SC

平成23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〕

選択欄	
2問選択	(問1)
	問2
	(問3)
	問4

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　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1～3に答えよ。

E社は，従業員数100名の自動車部品販売会社であり，販売先は日本各地に散在している。5年前に社内LANを導入した際，営業報告管理システム（以下，Xシステムという）を開発し，社内LAN上で運用を始めた。Xシステムは C++で開発したWebアプリケーション（以下，Xシステムの Web アプリケーションを X-Web アプリという），Webサーバ及びデータベースで構成されている。

〔Xシステムへの新たな要望とその対応〕

これまで営業報告は，その日の営業活動終了後に営業社員が会社に戻り，Xシステムを用いて営業報告書を作成して，更に Xシステム上で営業部長に提出し，必要な場合は口頭によって補足する方法がとられてきた。また，遠方の販売先に出張した場合には電話で報告を行い，後日出社した際に営業報告書を作成して営業部長に提出してきた。

インターネットが普及したことから，会社に戻らなくても出張先で営業報告を行えるようにしてほしいという要望が営業社員から出されていた。さらに，他社との競争も激しくなっていることから，E社としても営業力強化が必要であると経営者が判断し，この要望に対応することになった。具体的には，営業活動の都度，インターネットを利用して報告することで，営業部長が営業活動の状況を逐次把握し，必要に応じて指示ができるようにすることにした。情報システム部のB君が X-Web アプリの改修を担当することになった。

なお，Xシステムのデータベースは現状のものを使うことにした。現状の X-Web アプリは，社外からインターネット経由でアクセスすることを想定しておらず，脆弱(ぜいじゃく)性対策も行われていない。

〔代表的な脆弱性への対策方法の確認〕

社内の他の Web アプリケーションは Java で開発されている。B君は，X-Web アプリを Java で書き直す案もあると考え，先輩の D主任に相談した。D主任から，“一般的には Java が良いと言われているよ”という助言をもらったが，B君は，C++と Java のそれぞれを採用するメリットとデメリットを比較することにした。B君は，X-Web

アプリの中で SQL インジェクションの脆弱性がある関数を一つ見つけたので，C++ と Java での対策方法を比較してみることにした。その関数 getReport の仕様を図 1 に示す。

```
void getReport(sql::Connection *con, string user, string day)
  概要：営業報告を表示する。
  引数：次の三つの引数がある。
        con － データベースにアクセスするためのコネクションオブジェクト
        user － 利用者画面からの入力を基に作成した営業社員名
        day － 利用者画面からの入力を基に作成した，表示したい営業報告の日付情報
  処理：営業社員 user が日付 day の営業活動として登録した全ての営業報告を，データベースへのコネクションオブジェクト con を用いて取得し，その営業報告を表示するための HTML を出力する。
  備考：この関数を呼び出す前処理として，この関数に引き渡す引数の値は，サーバ上の設定情報や利用者画面の入力データから取り出され，セットされている。その他実行に必要な環境も準備されている。
  （省略）
```

図 1　getReport の仕様（抜粋）

SQL インジェクション対策前の C++コードを図 2 に示す。

```
（#include などは省略）
void getReport(sql::Connection *con, string user, string day) {
   string query = "SELECT report FROM reports WHERE user = '" + user + "'";
   query += " AND day = '" + day + "'";
   sql::Statement *stmt;
   sql::ResultSet *res;
   cout << "<HTML><BODY>";
   try {
      stmt = con->createStatement();
      res = stmt->executeQuery(query);
      cout << "user = '" << user << "'<BR>";
      cout << "day = '" << day << "'<BR>";
      while(res->next()) {
         string rep = res->getString("report");
         cout << "report = '" << rep << "'<BR>";
      }
      delete res;
      delete stmt;
   } catch(const Exception& e) {
      cout << "ERROR!";
   }
   cout << "</BODY></HTML>";
}
```

図 2　SQL インジェクション対策前の C++コード

B 君は，このコードに対し，SQL インジェクション対策を行ってみた。この対策は，［ a ］を用いて SQL 文を組み立てるというものである。対策後の C++コードを図 3 に示す。

```
（#include などは省略）
void getReport(sql::Connection *con, string user, string day) {
   string query = "SELECT report FROM reports WHERE user = ? AND day = ?";
   sql::PreparedStatement *pstmt;
   sql::ResultSet *res;
   cout << "<HTML><BODY>";
   try {
      pstmt = con->prepareStatement(query);
      pstmt->setString(1, user);
      pstmt->setString(2, day);
      res = pstmt->executeQuery();
      cout << "user = '" << user << "'<BR>";
      cout << "day = '" << day << "'<BR>";
      while(res->next()) {
         string rep = res->getString("report");
         cout << "report = '" << rep << "'<BR>";
      }
      delete res;
      delete pstmt;
   } catch(const Exception& e) {
      cout << "ERROR!";
   }
   cout << "</BODY></HTML>";
}
```

図 3　SQL インジェクション対策後の C++コード

B 君は，図 3 の C++コードと同様の対策を実施した同じ仕様のプログラムを Java で作成してみた。そのコードを図 4 に示す。

```
（import などは省略）
public void getReport(Connection con, String user, String day) {
   String query = "SELECT report FROM reports WHERE user = ? AND day = ?";
   PreparedStatement ps = null;
   ResultSet rs = null;
   out.write("<HTML><BODY>");
   try {
      ps = con.[ b ](query);
      ps.setString(1, user);
      ps.setString(2, day);
      rs = ps.executeQuery();
      out.write("user = '" + user + "'<BR>");
      out.write("day = '" + day + "'<BR>");
      while (rs.next()) {
         String rep = rs.getString("report");
         out.write("report = '" + rep + "'<BR>");
      }
      ps.close();
   } catch (Exception e) {
      out.write("ERROR!");
   }
   out.write("</BODY></HTML>");
}
```

