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。

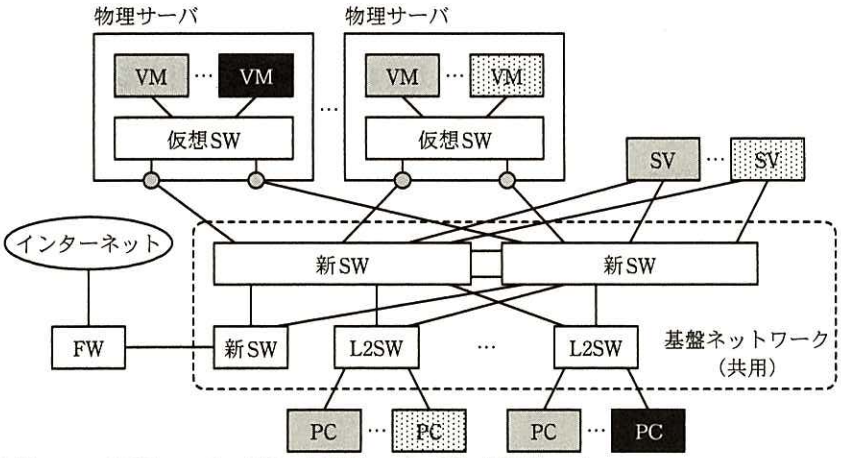
(1) サーバを仮想環境に移行することで，新たなサーバ増設要求への対応時間の短縮及び必要に応じた柔軟な構成の変更を実現する。ただし，移行当初は，既設サーバをそのまま活用する。

