次の問1は必須問題です。必ず解答してください。

問1　生体認証システムの導入に関する次の記述を読んで，設問1～3に答えよ。

S社は，個人投資家を対象とした，従業員約200人の証券会社である。事務所では従業員に一人1台のPCが割り当てられている。社内ではディジタル証明書による認証は利用しておらず，全ての業務システムは従業員ID（以下，IDという）とパスワードでログインできるようになっている。S社では，システム管理者がIDを一括管理できるようにするために，ID管理システムを導入している。ID管理システムは，氏名などの個人情報とIDを関連付けており，認証サーバとしての役割も兼ねている。

業務システムには，出張手配や勤怠管理を行う総務システム，顧客との取引情報を管理する顧客管理システムなどがある。個別の顧客との取引情報は，その顧客を担当している従業員と直属の上司だけが閲覧することを許されている。

〔セキュリティインシデントの発生〕

ある従業員が担当している顧客の取引情報を，別の従業員が不正に入手して利用するというセキュリティインシデントが発生した。調査の結果，IDとパスワードの不適切な管理によって，IDとパスワードを不正利用されてしまったことが分かった。この事態を重く見たS社は，業務システムへの不正アクセスを防ぐために，セキュリティの強化を図ることにした。

〔不正アクセス予防策の実施〕

S社では，IDとパスワードのクラッキングや業務システムへの不正アクセスの対策として，予想される不正アクセスに対応する予防策を実施した。予防策は，実施されたことが確実に確認できるものに限定した。その抜粋を表1に示す。

表1　予想される不正アクセスとその予防策（抜粋）

| 予想される不正アクセス | 予防策 |
|---|---|
| 他の従業員が，ログインが成功するまでパスワードを変えて試行する。 | a |
| 他の従業員がパスワードを類推してIDを使用する。 | b |
| 他の従業員がパスワードを入手して，長期間にわたって業務システムを不正利用する。 | 3か月に1回のパスワード変更を強制し，過去4回分のパスワードを使用できないように設定する。 |

対策を導入してから 6 か月経過した時点でセキュリティ監査を実施し，次の問題を確認した。

・パスワードを書いたメモ用紙をディスプレイに貼っている従業員がいる。

・パスワードを忘れた従業員に対する，システム管理者によるパスワード再発行業務の負荷が高まっている。

〔生体認証システムの導入〕

S 社では，業務システムへの不正アクセスを防止するために，ID とパスワードによる認証以外の手段を用いた，新たな認証システムの導入を検討することにした。総務部では，新たな認証システムの導入に当たって，認証に必要な情報をシステム管理者側で一括管理できることと，導入コストが安価であることを基本方針とした。

導入担当となった総務部システム課の T 君は，新たな認証システムの方式として，IC カード方式と生体認証方式を検討した。

基本方針に基づき T 君が検討した認証方式を表 2 に示す。

表 2　T 君が検討した認証方式

| 認証方式 | 概要 | 導入時の注意事項 |
|---|---|---|
| IC カード方式 | IC カードに埋め込んだ利用者の秘密鍵と PIN コードで認証する。 | ・新たに［ c ］の導入が必要となる。<br>・使用する PC ごとに IC カードリーダが必要となる。<br>・IC カードの盗難や紛失時に，対象の IC カードの利用停止と新たな IC カードの発行が必要である。 |
| 生体認証方式 | 生体情報をセンサで読み取り，あらかじめ登録しておいた生体情報との類似度が高いことで認証する。導入コストが安価なものとして指紋認証方式がある。 | ・使用する PC ごとにセンサが必要となる。<br>・誤って他人を本人と認識する確率（以下，他人受入率という）と，誤って本人を拒否する確率（以下，本人拒否率という）は，いずれもできるだけ低いことが望ましい。<br>・他人受入率が低い製品を選ぶと，本人拒否率は高くなる傾向にあるので，両者のバランスを考慮する必要がある。 |

T 君は，導入コスト，新たな認証システムの運用に掛かる業務負荷の軽減，及びセキュリティ強化の契機となったセキュリティインシデントへの対応の観点から，指紋認証方式を採用することにした。

この方式の採用に当たり，氏名などの個人情報と指紋情報が同時に漏えいしないように，個人情報と指紋情報を物理的に分けた上で，一括管理を行う方針とする。

〔導入製品の決定〕

指紋認証には，次の2種類の方式がある。

・マニューシャ方式

皮膚が線状に隆起した隆線の分岐や終端部分の位置・種類・方向などの指紋特徴点（マニューシャ）を登録する。指紋特徴点だけでは元の指紋全体を再現できない。

・パターンマッチング方式

指紋全体をスキャンしてデータ化し，パターンマッチングする。

T君は，他社における指紋認証システム導入の事例を調査した。その結果，登録された指紋情報が漏えいすることや，他の目的で利用されることへの従業員の不安が大きいことが分かった。

T君は，万が一指紋情報が漏えいした場合でも①実害が少ないと考えて，マニューシャ方式を採用している製品を調査して，導入コストがほぼ同じ製品について比較検討した。その比較結果を表3に示す。

表3　指紋認証製品の比較結果

| 製品名 | 他人受入率 | 本人拒否率 | 指紋情報の格納場所 |
|---|---|---|---|
| A | 0.0001 | 0.001 | PC内 |
| B | 0.00001 | 0.002 | 専用の認証サーバ内 |
| C | 0.00001 | 0.005 | PC内 |
| D | 0.00009 | 0.002 | 専用の認証サーバ内 |
| E | 0.00001 | 0.007 | 従来の認証サーバ内の拡張領域 |

T君は，認証に必要な情報を一括管理するために，指紋情報がPC内に格納される製品を除外した。残った製品から［ d ］という理由と［ e ］という理由で，製品名［ f ］の製品を選択し，上司に報告した。

設問1　〔不正アクセス予防策の実施〕について，(1)，(2)に答えよ。

(1)　表1中の［　a　］に入れる最も適切な予防策を解答群の中から選び，記号で答えよ。

解答群

ア　業務システムとPCとの通信を暗号化する。

イ　直前のログイン記録を次回ログイン時に表示する。

ウ　パスワードを3回続けて間違えると，アカウントをロックする。

エ　ログインエラーが発生した日時を本人にメールで後日通知する。

(2)　表1中の［　b　］に入れる適切な予防策を解答群の中から二つ選び，記号で答えよ。

解答群

ア　IDと同じ文字列をパスワードに含めることを禁止する。

イ　英字，数字，記号が混在する8字以上のパスワードを設定させる。

ウ　他人とのパスワードの共有を禁止する。

エ　パスワードのヒントを設定して，自分だけが知っている答えをパスワードの一部に使用させる。

設問2　表2中の［　c　］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　LDAP　　イ　PKI

ウ　SSL　　エ　リバースプロキシ

設問3　〔導入製品の決定〕について，(1)，(2)に答えよ。

(1)　本文中の下線①で，マニューシャ方式は実害が少ないとT君が考えた理由を，その特徴に着目して25字以内で述べよ。

(2)　本文中の［　d　］，［　e　］に入れる適切な理由を，それぞれ30字以内で述べよ。また，［　f　］に入れる適切な製品名を，A～Eの中から選んで答えよ。