SC

平成21年度　秋期
情報セキュリティスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
5. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問4
選択方法	2問選択

6. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に，**受験番号**を記入してください。正しく記入されていない場合は，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。
   (4) **選択した問題**については，次の例に従って，**選択欄の問題番号**を**○印**で囲んでください。
   なお，○印がない場合は，採点の対象になりません。3問以上○印で囲んだ場合は，はじめの2問について採点します。
   (5) 解答は，問題番号ごとに指定された枠内に記入してください。
   (6) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3を選択した場合の例〕

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　電子メールからの情報漏えいとその対策に関する次の記述を読んで，設問1～5に答えよ。

A社は，業務用機械の製造と販売を行う従業員数800名の会社である。営業部門には全国10都市の支店を含めて100名の部員がいる。営業活動においては，顧客への訪問回数を増やすことによる受注拡大や，顧客からの質問への迅速な対応による顧客満足度向上の取組みに重点を置いている。そのため，外出が中心になってもこまめに電子メール（以下，メールという）のチェックを行えるよう，日常的にPCを持ち歩く部員が多い。メールでは価格表や提案書などの機密データを社内関係者とやり取りすることが多い。また，営業部門の部員は顧客との連絡用に会社貸与の携帯電話を持ち歩いている。A社では情報セキュリティの管理体制として情報セキュリティ委員会を設置し，情報セキュリティ対策基準を2年前に策定している。

〔事故の発生〕

営業部門では，最近の報道で，PCの紛失や盗難による情報漏えい事故が目立っていることを受け，PCの持出しを自粛することに決めた。しかし，営業部門の部員の中には，PCを持ち出さないまでもメールの閲覧だけはしたいと考え，会社貸与の携帯電話の従業員用メールアドレスにメールを転送する者がいた。自粛を決めてから数か月たったある日，①会社貸与の携帯電話の紛失による情報漏えい事故が発生した。携帯電話を紛失したこと，携帯電話端末にメールが保存されていたこと，そして，キーロック解除用の暗証番号が設定されていなかったことが情報システム部門に直ちに報告された。後日，特定の顧客にしか開示しない価格表の漏えいが確認された。

〔再発防止のための検討〕

今回の事故の報告を受け，事態を深刻に受け止めた情報システム部長は，情報システム部門のG課長に改善策を検討するよう指示した。G課長は，営業部門の関係者から事情を聞いた結果，情報セキュリティ対策基準及びメールシステムが情報漏えい対策の観点で不十分ではないかと考え，見直しをF主任に指示した。

A社の情報セキュリティ対策基準には，端末の利用とメールの利用について図1に示す規定がある。

5.9 端末利用
(1) 業務に利用する端末（PC，携帯電話及びPDA）は会社から貸与されたものだけとする。
(2) 端末の利用者を限定するために，利用者認証機能を有効にしなければならない。PC 及び PDA であればログイン時利用者認証機能を，携帯電話であれば暗証番号による端末操作制限機能やデータ保護機能を有効にしなければならない。
(3) 端末上で機密データを取り扱う場合，ファイル保存中は重要度に応じて［ a ］などの処置をとり，取扱いが不必要となった時点でデータを削除しなければならない。また，機密データを社外に提供する場合，提供者は情報システム部門の許可を得なければならない。
(4) 端末の盗難や紛失が発生した場合，速やかに情報システム部門に報告しなければならない。
（5.10～5.12 は省略）
5.13 メール利用
(1) 従業員用メールアドレスを利用するものとし，業務上での私有メールアドレスの利用を禁止する。
(2) 業務目的のメールを私有メールアドレスに転送することを禁止する。
(3) メールの送信に当たっては，［ b ］がないことを確認しなければならない。
(4) メールの受信に当たっては，別途定めるウイルス対策基準に基づき，ウイルスチェック機能を有効にしなければならない。
(5) やむを得ず機密データをメールで送信する場合には［ a ］しなければならない。
（以下，省略）

図1　A社における端末利用とメール利用に関する規定
（情報セキュリティ対策基準からの抜粋）

F 主任は，携帯電話に関して，別途定めた規程の内容と対策状況を確認した。まず，②A 社で使用している携帯電話の場合，盗難・紛失が起きたときの事後対策を情報システム部門が施せるにもかかわらず，実施していなかったので，実施した方がよいと考えた。また，営業部門では携帯電話端末にメールを保存しており，機密データが蓄積されがちな状況となっている。そこで，携帯電話から直接メールを安全に閲覧するシステム（以下，S システムという）を提供して，情報漏えいリスクを低減した方がよいと考えた。F 主任は，これらの改善方針を情報システム部門として取りまとめ，情報セキュリティ委員会に提示し，実現に向けた検討開始の承認を得た。

