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。

こうした背景の基に，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，これまでの情報セキュリティスペシャリスト試験の流れをそのまま受け継ぐものですから，午前Ⅰ，午前Ⅱ，午後Ⅰ，午後Ⅱという四つの試験が行われることには変わりありません。

令和 3 年度春期（第 8 回）から令和 4 年度春期（第 10 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 8 回までは 18.5%から 21.2%まで向上しましたが，第 9 回，第 10 回とも，約 1%ずつ低下しています。そして，IPA の発表によりますと，令和 4 年 4 月 1 日現在，“登録セキスペ”の登録者数は 20,253 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ます。

年　度	応募者数	受験者数	合格者数
令和 3 年度春期	16,273（-2.0%）	10,869（66.8%）	2,306（21.2%）
令和 3 年度秋期	16,354（0.5%）	11,713（71.6%）	2,359（20.1%）
令和 4 年度春期	16,047（-1.9%）	11,117（69.3%）	2,131（19.2%）

（　）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 3 年度春期から令和 4 年度春期までの 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がクリアできれば，比較的多くの受験者はクリアできるレベルのものと考えられます。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 3 年度春期	55.9%	90.2%
令和 3 年度秋期	47.9%	80.4%
令和 4 年度春期	56.6%	87.4%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

令和 4 年度春期の午前Ⅰ試験の合格率は，令和 3 年度秋期に比べると約 9 ポイント向上するとともに，令和 3 年度春期に比べても約 1 ポイント向上しています。特に，令和 4 年度春期試験は，これまでの 10 回の試験において，第 3 回（平成 30 年度春期試験）の合格率 58.2%に次ぐ高い合格率でしたが，依然として約半数の受験者が，午前Ⅱ試験の受験資格を失っています。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を十分に把握して試験に臨むことが必要です。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，87.4%でした。支援士試験はこれまで 10 回実施され，最近の第 6 回から第 10 回までは，第 9 回を除き，いずれも 85%～90%で推移しています。特に，午前Ⅱ試験の出題内容は，過去問題からの再出題が多いことが特徴ですから，過去問題を中心にしっかり学習していけば，午前Ⅱ試験は比較的容易に合格できると考えられます。このため，午前Ⅰ試験のように特段の対策を考える必要はないでしょう。例えば，午前Ⅱ試験の対策としては，3 期前や 4 期前に行われた試験の問題（令和 4 年度秋期試験では令和 3 年度春期試験や令和 2 年度 10 月試験の問題）を中心に，それ以前の過去問題を重点的に学習しておくとよいでしょう。その半面，新規問題が増加したり，レベル 4 の出題数が増加したりすると，令和 3 年度秋期試験のように合格率は低下する傾向が見られます。このため，初めて支援士試験を受験される方は午前Ⅱ試験を軽視しないことも必要です。

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 3 年度春期から令和 4 年度春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 3 年度春期	令和 3 年度秋期	令和 4 年度春期
テクノロジ系（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	3	2	2
	サービスマネジメント	2	3	3
ストラテジ系（8 問）	システム戦略	3	3	3
	経営戦略	4	3	3
	企業と法務	1	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。この他には，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 3 年度春期から令和 4 年度春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 3 年度 春期	令和 3 年度 秋期	令和 4 年度 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

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，ネットワークは，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は，ほぼ全問正解できるレベルになってくると考えられます。例えば，技術要素から 21 問出題された場合には，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，特別な対策を実施する必要はなく，午後対策に必要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Ⅰ試験，午後Ⅱ試験

午後Ⅰの試験時間は 90 分で，3 問の中から 2 問を選択して解答します。第 1 回から第 5 回までの試験では，3 問のうち 1 問は，Web サイトのセキュリティないしはセキュアプログラミングに関する問題が出題されていました。また，最近の傾向としては，DNS や電子メールなどのネットワークに関するセキュリティ問題の比重が高くなっているほか，クラウドセキュリティや認証連携，セキュリティインシデントをテーマとした問題が出題されています。このため，できるだけ Web サイトに関連する様々な脆弱性や HTML，cookie，セキュアプログラミングなどの知識をはじめ，DNS や電子メールなどネットワークに関する知識，SAML や OAuth，マルウェア感染における対処方法などの関連知識を身に付けておくことが大切です。

