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，そ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。しかし，IPA は，令和 4 年 12 月に支援士試験における出題構成等を変更し，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すると発表しています。

令和 3 年度秋期（第 9 回）から令和 4 年度秋期（第 11 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 10 回までは 18.5%から 21.2%まで向上しました。今回の合格率も 21.1%で，令和 3 年度春期試験の 21.2%に次いで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 4 年 10 月 1 日現在，“登録セキスペ”の登録者数は 20,744 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%）
令和 4 年度秋期	18,749（16.8%）	13,161（70.2%）	2,782（21.1%）

（ ）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 3 年度秋期から令和 4 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 3 年度秋期	47.9%	80.4%
令和 4 年度春期	56.6%	87.4%
令和 4 年度秋期	52.6%	73.0%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

令和 4 年度秋期の午前Ⅰ試験の合格率は，令和 4 年度春期に比べると 4 ポイント低下しましたが，令和 3 年度秋期に比べると約 5 ポイント向上しています。令和 4 年度秋期の合格率は，これまでの 11 回の試験において，ほぼ平均的といえますが，この数値からも分かるように，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，73.0%でした。最近の試験では，概ね 85%～90%で推移してきましたが，今回の合格率は，平成 30 年度秋期の 71.2%に次いで，低い合格率にとどまりました。問題の難易度は，過去問題からの出題数が多く，基本的な内容を問うものが多かったので，例年どおりの合格率になると想定していましたが，意外な結果だったと思います。午前Ⅱ試験は，過去問題を中心にしっかり学習していけば，比較的容易に合格できるレベルの内容ですから，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 5 年度春期試験では令和 3 年度秋期試験や令和 3 年度春期試験の問題）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，令和 4 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 年度秋期から令和 4 年度秋期までの分野別の出題数は，図表 12

分　野	大分類	令和 3 年度秋期	令和 4 年度春期	令和 4 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	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

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。

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 年度秋期から令和 4 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 3 年度 秋期	令和 4 年度 春期	令和 4 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。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。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，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４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午前の問題 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，今回もこれまでと同じ 4 問の出題でした。

新傾向といえる問題は次の 6 問で，前回の 3 問と比較してかなり増えています。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 15 問で前回の 14 問とほぼ同じでした。

・問 2　AI における過学習の説明
・問 4　2 段のキャッシュをもつキャッシュシステムのヒット率

・問 17　KPT 手法で行ったスプリントレトロスペクティブの事例
・問 19　多基準意思決定分析の加重総和法を用いた製品の評価
・問 25　ハードウェア製造の外部委託に対するコンティンジェンシープラン
・問 27　API エコノミーの事例

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といえる過去問題が 15 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 16 問（前回 18 問），用語問題が 5 問（前回 7 問），計算問題が 5 問（前回 3 問），考察問題が 4 問（前回 2 問）で，計算・考察問題が増え，文章・用語問題が減っています。今回は考える過去問題が多かったことから，難易度としては普通レベルだったといえます。

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……カルノー図，「AI の過学習」，データ衝突，「2 段キャッシュシステムのヒット率」，コンテナ型仮想化，デッドロック発生防止，論理回路，コードの桁数，前進復帰の障害回復，ACID 特性，DHCP サーバ，デジタル証明書失効確認，リスクアセスメント，WAF，無線 LAN セキュリティ，問題発見手法，「スプリントレトロスペクティブ」
・マネジメント分野……プレシデンスダイアグラム法，「加重総和法を用いた製品評価」，問題管理プロセス，監査報告書の記載事項，監査手続
・ストラテジ分野……BCP，投資効果，「コンティンジェンシープラン」，コンジョイント分析，「API エコノミー」，サイバーフィジカルシステム，事実やアイディアの収束技法，著作権の帰属

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試験からですが，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。