図4　SQLインジェクション対策を実施したJavaコード

この後，図2～4のコードにはSQLインジェクション以外にも①代表的な脆弱性の原因となるコードが含まれていることが分かり，B君は，[c]を[d]処理するという対策を図3と図4のコードにそれぞれ追加した。

次に，B君は，インターネット上の信頼できるWebサイトを調査し，図5に示すような，脆弱性につながるC++の特性の解説を見つけた。

C++は，メモリ内容への柔軟なアクセスが可能である。ただし，プログラムに次のような問題があっても言語処理系自体では防止できないので，プログラマ自身がこれを回避するコーディングをする必要がある。

脆弱性の要因となる問題

- データを転記する際のメモリ領域の境界チェック漏れ
- [e]による誤った領域へのアクセス
- データへの[e]と，関数への[e]を混同したアクセス
- 整数演算での桁あふれ

上記問題が引き起こす代表的な脆弱性

- [f]
- 整数オーバフロー

図5　脆弱性につながるC++の特性の解説（抜粋）

B 君は，この C++の特性に対して，Java の特性を図 6 に整理した。

Java が提供しているメモリ内容へのアクセス手段は限定的であり，メモリマネジメントは言語処理系の一部である Java VM が行う。長時間連続動作させる場合には [g] の実行による応答性への影響を考慮する必要がある。

図 6　Java の特性

B 君は，以上の調査結果を踏まえ，X-Web アプリの改修でどちらの言語を採用するかを検討するために，両言語を採用する場合のメリット，デメリットを整理した。両言語の比較表を表 1 に示す。

表 1　両言語の比較表（抜粋）

言語	メリット	デメリット
C++	・X-Web アプリで使用している言語なので，改修作業量が少なくなる。 ・処理が高速である。	・利用可能な既存のアプリケーションフレームワークが少ない。 ・特に [f] に関係した脆弱性対策が必要である。
Java	・利用可能な既存のアプリケーションフレームワークが豊富である。 ・多くの環境で動作可能である。	・X-Web アプリで使用していない言語なので，改修作業量が多くなる。 ・[g] への対応が必要な場合がある。

〔その後の状況〕

今回の対応では，C++を用いた場合に [f] 対策が多くの部分で必要となることが確認されたので，表 1 を基に B 君は Java を採用することを提案した。その提案を受けて，情報システム部内で検討を重ね，情報システム部長が Java を採用することを承認した。言語を変更したことで X-Web アプリを書き直すことになったが，B 君はこの改修を無事に行うことができた。

設問1　図2～4のコードについて，(1)～(6)に答えよ。

(1) 図2でSQLインジェクションの原因となるコーディング部分が複数ある。そのコーディング部分に書かれた変数名を，コード上から選び，全て答えよ。

(2) 本文中の［　a　］に入れる適切なプログラミング技法を12字以内で答えよ。

(3) 図4中の［　b　］に入れる適切な文字列を英字で答えよ。

(4) 本文中の下線①の代表的な脆弱性を解答群の中から選び，記号で答えよ。

解答群

ア　クロスサイトスクリプティング

イ　クロスサイトリクエストフォージェリ

ウ　コマンドインジェクション

エ　セッションフィクセーション

(5) 本文中の［　c　］，［　d　］について，［　d　］に入れる適切なプログラミング技法を10字以内で，その技法の対象を明確に示す［　c　］に入れる適切な字句を20字以内で答えよ。

(6) 上記(5)の技法の対象となる変数が図3中に複数ある。その変数名を図3中から選び，全て答えよ。

設問2　図5中の［　e　］に入れる適切な字句を6字以内で，図5中，表1中及び本文中の［　f　］，並びに図6中及び表1中の［　g　］に入れる適切な字句を，それぞれ12字以内で答えよ。

設問3　図6及び表1には，脆弱性を狙った［　f　］攻撃がC++では問題となるのに，Javaでは問題とならない根本的な理由が具体的に記述されていない。図5の内容を踏まえて，根本的な理由であるJavaの言語仕様上の特徴を20字以内で述べよ。

問2　販売システムへの機能追加設計に関する次の記述を読んで，設問1～5に答えよ。

A社は，部品製造を営む従業員数250名の中堅会社である。インターネットを介した販売システム（以下，Nシステムという）を利用し，企業向けに自社製品を販売している。Nシステムは，A社の販売部が3年前に開発し，運用している。

Nシステムの利用者は，利用者ID（以下，UIDという）を保有しており，ブラウザからインターネット経由でNシステムにアクセスし，ログイン画面でUID名とパスワードを入力することによってログインした上で，製品の在庫確認，注文を行う。Nシステムを利用する企業（以下，契約企業という）は，Nシステムの利用契約時に，利用責任者を1名登録する。利用責任者は，ヘルプデスクに対して，UIDの新規登録の他，UIDの削除，パスワード初期化，サスペンド解除を申請できる。申請の際は，利用責任者が申請書を電子メール（以下，メールという）でヘルプデスクに送付する。

Nシステムでは，UIDに対して表1に示す属性を定義し，その値をログイン処理に利用している。NシステムのUID及びログイン処理に関する，セキュリティ要件は図1のとおりである。

表1　UIDに定義している属性（Nシステムの設計書からの抜粋）

属性名	属性の定義
password	ソルトを付加したパスワードの，ハッシュ関数 [a] によるハッシュ値を表す。
mailaddr	利用者のメールアドレスを表す。
status	当該UIDによるログインの可否を表す。 0：ログイン可能　　1：ロックアウト状態　　2：サスペンド状態
temppass	パスワードが仮パスワードか否かを表す。 0：仮パスワードではない　　1：仮パスワードである
fails	パスワード間違いによる連続したログイン失敗回数を表す。
lastlogin_t	ログインに成功した直近の時刻を表す。
lockout_t	ロックアウトが発生した直近の時刻を表す。

