平成１８年度　秋期　テクニカルエンジニア（ネットワーク）　午後Ⅰ問題

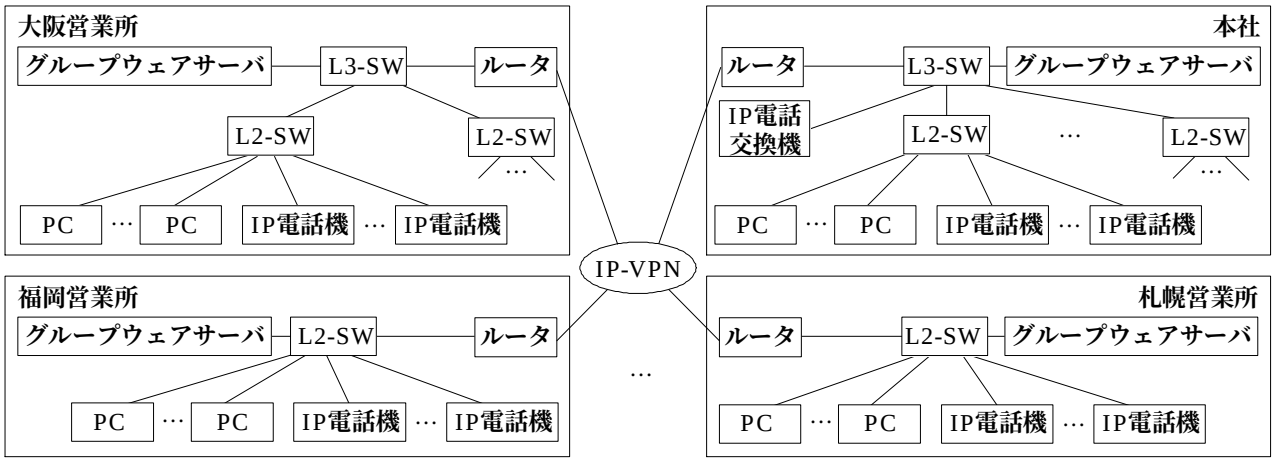
問１　ネットワークの再構築に関する次の記述を読んで，設問 1～3 に答えよ。

Z 社は，通信機器の販売及びネットワークの設計，構築を行っている。このたび，Z 社では，衣料品販売会社である X 社からネットワーク再構築の案件を受注した。

次は，Z 社の U 君が，X 社のネットワークの調査結果を基に，T 主任と再構築の検討をしているときの会話である。

〔再構築の検討〕

U 君：X 社は，東京にある本社と全国 9 か所の営業所を，IP-VPN を使って接続しています。現在の X 社のネットワーク構成を，図 1 に示します。X 社からは，通信経費の削減のために，通信回線を見直したいとの要求がありました。X 社には，本社内や各営業所内の LAN 構成は変更せずに，IPsec を使ったインターネット VPN への置換えを提案するつもりです。トラフィックは，本社と各営業所間だけでなく，各営業所間でも多いことが分かりました。これは，グループウェアサーバ間の通信と，IP 電話の通信によるものです。



L3-SW：レイヤ3スイッチ
L2-SW：レイヤ2スイッチ

図１　現在のＸ社のネットワーク構成

T 主任：なるほど。IPsec での仮想的な通信路を SA（Security Association）というが，トラフィック要件からは，①本社と各営業所のルータ間だけに SA を確立する構成は，適当ではなさそうだな。

U 君：はい。すべてのルータ間で SA を確立する構成が望ましいと考えています。でも，ルータの台数が多いので，設定が大変になりそうです。

T 主任：確かにそうだな。IPsec では，ルータ間に鍵交換用の［　ア　］SA が一つとデータ通信用の Ipsec SA が二つ確立されるので，すべてのルータ間で SA を確立すると，SA の合計数は［　a　］になる。さらに，Ipsec SA の［　イ　］鍵を更新するリキー（Re-keying）が行

われると，後続して使用される IPsec SA が新たに確立されるので，一時的に SA の合計数が増加する。X 社の案件には，新型ルータを採用してはどうか。このルータには，本社と各営業所のルータ間に固定的に SA を確立させる設定を行えば，通信する IP パケットの検知を契機に，各営業所のルータ間の SA を動的に確立する機能がある。ところで，インターネット接続回線と通信速度はどうするのかな。

U 君：本社では，FTTH を使用して 50M ビット／秒を見込んでいます。各営業所では，ADSL を使用してインターネットからの受信方向（以下，下り方向という）に 10M ビット／秒を見込んでいます。それぞれの接続回線について，ルータに固定 IP アドレスを割り当てるサービスを利用する予定です。

T 主任：分かった。新型ルータは，まだ当社では導入実績がないので，ルータの機能や負荷を検証すべきだろう。IPsec 通信では，IP パケットの転送処理に加え，ヘッダを付加してパケットを構成する［　ウ　］化や暗号化の処理の負荷を考慮する必要があるのは知っているかな。

