NW

平成27年度　秋期
ネットワークスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	問2 ○

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　ネットワーク基盤の拡張に関する次の記述を読んで，設問1～4に答えよ。

K社は，様々な用途の空調設備（以下，設備という）を製造し，保守サービスにも力を入れている。全国の保守センタに配備された保守員が，顧客のオフィスや工場などを訪問して，設備の点検や修理を行っている。今後は，リモート保守などの新サービスを提供する予定である。

〔現在の保守システム〕

現在の保守システムの構成を図1に示す。

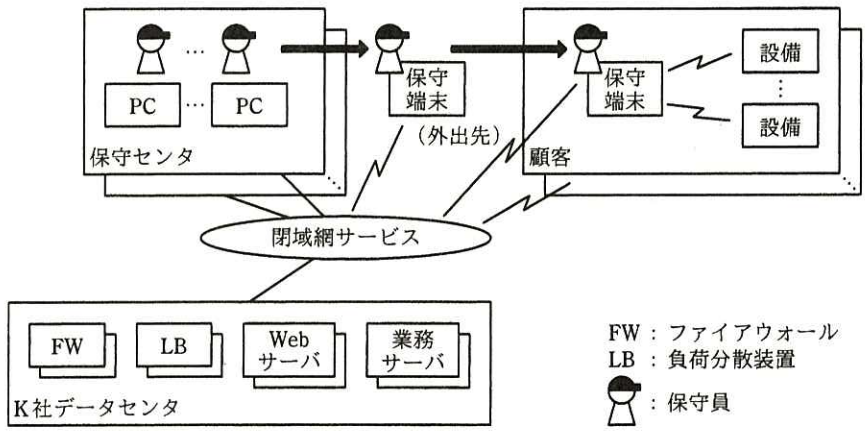


図1　現在の保守システムの構成

・保守員は，保守端末を携帯して顧客へ出向き，設備の点検，修理を行う。
・保守員は，無線LANを介して保守端末から設備に，HTTPを使ったアクセスを行うことができ，設備の稼働情報を参照したり，設備を操作したりする。
・K社データセンタには，2台のWebサーバと2台の業務サーバが設置され，両サーバによって保守情報が管理されている。
・必要に応じて，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。

