問2　インターネット接続システムにおける迷惑メール対策に関する次の記述を読んで，設問1～4に答えよ。

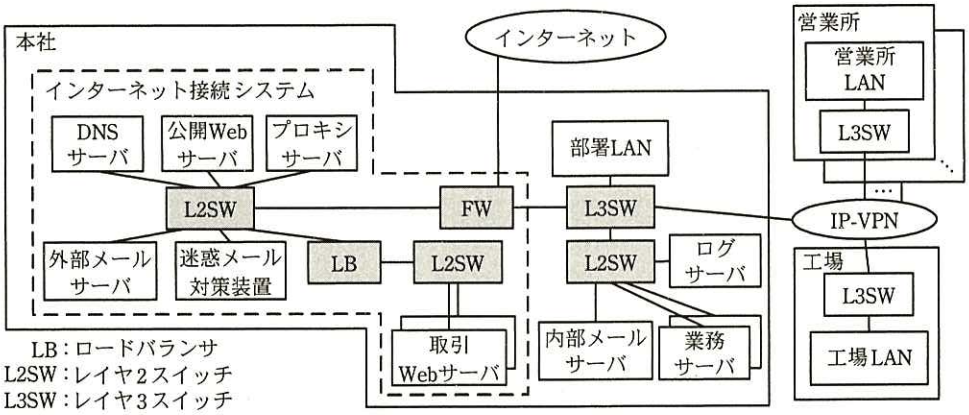
A社は，従業員数2,000名のスポーツ用品製造会社である。東京に本社，国内8か所に営業所，国内1か所に工場がある。A社では，本社にインターネット接続システムを導入し，電子メール（以下，メールという）やWeb閲覧などに利用している。本社，営業所及び工場のLANは，IP-VPNで接続されている。

〔インターネット接続システムの概要〕

インターネット接続システムの運用は，責任者である情報システム部のD部長の下で，E主任とFさんが担当している。インターネット接続システムの各サーバでは，サーバへのアクセス及びサーバ上でのプログラムの動作のログをログサーバに保存している。ログを収集，転送する方式には，UNIXで一般的に使われている［　a　］というプロトコルを利用している。ファイアウォール（以下，FWという）では，拒否した通信のログを保存している。

A社では，ドメイン名a-sha.co.jp（以下，A社ドメイン名という）を取得している。メールアドレスのドメイン名にはA社ドメイン名を使用している。

A社のネットワーク構成を図1に，インターネット接続システムの主な機器と機能概要を表1に示す。



注記1　A社のPCは全て，部署LAN，営業所LAN又は工場LANのいずれかに接続している。
注記2　PCの記載は省略している。
注記3　網掛けの機器は二重化している。

図1　A社のネットワーク構成

表１　インターネット接続システムの主な機器と機能概要

機器名称	機能概要
LB	HTTP，SMTP などのサービスの振分け機能及び IP アドレス変換機能がある。送信元 IP アドレスによって，振分け機能及び IP アドレス変換機能を使用しない設定もできる。
迷惑メール対策装置	インターネットから内部メールサーバへのメール転送機能，迷惑メールフィルタリング機能及びメールに対するウイルススキャン機能がある。迷惑メール対策装置のベンダの Web サーバから 1 時間ごとにウイルス定義ファイルをダウンロードし，更新する。
外部メールサーバ	内部メールサーバからインターネットへのメール転送機能及びメールに対するウイルススキャン機能がある。迷惑メール対策装置の故障に備えて，インターネットから内部メールサーバへのメール転送も行うことができる。ウイルス対策ソフトのベンダの Web サーバから 1 時間ごとにウイルス定義ファイルをダウンロードし，更新する。
プロキシサーバ	プロキシ機能，Web コンテンツキャッシュ機能，URL フィルタリング機能及び Web コンテンツに対するウイルススキャン機能がある。プロキシソフトのベンダの Web サーバから 1 時間ごとに URL フィルタリング定義ファイル及びウイルス定義ファイルをダウンロードし，更新する。サーバ管理者の URL の登録によって URL フィルタリングを行うことができるプロキシブラックリスト（以下，ブラックリストを BL という）がある。
取引 Web サーバ	販売店からの注文受付機能がある。注文情報は業務サーバに保存される。

