NW

平成25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)

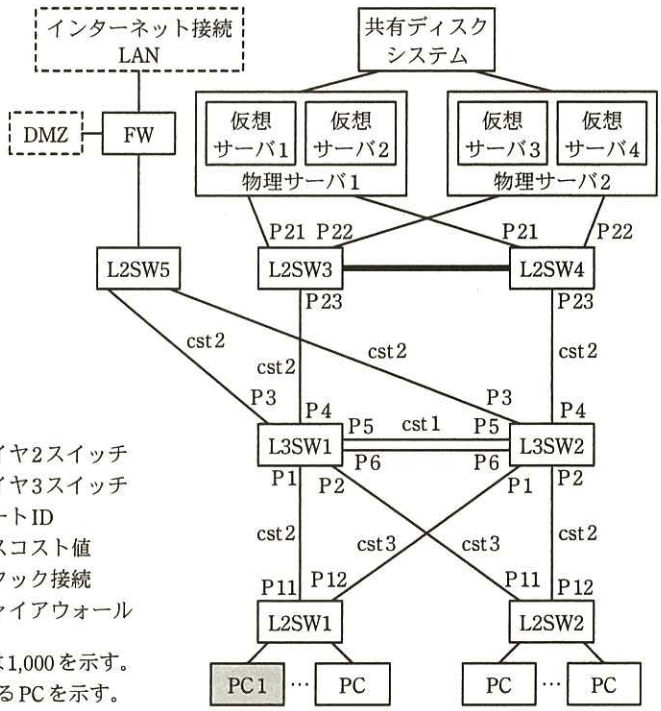
注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　無線 LAN の導入に関する次の記述を読んで，設問１～５に答えよ。

E 社は，コンピュータ関連製品の販売会社である。本社の他に複数の営業所があり，販売代理店経由で製品を販売している。本社では，販売，購買，会計などの基幹システムと，販売業務を支援する各種業務システムを運用している。これらのシステムは，複数台の物理サーバ上の仮想サーバで稼働させている。本社のネットワークシステム構成を，図１に示す。

VLANが設定されているポートと
VLAN設定内容

ポートID	VLAN ID
P1	10
P2	20
P3	120
P4，P23	100，110
P5，P6	10，20，100，110，120
P21，P22	100，110



L2SW1～L2SW5：レイヤ2スイッチ
L3SW1，L3SW2：レイヤ3スイッチ
P1～P6，P11，P12，P21～P23：ポートID
cst1～cst3：パスコスト値
：スタック接続
FW：ファイアウォール

注記1　cst1は10，cst2は100，cst3は1,000を示す。
注記2　網掛け部分は，設問で使用されるPCを示す。

図１　本社のネットワークシステム構成（抜粋）

ここ数年，E 社の売上は低迷している。そこで，E 社では競争力を強化するために，急速に発展したスマートフォンやタブレット端末などのモバイル端末（以下，MN という）を活用して，顧客の要望に即応できるような体制づくりに着手することを決めた。第１段階として，本社に MN の活用環境を構築・整備することになり，情報システム部の R 課長は，部下の S 主任に無線 LAN 導入案の検討を指示した。

S 主任は，無線 LAN 導入案の検討に先立ち，ネットワーク構成の解析訓練を兼ねて，後輩の J 君に本社のネットワーク構成，ネットワークの運用状況などの調査を指示した。

〔現状調査〕

S 主任の指示を受けた J 君は，本社のネットワークシステムの現状調査を行った。調査結果は，次のとおりである。

・現在，本社の機器には固定 IP アドレスが設定されている。利用できる基幹システムと業務システムは，部署ごとに決められている。利用制限は，二つの方法によって行われている。一つは，アプリケーションプログラムに組み込まれた認証処理によるアクセス制御である。もう一つは，図 1 中の，PC からサーバへの経路上の機器である［　ア　］に設定された，パケットフィルタリング条件の適用である。パケットフィルタリング条件は，接続を許可する PC とサーバの IP アドレスの組合せで記述されている。

・物理サーバ又は仮想サーバに障害が発生したときには，他の物理サーバで新たに仮想サーバを起動して，基幹システム，業務システムを再稼働させる。

・図 1 中の，L3SW1 及び L3SW2 の P5，P6 には，リンクアグリゲーションが設定されている。

・物理サーバの，L2SW3 と L2SW4 への接続ポートには，アクティブ／アクティブ構成のチーミング機能が設定されている。

・L2SW と L3SW では，STP（Spanning Tree Protocol）が動作している。L3SW1 をルートブリッジとするために，L3SW1 のブリッジ ID は［　イ　］の値となっている。各リンクのパスコスト値と VLAN ID は，図 1 中に記載された内容である。

・L3SW1 と L3SW2 には，VRRP で仮想ルータが設定されている。L3SW1 と L3SW2 の仮想ルータの設定内容は，表 1 のとおりである。

表 1　L3SW1 と L3SW2 の仮想ルータの設定内容

項目＼スイッチ	L3SW1					L3SW2				
	VR1	VR2	VR3	VR4	VR5	VR1	VR2	VR3	VR4	VR5
VRRP グループ ID	1	2	10	11	12	1	2	10	11	12
仮想 IP アドレス	VIP1	VIP2	VIP3	VIP4	VIP5	VIP1	VIP2	VIP3	VIP4	VIP5
Priority 値	200	100	200	100	200	100	200	100	200	100
所属 VLAN ID	10	20	100	110	120	10	20	100	110	120

注記　VR1 ～ VR5 は，仮想ルータ名を示す。

・L2SW1 に接続された PC のデフォルトゲートウェイには VIP1 が，L2SW2 に接続された PC のデフォルトゲートウェイには VIP2 が設定されている。また，仮想サーバ

1と仮想サーバ2のデフォルトゲートウェイにはVIP3が，仮想サーバ3と仮想サーバ4のデフォルトゲートウェイにはVIP4が設定されている。これらの設定によって，仮想ルータの負荷分散が行われている。

J君は，調査結果を整理し，S主任に報告した。現状のネットワーク構成の解析ができたので，S主任は，MNでネットワークシステムを利用するための，無線LANの導入方法を検討することにした。さらに，無線LANの導入では，社内の電波状態を調査するサイトサーベイも必要と考え，サイトサーベイで実施すべき内容についても併せて検討するよう，J君に指示した。

〔無線LANの調査と導入検討〕

J君は，まず，無線LANの特徴とセキュリティ上の問題点を調査した。

無線LANの最初の標準規格IEEE［ウ］は，物理レイヤとMACレイヤの規格で構成され，その規格中には，次に示す認証と暗号化方式が標準化されている。

(1) 認証

① オープンシステム認証

本認証は，アクセスポイント（以下，APという）での端末認証が，実質的には行われない。

② 共有鍵認証

本認証は，MNが，APと共有するWEPキーを使用して，APから受信した乱数を［エ］して返送する，チャレンジレスポンス方式で行われる。ただし，WEPキーが，電波を不正に傍受している装置に見破られると，（あ）不正アクセス以外にも重大なセキュリティリスクが発生するので，この認証方式は，一般に利用されない。

