NW

平成 30 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〕

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　ネットワークシステムの設計に関する次の記述を読んで，設問1～4に答えよ。

機械メーカのX社は，顧客に販売した機械の運用・保守と，機械が稼働している顧客の工場の自動化支援に関する新事業を拡大しようとしている。

機械は工作装置及び通信装置の2種類である。工作装置には，センサ，アクチュエータなどを制御する機構（以下，デバイスという），及びレイヤ2スイッチが内蔵されている。通信装置は，デバイスをインターネットに接続するための機器で，エッジサーバ，ファイアウォール及びレイヤ3スイッチが内蔵されている。

X社の情報システム部は，新事業用のサービス基盤システム（以下，Xシステムという）を計画中である。情報システム部に所属するネットワーク担当のWさんが，Xシステムの構想について，検討を行っている。

〔Xシステムの構想〕

Xシステムは，X社が運用・保守を行う顧客の工場内の機器，X社内のサーバ，及びそれらを接続するためのネットワーク機器から構成されている。

Xシステムの導入構成例を図1に示す。

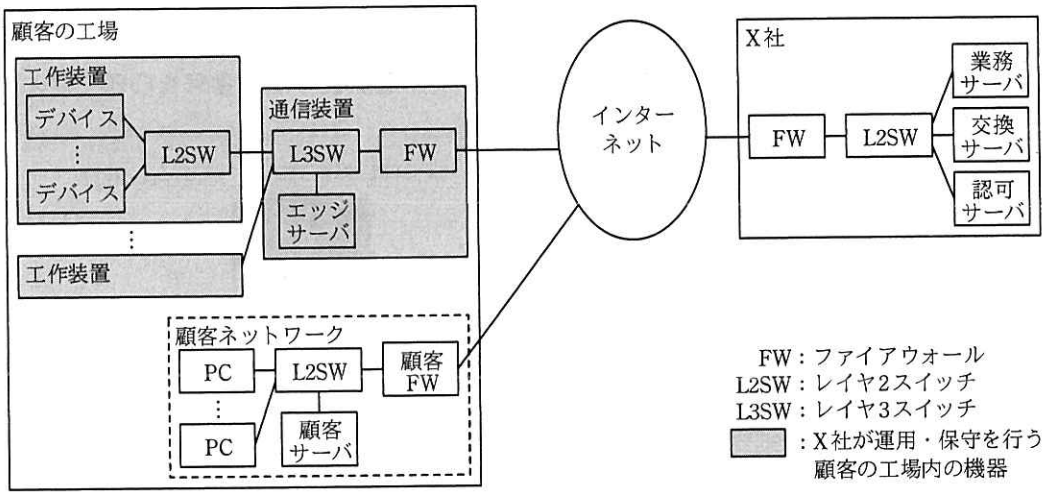


図1　Xシステムの導入構成例（抜粋）

Xシステムの業務アプリケーションプログラムは，エッジサーバと業務サーバ上で

動作する。これらのサーバとデバイスは，デバイスの運用・保守に関する情報を，自動的に交換する。この情報交換に関する説明を次に示す。

・工作装置と通信装置を接続し，顧客の工場内に X システム専用のネットワークを構成する。顧客ネットワークは利用しない。

・publish/subscribe 型のメッセージ通信プロトコル MQTT（Message Queuing Telemetry Transport）を使って，交換サーバを介して，デバイス，エッジサーバ及び業務サーバの間でメッセージを交換する。

・デバイス，エッジサーバ及び業務サーバに MQTT クライアント機能を，交換サーバに MQTT サーバ機能をそれぞれ実装する。

業務サーバは，顧客向けに API（Application Programming Interface）を提供する。顧客は，インターネット経由で API にアクセスし，デバイスの運用・保守に関する情報を参照する。この API に関する説明を次に示す。

・X 社の業務サーバと認可サーバに HTTP サーバ機能をそれぞれ実装する。

・顧客は，顧客サーバに，API アクセス用の Web アプリケーション（以下，WebAP という）と HTTP サーバ機能を実装する。

・顧客は，PC の Web ブラウザを使い，顧客サーバを経由して，API にアクセスする。

・X 社の認可サーバは，顧客サーバから API へのアクセスを認可する。

W さんは，上司から，X システムの構想に関する四つの技術検討を指示されている。四つの技術検討項目を次に示す。

・ネットワークセキュリティ対策

・MQTT を使ったメッセージ交換方式

・API にアクセスする顧客サーバの管理

・エッジサーバを活用する将来構想

〔ネットワークセキュリティ対策〕

X システムは，インターネット及び顧客の工場内の X システム専用のネットワークを利用するので，これらの X 社外の通信区間に関するネットワークセキュリティ対策が必要となる。W さんが検討したネットワークセキュリティ対策を次に示す。

・情報の漏えい及び改ざん対策のために TLS を利用する。TLS には，情報を［ア］する機能，情報の改ざんを［イ］する機能，及び通信相手を［ウ］する機能がある。

・工場内の機器と X 社内の機器との通信は，いずれもクライアントサーバ型の通信であり，機器間の［エ］コネクションの確立要求は，工場から X 社の方向に行われる。それを踏まえて，次の侵入及びなりすまし対策を採用する。

