問1　Javaプログラミングに関する次の記述を読んで，設問1～3に答えよ。

S社は，従業者数500名（従業員30名，パートタイマ（以下，パートという）470名），営業所が1か所の警備業者であり，各種イベントの警備や交通誘導警備を請け負っている。これまで，パートの勤務時間の集計と給与計算は，手書き帳票を基にして経理課にて行っていた。今回，情報システム課でWebアプリケーションによる勤務時間管理システムを開発して，集計などの作業をシステム化することとした。このシステム化によって，毎月初めの5営業日以内にパートが営業所に赴き，PC操作によって自分の前月分の勤務時間集計表を印刷した後，その表に記載された勤務時間と給与支給金額に誤りがないことを確認して押印し提出するという作業の流れとなった。

なお，パートの勤務時間は，業務監督者が記録し，専任の担当者がデータベースに入力する。

〔システム構成〕

S社の勤務時間管理システムのシステム構成は，図1のとおりである。

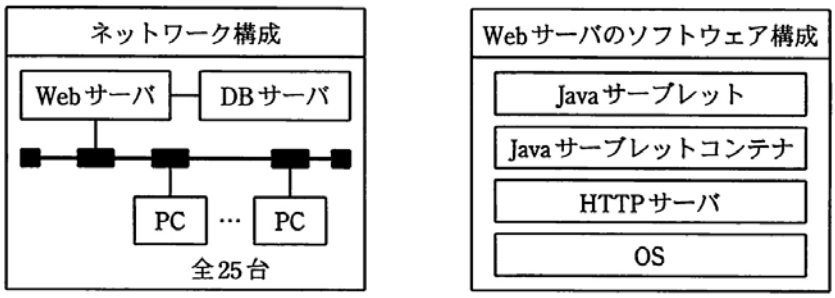


図1　勤務時間管理システムのシステム構成

HTTPサーバ及びJavaサーブレットコンテナはオープンソースソフトウェアを使用しており，Javaサーブレットコンテナは Java Platform, Enterprise Edition 5 （Java EE 5）に準拠したものである。また，利用者用PCは，25台を用意してパート全員で共用する。

システムの利用者IDには，6けたの数字からなる従業者番号を使用する。

〔システム仕様〕

S社の情報システム課には従業員が4名在籍しているが，これまでT君がほぼ1人でシステム開発，管理を行っており，今回の開発もT君が1人で担当することとなった。T君は，これまでJavaサーブレットモデルを用いたシステム開発を経験したことがなかった。しかし，プログラム上でメモリを使用する際の境界チェックをしなくてもJavaバーチャルマシンによってメモリの使用状況が管理されるために，C言語又はC++言語で開発したプログラムにおいてよく発生する［ a ］によるセキュリティ上の脆弱性が発生しないという利点を重視して，Javaサーブレットモデルを用いた開発を決定した。

今回開発する勤務時間管理システムの仕様は，図2のとおりである。

1. 勤務時間管理システムは，利用者 ID 及びパスワードを使用して本人確認を行う。
2. 利用者用 PC 上のブラウザ操作によって，Web サーバ内の Java サーブレットは勤務時間集計表を PDF ファイルとして動的に作成し，HTTP サーバの Web 公開領域に保存する。
   なお，勤務時間集計表の作成においては既存の勤務時間集計表作成プログラムを呼び出す。
3. Web サーバ内の Java サーブレットは，勤務時間集計表へアクセスするためのリンク情報を含んだ HTML 文書をブラウザへ送信する。利用者は，ブラウザ上に表示されたリンクをクリックして，勤務時間集計表をダウンロードする。
4. 定期的に起動されるプロセスによって，作成から 1 時間以上経過した勤務時間集計表を自動的に削除する。

図 2　勤務時間管理システムの仕様（抜粋）

〔勤務時間集計表の作成及びリンク表示のプログラム〕

T 君は，図 2 の仕様に基づいて Java プログラムを作成した。その Java プログラムのうち，勤務時間集計表を作成して，その表へのリンクを表示する部分について図 3 に示す。プログラム完成後，仕様に基づいた機能試験を試験環境にて行い，問題がないことを確認した。

```
package jp.co.s_sha.kinmuhyo;

import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;

public class PDFDownloader extends HttpServlet {
   private static final long serialVersionUID = 1L;

   static final String KINMUHYO_LOCAL_PATH = "c:\\inetpub\\wwwroot\\KinmuHyo";
   static final String KINMUHYO_URL_PATH = "../KinmuHyo/";
   File tempPDF;

   public void init() {
      (省略)   // データベースへ接続
   }

   public void destroy() {
      (省略)   // データベースから切断
   }

   protected void doGet(HttpServletRequest request, HttpServletResponse response)
            throws ServletException, IOException {
      String tempUserID = request.getRemoteUser();   // tempUserID に利用者 ID を代入
      tempPDF = new File(KINMUHYO_LOCAL_PATH, tempUserID + ".pdf");
      makePDF(tempUserID, tempPDF);
      response.setContentType("text/html; charset=utf-8");
      PrintWriter out = response.getWriter();
      (省略)   // 定型的な HTML 出力
      out.println("<a href=\"" + KINMUHYO_URL_PATH + tempPDF.getName() +
                  "\">こちら</a>からダウンロードしてください。");
      (省略)   // 定型的な HTML 出力
   }

   protected void doPost(HttpServletRequest request, HttpServletResponse response)
            throws ServletException, IOException {
      (省略)   // doGet メソッドの呼出し
   }

   protected void makePDF(String userID, File output)
            throws IOException {
      (省略)   /* 勤務時間集計表作成プログラムを呼び出し，利用者 ID（userID）で示され
                  るパートの勤務時間集計表を output で示されるファイルとして作成 */
   }
}
```

図 3　勤務時間管理システムのプログラム（抜粋）

〔トラブルの発生と対策〕

その後，S 社では勤務時間管理システムの運用を開始した。しかし，パートから，①マニュアルどおりに操作したにもかかわらず，ダウンロードした勤務時間集計表が他人のものだったという苦情があった。この問題が発生したときには 25 名の利用者が同時に勤務時間管理システムへアクセスしていた。T 君は，この問題の原因を調査するためにプログラムを見直していたが，なかなか原因を特定できなかった。さらに，最初にこの問題が発生してから 3 日後に，23 名の利用者が同時に勤務時間管理システムへアクセスしていた際にも，同じ問題が発生した。

