情報処理安全確保支援士

1.　はじめに

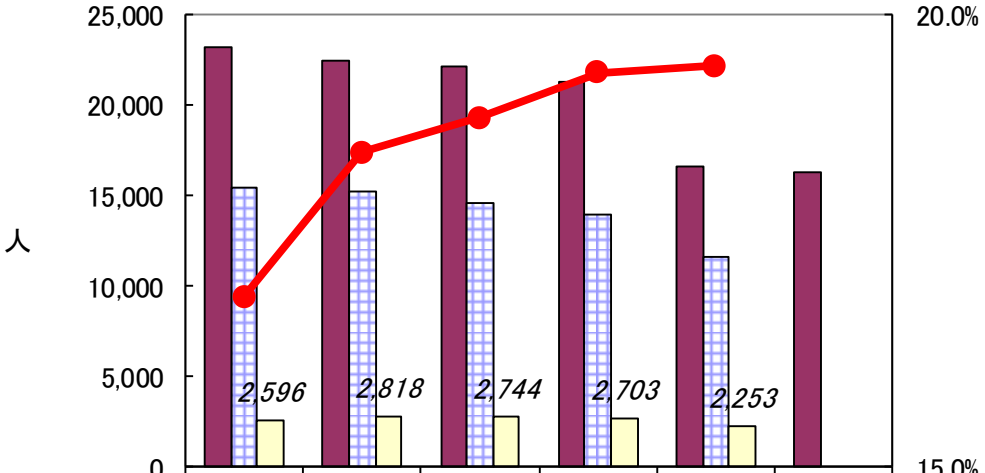
1.1　総評

今回の情報処理安全確保支援士試験は，情報セキュリティの実務で柱となるマルウェア対策，インシデント対応，脆弱性対策，ネットワークセキュリティなどに関する出題のほか，特に認証サービスとの認証連携についての出題が目立っていました。また，積極的に新しいセキュリティ技術を出題する傾向が感じられる試験でもありました。

午後問題の特徴は，認証サービスとの認証連携に関する問題が午後Ⅰと午後Ⅱの両方で出題されたこと，DNS セキュリティを主題とした問題が出題されたこと，前回に続いてテレワーク環境整備を意識したクラウドセキュリティに関する出題があったこと，セキュアプログラミングに関する出題が一切なかったことです。

午前Ⅱ試験の難易度は標準的で，午後Ⅰ試験は前回に比べると難易度は下がっていますが，特定の技術的知識が求められる難易度の高い問題も含まれていました。午後Ⅱ試験の難易度も前回よりは下がっていますが，ネットワークセキュリティを中心に幅広い技術的知識が問われたクラウドセキュリティの問題は難易度の高い問題でした。

1.2　受験者数の推移



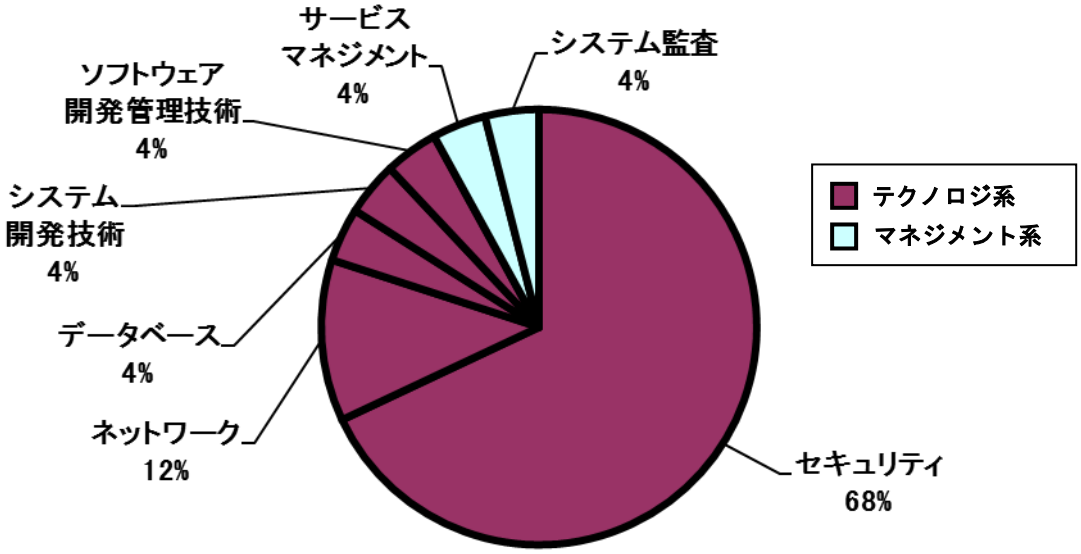
	H30春	H30秋	H31春	R1 秋	R2 10月	R3 春
応募者数	23,180	22,447	22,175	21,229	16,597	16,273
受験者数	15,379	15,257	14,556	13,964	11,597	
合格者数	2,596	2,818	2,744	2,703	2,253	
合格率	16.9%	18.5%	18.9%	19.4%	19.4%	