〔S システムの検討〕

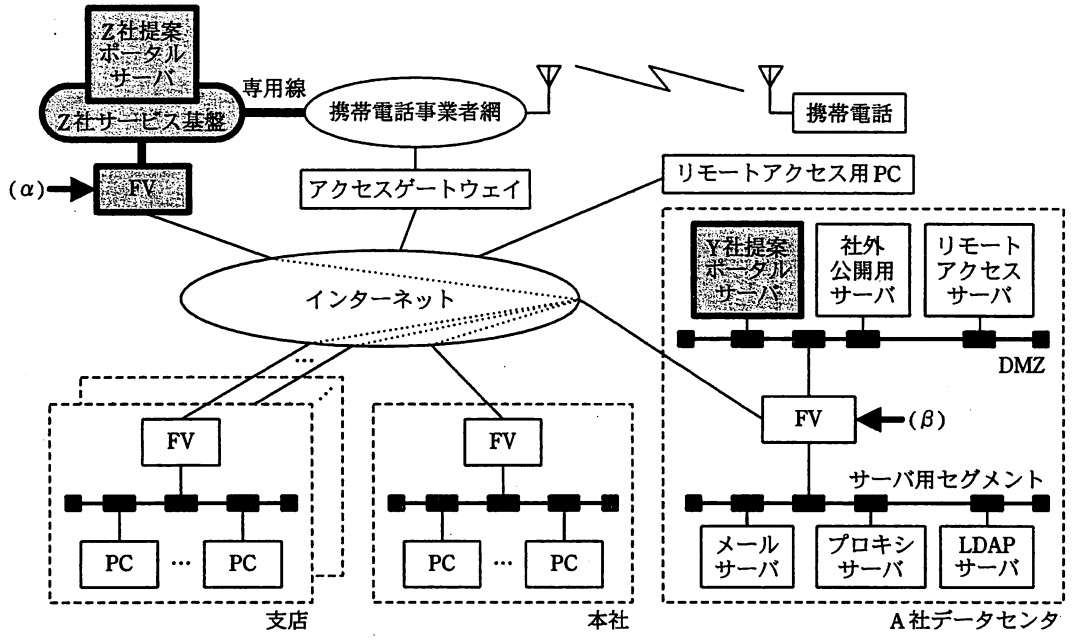
検討を開始するに当たり，G 課長からは，S システムでは，既存の PC 用のリモートアクセスシステムを参考に，認証の強度が同程度かそれ以上になるようにすること，との指示があった。

携帯電話端末にメールが保存されないようにしたいとの要望や，会社貸与の携帯電

話の事業者は 1 社であるといった現状を，F 主任が情報システムベンダ各社に伝えて S システムの提案を求めたところ，Y 社と Z 社の 2 社から提案があった。F 主任は，図 2 に示すように，A 社の現在のネットワーク構成図に Y 社と Z 社の提案の構成を書き加えるとともに，2 社の提案の特徴を表にまとめて比較した。

A 社内では，本社，支店，自社データセンタ間を IPsec によるインターネット VPN で接続している。各種サーバは自社データセンタに設置し，ファイアウォール兼 VPN ルータ（以下，FV という）及び社外公開用サーバを含めて自社で運用している。

本社や支店の PC からインターネット上の Web サーバへのアクセスは，サーバ用セグメント上のプロキシサーバを経由している。リモートアクセス用 PC が利用するリモートアクセスサーバは，DMZ 上に設置され，利用者認証にはワンタイムパスワードを利用している。ただし，既存の PC 用のリモートアクセスシステムは携帯電話からのアクセスに対応していない。



注　図中の網掛けの部分は，現在のネットワークへの追加部分であることを表す。
インターネット内の点線はインターネットVPNを表す。

図 2　A 社のネットワーク構成

表　Y社及びZ社の提案の特徴

比較項目	Y社	Z社
利用手順	携帯電話からブラウザでポータルサーバにアクセスし，認証後，業務メニュー画面からメールサービスを選択し，メールを閲覧する。メール送信はできない。	
新設サーバの有無と設置環境	ポータルサーバをA社データセンタのDMZ上に新設する（図2）。携帯電話とポータルサーバ間は携帯電話事業者網とインターネットを経由してSSLで通信する。	ポータルサーバをZ社が運営するサービス基盤上に新設する（図2）。サービス基盤は携帯電話事業者網と専用線で接続され，サービス基盤とサーバ用セグメント間はインターネットVPNで接続する。
メールサーバへの接続方法	ポータルサーバからメールサーバにIMAPで接続し，メールを閲覧する。 ③メールサーバにログインするための利用者IDとパスワードは，ポータルサーバとメールサーバ間でID連携するので，携帯電話からは直接入力しない。	
メールの保存先	メールサーバ上に保存され，削除しなければ繰り返し閲覧できる。 携帯電話端末及びポータルサーバ上への保存機能はない。	
携帯電話（利用者）の認証方法	ポータルサーバにおいてSSLクライアント認証で認証する。電子証明書は，携帯電話事業者が携帯電話のSIMカードに対して発行するサービスを利用して入手する。電子証明書のコモンネーム（Common Name）には携帯電話のSIMカードを一意に識別できる情報が記載されている。認証時，ポータルサーバはLDAPサーバへの問合せを行い，登録済の従業員であることを確認する。	ポータルサーバにおいて，Z社が提供するワンタイムパスワード方式で認証する。
PC対応の有無	あり（オプション対応）	なし

