2018 秋 ネットワークスペシャリスト 全国統一公開模試 講評と採点基準

2018 年 9 月 25 日 (株)アイテック IT 人材教育研究部

■ 全体講評

1. 午前試験について

午前Ⅰ，午前Ⅱ試験が合格点に届いていない方は，底上げのための追込み学習を行って万全を期するようにしましょう。午前Ⅰ試験は，頻出用語の整理が効果的です。午前Ⅱ試験は，最近の問題の再出題も多いので，2～5 回前を中心とした過去問題の演習が効果的です。

2. 午後試験について

過去問題演習や専門知識の学習を積み重ねたことが伝わる安定感のある答案から，基礎的な知識の不足や記述式問題に慣れていないと思われる答案まで，得点力には幅があります。

模擬試験で合格点を取れた方は，自信を持って本試験でも実力を発揮してください。一方，模擬試験では思うように得点できなかった方も，残りの期間を有効に活用すれば勝負になります。実際に，過去には模擬試験の D 判定や E 判定に奮起して，見事に合格した方もいます。

時間不足や逆に時間が余って得点不足になった方は，時間管理の強化を検討しましょう。本来であれば得点できたはずの設問に時間をかけられなかったという状況や，急ぎ過ぎて問題文を読み違えるケアレスミスはもったいないです。

追込み学習のポイントは次の二つです。

(1) 重点技術の整理

重点技術とは，本試験で繰返し出題されている技術で，NW 試験向けの参考書で説明されている内容です。重点技術の知識の差は得点に影響します。NW 試験では毎回，試験として初めて取り上げられる技術も出題されます。本文を読みながら新しい技術を理解するためにも，重点技術の整理が大切です。参考書だけではなく，過去の午後Ⅰ／Ⅱ問題を事例として読み込むことによって，理解が深まります。

(2) 記述式問題の解法の見直し

過去問題を使って，記述式問題の解法を確認しましょう。重要なことは次の 2 点で，具体的には問題ごとの講評に記載します。

① 設問で問われていることを十分に押さえる

「目的」が問われているのに，「原因」を解答したり，「設定内容」が問われているのに，「理由」や「目的」を解答したりする設問とずれた解答があります。また，設問文に「○○○を含めて」や「○○○に着目して」とあるのを読み落とし，要求事項を充足しない解答もあります。設問文や下線部，下線の前後の条件を正しく読まないと，いくら考察しても，正解につながりません。

② 解答文は掘り下げて説明するスタンスでまとめる。

本文の文章をそのまま転記するだけの解答は少ないと考えてください。設問文や本文のキーワードを使うことはよいのですが，丸写しはほぼありません。解答文のまとめ方に慣れるために，過去問題を演習して，試験センターの解答例をよく吟味しましょう。

3. 本試験に向けて

試験当日は，集中力，精神力，体力の勝負になります。最後まであきらめずに，必ず合格するという強い意志をもって，解答作業に集中しましょう。最後の 5 分が合否を分けることもあります。特に午後Ⅱ試験では，本試験においても得点しやすい設問と得点しにくい設問が混在しています。非常に難しいと感じる設問は後回しにして，その他の設問を一つ一つ仕上げていく姿勢が大切です。模擬試験でも，最後まで粘ったと思われる答案は，相応の得点を取れています。

【部分点の配点について】

部分点は，配点の半分の点数です。配点が 5 点や 3 点のように奇数点の設問については，原則として端数切上げにしていますが，答案の内容に応じて端数切捨てにしている箇所もあります。また，内容に応じて，例外的に配点の半分の点数ではない場合もあります。

＜午後Ⅰ＞

問1 ネットワークの冗長化

【採点基準】

［設問1］

ア～キ：解答例だけを正解としました。

［設問2］

(1) 解答例のように，LAG の負荷分散アルゴリズムと TCP コネクションの性質を組み合わせて説明できているものを正解としました。

(2) 解答例のように，受信側のホストで発生する問題に関して，TCP による制御と組み合わせて説明できているものを正解としました。単に「再送が必要になる」などのように，着眼は正しいものの，問題として明確に表現できていないものは部分点としました。

