平成１７年度　秋期　ﾃｸﾆｶﾙｴﾝｼﾞﾆｱ（ネットワーク）　午後Ⅱ問題

問１　ネットワークのセキュリティ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，社員数が 300 名で 200 社の販売代理店をもつ，電子機器卸販売会社である。本社は東京にあり，大阪と名古屋に営業所をもち，大阪営業所には 40 名，名古屋営業所には 20 名の社員が勤務している。本社と営業所の LAN（以下，社内 LAN という）は，広域イーサネットサービス（以下，広域イーサという）を利用して接続されている。社内 LAN は，一つのネットワークアドレスで運用されている。社内 LAN には，各種のサーバ，パソコン（以下，PC という）が接続され，ネットワークシステムを構成している。図 1 に，Y 社のネットワークシステム構成を示す。

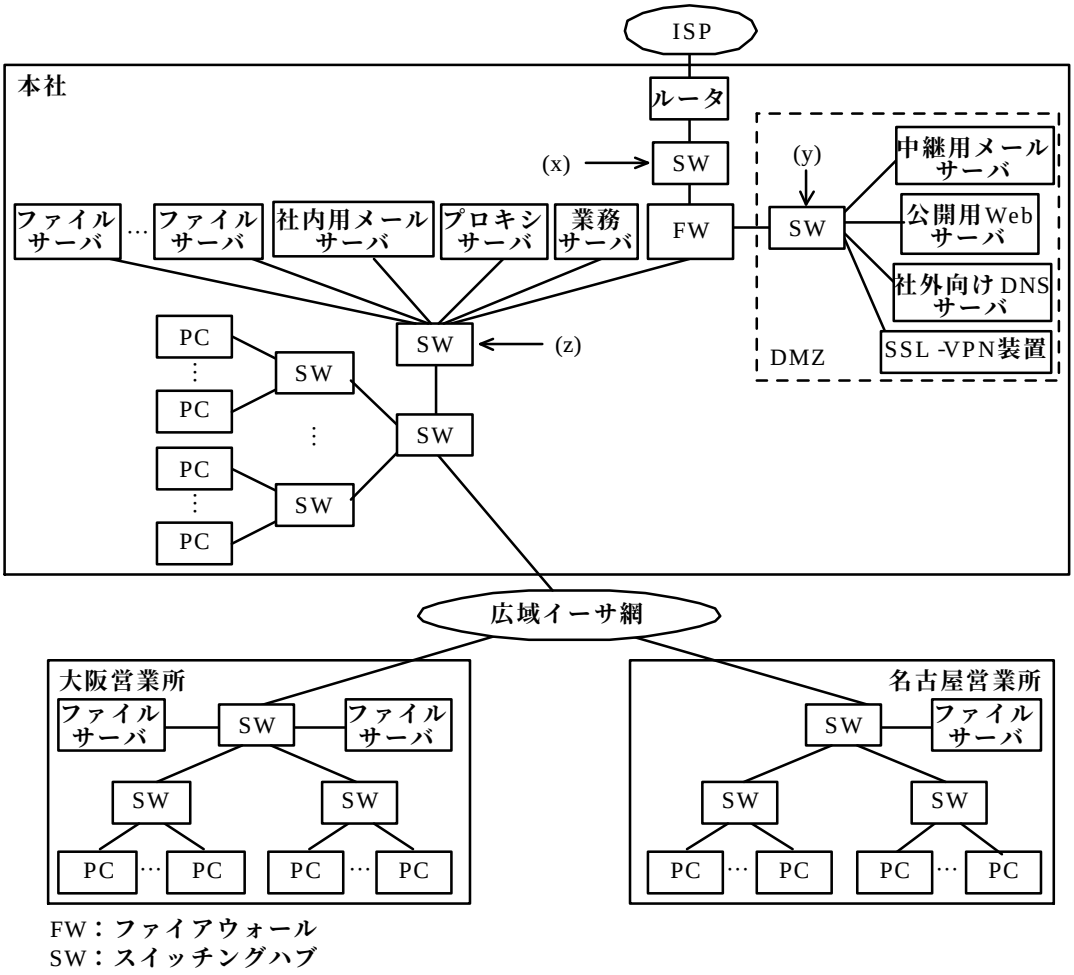


図１　Ｙ社のネットワークシステム構成

〔ネットワークシステムの運用方法〕

Y 社では，全社員向けに PC を導入し，社内 LAN に接続して業務に利用している。100 名の営業員は客先に PC を携帯して，プレゼンテーションを行ったり，商品情報検索，在庫確認，受注処理などの業務システムを利用したりしている。

また，Y 社では，本社からインターネットに接続しており，営業所からも広域イーサ網経由でインターネットを利用できる。FW の社内側に社内用メールサーバが設置され，本社と営業所の社員は，社内用メールサーバから電子メール（以下，メールという）を受信するとともに，社内用メールサーバを介して社内外にメールを送信している。DMZ には，社外とのメール送受信を中継する中継用メールサーバ，公開用 Web サーバ，社外向け DNS サーバ及び SSL-VPN 装置が設置されている。SSL-VPN 装置は，業務サーバで稼働する業務システムをインターネット経由で利用するためのものである。社内 LAN からは，メールのほかに，Web や FTP を使ったファイル転送を利用できる。Web や FTP を使ったファイル転送の利用は，プロキシサーバを介して行われる。

PC には，IP アドレスなど，ネットワーク利用に必要な情報が固定的に設定されている。大阪営業所と名古屋営業所の社員は，営業所内のファイルサーバのほか，本社に設置されている各種のサーバを利用している。また，本社に出張したときには，携帯した PC を本社の LAN に接続して業務を行っている。営業員が，社外から業務システムを利用するときには，SSL-VPN 装置に接続して認証を受けた後，業務システムが利用可能になるとともに，通信データは暗号化される。

社内用メールサーバではウイルス対策ソフトが稼働し，社内外から転送されたメールのウイルスチェックを行っている。また，プロキシサーバでもウイルス対策ソフトが稼働しており，HTTP と FTP によるウイルス侵入を防御している。さらに，PC にもウイルス対策ソフトがインストールされている。ウイルス定義ファイルの更新や OS のセキュリティパッチの適用が必要になったときには，情報システム部の担当者が全社員にその旨を告知して，更新を促すようにしている。この作業の必要性と方法については，ウイルス対策ソフトの導入時に，情報システム部が全社員向けに説明会を開催し，その後は新入社員教育の一環として実施している。

