

■ 全体講評

1. 午前試験について

午前試験が模試の合格点に届いていない場合は、学習計画を見直して本試験に備えましょう。直前ですので、午前Ⅰは AP（応用情報）の過去問題を、午前Ⅱは 1～8 回前の NW 試験の午前Ⅱの過去問題を集中的に確認してください。セキュリティ分野は SC 試験の午前Ⅱからの再出題もあります。

2. 午後試験について

日々、ネットワーク技術者として実務に取り組んでいるか、学習を積み重ねたことが伝わる答案から、基本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。

途中であきらめてしまったと思われる答案がある一方で、多くの答案は最後まで解答を書き上げて得点を重ねています。難しい設問も含まれますが、「落ち着いて考えれば得点できた」といった設問もあると思います。本試験では時間いっぱい粘り強く考え抜くことが大切です。

時間不足の場合や、逆に時間が余って得点不足になった場合には、時間管理を修正しましょう。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、急ぎ過ぎて起こるケアレスミスをなくすことが得点アップにつながります。

得点力アップ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、本試験で繰り返し出題されている基本技術です。今回の公開模試の問題では、LAG、TCP の通信制御、代表的なトンネリングプロトコル、DNS の資源レコード、ルータの機能、VRRP、ポートミラーリング、TLS におけるサーバ証明書及びクライアント証明書の役割などです。重点技術の理解の差は得点に影響します。参考書による学習に加えて、過去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

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「理由」を解答したり、「接続動作の特徴」が問われているのに「データ通信の特徴」を解答したりする、ずれた解答が見られます。

また、設問文に「〇〇に着目して」や「〇〇の観点を除いて」などとあるのを考慮せず、要求を満たさない解

答があります。設問文や下線部、さらに下線や空欄の前後を正しく読まないと、いくら考察しても正解に到達しません。

② 解答文は掘り下げて説明するスタンスでまとめる

設問文や本文のキーワードを引用することはよくありますが、本文の記述の単純な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は、過去問題を演習して、IPA の解答例をよく吟味しましょう。

【問題選択について】

選択問題を○で囲っていない答案があります。午後Ⅰの間 2 と間 3 を逆に記入したものや、午後Ⅱの記入なしがありました。本試験では注意してください。

【部分点の配点について】

部分点は、基本的には配点の半分の点数ですが、解答の内容に応じて調整しています。

< 午後Ⅰ >

問1 ネットワークの冗長化

【採点基準】

【設問1】

ア～カ：解答例だけを正解としました。

キ：“ボンディング”も正解としました。

【設問2】

(1) 解答例のように、LAG の負荷分散アルゴリズムと一つの TCP コネクションの性質を組み合わせで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で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、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 を設定する必要がある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 と解答した上で理由を「ポートが特定になる」としたものは、原則として理由を部分点

としました。

【講評】

【設問1】

全体として正答率は高かったです。(カ)で“VM”は仮想PCを指します。“仮想化基盤”は空欄の前の記述と同様の表現で、他の仮想化方式を包含する表現なので不正解としました。“コンテナ”は仮想化機構を動作させるためのOSが必要です。また、“VMware”や“Hyper-V”などの固有の名称は、本文に記述がない限り使わずに一般名称で答えます。

【設問2】

- (1) 正答率は高かったです。設問文で「TCP接続の性質に着目して」と指示された場合には、TCP接続の性質がどのような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の内容から、接続を識別するIPアドレスとポート番号を軸に説明します。単に“TCP接続を確立しているから”は、どのような性質に着目しているかが説明不足です。
- (2) 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”とする解答などは、内容に応じて部分点あるいは不正解としました。“組み立てられない”は、順序制御によって組み立てられるので、不正解です。
- (3) 正答率は高めでした。下線③の前の記述から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。スイッチのポートとヘッダ情報のポート番号の混同も散見されました。MACアドレステーブルは重要な基本ですので、よく確認しておきましょう。

【設問3】

- (1) 補足します。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アドレスで、送信元IPアドレスと送信元MACアドレスは1対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。また、本文に「仮想PCをTCと1対1で生成」とあるので、“通信先のTCによって宛先IPアドレスが異なる”は正確ではありません。
- (2) 正答率は低かったです。RDP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、性能の観点から往路と復路のどちらがより留意すべきかを吟味する問題でした。また、理由として往路と復路の通信量の違いを指摘した解答がありましたが、これはトラフィックが偏る理由ではありません。

