平成20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

試験時間	14:10 ～ 16:10（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. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **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。**
5. 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

6. 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，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**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。
   (4) **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。
   なお，○印がない場合は，採点の対象になりません。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。
   (5) 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。
   (6) 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
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　分散オフィスの構築に関する次の記述を読んで，設問1～5に答えよ。

S社は，システムの構築を業務とする情報システム会社である。顧客から依頼されたシステム要件に基づいて，アプリケーションの開発を行うとともに，顧客先でサーバやネットワークシステムの構築を行っている。

社員は，顧客先への出張が多いので，外出先でも電子メール（以下，メールという）のやり取り，ドキュメントの作成，アプリケーションの開発などが，社内にいるときと同様に行える必要がある。

また，外出した社員は，顧客先から直接帰宅する場合も多く，連絡事項の確認や報告のために，自宅からのメール送受信は必須である。

S社では，外出先での業務が多い社員には，モバイルPCと通信カードを支給して対応してきた。最近，PCの盗難や記憶媒体の紛失という問題が発生し，情報の持出しに伴う情報漏えいを防止するために，新しいシステムを検討することになった。

〔新システムの要件〕

S社では，システムの見直しのために，要件を次のようにまとめた。

(1)　情報を記憶媒体に格納して持ち出すと，紛失や盗難といったリスクが避けられないので，情報漏えい対策としては情報を持ち出さない方式を考えている。具体的には，モバイルPCを，シンクライアントと呼ばれる，ハードディスクなどの情報蓄積機能のない端末（以下，TPCという）に順次入れ替え，本人確認用のUSB認証デバイスと組み合わせて使用することにする。

(2)　業務効率の向上を図るとともに，働く人の仕事と生活の調和（ワークライフバランス）を重視し，“テレワーク”を含む，場所と時間にとらわれずに働く環境の実現に，積極的に取り組むことにする。また，電話については，遠隔地でもVoIPを使用した内線通話ができるようにする。

(3)　最近では，ホテルや喫茶店などからネットワークを利用できるようになり，社員の自宅でも，ADSLやFTTHによる高速のインターネット利用が普及してきている。社員の自宅，出張者用サテライトオフィス，ホテル，喫茶店など必要なときに本社と接続する場合には，極力これらのネットワーク接続サービスを利用できるようにする。

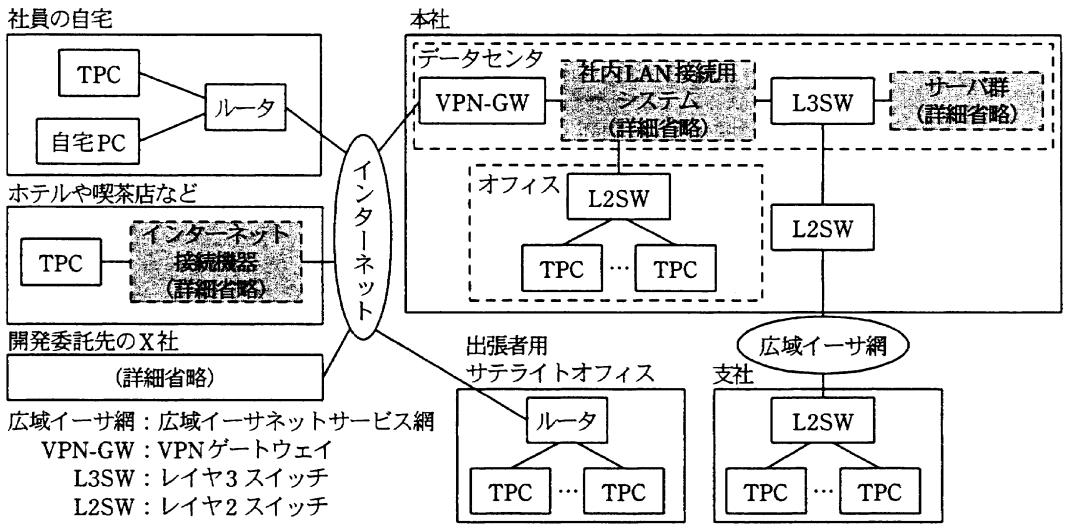
(4) S 社は，顧客から受注したアプリケーション開発の一部について外部の X 社に委託している。X 社での開発は，情報漏えいを防止するために，X 社側に設置した TPC から S 社データセンタ内に用意したサーバ群を利用させることにする。

(5) システムの構築に当たっては，省コスト，省スペース及び運用効率の向上を目指すことにする。

これらの要件を満たす新しいオフィスシステム（以下，分散オフィスシステムという）の実現を目指し，プロジェクトがスタートした。システム部の T 君が，このプロジェクトの担当となった。

〔分散オフィスシステムの構想〕

図 1 は T 君がまとめた，分散オフィスシステムの構想図である。



注1 図中のルータは，NAPT（Network Address Port Translation）機能及び DHCP サーバ機能が有効に設定されている。
注2 図示していないが，TPC には USB 認証デバイスを接続して使用している。
注3 社内 LAN 接続用システムはセキュリティを確保するためのシステムである。

図 1　分散オフィスシステムの構想図

社員の自宅，出張者用サテライトオフィス，ホテルや喫茶店などの公衆のアクセスポイント，及び X 社から本社への接続には，インターネット VPN を利用することにしている。

社内の PC の機能をサーバ上で実現し，PC は撤去する。そのサーバ上の PC の機能を TPC から遠隔制御するというのが，T 君の構想である。

TPC は，インターネット VPN 接続の機能と，ネットワーク経由で遠隔制御を行う通信プロトコル（以下，RDP という）に対応した PC を遠隔制御する機能（具体的には，PC の画面情報を受け取って表示する機能と TPC での操作を PC に伝える機能）を備えている。RDP は，特定のポート番号で動作し，通信の帯域をそれほど必要としないので，リモートからのアクセスに向いているという特長がある。

〔インターネット VPN 方式の検討〕

T 君は，社員の自宅や出張先から本社にアクセスする方法として，次の三つのインターネット VPN 方式について調査及び検討を行った。

最初に，現在使用している PC の OS が標準でサポートしている VPN プロトコルの PPTP について調べてみた。このプロトコルは，PPP パケットに GRE（Generic Routing Encapsulation）ヘッダと呼ばれるヘッダを付けてカプセル化する方式である。GRE を使うことによって，［　ア　］を転送できるので，各種のアプリケーションに対応できる柔軟性をもつ。GRE はポート番号情報をもたないので，ルータ経由でインターネットに接続する場合に問題が発生することがある。この問題に対応するためには，［　イ　］機能をもったルータが必要になる。

次に調べた IPsec-VPN についても，(i) UDP を使用した鍵交換と，ESP ヘッダを使ったカプセル化を行ったときのいずれの場合にも，ルータ経由では通信できない問題が発生することが分かった。対策として PPTP の場合と同様の機能をもったルータを使用する方法もあるが，RFC 3948 で規定されるダミーの UDP ヘッダを付加する NAT トラバーサル方式でないと，出張者用サテライトオフィスからアクセスする場合に問題が発生する。

