

# 令和7年度秋期

## 情報処理安全確保支援士試験分析と講評

### ■試験全体について

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17回(令和7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た。令和7年度秋期の応募者数は26,385名に達し、令和6年度秋期と比較すると、9.8%とわずかに増加しました。令和8年度からはCBT(Computer Based Testing)に変わるため、紙の問題冊子を用いた最後の試験になりました。

参考までに、令和6年度秋期以降の応募者数などの推移を示すと、次のようにになります。

年 度	応募者数	受験者数	合格者数
令和6年度秋期	24,032 (17.6%)	17,324 (72.1%)	2,615 (15.1%)
令和7年度春期	22,645 (15.7%)	16,526 (73.0%)	3,134 (19.0%)
令和7年度秋期	26,385 (9.8%)	18,816 (71.3%)	4,199 (22.3%)

( )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、ランサムウェアを中心としたサイバー攻撃による情報流出や、業務停止といった事例がニュースでも取り上げられており、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、暗号技術や、認証技術、アンチマルウェア対策、DNSのセキュリティ技術といった基礎的な知識に加え、安全な運用手順の確立や検証、インシデント対応といった管理の観点での応用力も必要です。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17問(前回14問)、用語問題が6問(前回5問)、計算問題が4問(前回4問)、考察問題が3問(前回7問)でした。少し難しかった問題としては、問1(平均待ち時間が平均処理時間以上となる利用率)、問2(機械学習の評価方法であるROC曲線で用いられる偽陽性率の説明)、問8(BASE特性を満たすNoSQLデータベースシステム)、問17(著作者人格権を行使しない記載をして発生を防ぐ問題)、問18(タックマンモデルでメンバーが意見を主張し合う段階)、問22(コントロールの視点から検証・評価する項目)、問28(生産事業所のシステムでMESが運用される層)が挙げられますが、全体として標準的な難易度の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8問で、令和7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6年度秋期から平成24年度秋期までの広い期間、そして応用情報技術者試験やネットワークスペシャリスト試験など別の試験科目の問題の中から出題されていました。

午後試験の出題テーマは、コンサルティング業務で利用するSaaS(問1)、暗号資産交換業におけるセキュリティ(問2)、情報システムのセキュリティ強化(問3)、製造業におけるセキュリティ管理(問4)でした。

問1では、SaaSにおけるスクリプトインジェクションといったセキュリティインシデントへの対策をテーマとしながら、HTTPレスポンスヘッダーによるセキュリティ対策や、レスポンス出力時のエスケープ処理に関する問題が出題されています。問2では、暗号資産交換業を営む企業における資産移転時の署名をいかに安全に行う体制にするかという点がテーマになっています。具体的には、サイドチャネル攻撃対策や、署名鍵の暗号化、HSM(ハードウェア・セキュリティ・モジュール)も交えた的確な運用体制・手順などが挙げられています。問3では、インターネットバンキングにおける認証方式の検証と、リモート接続用のサービスを導入する際の通信許可の変更内容といった複数のテーマが盛り込まれています。具体的にはDNSSECやDoH

(DNS over HTTPS) といった用語知識を問う問題と、示された通信要件に沿った通信許可設定の変更内容を問う問題などが出題されています。問 4 では、製造業におけるセキュリティ管理がテーマになっています。具体的には、製造系と非製造系のコンピュータをファイアウォールで隔離したり、的確なアンチマルウェアソフトの導入や運用をしたりする点、及びバックアップからの復旧手順に関する点が出題されています。

令和 7 年度秋期試験は、問 1、2 が IT サービスを提供する側の組織のセキュリティ対策をテーマにした問題、問 3、4 が IT サービスを利用する側の組織でのセキュリティ対策をテーマにした問題だったともいえます。また、昨今の潮流を反映してか、暗号資産交換業をテーマにした問題も特筆すべきものであったと思われます。

## ■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、ユーザーインターフェースと情報メディア、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（新傾向）といえる問題は次の 7 問（前回 8 問）で 1 問少なくなりましたが、選択元の AP 試験は 20 問（前回 25 問）で 5 問減っています。

問 7 スイッチが押された状態に変化したことを検出する論理式

問 8 BASE 特性を満たす NoSQL データベースシステム

問 17 著作者人格権を行使しない記載をして発生を防ぐ問題

問 18 タックマンモデルでメンバーが意見を主張し合う段階

問 21 システム監査で使用される用語の説明

問 22 コントロールの視点から検証・評価する項目

問 28 生産事業所のシステムで MES が運用される層

これまで繰り返し出題されている定番といえる問題は 16 問あり、前回の 14 問から 2 問増えています。なお、やや難しいと考えた問題は 7 問（問 1、2、8、17、18、22、28）で、前回の 6 問から 1 問増えています。