〔セキュリティ問題の発生〕

Y 社では，最近二つのセキュリティ問題に直面し，解決策の検討を迫られた。一つ目は，メールによる情報漏えいの問題である。営業員及びそのほかの一部社員にアクセスが許可されている社外秘の仕切り率に関する情報が流出し，複数の販売代理店からクレームが付き，対応に苦慮した。メールによる流出が想定されたが，経路と当事者を特定できず，厳格な処置を行うことができなかった。

二つ目は，社内 LAN のウイルス被害の問題である。営業員が利用している PC から，ウイルスが社内 LAN に侵入し，丸 1 日ネットワークシステムが停止するという被害が発生した。

これらの問題に対する反省から，メールによる情報漏えいとウイルスによるネットワークシステム停止の被害を防止するための対策を検討することになり，情報システム部の M 課長は，ネットワークインフラ担当の N 係長に対策案の検討を指示した。

〔被害額の試算〕

N 係長は，今回発生したセキュリティ問題の被害額を試算することにした。まず，メールによる情報漏えいの被害の大きさについて検討した。関係者にヒアリングした結果，次のことが判明した。

・問題を終息させるために，営業部長を始め複数の営業員が合計 5 日程度の工数を費やした。
・複数の販売代理店から仕切り率の見直しを求められ，2 社の販売代理店に対して仕切り率を下げざるを得なくなった。この見直しによって，年に 300 万円程度の減収が予想される。

次に，ウイルスによるネットワークシステム停止の被害額を，図 2 に示す被害額算出モデルを基に試算した。

ウイルスによる一次的被害額 ＝（表面化被害額）＋（潜在化被害額）
（1）表面化被害額 ＝（逸失利益）＋（システム復旧コスト）
＝（a1×a2）＋（a3×a4×a5＋a6）
（2）潜在化被害額＝（システム停止中の業務効率低下コスト）
＋（復旧作業に係る一般業務コスト）
＝（b1×a2×a7×b3）＋（b1×b2×a7）

図２　被害額算出モデル

ここで，図 2 中の項目 a1～a7 及び b1～b3 の説明を次に示す。

al：時間当たりの利益（円）
a2：システム停止時間（時間）
a3：（システム管理部門の）時間当たりの人件費（円）
a4：システム復旧所要時間（時間）
a5：システム復旧所要人数（人）
a6：代替ハードウェアとソフトウェアの購入費（円）
a7：ウイルス被害の影響を受けた人数（人）
b1：（業務部門の）時間当たりの人件費（円）
b2：業務復旧所要時間（時間）
b3：業務効率低下割合

N 係長は被害状況を次のように整理し，被害額の試算条件とした。

・ウイルス侵入によって，ネットワークシステム全体が 8 時間停止した。ウイルスに感染した PC は 40 台で，ネットワークシステム復旧後に PC のウイルス駆除作業が行われたので，この PC の使用者 40 名は，平均 12 時間 PC を使用した業務を行うことができなかった。
・ネットワークシステム復旧と PC のウイルス駆除などのシステム復旧作業は，情報システム部員 2 名が担当し，16 時間を要した。
・ネットワークシステム停止やウイルス感染の被害を受けた社員は 250 名で，これらの社員は，ネットワークシステムや PC の復旧後に，業務を正常に行えるようにするためのデータの入力や整合性チェック，メールの処理などの業務復旧作業に，平均 4 時間を費やした。
・人件費は各部門とも同額で，時間当たり 4,000 円であり，ネットワークシステム停止による業務効率

低下割合は，0.3 である。

・逸失利益は発生せず，また，復旧のための代替ハードウェア及びソフトウェアも購入しなかった。

これらの条件を基に，ウイルスによる一次的被害額を試算したところ，表面化被害額は 128,000 円であったが，潜在化被害額が 6,592,000 円になった。

情報漏えいとウイルスによる被害額が予想以上に大きかったので，N 係長は，今後もこのような被害を発生させないための対策に，ある程度の投資が必要であると判断した。

〔メールによる情報漏えいの防止対策〕

まず，N 係長は，メールによる情報漏えいの防止対策を検討した。技術的防止策としてメールフィルタリングシステムを検討したが，情報漏えいの防止精度を高めるための作業負荷が大きく，現在の体制では導入は困難と判断した。ファイルの添付を禁止することも検討したが，何人かの社員に聞いた限りでは，業務に支障を来すという意見が多く，採用は困難と考えられた。

幾つかの防止対策を検討した結果，管理面の対策を強化して技術面の対策と併せて実施するのがよいと判断した。そこで，管理面の対策として，取引記録のような営業秘密，投資計画のような機密情報及びセミナ参加者リストのような［　ア　］など，企業として守るべき情報を洗い出し，これらを利用できる社員を必要最低限に抑えるとともに，情報へのアクセス制御を厳密に行うことにした。さらに，メールの運用規程を作成し，メール監査も併せて実施する旨を社員に周知することで，抑止力を高めながら規程に準じた運用に導く取組を提案することにした。一方，技術面の対策として，メール監査のために，送受信されるメールをアーカイブして送受信履歴を確実に保存できる，メール収集システムを導入することにした。

メール収集システムには，収集したメールの中から複数の条件による検索，メール内容の表示，各種分析など，監査のための機能が装備されている。収集の方式には，中継型，トラフィックモニタ型（以下，モニタ型という）などがある。中継型とは，SMTP を使っていったんメールを受信し，受信データを記憶装置に記録するとともに，指定された転送先に転送する方式である。一方，モニタ型は，LAN に流れているメール関連のパケットを抽出して，これを記憶装置に記録する方式である。両方式とも，それぞれ長所と短所があるが，送受信されるすべてのメールを収集するために，モニタ型を採用することにした。

モニタ型のメール収集システムで，送受信されるすべてのメールを収集するためには，メール関連パケットの抽出を無停止で行う必要がある。また，抽出処理と監査関連処理を同時に行わなければならない。そのため，これらの処理をそれぞれ異なるサーバで稼働させ，パケット抽出装置とメール監査装置としてそれぞれ独立させることを考えた。このような構成にするためには，2 台のサーバが，収集したメールを保存する磁気ディスク装置（以下，ディスクという）を共有できなければならない。これは，SAN（Storage Area Network）や［　イ　］を用いることによって可能になる。SAN は，ファイバチャネルスイッチによって構成される，ストレージ共有のためのネットワークである。［　イ　］は LAN に接続され，ファイル共有プロトコルを用いてファイル共有を可能にするストレージである。ディスクの共有は，これまでの業務経験から，運用しやすい［　イ　］を採用することにした。図 3 に，モニタ型のメール収集システム構成を示す。

