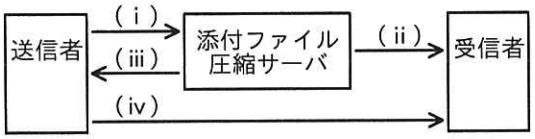
次の問１は必須問題です。必ず解答してください。

問１　電子メールのセキュリティ対策に関する次の記述を読んで，設問に答えよ。

K社は，IT製品の卸売会社であり，300社の販売店に製品を卸している。K社では，8 年前に従業員が，ある販売店向けの奨励金額が記載されたプロモーション企画書ファイルを添付した電子メール（以下，メールという）を，担当する全販売店の担当者宛てに誤送信するというセキュリティ事故が発生した。この事故を機に，メールの添付ファイルを，使い捨てのパスワード（以下，DPW という）によって復元可能な ZIP ファイルに変換する添付ファイル圧縮サーバを導入した。

添付ファイル圧縮サーバ導入後のメール送信手順を図１に示す。



（ｉ）添付ファイル付きメール
（ii）添付ファイルがZIPファイルに変換されたメール
（iii）DPW通知メール
（iv）DPWを記載したメール

凡例　⟶：メールの転送方向を示す。

図１　添付ファイル圧縮サーバ導入後のメール送信手順

〔現在のメール運用の問題点と対策〕

K 社では，添付ファイル圧縮サーバを利用して，最初に DPW で復元可能な ZIP ファイルを添付したメール（以下，本文メールという）を送信し，その後，ZIP ファイルを復元するための DPW を記載したメール（以下，PW メールという）を送信することによって，メールのセキュリティを確保する方式（以下，この方式を PPAP という）を運用している。

しかし，現在運用している PPAP は，政府のある機関において中止するという方針が公表され，K 社の販売店や同業者の中でも PPAP の運用を止める動きが見られるようになった。

このような状況から，K 社の情報セキュリティ委員会は，自社の PPAP の運用上の問題点を検証することが必要であると判断して，情報セキュリティリーダーのＬ主任に，PPAP の運用上の問題点の洗い出しと，その改善策の検討を指示した。

Ｌ主任は，現在の PPAP の運用状況を調査して，次の二つの問題点を洗い出した。

(1)　①本文メールの宛先を確認せずに，本文メールと同じ宛先に対して PW メールを

送信している従業員が多い。

(2) ほとんどの従業員が，PW メールを本文メールと同じメールシステムを使用して送信している。したがって，本文メールが通信経路上で何らかの手段によって盗聴された場合，PW メールも盗聴されるおそれがある。

問題点の(1)及び(2)は，ともに情報漏えいにつながるリスクがある。(1)の問題点を改善しても，(2)の問題点が残ることから，②L 主任は(2)の問題点の改善策を考えた。しかし，運用面の改善によってリスクは低減できるが，時間とともに情報漏えいに対する意識が薄れると，改善策が実施されなくなるおそれがある。そこで，L 主任は，より高度なセキュリティ対策を実施して，情報漏えいリスクを更に低減させる必要があると考え，安全なメールの送受信方式を調査した。

〔安全なメール送受信方式の検討〕

L 主任は，調査に当たって安全なメール送受信方式のための要件として，次の(ⅰ)～(ⅲ)を設定した。

(ⅰ) メールの本文及び添付ファイル（以下，メール内容という）を暗号化できること

(ⅱ) メール内容は，送信端末と受信端末との間の全ての区間で暗号化されていること

(ⅲ) 誤送信されたメールの受信者には，メール内容の復号が困難なこと

これら三つの要件を満たす技術について調査した結果，S/MIME（Secure/Multipurpose Internet Mail Extensions）が該当することが分かった。S/MIME は，K 社や販売店で使用している PC のメールソフトウェア（以下，メーラという）が対応しており導入しやすいと L 主任は考えた。

