平成15年度秋 情報セキュリティアドミニストレータ試験分析と講評

■ 全体講評

情報セキュリティアドミニストレータ試験は，平成13年秋から新たに設置された試験区分で，今年で3回目の試験となります。情報システムの企画，計画，構築，運用というシステムライフサイクルにおいて，対象者として情報セキュリティに関する企画，実施，運用，分析，見直しに関する業務に従事する人材像が想定され，出題内容も試験センターの出題範囲と「情報処理技術者スキル標準」（以下，スキル標準）の内容に沿って出題されます。

平成15年度の情報セキュリティアドミニストレータ試験の出題傾向としては，試験範囲とスキル標準を踏襲した形になっています。3回の本試験を経たことで全体の傾向がほぼ定着してきたと思います。昨年度はマネジメント系の問題が中心でしたが，本年度はむしろ平成13年度の出題傾向に近く，テクニカル系の設問が複数ありました。また，昨年度重視されたセキュリティ監査（システム監査）関連については，情報セキュリティ監査制度の告示施行に伴う経産省研究会報告書の「情報セキュリティ監査に関するスキルを加味するのが適当」との提言があったものの特に考慮されなかったと見られます。

午前問題は，昨年と同様，他の区分（システム監査，ネットワーク，基本情報ほか）で過去に出題された問題または類似問題の出題率が大変高く，他の区分の過去問題を十分に演習した受験者にはやさしく感じられたものと思います。さらに，H13年度の再出題が4題，同一知識内容を問う問題が4題ありました。また，セキュリティ分野からの出題は50問中13問と昨年度とほぼ同じ比率で出題されています。

午後Ⅰは大きく分けて，ISO17799/JISX5080中心のセキュリティポリシ分野，物理的セキュリティ対策分野，JISQ15001中心の個人情報保護対策分野，モバイルインターネットのセキュリティ対策分野がテーマとして取り上げられました。特にテクニカル系のみという問題はなく，基本はセキュリティマネジメントに関するものであり，その中で技術的な対策を問う設問が含まれるものがいくつかありました。物理的セキュリティは，これまでは踏み込んだ出題がありませんでしたが，ISMSの構築と運用という実務分野ではたいへん重要かつ必須な部分であり，インターネットセキュリティと同等にようやく取り上げられました。午後Ⅰの試験では，90分の時間内に3問を選択して解く必要があり，時間的には非常に厳しいのですが，極端に時間のかかる問題はなく適切な問題文のボリュームではなかったかと思います。なお，問題選択の参考になっていた，問題冊子の始めの[設問内容一覧]がなくなりましたので，選択に時間を要した受験生もいたかもしれません。

午後Ⅱに関しても，どちらかと言うと平成13年度の出題傾向に近く，テクニカル系とマネジメント系から1問づつ出題となりますが，テクニカル系の問1についても，事故対応フェーズにおけるISMSの運用に関するマネジメントの設問のウェイトが高くなっています。情報セキュリティアドミニストレータの人材像から言えば，あくまでマネジメント系を中心スキルとして，情報セキュリティ管理責任者として必要な技術的知識を補っていくというスタンスには変わりないと思います。

まとめると，午前問題は新作問題で難易度の高い問題も数問ありましたが，全体として他の試験区分も含めた過去問題からの出題が多く，受験対策を行った方にはやさしかったと思われます。逆に午後問題だけに焦点をあて，午前問題の対策を行わなかった方にはかなり難しかったと思われます。午後Ⅰ問題は，情報セキュリティアドミニストレータとしてはほぼ順当な試験問題でしたが，問1の「JISX5080の管理策に基づいて」や問3の「JISQ15001に基づいて」という設問の指定事項があり，昨年度以上にこれらの規格を十分学習したかどうかで差がでる点がひとつの特徴でした。また，問題文からは解答が一意に導けない設問もあり，解答そのものも解釈が分かれるものもありました。午後Ⅱ問題は，事前の予想通りテクニカル系への若干の揺り戻しがあったと言えますが，全般としてはマネジメント中心にテクニカルな要素が含まれるか，ほとんど含まれないかということなので，バランスのとれた学習が今後も必要です。午後Ⅰ（4問中3問選択／90分）と午後Ⅱ（2問中1問選択／90分）は，問題の難易度から考えても妥当であったと思います。

年 度	応募者数	受験者数	合格者数(合格率)
平成13年	23,778	15,988	2,111(13.2%)
平成14年	34,352	22,235	2,788(12.5%)
平成15年	42,417	28,082	?

