目　　次

＜出題分析＞

3．出題範囲と試験の概要

3-1　システム監査技術者試験の対象者像

システム監査技術者の対象者像は，情報処理技術者試験センターの「情報処理技術者試験　出題範囲」の中で次のように規定されています。
業務と役割，期待する技術水準，レベル対応も示されています。

対象者像	高度 IT 人材として確立した専門分野をもち，被監査対象から独立した立場で，情報システムや組込みシステムに関するリスク及びコントロールを総合的に点検，評価し，監査結果をトップマネジメントなどに報告し，改善を勧告する者
業務と役割	被監視対象から独立した立場で，情報システムや組込みシステムを監査する業務に従事し，次の役割を主導的に果たすとともに，下位者を指導する。 ① 情報システムや組込みシステム及びそれらの企画・開発・運用・保守に関する幅広く深い知識に基づいて，情報システムや組込みシステムに関するリスクを分析し，必要なコントロールを理解する。 ② 情報システムや組込みシステムに関するコントロールを検証又は評価することによって，保証を与え，又は助言を行い，IT ガバナンスの向上やコンプライアンスの確保に寄与する。 ③ ②を実践するための監査計画を立案し，監査を実施する。また，監査結果をトップマネジメント及び関係者に報告し，フォローアップする。
期待する技術水準	情報システムや組込みシステムが適切かつ健全に活用され，IT ガバナンスの向上やコンプライアンスの確保に貢献できるように改善を促進するため，次の知識・実践能力が要求される。 ① 情報システムや組込みシステム及びそれらの企画・開発・運用・保守に関する幅広く深い知識をもち，その目的や機能の実現に関するリスクとコントロールに関する専門知識をもつ。 ② 情報システムや組込みシステムが適用される業務プロセスや，企業戦略上のリスクを評価し，それに対するコントロールの問題点を洗い出し，問題点を分析・評価するための判断基準を自ら形成できる。 ③ IT ガバナンスの向上やコンプライアンスの確保に寄与するために，ビジネス要件や経営方針，情報セキュリティ・個人情報保護・内部統制などに関する関連法令・ガイドライン・契約・内部規定などに合致した監査計画を立案し，それに基づいて監査業務を適切に管理できる。

	④　情報システムや組込みシステムの企画・開発・運用段階において，有効かつ効率的な監査手続を実現するための監査技法を適時かつ的確に適用できる。 ⑤　監査結果を事実に基づく論理的な報告書にまとめ，有益で説得力のある改善勧告を行い，フォローアップを行うことができる。
レベル対応	共通キャリア・スキルフレームワークの 人材像：サービスマネージャのレベル 4 の前提要件

図表 11　システム監査技術者の対象者像

3-2　試験時間と出題形式

システム監査技術者試験の試験時間と出題形式は次のとおりです。

	午前 I	午前 II	午後 I	午後 II
試験時間	9:30～10:20 (50 分)	10:50～11:30 (40 分)	12:30～14:00 (90 分)	14:30～16:30 (120 分)
出題形式	多肢選択式 (四肢択一)	多肢選択式 (四肢択一)	記述式	論述式
出題数と解答数	30 問出題 30 問解答	25 問出題 25 問解答	4 問出題 2 問解答	3 問出題 1 問解答

図表 12　試験時間と出題形式

3-3　出題範囲

午前の出題範囲として，大分類の「6. サービスマネジメント」，「9. 企業と法務」が重点分野に該当します（図表 4 参照)。本書の巻末の付録に，具体的な分野ごとの出題範囲を収録しているので参考にしてください。

午後の試験の出題範囲は次のとおりです。

（午後Ⅰ：記述式，午後Ⅱ：論述式）

1　情報システム・組込みシステム・通信ネットワークに関すること

経営一般，情報戦略，情報システム，組込みシステム，通信ネットワーク，ファイルシステムやデータベース，ソフトウェアライフサイクルモデル，プロジェクトマネジメント，IT サービスマネジメント，リスク管理，品質管理，情報セキュリティ関連技術，情報セキュリティポリシ，事業継続管理　など