出題形式は、文章の正誤問題が 17 問（前回 14 問）、用語問題が 6 問（前回 5 問）、計算問題が 4 問（前回 4 問）、考察問題が 3 問（前回 7 問）で、文章問題が増え、考察問題が減っています。これらのことから、全体としては前回の

試験よりも易しく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
- ・テクノロジ分野……待ち行列、機械学習の偽陽性率、線形探索の比較回数、プロセッサの高速化、キャパシティプランニング、キャッシングのブロック置換、状態変化を検出する論理式、BASE 特性を満たす NoSQL、ビュー、パケット送信個数、リバースプロキシ、エクスプロイト、発行元証明書、真正性と信頼性、なりすましとメール改ざん検知、ダイアグラム、著作者人格権
  - ・マネジメント分野……タックマンモデルの段階、人件費の計算、問題管理、システム監査の用語、コントロールの視点
  - ・ストラテジ分野……プログラムマネジメント、SOA、PBP 法、バランススコアカード、アンゾフの成長マトリクス、MES、最大利益の計算、意匠法

分野別の出題数は次のような結果で、令和 7 年春期試験と同じでした。

分野	大分類	分野別	R6 年秋	R7 年春	R7 年秋
テクノロジ系	基礎理論	17	3	3	3
	コンピュータシステム		5	4	4
	技術要素		8	8	8
	開発技術		1	2	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

次回令和 8 年度の試験から PC で受験する CBT 試験になることが IPA から公表されました。午前 I は科目 A-1、午前 II は科目 A-2 と試験名称は変わりますが、出題内容は変わらないとされています。最近の午前 I 試験では、過去の試験で出題された少し難しい問題も増えてきているので、過去の応用情報技術者試験の午前問題を繰り返し解き、余裕をもって 7 割以上正解できるように、知識の理解度を上げてください。

IPA から公表されている統計情報を分析すると、高度試験を午前 I から受けた人で、60 点以上取れた人は 5 割から 6 割が多く、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。次回以降も高度共通の科目 A-1 試験では難しい内容が出題されると思われますが、苦手な分野の学習は基本情報技術者試験などの内容から復習し、基礎知識を確実に理解してください。

試験の出題範囲が広く、全体をまんべんなく学習するにはかなりの時間がかかります。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と必須問題を重点的に解説したアイテック刊行の「2026-2027 高度科目 A-1・応用情報 科目 A 試験対策書」で効率よく学習することをお勧めします。

## ■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前回の令和7年度春期試験から2問増え8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6年 秋期	令和7年 春期	令和7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5（AIに対するモデルインバージョン攻撃に該当する

もの）、問8（ドメインフロンティングを悪用した攻撃の例）、問9（情報理論的安全性に基づく暗号技術）、問11（Identity Proofingに該当するもの）、問12（MITREの役割に該当するもの）、問14（UEBAの機能）、問15（CSPMの機能）の7問です。これに対し、過去問題からの出題は、令和6年度秋期から1問、令和6年度春期から4問、令和5年度秋期から1問、令和5年度春期から4問と複数の期にわたっていました。

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（HTTPのステータスコードに関する説明）ですが、100番台、200番台、300番台、400番台の意味を問う初歩的なものでした。過去問題は、平成24年度秋期AP試験から1問、令和6年度春期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（DBMSがコミット処理を完了するタイミング）は、令和5年度春期SA試験で出題されていました。トランザクションに関する問題で、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（ソフトウェア結合テストの方式）は、平成30年度秋期SC試験で出題されていましたが、AP試験でも出題される内容もあり、レベル3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（請負契約における著作権の帰属先）は平成31年度春期PM試験で出題されており、レベル3の問題と評価されます。

### （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（ITサービスのサービス可用性の計算）は令和6年度春期SM試験で出題されており、レベル3の問題といえます。問25（リスク評価に基づいた監査計画の策定で考慮すべき事項）は新規問題でしたが、システム監査に関する知識をしっかりと覚えておけば解けるということで、レベル3の問題といえます。

## ■午後試験講評

令和7年度秋期試験は、前回や昨年同時期同様、Webセキュリティに関する問題4問中、2問を選択する形式でした。令和7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、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ことが必要になります。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。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25字程度を目安にして答案を作成するとよいでしょう。

科目B(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、特に業務要件や現状を記述している本文や図、表の内容を整理し、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。このように知識面だけではなく、問題に示された内容に対する読み解き力も重要な要素になります。特に読み解き力に関しては、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、鍛えておくことも忘れないようにしましょう。

## 問1 コンサルティング業務で利用する SaaS

本問は、コンサルティング業務用のSaaSを提供する企業のシステムの脆弱性をテーマにした問題でした。コンサルティング業務用という点はあまり関係ありません。内容としては、HTTPヘッダー項目であるX-Frame-Optionsや、Strict-Transport-Security、Content-Security-Policyなどが取り上げられ、その中でもContent-Security-Optionの指定内容と、それによるブラウザ側の動作制約の内容に関する前提知識が必要とされていました。また、実際にスクリプトをインジェクションされないようにする対策案を記述式で回答できる力が必要です。

