令和3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

認証サービスとの認証連携の出題が目立った

クラウドセキュリティの出題が連続した

セキュアプログラミングに関する出題が一切無かった

・ 試験全体の難易度⇒標準

午前Ⅱ　　標準

午後Ⅰ　　問1：標準，問2：易しい，問3：難しい

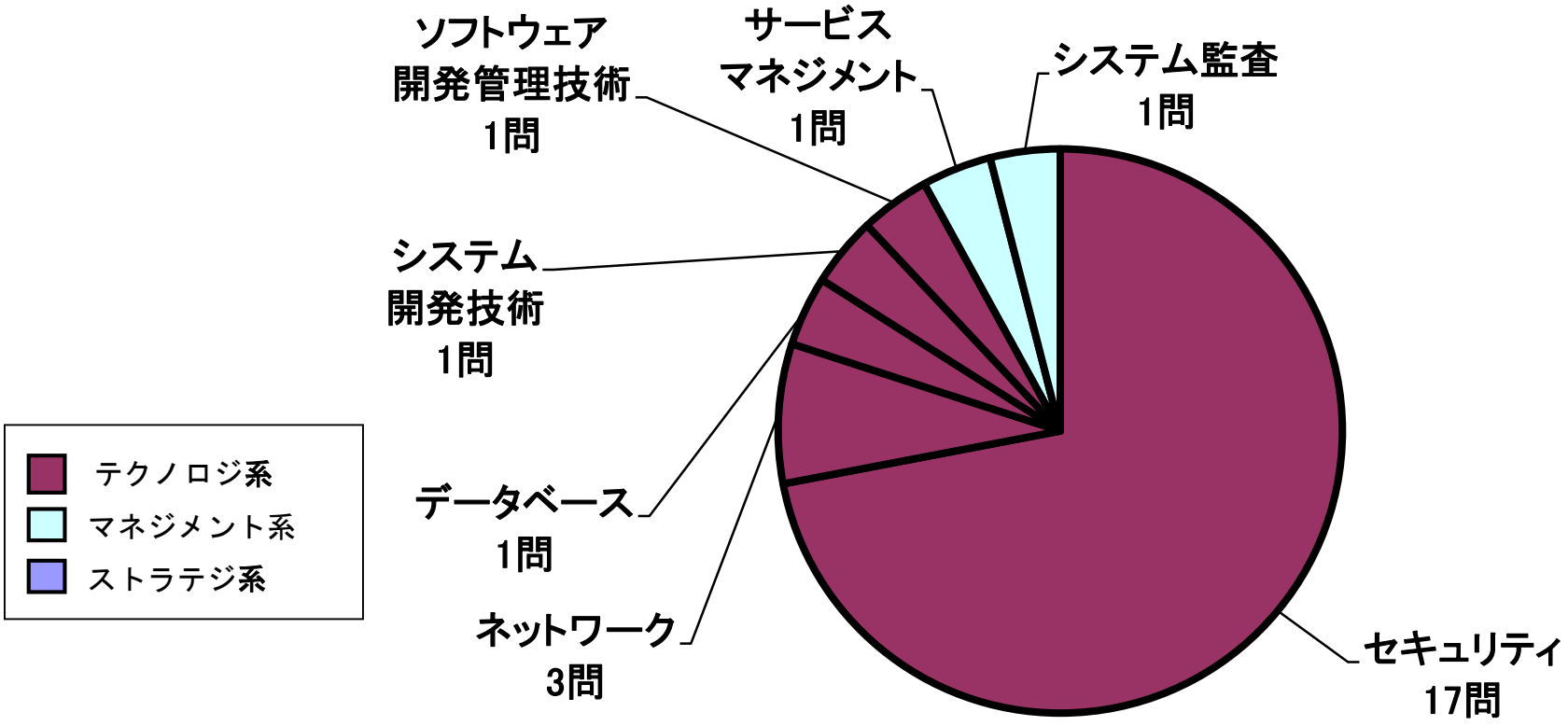
午後Ⅱ　　問1：標準，問2：難しい

午後問題の難易度が問題によって異なる

⇒選んだ問題によって差

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

- 情報セキュリティ,情報セキュリティ対策,セキュリティ実装技術⇒均等

小分類	R3春	R2	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・ネットワーク分野の新テーマは5問
  - 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，DNS CAAレコード，Enhanced Open
  - 欧州電気通信標準化機構の提唱するNFV，ループバックアドレス
- 過去問流用はセキュリティ分野で11問　7問がH31年春から
- セキュリティ分野はやや易しめ，ネットワーク分野は難しい
- 午前Ⅱ全体の難易度　⇒ 標準

SC　午後Ⅰ　全体の特徴と難易度

- 定番の出題がない(前回同様)
  セキュリティインシデント対応，セキュアプログラミング
  ⇒ OAuthを用いた認証連携，
  　DNSセキュリティ，
  　マルウェア対策や脆弱性対策