インターネット接続システムでは，迷惑メール対策装置及び外部メールサーバだけがメールを扱う。

FW はステートフルパケットフィルタリング型である。その FW のルールを表 2 に示す。

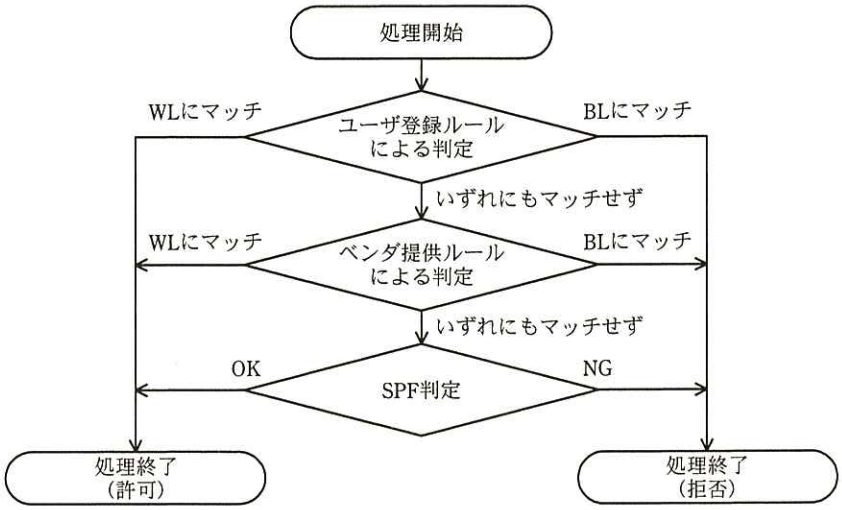
表２　FW のルール

項番	送信元	宛先	サービス	動作
1	インターネット	迷惑メール対策装置	SMTP	許可
2	インターネット	外部メールサーバ	SMTP	許可
3	迷惑メール対策装置	内部メールサーバ	SMTP	許可
4	外部メールサーバ	インターネット	SMTP	許可
5	外部メールサーバ	内部メールサーバ	SMTP	許可
6	内部メールサーバ	外部メールサーバ	SMTP	許可
⋮	⋮	⋮	⋮	⋮
25	全て	全て	全て	拒否

注記１　項番が小さいルールから順に，最初に一致したルールが適用される。
注記２　項番 7～24 は，SMTP に関連しないルールである。

迷惑メール対策装置は，図 2 に示すようにメールの転送に関する情報及びメールの

内容を検査し，転送を許可又は拒否する。転送の許可又は拒否の判定に用いられるルールには，利用者が設定可能な“ユーザ登録ルール”と，迷惑メール対策装置のベンダから提供される“ベンダ提供ルール”があり，これらのルールを利用した判定に加え，SPF（Sender Policy Framework）を利用して判定する“SPF 判定”がある。



WL ： ホワイトリスト

注記 WL と BL の優先度については表 3 を参照

図 2　迷惑メール対策装置における判定処理

ユーザ登録ルールとベンダ提供ルールはそれぞれ表 3 に示す WL 及び BL から構成される。ユーザ登録ルールの各リストへの登録は，社内からの要望を情報システム部が受け付け，サーバ管理者である F さんが行っている。ベンダ提供ルールは，迷惑メール対策装置のベンダの Web サーバから 1 時間ごとにダウンロードして更新される。ベンダ提供ルールの具体的な内容は，開示されていない。

表3　ユーザ登録ルールとベンダ提供ルール

項番	ルール種別	形式	マッチング対象
1	IP アドレス WL	IP アドレスの並び	メールの送信元 IP アドレス
2	IP アドレス BL	IP アドレスの並び	メールの送信元 IP アドレス
3	ドメイン名 WL	ドメイン名の並び	エンベロープの送信者メールアドレスのドメイン名
4	ドメイン名 BL	ドメイン名の並び	エンベロープの送信者メールアドレスのドメイン名
5	URL BL	URL の並び	ヘッダ及びメール本文中に含まれる URL
6	単語 BL	単語の並び	ヘッダ及びメール本文中に含まれる単語

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

A 社のメールアドレスを使ったなりすましを防ぐために，A 社の DNS サーバで SPF の設定を行っている。A 社のメールアドレスを使ったメールを送信するのは外部メールサーバだけである。メールに関する DNS の設定を図 3 に示す。

```
msv1.a-sha.co.jp.   IN A x1.y1.z1.3
msv2.a-sha.co.jp.   IN A x1.y1.z1.4
a-sha.co.jp.        IN MX 10 msv1.a-sha.co.jp.
a-sha.co.jp.        IN MX 20 msv2.a-sha.co.jp.
a-sha.co.jp.        IN TXT "v=spf1 +ip4:x1.y1.z1.4 [   b   ] "
```

