

■ 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、学習スケジュールを立て直して本試験に備えましょう。試験直前ですので、午前Ⅰ試験については応用情報技術者試験（AP）の過去問題を、午前Ⅱ試験については1～6回前の午前Ⅱの過去問題を集中的に確認してください。

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。

また、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るのが印象的でした。本文や図表中にヒントがある設問もありますので、本試験では時間一杯粘り強く考え抜くことが大切です。

時間不足や逆に時間が余って得点不足になった場合には、時間管理を見直しましょう。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、急ぎ過ぎて本文や設問文を読み落とす、あるいは読み違え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技術で、NW 試験向けの参考書で説明されている内容です。今回の公開模試の問題では、TCP, DNS, IPsec, VLAN, HTTPS 通信及びサーバ証明書の検証などです。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、過去の午後Ⅰ／Ⅱの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

「理由」が問われているのに「目的」を解答したり、「情報」が問われているのに「理由」を解答したりする、設問とずれた解答が見られます。

また、設問文に「〇〇に関して」や「〇〇の観点を除いて」などとあるのを考慮せず、要求事項を充足し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、いくら考察しても正解として完成しません。

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。特に、午後Ⅰで後から2問目を選択する場合に2問目の○付けを忘れがちです。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。

【正誤表について】

午後1問2の答案用紙に間違いがあり、戸惑った方も多いと思います。申し訳ありませんでした。

<午後Ⅰ>

問1 HTTP/3の調査

【採点基準】

【設問1】

- (1) a, b: 解答例だけを正解としました。
c, d: 「NAPT」「IP マスカレード」なども正解としました。
- (2) 解答例のように、QUIC 向けに UDP を許可する旨を述べたものを正解としました。変更内容が曖昧なものは、部分点あるいは不正解としました。
- (3) 解答例のように、経路の違いや再送処理に着目したものを正解としました。その他に、到着が逆転し得る場合を指摘したものは、内容によって正解あるいは部分点としました。

【設問2】

- (1) 解答例だけを正解としました。
- (2) 解答例だけを正解としました。

【設問3】

- (1) 解答例のうち、最低限「送信元 IP アドレス」と「送信元ポート番号」を述べ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。「リフレクション攻撃」や「DoS 攻撃」は部分点としました。

【設問4】

- (1) 解答例のように、共有 DB を用いるセッション維

持に着目したものを正解としました。

- (2) 解答例のように、プロトコル変換機能を述べたものを正解としました。

【講評】

【設問1】

- (1) c, d について、「ARP」「ルーティング」「MAC アドレス」などの解答がありました。利用者側のネットワーク機器においては該当する可能性がありますが、F 社サイト側の FW やロードバランサには該当しません。
- (2) 設問では、変更内容が問われていますが、「ポートを変更する」のように、単に「変更する項目」を解答したものがありません。「変更内容」が問われた場合には、どのように変更するかを述べてください。
- (3) 設問では、どのような場合に順序が逆転するかが問われていますが、「後のパケットが先に到着」では逆転を言い換えただけで説明不足です。どのような場合に、この事象が発生するかを述べたいです。

【設問2】

- (1) e: 「CONNECT」の間違ひが多くありました。HTTP の CONNECT メソッドは、通常はプロキシサーバに対して宛先サーバとのトンネリングを要求するために、TCP コネクションの確立後に用いられます。
- f, g: 正答率は低かったです。TLS1.3 を組み入れた QUIC の効率の高いメッセージングや RTT の考え方を確認しておきましょう。
- (2) 正答率は低かったです。

【設問3】

- (1) IP アドレスだけの解答がありましたが、TCP コネクションを識別できません。基本的な内容ですので、確認しておきましょう。また、シーケンス番号だけを解答したものがありませんが、IP アドレスだけでなく TCP コネクションを識別できません。
- (2) 「UDP フラッド攻撃」という解答がありました。チャレンジレスポンス認証のやり取りを悪用しない点や、対策としては最大サイズを規定することが有効なので、下線⑤の対策とは整合せず、不正解としました。

