3）は考察問題で，設問 1 (c) が正答できればこちらも解答しやすいです。

設問 3（1）では「メールヘッダ内の IP アドレス」という解答が目立ちました。比較対象は接続元 IP アドレスです。また「DNS サーバの SPF レコードの IP アドレス」も多く見られました。これは設問の読み違いですので注意してください。ドメインと IP アドレスの関係も整理しておきましょう。（2）DKIM では送信元のメールサーバが署名を行います。送信元のクライアント（メールソフト）が署名するように理解していると思われる解答が多くありました。もう一度確認しておきたいです。

【問3】

設問 1（1）正答率が高かったです。（2）も正答率が高かったです。下線④の対策で「アカウントを無効化する」がありましたが，ここは「一時停止」あるい

は「アカウントロック」の方が妥当です。下線⑤の対策では「注文時にメール通知する」がありました。なりすましのログオンを検知するのが目的ですので,注文時だけでは不足です。プッシュ型で顧客に通知するしくみであることも正解の要件になります。(3) も比較的正答率は高かったです。ただし,忘れたパスワードを思い出させる施策などは文意に合いません。新しいパスワード(仮パスワードが安全)を新規発行するということと,画面上では通知しないということを押さえることがポイントです。

設問 2 では「なりすましで不正アクセスする」といった解答が多くありました。「初期パスワードの配布方法では～」という設問の論点の読み落としです。このような問題では,問題文中のキーワードを適切に引用することに留意してください。

設問 3 (1) は正答率が低かったです。このような観点も押さえておきましょう。(2) の照合用文字列では,不正プログラムが判読できない画像文字に着眼した解答がありました。この観点は今後出題可能性がありますが,この問題では電子メールで送信しますので画像文字は適切ではありません。(3) は解答した方のほぼ全てが正解しています。最後の設問が容易なこともよくありますので,本試験でも時間配分に気を使って得点できる設問で点数を重ねていきたいです。

【問4】

設問 1 は (b) の正答率が低かったです。セキュリティ管理分野の用語を押さえておきましょう。

設問 2 は正答率が低かったです。問題文中のヒントを参照できたかを振返ってください。

設問 3 (1) では,問題文中の「業務用 VLAN」といった用語を的確に引用したいです。「VLAN」だけでどちらの VLAN か区別できない解答表現も見られました。また,スイッチを交換する必要があるかは,問題文からは断定できません。解答文の中で「～の場合は…」というように想定を含ませるのは避けたいです。問題文の情報から導かれる内容を吟味したいです。(2) は技術的に掘り下げて説明することに留意したいです。たんに「感染する可能性がある」では説明になっていません。

設問 4 は「D 社 L2SW を使用してポート単位で隔離する場合」の接続方法が論点であることと,問題文中に関連するヒントが明示されていることを意識することが重要です。「D 社 L3SW に PC を直結」という観点については,幹線 D 社 L3SW が D 社検疫システムに対応していることから,D 社 L2SW を経由しないフレームは転送しないと判断できます。

■午後 I 採点基準

【問1】

〔設問 1〕解答例のみを正解としました。

〔設問 2〕(1) 解答例のみを正解としました。(2) パスワードを安全に通信させるという解答は部分点としました。(3)「送信元 IP アドレスを DMZ のアドレスに詐称する」は正解としました。

〔設問 3〕(1), (2) 解答例の主旨に合うものを正解としました。(3) 不正コードがパケットのペイロードに格納されていることに着眼できているものを正解としました。(4)「FW と連携したとしても防御機能が FW の機能に依存する」という主旨の解答は部分点としました。

【問2】

〔設問 1〕解答例のみを正解としました。

〔設問 2〕(1) 解答例の主旨のみを正解としました。(2) SMTP 送信時には POP 認証した IP アドレスで判断するという点に着眼できているものを正解としました。POP 認証のパスワードが平文でやり取りされるという脆弱性に着眼したもので解答表現が妥当なものは正解としました。(3) 社内の IP アドレスで制御できるという主旨のものを正解としました。

〔設問 3〕(1) 解答例の主旨のみを正解としました。(2)「複数の SMTP サーバを経由したメールの送信元を認証できる」は,署名の対象範囲によっては署名の検証に失敗するため,部分点としました。そこまで含めて表現できているものは正解としました。

【問3】

〔設問 1〕(2) 下線⑤の対策は「集約したログイン履歴をメールで通知する」などの観点も正解にしました。(3) パスワードを新規作成するということと電子メールで通知するという二つの要件が表現されていないものは,内容により部分点あるいは不正解としました。

〔設問 2〕解答例の主旨に合うもののみを正解としました。

〔設問 3〕(1) メールサーバの負荷増大に着眼したものを正解としました。(2)「ランダム」と「十分な長さ」の 2 つの要件を含むものを正解としました。(3) 解答例の主旨に合うものを正解としました。

【問4】

〔設問 1〕解答例のみを正解としました。

〔設問 2〕解答例のみを正解としました。

〔設問 3〕(1) タイミングは主旨が整合していて「IP アドレス取得後」が明示されていないものは部分点としました。範囲は「業務用 VLAN 以外」の領域であることが明示されているものを正解としました。(2) 解答例のほかに，IP 通信や HTTP 通信が可能であることに着眼できているものを正解としました。