問2 仮想デスクトップ環境の構築とネットワークの見直し

【採点基準】

【設問1】

- (1) ア、イ：解答例だけを正解としました。
ウ：“IPsecパススルー”、“PPTPパススルー”は部分点としました。
- (2) 利点：解答例と同じ主旨だけを正解としました。単に“一元管理できる”のような内容は部分点としました。
懸念点：解答例と同じ主旨だけを正解としました。同じ帯域不足の観点について、場所を細かく分けて二つ挙げたようなものは、合わせて一つ分の得点(6点)にしたものがあります。

【設問2】

- (1) 解答例だけを正解としました。
- (2) エ：解答例だけを正解としました。
オ：解答例と同じ主旨だけを正解としました。“東京本社の複合機”と“ファイルサーバ”という接続元と接続先を具体的に述べていないものは不正解としました。また、“ファイルサーバから複合機への接続”と明記したために、接続の方向が逆に表現されているものは不正解としました。

【設問3】

- (1) 解答例のように、“拠点間の通信”を含めているものを正解としました。単に、“テレビ会議システムを導入するから”という解答は部分点としました。
- (2) カ、キ：解答例だけを正解としました。

【講評】

【設問1】

- (1) (ウ)について、“NATトラバーサル”はIPsecクライアントに実装される仕組みで、この問題の構成においてはノートPCの機能になります。問題文では、「ネットワークの上位ルータが対応している」と記述されているので、“VPNパススルー”が入ります。
- (2) 利点について、問題文に従来の管理負荷に関する課題が記述されているので、一元管理による効果まで具体的に答えることができます。また、社内の通信に着目した解答がありましたが、社外のWeb閲覧のためのインターネット通信に着目して考察したい

です。

さらに、懸念として、データセンタ内部のネットワークの帯域不足に着眼したのも見られました。明らかな誤りではありませんが、帯域不足の観点としては、LAN 回線よりも WAN 回線の方の懸念が大きいという考え方は、過去問題でも出題されています。下線①では、インターネット通信を対象にしていますので、より直接的なアクセス回線を取り上げるのが妥当です。

“アクセスが集中する”は、下線①の「全てデータセンタを経由」を言い換えただけでも読めます。懸念として、想定される問題点（帯域不足）まで表現したいです。

セキュリティに関する観点は設問文で除外されています。他に、広域イーサネットの帯域に着目した解答もありましたが、問題文に帯域不足はないと記述されています。

【設問2】

- (1) “スタティックルーティング”や“ダイナミックルーティング”、“ソースルーティング”などの解答がありました。スタティックルーティングとダイナミックルーティングは、いずれも宛先 IP アドレスを基にする通常のルーティング方式で、それを静的（固定）に指定するか、動的に制御するかの違いです。ソースルーティングは、送信元で中継する経路を指定するルーティング方式です。

- (2) (エ) 正答率は高めです。勘違いした方はよく確認しておきましょう。

(オ) “応答用ルーティング”と正確に解答したものは少数でした。L3SW におけるルーティング設定では、通常は、要求の通信と応答の通信をそれぞれ設定する必要があります。ファイアウォールにおけるステートフルインスペクション方式（ダイナミックフィルタリング方式）のフィルタリングルールの設定とは異なることを押さえておきましょう。また、“東京本社の複合機”のように限定せずに、単に、“東京本社”などとする解答があります。必要最小の通信に限定するという問題文の記述の観点を踏まえて、正確に解答をまとめたいです。

【設問3】

- (1) ネットワーク設計の観点から、“拠点間の直接の通信”を含めたいです。
- (2) ケアレスミスが多いと思われますが、差がついています。解説をよく確認しておきましょう。

問3 セキュリティ機能の強化

【採点基準】

【設問1】

ア～エ：解答例だけを正解としました。

【設問2】

- (1) 解答例のように、アプライアンス型の場合に必要なとなる、UTM 製品を自社で導入・運用管理する作業をアウトソースできるメリットを答えたものを正解としました。
- (2) 解答例のように、インターネット接続回線の冗長構成を答えたものを正解としました。

【設問3】

- (1) 解答例だけを正解としました。
- (2) 解答例のように、インターネット接続回線の冗長構成を適切に答えたものを正解としました。
- (3) 解答例だけを正解としました。
- (4) 解答例のように、アクセスログに記録する IPv6 アドレスについて適切に答えたものを正解としました。

【設問4】

変更した内容：解答例のように、接続元を WAF サービスに制限する変更を適切に答えたものを正解としました。

追加した内容：DB サーバへの通信許可を適切に答えたものを正解としました。

【講評】

【設問1】

(ア) について、“(Web) アプリケーションファイアウォール”は、WAF に関する記述にもあるように、Web サーバへの攻撃に対する対策機能です。空欄アは、外部への Web アクセスを制御する機能です。(イ) の正答率は高く、(ウ) は低かったです。

