NW

平成26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〕

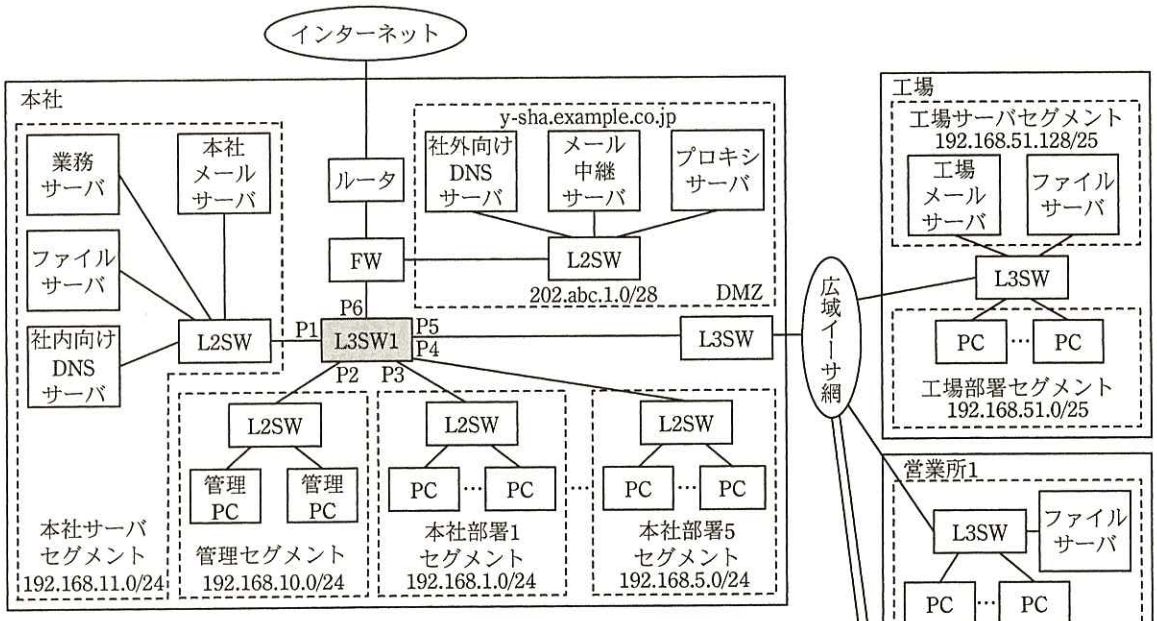
選択欄	
1問選択	問1
	(問2)

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　標的型メール攻撃の対策に関する次の記述を読んで，設問1～5に答えよ。

Y社は，産業機械の製造会社であり，本社の他に，工場と3か所の営業所がある。Y社の先進的な技術によって製造された製品は，顧客から高い評価を受けている。この優位性を維持するために，Y社ではこれまで，知財情報，個人情報などの安全な管理に注力してきた。

Y社では，製品の設計，開発及び外注先・顧客との情報交換に，電子メール（以下，メールという）を活用している。Y社のネットワークシステム構成を，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
L3SW1, L3SW：レイヤ3スイッチ
P1～P6：ポートID

メールサーバ名	IPアドレス
メール中継サーバ	202.abc.1.1
本社メールサーバ	192.168.11.1
工場メールサーバ	192.168.51.129

注記1　網掛け部分は，設問で使用されるレイヤ3スイッチを示す。
注記2　営業所1～営業所3のLANは，同じ構成である。
注記3　202.abc.1.0/28は，グローバルIPアドレスを示す。

図1　Y社のネットワークシステム構成

全社（本社，工場及び営業所）のネットワーク，サーバ及びPCのメンテナンスは，管理セグメントの管理PCを使用して行われている。各営業所には，当該営業所の営

業所員が使用するPCとファイルサーバが設置されている。管理PCを含む全社で使用されているPC（以下，全社のPCという）からインターネット上のWebサーバ，FTPサーバへのアクセスは，プロキシサーバを介してだけ可能である。本社と工場にはメールサーバが設置され，本社社員と営業所員は本社メールサーバで，工場社員は工場メールサーバで，メールの送受信を行っている。

