問1　電子メールからの情報漏えいとその対策に関する次の記述を読んで，設問1～5に答えよ。

A社は，業務用機械の製造と販売を行う従業員数800名の会社である。営業部門には全国10都市の支店を含めて100名の部員がいる。営業活動においては，顧客への訪問回数を増やすことによる受注拡大や，顧客からの質問への迅速な対応による顧客満足度向上の取組みに重点を置いている。そのため，外出が中心になってもこまめに電子メール（以下，メールという）のチェックを行えるよう，日常的にPCを持ち歩く部員が多い。メールでは価格表や提案書などの機密データを社内関係者とやり取りすることが多い。また，営業部門の部員は顧客との連絡用に会社貸与の携帯電話を持ち歩いている。A社では情報セキュリティの管理体制として情報セキュリティ委員会を設置し，情報セキュリティ対策基準を2年前に策定している。

〔事故の発生〕

営業部門では，最近の報道で，PCの紛失や盗難による情報漏えい事故が目立っていることを受け，PCの持出しを自粛することに決めた。しかし，営業部門の部員の中には，PCを持ち出さないまでもメールの閲覧だけはしたいと考え，会社貸与の携帯電話の従業員用メールアドレスにメールを転送する者がいた。自粛を決めてから数か月たったある日，①会社貸与の携帯電話の紛失による情報漏えい事故が発生した。携帯電話を紛失したこと，携帯電話端末にメールが保存されていたこと，そして，キーロック解除用の暗証番号が設定されていなかったことが情報システム部門に直ちに報告された。後日，特定の顧客にしか開示しない価格表の漏えいが確認された。

〔再発防止のための検討〕

今回の事故の報告を受け，事態を深刻に受け止めた情報システム部長は，情報システム部門のG課長に改善策を検討するよう指示した。G課長は，営業部門の関係者から事情を聞いた結果，情報セキュリティ対策基準及びメールシステムが情報漏えい対策の観点で不十分ではないかと考え，見直しをF主任に指示した。

A社の情報セキュリティ対策基準には，端末の利用とメールの利用について図1に示す規定がある。

5.9 端末利用
(1) 業務に利用する端末（PC，携帯電話及びPDA）は会社から貸与されたものだけとする。
(2) 端末の利用者を限定するために，利用者認証機能を有効にしなければならない。PC 及び PDA であればログイン時利用者認証機能を，携帯電話であれば暗証番号による端末操作制限機能やデータ保護機能を有効にしなければならない。
(3) 端末上で機密データを取り扱う場合，ファイル保存中は重要度に応じて［ a ］などの処置をとり，取扱いが不必要となった時点でデータを削除しなければならない。また，機密データを社外に提供する場合，提供者は情報システム部門の許可を得なければならない。
(4) 端末の盗難や紛失が発生した場合，速やかに情報システム部門に報告しなければならない。
（5.10～5.12 は省略）
5.13 メール利用
(1) 従業員用メールアドレスを利用するものとし，業務上での私有メールアドレスの利用を禁止する。
(2) 業務目的のメールを私有メールアドレスに転送することを禁止する。
(3) メールの送信に当たっては，［ b ］がないことを確認しなければならない。
(4) メールの受信に当たっては，別途定めるウイルス対策基準に基づき，ウイルスチェック機能を有効にしなければならない。
(5) やむを得ず機密データをメールで送信する場合には［ a ］しなければならない。
（以下，省略）

図1　A社における端末利用とメール利用に関する規定
（情報セキュリティ対策基準からの抜粋）

F 主任は，携帯電話に関して，別途定めた規程の内容と対策状況を確認した。まず，②A 社で使用している携帯電話の場合，盗難・紛失が起きたときの事後対策を情報システム部門が施せるにもかかわらず，実施していなかったので，実施した方がよいと考えた。また，営業部門では携帯電話端末にメールを保存しており，機密データが蓄積されがちな状況となっている。そこで，携帯電話から直接メールを安全に閲覧するシステム（以下，S システムという）を提供して，情報漏えいリスクを低減した方がよいと考えた。F 主任は，これらの改善方針を情報システム部門として取りまとめ，情報セキュリティ委員会に提示し，実現に向けた検討開始の承認を得た。

