NW

平成28年度　秋期
ネットワークスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（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. **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。**
4. 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

5. 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，**生年月日欄**に**受験票の生年月日**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。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **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。○印がない場合は，採点されません。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。
   (4) 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。
   (5) 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	
1問選択	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　ネットワークシステムの拡張に関する次の記述を読んで，設問1～5に答えよ。

工務店のA社は，全国規模で住宅や店舗の施工を請け負っている。施主への情報提供に力を入れており，次の三つの機能をもつ情報システムを稼働させている。

・施工情報管理：外出先又は社内にいるA社の社員や施主が，タブレット端末やPCで動作する，Webブラウザを使って，A社データセンタのWebサーバが管理する施工情報にHTTPSプロトコルでアクセスする（以下，Webブラウザと，Webブラウザが動作しているタブレット端末やPCを，どちらもブラウザという）。
・コールセンタ：施主からの問合せ電話を，データセンタのIP-PBXを使って，A社コールセンタのオペレータが受け付け，必要に応じて営業部や技術部へ転送する。
・インターネットアクセス：A社の社員が，社内からブラウザを使ってインターネットにアクセスする。

A社の現行情報システムの概要を図1に示す。

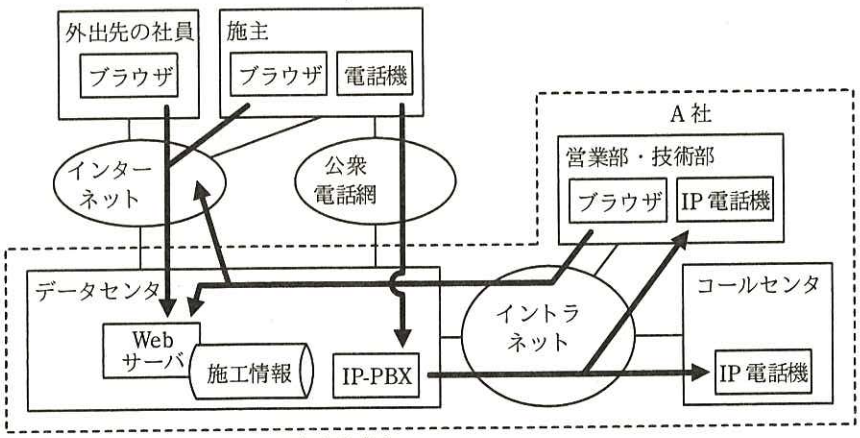


図1　A社の現行情報システムの概要

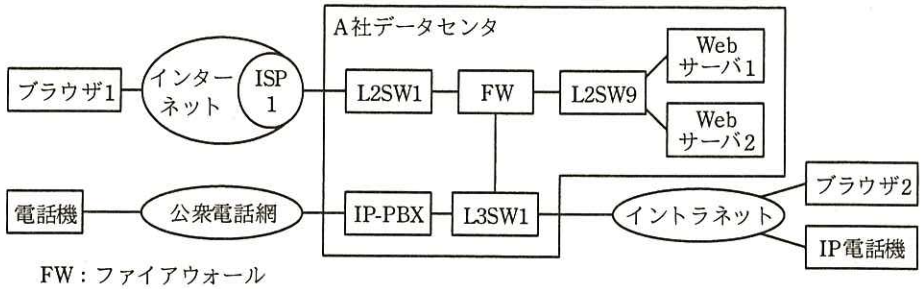
情報システム部は，現在，施主との情報連携を強化するために，ブラウザを活用した情報システムの機能拡張に取り組んでいる。ネットワーク担当のB君が，ネットワークシステムに関する現行仕様の調査と，機能拡張に伴うネットワーク拡張計画の作成を行っている。

情報システムの機能拡張の構想を次に示す。

・マルチホーミング：今後，社外との通信が更に重要になるので，データセンタとインターネットとの接続を二重化する。
・ブラウザを使ったビデオ電話：施主と A 社の社員がブラウザを使って，施工状況などを動画で確認できるようにする。このビデオ電話はブラウザ上で動作するアプリケーション（以下，AP という）を A 社の Web サーバからダウンロードし，AP 間の通信によって実現する。
・ブラウザを使った音声電話：施主や外出先の A 社の社員がブラウザを使って，社内の A 社の社員と音声電話ができるようにする。この電話機能にもビデオ電話と同じ AP を使う。IP-PBX を介した，社外のブラウザ上で動作する AP と社内の IP 電話機との通信によって実現する。

〔現行ネットワーク構成〕

A 社の現行ネットワーク構成を図 2 に，図 2 中のスイッチに定義された現行 IP アドレス空間を表 1 に，それぞれ示す。



FW：ファイアウォール
ISP：インターネットサービスプロバイダ
L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ

図 2　A 社の現行ネットワーク構成（抜粋）

表 1　図 2 中のスイッチに定義された現行 IP アドレス空間

スイッチ	VLAN 名	IP アドレス空間	用途
L2SW1	vlan1	ip1/29 （ip1 はグローバル IP アドレス）	ISP1 接続
L2SW9	vlan9	10.0.9.0/24	DMZ
L3SW1	vlan8	10.0.8.0/24	FW 接続
	vlan7	10.0.7.0/24	IP-PBX 接続
	vlan6	10.0.6.0/24	イントラネット接続

B 君が調査した，A 社の現行ネットワークシステムの仕様を次に示す。

・図 2 中のブラウザ 1 が Web サーバ 1 と Web サーバ 2 へアクセスする際に，FW の NAT 機能が宛先 IP アドレスを変換する。変換前と変換後の宛先 IP アドレスは，それぞれ表 1 中の IP アドレス空間［　ア　］と［　イ　］に属し，変換前と変換後の IP アドレスの組合せは 1：1 に固定されている（以下，宛先 NAT という）。

・図 2 中のブラウザ 2 がインターネットへアクセスする際に，FW の NAT 機能が送信元 IP アドレスと［　ウ　］の両方をそれぞれ動的に変換する（以下，送信元 NAPT という）。(a) 変換後の IP アドレス用に二つのグローバル IP アドレスが割り当てられている。

