

平成27年度  
秋期

## 午後Ⅱ問題の解答・解説

注：試験センターが公表している出題趣旨・採点講評・解答例を転載している。

## 問 1

## 出題趣旨

M2M (Machine to Machine) に関する、情報技術やシステム基盤が整備されつつあり、それらを活用した新しい情報システムの開発が進められている。M2M には、センサ、制御機器、設備などの多様な機械 (Machine) に関して、それらの性能や収容方法を考慮し、情報収集や制御などのユースケースを踏まえた、ネットワーク構築が必要となる。

本問では、リモート保守用の情報システム開発の初期検討を題材にしている。現行の TCP/IP ネットワークの拡張について、ネットワーク担当の視点から検討する。具体的には、利用形態から追加される通信を導き、その実現方法と、現行ネットワークへの影響を考察する。固有の知識を前提とはせずに、TCP/IP や HTTP に関する基本知識だけで推論できるよう記述を工夫し、ネットワーク基盤の拡張要件に関する、受験者の応用能力を問う。

## 採点講評

問 1 は、多数の設備を収容する情報システムを題材に、ネットワーク基盤の拡張に関する受験者の応用能力を求めている。近年注目を浴びている M2M (Machine to Machine) ネットワークを意識しながら、固有の知識を前提とはせずに、TCP/IP や HTTP に関する基本知識だけで解答できるような記述とした。

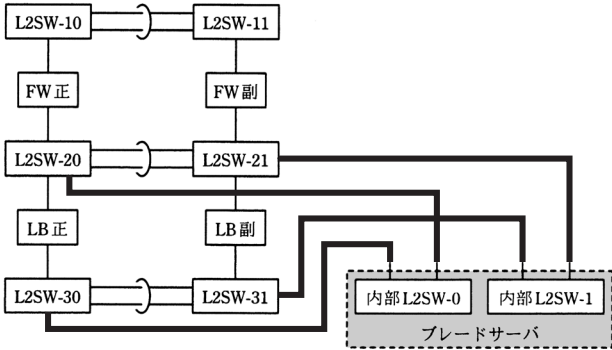
設問 1～4 に正答率の大きな偏りはなく、全体の内容はよく理解されていた。その中で、TCP/IP の基本に関する設問 1 (1) と設問 3 (2) と、HTTP に関する設問 4 (5)、(6) の正答率が比較的低かった。これらは、特別な知識は不要だが、複数の要素を理解し、正答を推論する問題である。日頃の勉強や実務でも、ネットワーク技術者として、複雑な状況から本質を見極め、課題を解決するという行動パターンを心掛けてほしい。

設問 1 は、サーバネットワークに関する理解を問うている。ヘッダ内のアドレスの変化など、基本事項に関する設問だが、誤答が少なからず見受けられた。この種の問題は落ち着いて取り組み着実に答えるようにしてほしい。

設問 2 は、提案された移動情報収集の通信方式への理解を問うている。HTTP/1.1 の基本知識を前提としたが、多くは提示した通信シーケンス例などから直接読み解く必要があることから、(2)、(5)、(6) は、受験者の経験によって差が出た設問だったようである。

設問 3 では CoAP (Constrained Application Protocol) という比較的新しい通信プロトコルを取り上げた。固有の知識は求めず、通信プロトコルの基本知識だけでも十分解ける問題とした。基本技術の正しい理解や、従来技術から新技術を理解・評価する能力は、実務でも大切である。

設問 4 は、“(1)、(2) 仮想サーバを含むネットワーク”と、“(3)～(6) HTTP における TCP コネクション (いわゆるセッション維持)”に関する設問である。どちらも過去に出題したテーマであるが、それらを通じて今回の題材への総合理解を問うた。限られた時間でもよく書けていた解答が多い一方で、“(5) クローズ接続オプションの使い方”や“(6) URL に関する設計指針”については理解不足の解答もやや目立った。本設問では、通常の“TCP コネクション維持による Web アクセスの応答時間改善”ではなく、“TCP コネクション解放によるファイアウォールの論理資源節約”という、いわば逆の要件になっていることに注意してほしい。

設問		解答例・解答の要点	備考
設問 1	(1)	あ 送信元 IP	
	(2)	い LB 正	
	(3)	①	
	(4)	⑥	
設問 2	(1)	う 中継装置	
		え 通信アダプタ	
		お リバース	
	(2)	稼働情報の収集周期の変更が容易である。	
	(3)	Tc	
	(4)	中継装置より通信アダプタのキャッシュの更新頻度が高く新しいから	
	(5)	① ・ 設備と TCP コネクションが確立できない場合 ② ・ 設備が Not Modified を応答した場合	
設問 3	(1)	か 通信アダプタ	
	(2)	IP ヘッダと UDP ヘッダ	
	(3)	① ・ TCP コネクションの確立と終了の手順が不要である。 ② ・ CoAP はヘッダ長が短いなど、データの格納効率が良い。	
設問 4	(1)	き LB	
	(2)		
	(3)	ア 30	
		イ 72	
		ウ 6	
	(4)	正常な通信に支障がない範囲でなるべく小さくする。	
	(5)	後続がないリクエストに付与し、コネクションを切断する。	
	(6)	通信アダプタに FQDN を付与し、同一コネクションを使って複数の設備から稼働情報を取得する。	

本問は、ネットワーク基盤の拡張をテーマに、負荷分散装置（以下、LB と称する）とブレードサーバを用いたネットワーク構成の設計、HTTP の機能（条件付き GET、同時コネクション数の軽減）と CoAP を用いたネットワーク負荷の改善等について問うている。

## ■設問 1

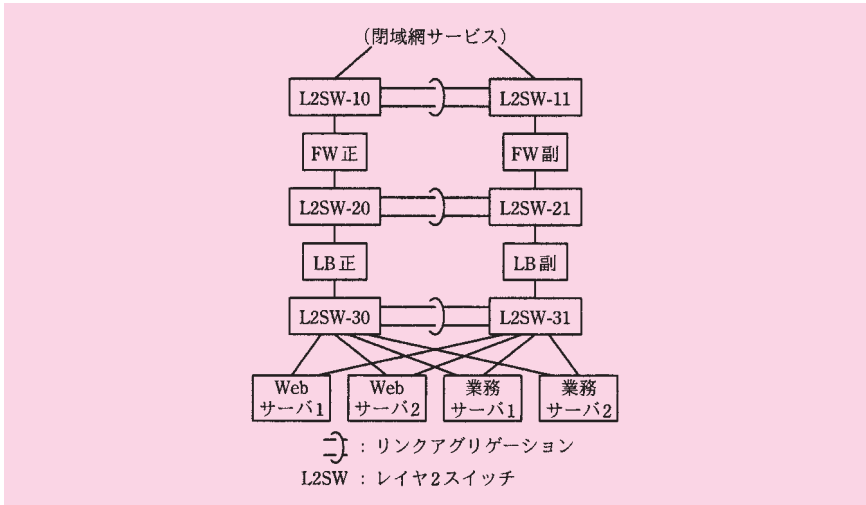
設問 1 の解説に入る前に、K 社の保守システムの構成（図 1）、K 社データセンタ内のネットワーク構成（図 2）における、サーバアクセスに関するデータの流れ（図 3）について解説する。

K 社の保守システムは、データセンタに置かれている。データセンタへのアクセスは二通りある。一つは、全国の保守センタから、PC を用いてアクセスする方法である。二つ目は、外出先（顧客のオフィスや工場など）から、保守端末用いてアクセスする方法である。

図 1 を見ると、保守センタとデータセンタが閉域網に接続されている。したがって、保守センタからのアクセスは、閉域網を経由することが分かる。

外出先からのアクセスは、本文には明記されていないので、一般的な知識から推論する。通常、閉域網サービスは、公衆無線 LAN サービス（Wi-Fi）等を用いて、インターネット経由で閉域網に接続する方法を提供している。それゆえ、それを用いてデータセンタにアクセスしていると考えられる。

K 社データセンタには、Web サーバと業務サーバが設置されている。そのネットワーク構成は、図 2「K 社データセンタ内のネットワーク構成（抜粋）」に示されている。



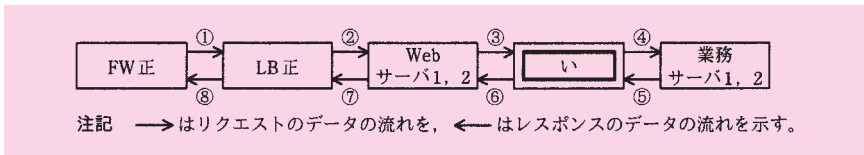
図：本文の図 2 の再掲「K 社データセンタ内のネットワーク構成（抜粋）」

現在、Web サーバは外部からアクセスを受け付けるが、業務サーバは Web サーバからのみアクセスを受け付ける。その点は、〔現在の保守システム〕の第 1 段落の 4 番目の箇条書きに「保守員は保守センタの PC 又は保守端末から Web サーバへアクセスし、保守情報を参照、更新する。アクセスを受けた Web サーバは、一部の処理を業務サーバに依頼する」と記述されていることから分かる。

K 社データセンタ内のネットワークには、FW、LB も設置されている。このネットワーク構成について、第 2 段落の中で次のように説明されている。

- ・リンクアグリゲーションで接続された 3 組の L2SW は、それぞれ単一の異なるセグメントを構成している。
- ・FW 及び LB は、Active-Standby 方式で冗長化されている。
- ・L2SW とサーバの接続は、サーバのチーミング機能によって冗長化されている。
- ・Web サーバと業務サーバのデフォルトゲートウェイは、LB である。
- ・Web サーバと業務サーバへのアクセスは、LB によって負荷分散されている。
- ・Web サーバと業務サーバへアクセスするための仮想 IP アドレスが、それぞれに定義されている。LB は、宛先の仮想 IP アドレスを実 IP アドレスに変換し、サーバへのアクセスを振り分ける。Web サーバから業務サーバへのアクセスについては、両サーバが同一セグメント内にあるので、あ アドレスも変換する。

通常時のサーバへのアクセスに関するデータの流れは、図3「通常時のサーバへのアクセスに関するデータの流れ」に示されている。



図：本文の図3の再掲「通常時のサーバへのアクセスに関するデータの流れ」

まず、情報を整理しよう。

### ●サブネットワーク

本文は、サブネットワークを「セグメント」と称している。

〔現在の保守システム〕の第2段落の最初の箇条書きから、三つのサブネットに分かれていることが分かる。

図2を使って説明すると、一つ目は、L2SW-10, L2SW-11 が収容されたセグメント（FWの外側）である。二つ目は、L2SW-20, L2SW-21 が収容されたセグメント（FWの内側とLBの外側との間）である。三つ目は、L2SW-30, L2SW-31 が収容されたセグメント（LBの内側）である。

### ●冗長構成

最初の箇条書きの記述から、L2SW間の接続はリンクアグリゲーションで冗長化されていることが分かる。

2番目の箇条書きの記述から、FW, LBは、Active-Standby方式で冗長化されていることが分かる。冗長化に用いている具体的な技術については記されていないが、FW, LBは、それぞれ仮想IPアドレスが定義されていると考えられる。本文は、通常時にActive側になっている系を「正」、Standby側になっている系を「副」と記しているの、この解説でもその表記を用いることにしよう。

3番目の箇条書きの記述から、サーバのNICはチームング機能によって冗長化されていることが分かる。チームング機能はベンダ固有の技術であるため、ひと口にチームング機能と言っても、Active-Standby方式であったり、Active-Standby方式かActive-Active方式のどちらかを選択できるものがあつたりする。通常、Active-Active方式であれば、リンクアグリゲーション（IEEE802.3ad）又はそれに類するベンダ固有技術が用いられている。本事例のチームング機能は、どの方式が採用されているだろうか。

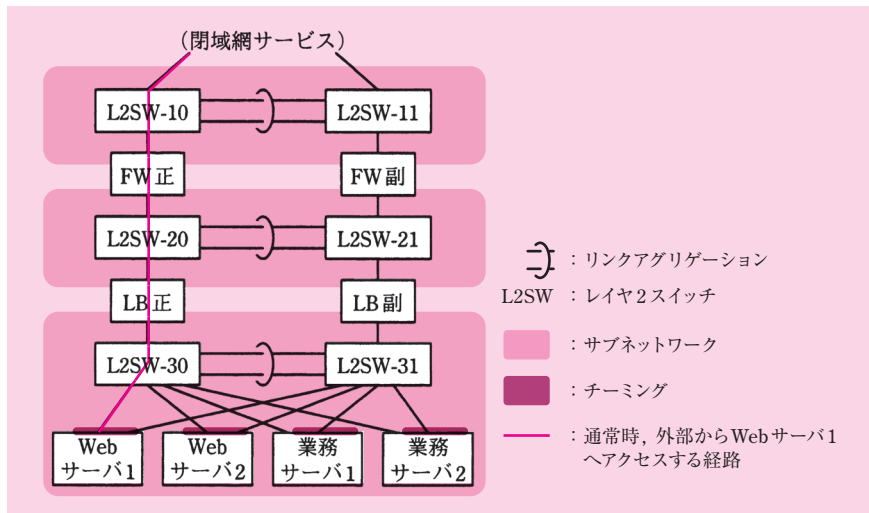
図2に記された、各サーバとL2SWとの接続から、本事例のチーミング機能は Active-Standby 方式であることが分かる。各サーバから出た2本のケーブルは、1本がL2SW-30に、もう1本がL2SW-31に接続されているからだ。

各サーバのNICは、どちらがActiveになっているのだろうか。通常時はLB正からサーバにアクセスするので、LB正と接続しているL2SW-30も通常時の経路になっている。したがって、L2SW-30に接続している側のNICがActiveになっていると考えられる。

チーミング機能がActive-Active方式（リンクアグリゲーション）であるとは言えない理由は、仮にActive-Active方式であれば、各サーバから出た2本のケーブルが、同一のL2SWに接続されているか、又は、スタック接続された2台のL2SWのそれぞれに接続されているか、そのどちらかでなければならないからである。

更に言えば、本文が「チーミング」と「リンクアグリゲーション」という用語を別々に使い分けていることも、ここで言うチーミング機能がActive-Active方式ではないことを示唆していると言えよう。

なお、チーミングについて、詳しくは本書の第6章「6.2.4 NICの冗長化」を参照していただきたい。



図：サブネットワーク及び冗長構成に関する情報の整理

### ●リクエストの送信とLBの振る舞い

Webサーバの仮想IPアドレスについて、6番目の箇条書きは、「Webサーバと業務サーバへアクセスするための仮想IPアドレスが、それぞれに定義されている。LBは、

宛先の仮想 IP アドレスを実 IP アドレスに変換し、サーバへのアクセスを振り分ける」と記述されている。

この記述から、LB に仮想 IP アドレスが設定されていることが分かる。それゆえ、Web サーバと業務サーバの仮想 IP アドレスを宛先とするパケットは、LB に転送される。

LB がサーバへのリクエストを受け取ったときの振る舞いは、次のようになることが分かる。

- クライアント端末からリクエストパケットを受信する
- 振り分け先サーバを決定する
- リクエストパケットの宛先を、仮想 IP アドレスから振り分け先サーバの実 IP アドレスへ変換する
- 振り分け先サーバへリクエストパケットを転送する

Web サーバの仮想 IP アドレスは、外部のクライアント端末が Web サーバにアクセスするときの宛先に指定するものである。それゆえ、Web サーバの仮想 IP アドレスは、LB の外側（FW と LB 間のサブネットの側）のインタフェースに設定される。

したがって、外部のクライアント端末（PC 又は保守端末）から Web サーバへリクエストを送信するとき、次のようにパケットが転送される。

- クライアント端末が送信するパケットは、宛先が Web サーバの仮想 IP アドレスである
- このパケットは、LB に転送される
- LB がこのパケットを受け取ると、振り分け先を、Web サーバ 1 又は Web サーバ 2 に決定する。その後、宛先をその実 IP アドレスに変換し、振り分け先サーバへ転送する

前述のとおり、業務サーバの仮想 IP アドレスも LB に設定されている。したがって、同様に、Web サーバから業務サーバへリクエストを送信するとき、次のようにパケットが転送される。

- Web サーバが送信するパケットは、宛先が業務サーバの仮想 IP アドレスである
- このパケットは、LB に転送される
- LB がこのパケットを受け取ると、振り分け先を、業務サーバ 1 又は業務サーバ 2 に決定する。その後、宛先をその実 IP アドレスに変換し、振り分け先サーバ

へ転送する

業務サーバの仮想 IP アドレスは、LB のどちらの側のインタフェースに設定されているのだろうか。外側（FW と LB 間のサブネットワーク側）だろうか、それとも、内側（Web サーバ 1 ～ 2、業務サーバ 1 ～ 2 が所属するサブネットワーク側）だろうか。実は、どちらの可能性も考えられる。

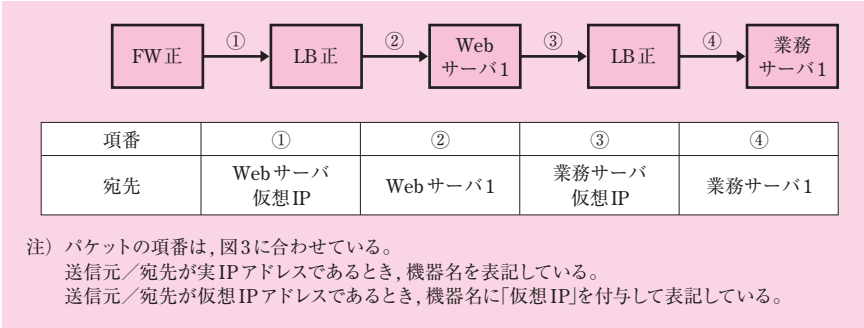
外側である場合、Web サーバの実 IP アドレスから見て、業務サーバの仮想 IP アドレスは、異なるサブネットに存在する。それゆえ、業務サーバの仮想 IP アドレスを宛先とするパケットが Web サーバから送信されると、このパケットは Web サーバのデフォルトゲートウェイに転送される。Web サーバのデフォルトゲートウェイは、4 番目の箇条書きに記述されているとおり、LB である。

内側である場合、（本文には明記されていないが）LB の内側インタフェースでプロキシ ARP を動作させる必要がある。Web サーバの実 IP アドレスから見て、業務サーバの仮想 IP アドレスは、同じサブネットに存在する。それゆえ、Web サーバは、業務サーバの仮想 IP アドレスを宛先とするパケットの送信に先立ち、業務サーバの仮想 IP アドレスを目標とする ARP 要求を送信する。LB は、この ARP 要求に対し、内側インタフェースの MAC アドレスを格納した ARP 応答を返信する（プロキシ ARP）。それゆえ、業務サーバの仮想 IP アドレスを宛先とするパケットが Web サーバから送信されると、このパケットは LB に転送される。

外側であるか内側であるかは本文の記述からは判断できないが、どちらの場合であっても、業務サーバの仮想 IP アドレスを宛先とするパケットは LB に到達することには変わりはない。どちらにせよ本問を解くことはできる（シンプルに設計するなら、Web サーバ、業務サーバのどちらも仮想 IP アドレスを外側に設定する。業務サーバの仮想 IP アドレスを内側に設定する場合、本文に明記されていない「プロキシ ARP」を前提とする必要が生じる）。

Web サーバと業務サーバへリクエストを送信するとき、宛先 IP アドレスが変化する様子を次の図に示す。この図では、Web サーバの振り分け先として Web サーバ 1 が、業務サーバの振り分け先として業務サーバ 1 が、それぞれ選択されたものとしている。





図：リクエスト送信における宛先 IP アドレスの変化

これと図 3 を見比べると、図 3 の空欄いに該当する機器は、「LB 正」となることが分かる。

●レスポンスの返信と LB の振る舞い

言うまでもなく、レスポンスパケットの宛先は、リクエストパケットの送信元である。これを図 3 に当てはめると、パケット①の送信元がパケット⑧の宛先になる。同様に、パケット②の送信元がパケット⑦の宛先に、パケット③の送信元がパケット⑥の宛先に、パケット④の送信元がパケット⑤の宛先になる。

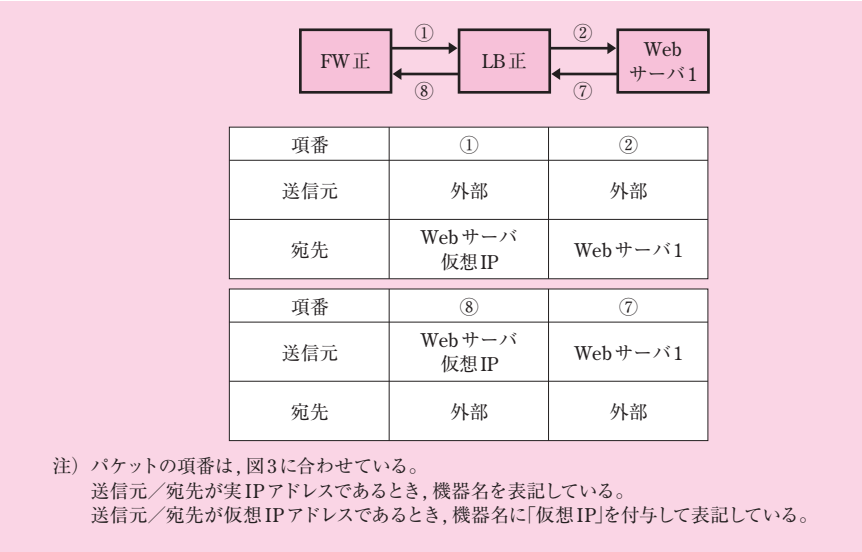
通常、LB の振る舞いは、リクエストパケットの転送時とレスポンスパケットの転送時とで異なる。リクエスト時の振る舞いは前述のとおりなので、レスポンス時の振る舞いを次に示す。

- 振り分け先サーバからレスポンスパケットを受信する
- レスポンスパケットの送信元を、振り分け先サーバの実 IP アドレスから仮想 IP アドレスへ変換する
- クライアント端末へレスポンスパケットを転送する

ここで、レスポンスパケットの送信元を変換してから転送する理由は、次のとおりである。

振り分け先サーバから受信するパケットの送信元 IP アドレスは、振り分け先サーバの実 IP アドレスになっている。これを仮想 IP アドレスに変換してからクライアント端末に返信することで、クライアント端末は、自分が送信したリクエストに対応するレスポンスであると識別することができるからだ。

K 社データセンタ内の Web サーバへのアクセスに当てはめると、送信元と宛先は次のようになる。図 3 と対比できるように、外部のクライアント端末は図示していない。



図：外部から Web サーバへのアクセス

この LB の振る舞いは、Web サーバから業務サーバへのアクセスにも同様に当てはめることができるように思えるが、実はそうではない。空欄あが示唆しているとおり、ある特別なアドレス変換が必要となる。この点は設問 1 (1) で問われているので、そこで詳しく解説する。

ここまで理解できれば、設問 1 を解く準備は整った。それでは、いよいよ小問の解説に移ろう。

(1)

解答例

あ：送信元 IP

空欄あを含む文章は、〔現在の保守システム〕第 2 段落の中にある。

第2段落は、現在のK社データセンタ内のネットワーク構成を箇条書きで説明している。6番目の箇条書きは、「Webサーバと業務サーバへアクセスするための仮想IPアドレスが、それぞれに定義されている。LBは、宛先の仮想IPアドレスを実IPアドレスに変換し、サーバへのアクセスを振り分ける。Webサーバから業務サーバへのアクセスについては、両サーバが同一セグメント内にあるので、あアドレスも変換する」と記述されている。

解を導くに当たり、まず、空欄あのアドレス変換を考慮せずに、第2段落の箇条書きに記された条件だけで、Webサーバから業務サーバにアクセスするケースを考察する。このとき、どのような問題が生じるかを見てみよう。

次いで、その問題を解決するために、どのようなアドレス変換が必要であるかを考察する。それが、空欄あの実解となる。

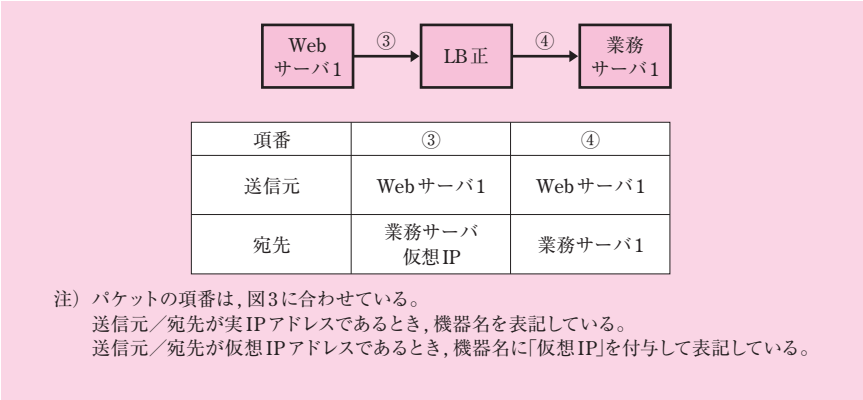
#### ●空欄あの実アドレス変換を考慮しない場合の問題

Webサーバから業務サーバにリクエストを送信するケースを考える。

送信元となるWebサーバの実体は、Webサーバ1又はWebサーバ2のどちらかである。ここでは、実際の送信元をWebサーバ1とする。同様に、宛先となる業務サーバの実体は、業務サーバ1又は業務サーバ2のどちらかである。ここでは、実際の宛先を業務サーバ1とする。

設問1の冒頭で解説したとおり、業務サーバへアクセスする際、宛先は業務サーバの仮想IPアドレスである。LBがこのパケットを受け取って業務サーバ1を振り分け先に決定すると、宛先が業務サーバ1の実IPアドレスに変換される。

ここまでの考察に基づき、空欄あの変換を考慮しない場合（つまり、通常のLBの振る舞いに基づいた場合）、リクエストの通信経路は次の図のとおりとなる。



図：Web サーバから業務サーバへのリクエストの送信（空欄あを考慮しない場合）

ここで注目できるのは、「パケット③、④の送信元が、Web サーバ 1 の実 IP アドレスである」ということだ。

このリクエストを受けて、業務サーバから Web サーバにレスポンスを返信するとき、通信経路はどうなるであろうか。

パケット④を受信した業務サーバ 1 は、その送信元に対して返信する。すなわち、レスポンスの宛先は、Web サーバ 1 の実 IP アドレスとなる。

業務サーバ 1 と Web サーバ 1 は同じサブネットに収容されている。したがって、宛先が Web サーバ 1 の実 IP アドレスであるパケットは、業務サーバ 1 から Web サーバ 1 に直接送信される。つまり、LB を経由しない。

業務サーバ 1 から Web サーバ 1 へのレスポンスの送信元（業務サーバ 1 の実 IP アドレス）は、パケット③の宛先（業務サーバの仮想 IP アドレス）とは異なっている。したがって、Web サーバ 1 がこれを受信したとき、自分が送信したリクエスト（パケット③）に対応するレスポンスであるとは識別できない。リクエストとレスポンスのやり取りが成立しない以上、通信が途絶えてしまうことが分かる。

したがって、空欄あのアドレス変換を考慮しない場合、Web サーバから業務サーバへのアクセスにおいて、リクエストに対応するレスポンスが返信されない、という由々しき問題がある。

●空欄あのアドレス変換による解決

空欄あを含む文を改めて見てみよう。それは、「LB は、宛先の仮想 IP アドレスを実 IP アドレスに変換し、サーバへのアクセスを振り分ける。Web サーバから業務サーバへのアクセスについては、両サーバが同一セグメント内にあるので、あ アド

レスも変換する」と記述されている。

空欄あのアドレス変換を行うのは、LB である。この変換が必要な理由は、Web サーバと業務サーバが「同一セグメント内にある」からだ。

先ほど解説したとおり、Web サーバと業務サーバが同一セグメント内にあるため、通常の LB の振る舞いでは、リクエストに対応するレスポンスが返信されないという問題が生じる。それゆえ、LB が空欄あに示されたアドレス変換を行うことで、この問題を解決できることが分かる。

図 3 を見ると、リクエストのパケット④に対応する返信は、レスポンスのパケット⑤である。このパケット⑤は、業務サーバから LB 正（空欄い）に転送されていることが分かる（設問 1 の冒頭で解説したとおり、空欄いには「LB 正」が入る）。

この転送を可能とするには、パケット⑤の宛先が、どのようになっていなければならないだろうか。次の二つの候補が考えられる。

候補（a）：Web サーバの仮想 IP アドレス

候補（b）：LB

パケット⑤の宛先は、パケット④の送信元と同じである。つまり、Web サーバ 1 から業務サーバ 1 にアクセスするとき、リクエストは次のように転送されることになる。レスポンスは、この逆方向をたどる。

Web  
サーバ 1

③

LB 正

④

業務  
サーバ 1

項番	③	④
送信元	Webサーバ1	候補 (a) または 候補 (b)
宛先	業務サーバ 仮想 IP	業務サーバ 1

注) パケットの項番は、図3に合わせている。  
送信元／宛先が実IPアドレスであるとき、機器名を表記している。  
送信元／宛先が仮想IPアドレスであるとき、機器名に「仮想IP」を付与して表記している。

図：Web サーバから業務サーバへのリクエストの送信（パケット⑤が LB に転送されることを考慮した場合）

LBは、パケット③を受信してパケット④を転送するとき、通常の振る舞いに加えて、空欄あのアドレス変換を行う。すなわち、それは、送信元IPアドレスの変換である。

それでは、候補(a)、(b)のうち、どちらが正解であろうか。

結論から言うと、正解は候補(b)である。以下、二つの候補を順に解説していく。

#### ・候補(a)：Webサーバの仮想IPアドレス

Webサーバの仮想IPアドレスは、外部のクライアント端末がWebサーバにアクセスするときの宛先に指定するものである。それゆえ、このサブネットは、Webサーバ1～2、業務サーバ1～2が収容されたサブネットとは異なっている。

パケット⑤の宛先がWebサーバの仮想IPアドレスである場合、業務サーバ1は、このパケットをデフォルトゲートウェイであるLBに転送する。それゆえ、ここまで読む限りでは、パケット⑤の宛先の候補と言える。

しかし、LBがこれを受け取った後の振る舞いはどうだろうか。

LBは、振り分け先サーバとして、Webサーバ1又はWebサーバ2のいずれかを選択する。このとき、Webサーバ1が選択された場合、リクエストパケット④に対応するレスポンスパケット⑥が返信され、リクエストとレスポンスのやり取りが成立する。

一方、Webサーバ2が選択された場合、レスポンスパケット⑥はWebサーバ2に返信されてしまう。その結果、リクエストとレスポンスのやり取りが成立しなくなってしまう。

したがって、候補(a)は不正解であると結論できる。

#### ・候補(b)：LB

候補(b)の意味するところは、パケット③を受信してパケット④を転送するとき、送信元を自分のアドレスに変換するということだ。この振る舞いは、NAPTによる変換と同じである。

要するに、LBは、送信元IPアドレスを変換すると同時に、送信元ポート番号も変換しているわけだ。NAPT変換を実行すると、LBは、変換前後の送信元IPアドレス／送信元ポート番号の組をNAPTテーブルに記録しておく。