(2) 暗号化方式

方式としてWEPが規定されている。WEPは，［オ］と呼ばれる暗号アルゴリズムを基にした共通鍵暗号を採用している。暗号化には，WEPキーと呼ばれる共通鍵が使用される。MNとAPには，同じWEPキーを設定する必要があり，動的に鍵の変更が行われないことから，解読される危険性が高い。

以上の，IEEE［ウ］のセキュリティ上の問題点を解決するために，IEEE

802.11i が規格化された。IEEE 802.11i を基に策定された WPA2（Wi-Fi Protected Access 2）では，セキュリティ面の改善の他に，（い）事前認証及び認証キーの保持（Pairwise Master Key キャッシュ）を行う方法が規定されているので，接続先の AP を切り替える時間を短縮することが可能になった。

無線 LAN において，MN が異なる AP 間を渡り歩けるような機能のことを，ローミングという。ローミングのためには，ローミングの対象となる全ての AP について，ネットワークの識別子である［　カ　］が同じである必要がある。MN が接続先の AP を切り替えるときには，新たな接続先となる AP との間で，論理的接続であるアソシエーション，認証処理などが行われる。

IEEE 802.1X 認証を行った場合の，無線 LAN への接続手順を，図 2 に示す。

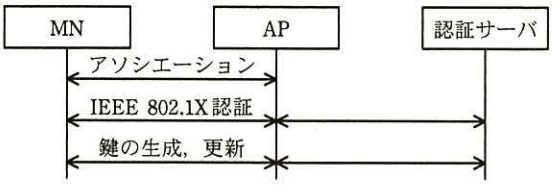
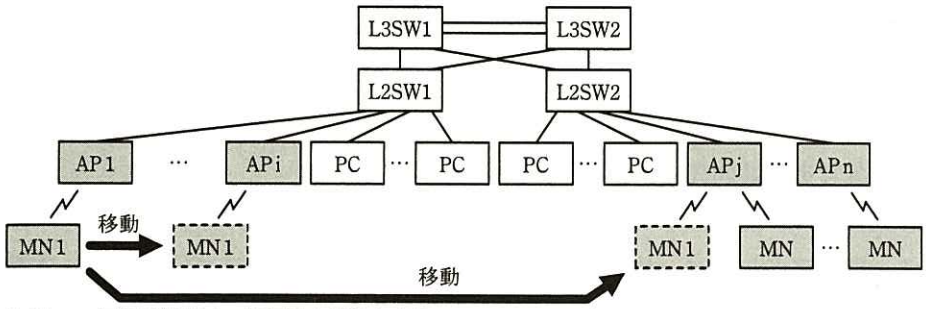


図 2　無線 LAN への接続手順

調査結果を基に，J 君は，導入する無線 LAN には WPA2 を利用し，認証には，IEEE 802.1X で利用可能な方式のうち，運用が容易な PEAP を採用することにした。

次に，J 君は，図 1 のネットワークシステムに，無線 LAN を導入する構成を検討した。J 君がまとめた，AP の導入構成案を，図 3 に示す。



注記 1　網掛け部分は，新規導入機器を示す。
注記 2　本図では，図 1 中の L3SW1 と L3SW2 から下側を示した。

図 3　AP の導入構成案（抜粋）

新規に導入する MN でも，現状と同等のセキュリティ対策が行われるように，MN には，部署ごとに割り当てられた固定 IP アドレスを設定したい。しかし，その場合，E 社の構成では次のような問題が発生する。図 3 において，AP1 と接続していた MN1 が移動して，図 2 の手順で AP i に接続したとき，MN1 は通信を継続できるが，AP j に接続すると，（う）サーバやインターネットとの通信ができなくなってしまう。

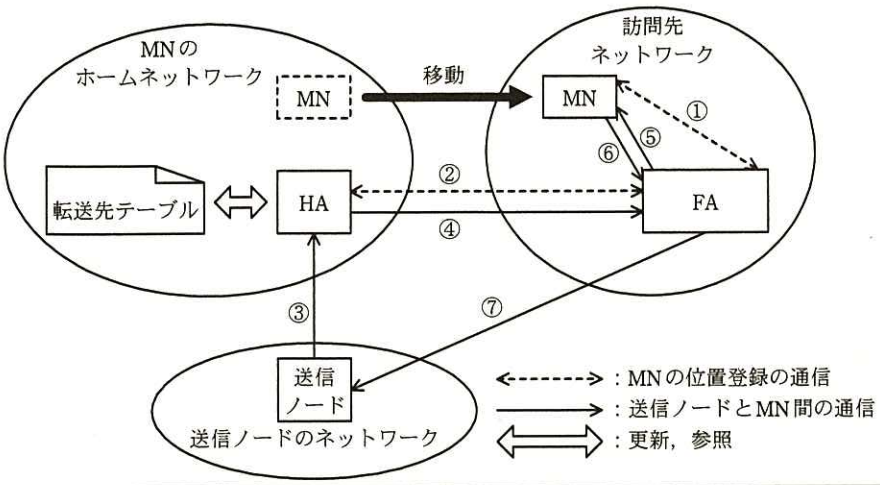
J 君は，この問題の対応策について S 主任に相談した。S 主任は，AP を集中管理・集中制御する無線 LAN コントローラ（以下，WLC という）を導入すれば，問題を解決できるのではないかと考え，WLC の調査を指示した。

〔サブネット間のローミングの調査と設計〕

指示を受けた J 君は，WLC について調査した。調査結果は，次のとおりである。

WLC は，AP と連携して認証，暗号化，電波出力調整，ローミングなどの機能を実現する。WLC の実装は，ベンダによって異なっている。ベンダ Y 社の WLC を導入すると，サブネット間のローミングが可能になることが分かった。Y 社の WLC は，RFC 2002 で基本動作の仕組みが定義されているモバイル IP 技術を基にして，これに Y 社独自の工夫を加えて，無線 LAN におけるローミングを可能にしている。そこで，J 君は，基になっている RFC 2002 のモバイル IP について調査した。調査結果は，次のとおりである。

・モバイル IP は，MN が異なるサブネットに移動しても，MN との通信を試みるホスト（以下，送信ノードという）が MN と通信できるようにする技術である。
・モバイル IPv4 では，MN と送信ノード間の通信を仲介する，home agent（以下，HA という）と foreign agent（以下，FA という）が存在する。
・MN が本来稼働すべきネットワークを，ホームネットワークという。MN には，ホームネットワークでホームアドレスと呼ばれる IP アドレスが付与されている。
・HA は，MN のホームネットワークに設置されている。それに対して FA は，MN の移動先である訪問先ネットワークに設置されている。
・移動先の MN にパケットを渡すための転送先 IP アドレスは，気付アドレスと呼ばれる。気付アドレスは，訪問先ネットワークに設置された FA の IP アドレスでもある。
・HA と FA を経由した MN の位置登録の通信手順及び送信ノードと MN 間の通信手順は，図 4 のとおりである。



