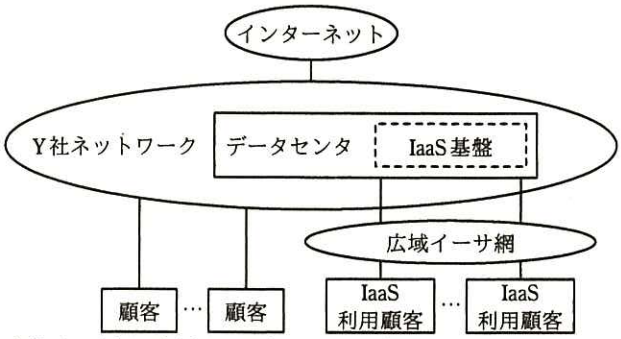
問２　サービス基盤の改善に関する次の記述を読んで，設問１～５に答えよ。

中規模の ISP である Y 社は，IPv4 アドレス（以下，IP アドレスという）を使用した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。現在の Y 社のネットワーク構成を図１に示す。



広域イーサ網：広域イーサネットサービス網

図１　現在の Y 社のネットワーク構成

Y 社では，顧客の増加に伴い，二つの課題への対応が急務になっている。一つは，保有するグローバル IP アドレスが不足する事態が近づいていることから，対応策を確立することである。もう一つは，IaaS 基盤のネットワーク（以下，基盤ネットワークという）を，顧客の増加に柔軟に対応できる構成に変更することである。

二つの課題への対応策は，ネットワーク技術部で立案することになり，ネットワーク技術部の T 部長は，基盤構築グループの I 主任と J 君に対応策の検討を指示した。そこで，I 主任と J 君は，まず，グローバル IP アドレス不足への対応策を検討し，その後に，基盤ネットワークの改善策を検討することにした。検討作業は J 君が行い，検討結果を I 主任が評価することにした。

〔グローバル IP アドレス不足への対応策の検討〕

グローバル IP アドレスの枯渇対策の中に，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，顧客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。そこで，J 君は NAT444 について調査した。

〔NAT444 の調査〕

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。

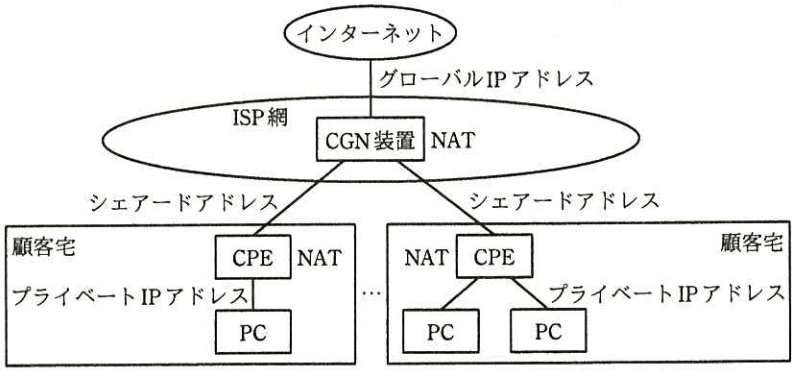


図 2　NAT444 の構成

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。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。

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

(1) は，一つのグローバル IP アドレスを複数の顧客で共用することによって発生する。CGN では，[b] 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。

(2) は，NAT444 を導入することで発生する。NAT が介在すると，例えば，次のようなアプリケーションで不具合が発生する。

・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アプリケーション

・SIP のように，送信先となる機器の IP アドレスをパケットのデータ部に埋め込んで指定するアプリケーション

ただし，NAT が介在しても，CGN 装置，利用するアプリケーションの実装などで，不具合は回避できる可能性がある。今後，その可能性について，より詳細な調査を行うとともに，評価試験も併せて行うことにする。

その他にも，NAT が介在すると，顧客が IPsec を利用している場合に問題が発生する危険性がある。J 君は，IPsec を利用する顧客への対応策について検討した。

