問 1　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 1～4 に答えよ。

D 社は，全国でマンションの開発・メンテナンスを手掛ける中堅の不動産デベロッパである。D 社は各地域を担当する四つの子会社をもち，各子会社はそれぞれ複数の事業部門をもつ。D 社及び子会社（以下，D 社グループという）は，積極的に人材交流を行い，人材育成及び人材活用を推進している。D 社グループの構成を表 1 に示す。

表 1　D 社グループの構成

会社名	役割
D 社	持株会社であり，D 社グループの戦略立案を担当する。グループ人事部門，グループ財務部門，研究部門などが，それぞれ D 社グループ全体の業務を担当する。
E 社	D 社の子会社であり，東日本地域の事業を担当する。
F 社	D 社の子会社であり，西日本地域の事業を担当する。
G 社	D 社の子会社であり，南日本地域の事業を担当する。
H 社	D 社の子会社であり，北日本地域の事業を担当する。

D 社グループの従業員（以下，グループ従業員という）には，D 社グループ内で一意となる番号（以下，グループ従業員番号という）が付与されている。また，オフィスや現場事務所の入室及び退室時に必要となる専用の IC カード（以下，入退室カードという）が貸与されている。D 社グループ各社にはそれぞれ IT 部門がある。D 社グループの全ての入退室カードは，D 社の IT 部門が管理している。各社の IT 部門は，自社従業員が利用する PC 及びネットワークを管理しており，D 社の IT 部門は，それらに加えて人事，経理などのバックオフィス系のシステムを管理している。

各事業部門は，それぞれ専用の Web システム（以下，事業用システムという）を多数運用している。D 社の子会社が実施するプロジェクトに参加する D 社グループ及び取引先のプロジェクトメンバには，必要に応じて事業用システムのアカウントが付与される。事業用システムは，今後も新しいシステムの導入や既存システムの更新が見込まれている。

〔IT 部門の統合〕

D 社では，IT による業務効率向上，コスト削減及び情報セキュリティ強化を目的に，D 社グループ各社の IT 部門を統合し，D 社内にシステム部を創設することにし

た。

システム部長に任命された M さんは，体制の整備とともに，D 社グループ各社のシステムに関する調査を進めた。事業用システムの多くは，利用者 ID とパスワードで利用者を認証していた。調査の結果，各事業用システムは，類似した利用者認証機能を備えており，利用者認証の統合又は共通化によって業務の効率向上が可能であることが分かった。また，事業用システムの多くは TLS を利用していた。このうち，社内向け事業用システムでは，D 社グループ各社が個別にプライベート認証局を準備し，サーバ証明書を発行していた。事業用システムの利用者認証には，次の問題点があることが分かった。

問題点 1　現場事務所において，現場担当者が自身の利用者 ID とパスワードを紙に書いて PC に貼り付けているケースが散見された。また，利用者 ID とパスワードを，他人に教えたケースも複数あった。

問題点 2　取引先に付与したアカウントについても問題点 1 と同様のケースがあった。

問題点 3　一部の事業用システムでは，取引先の従業者間でアカウントを共用することを許可している。

問題点 4　パスワード忘れへの対応及び新規利用者への初期パスワードの発行は，事業部門にとって大きな負担となっている。

〔新システムの導入〕

議論の結果，システム部が汎用的な利用者認証の仕組み（以下，共通サービスという）を構築し，各事業用システムに提供することが最善と判断された。各事業用システムは，今後，既存の利用者認証機能の代わりに，共通サービスを利用する。

共通サービスでは，利用者 ID とパスワードに代えて，新規に発行する IC カード（以下，認証カードという）を利用者認証に利用する。利用者は，PC に接続されたカードリーダに認証カードを挿入することで，事業用システムにログインする。

システム部は，共通サービスを提供するために，認証カードの発行機能と認証局の機能を備えた新システム（以下，J システムという）を導入することにし，J システムの基本要件を図 1 のとおりに整理した。

