3　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。

こうした背景の下に，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，午前Ⅰ，午前Ⅱ，午後Ⅰ，午後Ⅱという四つの試験が行われてきましたが，IPA は，令和 4 年 12 月に支援士試験における出題構成等を変更し，令和 5 年度秋期試験から，従来の午後Ⅰと午後Ⅱを統合し，一つの午後試験として実施すると発表しています。

令和 4 年度春期（第 10 回）から令和 5 年度春期（第 12 回）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，第 1 回から第 3 回までは 16%から 17%程度で推移し，第 4 回から第 11 回までは 18.5%から 21.2%までの範囲に向上しました。今回の合格率は 19.7%で，20%を若干下回る結果になりました。そして，IPA の発表によりますと，令和 5 年 4 月 1 日現在，“登録セキスペ”の登録者数は 21,633 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
令和 4 年度春期	16,047（−1.9%）	11,117（69.3%）	2,131（19.2%）
令和 4 年度秋期	18,749（16.8%）	13,161（70.2%）	2,782（21.1%）
令和 5 年度春期	17,265（−7.9%）	12,146（70.4%）	2,394（19.7%）

（　）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

令和 4 年度春期から令和 5 年度春期までの 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
令和 4 年度春期	56.6%	87.4%
令和 4 年度秋期	52.6%	73.0%
令和 5 年度春期	52.5%	80.3%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

令和 5 年度春期の午前Ⅰ試験の合格率は，令和 4 年度秋期とほぼ等しいレベルでしたが，令和 4 年度春期に比べると 4 ポイント低下しました。令和 5 年度春期の合格率は，これまでの 12 回の試験において，ほぼ平均的といえますが，この数値からも分かるように，約半数の受験者が，午前Ⅱ試験の受験資格を失っています。このため，午前Ⅰ試験を受験する必要のある方は，テクノロジ系，マネジメント系，ストラテジ系の幅広い分野にわたる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（AP）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，80.3%でした。問題の難易度は，新規問題の出題数が，

令和 4 年度秋期より 1 問多くなったことから，令和 4 年度秋期の合格率と同等以下になると想定していましたが，結果は 7%高くなりました。しかし，最近の試験では，概ね 85%～90%で推移してきましたので，今回の合格率は，低い水準にとどまったといえます。午前Ⅱ試験は，過去問題を中心にしっかり学習していけば，比較的容易に合格できるレベルの内容ですから，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試験の対策としては，3 期前や 4 期前に行われた試験の問題（令和 5 年度秋期試験では令和 4 年度春期試験や令和 3 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午前Ⅱ試験を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。令和 4 年度春期から令和 5 年度春期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，AP 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	令和 4 年度春期	令和 4 年度秋期	令和 5 年度春期
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	2	2
	サービスマネジメント	3	3	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習得するとともに，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，論理演算などの問題は，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。令和 4 年度春期から令和 5 年度春期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	令和 4 年度春期	令和 4 年度秋期	令和 5 年度春期
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ほか，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) 午後試験

これまで，午後試験は，午後Ⅰ試験と午後Ⅱ試験の二つが実施されてきましたが，令和 5 年度秋期試験からは，午後Ⅰ試験と午後Ⅱ試験が統合されますので，一つの午後試験として実施されます。このため，試験時間は 150 分（従来は二つの試験を合わせて 210 分）に短縮されるとともに，出題数 4 問の中から 2 問を選択して解答するようになります。

午後試験では，これまで Web システムに関する問題がよく出題されてきました。例えば，午後Ⅰ試験で，3 問のうち 2 問がセキュアプログラミングを含む Web 関連の問題と，cookie を含む HTTP を中心にした Web 関連の問題が出題された場合には，選択の余地は全くありませんでしたが，令和 5 年度秋期試験以降は，4 問の中から 2 問を選択できるので，こうした制約を受けることは少なくなると思われます。そして，午後試験の問題選択に当たっては，個々の受験者が持ち合わせている技術知識などの差に依存しますので，できるだけ自分自身が得意とする分野の問題を選択していくとよいでしょう。

