問1　メールシステムの情報セキュリティ対策に関する次の記述を読んで，設問1～5に答えよ。

P社は，従業員数300名のソフトウェア開発会社である。P社の主要事業は，ソフトウェア製品の開発及びWebアプリケーションの受託開発である。P社には，人事総務部，情報システム部，営業部及びシステム開発部がある。

P社のネットワーク構成を図1に示す。

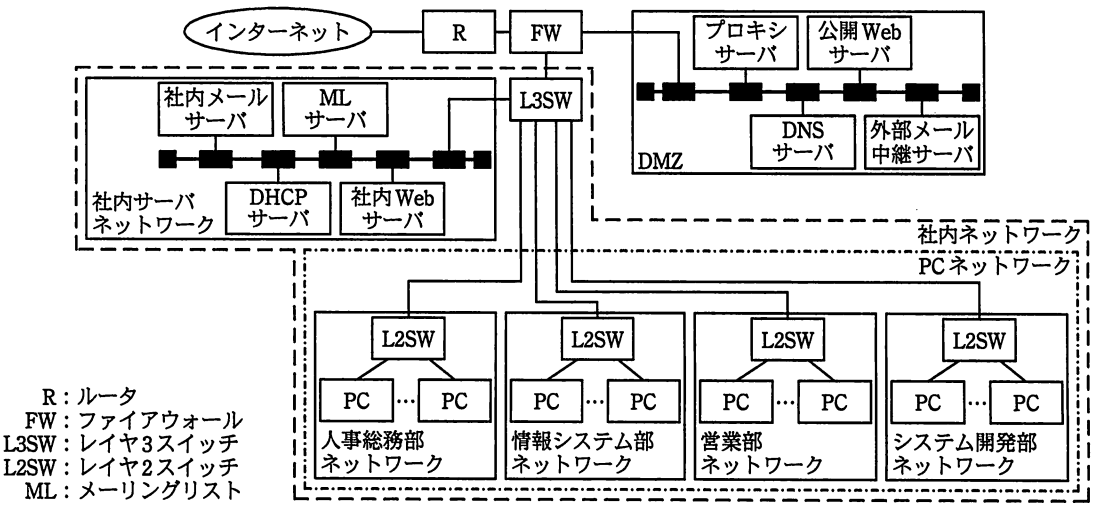


**図1　P社のネットワーク構成**

PCは，PCネットワークだけに接続されている。PCへのIPアドレス割当ては，DHCPサーバ及びL3SWのDHCPリレーエージェント機能によって行われる。PCは，従業員がソフトウェア開発，資料作成，社内Webサーバへのアクセス，電子メール（以下，メールという）の送受信及びプロキシサーバ経由でのインターネットWebサイトの閲覧に使用している。P社では，各開発プロジェクト（以下，プロジェクトという）内の連絡にMLサーバを使用している。

FWのフィルタリングルール（以下，FWルールという）では，通信の送信元，あて先及びサービスの組合せによって，通信の許可又は拒否を指定している。FWルールを表1に示す。

FWでは，通信の許可及び拒否の状況をログとして記録している。各サーバでは，アクセス及びプログラムの動作結果をログとして記録している。

表1　FWルール

| 項番 | 送信元 | あて先 | サービス | 動作 |
|---|---|---|---|---|
| 1 | インターネット | 外部メール中継サーバ | SMTP | 許可 |
| 2 | 外部メール中継サーバ | インターネット | SMTP | 許可 |
| 3 | 外部メール中継サーバ | 社内メールサーバ | SMTP | 許可 |
| 4 | 社内メールサーバ | 外部メール中継サーバ | SMTP | 許可 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 18 | すべて | すべて | すべて | 拒否 |

注記1　項番の小さいものから順に，最初に一致したルールが適用される。
注記2　項番5～17のFWルールは，SMTPに関連しないものである。

〔メールシステムの概要〕

P社のメールシステムのサーバには，外部メール中継サーバ，社内メールサーバ及びMLサーバがある。それ以外のサーバ及びFWでは，サーバ管理にメールを使用しているが，社外へのメールの送信は行わない。