・事業用システムに対して，利用者認証の仕組みを提供する。事業用システムにおける利用者の権限については，Jシステムで取り扱わない。
・利用者認証の対象者（以下，認証対象者という）は，業務上，いずれかの事業用システムを利用する必要があるグループ従業員及び取引先の従業者に限る。
・認証対象者に，本人用の公開鍵証明書（以下，利用者証明書という）を発行し，利用者証明書と，対応する秘密鍵とを格納した認証カードを貸与する。事業用システムは，利用者証明書のsubjectフィールドに記載された認証対象者の情報を用いて，認証対象者を識別する。
・グループ従業員に貸与する認証カードは，一人1枚とする。役職の変更，部署異動，D社グループ内での出向・転籍があっても，認証カード及び利用者証明書は再発行せず，そのまま継続利用する。ただし，更新などの認証カード切替え時においては，各地域と郵送でのやり取りが必要なので，最長1か月間，新旧2枚を貸与する。
・認証カードには有効期間をもたせ，認証カードの有効期間と利用者証明書の有効期間を一致させる。有効期間内に認証カードを失効させる場合，Jシステムは，当該認証カードの利用者証明書についての失効情報を事業用システムに開示し，提供する。失効情報の開示は，失効の必要性が生じてから1営業日以内に行う。
・事業用システムのサーバのサーバ証明書を発行する。
・サーバ証明書に依拠するPCなどの機器向けに，サーバ証明書の失効情報を開示し，提供する。

図1　Jシステムの基本要件

〔認証カードの方式設計〕

M部長は，部下のNさんに対して，D社の情報セキュリティ室のR主任の支援を受けつつ，方式設計を進めるように指示した。

次は，認証カードの方式設計についての，Nさんと R主任との会話である。

Nさん：パスワードを用いる利用者認証では，ログインする人の［ a ］を確認していました。認証カードを利用する利用者認証では，認証カードの［ b ］を確認することになりますね。

R主任：そうだね。加えて，認証カードの利用時にPINを入力させることで，2種類の方法を組み合わせた［ c ］認証にすることができる。ただし，①認証対象者が不適切な行為をすると，その効果は望めない。

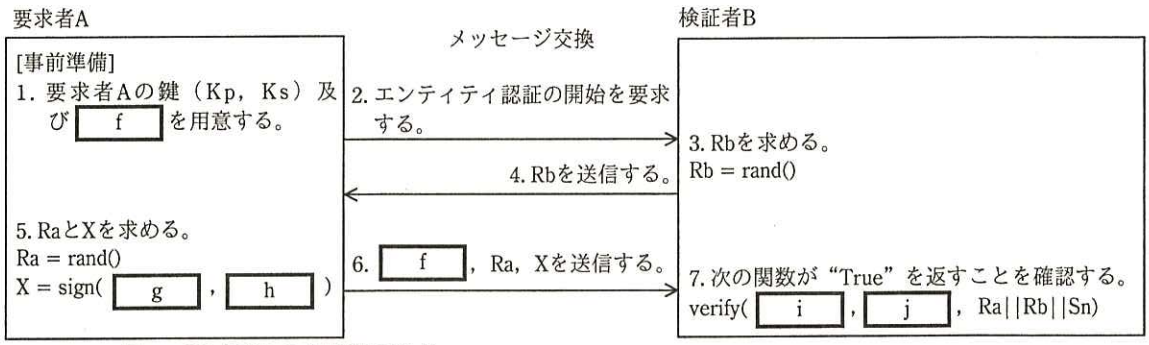
Nさん：認証カードを導入すると，利用者IDとパスワードを使わなくなるので，問題点1と問題点2は解決しますね。ICカードにPKIを組み合わせるのはなぜですか。

R主任：ICカードを利用者認証に用いる二つの方法を比べてみよう。一つ目は，PKIを用いない方法で，ICカードに利用者認証情報を記録し，利用者認証時にこれを読み出してその値を比較することによって認証する方法だ。この方