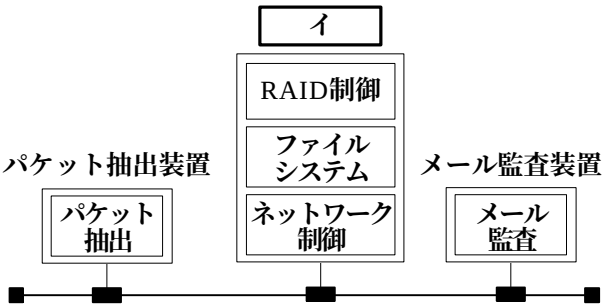


図３　モニタ型のメール収集システム構成

モニタ型のメール収集システムでは，保存したデータに証拠能力をもたせるために，保存したデータが［　ウ　］されていないことと，データの作成日時の正当性を併せて証明できるようにしている。これらは，電子署名及び作成日時を示す［　エ　］の付加によって実現されている。

〔ウイルスによるネットワークシステム停止の防止対策〕

ウイルスによるネットワークシステム停止の防止対策として，PC の接続規制，状態検査及び治療処理（以下，これらを検疫処理という）を行うことを考えた。

接続規制としては，PC を社内 LAN に接続してネットワークシステムを利用するときに，利用者を認証する方式を採用する。利用者認証には，IEEE 802.1x を用いることにした。図 4 に，IEEE 802.1x の認証手順の概略を示す。

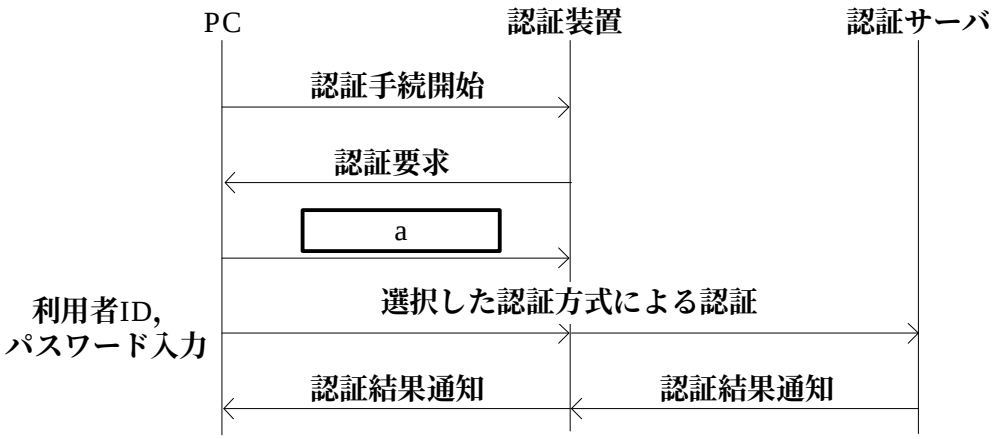


図４　IEEE 802.1x の認証手順の概略

IEEE 802.1x では，認証プロトコルである EAP（Extensible Authentication Protocol）での認証要求を行うために，PC に実装される［　オ　］，認証装置及び認証サーバが使用される。IEEE 802.1x では複数の認証方式を利用できるが，運用の容易性を考えて，①利用者認証に電子証明書を使用する EAP-TLS ではなく，利用者 ID とパスワードを使用する EAP-PEAP を利用することにした。

PC の接続規制方式の検討後，N 係長は，IEEE 802.1x による認証と，動的 VLAN 機能をもつ認証スイッチングハブ（以下，認証 SW という）を利用した検疫システムの提案を，SI 業者の T 氏に求め

た。図5に，T氏から提案された検疫システムの構成を示す。

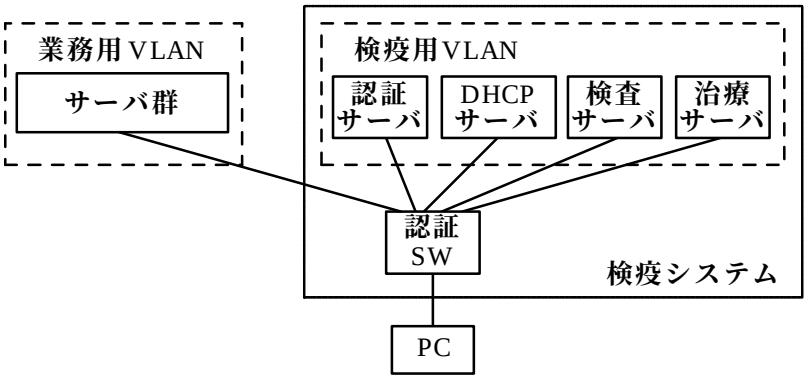


図５　T氏から提案された検疫システムの構成

T氏の提案は，PCのセキュリティ基準への適合状態を検査サーバによって検査し，適切なセキュリティ対策が実施されていないときには，治療サーバによって，セキュリティ基準に適合した対策をPCに施すというものであった。

図5を基に，T氏が説明した利用者認証，ネットワーク情報の配布，及び検疫処理手順の一部を，次に示す。

(1) PCは起動後，認証手続を開始する。

(2) PCに認証画面が表示され，PCの使用者は，画面指示に従って利用者IDとパスワードを入力する。

(3) 認証SWは，受信したデータを基に，認証サーバに対して認証要求を行う。正当なPC使用者と認証されたとき，認証サーバは認証SWに認証許可を通知する。

(4) 認証SWは，PCに認証許可を通知する。

(5) PCは，DHCPサーバに対してIPアドレスなどの必要な情報の配布を要求する。

(6) DHCPサーバが，PCに必要な情報を配布する。

(7) 検査サーバは，PCのOSの［　カ　］とウイルス対策のための［　キ　］の適用状態を検査し，検査結果をPCに表示させるとともに，認証サーバに通知する。検査結果がセキュリティ基準に適合していたときに，手順(10)に移る。

(8) セキュリティ基準に適合していないときには，PCにセキュリティのぜい弱性が表示されるので，PCの使用者は，治療用サーバから［　カ　］と［　キ　］の更新を受けるための操作を行う。

(9) 治療用サーバは，更新処理後にPCに対してウイルスチェックを指示する。ウイルスチェックが終了すると，PCに再起動を指示するとともに，検疫処理の完了を認証サーバに通知する。PCは，再起動によって手順(1)に戻る。

