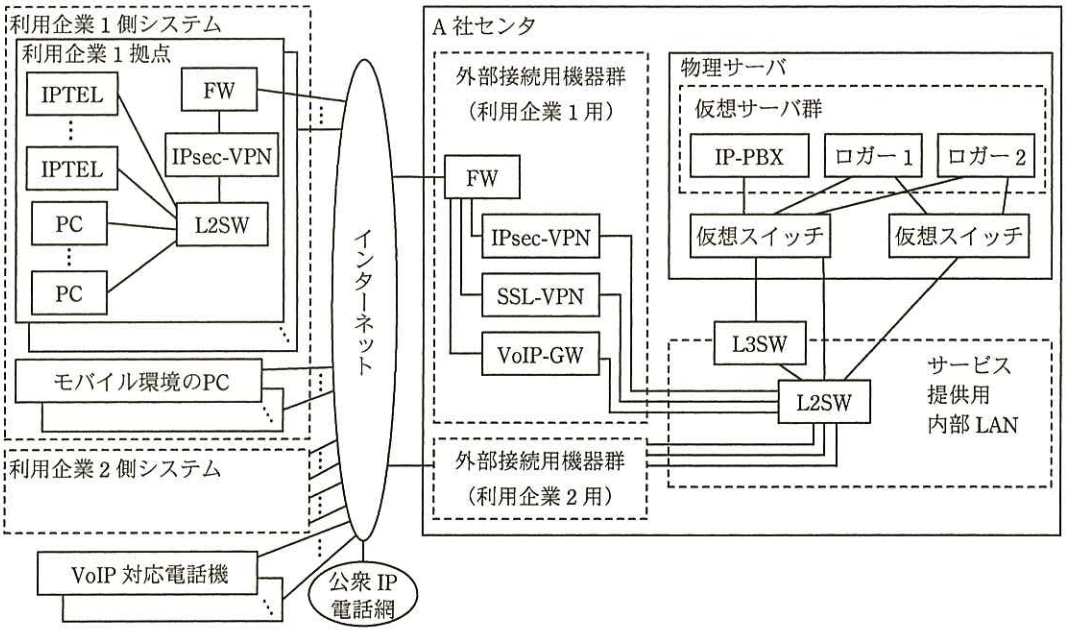
問2　サービス用システムの構築に関する次の記述を読んで，設問1～5に答えよ。

A 社では，VoIP 対応電話システム（以下，IPT システムという）を販売しているが，今後，A 社で設備を保有し，サービスとして提供したいと考えている。サービス提供時には，IPT システム用電話機（以下，IPTEL という）を利用企業に設置し，それ以外の IPT システム用機器を A 社センタに設置する形態を想定している。IPT システム担当部門の K 君は，最近のネットワーク技術に詳しい T 君の支援を受けながら，IPT システムのサービス化に向けて，実現性の検討を開始した。

〔サービス用 IPT システムの構成〕

図1は，K 君が T 君に示したサービス用 IPT システムの全体構成案である。



L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ　FW：ファイアウォール
IPsec-VPN：IPsec-VPN 装置　SSL-VPN：SSL-VPN 装置　VoIP-GW：VoIP 対応ゲートウェイ
IP-PBX：VoIP 対応 PBX

図1　サービス用 IPT システムの全体構成案

図1は，ある企業グループに属する利用企業1と利用企業2が，サービス用 IPT システムを利用する場合の構成を示している。利用企業1と利用企業2の内部ネットワークは，グループ内で重複しないプライベート IP アドレスを使用している。利用企業

内の拠点間通話は内線通話として処理される。

ロガーは，通話を録音するサーバである。ロガー1 及びロガー2 は，それぞれ利用企業 1 用及び利用企業 2 用である。IP-PBX は，その機能を利用企業ごとに独立して利用できるマルチテナント機能をもち，利用企業 1 と利用企業 2 で共用する。ロガー及び IP-PBX は，それぞれの仮想サーバで動作させる。利用企業の拠点と A 社間は，VPN で接続する。

利用企業の社員が，出張などで拠点外のモバイル環境にいても，サービス用 IPT システムが使えるようにする。このために，モバイル環境のソフトフォン（PC 上で動作するソフトウェアで実現する電話機能）を，内線電話機として利用できるようにする。モバイル環境の PC から A 社への接続に当たっては，セキュリティ確保のために接続 PC ごとに認証を行う。