また，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も必要です。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，午後の試験問題に取り組むに当たっては，問題に記述された内容を的確に把握できるように，できるだけ技術や知識のレベルを向上させる必要があります。例えば，次のような分野については，十分に学習するようにしましょう。

① Web システムの仕組み，システムが抱える様々な脆弱性に関する知識

HTTP リクエストとレスポンスでやり取りされる情報，HTML，cookie とその属性，システムが抱える脆弱性の問題（XSS，CSRF，SSRF，SQL インジェクション，パストラバーサル，クリックジャッキング，OS コマンドインジェクション，HTTP ヘッダーインジェクション，メールヘッダーインジェクションなど），セッション管理における問題（セッション固定化攻撃，リプレイ攻撃などの対策），セキュアプログラミングなど

② クラウドサービスにおける認証連携の仕組み

SAML，OAuth，OpenID Connect，state，nonce，ID トークン，アクセストークン，シングルサインオン，SaaS，IDaaS，DaaS など

③ サイバー攻撃やマルウェア感染などのインシデント発生時における対応

様々な攻撃手法とその手順，マルウェアの感染手順，マルウェアの振る舞い，マルウェアの動作の特徴など

④ 認証技術と暗号化技術

利用者認証，多要素認証，パスワードレス認証方式，メッセージ認証，デジタル署名，公開鍵証明書の種類とその検証方法，共通鍵の暗号利用モード，ブロック暗号とストリーム暗号，鍵交換方式（DHE など），離散対数問題など

⑤ セキュリティプロトコルなど

TLS 1.2 と TLS 1.3 の違い，IPsec，SSH，VPN 技術，IDS，IPS，ファイアウォールの設定など

⑥ ネットワーク技術分野における知識

DNS の仕組み，電子メールの配送の仕組み，迷惑メール対策などの電子メールに関するセキュリティ対策（SMTP-AUTH，SPF，DKIM，DMARC など），プロキシサーバ

ここで例示した項目は，ほんの一例にすぎません。以上のほかにも，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，情

報セキュリティポリシーやリスク分析，JIS Q 27001，不正競争防止法などに関する知識も問われることがあります。

試験で出題される問題としては，Web 関連をはじめ，クラウド利用や認証連携，セキュリティインシデントをテーマとした問題が取り上げられることが多くなっています。例えば，クラウド利用というテーマによって問題が出題されたとしても，OAuth，OpenID Connect などを用いた認証連携の問題に特化したものは少なく，Web サイトのサーバ証明書を利用するようなケースでは，サーバ証明書の検証方法，サーバ証明書に記載されるコモンネームの役割，クライアント側にインストールする必要があるものなど，複数の分野からの知識が問われるような問題が出題されます。つまり，午後問題は，複合的な観点から出題されるという特徴があるので，前述のキーワードだけを学習すれば十分であるとはいえません。

このため，前述のキーワードなどを手掛かりにして，一つ一つの技術知識の理解を深めていけば，理解の幅が必ず広がっていきます。このようなサイクルを繰り返し進めていくことによって，さらに幅広い関連する知識を，しっかりと身に付けることができると思います。こうして，試験に必要な知識を十分に身に付けていけば，午後試験を突破できる力が養われていくと考えられます。いずれにしても，支援士試験で合格するには，それなりの努力が必要ですから，地道に努力を重ねていくことを忘れないようにしましょう。一度，理解した技術知識でも，繰り返し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ことも必要です。

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ようにしましょう。そのためには，繰り返しになりますが，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ほか，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　令和５年度春期試験のデータ

(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。今回の分野別出題数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した。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午前問題 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，今回もこれまでと同じ 4 問の出題でした。

新傾向といえる問題は次の 3 問でしたが，前回の 6 問と比べて少なくなっています。参考までに，午前Ⅰ試験問題の選択元になっている応用情報技術者試験（80 問）の新傾向問題は 16 問（前回 15 問）でほぼ同じでした。

