問３　企業内ネットワーク再構築に関する次の記述を読んで，設問 1～4 に答えよ。

D 社は，東京の本社，名古屋支店及び大阪支店の 3 拠点にオフィスを構える出版会社である。D 社の社内ネットワークは，3 拠点をそれぞれ専用線で結ぶ WAN と，拠点内 LAN で構成されている。各拠点内の業務にはそれぞれ拠点内の業務サーバを使用し，全社的な業務には本社の業務サーバを使用している。また，各拠点では本社のプロキシサーバを経由してインターネットを利用している。D 社の現行ネットワーク構成を図 1 に示す。

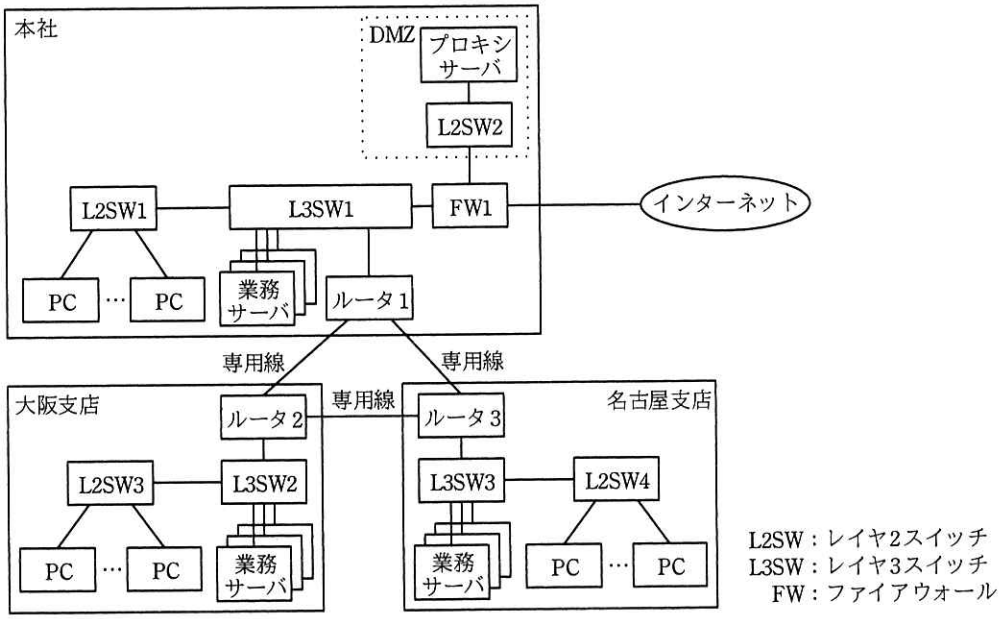

図 1　D 社の現行ネットワーク構成（抜粋）

D 社では，拠点間で利用しているルータの更改時期を迎えたことから，将来を見据えて WAN 構成を見直すことになり，情報システム部の E さんが検討することになった。

〔WAN 構成の検討〕

(1) WAN 構成の見直し方針案

E さんは，WAN 構成の見直しについてコストも含めて検討し，次の方針案を立

てた。

・IP-VPN を利用して 3 拠点間を接続する。

・IP-VPN へのアクセス回線は，安価なイーサネット回線サービスを利用する。

・通常時は拠点間通信に IP-VPN を用いるが，IP-VPN の障害時にはインターネット VPN をバックアップ回線として用いる。

・インターネット VPN は，FW に備わる IPsec 方式の VPN 機能を用いる。

・名古屋支店と大阪支店には，インターネット VPN 専用のインターネット回線を敷設し，FW を設置する。

・各拠点からのインターネットアクセスは，これまでと同様に本社のプロキシサーバ経由で行う。

(2) IP-VPN 及び IPsec の概要

E さんは，方針案の IP-VPN 及び IPsec について調査し，その結果を次のようにまとめた。

(i) IP-VPN

・IP-VPN は，通信事業者が運営する閉域 IP ネットワーク（以下，事業者閉域 IP 網という）を利用者のトラフィック交換に提供するサービスである。

・IP-VPN は，①事業者閉域 IP 網内で複数の利用者のトラフィックを中継するのに，RFC 3031 で規定された方式が用いられる。

・利用者のネットワークと事業者閉域 IP 網との接続点において，利用者が設置する CE（Customer Edge）ルータから送られたパケットは，通信事業者の PE（Provider Edge）ルータで［ア］と呼ばれる短い固定長のタグ情報が付与される。