(ア) UIDは，複数の利用者での共用を禁止する。
(イ) UID名は，英数字6文字で構成する。
(ウ) パスワードは10文字以上とし，英字，数字，記号を，それぞれ1文字以上含める。Nシステムにはパスワード変更ページが準備されており，ログイン中の利用者はパスワードを変更できる。
(エ) UIDの新規登録時，及び利用者がパスワードを忘れた場合のパスワード初期化時には，UIDに対して仮パスワードを設定する。仮パスワードは十分に長いランダムな文字列とし，ヘルプデスク担当者又はNシステムが決定する。UIDに仮パスワードが設定されている状態を仮パスワード状態と呼ぶ。仮パスワード状態のUIDでNシステムにログインすると，ログイン処理の中で強制的にパスワード変更ページへ遷移する。このとき，利用者はパスワードを変更しない限り，Nシステムへのログインは完了しない。
(オ) ログイン時に，パスワードを連続して5回間違えた場合，そのUIDはログイン不可能になる。このUIDの状態をロックアウト状態と呼ぶ。ロックアウト状態は，60分以上経過した後の最初のログイン時に解除される。連続したログイン失敗回数は，ログイン成功時，パスワード初期化時，及びロックアウト解除時に，0回にリセットされる。ロックアウト状態のUIDに対してパスワード初期化を行うと，ロックアウトが解除される。
(カ) 90日間ログインに成功していないUIDは，ログイン不可能になる。このUIDの状態をサスペンド状態と呼ぶ。サスペンド状態は，契約企業の利用責任者からのサスペンド解除申請によってだけ解除でき，利用者自身では解除できないようにする。
(キ) 利用者のブラウザとNシステムの間の通信には，SSLを用いる。

図1　Nシステムの UID 及びログイン処理に関する，セキュリティ要件

ヘルプデスクでは，図2に示す運用手順でUIDを管理している。ヘルプデスクによるUIDの設定変更時には，表2に示す値をUIDの属性に設定する。サスペンド設定は，バッチ処理で行う。バッチ処理は，毎日00:00に実行し，現在時刻がlastlogin_tの値から90日以上経過した全てのUIDに対して，表2の設定変更(e)に示す各属性値を設定する。

また，Nシステムのログイン画面で，UID名とパスワードが入力された場合のログイン処理の流れを図3に示す。ログイン成功時とロックアウト発生時に，利用者にメールで通知することで，不正ログイン及びその試行を利用者が把握できるようにしている。

1. 利用責任者からの申請書がメールで送付された際に，メールヘッダに記載された送信者メールアドレスが契約時に登録された利用責任者のものであることを確認する。さらに，利用契約時に登録された利用責任者の電話番号に電話をして，メール送信者の本人確認を行った後に，申請された設定変更を 3 営業日以内に行う。利用責任者が，他の契約企業の UID に対する設定変更を申請した場合は，申請を受け付けない。
2. 申請に基づく設定変更は，ヘルプデスク専用の UID 管理画面で行う。UID 管理画面では，設定変更 (a)～(c) に対応し，UID の各属性を表 2 に示す各値に設定する。設定変更 (d) の場合は，UID を削除する。UID 管理画面は，契約企業に公開しておらず，ヘルプデスク担当者だけが利用できる。
3. 2. のうち，UID の新規登録申請，又はパスワード初期化申請では，図 1 のセキュリティ要件を満たす仮パスワードをヘルプデスク担当者が決定し，UID に対して設定する。設定した仮パスワードは，ヘルプデスク担当者が利用責任者に電話し，読み上げて通知する。
4. 設定変更の完了後は，利用責任者に完了通知メールを送付する。
5. サスペンド状態の UID に対しては，UID の削除とサスペンド解除の申請だけを受け付け，それ以外の申請は受け付けない。

