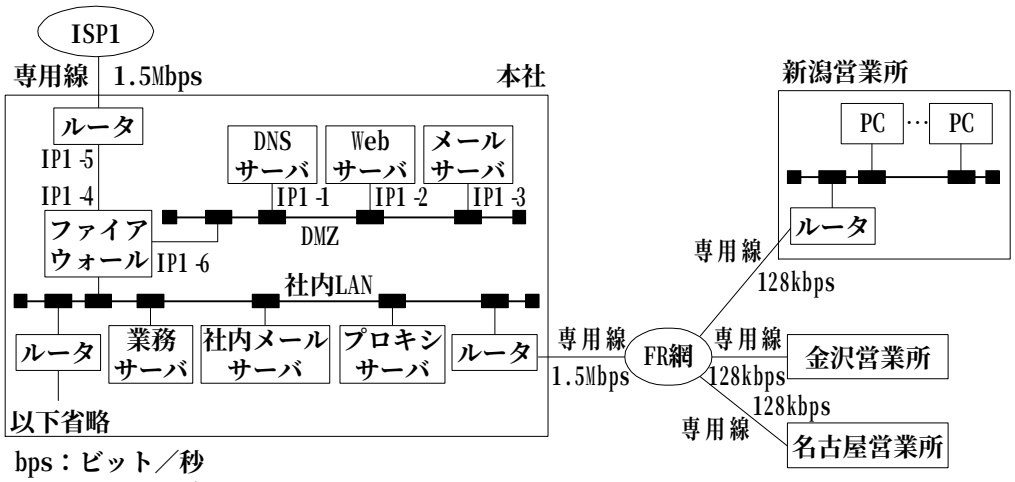
平成１５年度　秋期　ﾃｸﾆｶﾙｴﾝｼﾞﾆｱ（ネットワーク）　午後Ⅱ問題

問１　全社ネットワークの再構築に関する次の記述を読んで，設問１～５に答えよ。

Y社は，本社と 3 か所に営業所をもつ，建築材の卸売業者である。従業員は 200 名で，本社に 150 名，各営業所に 10～20 名が勤務している。Y社では，現在，図１に示すネットワークを構築して業務に利用している。本社の DMZ に DNS サーバ，Web サーバ及びメールサーバを設置して，これらをインターネットに公開している。



bps：ビット／秒
FR：フレームリレー
PC：パソコン
注　ISP1は，現在利用していISPを示す。
IP1-1～IP1-6は，ISP-1から割り当てられたグローバルIPアドレスを示す。

図１　Y社のネットワーク

本社と各営業所間は，FR サービスを利用して接続されている。また，本社から 1.5Mbps の専用線で ISP1 を経由してインターネットに接続されている。本社及び各営業所からの Web サーバの閲覧などによるインターネットの利用は，社内 LAN に設置されたプロキシサーバを経由して行われている。各営業所の従業員は，各自の PC から FR 網を経由して，社内 LAN に設置された社内メールサーバと業務サーバを利用している。

最近，全社的にインターネットの利用が増大したので，時間帯によっては応答時間が長く感じられるようになった。特に，各営業所では，インターネットの利用だけでなく，社内メールサーバや業務サーバを利用する際の応答時間も長くなり，不満が多くなってきた。

この問題の原因は，ISP1 への接続回線や FR 網を利用するための回線の帯域不足にあると判断されたので，ネットワーク運用管理責任者のH課長は，担当者のK君に次の 3 点の改善目標を示し，改善案の検討を指示した。

・インターネットの利用における応答時間の改善

・各営業所から社内メールサーバや業務サーバを利用する際の応答時間の改善
・ネットワークの利用における費用の削減

K君は，FTTH として普及が始まっている光接続サービスや，ADSL サービスを利用したネットワークの再構築が改善策として最適であると考え，改善方針を次の 3 点にまとめて SI 業者のM氏に提案を求めた。

・インターネットへの接続は，光接続サービスや ADSL サービスを利用して広帯域化する。
・本社と各営業所間の接続には，インターネット VPN（以下，VPN という）を利用する。
・ISP への接続回線や ISP のネットワークに障害が発生しても，Y社でのインターネットの利用や VPN の使用が継続できるようにする。

M氏は，K君の改善方針を基に，次のような提案を行った。

〔ネットワークの概要〕

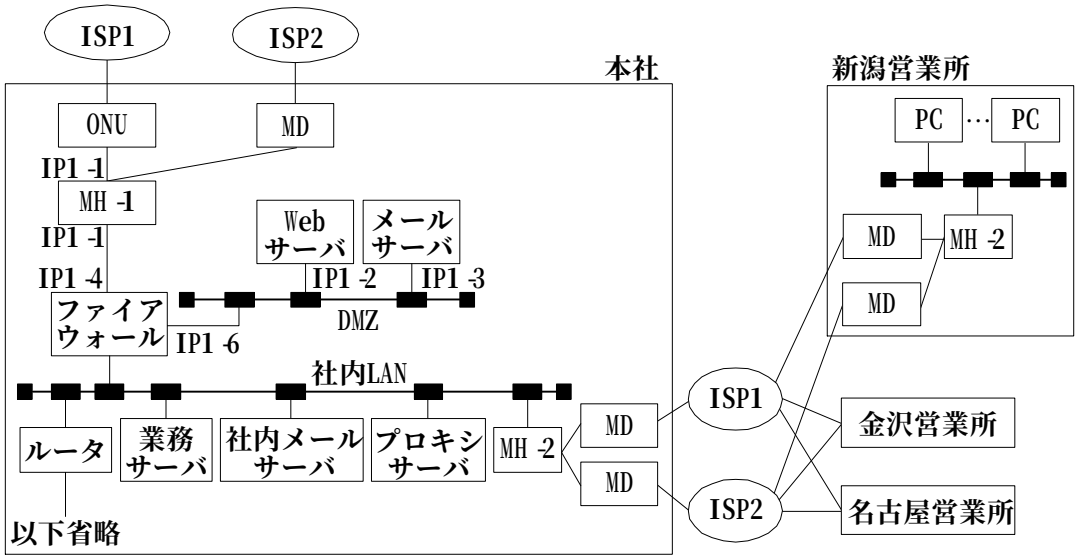
(1) インターネットへの接続

光接続サービスや ADSL サービスを利用するとともに，障害が発生してもインターネットの利用が継続できるようにするために，二つの異なった ISP への接続（以下，マルチホーミングという）を行うことにした。これには，マルチホーミング専用装置（以下，MH という）を利用することにした。

