平成１９年度　秋期　テクニカルエンジニア（ネットワーク）　午後Ⅱ問題

問１　フォレンジックシステムの設計に関する次の記述を読んで，設問 1～5 に答えよ。

証券会社の T 社では，企業の社会的責任が厳しく問われるとともに法的規制も強化される状況下で，内部統制を実現するシステムの検討を始めた。中でも，企業活動の各種履歴を証拠性のある形で保存するシステム（以下，フォレンジックシステムという）を構築し，事故発生時に，その保存した情報から適切な対応をとれることが必要であるという認識となった。そこで，必要な情報を漏れなく確実に採取するという観点で，ネットワーク上のパケットを採取する方式を検討することになり，システム部主任 M 氏と N 君が担当となった。

図 1 は，現在の T 社ネットワークシステムの構成である。

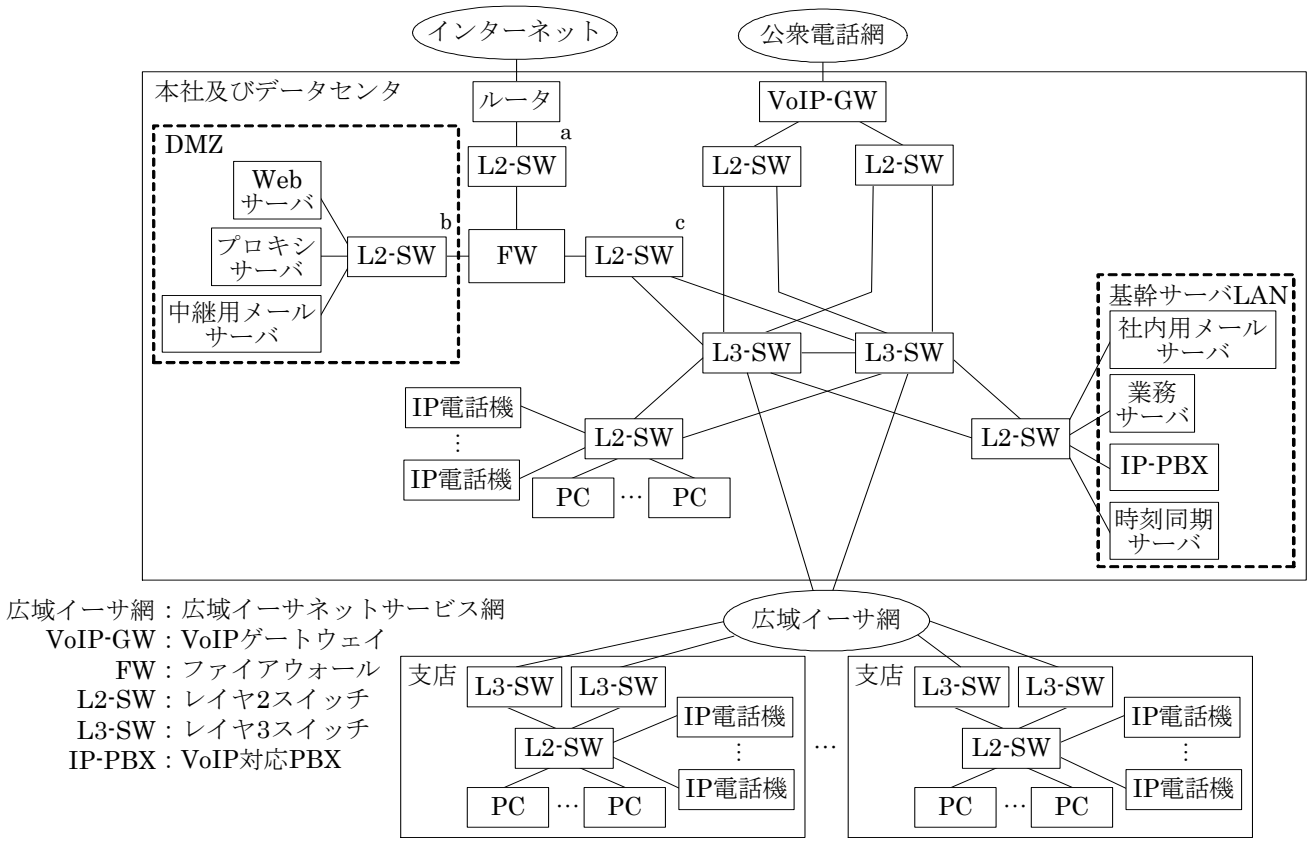


図１　現在のＴ社ネットワークシステムの構成

〔フォレンジックシステムの概要〕

情報漏えい対策としてアクセス管理の強化などを進めているが，こうした対策を実施しても，正規のアクセス権限をもった利用者による情報の不正利用の可能性を考えると，対策としては不十分である。フォレンジックシステムを導入することによって，インターネットへのアクセス履歴や電子メール（以下，メールという）の送受信データ，通話の音声データなどを保存することができるので，事故が起き

ても速やかに原因を突き止めるのに役立てることができる。

T 社では，主な保存対象として，社外の Web へのアクセス，社外とのメール，及び IP 電話での社外との通話を想定している。

次は，フォレンジックシステムに関する，M 氏と N 君の会話である。

M 氏：システムログでは，例えば，特定データへのアクセスや，メールを送ったのがだれかというレベルの状況証拠的な記録は取れるが，実際の内容が分からないと，事故の調査・分析の証拠としては不十分なんだ。

N 君：そうですね。最近はそうした問題を解決し，より高い証拠能力を確保するフォレンジック製品が注目されているようです。フォレンジックとは“法廷の”という意味で，あまり聞いたことがない言葉ですが，ディジタルデータの証拠保全，証拠収集のための活動や機能のことだそうです。

M 氏：よく勉強しているようだね。それでは，当社で保存したい情報を，どこで，どのようにして採取するか考えてみよう。

フォレンジックシステムでは，ネットワーク上を流れる必要なパケットをすべて採取するフォレンジックサーバ（以下，FS という）を設置する。

なお，FS の設置場所が適切でないと，期待する情報を採取できない。

FS で採取されたパケットの内容を分析して表示するためには，プロトコル解析機能と表示機能が必要である。T 社は HTTP 及び SMTP/POP3 のプロトコル解析機能と表示機能をもつ FS（以下，データ FS という）と，RTP（Real-time　Transport Protocol）及び SIP（Session Initiation Protocol）のプロトコル解析機能と表示機能をもつ FS（以下，音声 FS という）の 2 種類の FS を導入する。

〔データ系パケットの採取〕

今回導入を検討しているデータ FS では，社外の Web へのアクセス履歴と社外とのメールの送受信データだけを採取し，データセンタ内に新設する NAS（Network Attached Storage）に 3 年間保存する。データの保存量については，机上の計算で求めることが難しいので，FS のベンダは，試験的に FS を持ち込んで 1 週間程度実測の上，その実測結果を基に NAS の容量を決めることを推奨している。