・FW のフィルタリング定義は，図 1 に示す情報システムの通信だけを許可している。

・FW には，A 社のドメイン権限をもった DNS 機能がある。

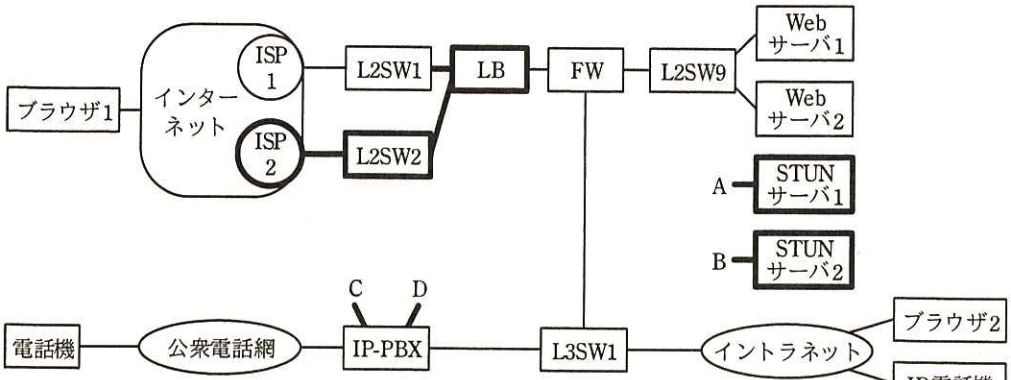
・2 台の Web サーバ（Web サーバ 1，2）は，FW の DNS ラウンドロビン機能を使って負荷分散しており，3 台以上の構成へもスケールアウトができる。(b) スケールアウトの際には，DNS 機能に関する設定変更など，FW に複数の設定変更が必要となる。

〔マルチホーミング〕

B 君は，二つの ISP サービス（ISP1，ISP2）を同時に利用するマルチホーミングの構成を考えた。この構成では，A 社が負荷分散の仕組みを用意する必要がある。調査したところ，マルチホーミング用の負荷分散装置（以下，LB という）があり，この装置は，負荷分散機能の他に，DNS 機能，NAT 機能をもつことが分かった。

B 君は LB を利用した新たなネットワーク構成を考えた。

A 社の新ネットワーク構成を図 3 に，図 3 中のスイッチに定義された LAN の新 IP アドレス空間を表 2 に，それぞれ示す。



A～D：サーバ，IP-PBXのインタフェース（設問のため接続を省略）
STUN：Session Traversal Utilities for NAT
注記　太線で示した部分は，新たに追加されるISP及び機器を示す。

図3　A社の新ネットワーク構成（抜粋）

表2　図3中のスイッチに定義された新IPアドレス空間

スイッチ	VLAN名	IPアドレス空間	用途
L2SW1	vlan1	ip1/29 （ip1はグローバルIPアドレス）	ISP1接続
L2SW2	vlan2	ip2/29 （ip2はグローバルIPアドレス）	ISP2接続
L2SW9	vlan9	10.0.9.0/24	DMZ
L3SW1	vlan8	10.0.8.0/24	FW接続
	vlan7	10.0.7.0/24	IP-PBX接続
	vlan6	10.0.6.0/24	イントラネット接続

LBを使ったマルチホーミングの概要を次に示す。

・インターネット向けのDNS機能をFWからLBへ移し，ISP2を経由してもそのDNS機能を提供できるように，ドメイン登録業者に定義の追加を依頼する。その際，ISP1，ISP2のいずれからでも同じゾーンファイルが参照されるようにする。

・LBのDNSラウンドロビン機能を使い，インターネットからA社内への通信の負荷分散を行う。(c)現行のWebサーバ用のグローバルIPアドレスに，新たなグローバルIPアドレスを加え，DNSクエリに対してそれらが交互に返るようにする。

・A社内からインターネットへの通信は，ISP1とISP2への接続ポートに対して負荷分散を行う。その際，ISPへ送信するIPパケットの送信元IPアドレスは，送信先のISPから貸与されたグローバルIPアドレスに変換されるので，FWのNAT機能をLBへ移して一元化する。

・(d)LB は，通信の行きと戻りを同じ ISP 経由にする。

・LB から ISP1 のルータ及び ISP2 のルータへそれぞれ定期的に ping 確認を行い，ISP の障害を検知した場合には，正常な ISP だけを利用する。

〔ブラウザを使ったビデオ電話の通信〕

情報システム部は，WebRTC（Web Real-Time Communication）に準拠した AP を導入する予定である。WebRTC は，ブラウザを使った音声，動画などの通信規約であり，W3C 及び IETF から仕様が公開されている。この WebRTC を使ったビデオ電話では，AP をダウンロードしたブラウザ間で直接通信（以下，AP 間通信という）を行う。NAT 機能が介在する場合の AP 間通信の例を，図 4 に示す。

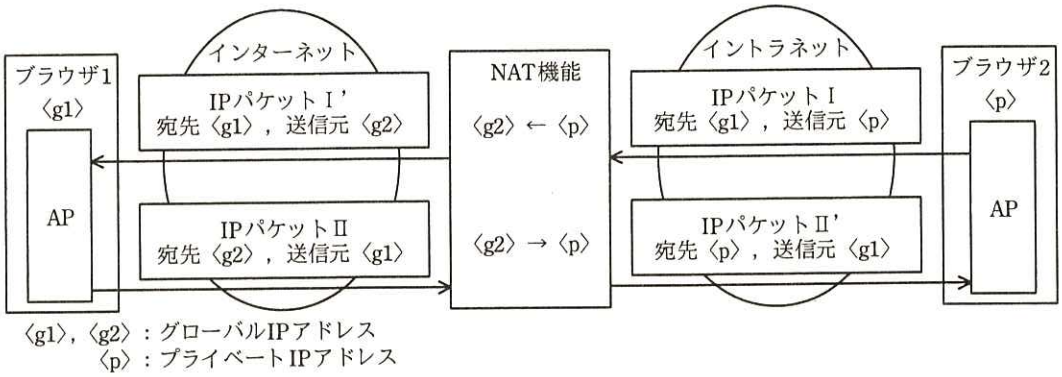


図 4　NAT 機能が介在する場合の AP 間通信の例

サーバを介さない通信では，通信相手の IP アドレスを知る仕組みが必要である。図 4 の例では，NAT 機能によってブラウザ 2 の IP アドレス〈p〉が〈g2〉に変換されている。その場合，ブラウザ 1 上の AP は，通信相手の IP アドレスとして，〈p〉ではなく〈g2〉を用いなければならない。

A 社が導入する AP は，NAT 機能によって変換された IP アドレスを，STUN サーバから得る仕様となっている。図 4 の例では，ブラウザ 2 上の AP が STUN プロトコルを用いて STUN サーバ 1，2 から〈g2〉を得て，それをブラウザ 1 上の AP に通知する。

