次の問1は必須問題です。必ず解答してください。

問1　テレワークの導入に関する次の記述を読んで，設問1～3に答えよ。

ソフトウェア開発会社である A 社では，従業員が働き方を柔軟に選択できるように，場所や時間の制約を受けずに働く勤務形態であるテレワークを導入することにした。

A 社には，事務業務だけが行える PC（以下，事務 PC という）と，事務業務及びソフトウェア開発業務が行える PC（以下，開発 PC という）がある。開発部の従業員は開発 PC を使用し，開発部以外の従業員は事務 PC を使用している。

A 社には事務室，開発室及びサーバ室があり，各部屋のネットワークはファイアウォール（以下，A 社 FW という）を介して接続されている。A 社のネットワーク構成を，図1に示す。

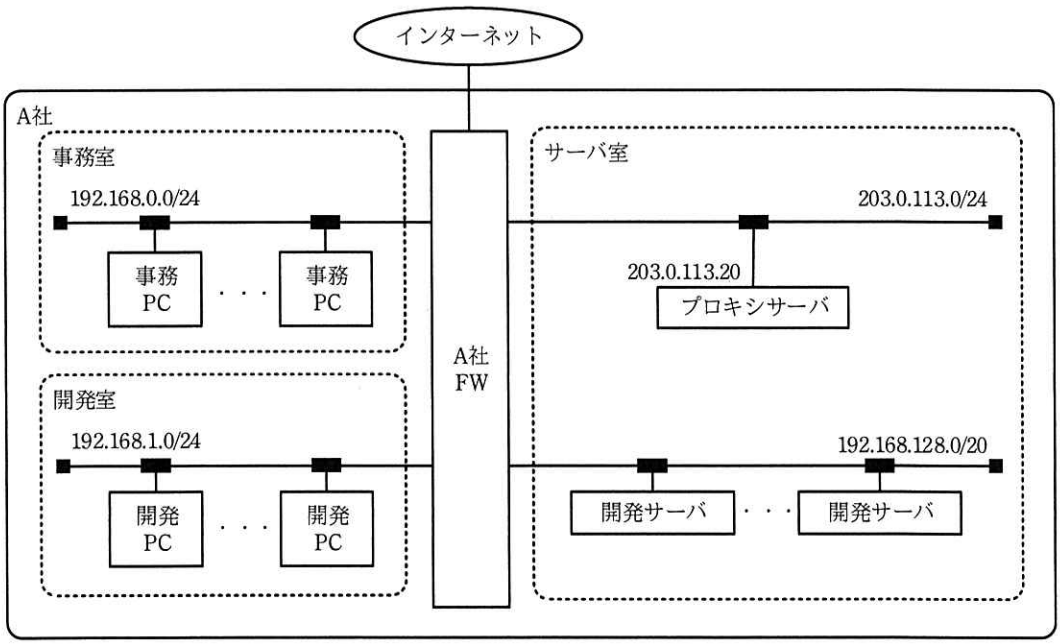

図1　A 社のネットワーク構成

事務室には，事務 PC だけが設置されている。開発室には開発 PC だけが設置されており，開発部の従業員だけが入退室できる。サーバ室には，プロキシサーバ 1 台と，ソフトウェア開発業務に必要なソースコード管理，バグ管理，テストなどに利用するサーバ（以下，開発サーバという）が複数台設置されている。

A 社 FW では，開発室のネットワークだけから開発サーバに HTTP over TLS（以下，HTTPS という）又は SSH でアクセスできるように通信を制限している。また，A 社ネットワークからのインターネットの Web サイト閲覧は，事務 PC 及び開発 PC だけからプロキシサーバを経由してできるように通信を制限している。

テレワークで働く従業員は，データを保存できないシンクライアント端末を A 社から支給され，遠隔からインターネットを経由して A 社のネットワークに接続し，業務を行う。そのために，安全に A 社のネットワークに接続する VPN，及び仮想マシンの画面を転送して遠隔から操作できるようにする画面転送型の仮想デスクトップ環境（以下，VDI という）の導入を検討した。テレワーク導入後の A 社のネットワーク構成案を，図 2 に示す。