・事業者閉域 IP 網内では，②タグ情報を参照して中継され，［ア］は対向側の［イ］で取り除かれる。

(ii) IPsec

・IPsec は，暗号技術を利用してノード間通信を行うためのプロトコルであり，IP パケット通信の完全性・機密性を確保する。

・IPsec は，OSI 基本参照モデルの［ウ］レイヤで動作する。

・3 拠点間には，バックアップ回線として 3 本の IPsec トンネルが必要である。

これらの検討を基に，E さんが考えた D 社のネットワーク構成を，図 2 に示す。

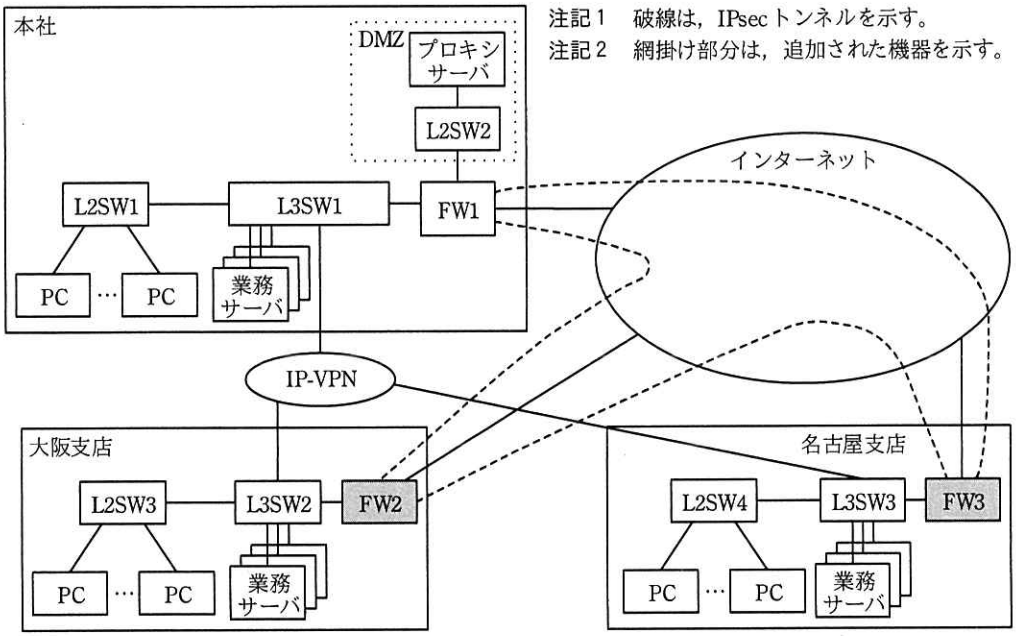

図 2　E さんが考えた D 社のネットワーク構成（抜粋）

〔冗長化ルーティングの検討〕

図 2 のネットワーク構成で拠点間通信を行う場合，正常時は［　エ　］を利用するが，［　エ　］の障害時は［　オ　］に切り替える必要がある。E さんはそのための方策の検討を行い，次のルーティング方式を考えた。

・各拠点間の IPsec トンネル及び各拠点内 LAN のルーティングは，OSPF を利用する。

・各拠点間の IPsec トンネル接続では，③GRE over IPsec を利用する。

・CE ルータでもある各拠点の L3SW は，IP-VPN 側で隣接する PE ルータと BGP4 で経路交換する。具体的には，各拠点の L3SW は，自拠点の経路情報を PE ルータに広告するとともに，④PE ルータから経路情報を受信する。