メールの転送経路を，表1に示す。

表1　メールの転送経路

送信元	宛先	転送経路
本社，営業所	本社，営業所	PC → 本社メールサーバ
	工場	PC → 本社メールサーバ → 工場メールサーバ
	社外	PC → 本社メールサーバ → メール中継サーバ → 社外
工場	本社，営業所	PC → 工場メールサーバ → 本社メールサーバ
	工場	PC → 工場メールサーバ
	社外	PC → 工場メールサーバ → 本社メールサーバ → メール中継サーバ → 社外
社外	本社，営業所	社外 → メール中継サーバ → 本社メールサーバ
	工場	社外 → メール中継サーバ → 本社メールサーバ → 工場メールサーバ

最近，特定の企業，官公庁などを標的にして，その組織が保有する知財情報，個人情報などの重要な情報を窃取又は破壊する，標的型メール攻撃が増加してきた。この状況に対応するために，Y社では，標的型メール攻撃の対策を行うことにした。そこで，情報システム部のM部長は，セキュリティ担当のS主任とネットワーク担当のN主任に，対策案の検討を指示した。

S主任とN主任は，対策案の検討に先立ち，今後の進め方について打合せを行った。そのときの会話の一部を，次に示す。

S主任：標的型メール攻撃に対しては，マルウェアの侵入を防ぐ入口対策だけではなく，社内のLANに侵入したマルウェアの活動を抑えたり，活動を発見しやすくしたりする対策（以下，出口対策という）も必要になっているようだ。N主任には，ネットワークでの入口対策と出口対策を検討してもらって，私は，サーバとPCに必要なマルウェア対策と運用規程を見直すことにする。

N主任：了解した。検討後に対策案を持ち寄って，実施する対策について話し合おう。

N主任は，S主任との打合せの後，部下のJ君に，標的型メール攻撃の手法の調査と対策案の検討を指示した。

〔標的型メール攻撃の手法と対策案〕

J君は，標的型メール攻撃の手法の調査と対策案の検討を行った。

標的型メール攻撃の多くは，ソーシャルエンジニアリング手法で収集した攻撃対象者の情報を基に，（ア）攻撃対象者と関係がありそうな組織，機関及び実在の人物を装ったメールを送り付けてくる手法をとる。送り付けられたメールには，悪意のあるコード，マルウェアが埋め込まれたファイルが添付されていたり，マルウェアが仕込まれたWebサイトへのリンク先を示す［ a ］が本文に記載されていたりする。

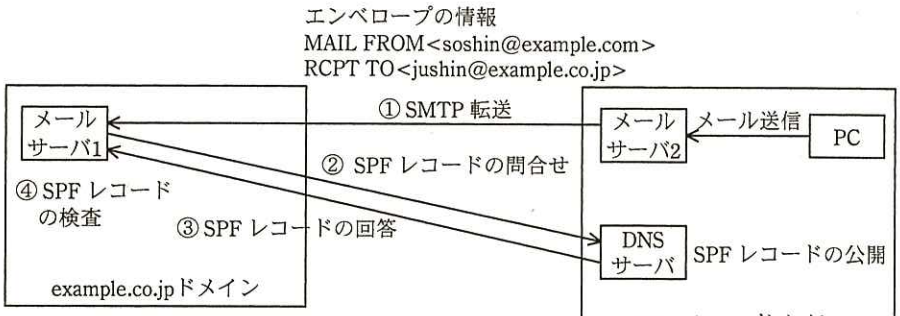
社内に侵入したマルウェアは，インターネット上の攻撃者のサーバとの通信路となるバックドアを開設して，攻撃基盤を構築することが多い。HTMLで作成されたコンテンツの送受信用プロトコルである［ b ］によってバックドアの通信が行われた場合，業務での通信との区別が困難である。マルウェアは，攻撃基盤を構築した後，システム内部への侵入を行い，拡散，重要情報の窃取，破壊などを行う。

SMTPでは，送信者が，自分自身のメールアドレスを容易に詐称することができる。しかし，送信元のMTA又はMUAが稼働するサーバ又はPCに設定されている［ c ］を書き換えることは困難である。そこで，（イ）ドメインを比較するだけでも，送信者のメールアドレスが詐称されているかどうかが，ある程度判別できる。

標的型メール攻撃の入口対策の一つとして，送信者のなりすましを検知する目的で開発された，送信ドメイン認証がある。送信ドメイン認証には，幾つかの手法があり，その中で，SPF（Sender Policy Framework）は，既存のネットワークシステムにも導入しやすい点が評価され，普及が進んでいる。

