3. 第５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 29 年度秋期から平成 30 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，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。支援士試験になってからの合格率は 16～17%程度に向上し，今回の合格率は過去最高に並ぶ結果になりました。そして，IPA の発表によりますと，平成 30 年 10 月 1 日現在，“登録セキスペ”の登録者数は 17,360 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 29 年度秋期	23,425（-6.8%）	16,218（69.2%）	2,767（17.1%）
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%）

（ ）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 29 年度秋期から平成 30 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
平成 29 年度秋期	47.9%	76.8%
平成 30 年度春期	58.2%	78.2%
平成 30 年度秋期	51.7%	71.2%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 30 年度秋期の午前Ⅰ試験の合格率は，平成 30 年度春期に比べると 6.5 ポイント低下しましたが，1 年前に実施された平成 29 年度秋期に比較すると約 4 ポイント向上しています。このように，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 51.7%という数字は，やや低めの合格率といえます。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，71.2%でした。支援士試験はこれまで 4 回実施され，過去 3 回の午前Ⅱ試験の合格率は，75%を超えていましたので，今回の合格率はそれらよりも低くなりました。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（平成 31 年度春期試験では平成 29 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，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 29 年度秋期から平成 30 年度秋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 29 年秋期	平成 30 年春期	平成 30 年秋期
テクノロジ系（17 問）	基礎理論	3	3	4
	コンピュータシステム	4	4	3
	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	1	2
	サービスマネジメント	3	4	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 29 年度秋期から平成 30 年度秋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 29 年 秋期	平成 30 年 春期	平成 30 年 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（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 30 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。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の 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 2 問で（前回 5 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 問あったのですが，今回は少ししか選ばれなかったといえます。

・問 25　システム化構想の立案プロセスで行うべきこと（AI 関連）
・問 27　IoT がもたらす効果の“自律化”の段階

問題の出題形式としては，文章の正誤問題が 15 問（前回 18 問），用語問題が 6 問（前回 4 問），計算問題が 5 問（前回 7 問），考察問題が 4 問（前回 1 問）で，前回と比べて文章問題と計算問題が減り，用語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く，前回は解答しやすい問題（ハミング符号，再帰関数）でしたが，今回また難しい内容（待ち行列，正規分布）に戻ったといえます。この分野以外も過去試験で出題されている内容でも常識的に解答できる問題が少なく，全体に従来よりも少し難しかったといえます。

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，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幾つかあります。

・テクノロジ分野……相補演算，平均待ち時間，正規分布，2 次元配列，誤り制御方式，ページインの処理，半加算器，レンダリング，ハッシュ値の衝突，並行実行のアクセスモード，スイッチングハブ，ディジタル証明書を用いた TLS 通信，クロスサイトスクリプティング対策，ブルートフォース攻撃，ファジング，プログラム設計方針，イテレーション
・マネジメント分野……トレンドチャート，ファンクションポイント法，サービスライフサイクル，サンプリング（試査），システムの可監査性
・ストラテジ分野……UML 活用シーン，IT 投資 KPI の例，システム化構想の立案プロセス，集団を分類し分析する手法，IoT の効果“自律化”，正味所要量の計算，変動費の計算，下請代金支払遅延防止法

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，日頃から 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，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 30 年度春期試験から 4 問

増加しましたので，難易度は高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，ここ 3 期は，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，16 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。新規問題は，問 3（ブロックチェーンに関する記述），問 4（マルチベクトル型 DDoS 攻撃に該当するもの），問 7（UDP の性質を悪用した DDoS 攻撃），問 8（EDSA 認証における評価対象と評価項目），問 10（クラウドサービスカスタマとプロバイダの責務），問 11（マルウェア Mirai の動作），問 12（HSTS の動作）の 7 問ですが，一部，レベル 4 の問題も含まれています。これに対し，過去問題からの出題は，平成 29 年度春期から 6 問，平成 28 年度秋期から 1 問，平成 28 年度春期から 1 問の他，平成 29 年度春期 AP 試験と平成 27 年度秋期 NW 試験から各 1 問の計 10 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 2 問，過去問題が 1 問という割合でした。新規問題は，問 19（クラス D の IP アドレス），問 20（無線 LAN の周波数帯域の組合せ）で，問 20 はレベル 4 の問題といえます。過去問題は問 18（TCP の 3 ウェイハンドシェイク）で，これは平成 28 年度秋期試験で出題されたものです。

