NW

平成29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〕

選択欄	
2問選択	○問1
	問2
	○問3

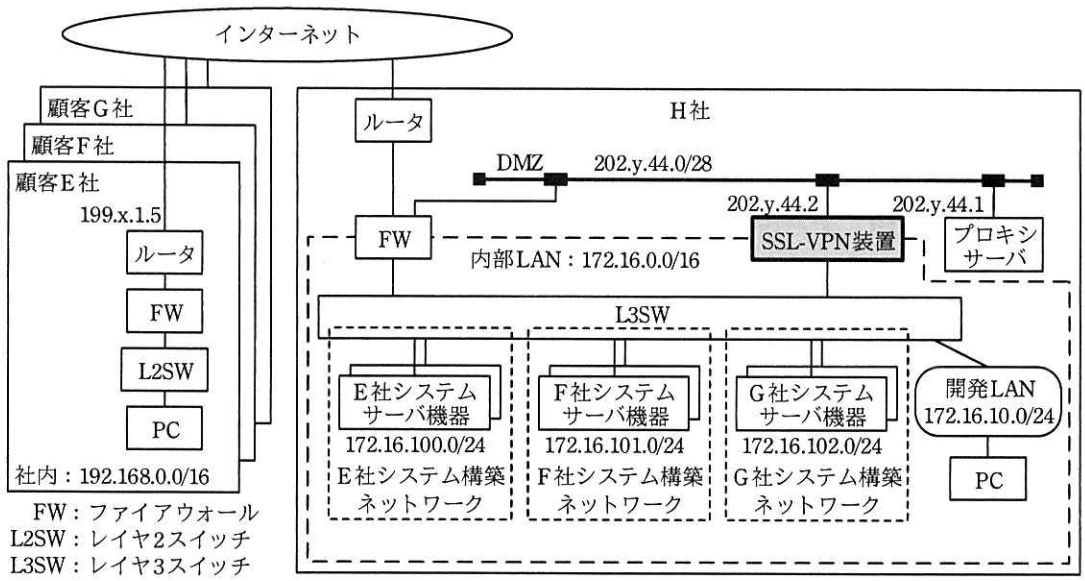
注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　SSL-VPN の導入に関する次の記述を読んで，設問 1～4 に答えよ。

H 社は，顧客の業務システムの構築（以下，顧客システム構築という）を主力業務とする，中堅のシステム開発会社である。顧客システムは，様々なサーバ機器，OS，ミドルウェアなどを組み合わせて構築され，利用されるプロトコルも様々である。H 社の拠点で構築されて，最終的に顧客の拠点に納入されたシステムは，顧客社内の PC などから利用される。

〔H 社の現行ネットワーク〕

H 社では，受注した顧客システム構築専用のネットワーク（以下，顧客システム構築ネットワークという）をそれぞれ設け，一つの顧客システム構築ネットワークに，H 社の内部 LAN のサブネットを一つ割り当てている。顧客システム構築は，開発 LAN に接続された PC から顧客システム構築ネットワークにアクセスして行っている。現在，E 社，F 社，G 社の 3 社から受注した顧客システムを構築中である。H 社は，内部 LAN からインターネットへの Web アクセスを，DMZ のプロキシサーバを経由して行っている。H 社の現行ネットワーク構成を，図 1 に示す。



注記1　199.x.1.5，202.y.44.0/28は，グローバルIPアドレスを示す。
注記2　網掛け部分は，追加予定の機器であることを示す。
注記3　E社システム構築ネットワーク，F社システム構築ネットワーク，G社システム構築ネットワークは，各社の顧客システム構築ネットワークを示す。

図1　H社の現行ネットワーク構成（抜粋）

〔顧客システム構築業務の問題とその解決策〕

H 社では，顧客システム構築業務において次に示す問題を抱えている。

（問題 1）顧客システム構築ネットワークに対して，当該構築業務とは関係がない PC から不正なアクセスを受ける可能性がある。

（問題 2）顧客システム構築を H 社の拠点で行っているので，顧客はシステムが納入されるまで動作確認ができない。

これらの問題に対処するために，解決策の検討を任された H 社情報システム部の S さんは，SSL-VPN を利用すれば解決できると考えた。S さんの検討結果を次に示す。

(1) SSL-VPN について

SSL-VPN は，SSL/TLS プロトコルを利用した VPN 技術である。その利用には，SSL/TLS のプロトコルのバージョン，及びプロトコルに含まれるアルゴリズムについて，次に示す点を考慮する必要がある。

・十分な安全性を確保できないとされるハッシュアルゴリズムである MD5 又は［ア］を使用しないで済むように，TLS プロトコルのバージョン［イ］以上を利用する。

・SSL/TLS のコネクション開設時に，クライアント側から送られる［ウ］メッセージと，サーバ側から返される［エ］メッセージの交換が行われる。このとき，それ以降で用いられる暗号スイート（アルゴリズムの組合せを示した情報）が決定される。その情報には，アプリケーション層の暗号化に使われる暗号アルゴリズム以外に，（Ⅰ）2 種類の暗号アルゴリズムと 1 種類のハッシュアルゴリズムが含まれる。