STUN プロトコルの概要は次のとおりである。

・STUN クライアントは，STUN サーバへ Binding リクエストを送る。

・STUN サーバは，受け取った IP パケットのヘッダから送信元の IP アドレスとポート番号を取り出し，Binding レスポンス中のデータに格納して返す。

・(e) STUN クライアントは，Binding レスポンス中のデータから，自分と STUN サーバ間の NAT 機能の有無を知り，NAT 機能が介在する場合には，そのデータから NAT 機能が変換した自分の IP アドレスを得る。

B 君は，STUN サーバへのアクセスから音声，ビデオ，データなどの交換までの AP 間通信の概要をまとめた。B 君がまとめた AP 間通信の概要を，図 5 に示す。

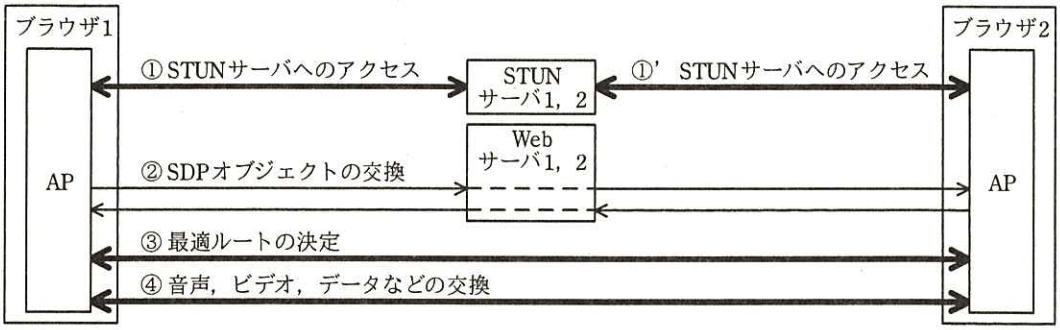


図 5　AP 間通信の概要

AP をダウンロードしたブラウザは，図 5 中の①～③で NAT 機能を経由した最適ルートを確立する（以下，ホールパンチという）。ホールパンチの概要を次に示す。

①，①’ AP は STUN サーバ 1，2 にアクセスし，NAT 機能が介在する場合の変換後のブラウザの IP アドレスを取得する。

② AP は，SDP（Session Description Protocol）オブジェクトを使って，①，①’ で取得した IP アドレスとブラウザ自身の IP アドレスを，通信相手の AP へ通知する。その際，ブラウザ 1，2 と Web サーバ 1，2 間に HTTPS が使われる。

③ AP は，通知された IP アドレスを宛先 IP アドレスにして通信相手との通信を試み，相互に通信が成功した場合に，その宛先 IP アドレスの組合せを最適ルートとする。

(f) 図 4 の AP 間通信は，このようにして確立した最適ルートを使っている。

なお，ホールパンチには，ブラウザの IP アドレスと NAT 機能の変換ルールが，そ

れぞれ一定時間変わらないという前提条件が必要である。例えば，図 4 中の〈p〉と〈g2〉は，AP 間通信の間，関連付けられている必要がある。また，IP アドレスだけではなくポート番号の考慮も必要である。

B 君は，AP 間通信において AP が使用するポート番号はあらかじめ決められていること，及び STUN サーバを図 3 のネットワーク内に適切に配置することによって，ホールパンチが LB の NAT 機能に対して有効に働くことをベンダに確認した。そして，(g) 片方の ISP が障害の場合にも利用できるように，STUN サーバのインタフェース（図 3 中の A，B）を，図 3 中の適切なスイッチに接続することにした。

次に，B 君は，A 社のマルチホーミング運用によって，図 5 中の通信が ISP1 と ISP2 に負荷分散されるかどうかを検討した。そして，図 5 から，データ量が多い④に用いられる ISP は，［　エ　］が［　オ　］をアクセスするときの LB の振分け結果によって決まることを確認し，負荷分散が行われると判断した。

〔ブラウザを使った音声電話の通信〕

ブラウザを使った音声電話の通信では，社外のブラウザ上で動作する AP が IP-PBX を介して社内の IP 電話機と通信を行う。

B 君は IP-PBX のベンダから IP-PBX の WebRTC 機能の情報を入手し，通信方式を検討した。B 君が考えた，社外の AP から社内の IP 電話機への通信の概要を，図 6 に示す。

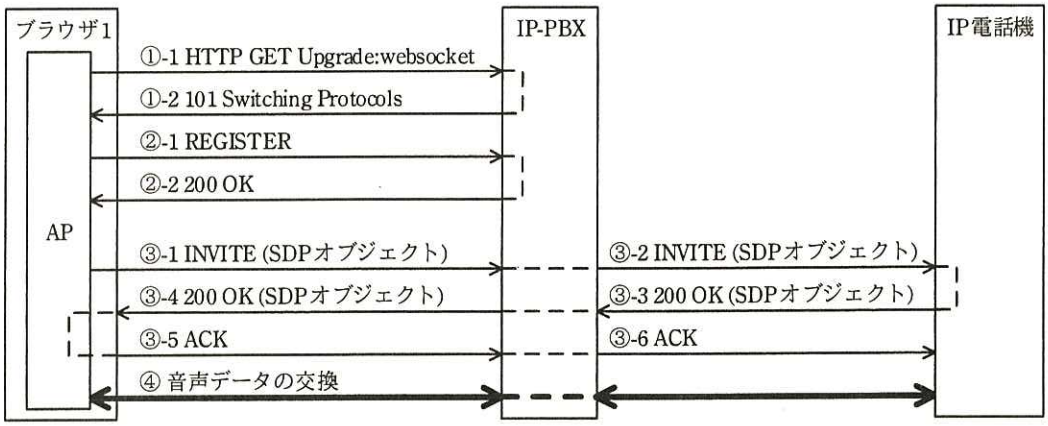


図 6　社外の AP から社内の IP 電話機への通信の概要

図6中の通信の概要は，次のとおりである。

・APは，通信プロトコル［　カ　］を使ってIP-PBXへアクセスし，①-1と①-2によって，通信プロトコルを［　キ　］に切り替え，切り替えた通信プロトコルの上でSIPプロトコルに基づくシグナリングを行う。

・IP-PBXは，2組のB2BUA（Back-to-Back User Agent）として動作する。(h)インターネット側の二つのUA（User Agent）には，それぞれグローバルIPアドレスを割り当てる。

