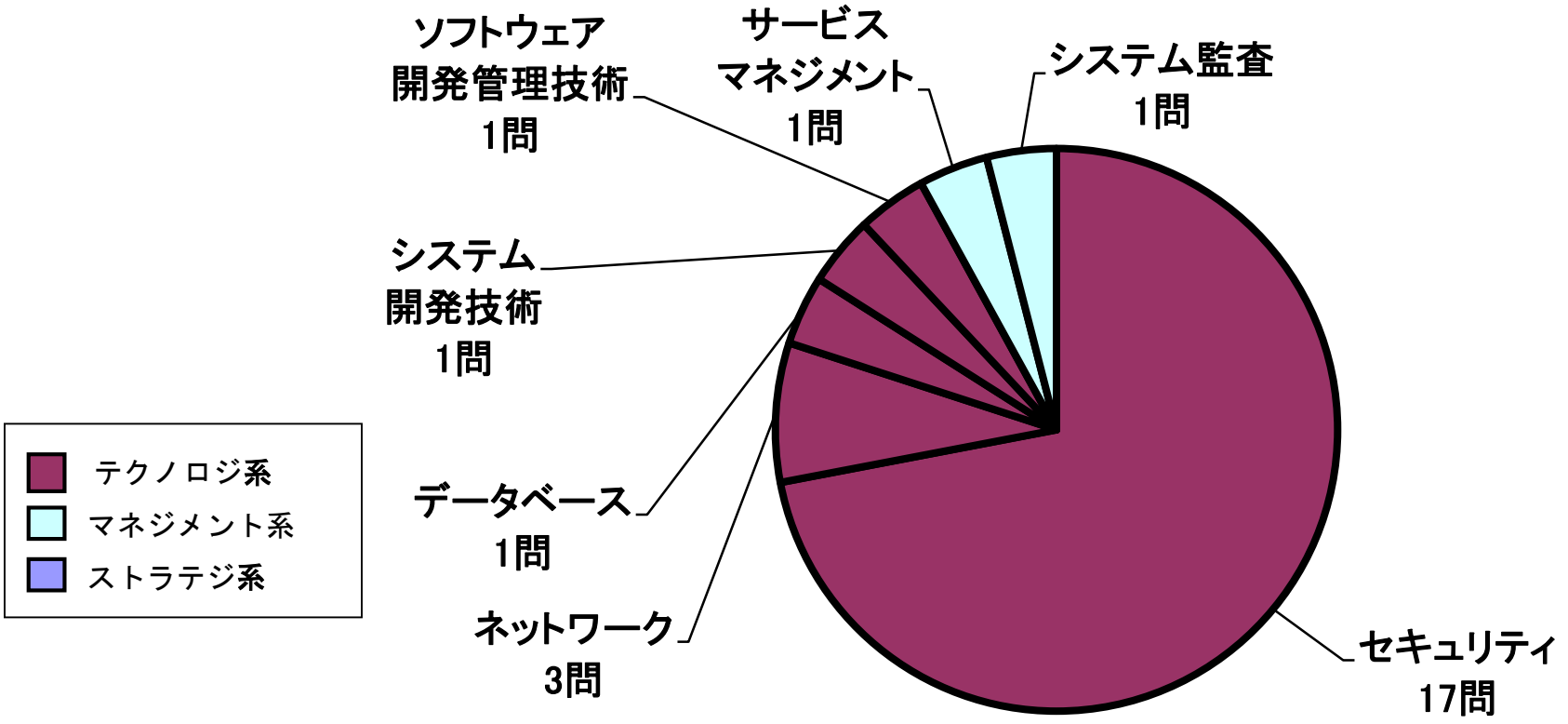
# 令和2年度　10月試験
# 情報処理安全確保支援士（SC）
# 出題傾向分析

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

- ほとんど出題されないセキュリティ管理からの出題が増加

| 小分類 | R2 | R1秋 | H31春 | H30秋 |
|---|---|---|---|---|
| 情報セキュリティ | 5問 | 9問 | 11問 | 6問 |
| 情報セキュリティ管理 | 3問 | 1問 | 0問 | 1問 |
| セキュリティ技術評価 | 0問 | 1問 | 0問 | 2問 |
| 情報セキュリティ対策 | 3問 | 0問 | 1問 | 2問 |
| セキュリティ実装技術 | 6問 | 6問 | 5問 | 6問 |

- セキュリティ分野の新テーマは5問　⇒　1問増
  - NOTICE，サイバー・フィジカル・セキュリティ対策フレームワーク，3Dセキュア，FWルールの変更，IP25B
  - 国の新しい取組みや指針，新技術など最近のテーマが増加
- セキュリティ分野は難，ネットワーク分野は易
- 過去問流用率は6割以上　⇒　前回と同じ
- 午前Ⅱ全体の難易度　⇒　やや難しい

