NW

平成30年度　秋期
ネットワークスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

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3
選択方法	2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。3問とも○印で囲んだ場合は，はじめの2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1，問3を選択した場合の例〕

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。

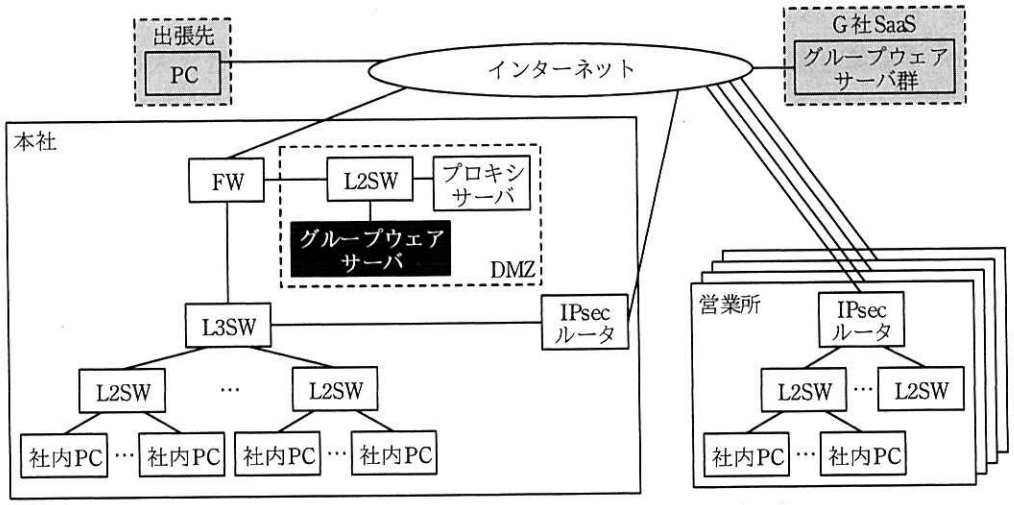
問1　SaaSの導入に関する次の記述を読んで，設問1～3に答えよ。

F社は，本社と四つの営業所を拠点として事業を展開している中堅商社である。本社を中心としたハブアンドスポーク構成のIPsec VPNを使って，本社と営業所を接続している。営業所からインターネットへの通信は，全て本社を経由させている。現在F社で利用しているグループウェア機能は，電子メール，スケジューラ，ファイル共有などである。このうち電子メールは社外との連絡にも利用している。

このたびF社では，グループウェアサーバの老朽化に伴い，グループウェアサーバを廃止し，グループウェア機能をもつG社SaaSを導入することにした。また，G社SaaSの導入に合わせたセキュリティ対策を講じることにした。

〔F社の現行ネットワーク構成とG社SaaS導入に合わせたセキュリティ対策〕

F社の現行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

注記1　[破線]は，G社SaaS導入に伴って追加予定の構成を示す。

注記2　[黒]は，G社SaaS導入後，廃止予定の機器を示す。

図1　F社の現行ネットワーク構成（抜粋）

・プロキシサーバ及びグループウェアサーバは，本社DMZに設置されている。

・L3SWでは，次のように静的経路設定を行っている。

- デフォルトルートのネクストホップをFWに設定している。
- 各営業所への経路のネクストホップを本社のIPsecルータに設定している。

・社内PCからインターネットへは，Webアクセスだけが許可されており，プロキシサーバを経由して通信を行っている。

一般に，プロキシには，［　ア　］プロキシと［　イ　］プロキシがある。F社のプロキシのように［　ア　］プロキシは，社内に対して，アクセス先URLのログ取得や，外部サーバのコンテンツをキャッシュして使用帯域を削減する目的で用いられる。一方，［　イ　］プロキシは，外部から公開サーバのオリジナルコンテンツに直接アクセスさせないことによる改ざん防止，キャッシュによる応答速度の向上，及び複数のサーバでの負荷分散を行う目的で用いられる。

G社SaaSの導入に合わせて，インターネットへのWebアクセスについてのセキュリティ対策を検討した。検討結果を次に示す。

・G社SaaSとの通信は，HTTPSによって暗号化する。
・出張先のPCから直接G社SaaSを利用できるようにするために，G社SaaSでは送信元IPアドレスの制限を行わない。
・G社SaaS導入に合わせてセキュリティ強化を行うために，プロキシサーバで次のログを取得する。
  - アクセス先URLと利用者ID
  - G社SaaSのファイルアップロード／ダウンロードのログと利用者ID
・社内PCからインターネットへのWebアクセスでは①プロキシサーバにおいて認証を行う。

