問1　セキュアプログラミングに関する次の記述を読んで，設問1～4に答えよ。

A社は，従業員数100名のソフトウェア開発会社である。A社では，PC向けソフトウェア製品として，“青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律”に基づいた青少年有害情報フィルタリングソフトウェア（以下，Bフィルタという）を開発することとなった。

A社では，Bフィルタの開発に当たって，F主任をリーグとした開発チームを編成した。この開発チーム内の体制は，設計を行うDグループ，作成を行うPグループ及び試験を担当するQグループの三つのグループとした。また，プログラム開発に用いる言語は，JIS X 3014 “プログラム言語C++”（以下，C++という）とした。

次は，この開発におけるセキュリティの脆弱性の発見から修正及び再発防止に至る経緯である。

〔URLマッチングの方式設計〕

Dグループでは，Bフィルタの概略機能を図1のようにまとめた。その後，要件定義を経て，URLマッチングによる有害の度合いを決定する方式設計を行い，図2の内容のとおり決定した。

(1) Bフィルタの提供形態は，特定のブラウザ（以下，Xブラウザという）へのプラグインとする。
(2) Xブラウザから Web サイトへのアクセスを監視し，有害情報と判定されるアクセスをブロックする。
(3) 次の要素を総合して，有害情報であるか否かを判定する。
　(a) URLマッチング
　　アクセスしようとしたURLと，有害情報のURLリストとのマッチングによって有害の度合いを決定する。有害情報のURLリストはA社が逐次更新し，自動ダウンロード機能によってBフィルタに取り込まれる。
　(b) キーワードマッチング
　　表示するコンテンツの内容と，有害情報であるか否かを判定するためのキーワードリストとのマッチングによって有害の度合いを決定する。キーワードリストは，青少年の保護者が設定する。
(4) 保護者による設定で，動画へのアクセスをすべてブロックすることが可能である。
（以下，省略）

図1　Bフィルタの概略機能

(1) Xブラウザのプラグイン用インタフェースを利用し，Xブラウザから Web サイトへのアクセスをトリガにしてURLマッチング処理を開始する。
　なお，Xブラウザからプラグインには，利用者がアクセスしようとしたURLがそのまま渡される。
(2) マッチングに先行して，Xブラウザから渡されるURLを次のとおり正規化する。
　・文字コード：UTF-8とする。
　・URLエンコード：RFC 3986に準拠する（パーセントエンコード）。
　・正規化後の文字列長：128バイト以下とする。128バイトを超える部分は切り捨てる。
（以下，省略）

図2　URLマッチングの方式設計結果

〔詳細設計と作成〕

Dグループでは，図2の方式設計結果に基づいて設計作業を進め，URLをパーセントエンコードする機能を一つの関数として作成することを決定し，その関数の仕様を

図3のとおりとした。

```
void urlPercentEncode(char *dst, char *src, int n)
返却値：なし。
  効果：src が指す文字列（終端ナル文字を含む）から dst が指す文字列に文字をすべて転記する。その
        際，エンコードすべき文字を検出した場合は，当該文字をパーセントエンコードした上で dst が指
        す文字列に転記する。
        なお，n の値は dst が指す文字列に書き込める最大バイト数とする。
        dst が指す文字列への転記に当たって，バイト数が n を超える場合は，n バイトを書き込んだ時点
        で処理を打ち切って終了する。この場合，dst が指す文字列がナル文字で終了することは保証され
        ない。
```

図3　作成するパーセントエンコード関数の仕様

その後，Pグループでは，パーセントエンコード関数の作成に取り掛かり，図4に示すソースコードを作成した。

```
1  void urlPercentEncode(char *dst, char *src, int n){
2     int srcPos = 0;
3     int dstPos = 0;
4     char x = 0;
5
6     while(src[srcPos] != '\0' && dstPos < n){
7        /* エンコードすべきか否かを判定 */
8        if(src[srcPos] == '-' || src[srcPos] == '.' ||
9                 src[srcPos] == '_' || src[srcPos] == '~' ||
10                ((src[srcPos] >= '0') && (src[srcPos] <= '9')) ||
11                ((src[srcPos] >= 'A') && (src[srcPos] <= 'Z')) ||
12                ((src[srcPos] >= 'a') && (src[srcPos] <= 'z'))){
13       /* エンコードしない場合 */
14          dst[dstPos++] = src[srcPos++];
15       }
16       else{
17       /* エンコードする場合 */
18          dst[dstPos++] = '%';
19          x = (src[srcPos] & 0x00f0) >> 4;
20          dst[dstPos++] = x <= 9 ? x + '0' : x - 10 + 'A';
21          x = src[srcPos++] & 0x000f;
22          dst[dstPos++] = x <= 9 ? x + '0' : x - 10 + 'A';
23       }
24    }
25    if(dstPos < n){
26       dst[dstPos] = '\0';
27    }
28    return;
29 }
```

図4　最初に作成したソースコード

〔脆弱性の発見〕

開発計画に基づき，URLマッチング機能だけがおおよそ完成した時点のものをプロトタイプ1として，Qグループによる試験を実施した。その試験の結果，ある特定の

条件下でURLマッチング機能が正常に動作しない不具合が発見された。その結果を受けてプロトタイプ1の動作について詳細に確認したところ，パーセントエンコード関数が実行された直後に，ほかの関数でフラグとして使用している変数（以下，フラグ変数という）が想定外の値に書き換わり，URLマッチング機能が正常に動作しないことが判明した。

ソースコードの調査を行ったところ，パーセントエンコード関数にバッファオーバフロー脆弱性があり，隣接したメモリ領域に置かれたフラグ変数が想定外の値に書き換えられることが分かった。

〔関数の仕様変更〕

Bフィルタの開発チームは，Bフィルタで同様の脆弱性を作り込まないようにするために，標準C++ライブラリの文字列クラスを使用してパーセントエンコード関数を作り直すとともに，ほかの関数においても作り直しを行った。パーセントエンコード関数の作り直しに当たって，引数及び返却値を文字列型に変更するのに伴い，Dグループでは関数の仕様を図5に示すように変更した。その後，Pグループは図5の仕様に基づいた関数の作成に取り掛かり，図6のソースコードを作成した。

