令和4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

Copyright © 2022 TAC CO., LTD.

SC　総評

- 問題テーマの特徴

  定番のテーマが出題されるが，新しい視点の出題も

  　法令に基づく身元確認方法，CDN活用時のセキュリティなど

  クラウドセキュリティの認証連携も連続出題

  午後Ⅰでセキュアプログラミングが出題(令和で初)

- 試験全体の難易度⇒やや高め

  午前Ⅱ　　標準

  午後Ⅰ　　問1：標準，問2：やや難，問3：標準

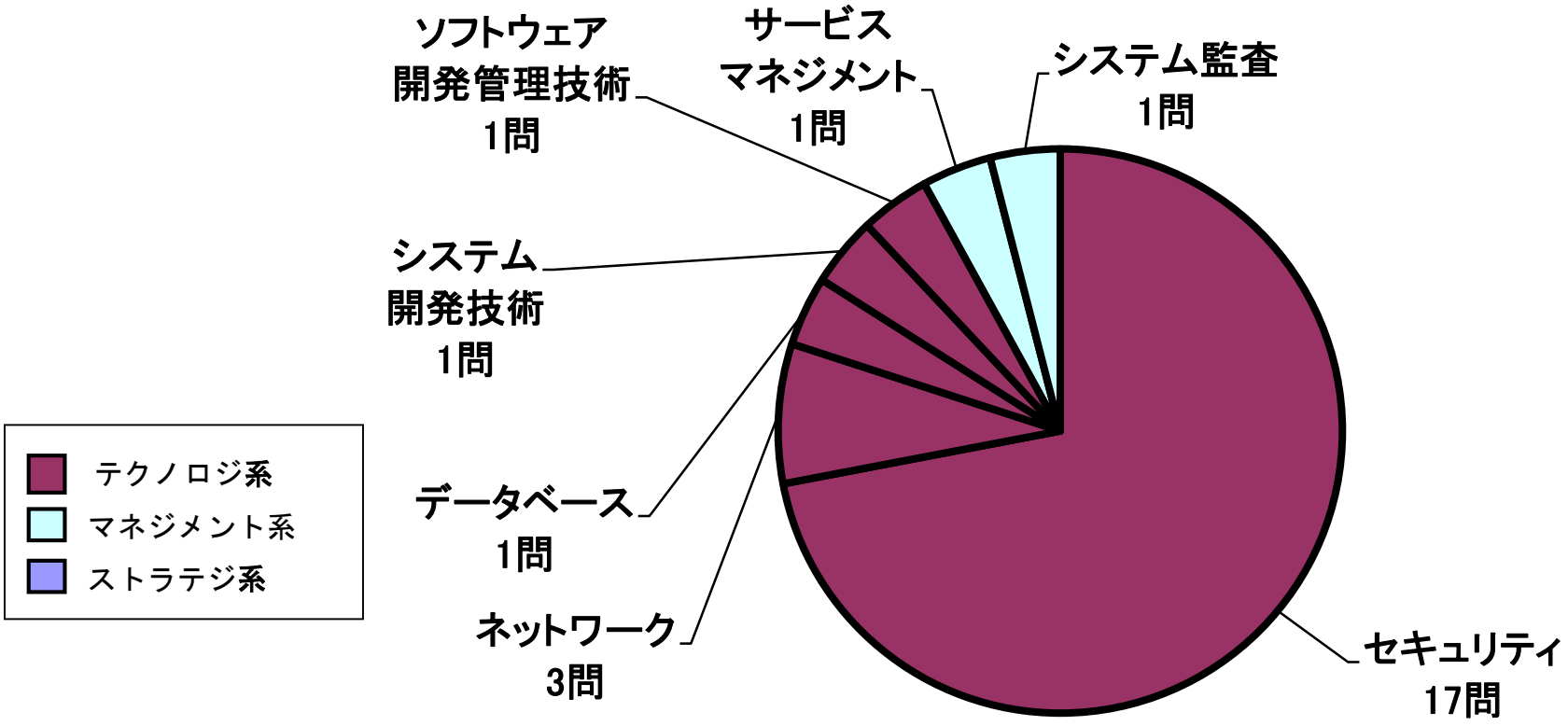
  午後Ⅱ　　問1：標準，問2：難

  午後問題：特定の技術的知識が求められる設問の割合が例年よりも高く感じられる

Copyright © 2022 TAC CO., LTD.

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



Copyright © 2022 TAC CO., LTD.

SC　午前Ⅱ　特徴と難易度

- 3回に一度の情報セキュリティ管理からの出題が多い試験

小分類	R4春	R3秋	R3春	R2秋
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・ネットワーク分野の新テーマは5問
  - サイバーキルチェーンにおける偵察，量子暗号，SECURITY ACTION，IMAPS
  - NTPのクライアント向け簡略版プロトコルSNTP
- 過去問流用はセキュリティ分野で11問　8問がR2年秋から
- 重点分野20問中13問が過去問(過去問対策をしていると有利)
- 午前Ⅱ全体の難易度　⇒ 標準

Copyright © 2022 TAC CO., LTD.

