

3. 第8回情報処理安全確保支援士試験に向けて

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。

平成 31 年度秋期から令和 2 年度までの受験者数、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、第 5 回とも 18%台に向上しました。今回の試験では、前回の試験と同様に過去最高の 19.4%になり、約 5.2 人に 1 人の割合で合格者が生まれることになりました。そして、IPA の発表によりますと、令和 2 年 10 月 1 日現在、“登録セキスペ”の登録者数は 19,752 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
平成 31 年度春期	22,175 (-1.2%)	14,556 (65.6%)	2,774 (18.9%)
令和元年度秋期	21,237 (-4.2%)	13,964 (65.8%)	2,703 (19.4%)
令和 2 年度	16,597 (-21.8%)	11,597 (69.9%)	2,253 (19.4%)

() 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

平成 31 年度春期から令和 2 年度までの 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
平成 31 年度春期	50.8%	79.8%
令和元年度秋期	51.9%	86.1%
令和 2 年度	52.8%	85.2%

図表 11 午前 I 試験と午前 II 試験の合格率の比較

令和 2 年度の午前 I 試験の合格率は、令和元年度秋期に比べると約 1 ポイント向上するとともに、2 期前に実施された平成 31 年度春期に比べても 2 ポイント向上しています。しかしながら、午前 I 試験の合格率は、支援士試験になって以来、一度も 60% を超えたことはなく、今回の 52.8% という数字も、決して高い合格率とはいえません。このため、午前 I 試験を受験する必要がある方は、図表 4 で示した、幅広い情報処理技術分野の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、85.2%でした。支援士試験はこれまで7回実施され、いずれも70%以上の合格率になっていますが、令和元年度秋期に次ぐ高い合格率でした。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。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3年度春期試験では平成31年度春期試験や平成30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、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。平成31年度春期から令和2年度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	平成31年 春期	令和元年 秋期	令和2年度
テクノロジー系 (17問)	基礎理論	3	4	3
	コンピュータシステム	4	4	5
	技術要素	8	7	7
	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修得するとともに、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がある方は、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。平成31年度春期から令和2年度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	平成31年 春期	令和元年 秋期	令和2年度
技術要素	セキュリティ	17	18	17
	ネットワーク	3	2	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ます。このため、できるだけ HTML や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とういでしょう。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をはじめ、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、最近の動向を的確

に把握していくことが必要です。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、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が必要になります。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、幅広い技術を修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ー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修得していくには、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く、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必要があります。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 令和元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、これまでと同じです。また、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 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。

また、新傾向問題といえるものは次の 8 問で（前回 6 問）、増加傾向にあった前回よりもさらに増えています。参考までに、午前 I 共通問題の選択元である応用情報技術者試験の新傾向といえる問題は 20 問もありました。

- ・問 3 オブジェクト指向のプログラム言語（Python）
- ・問 5 サーバコンソリデーションの説明
- ・問 6 仮想記憶方式のプリページングの特徴
- ・問 15 メール本文を含めて暗号化するプロトコル（IMAPS）
- ・問 17 アジャイル開発手法のスクラムの説明
- ・問 27 CPS（サイバーフィジカルシステム）を活用している事例
- ・問 28 企業システムにおける SoE の説明
- ・問 30 プロバイダ責任制限法が定める送信防止措置

問題の出題形式としては、文章の正誤問題が 14 問（前回 21 問）、用語問題が 7 問（前回 1 問）、計算問題が 5 問（前回 4 問）、考察問題が 4 問（前回 4 問）で、

文章問題がかなり減り、用語問題と計算問題が増えています。

新傾向以外の出題内容としては、基礎理論のコンパイラ理論（逆ポーランド記法）と符号理論の問題が少し難しかったですが、その他分野の問題は過去に何度も出題されている基本的な内容が多かったです。全体としては、新傾向問題が多かったため、少し難しく感じたと思われます。

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き、基礎知識を維持することが大切です。

出題内容全体を次に示します。下線を引いた問題（過去問）は午前Ⅰ試験であまり出題されていない内容ですが、基礎知識があれば、用語問題は消去法で、計算問題は丁寧に進めることによって解答できる内容が多いといえます。

- ・テクノロジー分野……逆ポーランド記法，符号理論，Python，メモリインタリーブ，サーバコンソリデーション，プリページング，DRAM，D/A変換，データモデル，伝送時間計算，グローバル IP アドレス，暗号化プロトコル，デジタル署名，暗号方式，メール暗号化プロトコル，アクティビティ図，スクラム
- ・マネジメント分野……EVM，リスク対応戦略，通減課金方式，可用性計算，監査証拠
- ・ストラテジ分野……投資効果，SOA，クラウドサービス，事業活動分析手法，CPS，SoE，売上高の計画，プロバイダ責任制限法