SPFでは，受信者が送信者のなりすましを検証するために，送信者のDNSの資源レコードにSPFレコードが追加されている必要がある。Y社でSPFを導入するときは，DMZの社外向けDNSサーバに，（ウ）メール中継サーバのIPアドレスを記述したSPFレコードを追加することになる。

SPFによる認証処理の概要を，図2に示す。



〔SPF による送信者のドメイン認証手順〕

① メールが，メールサーバ2からメールサーバ1に転送される。

② メールサーバ1は，エンベロープ中のメールアドレスを基に，DNS サーバにSPF レコードを問い合わせる。

③ DNSサーバから，SPF レコードが回答される。

④ メールサーバ1は，SPF レコードに登録されたメールサーバの IP アドレスを基に，受信したメールの正当性を検査する。不正なメールと判断したときには，受信したメールを廃棄又は隔離することができる。

図2 SPF による認証処理の概要

J 君は，標的型メール攻撃の入口対策として，SPF を導入することを考えた。

SPF を導入しても，マルウェアの社内への侵入を完全に阻止することはできない。そこで，攻撃基盤の構築を困難にしたり，バックドアの通信を発見しやすくしたりする出口対策が重要になる。

J 君は，ネットワークにおける出口対策には，プロキシサーバでの対策と社内の LAN での対策が有効と考えた。プロキシサーバでの対策として，既設のプロキシサーバを，認証機能と，HTTPS で暗号化されたデータを復号する機能とをもつ機種に交換する。認証機能によって，マルウェアによるプロキシサーバ経由の通信を困難にさせるだけでなく，取得できるログの情報が増える。復号機能によって，SSL/TLS（以下，SSL という）通信でも，受信したデータ中に不適切な言葉や文字列などが含まれていたとき，その通信を遮断する［ d ］や，Web サーバからダウンロードされるファイルに対するウイルスチェックなどの，セキュリティ対策が行えるようになる。

社内の LAN での対策としては，図 1 中の L3SW1 にパケットフィルタリングを設定して，業務に不要な通信を遮断する。

J 君は，これらの検討結果を N 主任に報告した。そのときの N 主任と J 君の会話の

一部を，次に示す。

N主任：SPFは入口対策として，容易に導入できそうだな。

J君　：はい。機器の交換とか，新たな機器の導入は必要ありません。

N主任：出口対策も効果がありそうだ。しかし，プロキシサーバがSSLを終端できると中間者攻撃が可能になってしまうので，復号機能の実現方法を調べてくれないか。パケットフィルタリングについては，具体的に検討してみなさい。

J君　：分かりました。早速，調査・検討してみます。

〔プロキシサーバの復号機能の実現方法〕

まず，J君は，プロキシサーバの復号機能の実現方法について調査した。

PCは，Webサーバとの間でSSL通信を行うときには，プロキシサーバ宛てにconnect要求を送信する。復号機能をもたない既設のプロキシサーバの場合，受信したconnect要求に含まれる接続先サーバとの間で，指定された宛先ポート番号に対してTCPコネクションを確立する。その後，プロキシサーバはPCにconnect応答を送信して，それ以降に受信したTCPデータをそのまま接続先に転送する，［　e　］処理の準備が整ったことを知らせる。