(2) 本社と各営業所間の接続

MH がもつ機能によって，ADSL の 2 回線を束ね，IPsec を使用して VPN トンネルを構成することにした。これによって，本社と各営業所間の接続にインターネットを利用した場合でも，MH を使用すれば，安全性が確保できるとともに信頼性も高められる。

上記(1)，(2)によって広帯域化され，ネットワークの利用における費用の削減も実現できることになった。図２に，M氏が提案したネットワーク構成を示す。



ONU：光終端装置
MD：ADSLモデム
注　ISP2は，新たに利用する予定のISPを示す。
　　社内LANと営業所では，プライベートIPアドレスを利用する。

図２　M氏が提案したネットワーク構成

本社と各営業所に導入する MH は，次のような機能をもっている。

① NAT 機能

ISP 側に転送される（以下，アウトバウンドという）パケットの送信元アドレス及び ISP 側から転送される（以下，インバウンドという）パケットのあて先アドレスを，NAT テーブルを参照して変換する。

② ルート障害対策機能

ping コマンドを発行して応答の有無を確認する方法（以下，ping 確認という）によってルートの障害を検知し，正常なルートだけを使用する。

③ アウトバウンドトラフィックの振り分け機能

ISP 側の二つのポートに対して，セション単位にアウトバウンドトラフィックを振り分けることで，回線の負荷分散を行う。振り分け比率は，任意に設定できる。

④ インバウンドトラフィックの振り分け機能

振り分けには，DNS 機能を利用する。具体的には，登録された複数の IP アドレスを交互に回答するラウンドロビン機能を利用して，インバウンドトラフィックを二つのルートに振り分ける。

⑤ VPN 機能

MH 間で，二つの ISP との接続回線を束ねて一つの VPN トンネルを構成することで，回線の負荷分散を同時に行う。

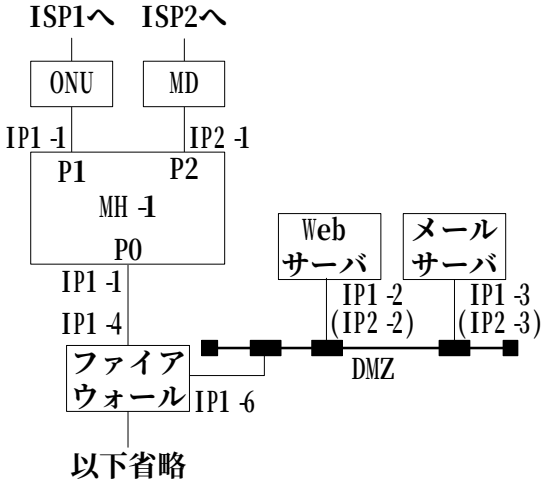
以上に示したように，MH は，マルチホーミングと VPN 機能を併せもっている。アウトバウンド処理では，アウトバウンドパケットを解析し，必要に応じて VPN 機能を働かせる。VPN 機能を働かせない場合には，アウトバウンドトラフィックの振り分け機能を働かせる。これらの機能にル

ート障害対策機能筆組み合わせることによって，インターネットの利用や VPN の使用が継続できるようにすることが可能になる。本提案では，図２中の MH-1 の VPN 機能は働かせないが，MH-2 の VPN 機能は働かせる。また，既存の DNS サーバは使用せず，MH-1 に内蔵された DNS 機能を使用する。

〔MH の設定と動作の概要〕

(1) IP アドレスと NAT テーブルの設定

図３に，MH-1 とサーバに設定される IP アドレスを示す。図３に示したように，MH-1 と公開されるサーバには，ISP1 から割り当てられた IP アドレスに加え，ISP2 から割り当てられる IP アドレスも付与する。



注　P0，P1及びP2は，ポートを示す。
IP2-1，IP2-2及びIP2-3は，ISP2から割り当てられるグローバルIPアドレスを示す。
括弧内は，ISP2経由で接続されるときのIPアドレスを示す。

図３　MH-1 とサーバに設定される IP アドレス

MH-1 は，図３に示すようなポート構成をもち，P1 と P2 のそれぞれに対して，NAT 機能を独立に設定することが可能である。本提案では，既存環境に極力影響を与えないで導入できるようにするために，P1 での NAT 機能を働かせない透過モードを利用して，P2 だけで NAT 機能を働かせる。MH-1 に内蔵された DNS 機能は，P1 と P2 に設定される IP アドレスで利用できる。既存の DNS サーバに設定されていた IP アドレスをそのまま利用するために，P1 には IP1-1 が設定される。MH-1 では透過モードが利用され，P0 と P1 が同一の IP アドレスになるので，P0 には IP1-1 が設定される。

表１に，P2 における NAT テーブルの設定内容を示す。

表１　P2 における NAT テーブルの設定内容

No.	アドレス 1	アドレス 2
1	IP1-2	IP2-2
2	IP1-3	IP2-3

P2 でのアドレス変換は，表１の設定に従って次の手順で行われる。パケットが P2 から出力されるときに，送信元 IP アドレスが NAT テーブルのアドレス 1 に存在する場合には，同一行のアドレス 2 に変換される。存在しない場合には，P2 に設定された IP アドレスに変換される。一方，パケットが P2 に入力されるときに，あて先 IP アドレスが NAT テーブルのアドレス 2 に存在する場合には，同一行のアドレス 1 に変換される。また，P2 に設定された IP アドレスの場合には，DNS 機能を利用するパケットを除いて，ポート番号に基づいてプライベート IP アドレスに変換される。それ以外の場合には，MH-1 によって廃棄される。

