問１　ネットワークシステムの拡張に関する次の記述を読んで，設問１～５に答えよ。

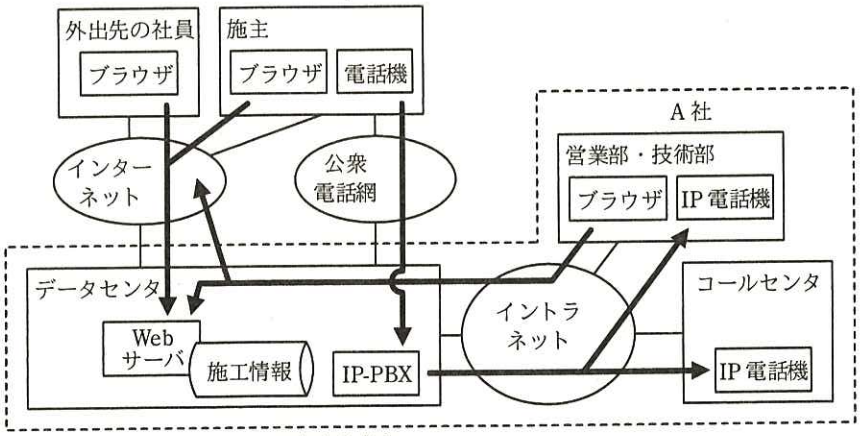
工務店の A 社は，全国規模で住宅や店舗の施工を請け負っている。施主への情報提供に力を入れており，次の三つの機能をもつ情報システムを稼働させている。

・施工情報管理：外出先又は社内にいる A 社の社員や施主が，タブレット端末や PC で動作する，Web ブラウザを使って，A 社データセンタの Web サーバが管理する施工情報に HTTPS プロトコルでアクセスする（以下，Web ブラウザと，Web ブラウザが動作しているタブレット端末や PC を，どちらもブラウザという）。

・コールセンタ：施主からの問合せ電話を，データセンタの IP-PBX を使って，A 社コールセンタのオペレータが受け付け，必要に応じて営業部や技術部へ転送する。

・インターネットアクセス：A 社の社員が，社内からブラウザを使ってインターネットにアクセスする。

A 社の現行情報システムの概要を図１に示す。



注記　→ は，アクセスの方向を表す。

図１　A 社の現行情報システムの概要

情報システム部は，現在，施主との情報連携を強化するために，ブラウザを活用した情報システムの機能拡張に取り組んでいる。ネットワーク担当の B 君が，ネットワークシステムに関する現行仕様の調査と，機能拡張に伴うネットワーク拡張計画の作成を行っている。

情報システムの機能拡張の構想を次に示す。

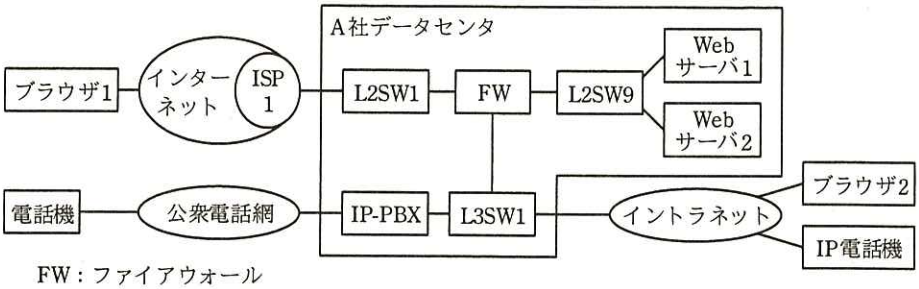
・マルチホーミング：今後，社外との通信が更に重要になるので，データセンタとインターネットとの接続を二重化する。

・ブラウザを使ったビデオ電話：施主と A 社の社員がブラウザを使って，施工状況などを動画で確認できるようにする。このビデオ電話はブラウザ上で動作するアプリケーション（以下，AP という）を A 社の Web サーバからダウンロードし，AP 間の通信によって実現する。

・ブラウザを使った音声電話：施主や外出先の A 社の社員がブラウザを使って，社内の A 社の社員と音声電話ができるようにする。この電話機能にもビデオ電話と同じ AP を使う。IP-PBX を介した，社外のブラウザ上で動作する AP と社内の IP 電話機との通信によって実現する。