(2) SSL-VPN の動作方式

SSL-VPN の基本的な動作には，［オ］，ポートフォワーディング，L2 フォワーディングの 3 方式がある。（Ⅱ）H 社の場合は L2 フォワーディング方式が望ましいと，S さんは判断した。S さんがベンダに確認した L2 フォワーディング方式の動作概要を次に示す。

・PC にインストールするクライアントモジュールから SSL/TLS 接続を行う。

・（Ⅲ）接続時の認証に応じて，PC に適切な IP アドレスを割り当てる。

・PC と SSL-VPN 装置間の SSL/TLS 接続トンネル上で，レイヤ 2 の中継を行う。

S さんは，これらの検討結果から，開発 LAN 及び顧客各社の PC から顧客システム構築ネットワークに対する必要なアクセスを全て SSL-VPN 経由で行うようにすることで，問題 1 と問題 2 に対応できると考え，SSL-VPN 装置を新たに導入することにした。また，その問題の対応には，FW，L3SW などの設定変更も必要になると考えた。

〔SSL-VPN 装置の導入のための検討〕

S さんは，SSL-VPN 装置導入のための具体的な項目の検討を行った。検討結果は，次のとおりである。

(1) SSL-VPN 装置の設置位置

・顧客からインターネット経由で VPN 接続することと，開発 LAN から VPN 接続することを考慮して，SSL-VPN 装置の設置位置は DMZ と L3SW の間とする。

・SSL-VPN 装置から内部 LAN への通信用に，L3SW に新たな VLAN（VLAN201）を設け，SSL-VPN 装置の内側のインタフェースを L3SW に接続する。PC から顧客システム構築ネットワークへのアクセス経路が［PC→SSL-VPN 装置→VLAN201→顧客システム構築ネットワーク］となるように経路を設定する。

(2) SSL-VPN 装置へのユーザに関する情報登録

・SSL-VPN 装置に，VPN を利用するユーザに関する情報（以下，ユーザ情報という）を登録する。ユーザ情報には，VPN 接続時のユーザ認証のための情報も含まれる。

・ユーザ情報中の設定項目であるグループ番号には，そのユーザに対応する顧客番号を設定する。顧客番号は，顧客ごとに割り当てられている 1 以上 100 以下の整数である。以下，この整数を k で表す。

