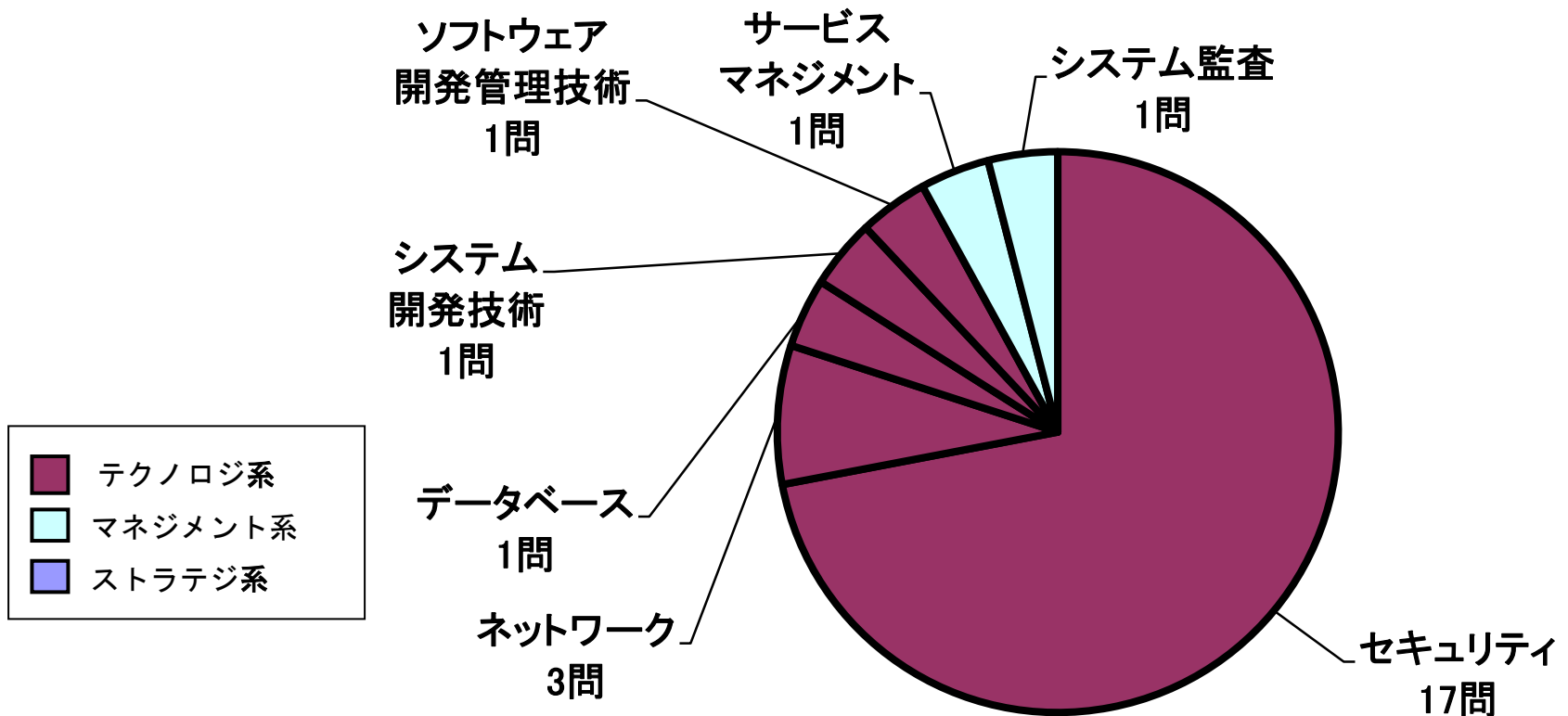


令和元年度 秋期試験 情報処理安全確保支援士試験(SC) 出題傾向分析

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

- ・ セキュリティ分野の出題比率が戻った
 - セキュリティ管理が出題されなかった前回と対照的

	R1秋	H31春	H30秋
情報セキュリティ	9	11	6
情報セキュリティ管理・情報セキュリティ技術評価	2	0	3
情報セキュリティ対策, 情報セキュリティ実装技術	6	6	8

- ・ セキュリティ分野の新テーマは4問 ⇒ 標準的な数
 - FIDO UAF, JIS Q 27014, BlueBorne, Exploit kit
 - ・ シラバス追補版(午前Ⅱ)からの用語は少な目
 - 全体的に知らないと答えにくい問題が多い
- ・ 午前Ⅱ全体では, 難しい問題は多くない ⇒ 標準的

SC 午後Ⅰ 全体の特徴と難易度

- ・ セキュアプログラミングが出題されていない
- ・ 電子メールのセキュリティ対策が久しぶりに出題
 - － 問1: 電子メールの送信ドメイン認証
 - － 問2: 標的型攻撃
 - － 問3: 標的型攻撃

頻出の標的型攻撃に寄った出題構成で選択しやすい

- ・ 全体的に定番の知識・解法を知っていれば対応可能
 - － 各問ともに新しいテーマ・概念を含む
 - ・ 問1: DMARC
 - ・ 問2: ISAC, DNSを用いたコネクトバック通信
 - ・ 問3: Windows系コマンド