(3) 解答例のように，MAC アドレステーブルに関する処理について，論理ポートに着目して説明できているものを正解としました。

［設問3］
（1）解答例のように，項番 1 のアルゴリズムを採用した場合の不都合や LAG を設定する目的に関して，理由として説明できているものを正解としました。
（2）項番と機器名は完全正答で，解答例だけを正解としました。理由は，解答例のように，RDP の通信特性に基づいて説明できているものを正解としました。項番を 4 と解答して，理由を「宛先ポートが特定になる」としたものは，理由に関して原則として部分点としました。

【講評】
［設問1］
・カで「VM」は仮想 PC を指すので不正解としました。また，「VMware」のように固有の企業名（製品名）の解答が見られましたが，本文内に記述が無い限り，固有の名称は使わずに解答します。
［設問2］
（1）正答率は高かったです。設問文で「TCP コネクションの性質に着目して」と指示された場合には，TCP コネクションの性質がどのようであると着目したかを含めて解答文を作成することがポイントです。表 2 のアルゴリズムに関する TCP コネクションの性質は，コネクションが IP アドレスとポート番号で識別されることです。そこで，この二つを軸に説明します。単に「TCP コネクションを確立しているから」は，性質に関して説明不足です。
(2) 設問の主旨を適切に把握できていない解答が多く見られました。具体的には，設問では受信側のホストで発生する問題が問われていますが，送信側のホストや途中のネットワーク経路で発生する問題がありました。また，「TCP による制御に着目して」と指示されていますので，(1)の講評と同様に，TCP による制御の何に着目したかを含めて解答文を作成します。TCP の制御に触れずに，単に「パケットロス」といった解答などは，内容に応じて部分点あるいは不正解としました。また，IP フラグメントに着目した解答がありましたが，IP フラグメント（IP パケットの断片化と再組立て）は IP の機能で，シーケンス番号を用いる TCP による順序制御とは異なります。
（3）正答率は高めでした。下線③の前の本文の記述から MAC アドレステーブルの処理に関する内容と読み取ります。MAC アドレステーブルは，MAC アドレスとスイッチのポートを関係付けます。IP アドレスやレイヤ 4 のポート番号に言及した解答もありました。MAC アドレステーブルは重要ですので，よく確認しておきましょう。

［設問3］
（1）理由として単に項番 1 のアルゴリズムを復唱して掘り下げていないものは不正解としました。また，項番 1 を選択した上で「送信元 IP アドレスが仮想 PC ごとに異なる」という解答がありましたが，L2SW4 が学習する送信元の MAC アドレスは，物理 NIC ではなく仮想 NIC の MAC アドレスなので，送信元 IP アドレスと送信元 MAC アドレスは 1:1 に対応し，フラッピングは発生しません。1 台の仮想 PC からの通信に関して，宛先 IP アドレスによって経路が異なるとフラッピングが発生します。
（2）正答率は低かったです。RDP の通信の往路に着目して項番 4 を選択した解答が多くありました。復路も同様なので，解説のとおり，往路と復路のどちらがより注意が必要であるかを吟味する問題でした。

問2 情報提供を行う Web サイトの増強

【採点基準】
［設問1］
ア，イ：解答例だけを正解としました。
［設問2］
（1）解答例のように，セッション維持に関して TCP ヘッダ情報では不都合があることや，IP ヘッダ情報（送信元 IP アドレス）が適していることを適切に説明しているものを正解としました。
（2）解答例のように Z 社のサービス特性を踏まえて，L4LB でもセッション維持機能が有効に機能することを説明できているものを正解としました。
［設問3］
（1）解答例のように，ソーリーサーバの停止の影響度が低いと言える理由を適切に述べたものを正解としました。
（2）解答例のように，FW と LB の機能の違いに着目して，適切に説明できているものを正解としました。「L4LB が Web サーバに対する負荷分散を行う」のように適切なものは正解としました。
（3）解答例だけを正解としました。
（4）解答例だけを正解としました。

【講評】
［設問1］
・アで「負荷分散」は，空欄の前の「増強に関して」という目的を踏まえて，さらにスケールアップと対比される用語として「スケールアウト」が適切ですので，不正解としました。
［設問2］
（1）設問の主旨を正確に押さえたかどうかで差がつい