(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。

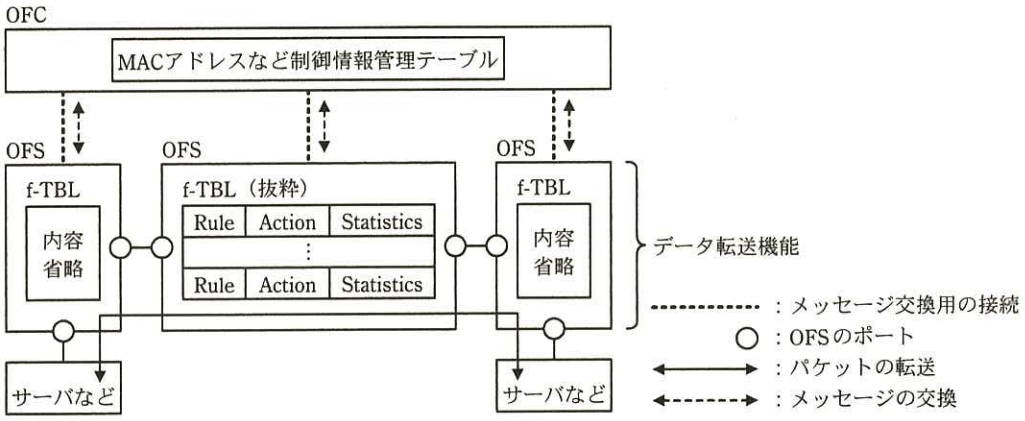


図 2　OF 方式での OFC と OFS の構成

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。

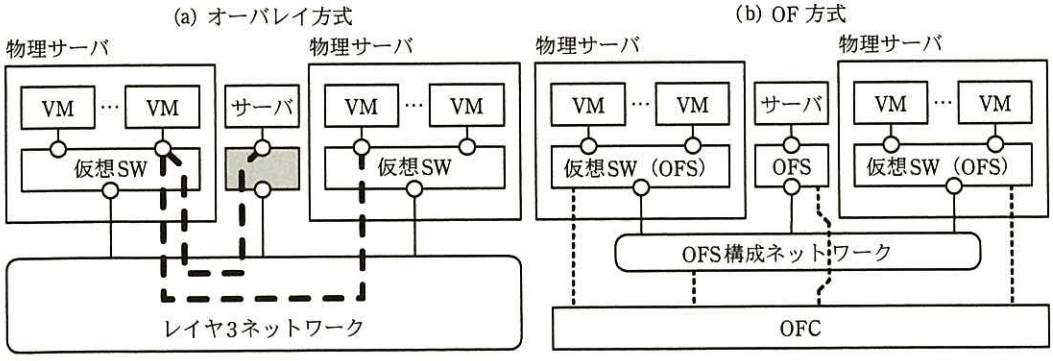
フローに対し，f-TBL 内に Rule が一致するエントリがあった場合，OFS は当該エントリに記述された Action の動作を行う。一方，なかった場合は，OFS は Packet In メッセージを OFC に送信し，そのパケットの処理方法を問い合わせるモードで動作する。Packet In を受信した OFC は，Flow Mod メッセージを使用して f-TBL に処理のエントリを登録したり，Packet Out メッセージを使用して指定ポートからのパケット送信を OFS に指示したりする。f-TBL 内の Rule 及び Action 内容の例を，表 2 に示す。

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。



○：スイッチのポート　　・・・・・・・・・：メッセージ交換用の接続[1)]