【MN の位置登録の通信手順】

① MN は，FA から送出される Advertisement メッセージを受信し，ホームネットワークにいるのか，訪問先ネットワークにいるのかを判別する。訪問先ネットワークへの移動を検出すると，Advertisement メッセージの中から気付アドレスを取得し，MN 自体のホームアドレスと気付アドレスを対応付けて，位置登録の要求を行う。

② FA は，MN から受信した位置登録情報を，MN のホームネットワークの HA 宛てに送信する。HA は，MN の気付アドレスとホームアドレスを対にして，転送先テーブルに登録する。登録後，登録完了メッセージを FA 宛てに送信する。

【送信ノードと MN 間の通信手順】

③ 送信ノードから送信された MN 宛てのパケットが，MN のホームネットワークに到達すると，（え）HA によって代理受信される。

④ HA は，転送先テーブルを参照して移動中の MN の気付アドレスを取得し，受信したパケットをカプセル化して，気付アドレス宛てに転送する。

⑤ FA は，受信したパケットのカプセル化を解除して，MN に送信する。

⑥ MN のデフォルトゲートウェイに FA が設定されている場合は，MN が送信ノード宛ての返送パケットを，デフォルトゲートウェイである FA 宛てに送信する。

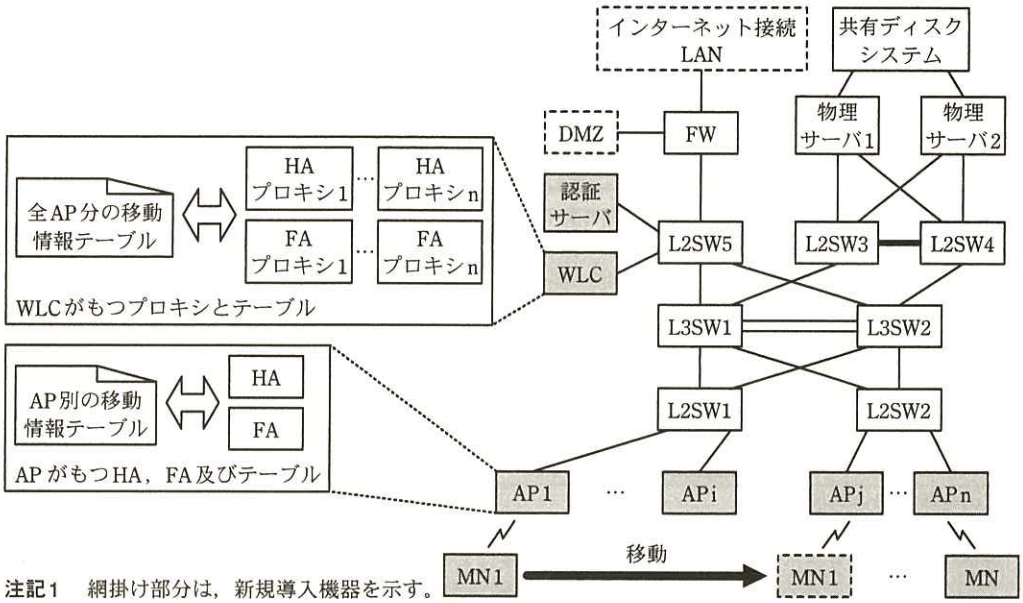
⑦ FA は，受信したパケットを送信ノードに中継する。

図 4　HA と FA を経由した MN の位置登録の通信手順及び送信ノードと MN 間の通信手順

図 4 に示されているように，RFC 2002 の MN にはモバイル IP 機能の実装が必要である。

E 社が想定する MN にはモバイル IP 機能がない。しかし，Y 社の WLC には，モバイル IP 機能が実装されていない MN でも，サブネット間のローミングができるような工夫が施されている。

Y 社の資料を参考に，J 君は，WLC と AP を導入するときの構成を，図 5 のように設計した。また，モバイル IP に関連して WLC と AP がもつ機能の名称と機能の概要を整理し，表 2 を作成した。



注記1　網掛け部分は，新規導入機器を示す。
注記2　HAプロキシは，HAの代理として，WLC内でHAの機能の一部を担う。
注記3　FAプロキシは，FAの代理として，WLC内でFAの機能の一部を担う。

図5　WLCとAPを導入するときの構成（抜粋）

表2　モバイルIPに関連してWLCとAPがもつ機能の名称と機能の概要

機器名	機能の名称	機能の概要
AP	HA	MNのホームネットワークに送信されたMN宛てのパケットを受信し，AP別の移動情報テーブルで調べ，そのMNが移動中のときは，受信したパケットをカプセル化してWLCのFAプロキシに送信する。
	FA	① 無線LAN側で受信したパケットの送信元IPアドレスが，当該FAが稼働するAPのサブネットと異なるサブネットのもののときは，保持する経路情報に基づいて，受信したパケットを中継処理する。 ② WLCから送信されたパケットを受信したときは，受信したパケットのカプセル化を解除して，MNに送信する。
WLC	（各APの）HAプロキシ	MNの認証時に，MNとMNのホームネットワークの情報，又はMNの訪問先ネットワークに関連する情報を，WLCが保持する全AP分の移動情報テーブルに登録するとともに，登録情報を該当するAPのHAに送信する。
	（各APの）FAプロキシ	HAから送信された移動中のMN宛てのパケットを受信し，カプセル化を解除して，移動情報テーブルから移動先のAPを判別した後，再度カプセル化してパケットを移動先のAPのFAに送信する。

図5に示したように，Y社のAPはHAとFAをもち，WLCはHAプロキシとFAプロキシをもつ。

MNがAPと接続するときに行われるIEEE 802.1Xの認証では，WLCがオーセンテ

ィケータとして働く。MN の認証時に，WLC で稼働する HA プロキシが MN の移動状態を把握して，移動情報テーブルに位置情報を登録する。この処理で，モバイル IP 機能をもたない MN でも，移動状態が管理され，サブネット間のローミングを可能にしている。

図 5 において，MN1 が AP1 と接続するときには，MN1 と WLC 間で認証処理が行われる。このとき，表 2 に示したように，HA プロキシが，認証時のパケットの情報を基に，全 AP 分の移動情報テーブル中に MN1 に関する位置情報を登録する。登録された情報は，MN1 のホームネットワークの AP1 の HA に送信される。

図 5 中の AP1 に接続していた MN1 が，インターネットを経由して社外と通信中に APj に移動したときの MN1 に関連する通信の内容は，図 6 のようになる。