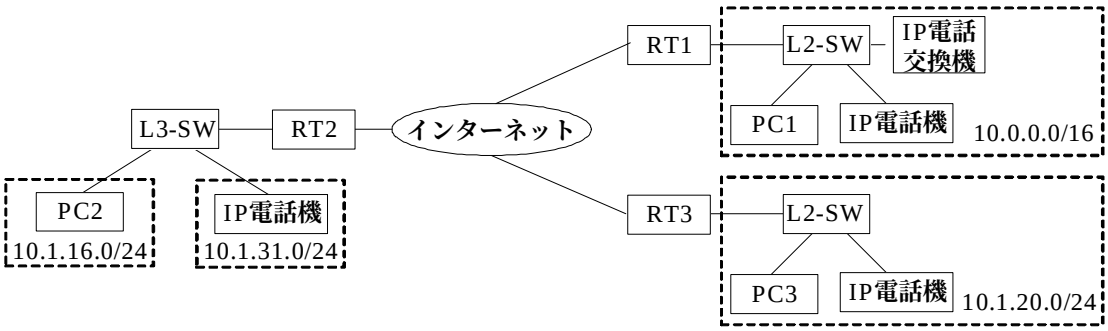
U 君：理解しています。それから，大阪営業所内の LAN には，連続していない二つのネットワークアドレスが割り当てられていますが，大丈夫でしょうか。

T 主任：経路集約ができれば問題ないと思うが，確認してみた方がいいな。

U 君：はい，分かりました。早速やってみます。

〔試験用ネットワークによる新型ルータの検証〕

U 君は，図 2 の試験用ネットワークを構築して新型ルータの検証に着手した。図 2 中の RT1 は本社に，RT2 は大阪営業所に，RT3 はそのほかの営業所に，それぞれ提案を予定している新型ルータである。インターネット接続回線は，再構築後のネットワークと同じ回線種別，サービスを使用している。



注 10.1.16.0/24，10.1.20.0/24，10.1.31.0/24 及び 10.0.0.0/16 は，ネットワークアドレスを示す。

図２　試験用ネットワークの構成

初めに，U 君は，RT1～RT3 に設定を行い，RT1 と RT2 間及び RT1 と RT3 間に SA を確立させた。SA を通過させる IP パケットのアクセス制御規則である［　エ　］には，あて先 IP アドレス空間の情報があり，経路表のエントリのあて先ネットワークアドレスに使用される。RT1 の経路表には，RT2 あてに経路集約されたネットワークアドレス 10.1.16.0/［　b　］のエントリが，RT3 あてに 10.1.20.0/24 のエントリが，それぞれ登録されている。RT3 あてのエントリに合致するあて先 IP アドレス空間は，RT2 あてのエントリにも合致するが，②経路選択アルゴリズムによって制御されるので混

乱は起こらない。

次に，RT2 の負荷を検証した。RT2 のインターネット接続回線の下り方向の通信容量と通信効率を考慮して，PC1 から PC2 にあてて 8M ビット／秒のトラフィックを加えたい。検証には，表の IP パケットを連続的に発生させるように，T 主任から指示されている。そこで，PC1 と PC2 のソフトウェアに対して，表の IP パケットが，1 秒当たり［　c　］組送信されるように設定した。

表　検証で使用するＩＰパケット

IP パケット長	パケット数
40 バイト	10
520 バイト	5
1,400 バイト	5

続いて，RT2 と RT3 間の SA の確立及び切断を検証した。RT1～RT3 の動作は，次のとおりである。RT1 と RT2 間及び RT1 と RT3 間に SA を確立した後に，RT1 は RT3 に対して，RT2 の IP アドレスと RT2 へ転送すべきあて先ネットワークアドレスを通知する。また，RT1 は RT2 に対して，RT3 の IP アドレスと RT3 へ転送すべきあて先ネットワークアドレスを通知する。RT2 及び RT3 は，RT1 から受け取った IP アドレスとあて先ネットワークアドレスを，経路表のエントリに登録する。RT2 は，RT3 あての IP パケットの検知を契機に RT3 と SA を確立し，RT2 と RT3 間の通信を可能にする。RT3 が RT2 あての IP パケットの検知を契機に，SA を確立してもよい。RT2 と RT3 間の通信が一定時間なければ，SA は切断される。

U 君は，試験用ネットワークによる検証によって，新型ルータの動作が仕様どおりであり，新型ルータの負荷による通信への支障もないことを確認した。

最後に，U 君は，新型ルータの優先制御を検証した。新型ルータには，IP ヘッダのフィールド値を参照して選択した IP パケットを，最優先で送信する機能がある。IP 電話の通信による IP パケットでは，IP ヘッダの［　オ　］フィールドにある優先ビットが，ほかの通信による IP パケットのものより大きな値である。この点に着目して RT1～RT3 の設定を行い，インターネットに送信される IP パケットを測定器で観察して，優先制御が機能していることを確認した。

U 君は，③再構築の検討で T 主任が指摘した以外にも，新型ルータに負荷があることに気付き，その確認も含めて，検証結果を T 主任に報告した。また，T 主任は，④各営業所では動的 IP アドレス割当てのサービスを利用すれば，通信経費をより削減可能であることを指摘し，X 社への提案に盛り込むよう U 君に指示した。

