2008 秋 情報セキュリティアドミニストレータ 総合実力診断模試 講評と採点基準

2008 年 8 月 25 日 (株)アイテック 商品開発本部

■午後Ⅰ講評

【問1】

［設問１］(1)暗号化技術の基礎知識と問題文の電子印鑑システムの仕組みの理解が必要です。正解できなかった方は，しっかりと見直しをしてください。(2)証明書の内容を解答したものが目立ちました。証明書と署名の関係を整理しておきましょう。

［設問２］公開かぎ証明書データに関する問題です。(1)は午前試験でも取り上げられる知識問題です。(2)は「証明書データの構成における設計上の問題」が問われています。過去の本試験で取り上げられたことがあるせいか，証明書の有効期間に着目した解答が多かったです。しかし，ここは証明書のデータの中身ではなく，構成が問題であるのでデータ項目に着目します。「公開かぎが含まれていない」などの解答もありましたが，X.509 フォーマットであり，6 か月間本番運用していますので，そのような基本的な欠落があるというのは妥当ではありません。(3)は再署名に関する問題です。この設問のように証明書データが変更になり再発行する場合の他に，署名した秘密かぎが無効になる，すなわち公開かぎ証明書が失効したり，有効期間を超過したりした場合には署名自体の有効性を確認できなくなります。署名の実効性を継続させたい場合には再署名（この問題では再承認）を行う必要があります。

［設問３］正答率が低かったです。電子政府などでも採用されている相互認証，ブリッジ認証という用語レベルでよいので押えておきましょう。

［設問４］企業で導入の進んでいるプライベート PKI システムについては，本試験でも自社でどのように設計するかというテーマで過去に出題されています。

【問2】

［設問１］無線 LAN に関連するセキュリティ技術の知識問題です。特に(a)(b)の正答率はかなり低くなりました。「無線 LAN 関連は用語が多く覚えるのが大変だ」という声をよく聞きますが, 新しいセキュリティ規格として IEEE802.11i を押さえ, その中で相手認証を行う IEEE802.1x, フレームの暗号化や改ざんの検出を行う TKIP と AES という大枠を押さえると覚えやすいです。

［設問２］(1)スナップショットの保存は，インシデント対応の作業の一つとして重要で過去の本試験でもたびたび登場しますが,「画面のハードコピー」のように十分理解できていない解答も目立ちました。スナップショットとは何か，その目的について解説で確認しておいてください。

(2)設問の論点は「影響範囲の特定」と「関係先への連絡」の順序であるのに，単に影響範囲の特定の目的などを述べた解答が目立ちました。設問のポイントとして対応手順の順序関係に留意して考察したいです。

［設問３］原因特定に含まれるような表現も目立ちました。少しでも原因特定に重なるような可能性のある解答は見直しが必要です。また「スナップショットの保存」はその前段階で行っていることですので，これも解答候補から外しながら考察します。

［設問４］(1)「盗聴されていないか確認する」は「電波が外に漏れていないかどうかの確認」と同じことになります。

(2)この設問には SU 試験特有の留意点があります。設問で「下線部に不十分な点がある」のように問われたときには,「これだけでは不十分で他にもいろいろやるべきことがある」とか「他の情報も伝えるべきだ」と考える前に，下線部の中での不具合点を検討することを優先します。書いていないことを検討するよりも，書いてあることでの問題点を優先します。そう考えないと解答が「何でも有り」になってしまいます。被害者が特定できない場合は，全ての被害者に直接連絡できない，という類似観点が過去の本試験でも出題されていますので正答率は高かったですが，問題の考え方として押さえておいてください。もちろん,「不十分」という設問の全てがこのパターンではなく，他にやるべきことを解答することもありますので，十分吟味することは必要です。

(3)正答率が高く，よく理解できているようでした。不正解だった方は MAC アドレスフィルタリングの脆弱性として押さえておいてください。

【問3】

［設問１］(1)(a)は知識問題でしたが正答率は高くなりました。(c)は論理的に考察すれば解答が決定できます。(2)(b)(d)(e)も問題文の情報を整理すれば解答を絞り込めます。設問２(1)の解答状況も合わせて分析しますと，ネットワークのやや踏み込んだ知識に関しては全般に弱いという印象を受けました。通常の DNS 問合せは UDP 通信であることから(b)は Web-2 と決定できます。

