問9　公開鍵基盤を用いた社員認証システムに関する次の記述を読んで，設問1～4に答えよ。

販売業を営むX社は，社内業務で利用している電子メールで顧客情報などの個人情報や機密性の高い販売業務に関する情報を安全に取り扱うために，公開鍵基盤を用いた社員認証システム（以下，本システムという）を導入している。本システムを含む社内業務システムの概要を図に示す。

〔本システムの概要〕

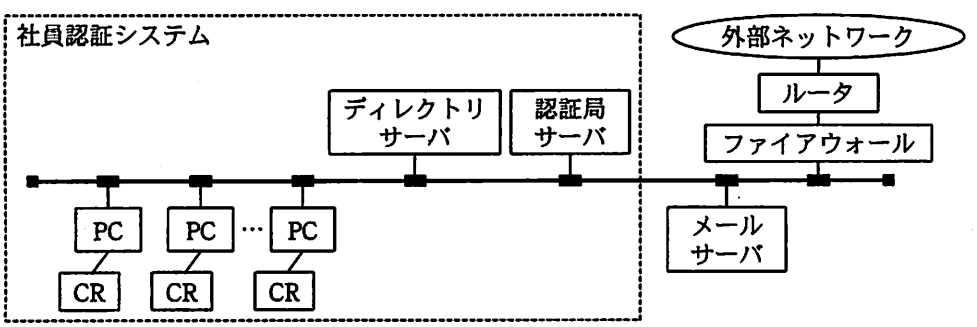
(1) 本システムは，ディレクトリサーバ，認証局サーバ，社員ごとのPC及びIC社員証カード（以下，ICカードという）から構成される。

(2) ディレクトリサーバでは，社員の公開鍵証明書や電子メールアドレスなどの属性情報の登録及び検索が行われる。

(3) 本システムでは，プライベート認証局を使用している。

(4) ICカードには，社員個人の秘密鍵，公開鍵証明書及びPIN（Personal Identification Number）が格納されている。社員が本システムを利用する際には，自分のICカードをPCのICカードリーダに挿入し，ICカードのパスワードであるPINを入力する。

(5) PCには，本システムにおける認証機能や暗号化機能及び電子メールのクライアント機能を提供するソフトウェア（以下，PCサブシステムという）が導入されている。



注 CR：ICカードリーダ

図　社内業務システムの概要

〔新規発行〕

システム管理者が，社員 A に IC カードを新規に発行する場合の処理の流れは，次のとおりである。

(1) システム管理者は，認証局サーバで，［ a ］と［ b ］の対を生成する。

(2) 認証局サーバは，［ b ］と社員名や有効期間などを結び付けた情報に［ c ］で署名し，［ d ］を生成する。

(3) 認証局サーバは，［ d ］をディレクトリサーバに登録する。

(4) 認証局サーバは，新規の IC カードに，生成した［ a ］と［ d ］，及び事前申請された PIN を記録する。

(5) システム管理者は，社員 A に IC カードを配付する。

〔電子メールのメッセージの送受信〕

社員 A が社員 B あてに，業務情報を暗号化して電子署名を付与したメッセージを送信し，社員 B が受信する際の処理の流れは，次のとおりである。

《送信側》

(1) 社員 A は，自分の IC カードを PC の IC カードリーダに挿入し，PIN を入力することで，PC サブシステムにログインする。

(2) 社員 A は，社員 B に送信したい電子メールのメッセージを作成した後，PC サブシステムに対し処理を依頼する。

(3) PC サブシステムは，作成したメッセージのハッシュ値を求め，そのハッシュ値を社員 A の秘密鍵で暗号化して，電子署名を生成する。

(4) PC サブシステムは，ディレクトリサーバから社員 B の公開鍵証明書を取得し，有効であることを確認する。

(5) PC サブシステムは，社員 B の公開鍵証明書に結び付けられた社員 B の公開鍵を用いて，作成したメッセージと電子署名を暗号化し，社員 B に送信する。

《受信側》

(1) 社員 B は，自分の IC カードを PC の IC カードリーダに挿入し，PIN を入力することで，PC サブシステムにログインする。

(2) [e]

(3) [f]

(4) [g]

設問1　IC カードを新規に発行する処理に関して，本文中の [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　システム管理者の公開鍵　　イ　システム管理者の公開鍵証明書

ウ　システム管理者の秘密鍵　　エ　社員Aとシステム管理者の共通鍵

オ　社員Aの公開鍵　　カ　社員Aの公開鍵証明書

キ　社員Aの秘密鍵　　ク　認証局とシステム管理者の共通鍵

ケ　認証局と社員Aの共通鍵　　コ　認証局の公開鍵

サ　認証局の公開鍵証明書　　シ　認証局の秘密鍵

設問2　受信後の処理の流れに関して，本文中の [e] ～ [g] 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　PC サブシステムは，社員 A の公開鍵証明書をディレクトリサーバから取得し，有効であることを確認する。

イ　PC サブシステムは，社員 B の公開鍵で暗号化されたメッセージと電子署名を受信し，社員Bの秘密鍵で復号する。

ウ　PC サブシステムは，復号されたメッセージのハッシュ値を計算し，社員 A の公開鍵証明書に結び付けられた社員 A の公開鍵で電子署名から復号されたハッシュ値と比較し，改ざんの有無を確認する。

設問3　本システムの機能では防止できない事象が発生する可能性がある。該当する事象を解答群の中からすべて選び，記号で答えよ。

解答群

ア　社員Aが自分のICカードとPINを利用して，社員Bになりすますこと

イ　社員Aが自分のICカードを紛失してしまうこと

ウ　社員Aが社員Bあてに送信した暗号化メッセージを，社員Cが解読すること

エ　社員Aが社員Bあてに送信した電子署名付きメッセージを，社員Aが否認すること

オ　社員Aが社員Bあてに送信した電子署名付きメッセージを，社員Bが改ざんしてその内容を変更すること

カ　社員Aが社員Bの電子署名を偽造すること

設問4　電子メールは，社内業務システムから社外にも送信することができる。その場合，例えば次に記述した処理の流れで，社員Aが作成したメッセージを，X社の社員ではない相手Dに送信すると，相手Dは，受信したメッセージが社員Aから送信されたものであることを検証できない。その理由を25字以内で述べよ。

〔電子メールのメッセージの送受信〕

《送信側》

(1) 社員Aは，自分のICカードをPCのICカードリーダに挿入し，PINを入力することで，PCサブシステムにログインする。

(2) 社員Aは，X社の社員ではない相手Dに送信したい電子メールのメッセージを作成した後，PCサブシステムに対し処理を依頼する。

(3) PCサブシステムは，作成したメッセージのハッシュ値を求め，そのハッシュ値を社員Aの秘密鍵で暗号化して，電子署名を生成する。

(4) PCサブシステムは，作成したメッセージと電子署名を相手Dに送信する。