3　令和 4 年度春期の試験に向けて

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 2 年度から令和 3 年度秋期までの受験者数，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 7 回までは 18.5%から 19.4%まで向上しました。令和 3 年度春期（第 8 回）の試験では，過去最高の 21.2%になり，今回も 20.1%という高い合格率でした。そして，IPA の発表によりますと，令和 3 年 10 月 1 日現在，“登録セキスペ”の登録者数は 19,450 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 2 年度 10 月	16,597（-21.8%）	11,597（69.9%）	2,253（19.4%）
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%）

（ ）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 2 年度から令和 3 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 2 年度 10 月	52.8%	85.2%
令和 3 年度春期	55.9%	90.2%
令和 3 年度秋期	47.9%	80.4%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

令和 3 年度秋期の午前Ⅰ試験の合格率は，令和 3 年度春期に比べると 8 ポイント低下するとともに，2 期前に実施された令和 2 年度 10 月に比べても約 5 ポイント低下しています。特に、今回の試験は、これまでの全 9 回の試験において、第 2 回の合格率 47.9%と並んで最も低いものでした。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，80.4%でした。支援士試験はこれまで 9 回実施され，最近の第 6 回から第 8 回までは、いずれも 85%～90%で推移していましたが，今回は，これらの水準よりも低下しました。これは、レベル 4 相当の新規問題の出題数が増えたことが要因と考えられます。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 年度春期試験では令和 2 年度試験や令和元年年度秋期試験の問題）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，今回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あまり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 2 年度 10 月から令和 3 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，応用情報技術者試験で出題された 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 2 年度 10 月	令和 3 年度 春期	令和 3 年度 秋期
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	5	4	4
	技術要素	7	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	3	2
	サービスマネジメント	3	2	3
ストラテジ系（8 問）	システム戦略	3	3	3
	経営戦略	3	4	3
	企業と法務	2	1	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 2 年度 10 月から令和 3 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 2 年度 10 月	令和 3 年度 春期	令和 3 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，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。最近の傾向としては，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る傾向にあります。このため，できるだけ HTML や Cookie，セキュアプログラミング関連の知識を身に付けておくことが必要といえますが，問題を解くレベルまで到達するには，相当の時間と努力が要求されます。問題選択に当たっては，あらかじめセキュアプログラミングに関する問題を選択するかどうかを決めておくことがよいでしょう。このほか，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，試験を受験するに当たっては，できるだけ技術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，ディジタル署名，電子証明書の検証方法，暗号化技術などの知識を確実に理解しておくことも必要になります。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。

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，情報処理安全確保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 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 7 問で，前回の 2 問と比較してかなり増加しました。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 20 問と多く，従来よりも多くなっています。

・問 1　接線を求めることによる非線形方程式の近似解法
・問 4　16 ビット整数の加算結果でオーバフローしないもの
・問 5　物理サーバの処理能力を調整するスケールインの説明
・問 12　IoT セキュリティガイドラインにおける対策例
・問 24　テレワーク導入後 5 年間の効果
・問 27　リーンスタートアップの説明
・問 30　特別条項を適用する 36 協定届の事例

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少なかったといえます。

問題の出題形式は，文章の正誤問題が 15 問（前回 17 問），用語問題が 5 問（前

回 5 問），計算問題が 2 問（前回 2 問），考察問題が 8 問（前回 6 問）で，文章問題が減り，考察問題が増えています。全体として，新傾向問題も増え，定番問題が少なく，計算と考察問題の割合が 30 問中 10 問と増えたことから，例年よりも難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問題です。“ ”または“ ”と下線の両方が付いた問題は，これまでの高度共通午前Ⅰ試験であまり出題されていない内容を示しています。