T 社では，社外の Web へのアクセスはプロキシサーバを経由している。当初 N 君は，図 1 中の a の L2-SW にデータ FS を接続しようと考えた。

次は，データ FS の設置場所に関する，M 氏と N 君の会話である。

M 氏：フォレンジックの観点からは，社内のどの PC からのアクセスかを特定できる情報が必要だと思うが，N 君の考えた設置場所で，採取できるのだろうか。

N 君：そうですね。この場所では，問題がありますね。当社ではプロキシサーバ経由で社外の Web にアクセスしているので，注意が必要ですね。

N 君は，M 氏の指摘を受けて，Web へのアクセスに関するパケットを採取するため，データ FS の接続先を，図 1 中の a から c の L2-SW に変更した。

〔音声系パケットの採取〕

T 社では，音声については，IP 電話での社外との通話を保存対象として考えている。フォレンジックのために，音声の通話内容を採取・保存する場合は，音声がどのようにパケット化されて転送されるのかを，よく知っておく必要がある。

音声は，リアルタイムに音声や動画を送受信するためのプロトコルである RTP を使用して転送される。RTP は，通常 [ア] の上位プロトコルとして動作しており，この場合パケットの廃棄があっても，パケットは再送されない。

次は，音声 FS に関する，M 氏と N 君の会話である。

M 氏：音声 FS では，通話の音声は RTP パケットを採取することで取得できるが，それに関しては，どのような注意が必要だろうか。

N 君：社外の通話相手と接続するまでの呼制御処理のフェーズでは，社内の IP 電話機は [イ] とやり取りをしますが，通話フェーズになると今度は，[ウ] と RTP パケットをやり取りすることになります。したがって，RTP パケットを採取するだけでは通話先情報の取得に関しては不十分なので，[イ] から送られる SIP パケットの呼制御情報も必要になります。

M 氏：そうか。いろいろと難しい問題があるな。ところで，それらの音声系パケットを採取すると，音声データ量は相当多くなると思うが，NAS の容量は大丈夫だろうか。

N 君：その点ですが，一般的な音声領域は 4kHz 以下なので，[エ] 定理によると，波形再現のためにはサンプリングのクロックは最小限 [オ] kHz 必要となります。1 サンプリング当たり 8 ビットで表現すると，5 分間の音声通話で音声データ量は 2.4M バイトにもなってしまいます。このように，音声データは大量になるので，採取した音声データは直ちに圧縮して格納する処理が必要になります。音声データについては専用の圧縮方式があり，それで圧縮することが必要です。

M 氏：なるほど。それで圧縮が必要なんだな。ところで，音声 FS を導入するに当たって，フォレンジックシステムとして考慮しておかなければならないことがあったら，教えてほしいのだが。

N 君：はい。社外とのやり取りを採取するという観点から，採取したい通話の音声系パケットが通過する図 1 中の VoIP-GW に隣接している L2-SW にミラーポートを設定し，ミラーポートの出力を音声 FS に接続する必要があります。

M 氏：そうか。そのほかにもまだ注意することはあるかね。

N 君：はい。現在導入検討中の音声 FS には，音声系パケットのキャプチャ性能を上げるために，搭載されている LAN 制御用チップに，①IP パケット内の優先制御用特定ビットが指定された値かどうかを判定して音声系パケットを取り込むという機能が実装されています。この機能を有効に活用して，音声系以外のパケットをサーバに取り込まないようにしています。このように，音声 FS では，音声系パケットの取込みに特化することで，サーバの性能を確保しています。

M 氏：なるほど。そうすると，音声系パケットを送出する機器の設定は，きちんと文書化して，間違いなく行われるようにしておく必要があるね。

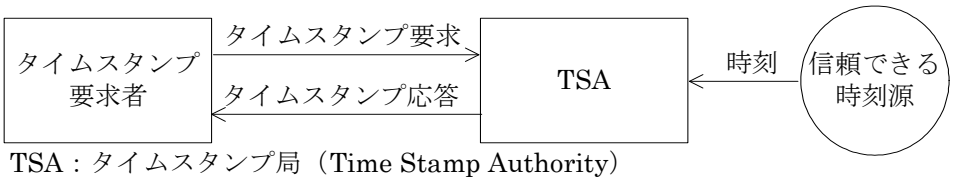
N 君：はい，そのとおりです。

〔証拠性の確保〕

次は，採取したデータの証拠性の確保に関する，M 氏と N 君の会話である。

M 氏：フォレンジックシステムでは，システム内の各所で採取したデータを順序付けるために，データの採取時刻が重要だ。機器間の時刻を合わせるには，図 1 中の時刻同期サーバを使用するが，NTP（Network Time Protocol）で設定した時刻が正しいとしても，②この時刻では，証拠性を担保するための手段としては使えないね。

N 君：そうです。その目的のためには，RFC 3161 で標準化されているタイムスタンププロトコルを使う必要があります。タイムスタンププロトコルの概要を，図 2 に示します。



TSA：タイムスタンプ局（Time Stamp Authority）

図２　タイムスタンププロトコルの概要

N 君：タイムスタンププロトコルに従った動作は次のようになります。まず，タイムスタンプ要求者は，TSA へのタイムスタンプ要求に，タイムスタンプを付けたいデータのメッセージダイジェストと呼ばれるハッシュ値を添付します。タイムスタンプ要求を受けた TSA は，信頼できる時刻源から取得した時刻とハッシュ値を合わせたものに電子署名を行って，証明書となる TST（Time Stamp Token）を作成し，返送します。この TST によって，③タイムスタンプの時刻と関係付けた，証拠性に関する二つのことが保証されることになります。

M 氏：ところで，TSA はインターネット上にあるので，FW 経由の社外とのアクセスになるが，TSA にはどのようにアクセスするのかね。

N 君：TSA にアクセスする方法としては，リアルタイム性を考慮するとポート番号 318 を使用した Socket Based Protocol，又は HTTP を使った通信が可能です。今回は，それらの中で HTTP を使用したアクセスを考えています。

〔データの保存方法・管理方法の検討〕

T 社では，データはすべてデータセンタ内の NAS で集中保存・管理することから，FS で採取したデータを NAS に転送する必要がある。図 3 は，データ採取のためのミラーポートを設定する L2-SW，FS 及び NAS の接続概念図である。FS は，FS_1 と FS_2 による冗長構成となっており，いずれか一方に障害が発生しても，もう一方でデータ採取が可能である。

