問3　ICカード認証に関する次の記述を読んで，設問1～5に答えよ。

D社は，従業者数3,000名の旅行業者である。従業者の半数は従業員で，残りは派遣従業員や嘱託従業員である。本社は東京にあり，支店や営業所が国内外70か所に点在する。売上は伸び悩んでおり，業務の更なる効率向上が急務となっている。また，顧客情報を扱っていることから万全のセキュリティ対策も欠かせない。

このため，D社は，全国3か所のデータセンタを，東西2か所に集約して相互にバックアップできるようにした。また，既存の従業者証を多目的型の非接触ICカード（以下，ICカードという）に切り替え，ICカードを用いて，入退室管理，自動ログイン及び認証プリントを実現することにした。自動ログインでは，ICカードに格納した利用者IDとパスワードによってPCや業務サーバにログインする。また，認証プリントでは，ICカードに格納した利用者IDによって本人を認証して印刷する。

ICカードを用いた本人認証（以下，ICカード認証という）によるセキュリティ強化方針（図1）が経営会議で承認されたので，情報システム部のJ部長は，同部のK主任にシステム方式設計に入るよう指示した。

1. 従業者証を兼ねた1枚のICカードを用いて，入退室管理，自動ログイン及び認証プリントを実現する。ICカードは有効期限（5年）満了時に回収し，引換えに新たなICカードを再発行する。
2. ICカード自体のセキュリティ機能を可能な限り利用する。
3. PCや業務サーバにログインするときの利用者IDやパスワードなどのアカウント情報は，LDAPサーバで一元管理する。
4. 事務室の出入口の内側と外側に，ICカードリーダ（以下，リーダという）を設置して入退室管理を行う。
5. すべてのPCにリーダを設置して，ICカードをログインに利用する。
6. プリンタを統廃合し，リーダを備えた認証プリンタに置き換える。

図1　ICカード認証によるセキュリティ強化方針（抜粋）

1か月後にシステム方式設計案が提出された。J部長は早速，レビューを実施した。最初に，設計前に提示した図2の要件が満たされているか確認を行った。

要件1　ICカード内部の情報が不正に読み出されたり，改ざんされたりしないこと
要件2　［　ア　］
要件3　リーダとICカードの間の通信が傍受されても，内容が分からないこと
要件4　ICカードが，正当な使用権限をもった者以外の者に使用されないこと

図2　ICカードのセキュリティ要件

レビューの結果，ICカードは，［　イ　］と図3中の認証シーケンス2によって要件1を，また，認証シーケンス1によって要件2を満たしていることが確認された。図3中の鍵1はPCを認証するための鍵，鍵2はICカードを認証するための鍵を示す。通信内容は暗号化されており，要件3を満たしている。さらに，ICカードを［　a　］していることと，暗証番号（以下，PINという）を［　b　］していることに基づく認証によって，要件4も満たしていることが確認された。

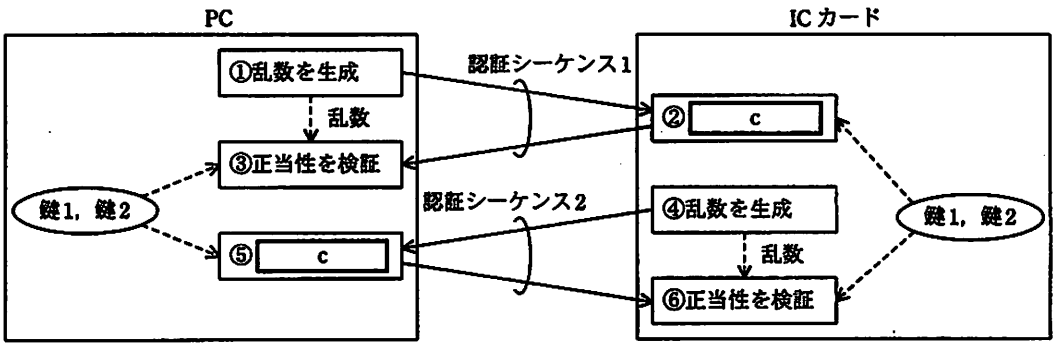

図3　ICカードとPCの間の相互認証シーケンス

次に，ICカードに格納する情報とそのアクセス制御について確認を行った。表は，K主任が提示した，ICカードに格納する情報とアクセス制御の一覧である。ICカード内の格納情報に対しては，利用者が入力する利用者PINと，運用管理者が入力する管理者PINによって，読出しの制限や書込みの保護を行う。