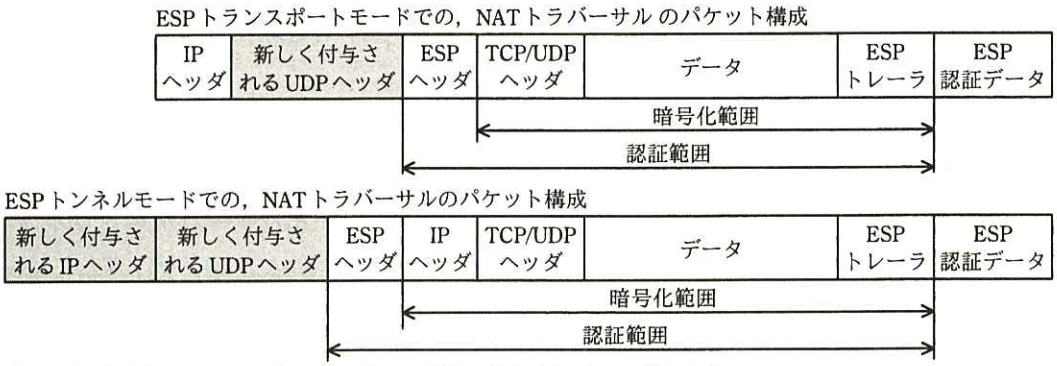
〔IPsec を利用する顧客への対応策〕

NAT 機器を経由した通常の 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 機器を経由した 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，（い）IP アドレス変換が行われると認証エラーが発生する。
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，（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。
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 機器による 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

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 メッセージを送受信する際に，経路上に NAT 機器が存在するかどうか検査する。

・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。

J 君は，これまでの調査で，CGN の導入には今後解決すべき問題が残されているが，CGN の導入によって，グローバル IP アドレスを節約できることが分かったので，調査結果を I 主任に説明した。I 主任は，J 君の考えが適切であると判断し，調査結果を基に CGN の導入案をまとめて，T 部長に報告することを提案した。

次に，J 君は，基盤ネットワークの改善策の検討に取り掛かった。

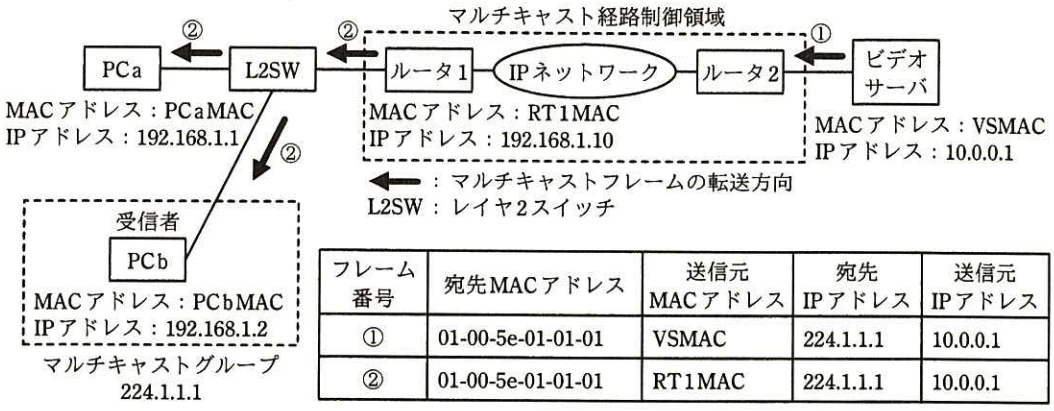
〔基盤ネットワークの課題とその対応〕

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。IEEE 802.1Q で規定された VLAN 数の制限は，4,094 である。各顧客に異なる複数の 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。そこで，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レイネットワークを実現する技術として，RFC 7348 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。そこで，J 君はまず，マルチキャスト通信について調査した。

〔マルチキャスト通信の調査〕

マルチキャスト通信は，特定の複数ノードに対して，一つのデータを同時に送信する通信方式である。マルチキャスト通信例を図 4 に示す。



フレーム番号	宛先MACアドレス	送信元MACアドレス	宛先IPアドレス	送信元IPアドレス
①	01-00-5e-01-01-01	VSMAC	224.1.1.1	10.0.0.1
②	01-00-5e-01-01-01	RT1MAC	224.1.1.1	10.0.0.1