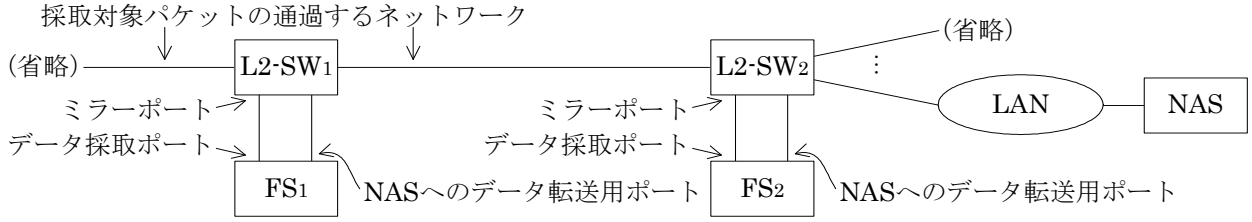


図３　L2-SW，FS 及び NAS の接続概念図

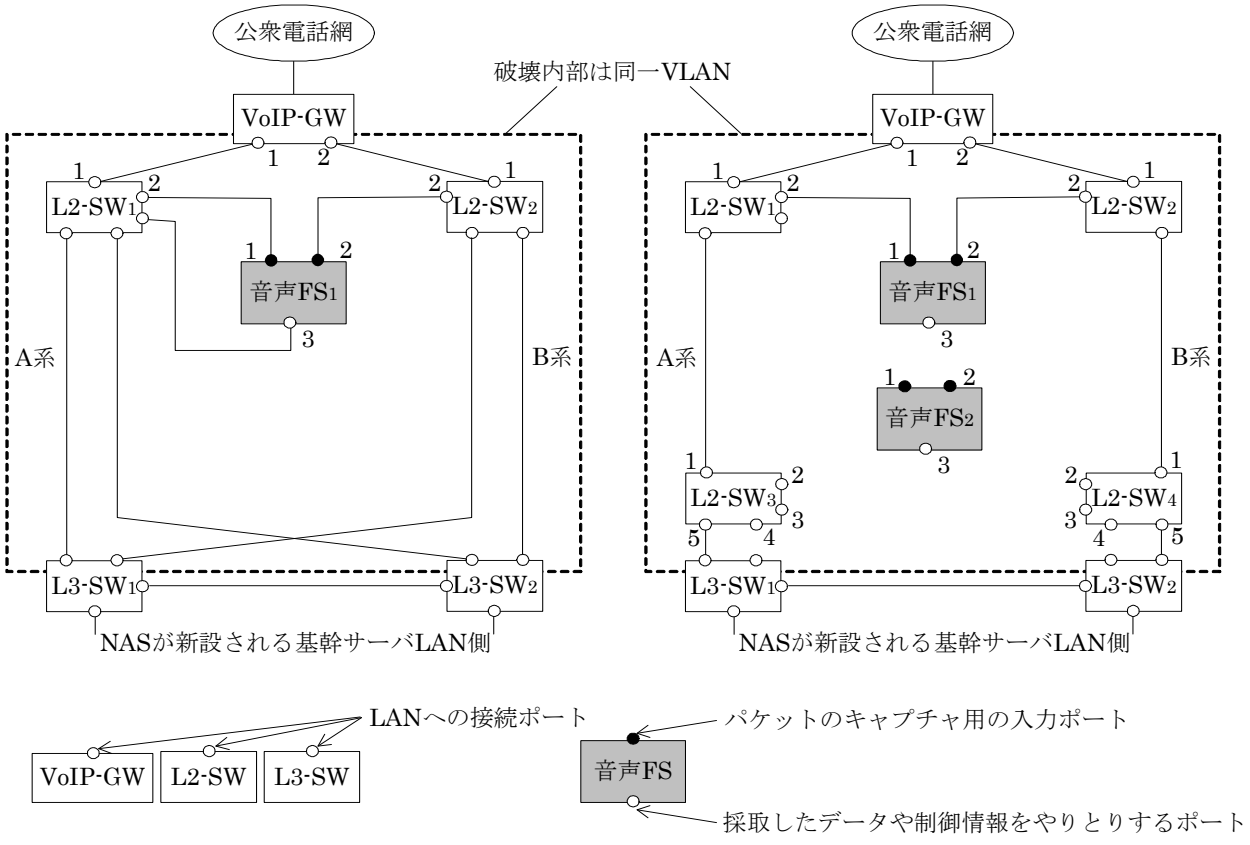
NAS にデータを保存する際には，NAS の WORM（Write Once Read Many）機能を使用することにした。WORM 機能を使うと，一度書き込んだデータは，設定した期間内は読み出すことしかできない。FS で採取したデータをファイル化したとき，そのファイルのタイムスタンプ認証も合わせて行う。タイムスタンプ認証をファイル単位に付与すると処理負荷が掛かるので，複数のファイルをまとめて認証できるように，認証に必要な情報の入った一覧表を作成する。その一覧表に対して認証を行うことで処理回数を削減するとともに，証拠性も確保する。NAS のデータは，1 か月単位でテープにバックアップすることにした。このとき，記憶媒体から情報が漏えいすることを防止するために，バックアップファイルは暗号化することにした。

〔音声 FS のネットワーク接続と信頼性の高い音声データ採取方式〕

これまでの検討結果を踏まえ，機器を実際に設置するための検討を行った。T 社では，信頼性を高めるために極力ネットワークの冗長化を図り，一方の系に障害が発生しても，もう一方の系で通信路を確保する方式を採用している。

図 4 は，N 君が検討中の，音声 FS とネットワークの接続構成で，音声系パケットの流れに着目し，音声 FS を導入する前提で，関係のある機器を抜き出して示している。図 4 中の（1）は，音声 FS を 1 台導入した場合の構成であり，<u>④一部の L2-SW に障害が発生した場合，音声データの採取又は保存上不具合のある構成となっている</u>。図 4 中の（2）は音声 FS を 2 台導入して，信頼性を高めた構成である。

（1）音声 FS を 1 台導入した場合の構成　　（2）音声 FS を 2 台導入した場合の構成



注１　(2)は，設問の関係上，接続の一部を表示していない。

注２　1台の L2-SW には，一つのミラーポートしか設定できないものとする。

図４　検討中の，音声ＦＳとネットワークの接続構成

L3-SW1 と L3-SW2 は，RFC 2338 で規定されているルータの冗長化機能である［　a　］によって，冗長構成をとっている。

VoIP-GW には，ネットワークの障害時に音声系パケットの経路切替えを高速化するための機能が実装されている。

VoIP-GW は，同じ IP アドレスをもつ二つの LAN インタフェースで，一つの VLAN に収容されている。VoIP-GW が，ポート 1，2 のうち，どちらをデータ転送に使用するかは，⑤VoIP-GW から，基幹サーバ LAN 側デフォルトゲートウェイへの in コマンドの応答によって決定している。障害が発生していない場合は，L2-SW1 側の経路が稼働系，L2-SW2 側の経路が待機系となって，パケットが流れるように設定されている。L2-SW1 と L3-SW1 を結ぶ経路を A 系，L2-SW2 と L3-SW2 を結ぶ経路を B 系という。

