3. 第６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 30 年度春期から平成 31 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，第 1 回から第 3 回までは 16%から 17%程度で推移し，第 4 回で 18.5%に向上しました。今回の試験では過去最高の 18.9%になり，約 5.3 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，平成 31 年 4 月 1 日現在，“登録セキスペ”の登録者数は 18,330 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
平成 30 年度春期	23,180（-1.0%）	15,379（66.3%）	2,596（16.9%）
平成 30 年度秋期	22,447（-3.2%）	15,257（68.0%）	2,818（18.5%）
平成 31 年度春期	22,447（-3.2%）	14,556（65.6%）	2,774（18.9%）

（ ）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 30 年度春期から平成 31 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 30 年度春期	58.2%	78.2%
平成 30 年度秋期	51.7%	71.2%
平成 31 年度春期	50.8%	79.8%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 31 年度春期の午前Ⅰ試験の合格率は，平成 30 年度秋期に比べると約 1 ポイント，1 年前に実施された平成 30 年度春期に比較すると 7.4 ポイント低下しています。このように，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%を超えたことはありませんが，今回の 50.8%という数字は，低めの合格率になっています。このため，午前Ⅰ試験を受験する必要のある方は，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，79.8%でした。支援士試験はこれまで 5 回実施され，いずれも 70%以上の合格率になっていますが，これまでの中で最も高い合格率になりました。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 期前に行われた試験の問題（令和元年度秋期試験では平成 30 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 30 年度春期から平成 31 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 30 年春期	平成 30 年秋期	平成 31 年春期
テクノロジ系（17 問）	基礎理論	3	4	3
	コンピュータシステム	4	3	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	2	2
	サービスマネジメント	4	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。平成 30 年度春期から平成 31 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 30 年 春期	平成 30 年 秋期	平成 31 年 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，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 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，パスワードレス認証方式など最近の動向，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（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 31 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 3 問で（前回 2 問），午前Ⅰ共通問題の選択元の応用情報技術者試験には 14 問ありましたが，少ししか選ばれなかったといえます。

・問 24　ワントゥワンマーケティングを実現するソリューション
・問 27　オープンイノベーションに関する事例
・問 28　IoT 活用におけるディジタルツインの説明

問題の出題形式としては，文章の正誤問題が 17 問（前回 15 問），用語問題が 3 問（前回 6 問），計算問題が 3 問（前回 5 問），考察問題が 7 問（前回 4 問）で，前回と比べて用語問題と計算問題が減り，文章問題と考察問題が増えています。

出題内容としては，基礎理論は従来少し難しい問題が多い傾向がありましたが，今回は結果を求めやすい問題を含む，論理演算，ディープラーニング，シェルソートが出題されました。この分野以外の問題も比較的解答しやすい問題が多く，全体に従来よりも少し易しかったと思われます。

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，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日ごろから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，出題内容全体を示します。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ることによって解答できる内容もいくつかあります。

・テクノロジ分野……2 進表現を求める論理演算，ディープラーニング，シェルソート，スーパスカラ，検索要求件数，デッドロック，回路の入力と出力，レンダリング，ACID 特性，NAPT 機能，イーサネットフレームと IP データグラム，リスクベース認証，ディジタルフォレンジックス，サンドボックス，WAF，フェールセーフ，バーンダウンチャート
・マネジメント分野……完成時総コスト見積り，アローダイアグラム，問題管理プロセス，バックアップに必要な磁気テープの本数，監査報告書
・ストラテジ分野……プログラムマネジメント，ワントゥワンマーケティング，要件定義で使用する図，コアコンピタンス，オープンイノベーション，ディジタルツイン，故障要因を表現する図，要配慮個人情報

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。

そのために，最近 2 年間ぐらいの応用情報技術者試験で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，ビッグデータ関連は新しい用語がこれからも出てくると思われるので，日ごろから IT 関連の話題には注目し，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，全体的な難易度を評価すると，新規問題の出題数が平成 30 年度秋期試験

から 4 問少なくなりましたので，難易度は易しくなったといえます。

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 問という比率で定着しています。

セキュリティ分野の 17 問のうち，17 問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 5（仮想通貨環境におけるクリプトジャッキング），問 8（署名の機能をもつハードウェアトークンでできること），問 10（クロスサイトリクエストフォージェリ攻撃の対策），問 15（SPF 導入時ドメイン所有者側で行う必要がある設定）の 4 問ですが，いずれもレベル 3 の問題といえます。これに対し，過去問題からの出題は，平成 29 年度秋期から 7 問，平成 29 年度春期及び平成 28 年度春期，平成 27 年度秋期，平成 27 年度春期，平成 26 年度秋期からそれぞれ 1 問の他，平成 29 年度秋期 NW 試験から 1 問の計 13 問が出題されていました。

ネットワーク分野の 3 問は，新規問題が 1 問，過去問題が 2 問という割合でした。新規問題は問 18（無線 LAN の隠れ端末問題）で，レベル 4 の問題といえます。過去問題は問 19（コネクション確立を行う LAN プロトコル）と問 20（SNMP の PDU）で，いずれも平成 24 年度春期試験で出題されていたものです。