K社データセンタ内のネットワーク構成を，図2に示す。

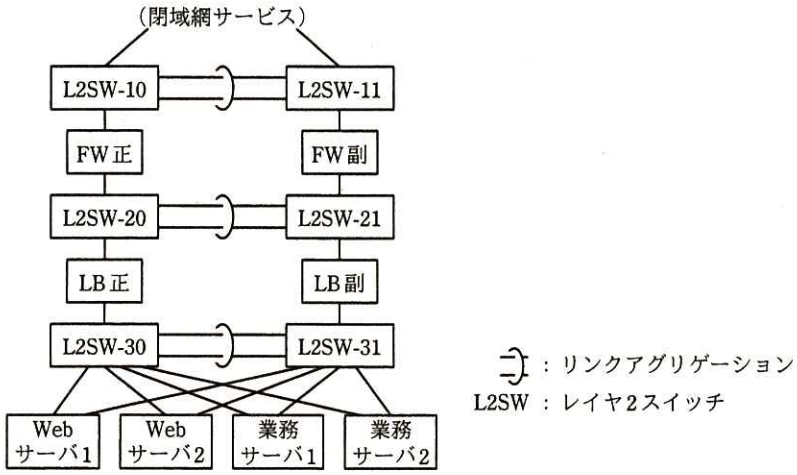


図2　K社データセンタ内のネットワーク構成（抜粋）

・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。

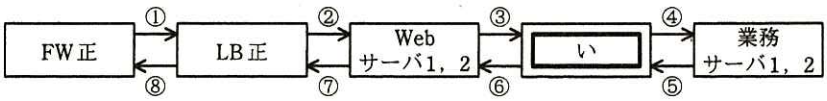
・L2SWとサーバの接続は，サーバのチーミング機能によって冗長化されている。

・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を，図3に示す。



注記　⟶はリクエストのデータの流れを，⟵はレスポンスのデータの流れを示す。

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

〔保守システムの機能強化〕

情報システム部では，新サービスの提供に当たり，保守システムの機能強化プロ

ジェクトを予定している。機能強化では，新業務サーバを K 社データセンタに設置して，全設備の稼働情報を継続的に収集し，それを保守員が参照する。また，保守センタから設備の操作（設定変更，ファームウェア更新）を行ったり，設備の稼働情報（運転実績，維持温度）を参照したりする。ところが，図 1 に示すように，現在の保守システムでは，ネットワークを介して設備へアクセスすることができない。そこで，情報システム部では，2 種類のネットワーク機器（通信アダプタと中継装置）を導入し，設備へのネットワークアクセスを実現しようとしている。

機能強化に伴う導入機器の設置場所を図 4 に，機能強化後の通信の概要を図 5 に，それぞれ示す。

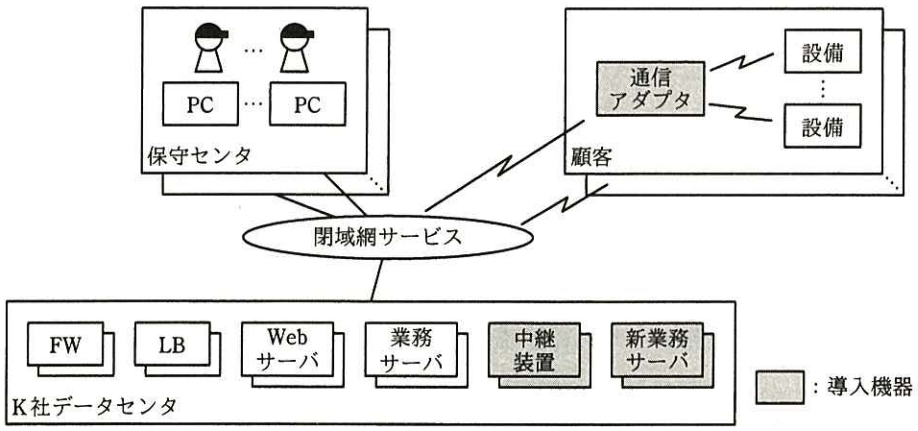
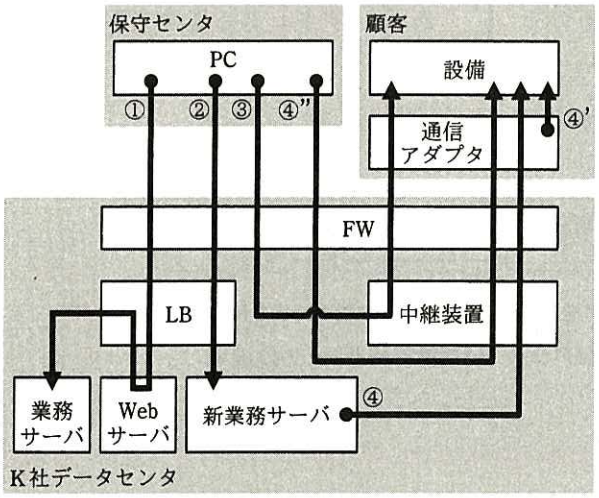


図 4　機能強化に伴う導入機器の設置場所



通信の説明

	用途	データ量／回	頻度
①	保守情報の参照	10^3～10^4 バイト	不定期
②	稼働情報の参照	10^3～10^4 バイト	不定期
③	設備の操作	数バイト～10^4バイト	不定期
④	稼働情報の取得	数バイト	定期（5分間隔～1時間間隔）
④’			定期（1分間隔）
④”			不定期