この状況を見て，情報システム課の H 課長は勤務時間管理システムの運用停止を指示するとともに，T 君単独でのシステム開発には無理があると考え，セキュリティにも詳しいシステムコンサルタントの U 氏に支援を要請した。

支援を開始した U 氏は，最初に図 3 のプログラムを検査して，問題の原因と修正方法を指摘した。その指摘に従い，T 君はプログラムを修正し，テストを行って問題が発生しないことを確認した。

さらに U 氏は，悪意をもったパートが②他人のパスワードを使用しなくても，容易に他人の勤務時間集計表をダウンロードできる脆弱性があることを指摘した。

指摘を受けた T 君は，作成する勤務時間集計表のファイル名をランダム文字列とすれば脆弱性は解消できるのではないかと提案した。しかし U 氏は，そもそも個人情報が記録されたファイルを Web 公開領域に保存することに問題があると指摘して，脆弱性を解消するために図 2 の仕様を図 4 のように修正することを提案した。

1. 勤務時間管理システムは，利用者 ID 及びパスワードを使用して本人確認を行う。
2. 利用者用 PC 上のブラウザ操作によって，Web サーバ内の Java サーブレットは勤務時間集計表を PDF ファイルとして動的に作成し，Web 公開領域ではなく Java サーブレット経由でだけアクセス可能な領域に保存する。
   なお，勤務時間集計表の作成においては既存の勤務時間集計表作成プログラムを呼び出す。
3. Web サーバ内の Java サーブレットは，［ b ］をブラウザへ送信する。利用者は，ブラウザの PDF プラグイン機能によって表示された内容を印刷する。
4. 定期的に起動されるプロセスによって，作成から 1 時間以上経過した勤務時間集計表を自動的に削除する。

図 4　勤務時間管理システムの修正仕様（抜粋）

その後，T 君は U 氏の支援を受けつつ，図 4 の仕様に沿って勤務時間管理システムの修正を行い，脆弱性が解消されたことを確認した。この結果を受けて，H 課長は勤務時間管理システムの運用再開を指示した。

設問 1　本文中の［ a ］に入れる適切な字句を 15 字以内で答えよ。

設問 2　本文中の下線①の苦情について，(1)～(4)に答えよ。

(1)マニュアルどおりに操作したにもかかわらず，他人の勤務時間集計表をダウンロードしてしまった原因について，図 3 のプログラム上の変数名を用いて，60 字以内で述べよ。

(2)この苦情の原因となるプログラムのバグで発生する問題は何と呼ばれるか。15 字以内で答えよ。

(3)上記(2)のバグを修正するためのプログラムの変更内容を，45 字以内で具体的に述べよ。ただし，図 2 に示した仕様は変更しないものとする。

(4)このプログラムに関して，上記(2)のバグの有無を確認するためにテストを

実施したい。どのようなHTTPリクエストをどのようにWebサーバに送信すればよいか。 50字以内で述べよ。

設問3　本文中の下線②の脆弱性について，(1)，(2)に答えよ。

(1)この脆弱性を突いて，他人の勤務時間集計表をダウンロードする方法を50字以内で述べよ。

(2)この脆弱性を解消する修正仕様に関して，図4中の［　b　］に入れる適切な字句を20字以内で答えよ。

問2　データの暗号化とバックアップに関する次の記述を読んで，設問1～3に答えよ。

G社は，従業員数800名の医薬品販売会社であり，全国15か所に営業所をもっている。3か月前，ある営業所で火災が発生し，その営業所内のPCとサーバが被害を受けた。顧客データや注文データなどの電子データが消失してしまい，顧客データを再入力したり，顧客に注文データを確認したりするなどの復旧作業に1か月を要するなど，事業に大きな影響が出た。G社の経営陣は，今後同様のデータ消失が起きないように，営業所を対象としたデータバックアップを見直すよう，情報システム部に指示した。また，営業所ではPCに顧客データなどの機密データを保管している一方，従業員が社外にPCを持ち出して仕事をしているので，これらの機密データの社外への漏えいを防ぐ対策についても見直すよう，経営陣は指示した。

情報システム部のL課長は，これら二つの指示を受けて，部員のY君にバックアップ方式と機密保護方式を検討するように指示した。

Y君は，対象とするデータを整理するために，営業所に対して，保有しているデータの洗出しを依頼した。その結果，PCに保存されているデータのうち，バックアップ又は機密保護が必要なものは表のとおりであった。

表　PCに保存されていて，バックアップ又は機密保護が必要なデータ

データ	バックアップ	機密保護	データの取扱い	データの保存形式
顧客データ	必要	必要	表計算ソフトで顧客（医療機関の関係者）の連絡先などを管理している。パスワードなどによる保護はしていない。電子メール（以下，メールという）による表計算ファイルの送受信は行っていない。	(a) 表計算ファイル
注文データ	必要	必要	顧客から送付されてくるメールの本文中に医薬品の注文が記載されており，これで注文を受け付けている。	(b) メールボックスファイル内のメール（MIME形式）
仕入原価データ	不要	必要	本社からメールの添付ファイル（PDFファイル）として医薬品の仕入原価などが定期的に送付されてくる。添付されているPDFファイルはパスワードなどによる保護はされていない。	(b) メールボックスファイル内のメール（MIME形式）
			本社からメールの添付ファイルとして送付されてくるPDFファイルをメールから取り出してPCに保存し，参照している。	(c) PDFファイル