前記 2 方式のいずれも，ホテルや喫茶店などの公衆のアクセスポイントでは TPC を接続する部分からインターネットに接続する部分までの設備が条件に合うとは限らないので，VPN 接続を実現するのは難しいと T 君は考えた。

最後に，T 君は SSL-VPN を調べた。調査した製品は，ブラウザに標準で実装されている SSL を使って，リモートアクセス VPN を実現する方式である。アドレス変換に伴う問題も少なく，ファイアウォール（以下，FW という）も通過しやすいが，(ii)

UDP が使えず，S 社の要件には対応できないことが分かった。

〔インターネット VPN 方式の決定〕

さらに，T 君が調べてみると，SSL-VPN によってリモート側 PC と VPN-GW との間に作った VPN トンネルを通して，リモート側 PC 内のソフトウェアで実現した擬似的な LAN カード（以下，ソフト NIC という）から，イーサネットフレームの転送を実現する方式（以下，SSL-VPN レイヤ 2 フォワード方式という）の製品があることが分かった。図 2 は，この方式の説明図である。図 2 では，リモート側 PC からセンタ側サーバに，VPN-GW を経由してデータを転送する処理の例を示している。ソフト NIC は，通常の LAN カード（以下，物理 NIC という）と同じように動作する。

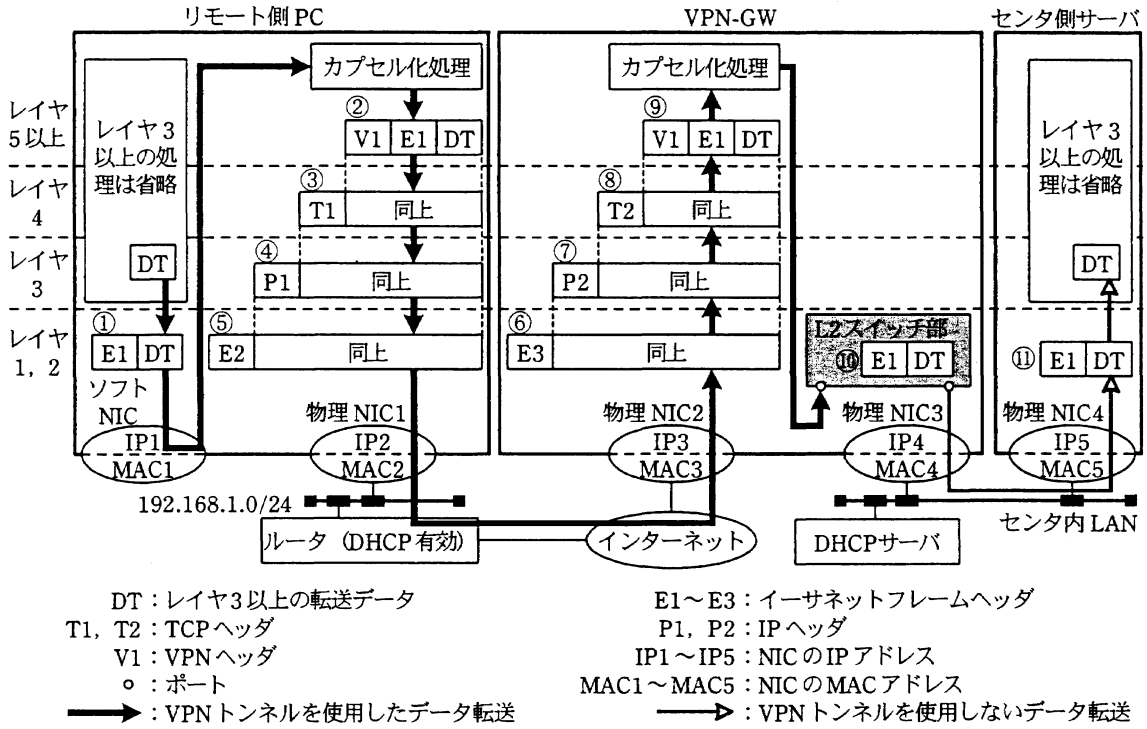


図 2　SSL-VPN レイヤ 2 フォワード方式の説明図

VPN-GW には，レイヤ 2 スイッチの動作を行う L2 スイッチ部がある。ソフト NIC と VPN-GW の L2 スイッチ部を VPN トンネルで接続することによって，物理 NIC とスイッチをケーブルで接続するのと同じように通信が可能になる。

図 2 中の V1 はカプセル化のための専用ヘッダである。ソフト NIC が上位層から受け取ったデータには V1 が付加され，物理 NIC を経由して，VPN-GW あてに送られる。MAC アドレスの学習も行われ，イーサネットフレームの中継が可能になる。

S 社では，これまでの調査結果を踏まえ，(iii)SSL-VPN レイヤ 2 フォワード方式を採用することにした。

〔PC の仮想化〕

T 君は，PC の機能をサーバに集約するのに，最近話題になっている仮想化方式を使えないか調べた。調査した方式は，サーバ上に，PC 単位の独立したプログラム実行環境（以下，仮想 PC という）をソフトウェアで実現する方式である。図 3 は，T 君が採用することにした仮想化方式の説明図である。