(エ) について、処理(3)の実現のために必要な個別の設定は、利用者の TLS クライアントに対して、Web サーバの代わりに、WAF サービスが TLS サーバとして動作するための Web サーバの秘密鍵です。また、“クライアント証明書”という解答について、Web サーバが WAF サービスを TLS クライアント認証するとは記述されていません。さらに、“ルート証明書”という解答について、Web サーバのサーバ証明書はパブリック証明書と考えられますので、WAF サービスが保持しています。ほかに、“公開鍵”という解答について、公開鍵はサーバ証明書に格納されています。

【設問2】

- (1) WAF に関する本文の記述の「導入や運用管理面」に着目するのが確実です。単に、“ネットワーク構

成の変更がない”は自明なことなので、メリットをもう一段具体的に説明したいです。

- (2) “UTM2 台構成”と限定した解答は、マルチホーミング構成は2台に限った構成ではないので部分点としました。

[設問3]

- (1) “利用者端末と Web サーバの間”などがありました。設問文で「最も適切な設置場所」と問われていますので、絞り込みを検討したいです。
- (2) A プロジェクトへの影響について、“インストール時に作業中断”など、限定し過ぎの解答は内容によって部分点としました。
- (3) A レコードを答えたものが多くありました。M 社の DNS サーバに設定するリソースレコードは、M 社ドメインの `www.m-sha.co.jp.` に対する正式名を回答するための CNAME レコードです。正式名の `www.m-sha.safe.p-sha.co.jp.` の A レコードを管理するのは、IP アドレスを変更する WAF サービスです。また、設定作業を文章で説明した解答がありましたが、「リソースレコードの内容を具体的に答えよ」なのでレコードを解答するのが妥当です。なお、FQDN のルートのドット表記のないものは部分点としました。実装ではトップレベルドメインまで指定すれば FQDN を意味する場合がありますが、本試験ではドットまで明記するようにしてください。
- (4) “WAF サービスのクライアント証明書の設定”は、通常の TLS 通信でも、クライアント証明書をサーバに設定する必要はありません。“サーバ証明書の設定”も Web サーバにおける設定変更なので該当しません。

[設問4]

変更した内容について、単に“許可する接続元”のように、変更した項目だけの解答があります。問われているのは「変更内容」なので、どのように変更したかを説明する必要があります。

追加した内容について、“インターネットから DB サーバへの通信を拒否”などがあります。拒否することは必要ですが、この設定だけでは不十分です。必要最小の通信だけを許可する設定として表現します。

<午後Ⅱ>

問1 IPv4 と IPv6 の共存環境

【採点基準】

[設問1]

a～j：解答例だけを正解としました。

[設問2]

- (1) 解答例のように、IP アドレスの重複が、ルータの

ルーティング機能に影響することを適切に答えたものを正解としました。

- (2) 解答例のように、IPv4 通信と IPv6 通信をプロキシサーバがプロトコル変換する動作を答えたものを正解としました。

[設問3]

- (1) 解答例のように、ローカルプリファレンス値については ISP 方向への通信経路、AS-PATH 値については Web 販売システム方向への通信経路について、いずれも回線 A を優先させる目的を適切に答えたものを正解としました。
- (2) 解答例のように、経路のループについて適切に答えたものを正解としました。
- (3) 解答例のように、機器名として“FW1”，機器の役割として“マスターータ”を含めて適切に答えたものを正解としました。
- (4) ア、イ：解答例だけを正解としました。

[設問4]

- (1) 解答例のように、パケットの構造に関するオーバーヘッドの問題を適切に答えたものを正解としました。
- (2) 解答例のように、XFF ヘッダの IPv6 アドレスの記録について適切に答えたものを正解としました。
- (3) 解答例のように、DNS サーバへのアクセスが IPv4 通信になる理由を適切に答えたものを正解としました。
- (4) 解答例の他に、“二つの IP アドレスが設定される”を正解としました。
- (5) 正引きレコード、逆引きレコードともに、解答例だけを正解としました。
- (6) 解答例のように、FW の IPS 機能と LB の WAF 機能の IPv6 対応を適切に答えたものを正解としました。

[設問5]

解答例のように、監視機能の IPv6 対応を適切に答えたものを正解としました。

【講評】

[設問1]

(e) に関して、“NA (Neighbor Advertisement)”は、アドレス解決や重複アドレスの検出など、IPv4 における ARP に相当する機能を提供します。

