問2　電子メールのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

R社は，従業員数100名のシステム開発会社である。

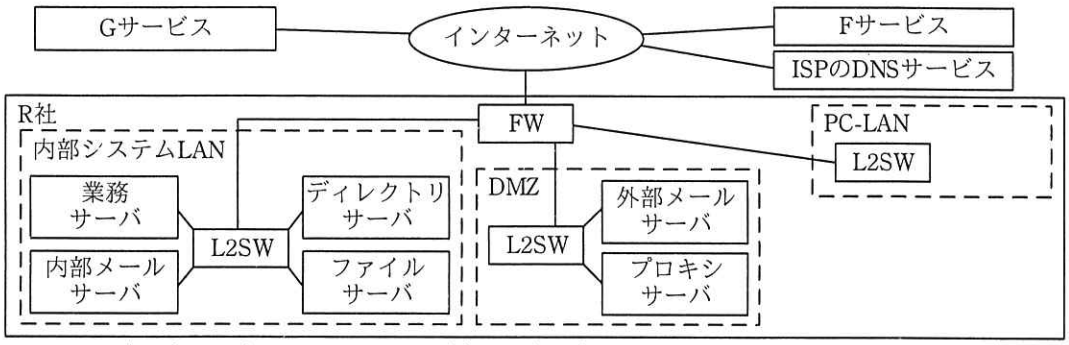
R社では，電子メール（以下，メールという）を利用している。メールアドレスのドメイン名には，r-sha.co.jp（以下，R社ドメイン名という）を使用している。R社では，委託先との設計ドキュメントファイルの交換に当たって，F社のファイル交換サービス（以下，Fサービスという）の利用を推進している。ただし，委託先が社内ルールで外部のファイル交換サービスの利用を禁止している場合は，設計ドキュメントファイルをパスワード付きZIPファイルにし，メールに添付して，メーリングリスト（以下，MLという）のメールアドレス宛てに送信している。ZIPファイルのパスワードは，平文のメールでMLのメールアドレス宛てに送信している。

MLには，G社のMLサービス（以下，Gサービスという）を利用している。MLのメールアドレスのドメイン名は，G社が取得したものである。MLのメールアドレスのローカル部は，プロジェクト名と委託先の会社名を組み合わせている。例えば，Bプロジェクトでの S社との交換では，MLのメールアドレスのローカル部は，*b-project_s-sha* にする。

Gサービスでは，メールをMLのメールアドレス宛てに送信すると，登録されたメンバ（以下，登録メンバという）のメールアドレス宛てに同報される。MLの登録メンバのメールアドレスの管理は，プロジェクトごとにR社のそれぞれのプロジェクト管理者が行う。各プロジェクト管理者は，自身が管理するプロジェクトのMLの登録メンバでもある。

〔R社の情報システム〕

R社の情報システムは，情報システム部が運用している。R社の情報システムの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

注記 1 PC-LAN に接続されている PC の記載は省略している。

注記 2 DMZ 内の各サーバには，グローバル IP アドレスを割り当てている。

注記 3 内部システム LAN 及び PC-LAN には，プライベート IP アドレスを割り当てている。

図 1　R 社の情報システムのネットワーク構成（抜粋）

内部システム LAN のサーバの機能概要を表 1 に示す。

表 1　内部システム LAN のサーバの機能概要（抜粋）

サーバ名	機能名	機能概要
内部メールサーバ	メール転送機能	・外部メールサーバとの間で，SMTP を用いてメールを転送する。
	メールボックス機能	・宛先メールアドレスのドメイン名が R 社ドメイン名であるメールをメールボックスに格納する。 ・POP3 を用いて，PC からメールボックス内のメールにアクセスできるようにする。
	メール受信機能	・SMTP を用いて，PC からメールを受信する。
ディレクトリサーバ	ディレクトリ機能	・X.500 モデルをサポートするディレクトリを管理し，当該ディレクトリへのアクセスを提供する。 ・ディレクトリへのアクセスは，標準で TCP ポートの 389 番を使用する［ a ］を用いる。 ・内部システム LAN のサーバでの認証に用いる。
	DNS 機能	・R 社内のサーバ及び PC のホスト名を管理する。

内部システム LAN のサーバではサーバ証明書を利用している。それらのサーバ証明書は，ネットワークに接続していない証明書発行専用機器上の R 社認証局（以下，R 社 CA という）で発行している。R 社 CA は情報システム部が運用している。

DMZ のサーバの機能概要を表 2 に示す。

表2　DMZ のサーバの機能概要（抜粋）

サーバ名	機能名	機能概要
外部メールサーバ	メール転送機能	・インターネットとの間で，SMTP を用いてメールを転送する。 ・内部メールサーバとの間で，SMTP を用いてメールを転送する。 ・SMTP over TLS にも対応している。
プロキシサーバ	プロキシ機能	・内部システム LAN 及び PC-LAN からインターネット上の Web サーバへのアクセスだけを中継する。

ISP の DNS サービスを，DNS キャッシュサーバ及び R 社ドメイン名の権威 DNS サーバとして利用している。

R 社では，従業員ごとに 1 台の PC を貸与している。各 PC には，R 社 CA のルート証明書を信頼できる発行元として登録している。

PC の Web ブラウザでは，HTTPS でアクセスする Web サーバのサーバ証明書が失効していないことを，RFC 6960 で規定されている［　b　］を利用して確認できるようにしている。