表　ICカードに格納する情報とアクセス制御

項番	格納情報	読出し	書込み	備考
1	ICカードの個体番号	○	×	納入時設定済（変更不可）
2	有効期限			
3	従業者番号			
4	利用者ID			
5	パスワード			
6	利用者PIN	×		納入時又は初期化時は初期値（ゼロ）
7	管理者PIN	×		
8	認証鍵（鍵1，鍵2）	×	×	納入時設定済（変更不可）

○：ICカードとPCの相互認証が成功した場合に格納情報の読出し又は書込みができる。
×：格納情報の読出し又は書込みができない。
注　網掛けの部分は，○と×を表示していない。

なお，ログイン時は IC カードをリーダにかざして，更にキーボードから利用者 PIN を入力するが，入退室と印刷時は，利便性を優先し，IC カードをかざすだけで利用者 PIN は入力しない。

PC や業務サーバにログインするときに必要なパスワードは，乱数を基に自動生成されて LDAP サーバと IC カードに格納される。IC カードの有効期限内はパスワードを変更しない。従業者番号は，従業員の入社時，派遣従業員又は嘱託従業員の受入れ時に割り当てられ，退職時，派遣又は嘱託終了時まで不変である。

次に，図 4 の IC カードの運用管理案について確認を行った。

1. 発行及び回収
 - 人事部は，従業員の入社時，派遣従業員又は嘱託従業員の受入れ時に初期化された IC カードを発行する。利用者は，受領後に利用者 PIN を設定する。
 - IC カードは，有効期限（5 年）満了時，退職時，派遣又は嘱託終了時に回収し，初期化する。
2. IC カード忘れ
 - IC カードを忘れて出社した者は，運用管理者に届け出る。
 - 運用管理者は，本人確認を行った後，臨時 IC カードに従業者番号，本人に割り当てられている利用者 ID，パスワード（以下，これらを本人情報という）及び有効期限（1 日）を書き込み，貸与する。
 - 臨時 IC カードは，その日の退社時に回収し，初期化する。
3. IC カード紛失
 - IC カードを紛失した者は，速やかに運用管理者に届け出る。
 - 運用管理者は，本人確認を行った後，IC カードの失効手続をとり，臨時 IC カードに本人情報及び有効期限（3 日）を書き込み，貸与する。
 - 臨時 IC カードは，人事部から再発行される IC カードと引換えに回収し，初期化する。
4. IC カード故障
 - IC カードが正常に動作しない場合は，運用管理者に届け出る。
 - 運用管理者は診断ツールで故障を確認した上で IC カードの失効手続をとり，臨時 IC カードに本人情報及び有効期限（3 日）を書き込み，貸与する。
 - 臨時 IC カードは，人事部から再発行される IC カードと引換えに回収し，初期化する。

図 4　IC カードの運用管理案

運用管理者は，本社，支店及び営業所（以下，事業所という）の各所に正副 1 名ずつ配置する。臨時 IC カードは，運用管理者が厳重に保管する。一時的な失効を含む失効手続をした IC カード（以下，失効 IC カードという）は，失効 IC カードリストに登録され，失効 IC カードがリーダにかざされると，このリストとの照合によって失効していることが検出される。

レビューの結果，IC カード忘れに対する運用管理に，セキュリティ対策上不備のあることが指摘され，修正した。

最後に，認証プリントを実現するシステム（以下，認証プリントシステムという）について確認を行った。

認証プリントでは，IC カードで本人を認証してからデータを印刷するので，これまで散見されていた，印刷物の取違えや長時間放置を防止することができる。

図 5 は認証プリントシステムの構成である。業務サーバからの印刷要求は，プリントサーバにスプールされる。認証プリンタの横に設置されたリーダに IC カードをかざすと，認証プリンタがプリントサーバにログインし，利用者 ID でひも付けされたデータが印刷される。スプールは共用されるので，決まった認証プリンタではなく，近くの空いている認証プリンタを使うことができる。