P社のメールアドレスのドメイン名には，P社が取得したドメイン名（以下，P社ドメイン名又はp-sha.co.jpという）及びそのサブドメイン名（以下，P社サブドメイン名という）を使用している。P社ドメイン名は，各従業員に割り当てる従業員用メールアドレスのドメイン名と，postmasterやwebmasterなどをメールアドレスのローカル部として使用するサーバ管理用メールアドレスのドメイン名に使用している。P社サブドメイン名は，MLアドレス用のドメイン名として使用する。MLアドレス用のドメイン名として，複数のP社サブドメイン名の使用が可能である。現在は一つだけ作成し，使用している。P社のメールアドレスのドメイン名及びメールアドレスは表2のとおりである。表2に基づいてDNSサーバのSPF（Sender Policy Framework）設定も行っている。

C
後II

表2　P社のメールアドレスのドメイン名及びメールアドレス

| 種別 | メールアドレスのドメイン名 | メールアドレス |
|---|---|---|
| 従業員用メールアドレス及びサーバ管理用メールアドレス | p-sha.co.jp | *user*@p-sha.co.jp [1] |
| MLアドレス | ml01.p-sha.co.jp | *project*@ml01.p-sha.co.jp [2] |

注 [1] *user*は利用者やサーバ管理用途によって異なる。
[2] *project*はプロジェクトによって異なる。

外部メール中継サーバ，社内メールサーバ及び ML サーバには，オープンリレー対策が導入されている。オープンリレー対策では，表 3 に示すように，SMTP の転送元の IP アドレス又は IP アドレスブロック（以下，転送元 IP アドレスという）とメールの受信者ドメイン名の二つの組合せで，転送の許可又は拒否を判定する。受信者ドメイン名は，メールのエンベロープの受信者メールアドレスのドメイン名部分である。各メールサーバには，転送元 IP アドレスのうち受信者ドメイン名にかかわらずメールの転送を許可するもの（以下，許可アドレスリストという）が，登録されている。

**表 3　オープンリレー対策**

| 転送元 IP アドレス | 受信者ドメイン名 | 処理 |
|---|---|---|
| 許可アドレスリスト中のアドレス | 社外のドメイン名 | 転送許可 |
| | P 社ドメイン名<br>P 社サブドメイン名 | 転送許可 |
| 許可アドレスリスト以外のアドレス | 社外のドメイン名 | 転送拒否 |
| | P 社ドメイン名<br>P 社サブドメイン名 | 転送許可 |

社内メールサーバの許可アドレスリストには，PC ネットワークの IP アドレスブロックが登録されている。

転送が許可されたメールは，表 4 に示すように受信者ドメイン名ごとの処理が行われる。

**表 4　メールシステムの受信者ドメイン名ごとの処理**

| 項番 | サーバ | 受信者ドメイン名 | 処理 |
|---|---|---|---|
| 1 | 外部メール中継サーバ | P 社ドメイン名 | 社内メールサーバに転送 |
| 2 | | 社外のドメイン名 | DNS に登録されているメールサーバに転送 |
| 3 | | 上記以外のドメイン名 | 転送を拒否 |
| 4 | 社内メールサーバ | P 社ドメイン名 | メールボックス保存プログラムに転送 |
| 5 | | P 社サブドメイン名 | ML サーバに転送 |
| 6 | | 社外のドメイン名 | 外部メール中継サーバに転送 |
| 7 | | 上記以外のドメイン名 | 転送を拒否 |
| 8 | ML サーバ | P 社ドメイン名 | 社内メールサーバに転送 |
| 9 | | P 社サブドメイン名 | 同報プログラムに転送 |
| 10 | | 上記以外のドメイン名 | 転送を拒否 |

社内メールサーバ及び PC にはウイルス対策ソフトが導入されている。社内メールサーバでのメール及びウイルス対策に関連した処理，並びに PC でのメール送受信処理は図2のとおりである。