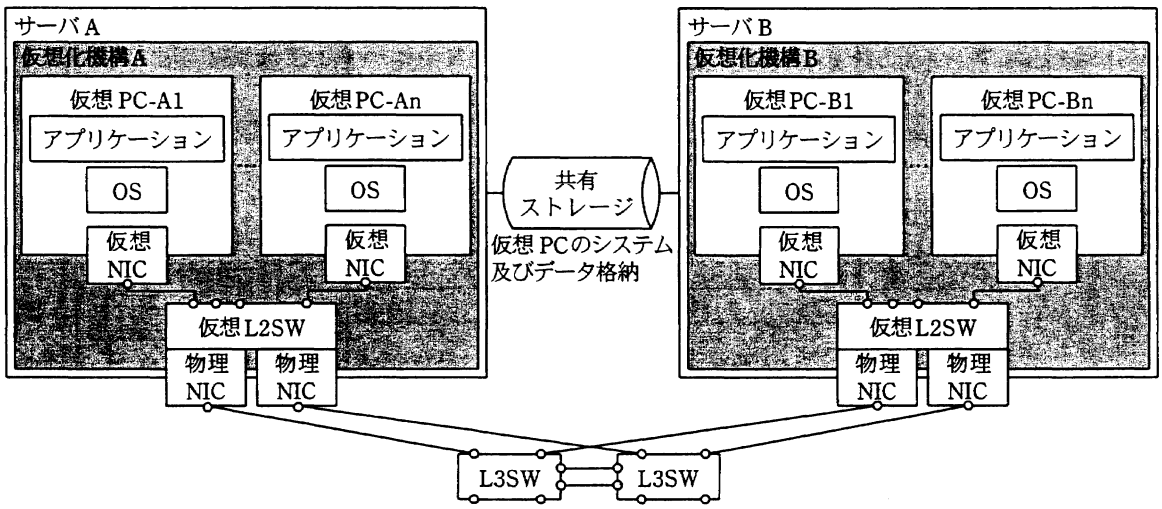


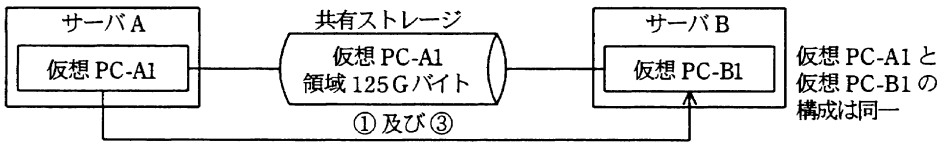
図 3　仮想化方式の説明図

図 3 の方式は，ハイパバイザ型と呼ばれる方式で，仮想化機構が，その上で動作する仮想 PC に対してハードウェアリソースの割当て，タスクスケジューリング及び仮想化されたシステム全体の管理を行う。生成された仮想 PC 上のプログラムは，サーバの構成や同じサーバ上にあるほかの仮想 PC を意識せずに動作することができる。

図 3 中の仮想 NIC は，仮想 PC 上の OS にとって，物理 NIC と同じように扱えるソフトウェアで実現された NIC である。図 3 中の仮想 L2SW は，仮想 PC が外部との通信を行う仕組みとして用意されたもので，ソフトウェアで実現した擬似的なレイヤ 2

スイッチである。仮想 NIC と仮想 L2SW の接続は，仮想化機構のコンソールで設定され，この接続によって仮想 PC はほかの仮想 PC や外部との通信が可能になる。仮想 L2SW の外部接続用ポートとして，物理 NIC が使われる。仮想 L2SW の物理 NIC を外部のスイッチに接続することで，外部のネットワークとの通信も可能になる。

仮想 PC は，基本的に仮想 PC に割り当てるリソースの構成情報を基に生成できる。したがって，動作している仮想 PC は，メモリ内容と構成情報のファイルとして，移動や複製が可能であり，サーバの増設，負荷バランス，障害時の切替えなどの構成変更が容易になる。そこで，T 君は，仮想 PC を別の物理サーバに移行する場合について検討した。図 4 は，仮想 PC を別のサーバに移行する処理順序の概要を示している。



サーバ A 上の仮想 PC-A1 をサーバ B 上の仮想 PC-B1 に切り替える処理順序

①: 仮想 PC-A1 のメモリ内容のスナップショット（1G バイト）を取得完了し（取得完了時刻 : t1），仮想 PC-B1 のメモリに転送

②: 仮想 PC-B1 側で仮想 PC-A1 側のメモリ内容と構成情報の引継準備が完了した時点で，仮想PC-A1 のプログラムを停止（停止時刻 : t2）

③: ①のスナップショット取得後に変化があったメモリ内容の差分情報を，仮想PC-B1 に転送

④: 仮想 PC-B1 が共有ストレージ上の仮想 PC-A1 用領域を引き継ぎ，動作開始（仮想 PC-B1 動作開始時刻 : t3）

⑤: 図 3 の構成で，L3SW へのアクセスパスの切替指示（切替完了時刻 : t4）

図 4　仮想 PC を別のサーバに移行する処理順序の概要

仮想 PC が動作しているサーバを切り替える時間は，メモリ内容を転送する時間でほぼ決まってしまう。図 4 中の③の処理で，20％のメモリ内容が更新されたと想定し，仮想 NIC 間の実効転送速度を 500M ビット／秒として切替時間を計算する。その結果，仮想 PC-A1 の停止時間 t2 ～ t3 に占める転送時間は約 [a] 秒，移行時間 t1 ～ t4 に占める転送時間は約 [b] 秒となる。したがって，十分に短い時間で移行できることが分かった。

現行のオフィス環境から新しいオフィス環境に移行するに当たって，T 君は社内で使用する仮想 PC の標準構成を決めた。その結果，仮想 PC の種類を増やさずに済むことから，仮想 PC の管理が容易になる。仮想 PC を収容するサーバは運用面を考慮して，余裕をもたせた構成にすることにした。

〔分散オフィスシステムの設計〕

T 君は仮想化方式を使って PC の機能を集約できる見通しがついたので，社員各自の PC を仮想 PC としてサーバ上に集約し，TPC から RDP で接続して利用する形態で分散オフィスシステムの具体的な設計に入った。

図 5 は，図 1 の社内 LAN 接続用システム及び開発委託先の X 社について，詳細を示した構成図である。ただし，支社，出張者用サテライトオフィス，ホテルや喫茶店などの公衆のアクセスポイントとの接続は省略している。

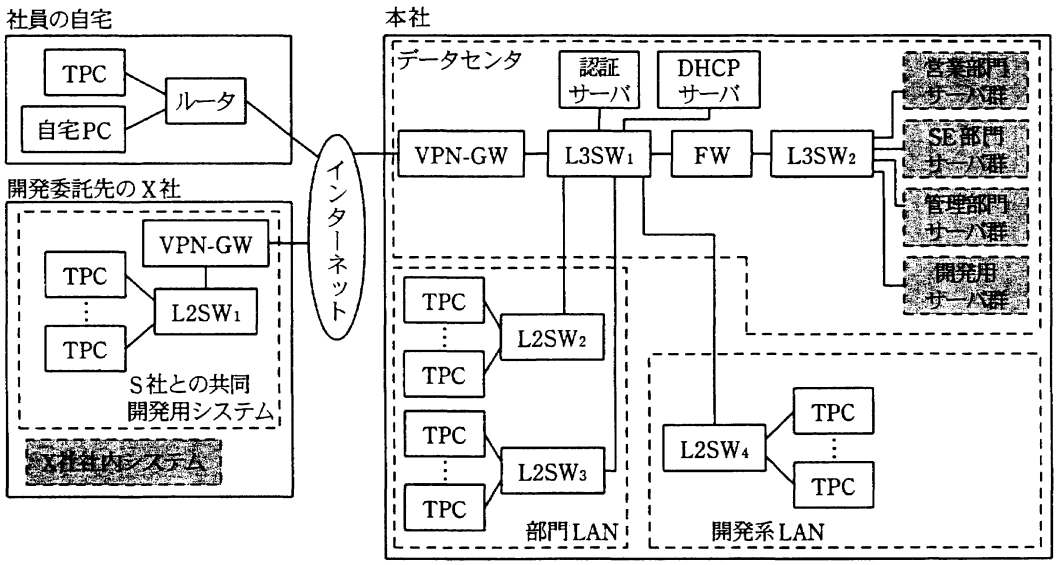


図 5　社内 LAN 接続用システム及び開発委託先の X 社の詳細構成図（抜粋）

S 社では，インターネット VPN を使った社内 LAN アクセスを行うので，アクセスしてくる利用者が正規の利用者であることを確認し，セキュリティを確保することが重要である。

