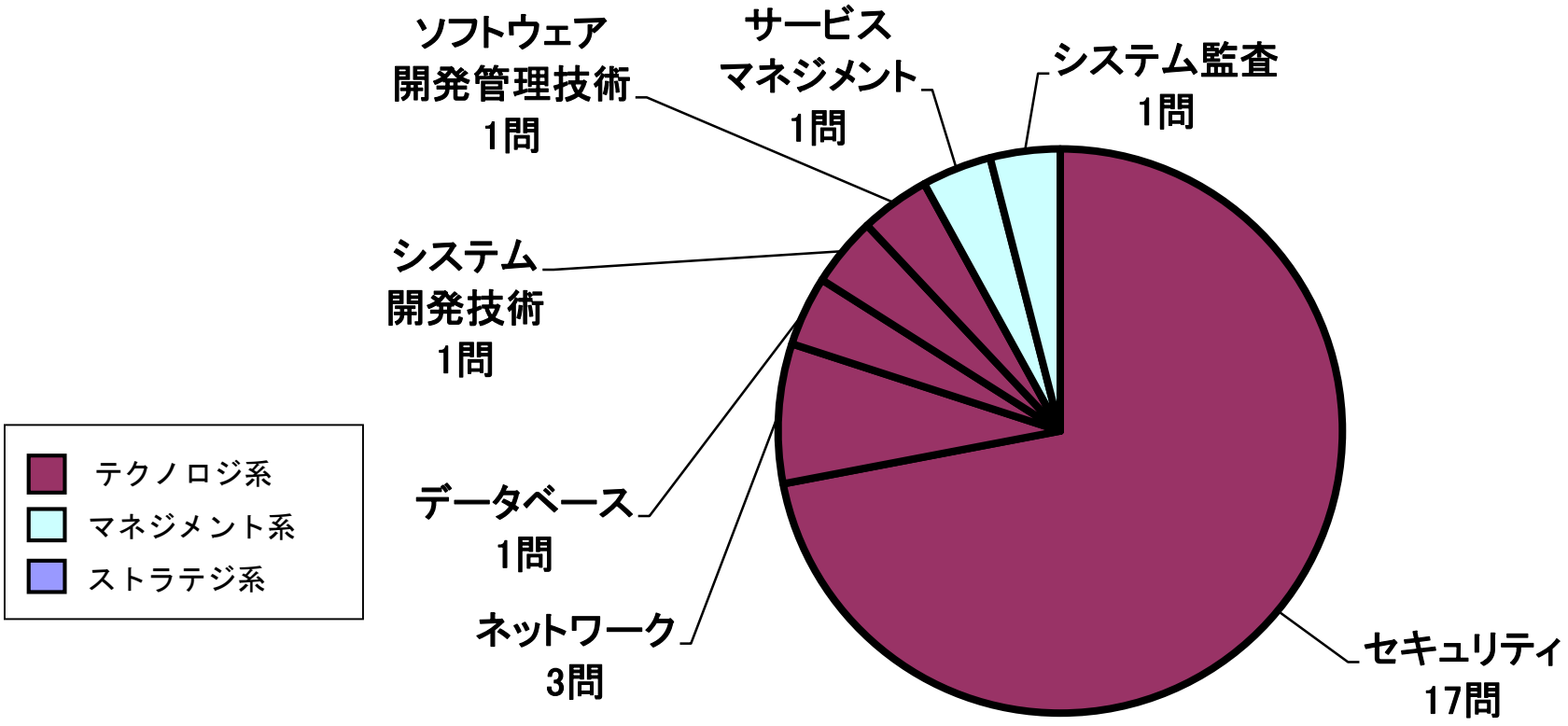
令和5年度　秋期試験
情報処理安全確保支援士（SC）
出題傾向分析

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　問題テーマの特徴

- セキュリティ分野：セキュリティ技術中心の出題傾向が継続

小分類	R5秋	R5春	R4秋	R4春
1. 情報セキュリティ	8問	6問	8問	6問
2. 情報セキュリティ管理	2問	2問	0問	4問
3. セキュリティ技術評価	1問	0問	1問	0問
4. 情報セキュリティ対策	0問	4問	2問	2問
5. セキュリティ実装技術	6問	5問	6問	5問

- 新規問題：8問（2問減）　このうち目新しい用語は2つのみ
  - クリプトジャッキング，SCAP，DNSSEC，OAuth 2.0，マルチキャスト通信で使用できるIPアドレス，IPアドレスの重複の確認に使用するプロトコル，DBMSのデータディクショナリ，カオスエンジニアリング
- SCからの流用：11問（2問減）
- 他の試験区分からの流用：6問（4問増）
  - 目新しい用語：公開鍵基盤のCPS，アジャイル開発手法のスクラム
- 目新しい用語は計4つ

