問５　セキュアWebゲートウェイサービスの導入に関する次の記述を読んで，設問に答えよ。

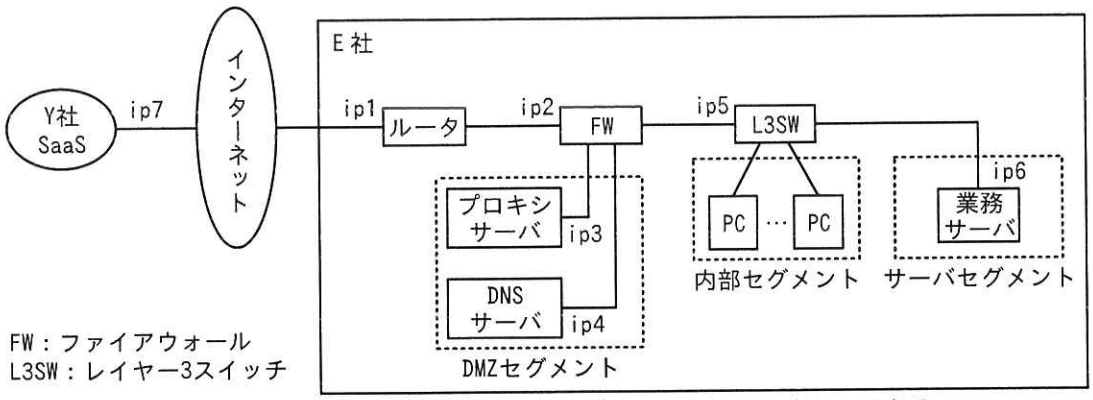
E社は，インターネットを利用した人材紹介業を営む会社である。

E社のネットワークは，DMZセグメント，内部セグメント及びサーバセグメントから構成されている。DMZセグメントには，コンテンツフィルタリング機能やWebサイトのアクセス制御機能をもつプロキシサーバ及びDNSサーバが設置されている。プロキシサーバでは，内部セグメントからインターネット向けのHTTP通信，HTTP Over TLS（以下，HTTPSという）通信を中継し，アクセスログを保管している。内部セグメントにはE社の従業員が利用するPCが，サーバセグメントには業務サーバが，それぞれ設置されている。

E社の従業員は，PCのWebブラウザを用いて，HTTP通信でサーバセグメントの業務サーバに直接アクセスして業務を実施したり，HTTPS通信でY社が提供するSaaS（以下，Y社SaaSという）にアクセスして，電子メールサービス，ファイル共有サービス，チャットサービスなどを活用したりしている。

〔E社のネットワーク構成〕

E社のネットワーク構成を，図1に示す。



注記　ip1，ip2，…，ip7はグローバル又はプライベートIPアドレスである。

図1　E社のネットワーク構成

E社のルータでは，［　a　］機能を用いて，E社内に割り当てられたプライベー

ト IP アドレスをグローバル IP アドレス及びポート番号に変換している。

Y 社 SaaS では，E 社からのアクセスに対して①送信元 IP アドレスでアクセス制限を行っている。

〔セキュア Web ゲートウェイサービスの導入検討〕

E 社では，近年の業務拡大に伴い，インターネット利用の機会が急激に拡大してきた。情報システム部の F 部長は，悪意のある Web サイトへ意図せずにアクセスしたり，社内の機密情報や顧客情報が漏えいしたりするおそれがあると考え，インターネットアクセスに対するセキュリティ対策を強化することにした。そこで，部下の G 主任に，社内のプロキシサーバに代えて，Z 社が SaaS として提供するセキュア Web ゲートウェイサービス（以下，サービス Z という）の導入検討を指示した。

〔サービス Z の概要〕

G 主任は，サービス Z の概要を調査した。

サービス Z は，PC からインターネット上の Web サイトへのアクセスを安全に行うためのサービスであり，主な機能は次の三つである。

(1) アクセス先の［ b ］や IP アドレスから悪意のある Web サイトであるかどうかを評価し，安全でないと評価された場合はアクセスを遮断する機能

(2) 機密情報や顧客情報が E 社外に漏えいしないように，TLS で暗号化された通信内容をサービス Z 内で復号して通信内容を検査し，これらの情報が含まれていないことを確認する機能