2. 午前Ⅱ問題の分析

2.1 問題テーマの特徴

分野ごとの出題数に変化はなく，重点分野でレベル 4 の「セキュリティ」が 17 問，「ネットワーク」が 3 問出題されました。レベル 3 の「データベース」「システム開発技術」「ソフトウェア開発管理技術」「サービスマネジメント」「システム監査」の各分野は 1 問ずつとなっています。

出題分野	出題比率	出題数
セキュリティ	68%	17 問
ネットワーク	12%	3 問
データベース	4%	1 問
システム開発技術	4%	1 問
ソフトウェア開発管理技術	4%	1 問
サービスマネジメント	4%	1 問
システム監査	4%	1 問



「セキュリティ」分野をさらに小分類に細分化してその内訳を見てみると，前回の試験において，それまでの攻撃手法や情報セキュリティ技術に関する「情報セキュリティ」からの問題が過半数を占めるという出題傾向が変化して，「セキュリティ技術評価」以外の各小分類から万遍なく出題されていました。今回もその傾向は続いていて，「情報セキュリティ」と「情報セキュリティ対策」「セキュリティ実装技術」の 3 分野から均等に，そして「情報セキュリティ管理」「セキュリティ技術評価」から 1 問ずつと，すべての小分類から出題されました。

セキュリティ分野の小分類	出題数			
	R3 春	R2 10 月	R1 秋	H31 春
情報セキュリティ	6 問	5 問	9 問	11 問
情報セキュリティ管理	1 問	3 問	1 問	0 問
セキュリティ技術評価	1 問	0 問	1 問	0 問
情報セキュリティ対策	4 問	3 問	0 問	1 問
セキュリティ実装技術	5 問	6 問	6 問	5 問

「セキュリティ」分野の新規出題には最新のセキュリティトピックをテーマとしたものが多いという特徴がみられます。2019 年に告示されたシラバス追補版(午前Ⅱ)で追加された知識事項からの出題としては，可視化や制御を担うポイントを設けて一貫性のあるポリシを適用可能とするような，クラウドサービスでの情報セキュリティの実装概念である CASB(Cloud Access Security Broker)を利用した際の効果を問う問題が挙げられます。また，2017 年から認証局の証明書発行時に確認が義務化された DNS CAA(Certification Authority Authorization)レコードの問題や，公衆無線 LAN などのオープンネットワークで認証なしに端末とアクセスポイント間の通信を暗号化できるセキュリティ規格である Enhanced Open の問題などが特徴的です。そのほかの新規問題としては，UDP サービスの視点からのリフレクタ攻撃の問題や HSTS に関する問題などがありますが，これらはこれまでも出題されてきた事項を新しい切り口で出題したものでした。

「ネットワーク」分野からの新規出題としては，ETSI(欧州電気通信標準化機構)が提唱するネットワーク機能をソフトウェアや仮想化技術などを用いて実現する NFV の問題とループバックアドレスに関する問題が挙げられます。