2　システム監査全般に関すること

IT ガバナンス，IT 統制，情報システムや組込みシステムの企画・開発・運用・保守の監査，業務継続管理の監査，システム開発プロジェクトの監査，情報セキュリティ監査，個人情報保護監査，他の監査（会計監査，業務監査）との連携・調整　など

3　システム監査の計画・実施・報告に関すること

監査計画，リスクアプローチ，監査の実施，コンピュータ支援監査技法，ディジタルフォレンジックス，監査報告，フォローアップの実施，システム監査業務の管理（監査業務の品質管理を含む）　など

4　システム監査関連法規に関すること

情報セキュリティ関連法規，個人情報保護関連法規，知的財産権関連法規，労働関連法規，法定監査関連法規，システム監査及び情報セキュリティ監査に関する基準・ガイドライン・施策，内部監査及び内部統制に関する基準・ガイドライン・施策　など

図表 13　午後の出題範囲

3-4　システム監査基準とシステム管理基準

システム監査を実施するための基準として公表されているものが，平成 16 年 10 月に改訂された「システム監査基準」です。また，システム監査の実施に当たって，監査上の判断の尺度として用いるために公表されている基準が，平成 16 年 10 月に制定された「システム管理基準」です。これらの内容は，本書の巻末の出題分析を参照してください。

4．平成 24 年度春期の試験に向けて

4-1　システム監査技術者試験について

平成 23 年度春期の応募者数は，前年よりも少し減りました。情報処理技術者試験全体の受験者数が前年よりも減っており，システム監査技術者試験にもその傾向が出ています。

年度	応募者数	受験者数（受験率）	合格者数（合格率）
平成 21 年度	5,313	3,271(61.6%)	455(13.9%)
平成 22 年度	5,415	3,534(65.3%)	506(14.3%)
平成 23 年度	4,990	3,278(65.7%)	475(14.5%)

図表 14　応募者数・受験者数・合格者数の推移

午前Ⅰ試験は，オーソドックスな問題が中心で，比較的対応しやすい問題でしたが，数問新傾向問題も出題されました。午前Ⅱ試験は，システム監査関連の問題が 14 問から 11 問に減り，その他の領域については，問題数が増えると同時に，内容的にも難しい問題が増えました。

午後Ⅰ試験は，問 1 がデータセンタ移転の問題であった点が目新しかったです。問 2～4 は，今までの傾向と大きな違いはない内容でした。

午後Ⅱ試験は，問 1 が海外拠点に対する情報セキュリティ監査の問題で，海外拠点に関する経験がないと選びにくい問題でした。問 2，問 3 は比較的オーソドックスな問題でしたので，それほど苦労する内容ではなかったと思います。

4-2　午前Ⅰの問題

新試験制度になって 5 回目の試験実施ですが，発表によれば，平成 22 年度秋期における高度の午前Ⅰ試験は平均して約 6 割の人が免除対象者で，かなり増えてきました。試験種別によって差がありますが，平成 22 年度秋期の試験では，午前Ⅰ試験を受験した人で基準点の 60 点以上取れた人は，午後Ⅱ試験が論文となる IT ストラテジストやシステムアーキテクト，サービスマネージャなどで約 3 割から 5 割となっていました。午前Ⅰ試験の免除者が増えた反面，午前Ⅰ試験を受験している方たちにとっては，易しい試験ではなくなってきていることが伺えます。

●平成 23 年度春期

午前Ⅱ問題 解答・解説

問1　イ

予備調査で実施するシステム監査手続（H23 春-AU 午前Ⅱ問 1）

予備調査は，監査対象の情報システムのリスクが適切に識別されているか，リスクアセスメントに基づいたコントロールが適切に整備されているかなど，監査対象の実態を可能な限り明確に把握するために行うものである。予備調査における監査手続でよく用いられるものに，質問書，インタビュー，資料の収集と閲覧などがある。監査精度を高め，監査効率を向上させるためにも，予備調査は欠かすことができない。