注記　●→ は，アクセスの方向を表す。

図 5　機能強化後の通信の概要

図5中の通信の概要は，次のとおりである。

・①は，現在の通信であり，通信プロトコルにはHTTPを用いている。同様に，新たに追加される②～④，④'，④"もHTTPを用いる。

・②は，保守員が新業務サーバにある，設備の稼働情報を参照するときの通信である。

・③は，保守員が設備を操作するときの通信である。その際，保守員は最新の稼働情報を参照するので，④"の通信も発生する。

・④は，新業務サーバが設備の稼働情報を自動的に取得するときの通信である。収集周期は，サービス開始時は1時間とし，段階的に5分間程度に短縮しサービス品質を向上させる。また，設備はいつも通電されているとは限らないので，それを考慮した仕組み（以下，稼働情報取得案という）を用意する。

・②の通信では，アクセスの際，新業務サーバ上の稼働情報を次の形式で指定する。

http://（新業務サーバのFQDN）/（稼働情報ファイル名）

・③，④，④'，④"の通信では，アクセスの際，設備の中の稼働情報又は操作対象の機能（以下，リソースという）を，次の形式で指定する。

http://（設備を指定するためのFQDN）/（リソース名）

情報システム部では，図5中の④，④'，④"の通信に関して，通信アダプタと中継装置のHTTPキャッシュ機能を使った次のような稼働情報取得案を構想している。

・中継装置と通信アダプタは，HTTPレスポンスに含まれる設備の稼働情報を，自装置にキャッシュする。

・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。

・④の通信では，2台の新業務サーバに実装されたHTTPクライアントが，定期的に配下の設備にGETリクエストをそれぞれ送信し，稼働情報を取得する。(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。各新業務サーバが取得した稼働情報は，データベースの機能を用いて新業務サーバ間で同期する。

・④' の通信では，通信アダプタは単独で，HTTP ヘッダ［If-Modified-Since : x］を付加した GET リクエストを設備へ 1 分間隔で送信し，取得した稼働情報を自装置にキャッシュする。

