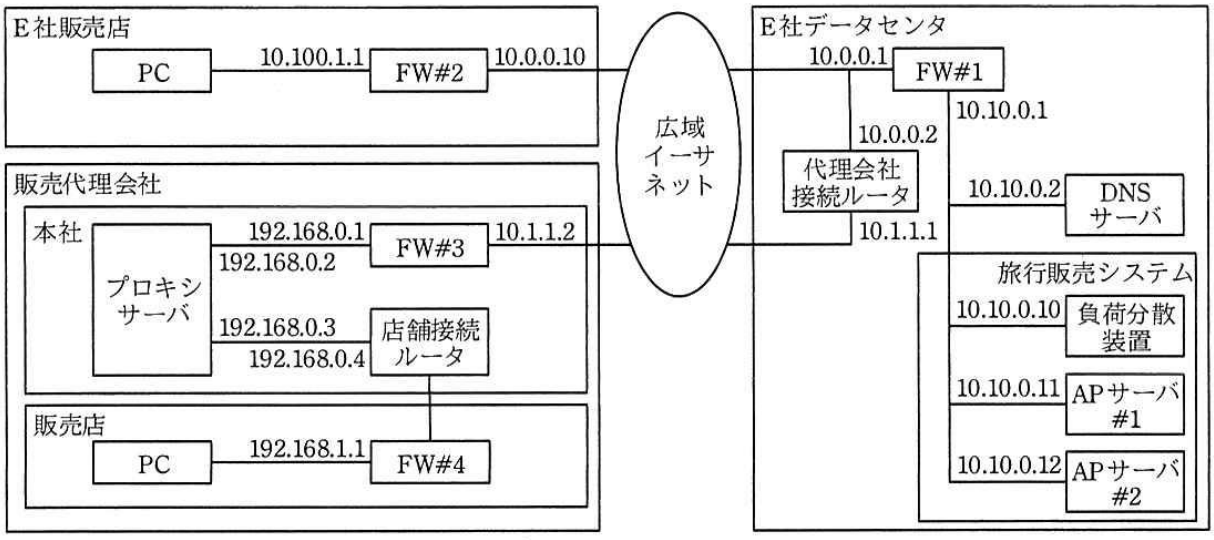
問５　チャット機能の開発に関する次の記述を読んで，設問 1～3 に答えよ。

E 社は，旅行商品の企画，運営，販売を行う旅行会社である。E 社の旅行商品は，自社の販売店と販売代理会社の販売店を通じて販売している。販売店に顧客が来ると，販売スタッフが E 社の旅行販売システムを利用して，顧客の要望に合う旅行商品を検索し，顧客に提案している。また，顧客からの旅行商品に関する質問の回答が分からない場合，E 社の販売店向けコールセンタに電話で問い合わせることになっているが，販売店からは“コールセンタに電話が繋がらない”などの苦情が出ている。

そこで E 社は，販売店とコールセンタのスタッフがテキストメッセージで相互にやり取りできるチャット機能を，旅行販売システムに追加することにした。チャット機能の開発は，E 社システム部門の F 君が担当することになった。

〔ネットワーク構成の調査〕

F 君は，チャット機能を開発するに当たり，現在のネットワーク構成を調査した。図 1 に F 君が調査したネットワーク構成（抜粋）を示す。



FW：ファイアウォール　　APサーバ：アプリケーションサーバ

図１　F 君が調査したネットワーク構成（抜粋）

旅行販売システムは，2 台の AP サーバと負荷分散装置から構成されている。負荷分散装置は AP サーバの負荷を分散させるために利用される。DNS サーバの A レコ

ードには，旅行販売システムのIPアドレスとして［ a ］が登録されている。

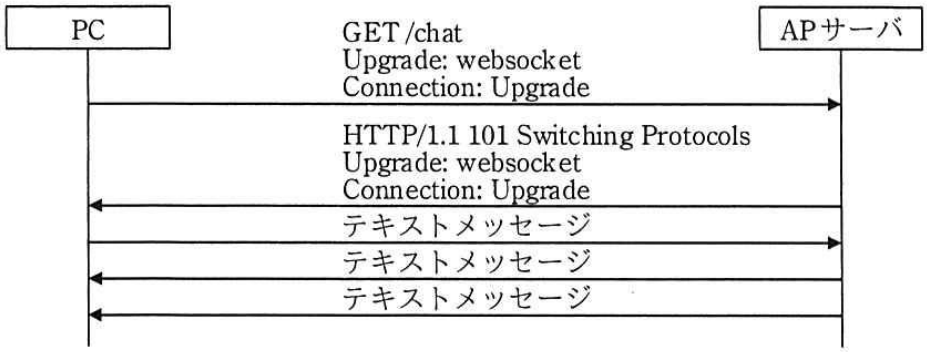
販売代理会社の販売店の PC から旅行販売システムへの通信は，FW，ルータ，プロキシサーバを経由している。FW#3 では，NAPT を行い，宛先ポートが 53 番ポート，80 番ポート又は 443 番ポートで宛先ネットワークアドレスが 10.10.0.0 の IP パケットとその返信 IP パケットだけを通信許可する設定となっている。

