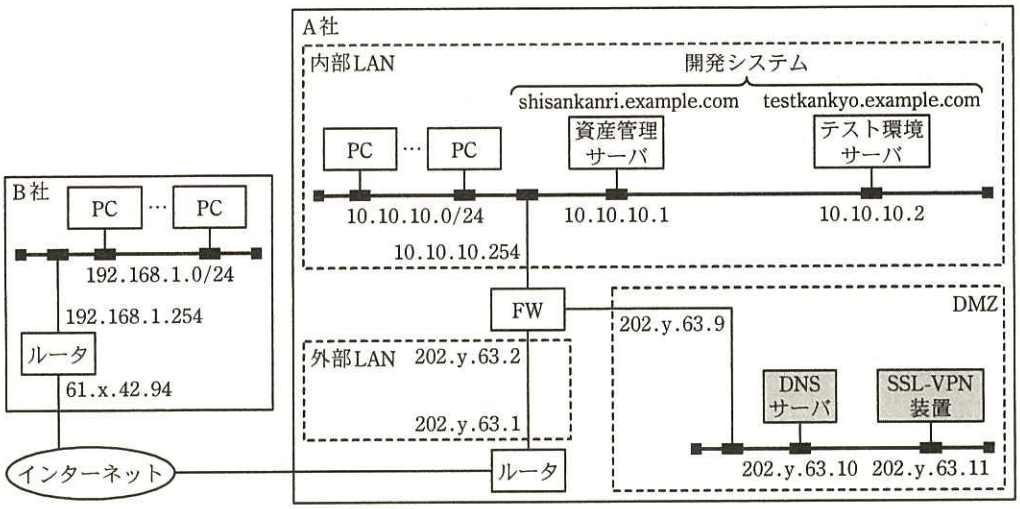
問1　リモート接続ネットワークの検討に関する次の記述を読んで，設問 1～4 に答えよ。

A 社は，従業員数 100 人のソフトウェア開発会社であり，開発の一部を関連会社である B 社に委託している。従来，B 社の開発者は，仕様書を自社に持ち帰って作業を行っていたが，このたび，情報保護，品質管理及び進捗管理の強化のために，A 社の開発システムを，インターネット経由で B 社にも利用してもらうことにした。

A 社の情報システム部の M 課長は，ネットワーク担当の N 君に対し，ネットワーク構成とその運用を検討するように指示した。B 社からの接続を可能にするために N 君が考えた，新ネットワークの構成を，図 1 に示す。



FW：ファイアウォール

注記 1　網掛け部分は，B 社からの接続を可能にするために追加した機器を示す。

注記 2　61.x.42.94，202.y.63.1 などの表記は，グローバル IP アドレスを示す。

図 1　新ネットワークの構成（抜粋）

開発システムは，設計書やソフトウェアモジュールなどを管理する資産管理サーバ，及びテストを行うためのテスト環境サーバから構成されている。A 社の情報システム部がまとめた，ネットワーク要件を次に示す。

・B 社の開発者は，B 社の自席 PC のブラウザからインターネット経由で A 社の開発システムを利用する。

・B 社のネットワークの変更は，最小限に抑える。

・A 社の FW で，DMZ と内部 LAN へは必要なパケットだけを通すようにする。
・A 社と B 社間の通信は暗号化する。
・サーバと PC は，ともに電子証明書を使った認証を行う。
・サーバの電子証明書は，信頼できる機関から発行されたものを利用する。
・B 社の PC からのウイルスによる感染や情報漏えいを防止する。

〔リモート接続ネットワーク構成の検討〕

N 君はまず，現状の B 社のネットワークを変更せず，既存の PC のブラウザから開発システムを利用するために，SSL-VPN を採用した。さらに，N 君は，B 社の開発者に，クライアント証明書を格納した USB デバイス（以下，トークンという）を貸与することによって不正アクセス防止を図ることにした。

SSL には，PC と SSL-VPN 装置間において，SSL セッションを確立させるためのハンドシェイクプロトコルが規定されている。ハンドシェイクプロトコルでは，［ア］メッセージによって暗号化アルゴリズムを決定し，公開鍵による電子証明書の確認後，共通鍵での暗号化と，メッセージ認証コードのチェックを行い，SSL セッションを確立する。

次に，N 君は，PC と SSL-VPN 装置の通信に SSL トンネルを利用するポートフォワード方式を採用した。

ポートフォワード方式の場合，PC から SSL-VPN 装置に接続したときに認証が行われ，SSL-VPN 装置から PC に Java アプレットがダウンロードされ，SSL トンネルが確立される。また，Java アプレットによって，PC の hosts ファイルに，ループバックアドレスと開発システムの各サーバの宛先を対応させた定義が追加される。①ループバックアドレスの利用は，社内で使用中のプライベートアドレスを利用するよりも利点があり，127.0.0.1 ～［イ］の範囲内で利用可能である。

N 君は，ループバックアドレス 127.0.1.10 を資産管理サーバの［ウ］に対応付けるように設計したので，Java アプレットは，“127.0.1.10 shisankanri.example.com”という定義を hosts ファイルに追加し，事前に指定したポート番号で待ち受ける。