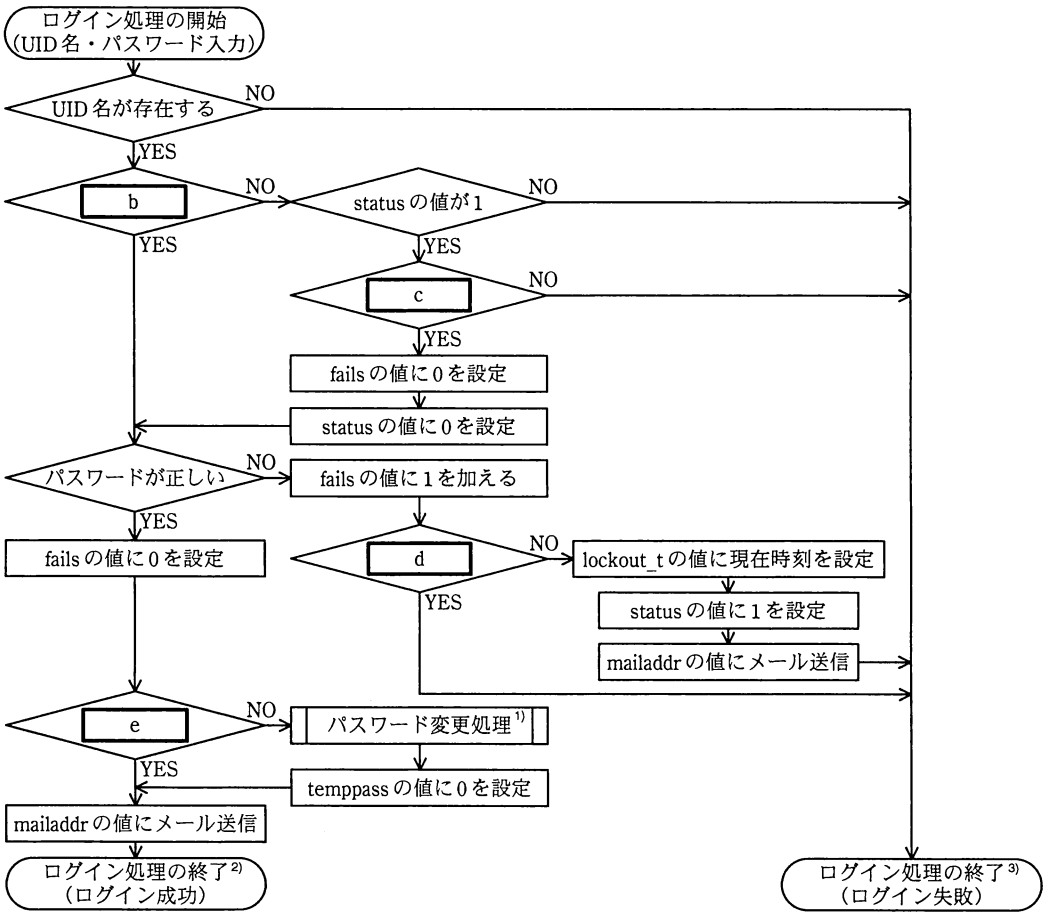
図 2　UID 管理に関するヘルプデスクの運用手順

表 2　設定変更時に UID の属性に設定する値

設定変更項目	設定変更内容	設定変更対象となる属性					
		password	mailaddr	status	temppass	fails	lastlogin_t
設定変更 (a)	新規登録	仮パスワード	メールアドレス	0	1	0	現在時刻
設定変更 (b)	パスワード初期化	仮パスワード	−	0	1	0	−
設定変更 (c)	サスペンド解除	−	−	0	−	−	現在時刻
設定変更 (d)	削除	UID を削除する					
設定変更 (e)	サスペンド設定	−	−	2	−	−	−

注記 1　表中の“−”は，値を変更しないことを意味する。表中に記載がない属性の値は変更されない。

注記 2　表中の“仮パスワード”はソルトを付加した仮パスワードのハッシュ値を，“メールアドレス”は利用者のメールアドレスを，また“現在時刻”は設定変更時の現在時刻を，それぞれ表す。



注 1) パスワード変更処理では，利用者にパスワード変更ページを表示し，新しいパスワードが図1のセキュリティ要件を満たす場合に，password の値を更新する。パスワード変更処理の流れ図は省略する。

2) ログイン処理の終了（ログイン成功）では，lastlogin_t の値に現在時刻を設定する。

3) ログイン処理の終了（ログイン失敗）では，ログイン失敗というメッセージを表示し，ログイン画面を再度表示する。

図3　Nシステムのログイン処理の流れ（Nシステムの設計書からの抜粋）

〔契約企業からの要望〕

Nシステムの利用者数と利用頻度が増えるにつれて，利用者がパスワードを忘れた場合のパスワード初期化に要する期間を短縮してほしいという要望が，利用責任者からヘルプデスクに多く寄せられるようになった。パスワード初期化の申請から完了までの期間に利用者がNシステムを利用できないことで，契約企業によっては業務に悪影響が発生していることが背景にあった。

販売部では，Nシステムの利便性向上を目的として，利用責任者とヘルプデスクを介さずに，利用者自身がパスワード初期化を短時間で行えるパスワード初期化機能をNシステムに追加することを決定した。

販売部のH部長は，新人のF君に対して，G主任の支援を受け，パスワード初期化機能を設計するように指示した。また，H部長は，アプリケーションへの不用意な機能追加が原因で，セキュリティ上の問題が発生する事例が一般的に少なくないことを挙げ，現状のNシステムの仕様を十分に理解した上で検討を進め，社内の有識者によるレビューを受けるようF君とG主任に伝えた。

〔パスワード初期化機能の設計〕

F君は，図1に示すセキュリティ要件に従って，Nシステムのパスワード初期化機能を検討した。F君が作成した設計案を，図4に示す。

- Nシステムにパスワード初期化の申請ページを準備する。Nシステムのログイン画面に，申請ページへのリンクを設定する。
  次の(i)～(v)に示す手順に従って，仮パスワードを発行する。
  (i) 利用者は，申請ページにブラウザでアクセスし，自身のUID名を入力する。
  (ii) 入力されたUID名が存在する場合は，プログラムがパスワード取得ページのURL（以下，取得ページURLという）を発行し，利用者にメールで通知する。取得ページURLには十分に長いランダムな文字列を含める。入力されたUID名が存在しない場合は，取得ページURLは発行されない。
  (iii) 利用者が，メールで通知された取得ページURLにブラウザでアクセスすると，プログラムが仮パスワードを発行し，ブラウザに表示する。このとき，UIDの各属性に対して，表2の設定変更(b)に示す値を設定する。
  (iv) パスワード初期化の完了通知メールを，利用者に送付する。完了通知メールには仮パスワードは記載しない。
  (v) 一度アクセスされた取得ページURLは無効にする。また，取得ページURLを発行後，10分以内にアクセスがない場合は，取得ページURLを無効にする。
- 利用者のブラウザと，申請ページ及びパスワード取得ページとの間の通信には，SSLを用いる。
- 発行する仮パスワードは，図1のセキュリティ要件を満たし，ヘルプデスク担当者でも推測できない文字列とする。

図4　パスワード初期化機能の設計案

G主任はF君の設計案に対して，次の点を指摘した。

指摘1：この設計案では，ある状態のUIDに対してパスワード初期化を行った場合に，図1に示すセキュリティ要件が満たされなくなる。

F君はG主任の支援を受け，指摘1の問題点に対して図4の設計案を修正した。その後，社内の有識者による設計案のレビューが実施された。そのレビューでは，指摘1とは別に，次の2点が指摘された。

指摘2：今回設計したパスワード初期化機能によって仮パスワードを発行した場合に

は，図1のセキュリティ要件のうち，(エ) に記されているログイン処理中の強制的なパスワード変更ページへの遷移は不要ではないか。

指摘3：現行のヘルプデスクによるパスワード初期化運用と比較した場合に，図4の設計案に示す (i)～(v) の手順には，攻撃者に不正に仮パスワードを取得されるリスクがある。

指摘2については，販売部での検討の結果，今回の機能追加においては図1のセキュリティ要件を変更しないという判断に基づき，指摘対象となったログイン処理中の強制的なパスワード変更ページへの遷移は残すこととした。