販売代理会社の販売店の PC が HTTP を利用して旅行販売システムにアクセスする場合，プロキシサーバは PC から受信した GET メソッドを参照して，AP サーバへ HTTP リクエストを送信する。一方，HTTP Over TLS を利用する場合は，プロキシサーバは旅行販売システムの機器と TCP コネクションを確立し，①PC から受信したデータをそのまま送信する。

また，販売代理会社の販売店の PC から旅行販売システムへアクセスする場合，PC から FW#4 に送信される IP パケットの宛先 IP アドレスは［ b ］となり，代理会社接続ルータから FW#1 に送信される IP パケットの送信元 IP アドレスは［ c ］となる。

〔チャット機能の実装方式の検討〕

次に F 君は，チャット機能の実装方式を検討した。チャット機能を実装する場合，旅行販売システムで利用している②HTTP では実装が困難である。そこで F 君は，チャット機能の実装のために WebSocket について調査を行った。図 2 に F 君が調査した WebSocket を利用した通信（抜粋）を示す。



注記　図中の PC は，E 社販売店の PC と販売代理会社の販売店の PC を指す。

図 2　F 君が調査した WebSocket を利用した通信（抜粋）

WebSocket を利用すると，PC と AP サーバの間の HTTP を用いた通信を拡張し，任意フォーマットのデータの双方向通信ができる。WebSocket を利用するためには，PC から AP サーバに HTTP と同様の GET メソッドを送信する。この GET メソッドの HTTP ヘッダに“Upgrade: websocket”と“Connection: Upgrade”を含めることで，PC と AP サーバの間で WebSocket の接続が確立する。接続が確立したら，PC と AP サーバのどちらからでも，テキストメッセージを送信できる。

この調査結果から F 君は，IRC（Internet Relay Chat）プロトコルや新たにチャット機能専用のプロトコルを利用する場合と比較し，③WebSocket を利用することで販売代理会社の FW やルータの設定変更を少なくできると考えた。

〔チャット機能の設計レビュー〕

F 君は，AP サーバにチャット機能を追加するための設計を行い，上司の G 課長のレビューを受けた。レビューの結果，G 課長から次の 2 点の指摘があった。

指摘 1. WebSocket は TCP コネクションを確立したままにするので，負荷分散装置を経由してチャット機能へアクセスすると，旅行販売システムの既存機能へのアクセスに影響がある。

指摘 2. チャット機能を WebSocket Over TLS に対応させないと，販売代理会社からプロキシサーバを経由してチャット機能にアクセスできない。

F 君は指摘 1 について，チャット機能では負荷分散装置を使わないことにし，E 社データセンタ内にある機器を利用した④ほかの負荷分散方式に変更した。

次に指摘 2 について，WebSocket を利用した通信では TCP コネクションを確立したままにする必要があるので，プロキシサーバの HTTP Over TLS のデータをそのまま送信する機能を利用することで，プロキシサーバ経由でチャット機能が利用できる。そこで，F 君は TLS 証明書を［ d ］にインストールし，チャット機能の通信を HTTP Over TLS に対応させた。

その後 F 君が，チャット機能を旅行販売システムに追加したことで，販売店でのチャット機能の利用が開始された。

設問1　〔ネットワーク構成の調査〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］～［ c ］に入れる適切なIPアドレスを図1中の字句を用いて答えよ。

(2) E社販売店のPC及び販売代理会社の販売店のPCが旅行販売システムにアクセスするためには，どの機器のDNS設定にE社のDNSサーバのIPアドレスを設定する必要があるか，解答群の中から全て選び，記号で答えよ。

解答群

ア　E社販売店のPC　　イ　FW#1

ウ　FW#2　　エ　FW#3

オ　FW#4　　カ　店舗接続ルータ

キ　販売代理会社の販売店のPC　　ク　負荷分散装置

ケ　プロキシサーバ

(3) 本文中の下線①について，プロキシサーバがPCから送信されたデータをそのまま送信するのはなぜか，30字以内で述べよ。

設問2　〔チャット機能の実装方式の検討〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，チャット機能をHTTPで実装するのはなぜ困難か，解答群の中から選び，記号で答えよ。

