

平成28年度  
秋期

## 午前Ⅱ問題の解答・解説

<input type="checkbox"/> 問 1	エ	<input type="checkbox"/> 問 11	ウ	<input type="checkbox"/> 問 21	イ
<input type="checkbox"/> 問 2	ウ	<input type="checkbox"/> 問 12	イ	<input type="checkbox"/> 問 22	イ
<input type="checkbox"/> 問 3	ウ	<input type="checkbox"/> 問 13	ア	<input type="checkbox"/> 問 23	ウ
<input type="checkbox"/> 問 4	イ	<input type="checkbox"/> 問 14	イ	<input type="checkbox"/> 問 24	ウ
<input type="checkbox"/> 問 5	ア	<input type="checkbox"/> 問 15	エ	<input type="checkbox"/> 問 25	ウ
<input type="checkbox"/> 問 6	ア	<input type="checkbox"/> 問 16	エ		
<input type="checkbox"/> 問 7	ウ	<input type="checkbox"/> 問 17	ア		
<input type="checkbox"/> 問 8	エ	<input type="checkbox"/> 問 18	ア		
<input type="checkbox"/> 問 9	エ	<input type="checkbox"/> 問 19	ア		
<input type="checkbox"/> 問 10	エ	<input type="checkbox"/> 問 20	ウ		

## 問 1：正解エ

Automatic MDI/MDI-X 機能とは、ポートに接続されたツイストペアケーブルがストレートかクロスかを判別し、自ポートの結線をストレート又はクロスに自動的に切り替えることにより、どちらのケーブルでも接続できるようにする機能である。

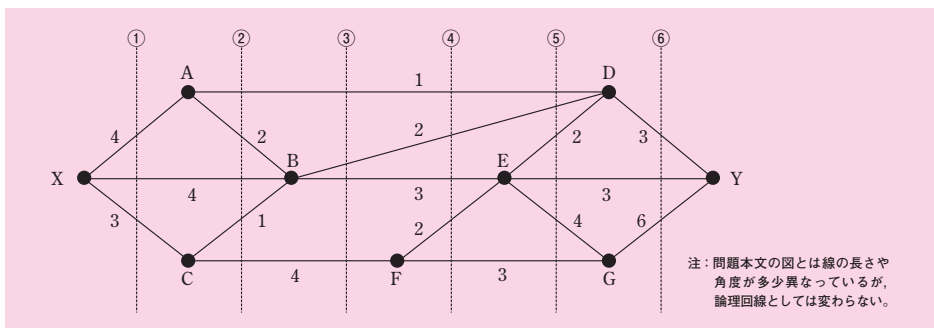
よって、正解は選択肢エとなる。

## 問 2：正解ウ

OFDM（Orthogonal Frequency Division Multiplexing：直交周波数分割多重方式）とは、高速無線通信で使用されている多重化方式の一つである。キャリア（搬送波）を複数のサブキャリアに分割した上で、サブキャリアごとにデータ信号を変調させて伝送する。各サブキャリアは相互に干渉しないように配置されているため、狭い周波数帯域を効率的に利用した高速伝送を実現している。よって、正解は選択肢ウである。

## 問 3：正解ウ

次の図に示すように、XY 間の通信路を分断する線を書き加える。なお、この図では破線①～⑥が描かれているが、これ以外にも分断線は多数考えられる。それぞれの分断線を横切る論理回線の多重度を合計する。例えば分断線③の場合、 $1 + 2 + 3 + 4 = 10$  となる。これら合計値の中で、最も小さい値が、XY 間で同時に設定可能な多重度の最大値である。考えられる分断線をしらみつぶしに検討すると、最も小さい合計値は 10 となる。よって、正解は選択肢ウとなる。



