

令和6年度秋期

午前 I 共通問題 (SC, DB, ES, PM, AU) 試験分析と講評

■午前 I 試験 (高度試験共通) 講評

共通知識として幅広い出題範囲の全分野から 30 問が出題される試験です。今回の分野別出題数はテクノロジー分野が 17 問、マネジメント分野が 5 問、ストラテジ分野が 8 問でこれまでと同じでした。出題された問題は、従来どおり全て同時期に実施された応用情報技術者試験の午前問題 80 問から選択されています。重点分野のセキュリティからの出題が 4 問と最も多く、今回、ユーザーインタフェースとソフトウェア開発管理技術分野からの出題はありませんでした。

これまでの試験で出題されていない新傾向といえる問題は、次の 3 問 (前回 4 問) でした。

問 1 AI における教師あり学習での交差検証

問 13 ディープフェイクを悪用した攻撃に該当するもの

問 26 コ・クリエーション戦略の特徴

これまで何度も出題されている問題が 16 問程度あり、前回の 18 問から減りましたが、解くのが難しい問題は少なく、オーソドックスな問題が多かったといえます。少し難しかった問題としては、問 20 の RTO と RLO を定めた例、問 24 の年間当たりの金額面の効果が最も高い BPR のシナリオ、などの問題が挙げられますが、全体として少し易しい試験だったといえます。

問題の出題形式は、文章の正誤問題が 18 問 (前回 15 問)、用語問題が 5 問 (前回 4 問)、計算問題が 4 問 (前回 5 問)、考察問題が 3 問 (前回 6 問) で、文章・用語問題が増え、計算・考察問題が減っています。

高度試験共通の午前 I の問題は出題範囲が広いので、対策として、基本情報技術者や応用情報技術者試験レベルの問題を日ごろから少しずつ解いて必要な基礎知識を維持し、新しい知識を吸収していくことが大切です。

(今回の分野別出題内容) は新傾向問題、 は既出の定番問題

- ・テクノロジー分野……AI における交差検証、逆ポーランド表記法、ハッシュ関数の衝突、キャッシュメモリ、サーバの信頼性、ページング方式、コンパイラ、アクチュエーター、帯域幅、表の設計、DNS、アドレスを調べるコマンド、ディープフェイクを悪用した攻撃、CVE 識別子、DNS キャッシュポイズニング、エクスプロイトコード、ソフトウェアの使用性

- ・マネジメント分野……スコープの管理、ファストトラッキング、RTO と RLO の例、監査手続の技法、システム監査のフォローアップ
- ・ストラテジ分野……DX 推進指標、効果が高い BPR のシナリオ、UML の図、コ・クリエーション戦略、事業化から産業化への障壁、正味所要量の計算、経営理念・経営戦略・事業戦略の関係性、労働者派遣法

分野別の出題数は次のような結果で、従来と同じでした。

分野	大分類	分野別	R5 年秋	R6 年春	R6 年秋
テクノロジー系	基礎理論	17	3	3	3
	コンピュータシステム		4	4	5
	技術要素		8	8	8
	開発技術		2	2	1
マネジメント系	プロジェクトマネジメント	5	2	2	2
	サービスマネジメント		3	3	3
ストラテジ系	システム戦略	8	3	3	3
	経営戦略		3	3	3
	企業と法務		2	2	2
合計		30	30	30	30

出題される問題の 7 割程度は、過去の基本情報技術者や応用情報技術者試験で出題された基本的な内容です。高度試験で専門分野の力を発揮するのは午前 II の専門知識の試験からになりますが、午前 I 試験から受験する人は、過去の応用情報技術者試験の午前問題を解いてみて、余裕をもって 7 割以上正解できるように、不足している知識を確実に理解してください。

IPA の試験統計情報を分析すると、高度情報処理技術者試験を午前 I 試験から受けた人のうち、60 点以上取れた人は 5 割から 6 割台で推移していて、半数近くが次の午前 II 以降の採点に進んでいない状況です。出題元の応用情報技術者試験の午前問題は難しい内容も多いので、苦手な分野の学習は易しい問題が多い基本情報技術者の内容から復習を始めるとよいといえます。