なお，図3の仕様に基づく関数`urlPercent Encode()`を呼び出していた部分は，すべて図5の仕様に基づく関数`urlPercent EncodeString()`を呼び出すように修正した。

```
string urlPercentEncodeString(string src)
返却値：処理済の文字列。
  効果：src 文字列から，返却値に文字をすべて転記する。その際，エンコードすべき文字を検出した場合
        は，当該文字をパーセントエンコードした上で返却値に転記する。
```

図５　変更したパーセントエンコード関数の仕様

```
#include <string>
#include <iterator>

using namespace std;

string urlPercentEncodeString(string src){
   string dst("");
   string::iterator readPoint = src.[ a ]();
   string::iterator atEOL = src.[ b ]();
   char x = 0;

   while(readPoint != atEOL){
      /* エンコードすべきか否かを判定 */
      if(*readPoint == '-' || *readPoint == '.' ||
               *readPoint == '_' || *readPoint == '~' ||
               ((*readPoint >= '0') && (*readPoint <= '9')) ||
               ((*readPoint >= 'A') && (*readPoint <= 'Z')) ||
               ((*readPoint >= 'a') && (*readPoint <= 'z'))){
      /* エンコードしない場合 */
         dst.push_back(*(readPoint++));
      }
      else{
      /* エンコードする場合 */
         dst.push_back('%');
         x = (*readPoint & 0x00f0) >> 4;
         x = x <= 9 ? x + '0' : x - 10 + 'A';
         dst.push_back(x);

         x = *readPoint++ & 0x000f;
         x = x <= 9 ? x + '0' : x - 10 + 'A';
         dst.push_back(x);
      }
   }
   return dst;
}
```

図６　作り直したソースコード

図４のソースコードでは文字列を配列として取り扱っていたので領域の境界をプログラムで管理する必要があったが，図６のソースコードでは [c] ので，バッファオーバフローが発生することはなくなった。

〔修正後の確認と再発防止〕

その後，Q グループでは，作り直したプロトタイプ１を試験して，バッファオーバフローが発生しないことを確認した。最後に，F 主任は再発防止策として，従来の A

社における C++開発標準ルールを図 7 に示すように改訂した。
なお，図 7 中の下線部は，この改訂によって追加した項目である。

1. 識別子
（省略）
2. 型・定数
- 共用体の使用を禁止する。構造体の使用は，最小限にとどめる。
- オブジェクトを生成する場合，できる限り標準 C++ライブラリで定義されたクラスを使用する。
（省略）
3. 宣言・定義・初期化
- 直接アクセス可能なグローバル変数は使用しない。必要な場合は，専用のアクセサを使用する。
- すべてのオブジェクトは，明示的に初期化する。
（省略）
4. ポインタ・配列
- ポインタ変数に対する演算操作は禁止する。
- 文字列処理を行う場合，文字列を格納するための［ d ］の使用を禁止する。
- 配列又はポインタに添字を指定して書込みを行う場合，［ e ］を毎回実施する。
（省略）
5. 関数
- 関数の返却値及び引数に関して，明示的に型を宣言する。
- 関数内で値を変更する場合を除き，関数の引数であるポインタは const へのポインタとする。
- 引数としてポインタを受け取った場合，添字指定での［ f ］は禁止する。
- 文字列処理を行う関数では，処理が成功したときは，原則として処理結果の文字列を返却値として返す。
（以下，省略）

図 7　A 社における C++開発標準ルール（改訂版）

この改訂によって，A 社におけるプログラム開発では本件と類似した問題点を作り込むことがなくなり，より安全なソフトウェアを提供することができるようになった。

設問 1　図 6 中の［ a ］，［ b ］に入れる適切なメンバ関数名(メソッド名)を解答群の中から選び，記号で答えよ。

解答群

ア　begin　　イ　clear　　ウ　end　　エ　get
オ　set　　カ　size　　キ　start　　ク　tail

設問 2　図 4 のソースコードで発見された脆弱性について，(1)，(2)に答えよ。

(1)バッファオーバフローが発生するメモリ領域はどこか。図 4 中の変数名を用いて 20 字以内で述べよ。

(2)図 4 の 6 行目から始まる while 文の副文(ループ本体)の実行において，バッファオーバフローが発生するための条件を，図 4 中の変数名を用いて 60 字以内で述べよ。

設問 3　本文中の［ c ］では，図 4 で存在したバッファオーバフロー脆弱性が，図 6 では存在しない技術的理由を述べている。［ c ］に入れる適切な字句を 60 字以内で述べよ。

設問 4　図 7 について，文字列の取扱いで本件と類似した問題点の作り込みを未然に防ぐのに有効となるように［ d ］～［ f ］に入れる適切な字句を，それぞれ 8 字以内で答えよ。

問2　ソフトウェア資産管理に関する次の記述を読んで，設問1～5に答えよ。

C社は，従業員数400名の広告代理店である。C社では，主にテレビ，雑誌，新聞などのマスメディアの広告枠の販売並びに広告の企画及び制作を行っている。C社のすべてのサーバとPCは，ネットワークで接続されている。C社の情報システム部のT部長は，ソフトウェアライセンス（以下，ライセンスという）に対する違反行為が，最近，社会問題になっているという話を聞き，ライセンスに関する社内外の状況を整理して報告するよう，部下のU主任に指示した。U主任の報告は図1のとおりである。

(1) ライセンスの形態には，PCの台数，CPU数，利用者数などに応じてライセンス料を支払うものと，ライセンス料不要というものがある。社内で使用しているライセンスは，PCの台数に応じてライセンス料を支払う法人向けのものか，ライセンス料不要のもののいずれかである。
(2) 通常のライセンスに加えて，学校などの教育機関に所属する利用者だけに許諾されるアカデミックライセンスや，旧バージョンのライセンス保持者だけに許諾される［ a ］ライセンスが提供される場合もある。
(3) ライセンス契約違反に問われた場合は，ソフトウェア開発元から，正規のライセンス料のほかに，［ b ］金や訴訟費用を請求される場合もある。また，海賊版の使用，許諾ライセンス数を超えるインストールなどが［ c ］法に違反すると指摘された事例もある。
(4) 社内の各部門が購入するソフトウェアは，購買部が依頼を受け，発注・受領を行い，各部門に渡している。各部門にソフトウェアの購入履歴はあるが，購入後のライセンス管理は行われていない。