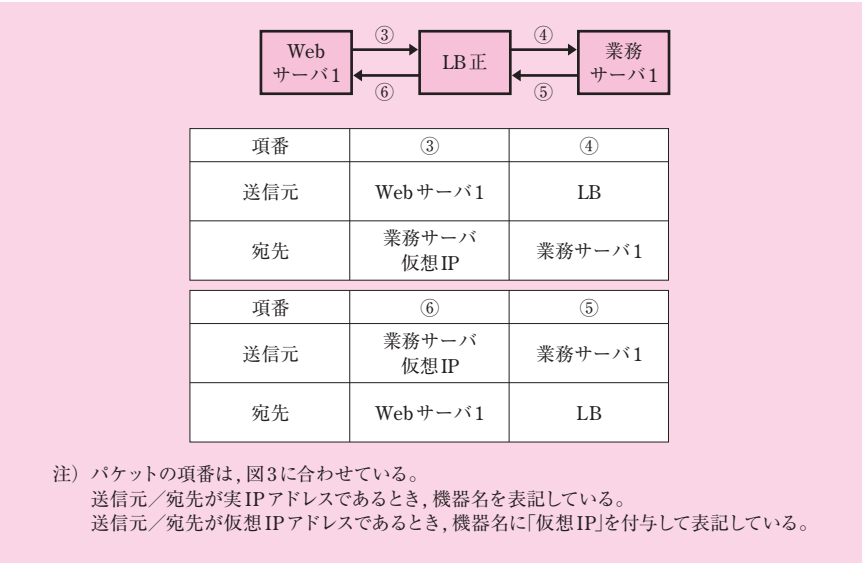
変換の結果、パケット④の送信元は、LBとなる。それに対応するレスポンスであるパケット⑤の宛先は、LBに他ならない。当然、パケット⑤はLBに転送されるわけだ。

LBは、パケット⑤を受信すると、宛先IPアドレスと宛先ポート番号を基にNAPTテーブルを走査し、宛先IPアドレスを変換する。その後、パケット⑥を転送する。

変換の結果、パケット⑥の宛先は、Webサーバ1の実IPアドレスとなる。

Webサーバ1は、パケット⑥を受信すると、これがパケット③に対応するレスポンス

スであると識別できる。こうして、リクエストとレスポンスのやり取りが成立する。  
したがって、候補 (b) が正解であると結論できる。



図：Web サーバから業務サーバへのリクエストの送信（正解）

●解の導出

前述のとおり、空欄あの実アドレス変換は、送信元 IP アドレスを、Web サーバ 1（又は Web サーバ 2）の実 IP アドレスを、Web サーバの仮想 IP アドレスに変換することであった。

よって、正解は、「送信元 IP」となる。

(2)

解答例

い：LB 正

本問は、図 3 中の空欄いに入れる適切な機器名を問うている。  
設問 1 の冒頭で解説したとおり、Web サーバから業務サーバにリクエストを送信す

るとき、業務サーバの仮想 IP アドレスを宛先に指定する。この仮想 IP アドレスは LB に設定されている。

業務サーバから Web サーバにレスポンスを返信するとき、設問 1 (1) で解説したとおり、リクエストと逆方向をたどる。

したがって、Web サーバから業務サーバへのアクセスは、リクエストもレスポンスも LB を経由する。

ただし、本問は「機器名」を問うているため、物理的に存在している機器を解答しなければならない。LB は Active-Standby 方式で冗長化されているので、実際に存在しているのは、「LB 正」と「LB 副」の 2 台である。解答に際しては、そのどちらかの機器名を答える必要がある。

本文の図 3 は、通常時に Active 側になっている系を「正」、Standby 側になっている系を「副」と記している。図 3 は「通常時」のデータの流れを示しているため、「LB 正」を経由することが分かる。

実際、図 3 中には、同じく冗長化された FW、LB がそれぞれ「FW 正」「LB 正」と記されているので、空欄いもこれに倣って解答すべきことは明らかだ。

よって、正解は、「LB 正」となる。

### (3)

#### 解答例

①

本問は、図 3 中の①～⑧のパケットのうち、送信元 IP アドレスが②と同じになるものを問うている。

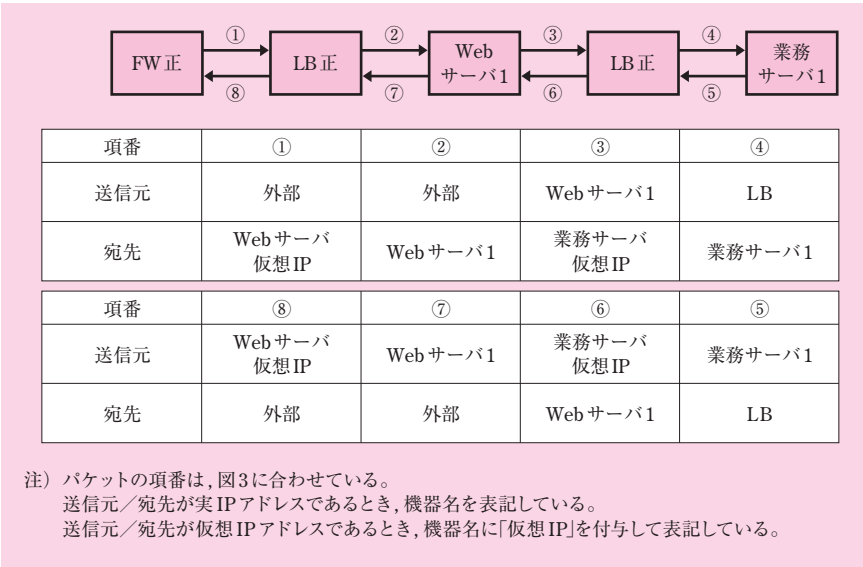
外部から Web サーバにアクセスするときのパケットは、設問 1 の冒頭で解説したとおり、図「外部から Web サーバへのアクセス」となる。この図には、リクエスト方向のパケット①、②、及び、そのレスポンス方向のパケット⑦、⑧が記されている。

Web サーバから業務サーバにアクセスするときのパケットは、設問 1 (1) で解説したとおり、「Web サーバから業務サーバへのリクエストの送信（正解）」となる。この図には、リクエスト方向のパケット③、④、及び、そのレスポンス方向のパケット⑤、⑥が記されている。

したがって、図 3 中の①～⑧のパケットについて、その送信元 IP アドレスと宛先 IP アドレスを全て記すと、次の図のとおりとなる。なお、この図では、Web サーバ 1、



業務サーバ 1 が振り分け先に選択されたものとしている。



図：サーバにアクセスするときのデータの流れ

パケット②の送信元 IP アドレスは, 「外部」である。具体的に言うと, 保守センターの PC, 又は, 外出先の保守端末を指している。  
これと同じ送信元 IP アドレスをもつパケットは①である。  
よって, 正解は, 「①」となる。

(4)

解答例

⑥

本問は, 図 3 中の①～⑧のパケットのうち, 宛先 IP アドレスが②と同じになるものを問うている。  
設問 1 (3) で解説したとおり, 図 3 中の①～⑧のパケットの送信元 IP アドレスと宛先 IP アドレスを全て記したものは, 図「サーバにアクセスするときのデータの流

れ」となる。

パケット②の宛先 IP アドレスは、「Web サーバ 1」である。これと同じ宛先 IP アドレスをもつパケットは⑥である。

よって、正解は、「⑥」となる。

■設問 2  
(1)

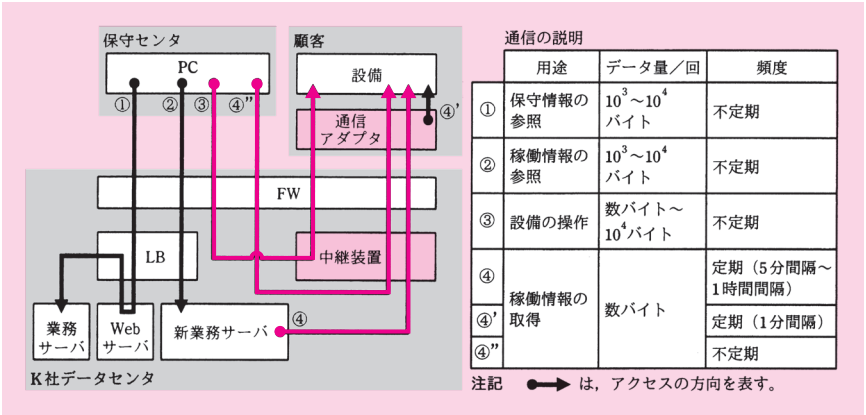
解答例

う：中継装置  
え：通信アダプタ  
お：リバース

空欄う～おを含む文章は、「保守システムの機能強化」の第5段落にある。その中には、「この稼働情報取得案に従うと、  う  はフォワードプロキシ、  え  は  お  プロキシとして動作しているとみなすことができる」と記述されている。

稼働情報取得案は、第2～第4段落、図4「機能強化に伴う導入機器の設置場所」、図5「機能強化後の通信の概要」に記されている。

通信は全部で6種類ある。図5には、各通信の経路、用途等の説明が記されている。



図：本文の図5の再掲「機能強化後の通信の概要」

6種類ある通信のうち、中継装置と通信アダプタを経由しているのは、③、④'、④の3種類である。

③、④'、④の通信で指定する URI について、第3段落の6番目の箇条書きに、

http://（設備を指定するための FQDN）/（リソース名）

と記述されている。

中継装置と通信アダプタの役割について、第4段落の2番目の箇条書きの中で、「中継装置と通信アダプタは、稼働情報に関する GET リクエストを中継する際に、自装置がキャッシュしている最新の稼働情報よりも新しい稼働情報を取得するように、HTTP ヘッダ [If-Modified-Since : x] を付加する (x は時刻)。そして、新しい稼働情報が得られない場合には、自装置がキャッシュしている最新の稼働情報を利用する」と記述されている。

つまり、

- [1] URI は設備を指定しているが、中継装置と通信アダプタを経由している
- [2] 中継装置と通信アダプタは、自装置がキャッシュしている稼働情報よりも新しい稼働情報がサーバ側にある場合に限り、その新しい稼働情報を返信する。さもなければ、キャッシュしている情報を返信する

ということが分かる。

結論から言うと、特に項番 [2] の振る舞いから、「中継装置と通信アダプタがプロキシである」と言える。この振る舞いは、まさにプロキシが通常行っているものだからだ。

これを実現するには、先ほど引用した本文に記されているとおり、HTTP のヘッダフィールド [If-Modified-Since : x] を付与した GET リクエストを発行する。これは「条件付き GET」(conditional GET) と呼ばれている。「x」に指定するのは、プロキシが保持しているコンテンツ情報のタイムスタンプである。

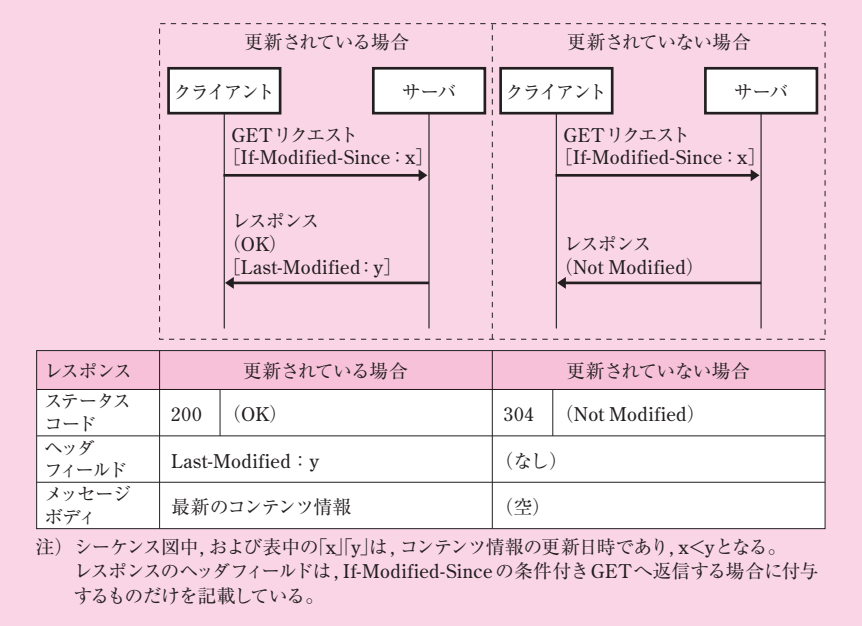
指定された URI のコンテンツがサーバに存在する場合、「x」以降に更新されているか否かによって、サーバが返信するレスポンスは異なる。

更新されているとき、最新のコンテンツ情報をメッセージボディに格納して返信する。その際、ヘッダフィールド [Last-Modified : y] を付与する。「y」に指定するのは、サーバが保持している最新のコンテンツ情報のタイムスタンプである。

更新されていないとき、ステータスコードを 304 番 (Not Modified) に設定し、メッ

セージボディを空のまま返信する。このメッセージボディの転送時間が削減されるため、応答性能が向上する。

なお、「x」の指定が不正であるか、サーバの現在日時より大きい場合、通常の GET リクエストを受け取ったときと同じ処理をする。



図：条件付き GET (If-Modified-Since) の送受信

以上、項番 [2] の振る舞いから、中継装置と通信アダプタがどちらもプロキシであることが分かった。

さて、空欄う～おを含む文章を見てみると、「はフォワードプロキシ、はプロキシとして動作しているとみなすことができる」とあるので、プロキシの種類を踏まえて解を導く必要があることが分かる。

プロキシにはフォワードプロキシとリバースプロキシの2種類がある。この点を具体的に示すと、次のように中継装置と通信アダプタを設定する。

● 中継装置

中継装置はクライアント側にあるので、これをフォワードプロキシとして動作させる。

具体的に言うと、クライアント側のブラウザで、中継装置をプロキシに指定する。

その結果、クライアントが送信する全ての HTTP 通信（80 番ポートの TCP 通信）は、中継装置と TCP コネクションを確立する。そして、中継装置に対し、次の GET リクエストを発行する（HTTP のバージョンを 1.1 とする）。GET リクエストの URL は、絶対パスを指定する。

`GET http://（設備を指定するための FQDN）/（リソース名）HTTP/1.1`

### ● 通信アダプタ

通信アダプタはサーバ側にあるので、これをリバースプロキシとして動作させる。

具体的に言うと、DNS サーバ（又は中継装置の hosts ファイル）にて、設備を指定する FQDN（ホスト名）に、通信アダプタの IP アドレスを対応付ける。その結果、ブラウザから見ると装置にアクセスしているが、実際には通信アダプタにアクセスしている。

なお、通信アダプタは、自ら定期的に 1 分間隔で設備にアクセスし、コンテンツをキャッシュしている。フォワードプロキシとは異なり、リクエストをそのまま中継しているわけでないことに留意しておこう。

よって、空欄うには「中継装置」、空欄えには「通信アダプタ」、空欄おには「リバース」がそれぞれ該当する。

### ●参考：通信アダプタを多段プロキシ（フォワードプロキシ）とする解

正確に言うと、通信アダプタは、前述のとおりリバースプロキシとして動作させるか、又は、中継装置を多段プロキシとして動作させるか、そのいずれかが可能である。後者の場合、通信アダプタはフォワードプロキシとなる。

しかし、後者では空欄おに当てはまらないため、これは正解ではない。空欄いがフォワードプロキシであるため、文脈上、それとは異なる字句が空欄おに入らなければならないからだ。

更に、通信アダプタが多段プロキシであることを示唆する記述が、本文に一切ない。多段プロキシの設置は一般的なものではないので、本文に記されていない特殊な設定を付け加えるべきではない。その点からも、これは正解ではないと言える。

## (2)

## 解答例

稼働情報の収集周期の変更が容易である。(19字)

問題文は、「本文中の下線(a)の利点を……述べよ」と記述されている。

下線(a)は、「保守システムの機能強化」の第4段落の3番目の箇条書きにある。そこには、「④の通信では、……(a)稼働情報取得のトリガは、設備ではなくK社データセンタ側にあるが、それは運用上の利点となっている」と記述されている。

項番④の通信は、稼働情報を取得する目的で、新業務サーバから設備に対し定期的を実施するものである。そのトリガについて、第3段落の4番目の箇条書きで、「収集周期は、サービス開始時は1時間とし、段階的に5分程度に短縮しサービス品質を向上させる」と記述されている。この点と調和して、図5の中で、通信の頻度は「定期(5分間隔～1時間間隔)」と記されている。

一般的に言って、本事例に登場する設備(様々な用途の空調設備)は、新業務サーバと比べて、限定的な情報通信機能しか装備していないと考えられる。したがって、収集周期の段階的な短縮という高度な制御は、新業務サーバの方が容易に実施できる。

更に、同じく第3段落の4番目の箇条書きで、「設備はいつも通電されているとは限らない」と記述されており、そもそも稼働監視の対象になっていることからしても、設備の稼働率は新業務サーバよりもずっと低いと考えられる。設備が通電していない間、情報取得のトリガを発生させることも、トリガの周期を変更することもできない。設備がこのような不安定な状況に置かれていることも考え合わせるなら、収集周期の段階的な短縮は、新業務サーバが実施すべきである。

よって、正解は、「稼働情報の収集周期の変更が容易である」となる。

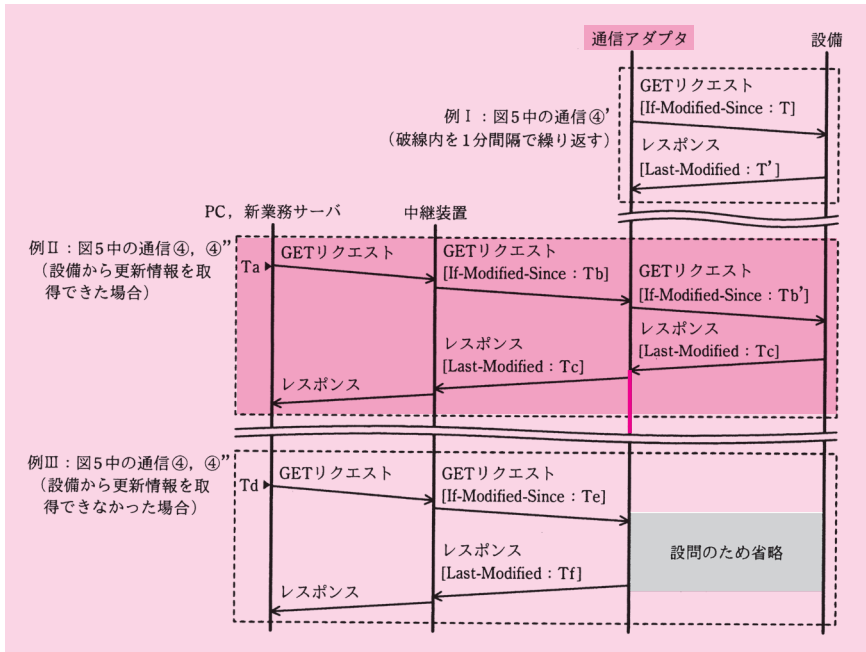
## (3)

## 解答例

Tc

問題文は、「図6中の例Ⅱのシーケンスによって、通信アダプタのキャッシュが更新される。更新後の最新稼働情報のタイムスタンプの時刻を答えよ」と記述されている。

具体的に問われているのは、次の図の赤線で示した位置における、通信アダプタが保持しているキャッシュの時刻である。



図：設問2(3)で問われている箇所(本文の図6を掲載)

設問2(1)でHTTPヘッダ [If-Modified-Since : x] の振る舞いについて解説したとおり、指定日時「x」以降にコンテンツ情報が更新されているか否かによって、設備が返信するレスポンスは異なってくる。

### [1] 更新されている

設備は、最新のコンテンツ情報を返信する。レスポンスのHTTPヘッダに、[Last-Modified : y] が付与される。yは最新のコンテンツ情報のタイムスタンプであり、 $x < y$  を満たす。

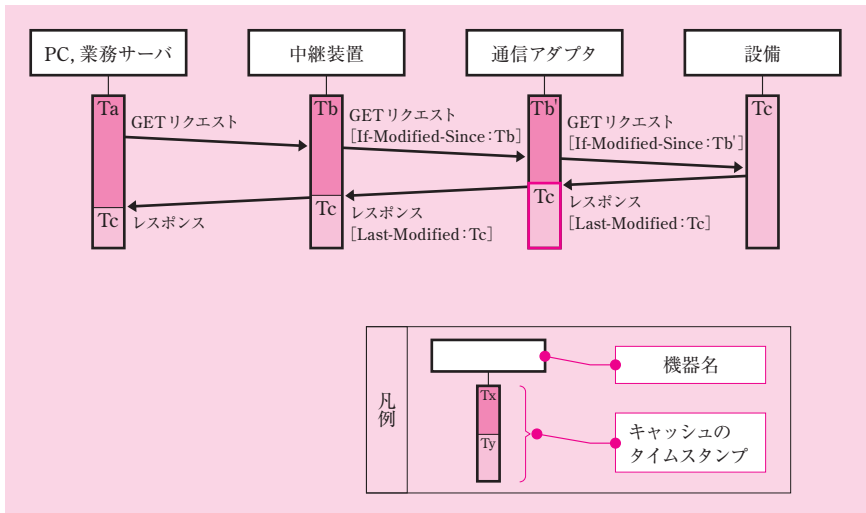
### [2] 更新されていない

設備は、コンテンツを返信しない。レスポンスのステータスコードに、304番 (Not Modified) を設定し、更新されていない旨を通知する。

例Ⅱのシーケンスは、設備の更新情報を取得できた場合のやり取りである。したがって、前述の項番 [1], [2] のうち、例Ⅱのシーケンスに該当するものは、項番 [1] の方である。

各機器がキャッシュしているコンテンツ情報のタイムスタンプを明確にするため、図6の縦線（シーケンス図のライフライン）の位置に、これを書き加えてみよう。

例Ⅱのシーケンス部分を抜粋すると、次の図のようになる。



図：例Ⅱのシーケンス（タイムスタンプを明記）

通信アダプタのシーケンスを解説する。

例Ⅱのシーケンスの開始時点で、通信アダプタのキャッシュのタイムスタンプは、「Tb'」である。そうように言える理由は、通信アダプタから設備に発行した GET リクエストの [If-Modified-Since: Tb'] ヘッダ中の時刻が、その時点で保持しているキャッシュのタイムスタンプを示しているからだ。すなわち、それは「Tb'」である。

この GET リクエストに対するレスポンスには、[Last-Modified: Tc] ヘッダが付与されている。したがって、時刻「Tb'」より後の時刻「Tc」に更新されたコンテンツ情報を設備が保持しており、設備がそのコンテンツ情報を返信したことを意味している。

図6中の各時刻の前後関係について、第7段落に記述されているので、確認しておこう。そこには

$$Tb' < Tc$$



とあるので、「Tb'」より「Tc」が後であることが分かる。

そのコンテンツ情報を受け取った時点で、通信アダプタはキャッシュを更新する。したがって、この時点以降、通信アダプタが保持しているキャッシュのタイムスタンプは、「Tc」である。

よって、正解は、「Tc」となる。

#### (4)

##### 解答例

中	継	装	置	よ	り	通	信	ア	ダ	プ	タ	の	キ	ャ	ッ	シ	ユ	の	更	新	頻	度	が	高
く	新	し	い	か	ら	(31字)																		

問題文は、「図6中の例ⅡのGETリクエストの中継において、TbとTb'は異なる場合が多いが、それはなぜか。キャッシュに着目して……述べよ」と記述されている。

図6中の各時刻の前後関係が、第7段落に記述されている。TbとTb'の前後関係は

$$Tb \leq Tb'$$

とある。つまり、「Tb = Tb'」となる事象と「Tb < Tb'」となる事象の2通りがあるわけだ。

問題文にある「TbとTb'は異なる場合が多い」とあるが、大小関係は比較により定まるので、何と比べて「多い」と述べているのだろうか。「Tb = Tb'」より「Tb < Tb'」となる方が多い、と普通は解釈できるはずだ。

しかし、そのように考えを進めてしまうと、「なぜ多いのか」を解き明かすことができなくなる。詳しくは後述するが、「Tb = Tb'」となる事象と「Tb < Tb'」となる事象のそれぞれの確率について、本文からは何も読み取れないからだ。更に言えば、そのような確率の問題はネットワークスペシャリスト試験の出題趣旨から大きく逸脱しているので、これ以上、深入りしない方が賢明である。

要は、問題文に「異なる場合が多い」とあるけれど、過度にとらわれないようにしたい。ここでは、根拠を特に示さずに、「異なる場合が意外と多いようだ」という注釈を述べたに過ぎないのだろう。

むしろ注目すべきは、問題文に「キャッシュに着目して」と記されていることであ

る。この記述から、キャッシュの働きを問うていることが明らかだ。これこそネットワークスペシャリスト試験にふさわしいテーマである。

そこで、本書は、問題文を次のように読み替えることにする。こうすれば、出題趣旨であるキャッシュに着目して、解を導きやすくなるはずだ。

**【出題趣旨を踏まえ、本書が作成した問題文】**

図6中の例ⅡのGETリクエストの中継において、 $Tb$ と $Tb'$ は異なる場合があるが、それはなぜか。キャッシュに着目して、35字以内で述べよ。

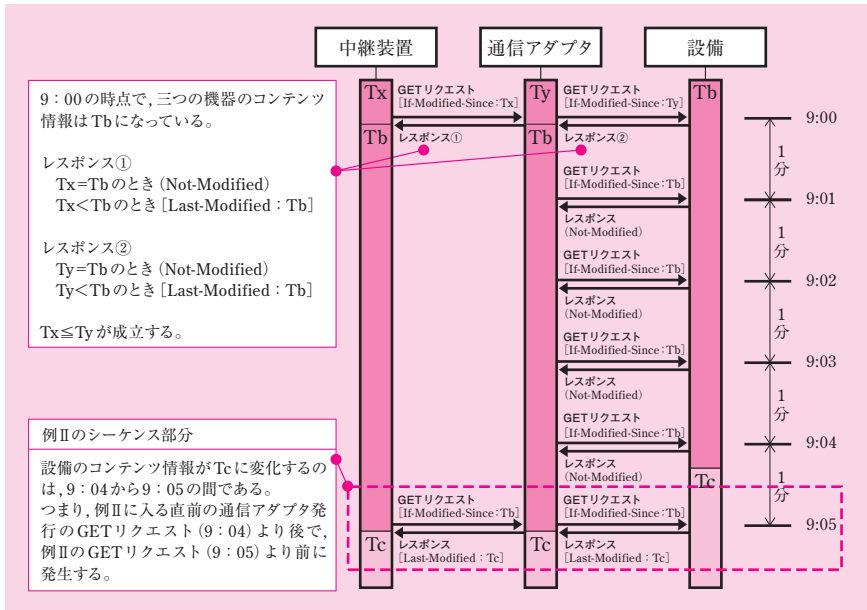
※変更箇所を下線で示す

前置きが長くなったが、いよいよ解を導こう。

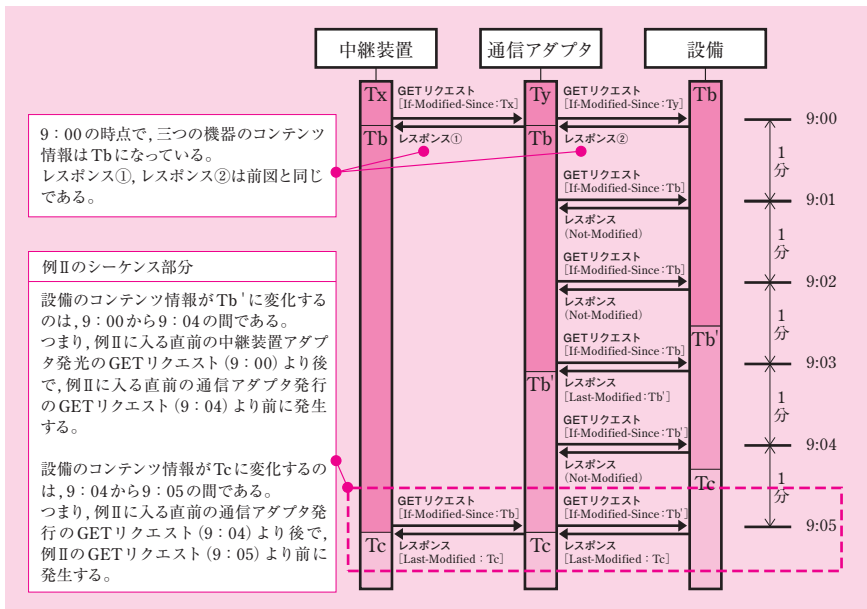
前述のとおり、例Ⅱのシーケンスには、「 $Tb = Tb'$ 」となる事象と「 $Tb < Tb'$ 」となる事象がある。

二つの事象それぞれについて、例Ⅱに至るシーケンスを次の図に示す。

ここでは、中継装置から通信アダプタに向けて、9:00と9:05にGETリクエストをそれぞれ発行している（図5の④の通信）。その間、通信アダプタから設備に向けて、9:00から1分間隔で、GETリクエストをそれぞれ発行している（図5の④'の通信）。例Ⅱのシーケンスに該当する部分は、9:05である。



図：例Ⅱに至るシーケンス (Tb = Tb')



図：例Ⅱに至るシーケンス (Tb < Tb')

このとき、例Ⅱのシーケンスが生じるには、次に示す条件が成立していなければならない。

**【例Ⅱのシーケンスが生じる条件】**

- 9:05 に中継装置が GET リクエストを [If-Modified-Since: Tb] の条件付きで発行していることから、前回の 9:00 に稼働情報取得が完了した時点で、中継装置、通信アダプタ、設備の稼働情報は Tb になっている。
- 9:05 に通信アダプタが GET リクエストを [If-Modified-Since: Tb'] の条件付きで発行していることから、「Tb = Tb'」の事象においては、9:00～9:04 の間に設備の稼働情報が変化していない。一方、「Tb < Tb'」の事象においては、9:00～9:04 の間に設備の稼働情報が 1 回以上変化し、Tb' になっている（前図では、9:02～9:03 の間に 1 回変化した例を示している。実際には、任意の 1 分間隔で複数回の変化が生じてよい）。
- 9:05 に設備がレスポンスに [Last-Modified: Tc] を付けて返信していることから、9:04～9:05 の間に設備の稼働情報が Tc に変化している。

本書が読み替えた問題文は、「Tb と Tb' は異なる場合があるのはなぜか」を問うている。Tb と Tb' が異なるのは、要するに、「Tb < Tb'」の事象である。

このとき、9:00～9:04 の間に、設備の稼働情報が変化している。その時刻を Tb' としよう。通信アダプタは 1 分間隔で GET リクエストを発行しているため、その変化に追従することができ、通信アダプタがキャッシュしているタイムスタンプが、Tb から Tb' に変化する。

一方、中継装置は、（この解説では）5 分間隔で GET リクエストを発行しているため、9:00～9:04 の間に生じた変化に追従することができず、中継装置がキャッシュしているタイムスタンプは Tb のままである。