また、出題範囲が広いため、全体をまんべんなく学習するのにかなり時間がかかります。そのため、試験対策としては、これまで出題された出題内容のポイント事項を重点的に解説したアイテック刊行の「2025 高度午前 I ・応用情報 午前試験対策書」で効率よく学習することをお勧めします。

以上

令和 6 年度秋期

情報処理安全確保支援士試験分析と講評

■試験全体講評

平成 29 年度春期に第 1 回の情報処理安全確保支援士(以下、支援士という)試験が開始されて以来、今回の試験で第 15 回(令和 6 年度秋期)を迎えました。第 1 回は 25,130 名の応募者を集め、それ以降、回を追うごとに応募者が漸減する傾向にありましたが、令和 4 年度秋期から回復傾向が見られるようになりまし。令和 6 年度秋期の応募者数は 24,032 名に達し、令和 6 年度春期に比較すると、22.8%と大きく増加しました。令和 5 年度秋期に午後 I と午後 II 試験が統合されてから 3 回目の実施になります。

参考までに、令和 5 年度秋期以降の応募者数などの推移を示すと、次のようになります。

年 度	応募者数	受験者数	合格者数
令和 5 年度秋期	20,432 (18.3%)	14,964 (73.2%)	3,284 (21.9%)
令和 6 年度春期	19,565 (-4.2%)	14,342 (73.3%)	2,769 (19.3%)
令和 6 年度秋期	24,032 (22.8%)	17,324 (72.1%)	2,615 (15.1%)

()内は、順に対前期比増減率、受験率、合格率を示す。

今日の社会においては、サイバー攻撃や標的型メール攻撃、マルウェア感染などに関する対策をはじめ、情報セキュリティの重要性は高くなる一方です。これらのセキュリティ問題全般について十分に理解していくには、Web システムをはじめ、クラウドサービスと認証連携、多要素認証技術、インシデント対応、電子メールや DNS の仕組みなどの基本的な知識を把握することが必要です。そして、支援士試験は、これまでの情報処理技術者試験という国家試験から、国家資格試験に格上げされました。資格取得後における講習受講義務が課せられるなどの条件がありますが、支援士試験に合格した上で、情報処理安全確保支援士(登録セキスペ)に登録すれば、社会的に認知された資格を有することができます。まずは支援士試験に合格し、登録セキスペの有資格者を目指してください。

午前 I (共通知識) 試験は 30 問出題され、出題分野の内訳はテクノロジー分野が 17 問、マネジメント分野が 5 問、ストラテジ分野が 8 問で、これまでと同じです。問題の出題形式は、文章の正誤問題が 18 問(前回 15 問)、用語問題が 5 問(前回 4 問)、計算問題が 4 問(前回 5 問)、考察問題が 3 問(前回 6 問)でした。少し難しかった問題としては、問 20 の RTO と RLO を定めた例、問 24 の年間当たりの金額面の効果が最も高い BPR のシナリオなどの問題が挙げられますが、全体として少し易しい試験だったといえます。

午前 II (専門知識) 試験の出題範囲は、技術要素のうち、セキュリティとネットワークが重点分野になっており、この 2 分野からの出題数は 20 問でこれまでと同じです。また、出題内容としては、情報セキュリティに関する個々の知識を問うものが大半を占めています。20 問のうち新規問題の出題数は 7 問で、令和 6 年度春期に比べると、2 問増加しました。また、過去問題は、令和 5 年度春期から平成 28 年度秋期までの広い期間の中から出題されていたことなどから、難易度は令和 6 年度春期に比べると、少し難しくなったといえます。