社外から S 社の社内 LAN に接続するためには，(1) インターネット VPN による VPN トンネルの生成，(2) アクセスしてきた PC の認証，(3) 適切な VLAN への接続，(4) IP アドレスの割当て，という処理が必要である。S 社では，(1) と (2) の処理において電子証明書による認証を行うことにしている。

TPC では，図 2 で説明された SSL-VPN レイヤ 2 フォワード方式をサポートしてお

り，2 種類の NIC を使って動作している。TPC が本社の LAN にブリッジ接続するときの動作は，社員が自宅から本社にアクセスする場合を例にとると，次のようになる。TPC は［ ウ ］NIC の IP アドレスを使用して，社内 VPN-GW に対して SSL-VPN による VPN トンネル生成の要求を行う。要求を受けた VPN-GW は，SSL による認証を行うために，認証サーバにアクセスして認証可否を問い合わせる。TPC の認証が終了すると VPN トンネルが生成される。その結果，TPC の［ エ ］NIC が VPN-GW を経由して，社内 LAN（VLAN）側とブリッジ接続される。このとき VPN-GW には，登録された利用者に対応した部門 VLAN の ID が認証サーバから通知されるので，VPN-GW は指定された VLAN に対して TPC からのフレームの転送が可能になる。

次に，TPC の［ オ ］NIC は，IP アドレスを取得するために，DHCP サーバに DHCPDISCOVER を送信する。本社にアクセスしてくるすべての TPC に対して IP アドレスを配布するために，DHCP サーバは，VPN-GW とは別のネットワークに設置されている。TPC が部門サーバ内の仮想 PC を利用するときには，RDP による接続を行うだけなので，部門サーバへの接続経路には FW を設置し，RDP にかかわるパケット以外は通過させないようにしてセキュリティを確保する。社員各自の仮想 PC には固定の IP アドレスを設定している。

〔開発委託先の X 社との接続〕

X 社との接続では，RDP による接続だけでなく，IP 電話やテレビ会議などの実現を考慮して，S 社と X 社の双方に VPN-GW を対向で設置する LAN 間接続方式とした。

X 社から S 社内の開発環境を使う場合の接続動作については，次のようになる。X 社内の VPN-GW は，起動すると，S 社内の VPN-GW に対して SSL-VPN による VPN トンネル生成の要求を行う。TPC からの接続要求と同様に認証処理を終えると，VPN トンネルが生成される。これによって，X 社内の $L2SW_1$ は VPN-GW 経由で，S 社内の LAN とブリッジ接続される。X 社内の TPC の IP アドレスも，S 社内の DHCP サーバから割り当てるようにした。

この状態では，X 社内の $L2SW_1$ に接続された TPC が，制限なく S 社内の LAN に接続できてしまうので問題である。この対策として，IEEE 802.1X による認証を行う方法があり，認証された TPC だけが S 社内の LAN と接続できる。しかし，(iv) TPC をリピータハブ経由で認証を行うスイッチに接続してしまうと，セキュリティ上の問題

が残ってしまう。T 君は，いろいろな対応方法を調べ対策した。

以上のようにして，T 君は，場所によらずにアクセスが可能なインターネット VPN，仮想化方式による PC 機能の集約，及びセキュリティを確保した分散オフィスシステムの設計を終え，システムの構築を開始した。

設問 1　〔インターネット VPN 方式の検討〕について，(1) ～ (4)に答えよ。

(1) 本文中の［　ア　］，［　イ　］に入れる適切な字句を答えよ。

(2) 本文中の下線 (i) について，通信できない理由を，二つの場合についてパケット形式と関連して，それぞれ 50 字以内で述べよ。

(3) 本文中の NAT トラバーサル方式でないと，出張者用サテライトオフィスからアクセスする目的には適さない理由を，25 字以内で述べよ。

(4) 本文中の下線(ii)について，対応できない S 社の要件は何か。15 字以内で述べよ。

設問 2　〔インターネット VPN 方式の決定〕について，(1) ～ (4)に答えよ。

(1) 図 2 中の L2 スイッチ部は，どの NIC の MAC アドレスを学習する必要があるか。図 2 中の NIC の名称で，すべて答えよ。

(2) 図 2 中の② ～ ⑤の転送データの中で暗号化されているヘッダ又はデータは，どの部分か。図 2 中の字句を用いて，すべて答えよ。

(3) 図 2 中の，①の E1 のあて先 MAC アドレス，及び④の P1 のあて先 IP アドレスは何か。図 2 中の字句を用いて答えよ。

(4) 本文中の下線(iii)について，その採用理由を二つの観点から，それぞれ 25 字以内で述べよ。

設問 3　〔PC の仮想化〕について，(1) ～ (4)に答えよ。

(1) 本文中の［　a　］，［　b　］に入れる適切な数値を答えよ。答えは，小数第 1 位を四捨五入して整数で答えよ。

(2) 図 4 中の①の処理で，最初にメモリ内容を転送する目的は何か。20 字以内で述べよ。

(3) 図 4 中の⑤の処理で，L3SW への切替指示には，仮想 PC 側からどのような通信を行えばよいか。40 字以内で述べよ。

(4) S 社のように仮想 PC を収容するサーバの構成に余裕をもたせることによって得られる運用面の効果を二つ挙げ，それぞれ 35 字以内で述べよ。

設問 4 〔分散オフィスシステムの設計〕について，(1) ～ (3)に答えよ。

(1) 電子証明書による認証を行うためには，3 種類の証明書が必要である。認証サーバ及び USB 認証デバイスのそれぞれに保持しておく必要がある証明書をすべて答えよ。

(2) 本文中の［ ウ ］～［ オ ］に入れる適切な字句を，“物理”又は“ソフト”から選び，どちらかを答えよ。

(3) 図 5 において，別ネットワークにある DHCP サーバを利用するためには，経路にある機器にどのような機能が必要か。20 字以内で答えよ。

設問 5 〔開発委託先の X 社との接続〕について，(1) ～ (3)に答えよ。

(1) 図 5 において，IEEE 802.1X の認証を行うスイッチはどれか。図 5 中の機器名で答えよ。

(2) 本文中の下線(iv)で，発生するセキュリティ上の問題は何か。40 字以内で述べよ。

(3) 上記(2)の問題への対策としてどのような手段があるか。40 字以内で述べよ。

問2　ネットワークシステムの変更に関する次の記述を読んで，設問1～5に答えよ。

〔Z社のネットワークシステム〕

機械の保守サービスを行っている Z 社では，ネットワークシステムを業務システムの共通基盤として利用している。稼働している業務システムには，Web サーバとアプリケーションサーバ（以下，AP サーバという）を使った“ポータルシステム”や，在庫管理サーバを使った“在庫管理システム”などがある。現在のネットワークシステムを図1に示す。