復号機能をもつプロキシサーバの場合，PCからのconnect要求を受信した後の動作は，次のようになる。

復号機能をもつプロキシサーバの動作手順の概要を，図3に示す。

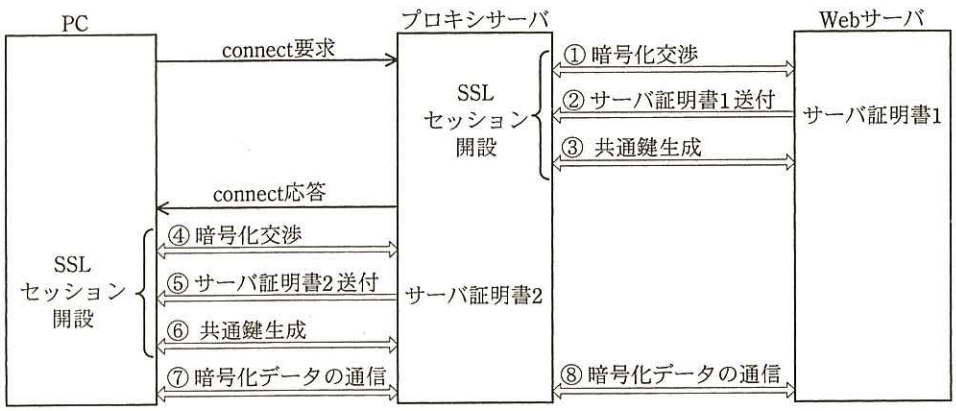


図3　復号機能をもつプロキシサーバの動作手順の概要

図 3 に示したように，PC からの connect 要求を受信したプロキシサーバは，まず，①～③の手順で Web サーバとの間で SSL セッションを開設し，更に PC との間でも，④～⑥の手順で SSL セッションを開設する。このとき，⑤で，プロキシサーバは，サブジェクト（Subject）に含まれるコモン名（CN：Common Name）に，サーバ証明書 1 と同じ情報をもたせたサーバ証明書 2 を生成して，PC 宛てに送信する。PC はサーバ証明書 2 を検証し，認証できたときに⑥が行われ，SSL セッションが開設される。ここで，PC がサーバ証明書 2 を正当なものと判断してプロキシサーバを認証するためには，PC に，（エ）サーバ証明書 2 を検証するのに必要な情報を保有させる必要がある。

なお，仮に，図 3 中の⑤で，プロキシサーバが Web サーバから取得したサーバ証明書 1 を PC に送信した場合，PC によるプロキシサーバの認証は成功する。しかし，（オ）⑥において，プリマスタシークレット（Premaster Secret）の共有に失敗するので，このような方法で SSL セッションを開設することはできない。

調査の結果，J 君は，プロキシサーバの復号機能の実現方法を確認できたので，次のステップとして，社内の LAN におけるセグメント間のパケットフィルタリングについて検討した。

〔パケットフィルタリングの検討〕

パケットフィルタリングの検討に当たって，J 君は，業務における各サーバの利用状況を調査し，用途とアクセス元を表 2，3 にまとめた。表 2 は，DMZ で稼働しているサーバの用途とアクセス元を，表 3 は，DMZ 以外で稼働しているサーバの用途とアクセス元をまとめたものである。

表 2　DMZ で稼働しているサーバの用途とアクセス元

サーバ名	用途	アクセス元
社外向け DNS サーバ	y-sha.example.co.jp ドメインのゾーン情報の管理	社外 社内向け DNS サーバ
メール中継サーバ	社外から Y 社宛てに送信されるメールの中継 Y 社から社外宛てに送信されるメールの中継	社外 本社メールサーバ
プロキシサーバ	全社の PC による社外の Web サイトへのアクセスの代理処理	全社の PC

表3　DMZ以外で稼働しているサーバの用途とアクセス元

設置場所	サーバ名	用途	アクセス元
本社サーバセグメント	本社メールサーバ	本社社員と営業所員のメールボックスの保持	本社と営業所のPC[1)] メール中継サーバ 工場メールサーバ
	業務サーバ	全社員向けの各種業務処理サービスの提供	全社のPC
	ファイルサーバ	本社社員と営業所員向けのファイルサービスの提供	本社と営業所のPC[1)]
	社内向けDNSサーバ	全社のPC及びメールサーバからの名前解決要求への応答	全社のPC メール中継サーバ 本社メールサーバ 工場メールサーバ
工場サーバセグメント	工場メールサーバ	工場社員のメールボックスの保持	工場のPC 本社メールサーバ
	ファイルサーバ	工場社員向けのファイルサービスの提供	工場のPC
各営業所	ファイルサーバ	営業所員向けのファイルサービスの提供	当該営業所のPC

注[1)]　本社と営業所のPCは，管理PCを含んでいる。

次に，表2，3の情報を基に，マルウェアの拡散を阻止するためのパケットフィルタリングポリシを，図4にまとめた。

①PCからサーバへの業務用通信及びサーバ間の業務用通信を，表2，3どおり許可する。
②上記①に加え，業務用通信区間における疎通テストのための通信を許可する。
③管理PCについては，上記①，②の他に，他のセグメントのPC及びサーバへのリモート接続と疎通テストのための通信を許可する。
④上記①～③以外の通信を禁止する。

図4　パケットフィルタリングポリシ

その後，図4を基に，パケットフィルタリングルールを検討した。

J君が検討してまとめた，ポートA，Bに設定するパケットフィルタリングルールを，表4，5に示す。ここで，ポートA，Bは，L3SW1のP1～P6のいずれかのポートであるが，設問の関係でどのポートかは明記しない。