A 社の IPT システムは，RFC 3261 で規定された SIP（Session Initiation Protocol）に準拠している。K 君は，IPT システムについては経験が浅い T 君に，概要を説明することにした。次は，K 君が T 君に説明した内容についてまとめたものである。

SIP は，ユーザエージェントと呼ばれる端末（以下，UA という）間で，セッションの生成，変更，切断を行うプロトコルである。SIP では，セッション上でやり取りされるデータそのものについては規定していない。生成したセッション上で，どのような通信を行うかは，SIP を使う上位のアプリケーションが，通信相手とのネゴシエーションによって決定する。このとき，セッション生成の過程でのやり取りには，RFC 4566 で規定された SDP（Session Description Protocol）が用いられる。したがって，アプリケーションが，SIP によって制御されたセッションでデータをやり取りする場合，音声データだけなら電話，テキストだけなら [a]，音声と動画を組み合わせることでビデオ会議，というように，幅広い応用の可能性がある。音声データを転送する場合の一般的なプロトコルは，RFC 3550 で規定された [b] であり，そのトランスポート層のプロトコルには，リアルタイム性を重視し，再送制御を行わない [c] が使われる。

UA の識別には，sip:xxx@example.ne.jp（xxx は利用者識別子）のような URI（Uniform Resource Identifier）形式が使われる。SDP のセッション生成情報には，接続相手の URI，自分の URI と IP アドレス，使用するコーデックなどの通信に必要な

情報が用いられる。

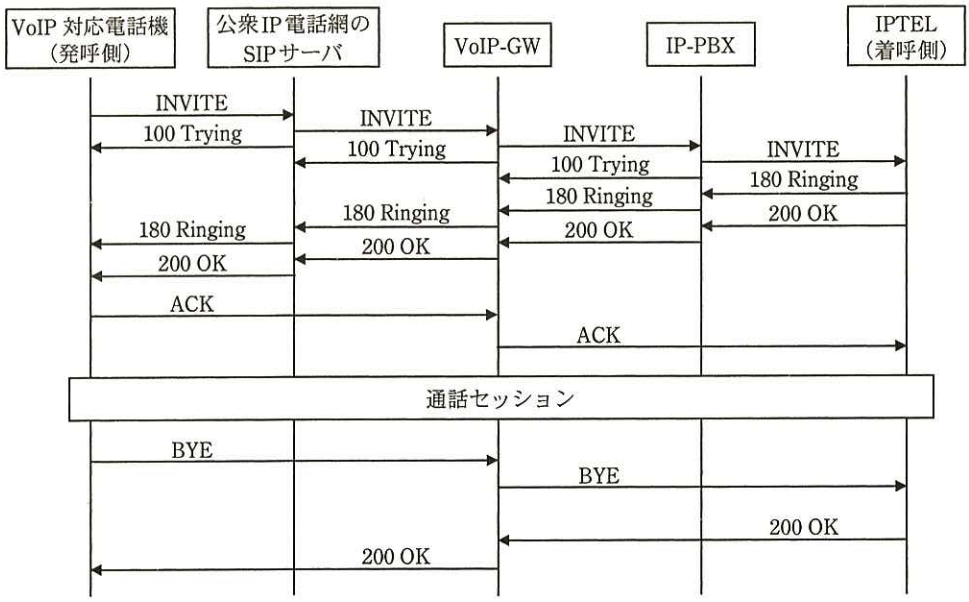
セッションは，通信を行う UA 間で直接やり取りして生成することもできるが，規模の大きな組織の場合は利用者が多く，URI の登録に手間が掛かるので，①セッションの生成を仲介するサーバを設置する。このサーバは SIP サーバと呼ばれ，図 1 のサービス用 IPT システムでは，IP-PBX がその役割を果たしている。

SIP で使われるメッセージは，［ d ］形式で記述されるので，判読しやすい。

〔IPT システムの概要〕

IP-PBX は，VoIP-GW を経由して通信事業者の公衆 IP 電話網と接続する。VoIP-GW は，両側の SIP 制御の実装上の差異を吸収して整合性をとる。

IPT システムでは，UA は起動後，自分の利用者識別子，自分の IP アドレスを含む登録メッセージを SIP サーバに送信し，初期登録をする。VoIP 対応電話機から発呼して IPTEL に着呼する場合について，SIP による電話接続シーケンス例を，図 2 に示す。