【設問4】

- (1) 正答率は高かったです。
- (2) 正答率は低かったです。「Cookie による振り分け機能」や「スティッキーセッション機能」、「L7 ロードバランシング機能」など、表 1 で既に対応している機能をそのまま挙げた解答がありました。解答がすぐには思い浮かばない問題だと思います。その

ような場合には本文を確認し、下線⑦の前の「Web サーバの HTTP/3 対応は前提としない」の記述に着目すると、正解に近づくことが期待できます。

問2 Web システムの構成変更

【採点基準】

【設問1】

- (1) 解答例だけを正解としました。
- (2) 解答例だけを正解としました。配点表は“完答”となっていますが、一方のルールが正解の場合には部分点としました。

【設問2】

- (1) 解答例のように、ターンアラウンドタイムの改善などの性能観点の利点を正解としました。ほかに、運用保守管理の負荷低減など、B 社にとっての利点を適切に述べたものも正解としました。
- (2) 解答例だけを正解としました。
- (3) 解答例のように、DNS クライアント（利用者）とフルサービスリゾルバ（名前解決の問合せ元）がネットワーク的に離れている点を適切に述べたものを正解としました。
- (4) 解答例のように、DNS クライアント（利用者）のサブネット情報（IP アドレス情報）を述べたものを正解としました。
- (5) 解答例のように、エッジサーバの IP アドレスだけを送信元として許可することを述べたものを正解としました。

【設問3】

時間：解答例だけを正解としました。

対策：解答例のように、リソースレコードの TTL の値を短くすることを述べたものを正解としました。配点表は“完答”となっていますが、一方が正解の場合には部分点としました。

【講評】

【設問1】

- (1) a, b: DNS レコードのタイプは、最近の本試験でも出題されています。よく整理しておきたいです。
- d, e: やや難しかったと思いますが、今後の本試験に向けて確認しておきましょう。
- f: 正答率は高かったです。「LB の IP アドレス」という解答がありました。XFF を用いる目的や、解説で補足している、CDN サービス導入後の XFF ヘッダの情報の取扱い方などを確認しておきましょう。
- (2) 通常のゾーン転送は TCP 通信であることと、アクセスは C 社セカンダリサーバ（スレーブサーバ）か

らプライマリサーバ（マスタサーバ）であることを確認しておきましょう。一方、DNS NOTIFY は本文のとおり、プライマリサーバから C 社セカンダリサーバに送信されます。

また、「163.x.y.11」を挙げたものがありました。既存のセカンダリ DNS サーバは、プライマリ DNS サーバと同一セグメントにあり、ルールの追加は不要です。

[設問2]

(1) 「オリジンサーバへの接続元を制限できる」のようなセキュリティの観点、「障害時に迅速にリカバリできる」や「障害時にサービスを継続できる」のような可用性の観点の解答がありました。設問文をよく読み、ケアレスミスをなくしたいです。

(2) CNAME レコードも最近出題されていますので、整理しておきましょう。「CN」という解答がありましたが、CN ではなく CNAME です。

(3) エッジサーバの選択は、DNS クエリの送信元 IP アドレスに基づきます。そのために問題が発生し得ることを確認しておきましょう。

設問では、利用者の環境を問うていますが、エッジサーバやオリジンサーバの環境だけを述べて、結果的に説明不足の解答がありました。

また、「インターネット接続時にプロキシサーバ経由」のような解答がありました。この表現だと、Web アクセス時にプロキシサーバを経由するように読めます。仮に DNS プロキシを述べようとするのであれば、明記するのが確実ですし、フルサービスリゾルバ（キャッシュ DNS サーバ）と表現する方が明解です。

(4) 「選択されたエッジサーバの IP アドレス」や「TTL」など、リソースレコードに含まれる情報が多くありました。設問文では、「リソースレコードと一緒に保持」と問うており、EDNS-Client-Subnet の機能を有効に利用するという目的を押さえて考察します。