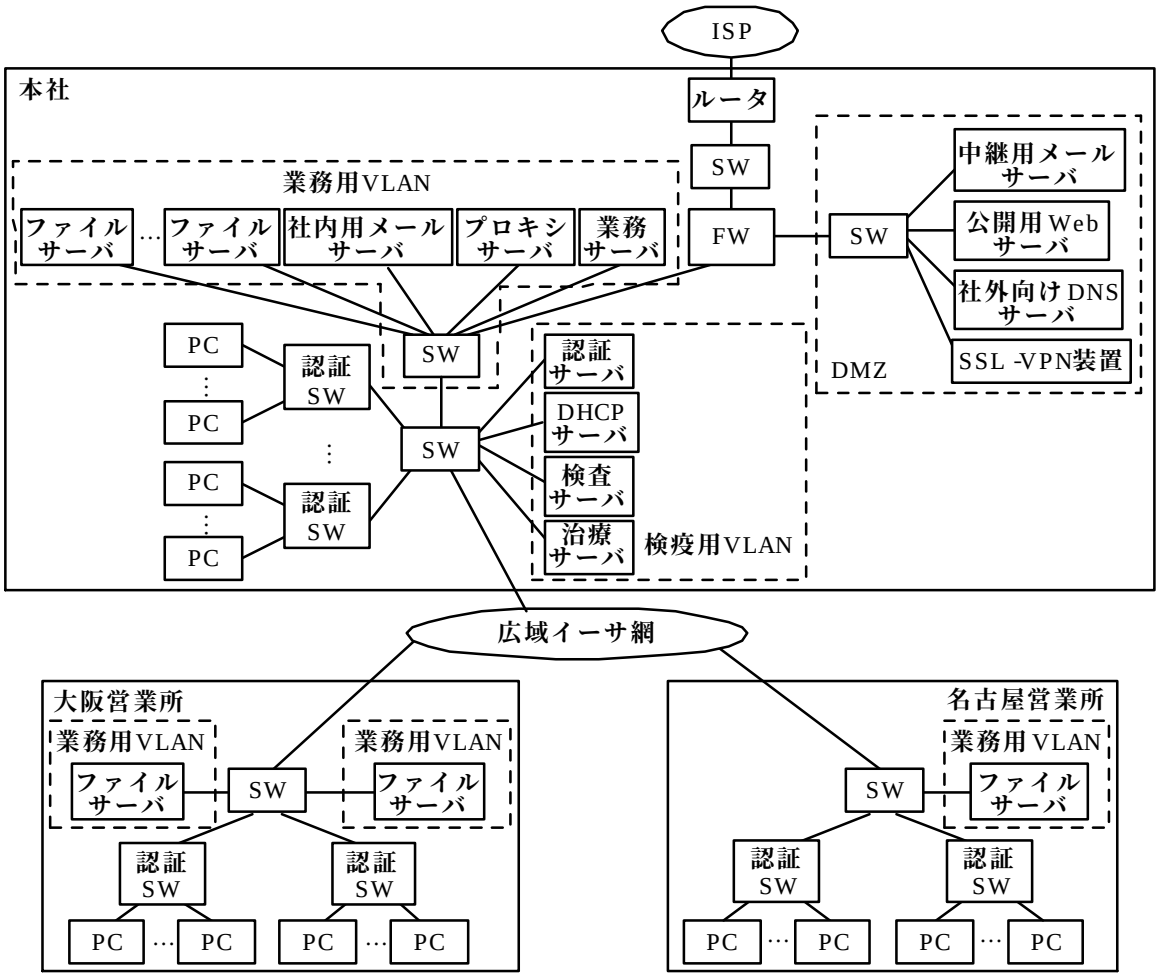
(10) ②認証サーバと認証SWの処理によって，認証SWに設定されたPCが所属するVLANが，［　b　］から［　c　］に変更される。

(11) PCは，ネットワークシステムを利用できる。

図5中の検疫システムでは，セキュリティ状態を維持するために，認証SWに設定されたVLANと，認証サーバが保持する認証許可状態の初期化が必要である。PCの終了処理が正常に行われたときには，PCでVLANリセットのための処理が実行されるので，VLANと認証許可状態が初期化される。しかし，PCの終了処理が正常に行われないときは，PCでVLANリセットのための処理が実行されないので，認証SWがVLANと認証許可状態を初期化できない。その結果，一度認証許可されると，検疫処理が行われなくてもネットワークシステムを利用できるという問題が発生する。この問題を解決するために，③認証SWは，配下のPCの状態を監視する機能をもっている。

〔新ネットワークシステム構成〕

以上の検討を基に，N係長は，メール収集システムと検疫システムを導入する対策案をまとめた。これらのシステムの導入によって，メールによる情報漏えいの抑止や検出と，ウイルスの侵入を防止できるが，④これら以外にも，ネットワークシステムの運用上の効果が得られる。図6に，対策案を盛り込んだ新ネットワークシステム構成を示す。



注　メール収集システムは設問の関係で省略している。

図6　対策案を盛り込んだ新ネットワークシステム構成

図 6 の構成の場合，ウイルスに感染した PC が接続されたとき，本社では検疫処理が，営業所ではインターネット利用，本社のサーバを使用した業務処理及び検疫処理が影響を受ける危険性がある。しかし，この構成によって投資額を低く抑えられるとともに，ウイルス対策に関しても⑤本来の目的を達成できるので，採用することに決めた。

以上のような結論に達したので，N 係長は，この対策案を M 課長に報告することにした。

設問１　本文中の［　ア　］～［　キ　］に入れる適切な字句を答えよ。

設問２　メール収集システムについて，(1)～(3) に答えよ。

(1) 中継型メール収集システムを設置する場合，FW 以外に設定内容の変更が必要になる機器を，図 1 中から二つ選び答えよ。

(2) Y 社で送受信されるすべてのメールが収集できるパケット抽出装置の設置場所を，図 1 中の(x)～(z) の中から選び答えよ。また，この装置を設置するときに実施しなければならない SW の設定内容を，50 字以内で述べよ。

(3) 図 3 のシステムを導入する場合は，トラフィックの観点から LAN 構成上の考慮が必要である。考慮すべき内容を，50 字以内で述べよ。

設問３　ウイルス被害とその対策について，(1)，(2) に答えよ。

(1) ウイルス感染によって発生した，復旧作業に係る一般業務コスト（円）を答えよ。

(2) ウイルス被害を発生させた運用面の問題点を，50 字以内で具体的に述べよ。

設問４　利用者認証について，(1)～(3) に答えよ。

(1) 図 4 中の［　a　］の応答処理で送信される，認証を受けるために必要な情報を，15 字以内で述べよ。

(2) 本文中の下線①で，管理者の運用負荷が大きい作業内容を二つ挙げ，それぞれ 15 字以内で述べよ。

(3) 利用者認証のためのプロトコルが位置する層を，OSI 基本参照モデルの名称で答えよ。また，T 氏が説明した手順の中から，その判断根拠を，20 字以内で述べよ。

