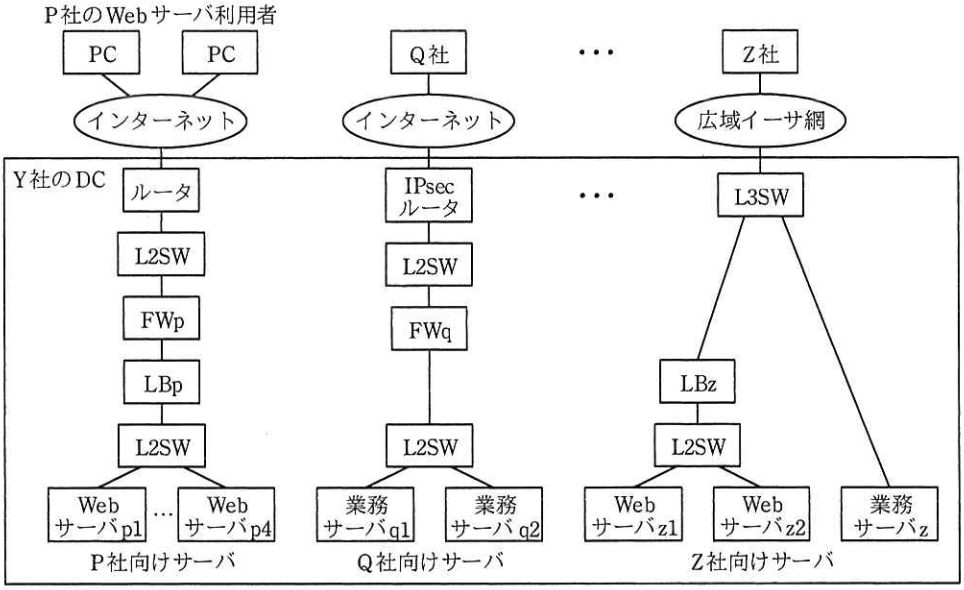
問２　サービス基盤の構築に関する次の記述を読んで，設問 1～5 に答えよ。

Y 社は，データセンタ（以下，DC という）を運営し，ホスティングサービスを提供している。ホスティングサービスのシステムは，顧客ごとに独立したネットワークとサーバから構成されている。Y 社が運営しているホスティングサービスのシステム構成を図 1 に示す。



広域イーサ網：広域イーサネットサービス網　　FW：ファイアウォール
L2SW：レイヤ2スイッチ　　L3SW：レイヤ3スイッチ　　LB：サーバ負荷分散装置
注記　P 社，Q 社，Z 社は，Y 社の顧客である。

図 1　Y 社が運営しているホスティングサービスのシステム構成（抜粋）

このたび，Y 社では，新規顧客へのサービスの提供やサーバの増設を迅速に行えるようにするとともに，導入コストや運用コストを削減してサービスの収益性を高める目的で，サービス基盤の構築を決定した。このサービス基盤では，ネットワークと物理サーバを顧客間で共用し，論理的に独立した複数の顧客システムを稼働させる，マルチテナント方式の IaaS（Infrastructure as a Service）を提供する。

サービス基盤構築プロジェクトリーダに指名された，基盤開発部の M 課長は，部下でネットワーク構築担当の N 主任に，次の 3 点の要件を提示し，サービス基盤の構成を検討するよう指示した。

(1) サーバの仮想化によって，サーバ増設要求に迅速に対応可能とすること

(2) サービス基盤で稼働する顧客システムは，顧客ごとに論理的に独立させること

(3) サービス基盤は冗長構成とし，サービス停止を極力抑えられるようにすること

N 主任は，SDN（Software-Defined Networking）技術を用いず，従来の技術を用いた方式（以下，従来方式という）と SDN 技術を用いた方式（以下，SDN 方式という）の二つの方式に関して，サービス基盤を構築する場合や顧客が増減した場合の作業内容などを比較して，構築方式を決めることにした。この方針を基に，N 主任は，部下の J さんに，サービス基盤の構成について検討するよう指示した。