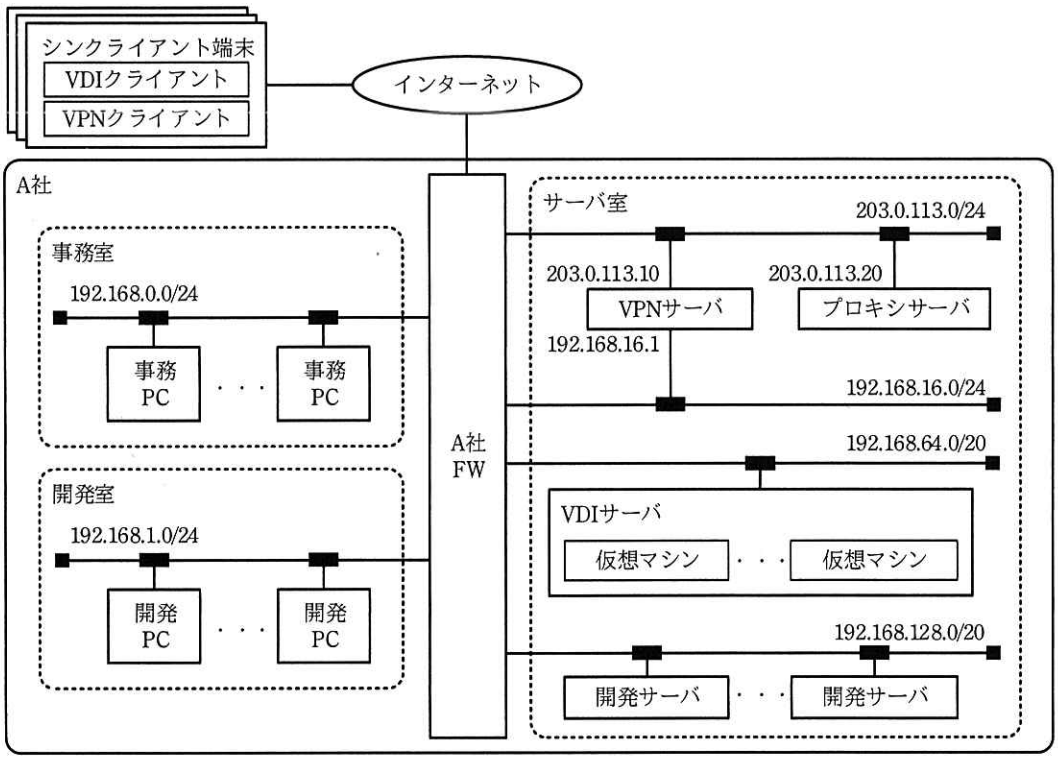

図 2　テレワーク導入後の A 社のネットワーク構成案

〔A社が検討したテレワークによる業務の開始までの流れ〕

(1) 利用者は，シンクライアント端末の VPN クライアントを起動して，VPN サーバに接続する。

(2) VPN サーバは，VPN クライアントが提示するクライアント証明書を検証する。検証に成功した場合，処理を継続する。

(3) VPN サーバは，利用者を認証する。認証が成功した場合，VPN クライアントに対して，192.168.16.0/24 の範囲で使用されていない IP アドレスを一つ選択して割り当てる。

(4) VPN クライアントは，(3)で割り当てられた IP アドレスを使用して，VPN サーバ経由でA社のネットワークに接続する。

(5) 利用者は，シンクライアント端末の VDI クライアントを起動して，VDI サーバに接続する。

(6) VDI サーバは，VPN サーバで認証された利用者が開発部以外の従業員であれば事務業務だけが行える仮想マシン（以下，事務 VM という）を，開発部の従業員であれば事務業務及びソフトウェア開発業務が行える仮想マシン（以下，開発 VM という）を割り当てる。また，VDI サーバは，事務 VM には 192.168.64.0/24，開発 VM には 192.168.65.0/24 の範囲で使用されていない IP アドレスを一つ選択して割り当てる。