図：分断線を書き加えたネットワーク

## 問 4：正解イ

OSPF は、宛先までのコストが最小となる経路が選択されるプロトコルである。

### ●拠点 1 と拠点 3 の間の通信のコスト

WAN1 を通過する場合、拠点 1 と拠点 3 の間の通信のコストは次のようになる。

経路：ルータ a - ルータ b - WAN1 - ルータ e - ルータ h - ルータ i

コスト： $30 + 100 + 30 + 10 = 170$

WAN2 を通過する場合は、x と y のコストが不明なので、経路は二つ考えられる。

#### ●ルータ f を通過する場合

経路：ルータ a - ルータ d - WAN2 - ルータ g - ルータ f - ルータ i

コスト： $40 + 100 + x + 10 = 150 + x$

#### ●ルータ h を通過する場合

経路：ルータ a - ルータ d - WAN2 - ルータ g - ルータ h - ルータ i

コスト： $40 + 100 + y + 10 = 150 + y$

拠点 1 と拠点 3 の間の通信が WAN1 を通過するには、前述の三つの中で WAN1 を通過する経路のコストが最小になっていなければならない。つまり、WAN2 を通過する経路が 170 より大きければよい。x と y の値はそれぞれ、

$$150 + x > 170 \quad \therefore 20 < x \quad \cdots \cdots \text{式①}$$

$$150 + y > 170 \quad \therefore 20 < y \quad \cdots \cdots \text{式②}$$

となる。ただし、式①及び式②の両方が成立していなければならない。

### ●拠点 2 と拠点 3 の間の通信のコスト

WAN1 を通過する場合、拠点 2 と拠点 3 の間の通信のコストは次のようになる。

経路：ルータ c - ルータ b - WAN1 - ルータ e - ルータ h - ルータ i

コスト： $50 + 100 + 30 + 10 = 190$

WAN2 を通過する場合、 $x$  と  $y$  のコストが不明なので、経路は二つ考えられる。

- ルータ  $f$  を通過する場合

経路 : ルータ  $c$  - ルータ  $d$  - WAN2 - ルータ  $g$  - ルータ  $f$  - ルータ  $i$

コスト :  $40 + 100 + x + 10 = 150 + x$

- ルータ  $h$  を通過する場合

経路 : ルータ  $c$  - ルータ  $d$  - WAN2 - ルータ  $g$  - ルータ  $h$  - ルータ  $i$

コスト :  $40 + 100 + y + 10 = 150 + y$

拠点 2 と拠点 3 の間の通信が WAN2 を通過するには、前述の三つの中で WAN2 を通過する経路のコストが最小になっていなければならない。WAN2 を通過する経路は二つあるので、どちらか一方又は両方が 190 より小さければよい。 $x$  と  $y$  の値はそれぞれ、

$$150 + x < 190 \quad \therefore \quad x < 40 \quad \cdots \cdots \text{式③}$$

$$150 + y < 190 \quad \therefore \quad y < 40 \quad \cdots \cdots \text{式④}$$

となる。ただし、式③又は式④のどちらか一方又は両方が成立していなければならない。

### ● $x$ と $y$ に設定するコストの組合せ

$x$  と  $y$  に設定するコストの組合せは、次の 3 通りとなる。

- |                   |  |
|-------------------|--|
| ● 式①、②及び③を満たす場合   | 組合せ 1 : $20 < x < 40, \quad 20 < y$      |
| ● 式①、②及び④を満たす場合   | 組合せ 2 : $20 < x, \quad 20 < y < 40$      |
| ● 式①、②、③及び④を満たす場合 | 組合せ 3 : $20 < x < 40, \quad 20 < y < 40$ |

選択肢イは、 $x = 30, y = 30$  なので、組合せ 1 ～ 3 のいずれも満たす。しかし、残りの選択肢は、組合せ 1 ～ 3 のいずれも満たさない。よって、正解は選択肢イである。

## 問 5 : 正解ア

ア : 正解。アドミSSION制御について適切に記述している。

イ : シューピングではなく、ポリシングについて記述したものである。TCP で通信しているとき、途中経路でパケットが廃棄されると TCP の輻輳制御が働くため、輻

輾が生じない程度までトラフィックの出力レートが調整される。

ウ：ポリシングではなく、シェーピングについて記述したものである。最大速度を超過したパケットはバッファにいったん蓄えられ、後から送信される。そのため、大幅な遅延が許されない音声通信には不向きである。なお、バッファの容量を超えてしまうとパケットは廃棄される。