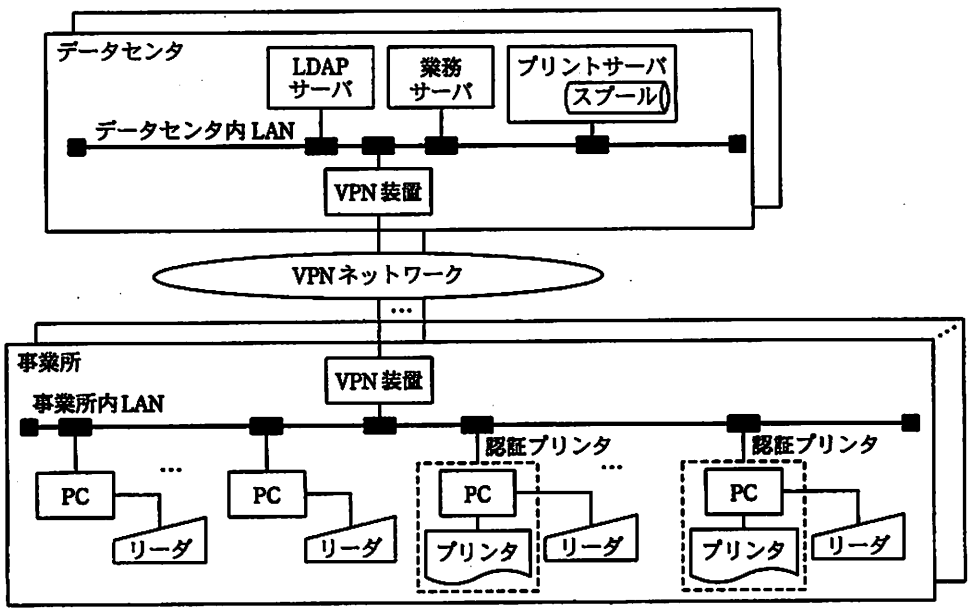

図 5　認証プリントシステムの構成

2 日間にわたるレビューが終了し，K 主任は指摘事項を反映して詳細設計に入った。

設問1　ICカードのセキュリティ要件について，(1)～(3)に答えよ。

(1) 図2中の［　ア　］に入れる要件を25字以内で述べよ。

(2) 本文中の［　イ　］に入れる性質を10字以内で答えよ。

(3) 本文中の［　a　］，［　b　］に入れる適切な字句を，それぞれ2字で答えよ。

設問2　ICカードとPCの間の相互認証について，(1)，(2)に答えよ。

(1) 図3中の②，③，⑤，⑥の処理でそれぞれ使用する鍵を番号で答えよ。

(2) 図3中の［　c　］に入れる処理の内容を，10字以内で答えよ。

設問3　PINによる制御について，(1)，(2)に答えよ。

(1) ICカード内の格納情報のうち，利用者PINを入力したときだけ読み出せるようにすべき情報と，書き込めるようにすべき情報を，それぞれ一つずつ，表の項番で答えよ。

(2) ICカード内の格納情報のうち，管理者PINを入力したときだけ書き込めるようにすべき情報は何か。表の項番を五つ選んで答えよ。

設問4　ICカードの運用管理について，(1)，(2)に答えよ。

(1) 失効ICカードリストに登録するICカード内の格納情報は，何が最も適切か。表の項番を一つ選んで答えよ。また，その理由を20字以内で述べよ。

(2) ICカードの不正使用を防止するために，ICカード忘れに対する運用管理に追加すべき措置を35字以内で述べよ。

設問5　認証プリントシステムの残留リスクについて，(1)，(2)に答えよ。

(1) PINを入力しないことで生じる認証プリントシステムの残留リスクを，50字以内で述べよ。

(2) (1)の残留リスクを低減するために，プリントサーバにおいてとるべき措置を30字以内で述べよ。