設問１　本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

設問２　〔再構築の検討〕について，(1)，(2) に答えよ。

（1）本文中の［　a　］に入れる適切な数値を答えよ。

（2）本文中の下線①の構成では，検討後の構成と比較すると，各営業所間の通信遅延が増加する。その増加要因を二つ挙げ，それぞれ 25 字以内で述べよ。

設問３　〔試験用ネットワークによる新型ルータの検証〕について，(1)～(4) に答えよ。

（1）本文中の［　b　］，［　c　］に入れる適切な数値を答えよ。

（2）本文中の下線②の仕組みを，40 字以内で述べよ。

（3）本文中の下線③について，新たに U 君が気付いた新型ルータの負荷とは何か。15 字以内で述べよ。

（4）本文中の下線④を利用しても，各営業所の新型ルータ間で SA の確立が可能であるのは，新型ルータのどのような動作によるものか。40 字以内で述べよ。

問２　ネットワークシステムの改善に関する次の記述を読んで，設問 1～3 に答えよ。

A 社は，社内に 300 台の PC を設置し，ファイルサーバによる情報共有や，インターネット上の Web サーバのアクセスなどに利用している。PC は，IEEE 802.11b 規格の無線 LAN（以下，無線 LAN という）を経由して，社内のサーバやインターネットに接続する。B 君と C 君は，ネットワークシステム担当である。C 君は入社 2 年目で，先輩の B 君の指示に従って作業を行う場合が多い。

図 1 に，A 社ネットワークシステムの構成を示す。

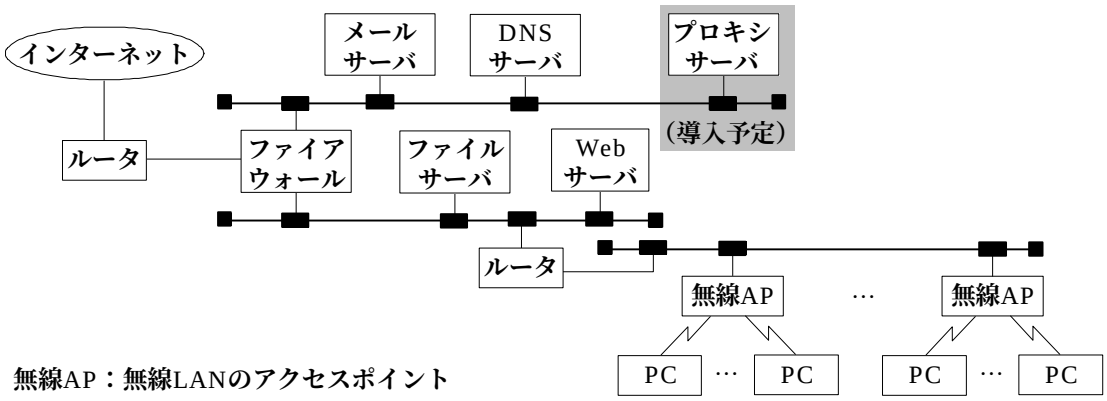


図１　Ａ社ネットワークシステムの構成

最近，ある部署から，ファイルサーバのレスポンスが遅いという指摘があった。その部署の PC とファイルサーバ間のファイル転送時間を実測したところ，通常時と最繁時とでは転送時間が異なることが分かった。C 君は，有線 LAN に比べて伝送速度が遅い無線 LAN がボトルネックになっていると考え，B 君に無線 LAN のスループットについて質問した。次は，無線 LAN のスループットに関する B 君の説明である。

〔無線 LAN のスループット〕

無線 LAN のアクセス制御方式は［　a　］と呼ばれ，IEEE 802.3 規格の LAN における CSMA/CD に相当する。無線 LAN の伝送速度は，通信状態によって 1M ～［　b　］M ビット／秒の間で変化する。ただし，プリアンブルを含む物理ヘッダの伝送速度は固定されている。

図 2 に，無線 LAN の伝送フレームの形式と伝送時間を示す。

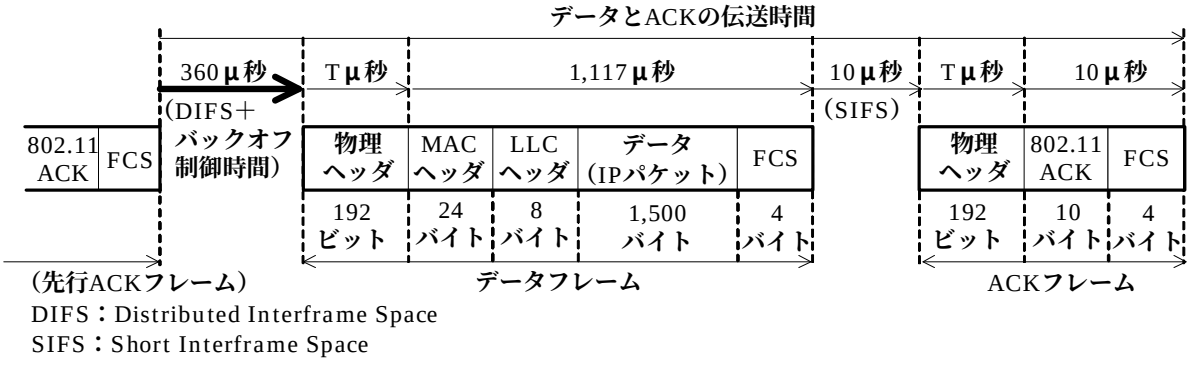


図２　伝送フレームの形式と伝送時間

図 2 中の各時間は，最大伝送速度における所要時間を示している。ただし，①バックオフ制御時間はランダムなので，先行 ACK フレームの伝送完了からデータフレーム送信開始までの待ち時間（図 2 中の太線矢印）は，平均値を用いている。

これらを利用すると，無線 LAN のスループットの上限は次の式のように算出でき，その値は 6M ビット／秒以上 7M ビット／秒未満となる。

無線 LAN のスループットの上限
＝（データ長）÷（データと ACK の伝送時間）
＝（1,500×8）ビット÷（360＋T＋1,117＋10＋T＋10）μ秒

〔ファイル転送のスループット〕

図 2 中のデータフレームが，図 1 中の PC からファイルサーバへの転送データであるとしたとき，MAC ヘッダには，三つの MAC アドレスが設定され，あて先が [c]，送信元が [d]，BSSID（Basic Service Set ID）が [e] となっている。