2.2　難易度の特徴

過去問題の再出題率は，これまでと大きな変化は見られませんが，特に「セキュリティ」分野では，17 問中 11 問を SC からの過去問題が占めていました。中でも平成 31 年度春の SC 試験からは 7 問も出題されていて，平成 31 年度春の問題演習を行っていれば，明らかに有利だったと考えられます。「セキュリティ」分野の 17 問中 6 問が新規問題でしたが，このうち“Web アプリケーションにおける攻撃と対策の組合せ”はこれまでに何度も出題されてきた SQL インジェクション対策の問題でした。また，“HSTS”，“リフレクタ攻撃”の問題は新しい切り口からの出題ではありますが，難易度的にはそれほど高い問題ではありません。問題テーマの特徴で紹介した 3 問は，最新のセキュリティトピックをテーマとした難易度の高い問題でしたが，「セキュリティ」分野全体で見れば，やや易しめといえるでしょう。

重点分野の一つである「ネットワーク」分野では，3 問中 2 問で新規テーマが出題されていましたので，「セキュリティ」分野に比べると難易度は高かったといえるでしょう。

総合的に判断すると，前回と比較すればやや易しめではありますが，SC 試験としては標準的な難易度の試験でした。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	リフレクタ攻撃に悪用されることの多いサービス	B
2	OCSP の利用目的	A
3	ハッシュ関数の衝突発見困難性	B
4	Smurf 攻撃	A
5	サイドチャネル攻撃	A
6	ステートフルパケットインスペクション方式のファイアウォールの特徴	A
7	AES における鍵長の条件	B
8	CVE 識別子の説明	B
9	サイバー情報共有イニシアティブ(J-CISP)	B
10	DNS CAA レコードによるセキュリティ上の効果	C
11	CASB の効果	C
12	Web アプリケーションにおける攻撃と対策の組合せ	A
13	ビヘイビア法	A
14	OP25B の導入目的	A
15	HSTS	B
16	VDI サーバを利用した情報流出防止	B
17	RFC 8110：Enhanced Open	C
18	NFV	C
19	リンクアグリケーション	B
20	ループバックアドレス（127.0.0.1）	C
21	バッチ処理におけるデッドロックの回避	B
22	JIS X 25010　機能適合性	B
23	XP におけるテスト駆動開発	A
24	ディスク障害時のデータベース回復　ロールフォワード	B
25	セキュリティ確保の取組における監査人の指摘すべき事項	B

注)難易度は 3 段階評価で，C が難，A が易を意味する。

3. 午後Ⅰ問題の分析

3.1 全体の出題傾向及び難易度について

今回の午後Ⅰ試験は，セキュリティ技術知識とその応用に重点が置かれているという点でこれまでと同様です。大枠のテーマの特徴は，DNS セキュリティを主題とした問題が出題されたことと，セキュアプログラミングやインシデント対応を題材とした問題が出題されなかったことです。午後Ⅰ試験でセキュアプログラミングとインシデント対応が出題されないという傾向は前回に続くものです。

扱われた題材は，認証システム，DNS セキュリティ，脆弱性対策やマルウェア対策といった頻出テーマですが，基礎的な内容から新しい技術的知識までが幅広く出題されている問題といえるでしょう。

新しい技術的知識が問われた例としては，問 1 の認証システムの開発で，多要素認証を実現するために，認証及び認可を提供する SNS と OAuth を用いて認証連携することに関する問題や，問 3 のエンドポイントでの不正な挙動を検知して速やかに対応する EDR を絡めたマルウェア対策や脆弱性対策が問われた点，遠隔地から PC の電源を入れる Wake on LAN について出題された点などが挙げられます。

セキュリティ技術に関する知識をそのまま解答する設問は少なく，多くは，事例として提示されている記述や図表を読み取り，その内容や条件に合わせて知識を応用させて解答を導く設問がほとんどでした。ただ，詳細な専門的知識が問われた設問はそれほど多くはありませんでした。

3.2 各問題のテーマ，特徴

問 1 は，OAuth による認証及び認可を提供する SNS との認証連携を題材にした認証技術に関する問題です。OAuth については，午前Ⅱ問題では何度か出題されましたが，午後問題で取り上げられたのは初めてです。OAuth に関する知識が必要ですが，提示された「OAuth を用いた認可のシーケンス」の図や「攻撃のシーケンス」の図に示された中間者攻撃を理解することで解答できる設問が多い問題でした。また，穴埋め問題はどれも専門知識を問うタイプの問題ではなく，図や問題文の内容の理解を確認するタイプの問題でした。難易度は標準的です。

