3．第２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 月に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。このため，これまでの情報セキュリティスペシャリスト試験の傾向を分析し，その結果に基づいて，受験対策を行うことは有効であるといえます。

平成 28 年度春期から平成 29 年度春期までの受験者数，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，平成 21 年度秋期試験の合格率（18.5%）をピークに，その後，徐々に低下し，おおむね 13%台ないしは 14%台で推移してきましたが，平成 27 年度秋期試験と平成 28 年度春期試験の 2 期連続で 16%を超えました。支援士試験への橋渡しと位置づけられる平成 28 年度秋

期試験では，13.5%に低下したものの，平成 29 年度春期試験では，再び 16.3%に回復しています。一般に受験者数が多くなると，合格率が低くなる傾向があるようです。

年　度	応募者数	受験者数	合格者数
平成 28 年度春期	26,864（-5.0%）	18,143（67.5%）	2,988（16.5%）
平成 28 年度秋期	32,492（20.9%）	22,171（68.2%）	3,004（13.5%）
平成 29 年度春期	25,130（-22.7%）	17,266（68.7%）	2,822（16.3%）

（ ）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

平成 28 年度春期から平成 29 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
平成 28 年度春期	65.8%	66.6%
平成 28 年度秋期	46.3%	76.6%
平成 29 年度春期	53.0%	77.8%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 29 年度春期の午前Ⅰ試験の合格率は，平成 28 年度秋期に比べると約 7 ポイント向上していますが，1 年前に実施された平成 28 年度春期に比較すると約 13 ポイント低下しています。午前Ⅰ試験の合格率は，変動幅が大きいことが特徴ですが，今回の 53.0%という数字は，決して良いとはいえません。このため，午前Ⅰ試験を受験する必要のある方は，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，77.8%でした。約 8 割の受験者が合格基準点をクリアできるものですから，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れば，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Ⅱ試験の対策としては，3 期前に行われた試験の問題（平成 29 年度秋期試験では平成 28 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，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。平成 28 年度春期から平成 29 年度春期試験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 28 年春期	平成 28 年秋期	平成 29 年春期
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	1	3	2
	サービスマネジメント	4	2	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，論理回路の問題などは，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が必要です。なお，支援士試験では，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試験から受験される必要のある方は，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。平成 28 年度春期から平成 29 年度春期試験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 28 年 春期	平成 28 年 秋期	平成 29 年 春期
技術要素	セキュリティ	17	17	18
	ネットワーク	3	3	2
	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他，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よいでしょう。この他，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 アプリケーションなどにおけるセキュアプログラミングをはじめ，メッセージ認証，本人認証，ディジタル署名，電子証明書の検証方法，暗号化技術，ネットワークやデータベースに対する様々な攻撃とその対策，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，迷惑メール対策など，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，TCP/IP（HTTP，HTTPS，IPsec，TLS など）やインターネット利用・接続技術，DNS の仕組み，電子メールの配送の仕組みなど，データベース技術分野では，データベースに対するアクセス制御，SQL 文，RDB，データベースの排他制御やリカバリなど，幅広い技術を修得していく必要があります。さらに，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 IoT のセキュリティなど最近の動向，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も出題されるので，幅広く知識を吸収していくことが必要です。また，JIS Q 27001 や JIS X 5070 などの標準化動向の把握も忘れないようにしましょう。

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，ネットワークあるいはデータベース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他，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（通称名は“登録情報セキュリティスペシャリスト（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　平成 29 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。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，ここ数回同じ出題数です。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。

平成 26 年秋期試験から重点的に出題されているセキュリティ分野の問題は今回もこれまでと同じ 4 問でした。また，新傾向問題といえるものは次の 4 問で前回の 2 問から増えています。問 11 は少し難しい内容でした。

・問 11　OpenFlow を使った SDN の説明
・問 14　サイバーセキュリティ経営ガイドラインの説明
・問 17　アジャイル開発でイテレーションを行う目的
・問 26　事業戦略の浸透価格戦略に該当するもの