表4　ポートAに設定するパケットフィルタリングルール

項番	動作	送信元IPアドレス	宛先IPアドレス	プロトコル	送信元ポート番号	宛先ポート番号	TCP制御ビット
1	許可	192.168.1.0/24	192.168.11.0/24	TCP	any	any	any
2	許可	192.168.1.0/24	192.168.11.0/24	ICMP	any	any	any
3	禁止	192.168.1.0/24	192.168.10.0/24	TCP	any	any	SYN=1 ACK=0
4	許可	192.168.1.0/24	192.168.10.0/24	TCP	any	any	any
5	許可	192.168.1.0/24	192.168.10.0/24	ICMP	any	any	any
6	許可	192.168.1.0/24	202.abc.1.0/28	TCP	any	any	any
7	許可	192.168.1.0/24	202.abc.1.0/28	ICMP	any	any	any
8	禁止	any	any	any	any	any	any

注記1　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。
注記2　パケットフィルタリングルールは，項番の小さい順に参照され，最初に該当したルールが適用される。

表5　ポートBに設定するパケットフィルタリングルール

項番	動作	送信元 IPアドレス	宛先 IPアドレス	プロトコル	送信元 ポート番号	宛先 ポート番号	TCP 制御ビット
1	許可	192.168.10.0/24	192.168.48.0/21	TCP	any	any	any
2	許可	192.168.10.0/24	192.168.48.0/21	ICMP	any	any	any
3	許可	192.168.11.0/24	192.168.51.128/25	TCP	any	any	any
4	許可	192.168.11.0/24	192.168.51.128/25	UDP	53	any	any
（省略）							
10	禁止	202.abc.1.0/28	192.168.51.128/25	any	any	any	any
11	禁止	202.abc.1.0/28	192.168.48.0/21	TCP	any	any	SYN=1 ACK=0
12	許可	202.abc.1.0/28	192.168.48.0/21	TCP	any	any	any
13	許可	202.abc.1.0/28	192.168.48.0/21	ICMP	any	any	any
14	禁止	any	any	any	any	any	any

注記 1　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。
注記 2　パケットフィルタリングルールは，項番の小さい順に参照され，最初に該当したルールが適用される。

J君は，全ての調査・検討が終了した後，プロキシサーバの復号機能の実現方法と，パケットフィルタリングルールの内容をN主任に説明した。説明を聞いたN主任は，プロキシサーバの復号機能については中間者攻撃に対して安全であることを了解した。しかし，パケットフィルタリングルールの内容については，（カ）表4にルールの漏れが一つあるので，項番1，2の間に追加するよう指示した。

〔入口対策と出口対策の実施項目〕

N主任は，J君の報告を基に対策案をまとめ，実施に移す対策（以下，実施策という）についてS主任と打合せを行った。そのときのN主任とS主任の会話を，次に示す。

N主任：ネットワークでの入口対策と出口対策の案をまとめた。入口対策としては，SPFを導入する。出口対策としては，既設のプロキシサーバを認証機能と復号機能をもつ機種に交換し，L3SW1にパケットフィルタリングを設定する。

S主任：分かった。私の方では，サーバ，PC及びFWでのマルウェア対策の実施状況について調査したところ，ウイルス対策ソフトの運用とセキュリティパッチの適用は，運用規程どおり実施されていた。また，FWでは，社内のLANからインターネットへの不必要な通信の遮断設定が適切に行われていた。しかし，不審なメールへの対応と，社内に侵入したマルウェアの活動を発見する

ためのログの検査が，適切には行われていなかった。今後，不審なメールへの対応に関する規程を定め，ログの検査方法・検査内容を見直すことにする。

N主任：プロキシサーバの交換で，マルウェアの活動を発見しやすくなるな。

S主任：そうだな。プロキシサーバで利用者認証を行えば，マルウェアによるバックドアの通信路の開設を困難にできるだけでなく，バックドアの通信が発見しやすくなる。セキュリティチームで，認証効果を高めるための全社のPCへの対策と，プロキシサーバのログの定期的な検査を行うことにする。