(1) 社内メールサーバでのメール転送

[ a ] は，SMTP を使用し，メールを転送する。[ a ] のメール転送中に，ウイルス対策ソフトのウイルススキャン（以下，SMTP スキャンという）を行う。SMTP スキャンでウイルスを検知した場合，メール本文をウイルス検知通知に置き換える。次に，受信者ドメイン名ごとの処理を行う。

(2) 社内メールサーバでのメールボックス保存

P 社ドメイン名あてのメールは，メールボックス保存プログラムである [ b ] によって，従業員用メールアドレス又はサーバ管理用メールアドレスごとのメールボックスに保存される。

(3) PC でのメール送受信

・メール送信

次の二つのどちらかを使用可能であるが，P 社の PC では (a) を使用している。

(a) PC の [ c ] は，SMTP で 25 番ポートを使用し，社内メールサーバの [ a ] にメールを送信する。

(b) PC の [ c ] は，SMTP で 587 番ポートを使用し，社内メールサーバの [ d ] にメールを送信し，[ d ] は，[ a ] にメールを転送する。

・メール受信

PC の [ c ] は，POP3 を使用し，社内メールサーバの MRA（Mail Retrieval Agent）と通信し，従業員用メールアドレス又はサーバ管理用メールアドレスのメールボックスからメールを取り出す。

MRA のメール取り出し中に，ウイルス対策ソフトのウイルススキャン（以下，POP3 スキャンという）を行うことも可能である。POP3 スキャンでウイルスを検知した場合，メール本文をウイルス検知通知に置き換える。しかし，PC のウイルス対策ソフトに同等機能があるので POP3 スキャンを使用していない。

(4) 社内メールサーバのウイルス対策ソフトのウイルス定義ファイル更新

15 分おきに，次の処理を自動的に実行する。

・プロキシサーバ経由で，インターネット上のウイルス対策ソフトベンダの Web サーバに未更新ウイルス定義ファイルがあるかを確認し，未更新ウイルス定義ファイルがある場合はダウンロードを行い，更新を行う。

この処理は，手動による実行も可能である。プロキシサーバでは，キャッシュする対象からウイルス対策ソフトベンダの Web サーバを外している。

**図2　社内メールサーバ及び PC での処理**

ML の管理及び処理は図3のとおりである。

・プロジェクトごとにMLアドレスを割り当てる。
・プロジェクト開始時に，プロジェクト管理者は情報システム部にMLアドレスの割当てを申請する。情報システム部は，MLアドレス及びMLアドレスごとの管理機能の利用者ID（以下，MLアドレス管理者IDという）とパスワードを設定して，プロジェクト管理者に通知する。
・プロジェクト管理者は，MLアドレスの管理機能を使用し，同報する受信者メールアドレス（以下，同報メールアドレスという）を同報リストに登録する。同報メールアドレスとして，従業員用メールアドレスだけが登録可能である。
・プロジェクト終了時に，プロジェクト管理者は情報システム部にMLアドレスの削除を申請する。情報システム部は，MLアドレス，MLアドレス管理者ID及び同報リストを削除する。
・MLサーバにMLアドレスあてのメールが届くと，同報プログラムが起動される。同報プログラムは，エンベロープの受信者メールアドレスをMLアドレスの同報リストの各同報メールアドレスに書き換えたメールを生成する。生成したメールを，SMTPを使用して社内メールサーバに転送する。

**図3　MLの管理及び処理**

同報プログラムには，設定可能な項目があり，それら設定項目と現在の設定値は，表5のとおりである。

**表5　同報プログラムの設定項目と現在の設定値**

| 設定項目名 | 説明 | 現在の設定値 |
|---|---|---|
| MLアドレス管理者のメールアドレス | 次のいずれかを選択する。<br>・*project*-admin@p-sha.co.jp [1)]<br>・プロジェクト管理者の従業員用メールアドレス | プロジェクト管理者の従業員用メールアドレス |
| エンベロープの送信者メールアドレス | 次のいずれかを選択する。<br>・同報前のメールのエンベロープの送信者メールアドレス<br>・MLアドレス管理者のメールアドレス | 同報前のメールのエンベロープの送信者メールアドレス |
| 登録外メールアドレス制限 | 同報前のメールのヘッダの送信者メールアドレスが，登録された同報メールアドレス以外の場合にメールの同報を拒否する設定が可能である。 | 拒否する。 |
| メールサイズ上限制限 | あらかじめ設定した値を超える大きさのメールの同報拒否が可能である。 | 10Mバイト |