〔従来方式でのサービス基盤の構成案〕

J さんは，まず，従来方式で構築する場合のサービス基盤の構成を検討した。J さんが設計した，従来方式によるサービス基盤の構成案を図 2 に示す。

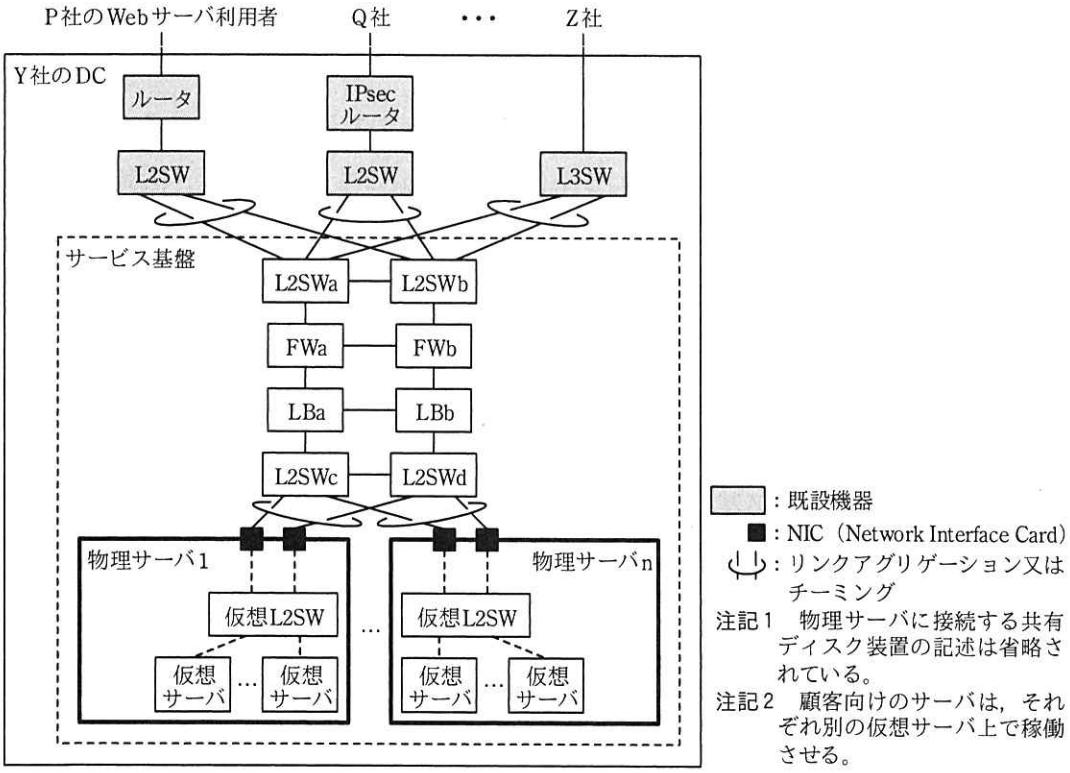


図 2　従来方式によるサービス基盤の構成案

サービス基盤は，VLAN によって顧客間のネットワークを論理的に独立させる。

図 2 中の既設の L2SW 及び L3SW のサービス基盤への接続ポートには，それぞれリンクアグリゲーションを設定する。既設の L2SW 又は L3SW に接続する L2SWa と L2SWb のポートには，接続先の顧客ごとにリンクアグリゲーションと VLAN を設定する。L2SWa と L2SWb の間及び L2SWc と L2SWd の間は，［　ア　］接続して，それぞれ，一つの L2SW として動作できるようにする。

FW は，①装置の中に複数の仮想 FW を稼働させることができ，②装置の冗長化ができる製品を選定する。冗長構成では，アクティブの仮想 FW が保持しているセッション情報が，装置間を直結するケーブルを使って，スタンバイの仮想 FW に転送される。セッション情報を継承することで，仮想 FW の［　イ　］フェールオーバを実現している。

LB は，負荷分散対象のサーバ群を一つのグループ（以下，クラスタグループという）としてまとめ，クラスタグループを複数設定できる製品を選定する。クラスタグループごとに仮想 IP アドレスと［　ウ　］アルゴリズムが設定できるので，複数の顧客の処理を 1 台で行える。LB も冗長化が可能であり，FW と同様の方法で冗長構成を実現している。