- X 社に設置された FW を使った対策
- ①通信装置内の FW を使った対策
- ② TLS の機能を使った，デバイス及びエッジサーバに関する対策

〔MQTT を使ったメッセージ交換方式〕

W さんは，MQTT を使ったメッセージ交換方式を調査した。

このメッセージ交換方式では，固定ヘッダ，可変ヘッダ及びペイロードから構成された MQTT コントロールパケットを使う。MQTT コントロールパケットの種別を表 1 に示す。

表 1　MQTT コントロールパケットの種別（抜粋）

種別	用途	固定ヘッダ，可変ヘッダ又はペイロードに含まれる情報
CONNECT	クライアントからサーバへの接続要求	（省略）
CONNACK	CONNECT に対する確認応答	（省略）
PUBLISH	メッセージの送信	QoS レベル[1)]，トピック名[2)]，パケット ID[3)]，メッセージ
PUBREC	メッセージ受信の通知	パケット ID[3)]
PUBREL	メッセージリリースの通知	パケット ID[3)]
PUBCOMP	メッセージ送信終了の通知	パケット ID[3)]
SUBSCRIBE	クライアントからサーバへの購読要求	QoS レベル[1)]，トピック名[2)]，パケット ID[3)]
SUBACK	SUBSCRIBE に対する確認応答	パケット ID[3)]

注 1)　QoS レベルは，送信者と受信者間のメッセージの送達確認手順を指定する識別子である。
2)　トピック名は，メッセージの種類を表す識別子である。
3)　パケット ID は，PUBLISH 又は SUBSCRIBE に付与する識別子である。

MQTT を使ったメッセージ交換方式の通信シーケンス例を図 2 に示す。

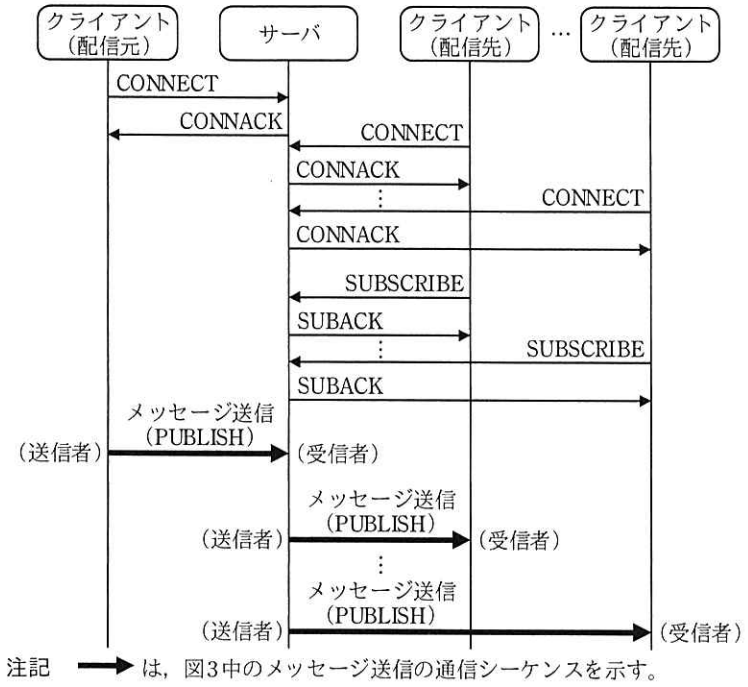


図 2　MQTT を使ったメッセージ交換方式の通信シーケンス例

図 2 中の通信シーケンスでは，配信元から複数の配信先へメッセージが配信されている。通信シーケンスの説明を次に示す。

・クライアントは，サーバの TCP ポート 8883 番にアクセスし，TCP コネクションを確立する。この TCP コネクションは，メッセージ交換の間は常に維持される。

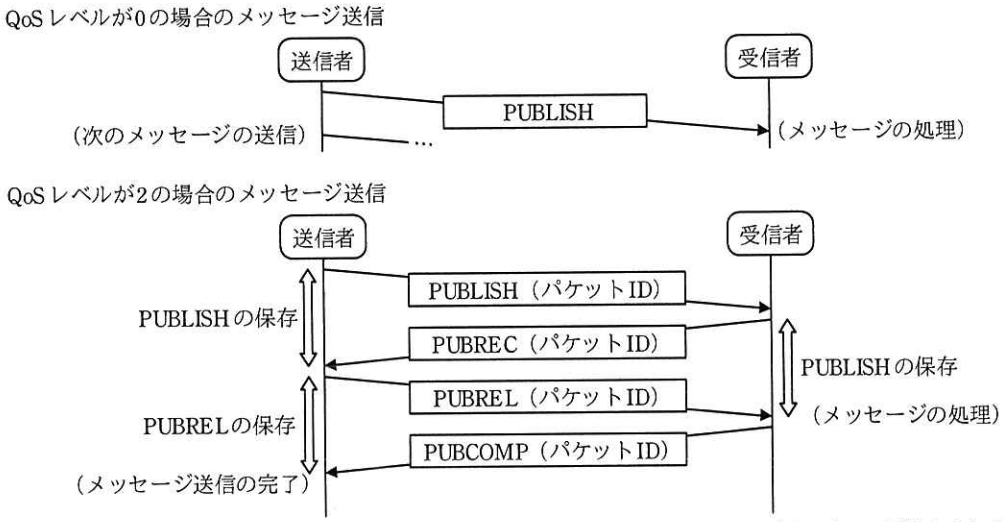
・クライアントは CONNECT を送信し，サーバは CONNACK を返信する。