注 [1)] *project*はプロジェクトごとに異なる。

〔PCの情報セキュリティ対策〕

PCには，表6に示す機能をもつウイルス対策ソフトが導入されている。PC配布時には，各機能を利用できるように設定されている。

表6　PCのウイルス対策ソフトの機能

| 機能の名称 | 機能の概要 |
|---|---|
| ウイルス定義ファイル更新 | PC起動時及びその後1時間ごとに，次の処理を自動的に実行する。<br>・プロキシサーバ経由で，インターネット上のウイルス対策ソフトベンダのWebサーバに未更新ウイルス定義ファイルがあるかを確認し，未更新ウイルス定義ファイルがある場合はダウンロードを行い，更新を行う。<br>この処理は，手動での実行も可能である。 |
| 定時スキャン | 毎日，決められた時刻にPCの全ファイルのウイルススキャンを行う。ウイルスを検知した場合，ウイルスの駆除及びファイルの修復を行う。P社では，正午に実行される。 |
| メール送信スキャン | PCのメールソフトと連携し，メール送信時にウイルススキャンを行う。ウイルスを検知した場合，その通信を遮断する。 |
| メール受信スキャン | PCのメールソフトと連携し，メール受信時にウイルススキャンを行う。ウイルスを検知した場合，メール本文をウイルス検知通知に置き換える。 |
| ⋮ | ⋮ |

P社では，他社におけるメールアドレスの誤入力による情報漏えい事故の報道をきっかけに，情報漏えい対策の強化が必要であると認識し，情報システム部で対策を検討することにした。検討の結果，メールによる情報漏えいを防止する対策の一つとして，PCのメールソフトに装備されているあて先確認要求機能を使用することにした。この機能は図4のとおりである。

・環境設定
　あて先確認要求なしにメールの送信を許可するドメイン名（以下，許可済ドメイン名という）を社内Webサーバに設定しておく。現在の許可済ドメイン名は表2のメールアドレスのドメイン名とすることにした。
・メールソフト起動時の処理
　メールソフト起動時に，社内Webサーバから許可済ドメイン名をダウンロードし，PCに保存する。社内Webサーバと通信ができない場合は，PCに許可済ドメイン名が保存されていたなら，それを参照する。
・メール送信時の処理
　メール送信時に，メールに入力した受信者メールアドレスのドメイン名と許可済ドメイン名とを照合する。一致した場合は，メールを送信する。一致しなかった場合は，受信者メールアドレスの確認を促すメッセージを表示する。確認ボタンを押すとメールを送信する。取消ボタンを押すと，メール編集画面に戻る。

図4　メールソフトに装備されているあて先確認要求機能

〔PCのリプレースとメールソフト誤設定に関する対策の検討〕

情報システム部では，PCのリース期間満了に合わせ，部ごとにPCのリプレースを行っている。

人事総務部のPCのリプレースでは，新しいPCの導入並びにOS及びソフトウェアの設定に用いる手順書（以下，PC導入手順書という）を情報システム部が作成した後，PCの納入ベンダがPC導入手順書に基づいてPCの導入を行い，人事総務部がパスワードの設定を行った。

人事総務部のPCのリプレースが完了した翌日，人事総務部のSさんから情報システム部に，“午前中にメールを1通送信したが，相手に届いたメールの送信者メールアドレスが，人事総務部のAさんとなっていた”との申告があった。情報システム部のL部長は，部下のM主任とNさんに調査を指示した。M主任とNさんは，DHCPサーバのログ及びAさんとSさんのメールアドレスを調査した。続いて，①メールシステムのサーバのログを調査し，Sさんの申告どおりであることを確認した。さらに，SさんのPCの調査を行った。調査結果を図5に示す。

