情報処理安全確保支援士

1.　はじめに

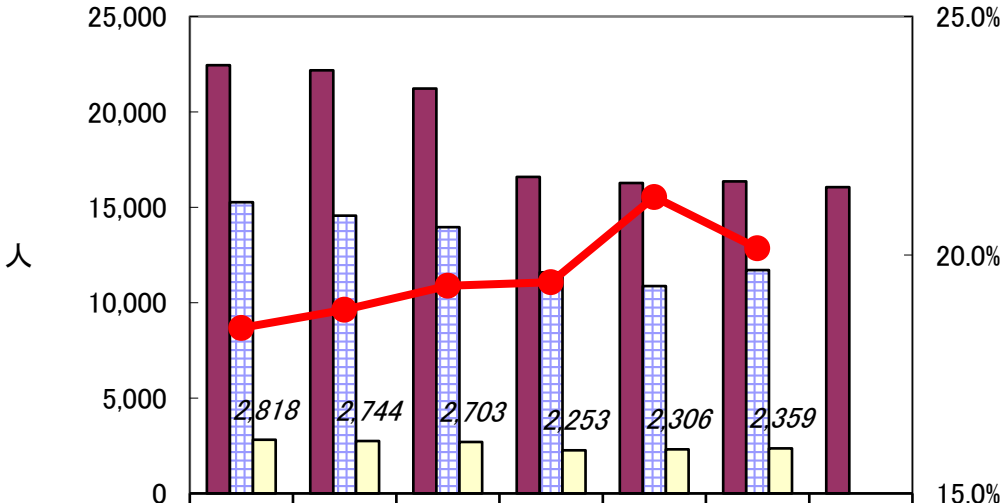
1.1　総評

今回の情報処理安全確保支援士試験(SC)の特徴は，情報セキュリティ実務で柱となるセキュリティインシデント対応，定番の Web サイトのセキュリティ対策やセキュアプログラミング，脆弱性対策などに関する出題のほか，特に，各種法令に基づく身元確認方法，CDN(Content Delivery Network)活用時のセキュリティ，アジャイル開発での脆弱性診断など，新しい視点の出題内容が目立つことです。また，最近よく扱われる認証連携に関する内容も継続して出題されていました。

午前Ⅱ試験は，前回，例年より難易度の高い試験になっていましたが，今回はセキュリティ分野の新規問題は前回よりも減っており，その分過去問題の再出題が増えていましたので，難易度は標準的です。

一方，午後Ⅰ・午後Ⅱ試験はともに，特定の技術的知識や対応力が求められる設問の割合が例年に比べると高く感じられ，全体的な難易度は前回に比べてやや高めといえます。

1.2　受験者数の推移



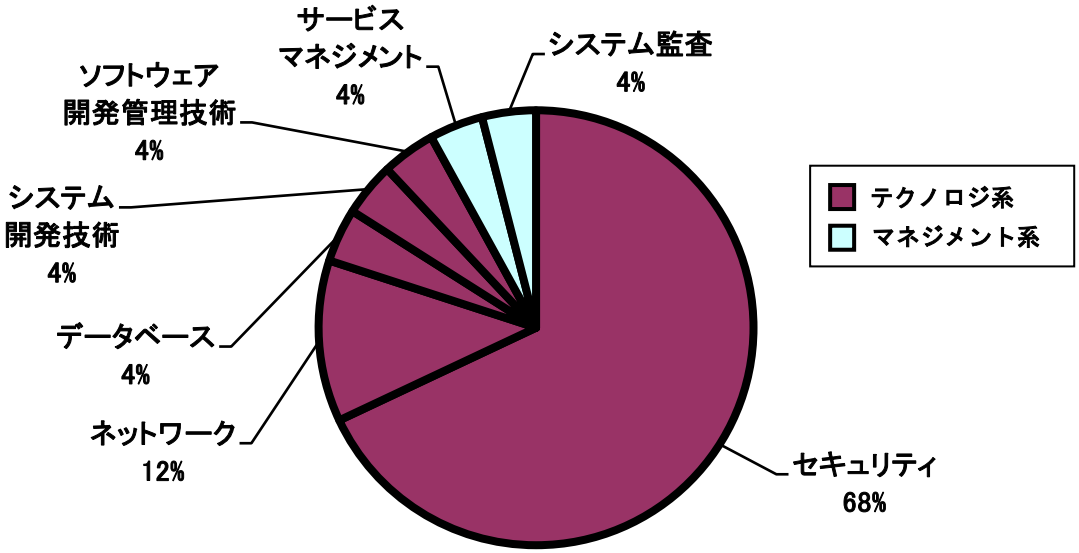
	H30秋	H31春	R1秋	R2 10月	R3春	R3秋	R4春
応募者数	22,447	22,175	21,229	16,597	16,273	16,354	16,047
受験者数	15,257	14,556	13,964	11,597	10,869	11,713	
合格者数	2,818	2,744	2,703	2,253	2,306	2,359	
合格率	18.5%	18.9%	19.4%	19.4%	21.2%	20.1%	

