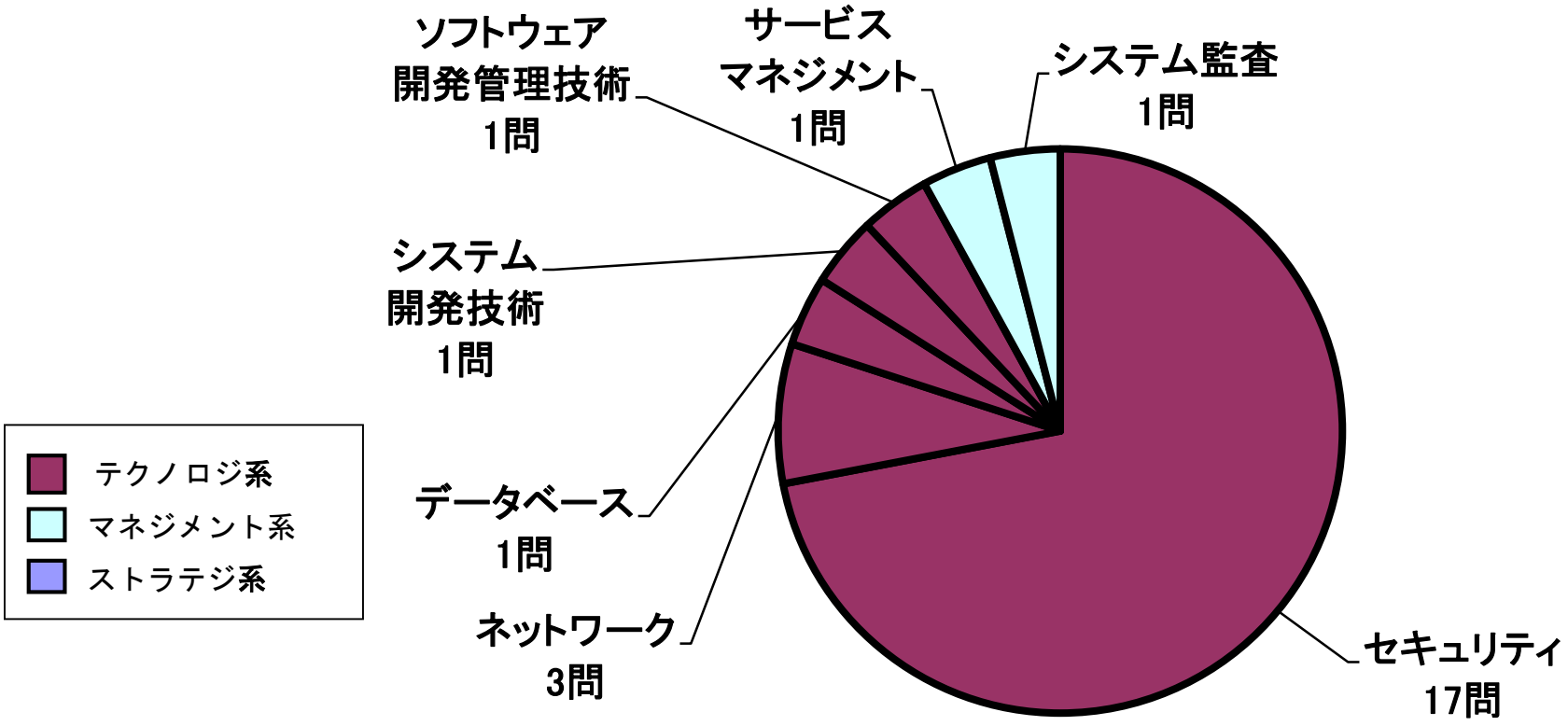
令和4年度　秋期試験
情報処理安全確保支援士（SC）
出題傾向分析

TAC株式会社

SC　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

- セキュリティ分野：ほぼすべて技術寄り

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

- セキュリティ分野の新規問題：5問　⇒　2問増
  - メッセージ認証符号，パスワードスプレー攻撃，シングルサインオン，ISO/IEC 15408，クリックジャッキング攻撃対策
  - 初出題の用語は1問のみ　⇒　2問減
- 過去問題の流用率：約7割　例年どおり
- 他の試験区分の過去問題が増加　平均3問　⇒　今回8問
  - SCでも既出のテーマの問題やレベル3以下の問題で，対応可能
- 午前Ⅱ全体の難易度：やや易しい

SC　午後Ⅰ　全体の特徴と難易度

- 定番テーマからの出題で，取り組みやすい
  - セキュリティインシデント対応　2問
  - Webアプリケーションの脆弱性　1問
- 詳細なセキュリティ技術知識は要求されない
- セキュリティとネットワークの基本的な知識をもとに，応用力，思考力が求められる
- 図表点数が多く，必要な情報を図表から読み取るためには慣れが必要　⇒　問題演習の効果発揮
- 問題文の分量：3問とも6ページで平均的
- 午後Ⅰ全体の難易度：標準的

SC　午後Ⅰ　特徴と難易度　　問1

問1 「 IoT製品の開発」

- IoT製品の開発において各機能のセキュリティ対策や脆弱性について検討する事例
- 脆弱性を悪用した3つの攻撃の知識が必要
  - DNSキャッシュポイズニング
  - OSコマンドインジェクション
  - クロスサイトリクエストフォージェリ