(1) DHCPサーバのログ
Sさんの PCに割り当てたIPアドレスを特定した。
(2) メールアドレス
Aさん　ato.taro@p-sha.co.jp
Sさん　sato.taro@p-sha.co.jp
(3) メールシステムのサーバのログ
（省略）
(4) SさんのPCの調査結果
PCのメールソフトの送信者メールアドレスの設定において，Aさんのメールアドレスが設定されていた。納入ベンダに確認したところ，メールアドレス設定ツールで使用する設定情報一覧の作成時に，Sさんのメールアドレスの先頭の“s”の入力が漏れ，一覧作成後の確認においても入力ミスを発見できなかったとの説明であった。

**図5　調査結果**

M主任とNさんは，調査結果，対策及び再発防止策をL部長に報告し，対策及び再発防止策は実施された。

〔ウイルス感染とその対策に関する検討〕

大型連休明け，営業部長からL部長に，“BさんのPCがウイルス感染した可能性があり，ネットワークから切り離した”との連絡があった。L部長は，M主任とNさんに調査を指示した。M主任とNさんは，PCの調査と対処を行った。調査結果と対処を図6に示す。

(1) Bさんへの聴取結果
午前8時40分ごろ　PCをロッカーから取り出し，起動した後，席を離れた。
午前8時50分ごろ　自席に戻り，PCを営業部ネットワークに接続した。
午前9時20分ごろ　メールを受信した。
午前9時30分ごろ　受信したメールのうち，題名に“メールソフトについての重要なお知らせ”と書かれたメールを同僚のCさんのメールアドレスあてに，メールソフトの転送機能を使用して送信した。
午前9時55分ごろ　Cさんから“Bさんが送信したメールがウイルス検知通知メールに置き換わって届いた”と電話連絡があった。
(2) BさんのPCのウイルス対策ソフトの設定
PC配布後，Bさんは，メールの送信及び受信が遅いという理由で，メール送信スキャン機能及びメール受信スキャン機能を使用しない設定に変更していた。
(3) DMZ及び社内サーバネットワークに設置されているサーバ群のログ調査結果
午前8時50分　BさんのPCに営業部ネットワーク用のIPアドレスを割り当てた。
午前9時20分　同IPアドレスで，メール受信が行われた。
午前9時30分　同IPアドレスからメール送信が行われ，社内メールサーバでSMTPスキャンが動作した。
午前9時40分　②同IPアドレスからのリクエストで，ウイルス定義ファイルのダウンロードが行われた。
(4) ウイルス感染
当該メールには，Xウイルスが添付されており，Bさんの PC はこのメールの受信時に X ウイルスに感染した。Xウイルスに対応したウイルス定義ファイルは，大型連休最終日にリリースされていた。
(5) 対処
緊急対応ツールによってXウイルスの駆除とファイルの修復を行った。さらに，メール送信スキャン機能とメール受信スキャン機能を使用するよう設定した。
Xウイルスに関する注意喚起情報を社内Webサーバに掲載した。

**図6　BさんのPCの調査結果と対処**

M主任とNさんは，情報セキュリティ対策についての支援を委託しているT社のU氏に調査結果と対処を説明し，対策についての助言を求めた。N さんは，今後の対策として，PC の利用に当たって，PC を起動後，メール受信前に手動でウイルス定義ファイル更新をさせようと考えていることを説明した。U氏は，③PCでの対策以外に，メールシステムのサーバでの対策もあると助言した。この助言に従い，N さんは新たな対策案を作成した。

M主任とNさんは，調査結果，対処及び新たな対策案をL部長に報告し，対策は即日実施された。

〔MLに関する検討〕

システム開発部では，あるプロジェクトで受託開発の一部を協力会社に再委託することになり，協力会社との間でプロジェクトにおいて扱うドキュメントなどのファイルを暗号化して送受信するために，同報メールアドレスに協力会社のメンバのメール

アドレスも登録可能にしてほしいという要望が，システム開発部長から L 部長に伝えられた。L 部長は，M 主任と N さんに社外メンバのメールアドレスも登録可能な ML（以下，社外メンバ登録 ML という）の検討を指示した。