(5) 正答率は高かったです。NAT の設定などを述べた解答がありましたが、FW に設定しているアクセス制御の設定変更ですので、表 1 のルール変更と考えます。

[設問3]

対策について、「リトライ時間を短くする」や「NOTIFY メッセージを送信する」など、ゾーン転送に着目した解答がありました。ゾーン転送では、セカンダリ DNS サーバが保持するリソースレコードを更新するだけで、フルサービスリゾルバや利用者のキャッシュの更新には影響しません。

「DNS サーバのキャッシュをクリアする」という解

答がありましたが、B 社からフルサービスリゾルバのキャッシュをクリアすることはできません。DNS クライアントやフルサービスリゾルバがリソースレコードをキャッシュ済みの場合、障害発生後の対応では問題を解決できません。そのため、さらなる修正としては、あらかじめ TTL を短縮することが有効です。

また、「エッジサーバ宛の通信をリダイレクト」は、サービス停止中にリダイレクトを応答できません。

答案用紙誤植のお詫び

問2 設問 1(1)の解答欄に g の解答欄が余分にあり、誠に申し訳ございませんでした。

今後、再発防止策を講じ、より一層、慎重に公開模試制作を行ってまいります。

問3 PC 環境の更改

【採点基準】

[設問1]

(1) ア：解答例だけを正解としました。

イ：解答例のほかに、「テンプレート」や「システムイメージ」など、仮想 PC のマスタの呼び方として適切なものを正解としました。

(2) リスクについて、解答例のように、端末を介してデータが漏えいするリスクを述べたものを正解としました。

理由について、解答例のように、端末にはデータとして保存されない点を述べたものを正解としました。

(3) 解答例のように、代替機を用いて、代替機自体の個別の設定を行わずにデスクトップ環境を復旧できる旨を述べたものを正解としました。

[設問2]

(1) 解答例だけを正解としました。

(2) 解答例だけを正解としました。

[設問3]

(1) 見直し案について、解答例のように、ファイルサーバを本社に統合することを述べたものを正解としました。

問題について、解答例のように、仮想 PC とファイルサーバ間の広域イーサネットを経由する通信を指摘したものを正解としました。

(2) 解答例のほかに、「無線 LAN ルータ」も正解としました。「無線」や「Wi-Fi」がなく、単に「アクセスポイント」とした解答は部分点としました。

【講評】

【設問1】

- (1) イの正答率は高かったです。
- (2) 正答率は高かったです。リスクについて、「不正アクセス」などの解答がありました。下線①の前の「VDI サーバ上の情報を表示するので」とのつながりを確認し、思いついた解答を吟味したいです。
その他に、「TC 端末の盗難リスク」という解答がありましたが、VDI サーバ上の情報を表示することと端末自体の盗難は関係なく、盗難リスクは回避できません。
- (3) 正答率は高かったです。設問では、「故障が発生した際の対応方法に着目して」と要求しています。このように「〇〇に着目して」とある場合には、どのように着目したかが分かるように表現します。そのため、単に「データがサーバにあるから」だけでは説明不足です。多くの解答は、代替機でデスクトップ環境をリカバリするという対応方法を含めて表現できていましたが、説明不足の解答がありました。

【設問2】

- (1) エの正答率は低かったです。IPsec に関して、鍵交換を含む折衝を行う IKE や、トンネルモード、トランスポートモードなどの基本的な用語は整理しておきたいです。
- (2) 正答率は低かったです。暗号化範囲について、「ESP ヘッダ」という解答がありました。IPsec に限らず、セキュアプロトコルのヘッダには、復号に必要な情報が格納されています。ESP ヘッダであれば、SA を特定する SPI です。そのため、セキュアプロトコルのヘッダは暗号化の範囲外です。
また、暗号化範囲について、「グローバル IP ヘッダ」という解答もありました。IPsec は、ネットワーク層（レイヤ 3）の暗号化メカニズムなので、ネットワーク層のアウトター（最も外側）のヘッダは暗号化の範囲外です。