データベース分野の問 21（GRANT 文付きの SQL 文の実行結果）は，レベル 4 の問題に位置付けられます。

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。問 22（ソフトウェア結合のテスト方法）は平成 25 年度春期 ES 試験，問 23（SOA でサービスを設計する際の注意点）は平成 25 年度春期 SC 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（IT サービスマネジメントの情報セキュリティ管理プロセス）は平成 28 年度春期 SC 試験，問 25（IT に係る保証業務の三当事者）は平成 29 年度春期 SC 試験で出題されていたものです。

(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。問 1 として C++に関するセキュアプログラミングの問題が出題されましたが，全体としてバランスのとれた出題であったといえます。平成 30 年度春期試験では，問 1 と問 2 における小問数が少なく，配点が大きくなる傾向がありましたが，今回は，3 問とも小問数が多く設定されていましたから，その点は改善されています。このため，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　ソフトウェア開発

問題のテーマはソフトウェア開発ですが，C++を使用したプログラムで発生するバッファオーバフロー脆弱性に関する問題です。C++に関しては，平成 26 年度秋期午後 I 問 1，平成 28 年度秋期午後 I 問 2，平成 30 年度春期午後 I 問 1 として，スタックバッファオーバフロー，データ実行防止機能（DEP），アドレス空間配置ランダム化技術（ASLR），ヒープバッファオーバフロー，Use-After-Free などに関する問題が出題されています。これらの過去問題を演習していた受験者にとっては，基本的な問題が多かったことなどから比較的易しい問題といえます。

問 2　セキュリティインシデント対応

問題のテーマはセキュリティインシデント対応ですが，ネットワークセキュリティに関する技術知識が必要とされる問題です。特に，設問 3 は，時系列的にログ情報を正確に読み取っていくことがポイントになりますが，設問 4 (1)については，問題文に記述された内容を基にすれば解答を導くことができます。全体的に難易度を評価すると，標準レベルの問題といえます。

問 3　ソフトウェアの脆弱性対策

本問は，ソフトウェアの脆弱性対策をテーマとして，Web サーバのソフトウェ

アに脆弱性が存在し，セキュリティインシデントが発生した場合の対処方法や調査，並びにリスク軽減策を考える問題です。必要な知識としては，時刻同期やログの分析方法，Web サーバの運用方法，WAF，DNS に関する知識が挙げられます。なお，難易度を全体的に評価すれば，標準レベルの問題といえます。

(4) 午後Ⅱの問題

午後Ⅱ試験は，問 1 がクラウド環境におけるセキュリティ対策，問 2 がセキュリティインシデントへの対応というテーマでした。平成 30 年度春期試験では，問 1 も問 2 も，Web 関連のセキュリティに関する知識が要求される問題でしたが，今回は，問 2 でマルウェアが HTTP リクエストとレスポンスを用いて行われる活動内容は何かを述べるものだけでした。

今回の午後Ⅱ試験は，前回とは異なり，小問数がかなり増加したことが特徴です。このため，一つのミスが致命傷になることはありませんが，各小問に丁寧に答えて，合格基準点をクリアできる点数を積み上げていくことが必要になります。また，問 1，問 2 とも，問題の記述内容を基にして解答を作成できるようになっていましたから，設問で問われていることを確認し，注意深く問題文を読み解いて解答を作成することがポイントといえます。

問 1　クラウド環境におけるセキュリティ対策

本問では，オンプレミス環境からハイブリッドクラウド環境に移行するに当たって，クラウド環境によって制約を受ける条件，ID 管理及び利用者認証による利害得失，エンドポイントにおける制約，モバイル環境での利用方法などの問題が出題されています。設問 2 や設問 4 (3) などは，問題文中に解答を作成するに当たってのキーワードが記述されているほか，設問 3 (1) はシングルサインオンの特徴を述べるもの，設問 3 (2) や設問 5 (1) は，利用者認証後の通信経路上の負荷が高くなる構成要素を考えるもの，設問 5 (2) は，SAML による通信シーケンスを考えるものとなっています。専門知識が要求される小問が少ない上，問題文の記述内容などを冷静に読み取っていけば，正解できる小問が多い出題構成になっています。このため，難易度を全体的に評価すれば，やや易の問題といえます。

問 2　セキュリティインシデントへの対応

本問は，セキュリティインシデントへの対応というテーマが示すように，出題

内容としては,インシデント発生時における取り組むべき事項や対応能力の向上,マルウェアをダウンロードした際の調査内容やログ分析に関する考察，インシデント発生時におけるタイムラインの整理などの問題が出題されています。解答作成に当たっては，マルウェアがインターネットと通信する際に利用するサーバは何かなどの知識のほか，ログを調査するに当たって時系列を丁寧に整理することなどが必要です。難易度を全体的に評価すれば，標準レベルの問題といえます。