解答群

ア　PCはAPサーバ上のファイルを取得することしかできないから

イ　PCへのメッセージ送信はAPサーバ側で発生したイベントを契機として行うことができないから

ウ　TCPコネクションを確立したままにできないから

エ　どのPCから送られたメッセージか，APサーバが判別できないから

(2) 本文中の下線③について，FWやルータへの設定変更を少なくできるのはなぜか，WebSocketとHTTPの共通点に着目して，20字以内で述べよ。

設問3　〔チャット機能の設計レビュー〕について，(1)，(2)に答えよ。

(1) 本文中の下線④について，どのような負荷分散方式に変更したか，20字以内で答えよ。

(2) 本文中の［ d ］に入れる適切な機器名を，図1中の字句を用いて全て答えよ。

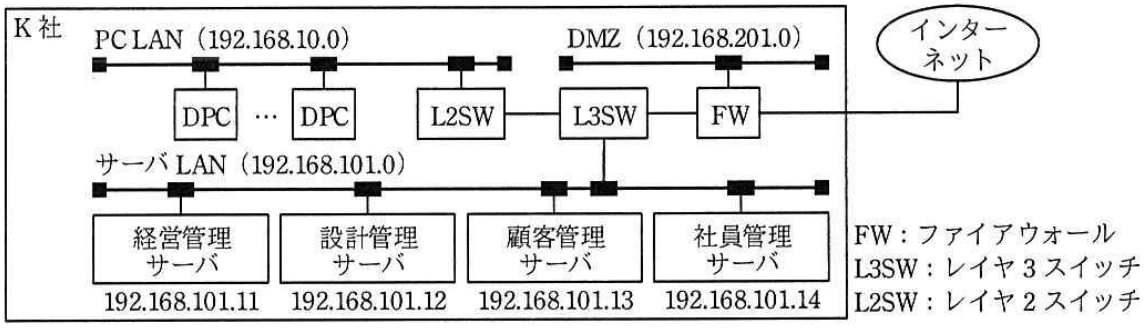
問5　LANのネットワーク構成変更に関する次の記述を読んで，設問1～4に答えよ。

K社は，従業員約200名の自動車部品製造会社である。主に国内自動車メーカから注文を受けて，駆動系部品の開発・設計・製造を行っている。K社の事務所は，工場敷地内の3階建ての事務棟に置かれており，各フロアで企画部，開発製造部，営業部及び総務部の，事務所勤務を行う社員約100名が業務を行っている。

事務棟にはK社LANが敷設されており，社員は一人1台のデスクトップPC（以下，DPCという）を使って各自の業務を行っている。現在のK社LANは，サーバを接続するサーバLAN，DPCを接続するPC LAN，及びDMZの三つのサブネットワークで構成されている。無線LANは未導入で，DPCは有線LANで接続している。各部署の業務で扱っている重要情報と，それを管理するサーバを表1に示す。また，現在のK社ネットワーク構成を図1に示す。

表1　K社が各部署で扱っている重要情報とそれを管理するサーバ

部署名	重要情報名	サーバ名
企画部	経営情報	経営管理サーバ
開発製造部	設計情報	設計管理サーバ
営業部	顧客情報	顧客管理サーバ
総務部	社員情報	社員管理サーバ