M 主任と N さんは，要望内容と表 4 を基に検討を行い，表 7 のメールシステムの受信者ドメイン名ごとの処理変更案を作成し，U 氏に相談した。P 社のシステムにほかの変更はない。

**表 7　メールシステムの受信者ドメイン名ごとの処理変更案**

| 項番 | サーバ | 受信者ドメイン名 | 処理 |
|---|---|---|---|
| 1 | 外部メール中継サーバ | P 社ドメイン名 | 社内メールサーバに転送 |
| 2 | | P 社サブドメイン名 | ML サーバに転送 |
| 3 | | 社外のドメイン名 | DNS に登録されているメールサーバに転送 |
| 4 | | 上記以外のドメイン名 | 転送を拒否 |
| 5 | 社内メールサーバ | P 社ドメイン名 | メールボックス保存プログラムに転送 |
| 6 | | P 社サブドメイン名 | ML サーバに転送 |
| 7 | | 社外のドメイン名 | 外部メール中継サーバに転送 |
| 8 | | 上記以外のドメイン名 | 転送を拒否 |
| 9 | ML サーバ | P 社ドメイン名 | 社内メールサーバに転送 |
| 10 | | P 社サブドメイン名 | 同報プログラムに転送 |
| 11 | | 社外のドメイン名 | 外部メール中継サーバに転送 |
| 12 | | 上記以外のドメイン名 | 転送を拒否 |

U 氏は，M 主任と N さんの考えも聞きながら，表 7 のメールシステムの受信者ドメイン名ごとの処理変更案を基にレビューし，指摘事項を図 7 にまとめた。

(A)　あて先確認要求機能について
　メールソフトでは社外メンバ登録 ML アドレスあて送信時に，あて先確認要求なしにメールが送信される。
(B)　メールシステムの受信者ドメイン名ごとの処理変更案について
　表 7 には，誤りがある。
(C)　ウイルス対策について
　社外メンバ登録 ML で同報されたメールがウイルスに感染していた場合に，同報リストに登録された協力会社のメンバに連絡する手段が決められていない。
(D)　迷惑メールと判定されることについて
　協力会社のメールサーバが，迷惑メールの判定に SPF を使用している場合，P 社からのメールが迷惑メールと判定されることがある。

**図 7　指摘事項**

まず，M主任とNさんは，図7の(A)について検討し，④メールアドレスのドメイン名の使用方法も含めてMLサーバの設定を見直すとともに，社内Webサーバでの許可済ドメイン名の設定ルールとして明示する案を作成した。さらに，この見直しに伴うDNSサーバのSPF設定の変更は不要であることを確認した。U氏は，図7の(A)が解決されることを確認した。

次に，M主任とNさんは，図7の(B)について検討し，⑤表7の処理を2か所修正し，社内メールサーバの許可アドレスリストに［　e　］のIPアドレスを追加する案を作成した。U氏は，図7の(B)が解決されることを確認した。

続いて，M主任とNさんは図7の(C)について検討し，連絡手段をメールとする案を作成した。U氏は，⑥連絡手段をメール以外の方法とするように助言した。M主任とNさんは，U氏の助言に従い，発信者番号を通知した電話で連絡する案に修正した。

さらに，M主任とNさんは図7の(D)について協力会社でのSPF利用状況について確認し，問題があるということが分かったので，対策を検討し，⑦MLサーバの設定を変更する対策案を作成した。U氏は，図7の(D)が解決されることを確認した。

M主任とNさんは，社外メンバ登録MLの実現案をL部長に説明した。L部長は，システム開発部には複数のプロジェクトを担当している部員がいるので，社外メンバ登録MLアドレスの取り違えによるメールの誤送信が起こる可能性があると指摘した。プロジェクトにおける情報交換での情報漏えい対策（以下，情報交換対策という）も併せて導入する条件で社外メンバ登録MLの実現案を承認した。

〔情報交換対策に関する検討〕

M主任とNさんはU氏とともに，情報交換対策の検討を行った。U氏は，P社のメールシステムにおいては，社外メンバ登録MLアドレスの取り違えによるメールの誤送信の防止が難しいことを指摘した。

