2010 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

2010 年 8 月 18 日 (株)アイテック 商品開発本部

■ 全体講評

知識学習と解答作成の 2 点について全体的な講評を述べます。

専門知識の知識習得では，順調に学習が進んでいる方がおおよそ 3 割程度とみます。IPA のセキュアプログラミング講座の内容や，IEEE802.1X や認証 VLAN のメカニズム，セキュアな Web アプリケーションの設計方法，証明書やディジタル署名など，分野ごとに十分理解していることが伝わる解答があります。「3 割」は合格圏に達している割合と同じと分析します。学習が進んでいるということは，教材の勉強や午後問題演習に十分取り組んでいる成果です。逆に言うと「7 割」の解答には，理解不足箇所が見られます。この模擬試験を受験して，専門知識が不足していると感じた方は，知識学習を強化してください。

解答作成では，設問に整合しない解答が多く見られました。個々には以下の講評で書きますが，例えば，午後Ⅰ問 1 設問 1(3)では「読み出すときの現象」が問われているのに，「書き込むときの現象」を解答しているなどです。設問や下線部，下線部の前後で論点が絞られることがしばしばあります。設問を正確に把握するだけで得点アップする余地は大きいです。

また，「Promiscan」や「ベリサイン」などのように，問題文に書かれていない固有のツール名や企業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。

平成 22 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。

なお，以下の採点基準で「部分点」は配点の半分（少数切り上げ）です。

＜午後Ⅰ＞問1 プログラム開発におけるセキュリティ

【採点基準】

[設問1]

（1）a :「制御」は部分点としました。b :「クリア」「初期化」は部分点としました。c :「修正プログラム」なども正解としました。d :「実証」,「検証」は正解としました。e : 解答例のみを正解としました。

（2）～（4）解答例と同じ主旨のみを正解としました。

[設問2]

（1），（2）解答例のみを正解としました。

（3）「サーバからの SYN-ACK 応答に対して，ACK を返さない」も正解としました。

（4）「SYN クッキー」や「ディレイドバインディング」など妥当な方法を説明したものは正解としました。

[設問3]

（1）「エンコード」は部分点としました。

（2）解答例と同じ主旨のみを正解としました。

〔講評〕

[設問1]

（1）a :「制御」という解答がありました。次の「サーバを支配され」を考慮すると「管理者権限」が妥当です。e :「脆弱性診断」などは空欄の後ろの「脆弱性を検査」と重複します。別な表現や用語を検討すべきです。

（2）「バッファをゼロクリアしていない」という解答がありましたが，strncpy 関数で n 文字を指定するので条件として不足です。

（3）全体講評でも述べたように，設問の論点を見落としている解答が多くありました。

（4）正答率は高かったです。「問題が発生する」理由が問われているのに対し，「事前検証が必要」のように対策を解答しているものがありました。

[設問2]

（1），（2）正答率は高かったです。

（3）設問に「TCP コネクションの確立方式に着目し」とありますので，具体的に説明する必要があります。抽象的な表現の解答がありました。

（4）「IP アドレスで制限する」は問題文の「TCP コネクション数の制限」と同じ主旨なので除外する必要があります。

[設問3]

（2）正答率が低くなりました。設問では「どのように処理すべきか」が問われているのに，現状の問題点を指摘する解答がありました。

問2 ネットワークのセキュリティ対策

【採点基準】

[設問1]

解答例のみを正解としました。e は「証明書」や「クライアント証明書」など同じ内容は正解です。

[設問2]

（1）a : 解答例のみを正解としました。b : 解答例と同じ主旨のみを正解としました。c : 物理的なアクセス制

御を説明できているものは正解としました。
［設問3］
（1）解答例と同じ主旨のみを正解としました。
（2）解答例と同じ主旨のみを正解としました。ユーザごとの規定のVLANに接続ことの説明が不足のものは，内容によって部分点としました。
（3）解答例と同じ主旨のみを正解としました。

〔講評〕
［設問1］
a～e の正答率は高かったです。EAP の認証方式の c と d の正答率がやや低くなりました。f の「EAPOL」は正答率が低くなりました。
［設問2］
（1）a：装置名として表現されていない解答がありました。「LAN アナライザ」はスニファリング機能を提供しますので，「スニファリングツールで盗聴」という問題文の流れに合いません。
b：ミラーポートの機能を説明した解答がありました。前の設問で機能を解答済みであることを考慮し，「スニファリングツールで盗聴可能な理由」としては，パケットを取得できる理由ではなく，パケットを読める理由を優先します。
c：「データを暗号化する」のように，物理的な対策に整合しない解答が多くありました。
［設問3］
（1）必要な情報名とプロトコル名の片方のみの解答がありました。また，「DHCP サーバが IP アドレスを割り当てる」という主旨の解答が多くありました。認証サーバが VLAN-ID を管理しているなど，本文の説明に基づいて解答を吟味してください。
（2）問題文を十分理解した解答と理解不足の解答で大きな差が出ました。大きく間違えた方，あるいは問題文を読み切れずに空欄になった方は，もう一度問題文を読み返してみるのも学習になります。
（3）「MAC アドレスは詐称されるリスクがある」のように，「既存のアクセススイッチを流用する場合」という設問の視点に依存しない解答は除外する必要があります。