- 午後問題で初めて出題された技術的知識
  - OAuth，EDR，Wake on LAN

  基礎的な知識から新しい技術的知識までが幅広く出題

- 問題ごとに難易度が異なる　⇒ 難易度：標準

SC 午後Ⅰ 特徴と難易度 問1

問1 「認証システムの開発」 ⇒ 認証技術

- OAuthによる認証及び認可を提供するSNSとの認証連携
- OAuthを用いた認可のシーケンス図の理解が必須
- 攻撃のシーケンス図に示された中間者攻撃の理解
- 知識が問われるのではなく，図や問題文の内容の理解が問われる
- OAuthについての知識があれば有利 しかし，シーケンス図を理解することで解答可能

難易度： 標準

SC　午後Ⅰ　特徴と難易度　　問2

問2 「ネットワークのセキュリティ対策」
DNSセキュリティを主題にした問題

- DNSサーバに対する代表的な攻撃手法や対策
  - 権威DNSサーバ，フルサービスリゾルバ，スタブリゾルバ
  - 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サーバのゾーン転送要求に対する設定
  - DNSサーバの変更に対応するためのFWの設定変更

- 頻出事項も多く，基本的な知識と問題文を正しく読み取ることで対応可能　⇒　難易度：易しい

SC　午後Ⅰ　特徴と難易度　　問3

問3 「セキュリティ運用」　　新規性が高い

EDRを絡めたマルウェア対策・パッチマネジメント

- 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，Wake on LANの起動パケットの知識
- 3問中で一番専門知識が求められた問題
  - 起動パケットの内容
  - ブロードキャストを他のLANに送信するため：L3SWの設定

難易度　：　難しい

SC　午後Ⅱ　全体の特徴と難易度

- 標準的な総合問題
  - 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る
- 問われた内容
  - 定番の情報セキュリティインシデント対応，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
  - NIST文書のインシデント対応のライフサイクル，クラウドサービス事業者の第三者認証の規格や制度
- 2問の難易度が異なるため，選択によって差
  ⇒ 難易度：標準的

SC 午後Ⅱ 特徴と難易度 問1

問1 「インシデント対応体制の整備」

パスワードリスト攻撃，SSHによる不正アクセスなどを題材としたインシデント対応や体制整備の問題

- 多彩な知識や応用が問われる
  - パスワードリスト攻撃の説明，パスワードの設定方法
  - 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
  - プレフィックス表記の理解，計算問題
  - 日本標準時が協定世界時に対し進んでいる時間
- 図表が合わせて13点 ⇒ 図の注記まで読む必要あり
  - 問題文と設問文で12ページと長い
- 解答字数の制限には余裕があった
- 単純な知識問題もあったが，読解力や思考力も必要

⇒ 難易度：標準

SC　午後Ⅱ　特徴と難易度　問2

問2 「クラウドセキュリティ」

ネットワークセキュリティを中心に幅広い知識が問われる

- 出題内容
  - SAMLによる認証連携，無線LANセキュリティ
  - DHCPサーバの割り当て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
- クラウドサービスの認証連携の出題頻度が高まっている
  - R2秋午後Ⅱ，H30秋午後Ⅱ，H29春午後Ⅰ
- 絞り込みに迷う解答を“一つ答えよ”という設問が多かった
- 設問で求められた知識レベルが高い

⇒　難易度：難しい

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
  - 少なくとも過去5回分は演習を繰り返す
  - 特に3回前からの出題率が高い
- IPAのシラバス追補版(午前Ⅱ) v3.1についても目を通す

今後の対策(2)　午後Ⅰ対策

- 主要な攻撃手法・セキュリティ技術は詳細まで理解
  - マルウェアの種類・攻撃手法，対策
  - ディジタル証明書や認証局の役割などのPKIに関する知識
  - FWのルール設定，セキュアプロトコル(TLS，IPsec)
  - ネットワークの主要なプロトコル(ARP，HTTP，DNSなど)
- 認証連携技術，クラウドサービスのセキュリティ
  - SSOのケルベロス認証，SAML，アクセス認可に利用されるOAuth
- 新しい技術や攻撃の動向を確認(IPAのサイトなど)
- 過去問題演習は必須
  - 知識の応用の仕方や知識レベルの確認
  - 問題文の読解、解答表現の適切性の確認
  - 定番論点の把握

今後の対策(3)　午後Ⅱ対策

- 基本は午後Ⅰ対策と同様
- 事例が長く複雑化，幅広い知識が必要
  - ⇒　まずは午後Ⅰ対策を重点的に行う
    学習不足の項目を把握して補強後，午後Ⅱ対策へ
  - ⇒　出題された攻撃手法や対策を体系的に整理
  - 複雑な長文問題
    - ⇒　問題文を分割して読解する練習
    - ⇒　隅々まで丁寧に読み込むように注意
- 管理面の知識・セオリーも重要
  - 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セオリーを習得