応募者数，受験者数の試験センターからの速報数字は上記のとおりです。全試験区分の応募者，受験者数がほぼ一定の中で，群を抜いての増加傾向が続き，ネットワークの受験者数に近づいてきました。受験率(66.2%)の高さは，他の旧高度区分（システムアナリスト，アプリケーションほか）に比べて4～10%高い数字で，基本情報処理技術者の受験率より5%低い水準です。

■ 午前講評

全体的にこれまで情報セキュリティアドミニストレータを含む他の区分（システム監査，ネットワーク，基本情報など）において過去に出題された問題が約半数もあり，全く同じ，または一部変更（用語や数値など）した問題がかなりの部分を占めています。他区分の過去問題の演習がそのまま得点に結びつく形となっています。

その中で，少し目新しい問題についてピックアップしてみます。

問25のシングルサインオン関する問題は，クッキーやリバースプロキシという専門用語と組み合わせて出題されたので，難易度が高くなりました。クッキーについて日常のパソコンのセキュリティ対

策でなじみがあり，シングルサインオンの基本的な考え方を理解していれば，消去法でも正解を導けたと思います。問 28 のクロスサイトスクリプティングは午後問題でも取り上げられました。昨年かなり話題になりながら出題されませんでしたが，本年の出題となりました。代表的な不正アクセスや攻撃の概要を学習していれば正答できたと思います。問 29 は，問 25 とも関連しますがクッキーをテーマにした出題でした。ブラウザ等でクッキーの扱いをどのように設定するかは日常的なことであるので，そのような経験があれば容易であったと思います。問36のSAMLは比較的新しい規格なので初めて目にした受験生も多かったと思います。情報セキュリティは技術革新のスピードが速い分野ですので，スキル標準とは別に，最新（試験半年程度前まで）の動向をキャッチし，概要を理解しておくようにしなければなりません。

基本的に「スキル標準」を前提とした情報セキュリティアドミニストレータ試験として実施されましたが，以上の結果を見る限り，システム監査や上級シスアド，ネットワークの過去問題からの出題という傾向が強く，ほぼ昨年度と同様の傾向が続いています。午前問題については他区分の過去問題の研究が非常に有効な対策といえそうです。

スキル標準の分野別出題傾向をまとめてみます。情報セキュリティアドミニストレータの必要な知識体系は，

① IT 共通知識体系

② 情報セキュリティアドミニストレータ実務知識体系･コア知識体系

の2種類からなります。情報セキュリティアドミニストレータ試験においては，IT 共通知識体系の分野のうち，下表に示す分野で技術レベルが問われることになります。下表は，IT 共通知識体系の該当分野における今回の試験の出題傾向を分類した表になります。

IT 共通知識体系	分野	H13 年度	H14 年度	H15年度
II	コンピュータシステム（レベルII）	9	4	8
III	システムの開発と運用（レベルI）	4	6	6
IV	ネットワーク技術（レベルII）	8	10	9
V	データベース技術（範囲外）	2	0	0
VI	セキュリティ（レベルIII）	12	12	13
VII	標準化（レベルIII）	1	3	1
VIII	情報化と経営（レベルII）	9	11	10
IX	監査（レベルII）	5	4	3
合計		50	50	50

■ 午後 I 講評

全４問中３問を 90 分で解答するということで，いかにすばやく受験者の得意分野の問題，あるいはより解答を導きやすい問題を選ぶかが，合否に大きく影響してきます。問題冊子の冒頭の[設問内容一覧]がなくなりましたので，設問文をながめて選択問題を決めてしまってもよいでしょう。また午後Ｉは，問題のボリュームに比べ試験時間が短いため，効率的な時間配分と集中力がポイントになります。