ています。設問の主旨は，セッション維持であり，単に負荷を分散させるだけではありません。単に負荷を均等に振り分けるだけととらえると，「接続元IPアドレスが不特定多数に分散するから」のような解答になります。セッション維持は，本文の記述のとおり，同じ宛先サーバに対してリクエストを振分けします。また，「送信元IPアドレスは重複することがない」と断定している解答がありましたが，顧客の接続環境によって重複することはあり得ます。断定表現をするときには，絶対にそう言えるかを吟味したいです。そして，仮に「重複しない」としても，それはポイントではなく，Web通信の途中で変化することが少ないことがポイントです。また，「同じ送信元IPアドレスのリクエストは同じWebサーバに振り分けるため」のように理由として説明不足なものは不正解としました。

(2) 下線②の前に「Z社のサービスの特性を考慮すると」とありますので，サービスの特性を含めていないものは説明不足で，部分点あるいは不正解としました。また，逆に単にサービスの特性だけを説明して，L4LBの特徴に関連付けていないものは不正解としました。解答では，表1などの機器の性能に着目して，「L4LBの性能が高いから」という着眼がありましたが，この着眼だと「L4LBの方がよい」という結論になり，「L4LBでもよい」の理由にはなりません。また，「Webサイトが Cookieを使用していないから」という解答もありました。仮に，Cookieを使用していない場合には，Cookieを用いるL7LBによるセッション維持は実現できなくなりますので，「L4LBでないといけない」という結論になり，「L4LBでもよい」理由にはなりません。また，「Webサイトでは単一のTCPコネクションで通信するから」という主旨の解答がありました。この仮定が正しいとすると，下線①の結論（TCPヘッダ情報ではなく，送信元IPアドレスが適切）と矛盾しますので，不正解としました。

［設問3］

(1) 適切な説明が多く見られ，正答率は高かったです。

(2)「FWの方がLBよりも処理性能が高い」という着眼の解答がありますが，性能が高いから上位に配置するのではなく，内部ネットワークを防御するために上位に配置し，LBはWebサーバに対する負荷分散を行うために下位に配置します。そして，その配置で動作させるために，結果的にFWに関して必要な高い性能の機種を選定していることになります。FWの必要台数に着眼した解答があり，構成方法によっては正しい内容ですが，台数は結果的にそうなると考えられますので，機能の役割分担への着眼が適切と判断して不正解としました。

(3) FWやLB，Webサーバに関して，本文や表2で示されているように冗長化種類のM/SとCLUSTERを読み落としていると思われる数値が散見されました。正答率は高めでした。

(4) 正答率は低めでした。ソーリーサーバの動作条件については，本文の記述に則して考察することがポイントです。

問3 IoTシステムのネットワークの検討

【採点基準】

［設問1］

(1) ア～エ：解答例だけを正解としました。

(2) 解答例のように，周波数帯域を含めて無線通信の干渉などの支障の内容を説明したものを正解としました。「2.4GHz」がないものは減点しています。

［設問2］

解答例だけを正解としました。

［設問3］

(1) 解答例だけを正解としました。

(2) 解答例だけを正解としました。

(3) 解答例だけを正解としました。

［設問4］

(1) 解答例のように，理由として専用線や閉域網接続に着眼し，セキュリティ面の利点を説明できているものを正解としました。

(2) 解答例のように，TCPとUDPの違いである再送機能に着目したものを正解としました。

【講評】

［設問1］

(1) ウに関して「伝送距離」を答えた解答が見られましたが，伝送距離は「TCP/IPを使う通信」と直接に関連しません。エ（802.15.4）は正答率が低かったです。過去問題の問題文には登場している規格ですので，押さえておきましょう。

(2) 支障の内容に関しては正解率が高かったです。一方，設問の指示事項の読み落とし，あるいは単に「周波数帯」という字句を含めてと誤解釈した解答が見られました。特定の字句を含める指示の場合には，「○○という字句を含めて（用いて）」のようになります。