PC とファイルサーバ間の通信において，IP ヘッダと TCP ヘッダをそれぞれ 20 バイトとし，データフレームの分割は発生しないとしたとき，ファイル転送のスループットを最大にするには，TCP のデータ長を [f] バイトにすればよい。A 社では，無線 AP を導入する際，ファイルサーバのパラメタなどを調整し，ファイル転送のスループットを実測した。その結果，②PC やファイルサーバなどの機器の応答時間を除外した上限値である約 5M ビット／秒に近い値が得られている。

ファイルサーバのレスポンスが遅くなる部署では，トラフィックの増加に対応するために，昨年，無線 AP を 1 台増設して 2 台の無線 AP を利用している。B 君は，無線 AP の増設作業に問題があったと考え，作業を行った C 君に内容を確認した。C 君の説明は，次のとおりであった。

・60 台の PC の中から，増設した無線 AP に収容する 30 台の PC を選んだ。
・増設した無線 AP に，新しい SSID と WEP（Wired Equivalent Privacy）キーを設定した。利用周波数は，無線 AP に設定されていた既定値をそのまま使った。
・選んだ 30 台の PC には，増設した無線 AP と同じ SSID と WEP キーを設定した。
・二つの無線 AP に対し，それぞれ収容した PC とファイルサーバ間でファイル転送を行った。ファイル転送のスループットは，いずれも約 5M ビット／秒であった。

B 君は C 君の説明を聞き，ファイル転送が遅くなるのは③C 君の設定の誤りが原因ではないかと指摘した。二つの無線 AP は SSID によって識別され，一方の無線 AP とそこに収容した PC との通信は可能である。しかし，C 君の設定では二つの無線 AP が同時に通信を行うことはできないので，無線 LAN のスループットは低下する可能性がある。

C 君が B 君の指摘を基に設定を修正したところ，最繁時でも通常時と同じファイル転送のスループットが得られるようになった。

〔プロキシサーバの導入〕

A 社では，定期的にファイアウォールの稼働状況を確認している。インターネット上の Web アクセスは年々増加しており，このままではファイアウォールの CPU 使用率が限界に達することが予想された。ベンダに相談したところ，A 社がインターネット上の Web アクセスに利用している NAPT（Network Address Port Translation）の負荷が高く，プロキシサーバを新たに設置すれば改善可能であることが分かった。A 社はプロキシサーバの導入を決め，B 君が導入計画を作成することになった。導入計画では，業務に支障が出ないよう 1 か月の並行稼働期間を設けることにした。

プロキシサーバを利用するには，PC の Web ブラウザにプロキシサーバの情報を設定する必要がある。その方法としては，プロキシサーバの IP アドレスを直接設定する方法と，プロキシサーバの利用情報を定義したファイル（以下，自動設定ファイルという）を Web サーバに登録し，その登録場所の URL を PC の Web ブラウザに設定する方法とがある。B 君はこれらの方法を比較し，自動設定ファイルを用いる方法を採用した。URL を 300 台の PC に設定する作業は，利用者の業務の合間を利用して順次行うことにした。図 3 に，B 君が作成した導入作業スケジュールを示す。