問3 Web サイトの個人情報保護

【採点基準】
［設問1］
「同意を得る」「了解を得る」「確認する」など本人の意思を確認することが含まれているものを正解としました。
［設問2］
（1），（2）解答例のみを正解としました。
（3）「正当なリクエストであることを確認できる」のように CSRF の特徴を理解しているが，理由の説明が不足な解答は部分点としました。CSRF の特徴を含まず，単に不正アクセスを防止できるという内容は不正解としました。
（4）b：「セッションキー」などセッション ID と同義のものを正解としました。c：「セッションの切断」「強制ログアウト」なども正解としました。
（5）クッキーの属性項目を含めて説明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）～（3）解答例と同じ主旨のみを正解としました。
（4）解答例と同じ主旨のみを正解としました。記号が不正解の場合，確認方法の内容が解答例と同じでも不正解としました。

〔講評〕
［設問1］
正答率は高かったです。
［設問2］
（1）装置名ではなく単に機能を書いた解答が見られました。「WAF 以外」とありますので，ファイアウォールは除外すべきです。「IDS」も多くありましたが，「検知したパケットを破棄」から「IPS」と解答したいです。
（2）正答率は低かったです。
（3）CSRF の特徴を理解している解答は少なかったです。本試験ではまだ出題されていませんが，今後の出題可能性があります。
（4）b：「パスワード」が多くありました。パスワードは利用者の認証情報です。
c：正答率は高かったです。
（5）「Max-Age 属性をゼロにする」主旨の解答がありましたが，この場合ブラウザはクッキーを即座に破棄するので適切ではありません。
［設問3］
（1）正解率は高かったです。
（2）「証明書は誰でも自分で作成できる」主旨の解答が多くありました。攻撃者が自分で作成した，つまり自己署名証明書などの場合，会員のブラウザでは証明書の検証で失敗します。鍵マークが表示されるということは，証明書の検証は正常に終了していますので，信頼できる CA から発行された証明書になります。ただし，それは証明書が J 社のものであることを保証するものではないということです。また，「接続している Web サイトが

J 社のものであるかを確認するため」のような表現は問題文そのままです。キーワードの「証明書」などを用いて説明し直します。
（3）下線部や前後の問題文をそのまま引用している解答が多くありました。ブラウザの警告メッセージを整理しておきたいです。
（4）正答率は低かったです。メールセキュリティのしくみを整理しておきたいです。また，メール会員側（受信側）のメールソフトの確認方法ではなく，送信元のメールの送信方法を説明した解答が多く見られました。

問4 情報セキュリティ管理の検討

【採点基準】

［設問1］

（1）a :「NDA」も正解です。b :「退職後」などは部分点としました。
（2）解答例と同じ主旨のみを正解としました。

［設問2］

（1），（2）解答例と同じ主旨のみを正解としました。
（3）個人の属性情報を登録することへの抵抗心や管理要求強度などの観点での妥当な説明は正解としました。

［設問3］

（1）f :「自動認識」なども正解としました。g : 解答例のみを正解としました。
（2）解答例と同じ主旨のみを正解としました。
（3）「感染 USB メモリを接続したパソコンを確認する」など，USB メモリの利用形態に応じて妥当なものは正解としました。
（4）「USB メモリは電子メモリなので，元の情報が残らない」など，磁気ディスクと電子メモリの違いを表現して妥当な内容は正解としました。

〔講評〕

［設問1］

（1）a :「個人情報保護」という解答がありました。外部のインストラクタの責任ですので，解答例の「守秘義務」などが適切です。b :「契約」など問題文の空欄に代入すると不適切な解答が多くありました。ていねいに確認してください。
（2）項番 5 の問題点を指摘して，修正内容を説明していない解答が多くありました。

［設問2］

（1）「その都度の暗証番号変更が負担になる」という主旨の解答が多くありました。本文には「暗証番号を毎回変更することは運用上容易です」とあるので除外して考察します。
（2）生体認証の誤認証を指摘した解答がありましたが，本文で「誤認証率はほぼゼロ」と述べられていますので，解答候補から除外します。
（3）正答率は高かったです。「身体的状況のために生体情報を登録できない場合がある」という解答は，一般的な課題であり，下線③の「セミナールームの入退室管理としては」という論点につながりません。