〔設問 4〕ハブの接続を明示せずに認証済みの D 社 L2SW のポートに接続するという観点は部分点としました。L3SW に直接接続するという観点は不正解としました。

■午後Ⅱ講評

【問1】

設問 1 (1) (ア)「情報を保存しない」という観点は，この後の問題文でシンクライアント導入がテーマになりますので除外すべきです。(イ) (ウ)「ＰＣの置き忘れ対策がテーマで，物理的セキュリティ対策の観点が強いことを意識して考察したいです。(2)「置き忘れ対策」が観点であり，「BIOS パスワードを設定していたとしても～」とありますので，「ソーシャルエンジニアリングによる盗み見」のように，利用中の情報漏えいは除外できます。

設問 2 (1) g : 空欄 g のうしろに「特殊文字」とありますので，「バインド変数」や「プリペアド・ステートメント」などを除外します。(2) 設問のキーワード「可用性」からストレートに考えるとよいでしょう。また，「可用性の問題」が問われているのに，解決策を中心に記述した解答も見られました。(3) エラーメッセージの内容に起因するリスクが論点ですが，例えば「ユーザの視点での使いやすさ」に着眼した解答もありました。常にセキュリティの観点で考察することに留意してください。

設問 3 (3) は「インターネット区間以外にも」という設問の記述から，まずリスクのある「区間」を特定して，その理由を技術的に説明したいです。(4) は正答率が低かったです。認証の制御方法の一つとして理解しておいてください。

設問 4 (2) では CRC-32 を暗号化方式と解釈した解答が目立ちました。WEP の脆弱性の一つとして覚えてください。(3)，(4) は技術的に難易度が高い内容になっていますが，(3) は問題文にヒントがあります。問題文のヒントとユニキャストとマルチキャスト通信の違いといった既知の技術的知識を組み合わせて考察するという解法も確認してください。

【問2】

設問 1 (1) (c) 認証と認可の違いでの誤りが多くありました。(2) 最後のパイプ文字が不足している解答が多く見られました。(3) 正答率は高かったです。SQL インジェクション関連の内容の解答が見られました。まず，セキュアプログラミングにおけるどのテーマが論点かを意識するとよいでしょう。

設問 2 (1) ログを考察する問題はときどき出題されます。間違った方は，解説を確認してどの程度じっくり読み取る必要があるかの感覚をつかんでおくとよいでしょう。(2) 正答率は高かったです。(3) エスケープ処理は入力データに対して行うことを確認しておきましょう。(4)「DB 管理 TBL に対する参照権限を削除する」という解答が多く見られました。空欄 b の後ろには「定石」と表現されていることと，制限文字数が 50 字と十分とられていることも考慮して，「定石」として，しっかり表現したいです。正解になっている方も，解答例の表現を十分確認してください。

設問 3 (1) 正答率はたいへん高かったです。(2) (不足している情報) 正答率は低かったです。問題文に全ての条件が示されていないことから，難易度の高い問題になっています。(改修内容) たんに「必要なログを記録する」というレベルの解答も見られました。それでは (不足している情報) の解答を裏返しただけですので，改修内容としてはもう 1 段掘り下げて説明することが求められています。(3)「専門家を育成する」という主旨の解答がありましたが，下線④の後ろの「だれが対応しても～」と整合しません。同じようにシステム的な対策の観点だけでは不足です。

■午後Ⅱ採点基準

【問1】

〔設問 1〕(1) (ア) 解答例の主旨のみを正解としました。(イ)「監視カメラの設置」，「手荷物検査」は正解としました。たんに「持ち出し管理」は部分点としました。(2) 解答例の主旨のみを正解としました・

〔設問 2〕(1) d : IPS は部分点，IDS は不正解としました。f : サニタイジングも正解としました。その他は解答例のみを正解としました。

(2)「高いスペックが必要だ」などのようにたんに性能だけの観点で表現し，可用性に関するリスクが示されていないものは不正解としました。

〔設問 3〕(1) ～ (4) 解答例の観点のみを正解とし

ました。(4) はしくみを表現できていないものは不正解としました。
〔設問 4〕(1) 解答例のみを正解としました。(2) ～ (4) 解答例の観点のみを正解としました。(3) はMACアドレスの利用法に着眼していることが伝わるものを正解としました。

【問2】
〔設問 1〕(1) ～ (2) 解答例のみを正解としました。(3) 解答例の観点のみを正解としました。
〔設問 2〕(1) ～ (3) 解答例のみを正解としました。(4) アクセス権限を最小化するという観点を表現できているものを正解としました。
〔設問 3〕(1) 解答例のみを正解としました。(2)（不足している情報）解答解説冊子では 2 点×3 となっていますが，TRN ログ単独，DB ログ単独それぞれ完全正答で 3 点×2 で配点しました。(改修内容) 利用者の識別子に言及できていないものは不正解としました。しくみの説明が不十分な場合は部分点あるいは不正解としました。(3) 例えば「手順策定」と「体制構築」は二つで全体の半分 (8 点) の配点としました。

以上