(7) 利用者は，仮想マシンにログインして業務を開始する。VDI クライアントと仮想マシンとの間では，画面データ，並びにキーボード及びマウスの操作データだけが送受信される。

テレワーク導入後の A 社 FW に設定するパケットフィルタリングのルール案を，表1に示す。

表1　A社FWに設定するパケットフィルタリングのルール案

ルール番号	送信元	宛先	サービス	動作
1	インターネット	203.0.113.10	VPN	許可
2	203.0.113.20	インターネット	HTTP，HTTPS，DNS	許可
3	192.168.16.0/24	192.168.64.0/20	VDI	許可
4	192.168.0.0/23	203.0.113.20	プロキシ	許可
5	192.168.64.0/23	203.0.113.20	プロキシ	許可
6	192.168.1.0/24	192.168.128.0/20	HTTPS，SSH	許可
7	192.168.64.0/23	192.168.128.0/20	HTTPS，SSH	許可
8	全て	全て	全て	拒否

注記1　ルール番号の小さいものから順に，最初に一致したルールが適用される。
注記2　許可された通信に対する戻りのパケットは，無条件に許可される。

ところが，表1のルール案ではルール番号7の条件に誤りがあり，［　a　］ことが分かった。そこで，開発サーバに対するアクセスを正しく制限するために，ルール番号7の条件について，送信元を［　b　］に変更した。

設問1　本文中の［　　］に入れる適切な答えを，解答群の中から選べ。

aに関する解答群

ア　開発PCから開発サーバにアクセスできない
イ　開発VMから開発サーバにアクセスできない
ウ　事務PCから開発サーバにアクセスできる
エ　事務VMから開発サーバにアクセスできる

bに関する解答群

ア　192.168.0.0/24	イ　192.168.1.0/24	ウ　192.168.16.0/24
エ　192.168.64.0/24	オ　192.168.65.0/24	カ　192.168.128.0/20
キ　192.168.128.0/24	ク　203.0.113.0/24	ケ　インターネット

設問２　シンクライアント端末から開発サーバにアクセスするときの接続経路として適切な答えを，解答群の中から選べ。

解答群

ア　シンクライアント端末 → VDI サーバ → VPN サーバ → 開発 PC → 開発サーバ

イ　シンクライアント端末 → VDI サーバ → VPN サーバ → 開発 VM → 開発サーバ

ウ　シンクライアント端末 → VDI サーバ → 開発 VM → 開発 PC → 開発サーバ

エ　シンクライアント端末 → VPN サーバ → VDI サーバ → 開発 PC → 開発サーバ

オ　シンクライアント端末 → VPN サーバ → VDI サーバ → 開発 VM → 開発サーバ

カ　シンクライアント端末 → VPN サーバ → 開発 PC → 開発 VM → 開発サーバ

設問３　A 社がテレワークの検討を進める過程で，“常に同一の業務環境を使用できるように，テレワークで働くときだけでなく，事務 PC 及び開発 PC からも仮想マシンを使用したい”との要望が挙がった。検討した結果，この要望に応えてもセキュリティ上のリスクは変わらないと判断した。また，A 社のネットワーク内からアクセスするので VPN で接続する必要はなく，利用者認証を VPN サーバではなく VDI サーバで行えばよいことを確認した。

この要望に応えるとき，表 1 のルール案に必要な変更として適切な答えを，解答群の中から選べ。ここで，表 1 のルール番号 7 の送信元には，設問 1 で選択した適切な答えが設定されているものとする。

解答群

ア　変更する必要はない。

イ　ルール番号 3 と 4 の間に，送信元を 192.168.0.0/23，宛先を 192.168.64.0/20，サービスを VDI，及び動作を許可とするルールを新たに挿入する必要がある。

ウ　ルール番号 3 と 4 の間に，送信元を 192.168.64.0/23，宛先を 192.168.0.0/23，サービスを VDI，及び動作を許可とするルールを新たに挿入する必要がある。

エ　ルール番号 3 と 4 の間に，送信元をインターネット，宛先を 192.168.64.0/20，サービスを VDI，及び動作を許可とするルールを新たに挿入する必要がある。