2.　午前Ⅱ問題の分析

2.1　問題テーマの特徴

分野ごとの出題数は毎回同じです。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，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 問ずつです。

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



セキュリティ分野について，小分類に細分化してその内訳を見てみると，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」からの出題は前回に比べると減っています。今回のセキュリティ分野の新規問題は 6 問でしたが,そのうちの 2 問が「情報セキュリティ」の問題でした。また，今回の試験では例年に比べて「情報セキュリティ管理」からの出題が多くなっています。これは，3 回前の過去問題が多く出題されるという傾向によるものと考えられます。

セキュリティ分野の小分類	出題数			
	R4 春	R3 秋	R3 春	R2 10 月
情報セキュリティ	6 問	9 問	6 問	5 問
情報セキュリティ管理	4 問	1 問	1 問	3 問
セキュリティ技術評価	0 問	1 問	1 問	0 問
情報セキュリティ対策	2 問	2 問	4 問	3 問
セキュリティ実装技術	5 問	4 問	5 問	6 問

セキュリティ分野の新規問題は，次のとおりです。

・パスワードの理論的総数の数式
・サイバーキルチェーンにおける偵察段階の行動
・量子暗号の特徴
・SECURITY ACTION
・サイバーセキュリティ経営ガイドライン(Ver2.0)
・IMAPS

このうち，初出題の用語は“サイバーキルチェーンにおける偵察”，“量子暗号”，“SECURITY ACTION”，“IMAPS”です。サイバーキルチェーンという用語そのものは，前回の試験でも出題されましたが，今回はさらに具体的に“偵察”という段階における行動について問われていて，難易度が高くなっています。量子暗号の問題では，通信におけるワンタイムパッド(OTP：One Time PAD)方式について問われ，他には中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度である SECURITY ACTION や，メール受信者がメールサーバからメールを受信する時に暗号化をするプロトコル IMAPS について問われました。

その他の分野の新規用語は，ネットワーク分野の NTP のクライアント向け簡略版プロトコルである“SNTP(Simple Network Time Protocol)”と，データベース分野のデータウェアハウス内のデータのトレーサビリティを確保するためのメタデータである“データリネージ(data lineage)”，ソフトウェア開発管理技術分野のソフトウェアライフサイクルプロセスの JIS 最新版である JIS X 0160:2021 での“修整(tailoring)”でした。

2.2 難易度の特徴

前回の午前Ⅱ試験は難易度が高く，例年 85%以上ある突破率が 80%に下がっていました。しかし，今回の午前Ⅱ試験はセキュリティ分野の新規問題の数も前回よりも少なく，その分，過去問題が増えていましたので，標準的な難易度と言えます。午前Ⅱ試験の突破率も例年どおり，85%以上に戻ると思われます。

過去問題の再出題率は，セキュリティ分野で 17 問中 11 問と 64%を超えています。ネットワーク分野でも 3 問中 2 問が過去問題でしたので，重点分野 20 問中の 13 問が過去の SC からの過去問題です。過去問題演習が非常に効果的な学習方法であることが分かります。SC では 3 回前の試験の再出題率が高い傾向がありますが，今回も 3 回前の令和 2 年度秋から 8 問が出題されています。この回を含めた過去問題演習を行っていれば，明らかに有利でした。