注記1　DMZ上のサーバは省略している。
注記2　各サブネットワークのサブネットマスクは，255.255.255.0である。

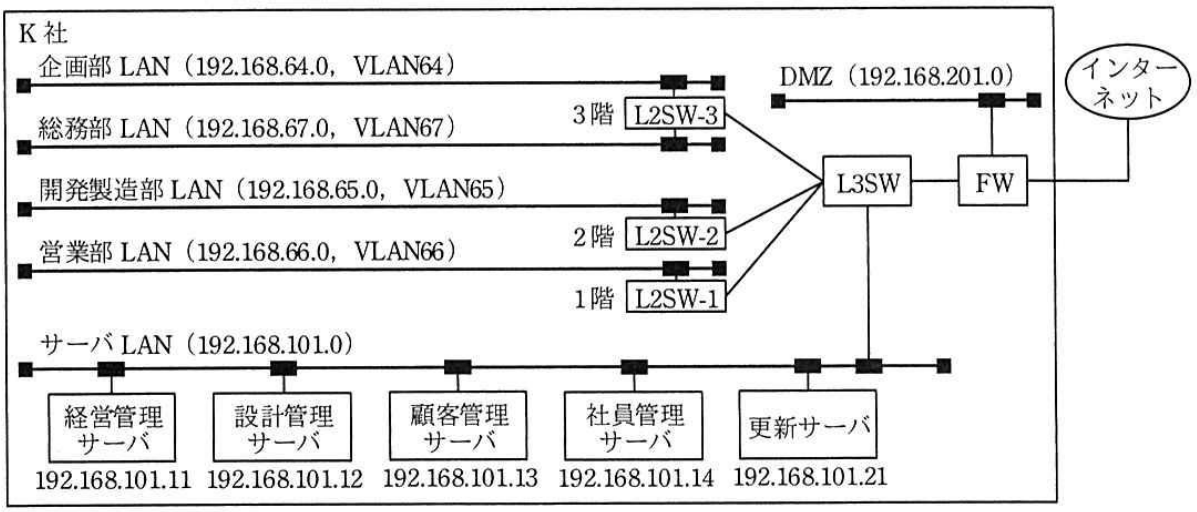
図1　現在のK社ネットワーク構成

PC LANとサーバLANはL3SW及びL2SWで接続されており，各DPCから全てのサーバにアクセスすることができる。各サーバ内の情報には，社員IDとパスワードで認証を行い，許可された社員だけがアクセスできる。

〔セキュリティ強化のための対策〕

K 社では，サーバの認証情報の設定ミスによって，総務部の一部の社員が顧客情報を入手して閲覧できる状態になっていたというインシデントが発生した。K 社では同種のインシデントへの対策として，セキュリティの強化を行うことになった。まず，PC LAN を部署ごとに異なるサブネットワークに分割し，サブネットワークごとに接続可能なサーバを定め，それ以外のサーバへのアクセスを遮断することにした。また，ランサムウェアなどの新たな脅威に対応できるウイルス対策ソフトを全ての DPC に導入することにした。サーバ LAN 上にウイルス対策ソフトの更新サーバを導入し，全ての DPC から定期的にアクセスして，ウイルス定義ファイルを最新の状態にすることにした。更新サーバの IP アドレスは 192.168.101.21 とした。

ネットワーク構成の変更を担当することになった総務部の L さんは，各フロアに設置されている L2SW を利用して，既設の PC LAN を部署ごとに異なるサブネットワークに分割し，各サブネットワークに VLAN を割り当てることを考えた。分割後の K 社ネットワーク構成案を図 2 に，L3SW のアクセスコントロールリストを表 2 に示す。



注記 1　DMZ 上のサーバや各 LAN 上の DPC は省略している。
注記 2　VLAN64～VLAN67 は VLAN ID を示す。
注記 3　各サブネットワークのサブネットマスクは，255.255.255.0 である。

図 2　サブネットワーク分割後の K 社ネットワーク構成案

表 2　L3SW のアクセスコントロールリスト（抜粋）

項番	送信元 IP アドレス	宛先 IP アドレス	処理
1	192.168.64.0/24	（省略）	許可
2	192.168.65.0/24	a	許可
3	192.168.66.0/24	（省略）	許可
4	192.168.67.0/24	（省略）	許可
5	192.168.64.0/ b	192.168.101.21	許可
6	ANY	ANY	遮断

注記 1　サブネットマスク長を指定しない IP アドレスはホスト IP アドレス（サーバや DPC に付与する IP アドレス）を示す。

注記 2　ANY は対象が全ての IP アドレスであることを示す。

注記 3　L3SW のダイナミックパケットフィルタリング機能によって，戻りパケットは通過できるものとする。

注記 4　アクセスコントロールリストは，項番の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。

L さんが検討したセキュリティ強化のための対策案を総務部内で説明したところ，表 3 に示す課題が指摘された。L さんは，各課題に対して対策を検討した。

表 3　総務部内で指摘された課題

項番	課題
1	既設の PC LAN はカテゴリ 5 の UTP ケーブルを使って配線されており，DPC とは 100BASE-TX で接続している。ネットワークの速度が遅く業務に支障が出ているので，改善してほしいと各部署から要望があがっている。
2	フロア間の管路に余裕がなく，既設のケーブルを撤去しないとフロア間に新しいケーブルを配線できない。
3	近い将来，無線 LAN を導入し，DPC をノート PC に置き換えることを検討したい。各フロアに無線 LAN アクセスポイント（以下，無線 AP という）を設置する準備をしておきたい。
4	部署ごとの人員増減に伴って，近い将来部署を配置するフロアが変更となる可能性がある。その際にもケーブルの配線変更を最小限にしたい。

〔物理配線の検討〕

表 3 の項番 1，項番 2 の課題に対応して，既設の PC LAN 用のケーブルを撤去し，新たなケーブルを配線することにした。フロア内の L2SW から DPC までの配線は，①1000BASE-T 方式に対応した UTP ケーブルとした。また，1 階のサーバルームに設置した L3SW から各フロアの L2SW までは，②最大 10 G ビット／秒で通信可能な光ファイバケーブルとした。

