令和5年度　春期試験
情報処理安全確保支援士（SC）
出題傾向分析

TAC株式会社

SC　総評

・　問題テーマの特徴

　インシデント対応，Webサイトのセキュリティ対策，クラウドサービスを題材のネットワークセキュリティなど定番テーマ

　午後Ⅰでセキュアプログラミングが出題(令和で2回目)

　認証連携の出題も継続

・　試験全体の難易度⇒やや高め

　午前Ⅱ　　標準

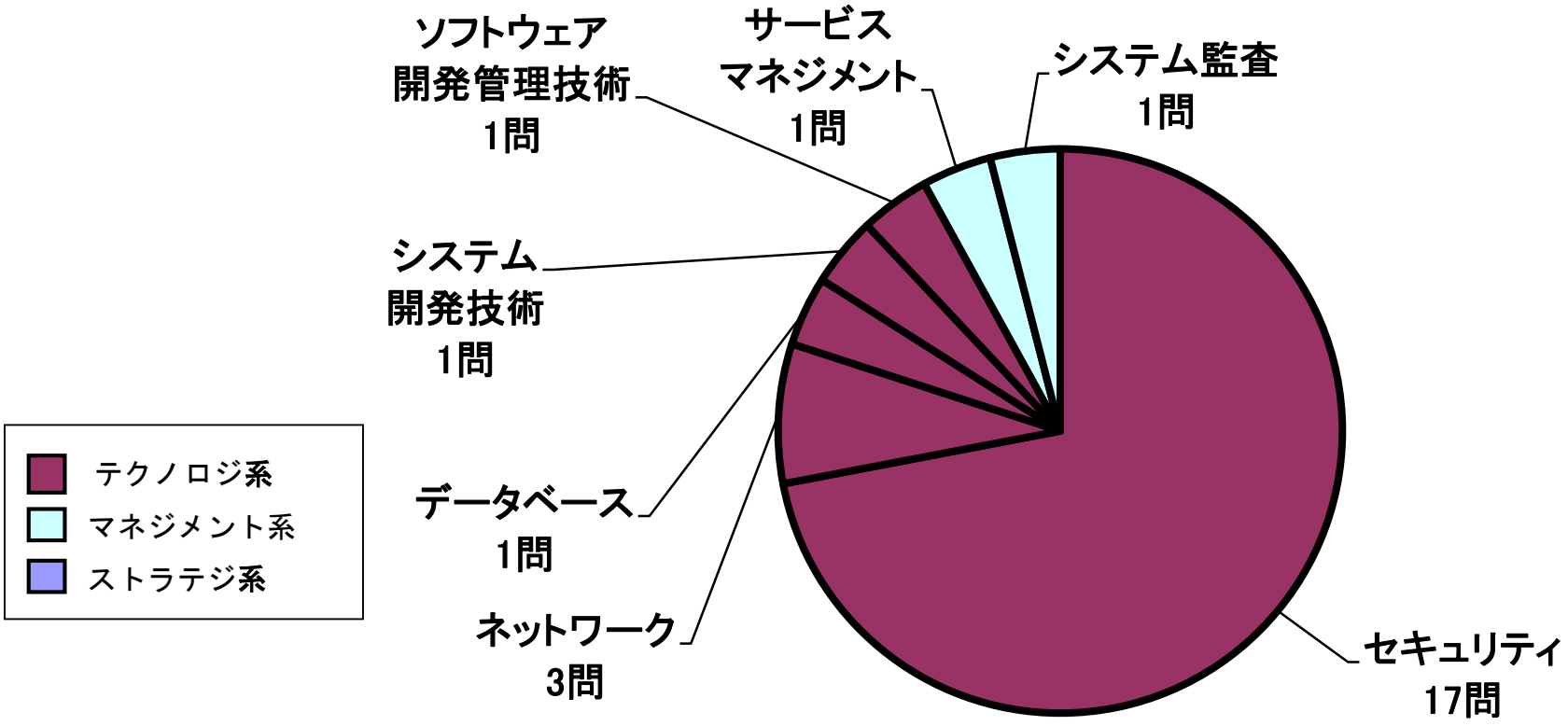
　午後Ⅰ　　問1：やや難，問2：やや難，問3：標準

　午後Ⅱ　　問1：難，問2：難

　午後問題：特定の技術的知識・具体的な技術的知識や対応が求められる設問の割合が例年よりも多く感じられる

SC　午前Ⅱ　分野別出題数

- 分野別出題比率は変化なし
- 重点分野：セキュリティ＋ネットワーク　8割



SC　午前Ⅱ　特徴と難易度

- 多少の増減はあるものの大きな変化はみられない

小分類	R5春	R4秋	R4春	R3秋	R3春
情報セキュリティ	6問	8問	6問	9問	6問
情報セキュリティ管理	2問	0問	4問	1問	1問
セキュリティ技術評価	0問	1問	0問	1問	1問
情報セキュリティ対策	4問	2問	2問	2問	4問
セキュリティ実装技術	5問	6問	5問	4問	5問

- セキュリティ・ネットワーク分野の新規問題
  - ブロック暗号のCTRモード，ISMAP管理基準，サイバーセキュリティフレームワークのフレームワークコア，シグネチャ型IPS
  - 代表ポート，ディレクティッドブロードキャストとリミテッドブロードキャスト
- 過去問流用はセキュリティ分野17問中11問
- 過去問対策：特定の回への偏りがない⇒広範囲の学習が必要
- 午前Ⅱ全体の難易度　⇒ 標準