【設問3】

- (1) 正答率は高かったです。
見直し案について、「拠点に VDI サーバ導入」という解答がありました。問題については正しく指摘しており、その問題を解決することができます。しかし、サーバの追加導入は、下線④の後ろの「この見直しによって、機器管理の効率化を図ることもできる」の記述に整合しません。正解を絞り込む条件は、下線の後ろに記述されていることもあります。
また、見直し案や問題について、本社内のルータや L3SW の負荷に着目したものがありません。下線④の「広域イーサ網のトラフィック量削減の観点」を踏ま

えて、広域イーサ網のトラフィック量についてストレートに述べるべきです。

- (2) 正答率は高かったです。「VPN ルータ」のようにテレワーク利用を想起したと思われる解答がありました。解説のとおり、「社内利用」に関して本文に記述があります。このように、本文の記述を踏まえて考察することにも留意したいです。

<午後Ⅱ>

問1 工場のネットワーク更新

【採点基準】

【設問1】

解答例のほかに、b について、規格名称の「MAC ブリッジ」も正解としました。g について、「GNSS」は部分点としました。

【設問2】

- (1) 解答例のように、情報系 NW から工場のネットワークへのマルウェア拡大を制限する効果を適切に述べたものを正解としました。セキュリティ上の効果の内容が曖昧で、単にネットワークを論理的に分離することを述べたものは部分点としました。
- (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。
- (5) 解答例だけを正解としました。
- (6) 解答例のように、「プライオリティ」あるいは「CoS ビット」を具体的に示して優先制御する動作を適切に述べたものを正解としました。単に「QoS に従って動作する」のように VLAN 機能に基づく動作の説明として曖昧なものは、内容によって部分点あるいは不正解としました。

【設問3】

- (1) 解答例のように、下線③のトークンの送信方法によって、一定時間以内に確実に送信機会が与えられる点を適切に述べたものを正解としました。「衝突が発生しない」のように、トークンの送信方法との関連が弱いものは、内容によって部分点あるいは不正解としました。
- (2) 解答例と同様の意味の機能を述べたものを正解としました。折り返しの表現が曖昧な「迂回する」などは、内容によって部分点あるいは不正解としました。

【設問4】

- (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。

【設問5】

- (1) 解答例のように、衝突（コリジョン）の発生を述

べたものを正解としました。

- (2) 解答例のように、「送信権」をもつノードだけが送信することを述べたものを正解としました。
- (3) 解答例のように、ネットワークの帯域に関わる課題である、遠隔監視や遠隔操作の通信を述べたものを正解としました。
- (4) 解答例だけを正解としました。
- (5) 解答例のように、NICにおける送出時刻を述べたものを正解としました。送出時刻ではなく、「差分の時間」を述べたものは、内容によって部分点あるいは不正解としました。

【講評】

【設問1】

- a：正答率は高かったです。
- d：「RJ-45」という解答がありました。RJ-45は、シリアルインタフェースの規格ではなく、コネクタの仕様の規格です。
- g：「NTP サーバ」や「stratum」は、PTPではなくNTPに関して使われる用語です。

【設問2】

- (1) 正答率は高かったです。一方で、採点基準で述べたように、セキュリティ上の効果として、説明不足なものがありました。また、セキュリティの観点であっても、本文に記述されている現在のA工場における課題に関わらない、一般的な効果を述べたものもありました。設問文の「A工場における」から、A工場の課題に着目したいです。
- (2) 正答率は全体の平均と同等でした。
- (3) 標準のイーサネットフレームの最大データ長(MTU)が1,500バイトであることを押さえておきましょう。
- (4) ア、イ：正答率は高かったです。アで「MC2」だけの解答はケアレスミスです。
ウ、エ：正答率は低かったです。解答に必要な情報は、本文と図2で示されているので、確実に得点したいです。
- (5) 正答率はやや低かったです。本試験では、あわずに時間をかけて確実に得点したいです。
- (6) 正答率は高かったです。設問では、L2SW及びL3SWの動作が問われていますが、スイッチの動作ではなく、設定や仕組みを述べた解答がありました。設問の主旨に沿って解答をまとめましょう。