設問５　対策案を盛り込んだ新ネットワークシステムについて，(1)～(5) に答えよ。

(1) 本文中の下線②の処理で，認証サーバが認証 SW に対して行う処理内容を，30 字以内で述べよ。

(2) 本文中の［　b　］，［　c　］に入れる適切な字句を答えよ。

(3) 本文中の下線③の監視方法を二つ挙げ，それぞれ 20 字以内で述べよ。

(4) 本文中の下線④の効果を二つ挙げ，それぞれ 20 字以内で述べよ。

(5) 本文中の下線⑤の本来の目的を，対象となる機器とともに，40 字以内で具体的に述べよ。

問２　ネットワークの運用管理に関する次の記述を読んで，設問 1～5 に答えよ。

S 社は，情報機器の卸販売会社である。社員数は 300 人で，本社は東京にある。営業所は全国に 10 か所あり，営業所の社員は 1 営業所に 10 人である。S 社は，販売管理を行う業務システムを運用しており，本社と営業所間を通信事業者 X 社の提供する IP-VPN で接続している。また，X 社のインターネット接続サービスを利用して，本社からインターネットへ接続している。S 社では，社外との電子メール（以下，メールという）の交換は本社のメールサーバで行っている。現ネットワークシステム構成を，図 1 に示す。

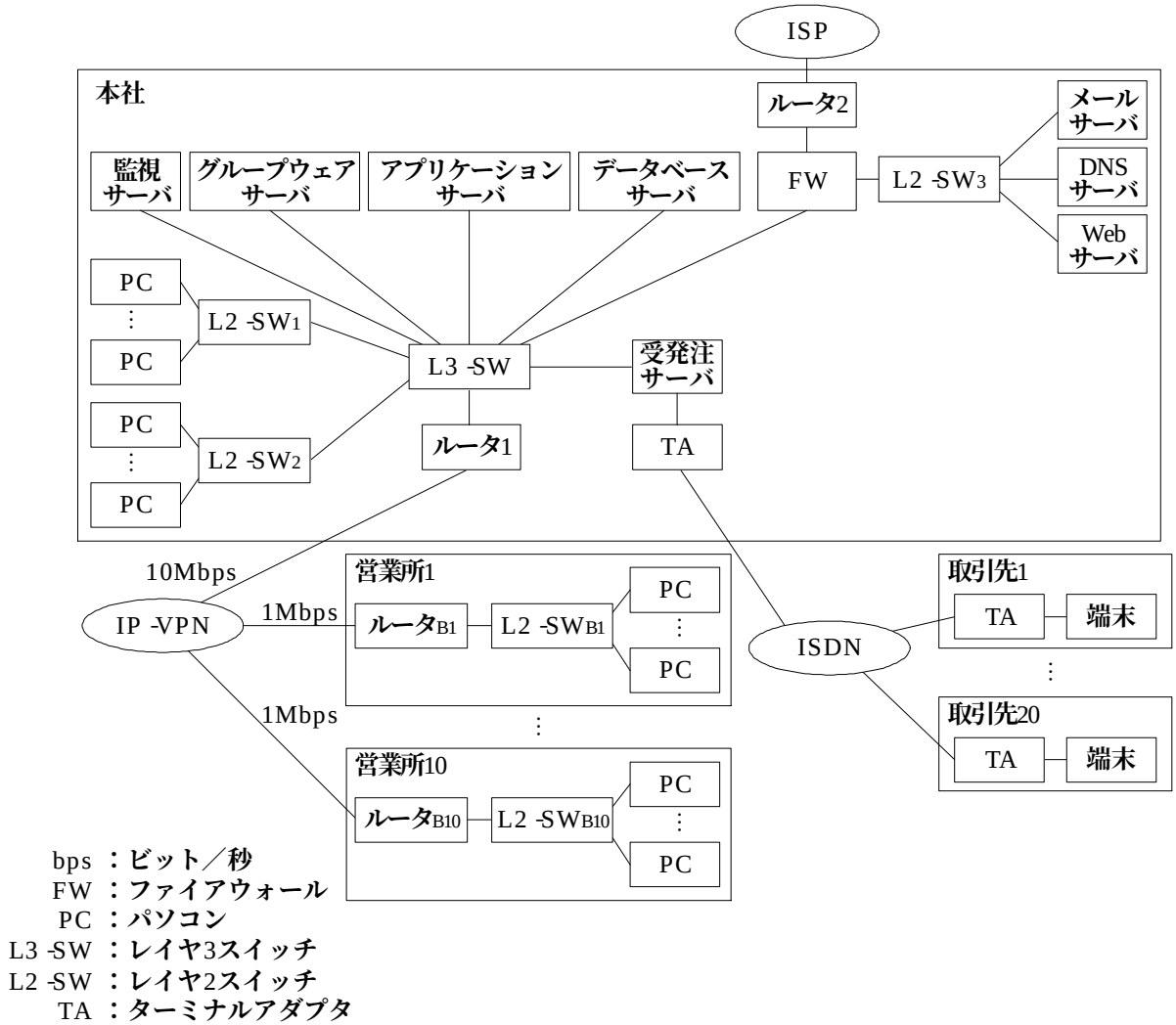


図１　現ネットワークシステム構成

データベースサーバ，アプリケーションサーバ及び受発注サーバは，業務システムのサーバである。販売管理に必要なデータは，アプリケーションサーバで処理され受発注サーバによって受発注ファイルとして取引先との間で転送される。取引先は 20 社あり，接続回線は ISDN を用いている。接続には，取引先からの発信と S 社からの発信とがある。その際，ISDN の発信者番号通知機能を利用して，誤接

続を防止している。

業務システムは，営業日の 8 時から 20 時までサービスを提供している。サービス終了後，バックアップデータの取得を行い，バックアップが終了した時点で各サーバの稼働を停止し，翌営業日の 7 時半に起動している。

グループウェアサーバは，掲示板の処理及び社内メールの交換を行うサーバであり，メールサーバを介して社外とのメール交換も行う。グループウェアサーバは，金曜日の 20 時にバックアップデータを取得するために一時的に処理を中断する以外は，24 時間稼働している。