  } 頻出
- 知識解答型の設問が多い　⇒　教科書的な知識で対応可能
- 攻撃の仕組みを長文で解答　⇒　難易度が多少アップ
- 難易度：やや易しい

SC 午後Ⅰ 特徴と難易度 問2

問2 「脆弱性に起因するセキュリティインシデントへの対応」

- 問題が発生したサーバの調査→その他のサーバの調査→再発防止策の検討という流れの事例
- 図表から必要な情報を得て，思考しながら解答を導く
  - ・プロセス一覧，コネクション一覧⇒通信先の特定，調査すべきソフトウェアの判定
  - ・脆弱性の概要，ログ⇒攻撃の流れの把握
- 特定の高度なセキュリティ知識は必要なく、思考力重視
- 正確に情報を読み取るための基礎知識と慣れが重要
  ⇒業務経験がない場合は問題演習が効果を発揮
- 難易度：標準的

SC 午後Ⅰ 特徴と難易度 問3

問3 「オンラインゲーム事業者でのセキュリティインシデント対応」

- ゲームアプリ更新時のゼロデイ攻撃の事例
  被害の調査→再発防止策の検討という流れ
- 図表から必要な情報を得て，思考しながら解答を導く
  - サーバの概要，コンテナ一覧⇒原因の特定
  - アクセスログ⇒攻撃者が判断に用いた情報の把握
  - サーバの概要，更新手順，アクセスログ⇒被害拡大防止の対処の把握
- REST API，コンテナエスケープ：初登場，設問には影響ない
- 特定の高度なセキュリティ知識は必要なく，思考力重視
- 難易度：標準的

SC　午後Ⅱ　全体の特徴と難易度

- 特異なテーマはなく、取り組みやすい
- セキュリティの技術面と管理面の両面から問う総合問題
- 要求される知識レベルは高くない
- セキュリティ技術，セキュリティ管理，ネットワークの幅広い知識の応用力，思考力が必要
- 多くの図表も含めて事例内容を正確に読み取る読解力が必要
- 問題文の分量：13ページ　平均より多め，2問で差はない
- 午後Ⅱ全体の難易度：標準的

SC　午後Ⅱ　特徴と難易度　問1

問1　「脅威情報調査」

- 脅威情報を調査する部門における模擬攻撃試験の事例
- 技術面：マルウェアに感染した検体の調査，攻撃と対策
  管理面：運用に関する改善提案
- 必要とされるセキュリティ技術知識
  - ARPスプーフィング（H29春）
    - ARPの仕組み，中間者攻撃
  - パスワード攻撃と対策
    - ソルト（H27春），ストレッチング（初）
- 幅広いセキュリティとネットワークの知識と応用力が必要
- 知識レベル，時間的なレベルともに標準的
- 難易度：標準的

SC　午後Ⅱ　特徴と難易度　問2

問2 「インシデントレスポンスチーム」

- マルウェア検知のインシデント対応とその運用体制の事例
- 技術面：マルウェアの解析，再発防止策の検討
  管理面：インシデントの重大さを考慮した運用体制，
  　　検知ルールの作成
- 事例内容を的確に把握する読解力と管理面の思考力が必要
  - 体制見直しのタイミング，EDRの検知ルール
- 特定の攻撃に関する知識は必要ない
- 管理面での出題は解答表現に時間がかかりやすい
- 難易度：標準的

今後の対策　午前Ⅱ

【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
  - 午後問題の読解にも必要な知識なので確実に習得
- テキストを用いた体系的な知識習得を行う
  - 用語を覚えるのではなく，仕組みを理解する
  - 知識項目間の関連性を把握する
  - 攻撃手法とその対策，暗号・認証技術，PKIなどは頻出
- 過去問題演習で理解度・弱点を確認する
  - 少なくとも直近の3年分(6回分)は演習を繰り返す
  - 誤答の選択肢についても確認し，知識の幅を広げる
- IPAのシラバス追補版(午前Ⅱ)についても目を通す
- 日頃から新しい攻撃やセキュリティ技術の情報収集を行う

今後の対策　午後Ⅰ

【午後Ⅰ対策】

- 主要な攻撃手法やセキュリティ技術は詳細まで理解
  - Webアプリケーション，DNS，メールのセキュリティ
  - マルウェアの特徴と対策
  - PKIに関する知識（証明書，認証局の役割）
  - アイデンティティ連携，認証技術
  - セキュアプロトコル(TLS，SSH ，IPsec)
  - 攻撃に利用されるプロトコル（ARP，HTTP，DNS，LDAP）
- 過去問題演習は必須
  - 問題演習を通して実務に近いさまざまな事例に接する
  - 問題文の読解，解答表現の適切性の確認
  - 定番論点の把握
  - 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，感染範囲の特定，一時対策，再発防止策

今後の対策　午後Ⅱ

【午後Ⅱ対策】

- 基本は午後Ⅰ対策と同じ
- 事例が長く複雑化，幅広い知識が必要
  - ⇒ まずは午後Ⅰ対策を重点的に
    学習不足の項目を把握して補強後，午後Ⅱ対策へ
  - ⇒ 攻撃手法や対策を体系的に整理
- 管理面の知識も確認
  - ・セキュリティ関連の基準や法規，評価指標を確認
  - ・運用管理面の対策
  - ⇒ 経験がなければ過去問題演習で習得
- 複雑な長文問題に慣れるための午後Ⅱの過去問題演習
  - ⇒ 問題文を分割して隅々まで丁寧に読み込む
  - ⇒ 試験時間を意識して取り組む