(3) IP アドレスの割当て

・顧客番号 k の顧客（以下，顧客 k という）に対応する顧客システム構築ネットワーク：172.16.z.0/24（ここで，z は 99＋k とする）

・顧客 k に対応する VPN 接続 PC 用 IP アドレスプール：10.100.k.1～10.100.k.200

・VPN 接続時には，認証されたユーザに対応する顧客番号を用いて，IP アドレスプールを選択する。

(4) FW のルール設定

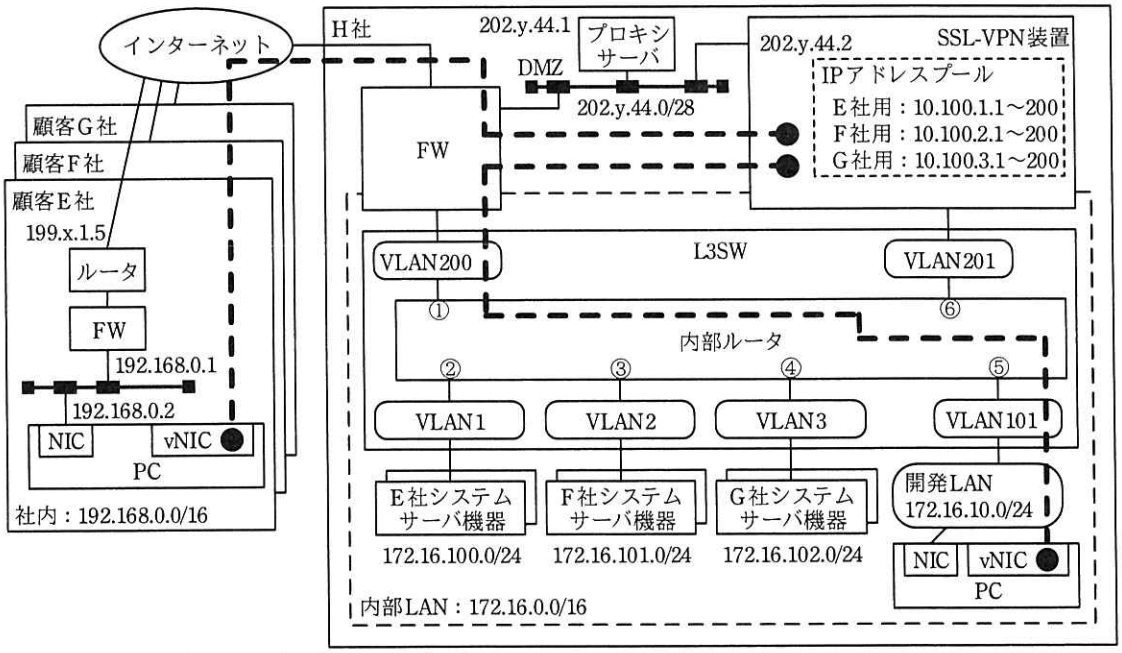
SSL-VPN 導入後の FW のルールは，表 1 のとおり設定する。

表 1　通信を許可する FW ルール設定（抜粋）

アクセス経路	送信元 IP アドレス	宛先 IP アドレス	プロトコル／宛先ポート	アドレス変換
カ → キ	ク	202.y.44.0/28	任意	無
DMZ→インターネット	202.y.44.0/28	任意	任意	無
インターネット→DMZ	任意	ケ	TCP/443	無

〔検討後のネットワーク構成〕

S さんは，更に検討を進め，図 2 に示すネットワーク構成を作成した。



NIC：ネットワークインタフェースカード
vNIC：仮想ネットワークインタフェースカード
内部ルータ：L3SW 中の L3 処理機能
注記 1　●－－● は，SSL-VPN トンネルを示す。
注記 2　①～⑥は，内部ルータの仮想インタフェースを示す。

図 2　検討後のネットワーク構成（抜粋）

〔問題 1 の解決策〕

S さんは，問題 1 の解決策として，次の二つの通信制限をすることにした。

(1) VLAN 間の不正通信制限

（Ⅳ）表 2 に示すアクセスリストを L3SW に設定して通信制限する。

表 2　VLAN 間通信制限のためのアクセスリスト

項番	動作	送信元 IP アドレス	宛先 IP アドレス
1	禁止	Any	172.16.0.0/16
2	許可	Any	Any

注記 1　Any は，パケットフィルタリングにおいてチェックしないことを示す。
注記 2　アクセスリストは，項番が小さい順に参照され，最初に該当したルールが適用される。
注記 3　どのルールにも該当しないものは禁止される。

表 2 のアクセスリストは，H 社内の VLAN 間通信のうちで不正なものを禁止する。具体的には，開発 LAN から顧客システム構築ネットワークへの直接アクセス（SSL-VPN を経由しないアクセス）と，（Ⅴ）それ以外の不正な通信を禁止する。

(2) SSL-VPN 接続する PC（以下，VPN-PC という）の通信制限

（Ⅵ）表 3 に示すアクセスリストを L3SW に設定して通信制限する。

表 3　VPN-PC の通信制限のためのアクセスリスト

項番	動作	送信元 IP アドレス	宛先 IP アドレス
1	許可	10.100.1.0/24	172.16.100.0/24
2	許可	10.100.2.0/24	172.16.101.0/24
3	許可	10.100.3.0/24	172.16.102.0/24

注記 1　アクセスリストは，項番が小さい順に参照され，最初に該当したルールが適用される。
注記 2　どのルールにも該当しないものは禁止される。

表 3 のアクセスリストは，VPN-PC からの不正な通信を禁止する。その通信は，VPN-PC から，その VPN-PC と関係がない顧客システム構築ネットワークへのアクセスである。

H 社では，S さんの検討結果を踏まえて SSL-VPN の導入を行った。その結果，社内 PC からも顧客 PC からも安全にアクセスできる，利便性が高い顧客システム構築ネットワークが実現した。

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　〔顧客システム構築業務の問題とその解決策〕について，(1)～(3)に答えよ。

(1) 本文中の下線（Ⅰ）について，2種類の暗号アルゴリズムと1種類のハッシュアルゴリズムのそれぞれの用途を答えよ。

(2) 本文中の下線（Ⅱ）について，判断の根拠となった，H社が構築する顧客システムの特徴を，30字以内で述べよ。

(3) 本文中の下線（Ⅲ）について，割り当てられたIPアドレスは，PCのどのネットワークインタフェースに設定されるか。図2中の字句を用いて答えよ。

設問3　表1中の［　カ　］～［　ケ　］に入れる適切な字句を答えよ。

設問4　〔問題1の解決策〕について，(1)～(3)に答えよ。

(1) 本文中の下線（Ⅳ）について，表2のアクセスリストを設定すべきインタフェースを，図2中の①～⑥の記号で全て答えよ。ここで，アクセスリストはインタフェースの入力方向に設定するものとする。

