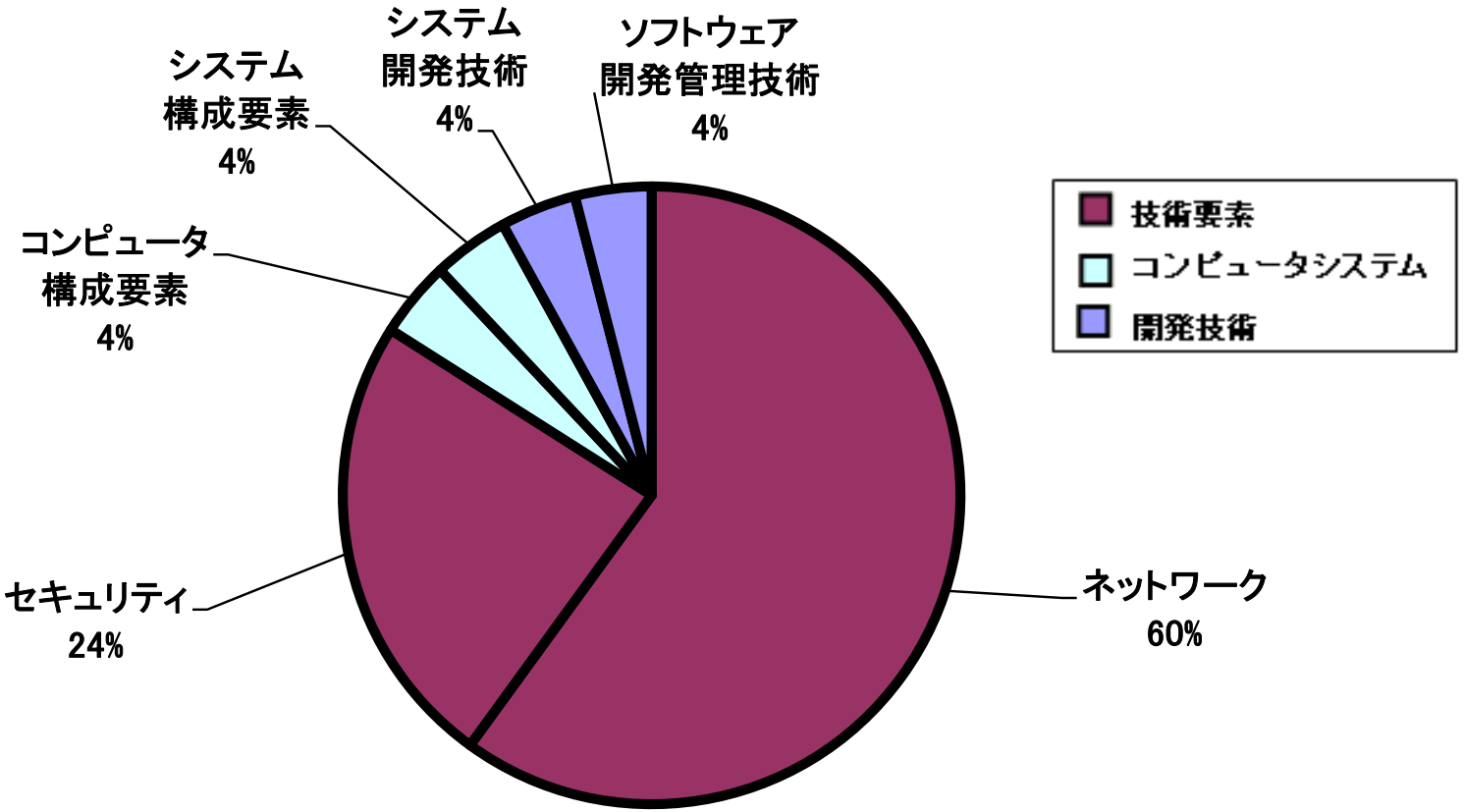
令和4年度　春期試験
ネットワークスペシャリスト（NW）
出題傾向分析

TAC株式会社

NW　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：ネットワーク＋セキュリティ　8割以上



NW　午前Ⅱ　特徴と難易度

- TCP/IPベースの通信プロトコルの出題が半数以上

小分類	R4春	R3春	R1秋
ネットワーク方式	2問	3問	0問
データ通信と制御	1問	3問	2問
通信プロトコル	10問	8問	9問
ネットワーク管理	1問	0問	1問
ネットワーク応用	1問	1問	3問

- 新テーマは（2問→5問）3問増　⇒　知識的な難易度は上昇
  RMON，RLOの利用手口，サイドチャネル攻撃，
  量子アニーリング方式の量子コンピュータ，ステージング環境
- 計算問題が減（6問→3問）3問減　⇒　時間的な難易度は低下
- 過去問流用率は約7割で例年どおり

⇒午前Ⅱ全体の難易度：標準的

NW　午後Ⅰ　全体の特徴と難易度

- セキュリティに関する設問が復活
- 大枠のテーマが分散しており，得意なテーマを選択しやすい
  - 問1　ネットワークの更改
  - 問2　経路制御
  - 問3　シングルサインオン
- ピンポイントの詳細なネットワーク技術知識は要求されない
  - →知識的な難易度は高くない
- 問題分量が増加（6ページ）
  - →読解に時間がかかり，読み落としも生じやすい
- 問題ごとの難易度の差はほとんどない