〔無線 LAN 導入の検討〕

表 3 の項番 3 の課題に対して，事務棟の各フロアで無線 AP の設置に適した場所の調査を行った。その結果，電源の確保が困難な設置場所が判明した。また，事務棟が東西方向に約 50 m と細長く，部屋を仕切る壁が厚いことや金属製の扉が多いことも確認した。

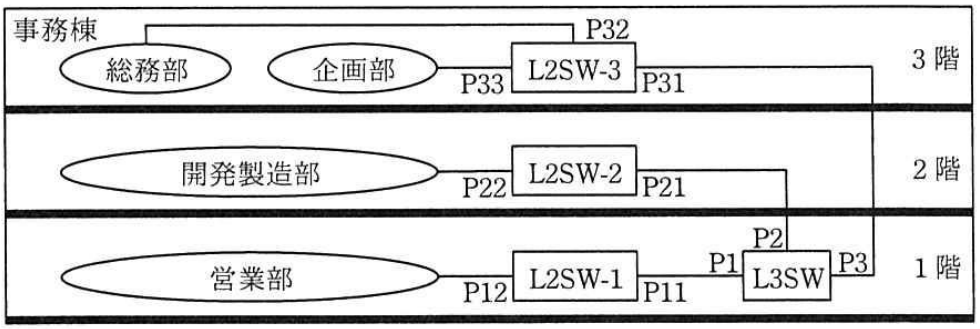
そこで，各フロアに設置する L2SW を今後リプレースする場合には，UTP ケーブルで無線 AP に電力供給が可能な［ c ］機能を備える機器を導入することにした。また，③導入予定の無線 AP と各 DPC の設置位置での電波強度の調査を行うことにした。

〔VLAN 構成の検討〕

表 3 の項番 4 の課題に対して，一つのフロアに複数部署が混在したり，部署がフロア内やフロア間で移動する可能性を考慮して，ネットワークスイッチのポート単位に VLAN を設定するポートベース VLAN ではなく，一つのポートに複数の VLAN を同時に設定できる［ d ］VLAN の機能を備えるネットワークスイッチを導入することにした。

現状の部署の配置を前提とした，ネットワークスイッチのフロア配置を図 3 に示す。図 2 のネットワーク構成を図 3 のネットワークスイッチで構成した場合の，各ネットワークスイッチの VLAN 構成の案を表 4 に示す。

L さんの検討案は総務部内で承認され，具体的な実施計画を策定することになった。



注記　Pn は各ネットワークスイッチのポート ID を示す。

図 3　現状の部署の配置を前提としたネットワークスイッチのフロア配置

表4　各ネットワークスイッチの VLAN 構成の案

ネットワークスイッチ	ポート ID	設定する VLAN ID
L3SW	P1	VLAN66
	P2	VLAN65
	P3	e
L2SW-1	P11	VLAN66
	P12	VLAN66
L2SW-2	P21	f
	P22	f
L2SW-3	P31	e
	P32	VLAN67
	P33	VLAN64

設問1　表2中の［ a ］，［ b ］に入れる適切な字句を答えよ。

設問2　〔物理配線の検討〕について，(1)，(2) に答えよ。

(1)　本文中の下線①に該当する UTP ケーブルの規格を，解答群の中から全て選び，記号で答えよ。

解答群

ア　カテゴリ3　　イ　カテゴリ5e　　ウ　カテゴリ6　　エ　カテゴリ6a

(2)　本文中の下線②で，光ファイバケーブルを採用した理由を，UTP ケーブルの伝送特性と比較して，20字以内で述べよ。

設問3　〔無線 LAN 導入の検討〕について，(1)，(2)に答えよ。

(1)　本文中の［ c ］に入れる適切な字句を，アルファベット3字で答えよ。

(2)　本文中の下線③について，電波強度の調査を実施せずに無線 AP を導入した場合に，発生するおそれのある不具合を，L さんの調査結果を踏まえて，30字以内で述べよ。