〔現行ネットワーク構成〕

A 社の現行ネットワーク構成を図 2 に，図 2 中のスイッチに定義された現行 IP アドレス空間を表 1 に，それぞれ示す。



FW：ファイアウォール
ISP：インターネットサービスプロバイダ
L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ

図 2　A 社の現行ネットワーク構成（抜粋）

表 1　図 2 中のスイッチに定義された現行 IP アドレス空間

スイッチ	VLAN 名	IP アドレス空間	用途
L2SW1	vlan1	ip1/29 （ip1 はグローバル IP アドレス）	ISP1 接続
L2SW9	vlan9	10.0.9.0/24	DMZ
L3SW1	vlan8	10.0.8.0/24	FW 接続
	vlan7	10.0.7.0/24	IP-PBX 接続
	vlan6	10.0.6.0/24	イントラネット接続

B 君が調査した，A 社の現行ネットワークシステムの仕様を次に示す。

・図 2 中のブラウザ 1 が Web サーバ 1 と Web サーバ 2 へアクセスする際に，FW の NAT 機能が宛先 IP アドレスを変換する。変換前と変換後の宛先 IP アドレスは，それぞれ表 1 中の IP アドレス空間 [ア] と [イ] に属し，変換前と変換後の IP アドレスの組合せは 1：1 に固定されている（以下，宛先 NAT という）。

・図 2 中のブラウザ 2 がインターネットへアクセスする際に，FW の NAT 機能が送信元 IP アドレスと [ウ] の両方をそれぞれ動的に変換する（以下，送信元 NAPT という）。(a) 変換後の IP アドレス用に二つのグローバル IP アドレスが割り当てられている。

・FW のフィルタリング定義は，図 1 に示す情報システムの通信だけを許可している。

・FW には，A 社のドメイン権限をもった DNS 機能がある。

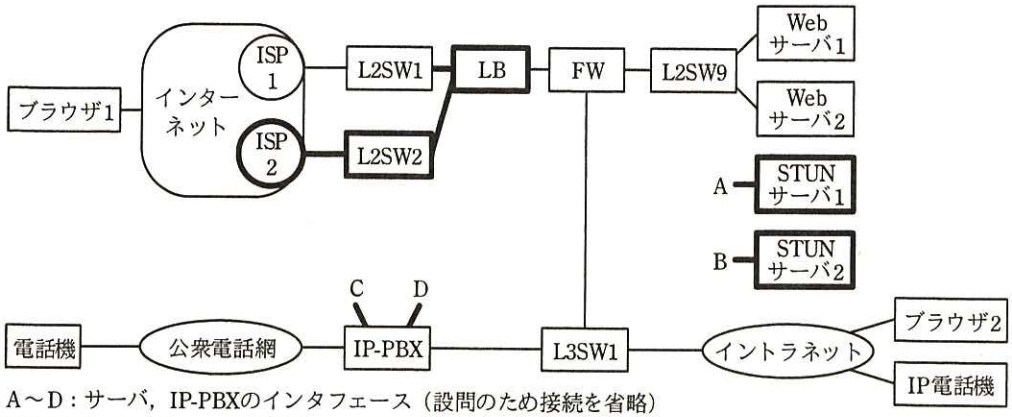
・2 台の Web サーバ（Web サーバ 1，2）は，FW の DNS ラウンドロビン機能を使って負荷分散しており，3 台以上の構成へもスケールアウトができる。(b) スケールアウトの際には，DNS 機能に関する設定変更など，FW に複数の設定変更が必要となる。

〔マルチホーミング〕

B 君は，二つの ISP サービス（ISP1，ISP2）を同時に利用するマルチホーミングの構成を考えた。この構成では，A 社が負荷分散の仕組みを用意する必要がある。調査したところ，マルチホーミング用の負荷分散装置（以下，LB という）があり，この装置は，負荷分散機能の他に，DNS 機能，NAT 機能をもつことが分かった。