法では，IC カードに記録された利用者認証情報を読み出して処理するため，それが何らかの理由で漏えいした場合に，簡単に悪用されるおそれがある。二つ目は，PKI を用いて，IC カードに公開鍵暗号方式の秘密鍵とそれに対応する利用者証明書を格納する方法だ。

N さん：後者の方法では，どのように認証するのですか。

R 主任：公開鍵暗号技術を用いてエンティティ認証を行うプロトコルを，図 2 に示す。これは片方向認証の場合で，検証者 B が要求者 A を認証している。J システムでは，検証者 B は［ d ］に相当し，要求者 A は［ e ］に相当する。



Kp ： 要求者Aの公開鍵である。
Ks ： 要求者Aの秘密鍵である。
rand() ： 擬似乱数生成関数。ランダムな値を生成して返す。
sign(x, y) ： ディジタル署名生成関数。秘密鍵 x と署名対象データ y を受け取り，署名値を返す。
verify(s, t, u) ： ディジタル署名検証関数。公開鍵 s, 署名値 t 及び署名対象データ u を受け取り，t が u に対する正しい署名値であれば“True”，それ以外の場合は“False”を返す。
Sn ： 検証者 B の名称。公知の情報である。
|| ： この記号の左右のデータを連結することを示す。
注記　公開鍵証明書の正当性の確認についての記述は省略している。

図 2　公開鍵暗号技術を用いたエンティティ認証のプロトコル

N さん：図 2 のプロトコルを使う上での注意点はありますか。

R 主任：2 点ある。1 点目は，認証が成立するためには，鍵が［ k ］していないことが必要であることだ。事業用システムは，利用者証明書の失効情報を確認しなければならない。認証カードの紛失時などの場合，認証局は速やかに当該利用者証明書についての失効情報を提供する。失効情報は，CRL の配布により，又は［ l ］を使って提供されることが多い。

2 点目は，暗号技術は常に攻撃にさらされているので，米国国立標準技術

研究所（NIST）や②CRYPTREC の文書などを参考に，適切な暗号技術を利用するようにしなければならないことだ。

Nさん：よく分かりました。

市販されている IC カードの中には，認証カードとして利用できるとともに，D 社グループの入退室管理システムにおいて入退室カードとしても利用できるものがあり，Nさんは，そのうちの一つを採用することにした。

Jシステムの導入は，次の四つのフェーズに分けて行う。

試験フェーズ1　グループ従業員の一部だけに認証カードを貸与し，サーバ証明書の発行を開始する。認証カードは，事業用システムの利用者認証のためだけに利用する。

試験フェーズ2　一部の取引先の従業者にも認証カードを貸与する。

試験フェーズ3　認証カードを入退室カードとしても利用する。認証カードを貸与された者は，それまで利用していた入退室カードが無効化され，利用できなくなる。

本番フェーズ　事業用システムにアクセスする必要がある全グループ従業員と取引先の従業者に対して，認証カードの貸与を開始する。

〔認証カードの運用設計〕

Nさんは，試験フェーズ1における認証カードの利用開始及び失効の手順について，図3及び図4に示す案を作成した。

1. グループ従業員は，システム部が準備する申請受付用のサーバ（以下，受付サーバという）にアクセスし，認証カードの利用を申請する。
2. システム部は，毎週月曜日に，前週の月曜日から前日の日曜日までの受付分について，グループ従業員本人による申請であることの確認及び③他の必要な確認を行う。
3. システム部は，認証カード作成専用 PC を用いて認証カードを作成する。申請者専用の鍵と利用者証明書を作成し，認証カードに登録する。認証カードにはそれぞれ固有の識別番号を付与する。識別番号は認証カードの裏面に記す。
4. システム部は，作成した認証カードを申請者に送付する。別途，識別番号を記した紙を申請者に配布する。
5. 申請者は，認証カードを用いて受付サーバにログインし，認証カードの受領を登録する。