注　G社が使用しているメールソフトは，すべてのメールをPC上の一つのメールボックスファイルに格納する。

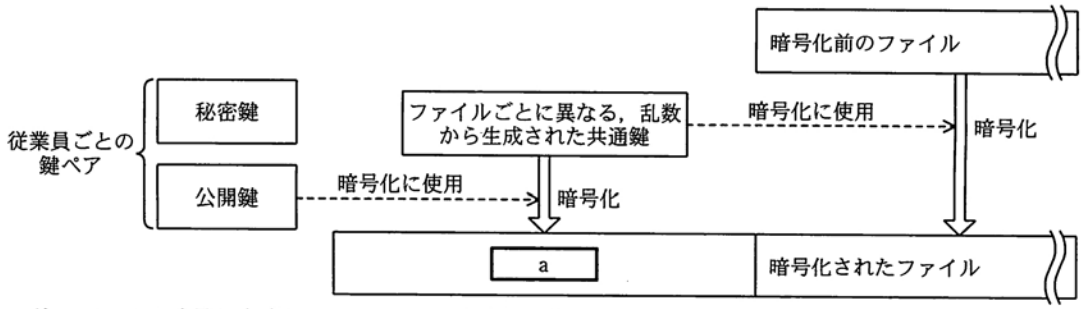
各営業所には，営業所内での情報共有のために医薬品のカタログデータなどを保管しているファイルサーバ（以下，営業所サーバという）が，サーバルーム内に設置されている。機密保護の観点から営業所サーバの管理状況を確認したところ，データの管理に問題はなかった。また，営業所サーバについては容量が比較的小さいので全データをバックアップの対象にすることにした。

〔暗号化方式の検討〕

まずY君は，表中の（a）と（c）の形式のデータについて暗号化を検討した。

Y君は，暗号化の方法として，PCのハードディスクをすべて暗号化するソフトウェアを利用する方式（以下，ハードディスク暗号化方式という）と，従業員ごとに公開鍵暗号方式の鍵ペアをもち，ファイル単位で暗号化を行うソフトウェアを利用する方式（以下，ファイル暗号化方式という）の比較を行った。その結果，ファイル暗号化方式に比べ，ハードディスク暗号化方式はG社で利用しているPCでは動作速度が著しく低下することが分かり，ファイル暗号化方式を採用することにした。

ファイル暗号化方式における暗号化は，図1のように行われる。従業員は，暗号化を開始するに当たって，まず秘密鍵と公開鍵の鍵ペアを生成する。ファイルの暗号化は，ファイルごとに異なる，乱数から生成された共通鍵を使用して行われる。暗号化に使われた共通鍵は従業員の公開鍵を使用して暗号化され，暗号化されたファイルとともにハードディスクに保存される。



注　ファイル暗号化方式によってファイルを暗号化すると，暗号化に関する情報がファイルに付加される。

図1　ファイル暗号化方式におけるファイルの暗号化

また，ファイル暗号化方式におけるファイルの復号は図2のように行われる。

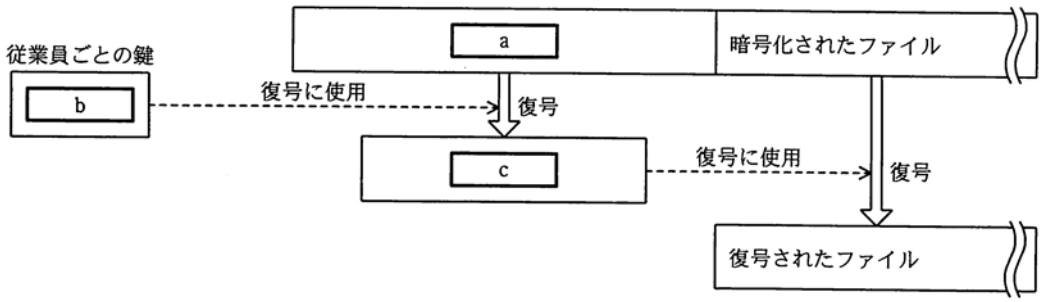


図2　ファイル暗号化方式におけるファイルの復号

従業員がOSにログインしている状態であれば，暗号化されたファイルは通常のファイルと同様に，暗号化・復号を意識することなく利用することができる。しかし，

従業員が OS にログインしていない状態では，従業員の [b] にアクセスすることができないので，ファイルが暗号化されたままの状態となり，PC からハードディスクが外された場合でも，ハードディスクからのデータ漏えいを防止することができる。

次に Y 君は，表中の(b)の形式のデータについて，暗号化を検討した。調査の結果，G 社及び顧客のメールソフトはすべて S/MIME に対応しており，暗号メールの利用に問題がなかったので，注文データ又は仕入原価データを含むメールはすべて S/MIME で暗号化してやり取りすることにした。さらに，G 社のすべての PC には，[d] に基づいて評価及び認証された TPM(Trusted Platfolrm Module)バージョン 1.2 対応製品が搭載されていることが分かった。そこで，この TPM を用いて，ファイル暗号化方式の鍵ペア及び S/MIME 用の鍵ペアを安全に保管することにした。

〔バックアップ方式の検討〕

続いて Y 君は，バックアップ方式の検討を行った。営業所から，PC だけが被害を受けてデータが消失した場合は前営業日のデータに回復し，営業所全体が被害を受けた場合は最悪でも 2 週間前のデータに回復したいとの要望が出たので，これらの要望に基づいて検討することにした。Y 君は，バックアップ方式として，図 3 のように，PC のデータを営業所サーバにバックアップし，次に営業所サーバのデータを磁気テープ(以下，テープという)にバックアップする方式を考えた。

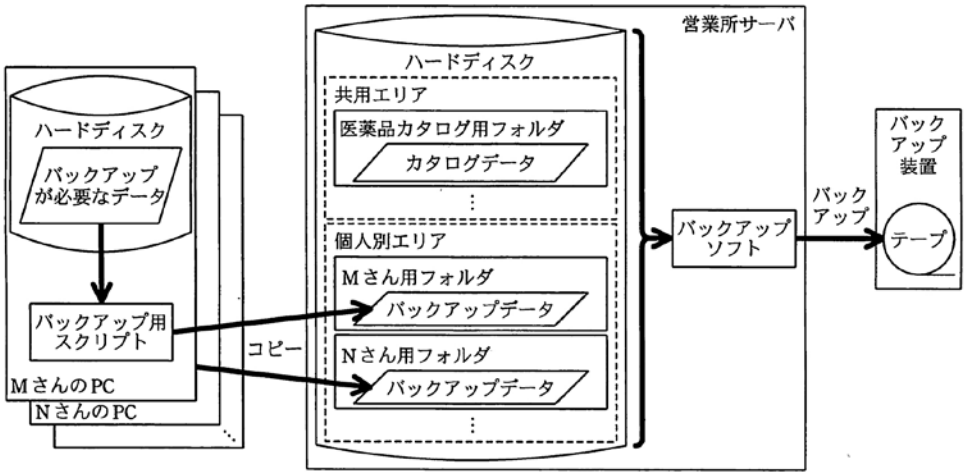


図 3　バックアップ方式

〔バックアップ方式の検証と改善〕

Y 君は，検討したバックアップ方式で運用できることを検証するために，まず，バックアップ用スクリプトで PC のデータを営業所サーバにコピーし，次に PC のデータ領域のファイルを消去した上で，営業所サーバからバックアップしたデータを PC に戻し，データを確認した。その結果，すべてのデータが問題なく使用できたので，一つの営業所でパイロット運用を開始した。