図３に示した Web サーバから ISP に送信されるパケットが，P1 から転送される場合には，送信元アドレスが［　a　］になる。また，P2 から転送される場合には，表１の設定によって，［　b　］になる。MH を導入してアウトバウンドトラフィックの振り分けだけを目的にする場合には，(a)MH-1 に図３に示した IP アドレスを付与して表１の設定を行うことで，図１に示した既存の DNS サーバの設定を変更しないでそのまま利用できる。しかし，その場合には，(b)Y 社から転送される電子メールの受信が ISP のポリシによって拒否されるという問題が発生する可能性がある。この問題を発生させないようにするためには，既存の DNS サーバの設定を変更する必要がある。本提案では，インバウンドトラフィックの振り分けも目的にするので，既存の DNS サーバを使用する方法は行わないことにした。

(2) ping コマンドのあて先の設定

MH は，ping 確認によってルートの障害を検知する。MH-1 では，アウトバウンドのルートの障害を検知するために，ping コマンドのあて先として，ISP 側のポートごとに，接続先の ISP のエッジルータを設定する。しかし，(c)MH-2 に対して ping コマンドのあて先にエッジルータを設定しても，VPN のルートの障害を検知できないので，ping コマンドのあて先に違う場所を設定する。

(3) DNS 機能の設定

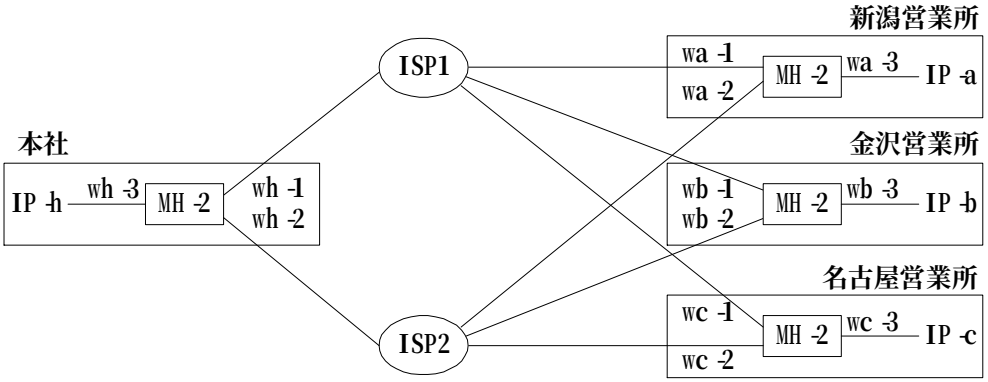
インバウンドトラフィックの振り分けは，MH-1 の NAT 機能と DNS 機能によって行われる。図３において，P1 又は P2 のどちらかのルートに障害が発生しても，DNS 機能は正常なルートから利用されなければならない。そのため，JP ドメインを管理する DNS サーバには，MH-1 に内蔵された DNS 機能を利用するための IP アドレスを基に，登録データの変更が必要になる。また，DNS 機能が回答するホストアドレスも，ISP1 と ISP2 の両方を経由して接続されるものでなければならない。この回答を行うために，Web サーバとメールサーバに対して，図３に示したように，ISP2 経由で接続されるときの IP アドレスを割り当てる必要がある。これらの設定によって，MH-1 に内蔵された DNS 機能では，インバウンドのルート障害対策機能を実現させることができる。図４に，図２のネットワーク構成に移行するための MH-1 に内蔵された DNS 機能の設定内容の一部を示す。

@	IN	SOA	ns.y-sha.co.jp.…
⋮	⋮	⋮	⋮
	IN	NS	ns.y-sha.co.jp.
	IN	NS	ns1.y-sha.co.jp.
⋮	⋮	⋮	⋮
$ORIGIN	y-sha.co.jp.		
ns	IN	A	ア
ns1	IN	A	イ
mail	IN	A	IP1-3
	IN	A	ウ
www	IN	A	IP1-2
	IN	A	エ

図４　MH-1 に内蔵された DNS 機能の設定内容の一部

(4)VPN 機能の設定

図５に，MH-2 を利用して VPN を構成するための本社と各営業所の接続構成を示す。MH-2 では，透過モードと内蔵された DNS 機能は使用しない。



注　ADSLモデムは省略。
IP-h，IP-a，IP-b及びIP-cは，ネットワークアドレスを示す。また，wh-1～wh-3，wa-1～wa-3，wb-1～wb-3及びwc-1～wc-3は，IPアドレスを示す。

図５　本社と各営業所の接続構成

VPN は，本社に設置する MH-2 と各営業所に設置する MH-2 との間で設定される。表２に，本社に設置する MH-2 の VPN 機能の設定を，表３に，金沢営業所に設置する MH-2 の VPN 機能の設定を示す。表２，３では，二つの ISP との接続回線を束ねて一つの VPN トンネルを構成する設定を示している。

表２　本社に設置する MH-2 の VPN 機能の設定

VPN No.	始点	終点	対象
VPN#1	wh-1	wa-1	IP-a
	wh-2	wa-2	
VPN#2	wh-1	wb-1	IP-b
	wh-2	wb-2	
VPN#3	wh-1	wc-1	IP-c
	wh-2	wc-2	

表３　金沢営業所に設置する MH-2 の VPN 機能の設定

VPN No.	始点	終点	対象
VPN#1	wb-1	オ	キ
	wb-2	カ	

MH-2 は，アウトバウンドパケットのあて先ネットワークアドレスが，表２，３中の対象欄のネットワークアドレスと一致する場合に，IPsec 形式への変換を施して接続先の MH-2 に対してパケットを転送する。