エ：ベストエフォートではなく、優先制御について記述したものである。フレームの種類や宛先に応じてクラス分けを行い、クラスごとに設けられたキュー（待ち行列）に配置する。それぞれのキューには異なる優先度が割り当てられており、これは優先キューと呼ばれる。優先キューからフレームを取り出す処理のことをスケジューリングといい、様々な方式がある。

## 問 6：正解ア

Gratuitous ARP とは、ARP の一種であり、ターゲット IP アドレスフィールドに自端末が使用する IP アドレスを入れて、MAC アドレスを問い合わせるものである。

これは、自端末と重複する IP アドレスの検出、同一ブロードキャストドメイン内の全端末の ARP キャッシュ更新に用いられている。

よって、正解は選択肢アとなる。

イ：通常の ARP について説明したものである。

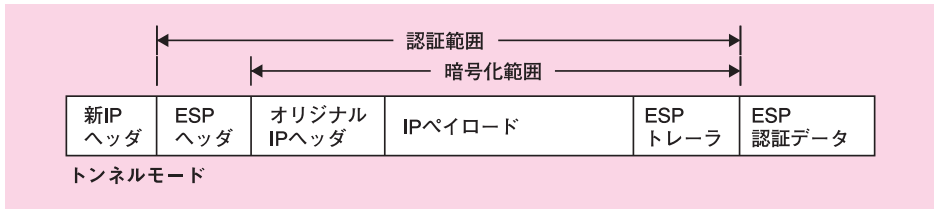
ウ、エ：RARP について説明したものである。選択肢の説明において、問合せを受けた MAC アドレスに対応する IP アドレスを返答するのは、RARP サーバである。

Gratuitous ARP について、詳しくは《基礎編》第 3 章「3.4.2 特別な用途の ARP」を参照していただきたい。

## 問 7：正解ウ

IPv4 における、IPsec の ESP トンネルモードの暗号化範囲と認証範囲を次の図に示す。

暗号化範囲は、オリジナル IP ヘッダから ESP トレーラまでである。よって、正解は選択肢ウとなる。



図：IPv4 における、IPsec の ESP トンネルモードの暗号化範囲と認証範囲

IPsec について、詳しくは本書の第 4 章「4.4.4 IPsec」を参照していただきたい。

## 問 8：正解エ

クラス D の IP アドレスはマルチキャストアドレスを割り振る場合に使用する。よって、正解は選択肢エである。

選択肢アはクラス C、選択肢イはクラス A の記述である。

プライベートアドレスは、10.0.0.0/8、172.16.0.0/16、192.168.0.0/16 の範囲が割り当てられている。

## 問 9：正解エ

MPLS とは、ラベルと呼ばれる識別子を用いてパケットを高速に転送する技術である。

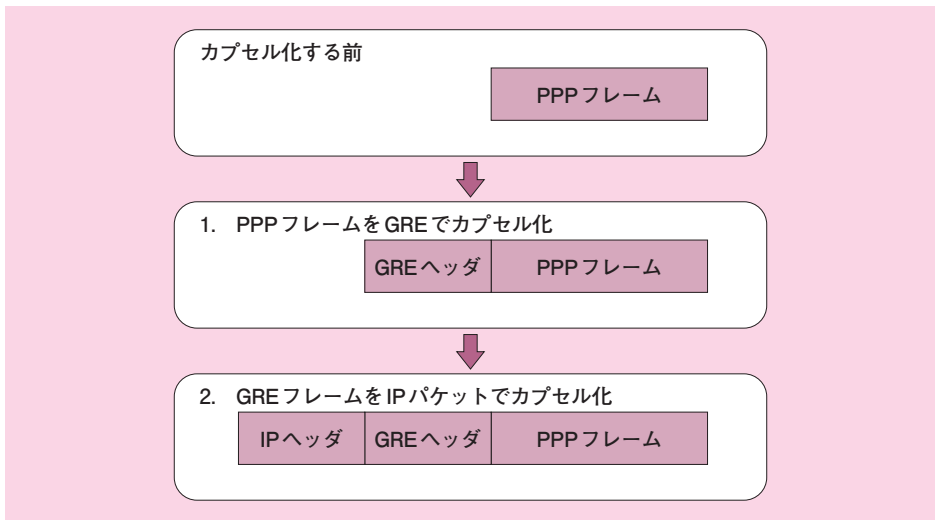
MPLS では、MPLS 網に入ったときラベルが付与され、網を出るときにこれが除去される。