(i) MN1 は，移動後に APj への接続処理を行う。そのとき，MN1 と WLC 間で認証処理が行われる。
(ii) WLC の [a] は，移動情報テーブルの MN1 に関する位置情報を更新し，更新内容を MN1 のホームネットワークの AP1 の HA に送信する。
(iii) MN1 は APj と接続した後，インターネット経由の社外宛てパケットを APj に送信する。
(iv) AP j の [b] は，受信したパケットの送信元 IP アドレスと宛先 IP アドレスが，AP j のサブネットとは異なるサブネットのものなので，受信したパケットを L3SW に送信する。
(v) 社外から，インターネット経由で MN1 宛てに送信された応答パケットが，MN1 のホームネットワークに到達し，AP1 が受信する。
(vi) AP1 の [c] は，宛先の MN1 が移動中であることを，移動情報テーブルを参照して知り，受信したパケットをカプセル化して WLC に送信する。
(vii) WLC の [d] は，受信したパケットのカプセル化を解除し，宛先 IP アドレスから MN1 宛てであることを知る。このとき，移動情報テーブルを参照すると，MN1 は AP j のサブネットに移動中なので，再度パケットをカプセル化して APj に送信する。
(viii) APj の [e] は，受信したパケットのカプセル化を解除して，MN1 にパケットを送信する。
(以下，省略)

図 6　MN1 が APj に移動したときの MN1 に関連する通信の内容

J 君は，無線 LAN の導入方法の検討が完了したので，次に，サイトサーベイの検討を行った。

〔サイトサーベイの検討〕

J 君は，無線 LAN 導入に当たって留意すべき事項を調査し，その結果，サイトサーベイの実施について，次のように進めた。

本社は，テナントビルに入居し，隣接した複数のフロアを使用している。各フロア

のオフィスは，壁やパーティションなどで分割されている。本社のオフィスに複数のAP を導入するとき，サイトサーベイを実施しないと，（お）(a) 導入後に通信できないエリアが発生する，(b) 他社の無線 LAN の影響を受ける，(c) 期待どおりの通信速度が得られない，などの問題が発生する可能性が高い。この問題を防ぐためには，専用機材を用いて，AP から送出される電波の伝搬状態及び電波干渉の発生源を十分に把握しておくことが重要である。

AP から送出される電波の伝搬状態を把握していないと，AP の最適な場所への設置，適切な電波強度の設定ができない。電波状態の調査には専門的なノウハウが必要であることから，J 君は，サイトサーベイは，専門業者に委託するのがよいと判断し，調査・検討の結果を，S 主任に報告した。

S 主任と J 君は，これまでの検討を基に設計した無線 LAN 導入構成及びサイトサーベイの実施方法を，R 課長に報告した。説明を受けた R 課長は，設計内容及びサイトサーベイの実施方法に問題がないことを確認できたので，無線 LAN の導入を進めることにした。

設問 1　本文中の［　ア　］～［　カ　］に入れる適切な字句を答えよ。

設問 2　〔現状調査〕について，(1) ～ (5) に答えよ。

(1) 図 1 において，L3SW1 の P5 と L3SW1 の P6 の組，及び L3SW2 の P5 と L3SW2 の P6 の組以外に，リンクアグリゲーションが 2 組設定されている。その組を，それぞれ図 1 中の機器名，ポート ID で答えよ。

(2) 表 1 中の仮想ルータ VR1 がマスタルータとなるスイッチ名を，図 1 中の機器名で答えよ。

(3) L2SW2 と L3SW1 間の経路において，L2SW2 の P11 がブロッキングポートになる。その理由を，STP の経路計算アルゴリズムを基に，図 1 を参照して，40 字以内で述べよ。

(4) L3SW1，L3SW2，L2SW3 及び L2SW4 の間を接続する経路のブロッキングポートを，図 1 中の機器名とポート ID で答えよ。

(5) 図 1 中の PC1 と仮想サーバ 3 間のフレーム転送経路を，次の【転送経路】に示す。(A)，(B) に入れる適切な機器名を，【転送経路】の表記方法に従い，経由する順に列挙せよ。

【転送経路】

PC1 → [　　(A)　　] → L2SW3 及び L2SW4 → 仮想サーバ 3

仮想サーバ 3 → L2SW3 及び L2SW4 → [　　(B)　　] → PC1

設問 3　〔無線 LAN の調査と導入検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線（あ）のセキュリティリスクの内容を，25 字以内で述べよ。

(2) 本文中の下線（い）によって，ローミング時間が短縮される。その理由を，図 2 の手順を参考にして，25 字以内で述べよ。

(3) 本文中の下線（う）が発生する理由を，MN1 に設定されているネットワーク情報が変更されないことに着目して，35 字以内で述べよ。

設問 4　〔サブネット間のローミングの調査と設計〕について，(1) ～ (4) に答えよ。

(1) 図 4 中の ① で，FA から送信される Advertisement メッセージには，IP ヘッダが付加される。この IP ヘッダの宛先 IP アドレスの種類を答えよ。

(2) 図 4 中の ② で，転送先テーブルを更新した後，HA は，サブネット内のホスト宛てに，ある通信を行う。その通信プロトコルの名称を答え，その目的を，40 字以内で述べよ。

(3) 図 4 中の下線（え）のために，MN 宛ての ARP 要求に対して HA が行う処理の内容を，20 字以内で述べよ。

(4) 図 6 中の [　a　] ～ [　e　] に入れる適切な字句を，表 2 中の機能の名称で答えよ。

設問 5　〔サイトサーベイの検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線（お）の問題が発生するのを避けるために，サイトサーベイで調査すべき電波の状態を二つ挙げ，それぞれ 25 字以内で答えよ。

(2) サイトサーベイの調査結果を基に，導入作業前に確定すべき設計項目を二つ挙げ，それぞれ 15 字以内で答えよ。

(3) 無線 LAN を設置した後，ping コマンドによる接続確認テストの他に，MN を使用して実施すべきテストを二つ挙げ，それぞれ 25 字以内で答えよ。

問2　開発システムの再構築に関する次の記述を読んで，設問1～3に答えよ。

IT関連会社のF社とG社は，両社の強みを生かして合併することになった。両社とも，複数の開発部門で各種の製品やシステムを開発している。開発のため，各開発部門は，独自に開発・評価用システム（以下，開発システムという）を構築している。その結果，全社的に見て，サーバ，ストレージ及びネットワークを十分に有効活用できていなかった。

そこで，F社とG社では，合併を機に，情報システム部門が開発システムを一括管理し，利用者である開発部門にITプラットフォームを提供するという形態の新システムに移行することになった。新システムへの移行に伴い，情報システム部門のK主任とT君は，新システムを実現する基盤ネットワークの構築担当になった。