## 問2 暗号資産交換業におけるセキュリティ

本問は、暗号資産交換業において、自社で保管している暗号資産を外部に移転(送金と同等の行為)させる際のデジタル署名に関して、その署名鍵の取扱いの妥当性をテーマにした問題でした。電磁波によって署名鍵が盗聴されてしまうことを防ぐような対策や、マルウェアによる不正行為を防ぐ対策、従業員の不正行為を防ぐ対策と複数の観点での対策を考える問題でした。途中、企業買収によって加わった企業のHSM(ハードウェア・セキュリティ・モジュール)の運用形態にも焦点が当たっており、昨今のトレンドをキャッチした良問と言えます。

## 問3 情報システムのセキュリティ強化

本問は、ある企業において、インターネットバンキングの安全性をユーザー側企業として考査するテーマ、及びリモートアクセス用のKサービスというサービスの導入に当たって、ファイアウォールの設定変更や、取引先への依頼内容を考えるというテーマが組み合わさった問題でした。前者に関しては、インターネットバンキングのワンタイムパスワードによる認証機能とMITM(マン・イン・ザ・ミドル)攻撃の可能性を考査するという技術的な内容、後者に関しては、本文や図、表で示されている通信要件を整理し、必要な通信許可設定を考えるという読み解き力・応用力が試されました。

## 問4 製造業におけるセキュリティ管理

本問は、製造業を営む企業におけるマルウェア対策や権限の管理をテーマにした問題でした。営業部や設計課、製造課、品質保証課といった部署ごとの役割や、ネットワークセグメント分割が既に行われており、USBメモリを用いた製造データの持ち運びにおけるセキュリティインシデント対応、再発防止策に焦点が当たっていました。

ネットワークセグメント分離に関して、ファイアウォールによって不要な通信を遮断することや、ファイルサーバーにある特定の格納領域に最低限必要なアクセス権限、未知のマルウェアの検知に向けた取組み、マルウェア被害を受けた際の復旧体制などが問われていました。この問題も特に本文や図、表で示された業務要件の読み解き力が求められる問題でした。

### ■次回の試験に向けて(※次回からはCBT化に伴い科目名が変更になります)

今回の令和7年度秋期試験が、紙の冊子を用いた最後の試験になり、次回、令和8年度からはコンピュータ画面に向きあって回答を入力していくCBT(Computer Based Test)方式になります。科目A-1(午前I)試験の免除制度や、出題形式(多肢選択式・記述式・論述式)、出題数及び試験時間に変更はありませんが、従来の午前試験に相当する科目A群と、従来の午後試験に相当する科目B群の受験日が別日になる点に留意が必要です(申込みは同時)。詳細については下記のIPAからの案内をご参照ください。

[https://www.ipa.go.jp/shiken/2026/ap\\_koudo\\_sc-cbt.html](https://www.ipa.go.jp/shiken/2026/ap_koudo_sc-cbt.html)

従来の午前試験に相当する科目A群は、科目A-1試験(共通知識;従来の午前I)と科目A-2試験(専門知識;従来の午前II)という二つの試験が行われます。科目A-1試験と科目A-2試験を比較すると、科目A-1試験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、科目 A-2 試験は、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、科目 A-1 試験を受験する必要がある方は、科目 A-1 試験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、科目 A-1 試験で出題される 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、科目 A-1 試験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。

科目 A-2 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科目 A-2 試験の問題は、科目 B 試験対策を十分に実施していくべき、ほぼ全問正解できるレベルになってきます。したがって、科目 A-2 試験は、特別な対策を実施する必要はなく、科目 B 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。

従来の午後試験に相当する科目 B 群ですが、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ました、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

選択して解答する形式です。CBT 方式では科目 B 試験という名称に変わりますが形式は変わりません。なお、試験種別によっては、科目 B 群の中に科目 B-1 試験、科目 B-2 試験と分かれるものもありますが、情報処理安全確保支援士試験は科目 B 試験の一つだけなので、科目 B 群=科目 B 試験になります。

令和 7 年度秋期の午後試験は、4 問中、2 問が IT サービス提供企業側をテーマにした問題、2 問が IT サービス利用企業側をテーマにした問題ですが、技術的な観点でいうと Web システムの安全性（問 1）、暗号化やデジタル署名（問 2）、必要最小限の通信路の確保（問 3）、マルウェア対策（問 4）という様に多岐にわたっていました。暗号化やデジタル署名、マルウェア対策については、科目 A 群の対策で得られる知識で十分ですが、Web 関連のセキュリティ対策については、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、十分に理解することもおすすめです。

科目 B 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、AI を使った不正行為や、AI による情報漏えい、サイバー攻撃に関する対策、IoT 機器に関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。

科目B試験では、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くかないと、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、科目B試験は數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