指摘3については，今回予定していた開発予算を考慮すると，これ以上のセキュリティ強化は困難であると販売部では判断した。また，設計したパスワード初期化機能の利用を契約企業単位で選択できるようにした。その後，販売部では，F君の設計に基づいてパスワード初期化機能の開発に着手した。

設問1　表1中の［　a　］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　AES　　イ　RC4　　ウ　RSA　　エ　SHA-256

設問2　図3中の［　b　］～［　e　］に入れる適切な字句を，表1中の属性名を用いて，［　b　］，［　d　］，［　e　］は15字以内で，［　c　］は30字以内で，それぞれ答えよ。

設問3　指摘1について，(1)，(2) に答えよ。

(1)　図1のセキュリティ要件がどのように満たされなくなるか。45字以内で具体的に述べよ。

(2)　上記 (1) の問題点の発生を防止するためには，パスワード初期化機能にどのような修正が必要か。表1中の属性名を用いて，35字以内で述べよ。

設問4　指摘2の内容が指摘された理由を，図2のヘルプデスクによる運用手順との違いを踏まえて，30字以内で述べよ。

設問5　指摘3について，攻撃者が不正に仮パスワードを取得する手口を45字以内で述べよ。

問3　プロキシ経由のWebアクセスに関する次の記述を読んで，設問1～3に答えよ。

T社は従業員数3,000名の食品卸売業を営む企業であり，全国10都市に支社を展開している。T社ではデータセンタ（以下，T社DCという）内に各種サーバを設置し，本社と各支社間を広域イーサネットで接続している。

T社の従業員には1台ずつPCが貸与されている。T社では広域イーサネットとは別にインターネットも利用しており，インターネットへのアクセス管理ルールでは，業務目的に限りインターネット上のWebサイト（以下，インターネットサイトという）へのアクセスを許可すること，並びに各従業員のインターネットサイトへのアクセス状況を記録するために，アクセスログを取得すること及びインターネットサイトに向けて送信された内容をログとして取得することを定めている。

T社本社及び各支社のLANに設置したPCからは直接インターネットにアクセスできないように，ルータ及びファイアウォールを設定している。ブラウザからインターネットサイトへのアクセスは，T社DCに設置したプロキシを経由して行う。T社のネットワーク構成の概要を図1に示す。

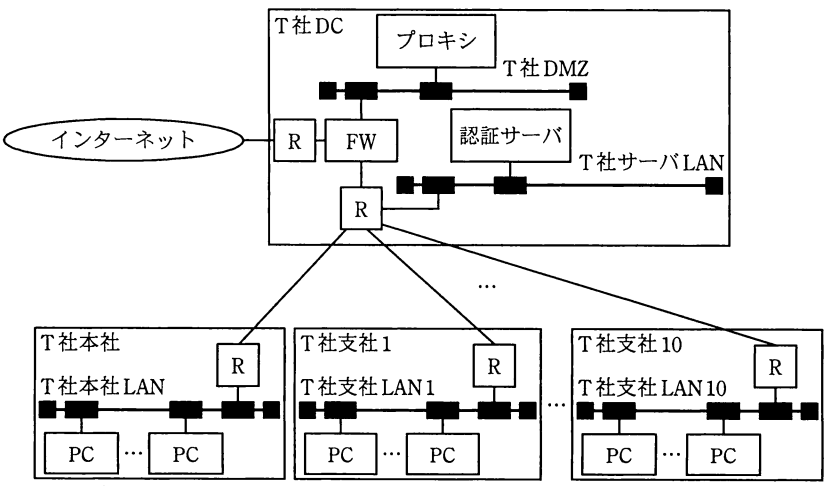


図1　T社のネットワーク構成（概要）

プロキシにはU社のプロキシ製品（以下，Uプロキシという）が使われている。

T社がUプロキシで利用している機能の利用目的を図2に示す。

(1) 利用者認証機能
利用目的：インターネットサイトにアクセスする従業員を識別し認証する。
ブラウザがHTTPリクエストのProxy-Authorizationヘッダに付与し，Uプロキシに送信した認証情報を，各従業員に一意に割り当てられた利用者IDとパスワードに照らして，アクセスした利用者を識別し認証する。
(2) アクセスログ取得機能
利用目的：従業員によるインターネットサイトへのアクセスについて，HTTPリクエストごとに，次の項目を取得する。
アクセス日時，アクセス元のIPアドレス，利用者ID，リクエストライン（HTTPメソッド，URL，HTTPプロトコルのバージョン），インターネットサイトのIPアドレス，受信データサイズ，インターネットサイトからのレスポンスコード
(3) 送信内容取得機能
利用目的：インターネットサイトにデータが送信された場合（POSTリクエスト，PUTリクエストの利用時など）に，その送信内容を取得する。
(4) フィルタリング機能
利用目的：インターネットサイトへのアクセスを業務目的だけに制限する。
HTTP通信ではブラックリスト方式，HTTPS通信ではホワイトリスト方式で，インターネットサイトのホストのFQDNに基づいたアクセス規制をする。
(5) ウイルスチェック機能
利用目的：インターネットサイトからのウイルス感染やインターネットサイトへのウイルス送信を防止する。
送受信データ内のウイルスをチェックする。

図2 T社がUプロキシで利用している機能の利用目的（抜粋）

〔HTTPS通信の制限〕

T社では，①インターネットへのアクセス管理ルールに基づき，インターネットサイトへのHTTPS通信によるアクセスを原則として禁止している。業務上，HTTPS通信が必要なインターネットサイトはホワイトリストに登録し，Uプロキシのフィルタリング機能を用いて，アクセスを許可している。

