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 5 年度春期（第 12 回）から令和 6 年度春期（第 14 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 13 回までは 18.5%から 21.9%までの範囲に向上しました。今回の合格率は 18.3%と，第 4 回以降では最も低い合格率でした。そして，IPA の発表によりますと，令和 6 年 4 月 1 日現在，“登録セキスペ”の登録者数は 22,692 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 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%）
令和 6 年度春期	19,565（−4.2%）	14,342（73.3%）	2,624（18.3%）

（　）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 5 年度春期から令和 6 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 5 年度春期	52.5%	80.3%
令和 5 年度秋期	47.9%	68.6%
令和 6 年度春期	48.2%	75.2%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

令和 6 年度春期の午前Ⅰ試験の合格率は，令和 5 年度秋期に比べても 0.3 ポイント向上したに過ぎず，これまでの全 14 回の試験においても，低い合格率といえます。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，最新の知識などを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，75.2%でした。令和 5 年度秋期に比べると，6.6 ポイ

ント向上しましたが，以前の合格率に比較すると，低い部類に入るといえます。午前Ⅱ試験の合格率が，午前Ⅰ試験の合格率に比較して高い要因の一つに，過去問題からの再出題が多いことが挙げられますので，過去問題の学習は欠かせません。加えて，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 5 年度春期から令和 6 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 5 年度春期	令和 5 年度秋期	令和 6 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	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，日頃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 5 年度春期から令和 6 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 5 年度春期	令和 5 年度秋期	令和 6 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 6 年度春期試験の午後試験の合格率は，32.7%（午前Ⅱ試験の通過者数 8,053 名に対する午後試験の合格者数 2,624 名の割合）でした。令和 5 年度秋期試験の 42.2%に比較すると，約 10 ポイント低下しています。これは，令和 6 年度春期試験では，4 問中，3 問が Web 関連の知識を要求されるというように，出題分野に偏りが見られたことが主な要因であると思われます。

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，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 インジェクション，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サブジェクト代替名（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６年度春期試験のデータ

(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，マルチメディア分野からの出題は今回ありませんでした。

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 4 問（前回 5 問）でした。なお，問 21 のシステム監査基準は令和 5 年版での出題ですが，問われていることは基本的な内容です。

・問 3　再帰処理を 2 分木の根から始めたときの出力
・問 4　量子ゲート方式の量子コンピュータの説明
・問 12　3D セキュア 2.0 で利用される本人認証の特徴
・問 21　システム監査基準において総合的に点検・評価を行う対象

これまで何回か出題されている問題が 18 問程度あり，前回の 14 問から増えましたが，それ以前の傾向に戻ったといえます。なお，これらの問題の中で，オブジェクト指向のクラス間の関係，EVM，調達関連の EMS などは少し難しい問題でしたが，全体として例年どおりの難易度だったといえます。

問題の出題形式は，文章の正誤問題が 15 問（前回 15 問），用語問題が 4 問（前回 5 問），計算問題が 5 問（前回 2 問），考察問題が 6 問（前回 8 問）で，計算問題が増え，用語・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頃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。

・テクノロジ分野……待ち行列（平均待ち時間），ハミング符号，□2 分木の再帰処理□，□量子コンピュータ□，システムの信頼性設計，デッドロック，論理回路，アウトラインフォント，ストアドプロシージャ，CSMA/CD 方式，誤りが含まれるパケット個数，□3D セキュア 2.0□，公開鍵の総数，PSIRT，IPsec，クラス間の関係，ゴンペルツ曲線

・マネジメント分野……EVM，期待金額価値，サービスレベル管理，システム監査基準で点検・評価を行う対象，全般統制と業務処理統制
・ストラテジ分野……SOA，EMS，コンティンジェンシープラン，業界を分析するフレームワーク，フィージビリティスタディ，エッジコンピューティング，損益分岐点売上高，不正競争防止法

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 点以上取れた人はおおむね 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 1 レベル易し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を重点的に解説したアイテック刊行の「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。