注記　初期登録は，事前に完了しているものとし，図中には含めていない。

図 2　SIP による電話接続シーケンス例

IP-PBX 配下の IPTEL を識別するための 050 電話番号は，公衆 IP 電話網の通信事業者から割り当てられる。通信事業者の公衆 IP 電話網の中にも SIP サーバが存在するの

で，VoIP-GW は，②両方の SIP ネットワークに対して UA として振る舞う特殊な UA である B2BUA（Back-to-Back User Agent）になる。また，VoIP-GW は，SIP ネットワークの境界に存在してセッション生成を仲介するとともに RTP パケットの中継も行う Session Border Controller（以下，SBC という）と呼ばれる機能をもつ。

SIP メッセージの例として，セッション生成開始時に使われる INVITE リクエストの内容例を，図 3 に示す。

```
INVITE sip:050yyyy1234@example.ne.jp;user=phone SIP/2.0
Via: SIP/2.0/UDP （発信元の IP アドレス）:5060;branch=（省略）
Max-Forwards: 70
From: <sip:050yyyy5678@example.ne.jp>;tag=（省略）
To: <sip:050yyyy1234@example.ne.jp;user=phone>
Call-ID: （省略）
CSeq: （省略） INVITE
Contact: <sip:050yyyy5678@（発信元の IP アドレス）>
Content-Type: application/sdp
Content-Length: （省略）

v=0
o=- （省略） （省略） IN IP4 （発信元の IP アドレス）
s=-
c=IN IP4 （発信元の IP アドレス）
t=0 0
m=audio 5090 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

先頭行

SIP ヘッダ

空白行

ボディ（SDP）

注記　yyyy は，URI の利用者識別子の一部を構成する数字を表す。

図 3　INVITE リクエストの内容例（抜粋）

インターネット網を経由して，SIP を使った通話を行う場合，企業内のプライベート IP アドレスの UA と外部とを接続するために，アドレス変換を行う必要がある。このときに，③標準的な NAT 装置では，通話セッションが生成できないという問題が発生する。K 君によれば，④この問題への対応機能をもつ SBC があるということであった。

〔パッシブ方式による音声パケットの収集〕

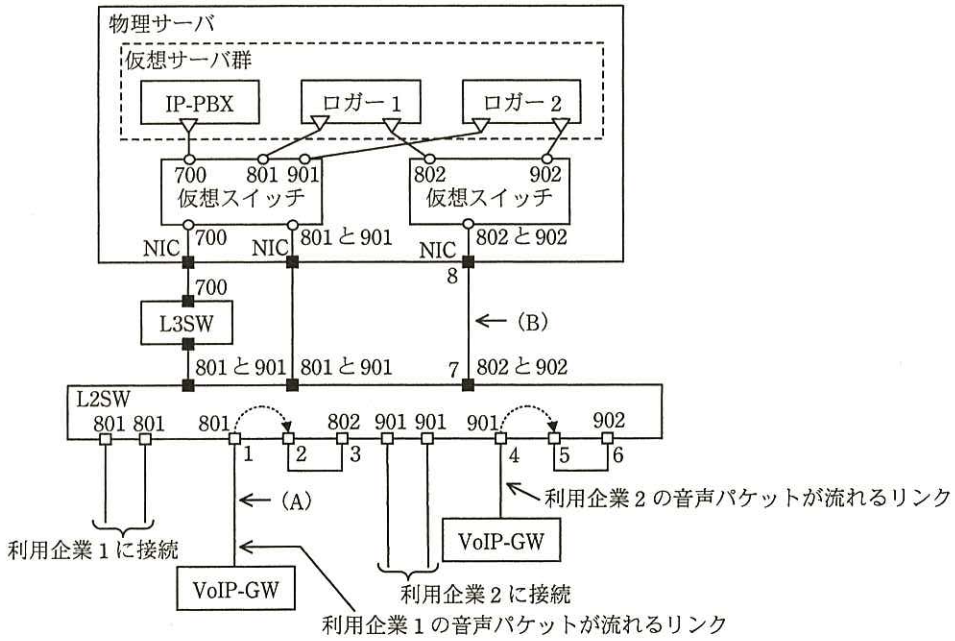
最近，コンプライアンスの観点から“通話を録音して保存したい”という要望が増

えている。そこで，この要望に対応するために，仮想サーバを使って，どのようなシステムを構築できるかを検討することになった。

従来，A 社では，IP-PBX システムに影響を与えない録音の方法を採用していた。この方法は，音声の通信経路にあるスイッチに，音声パケットが通過するポートのフレームをミラーポートに出力するように設定し，ミラーポート出力フレームを，ロガーの NIC で直接受ける方式である。この方式を，パッシブ方式と呼ぶ。

ミラーポート出力フレームを，仮想サーバで動作するロガーに取り込む場合には，単純にミラーポートを物理サーバの NIC に接続する方式だと，ミラーポートごとに NIC が必要となり，NIC 搭載数が限られる環境では使いにくい。