【設問3】

- (1) 採点基準でも述べたように、「衝突が発生しない」ことも時間制約を充足するための条件の一つです。しかし、下線③の記述を踏まえて、1通信周期が一

定時間であることが、時間制約の充足のためにどのように有効になるかを考えると、設問の主旨に整合します。

- (2) 的確に表現した解答は少なかったですが、本文や図を参考にして、妥当性のある機能を導いたと思われる説明もありました。考えることで得点できる問題もあります。

【設問4】

- (1) 「タイムスロット時間幅」などの通信仕様を合わせることは確かに必要ですが、「正確なある情報を共有する」には整合しないので不正解としました。
- (2) 待ち時間の考え方は、本文のほかに、図4の注記を参考にすると把握しやすかったと思います。

【設問5】

- (1) 正答率は高かったです。
- (2) 正答率は高かったです。
- (3) 「メンテナンスデータ」に着目した解答がありました。これは、相互接続性に関する課題として記述されています。帯域の増加に関連する課題を拾います。
- (4) 「20 ミリ」や「200 ミリ」など、ケアレスミスと思われる解答がありました。
- (5) 「高精度」を述べた解答がありました。設問文の内容から、単に高精度という観点ではなく、プロトコルスタックの各層の処理のオーバーヘッドをどのように補正するかを考えることを期待しました。また、「遅延時間(差分)」という解答もありました。実際には、時刻なので、内容によって部分点としました。

問2 SaaSの導入

【採点基準】

【設問1】

- (1) 解答例だけを正解としました。表現として「Webブラウザ」は「社内PC」などでも正解としました。
- (2) 解答例だけを正解としました。
- (3) 解答例のように、プロキシサーバのサーバ証明書のコモンネームに、Webサーバのコモンネームを設定することを述べたものを正解としました。
- (4) 解答例のように、問題として、サーバ証明書の検証に失敗すること、作業として、プロキシサーバのルート証明書を社内PCにインストールすることを適切に述べたものを正解としました。

【設問2】

- (1) 解答例だけを正解としました。eで「Web」は部分点としました。
- (2) 解答例だけを正解としました。
- (3) 解答例のように、コネクションの確立要求パケットが、正しくインターネットブレイクアウトできな

い事象をルーティングの観点として述べたものを正解としました。

- (4) 解答例のように、プロキシ自動設定ファイルの指定として、G 社 SaaS 宛て通信をプロキシ経由から除外することを述べたものを正解としました。
- (5) 解答例だけを正解としました。配点表は“完答”となっていますが、デフォルトルートとプロキシサーバのネクストホップが正しいものは部分点としました。
- (6) 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) 解答例のように、FEC パケットによるオーバーヘッドが通信に与える影響を適切に述べたものを正解としました。
- (4) 解答例だけを正解としました。
- (5) 解答例だけを正解としました。
- (6) 解答例だけを正解としました。