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，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，令和になって初めて

- 午後問題で求められた特定の専門知識
  - PreparedStatement
  - Linuxのsudoコマンド，tarコマンド
  - “犯罪収益移転防止法(犯収法)におけるオンラインで完結可能な本人確認方法の概要”

- 選択問題や字句を解答する設問が多い
- 問題ごとのボリュームは問1，問2が多め
- 午後Ⅰ試験の難易度：標準～やや高め

Copyright © 2022 TAC CO., LTD.

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のセキュリティ対策」

- Webサイトセキュリティとセキュアプログラミングの問題
  - HTTPヘッダインジェクション，SQLインジェクション，メールヘッダインジェクション
  - アクセス制御要件に関する脆弱性
  - PreparedStatement：　H29秋にも出題
  - SELECT文のWHERE条件：E-R図から
- 知識の有無が問われるものが多いが，それほど高い知識は求められていない　⇒　難易度 ：　標準

Copyright © 2022 TAC CO., LTD.

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対応」
NAS製品とUPnP機能を持つルータを題材

- セキュリティインシデント対応の問題
  - ルータのUPnP機能がWAN側から有効化できない理由
  - ランサムウェア感染は，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　正規化の処理の順番
  - POSTメソッドで実行されると内容が分からない理由
  - Tarコマンドのオプション悪用を防ぐ策
  - 検索エンジンで検索されないようにする設定

- 専門性の高い特定の知識が求められる問題がある
  ⇒　難易度：やや高め

Copyright © 2022 TAC CO., LTD.

SC　午後Ⅰ　特徴と難易度　　問3

問3 「スマートフォン向けQRコード決済サービスの開発」
身元確認・当人認証，スマホやICカードのセキュリティ

- 身元確認・当人認証を実施するタイミング，本人確認の方法
- ログイン状態を1か月保持した場合のサービス不正利用
  - “犯収法におけるオンラインで完結可能な本人確認の方法の概要”(金融庁)の本人確認方法，“警察庁及び共管各省庁の考え方”の他人画像を利用させない方法

- 法令を知らなくてもほとんどは対応可能

⇒　難易度　：　標準

Copyright © 2022 TAC CO., LTD.

SC　午後Ⅱ　全体の特徴と難易度

- 問題によって差が見られる
  - 問1は，標準的な技術と管理のテーマを含む総合問題
  - 問2は，認証連携を全面的に扱い，技術的テーマのみ
- 目新しい設問
  - SSRFの脆弱性，アジャイル開発のセキュリティ確保
  - CDNを用いたドメインフロンティング攻撃，PKCE利用の攻撃対策
- 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　R4春，R3秋，R3春，R2秋，H30秋
- 問題文の分量：増加(11，14ページ)　図表：11点と13点
- 選択問題と字句のみで解答する設問割合が高い
- 2問の難易度に差があり(標準，難)，選択によって差

Copyright © 2022 TAC CO., LTD.

SC　午後Ⅱ　特徴と難易度　問1

問1　「Webサイトのセキュリティ」

- 脆弱性の診断や対策に関するWebサイトの総合問題
  - XSS脆弱性，CSRF脆弱性，クリックジャッキング脆弱性，SSRF脆弱性（初出題）
  - アジャイル開発にWebセキュリティ管理基準を適用する策，開発プロセス見直し

- 図表が11点で，問題文と設問文で11ページと長い
- 7割が選択問題or字句を解答する問題　⇒時間は余裕
- 幅広い知識が求められたが，全体的に解きやすい

　⇒　難易度：標準

Copyright © 2022 TAC CO., LTD.

SC　午後Ⅱ　特徴と難易度　問2

問2 「クラウドサービスへの移行」

- 認証連携によるシングルサインオンを実現するための代表的プロトコルをすべて出題
  - CDN利用の配信の仕組みや動作，
    ドメインフロンティング攻撃，Kerberos認証，
    SAML認証，IDaaSとSaaSが事前共有する情報，
    OAuth2.0を利用した場合，OpenID Connect利用の連携
- 図表が13点もあるうえ，問題文と設問文で14ページと長い
- 設問の9割弱は選択問題と字句での解答
- 各認証連携プロトコルの技術的知識が必要

⇒　難易度：難

Copyright © 2022 TAC CO., LTD.

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) v3.2についても目を通す

Copyright © 2022 TAC CO., LTD.

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，SSH)
  - メールの送信ドメイン認証
  - ネットワークの主要なプロトコル(ARP，HTTP，DNSなど)
- 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，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
- 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

Copyright © 2022 TAC CO., LTD.

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

Copyright © 2022 TAC CO., LTD.