(2) 本文中の下線（Ⅴ）について，禁止される通信は何か。本文中の字句を用いて，45字以内で答えよ。

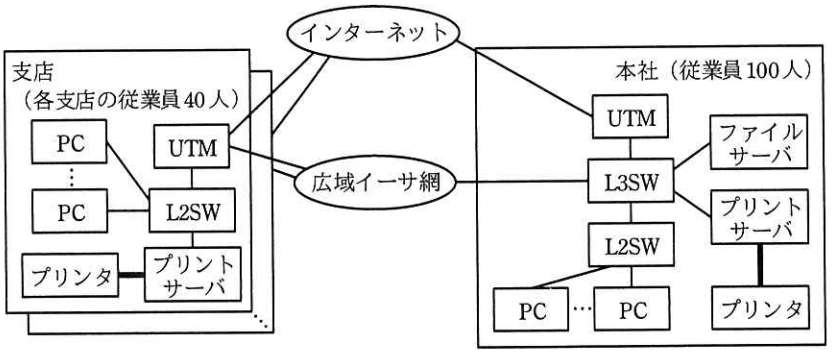
(3) 本文中の下線（Ⅵ）について，表3のアクセスリストを設定すべきインタフェースを，図2中の①～⑥の記号で答えよ。ここで，アクセスリストはインタフェースの入力方向に設定するものとする。

問2　仮想デスクトップ基盤の導入に関する次の記述を読んで，設問1～4に答えよ。

T社は，従業員数500人の建設会社で，全国10か所に支店がある。T社では，従業員1人にPC 1台を貸与し，従業員は設計業務や電子メール（以下，メールという），Webサイトの閲覧などにPCを活用している。現在，各従業員のPC内のハードディスクには，T社の秘密情報を含む書類が保存されている。そこで，T社では，情報セキュリティ強化を図るために，仮想デスクトップ基盤（以下，VDIという）を導入することを決めた。そのための事前調査，検討から設計までを情報システム部のUさんが担当することになった。

〔現行ネットワークの概要〕

T社の現行ネットワーク構成を図1に示す。



L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ　UTM：Unified Threat Management
広域イーサ網：広域イーサネットサービス網
注記1　L2SW，L3SW，UTMは，全てのポートがギガビットイーサネットである。
注記2　プリンタとプリントサーバは，USBケーブルで接続されている。

図1　T社の現行ネットワーク構成（抜粋）

各拠点は広域イーサ網で接続されており，アクセス回線の契約帯域は，本社が1Gビット／秒，各支店が100Mビット／秒である。インターネット接続回線は，拠点ごとに契約しており，契約帯域は本社が100Mビット／秒，各支店が40Mビット／秒である。

現行ネットワークでは，次の3種類の通信が行われる。

(1)　ファイル転送通信

・設計資料の共有，バックアップのために，PCがファイルサーバと通信を行う。

・ピーク時に必要な帯域は，本社従業員向けに 200 M ビット／秒，全ての支店従業員向けの合計が 800M ビット／秒である。

(2) プリント通信

・設計資料の印刷のために，PC から自拠点に設置しているプリントサーバに印刷データを送信する。

・印刷量は拠点によって異なるので，必要な帯域は把握していない。PC からプリントサーバに印刷データを送信したときは，①一時的に大量の帯域を使用する。

(3) インターネット通信

・インターネット上の Web サイトの閲覧，ISP が提供するメールサービスの利用のために，PC が Web サーバ，メールサーバと通信を行う。

〔VDI の事前調査〕

U さんは，PC 単位のプログラム実行環境（以下，仮想 PC という）をソフトウェアで実現する VDI と，従業員が仮想 PC を操作するために使うシンクライアント（以下，TC という）について調査した。調査結果は次のとおりである。

(1) VDI を実現する装置とその関連装置

・VDI サーバ：VDI を組み込んだサーバ

・TC：ハードディスクなどの情報蓄積機能がない PC

(2) VDI の動作概要

・VDI は，VDI サーバ上に仮想 PC を TC と 1 対 1 で生成する。そのとき，VDI は仮想 PC に対して IP アドレスを動的に割り当てる。

・VDI は，VDI サーバ上に仮想スイッチ（以下，仮想 SW という）を生成する。仮想 PC は仮想 SW との接続によって，外部との通信が可能になる。

・仮想 SW は，外部接続用のポートに VDI サーバの物理 NIC（Network Interface Card）を使用する。

(3) 仮想 PC から行われる通信

・画面転送通信：仮想 PC の画面を TC に転送する。TC 1 台が使用する帯域は，最大 200k ビット／秒である。

・ファイル転送通信，プリント通信及びインターネット通信：使用帯域は，現行と同じである。

〔SSL 可視化装置・標的型攻撃対策装置の導入〕

U さんは，T 社のサイバーセキュリティ対策の一環として，VDI とともに SSL 可視化装置と標的型攻撃対策装置を導入して情報セキュリティ強化を図ることにした。そのために U さんが選定した装置は，次のとおりである。