そのほかのサーバは，原則として 24 時間稼働している。

〔情報管理部の業務の運用状況〕

S 社では，従来，本社の情報管理部でシステムの開発とメンテナンスを行うかたわら，各サーバの起動，停止及びバックアップデータの取得を行い，更にサーバの監視，障害対応及び社員からの問合せにも対応してきた。

サーバの障害時には，障害の切分けと復旧に相当の時間を費やしていた。また，月に一度の締め処理で社員から業務システムのサービス延長依頼があれば，情報管理部員が残業して対応している姿もよく見受けられた。業務システム及び PC の利用における問合せへの対応は，原則として電話及びメールで行っている。各 PC の利用者，設置場所，ハードウェア諸元及び搭載ソフトウェアは，機器管理台帳で把握している。機器管理台帳は，年 1 回，内部監査のときに更新される。事実と違う場合，情報管理部員が現場に出向くか，多少 PC に詳しい社員の応援を依頼する。

〔当初のサーバ監視の状況〕

S 社では，サーバ監視のため，監視ツールを導入して障害に対応していた。監視サーバ上の監視ツールは，監視対象のサーバの動作状況を監視するものであり，監視対象のサーバに対して監視に必要な要求を行い，応答の有無，応答時間及び応答内容を基に障害を検知していた。障害検知の方式を図 2 に示す。

図２　障害検知の方式

図 2 の方式には，RFC792 で決められている ICMP を利用する，ping コマンドによって［　ア　］層の応答監視を行う（以下，ping 監視という）ものと，サーバで稼働しているサービスの応答監視を行う（以下，サービス監視という）ものがある。監視ツールの導入時に，担当の K 君は，次のような方法で動作確認を行った。

まず，監視対象のサーバとしてアプリケーションサーバのホスト名を設定し，ping 監視で応答を確認した。ping 監視の際，監視サーバが送受信したパケットを図 3 に示す。さらに，ping 監視の応答がない場合のエラーメッセージを確認するため，①業務システムの 1 日の運用における特定の時間帯を選ん

で，ping 監視を行った。

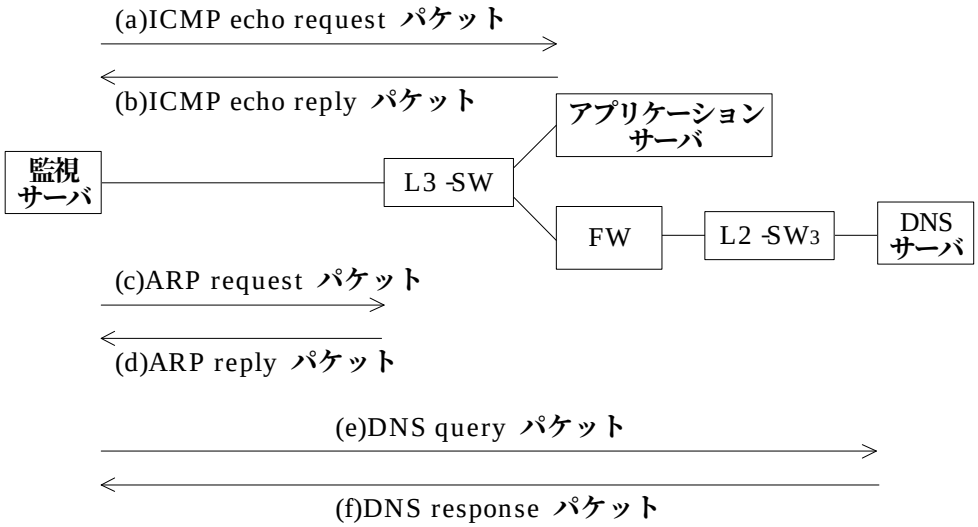


図３　ping 監視における送受信パケット

続いて，サービス監視の動作を確認した。サービス監視は，監視対象のサーバの該当サービスに次の方法で接続して，応答監視を行う機能である。

・メールサーバ及び Web サーバについては，［　イ　］コマンドを用いることで確認する。
［　イ　］コマンドは，ネットワーク経由でほかのコンピュータを遠隔操作するために利用されるが，ここではホスト名と［　ウ　］を指定して，該当するサービスに接続して確認を行う。メールサーバでは，［　エ　］，POP3 及び IMAP4 に対する接続確認を行い，Web サーバに対しては，HTTP に対する接続確認を［　イ　］コマンドを用いて行う。
・DNS サーバについては，検索に対する応答を［　オ　］コマンドで確認する。

K 君は，表に示す監視対象一覧を作成し，その情報を監視ツールに設定して自動監視を行うことにした。このとき，②ホスト名ではなく IP アドレスを用いた。

表　監視対象一覧

サーバ名	ホスト名	IP アドレス	監視方法
メールサーバ	host -mail	IP アドレス 1	［　イ　］コマンド
DNS サーバ	host -dns	IP アドレス 2	［　オ　］コマンド
Web サーバ	host -web	IP アドレス 3	［　イ　］コマンド
データベースサーバ	host -db	IP アドレス 4	ping コマンド
アプリケーションサーバ	host -ap	IP アドレス 5	ping コマンド
グループウェアサーバ	host -gr	IP アドレス 6	ping コマンド
受発注サーバ	host -jh	IP アドレス 7	ping コマンド

この自動監視における，監視対象のサーバに対する定期的な ping 監視は，具体的には，次のようなものであった。監視対象のサーバに対して ping 監視を行い，応答監視タイマの初期値である 4 秒以内に応答を受信したら正常応答と判断し，受信後 2 分で再び ping 監視を行う。4 秒以内に応答がなければ，直ちに二度目の ping 監視を行うが，応答監視タイマを 8 秒にして応答を待つ。応答があれば正常応答と判断するが，応答がない場合は，応答監視タイマを 12 秒にして三度目の ping 監視を行う。ここで応答があれば正常応答と判断するが，応答がない場合は，エラーメッセージを表示し，表示後 2 分で再び ping 監視を行う。

なお，RFC792 では，サーバに起因する場合のほか，“ICMP あて先到達不能”として様々な原因で発生する ICMP エラーメッセージが定められている。そこで，K 君は，ネットワーク機器も ping 監視の対象にした。その際，レイヤ 2 のスイッチである L2-SW_1, L2-SW_2, L2-SW_3, L2-SW_{B1}～L2-SW_{B10} は，IP アドレス，サブネットマスク及び［　カ　］の設定が可能で，ping に応答する機能をもつことを確認した。