問題の出題分野は大きく分けて，セキュリティポリシ分野，物理的セキュリティ対策分野，個人情報保護対策分野，モバイルインターネットのセキュリティ対策分野がテーマとして取り上げられました。情報セキュリティアドミニストレータの知識水準を問う問題としては，非常に適切な内容といえるでしょう。昨年度まで2年連続で出題されてきた，PKI関連分野，リスク分析分野は出題されませんでした。入退室･入退館管理は昨年度も午後Ⅱで出題されていますが，物理的セキュリティに特化した出題があったことで，ISMSのマネジメント領域がほぼ網羅的に一巡したと言えます。また，昨年度まで出題のあった計算問題が今年は出題されませんでした。

マネジメント系の問題では，JISX5080（ISO17799）やJISQ15001 を前提とした問題が目立ち，問題文から解答を導くだけではなく，規格に関する相応の知識が要求されてきています。全般に設問の趣旨を的確に理解することが重要で，出題者の意図や問題文に書かれた状況を読み違えると，まったく的外れの解答をしてしまう危険性もあるので，受験者にとっては注意が必要です。

次に，各問題について簡単に見ていきます。

問1 情報セキュリティポリシに基づくセキュリティ対策

JISX5080（ISO17799）をベースにしたセキュリティポリシの策定とセキュリティマネジメントシステムの運用に関する問題です。設問2ではJISX5080 のセキュリティ管理策の内容を理解している必要があり，また設問3は同じくJISX5080 のうち人的セキュリティの管理策について内容を理解している必要がありますので，この設問の条件指定の分やや難しくなったと思います。特に設問2は判断に迷った受験生も多かったと思われます。

問2 物理的セキュリティの確保

JISX5080（ISO17799）では「物理的･環境的セキュリティ」と位置付けているマネジメント領域に関する問題です。情報セキュリティアドミニストレータの試験制度が外部からの不正アクセスなどインターネットセキュリティ事故を契機に誕生した経緯もあり，これまでは踏み込んで出題されませんでしたが，実務レベルでは技術的セキュリティと同等に重要な当該分野がようやく出題されました。問題文と設問をていねいに読めばとくに難易度の高い設問はなかったと思います。

問3 企業グループ内の顧客情報の活用

企業グループにおけるポイントサービスや販促事業における個人情報（顧客情報）の取扱いに関する問題です。テーマが個人情報保護に特化しているので，JISQ15001 も含めて当該分野をよ

く学習した受験生には取り組みやすかったと思います。特に，設問4はＪＩＳQ15001に基づいての解答が要求されていますので，一般的な表現では得点できないでしょう。設問2と設問4が若干似たような観点になっていますので，設問ごとの出題者の要求内容を的確に捉えて解答することが必要で，その点でやや難しかったと思います。

問4　営業支援システムの機能追加

定番テーマであるリモートアクセス，モバイルコンピューティングに関する問題です。昨年度までは公衆回線経由のリモートアクセスでしたが，今年はインターネット経由の接続に変わりました。今後はこのシステム構成が主となるでしょう。設問3はファイアウォールのルールベースに関するテクニカルな問題ですが，類似の過去問題を学習していれば正答できたと思います。設問2，設問4は内容としては特に難易度の高いものではありませんが，限られた時間で問題文と設問を的確に理解して記述文を作成する訓練が不十分だと時間不足になったのではないかと思われます。

■　午後Ⅱ講評

全2問中1問を 90 分で解答する形式ですが，問題文のボリュームが午後Ⅰに比べ大きく（1 問あたり8ページ）やはりどちらの問題を選択するかで，合否に大きく影響してきます。一度選択し，問題に取り組み始めたあとで，他方の問題に切り替えるというのは，時間的なロスが大きいためできれば避けたいものです。午後Ⅱも午後Ⅰ同様に効率的な時間配分と集中力，そして問題文を適切に解釈する読解力が必要となってきます。

