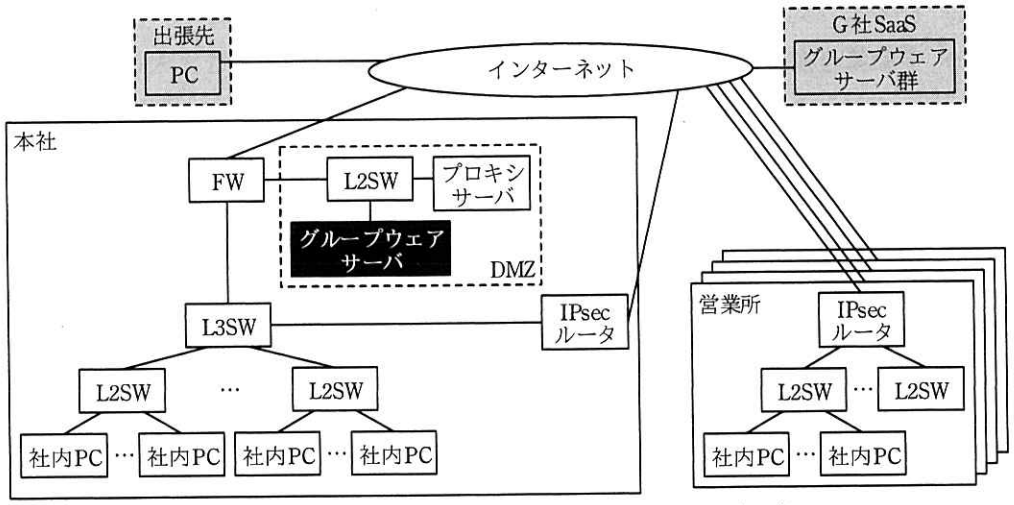
問1　SaaSの導入に関する次の記述を読んで，設問1～3に答えよ。

F社は，本社と四つの営業所を拠点として事業を展開している中堅商社である。本社を中心としたハブアンドスポーク構成のIPsec VPNを使って，本社と営業所を接続している。営業所からインターネットへの通信は，全て本社を経由させている。現在F社で利用しているグループウェア機能は，電子メール，スケジューラ，ファイル共有などである。このうち電子メールは社外との連絡にも利用している。

このたびF社では，グループウェアサーバの老朽化に伴い，グループウェアサーバを廃止し，グループウェア機能をもつG社SaaSを導入することにした。また，G社SaaSの導入に合わせたセキュリティ対策を講じることにした。

〔F社の現行ネットワーク構成とG社SaaS導入に合わせたセキュリティ対策〕

F社の現行ネットワーク構成を，図1に示す。



FW：ファイアウォール　L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ

注記1　[破線]は，G社SaaS導入に伴って追加予定の構成を示す。

注記2　[黒]は，G社SaaS導入後，廃止予定の機器を示す。

図1　F社の現行ネットワーク構成（抜粋）

・プロキシサーバ及びグループウェアサーバは，本社DMZに設置されている。

・L3SWでは，次のように静的経路設定を行っている。

- デフォルトルートのネクストホップをFWに設定している。
- 各営業所への経路のネクストホップを本社のIPsecルータに設定している。

・社内PCからインターネットへは，Webアクセスだけが許可されており，プロキシサーバを経由して通信を行っている。

一般に，プロキシには，［　ア　］プロキシと［　イ　］プロキシがある。F社のプロキシのように［　ア　］プロキシは，社内に対して，アクセス先URLのログ取得や，外部サーバのコンテンツをキャッシュして使用帯域を削減する目的で用いられる。一方，［　イ　］プロキシは，外部から公開サーバのオリジナルコンテンツに直接アクセスさせないことによる改ざん防止，キャッシュによる応答速度の向上，及び複数のサーバでの負荷分散を行う目的で用いられる。

G社SaaSの導入に合わせて，インターネットへのWebアクセスについてのセキュリティ対策を検討した。検討結果を次に示す。

・G社SaaSとの通信は，HTTPSによって暗号化する。
・出張先のPCから直接G社SaaSを利用できるようにするために，G社SaaSでは送信元IPアドレスの制限を行わない。
・G社SaaS導入に合わせてセキュリティ強化を行うために，プロキシサーバで次のログを取得する。
  - アクセス先URLと利用者ID
  - G社SaaSのファイルアップロード／ダウンロードのログと利用者ID
・社内PCからインターネットへのWebアクセスでは①プロキシサーバにおいて認証を行う。

〔G社SaaSの試用〕

F社は，G社SaaSの本格導入に先立って，本社と一つの営業所を対象に少数ライセンスでG社SaaSを試用し，システムの利便性と性能を確認することにした。試用に先立ち，G社SaaS以外のアクセス先について，プロキシサーバでHTTPSのアクセスログを確認したところ，②アクセス先のホスト名は記録されていたが，URLは記録されていなかった。そこで，アクセス先のURLを把握するために，プロキシサーバで暗号化通信を一旦復号し，必要な処理を行った上で再度暗号化した。しかし，

社内 PC でエラーメッセージ“証明書が信頼できない”が表示されたので，社内 PC に［　ウ　］をインストールして解決した。

G 社 SaaS を試用した結果，次の事実が判明した。

・G 社 SaaS にアクセスした際にプロキシサーバを通過するセッション数を実測したところ，スケジューラにアクセスする 1 人当たりのセッション数が大幅に増加した。