それゆえ、9:05 の時点で、「Tb < Tb'」になっているわけだ。

よって、正解は、「中継装置より通信アダプタのキャッシュの更新頻度が高く新しいから」となる。

**●参考：事象「Tb = Tb'」と事象「Tb < Tb'」の発生確率の比較**

本書が読み替えた問題文は、「Tb と Tb' は異なる場合があるが、それはなぜか」となっている。

仮に、通信アダプタが自律的に 1 分間隔で稼働情報を取得しなかったならば（つま

り、中継装置からのリクエストを中継するだけであれば), 必ず「 $Tb = Tb'$ 」になる。「 $Tb$ と $Tb'$ は異なる場合がある」のは、まさにキャッシュの効果であると言えよう。

元の問題文は、「 $Tb$ と $Tb'$ は異なる場合が多いが、それはなぜか」と記されている。「多い」かどうかを判断するには、キャッシュとは別の要因も併せて検討する必要がある。

問題文を素直に読めば、事象「 $Tb = Tb'$ 」より事象「 $Tb < Tb'$ 」の発生確率が大きいのはなぜかを問うている、と解釈できるだろう。その点について、簡潔に触れてみたい。

ただし、あらかじめ断っておくが、次に述べることは、ネットワークスペシャリスト試験の範囲を逸脱した、確率に関する問題を扱っている。興味がない読者は読み飛ばしていただいて一向に差し支えない。

本事例の設備は、オフィスや工場の空調設備である。取得する稼働情報の内訳について、[保守システムの機能強化]の第1段落には、「稼働情報（運転実績、維持温度）」とだけ簡潔に述べられている。詳細は不明だが、設備電源のON / OFF、運転モード、風量、維持温度、等が含まれているのだろう。

稼働情報が変化する確率は、時間帯によって異なるはずだ。出勤時間帯であれば、最初に出社した人がONに変化させるだろう。更には、天候の影響もかなり受けるはずだ。夏場や冬場の勤務時間帯には、自動運転又は手動操作による調整が、適宜行われるだろう。

単刀直入に言って、稼働情報の変化がどれほどの頻度で生起するのか、その予測は困難だ。何らかの条件を設定しない限り、確率を求めることはできない。

そこで、(机上の空論かもしれないが、) ある短い時間帯に限定した場合、「稼働情報変化がランダムに生起する」という仮説を立てる。例えば、冬場の朝方の時間帯(9時台)に限定し、空調設備の維持温度等の変化に着目する。当該時間帯の中で、9:01に変化する日があったり、9:05と9:45に変化する日があったり、あるいは、変化しない日があったりする、という具合に、稼働情報変化がランダムに起きるわけだ。

ランダムに生起する出来事について、その発生回数はポアソン分布に従うことが知られている。ある時間帯において、稼働情報変化という出来事が起きる確率を「 $\lambda$ 」(1分あたりに生起する回数)とし、ポアソン分布を使って計算してみよう。

例Ⅱのシーケンスに至る二つの事象は、どちらも、前述の「例Ⅱのシーケンスが生じる条件」が成立していなければならない。そこで、この条件が発生したという前提の下、確率(条件付き確率)を求めてみよう。

- 事象「 $Tb = Tb'$ 」

N 分間に、出来事が 0 回起きる確率は、次式となる。この解説では、9:00 ~ 9:04 の 4 分間を考えているので、 $N=4$  となる。

$$e^{-N\lambda} \quad \text{式 (1)}$$

- 事象「 $Tb < Tb'$ 」

N 分間に、出来事が 1 回以上起きる確率は、次式となる。同じく、9:00 ~ 9:04 の 4 分間を考えているので、 $N=4$  となる。

$$1 - e^{-N\lambda} \quad \text{式 (2)}$$

「 $Tb$  と  $Tb'$  は異なる場合が多い」という問題文の主張は、式 (1) より式 (2) の値が大きくなる場合、正しい。 $N=4$  を代入して  $\lambda$  を求めると、「 $0.17... < \lambda$ 」という不等式が成立すれば、式 (2) の方が大きくなる。つまり、1 分当たり 0.17 回以上（同じことだが、1 時間当たり 10.4 回以上）、稼働情報変化が起きる場合、問題文の主張と言える。

詳細は省くが、中継装置による稼働情報取得の間隔が 1 時間のときは、 $N=59$  となる。以上、大胆な仮説に基づく机上の検討であるが、参考になれば幸いである。

## (5)

### 解答例

① 設備と T C P コネクションが確立できない場合 (21 字)

② 設備が N o t M o d i f i e d を応答した場合 (22 字)

問題文は、「図 6 中の例Ⅲの通信シーケンスになるのは、どのような場合が考えられるか。通信アダプタと設備の間の通信に着目して二つ（挙げよ）」と記述されている。

図 6 中の例Ⅲを見ると、「設備から更新情報を取得できなかった場合」と記されている。したがって、考えられるのは次の二つケースである。

[1] 設備との間で通信障害が発生し、そもそも取得できなかった

[2] 設備の稼働情報が更新されていないため、「更新情報」を取得できなかった

まず、項番 [1] から解を導こう。

これは、一般的な知識に基づき、何らかの通信障害について具体的に言及すればよいだろう。

よって、正解は、「設備と TCP コネクションが確立できない場合」などとなる。

次いで、項番 [2] から解を導こう。

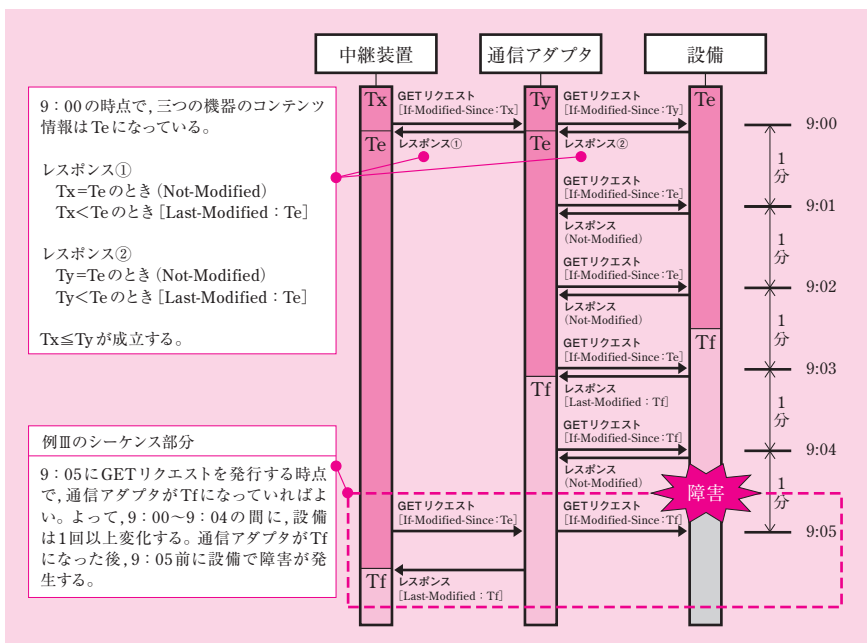
If-Modified-Since の条件付きで発行した GET リクエストにおいて、指定されたコンテンツ情報が更新されていないときは、設問 2 (1), (3) で解説したとおり、「Not Modified」の応答が返ってくる。

解答に際し、HTTP の仕様についてどの程度まで詳しく述べるべきか、判断に迷うかもしれない。そのときは、本文にどこまで詳しく説明されているのかを参考にするとういだろう。

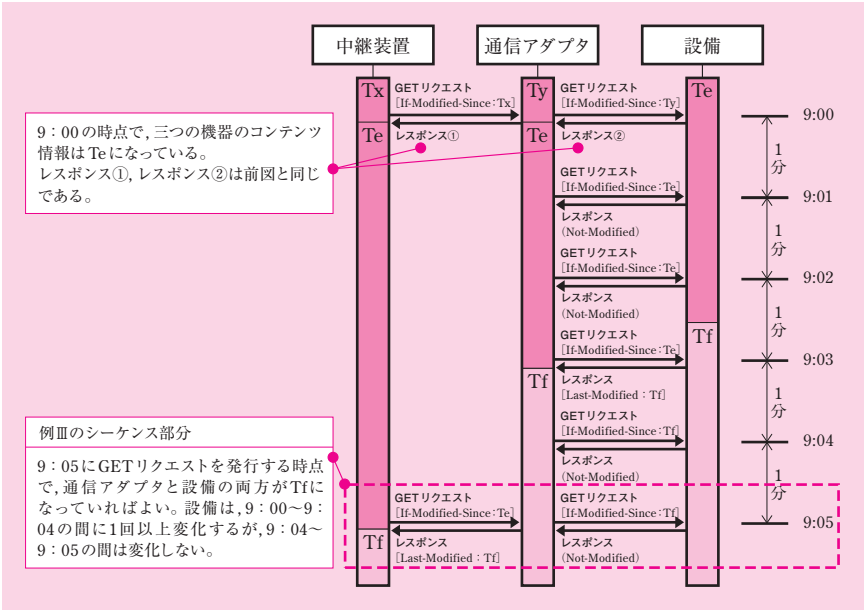
本文には、条件付き GET リクエストについて、If-Modified-Since や Last-Modified などのヘッダフィールド名を使って具体的に説明している。したがって、ここでは「Not Modified」というステータス名を解答しておくべきだと言えよう。

よって、正解は、「設備が Not Modified を応答した場合」などとなる。

参考までに、図 6 中の省略部分を埋めて、例Ⅲに至る二つのケースについて、それぞれシーケンス図を示しておこう。



図：例Ⅲに至るシーケンス（通信障害）



図：例Ⅲに至るシーケンス (Not Modified)

(6)

解答例

電源断などで設備との通信ができない場合の稼働情報が古くなる。(30字)

問題文は、「図6中の例Ⅰの周期を長くした場合（例えば1分間隔から2分間隔へ変更）、HTTPクライアントが受け取る応答への影響を……述べよ」と記述されている。

図6中の例Ⅰを見ると、「図5中の通信④」と記されている。これは、通信アダプタが1分間隔で設備から稼働情報を取得する通信である。

この通信のHTTPクライアントは、通信アダプタとなる。したがって、本問は、通信④'の周期を長くした場合、通信アダプタが受け取る応答がどのような影響を受けるかを問うている。

周期が長くなった場合、通信アダプタが受け取る稼働情報はどのように変化するだろうか。



当然ながら、通信アダプタが保持しているキャッシュ情報と、設備の実際の稼働情報との間で、ずれが生じるケースが増えてくる。要するに、キャッシュ情報が陳腐化する度合いが、よりいっそう大きくなる。

この点について、具体例を挙げて説明しよう。

通信アダプタが9時04分に収集した後、9時04分30秒の時点で設備が故障したとする。

1分間隔で収集した場合、9時05分の時点で、通信アダプタのキャッシュ情報には、設備の故障が反映される。

しかし、2分間隔で収集した場合、9時05分の時点で、通信アダプタのキャッシュ情報にその事実が反映されない。なお悪いことに、中継装置が9時05分に収集した時点で、中継装置のキャッシュ情報にも反映されないことになる。

このように、周期が長くなった場合、通信アダプタが受け取る稼働情報が古くなってしまうわけだ。

さて、ここで考察を止めてしまうと、本問の解は「通信アダプタが受け取る稼働情報が古くなるため」と思えるだろう。

しかし、試験センターの解答例は、「電源断などで設備との通信ができない場合の稼働情報が古くなる」となっている。つまり、わざわざ「電源断などで設備との通信ができない場合」と具体的に記されているのだ。

これはなぜだろうか。

●試験センターの解答例にある「電源断などで設備との通信ができない場合」について  
本事例の「稼働情報」の中身について熟考すると、この解答例の適切さが理解できる。  
取得する稼働情報の内訳について、[保守システムの機能強化]の第1段落には、「稼働情報（運転実績、維持温度）」とだけ簡潔に述べられている。

「維持温度」は読んで字のごとくであるが、「運転実績」は何を表しているのだろうか。  
詳細は不明だが、少なくとも、設備電源のON / OFFは含まれているはずだ。他には、運転モード（冷房／暖房）、風量等、より細かい情報が含まれているのかもしれない。

これらの情報の中で、最も大切なものは、設備電源のON / OFFであるに違いない。「稼働」情報という呼び名が用いられていることから、これが主たるものと推察できる。

空調設備の稼働情報（運転実績、維持温度）のうち、設備電源のON / OFFは重要度が高い。そのため、できるだけキャッシュが陳腐化しないことが望ましい。それ以外の情報は、どちらかというと付随的なものだろうし、そもそも分刻みで頻繁に変化する性質のものではないため、キャッシュの陳腐化はさほど問題視されないだろうと

考える。

ここまで考察を進めるなら、正解は解答例のとおりとなる。

## ■設問 3

### (1)

#### 解答例

#### か：通信アダプタ

空欄かを含む文章は、[次世代設備に関する通信方式]の第2段落にある。その中には、「M君は、(b) TCP 上の HTTP を UDP 上の CoAP に置き換えることによって、通信アダプタと中継装置を用いた通信の TAT (Turn Around Time) を向上させることができると判断した。また、その際 FW の設定を変更しなくてもよいように、HTTP と CoAP の変換機能は、図 5 中の か に実装することにした」と記述されている。

CoAP (Constrained Application Protocol) について、第 1 段落の最初と 2 番目の箇条書きには次のように記述されている。

- ・ CoAP は、UDP 上で動作可能な、HTTP に似た通信プロトコルである。
- ・ HTTP リクエストを CoAP リクエストに変換したり、CoAP レスポンスを HTTP レスポンスに変換したりすることもできる。

CoAP の検討は、次世代設備向けに効率の良い通信を調査する過程で、行われている。その点は、[保守システムの機能強化]の第9段落にある N 氏の 2 番目の発言の中で、「次世代設備では、……HTTP 以外の通信プロトコルも実装できる。……次世代設備向けにもっと効率が良い通信方式がないか調査して報告してほしい」と記述されていることから分かる。

したがって、CoAP 通信のサーバに相当するもの、すなわち、CoAP リクエストの受信と CoAP レスポンスの返信を行うのは、次世代設備である。

一方、CoAP 通信のクライアントに相当するもの、すなわち、CoAP リクエストの送信と CoAP レスポンスの受信を行うのが、空欄かの機器である。

空欄かの機器は、更に、HTTP と CoAP の変換機能も実装する。それゆえ、空欄かの機器は、HTTP 通信のクライアントではない。図 5 中の通信に当てはめると、PC、新業務サーバではないことが分かる。

したがって、空欄かの候補は、図5中で通信を中継している機器に絞られる。つまり、中継装置、又は、通信アダプタのいずれかだ。

どちらの機器もプロキシなので、TCPコネクションの終端になっている。したがって、TCP上のHTTPを、UDP上のCoAPに変換して転送することができる。

中継装置に変換機能を実装する場合、次の手順で通信が行われる。

- **中継装置が変換する場合**

- [1] クライアント（PC又は新業務サーバ）は、HTTPリクエストを送信する
- [2] 中継装置は、HTTP通信のフォワードプロキシと変換装置を兼用する。HTTPリクエストをCoAPリクエストに変換し、CoAPリクエストを送信する
- [3] 通信アダプタは、CoAP通信のリバースプロキシとなる。CoAPリクエストを転送する
- [4] 設備は、CoAPリクエストを受信し、リクエストに対応するCoAPレスポンスを返信する
- [5] 通信アダプタは、CoAPレスポンスを転送する
- [6] 中継装置は、CoAPレスポンスをHTTPレスポンスに変換し、HTTPレスポンスを返信する
- [7] クライアントは、HTTPレスポンスを受信する

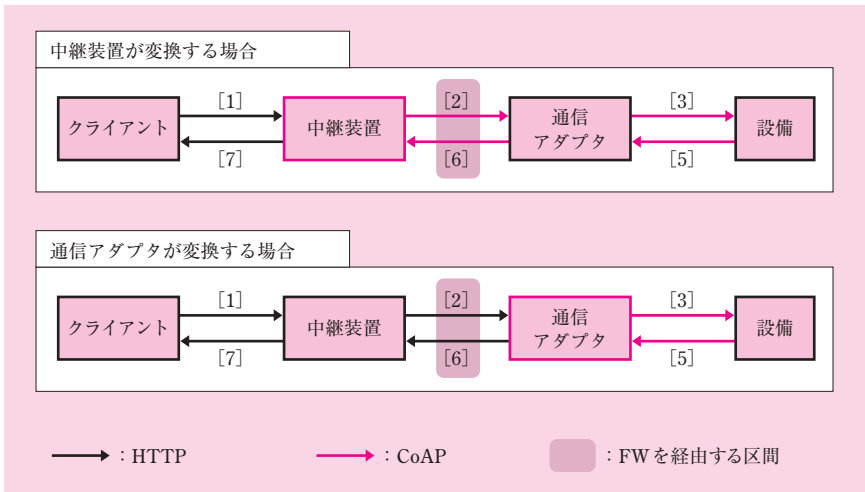
通信アダプタに変換機能を実装する場合、次の手順で通信が行われる。

- **通信アダプタが変換する場合**

- [1] クライアント（PC又は新業務サーバ）は、HTTPリクエストを送信する
- [2] 中継装置は、HTTP通信のフォワードプロキシとなる。HTTPリクエストを転送する
- [3] 通信アダプタは、HTTP通信のリバースプロキシと変換装置を兼用する。HTTPリクエストをCoAPリクエストに変換し、CoAPリクエストを送信する
- [4] 設備は、CoAPリクエストを受信し、リクエストに対応するCoAPレスポンスを送信する
- [5] 通信アダプタは、CoAPレスポンスをHTTPレスポンスに変換し、HTTPレスポンスを返信する
- [6] 中継装置は、HTTPレスポンスを転送する
- [7] クライアントは、HTTPレスポンスを受信する

本文には、「FWの設定を変更しなくてもよい」という点を考慮に入れて、空欄かの機器でHTTPとCoAPを変換させている。FWは中継装置と通信アダプタ間にあるので、前述の手順では項番[2]、[6]に該当する。

これまで解説した内容を、図にまとめてみよう。図中の項番は、前述の手順である。



図：HTTPとCoAPを変換する装置

図5の通信は全てHTTPで行われているため、FWはHTTPを通過させている。CoAPはHTTPとは異なるUDP上の通信なので、設定を変更しない限り、FWはこれを遮断する。それゆえ、項番[2]、[6]は、従来どおりHTTPでなければならない。したがって、HTTPとCoAPの変換機能は、通信アダプタに実装する必要がある。よって、空欄かに該当する機器名は、「通信アダプタ」となる。

## (2)

### 解答例

IPヘッダとUDPヘッダ (12字)

問題文は、「図7中のCoAPメッセージ以外に、IEEE802.15.4フレームのデータ部に含まれるデータを、……答えよ」と記述されている。

IEEE802.15.4 について、〔次世代設備に関する通信方式〕の第1段落の4番目の箇条書きで、「ZigBee に用いられる IEEE802.15.4 フレーム」と記述されている。ZigBee について、〔保守システムの機能強化〕の第9段落にある N 氏の2番目の発言の中で、「次世代設備では、通信インタフェースとして、低電力でも稼働できる ZigBee を採用する」と記述されている。したがって、IEEE802.15.4 は、次世代設備の通信インタフェースであることが分かる。

本問は、IEEE802.15.4 フレームのデータ部を問うている。したがって、解を導くには、この IEEE802.15.4 が OSI 基本参照モデルのどの階層に位置付けられるのかを知る必要がある。

この点について、本文中にヒントが用意されている。〔次世代設備に関する通信方式〕の第1段落の4番目の箇条書きで、「ZigBee に用いられる IEEE802.15.4 フレームのデータ部は、IEEE802.3 (Ethernet) フレームのデータ部よりもかなり短く、CoAP のメッセージ形式は、それに適したものになっている」と記述され、IEEE802.15.4 フレームと IEEE802.3 (Ethernet) フレームを、データ部の最大転送長 (MTU) の観点から対比している。

この記述から、IEEE802.15.4 の階層は、OSI 基本参照モデルにおいて、IEEE802.3 (Ethernet) と同じ位置にあると推論できる。それゆえ、第2階層以下である。

したがって、IEEE802.15.4 フレームのデータ部には、第3階層以上が格納される。CoAP メッセージは UDP 上であるので、データ部分は、IP、UDP、CoAP となる。このうち、問題文は「CoAP メッセージ以外」のものを解答するよう求めている。

よって、正解は、「IP ヘッダと UDP ヘッダ」となる。

### ●参考：ZigBee とは

ZigBee (IEEE802.15.4) とは、短距離無線通信の規格である。使用周波数帯域は（日本国内では）2.4GHz 帯の ISM バンドである。伝送速度は低く通信距離も短い、安価で省電力であるという長所をもつ。ZigBee 端末は転送機能を有し、直接電波の届かない端末間でも通信できる。ZigBee 端末は多数の端末と通信でき、大規模なメッシュ状のトポロジを形成できる。安価で省電力であるという特性を生かし、ビル内のセンサネットワークなど低速通信に用いられている。

## (3)

## 解答例

① T C P コネクションの確立と終了の手順が不要である。 (25字)

② C o A P はヘッダ長が短いなど、データの格納効率が良い。 (27字)

問題文は、「本文中の下線 (b) について、TAT の向上に寄与する、CoAP と UDP の特長を二つ (挙げよ)」と記述されている。

下線 (b) を含む文章は、「次世代設備に関する通信方式」の第2段落にある。その中には、「(b) TCP 上の HTTP を UDP 上の CoAP に置き換えることによって、通信アダプタと中継装置を用いた通信の TAT (Turn Around Time) を向上させることができる」と記述されている。

「通信の TAT」とは、通信処理が開始してから終了するまでの全ての時間のことである。

TCP 上の HTTP 通信の場合、TAT は次の時間を合計したものとなる。

- [1] TCP コネクションの確立
- [2] HTTP のリクエストの送信とレスポンスの受信の全てのやり取り
- [3] TCP コネクションの切断

この TCP 上の HTTP を、UDP 上の CoAP に置き換えると、TAT がなぜ向上するのだろうか。

UDP、CoAP のそれぞれに着目して解を導くことにしよう。

- TCP を UDP に置き換えることによる TAT の向上

TCP を UDP に置き換えることによって、TCP コネクションの確立と切断に掛かる時間が削減される。したがって、項番 [1] と [3] がなくなる分、TAT が向上する。

- HTTP を CoAP に置き換えることによる TAT の向上

HTTP を CoAP に置き換えることによって、ヘッダ長が大幅に小さくなる。

HTTP のヘッダは、リクエストライン／ステータスライン、数種類のヘッダ

フィールドからなる。一方、CoAP のヘッダは、図7に示されているとおり、僅か4バイトである。

したがって、項番 [2] のメッセージサイズが大幅に小さくなる分、TAT が向上する。

このように、UDP、CoAP のそれぞれの特長が、TAT の向上に寄与していることが分かる。

よって、正解は解答例に示したとおりとなる。

## ■設問 4

### (1)

#### 解答例

き：LB

空欄を含む文章は、「LAN の構成とネットワーク負荷」の第2段落の5番目の箇条書きにある。その中には、「新業務サーバのデフォルトゲートウェイには  き を、中継装置のデフォルトゲートウェイにはFWを、それぞれ定義する」と記述されている。

図5を見ると、新業務サーバを宛先とする②の通信は、LBを経由している。②の通信について、第1段落の4番目の箇条書きに「図5中の②の通信はLBを経由させ、2台の新業務サーバに負荷分散させる」と記述されている。

LBによる負荷分散の実施は、①の通信と同じである。したがって、①の通信の「Webサーバ」を、②の通信の「新業務サーバ」に置き換えることで、①と同じ負荷分散を実現できるはずだ。

設問1で解説したとおり、①の通信において、PCからWebサーバへリクエストを送信するとき、Webサーバの仮想IPアドレスを宛先に指定していた。この仮想IPアドレスはLBに設定されている。

レスポンスの通信経路はリクエストと逆方向をたどる。したがって、WebサーバからPCへレスポンスを返信するとき、PCを宛先とする通信はLBを経由しなければならない。この点は、WebサーバのデフォルトゲートウェイがLBになっていることで達成されていた。

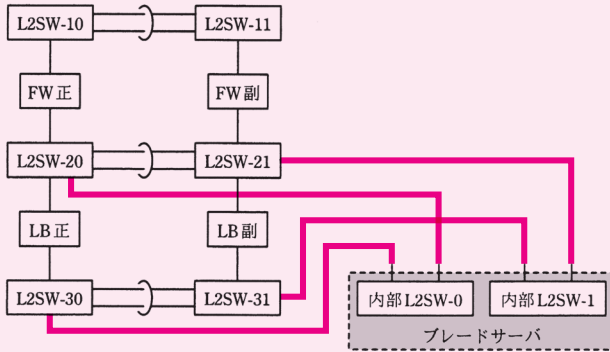
前述の説明を②の通信に当てはめると、新業務サーバのデフォルトゲートウェイが

LB になっていることが分かる。

よって、空欄きに該当する機器名は、「LB」となる。

## (2)

### 解答例

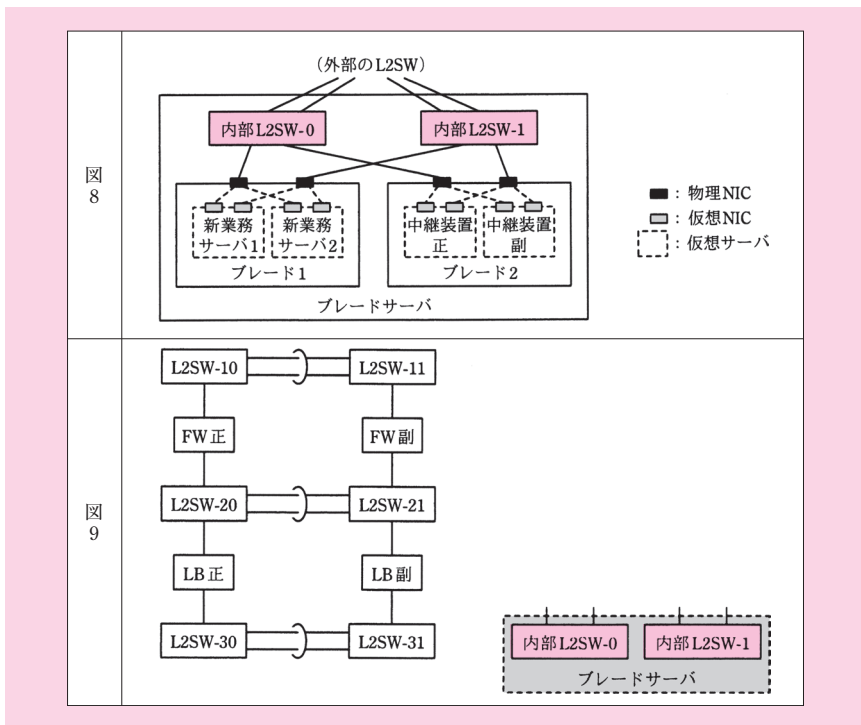


問題文は、「本文中の下線 (c) について、内部 L2SW と L2SW との接続を、図 9 に示す。内部 L2SW と L2SW との接続を追記し、図 9 を完成させよ」と記述されている。

下線 (c) は、「LAN の構成とネットワーク負荷」の第 2 段落の 6 番目の箇条書きである。それは、「(c) 図 8 中の二つの内部 L2SW に、図 2 中の 2 組の L2SW を接続する」と記述されている。

図 8 は、第 2 段落の最初の箇条書きにある。まず、問題文中の図 9 と、本文の図 8 をここに掲載する。図 9 のブレードサーバの内訳は、図 8 に示されている。本問は、ブレードサーバ内の「内部 L2SW」と、図 2 の L2SW を接続することを求めている。





図：本文の図8と図9の再掲

### ●ブレードサーバの内部構成

本問を解くには、様々な情報を整理する必要がある。

まず、本文に記述されている内容のうち、本問に関係するものだけをリストアップしよう。

ブレードサーバの内部には、新業務サーバ、中継装置が収納される。それらサーバについて、〔LANの構成とネットワーク負荷〕の第1段落の2番目～4番目の箇条書きには、次のように記述されている。

- ・2台の新業務サーバと2台の中継装置を、ブレード上の仮想サーバに実装する。
- ・中継装置はActive-Standby方式で冗長化させる。
- ・図5中の②の通信はLBを経由させ、2台の新業務サーバに負荷分散させる。

ブレードサーバ内部のLAN構成について、第2段落の2番目～5番目の箇条書きに

は、次のように記述されている。

- ・ 仮想サーバの二つの仮想 NIC は、ブレードの二つの物理 NIC にそれぞれ接続され、仮想サーバのチーミング機能によって冗長化されている。
- ・ ブレードの二つの物理 NIC は、ブレードサーバの二つの内部 L2SW にそれぞれ接続され、ブレードのチーミング機能によって冗長化されている。
- ・ LB 利用の有無を考慮し、新業務サーバと中継装置は別の VLAN に収容する。
- ・ 新業務サーバのデフォルトゲートウェイには LB を、中継装置のデフォルトゲートウェイには FW を、それぞれ定義する。

必要な情報が出揃ったところで、次に情報を整理しよう。

#### ・ 仮想サーバ、仮想 NIC、物理 NIC

新業務サーバ、中継装置は仮想サーバとなる。

仮想サーバは仮想 NIC をもち、サーバを終端とする通信は仮想 NIC 上で行われる。つまり、仮想サーバから送信／受信される Ethernet フレームは、仮想 NIC の MAC アドレスが送信元／宛先になる。

ブレードサーバの物理 NIC は、論理的には、ケーブル接続と同等であるとみなすことができる。物理的には、ブレードのチーミング機能によって冗長化されている。

#### ・ 新業務サーバ

新業務サーバは、LB による負荷分散の対象である。この点は、Web サーバ、業務サーバと同様である。

新業務サーバの NIC（仮想サーバの仮想 NIC）は、「チーミング機能によって冗長化されている」。この点も、Web サーバ、業務サーバと同様である。

したがって、新業務サーバと LB 間の接続は、Web サーバ、業務サーバに倣えばよい。

#### ・ 中継装置

中継装置は、LB による負荷分散の対象ではない。

図5の各通信の通信経路を見ると、中継装置を経由する3種類の通信（③、④、④'）は、いずれも LB を経由しない。したがって、LB の内側にあるサブネット（L2SW-30, L2SW-31 のセグメント）には収容しない。

一方、それら3種類の通信は、いずれも FW を経由する。中継装置のデフォルトゲートウェイは「FW」である。したがって、FW の内側にあるサブネット（L2SW-20,



それぞれ異なっている（第 2 段落の 4 番目の箇条書き）。

新業務サーバは LB を使用するので、LB の内側にあるサブネットに接続する。一方、中継サーバは LB を使用しないので、FW の内側にあるサブネットに接続する。