F主任は，営業部門による携帯電話の規程遵守状況から，Z社の提案を選択したいと考え，G課長に検討結果を報告した。しかし，G課長は今回の事故が発生する前から既存のPC用のリモートアクセスシステムの見直しを情報システム部長から指示されており，PC用のリモートアクセスとの統合を見込めるY社の提案も捨て難いと考えたため，F主任と意見が一致しなかった。そこで，G課長は情報システム部長に両案を説明して判断をゆだねたところ，G課長の考えどおりにY社の提案を選択することに決まった。情報システム部長からは，今回の検討では事故の再発防止のための抜本的な解決には至っていないので，運用面での改善を含めて更に詰めるようにとの指示が加えられた。その後，F主任は，営業部門を対象にした導入準備に取り掛かった。

設問1　図1中の［　a　］，［　b　］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　圧縮	イ　あて先ミス	ウ　暗号化
エ　改ざん	オ　時刻同期	カ　ディジタル署名

設問2　情報漏えい事故について，(1)，(2)に答えよ。

(1) 本文中の下線①について，どの規定の遵守が不十分であったと考えられるか。図1中から三つ選んで，“5.9 (1)”のように箇条と項番で答えよ。

(2) 本文中の下線①に記載されている価格表以外に漏えいした可能性が高い顧客の情報を，7字以内で答えよ。また，その情報について，携帯電話の紛失が判明した後，紛失した携帯電話が戻ってこなくても，情報漏えいによる被害を受ける可能性がある顧客の特定を迅速に行えるようにするための対策を，45字以内で具体的に述べよ。

設問3　本文中の下線②の対策を実現するために情報システム部門が利用する，携帯電話サービスによって提供される管理上の機能を，30字以内で具体的に述べよ。

設問4　Sシステムの構築について，(1)～(3)に答えよ。

(1) Y社の提案について，登録された従業員だけがメールを閲覧できるようにするために図2中のLDAPサーバに従業員ごとに追加登録する内容を，20字以内で述べよ。

(2) Y社の提案について，表中の下線③の特徴があるにもかかわらず，図1中の5.9の，ある規定の遵守が不十分な場合には，第三者にメールを閲覧される可能性がある。その箇条と項番を答えよ。また，その箇条と項番の規定に関連して，第三者によるメールの閲覧防止を徹底する対策について，50字以内で具体的に述べよ。

(3) Z社の提案について，図2中の(α)と(β)で示したFV間で特定のアプリケーションに絞ってIPsecを適用するとしたとき，どのサーバ間の通信の，どのプロトコルを対象にすればよいか。図2中又は表中の用語を用いて答えよ。

設問5　携帯電話端末へのメールの保存による情報漏えいを防ぐために，図1中の5.13(2)に追記したい。追記する内容を，45字以内で具体的に述べよ。

問2　Javaアプレットに関する次の記述を読んで，設問1～4に答えよ。

B社は，従業員数100名の電子部品の卸業者で，メーカから商品を仕入れ，小売業者へ販売している。B社では，2年前にリリースされたC社のソフトウェアパッケージに独自機能をもつモジュール（以下，カスタムモジュールという）を追加した在庫管理システム（以下，Xシステムという）を，3か月前に導入した。その運用と保守はC社に委託している。

〔Xシステムの概要〕

Xシステムは，ソフトウェアパッケージの本体モジュールとカスタムモジュールから構成され，それらはJavaを用いて実現されている。Xシステムの利用の操作は，普段B社従業員らがインターネットの閲覧にも用いる社内標準仕様のブラウザを用いて，クライアントPC上で行っている。

B社では，在庫管理のために，以前から携帯型のバーコード読取り端末を利用していた。読取り端末で読み取ったデータのファイルを，B社従業員がクライアントPC上でXシステム用に編集している。Xシステムでは，そのファイルを用いて在庫管理情報を更新している。

〔Xシステムのカスタムモジュール〕

カスタムモジュールのうち，ファイルが決められた書式であることとサイズが規定値以下であることの適合性チェック（以下，入力チェックという）機能，入力チェック結果を利用者に通知する機能と，適合したファイルをアップロードする機能はJavaアプレット（以下，入力チェックアプレットという）で実現されており，クライアントPC上のブラウザで実行される。また，サーバマシン上では，Xシステムとして，本体モジュールに加え，クライアントPC上の入力チェックアプレットからのファイル受信と本体モジュールへのファイル引渡しを行うモジュール（以下，ファイル受信モジュールという）があり，Javaアプレットではないアプリケーションで実現されている。したがって，Xシステム全体は，入力チェックアプレット，本体モジュールとファイル受信モジュールで構成されている。図1にXシステムの構成を示す。