図3　認証カードの利用開始手順案

1. グループ従業員又はその上長が，受付サーバにログインし，失効させる認証カードの識別番号又はグループ従業員番号と，失効させる事由を入力し，失効を申請する。失効させる事由は，表2に示す選択肢から選ぶ。
2. 失効の申請者は，可能であれば，当該認証カードをシステム部に送付して返却する。
3. システム部は，毎週火曜日に，前週の月曜日から前々日の日曜日までの受付分について，グループ従業員本人又はその上長による申請であることを確認した後，利用者証明書の失効を失効情報サーバに登録して公開する。表2に示す失効事由の値を公開情報に含める。

図4　認証カードの失効手順案

表2　失効事由

失効申請時の失効事由の選択肢	失効事由の値 [1)]
退職又は事業用システムの利用終了	affiliationChanged
認証カードの紛失	keyCompromise
認証カードの故障	cessationOfOperation
認証カードの更新	superseded
鍵の不正利用のおそれ	keyCompromise

注 [1)]　失効事由の値は，JIS X 5731-8:2003（ITU-T X.509）に規定された“CRLReason”に相当する。

Jシステムの運用に係る補足情報を図5に示す。

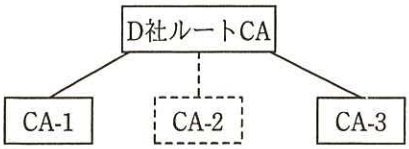
1. システム部の定常業務
   ・認証カードの利用開始，失効などを，認証カード管理簿に記録し，管理する。
   ・認証カードの申請者に認証カードを送付した後，1週間たっても受領の登録がない場合，上長経由の確認など何らかの対応を行う。
   ・人事情報を基に退職者の利用者証明書を失効させる。認証カードは退職時に返却を求める。
2. その他の補足事項
   ・認証カードと利用者証明書の有効期間は5年とする。継続利用の場合には，新しい認証カードを発行する。有効期間終了時，認証カードを回収する。

図5　Jシステムの運用に係る補足情報（抜粋）

R主任は，Nさんの設計案をレビューし，④失効情報の提供手順に不備があるので改善すべきであると指摘した。Nさんが設計案を修正した後，R主任は再レビューを行い，指摘した不備が解決していることを確認した。

〔認証局階層とサーバ証明書〕

Jシステムは，複数の認証局の鍵を管理し，利用者証明書及びサーバ証明書を発行する機能をもつ。D社の認証局の階層案を図6に示す。



CA-1：グループ従業員用の利用者証明書を発行
CA-2：取引先の従業者用の利用者証明書を発行
CA-3：サーバ証明書を発行

注記　破線は，試験フェーズ2で整備する予定のものを示す。

図6　D社の認証局の階層案

CA-3 が発行したサーバ証明書は，社内向け事業用システムのサーバに加え，特定の取引先がアクセスする社外向け事業用システムのサーバにも利用される予定である。サーバ証明書の失効情報は，D社グループ社内の各機器及び取引先からアクセス可能な場所で開示する。システム部は，D社グループ各社の要請に従い，サーバ証明書の発行・失効を行う。

システム部は，既存の PC 管理の仕組み及び PC のメンテナンスの機会を利用し，⑤グループ従業員が利用する PC に D 社ルート CA の公開鍵証明書を登録する。取引先の従業者がアクセスするサーバで J システムのサーバ証明書を利用する場合には，当該サーバを利用する全ての取引先に対して，D 社ルート CA の公開鍵証明書を配布する。この際，D 社の認証局が万が一何らかの原因で不正操作される可能性を想定し，⑥取引先においては，D 社ルート CA の公開鍵証明書を，当該サーバだけにアクセスする専用の PC にインストールするよう要請する。

これらの設計案は M 部長に報告され，承認された。J システムは実装され，試験フェーズ 1 が開始された。一部の事業用システムは，J システムの利用者証明書を用いて認証を行うように改修された。また，一部のサーバでは，CA-3 が発行したサーバ証明書の利用が開始された。