問題の出題形式としては，文章の正誤問題が 18 問（前回 15 問），用語問題が 2 問（前回 4 問），計算問題が 2 問（前回 5 問），考察問題が 8 問（前回 6 問）で，前回と比べて文章の正誤問題と考察問題が増え，用語問題と計算問題は減っています。出題内容としては，前回，基礎理論の問題が基本情報技術者試験レベルで易しかったのですが，今回は応用情報技術者試験レベルの内容で少し難しかったといえます。また，全体としても，新傾向問題が例年より多かったこと，考察問題が増えたことなどから，少し難しく感じられた試験だったといえます。

高度情報処理技術者の午前 I 試験は出題範囲が広い中からの 30 問なので，対策としては日ごろから，基本情報技術者から応用情報技術者試験レベルの問題を

少しずつ解いて基礎知識を維持することが大切です。

次に，新傾向問題を含む出題内容全体を示します。定番問題も多いですが，下線を引いた問題は高度午前Ⅰ試験ではあまり出題されていない内容です。あまり聞かない用語や解答に少し時間がかかる問題といえますが，基礎知識を確実に理解していれば，用語問題は消去法で，計算問題は少し時間をかけて丁寧に考えれば，解答できる問題です。

・テクノロジ分野……近似計算，BNF，流れ図の処理結果，圧縮プログラムの展開時間，稼働率の計算，ブロック置換アルゴリズム，論理式，デッドロック，データマイニング，CSMA/CD，OpenFlow を使った SDN，認証局の公開鍵を利用する操作，暗号方式，サイバーセキュリティ経営ガイドライン，WPA2-PSK，汎化の例，イテレーション
・マネジメント分野……アローダイアグラム，定量的リスク分析，可用性と信頼性に関わる KPI，問題管理プロセスの活動，監査報告の改善勧告
・ストラテジ分野……プログラムマネジメント，IT 投資の KPI，業務フローの記述図，浸透価格戦略，予測技法，セル生産方式，損益分岐点の特性，Web ページの著作権

出題される内容は，過去に応用情報技術者試験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が，午前Ⅰ試験はそのための“入場券”に当たるので，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。

(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，平成 22 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，全体的な難易度を評価すると，新規問題の出題数が平成 28 年度秋期と同じ 6 問でしたから，平成 28 年度秋期とほぼ同じレベルの合格率（76.6%）になるのではないでしょうか。

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，分野別の出題数は，これまでセキュリティが 17 問，ネットワークが 3 問，データベースが 1 問という比率でしたが，今回，はじめてセキュリティが 18 問，ネットワークが 2 問に変更されました。

セキュリティ分野の 18 問のうち，17 問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）は 1 問でした。また，攻撃の説明やその手口などに関する問題が 6 問（全体の 3 分の 1）出題されたことも，支援士試験における一つの特徴を示すものといえます。新規問題は，問 2（SSL/TLS のダウングレード攻撃），問 5（セッション ID の固定化攻撃の手口），問 6（DNS 水責め攻撃の手口と目的），問 11（MITB 攻撃に有効な対策），問 13（フォールスネガティブに該当するもの）の 5 問でした。これに対し，過去問題からの出題は，平成 27 年度秋期から 6 問，平成 27 年度春期が 2 問，平成 26 年度秋期が 2 問，平成 26 年度春期が 1 問，平成 25 年度春期が 2 問となっています。

ネットワーク分野の 2 問は，新規問題が 1 問，平成 25 年度春期の過去問題が 1 問という内訳でした。新規問題の問 19（Automatic MDI/MDI-X の機能）は，標準のレベル 3 の問題です。

データベース分野の問 21（SQL 文の意味）は，平成 23 年度春期試験に出題されていたものです。

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。問 22（JIS X 2510：2013 で定義された品質特性）は新規問題，問 23（コンテンツの不正複製を防止する方式の説明）は平成 26 年度秋期で出題された過去問題ですが，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（データベースのバックアップ又は復旧）は他種別の過去問題，問 25（IT に係る保証業務の三当事者）は新規問題ですが，いずれもレベル 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。Web サイトに関するセキュリテ

ィ問題は，問２の１問に限られていましたので，全体としてバランスのとれた出題であったといえます。また，詳細な知識を要求される問題が少なかったことから，基本的な知識を十分に身に付けて試験に臨んだ受験者にとっては有利だったと思われます。そして，それぞれの問題に丁寧に取り組んでいけば，比較的容易に合格基準点をクリアできると考えられます。しかしながら，各問題とも小問数が，これまでの試験に比べると少なかったことから，1 小問当たりの配点が高くなり，一つのミスが致命傷になる可能性があります。いずれにしても，午後問題に取り組む際には，問題文の記述内容や条件を考慮するとともに，設問で問われていることを確認しながら，解答を作成していくことが大切です。