〔新システムへの移行方針と移行後の開発システムの構成〕

K主任は，新システムの検討に当たって，次のような移行方針で進めることにした。

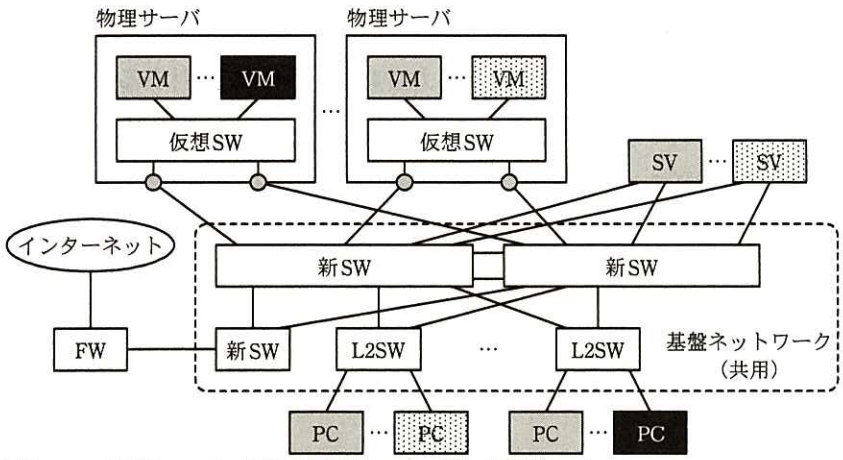
(1) サーバを仮想環境に移行することで，新たなサーバ増設要求への対応時間の短縮及び必要に応じた柔軟な構成の変更を実現する。ただし，移行当初は，既設サーバをそのまま活用する。

(2) PCを収容するレイヤ2スイッチは，コスト削減のために，できるだけ既設のものを流用する。

(3) 利便性向上のために，開発部門のPCは，社内のどこからでも所属部門の開発システムに接続できるようにする。

(4) 各開発部門は，これまで独自に開発システムを運用していたので，各開発・評価用ネットワーク（以下，開発ネットワークという）間でIPアドレスの重複があるが，再設定をせずに新システムに移行できるようにする。

K主任から移行後の開発システムについて検討するよう指示されたT君は，図1に示すような移行後の構成（概要）を考えた。図1中の，異なる網掛けのサーバとPCは，それぞれ別の開発部門に属しているが，新規に導入するスイッチによって物理ネットワークの共用化を目指している。



FW：ファイアウォール　VM：仮想サーバ　SV：既設サーバ
L2SW：レイヤ2スイッチ（主に既設流用）　新SW：新設スイッチ　仮想SW：仮想スイッチ
○：仮想SWの外部接続インタフェースとなる物理サーバのNIC
注記　異なる網掛けのサーバとPCは，それぞれ別の開発部門に属していることを示す。

図1　移行後の開発システムの構成（概要）

〔ネットワーク仮想化技術の調査〕

新システムを実現するためには，各開発部門が独自に構築したネットワークを，一つの物理ネットワークに収容する必要がある。そこで，K 主任は，物理ネットワークに依存しない，開発部門ごとの論理的なネットワーク（以下，テナントネットワークという）を構築することにし，T 君にネットワーク仮想化技術の調査を指示した。

T 君が調査したところ，大別して二つの新しい技術があることが分かった。

一つは，オーバレイ方式と呼ばれるネットワーク仮想化方式で，レイヤ 3 ネットワーク上にレイヤ 2 をカプセル化して，同一テナントネットワークに属するサーバ間の接続用トンネルを作ることによって，ネットワーク仮想化を実現する。

もう一つは，スイッチを，経路制御などの管理機能を実行するフローコントローラ（以下，OFC という）と，データ転送を行うフロースイッチ（以下，OFS という）に分け，OFS に入るパケットの経路制御を OFC が集中制御する方式（以下，OF 方式という）である。OF 方式は，カプセル化を使わず，OFS それぞれの転送によって実現されることから，ホップバイホップ方式と呼ばれることもある。

オーバレイ方式又は OF 方式で実現されたネットワークは，どちらもソフトウェアで定義できることから，［　a　］と呼ばれている。

OF 方式では，OFS に入ってきたパケットの MAC アドレス，IP アドレス，TCP ポ

ート番号などの属性の組合せを“フロー”と呼び，そのパケットをどのように処理するかの判定に使用する。フローを識別し，入力されたパケットに対する処理を，OFS内のフローテーブル（以下，f-TBLという）に設定する。OF方式でのOFCとOFSの構成を，図2に示す。OFCとOFS間の制御情報（以下，メッセージという）の交換のプロトコルを，OF Protocolと呼ぶ。

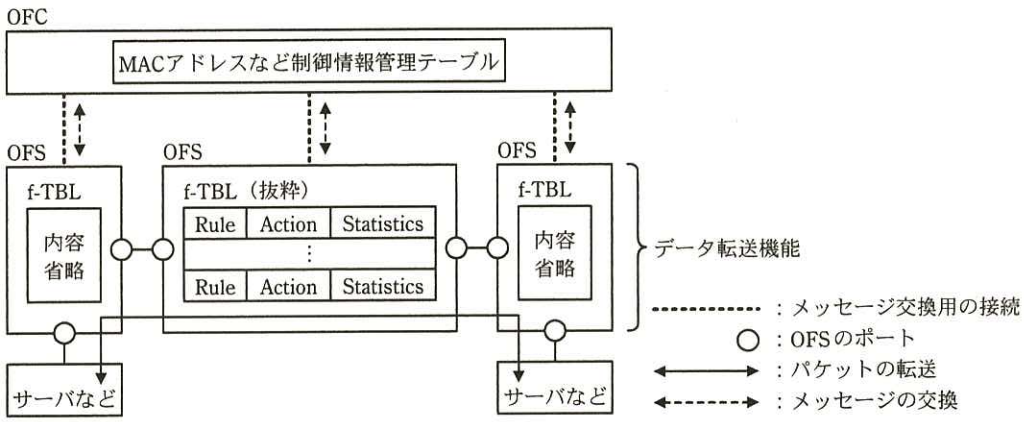


図2　OF方式でのOFCとOFSの構成

図2中のf-TBLの一つのエントリには，フローの識別情報（以下，Ruleという）を保持するRuleフィールド，Ruleに一致したフローをもつパケットに対する処理内容（以下，Actionという）を記述したActionフィールド，一致したフローのカウント値を保持するStatisticsフィールドなどがある。RuleとActionは，OFCが設定する。Ruleとして利用できる情報，Action及びメッセージの例を，表1に示す。

表1　Ruleとして利用できる情報，Action及びメッセージの例（抜粋）

Ruleとして利用できる情報例

レイヤ	内容
L1	受信物理ポート番号
L2	宛先／送信元MACアドレス
	イーサネットタイプ
	VLAN ID／VLAN Priority
L3	送信元／宛先IPアドレス
	IPプロトコル種別／ToS値
L4	送信元／宛先ポート番号