サービス監視も，同様に応答監視タイマを用いて監視している。ping 監視又はサービス監視で正常応答を確認できたということは，サーバとネットワークの正常稼働が確認できたことを示す。万一，正常応答を確認できなかった場合は，③監視サーバから監視対象のサーバまでのネットワーク経路を理解して，障害の切分けを行う必要がある。

〔サーバ監視及びネットワーク監視の改善〕

最近，サーバ及びネットワークに障害が発生した。その障害事例を次に示す。

・障害事例 1

ある日，取引先から受発注ファイルを転送できないという連絡を受け，ISDN 及び TA を調べたが異常はなく，受発注サーバも ping 監視の結果は正常であった。受発注サーバのログを調べたところ，受発注ファイルを書き込む領域が確保できていないというエラーを発見した。そこで，不要な受発注ファイルを削除して復旧した。

情報管理部の担当者が，不要な受発注ファイルを定期的に，確実に削除するには負担もかかり，ミスの再発防止策が必要とされた。

・障害事例 2

ある日，社員から在庫検索ができないという苦情があったが，アプリケーションサーバの ping 監視の結果は正常であった。そこで，アプリケーションサーバのログを調べてみると，起動時のエラーメッセージがあり，データベースサーバとの間の通信障害でプロセスが異常終了していることが判明した。データベースサーバも ping 監視の結果は正常であった。業務の復旧を優先するため，アプリケーションサーバを緊急に再起動したところ，正常に稼働した。異常終了したトランザクションの再投入は，手作業で行った。

原因追求のため，L3-SW のログを調べて，パケットの伝送エラーが前日から発生していることを突き止めた。この伝送エラーによって，アプリケーションサーバとデータベースサーバとの間で通信障害が発生し，アプリケーションサーバが正常に起動しなかったと判断された。L3-SW を交換したらパケットの伝送エラーはなくなった。

障害の迅速な切分けのため，障害検知の強化が必要とされた。

・障害事例 3

ある日，人事部から社員向けに人事処遇及び給与体系について，掲示板で通知があった。重要な情報とのことで社員が一斉にグループウェアサーバにアクセスしたので，応答が遅くなり，多くの社員から苦情が寄せられた。調査したところ，今回の応答遅延は一時的なものではなく，最近，メールの読み書きを含め，グループウェアサーバの応答遅延があることが判明した。更に分析を進めた結果，ネットワークに問題はなく，グループウェアサーバの性能不足と分かり，性能向上を計画することにした。

事前に性能不足を検知するためのサーバの監視が必要とされた。

これらの障害事例を踏まえ，K 君は，次のような改善を行った。まず，監視対象のサーバに監視プローブをインストールして，サーバのシステムリソースのデータを定期的に監視サーバに送信する（以下リソース監視という）ことにした。ネットワーク機器については，トラフィックレポート機能を利用して，リソース監視を行うことにした。

次に，サーバ及びネットワーク機器に対して，起動メッセージやステータスメッセージなどのログデータを監視する（以下，ログ監視という）ことにした。具体的には，サーバの監視プローブ及びネットワーク機器のエラーレポート機能を利用して，ログデータを監視サーバに送信し，監視サーバが致命的なエラーメッセージを特定して，アラームを発するように設定した。このアラームは，監視サーバ画面への表示と，アラーム音で，情報管理部員に異常を気付かせるようになっている。

これらについては，既存の監視ツールの機能拡張版を導入して可能となった。④ただし，ログ監視はエラーメッセージだけでなく　起動時の特定のメッセージの有無についても確認する必要があり，情報管理部が手順書を作成して手動で確認している。

このように，監視ツールの機能を拡張し，ある程度の自動化を行ったが，まだ手動部分もあることから，情報管理部員の負担は依然として大きいままである。

〔システムの運用のアウトソーシング〕

一方で，S 社の事業が順調に伸びてきたこともあって，業務システムの性能向上及びサービス拡張が必要となっている。情報管理部がその対応に取り組んでいるが，システム開発ははかどらない状況であった。そこで，アウトソーシングの活用によって，サーバとネットワークの拡張及び情報管理部員の負担軽減を図ることになった。情報管理部の Z 部長の指示で，K 君は，サーバの運用を X 社データセンタ（以下，データセンタという）に委託する場合の要件を洗い出すことになった。K 君は，まず，S 社における運用管理項目を次のようにまとめた。

・サーバの起動，停止，バックアップデータの取得などのオペレーション
・サーバとネットワークの ping 監視，サービス監視，リソース監視及びログ監視
・サーバとネットワークの障害の切分けと復旧
・サーバとネットワークのリソースデータの傾向分析，リソース増強策の検討と実施
・業務システム及び PC の利用に関する問合せへの対応

この中から，X 社にアウトソーシングする部分を取り出す。X 社のアウトソーシングメニューには，ヘルプデスク，オペレーション，監視及び障害対応がある。それぞれのメニューを利用した委託内容を次のように設定し，業務システムのサーバとグループウェアサーバ，メールサーバ，DNS サーバ及び Web サーバの運用を委託する。

（1）ヘルプデスク

S 社の業務時間内における，本社及び営業所の社員からの PC の利用に関する問合せへの対応

（2）オペレーション

（a）業務システムのサーバのオペレーション

・7 時半に起動し，［　　a　　］を確認

・サービス終了後，バックアップデータを取得

・バックアップデータの取得後，サーバを停止

（b）そのほかのサーバのオペレーション

・グループウェアサーバについては，金曜日の 20 時にバックアップデータを取得

・ほかのサーバは，S 社からの特別な依頼時だけ停止及び起動

（3）監視及び障害対応

・データセンタが所有する監視装置による終日（24 時間）の ping 監視，サービス監視，リソース監視及びログ監視

・障害検知時，障害の切分けとあらかじめ定められた手順（再起動，保守会社によるハードウェアの交換など）による復旧作業

・業務プログラム障害から復旧できない場合，S 社へ連絡

・毎週月曜日に，障害検知，復旧作業結果を S 社へ定期的に報告

S 社で引き続き行う管理項目は，次のとおりとする。

（4）業務プログラム障害から復旧できない場合の，障害切分けと復旧のためのログデータの分析

（5）リソースデータの傾向分析及びリソース増強策の検討と実施

適宜にリソース増強を行い，リソース不足によるサーバの性能低下及びサーバの停止を防止する。そのため，アウトソーシングするサーバのリソースデータを監視サーバに蓄積して，傾向分析を行う。その分析結果に基づくリソース増強策の検討は S 社で引き続き行い，実際の作業はその都度 X 社に依頼する。