・配信先となるクライアントは，サーバに SUBSCRIBE を送信し，購読対象のメッセージを，トピック名を使って通知する。サーバはクライアントに SUBACK を返信し，購読要求を受け付けたことを通知する。

・配信元クライアントは，PUBLISH を使ってサーバにメッセージを送信する。

・メッセージを受信したサーバは，PUBLISH に含まれるトピック名について購読要求を受け付けている全てのクライアントに，そのメッセージを送信する。

PUBLISH を使ったメッセージ送信では，QoS レベルを使って送達確認手順を指定する。QoS レベルとメッセージ送信の通信シーケンスを図 3 に示す。



注記 1　QoS レベルが 2 の場合，送達確認を行う PUBLISH を識別するために，パケット ID が付与される。
注記 2　QoS レベルが 2 の場合，受信者は，メッセージの処理を開始した以降に受信した PUBLISH は，パケット ID の重複にかかわらず新しいパケットとみなす。

図 3　QoS レベルとメッセージ送信の通信シーケンス

図 3 中の通信シーケンスの説明を次に示す。

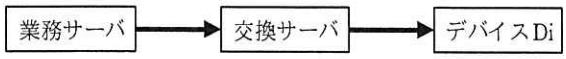
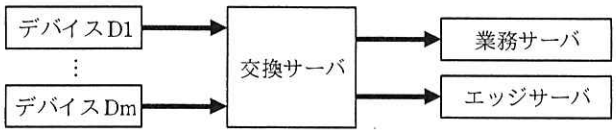
・QoS レベルが 0 の場合，MQTT 層における PUBLISH の送達確認は行わない。TCP 層による送達確認だけが行われる。

・QoS レベルが 2 の場合，MQTT 層においても PUBLISH の送達確認が行われる。MQTT 層の送達確認の説明を次に示す。

- TCP コネクションが切断された場合のために，PUBLISH 及び PUBREL は送信者によって保存され，送信者から受信者への再送に利用される。
- ③ PUBLISH を受信した受信者は，メッセージの処理を始める前に送信者に PUBREC を送信し，その応答である PUBREL を受信してからメッセージの処理を開始する。
- PUBREL を送信した送信者は，その応答である PUBCOMP を受信してから，メッセージ送信を完了する。

次に W さんは，X システムの 2 種類のメッセージ交換について，トピック名，QoS レベル，及び配信元と配信先を整理した。

X システムのメッセージ交換を図 4 に示す。

項番	メッセージ交換の概要	QoS レベル	トピック名	メッセージ
1	業務サーバから，特定のデバイス Di に対して，設定情報を送信する。 	2	config/Di	デバイス Di の設定情報
2	全てのデバイス Di（i=1，2，…，m）から，業務サーバ及び同じ工場のエッジサーバに対して，稼働情報を定期的に送信する。 	0	status/Di	デバイス Di の稼働情報

注記　Di は，デバイスの識別子を表す。

図4　Xシステムのメッセージ交換

図4の説明を次に示す。

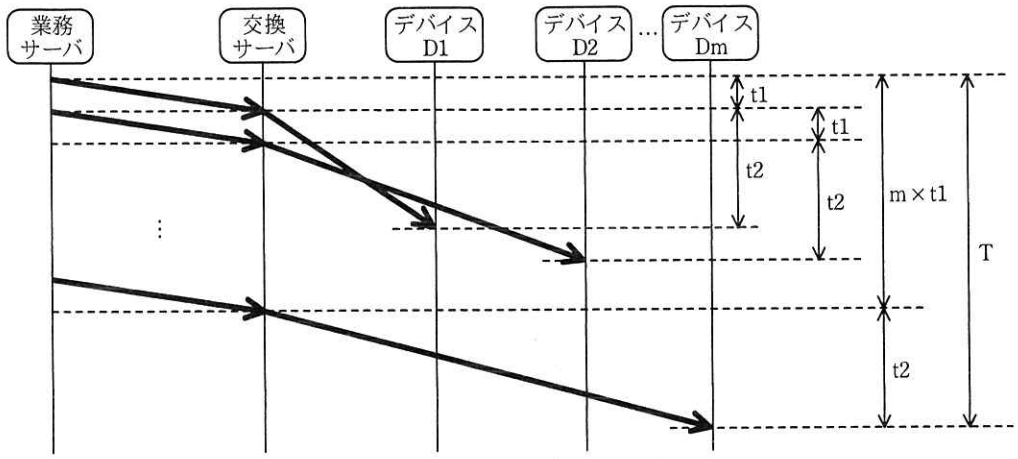
・項番 1 では，デバイス Di は，あらかじめ［　オ　］を交換サーバに送信し，トピック名が［　カ　］の PUBLISH が送信されるようにする。