［設問2］

管理用のデータを含めていない数値が多く見られました。設問文に書いてある内容の見落としは避けたいです。

［設問3］
（1）想定よりは正答率が低かったです。SYN+ACK を二つのシーケンスに分けた解答がありましたが，3 ウェイハンドシェイクですので，1 シーケンスです。
（2）こちらも管理用データを含めていないケアレスミスが見られました。
（3）(2)よりは正答率が低かったです。小数第 2 位切上げという指示に関するケアレスミスもありました。
［設問4］
（1）正答率は高かったです。セキュリティ面の利点が問われていますので，単に「セキュリティが高い」や「安全」では利点を説明できていません。
（2）設問では，「どのような機能か」が問われていますが，機能として表現できていない解答が多くありました。

＜午後Ⅱ＞
問1　検疫ネットワークの構築
【採点基準】
［設問1］
（1）解答例だけを正解としました。
（2）解答例のように，DHCP におけるブロードキャスト通信に着眼して説明できているものを正解としました。
（3）解答例のように，本文の記述に整合する FW の設定内容を適切に説明できているものを正解としました。
（4）解答例のように，NPC におけるネットワーク設定情報（デフォルトゲートウェイ，あるいは IP アドレスや所属するサブネット）を用いて適切に説明できているものを正解としました。
（5）解答例と同じ主旨だけを正解としました。
（6）解答例のように，ポートの監視や制御に着目した説明を正解としました。
（7）解答例と同じ主旨だけを正解としました。
［設問2］
（1）オは解答例だけを正解としました。カは，「検査結果（合格）」など合理性のあるものは正解としました。「認証結果」は，認証サーバからの応答で通知済みですので，不正解です。
（2）解答例だけを正解としました。
（3）解答例と同じ主旨だけを正解としました。
［設問3］
（1）コ：「トランスポート層」は部分点としました。サ：「Certificate」も正解としました。
その他は，解答例だけを正解としました。
（2）解答例と同じ主旨だけを正解としました。
（3）解答例と同じ主旨だけを正解としました。証明書と秘密鍵の役割分担に踏み込まずに，単に「端末を認証する」は，二つ合わせて部分点などとしました。
（4）解答例のように，クライアント証明書の有効期間に関する留意点について，有効期限切れの前に行うべきことを説明しているものを正解としました。
（5）機能に関しては，解答例のように CA の機能を挙げているものを正解としました。「証明書の管理機能」は，発行機能とは別の機能と読めますので，不正解としました。情報に関しては，解答例と同じ主旨だけを正解としました。「CA の公開鍵」は間違った内容ではありませんが，正確ではないので不正解としました。

【講評】
［設問1］
（1）「IPv4 アドレスで」や「MAC アドレスを 16 進表現で」という指示に沿わない解答が散見されました。イの「DHCP リレーエージェント」は頻出の用語です。空欄前後の記述の読み違いと思われる誤りが見られました。
（2）単に「TCP コネクションが確立できない」という主旨の解答は，DHCP が UDP を使用する理由としては遠い理由です。DHCP の通信と関連付けて説明したいです。
（3）パケットフィルタリングの一般的な機能や設定を説明した解答がありましたが，「FW の設定内容」のように「内容」が問われた場合には，本文の記述に基づいて具体的に説明するようにしたいです。業務ネットワークだけに関する設定では不十分なので不正解としました。また，単に「NPC と検疫ネットワーク間の DHCP を許可」のように不明確な説明は部分点あるいは不正解としました。「DHCP リレーの設定」だけの解答は，空欄イの箇所に記述されているので，不正解としました。「DHCP サーバからリースされた IP アドレスを通信許可する」や「検査に合格した NPC について～」のように，検疫の状態に応じて通信を制御する内容に関しては，FW におけるパケットフィルタリングでは，あくまで IP ヘッダや TCP/UDP ヘッダの情報に基づいて通信を制御しますので，不正解としました。さらに，FW はネットワークの境界ですので，検疫ネットワークと検疫ネットワーク用のネットワークアドレス，業務ネットワークと業務ネットワーク用のネットワークアドレスはそれぞれ異なります。
（4）単に「検疫前と検疫後の NPC が異なるネットワークに所属する」という解答は，IP 通信ができない理由としては説明不足で，内容によって部分点あるいは不正解としました。「検疫前は NPC に IP アドレスが付与されていない」という解答は，下線②の

前に，検疫に先立ってIPアドレスを受け取る旨が述べられているため，不正解としました。「検疫前のNPCからは業務ネットワークに接続できない」という解答は，(3)の講評の最後に補足したように，検疫後のNPCは業務ネットワークには含まれず，業務ネットワーク用のネットワークに含まれるので不正確です。また，下線②をDHCP方式以外の方式に関する記述と読み違えている解答が見られました。