Action例

名称	意味
Output	パケットを指定物理ポートやOFCに転送する。
Drop	パケットを破棄する。
Set-Field	パケットの指定フィールドを書き換える。

メッセージ例

名称	用途
Packet In	OFSが，受信したパケットと関連情報をOFCに送信する。
Packet Out	OFCが，パケットとポート指定情報を送り，OFSからパケットを送信させる。
Flow Mod	OFCが，f-TBLの内容の登録・更新をOFSに指示する。

なお，ネットワークに参加する OFS は最初に必ず OFC に接続し，OFS のポート情報などを OFC に通知する。OFC は，OF Protocol を使ってトポロジを把握する。

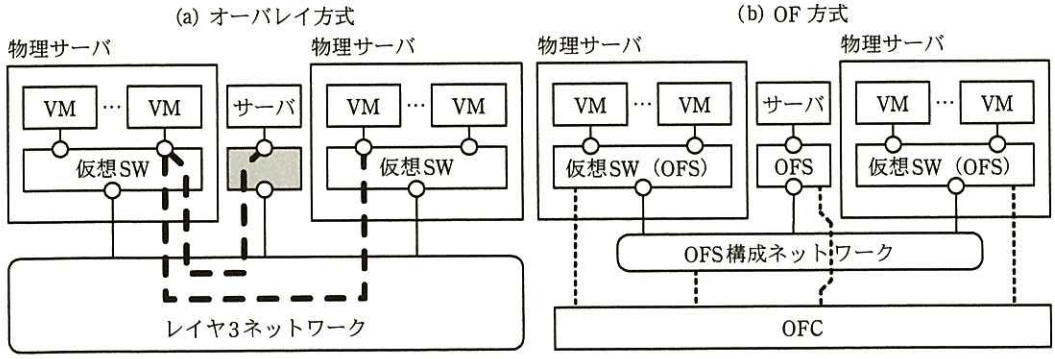
フローに対し，f-TBL 内に Rule が一致するエントリがあった場合，OFS は当該エントリに記述された Action の動作を行う。一方，なかった場合は，OFS は Packet In メッセージを OFC に送信し，そのパケットの処理方法を問い合わせるモードで動作する。Packet In を受信した OFC は，Flow Mod メッセージを使用して f-TBL に処理のエントリを登録したり，Packet Out メッセージを使用して指定ポートからのパケット送信を OFS に指示したりする。f-TBL 内の Rule 及び Action 内容の例を，表 2 に示す。

表 2　f-TBL 内の Rule 及び Action 内容の例

機能例	Rule 内容	Action 内容
転送	宛先 MAC アドレスが aaa のとき	物理ポート n から受信パケットを送信する。
パケット書換え	宛先 IP アドレスが bbb のとき	宛先 MAC アドレスを，指定した MAC アドレスに書き換え，指定物理ポートから送信する。

表 2 中に示した機能のうち，転送機能はネットワーク機器の［　b　］としての機能を実現するために使われる。また，パケット書換え機能は［　c　］としての機能を実現するために使われる。

K 主任から，これまで調べた二つの仮想化方式の違いを説明するように指示された T 君は，ネットワーク仮想化方式の説明図を図 3 に，オーバレイ方式と OF 方式の比較を表 3 にまとめた。OF 方式では，仮想 SW も OFS として動作する。



注 1)　通信には，OFSによるネットワークと独立した管理用LANを使用する。

図 3　ネットワーク仮想化方式の説明図

表3　オーバレイ方式とOF方式の比較

比較項目＼仮想化方式		オーバレイ方式	OF方式	（参考）VLAN方式
仕様	仮想ネットワーク数	約1,677万[1)]	使用する装置の仕様に依存	4,094
	転送用ヘッダの追加	50又は54バイト[1)]	0バイト	4バイト
運用	既設ネットワーク再利用性	高い	低い	
	QoS制御	コアのL3ネットワークに依存	柔軟な制御が可能	
	経路制御	コアのL3ネットワークに依存	柔軟な制御が可能	

注[1)]　VXLAN（Virtual eXtensible Local Area Network）の場合

次は，表3に関するK主任とT君の会話である。

K主任：技術の動向としては，どういうところがポイントなのかな。

T君　：そうですね。集中管理によるネットワークの運用性の改善や帯域の有効利用を目指した技術の開発が進んでいるといったところです。

K主任：オーバレイ方式は既設ネットワークの再利用性が高いが，既設サーバの接続や拠点間接続がある場合には，何か対応が必要ではないのか。

T君　：既設サーバの接続では，図3中のサーバ接続用スイッチに［　ア　］する機能が必要になりますし，拠点間の接続では［　イ　］への対応が必要となる可能性があります。

K主任：既存システムでは老朽化した機器も多いし，合併を機にシステムも刷新したいから，OF方式を取り入れた新システムを開発できるかどうか検討してくれないか。

T君　：分かりました。

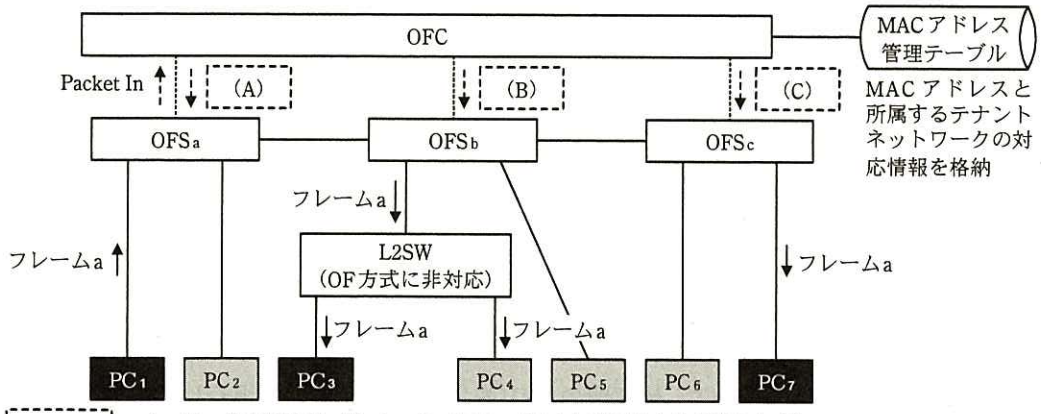
〔テナントネットワーク実現性の検討〕

新システムの検討に先立ち，T君は，共用する物理ネットワーク内の，テナントネットワークの実現性について検討することにした。

OF方式では，基本的にレイヤ2でネットワークを構成するので，レイヤ2で接続機器を識別するMACアドレスと，接続機器がどのテナントネットワークに属するかを識別するテナントネットワーク識別情報（以下，テナントIDという）は，全て，OFC側で集中管理される。また，OFSのポートに，どのテナントネットワークに属する機器が接続されるかも，OFC側で集中管理される。この前提を基に，ブロードキャストとユニキャストについて，どのようにフレーム転送を制御すればよいかを検討し