・項番 1 では，QoS レベルとして 2 が使用されている。交換サーバからデバイス Di への PUBLISH 送信中に［　キ　］が電源断などで非稼働になった場合，その PUBLISH は，［　ク　］の中に保存され，稼働再開後に再送される。

・項番 2 では，QoS レベルとして 0 が使用されている。これは，［　ケ　］及びエッジサーバは安定した稼働が見込めるからである。

W さんは，1 台の業務サーバが 6,000 台のデバイスの設定を変更する場合の送信時間（T）を概算した。

W さんが T の概算に用いた通信シーケンスを図5に示す。



注記　太線の矢印は，QoSレベルが2の場合のメッセージ送信を表す。

図5　WさんがTの概算に用いた通信シーケンス

図5中の装置の処理時間を無視し，図5中のt1及びt2は，それぞれの装置間のRTT（Round Trip Time）の2倍に等しいとし，LANのRTTを20ミリ秒，WANのRTTを200ミリ秒とすると，Tは次のように概算できる。

T = m × t1 + t2 = 6,000 × 2 × 20 + 2 × 200（ミリ秒）≒ 4（分）

この概算を基に，Wさんは，次のように報告することにした。

・TCP コネクションが正常であれば，全デバイスへの設定情報の送信は 4 分間程度で完了する。

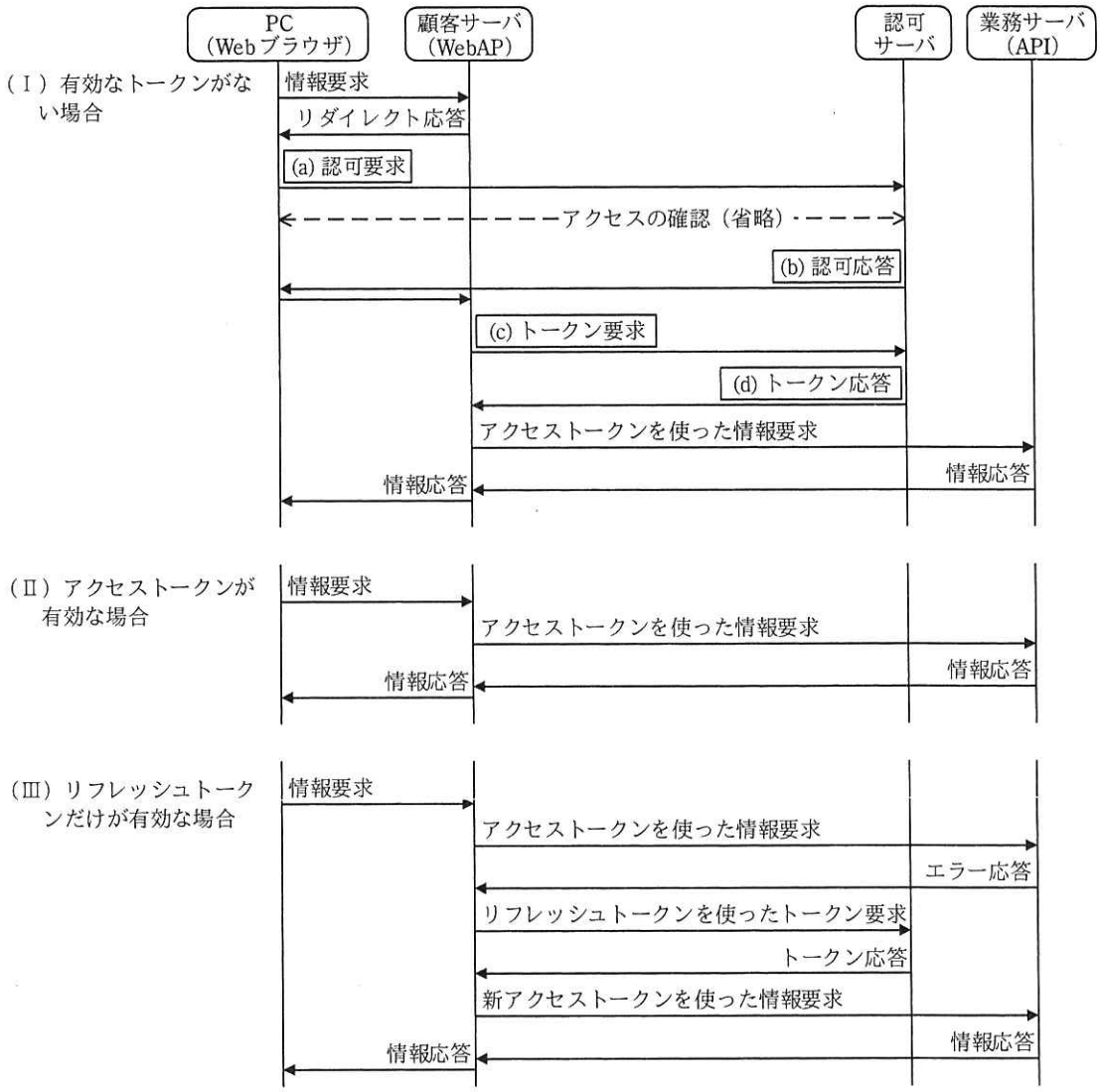
・ただし，図1に示すように，［　コ　］は同一拠点に設置されている必要がある。

〔APIにアクセスする顧客サーバの管理〕

Wさんは，顧客サーバからのAPIアクセスに関する検討を行った。

X システムでは，認可サーバを使って，顧客サーバからの API アクセスを認可する。契約及びサービス仕様の変更が顧客ごとに発生するので，それらを前提とした認可の仕組みが必要になる。W さんは，認可コード，アクセストークン，及びリフレッシュトークンを使った，認可の仕組みを採用することにした。