パイロット運用を開始して 2 週間後，ある従業員の PC が故障し，マザーボードの交換修理を行った。すると，暗号化されたデータが全く読めなくなってしまった。そこで，営業所サーバからバックアップしたデータを PC に戻したが，②それでもサーバから戻したデータの一部は PC で読めなかった。

Y 君は，この原因を調査したところ，TPM の利用方法を改善する必要があることが分かった。そこで，③ファイル暗号化方式の手順を一部修正した。修正された方式に

基づいて実施したパイロット運用の結果は順調で，順次，すべての営業所で本格運用を開始していくこととなり，G 社営業所データの，暗号化とバックアップが実施されるようになった。

設問 1　〔暗号化方式の検討〕について，(1)～(3)に答えよ。

(1)図 1，2 及び本文中の [a] ～ [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　暗号化された共通鍵　　イ　公開鍵　　ウ　電子署名
エ　ハッシュ値　　オ　秘密鍵　　カ　ファイルを復号する共通鍵

(2)ファイル暗号化方式において，G 社が利用している PC の TPM で必ず実行できる機能はどれか。解答群の中から二つ選び，記号で答えよ。

解答群

ア　暗号化された共通鍵を，ハードディスクに格納する機能
イ　共通鍵でファイルを暗号化する機能
ウ　従業員の鍵ペアを生成する機能
エ　乱数を生成する機能

(3)本文中の [d] に入れる適切な情報セキュリティに関係した評価基準を解答群の中から選び，記号で答えよ。

解答群

ア　CC(ISO/IEC 15408)　　イ　JIS Q 15001
ウ　JIS Q 27001 (ISO/IEC 27001)　　エ　PCI DSS

設問 2　〔バックアップ方式の検討〕について，(1)，(2)に答えよ。

(1)本文中の下線①において，どのような情報漏えいのリスクが高くなる可能性があると L 課長は指摘したか。 40 字以内で述べよ。

(2)上記(1)で述べた情報漏えいのリスクが高くなる可能性について，それに対する対策を 30 字以内で述べよ。

設問 3　〔バックアップ方式の検証と改善〕について，(1)～(3)に答えよ。

(1)本文中の下線②において，読めなかったデータは表中のどれか。そのデータの保存形式を，表中の(a)～(c)からすべて選び，記号で答えよ。

(2)本文中の下線②において，一部のデータが読めなかった理由を 60 字以内で述べよ。

(3)本文中の下線③において，どのように暗号化方式の手順を修正したか。60 字以内で述べよ。

問 3　転職サイトにおける個人情報保護に関する次の記述を読んで，設問 1，2 に答えよ。

P 社は，従業員数 30 名の人材紹介会社である。コンサルタントによる人材紹介だけでなく，転職サイトも立ち上げている。この転職サイトには，求職者，求人企業が多数，登録している。求職者は，転職サイトの個人プロフィール登録画面で，氏名，生年月日，住所，電話番号，職歴などの個人プロフィールを登録する。求職者の転職サイトの利用は無料である。求人企業は，業種，募集職種，職務内容，給与，勤務地，応募資格などの求人募集内容の掲載を P 社に依頼する。求人企業は，求人募集時には

求人件数に応じた利用料を，採用成立時には紹介料を P 社に支払う。

〔求職者の個人情報の保護〕

求職者は，求人募集内容を見て応募したい求人企業があれば，転職サイト内のそれぞれの求人企業の応募入力画面を利用して応募することができる。応募入力画面では，あらかじめ個人プロフィール登録画面で登録しておいた個人プロフィールをそのまま利用することもできるが，新たに入力することもできる。さらに，各求人企業に対する応募理由などを追加入力することもできる。この応募時の個人プロフィールは，P 社の Web サーバから，求人企業に，電子メール（以下，メールという）で自動送信される。

なお，求職者の個人情報を求人企業に提供することについては，求職者から事前に転職サイトの画面で同意を得ており，また，求人企業に対しても提供する個人情報の利用目的を利用規約で制限しており，特に問題ないと P 社は認識している。

求人企業のうち，数社から，暗号化されていないメールで求職者の個人情報を送信することについて，漏えいする危険性があるので改善してほしいとの要望があった。これを受けて，P 社の情報システム部の F 部長は，システム担当の Z 主任に，メールが盗聴される危険性を踏まえた改善案を作成するよう命じた。

Z 主任は，F 部長の指示に従って，改善案を表 1 にまとめた。

表 1　個人情報を含むメールが盗聴される危険性を踏まえた改善案

	案 1	案 2	案 3
方式	メールの暗号化	パスワード付きファイルの添付	求人企業向け Web ページの追加
実現手段	個人プロフィールを送信するメールを S/MIME 又は PGP を用いて暗号化する。	個人プロフィールを含む文書ファイルなどをパスワードで保護した状態でメールに添付して送信する。	応募があったときに，個人プロフィールを含めず，応募があったことだけを通知するメールを送信する。求人企業は，パスワード認証と TLS（SSL）で保護されている求人企業向け Web ページから個人プロフィールをダウンロードする。
利点	秘匿性が高い。	ほとんどの求人企業で利用可能である。	メールに個人情報を含まない。
欠点	S/MIME，PGP は，求人企業に普及していない。	秘匿性が低い。パスワードの管理が必要となる。	求人企業の利用者が個人プロフィールにアクセスする際の手順が増える。パスワードの管理が必要となる。