〔取引先の従業者への認証カードの貸与〕

試験フェーズ1の開始から3か月後に，試験フェーズ2の準備が開始された。

N さんは，取引先に認証カードを貸与する方式を設計し，表3の二つの案にまとめた。取引先へ認証カードを導入するに当たっての機能要件は，従業者を個人ごとに識別・認証できること，及び事業用システムの操作履歴を記録し，プロジェクトごとに表示できることである。N さんは，方式 A 及び方式 B はともに機能要件を満たしていると判断した。また，方式の選択に際して優先される非機能要件は，第 1 に

事業部門での管理工数が少ないこと，第 2 にシステム部での管理工数が少ないことである。

表 3　取引先の従業者への認証カード貸与方式案（抜粋）

項目	方式 A	方式 B
概要	プロジェクトごとに，取引先の従業者に認証カードを貸与。複数のプロジェクトに参加する者には，複数枚を貸与	取引先の従業者に，認証カードを一人 1 枚貸与
貸与対象者	取引先の従業者（ただし，試験フェーズ中は一部の取引先の従業者に限定）	
貸与枚数	貸与対象者に対してプロジェクトごとに 1 枚	貸与対象者ごとに 1 枚
貸与期間	プロジェクトへの参加期間	いずれかのプロジェクトへの参加期間（ただし，半年以内に次のプロジェクトへの参加が見込まれる場合は貸与を継続）
管理責任者	プロジェクト責任者	システム部（ただし，プロジェクト責任者は，プロジェクトへの参加期間を届け出る。）
システムの権限管理	事業用システムの利用権限は，プロジェクト責任者の要請に従い，事業部門で登録及び解除。事業部門は，プロジェクトへの参加期間だけ有効な権限をシステムに登録	
操作履歴の取得	複数のプロジェクトに参加する従業者の操作履歴は，認証のログを基に，プロジェクトごとに識別可	複数のプロジェクトに参加する従業者の操作履歴は，認証のログと事業用システムの利用権限に係るログを組み合わせることで，プロジェクトごとに識別可
その他の補足事項	業務上の役割と認証カードを結び付け，権限管理をシンプルかつ柔軟に運用可	

注記 1　管理責任者は，貸与対象者への認証カードの配布及び貸与対象者からの回収を行う。
注記 2　認証カードに登録された利用者証明書は，認証カードの紛失時を除き，管理責任者が認証カードを回収した後にシステム部が失効処理を行う。紛失時は，遅滞なく失効処理を行う。

N さんが取引先について過去数年分のプロジェクトへの参加状況を調査したところ，取引先の従業者は最多で五つのプロジェクトに同時に参加していた。また，専門技術をもつ工事関係取引先の従業者は，各プロジェクトへの参加期間は短いが，1 か月以内に次のプロジェクトに参加することが多いことが分かった。取引先の従業者の 3 割程度が，このような工事関係取引先の従業者であった。

検討の結果，N さんは，方式 B が非機能要件の面で優位と考え，M 部長に提案し

た。M 部長は提案された方式を承認し，実装が開始された。その後，試験フェーズ 2 が開始され，取引先の従業者への認証カードの貸与が始まった。

試験フェーズ 2 は，おおむね順調だったが，問題が二つ確認された。

・グループ従業員が認証カードをオフィスに置き忘れ，現場事務所で同僚に認証カードを借りて利用するケースが複数あった。
・グループ従業員が現場事務所に認証カードを保管し，本人以外に利用させているケースがあった。

これらの不正の防止には，当初から計画されていた，⑦認証カードを入退室カードとしても利用するという措置が一定の効果をもつと判断された。試験フェーズ 3 では，この措置が実施された。

〔本番フェーズの開始〕

その後，本番フェーズへの移行は順調に進んだ。事業用システムは全て，J システムの利用者証明書を用いて認証を行うように改修が進められた。また，TLS を利用する社内向け事業用システムのサーバは全て，CA-3 が発行したサーバ証明書を利用することになった。J システムの導入によって，事業用システムに係る問題点 1〜4 は全て解決した。

