3. 第3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。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 年度秋期から平成 29 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。支援士試験としては，これまでに 2 回実施されましたが，平成 29 年度秋期試験の合格率は，第 1 回の 16.3%を超える 17.1%になりました。

合格者の比率は，約 6 人弱に対して 1 人の割合ですから，しっかり準備して試験に臨めば，資格を取得することはそれほど難しいというわけではないでしょう。

年　度	応募者数	受験者数	合格者数
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%）
平成 29 年度秋期	23,425（-6.8%）	16,218（69.2%）	2,767（17.1%）

（ ）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

平成 28 年度秋期から平成 29 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 28 年度秋期	46.3%	76.6%
平成 29 年度春期	53.0%	77.8%
平成 29 年度秋期	47.9%	76.8%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 29 年度秋期の午前Ⅰ試験の合格率は，平成 29 年度春期に比べると約 5 ポイント低下し，1 年前に実施された平成 29 年度春期に比較しても 1.6 ポイントしか向上していません。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 47.9%という数字は，低い部類に入る数値です。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，76.8%でした。約 8 割弱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 30 年度春期試験では平成 28 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 28 年度秋期から平成 29 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 28 年秋期	平成 29 年春期	平成 29 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	3	2	2
	サービスマネジメント	2	3	3
ストラテジ系（8 問）	システム戦略	3	3	2
	経営戦略	3	3	4
	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 年度秋期から平成 29 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 28 年秋期	平成 29 年春期	平成 29 年秋期
技術要素	セキュリティ	17	18	17
	ネットワーク	3	2	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（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，ここ数回変わっていません。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，定着したといえます。また，新傾向問題といえるものは次の 5 問で前回から 1 問増えています。細かい知識を問う少し難しい問題が多いといえます。

・問 8　アクセシビリティ設計に関する規格の適用目的
・問 14　サイバーレスキュー隊（J-CRAT）の役割
・問 24　情報システムの開発で多段階契約を採用する目的
・問 27　国際標準に適合した製品を製造及び販売する利点
・問 28　IoT 技術のエッジコンピューティングの説明

問題の出題形式としては，文章の正誤問題が 19 問（前回 18 問），用語問題が 4 問（前回 2 問），計算問題が 4 問（前回 2 問），考察問題が 3 問（前回 8 問）で，前回と比べて考察問題が減った分，他の計算，文章の正誤，用語問題が増えました。出題内容としては，従来，少し難しい問題が多い傾向にあった基礎理論の問題が比較的解答しやすい内容だったといえます。全体としては，新傾向問題が少し難しい内容でしたが，従来からよく出題されている定番の内容も多かったこと

から，普通レベルだったといえます。

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，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……相関係数，符号化されたビット列の長さ，再帰関数，平均アクセス時間，MTTR の短縮，タスクの状態遷移，論理回路，アクセシビリティ設計，射影と同じになる SQL 文，データマイニング，CSMA/CD，ドライブバイダウンロード攻撃，暗号方式，サイバーレスキュー隊（J-CRAT），WAF，モジュール強度（結束性），CMMI

・マネジメント分野……EVM の管理対象，保守性の評価指標，可用性の計算，システム監査人の行動，在庫データの網羅性チェック

・ストラテジ分野……エンタープライズアーキテクチャ，多段階契約，半導体ファブレス企業，CRM，国際標準の適合，IoT 技術のエッジコンピューティング，デルファイ法，著作権の帰属

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 29 年度春期試験から減少した他，過去問題の出題は平成 28 年度春期試験から 9 問もあったことから，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，平成 29 年度春期試験で，はじめてセキュリティが 18 問，ネットワークが 2 問になりましたが，今回，再びセキュリティが 17 問，ネットワークが 3 問という比率に戻りました。

セキュリティ分野の 17 問のうち，15 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 2 問でした。また，攻撃手法の説明やその対策などに関する問題は，前回の 6 問に続き，今回も 4 問出題されていました。新規問題は，問 6（DNS に対するカミンスキー攻撃への対策），問 8（暗号化装置の秘密鍵を推定する攻撃），問 11（是正処置の定義），問 16（ディジタルフォレンジックスで行う証拠の保全順序）の 4 問でした。これに対し，過去問題からの出題は，平成 28 年度春期から 9 問，平成 27 年度秋期，平成 26 年度秋期，平成 26 年度春期から各 1 問の他，平成 28 年度春期 AP 試験から 1 問の計 13 問が出題されていました。17 問のうち，レベル 4 の問題といえるものは，問 4（ハッシュ関数の衝突発見困難性），問 13（情報システムの脆弱性の深刻度に対する評価基準）と問 16 で，その他はいずれも標準レベルといえます。

ネットワーク分野の 3 問は，いずれも過去問題で，平成 23 年度春期から 1 問，平成 22 年度秋期から 1 問の他，平成 27 年度秋期 NW 試験から 1 問が出題されていました。いずれも，標準のレベル 3 の問題です。