検討の結果，次のような案を作成した。

社外メンバ登録MLアドレスは，プロジェクトでの連絡手段としてだけ使用させ，ドキュメントなど重要情報の送信には使用させない。そこで，社外メンバ登録MLアドレスあてのメールにファイルが添付されていたら，転送を拒否する機能をメールシステムに設定する。

メールによる情報交換の代替手段として，情報交換のためのWebサーバ（以下，

PJWeb サーバという）を DMZ に導入する。PJWeb サーバでは，利用者の認証を行い，ドキュメントなどのアップロード及びダウンロードによる情報交換を実現する。加えて，アクセス状況をログとして記録する。PJWeb サーバへの通信を FW で制限する。⑧これらのほかに，メールシステムの機能及び利用計画を踏まえ，PJWeb サーバに必要な情報セキュリティ機能を追加する。

PJWeb サーバの運用は，次のようにする。

プロジェクト管理者は，プロジェクト開始時にプロジェクトの名称，期間，協力会社情報，メンバなどのプロジェクト情報を添えて登録申請を行い，プロジェクト終了時に削除申請を行う。情報システム部は，申請内容に基づき，PJWeb サーバへの利用者 ID，パスワード及び格納領域の登録又は削除設定を行う。さらに，DMZ に設置されているサーバと同様に，定期的な PJWeb サーバの脆弱性検査及び修正プログラムの適用を行う。⑨これらのほかに，情報システム部は，PJWeb サーバの情報セキュリティ対策にかかわる運用も行う。

M 主任と N さんは，この情報交換対策案を L 部長に説明し，承認を得た。3 か月後，情報交換対策は導入され，社外メンバ登録 ML の運用が開始された。

**設問 1**　〔メールシステムの概要〕について，図 2 中の［ a ］～［ d ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　MDA（Mail Delivery Agent）　　イ　MSA（Mail Submission Agent）

ウ　MTA（Mail Transfer Agent）　　エ　MUA（Mail User Agent）

**設問 2**　〔PC のリプレースとメールソフト誤設定に関する対策の検討〕について，(1)，(2) に答えよ。

(1) PC のメールソフトの送信者メールアドレスを誤って設定しても，社内メールサーバが PC のメールソフトからのメールの送信を拒否しない理由を，40 字以内で述べよ。

(2) 本文中の下線①のログ調査結果を得るために調査したサーバの名称を図 1 中の字句を用いて答えよ。また，確認した内容を 50 字以内で述べよ。

**設問3**　〔ウイルス感染とその対策に関する検討〕について，(1)，(2) に答えよ。

(1) 図 6 中の下線②のログ調査結果を得るために調査したサーバの名称を図 1 中の字句を用いて答えよ。

(2) 本文中の下線③について，U 氏が助言した対策を 30 字以内で述べよ。

**設問4**　〔ML に関する検討〕について，(1)～(5) に答えよ。

(1) 本文中の下線④について，ML サーバの設定の見直し案を 45 字以内で，許可済ドメイン名の設定ルール案を 35 字以内で述べよ。

(2) 本文中の下線⑤について，表 7 中の修正箇所 2 か所の項番と修正後の処理を答えよ。

(3) 本文中の［　e　］に入れる適切なサーバの名称を図 1 中の字句を用いて答えよ。

(4) 本文中の下線⑥について，U 氏が連絡手段をメール以外の方法に変更するように助言した理由を 40 字以内で述べよ。

(5) 本文中の下線⑦について，SPF によって P 社からのメールが迷惑メールと判定されないために ML サーバの設定を変更する対策案を 50 字以内で述べよ。

**設問5**　〔情報交換対策に関する検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑧について，PJWeb サーバに必要な情報セキュリティ機能として追加すべきもののうち，情報漏えい対策に効果があるものを二つ挙げ，具体的な内容を，それぞれ 40 字以内で述べよ。

(2) 本文中の下線⑨について，PJWeb サーバの情報セキュリティ対策のうち，情報漏えい対策として，情報システム部が行うべき運用方法を，想定するリスクを含めて，60 字以内で具体的に述べよ。