XシステムのAPIアクセスの通信シーケンスを図6に示す。



(a) 認可要求：
GET /authorize?redirect_uri=【WebAPのURI】（省略）
HOST:【認可サーバ】

(b) 認可応答：
HTTP/1.1 302 Found
Location: 【WebAPのURI】?code=【認可コード】

(c) トークン要求：
POST /token HTTP/1.1
（省略）
（省略）code=【認可コード】&redirect_uri=【WebAPのURI】（省略）

(d) トークン応答：
HTTP/1.1 200 OK
(省略)
【アクセストークン】,【リフレッシュトークン】(省略)

図 6　X システムの API アクセスの通信シーケンス

図 6 中の（Ⅰ）に示すように，有効なトークンがない場合，Web ブラウザから

WebAP への情報要求は，［　サ　］サーバにリダイレクトされる。認可応答では，認可要求で通知された URI を用いたリダイレクトによって，［　シ　］に認可コードが通知される。続いて，認可コードを用いたトークン要求とトークン応答が行われ，WebAP はアクセストークンとリフレッシュトークンを獲得する。

図 6 中の（Ⅰ）～（Ⅲ）に示すように，業務サーバへの情報要求には，アクセストークンが用いられる。アクセストークンには，アクセス可能な API と有効期間に関する情報が含まれており，業務サーバはそれらの情報からアクセスの可否を決める。アクセストークンの有効期間を過ぎた場合でも，［　ス　］の有効期間内であれば，利用者の確認を行わずに，新しいアクセストークンが発行される。

X システムでは，顧客ごとに異なるアクセストークンを定義し，認可サーバに格納しておく。ある顧客に提供する API の範囲が変わる場合，X 社は認可サーバのアクセストークンを変更する。W さんは，④アクセストークンの有効期間を 10 分間，リフレッシュトークンの有効期間を 60 分間と想定し，トークンの運用を確認した。

図 6 の通信シーケンスでは，図 6 中の“(a) 認可要求”の redirect_uri パラメタが書き換えられ，図 6 中の［　セ　］に含まれる認可コードが意図しない宛先に送信される可能性がある。W さんは，その対策として“redirect_uri パラメタの確認”を行うことにした。これは，図 6 中の［　ソ　］サーバに，HTTP リクエストに含まれる URI とあらかじめ登録されている絶対 URI が一致することを確認させる，という対策である。⑤顧客向けの API 利用ガイドラインには，この対策に必要な顧客への依頼内容を明記することにした。

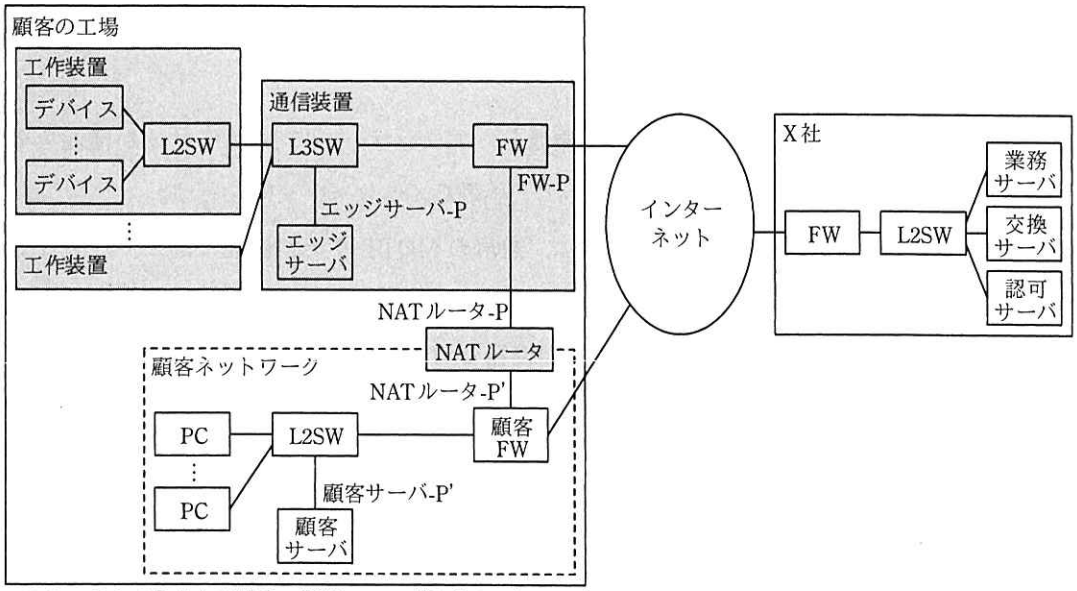
〔エッジサーバを活用する将来構想〕

図 4 中のメッセージ交換では，X 社内の交換サーバを利用するので，顧客の企業秘密を含むような設定情報及び稼働情報（以下，これらを内部情報という）は，対象外としている。しかし，内部情報についても図 4 と同様にメッセージ交換を行いたい顧客も多い。X 社では，エッジサーバを活用して，内部情報も X システムに取り込む将来構想をもっている。

