

令和7年度 春期

午前 I 共通問題(SC, NW, ST, SA, SM)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(以下、AP 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技術戦略マネジメント分野からの出題はありませんでした。

新しい内容の新傾向といえる問題は次の 8 問(前回 3 問)で、かなり増えていますが、選択元の AP 試験で増えていることによるものといえます。

- 問 2 機械学習の過程で過学習と疑われたときの解消方法
- 問 5 稼働率, MTBF, MTTR で成り立つ関係式
- 問 7 間欠動作の平均電流を $1\mu A$ 以下にするための待機時間
- 問 10 同じ値のコードをもつ表の行を自動的に削除する SQL 文
- 問 12 CRYPTREC 暗号リストの説明 (ST 既出問題, AP では初)
- 問 23 DX 認定制度における認定基準に含まれている事項
- 問 27 エッジ AI においてエッジデバイスで行われる推論処理
- 問 30 生成 AI を利用した画像生成と利用の著作権侵害について

これまで繰り返し出題されている定番といえる問題は 14 問程度で、前回の 16 問から少し減っています。なお、やや難しいと考えた問題は 6 問(問 5, 7, 12, 18, 24, 25)で、前回の 2 問から増えています。

問題の出題形式は、文章の正誤問題が 14 問(前回 18 問)、用語問題が 5 問(前回 5 問)、計算問題が 4 問(前回 4 問)、考察問題が 7 問(前回 3 問)で、考察問題が増え、文章問題が減っています。これらのことから、全体として少し難しいと感じた受験者が多かったと思われます。

(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……近似値, 機械学習の過学習, スタック, CPU 処理時間, 稼働率の関係, LRU 方式, 待機時間, SVG 画像, 正規形の変換, SQL (CASCADE), PoE, CRYPTREC 暗号リスト, SBOM, OS コマンドインジェクション, プロトコルの関係, デザインレビュー, スプリントレビュー

- ・マネジメント分野……EVM によるプロジェクト評価, クラッシング, サービス停止時間, 監査のウォークスルー法, 監査手続
- ・ストラテジ分野…… DX 認定制度, クラウドを実現するプロビジョニング, 契約形態, PPM, エッジ AI の推論処理, AI を用いたマシンビジョン, 変動費の計算, 生成 AI 利用の著作権侵害

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	R6年春	R6年秋	R7年春
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	5	4
	技術要素		8	8	8
	開発技術		2	1	2
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

これまで、出題される問題の約 7 割は、過去の基本情報技術者試験や AP 試験で出題された基本的な内容でしたが、今回は 5 割程度に減りました。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き、余裕をもって 7 割以上正解できるように、理解度を上げてください。

IPA の試験統計情報を分析すると、高度試験を午前 I 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、半数近くの人が次の午前 II 以降の採点に進んでいない状況です。高度共通の午前 I 試験では難しい内容も出題されますが、苦手な分野の学習は基本的な問題が多い基本情報技術者試験の内容から始め、基礎知識を確実に理解するようにしてください。

また、出題範囲が広いいため、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 7 年度春期

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 16 回(令和 7 年度春期)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 7 年度春期の応募者数は 22,645 名に達し、令和 6 年度秋期と比較すると、5.8%減少しましたが、1 年前の令和 6 年度春期と比較すると、大きく増加しています。参考までに、令和 6 年度春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 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%)
令和 7 年度春期	22,645 (-5.8%)	16,526 (73.0%)	3,134 (19.0%)

()内は、左から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になっておくとういでしょう。

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 14 問(前回 18 問)、用語問題が 5 問(前回 5 問)、計算問題が 4 問(前回 4 問)、考察問題が 7 問(前回 3 問)で、考察問題が増え、文章問題が減っています。また、少し難しかった問題としては、問 2(機械学習の過程で過学習と疑われたときの解消方法)、問 5(稼働率、MTBF、MTTR で成り立つ関係式)、問 7(間欠動作の平均電流を 1 μ A 以下にするための待機時間)など計 6 問もあり、全体として少し難しかった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。この 20 問のうち、新規問題の出題数は 6 問で、令和 6 年度秋期に比べると、1 問減少したこと、過去問題は、令和 5 年度秋期と令和 5 年度春期の 2 期に集中して 11 問出題されていたことなどから、難易度は、令和 6 年度秋期に比べると、易しくなったといえます。