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「2023　高度午前Ⅰ・応用情報　午前試験対策書」で確実に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令和 4 年度春期試験の 6 問から 2 問増えて，8 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 1（メッセージ認証符号を付与したときの効果），問 6（パスワードスプレー攻撃に該当するもの），問 7（シングルサインオンに関する記述），問 9（セキュリティ評価結果に関する規格），問 11（クリックジャッキング攻撃に有効な対策）の 5 問です。これに対し，過去問題からの出題は，令和 3 年度春期から 2 問，令和 2 年度秋期から 2 問，令和元年度秋期から 1 問，平成 31 年度春期から 2 問，平成 30 年度秋期から 1 問のほか，令和 3 年度春期 NW 試験から 1 問，令和 2 年度秋期 AP 試験から 1 問，令和元年度秋期 NW 試験から 1 問，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，3 期前に当たる令和 3 年度春期の過去問題からの出題数が多いという傾向がありましたが，今回は，各期からの出題数がほぼ均等に割り振られていたほか，ほとんどがレベル 3 の問題であったことなどが特徴といえます。

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（IPv6 の特徴）ですが，レベル 3 の問題です。過去問題は，令和元年度秋期 NW 試験と平成 28 年度秋期 NW 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（SQL 文を実行した結果（LEFT OUTER JOIN））は新規問題ですが，LEFT OUTER JOIN を知っているかどうかが正解するポイントといえます。

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（判定条件網羅（分岐網羅））は令和 3 年度春期 SA（システムアーキテクト）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（SD メモリカードに使用される著作権保護技術）は令和元年度秋期 NW 試験で出題されており，いずれもレベル 3 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（最も投資利益率の高いシステム化案）は新規問題で，問 25（SaaS へのアクセスコントロールを評価できる対象）は平成 25 年度秋期 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 I の問題

午後 I 試験は，3 問の中から 2 問の選択です。令和 4 年度春期の午後 I 試験では Web 関連のセキュリティ問題が 2 問出題されるなど，出題分野に少し偏りがあったように見受けられました。今回は，セキュリティインシデント対応を題材にしているものの，設問で問われている内容としては，攻撃手法の仕組みや，脆弱性に対する対応策などを問うものが比較的多く見られ，バランスの取れた問題設定になっているといえます。

このため，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繰り返し読んで，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解答を作成していけば，合格基準点の 60 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。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，少な目でしたから，些細なミスで得点を失わないようにすることが必要です。

問１　IoT 製品の開発

本問は，IoT 製品の開発というテーマですが，設問 1 は，DNS キャッシュポイズニング攻撃に関する仕組みや，攻撃者のサーバから偽のファームウェアをダウンロードさせる攻撃の回避策を考えるものです。設問 2〜4 は，Web アプリ R がもつ IP アドレス設定機能における脆弱性に関する問題です。具体的には，HTTP リクエストの setvalue 処理における脆弱性と，ログイン済みの利用者が攻撃者によって設定された罠サイトにアクセスし，利用者が意図せずに悪意のあるリクエストを Web アプリ R に送信させられた場合に，Web アプリ R がそのリクエストを受け付けて処理してしまう脆弱性に関する問題が出題されています。ネットワークセキュリティと，Web に関連するセキュリティの知識を持ち合わせていれば，かなりの設問に正解できると考えられます。

問２　脆弱性に起因するセキュリティインシデントへの対応

本問のテーマは，脆弱性に起因するセキュリティインシデントへの対応ですが，設問 1 は，予約サーバの CPU 使用率が高い状態が継続している事象から，予約サーバが通信している宛先の IP アドレスを答えるものです。設問 2 では，run プロセスが稼働している原因の追究には T ソフトを調べる必要があると判断した理由や，予約サーバへの攻撃の流れを考える問題が出題されています。設問 3 は，会員サーバの調査において，脆弱性 Y は認証前のアクセスでも悪用可能である理由，予約サーバとは違って攻撃が失敗した理由を，設問 4 は，URL フィルタリングルールの設定を答えるものです。Java の知識があれば，得点しやすいと思いますが，たとえ Java の知識があまりない場合でも，問題の条件，各表で示されている内容などを十分に吟味し，それらを丁寧に突き合わせていくことによって，正解を導き出すことができると思われます。