図 2 の構成案では，FW と LB は，FWa と LBa をアクティブに設定する。スタンバイの装置がアクティブに切り替わる条件は，両装置とも同様であり，両装置は連動して切り替わる。

物理サーバには 2 枚の NIC を実装し，［　エ　］機能を利用してアクティブ／アクティブの状態にする。L2SWc と L2SWd には，リンクアグリゲーションのほかに，③仮想サーバの物理サーバ間移動に必要となる VLAN を設定する。

〔SDN 方式でのサービス基盤の構成案〕

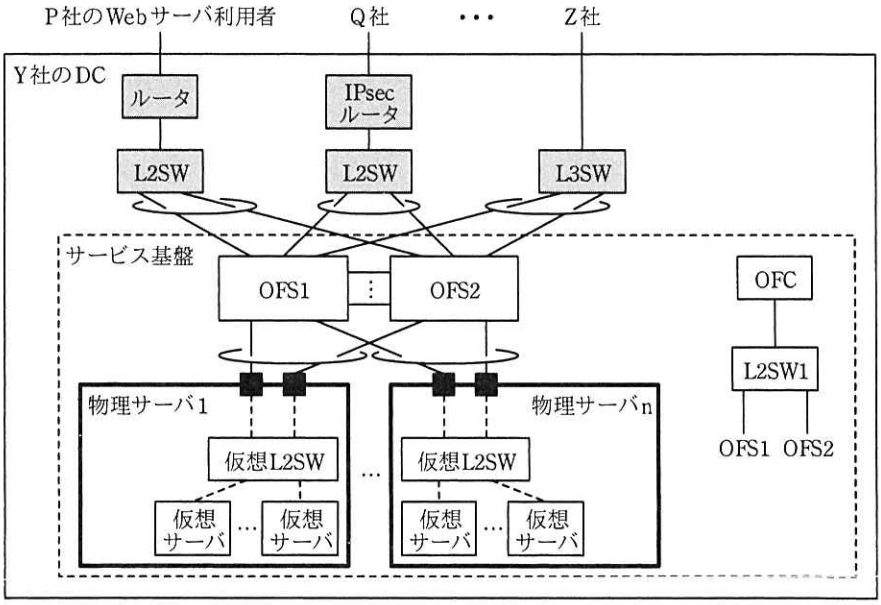
次に，J さんは，SDN 製品のベンダの協力を得て，SDN 方式で構築する場合のサービス基盤の構成を検討した。

SDN を実現する技術の中に，OpenFlow（以下，OF という）がある。今回の検討では，標準化が進んでいる OF を利用することにした。

OF は，データ転送を行うスイッチ（以下，OFS という）と，OFS の動作を制御するコントローラ（以下，OFC という）から構成される。OFS によるデータ転送は，

OFC によって設定されたフローテーブル（以下，F テーブルという）に基づいて行われる。

J さんが設計した，OF によるサービス基盤の構成案を図 3 に示す。



注記 1　物理サーバに接続する共有ディスク装置の記述は省略されている。
注記 2　OFC は L2SW1 を介して，OFS1 と OFS2 の管理用ポートに接続される。
注記 3　顧客向けのサーバ，FW 及び LB は，それぞれ別の仮想サーバ上で稼働させる。

図 3　OF によるサービス基盤の構成案

OFS は 2 台構成とし，相互に接続する。図 3 中の 既設の L2SW 及び L3SW のサービス基盤への接続ポートには，リンクアグリゲーションを設定し，OFS1 と OFS2 に接続する。物理サーバには，図 2 と同様に 2 枚の NIC を実装して各 NIC をアクティブ／アクティブの状態にする。FW と LB には，仮想サーバ上で稼働する仮想アプライアンス製品を利用する。OFC は，OFS1 と OFS2 の管理用ポートに接続する。

これらの OFS は，起動すると OFC との間で TCP コネクションを確立する。その後は，OFC との間の通信路となる OF チャネルが開設され，それを経由して OFC から F テーブルの作成や更新が行われる。したがって，OFS の導入時には，④ OFC との TCP コネクションの確立に必要な最小限の情報を設定すればよく，導入作業は容易である。