［設問3］

（1）正答率は高かったです。
（2）論点は隠しファイルの表示です。拡張子に着眼した解答がありました。
（3）USB メモリの利用形態を踏まえていない解答が多くありました。USB メモリを解答文に含めるのが確実です。
（4）「1 回で完全に消去できる」などは説明不足です。

＜午後Ⅱ＞問1 ネットワークのセキュリティ対策

【採点基準】

［設問1］

（1）解答例のみを正解としました。
（2）「PC を社内 LAN に接続する際のチェックがない」点を指摘したものも正解としました。

［設問2］

（1），（2）解答例のみを正解としました。
（3）解答例と同じ主旨のみを正解としました。メールパケットを対象にすることが表現できていないものは不正解としました。

［設問3］

（1）解答例のみを正解としました。
（2）解答例と同じ主旨のみを正解としました。
（3）利用者用の証明書の運用負荷に着眼して妥当なものを正解としました。
（4），（5）解答例と同じ主旨のみを正解としました。

［設問4］

（1）「IP アドレスの管理を一元化，自動化できる」や「PC のセキュリティレベルの維持」など妥当なものは正解としました。
（2）解答例と同じ主旨のみを正解としました。「社内ネットワーク」など「機器」を明示していないものは不正解としました。

〔講評〕

［設問1］

（1）正答率は低かったです。
（2）正答率は高かったです。

［設問2］

（1）a～c は正答率が高かったですが，d は「電子署名」という間違いが多くありました。

（2）正答率は高かったです。
（3）この設問はモニタ型に関するものですが，中継型ととらえているものがありました。また，「SW を通過するすべてのパケットを抽出する」というものが多くありました。抽出対象はメールトラフィックです。

［設問3］

（1），（2）正答率は高かったです。
（3）利用者の電子証明書ではなく，サーバの鍵ペアの管理などに着目したものがありました。サーバの鍵ペアであれば「管理者の運用負荷が大きい作業」とは言えません。
（4）パソコンを対象とする処理内容が多くありました。設問文の「認証サーバが認証 SW に対して行う処理内容」に応じて解答すれば，大きくずれることを防止できます。
（5）「一定時間ごとに PC を再認証する」はセキュリティ対策としては有効ですが，設問で問われている「監視方法」には該当しません。

［設問4］

（2）メールに関する目的を解答したものがありました。

問2 システム統合時におけるアクセス制御の設計

【採点基準】

［設問1］

（1）a：職務分離，b：カラム，c：レコードも正解です。
（2）問題文中で「例えば」として記述されているデータベース管理とオペレーション業務を行うものを分けることを記述したものは部分点としました。
（3）単に「アクセス権限に応じたビューを作成する」など説明不足な場合は部分点としました。

［設問2］

（1）～（4）解答例のみを正解としました。

［設問3］

（1）解答例のみを正解としました。
（2）解答例と同じ主旨のみを正解としました。
（3）解答例と同じ主旨のみを正解としました。取扱レベルの変更を説明せずに，利用者に応じた権限クラスの見直しを説明したものは部分点としました。「だれが」は解答例のみを正解としました。
（4）解答例と同じ主旨のみを正解としました。解決策で，Q 氏に付与する権限クラスを「クラス 5」と具体的に示していないものは不正解としました。

〔講評〕

［設問1］

（1）a：「最小権限」という解答がありました。「同一のものが実施するのは問題」という記述から，責務の分離を採用します。c：「事業部」が多くありました。RDBMS の機能として言い換えます。
（2）正答率は高かったです。「体制」として表現できていないものもありました。
（3）単に下線②の前後の問題文を引用しただけの解答が多くありました。具体的な設計の方法を説明する必要があります。

［設問2］

（1）e：は正答率が低かったです。キーワードですのでしっかり覚えてください。
（4）この問題のアクセス制御方式を読み取れたかどうかがポイントです。十分読み取れなかった方は，もう一度問題にチャレンジすることも効果があります。

［設問3］

（1）j で「クラス 6」が多く見られました。カテゴリの読み間違いでしょうか。
（2）時間をかけて問題文を検証します。読取り型の午後Ⅱ問題は根気よく取り組むことが必要です。
（3）ここでは情報資産に付与するラベルの変更が必要です。利用者に付与するラベルの変更を解答したものがありました。また，処理手順が逆の解答が多くありました。手順は，機密情報管理サーバにデータ移動後にラベルを付与します。移動前にはラベルを付与できません。更に，設問の指示事項の「～（だれ）が～する」という記述形式に合っていない解答がありました。
（4）「E-R 図へのアクセスができてしまう」という解答がありました。E-R 図よりも機密度の高い処理記述へアクセスを許可しますので，現状の設定で生じる問題を優先します。この課題が気になる場合は，解決策で「暫定的にクラス 5 にする」といった表現を含めて，懸念事項を採点者に伝えてもよいでしょう。

以上