問題文に既存知識を適用して考えられたか？ ⇒ 標準的

SC 午後 I 特徴と難易度 問1

- ・ 電子メールのセキュリティ対策
 - 送信ドメイン認証による、なりすましメールの防止
 - SPF, DKIM, DMARCの3つの方式が出題
 - ・ SPFとDKIMは、定番テーマ ⇒ 難しくない
 - ・ **DMARCは初出題**
 - 実際にはSPFとDKIMの組合せ
 - 問題文中の説明を読み、SPFとDKIMを組み合わせて考えられたかがポイント
 - SPFやDKIMに関して、仕組みや実現できることなど、幅広い理解が必要
 - ・ 定番テーマなので対応は可能 ⇒ **標準的**

SC 午後 I 特徴と難易度 問2

- ・ セキュリティインシデント対応におけるサイバーセキュリティ情報の活用
 - ISACから提供された情報を基にマルウェアの調査
 - ・ ISAC自体は問われていないので特別な知識は不要
 - ・ ISACへフィードバックする情報は目新しい印象
 - 今回はHTTPとDNSを用いたコネクトバック通信が出題
 - ・ DNSを用いた通信がメイン
 - ・ DNSを正しく理解していないと、攻撃手法やC&Cサーバに情報を送る方式がイメージしづらい
- ・ 知識的な難易度は高いが、難しい設問には選択肢が設定
⇒ 標準的

SC 午後 I 特徴と難易度 問3

- ・ 標的型攻撃への対応
 - デジタルフォレンジックス, ログ解析
 - Windows系コマンドが出題されている点が特徴的
 - ・ ipconfig, systeminfo, tasklist, net viewなど
 - ・ 設問は選択式なので, 対応可能
 - ログ解析の設問は経験が必要でやや難
 - ・ 定番論点の設問も多く, 解きやすい
 - 不審PCの電源を切らない理由, 不審PCの隔離など
- ・ 過去問題演習の効果が出やすい ⇒ 標準的

SC 午後Ⅱ 全体の特徴と難易度

- ・ 従来通りの技術系設問＋管理系設問の構成
 - － 技術系の設問がほとんどの前回とは対照的
- ・ 問題ごとに難易度に差が
 - － 問1: 知識的難易度が高めで、ページ数や設問は少な目
 - ・ 運用面の知識, セキュリティ対策の標準, コンテナ技術
 - － 問2: 既存知識で対応可能だが、ページ数や設問が多い
 - ・ APT攻撃, 認証サーバ, USBメモリ
 - ・ データダイオード方式など初出題の概念もあるが、問題文の説明から判断可能
- ・ 問1と問2のどちらかは選択可能
 - － 午後Ⅱ全体としては標準的な構成・難易度

SC 午後Ⅱ 特徴と難易度 問1

- ・ ソフトウェア開発におけるセキュリティ対策
 - マイニングマルウェアへの感染, マルウェア対策, DevOpsによる開発・運用プロセスの改善, という流れ
 - ・ Linuxコマンド, マルウェア活動の痕跡, マルウェア対策改ざん検知, コンテナ技術などの知識を要求
 - マルウェア関連などは問題文をじっくり読めば解答可能
 - 運用関連の知識は経験がないと答えづらい
 - ・ 脆弱性情報収集の前に必要な措置, パッチの適用
 - コンテナ技術もコンテナ型仮想化を知らないと解きづらい
 - セキュリティ対策の標準では, 初出題の用語が複数登場
 - ・ CIS Benchmarks, OWASP ASVS, FedRAMPなど
 - ・ 選択式だが「全て選ぶ」ので, 難しい
 - 全体的に知らないと解けない設問が多く, **難しい**

SC 午後Ⅱ 特徴と難易度 問2

- ・ 工場のセキュリティ
 - ランサムウェアへの感染, 現状の把握(課題の抽出), セキュリティ対策の見直し, という流れ
 - ・ User-Agent, APT攻撃のステップ, 無線LANへの攻撃, データの安全な転送方法, ネットワークの隔離, 認証サーバの設置, 各機器の主管部署
 - データの安全な転送方法では4種類の方法を比較
 - ・ FW, USBメモリ, 中継PC, データダイオード
 - ・ どの方式も概要が詳しく説明されているので, 問題文に沿って考えれば解答可能
 - 全体的に問題文に沿って定番知識を適用する設問が多い
 - ・ 知識が定着していれば時間内に解答可能

標準的な難易度

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割超
 - ・ 午後のベースとなる(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を
 - ・ 問題演習だけでは問われた部分しか確認できない
 - ・ 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
ex) DNS, HTTP, ARPなど
- 問題演習で問われやすい技術・プロトコルを確認
 - ・ 特に3回前からの出題率が高い
- IPAのシラバス(知識と技能の細目)についても目を通す
 - ・ シラバス追補版(午前Ⅱ) v3.0
 - ・ シラバス

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
 - ・ 午前Ⅱ対策と併用すると無駄がない
 - － マルウェアの種類・攻撃手法, 対策
 - － ファイアウォール, セキュアプロトコル
 - ≫ 主要プロトコルも (ARP, HTTP, DNS, SSH)
- － 過去問題演習で定番論点を把握
 - ・ 標的型攻撃, 感染対策, 出口対策
 - ・ ログ解析, デジタルフォレンジック, インシデント対応
 - ・ OSのコマンド等も把握 (UNIX系, Windows系)
 - ・ セキュアプログラミング (経験者のみ)

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, 管理面の知識・セオリーも重要
 - ⇒ まずは午後Ⅰ対策を重点的に
 - ⇒ 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
- ・ 管理・運用面の対策
 - ⇒ 経験がなければ過去問題演習でセオリーを習得

焦らず計画的に幅広く学習

ご清聴ありがとうございました

