2008 秋 情報セキュリティアドミニストレータ 全国統一公開模試 講評と採点基準

2008 年 9 月 25 日 (株)アイテック

■全体講評

過去問題演習や専門知識学習の準備が進んでいることが伝わる答案と，まだ不十分な答案とに二極化していると感じます。また，今年が情報セキュリティアドミニストレータ試験の最終回であることの影響か，実務で ISMS に携わっているのではないかと感じさせる，しっかりした答案が多いことも特徴的です。

午後Ⅰ問 1 のウイルス対策の設問 2 や設問 3，午後Ⅰ問 4 のネットワークセキュリティ対策の設問 2 や設問 3 など，過去問題にも類題があります。残された時間はわずかながら，過去問題の学習が不十分な方は集中的に消化することで得点力アップが期待できます。

また問題文のヒントの見落しや設問に正しく答えていない解答も目立ちます。問題文や設問に基づいて解答するという当たり前のことを的確に進めることに十分留意してください。

■午後Ⅰ採点基準

【問1】 ウイルス対策

[設問1]

解答例のみを正解としました。

[設問2]

「ファイル交換ソフトをインストールしない」などのように解答例と同様の観点のみを正解としました。

[設問3]

サーバ名は，Web プロキシサーバのみを正解としました。内容は，コンテンツフィルタリングの観点を表現できているものを正解にしました。URL への接続コントロールと異なる観点の対策は不正解としました。機能（目的）があっていても，技術的な仕組みの説明が不十分なものは部分点としました。メール内の URL のチェック機能は部分点としました。IPS は本文にすでに記述されているので不正解としました。

[設問4]

「検疫システム」「検疫ネットワーク」などの技術用語を用いずに，社内ネットワーク接続後に PC のセキュリティ状況をチェックする仕組みを表現したものは部分点としました。技術的対策としての説明が不十分なものは，内容によって部分点または不正解としました。「新種のウイルスに感染する場合でも～」という文脈から，ノート PC 自身によるパターンファイル更新の仕組みは不正解としました。ノート PC の利用が前提なのでシンクライアントシステムは不正解としました。

【問2】 情報セキュリティ監査

[設問1]

(a)解答例のみを正解としました。

(b)「影響範囲」は正解としました。「対応費用」などは不正解としました。

(c)解答例のみを正解としました。

(d)「インフラ」は正解としました。

(e)「責任者」は部分点としました。

[設問2]

第三者監査が望ましいという観点が表現できているものを正解としました。「第三者＋客観性」や「独立性」を正解とし，「客観性」のみは不正解としました。

[設問3]

(1)「各部署からの依頼に基づく管理で，その妥当性の検証が不十分」という観点など，合理性のある内容は解答例以外にも正解としました。N 部長 1 人が担当している現状に対して，職務分離ではなく，迅速な運用ができないという観点は部分点としました。

(2)プレースホルダの利用はバインド機構に含まれるので不正解としました。入力チェックのみは部分点としました。

(3)「PC を 1 人 1 台にして PC 属性で管理する」という観点は，システム構成上の前提が必要になるため不正解としました。「生体認証の導入」などの新たなセキュリティソリューションの導入は不正解としました。

【問3】 個人情報保護対策

[設問1]

解答例のみを正解としました。(c)で「目的」，(d)で「委託先評価基準」など，解答例と同様なものは正解としました。(d)で単に「社内基準」は不正解としました。

[設問2]

問題点を説明せずに解決策のみを記述したものは不正解としました。解答例以外にも，規定の項番 2 の「部署ごとの PC 管理台帳の管理」について「全社管理が不十分」などのように，妥当な問題点を指摘できているものについては，内容により部分点としました。

[設問3]

(1)～(3)解答例の観点のみ正解としました。

[設問4]

持出し PC 紛失時の報告ルール追加など，問題文の記述に整合するものは内容によって正解または部分点としました。

【問4】 ネットワークセキュリティ対策

[設問1]

解答例のみを正解としました。

[設問2]

(1)解答例の観点のみを正解としました。「経営層へ報告」は不正解としました。

(2)解答例の観点のみを正解としました。

[設問3]

時刻同期の観点のみを正解としました。導入するサーバ名（NTP サーバ等）の表現されていないものは不正解としました。

[設問4]

解答例の観点のみを正解としました。表現不足なものは部分点としました。

■午後Ⅰ講評

【問1】

[設問1]

DDoS 攻撃を DoS 攻撃と間違う例が多数見られました。問題文の記述から確実に解答してください。ワームやトロイの木馬，ボットなどのキーワードもしっかり理解しておきたいです。

[設問2]

「追加すべき点」とあるのに，既存の規定を修正する解答が見られました。設問を十分読んでください。下線①の前の「今回の事件の直接の原因となっていないものも含めて」などのヒントも考慮して，明らかに追加すべき内容を吟味して特定することを心掛けてください。「メール内の URL クリック禁止」という解答も見られましたが，これは項番 2 の「Web 利用の規定」に重なります。

「FW で HTTP をパケットフィルタリングする」といった明らかに間違った解答もありましたので注意してください。受動型攻撃では，日常的に利用する HTTP などを介してウイルスに感染するリスクが高まっています。

