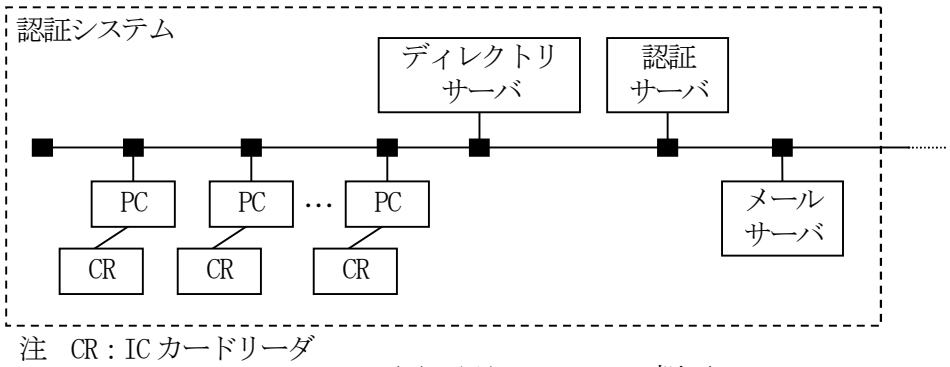
第３問　ICカードを用いた認証システムに関する次の記述を読んで、設問１，２に答えよ。

Ｚ社では、電子メールで顧客情報などの機密性の高い情報を安全に取り扱うために、認証システムを導入している。

(1)　認証システムは、認証サーバ、ディレクトリサーバ、社員用PC及びICカードから構成される。



注　CR：IC カードリーダ

図　認証システムの概要

(2)　認証サーバは、電子証明書の発行及びCRLの管理を行っている。

(3)　ディレクトリサーバでは、電子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。

(4)　ICカードには、社員個人の秘密鍵、電子証明書及びPIN（Personal Identification Number）が格納されている。社員が認証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。

〔電子メールの送信手順〕

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する際の処理の流れは、次のとおりである。

(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、認証システムにログインする。

(2)　社員Ａが社員Ｂに送信するメッセージを作成した後、認証システムは、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［　(a)　］で暗号化して、電子署名を生成する。

(3)　認証システムは、ディレクトリサーバから［　(b)　］の電子証明書を取得し、有効であることを確認する。

(4)　PCサブシステムは、(3)で入手した電子証明書に結び付けられた［　(c)　］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。

設問１　電子メールの送信手順中の［　(a)　］～［　(c)　］に入れる適切な字句を解答群の中から選べ。

(a)，(c)に関する解答群

ア　社員Ａの公開鍵　　イ　社員Ｂの公開鍵　　ウ　認証サーバの公開鍵
エ　社員Ａの秘密鍵　　オ　社員Ｂの秘密鍵　　カ　認証サーバの秘密鍵

(b)に関する解答群

ア　社員Ａ　　イ　社員Ｂ　　ウ　認証サーバ

設問２　本文中の下線部分について、適切な電子証明書と判断するための確認内容として適切なものを解答群から二つ選び、(d)，(e)に答えよ。

解答群

ア　認証サーバが発行した電子証明書であること
イ　電子証明書がCRLに記載されていること
ウ　電子証明書が暗号化されていること
エ　電子証明書が有効期限内であること
オ　電子証明書と電子署名の内容が等しいこと
カ　電子証明書に誤りがないこと