・テクノロジ分野……「非線形方程式の近似解法」，パリティビット，“バブルソート”，「オーバフロー」，「スケールイン」，仮想記憶システム，半加算器，“関係演算”，データベースの障害回復，ARP，“ブロードキャストアドレス”，「IoT セキュリティガイドライン」，“否認防止”，“クレジットカードの不正利用防止”，“認証ヘッダと暗号ペイロードを含むプロトコル”，UML のアクティビティ図，バーンダウンチャート

・マネジメント分野…… “プレシデンスダイアグラム”，リスクの定量的分析，問題管理，バックアップの運用，システム監査技法

・ストラテジ分野……業務プロセスの改善，「テレワークの効果」，RFI，バリューチェーン，「リーンスタートアップ」，エッジコンピューティング，“マクシミン原理に従う投資”，「36 協定届の事例」

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。

出題範囲が広いため，全体をまんべんなく学習するのは時間がかかりすぎます。そのため，次回試験対策としては，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 1・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 年度春期試験の 6 問から 2 問増加し，8 問になりました。しかも，セキュリティとネットワーク分野の新規問題（8 問のうち，7 問）は，レベル 4 といえるものが多く，難易度は，前回よりも難化したといえます。

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 1（AI の特性を悪用し，判定結果を誤らせる攻撃），問 2（Pass the Hash 攻撃），問 3（PQC（Post-Quantum Cryptography）），問 4（SAML 認証の特徴），問 5（サイバーキルチェーンに関する説明），問 17（TLS1.3 の暗号スイート）の 6 問です。これに対し，過去問題からの出題は，令和元年度秋期から 4 問，平成 31 年度春期と平成 30 年度秋期からそれぞれ 1 問，平成 30 年度春期から 2 問，平成 29 年度秋期から 1 問，令和元年度秋期情報セキュリティマネジメント試験から 2 問の計 11 問でした。過去問題からの出題が全体的に少なく，新規問題の出題数が増加し，しかもレベル 4 の問題が多かったこと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 18（レイヤ 3 ネットワーク内にレイヤ 2 ネットワークを構築するプロトコル）で，少し難度が高いと思われます。過去問題は，平成 29 年度秋期 SC 試験から 1 問と，平成 30 年度秋期 NW 試験から 1 問で，いずれも標準レベルの問題です。

データベース分野の問 21（データベースの参照制約）は，平成 31 年度春期 SC 試験で出題されていました。

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（自身の経験に基づき動的に計画して進めるテストの方法）は平成30年度春期DB試験で出題されていました。ソフトウェア開発管理技術分野の問23（ブルーレイディスクのコンテンツ保護技術）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（フェールソフトの考え方）は令和元年度秋期SC試験で，問25（クラウドサービス上の情報消失の予防に関するチェックポイント）は令和元年度秋期AP試験で出題されており，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試験では，これまで毎回のようにWeb関連のセキュリティ問題が出題されていましたが，令和元年度秋期試験以降，今回も出題されませんでした。また，前回の試験では，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少し高く，専門知識が要求されるような問題もありましたが，今回は3問とも，基本的な知識を問うものが比較的多く見られました。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だったと思われます。

これまでの試験の穴埋め問題は，ほとんど字句選択方式で出題されていましたが，今回の試験では，空欄に入れる字句を答える形式でしたから，この点に関しては難度が上がったといえます。各問とも解答する小問数については，比較的多く設定されていましたので，問題の条件などを十分に把握して問題に取り組めば，どの問題も合格基準点をクリアすることはそれほど難しくないと思われます。

問1　セキュリティインシデント

本問は，保守用PCを使って顧客管理サーバを保守するシステムにおいて，セキュリティインシデントが発生した事例について，顧客管理サーバの保守方法やセキュリティインシデントの再発防止策を考察する問題です。設問1は，SSH接

続する際に警告メッセージが表示され，接続が切断された場合に想定される状況を述べるものだけが，専門知識を要求されますが，その他は基本的な知識があれば正解できそうです。設問 2 は，セキュリティインシデントが発生したときの状況を，問題文の記述に基づいて特定するものです。設問 3 は，SSH の認証方式のうち，公開鍵認証を十分に理解していれば，多くの小問に正解できると思われます。難易度については，やや易のレベルといえます。