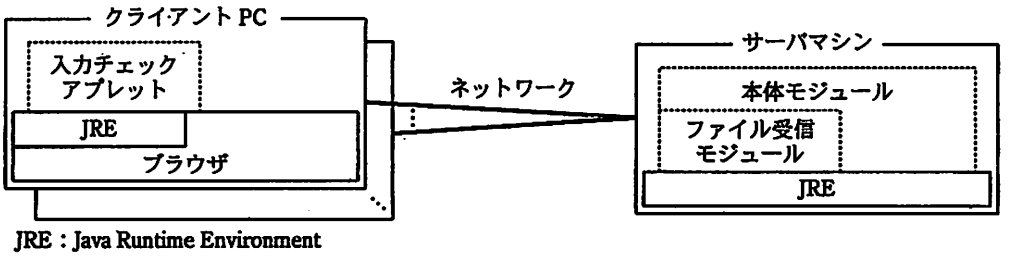


図1　Xシステムの構成

図2は，入力チェックアプレットのJavaのクラスのソースコードである。Xシステムでは，入力チェックアプレットとして構成するクラス群を［　a　］形式で一つにまとめ，［　b　］によって署名した［　a　］形式ファイルをサーバマシン上の特定のディレクトリに置き，ブラウザにダウンロードさせる。ここで，［　b　］は，有限体上の離散対数問題に基づく署名方式である。

```
public class InputCheck extends JApplet {
   private static final long MAX_FILE_SIZE = 1000000; //読み込むことを許すファイルの最大サイズ
   public void init() {
      setSize(500, 200);
      getContentPane().setLayout(null);
  (ア) JButton loader = new JButton("ファイル読込み");
      loader.setBounds(4, 3, 200, 25);
      loader.addActionListener(new ActionListener() {
         public void actionPerformed(ActionEvent e) {
            JFileChooser fileChose = new JFileChooser();
            int selected = fileChose.showOpenDialog(null);
            if (selected == JFileChooser.APPROVE_OPTION) {
               File file = fileChose.getSelectedFile();
               String filePath = file.getPath(); //ファイルのパス名の取得
               if (filePath != null) {
                  loadFile(filePath);
               } else {
                (省略) //エラー処理1
               }
            }
         }
      });
      getContentPane().add(loader);
   }

   private void loadFile(String filePath) {
      byte[] fileData = null;
      int errNo = 0;
      int length, offset = 0;
      File file = new File(filePath);
      long size = file.length();
```

```
    if ( c  MAX_FILE_SIZE) {
       try {
          FileInputStream in = new FileInputStream(filePath);
       (イ) fileData = new byte[(int)size];
          //ファイルの読込み
          while ((length = (in.read(fileData, offset, (int)size - offset))) > 0) {
             offset += length;
          }
          in.close();
       } catch (FileNotFoundException e) {
          (省略) //例外処理1
       } catch (IOException e) {
          (省略) //例外処理2
       }
    (ウ) errNo = inputCheck(fileData); //入力チェック
     } else {
        (省略) //エラー処理2
     }
     (省略) //入力チェック結果の表示，適合時はアップロード，不適合時は破棄
  }

  private int inputCheck(byte[] filePath) {
     (省略)
  }
}
```

図2　入力チェックアプレット（抜粋）

入力チェックアプレットが，クライアントPC上のブラウザ上で実行されると，図2中の下線(ア)の文の処理によってボタンが作成される。利用者がそのボタンを押すと，クライアントPCのローカルファイルを選択するダイアログボックスが図3のように表示される。次に，利用者がファイルを選択すると入力チェックが行われ，適合している場合，その旨が利用者に通知され，ファイル受信モジュールを通してアップロードされ，サーバマシン上にファイルとして保存される。適合していない場合，その旨が通知され，読み込んだデータは破棄されアップロードされない。

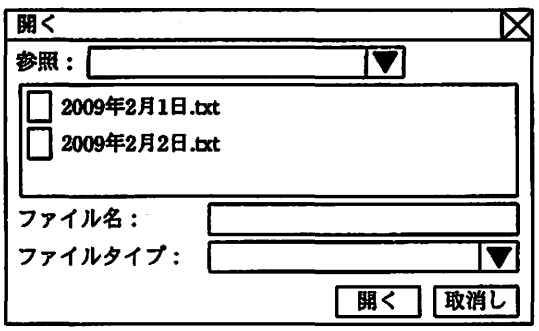


図3　JFileChooserによるファイルダイアログボックス

〔サンドボックスの概要とその脆弱性の公表〕

X システムの導入後，X システムの実行環境として想定するバージョンの JRE において，サンドボックスを回避する脆弱性（以下，当該脆弱性という）が公表され，修正された JRE の新バージョンがリリースされた。JRE のサンドボックスと当該脆弱性の概要は次のとおりである。

