

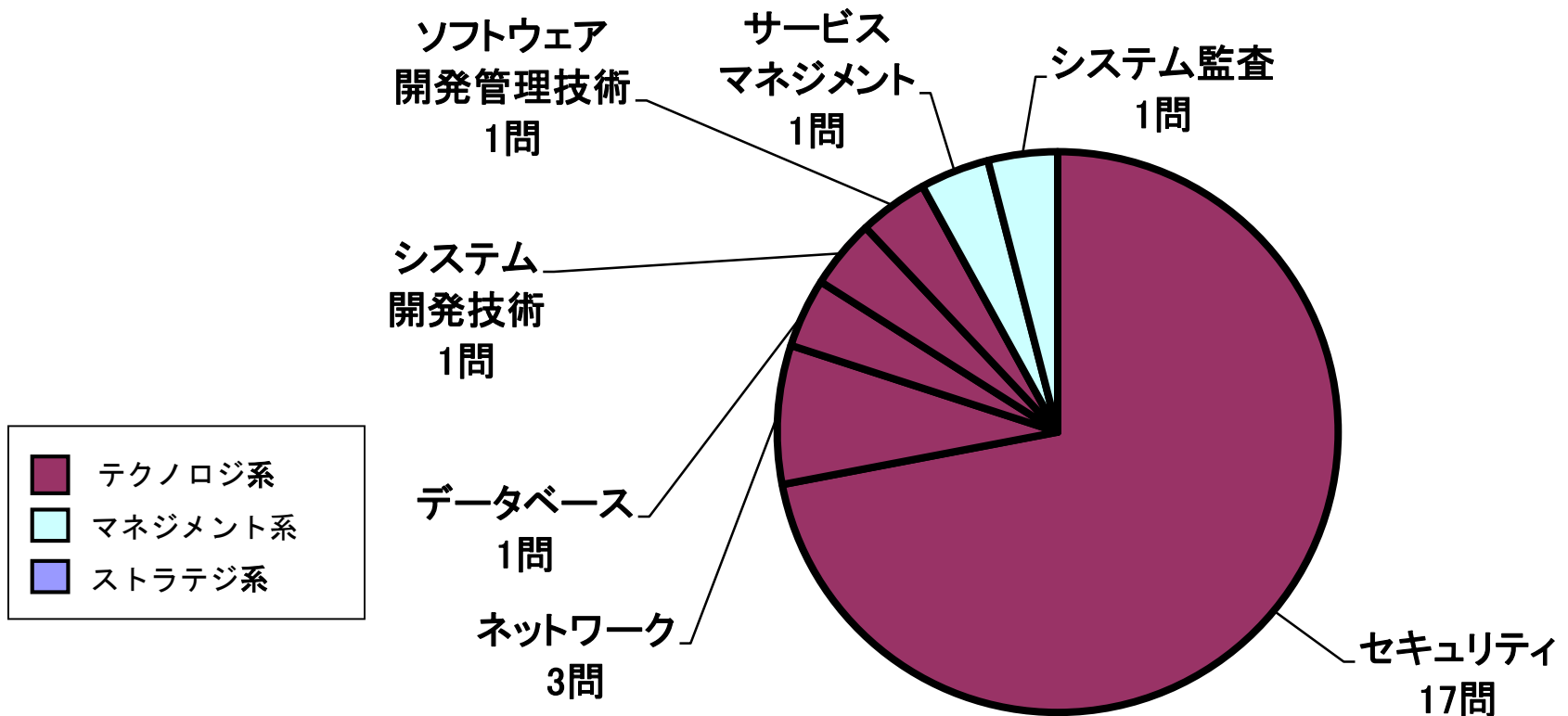
令和3年度 秋期試験 情報処理安全確保支援士(SC) 出題傾向分析

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

- 情報セキュリティ(攻撃・暗号・認証)からの出題が増加

小分類	R3秋	R3春	R2 10月	R1秋
情報セキュリティ	9問	6問	5問	9問
情報セキュリティ管理	1問	1問	3問	1問
セキュリティ技術評価	1問	1問	0問	1問
情報セキュリティ対策	2問	4問	3問	0問
セキュリティ実装技術	4問	5問	6問	6問

- セキュリティ分野の新テーマは7問 ⇒ 2問増
 - Adversarial Examples攻撃, Pass the Hash攻撃, PQC, SAML認証, サイバーキルチェーン, FWのステートフルパケットインスペクション, TLS1.3の暗号スイート
- 最新のセキュリティ動向に関する知識が多数出題
 - AI, 量子コンピュータ, TLS1.3, FIPS PUB 140-3, WPA3
- 他の試験区分の過去問題が多い 平均3問 ⇒ 今回5問
- 午前Ⅱ全体の難易度 ⇒ 難しい