〔G社SaaSの試用〕

F社は，G社SaaSの本格導入に先立って，本社と一つの営業所を対象に少数ライセンスでG社SaaSを試用し，システムの利便性と性能を確認することにした。試用に先立ち，G社SaaS以外のアクセス先について，プロキシサーバでHTTPSのアクセスログを確認したところ，②アクセス先のホスト名は記録されていたが，URLは記録されていなかった。そこで，アクセス先のURLを把握するために，プロキシサーバで暗号化通信を一旦復号し，必要な処理を行った上で再度暗号化した。しかし，

社内 PC でエラーメッセージ“証明書が信頼できない”が表示されたので，社内 PC に［　ウ　］をインストールして解決した。

G 社 SaaS を試用した結果，次の事実が判明した。

・G 社 SaaS にアクセスした際にプロキシサーバを通過するセッション数を実測したところ，スケジューラにアクセスする 1 人当たりのセッション数が大幅に増加した。

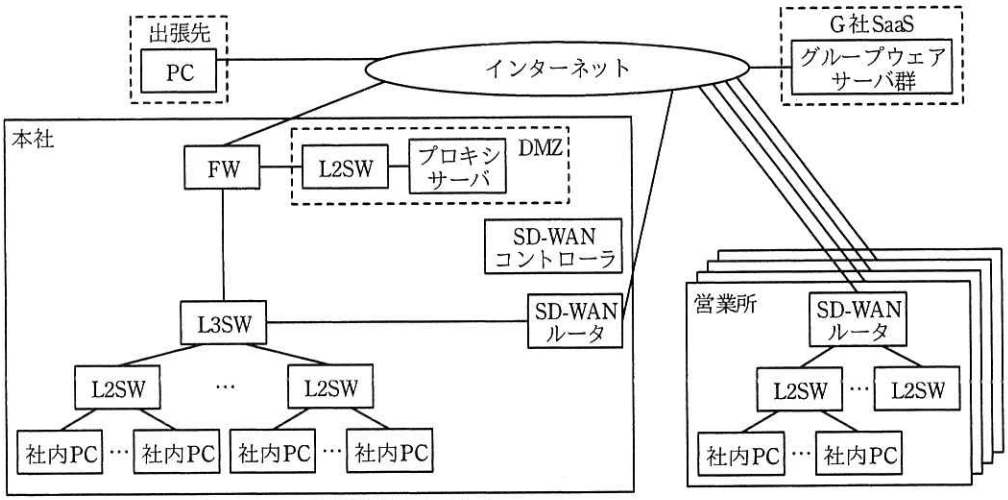
・複数人が同時に大容量のファイルを G 社 SaaS に転送している間，本社の FW を経由するインターネット接続回線のスループットが低下した。

このまま全社で G 社 SaaS の利用を開始すると，プロキシサーバの処理可能セッション数の超過，インターネット接続回線の帯域不足が予想された。

〔SD-WAN ルータの導入〕

F 社は，G 社 SaaS の試用で判明した問題を解決するために，IPsec ルータの代わりに SD-WAN（Software-Defined WAN）ルータを使用することにした。

SD-WAN ルータを使用したネットワーク構成案を，図 2 に示す。



注記　SD-WAN コントローラの接続構成は省略する。

図 2　SD-WAN ルータを使用したネットワーク構成案（抜粋）

(1) SD-WAN ルータの概要

今回使用する予定の SD-WAN ルータは，SDN（Software-Defined Networking）によって制御される IPsec ルータである。SDN は，利用者の通信トラフィックを転送するデータプレーンと，通信装置を集中制御する［　エ　］プレーンから構成されており，［　エ　］プレーンのソフトウェアでデータ転送を制御する方式である。

F 社が導入する SD-WAN ルータの仕様を次に示す。

・SD-WAN ルータの設定は，SD-WAN コントローラによって集中制御される。

・SD-WAN ルータの WAN 側には，インターネットに接続するインタフェースだけでなく，ほかの SD-WAN ルータに接続する IPsec VPN の論理インタフェースがある。