したがって、エンドノードはラベルの存在を意識する必要がない。よって、正解は選択肢エとなる。

ア：IPsec について説明したものである。

イ：L2TP について説明したものである。

ウ：GRE (Generic Routing Encapsulation) を用い、PPP フレームを IP パケットでカプセル化して転送する技術について説明したものである。問題文の「PPP データフレーム」は、上位層データをペイロードにもつ PPP フレームを指す。カプセル化の順序を次の図に示す。



図：GRE を用いた、PPP フレームの IP パケットによるカプセル化

## 問 10：正解エ

選択肢のうち、TCP と UDP 両方のヘッダに存在するものは、送信元ポート番号である。よって、正解は選択肢エとなる。

ア：宛先 IP アドレスは、IP ヘッダに存在する。

イ：宛先 MAC アドレスは、MAC ヘッダに存在する。

ウ：生存時間（TTL）は、IP ヘッダに存在する。

TCP ヘッダ、UDP ヘッダについて、詳しくは《基礎編》第 3 章「3.3.2 TCP ヘッダ」,「3.3.3 UDP ヘッダ」を参照していただきたい。

## 問 11：正解ウ

問題文に示された IP アドレスの範囲「192.168.10.0/24 ～ 192.168.58.0/24」を 2 進数で表記すると、網掛けの範囲を集約することになる。

192.168.10.0	11000000	10101000	00001010	00000000
⋮	⋮	⋮	⋮	⋮
192.168.58.0	11000000	10101000	00111010	00000000

したがって、サブネットマスクの長さは 18 である。よって、正解は選択肢ウとなる。

## 問 12：正解イ

受信確認をメッセージ単位で行うと、メッセージを一つ受信するたびに応答確認を返信する必要が発生するため、効率の良い伝送ができない。そこで TCP では、受信確認を待たずに複数のメッセージを連続して送信する方法を採用している。受信確認を待たずに送信できる最大サイズを「ウィンドウサイズ」と呼ぶ。

よって、正解は選択肢イとなる。

## 問 13：正解ア

ルータ Z のルーティングテーブルには、5 個の経路情報がある。

このうち、宛先 IP アドレス「10.100.100.1」にマッチする経路情報は、1 行目と 5 行目である。1 行目のサブネット長は 8 であり、5 行目のサブネット長は 0 であるので、最長のサブネットをもつものは 1 行目である。

〔ルータ Z のルーティングテーブル〕

宛先アドレス	サブネットマスク	ネクストホップ
10.0.0.0	255.0.0.0	192.168.1.254
10.64.0.0	255.224.0.0	192.168.2.254
10.96.0.0	255.252.0.0	192.168.3.254
10.128.0.0	255.128.0.0	192.168.4.254
0.0.0.0	0.0.0.0	192.168.0.1

図：ルータ Z のルーティングテーブル

1 行目の経路情報のネクストホップは「192.168.1.254」である。この IP アドレスをもつルータは、ルータ A である。



よって、正解は選択肢アとなる。

## 問 14：正解イ

---

WebDAV (Web-based Distributed Authoring and Versioning) は、HTTP 1.1 の仕様を拡張し、コンテンツの作成／コピー／移動／ロック、コンテンツ属性の取得／設定／削除などのメソッドをもつプロトコルである。

よって、正解は選択肢イとなる。

## 問 15：正解エ

---

WebSocket は、Web コンピューティングにおける双方向のプッシュ配信を実現する技術である。プロトコルの規格は IETF が策定し、RFC6455 で標準化されている。API の規格は W3C が策定しており、これを受けてクライアント側（主要ブラウザの JavaScript）、サーバ側（Java EE、PHP、Node.js など）の双方で、WebSocket の実装が普及している。