(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 年度秋期試験の 6 問から 2 問増えて 8 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 7（ISMAP-LIU クラウドサービス登録規則に関する記述），問 8（Open CSIRT Foundation が開発したモデル），問 14（IEEE 802.1X におけるサプリカント），問 17（ソフトウェア脆弱性管理のツールとして利用される SBOM）の 4 問です。これに対し，過去問題からの出題は，令和 4 年度秋期から 6 問，令和 4 年度春期から 1 問，令和 3 年度秋期から 2 問，令和 3 年度春期から 2 問，平成 31 年度春期から 1 問，平成 26 年度春期から 1 問の計 13 問です。なお，過去問題からの再出題については，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という特徴がありましたが，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（Web サーバからの応答内容を保持させない HTTP ヘッダー）ですが，レベル 3 の問題といえるでしょう。過去問題は，平成 28 年度春期から 1 問，平成 27 年度春期から 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，新規問題ですが，SQL 文の条件をよく確認すれば正解できるので，レベル 2 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（成果物の振る舞いを机上でシミュレートして問題点を発見する手法）は，令和 4 年度秋期 AP 試験で出題されていました。基本的な用語問題ですから，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（ソフトウェアの品質確保に用いる形式手法の検証方法）は新規問題で，レベル 3 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（逓減課金方式を表すグラフ）は令和 2 年度秋期 AP 試験で出題された問題ですが，常識的なものですから，レベル 2 といえます。問 25（財務報告に係る内部統制の評価及び監査に関する実施基準）は新規問題で，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ていました。しかし，令和 6 年度春期試験では，4 問中，3 問が Web 関連の問題でしたから，Web 関連のセキュリティ問題を得意とする受験者を除き，選択の自由度は全くなかったといっても過言ではありません。また，従来の試験では，記述式の設問では字数制限が設けられていましたが，令和 6 年度春期試験においても，令和 5 年度秋期試験に続き，字数指定のない設問が，随所に見られました。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，攻撃の手順などを分かりやす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。これからの支援士試験では，字数指定のない設問が定着するかもしれません。

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　API セキュリティ

本問は，API セキュリティというテーマによって出題されています。設問 1 は基本的な用語問題でした。設問 2 は，総当たり攻撃に要する時間の計算，JSON Web Token の検証内容，アクセスコントロールの不備を補うための対策，2 要素認証を突破されないようにするための対策などが問われています。設問 3 は，作成した検証コードを確認する仕組み，WAF のルールを記述するために用いる正規表現を用いた記述形式，WAF ルールの動作を“遮断”ではなく“検知”にすることによる利点と，“検知”に設定した際の被害を最小化するために実施すべき

内容を答えるものです。少なくとも HTTP リクエストによってやり取りされる情報などを理解していることが必要ですが，問題の条件を十分に読みこなすことができれば，ある程度の設問には正解できそうな問題といえます。

問2　サイバー攻撃への対策

本問は，サイバー攻撃への対策というテーマによって出題されています。設問 1 では，HTTP GET Flood 攻撃の例を，攻撃対象を示して具体的に答えるもののほか，アノマリ型 IPS 機能でトラフィック量をしきい値によって制御する場合，しきい値を低く設定した場合の弊害などが問われています。設問 2 では，多要素認証を狙った攻撃例において，攻撃者が不正な接続を行うまでの攻撃手順を具体的に答えたり，罠サイトへのリンクをクリックした場合，不正なリモート接続をされないようにする注意喚起の内容を答えたりするものです。これらはいずれも字数指定がないので，採点者に理解されやすい文章を記述することがポイントといえます。設問 3 は，VPN ゲートウェイの接続制御に関する問題で，問題の条件をよく確認しながら解答を作成することがポイントといえます。設問 4 は，DDoS 攻撃に対して外部のサービスを利用する例や，取引先 Web サーバについて，DDoS 攻撃の影響が軽減できる理由を述べたりするものです。比較的，オーソドックスな問題であったといえます。

問3　Web セキュリティ

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。問われている内容も，クロスサイトスクリプティング，クロスサイトリクエストフォージェリ，認可制御の不備，サーバサイドリクエストフォージェリ（SSRF）の脆弱性が取り上げられています。IPA が公開している「安全なウェブサイトの作り方」などの資料に加え，HTTP リクエストやレスポンスにおけるヘッダー情報，cookie の属性などを十分に学習したり，Web サイトに関連する過去問題（例えば，SSRF は令和 4 年度春期 SC 午後Ⅱ問 1）を十分に学習したりしてきた受験者にとっては，取り組みやすい問題だったといえます。

問4　Web アプリケーションプログラム

本問は，個人顧客から注文を受け付けるための Web システムを構築するに当たって，既存の業務システムとのデータ連携を行う機能と，Java コードによって記

述されたユーザー登録機能のセキュリティレビューにおいて指摘された脆弱性及びその修正案を考える問題です。問題の大半は，ユーザー登録機能のセキュリティレビューに関するものなので，少なくとも Java コードを正確に読み取ることが必要になるほか，表 1 の Web 受注システムの要件を的確に把握し，解答を考えていくことがポイントといえます。