・IP-PBXはSession Border Controllerとして動作し，グローバルIPアドレスとプライベートIPアドレスを変換する。

・(i)IP-PBXのLANインタフェース（図3中のC，D）を追加し，図3中の適切なスイッチと接続する。

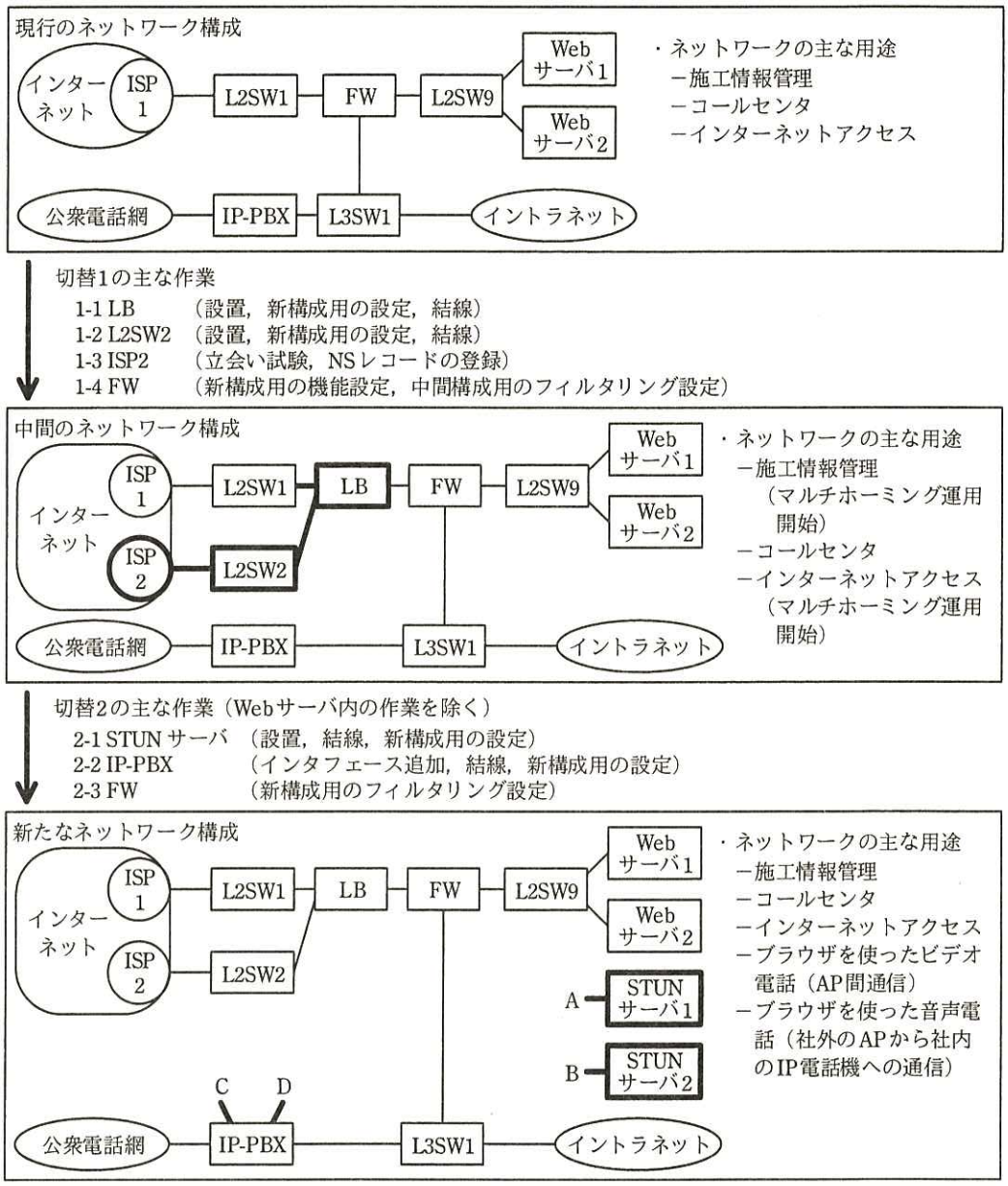
・図6中の通信の前に，［　ク　］のFQDNに関する［　ケ　］クエリが，APから［　コ　］へ発行されることによって，図6中のAPとIP-PBX間の通信はISP1とISP2に負荷分散される。

〔移行計画〕

情報システム部では，保守などでサービス停止の可能性がある場合には，サービス停止時間を関係部署へ連絡することになっている。また，連絡したサービス停止時間内に保守を終えてサービスを再開できるように，部内で作業計画を十分にレビューした上で保守を行う運用ルールも設けられている。

B君は，今回の機能拡張に関して，サービス停止時間を見積もりながら，利用者への影響が極力小さくなるような移行を考えた。ここで，サービス停止時間とは，切替作業，切替作業後の動作確認及び問題発生時の［　サ　］に要する時間の合計である。

B君が作成したネットワークの移行計画案を，図7に示す。



A ～ D：サーバ，IP-PBX のインタフェース（設問のため接続を省略）

図 7　ネットワークの移行計画案

ネットワーク移行のための切替えは 2 段階で行う。図 7 中の切替 1 と切替 2 について，B 君は次のように考えた。

（切替 1 について）

・LB の設定は，切替 1 で全ての定義を盛り込み，その後の変更を不要にする。例え

ばDNS機能については，新たなネットワーク構成に必要な次のAレコードを全て設定する。

－(j)Webサーバ1とWebサーバ2に関する四つのAレコード

－(k)APが名前解決しなければならないFQDNに関するAレコード（AP内の定義には，IPアドレスではなく，FQDNを用いることにする。）

・FWのフィルタリング変更は，中間のネットワーク構成の通信に関して変更する。

・次の点を考慮し，切替1のサービス停止時間は2時間とする。

－(l)機器の変更は，あらかじめ2通りの定義ファイルをもたせておき，定義ファイルを指定した再起動によって行う。

－約1時間，一部の利用者に情報システムを利用してもらい，(m)3種類の通信を発生させて，動作の正常性を確認する。

－(n)ドメイン登録業者に依頼する定義変更に関しては，情報システム部が正常性を確認する。利用者サービスへ直接影響しないので，その作業はサービス停止時間には含まない。

（切替2について）

・(o)FWのフィルタリング変更は，新たなネットワーク構成の通信に関して変更する。

・機器の変更と動作の正常性確認を含めた切替2のサービス停止時間について，IP-PBXのベンダに見積りを依頼する。

B君は，検討結果をまとめ，情報システム部長に報告した。その後，顧客システムの機能拡張のプロジェクトが発足し，B君はネットワークチームのリーダとして参画することになった。