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。

稼働情報取得案の通信シーケンス例を，図 6 に示す。

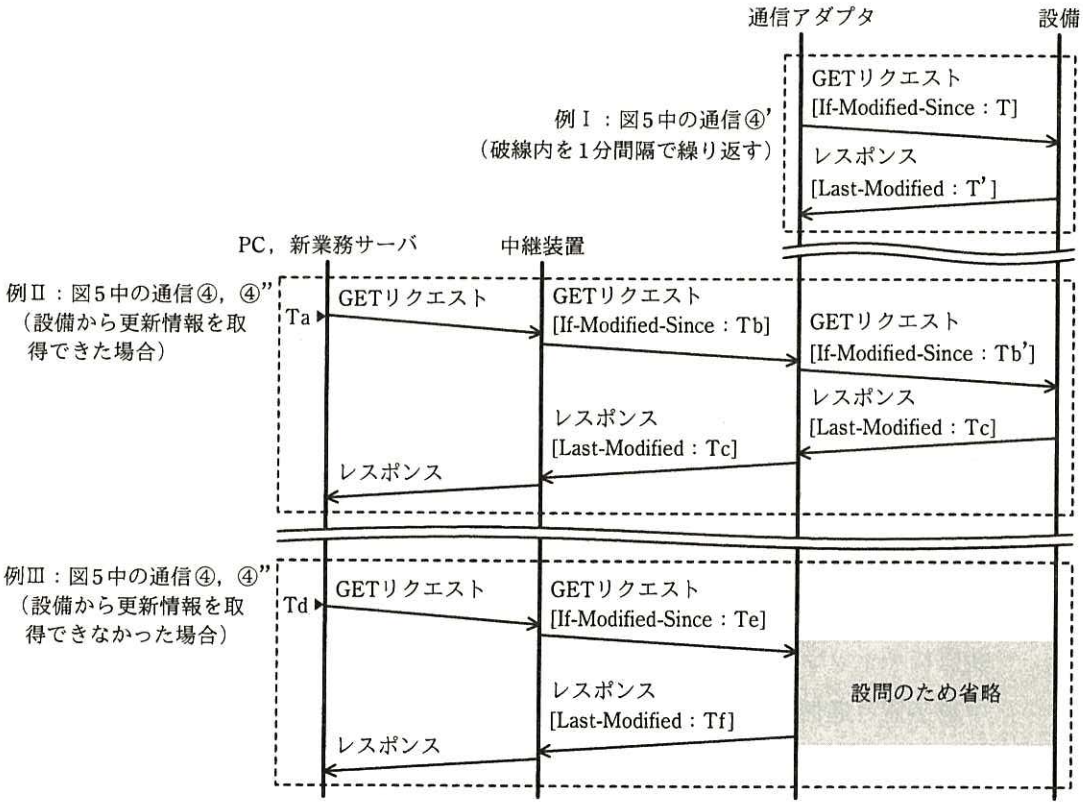


図 6　稼働情報取得案の通信シーケンス例

図 6 中の時刻（T，Ta～Tf，T'，Tb'）のうち，Ta，Td はリクエストの開始時刻，Tb，Tb'，Te，Tf はキャッシュされている最新稼働情報のタイムスタンプの時刻である。また，時刻の前後関係は次のとおりである。

$Tb \leqq Tb' < Tc$

$Te < Tf$

ここで，$x < y$ は，x が y に先行することを示す。

K 社情報システム部の M 君は，保守システムのネットワーク基盤を担当している。上司の N 氏から指示を受けた M 君は，保守システムの機能強化プロジェクトに先立ち，そこで必要となるネットワーク基盤の拡張について調査を進めてきた。

M 君は，図 4 ～ 6 を使って，その調査結果を N 氏に説明した。次はそのときの会話である。

N 氏：図 4 ～ 6 の内容は分かった。保守システムの機能強化プロジェクトで具体的な検討を行うことにしよう。ただ，その前に二つ確認したいことがある。

M 君：どのようなことでしょうか。

N 氏：今，保守システムの機能強化と並行して，次世代設備の企画も進められている。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。さらに，HTTP 以外の通信プロトコルも実装できる。一方，サービスの拡充に伴い，通信トラフィックは増加していくだろう。そこで，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。図 4 ～ 6 の案が，その新しい通信方式にも拡張可能かどうかも，事前に確認しておきたい。

M 君：分かりました。調べてみます。

N 氏：もう一つは，LAN 構成とネットワーク負荷に関する確認だ。今回，初めてブレードサーバを導入する予定だが，LAN 構成をどのように変えるのかを確認してほしい。それから，稼働情報収集では大量の通信が発生するはずだ。現行のネットワーク機器への影響が懸念される。その調査もお願いする。

M 君：分かりました。それらについても確認します。

〔次世代設備に関する通信方式〕

M 君は早速，新しい通信方式について調査し，RFC 7252 によって標準化が進められている通信プロトコルである CoAP（Constrained Application Protocol）が HTTP の代わりに利用できそうだと考えた。M 君が CoAP について調査した結果を次に示す。

・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 のメッセージ形式を図 7 に示す。

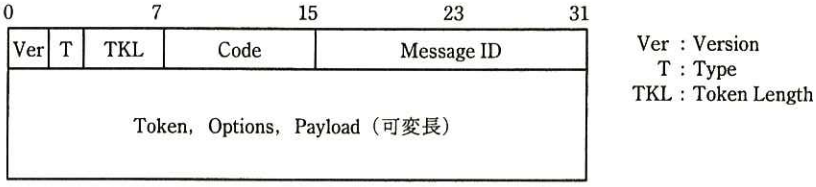


図 7　CoAP のメッセージ形式

・CoAP のメッセージは，4 バイトのヘッダと可変長の Token，Options，Payload から構成されている。1 バイトの Code を使い，リクエストの種別やレスポンスの状態コードを指定する。ZigBee に用いられる IEEE 802.15.4 フレームのデータ部は，IEEE 802.3（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。

以上の調査から，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。

M 君は，調査結果を基に，現在の設備に関する通信方式が次世代設備に関しても拡張可能であることを N 氏に説明した。

〔LAN の構成とネットワーク負荷〕

情報システム部は，新機能の開発に先立ち，次のような方針を立てている。

・2 台のブレードを内蔵したブレードサーバを K 社データセンタに導入する。
・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。