た。

T 君が作成した，テナントネットワーク実現のための OFC と OFS の動作説明図を図 4 に示す。



注記 1　2 種類の濃淡によって区別された PC は，それぞれ異なるテナントネットワークに属していることを示す。
注記 2　フレーム a は，ARP 要求転送用のフレームを示す。

図 4　テナントネットワーク実現のための OFC と OFS の動作説明図

T 君は，ARP によるアドレス解決がされていれば，ユニキャストのフレーム転送では，送信端末がどのテナントネットワークに属しているかを判断することなく，宛先 MAC アドレスをもつ端末に向けてフレームを中継していくという単純な実装ができると考えた。①図 4 中の PC_1 から PC_7 へユニキャストフレームを転送する場合について，f-TBL に一致する Rule がなかった場合の処理を，T 君は次のように考えた。“OFC は中継する OFS に対して宛先 MAC アドレスをもつ機器までの Rule と Action を f-TBL に設定し，転送を指示すればよい。”

一方，ARP や DHCP といったブロードキャストフレームの転送では，送信端末の属するテナントネットワークに限定してフレームを送出する必要がある。例えば，②図 4 中の PC_1 が，所属するテナントネットワークの PC_7 にパケットを送信するために，ARP 要求を送信した場合について，T 君は次のように考えた。“機器の MAC アドレスと所属するテナントネットワークの対応情報は，OFC にあらかじめ登録されている。その情報を使って，OFC から，同一テナントネットワークに属する機器が接続されているポートをもつ OFS に対し，直接ブロードキャストフレーム（複製）の送信を指示

すればよい。”

しかし，OF 方式に非対応の L2SW が図 4 のように接続されている場合には，③T 君が考えた単純な方式で PC_1 からの ARP 要求を処理しようとすると，問題が発生する可能性がある。このため，OF 方式に非対応の L2SW に，異なるテナントネットワークに属する PC を同時に接続することはできない。

〔テナントネットワークへの PC 接続方式の検討〕

T 君は，OFC と OFS で構成された基盤ネットワーク上のテナントネットワークに PC を接続する方式について，次のように考えた。

・開発部門の PC は，社内各所に用意された自部門の接続用ポートを利用して，所属部門の開発システムに接続できるようにする。
・ある部門の接続用ポートに，他部門の PC を接続しようとした場合には，通信できないようにする。
・これまでと同様に，テナントネットワーク内の IP アドレスの管理は，開発システム側の事情に配慮し，各利用部門に任せる。

ネットワークに接続される機器の MAC アドレスは，テナントネットワーク実現のために，OFC で参照できるように登録管理されている。そこで，T 君は，④各テナントネットワークとそれに属する機器の MAC アドレスの一覧表を使えば，PC の OFS への接続可否制御が可能になると考えた。

さらに，T 君は，今後，無線 LAN 経由の接続が必要になった場合や，よりセキュリティの高い認証方式の採用が必要になった場合でも，OF 方式で対応が可能かどうかを評価することにした。この目的で，IEEE 802.1X の認証方式を選び，OF 方式のネットワークとの組合せについて評価することにした。T 君がまとめた IEEE 802.1X 認証方式の概要を，表 4 に示す。表 4 には，OF 方式に非対応の L2SW を使用した中継スイッチ（以下，中継 SW という）を経由した複数 PC の接続についても示している。

表 4　IEEE 802.1X 認証方式の概要

No.	比較項目	IEEE 802.1X 認証	
		ポートベース認証	MAC ベース認証
1	利用者認証	可能	不可
2	機器認証	可能	可能
3	中継 SW 経由の接続可否	可能	可能
4	中継 SW の要件		
5	中継 SW を介した同一ポートへの複数 PC 接続	セキュリティ問題あり	可能
6	EAPOL-Start [1] 対応要否	必要	必要

注記　表中の網掛けの部分は，設問の都合上表示していない。
注 [1]　PC 側から認証を開始する機能

中継 SW を用いて接続する場合を含め，IEEE 802.1X 対応認証 SW への PC の接続形態を，図 5 のようにまとめた。

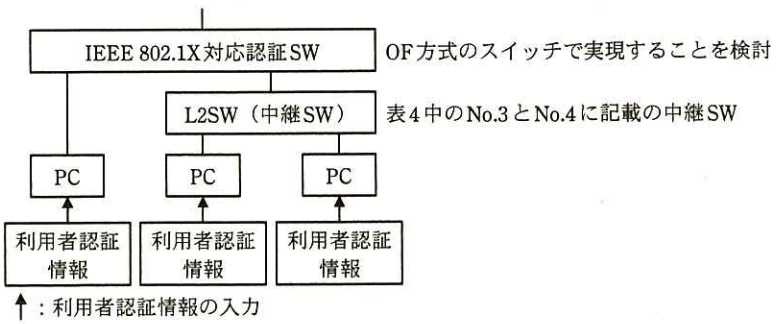


図 5　IEEE 802.1X 対応認証 SW への PC の接続形態

既設スイッチを活用して，PC を OFS に接続したいと考えている T 君は，表 4 に示された No.3～6 の中継 SW を使用した場合について詳細に検討することにした。

⑤ 同一テナントネットワークに属する PC を中継 SW を経由して複数台接続する場合，中継 SW は，表 4 中の No.4 の要件を満たす必要がある。既設 SW について，この要件を満たすかどうかを調査したところ，満たさないものがあることが分かった。しかし，それらを入れ替えた場合でも，費用への影響は少ないと考えられた。一方，⑥ ポートベース認証を使用した場合は，表 4 中の No.5 のセキュリティ問題が発生する。しかし，OF 方式では，この問題への対処が容易なことが分かった。

