

## 3 試験に向けて

### 3-1 情報処理安全確保支援士試験について

平成 28 年 10 月 21 日、経済産業省からサイバーセキュリティ分野において初の国家資格となる「情報処理安全確保支援士」制度を開始する旨の発表が行われました。それによりますと、情報処理安全確保支援士制度は、「近年、情報技術の浸透に伴い、サイバー攻撃の件数は増加傾向にあり、企業等の情報セキュリティ対策を担う実践的な能力を有する人材も不足する中、情報漏えい事案も頻発しています。このため、サイバーセキュリティの対策強化に向け情報処理の促進に関する法律の改正法が本日（平成 28 年 10 月 21 日）施行され、我が国企業等のサイバーセキュリティ対策を担う専門人材を確保するため、最新のサイバーセキュリティに関する知識・技能を備えた高度かつ実践的な人材に関する新たな国家資格制度を開始しました」とされています。また、情報処理安全確保支援士は、「サイバーセキュリティに関する知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、また、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う者です。サイバーセキュリティの確保に取り組む政府機関、重要インフラ事業者、重要な情報保有する企業等のユーザー側及びこれら組織に専門的・技術的なサービスを提供するセキュリティ関連企業等のいわゆるベンダー側の双方において活躍が期待されます」と説明されています。

こうした背景の下に、平成 29 年 4 月から情報処理安全確保支援士試験（以下、支援士試験という）が実施されるようになりました。この支援士試験は、午前Ⅰ、午前Ⅱ、午後Ⅰ、午後Ⅱという四つの試験が行われてきましたが、令和 5 年度秋期試験から、従来の午後Ⅰと午後Ⅱを統合し、一つの午後試験として実施されるようになりました。

令和 4 年度秋期（第 11 回）から令和 5 年度秋期（第 13 回）までの受験者数、合格者数などの推移を図表 10 に示します。なお、合格率については、第 1 回から第 3 回までは 16%から 17%程度で推移し、第 4 回から第 12 回までは 18.5%から 21.2%までの範囲に向上しました。今回の合格率は 21.9%と、これまでで最も高い合格率になりました。そして、IPA の発表によりますと、令和 5 年 10 月 1 日現在、「登録セキスペ」の登録者数は 21,727 名に達し、登録することの有効性が意識されるようになっていきます。

年 度	応募者数	受験者数	合格者数
令和4年度秋期	18,749 (16.8%)	13,161 (70.2%)	2,782 (21.1%)
令和5年度春期	17,265 (-7.9%)	12,146 (70.4%)	2,394 (19.7%)
令和5年度秋期	20,432 (18.3%)	14,964 (73.2%)	3,284 (21.9%)

( ) 内は、それぞれ対前期比増減率、受験率、合格率を示す。

図表 10 応募者数・受験者数・合格者数の推移

## 3-2 出題予想

### (1) 午前Ⅰ試験、午前Ⅱ試験

令和4年度秋期から令和5年度秋期までの3期にわたる試験から判断すると、午前試験については、次のようにいえます。まず、午前Ⅰ（共通知識）と午前Ⅱ（専門知識）を比較すると、午前Ⅰの出題範囲が広範囲にわたることなどから、合格基準点をクリアすることが難しく、午前Ⅱは、午前Ⅰに比較すると、クリアするレベルのハードルが少し低くなるといえます。ちなみに、午前Ⅰ試験と午前Ⅱ試験の合格率を示すと、図表11のようになります。

年 度	午前Ⅰ試験	午前Ⅱ試験
令和4年度秋期	52.6%	73.0%
令和5年度春期	52.5%	80.3%
令和5年度秋期	47.9%	68.6%

図表 11 午前Ⅰ試験と午前Ⅱ試験の合格率の比較

令和5年度秋期の午前Ⅰ試験の合格率は、令和4年度秋期、令和5年度春期に比べると約4.5ポイント低下し、これまでの全13回の試験において、低い合格率になりました。この数値からも分かるように、約半数以上の受験者が、午前Ⅱ試験の受験資格を失います。このため、午前Ⅰ試験を受験する必要のある方は、テクノロジー系、マネジメント系、ストラテジ系の幅広い分野にわたる知識に加え、DXを推進するために必要となる知識（AIなどに関する技術、AIやデータの利活用などの動向）を含め、十分に把握しておくことが必要です。なお、午前Ⅰ試験には免除制度がありますので、この制度を利用できるように、応用情報技術者（AP）試験に合格するか、いずれかの高度試験の午前Ⅰ試験に合格しておくことも一つの方法です。