［設問２］(2)は正答率が高くなりました。ただし，理由を一つしか述べていないものもありましたので注意してください。

［設問３］正答率が高くなりました。アノマリ型の IDS にお

ける代表的な課題でしたが，理解できている受験者が多かったです。

［設問４］(1)はやや解答が分かれました。唯一絶対というわけではありませんが，解説の根拠を最も優先しました。(2)は「ping を通さない」という解答が目立ちました。間違いではありませんが，解説のように「プロトコルの観点から」という設問の指示事項も十分吟味する必要があります。

【問4】

［設問１］下線①では，「社員の利便性」のみや「一元管理による経費節減」に着目した解答も目立ちました。SU 試験ではまずはセキュリティの観点で考察したいです。過去の本試験でも，IC カードの貸し借りの問題は取り上げられています。下線②では「社員とその他を見分ける」という解答が目立ちました。重要な情報は下線部の後ろにあることも多いです。

［設問２］(1)正答率は高くありませんでした。間違えた方は解説で十分確認しておいてください。

(2)一般解の解答が目立ちました。一般解で多くの解答候補が想定できるときは，ヒントがないか確認する必要があります。設問で「取るべき対応」などとあるときに，ポリシや規定を確認するのは SU 試験では定石です。「同行する」という解答も多かったですが，ここは確実に「作業中同席」や「立会い」とポリシを踏まえて明確に表現したいです。

［設問３］(a)設問１の下線①の狙いで IC カードの重要性を意識させているにもかかわらず，同じ観点での解答が目立ちました。設問３の論点は，入退室管理とパソコン利用履歴管理の導入順序ですから，IC カードそのものだけでなく，入退室管理との関連で思考することが要求されています。

(b)「内部統制」など在室者管理の目的を表現している解答が目立ちました。解答を問題文に代入してレビューすると見直しできます。N 部長の発言では，［ b ］をすることで在室者管理が可能になるとなっています。したがって，解答の観点は在室者管理の手段になることが分かります。「内部統制をすると在室者管理ができる」では，手段と目的が逆になっています。

■午後Ⅰ採点基準

【記述文字数について】

記述文字数が少ないために，解答の要点を十分に表現できていないものは，内容によって部分点あるいは不正解としました。

【問1】

[設問1] (2)証明書データ，印影データは不正解としました。電子文書のメッセージダイジェストあるいはハッシュ値は部分点としました。

[設問2] (2)部署情報に着目した解答を正解としました。

(3)署名を証明する公開かぎ証明書が存在しなくなることに着目できている解答を正解としました。

[設問3] ポイントはアプリケーションレベルの統一ではなく，証明書の相互認証を実現するという観点です。証明書データの統一などは不正解としました。ブリッジ認証局の追加，統合認証局設置などは正解としました。

[設問4]（メリット）リスクが局所化できるといった観点は正解としました。（デメリット）外部から認証できないなどの拡張性に欠けるという観点は，設問３の方法で対応可能なため，運用負荷に着目するなど合理的な説明のあるものを部分点としました。コストに着目した解答は，なぜメリットになるか，あるいはなぜデメリットになるか合理的な説明を含むものは正解としました。

【問2】

[設問1] 解答のみを正解としました。

[設問2] (1)解答（解説含む）の観点のみを正解としました。

(2)解答の観点のみを正解としました。

[設問3] 事実の確認や影響範囲の特定の観点を正解としました。スナップショットの対象としてのログの保存の目的を表現した「証拠保全」などは不正解としました。

[設問4] (1)「外部から内部へ不正電波の検出」の観点も正解としました。

(2)理由を正しく記述した上で，追加措置の「メールの送信記録を調査して発信先に通知する」など合理性のあるものは正解としました。

(3)解答の観点のみを正解としました。

【問3】

[設問1] 解答のみを正解としました。

[設問2] (1)解答のみを正解としました。

(2)理由が一つしか述べられていないもの，あるいは明確に二つとして表現できていないものは部分点としました。「NAT 等で元の IP アドレスが隠蔽される」観点も妥当な表現は正解としました。

[設問3] しきい値設定の留意点が表現できていないものは不正解としました。

[設問4] (1)解答のみを正解としました。

(2)ICMP の制御に言及できているものを正解としました。

【問4】

[設問1] 解答の観点のみを正解としました。

[設問2] (1)解答のみを正解としました。

(2)図 2 に示されている解答の観点のみを正解としました。
[設問3] (a)解答の観点のみを正解としました。設問１下線①で紛失や貸し借りのリスクを解答せず，本設問で貸し借りリスクを解答した場合には部分点としました。
(b)「入退室の記録とパソコンの利用情報を関連付ける」などの観点も正解としました。「入退室履歴と社員情報の関連付け」などは部分点としました。