この方式で，本社，名古屋支店，大阪支店の L3SW からそれぞれの別拠点への経路の冗長化を行う。各拠点の L3SW は，⑤複数のルーティングプロトコルから得た同一宛先への異なる経路情報から，適切な経路を選択する。

〔拠点追加の場合の IPsec トンネル接続追加の検討〕

E さんは，IPsec トンネル接続の追加について，今後拠点が追加になった場合を想定した検討を始めた。図 2 のような⑥フルメッシュの IPsec トンネルのネットワーク構成に，追加拠点向け IPsec トンネルを手動で追加設定するネットワーク拡張方式は望ましくないと考え，ネットワーク機器ベンダの技術者に改善案を相談した。その結果，FW の IPsec 方式の VPN 機能のオプションである，IPsec トンネルを動的に確立する機能（以下，自動トンネル機能という）を活用した方式を提案された。そこで，E さんは，その方式を前提として次の設計方針を立てた。

・本社をハブ拠点，支店の 2 拠点をスポーク拠点とするハブアンドスポーク構成とし，ハブ拠点とスポーク拠点間の IPsec トンネルを従来どおり固定的に設定する。
・スポーク拠点間 IPsec トンネル（以下，S-S トンネルという）については，拠点間のトラフィックの発生に応じてトンネルを動的に確立させる。
・S-S トンネルは，一定時間トラフィックがなければ自動的に切断するようにする。
・動的に S-S トンネルを確立するために，NHRP（Next Hop Resolution Protocol）を用いる。

NHRP は，IPsec トンネル確立に必要な対向側 IP アドレス情報を，トンネル確立時に動的に得るのに利用される。IPsec トンネルの確立は，スポーク拠点間での通信の発生を契機にして行われる。例えば，名古屋支店内の PC から大阪支店内のサーバへの通信が行われる場合，⑦名古屋支店の FW3 は NHRP によって得られた情報を利用して S-S トンネルを確立する。このように，自動トンネル機能を利用すれば，フルメッシュ構成のトンネルを手動で設定する必要がない。

E さんは，それまでの設計方針をまとめ，ネットワーク機器ベンダの技術者に確認を依頼した。ネットワーク機器ベンダの技術者からは，OSPF と自動トンネル機能を組み合わせて利用する場合の留意点の指摘があった。その指摘の内容は，“スポークとなる機器が OSPF の代表ルータに選出されてしまうと，スポーク拠点間の IPsec トンネルが解放されなくなってしまうので，それを防ぐために，スポークとなる機器の OSPF に追加の設定が必要になる”というものであった。そこで，E さんは，防止策として⑧追加すべき設定内容を定めた。

その後，E さんが考えたネットワーク構成が情報システム部で承認され，E さんを

構築プロジェクトリーダとして，WAN の再構築が開始された。

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　〔WAN 構成の検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線①について，IP-VPN サービス提供のために事業者閉域 IP 網内で用いられるパケット転送技術を答えよ。

(2) 本文中の下線②について，事業者閉域 IP 網内の利用者トラフィック中継処理において，タグ情報を利用する目的を，25 字以内で述べよ。

設問３　〔冗長化ルーティングの検討〕について，(1)～(3) に答えよ。

(1) 本文中の下線③について，GRE over IPsec を利用する目的を，25 字以内で述べよ。

(2) 本文中の下線④について，各拠点の CE ルータが受信する経路情報を，15 字以内で答えよ。

(3) 本文中の下線⑤について，E さんが検討したルーティング方式において，L3SW での経路の優先選択の考え方を，25 字以内で述べよ。

設問４　〔拠点追加の場合の IPsec トンネル接続追加の検討〕について，(1)～(3) に答えよ。

(1) 本文中の下線⑥について，望ましくない理由を，30 字以内で述べよ。

(2) 本文中の下線⑦について，NHRP から得られる情報を，25 字以内で答えよ。

(3) 本文中の下線⑧について，追加設定が必要な機器を，図 2 中の機器名で全て答えよ。また，追加すべき OSPF の設定を，25 字以内で述べよ。