IPsec には、セキュリティサービスを実施するために，［　c　］と SPI(Security Parameter Index)という概念が導入されている。図５において，ある営業所の PC から本社の業務サーバへの通信が開始されると，その営業所の MH-2 は，自身がもつかぎ管理機能によって［　c　］と SPI を取得する。さらに，これらの情報に基づいて IPsec 形式に変換を施したパケットを，本社の MH-2 あてに転送する。パケットを受信した本社の MH-2 は，パケット中の SPI に基づいて，復号処理を行う。IPsec 通信で必要になるかぎは，本社とある営業所の MH-2 間で共有される。共有のためのかぎ交換方式には，事前に設定する方式と RFC2409 に明記された［　d　］による交換方式があるが，本提案では，事前に設定する方式を採用することにした。

K君がまとめたネットワークの再構築案の説明を受けたH課長は，社内手続を経て，K君に社内ネットワークの再構築を指示した。H課長の指示を受け，K君は，M氏の会社にネットワークの再構築を発注した。

〔ネットワークの移行〕

(1) 関連機器の設置と設定

まず，M氏の会社の作業者は，関連機器の設置と設定及び既存の DNS サーバとインターネット接続用のルータの撤去を行った。その後，MH-1 をファイアウォールの ISP 側のポートに直結した。ファイアウォールのポートがオートネゴシエーションモードであったので，MH-1 の各ポートもこ

れに合わせてオートネゴシエーションモードにした。しかし，MH-1 を稼働させたところ，MH-1 のファイアウォール側のポートのリンクランプが点灯しなかった。そこで，作業者は，ケーブルと MH-1 のポートを調べたが問題は発見できなかった。試行錯誤の末，速度の不一致が原因であると推定して対策を施した結果，問題は解決できた。

MH-1 の設定は，社内 LAN に設置されている 1 台の PC を使用して行われた。すべての設定が完了した後に MH-1 のモニタ画面で確認したところ，ISP へのルートは正常と認識されていた。

次に，作業者は，本社と各営業所で FR 網接続用のルータを LAN から取り外し，MH-2 や関連機器の設置と設定を行った。本社の MH-2 の設定は，MH-1 を設定した PC を使用して行われた。また，各営業所の MH-2 の設定は，その営業所に設置されている 1 台の PC を使用して行われた。

(2) 各機器の動作確認

関連機器の設置と設定が完了した後，作業者は，表４に示す動作確認の方針に従って，各機能の動作確認を行った。

表４　動作確認の方針

番号	確認機能	確認順序	接続先	確認手段
1	アウトバウンド	①	社外の Web サーバ	閲覧
		②	社内メールサーバ	社外へのメール送信
2	VPN	③	業務サーバ	業務アプリケーションの実行
		④	社内メールサーバ	社内でのメール送受信
		⑤	プロキシサーバ	社外の Web サーバの閲覧
3	インバウンド	⑥	本社の Web サーバ	閲覧
		⑦	本社のメールサーバ	社内へのメール送信

まず，作業者は，アウトバウンドの動作確認を，MH-1 を設定した PC を使用して行った。表４中の①，②の確認は，一方の ISP へのルートと対になるルートの MH-1 の ISP 側のポートに接続されている LAN ケーブルを外して行った。両方のポートからのインターネットの利用が正常に行えることを確認した後に，両方のポートに LAN ケーブルを接続して，アウトバウンドトラフィックの振り分け動作を表４中の①について確認した。MH-1 のログで振り分け状態を調べたところ，トラフィックは振り分けられていたが，ポートごとに送受信された累積データ量は，設定された比率と大きく異なっていたので，(d)運用開始後に再度確認することにした。

次に，作業者は，VPN の動作確認を，各営業所の PC の設定を変更しないで，業務サーバや社内メールサーバの利用及び社外の Web サーバの閲覧が可能かどうかを検証する方法で行った。

その後，作業者は，インバウンドの動作確認を，VPN の動作を確認した PC を使用して行った。表４中の⑥の確認は，(e)PC のプロキシサーバを利用する設定を外し、ブラウザに本社の Web サーバの IP アドレスを直接入力して行った。さらに，PC に ISP1 の DNS サーバの IP アドレスを設定し，ブラウザに本社の Web サーバの URL を入力して行った。

すべてのテストが計画どおり完了し，ネットワークは無事に移行できた。

設問１　本文中の［　a　］～［　d　］に入れる適切な字句を答えよ。

設問２　インターネットへのアウトバウンドに関する次の問いに答えよ。

(1) 本文中の下線(a)の場合には，社内 LAN からのインターネットの利用によって発生するパケットが，MH-1 によってどのように転送され，MH-1 のどこに返送されてくるか。50 字以内で述べよ。

(2) 本文中の下線(b)の問題は，P2 側から ISP に送信された場合に発生する。その理由を，70 字以内で述べよ。

設問３　インターネットからのインバウンドに関する次の問いに答えよ。

(1) 図４中の［　ア　］～［　エ　］に入れる適切な記号を答えよ。

(2) インバウンドにおけるルート障害対策機能を実現するために，DNS 機能はどのように動作するか。50 字以内で述べよ。

設問４　VPN に関する次の問いに答えよ。

(1) 本文中の下線(c)の理由を，50 字以内で述べよ。また，MH-2 の ping コマンドのあて先をどこに設定すべきか。25 字以内で述べよ。

(2) 表３中の［　オ　］～［　キ　］に入れる適切な記号を答えよ。

設問５　ネットワークの移行に関する次の問いに答えよ。

(1) M氏の会社の作業者は，MH-1 を稼働させたときにリンクランプが点灯しなかった問題に対して，どのような対策を施したか。50 字以内で述べよ。

(2) 本文中の下線(d)を行ったところ，ポートごとに送受信された累積データ量は，設定した比率に近い値になった。最初に調べたときに，設定された比率と大きく異なった原因を，60 字以内で述べよ。