SC 午後 I 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
 - 情報セキュリティインシデント対応 2問 定番問題が復活
 - システムの情報漏えい対策の設計 1問
- ・ 3問とも深いセキュリティ技術知識は要求されない
- ・ 単純な用語問題は皆無
- ・ 事例内容を正確に読み取る読解力が必要
- ・ セキュリティとネットワークの基本知識を応用させる力が必要
- ・ 3問とも分量は同じ 6ページ, 図表6点
 - ⇒ 難易度に差はなく, いずれも標準的

SC 午後Ⅰ 特徴と難易度 問1

問1 「セキュリティインシデント」

- 不正アクセスによる顧客情報漏えいのインシデント対応
- 主な設問内容
 - ・ FWのフィルタリングルールの設定
 - ・ アクセス権限種別
 - ・ ログの分析
 - ・ SSH フィンガプリント, パスワード認証, 公開鍵認証
- 深い知識, 最新の知識は要求されない
- 過去に繰り返し問われた論点がある
- 事例に合わせた具体的な設定内容を導く読解力が必要
⇒ 難易度: 標準的

SC 午後Ⅰ 特徴と難易度 問2

問2 「システム開発での情報漏えい対策」

- IRM製品を用いた設計秘密の情報漏えい対策
 - ・ **IRM**は初出題だが，機能の知識は不要
- 主な設問内容
 - ・ アカウントの種類に応じた権限の設定
 - ・ プロジェクト離任者への対応
 - ・ 暗号化ファイルの解読に要する計算量
 - ・ パスワード攻撃と対策
 - ・ マルウェア感染による秘密情報の不正取得方法
- 高度な知識は必要ないが，思考力が求められる
⇒ 難易度：**標準的**

SC 午後Ⅰ 特徴と難易度 問3

問3 「PCのマルウェア対策」

- PCのマルウェア感染のインシデント対応
 - 主な設問内容
 - ・ インシデント発生時の初動対応
 - ・ マルウェア定義ファイルの更新方法
 - ・ FWのフィルタリングルールの設定
 - ・ 実行ファイルのハッシュ値チェックの問題点
 - 新しい攻撃の知識が必要 ファイルレスマルウェア
 - 過去に繰り返し問われた論点がある
 - 問題文の記述内容をそのまま解答する問題がある
- ⇒ 難易度: 標準的

SC 午後Ⅱ 全体の特徴と難易度

- ・ 定番テーマ, 最近出題が増えているテーマで取り組みやすい
 - － 問1 セキュアプログラミング, IDaaS
 - － 問2 情報セキュリティインシデント, テレワークの導入
 - ・ セキュリティ技術中心に一部セキュリティ管理を問う総合問題
 - － 管理面: 問1 ISO/IEC 27017, 27018
 - 問2 独自のテレワークセキュリティ規程
 - ・ 2問とも要求される知識レベルは高くない
 - ・ セキュリティとネットワークの基本知識を応用させる力が必要
 - ・ 事例内容を正確に読み取る読解力が必要
 - ・ 2問とも分量は同じ 12ページ, 図表14点
- ⇒ 難易度に差はなく, いずれも**標準的**

SC 午後Ⅱ 特徴と難易度 問1

問1 「協力会社とのファイルの受渡し」

- システムの脆弱性診断と対策, クラウドへの移行
- 主な設問内容
 - ・ XSS脆弱性に関するセキュアプログラミング
 - エスケープ処理, **Content-Security-Policy** (初出題)
 - ・ SaaSへの移行時のセキュリティ対策の検討
 - **ISO/IEC 27017** (午前Ⅱでも出題), **ISO/IEC 27018**
 - ・ SIEMを利用したログからの不正アクセス検知
 - **SIEM**は初出題だが, 問われたのは既出のパスワード攻撃
 - ・ IDaaSとの連携による多要素認証の実現
 - FIDO認証 H31春午後Ⅰと同様の認証処理図の出題
- 幅広い知識が必要となるが, 知識レベルは高くない
⇒ 難易度: **標準的**

SC 午後Ⅱ 特徴と難易度 問2

問2 「マルウェア感染への対処」

- マルウェア感染による秘密情報漏えいのセキュリティインシデント対応
- 主な設問内容
 - ・ テレワーク導入時のセキュリティ規程の作成
 - ・ CRYPTREC暗号化リスト
 - ・ UTMを利用したC&Cサーバへの通信の遮断方法
 - DNSシンクホール 初出題
 - ・ マルウェアの感染範囲の絞り込み
- 問1ほど幅広い知識は求められていない
- 事例内容を的確に把握し、思考する能力が必要
⇒ 難易度: **標準的**

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
 - ・ 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
 - ・ 少なくとも過去5回分は演習を繰り返す(3回前を直前に)
 - ・ 誤答の用語についても確認し, 知識の幅を広げる
- IPAのシラバス追補版(午前Ⅱ) v3.2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(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
- アイデンティティ連携技術, クラウドセキュリティは要チェック
- **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

今後の対策(3)

・ 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**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