午前Ⅱ試験の合格率は、68.6%でした。第1回から第12回までの合格率は71%～90%の範囲で推移していたので、今回が最も低い合格率でした。問題の難易度については、詳細な技術知識を問う問題が、比較的多く見られたので、合格率は低下すると想定していましたが、70%を切るとは思いませんでした。IPAが令和5年12月25日に発表した、令和6年度秋期試験以降の情報処理安全確保支援試験(レベル4)シラバス追補版(午前Ⅱ) Ver.4.0では、“AIを悪用した攻撃”、“PQC(Post Quantum Cryptography；耐量子計算機暗号)”、“軽量暗号”、“AIを使ったセキュリティ技術”などの用語が追加されているので、令和6年度秋期試験以降ではなく、令和6年度春期試験から出題される可能性があります。このため、AI関連のセキュリティ問題だけではなく、内容的に詳細な知識を問う問題の出題が多くなると予想されるので、支援士試験のシラバスに載せられている用語はできるだけ理解していくようにしましょう。

次に、午前Ⅰ試験の出題分野についてです。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)の全分野にわたりますので、幅広い分野に関する知識が要求されます。令和4年度秋期から令和5年度秋期までの分野別の出題数は、図表12に示すとおりです。なお、午前Ⅰ試験で出題される30問は、AP試験で出題された80問の中から抽出されていることが特徴です。

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

図表12 午前Ⅰ試験 分野別出題数

午前Ⅰ試験の分野別の出題数は、基本的にテクノロジ系が17問、マネジメント系が5問、ストラテジ系が8問という比率になっています。情報処理技術分野の知識だけではなく、プロジェクトマネジメントやシステム戦略、経営戦略などの知識も要求されます。このため、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、出題数が多いテクノロジ系やストラテジ系に関連する過去問題を多く解いていくようにしましょう。しかし、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、論理演算などの問題は、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ことも必要です。なお、支援士試験は、情報セキュリティの専門家の方が多く受験されると思います。特に、午前Ⅰ試験から受験する必要のある方は、午前Ⅰ試験が大きな関門となることがありますので、午前Ⅰ試験の対策には、手を抜かないことが必要です。

次は、午前Ⅱ試験です。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。その他には、技術要素のうちデータベース、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出題されます。令和4年度秋期から令和5年度秋期までの分野別の出題数は、図表13に示すとおりです。

大分類	中分類	令和4年度 秋期	令和5年度 春期	令和5年度 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

図表13 午前Ⅱ試験 分野別出題数

午前Ⅱ試験の分野別出題数は、これまでの傾向から判断すると、セキュリティ分野とネットワーク分野とを合わせて 20 問、データベース分野が 1 問という比率になっています。このため、技術要素から 21 問、開発技術とサービスマネジメントは、それぞれ 2 問の出題となっており、この比率は変化することはないでしょう。

なお、技術要素のうちセキュリティとネットワーク分野は、出題の重点分野であるほか、データベース技術を含めた技術知識については、午後試験対策を行う上で重要な位置付けにある技術知識です。このため、これら三つの分野の技術については、十分に学習していくことが必要です。そうすれば、午前Ⅱ試験で出題される技術要素分野の問題の多くには、かなり正解できると考えられます。例えば、技術要素の 21 問については、少なくとも 15 問以上は正解できるようになるでしょう。15 問正解できれば、合格基準点に達します。このため、午前Ⅱ試験は、単独の対策として実施していく必要はなく、午後対策にとっても必要になる詳細な技術知識を十分に身に付けていく方がよいと考えられます。

## (2) 午後試験

午後試験の試験時間は 150 分で、出題数 4 問の中から 2 問を選択して解答します。令和 5 年度秋期試験の午後試験の合格率は、42.2%（午前Ⅱ試験の通過者数 7,788 名に対する午後試験の合格者数 3,284 名の割合）でした。

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、できるだけ自分自身が得意とする分野の問題を選択することが基本です。また、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、午後試験の問題に取り組むに当たっては、問題に記述された内容を的確に把握できるように、できるだけ技術や知識のレベルを向上させる必要があります。例えば、次のような分野については、十分に学習するようにしましょう。