▬ ▬ ▬：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　　▭：サーバ接続用スイッチ

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。

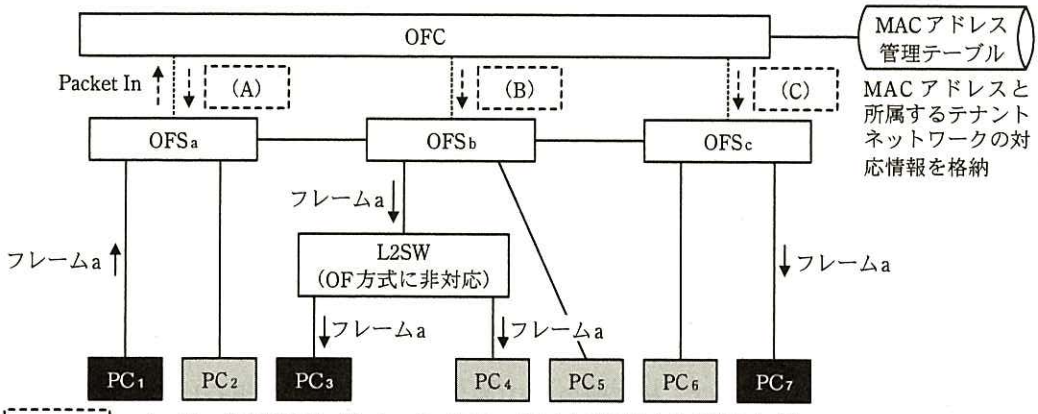
〔テナントネットワーク実現性の検討〕

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。



：メッセージの組合せ（Packet Out や Flow Mod などの組合せが使われる）

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。

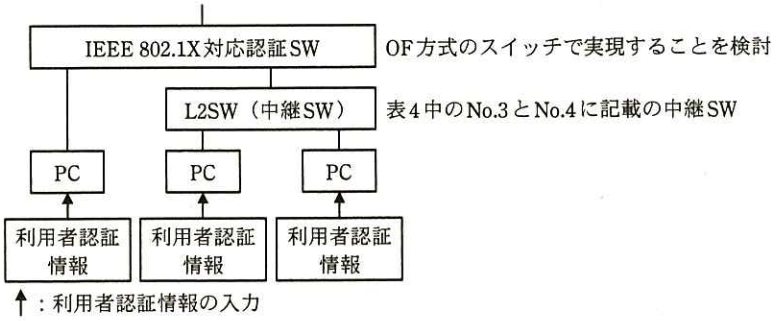


図 5　IEEE 802.1X 対応認証 SW への PC の接続形態

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。

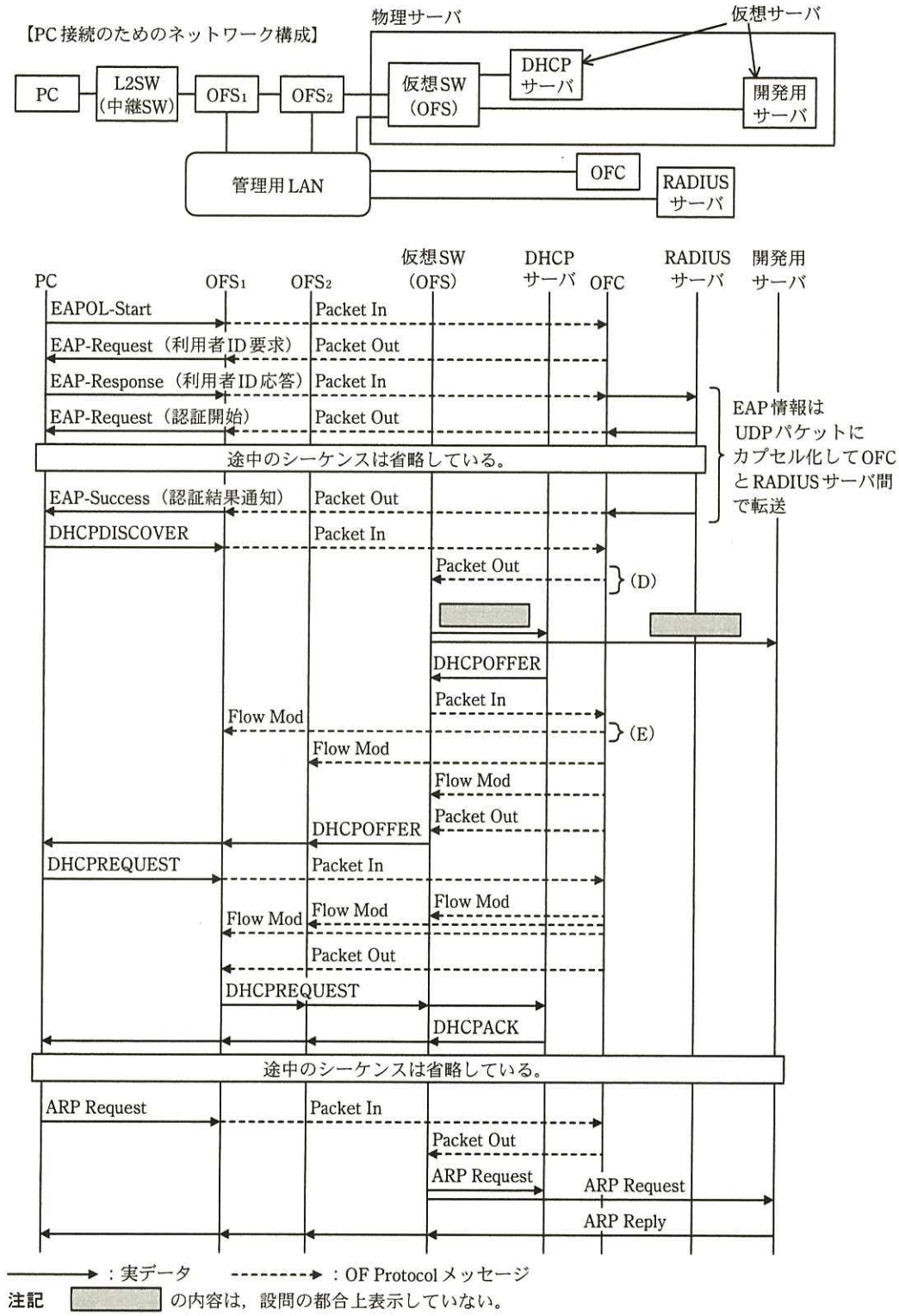


図6　IEEE 802.1X認証方式によるPCのテナントネットワークへの接続シーケンス例（概要）

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。