(3) 本文中の下線(e)の手順によって，インバウンドの動作確認を行うことができる理由を，70 字以内で述べよ。

問２　リモートアクセス環境の構築に関する次の記述を読んで，設問１～４に答えよ。

自動車販売会社のA社は，都内に本社と 30 の店舗を構えている。営業員は，店舗ごとに 20 人程度が配置されており，顧客先に出向いて営業活動を行っている。夕方以降の時間帯に個人向けの営業活動を行う場合などには，顧客先から直接帰宅することが多い。

A社では，3 年前から本社にグループウェアサーバ（以下，GS という）を設置し，全社員で電子メールやスケジュール管理などのサービスを利用していた。GS は，専用のクライアント側アプリケーションプログラム（以下，CL-AP という）をパソコンに搭載し，TCP/IP を用いて利用されていた。図１に，A社のネットワーク構成を示す。

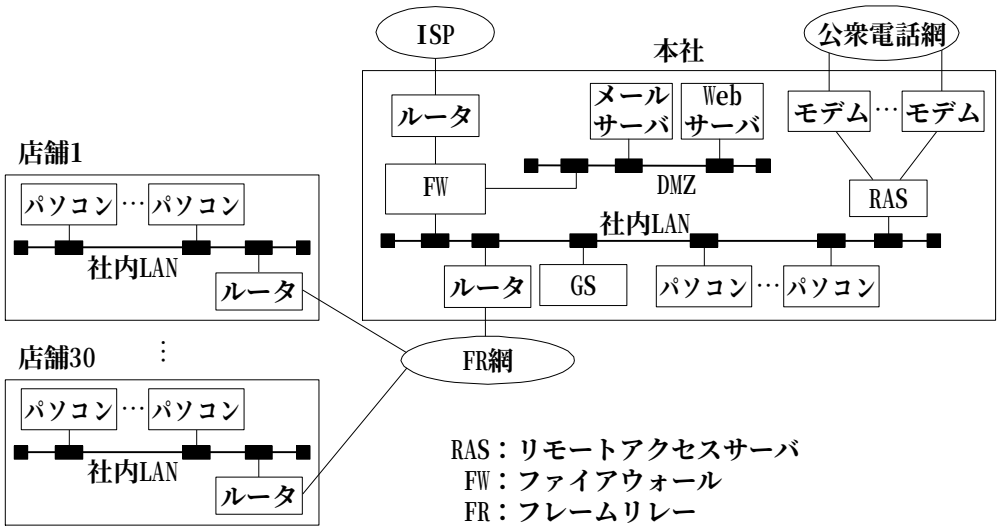


図１　A社のネットワーク構成

営業員は，顧客との連絡に電子メールを利用していたので，自宅で電子メールを読んだり，送信したりする必要があった。そのため，A社では，営業員に対して，登録された電話番号へのコールバックを利用したリモートアクセスを許可している。

RAS と GS のパスワードは，互いに異なる文字列を使用することになっている。また，双方のパスワードは，推定が困難な文字列で構成され，社員が定期的に変更する仕組みになっている。

多くの営業員は，自宅におけるインターネットへのアクセス手段として，ADSL を利用したブロードバンド通信を利用している。これに比べて，A社における RAS を使った現状のリモートアクセス環境では，通信速度が遅いので不満を感じていた。また，GS への同時アクセス数は，図１のモデムの台数に制約を受けるので，GS に対する接続要求が集中すると，待ち時間が長くなることが多かった。

A社では，現状の GS を利用したサービスに加えて，メーカなどに対する発注業務の電子化と各種保険料の見積りなどのサービスを提供する次期システムの開発を計画していた。次期システムでは，RAS を使った現状のリモートアクセス環境を廃止し，新たにインターネットを使ったリモートアクセス環境を構築することにした。

システムインテグレータであるB社のC君は，リモートアクセス環境を中心に，セキュリティ担

当のD氏と協議しながら次期システムの設計を行っている。

〔次期システムの要件〕

営業員は，ある顧客先での営業活動が終了した後，別の顧客先に直接向かう場合などに，訪問先の顧客に関する電子メールを確認する必要があり，外出先からもリモートアクセス環境を利用したいとの要望をもっている。そのため，次期システムでは，インターネットへの多様なアクセス手段を利用し，営業員の利便性を向上させることにした。

開発するサービスでは，開発や運用管理の効率化を目的として，業務サーバに Web アプリケーション方式を適用する予定である。また，社員の要望を反映しながら，必要なサービスを 1 年かけて順次追加し，必要に応じて業務サーバも増設する予定である。そのため，業務サーバで稼働するアプリケーションプログラム（以下，業務 AP という）には，段階的な開発が行われても，システムへの追加が容易になるようなソフトウェア設計が求められる。

なお，社員は，次期システムにおいても，これまで使い慣れた CL-AP を継続して利用したいと要望している。

今後，他社との電子データのやり取りにおいては，PKI(公開かぎ基盤)を利用した電子署名の適用が想定されるので，ユーザ ID とパスワードだけでなく，社員の証明書を使用した電子認証の利用も視野に入れる必要がある。

〔RAS を使った現状のリモートアクセス環境におけるセキュリティ上の問題点〕

C君は，次期システムのリモートアクセス環境を構築するために，図1における RAS の利用状況を調査した。まず，RAS や GS のログなどを基にした利用時間帯や接続数などを分析し，A社の運用担当者に対するヒアリング調査を行った。そのとき，運用担当者から，“先日，RAS のログでは認証に成功しているが，GS のログでは認証に失敗している事象があった”と告げられた。そこで，C君は，社内でも頻繁に GS を利用する営業員が，そのパスワードだけを間違えていることに疑念を抱いた。

次は，運用担当者から告げられた事象に関するC君とD氏の会話である。

C君：A社では，RAS にログインする場合と GS にログインする場合とで，異なるパスワードを使用しています。双方のパスワードは，社員が定期的に変更する仕組みになっています。