午後試験の出題テーマは、インシデントレスポンス(問 1)、ドメイン名変更(問 2)、クレジットカード情報の漏えい(問 3)、セキュリティ診断(問 4)でした。

問 1 では、インシデント発生時における、暫定対策と追加調査の内容を考察する問題と、攻撃者による目的実行までの活動を阻止するための技術的対策などの問題が出題されています。問 2 では、ドメイン名変更というテーマですが、内容的にはメールの詐称対策などに関する問題です。具体的には、第三者中継防止のためのルール、送信ドメイン認証技術の SPF, DKIM, DMARC の仕組み、ドメイン名を契約解除する場合に発生する悪用例、メールサービスを移行する際に発生する問題などが出題されています。問 3 は、Web セキュリティに特化した問題で、典型的な Web アプリの脆弱性、攻撃者によって偽フォームが表示された原因の調査とその対策、クレジットカード情報の漏えいの調査とその対策などの問題です。問 4 は、セッションフィクセッション脆弱性、メールヘッダーインジェクション脆弱性、HTTP ヘッダーの不備、TLS のバージョンに関する脆弱性などに関するセキュリティ問題を考えるものです。

令和 6 年度秋期試験は、Web 関連の問題の比重が幾分高かったものの、令和 6 年度春期試験のように、Web に関連する問題が 4 問中、3 問出題されていたことに比べると、比較的バランスの取れた出題であったといえます。

■午前Ⅱ（専門知識）試験講評

25問のうち、分野別の出題数は、「技術要素」から21問、「開発技術」から2問、「サービスマネジメント」から2問という比率でした。この比率は、第1回の平成29年度春期試験以降、同じですから、今後も変更はないと考えられます。なお、25問のうち、新規問題の出題数は7問でした。

午前Ⅱ試験の分野別出題数の推移（3期分）は、次のようになっています。

大分類	中分類	令和5年 秋期	令和6年 春期	令和6年 秋期
技術要素	セキュリティ	17	17	17
	ネットワーク	3	3	3
	データベース	1	1	1
開発技術	システム開発技術	1	1	1
	ソフトウェア開発管理技術	1	1	1
サービス マネジメント	サービスマネジメント	1	1	1
	システム監査	1	1	1
合計		25	25	25

(1) 技術要素

技術要素からの出題範囲は、セキュリティ、ネットワーク、データベースの3分野です。分野別の出題数は、セキュリティが17問、ネットワークが3問、データベースが1問でした。これからも分野別の出題数は、セキュリティが17問、ネットワークが3問、データベースが1問という割合には変化がないと考えられます。

セキュリティ分野の17問は、基本的に情報セキュリティ技術に関する問題です。新規問題は、問3（サイバー攻撃手法を分類したナレッジベース）、問7（パスキー認証で利用される利用者の生体情報の組合せ）、問10（送信ドメイン認証失敗時の処理をメールの送信側が指定する仕組み）、問11（SOARの説明）、問13（インラインモードで動作するアノマリ型IPS）、問16（DTLSの特徴）の6問です。これに対し、過去問題からの出題は、令和5年度春期から1問、令和4年度秋期から3問、令和4年度春期から2問、令和3年度秋期から2問、平成29年度春期から1問、平成28年度秋期から2問の計11問です。なお、過去問題からの再出題については、令和6年度春期試験は、3期前に当たる過去問題からの出題数が最も多い6問でしたが、令和6年度秋期

試験では、複数の期にわたって、1問ないしは2問などのように分散するというパターンに戻りました。

ネットワーク分野の3問は、新規問題が1問で、過去問題は2問でした。新規問題は、問20（ネットワークから信号を光学的に分岐させて取り出す装置）ですが、消去法によって選択肢を絞り込むことができるので、レベル3の問題といえます。過去問題は、令和4年度春期NW試験から1問、令和元年度秋期NW試験から1問ずつ出題されていました。いずれも専門知識が必要な問題といえます。

データベース分野の問21（関係モデルにおける外部キー）は、平成26年度春期SC試験で出題されていました。外部キーに関する基本的な特性ですから、レベル3の問題といえます。