次は，各案を比較した際の F 部長と Z 主任の会話である。

Z 主任：案 1 の S/MIME はどうでしょうか。

F 部長：S/MIMEI は，各求人企業が［　a　］を用意するために認証サービスを年間契約することなどが必要である。コストが掛かるから難しいだろう。

Z 主任：各求人企業が自社で［　a　］を発行する方法は，採用できないのでしょうか。

F 部長：①各求人企業が自社で発行したものは，当社では［　a　］として受け入れてれられない。

Z 主任：当社で認証局システムを構築して，求人企業の各利用者分も含めて
[a] を発行するのはどうでしょうか。
F 部長：その場合，導入コストに加えて運用コストも必要だ。
Z 主任：それでは，PGP はどうでしょうか。
F 部長：PGP は，自社で鍵の生成システムを用意できるとしても，クライアント PC の [b] ソフトが対応していないことが多く，操作手順が複雑になるので，一般の利用者には使いにくいだろう。案 1 の採用は難しいようだね。
Z 主任：案 2 はどうですか。
F 部長：もし攻撃者が添付ファイルを入手したら，総当たり攻撃をかけることができるので，パスワードは十分に長くしないといけないね。
Z 主任：最短パスワード長は，8 文字でどうでしょうか。
F 部長：それでは足りないだろう。サーバへのログインのように，②オンラインでパスワードを入力させる場合は，試行回数を多くできないように制限することもできるから 8 文字程度でも十分な場合が多い。しかし，案 2 の場合は，添付ファイルを攻撃者に入手されたら，ファイルに対してオフラインで直接的に攻撃されて試行回数が制限できない上に，解析ツールを利用して，ごく短時間でパスワードを解析される危険性もある。だから，パスワードはかなり長くする必要があるが，運用上はなかなか難しいだろう。
Z 主任：そうすると，案 3 でしょうか。
F 部長：そうだね。案 3 は，求人企業の利用者の手間が増えるという欠点はあるが，この欠点は操作性の高い求人企業向け Web ページを用意することによって補うことができるだろう。また，当社で求人企業の利用者の初期パスワードを管理する必要があるが，求人企業の利用者の総数から考えて，大きな手間にはならないだろう。

F 部長と Z 主任は，案 3 を採用することにした。求人企業向け Web ページの操作性については，求職者の個人プロフィールを簡単な手順で確認できるように設計することにした。

P 社では，求人企業向け Web ページを追加し，各求人企業に運用方法の変更を通知した上で，案 3 に沿った運用方法に切り替えた。

〔求人企業向け Web ページのパスワード〕

求人企業向け Web ページでは，表 2 に示すような利用者 ID とパスワードを求人企業の利用者ごとに発行し，各求人企業向けの Web ページだけにアクセスできるようになっている。求人企業の利用責任者は，最初に P 社に依頼するときに，各利用者のメールアドレスを含む申込書と，求人企業の登記事項証明書を郵送する。P 社では，利用者 ID は求人企業の各利用者にメールで送信するが，③初期パスワードの通知書は登記事項証明書に記載された所在地気付で利用責任者あてに一括して郵送している。求人企業の各利用者は，初めて求人企業向け Web ページにログインしたときには，パスワードを変更してから利用する。

なお，初期パスワードの通知書は，パスワードを変更した後も，各利用者が保管するように P 社からお願いしている。

表2　求人企業向けWebページの利用者IDとパスワード

項目	生成方法／設定方法	例
利用者ID	P社が，求人企業の利用者に対して，登録順に1人に一つずつ割り振る連続番号（数字8けた）。	00000099
初期パスワード	利用者IDを3倍した数字の下8けたと，発行日（西暦4けた，月2けた，日2けた）を合わせた16けたの数字。	0000029720100405
パスワード	初回ログイン時に，求人企業の利用者が設定する。8けた以上の文字列で，英字，数字，記号が使用可能。	A9d3&jw27

このような方法で運用していたところ，求人企業のQ社から3名の利用者を含む申込みがあり，各利用者の初期パスワードを利用責任者あてに郵送した。その3名の初期パスワードを見たQ社の利用責任者は，④他人の初期パスワードを推定可能であるという問題があると，P社に指摘した。F部長とZ主任は，その指摘に対して，直ちに改善を行った。

また，別の問題点として，パスワード変更後にパスワードを忘れたという問合せがしばしば発生するようになった。そこで，Z主任は，図のようなパスワード再設定手順を追加することを考え，F部長に提案した。

(1) 求人企業の利用者が，パスワード再設定の申請ページに利用者IDを入力する。
(2) Webアプリケーションが自動的に，パスワード再設定の申請があった旨と，パスワード再設定の実行ページのURLを，P社に登録されている利用者のメールアドレスあてにメールで通知する。第三者からのアクセスを避けるためにURLには十分に長いランダムな文字列を含める。
(3) 求人企業の利用者が，URLの示すパスワード再設定の実行ページにアクセスし，新パスワードを入力すると新パスワードが設定される。
(4) パスワード再設定の実行ページのURLを通知後，20分以内にアクセスがない場合は，実行ページのURLを自動的に無効にする。

図　求人企業向けWebページのパスワード再設定手順（当初案）

F部長は，⑤図のパスワード再設定手順では第三者にパスワードを再設定されてしまう危険性があることを指摘し，Z主任に対応を指示した。Z主任は，F部長の指示に従い，⑥パスワード再設定手順を見直し，再提案した。

その後，P社では，Z主任の再提案を採用して，見直し後のパスワード再設定手順での運用を開始した。

設問1　〔求職者の個人情報の保護〕について，(1)～(4)に答えよ。

(1)本文中の［ a ］，［ b ］に入れる適切な字句を［ a ］については10字以内で，［ b ］については5字以内で答えよ。

(2)F部長が，本文中の下線①のように述べている理由を30字以内で述べよ。

(3)PGPでは，通常，証明書のフィンガプリントを確認するが，正しいフィンガプリントの入手方法として安全と考えられるものを一つ挙げ，30字以内で述べよ。

(4)本文中の下線②を実現する対策の内容を50字以内で具体的に述べよ。

設問2　〔求人企業向けWebページのパスワード〕について，(1)～(4)に答えよ。

(1)本文中の下線③について，初期パスワードの通知書の郵送先を求人企業の登

記事項証明書に記載された所在地としたP社の意図は何か。40字以内で述べよ。

(2)本文中の下線④について，問題を解決するためには初期パスワードをどのように生成すればよいか。30字以内で述べよ。

(3)本文中の下線⑤について，総当たり攻撃以外には，どのような手口で第三者にパスワードを再設定されてしまうか。40字以内で述べよ。

(4)本文中の下線⑥について，Z主任の考えた見直し案はどのようなものであったと考えられるか。 40字以内で述べよ。

問4　ウイルスの駆除及び感染防止に関する次の記述を読んで，設問1～4に答えよ。

K社は，従業員数1,000名の事務機器販売会社である。K社には，人事総務部，営業部，商品管理部，情報システム部がある。K社のネットワークは図1に示すとおり，DMZと社内ネットワークで構成されている。社内ネットワークは，内部サーバネットワークと部ごとの部門ネットワークに分割されている。社内ネットワーク上のPCから，インターネット上のWebサーバへのアクセスは，DMZのプロキシサーバを経由して行うように，各PCのブラウザが設定されている。

