3. 第1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）という新しい試験が実施されます。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考えられます。

平成 27 年度秋期から平成 28 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。しかし，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%に低下しています。このため，支援士試験で合格を目指すには，午後試験で合格基準点をクリアすることが必要ですから，受験対策を十分に行って試験に臨むことが大切です。

年　度	応募者数	受験者数	合格者数
平成 27 年度秋期	28,274（3.4%）	18,930（67.0%）	3,141（16.6%）
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%）

（ ）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 27 年度秋期から平成 28 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 27 年度秋期	51.2%	81.0%
平成 28 年度春期	65.8%	66.6%
平成 28 年度秋期	46.3%	76.6%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 28 年度秋期の午前Ⅰ試験の合格率は，平成 28 年度春期に比べると約 20 ポイント低下し，1 年前に実施された平成 27 年度秋期に比較しても約 5 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 46.3%という数字は，最近の試験ではかなり低いものです。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，平成 27 年度秋期試験では 81.0%でしたが，平成 28 年度春期試験では 66.6%へと急激に低下しました。しかし，今回の平成 28 年度秋期試験では 76.6%に回復しています。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 年度春期試験では平成 27 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ことが有効です。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ので，初めて支援士試験を受験される方は，軽視しないことが必要です。

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 27 年度秋期から平成 28 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 27 年秋期	平成 28 年春期	平成 28 年秋期
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	1	3
	サービスマネジメント	3	4	2
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，支援士試験になると，情報セキュリティの専門家の方が多く受験されることが予想されます。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。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 27 年度秋期から平成 28 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 27 年秋期	平成 28 年春期	平成 28 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)”）という国家資格を有する者になることができます。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 28 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，出題数が定着したといえます。

今回の試験で新傾向問題といえるものは次の 2 問でしたが，問 9 の問題はやや難の内容です。

問 9　B^+木インデックスのアクセス回数のオーダ

問 18　PMBOK の統合変更管理プロセス

問題の出題形式としては，文章の正誤問題が 15 問（前回 19 問），用語問題が 4 問（前回 5 問），計算問題が 5 問（前回 2 問），考察問題が 6 問（前回 4 問）で，前回と比べて文章の正誤問題が減り，計算問題と考察問題が増えています。出題内容としては，基礎理論の問題が基本情報技術者試験レベルでこれまでの問題と比べて少し易しかったといえますが，アルゴリズムの問題が突然現れて，驚いた方も多かったと思われます。全体としては，計算問題と考察問題が増えた分，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。定番問題もありますが，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ることで，解答できる問題です。

・テクノロジ分野……近似値を求めるアルゴリズム，有限オートマトン，ヒープソート，メモリインタリーブ，アベイラビリティの変化，主記憶管理，論理回路，SMIL，B^+木インデックスのアクセス回数，DBMS の再立上げ，ARP，IPv6 の拡張ヘッダ，チャレンジレスポンス認証，認証デバイス，ハイブリッド暗号方式，UML のユースケース図，ソフトウェアの使用許諾

・マネジメント分野……PMBOK の統合変更管理プロセス，アローダイアグラム，プロジェクト完了日数，バックアップ，内部統制

・ストラテジ分野……ソリューションビジネスの KPI，BI の活用事例，契約形態，ベンチマーキング，アンゾフの成長マトリクス，部品所要量の計算，故障率曲線，産業財産権

出題される内容は，過去に何度も出題されてい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，第 3 回（平成 22 年度春期）以降，同じですから，支援士試験になって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，前回（平成 28 年度春期）と比較して，新規問題が前回より減少し，過去問題からの出題が多かったことから，少し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，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。支援士試験でも，この出題比率は維持されていくものと考えられます。

セキュリティ分野の 17 問は，全てが基本的に情報セキュリティ技術に関するものです。新規問題は，RADIUS などが提供する AAA の構成要素（問 1），NTP リフレクション攻撃の特徴（問 2），POODLE（CVE-2014-3566）攻撃の説明（問 3），リスクベース認証に該当するもの（問 6），Cookie の secure 属性の動作（問 9）の 5 問でした。これに対し，過去問題からの出題は，平成 27 年度春期から 8 問，平成 26 年度秋期と春期からそれぞれ 1 問，平成 25 年度秋期から 2 問の出題となっています。

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 問という内訳でした。新規問題の，DNS に関する記述（問 18）は，DNS の知識が必要ですが，他の 2 問は，平成 25 年秋期と春期に出題されていたもので，標準レベルの問題です。また，データベース分野では，コミット処理完了とみなすタイミング（問 21）が出題されましたが，レベル 3 の標準的な問題といえます。