午後試験の出題テーマは、サプライチェーンのリスク対策(問 1)、脆弱性管理(問 2)、スマートフォン用アプリケーションプログラムの開発(問 3)、IT 資産管理及び脆弱性管理(問 4)でした。問 1 は、サプライチェーンリスク対策のガイドラインを作成し、全てのシステム開発プロジェクト及び運用サービスの点検における諸問題を考えるものです。問 2 は、プラットフォーム診断と Web アプリ診断で指摘された脆弱性の問題が出題されていますが、CVSS 値と EPSS 値の評価に関する事項なども問われています。問 3 は、スマホアプリに関する脆弱性に関する問題で、サーバ証明書や TLS の通信シーケンスなども問われています。問 4 は、公開 IT 資産管理と脆弱性管理に関するもので、公開 IT 資産管理のリストアップについての調査方法及び対応方法の問題のほか、KEV カタログに掲載される脆弱性などの知識問題でした。難易度を全体的に評価すると、前回の令和 6 年度秋期試験とほぼ同程度と考えられます。

■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 8 問で、前回の令和 6 年度

秋期試験から 1 問増加しています。

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 6 年 春期	令和 6 年 秋期	令和 7 年 春期
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 1 (DRDoS 攻撃に該当するもの)、問 3 (SHA-512/256 の説明)、問 8 (サイバー攻撃におけるコネクタバックの説明)、問 12 (NIST の CSF 2.0 のコアにある機能)、問 13 (IoC (Indicator of Compromise) に該当するもの) の 5 問です。これに対し、過去問題からの出題は、令和 5 年度秋期から 5 問、令和 5 年度春期から 6 問のほか、令和 5 年度春期 AP 試験から 1 問の計 12 問です。なお、過去問題からの再出題については、これまでの複数の期にわたって出題されるというパターンではなく、令和 5 年度秋期試験と令和 5 年度春期試験の 2 期に集中していたことが特徴です。

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 (GET/POST メソッドを用いたリクエストメッセージ) ですが、HTTP メッセージの基本構成に関するものですから、レベル 3 の問題といえます。過去問題は、令和 3 年度秋期 SC 試験から 1 問、平成 27 年度秋期 SC 試験から 1 問ずつ出題されていました。いずれも基本的な問題といえます。

データベース分野の問 21 (SQL 文を実行して得られる結果) は、令和 4 年度秋期 DB 試験で出題されていました。SQL 文の NOT EXISTS 述語の知識が必要ですが、レベル 3 の問題に位置付けられます。

(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 (ソースコードのソース品質を向上させる OSS のツール) は、新規問題です。OSS のツールの名称を知っているかどうかはポイントですが、難易度はレベル 4 の問題と評価されます。ソフトウェア開発管理技術分野の問 23 (スクラムにおける KPT の三つの視点) は令和元年度秋期 SA 試験で出題されていましたが、レベル 3 の問題といえます。

(3) サービスマネジメント

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 (サービス可用性の計算) は令和 5 年度春期 SM 試験で出題されていました。基本的な計算問題ですから、レベル 3 に位置づけられます。問 25 (金融庁「内部統制・監査の実施基準」の IT の統制目標) は新規問題ですが、基本的な用語問題ですから、レベル 3 の問題といえます。

■午後試験講評

令和 7 年度春期試験は、令和 6 年度秋期試験の出題構成から少し変更され、Web アプリ関連の問題がやや少なくなり、脆弱性管理をテーマとした問題が多く見られました。また、令和 6 年度秋期試験では、字数指定のない設問が、ほとんどでしたが、令和 7 年度春期試験では、字数が指定された設問がかなり見られました。次回以降の支援士試験の記述式の設問で、字数指定のない設問が増加するかどうかは定かではありませんが、字数指定のない設問の答案作成にも慣れておきましょう。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 20～25 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 サプライチェーンのリスク対策