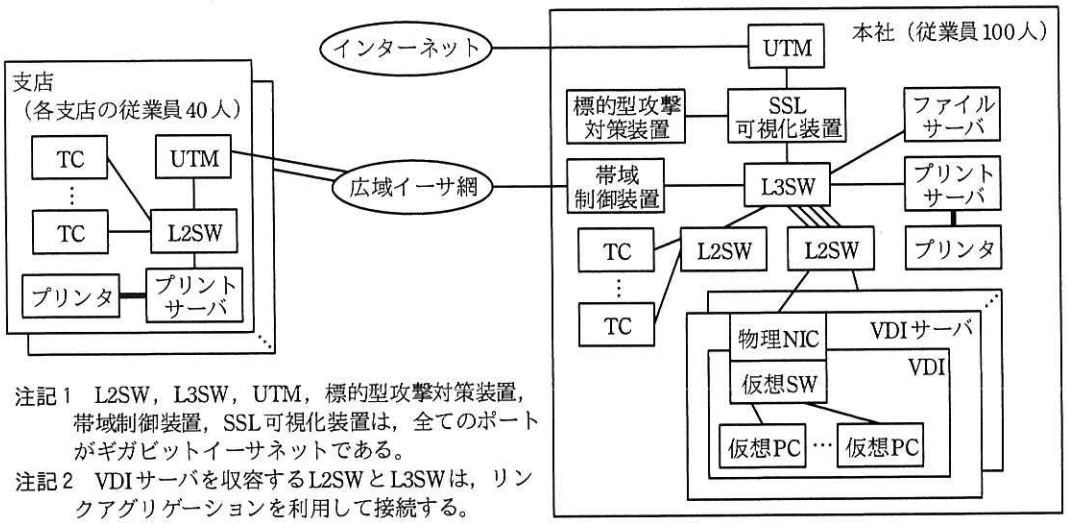
・SSL 可視化装置：平文で行われる通信だけでなく，SSL/TLS による暗号化通信も監視するために，暗号化通信の復号，復号した通信データを標的型攻撃対策装置に転送，復号した通信データを再度暗号化する装置

・標的型攻撃対策装置：マルウェアに感染した仮想 PC がインターネット上の C&C（Command & Control）サーバと行う不正通信を検知し，C&C サーバの IP アドレスを特定する装置

〔ネットワーク構成の検討〕

(1) VDI 導入後のネットワーク構成案

U さんは，これらの事前調査の結果から，VDI サーバなどの装置を本社に設置することにした。U さんが考えた VDI 導入後のネットワーク構成案を，図 2 に示す。



注記 1　L2SW，L3SW，UTM，標的型攻撃対策装置，帯域制御装置，SSL可視化装置は，全てのポートがギガビットイーサネットである。

注記 2　VDIサーバを収容するL2SWとL3SWは，リンクアグリゲーションを利用して接続する。

図 2　VDI 導入後のネットワーク構成案（抜粋）

VDI 導入後は，<u>②支店のインターネット接続回線を廃止し</u>，本社のインターネット接続回線の契約帯域を 1G ビット／秒に変更する。

(2) VDI 導入後の広域イーサ網

③本社と支店間の広域イーサ網を経由する通信は，VDI の導入で変化する。U さんは，広域イーサ網のアクセス回線の契約帯域について，次のとおり整理した。

・現行のアクセス回線の安全率は，“アクセス回線の契約帯域÷ピーク時に必要な帯域＝ [a] ”である。VDI 導入後も現行の安全率を確保する。

・全従業員が同時に仮想 PC を利用しても，TC の操作に遅れが発生しないようにするためには，画面転送通信の帯域を確保する必要がある。

・印刷量を把握できないプリント通信の帯域は確保しない。

・VDI の導入でアクセス回線の契約帯域を下げることができる。契約帯域は現行の安全率を考慮した最低限必要な帯域とし，本社は [b] M ビット／秒，各支店は [c] M ビット／秒に変更する。

・プリント通信も広域イーサ網を経由するので，本社から広域イーサ網方向の通信に対して，帯域制御が必要になる。

〔帯域制御の設計〕

(1) 帯域制御装置の機能

U さんは，ネットワークセグメントの構成変更が不要で，帯域制御を行うことができる帯域制御装置の導入を決めた。U さんが選定した装置の機能は，次のとおりである。

・パケットを送出するときに，支店ごとに二つの制御（分類制御，送出制御）が可能である。

・分類制御では，IP アドレス，ポート番号などでパケットを分類し，グループ化する。グループ化の単位をクラスとし，クラス単位でキューを割り当て，パケットを格納する。