N 君は，音声 FS のネットワーク接続について検討するよう，M 氏から指示された。

次は，音声 FS のネットワーク接続についての検討に関する，M 氏と N 君の会話である。

M 氏：今回構築するのはフォレンジックシステムなので，24 時間 365 日の音声データを採取できるように設計する必要があるね。

N 君：はい。そのために，ネットワークや，音声 FS などの障害対応だけでなく，定常的に行うべきバックアップなどのメンテナンスについても考える必要があります。

M 氏：当然，音声 FS も二重化しておかなければならないだろうね。そうすると，必要なミラーポートを確保するために L2-SW も 2 台追加しなければならないが，音声 FS のネットワーク接続を考える上での要件は，どうなるのだろうか。

N 君：はい。整理すると，次のようになります。

（要件 1）音声 FS の障害対応として，一方の系が障害になっても，もう一方の系で必ず音声系パケットの採取ができること

（要件 2）L2-SW 及び L3-SW の障害対応として，音声系パケットがどの経路を通過しても音声系パケットの採取ができること

（要件 3）L2-SW 及び L3-SW に障害が発生しても，音声 FS で採取した音声データを NAS に保存するための経路を確保できること

M 氏：これらの要件から，音声 FS とネットワークの接続をどのように考えたのかね。

N 君：はい。まず，要件 1 について，2 台の音声 FS を正常時の音声系パケット通過経路にどのように接続するかを検討しました。次に，要件 2 について，2 台ある音声 FS のうちのいずれかを L2-SW 障害時の音声系パケット通過経路に接続させるようにしました。さらに，要件 3 に沿って，採取した音声データを NAS に保存するための経路を確保する方式を考えました。

M 氏：それでは，N 君の検討した構成を見せてくれないか。

N 君：はい。特に複雑な L2-SW 障害時に着目し，音声系パケットの取込み可否及び NAS への音声データ保存可否についてチェックし，表のようにまとめました。

表　SW 障害時の音声系パケットの取込み可否及び NAS への音声データ保存可否チェック

障害部位	音声系パケットの通過経路		音声系パケットの取込み		NAS への音声データ保存	
	A 系	B 系	音声 FS_1	音声 FS_2	音声 FS_1	音声 FS_2
L2- SW_1	不可	可	可	可	可	可
L2-SW_2	可	不可	可	可	可	可
L2-SW_3	不可	可	可	可	不可	可
L2-SW_4	可	不可	可	可	可	不可

M 氏：なるほど。よく検討してあるようだ。音声 FS の空きのキャプチャ用ポートと L2-SW を追加接続しているので，L2-SW と音声 FS の同時障害に対しても，強い構成になっているね。
N 君：はい。構成をいろいろ検討することができ，よい勉強になりました。

このようにして，M 氏と N 君は，L2-SW と音声 FS の同時障害にも強い音声 FS のネットワーク接続を設計することができた。

以上のように，M 氏と N 君はフォレンジックシステムの設計を終え，システム構築のフェーズに進むことになった。

設問１　〔データ系パケットの採取〕について，(1) ～ (3) に答えよ。

(1) フォレンジックの観点から，Web へのアクセスのアクセス元を特定するために採取すべき情報を，20 字以内で述べよ。

(2) プロキシサーバ経由の場合，当初 N 君が考えていた設置場所（図 1 中の a）では，アクセス元を特定するのに問題となる理由を，50 字以内で述べよ。

(3) N 君は FS を接続する L2-SW の場所を，図 1 中の a から c に変更したが，b ではなく，c を選んだ理由を，35 字以内で述べよ。

設問２　〔音声系パケットの採取〕について，(1) ～ (3) に答えよ。

(1) 本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

(2) 通話先情報について，音声 FS が，RTP パケットから取得できる情報と，SIP パケットからでないと取得できない情報を，それぞれ 25 字以内で述べよ。

(3) 本文中の下線①について，値を指定して使用しているフィールド名を答えよ。

設問３　〔証拠性の確保〕について，(1) ～ (4) に答えよ。

(1) 本文中の下線②について，その理由を，25 字以内で述べよ。

(2) タイムスタンプ要求時に，データそのものを送る代わりにハッシュ値を送るメリットを二つ挙げ，それぞれ 25 字以内で述べよ。

(3) 本文中の下線③について，TST によって保証されることを二つ挙げ，それぞれ 25 字以内で述べよ。

(4) T 社で，TSA にアクセスするプロトコルとして，HTTP を採用するメリットを，25 字以内で述べよ。

設問４　〔データの保存方法・管理方法の検討〕について，(1) ～ (3) に答えよ。

(1) FS がミラーポートから出力されるパケットをすべて採取する方式の場合，図 3 の接続構成では，採取データ量の観点で問題がある。その問題点を，55 字以内で具体的に述べよ。

(2) T 社は WORM 機能を使用することによって，どのようなことを防止しているのか。30 字以内で述べよ。

(3) 複数のファイルをまとめて認証するために，どのような内容を含む一覧表を作成したと考えられるか。30 字以内で述べよ。

設問５　〔音声 FS のネットワーク接続と信頼性の高い音声データ採取方式〕について，(1) ～ (4) に答えよ。

(1) 本文中の [a] 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，音声 FS での音声データの採取又は保存上の不具合を，音声データの通過経路に着目して，35 字以内で述べよ。

(3) VoIP-GW が，データ転送用のポートを決定するために，本文中の下線⑤の判定を必要とする理由は何か。L2-SW$_1$～L2-SW$_4$ の経路制御がどのようになっているかに着目して，25 字以内で述べよ。

(4) N 君が提示した音声 FS を 2 台導入した図 4 中の (2) の最終的なシステム構成は，どのような接続になるか。図 4 中の (1) の表記に倣い，次の規則に従って，解答欄に接続線を図示せよ。