問 2 は，DNS サーバに対する代表的な攻撃手法やその対策を題材とした DNS セキュリティを主題とした問題です。権威 DNS サーバやフルサービスリゾルバ，スタブリゾルバに関する基礎的知識と DNS リフレクタ攻撃と対策，DNS キャッシュポイズニング攻撃と対策，DNSSEC，権威 DNS サーバのゾーンファイルやゾーン転送要求に対する設定と DNS サーバの変更に対応するための FW の設定内容と，DNS を主題に幅広く問われました。頻出事項も多く，いずれの問題も基本的な知識と問題文を正しく読み取ることで解答が可能な問題で，難易度は易しめといえるでしょう。

問 3 は，EDR を絡めたマルウェア対策・パッチマネジメントについて問う問題です。新規

性の高い問題で，エンドポイントでの不正な挙動を検知して速やかに対応する EDR を用いたシステム構成でのエージェントによる対策の実現方法や Wake on LAN の起動パケット(マジックパケット)に関する知識が問われました。3 問の中では，もっとも専門知識の有無が問われる問題といえます。特に，起動パケットの内容についての設問やブロードキャストを他の LAN に送信するための L3SW の設定について問われた設問は難易度の高いものといえるでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	認証システムの開発	B
2	ネットワークのセキュリティ対策	A
3	セキュリティ運用	C

注)難易度は 3 段階評価で，C が難，A が易を意味する。

4. 午後Ⅱ問題の分析

4.1 全体の出題傾向及び難易度について

午後Ⅱ問題は，午後Ⅰ問題の 2 倍以上の長さの問題文が提示されます。そのため，単にセキュリティ技術を問うだけでなく，セキュリティ管理の側面からも解答を導き出すことが求められる設問が含まれることが多くなります。また，幅広い設問テーマを含めることができる容量や柔軟性が問題文にあるため，個々の設問レベルのテーマとしては，大枠のテーマに直接関係のある内容だけでなく，幅広い分野について問われる総合問題となることが多いという傾向があります。今回の問題も標準的な総合問題で，セキュリティ技術とセキュリティ管理の設問テーマがバランスよく配置されていました。

問題テーマとしては，定番の情報セキュリティインシデント対応と体制の整備，認証連携技術や無線 LAN セキュリティ，クラウドサービスの連携が扱われていました。なお，問 1 では NIST 文書(SP 800-61 Rev.2)のインシデント対応のライフサイクルが，問 2 ではクラウドサービス事業者の第三者認証の規格・制度について出題された点が目を引きます。

4.2 各問題のテーマ，特徴

問 1 は，パスワードリスト攻撃や SSH による不正アクセス等を題材にしたインシデント対応や体制整備に関する問題です。プレフィックス表記の理解が問われる設問や，状況設定に応じた計算が必要な設問，リスクベース認証，NIST のインシデント対応のライフサイクルなど，多彩な知識や応用が問われていました。パスワードリスト攻撃の説明やその対策としてのパスワードの設定方法，N-CSIRT の構成部門である情報セキュリティ委員会などのような基本的な知識が問われた設問や日本標準時が協定世界時に対し何時間進んでいるかといった設問など単純な知識問題も含まれていて，取り組みやすい問題となっていました。

また，解答字数の制限は余裕を持たせたものが多く，解答をまとめる際に字数不足で困ったという受験者は少なかったでしょう。しかし，問題文と設問文で 12 ページと長く，図と表も合わせて 13 も含まれていて，図の注記までしっかりと読む必要があることから，難易度は標準的と判断しました。

問 2 は，クラウドセキュリティという大枠のテーマに，SAML による認証連携や無線 LAN セキュリティ，DHCP サーバの割当て IP アドレスの枯渇，PKI によるクライアント認証，クラウドセキュリティ認証制度など，ネットワークセキュリティを中心とした幅広い技術的知識が問われた問題でした。クラウドサービスの認証連携は，前回の午後Ⅱ試験でも問われていて，連続での出題になりました。それ以前では平成 30 年秋の午後Ⅱ問題，平成 29 年春の午後Ⅰ問題でも出題されていて，出題頻度が高まっています。

また，この問題では絞り込みに迷う解答を，“一つ答えよ”という形でさばく設問が多く見られたという特徴があります。

設問で問われた専門的知識の難易度の高さから，難易度は高いと判断しました。

4.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	インシデント対応体制の整備	B
2	クラウドセキュリティ	C