図1　ライセンスに関する社内外の状況

〔ライセンスの実態調査〕

T部長は，U主任の報告を踏まえて，C社における保有ライセンスと，ソフトウェアのインストールの詳細な状況を次のような手順で調査することにした。

(1) 各部門の購入履歴から，各部門で購入したソフトウェアの名称，保有ライセンス数などを調査し，保有ライセンス一覧表を作成する。
(2) ソフトウェアをインストールしたときにOSに記録されるソフトウェアの識別情報（以下，インストール情報という）を利用して，PC上にインストールされているソフトウェアを把握し，使用ソフトウェア一覧表を作成する。
(3) 保有ライセンス一覧表と使用ソフトウェア一覧表を突き合わせる。

なお，サーバ上のソフトウェアのライセンスは適切に管理できていることから，今回の調査はPC上のソフトウェアだけを対象とすることにした。また，ライセンス料不要のものとOSは，調査の対象外とした。

U主任が調査した結果，各部門で使用実態に比べて十分な数のライセンスを保有していることが確認できた。ただし，ソフトウェアの使用数に比べて保有ライセンス数がかなり多い部門も存在していた。このようなライセンスの中には，他部門が購入を予定しているものも含まれていた。

〔ソフトウェア資産管理ツールの導入〕

U主任は，①インストール情報が記録されないソフトウェアがあることや，インストール情報を書き換えてソフトウェアの存在を隠ぺいするツールがインターネット上

に存在していることなどから，インストール情報による調査では把握できないソフトウェアが，使用ソフトウェア一覧表以外にもインストールされているおそれがあるとT部長に報告した。そこで，T部長は，ソフトウェア資産管理ツール（以下，管理ツールという）の導入を経営陣に提案し，承認を得て実行に移した。管理ツールは，保有ライセンスとソフトウェアの使用状況を管理するためのものであり，管理サーバに導入するサーバプログラムと，PCに導入するエージェントで構成されている。管理ツールの主な機能を表1に，管理サーバ上に保存される情報を表2にそれぞれ示す。

表1　管理ツールの主な機能

機能名称	機能の説明
保有ライセンス登録機能	管理ツール利用者が入力した保有ライセンスの情報を，管理サーバ上に保有ライセンス情報として登録する。保有ライセンス情報は，削除又は更新することも可能である。
インストール情報収集機能	PC上のソフトウェアのインストール情報を定期的に収集し，PCごとの収集インストール情報として管理サーバ上に保存する。
実行情報収集機能	PC上でソフトウェアが実行されたときに，PCのOSが採取した実行情報を収集し，PCごとの収集実行情報として管理サーバ上に保存する。
ソフトウェア比較機能	・収集インストール情報又は収集実行情報が，それまでになかった新しい情報の場合には，ライセンス未登録とマークした上で，既存インストール情報又は既存実行情報に追加する。 ・既存インストール情報又は既存実行情報にライセンス未登録とマークされたものが存在する場合には，警告を表示して，管理ツール利用者に，使用ライセンス登録機能を用いてライセンスを割り当てるよう促す。
使用ライセンス登録機能	ライセンス未登録とマークされたものに対応するライセンスの情報は，管理サーバ上の保有ライセンス情報に余裕があることを確認した上で，使用ライセンス情報として追加登録する。さらに，ライセンス未登録とマークされた既存インストール情報及び既存実行情報のうち，管理ツール利用者が指定したものについて，ライセンス未登録のマークを取り消す。使用ライセンス情報，既存インストール情報，及び既存実行情報は削除又は更新することも可能である。

表2　管理サーバ上に保存される情報

情報名称	格納されている情報	管理単位
保有ライセンス情報	ライセンス管理番号，ソフトウェア名称，購入日，ライセンス数，ライセンス購入申請部門など	C社全体
使用ライセンス情報	ライセンス管理番号，ライセンス使用PC名，PC利用者名，利用者所属部門など	C社全体
収集インストール情報	各エージェントが収集したソフトウェアのインストール情報	PCごと
収集実行情報	各エージェントが収集した実行ファイル名，実行プロセス名などの実行情報	PCごと
既存インストール情報	以前に収集され，まだ削除されていないインストール情報	PCごと
既存実行情報	以前に収集され，まだ削除されていない実行情報	PCごと

〔管理ツールの活用〕

管理ツールを導入して1か月たったある日，新種のウイルスが急速に感染を拡大しているという情報が入ってきた。そのウイルスは，PC用のあるソフトウェアの脆弱性を悪用して感染するもので，そのソフトウェアに特定のセキュリティパッチを適用すれば感染しないというものであった。T部長が管理ツールの機能を確認したところ，

表 1 中の機能で，該当するセキュリティパッチの適用状況を把握できることが判明した。C 社では，管理ツールの機能を活用して，このウイルスの感染を未然に防ぐことができた。

その 1 週間後，T 部長は，開発元のセキュリティパッチ提供が終了したソフトウェアの利用が問題になっているという記事を見た。管理ツールには，インストール情報の一部として，ソフトウェアのバージョン（セキュリティパッチの情報を含む）を管理する機能がある。T 部長は，この機能を活用して，開発元のセキュリティパッチ提供が終了したソフトウェアを抽出できるのではないかと考え，早速，活用を開始することにした。

定期人事異動を 2 か月後に控えたある日，T 部長は人事異動のときのライセンス管理手順に問題がないかを確認することにした。C 社では，人事異動に伴い，異動前に使用していた PC を異動前の部門に残していく場合と，PC を異動後の部門に持っていく場合がある。 PC 管理情報を更新するとともに，PC を異動前の部門に残していく場合には，使用ライセンス登録機能で，使用ライセンス情報の PC 利用者名を次の利用者に更新する。PC を異動後の部門に持っていく場合には，使用ライセンス登録機能で，使用ライセンス情報の利用者所属部門を更新するとともに，業務内容の変更に伴って新たに必要となるソフトウェアがあれば PC にインストールし，使用ライセンス登録機能で使用ライセンス情報に追加登録する。

T 部長は，<u>②異動後の部門に PC を持っていく場合に PC 上と管理ツール上でそれぞれ更に実施すべきことがある</u>と考え，手順に項目を追加することにした。