そして，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も必要です。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，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，セキュリティ技術では，Web アクセスに関する様々な技術知識，サイバー攻撃とその対策に関する知識，クラウドサービスにおける認証連携の仕組み，IoT に関するセキュリティなどといった最近の動向に加え，マルウェアに関する問題では，その問題で説明されたマルウェアはどのように振る舞い，その動作の特徴は何かなどを的確に把握していくことが必要です。そして，これらに関する知識を十分に深めていくためには，基礎となる利用者認証，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，暗号化技術などの知識を確実に理解しておくことが必要です。さらに，TLS や IPsec などの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，セキュアプログラミングなど，多くの技術知識を吸収していくことが必要です。また，ネットワーク技術分野では，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のほか，TCP/IP における基本的な技術知識など，幅広い技術を習得していく必要があります。そして，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やリスク分析などのマネジメント系の問題，JIS Q 27001 や JIS X 5070 などの標準化動向に関する問題も出題されることがありますので，幅広く知識を吸収していくことが必要です。こうした技術知識については，午後Ⅰ試験だけではなく，午後Ⅱ試験でも必要とされます。例えば，Web 関連のセキュリティは，午後Ⅱ試験では出題されやすいので，幅広く理解しておくことが必要といえます。

次に，午後Ⅱ試験です。試験時間は 120 分で，2 問の中から 1 問を選択して解答します。午後Ⅱは，問題分量が 10 ページ以上にわたりますので，問題をよく読んで，解答を導いていくという基本的な姿勢を貫くことが大切です。そうすれば，正解を導くことができる問題が必ず出てきます。情報セキュリティに関する一定の技術知識を身に付けた上で，午後Ⅱ試験では，「あわてず，あせらず，あきらめず」という精神で臨むことが必要です。

また，午後問題の特徴は，出題内容が一つの技術に絞ったものよりも，複合的な観点から出題されることです。この傾向は，午後Ⅱ問題では特に顕著になります。そこで，セキュリティとネットワークの相互に関連した総合問題に対応できる技術力を養っていくことが必要になります。しかし，幅広いこれらの技術を十分に習得していくには，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必要です。また，一度，理解しても繰り返し技術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するようにしましょう。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，問題の記述内容を正しく理解し，その範囲内で考えていくとよいでしょう。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必要です。

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３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。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。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 問から選択された問題になっています。以前から重点的に出題されているセキュリティ分野の問題が最も出題数が多く，これまでと同じ 4 問でした。

新傾向といえる問題は次の 3 問で，前回の 7 問と比較してかなり少なかったといえます。参考までに，午前Ⅰ試験問題の選択元になっている応用情報技術者試験（80 問）の新傾向問題は 14 問で前回の 20 問から減っています。

・問 5　アムダールの法則に基づいた，性能向上へ及ぼす影響
・問 13　複数の Web サーバにシングルサインオンを行うシステム
・問 24　投資によるキャッシュアウトをいつ回収できるかを表す指標

新傾向問題以外の内容としては，従来からよく出題されてきた定番の過去問題が 10 問程度あり，前回よりも多かったといえます。

問題の出題形式は，文章の正誤問題が 18 問（令和 3 年度秋期試験 15 問），用語問題が 7 問（令和 3 年度秋期試験 5 問），計算問題が 3 問（令和 3 年度秋期試験 2 問），考察問題が 2 問（令和 3 年度秋期試験 8 問）で，文章問題，用語問題，計算問題が増え，考察問題が減っています。全体として，新傾向問題が少なめで定番問題が増え，難易度が高くなる傾向のある計算問題と考察問題が計 5 問に減ったことから，例年よりも易しい内容だったといえます。

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。「」は新傾向問題，下線を引いた問題は過去に出題された内容と同じ問題です。

・テクノロジ分野……ハミング符号，リスト，Python，キャッシュメモリ，「アムダールの法則」，リアルタイム OS の機能，アクチュエータ，正規形，データマイニング，UDP，SDN，署名鍵，「シングルサインオン」，VDI サーバ，ファジング，判定条件網羅，保守の分類