Jさんは，二つの方式で設計したサービス基盤の構成をN主任に説明したところ，二つの方式を比較し，Y社に適した方式を提案するよう指示を受けた。

〔二つの方式の比較〕

Jさんは，図2と図3のサービス基盤を構築する場合について，二つの方式で実施することになる作業内容などを基に，比較表を作成した。Jさんが作成した二つの方式の比較を表1に示す。

表1　Jさんが作成した二つの方式の比較

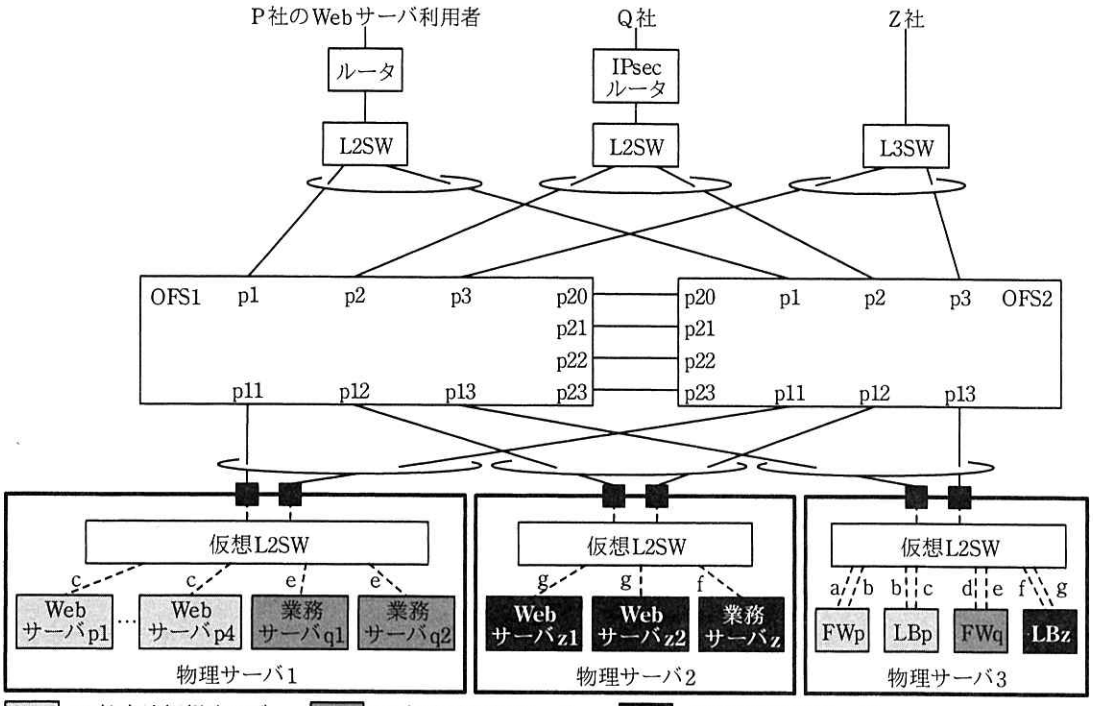
項番	比較項目	従来方式	SDN方式（図3の方式）
1	導入機器の数	多い	少ない
2	構築時の設定作業	（設問のため省略）	（設問のため省略）
3	顧客追加時の設定作業	（設問のため省略）	（設問のため省略）
4	サービス基盤の増設時の作業	（省略）	（省略）
5	必要技術の習得	習得済み	未習得

以上の比較検討を基に，Jさんは，OFを用いると技術習得などに時間を要することになるが，今後のサービス拡大に柔軟に対応できるようになると判断し，OFによるサービス基盤の構築を，N主任に提案した。N主任は，Jさんの提案がY社にとって有益であると考え，Jさんの提案を基にサービス基盤の構築案をまとめ，M課長に報告したところ，テストシステムを構築して，OFの導入効果を確認するようにとの指示を受けた。

〔技術習得を目的とした制御方式の設計〕

テストシステムの構築に当たって，N主任とJさんの2人は最初に，OFの技術習得を目的として，MACアドレスの学習によるパケットの転送制御方式を考えることにした。

テストシステムは，図1中のP社，Q社及びZ社の3顧客向けのシステムを収容した構成である。テストシステムの構成を図4に，テストシステム中の機器と仮想サーバのMACアドレスを表2に示す。