〔管理ツール運用上の問題点の改善〕

管理ツールを導入して 1 年後，保有ライセンス情報を不正に登録されると，ライセンス管理がうまく機能しないおそれがあることが分かった。現状では，管理ツール利用者が自分自身で利用するソフトウェアであっても保有ライセンス情報を登録できる一方，登録された保有ライセンスが購入されたライセンスであるかどうかを C 社では確認していない。このため，T 部長は，管理ツール利用者は，自分自身が利用するソフトウェアの保有ライセンス情報を登録できないようにする運用方針を経営陣に提案し，承認を得て実行に移した。その後，C 社では，管理ツールを活用して順調にライセンス管理を行っている。

設問 1　図 1 中の [a] ～ [c] に入れる適切な字句をそれぞれ答えよ。

設問 2　〔ライセンスの実態調査〕において，部門内だけの調査結果からは把握できないが，全社としての調査結果から把握できることは何か。25 字以内で述べよ。

設問 3　〔ソフトウェア資産管理ツールの導入〕において，管理ツールが，本文中の下線①のようなソフトウェアを検出できる理由は何か。 4o 字以内で述べよ。

設問 4　〔管理ツールの活用〕について，(1) ～ (3) に答えよ。

(1) ウイルスの感染を防ぐために，管理ツールの機能をどのように活用したのか。45 字以内で述べよ。

(2) 管理ツールの機能を利用して，開発元のセキュリティパッチ提供が終了したソフトウェアを抽出することは，情報セキュリティの観点からどのような意義があるか。 45 字以内で述べよ。

(3) 本文中の下線②について，Pc 上で実施すべきと T 部長が考えたことは何か。30 字以内で述べよ。

設問 5　〔管理ツール運用上の問題点の改善〕において，T 部長が提案した運用方針が，

保有ライセンス情報の不正登録の対策となる理由は何か。30 字以内で述べよ。

問 3　情報漏えい対策に関する次の記述を読んで，設問 1～4 に答えよ。

E 社は，雑貨やアイディア商品の企画・販売を行う従業員数 100 名の会社である。大手通販会社や生活用品店，雑貨店，全国チェーンのドラッグストアなどを顧客にもち，E 社ブランド商品の販売のほか，顧客のプライベートブランドで販売される OEM 商品の企画や各種イベントとタイアップした商品の企画なども手掛けている。

〔情報漏えい事故の発生と対策の指示〕

ある日，E 社の従業員が帰宅後も資料を作成するために，USB メモリに商品の企画書をコピーして持ち帰り，その USB メモリを紛失するという事故が起こった。USB メモリにコピーした企画書は，顧客である L 社のプライベートブランドで販売される予定の OEM 商品に関するものであり，L 社への事情説明と謝罪に加え，商品の企画をやり直す事態となった。

当該商品が企画の初期段階であり，幸い大事に至らなかったが，今後，業務情報の社外持出しに起因する重大な情報漏えい事故が発生しないとも限らないと E 社社長は考えた。そこで，E 社社長は，情報システム部長を通じて，情報システム部の Y 課長に，E 社における業務情報の社外への持出しの現状を調査し，必要であれば情報漏えい対策を検討するよう指示した。

〔業務情報の持出しに関する現状調査〕

Y 課長は，まず，“業務情報の持出し”を，“会社貸与のノート PC（以下，貸与 PC という）や会社貸与の USB メモリ（以下，貸与 USB メモリという）に業務情報を保存して社外に持ち出すこと”と定義した上で，業務情報の持出しの状況についての調査と対策の検討を進めることにした。一方，電子メールやファイル転送などによる社外への情報の送信についての調査と対策の検討は，別途実施することにした。

Y 課長は，E 社における業務情報の持出しの現状を調査するために，情報システム部の Z 君とともに従業員のうちの何人かにヒアリングを行った。

ヒアリングの結果，従業員が業務情報を持ち出す目的は，顧客との打合せ（以下，M という）か，自宅での資料作成（以下，H という）のいずれかであることが分かった。現状，いずれの場合においても申請や承認などについて規定されていない。

Z 君は，E 社の業務情報の持出しの状況について，概要を表 1 に整理した。

表 1　E 社の業務情報の持出しの状況

持ち出す目的	持ち出す者	持出先	持ち出す業務情報（以下，持出情報という）と開示可能範囲		現状の持出手段
			持出情報の内容	開示可能範囲	
M	E 社営業担当者	顧客先	E 社ブランド既存商品の情報	制限なし	貸与 PC
			OEM 商品やタイアップ商品の企画書及び提案書	E 社内の案件関係者並びに OEM 又はタイアップ先の顧客	
H	E 社従業員	自宅	・公開前のプレスリリース ・E 社ブランド商品の企画書 ・キャンペーン，プロモーションなどの企画書	E 社内の案件関係者	貸与 PC 又は貸与 USB メモリ
			E 社ブランド既存商品の情報	制限なし	
			OEM 商品やタイアップ商品の企画書及び提案書	E 社内の案件関係者並びに OEM 又はタイアップ先の顧客	

貸与 PC で業務情報が持ち出された場合は，M，H のいずれにおいても，持出先での業務情報へのアクセスには，その貸与 PC 自体が利用されている。一方，H において，貸与 USB メモリで業務情報が持ち出された場合は，従業員が私有する PC（以下，私有 PC という）を利用して業務情報にアクセスすることがあると判明している。

M については，顧客に資料を提示しなければならないという業務上の必要性があるのに対し，H については，E 社オフィス内で資料作成を実施すればよく，必要性に乏しい。そこで Y 課長は，H のための持出しについては，禁止することを会社規則として規定した上でそれを全社に周知することとし，M については，情報漏えい対策の検討を Z 君に指示した。