B 君は LB を利用した新たなネットワーク構成を考えた。

A 社の新ネットワーク構成を図 3 に，図 3 中のスイッチに定義された LAN の新 IP アドレス空間を表 2 に，それぞれ示す。



A～D：サーバ，IP-PBXのインタフェース（設問のため接続を省略）
STUN：Session Traversal Utilities for NAT
注記　太線で示した部分は，新たに追加される ISP 及び機器を示す。

図 3　A 社の新ネットワーク構成（抜粋）

表 2　図 3 中のスイッチに定義された新 IP アドレス空間

スイッチ	VLAN 名	IP アドレス空間	用途
L2SW1	vlan1	ip1/29 （ip1 はグローバル IP アドレス）	ISP1 接続
L2SW2	vlan2	ip2/29 （ip2 はグローバル IP アドレス）	ISP2 接続
L2SW9	vlan9	10.0.9.0/24	DMZ
L3SW1	vlan8	10.0.8.0/24	FW 接続
	vlan7	10.0.7.0/24	IP-PBX 接続
	vlan6	10.0.6.0/24	イントラネット接続

LB を使ったマルチホーミングの概要を次に示す。

・インターネット向けの DNS 機能を FW から LB へ移し，ISP2 を経由してもその DNS 機能を提供できるように，ドメイン登録業者に定義の追加を依頼する。その際，ISP1，ISP2 のいずれからでも同じゾーンファイルが参照されるようにする。

・LB の DNS ラウンドロビン機能を使い，インターネットから A 社内への通信の負荷分散を行う。(c) 現行の Web サーバ用のグローバル IP アドレスに，新たなグローバル IP アドレスを加え，DNS クエリに対してそれらが交互に返るようにする。

・A 社内からインターネットへの通信は，ISP1 と ISP2 への接続ポートに対して負荷分散を行う。その際，ISP へ送信する IP パケットの送信元 IP アドレスは，送信先の ISP から貸与されたグローバル IP アドレスに変換されるので，FW の NAT 機能を LB へ移して一元化する。

・(d)LB は，通信の行きと戻りを同じ ISP 経由にする。

・LB から ISP1 のルータ及び ISP2 のルータへそれぞれ定期的に ping 確認を行い，ISP の障害を検知した場合には，正常な ISP だけを利用する。

〔ブラウザを使ったビデオ電話の通信〕

情報システム部は，WebRTC（Web Real-Time Communication）に準拠した AP を導入する予定である。WebRTC は，ブラウザを使った音声，動画などの通信規約であり，W3C 及び IETF から仕様が公開されている。この WebRTC を使ったビデオ電話では，AP をダウンロードしたブラウザ間で直接通信（以下，AP 間通信という）を行う。NAT 機能が介在する場合の AP 間通信の例を，図 4 に示す。

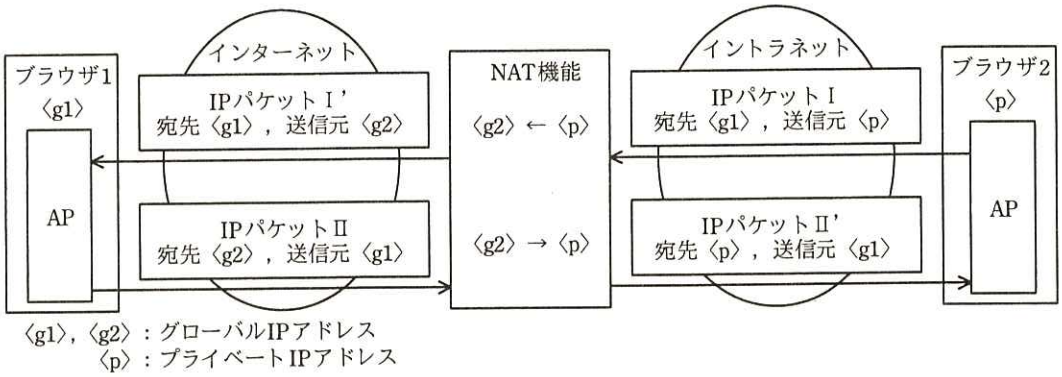


図 4　NAT 機能が介在する場合の AP 間通信の例

サーバを介さない通信では，通信相手の IP アドレスを知る仕組みが必要である。図 4 の例では，NAT 機能によってブラウザ 2 の IP アドレス〈p〉が〈g2〉に変換されている。その場合，ブラウザ 1 上の AP は，通信相手の IP アドレスとして，〈p〉ではなく〈g2〉を用いなければならない。