データベース分野の問 21（データベースの参照制約）は，レベル 3 の問題と考えてよいでしょう。

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（ソフトウェアの脆弱性を検出するテスト手法）は平成 27 年度春期 ES 試験，問 23（マッシュアップに該当するもの）は平成 26 年度春期 AP 試験で出題されていたものですが，いずれもレベル 3 の問題です。

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に関する記述）は

平成 29 年度春期 SC 試験で出題されていました。問 25（システム監査における監査調書の説明）は新規問題ですが，いずれもレベル 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，セキュアプログラミングに関連する問題が出題されますが，今回は HTTP リクエストとレスポンスのヘッダなどを中心としたものでした。このため，必ずしも C++や Java などの知識がなくても取り組める問題でしたから，Web サイトのセキュリティに関する基本的な知識があれば選択しやすかったといえます。一方，各問とも設定されている小問数が少なかったことなどから，1 小問当たりの配点が大きくなりますので，些細なミスをしないようにすることが必要です。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ができると思われます。

問 1　Web サイトのセキュリティ

問題のテーマは Web サイトのセキュリティですが，Same Origin Policy の基本知識のほか，問題で説明されている CORS（Cross-Origin Resource Sharing）の仕組みを十分に理解しながら，それぞれの設問に丁寧に取り組んでいくことが必要です。また，これまでのセキュアプログラミング関連の問題と比較して，基本的な設問が多く，出題形式も解答しやすいように工夫されていたことなどから，得点しやすい問題といえます。

問 2　クラウドサービスのセキュリティ

問題のテーマはクラウドサービスのセキュリティですが，偽の無線 LAN アクセスポイントに誘導される手法，HTTP 接続とサーバ証明書の関係，TOTP（Time-based One-Time Password algorithm）と WebAuthn（Web Authentication API）についての仕組みと両者の比較などに関する問題が出題されています。技術的な要素が強く，特に TOTP を利用する際のリスクを考察する設問は，どのような点に着目するかどうかがポイントになるので，やや難の問題といえます。

問３　IoT 機器の開発

本問は，IoT 機器の開発をテーマとして，ゲーム機，ゲームサーバ，認証サーバという構成要素でゲームシステムを構築した際に発生するセキュリティ問題を考えるものです。システムのセキュリティレビューを実施した際に指摘された脆弱性の原因などについて，ゲームサーバや認証サーバの仕様に基づいて解答するものや，秘密鍵とクライアント証明書を不正に読み取る方法，TPM（Trusted Platform Module）がもつべき性質とは何かなどの問題が出題されています。問題の記述内容に従って，丁寧に解答を作成していくことが求められますが，専門的な知識が要求される設問が少ないことから，比較的正解を導きやすいといえます。

(4)　午後Ⅱの問題

午後Ⅱ試験は，問 1 がマルウェア感染と対策，問 2 が情報セキュリティ対策の強化というテーマでした。前回の平成 30 年度秋期試験は，問 1 がクラウド環境における認証連携を考察する問題，問 2 がマルウェア感染というインシデント対応を例としてログ分析などを中心にした問題でしたが，今回の問題は，2 問ともネットワークセキュリティに関する知識が要求されるものでした。

また，今回は，前回の試験とは異なり，解答する小問数がかなり減少しましたので，1 小問当たりの配点が高くなります。このため，少しのミスでも致命傷になり，合格基準点をクリアすることが難しくなると考えられます。しかも，問 1，問 2 とも，知識をベースにした小問の比率がこれまでの試験と比較して多く見られましたので，問題の記述内容を基にして解答を作成できる小問については，確実に正解を導いていくことが求められます。

問１　マルウェア感染と対策

本問は，マルウェア感染と対策をテーマとしたものですが，出題内容としては，設問 l でマルウェア感染を特定するために必要なログをもつ機器名，設問 2 でファイル単位ではなくセクタ単位でコピーする理由，設問 3 で無線 LAN 通信の特徴，設問 4 で ECB モードと CTR モードによる暗号化処理の問題，設問 5 で HTTP 通信と HTTPS 通信で取得できるログの内容及びマルウェアが窃取した情報を社内 PC から社外へ送信する経路，設問 6 でプロキシサーバにおいて HTTPS 通信を復号する機能をもたせた場合に発生する制約などを答えるものが出題されてい

ます。設問１から設問５は比較的技術要素の強い問題であり，設問６はディジタル証明書の検証に関する条件を答えることが必要です。このため，難易度を全体的に評価すれば，やや難の問題といえます。

問２　情報セキュリティ対策の強化

本問は，情報セキュリティ対策の強化というテーマですが，設問１は営業秘密の３要件，設問２から設問４はネットワークセキュリティや電子政府における調達のために参照すべき暗号リストなどの基礎知識，設問５と設問６は問題の記述内容に従って理由や根拠，設定変更の内容，見直し後の運用方法などを答えるもの，設問７はマルウェアの検知を集中管理する仕組みの穴埋め問題が出題されています。これらのうち，設問５と設問６の占める比重が高いので，設問で問われていることを確認し，問題の条件などを考慮して解答を作成すれば，合格基準点をクリアすることができると思われます。このため，問１に比べるとやや易と判断されます。