〔M における情報漏えい対策の検討〕

Z 君は，M における情報漏えい対策を検討するに当たって，M のための業務情報の持出しに関連した情報漏えいリスクへの現状の対応状況を表 2 に整理した。

表２　Ｍのための業務情報の持出しに関連した情報漏えいリスクへの現状の対応状況

情報漏えいリスク		リスクに対して有効と考えられる対策	E 社における左記対策の実施状況
(ア) 盗難，紛失	持出中に貸与 PC が盗まれる又は紛失する。	・情報を秘匿するための［ a ］ ・①貸与 PC の安全な持運びに関する注意点の周知	・情報は［ a ］していない。 ・貸与 PC の社外での取扱方法に関する規定はない。
(イ) マルウェアに感染	・持出中に貸与 PC がマルウェアに感染する。 ・マルウェアに感染した貸与 PC で情報を持ち出す。	・社外でのインターネット接続の禁止 ・ウイルス対策ソフトの導入 ・会社指定ソフトウェア以外のインストール禁止 ・セキュリティパッチ適用の徹底	・貸与 PC による社外でのインターネット接続は禁止していない。 ・貸与 PC にウイルス対策ソフトを導入済 ・会社指定ソフトウェアの規定はないが，従業員に貸与 PC の管理者権限が与えられていないので，管理者権限が必要なソフトウェアのインストールはできない。 ・貸与 PC に対してセキュリティパッチの強制適用を定期的に実施している。
(ウ) 不正開示	持出中に E 社従業員が，開示が許可されている対象者以外に（故意又は過失で）情報を開示してしまう。	開示可能範囲の周知	開示可能範囲は規定されているが，それを制限する技術的な対策は導入していない。
(エ) 盗み見	持出中に貸与 PC の画面をのぞき見られる。	・プライバシフィルタの利用 ・第三者から見られる場所での利用を禁止した規定の周知	・プライバシフィルタは利用していない。 ・貸与 PC の社外での取扱方法に関する規定はない。

Ｍでは，営業担当者が持出情報を持ち歩いていることに加え，②日常業務に利用している貸与 PC を持ち出していることで　万一　情報漏えい事故が発生すると被害が大きくなるおそれがあることから，Z 君は，営業担当者が業務情報を持ち出す必要をなくし，貸与 PC の社外への持出しも禁止することが情報漏えい対策として望ましいと考えた。そこで，情報漏えい対策として，ハードディスクなどの記憶装置をもたず USB メモリなどの外部記憶媒体も利用できないシンクライアント端末（以下，専用端末という）を利用する案（以下，案 1 という）と，公開 Web サーバのディスク領域を利用する案（以下，案 2 という）の二つの案を提案することにした。それぞれの案では，貸与 PC の社外への持出しは禁止した上で，図 1 のような手順によって，業務情報を持ち出すことなく顧客に見せることができる。

（案 1 の場合）
(1)　E 社内のサーバ上に，専用端末からアクセス可能なディスク領域をあらかじめ作成しておく。
(2)　E 社の営業担当者は，(1) で作成したディスク領域に業務情報を保存する。
(3)　E 社の営業担当者は，専用端末を用いて顧客先からそのサーバに VPN でリモートアクセスする。

（案 2 の場合）
(1)　E 社の公開 Web サーバ上に，各顧客専用のディスク領域をあらかじめ作成しておく。
(2)　各顧客には，専用のディスク領域にアクセスするための ID とパスワードを登録しておいてもらう。
(3)　E 社の営業担当者は，業務情報を当該顧客専用のディスク領域にアップロードした上で，当該顧客にダウンロードをしておくよう依頼する。

図１　案１及び案２による顧客への業務情報の提示手順

案2の場合は，③万一，公開Webサーバが不正アクセスされても．業務情報が漏えいするリスクをできるだけ小さくするための運用上の対策を併せて実施する。

案1，案2は，いずれも表2の(ア)及び(イ)のリスクを［b］することができる。表2の(ウ)のリスクについては，業務として特定顧客向けの業務情報を取り扱う以上，案1と案21のいずれであっても［b］することはできないので，［c］策を取ることとし，案1と案2のそれぞれの場合についてどの程度［c］できるかを検討し，次のようにまとめた。

(案1の場合)
業務情報ごとに開示が許可されている範囲を明確にし，ディスク領域に保存することを周知することはできるが，E社従業員の故意又は過失による他社への情報開示を技術的に禁止することは困難である。

(案2の場合)
アップロード時に故意又は過失で当該顧客向け業務情報を他社に開示するリスクがあるが，業務情報のアップロードに際して，④アップロードする営業担当者の上司による確認がなされれば，そのリスクを［c］することができる。

表2の(エ)のリスクについては，案2では顧客が業務情報をダウンロードすることによって［b］できる一方で，案1では［b］できない。
Z君は，以上の検討結果から，Mにおいては案2を採用するという対策をまとめ，Y課長に報告し，了承を得た。

〔対策案の見直し〕
Y課長が情報漏えい対策について情報システム部長に報告したとき，部長から次のコメントがあり，Hのための業務情報の持出しについて追加の検討をすることになった。
(a)E社では，テレワーキングの導入を検討しており，Hは，近い将来，許可される方向にある。
(b)当面はHを禁止することを前提として検討を進めて構わないが，テレワーキングの導入に伴ってHが許可された場合の対策も併せて検討しておいてほしい。

Y課長とZ君は，Hが許可された場合の対策を検討するに当たって，表2の内容を見直し，Hのための業務情報の持出しの対応状況も含めて整理することにした。
なお，表3は，変更後の表2から，(ア)及び(イ)の行を抜粋したものである。

表 3　M と H のための業務情報の持出しに関連した情報漏えいリスクへの対応状況（変更後の表 2 の抜粋）

情報漏えいリスク		リスクに対して有効と考えられる対策	E 社における左記対策の実施状況
(ア) 盗難，紛失	持出中に貸与 PC 又は貸与 USB メモリが盗まれる又は紛失する。	・情報を秘匿するための［ a ］ ・貸与 PC 及び貸与 USB メモリの安全な持運びに関する注意点の周知	・情報は［ a ］していない。 ・貸与 PC 及び貸与 USB メモリの社外での取扱方法に関する規定はない。
(イ) マルウェアに感染	・持出中に貸与 PC 又は貸与 USB メモリがマルウェアに感染する。 ・マルウェアに感染した貸与 PC 又は貸与 USB メモリで情報を持ち出す。 ・マルウェアに感染した私有 PC で持出情報を扱う。	（表 2 から変更なし）	（表 2 の内容に次を追記） ・私有 PC におけるマルウェアの対策状況を定常的に把握できていない。 ・私有 PC については，インストールできるソフトウェアを会社指定のものだけに制限できていない。 ・私有 PC については，セキュリティパッチの適用は徹底できていない。