IEEE 802.1X 認証方式による PC のテナントネットワークへの接続シーケンス例を，図 6 に示す。

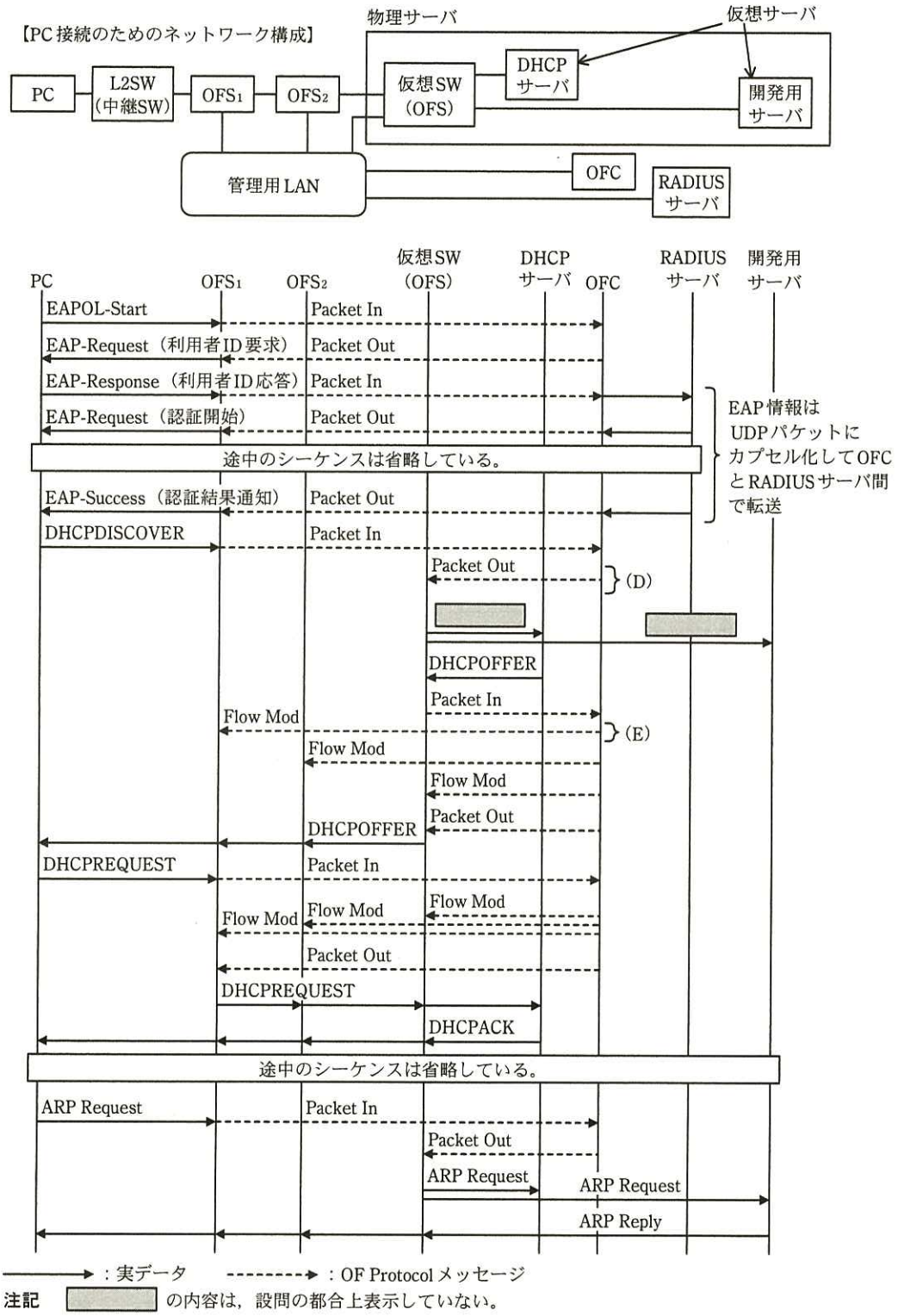


図6　IEEE 802.1X 認証方式による PC のテナントネットワークへの接続シーケンス例（概要）

図 6 中の管理用 LAN は，図 3 に示した OFC と OFS 間のメッセージ交換用及び RADIUS サーバと OFC 間の通信に使われる専用の LAN である。また，複数の PC を接続するために，PC と OFS_1 は，中継 SW を経由して接続する構成にしている。

図 6 では，PC がネットワークに接続し，自部門の仮想化された開発用サーバに接続するためのアドレス解決までのシーケンスを表示している。PC の OS によっては，デフォルトでは EAPOL-Start を出さない場合もある。その場合，認証 SW が PC 間のリンクアップを検出して，EAP-Request を発行する設定で対応する方法があるが，⑦中継 SW を経由した図 6 の構成では，PC が EAPOL-Start を送信することによって認証を始める必要がある。

T 君は，これまでの検討から，今後，無線 LAN 経由の接続が必要になった場合，よりセキュリティの高いポートベースの認証方式の採用が必要になった場合でも，OF 方式で対応可能と考え，検討結果を K 主任に報告し，了承された。

このようにして，K 主任と T 君は新しい基盤ネットワークの実現性に目途をつけることができたので，必要機器の選定・調達と詳細な設計を開始した。

設問 1　〔ネットワーク仮想化技術の調査〕について，(1) ～ (3) に答えよ。

(1) 本文中の［ a ］～［ c ］に入れる適切な字句を答えよ。

(2) 本文中の［ ア ］，［ イ ］に入れる適切な字句を，それぞれ 20 字以内で答えよ。

(3) OF 方式は，TRILL（Transparent Interconnection of Lots of Links）方式と異なり，経路選択に柔軟性があるので回線を有効利用できる。TRILL 方式と比較したときの柔軟性を，20 字以内で述べよ。

設問 2　〔テナントネットワーク実現性の検討〕について，(1) ～ (3) に答えよ。

(1) テナントネットワーク実現のためのメッセージ使用例を，次の表 5 のようにまとめたい。本文中の下線 ① 及び下線 ② の場合に，図 4 中の（A），（C）ではどのようなメッセージを使用しているか。表 1 中の字句を用いて，表 5 の空欄を埋めて，表を完成させよ。ここで，PC_4 は接続されておらず，構成上の問題はない環境で動作しているものとする。

なお，各欄には複数のメッセージが入る場合がある。また，該当するメッセージがない場合には，“なし”と記入すること。

表5　テナントネットワーク実現のためのメッセージ使用例

	(A)	(B)	(C)
下線① の場合		Flow Mod	
下線② の場合		Packet Out	

(2) 本文中の下線③について，図4中の PC_4 と PC_7 の IP アドレスが重複していた場合に，PC_1 に発生する可能性のある問題を挙げ，50字以内で述べよ。

(3) 本文中の下線③について，図4中の PC_1 と PC_2 の IP アドレスが重複していた場合に，PC_4 に発生する可能性のある問題を挙げ，50字以内で述べよ。

設問3　〔テナントネットワークへの PC 接続方式の検討〕について，(1)～(6)に答えよ。

(1) 本文中の下線④について，OFC はどのような接続制御処理をすればよいか。35字以内で述べよ。

(2) 本文中の下線⑤について，図5中の中継 SW に必要な機能を，特別の MAC グループアドレスを使用する EAP フレームの転送の観点から，20 字以内で答えよ。

(3) 本文中の下線⑥について，発生するセキュリティ問題を，35 字以内で述べよ。また，この問題に関して OF 方式で考えられる対処方法を，40 字以内で述べよ。

(4) 図6中で，IEEE 802.1X のオーセンティケータとして動作している機器を，図6中の機器名で答えよ。

(5) 本文中の下線⑦について，PC が EAPOL-Start を送信することによって認証を始める必要がある。その理由を，50字以内で述べよ。

(6) 図6中の（D），（E）の処理内容について，どのような種類のフレームを，どのポートに出力するかを含め，それぞれ55字以内で述べよ。

〔 メ モ 用 紙 〕

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（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。

午