・マネジメント分野……アーンドバリューマネジメント，最短日数，ITIL の保守性を表す指標，データ管理者，監査証拠

・ストラテジ分野……BPO，「キャッシュアウトの回収」，UML の図，PPM，ファウンドリ企業，XBRL，PM 理論，プログラム著作権

出題される内容の多くは，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ことがある基本的な問題です。高度系試験で専門分野の力を発揮するのは午前Ⅱ試験からになりますが，試験対策としては，過去の応用情報技術者試験の午前問題を解き，余裕をもたせて 7 割以上正解できるよう確実に実力を付けてください。

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は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「2022　高度午前Ⅰ・応用情報　午前試験対策書」での学習をお勧めします。

(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令和 3 年度秋期試験の 8 問から 2 問減少し，6 問になりました。全体的に難度の高い問題がほとんど見られなかったことから，難易度は易化したといえます。

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（攻撃者の行動のうち，偵察段階に分類されるもの），問 6（量子暗号の特徴）の 2 問です。これに対し，過去問題からの出題は，令和 2 年度秋期から 7 問，平成 30 年度秋期から 3 問，平成 29 年度秋期から 1 問のほか，令和 3 年度春期 AP 試験から 1 問，令和 2 年度秋期 AP 試験から 1 問，平成 30 年度秋期情報セキュリティマネジメント（SG）試験から 1 問，平成 29 年度秋期 AP 試験から 1 問の計 15 問でした。3 期前に当たる令和 2 年度秋期の過去問題からの出題が多かったことのほか，ほとんどがレベル 3 の問題であったことなどが今回の特徴といえます。

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 19（PC の時刻合わせに使用されるプロトコル）ですが，レベル 3 の問題です。過去問題は，令和 2 年度秋期 SC 試験と平成 29 年度春期 SC 試験からそれぞれ 1 問で，いずれもレベル 3 相当の問題です。

データベース分野の問 21（メタデータに関するデータリネージ）は新規問題であり，レベル 4 相当の問題と考えられます。

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（正しい入力を促しシステムを異常終了させない設計）は平成 29 年度春期エンベデッドシステムスペシャリスト（ES）

試験で出題されていましたが，レベル 2 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（ライフサイクルプロセスの修正又は新しく定義すること）は新規問題ですが，標準レベルの問題といえます。

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（IT サービスのサービス可用性計算）は令和 2 年度秋期 AP 試験で，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）は新規問題ですが，いずれもレベル 3 相当の問題といえます。

(3) 午後 I の問題

午後 I 試験は，3 問の中から 2 問の選択です。午後 I 試験は，令和元年度秋期試験以降，4 期続けて出題されていなかった Web 関連のセキュリティ問題が 2 問出題された半面，ネットワークセキュリティに関連した問題の出題比率が大きく低下しました。また，問題の難易度については，令和 3 年度秋期試験と同様に，基本的な知識を問うものが比較的多く見られましたので，前回とほぼ同程度と考えられます。このため，問題文に記述された内容を丁寧に読んで，条件などを整理した上で，設問で問われていることを的確に把握し解答を作成していくことが必要です。

令和 3 年度秋期 SC 試験の穴埋め問題は，空欄に入れる字句を答える形式がほとんどでしたが，今回は，字句選択方式で答えるものが増加していましたので，正解を得られやすいと思われます。一方，各問とも解答する小問数については，前回試験と同様に，少なめでしたから，些細なミスで得点を失わないようにすることが必要だったと思われます。

問 1　Web アプリケーションプログラム開発のセキュリティ対策

本問は，Web アプリケーションの典型的な脆弱性と Java プログラミングに関する問題です。設問 1 は，改行コードを意味する文字列，SQL インジェクション対策で使用される“？”の名称などを答える基本的な知識問題です。設問 2 は，情報選択機能の脆弱性について，プロジェクトに参加していない利用者が，そのプロジェクトに参加しているように見せかける操作方法，その操作方法からセッション情報を利用する方法に変更すると解決できる理由を述べるほか，Java の基

本的なコードに関する問題です。設問 3 は，テーブル検索における条件式を解答するものです。基本的な問題が多いので，Web 関連技術者にとっては，易しいレベルの問題といえます。