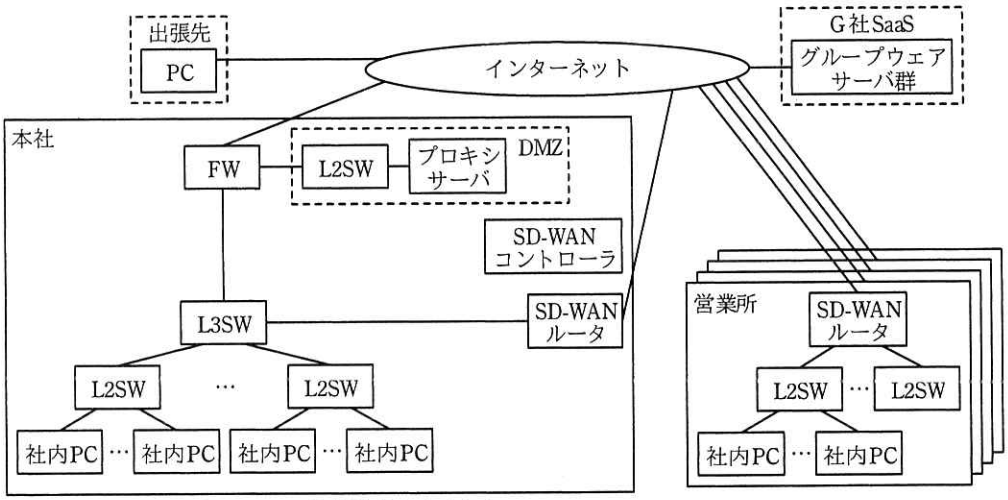
・複数人が同時に大容量のファイルを G 社 SaaS に転送している間，本社の FW を経由するインターネット接続回線のスループットが低下した。

このまま全社で G 社 SaaS の利用を開始すると，プロキシサーバの処理可能セッション数の超過，インターネット接続回線の帯域不足が予想された。

〔SD-WAN ルータの導入〕

F 社は，G 社 SaaS の試用で判明した問題を解決するために，IPsec ルータの代わりに SD-WAN（Software-Defined WAN）ルータを使用することにした。

SD-WAN ルータを使用したネットワーク構成案を，図 2 に示す。



注記　SD-WAN コントローラの接続構成は省略する。

図 2　SD-WAN ルータを使用したネットワーク構成案（抜粋）

(1) SD-WAN ルータの概要

今回使用する予定の SD-WAN ルータは，SDN（Software-Defined Networking）によって制御される IPsec ルータである。SDN は，利用者の通信トラフィックを転送するデータプレーンと，通信装置を集中制御する［　エ　］プレーンから構成されており，［　エ　］プレーンのソフトウェアでデータ転送を制御する方式である。

F 社が導入する SD-WAN ルータの仕様を次に示す。

・SD-WAN ルータの設定は，SD-WAN コントローラによって集中制御される。

・SD-WAN ルータの WAN 側には，インターネットに接続するインタフェースだけでなく，ほかの SD-WAN ルータに接続する IPsec VPN の論理インタフェースがある。

(2) SD-WAN ルータを用いたときの通信

図 2 の説明を次に示す。

・社内 PC から G 社 SaaS への Web アクセスは，プロキシサーバを経由せず各 SD-WAN ルータを経由する。

・社内 PC から G 社 SaaS 以外のインターネットへの Web アクセスは，プロキシサーバを経由する。

・L3SW にプロキシサーバへの静的経路情報を追加する。

・営業所と本社間の通信は，SD-WAN ルータ間で IPsec によって暗号化する。

・本社の社内 PC から G 社 SaaS への通信について，③G 社 SaaS の IP アドレスが変更された場合でもその都度 L3SW を設定しなくても済むように，L3SW の静的経路情報を設定変更する。

(3) SD-WAN ルータの運用

G 社は SaaS に必要なサーバを随時追加している。G 社 SaaS が利用している IP アドレスブロックの更新があるたびに，F 社は SD-WAN ルータの設定を変更する必要がある。F 社は，G 社 SaaS の IP アドレスブロックの更新を，RSS（Really Simple Syndication）を利用して知ることができる。

F 社は，RSS 配信された IP アドレスブロックを検知するツールを作成して，自動的にツールから［　オ　］に指示を行い，全社の SD-WAN ルータの設定を変更することにした。さらに，社内 PC から参照する④プロキシ自動設定ファイルを作

成することにした。

(4) G社SaaSアクセスログの取得

G社SaaSへのアクセスログは，⑤プロキシサーバからではなく，G社SaaSのAPIにアクセスして取得することにした。

F社は，G社SaaSの本格導入に向けてSD-WANルータを利用したネットワークの構築プロジェクトを立ち上げた。

設問1　〔F社の現行ネットワーク構成とG社SaaS導入に合わせたセキュリティ対策〕について，(1)，(2)に答えよ。

(1) 本文中の［　ア　］，［　イ　］に入れる適切な字句を答えよ。

(2) 本文中の下線①について，プロキシサーバで認証を行うことによってアクセスログに付加できる情報を答えよ。

設問2　〔G社SaaSの試用〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，HTTPSでアクセスするためのHTTPプロトコルのメソッド名を答えよ。また，このメソッドを用いる場合，社内に侵入したマルウェアによる通信（ただし，HTTPS以外の通信）を遮断するためのプロキシサーバでの対策を，30字以内で述べよ。

(2) 本文中の［　ウ　］に入れる適切な字句を，20字以内で答えよ。

設問3　〔SD-WANルータの導入〕について，(1)～(5)に答えよ。

(1) 本文中の［　エ　］に入れる適切な字句を答えよ。

(2) 本文中の下線③について，設定変更後の静的経路情報を，35字以内で答えよ。

(3) 本文中の［　オ　］に入れる適切な字句を，図2中の機器名で答えよ。

(4) 本文中の下線④について，このファイルを作成することによってプロキシから除外する通信を，20字以内で答えよ。

(5) 本文中の下線⑤について，G社SaaSのAPI経由で取得する理由を二つ挙げ，それぞれ40字以内で述べよ。