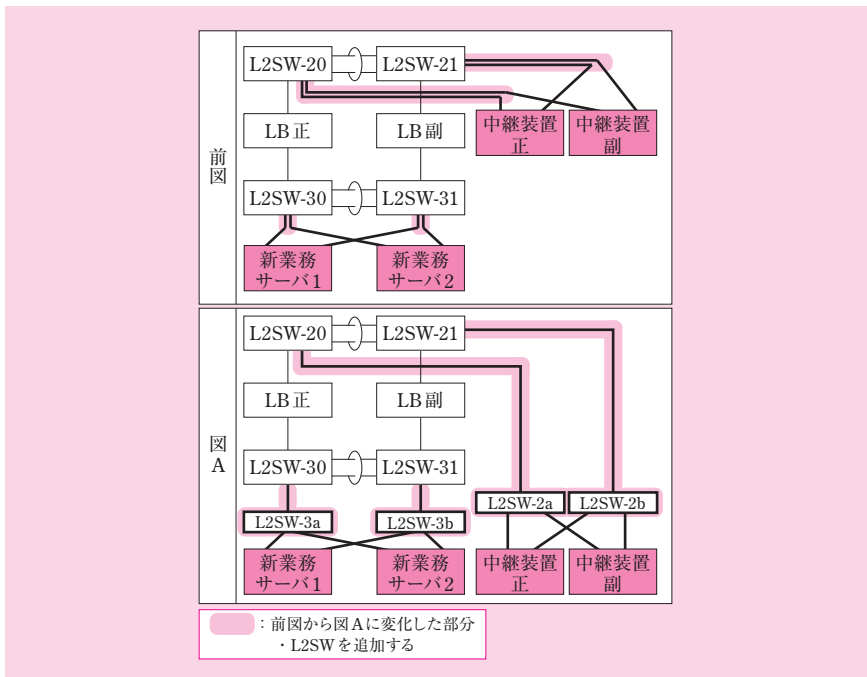
新業務サーバの NIC（仮想 NIC）はチームング機能で冗長化する。1 台のサーバから 2 本のケーブルが出ており、1 本は L2SW-30 に、もう 1 本は L2SW-31 に接続する。

中継装置の NIC（仮想 NIC）はチームング機能で冗長化する。1 台の装置から 2 本のケーブルが出ており、1 本は L2SW-20 に、もう 1 本は L2SW-21 に接続する。

### ●論理的ネットワークを物理的ネットワークに変更

図 9 のネットワーク構成に近づけるため、前図のネットワークを変更する。もちろん、論理的には同等であるように手を加えていく。

次の図に示すとおり、新たに 4 台の L2SW を追加し、この L2SW からケーブルが 2 本ずつ出るようにする。この変更を施したネットワーク構成図を「図 A」と呼ぶことにする。

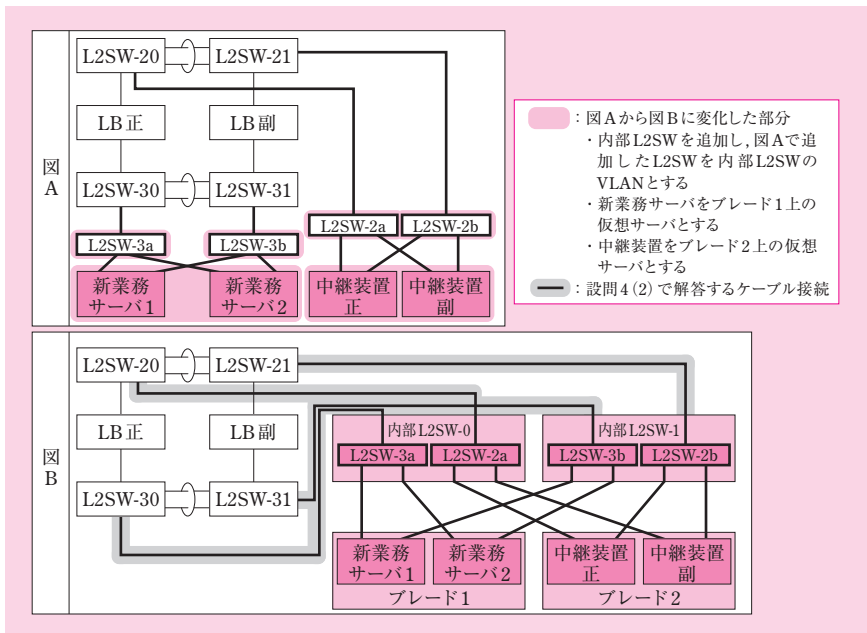


図：前図を図 A に変更

それでは、いよいよ仕上げに入る。論理的ネットワークを物理的ネットワークに変更しよう。

図Aを次のように変更する。この変更を施したネットワーク構成図を「図B」と呼ぶことにする。

- 内部 L2SW を追加し、図Aで追加した L2SW を内部 L2SW の VLAN とする。  
内部 L2SW-0 の中に、L2SW-3a, L2SW-2a を VLAN として設定する。内部 L2SW-1 の中に、L2SW-3b, L2SW-2b を VLAN として設定する
- 新業務サーバ（新業務サーバ1, 新業務サーバ2）をブレード1上の仮想サーバとする
- 中継装置（正, 副）をブレード2上の仮想サーバとする



図：図Aを図Bに変更

図B中の内部 L2SW、ブレード1、ブレード2が、図9のブレードサーバに物理的に収納される。

求める解は、図B中の内部 L2SW から出ているケーブル接続となる。

よって、正解は解答例に示したとおりとなる。

## (3)

## 解答例

ア：30

イ：72

ウ：6

●設問4(3)で問われていること：FWを経由する区間における、④の通信の見積り本問は、空欄ア～ウに入れる適切な数値を問うている。

空欄ア～ウは、図5中の④の通信の同時コネクション数を見積もっている、「LANの構成とネットワーク負荷」の第4段落の中にある。見積りの前提となる数値は、表1に記されている。

④の通信は様々な機器を経由するが、表1の見積りは、FWを経由する通信区間のものである。設問4(3)の解説に入る前に、この点を本文の記述から確認しておこう。

「LANの構成とネットワーク負荷」の第3段落の中で、「図5中の④の通信では、大量のHTTPリクエストとHTTPレスポンスの対（トランザクション）が発生（する）。……FWは、TCPコネクションの確立開始から切断完了までの状態（以下、コネクションという）を管理するので、④の通信の同時コネクション数はFWの性能に影響を与える可能性がある」とある。

図5を見ると、④の通信経路は、「新業務サーバ→中継装置→FW→通信アダプタ→設備」である。

設問2(1)で解説したとおり、中継装置はフォワードプロキシとして動作し、通信アダプタはリバースプロキシとして動作する。したがって、この通信経路上には、三つの通信区間で、TCPコネクションが接続されている。

[i] 新業務サーバと中継装置との間

[ii] 中継装置と通信アダプタとの間

[iii] 通信アダプタと設備との間

FWは、これらの通信区間のうち、[ii]の中に設置されている。つまり、第3段落で「FWの性能に影響を与える可能性がある」と懸念されるTCPコネクションとは、具体的に言うと、中継装置と通信アダプタを終端ノードとするものである。この通信



ア

まず、毎秒のトランザクション数（空欄ア）を求める。

本問が定義する「トランザクション」とは、「HTTP リクエストと HTTP レスポンスの対」（第3段落）のことだ。④の通信におけるトランザクションは、稼働情報の収集のやり取りである。

④の通信では、アクセスする際、次に示す URI を指定する。この点は、「保守システムの機能強化」の第3段落に記されている。

http://（設備を指定するための FQDN）/（リソース名）

URI に設備の FQDN があるので、設備ごとに、トランザクションをやり取りしている。したがって、トランザクションの数は、設備の数だけ存在することが分かる。

通信アダプタは顧客側にあるので、その数は複数ある。この通信アダプタに、複数の設備が接続されている。その数は1～100台である（表1項番2）。

収集対象となる設備数は、全部で「108,000 台」に上る（表1項番1）。

新サービス開始時、稼働情報の収集周期は、「3,600 秒」である（表1項番6）。つまり、この周期ごとに、1台の設備に対して1回のトランザクションが発生する。

毎秒のトランザクション数を計算する際、「④の通信の起動タイミングは平準化されている」との仮定を置く（第4段落）。常時、同数のトランザクションが発生していると考えられる。

したがって、毎秒のトランザクション数は、次式で求まる。

$$\begin{aligned}\text{毎秒のトランザクション数} &= \frac{\text{設備数}}{\text{収集周期}} \\ &= \frac{108,000}{3,600} = 30\end{aligned}$$

よって、空欄アに該当する数値は、「30」となる。

イ

ウ

空欄イ、ウは、同時コネクション数の平均値を求める式の中にある。そこには、

$$\text{同時コネクション数の平均値} = (\text{イ} + \text{ウ}) \times T_{out} [\text{秒}]$$

とある。



一般的に言って、同時接続数の平均値は、次式で求まる。

$$\text{同時接続数の平均値} = \text{毎秒の接続発生数} \\ \times \text{接続保持時間の平均値}$$

空欄イ、ウを求めるため、毎秒の接続発生数、接続保持時間の平均値がどのように求まるかを考察する。その上で解を導こう。

### ●毎秒の接続発生数

毎秒の接続発生数を求めるに当たり、第4段落の2番目の箇条書きの中で、「1トランザクションは1接続で処理される」という仮定を置いている。

したがって、毎秒の接続発生数は、毎秒のトランザクション数に等しくなる。これは空欄アの解に他ならない。すなわち、「30」となる。

### ●接続保持時間の平均値

先ほどの仮定に従うと、接続の保持時間の平均値は、トランザクションの通信時間の平均値と等しくなる。そこで、この値を求めることにしよう。

表1の項番3に「稼働情報収集の成功率」が「80%」とある。裏を返せば失敗率は「20%」となるが、平均値を求めるに当たって、これは無視できない大きさである。トランザクションの通信時間の平均値は、成功率で重み付けした、成功時と失敗時の加重平均となる。

稼働情報収集に成功した場合、通信時間は「3秒」となる（表1項番4）。一方、失敗した場合、通信時間は「 $T_{out}$ 秒」となる（表1項番5）。

したがって、トランザクションの通信時間の平均値は、次式で求まる。

$$\begin{aligned} \text{通信時間の平均値} &= \text{成功率} \times \text{通信時間} + (1 - \text{成功率}) \times T_{out} \\ &= (0.8 \times 3 + (1 - 0.8) \times T_{out}) \text{ [秒]} \\ &= (2.4 + 0.2 \times T_{out}) \text{ [秒]} \end{aligned}$$

### ●解の導出

前述の「同時接続数の平均値」を求める式に、「毎秒の接続発生数」（毎秒のトランザクション数）、「接続の保持時間の平均値」（トランザクションの通信時間の平均値）を代入すると、

$$\begin{aligned}
 & \text{同時コネクション数の平均値} = \text{毎秒のコネクション発生数} \\
 & \quad \times \text{コネクション保持時間の平均値} \\
 & = 30 \times (2.4 + 0.2 \times T_{out}) \text{ [秒]} \\
 & = (72 + 6 \times T_{out}) \text{ [秒]}
 \end{aligned}$$

となる。

この式を、本文中の同時コネクション数の平均値を求める式と見比べれば、解が求まる。

$$\text{同時コネクション数の平均値} = ((\boxed{\text{イ}} + \boxed{\text{ウ}} \times T_{out}) \text{ [秒]})$$

よって、空欄イには「72」が、空欄ウには「6」が、それぞれ当てはまる。

#### (4)

##### 解答例

正常な通信に支障がない範囲でなるべく小さくする。(24字)

#### ●設問 4 (4) ～ (6) で問われていること：FW を経由する区間における、④の通信に関する同時コネクション数の軽減

以下の設問 4 (4) ～ (6) は、いずれも、④の通信について、FW を経由する同時コネクション数を軽減するために提案された内容について問うている。設問 4 (4) の解説に入る前に、この点を本文の記述から確認しておこう。

設問 4 (3) の冒頭で解説した事柄と一部重複するが、解を導く上で重要な着眼点となるので、改めて解説しておこう。

まず、[LAN の構成とネットワーク負荷] の第 3 段落の中で、「図 5 中の④の通信では、大量の HTTP リクエストと HTTP レスポンスの対 (トランザクション) が発生 (する)。……FW は、TCP コネクションの確立開始から切断完了までの状態 (以下、コネクションという) を管理するので、④の通信の同時コネクション数は FW の性能に影響を与える可能性がある」とある。

図 5 を見ると、④の通信経路は、「新業務サーバ→中継装置→FW→通信アダプタ→設備」である。

図 4 (3) で解説したとおり、この通信経路上には、三つの通信区間がある。それぞ

れの区間で、TCP コネクションが接続されている。

- [ i ] 新業務サーバと中継装置との間
- [ ii ] 中継装置と通信アダプタとの間
- [ iii ] 通信アダプタと設備との間

FW は、これらの通信区間のうち、[ ii ] の中に設置されている。つまり、第3段落で「FW の性能に影響を与える可能性がある」と懸念される TCP コネクションとは、具体的に言うと、中継装置と通信アダプタを終端ノードとするものである。

この TCP コネクションは FW の性能に影響を及ぼすため、第5段落の中で、「同時コネクション数を軽減するために、HTTP/1.1 の実装に関する次の三つの提案」をまとめている。

- TCP コネクション保持時間の短縮案 1
- TCP コネクション保持時間の短縮案 2
- 同時コネクション数の削減案

ここで、TCP コネクション保持時間の短縮が同時コネクション数の削減に寄与する理由は、設問 4 (3) で解説したとおり、次の式が成立するからである。

$$\text{同時コネクション数の平均値} = \text{毎秒のコネクション発生数} \\ \times \text{コネクション保持時間の平均値}$$

設問 4 (4) ～ (6) は、これら三つの提案の具体的な内容について、上から順に一つずつ問うている。解を導くに当たり、この提案にある「コネクション」が「FW を経由するコネクション」を指していることを、常に念頭に置いておく必要がある。

この提案内容には、「HTTP/1.1 の実装」が関わっている。「実装」とあるので、HTTP/1.1 の仕様を踏まえ、FW を経由する HTTP 通信を具体的にどのように行うかを提案していることが分かる（ただし、設問 4 (4) は、TCP に関するものであるが）。

それでは、この点を踏まえて、いよいよ設問 4 (4) の解を導こう。

## ●解の導出

問題文は「本文中の下線 (d) の設定方針を……述べよ」と記述されている。

下線 (d) は、[LAN の構成とネットワーク負荷] の第5段落の最初の箇条書きにあ

る。そこには、「TCP コネクション保持時間の短縮案 1: (d) 中継装置の  $T_{out}$  の設定方針」と記述されている。

下線 (d) の提案は、中継装置の  $T_{out}$  の設定によって TCP コネクション保持時間を短縮し、以って FW を経由する同時コネクション数を削減することを意図するものだ。

$T_{out}$  とは、表 1 項番 5 に記されているとおり、「TCP の無通信タイムアウト時間」である。TCP の終端ノードは、通信相手のノードからの応答がない場合、再送タイムアウトまで待った後、再送を試みる。一定回数の再送を試行し、その全てがタイムアウトに至ったとき、TCP コネクションを切断する（再送を試行するたびに、タイムアウト値が 2 倍ずつ増えていく）。

このタイムアウト時間は、稼働情報の取得に失敗した時間であることから、通信切断に至るまでの時間の合計を指している。それゆえ、ここで提案していることは、中継装置の OS で、このタイムアウト時間に関わるパラメータを設定することだ。

設問 4 (3) で解説したとおり、本事例の見積りの前提条件に従えば、TCP コネクション保持時間、及び、同時コネクション数は次式で表される。

$$\text{コネクション保持時間の平均値} = (2.4 + 0.2 \times T_{out}) \text{ [秒]}$$

$$\text{同時コネクション数の平均値} = 30 \times (2.4 + 0.2 \times T_{out}) \text{ [秒]}$$

したがって、 $T_{out}$  を短く設定すれば、コネクション保持時間を短縮し、同時コネクション数を削減することができる。

先ほど述べたとおり、TCP の終端ノードは、相手ノードから応答がない場合、再送を試みる。通常、再送タイムアウト値は、コネクションの接続中に計測された RTT (Round Trip Time: 往復時間) に基づいて決定される。とはいえ、OS によっては、固定値に設定することも可能である。下線 (d) の提案は、 $T_{out}$  に関わるパラメータを意図的に値を小さくすることを狙ったものだ。

ただし、むやみに短くするべきではない。通信アダプタは顧客拠点に設置されているので、中継装置と通信アダプタ間の通信には、無線 LAN で伝送する区間が含まれる。それゆえ、ネットワーク遅延の影響を受けやすい環境下である。本来は正常とみなされるべき通信であるにもかかわらず、容易に再送タイムアウトに達してしまい、再送処理をかえって誘発しかねないからだ。下線 (d) の提案は、その点に注意を払っているはずである。

したがって、 $T_{out}$  の設定方針は、「正常な通信に支障がない範囲でなるべく小さくする」となる。よって、これが求める解となる。

## (5)

## 解答例

後続がないリクエストに付与し、コネクションを切断する。

(27字)

問題文は、「本文中の下線 (e) の使い方を……述べよ」と記述されている。

下線 (e) は、「LAN の構成とネットワーク負荷」の第5段落の2番目の箇条書きにある。そこには、「TCP コネクション保持時間の短縮案 2: (e) 新業務サーバからのリクエストにおけるクローズ接続オプションの使い方」と記述されている。

本問の解を導くには、HTTP/1.1 の持続的接続 (persistent connection)、及び、下線 (e) にある「クローズ接続オプション」を理解しておく必要がある。そこで、この技術について概要を解説する。

### ●持続的接続

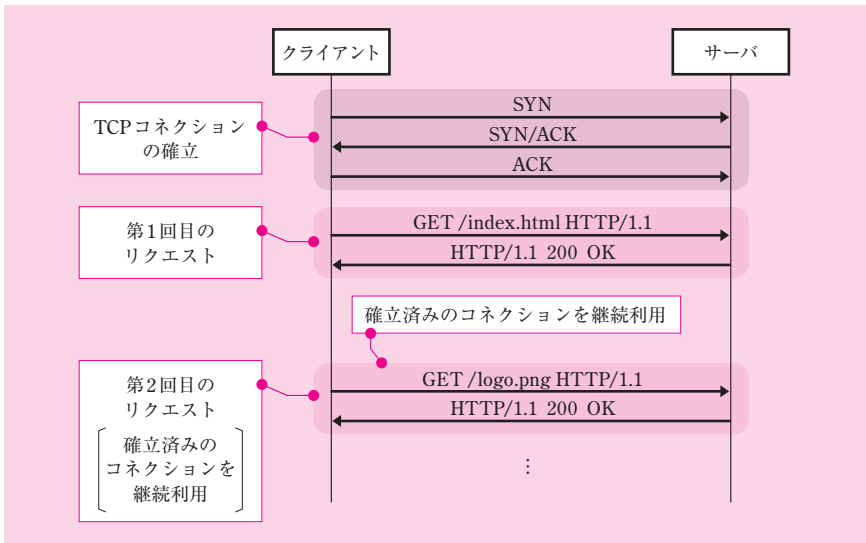
HTTP/1.1 (HTTP バージョン 1.1) は、持続的接続と呼ばれる機能をもっている。

HTTP/1.1 以上をサポートしているクライアントと Web サーバは、デフォルトでこの機能を使用する。

クライアントは、Web サーバとの間で TCP コネクションを確立した後、ページ取得等のリクエストを発行する。その後、同じ Web サーバに対し、更なるリクエストを発行するときがある。

例えば、クライアントがブラウザであり、あるサイトのトップページ (例: index.html) を取得するリクエストを発行したとする。そのページコンテンツが HTML で記述されており、その中に画像ファイル (例: logo.png) を参照する img タグがあったとしよう。このとき、ブラウザは、その画像ファイルを含めてトップページを表示する必要があると判断する。そこで、その画像ファイルを取得するリクエストを、すぐさま発行する。

この例のように、同じ Web サーバに対して、クライアントがリクエストを続けざまに発行することが、Web アクセスでは一般的に行われている。その際、HTTP/1.1 は、第1回目のリクエスト発行時に確立した TCP コネクションを、第2回目以降のリクエスト発行のために継続利用 (再利用) する。これが持続的接続である。



図：持続的接続のやり取り

HTTP/1.0はこの機能が規定されていなかったため、HTTPのリクエストとレスポンスの対ごとに、TCPコネクションの確立と切断を行う必要があった。持続的接続によって、TCPコネクションの継続利用を実現できるので、TCPコネクション確立に掛かる時間を削減できる。更に、やり取りするバケット数の削減によって、ホストやルータのCPU時間やネットワーク帯域などのリソースの消費も抑えられるため、ネットワーク全体のパフォーマンス向上も期待できる。

しかし、持続的接続は、Webサーバにとっては、一定の負荷がかかる処理である。クライアントからのリクエストが複数回発行される可能性があるため、一定時間、TCPコネクションを保持しておかなければならないからだ。これをキープアライブと呼ぶ。

参考までに、Apache 2.4では、キープアライブのタイムアウトは、デフォルトで5秒に設定されている。

### ●バーチャルホストと持続的接続との関係

Apache等のWebサーバアプリケーションは、バーチャルホスト機能をもっている。Apacheを例に、バーチャルホストを使っている場合、持続的接続がどのように動作するかを解説する。

バーチャルホストには、IPベースと名前ベースがある。IPベースは、バーチャルホストごとに異なるIPアドレスを対応付けている。一方、名前ベースは、複数のバー

チャルホストで同じ IP アドレスを対応付けている。

Web サーバが、ある IP アドレスを宛先とする接続を受け付けると、その IP アドレス上で稼働する全てのバーチャルホストをリストアップする。この動作を IP ルックアップという。

IP ルックアップの結果、IP ベースの場合、バーチャルホストを 1 台だけ選択する。一方、名前ベースの場合、複数のバーチャルホストがリストアップされ得る。バーチャルホストを 1 台に絞り込むため、リクエストパケットの Host ヘッダフィールドを用いる。HTTP/1.1 の仕様上、Host ヘッダフィールドには、アクセス先となる Web サーバのホスト名が指定されているからだ。これにより、バーチャルホストを 1 台選択する。

この IP ルックアップは、一つの TCP コネクションに対し、一度限り行われる。一方、ホスト名の絞り込みは、1 回の持続的接続の間、リクエストのたびに行われる。

したがって、名前ベースのバーチャルホストを使用している場合、単一の持続的接続の期間中、同じ IP アドレスに対応付けられた、複数のバーチャルホストのページをリクエストされることがある。

詳しくは、次の Apache のサイトを参照していただきたい（URL は本書執筆時点のもの）。

「An In-Depth Discussion of Virtual Host Matching」

<https://httpd.apache.org/docs/trunk/vhosts/details.html>

## ●クローズ接続オプション

HTTP/1.1 は、キープアライブのタイムアウトを待たずとも、明示的に持続的接続を閉じる方法を規定している。

その方法とは、Connection ヘッダフィールドに、次に示す「close」オプションを指定することである。

Connection : close

これは、本文の下線 (e) の中で、「クローズ接続オプション」と呼ばれている。本文に倣い、本書でもこの呼称を使うことにしよう。

Web サーバ、クライアントの双方が、これを用いることができる。

Web サーバがこのオプションを付与してレスポンスを返信することで、「今のレスポンスを最後とし、後続するリクエストを受け付けない」旨をクライアントに通知する。Web サーバは、当該レスポンスのパケットを送信した後、TCP コネクションを切断する。それゆえ、当該レスポンスを受信したクライアントは、新たなリクエストを

今のTCPコネクションを利用して送信することができなくなる。なお、後続するリクエストがあれば、別のTCPコネクションを利用することができる。

クライアントがこのオプションを付与してリクエストを送信することで、「今のリクエストが最後であり、後続するリクエストを送らない」旨をWebサーバに通知する。クライアントは、当該リクエストに対応するレスポンスを受け取った後、今のTCPコネクションを切断する。

クライアントからのクローズ接続オプションによって、不要となったTCPコネクションを、キープアライブタイムアウトを待たずに切断することができる。それゆえ、同時コネクション数の削減とWebサーバの負荷軽減がもたらされる。

ここまで理解できれば、本問を解く準備は整った。それでは、いよいよ解説に移ろう。

### ●解の導出

先ほど解説したとおり、クローズ接続オプションを付与することで、TCPコネクションの保持時間を短縮することができる。

④の通信において、これをどのように適用したらよいだろうか。

この点について、下線(e)には、「新業務サーバからのリクエストにおけるクローズ接続オプションの使い方」と記述されている。新業務サーバは、④の通信のクライアントに該当する。したがって、この記述は、クライアントから通知するクローズド接続オプション、すなわち、後続するリクエストがないときに通知するクローズ接続オプションを意味している。

新業務サーバは、リクエストに対応するレスポンスを受信した後、TCPコネクションを切断する。この結果、TCPコネクションの保持時間を短縮できるわけだ。

さて、本問で問われている提案は「TCPコネクション保持時間の短縮案2」である。設問4(4)の冒頭で解説したとおり、この「TCPコネクション」は、FWを経由するTCPコネクションを指している。

これまでの解説で、新業務サーバをクライアントとするTCPコネクションの保持時間の短縮については理解できた。このことが、FWを経由するTCPコネクションの保持時間の短縮と、どのように関係しているのだろうか。

(設問4(3)の冒頭で解説した事柄の繰返しになるが、)④の通信経路上には、三つの通信区間で、TCPコネクションが接続されている。

[i] 新業務サーバと中継装置との間

[ii] 中継装置と通信アダプタとの間

[iii] 通信アダプタと設備との間



中継装置がフォワードプロキシであるため、[i]と[ii]のTCPコネクションは連動して生成される。つまり、[i]のTCPコネクションが確立／切断されると[ii]の方も確立／切断される。

したがって、[i]の新業務サーバを終端ノードとするTCPコネクションの保持時間を短縮することで、[ii]のFWを経由するTCPコネクションの保持時間を短縮できることが分かる。

よって、正解は、「後続がないリクエストに付与し、コネクションを切断する」となる。

## (6)

### 解答例

通	信	ア	ダ	プ	タ	に	F	Q	D	N	を	付	与	し	,	同	一	コ	ネ	ク	シ	ヨ	ン	を	
使	っ	て	複	数	の	設	備	か	ら	稼	働	情	報	を	取	得	す	る	。						

(45字)

問題文は、「本文中の下線 (f) の設計方針を……述べよ」と記述されている。

下線 (f) は、[LANの構成とネットワーク負荷]の第5段落の3番目の箇条書きにある。そこには、「同時コネクション数の削減案: トランザクションをパイプライン化する工夫と、その前提となる、(f) 設備のリソースを指定する際のURLに関する設計方針」と記述されている。

本問の解を導くには、下線 (f) の前にある「パイプライン化」を理解しておく必要がある。これは、HTTP/1.1の持続的接続機能の一部として規定されたものである。そこで、この技術について概要を解説する。

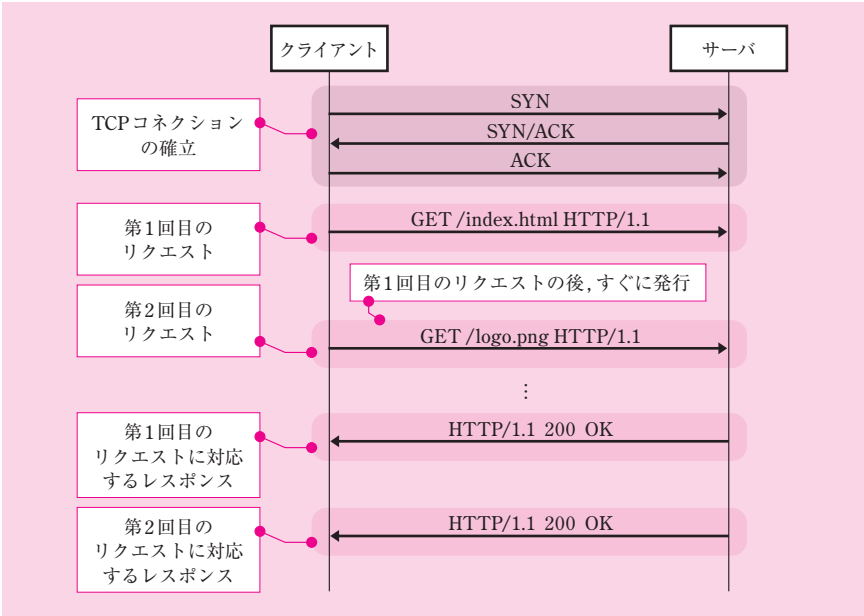
### ●パイプライン化

まず、下線 (f) の前にある「トランザクション」とは、本文が第3段落で定義したものであり、「HTTPリクエストとHTTPレスポンスの対」のことだ。

次いで、下線 (f) の前にある「トランザクションのパイプライン化」とは、HTTP/1.1の持続的接続の規定に含まれたパイプライン化を指している。

このパイプライン化とは、HTTPのリクエストを送信した後、それに対応するレスポンスを待たずに、後続のリクエストを次々に送信する仕組みのことである。

Webサーバは、パイプライン化されたリクエストを受信すると、その受け取った順番に、リクエストに対応するレスポンスを返信する。



図：パイプライン化されたリクエストのやり取り

パイプライン化によるリクエストの連続転送は、クライアントとサーバ間の RTT (Round Trip Time) が大きいとき、転送効率の向上に寄与する。

この点について、具体例を使って解説しよう。

あるページを 2 回の HTTP リクエストで取得するとき、パイプライン化しない場合とした場合について、次の条件で比較してみよう。

表：パイプライン化しない場合とした場合の比較条件

パケットの転送時間 (シリアル化遅延時間)	リクエストパケット	無視できるほど小さいとする
	レスポンスパケット	$T_{res}$
クライアントとサーバ間の RTT		$T_{rtt}$
その他の処理時間		無視できるほど小さいとする

・パイプライン化しない場合

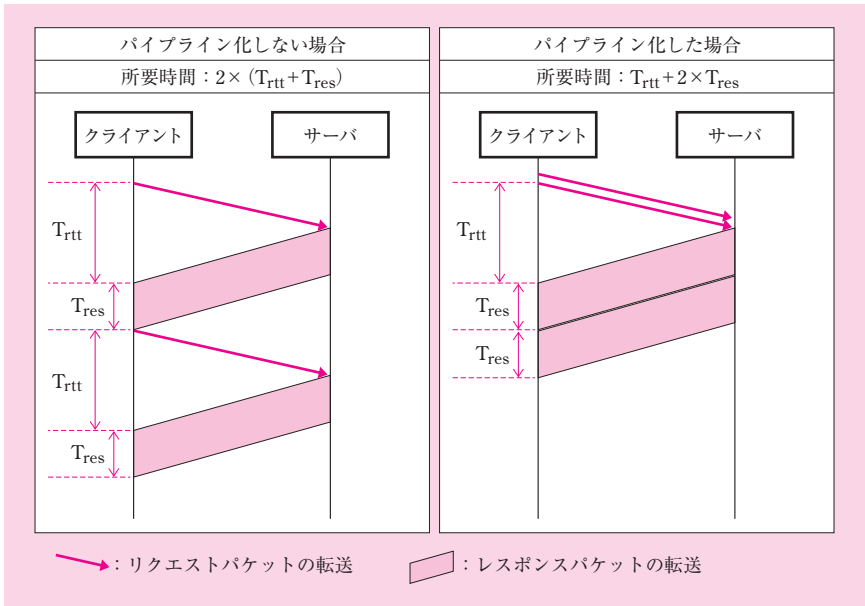
1 回目のリクエストとレスポンスの所要時間 =  $T_{rtt} + T_{res}$