HTTPS通信を許可するホワイトリストは，定期見直しを情報システム部で四半期ごとに行っている。この見直しにおいて，インターネットで電子ファイルをやり取りできるファイル共有サービスのURLが登録されていたことが判明した。このURLのインターネットサイトにアクセスしていた従業員に確認したところ，顧客との間で電子ファイルをやり取りしていたことが分かった。業務上，同インターネットサイトを利用する必要があるので，アクセスは禁止できないが，同インターネットサイトを利用すれば社外に情報を持出し可能なこと，また，電子ファイルを不正に社外へ持ち出された場合に，当該電子ファイルを特定できないことが懸念として浮上した。そのため，情報システム部のS部長は，インターネットサイトへのアクセスに対するプロキシでのログ取得方式の改善を検討するよう，情報セキュリティ担当のK主任に指示した。

〔新たなプロキシ製品導入の検討〕

K 主任は，HTTPS 通信時にプロキシで詳細なログを取得するためには，U プロキシとは異なる仕組みをもつプロキシ製品を導入する必要があると考えた。そこで，U プロキシを，HTTPS 通信を一旦復号する機能をもつ L 社のプロキシ製品（以下，L プロキシという）で置き換えることが可能かどうかを確認することにした。

U プロキシを利用した HTTPS 通信では，暗号化された通信路をブラウザと Web サーバ間で確立する。U プロキシを利用した場合の HTTPS 通信を図 3 に示す。

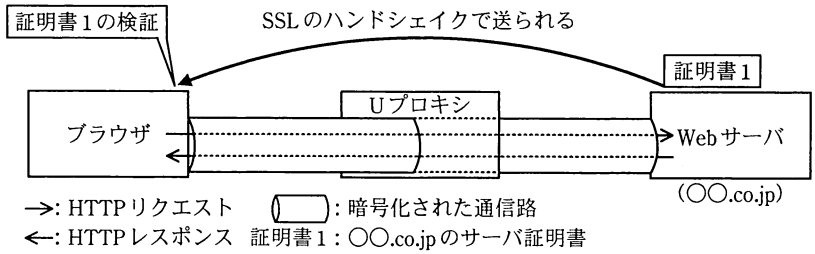


図 3　U プロキシを利用した場合の HTTPS 通信

一方，L プロキシを利用した HTTPS 通信では，ブラウザと L プロキシ間，及び L プロキシと Web サーバ間において，それぞれ独立の暗号化された通信路を確立する。L プロキシは証明書 1 を受け取ると，ブラウザには転送せずに，自身で証明書 1 の検証を行う。次に，L プロキシは認証局として証明書 1 と同じコモンネームのサーバ証明書（以下，証明書 2 という）を新たに作成し，ブラウザに送る。L プロキシを利用した場合の HTTPS 通信を図 4 に示す。

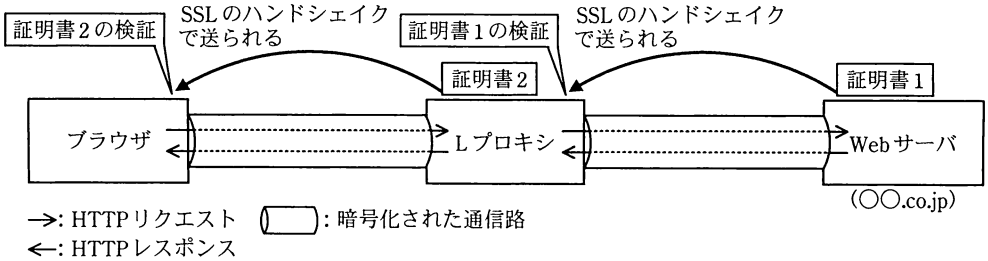


図 4　L プロキシを利用した場合の HTTPS 通信

ブラウザがLプロキシ経由でWebサーバとHTTPS通信を行うとき，ブラウザが暗号化してLプロキシに送信したデータはLプロキシで一旦復号される。Lプロキシでアクセスログの取得，送信内容の取得及びウイルスチェックが行われた後，送信データは再度暗号化されて，Webサーバに送信される。受信データについてもLプロキシで同様の処理が行われる。

〔HTTPS通信時の安全性の確認〕

K主任は，確認したLプロキシの仕様をS部長に説明した。次は，K主任とS部長の会話である。

S部長：HTTPS通信でWebサーバのサーバ証明書の正当性を確認しないまま，ブラウザがアクセスを継続すると，偽サイトに誘導された場合でなくても，［ a ］攻撃を受けて，通信を盗聴される可能性があるので，アクセスを許可してはいけない。そこで，まずLプロキシを利用したHTTPS通信時のサーバ証明書の検証について確認したい。Lプロキシでは二つのサーバ証明書を利用しているが，②ブラウザは証明書2の検証において，証明書2の正当性を確認できないのではないか。

K主任：ご指摘のとおり，事前に何の準備もしなかった場合は，証明書2の正当性を確認できません。証明書2の正当性を確認できるようにするためには，事前にブラウザで［ b ］必要があります。

S部長：証明書1の正当性はどこで確認するのかね。

K主任：証明書1の正当性はLプロキシで検証します。証明書1の正当性を確認できなかった場合のWebサーバへのアクセスの可否は，Lプロキシで設定できます。

S部長：なるほど。サーバ証明書の検証については問題なさそうだね。

情報システム部における検討結果を踏まえ，T社ではLプロキシを採用する方針とし，Lプロキシの導入に向けた動作検証を行うことにした。

設問1　T社におけるインターネットサイトへのアクセスについて，(1)～(3)に答えよ。

(1) 本文中の下線①について，T社がHTTPS通信によるアクセスを原則として禁止しているのは，どのような理由からか。20字以内で述べよ。

(2) 図2について，HTTPS通信を行うことで利用目的を達成できなくなるものはどれか。図2中の項番(1)～(5)から選び，全て答えよ。

(3) ブラウザのURL入力欄に次のURLを入力したときに，ブラウザがプロキシに最初に送信するHTTPメッセージのリクエストラインはどれか。解答群の中から選び，記号で答えよ。