(2) SD-WAN ルータを用いたときの通信

図 2 の説明を次に示す。

・社内 PC から G 社 SaaS への Web アクセスは，プロキシサーバを経由せず各 SD-WAN ルータを経由する。

・社内 PC から G 社 SaaS 以外のインターネットへの Web アクセスは，プロキシサーバを経由する。

・L3SW にプロキシサーバへの静的経路情報を追加する。

・営業所と本社間の通信は，SD-WAN ルータ間で IPsec によって暗号化する。

・本社の社内 PC から G 社 SaaS への通信について，③G 社 SaaS の IP アドレスが変更された場合でもその都度 L3SW を設定しなくても済むように，L3SW の静的経路情報を設定変更する。

(3) SD-WAN ルータの運用

G 社は SaaS に必要なサーバを随時追加している。G 社 SaaS が利用している IP アドレスブロックの更新があるたびに，F 社は SD-WAN ルータの設定を変更する必要がある。F 社は，G 社 SaaS の IP アドレスブロックの更新を，RSS（Really Simple Syndication）を利用して知ることができる。

F 社は，RSS 配信された IP アドレスブロックを検知するツールを作成して，自動的にツールから［　オ　］に指示を行い，全社の SD-WAN ルータの設定を変更することにした。さらに，社内 PC から参照する④プロキシ自動設定ファイルを作

成することにした。

(4) G社SaaSアクセスログの取得

G社SaaSへのアクセスログは，⑤プロキシサーバからではなく，G社SaaSのAPIにアクセスして取得することにした。

F社は，G社SaaSの本格導入に向けてSD-WANルータを利用したネットワークの構築プロジェクトを立ち上げた。

設問1　〔F社の現行ネットワーク構成とG社SaaS導入に合わせたセキュリティ対策〕について，(1)，(2)に答えよ。

(1) 本文中の［　ア　］，［　イ　］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，プロキシサーバで認証を行うことによってアクセスログに付加できる情報を答えよ。

設問2　〔G社SaaSの試用〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，HTTPSでアクセスするためのHTTPプロトコルのメソッド名を答えよ。また，このメソッドを用いる場合，社内に侵入したマルウェアによる通信（ただし，HTTPS以外の通信）を遮断するためのプロキシサーバでの対策を，30字以内で述べよ。

(2) 本文中の［　ウ　］に入れる適切な字句を，20字以内で答えよ。

設問3　〔SD-WANルータの導入〕について，(1)～(5)に答えよ。

(1) 本文中の［　エ　］に入れる適切な字句を答えよ。

(2) 本文中の下線③について，設定変更後の静的経路情報を，35字以内で答えよ。

(3) 本文中の［　オ　］に入れる適切な字句を，図2中の機器名で答えよ。

(4) 本文中の下線④について，このファイルを作成することによってプロキシから除外する通信を，20字以内で答えよ。

(5) 本文中の下線⑤について，G社SaaSのAPI経由で取得する理由を二つ挙げ，それぞれ40字以内で述べよ。

問2　ネットワーク監視の改善に関する次の記述を読んで，設問1～4に答えよ。

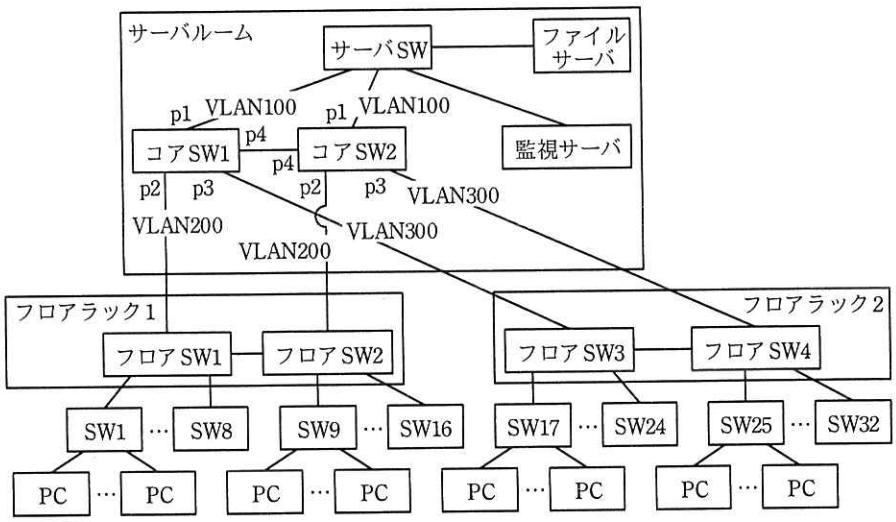
A社は従業員数200人の流通業者である。A社のシステム部門では，統合監視サーバ（以下，監視サーバという）を構築し，A社のサーバやLANの運用監視を行っている。