そこで，この問題を解決するために，K 君は，図 1 に対応して，図 4 に示す仮想サーバでロガーを動作させるためのテスト用ネットワークを作成した。



■：物理ポート（トランクポート）　□：物理ポート（アクセスポート）　○：仮想ポート　▽：仮想NIC
1～8：物理ポート番号　700，801，802，901，902：VLAN 番号　：ミラーフレームの転送

注記1　ポート2は，ポート1を通過するフレームのミラーフレーム出力ポートである。

注記2　ポート5は，ポート4を通過するフレームのミラーフレーム出力ポートである。

注記3　(A) と (B) は，調査のためにモニタした場所を示す。

図 4　仮想サーバでロガーを動作させるためのテスト用ネットワーク

ロガーは，音声パケットを収集するための専用の仮想 NIC と，運用・保守に使用す

る仮想NICの二つの仮想NICをもち，それぞれが異なる仮想スイッチに接続する。

K 君が考えた方法は，ミラーポート出力フレームを仮想サーバで動作するロガーに転送するためのVLANを定義し，物理サーバのNICとL2SWはトランク接続にする方法である。具体的には，L2SWの別々のVLANに属するポート3とポート6に，それぞれ異なるミラーポート出力フレームを入力して仮想スイッチに転送した後，宛先となるロガーに振り分ける。今回使用した仮想スイッチでは，接続する仮想サーバのMAC アドレスは仮想化のための仕組みで把握しているので，通過するフレームによる MAC アドレスの学習は行わない。ミラーポート出力フレームを取り込むために，仮想スイッチに接続する⑤ロガーの仮想 NIC と仮想スイッチの接続ポート間で，適切な動作をさせる。

なお，図4の構成で使用しているL2SWは，VLAN単位に独立したMACアドレステーブルをもつ仕様になっている。したがって，VLANが異なれば同じ MAC アドレスが学習されても問題がない。

K 君がこの構成で実験したところ，期待するフレームがロガーに転送されていないことが分かった。そこで，原因を調べるために，T 君とともに次のような点について検討した。

スイッチの設定の不具合の可能性もあり得るので，サーバと L2SW 間のフレームをモニタして調べることにした。K 君は，図4の（A）と（B）の位置で通過するフレームをモニタしてみた。すると，VoIP-GW が送受信したフレームを，（A）では確認できたが，（B）ではミラーリングしたそれらのフレームの通過が確認できなかった。相談を受けた T 君は，L2SW の MAC アドレステーブルがどのような状態であるかを調べるよう指示した。その結果を見た T 君は，⑥L2SW のポート3に流入するフレームの送信元MACアドレスと宛先MACアドレスの組合せに着目して原因を説明し，対応策を示した。

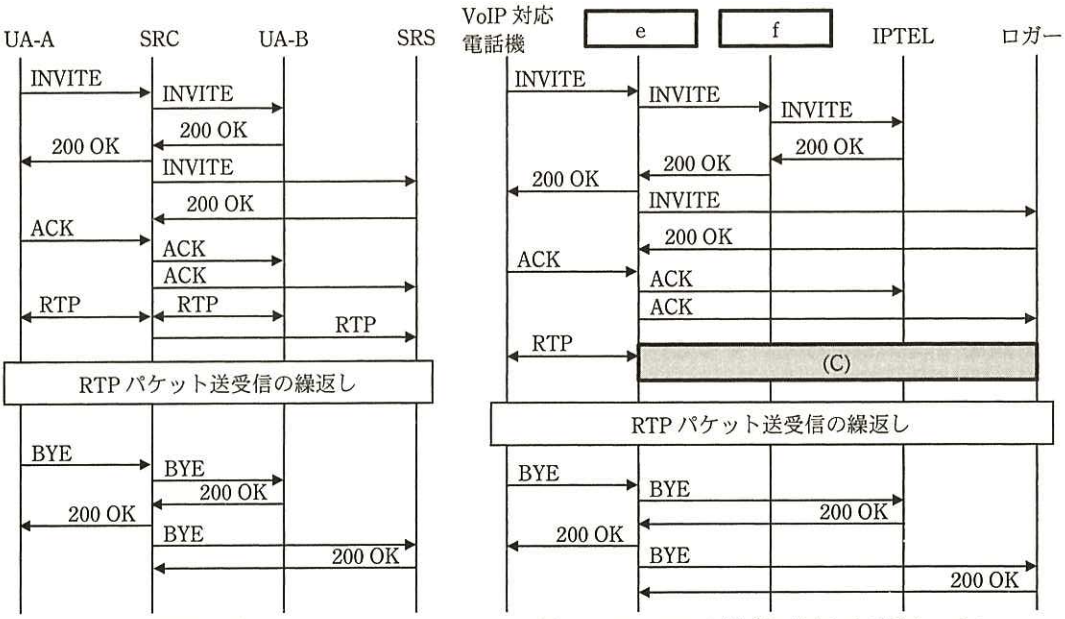
苦労して音声パケットの収集ができるようにはなったものの，音声パケットを収集するためのネットワークを構成する作業が大変だったので，T 君は，別の手段を調査するよう，K君にアドバイスした。

〔アクティブ方式による音声パケットの収集〕

K 君は，ミラーポート出力を使わない音声パケットの収集方式について調査した。その結果，アクティブ方式と呼ぶ収集方式があることが分かった。