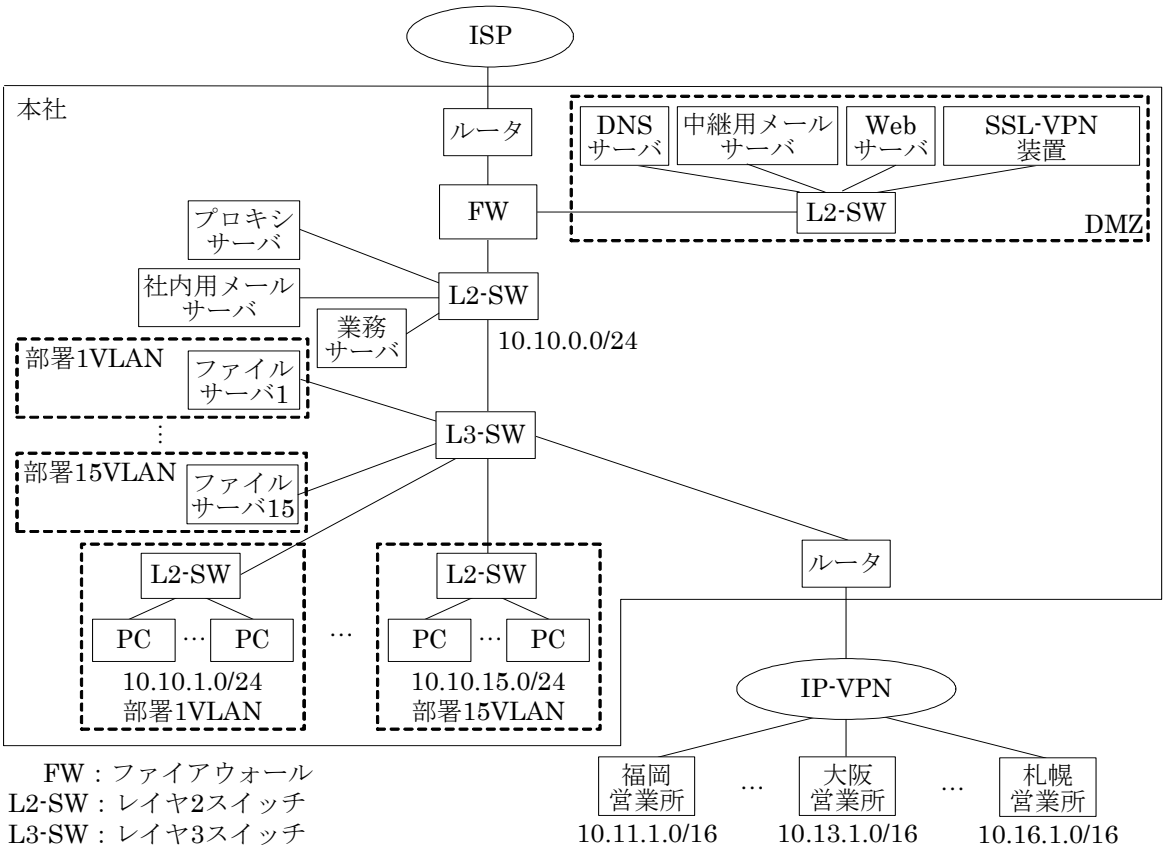
（規則 1）追加する L2-SW$_3$ 及び L2-SW$_4$ のポート番号 4 は，L3-SW$_1$ 又は L3-SW$_2$ との接続に使用すること

（規則 2）音声 FS$_2$ のポート 1 は A 系への接続，ポート 2 は B 系への接続に使用すること

問２　ネットワークシステムの運用管理に関する次の記述を読んで，設問 1～6 に答えよ。

Y 社は，東京に本社があり，全国に 6 か所の営業所をもつ，社員数 300 名の医療機器の輸入販売会社である。Y 社では，200 名の営業員が，全国の各種病院や健康管理センタなどに対して営業活動を行っている。

Y 社では，PC を全社員に配布している。社員は，PC を社内 LAN に接続して，業務に活用している。図 1 に，Y 社のネットワークシステム構成を示す。



注　10.10.0.0/24，10.11.1.0/16 などの表記は，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

〔営業員の活動状況〕

営業員は，朝出社して資料の整理，見積書や提案書の作成などを行った後，外出する。外出すると，直帰になることが多い。外出時には PC を携帯して，顧客先での業務に活用している。営業員の PC にはデータ通信カードが装備され，外出先からインターネットを介して，SSL-VPN 装置経由で Y 社のネットワークシステムを利用している。顧客先では，カタログを利用した商品説明だけでなく，PC を使って，ソリューションの提案や最新の技術情報の提供などを行っている。また，外出時に，報告書や資料の作成なども行っている。営業員は，メーカや顧客などとの連絡や情報交換に，電子メール（以下，メールという）を利用しているので，送受信したメールを各自が分類して，PC のハードディスクに保

存し，管理している。

〔ネットワークシステムの運用状況〕

本社のサーバは，サーバルームに設置されている。営業所にはファイルサーバがあり，オフィス内に設置されている。すべてのサーバのデータは，本社で定期的にテープにバックアップされている。テープには，バックアップ日付やサーバ名などが記載されて，サーバルームに保管されている。

PC には，企業向けウイルス対策ソフトがインストールされ，社内 LAN 接続時に，最新のウイルス定義ファイルが自動的に適用される。PC のハードディスクに保存されているデータ（以下，PC データという）は，ディスク暗号化ソフトによって暗号化されている。

メールは，社内用メールサーバを介して利用できる。社外へのメールは，社内用メールサーバから中継用メールサーバを経由して社外に転送される。社外からのメールは，中継用メールサーバを経由して，社内用メールサーバに転送される。

社外の Web サーバや FTP サーバ，DMZ に設置された Web サーバなどは，本社に設置されたプロキシサーバを経由して利用できる。

FW には，ネットワークシステムの利用のために必要な通信だけを許可する設定が施されている。

〔ネットワークシステム運用管理規程の策定〕

このたび Y 社では，ネットワークシステムの機密性，完全性及び可用性の確保を目的として，セキュリティコンサルティング会社の指導の下に，ネットワークシステムの運用管理規程を作成した。図 2 に，作成されたネットワークシステム運用管理規程を示す。

ネットワークシステム運用管理規程

第 1 章　総則

第 1 条　〔目的〕本規程は，情報資産の機密性，完全性及び可用性を適切に確保するために，ネットワークシステムの管理上及び利用上の取決めを明らかにすることを目的とする。

（省略）

第 2 章　機器の管理

第 7 条　〔社内サーバの管理〕セキュリティ管理責任者は，サーバ及び PC の利用者名，コンピュータ名，機種，OS などを“システム機器管理台帳”に記録し，管理する。