顧客サーバが一つの場合について，将来構想で追加される X システムのメッセージ交換例を図 7 に，W さんが考えた将来構想におけるネットワーク構成案を図 8 に，それぞれ示す。

メッセージ交換の概要	トピック名	メッセージ
顧客サーバと同じ工場のデバイス Di（i=1, 2, …, m'）間で，エッジサーバを使って，顧客の工場に閉じた情報交換を行う。 	Confidential/Di	デバイス Di に関する内部情報

図 7　将来構想で追加される X システムのメッセージ交換例



ddd-P　：Xシステムにおける，機器dddのプライベートIPアドレス
ddd-P'：顧客ネットワークにおける，機器dddのプライベートIPアドレス

図 8　W さんが考えた将来構想におけるネットワーク構成案（抜粋）

図 8 に示すように，W さんは，NAT ルータを使って，顧客ネットワークと X システムを接続する案を考えた。NAT ルータは，1：1 静的双方向 NAT として動作させ，図 8 中の NAT ルータ-P と NAT ルータ-P' を利用して，宛先 IP アドレスと送信元 IP アドレスの両方を変換させる。

W さんが考えた将来構想におけるメッセージの流れを図 9 に示す。

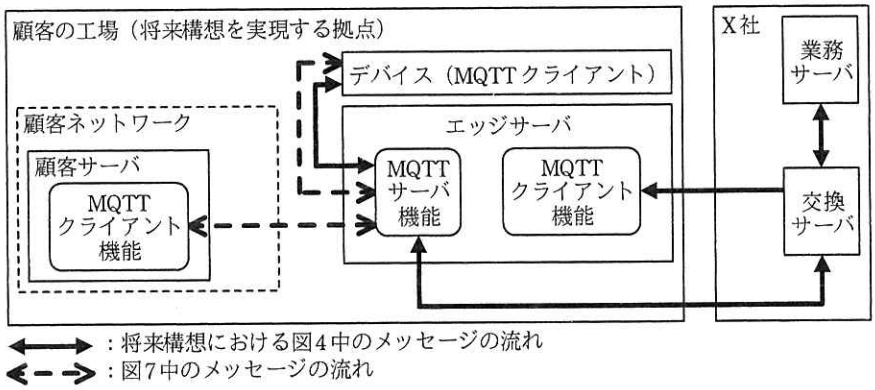


図 9　W さんが考えた将来構想におけるメッセージの流れ

図 9 の説明を次に示す。

・顧客サーバに MQTT クライアント機能を，エッジサーバに MQTT サーバ機能をそれぞれ実装し，顧客サーバとエッジサーバ間でメッセージ交換を行う。

・エッジサーバの MQTT サーバ機能は，通常の MQTT サーバ機能に加えて，メッセージをほかの MQTT サーバと送受信する機能（以下，MQTT ブリッジという）をもつ。X システムのデバイスは複数の機器と TCP コネクションを確立できないので，この MQTT ブリッジを利用する。

・⑥ MQTT ブリッジには，トピック名をあらかじめ定義しておき，そのトピック名のメッセージを交換サーバと送受信させる。

W さんは，図 7～9 を使って，ネットワークの動作について検討し，将来構想への対応が可能であると判断した。

W さんは，以上の検討結果を上司に報告した。X 社の情報システム部は，X システム構想を実現するためのプロジェクトを発足させた。

設問 1　〔ネットワークセキュリティ対策〕について，(1)～(3) に答えよ。

(1) 本文中の［ア］～［エ］に入れる適切な字句を答えよ。

(2) 本文中の下線①の対策を，50 字以内で述べよ。

(3) 本文中の下線②の対策を，30 字以内で述べよ。

設問２　〔MQTT を使ったメッセージ交換方式〕について，(1)～(4) に答えよ。

(1) 図 3 中の QoS レベルが 0 の場合のメッセージ送信について，TCP の再送機能だけではメッセージの消失が防げないのはどのような場合か。45 字以内で具体的に答えよ。