アクティブ方式では，音声パケットを中継する機器上に，録音したい音声パケットをコピーして転送する機能を実装し，録音クライアント（以下，SRC という）とする。SRC は，音声パケットを受け取って録音する役割の録音サーバ（以下，SRS という）との間に SIP を用いて録音用セッションを生成し，コピーした音声パケットを，そのセッションを用いて転送する。また，音声パケット以外に，音声パケットに関係した通話の属性情報も，通知できる。

通話の収集対象となる二つの UA を UA-A と UA-B としたとき，アクティブ方式による動作シーケンスの概要を，図 5 に示す。



(a) 概念を示す動作シーケンス　(b) 図 1 の IPT システム構成に対応した動作シーケンス

注記1　(C)は，設問 4 のために処理シーケンスを表示していない。
注記2　RTP パケットの送受信のシーケンスは，通話が継続する間繰り返される。
注記3　ステータスコードが100番台の暫定応答のシーケンスは省略している。
注記4　e ，f は図 1 中の機器である。

図 5　アクティブ方式による動作シーケンスの概要

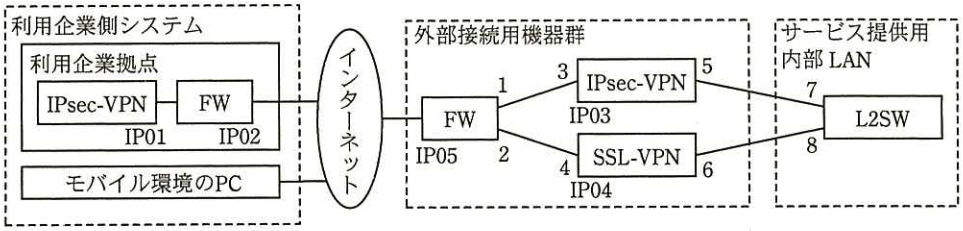
ここでは，アクティブ方式の概念を示すために，必要な機器だけを示している。図

5(a)では，SRC が，UA-A と UA-B 間の通話の音声パケットを中継するとともに，コピーした音声パケットを SRS に送る場合を，例示している。図 5(a)中の SRC は，音声パケットの中継だけでなく，UA-A と UA-B 間の通話用セッションの生成にも関与している。

K 君は，図 5(a)に示すシーケンスを参考に，⑦図 1 において SRC を実装する機器を選択し，図 5(a)に対応した図 1 におけるシーケンスとして図 5(b)を作成した。

〔外部接続用機器群の検討〕

K 君は，外部接続用機器の接続構成について検討した。図 6 は，図 1 に示した構成を実現するために K 君が作成した，外部接続用機器の構成図である。モバイル環境の PC は，A 社センタへ接続するために HTTPS を使用する。ここで，外部接続用機器は，利用企業ごとに用意するものとする。



1～8：物理ポート番号　IP01～IP05：固定のグローバルIPアドレス

図 6　外部接続用機器の構成図

A 社では，インターネット接続に関し，セキュリティ強化のために，接続元からのアクセスの違いによって，FW のポート 1 とポート 2 のアウトバウンドでは，表 1 に示すフィルタリングルール（許可条件）を適用する予定である。

表 1　フィルタリングルール（許可条件）

FW 物理ポート	送信元 IP アドレス	宛先 IP アドレス	ポート番号	プロトコル番号
1	ア	IP03	500	17（UDP）
			ウ	50（ESP）
2	イ	IP04	エ	any

ESP：Encapsulating Security Payload

注記　any は，パケットフィルタリングにおいてチェックしないことを示す。

SSL-VPN 装置では，モバイル環境の PC からのアクセスに対し，トークンを利用した利用者認証を行っている。認証された PC は，⑧新たな仮想 NIC を生成し，レイヤ 2 のトンネルを通して，サービス提供用内部 LAN との通信が可能になる。

K 君は，最近，長期間使用していた SSL-VPN 装置が故障した際，保守期間を過ぎていて，大至急別の機器を導入してネットワークを再設計しなければならないという経験をした。そこで，このような事態に対処しやすい方法について，T 君に質問した。T 君は，これまでの経験と知識を基に，次のように説明した。