2. セキュリティ管理責任者は，サーバ及び PC のセキュリティパッチの適用を，社員に指示する。

（省略）

第 15 条　〔私有機器の使用〕個人の所有する PC の社内への持込み，及び社内 LAN への接続を禁止する。

（省略）

第 18 条　〔情報漏えい防止対策〕セキュリティ管理責任者は，サーバ及び PC からの機密情報の漏えい防止対策を，社員に講じさせる。

第 3 章　ソフトウェアの管理

第 19 条　〔標準ソフトウェアの使用〕セキュリティ管理責任者は，社内の標準となるソフトウェアを選定し，社員に告知する。

2. 社員は，業務を行う際には標準ソフトウェアを使用する。

3. 社員は，セキュリティ管理責任者の指示に従って，不要なソフトウェアを削除又は無効にし，PC の安全な運用に努める。

（省略）

第 7 章　インターネットの利用

第 30 条　〔利用目的など〕社員は，業務の促進と効率向上を図り，生産性向上のためにインターネットを利用する。

2. 社員によるインターネットの私的利用を禁止する。

（省略）

第 31 条　〔メールの利用〕セキュリティ管理責任者は，メールの利用者に対し，次の事項について指示する。

① 使用するメールソフト
② メールソフトの設定
③ メールアドレスの設定

2. 社員は，セキュリティ管理責任者の指示に従って，メールを適切に利用する。また，Web サーバで提供されるメールの利用は禁止する。

（省略）

第 8 章　情報システムの運用

第 40 条　〔データのバックアップ〕セキュリティ管理責任者は，重要なデータのバックアップを行う。さらに，バックアップデータを適切に管理することによって，システム障害，事故，災害などが生じた場合に，情報システムの停止，業務の中断などの問題を最小限に抑える。

（以下，省略）

図２　ネットワークシステム運用管理規程

セキュリティ管理責任者の H 部長は，運用管理規程にのっとった運用を確立するために，システム運用課の K 課長に，現在のネットワークシステム運用管理上の問題点の洗出しと改善策の立案を指示した。

〔問題点の洗出し〕

K 課長は，ネットワーク運用担当の S 係長とともに，最初に問題点の洗出しを行った。その結果，次の問題点が挙げられた。

・PC データが，バックアップされていない。
・インターネットの私的利用が行われている。
・添付ファイル付きメールの社外への送信や USB メモリの利用によって，情報漏えいの危険性がある。
・PC へのセキュリティパッチ（以下，パッチという）の適用が適時に行われていない。
・業務に不要なソフトウェアが PC にインストールされ，使用されている。
・災害の発生を想定したバックアップデータの管理が行われていない。

K 課長と S 係長は，これらの問題点の解決方法を検討し，次の改善案をまとめた。

〔改善案〕

（1）PC データのバックアップ

PC データのバックアップには，クライアントバックアップシステムを導入する。クライアントバ

ックアップシステムは，バックアップサーバ（以下，BU サーバという）と，PC にインストールされるエージェントから構成される。

クライアントバックアップシステムによるバックアップは，初回バックアップと差分バックアップの 2 段階で行われる。初回バックアップは，PC にエージェントがインストールされたときに行われ，指定されたフォルダ内のすべてのファイルが，BU サーバにバックアップされる。その後は，差分データだけがバックアップされる，差分バックアップが行われる。差分バックアップは，(a)ログイン時及びログアウト時，(b)ファイル更新時，(c)指定時刻の 3 種類の方式から一つを選択する。

差分データは，PC のディスクに設定されたバックアップフォルダにいったん記録され，選択された方式で BU サーバにバックアップされる。バックアップできないときには，バックアップできるまでバックアップフォルダに蓄積される。(a)の場合はログイン時及びログアウト時に，(b)の場合はファイルの更新時に，(c)の場合は指定された時刻に，そのときまでに蓄積された差分データがまとめてバックアップされる。営業員による PC の利用形態を考慮すると，①(a)の方式では，業務開始時にログインが集中するので，バックアップ時間の増大が考えられ，②(c)の方式では，長期間バックアップされない問題が考えられる。K 課長と S 係長は，これらの状況を基に，(b)の方式で差分バックアップを行うことにした。また，バックアップデータ量が大量にならないことから，機器やソフトウェアの購入費，［　a　］費及び保守，運用費を抑えるために，BU サーバは，本社に 1 台だけ設置することにした。

(2) インターネットの私的利用の制限と添付ファイル付きメールの社外への送信制限

インターネットの私的利用の制限と添付ファイル付きメールの社外への送信制限には，Web とメールのフィルタリングシステムをそれぞれ導入する。

Web のフィルタリングシステムを構成する Web フィルタリングサーバ（以下，WF サーバという）は，Web サーバへの接続の遮断を，URL フィルタリングと，指定された語句の組合せによるコンテンツのスキャニングによって行う。WF サーバは，HTTP と FTP のプロキシサーバとしても機能するので，既設のプロキシサーバと置き換え，PC の設定変更を不要にする。

メールのフィルタリングシステムを構成するメールフィルタリングサーバ（以下，MF サーバという）は，SMTP で転送されたメールを受信し，検査条件に基づいて検査を行う。検査条件は，指定された語句の組合せがメールに含まれるか，ファイルが添付されているか，などである。MF サーバが受信したメールは，あらかじめ指定された転送先に SMTP で転送されるが，検査の結果，不適正と判断されたメールは MF サーバに蓄積される。蓄積されたメールから，メールの利用者が［　b　］を遵守しているかどうかを評価できる。MF サーバでは，社内から社外へのメールだけを中継させる。

(3) USB メモリの使用制限と PC のポリシ適合制御

USB メモリの使用制限と PC のポリシ適合制御（不要ソフトのアンインストール指示，パッチの適用など）には，PC 構成管理システムを導入する。PC 構成管理システムは，PC のポリシ適合制御機能（パッチ配布，ポリシ不適合の警告，通信の遮断など）をもつ構成管理サーバ（以下，CM サーバという）と PC にインストールされるエージェントから構成される。図 3 に，PC 構成管理システムによる PC のポリシ適合制御方法を示す。

(i)　PCの識別子と構成情報の送信
(ii)　PCのポリシ適合状態のデータベース化
(iii) 送受信されるパケットのキャプチャ
(iv) パッチの適用
(v)　ポリシ不適合の警告表示指示
(vi) 未登録PCの警告表示指示
(vii)通信の遮断