表 3 に基づいて，Y 課長と Z 君は，M について検討した案 1 と案 2 を H のための案として読み替えたものを対策候補として検討を進めた。H の場合，⑤案 2 では，（イ）のリスクに対する有効な対策を取ることが困難なので，案 1 の方が有効であると考えられる。(ウ)と(エ)のリスクも検討の上で総合的に判断し，Y 課長と Z 君は，M は案 2，H は案 1 で対応することとした。手順が複数となることで業務効率上の問題が生じた場合は，手順の一本化について後日検討することとした。

Y 課長は，これらを情報システム部長に報告し，了承を得た。また，社長にも概要報告がなされ，了解が得られた。

設問 1　表 21 及び表 3 中の［ a ］並びに本文中の［ b ］，［ c ］について，(1)，(2)に答えよ。

(1) ［ a ］に入れる適切な字句を 3 字以内で答えよ。

(2) ［ b ］，［ c ］に入れる適切な字句の組合せを解答群の中から選び，記号で答えよ。

解答群

	b	c
ア	移転	回避
イ	回避	低減
ウ	低減	移転
エ	低減	回避

設問 2　表 2 中の下線①の持運びに関する注意点を 15 字以内で具体的に述べよ。

設問 3　〔M における情報漏えい対策の検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線②について，被害が大きくなるおそれがある理由を 45 字以内で述べよ。

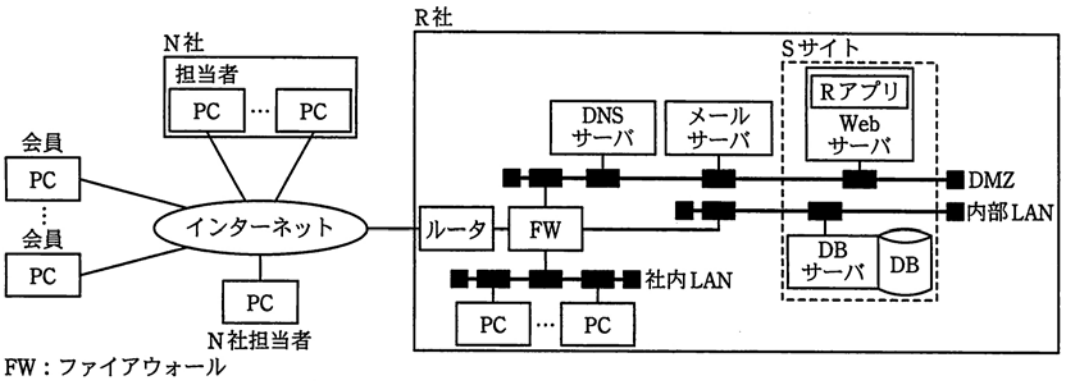
(2) 本文中の下線③とは，どのような運用上の対策か。45 字以内で述べよ。
(3) 本文中の下線④では，何を確認すべきか。 35 字以内で述べよ。

設問 4 〔対策案の見直し〕について，本文中の下線⑤の有効な対策を取ることが困難な理由を 55 字以内で述べよ。

問 4 Web サイトのセキュリティ対策に関する次の記述を読んで，設問 1，2 に答えよ。

R 社は，おもちゃの会員制オークションサイト（以下，S サイトという）を運用し，その販売手数料を主な収入源としている従業員数 40 名のネットオークション会社である。

S サイトは図 1 のとおり，主に Web サーバ及び Web サーバ上で動作する Web アプリケーションであるオークションアプリケーション（以下，R アプリという），並びにデータベース（DB）で構成されている。



FW：ファイアウォール
注記 FW ではドロップログ（通信を拒否したログ）だけを収集している。

図 1 R 社のシステム構成

S サイトのサーバの管理と R アプリの保守は R 社のシステム課が担当しており，社内 LAN からアクセスしている。DB の保守においては，Web サーバにある DB 接続用クライアントツール（以下，DB 接続ツールという）を使って接続する。

一方，HTML ファイルや画像ファイルなどのコンテンツファイルの保守はホームページデザイン会社である N 社に委託している。N 社の担当者には FTP で Web サーバにコンテンツファイルを転送するためのアカウント（以下，CNT-MGR という）が付与されており，N 社内で作成されたファイルを Web サーバに転送している。

R アプリは，Perl で開発されたスクリプトである。R アプリのスクリプトには，DB への接続情報（DB 利用者 ID，パスワード），ビジネスロジック，及び画面表示処理が含まれている。R アプリが DB に接続するときには，DB 接続ツールとは異なる Perl 用の DB 処理モジュールを利用している。DB には，会員データが約 3 万件あり，暗号化されていない状態で格納されている。

S サイトでは，会員のメールアドレスを会員 ID としており，会員は S サイトのログインページで，会員 ID とパスワードを入力してログインする。

R 社のシステム課は K 課長を中心に，会員向けの機能追加を目的として R アプリの改修に取り組んでおり，現在は設計フェーズである。

〔ペネトレーションテストによる現状確認〕

他社のオークションサイトで，会員情報の流出事件が起きたことから，R 社の経営陣は K 課長に S サイトのセキュリティ対策を確認するように指示した。K 課長は現状のセキュリティ対策の有効性を確認するために，セキュリティ専門会社である W 社に，インターネット及び N 社のオフィスからのペネトレーションテスト（以下，P テストという）を依頼した。表 1 は，W 社が報告した P テストの結果である。

表 1　P テストの結果

項番	問題点
V-1	S サイトのログインページで，P テスト用の会員 ID によるログインが何度も失敗したにもかかわらずアカウントがロックされなかった。
V-2	S サイトからいったんログアウトした後に，再びログインせずに，URL を直接指定することで S サイトの会員個人の専用情報ページを閲覧できた。
V-3	Web サーバの HTTP サービスの脆弱性を突いて，Web サーバに侵入できた。
V-4	V-3 の侵入方法によって Web サーバに侵入後，Web サーバ内のファイルを FTP で R 社の外部に送信できた。
V-5	CNT-MGR のパスワードを推測して，Web サーバへの FTP 接続を何度か試行し，最終的に成功した。
V-6	Web サーバへのコンテンツファイル転送時の通信を盗聴して，CNT-MGR のパスワードを窃取できた。
V-7	CNT-MGR で Web サーバにログインした後，Web サーバ内の DB 接続ツールを実行し，DBMS 標準アカウントの初期パスワードで DB に接続できた。