：P社向け仮想サーバ　：Q社向け仮想サーバ　：Z社向け仮想サーバ

a：VLAN ID＝100　b：VLAN ID＝110　c：VLAN ID＝120　d：VLAN ID＝200
e：VLAN ID＝210　f：VLAN ID＝300　g：VLAN ID＝310

注記 1　p1～p3，p11～p13，p20～p23 は，ポート番号を示す。
注記 2　OFC と共有ディスク装置の記述は省略されている。

図 4　テストシステムの構成

表 2　テストシステム中の機器と仮想サーバの MAC アドレス

機器名又は仮想サーバ名	MAC アドレス
P 社の Web サーバ p1～p4	mWSp1～mWSp4
Q 社の業務サーバ q1，q2	mGSq1，mGSq2
Z 社の Web サーバ z1，z2	mWSz1，mWSz2
Z 社の業務サーバ z	mGSz

機器名又は仮想サーバ名	内部側[1]の MAC アドレス	WAN 側[2]の MAC アドレス
ルータ	mRT	（省略）
IPsec ルータ	mIPSRT	（省略）
L3SW	mL3SW	（省略）
LBp	mLBp	mLBpw
LBz	mLBz	mLBzw
FWp	mFWp	mFWpw
FWq	mFWq	mFWqw

注記　MAC アドレスの重複はないものとする。
注 1)　内部側は，図 1 中の各機器の下側のポートを指す。
2)　WAN 側は，図 1 中の各機器又はサーバの上側のポートを指す。

図 4 に示したように，P 社には VLAN ID に 100，110，120，Q 社には VLAN ID に

200，210，Z 社には VLAN ID に 300，310 を，それぞれ割り当てる。各顧客の Web サーバと業務サーバ間の通信は発生しない。

2 人は，F テーブルの構成について検討した。F テーブルは，OFS のデータ転送動作を確認しやすくするために，最初に処理される F テーブル 0 と，パケットの入力ポートに対応して処理される F テーブル 1～4 の五つの構成とした。2 人がまとめた，五つの F テーブルの役割を表 3 に示す。

表 3　五つの F テーブルの役割

項番	F テーブル名	役割
1	F テーブル 0	パケットの入力ポートを基にした，処理の振分け
2	F テーブル 1	顧客のネットワークから，p1～p3 経由で OFS に入力したパケットの処理
3	F テーブル 2	物理サーバ 1 から，p11 経由で OFS に入力したパケットの処理
4	F テーブル 3	物理サーバ 2 から，p12 経由で OFS に入力したパケットの処理
5	F テーブル 4	物理サーバ 3 から，p13 経由で OFS に入力したパケットの処理

F テーブルは，複数のフローエントリ（以下，F エントリという）からなる。

F エントリは，OFS に入力されたパケットがどの F エントリに一致するかを判定するためのマッチング条件，条件に一致したパケットに対する操作を定義するアクション，パケットが複数の F エントリに一致した場合の優先度などで構成される。入力されたパケットが，F テーブル内の複数の F エントリのマッチング条件に一致した場合は，優先度が最も高い F エントリのアクションが実行される。また，どのマッチング条件にも一致しないパケットは廃棄される。一つの F エントリには，複数のアクションを定義できる。

OFC と OFS の間では，メッセージの交換が行われる。このメッセージの中には，OFS に対して F エントリを設定する Flow-Mod メッセージ，OFS が受信したパケットを OFC に送信する Packet-In メッセージ，OFC が OFS に対して指定したパケットの転送を指示する Packet-Out メッセージなどがある。

次に，2 人は，3 顧客で全てのサーバとの通信が正常に行われたとき（以下，正常通信完了時という）に，OFC によって OFS に生成される F エントリを，机上で作成した。正常通信完了時の F テーブル 0～4 を，それぞれ表 4～8 に示す。