M 君は，新機能開発の方針を基に，NIC（Network Interface Card）を含む，ブレードサーバに関する LAN 構成について，次のような確認・検討を行った。

・ブレードサーバ内の LAN 構成を，図 8 に示す。

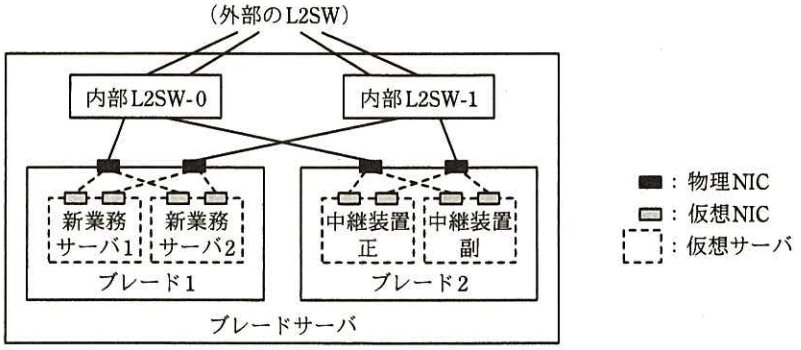


図 8　ブレードサーバ内の LAN 構成

・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［　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。
・(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。

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（以下，トランザクションという）が発生し，現行ネットワークの通信帯域に影響を与える可能性がある。また，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。そこで，M 君は，これらの通信負荷を見積もることにした。図 5 中の ④ の通信に関する見積りの前提を，表 1 に示す。

表1　図5中の④の通信に関する見積りの前提

項番	項目	前提値	備考
1	稼働情報の収集対象となる設備数	108,000 台	
2	通信アダプタ1台当たりの設備数	1～100 台	通信アダプタ 1 台に対して，複数の設備が接続される。
3	稼働情報収集の成功率	80 %	通信アダプタの約 20%は，電源断の状態にある。
4	トランザクションの通信時間	3 秒	
5	TCP の無通信タイムアウト時間	T_{out} 秒	
6	新サービス開始時の収集周期	3,600 秒	将来，5 分間に短縮される。

表1を前提にした見積り結果は次のとおりである。

・④の通信の起動タイミングは平準化されていると仮定すると，新サービス開始時には，表1中の項番1，6から，毎秒［　ア　］トランザクションが発生する。

・1 トランザクションは 1 コネクションで処理されると仮定すると，各コネクションの保持時間は，項番3～5から，平均（$2.4 + 0.2 \times T_{out}$）秒と推定できる。

・したがって，2 台の新業務サーバの④の通信に関する同時コネクション数の合計は，平均（［　イ　］＋［　ウ　］$\times T_{out}$）コネクションと推定できる。この値は，将来，収集周期が5分間になると，12 倍に増加する。

・各コネクションにおける通信データ量は，稼働情報が数バイトに過ぎない（図5）ことから，オーバヘッドを考慮しても，図2中の現行ネットワーク機器や閉域網サービスに与える影響は限定的である。

このような検討の結果から，M 君は，通信帯域については当面懸念しなくてもよいと判断した。しかし，同時コネクション数は，FW の性能に大きく影響すると考え，負荷の予測と FW の増強について提言をまとめた。提言には，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含めた。