⇒ 午後Ⅰ全体の難易度：標準的（前回より易しい）

NW 午後Ⅰ 特徴と難易度 問1

問1 「ネットワークの更改」

- ファイルの受渡しをUSBメモリからネットワーク転送へ
- 基礎知識をベースとした出題内容
  - ネットワーク技術：ミラーパケット取得時の接続・設定，必要なディスク容量
  - セキュリティ技術：DMZを設置する目的，認証・認可
  - 用語穴埋め問題：syslog，HTTPのDigest認証，CONNECTメソッドは既出
- 知識レベルは易しめ
- 一部，解答表現の方向性を定めにくい

⇒ 難易度：標準的

NW 午後Ⅰ 特徴と難易度 問2

問2 「セキュアゲートウェイサービスの導入」

- 既出のネットワーク技術に関する出題内容
  - VRF：H25年午後Ⅰで既出。具体的な設定内容は初出題
  - OSPF：頻出。過去にも問われた再配布について出題
  - IPsec VPN：頻出。IKEv2，Diffie-Hellmanグループ番号は初出題
- PaaSとセキュアゲートウェイサービスの導入
  - セキュリティの観点での確認事項
- 丁寧に読み取れば解答可能なものが多いが，一部初出題の項目が含まれる

⇒ 難易度：標準的

NW 午後Ⅰ 特徴と難易度 問3

問3 「シングルサインオンの導入」

- H27年午後Ⅰと同一テーマ
  - 今回はケルベロス認証について初出題
- ネットワーク技術とセキュリティ技術をバランスよく問う問題
  - PCのプロキシ設定，ケルベロス認証の通信手順，DNSのSRVレコード，DNSラウンドロビン
  - FWのフィルタリングルール，ケルベロス認証での盗聴による不正アクセス防止策
- 初出題の技術でも問題文中に丁寧に説明されている内容を読み取れるだけの基礎知識があれば十分対応可能

⇒ 難易度：標準的

NW　午後Ⅱ　全体の特徴と難易度

- 2問とも最近注目されているテーマでの出題
  - 問1：テレワーク導入
  - 問2：コンテナ仮想化
- 午後Ⅱのこれまでの出題傾向を踏襲した内容
  - 新技術が含まれる（問1，問2）
    - TLS1.3，コンテナ仮想化技術
  - セキュリティについて問われる（問1）
  - 運用管理について問われる（問2）
- ピンポイントの詳細な知識は必要とされない
- 問題ごとの難易度の差はほとんどない

⇒　午後Ⅱ全体の難易度：標準的

NW　午後Ⅱ　特徴と難易度　問1

問1 「テレワーク環境の導入」

- SSL-VPNを用いたテレワーク環境導入を出題
  - ポートフォワーディング方式：H25年午後Ⅰで既出
- ネットワーク技術とセキュリティ技術の幅広い知識が必要
  - IPアドレスの割当て
  - OSPF：頻出。Equal Cost Multi-Path機能は初出題
  - VRRP：頻出。既出の障害発生時の切替えについて出題
  - TLS1.3の特徴，ハンドシェイク：新技術の知識を直接問う
  - クライアント証明書を用いたクライアント認証
  - X.509証明書のフィールド名，証明書の発行と失効
- 新技術以外の知識レベルは標準的

⇒　難易度：標準的

NW　午後Ⅱ　特徴と難易度　問2

問2「仮想化技術の導入」

- コンテナ仮想化技術
  - ・サーバ仮想化技術との対比
  - ・仕組みや通信の流れの説明を読み取りながら解答可能
    →新技術そのものの知識は不要
- ネットワーク技術知識のほか運用管理知識も必要
  - ・VRRP，負荷分散，監視に関するネットワーク技術知識
  - ・障害発生箇所の特定，システム移行のネットワーク運用管理知識
- 技術知識レベルは標準的
- 移行手順は実務経験がなくても過去問演習で対応可能

⇒　難易度：標準的

今後の対策（1）

- 午前Ⅱ対策
  - ネットワーク分野とセキュリティ分野で8割以上
    - 午後のベースとなる知識なので十分に学習
  - テキストを用いた体系的な知識習得
    - 問題演習だけでは問われた部分しか確認できない
    - 技術やプロトコルの特徴だけでなく，仕組みを理解
    - 主な攻撃手法と対策についても確認
  - 過去問題の再出題率が高く，過去問題演習は必須
    - 少なくとも過去5回分は演習を繰り返す
    - セキュリティ分野はSC試験の過去問題演習も有効

今後の対策(2)

- 午後Ⅰ対策
  - 主要な技術やプロトコルは詳細まで理解
    - ルーティングプロトコル(OSPF，BGP)の出題頻度が増加
    - IP，ICMP，TCP，DHCP，DNS，HTTP，SNMP，SIPなど
    - VLAN，VRRP，スパニングツリー，仮想化，負荷分散，無線LANなど
    - セキュリティ関連(暗号化，認証，PKI，プロキシサーバ，FWのフィルタリングルール，TLS，VPN，スパムメール対策，無線LANセキュリティなど)
  - 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，弱点の洗い出し
    - 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
  - より幅広い知識，より深い知識が必要
    - まずは午後Ⅰ対策を徹底的に行い，弱点を把握
    - 弱点テーマの知識を補強後，午後Ⅱ対策へ
  - 管理面の知識も重要
    - 移行・運用管理面の対策
      ⇒　経験がなければ過去問題演習でポイントを習得
  - 複雑な長文問題への対応
    - 問題文を分割して読解する練習
    - 図表から必要な情報を読み取る練習
  - 新技術への対応
    - 日頃から情報収集を