（イ）は，アンケート調査によってリスクの認識に関する情報を収集しており，予備調査の監査手続に該当するため，正解である。

ア：監査証拠とは，本調査の監査手続を適用して入手されるものであり，予備調査の対象ではない。更に，指摘事項をまとめるのは監査報告書を作成する段階の作業である。

ウ：本調査で用いられる現地調査に関する記述である。予備調査の段階では，まだ明確な改善提案はまとまっていない。

エ：本調査に関する記述である。そもそも，監査手続書は予備調査の結果を基に作られるものである。

問2　エ

システム監査人の精神上の独立性（H23 春-AU 午前Ⅱ問 2）

システム監査人に求められる独立性のうち，精神上の独立性についての問題である。システム監査基準では，一般基準の「2. 独立性，客観性と職業倫理」に，システム監査人に求められる独立性や客観性と職業倫理に関する記載があり，「外観上の独立性」，「精神上の独立性」，「職業倫理と誠実性」の 3 項目に分けて説明している。精神上の独立性については，「システム監査人は，システム監査の実施に当たり，偏向を排し，常に公正かつ客観的に監査判断を行わなければならない」と示されている。したがって，（エ）が正解である。

なお，このほかに，システム監査基準では，一般基準の「4. 業務上の義務」において，システム監査人に求められる「注意義務」と「守秘義務」を定めている。

ア：「外見上の独立性」に関する記述である。

イ：「守秘義務」に関する記述である。

ウ：「職業倫理と誠実性」に関する記述である。

問3 エ

外部委託に関するシステム監査上の確認事項（H23 春-AU 午前Ⅱ問 3）

ソフトウェアやシステムの開発・運用などの委託先が経営破綻などを起こすと，ソフトウェア資産のメンテナンスが受けられない可能性がある。このようなリスクを防止するために，ソフトウェアのソースコードなどを第三者に預託し，仮に経営破綻などが発生した際には，そのソースコードを基に対応することができる。

エスクロウ（エスクロー）とは，商取引の際に，売り手と買い手以外に中立の第三者を介在させることによって安全性を担保するサービスのことで，第三者預託という。従来，不動産など高額商品の取引で用いられてきたが，最近ではネットオークション取引でも用いられている仕組みである。クラウドコンピューティングの普及などもあって，システムにおける外部委託に関するシステム監査においては，このような条項が含まれているかどうかを確認しておくことが必要である。したがって，（エ）が正解である。

ア～ウ：いずれも，経営破綻によるソフトウェア資産のメンテナンスが受けられなくなることを防止する効果はない。

問4 エ

他社プログラマによる開発に関する監査指摘事項（H23 春-AU 午前Ⅱ問 4）

B 社の要員が A 社の監督者の指揮監督下でプログラム開発業務を担当する状況は，派遣契約による場合しかあり得ない。請負契約なら，B 社のプログラマは B 社の監督者の指揮監督下で作業をしなければならない。

B 社の要員が A 社からの委託によって派遣契約で作業をする場合，B 社のプログラマが A 社の著作権を侵害することがあり得るので，そうした侵害に対する措置に関する規定をあらかじめ定めておくことが望ましい。したがって，（エ）が適切である。

ア：一般労働者派遣事業の許可を得ていなくても，B 社の常用労働者（B 社のプログラマ）の場合，特定労働者派遣事業として届け出ていれば，派遣契約は可能である。

イ，ウ：問題文の状況は請負契約ではなく，派遣契約である。

問5 エ

情報システムのコントロールの評価（H23 春-AU 午前Ⅱ問 5）

情報システムのコントロールの評価は，把握したリスクに対するコントロールが整備されているかどうかを評価する整備状況の評価と，整備されたコントロールが適切に運用され，継続的に改善されているかどうかを評価する運用状況の評価の二つに分類されることが多い。また，その評価においては，まず整備状況の評価を実施してから，次に運用状況の評価を行うという手順で進められるのが一般的である。ユーザのシステムへのログインパスワード管理については，パスワード設定や管理に関する方針・ルールが定められていることを確認することが整

●平成 23 年度春期

午後Ⅰ問題 解答・解説

問１　データセンタ移転に伴うサーバ移転計画のシステム監査　(H23 春-AU 午後Ⅰ問 1)