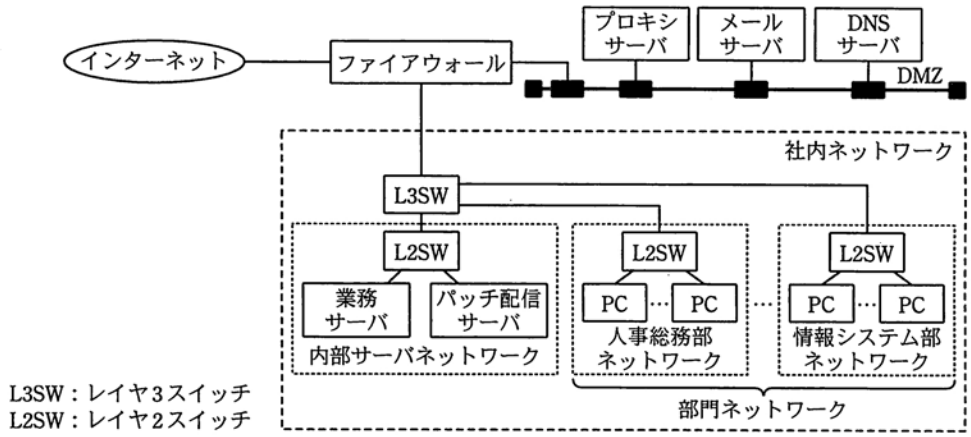


図1　K社のネットワーク（抜粋）

〔新種ウイルスの感染と駆除〕

ある日，情報システム部のA主任は，営業部のC課長から，PCの動作がおかしいので調べてほしいとの依頼を受けた。A主任は，早速，C課長の席を訪れ，PCの状態を確認したところ，全般的に動作が非常に遅く，業務に支障を来す状態となっていた。ハードウェアやソフトウェアの障害についてログを確認したが，障害発生を示す記録は見当たらなかった。そこで，A主任は，ウイルス感染を疑い，その検査を行うことにした。K社では，図2に示すウイルス駆除手順が決められており，A主任はその手順に従って作業を進めた。

(1) 感染が疑われるPCを社内ネットワークから切断する。
(2) 情報システム部では，最新のウイルス定義ファイルを入れたCD-ROMを作成し，そのCD-ROMを用いて，PCのウイルス対策ソフトのウイルス定義ファイルを最新に更新する。
(3) すべてのハードディスクドライブに対してウイルス検査を行い，検知されたウイルスの駆除を行う。
(4) すべてのウイルスの駆除を行った後，社内ネットワークに接続する。
(5) OSとアプリケーションのセキュリティパッチの適用状態を確認して，もし未適用のものがある場合は，最新のセキュリティパッチまですべてを適用する。

図2　K社のウイルス駆除手順

しかし，手順(3)まで行ったが，ウイルスは検知されなかった。セキュリティパッチの適用状態を確認したところ，前月にリリースされたOSのセキュリティパッチが適用されていないことが判明した。そこで，A主任は，PCを社内ネットワークに接続した上で，OSに対して最新のセキュリティパッチまでをすべて適用した。この時点で，PCの状態を確認したが，最初に確認したときと同様な状態であった。

A主任は，情報システム部のB課長に状況を説明して，指示を仰いだところ，現在導入されているI社製ウイルス対策ソフトとは異なるベンダのウイルス対策ソフトで，ウイルス検査を試みるよう指示があった。そこで，PCを社内ネットワークから再び切断して，I社製ウイルス対策ソフトをいったん削除した後，J社製ウイルス対策ソフトを導入し，再度，検査を行ったところ，Xウイルスを検知したという警告が表示された。A主任は，Xウイルスの駆除を行い，駆除が成功したと表示されたことを確認した。その後，J社のWebサイトで，Xウイルスについて情報収集を行った。その結果，Xウイルスは新種のウイルスであることと，図3に示す感染方法と特徴が報告されていることが分かった。

Xウイルスは，次の二つの感染方法をそれぞれ，同一サブネット内の，自らのIPアドレスを除くすべてのIPアドレスに対して，IPアドレスの昇順に試みる。

感染方法1　OSの脆弱性(1)を攻撃することによる感染
OSの脆弱性を攻撃して，感染しようとする。この動作を10分間隔で行う。

感染方法2　OSの管理者IDに対するパスワード辞書攻撃による感染
OSの管理者IDとしてよく使用される識別名のアカウントに対して，よく使われる約1,000個のパスワードを使用した攻撃を試みて，管理者権限を取得した上で，Xウイルス自身をコピーし実行することで感染しようとする。この動作を30分間隔で行う。

また，三つ目の感染方法として，PCに接続されたすべてのUSBメモリに対し，次の方法を試みる。

感染方法3　USBメモリを媒介する感染
USBメモリにXウイルス自身のコピーと，自動実行ファイルを作成して，別のPCにそのUSBメモリが接続されたときに感染しようとする。

感染したPCの動作の特徴として，次のことが確認されている。

特徴1　Xウイルス自身は動的リンクライブラリであり，OSのシステムプログラムの一部として起動されるので，そのプロセスの停止を行うことはできない。

特徴2　Xウイルスはインターネット上の特定のWebサーバに接続し，決められた名前のファイルをダウンロードした後，そのファイルを実行しようとする。今のところ，そのWebサーバに決められた名前のファイルが存在しないので，ダウンロードは失敗する。Webサーバへの接続には，ブラウザのプロキシ設定情報を利用する。この動作を60分間隔で行う。