問 2　セキュリティインシデント対応

本問のテーマは，セキュリティインシデント対応ですが，内容的には，ネットワークセキュリティ，WebShell などの知識が必要になる問題です。設問 1 は，DNS のリソースレコード，UPnP 機能を有効とした場合のセキュリティ上の問題，NAS（Network Attached Storage）がランサムウェアに感染した根拠の理由を述べるものです。設問 2 は，基本的な Web の脆弱性を答えるものです。設問 3 は，GET メソッドと POST メソッドの違い，Linux の tar コマンドのオプションが悪用されるのを防ぐ対策を述べるものです。設問 4 は，インターネットの検索エンジンで検索されないようにするための指定方法を答える穴埋め問題です。一部，難度の高い設問がありますので，基本的な設問ではミスをしないことがポイントといえます。

問 3　スマートフォン向け QR コード決済サービスの開発

本問のテーマは，スマートフォン向け QR コード決済サービスの開発ですが，eKYC（electronic Know Your Customer；電子本人確認）における身元確認と当人認証，スマートフォンにおける QR コード決済に関する問題です。設問 1 は，本人確認に関する穴埋め問題ですが，安易に考えないようにすることが必要です。設問 2 では，銀行口座とのひも付け処理において，攻撃者が他人の銀行口座とのひも付け処理を成功させる方法，身元確認方法に関する穴埋め問題，マイナンバーカードに記録された署名用電子証明書の扱いなどが出題されています。設問 3 では，スマートフォンが不正利用されるケースと，その不正利用を防ぐための機能を述べるものです。一部，具体的な方法をあらかじめ知らなければ答えにくいものもありますが，比較的取り組みやすい問題といえます。

(4) 午後Ⅱの問題

午後Ⅱ試験は，問 1 が Web サイトのセキュリティ，問 2 がクラウドサービスへの移行というテーマでした。問 1 は，Web サイトの脆弱性に関する問題が大半を占めており，開発プロセスの見直しに関する改善方法を述べる問題などが一部

含まれていますが，Web 関連技術を中心に対策を行ってきた受験者にとっては取り組みやすい問題になっています。問 2 は，CDN の構成やドメインフロンティング攻撃の考え方，シングルサインオンの実現方式と認証連携などに関する問題ですが，多くの設問は穴埋め問題の形式で出題されていたことが特徴です。

今回の試験では，問 1，問 2 とも字句選択式の穴埋め問題が多く見られ，解答しやすい形式になっていましたので，解答できそうな設問に対しては，着実に得点を積み上げていくことが求められます。知識問題も幾つか見られましたが，問 1，問 2 とも，問題文をよく読んで，条件などを十分に整理した上で解答を考察していけば，合格基準点をクリアすることは，それほど難しくはないと思われます。

問 1　Web サイトのセキュリティ

本問は，Web サイトのセキュリティというテーマのとおり，出題内容としては，Web サイトの脆弱性対策を中心にした問題です。設問 1 では，XSS 脆弱性を確認するための診断用リクエストと，その再発防止策が問われています。設問 2 は，CSRF 脆弱性の原因となる根拠を示すものです。設問 3 は，クリックジャッキング脆弱性に関する字句選択問題です。設問 4 と設問 5 は，サーバサイドリクエストフォージェリ（SSRF）脆弱性の確認方法と，リダイレクト先の URL や SSRF 脆弱性への対策を述べるものです。設問 6 は，四つの小問がありますが，基本的に問題文の記述内容を基にして答えるものが多いので，どの記述が該当するかを見極めながら解答を作成していくことがポイントです。Web の脆弱性に関する一定の知識があれば，合格基準点をクリアすることは，それほど難しくないでしょう。

問 2　クラウドサービスへの移行

本問は，クラウドサービスへの移行をテーマにしていますが，設問 1 は，CDN の利用について，HTTP の Host ヘッダの使い方や，ドメインフロンティング攻撃などに関するやや専門的な知識が要求される問題です。設問 2 は，Kerberos 認証に関するもので，ST（Service Ticket）の偽造を認証サーバで検知できない理由と，総当たり攻撃はサーバ側でアカウントロックを有効にしていても対策にならない理由が問われています。設問 3 から設問 5 までは，字句選択などの穴埋め問題のため，解答しやすいといえます。設問 3 は，SAML 認証による連携の仕

組みで，平成 29 年度春期 SC 試験の午後 I 問 3 で，設問 4 は，OAuth 2.0 に関するもので，令和 3 年度春期 SC 試験の午後 I 問 1 で出題されていました。設問 5 は，OpenID Connect に関するもので，若干専門知識が必要なものがありましたが，問題の説明を理解しながら，丁寧に取り組んでいくとよいでしょう。