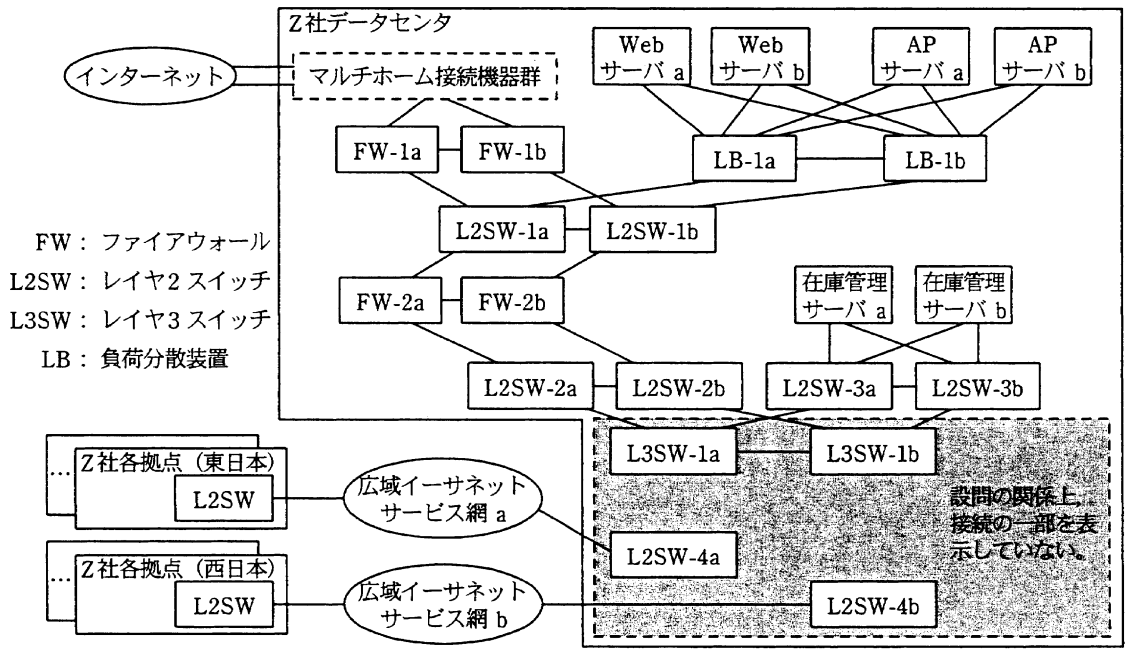


図1　現在のネットワークシステム（抜粋）

データセンタ内の LAN は冗長化され，マルチホーム接続機器群によってインターネットに接続されている。マルチホーム接続機器群は，マルチホーム接続を行うための機器と DNS サーバから構成されている。

L3SW は VRRP（Virtual Router Redundancy Protocol）を利用して二重化されている。LB と2組の FW はアクティブスタンバイ方式によって二重化されている。

サーバの収容ゾーンは，2組の FW によって DMZ と内部ゾーンに分けられている。いずれのゾーンもプライベート IP アドレスを使用しており，インターネットと DMZ の間の通信では，FW-1a 又は FW-1b が NAT を用いて IP アドレスを変換する。

Z 社のネットワークセキュリティポリシに従い，2 組の FW は TCP/IP のフィルタリングを行っている。インターネットと内部ゾーンとの直接の通信はすべて禁止され，インターネットと DMZ 及び DMZ と内部ゾーンの間で，必要な通信だけが許可されている。

ポータルシステムは顧客向けのシステムである。顧客は PC を使いインターネットを経由して Web サーバにアクセスする。Web サーバと AP サーバは LB を利用して冗長化されている。図 2 に LB の概念図を示す。

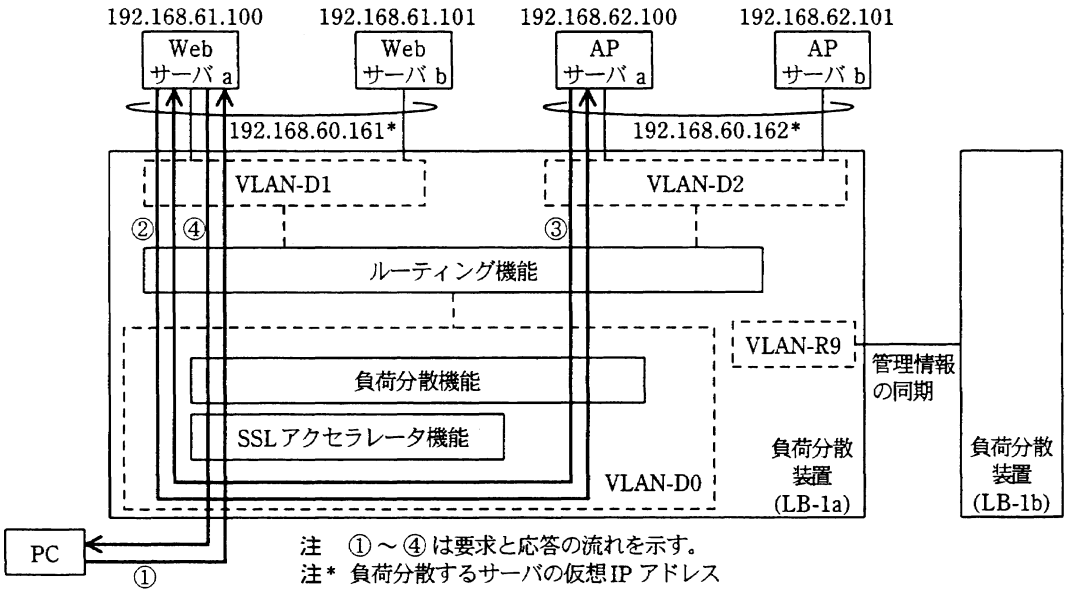


図 2 LB の概念図

LB には四つの VLAN を定義している。VLAN-D0 は負荷分散するサーバの仮想 IP アドレスをもち，SSL アクセラレータ機能と負荷分散機能が動作する。SSL アクセラレータ機能は TLS（Transport Layer Security）のエンドポイントとして機能する。負荷分散機能は，TCP コネクションを確立するときに実行中の TCP コネクション数が少ない方のサーバを選択する（Least Connection モード）。

ポータルシステムの監視は，サービスプロバイダの監視サービスを使って行われている。監視サービスでは，URL を用いて http の要求をインターネット経由で Web サーバに送信し，その応答を確認する。① ポータルシステムの監視では，顧客に公開されている URL のほかに，公開 URL の中のホスト名の代わりに IP アドレスを用いた監視用 URL を三つ用意し，合計四つの URL で確認を行っている。