出題される内容は、過去の応用情報や基本情報技術者試験で出題されたことがある基本的な問題が大半を占めます。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。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。

そのために、過去に出題された問題を解いてみて、理解できていない内容を中心に学習することをお勧めします。また、AI、IoT、ビッグデータ、アジャイル関連は新しい用語が今後も出題が予想されるので、日ごろからこれらの話題には注目し、内容把握しておきましょう。

(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元年度秋期試験の 7 問から 1 問増え、8 問になりました。また、セキュリティとネットワークの 20 問を比較すると、新規問題は 6 問で、前回よりも 1 問増加しましたが、難易度はほぼ例年通りと考えられます

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。前回は、セキュリティが 18 問、ネットワークが 2 問という比率でしたが、分類上、どちらの分野にも入れることができる問題がありますので、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 問という比率が基本になっていると考えられます。

セキュリティ分野の 17 問のうち、全てが情報セキュリティ技術に関するもので、情報セキュリティ管理（マネジメント系）分野からの出題はありませんでした。新規問題は、問 6（“NOTICE”に関する記述）、問 7（サイバー・フィジカル・セキュリティ対策フレームワーク）、問 9（3D セキュアに関する記述）、問 14（FW のフィルタリングルールの変更）、問 17（IP25B に該当するもの）の 5 問です。いずれもレベル 3 の問題といえますが、問 17 では OP25B ではなく、IP25B が問われていますので、注意が必要です。これに対し、過去問題からの出題は、平成 30 年度秋期から 4 問、平成 30 年度春期から 3 問、平成 29 年度春期から 1 問、平成 28 年度秋期から 1 問、平成 28 年度春期から 1 問、平成 27 年度秋期から 1 問のほか、平成 28 年度秋期 NW 試験から 1 問の計 12 問でした。これまでは、過去問題は 3 期前（今回では平成 30 年度秋期が該当）の試験の中から、6、7 問出題されていましたが、今回 4 問に減少したことが特徴の一つです。

ネットワーク分野の 3 問は、新規問題が 1 問、過去問題（平成 26 年度秋期 SC 試験、平成 21 年度秋期 SC 試験）が 2 問でした。新規問題は問 18（DHCP で使用されるブロードキャストアドレス）ですが、レベル 4 の問題と考えられます。

データベース分野の問 21（コミット処理完了とみなすタイミング）は、平成 30 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間22（ソフトウェアの利用者を役割ごとに描いた仮想の人物）は新規問題ですが、ソフトウェア開発管理技術分野の間23（アジャイル開発でふりかえり（レトロスペクティブ）を行うタイミング）は平成30年度春期AP試験で出題されていました。

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（TCOが最小になるもの）は平成29年度春期AP試験で出題されていました。問25（監査人が指摘事項として監査報告書に記載すべきもの）は新規問題ですが、レベル3の問題です。

(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。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、前回（令和元年度秋期試験）に引き続き、今回も出題されませんでした。問1は、スマートフォンの決済アプリに関する問題でした。問2は、電子メールのセキュリティ対策の問題で、前回に引き続き、電子メールのセキュリティに関するものが出題されました。問3は、Webシステムのセキュリティ診断というテーマになっていますが、出題内容としては、診断を行う際の留意点などが問われています。

また、前回は、各問とも解答する小問数が比較的多く設定されていましたが、今回はかなり少なくなっています。このため、些細なミスをしてしまうと、合格基準点をクリアすることが難しくなってきます。いずれにしても、問題文に記述された内容や条件を十分に把握しながら、設問で問われていることに対して丁寧に取り組み、解答を作成していけば、合格基準点をクリアすることは決して難しくありません。

問1 スマートフォンを用いた決済

スマートフォン用ポイントアプリを使ったポイント付与サービスのセキュリティを考える問題です。設問1は、現状のバーコードを使用したポイント付与サービスにおいて、他者になりすます方法と、QRコードを検証する仕組みが問われ

ています。設問 2 は、無線 LAN ルータの設定を変更する方法と、仮想ホストにおけるサーバ証明書の検証方法が問われており、やや技術的な問題といえます。設問 3 は、パスワードリストをスクリーニングする方法を、問題の記述内容から考察するものです。問題の条件を確認しながら解答を作成していくことがポイントになりますが、難易度はやや易と判断されます。