A 社が導入する AP は，NAT 機能によって変換された IP アドレスを，STUN サーバから得る仕様となっている。図 4 の例では，ブラウザ 2 上の AP が STUN プロトコルを用いて STUN サーバ 1，2 から〈g2〉を得て，それをブラウザ 1 上の AP に通知する。

STUN プロトコルの概要は次のとおりである。

・STUN クライアントは，STUN サーバへ Binding リクエストを送る。

・STUN サーバは，受け取った IP パケットのヘッダから送信元の IP アドレスとポート番号を取り出し，Binding レスポンス中のデータに格納して返す。

・(e) STUN クライアントは，Binding レスポンス中のデータから，自分と STUN サーバ間の NAT 機能の有無を知り，NAT 機能が介在する場合には，そのデータから NAT 機能が変換した自分の IP アドレスを得る。

B 君は，STUN サーバへのアクセスから音声，ビデオ，データなどの交換までの AP 間通信の概要をまとめた。B 君がまとめた AP 間通信の概要を，図 5 に示す。

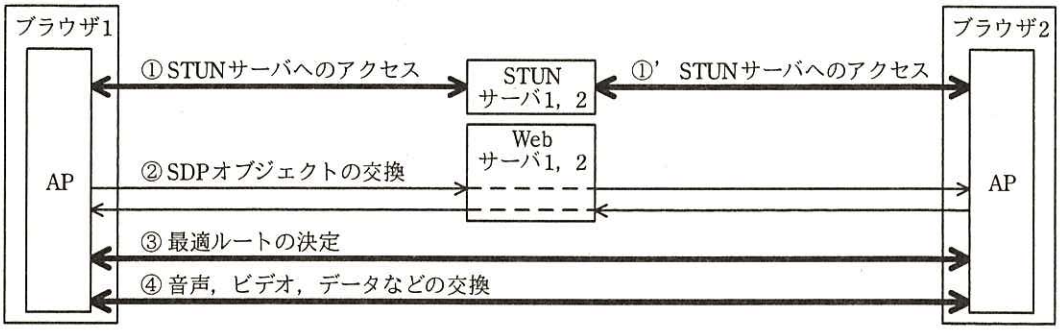


図 5　AP 間通信の概要

AP をダウンロードしたブラウザは，図 5 中の①～③で NAT 機能を経由した最適ルートを確立する（以下，ホールパンチという）。ホールパンチの概要を次に示す。

①，①' AP は STUN サーバ 1，2 にアクセスし，NAT 機能が介在する場合の変換後のブラウザの IP アドレスを取得する。

② AP は，SDP（Session Description Protocol）オブジェクトを使って，①，①' で取得した IP アドレスとブラウザ自身の IP アドレスを，通信相手の AP へ通知する。その際，ブラウザ 1，2 と Web サーバ 1，2 間に HTTPS が使われる。

③ AP は，通知された IP アドレスを宛先 IP アドレスにして通信相手との通信を試み，相互に通信が成功した場合に，その宛先 IP アドレスの組合せを最適ルートとする。

(f) 図 4 の AP 間通信は，このようにして確立した最適ルートを使っている。

なお，ホールパンチには，ブラウザの IP アドレスと NAT 機能の変換ルールが，そ

れぞれ一定時間変わらないという前提条件が必要である。例えば，図 4 中の〈p〉と〈g2〉は，AP 間通信の間，関連付けられている必要がある。また，IP アドレスだけではなくポート番号の考慮も必要である。

B 君は，AP 間通信において AP が使用するポート番号はあらかじめ決められていること，及び STUN サーバを図 3 のネットワーク内に適切に配置することによって，ホールパンチが LB の NAT 機能に対して有効に働くことをベンダに確認した。そして，(g) 片方の ISP が障害の場合にも利用できるように，STUN サーバのインタフェース（図 3 中の A，B）を，図 3 中の適切なスイッチに接続することにした。