注記 1　x1.y1.z1.3 は迷惑メール対策装置の IP アドレス，x1.y1.z1.4 は外部メールサーバの IP アドレスである。

注記 2　逆引き定義は省略しているが，適切に設定されている。

図3　メールに関する DNS の設定

〔迷惑メールの増加の調査〕

先週，“2 週間前から，社外が送信元とみられる迷惑メールが増加している”と営業部から情報システム部に連絡があった。D 部長は，E 主任と F さんに調査を指示した。調査したところ，全ての機器は設定どおり動作していた。次に，ログサーバに保存されているログを調査したところ，①迷惑メールが外部メールサーバから内部メールサーバに転送されており，2 週間前からその数が増加していた。

報告を受けた D 部長は，E 主任と F さんに迷惑メール対策装置のユーザ登録ルールの見直しを行ってから，今回の迷惑メールの増加への対策を行うよう指示した。

〔迷惑メール対策装置のユーザ登録ルールの見直し〕

E 主任と F さんは，迷惑メール対策装置のユーザ登録ルール全般を見直すことにし

た。

まず，IP アドレス WL と IP アドレス BL への登録の効果の持続性について検討した。たとえ取引先の IP アドレスを IP アドレス WL に登録していたとしても，メールが急に届かなくなる可能性もある。届かなくなった場合は，IP アドレス WL の登録内容を見直す必要がある。そこで，F さんは，IP アドレス WL の登録内容の見直し方法を運用手順に追加した。

次に，ドメイン名 WL とドメイン名 BL への登録について検討した。F さんは，SPF 判定があれば，ドメイン名 WL とドメイン名 BL への登録は不要ではないかと E 主任に質問した。E 主任は，“SPF を使えばドメイン名を詐称する迷惑メールの拒否が可能である。しかし，②迷惑メール送信者の行為によっては，迷惑メール対策装置が SPF を使って正しいと判定したサーバから送信された迷惑メールを防ぐことができないので必要である”と，F さんに説明した。

さらに，URL BL について検討した。F さんは，③ [c] に登録する設定を URL BL にも登録することを提案し，効果があることを説明した。この提案には，E 主任も同意した。

最後に，単語 BL について検討し，現状のままでも問題がないことを確認した。

〔迷惑メールの増加への対策の検討〕

E 主任と F さんは，迷惑メールの増加への対策について検討した。検討の結果，④図 1 のネットワーク構成と LB の設定を変更することで，インターネット上のメールサーバからの SMTP 通信を制御することにした。さらに，表 2 のルール及び図 3 の設定を LB による制御に対応するように変更することにした。

E 主任と F さんは，検討した対策を D 部長に報告し，了承を得た。D 部長は，この対策で従業員に届く迷惑メールの減少が期待できるものの，迷惑メール対策装置だけでは，防ぐことができない迷惑メールがあるので，次の 2 点を周知するように指示した。

・不審なメールの添付ファイルを開かない。

・不審なメール中の URL をクリックしない。

指示を受けたE主任とFさんは，設定の変更と従業員への周知を行った。

これらの対処によって，従業員に届く迷惑メールが減少するとともに，不審なメールに対する従業員の対処が定着した。

設問1　〔インターネット接続システムの概要〕について，(1)，(2) に答えよ。

(1)　本文中の [a] に入れる適切な字句を，英字8字以内で答えよ。

(2)　図3中の [b] に入れる適切な字句を，英字及び記号5字以内で答えよ。

設問2　本文中の下線①について，増加した迷惑メールは，外部メールサーバにどのように送られていたか。表2のルール及び図3の設定を考慮して，35字以内で述べよ。

設問3　〔迷惑メール対策装置のユーザ登録ルールの見直し〕について，(1)～(3) に答えよ。

(1)　IPアドレスWLを見直す必要があるのは，取引先でどのような事象が発生した場合か。25字以内で具体的に述べよ。

(2)　本文中の下線②について，迷惑メールを防ぐことができなくなる迷惑メール送信者の行為を，30字以内で述べよ。

(3)　本文中の [c] に入れる適切な機器名を図1中から選び，答えよ。また，本文中の下線③における，登録の効果とは何か。15字以内で述べよ。

設問4　本文中の下線④について，迷惑メール対策装置が正常に稼働している場合，SMTP通信をどのように制御すべきか。30字以内で具体的に述べよ。