■午後Ⅱ講評

【問1】

ISMS の構築と運用に関して，人的資源のセキュリティ，資産の分類と管理，物理的および環境的セキュリティ，事業継続管理などの分野に関して, ISMS 管理策に関する知識と読解考察力，論理的思考能力を問う設問を出題しました。
［設問１］(a)の多くは人的セキュリティの観点をとらえていましたが, 的確に把握している解答は少なかったです。「人事」を含む解答も目立ちました。(b)，(c)は比較的良くできていましたが，勘違いと思われる解答も散見しましたので，間違えた受験者は一つ一つ丁寧に検証しながら解答することに留意してください。(d)も，ISMS 管理策の知識があれば，単に「(システム）障害対策」といった観点ではないことが判断できると思います。
［設問２］(1)は，問１の中では正答率が低くなりました。問題文および図１の情報資産の区分と営業部の運用を精査，検証することが必要です。問題点の可能性があっても，断定できない場合は，より確実な解答がないか問題文を再検討することが必要です。(2)の正答率は高くなりました。単にバックアップデータとなると取り扱いは様々ですが，サーバには機密情報がある，バックアップデータはサーバまるごと取得している，といった記述から論理的に解答が確定します。
［設問３］(1)はやや正答率が低くなりました。図 2 の規定には，詳細の手順が記載されていないため，項番④も含めて他の項番についても「詳細手順が不明だから十分に運用できない」という観点の解答が目立ちました。しかしながらこの観点で解答を検討しても項番が絞れません。このようなパターンのときは，あくまでも現状の規定に記載されている範囲で，何か運用上支障がないかと考える必要があります。多少時間がかかりますが，一つずつ検証していくことが求められています。(2)の正答率は高くなりました。ただし，媒体と出力帳票の取り扱いの相違点まで的確に把握できていた受験者は少数でした。結果的に得点できている受験者も，ここはもう一度問題文を確認しておいてください。
［設問４］(1)は入退室の記録漏れに対する施策が求められています。「営業部の担当者が確実にチェックする」といった解答も目立ちましたが，これはセキュリティ対策としては不十分です。運用体制が変更されていないという点で設問の指示に整合していませんし，現状と同じ仕組みで「ちゃんとやりましょう」は非常に弱い施策といえます。第三者のチェック，相互チェックといった観点も ISMS 管理策の基本です。問題文にもヒントがありますので活用したいです。(2)の正答率は高くありませんでした。ここも，明らかに不備があるのか，不備があるかもしれないものかを十分吟味する必要があります。
［設問５］(1)は「対象業務」に関しては設問の解釈が難しかったようです。妥当な解答は得点できています。解答は事業継続管理についての重要なポイントでもありますので，解説の内容も押さえておいてください。「訓練」はよくできていました。(2)は「データの喪失」という観点で保証ができないケースを求めていましたので，単に「停電」などは対象外としました。このような観点でも「長期の電源供給停止」といった解答をすると正解になりますので，問題文との整合性を維持する配慮も確実に得点するために必要です。RAID5 に踏み込んだ解答の場合，かえって技術的に間違った内容があると不正解になりますので，踏み込む場合は正確性に留意してください。

【問2】

［設問１］個人情報保護法の知識をベースとした問題です。個人情報取扱事業者の義務については一通り確認・理解しておきたいです。
［設問２］リスクのスコア計算で，正答率は低かったです。ただし，合格率程度の正答率だと推定されることから考えると，合格者レベルはこのくらい丁寧に解答作業が行えるレベルだともいえます。解説に詳細な説明がありますので，じっくり確認しておいてください。基本的なリスク評価の手法の考え方を理解しているのは前提であり，さらに問題文中の条件を論理的に対象スコアに投影していく作業が求められています。
［設問３］(1)①はバックアップ方式に着目した解答やシステム全体の可用性に着目した解答などが目立ちました。この問題では差分バックアップを毎日取得して毎翌朝 C 社にも預けているので，バックアップ方式には直接的な問題点はありません。また，後者の解答は「バックアップデータの可用性」という設問中のポイントを見落としていると思われます。設問文に基づき解答を作成するという基本姿勢に留意してください。(1)②の Web サーバの脅威の人為的ミスが 2（中程度）の理由は，観点が分かれました。なぜ中程度のリスクがあるかという観点と，なぜ中程度しかないかという観点です。出題者の観点は前者でした。確かに後者の観点が全く間違いとも言い切れませんが，人為的な作業に関する具体的な問題文