図 4　マルチキャスト通信例

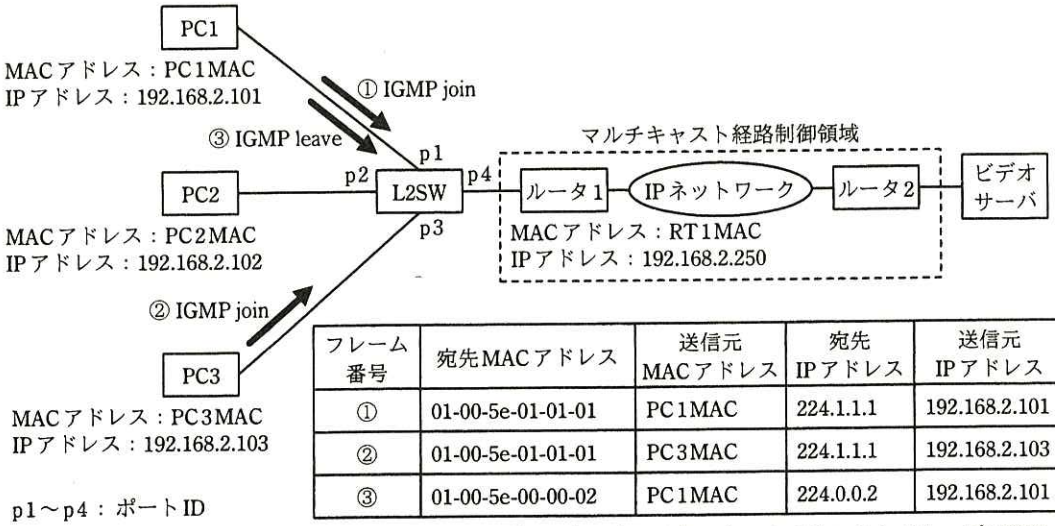
図 4 の例では，PCb をビデオサーバから送信される画像データの受信者とする。

マルチキャスト通信では，データを受け取りたい PC を，マルチキャスト IP アドレスでグループ化する。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。（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ので，PC a と PC b にマルチキャストフレームが届く。ただし，PC a は，当該マルチキャストグループに参加していないので，受信しない。

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] 宛てのフレームを受信するように，NIC（Network Interface Card）が動作する。

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。



フレーム番号	宛先MACアドレス	送信元MACアドレス	宛先IPアドレス	送信元IPアドレス
①	01-00-5e-01-01-01	PC1MAC	224.1.1.1	192.168.2.101
②	01-00-5e-01-01-01	PC3MAC	224.1.1.1	192.168.2.103
③	01-00-5e-00-00-02	PC1MAC	224.0.0.2	192.168.2.101

注記 1　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。

注記 2　マルチキャストグループは，224.1.1.1 である。

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。

ルータ 1 は，IGMP join メッセージを受信することによって，配下のサブネットにマルチキャストグループ 224.1.1.1 が存在するのを知り，ビデオサーバから受信した 224.1.1.1 宛てのパケットを L2SW に送信する。L2SW は，図 4 に示したように，受信したフレームを，受信ポート以外の全てのポートにフラッディングするので，どの PC にも 224.1.1.1 宛てのパケットが届く。しかし，L2SW が，図 5 中の ①と② のフレームを受信した段階では，PC2 は 224.1.1.1 に所属していないので，L2SW の p2 からのマルチキャストフレームの転送は不要である。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を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。

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。

表 2　L2SW に作成される MAC アドレステーブル

MAC アドレス	ポート ID
PC 1 MAC	p1
PC 3 MAC	p3
ア	イ

J 君は，マルチキャスト通信の調査を終え，次に VXLAN の導入について検討した。

〔VXLAN の導入検討〕

VXLAN は，カプセル化によってオーバ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。

J 君は，VXLAN を Y 社の基盤ネットワークに導入したときの動作について検討した。Y 社の基盤ネットワークへの VXLAN 導入構成案を，図 7 に示す。図 7 では，物理サーバ 1 に存在していた VM3 が，物理サーバ 2 に移動した状態を示している。