2.3 問題テーマ難易度一覧表

問	テーマ	分野名	難易度
1	OS コマンドインジェクション	セキュリティ	B
2	SAML	セキュリティ	B
3	サイドチャネル攻撃	セキュリティ	A
4	パスワードの理論的な総数を求める数式	セキュリティ	A
5	サイバーキルチェーン　偵察	セキュリティ	C
6	量子暗号の特徴	セキュリティ	C
7	SECURITY ACTION	セキュリティ	B
8	NOTICE	セキュリティ	B
9	サイバーセキュリティ経営ガイドライン(Ver2.0)	セキュリティ	C
10	CRYPTREC の活動内容	セキュリティ	A
11	MITB 攻撃の対策	セキュリティ	B
12	クラウドサービス：PaaS	セキュリティ	B
13	DNSSEC で実現できること	セキュリティ	B
14	HTTP Strict Transport Security の動作	セキュリティ	B
15	TLS	セキュリティ	A
16	IMAPS	セキュリティ	B
17	無線 LAN 環境実現の標準的方法	セキュリティ	B
18	CSMA/CA	ネットワーク	B
19	SNTP	ネットワーク	B
20	スパニングツリープロトコル	ネットワーク	B
21	データリネージ	データベース	C
22	フールプルーフ	システム開発技術	A
23	JIS X 0160:2021 修整	ソフトウェア開発管理技術	B
24	サービス可用性の計算	サービスマネジメント	C
25	IT に係る業務処理統制	システム監査	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

午後Ⅰ試験は，Web アプリケーション開発のセキュリティ対策としてセキュアプログラミング，定番の情報セキュリティインシデント対応の問題，スマートフォン向け QR コード決済サービスの問題として身元確認と当人認証などスマートフォンや IC カードのセキュリティについて出題されました。午後Ⅰ試験でセキュアプログラミングについて問われたのは，令和になって初めてのことです。

3 問ともに，システム機能，設定内容，アクセスログ，ソースコードといった関連図表に示された条件などに基づいて，具体的な状況判断や技術的対応力などを問う構成の問題で占められています。問題分量は，問 1 と問 2 が 6 ページで図表も多く含まれていましたが，問 3 は問題文が 5 ページ，図表は 2 つとややバラつきが見られました。

解答するうえで前提となる技術的知識として，問 1 では PreparedStatement に関連する知識が，問 2 では Linux の sudo コマンドの設定ファイルや tar コマンドに関する知識が，問 3 では金融庁が公表している“犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概要”や政府が犯収法規則の改正において意見公募を実施した際の“警察庁及び共管各省庁の考え方”における本人確認の方法についての知識が求められるなど，かなり特定の専門知識を要求する設問が含まれていましたが，合格点である 60%を取れるかどうかという視点で見るとそこまで難易度の高い問題とはいえません。

また，全体的に記述解答の設問割合が少なめで選択問題や字句を解答する設問が多いため，要求される解答量はそれほど多くはありませんが，技術的知識の有無で解答できるかどうかが決まってしまう設問が多いという傾向が見られます。

3.2 各問題のテーマ，特徴

問 1 は「Web アプリケーションプログラム開発のセキュリティ対策」というテーマで，情報の投稿と表示が可能な情報共有システムの改修を題材にした Web サイトセキュリティとセキュアプログラミングに関する問題でした。午後Ⅰ問題では，H31 年度春試験以来のセキュアプログラミング問題でしたが，問われたのは PreparedStatement に関連する知識で，H29 年秋の午後Ⅰ問題でほぼ同じ内容について問われていました。

具体的には，HTTP ヘッダインジェクションや SQL インジェクション，メールヘッダインジェクションの脆弱性についての知識や対策方法，Web アプリのアクセス制御要件に関する脆弱性，脆弱性を修正したソースコードの穴埋め問題が出題されました。各インジェクションの脆弱性についての設問は基本的な知識で対応が可能で，アクセス制御要件に関する脆弱性も解答ポイントは，GET リクエストのクエリ文字列からの情報取得という設問でした。ソースコードの穴埋め部分も PreparedStatement についての基本的知識があれば対応可能で，SELECT 文の WHERE 条件も，データベースの E-R 図から解答を導ける問題でした。知識の有無で解答できるかどうかが決まる設問が多く，受験者によって感じられる難易度