〔セキュリティ対策の検討〕

K 課長は，表 1 の結果を踏まえて対策の検討を行うために，W 社の G 氏に相談した。G 氏は表 1 を見ながら，システム課のメンバから状況を聞いた上で，対策について助言した。次は，検討時の会話である。

K 課長：V-1 の対策としては，ログインページで，3 回連続してログインが失敗したらアカウントをロックし，5 分間は当該会員 ID によるログインを受け付けなくします。また，V-2 の対策としては，ログアウト時に［　a　］処理を実装します。

G 氏　：それでよいでしょう。少し気になることがありますが，後ほど説明します。

K 課長：P テストの時点では Web サーバのセキュリティパッチの適用を忘れていましたが，V-3 と V-4 の対策としては，システム課が DMZ に配置された全サーバに最新のセキュリティパッチを適用するよう徹底します。

G 氏は，サーバへのセキュリティパッチの適用だけでは V-4 の対策として不十分であるので，外部向けの不要な通信を拒否するように FW のフィルタリングルール（以下，FW ルールという）を変更することを提案した。さらに，①FW ルールに違反してファイルを外部送信する試みの有無をシステム課の担当者が調べるための方法についても説明した。

K 課長：なるほど，そうします。V-5，V-6 の対策としては，パスワードを複雑なものに設定し直した上で，コンテンツファイル転送時の認証方法を FTP の認証ではなく SSH のパスワード認証に変更しようと思います。その場合，ログ

インが連続失敗したらアカウントをロックするよう SSH を設定します。しかし，N 社の担当者が N 社以外からもアクセスする必要があるので，アクセス元を IP アドレスで制限できません。アクセス元を限定できないのが不安です。

G 氏　：SSH では，IP アドレス制限に頼らなくても，認証方式を［　b　］にすることによって，更にアクセス者を限定できます。

K 課長：なるほど，そうします。最後に V-7 の対策ですが，現状の Web サーバで CNT-MGR に付与されているファイルアクセス権限は図 2 のようになっています。第三者によって CNT-MGR が不正に使われた場合の対処も必要ですし，N 社の担当者にも DB 内の会員データの閲覧はもちろん DB 接続もさせたくないので，DBMS 標準アカウントの初期パスワードを変更した上で，CNT-MGR からコンテンツファイルの保守には必要のない DB 接続ツールの実行権限を削除します。それから，R アプリで鍵長 256 ビットの AES を使って，会員データを暗号化しようと考えています。その場合，暗号鍵は定数としてスクリプト内に定義します。

・スクリプトファイルに対して，読取り，書込み及び実行が可能である。
・コンテンツファイルに対して，読取り及び書込みが可能である。
・コンテンツ保守に必要なコマンドと，DB 接続ツールの実行が可能である。
（以下，省略）

図 2　CNT-MGR に付与されているファイルアクセス権限

G 氏は，CNT-MGR に付与されているファイルアクセス権限の現状を考慮すると，K 課長が示した対策だけでは②N 社の担当者に会員データを閲覧されてしまう可能性が残ることを説明した。さらに，本来であればコンテンツファイルの確認のために新たに独立したテスト環境を構築し，N 社にはそのテスト環境にだけアクセスさせ，本番環境にはアクセスさせないようにすべきであることを説明した。その上で，テスト環境を用意するまでの③暫定対策を提示した。

G 氏　：先ほどの S サイトへのログインに関する件ですが，多くの会員は，S サイトに登録しているメールアドレスとパスワードの組合せ（以下，認証情報という）と同じものを，ほかの Web サイトでも登録していると思われます。④ほかの Web サイトで大量に盗まれた認証情報が悪用されて S サイトにログイン試行が行われ，結果として幾つかの会員 ID でのログインが成功してしまう可能性があります。V-1 の対策のアカウントロックは一つの会員 ID に対するログイン試行を想定しているので，大量のほかの Web サイトの認証情報を悪用するログイン成功を防ぐことはできません。

K 課長：それは，S サイトの脆弱性ではなく会員のパスワード設定の問題ですが，なりすまして S サイトにログインされた場合には，我々が会員への対応に追われることになるので，何らかの手を打った方がよさそうですね。

G 氏は，下線④のようなログイン試行をできる限り R アプリで検知して遮断するための方法を説明した。こうして K 課長は P テストの結果について対策案をまとめ，経

営陣から承認を得た。その後，対策を順調に終え，無事に新しいRアプリをリリースすることができた。

設問I　Pテストの結果と対策について，(1)～(5)に答えよ。

(1)本文中の［　a　］に入れる適切な処理を解答群の中から選び，記号で答えよ。

解答群

ア　クッキーにパスワードをセットする　　イ　再認証を行う

ウ　セッション情報を破棄する　　エ　ログを採取する

(2)表1中のv-6の対策として，コンテンツファイル転送時に使用するサービスをSSHに変更した際，N社の担当者がコンテンツファイル転送時に使用するコマントを，5字以内で答えよ。

(3)本文中の［　b　］に入れるべき，表1中のV-5の問題を解決できるSSHの認証方式を10字以内で答えよ。

(4)本文中の下線①の，FWルールに違反してファイルを外部送信する試みの有無を調べるための方法を35字以内で具体的に述べよ。

(5)本文中の下線②の可能性について，N社の担当者がスクリプトファイルを悪用して会員データを閲覧するための方法を50字以内で具体的に述べよ。また，本文中の下線③の暫定対策の内容を40字以内で述べよ。

設問2　本文中の下線④に示すログイン試行を，Rアプリで検知して遮断するためには，どのような条件を用いて検知することが適切か。60字以内で述べよ。

解答例

問 1

出題趣旨

堅ろうなプログラムを開発するためにはバッファオーバフロー脆弱性を作り込まないことが重要なポイントである。

本問では，バッファオーバフロー脆弱性の理解と，その対策について問う。特に対策については，脆弱性の発見と修正だけでなく，そもそも脆弱性を作り込まないための仕組みまで踏み込める能力を問う。