中の記述を探すと，パッチ作業の問題点は抽出できます。切替作業の自動化は人為的作業ではないので，人為的作業がないからリスクが中程度しかないのか，問題のある人為的作業があるので中程度のリスクがあるのかの観点を比較した場合，後者の方が確実性が高いといえます。(2)はリスク調整の観点が表現できていれば多くは正解になっていました。

［設問４］(1)は設問２が正解ならばほぼ正解になったはずです。設問２が正解にもかかわらず，ここが不正解の場合は設問の解釈違いが想定されるので確認しておきましょう。ここも「脆弱性のコントロールでリスクを低減できる」ものを慎重に選択していくと，8 と 10 に絞られるので，そこまで丁寧に作業できた受験者は高得点を得ています。問１は，設問２，４において解説にあるような作業を論理的に進める必要があり，全体としてはこの部分の正答率がかなり低くなりました。このような問題でも落ち着いてじっくり取り組むという心構えをあらかじめ持っておきたいです。(4)は問２の中では得点源の問題といえます。(3)までで力尽きて（時間を費やしてしまい？）解答なしの答案も見られました。リスクのスコア計算がうまくいかなくても，この設問４(4)や設問５，設問１などで合格点を確保できるはずです。あきらめないで最後まで取り組んでください。この設問では「情報資産別」を適切にとらえられれば，満点あるいはスコア計算を間違っても 24 点の得点が十分期待できます。

［設問５］は「リスク対応計画」のとらえ方が分かれました。問題文の流れから出題者は ISMS の再構築とスタートというやや高い視点にいるということを読み取ってほしいです。解答の内容は情報セキュリティアドミニストレータの業務の基本的な内容なので，本試験に向けて押さえておきたいです。

■午後Ⅱ採点基準

【記述文字数について】

記述文字数が少ないために，解答の要点を十分に表現できていないものは，内容によって部分点あるいは不正解としました。

【問1】

[設問1] (a)は「人的管理」など同義のものを正解としました。「人的」は部分点としました。(b）は「履歴」「身元」など妥当なものを正解としました。(c)「変更」は部分点としました。(d）は「緊急事態計画」も正解としました。その他は解答および同義語のみを正解としました。「復旧対策」は部分点としました。「バックアップ」「リカバリ」などは不正解としました。

[設問2] 解答の観点のみを正解としました。

[設問3] (1)条項番号は「4」のみを正解としました。「廃棄委託業者との秘密保持契約が明示されていない」という観点は「安全に処分」に包含されると解釈できるので不正解としました。(2)リスクとして「情報機器や媒体からの情報漏えい」のみは不正解としました。

[設問4] (1)「入退室管理システムの導入」など運用体制という観点の含まれないものは不正解としました。

(2)解答のような具体的表現ができているもののみを正解としました。

[設問5] (1)対象業務では「システムの復旧作業」など行うべき業務を取り上げた妥当性のあるものも正解としました。その他「体制整備」など妥当性のあるものは正解としました。訓練は「事業継続」に関する訓練の必要性を表現できているものを正解としました。

【問2】

[設問 1] 個人情報保護法，JIS Q 15001 に準じた内容のみを正解としました。「情報主体への対応窓口の設置」，「個人情報保護方針の公表」など妥当なものは正解としました。

[設問2] 解答のみを正解としました。

[設問3] (1)①単に「フルバックアップが 1 週間毎, 差分が毎日」という観点は不正解としました。

②セキュリティパッチに着目して妥当性のあるものを正解としました。「パッチの適用がめったにない」のような観点は不正解にしました。

(2)人間による判断が必要な状況を表現できているものは，内容によって正解または部分点としました。

[設問4]

(1)対象外のものを解答した場合はその分マイナスしました。

(2)リスク番号「8」のみを正解としました。

(3)リスク番号「10」のみを正解としました。リスク移転の具体的方法が表現できていないものは不正解としました。「逸失利益」が的確に表現できていないものは部分点にしました。

(4)対象とする情報資産は「デスクトップパソコン」「ノートパソコン」「顧客台帳」で，それぞれ一つずつで妥当性のあるものを正解としました。例えば「顧客台帳」に関して二つの解答を記述した場合は一つ分として採点しました。ダウンロードしたデータ（顧客情報）に着目したものも妥当なものは正解としました。

[設問5] 解説にあるように，情報セキュリティポリシや適用宣言書など ISMS 文書の改訂，詳細運用規程の策定，経営陣の承認，全社員への周知徹底と教育の四つの観点で満点としました。観点が不足する場合は，一つにつきマイナス 4 点としました。その他の観点として「外部委託の準備」など妥当な具体策は一つ 4 点としてプラスしました。

以上