(5) 正答率は高かったです。回避手段を，その手段に対する回避策（対抗策）と読み違えた解答がありました。

(6) MACアドレスに着眼した解答は，下線④の後ろの記述に「その他に，～」とありますので，下線④の機能には該当しません。また，「許可されていないPCからの接続を拒否」のように，PCの認証状態を管理できるのは，設問3で登場する802.1X認証の機能です。ここで考察する認証スイッチ方式は，あくまでVLANを利用してポート単位で制御する方式であることを押さえたいです。

(7) 正答率は高かったです。「ポート数」に着目した解答もありましたが，解説のとおり，本文の記述の中にメリット／デメリットの観点が示されている場合には，本文の記述を踏まえた解答をすることが確実です。また，「認証サーバが必要」を含む解答がありましたが，下線⑤に関わる図4の認証スイッチ方式では，認証サーバは使いません。(6)の講評と同様に，設問で問われている検疫方式がどの方式なのかをよく確認しながら解答したいです。

［設問2］

(1) オに関して，「FW」という解答がありましたが，解説のとおり，802.1Xではオーセンティケータの認証SWが通信を制御します。

(2) 正答率は高かったです。

(3) 単に「取引先向けのVLAN」のような解答は「どのようなVLANか」という設問に対して説明不足です。ネットワーク設計の視点で本文の要望を的確にまとめたいです。同様に「業務ネットワークに接続できないVLAN」もどういうVLANか不明確です。

［設問3］

(1) キの802.1XやケのEAPOLは，頻出のキーワードですが，正答率は想定よりも低かったです。

(2) 単に「クライアントとサーバの相互認証」や「認証情報の暗号化」，「一般的なプロトコル」は，PEAPやEAP-TTLSでも該当するため不正解としました。解答例は，本文の記述を使っていますが，EAP-TLSの特徴は，クライアント認証をPKIに基づくディジタル署名で行うことです。つまり，パスワード認証のような利用者単位の認証ではなく，A社の要件である許可された端末単位の認証を実現できることがポイントです。そのような特徴を的確にまとめた解答も見られました。

(3) 設問文では，「EAP-TLSクライアント認証の処理における～」と述べられていますが，クライアント認証ではなく，メッセージの完全性保持や暗号化について説明した解答が多く見られました。また，秘密鍵に関して，「証明書を暗号化する」のようにディジタル署名に関する誤った説明が見られました。TLSクライアント署名は，TLSメッセージを署名対象データとして，クライアント秘密鍵を用いて計算されます。証明書は公開情報なので，暗号化する必要はありません。また，暗号化鍵の交換ではクライアントの鍵ペアは使用されません。

(4)「有効期限が過ぎた証明書を失効」は，有効期間が過ぎた証明書の失効は不要です。失効手続は，有効期間中の証明書に対して行います。また，「退職時の失効手続」など，有効期間の長さや業務の継続性と直接関連しないものは不正解としました。

(5) プライベートCAを導入してサーバ証明書を用いる場合には，そのサーバ証明書を検証するためのルート証明書を端末に事前に導入する必要があることを押さえておきましょう。