(2) 開発技術

開発技術からの出題範囲は、システム開発技術とソフトウェア開発管理技術の2分野です。システム開発技術分野の問22（GoFのデザインパターンの説明）は、令和4年度春期SA試験で出題されていましたが、オブジェクト指向プログラミングに関する専門用語でしたから、レベル4の問題といえます。ソフトウェア開発管理技術分野の問23（XPにおけるテスト駆動開発の特徴）は令和3年度春期SC試験で出題されており、レベル3の問題と評価されません。

(3) サーマネジメント

サービスマネジメントからの出題範囲は、サービスマネジメントとシステム監査の2分野です。問24（サービスマネジメントシステム（SMS）における継続的改善）は令和5年度春期AP試験で出題されており、レベル3の問題といえます。問25（アクセス管理に関してITに係る業務処理統制に該当するもの）は令和4年度春期SC試験で出題されており、レベル3の問題といえます。

■午後試験講評

令和6年度秋期試験は、令和6年度春期試験の出題構成から少し変更され、Webセキュリティに関する問題が4問中、2問になり、比較的選択しやすい構成になっていたと思われます。また、令和6年度秋期試験の特徴は、令和5年度秋期試験からの記述式の設問において、採用された字数指定のない設問に統一されたことです。字数指定のない設問は、各自の考え方を自由に記述で

きますが、例えば、攻撃の手順などを順序よく述べる必要があります。自身の考え方を、論理的に整理できるかどうかといったことなどがポイントといえます。次回以降の支援士試験の記述式の設問では、字数指定のない記述式の設問について、適切に対応していくことが求められます。答案用紙の形式を見ると、マスありの場合、1行は20マスで構成されていますので、マスなしの場合には、1行当たり20字～25字程度を目安にして答案を作成するとよいでしょう。

午後試験で合格基準点をクリアするためには、情報セキュリティ全般に関する知識を十分に身に付けた上で、問題文に記述された内容をよく読んで、本文や図、表に記述された条件などを丁寧に整理し、設問で問われていることを的確に把握した上で解答を作成していくことが基本です。こうした知識面だけではなく、問題に対する取り組み方も重要になってきます。過去に出題された、午後Ⅰや午後Ⅱを含む午後問題に取り組んで、解答作成のコツをつかむように訓練を重ねておくことも忘れないようにしましょう。

問1 インシデントレスポンス

本問は、インシデントレスポンスというテーマによって出題されています。プロキシサーバから送信されたアラートメールを契機として、インシデントの証拠データを収集するツールによって出力されたログなどを用いて、マルウェアに感染したPCを特定し、その対策などを考える問題です。設問1では、暫定対策を行う際に必要となる作業内容や、さらにマルウェア感染が拡大しているかどうかの追加調査の内容が問われています。設問2は、攻撃者による目的実行までの活動を阻止するための技術的対策について、マルウェアが感染の拡大を阻止するための対策と、ファイルを不正に持ち出されないようにする対策が問われています。問題で示された図表類を基に、マルウェアがどのような動作を行うものかなどを見極めながら解答を作成することがポイントといえます。

問2 ドメイン名変更

本問は、ドメイン名変更というテーマによって出題されています。設問1は、第三者中継を防止するためのルール、設問2は、SMTPをTLSで暗号化するプロトコル、設問3は、DKIMレコードで指定されるFQDNと、DMARCレコードのポリシーの指定方法を答えるもので、いずれも基本的な問題です。設問4は、ドメイン名を悪用された場合、顧客に影響を及ぼす攻撃内容と、受信メールを使って続きの攻撃を行う内容などを答えるもので、問題の条件を考

慮して答案を作成することが必要です。設問5は、SPF認証とDKIM認証についての技術的な仕組みを答えるものです。送信ドメイン認証技術について、十分に理解していれば、かなりの設問に正解できそうです。