【解答例】

［設問１］　バックアップ機の設置及び稼働確認を先に行い，本番機を搬出する。

［設問２］　監査証拠：各オーナ部門が策定した互換性確認テスト計画
内容：全テスト項目が１週間で完了できる作業量かどうか。

［設問３］　監査手続：アプリケーションプログラム一覧と調査済の仕様書の突合せ
理由：調査されていないアプリケーションプログラムが存在するリスクがあるから

［設問４］　理由：切戻し計画はサーバ移転後の災害などの発生を想定したものでないから
対策：本番機移転の前に，システム構成の変更に合わせて BCP を更新する。

【解説】

データセンタの移転という新傾向の問題である。設問内容も，問題文のヒントから解答するというよりは，移転に伴うリスクを一般論も含めて考える内容であるので，難しく感じた受験者が多かったのではないかと思われる。

［設問１］

〔データセンタ移転に伴うサーバ移転計画〕3. バックアップ機設置には，「4 月第 2 週の週末に DC-A から DC-N に実機移設される 13 台の本番機では，業務優先度の低い社内業務システムが稼働していたので，バックアップ機が存在しない。しかし，3 か月前に用途が見直され，重要なアプリケーションシステムが導入されたので，移転作業期間中に 13 台のバックアップ機を BC に新規設置することになった」という記述があり，4 月第 2 週の週末においてバックアップ機がまだ存在していないことが分かる。その場合，サーバ移転作業で障害が発生したとすると，代替手段がないことになる。これは，監査チームが指摘したリスクの原因になるものである。したがって，BC に新規設置する 13 台のバックアップ機が本番機の DC-N への搬入以前にも機能するように考えておけばよいので，対策としては，BC への「バックアップ機の設置及び稼働確認を先に行い」ついで「本番機を搬出する」といった手順を取ることが考えられる。

［設問２］

〔システム監査の実施〕2. 本調査での発見事項の(2)及び表 2 の項番 1 の検討結果①に記述されているように，OS，ミドルウェア及びアプリケーションシステムの導入完了期限が移転 1 週間前なので，互換性確認テストの期間は 1 週間しかとれないことが分かる。したがって，この 1 週間でテストが可能かどうかが判定できる監査証拠を挙げればよい。表 2 の項番 1 の検討結果③には，「各オーナ部門が，互換性比較表に基づいて，互換性確認テスト計画を策定して実施」と記述されているので，監査証拠として互換性確認テスト計画が使えることが分かる。したがって，監査証拠としては，「各オーナ部門が策定した互換性確認テスト計画」と解答する。

検証内容は，素直にこの互換性確認テスト計画を調べて，「全テスト項目が 1 週間で完了できる作業量かどうか」を確認すればよい。

［設問３］

情報システム部の調査結果の適切性を判断するために必要な監査手続と，その手続が必要な理由が問われている。まず，そのような監査手続が必要な理由，すなわち調査結果の適切性に関する問題点を先に考える。

〔システム監査の実施〕表 2 の項番 3 の検討結果には，「情報システム部が，移転 2 週間前までに調査し，IP アドレスを直接指定しているアプリケーションプログラムを識別」と記述されているが，この調査結果が適切であることは検証されていないので，影響を受けるアプリケーションプログラムがすべて識別されているという保証がない。これが監査手続を必要とする理由である。したがって，解答としては，「調査されていないアプリケーションプログラムが存在するリスクがあるから」ということを指摘すればよい。

検証のための監査手続としては，すべてのアプリケーションプログラムについて，こうした調査が行われていることが確認できればよい。具体的には，「プログラム一覧と調査済の仕様書の突合せ」という方法が考えられる。このプログラム一覧の帳票名は問題文には記述されていないので，一般的な“アプリケーションプログラム一覧”のような記述でよいであろう。

［設問４］

〔システム監査の実施〕表 2 の項番 4，5 を見ると，BCP の更新よりも前に切戻し計画が策定されていることが分かる。したがって，この切戻し計画は，当然サーバ移転後の災害などの発生を想定したものでないことになる。このため，現在の状態では，サーバ移転後の災害時などには対応できないはずである。サーバの移転を進めている段階ではまだ BCP は更新されていないので，移転作業実施段階でなんらかの災害が発生したとすると，各サーバの切戻し計画で対応しようとしても前提となるシステム構成条件などの相違のために適切な対応にならない可能性がある。そこで，切戻し計画だけでは不十分であると考えた理由としては，「切戻し計画はサーバ移転後の災害などの発生を想定したものでないから」ということになり，そのようなリスクに対処す