問 2　システム開発での情報漏えい対策

本問のテーマは，システム開発での情報漏えい対策ですが，内容的には，アクセス権限や暗号化，利用者認証などを中心とした問題です。設問 1 は，設計秘密の管理についての問題を，問題文の記述に基づいて考察するものです。設問 2 は，IRM（Information Rights Management）製品に関する特徴などを問題文の記述に基づいて考察するものや，暗号の強度や利用者認証を強化する仕組みなどを解答するものです。設問 3 は，設計秘密を不正に取得するマルウェアの動作を述べるものです。問題文を丁寧に読んで考えていけば，正解が得られる小問が多いといえます。日ごろからセキュリティに対する意識を十分に高めていれば，得点しやすい問題だったといえます。

問 3　PC のマルウェア対策

本問のテーマは，PC のマルウェア対策ですが，基本的な事項に関するものが多く出題されていたように思います。設問 1 では，PC がマルウェアに感染した際の初動対応や取得すべき情報のほか，問題文の記述を基にして，空欄に入れる字句を考えたり，追加調査の範囲を述べたりするものです。設問 2 は，FW のフィルタリングルールの変更や，URL フィルタリングルールの基本的な問題です。設問 3 は，あらかじめ登録した実行ファイルだけの実行を許可する仕組みに関するもので，特に設問 3 (2)は，若干難度が高いと感じられました。全体の難易度を評価すると，やや易のレベルといえます。

(4) 午後 II の問題

午後Ⅱ試験は，問 1 が協力会社とのファイルの受渡し，問 2 がマルウェア感染への対処というテーマでした。問 1 は，XSS 脆弱性に関する問題が約 4 割，残りの約 6 割がクラウドサービスを利用する際の留意点，パスワードや利用者 ID に

対する総当たり攻撃，FIDO 認証を用いた IDaaS との連携に関する問題となっています。問 2 は，テレワーク実施に当たっての役割の決定，ネットワーク構成の見直しに当たっての検討，マルウェアの特徴に基づく動作に関する問題などが出題されており，日ごろから情報セキュリティ全般について，地道に学習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思われます。

今回の試験でも，前回（令和 3 年度春期試験）に引き続き，小問数が少し多めに設定されていましたので，解答できそうな設問を見極め，確実に得点を積み上げていくことが必要です。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　協力会社とのファイルの受渡し

本問は，協力会社とのファイルの受渡しをテーマとしていますが，出題内容としては，設問 1 で XSS 脆弱性に関する基礎知識の問題が出題されています。設問 2 は，URL の出力処理における XSS 対策や，Content-Security-Policy に関する，やや専門的な問題です。設問 3 は，クラウドサービス利用時における字句選択問題と，受け渡すファイルの内容を保護するための措置を述べるもので，問題の条件を十分に加味する必要があります。設問 4 は，利用者 ID やパスワードに対する総当たり攻撃に関する基本的な記述式の問題です。設問 5 は，IDaaS との連携による多要素などに関するもので，中には少し専門知識が要求される問題もあります。前半の XSS 脆弱性に関する設問がある程度，正解できれば，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　マルウェア感染への対処

本問は，マルウェア感染への対処というテーマですから，問題文に記載されているマルウェアの特徴などを押さえながら解答を作成していくことがポイントです。設問 1 は，テレワーク実施に当たっての役割を決定する役職などの基本的な知識問題です。設問 2 は，ネットワーク構成に関するもので，問題の条件を確認すれば正解できるレベルの問題です。設問 3 は，DNS に関する知識が必要ですが，問題文を丁寧に読んでいけば，正解を導き出すことは可能であると考えられます。設問 4 も，設問に関連する問題文を丁寧に読んで解答を考えていくことが大切です。難易度を全体的に評価すると，やや易といえるでしょう。