今回の問題は［設問内容一覧］がなくなったため，どちらかの問題を選択するかでまず悩むケースが多かったのではないかと思います。両方とも始めのほうにネットワーク構成図が示され，問題文の用語を眺めると特に問1でテクニカルなものが目立ちます。一方設問を確認すると，どちらかと言うとマネジメント系の内容に読めます。問1はセキュリティ事件に絞った内容ですので，テクニカル系が得意か，セキュリティインシデント対応分野が得意な受験生が選択したのではないかと思います。マネジメント系が得意な受験生は問2を選択したと思います。

次に各問題について見ていきます。

問1　セキュリティ事件への対応

問題文の前半は，ネットワーク機器を中心としたシステム設定やクロスサイトスクリプティングやバッファオーバフローの脆弱性に関する記述などテクニカルな内容です。後半は，セキュリティ事故への対応で，セキュリティマネジメントプロセスの1フェーズに焦点を当てています。設問1の穴埋め問題は選択肢が提示されていますが，やや専門的です。残りの設問はいずれもセキュリティ事故対応がテーマで，例えば設問2と設問4がいずれも影響範囲の特定に関連する出題，設問2と設問5が「本来どうすべきであったか？」という観点の出題で，一見同質の設問に見えた受験生もいたのではないかと思います。各設問で出題者が要求していることを十分整理してから解答をする必要があり，慎重さが必要だったと思います。結果的にはテクニカルのみの設問ではなく，セキュリティ事故に関連するマネジメントプロセスの理解を問う問題です。

問2　企業情報ネットワークの構築におけるセキュリティ対策

ＩＰ－ＶＰＮを利用した新ネットワークシステム導入を題材としたＩＳＭＳの運用に関する問題です。問題文が読みやすく，また，設問が取り上げているテーマがパスワードの運用，情報資産の管理項目，コンテンツフィルタリング，外注した新システムの受入れ導入時の留意点，派遣社員活用時の留意点，などと多岐にわたるのですが，それぞれの設問の独立性が高いのと，設問の要求事項が明快なので実質的に解答を考える時間が多くとれたのではないかと思います。セキュリティマネジメントの幅広い知識や考え方が要求される反面，ひとつのテーマがわからなくても他の設問に影響しにくいと思います。

■　平成 16 年度の試験に向けて

まず午前試験に関しては，今年の情報セキュリティアドミニストレータ試験の問題もそうですが，情報セキュリティアドミニストレータを含めて他の試験区分の過去問題に習熟することが高得点に結びつく近道といえます。特にネットワーク，システム監査，基本情報（旧第二種）の過去問題が有効でしょう。過去問題の中には繰返し出題されているものが多く，頻出問題を研究した問題集等を用いて学習するのが効果的です。そして，解答が導けるだけでなく，すべての選択肢の内容を理解するようにして，知識の幅を広げるのがよいでしょう。

午後Ⅰと午後Ⅱは，今年度の試験を見る限り，特に分けて対策を考える必要はなさそうです。まず，セキュリティアドミニストレータとして押さえるべき知識を網羅し，実際のケースを想定した応用力を養っておくことが重要です。また，試験時間が非常に限られているため，予想問題集などを用いて，問題解法のプロセスや要領をつかみ，時間内に解く感覚をつかんでおくことが必要でしょう。最初の方の設問は，穴埋めの問題が多く出題されることが予想されるため，セキュリティに関するキーワードを理解し，正確に書けるようにしておくことが重要です。また，多くの設問では問題文や図表の中に，解答や解答のためのヒントが書かれていることが多いので，注意して問題文を読み，読解力を鍛えておくことが有効でしょう。

昨年度までは，プライバシーマーク制度に関する出題が目立ちました。今年は JIPDEC の運用するＩＳＭＳ適合性評価制度やプライバシーマーク制度そのものに関する出題は見られませんでしたが，制度の準拠対象である「ISMS 認証基準」の詳細管理策の基になっているＪＩＳＸ5080（ISO17799）や，JISQ15001 について一歩踏み込んだ出題がありました。今後も両制度の概要理解とともに，これらの規格を核としたＩＳＭＳと個人情報保護に関するコンプライアンスプログラムの構築と運用のより実践的なスキル習得と，セキュリティシステムの設計・導入・運用に必要なセキュリティ技術を中心に学習を行っていくのが基本的な方針になります。