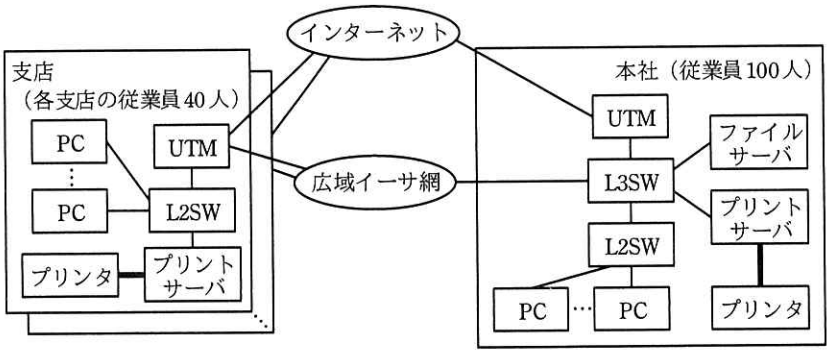
問2　仮想デスクトップ基盤の導入に関する次の記述を読んで，設問1～4に答えよ。

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 200 k 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。

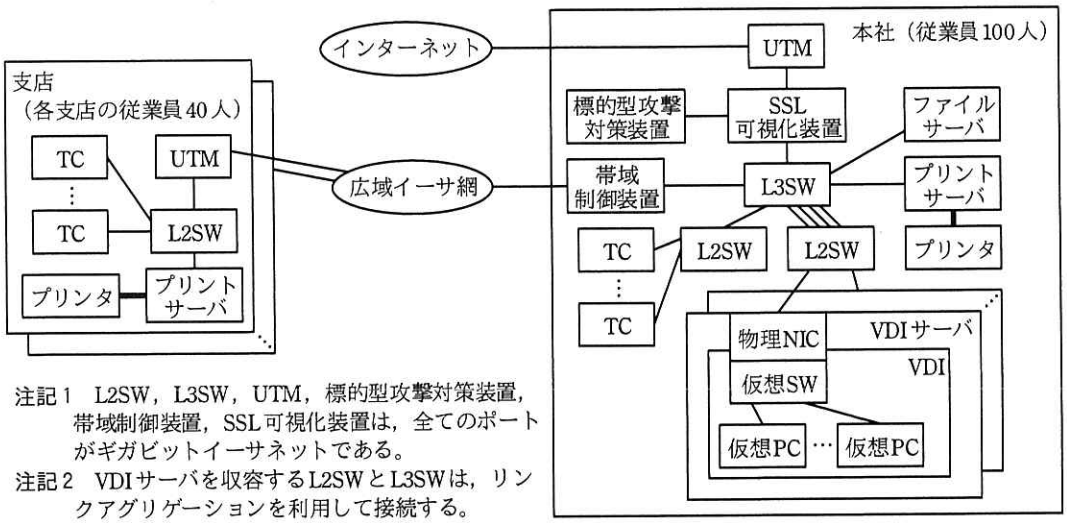
・SSL 可視化装置：平文で行われる通信だけでなく，SSL/TLS による暗号化通信も監視するために，暗号化通信の復号，復号した通信データを標的型攻撃対策装置に転送，復号した通信データを再度暗号化する装置

・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，②支店のインターネット接続回線を廃止し，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。