### ① Web システムの仕組み、システムが抱える様々な脆弱性に関する知識

HTTP リクエストとレスポンスでやり取りされる情報、HTML、cookie とその属性、システムが抱える脆弱性の問題（XSS、CSRF、SSRF、SQL インジ

- エクシジョン，パストラバーサル，クリックジャッキング，OS コマンドインジェクション，HTTP ヘッダーインジェクション，メールヘッダーインジェクションなど），セッション管理における問題（セッション固定化攻撃，リプレイ攻撃などの対策），セキュアプログラミング（Java，C++，ECMAScript（JavaScript）の言語）など
- ② クラウドサービスにおける認証連携の仕組み  
SAML，OAuth，OpenID Connect，state，nonce，ID トークン，アクセストークン，シングルサインオン，SaaS，IDaaS，DaaS など
  - ③ サイバー攻撃やマルウェア感染などのインシデント発生時における対応  
様々な攻撃手法とその手順，マルウェアの感染手順，マルウェアの振る舞い，マルウェアの動作の特徴など
  - ④ 認証技術と暗号化技術  
利用者認証，多要素認証，パスワードレス認証方式，メッセージ認証，デジタル署名，公開鍵証明書の種類とその検証方法，共通鍵暗号方式における暗号利用モード，ブロック暗号とストリーム暗号，鍵交換方式（DHE など）と PFS，離散対数問題など
  - ⑤ セキュリティプロトコルなど  
TLS 1.2 と TLS 1.3 の違い，IPsec，SSH，VPN 技術，IDS，IPS，ファイアウォールの設定など
  - ⑥ ネットワーク技術分野における知識  
DNS の仕組み，電子メールの配送の仕組み，迷惑メール対策などの電子メールに関するセキュリティ対策（SMTP-AUTH，SPF，DKIM，DMARC など），プロキシサーバ

ここで例示した項目は，ほんの一例にすぎません。以上のほかにも，JVN（Japan Vulnerability Notes）として公表されている脆弱性情報のうち重要なものや，情報セキュリティポリシーやリスク分析，JIS Q 27001，不正競争防止法などに関する知識も問われることがあります。

試験で出題される問題としては，Web 関連をはじめ，クラウド利用や認証連携，セキュリティインシデントをテーマとした問題が取り上げられることが多くなっています。例えば，クラウド利用というテーマによって問題が出題されたとしても，OAuth，OpenID Connect などを用いた認証連携の問題に特化したものは少

なく、Webサイトのサーバ証明書を利用するようなケースでは、サーバ証明書の検証方法、サーバ証明書に記載されるコモンネームの役割、クライアント側にインストールする必要があるものなど、複数の分野からの知識が問われるような問題が出題されます。つまり、午後問題は、複合的な観点から出題されるという特徴があるので、前述のキーワードだけを学習すれば十分であるとはいえません。

このため、前述のキーワードなどを手掛かりにして、一つ一つの技術知識の理解を深めていくことによって、理解の幅が必ず広がっていきます。このようなサイクルを繰り返し進めていくことによって、さらに幅広い関連する知識を、しっかりと身に付けることができると思います。こうして、試験に必要な知識を十分に身に付けていけば、午後試験を突破できる力が養われていくと考えられます。いずれにしても、支援士試験で合格するには、それなりの努力が必要ですから、地道に努力を重ねていくことを忘れないようにしましょう。一度、理解した技術知識でも、繰り返し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することも必要です。

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、問題の記述内容を正しく理解し、その範囲内で考えていくようにしましょう。そのためには、繰り返しになりますが、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いくことが必要です。また、午後試験は数十字程度の記述式で解答します。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解答を作成することが大切です。

以上のように、支援士試験で合格するには、それなりの努力が要求されますが、合格すれば、情報処理安全確保支援士（登録セキスペ）の登録資格を有することができます。そして、登録申請など所定の手続きを経れば、正式に情報処理安全確保支援士として認められ、活動していくことが期待されています。学習計画をしっかりと立てて、支援士試験に合格できるように努力していきましょう。

### 3-3 令和5年度秋期試験のデータ

#### (1) 午前Iの問題

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、ヒューマンインタフェース分野からは前回に続き出題がありませんでした。

これまで試験で出題されていない新傾向の問題は次の 5 問 (前回 3 問) でした。なお、問 18 のスコープ記述書は PMBOK®ガイド第 7 版からの初出題でしたが、問われていることは過去に出題された内容と同じです。