SC　午前Ⅱ　難易度

- 難易度が高いと判定した問題：7問(前回より1問増)
  - 目新しい用語：4問(前回と同数)
  - 久しぶりの出題で技術レベルが高い：3問
    （例） XMLデジタル署名：7回前に出題
- 過去問題の流用率：約7割で平均的
- 過去問題演習の効果はやや低下
  - 流用される年度の範囲が拡大
    - 3～5回前に集中（特に3回前） → 3～10回前に拡大
  - 他の試験区分からの流用が増加，SCからは4割強
    - AP，SG，NW，AU，SM，ESから1問ずつ
- 午前Ⅱ試験全体の難易度：標準的

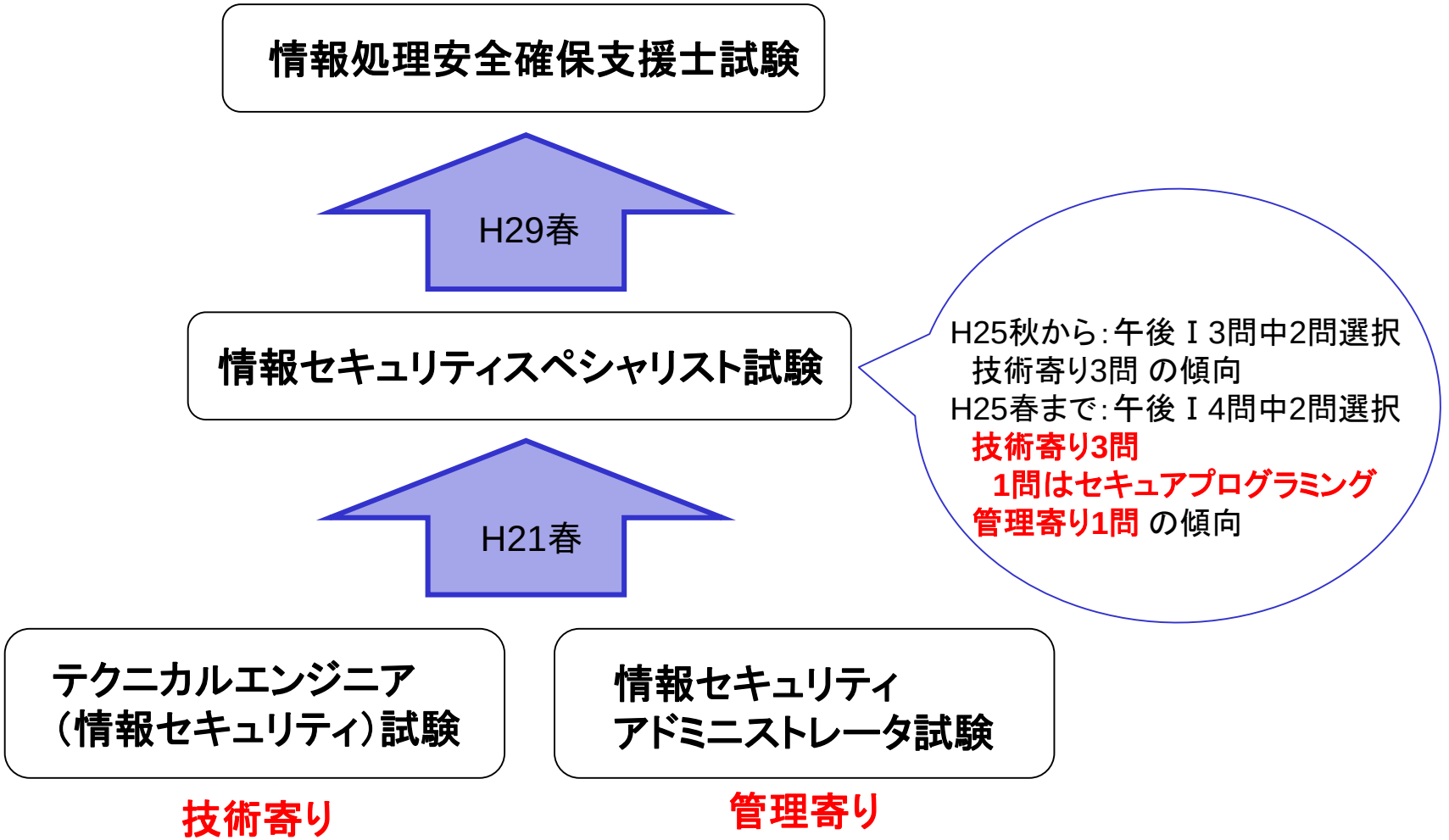
SC　午後　全体の特徴と難易度

- 午後試験の出題構成変更後，初回の試験

変更前	変更後
午後Ⅰ試験：90分，3問中2問解答	午後試験：150分，4問中2問解答
午後Ⅱ試験：120分，2問中1問解答	

- 問われる知識や技能の範囲に変化はない
- 大枠のテーマも過去に取り上げられたもので変化はない
- 午後Ⅱのような総合問題は出題されず，午後Ⅰに近い
- 技術寄り3問(1問はセキュアプログラミング)，管理寄り1問
  - 技術者、管理者などそれぞれの立場の人が選択しやすい
  - SCの歴史的背景から妥当
    ⇒今後もこの出題傾向が続くと予想