問１　社内で発生したセキュリティインシデント

問題のテーマはセキュリティインシデントですが，ARP ポイズニングによる通信の盗聴手法，サーバ証明書の検証に失敗した場合は接続しない設定にするという対策の意味，セグメント分けによって得られるセキュリティ上の効果などが問われています。ネットワークセキュリティを得意とする受験者にとっては，少し易しいレベルの問題ですが，その他の受験者にとっても，問題の記述内容が理解できれば，合格基準点をクリアできる点数を獲得することはそれほど難しいというわけではありません。

問２　Web サイトのセキュリティ対策

Web サイトにおけるクロスサイトリクエストフォージェリ（CSRF）脆弱性やクロスサイトスクリプティング（XSS）脆弱性などに関するオーソドックスな問題です。ログイン時における動作，セッション ID の管理方法，HTML に含まれるスクリプトの扱いなどの問題が出題されていますが，Web サイトに関するセキュリティ対策に関する知識を十分に身に付けていれば，比較的容易に合格基準点をクリアできると思われます。

問３　クラウドサービスの認証連携

問題のテーマはクラウドサービスの認証連携ですが，出題の中心は，SAML を用いた認証連携と，連携を行うに当たっての接続元を制限する方法などを考えるものです。SAML 自体に関する専門知識が要求されるわけではないので，問題の記述内容を丁寧に読んでいき，設問で問われていることに対し，的確に答えてい

けばよいでしょう。そうすれば，比較的容易に合格基準点をクリアできると思われます。

(4) 午後Ⅱの問題

午後Ⅱ試験は，問１がマルウェアの解析，問２が社内システムの情報セキュリティ対策というテーマですが，いずれもマルウェア感染に関する対策をどのように実施していくかなどに焦点が当てられています。このため，問１と問２の選択に迷ってしまったという受験者もいたと思われますが，問１は，問題のテーマのとおり，マルウェア自体を解析する手法に主眼が置かれています。これまでの試験では，マルウェアの解析方法について出題されたことはなかったので，デバッガによる解析などの記述内容が難しく感じられたと思われます。一方，問２は，メールサーバ，プロキシサーバ，DNS サーバなどのネットワークセキュリティを中心とした出題です。ネットワーク技術に強い受験者にとっては取り組みやすい問題です。

なお，記述式の問題は，自分自身が意図した内容を的確に文章で表現できるかどうかがポイントになります。設問で問われていることをよく確認し，丁寧に解答を作成していくことを心掛けるようにしてください。

問１　マルウェアの解析

本問では，インシデントの発生を契機として，インシデントへの初動対応，マルウェアが C&C サーバと HTTPS 通信を行うときの解析方法，デバッガによるマルウェアの解析とマルウェアがもつパッカーの仕組み，インシデントに対応する応急措置，感染経路の特定と対処，インシデント対応の事後評価などを問う問題が出題されています。マルウェアが C&C サーバと HTTPS 通信を行う方法や，デバッガによるマルウェアの解析などは，専門知識が必要ですから，問題の記述内容を理解するのに苦労するかもしれません。しかし，その他の設問は，問題の記述内容に照らし合わせて，丁寧に解答を作成していけば正解を導くことができると考えられます。こうした正解できそうな設問については，問題の記述内容を考慮し，的を射た解答を作成していくとよいでしょう。

問２　社内システムの情報セキュリティ対策

本問のテーマは，社内システムの情報セキュリティ対策ですが，出題内容は，

メールサーバ，プロキシサーバ，DNS サーバに関する技術知識が要求されるものとなっています。感染したマルウェアの動作から，プロキシサーバやメールサーバにおける設定内容を考察するものや，DNS の再帰的な問合せについては，どのような範囲にあるクライアントに制限すべきかなどの問題が出題されています。ネットワークセキュリティに詳しい受験者にとっては取り組みやすい問題ですが，小問数が問 1 に比べてかなり少ないので，1 問当たりの配点が高くなり，些細なミスをしないことが必要です。