[設問3]

「技術的対策」が要求されていますので，単に本文を復唱して「有害サイトにアクセスさせない」という目的だけではなく，「コンテンツフィルタリング」などのキーワードを使うことで，技術的なポイントが分かっていることを解答文で表現するようにするとよいでしょう。

[設問4]

この設問では「パターンファイルの更新が省略されてしまう」という前提を踏まえた技術的対策を要求しています。PC だけの対策の解答も多く見られました。PC が感染しても社内ネットワークを安全にする仕組みが必要です。パーソナル FW，監視エージェント（自己チェック）などは PC に依存する仕組みですので，検疫ネットワークのように PC から見て第三者がチェックする方がセキュアであるという観点も重要です。IPS などは将来導入と書かれています。

【問2】

[設問1]

正答率は低かったです。(a)～(c)は基本用語ですので，間違えた方は十分確認しておきましょう。

[設問2]

情報セキュリティ監査における独立性と客観性を理解しておきましょう。この設問のポイントは外観上の独立性で，被監査主体と利害関係のない第三者であることが求められます。公正かつ客観的に監査判断を行うのは精神上の独立性と呼ばれています。

[設問3]

(1)問題文に書かれていない前提に基づく解答も散見されました。問題文に書いてあることを基に解答をつくることに十分留意してください。

(2)セキュアプログラミングの正確な知識が必要な問題です。誤りの例として，クライアント側の入力チェック（不正な HTTP メッセージを直接送信できるのでサーバ側での対応が必要），SSL の利用（復号された HTTP メッセージのデータから SQL 文を構築する）などが見られました。

(3)ISMS の運用では記録が重要なことを理解しておきましょう。

【問3】

[設問1]

正答率は高いとはいえません。十分確認しておきましょう。

[設問2]

問題点を要求されているのに，解決策のみを表現しているものが非常に多くありました。項番 1 で「自動更新」に対し「手動更新が好ましい」という観点がありましたが，一概には言い切れません。

[設問3]

(1)「二次被害防止」というキーポイントに着眼することがポイントです。

[設問4]

従来から必要だった規定ではなく，文脈にそった新たに必要となる規定を考察すべきです。下線①の前に書いてある，紛失時の報告や部門共有のノート PC の運用に関する規定を考えます。

【問4】

［設問1］

全般的に好調でした。午前問題でも登場する専門用語が多いです。間違えた方は十分確認しておいてください。

［設問2］

(1)ヒントを的確に使うことを確認してください。

(2)スナップショットの目的を誤って理解している解答も目立ちます。スナップショットは単なるバックアップではなく，証拠保全が目的であることを理解してください。

［設問3］

サーバ名がない解答が目立ちました。

［設問4］

「他にもこのようなことが必要だ」という観点ではなく，書かれている(1)～(3)の中の問題点を抽出することを優先させてください。この解答アプローチは本試験でも同様です。ログ保存サーバの設置場所が不適切という観点も目立ちましたが，DMZ ではなく社内 LAN に設置する図 1 が妥当です。

■午後Ⅱ採点基準

【問1】 システムの安全・信頼性対策

［設問1］

解答例のみを正解としました。

［設問2］

(1)増分バックアップの特徴を踏まえた内容を正解としました。フルバックアップのリストアが明示的に表現されていないなど不十分なものは内容によって部分点にしました。増分バックアップと差分バックアップを混同している内容は不正解としました。

(2)解答例のみを正解としました。

(3)解答例のみを正解としました。

［設問3］

(1)キュー上の未送信データを具体的に言及したものを正解としました。単にタイムラグがあるという観点は部分点としました。

(2)ユーザ企業の観点から応答性能に着目できている解答を正解としました。「SaaS システム」などの字句は必須要件ではありません。

［設問4］

(1)解答例のみを正解としました。

(2)TCP/UDP ヘッダのチェックサムの変換の観点に着目した解答を正解としました。

［設問5］

(1)DNS のキャッシュの観点に着目したものを正解としました。

(2)DNS の構成としてセカンダリ DNS の設置場所に言及しているものを正解としました。

［設問6］

利用者のアクセス認証方法に着目できている解答例の観点のみ正解としました。パターン 1 以外に着目したものは不正解としました。

【問2】 企業の情報セキュリティ対策

［設問1］

(1)解答例のみを正解としました。

(2)解答例の観点のみを正解としました。

［設問2］

(4)⑤「従業員（あるいは部外者）を即座に判断できるようにできる」などの表現も正解としました。単に「不審者の侵入防止」は部分点としました。

(5)①個人を特定するという観点を正解としました。

［設問3］

解答例の観点のみを正解としました。「執務室の出入口が施錠されていない」は，「現状のまま常時施錠せずにいこう」という本文中の発言があるので施錠可能と判断できるので不正解としました。