〔保守情報システム〕

Z 社では，“保守情報システム”の企画を進めている。保守情報システムは，機械の設置場所で行われる保守作業を支援するためのシステムである。保守員にインターネットに接続可能な携帯端末を持たせ，その携帯端末を使って Z 社の関連部署とリアルタイムに情報を交換する。

Z 社のネットワーク技術グループに所属している G 君は，ネットワークシステムを担当しており，新しいネットワーク技術にも詳しい。ある日，G 君は上司から M 氏の依頼に対応するよう指示を受けた。プロジェクトマネージャの M 氏は保守情報システムの導入計画を検討中である。次は，G 君と M 氏の会話である。

M 氏：計画中の保守情報システムでは，開発を委託する開発ベンダの提案に従って，IM（Instant Messaging）と SIP を使います。それに伴い，ネットワークシステムの変更も必要だと思います。その概要を知りたいのです。

G 君：新しい仕組みを使うのですね。開発ベンダの提案内容について，もう少し教えてもらえませんか。

M 氏：携帯端末と保守情報サーバを新たに導入し，既設の在庫管理サーバと連動させます。これらの機器に開発ベンダの製品であるミドルウェアを実装し，IM と SIP を使ってデータをやり取りします。保守情報サーバは，顧客情報や技術情報などの保守情報を管理します。図 3 が保守情報システムの概念図です。

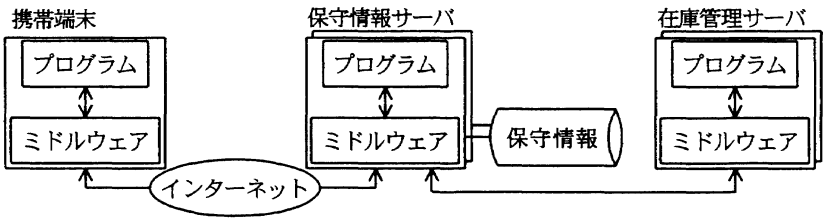


図 3　保守情報システムの概念図

G 君：セキュリティ対策も必要ですね。これについては検討されているのですか。

M 氏：いいえ，これからです。ミドルウェアは幾つかセキュリティ機能をもっています。それらを参考に，必要となるネットワークシステムのセキュリティ対策も盛り込んだ，ネットワークシステムの変更案を作ってください。

G 君：分かりました。変更案を検討し，2 週間後に結果を報告します。

〔ミドルウェア〕

G 君は，開発ベンダの提案を基に，ミドルウェアの機能を次のように整理した。

IM と SIP は，RFC 3860，RFC 3261，RFC 3428 などで標準化されている。ミドルウェアはこれらの標準に準拠しており，データの交換と制御に IM と SIP を使用し，データの転送に TCP を使用する。交換するデータの送信元とあて先は，Web における URL に似た SIP URI（Uniform Resource Identifier）を用いて指定する。

SIP には多くのリクエストが定義されている。例えば，SIP セッションの開始には［ア］リクエスト，終了には［イ］リクエストが用いられ，データの転送には MESSAGE リクエストが用いられる。図 4 は，MESSAGE リクエストを利用した，保守情報サーバから携帯端末への SIP メッセージの例である。

```
 1  MESSAGE sip:hoshuina@α1.α2.α3.jp  SIP/2.0
 2  Via: SIP/2.0/TCP hoshujohosv@α4.α5.α6.jp
 3  From: HoshujohoSV <sip:hoshujohosv@α4.α5.α6.jp>
 4  To: HoshuinA <sip:hoshuina@α1.α2.α3.jp>
 5  Call-ID: ...
 6  CSeq: 1 MESSAGE
 7  Contact: hoshujohosv@α4.α5.α6.jp
 8  Content-Type: text/plain
 9  Content-Length: 540
10
10  Information 1st line
11  Information 2nd line
12  ...
13  Information last line
```

注1 1～13はメッセージの行番号を表す。
注2 α1～α6は特定の文字列を表す。

図 4 保守情報システムの SIP メッセージ例

ミドルウェアでは HTTP ダイジェスト認証が可能である。ミドルウェアを実装した機器が対になっており，一方から他方へ SIP セッション開始のリクエストが送られたとする。SIP のサーバは 407（Proxy Authentication Required）を SIP のクライアントに送り，秘密情報に［ウ］関数を適用した計算結果を要求する。これによって［エ］の認証が可能となる。

ミドルウェアでは TLS による認証と暗号化が可能である。TCP コネクションの確立要求を行う際，クライアントは，サーバがもつ証明書を確認することによって［オ］を認証する。また，サーバの［カ］鍵を使い，暗号化鍵を生成するための秘密情報（Premaster Secret）を暗号化して，それをサーバに送る。

ミドルウェアでは，SMTP と同様に S/MIME による暗号化が可能である。この機能を用いて，図 4 の SIP メッセージを暗号化した場合には，SIP ヘッダの［キ］

の部分が application/pkcs7-mime に置き換えられ，［　ク　］の範囲が暗号化される。

〔ネットワークセキュリティ対策〕

ネットワークセキュリティ対策の検討に当たり，G 君は保守情報サーバを内部ゾーンに置き，DMZ には SIP の通信を中継する機器（以下，SIP 中継サーバという）を置く案を採用することにした。

SIP 中継サーバとして利用できる製品を探したところ，SIP プロキシサーバと SIP リダイレクトサーバの 2 種類の方式があることが分かった。②G 君はこれらのうち Z 社のネットワークセキュリティポリシに合った方式を選択した。開発ベンダは該当する製品を扱っていなかったので，候補の製品はほかのベンダのものを選んだ。図 5 は，SIP 中継サーバを利用したネットワークシステムの構成変更案である。