〔S システムの検討〕

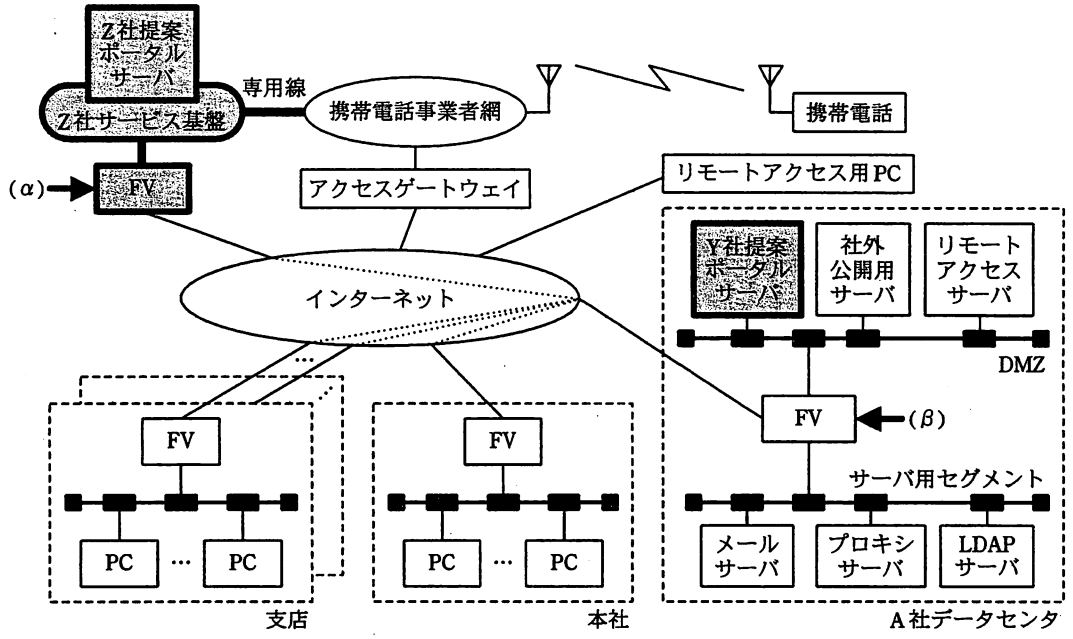
検討を開始するに当たり，G 課長からは，S システムでは，既存の PC 用のリモートアクセスシステムを参考に，認証の強度が同程度かそれ以上になるようにすること，との指示があった。

携帯電話端末にメールが保存されないようにしたいとの要望や，会社貸与の携帯電

話の事業者は 1 社であるといった現状を，F 主任が情報システムベンダ各社に伝えて S システムの提案を求めたところ，Y 社と Z 社の 2 社から提案があった。F 主任は，図 2 に示すように，A 社の現在のネットワーク構成図に Y 社と Z 社の提案の構成を書き加えるとともに，2 社の提案の特徴を表にまとめて比較した。

A 社内では，本社，支店，自社データセンタ間を IPsec によるインターネット VPN で接続している。各種サーバは自社データセンタに設置し，ファイアウォール兼 VPN ルータ（以下，FV という）及び社外公開用サーバを含めて自社で運用している。

本社や支店の PC からインターネット上の Web サーバへのアクセスは，サーバ用セグメント上のプロキシサーバを経由している。リモートアクセス用 PC が利用するリモートアクセスサーバは，DMZ 上に設置され，利用者認証にはワンタイムパスワードを利用している。ただし，既存の PC 用のリモートアクセスシステムは携帯電話からのアクセスに対応していない。