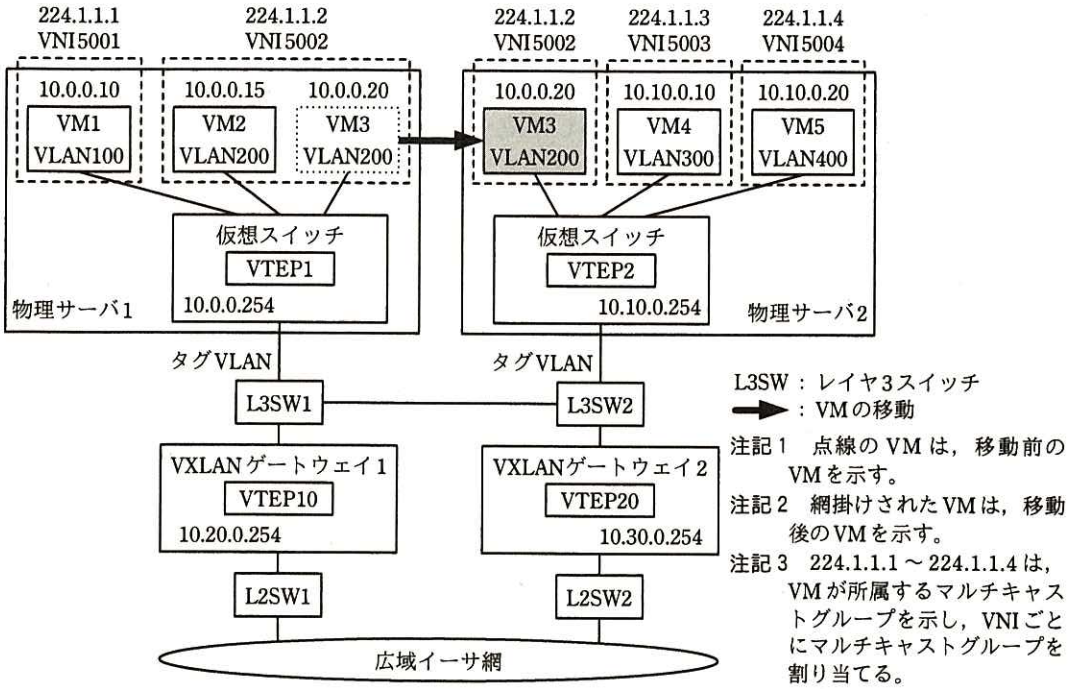


図7　基盤ネットワークへのVXLAN導入構成案（抜粋）

J君は，図7の構成でVXLANを導入したときのVM2とVM3間の通信方法について考え，VM3が物理サーバ2に移動したときの，VM2とVM3間の通信手順を，図8にまとめた。

（i）VM2は，VM3のMACアドレスを取得するために，ARP要求を送信する。
（ii）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。
（iii）VTEP1が送信したフレームは，L3SWで経路制御され，VTEP2に届く。
（iv）VTEP2は，VM3が物理サーバ2に移動してきていることを認めると，カプセル化を解除してARP要求をVM3宛てに転送する。
（v）VM3は，受信したARP要求に対して，ARP応答を送信する。
（vi）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。
（vii）VTEP2が送信したフレームは，L3SWで経路制御され，VTEP1に届く。
（viii）VTEP1は，VM2が物理サーバ1に存在することを認めると，カプセル化を解除してARP応答をVM2宛てに転送する。
（ix）VM2は，VM3のMACアドレスを取得したので，VM3宛ての通信を行う。
（以下，省略）

図8　VM2とVM3間の通信手順

J君は，広域イーサ網を介した顧客のPCとVM3間でも，移動後のVM3との通信は正常に行えることを確認した。基盤ネットワークにVXLANを導入することによって，顧客の増加に対応できる見通しが立ったので，検討結果をI主任に説明した。I主任は，VXLANの導入が効果的な改善策であると判断した。

I主任とJ君は検討結果を基に，グローバルIPアドレスの不足への対応策と基盤ネットワークの改善策及び今後の進め方をまとめ，T部長に報告した。

設問1　本文中の［ a ］～［ e ］に入れる適切な字句又は数値を答えよ。

設問2　〔NAT444の調査〕について，(1)，(2)に答えよ。

(1) 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，50字以内で述べよ。

(2) 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，それぞれ10字以内で答えよ。

設問3　〔IPsecを利用する顧客への対応策〕について，(1)～(3)に答えよ。

(1) 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，60字以内で述べよ。

(2) 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，50字以内で述べよ。

(3) 本文中の下線（え）で必要とする変更を，50字以内で具体的に述べよ。

設問4　〔マルチキャスト通信の調査〕について，(1)～(3)に答えよ。

(1) 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，40字以内で述べよ。

(2) 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，35字以内で述べよ。

(3) 表2中の［ ア ］に入れる適切なマルチキャストMACアドレスを答えよ。また，［ イ ］は，図5中の①～③のフレームを受信した順に遷移

する。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，それぞれ答えよ。ここで，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。

設問 5　〔VXLAN の導入検討〕について，(1) ～ (4) に答えよ。

(1) 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，25 字以内で述べよ。

(2) 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，20 字以内で述べよ。また，（ii）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。

(3) 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，60 字以内で述べよ。

(4) 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，60 字以内で述べよ。また，（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。