●平成 23 年度春期

午後Ⅱ問題 解答・解説

問 1　システム開発や運用業務を行う海外拠点に対する情報セキュリティ監査 (H23 春-AU 午後Ⅱ問 1)

【解説】

よく出題される情報セキュリティ監査に関する問題であるが，海外拠点という制約が付いているのが最大の特徴であり，この制約をうまく述べられるかどうかが合否を分ける大きなポイントである。設問内容は，設問イがリスクとコントロール，設問ウが監査実施上の留意点というオーソドックスな内容である。

［設問ア］

システム開発や運用業務を海外拠点で行っている，又は海外拠点で行うことを検討している場合の背景，目的及び実施状況や検討状況について述べる設問である。述べる対象がいろいろと選択できるので，整理すると次の四つのケースが選べることになる。

	実施状況	検討状況
システム開発	ケース 1	ケース 2
運用業務	ケース 3	ケース 4

実施状況と検討状況は，既に行っていれば実施状況を，将来行う予定であれば検討状況を述べることになる。実施状況を選ぶ場合が多いと思われるが，検討状況を選ぶと述べる内容の自由度が増すという利点がある。

システム開発と運用業務も，実態に合わせてどちらかを選べばよいが，大手 SI ベンダ等を除いて，システム開発だけを海外で行っている場合は少ないと思われるので，システム開発を選んだときに，運用業務も合わせて述べる場合が多いと思われる。

背景，目的は，システム開発や運用業務を海外拠点で行っている背景や目的を述べることになる。ここでは，なぜ海外で行う必要があったのかの理由を明確にすることが重要である。問題文には，目的として次の例が示されている。

・安価な労働力を求める。

・おう盛な消費意欲を求める。

確かに，この二つのケースが非常に多いと思われるが，このほかにも次のような目的が考えられる。

・顧客企業の海外進出に対応する。

・商品や材料の仕入を行う。

また，問題文には，海外進出の形態として次の例が挙げられているので，これらの進出形態は背景の一つとして述べておいた方がよいであろう。

・現地企業との提携
・現地に支店や子会社を設立

実施状況や検討状況については，特に制約はないので，自由に記述してよいが，設問イで述べる情報セキュリティ上のリスクと関連する部分を強調して，設問イにスムーズにつながるようにすることが重要である。

［設問イ］

リスク及びコントロールに関する記述なので，前半でリスクを述べ，後半でコントロールを述べるのが一般的であるが，リスクの種類別にリスクとコントロールを一緒に述べてもよい。問題文には，次のような，扱う情報の種類についての記述がある。どのような情報を扱っているかは，設問イで述べるリスクと密接な関係があるので，扱っている情報の種類を述べておく方がよいであろう。

・経営，人事，財務，営業などに関する企業情報
・製品の技術情報
・顧客の個人情報

情報セキュリティ上のリスクに関しては，設問に「システム開発や運用業務を海外拠点で行う場合」という制約が付いている点に留意することが最も重要である。つまり，国内でも一般的に発生するようなリスクを挙げても合格論文にはならないということである。問題文には，留意すべき状況として，次のようなものが挙げられている。リスクを述べる際には，これらの海外拠点特有の状況と絡めて述べなくてはならない。

・文化
・商慣習
・従業員の労働条件
・法規制
・電力やネットワークなどの社会的インフラ

コントロールに関して重要なことは，必ずリスクと対応させて述べることである。海外拠点特有のリスクに対して，どのようなコントロールが有効かを述べていけばよい。情報セキュリティ対策は一般的に，次のように分類されることが多いので，これらも参考に必要なコントロールを考えていけばよい。

	概要	具体策
物理的セキュリティ	設備や施錠などの物理的な手段による対策	入室管理，施錠，耐震対策，バックアップ施設の設置
技術的セキュリティ	情報システム自体に施される対策	アクセス制御，ウイルス対策，暗号化
運用管理（人的）セキュリティ	労務管理，教育などの人に対する対策	教育・訓練，対応手順の明確化，ルールの徹底