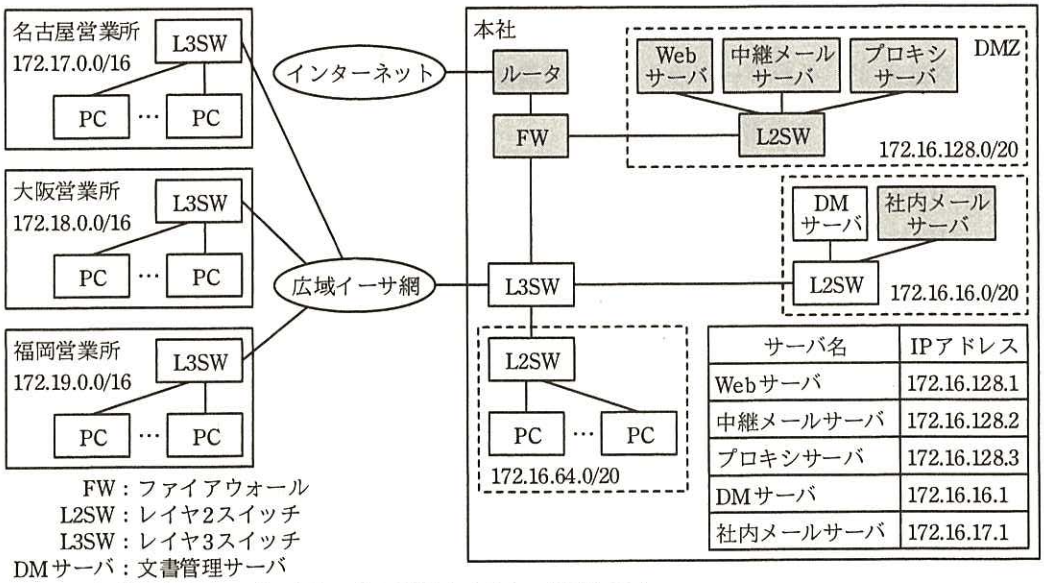
問２　WAN 回線の冗長化設計に関する次の記述を読んで，設問１～５に答えよ。

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。



サーバ名	IPアドレス
Webサーバ	172.16.128.1
中継メールサーバ	172.16.128.2
プロキシサーバ	172.16.128.3
DMサーバ	172.16.16.1
社内メールサーバ	172.16.17.1

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。

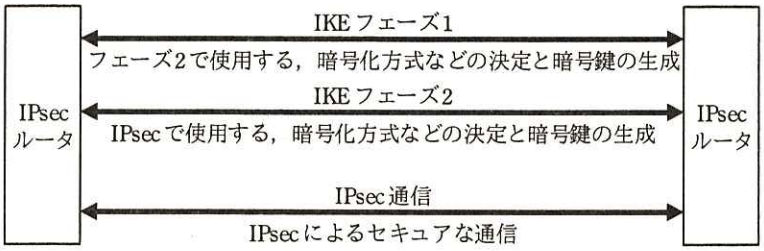


図 2　IPsec の通信手順

・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。

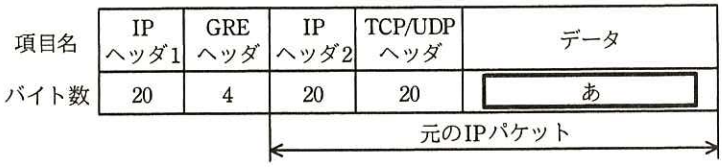
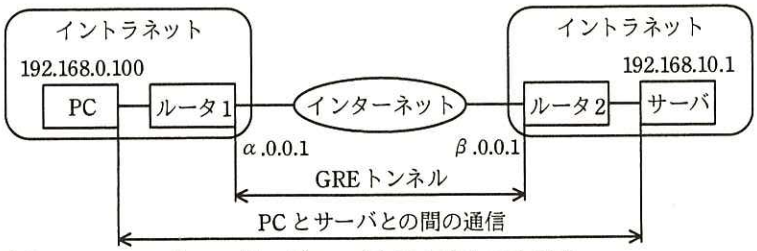


図 3　IP パケットが GRE でカプセル化されたときのパケット形式

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

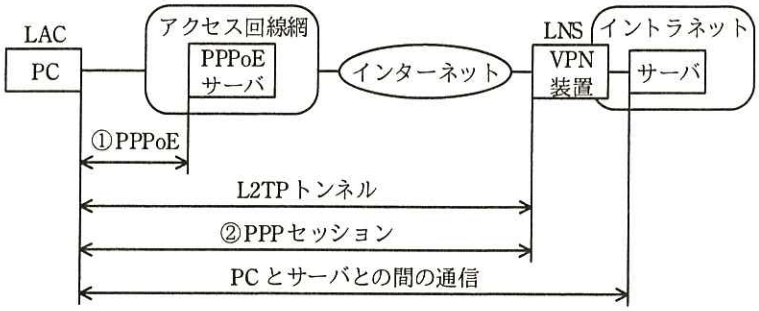
図 3 に示したカプセル化によって，図 4 中の，GRE トンネルインタフェースの MTU は，イーサネットインタフェースの MTU よりも 24 バイト小さくなる。このとき，図 4 中の PC 及びサーバのイーサネットインタフェースの MTU サイズを適切な値に変更することによって，パケットの［　オ　］を防げる。

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）

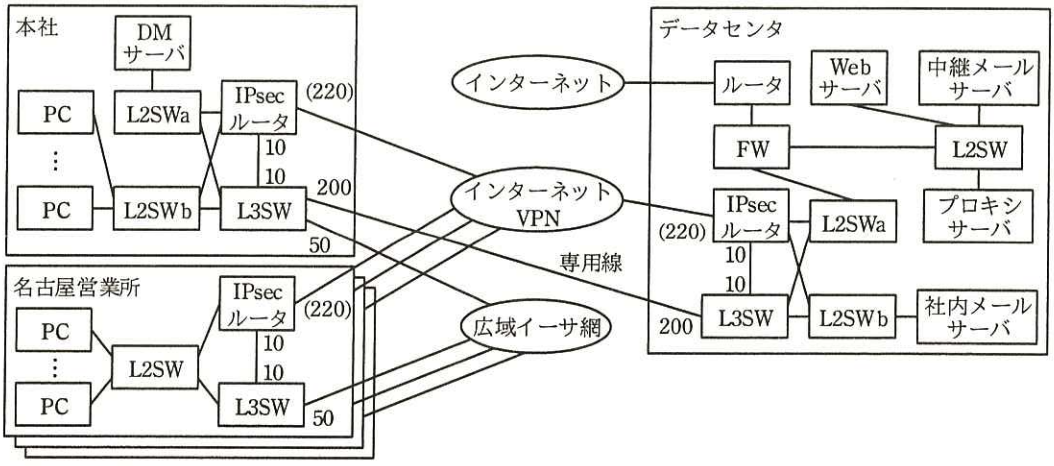
を適切な値に書き換えるとともに，トンネルインタフェースに適切な MTU の値を設定する。

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。