【講評】

【設問1】

- (1) 正答率は高かったです。CONNECT メソッドや HTTPS 通信におけるサーバ証明書の検証は、基本的に重要ですので、間違った方はよく確認しておきましょう。
- (2) 名前解決を考慮して、「DNS サーバ」を加えた解答がありました。一理ありますが、G 社 SaaS はグループウェア機能をもつことや、下線①の前の記述からプロキシサーバが妥当と判断できるので、不正解としました。
- (3) ブラウザがサーバ証明書を検証する際には、発行者の署名の検証、有効期間及び失効情報の確認に加えて、コモンネーム (CN) の正当性を検証することを整理しておきましょう。
- (4) 問題については、正答率は高かったです。作業については、サーバ証明書とルート証明書を混同していると思われる解答がありました。HTTPS 通信における TLS ハンドシェイクプロトコルによる折衝で、ブラウザはサーバから受信したサーバ証明書を、ルート証明書に格納されている公開鍵を用いて検証します。サーバ証明書をあらかじめブラウザにインストールしておくことはありません。あらかじめインストールしておくのは、サーバ証明書を検証するためのルート証明書です。また、「Web サーバの秘密鍵をプロキシサーバに設定する」といった解答がありました。Web サーバの秘密鍵を第三者が利

用することはできません。プロキシサーバの鍵ペアは、Web サーバとは異なる鍵ペアです。

【設問2】

- (1) e:「WebDAV」は、続く「JSON (空欄 f) 形式で返される」という記述に整合しないので、不正解としました。
f:「テキスト」は、確かに JSON はテキスト形式ですが、空欄 f の前の記述を踏まえて不正解としました。
- (2) 正答率は低かったです。ESP 用の SA は、一つの経路で送受信 2 本確立され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。DPI によるインターネットブレークアウトにおいて、コネクションの確立要求パケットが正しくルーティングされない事象は、ファーストパケット問題と呼ばれます。本文のように、IP アドレスを用いて制御する対応策が一般的です。ネットワーク構成によりますが、他に DNS Snooping によって制御する仕組みなどがあります。「暗号化されているのでルーティングできない」という解答がありました。この点は、設問文の「HTTPS 通信に対する DPI に対応」からクリアしています。
その他に、遅延や暗号処理時間、IPsec VPN に着目した問題など、ルーティングの観点と異なるものがありました。設問に従ってルーティングにフォーカスします。IPsec VPN に関して、拠点の SD-WAN ルータでは、インターネットブレークアウトの判断後に、G 社 SaaS 宛て以外の本社宛ての通信を IPsec でカプセル化します。
- (4) 設問で問われている、プロキシ自動設定ファイルの指定とは別の設定を述べた解答がありました。まずは、設問の主旨をよく把握することが重要です。
- (5) G 社 SaaS の状況を踏まえ、都度の L3SW の設定を不要とするという要件を満たすような、経路設定の見直し内容をよく理解しておきたいです。
静的経路情報の宛先として業務サーバを解答したものがありません。業務サーバは、L3SW に直接接続しているので、宛先経路として設定する必要はありません。ルーティングテーブルの情報は、L3SW のインタフェースの設定に基づいて自動的に生成されます。
- (6) 「SD-WAN コントローラ」を含めた解答がありました。SD-WAN ルータの説明の中に、SD-WAN コントローラへの指示は、ツールを用いて行う旨が記述されており、G 社 SaaS へのアクセスが必要とは述べられていません。

[設問3]

- (1) 解答が書かれた中では、g の正答率は高く、h の正答率は低めでした。
- (2) m, n: 設問では、データ量そのものを削減する仕組みが問われていますが、シェーピングや送信方式の仕組みなど、データ量が変わらないものがありました。「ポリシング」は、パケットを破棄することによってトラフィック量を低減させますが、社内の通信に関しては必要な通信が制限されてしまう弊害があるので、不正解としました。また、圧縮に着目して、「圧縮」と「復元」という解答は、日本語的には空欄に入り得ますが、一つ分の得点としました。
- (3) 正答率は高かったです。
- (4) 「6 往復目、4 往復目」という解答がありました。
RWIN の最大値に達するタイミングの捉え方の違いだったと推察します。
- (5) 正答率は低かったです。
- (6) 正答率は低かったです。

問 2 は、計算問題が多めであったことから、思うように得点できなかった方もいるかも知れません。特に、設問 3 (5)(6) では未解答の答案が多くありました。本試験では、計算問題は少ないので、解答時間を確保して、根気よくケアレスミスのないように取り組んでください。

以上