〔要望への対応〕

営業部と開発部から，委託先とのメール利用についての要望が情報システム部の D 部長に提出された。D 部長はその要望を基に，表 3 の要件をまとめた。

表3　委託先とのメール利用についての要件

項番	目的	要件
1	メールの暗号化	送信者から受信者まで暗号化された状態で，メールを送受信する。
2	送信者の検証	委託先とのやり取りのメールがなりすまされたものでないかどうかを確認できるように，送信者を検証する。

D 部長は，部下の E 主任と H さんに表 3 についての対応策の検討を指示した。

H さんは，メールの通信を暗号化することによって，表 3 の二つの要件に対応できるのではないかと E 主任に話した。

それに対して，E 主任は次の指摘をした。

・<u>①メールの通信を暗号化しただけでは，表 3 の項番 1 を満たせない。</u>

・攻撃者が委託先を装った［　c　］を用意するようななりすましは，送信元の［　c　］の真正性を確認して検出できる。一方，送信者メールアドレスとして

委託先のメールアドレスを使うようななりすましは検出できないので，表 3 の項番 2 を満たせない。

そこで，E 主任と H さんが他の対応策を調査したところ，S/MIME を利用すれば表 3 の要件を実現できることが分かった。E 主任と H さんは，S/MIME の利用を想定した次の方式を考えた。

（あ）R 社 CA で，S/MIME で利用する鍵ペアを生成し，S/MIME に利用可能なクライアント証明書（以下，S/MIME 証明書という）を発行する。

（い）S/MIME 証明書の失効情報を提供する機能をもつサーバ（以下，失効情報サーバという）を導入し，S/MIME 証明書の失効情報を登録する。

（う）S/MIME 証明書が失効していないことをメールクライアントから確認する。

（え）後でも参照する必要があるメールは，②復号できなくなる場合に備えて，復号してファイルサーバに保存する。

〔S/MIME 利用に向けた課題と解決策〕

E 主任と H さんは，S/MIME の利用に向けて，解決すべき課題を次のとおりリストアップした。

（ア）R 社 CA のようなプライベート認証局のルート証明書を PC に登録することが，委託先によっては禁止されており，その場合，R 社の従業員が送信したメールの［ d ］を［ e ］することができない。

（イ）委託先に事前に S/MIME 証明書を渡す必要があり，その方法を決める必要がある。

（ウ）ML 宛てのメールを暗号化できない。

E 主任と H さんは，（ア）～（ウ）それぞれの解決策を検討した。

（ア）については，認証局サービス事業者が発行する S/MIME 証明書であれば，委託先での R 社 CA のルート証明書を PC に登録しなくてもよいことが分かった。加えて，失効情報サーバの導入も不要であることが分かった。そこで，認証局サービス事業者が発行する S/MIME 証明書を利用することにした。

（イ）については，S/MIME 証明書を外部記憶媒体に保存して手渡す方法と，メー

ルで送信する方法を調査した。調査の結果，S/MIME を用いて［ d ］を付与したメールを送信すれば，受信者は S/MIME 証明書も受け取れるし，送信者が他者になりすましていないことも確認できることが分かり，便利でもあるので，メールで送信する方法にすることにした。

（ウ）については，表 3 の項番 1 を完全に満たすわけではないが，次の案を考えた。

（1）R 社のプロジェクト管理者は，あらかじめ，G サービスに［ f ］のメールアドレスの S/MIME 証明書を登録する。

（2）R 社のプロジェクト管理者は，あらかじめ，［ g ］のメールアドレスの S/MIME 証明書の発行手続を G 社に依頼する。

（3）メール送信者は，［ g ］のメールアドレスの S/MIME 証明書を使って暗号化したメールを送信する。

（4）G サービスは，メールを復号する。

（5）G サービスは，［ f ］のメールアドレスのそれぞれの S/MIME 証明書を使い，受信後にそれぞれが復号できるようにしてメールを暗号化する。

（6）G サービスは，暗号化したメールを送信する。

E 主任が G 社に確認したところ，この案には対応できないと回答があった。そこで，委託先との間で暗号化したメールを送信する場合は，ML を利用せずに委託先担当者の S/MIME 証明書で暗号化し，当該担当者のメールアドレスに送信することにした。

E 主任と H さんは，S/MIME の利用について，D 部長に報告した。D 部長は，S/MIME の利用を営業部長と開発部長に説明し，了承を得た。営業部経由で委託先に S/MIME の利用を打診したところ，S/MIME の利用の内諾が得られた。その後，必要な準備を行い，S/MIME を試行した。その結果，問題ないことが確認でき，S/MIME の利用が始まった。

設問1　〔R社の情報システム〕について，(1)，(2)に答えよ。

(1)　表1中の［　a　］に入れる適切なプロトコル名を，英字5字以内で答えよ。

(2)　本文中の［　b　］に入れる適切なプロトコル名を，英字5字以内で答えよ。

設問2　〔要望への対応〕について，(1)~(3)に答えよ。

(1)　本文中の下線①の理由を，35字以内で述べよ。

(2)　本文中の［　c　］に入れる適切な字句を，10字以内で答えよ。

(3)　本文中の下線②について，復号できなくなるのはどのような場合か。25字以内で述べよ。

設問3　本文中の［　d　］～［　g　］に入れる適切な字句を，［　d　］，［　f　］は，それぞれ10字以内で，［　e　］，［　g　］は，それぞれ5字以内で答えよ。