［設問4］

(1)社員証や USB メモリを活用して離席時に自動的にログオフする仕組みは，「現在実施している対策に加える」必要がなくなるので不正解としました。

(2)ノート PC の社外持出し手続きに着目した解答例の観点のみを正解としました。手続き以外の PC に対するリスクに着目したものは不正解としました。

(3)単に「自動出力させない」のように，出力時の本人確認が明示されていないものは内容によって部分点または不正解としました。

［設問5］

(1)W 社外の派遣先を対象とする規定が欠落している点に着目できて妥当なものを正解としました。B 社から預かる情報の取扱いに着目したものは，現行ポリシでも対応可能であること，派遣案件であること，解答例の観点は明らかに見直し必要な大きな点であることから不正解としました。責任者が明確でないなど，見直しではなく，単にポリシに明記されていないことを指摘したものは不正解としました。

(2)雇用関係に着目できている解答例の観点を正解としました。また，B 社の委託先選定基準をもとに，W 社が派遣社員と誓約書を結ぶ必要があるという主旨も正解としました。その他，B 社の選定基準の主旨に基づく妥当なものを正解としました。

■午後Ⅱ講評

問 1 はテクニカルな問題を含む情報セキュリティアドミニストレータ試験としては新傾向問題です。ネットワークエンジニアや情報セキュリティエンジニアの学習経験がない受験者は，問 2 を選択するほうが賢明だったと思われます。

【問1】

［設問1］

正答率は高かったです。

［設問2］

(1)正答率は高かったです。問題文にも説明がありますが，増分バックアップの特徴を理解できていない解答もありましたので，十分確認しておいてください。

(2)このような計算問題は，後回しでもよいので，じっくり時間をかけて丁寧に取組むとよいでしょう。

［設問3］

(1)単に「同期が取れていない」という説明だけではなく，同期式と非同期式の同期方法の違いも含めて説明するように留意してください。問題文中のキーワードを引用するという解答の作り方は，過去問題でも頻繁に見られます。

［設問4］

(2)技術的な問題のためか正答率は低くなりました。トンネルモードでは，カプセル化する IP パケットの中身を書き換えずに，ESP ヘッダとトンネルヘッダを付加するので，TCP ヘッダチェックサムの認証が正しく行えます。また，ESP の認証データもカプセル化する IP パケットが認証の対象範囲なので，メッセージ認証も正しく行えます。「TCP ヘッダ内の IP アドレス」という表現も多く見られました。TCP ヘッダには IP アドレスは含まれません。

［設問5］

(1)ネットワーク技術の知識が必要なテクニカルな問題です。サーバの移行時に DNS の情報を変更しても，アクセスするホストによる名前解決にはタイムラグが発生することを理解しておきましょう。「ブラウザにキャッシュされている」という解答も多く見られましたが，下線⑥の前の部分は，DNS サーバの設定変更がテーマになっていますので，適切ではありません。

(2)DNS の「構成」が設問のポイントです。どのように変更依頼すべきかが要求されているのに，問題点のみを表現した解答もありました。設問を十分把握するように留意してください。プライマリ DNS サーバとセカンダリ DNS サーバを物理的に別の場所に置くことは信頼性向上の定石の一つです。

［設問6］

「ガイドラインの要求事項の観点から」という設問の指示事項を見落としている解答も目立ちました。見落としがなければ，解答しやすい問題だったはずです。設問の指示事項には十分留意してください。

【問2】

［設問1］

(2)(b)内部監査などに着眼した解答がありました。代表的な人的セキュリティの管理策としての教育訓練を押さえておきましょう。

［設問2］

(4)⑤「着用する」ことによって「判別しやすくなる」ことがポイントです。ポイントをしっかり表現することに留意してください。着用するのは従業員なのに，外来者も含めた内容のものも見られました。

(5)①共有 ID 禁止の目的で「アクセス権の適切な付与」の観点がありました。本試験でも出題された内容ですが，第一の目的としては「行為者の特定」と押さえて下さい。「アクセス権の適切な付与」や「1 人が退職などした際にパスワードを変更する必要がある」などは第二の目的と考えて下さい。

［設問3］

問題文の説明から明らかにポリシ違反と判断できる点を抽出するまで探すようにしてください。

［設問4］

(1)下線①の前の「現在実施している対策に加えて」の条件に合致しない解答が見られました。

(2)単にノート PC 内の情報漏えいリスクなどに着眼した解答もありましたが，文脈では手続きのあいまいさが論点になっています。設問の対象になっている下線部の前後の文脈を的確に把握することに留意してください。

(3)「印刷せずにデータとして扱う」などは一つのアイデアですが，そのように印刷を一切制限する施策は業務の制限につながるので，現実に可能かどうかを検討する必要があります。できるだけ現状業務に影響を与えない施策を提案することを目指してください。「メールで通知する」は「一方的な送信時」には宛て名不在時に解決策になりません。

［設問5］

(1)セキュリティポリシに書いていない点を指摘する解答も目立ちましたが，書いてあることで大きな見直しが必要なことを優先してください。また，設問 5 のテーマを踏まえて外部委託に関連した内容表現にすべきです。問題点が要求されていますが，解決策の解答も散見されました。

(2)一般的な内容に飛躍せずに，問題文の記述や B 社の委託先選定基準に基づいた内容になるように留意してください。

以上