注)難易度は 3 段階評価で，C が難，A が易を意味する。

5. 今後の対策

5.1 午前Ⅱ対策

午前Ⅱ試験は，重点分野の「セキュリティ」と「ネットワーク」の 2 分野の合計が 8 割を占めます。午前Ⅱ試験に合格する基準は 60 点以上なので，この 2 分野で取りこぼすことなく確実に得点できれば，午前Ⅱ試験に合格できます。したがって，「セキュリティ」と「ネットワーク」の 2 分野に的を絞った学習が，効率の良い午前Ⅱ対策です。

セキュリティやネットワークに関する学習は，まずはテキストを用いて体系的に知識を習得することが大切です。そのほうが知識の関連性も把握しやすく，単独の知識を詰め込むよりも学習効果が高いでしょう。この 2 分野の知識はそのまま午後試験でも必須の知識となるので，一度体系的な学習を行っておくことで，午前Ⅱ対策から午後対策へとスムーズに移ることができます。特に出題されやすいのが，攻撃と PKI です。さまざまな攻撃手法とその対策について，暗記するのではなく，仕組みをよく理解するように学習してください。PKI についても，認証局の役割，認証局の階層構造に基づいて証明書の信頼性を保証する仕組み，証明書の構成，証明書発行手順，失効確認など，午後対策も見据えて体系的に学習しておくとよいでしょう。

過去問題の再出題率が 7 割近くあることを踏まえますと，知識習得後は過去問題の演習が必須です。過去問題演習も「セキュリティ」と「ネットワーク」の 2 分野に絞って効率的に行うとよいでしょう。できるだけ多くの過去問題演習を行うのに越したことはありませんが，少なくとも直近 5 回分は繰り返し行ってください。特に 3 回前の試験からの再出題率が高いことから，試験直前に 3 回前の過去問題演習を行うことは非常に効果的です。演習後は正解した場合でも必ず解説を読み，誤答の選択肢についての知識も確認しておくと，知識が広がり，類似問題が出題された場合にも対応できるようになります。また，問題演習を通じて苦手なテーマを洗い出し，あいまいな知識をテキストで再確認すると，弱点補強に役立ちます。

また，IPA のホームページに掲載されている「情報処理安全確保支援士試験　シラバス追補版(午前Ⅱ)Ver3.1」には，午前Ⅱにおける知識の細目が示されています。具体的な用語例が掲載されているので，確認しておくとよいでしょう。

さらに，新しい攻撃について出題されることがたびたびあるので，日頃から IT 関連のニュースに注目し，新しい攻撃についての情報収集を行っておくと役立つでしょう。国の組織の新たな取組みや新たに策定された基準などが出題されることも考えられ，IPA や NICT のホームページで公開されているセキュリティ情報もチェックするとよいでしょう。

5.2 午後Ⅰ対策

午後Ⅰ対策でまず必要となるのは，より深い知識の習得です。午前Ⅱレベルの知識だけでは，問題事例の内容を正しく理解することはできません。たとえ，問題文中に解答のヒントとなる記述があっても，気付くことさえできないかもしれません。よく出題されるテ

ーマは，アクセス管理，マルウェア対策，暗号技術，認証技術，ログ管理，ネットワークセキュリティ，Web アプリケーションセキュリティ，メールシステムのセキュリティ，DNS のセキュリティ，PKI，無線 LAN セキュリティ，TLS，プロキシサーバ，クラウドセキュリティなどです。これらについて，重点的に学習し，理解を深めておいてください。

今回，認証連携についての出題が目立ちましたが，SSO のケルベロス認証や SAML，アクセス認可に利用される OAuth などを確認しておくこともお勧めします。

また，セキュリティインシデント対応の事例は午後Ⅰ・午後Ⅱ試験ともに頻繁に出題されていることから，インシデント対応の流れに沿って学習することも欠かせません。インシデント対応に関する過去問題をピックアップして集中的に演習を行うのも効果的です。そして，異常が発生している PC を特定するのに必要となるログの見方やネットワークコマンドの表示結果の見方，証拠を保全するための手順や注意点，マルウェア感染範囲や感染経路を特定するためのファイアウォールのルールの読取り，マルウェア対策ソフトや脆弱性修正プログラムの運用上の注意点，出口対策としてのフィルタリングの設定など，共通的な知識を洗い出して習得しておくと，さまざまなインシデント対応事例の問題に活用できると思います。