・問 15　特定の IP セグメントからだけアクセス許可するセキュリティ技術
・問 17　サーバプロビジョニングツールを使用する目的
・問 24　システム要件定義プロセスにおけるトレーサビリティ

新傾向問題以外の内容としては，従来からよく出題されてきた定番といえる過去問題が 17 問程度あり，前回よりも多くて解答しやすかったといえます。

問題の出題形式は，文章の正誤問題が 19 問（前回 16 問），用語問題が 2 問（前回 5 問），計算問題が 2 問（前回 5 問），考察問題が 7 問（前回 4 問）で，文章・考察問題が増え，用語・計算問題が減っています。今回は問 3 のクイックソートのような少し難しい問題もありましたが，全体として定番問題が多く，従来よりもやや易しかったといえます。

高度試験の午前Ⅰは出題範囲が広いので，対策としては，基本情報技術者や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必要な基礎知識を維持し，新しい知識を吸収していくことが大切です。

出題内容を分野別に示します。「」は新傾向問題，下線を引いた問題は過去に出題された内容と同じ問題です。

・テクノロジ分野……論理演算，正規分布のグラフ，クイックソートの結果，CPU の平均 CPI，スケールイン，ハッシュ表探索時間，組合せ回路，コンピュータグラフィックス，UML の多重度，イーサネットフレームの宛先情報，ハンドオーバー，C&C サーバの役割，デジタルフォレンジックスの手順，サブミッションポート導入目的，「特定セグメントのアクセス許可」，モジュール結合度，「サーバプロビジョニングツール」

・マネジメント分野……プロジェクト憲章，作業完了日数，JIS Q 20000-1 におけるレビュー実施時期，予備調査，監査手続で利用する技法
・ストラテジ分野……ROI，「トレーサビリティ」，RFI，バランススコアカードの戦略マップ，エネルギーハーベスティング，アグリゲーションサービス，経費に算入する費用，派遣元事業主の講ずべき措置

出題される内容の多くは，過去の基本情報技術者試験や応用情報技術者試験で出題された基本的な問題です。高度試験で専門分野の力を発揮するのは午前Ⅱ試験からですが，試験対策として過去の応用情報技術者試験の午前問題を，余裕をもって 7 割以上正解できるよう確実に実力を付けてください。

試験の統計情報を分析すると，高度情報処理技術者試験を午前Ⅰ試験から受けた人で 60 点以上取った人は 5 割から 6 割台で推移していて，半数近くの方が次の午前Ⅱ以降の採点に進んでいない状況です。出題元の応用情報技術者の午前試験問題は細かい内容が問われ難しいことが多いので，苦手な分野の学習は基本情報の問題から復習を始めるとよいといえます。

また，出題範囲が広いため，全体をまんべんなく学習するのはかなり時間がかかります。そのため，試験対策としては，これまで出題された出題内容のポイント事項を重点的に解説した「2023　高度午前Ⅰ・応用情報　午前試験対策書」で確実に学習することをお勧めします。

(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 1 回の平成 29 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，25 問のうち，新規問題の出題数は令和 4 年度秋期試験の 8 問と同じでした。

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，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。これからも分野別の出題数は，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 問という割合には変化がないと考えられます。

セキュリティ分野の 17 問は，基本的に情報セキュリティ技術に関する問題です。新規問題は，問 7(暗号利用モードの CTR モードに関する記述)，問 8(“ISMAP 管理基準”が基礎としているもの)，問 9（サイバーセキュリティフレームにおける“フレームコア”を構成する機能)，問 12（インラインモードで動作するシグネチャ型 IPS の特徴)，問 13（電源を切る前に全ての証拠保全を行う際に最も優先して保全すべきもの）の 5 問です。これに対し，過去問題からの出題は，令和 3 年度秋期から 3 問，令和 3 年度春期から 2 問，令和元年度秋期から 2 問，平成 31 年度春期から 1 問，平成 29 年度秋期から 2 問，平成 28 年度秋期から 1 問のほか，令和元年度秋期 SG 試験から 1 問の計 12 問でした。3 期前に当たる令和 3 年度秋期の過去問題からの出題数が 3 問と最も多くなりましたが，今回も，複数の期にわたって，1 問ないしは 2 問のように分散して出題されていたことなどが特徴といえます。