設問 1　〔認証カードの方式設計〕について，(1)〜(5)に答えよ。

(1)　本文中の［ a ］〜［ c ］，［ k ］及び［ l ］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　HMAC	イ　OCSP	ウ　記憶
エ　危たい化	オ　所持	カ　生体情報
キ　多機能	ク　単要素	ケ　ディジタル署名
コ　ハッシュ値	サ　非アクティベート	シ　フィンガプリント
ス　複数要素	セ　ルート CA	

(2)　本文中の下線①について，R 主任が想定している不適切な行為を，35 字以内で具体的に述べよ。

(3) 本文中の［ d ］，［ e ］及び図 2 中の［ f ］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 共通鍵	イ サーバ証明書	ウ 事業用システム
エ 信頼できる第三者	オ 認証局	カ 認証対象者
キ 秘密鍵	ク 利用者証明書	

(4) 本文中の下線②について，CRYPTREC の“電子政府推奨暗号リスト”に含まれている暗号技術を解答群の中から全て選び，記号で答えよ。ただし，“電子政府推奨暗号リスト”は，CRYPTREC 暗号リスト（平成 28 年 3 月 29 日版）に掲載されているものとし，暗号技術はハッシュ関数を含むものとする。

解答群

ア AES	イ Camellia	ウ DES
エ ECDSA	オ MD4	カ MD5
キ RSA-OAEP	ク SHA-256	ケ SHA-512

(5) 図 2 中の［ g ］～［ j ］に入れる適切な式を解答群の中から選び，記号で答えよ。

解答群

ア Kp	イ Ks	ウ Ra	エ Ra||Rb
オ Ra||Rb||Sn	カ Ra||Sn	キ Rb	ク Rb||Ra
ケ Rb||Ra||Sn	コ Rb||Sn	サ Sn	シ Sn||Ra||Rb
ス Sn||Rb||Ra	セ X	ソ rand( )	

設問 2 〔認証カードの運用設計〕について，(1)～(3)に答えよ。

(1) 図 3 中の下線③について，J システムの基本要件を満たすために，システム部が確認すべき事項を二つ挙げ，それぞれ 30 字以内で述べよ。

(2) グループ従業員用の利用者証明書の subject フィールドに記載するグループ従業員の情報について，必要不可欠なものを解答群の中から全て選び，記号で答えよ。

解答群

ア グループ従業員番号	イ 氏名	ウ 所属会社名
エ 所属部署の電話番号	オ 所属部署名	カ 役職名

(3) 本文中の下線④について，改善すべき不備を 40 字以内で具体的に述べよ。また，この不備は，失効事由の値がどのような値となっている場合に事業用システムの不正利用に結び付く可能性が高いか。該当する失効事由の値を解答群の中から全て選び，記号で答えよ。

解答群

ア affiliationChanged　　イ cessationOfOperation

ウ keyCompromise　　エ superseded

設問３　〔認証局階層とサーバ証明書〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑤について，この措置を行わない場合，CA-3 が発行したサーバ証明書を利用するサーバにグループ従業員が Web ブラウザでアクセスすると，どのような不都合が生じるか。30 字以内で具体的に述べよ。

(2) 本文中の下線⑥の要請は，取引先のどのようなリスクを軽減するためか。45 字以内で具体的に述べよ。

設問４　〔取引先の従業者への認証カードの貸与〕について，(1)～(3)に答えよ。

(1) 方式 A 及び方式 B では，管理責任者による認証カードの回収の遅れ又は漏れがあっても事業用システムの不正利用の影響を抑えることができる。この理由について，“認証”，“認可”の二つの字句を用いて，40 字以内で述べよ。

(2) 方式 B の方が非機能要件に適合している理由を表 3 の内容に基づいて二つ挙げ，それぞれ 40 字以内で具体的に述べよ。

(3) 本文中の下線⑦について，見つかった不正に対して，この措置が効果をもつと判断した根拠を，40 字以内で述べよ。