設問1　〔現行ネットワーク構成〕について，(1)～(3)に答えよ。

(1) 本文中の［ア］～［ウ］に入れる適切な字句を答えよ。

(2) 本文中の下線(a)について，送信元NAPTが同時に処理できるTCPコネクション数の上限を答えよ。ここで，2^{16} = 65,536である。

(3) 本文中の下線(b)について，DNS機能以外のFWの設定変更内容を二つ挙げ，それぞれ20字以内で答えよ。

設問2　〔マルチホーミング〕について，(1)，(2)に答えよ。

(1) 本文中の下線(c)について，現行のグローバル IP アドレスと追加するグローバル IP アドレスとの違いを 20 字以内で述べよ。

(2) 本文中の下線(d)において，通信の行きと戻りが同じ ISP ではない場合の問題を，社外から Web サーバへのアクセスを例に，IP アドレスという用語を用いて 40 字以内で述べよ。

設問3　〔ブラウザを使ったビデオ電話の通信〕について，(1)～(4)に答えよ。

(1) 本文中の下線(e)について，STUN クライアントはどのようにして NAT 機能の有無を判定するかを，50 字以内で述べよ。

(2) 本文中の下線(f)について，図 4 の通信のために，ブラウザ 2 が SDP オブジェクトに格納する二つの IP アドレス候補を，図 4 中の字句を用いて答えよ。

(3) 本文中の下線(g)の接続先を，表 2 中の VLAN 名でそれぞれ答えよ。

(4) 本文中の［　エ　］，［　オ　］に入れる適切な字句を答えよ。

設問4　〔ブラウザを使った音声電話の通信〕について，(1)～(4)に答えよ。

(1) 本文中の［　カ　］，［　キ　］に入れる適切な字句を答えよ。

(2) 本文中の下線(h)について，マルチホーミングのために，グローバル IP アドレスをどのように割り当てるかを，40 字以内で述べよ。

(3) 本文中の下線(i)の接続先を，表 2 中の VLAN 名でそれぞれ答えよ。

(4) 本文中の［　ク　］～［　コ　］に入れる適切な字句を答えよ。

設問5　〔移行計画〕について，(1)～(7)に答えよ。

(1) 本文中の［　サ　］に入れる適切な字句を答えよ。

(2) 本文中の下線(j)の四つの A レコードに記述されている，FQDN とグローバル IP アドレスの数をそれぞれ答えよ。

(3) 本文中の下線(k)の FQDN に対応する機器名を，全て答えよ。

(4) 本文中の下線(l)について，2 通りの定義ファイルが必要な機器名を答えよ。

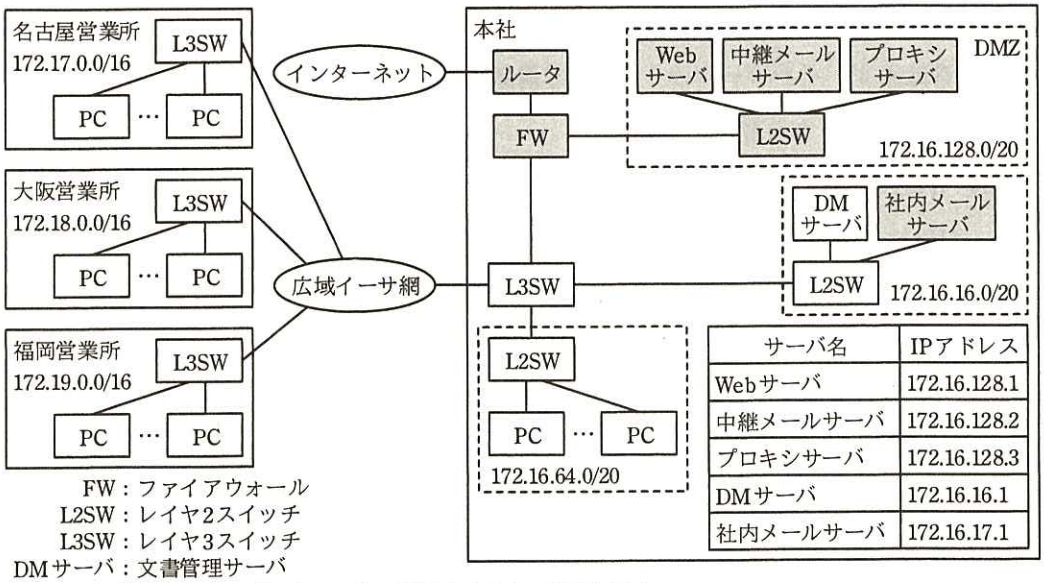
(5) 本文中の下線(m)の 3 種類の通信を，それぞれ 20 字以内で答えよ。

(6) 本文中の下線(n)の確認内容を，30 字以内で述べよ。

(7) 本文中の下線(o)のフィルタリング変更について，切替 2 で許可する通信を全て挙げ，図 5 中の記号（①，①'，②～④）を用いて答えよ。

問2　WAN 回線の冗長化設計に関する次の記述を読んで，設問 1 ～ 5 に答えよ。

Y 社は，従業員 400 名の医療機器販売会社で，東京本社の他に名古屋，大阪，福岡に営業所がある。本社と営業所間は，広域イーサネットサービス網（以下，広域イーサ網という）で接続されている。本社で各種のサーバを運用し，営業所は，広域イーサ網経由でサーバにアクセスしている。また，本社及び営業所からのインターネットアクセスは，本社のプロキシサーバ経由で行っている。現在の Y 社のネットワーク構成を図 1 に示す。



FW：ファイアウォール
L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ
DMサーバ：文書管理サーバ

注記 1　網掛け部分は，データセンタに移設する予定の機器を示す。
注記 2　FW は，ルータに接続するポートで NAT を行っている。
注記 3　広域イーサ網へのアクセス回線は，本社が 100M ビット／秒，営業所が 10M ビット／秒である。
注記 4　インターネットへのアクセス回線は，100M ビット／秒である。

図 1　現在の Y 社のネットワーク構成

このたび，Y 社では，WAN 回線の可用性向上を目的に，ネットワーク再構築プロジェクトを発足させた。プロジェクト責任者には情報システム部の M 課長が任命され，M 課長は，ネットワーク担当の N 主任と J 君をプロジェクトメンバに指名し，新ネットワークの検討を指示した。その際，M 課長が示した新ネットワークの要件を，次に示す。

・インターネット VPN を新たに導入して WAN 回線を冗長化し，アクセス先のサーバによって使用する WAN 回線を分け，WAN 回線を有効に活用すること
・本社の DM サーバ以外のサーバを，Z 社のデータセンタに移設する。このとき，サーバの IP アドレスの変更が生じないようにすること

N 主任は，インターネット VPN と既設の広域イーサ網間で OSPF を稼働させれば，これらの要件を満たすことができると考えた。そこで，J 君に，インターネット VPN の構築技術の検討を指示した。