D氏：それは，正しい運用方法だと思います。まず，現状のシステムにおいて，認証が失敗する条件を教えてください。

C君：RAS と GS における認証は，双方ともに，パスワードを連続して 5 回間違えた場合に失敗します。営業員が，GS のパスワードだけを連続して 5 回も間違えているのは不思議です。

D氏：これは，不正にアクセスされたと考えられます。A社の利用形態から判断すると，GS へのログインだけに失敗するのは不自然だと思います。この場合に想定されるのは，コールバック時のモデム制御の不具合です。コールバック手順は，どのようになっていますか。

C君：コールバック手順の概要は，図２のとおりです。ログを分析した結果から，RAS のパスワードが正確に入力されていると判断できるので，正当なアクセス権限を有した社員に対してコールバックされているはずです。

①営業員は，自宅から目的のモデムに接続する。
②RAS は，営業員に対してユーザ ID とパスワードを要求する。
③営業員は，定められたユーザ ID とパスワードを入力する。
④RAS は，パスワードを検証後に回線を切断する。
⑤RAS は，営業員の登録済電話番号にコールバックする。

図２　コールバック手順の概要

D氏：営業員を識別するまでの処理に関しては，間違いないと思います。この事象では，図２中の“④の回線を切断する”から“⑤のコールバックする”までの間で不正なアクセスが生じたと考えられます。この原因は，RAS がモデムにコールバックさせるときの制御方法にあります。図３に，図２中の④と⑤におけるモデムの状態遷移の概要を示します。

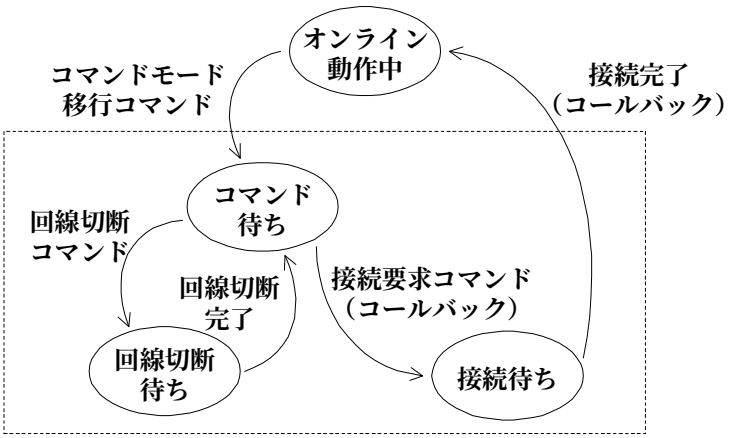


図３　図２中の④と⑤におけるモデムの状態遷移の概要

C君：不正なアクセスの防止には，どのような対策があるのでしょうか。
D氏：図３中の点線内の状態遷移において，モデムを［　a　］状態に保つように，RAS のファームウェアを変更する必要があります。

次期システムが設計段階であったので，サービスの開始までには半年以上の期間が必要であった。そのため，C君は，RAS のファームウェアを，今回の事象に関する対策を施したバージョンに更改するようA社に提言した。A社は，C君からの指摘を受けて，速やかに RAS のファームウェアを更改した。

〔インターネットを経由した認証方式に関する予備検討〕

CL-AP を利用した GS へのアクセスでは，リモートアクセス環境の伝送路上において，パスワードの機密性を確保する機能がない。しかし，次期システムでは，GS がインターネットを経由して利用されるので，新しい認証方式が必要である。

次は，その新しい認証方式の予備検討に関するC君とD氏の会話である。

C君：インターネットを経由させる場合には，パスワードの機密性の確保が必要になります。A社では，次期システムに，社員が使い慣れた CL-AP を継続して利用したいと要望しています。

そのため，パソコンではブラウザと CL-AP の双方を利用することを前提にして，認証方式を検討したいと思います。

D氏：それならば，ワンタイムパスワード（以下，OTP という）の利用が考えられます。図４に，OTP 方式の概要を示します。

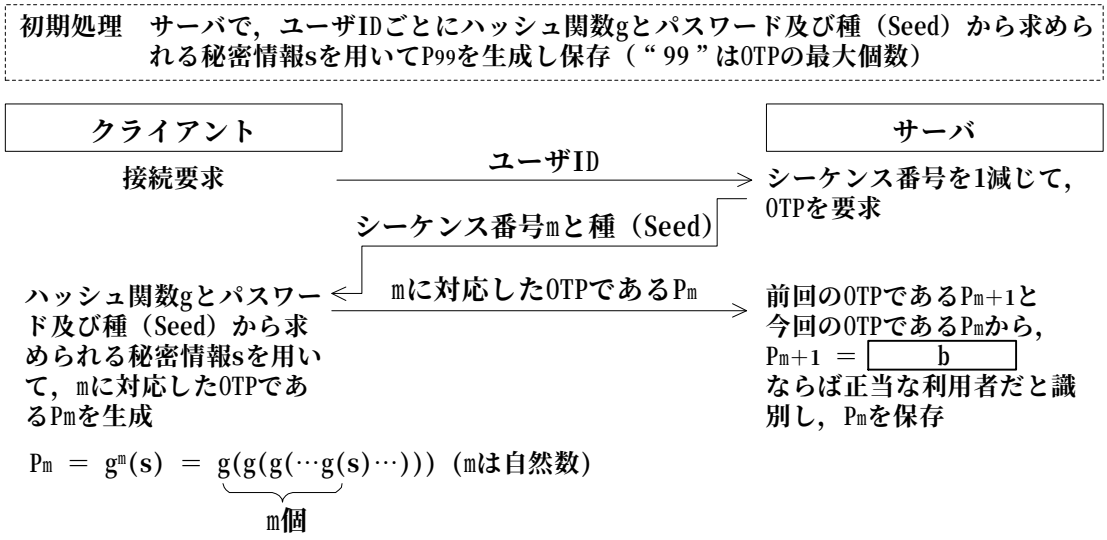


図４　OTP 方式の概要

C君：OTP を利用する場合には，どのような留意点がありますか。

D氏：次の三つです。

① 図４で示した初期処理は，社内 LAN などの通信路を経由させてリモートから実行させずに，サーバのコンソールを用いて実行させる必要がある。

② OTP の利用が一定回数を超えると，その OTP は機能しなくなる。そのため，OTP の利用回数が一定回数に近づいた営業員には，初期処理を再度行うように促す必要がある。