注　図中の網掛けの部分は，現在のネットワークへの追加部分であることを表す。
インターネット内の点線はインターネットVPNを表す。

図 2　A 社のネットワーク構成

表　Y社及びZ社の提案の特徴

比較項目	Y社	Z社
利用手順	携帯電話からブラウザでポータルサーバにアクセスし，認証後，業務メニュー画面からメールサービスを選択し，メールを閲覧する。メール送信はできない。	
新設サーバの有無と設置環境	ポータルサーバをA社データセンタのDMZ上に新設する（図2）。携帯電話とポータルサーバ間は携帯電話事業者網とインターネットを経由してSSLで通信する。	ポータルサーバをZ社が運営するサービス基盤上に新設する（図2）。サービス基盤は携帯電話事業者網と専用線で接続され，サービス基盤とサーバ用セグメント間はインターネットVPNで接続する。
メールサーバへの接続方法	ポータルサーバからメールサーバにIMAPで接続し，メールを閲覧する。 ③メールサーバにログインするための利用者IDとパスワードは，ポータルサーバとメールサーバ間でID連携するので，携帯電話からは直接入力しない。	
メールの保存先	メールサーバ上に保存され，削除しなければ繰り返し閲覧できる。 携帯電話端末及びポータルサーバ上への保存機能はない。	
携帯電話（利用者）の認証方法	ポータルサーバにおいてSSLクライアント認証で認証する。電子証明書は，携帯電話事業者が携帯電話のSIMカードに対して発行するサービスを利用して入手する。電子証明書のコモンネーム（Common Name）には携帯電話のSIMカードを一意に識別できる情報が記載されている。認証時，ポータルサーバはLDAPサーバへの問合せを行い，登録済の従業員であることを確認する。	ポータルサーバにおいて，Z社が提供するワンタイムパスワード方式で認証する。
PC対応の有無	あり（オプション対応）	なし

F主任は，営業部門による携帯電話の規程遵守状況から，Z社の提案を選択したいと考え，G課長に検討結果を報告した。しかし，G課長は今回の事故が発生する前から既存のPC用のリモートアクセスシステムの見直しを情報システム部長から指示されており，PC用のリモートアクセスとの統合を見込めるY社の提案も捨て難いと考えたため，F主任と意見が一致しなかった。そこで，G課長は情報システム部長に両案を説明して判断をゆだねたところ，G課長の考えどおりにY社の提案を選択することに決まった。情報システム部長からは，今回の検討では事故の再発防止のための抜本的な解決には至っていないので，運用面での改善を含めて更に詰めるようにとの指示が加えられた。その後，F主任は，営業部門を対象にした導入準備に取り掛かった。

設問1　図1中の［　a　］，［　b　］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　圧縮	イ　あて先ミス	ウ　暗号化
エ　改ざん	オ　時刻同期	カ　ディジタル署名

設問2　情報漏えい事故について，(1)，(2)に答えよ。

(1) 本文中の下線①について，どの規定の遵守が不十分であったと考えられるか。図1中から三つ選んで，“5.9 (1)”のように箇条と項番で答えよ。

(2) 本文中の下線①に記載されている価格表以外に漏えいした可能性が高い顧客の情報を，7字以内で答えよ。また，その情報について，携帯電話の紛失が判明した後，紛失した携帯電話が戻ってこなくても，情報漏えいによる被害を受ける可能性がある顧客の特定を迅速に行えるようにするための対策を，45字以内で具体的に述べよ。

設問3　本文中の下線②の対策を実現するために情報システム部門が利用する，携帯電話サービスによって提供される管理上の機能を，30字以内で具体的に述べよ。

設問4　Sシステムの構築について，(1)～(3)に答えよ。

(1) Y社の提案について，登録された従業員だけがメールを閲覧できるようにするために図2中のLDAPサーバに従業員ごとに追加登録する内容を，20字以内で述べよ。

(2) Y社の提案について，表中の下線③の特徴があるにもかかわらず，図1中の5.9の，ある規定の遵守が不十分な場合には，第三者にメールを閲覧される可能性がある。その箇条と項番を答えよ。また，その箇条と項番の規定に関連して，第三者によるメールの閲覧防止を徹底する対策について，50字以内で具体的に述べよ。

(3) Z社の提案について，図2中の(α)と(β)で示したFV間で特定のアプリケーションに絞ってIPsecを適用するとしたとき，どのサーバ間の通信の，どのプロトコルを対象にすればよいか。図2中又は表中の用語を用いて答えよ。

設問5　携帯電話端末へのメールの保存による情報漏えいを防ぐために，図1中の5.13(2)に追記したい。追記する内容を，45字以内で具体的に述べよ。