WebSocket は、プッシュ配信に先立ち、既存の HTTP 通信を用いて、クライアントがサーバに WebSocket 通信の開始を要求する。より正確に言うと、この HTTP 通信を WebSocket 通信に切り替えることを要求する。次いで、サーバがこの要求を受理した旨を応答する。その後、WebSocket による双方向通信が行われる仕組みになっている。

よって、正解は選択肢エとなる。

## 問 16：正解エ

---

SAML (Security Assertion Markup Language) は異なるシステム間において、認証情報や属性情報を相互間で情報交換する内容を規定した Web サービスプロトコルである。SAML を用いると、複数のドメイン (Web サイト) をまたがったシングルサインオンを実現することができる。よって、正解は選択肢エである。

ア：UDDI (Universal Description, Discovery and Integration) に当てはまる記述である。

イ：S/MIME (Secure Multipurpose Internet Mail Extensions) に当てはまる記述である。

ウ：XKMS (XML Key Management Specification) に当てはまる記述である。

## 問 17：正解ア

無線 LAN で IEEE802.1X を使用したとき、アクセスポイントと無線 LAN 端末がアソシエーションを確立した時点で、利用者認証を実施する。この認証に成功した無線 LAN 端末だけが、アクセスポイントを経由した無線 LAN 通信を行うことができる。

実際の認証は認証サーバ（RADIUS サーバ）が実施しているが、アクセスポイントは無線 LAN 端末と認証サーバの間で認証プロトコルのやり取りを中継している。この認証プロトコルが EAP である。

アクセスポイントは、無線端末との間では EAP パケットをイーサネットフレームに格納して通信し、認証サーバとの間では EAP パケットを RADIUS パケットに格納して通信している。

よって、正解は選択肢アとなる。

IEEE802.1X について、詳しくは本書の第 4 章「4.4.3 IEEE802.1X」を参照していただきたい。

## 問 18：正解ア

NTP は、トランスポート層プロトコルに UDP を用いている。

NTP サーバや DNS サーバなど、UDP 上で伝送されるアプリケーション層プロトコルを利用したサービスを提供しているサーバには、リフレクション攻撃（リフレクタ攻撃とも呼ばれる）の踏み台に利用されるという脆弱性をもつ。

問題文は、リフレクション攻撃のことを「増幅型の DDoS 攻撃」と呼んでいる。この攻撃を理解するには、リフレクション攻撃に悪用される UDP の脆弱性、及び、リフレクション攻撃に悪用されるパケットサイズの特徴を理解する必要がある。そこで、これらの点について、まずは解説する。次いで、NTP を用いたリフレクション攻撃について解説し、解を導こう。

### ●リフレクション攻撃に悪用される UDP の脆弱性

コネクションレス型の UDP では、コネクションを確立せず、最初のパケットからアプリケーション層プロトコルのやり取りが始まる。それゆえ、パケットの送信元 IP アドレスが、パケットを本当に送信したホストのものであるのか、あるいは詐称されたものであるのかを（少なくとも、トランスポート層以下のヘッダ情報だけでは）、見分けることができない。

したがって、NTP など、トランスポート層プロトコルに UDP を使用する通信は、送信元 IP アドレスの詐称が容易であるという脆弱性をもっている。リフレクション攻撃は、これ

を悪用している。

攻撃者は、NTP サーバに対し、送信元 IP アドレスを攻撃対象ホストの IP アドレスに詐称したリクエストパケットを送信する。その結果、攻撃対象ホストは、同サーバからのレスポンスパケットを受信してしまう。このとき、同サーバは、リフレクション攻撃の踏み台となっている。

### ●リフレクション攻撃に悪用されるパケットサイズの特徴

リフレクション攻撃は、攻撃する側にもされる側にも負荷がかかるという両側面をもっている。すなわち、攻撃する側にはリクエストパケットの送信に伴う負荷がかかり、攻撃される側にはレスポンスパケットの受信に伴う負荷がかかる。その負荷とは、具体的に言うと、ホストがパケットを送受信する際の CPU 負荷であったり、回線がパケットを伝送する際の帯域負荷であったりする。