問３　オンラインゲーム事業者でのセキュリティインシデント対応

本問のテーマは，オンラインゲーム事業者でのセキュリティインシデント対応ですが，ゲームサーバで開発したゲームアプリを更新する手順において，インシデントが発生した場合のセキュリティ上の問題を考えるものです。設問 1 では，どのようにしてインシデントが発生したかを確認する方法などが問われています。設問 2 では，ゲームサーバ上での被害の調査に関する問題が出題されています。設問 3 は，再発防止と被害低減のための対策を考えるものです。問われてい

ることは，基本的な事項が中心なので，正解を導きやすいと考えられます。

(4) 午後Ⅱの問題

午後Ⅱ試験は，問1が脅威情報調査，問2がインシデントレスポンスチームというテーマで，どちらの問題も情報セキュリティにおける実務を意識したような観点からの出題になっています。問1は，ARPスプーフィングなどの知識を要求されるものがありますが，問1，問2とも問題の記述内容を確認し，何がセキュリティ上の問題になっているのか，それはどのような理由によるものか，その問題を解決するには，どのようにすればよいかなどを，本文や図表類から条件を見つけ出し，論理的に考察していくことによって，正解にたどり着くことができると思われます。

今回の試験は，前回と同様に，字句の穴埋め問題が多く見られたことから，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，前述したように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　脅威情報調査

本問は，マルウェアを解析したり，攻撃者グループの攻撃手法を調査したりするセキュリティ関連会社を舞台とした問題です。このため，設問1では，マルウェアの特徴，マルウェアの検体の解析作業に関する問題が出題されています。設問2は，システム内に検体を持ち込んで解析する必要があることから，ファイルの転送手順を改善するための方法を考えるものとなっています。設問3は，ARPスプーフィングによって，攻撃者が標的PCの通信を盗聴する場合，それぞれのPCのARPテーブルにおけるIPアドレスとMACアドレスの関係がどのようになっているかを追跡するものです。頭の中で考えていると混乱しますので，メモ書きをするなどして丁寧に取り組んでいくことが必要です。設問4は，パスワードの解読に関するものですが，問題で示されている図と表の中身をよく確認することによって，正解を導くことができると思われます。設問5は，ARPスプーフィング，パスワードの解読における運用上の改善策を考えるものです。設問で問われていることを的確に押さえれば，かなりの設問に答えることができると考え

られます。

問２　インシデントレスポンスチーム

本問は，インシデントレスポンスチームというテーマになっていますが，マルウェアの検知などにどのように取り組んでいくかという内容の問題です。設問 1 は，定義ファイルに登録されていないマルウェアの検知を行う場合，問題で提示されているルールを参考にして，検知するための単純ルールを答えるものです。設問 2 は，別のマルウェアβを検知するための追跡と，マルウェアβが埋め込まれたファイルを特定する問題です。設問 3 は，マルウェアβと同じ手段による感染の拡大を検知するための検知ルールを考えるものです。設問 4 は，秘密ファイルが流出したことの経緯を調査するための方法を考えるものですが，出題形式が適切な字句を入れる穴埋め問題なので，解答しやすいと思います。設問 5 は，ファイルの持出しに起因するインシデントの再発を防止するために，新たに作成すべき検知ルールを答えるものです。設問 6 は，インシデントレスポンスチームがインシデント対応を行う際の修正案を答える問題になっています。基本的な知識を十分に習得していれば，取り組みやすい問題といえますが，解答数がやや少なめなので，50〜60 字で答える記述式の設問に幾つ正解できるかが，合格基準点をクリアできるかどうかの分かれ目になると思われます。