問3 クレジットカード情報の漏えい

本問は、典型的なWebアプリケーションの脆弱性に関する問題です。設問1は、XSSとSQLインジェクションに関するものです。設問2は、攻撃者が表示した偽フォームの画面や、ECMAScriptによる処理内容などが問われています。設問3は、攻撃者が自身のWebサーバ上でクレジットカード情報を取得する方法、被害に遭ったと想定される利用者をアプリケーションログから抽出する方法が問われています。少なくともECMAScriptのコードが読めることが必要です。

問4 セキュリティ診断

本問は、セキュリティ診断報告書において、セッションフィクセーション、メールヘッダーインジェクション、HTTPヘッダーの不備のほか、TLS1.1が利用可能であったこと、HTTPサーバのバージョンの露出という問題を取り上げ、それぞれの問題が、転職支援Webサイトで用いられている仕様や画面遷移などに関する脆弱な点を指摘するものです。問題の形式は、全て空欄に入れるものですが、そのほとんどが操作の内容、修正方法、効果、攻撃手順、改善の方針案と改善すべき理由などを記述式で答えるものです。問題で提示されている診断報告書を十分に把握し、どのような点が脆弱になっているかなどを確認しながら、解答を作成していくことがポイントといえます。

■ 次回の試験に向けて

午前試験は、午前Ⅰ（共通知識）と午前Ⅱ（専門知識）という二つの試験が行われます。午前Ⅰと午前Ⅱを比較すると、午前Ⅰの出題範囲が広範囲にわたることから、合格基準点をクリアすることが比較的難しいといえます。これに対し、午前Ⅱは、過去問題からの出題が半数以上あること、専門知識に特化していることなどから、事前の準備さえ怠らなければ、比較的容易にクリアできると考えられます。

こうしたことから、午前Ⅰ試験を受験する必要がある方は、午前Ⅰの試験対策については手を抜くことはできません。出題分野は、テクノロジー系（基礎理論、コンピュータシステム、技術要素、開発技術）、マネジメント系（プロジェクトマネジメント、サービスマネジメント）、ストラテジ系（システム戦略、

経営戦略、企業と法務)の全分野にわたるので、幅広い分野に加え、生成 AI などの新しい技術動向に関する知識も要求されます。日ごろから情報処理技術全般に関する知識を習得するとともに、関連する過去問題を多く解いておくようにしましょう。また、午前Ⅰで出題される 30 問は、応用情報技術者試験で出題される問題の中から抽出されるようになっていきます。なお、午前Ⅰの出題分野の全分野に関し時間を費やしていくことは、あまりお勧めできません。例えば、論理回路の問題などは、考え方を理解するのに少し時間がかかります。こうした問題に時間をかけても意味がありません。捨てる分野の問題を決めながら、効率的に学習していくとよいでしょう。

午前Ⅱ試験の出題数は 25 問、試験時間は 40 分です。出題の重点分野は、技術要素のうち、セキュリティとネットワークです。この他には、技術要素のデータベース、開発技術のうち、システム開発技術とソフトウェア開発管理技術、サービスマネジメントのうち、サービスマネジメントとシステム監査の分野からも出題されます。令和 6 年度秋期試験の出題数は、技術要素が 21 問、開発技術とサービスマネジメントが、それぞれ 2 問ずつで、これまでの試験と同じです。なお、技術要素のうち、セキュリティとネットワークの出題数は、どちらの技術に分類しても差し支えない問題(例えば、TLS や IPsec, DNS, 電子メールのセキュリティなど)があるので、セキュリティが 17 問、ネットワークが 3 問という比率で定着していると考えて問題ありません。難易度についてはレベル 4 の問題も出題されますが、セキュリティとネットワークに関する午前Ⅱ試験の問題は、午後試験対策を十分に実施していけば、ほぼ全問正解できるレベルになってきます。したがって、午前Ⅱ試験は、特別な対策を実施する必要はなく、午後試験に必要な技術知識を十分に身に付けていくとよいでしょう。

午後試験は、令和 5 年度秋期試験から、午後Ⅰ試験と午後Ⅱ試験が統合され、一つの午後試験として実施されるようになり、試験時間は 150 分になりました。そして、出題数 4 問の中から 2 問を選択して解答します。