[設問2]

- (1) 単に“IP アドレスの重複可能性”という事象を答えたものは不正解としました。「〇〇に着目して」と問われた場合には、どのように着目したか、つまり、どの機能に着目したかを含めて解答したいです。

(2) 単に“通信を中継する”というプロキシサーバの一般的な動作を説明したものは、部分点あるいは不正解としました。ゲートウェイの重要な機能であるプロトコル変換を軸にまとめたいです。また、「通信区間に着目し」や「動作を例に挙げて」という設問文の要求事項に答えていない解答も目立ちました。他に、“IP アドレスを変換”は、変換するのは IP アドレスだけではないので、正確性にも留意してまとめたいです。

[設問3]

- (1) 単に“通信経路を決定するため”のようなざっくりとした解答があります。下線③の属性値ごとの設定内容を踏まえて、それぞれの目的の違いを含めて説明したいです。また、下線③の内容をそのまま復唱したような解答も見られました。設問で問われている目的としてまとめたいです。
- (2) 正答率が高かったです。
- (3) FW1 を答えていても、役割のないものが多くありました。“マスターータに設定するため”は、VRRP 自体の機能です。
- (4) ケアレスミスが多いと思われるが、差が付く問題になっています。経路を答える問題は、確実に得点したいです。

[設問4]

- (1) “フラグメントの発生”という解答について、サービスを提供する ISP では、トンネルインタフェースの MTU は、トンネルのオーバーヘッドを考慮して設定され、利用者には通常より小さい MTU が通知されるのでフラグメントは発生しません。また、“通信できない”ことはありません。下線⑥の前にも「利用できる」と記述されています。
- (2) Web サーバ側での動作検証が問われていますが、LB に関する検証が見られました。
- (3) “AAAA レコードを登録すればよいから”という主旨の解答は、設問文の「DNS サーバでは IPv6 アドレス用のレコードを追加すればよく」の部分を具体化して言い換えたものなので不正解としました。登録する前提で、当面は必要のない理由を一段掘り下げて説明したいです。
- (4) “二つの IP アドレスが設定される”について補足します。2 台ルータのプレフィックスが異なる場合には、それぞれのプレフィックスの IP アドレスが設定されます。ただし、プレフィックスが同じ場合には、IP アドレスは一つになります。

また、“ホストの IP アドレスが変更される”ことはありません。さらに、“セグメント内で他のホストと IP アドレスが重複する”は、ルータの台数に

関わらず、IPv4 における GARP を用いる重複チェックと同様に、IPv6 でも NDP の Neighbor Solicitation メッセージを用いる重複チェックが行われます。

(5) FQDN のルートのドット表記のないものは部分点としました。(午後 I 問 3 設問 3(3)の講評参照)

(6) “不正な RA の検知”などがありましたが、本文の記述を優先させます。

[設問5]

単に“IPv6 対応”だけのものや、逆に、追加する機能を答えているものの、IPv6 対応の言及がないものは不正解としました。

問2 IoT ネットワークの設計と構築

【採点基準】

[設問1]

ア～カ：解答例だけを正解としました。(エ)について、“プラチナバンド”は部分点としました。

[設問2]

- (1) 解答例のように、データを分割することを答えたものを正解としました。
- (2) ～ (4) 解答例だけを正解としました。
- (5) 解答例のように、屋外における通信の制限を説明したものを正解とし、「屋外」を指摘していないものは不正解としました。

[設問3]

- (1) 解答例のように、デバイスが多数であること、小容量データ通信であること、あるいは、間欠的な通信を行うことなど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、PoE の給電距離の制限について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、WLC のポート 1/2 と PE のポート A、PE のポート B と AP3/4、WLC のポート 3/4 と AP1/2 を接続したものを正解としました。

[設問4]

- (1) 解答例のように、ポート番号を含めて A 社の FW を通過させる目的を適切に説明したものを正解としました。
- (2) 解答例だけを正解としました。
- (3) 解答例のように、ProtocolNameList に着目するなど、ClientHello メッセージで通知することを具体的に説明したものを正解としました。
- (4) 解答例の他に、“エッジサーバの証明書”を正解としました。

[設問5]