監視サーバは，pingによる死活監視（以下，ping監視という）とSYSLOGによる異常検知監視（以下，SYSLOG監視という）を行っている。現在定義されているLANに関するSYSLOG監視は，ポートのリンク状態遷移，STP（Spanning Tree Protocol）状態遷移及びVRRP（Virtual Router Redundancy Protocol）状態遷移の3種類である。

ある日，“従業員が使用するPCからファイルサーバを利用できない”という苦情が，システム部門に多数寄せられた。調査した結果，ケーブルの断線による障害と判明して対処したが，監視サーバで検知できなかったことが問題視された。

〔A社LANの概要〕

A社は，オフィスビルの1フロアを利用している。A社LANの構成を，図1に示す。



SW：スイッチ
注記1　コアSW1，コアSW2は，レイヤ3スイッチである。
注記2　フロアSW1～フロアSW4，サーバSW，SW1～SW32は，レイヤ2スイッチである。
注記3　p1～p4は，スイッチのポートを示す。
注記4　VLAN100，VLAN200，VLAN300は，スイッチのアクセスポートのVLAN IDを示す。

図1　A社LANの構成（抜粋）

コアSWには，サーバSWとフロアSWが接続されている。サーバSWは，監視サーバとファイルサーバを収容している。フロアSWには，従業員が使用するPCを収容するSWが接続されている。

A社LANは次のように設計されている。

・コアSWには，①VRRPが設定してあり，②正常時は，コアSW1がマスタルータで，コアSW2がバックアップルータとなるように設定している。

・A社LANは，ループ構成を含んでいる。例えば，コアSW1 - サーバSW - コアSW2 - コアSW1はループ構成の一つである。IEEE 802.1Dで規定されているSTPを用いて，レイヤ2ネットワークのループを防止している。正常時はコアSW1がルートブリッジとなるように設定している。

・コアSWのp1ポート，p2ポート及びp3ポートはアクセスポートで，③p4ポートをIEEE 802.1Qを用いたトランクポートに設定している。

〔監視サーバの概要〕

監視対象機器は，コアSW，サーバSW及びフロアSWである。

ping 監視には，RFC 792 で規定されているプロトコルである［　ア　］を利用する。echo request パケットの宛先として，監視対象機器には［　イ　］を割り当てる必要がある。

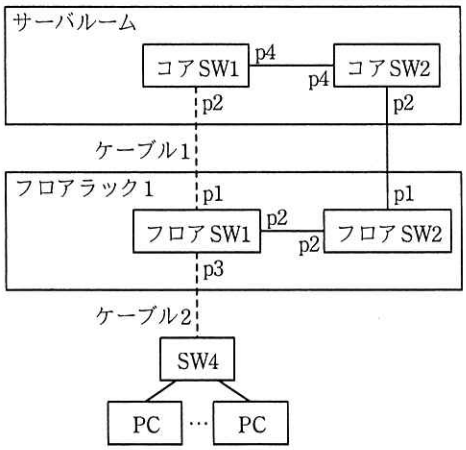
リンクダウンなどの異常が発生した機器は，監視サーバに対して直ちに SYSLOG メッセージを送信する。監視サーバは，受信した SYSLOG メッセージの分析を直ちに行い，定義に従って異常として検知する。SYSLOG は，トランスポートプロトコルとして RFC 768 で規定されている［　ウ　］を用いている。

〔監視サーバの問題〕

ネットワークに異常が発生した際に，監視サーバで検知できなかった問題について，システム部門の B 課長は，部下の C さんに障害発生時の状況確認とネットワーク監視の改善策の立案を指示した。

〔障害発生時の状況確認〕

ケーブルの断線による障害発生時の構成を，図 2 に示す。



注記　破線は，断線したケーブルを示す。

図 2　ケーブルの断線による障害発生時の構成（抜粋）

C さんが行った状況確認の結果は，次のとおりである。

・障害発生時，フロアラック 1 の近くでフロアのレイアウト変更が行われていた。その影響で，フロア SW1 の p1 ポートとコア SW1 の p2 ポートを接続するケーブル 1