・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

・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

・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

M君は，以上の検討結果をまとめ，N氏に報告した。

その後，保守システムの機能強化プロジェクトが開始されることになり，M君はネットワークグループのリーダに任命された。

設問1　〔現在の保守システム〕について，(1)～(4)に答えよ。

(1) 本文中の［　あ　］に入れる適切な字句を答えよ。

(2) 図3中の［　い　］に入れる適切な機器名を答えよ。

(3) 図3中の①～⑧のIPパケットのうち，送信元IPアドレスが②と同じになるIPパケットの番号を全て答えよ。

(4) 図3中の①～⑧のIPパケットのうち，宛先IPアドレスが②と同じになるIPパケットの番号を全て答えよ。

設問2　〔保守システムの機能強化〕について，(1)～(6)に答えよ。

(1) 本文中の［　う　］～［　お　］に入れる適切な字句を答えよ。

(2) 本文中の下線(a)の利点を，25字以内で述べよ。

(3) 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。

(4) 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，35字以内で述べよ。

(5) 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，それぞれ30字以内で述べよ。

(6) 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40字以内で述べよ。

設問3　〔次世代設備に関する通信方式〕について，(1)～(3)に答えよ。

(1) 本文中の［　か　］に入れる適切な機器名を答えよ。

(2) 図7のCoAPメッセージ以外に，IEEE 802.15.4フレームのデータ部に含まれるデータを，20字以内で答えよ。

(3) 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，それぞれ30字以内で述べよ。

設問4　〔LANの構成とネットワーク負荷〕について，(1)～(6)に答えよ。

(1)　本文中の［　き　］に入れる適切な機器名を答えよ。

(2)　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。

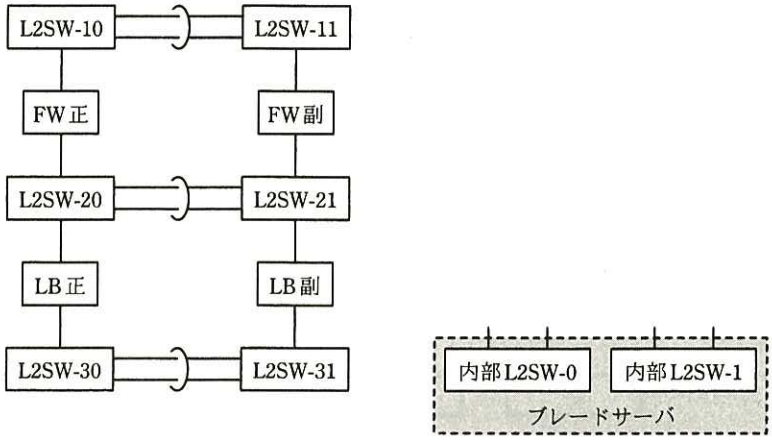


図9　内部L2SWとL2SWとの接続

(3)　本文中の［　ア　］～［　ウ　］に入れる適切な数値を答えよ。

(4)　本文中の下線(d)の設定方針を，30字以内で述べよ。

(5)　本文中の下線(e)の使い方を，30字以内で述べよ。

(6)　本文中の下線(f)の設計方針を，50字以内で述べよ。

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。

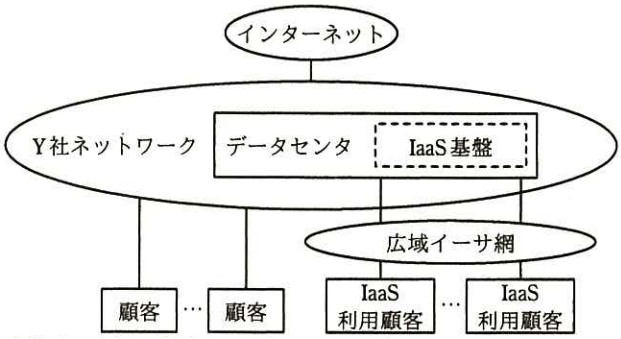


図1　現在のY社のネットワーク構成

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。

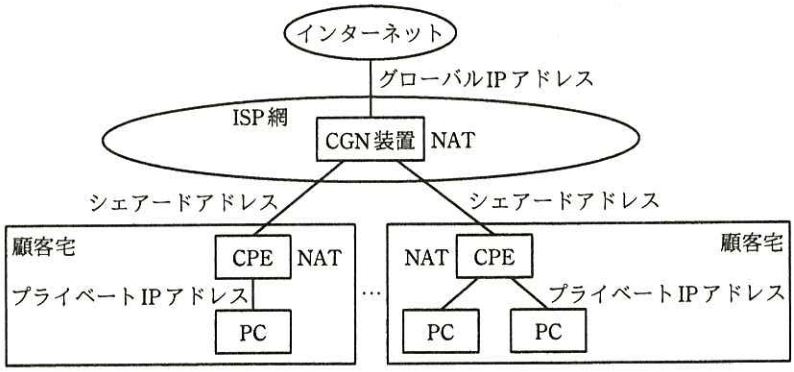