令和 6 年度秋期の午後試験でも、4 問中、2 問が Web システムに関連する問題でした。これまでの傾向から判断すると、Web 関連のセキュリティ問題に重点が置かれていますので、IPA が公表している「安全なウェブサイトの作り方」,「セキュア・プログラミング講座」などの資料を事前に学習し、HTML コードのほか、HTTP のヘッダー情報やクッキー属性などについては、十分に理解するとともに、できるだけ様々な分野に対するセキュリティ問題に幅広く対応できる能力を身に付けるようにしましょう。

午後試験の問題選択に当たっては、個々の受験者が持ち合わせている技術

知識などの差に依存しますので、できるだけ自身の得意とする分野の問題を選択していくことが基本です。なお、一度選択した問題については、最後までやり抜くようにすることが必要です。それは、問題文をよく読んでいけば、問題の中にヒントが記述されていることが多く、それらを手掛かりにして正解を導いていくことが可能だからです。しかし、ヒントを見つけることができるかどうかについては、各自が持ち合わせている知識が多いか少ないかなどの差によって決まります。そこで、試験を受験するに当たっては、できるだけ知識レベルを向上させておくことが必要です。

例えば、セキュリティ技術分野では、Web アプリケーションに対する様々な攻撃とその対策、迷惑メール対策や標的型攻撃、サイバー攻撃に関する対策、IoT 機器に関連するセキュリティ問題、クラウドサービスの利用と認証連携、電子証明書の検証方法、パスワードレス認証や多要素認証による利用者認証、メッセージ認証、デジタル署名、暗号化技術、セキュリティプロトコル、VPN 技術、ファイアウォールの設定、IDS や IPS など、多くの技術知識を吸収していくことが必要です。また、Web アプリケーションなどに対するセキュア・プログラミングの問題では、C/C++ や Java, ECMAScript (JavaScript) をはじめ、HTML などの知識が要求されます。

以上のほか、ネットワーク技術分野では、TCP/IP (HTTP, HTTPS, IPsec, TLS など)、インターネット利用・接続技術、DNS の仕組み、電子メールの配送の仕組みなど、データベース技術分野では、データベースへのアクセス権限、SQL 文の読み方、ログ管理など、幅広い技術知識を習得していくことが必要です。さらに、情報セキュリティポリシーやリスク分析などのマネジメント系の問題に加えて、新たな攻撃手法など最新のトピックも含めて出題対象になり得るので、幅広く知識を吸収していくことが必要です。また、JIS Q 27001 や ISO/IEC 15408 などをはじめ、NIST や CRYPTREC などの様々な情報セキュリティ機関が策定している標準化の動向を把握していくことも忘れないようにしましょう。

午後問題では、セキュリティとネットワークの相互に関連した問題の出題頻度が高いことも特徴の一つです。これらの幅広い技術を十分に習得するには、かなりの時間が必要です。試験の直前になってあせらないように、あらかじめ多くの学習時間を見込んでおき、計画的に学習していくことが大切です。また、一度、理解しても繰り返し知識をインプットしていかないと、すぐに忘れてしまいます。工夫をしながら継続的に学習していく姿勢を確立しましょう。なお、試験問題では、単なる技術的な知識から解答する問題はそれほど多くありません。問題文に記述された内容に従って解答する問題の方が多いの

で、問題で記述された内容を正しく理解し、その条件内で考えていくようにしましょう。そのためには、問題文に記述された内容を理解できるだけの基本的な技術力をまず身に付けておくことが必要です。また、午後試験は数十字程度の記述式で解答する小問が多く設定されます。記述内容については、考え方や根拠を明確に示すほか、キーワードをしっかりと押さえた上で、解答を作成するようにしましょう。

以上のように、支援士試験に合格するためには、それなりの努力が要求されます。したがって、この試験に合格することは、それだけ価値が高いということになります。学習計画をしっかりと立てて、必ず合格するように努力していきましょう。

以上