- (1) 解答例だけを正解としました。

- (2) 解答例のように、設定内容（ミラーリング）、及びモニターポート、ミラーポートを具体的に説明したものを正解としました。説明不足なものは、内容によって部分点あるいは不正解としました。
- (3) 解答例のように、宛先/送信元 IP アドレスに着目したものの他に、TCP や MQTT というプロトコルに着目した適切な内容を正解としました。
- (4) 解答例のように、パケットについて発生している現象を適切に答えたものを正解としました。
- (5) 解答例のように、A システムの特殊な使い方を含めて、認証手続という処理性能に影響する接続動作の特徴を適切に説明したものを正解としました。接続動作に言及せずに、データ転送だけを答えたものは内容によって部分点あるいは不正解としました。
- (6) データ項目：解答例のように、センシングの時刻情報を正解としました。

伝送の仕様：解答例のように、データ送信のタイミングを分散させることを答えたものを正解としました。

【講評】

【設問1】

正答率は、ア（BLE）、イ（LTE）、ウ（省電力）の考察問題は高く、エ（サブギガ）、オ（Wi-SUN）、カ（LPWA）の用語問題は低かったです。IoT ネットワークの用語を確認しておきましょう。

【設問2】

- (1) 正答率は高かったです。
- (2) ～ (4) 計算問題で、正答率は低かったです。計算のケアレスミスと思われるものもありました。計算問題は少ないですので、時間をとって確実に解答したいです。また、このような問題を活用して、無線通信の特徴やポイントを整理するとよいでしょう。
- (5) 採点基準のとおり、「屋外」に言及できているかどうかで差がつかしました。“W56（5.6GHz 帯）だけが利用できる”については、W56 は制限なく屋外利用が可能ですが、この問題では表 2 の備考の記述から W52 と W53 について考察します。

【設問3】

- (1) 正答率は高めでした。設問では、「デバイス数」と「データ通信の特性」の二つを考慮することを求めています。どちらか一方だけのものがありました。
- (2) 設問は給電の距離の制限に関するものですので、データ通信について説明し、給電について述べていないものは部分点としました。
- (3) 正答率は高めでした。本文の記述を正確に読みとれています。間違っただ方は確認しておきましょう。

【設問4】

- (1) 設問では、目的が問われていますので、解答例のようなまとめ方が適切です。“ポート 8883 は通らないから”は、目的ではなく理由を答えています。
- (2) 正答率は高かったです。
- (3) “ハンドシェイクメッセージが平文だから”という主旨だけを答えたものは、設問文に「内容に着目して」とあることから不正解としました。

本試験で未出題の新しい技術に関する問題でしたが、未解答を除くと正答率は高かったです。新しい技術領域が出題された場合には、本文で説明されます。本文の記述をよく読めば解答できる設問も多いので、本試験では粘り強く解答することが大切です。

- (4) “サーバ証明書”があります。特に、IoT ネットワークにおける TLS 通信では、TLS クライアントと TLS サーバを的確に押さえ、さらに、認証について、サーバ認証とクライアント認証のどちらの認証について論じているかを意識することが大切です。この問題で問われている通信においては、下線⑤の前に「クライアントのなりすましを防止する」などあるように、エッジサーバは TLS クライアントです。

また、“クライアント証明書の公開鍵”と公開鍵に限定した解答は不正解としました。TLS クライアント認証に必要な情報は、より正確にはクライアント証明書及びクライアント秘密鍵ですので、公開鍵に限定してしまうと、認証に必要な秘密鍵が漏れてしまいます。

さらに、“認証情報”だけでは曖昧なので不正解としました。

【設問5】

- (1) ブロードキャストアドレスを具体的に表記した“FF-FF-FF-FF-FF-FF”は部分点としました。MAC アドレスの“種類”が問われた場合には、特定のアドレスではなく種類で答えます。類題として IP アドレスの“種類”などが問われた場合も同様です。
- (2) “プロミスキャスモードの設定”を含めた解答がありますが、これは L2SW における設定ではなく、調査用ノート PC の NIC に対する設定です。
- (3) 未解答を除くと、正答率は高かったです。一方で、図 7 のフィルタ設定後の解析結果と一部が整合しなくなってしまうケアレスミスもありました。
- (4) 設問で問われている IP パケットに多発している事象として表現できていないものがありました。例えば、“通信できない”と表現すると、事象が曖昧です。
- (5) 設問で問われている「接続動作の特徴」ではなく、

その後の「データ通信の特徴」を答えたものも多くありました。設問文を正確に読むことが重要です。

(6) データ項目について，“データ転送時刻情報”が見られました。記録する必要がある時刻情報は，規定時刻である“センシングの時刻情報”です。問題文の記述内容から，センシングは規定時刻どおりに実行し，データ伝送を分散させることによって通信遅延の問題を解決しつつ，サービスの要求を満たすデータ蓄積を実現しようとしていることが読み取れます。

以上

itec