両刃の剣と言えるリフレクション攻撃であるが、リクエストパケットに比べてレスポンスパケットのサイズが大きいとき、当然ながら攻撃される側の方に大きな負荷がかかる。そこで、リフレクション攻撃では、極めて大きなサイズのレスポンスを応答するようなリクエストを発行することで、サービス妨害を引き起こすことを狙っている。

リクエストに比べてレスポンスのパケットサイズが何倍、何十倍にもなるというリフレクション攻撃の特徴を指して、問題文は本攻撃のことを「増幅型」と呼んでいる。

実際には、サービス妨害を狙う攻撃者は、踏み台とする NTP サーバを複数用いた DDoS 攻撃（分散型 DoS 攻撃）を仕掛けてくる。すなわち、1 台のホストを目掛けてリフレクション攻撃を同時に実行し、より一層大きな被害をもたらしている。

### ●NTP を用いたリフレクション攻撃

本問の選択肢 A に挙げられている、NTP サーバの状態確認機能（monlist）の問合せは、リクエストパケットに対して何倍、何十倍も大きなサイズのレスポンスパケットを応答する（100 倍を超えることもある）。この特徴を悪用し、次の手順に従って、NTP サーバを踏み台にしたリフレクション攻撃が行われる。

1. 攻撃者は、ボットを多数用意する。
2. 攻撃者のボットは、送信元 IP アドレスを攻撃対象ホストに詐称した状態確認機能の問合せを、踏み台となる NTP サーバに一斉に発行する。このとき、踏み台となる NTP サーバを複数用いる。
3. 問合せを受けた NTP サーバは、攻撃対象ホスト宛てに、当該問合せに対する応答を送信する。

この結果、攻撃を受けたホストは大容量のパケットを同時に多数受信するため、サービス不能に陥る。

### ●解の導出

本問は、リフレクション攻撃に対して、NTP サーバが踏み台にされることを防止する対策を問うている。本攻撃が成立するには、NTP サーバの状態確認機能が有効になっていなければならない。したがって、対策は、この機能を無効にすることである。

よって、正解は選択肢アとなる。

## 問 19：正解ア

テンペスト技術とは、コンピュータが発する電磁波を傍受し、それを解読する技術である。その対応策として、電磁波遮断が施された部屋に機器を設置する方法がある。よって、正解は選択肢アとなる。

## 問 20：正解ウ

問題文に登場するファイアウォールは、ステートフルインスペクション機能をもっていない。したがって、許可したい通信を登録する際、リクエストとレスポンスのそれぞれについて、送信元と宛先の IP アドレス、ポート番号の組を設定する必要がある。

社内の PC からインターネット上の SMTP サーバに電子メールを送信できるようにするには、リクエストとレスポンスを次の表のとおり設定する。

	IP アドレス		ポート番号	
	送信元	宛先	送信元	宛先
リクエスト	PC	SMTP サーバ	1024 以上	25
レスポンス	SMTP サーバ	PC	25	1024 以上

ここで、ポート番号について補足しておこう。

リクエストの宛先ポート番号は、SMTP のウェルノウンポート番号である 25 を指定する。リクエストの送信元ポート番号は、OS がウェルノウンポート番号以外のものを任意に選ぶので、1024 以上を指定する。

当然ながら、レスポンスの宛先／送信元ポート番号は、リクエストのそれと入れ替わったものになる。

この表と一致するのは選択肢ウである。よって、これが正解となる。

## 問 21：正解イ

無線 LAN のアクセスポイントがもつプライバシーセパレータ機能とは、同じアクセスポイントに接続している無線 LAN 端末同士が直接通信できないようにする機能である。

よって、正解は選択肢イである。

ア：ステルス機能の説明である。

ウ：MAC アドレスフィルタリング機能の説明である。

エ：アクセスポイントには、建物外への無線 LAN 電波漏れを防ぐ機能は存在しない。  
盗聴を防止するには、無線 LAN 電波漏れを防ぐことよりも、暗号化が有効な対策となる。