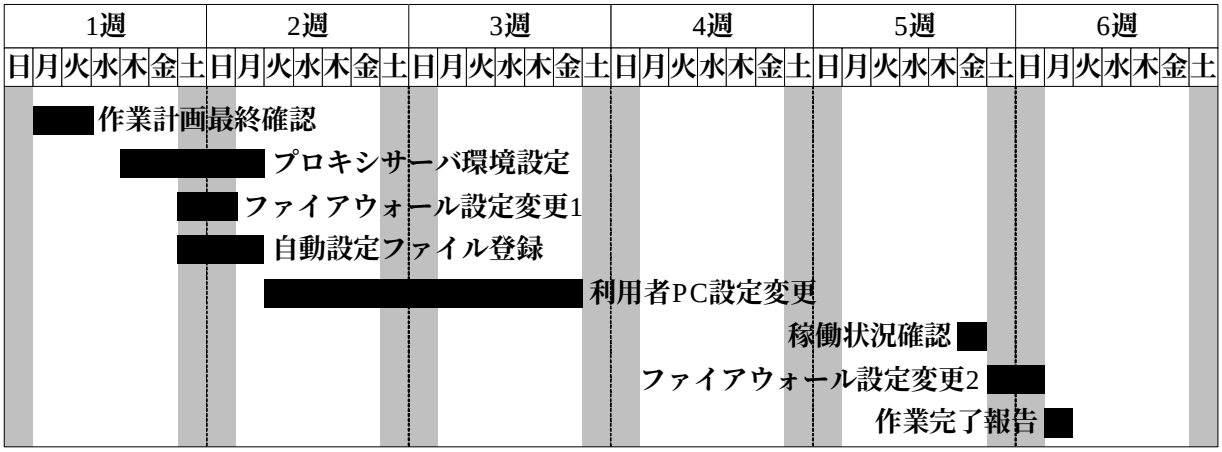


図３　プロキシサーバの導入作業スケジュール

B 君と C 君は導入作業スケジュールに従って予定どおりに作業を終え，ファイアウォールのボトルネックを未然に防ぐことができた。

設問１　〔無線 LAN のスループット〕について，(1)～(3) に答えよ。

（1）本文中の［ a ］，［ b ］に入れる適切な字句を答えよ。

（2）本文中の下線①について，IEEE 802.11b 規格では，バックオフ制御時間をランダムにしている理由を，20 字以内で述べよ。

（3）図 2 中の T を求めよ。

設問２　〔ファイル転送のスループット〕について，(1)～(4) に答えよ。

（1）本文中の［ c ］～［ e ］に入れる図 1 中の機器名を答えよ。

（2）本文中の［ f ］に入れる適切な数値を答えよ。

（3）本文中の下線②について，ファイル転送の最大スループットが，無線 LAN のスループットの上限に達しない理由を，30 字以内で述べよ。

（4）本文中の下線③について，C 君の設定の誤りを，20 字以内で述べよ。

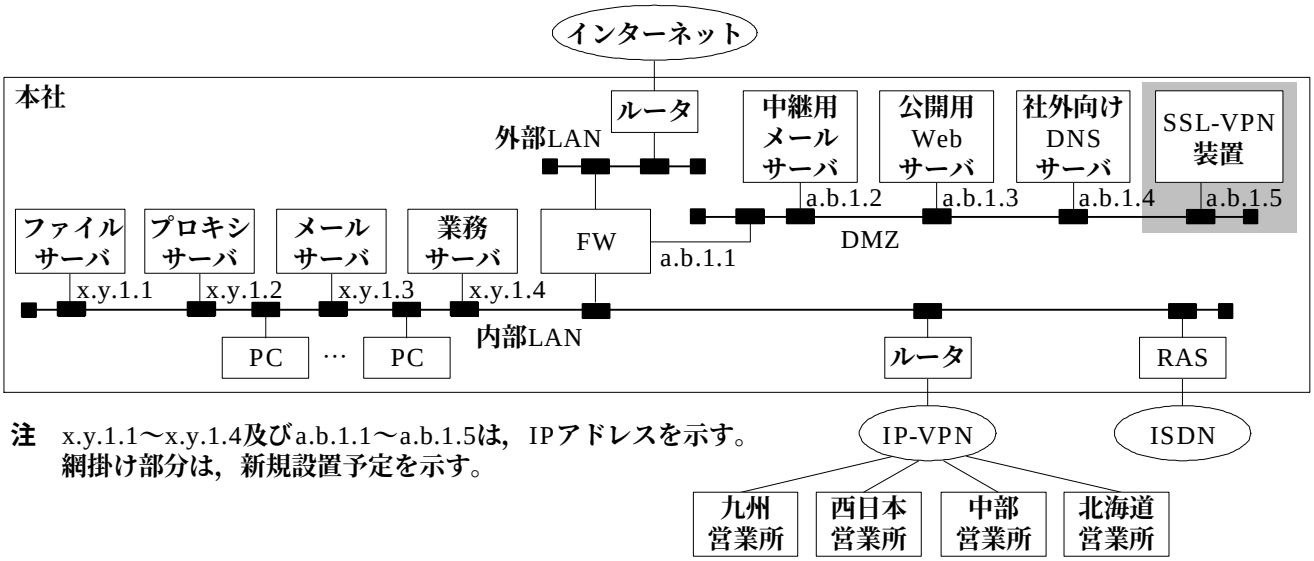
設問３　〔プロキシサーバの導入〕について，(1)，(2) に答えよ。

（1）自動設定ファイルを用いる方式は，導入作業上どのような利点があるか。30 字以内で述べよ。

（2）図 3 中のファイアウォール設定変更 1，2 の作業内容を，それぞれ 40 字以内で述べよ。

問３　リモート接続の見直しに関する次の記述を読んで，設問 1～4 に答えよ。

Y 社は，東京に本社があり，全国に 4 か所の営業所をもつ，社員数 300 名の情報機器販売会社である。本社と各営業所には，LAN が設置されている。これらの LAN は，IP-VPN によって相互に接続され，Y 社ネットワークを構成している。120 名の営業員は，社外から携帯用のノート PC（以下，モバイル PC という）を使って，本社のファイアウォール（以下，FW という）の内側に設置されたリモートアクセスサーバ（以下，RAS という）に PIAFS 方式でリモート接続し，Y 社ネットワークを利用している。RAS を経由した Y 社ネットワークの利用においては，社内と同様の作業が行える。図 1 に，Y 社ネットワークの構成を示す。



注　x.y.1.1～x.y.1.4及びa.b.1.1～a.b.1.5は，IPアドレスを示す。
網掛け部分は，新規設置予定を示す。

図１　Ｙ社ネットワークの構成

最近，モバイル PC の活用が進み，社外からの Y 社ネットワークの利用頻度が高まっている。その結果，回線がつながらず，業務に支障を来しているというクレームが寄せられるようになった。また，リモート接続を行うための通信費の削減と，社外から行うことのできる作業を制限するセキュリティ対策も求められるようになった。そこで，これらの問題を解決するために，情報システム部の K 課長はネットワーク担当の F 君に対し，リモート接続方式の改善策の検討を指示した。

〔リモート接続方式の検討〕

最初に，F 君は，リモート接続方式について検討した。その結果，インターネットを経由した接続方式に変更すれば通信費を削減できるとともに，回線がつながらないという問題も解決できることが分かった。この方式では，セキュリティ確保のための対策が必要になるので，SSL によって VPN を構成する SSL-VPN 装置について調査した。