Java 2 以降の JRE では，サンドボックス機構における［ d ］又は SecurityManager を用いて，任意のセキュリティポリシを適用できる。JRE に用意されたデフォルトのポリシファイルを用いると，Java アプレットではない Java アプリケーションを実行する場合と，署名された Java アプレットを実行する場合，ローカルのコンピュータリソースにアクセスが可能である。他方，署名がない Java アプレットを実行する場合，そのアクセスは制限される。例えば，クライアント PC のブラウザ上で，入力チェックアプレットのようなローカルファイルへアクセスする Java アプレットを，署名なし Java アプレットとして実行した場合，［ d ］クラスによって，［ e ］がスローされる。ところが，当該脆弱性を悪用すると，署名なし Java アプレットであっても，この制限を回避して，ローカルのコンピュータリソースにアクセスできてしまう。

〔X システムでの対処〕

B 社は，当該脆弱性への対策に関して C 社と検討を行った。まず，①X システムのサーバ側とクライアント側の JRE のバージョンアップに伴う確認作業の負荷を考慮した結果，現段階では，バージョンアップに伴う作業工数の確保は難しいと判断した。しかし，②X システムのクライアント PC の JRE をバージョンアップしない場合，クライアント PC 上のブラウザで当該脆弱性が悪用される可能性がある。そこで，③Java アプレットを利用しない代替方式を検討したが，予定する期間内に実現することは難しいと判断した。よって，B 社は，④当該脆弱性への暫定処置として，サーバ側の JRE はバージョンアップせず，JRE の利用が Java アプレットに限定されているクライアント側の JRE だけバージョンアップすることとした。サーバ側の JRE のバージョンアップは，次回のシステム更新時に行うこととし，X システムを再稼働した。

設問1　本文中の［ a ］，［ b ］，［ d ］，［ e ］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　AccessController　　イ　DH　　ウ　DSA　　エ　jar

オ　java.io.IOException　　カ　java.security.AccessControlException

キ　policytool　　ク　RSA　　ケ　xml

設問2　Xシステムの Java アプレットについて，(1)，(2)に答えよ。

(1)　図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　`file <=`　　イ　`file >=`　　ウ　`size <=`　　エ　`size >=`

(2)　当該脆弱性のない JRE を用いた X システムにおいて，仮に署名がない入力チェックアプレットを実行する場合，図 2 中の下線(ア)～(ウ)の中で実行される文をすべて選び，記号で答えよ。ここで，実行の際，JRE に用意されたデフォルトのポリシファイルを用いていることとする。

設問3　当該脆弱性への対策について，(1)，(2)に答えよ。

(1)　クライアント PC の JRE をバージョンアップしない場合，どのようなときに，本文中の下線②で示す可能性が高まるか。B 社のクライアント PC の利用状況を考慮し，45 字以内で述べよ。

(2)　本文中の下線③で示す代替方式として，HTML フォームによってファイルを選択する機能と，アップロード後にサーバへファイルを保存する機能を追加したとする。このとき，X システムのサーバ側で，更にどのような機能を追加すれば代替方式となるか。追加すべき機能を二つ挙げ，それぞれ 20 字以内で述べよ。

設問4　JRE のバージョンアップについて，(1)，(2)に答えよ。

(1)　本文中の下線①にある，JRE のバージョンアップに伴う確認作業とは何か。X システムでの作業対象を図 1 中の用語を用いて示し，確認作業の内容を 55 字以内で述べよ。