（6）業務システムに関する問合せへの対応

業務システムについての社員の問合せに対応する。

(4)～(6) については，情報管理部員が引き続き行うので，K 君は，⑤監視サーバを S 社に残すことにした。

以上の検討結果を基に，K 君は，X 社と相談し，図 4 に示す新ネットワークシステム構成を考え，次のような内容の報告を Z 部長に行った。

・データセンタとは，新たな IP -VPN 接続回線を開通する。

・本社の IP -VPN 接続回線の通信速度は見直す。

・メールサーバ，DNS サーバ及び Web サーバは，X 社 FW に接続する。

・業務システムのサーバとグループウェアサーバは，ルータ $_{x1}$ に接続する。
・受発注サーバの移設によって，利用している ISDN の電話番号が変更になる。

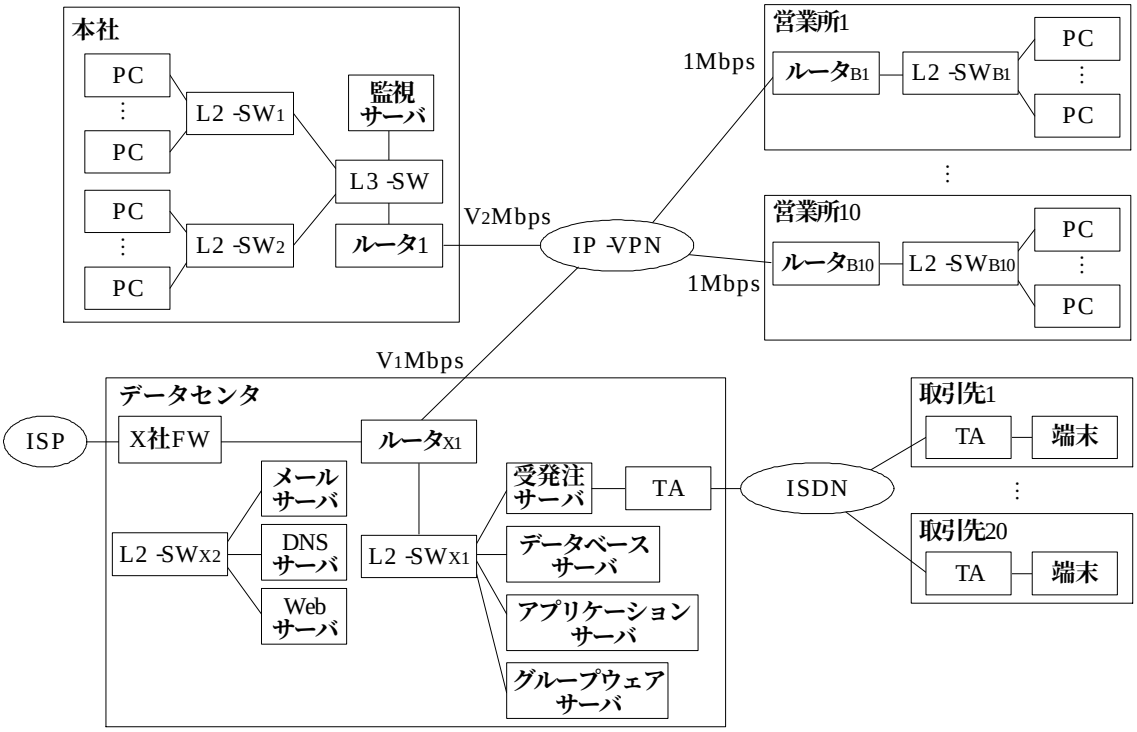


図４　新ネットワークシステム構成

K 君の報告を受けた Z 部長は，更に徹底した省力化のために監視サーバを廃止するよう，再検討を指示した。K 君は，X 社と検討を重ね，⑥常時起動している監視サーバがなくても運用できるように，X 社に新たな提供メニューを設定してもらい，情報管理部の PC で一部機能を代替できるようにした。

K 君は，監視サーバの廃止が可能であることを Z 部長に報告した。こうして，S 社は，K 君の提案どおりデータセンタにサーバの運用を委託することに決定した。

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　〔当初のサーバ監視の状況〕について，(1)～(5) に答えよ。

(1) 本文中の下線①の特定の時間帯について，30 字以内で具体的に述べよ。
(2) 図 3 の各パケット(a)～(f) を発生した順に並べ，記号で答えよ。
(3) 本文中の下線②の理由を，30 字以内で述べよ。
(4) ping 監視において，障害発生後，障害検知に要する時間（秒）の最大値及び最小値を答えよ。
(5) 本文中の下線③について，メールサーバに対するサービス監視を行い，応答がない場合に，メールサーバ以外に確認すべき機器を，図 1 中から三つ選び答えよ。

設問３　〔サーバ監視及びネットワーク監視の改善〕について，(1)，(2) に答えよ。

(1) 監視ツールによって監視すべき情報の具体的項目を，障害事例 1～3 に即して一つずつ答えよ。

(2) 本文中の下線④について，起動時のメッセージを確認する理由を，40 字以内で述べよ。

設問４　X 社へのアウトソーシングについて，(1)～(4) に答えよ。

(1) ヘルプデスクにおいて，X 社に渡すべき情報を本文中の字句を用いて答えよ。さらに，その扱いに関して必要な改善策を，30 字以内で述べよ。

(2) 本文中の［ a ］に入れる確認作業内容を，20 字以内で答えよ。

(3) バックアップデータの取得において，X 社が業務システムのサービス終了と判断するために明確にすべき条件を，社員からの業務システムのサービス延長依頼以外に，30 字以内で述べよ。

(4) 受発注サーバのアウトソーシングにおいて，移行後の本番運用までに，取引先に依頼すべき作業を二つ挙げ，それぞれ 20 字以内で述べよ。

設問５　新ネットワークシステムについて，(1)～(3) に答えよ。

(1) 本文中の下線⑤を踏まえた，X 社 FW に必要な S 社向け設定作業の内容を，50 字以内で具体的に述べよ。

(2) 営業所の IP-VPN 接続回線の通信速度が 1Mbps であることから，社員 10 人当たりのトラフィックを 1Mbps と仮定して，データセンタ及び本社で必要な IP-VPN 接続回線の最低通信速度（Mbps）V_1，V_2 を答えよ。

(3) 監視サーバの廃止において，本文中の下線⑥を踏まえ，リソースデータ及びログデータの扱いに着目して，必要な運用の変更点を三つ挙げ，それぞれ 30 字以内で具体的に述べよ。