設問4　〔VLAN 構成の検討〕について，(1)～(3)に答えよ。

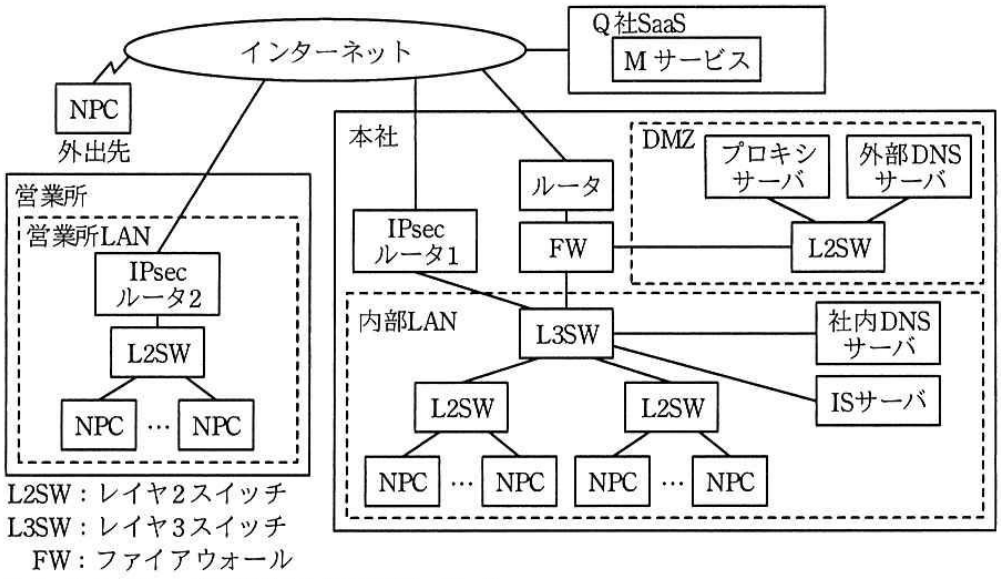
(1)　本文中の［ d ］に入れる適切な字句を5字以内で答えよ。

(2)　表4中の［ e ］，［ f ］に入れる適切な VLAN ID を全て答えよ。

(3)　図3のフロア配置に対して，総務部が1階に移動した場合，VLAN 構成に変更を加える必要がある。このうち，変更を加えるべき L3SW のポートのポート ID を全て答えよ。また，変更内容を30字以内で述べよ。

問5　ネットワークの構成変更に関する次の記述を読んで，設問1～3に答えよ。

P 社は，本社と営業所をもつ中堅商社である。P 社では，本社と営業所の間を，IPsec ルータを利用してインターネット VPN で接続している。本社では，情報共有のためのサーバ（以下，IS サーバという）を運用している。電子メールの送受信には，SaaS 事業者の Q 社が提供する電子メールサービス（以下，M サービスという）を利用している。ノート PC（以下，NPC という）から IS サーバ及び M サービスへのアクセスは，HTTP Over TLS（以下，HTTPS という）で行っている。P 社のネットワーク構成（抜粋）を図1に示す。



注記1　Q 社 SaaS 内のサーバの接続構成は省略している。

注記2　本社の内部 LAN の NPC，内部 LAN のサーバ，IPsec ルータ 1，FW 及び DMZ は，それぞれ異なるサブネットに設置されている。

図1　P 社のネットワーク構成(抜粋)

〔P 社のネットワーク機器の設定内容と動作〕

P 社のネットワークのサーバ及び NPC の設定内容と動作を次に示す。

・本社及び営業所（以下，社内という）の NPC は，社内 DNS サーバで名前解決を行う。

・社内 DNS サーバは，内部 LAN のサーバの IP アドレスを管理し，管理外のサーバの名前解決要求は，外部 DNS サーバに転送する。

・外部 DNS サーバは，DMZ のサーバのグローバル IP アドレスを管理するとともに，

DNS キャッシュサーバ機能をもつ。

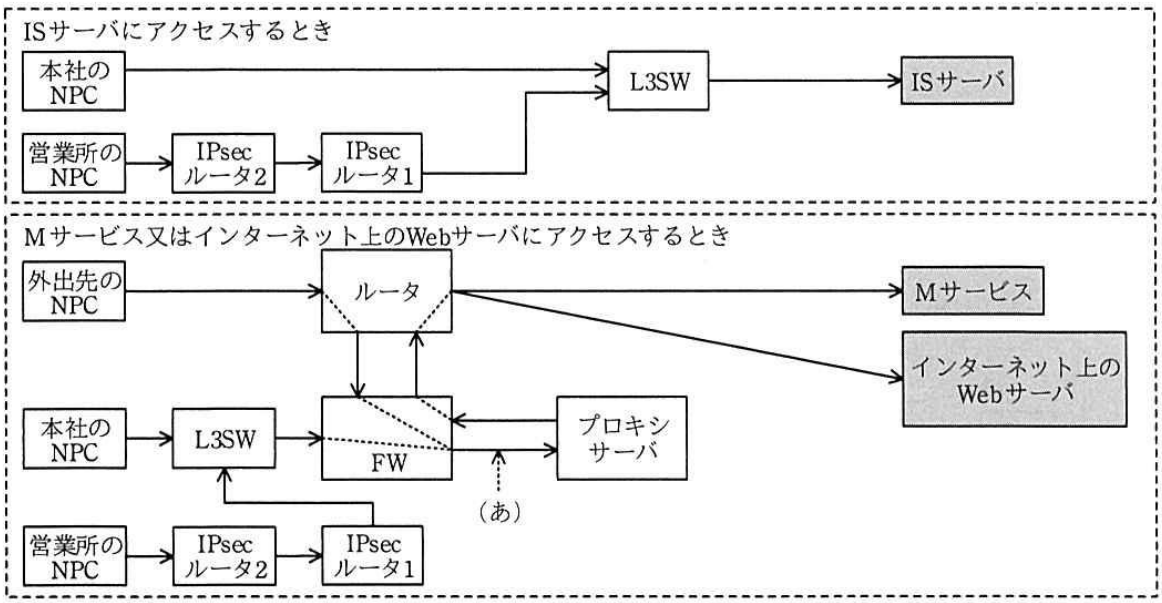
・プロキシサーバでは，利用者認証，URL フィルタリングを行うとともに，通信ログを取得する。