次に，B 君は，A 社のマルチホーミング運用によって，図 5 中の通信が ISP1 と ISP2 に負荷分散されるかどうかを検討した。そして，図 5 から，データ量が多い④に用いられる ISP は，［　エ　］が［　オ　］をアクセスするときの LB の振分け結果によって決まることを確認し，負荷分散が行われると判断した。

〔ブラウザを使った音声電話の通信〕

ブラウザを使った音声電話の通信では，社外のブラウザ上で動作する AP が IP-PBX を介して社内の IP 電話機と通信を行う。

B 君は IP-PBX のベンダから IP-PBX の WebRTC 機能の情報を入手し，通信方式を検討した。B 君が考えた，社外の AP から社内の IP 電話機への通信の概要を，図 6 に示す。

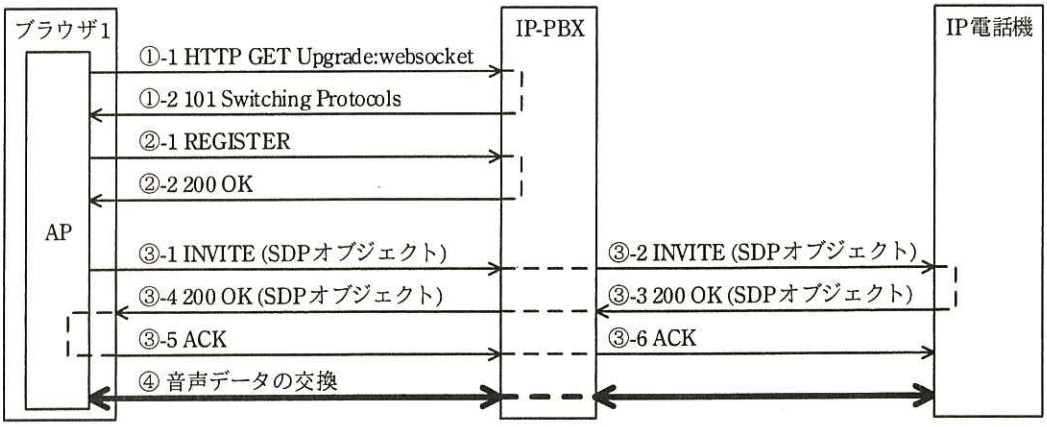


図 6　社外の AP から社内の IP 電話機への通信の概要

図6中の通信の概要は，次のとおりである。

・APは，通信プロトコル［　カ　］を使ってIP-PBXへアクセスし，①-1と①-2によって，通信プロトコルを［　キ　］に切り替え，切り替えた通信プロトコルの上でSIPプロトコルに基づくシグナリングを行う。

・IP-PBXは，2組のB2BUA（Back-to-Back User Agent）として動作する。(h)インターネット側の二つのUA（User Agent）には，それぞれグローバルIPアドレスを割り当てる。