# SC　午後Ⅰ　全体の特徴と難易度

- 午後の出題範囲とシラバス改訂の影響は感じられない
- 定番の出題がない
  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
  ⇒ システム設計・開発時のセキュリティ確保，
  　システム利用時のセキュリティ対策が出題の中心
- 問1は話題性の高いスマホ決済が題材
  「情報セキュリティ 10大脅威 2020」個人編の脅威 第1位
  問2のメールセキュリティは前回から継続出題
  　ただし、問われた技術は異なる
  問3のWebセキュリティ診断は問題の一部で過去に出題あり
  ⇒ さまざまなテーマから出題され，選択の余地がある
  　新しいテーマは問1のみ
- 深い思考力，実務経験が要求される　⇒ やや難しい

# SC　午後Ⅰ　特徴と難易度　　問1

問1 「スマートフォンを用いた決済」　⇒　新しいテーマ

- なりすまし決済の手段と対策
  - ・ メッセージ認証に用いるQRコードの生成と検証
- 店舗の無線LANルータの管理者機能への不正アクセス
- サーバ証明書の検証条件
  - ・ subjectAltName　⇒　新しい設定項目
- パスワードリスト攻撃
  - ・ スクリーニングの方法と対策　⇒　初出題

- 新テーマ，新知識項目により要求される知識レベルが高い
- 提示された機能や処理を読み取り，思考させる設問が多い

⇒　難しい

# SC　午後Ⅰ　特徴と難易度　　問2

問2 「電子メールのセキュリティ対策」

- S/MIMEの利用
  - ・ S/MIMEによるメールの暗号化とメールの通信の暗号化との違い
  - ・ S/MIMEの利用でメールを復号できなくなる場合
  - ・ S/MIME証明書の発行手続

- S/MIMEは午後問題での出題は10年ぶり
- メーリングリスト利用時を含めることで難易度がややUP

⇒　やや難しい

# SC　午後Ⅰ　特徴と難易度　　問3

問3 「Webシステムのセキュリティ診断」

- プラットフォーム診断とWebアプリケーション診断
  - ・診断時のIPSの設定・・・・攻撃か診断の通信か
  - ・診断PCの接続場所
- 本番環境での診断とステージング環境での診断
  - ・ステージング環境での診断終了後の処理
  - ・本番環境での診断実施時の影響の最小化

- 知識レベルの高いものは要求されない
- 問題文を丁寧に読み込むことで対応可能

⇒　標準的

# SC　午後Ⅱ　全体の特徴と難易度

- 午後の出題範囲とシラバス改訂の影響は感じられない
- セキュリティ技術中心の出題内容
  - 管理面の出題：問1　個人情報の取扱い
    問2　脆弱性情報の収集
- 比較的新しいテーマでの出題
  - 問1　複数のWebサイト間のアカウント連携の設計
    問2　クラウドサービス間の認証連携とテレワークにおける情報漏えい
- 2問とも要求される知識レベルが高い
- 2問とも事例内容が複雑で読み解くのに時間がかかる

⇒ どちらを選択しても難易度が高い

# SC　午後Ⅱ　特徴と難易度　問1

問1 「百貨店におけるWebサイトの統合」

- サイト間でのアカウント連携の設計
  - FWルールの変更
  - 個人情報の取扱い
  - アカウントの紐付けの例外処理のセキュアプログラミング(Java)
  - パスワード失念時の処理の脆弱性
  - SAMLによるシングルサインオン　⇒　出題頻度UP

- 幅広い高度な知識が要求されている
- 図表が合わせて10点　⇒　理解に時間がかかる
  - ソースコードは2頁以上　⇒　プログラミング未経験者は難問
- 事例内容に合わせた深い思考力が必要

⇒　難しい～非常に難しい

# SC 午後Ⅱ 特徴と難易度 問2

問2 「クラウドサービスを活用したテレワーク環境」

- 2要素認証の追加の方式
  - スマホのOTPアプリの初期設定
- クラウドサービス間の認証連携
  - RADIUS，OpenID Connect ⇒ 初出題
- 内部不正，マルウェア感染による情報の持ち出し
- 脆弱性情報の収集
- 公衆無線LAN利用時のリスク
- ノートPCの盗難・紛失時の情報漏えい

- 多くのクラウドサービス(SaaS，IDaaS，DaaS，・・・・) ⇒ 複雑
- クラウドサービス間の連携を読み取るのに時間がかかる
- 新しい技術やサービスを含む幅広い知識が要求されている
  ⇒ 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
    - 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
  - 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)
  - アイデンティティ連携技術，クラウドサービスのセキュリティの出題率が高まっているため要チェック
  - 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