N 君が設計した，B 社の PC から開発システムへの接続概念図を，図 2 に示す。

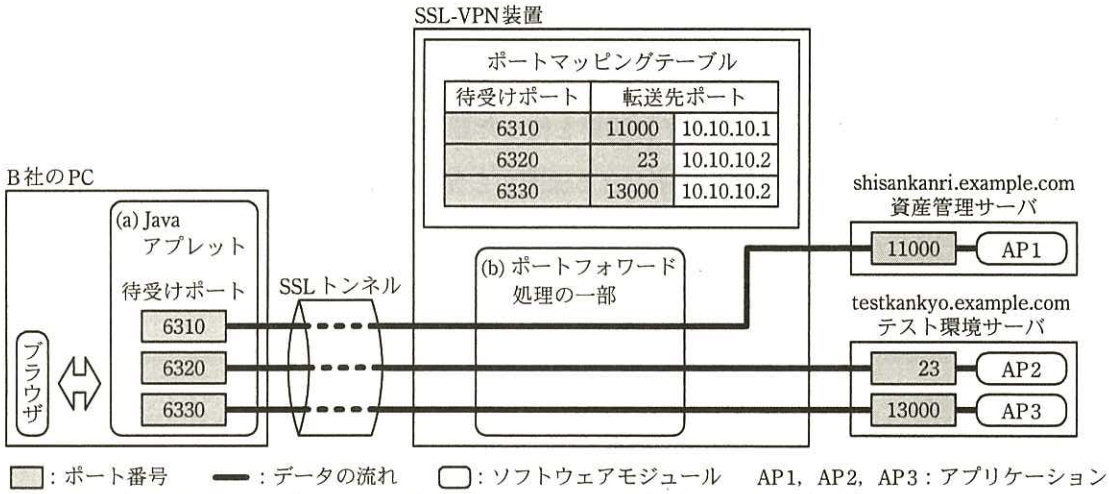


図2　B社のPCから開発システムへの接続概念図（抜粋）

B社のPCでは，図2中で示した(a)において，Javaアプレットが事前に指定したポート番号で待ち受け，B社の開発者がPCのブラウザに表示されたメニューの中からアプリケーション名を選択することで，SSLトンネルを経由してSSL-VPN装置へアクセスしデータを送る。SSL-VPN装置では，図2中で示した(b)において，ソフトウェアモジュールがポートマッピングテーブルを参照して，待受けポートとプライベートアドレスに対応する転送先ポートへデータを送る。② この方式では，使用できないアプリケーションが発生するが，今回の開発システムでは問題がないことをN君は確認した。また，SSL-VPN装置のログアウト時に，Javaアプレットがhostsファイルを編集前の設定に戻すことも確認した。さらに，N君は，開発作業のピーク時に開発システムの利用頻度が増大することを考慮し，③ SSL-VPN装置において，SSLセッションのキャッシュ時間を延ばす設定を行うことにした。

N君は，図1と図2を基に，FWの通信を許可する追加設定を，表1にまとめた。

表1　FWの通信を許可する追加設定（抜粋）

アクセス経路	送信元IPアドレス	宛先IPアドレス	宛先ポート番号	備考
外部LAN → DMZ	任意	オ	53	
外部LAN → DMZ	61.x.42.94	202.y.63.11	カ	
⋮				
DMZ → 内部LAN	キ	10.10.10.1	11000	AP1用
DMZ → 内部LAN	ク	10.10.10.2	23	AP2用
DMZ → 内部LAN	ケ	10.10.10.2	13000	AP3用

〔リモート接続ネットワークの運用の検討〕

N 君は，リモート接続ネットワークの運用の検討を行った。サーバ証明書の正当性は，証明書が，信頼できる認証機関である［　エ　］から発行されていることを，PC 側で検証することで確認される。また，B 社の PC 側の利用者の正当性は，トークンに格納されたクライアント証明書で確認される。今回，A 社では，独自にクライアント証明書を発行するとともに，クライアント証明書を管理する運用担当者を選定することにした。N 君は，④クライアント証明書の管理に必要な情報を，運用担当者に自動的に通知する仕組みを作ることにした。さらに，N 君は，B 社内の PC から A 社の開発システムを利用するときの，ウイルスによる感染や情報漏えいを防止する要件を満たすために，⑤SSL-VPN 装置へのログイン時とログアウト時に，Java アプレットがもつべき機能を調査し，問題がないことを確認した。

リモート接続ネットワークの基本構成が了承され，構築作業が開始された。

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　〔リモート接続ネットワーク構成の検討〕について，(1)～(4)に答えよ。

(1) 本文中の下線①について，ループバックアドレスを用いる利点を，セキュリティ面に着目して，20 字以内で述べよ。

(2) 本文中の下線②について，使用できないアプリケーションの通信の特徴を，図 2 に着目して，20 字以内で述べよ。

(3) 本文と図 2 の内容を基に，PC のブラウザから資産管理サーバの AP 1 への接続に際し，Java アプレットが受け付ける IP アドレスとポート番号を答えよ。また，そのときの Java アプレットと資産管理サーバとの間で確立される TCP コネクションを，図 2 中の名称を用いて二つ答えよ。

(4) 本文中の下線③について，設定の目的を，“SSL セッション”という字句を用いて，30 字以内で述べよ。

設問 3　表 1 中の［　オ　］～［　ケ　］に入れる適切な字句を答えよ。

設問 4　〔リモート接続ネットワークの運用の検討〕について，(1)，(2)に答えよ。

(1) 本文中の下線④の情報を，20 字以内で述べよ。

(2) 本文中の下線⑤の機能を，ログイン時とログアウト時のそれぞれについて，35 字以内で具体的に述べよ。