・IP-PBXはSession Border Controllerとして動作し，グローバルIPアドレスとプライベートIPアドレスを変換する。

・(i)IP-PBXのLANインタフェース（図3中のC，D）を追加し，図3中の適切なスイッチと接続する。

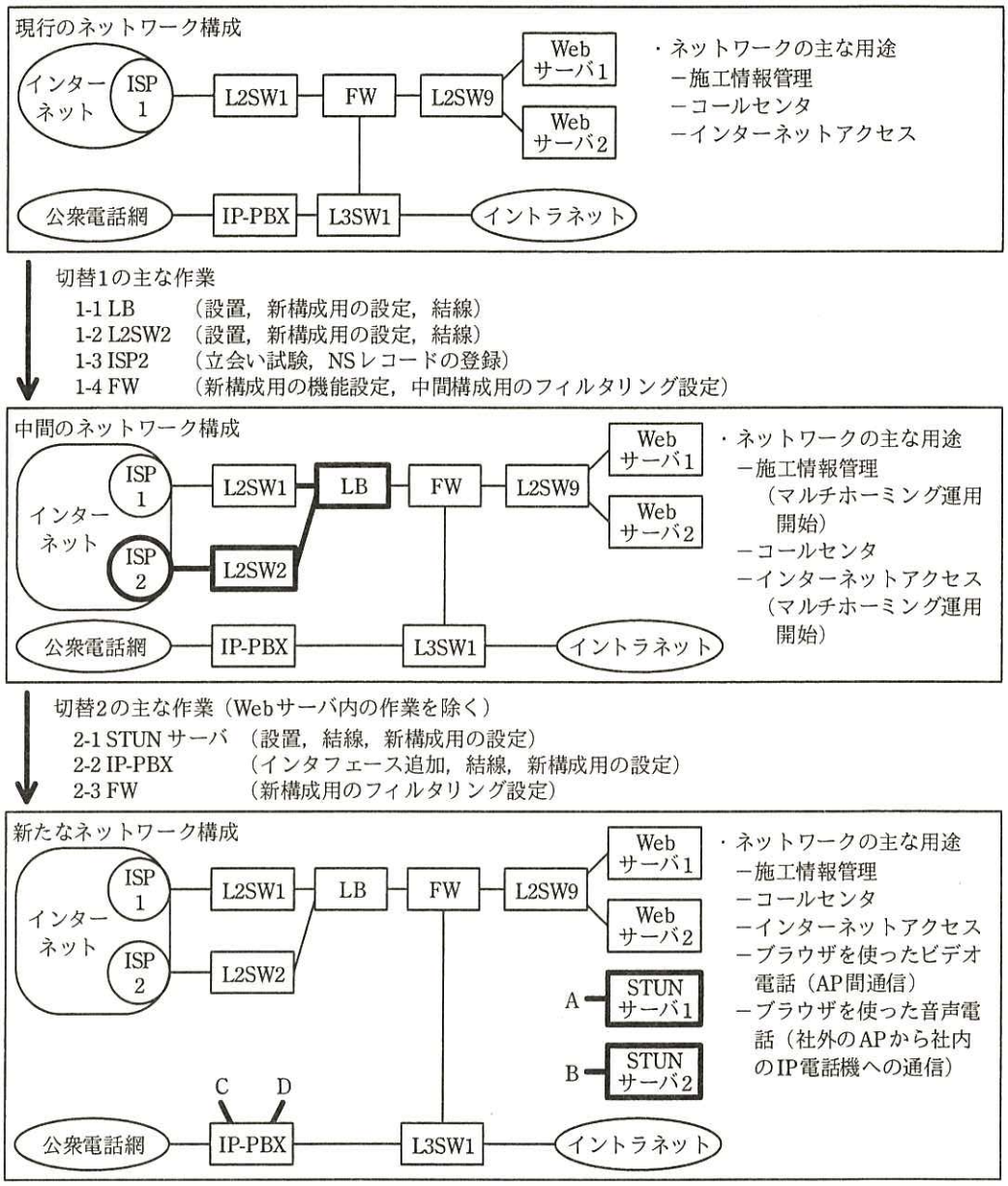
・図6中の通信の前に，［　ク　］のFQDNに関する［　ケ　］クエリが，APから［　コ　］へ発行されることによって，図6中のAPとIP-PBX間の通信はISP1とISP2に負荷分散される。

〔移行計画〕

情報システム部では，保守などでサービス停止の可能性がある場合には，サービス停止時間を関係部署へ連絡することになっている。また，連絡したサービス停止時間内に保守を終えてサービスを再開できるように，部内で作業計画を十分にレビューした上で保守を行う運用ルールも設けられている。

B君は，今回の機能拡張に関して，サービス停止時間を見積もりながら，利用者への影響が極力小さくなるような移行を考えた。ここで，サービス停止時間とは，切替作業，切替作業後の動作確認及び問題発生時の［　サ　］に要する時間の合計である。