③ OTP を正しく入力しても GS に接続できない場合には，セキュリティに関する問題が発生した可能性がある。このような場合には，営業員に速やかにA社の運用担当者へ申告してもらうように徹底させる必要がある。

C君：分かりました。OTP 方式を採用する場合には注意します。

〔無線 LAN を使用したインターネットの利用に関する予備検討〕

最近，駅や喫茶店などでは，無線 LAN を使用したインターネットへの接続サービス（以下，無線 LAN サービスという）の利用が可能である。また，無線 LAN サービスは広帯域であるので，営業員が外出しているときなどに，GS や業務サーバを利用する目的で活用できる。そのため，C君は，インターネットへの接続方法として，無線 LAN サービスも利用する予定である。

次は，無線 LAN サービスを利用する場合のセキュリティの予備検討に関するC君とD氏の会話である。

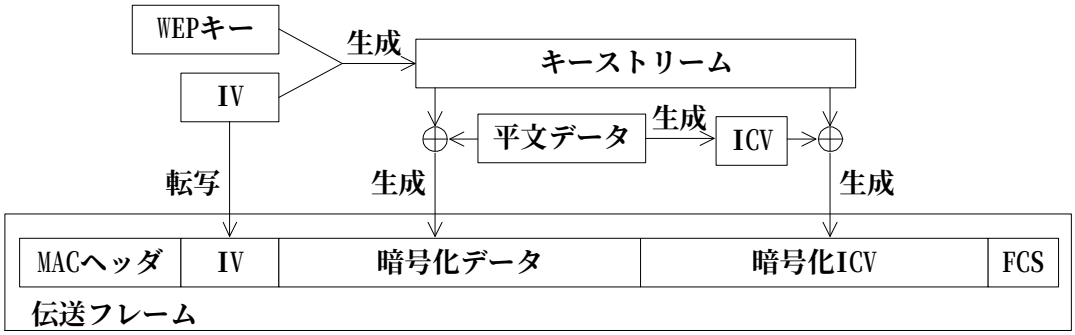
C君：次期システムには，無線 LAN サービスを利用したいと考えています。

D氏：無線 LAN サービスを利用する場合でも，公開情報などを発信している Web サイトを参照し

たり，サーチエンジンを利用したりするだけならば，大きな問題はありません。しかし，GS や業務サーバにアクセスする場合には，OTP を利用しても，解決できない問題があります。

C君：無線 LAN サービスでは，WEP(Wired Equivalent Privacy)を使用することによってセキュリティが確保されているので，ADSL を利用するときと同様に，OTP で十分だと思っていました。

D氏：WEP を使用したとしても，セキュリティを確保するためには，ADSL を利用するとき以上に注意が必要です。その理由は，WEP の仕組みと無線 LAN サービスの利用方法にあります。図５に，WEP の伝送フレームの概要を示します。



IV：Initialization Vector
ICV：Integrity Check Value
FCS：Frame Check Sequence

図５　WEP の伝送フレームの概要

C君：もし，伝送フレームが盗聴されても暗号化されているので安全だと思います。

D氏：A社が利用を予定しているプロバイダの無線 LAN サービスでは，WEP キーやローミングなどに利用される［　c　］に，利用者全員が同じ値を使用して，無線 LAN サービスのアクセスポイントを利用しています。そのため，一定の条件が成立すると危険性が高まります。

C君：もう少し詳しく説明してください。

D氏：図５に示すとおり，WEP キーと IV から生成した［　d　］系列をキーストリームとして利用し，平文データとの排他的論理和を求めて平文データを暗号化します。同時に，平文データから伝送データの完全性を確保するために利用する ICV を生成して，同様に暗号化します。ここで，伝送フレーム数が［　e　］なると，同じキーストリームが使用される場合があるので，平文データを推定できる確率が高くなります。

C君：なぜ，推定できる確率が高くなるのですか。

D氏：同じキーストリームが使用された伝送フレーム同士の排他的論理和を求めると，［　f　］同士の排他的論理和が算出されるので，片方の［　f　］が推定できると，もう一方が簡単に特定できるからです。

C君：標準的なプロトコルを使用していると，定型文字列(“ http：//www ”など)が伝送フレームに含まれるので，推定できる確率が高まるのですね。

D氏：はい，そうです。ほかにも，考慮する点があります。例えば，暗号を解かなくても伝送フレームを改ざんできる場合があります。つまり，WEP の伝送フレームを入手し，これに含ま

れる IP アドレスを変更して無線 LAN サービスのアクセスポイントに送ると，変更した IP アドレスあてに平文データを送信する攻撃（以下，パケット偽造攻撃という）が成立する可能性があります。

C君：WEP だけを使用することでセキュリティを確保するのには問題が多そうですね。

D氏：はい。情報の漏えい以外に，正当な利用者の識別が行われた後で，そのセションを不正な利用者が使用する攻撃（以下，ハイジャック攻撃という）が成立する可能性もあります。

C君：無線 LAN サービスの利用状況は分かりました。次期システムの拡張も考慮して，必要なセキュリティを確保するための対策を考えます。

〔次期システムの認証方式に関する検討〕

C君は，これまでの予備検討の結果から，無線 LAN サービスや自宅からのインターネットを経由したリモートアクセス環境と社内の双方で共通な認証方式を適用し，社員の利便性を向上したいと考えていた。