問 2 電子メールのセキュリティ対策

前回に引き続き、電子メールのセキュリティ対策が出題されましたが、設問内容は異なっています。設問 1 は、プロトコルの名称を答えるという知識問題です。設問 2 と設問 3 は、メール転送の仕組みやメーリングリスト、S/MIME 証明書の知識が要求されます。例えば、メール送信者がメールを暗号化して受信者に送信しても、エンドーエンドでメールが暗号化できない理由や、S/MIME 証明書でメールを暗号化した場合、復号できなくなるのはどのような場合かなどが問われています。問 2 は、特に小問数が少なかったので、小問当たりの配点が高いことに注意することが必要です。

問 3 Web システムのセキュリティ診断

本問は、Web システムのセキュリティ診断をテーマとしていますが、Web 技術に特化した知識が要求されるものではなく、診断を実施する際のネットワーク型 IPS (N-IPS) の動作などを中心としたものです。設問 1 では、N-IPS の脅威通信判定を無効にすると、より多くの脆弱性を検出できる理由や、無効にするのではなく、N-IPS の設定変更によって対応する方法が問われています。設問 2 は、問題の条件を基にして、解答を考えるものですから、問題文を丁寧に読んでいくとよいでしょう。難易度については、やや易と判断されます。

(4) 午後Ⅱの問題

午後Ⅱ試験は、問 1 が百貨店における Web サイトの統合、問 2 がクラウドサービスを活用したテレワーク環境というテーマでした。問 1 は、Java コードに関する設問のほか、パスワード失念時における処理方法、サイト間における認証連携などが出題されていました。問 2 は、コロナ禍においては時宜を得たテーマですが、問題で記述されたテレワーク環境を実現するための要件が複雑でした。問 1、問 2 ともに、問題の条件を十分に整理した上で解答を考察していくことが必要です。

今回は、午後 I 試験と同様、前回の試験とは異なり、解答する小問数がかかなり少なくなっていました。小問当たりの配点が高くなりますので、問題文の条件を十分に確認しながら、根気よく解答を作成していくことが必要です。また、問 1、問 2 とも、セキュリティ上、どのような対応が必要かなどの前提知識から、解答する設問も幾つか見られました。十分に学習を積み重ねてきた受験者にとっては、解答しやすかったかも知れませんが、問題の条件をうまく整理することができなければ、合格基準点をクリアすることは、やや難しいと想定されます。

問 1 百貨店における Web サイトの統合

本問は、百貨店における Web サイトの統合をテーマとしたものですが、出題内容としては、設問 1 でアカウント情報を統合した後に必要となる FW の変更内容、設問 2 で事業継承に伴って取得した個人情報の取扱いに関する知識問題が出題されていました。設問 3 は、Java コードによるアカウントの紐付け処理の問題ですから、Java の経験がない受験者にとっては、厳しい設問でした。設問 4 は、パスワード失念時の操作画面における脆弱性を見つける問題とそれを解決する方法、アカウントを乗っ取られた際に発生する具体的な被害を述べるものです。具体的な被害については、解答しやすいと思いますが、パスワード失念時の操作画面における脆弱性を見つける問題とそれを解決する方法は、問題中に適切な内容の字句を入れる穴埋め問題として出題されており、少し解答を考えにくいものでした。設問 5 は、SP と IdP における連携処理に関するものですが、処理が図示されていますので、正解を導きやすいと思います。難易度を全体的に評価すれば、やや難といえます。

問 2 クラウドサービスを活用したテレワーク環境

本問は、クラウドサービスを活用したテレワーク環境というテーマですが、利用するクラウドサービスが、SaaS-X、IDaaS-Y、DaaS-V、MDM-W の四つありましたから、混乱しないように注意することが必要です。設問 1 は、OTP による 2 要素認証を実現するため、OTP の生成に使用する情報や、QR コードを表示する機能へのアクセスを E 社のネットワークからのアクセスに制限する理由のほか、VD、SaaS-X、IDaaS-Y の認証連携について考えるものでした。設問 2 は、ノート PC を介して社内情報を持ち出す方法を述べるもので、どのような場面を想定できるかがポイントになりそうです。設問 3 (1) は、マルウェアが社内情報を

取得する方法を述べるもの、(2)はテレワーク実証実験環境内のアクセスを必要最小限にする場合に許可するアクセス先を選ぶもので、比較的易しいと思われます。設問 4 はクラウドサービスプロバイダの脆弱性検査を確認する方法を述べるもの、設問 5 はフィッシングサイトで利用者の入力 that 詐取された場合、その情報を悪用した不正アクセスを防止できる根拠を述べるものです。設問 6 は、三つの小問が設定されており、(1)、(2)はやや常識的なものですから、設問 6 の得点によって合格基準点をクリアできるかどうかの分かれ目になりそうです。全体的に難易度を評価すれば、やや難といえます。