SC　午後Ⅰ　全体の特徴と難易度

- 定番のセキュリティインシデント対応，クラウドサービス題材，セキュアプログラミング
  午後Ⅰでのセキュアプログラミングは，令和4年春に続く出題

- 求められた特定の専門知識
  - PreparedStatement，レースコンディション
  - FTPの接続モード，DNSトンネリング，ウェルノウンポート
  - psコマンド，netstatコマンド

- 解答群の提示された選択問題が全体で3つという少なさ
- 問題ごとのボリュームは標準的だが図表が多い
- 午後Ⅰ試験の難易度：標準～やや高め

SC　午後Ⅰ　特徴と難易度　　問1

問1　「Webアプリケーションプログラム開発」

- Webアプリケーションのセキュリティとセキュアプログラミングの問題
  - SQLインジェクション対策
    ディレクトリトラバーサル対策
  - PreparedStatement：令和4春に出題
  - レースコンディション：H22春，H25春に出題されて以来
- 解答群から選択する設問が一つもない

　　⇒　難易度：　やや高め

SC　午後Ⅰ　特徴と難易度　　問2

問2 「セキュリティインシデント」
DMZ上のサーバへの不正アクセスを題材

- セキュリティインシデント対応の問題
  - FTPの接続モード
  - DNSトンネリング

- 特定の知識が求められる
  - TCPのウェルノウンポート，FTPのパッシブモード
  - psコマンド，netstatコマンド

- 解答群から選択する設問が一つもない
  ⇒　難易度 ： やや高め

SC　午後Ⅰ　特徴と難易度　　問3

問3 「クラウドサービス利用」

　複数のクラウドサービス利用時の認証連携や在宅勤務のリモート接続におけるクラウドサービスの活用を題材

- クラウドサービスの機能設定
  　問題文中の条件を正しく把握すれば解答が導ける
- 多要素認証機能の選択
  　要件の意図を読み誤ると選択を誤りかねない

⇒　難易度　：　標準

SC　午後Ⅱ　全体の特徴と難易度

- どちらの問題も技術面・管理面が出題された総合問題
  - 問1は，Webサイトセキュリティの総合問題
  - 問2は，クラウドサービス活用に関する総合問題
- 求められた技術的知識
  - XSSやSQLインジェクション：高度な知識が必要な設問はない
  - OAuth2.0：データのパラメータからフロー図の部分かを答える，PKCE利用の攻撃対策(再出題)　⇒高い技術的知識
- クラウドサービスの認証連携の出題頻度が高い
  - 午後Ⅱでは　R5春，R4春，R3秋，R3春，R2秋，H30秋
- 問題文の分量：11，12ページ　　図表：9点と13点
- 問1の解答分量が多い　制限字数を加算すると430字
- 2問とも難易度が高い

SC　午後Ⅱ　特徴と難易度　問1

問1　「Webセキュリティ」

- 脆弱性の診断・対策に関するWebサイトセキュリティの総合問題
  - Webサイトの脆弱性診断ツールの設定
  - 代表的な脆弱性の内容
  - 診断業務における組織的管理策
- 診断用データの設問　　最近出題が増加
  - SQLインジェクションにおける検出パターンの違いによるレスポンスの差異に着目した出題
- 図表が9点で，問題文と設問文で11ページ
- 技術的知識や管理策の知識は基本的レベル，問題文を正しく読み解けば解答ポイントを見つけられる
- 解答ボリュームが多い⇒解答表現力，時間的難易度が高い

SC　午後Ⅱ　特徴と難易度　問2

問2 「Webサイトのクラウドサービスへの移行と機能拡張」

- クラウドサービスの選定・移行・運用を題材に，リポジトリサービスを活用して開発されるモジュール開発時のセキュリティまで含む総合問題
  - 複数のクラウドサービスの仕様を正しく読み解く
    誤まりやすい設問も（付与権限の設定）
    OAuth2.0　PKCEを利用した認可コード横取り攻撃への対策
    令和4年春よりもより具体的な内容で出題
    OSSリポジトリサービス活用で開発するモジュール
    アクセス権限管理に関する設問が主体
- 問題文と設問文で12ページ，図表が13点とかなり多い
- 技術的難易度が高い

今後の対策（1）　午前Ⅱ対策

- セキュリティ分野とネットワーク分野で8割
  - 2分野に絞った学習を
  - 午後試験でも問われる知識なので確実に
- テキストを用いた体系的な知識習得が必須
  - 知識の関連性を把握できて学習効果が高い
  - 攻撃手法とその対策，暗号化・認証技術など
  - ネットワークの主要プロトコルについても確認
- 問題演習で問われやすい攻撃・技術・プロトコルを確認
  - 特定の回に偏った出題がなくなった
  - 3回前～12回前の演習を繰り返す
- IPAのシラバス追補版(午前Ⅱ) v3.2についても目を通す

今後の対策(2)　午後対策

- 令和5年秋試験から午後試験が一本化
- 問題数　4問から2問を選択して解答
- 試験時間　150分

- 目的:　問題選択の幅と時間配分の自由度を拡大する
  - 試験で問われる知識や技能の範囲は変わらない

  ⇒　午後試験の対策はこれまでと同様の対策でよい

  過去問演習は午後Ⅰ問題からはじめ，午後Ⅱ問題も

  ※管理面の問題は午後Ⅱ問題にしかない

今後の対策(3)　午後対策

- 主要な攻撃手法・セキュリティ技術は詳細まで理解
  - 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・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
  - ISOやJISのセキュリティ関連の規格，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
- インシデント対応の一連の流れを確認
  - 初動対応，ログ分析，感染範囲や経路の特定，出口対策
- 認証連携技術，クラウドサービスのセキュリティ
- セキュアプログラミング　増加傾向
- 過去問題演習は必須　⇒　知識の適用力を習得