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。

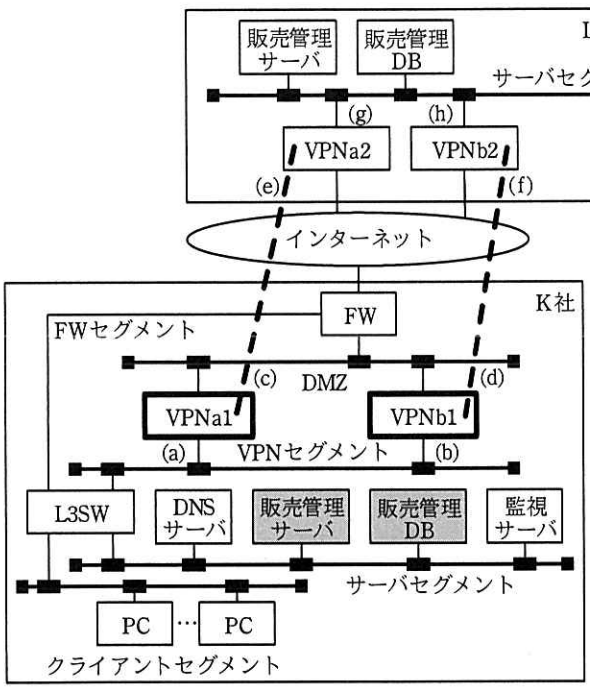


図１　L 社クラウドサービスとのネットワーク接続構成（抜粋）

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。

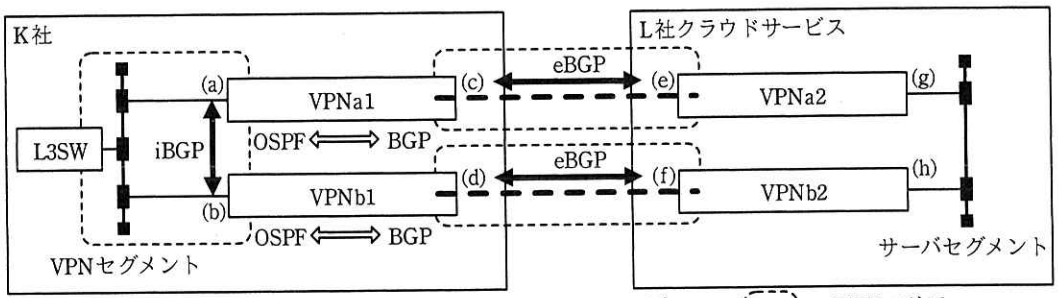
IP in IP でトンネルを構成し，更に IPsec を用いて暗号化することによって，②元の IP パケットと比較してパケットサイズは大きくなる。そこで，IP in IP で作成されたトンネルインタフェースでは MTU のサイズを適切な値に設定し，さらに，トンネルインタフェースを通過するパケットの TCP MSS（Maximum Segment Size）を適切

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。