問2 情報共有システムの構築

【採点基準】

［設問1］

(1) 解答例のように，TCPのフロー制御機能がない場合に受信側のコンピュータで起こり得る事象を適切に説明したものを正解としました。

(2) 解答例のように，TCPの順序制御機能がない場合に受信側のコンピュータで起こり得る事象を適切に説明したものを正解としました。

(3) 解答例のように，エントリ生成後に表1のNAT方式のいずれの場合にも通信ができないアプリケーションの仕様を適切に説明したものを正解としました。

(4) 解答例と同じ主旨だけを正解としました。

(5) 解答例だけを正解としました。

［設問2］

(1) 解答例だけを正解としました。

(2) 解答例のように，図3の応答電文を踏まえて適切に説明できているものを正解としました。

(3) 解答例のように，サーバに関して確認できることを説明しているものを正解としました。

(4) 解答例のように，新設する中継サーバに関して，

RP サーバのバックエンドに配置するメリットを適切に説明しているものを正解としました。

［設問3］

(1) 解答例と同じ主旨だけを正解としました。

(2) 解答例だけを正解としました。

(3) 解答例だけを正解としました。

(4) 解答例だけを正解としました。

［設問4］

(1) キで「認証失敗」は部分点としました。その他は，原則的に解答例だけを正解としました。

(2) 解答例と同じ主旨のみを正解としました。

(3) 解答例と同じ主旨だけを正解としました。WebSocket が HTTP ベースであることに着目したものは，内容によって部分点としました。

【講評】

［設問1］

(1) TCP のフロー制御は解説のとおりですが，フロー制御ではなく，TCP の再送制御に関する事象を説明した解答が見られました。午後 I 問 1 設問 2(2)の講評でも触れましたが，フロー制御や次の順序制御と IP フラグメントを混同している解答が見られました。パケットの断片化と組立ては IP の機能です。

(2)「受信するパケットの順序が入れ替わる」は，解釈の違いかもしれませんが，受信を到着ととらえると，順序制御の有無に関係なく発生します。受信したパケットに対する，その後の並替えができるかどうかがポイントです。

(3) FTP や SIP の NAT 越え問題は過去問題でも出題されていましたが，正答率は低かったです。下線(c)には「エントリ生成後」という条件が示されています。「通信途中でポート番号が変化する」という解答がありましたが，ポート番号が変わった場合には，新しいエントリが追加されるので，NAT 越えの問題は発生しません。

(4) 表 1 の NAT 方式を適切に理解した解答が多く，正答率は高かったです。単に表 1 のフルコーン NAT の機能を整理しただけで，他の方式との比較をしていないものは，内容によって部分点又は不正解としました。単に「内部からの通信のない外部ホストからの通信を許可する」は，制限付きコーン NAT 方式でもあり得るので部分点としました。

(5) 正答率は想定よりも低かったです。本文の「許可した通信に対する応答だけを許可する」機能は，通常のステートフルパケットフィルタリングと同様の機能です。

［設問2］

(1) WebSocket は平成 28 年の本試験に出題されているためか，「Upgrade」の正答率は高かったです。

(2) 正答率は低かったです。空欄ウの前の本文に「図 3 の応答電文に関して」とあるので，図 3 の電文をベースに考察することを期待しました。「受入可能なプロトコルが 0」という解答がありました。本文の記述に基づいて解答を作成されたと思います。「1 個，あるいは 0 個」というのは，応答電文における Sec-WebSocket-Protocol ヘッダの数の意味です。やや紛らわしかったと思います。図 3 の応答電文は Sec-WebSocket-Protocol ヘッダが 0 個の例です。

(3) メッセージの完全性に着眼した解答がありましたが，設問ではサーバに関する確認事項が問われているので不正解としました。また，「サーバの真正性」のようにサーバ認証に着眼した解答がありましたが，確認できることは，あくまでクライアントが接続したサーバであることまでですので，内容によって正解あるいは部分点としました。

(4) 性能上のメリットに関して，RP サーバのキャシュ機能に着眼したものがありましたが，本文中には，情報共有システムにおけるキャッシュ利用に関する記述がないので，内容により部分点又は不正解としました。

［設問3］

(1) 中継サーバの前に RP サーバがあることを指摘した解答がありました。設問文では「中継サーバに向かう通信」と述べていることから，RP サーバへの通信の許可も不要である理由を期待しました。

(2) リダイレクト先を指定する Location ヘッダを押さえておきましょう。

(3) 正答率は低かったです。NW 試験では出題実績のない領域ですが，この問題をとおして認証連携について学習しておきましょう。SAML は異なるドメイン間で認証情報などを連携させますが，Cookie は異なるドメイン間では転送されません。

(4)「CONNECT」がありましたが、CONNECT はプロキシサーバに中継を依頼するメソッドです。

［設問4］

(1) 空欄クで「トンネル」は，続く下線（h）の確立に該当するので不正解としました。

(2) リバースプロキシサーバを用いるシステムでは，クライアントから見るとリーバスプロキシが Web サーバになることを確認しておきましょう。

(3) 正答率は低かったです。プロキシサーバにおけるトンネリングの基本知識からの考察も可能です。

以上