・外出先及び社内の NPC の Web ブラウザには，HTTP 及び HTTPS 通信がプロキシサーバを経由するように，プロキシ設定にプロキシサーバの FQDN を登録する。ただし，社内の NPC から IS サーバへのアクセスは，プロキシサーバを経由せずに直接行う。

・IS サーバには，社内の NPC だけからアクセスしている。

・外出先及び社内の NPC から M サービス及びインターネットへのアクセスは，プロキシサーバ経由で行う。

NPC による各種通信時に経由する社内の機器又はサーバを図 2 に示す。ここで，L2SW の記述は省略している。



注記　網掛けは，アクセス先のサーバ又はサービスを示す。

図 2　NPC による各種通信時に経由する社内の機器又はサーバ

FW に設定されている通信を許可するルール（抜粋）を表 1 に示す。

表1　FWに設定されている通信を許可するルール（抜粋）

項番	アクセス経路	送信元	宛先	プロトコル／宛先ポート番号
1	インターネット→DMZ	any	a	TCP／53，UDP／53
2		any	プロキシサーバ	TCP／8080[1)]
3	DMZ→インターネット	外部DNSサーバ	any	TCP／53，UDP／53
4		b	any	TCP／80，TCP／443
5	内部LAN→DMZ	c	外部DNSサーバ	TCP／53，UDP／53
6		社内のNPC	プロキシサーバ	TCP／8080[1)]

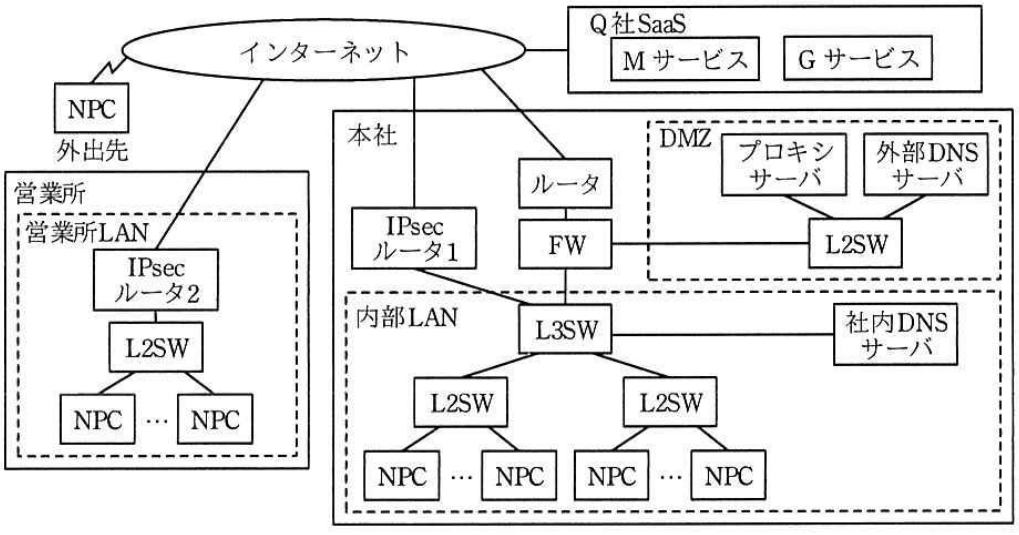
注記　FWは，応答パケットを自動的に通過させる，ステートフルパケットインスペクション機能をもつ。

注 1)　TCP／8080は，プロキシサーバでの代替HTTPの待受けポートである。

このたび，P社では，サーバの運用負荷の軽減と外出先からの社内情報へのアクセスを目的に，ISサーバを廃止し，Q社が提供するグループウェアサービス（以下，Gサービスという）を利用することにした。Gサービスへの通信は，Mサービスと同様にHTTPSによって安全性が確保されている。Gサービスを利用するためのネットワーク（以下，新ネットワークという）の設計を，情報システム部のR主任が担当することになった。