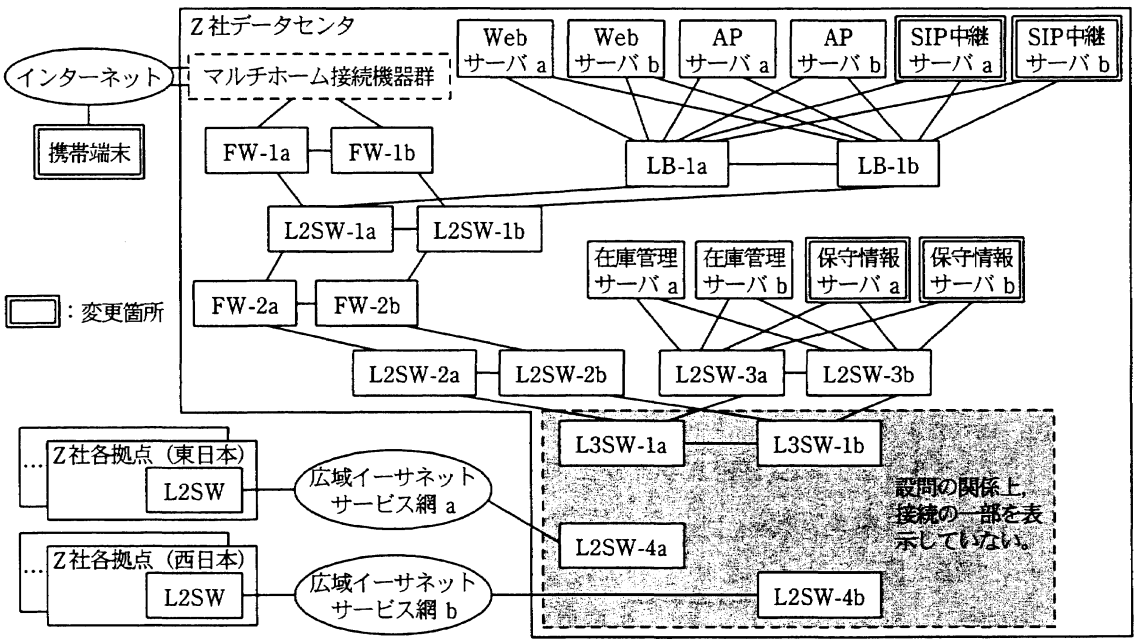


図 5　ネットワークシステムの構成変更案

次に，G 君は通信データの暗号化対策として，TLS と S/MIME を比較した。IP パケットの中で暗号化されるデータの範囲は，TLS の方が S/MIME よりも広く，それだけ情報漏えいのリスクは低い。一方，暗号化区間に関しては，S/MIME では携帯端末と保守情報サーバを暗号化区間にできるが，③TLS では携帯端末と対向させる暗号化区間のエンドポイントを途中に置かなければならない。G 君はインターネット上の通

信データに対する安全性を重視し，TLS を採用した構成案を作ることに決めた。

続いて，G 君は携帯端末と保守情報サーバの間の通信に関する認証について検討した。ポータルシステムでは，HTTP ダイジェスト認証と TLS の認証を利用している。運用も確立しており，保守情報システムでも同じ認証方式を採用したい。保守情報システムのミドルウェアは，これらの認証機能をもっており，システム開発に関する問題はないと思われる。しかし，認証情報の運用については確認が必要である。多数の携帯端末に，それぞれ異なる認証情報を登録するような運用は避けたい。

最後に，G 君は FW-1a と FW-1b の定義について検討した。FW-1a と FW-1b 上で稼働している TCP/IP フィルタに関しては，新たな TCP/IP 通信の定義を追加すればよい。しかし，NAT に関しては細部の確認が必要である。例えば，図 5 の構成において図 4 の行番号 2 の Via ヘッダフィールドには，保守情報サーバではなく SIP 中継サーバのアドレス情報が格納されることになる。④図 4 の SIP メッセージを受け取った携帯端末のミドルウェアが，その応答を Via ヘッダフィールドに指定されたアドレスに返す仕様になっているような場合，NAT だけではその応答は正しく SIP 中継サーバに戻らない。

このように，ネットワークセキュリティ対策を検討していくうちに，ミドルウェアに関して確認すべき点が幾つか出てきた。G 君はそれらを開発ベンダに問い合わせた。図 6 は，G 君の問合せに対する開発ベンダからの回答の一部である。G 君はこの回答を基に，ネットワークセキュリティ対策案を完成させた。

(質問 1) SIP中継サーバを使う場合のあて先の指定方法を教えてください。
回答：各機器のミドルウェアに関する定義情報の中に，SIP中継サーバのIPアドレス情報をあらかじめ登録しておきます。その際，プライマリとセカンダリの二つを登録できます。ミドルウェアは，登録されたSIP中継サーバとの間でTCPコネクションを確立します。
(質問 2) 携帯端末と保守情報サーバ間の通信において，TCPコネクションはどちらの方向から確立されるのでしょうか。
回答：TCP コネクションは，常に，携帯端末から保守情報サーバの方向に確立されます。
(質問 3) TCPコネクションのあて先とViaヘッダフィールドで指定された送信元が異なる場合，SIP リクエストに対するレスポンスはどこに送り返されますか。
回答：TCPコネクションが優先され，TCPコネクションのあて先にレスポンスが返ります。

図 6　開発ベンダからの回答（抜粋）

〔既設機器の変更〕

G君は，図5の構成案を基に既設機器に関する変更箇所を整理した。⑤変更が必要な既設機器は，FW-1a，FW-1b，LB-1a，LB-1bなど合計8台である。G君は各機器の構成管理表や運用に関する文書を入手して詳細を調べ，ハードウェアの増強や新たな変更手順などが不要なことを確認した。そして，各機器の変更箇所を構成管理表のコピーに記入した。表1と表2はその一部である。

表1　G君が変更したFW-1aの構成管理表のコピー（抜粋）

1. ポート情報

ID	速度/モード	設定	接続先機器名	接続先VLAN名
P1	auto/auto	active	マルチホーム接続機器群	VLAN-EX
P2	auto/auto	active	L2SW-1a	VLAN-D0
P9	auto/auto	active	FW-1b	VLAN-R8

2. IP情報

ID	所属VLAN	実IPアドレス	仮想IPアドレス（アクティブスタンバイ共有）
I1	VLAN-EX	x.y.z.210	x.y.z.211
I2	VLAN-D0	192.168.60.206	192.168.60.209

3. NAT情報

ID	所属ポート	外部IPアドレス	内部IPアドレス	接続先機器名
N1	P1	x.y.z.213	192.168.60.161	Webサーバ（仮想IPアドレス）
N2	P1	x.y.z.214	192.168.61.100	Webサーバa
N3	P1	x.y.z.215	192.168.61.101	Webサーバb
N4	P1	x.y.z.216	192.168.60.163	SIP中継サーバ（仮想IPアドレス）
N5	P1	x.y.z.217	a	SIP中継サーバa
N6	P1	x.y.z.218	b	SIP中継サーバb

4. ファイアウォール情報（ポートP1に対するTCP/IPフィルタリングの定義）

ID	送信元IPアドレス	あて先IPアドレス	サービス	フィルタの動作
F1	any	x.y.z.213	http,https	Accept
⋮	⋮	⋮	⋮	⋮
Fn	any	c	sip,sips	Accept
⋮	⋮	⋮	⋮	⋮

注　x.y.z.210，x.y.z.211，x.y.z.213 ～ x.y.z.218は，グローバルIPアドレスを表す。

表２　G 君が変更した LB-1a の構成管理表のコピー（抜粋）

1. ポート情報

ID	速度/モード	設定	接続先機器名	接続先 VLAN 名
P1	auto/auto	active	Web サーバ a	VLAN-D1
P2	auto/auto	active	AP サーバ a	VLAN-D2
P3	auto/auto	active	SIP 中継サーバ a	VLAN-D3
P4 ～ P15	auto/auto	disable	－	－
P16	auto/auto	active	L2SW-1a	VLAN-D0
P17	auto/auto	active	Web サーバ b	VLAN-D1
P18	auto/auto	active	AP サーバ b	VLAN-D2
P19	auto/auto	active	SIP 中継サーバ b	VLAN-D3
P20 ～ P31	auto/auto	disable	－	－
P32	auto/auto	active	LB-1b	VLAN-R9