- ・問 5 IaC (Infrastructure as Code) に関する記述
- ・問 16 開発環境上でソフトウェアを開発する手法 (ローコード開発)
- ・問 18 プロジェクト・スコープ記述書に記述する項目 (PMBOK®ガイド第 7 版)
- ・問 23 バックキャストの説明
- ・問 28 AI を用いたマシンビジョンの目的

これまで何回か出題されている定番の問題が 14 問程度ありましたが、前回の 17 問と比べて減っています。また、定番問題でも、タスク実行時間と周期、多数決回路、第三者中継のログ、スケジュール短縮日数など、少し難しい問題があり、全体として前回よりも少し難しかったといえます。

問題の出題形式は、文章の正誤問題が 15 問 (前回 19 問)、用語問題が 5 問 (前回 2 問)、計算問題が 2 問 (前回 2 問)、考察問題が 8 問 (前回 7 問) で、用語・考察問題が増え、文章問題が減っています。

高度試験の午前 I は出題範囲が広いので、対策としては、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。

出題内容を分野別に示します。□ で囲んだものは新傾向問題、下線を引いたものは過去に出題されたことのある定番問題です。

- ・テクノロジー分野……逆ポーランド記法、パリティビット、整列、投機実行、**IaC**、タスク実行時間と周期、多数決回路、レンダリング、DBMS 障害対応、IP アドレス、マルチキャスト、レインボーテーブル攻撃、第三者中継、コーディネーションセンター、DKIM、**ローコード開発**、IDE
- ・マネジメント分野……**プロジェクト・スコープ記述書(PMBOK®ガイド第 7 版)**、スケジュール短縮日数、サービス停止時間、バックアップ方式、伝票入力の監査手続
- ・ストラテジ分野……**バックキャスト**、SOA、ファウンドリーサービ

ス、人口統計的変数、オープンイノベーション、マシンビジョン、故障要因の表現に適した図、匿名加工情報の第三者提供

出題される内容の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問題です。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ですが、午前Ⅰ試験から受験する人は、試験対策として、過去の応用情報技術者試験の午前問題を、余裕をもって7割以上正解できるよう確実に実力を付けてください。

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試験から受けた人で60点以上取れた人は5割前後で推移していて、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。出題元の応用情報技術者の午前問題は細かい内容で難しいことが多いので、苦手な分野の学習では一つレベルが低い基本情報技術者の問題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「2024 高度午前Ⅰ・応用情報 午前試験対策書」で効率良く学習することをお勧めします。

## (2) 午前Ⅱの問題

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5年度春期試験の7問から1問減って6問でした。

### 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 12 (脆弱性管理, 測定, 評価を自動化するため NIST が策定した基準), 問 13 (DNSSEC に関する記述), 問 14 (OAuth 2.0 に関する記述) の 3 問です。これに対し, 過去問題からの出題は, 令和 4 年度春期から 2 問, 令和 3 年度秋期から 1 問, 令和 2 年度秋期から 1 問, 令和元年度秋期から 2 問, 平成 31 年度春期から 1 問, 平成 30 年度秋期から 2 問, 平成 29 年度秋期から 1 問, 平成 26 年度秋期から 1 問の計 11 問です。このほか, 令和 2 年度秋期 AU 試験, 令和元年度秋期 SG 試験, H31 年度春期 ES 試験から 1 問ずつ出題され, これらのうち, MITB 攻撃や SAML の問題は, 同種の問題が SC 試験でも出題されていましたが, 細かい内容を問うものでしたから, 難度の高い問題といえます。なお, 過去問題からの再出題は, これまでは 3 期前に当たる過去問題からの出題数が最も多いという傾向がありましたが, 令和 5 年度秋期試験では, 複数の期にわたって, 1 問ないしは 2 問のように分散していることが特徴です。

ネットワーク分野の 3 問は, 新規問題が 2 問で, 過去問題は 1 問でした。新規問題は, 問 19 (宛先として使用できるマルチキャスト IP アドレス), 問 20 (IP アドレスの重複確認に使用されるプロトコル) ですが, 問 20 はレベル 4 の問題といえるでしょう。過去問題は, 問 18 (サブネットマスク) は, 平成 20 年度秋期 NW 試験で出題されていました。今回は, 3 問とも IP アドレスに関する問題だったことが特徴です。