初期の SSL-VPN 装置は，SSL のサーバ機能と，［　ア　］プロキシ機能だけで構成されていたこともあって，Web ブラウザ（以下，ブラウザという）を使用するアプリケーションしか利用できなかった。改善策として，①SSL のクライアントとなる，ローカルプロキシ機能をもつ Java アプレットを，

モバイル PC で動作させる方式が考えられた。この方式によって，SSL に未対応の多くのアプリケーションを，プログラムの変更なしに SSL に対応させられるようになった。Java アプレットは，アプリケーションが使用する TCP のポート番号が含まれたパケットを待ち受け，これを受け取ると SSL-VPN 装置との間で SSL を利用した通信（以下，SSL 通信という）を行う。SSL-VPN 装置は，モバイル PC から受信したパケットを，ポート番号に対応付けられたサーバあてに転送することで，モバイル PC とサーバ間の通信を可能にする。この転送は，［　イ　］フォワードと呼ばれている。モバイル PC で動作させる Java アプレットは，②SSL-VPN 装置からダウンロードされる。また，社外から行うことのできる作業は，SSL-VPN 装置と FW によって制限できる。

F 君は，この SSL-VPN 装置の利用によって，リモート接続方式を改善できると判断した。

〔SSL-VPN 装置の利用方法の検討〕

次に，F 君は，SSL-VPN 装置の利用方法について検討した。SSL-VPN 装置を経由したアプリケーションの利用は，次の手順で行われる。

（1）モバイル PC でブラウザを起動し，HTTPS で SSL-VPN 装置に接続する。
（2）モバイル PC に表示される認証画面で，認証情報を入力する。
（3）モバイル PC に表示される利用可能なアプリケーションのリストの中から，利用するアプリケーションを選択して起動する。

手順(1)によって，SSL 通信が開始される。手順(2)，(3)は，SSL-VPN 装置とモバイル PC 間での相互認証完了後に実施される。図 2 に，SSL 通信のシーケンスを示す。

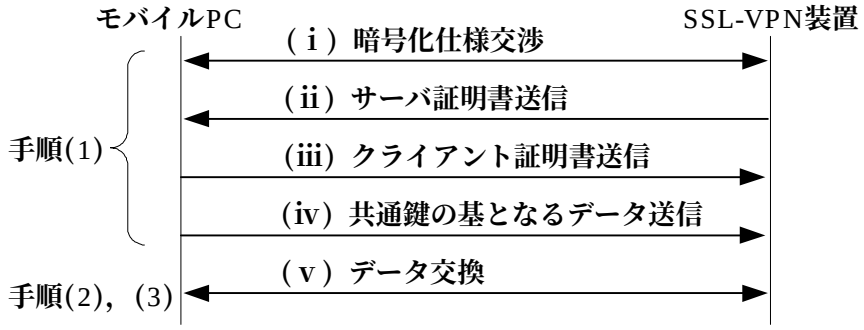


図２　ＳＳＬ通信のシーケンス（概略）

図 2 中の(ⅱ)で，SSL-VPN 装置は，自らを認証してもらうために，サーバ証明書を送信する。［　ウ　］は，サーバ証明書を発行した CA 局の証明書を保持しているので，この③証明書に含まれる鍵を使って，サーバ証明書の正当性を検証する。(ⅲ)はオプション処理で，クライアント証明書による認証が要求されていたときに実施される。(ⅳ)によって，モバイル PC と SSL-VPN 装置の双方で，共通鍵が生成される。

RAS では，パスワードによる利用者認証のほかに，認証された利用者の情報を基にして，RAS から再接続を行う［　エ　］によって，Y 社ネットワークの不正利用を防止している。そこで，SSL-VPN 装置では，手順(2)の認証だけでなく，(ⅲ)も利用して 2 要素認証を行うことにした。クライアント証明書の使用方法は幾つか考えられるが，今回は，④モバイル PC に管理者がインストールして使用するこ

とにする。

〔SSL-VPN 装置の設置の検討〕

最後に，F 君は，SSL-VPN 装置の設置について検討した。社外からの内部 LAN の利用は，SSL-VPN 装置を経由して行わせる。SSL-VPN 装置は，安全性を考慮して図 1 に示した場所に設置する。モバイル PC とサーバ間の通信が，SSL-VPN 装置を経由して行われるように，SSL-VPN 装置は，モバイル PC から受信したパケットの送信元 IP アドレスと⑤あて先 IP アドレスに変換を施して転送する。

現在，インターネットを経由した Y 社のサーバとの通信は，DMZ に設置されているサーバだけに制限されている。そのため，SSL-VPN 装置の設置によって，FW の設定変更が必要になる。表に，FW に追加で許可する通信内容を示す。

表　ＦＷに追加で許可する通信内容

通信方向	送信元 IP アドレス	あて先 IP アドレス	あて先ポート番号
方向 1	任意	a.b.1.5	オ
カ	キ	ク	15000
方向２	a.b.1.5	ケ	25
方向２	a.b.1.5	x.y.1.3	110

注１　Y 社で利用する主要アプリケーションのポート番号を，次に示す。
SMTP：25，POP3：110，HTTP：80，HTTPS:443，DOMAIN：53
業務用アプリケーションプロトコル:15000