〔インターネット VPN の構築技術の検討〕

J 君はまず，インターネット VPN の構築に広く利用されている IPsec を調査し，その結果を次のとおり整理した。

(1) IPsec ルータ

・IPsec で使用される認証方式，暗号化方式，暗号鍵などは，IPsec ルータ同士による IKE（Internet Key Exchange）のネゴシエーションによって，IPsec ルータ間で合意される。この合意は，SA（Security Association）と呼ばれる。
・SA の内容が確定すると，SA に関連付けされた SPI（Security Parameters Index）が，［ ア ］ビットの整数値で割り当てられる。SPI は，IPsec 通信の各パケット中に挿入され，そのパケットに適用された SA の識別キーとなる。
・IPsec ルータは，通信相手の IPsec ルータにパケットを送信するとき，IPsec 通信を行うか否か，IPsec 通信を行うときはどの SA を使うかなど，当該パケットに施す処理を示したセキュリティポリシ（以下，SP という）を選択する。処理には，PROTECT（IPsec を適用して送信），BYPASS（IPsec を適用せずに送信），DISCARD（廃棄）の 3 種類がある。
・SP を選択するキーを［ イ ］と呼び，IP アドレス，プロトコル，ポート番号などが利用される。SP は，SP データベースで管理される。SP データベースは経路表に似た構造をもっている。
・IPsec ルータは，通信相手の IPsec ルータからパケットを受信すると，パケット中の SPI で SA を識別し，当該 SA に関連する情報を取り出す。その情報を基に，受信したパケットを処理する。

(2) IPsec の通信

・IPsec の通信手順は，図 2 のとおりである。

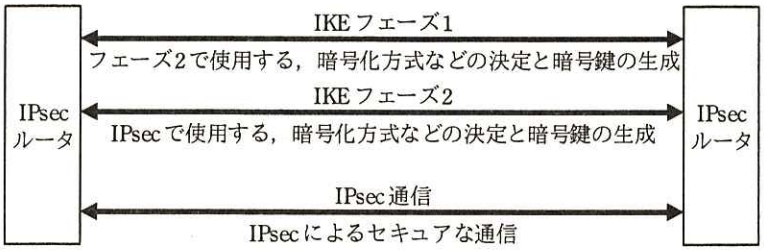


図 2　IPsec の通信手順

・IKE フェーズ 1 では，IKE フェーズ 2 で使用する ISAKMP（Internet Security Association and Key Management Protocol）SA 又は IKE SA（以下，両方を ISAKMP SA という）に必要なパラメータの交換，鍵交換及び認証が行われる。IKE フェーズ 1 には，メインモードと［　ウ　］モードがある。メインモードでは 3 往復の通信が行われるが，［　ウ　］モードは 1 往復半の通信で完了する。IKE フェーズ 1 で決定されるパラメータを表 1 に示す。

表 1　IKE フェーズ 1 で決定されるパラメータ（抜粋）

パラメータ	説明
暗号化方式	ISAKMP メッセージの暗号化アルゴリズム
ハッシュ方式	ISAKMP メッセージの完全性の検証と鍵計算に使用するハッシュアルゴリズム
ライフタイム	ISAKMP SA の生存期間
認証方式	IPsec 通信相手機器の認証方式
鍵交換方式	鍵交換のためのアルゴリズム

・IKE フェーズ 2 では，IPsec SA に必要なパラメータが決定される。IKE フェーズ 2 で決定されるパラメータを表 2 に示す。

表2　IKE フェーズ2で決定されるパラメータ（抜粋）

パラメータ	説明
セキュリティプロトコル	IPsec 通信で使用するセキュリティプロトコル
暗号化方式	IPsec 通信で使用する暗号化アルゴリズム
認証方式	IPsec 通信で使用する認証アルゴリズム
ライフタイム	IPsec SA の生存期間
通信モード	トンネルモード又はトランスポートモード

・IKE フェーズ2の通信は，IKE フェーズ1で確立した ISAKMP SA を使って行われる。IKE フェーズ2では，1往復半の通信で IPsec SA を確立する。IPsec 通信は，IKE フェーズ2で確立した IPsec SA を使って行われる。

・IPsec は，暗号化機能とトンネリング機能をもち，通信相手の IPsec ルータの認証，安全な鍵生成，転送データの暗号化，転送データの完全性の認証などを行う。

・トンネリングは，インターネットのような共用ネットワーク上の 2 点間で，仮想の専用線を構築することである。トンネリングは，あるプロトコルのトラフィックを別のプロトコルでカプセル化することで実現する。

・IPsec では，ユニキャストの IP パケットをカプセル化して転送する。

調査の結果，(a) Y 社で検討中の IPsec ルータは，OSPF の通常の設定では，リンクステート情報の交換パケットをカプセル化できないので，J 君は，IPsec によってインターネット VPN を構築したとき，OSPF を稼働することができないと考えた。静的経路制御でも広域イーサ網との間で負荷分散を行うことができるが，運用管理を容易にするために OSPF を稼働させたい。

そこで，J 君は，調査結果を基に N 主任に相談したところ，“他のトンネリング技術についても調査するように”という指示を受けた。

〔トンネリング技術の調査〕

ネットワーク層のプロトコルをトンネリングするプロトコルには，GRE（Generic Routing Encapsulation）があり，データリンク層のプロトコルをトンネリングするプ

ロトコルには，L2TP（Layer 2 Tunneling Protocol）がある。

J 君が調査した結果，OSPF のリンクステート情報の交換パケットを GRE 又は L2TP でカプセル化すれば，そのパケットは IPsec でカプセル化できるので，インターネット VPN で OSPF を稼働できることが分かった。

そこで，J 君はまず，GRE を調査した。

GRE は，RFC 1701，RFC 2784 で仕様が公開されている。GRE は，ネットワーク層のプロトコルのパケットをカプセル化して転送する機能をもつ。GRE では，IP ブロードキャストも IP マルチキャストパケットもカプセル化して転送できる。カプセル化とカプセル化の解除は，GRE トンネリングを行う両端の機器で行われる。IP パケットが GRE でカプセル化されたときのパケット形式を，図 3 に示す。

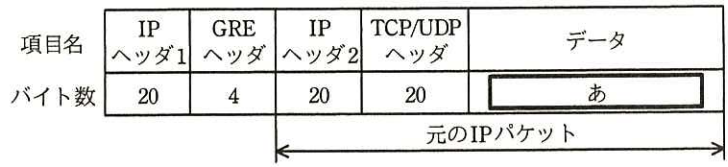
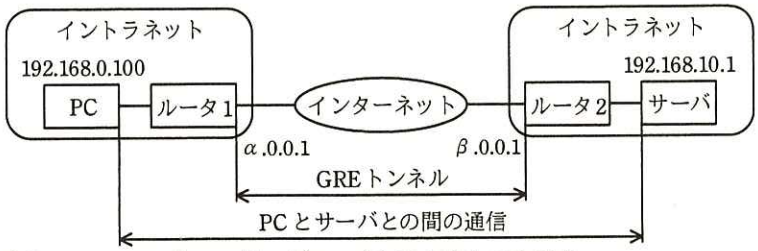