〔新ネットワーク構成と利用形態〕

R主任が設計した，新ネットワーク構成（抜粋）を図3に示す。



注記　Q社SaaS内のサーバの接続構成は省略している。

図3　新ネットワーク構成（抜粋）

新ネットワークでは，サービスとインターネットの利用状況を管理するために，外出先及び社内の NPC から M サービス，G サービス及びインターネットへのアクセスを，プロキシサーバ経由で行うことにした。

R 主任は，IS サーバの廃止に伴って不要になる，次の設定情報を削除した。

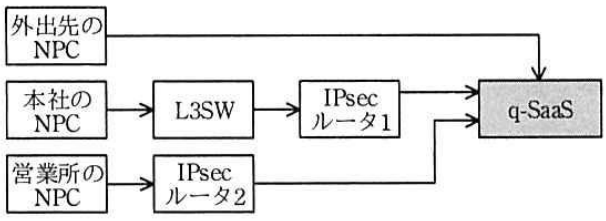
・①NPC の Web ブラウザの，プロキシ例外設定に登録されている FQDN

・社内 DNS サーバのリソースレコード中の，IS サーバの A レコード

〔G サービス利用開始後に発生した問題と対策〕

G サービス利用開始後，インターネットを経由する通信の応答速度が，時間帯によって低下するという問題が発生した。FW のログの調査によって，FW が管理するセッション情報が大量になったことによる，FW の負荷増大が原因であることが判明した。そこで，FW を通過する通信量を削減するために，M サービス及び G サービス（以下，二つのサービスを合わせて q-SaaS という）には，プロキシサーバを経由せず，外出先の NPC は HTTPS でアクセスし，本社の NPC は IPsec ルータ 1 から，営業所の NPC は IPsec ルータ 2 から，インターネット VPN を経由せず HTTPS でアクセスすることにした。この変更によって，q-SaaS の利用状況は，プロキシサーバの通信ログに記録されなくなるので，Q 社から提供されるアクセスログによって把握することにした。

外出先及び社内の NPC から q-SaaS アクセス時に経由する社内の機器を図 4 に示す。ここで，L2SW の記述は省略している。



注記　網掛けは，アクセス先のサービスを示す。

図 4　外出先及び社内の NPC から q-SaaS アクセス時に経由する社内の機器

図 4 に示した経路に変更するために，R 主任は，②L3SW の経路表に新たな経路の追加，及び IPsec ルータ 1 と IPsec ルータ 2 の設定変更を行うとともに，NPC の Web

ブラウザでは，q-SaaS利用時にプロキシサーバを経由させないよう，プロキシ例外設定に，Mサービス及びGサービスのFQDNを登録した。

設定変更後のIPsecルータ1の処理内容（抜粋）を表2に示す。IPsecルータ1は，受信したパケットと表2中の照合する情報とを比較し，パケット転送時に一致した項番の処理を行う。

表2　設定変更後のIPsecルータ1の処理内容（抜粋）

項番	照合する情報			処理
	送信元	宛先	プロトコル	
1	内部LAN	d	HTTPS	NAPT後にインターネットに転送
2	内部LAN	e	any	インターネットVPNに転送

IPsecルータ2もIPsecルータ1と同様の設定変更を行う。これらの追加設定と設定変更によってFWの負荷が軽減し，インターネット利用時の応答速度の低下がなくなり，R主任は，ネットワークの構成変更を完了させた。

設問1　〔P社のネットワーク機器の設定内容と動作〕について，(1)～(3)に答えよ。

(1) 営業所のNPCがMサービスを利用するときに，図2中の（あ）を通過するパケットのIPヘッダ中の宛先IPアドレス及び送信元IPアドレスが示す，NPC，機器又はサーバ名を，図2中の名称でそれぞれ答えよ。

(2) 外出先のNPCからインターネット上のWebサーバにアクセスするとき，L2SW以外で経由する社内の機器又はサーバ名を，図2中の名称で全て答えよ。

(3) 表1中のa～cに入れる適切な機器又はサーバ名を，図1中の名称で答えよ。

設問2　本文中の下線①について，削除するFQDNをもつ機器又はサーバ名を，図1中の名称で答えよ。

設問3　〔Gサービス利用開始後に発生した問題と対策〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，新たに追加する経路を，“q-SaaS”という字句を用いて，40字以内で答えよ。

(2) 表2中のd，eに入れる適切なネットワークセグメント，サーバ又はサービス名を，本文中の名称で答えよ。