注(1)　この脆弱性に対するセキュリティパッチは前月にリリースされている。

図3　Xウイルスの感染方法と特徴

〔X ウイルス駆除手順の作成〕

A 主任は，J 社製ウイルス対策ソフトをすべての PC とサーバに導入することは，費用的な問題ですぐにはできないことや，I 社製ウイルス対策ソフトでも近々検知できるようになると思われることから，C 課長以外の PC については，J 社製ウイルス対策ソフトの導入は，ひとまず行わないことにした。そこで，X ウイルスの感染方法と特徴から，X ウイルスに特化した駆除手順を作成することにした。駆除手順を作成するに当たっては，感染 PC の特定方法，X ウイルスの駆除作業，感染防止策の三つを検討した。まず，X ウイルスの感染方法と特徴を基にして，感染 PC の特定方法を検討した。X ウイルスに感染した PC の特定方法を図 4 に示す。

特定方法 1

感染方法 1 から，部門の L2SW の空きポートに接続したパケットモニタで，［ a ］パケットを監視し，連続した［ b ］に対して昇順に問い合わせ，［ c ］を要求している PC を，感染 PC として特定する。（部門の L2SW には，モニタポートは付いていない。）

特定方法 2

特徴 2 から，［ d ］サーバのログ解析を行い，［ e ］に接続を試みている PC を，感染 PC として特定する。

図 4　X ウイルスに感染した PC の特定方法

X ウイルスの駆除作業については，J 社から無償で提供されている，X ウイルス専用駆除ツールを利用することにした。

感染防止策については，感染方法 1～3 に対応して，それぞれ，図 5 の感染防止策 1～3 を行うこととした。

なお，X ウイルスに感染していない PC だけではなく，①X ウイルスの駆除に成功した PC にも，図 5 の感染防止策を行うことにした。

感染防止策 1

OS とアプリケーションの脆弱性を解消するために，一時的に②特別な接続方法で社内ネットワークに接続し，内部サーバネットワーク上にあるパッチ配信サーバから，セキュリティパッチのダウンロードを行い，最新のセキュリティパッチまでを適用する。

感染防止策 2

［ f ］

感染防止策 3

USB メモリの使用を規則で禁止するとともに，USB メモリ接続時の自動実行機能を，PC の設定で無効化する。

図 5　X ウイルスの感染防止策

以上の検討結果を踏まえ，図 6 の駆除手順を決めた。

(1)　感染 PC を特定する。（具体的な方法は図 4 参照）
(2)　感染 PC を社内ネットワークから切断する。
(3)　感染 PC に，X ウイルス専用駆除ツールを利用する。
(4)　駆除が成功したと表示された場合は，(5)へ進む。そうでない場合は，その PC の使用を禁止し，X ウイルス専用駆除ツールの更新を待って再度駆除を試みるか，ハードディスクドライブを初期化して，OS とアプリケーションの再インストールを行う。
(5)　感染防止策 1～3 を実施する。（具体的な方法は図 5 参照）
(6)　社内ネットワークに接続する。

図 6　X ウイルスの駆除手順

〔X ウイルス駆除の実行〕

A 主任は，情報システム部員とともに，まず，図 6 の(1)を実施した。その結果，営業部で使用している 180 台の PC のうち，30 台が感染 PC であることが分かった。その他の部門ネットワークで，感染 PC は発見されなかった。これら 30 台の感染 PC のうち 23 台については，前月のセキュリティパッチが適用されていなかった。残り 7 台については，OS の管理者 ID のパスワードが，感染方法 2 で使用されるパスワード辞書のものと一致していた。

また，営業部員へのヒアリング調査の結果，この X ウイルス感染は，ある営業部員が，自宅で仕事をしようとファイルを持ち帰るときに使用した，個人所有の USB メモリからの感染が発端であることが判明した。

これら 30 台の感染 PC に対して，X ウイルスの駆除手順に従って，情報システム部員が駆除作業を行い，無事，X ウイルスの駆除を完了した。また，X ウイルスに感染していない PC に対しても，感染防止策を実施し，X ウイルスへの対応を完了した。

その後，B 課長は，セキュリティパッチ適用の時期を，PC の利用者の判断にゆだねていたことが，X ウイルスの感染を広げた原因の一つと考え，K 社が保有するすべての PC への強制的なセキュリティパッチ適用と，サーバへの速やかなセキュリティパッチ適用の方法を検討するよう，A 主任に指示した。

設問 1　図 3 中の特徴 2 について，感染 PC 上のファイルを攻撃者のサーバにアップロードするようなプログラムのファイルがダウンロードされた場合，どのような被害が発生する可能性があるか。30 字以内で具体的に述べよ。

設問 2　感染 PC の特定方法について，図 4 中の [a] ～ [e] に入れる適切な字句を答えよ。[a] についてはプロトコル名を 5 字以内で，[b]，[c] についてはそれぞれ 10 字以内で，[d] については 5 字以内で，[e] については 20 字以内で答えよ。

設問 3　本文中の下線①について，駆除に成功した PC に対して，感染防止策をとらなかった場合には，どのようなことが起こり得るか。15 字以内で述べよ。

設問 4　図 5 の感染防止策について，(1)，(2)に答えよ。

(1)感染防止策 1 を実行するに当たって，下線②のように接続する必要がある。特別な接続方法を 50 字以内で具体的に述べよ。

(2)感染防止策 2 として，[f] に入れる適切な字句を，30 字以内で述べよ。

解答例

問 1

出題趣旨

レースコンディションを発生させるバグは，通常の機能テストでの発見が困難である。さらに，レースコンディションに起因する叙弱性は，その原因の発見と対策に時間が掛かる。したがって，レースコンディションの正しい理解に基づいて，プログラムの設計及びコーディングの時点で十分な注意を払うことが必要である。

本問では，Web アプリケーション開発における脆弱性対策に必要な知識として，主にレースコンディションの仕組みとその対策についての理解を問う。

設問 l　a　バッファオーバフロー

設問 2　(1) インスタンス変数 tempPDF が複数のスレッドからほぼ同時に書き込まれたので，想定外の値となった。

(2)・レースコンディション

・競合状態

(3) インスタンス変数 tempPDF を doGet メソッドのローカル変数として定義する。

(4) 利用者 ID が異なる，多数の HTTP リクエストを，ほぼ同時に Web サーバに送信する。

設問 3　(1) 他人の従業者番号を基に，勤務時間集計表の URL を推測し，ダウンロードを試みる。

(2) b　PDF ファイル形式の勤務時間集計表

問 2

出題趣旨

機密保護を実現する際には暗号化か有力な候補となるが，十分な検討を行わずに暗号化機能を導入すると，システム障害などが発生した際に，暗号化されたデータを復号することができず，結果として業務に支障を来してしまう可能性がある。