が断線した。同時に，フロア SW1 の p3 ポートと SW4 を接続するケーブル 2 が断線した。

・ケーブル 1 の断線によって，④フロア SW2 の p1 ポートの STP のポート状態がブロッキングから，リスニング，ラーニングを経て，フォワーディングに遷移した。また，監視サーバでは，SYSLOG 監視によって，ケーブル 1 が接続されているポートのリンク状態遷移が発生したことを検知した。

・ケーブル 2 の断線に伴って⑤フロア SW1 が送信した，リンク状態遷移を示す SYSLOG メッセージが監視サーバに到達できなかった。その結果，監視サーバは，ケーブル 2 が接続されているポートのリンク状態遷移を検知できなかった。

〔ネットワーク監視の改善策の立案〕

C さんは，ネットワーク監視の改善策として，新たに SNMP（Simple Network Management Protocol）を使って監視することを検討した。C さんは，監視対象機器で利用可能な SNMPv2c について調査を行った。

SNMP は機器を管理するためのプロトコルで，⑥SNMP エージェントと SNMP マネージャで構成される。SNMP エージェントと SNMP マネージャは，同じグループであることを示す［　エ　］を用いて，機器の管理情報（以下，MIB という）を共有する。

SNMP の基本動作として，ポーリングとトラップがある。ポーリングは，SNMP マネージャが，SNMP エージェントに対して，例えば 5 分ごとといった定期的に MIB の問合せを行うことによって，機器の状態を取得できる。一方，トラップは，MIB に変化が起きた際に，SNMP エージェントが直ちにメッセージを送信し，SNMP マネージャがメッセージを受信することによって，機器の状態を取得できる。

C さんは，⑦5 分間隔のポーリング，又はトラップを使用して監視しても，今回発生したネットワークの異常においてはそれぞれ問題があることが分かった。しかし，SNMP のインフォームと呼ばれるイベント通知機能を利用すれば，これらの問題に対応できると考えた。

SNMP のインフォームでは，MIB に変化が起きた際に，SNMP エージェントが直ちにメッセージを送信し，SNMP マネージャからの確認応答を待つ。確認応答を受信できない場合，SNMP エージェントは，SNMP マネージャがメッセージを受信し

なかったと判断し，メッセージの再送信を行う。C さんは，⑧今回と同様なネットワークの異常が発生した場合に備えて，SNMP マネージャがインフォームの受信を行えるよう，SNMP エージェントの設定パラメタを考えた。

その後，C さんは SNMP のインフォームを用いたネットワーク監視の改善策を B 課長に報告し，その内容が承認された。

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　〔A 社 LAN の概要〕について，(1)～(3) に答えよ。

(1) 本文中の下線①について，PC 及びサーバに設定する情報に着目して，VRRP による冗長化対象を 15 字以内で答えよ。

(2) 本文中の下線②について，バックアップルータはあるメッセージを受信しなくなったときにマスタルータに切り替わる。VRRP で規定されているメッセージ名を 15 字以内で答えよ。

(3) 本文中の下線③について，p4 ポートでトランクポートに設定する VLAN ID を全て答えよ。

設問３　〔障害発生時の状況確認〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，BPDU（Bridge Protocol Data Unit）を受信しなくなったフロア SW2 のポートを，図 2 中の字句を用いて答えよ。

(2) 本文中の下線⑤について，フロア SW1 が送信した SYSLOG メッセージが監視サーバに到達できなかったのはなぜか。“スパニングツリー”の字句を用いて 25 字以内で述べよ。