入力したURL：https://○○.co.jp/index.html

解答群

ア　CONNECT ○○.co.jp:443 HTTP/1.1

イ　GET ○○.co.jp:443/index.html HTTP/1.1

ウ　POST ○○.co.jp:443/index.html HTTP/1.1

エ　SSL ○○.co.jp:443 HTTP/1.1

設問2　HTTPS通信時の安全性の確認について，(1)，(2)に答えよ。

(1) 本文中の［　a　］に入れる用語を答えよ。

(2) サーバ証明書の検証においてブラウザが確認すべき内容のうち，［　a　］攻撃のような攻撃への対策となるものを二つ挙げ，それぞれ35字以内で述べよ。

設問3　Lプロキシについて，(1)～(3)に答えよ。

(1) 本文中の［　b　］に入れる，事前にブラウザで実施することは何か。40字以内で述べよ。

(2) 本文中の下線②について，上記(1)を実施しないとブラウザが証明書2の正当性を確認できないのはなぜか。40字以内で述べよ。

(3) 図4中の証明書2について，Lプロキシ自身のサーバ証明書を利用するのではなく，Webサーバのサーバ証明書と同じコモンネームのサーバ証明書をLプロキシが新たに作成する必要があるのはなぜか。40字以内で述べよ。

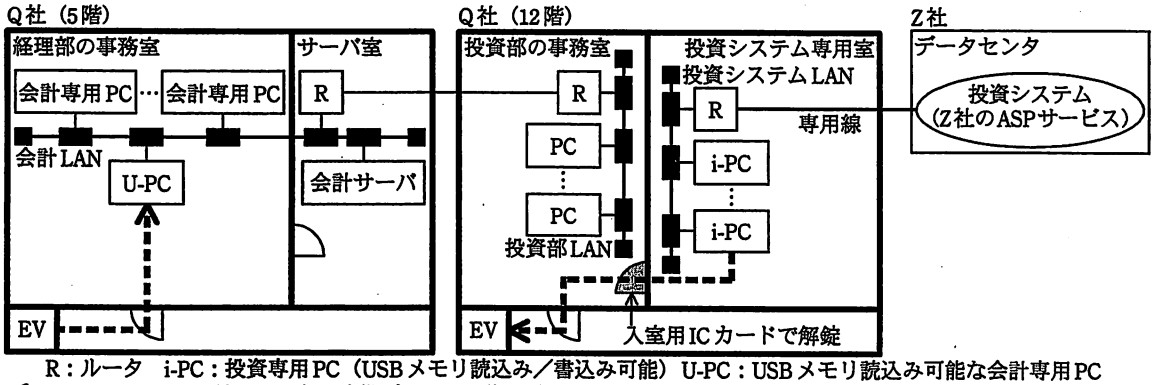
問4　財務報告に係る内部統制に関する次の記述を読んで，設問1～4に答えよ。

Q社は，従業員数500名の保険業を営む未上場会社であり，上場を目指している。2008年4月1日以後に開始する事業年度からは，財務報告の信頼性の確保を目的に，上場会社に対して内部統制報告書の作成が義務付けられた。そこで，Q社は，本年度から内部統制報告書を作成することにした。Q社は，内部統制報告書作成に際して，財務報告に係る内部統制のうち，特に情報システムに関する統制が有効であるかを評価するため，コンサルティング会社Y社にIT全般統制に関する状況の確認及び不備の指摘を依頼した。

Q社の資産運用を行う投資部には，投資部長の他に50名が所属しており，うち20名が投資システムを用いた業務を行う従業員（以下，投資担当者という）で，残りはその他の業務を行う従業員（以下，事務担当者という）である。投資部は12階にある。

現在利用中の投資システムは，証券会社を親会社にもつ情報システム会社のZ社がASPサービスとして提供しているものであり，Q社と専用線で接続されている。また，端末として投資専用PCが20台ある。多額の資金を運用することから，投資専用PCは，Q社の投資部LANとは分離されており，入室用ICカードでの入室管理が行われている投資システム専用室内に設置されている。入室及び投資専用PCの利用は，投資担当者20名及び投資部長1名だけに許可されている。

経理部は，投資部と同じビルの5階にあり，会計専用PCで会計サーバにアクセスして業務を行っている。投資部では，市場の取引終了後，財務報告のために，投資システムの特定のデータ（以下，会計連携データという）を抽出し，経理部にUSBメモリで運搬し会計サーバに入力している。経理部及び投資部関連の情報システムを，図1に示す。



R：ルータ　i-PC：投資専用PC（USBメモリ読込み／書込み可能）　U-PC：USBメモリ読込み可能な会計専用PC
<--- ：USBメモリを利用した会計連携データの運搬経路　　EV：エレベータ

図1　経理部及び投資部関連の情報システム

〔情報セキュリティガイドライン〕

投資部は，投資システム利用のための情報セキュリティガイドライン（以下，情報セキュリティガイドラインという）を作成し，情報セキュリティ上の事故が起こらないようにしている。情報セキュリティガイドラインを図2に示す。