本問は、サプライチェーンのリスク対策というテーマですが、サプライチェーンリスク対策のセキュリティガイドラインを作成し、全てのシステム開発プロジェクト及び運用サービスの点検における諸問題を考えるものです。設問1では、セキュリティ・バイ・デザインの考え方や、再委託する場合に契約書に明記する事項が問われています。設問2は、過去のインシデントに基づいた事例の分析などの問題、設問3は、システムの開発プロジェクト及び運用サービスに対してガイドラインを用いた点検結果、設問4はSBOMを利用すると脆弱性管理がしやすくなる理由、設問5では、開発工程のどの時点でSASTツールを使用する場合に効果が得られるかなどが問われています。基本的な事項が問われていますので、難易度はそれほど高くないと思われます。

問2 脆弱性管理

本問は、脆弱性管理というテーマですが、プラットフォーム(PF)診断とWebアプリ診断に関する問題が出題されています。設問1は、SQLインジェクションの応答結果、設問2は、診断結果が異なっていた要因を考えるものです。設問3は、鍵交換におけるビットセキュリティ基準、認証タイムアウトメッセージに基づき攻撃を早期に検知する方法、アクセス元のPCを認証する方法を答えるものです。設問4は、Webアプリ診断で検出された脆弱性について、深刻度レベルが低く評価された評価根拠と高く評価された評価根拠、管理者権限が必要な操作ができなかった仕様をサイトCの仕様の中から選ぶものです。設問5、6は、CVSSv3の現状値は手間が掛かりEPSS値では手間が掛からない理由、PF診断とWebアプリ診断で検出された脆弱性に対する評価結果の対応優先度を定める問題などが出題されています。問題の難易度は、標準レベルと思われるが、小問数が多いことから、正解できるものについては、着実に点数を積み上げていくことが必要です。

問3 スマートフォン用アプリケーションプログラムの開発

本問は、新規に開発したスマートフォン用アプリケーションプログラムの脆弱性診断結果に基づいて考える問題です。設問1では、サーバ証明書の検証不備がある場合、攻撃者がアクセスキーを取得する方法、アクセスキーの保護に不備がある場合、攻撃者がアクセスキーを取得する方法及び全利用者の

写真をダウンロードする方法などが問われています。設問2は、サーバ証明書に記載される名前や、TLSの通信シーケンス、プライベート認証局を用いた場合にスマホ側に必要となる設定内容などを答えるものです。設問3は、署名付きURLの生成時点、設問4は、フィッシングサイトにアクセスしても気付くことができないというスマホアプリの仕様上の問題点と、アクセスできないようにする機能を具体的に答えるものです。正解を導くためには、問題の条件を丁寧に確認することなどが求められますが、問題の難易度は、標準レベルといえます。

問4 IT資産管理及び脆弱性管理

本問は、IT資産管理、ドメイン名などの管理、導入ソフトウェアの管理、脆弱性管理の改善などに関する問題です。設問1では、CDNサービスを解約したときに必要となる設定の変更内容が問われています。設問2は、公開IT資産管理及び脆弱性管理の目標設定に関するもので、未登録の公開IT資産の調査方法などに関する字句選択の穴埋め問題が出題されています。設問3は、IT資産の調査漏れリストに挙げられた事項に対し、追加の調査方法や対応方法を考えるものです。設問4は、KEVカタログに掲載される条件や、導入ソフトウェアの管理及び脆弱性管理についての改善策などを答えるものになっています。一部、用語自体の意味を知らないと答えられない設問がありますが、全体的に難易度を評価すれば、標準レベルといえます。

■令和7年度秋期の試験に向けて

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7年度春期試験の出題数は、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7年度春期の午後試験では、Webに関連するセキュリティ問題の比率が少なかったようですが、これまでの傾向から判断すると、WebアプリやWebAPIなどのセキュリティに関連する問題が2問程度出題されることがあります。このため、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」などをはじめ、様々な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を含め、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、個々の受験者がも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、各自がも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焦らないように、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く、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必要があります。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、次回の試験では必ず合格するように努力していきましょう。

以上