B君が作成したネットワークの移行計画案を，図7に示す。



A～D：サーバ，IP-PBX のインタフェース（設問のため接続を省略）

図7　ネットワークの移行計画案

ネットワーク移行のための切替えは 2 段階で行う。図 7 中の切替 1 と切替 2 について，B 君は次のように考えた。

（切替 1 について）

・LB の設定は，切替 1 で全ての定義を盛り込み，その後の変更を不要にする。例え

ば DNS 機能については，新たなネットワーク構成に必要な次の A レコードを全て設定する。

－(j) Web サーバ 1 と Web サーバ 2 に関する四つの A レコード

－(k) AP が名前解決しなければならない FQDN に関する A レコード（AP 内の定義には，IP アドレスではなく，FQDN を用いることにする。）

・FW のフィルタリング変更は，中間のネットワーク構成の通信に関して変更する。

・次の点を考慮し，切替 1 のサービス停止時間は 2 時間とする。

－(l) 機器の変更は，あらかじめ 2 通りの定義ファイルをもたせておき，定義ファイルを指定した再起動によって行う。

－約 1 時間，一部の利用者に情報システムを利用してもらい，(m) 3 種類の通信を発生させて，動作の正常性を確認する。

－(n) ドメイン登録業者に依頼する定義変更に関しては，情報システム部が正常性を確認する。利用者サービスへ直接影響しないので，その作業はサービス停止時間には含まない。

（切替 2 について）

・(o) FW のフィルタリング変更は，新たなネットワーク構成の通信に関して変更する。

・機器の変更と動作の正常性確認を含めた切替 2 のサービス停止時間について，IP-PBX のベンダに見積りを依頼する。

B 君は，検討結果をまとめ，情報システム部長に報告した。その後，顧客システムの機能拡張のプロジェクトが発足し，B 君はネットワークチームのリーダとして参画することになった。

設問 1　〔現行ネットワーク構成〕について，(1) ～ (3) に答えよ。

(1) 本文中の［　ア　］～［　ウ　］に入れる適切な字句を答えよ。

(2) 本文中の下線 (a) について，送信元 NAPT が同時に処理できる TCP コネクション数の上限を答えよ。ここで，2^{16} ＝ 65,536 である。

(3) 本文中の下線 (b) について，DNS 機能以外の FW の設定変更内容を二つ挙げ，それぞれ 20 字以内で答えよ。

設問2　〔マルチホーミング〕について，(1)，(2) に答えよ。

(1) 本文中の下線 (c) について，現行のグローバル IP アドレスと追加するグローバル IP アドレスとの違いを 20 字以内で述べよ。

(2) 本文中の下線 (d) において，通信の行きと戻りが同じ ISP ではない場合の問題を，社外から Web サーバへのアクセスを例に，IP アドレスという用語を用いて 40 字以内で述べよ。

設問3　〔ブラウザを使ったビデオ電話の通信〕について，(1) ～ (4) に答えよ。

(1) 本文中の下線 (e) について，STUN クライアントはどのようにして NAT 機能の有無を判定するかを，50 字以内で述べよ。

(2) 本文中の下線 (f) について，図 4 の通信のために，ブラウザ 2 が SDP オブジェクトに格納する二つの IP アドレス候補を，図 4 中の字句を用いて答えよ。

(3) 本文中の下線 (g) の接続先を，表 2 中の VLAN 名でそれぞれ答えよ。

(4) 本文中の［　エ　］，［　オ　］に入れる適切な字句を答えよ。

設問4　〔ブラウザを使った音声電話の通信〕について，(1) ～ (4) に答えよ。

(1) 本文中の［　カ　］，［　キ　］に入れる適切な字句を答えよ。

(2) 本文中の下線 (h) について，マルチホーミングのために，グローバル IP アドレスをどのように割り当てるかを，40 字以内で述べよ。

(3) 本文中の下線 (i) の接続先を，表 2 中の VLAN 名でそれぞれ答えよ。

(4) 本文中の［　ク　］～［　コ　］に入れる適切な字句を答えよ。

設問5　〔移行計画〕について，(1) ～ (7) に答えよ。

(1) 本文中の［　サ　］に入れる適切な字句を答えよ。

(2) 本文中の下線 (j) の四つの A レコードに記述されている，FQDN とグローバル IP アドレスの数をそれぞれ答えよ。

(3) 本文中の下線 (k) の FQDN に対応する機器名を，全て答えよ。

(4) 本文中の下線 (l) について，2 通りの定義ファイルが必要な機器名を答えよ。

(5) 本文中の下線 (m) の 3 種類の通信を，それぞれ 20 字以内で答えよ。

(6) 本文中の下線 (n) の確認内容を，30 字以内で述べよ。

(7) 本文中の下線 (o) のフィルタリング変更について，切替 2 で許可する通信を全て挙げ，図 5 中の記号（①，①'，②～④）を用いて答えよ。