ネットワーク機器の機能が，仮想サーバで動作するソフトウェアとして提供される（これを，ネットワーク機器の仮想化という）ようになると，K 君が経験した販売・保守の終了という問題への対応ができ，更にそれ以外にもいろいろな利点がある。

例えば，新たな利用者への機能提供の迅速化，構成変更への柔軟性が実現できる。また，保守・運用管理上，FW や VPN 装置などの⑨ネットワーク機器が仮想化されている場合，ハードウェア障害に備えた冗長化を実現する上で，コスト面での利点もある。

K 君は，T 君のアドバイスを参考に，ロガーだけでなく外部接続用機器群も，仮想サーバで動作するソフトウェアとして実現するよう提案することにした。

このようにして，K 君と T 君は，サービス用 IPT システムを仮想環境上に構築することについて，実現性と将来への考慮点に関する検討結果をまとめた。この検討結果は，プロジェクトの責任者である上長に報告され，了承された。

設問 1　〔サービス用 IPT システムの構成〕について，(1)，(2) に答えよ。

(1) 本文中の [a] ～ [d] に入れる適切な字句を答えよ。

(2) 本文中の下線①の動作を，40 字以内で具体的に述べよ。

設問 2　〔IPT システムの概要〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線②の B2BUA がその役割を果たすために，UA として初期登録する必要がある登録先を，本文中の名称を用いて全て答えよ。

(2) 本文中の下線③に示す問題の原因を，図 3 を参考にして，50 字以内で述べよ。

(3) 本文中の下線④について，図 2 の電話接続シーケンス例の場合に，SBC が行うアドレス変換の内容を，60 字以内で具体的に述べよ。

設問 3 〔パッシブ方式による音声パケットの収集〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑤について，適切な動作の内容を，60 字以内で述べよ。

(2) 本文中の下線⑥について，MAC アドレステーブルがどのような状態になっていたことが原因だったと考えられるか。50 字以内で述べよ。また，T 君の示した対応策を，50 字以内で述べよ。

設問 4 〔アクティブ方式による音声パケットの収集〕について，(1) ～ (5) に答えよ。

(1) 本文中の下線⑦について，IP-PBX は選択できない。その理由を，20 字以内で具体的に述べよ。

(2) 図 5 中の [e]，[f] に入れる適切な機器名を，図 1 中の機器名で答えよ。

(3) 図 5 中の (C)に処理シーケンスを追加して，図 5 (b)のシーケンスを完成させよ。

(4) 図 1 の構成で，図 5 (b)の方式を使用した場合，呼情報も録音用セッションを介して取得できる。その理由を 40 字以内で述べよ。

(5) パッシブ方式に比べてアクティブ方式の方が有利な点を，30 字以内で述べよ。

設問 5 〔外部接続用機器群の検討〕について，(1) ～ (3) に答えよ。

(1) 表 1 中の [ア] ～ [エ] に入れる適切な字句を答えよ。

(2) 本文中の下線⑧において，生成された仮想 NIC に対してどのような IP アドレスが付与される必要があるかを，35 字以内で述べよ。

(3) 本文中の下線⑨において，T 君がコスト面での利点が得られるとした理由を，40 字以内で述べよ。