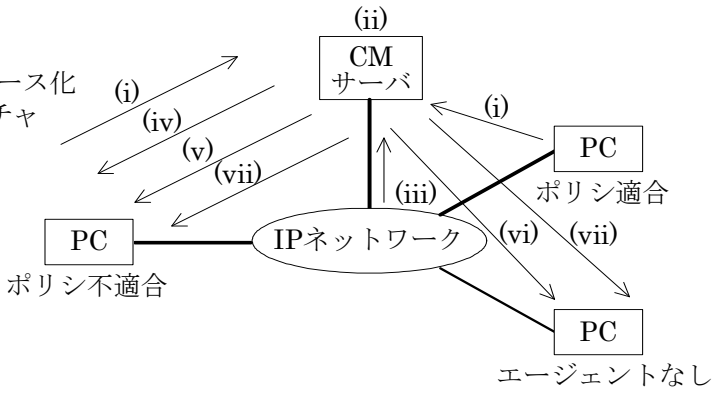


図３　ＰＣ構成管理システムによるＰＣのポリシ適合制御方法

PC のポリシ適合状態データベース（以下，DB という）は，次の手順で作られる。PC の稼働時とあらかじめ設定されたタイミングに，エージェントが，PC の識別子と構成情報を CM サーバに送信する。CM サーバは，受信した情報を基に PC のポリシ適合状態をチェックし，DB を更新する。同一識別子の情報が DB に登録されているときは当該レコードを更新し，未登録のときには追加登録する。また，CM サーバは，エージェントがインストールされていない PC の検出精度を高めるために，③DB のレコードを，一定時間後に削除する。MAC アドレスや④IP アドレスだけでは，PC を特定できない可能性があるので，識別子は，エージェントがインストールされたとき，MAC アドレスとそのときの時刻を基に自動生成され，PC に記録される。表 1 に，DB の登録レコードの例を示す。

表１　ＤＢの登録レコードの例（抜粋）

コンピュータ名	識別子	IP アドレス	パッチ	不要ソフト
chiyo	abc10	10. 10. 1. 6	1	1
ofuku	xc150	10. 10. 1. 12	1	1
bunshiro	zdwjkl	10. 10. 1. 3	0	0

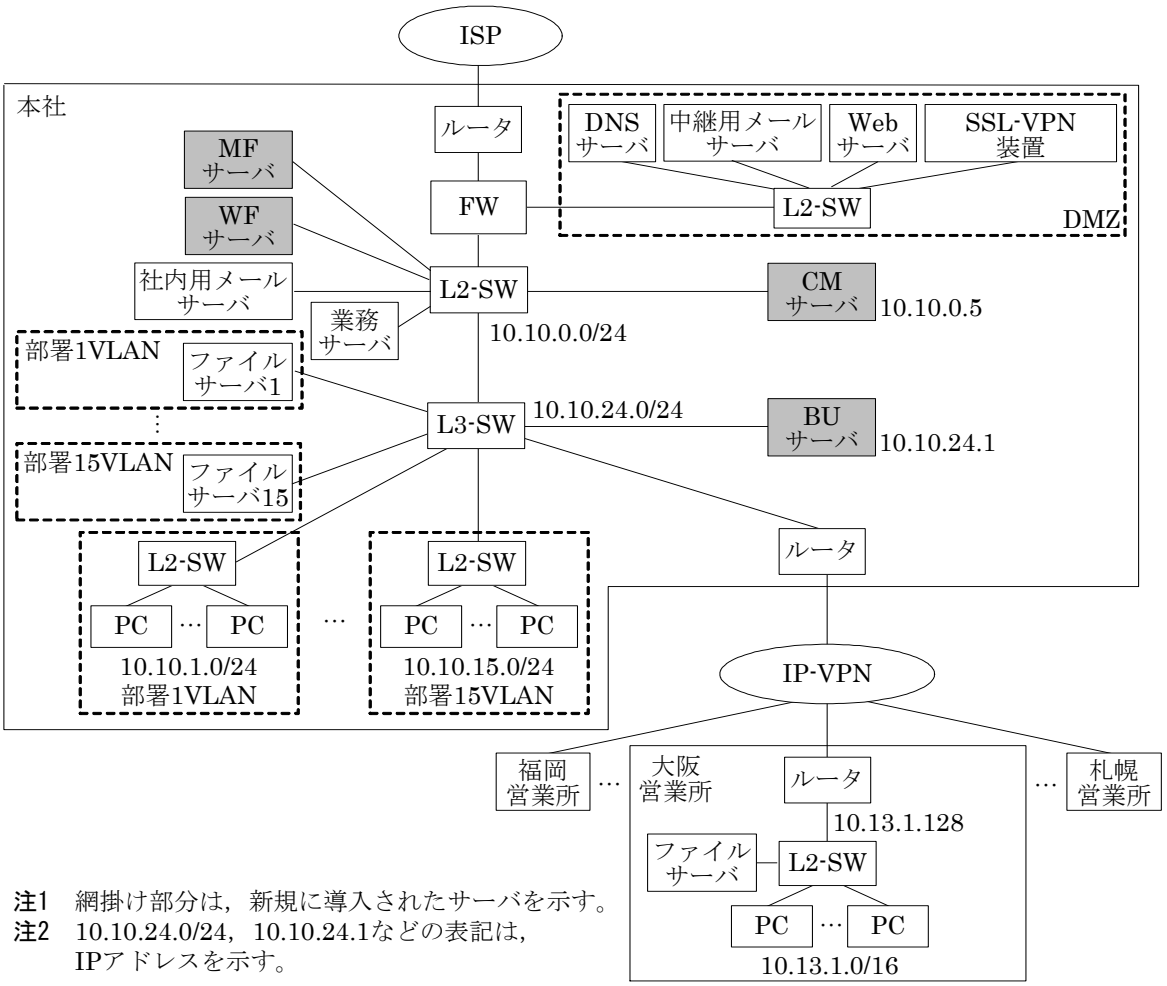
1：ポリシ適合
0：ポリシ不適合

CM サーバは，常時，送受信されるパケットをキャプチャし，キャプチャしたパケットの［　c　］をキーとして DB を検索し，PC のポリシ適合状態をチェックする。パッチのポリシ不適合の PC に対しては，CM サーバによってパッチが自動適用され，DB の当該レコードが更新される。不要ソフトのポリシ不適合の PC に対しては，その旨の警告が表示される。また，キャプチャしたパケットを送信した PC の識別子と構成情報が DB に未登録のときには，その PC にはエージェントがインストールされていないので，当該 PC に対しては，未登録 PC の警告が表示される。これらの警告が表示された不正な PC から保護サーバリストに登録されているサーバへのアクセスは，CM サーバによって遮断される。保護サーバリストには，不正な PC からのアクセスを禁止するサーバが登録されている。本改善案では，社外の Web サーバや FTP サーバ，DMZ に設置された Web サーバとの通信を遮断し，インターネットの利用を制限する。

USB や［　d　］1394 インタフェースで接続される外部記憶装置の使用は，エージェントによ

って禁止される。

K課長は，前記（1）～（3）の改善案を基に改善策をまとめ，H部長に報告した。検討の結果，改善策の実施が決定された。図4に，改善策実施後のネットワークシステム構成を示す。