注２　表中の通信方向は，次のように定義する。
方向 1：外部 LAN から DMZ 向け，方向 2：DMZ から内部 LAN 向け

注３　表中では，戻りパケットに関する通信内容を省略している。

F 君は，以上の結果を基にリモート接続方式の改善策をまとめ，K 課長に報告した。K 課長は，改善策の実施によって問題を解決できると判断し，再構築を進めることにした。

設問１　本文中の［　ア　］～［　エ　］に入れる適切な字句を答えよ。

設問２　SSL-VPN 装置について，(1)，(2) に答えよ。

(1) 本文中の下線①の方式でも，SSL に対応させることのできないアプリケーションがある。それはどのような IP 通信の特徴をもったアプリケーションか。25 字以内で述べよ。

(2) 本文中の下線②によって容易になる点を，25 字以内で述べよ。

設問３　SSL の動作について，(1)，(2) に答えよ。

(1) 本文中の下線③の鍵の種類を答えよ。

(2) 共通鍵が利用される場所を，図 2 中の(ⅰ)～(ⅴ) で答えよ。また，共通鍵を利用することによる利点を，15 字以内で述べよ。

設問４　SSL-VPN 装置の導入について，(1)～(4) に答えよ。

（1）表中の［　オ　］～［　ケ　］に入れる適切な字句を答えよ。

（2）本文中の下線④によって可能となる接続制御の内容を，30 字以内で述べよ。

（3）本文中の下線⑤は何に変換されるか。25 字以内で述べよ。

（4）SSL-VPN 装置の設置によって実施される，認証と暗号化以外のセキュリティ対策の内容を，25 字以内で述べよ。

問４　インターネット販売システムに関する次の記述を読んで，設問 1～3 に答えよ。

H 社は，インターネット上で商品を販売する会社である。H 社では，電子メール（以下，メールという）を受信することに同意した会員に対して，商品を紹介するメール（以下，商品紹介メールという）を送信することで，Web サイトへ会員を誘導し，商品を販売している。

日々多数の商品紹介メールを送信することが，H 社の重要な営業活動となっている。一方，商品への質問や会員情報の変更など，会員からの要求はすべて Web サイト上で受け付けることから，メールの受信量は非常に少ない。

H 社では，外部メールサーバ，Web サイトを開設している Web サーバ，及び自社のドメインを管理している DNS サーバを DMZ に設置し，ほかのサーバや PC は社内 LAN に設置している。図に，H 社のシステム構成を示す。

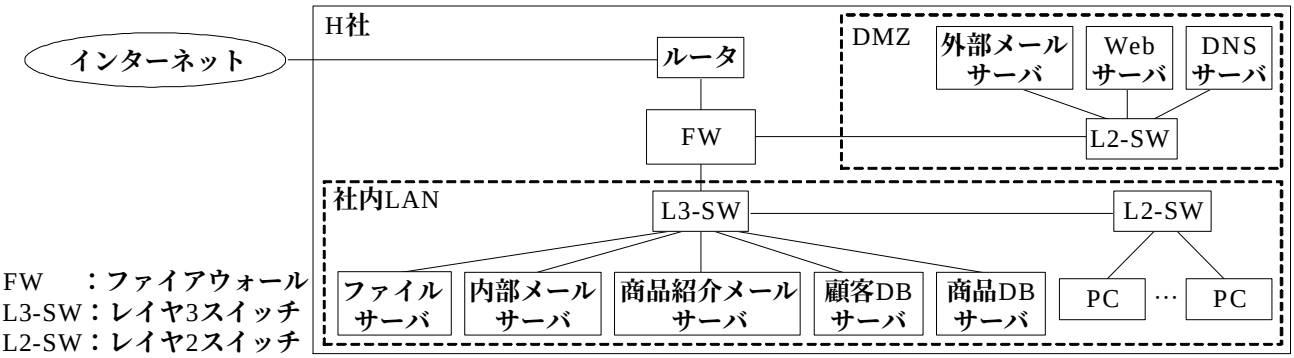


図　H社のシステム構成

FW のフィルタリング設定では，通信プロトコル，送信元 IP アドレス及びあて先 IP アドレスを指定することによって，業務上必要な通信だけを許可している。

各社員のメールボックスは，内部メールサーバ内にあり，インターネットから H 社あてのメールは，外部メールサーバ経由で内部メールサーバに届く。

一方，商品紹介メールの送信に当たっては，商品のターゲットとなる会員のメールアドレスを顧客 DB サーバから抽出し，商品紹介メールの文章とともに商品紹介メールサーバに登録し，送信時刻を設定する。各商品紹介メールの送信時刻になると，商品紹介メールサーバは外部メールサーバ経由で送信を開始する。

〔迷惑メールの受信と削減対策〕

H 社では，1 か月ほど前から，商品紹介メールの送信遅延が発生するようになった。システム管理者の S 君が調査したところ，インターネットから頻繁に大量のメールを受信していたことが分かった。大量のメールの受信と商品紹介メールの送信のタイミングが重なった場合に，外部メールサーバ内に商品紹介メールが滞留し，送信遅延が発生していた。商品紹介メールの送信遅延が多発すると売上に影響することから，S 君は送信遅延の防止策を検討することにした。

インターネットから受信した大量のメールは，受信者の承諾を得ずに一方的に送信してくる迷惑メールであった。そこで，S 君は，迷惑メールを FW で遮断することを考えた。まず，FW のログからメー

ル数の多い送信元 IP アドレスを抽出した。次に，送信元 IP アドレスをアドレス帯に集約し，そのアドレス帯からのメールを FW で遮断することにした。ある 1 日の FW のログから抽出した，メール数の多い送信元 IP アドレスを表に示す。