図 3　IP パケットが GRE でカプセル化されたときのパケット形式

IP パケットを GRE でカプセル化すると，カプセル化された元のパケットの宛先への［　エ　］情報をインターネットがもたなくても，元のパケットによるエンドツーエンドの通信が可能になる。GRE 利用時の通信例を図 4 に示す。



注記　α.0.0.1，β.0.0.1 は，グローバル IP アドレスを示す。

図 4　GRE 利用時の通信例

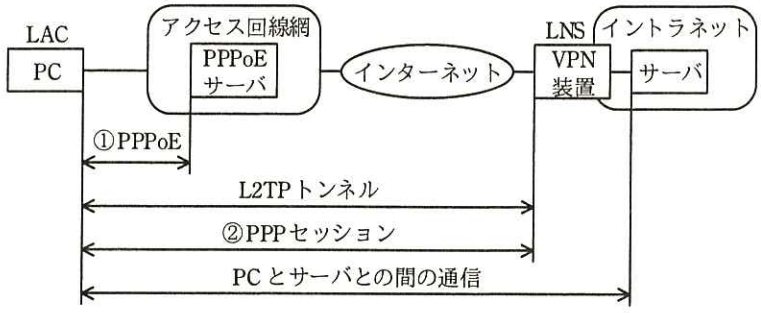
図 3 に示したカプセル化によって，図 4 中の，GRE トンネルインタフェースの MTU は，イーサネットインタフェースの MTU よりも 24 バイト小さくなる。このとき，図 4 中の PC 及びサーバのイーサネットインタフェースの MTU サイズを適切な値に変更することによって，パケットの［　オ　］を防げる。

次に，J 君は，RFC 2661 で仕様が公開されている L2TP を調査した。

L2TP は，PPP フレームをカプセル化して転送する機能をもつ。カプセル化とカプセル化の解除は，L2TP トンネリングを行う LAC（L2TP Access Concentrator）又は LNS（L2TP Network Server）の機能をもつ両端の機器で行われる。LAC は，トンネリングを要求する機器で，LNS は受け入れる機器である。L2TP でカプセル化されたときのパケット形式を，図 5 に示す。

図 5　L2TP でカプセル化されたときのパケット形式

L2TP を利用することによって，LAC 機能を実装した PC は，LNS 機能をもつ VPN 装置にインターネット経由で接続して，イントラネット内のサーバにリモートアクセスできる。PC が PPPoE で WAN に接続する構成における，L2TP 利用時の通信例を図 6 に示す。



注記　本例では，PC が PPPoE によって，IP アドレスを動的に取得する構成例を示す。

図 6　L2TP 利用時の通信例

J君は，GRE及びL2TPの機能と動作については理解できたが，どちらのプロトコルを利用すべきか判断できなかったので，調査結果を基にN主任に相談した。N主任からは，“トンネリングプロトコルを使用する目的と，使用したときの影響の度合いを考慮して判断するように”という指示を受けた。

J君は，(b) GREを利用することにして，GRE over IPsecを稼働させる方法について検討した。

〔GRE over IPsecの稼働方法の検討〕

インターネットVPNではデータの暗号化が必要になるので，ESPを利用する。(c) 通信モードは，トランスポートモードを選択する。そのときの，GRE over IPsecのパケット形式を図7に示す。

元のパケットの構成

項目名	IPヘッダ	TCP/UDPヘッダ	データ

カプセル化されたパケットの構成

項目名	IPヘッダ1	ESPヘッダ	GREヘッダ	IPヘッダ2	TCP/UDPヘッダ	データ	ESPトレーラ	ESP認証データ
バイト数	20	8	4	20	20	可変	不定	不定

図7　GRE over IPsecのパケット形式

J君は，GRE over IPsecを稼働させたときのOSPFの通信の概要を図8にまとめた。

図8　GRE over IPsecを稼働させたときのOSPFの通信の概要

図7に示したように，GRE over IPsecを稼働させるとカプセル化のオーバヘッドが大きくなる。そこで，必要に応じてIPsecルータでMSS（Maximum Segment Size）

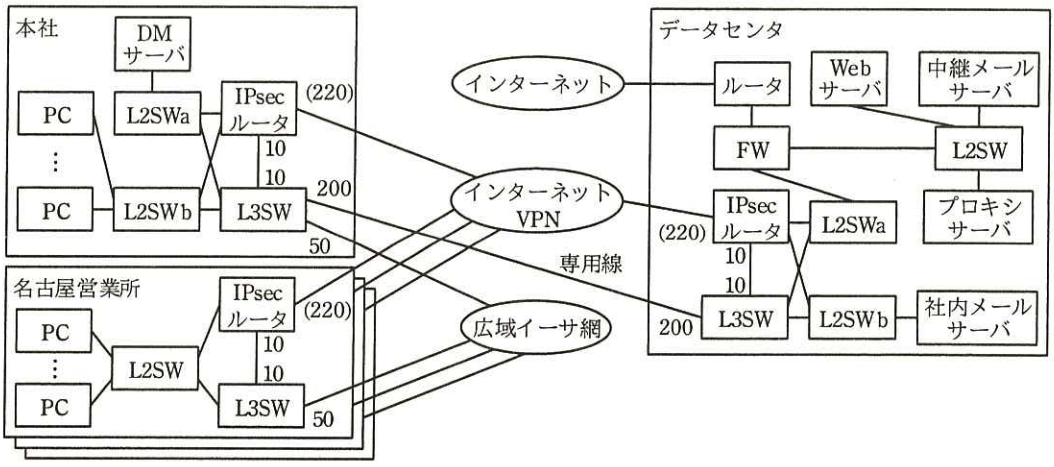
を適切な値に書き換えるとともに，トンネルインタフェースに適切な MTU の値を設定する。

図 8 中の IPsec ルータには，IPsec，GRE 及び OSPF の設定を行う。PC とサーバからインターネット VPN 向けに送信されるパケット，及び OSPF によってインターネット VPN に広告されるリンクステート情報には，GRE によるカプセル化と IPsec による暗号化を設定する。