(2) 本文中の下線③について，PUBREL を受信するまで，メッセージの処理を保留する目的を，20 字以内で述べよ。

(3) 本文中の［　オ　］～［　ケ　］に入れる適切な字句を答えよ。

(4) 本文中の［　　コ　　］に入れる適切な機器名を全て答えよ。

設問３　〔API にアクセスする顧客サーバの管理〕について，(1)～(3) に答えよ。

(1) 本文中の［　サ　］～［　ソ　］に入れる適切な字句を答えよ。

(2) 本文中の下線④について，提供する API の範囲を変更する場合，変更が有効になるのは，X 社がアクセストークンを変更してから最長で何分後かを答えよ。

(3) 本文中の下線⑤について，顧客への依頼内容を，40 字以内で述べよ。

設問４　〔エッジサーバを活用する将来構想〕について，(1)～(4) に答えよ。

(1) 図 8 中の NAT ルータについて，顧客ネットワークから X システムの方向の通信におけるアドレス変換の内容を，60 字以内で具体的に述べよ。

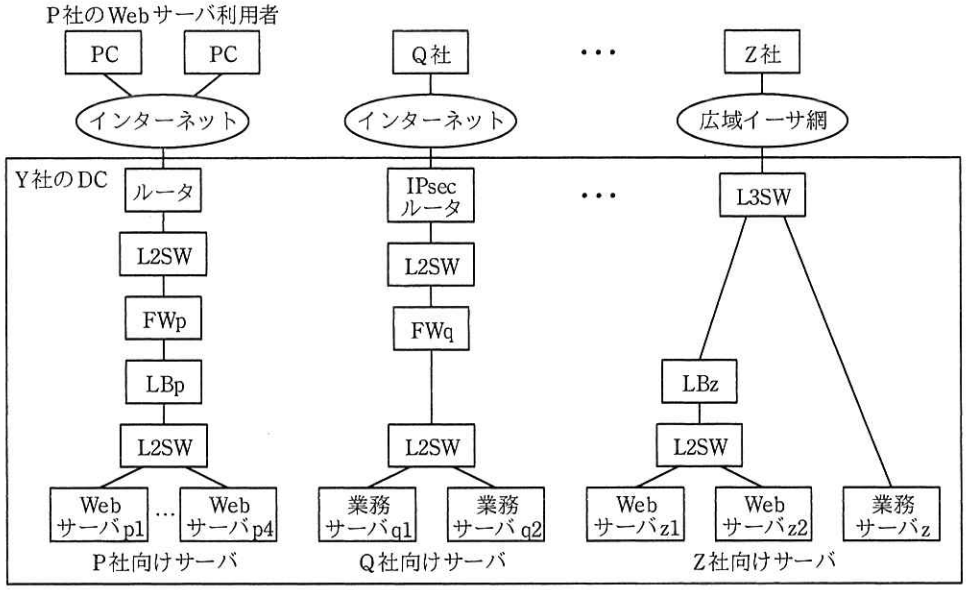
(2) 図 8 中の顧客 FW について，X システムとの接続のために，新たに許可が必要になる通信を 40 字以内で答えよ。