データベース分野の問 21（ビッグデータ解析に利用されるニューラルネットワーク）は，新規問題であることから，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（満足性の品質副特性の一つである実用性の説明），問 23（著作権の帰属先）とも新規問題ですが，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（フェールソフトの考え方）は平成 25 年度春期で出題されたもの，問 25（システム監査を実施する場合の監査責任者とメンバ）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。しかし，各問とも，数十字で述べる記述式の設問が，平成29年度春期試験よりも増加しているので，それぞれの問題の記述内容を十分に把握しながら丁寧に取り組んでいくことが必要です。また，各問とも小問数が，平成29年度春期試験に比べると多かったことから，些細なミスを積み重ねると，合格基準点に達しなくなります。あくまでも問題文に記述された内容や条件を十分に考慮するとともに，設問で問われていることを確認しながら，丁寧に解答を作成していくことが要求されます。

問1　ランサムウェアへの対策

問題のテーマはランサムウェアへの対策ですが，ランサムウェアが被害を拡大する原因となったPCの設定とランサムウェアの特徴，ランサムウェアによって暗号化されたファイルの復号が困難である理由，シャットダウンしてしまうとファイルの復号できる可能性が低くなる理由などを答える問題です。解答を作成するためのキーワードは，問題文中に記述されていますので，一定の知識レベルにあれば，問題の記述内容から解答を導いていくことができます。記述式の設問が多くありますが，難易度については，標準レベルの問題といえます。

問2　Webアプリケーション開発におけるセキュリティ対策

本問は，Javaコードによるプログラムに含まれるSQLインジェクションやクロスサイトスクリプティング（XSS）脆弱性の他，Cookieの属性，リダイレクタ機能を利用するためのホワイトリスト方式の仕様，脆弱性検査手順の改善方法，WAFの導入によって低減できるリスクなどを述べるものです。Javaや Cookieの知識が要求されるほか，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必要となります。難易度については，標準レベルの問題といえます。

問3　SSL/TLSを用いたサーバの設定と運用

問題のテーマは SSL/TLS を用いたサーバの設定と運用ですが，出題内容は，サーバ証明書の検証などを中心とした問題となっています。また，POODLE 攻撃や，PFS（Perfect Forward Secrecy）とは何か，ドメイン認証証明書とEV証

明書の違いなどをしっかりと把握していれば，解答を作成しやすいといえます。難易度を全体的に評価すれば，標準レベルの問題でしょう。

(4) 午後Ⅱの問題

午後Ⅱ試験は，問 1 が IoT システムのセキュリティ対策，問 2 がデータ暗号化の設計というテーマですが，問 2 は，暗号化と DBMS を中心とした問題となっていますから，問 2 の選択者はかなり絞られるのではないかと思われます。

また，問 1，問 2 とも，問題文の中でシステムに関する仕様の部分がかなり多く記述されていました。これらの仕様をよく把握しながら，解答を作成していく必要がありますので，受験者の中には苦労された方も多かったのではないでしょうか。時間的な余裕はあまりなかったと思われますが，設問に関連した必要な記述箇所をよく読み返しながら，解答を作成すれば，正解にたどり着くことができると考えられます。今回の午後Ⅱ試験は，あわてず，あせらず，あきらめずの精神で臨むことが，特に必要だったと思われます。難易度を全体的に評価すると，平成 29 年度春期試験とほぼ同程度と考えられます。

問 1　IoT システムのセキュリティ対策

本問では，IoT 機器（Z カメラというネットワークカメラ）のセキュリティ検査，Z カメラがもつカメラ IF（インタフェース）通信に対する脅威，Z カメラ操作及び動画管理のアプリケーションを提供する Z クラウドに対する脅威についての問題が出題されています。問題が 14 ページにわたっていますので，設問に関連する記述箇所を的確に読み直すなどして，うまく解答を考えていくことが必要です。技術的な知識については，TCP ポートスキャンや中間者攻撃，DNS キャッシュポイズニング攻撃などに限られていた半面，その分，問題文に記述されたシステムの仕様を的確に捉えた上で，解答を作成するという記述式の設問が大半を占めています。このため，これらの記述式の設問にどれだけ正解できるかが，合格基準点をクリアできるかどうかの分かれ目となりそうです。

問 2　データ暗号化の設計

本問のテーマは，データ暗号化の設計ですが，出題内容は，DES アルゴリズムの解読時間，安全な鍵管理の仕組み，暗号モジュールに求められるセキュリティ要件，製品の仕様に基づいてバックアップシステムのデータベースを暗号化する

方法，システムから契約情報を取得するための方法などとなっています。穴埋め問題は，字句の選択方式ではなく，用語をそのまま答えるものでしたから，用語自体を正確に覚えている必要があります。また，記述式の設問は，暗号モジュール製品の仕様に基づいて答えるものに比重が置かれていましたし，一部，複雑な仕様の条件をうまく整理しながら解答を考察していく必要のものも見られました。問 1 と同様に，問題が 14 ページにわたっている上に，暗号モジュール製品の仕様を理解することが大変だったと思われます。このため，問 2 の方が，問 1 よりも解答作成に苦労するかもしれません。