図 2　NAT444 の構成

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。

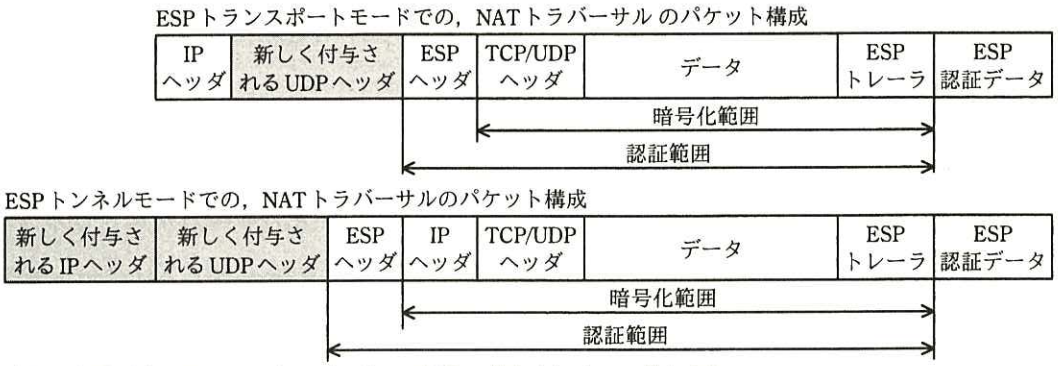
〔IPsec を利用する顧客への対応策〕

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。

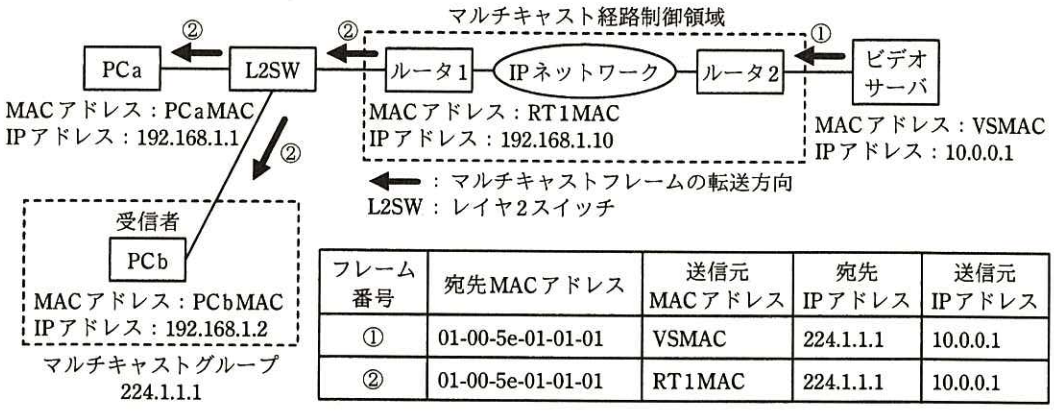
〔基盤ネットワークの課題とその対応〕

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

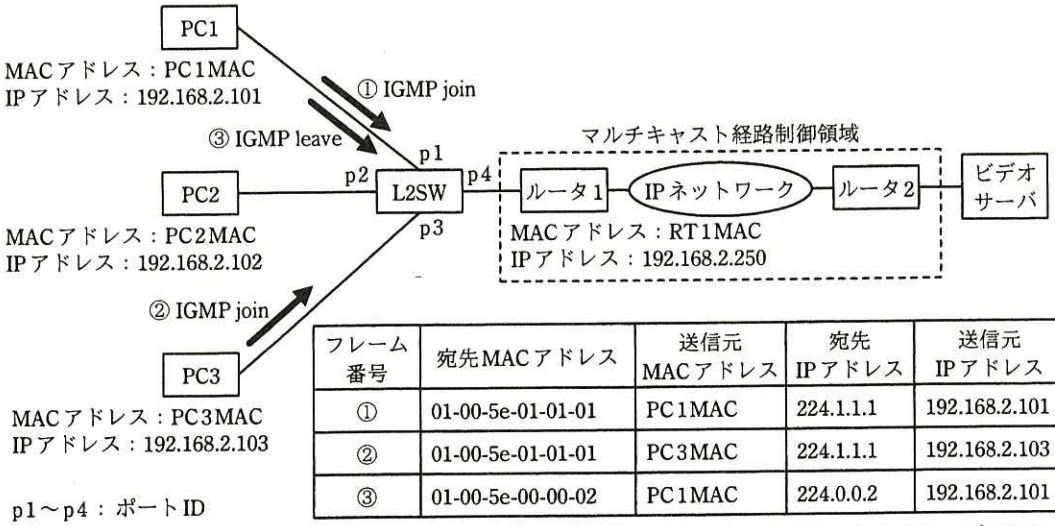
図 4 の例では，PCb をビデオサーバから送信される画像データの受信者とする。

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，PCaとPCbにマルチキャストフレームが届く。ただし，PCa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。

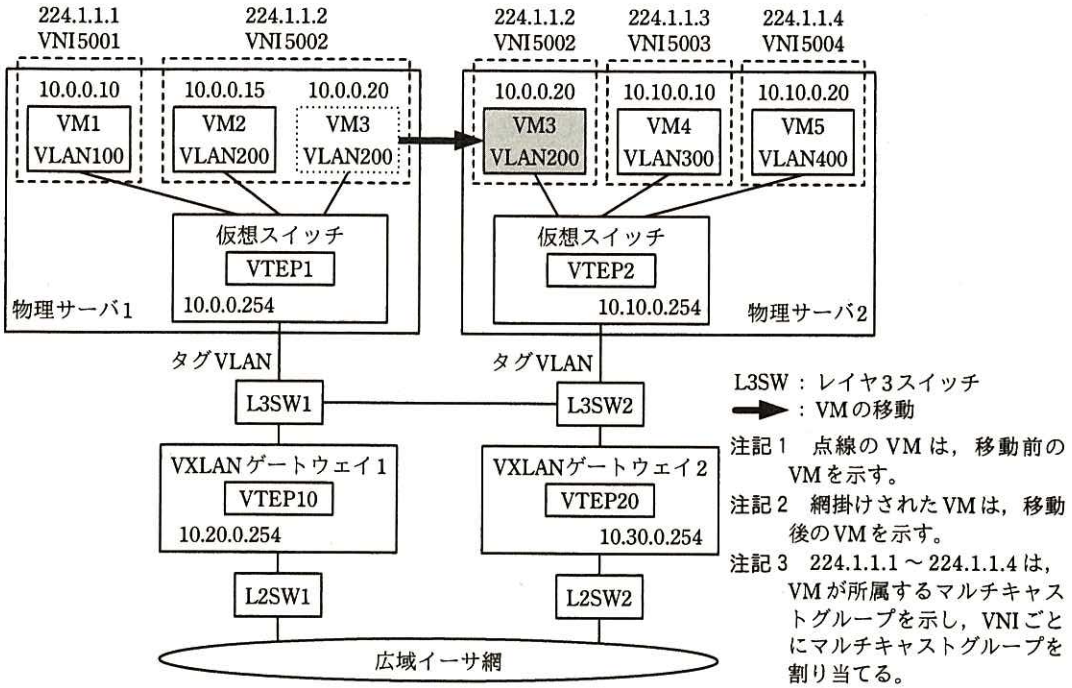


図7　基盤ネットワークへのVXLAN導入構成案（抜粋）

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。

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。
なお，試験問題では，™ 及び ® を明記していません。

©2015　独立行政法人情報処理推進機構