次は，次期システムの認証方式の検討に関するC君とD氏の会話である。

C君：OTP の運用は，社員数が多いことから困難だと考えられます。さらに，OTP を利用して正当な利用者の識別が行われた後で，なりすましの危険性があるのではないかと心配です。

D氏：現行のように，RAS によるコールバックを利用しているのであれば，識別が行われた後のセション維持のために，詐称が比較的困難な情報を使用しているので安全性が保てます。しかし，多様なアクセス方法を許容するリモートアクセス環境では，正当な利用者の識別が行われた後のセション維持の方法を検討する必要があります。

C君：ブラウザを利用するのであれば，社員の識別が行われた後の認証情報を［　g　］や［　h　］などを用いて保持し，セション維持を行うことができます。

D氏：OTP を使わないのであれば，伝送されるパスワードや認証情報などの機密性を確保する機能を考えておく必要があります。

C君：GS へのアクセスをブラウザから行えるように，GS のソフトウェアの更改が可能なので，GS や業務サーバへのアクセスに SSL を利用するのが適切だと考えます。

D氏：その場合には，パスワードの漏えい防止策として，社員が SSL で使用するサーバ側の証明書の正当性を確認する必要があります。

C君：分かりました。パスワードを入力する前に，社員が SSL で使用するサーバ側の証明書の正当性を確認するようにします。

〔次期システムのネットワーク構成〕

C君は，ブラウザに移行してもリモートアクセス環境での利便性の向上によって，社員の理解が得られるものと考え，社員からの要望である CL-AP の利用について，セキュリティ対策の観点からブラウザに移行することにした。また，GS のソフトウェアの更改だけで，ブラウザを利用して GS が利用できることを確認した。その後，これまでのリモートアクセス環境の認証方式に関する検討を踏まえ，CL-AP からブラウザへの移行を前提に，次期システムのネットワーク構成を提案することにした。

次期システムの認証には，サーバ側の証明書だけを使用した SSL を適用して，社員のパスワー

ドを検証する方法をとることにした。この SSL やパスワードの検証などの機能については，各サーバで独立に実装すると，業務 AP の開発効率や社員の利便性が低下すると考え，リバースプロキシサーバで実装することにした。

リバースプロキシサーバは，GS と業務サーバに対して，認証結果を環境変数などに格納して通知するので，シングルサインオンが実現されて社員の利便性が向上する。また，GS と業務サーバは，リバースプロキシサーバを介するときだけブラウザと通信するので，社内 LAN に配置することができる。その結果，次期システムの安全性が確保でき，運用性も向上する。

図６に，次期システムのネットワーク構成案の抜粋を示す。

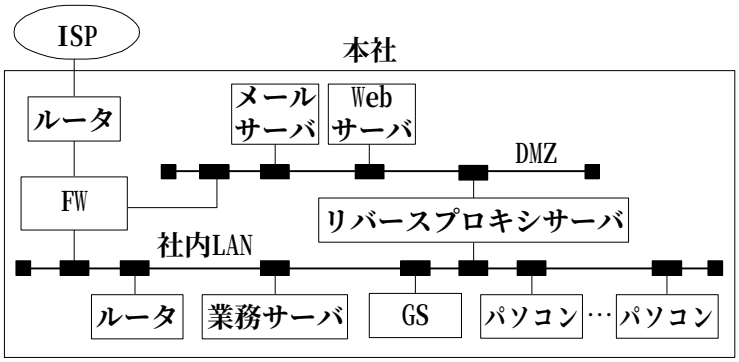


図６　次期システムのネットワーク構成案の抜粋

C君は，これまでの検討結果を基に，ブラウザから利用できるような GS のソフトウェアの更改と次期システムのネットワーク構成をA社に提案し，了承された。

設問１　モデムを利用したコールバック方式に関する次の問いに答えよ。

(1) 本文中の［　a　］に入れる適切な字句を答えよ。

(2) C君が，GS における RAS 経由のログインの失敗に疑念を抱いた理由を，30 字以内で述べよ。

設問２　インターネットを経由した認証方式に関する次の問いに答えよ。

(1) 図４中の［　b　］に入れる適切な式を答えよ。

(2) OTP 利用時の留意点①において，初期処理を実行する場合に，社内 LAN などの通信路を経由させない理由を，25 字以内で述べよ。

(3) OTP 利用時の留意点③で想定した，不正なサーバを用いた脅威と，その脅威が発生する理由を，OTP 方式の特徴を踏まえて，それぞれ 30 字以内で述べよ。

設問３　無線 LAN サービスを利用した認証方式に関する次の問いに答えよ。

(1) 本文中の［　c　］～［　f　］に入れる適切な字句を答えよ。

(2) 暗号を解かなくとも，同じキーストリームを使っていることが判明してしまう理由を，30 字以内で述べよ。

(3) WEP のパケット偽造攻撃は，あて先 IP アドレスだけを詐称しても成立しない。この攻撃が成立するために，ほかに変更する必要がある情報を，変更内容も含めて，25 字以内で述べよ。

(4) ハイジャック攻撃の成立が比較的容易な理由を，営業員の識別が行われた後の端末識別情報に着目して，40 字以内で述べよ。

設問４　次期システムの認証方式に関する次の問いに答えよ。

(1) 本文中の［ g ］，［ h ］に入れる適切な字句を答えよ。

(2) リバースプロキシサーバを利用する利点を，アタックに対する防御と監視の観点から，それぞれ 20 字以内で述べよ。

(3) 社員がパスワードを入力する前に，リバースプロキシサーバの証明書を確認しなければならない理由を，40 字以内で述べよ。

(4) SSL を使用した場合に，ハイジャック攻撃の成立が比較的困難な理由を，社員の識別が行われた後にクライアントとリバースプロキシサーバ間で共有される情報に着目して，40 字以内で述べよ。

(5) 提供するサービスや利用形態の追加及び認証方式の変更があっても，効率的な開発ができるように SSL を使用した理由を，80 字以内で述べよ。