(2)　本文中の下線④に関して，X システムのサーバ側の JRE をバージョンアップしなくても問題ないと判断するためには何を確認すべきか。60 字以内で述べよ。

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。

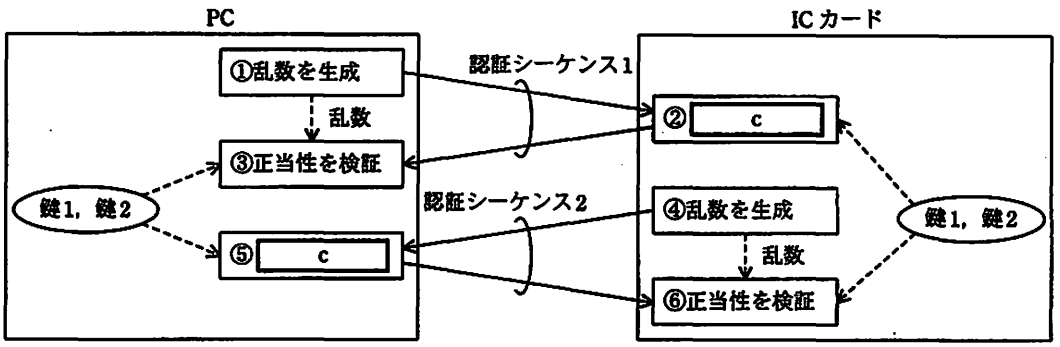


図3　ICカードとPCの間の相互認証シーケンス

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。

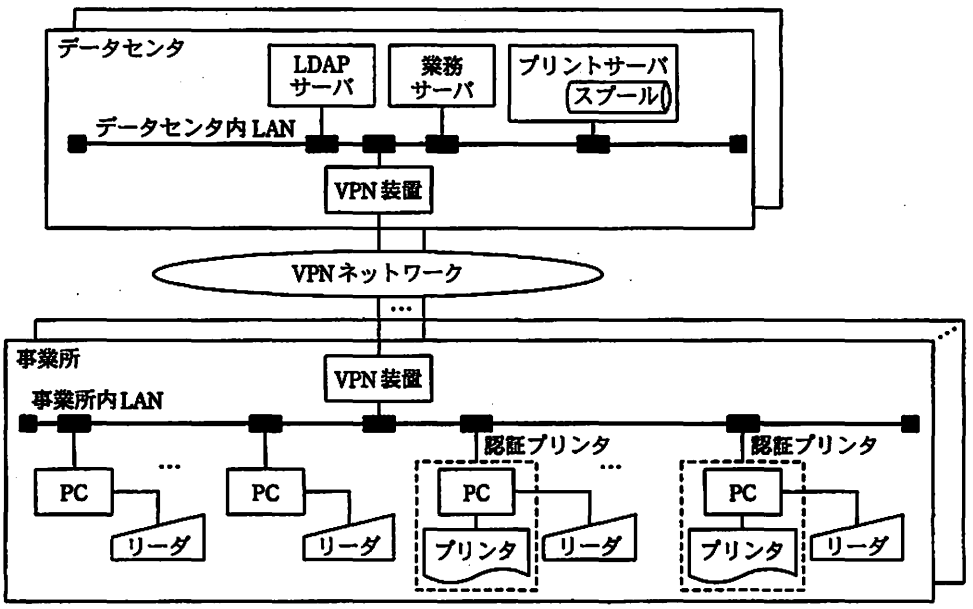


図 5　認証プリントシステムの構成

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。

問4　ノートPCの情報漏えい対策に関する次の記述を読んで，設問1～5に答えよ。

E社は，事業戦略策定などに関するコンサルティングを業務としている中堅のコンサルティング会社である。オフィスのフリーアドレス化及び出先での業務推進のため，E社に所属する200名のコンサルタント（以下，従業員という）にはノートPC（以下，NPCという）が配布されている。従業員は，社内や顧客オフィスでNPCを用いて業務を行う。また，従業員には通信カードも配布されており，社外からも，E社の情報システムにアクセスしている。

ここ最近，E社では，通勤途中の従業員が，顧客の重要情報を保存したNPCやUSBメモリを紛失するという事故が連続して発生した。それによって，顧客からは，E社のセキュリティ管理状況に対して強い不信の念をもたれることとなった。

そこで，E社の幹部は，情報セキュリティの専門家であるH氏の支援の下，再発防止プロジェクトチーム（以下，対策チームという）を立ち上げ，情報漏えい事故に対して抜本的な対策を実施することにした。

〔管理状況の把握〕

対策チームではまず，NPCやUSBメモリを紛失した従業員及びE社の各部門から選んだ数名の従業員に対してヒアリングを行い，NPC及びUSBメモリにおける顧客の重要情報の管理状況について把握することにした。その結果，次のような管理状況が明らかになった。

(1) E社の規程では，重要情報をNPC又はUSBメモリに保存する場合，暗号化しなければならないことになっている。しかし，E社指定の暗号ソフトでは，保存の都度，ファイル単位で暗号化の操作を行う必要がある。その手間を嫌い，平文のままファイルを保存してしまう場合が多い。

(2) E社指定の暗号ソフトでは，暗号化の際，復号のためのパスワードを入力する必要があるが，パスワードを忘れることを懸念して，自分の名前や顧客名，ファイル名など，単純なものをパスワードにしている場合が多い。

これらの管理状況に対するH氏のコメントは，次のとおりである。

(a) 暗号化を利用するのであれば，重要情報を確実に暗号化できるような仕組みを考

える必要がある。

(b) 幾ら強力な暗号ソフトを利用しても，現在の管理状況では，簡単に復号されてしまう可能性がある。

(c) (a) への対応のためには，ハードディスク全体を暗号化し，データの暗号化と復号を利用者に意識させることなく行う方法が有効である。ただし，この方法では，スリープ状態で NPC を持ち運んでいると，紛失や盗難時の情報漏えい対策として暗号化が意味を成さなくなることがあるので注意が必要である。

(d) 暗号化の代わりとして，シンクライアントシステムと呼ばれる仕組みを導入することで，NPC 上にデータを保存せずに済ませるという対策も考えられる。

(e) USB メモリへの重要情報の保存についても，データを確実に暗号化するための対策が必要である。USB メモリの利用を禁止するという対策も考えられる。

〔対策の検討〕

対策チームでは，H 氏のコメントの (c) 及び (d) で挙げられた，ハードディスク全体の暗号化による対策とシンクライアントシステムによる対策の二つについて検討を進めた。シンクライアントシステムには，幾つかの方式が存在しているが，従業員に配布済の NPC を有効に活用するため，NPC にシンクライアント用ソフトウェアを導入する方式を前提に検討することにした。表 1 は，二つの対策について，幾つかの観点から比較した内容を整理したものである。