表　メール数の多い送信元ＩＰアドレス（上位だけ抜粋）

送信元 IP アドレス	メール数	送信元 IP アドレス	メール数
A.B.71.18	530	A.B.127.79	290
C.D.129.121	450	C.D.240.58	200
A.B.89.124	320	A.B.129.12	190
C.D.201.25	300	C.D.99.251	90

表から，A.B.64.0/18 と C.D.128.0/17 の二つのアドレス帯からのメールを遮断することによって，削減できるメール数は，それぞれ［　ア　］と 950 になった。

S 君は，①迷惑メールの送信元の ISP を調べて苦情を言ったが，迷惑メールの送信は止まらなかった。また，FW のログは，過去 24 時間分しか保存していないので，送信元 IP アドレスが頻繁に変わる迷惑メールを継続的に削減するためには，FW の遮断設定を毎日見直す必要があり，S 君の作業負担が増大した。

そこで，S 君は，過去 1 か月分保存している外部メールサーバのログを利用して，より長い期間にわたってメール数の多い送信元 IP アドレスを抽出することによって，継続的に迷惑メールを削減できる遮断設定を FW に実施することにした。さらに，迷惑メールの削減数を増やすために，外部メールサーバでも遮断する方法を検討することにした。

S 君は，まず，多くの迷惑メールの文章中に含まれている URL を利用して，外部メールサーバで遮断することを考えた。しかし，H 社の外部メールサーバは，SMTP 通信の［　a　］の情報では遮断できるが，［　b　］やヘッダなどのコンテンツの情報では遮断できない。

また，FW と外部メールサーバの仕様を確認したところ，フィルタリング可能な設定数が限られていることが分かり，できるだけ少ない設定数で多くの迷惑メールを削減する必要があった。そこで，S 君は，次の手順で迷惑メールを削減することにした。

（1）FW の設定

・外部メールサーバのログには，受信したメールごとに MAIL FROM で指定される送信者メールアドレス，［　c　］で指定される受信者メールアドレス及び送信元 IP アドレスが記録されているので，送信元 IP アドレスの情報を利用して，インターネットから受信したメールのログだけを抽出する。
・抽出したログから，メール数の多い送信元 IP アドレスを幾つか選定し，アドレス帯に集約して FW で遮断する。

（2）外部メールサーバの設定

・迷惑メールの削減数を増やすために，②抽出したログから一部のログを除外する。
・除外後のログから，メール数の多い送信者メールアドレスを選定して，外部メールサーバで遮断する。

外部メールサーバでの遮断時，SMTP 通信の応答コードに，［　d　］なエラーを示す 400 番台ではなく，［　e　］なエラーを示す 500 番台を利用し，遮断した迷惑メールを再度受信することを抑止する。

〔外部メールサーバの分離〕

迷惑メールの削減対策を実施した後，商品紹介メールの送信遅延は発生しなくなったが，迷惑メールを完全に遮断することはできないので，大量の迷惑メールを受信する可能性は残っていた。

そこで，S 君はインターネットへの送信用とインターネットからの受信用に，それぞれ外部メールサーバを分離し，送信用外部メールサーバへのインターネットからの SMTP 通信を遮断するために，システム変更を行うことにした。

サーバを新規に購入するには数か月を要することから，現在は利用していない処理能力の低いサーバを，受信用外部メールサーバとして設置することにした。また，現在の外部メールサーバは，設定変更を行わずに送信用外部メールサーバとして利用することにした。

S 君が考えたシステム変更手順は，次のとおりである。

（1）受信用外部メールサーバを DMZ に設置する。
（2）FW のフィルタリング設定に，③新たに許可すべき通信を追加する。
（3）④DNS サーバの設定変更を実施する。
（4）DNS サーバの設定変更がインターネット上で⑤反映されるまで待つ。
（5）インターネットから送信用外部メールサーバへの SMTP 通信を，FW で遮断する。

システム変更後は，遮断できない大量の迷惑メールを受信した場合にも，商品紹介メールの送信遅延は全く発生しなくなり，システム変更の有効性が実証された。

設問１　本文中の［　a　］～［　e　］に入れる適切な字句を解答群の中から選び記号で答えよ。

解答群

ア　MAIL TO	イ　RCPT TO	ウ　TO	エ　一時的
オ　永久的	カ　エンベロープ	キ　軽微	ク　重大
ケ　セグメント	コ　ペイロード	サ　ボディ	シ　メッセージ

設問２　〔迷惑メールの受信と削減対策〕について，(1)～(3) に答えよ。

（1）本文中の［　ア　］に入れる適切な数値を答えよ。
（2）本文中の下線①について，S 君が ISP 名や連絡先窓口を調べるために利用した，インターネットで利用できる仕組みを，10 字以内で答えよ。
（3）本文中の下線②について，除外すべきログとは何か。20 字以内で述べよ。

設問３　〔外部メールサーバの分離〕について，(1)～(3) に答えよ。

（1）本文中の下線③の許可すべき通信を二つ挙げ，システム変更手順(5)の記述形式に従って，それぞれ 35 字以内で述べよ。
（2）本文中の下線④の設定変更の内容について，“MX レコード”という字句を用いて，30 字以内で述べよ。
（3）本文中の下線⑤について，DNS サーバの設定変更がすぐに反映されない理由を，35 字以内で述べよ。