

次の問 1 は必須問題です。必ず解答してください。

問 1 電子メールのセキュリティに関する次の記述を読んで、設問 1～5 に答えよ。

R 社は、医薬品の輸出入や薬局などへの販売を行っている商社である。R 社では、十数年前から業務処理や顧客からの問合せ対応などを目的として、自社内で電子メールシステム（以下、メールシステムという）を運用している。R 社の社員は、各自の社内 PC を使ってメールシステムを利用する。一部の社員は、モバイル端末を使って社外からもメールシステムを利用している。メールシステムが受信した電子メール（以下、メールという）は、メールサーバに保存される。社内 PC で開封したメールは、メールサーバから削除され、社内 PC に保存される。モバイル端末で開封したメールは、削除はされず、メールサーバに残される。

R 社システム部の S 部長は、メールシステムの老朽化、陳腐化への対応とセキュリティ強化が必要と判断し、現在のメールシステムの問題点を洗い出すために、システム監査会社に外部監査を依頼した。表 1 は、外部監査での指摘事項の抜粋である。

表 1 外部監査での指摘事項の抜粋

指摘事項	
送信	(ア) 差出人を R 社と偽ったメールが届いたという苦情が顧客から寄せられたことがあったが、対策が立てられていない。
	(イ) メールによる重要情報などの漏えいを抑止するために、社外への送信メールは上司に同報され、チェックされることになっている。しかし、上司が漏えいに気付いたとしても、メール自体は既に宛先に送られてしまっている。
	(ウ) 営業部では、顧客へのメールを S/MIME で暗号化することになっているが、一部の顧客しか利用できる環境にない。
	(エ) R 社の重要情報が記述されたメールを顧客へ平文で送っている場合がある。
受信	(オ) 社内 PC で開封したメールが社外から読めなくなってしまう、業務に支障を来すことがある。
	(カ) 迷惑メールが受信されている。一部、標的型攻撃メールと思われるものも混在している。

〔新メールシステムの検討〕

S 部長は、外部監査での指摘を受け、メールシステム担当の T 君に新メールシステムの概要設計を指示した。T 君は、新メールシステムの機能の概要をまとめ、S 部長に提出した。T 君が作成した新メールシステムの機能概要を表 2 に示す。

表 2 新メールシステムの機能概要

項目	目的
メールのプロトコルを POP から IMAP に変更する。	社外でモバイル端末を利用しているときでも、開封済みのメールを読めるようにする。
メールのチェックツールを導入し、社外とのメールをフィルタリングする。	社外とのメールの内容チェックを行う。 社外からの受信メールについて、送信元の認証を行う。
メール保存ツールを導入する。	全てのメールを保存する。
メールを暗号化するためのツールを導入する。	顧客への送信メールについて、添付ファイルを全て暗号化する。
電子署名を添付するためのツールを導入する。	顧客への送信メールに、R 社の電子署名を添付する。その際、送信元メールアドレスには、R 社の送信専用メールアドレスを使用し、送信者自身のメールアドレスは、返信先メールアドレスフィールドに設定する。

T 君は S 部長に、新メールシステムの機能概要を報告した。

〔メールのプロトコル〕

T 君 : 当社ではメール受信のプロトコルとして、POP を利用してきました。新メールシステムでは、指摘事項(オ)に対応するために IMAP に変更し、社内 PC で開封したメールも含め、全ての受信メールが一定期間メールサーバに残るようにすることを考えています。

S 部長 : なるほど。しかし、そうになると、①パスワードが流出した場合のリスクが高まることを認識しておく必要がある。特にモバイル端末の利用時には盗難なども考えられる。IMAP サーバでのモバイル端末の認証にはワンタイムパスワードを導入し、モバイル端末と IMAP サーバの間の通信は暗号化するように。

T 君 : 分かりました。

〔社外とのメールの内容チェック〕

T 君は社外とのメールについて、メールの内容チェックの詳細を報告した。メールの内容チェックの詳細を表 3 に示す。

表3 メールの内容チェックの詳細

	チェック項目	チェック後の対応
送信	会社の重要情報が含まれていないか。	問題があったメールは、チェックコメントを付けて、宛先には送信せずに送信元に返送する。
	顧客の重要情報が含まれていないか。	
受信	送信元メールアドレスが、迷惑メール送信者としてブラックリストに掲載されていないか。	メールを迷惑メールボックスに転送し、10日後に自動削除する。
	送信元メールアドレスは、偽称されていないか。	本文を削除して宛先メールボックスに転送する。元のメールは一時保管メールボックスに転送し、10日後に自動削除する。
	実行形式や不審なファイルが添付されていないか。	添付ファイルを削除して宛先メールボックスに転送する。元のメールは一時保管メールボックスに転送し、10日後に自動削除する。
	ウイルスに感染していないか。	ウイルスを駆除した上で、宛先メールボックスに転送する。
	本文がHTMLで記述されていないか。	注意を促すコメントを付けて、宛先メールボックスに転送する。
	本文中にURLが記載されていないか。	