・送出制御では，クラス単位の帯域確保の制御と，同一支店への複数クラスのパケットに対するシェーピングが可能である。

(2) 帯域制御方式の設計

装置の機能を踏まえ，U さんが考えた帯域制御方式の設計は，次のとおりである。

・最初にパケットは，IP アドレスで宛先の支店が決定され，支店ごとに設定した分類制御，送出制御に送られる。

・分類制御では，画面転送通信のクラスとそれ以外の通信のクラスを定義する。

各クラスへのパケットの分類は，ポート番号で識別して行う。

・送出制御では，④画面転送通信のクラスに，各支店の従業員が同時に仮想 PC を利用するときに，最低限必要な帯域を確保する設定を行う。

・それ以外の通信のクラスでは，帯域確保の制御を行わない。このクラスに分類されたパケットは，帯域が空いているときにだけ送出される。

・⑤シェーピングの設定は，各支店における広域イーサ網のアクセス回線の契約帯域とする。

〔仮想 PC のマルウェア感染時の対応〕

仮想 PC に感染したマルウェアは，別の仮想 PC に感染拡大を試みる場合がある。仮想 PC では物理的に LAN ケーブルを抜くことができないので，従来の対処方法は利用できない。そこで，U さんが考えた対策案は，次のとおりである。

・ある仮想 PC で，ウイルス対策ソフトがマルウェアの感染を検知したときは，情報セキュリティ管理者がその仮想 PC を隔離すべきか否かを判断する。隔離するときは，VDI のコンソールを使って，その仮想 PC を［　ア　］から切り離す。

・標的型攻撃対策装置が，ある仮想 PC の通信から C&C サーバの IP アドレスを特定したときは，本社の UTM にフィルタリングを設定する。被害の拡大を防ぐために，他の仮想 PC も含めて C&C サーバと通信を行うことを防ぐ必要があるので，“送信元＝［　イ　］，宛先＝［　ウ　］，ポート番号＝任意，動作＝拒否”のフィルタリングルールを設定し，インターネット方向の通信を遮断する。

その後，VDI の導入に関する U さんの報告書は企画会議で承認され，導入の準備を開始した。

設問 1　本文中の下線①の現象を引き起こすトラフィックを何というか。15 字以内で答えよ。

設問 2　〔ネットワーク構成の検討〕について，(1)～(3) に答えよ。

(1)　本文中の下線③について，VDI 導入前に広域イーサ網を経由する通信を一つ，VDI 導入後に経由する通信を二つ，本文中の通信名を用いてそれぞれ答えよ。

(2) 本文中の［ a ］～［ c ］に入れる適切な数値を求めよ。

(3) 本文中の下線②について，インターネット接続回線を廃止する理由を，インターネット通信に着目して 30 字以内で述べよ。また，現行ネットワーク構成と比べたときの情報セキュリティ対策上の利点を 30 字以内で述べよ。

設問３　〔帯域制御の設計〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，帯域確保の設定を行わなかった場合，TC の操作性が悪化することが懸念される。TC の操作性が悪化する原因を，プリント通信の特性に着目して 25 字以内で述べよ。

(2) 本文中の下線⑤について，本社から各支店方向の通信の帯域が，各支店のアクセス回線の契約帯域を超過したときに，帯域制御装置がパケットに対して行う制御の内容を，15 字以内で述べよ。

設問４　本文中の［ ア ］～［ ウ ］に入れる適切な字句を答えよ。

問３　社内ネットワークとクラウドサービスとのネットワーク接続に関する次の記述を読んで，設問 1～4 に答えよ。

K 社は，中堅の加工食品販売会社である。K 社では，幾つかあるシステムのうち，販売管理システムを更改する予定である。販売管理システムは，K 社製品の在庫の管理，販売計画及び販売実績の管理に使用されている。

〔クラウドサービスとのネットワーク接続の検討〕

販売管理システムの更改に当たって発足したプロジェクトチームが検討を進めた結果，L 社が提供しているクラウドサービス（以下，L 社クラウドサービスという）を利用する案が有力視されている。そこで，L 社クラウドサービスを試験的に利用して評価することになった。プロジェクトチームの O さんが，K 社ネットワーク（以下，K 社 NW という）と L 社クラウドサービスとのネットワーク接続を担当することになった。L 社クラウドサービスのサービス仕様に従って O さんが考えた，L 社クラウドサービスとのネットワーク接続構成を図 1 に示す。