ネットワーク分野の 3 問は，新規問題が 2 問で，過去問題は 1 問でした。新規問題は，問 19（スパニングツリープロトコルにおけるポートの種類)，問 20（2 種類のブロードキャストアドレスに関する記述）ですが，いずれもネットワークの専門知識が必要ですから，内容的にはレベル 4 の問題に位置づけられます。過去問題は，問 18（ピーク時に同時使用可能なクライアント数）は，平成 29 年度秋期 SC 試験で出題されていました。

データベース分野の問 21（GRANT 文の意味）は，平成 29 年度春期 SC 試験で出題されており，レベル 3 の問題といえます。

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 分野です。システム開発技術分野の問 22（IoT 機器のペネトレーションテストの説明）は新規問題ですが，ペネトレーションテストはセキュリティの基本的な用語ですから，容易に正解できるでしょう。ソフトウェア開発管理技術分野の問 23（プログラムの著作権管理上の不適切な行為）は平成 24 年度秋期 AP 試験で出題されたものですが，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（サービスマネジメントにおける問題管理において実施す

る活動）は平成 31 年度春期 AP 試験で，問 25（監査計画の策定で考慮すべき事項）は令和元年度秋期 SM 試験で出題されていましたが，どちらもレベル 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。今回は，Java に関するセキュアプログラミング問題が，令和 4 年度春期の午後Ⅰ試験に引き続き出題されましたが，その他の 2 問は，Web 関連のセキュリティ問題ではなかったことから，令和 4 年度秋期試験と同様に，比較的バランスの取れた出題構成であったといえます。

このため，情報セキュリティ全般に関する知識を十分に身に付けた上で，問題文に記述された内容をよく読んで，本文や図，表に記述された条件などを丁寧に整理し，設問で問われていることを的確に把握したうえで解答を作成していけば，合格基準点の 60 点をクリアすることは，それほど難しくないと思われます。一方，各問とも解答する小問数については，前回試験と同様に，少な目でしたから，些細なミスで得点を失わないようにすることも必要です。

問 1　Web アプリケーションプログラム開発

本問は，Web アプリケーションプログラム開発というテーマのとおり，Java を利用したセキュアプログラミングに特化したもので，Java のコードを読めることが前提条件になります。設問 1 は，ソースコードの静的解析に基づき，“ディレクトリトラバーサル”が発生する箇所や，確保した“リソースの解放漏れ”を引き起こす変数名のほか，それらの修正コードを答えるものです。設問 2 は，注文情報照会機能において不都合が発生した原因となった変数と宣言方法に加え，修正後のソースコードを答えたり，並列動作する複数の処理が同一のリソースに同時にアクセスしたときに想定外の処理結果となる事象の名称を答えたりするものです。Java の知識がある受験者にとっては，難度は高くないでしょう。

問 2　セキュリティインシデント

本問のテーマは，セキュリティインシデントですが，内容的には，ネットワークや Linux に関する知識が要求されます。設問 1 は，FTP のファイル転送モードを答えるものです。設問 2 では，SNMP の用語，ファイアウォールのログや ps コマンドの実行結果などに基づいて攻撃者が C&C サーバとの接続に失敗した

場合と成功した場合の理由を答えるものです。設問3は，DNSのTXTレコードを用いると，リソースデータの内容をそのままコマンドとして実行できる理由を答えるものや，ダウンロードしたファイルを解析対象にするのは適切ではない理由などを答えるものです。ネットワークに関する知識があれば，正解しやすい設問が多いと思われます。

