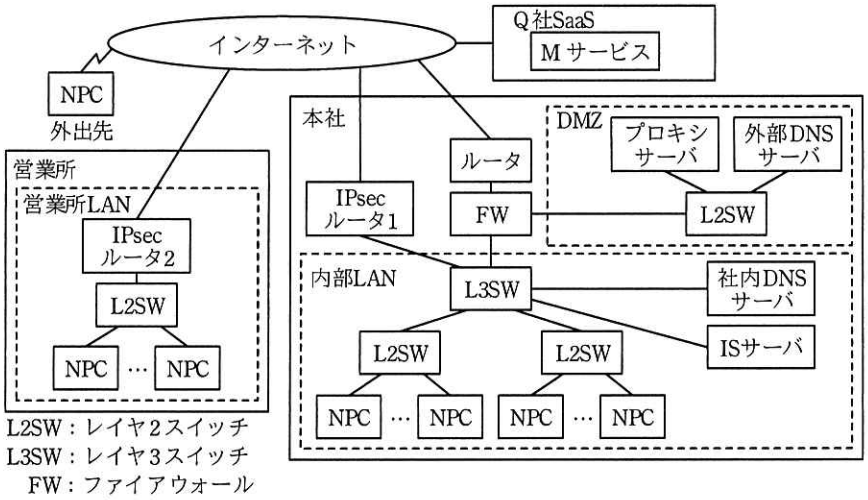
問5　ネットワークの構成変更に関する次の記述を読んで，設問1～3に答えよ。

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。

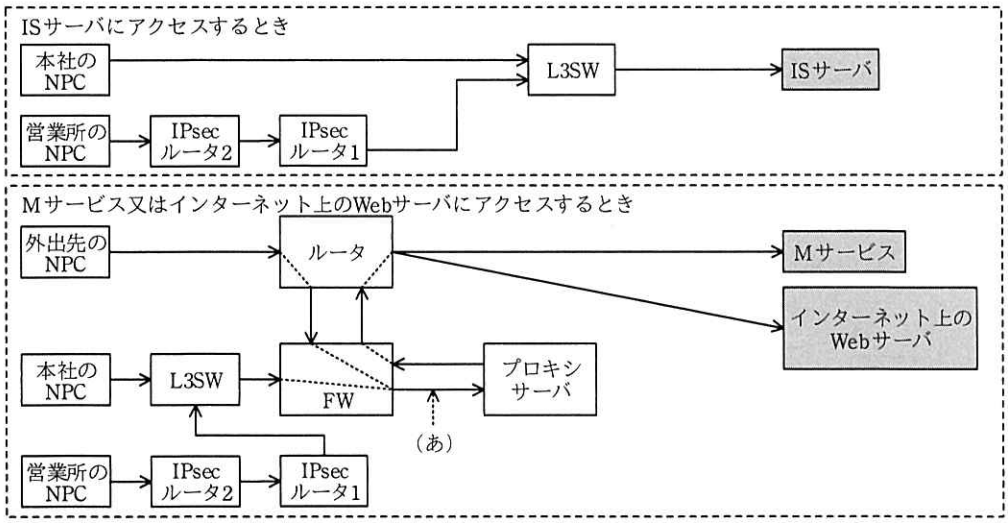
・プロキシサーバでは，利用者認証，URL フィルタリングを行うとともに，通信ログを取得する。

・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)]

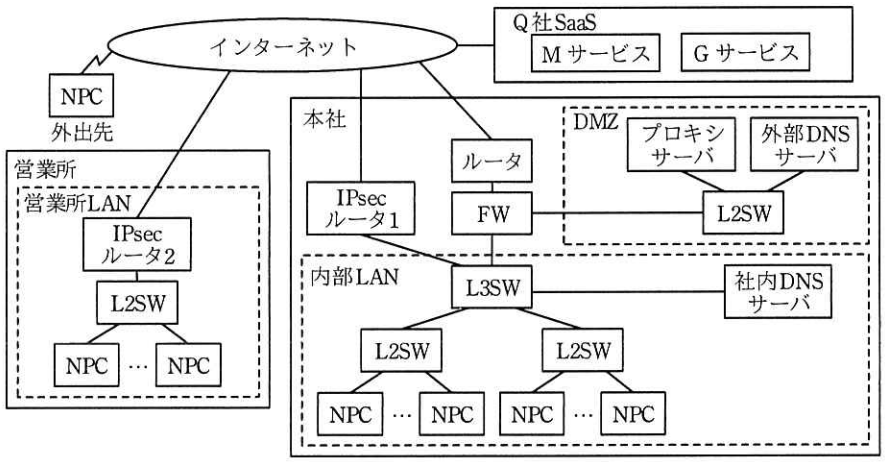
注記　FWは，応答パケットを自動的に通過させる，ステートフルパケットインスペクション機能をもつ。

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。

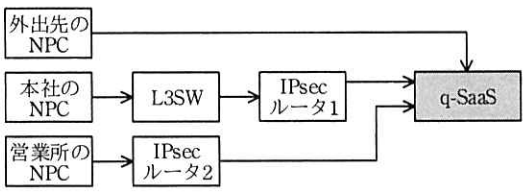
・①NPC の Web ブラウザの，プロキシ例外設定に登録されている FQDN

・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。