には差が生じる問題といえますが，求められる技術的知識はそれほど高いものではないため，難易度は標準的です。

問 2 は「セキュリティインシデント対応」というテーマで，NAS(Network Attached Storage)製品及び UPnP 機能を持つルータの脆弱性対策を題材にしたセキュリティインシデント対応の問題でした。

具体的には，ルータの UPnP 機能が WAN 側からは有効化できない理由，ランサムウェアに感染したのが NAS 自体だと判断した理由，ディレクトリトラバーサル対策としてパス名の正規化をする処理の順番，POST メソッドで実行されたコマンドの内容が分からない理由，tar コマンドのオプションが悪用されるのを防ぐ対策，インターネットの検索エンジンで検索されないようにする設定などについて問われています。

URL デコードとパス名の正規化，除外リストとの比較をどの順に行うべきかの設問は実務的な切り口からの出題でした。また，Linux での sudo コマンドの設定ファイルと tar コマンドのオプションを悪用する例を示したうえでの tar コマンドのオプション悪用を防ぐ対策が問われた設問や，検索エンジンに検索されないようにする設定などは，専門性の高い特定の知識が求められるものです。頻出の問題や単純な問題も含まれていますので，問題全体としてみると難易度はやや高めと判断します。

問 3 は「スマートフォン向け QR コード決済サービスの開発」というテーマで，スマートフォン向け決済サービスのサーバプログラムとスマホアプリの開発を題材にした身元確認・当人認証やスマートフォン・IC カードのセキュリティに関する問題でした。

身元確認や当人認証を実施するタイミングや本人確認の方法，ログイン状態を 1 か月保持した場合にサービスが不正利用されるケースやその対策についての，スマートフォンならではの具体的方法などが問われています。この問題では，金融庁による“犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概要”の本人確認方法や“警察庁及び共管各省庁の考え方”に記載されている他人の画像を用いられないようにする方法などが問われているのが特徴的です。これらの知識がなくても多くの設問には対応できますが，他人の画像を用いられないようにする方法は，知識がないと完全に正解するのは難しいと思われます。また，スマートフォンならではの画面ロックをしていない場合の不正利用やその対策は，問題文中にヒントがないため推測して解答することになります。問 3 の難易度は標準的と判断しました。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	Web アプリケーションプログラム開発のセキュリティ対策	B
2	セキュリティインシデント対応	C
3	スマートフォン向け QR コード決済サービスの開発	B

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，長時間で受験者の専門知識の適用能力を探る都合上，設定事例が午後Ⅰ問題の2倍以上の長さの問題文で提示されるため，通常，単にセキュリティ技術を問うだけの設問テーマよりは，技術面・管理面の両側面から解答を導き出すことが求められる設問テーマが多いといえます。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う総合問題となりやすい傾向があります。今回の午後Ⅱ問題も問1については標準的な総合問題といえ，技術面・管理面の設問テーマがバランスよく配置されていますが，問2については，認証連携の方式をひととおり取り上げるという問題の性質上，技術面の設問テーマで占められています。また，問1でサーバサイドリクエストフォージェリ(SSRF)の脆弱性や，アジャイル開発におけるセキュリティ確保に関して出題された点,問2のContent Delivery Network(CDN)を悪用したドメインフロンティング(Domain Fronting)攻撃に関する出題，RFC 7636で規定されたOAuth 2.0の拡張機能であるPKCE(Proof Key for Code Exchange)を利用した認可コード横取り攻撃への対策に関する出題が含まれていた点などは目を引きます。

問題文の分量は，問1は11ページで図表が11点と例年並みでしたが，問2は14ページで図表が13点と非常に多く，午後Ⅰ試験よりもさらに読解力が必要となります。今回の午後Ⅱ試験では，選択問題や字句を解答する問題の比重がとても高いという特徴も見られます。問1で7割，問2に至っては9割近くが選択問題，あるいは字句を解答する問題になっていました。制限字数内に解答をまとめるための時間はあまり必要ないことから，時間的な難易度という点からみると，問2も問題分量の割にはそれほど高くはありません。ただ，各認証連携プロトコルに関する技術的知識がある程度なければ，最終的には判断しにくい設問が含まれていて，問1よりも難易度は高いといえるでしょう。