2. IP 情報

ID	所属 VLAN	実 IP アドレス	仮想 IP アドレス（アクティブスタンバイ共有）
I1	VLAN-D0	192.168.60.221	192.168.60.229
I2	VLAN-D1	－	192.168.61.229
I3	VLAN-D2	－	192.168.62.229
I4	VLAN-D3	－	192.168.63.229

3. 負荷分散情報

ID	サーバ仮想 IP アドレス	サーバ実 IP アドレス	サービス	SSL アクセラレータ機能
D1	192.168.60.161	192.168.61.100	https	有
		192.168.61.101		
D2	192.168.60.162	192.168.62.100	rpc	無
		192.168.62.101		
D3	192.168.60.163	192.168.63.100	sips	有
		192.168.63.101		

〔実機検証案〕

以上の検討から変更案はまとまったが，そこには今回の机上検討だけでは確認が不十分と思われる部分も含まれていた。そこで，G 君は実機を使った動作検証を提案することにした。また，検証で問題があった場合でも図 5 の構成案に新たなネットワーク機器を追加しなくても実現できる代替案を提示することにした。

G 君は，実機による動作検証と問題があった場合の代替案の組合せを，表 3 に示すように三つにまとめ，ネットワークシステムの変更案に付け加えた。

表3　実機検証と代替案

項番	実機による検証内容	問題があった場合の代替案
1	携帯端末と保守情報サーバのミドルウェア間の通信が，SIP 中継サーバによって中継可能かどうかを検証する。	保守情報サーバを DMZ に設置し，SIP 中継サーバは使用しない。
2	携帯端末と LB の SSL アクセラレータ機能間の TLS が正常に動作し，データの暗号化が正常に行われることを検証する。	d
3	携帯端末から SIP 中継サーバ，保守情報サーバへアクセスする際，LB による振分けが正常に行われることを検証する。	e

依頼を受けてから 2 週間後，G 君は，図 5，表 1～3 を中心としたネットワークシステムの変更案を M 氏に提出した。

その後，G 君の変更案は正式に採用され，ネットワークシステムの変更作業が始まった。実機検証作業のリーダに任命された G 君は，実機検証作業の作業計画を作ることになった。作成に先立ち，G 君は上司から，短期間に十分な評価を行うために，実施体制と検証環境について十分に検討するよう指示を受けた。

G 君は，ネットワーク技術グループのメンバ以外にテストプログラムの担当も参加させること，開発ベンダや製品ベンダのサポート体制を確保することなどを計画に盛り込んだ。また，⑥検証環境についても，SIP 中継サーバ，LB，携帯端末，保守情報サーバを用意する前提で，上司の指示を参考に十分な配慮を行った。

実機検証以降，ネットワークシステムの変更作業は順調に進んだ。半年後，保守情報システムは予定どおりに本番稼働を迎えた。

設問1　〔Z 社のネットワークシステム〕について，(1)～(5)に答えよ。

(1) 図 1 中の機器のうち，ポータルシステムの通信において，TCP/IP ヘッダの IP アドレスを書き換える機器が四つ（2 組）ある。それらをすべて答えよ。ただし，マルチホーム接続機器群とサーバは除く。

(2) 本文中の下線①の三つの監視用 URL の IP アドレスを，表 1 中の表記を用いて答えよ。

(3) 本文中の下線①において，監視用 URL の応答はすべて正常だが，公開 URL の応答が異常だった場合，疑うべき障害箇所を答えよ。

(4) 本文中の下線①において，公開 URL の応答は正常だが，監視用 URL の応答に異常がある障害の例を，図 1 中の機器名を用いて 25 字以内で述べよ。

(5) 図 1 において，L3SW-1a，L3SW-1b，L2SW-4a，L2SW-4b 間の接続を解答欄

に図示せよ。また，図示した構成において，L3SW-1a，L3SW-1b に定義する VRRP の仮想ルータの数を答えよ。ただし，L3SW-1a の L2SW-2a と L2SW-3a への接続ポートには，別の VLAN が定義されているものとする。

設問 2　〔ミドルウェア〕について，(1) ～ (3)に答えよ。

(1) 本文中の［ア］～［カ］に入れる適切な字句を答えよ。

(2) 本文中の［キ］に入れる適切な図 4 中の字句を答えよ。

(3) 本文中の［ク］に入れる適切な図 4 中の行番号を答えよ。

設問 3　〔ネットワークセキュリティ対策〕について，(1) ～ (4)に答えよ。

(1) 本文中の下線②において，G 君が選択した方式を答えよ。また，その方式を選択した理由を，40 字以内で述べよ。

(2) 本文中の下線③において，携帯端末と対向させる暗号化区間のエンドポイントに関する TLS の制約を，図 5 中の機器名を用いて 40 字以内で述べよ。

(3) 本文中の下線④において，Via ヘッダフィールドのアドレスがどのような場合に応答が正しく戻らないか。20 字以内で述べよ。

(4) 図 6 中の質問 2 は，どのネットワークセキュリティ対策案の完成のための質問か。G 君が検討したセキュリティ対策のうち，質問 2 の確認が必要な対策を二つ挙げ，それぞれ 30 字以内で述べよ。

設問 4　〔既設機器の変更〕について，(1) ～ (3)に答えよ。

(1) 表 1 中の［a］～［c］に入れる適切な IP アドレスを答えよ。

(2) 表 2 において，G 君が追加したすべての行を，行番号で答えよ。

(3) 本文中の下線⑤に示された 2 組以外の既設機器を 1 組選び，機器名とその機器に対する変更内容を，合わせて 40 字以内で述べよ。

設問 5　〔実機検証案〕について，(1) ～ (4)に答えよ。

(1) 表 3 中の項番 1 の代替案を採用した場合の表 1 の変更箇所と変更内容を合わせて，30 字以内で述べよ。

(2) 表 3 中の項番 1 の代替案を採用した場合，変更案と比較して，どのような運用上の注意が必要か。30 字以内で述べよ。

(3) 表 3 中の［d］，［e］に入れる代替案を，それぞれ 40 字以内で述べよ。

(4) 本文中の下線⑥において，G 君が配慮すべき点を二つ挙げ，それぞれ 20 字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

7. 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	14:50 ～ 16:00

8. **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。
9. 問題冊子の余白などは，適宜利用して構いません。
10. 試験中，机上に置けるもの及び使用できるものは，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，黒鉛筆又はシャープペンシル，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，ティッシュ

    これら以外は机上に置けません。使用もできません。
11. 試験終了後，この問題冊子は持ち帰ることができます。
12. 答案用紙は，いかなる場合でも，すべて提出してください。回収時に提出しない場合は，採点されません。
13. 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。