表 4　正常通信完了時の OFS1 と OFS2 の F テーブル 0

項番	マッチング条件	アクション	優先度
1	入力ポート＝p1	VLAN ID が 100 のタグをセット，F テーブル 1 で定義された処理を行う。	中
2	入力ポート＝p2	VLAN ID が 200 のタグをセット，F テーブル 1 で定義された処理を行う。	中
3	入力ポート＝p3	VLAN ID が 300 のタグをセット，F テーブル 1 で定義された処理を行う。	中
4	入力ポート＝p11	F テーブル 2 で定義された処理を行う。	中
5	入力ポート＝P12	F テーブル 3 で定義された処理を行う。	中
6	入力ポート＝p13	F テーブル 4 で定義された処理を行う。	中

表 5　正常通信完了時の OFS1 と OFS2 の F テーブル 1

項番	マッチング条件	アクション	優先度
1	eTYPE [1] ＝ARP	OFC に Packet-In メッセージを送信	低
2	mDES [2] ＝mFWpw	p13 から出力	中
3	mDES [2] ＝mFWqw	p13 から出力	中
4	mDES [2] ＝mLBzw	p13 から出力	中
5	mDES [2] ＝mGSz	p12 から出力	中

注 [1]　eTYPE は，イーサタイプを示す。
　 [2]　mDES は，宛先 MAC アドレスを示す。

表 6　正常通信完了時の OFS1 と OFS2 の F テーブル 2

項番	マッチング条件	アクション	優先度
1	eTYPE＝ARP	OFC に Packet-In メッセージを送信	低
2	eTYPE＝ARP，VLAN ID＝120， mDES＝FF-FF-FF-FF-FF-FF	p13 から出力	高
3	eTYPE＝ARP，VLAN ID＝210， mDES＝FF-FF-FF-FF-FF-FF	p13 から出力	高
4	mDES＝mLBp，mSRC [1] ＝mWSp1	p13 から出力	中
5	eTYPE＝RARP	OFC に Packet-In メッセージを送信	高
以下，省略			

注記　項番 5 は，仮想サーバが物理サーバ 1 に移動してきたことを OFC に知らせるための F エントリである。

注 [1]　mSRC は，送信元 MAC アドレスを示す。

表 7　正常通信完了時の OFS1 と OFS2 の F テーブル 3

項番	マッチング条件	アクション	優先度
1	eTYPE＝ARP	OFC に Packet-In メッセージを送信	低
2	eTYPE＝ARP，VLAN ID ＝310， mDES＝FF-FF-FF-FF-FF-FF	p13 から出力	高
3	mDES＝mLBz，mSRC＝mWSz1	p13 から出力	中
4	mDES＝mL3SW，mSRC＝mGSz	VLAN タグを削除，p3 から出力	中
5	eTYPE＝RARP	OFC に Packet-In メッセージを送信	高
以下，省略			

注記　項番 5 は，仮想サーバが物理サーバ 2 に移動してきたことを OFC に知らせるための F エントリである。

表 8　正常通信完了時の OFS1 と OFS2 の F テーブル 4

項番	マッチング条件	アクション	優先度
1	eTYPE＝ARP	OFC に Packet-In メッセージを送信	低
2	eTYPE＝ARP，VLAN ID ＝100， mDES＝FF-FF-FF-FF-FF-FF	VLAN タグを削除，p1 から出力	高
3	eTYPE＝ARP，VLAN ID ＝120， mDES＝FF-FF-FF-FF-FF-FF	p11 から出力	高
4	eTYPE＝ARP，VLAN ID ＝300， mDES＝FF-FF-FF-FF-FF-FF	VLAN タグを削除，p3 から出力	高
5	eTYPE＝ARP，VLAN ID ＝310， mDES＝FF-FF-FF-FF-FF-FF	p12 から出力	高
6	mDES＝mWSp1，mSRC＝mLBp	p11 から出力	中
7	mDES＝mWSp4，mSRC＝mLBp	p11 から出力	中
8	mDES＝mWSz1，mSRC＝mLBz	p12 から出力	中
9	mDES＝mRT，mSRC＝mFWpw	VLAN タグを削除，p1 から出力	中
10	mDES＝mIPSRT，mSRC＝mFWqw	VLAN タグを削除，p2 から出力	中
11	mDES＝mL3SW，mSRC＝mLBzw	VLAN タグを削除，p3 から出力	中
12	eTYPE＝RARP	OFC に Packet-In メッセージを送信	高
以下，省略			