N主任：それでは，2人の検討結果をまとめて，M部長に提案しよう。

N主任とS主任は，検討結果を基に，次の6項目から成る標的型メール攻撃に対する実施策をまとめ，M部長に提出した。

・図1のネットワークシステムにSPFを導入する。
・プロキシサーバを交換し，プロキシサーバで利用者認証を行うとともに，復号機能を利用してSSL通信に対してもセキュリティ対策を行う。
・L3SW1で，セグメント間のパケットフィルタリングを行う。
・プロキシサーバの認証効果を高めるために，PCのWebブラウザの設定を変更する。
・(キ) 利用者が不審メールを発見したときの対応に関する規程を定め，運用規程に組み入れる。
・プロキシサーバのログの検査方法・検査内容を見直し，(ク) ログの検査間隔を可能な限り短縮して，定期的に検査を行う。

実施策が承認され，N主任とS主任は，ネットワークシステムの変更及び運用の見直しを進めることにした。

設問1　本文中の［ a ］～［ e ］に入れる適切な字句を答えよ。

設問2　〔標的型メール攻撃の手法と対策案〕について，(1)～(4)に答えよ。

(1) 本文中の下線（ア）のメールによって，メール送信者が誘導しようとする受信者の行動を，40字以内で述べよ。

(2) 本文中の下線（イ）で，比較する二つのドメインを，50字以内で述べよ。

(3) 本文中の下線（ウ）について，Y社には3台のメールサーバがあるが，その

中でメール中継サーバのIPアドレスを記述する理由を，30字以内で述べよ。

(4) Y社でSPFを導入するとき，社外向けDNSサーバへのSPFレコードの追加とともに，SPFによる認証処理を実施することになる。その認証処理を実施させるサーバ名を，図1中の名称で答えよ。また，認証処理を正しく行うには，そのサーバでなければならない理由を，30字以内で述べよ。