(3) 本文中の下線⑥について，定義するトピック名を全て答えよ。

(4) 図 7～9 中の顧客サーバを 1 台追加する場合，X システム側で必要となる対応を二つ挙げ，それぞれ 30 字以内で述べよ。

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。

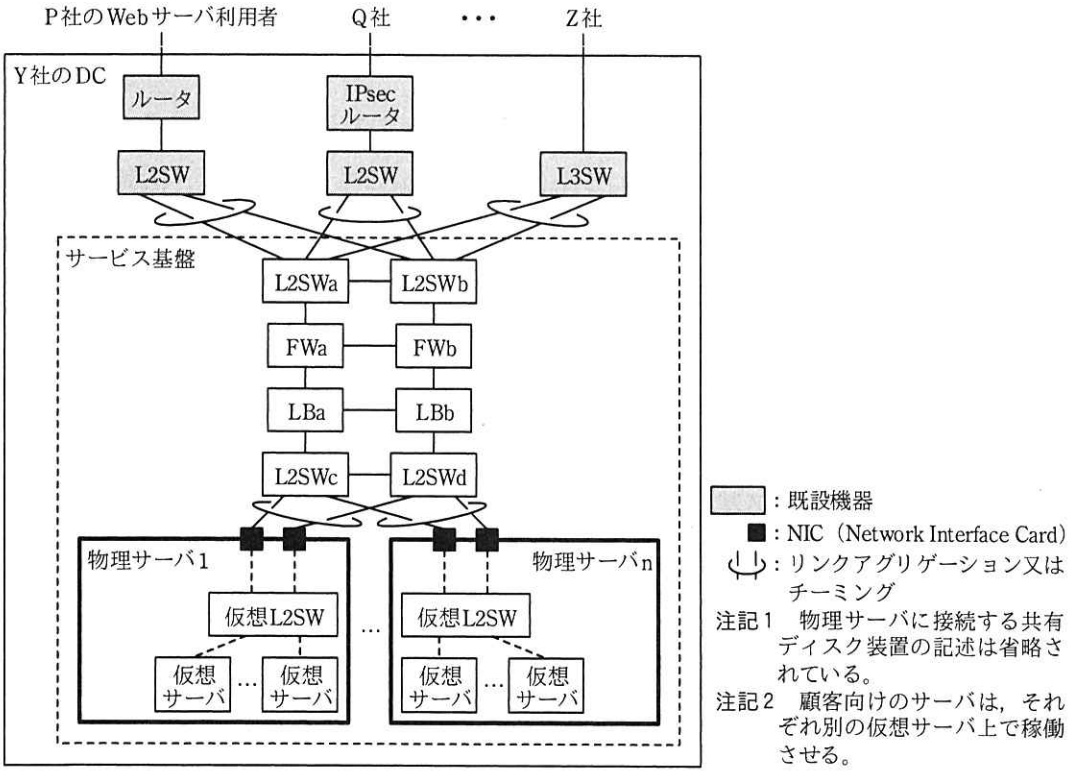


図 2　従来方式によるサービス基盤の構成案

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〕

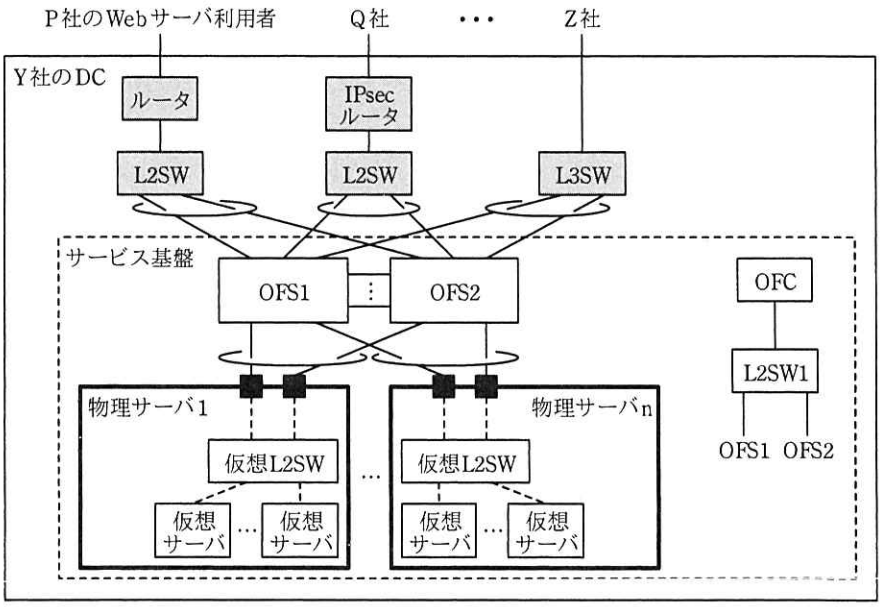
次に，Jさんは，SDN製品のベンダの協力を得て，SDN方式で構築する場合のサービス基盤の構成を検討した。

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

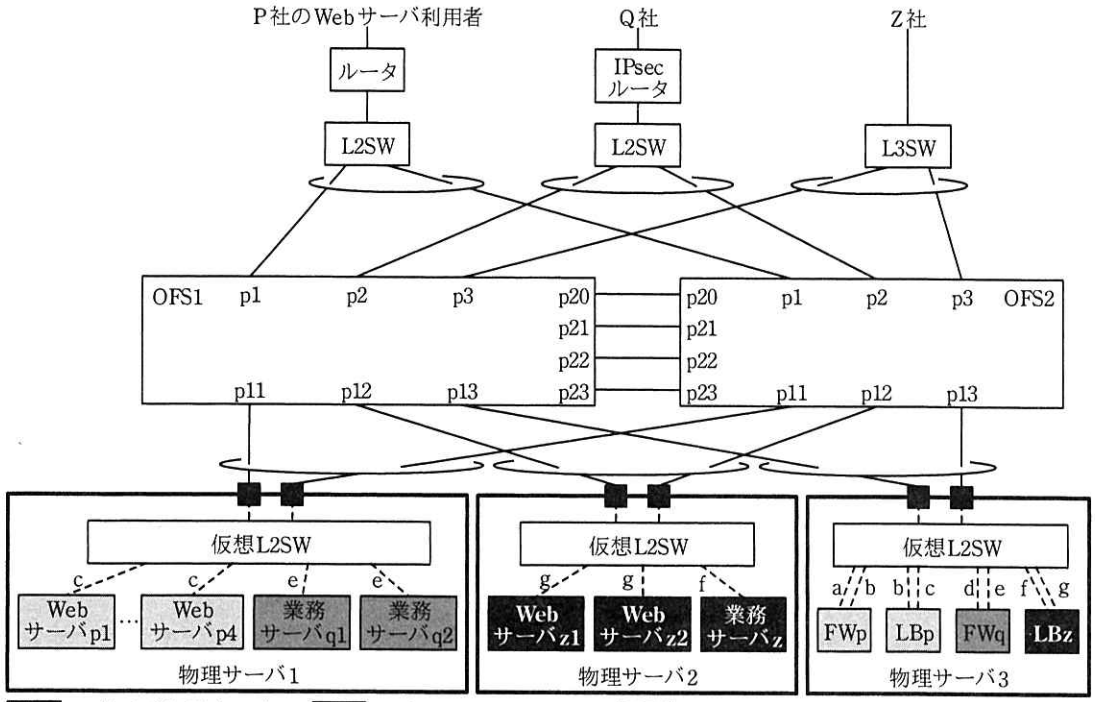
項番	比較項目	従来方式	SDN方式（図3の方式）
1	導入機器の数	多い	少ない
2	構築時の設定作業	（設問のため省略）	（設問のため省略）
3	顧客追加時の設定作業	（設問のため省略）	（設問のため省略）
4	サービス基盤の増設時の作業	（省略）	（省略）
5	必要技術の習得	習得済み	未習得

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。



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。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，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。ただし，問題冊子を切り離して利用することはできません。
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。