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，それぞれ 1 問ずつ出題されました。システム開発におけるテスト（問 22）は平成 24 年春期，開発方針と開発モデルの組合せ（問 23）は，平成 25 年秋期に出題されたものです。

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，それぞれ 1 問ずつ出題されました。JIS Q 20000-1 で定義されるインシデント（問 24）は平成 26 年秋期に出題されていました。データベースのアクセスコントロールを確認する監査手続（問 25）は，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 問を選択し解答します。今回は，C++のコード問題が問 2 で出題された他，技術的な内容を問うものがやや多く見られたので，少し難しく感じられたかもしれません。その半面，用語に関する穴埋め問題は，

全て解答群からの字句を選択する方式になりましたので，難易度は，これまでの試験とほぼ同程度と考えられます。なお，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。支援士試験に向けてもこうした姿勢をしっかりと身に付けて臨むことが必要であると考えられます。

問１　組込み機器を利用したシステムのセキュリティ対策

netstat コマンドの出力内容や，SSH がもつ機能，TCP Wrapper とは何かという知識が要求される問題です。これらの技術知識を有していれば，比較的容易に合格基準点をクリアできると思われます。その一方，知識があやふやな場合には，用語の穴埋め問題が少なかった分だけ得点源が少なくなります。このため，イメージファイルのディジタル署名に関連した処理の設問には確実に正解する他，問題の記述内容から正解を導くことができる記述式問題を一つでも見つけていくことが必要になります。

問２　ソフトウェア開発における脆弱性対策

本問は，ソフトウェア開発における脆弱性対策というテーマですが，スタックベース及びヒープベースのバッファオーバフロー（BOF）脆弱性の問題です。また，C++のプログラムも含まれていますので，ヒープベース BOF 脆弱性や C++の知識がない受験者にとっては，荷の重い問題だったといえます。なお，データ実行防止機能（DEP）については，理解されている受験者が多いので，DEP によって利用者認証が回避できない理由は，正解できるのではないかと思われます。

問３　プロキシサーバによるマルウェア対策

プロキシサーバにおける URL フィルタリングや，利用者認証機能に関する問題です。これまでの試験において，よく出題されているテーマであることから，多くの受験者にとっては，取り組みやすい問題であったといえます。少し注意を要する設問は，設問 2 (1)です。冷静に考えれば正解できるので，これに正解できれば高得点を期待できます。

(4)　午後Ⅱの問題

午後Ⅱ試験は，問 1 が IC カードを用いた認証システム，問 2 が脆弱性対策と

いうテーマでした。特に，問 1 は用語に類する語句選択の穴埋め問題が 12 問ありましたので，一定の技術レベルにあれば，解答しやすいといえます。問 2 は問題全文が 14 ページにわたっていますが，記述式の設問が比較的少なく，考察問題が多かったので，問題の記述内容の他，図や表で示された条件をよく確認していくことが必要です。なお，今回の試験は，平成 29 年度春期から行われる支援士試験への橋渡しとなります。出題形式としては，用語をはじめ，字句を解答群の中から選択するものが多くなり，これは支援士試験でも踏襲されるものと思われます。また，問 2 のテーマにもみられるように，支援士としては，脆弱性対策に関する理解を一段と高める必要があります。このため，JVN（Japan Vulnerability Notes）として公表されている脆弱性情報のうち，重要なものについては，しっかりウォッチしていくことなどが必要になります。

問 1　IC カードを用いた認証システム

本問では，認証カードの方式設計として，認証技術の基本知識，ディジタル署名の検証方法，認証対象者の不適切な行為などが問われています。また，認証カードの運用設計として，認証カードを発行する条件や，失効情報を公開するための条件の考察の他，認証局階層とサーバ証明書に関する記述式の設問が設定されています。さらに，取引先の従業者へ認証カードを貸与する場合における利点や，認証カードの管理方法などが問われています。用語の穴埋め問題については，解答群の中から選択するものでしたから，記述式の設問に落ち着いて取り組むことができたと思われます。全体の難易度を評価すると，少し易しいレベルといえます。

問 2　脆弱性対策

本問は，UNIX/Linux で利用されている shell の一つである bash の脆弱性を題材にし，Web サーバにおいて bash 脆弱性が悪用される事例を考察するものです。具体的には，Web サーバが被害を受ける条件をはじめ，WAF による脆弱性対策，Web ブラウザが攻撃者のサイトを経由して社内 Web サーバにアクセスする方法などに関する技術的な問題の他，リスクレベルの評価を行う条件を考察する問題が出題されています。問 1 よりも Web サーバにおける技術知識が必要なことから，難易度は問 1 より高いといえます。