SCの歴史



SC　午後　全体の特徴と難易度

- 問題分量は午後Ⅰと午後Ⅱの間だが，問題ごとに大きな差がある
  - 5ページ(午後Ⅰと同等)～9ページ(午後Ⅰ・Ⅱの中間)
  - 1問当たりの解答時間は午後Ⅰより30分長い75分
    - 5ページの場合、時間的難易度が大幅に低下
    - 問題選択によっては時間に余裕はない
      ⇒問題ごとの時間的難易度の差が大きい
- 解答の字数制限が長くなり，制限のないものもある
  - より正確な知識と解答表現力が必要
    ⇒知識的難易度をやや上昇させる出題形式
- 午後試験全体の難易度：前回(午後Ⅰ＋午後Ⅱ)よりも易しい

SC　午後　特徴と難易度　　問1

問1　「Webアプリケーションプログラムの開発」

- クロスサイトスクリプティング(XSS)の脆弱性に関するセキュアプログラミング問題
- プログラムの処理内容が直接問われる
  - HTML，JavaScriptの知識が必須
- 開発者にとっては取り組みやすい
  - 脆弱性は頻出テーマであるXSS一つのみ
  - 問題文が5ページで午後Ⅰと同等，解答時間は30分長い
    ⇒時間的難易度が大幅に低下
  - 攻撃の仕組みを長文で解答
    ⇒知識的難易度をやや上昇させる出題形式
- 難易度：標準的　　※午後Ⅰとの比較

SC　午後　特徴と難易度　　問2

問2 「セキュリティ対策の見直し」

- オフィスの無線LAN環境を悪用した攻撃を防ぐためのセキュリティ対策の見直しの問題
- 4問中で最も幅広い知識が問われる
  - 無線LAN，VLAN，ファイアウォールのフィルタリング設定，サーバ証明書の検証，HSTS，EAP-TLS，TPM
  - いずれも頻出の技術知識⇒知識レベルは高くない
- 問題分量が多く(9ページ)，図表も多い(7個)
  ⇒時間的難易度はやや高い
- 難易度：標準的

SC 午後 特徴と難易度 問3

問3 「継続的インテグレーションサービスのセキュリティ」

- クラウドサービスを利用したソースコード管理に関するインシデント対応の問題
- 初出題の知識，比較的新しい技術知識が複数含まれる
  - 初出題：TLSのSNI(Server Name Indication)，ドメインフロンティング，FIPS 140-2 Security Level 3
  - コンテナ（H30春，R4秋），WebAuthn(H31春)
    ⇒ 4問中で知識レベルは最も高い
- 過去に問われた論点なども含まれる
- 時間的難易度は標準的
- 難易度：やや難しい

SC　午後　特徴と難易度　　問4

問4 「リスクアセスメント」

- 顧客情報を扱う配送業務を委託している企業におけるリスクアセスメントに関する管理寄りの問題
  - リスクアセスメント(H28秋)
- 知識レベルは高くない
  - パスワード漏えい，サイバー攻撃への技術的セキュリティ対策，物理的セキュリティ対策，人的セキュリティ対策
- 知見に基づく解答を求める，記述式試験では初めての出題
  - 字数制限もなく，自由度が高い⇒思考力重視
- 問題文が9ページ⇒時間的難易度はやや高い
- 難易度：やや難しい

今後の対策　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
  - 用語を暗記するのではなく，仕組みを理解する
  - 技術間の関連性を把握する
  - 攻撃手法，暗号・認証技術，PKI，セキュアプロトコルは頻出
- 過去問題演習で理解度・弱点を確認する
  - 直近の5年分(10回分)の演習を繰り返す
  - 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　午後対策

- 主要な攻撃手法やセキュリティ技術は体系的に整理し詳細まで理解
  - 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・認可技術
    - SAML，FIDO，WebAuthn，OAuth，ケルベロス認証
  - セキュアプロトコル(TLS，SSH ，IPsecなど)
  - 攻撃に利用されるプロトコル（ARP，HTTP，DNS，LDAPなど）
- 管理面の知識の補充
  - セキュリティ関連の基準や法規
  - 脆弱性評価指標（CVSSなど）
  - 人的管理，リスク管理

今後の対策　午後対策

- 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，一時的な対策，再発防止策
  - 運用管理面の対策
    - 午後Ⅱの管理寄り問題
- 長文問題に慣れる
  - 問題文を分割して隅々まで丁寧に読み込む
  - 解答に影響する記述を見落とさない工夫をする