2 回目のリクエストとレスポンスの所要時間 =  $T_{rtt} + T_{res}$

所要時間 =  $2 \times (T_{rtt} + T_{res})$

- パイプライン化した場合

$$\text{所要時間} = T_{\text{rtt}} + 2 \times T_{\text{res}}$$



図：パイプライン化しない場合とした場合の比較

パイプライン化について理解できたところで、次に、本問の解を導くのに必要な情報を整理しよう。

### ●リソース指定方式の問題

本問は、下線 (f) の設計方針を問うている。下線 (f) の設計は、設備のリソースを指定する URL を、どのように設計するかを述べている。その設計は、トランザクションのパイプライン化を前提としている。

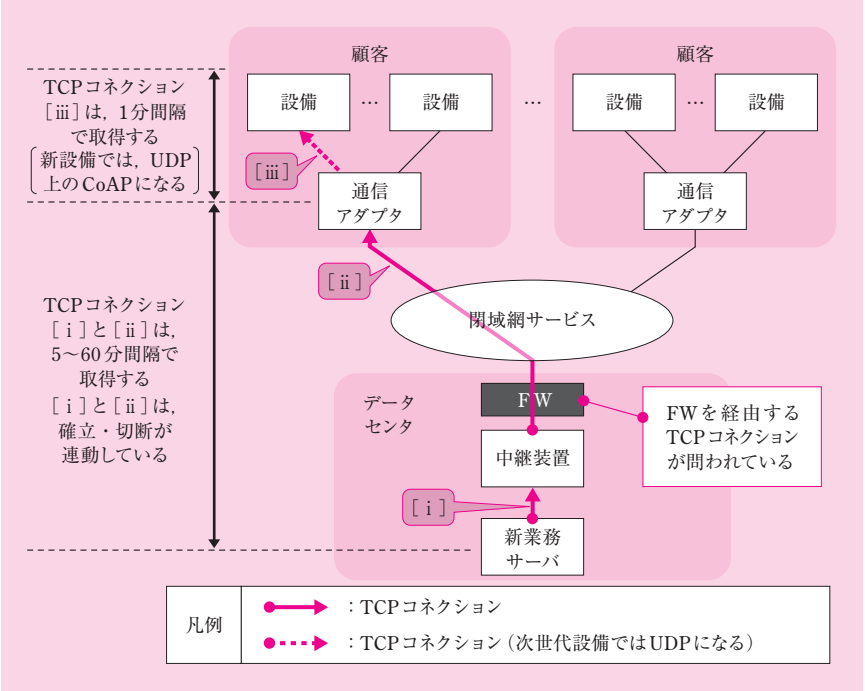
そこで、まず、現在検討中のリソースを指定する方法を考察し、その問題点を洗い出してみよう。

④の通信に際し、設備のリソースを指定する方法について、〔保守システムの機能強化〕の第3段落の6番目の箇条書きに

`http://(設備を指定するためのFQDN)/(リソース名)`

と記述されている。設備のリソースとは、同じく6番目の箇条書きに、「設備の中の稼働情報又は操作対象の機能」とある。

設問4(3)で解説したとおり、④の通信は、個々の設備に対して行われる。つまり、TCPコネクションは設備ごとに生成する。イメージしやすくするため、図「④の通信でTCPコネクションが発生する様子」を再掲する。



図：④の通信でTCPコネクションが発生する様子（再掲）

現在検討中の方法では、リソースを指定する際、設備と通信する順序を一切考慮していない。通信アダプタの配下に設備が複数ぶら下がっているという構成上の特長を、全く生かしていないのである。

例えば、新業務サーバが、ある通信アダプタAの配下にある設備Pと通信するため、前図のようなTCPコネクションを生成したとしよう。その後、更に別の通信アダプタBの配下にある設備Qと通信するため、別のTCPコネクションも生成したとする。この時点で、FWを経由するTCPコネクションは2本である。そのようにバラバラに通信しているうちに、設備Pと通信するためのTCPコネクションが切断されてしまう。

最悪の場合、1回のTCPコネクションの中で、1個の設備に対してのみ、トランザクションが発生する。HTTPリクエスト数は、高々、当該設備内のリソース数に留まる。これでは、トランザクションをパイプライン化したところで、その効果は限定的だ。

本事例において、通信④で発生するHTTPリクエストの数は、URIの数と等しくなる。つまり、取得したい設備のリソースの総数である。1回のTCPコネクションでパイプライン化できるHTTPリクエスト数が少ないということは、必然的に、TCPコネクションの数が多くなることを意味している。

これが、現在検討中のリソース指定方法がもつ問題点である。

これまで解説した内容を、表にまとめてみよう。

表：現在検討中のリソース指定方法の問題点

URI	指定する値	効果
ホスト名 (FQDN)	設備	TCPコネクションが設備ごとに生成される
パス名	リソース	パイプライン化できるトランザクション数は、(最悪の場合、) 設備内にあるリソースの数

### ●リソース指定方式の改善

パイプライン化の効果を高めるには、1回のTCPコネクションの中で、できるだけ多くのHTTPリクエストを続けざまに発行するように、設計する必要がある。

リソース指定方法をどのように改善すれば、この効果が得られるのだろうか。

ここで、鍵となる重要な二つの点に着目しよう。

一つ目は、通信アダプタが、リバースプロキシとして動作していることである。

二つ目は、通信アダプタに、最大100個の設備が接続されていることである。

#### ・通信アダプタが、リバースプロキシとして動作していること

設問2(1)で解説したとおり、通信アダプタはリバースプロキシとして動作しており、中継装置から受信したHTTPリクエストを設備に転送している。設備を指定するFQDN(ホスト名)に対応するIPアドレスは、通信アダプタになっている。

リバースプロキシなので、TCPコネクションの終端は、通信アダプタになっている。ただし、現在検討中の方法では、バラバラのタイミングで、設備単位にTCPコネクションを生成している。

この点に着目し、次のように考えてみよう。

「設備単位に生成していたTCPコネクションを、通信アダプタ単位に生成できない

だろうか」と。

この検討を進めるため、二つ目の重要な点に着目することにしよう。

・通信アダプタに、最大 100 個の設備が接続されていること

通信アダプタには、1～100 台の設備が接続されている。

この構成上の特長に着目するなら、これまで設備単位でバラバラに生成していた TCP コネクションを、通信アダプタ単位に集約して生成できることが分かる。その接続を持続的に利用して、配下の設備に対して HTTP リクエストをまとめて発行すれば、「新業務サーバー→中継装置→通信アダプタ」の通信区間の TCP コネクションを 1 個に集約できる。この結果、この通信区間では、HTTP/1.1 の持続的接続の恩恵を受けて、パイプライン化の効果が得られるはずだ。

このようにリクエストの発行方式を変更する結果、この通信区間の途中に位置する、FW 経由の TCP コネクションの同時接続数を削減できる。

なお、この方式においても、通信アダプタと設備間の TCP コネクションは、(設備が終端ノードである以上、当然であるが、) 従来のまま設備単位に生成されることに留意しておこう。実は、設問 3 (1)、(3) で解説したとおり、通信アダプタと設備間の通信区間を UDP 上の CoAP に置き換えることで、本事例では性能改善を図ることになる。

話を元に戻し、通信アダプタ単位に TCP を生成することによるパイプライン化の効果を、計算で確かめてみよう。通信アダプタ当たり平均  $N$  個の設備が接続されており、設備当たり平均  $M$  個のリソースをもっていたら、トランザクション当たりの HTTP リクエスト数は「 $N \times M$ 」となる。最大 100 個の設備が通信アダプタに接続されていることを考えるなら、パイプライン化は効果てきめんである。

したがって、このような効果が得られるように、リソース指定方法を改善すればよいわけだ。

改善した結果については、次の表のようになる。リソース指定方法はすぐ後の「●解の導出」で具体的な値を導くため、とりあえず「？」と置いておこう。

表：現在検討中のリソース指定方法の改善点

URI	指定する値	効果
ホスト名 (FQDN)	?	TCP コネクションが通信アダプタごとに生成される
パス名	?	パイプライン化できるトランザクション数は、通信アダプタ配下にある、設備とそのリソースの数

注) リソース指定方法の具体的な改善内容は「？」と表記している。

ここまで情報を整理できたところで、いよいよ解を導こう。

### ●解の導出

現在検討中のリソース指定方法について、問題点と改善点を解説し、それぞれの論点を表にまとめてみた。問題点の表を見ると、次のことが分かる。

- ホスト名に指定した内容が、TCP コネクションの生成単位となる
- パス名に指定した内容が、パイプライン化する HTTP リクエストとなる

これを改善点の表を当てはめるなら、「?」の部分

- TCP コネクションの生成単位である「通信アダプタ」を、ホスト名に設定する
- パイプライン化する HTTP リクエストである「設備とそのリソース」を、パス名に設定する

とすればよいはずだ。

つまり、リソースの指定方法は、次のようになる。

http:// (通信アダプタを指定するための FQDN) / (設備を指定するためのパス) / (リソース名)

この設計に従えば、FQDN の部分を通信アダプタに指定して接続し、新業務サーバと通信アダプタとの間で HTTP/1.1 の持続的接続を行う。そして、この TCP コネクションの中で、通信アダプタの配下にある複数の設備、及びそのリソースをまとめて取得すればよいわけだ。

この結果、FW を経由する同時コネクションが削減されると共に、トランザクションが極めて効果的にパイプライン化される。

言うまでもなく、この設計方針に沿って、トランザクションを開始する新業務サーバは、稼働情報取得の通信を適切に実行する必要がある。通信アダプタも、新たなリソース指定方法に対応するように適切に設定する必要がある。

よって、正解は、「通信アダプタに FQDN を付与し、同一コネクションを使って複数の設備から稼働情報を取得する」となる。

## 問2

## 出題趣旨

グローバル IPv4 アドレスの枯渇が、インターネット経由で提供される各種のサービス拡大の足かせになってきた。また、サーバ仮想化技術を活用して多数の顧客を収容したサービス基盤の基盤ネットワークが、仮想サーバの急激な増大に柔軟に対応できない問題も顕在化してきた。

これらの状況を基に、本問では、インターネット接続サービスと IaaS を提供する ISP を取り上げ、インターネット接続サービスで使用するグローバル IPv4 アドレスの節約策と IaaS の基盤ネットワークを仮想サーバの増大に対応させる方策を題材にした。本文に、NAT444、マルチキャスト通信及び VXLAN (Virtual eXtensible Local Area Network) などの技術の概要を説明し、受験者が習得した技術や経験を基に、説明された新技術の仕組みや動作を理解し、それを実務に適用できるかどうかを問う。

## 採点講評

問2では、サービス基盤の改善をテーマに、インターネット接続サービスと IaaS を提供する ISP が直面する課題を取り上げた。その中で、NAT444、マルチキャスト通信及び VXLAN (Virtual eXtensible Local Area Network) などの技術の理解を問うた。全体として、よく理解されていた。記述問題の中では、設問3(1)、(2)の正答率が高かった。一方、設問4(1)、(2)の正答率は低かった。これは、IPsec NATトラバースルが広く利用されているのに対し、マルチキャスト通信を利用する機会が少ない結果と考えられた。しかし、マルチキャスト通信は、今後拡大すると考えられる、VXLANのようなオーバーレイネットワークの構築に欠かせない技術なので、理解しておいてほしい。

設問1では、cの正答率が低かったが、全体では正答率が高かった。cは、FTPのモードの知識問題だったので、本問を機に理解しておいてほしい。

設問2は、NAT444に関連する問題だったが、(2)に比して(1)の正答率が低かった。設問の趣旨が適切に理解されていない解答が散見された。本文に記述された内容と設問で問われている内容とをよく理解して、解答を導き出すよう心掛けてほしい。

設問3では、IPsec通信がNATを介したときに発生する問題について問うた。正答率が高く、この問題は、受験者に広く理解されていることがうかがえた。

設問4では、マルチキャスト通信について問うた。(1)と(2)の正答率が低かった。マルチキャスト通信では、宛先は、IPアドレスとMACアドレスともマルチキャストのアドレスになるが、送信元は、必ず、ユニキャストのアドレスになること、及びスイッチによるMACアドレスの学習は、送信元のMACアドレスを基に行われることを忘れないでほしい。

設問5は、VXLAN関連の設問だったが、正答率は比較的高かった。本設問は、VXLANに関する知識や経験がなくても、TCP/IP通信の基本的な技術と、本文に記述された内容から解答が導き出せるものだったので、受験者の基本技術の理解度が高いことがうかがえた。

設問	解答例・解答の要点		備考
設問1	a	3	
	b	16	
	c	アクティブ	
	d	D	
	e	マルチキャスト MAC アドレス	

(表は次ページに続く)



設問	解答例・解答の要点			備考
設問2	(1)	PCのネットワークアドレスと、CPEとCGN装置間のネットワークアドレスが重なったとき		
	(2)	①	・送信元IPアドレス	
		②	・送信元ポート番号	
		③	・アクセス時刻	
設問3	(1)	IPヘッダが認証対象なので、IPアドレスが書き換えられると認証データが計算値と一致なくなるから		
	(2)	・TCP又はUDPヘッダが暗号化の対象であり、ポート番号が暗号化されていて分からないから ・ESPヘッダには、ポート番号が存在しないから		
	(3)	送信元ポート番号が500と4500以外のISAKMPメッセージも受信できるようにする。		
設問4	(1)	マルチキャストMACアドレスが送信元アドレスになることがないから		
	(2)	ビデオサーバは、マルチキャストパケットを送信する側だから		
	(3)	ア	01-00-5e-01-01-01	
		イ	①を受信したとき	p1
			②を受信したとき	p1, p3
設問5	(1)	・ $2^{24}$ のVXLANセグメントが構成できるから ・膨大な数の論理セグメントが構成できるから		
	(2)	理由	宛先となるVMの存在場所が不明だから	
		宛先IPアドレス	224.1.1.2	
		送信元IPアドレス	10.0.0.254	
	(3)	マルチキャストグループ224.1.1.2のIGMP joinメッセージを、L3SW2に送信する。		
	(4)	問題	不要なマルチキャストパケットがネットワーク内に転送されるので、L3SWやネットワークの負荷が高まる。	
		宛先IPアドレス	10.0.0.254	
		送信元IPアドレス	10.10.0.254	

本事例には、インターネット接続サービスとIaaS（Infrastructure as a Service）を提供しているISPのY社が登場する。

本問は、Y社のサービス基盤の改善をテーマにしている。

インターネット接続サービスに関しては、グローバルIPアドレスの枯渇対策として、NAT444を用いたキャリアグレードNAT（以下、CGNと称する）の実現を問うている。それに関連して、NAT機器を経由したIPsec通信の問題点とIPsec NATトラバースによる解決策についても問うている。

IaaS 基盤のネットワーク（以下、基盤ネットワークという）に関しては、マルチキャスト通信と VXLAN を用いたオーバーレイネットワークの実現について問うている。

特別な知識を必要とせずに解答できるよう、NAT444、マルチキャスト通信、VXLAN に関しては、本文中で詳しく説明されている。一方、IPsec は、午後試験でよく出題されるテーマであり、本試験の前提知識であると言える。そのため、NAT トラバーサル実行時のパケット構造に関する部分が主に説明されているだけだ。

本問を首尾よく解くには、これら要素技術の仕組みを理解しておく必要がある。そこで、設問で取り上げられた順番に従い、NAT444 を設問 2 で、IPsec NAT トラバーサルを設問 3 で、マルチキャスト通信を設問 4 で、VXLAN を設問 5 で、それぞれ解説する。

## ■設問 1

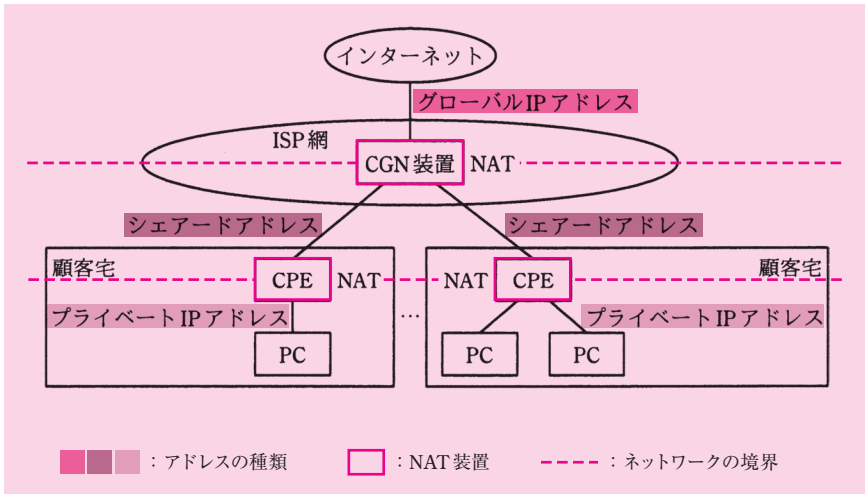
### 解答例

- a : 3
- b : 16
- c : アクティブ
- d : D
- e : マルチキャスト MAC アドレス

a

空欄 a を含む文章は、[NAT444 の調査] の第 2 段落の中にある。そこには「NAT444 の“444”は、図 2 に示したように a 種類のネットワークアドレスで運用されるネットワークを指し、各ネットワークの境界で NAT を実行することで、グローバル IP アドレスを節約する」と記述されている。

図 2 は同段落のすぐ上にある。この図は、NAT444 の構成を示している。



図：本文の図2の再掲「NAT444の構成」

図中の NAT 機器は、顧客宅内の CPE と、ISP 網内の CGN 装置の2種類である。

これらの NAT 機器が実施しているアドレス変換については、設問2の冒頭で詳しく解説するので、ここでは結論だけ述べることにする。

顧客宅内の CPE が実施する NAT は、顧客宅内のプライベート IP アドレスから ISP 網内の ISP Shared Address（以下、シェアードアドレスと称する）への変換である。CGN 装置が実施する NAT は、ISP 網内のシェアードアドレスからインターネットのグローバル IP アドレスへの変換である。

したがって、NAT444 を用いたネットワークには、3種類のネットワークアドレスが使用されている。

よって、空欄 a に該当する字句は、「3」である。

b

空欄 b を含む文章は、[NAT444 の調査]の第4段落の中にある。そこには「bビットで構成されている TCP/UDP のポート番号」と記述されている。

TCP、UDP のヘッダにあるポート番号は、16ビット長のフィールドである。

よって、空欄 b に該当する字句は、「16」である。

c

空欄 c を含む文章は、[NAT444 の調査] の第 5 段落の中にある。そこには「FTP の c モードのように、インターネット上のサーバからクライアントが指定したポートに対して TCP コネクションの確立を試みる」と記述されている。

本問を解くには、FTP が用いるコネクションやモードに関する一般的な知識が必要である。そこで、まずはその点について解説する。それを踏まえて、解を導こう。

## ● FTP

FTP (File Transfer Protocol) は、クライアントとサーバ間でファイル転送を行うプロトコルである。その通信に際し、制御用コネクションとデータ転送用コネクションの二つのコネクションを用いる。

制御用コネクションは、クライアントから FTP サーバへのコマンドの送信、及び、同コマンドに対する FTP サーバからクライアントへの応答に用いられる。主なコマンドには、クライアントから FTP サーバへのファイルのアップロード、FTP サーバからクライアントへのファイルのダウンロード、FTP サーバ側のファイル一覧の取得、ユーザ認証 (FTP サーバがクライアントを認証) などがある。

データ転送用コネクションは、コマンドの内容に応じた、クライアントと FTP サーバ間のデータ転送に用いられる。

制御用コネクションは、一度確立したら、クライアント側から切断するまで (又は、タイムオーバによってサーバから強制的に切断するまで)、存続する。一方、データ転送用コネクションは、コマンドごとに確立と切断が行われる。つまり、必要なときだけ接続されるわけだ。

二つのコネクションを用いたやり取りについて、ファイルのダウンロードを例に説明しよう。

クライアントは、ダウンロードしたいファイル名を指定して、コマンドを FTP サーバに送信する。指定されたファイルがダウンロード可能であれば、FTP サーバはその旨をクライアントに応答する。ここまでのやり取りは、制御用コネクション上で行われる。その後、データ転送用コネクションが確立され、同コネクション上で指定されたファイルのデータ転送が行われる。データ転送が終了したら、同コネクションが切断される。

制御用コネクションの確立は、クライアントから FTP サーバに対して行われる。FTP サーバ側のポート番号は 21 番である。

一方、データ転送用コネクションの確立は、2 種類の方法がある。一つ目は、FTP サーバからクライアントに向けて行われるもので、アクティブモードと呼ばれる。二

つ目は、クライアントからFTPサーバに向けて行われるもので、パッシブモードと呼ばれる。

データ転送用のコネクション確立に先立ち、それぞれのモードにおいて、クライアントとFTPサーバは、コネクションに用いるポート番号を通知する。

アクティブモードの場合、クライアントは、FTPサーバからの宛先となるポート番号（ウェルノウンポート番号以外のもの）を通知する。送信元となるFTPサーバのポート番号は、20番となる。

パッシブモードの場合、クライアントは、パッシブモードを行う旨のコマンドを送信する。これがFTPサーバによって受理されたとき、FTPサーバは、クライアントからの宛先となるポート番号を通知する。このポート番号は、実行時にランダムに決定される。送信元となるクライアントのポート番号は、通常のクライアントサーバモデルと同様、任意のポート番号（ウェルノウンポート番号以外のもの）となる。

### ●解の導出

前述のとおり、クライアントが指定したポートに対し、FTPサーバからTCPコネクションの確立を試みるのは、アクティブモードである。

よって、空欄cに該当する字句は、「**アクティブ**」である。

d

空欄dを含む文章は、[マルチキャスト通信の調査]の第2段落の中にある。そこには「マルチキャストIPアドレスは、クラス d のIPアドレスである」と記述されている。

IPが規格化された当初、IPアドレスは五つのクラスに分かれていた。

クラス名は、アルファベット1文字で、AからEまでである。クラスごとに、アドレスの範囲、用途、ネットワークアドレス部のビット長が決められている。

クラスA～Cの用途はユニキャストアドレス、クラスDの用途はマルチキャストである。クラスEは予約扱い（実験用）で、現在に至るまで使用されていない（255.255.255.255の限定的ブロードキャストアドレスを除く）。

各クラスのアドレスの範囲、用途、ネットワークアドレス部のビット長の内訳は次のとおりである。

表：IP アドレスのクラス

クラス	アドレスの先頭ビット (2進数)	アドレスの範囲		ネットワークアドレス部のビット長
		先頭	末尾	
A	0	0.0.0.0	127.255.255.255	8
B	10	128.0.0.0	191.255.255.255	16
C	110	192.0.0.0	223.255.255.255	24
D	1110	224.0.0.0	239.255.255.255	—
E	1111	240.0.0.0	255.255.255.255	—

※ネットワークアドレス部の長さは、ユニキャストアドレスに必要なものなので、クラスA～Cに定義されている。

1990年代に入りインターネットが世界的に普及していき、多数のネットワークアドレスを割り当てる必要性が生じた。そこで、サブネットマスクを用い、クラスAやクラスBのネットワークを細分化して新たなネットワーク（サブネット）を定義する技術が規格化された。これを CIDR（Classless Inter-Domain Routing）という。

CIDRの登場により、ユニキャストアドレスにおけるクラスの概念は、事実上消滅した。

一方、マルチキャストアドレスは、今に至るまで、クラスD（224.0.0.0/8）の範囲内にあるアドレスを使用している。そこで、慣例的に、マルチキャストアドレスの範囲を「クラスD」と言い表すことがある。

よって、空欄dに該当する字句は、「D」である。

e

空欄eを含む文章は、〔マルチキャスト通信の調査〕の第3段落の中にある。そこには「マルチキャストIPアドレスが設定されたPCでは、当該マルチキャストIPアドレスを基に生成される e 宛でのフレームを受信するように、NIC（Network Interface Card）が動作する」と記述されている。

宛先IPアドレスがマルチキャストアドレスであるとき、イーサネットフレームの宛先は、マルチキャストMACアドレスとなる。

よって、空欄eに該当する字句は、「マルチキャストMACアドレス」である。

IPv4だけでなくIPv6においても、ネットワーク層の宛先がマルチキャストであれば、データリンク層の宛先もマルチキャストアドレスになる。詳しくは本書の第1章「1.2.2 DIX規格のフレームフォーマット」の「●宛先MACアドレス／送信元MACアドレス」を参照されたい。

## ■設問2

設問2の解説に入る前に、NAT444について解説する。

### ● NAT444 とは

本文に詳しく説明されているので、適宜抜粋しながら解説していこう。

まず、〔グローバル IP アドレス不足への対応策の検討〕の中で、次のように記述されている。

グローバル IP アドレスの枯渇対象の中に、大規模 NAT 又はキャリアグレード NAT（以下、CGN という）と呼ばれる、ISP 向けのソリューションがある。CGN を導入することによって、インターネット接続サービスで使用しているグローバル IP アドレスを削減でき、それを IaaS に振り向けることができる。CGN では、アクセスネットワークにプライベート IP アドレスを割り当て、ISP 網内でグローバル IP アドレスに変換する。CGN を実現する技術の中に、NAT444 がある。NAT444 には、網内の宅内に設置された機器（以下、CPE という）に変更を加えずに CGN に移行できる利点がある。

「アクセスネットワーク」の定義は、本文中に明確に与えられていない。とはいえ、この段落の中で、「プライベート IP アドレスを割り当て（る）」とあるので、顧客宅内のネットワークを指していると考えられる。

通常、プライベートアドレスをグローバル IP アドレスに変換しているのは、顧客の宅内に設置された機器（Customer Premises Equipment。以下、CPE と称する）であった。一方、CGN では、この変換を「ISP 網内」で行う。このアドレス変換に用いる技術が、NAT444 である。

CGN の実現には複数の要素技術が関与しているが、その中核をなすのが NAT444 である。

本文は、この後に続けて NAT444 について詳しく説明している。〔NAT444 グローバルの調査〕の第1、第2段落を見てみよう。

現在、Y 社の個人顧客向けのインターネット接続サービスでは、顧客に一つずつグローバル IP アドレスを割り当てている。これを ISP Shared Address（以下、シェアードアドレスという）と呼ばれる IP アドレスに置き換え、複数の顧客間でグローバル IP アドレスを共用するのが NAT444 である。NAT444 では、IP アドレスとポート番号を対にした変換が 2 回行われる。NAT444 の構成を図 2 に示す。

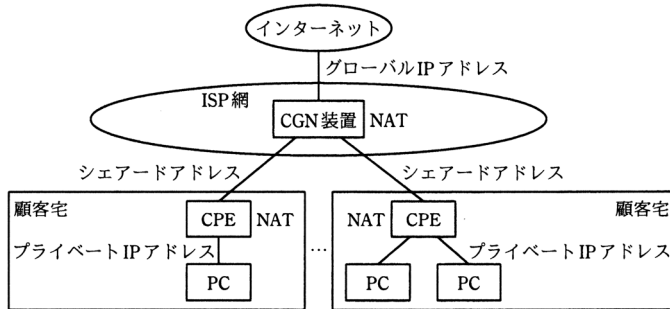


図 2 NAT444 の構成

図 2 に示したように、NAT444 では、インターネットと顧客宅の LAN との間、シェアードアドレスとして定義された、100.64.0.0/10 のネットワークプレフィックスのネットワークを設ける。NAT444 の“444”は、図 2 に示したように 3 種類のネットワークアドレスで運用されるネットワークを指し、各ネットワークの境界で NAT を実行することで、グローバル IP アドレスを節約する。

図 2 は、NAT444 の構成を示している。その大きな特徴は、インターネットと顧客宅内の LAN との間、すなわち ISP 網内に、シェアードアドレスを定義していることである。

シェアードアドレスとは、CGN の実現のために IANA で割り当てられたアドレスであり、RFC6598 で標準化されている。アドレスの範囲は 100.64.0.0/10 であり、IP アドレス数は約 400 万個以上である。

第 1 段落の中を見ると、シェアードアドレスの使い方を理解できる。

従来は顧客に一つずつグローバル IP アドレスを割り当てていたが、「これをシェアードアドレスに置き換え（る）」旨、記されている。従来は、顧客宅内の複数のプライベート IP アドレスが 1 個のグローバル IP アドレスを共用し、インターネットにアクセスしていた。CGN では、複数のプライベート IP アドレスが 1 個のシェアードアドレスを共用する。



更に、「複数の顧客間でグローバル IP アドレスを共用する」と記述されている。顧客に一つずつシェアードアドレスを割り当てているので、複数のシェアードアドレスが1個のグローバル IP アドレスを共用し、インターネットにアクセスすることが分かる。

このアドレスの共用を実現する仕組みが NATP である。本文はこれを「IP アドレスとポート番号を対にした変換」と記している。この変換は、「2 回行われる」。1 回目は、プライベート IP アドレスからシェアードアドレスへの変換であり、CPE で実施される。2 回目は、シェアードアドレスからグローバル IP アドレスへの変換であり、ISP 網内の CGN 装置で実施される。

ネットワークスペシャリスト試験を受験する読者にとって、NAPT は前提知識であるため、ここでは解説を省略する。念のため、詳しくは本書の第3章「3.7.1 NAT / NAPT」を参照されたい。

ISP が従来から実施している NATP(プライベート IP アドレスからグローバル IP アドレスへの変換)にせよ、あるいは、NAT444 における2回の NATP にせよ、IP アドレスの共用を実現するため、TCP/UDP ポート番号の分配が行われている。

CGN 装置が実施する NATP におけるポート番号の分配について、第4段落の中で、次のように記述されている。

CGN では、16 ビットで構成されている TCP/UDP ポート番号を複数の顧客に分配するので、1 顧客が使用できるポート数が少ない。例えば、CGN 装置に設定する 1 顧客に割り当てるポート数が、実際に使うポート数よりも少ない場合、Web ページの閲覧などで不具合が発生してしまう。そこで、仮に、1 顧客に割り当てるポート数を 10,000 に設定したとすると、インターネット接続サービスで使用するグローバル IP アドレスを約  $1/6$  に削減できる。

第4段落は、具体的な数値を挙げて説明している。ここには「インターネット接続サービスで使用するグローバル IP アドレスを約  $1/6$  に削減する」とある。分かりやすく言い換えると、6 か所の顧客宅があり、それぞれに1個ずつシェアードアドレスを割り当てている。それゆえ、これら6個のシェアードアドレスが1個のグローバル IP アドレスを共用している。

この場合、16 ビットあるポート番号を6か所に分配する必要がある。16 ビット長に相当するポート数は 65,536 である。ウェルノウンポート番号等を除いても、NAPT で使用できるポート数は 60,000 を下らない。それゆえ、単純に計算すると、1 顧客に割り当てることができるポート数は、「10,000」となるわけだ。

NAT444 では、CPE においても NATP を実施するため、ここでもポート番号の分配が行われる。1 か所の顧客宅の中に複数のクライアント端末があり、それぞれの端末に 1 個ずつプライベート IP アドレスを割り当てている。端末数を  $N$  台とすると、1 端末に割り当てることができるポート数は、「 $10,000 / N$ 」となる。