表1　ハードディスク全体の暗号化とシンクライアントシステムの比較

比較項目	ハードディスク全体の暗号化	シンクライアントシステム
PC の紛失や盗難時の情報漏えい対策	(ア) 暗号鍵が漏えいしない限り，情報漏えいを防止できる。	(イ) 重要情報が NPC 上に保存されないため，情報漏えいを防止できる。
USB メモリ紛失や盗難時の情報漏えい対策	(ウ) USB メモリ上のデータについても利用者に意識させることなく暗号化することによって，USB メモリからの情報漏えいを防止できる。	(エ) USB メモリを使用禁止にすることによって，結果的に USB メモリからの情報漏えいを防止できる。
パフォーマンス	(オ) ファイルの読み書きの都度，暗号化又は復号の処理に伴うオーバヘッドが生じるが，最近の PC の性能から考えて，業務効率に与える影響は少ない。	(カ) サーバと接続しているネットワークや通信回線の速度に大きく依存するが，モバイルでの利用であっても，最近の高速モバイル通信であれば，E 社の業務には支障がない。
懸念事項	(キ) NPC をスリープ状態で持ち運んでいて，紛失したり盗難に遭ったりした場合，暗号化が意味を成さなくなることがある。 (ク) 製品の仕様上の問題や利用者の不適切な運用によって，暗号鍵が適切に管理されない場合，漏えいした暗号鍵によってデータを復号されてしまう可能性がある。 (ケ) 暗号鍵が紛失又は破損した場合，若しくは暗号鍵を保護するパスワードを忘れた場合は，NPC 上のデータにアクセスできなくなる。	(コ) データへアクセスするためにネットワーク接続が必須となる。

対策チームは，表1中の比較項目の検討と並行して，従業員の NPC 及び USB メモリの利用形態について調査した。その結果，図1のことが判明した。

(i) 顧客先などインターネットによる通信ができない場所で，NPC に保存された資料のデータにアクセスしなければならないことが多い。
(ii) 顧客先で資料のデータを顧客に渡す必要が出る場合が多く，USB メモリの利用頻度が高い。

図1　従業員の NPC 及び USB メモリの利用形態についての調査結果

シンクライアントシステムによる対策は，［a］や［b］といった点から，ハードディスク全体の暗号化による対策に比べて情報漏えいのリスクをより小さくできる点が評価されたものの，［b］や［c］といった点が現状の E 社の業務形態に合わない点が問題とされた。一方，ハードディスク全体の暗号化による対策には，表1中の(キ)，(ク)，(ケ)といった懸念事項があるものの，いずれも技術的に対応可能であると考えられた。

以上から，対策チームは，シンクライアントシステムの導入を今回は見送ることにし，情報漏えい対策としては，NPC のハードディスク全体の暗号化による対策を実施することにした。

〔製品の選定〕

対策チームは，ハードディスク全体を暗号化できる製品の選定を進めた。H 氏から実績が豊富な製品として挙げられた P 社，Q 社及び R 社の製品が候補となった。いずれも，NPC の起動時にパスワードを入力することによって，暗号化されたハードディスクにアクセスできるようになるという製品である。表 2 は各社の製品の比較表である。

表2　製品の比較

比較項目	P社製品	Q社製品	R社製品
暗号化の対象となるデバイス	ハードディスク及び USB メモリ	ハードディスク及び USB メモリ	ハードディスク（USB 接続のものを除く）
データ鍵(1)の保管方法	ハードディスク上に暗号化して保管する。	ハードディスク上に暗号化して保管する。	ハードディスク上に暗号化して保管する。データ鍵を使用するためには，保管時に指定したパスワードの入力が必要である。
マスタ鍵(2)の保管方法	鍵メモリ(3)に暗号化して保管する。マスタ鍵を使用するためには，保管時に指定したパスワードの入力が必要である。	PC 内にある TPM（Trusted Platform Module）(4) に保管する。マスタ鍵を使用するには，マスタ鍵の保管時に指定したパスワードの入力が必要である。	マスタ鍵に相当する鍵はない。
PC 利用開始時の操作	鍵メモリを PC に接続した上で，パスワードを入力する。 PC を利用している間は，常に鍵メモリを接続している必要がある。	パスワードを入力する。	パスワードを入力する。
USB メモリによるデータ交換のサポート	USB メモリ上のファイルを暗号化する PC 及び復号する PC の双方に P 社製品のインストールが必要である。	自己復号ファイル(5)として書き出すこともできるので，復号する PC への Q 社製品の導入は不要である。	USB メモリへの書出し時は暗号化されない。
スリープ状態からの復帰	パスワードの入力が必要である。	パスワードの入力が必要である。	パスワードの入力は不要である。
パスワードを忘れたときの対応	管理ツールによって，リカバリ用のパスワードを発行できる。	特にない。	特にない。

