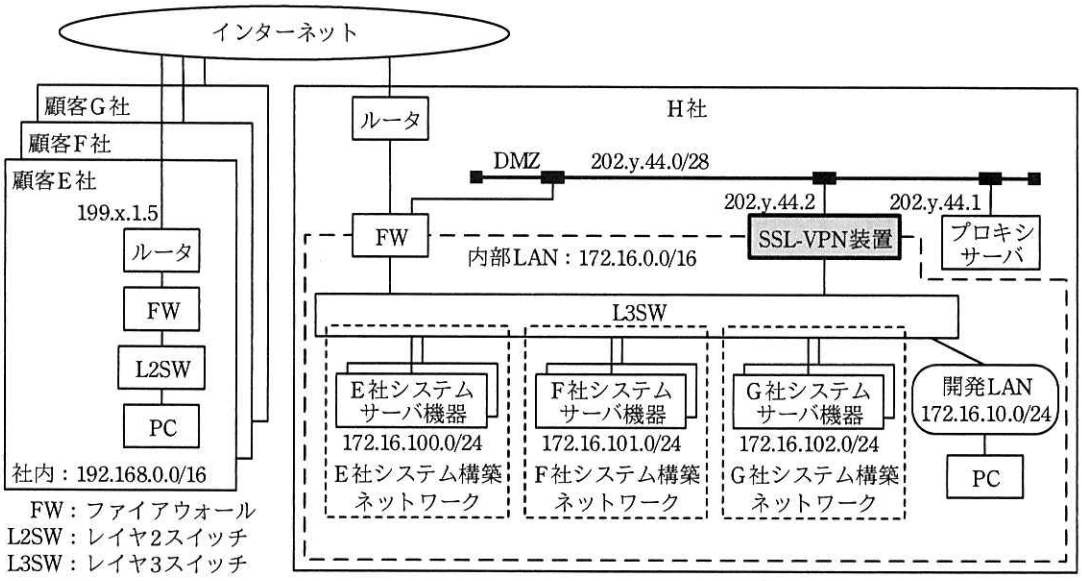
問１　SSL-VPN の導入に関する次の記述を読んで，設問 1～4 に答えよ。

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

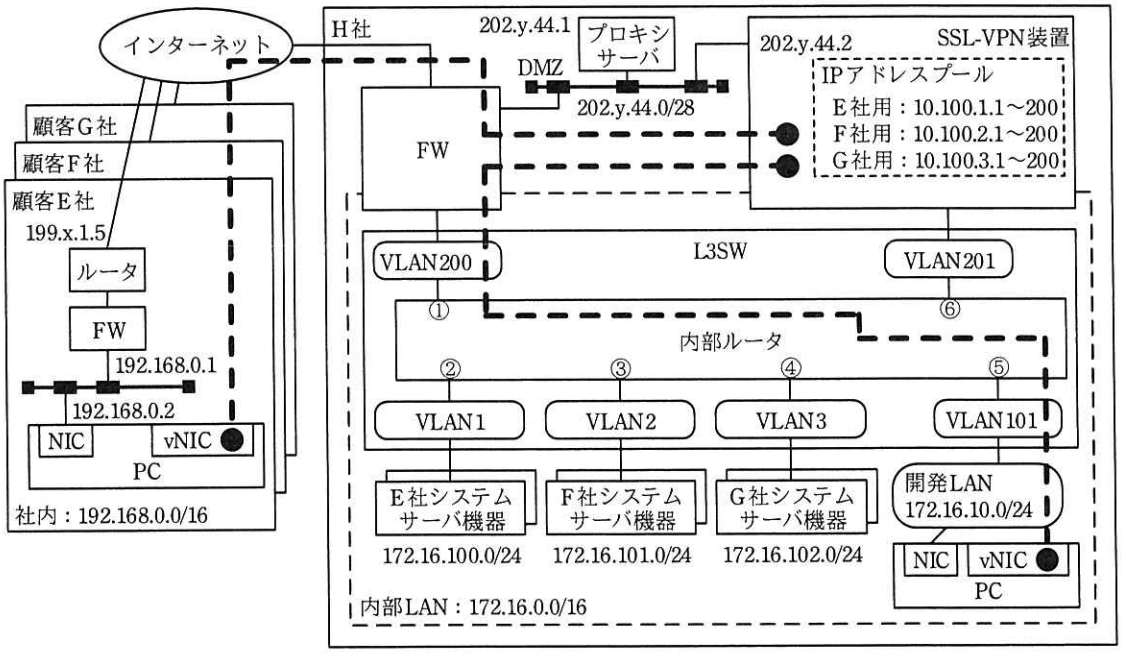
SSL-VPN導入後のFWのルールは，表1のとおり設定する。

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。