設問3 〔プロキシサーバの復号機能の実現方法〕について，(1)～(3)に答えよ。

(1) 既設のプロキシサーバの場合，SSLセッションはどの機器間で開設されるかを，図3中の名称で答えよ。

(2) 本文中の下線（エ）の情報を，20字以内で答えよ。

(3) 本文中の下線（オ）について，失敗する理由を，40字以内で述べよ。

設問4 〔パケットフィルタリングの検討〕について，(1)～(4)に答えよ。

(1) 表4，5のパケットフィルタリングルールを適用するポートA，Bを，図1中のポートIDで答えよ。また，通信の方向を，IN又はOUTで答えよ。

(2) 表4中の項番2のパケットフィルタリングルールの目的を，25字以内で述べよ。

(3) 本文中の下線（カ）で，N主任が表4への追加を指示したパケットフィルタリングルールを，表4の記述方法で答えよ。

(4) 表4中の項番3，4の二つのパケットフィルタリングルールによって制御される通信の内容を，70字以内で述べよ。

設問5 〔入口対策と出口対策の実施項目〕について，(1)～(3)に答えよ。

(1) プロキシサーバの交換によって，新たにログとして取得できる情報について，60字以内で述べよ。

(2) 本文中の下線（キ）で定めるべき規程の内容を三つ挙げ，それぞれ30字以内で述べよ。

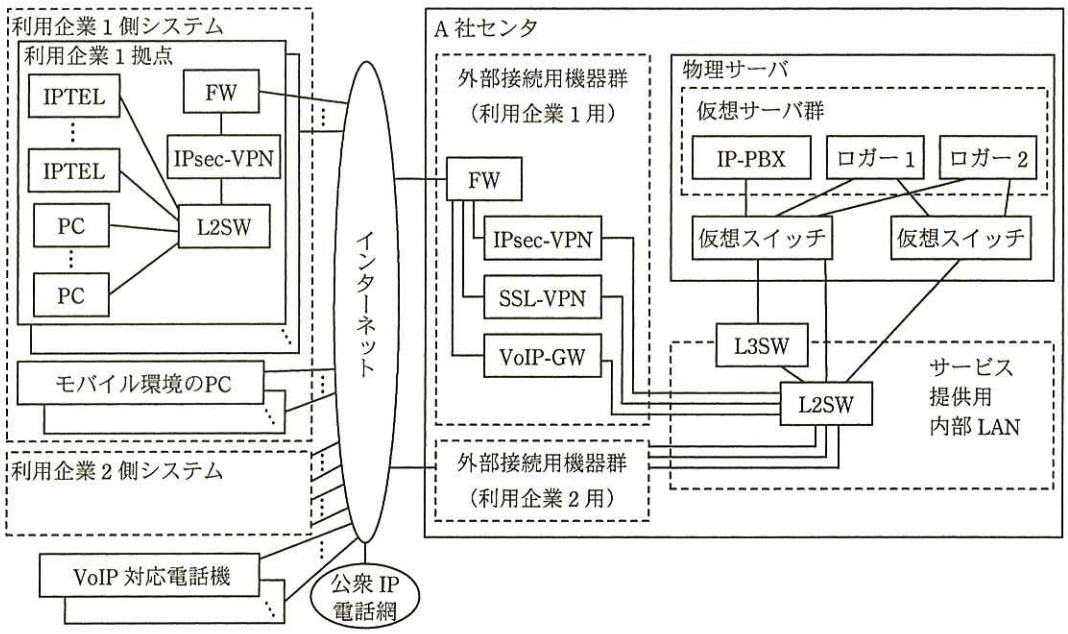
(3) 本文中の下線（ク）によって期待される効果を，30字以内で述べよ。

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。

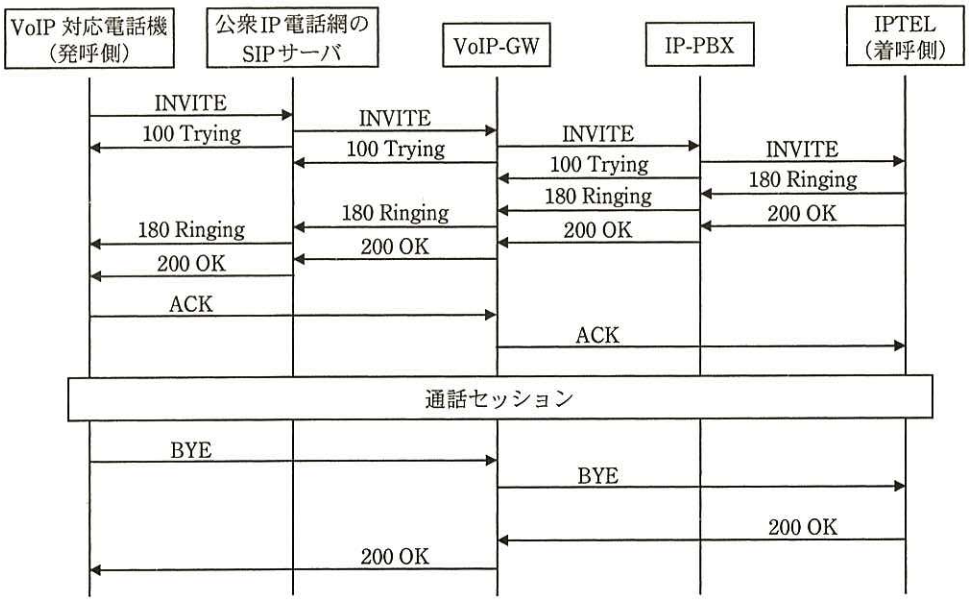
セッションは，通信を行う UA 間で直接やり取りして生成することもできるが，規模の大きな組織の場合は利用者が多く，URI の登録に手間が掛かるので，①セッションの生成を仲介するサーバを設置する。このサーバは SIP サーバと呼ばれ，図 1 のサービス用 IPT システムでは，IP-PBX がその役割を果たしている。