注(1) ハードディスク上のデータの暗号化に用いる鍵
注(2) データ鍵の暗号化に用いる鍵
注(3) マスタ鍵を保管する USB メモリ
注(4) 暗号化やハッシュの演算，プラットフォームの完全性検証の機能をもったセキュリティチップで，TPM 内に保管された暗号鍵は，チップ外へ読み出すことができない。物理的な方法によって無理に読み出そうとしても，チップの動作停止や回路の物理的破壊などによって，攻撃を防ぐようになっている。
注(5) 復号のためのプログラムと暗号化データを一体化した実行可能形式のファイルで，ファイルを実行することでデータを復号することができる。

Q 社製品の利用には TPM を内蔵した PC が必要であるが，E 社が従業員に配布している NPC は TPM 内蔵のモデルであり，この点は問題にならなかった。また，NPC に内蔵された TPM は，TPM に保管されたパスワードを間違えた場合，一定時間，マスタ鍵へのアクセスがロックされるという機能をもっている。

対策チームは，表1に挙げられた(キ)，(ク)，(ケ)といった懸念事項を中心に各社の製品を評価し，結果を表3にまとめた。

表3　製品の評価結果（一部）

評価の観点	優れている製品	理由
懸念事項(キ)への対応	P社製品，Q社製品	スリープ状態のNPCが盗まれてもパスワードが分からなければデータにアクセスできない。
懸念事項(ク)への対応	d 社製品	〔懸念事項(ク)に関する製品比較〕に記述
懸念事項(ケ)への対応	P社製品	従業員がパスワードを忘れても，データへのアクセスが可能となる。
USBメモリによるデータ交換への対応	e 社製品	f

〔懸念事項(ク)に関する製品比較〕

〔管理状況の把握〕の(2)から考えて，マスタ鍵を保護するパスワードとして，総当たり攻撃によって解析可能な程度の強度しかもたないものが設定される可能性がある。その点を踏まえて，対策チームでは，懸念事項(ク)への対応については，図2のような検討を行った。

(i)　P社製品を利用するとした場合，NPCと鍵メモリを同時に持ち歩く必要がなく，両方が同時に紛失したり盗難に遭ったりする可能性が低いならば，P社製品が優れている。
(ii)　P社製品を利用するとした場合，NPCと鍵メモリを同時に持ち歩く必要があり，両方が同時に紛失したり盗難に遭ったりする可能性が高いならば，Q社製品が優れている。

図2　懸念事項(ク)に関する製品比較

〔製品の選定と懸念事項(ケ)への対応〕

対策チームは，表3に基づいてQ社製品を選定し，NPCのハードディスク全体の暗号化を推進した。ただし，Q社製品では，懸念事項(ケ)への対応が不十分なことから，対策チームは，NPC上のデータをバックアップしておき，NPC上のデータにアクセスできなくなっても，バックアップ先から復旧できるようにしておくことで懸念事項(ケ)に対応することにした。

設問1　本文中の［　a　］～［　c　］に入れる適切な字句を，表 1 中の (ア)～(コ) から選び，記号で答えよ。

設問2　〔管理状況の把握〕において H 氏がコメント (b) の指摘をした理由を，40 字以内で述べよ。

設問3　〔管理状況の把握〕における H 氏のコメント (c) にあったスリープ状態での NPC の持ち運びについて，(1)，(2)に答えよ。

(1) 紛失や盗難時の情報漏えい対策として暗号化が意味を成さなくなることがあるのは，どのような場合か。35 字以内で述べよ。

(2) (1)の場合に暗号化が意味を成さなくなる理由を 40 字以内で述べよ。

設問4　E 社従業員の USB メモリの利用形態から考えて，表 3 中の［　e　］に入れるべき，USB メモリによるデータ交換への対応が優れていると考えられる製品を P～R から選び，記号で答えよ。また，表 3 中の［　f　］に入れるべき理由を，40 字以内で述べよ。

設問5　〔懸念事項 (ク) に関する製品比較〕について，(1)～(3) に答えよ。

(1) 図 2 中の (i) で P 社製品が優れているとした理由を，30 字以内で述べよ。

(2) 図 2 中の (ii) で Q 社製品が優れているとした理由を，マスタ鍵を保護するパスワードの強度に関する懸念を踏まえて 50 字以内で述べよ。

(3) E 社従業員の NPC の利用形態も踏まえて，表 3 中の［　d　］に入れるべき，懸念事項 (ク) への対応が優れていると考えられる製品を P～R から選び，記号で答えよ。

7. 途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

8. 問題に関する質問にはお答えできません。文意どおり解釈してください。
9. 問題冊子の余白などは，適宜利用して構いません。
10. 試験時間中，机上に置けるもの及び使用できるものは，次のものに限ります。
なお，会場での貸出しは行っていません。
受験票，黒鉛筆又はシャープペンシル，鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ティッシュ
これら以外は机上に置けません。使用もできません。
11. 試験終了後，この問題冊子は持ち帰ることができます。
12. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
13. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
14. 午後Ⅱの試験開始は 14:30 ですので，14:10 までに着席してください。