設問４　〔ネットワーク監視の改善策の立案〕について，(1)～(3) に答えよ。

(1) 本文中の下線⑥について，SNMP エージェントと SNMP マネージャに該当する機器名を，図 1 中の機器名を用いてそれぞれ一つ答えよ。

(2) 本文中の下線⑦について，ポーリングとトラップの問題を，それぞれ 35 字以内で述べよ。

(3) 本文中の下線⑧について，SNMP エージェントが満たすべき動作の内容を，40 字以内で述べよ。

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。

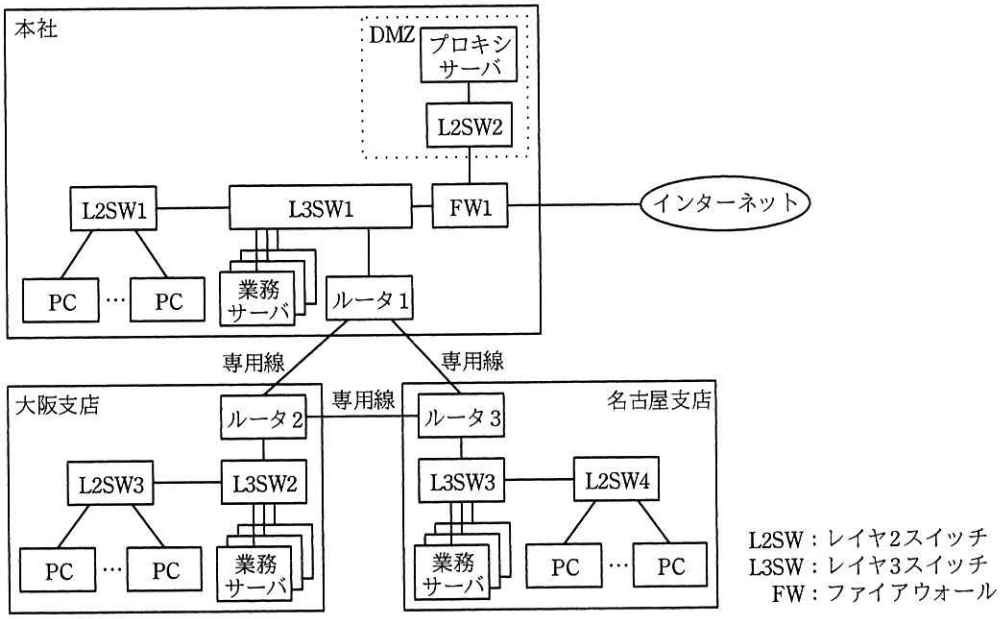


図 1　D 社の現行ネットワーク構成（抜粋）

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。

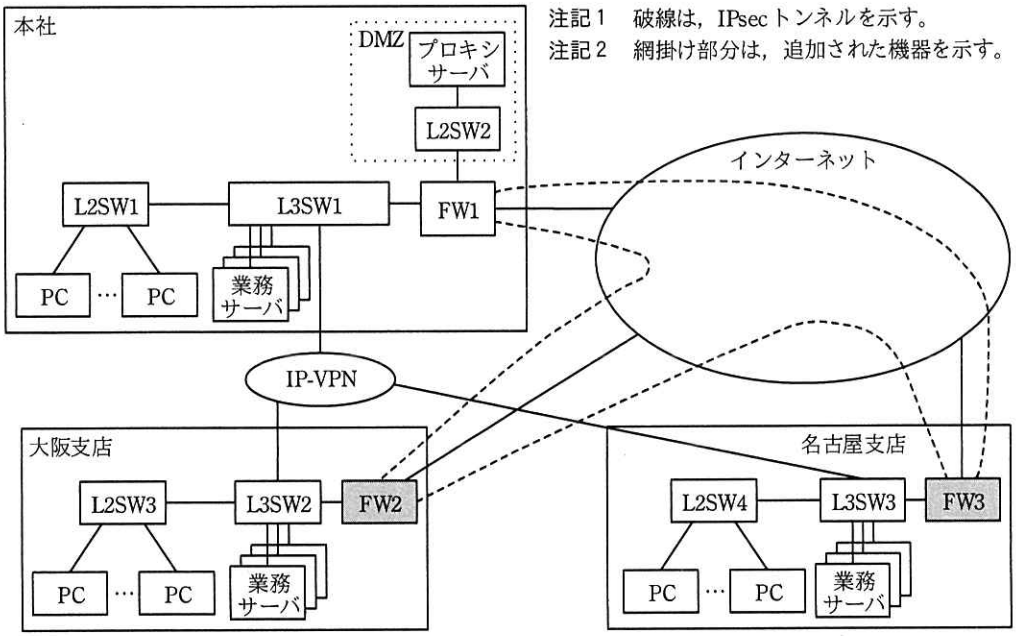


図 2　E さんが考えた D 社のネットワーク構成（抜粋）

〔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。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，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	13:10 ～ 13:50

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。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。