データベース分野の問 21 (DBMS のデータディクショナリ) は基本的な用語で, レベル 3 の問題といえます。

## 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 (システムに意図的な障害を起こして信頼性を高める手法) は新規問題ですが, 用語の選択問題ですから, 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 (アジャイル開発手法のスクラムの説明) は令和 2 年度秋期 AP 試験で出題されていましたが, 内容的にみてレベル 4 の問題と評価されます。

## 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 (JIS Q 20000 を適用している組織が定めた間隔で実施す

るもの)は令和4年度春期SM試験で、問25(監査人が報告すべき指摘事項)は平成30年度春期SC試験で出題されていましたが、どちらもレベル3の問題といえます。

### (3) 午後問題

午後試験は、4問の中から2問の選択になり、選択の自由度が増すと思われました。しかし、令和5年度秋期試験では、問1がHTMLに特化した問題、問4がリスクアセスメントに特化していたことから、かなり制約があったと思われまます。また、これまでの午後I試験や午後II試験では、それぞれの段落に対応して設問が設定される形式でしたが、今回の問1と問4は、このような区別はなく、問題全体に対して複数の設問が設定される形式になっていたことが特徴といえます。

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必要です。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ので、過去に出題された、午後Iや午後II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 Webアプリケーションプログラムの開発

HTMLに含まれるスクリプトによって、格納型XSS脆弱性が引き起こされる事例に関する問題です。具体的には、XSS脆弱性を防ぐ基本的な対策、入力文字数制限を超える長さのスクリプトが実行されるようにする方法、問題で提示されているスクリプトの処理内容、そのスクリプトによって攻撃者がアップロードされた情報を取得する方法と、それを悪用する攻撃の例、Same Origin Policyの効果などが問われています。問題で提示されているスクリプトの意味を十分に理解できるだけの知識を有していれば、得点しやすい問題といえます。

#### 問2 セキュリティ対策の見直し

本問のテーマは、セキュリティ対策の見直しですが、段落ごとに設問が設定されるという、これまでの出題形式を踏襲した問題です。設問1では、サーバ証明

書の検証に失敗したときに出力されるエラーメッセージ、そのエラーメッセージが表示される直前までの Web ブラウザの動きが問われています。設問 2 は、ファイルのダウンロードを可能にするためのファイル共有機能の運用方法などを答えるものです。設問 3 は、秘密鍵の取り扱い方と、TPM に格納する方法が安全である理由、従業員用無線 LAN と来客用無線 LAN を分離するために NAT の設定を変更する方法などを答えるものです。基本的な知識を十分に把握していれば、かなりの設問に正解できそうです。

### 問 3 継続的インテグレーションサービスのセキュリティ

継続的インテグレーションサービスのセキュリティを題材にした問題ですが、問 2 と同様に、これまでの出題形式を踏襲した問題です。設問 1 は、コンテナによる仮想化の脆弱性を悪用しなくても成功する例を、解答群の中から全て選ぶものです。設問 2 は、TOTP を用いた場合に、攻撃者が不正ログインする方法、中間者攻撃を受けた場合、WebAuthn では、不正ログインできない仕組みなどが問われていますが、これらは、平成 31 年度春期午後 I 問 2 で同様の内容が出題されています。ドメインフロンティングや CAA レコードも過去問題で見ることができた用語です。設問 3 は、コード署名に関する問題ですが、問題の記述内容をどれだけ正確に把握し、解答を作成していけるかがポイントといえます。難易度は、やや難と想定されます。

### 問 4 リスクアセスメント

これまで出題されることが少なかったリスクアセスメントに特化した問題です。また、出題形式は、問 1 と同様に、段落対応に設問が設定されるものではなく、情報処理安全確保支援士が作成したリスクアセスメントの結果の表を埋める形式でした。解答箇所は、空欄ア～エ、空欄あ～き、空欄 a、b の 13 個で、文字数の指定がない字句を答える問題が四つ、該当する項番を全て選ぶものが四つ、リスクレベルの判定を示す文字を○で囲むものが五つです。該当する項番を全て選ぶものは、項番で説明されているセキュリティの状況をどのように解釈するかによって、選ぶ項番に差異が出やすいので、完答することは難しいと思われます。このため、四つの字句を答える問題にどれだけ正解できるかが合格基準点をクリアするためのポイントといえます。