注記　項番 12 は，仮想サーバが物理サーバ 3 に移動してきたことを OFC に知らせるための F エントリである。

表 8 中の項番 2 は，イーサタイプが ARP，VLAN ID が 100 及び宛先 MAC アドレスが FF-FF-FF-FF-FF-FF のパケットを，VLAN タグを削除して p1 から出力することを示している。

OFS にパケットが入力されると，OFS は表 4 の F テーブル 0 の処理を最初に実行

する。例えば，図4中のQ社のIPsecルータからOFS1のp2にARPリクエストパケットが入力された場合，そのパケットは，表4中の項番2に一致するので，パケットにVLAN IDが200のVLANタグをセットし，次に表5のFテーブル1で定義された処理を行う。表5のFテーブル1では，項番1に一致するので，当該パケットはPacket-Inメッセージに収納されて，OFCに送信される。OFCは受信したパケットの内容を基に，Flow-ModメッセージでFエントリを生成したり，Packet-Outメッセージなどを OFSに送信したりする。

N主任とJさんは，作成したFテーブルの論理チェックを行い，五つのFテーブルによってテストシステムを稼働させることができると判断した。

パケット転送制御方式の机上作成を通してOFの動作イメージが学習できたので，次に，2人は，実際にテストシステムを構築して，動作検証と性能評価を行うことにした。

設問1　本文中の［　ア　］～［　エ　］に入れる適切な字句を答えよ。

設問2　〔従来方式でのサービス基盤の構成案〕について，(1)～(3)に答えよ。

(1) 本文中の下線①の要件が必要になる理由を，30字以内で述べよ。

(2) 本文中の下線②の機能について，アクティブのFWをFWaからFWbに切り替えるのに，FWa又はFWbが監視する内容を三つ挙げ，図2中の機器名を用いて，それぞれ25字以内で答えよ。

(3) 本文中の下線③について，VLANを設定するポート及び設定するVLANの内容を，50字以内で具体的に述べよ。

設問3　本文中の下線④の情報を，15字以内で答えよ。

設問4　〔二つの方式の比較〕について，(1)，(2)に答えよ。

(1) 表1中の項番2について，従来方式の場合，FWでは複数の仮想FWを設定することになる。仮想FWの設定に伴って，各仮想FWに対して設定が必要なネットワーク情報を三つ挙げ，それぞれ15字以内で答えよ。

(2) 表1中の項番3について，従来方式の場合，追加する顧客に対応したVLAN設定がサービス基盤の全ての機器及びサーバで必要になる。その中で，ポートVLANを設定する箇所を，図2中の名称を用いて，40字以内で答えよ。

設問5　〔技術習得を目的とした制御方式の設計〕について，(1)～(4) に答えよ。

(1) 本番システムにおいて，図 4 の形態で 3 顧客の仮想サーバを配置した場合に発生する可能性がある問題を，40 字以内で述べよ。また，その問題を発生させないための仮想サーバの配置を，40 字以内で述べよ。

(2) 表 8 の F テーブル 4 中には，FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートに，パケットを転送させるための F エントリが生成されない。当該 F エントリがなくても FWp と LBp 間の通信が行われる理由を，70 字以内で述べよ。

(3) P 社の Web サーバ利用者から送信された，Web サーバ宛てのユニキャストパケットが Web サーバ p1 に転送されるとき，パケットの転送は，次の【パケット転送処理手順】となる。

【パケット転送処理手順】

ルータ→L2SW→F テーブル 0，項番 1→［　オ　］→FWp→LBp→［　カ　］→［　キ　］→Web サーバ p1

【パケット転送処理手順】中の［　オ　］～［　キ　］に入れる適切な F テーブル名と項番を答えよ。F テーブル名は，F テーブル 0～4 から選べ。また，項番は表 4～8 中の項番で答えよ。ここで，パケット転送制御を行う OFS は特定しないものとする。

(4) P 社の Web サーバ p4 が物理サーバ 2 に移動し，表 7 の OFS1 の F テーブル 3 中の項番 5 によって，OFC に Packet-In メッセージが送信されると，OFC は表 8 の F テーブル 4 中の二つの項番を変更する。F テーブル 4 が変更される OFS 名を全て答えよ。また，項番 3 のほかに変更される項番及び変更後のアクションを答えよ。