### ● NAT444 で 2 回の NATP を実施した例

ここまで解説した内容について、具体例を用いて補足しよう。

今、顧客宅内の LAN にある PC から、インターネット上の Web サーバにアクセスするものとする。

PC は、デフォルトゲートウェイである CPE にパケットを転送する。

CPE は、これを受け取ると 1 回目の NATP を実施し、デフォルトゲートウェイである CGN 装置にパケットを転送する。

CGN 装置は、これを受け取ると 2 回目の NATP を実施し、Web サーバにパケットを転送する。

ここで、Web サーバの IP アドレスを「W」とする。PC から Web サーバに送信されるパケットは、宛先 IP アドレスが「W」、宛先ポート番号が「80」となる。

NAPT が変換するのは、送信元 IP アドレスと送信元ポート番号の対である。

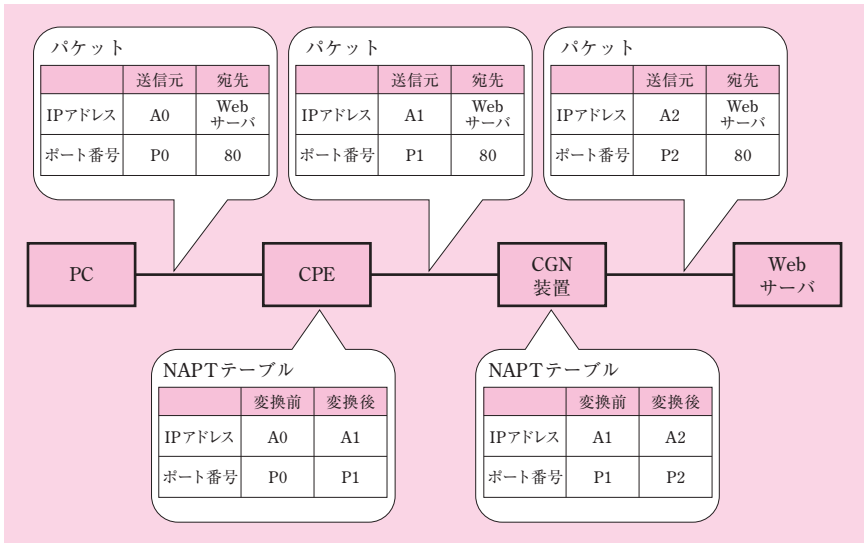
PC が送信した時点の送信元 IP アドレスを「A0」、送信元ポート番号を「P0」とする。

1 回目の NATP で、CPE は送信元 IP アドレスを「A1」、送信元ポート番号を「P1」に変換する。A1 はシェアードアドレスであり、複数のプライベート IP アドレスで共用される。プライベート IP アドレスごとに異なるポート番号を対応付けることによって、アドレスの共用を実現している。

2 回目の NATP で、CGN 装置は送信元 IP アドレスを「A2」、送信元ポート番号を「P2」に変換する。A2 はグローバル IP アドレスであり、複数のシェアードアドレスで共用される。ここでも、シェアードアドレスごとに異なるポート番号を対応付けることによって、アドレスの共用を実現している。

NAPT を実施した装置は、変換前後の IP アドレスとポート番号の組を NATP テーブルに登録している。Web サーバから返信パケットを受信したら、テーブルに登録された内容に基づいて逆変換を行う。

以上のまとめとして、一連の NATP を次の図に示しておこう。



図：NATP が2回実施される様子

### ● NAT444 導入時の問題点

第3段落は、NAPTの導入に伴う問題点に言及している。

NAT444を導入すると、一部のアプリケーションの動作に不具合が発生する危険性がある。その主因として想定されるのは、次に示す2点である。

- (1) 1顧客が開設できるセッション数の制限
- (2) 通信経路中のNAT介在

第4段落は、主因(1)について詳しく説明している。

前述のとおり、NAT444では2回のNAPTを実施しており、それぞれのNAPTでTCP/UDPポート番号の分割が行われている。割り当てるポート数は、同時に開設できるコネクション数(セッション数)と同じである。それが(1)のいう、「セッション数の制限」をもたらしている。

例えば、Ajaxの機能を使ったページの中には、利用者が閲覧している背後で、多数のセッションを同時に開設している。1顧客内の同時利用者数が多い時間帯で、このようなページを閲覧していると、同顧客に分配したポート数の上限に達してしまう可能性がある。

続く第5～第6段落は、主因(2)について詳しく説明している。

アプリケーションの中には、自ホストの IP アドレスやポート番号を、アプリケーション層プロトコルのやり取りで通知するものがある。NAT 機器がネットワーク層とトランスポート層を書き換えることにより、アプリケーション層の通知内容と齟齬が生じ、通信が成り立たなくなってしまう。

第5段落は、その例として、アクティブモードで動作する FTP と、SIP を挙げている。

第7段落で言及されている IPsec も、主因(2)がもたらす問題を抱えた通信である。ただし、第5段落で指摘されたものとは、問題の内容が異なっている。どのような問題があるのかは、[IPsec を利用する顧客への対応策]の中で具体的に説明されている。この点については設問3で取り上げられているので、詳しくはそこで解説しよう。

参考までに、CGN の仕組みや CGN の抱える問題点について、具体例を交えながら簡潔に説明しているサイトがあるので、紹介しておく。

インターネット 10 分講座：大規模 NAT (Large Scale NAT:LSN) あるいはキャリアグレード NAT (CGN)

<https://www.nic.ad.jp/ja/newsletter/No41/0800.html> (URL は本書執筆時点のものです)

ここまで理解できれば、設問2を解く準備は整った。それでは、いよいよ小問の解説に移ろう。

## (1)

### 解答例

P	C	の	ネ	ッ	ト	ワ	ー	ク	ア	ド	レ	ス	と	,	C	P	E	と	C	G	N	装	置	間
の	ネ	ッ	ト	ワ	ー	ク	ア	ド	レ	ス	が	重	な	っ	た	と	き	(43字)						

問題文は、「本文中の下線(あ)について、シェアードアドレスではなく、プライベート IP アドレスを用いたときに、インターネットアクセスができなくなる不具合が発生する可能性がある。どのような場合に発生するかを、図2中の機器名称を用いて……述べよ」と記述されている。

下線(あ)は、[NAT444の調査]の第2段落の中にある。そこには、「NAT444では、インターネットと顧客宅の LAN との間に、(あ)シェアードアドレスとして定義された、100.64.0.0/10のネットワークプレフィックスのネットワークを設ける」と記述されている。

「インターネットと顧客宅の LAN との間」とは、ISP 網にある、CPE と CGN 間のネットワークを指す。本問は、このネットワークにプライベート IP アドレスを割り当てる運用を行ったとの仮定を置き、ある条件が成立した場合、「インターネットアクセスができなくなる」と述べている。ここで問われているのは、その条件とは具体的に「どのような場合」であるか、という点である。

顧客は、自ネットワークにプライベート IP アドレスを自由に割り当てて運用している。したがって、CPE と CGN 間のネットワークにプライベート IP アドレスを割り当ててしまうなら、既に顧客が使用しているネットワークアドレスと重なってしまう可能性がある。

この点について、具体例を使って解説しよう。

説明を分かりやすくするため、CPE と CGN 装置間には 1 個のネットワークセグメントしか存在しないものとする。以下の解説で、このセグメントを「ISP セグメント」と呼ぶことにしよう。なお、ISP セグメントが複数のサブネットに分割されていようとも、結論は変わらない。

ISP セグメントに割り当てたネットワークアドレスを「192.168.0.0/27」とする。このネットワークには、CGN 装置と配下の CPE を合わせて、最大  $30 (= 2^5 - 2)$  台の機器を接続する。CGN 装置の外側には、変換用のグローバル IP アドレスを 5 個用意している。つまり、1 個のグローバル IP アドレスを、約 6 か所の顧客宅の CPE で共用するわけだ（ちなみに、顧客宅数を 6 とした理由は、第 4 段落の説明に登場する具体例に合わせたためである）。

このうちの 1 台の CPE において、顧客セグメントに割り当てているネットワークアドレスが、ISP セグメントに割り当てているものと重なっていたとしよう。

重なるパターンは全部で 3 種類ある。それは、(Ⅰ) サブネットマスク長が同じ場合、(Ⅱ) ISP セグメントのサブネットマスク長が顧客セグメントより長い場合、(Ⅲ) ISP セグメントのサブネットマスク長が顧客セグメントより短い場合、である。

一つ言えることは、CPE が起動する時点でこのような設定を異常と判断し、起動しない可能性がある。そうなれば、インターネットアクセスはできなくなる。

もしも CPE が起動した場合、インターネットアクセスの通信はどのように行われるだろうか。

顧客セグメントからインターネットにパケットを送信するとき、NAPT によるアドレス変換が行われる。このとき、顧客端末の IP アドレスと変換後の IP アドレスがたまたま一致していたら、NAPT に失敗したと判断してパケットを転送しない可能性がある。

NAPT に成功したならば、CPE から CGN 装置に転送され、そこからインターネットに出ていく。つまり、送信も成功することになる。

それでは、インターネットから返信されたとき、どうなるだろうか。まず、CGN 装置から元の CPE にパケットが転送される。問題が発生する可能性があるのは、CPE が NAPT の逆変換を実施した後、ルーティングテーブルに基づいてパケットを転送するときである。(Ⅰ)～(Ⅲ)のどの場合に該当するかによって結果が異なってくる。

(Ⅰ)の場合、顧客側も ISP 側も同一のネットワークプレフィックスになっているため、ロングストマッチアルゴリズムでは宛先を決定できない。それゆえ、インターネットアクセスの通信に失敗する。このような理由で、そもそも CPE は異常と判断し、起動しないに違いない。

(Ⅱ)の場合、二つのケースがあり得る。本来の返信先となる顧客端末（最初に送信した端末）の IP アドレスが、ISP セグメントのネットワークアドレスの範囲内にあるケース、及び、そうではないケースである。

前者のケースでは、ロングストマッチアルゴリズムに基づき、CPE は ISP 側に宛先があると判断し、ISP セグメント内で同一 IP アドレスをもつ CPE に転送を試みる。それゆえ、インターネットアクセスの通信に失敗する。

後者のケースでは、CPE は顧客側に宛先があると判断する。それゆえ、通信に成功する。

(Ⅲ)の場合、ロングストマッチアルゴリズムに基づき、CPE は顧客側に宛先があると判断する。それゆえ、通信に成功する。

以上をまとめると、成功する可能性もあるが、失敗する可能性もあると言える。失敗するとしたら、そもそも CPE が起動しないかもしれず、送信時の NAPT で失敗するかもしれず、返信時の転送で失敗するかもしれない。

これまで解説してきたことは、顧客セグメントのネットワークアドレスと、IPS セグメントのそれとが重なっている場合にのみ生じることだ。したがって、この旨を解答すればよい。

よって、正解は解答例に示したとおりとなる。

## (2)

### 解答例

① 送信元 IP アドレス (9字)

② 送信元ポート番号 (8字)

③ アクセス時刻 (6字)

問題文は、「顧客宅の PC がインターネット上の Web サーバにアクセスしたとき、

PCを特定するのにWebサーバがログとして記録する必要がある情報を三つ挙げ(よ)」と記述されている。

設問2の冒頭の「●NAT444で2回のNAPTを実施した例」で解説したとおり、顧客のPCがインターネットにアクセスするとき、NAT444によりNAPTが2回実施されてパケットがインターネットに出ていく。

ここでは、前述の例を再び用いて、本問の解を導こう。

PCが送信した時点の送信元IPアドレスを「A0」、送信元ポート番号を「P0」とする。

1回目のNAPTで、CPEは送信元IPアドレスを「A1」、送信元ポート番号を「P1」に変換する。

2回目のNAPTで、CGN装置は送信元IPアドレスを「A2」、送信元ポート番号を「P2」に変換する。

Webサーバが受信するパケットは、送信元IPアドレスがA2、送信元ポート番号がP2である。

Webサーバがこれに返信したとき、PCはそのパケットを受信する。このことから、送信元のIPアドレスとポート番号の組「A2、P2」と「A0、P0」が、1対1に対応していることが分かる。

ただし、この対応付けは、当該通信が行われている間だけ有効なものである。ひとたび通信が終了すると、IPアドレスとポート番号を対とした変換が、別の通信に実施されるからだ。したがって、送信元を特定するには、アクセスした時刻の情報も必要となる。

以上をまとめると、Webサーバが送信元のPCを特定するのに必要な情報は、送信元IPアドレス、送信元ポート番号、アクセス時刻となる。

よって、正解は解答例に示したとおりとなる。

### ■設問3

設問3の解説に入る前に、IPsec、及び、IPsec NATトラバーサルについて解説する。

ネットワークスペシャリスト試験において、IPsecプロトコルや通信モードなどは、前提知識に位置付けられている。そのことは、これらが本文中で説明されていないことから明らかである。それゆえ、ここでは、IPsecに関し、設問3を解くのに必要となる「IPsecプロトコル」「通信モード」「IKE」だけを取り上げて解説する。より詳しくは本書の第8章「8.4.5 IPsec」を参照されたい。

一方、IPsec NATトラバーサルは、IPsec通信をNAT経由で行うときに必要な技術であり、本文の中で詳しく説明されている。これを受けて、本文の説明を補足しつつ詳しく解説することにしよう。

## ● IPsec プロトコル (AH, ESP)

IP パケットを IPsec でカプセル化するプロトコルは2種類ある。IPsec 通信では、どちらか一方 (又は両方) を用いることができる。一つ目は AH (Authentication Header) であり、二つ目は ESP (Encapsulating Security Payload) である。AH, ESP のどちらも、IP の上位層プロトコルに位置付けられる。

AH は、パケットのメッセージ認証 (改ざん検出) とリプレイ攻撃防止の機能を備えている。ESP は、AH の機能に加えて、ペイロードを暗号化する機能を備えている。

## ● 通信モード (トランスポート, トンネル)

IPsec は、通信経路上でカプセル化する範囲を一部の区間とするのか、それとも全区間とするのかに応じて、2種類ある通信モードのうち一つを選択する。全区間にわたって実施する場合はトランスポートモードを用い、一部の区間だけで実施する場合はトンネルモードを用いる。

これら二つのモードは、IPsec の機能を、通信経路上のルータがもつか、終端ノードがもつかによって使い分ける必要がある。以下の解説で、IPsec の機能をもつ IP ノードをゲートウェイと呼ぶことにする。

### ● トランスポートモード

トランスポートモードでは、ゲートウェイになる IP ノードは2台の終端ノードである。それゆえ、通信経路全体がカプセル化の範囲となる。

送信側ノードは、IP パケットを組み立てた後、カプセル化してから IPsec パケットを送信する。

受信側ノードは、IPsec パケットを受信し、カプセル化を解除して IP パケットを取り出す。その後は IP パケット受信時と同じ処理をする。

### ● トンネルモード

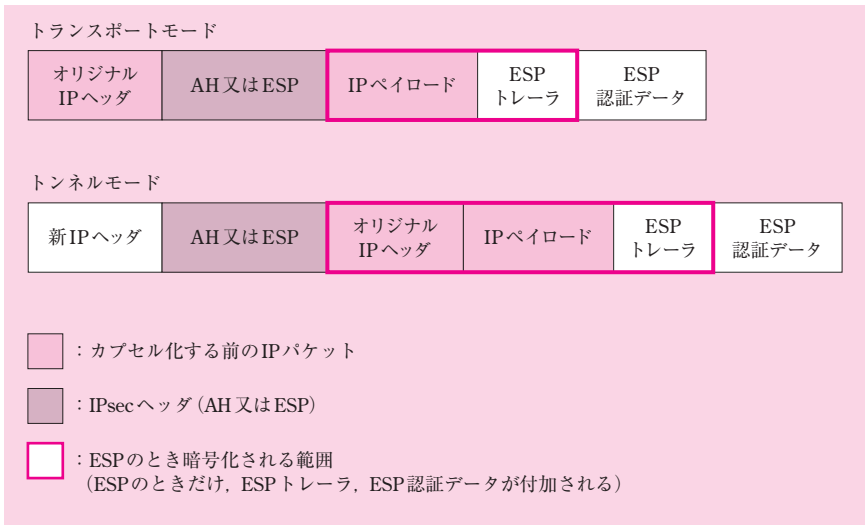
トンネルモードでは、ゲートウェイになる IP ノードは、ルータであっても終端ノードであってもよい。つまり、通信経路上の2台のルータがゲートウェイになることも、1台のルータと1台の終端ノードがゲートウェイになることもある。これら2台のゲートウェイで挟まれた区間が、カプセル化の範囲となる。

ゲートウェイは、カプセル化区間側に IP パケットを送信するとき、カプセル化してから IPsec パケットを送信する。一方、カプセル化区間側から IPsec パケットを受信したとき、カプセル化を解除して IP パケットを取り出す。その後は IP パケット受信



時と同じ処理をする。

次の図は、トンネルモード、トランスポートモードのカプセル化区間を流れる IP パケットのフォーマットを示している。



図：カプセル化区間を流れる IP パケットのフォーマット

図中の「オリジナル IP ヘッダ」と「IP ペイロード」は、カプセル化前のオリジナルの IP パケットである。

カプセル化区間では、IP の上位層は IPsec となる。図中の「AH 又は ESP」は、IPsec ヘッダであり、AH ヘッダ又は ESP ヘッダとなる。

トランスポートモードは、オリジナル IP ヘッダと IP ペイロードの間に IPsec ヘッダを挿入する。トランスポートモードのペイロード（IPsec ヘッダの後続部分）に該当する部分は、IP ペイロードとなる。

トンネルモードは、新 IP ヘッダと IPsec ヘッダを先頭に付与する。トンネルモードのペイロードに該当する部分は、オリジナル IP ヘッダと IP ペイロードである。

IPsec プロトコルが ESP のとき、ペイロードの後に ESP トレーラと ESP 認証データが付加される。このペイロードと ESP トレーラを合わせた部分が、暗号化範囲となる。

## ●セキュリティポリシ

ゲートウェイは、受信したパケットの種類を調べ、その種類に応じて動作を決定す

る。カプセル化対象の IP パケットであるか、又は、カプセル化解除対象の IPsec パケットであれば、ゲートウェイとして動作する。さもないと、通常の IP ノード（ルータ又は終端ノード）として動作する。

パケットの種類を識別する情報をセレクトといい、IP アドレス、ポート番号、上位層プロトコル、等がある。

セレクトに応じた動作は、PROTECT（IPsec の処理を行う）、BYPASS（IPsec の処理を行わず、通常の処理を行う）、DISCARD（パケットを破棄する）の3種類がある。

この決定を下すための情報（セレクトと動作の組）をセキュリティポリシーという。ゲートウェイは複数のセキュリティポリシーをもつことができ、SPD（Security Policy Database）に登録される。

## ● IKE

IPsec の通信に先立ち、ゲートウェイは、通信に必要な情報を交換する。そのやり取りに用いられるプロトコルが、IKE（Internet Key Exchange）である。

交換する情報には、メッセージ認証と暗号化を処理するアルゴリズム、メッセージ認証と暗号化に使用する鍵、お互いのエンティティ認証のためのデータ（事前共有鍵や電子署名など）、使用する IPsec プロトコル（AH、ESP）、使用する通信モード（トンネルモード、トランスポートモード）、等である。

## ● IPsec NAT トラバース

本文に詳しく説明されているので、適宜抜粋しながら解説していこう。

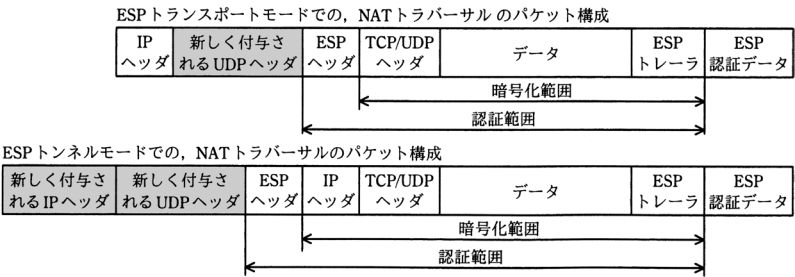
まず、[IPsec を利用する顧客への対応策] の第1～第2段落には次のように記述されている。

NAT 機能を経由した通常の IPsec の通信は、AH、ESP 及び IKE プロトコルで問題が発生する。NAT 機器を経由した IPsec 通信で発生する問題を、表 1 に示す。

表 1 NAT 機能を経由した IPsec 通信で発生する問題

プロトコル名	問題の内容
AH	トランスポートモード、トンネルモードともに、 <u>(い) IP アドレス変換が行われると認証エラーが発生する。</u>
ESP	トランスポートモード、トンネルモードともに、AH のような問題は発生しない。しかし、 <u>(う) どちらのモードでもポート変換を行えないので、ESP でカプセル化されたパケットは、NAT 機器を通過することができない。</u>
IKE	ISAKMP メッセージは、送信元ポート、宛先ポートともに UDP の 500 番の使用が求められるので、NAT 機器でポート番号を変換できない。

表 1 の問題を解決する手段として、ESP プロトコルに対して IPsec NAT トラバーサルが規格化された。IPsec NAT トラバーサルは、ESP パケットを UDP でカプセル化することによって、NAT 機能による IP アドレスとポート番号の変換を可能にしている。IPsec NAT トラバーサルのパケット構成を、図 3 に示す。



注記 網掛け部分は、NAT トラバーサルで新たに付与されるヘッダを示す。

図 3 IPsec NAT トラバーサルのパケット構成

表 1 中の下線 (い)、(う) は設問 3 で出題されているため、そこで詳しく解説する。

表 1 の問題を解決するため、IPsec NAT トラバーサルが規格化された。NAT トラバーサルで使用できる IPsec プロトコルは、ESP のみである。

本文の図 3 を見ると、IPsec NAT トラバーサルでは、IP ヘッダと ESP ヘッダの間に UDP ヘッダが挿入されている。通信経路上の NAT 機器が NAT を実施するとき、この UDP ヘッダ中のポート番号を変換する。

IPsec 通信で NAT トラバーサルを使うには、まずこれがどうかを前もって判断する。IPsec 通信に先立ってやり取りされる IKE 通信で、この判断を行う。その点について、第3段落には次のように記述されている。

UDP によるカプセル化は、IKE で次のように自動的に決定される。

- IKE は、IPsec を使用する機器間で ISAKMP メッセージを受信する際に、経路上に NAT 機器が存在するかどうかを検査する。
- NAT 機器を検出した場合、ISAKMP メッセージの送信元ポート番号及び宛先ポート番号を 500 から 4500 に変更して、NAT トラバーサルを使用することを通知する。このとき、NAT が行われると送信元ポート番号が変換されるので、(え) IPsec を使用する機器の、受信パケットに対するフィルタリング設定を変更する必要がある。

本文中の下線 (え) は設問3で出題されているため、そこで詳しく解説する。

最初の箇条書きに、「ISAKMP メッセージ」とあるが、これは IKE 通信でやり取りされるメッセージを指している。IKE 通信のポート番号は、送信元と宛先の両方とも 500 番である。通信経路上に NAT 機器があると、パケットの送信元ポート番号が変換される。ISAKMP メッセージを送受信する際、つまり、1 往復のやり取りをする際、2 台のゲートウェイはそれぞれ、受信したパケットの送信元ポート番号が 500 番から変化しているかどうかを検知する。これにより、「経路上に NAT 機器が存在するかどうか」を判断している。

2 番目の箇条書きには、NAT 機器を検出した後の動作が説明されている。そこに記されているとおり、「ISAKMP メッセージの送信元ポート番号及び宛先ポート番号を 500 から 45000 に変更して、NAT トラバーサルを使用することを通知する」。

ここまで理解できれば、設問3を解く準備は整った。それでは、いよいよ小問の解説に移ろう。

## (1)

### 解答例

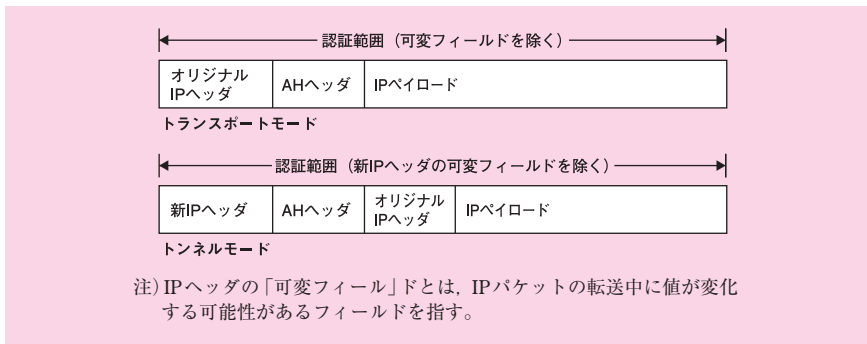
I	P	ヘ	ッ	ダ	が	認	証	対	象	な	の	で	,	I	P	ア	ド	レ	ス	が	書	き	換	え
ら	れ	る	と	認	証	デ	ー	タ	が	計	算	値	と	一	致	し	な	く	な	る	か	ら		(48字)

問題文は、「表1中の下線(い)の認証エラーが発生する理由を、認証対象に着目して……述べよ」と記述されている。

下線(い)は、[IPsecを利用する顧客への対応策]の表1「NAT機器を経由したIPsec通信で発生する問題」の中にある。プロトコルがAHである場合、「トランスポートモード、トンネルモードともに、(い) IPアドレス変換が行われると認証エラーが発生する」と記述されている。

AHは、パケットのメッセージ認証を行い、認証データをAHヘッダ中に格納している。

認証範囲は、トランスポートモード、トンネルモードともに、IPパケット全体に及んでいる。

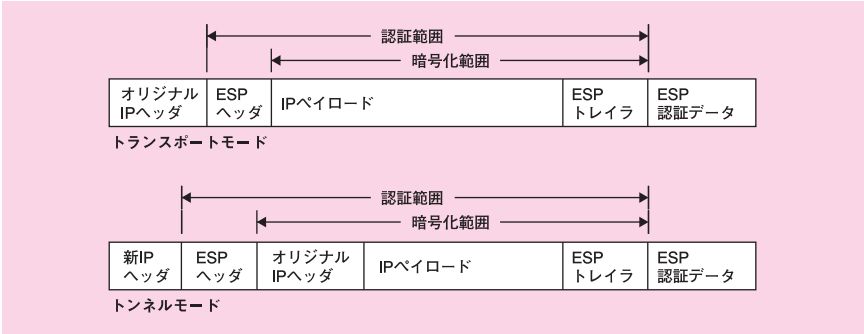


図：AHの認証範囲

したがって、NAT機器でIPアドレスの変換が行われると、AHヘッダ中の認証データと齟齬が生じる。受信側のゲートウェイでカプセル化を解除する際、受け取ったIPパケットからメッセージ認証の値を計算し、これをAHヘッダ中の認証データと照合する。このとき、認証エラーが発生してしまうのだ。

よって、正解は、「IPヘッダが認証対象なので、IPアドレスが書き換えられると認証データが計算値と一致しなくなるから」となる。

参考までに、ESPもメッセージ認証の機能を備えているが、次の図に示すとおり、AHとは認証範囲が異なっている。経路上のNAT機器が変換するIPアドレスは、トランスポートモードにおいてはオリジナルIPヘッダの中に、トンネルモードにおいては新IPヘッダの中にあるが、それらはいずれも認証の対象ではない。したがって、下線(い)の問題はAH固有のものとなる。



図：ESP の認証範囲

(2)

**解答例**

T C P 又 は U D P ヘ ッ ダ が 暗 号 化 の 対 象 で あ り , ポ ー ト  
番 号 が 暗 号 化 さ れ て い て 分 か ら な い か ら (43 字)

又 は

E S P ヘ ッ ダ に は , ポ ー ト 番 号 が 存 在 し な い か ら (22 字)

問題文は、「表1中の下線(う)のESPにおいてポート変換が行えない理由を……述べよ」と記述されている。

下線(う)は、「IPsecを利用する顧客への対応策」の表1「NAT機器を経由したIPsec通信で発生する問題」の中にある。プロトコルがESPである場合、「トランスポートモード、トンネルモードともに、……(う)どちらのモードでもポート変換を行えないので、ESPでカプセル化されたパケットは、NAT機器を通過することができない」と記述されている。

IPパケットがIPsecでカプセル化されると、その上位層プロトコルはAH又はESPとなる。そのパケットフォーマットは、設問3の冒頭の図「カプセル化区間を流れるIPパケットのフォーマット」に示している。

この通信区間では、IPの上位層がTCP/UDPではないため、変換すべきポート番号が存在しない。したがって、カプセル化区間の経路上にあるNAT機器は、このIPパケットにNAPTを実施することができない。

よって、正解は、「ESPヘッダには、ポート番号が存在しないから」となる。

別解として、次のような解を導くこともできる。

オリジナル IP パケットの TCP/UDP ヘッダは IP ペイロードの中にある。何が何でも NATP を実施しようと画策するあまり、「IPsec のパケットフォーマットを解析し、IP ペイロード中の TCP/UDP ヘッダのポート番号を変換する」という特殊な NATP を思いつくかもしれない。

しかしながら、このアイデアはうまくいかない。なぜなら、IPsec プロトコルが ESP であるとき、TCP/UDP ヘッダを含む IP ペイロードは、暗号化の対象となるからだ。ポート番号が暗号化されている以上、その変換は端から無理な話となる。つまり、そのような特殊な NAT は実現できない（本問の趣旨から外れるが、AH であるときは、ポート番号の変換が認証エラーを引き起こすため、やはりうまくいかない）。

要は、このような奇抜なアイデアをもってしても、いわず何をしようにも、NAPT は不可能だという結論に至る。

本問は ESP について問うているので、その点を踏まえると、もう一つの正解は、「TCP 又は UDP ヘッダが暗号化の対象であり、ポート番号が暗号化されていて分からないから」となる。

### (3)

#### 解答例

送	信	元	ポ	ー	ト	番	号	が	5	0	0	と	4	5	0	0	以	外	の	I	S	A	K	M
P	メ	ッ	セ	ー	ジ	も	受	信	で	き	る	よ	う	に	す	る								

(43字)

問題文は、「本文中の下線（え）で必要とする変更を……述べよ」と記述されている。

下線（え）を含む文章は、「IPsec を利用する顧客への対応策」の第3段落の2番目の箇条書きの中にある。その中には、「NAT 機器を検出した場合、ISAKMP メッセージの送信元ポート番号及び宛先ポート番号を 500 から 4500 に変更して、NAT トラバースを使用することを通知する。このとき、NAT が行われると送信元ポート番号が変換されるので、（え）IPsec を使用する機器の、受信パケットに対するフィルタリング設定を変更する必要がある」と記述されている。

下線（え）に「IPsec を使用する機器」とあるが、これは IPsec 機能をもつ機器のことである。設問3の解説の冒頭の「●通信モード（トランスポート、トンネル）」では「ゲートウェイ」と呼んでいる。2台のゲートウェイで挟まれた区間で、ISAKMP メッ

セージ、IPsec パケットをやり取りする。

本問は、「NAT が行われると送信元ポート番号が変換される」という状況に適應できるように、受信パケットに対するフィルタリングをどのように設定するかを問うている。

設問3の解説の冒頭の「●IPsec NAT トラバーサル」で述べたとおり、NAT 機器が介在していない通信では、ISAKMP メッセージのポート番号は、送信元と宛先の両方とも 500 番である。しかし、NAT 機器が介在していると、送信元ポート番号が 500 番以外の値になる。