設問 1　a　ア
　　b　ウ

設問 2　(1) dst が指し示す領域
　　(2) dst が指し示す領域の残りが 2 バイト以下となった時点で，src にエンコードすべき文字があった場合

設問 3　c　文字列を string クラスとして取り扱っており，領域の境界は処理系が管理することとなる

設問 4　d　文字型の配列
　　e　上限チェック
　　f　代入

問 2

出題趣旨

ソフトウェアライセンスに対する違反行為が，最近，社会問題になっている。

本問では，管理ツールによるソフトウェアの実態把握を通じて，ソフトウェアライセンス，セキュリティパッチ，運用管理に関する知識と対応能力を問う。

設問 1　a　アップグレード
　　b　損害賠償
　　c　著作権

設問 2　遊休ライセンスを全社で有効利用する可能性

設問 3　インストール情報が存在しなくても，実行贋報は存在するから

設問 4　(1) インストール情報に，特定のセキュリティパッチが含まれていない PC を抽出する。
　　(2) 脆弱性が発見されても対処する手段がない，という状況を回避することができる。
　　(3) 異動に伴い不要になったソフトウェアを削除する。

設問 5　ライセンスの利用者と登録者の間で相互けん制が働くから

問 3

出題趣旨

情報セキュリティ対策の立案に当たっては，情報資産の利用状況から想定されるリスクへの対応の有効性確保という観点が必要である。利用状況からは想定されないリスクにだけ対応した対策や，想定されるリスクに対して無効な対策を立案するようなことは避けな

ければならない。
本問では，情報（情報を保存した機器や媒体）の持出しという題材を通して，リスクを考慮して情報セキュリティ対策を立案する能力を問う。

設問 1　(1) 暗号化
(2) イ
設問 2　移動中は肌身離さず持つ。
設問 3　(1) 当該持出時に必要な情報以外に貸与 PC に入っている業務情報も漏えいする可能性があるから
(2) 顧客を訪問する直前に業務情報をアップロードし，ダウンロードされたらすぐに削除する。
(3) アップロードする業務情報が，当該顧客向けの情報であること
設問 4　セキュリティ対策が十分でない可能性のある私有 PC に業務情報をダウンロードすることができてしまうから

問 4

出題趣旨

インターネットに公開する Web システムでは，セッション管理の不備，クロスサイトスクリプティング，SQL インジェクションなどのアプリケーションの脆弱性に加え，アカウント窃取やコンテンツ管理業者による内部不正についての対策も欠かせない。
本問では，インターネットに公開する Web システムにありかちな脆弱性と攻撃手法という題材を通して，これらへのセキュリティ対策を立案する能力を問う。

設問 1　(1) a　ウ
(2) scp　又は　sftp
(3) b　公開鍵認証方式
(4) 定期的に FW のドロツプログを分析し，拒否した通信から調べる。
(5) **閲覧するための方法**　DB に接続して会員データを復号し表示するスクリプトファイルを作成し，実行して閲覧する。
暫定対策の内容　CNT-MGR から全てのスクリプトファイルへのアクセス権限を削除する。

設問 2　一定時間内に同一 IP アドレスから複数の会員 ID でログイン試行し，かつ，一定回数以上認証失敗していること

採点講評

問 1

問 1 では，C++におけるバッファオーバフロー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 3 は，正答率が低かった。図 6 では領域の境界をプログラムで管理する必要がないことは問題中の記述から読み取れる。その上で，なぜ必要がないのか，代わりにどのような仕組みで管理するのかという点を具体的に解答してほしかった。これは類似の脆弱性を

回避するために重要な点であり，確実に理解しておいてほしい。
設問 4 では，開発標準ルールの具体的な記述を問うた。プログラム開発では，脆弱性対策だけでなく品質確保の面からも，開発標準ルールを決めることは重要である。具体的な開発標準ルールなどを参考に学習してほしい。

問 2
問 2 では，ソフトウェア資産管理に関連する情報セキュリティ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 は，正答率が低かった。全社としての調査で初めて把握できる内容を解答してほしかったが，各部門の調査でも把握できるような誤った解答が散見された。
設問 4（2）は，正答率が低かった。セキュリティパッチの提供が終了したソフトウェアを抽出することの意義として，“新たな脆弱性が発見されたら速やかに対処できる”という解答も見られたが，脆弱性が発見されたとしても，開発元からセキュリティパッチは提供されない。このような危険な状況は，直ちに回避する必要がある。
設問 5 は，正答率が低かった。権限の集中による不正行為を防ぐために，“権限分離”又は“相互けん制”という考え方に基づき，ソフトウェアの利用者以外の第三者が登録することを理解してほしかった。

問 3
問 3 では，PC や記憶媒体による情報の社外への持出しを題材として，情報漏えい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 は, 正答率が低かった。PC の持運びに関する注意点を問うているにもかかわらず, 持運び自体を禁止するといった誤った解答が散見された。設問で何か問われているのかを, 落ち着いて把握するようにしてほしい。
設問 3(2)は，正答率が高かったものの，認証やアクセス制限，DMZ の設置による Web サーバ自体の防御といった誤った解答が散見された。これらは，いずれも不正アクセスを防ぐための方法であり，設問で問われている不正アクセス後の被害の拡大防止には寄与しない。各種の対策がどのようなリスクに対して効果をもっているのかを，改めて確認しておいてほしい。
設問 4 は，正答率が低かった。マルウェア対策が困難な理由を問うたが，Web サーバへの感染拡大といったウイルス感染後の事象を述べた誤った解答が散見された。感染後に何か起こるかは，感染対策が困難であることとは直接の関係がないことを理解した上で解答してほしかった。

問 4
問 4 では，Web サイトのセキュリティ対策について出題した。全体として，正答率は低かった。
設問 1(3)は，正答率が低かった。パスワード認証方式の SSH は，活発なブルートフォース攻撃によって危険性が高くなっているので，公開鍵認証方式の理解が不可欠である。
設問 1(4)は，ログを保存するという趣旨だけの誤った解答が多く見受けられた。 FW のドロツプログを分析することで様々なインシデントやその予兆を検知できることを理解しておいてほしい。

設問 1(5)は，正答率が低かった。本来ならば必要のないスクリプトファイルへのアクセス権限を付与することでリスクは増大する。最小権限の原則を改めて意識してほしい。

設問 2 は，ログイン試行の時間，アクセス元，回数に関しては触れていたが，ログイン試行の結果(成功又は失敗)に関する条件が欠けている解答が多く見られた。結果に関する条件を明確にしないで検知しようとすると誤検知が大量に発生してしまうことを覚えておいてほしい。