J 君は，GRE over IPsec の稼働方法をまとめた後に，WAN の設計を行った。

〔WAN の設計〕

現在使用中の広域イーサ網へのアクセス回線は，継続して使用する。本社とデータセンタ間は，10 M ビット／秒の専用線を新たに導入して直接接続する。インターネット VPN のアクセス回線は，営業所に 100 M ビット／秒，データセンタに 1 G ビット／秒のものを新たに導入する。本社では，既設のインターネットアクセス回線をインターネット VPN のアクセス回線として転用する。データセンタには，インターネットアクセス用に，1 G ビット／秒のアクセス回線を導入する。インターネットに公開される DMZ のサーバのグローバル IP アドレスは，FW の静的 NAT 機能によって，サーバに設定されているプライベート IP アドレスに変換される。J 君が設計した WAN 回線の構成を図 9 に示す。



注記 1　大阪営業所と福岡営業所は，名古屋営業所と同構成である。
注記 2　IPsec ルータと L3SW のポートの数値は，OSPF で設定するコスト値である。
注記 3　IPsec ルータのポートに示した ( ) 内の数値は，トンネルインタフェースに設定するコスト値を示す。

図 9　J 君が設計した WAN 回線の構成

図 9 中の IPsec ルータと L3SW で OSPF を稼働させる。インターネット VPN は，データセンタと本社間，及びデータセンタと営業所間で設定する。

図 9 中の，本社，営業所及びデータセンタ内の L3SW と IPsec ルータ間では，それぞれ VRRP を稼働させる。OSPF のリンクステート情報の交換は，L3SW と IPsec ルータの WAN へのアクセス回線を接続するポートだけでなく，L3SW と IPsec ルータを直接接続するポートでも行わせる。このとき，L3SW と IPsec ルータのポートには，図中に示したコスト値を設定する。

図 9 に示した WAN 回線の構成で，図中のコスト値を設定することによって，営業所の PC からサーバへのアクセスは，広域イーサ網とインターネット VPN を使い分けることができる。PC からサーバへのアクセス経路の一覧を表 3 に示す。

表 3　PC からサーバへのアクセス経路の一覧（抜粋）

障害箇所	送信元	宛先	経路
なし	本社の PC	データセンタのサーバ	PC→専用線→データセンタ→サーバ
		インターネット	(d) PC→専用線→データセンタ→プロキシサーバ→インターネット
		DM サーバ	PC→DM サーバ
	営業所の PC	データセンタのサーバ	PC→インターネット VPN→データセンタ→サーバ
		インターネット	PC→インターネット VPN→データセンタ→プロキシサーバ→インターネット
		DM サーバ	PC→広域イーサ網→本社→DM サーバ
名古屋営業所のインターネット VPN 接続	名古屋営業所の PC	データセンタのサーバ	PC→［　う　］→データセンタ→サーバ
		インターネット	PC→［　う　］→データセンタ→プロキシサーバ→インターネット
		DM サーバ	変更なし
名古屋営業所の広域イーサ網接続	名古屋営業所の PC	データセンタのサーバ	変更なし
		インターネット	変更なし
		DM サーバ	PC→［　え　］→本社→DM サーバ

以上の検討を基に，J 君は M 課長から示された要件を満たす WAN 回線の冗長化構成の設計を完了させ，検討結果を N 主任に説明した。N 主任は，設計内容に問題がないことを確認し，J 君とともに検討結果を M 課長に報告したところ，設計内容が承認された。

設問1　本文中の［　ア　］～［　オ　］に入れる適切な字句又は数値を答えよ。

設問2　〔インターネット VPN の構築技術の検討〕について，(1) ～ (3) に答えよ。

(1) 表 2 中のライフタイムの終了時点に，IPsec ルータで行われる処理を答えよ。

(2) 表 2 中の認証方式によって認証できる対象と，その認証内容を，40 字以内で述べよ。

(3) 本文中の下線 (a) について，カプセル化できない理由を，“OSPF” 及び “リンクステート情報” という字句を用いて，40 字以内で述べよ。

設問3　〔トンネリング技術の調査〕について，(1) ～ (4) に答えよ。

(1) 図 3 中の［　あ　］及び図 5 中の［　い　］に入れる最大バイト数を，それぞれ答えよ。ここで，ジャンボフレームは使用されないものとする。

(2) 図 4 中の PC からサーバへの通信における，図 3 中の IP ヘッダ 1 と IP ヘッダ 2 の送信元 IP アドレス及び宛先 IP アドレスを，図 4 中の字句を用いて，それぞれ答えよ。

(3) 図 6 中の ① 及び ② の通信で PC が取得する IP アドレスが格納されるヘッダを，図 5 中の項目名でそれぞれ答えよ。

(4) 本文中の下線 (b) について，GRE を利用する利点を，L2TP を利用する場合と比較して，60 字以内で述べよ。

設問4　〔GRE over IPsec の稼働方法の検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線 (c) については，トンネルモードで行う必要がない。その理由を，トンネリングに着目して，20 字以内で述べよ。

(2) 図 7 中の ESP 認証データ長は，表 2 中のパラメータで選択された方式によって変化する。その理由を，40 字以内で述べよ。

(3) 図 7 において，暗号化される項目名を全て答えよ。

設問5　〔WAN の設計〕について，(1) ～ (6) に答えよ。

(1) 図 9 の構成において，図 1 の構成からサーバをデータセンタに移設するのに伴い，サブネットを再設計して，データセンタに移動するサブネットを全て答えよ。ここで，移動するサブネットのプレフィックス長は 16，20 又は 24 とする。

(2) 図 9 中のデータセンタの IPsec ルータ，L3SW，L2SWa 及び L2SWb の間で

レイヤ 2 のループを発生させないためには，どのようにサブネットを設計すればよいか。“L2SWa” 及び “L2SWb” という字句を用いて，30 字以内で述べよ。

(3) 図 9 において，本社，営業所及びデータセンタで設定する仮想 IP アドレスの最少の個数を，それぞれ答えよ。

(4) 図 9 中の名古屋営業所の IPsec ルータと L3SW を直接接続する経路が切断されたときの，名古屋営業所の PC から本社及びデータセンタのサーバへのアクセス経路を，“VRRP のマスタルータ” という字句を用いて，60 字以内で述べよ。

(5) 表 3 中の下線 (d) について，インターネット VPN 経由の経路とならないことを，コスト値を示して，60 字以内で述べよ。ここで，PC が接続する VRRP のマスタルータは，L3SW で稼働しているものとする。

(6) 表 3 中の［ う ］，［ え ］に入れる適切な経路を，表 3 中の表記に従って全て列挙せよ。

6. 退室可能時間に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	15:10 ～ 16:20

7. **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。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，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，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

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