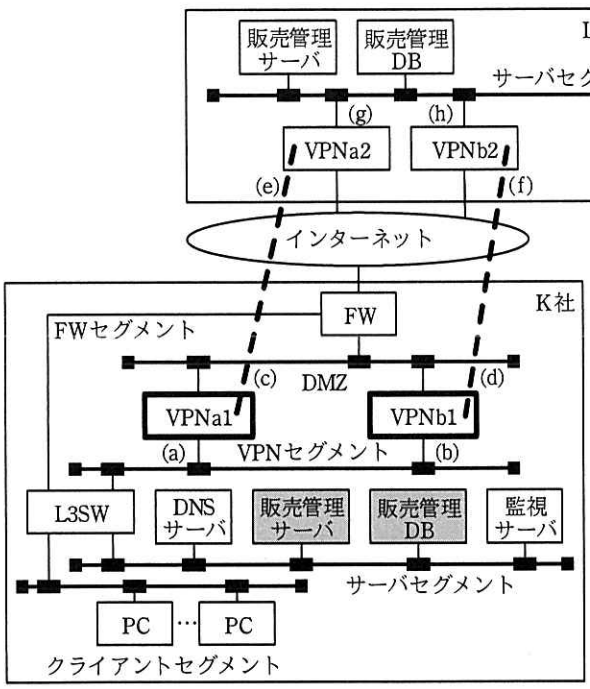


図１　L 社クラウドサービスとのネットワーク接続構成（抜粋）

図 1 の L 社クラウドサービスとのネットワーク接続構成の概要は，次のとおりである。

・L3SW に VPN セグメントを作成する。VPN ルータとして VPNa1 と VPNb1 を新たに設置し，DMZ と VPN セグメントに接続する。
・VPNa1 は VPNa2 との間に，VPNb1 は VPNb2 との間に，VPN トンネルを構成する。
・VPN トンネルは，VPNa1 側をアクティブ，VPNb1 側をスタンバイとする。
・VPNa1，VPNb1 及び L3SW の間では OSPF で経路情報の交換を行う。
・L 社クラウドサービス内では，評価のために，販売管理サーバと販売管理 DB を構築し，K 社 NW のクライアントセグメントから利用できるようにする。
・K 社 NW のクライアントセグメントの PC 及びサーバセグメントのサーバには，L3SW をデフォルトゲートウェイとして設定する。また，L3SW には，FW をデフォルトゲートウェイとして設定する。
・K 社 NW の PC とサーバには，プライベート IP アドレスを割り当てる。PC 及びサーバからインターネットへの Web 閲覧などの通信は，FW で IP アドレスとポート番号の変換処理である［　ア　］を行う。

〔インターネット VPN 接続の検討〕

L 社クラウドサービスの VPN ルータと K 社 NW の VPN ルータでは，互いのグローバル IP アドレスを利用して，RFC 1853 に記載されている IP in IP を用いて，トンネルが構成される。このトンネルの通信を，IPsec を用いて暗号化する。

暗号化は，フェーズ 1 と呼ばれる IKE SA の確立，フェーズ 2 と呼ばれる IPsec SA の確立を経て行われる。

フェーズ 1 では，接続する相手を認証する方式として，両方の機器であらかじめ，［　イ　］と呼ばれる同じ鍵を共有する方式を利用する。

フェーズ 2 では，①IP ヘッダを暗号化対象とするトンネルモードではなく，IP ヘッダを暗号化対象としないトランスポートモードを選択する。

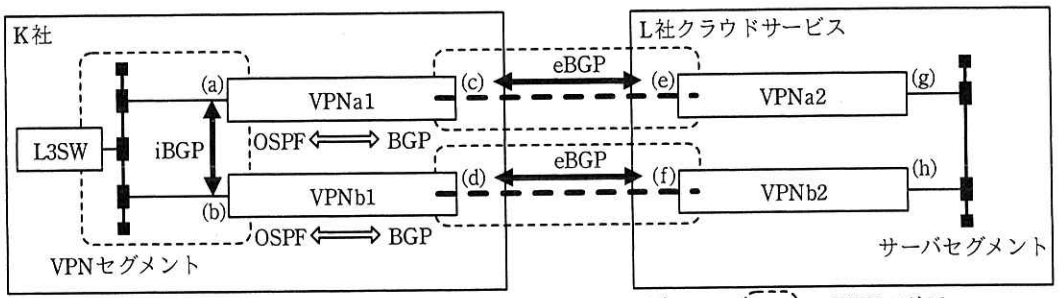
IP in IP でトンネルを構成し，更に IPsec を用いて暗号化することによって，②元の IP パケットと比較してパケットサイズは大きくなる。そこで，IP in IP で作成されたトンネルインタフェースでは MTU のサイズを適切な値に設定し，さらに，トンネルインタフェースを通過するパケットの TCP MSS（Maximum Segment Size）を適切

な値に書き換える。

〔K社NWとL社クラウドサービスとの経路情報の交換の検討〕

L社クラウドサービスとのネットワーク接続では，静的経路制御，又はBGPを用いた動的経路制御を選択できる。Oさんは，③BGPを用いた動的経路制御を選択した。

Oさんが考えた，K社NWとL社クラウドサービスとの経路情報の交換の概要を図2に示す。



注記1　太い破線は，VPNトンネルを示す。

注記2　(a)～(h)は，VPNルータに割り当てたプライベートIPアドレスを示す。

図2　K社NWとL社クラウドサービスとの経路情報の交換の概要

BGPはルーティングプロトコルの一つであり，特定のルーティングポリシで管理されたルータの集まりを示す［ウ］の間で，経路情報の交換を行うために開発されたプロトコルである。