T君：メール送信時の内容チェックは、指摘事項の(イ)に対応し、メール受信時の内容チェックは、指摘事項の(カ)に対応します。メールサーバでのメール受信時の送信元メールアドレスが偽称されていないかのチェックは a と呼ばれ、送信元 IP アドレスを基にチェックする技術（SPF）、又は受信メールの中の電子署名を基にチェックする技術（DKIM）を導入します。

S部長：表3に従うと、業務に必要なメールまでチェックによって阻止されてしまうことがある。②それらのメールに対応するための機能も加えるように。

T君：分かりました。

[メールの暗号化]

S部長：暗号化方式の変更について説明してくれないか。

T君：暗号化方式の変更は、指摘事項の(ウ)と(エ)に対応します。現在のメールシステムでは、営業部でのメールの暗号化には、S/MIME を利用することになっています。メール宛先の b 鍵を利用して暗号化する方式で、安全性は高いのですが、先方が b 鍵をもっていなければ使えない方法なので、利用している顧客はごく一部です。

S 部長：新メールシステムでは、全顧客にメールの暗号化が利用できるのか。

T 君：はい。重要情報を含む文章はメール本文に記述するのではなく必ずファイルで作成する社内ルールに変更します。送信者が添付ファイル付きのメールを作成すると、メールサーバでは、鍵をメールごとに自動生成した上で、その鍵で添付ファイルを暗号化して送信し、さらに鍵を送信者に通知します。宛先への鍵の連絡は、送信者が電話などのメール以外の手段で行います。

[電子署名の添付]

S 部長：全ての送信メールに対する R 社の電子署名の添付について、説明してこないか。

T 君：電子署名の添付は指摘事項の(ア)への対応です。従来、営業部員は個別に電子証明書と暗号鍵を与えられ、本人の電子署名の添付と、公開鍵基盤を導入している宛先へのメールの暗号化ができました。しかし、対象を全社員に広げるとなると、社員の電子証明書の運用コストが掛かってしまいます。そこで、社員の電子署名の添付を廃止し、メールサーバで、全メールに R 社の電子署名を添付して、送信することにします。電子署名はメールの

c

 値を基に生成されるので、メールの

d

 検知も可能になります。

[標的型攻撃メールへの対応]

S 部長：標的型攻撃メールには、どのような対応をするのか。

T 君：標的型攻撃メールは、メールシステムでの対応には限界があるので、運用での対応も必要になると考えています。例えば、標的となった組織の複数のメールアドレスに届くことが多いので、一斉に、組織的に対応する必要があります。一人でも標的型攻撃メールと疑われるメールを受信した場合、メールシステムの管理者は、類似のメールが届いていないかを調査し、③ 不審なメールが届いた全ての受信者に対応を指示します。その後、受信者が添付ファイルを開けていないことや URL をクリックしていないことなどを管理者が確認します。

S 部長：類似の標的型攻撃メールが届いた宛先は、メールサーバの から調査できるな。

その後、S 部長と T 君は、機能のレビューを繰り返し、指摘に対しての対応策を決定して、S 部長は新メールシステムの導入を承認した。

設問 1 本文中の ， に入れる適切な名称をそれぞれ解答群の中から選び、記号で答えよ。

解答群

- ア OP25B イ 送信ドメイン認証 ウ フィルタリング
エ フロー制御 オ 迷惑メールボックス カ ログ

設問 2 本文中の ～ に入れる適切な字句を答えよ。

設問 3 S 部長が本文中の下線①の指摘を行った理由を、35 字以内で述べよ。

設問 4 本文中の下線②の機能に該当するものを解答群の中から二つ選び、記号で答えよ。

解答群

- ア 一時保管メールボックスに転送された受信メールの中から、受信者が必要なメールを取り出す機能
イ 会社や顧客の重要情報を含む送信メールは、フィルタリングの対象となるが、事前に承認されたメールについては宛先に転送されるようにする機能
ウ フィルタリングによって阻止された全ての送信メールについて、タイトル（主題）だけを宛先に転送する機能
エ フィルタリングの内容を、社員が設定する機能

設問 5 本文中の下線③で不審なメールが届いた全ての受信者に指示すべき事項は何か。15 字以内で述べよ。