4.2 各問題のテーマ，特徴

問1は「Webサイトのセキュリティ」というテーマで，クロスサイトスクリプティング(XSS)，クロスサイトリクエストフォージェリ(CSRF)，クリックジャッキング，SSRFといった脆弱性の診断や対策に関するWebサイトセキュリティの総合問題です。

具体的には，XSS脆弱性に関する診断用リクエストと再発防止策，CSRF脆弱性を確認した手順から判明した脆弱性，クリックジャッキング脆弱性の攻撃の仕組みと対策，SSRF脆弱性の具体的な手法や検出手順と対策，アジャイル開発におけるセキュリティ確保の方法や，開発プロセスの見直しなど，幅広い知識が要求されています。クリックジャッキング対策の標準化として，前回の試験でも出題されたContent-Security-Policyを解答する設問も出題されていました。SSRFについては初出題でしたが，問題文で丁寧にその手順などが説明されており，解答ポイントもGETリクエストのパラメタ値の変更やreturnURLの固定化な

どで解答しやすいものでした。目を引いたのは，アジャイル開発に Web セキュリティ管理基準を適用するための策に関する設問です。ネットワークやシステム管理系のバックグラウンドを持つ受験生にとってはやや取り組みにくかったかもしれませんが，この設問の多くは，提示されている表や図の注記に解答のヒントが埋め込まれているので，きちんと読み取れば解答できる設問になっています。問 1 は，幅広い基本的なセキュリティの知識が必要ですが，全体的に解きやすく，難易度は標準的と判断しました。

問 2 は「クラウドサービスへの移行」というテーマで，認証連携によるシングルサインオンを実現するための Kerberos，SAML，OAuth，OpenID Connect といった代表的なプロトコルがすべて扱われ，各方式の連携の流れや特徴的な技術を問う問題です。

令和 2 年 10 月試験以来，午後Ⅱ試験では毎回，クラウドサービスの利用と絡めた認証連携の問題が出題されてきましたが，今回の問 2 は代表的なプロトコルをすべて扱った集大成のような問題です。具体的には，動画サーバでの動画配信に CDN を利用した場合の配信の仕組みや動作，ドメインフロンティング攻撃とその対策，Kerberos 認証への攻撃，SaaS での SAML 認証の流れ，IDaaS と SaaS が事前に共有しておく情報，OAuth2.0 を利用したサービス要求からスケジュール情報取得までの流れ，OpenID Connect を用いた T 社投稿サイトと X 社動画サーバの連携の流れなどに関して出題されました。なかでも，比較的新しい攻撃手法である CDN を悪用したドメインフロンティング攻撃が扱われた点は注目点です。

また，問 2 は 9 割近くが，選択問題と字句で答える設問で，知識の有無で解答できるかどうかが決まる設問が多くなっていました。ただ，令和 3 年春の試験では，OAuth の認可シーケンスや IDaaS のサービス Q と SAML を採用している SaaS との動作概要図などに関して出題されています。認証連携に関する過去問題をきちんと学習していれば有利だったと思われます。以上のことから，問 2 の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	Web サイトのセキュリティ	B
2	クラウドサービスへの移行	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，認証技術，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。認証技術では SAML や IEEE802.1X は定番となっています。PKI については，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 割近くと高いことから，知識習得後は過去問題演習が必須です。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。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，新しい攻撃や認証技術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，新しい攻撃やセキュリティ技術についての情報収集を行っておくと役立つでしょう。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。

また，セキュリティインシデント対応の事例が午後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設定，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でしょう。

最近出題が増えているのがアイデンティティ管理の問題です。IDaaSを用いたSAML認証やFIDO認証などは認証の仕組みを手順も含めて把握しておいてください。

セキュアプログラミングに関する問題は，午後Ⅰ試験では令和になって出題されていませんでしたが，今回は問題の一部として出題されていました。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対策でも必ず問題演習を行うことが重要です。実務経験が少ない場合は特に，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は非常に有効です。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ることも考えられます。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対策と同じですが，クラウドサービスの利用と絡めた認証連携の問題が連続 4 回も出題されていますので，改めて知識の確認をしておくとよいでしょう。追加で補うべき知識としては，セキュリティ管理知識が挙げられます。ISO や JIS のセキュリティ関連の規格は最近出題が増えているので，確認しておくとよいでしょう。そのほか，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も，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。