セキュアプログラミングに関する問題は，これまで毎回 1 問は出題されてきましたが，3 回連続して出題されていない状況です。しかし，今後も出題されないとは限りませんので，バッファオーバフロー，クロスサイトスクリプティング，クロスサイトリクエストフォージェリ，SQL インジェクションなどを中心に学習しておくとよいでしょう。IPA の“安全なウェブサイトの作り方”や“セキュアプログラミング講座”に掲載されている内容から出題されることが多いので，活用するとよいと思います。

午後Ⅰ対策としては，ネットワーク技術知識の習得も重要です。問題事例には多くのプロトコルが出てきます。IP，ICMP，ARP，TCP，UDP，HTTP，DNS，SMTP，LDAP，NTP，DHCP，SSH などの知識は，問題文を読み取るうえで必須となります。午前Ⅱで出題されるような用語説明レベルの知識では不十分ですので，午後問題演習に入る前にネットワークの知識の再確認をするとよいでしょう。

そして，午後Ⅰ対策でも問題演習を行うことは必須です。特に実務経験が少ない場合は，さまざまな問題演習を通して実務に近い事例を見ておくことが非常に有効です。事例には，ネットワーク構成図が提示されることもよくあります。通信の流れがどのようになっているかを，事例中の記述，ファイアウォールのルール，ネットワーク構成図を照らし合わせて把握できるようにしておきましょう。知識を持っていても問題事例に合わせて知識を適用させることができない場合は，読解力不足であると考えられます。また，事例内容とは異なる自分の経験だけから解答を導いてしまい，正解を得られないこともあります。「問題文を図表も含めてよく読む」「設問文の要求に答える」ということは当たり前のことですが，久しぶりに受験する場合は特におろそかになりがちかもしれません。試験に慣れるためにも，多くの午後Ⅰ問題演習を行ってください。解説には，その問題を解くうえでの技術知識の説明だけでなく，解答を導出するまでのポイントも説明されているので，解説をしっ

かり読むことも大切です。繰り返し問題演習を行い，解答解説から正解表現と自分の解答表現の違いや解き方の違いを把握して見直すことで，問題文や設問文で見落としやすいポイントを学ぶと同時に，解答表現力を養ってください。

5.3　午後Ⅱ対策

午後Ⅱ対策は基本的には午後Ⅰ対策と同じです。追加で行うべき対策としては，セキュリティ管理面の知識を強化しておくことが挙げられます。例えば，人的管理，リスク管理，サイバーセキュリティ基本法，個人情報保護法，不正競争防止法などについて，知識を習得しておいてください。セキュリティ関連法規は，午前Ⅱ試験では出題範囲外ですが，午後試験では出題範囲に含まれているので，注意が必要です。

セキュリティ技術知識については，出題される範囲は午後Ⅰ試験と同一ですが，より詳細なレベルまで問われることがあります。問題演習を行う場合は，午後Ⅰ問題とは別に午後Ⅱ問題の演習も必ず行い，習得した技術知識のレベルが必要とされる技術知識のレベルに達しているかを確認しておくとよいでしょう。

そのほか，午後Ⅱ問題特有の長文問題に対する短時間での読解に慣れておく必要があります。細かい図表が多く提示される場合もあり，問題事例を把握するだけでも相当な時間と集中力が必要になります。午後Ⅱ問題では午後Ⅰ問題以上に設定条件も複雑になり，読解力が大きなカギを握っています。問題文や設問文で提示された条件や要求事項の関係がどのようになっているのかを整理し，誤りなく見極めることに留意して問題演習を行うことが重要です。問題文の分量が多いため，何度もページをめくることになり，ポイントとなる記述を見落としがちになります。また，ポイントとなる記述が複数箇所に埋め込まれており，何ページか離れた図の注記に記されているようなこともあります。重要と考えられる字句や，関連性があると思われる記述には線を引いたり，しるしをつけたりするなど，ポイントを見落とさない工夫を自分なりに見つけて問題演習を行うとよいでしょう。