〔S/MIME の調査〕

まず，L 主任は S/MIME について調査した。調査によって分かった内容を次に示す。

・S/MIME は，メールに電子署名を付加したり，メール内容を暗号化したりすることによってメールの安全性を高める標準規格の一つである。

・メールに電子署名を付加することによって，メーラによる電子署名の検証で，送信者を騙(かた)ったなりすましや③メール内容の改ざんが検知できる。公開鍵暗号と共通鍵暗号とを利用してメール内容を暗号化することによって，通信経路での盗聴や誤送信による情報漏えいリスクを低減できる。
・S/MIME を使用して電子署名や暗号化を行うために，認証局（以下，CA という）が発行した電子証明書を取得してインストールするなどの事前作業が必要となる。

メールへの電子署名の付加及びメール内容の検証の手順を表 1 に，メール内容の暗号化と復号の手順を表 2 に示す。

表 1　メールへの電子署名の付加及びメール内容の検証の手順

送信側		受信側	
手順	処理内容	手順	処理内容
1.1	ハッシュ関数 h によってメール内容のハッシュ値 x を生成する。	1.4	電子署名を［ b ］で復号してハッシュ値 x を取り出す。
1.2	ハッシュ値 x を［ a ］で暗号化して電子署名を行う。	1.5	ハッシュ関数 h によってメール内容のハッシュ値 y を生成する。
1.3	送信者の電子証明書と電子署名付きのメールを送信する。	1.6	手順 1.4 で取り出したハッシュ値 x と手順 1.5 で生成したハッシュ値 y とを比較する。

表 2　メール内容の暗号化と復号の手順

送信側		受信側	
手順	処理内容	手順	処理内容
2.1	送信者及び受信者が使用する共通鍵を生成し，④共通鍵でメール内容を暗号化する。	2.4	［ d ］で共通鍵を復号する。
2.2	［ c ］で共通鍵を暗号化する。	2.5	共通鍵でメール内容を復号する。
2.3	暗号化したメール内容と暗号化した共通鍵を送信する。		

〔S/MIME 導入に当たっての実施事項の検討〕

次に，L 主任は，S/MIME 導入に当たって実施すべき事項について検討した。

メーラは，⑤受信したメールに添付されている電子証明書の正当性について検証する。問題を検出すると，エラーが発生したと警告されるので，エラー発生時の対応方

法をまとめておく必要がある。そのほかに，受信者自身で電子証明書の内容を確認することも，なりすましを発見するのに有効であるので，受信者自身に実施を求める事項もあわせて整理する。

メール内容の暗号化を行う場合は，事前に通信相手との間で電子証明書を交換しておかなければならない。そこで，S/MIME 導入に当たって，S/MIME の適切な運用のために従業員向けの S/MIME の利用手引きを作成して，利用方法を周知することにする。

これらの検討結果を基に，L 主任は S/MIME の導入，導入に当たって実施すべき事項，導入までの間は PPAP の運用上の改善策を実施することなどを提案書にまとめ，情報セキュリティ委員会に提出した。提案内容が承認され S/MIME の導入が決定した。

設問１　〔現在のメール運用の問題点と対策〕について答えよ。

(1)　本文中の下線①によって発生するおそれのある，情報漏えいにつながる問題を，40 字以内で答えよ。

(2)　本文中の下線②について，盗聴による情報漏えいリスクを低減させる運用上の改善策を，30 字以内で答えよ。

設問２　〔S/MIME の調査〕について答えよ。

(1)　本文中の下線③が検知される手順はどれか。表 1，2 中の手順の番号で答えよ。

(2)　表 1，2 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　CA の公開鍵　　イ　CA の秘密鍵　　ウ　受信者の公開鍵

エ　受信者の秘密鍵　　オ　送信者の公開鍵　　カ　送信者の秘密鍵

(3)　表 2 中の下線④について，メール内容の暗号化に公開鍵暗号ではなく共通鍵暗号を利用する理由を，20 字以内で答えよ。

設問３　本文中の下線⑤について，電子証明書の正当性の検証に必要となる鍵の種類を解答群の中から選び，記号で答えよ。

解答群

ア　CA の公開鍵　　イ　受信者の公開鍵　　ウ　送信者の公開鍵