本問では，まず，暗号化とバックアップそれぞれについて，基本的な仕組みと，導入時に考慮すべき点を出題することによって，暗号化及びバックアップの導入に関する基本的な理解力を問う。続いて，暗号化とバックアップを同時に利用した場合に発生する問題と解決方法について出題することで，機密性と可用性の両面から施策を検討し，解決する能力を問う。

設問 1　(1) a　ア

b　オ

c　カ

(2) ①　ウ

②　エ　　順不同

(3) d　ア

設問 2　(1) バックアップテープを本社に宅配便で移送する際にテープが盗難に遭う。

(2)・テープにデータをバックアップする際，暗号化する。

・安全な移送サービスを利用する。

設問 3　(1) (b)

(2) TPM が交換され，メールボックスファイル内の暗号化されたメールを復号す

るための秘密鍵が使えなくなったから
(3) ファイル暗号化方式と S/MIME の鍵ペアを TPM 外で作成して安全にバックアップした後，TPM を用いて保管する。

問 3

出題趣旨

個人情報のように，送受信の際に暗号化か必要とされる情報を，企業間で安全に送受信するのは，容易なことではない。企業間の送受信において電子メールを暗号化することは難しい場合が多い。 TLS （SSL）で保護された Web ページを利用するのも一つの方法であるが，正当な利用者であることを確認する必要がある。

本問では，暗号化，電子メール，パスワードなどに関する基本的な知識を前提として，具体的な状況に応じて解決策を提案できる能力を問う。

設問 1 (1) a S/MIME 証明書
b メール
(2) 証明書の正当性を確認できないから
(3) 紙媒体でフィンガプリントを入手する。
(4) パスワードエラーが一定回数連続して発生したら，ログインを一定時間拒絶する。

設問 2 (1) あて先に実在する求人企業の従業員からの申込みであることを確認するため
(2) ランダムな文字列になるように生成する。
(3) メールを盗聴し，利用者よりも先に再設定実行ページにアクセスする手口
(4) パスワード再設定実行ページに，初期パスワードの入力を追加する。

問 4

出題趣旨

ウイルスには，ウイルス対策ソフトで検知，駆除ができないものもあり，その場合，そのウイルスに応じた対応が必要となる。

本問では，新種のウイルスの感染方法や感染後の動作の特徴などから，感染 PC の特定方法や，駆除手順，再感染防止策の立案について問う。

設問 1 秘密情報の入ったファイルが攻撃者に盗まれる可能性

設問 2 a ARP
b IP アドレス
c MAC アドレス
d プロキシ
e インターネット上の特定の Web サーバ

設問 3 X ウイルスに再び感染する。

設問 4 (1) 当該 PC と L2SW の間にファイアウォールを設置し，通信をパッチ配信サーバとの間に限定する。
(2) f 管理者 ID のパスワードを推測しにくいものに変更する。

採点講評

問 1

問 1 では，セキュアプログラミングの分野から，主にレースコンディションの発生の仕組みと対策について出題した。全体として正答率は想定どおりだった。

設問 2（2）は，正答率が低かった。レースコンディションという用語は，脆弱性を理解，説明する上で必須であるので確実に理解してほしい。また，設問 2（4）も正答率が低かった。レースコンディションの有無をテストするためには，“多数の”リクエストを“同時に”発行するというテスト方法が必須であることを理解しておいてほしい。

設問 3 は，URL 推測に関して出題したが正答率は高かった。 URL 推測に対する対策は Web サイト構築において必須の事項であり，確実に対策を行うことを期待したい。

問 2

問 2 では，PC に保存するデータの暗号化と，暗号化したデータをバックアップする際に検討すべき点について出題した。全体として正答率は想定どおりだった。

設問 1 では，暗号化の基本的な仕組みを出題した(1)は，正答率が高かったが，TPM に関して出題した(2)は，選択肢形式であるにもかかわらず正答率が低かった。 TPM が搭載されている PC も多くなっているので，TPM の基本的な機能は理解しておいてほしい。

設問 2 は，正答率は高かった。バックアップに限らず，何らかの対策を検討する際には，その対策を導入することで新たなリスクが生じないか確認する必要性について認識しておいてほしい。

設問 3 は，正答率は低かった。暗号化データのバックアップを検討する際には，バックアップデータの確実なリストアと，安全な保管を実現するために，データ保存形式と，鍵管理方法の理解が必要となってくる。代表的な暗号化アプリケーションについてはどのような対策が必要かを是非理解しておいてほしい。

問 3

問 3 では，個人情報保護に関連して，企業間で情報を安全に受け渡す方法について出題した。全体として正答率は想定どおりだった。

設問 1(3)は，正答率が低かった。証明書の真正性を確認するため，紙媒体や電話など，フィンガプリントのオフラインでの入手方法について解答してほしかったが，機密性に着目してしまい，暗号化を挙げた解答が多かった。

設問 2(1)も，正答率が低かった。登記事項証明書の所在地に実在する企業からの申込みであることを確認できる点を解答してほしかったが，“メールで送信すると盗聴のおそれがある"など，ほかの方法の欠点だけを述べた解答が散見された。(2)は，正答率が高かった。初期パスワードを推定されないようにするために，ランダムな文字列や乱数を含めるべきであるということは，よく理解されていた。

問 4

問 4 では，新種のウイルスに感染した場合の駆除手順や再感染防止策の立案について出題した。全体として正答率は想定どおりだった。

設問 2 の a 及び c は，正答率が低かった。モニタポートのない L2SW に接続したパケットモニタで感染 PC を特定するためには，ブロードキャストパケットを監視しなければなら

ないことに気づいてほしかった。

設問 4(1)は，正答率は低かった。X ウイルスの感染方法から，同一ネットワーク上に感染 PC がある場合に，感染する可能性があることに注目して，解答してほしかった。