問3　クラウドサービス利用

本問のテーマは，クラウドサービス利用ですが，SAMLを利用したSPとIdPとの間における認証連携と，それに基づいてネットワーク構成の見直しに関するものが出題されています。設問1では，認証連携の関係と，クラウドサービスが提供する接続元制限機能の役割が問われています。設問2では，TLSで使用するデジタル証明書の関係と，クラウドサービスの可視化機能の用語問題が出題されています。設問3は，ネットワークの見直し前と見直し後のアクセス方法の違いや，クラウドサービスに接続するために必要になる追加設定，SaaS に対するアクセスを制限する際に必要になる条件などを答えるものです。問われていることは，基本的な事項が中心なので，正解を導きやすいと考えられます。

(4)　午後Ⅱの問題

午後Ⅱ試験は，問1がWebセキュリティ，問2がWebサイトのクラウドサービスへの移行と機能拡張というテーマで，問題が出題されています。問1は，Webサイトのセキュリティ全般に関する知識が要求されますが，問2は，クラウドサービスの提供形態をはじめとして，機能拡張に伴って発生するセキュリティ問題などを考察するものです。

今回の試験では，問1が記述式中心の問題構成，問2は随所に穴埋め問題が設定され，解答しやすい形式になっていましたが，全体的に小問数が少ないので，解答できそうな設問に対しては，着実に得点を積み上げていくことが求められます。また，両方の問題とも，問題の記述内容を十分に確認し，何がセキュリティ上の問題になっているのか，それはどのような理由によるものか，その問題を解決するには，どのようにすればよいかなどを，本文や図表類から条件を見つけ出し，論理的に考察していくことがポイントになると思われます。問1，問2とも，問題文をよく読んで，条件などを十分に整理した上で解答を考察していけば，合格基準点をクリアすることは，それほど難しくはないと思われます。

問１　Web セキュリティ

本問は，Web セキュリティというテーマどおり，Web サイトの脆弱性を診断するケースを想定した問題が出題されています。設問 1 は，Web サイトの全ての URL を診断対象とする場合，診断対象 URL を手動登録機能によって調べる方法を答えるものです。設問 2 では，担当者とツールによって診断を行い，両者を比較した結果に基づいて，SQL インジェクション脆弱性における，入力パラメータによる検索件数の違いや，SQL インジェクションを検出できるようにするための初期値の設定方法を答えるものや，XSS の検出を行うための設定内容を答えるものなどが出題されています。設問 3 は，診断手順案に従った診断の結果，URL が登録されていなかった画面名や，該当する画面遷移がエラーになってしまう理由を答えるものです。設問 4 は，XSS の対策として HttpOnly 属性が有効である理由，XSS を悪用して cookie 以外の情報を盗む手口を答えるものです。設問 5 では，アクセス制限の回避に関するものが出題されています。設問 6 は，それまでの診断で残された二つの課題に対する対策を答えるものです。Web 関連のセキュリティ問題を十分に把握していれば，設問で問われていることを的確に押さえることによって，かなりの設問に答えることができると考えられます。

問２　Web サイトのクラウドサービスへの移行と機能拡張

本問は，Web サイトのクラウドサービスへの移行と機能拡張というテーマですが，字句選択などの穴埋め問題が比較的多いので，取り組みやすいと思われます。設問 1 は，クラウドサービスの構成要素を○，×で答えるものです。設問 2 は，クラウドサービスにおける権限設計と，イベントの検知ルールを答えるものです。設問 3 は，OAuth 2.0 を利用した認証連携の穴埋め問題と，TLS 1.2 と TLS 1.3 の暗号スイートの選択問題です。設問 4 では，アクセストークンの取得に成功することが困難である理由，認可サーバがチャレンジコードと検証コードの関係を検証する方法が問われています。設問 5 は，第三者が X トークンを取得するための操作，権限管理の変更内容などを答えるものです。基本的な知識を十分に習得していれば，取り組みやすい問題といえますが，記述式の設問に幾つ正解できるかが，合格基準点をクリアできるかどうかのポイントになると考えられます。