## 問 22：正解イ

割込み処理とは、ユーザプログラムを実行している最中に、より優先度の高い処理を行うためにユーザプログラムを一時的に中断し、当該処理を実行することである、

OS は割込み処理の特権モード（カーネルモード）で実行するため、ハードウェアを制御したり、緊急性を有する例外事象に対処したりすることができる。割込み処理の実行が終わるとユーザモードに戻り、OS はユーザプログラムの実行を再開する。

ユーザプログラムの実行を中断してから割込みルーチンの実行を開始するまで、次に示す段階を踏む。

1. 割込み処理を実行するため、ユーザモードから特権モードへ移行する。
2. ユーザプログラムを一時的に中断し、後で再開できるようにするため、プログラムレジスタなどを退避する。
3. 割込み処理ルーチンの開始番地を決定し、プログラムカウンタにセットする。
4. 割込み処理ルーチンを特権モードで実行する。

よって、正解は選択肢イである。

## 問 23：正解ウ

処理 A が処理 B を呼ぶ関係になっているとき、処理 A（呼ぶ側）と処理 B（呼ばれる側）の実行時間の長さには、次に示す大小関係が成立する。

処理 A（呼ぶ側）の実行時間 > 処理 B（呼ばれる側）の実行時間

したがって、処理 A、処理 B のそれぞれの実行時間にタイムアウトを設定する場合、この大小関係を考慮し、次のように設定する必要がある。

処理 A（呼ぶ側）のタイムアウト > 処理 B（呼ばれる側）のタイムアウト

問題文の AP サーバの AP は業務処理を実行している。この処理の中からトランザクション処理が呼ばれている。ここで、業務処理を処理①、同処理から呼ばれるトランザクション処理を処理②と呼ぶことにしよう。

問題文のタイムアウト①、②は、この処理①、②の実行時間に設定したものに相当する。

したがって、呼ぶ側（①）と呼ばれる側（②）の関係を考慮するなら、これら二つのタイムアウトを次のように設定する必要がある。

タイムアウト① > タイムアウト②

Web サーバが AP サーバに業務処理のリクエストを送信してから、AP サーバがそのリクエストを受信して業務処理を開始するまでの間に、両サーバ間の通信時間がかかる。つまり、わずかながらタイムラグが生じる。同様に、AP サーバが業務処理を終了してから、Web サーバがその返信を受けるまでの間も、通信時間の分だけタイムラグが生じる。

問題文のタイムアウト③は、Web サーバが AP サーバにリクエストを送信してから返信を受けるまでの時間に設定したものに相当する。タイムアウト①は、前述の説明と同じく、AP サーバの処理①の実行時間に設定したものに相当する。