ゲートウェイは、送信元ポート番号の変化を検知し、受信したパケットの送信元ポート番号が 500 番から変化しているかどうかを検知する。これにより、第3段落にあるとおり、「経路上に NAT 機器が存在するかどうか」を判断している。

NAT 機器を検出した場合は、「送信元ポート番号及び宛先ポート番号を 500 から 4500 に変更して、NAT トラバーサルを使用することを通知する」。当然ながら、送信元ポート番号は、NAT 機器を経由するときに 4500 から変化する。

したがって、ISAKMP メッセージの送信元ポート番号が 500 番以外、4500 番以外であっても、これを ISAKMP メッセージとして受信できるようにフィルタリングを設定する必要がある。

よって、正解は解答例に示したとおりとなる。

## ■設問4

設問4の解説に入る前に、マルチキャスト通信について解説する。

マルチキャスト通信の全貌を理解するには、次に示す三つの知識を学習する必要がある。

- マルチキャストグループ
- マルチキャストグループへの参加と離脱
- マルチキャスト通信の経路制御

ただし、本問を解くに当たり、これらに熟知していることを前提とはしていない。主に問われているのは2番目に挙げた、マルチキャストグループへの参加と離脱であるが、その仕組みは本文中に詳しく説明されている。

ここでは、本問を解くのに必要な程度まで、マルチキャスト通信に関する基本的な知識を解説することにしよう。



## ●マルチキャストグループ

マルチキャスト通信は 1 対多で行われる通信である。マルチキャストグループのメンバーとなっている各ノードに向けて、同時に配信することができる。

マルチキャスト IP アドレスは、マルチキャストグループを識別する役割をもつ。つまり、あるマルチキャスト IP アドレスを宛先とするパケットは、そのアドレスが示すグループを宛先としている。したがって、そのパケットは、当該グループの各ノードが受信する。

マルチキャスト IP アドレスは、224.0.0.0/8 の範囲にある。更に、主要な用途に応じて幾つかのブロックに分けられている。このうち幾つかのブロックは、IANA がアドレスの割当てを管理している。詳しくは、RFC5771「IANA Guidelines for IPv4 Multicast Address Assignments」を参照されたい。

ちなみに、本事例に登場するマルチキャスト IP アドレスは、224.1.1.1 ～ 224.1.1.4 である。これは、前述の RFC では「予約済み (RESERVED)」のブロックに含まれている。RFC は「アプリケーションは、IANA の予約済みブロックを使用してはならない (Applications MUST NOT use addressing in the IANA reserved blocks)」と述べている。とはいえ、試験問題で用いているに過ぎないので、厳密に考えなくてよいだろう。

## ●マルチキャスト通信の経路制御

IP マルチキャストルーティングプロトコルには幾つかの種類がある。

ここでは、PIM (Protocol Independent Multicast) を念頭に置いて、ごく基本的な仕組みを解説しよう。なお、PIM は、ネットワーク規模に応じて動作モードが複数用意され、最適な経路表生成のための工夫点がいろいろと盛り込まれているのだが、ここではその詳細に深入りしない。本問を解くには、マルチキャスト通信の経路制御の仕組みをざっくりとイメージできれば十分だからだ。

マルチキャストの経路制御には、ルータの 2 種類の動作が重要な役割を果たしている。

一つ目は、マルチキャストパケットの転送である。二つ目は、マルチキャスト経路表の生成である。

### ・マルチキャストパケットの転送

ルータは、送信元ノードからマルチキャストパケットを受信すると、(受信時点の) マルチキャスト経路表に従って、これを転送する。

転送する際、マルチキャストパケットが送信元ノードにループして戻ることがないように、送信元ノードの IP アドレスに基づき、既存の経路表 (ユニキャスト経路表等)

を用いてチェックする。受信インタフェースの先に送信元が存在していなければ、このインタフェースからのマルチキャストパケットは転送しない。これを RPF (Reverse Path Forwarding) という。

### ・マルチキャスト経路表の生成

マルチキャスト通信は、送信元と配信先が1対多の関係にある。

説明を分かりやすくするために、設問4の解説では、送信元ノードが1台しかなく、配信先ノードが1台以上あるとしよう。

このマルチキャスト通信を実現するに当たって、どのような経路情報をルータは生成したらよいだろうか。その答えは、経路の全体像がツリー構造をとることである。

このツリー構造のルートに位置するのが、送信元ルータ（送信元ノードを配下にもつルータ）である<sup>(\*)</sup>。一方、リーフに位置するのが、配信先ルータ（配信先ノードを配下にもつルータ）である。

(\*) PIM-Dense Mode では、ここに書いているように、送信元ルータをルートとし、配信先ルータをリーフとするツリー構造となる。

PIM-Sparse Mode では、マルチキャスト経路制御を集中管理する「ランデブーポイント」（以下、RP と称する）と呼ばれるルータを設ける。通常、この RP をルートとし、配信先ルータをリーフとするツリー構造を採用する。又は、RP を介さず、送信元ルータをルートとするツリー構造を採用することもできる。

本書では詳しい説明を割愛する。

以降、この解説では、ツリー構造のルートの側を上流、リーフの側を下流と呼ぶことにする。

特定のマルチキャストグループにおいて、上流から下流に向かうマルチキャストパケットの通信の流れは、次のようになる。この流れにおいて、複数の下流をもつルータは、それら全ての下流に向けてマルチキャストパケットを送出する。

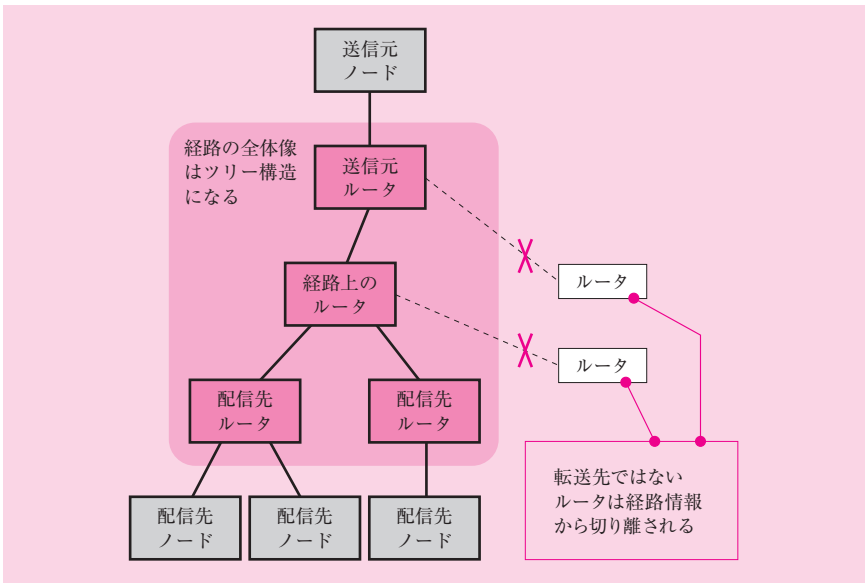
送信元ノード→送信元ルータ→

……経路上のルータ……→配信先ルータ→配信先ノード

送信元をルートとするこのツリー構造は、IP ネットワーク内で、送信元ごとに生成される。

なお、マルチキャストグループが自分の下流に存在しない場合、自分に向けてマルチキャストパケットを転送してもらう必要がない。無駄なトラフィックが流れないよ

う、自らをツリー構造の経路情報から切り離すことができるようになっている。



図：マルチキャスト通信の経路情報

このような経路構造は、どのように生成されるのだろうか。

ルータは、マルチキャストパケットを受け取ったとき、「どの送信元がこれを配信したのか、自分はこれをどのインタフェースから送出するのか」を判断する。RPFのチェックに成功したら、これを下流に向けて送出する。マルチキャスト経路表は、この判断を行うために存在している。

「下流」を知るには、宛先となるマルチキャストグループがどのサブネットに存在しているかが分かればよい。この情報をルータ間で伝達することによって、当該サブネットを配下にもつルータに向かうように、経路表を生成することができる。

結論から言うと、この情報は下流から上流に向かって順次伝達されてくる。

以下、幾つかのケースに分けて、生成の仕組みを解説しよう。ただし、ここではざっくりとしたイメージをつかんでいただくために、簡略化して書いている。本格的な説明は専門書を参照されたい。

#### ・配信先ルータ

自分のインタフェースに接続されたサブネットに、マルチキャストグループが存在

しているとしよう。言い換えると、当該グループの配信先ノードが存在しているとしよう。このとき、自分は配信先ルータである。

したがって、当該グループを宛先とするマルチキャストパケットが転送されるように、自分より上流にあるルータに伝達する必要がある<sup>(\*)</sup>。この情報伝達には、IP マルチキャストプロトコルのメッセージを用いる。

(\*) 「転送されるように伝達する」とここに述べたが、実際には、PIM のモードにより異なる。PIM-Dense Mode はマルチキャストパケットをデフォルトで転送するため、この情報を伝達する必要がない。一方、PIM-Sparse Mode はデフォルトでは転送しないため、下流から上流にこの情報を伝達する。  
後述の「上流ルータ」の説明も同様のことが言える。

マルチキャストグループの存否を、ルータはどのようにして知るのだろうか。それは、マルチキャストパケットの配信先ノードが、「特定のマルチキャストグループへの参加／離脱」を通知することにより、実現される。この仕組みについては、後ほど、「●マルチキャストグループへの参加と離脱」で詳しく解説しよう。

### ・上流ルータ

上流ルータについては、幾つかのケースに分けて解説する。

まず、一つ目のケースとして、自分のインタフェースに接続されたサブネットに、マルチキャストグループは存在していないが、配信先ルータが存在していたとしよう。この情報は、配信先ルータから伝達してもらうことで、知ることができる。このとき、自分は経路上のルータ（上流ルータ）であり、下流に向けてマルチキャストパケットを転送する立場にある。言うまでもなく、この下流とは、配信先ルータがいるインタフェースに他ならない。

したがって、当該グループを宛先とするマルチキャストパケットを転送されるように、自分より上流にあるルータに伝達する必要がある。この伝達には、IP マルチキャストプロトコルのメッセージを用いる。

次に、二つ目のケースとして、自分のインタフェースに接続されたサブネットに、マルチキャストグループは存在していないが、経路上のルータ（上流ルータ）が存在していたとしよう。この情報は、経路上のルータから伝達してもらうことで、知ることができる。このとき、自分もまた経路上のルータ（上流ルータ）であり、下流に向けてマルチキャストパケットを転送する立場にある。言うまでもなく、この下流とは、自分に伝達したルータがいるインタフェースに他ならない。

したがって、当該グループを宛先とするマルチキャストパケットが転送されるよう

に、自分より上流にあるルータに伝達する必要がある。

#### ・経路情報から切り離されるルータ

自分のインタフェースに接続されたサブネットに、マルチキャストグループが存在しておらず、配信先ルータも経路上のルータも存在していないでしょう。このとき、自分は経路情報から切り離されるべきである。

したがって、当該グループを宛先とするマルチキャストパケットが転送されないように、自分より上流にあるルータに伝達する必要がある<sup>(\*)</sup>。この情報伝達にも、IP マルチキャストプロトコルのメッセージを用いる。

(\*) 「転送されないように伝達する」とここに述べたが、実際には、PIM のモードにより異なる。PIM-Dense Mode はマルチキャストパケットをデフォルトで転送するため、下流から上流にこの情報を伝達する。一方、PIM-Sparse Mode はデフォルトでは転送しないため、この情報を伝達する必要がない。  
配信先ノードの離脱によって下流にグループが存在しなくなったときは、自らを切り離すため伝達する。

以上、ルータを3種類に分けて解説したが、このように下流から上流に向かって伝達された情報に基づき、各ルータは、マルチキャスト経路表を生成するのである<sup>(\*)</sup>。

(\*) この解説では最上流（ツリー構造のルート）を送信元としている。PIM-Dense Mode はデフォルトで転送するため、送信元ルータが自ずと最上流となる。PIM-Sparse Mode は、通常は RP が最上流となるが、下流（配信先ルータ）から上流（RP）に向かう情報伝達を通じてツリー構造が生成されることに変わりはない。RP を最上流とする場合、送信元ルータから RP へのマルチキャスト通信の経路はどうなっているのだろうか。簡単に言うと、送信元ルータは RP を知っているの、送信元ルータから RP にマルチキャストパケットが届けられる仕組みになっている。詳しい説明は専門書を参考されたい。

この点について、〔マルチキャスト通信の調査〕の第4段落の中では、次のように簡潔に述べられている。

マルチキャストグループが存在するサブネットの情報は、ルータ間で行われる IP マルチキャストルーティングプロトコルによって伝達され、各ルータでマルチキャスト経路表が生成される。

本問は特定の IP マルチキャストルーティングプロトコルの仕組みを出題している

わけではないので、これ以上は詳しく解説しないことにする。ここでは、最終的に「各ルータのマルチキャスト経路表が生成される」と考えればよい。

### ●マルチキャストグループへの参加と離脱

先ほど述べたとおり、マルチキャスト経路表を生成するには、ルータが「自分の配下に、マルチキャストグループの配信先ノードが存在しているか否か」を知る必要がある。

ルータはこれをどのようにして知るのだろうか。

それは、配信先ノードが、「特定のマルチキャストグループへの参加／離脱」を通知することによってである。この通知に用いられるのは、IGMPである。

#### ・IGMP

IGMP (Internet Group Management Protocol) とは、IP ネットワークでマルチキャスト通信を行うために、ルータと配信先ノードが使用するプロトコルである。IGMP は IP の上位層に当たる。主要な IGMP メッセージは、宛先 IP アドレスがマルチキャストアドレスである。TTL を 1 とする仕様になっているため、IGMP メッセージはルータを超えない。

IGMP の仕組みは、本文の中で詳しく説明されている。〔マルチキャスト通信の調査〕の第4～第6段落の中で、次のように記述されている。

マルチキャストグループが存在するサブネットの情報は、ルータ間で行われる IP マルチキャストルーティングプロトコルによって伝達され、各ルータでマルチキャスト経路表が生成される。PC が、あるマルチキャストグループに所属したり、離脱したりするのに、IGMP (Internet Group Management Protocol) が使用される。

ビデオサーバからマルチキャストグループ 224.1.1.1 宛ての画像データが配信されているときの、IGMP の通信例を図 5 に示す。

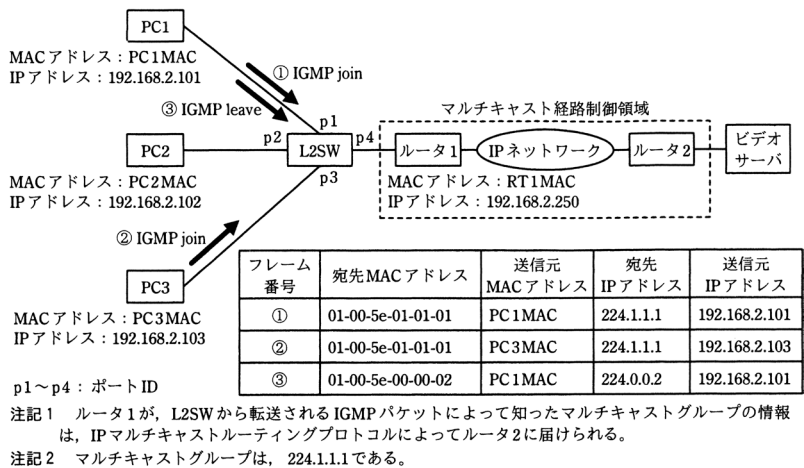


図 5 IGMP の通信例

図 5 の例では、IGMP が使用されるのは、PC とルータ 1 間である。(か) ビデオサーバとルータ 2 間では、IGMP は使用されない。PC が、あるマルチキャストグループに参加するときは、IGMP join メッセージによって、所属するサブネットのルータに対し、参加するマルチキャストグループを知らせる。逆に、PC が、参加しているマルチキャストグループから離脱するときは、所属するサブネットの全てのルータ宛てに、IGMP leave メッセージを送信する。

・マルチキャストグループへの参加

第 6 段落は、PC がマルチキャストグループに参加する方法を説明している。

そこには、「PC が、あるマルチキャストグループに参加するときは、IGMP join メッセージによって、所属するサブネットのルータに対し、参加するマルチキャストグループを知らせる」(\*)とある。

このように IGMP を通して知り得た情報が、マルチキャスト経路表の生成に用いられるわけだ。

(\*) 正確に言うと、IGMP join メッセージの宛先 IP アドレスは、参加するマルチキャストグループである。

図5の例では、①と②のフレームが、マルチキャストグループ「224.1.1.1」に参加するためにIGMP join メッセージを送信している。その宛先 IP アドレスは「224.1.1.1」となる。前述のとおり、IGMP メッセージの TTL は 1 なので、ルータを超えない。

### ・マルチキャストグループからの離脱

続く文章は、PC がマルチキャストグループから離脱する方法を説明している。

そこには、「逆に、PC が、参加しているマルチキャストグループから離脱するときは、所属するサブネットの全てのルータ宛てに、IGMP leave メッセージを送信する」(\*)とある。

もしも、マルチキャストグループへの参加ノードがサブネットに存在しなくなったならば、ルータはそのマルチキャストグループ宛での配信先となってはならない。それゆえ、ルータは、IP マルチキャストルーティングプロトコルのメッセージを用いてその旨を隣接ルータに伝える。それが伝達されていくことで、各ルータのマルチキャスト経路表が更新される。

(\*) 所属するサブネットの全てのルータを宛先とするには、IANA によって規定された「224.0.0.2」(ALLRouters) を宛先とするマルチキャストパケットを送信すればよい。

### ・マルチキャストグループの維持（参加ノードの存在確認）

本文中には登場しないが、IGMP には、ある重要なメッセージが規定されている。それは、ルータが、参加ノードの存否を検出するための IGMP query メッセージである。本問では出題されていないが、良い機会なので触れておこう。

このメッセージは、定期的送信される（デフォルトで 60 秒間隔）。これを受け取った PC が IGMP join メッセージを返信することで、ルータは参加ノードの存在を確認する。

なお、この返信は、ランダム時間経過後に 1 台の参加ノードだけが実行し、他の参加ノードは実行しない仕組みになっている。なぜなら、参加ノードが 1 台でも存在していれば、ルータはサブネットにマルチキャストを配信するので、最初の 1 台が返信すれば十分だからだ。残りの参加ノードは、1 台目の返信をマルチキャストで受け取って、返信を控えるようにする。

### ●具体例

これまで述べてきたことを、本文の図5を例にして説明しよう。

この図において、配信先となるマルチキャストグループは「224.1.1.1」である。



このマルチキャストグループにパケットを配信するノードは、ビデオサーバである。つまり、ビデオサーバは、224.1.1.1 を宛先とするマルチキャストパケットを配信する。

このマルチキャストグループに参加する配信先ノードは、PC1 と PC3 である。この点は、PC1 と PC3 が IGMP join メッセージ（図5中の①、②）を送っていることから分かる。なお、PC1 は、後に IGMP leave メッセージ（図5中の③）を送ってグループから離脱する。

ルータ1は、この IGMP メッセージのやり取りを通して、自分が接続しているサブネットに、マルチキャストグループ「224.1.1.1」に参加しているノードの存在を知る。

これに呼応して、ルータ1は、「自分は、224.1.1.1 宛てのパケットの転送先である」という情報を、IP マルチキャストルーティングプロトコルを用い、IP ネットワークに伝達する。

マルチキャスト経路表を生成するための情報は、IP マルチキャストルーティングプロトコルによって、最終的に、ルータ1からルータ2に伝達される。

この点を、図5の注記1は、「ルータ1が、L2SW から転送される IGMP パケットによって知ったマルチキャストグループの情報は、IP マルチキャストルーティングプロトコルによってルータ2に届けられる」と簡潔に説明している。

先ほど解説した「●マルチキャスト通信の経路制御」に照らし合わせると、下流がルータ1、上流がルータ2となる。図5の注記1は、経路表生成のための情報が、下流から上流に向かって伝達されていく様子を説明しているわけだ。

ここまで理解できれば、設問4を解く準備は整った。それでは、いよいよ小問の解説に移ろう。

## (1)

### 解答例

マ	ル	チ	キ	ャ	ス	ト	M	A	C	ア	ド	レ	ス	が	送	信	元	ア	ド	レ	ス	に	な	る
こ	と	が	な	い	か	ら	(32字)																	

問題文は、「本文中の下線（お）について、フラッディングされるのはマルチキャスト MAC アドレスが学習されないからである。その理由を……述べよ」と記述されている。

下線（お）を含む文章は、〔マルチキャスト通信の調査〕の第2段落の中にある。そこには、「（お）通常、L2SW は、受信したマルチキャストフレームを、受信ポート以外の全てのポートにフラッディングする」と記述されている。

これは一般的な知識から解を導く。

スイッチは、MAC フレームの受信を契機に、受信したポートの先に送信元ノードが存在していることを学習する。このとき学習した内容(受信ポートと送信元 MAC アドレスの対応付け)を、MAC アドレステーブルに登録する。これをアドレス学習という。

マルチキャストフレームを受信したとき、その送信元を学習することには変わりはない。このとき、送信元 MAC アドレスはどのようなになっているだろうか。

マルチキャスト通信は、送信元と宛先の対応が1対多になる通信である。つまり、送信元は1台のノードとなる。それゆえ、送信元 MAC アドレスは、そのノードが送信した NIC の MAC アドレスとなる。

この MAC アドレスは、特定の NIC を一意に識別できるものである。言い換えると、ユニキャスト通信の場合、宛先となり得るアドレスだ。つまり、マルチキャスト MAC アドレスが送信元 MAC アドレスになることはない。したがって、このアドレス学習の過程を通じて、マルチキャスト MAC アドレスが学習されることはあり得ない。

よって、正解は、「マルチキャスト MAC アドレスが送信元となることがないから」となる。

## (2)

### 解答例

ビデオサーバは、マルチキャストパケットを送信する側だから  
(28字)

問題文は、「本文中の下線(か)について、IGMPが使用されない理由を、図5の通信内容に着目して……述べよ」と記述されている。

下線(か)は、「マルチキャスト通信の調査」の第6段落の中にある。そこには、「(か) ビデオサーバとルータ2間では、IGMPは使用されない」と記述されている。

図5は、第5段落の下にある。図5について、第5段落には「ビデオサーバからマルチキャストグループ224.1.1.1宛ての画像データが配信されているときの、IGMPの通信例」と記述されている。

したがって、問題文が着目するように述べていた「通信内容」とは、「ビデオサーバがマルチキャスト通信の送信元ノードである」ということである。

結論から言うと、受信する側とは対照的に、送信する側は、マルチキャスト通信に先立って特別なメッセージをやり取りするわけではない。ただ、マルチキャストパケットを送信するだけでよい。

この点は、IGMPを使用するのはどのノードか、経路情報はどのように生成されるのかを考察することで、明らかになる。

IGMPについては、設問4の冒頭の「●マルチキャストグループへの参加と離脱」で解説している。そこで述べたとおり、IGMPを用いてルータに通知する必要があるのは配信先ノード、つまり、受信する側である。送信する側ではないわけだ。

経路情報の生成については、設問4の冒頭の「●マルチキャスト通信の経路制御」で解説している。そこで述べたとおり、経路情報は、配信先ノードからの通知をきっかけにして、下流から上流に向かう情報伝達を通じて生成されている。IPマルチキャストプロトコルの働きによって、送信元ルータをルートとするツリー構造が、ルータ側できちんと出来上がっているのだ。

したがって、送信元ノードは、マルチキャストパケットを送信するだけでよい。

この結論は、図5の注記1からも裏付けられる。そこには、「ルータ1が、L2SWから転送されるIGMPパケットによって知ったマルチキャストグループの情報は、IPマルチキャストルーティングプロトコルによってルータ2に届けられる」とある。

この記述から分かることは、「ルータの経路情報は、配信先ノードからの通知をきっかけにして、下流から上流に向かう情報伝達を通じて、既に生成済みである」ということだ。つまり、ルータ2は経路情報をもっている。

要するに、ビデオサーバは、自分に接続しているルータ2がマルチキャストパケットを受け取れば、後のことはルータ2に任せてよいのである。

以上をまとめると、ビデオサーバはマルチキャストパケットを送信する側なので、マルチキャストパケットを送信するだけでよい。受信する側と異なり、IGMPを使用してルータに伝達する必要がない。

よって、正解は、「ビデオサーバは、マルチキャストパケットを送信する側だから」となる。

### (3)

#### 解答例

ア：01-00-5e-01-01-01

イ：①を受信したとき：p1

②を受信したとき：p1, p3

③を受信したとき：p3

本問は、表2中の空欄ア、イについて、次の二つのことを問うている。

一つ目は、空欄アに入れる適切なマルチキャスト MAC アドレスを問うている。

二つ目は、空欄イに入れるポート ID である。ただし、ポート ID の内訳は、図5中の①～③のフレームを受信した順に遷移する。そこで、「①を受信したとき、②を受信したとき、及び③を受信したときのポート ID」をそれぞれ問うている。

表2は、「マルチキャスト通信の調査」の第8段落の中にある。表2について、第8段落には「図5中のL2SWでIGMPスヌーピング機能を働かせたとき、L2SWに作成されるMACアドレステーブルを、表2に示す」とある。したがって、表2は、図5のL2SWのMACアドレステーブルであり、IGMPスヌーピング機能を働かせたときに作成したものである。

IGMPスヌーピング機能については、第7段落の中で、次のように詳しく説明されている。

L2SWに実装されるIGMPスヌーピングによって、マルチキャストフレームに必要なポートだけに転送させることができる。IGMPスヌーピングとは、IGMPメッセージの中身をのぞき見することをいい、IGMPスヌーピング機能をもったL2SWは、IGMPメッセージの情報を基にMACアドレステーブルを更新する。J君が調査したL2SWでは、IGMP joinやIGMP leaveメッセージなどから、指定されたマルチキャストグループが存在するポートを知り、自分のMACアドレステーブルにマルチキャストエントリを作成する。通常、MACアドレステーブルには、複数のポートに同じMACアドレスが存在することはないが、マルチキャストMACアドレスは例外である。

本来、L2SWはマルチキャストフレームをフラッディングする。しかし、IGMPスヌーピング機能によって、「マルチキャストフレームに必要なポートだけに転送させることができる」。

これを実現するために、L2SWは「IGMPメッセージの情報を基にMACアドレステーブルを更新する」。MACアドレステーブルには、「マルチキャストエントリ」が作成される。

通常、MACアドレステーブルの中では、マルチキャストMACアドレスとポートIDが対応付けられることはない。しかし、IGMPスヌーピング機能を働かせた場合は、マルチキャストMACアドレスとポートIDとの対応付けが登録される。

マルチキャスト通信は1対多で行われるため、配信先ノードは複数のポートの先に存在している可能性がある。つまり、MACアドレステーブルの中で、1個のマルチキャストMACアドレスが複数のポートIDと対応付けられる可能性がある。この点について、「通常、MACアドレステーブルには、複数のポートに同じMACアドレスが存在す

ることではないが、マルチキャスト MAC アドレスは例外である」と記されている。

IGMP スヌーピングについて理解できたところで、改めて問題文を読み返すと、空欄イに入るポート ID は、図 5 中のフレーム①～③の受信によって遷移するとある。

図 5 を見ると、フレーム①～③は、IGMP join メッセージ、IGMP leave メッセージである。

これらのフレームは、MAC アドレステーブルに対し、2 種類の変化をもたらす。

一つ目は、MAC アドレス学習機能による、通常のエントリの作成である。つまり、フレーム①～③を送信したノードの MAC アドレスを、その受信ポートに対応付けて登録することである。

二つ目は、IGMP スヌーピング機能による、マルチキャストエントリの作成である。

表 2 を見ると、通常のエントリは既に記されている。フレーム①、フレーム③の送信元 MAC アドレスは PC1MAC であり、当該フレームの受信ポートは p1 である。そのエントリは 1 行目である。フレーム②の送信元 MAC アドレスは PC3MAC であり、当該フレームの受信ポートは p3 である。そのエントリは 2 行目である。それゆえ、残った 3 行目が、マルチキャストエントリだ。

したがって、ここで問われているのは、「フレーム①～③が示す IGMP join メッセージ、IGMP leave メッセージを L2SW が受け取ったとき、マルチキャストエントリがどのように作成され、更新されるか」ということである。

空欄アは、そのマルチキャスト MAC アドレスが入る。空欄イは、①～③で遷移するポート ID が入る。

ア

IGMP スヌーピング機能により作成されるマルチキャストエントリには、どのような値をもつマルチキャスト MAC アドレスが登録されるのだろうか。

第 7 段落には、IGMP スヌーピング機能について「マルチキャストフレームを必要なポートだけに転送させる」と記述されている。L2SW は、マルチキャストフレームを受信すると、その宛先 MAC アドレスを見て、これがマルチキャストであることを判断する。通常はフラッドイングするが、IGMP スヌーピング機能を働かせると、マルチキャストエントリに基づいて転送する。

したがって、L2SW がマルチキャストフレームを受信したとき、「マルチキャストエントリに、宛先 MAC アドレスと一致するマルチキャスト MAC アドレスが登録されていたら、そのエントリに登録されているポートからフレームを転送する」という仕組みになっていると推論できる。

それでは、図 5 に示された通信例において、マルチキャスト通信の宛先となるマルチキャスト MAC アドレスは、具体的にどのような値になるのだろうか。

図5のマルチキャスト通信について、第5段落には「ビデオサーバからマルチキャストグループ224.1.1.1宛ての画像データが配信されている」と記述されている。それゆえ、マルチキャストグループは、「224.1.1.1」である。

IPパケットの宛先がマルチキャストIPアドレスであるとき、これを格納するイーサネットフレームの宛先はマルチキャストMACアドレスになる。この点は、設問1の空欄eで解説した。

具体的には、次のようにMACアドレスが生成される。

- 1～24番目のビット列は、「01-00-5e」になる
- 25番目のビットは、「0」になる
- 26～48番目のビット列（下位23ビット）は、IPv4アドレスの下位23ビットをそのまま埋め込む

したがって、「224.1.1.1」というIPv4マルチキャストアドレスの場合、宛先MACアドレスは、「01-00-5e-01-01-01」となる。

よって、空欄アに該当するMACアドレスは、「01-00-5e-01-01-01」である。

## イ

L2SWのIGMPスヌーピング機能により、IGMPメッセージを受け取ると、マルチキャストエントリが作成されたり、更新されたりする。

問題文には、表2のエントリを生成する条件として、「表2は、PC1、PC2、PC3がマルチキャストグループに参加していない状態から、図5中の①～③のフレームを受信して作成されるものとする」とある。

項番①のフレームは、IGMP join（グループへの参加）メッセージである。送信元はPC1であり、そのMACアドレスがPC1MACである。L2SWの受信ポートがp1である。

したがって、L2SWは、p1の先にPC1が存在し、マルチキャストグループへの参加を通知していることが分かる。この内容に基づき、次に示すとおり、当該グループのマルチキャストエントリを作成する。

	MAC アドレス	ポート ID
①	01-00-5e-01-01-01	p1

項番②のフレームは、IGMP join（グループへの参加）メッセージである。送信元はPC3であり、そのMACアドレスがPC3MACである。L2SWの受信ポートがp3である。