注1　網掛け部分は，新規に導入されたサーバを示す。
注2　10.10.24.0/24，10.10.24.1などの表記は，IPアドレスを示す。

図4　改善策実施後のネットワークシステム構成

〔各システムの導入作業と動作テスト〕

各システムの導入作業と動作テストは，休日に，本社と情報システム担当者がいる大阪営業所で実施した。表2に，導入システムと各導入システムの作業項目・作業手順を示す。

表２　導入システムと各導入システムの作業項目・作業手順

項番	導入システム名	作業項目	作業手順
1	クライアントバックアップシステム	1.1 BU サーバのセットアップ	必要情報の設定など
		1.2 BU サーバの社内 LAN への接続	①L3-SW に接続 ②L3-SW の設定変更
		1.3 既設 PC にエージェントを導入	本社と大阪営業所でインストールと設定
		1.4 バックアップのテスト	初回バックアップと差分バックアップのテストと結果の評価
2	Web のフィルタリングシステム	2.1 WF サーバのセットアップ	必要情報の設定など
		2.2 WF サーバの社内 LAN への接続	①［　作業 1　］ ②L2-SW に接続
		2.3 Web フィルタリングのテスト	テストと結果の評価
3	メールのフィルタリングシステム	3.1 MF サーバのセットアップ	①メールの転送先を［　ア　］に設定 ②添付ファイル付きメールの扱いを定義 ③そのほかの必要情報の設定など
		3.2 MF サーバの社内 LAN への接続	L2-SW に接続
		3.3 社内用メールサーバの設定変更と関連作業	①メールの転送先を［　ア　］から，［　イ　］に変更 ②FW の設定変更
		3.4 メールフィルタリングのテスト	テストと結果の評価
4	PC 構成管理システム	4.1 CM サーバのセットアップ	必要情報の設定など
		4.2 CM サーバの社内 LAN への接続	①L2-SW に接続 ②L2-SW の設定変更
		4.3 テスト用に準備した PC（以下，テスト用 PC という）にエージェントを導入	本社と大阪営業所でインストールと設定
		4.4 PC 構成管理システムのテスト	①DB 内容の確認 ②パッチ適用の確認 ③ポリシ不適合の警告の確認 ④未登録 PC の警告の確認 ⑤［　作業 2　］ ⑥［　ウ　］機能を稼働 ⑦テストと結果の評価 ⑧［　ウ　］機能を停止

各システムの導入作業時と動作テスト時に発生した問題と対応内容を，次に示す。

(1) クライアントバックアップシステム導入作業時の問題

大阪営業所の既設 PC を使って，表 2 中の作業項目番号 1.4 の作業を行ったところ，エラーが発生した。そこで，本社の既設 PC で同じ作業を行ったが，同様のエラーが発生した。障害発生箇所を特定するために，本社の既設 PC で，BU サーバあてに ping コマンドを発行したところ，タイムアウトエラーになった。そこで，本社の既設 PC から L3-SW に［　e　］して，L3-SW から BU サーバあてに再度，ping コマンドを発行したところ，BU サーバからの応答があった。BU サーバの設定情

報を調査した結果，⑤設定の間違いが判明し，これを修正して問題が解決した。

(2) PC 構成管理システム導入作業時の問題

本社で，テスト用 PC を社内 LAN に接続して，表 2 中の作業項目番号 4.4 の作業を行い，次に，大阪営業所で，大阪営業所のネットワークの設定情報を基に，テスト用 PC に必要項目の設定を行った。確認のために，大阪営業所の既設 PC とテスト用 PC の設定内容を比較したところ，サブネットマスク値が異なっていることが判明した。表 3 に，既設 PC とテスト用 PC の設定内容を示す。

表３　既設ＰＣとテスト用ＰＣの設定内容

設定項目	既設 PC	テスト用 PC
IP アドレス	10. 13. .1. 1	10. 13. 1. 100
サブネットマスク	255. 0. 0. 0	255. 255. 0. 0
デフォルトゲートウェイ	10. 13. 1. 128	10. 13. 1. 128

調査の結果，⑥大阪営業所の既設 PC のサブネットマスクが，クラス A のネットマスク値のままであったことが判明した。そこで，大阪営業所のすべての既設 PC の設定内容を確認し，正しい値に変更した。その後，テスト用 PC を大阪営業所の社内 LAN に接続して，表 2 中の作業項目番号 4. 4 の作業を行い，すべての機能が問題なく動作することを確認した。

各システムの導入作業と動作テストが完了したので，全社の PC にエージェントを導入し，改善策実施後のネットワークシステムを稼働させた。

本改善策によって，問題点の解消に効果が見込める。しかし，この効果を，より確実なものとするには，運用時に行わなければならない作業がある。また，改善策では解消されない問題点も残っているので，これについては別途対策が必要である。そこで，K 課長と S 係長は，運用時に行わなければならない作業と対策を，H 部長に報告した。H 部長は，実施すべき作業と対策を，該当部署の責任者に指示し，実施に移させた。

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　PC データのバックアップについて，(1)，(2) に答えよ。

(1) 本文中の下線①のバックアップ時間の増大が発生する状況を，45 字以内で述べよ。

(2) 本文中の下線②は，どのような PC の利用形態で発生するか。40 字以内で述べよ。

設問３　図 4 の構成にしたとき，FW の設定変更が必要になる。この変更で，新たに禁止すべき通信と許可すべき通信を，それぞれ 25 字以内で述べよ。

設問４　PC のポリシ適合制御について，(1) ～ (5) に答えよ。

(1) 本文中の下線③が行われないとき，エージェントがインストールされていない PC を検出できないことがある。それはどのような場合か。30 字以内で述べよ。

(2) 本文中の下線④の理由を，20 字以内で述べよ。

(3) 保護サーバリストに登録すべきサーバ名を答えよ。

(4) CM サーバを接続するポートは，どのポートのミラーポートに設定すべきか。図 4 中の機器名を用いて，20 字以内で述べよ。

(5) CM サーバが PC とサーバ間の通信を遮断する方法を，TCP のフラグフィールドに着目して，40 字以内で述べよ。

設問５　〔各システムの導入作業と動作テスト〕について，(1) ～ (4) に答えよ。

(1) 表 2 中の［作業 1］，［作業 2］を，それぞれ 20 字以内で答えよ。

(2) 表 2 中の［ア］～［ウ］に入れる適切な字句を答えよ。

(3) 本文中の下線⑤の間違えた設定項目を，20 字以内で述べよ。

(4) 本文中の下線⑥の問題があったが，本社のサーバは利用できた。この理由を，PC から本社のサーバへの接続手順を基に推定して，60 字以内で述べよ。

設問６　改善策実施後の運用について，(1)，(2) に答えよ。

(1) 図 2 中の第 40 条に対応させるために，バックアップデータの管理面で実施すべき対策を，40 字以内で述べよ。

(2) メールによる情報漏えいを防止するために，MF サーバの運用時に定期的に実施すべき作業を，60 字以内で述べよ。