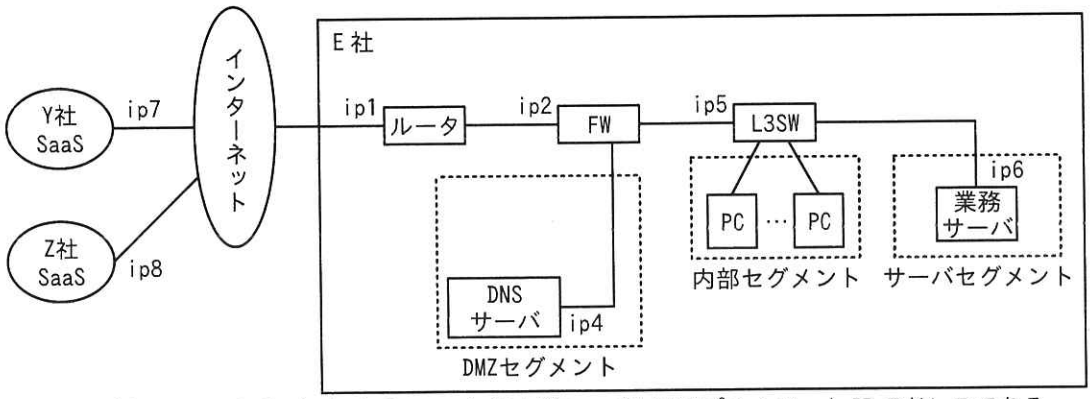
(3) ②インターネット上の Web サイトから受け取ったプログラムをサービス Z 内の保護された領域で動作させ，E 社システムが不正に操作されるおそれがないことを確認する機能

サービス Z を利用するためには，E 社の全ての PC に専用のクライアントソフトウェア（以下，ソフト C という）を導入し，PC の Web ブラウザからインターネット上の Web サイトへのアクセスを，ソフト C を介して行う必要がある。ソフト C からサービス Z には，HTTPS 通信を用いて接続する。サービス Z は，PC からインターネット上への全ての Web アクセスについて，どの PC からアクセスされたものかを識別して，ア

クセスの監視や各種制御を行う。

〔ネットワーク構成の変更〕

G 主任は，サービス Z の調査結果を基に，サービス Z 導入後の E 社のネットワーク構成案を図 2 のように考えた。



注記　ip1，ip2，ip4，ip5，…，ip8 はグローバル又はプライベート IP アドレスである。

図 2　サービス Z 導入後の E 社のネットワーク構成案

G 主任は，サービス Z 導入に当たって必要となる作業を検討し，次の四点に整理した。

(1)　現行の E 社のネットワーク構成からプロキシサーバを廃止し，社内の PC からインターネット上の Web サイトへのアクセスは，宛先 IP アドレスが［　c　］のものだけを許可するように，FW の許可ルールを変更する。

(2)　PC にソフト C を導入する。このソフト C は，各 PC 上でローカルプロキシとして動作する。各 PC のプロキシ設定を変更して，このソフト C をプロキシとして利用する。ソフト C から HTTPS 通信によってインターネット上の Web サイトへアクセスできるようにするために，［　c　］を宛先 IP アドレスとするようソフト C の通信設定を行う。

(3)　PC のプロキシ設定で，［　d　］については，これまでどおり直接 HTTP 通信ができるように設定する。

(4)　Y 社 SaaS の送信元 IP アドレスでのアクセス制限の設定を変更する。

〔FW の許可ルールの見直し〕

サービス Z 導入前の E 社 FW の許可ルールでは，PC の Web ブラウザからインターネットへの HTTP 通信や HTTPS 通信について，E 社プロキシサーバを経由する通信だけを許可する設定になっていた。

G 主任は，サービス Z 導入後に必要な FW の許可ルールを検討した。

サービス Z 導入前の E 社 FW の許可ルールを表 1 に，サービス Z 導入後の E 社 FW の許可ルールを表 2 に示す。なお，ルール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。

表 1　サービス Z 導入前の E 社 FW の許可ルール（抜粋）

項番	送信元	宛先	プロトコル名/ポート番号
1	内部セグメント	e	TCP/443
2	内部セグメント	e	TCP/80
3	e	インターネット	TCP/443
4	e	インターネット	TCP/80

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。

表 2　サービス Z 導入後の E 社 FW の許可ルール（抜粋）

項番	送信元	宛先	プロトコル名/ポート番号
1	内部セグメント	c	TCP/ f

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。

G 主任は，これまでの調査内容を F 部長に報告し，サービス Z の主な三つの機能を導入することになった。

設問1　〔E社のネットワーク構成〕について答えよ。

(1)　本文中の［　a　］に入れる適切な字句をアルファベット4字で答えよ。

(2)　本文中の下線①について，アクセスが許可される送信元IPアドレスを，図1中の字句を用いて答えよ。

設問2　〔サービスZの概要〕について答えよ。

(1)　本文中の［　b　］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②の機能の名称を解答群の中から選び，記号で答えよ。

解答群

ア　HTTPSデコード　　イ　アンチウイルス

ウ　サンドボックス　　エ　セキュアブラウジング

オ　トラフィック検査

設問3　〔ネットワーク構成の変更〕について答えよ。

(1)　本文及び表2中の［　c　］に入れる適切な字句を，図2中のIPアドレスを用いて答えよ。

(2)　本文中の［　d　］に入れる適切な字句を，図2中の機器の名称を用いて答えよ。

設問4　表1中の［　e　］，表2中の［　f　］に入れる適切な字句を，図1，図2又は表1中の字句を用いて答えよ。