BGP接続を行う2台のルータ間ではトランスポートプロトコルの一つである［エ］のポート179番を使用し，経路情報の交換を行う。このコネクションのことをBGPピアと呼ぶ。

［ウ］を識別する番号として，VPNa1とVPNb1では65505を使用し，VPNa2とVPNb2ではL社クラウドサービスが割当てを受けている64496を使用する。

VPNa1とVPNa2間及びVPNb1とVPNb2間ではeBGPピアを設定し，VPNa1とVPNb1間ではiBGPピアを設定する。

VPNa2とVPNb2は，それぞれVPNa1とVPNb1に対し，L社クラウドサービス内のサーバセグメントの経路だけBGPで経路広告する。

K 社 NW の VPN セグメントと接続する VPNa1，VPNb1 及び L3SW の各インタフェースでは OSPF のエリア 0 を構成し経路情報の交換を行う。さらに，IP in IP で作成されたトンネルインタフェースでは，OSPF のエリア 0 を構成するが，④経路情報の交換を行う必要がないのでパッシブインタフェースとする。

VPNa1 と VPNb1 では，OSPF と BGP の間で経路情報の再配布を行う。

O さんは，VPNa1 側をアクティブ，VPNb1 側をスタンバイとする構成について，I 主任に相談した。次は，そのときの O さんと I 主任の会話である。

O さん：VPN の経路設計で，VPNa1 側をアクティブ，VPNb1 側をスタンバイとしたいのですが，どのように設計したらよいでしょうか。

I 主任 ：通信の方向それぞれについて経路設計をする必要があります。まずは，社内から L 社クラウドサービスの方向は，L 社クラウドサービスを利用する PC からのパケットは全て L3SW に届くので，L3SW がパケットの転送先として，VPNa1 と VPNb1 のどちらを選択するか，転送先を決められるようにすればよいです。

O さん：VPNa1 と VPNb1 が，BGP で受けた経路情報を OSPF に再配布する際に，異なるコストを付与すると転送先を選択できそうですね。VPNb1 側のコストを VPNa1 側と比べて［ A ］します。

I 主任 ：次に，L 社クラウドサービスから社内の方向はどうでしょう。L 社クラウドサービスは，どのような BGP のパスアトリビュートをサポートしていますか。

O さん：MED と AS_PATH を利用できます。今回は AS_PATH を使おうと考えています。AS_PATH では，AS_PATH 長が短い方が選択されます。

I 主任 ：そうですね。そういえば，一点注意が必要です。経路情報の再配布を行うときには，経路のループを防止しなければいけません。

O さん：分かりました。⑤経路のループを防止する経路制御を行います。

〔ネットワーク監視の検討〕

K 社 NW のサーバセグメントには，ネットワーク及びサーバが正常かどうかを確認するために監視サーバを設置している。監視には ping を用いる。ping は，

［ オ ］の echo request パケットを監視対象に送り，［ カ ］パケットが監視対象から返ってくることで到達性を確認する。⑥二つある VPN トンネルがそれぞれ正常に動作しているかを常に確認するために，監視対象として(e)と(f)を選択した。実際に，VPN ルータを停止するテスト，及び VPN トンネルを切断するテストを行い，正しく検知できることを確認した。

O さんは，これまでの結果をまとめて，プロジェクトに報告した。その後，L 社クラウドサービスの試験利用の評価を行った。その結果は良好で，K 社では L 社クラウドサービスを利用した販売管理システムの更改が決定された。また，K 社内のその他のシステムも順次，L 社クラウドサービスへ移行する計画が立てられた。

設問 1　本文中の［ ア ］～［ カ ］に入れる適切な字句を答えよ。

設問 2　〔インターネット VPN 接続の検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線①について，今回の構成では，トランスポートモードを選択している。選択した根拠を，IP アドレスに着目して 30 字以内で述べよ。

(2) 本文中の下線②について，IP in IP で作成されたトンネルインタフェースの MTU の値を 1,500 とした場合，VPN ルータで発生する処理を，30 字以内で述べよ。ここで，インターネットを含む全てのインタフェースの MTU の値を 1,500 とする。

設問 3　〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕について，(1)～(4) に答えよ。

(1) 本文中の下線③について，静的経路制御と比較して動的経路制御を選択した利点を 40 字以内で述べよ。

(2) 本文中の下線④について，パッシブインタフェースの動作の特徴を，20 字以内で述べよ。

(3) 本文中の［ A ］に入れる適切な字句を答えよ。

(4) 本文中の下線⑤について，経路のループを防止するために必要な経路制御を 40 字以内で述べよ。

設問 4　本文中の下線⑥について，二つある VPN トンネルをそれぞれ監視する目的を 35 字以内で述べよ。

〔 メ モ 用 紙 〕

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	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。