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。

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〕

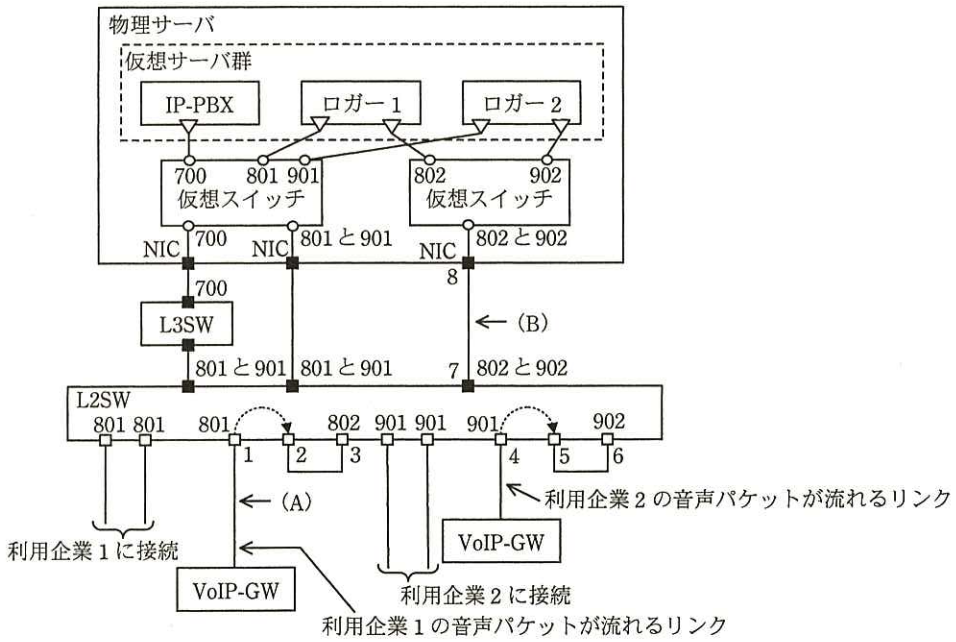
最近，コンプライアンスの観点から“通話を録音して保存したい”という要望が増

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。

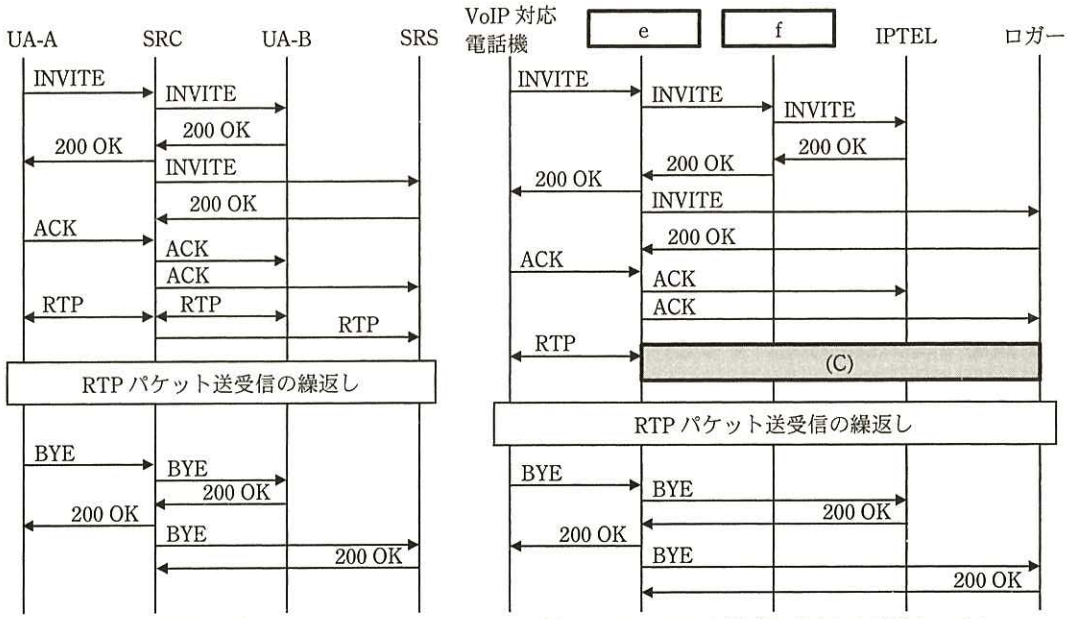
苦労して音声パケットの収集ができるようにはなったものの，音声パケットを収集するためのネットワークを構成する作業が大変だったので，T 君は，別の手段を調査するよう，K 君にアドバイスした。

〔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

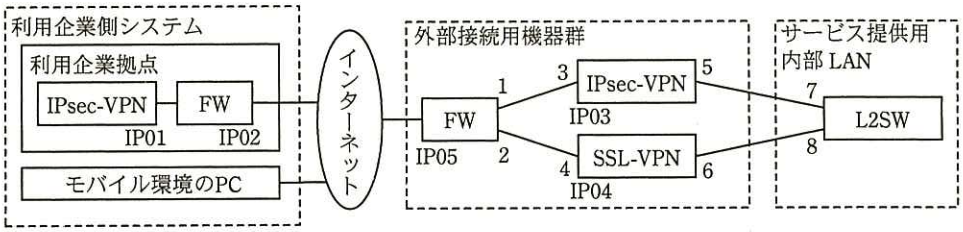
ここでは，アクティブ方式の概念を示すために，必要な機器だけを示している。図

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。

〔 メ モ 用 紙 〕

〔 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。