したがって、通信時間分のタイムラグを考慮するなら、これら二つのタイムアウトを次のように設定する必要がある。

タイムアウト③ > タイムアウト①

以上をまとめると、三つのタイムアウトには次の大小関係が成立する。

タイムアウト③ > タイムアウト① > タイムアウト②

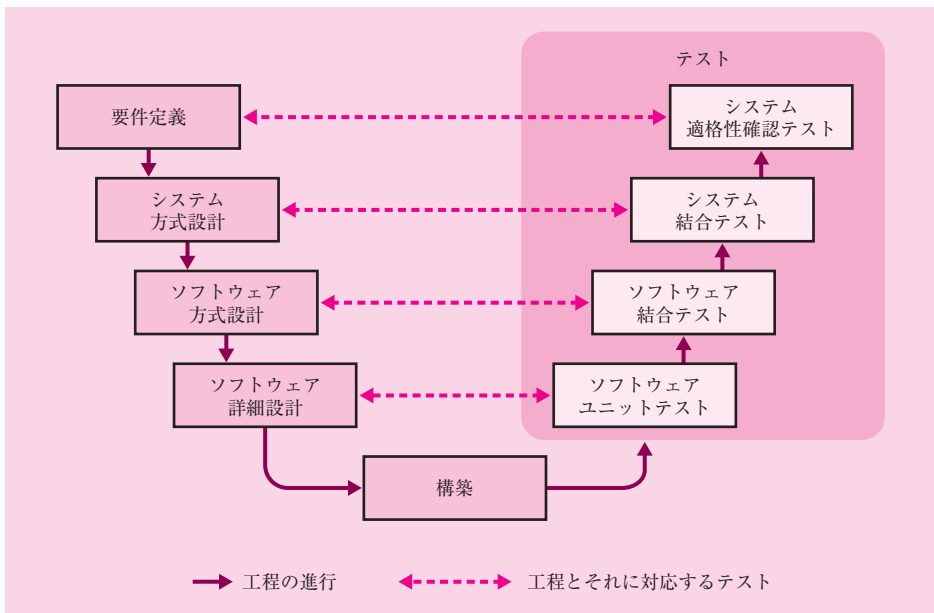
よって、正解は選択肢ウとなる。

## 問 24：正解ウ

システム開発プロセスは、ウォーターフォール型開発モデルに従う場合、およそ次に示す工程の順序に沿って進行する。これを V 字モデルという。なお、ここに列挙した工程の名称は、共通フレーム 2013 に準じたものである。

システム要件定義→システム方式設計→ソフトウェア方式設計  
→ソフトウェア詳細設計→実装→テスト

テスト工程は、何種類かのテストから成る。その主なものを挙げると、ユニットテスト、結合テスト、システム適格性確認テストなどがある。これらのテストが検証する内容は、各開発工程の成果物に基づいており、およそ次の図に示す対応関係がある。



図：システム開発の V 字モデルにおける、工程とテストの対応関係

この図が示すとおり、システム方式設計にはシステム結合テストが、ソフトウェア方式設計にはソフトウェア結合テストが、ソフトウェア詳細設計にはソフトウェアユニットテストが、それぞれ対応している。

よって、正解は選択肢ウとなる。

開発プロセスの工程の用語の意味は各社各様であるため、その感覚で解いてしまうと正解を導けないかもしれない。その対策として、共通フレームを一読し、用語の定義を確認することをお勧めする。

なぜなら、情報処理技術者試験のシラバスのうち、開発プロセスに関係するものは、原則的に共通フレームに基づいて作成されているからだ。完全に一致しているわけではないが、ほぼ似通った内容となっている。

その裏付けとして、参考までにシステムアーキテクト試験のシラバスを掲載しておく（本原稿執筆時点の最新版は Ver 4.1）。本問の解と一致した内容が書かれていることが見て取れるだろう。

大項目	小項目	概要
8 システム方式設計	8-3 システム結合のためのテスト要件の定義	開発者は、システム結合のために、暫定的なテスト要件及び予定を定義し、文書化する。
10 ソフトウェア方式設計	10-4 ソフトウェア結合のためのテスト要件の定義	ソフトウェア結合のために暫定的なテスト要件及びスケジュールを定義し、文書化する。
11 ソフトウェア詳細設計	11-5 ソフトウェアユニットのテスト要件の定義	ソフトウェアユニットをテストするために、テスト要件及びスケジュールを定義し、文書化する。テスト要件は、要件の限界においてソフトウェアユニットに負荷をかけることを含める。

注記）下線は著者が引いたものである

共通フレームは、試験対策だけではなく、実務でも有効活用できる。

用語の意味が異なっていると、他社と取引する際、誤解や軋轢を生じさせる原因になってしまう。それを解消すべく、ISO/IEC12207に準拠してIPAが作成したのが、共通フレームなのである。

コミュニケーションの場面で、相手と同じ用語を使って会話していても、相手が同じ意味で理解しているとは限らない。必要であれば、その定義を明確にし、誤解を未然に防ぐように心掛けたい。その用語が開発プロセスに関するものであれば、共通フレームが役に立つだろう。

## 問 25：正解ウ

SOA（Service Oriented Architecture）とは、既存のアプリケーションを部品化し、その部品を組み合わせるビジネスプロセスを設計する手法である。

よって、正解は選択肢ウとなる。



ア：WDSL（Web Services Description Language）の説明である。

イ：UDDI（Universal Description, Discovery and Integration）の説明である。

エ：SLA（Service Level Agreement）の説明である。