したがって、L2SW は、p3 の先に PC3 が存在し、マルチキャストグループへの参加を通知していることが分かる。この内容に基づき、次に示すとおり、当該グループのマルチキャストエントリを更新する。

②	MAC アドレス	ポート ID
	01-00-5e-01-01-01	p1, p3

項番③のフレームは、IGMP leave（グループからの離脱）メッセージである。送信元は PC1 であり、その MAC アドレスが PC1MAC である。L2SW の受信ポートが p1 である。

したがって、L2SW は、p1 の先に PC1 が存在し、マルチキャストグループからの離脱を通知していることが分かる。p1 の先には、PC1 以外に IGMP join メッセージを過去に送った PC は存在していない。したがって、もはや、p1 自体にマルチキャストフレームを転送しないことが分かる。

この内容に基づき、次に示すとおり、当該グループのマルチキャストエントリを更新する。

③	MAC アドレス	ポート ID
	01-00-5e-01-01-01	p3

よって、正解は解答例に示したとおりとなる。

## ■設問 5

設問 5 の解説に入る前に、VXLAN について解説する。

本文に詳しく説明されているので、適宜抜粋しながら解説していこう。

まず、〔基盤ネットワークの課題とその対応〕の第 1～第 2 段落の中で、次のように記述されている。

基盤ネットワークでは、レイヤ 3 ネットワークによって物理サーバが属するサブネットを分けている。課題は、このような構成で VM が他の物理サーバに移動した後も、移動後の VM との通信を可能にしたいというものである。

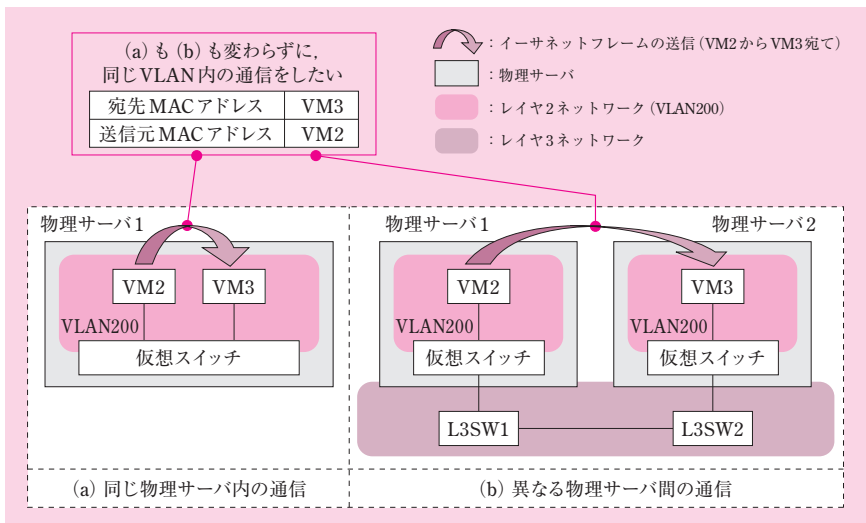
対応策として、J 君は、レイヤ 3 のネットワーク上にレイヤ 2 のネットワークを構成できる、オーバーレイネットワークが有効ではないかと考えた。VM で、マルチキャスト通信を利用してオーバーレイネットワークを実現する技術として、RFC7348 で提案された VXLAN（Virtual eXtensible Local Area Network）がある。VXLAN は、サーバ仮想化機構に実装されているので導入しやすい。

基盤ネットワークとは、Y社のIaaS基盤のネットワークを指す（序文の第2段落）。  
ここで言われている課題は、次のとおりである。

異なるサブネットに設置された2台の物理サーバがあり、物理サーバに仮想サーバ（以下、VMと称する）が2台稼働している。このとき、この2台のVMの通信が1台の物理サーバ上で稼働していようと、異なる物理サーバ上でそれぞれ稼働していようと、変わらずに通信することを可能にしたい、というものである。

この点について、具体例を使って解説する。

次のようなネットワークでVM間が通信するとしよう。ちなみに、このネットワークは、本文の図7の構成を念頭に置いて作成したものだ。



図：VM間の通信

この図には二つのネットワークが描かれている。左側の図 (a) は、物理サーバ1の上で、2台のVMが稼働している様子を示している。それぞれをVM2、VM3と呼ぶことにする。右側の図 (b) は、(a)の状態からVM3が物理サーバ2に移動した図である。その結果、物理サーバ1の上でVM2が、物理サーバ2の上でVM3が稼働している。

解決すべき課題をこの図に適用すると、次のように言える。

「図 (a) の方で、VM2 から VM3 宛てにイーサネットフレームを送信している。これと何ら変わりなく、図 (b) の方でも、VM2 から VM3 宛てにイーサネットフレームを送信することを可能にしたい」と。

ここではユニキャストフレームの送信を例に挙げたが、ARP 要求に代表されるブ



ロードキャストフレームの送信も同様である。要するに、VM2には、VM3が移動したことを全く意識させないようにするわけだ。これをどのように実現するかが課題となっている。

この解決策として、VXLANが使用される。

VXLANは、オーバーレイネットワークを実現する技術である。これを用いると、レイヤ3のIPネットワーク上に、レイヤ2のイーサネットを構成することができる。VXLANは、イーサネットフレームをIPパケットにカプセル化することで、これを実現している。

VXLANを用いたカプセル化について、〔VXLANの導入検討〕の第1～第3段落の中で、次のように記述されている。

VXLANは、カプセル化によってオーバーレイネットワークを実現する技術である。VXLANのフレーム構成を図6に示す。

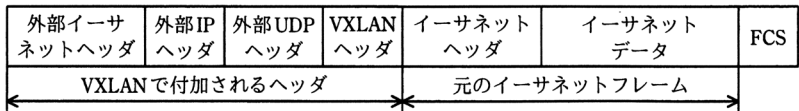


図6 VXLANのフレーム構成

VXLANでは、図6に示した4種類のヘッダを付加して元のイーサネットフレームをカプセル化し、IPネットワーク上で転送する。VXLANヘッダには、VXLANネットワーク識別子である24ビットのVNI (VXLAN Network Identifier) があり、VNIごとにVXLANセグメントが構成される。VXLANセグメントによって通信路が論理的に分離されるので、(き) VXLANを導入すれば、VLAN数の制限を緩和できる。

VXLANは、トンネルの終端ポイントであるVTEP (VXLAN Tunnel End Point) で元のイーサネットフレームにカプセル化を実施又は解除して、VTEP間でトンネルを構成する。レイヤ3のネットワーク上に構成されるオーバーレイネットワークでは、UDPを使ったマルチキャスト通信に対する応答によって通信先のVTEPが特定され、VM間でのデータリンク層の通信を可能にする。VNIはVMのMACアドレスとひも付けされ、同じ値のVNIのVXLANセグメントに属するVM同士は、VMが同一サブネットの他の物理サーバや、異なるサブネットの物理サーバに移動しても、移動前と同じ通信手順でVM間の通信を継続できる。VTEPは、サーバ仮想化機構の仮想スイッチやVXLANゲートウェイに実装されている。

VXLAN でカプセル化するときのフォーマットは図 6 に示されている。

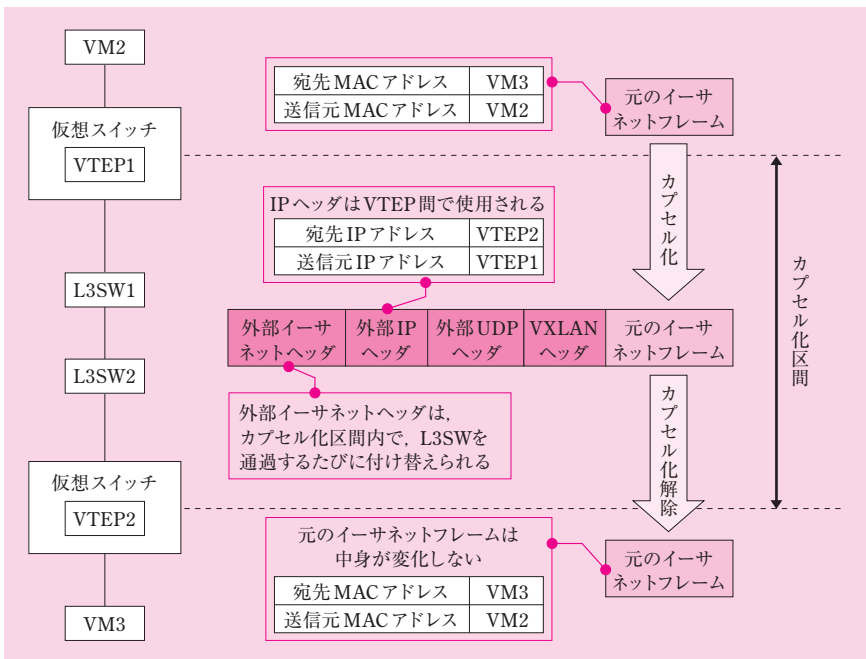
このカプセル化を行っているのが VTEP と呼ばれる機器である。この点について、「VXLAN は、トンネルの終端ポイントである VTEP（VXLAN Tunnel End Point）で元のイーサネットフレームにカプセル化を実施又は解除して、VTEP 間でトンネルを構成する」と記述されている。

カプセル化は、イーサネットフレームが送信元側の VTEP を通過するときに行われる。カプセル化の解除は、カプセル化された IP パケットが宛先側の VTEP を通過するときに行われる。

ここまでの内容を、図 7 のネットワークにある VM2、VM3（移動後）に適用してみよう。

VTEP は、物理サーバの仮想スイッチに実装されており、物理サーバ 1 の方を VTEP1、物理サーバ 2 の方を VTEP2 とする。

物理サーバ 1 上の VM2 から物理サーバ 2 の VM3 宛てにイーサネットフレームを送信する様子を次の図に示す。



図：VM2 から VM3 宛てに送信されるフレーム

- [ i ] VM2 は、VM3 宛てにイーサネットフレームを送信する。
  - [ ii ] 仮想スイッチは、これを受信する。ここで、VM3 が VTEP の先にあることを学習済みであるとする（本文の図8の ARP 要求／ARP 応答のやり取りを通じて、アドレス学習が済んでいるとしよう）。仮想スイッチは、VTEP1 にイーサネットフレームを転送する。
  - [ iii ] VTEP1 は、これを受信する。
  - [ iv ] VTEP1 は、イーサネットフレームのカプセル化を行い、VTEP2 宛てに IP パケットを転送する(\*)。
  - [ v ] VTEP2 は、この IP パケットを受信する。VM3 が物理サーバ2に存在することを認めると、カプセル化を解除して、VM3 宛てにイーサネットフレームを転送する。
- (\*) 元のイーサネットフレームがユニキャストのとき、これをカプセル化する IP パケットもユニキャストになる。この点は設問5 (4) で取り上げられている。

この [v] の説明で、「VM3 宛てにイーサネットフレームを転送する」と述べた。図7を見ると、物理サーバ2の仮想スイッチには、複数のネットワークが接続されている。VTEP2 は、どのようにして、VM3 が所属する VLAN の側に、イーサネットフレームを転送しているのだろうか。

この鍵を握るのが、VNI である。この点について、第3段落の中で、「VNI は VM の MAC アドレスとひも付けされ、同じ値の VNI の VXLAN セグメントに属する VM 同士は、VM が同一サブネットの他の物理サーバや、異なるサブネットの物理サーバに移動しても、移動前と同じ通信手順で VM 間の通信を継続できる」とある。つまり、カプセル化を解除する際に VNI を調べ、この値に基づき、仮想スイッチの中で VNI に対応するサブネットを選択しているわけだ。

ここまでで、VXLAN 技術の全体像は理解できた。小問で出題されている技術的な内容は、その中で適宜取り上げることにする。それでは、いよいよ小問の解説に移ろう。

## (1)

## 解答例

2<sup>24</sup>のVXLANセグメントが構成できるから (22字)

又は

膨大な数の論理セグメントが構成できるから (20字)

問題文は、「本文中の下線（き）について、VLAN 数の制限が緩和される理由を……述べよ」と記述されている。

下線（き）を含む文章は、〔VXLAN の導入検討〕の第2段落の中にある。そこには、「VXLAN ヘッダには、VXLAN ネットワーク識別子である 24 ビットの VNI (VXLAN Network Identifier) があり、VNI ごとに VXLAN セグメントが構成される。VXLAN セグメントによって通信路が論理的に分離されるので、（き）VXLAN を導入すれば、VLAN 数の制限を緩和できる」と記述されている。

「VLAN 数の制限」とあるが、これは、本事例において、オーバーレイネットワーク導入検討のきっかけとなった、ある懸案事項が関係している。この点について、〔基盤ネットワークの課題とその対応〕の第1段落の中で、「基盤ネットワークでは、通信路を顧客ごとに論理的に分離するために、顧客が利用する仮想サーバ（以下、VM という）に VLAN を設定している。IEEE802.1Q で規定された VLAN 数の制限は、4,094 である。各顧客に異なる VLAN ID を割り当てるので、顧客の増加に伴って VLAN 数が不足する可能性があった」と記述されている。

従来は、通信路を顧客ごとに論理的に分離するために VLAN を設定していた。VLAN 数の制限は 4,094 であり、VLAN 数の不足が懸念されていた。言うなれば、論理セグメントの枯渇が問題視されていたわけだ。

一方、VXLAN は 24 ビット（1,600 万以上）の VNI をもつ。通信路を顧客ごとに論理的に分離するために VXLAN を設定することで、膨大な論理セグメントを構成でき、枯渇問題を解消できる。

よって、正解は、「2<sup>24</sup>の VXLAN セグメントが構成できるから」「膨大な数の論理セグメントが構成できるから」などとなる。

## (2)

## 解答例

理由：宛先となるVMの存在場所が不明だから（18字）

宛先 IP アドレス：224.1.1.2

送信元 IP アドレス：10.0.0.254

本問は、二つのことを問うている。

一つ目は、「図8中の(ii)におけるVXLANの通信は、マルチキャストで行われる。ユニキャストで行われない理由を……述べよ」と記述されている。

二つ目は、「(ii)のVLANフレームの宛先IPアドレスと送信元IPアドレスをそれぞれ答えよ」と記述されている。

それでは以下、順番に解説しよう。

### ●(ii)におけるVXLANの通信がユニキャストで行われない理由

図8は、「VXLANの導入検討」の第5段落の下にある。これは、VM2とVM3間の通信手順を示したものである。およその流れは次のとおりである。

(i)～(iv)	VM2からARP要求フレームを送信
(v)～(viii)	VM3からVM2へARP応答フレームを送信
(ix)	VM2からVM3へイーサネットフレームを送信

(ii)の手順は、ARP要求フレームの送信手順の中にある。具体的な内容は「ARP要求を受信したVTEP1は、図6のカプセル化を行い、VXLANフレームを送信する」である。

それゆえ、本問は、「ARP要求をカプセル化したVXLANフレームがユニキャストで行われない理由」を問うていることが分かる。

まず、問題文にある「VXLANフレーム」について触れておこう。これは、設問5の冒頭で解説した、イーサネットフレームをカプセル化したIPパケットのことだと考えてよい。厳密に言うと、VXLANフレームは、このIPパケットに外部イーサネットヘッダを付与したものを指している。とはいえ、外部イーサネットヘッダは、VTEPを両端とするカプセル化区間において、L3SWを超えるたびに付け替えられる存在に過ぎない。一方、IPパケットの方は、VTEP間のカプセル化区間において変化せず、本問

を解く上で本質的なものである。実際、二つ目に問われているのは IP アドレスの方である。

事実、本問を次のように読み替えても、その解答は変わらないのである。「ARP 要求をカプセル化した IP パケットがユニキャストで行われない理由を……述べよ」。なぜなら、IP パケットの宛先がユニキャストであればイーサネットフレーム（VXLAN フレーム）もそうなるし、IP パケットの宛先がユニキャストでなければイーサネットフレームもそうならないからだ。

そこで、一つ目の解を導くに当たり、二つ目の解のことも見据えて、初めから IP パケットに着目することにしよう。

さて、ここで問われている ARP 要求は、ブロードキャストで送信される。その目的は、アドレス解決の目標となる端末（ARP 要求の目標プロトコルアドレスを IP アドレスにもつ端末）がサブネットのどこに存在しようとも、当該端末に ARP 要求を到達させるためである。ブロードキャストで送信された ARP 要求をスイッチが受信したとき、（受信ポートを除く）全てのポートにフラッドイングするので、サブネットのどこに存在しようとも、当該端末に ARP 要求が必ず届くわけだ。

図 8 の（ii）について言えば、アドレス解決の目標となる端末は、VM3 である。

VM3 は、異なるサブネットの物理サーバに移動している可能性がある。事実、図 7 では物理サーバ 2 に移動している。したがって、ARP 要求をカプセル化した VTEP1 は、自分以外の他の VTEP に ARP 要求を届ける必要がある。

VTEP は、物理サーバの仮想スイッチに実装されている。基盤ネットワーク内には複数台の物理サーバが存在している可能性があり、VTEP も然りである。つまり、基盤ネットワークのどの VTEP の先に VM3 が存在しているか、特定できない状況に置かれている。

したがって、ARP 要求をカプセル化した IP パケットの宛先を、ユニキャストアドレスにすることができない。

よって、一つ目に問われた「ユニキャストで行われない理由」は、「宛先となる VM の存在場所が不明だから」となる。

### ● VXLAN フレームの宛先／送信元 IP アドレス

先ほど、「ARP 要求をカプセル化した VTEP1 は、自分以外の他の VTEP に ARP 要求を届ける必要がある」と解説した。

「他の VTEP」と言ったが、基盤ネットワーク内に設置された、ありとあらゆる VTEP に届ける必要はない。IaaS の利用顧客は多数いるため、基盤ネットワークには何台もの物理サーバが収容されている。つまり、多くの VTEP が共存している。VM2 と VM3

の所属する論理セグメントを配下にもつ VTEP は、その一部に過ぎない。

設問5の冒頭で解説したとおり、VMの論理セグメントはVNIで識別されている。それでは、VNIとVTEPはどのように対応付けられているのだろうか。それが分かれば、同じ論理セグメントを収容したVTEPを見つけ出し、そのVTEPを宛先とするパケットを転送できる。

VNIとVTEPの対応付けについて、図7の注記3には、「224.1.1.1～224.1.1.4は、VMが所属するマルチキャストグループを示し、VNIごとにマルチキャストグループを割り当てる」とある。つまり、同じ論理セグメントに存在するVM同士は、自分と同じマルチキャストグループにも所属している。それゆえ、この記述から、VNIとマルチキャストIPアドレスが対応付けられていることが分かる。

したがって、VTEPは、ARP要求を受信したら、次の手順に従ってIPパケットにカプセル化する。

- [ i ] ARP 要求の送信元 MAC アドレスを調べる。つまり、送信元 VM を調べる。
- [ ii ] VM の MAC アドレスと VNI が対応付けられているので、送信元 MAC アドレスの値に基づき、VM が存在する論理セグメントの VNI を調べる。
- [ iii ] VNI とマルチキャストグループが対応付けられているので、VNI の値に基づき、マルチキャストグループのアドレスを調べる。
- [ iv ] そのマルチキャスト IP アドレスを宛先とする IP パケットに、ARP フレームをカプセル化する。

図7を見ると、VM2、VM3が所属する論理セグメントのVNIの値が「5002」であり、そのVNIに対応付けられたマルチキャストグループが「224.1.1.2」であることが分かる。

したがって、ARP要求をカプセル化したIPパケットの、宛先となるマルチキャストIPアドレスは、「224.1.1.2」となる。

当該IPパケットの送信元は、ARP要求を送信したVM2が存在するVTEPである。したがって、そのIPアドレスである、「10.0.0.254」となる。

よって、正解は解答例に示したとおりとなる。

## (3)

## 解答例

マ	ル	チ	キ	ャ	ス	ト	グ	ル	ー	プ	2	2	4	.	1	.	1	.	2	の	I	G	M	P
	j	o	i	n	メ	ッ	セ	ー	ジ	を	,	L	3	S	W	2	に	送	信	す	る	。		

(48字)

問題文は、「図8中の(iii)で送信されるマルチキャストパケットがVTEP2に届くのは、VM3が移動してきたことをVTEP2が知ったとき、VTEP2によって行われる通信の結果である。その通信について、宛先と送信されるパケットの内容を……述べよ」と記述されている。

(iii)の手順は、ARP要求フレームの送信手順の中にある。具体的な内容は「VTEP1が送信したフレームは、L3SWで経路制御され、VTEP2に届く」である。

「VTEP1が送信したフレーム」とは、(ii)の手順で送信したVXLANフレームのことだ。設問5(2)で解説したとおり、このフレームが運ぶIPパケットは、宛先IPアドレスが「224.1.1.2」のマルチキャストパケットである。

問題文を整理すると、次のようになる。まず、「VM3が移動してきたことをVTEP2が知ったとき、VTEP2によって行われる通信」という準備がある。その準備の結果、「図8中の(iii)で送信されるマルチキャストパケットがVTEP2に届く」ことが達成される。

本問が問うているのは、(iii)のマルチキャスト通信に先立って実施された、準備の方だ。解答する内容は、準備としてVTEP2が行った通信の宛先とその内容である。

ここで、マルチキャスト通信について、設問4の冒頭で解説した内容を振り返ってみよう。

送信元ノードから配信先ノードにマルチキャスト通信が行われるためには、送信元から配信先に至る経路情報が生成されていなければならない。つまり、経路情報の生成は、マルチキャスト通信の準備に当たる。

経路情報の生成は、配信先ノードがマルチキャストグループに参加する旨の通知をきっかけに、下流ルータから上流ルータに向かう情報伝達を通じて、行われている。最終的に、送信元をルートとし、配信先をリーフとするツリー構造をもつ経路情報が出来上がる。

したがって、(iii)のマルチキャスト通信に先立って実施された、「VM3が移動してきたことをVTEP2が知ったとき、VTEP2によって行われる通信」という準備は、「経路情報の生成」という準備の一部であると推論できる。



VTEP2は、(iii)のマルチキャスト通信の配信先ノードである。したがって、「VTEP2によって行われる通信」とは、経路情報生成の最初に行われる、配信先ノードがマルチキャストグループに参加する旨の通知であることが分かる。すなわち、それは、IGMP join メッセージである。

この点は、VTEP2によって行われる通信が、「VM3が移動してきたことをVTEP2が知ったとき」に行われることから、裏付けられる。VTEP2に接続しているVNI5002には、VM3しか記されていない。VM3が移動する前、VTEP2のVNI5002は空だったことが分かる。VTEP2は、自分のVNI5002にVM3が新規に登場したのをきっかけに、マルチキャストグループ224.1.1.2の配信先ノードとなる必要が生じたと判断した。それゆえ、当該グループへの参加を通知したのである。

以上をまとめると、準備としてVTEP2が行った通信の内容は、「IGMP join メッセージ」である。なお、解答に際しては、できるだけ具体的に記した方がよい。本文から読み取れる情報を当てはめると、通信の内容は、「マルチキャストグループ224.1.1.2のIGMP join メッセージ」となる。

それでは、宛先はどうだろうか。[マルチキャスト通信の調査]の第6段落は、「PCが、あるマルチキャストグループに参加するときは、IGMP join メッセージによって、所属するサブネットのルータに対し、参加するマルチキャストグループを知らせる」と記述されている。したがって、宛先は、VTEP2が接続しているルータに当たる、「L3SW2」となる。

よって、正解は、「マルチキャストグループ224.1.1.2のIGMP join メッセージを、L3SW2に送信する」となる。

### ●参考：IGMP join メッセージの宛先

先ほど解説したとおり、本文は、IGMP join メッセージの宛先を、「所属するサブネットのルータ」と説明している。当然、これを読んだ受験者は、「IGMP join メッセージの宛先IPアドレスは、所属するサブネットのルータだ」と判断するはずだ。

実際、本問の解答例も、宛先は「L3SW2」（つまりルータ）になっているので、出題者としても受験者がこのように判断することを期待していたはずだ。

しかし、正確に言うと、IGMP join メッセージの宛先は、「ルータ」のIPアドレスではない。実は、「参加するマルチキャストグループ」、すなわち、マルチキャストIPアドレスなのだ。

参考までに、本文の図5中にある表を見ていただきたい。①、②のフレームはIGMP join メッセージであるが、その宛先IPアドレスは「224.1.1.1」となっている。

とはいえ、IGMP join メッセージを受け取るべき存在は、基本的に言って、ルータ

である。経路情報生成が下流から上流に向かう情報伝達を通じて成し遂げられていることを考えれば、そのように言ってよい。だから、第6段落にある IGMP join メッセージの説明を見て、不適切であるとは著者は思わない。試験問題文中の説明として、受験者に概要をつかんでもらうために書いた内容としては、このくらいの掘り下げで十分であろう。

ただ、著者が気になることは、IGMP join メッセージの宛先 IP アドレスに関する仕様が熟知した受験者（あるいは、図5中の表を解析し得た受験者）が、本問を解くときに「宛先」をどのように解釈したかということだ。

おそらく、技術的に正確な「224.1.1.2」を宛先とする答案であっても、つまり、「L3SW2」を宛先とはしない答案であっても、正解として扱われたことだろう。試験センターの公表した内容は、あくまで「解答例」に過ぎないのだから。

#### (4)

##### 解答例

問題： 

不	要	な	マ	ル	チ	キ	ャ	ス	ト	パ	ケ	ツ	ト	が	ネ	ツ	ト	ワ	ー	ク	内	に	転	送
さ	れ	る	の	で	,	L	3	S	W	や	ネ	ツ	ト	ワ	ー	ク	の	負	荷	が	高	ま	る	。

(50字)

宛先 IP アドレス：10.0.0.254

送信元 IP アドレス：10.10.0.254

本問は、二つのことを問うている。

一つ目は、「図8中の(vi)における VXLAN の通信は、ユニキャストで行われる。仮に、VTEP 間の通信が全てマルチキャストで行われる場合を想定したとき、物理サーバ、VM 及び L3SW の数が多いネットワークの場合に顕在化する問題について……述べよ」と記述されている。

二つ目は、「(vi) の VXLAN フレームの宛先 IP アドレスと送信元 IP アドレスをそれぞれ答えよ」と記述されている。

それでは以下、順番に解説しよう。

#### ●顕在化する問題

問題文に「図8中の(vi)における VXLAN の通信は、ユニキャストで行われる」とある。設問5(2)、(3)では VXLAN の通信はマルチキャストで行われている。それゆ

え、VTEP 間の通信は、ユニキャスト通信とマルチキャスト通信の2種類があることが分かる。

ここで問われているのは、ユニキャスト通信が全てマルチキャスト通信に置き換わった場合、「物理サーバ、VM 及び L3SW の数が多いネットワークで顕在化する問題」ということである。つまり、ユニキャストであれば転送する必要がない通信であるのに、マルチキャストであるがゆえに余計に転送することによって、顕在化する問題である。

マルチキャストグループに参加している VM が多くなると、それらが多くの物理サーバに散在する可能性が高まり、物理サーバをまたぐ VTEP 間の通信の頻度が高まるだろう。更に、VM を抱える物理サーバの数が多くなると、VTEP 間の通信の経路上に位置する L3SW の数も多くなるだろう。

この状況において、VTEP 間の通信が全てマルチキャストになるならば、不要なマルチキャストパケットの転送によりトラフィック量が増加する。L3SW の負荷（不要な転送）、ネットワークの負荷（物理サーバの NIC の不要な受信、等）が高まると推察できる。

それでは、仮想スイッチの先にある論理セグメント（VM がいるネットワーク）はどうだろうか。図8の手順を見ると、VTEP は、VM が物理サーバに存在することを認めたときに、これを転送する。つまり、論理セグメントの側に転送するか否かを判断している。それゆえ、不要なマルチキャストパケットの流入はここで抑えられる。仮想スイッチの先にある論理セグメントは、VTEP 間の通信が全てマルチキャストになったとしても、トラフィック量が変わらない。したがって、こちらは解答から除外する。

よって、正解は、「不要なマルチキャストパケットがネットワーク内に転送されるので、L3SW やネットワークの負荷が高まる」となる。

#### ● (vi) の宛先 IP アドレスと送信元 IP アドレス

(vi) の手順は、ARP 応答フレームの送信手順の中にある。具体的な内容は「ARP 応答を受信した VTEP2 は、図6のカプセル化を行い、VXLAN フレームを送信する」である。

ここに「ARP 応答」と記述されている。これは、(v) の手順で VM3 が送信した ARP 応答であり、(i) の手順で VM2 が送信した ARP 要求に対するものである。その宛先は VM2 であり、ARP 応答はユニキャストフレームだ。

カプセル化した後の通信について、問題文に「図8中の (vi) における VXLAN の通信は、ユニキャストで行われる」とある。したがって、VXLAN は、「ユニキャスト

のイーサネットフレームを、ユニキャストの IP パケットでカプセル化する」という仕様になっていることが分かる。

本問が問うているのは、このユニキャスト通信の、宛先 IP アドレスと送信元 IP アドレスである。

それを解くには、この ARP 応答フレームの転送経路が分かればよい。これは VM3 から VM2 に宛てたものなので、次のようになる。

**VM3 → VTEP2 → VTEP1 → VM2**

カプセル化される区間、すなわち、VXLAN フレームが流れる区間は、「VTEP2 → VTEP1」である。したがって、この VXLAN フレーム中の IP パケットは、宛先 IP アドレスが VTEP1、送信元 IP アドレスが VTEP2 である。

図7を見ると、VTEP1 の IP アドレスは「10.0.0.254」であり、VTEP2 の IP アドレスは「10.10.0.254」である。

よって、正解は解答例に示したとおりとなる。

## Column



## 試験本番で役立つ心構え

本書の締めくくりとして、試験本番で役立つ心構えを挙げておきます。

- 合格点をねらおう

本試験の合格ラインは、100点満点中、60点です。

ここは試験と割り切り、完全主義を捨てましょう。「6割取れば合格」という心構えでよいのです。そう思うと、大分気持ちが楽になります。

- 分からない問題でも、あきらめずに部分点をねらおう

完全主義を捨てますが、必死になって合格圏内に食い込むように努力しましょう。よく分からない小問の一つ、二つは早々と切り上げ、「部分点ねらいでいく」と割り切るくらいの大胆さが必要です。そういう問題に出くわしたならば、せめてキーワードの一つだけでも書いて、「一矢報いる」くらいの気構えで臨みましょう。

- 手強そうな問題でも、「特殊な知識は問われないはずだ」と信じよう

あまり馴染みのない新技術が登場して、何やら手強そうに思えても、焦りは禁物です。一呼吸おいて、次のように自分に言い聞かせましょう。

「新技術そのものに関する前提知識は極力必要がないように配慮されているはずだ（平成25年度午後Ⅱ採点講評）。出題に値するテーマを選んでいるはずなので、その題材としてこの新技術が登場しているだけに過ぎない。素直に考えれば、きっと出題の意図が分かるはずだ。解法の糸口が見つかるはずだ」

おそらく、焦りを覚えた受験者は自分だけではないはずです。あなたはいち早く落ち着きを取り戻して、問題に取り掛かりましょう。

- 最後の1分1秒まであきらめない！

必死になって解いているうちに、答えがひらめくことがあります。最後の1分1秒まで、答案に向って部分点を積み上げましょう。決してあきらめないことが、何より大切です。