（省略）
5. 投資システムの利用者IDの発行
(1) 新規の投資担当者は，申請書にアクセス権やその他の必要事項を記入し，投資部長の承認後，投資システム担当者に提出する。
(2) 投資システム担当者は，Z社に利用者IDの登録を依頼する（利用者IDの登録は，Z社だけが行う）。
(3) 投資システム担当者は，発行された利用者IDの情報をZ社から受け取り，申請した投資担当者に通知する。
6. 投資システムの利用者IDの削除
（省略）
7. 入室用ICカードの発行
（省略）
8. 入室用ICカードの返却
（省略）
9. 投資システムの利用者IDと入室用ICカードの発行対象
投資システムの利用者IDと入室用ICカードの発行対象は表1のとおりである。
（省略）
13. USBメモリの利用許可
投資部でのUSBメモリの利用は，次の三つの業務だけに認め，それ以外には許可しない。
(1) 分析のための投資システムのデータをダウンロードし，データを投資部の事務室のPCに移すこと
(2) 会計連携データを経理部の事務室に運搬し，会計サーバに入力すること
(3) 監査用データの提出を求められたときに，データ提出用に使用すること
14. USB管理簿
USBメモリの貸出しは，USB管理簿を使い，USB管理者が管理する。
なお，USB管理簿には，USB番号，利用者氏名，貸出日時，返却日時，目的，提出先名称の欄がある。USB管理簿の提出先名称の欄は，監査用データの提出時に利用する。
15. USBメモリの利用
(1) USBメモリの利用者は，利用前に，USB管理簿に必要項目を記入の上，USB管理者へ申請する。
(2) USB管理者は，USB管理簿の内容を確認の上，USB番号を記入し，USBメモリを貸し出す。
(3) USBメモリの利用者は，USBメモリ内のデータを消去してUSB管理者に返却する。
(4) USB管理者は，データ消去を確認し，USB管理簿に返却日時を記入の上，USBメモリを保管場所に格納する。
（省略）
21. 会計連携データの運搬
(1) 会計連携データの抽出担当者（以下，抽出担当者という）は，USBメモリの貸出しを受けて，i-PCから投資システムにアクセスし，その日の会計連携データを抽出し，USBメモリに保存する。
(2) 抽出担当者は，会計連携データ管理簿に当日の運搬を行う事務担当者の氏名と運搬依頼日時を記入し，USBメモリと会計連携データ管理簿を事務担当者に手渡す。
(3) 事務担当者は，USBメモリと会計連携データ管理簿を経理部まで運搬し，経理部の担当者に手渡す。
(4) 経理部の担当者は，経理部にあるU-PCを使用して，会計連携データを直ちに会計サーバに入力する。
(5) 経理部の担当者は，会計連携データ管理簿に自分の氏名と入力完了日時を記入し，事務担当者にUSBメモリとともに手渡す。
(6) 事務担当者は，USBメモリと会計連携データ管理簿を投資部まで運搬し，抽出担当者に返却する。
22. （以下，省略）

図2 情報セキュリティガイドライン

表1　投資システムの利用者 ID と入室用 IC カードの発行対象

役割名称	役割の説明	投資システムの利用者 ID	入室用 IC カード
投資部長	投資部のマネジメント。	あり	あり
投資担当者	投資システムでの株式売買を担当。	あり	あり
抽出担当者	会計連携データの抽出を担当。投資担当者の中の 1 名。会計連携データ管理簿を管理。	あり	あり
事務担当者	投資システムを用いない業務を担当。	なし	なし
USB 管理者	USB メモリの貸出し，返却のための USB 管理簿の管理を担当。事務担当者の中の 2 名。	なし	なし
投資システム担当者	Z 社との窓口を担当。投資担当者の中の 1 名。投資部の情報セキュリティ担当も兼務。抽出担当者とは異なるメンバ。	あり	あり

〔会計連携データの運搬〕

投資部では，情報セキュリティガイドラインに従い，USB 管理者から，投資部用に用意してある 5 個の USB メモリの一つの貸出しを受けて，市場の取引終了後の 16 時頃に，会計連携データの抽出を行い，終業前に経理部へ運搬する。

〔Y 社による IT 全般統制に関する状況の確認〕

Y 社は，Q 社の IT 全般統制に関する状況を確認する一環として，JIS Q 27002:2006 を参考に，情報セキュリティ対策の予備調査用の状況チェックリストを作成した。状況チェックリストの大項目を図 3 に，図 3 中の“7. [a]”に関する状況チェックリストを表 2 に示す。

1. 情報セキュリティポリシ	2. 情報セキュリティのための組織
3. 資産の管理	4. 人的資源のセキュリティ
5. 物理的及び環境的セキュリティ	6. 通信及び運用管理
7. [a]	8. 情報システムの取得，開発及び保守
9. 情報セキュリティインシデントの管理	10. 事業継続管理
11. 遵守	

図3　状況チェックリストの大項目

表2　状況チェックリスト（抜粋）

項番	チェック項目		
	名称	概要	詳細
7.2.1	利用者登録	（省略）	（省略）
7.2.2	特権管理	（省略）	（省略）
7.2.3	利用者パスワードの管理	（省略）	（省略）
7.2.4	利用者のアクセス権のレビュー	（省略）	（省略）
7.3.1	パスワードの利用	（省略）	（省略）
7.3.2	無人状態にある利用者装置	（省略）	（省略）
7.3.3	[b]・クリアスクリーンポリシ	書類及び取外し可能な電子記憶媒体に対する[b]ポリシ，並びに情報処理設備に対するクリアスクリーンポリシを適用しているか。	(1) 重要な業務情報は，必要のない場合，特に部屋が無人状態のときには，施錠して保管をしているか。 (2) サーバ及びPCは，離席時にはログオフ状態にしておくか，若しくはパスワード，[c]又は類似の利用者認証機構を使用した[d]で保護しているか。また，使用していないときには，施錠，パスワード，又は他の対策で保護しているか。 (3) 重要な業務情報を含む文書は印刷後，[e]いるか。

Y社のコンサルタントは，状況チェックリストを基にしたアンケートを使って，投資システム担当者に予備調査を行った。その上で，現場の状況の確認及び投資システム担当者へのヒアリングも行い，他の確認結果と併せて，IT全般統制の状況についての報告をまとめた。

〔IT全般統制に関する指摘〕

Y社から，投資システムのIT全般統制の状況に関して報告があった。その中で，情報セキュリティ対策について，次の3点の指摘があった。

指摘1：会計連携データを運搬中のUSBメモリ内のデータ保護対策がとられておらず，財務情報の正確性確保の観点からみて不十分である。

指摘2：投資システム利用中の離席時に，不正利用の防止のために行うべき手続が定められておらず，操作者特定の観点からみて不十分である。

指摘3：投資システムへのアクセス権の付与状況を管理するために必要な，アクセス権付与状況の一覧表が作成されておらず，アクセス権管理の観点からみて不十分である。

〔Z 社の統制状況〕

指摘 3 のアクセス権管理については，情報セキュリティガイドラインに項目を追加し，アクセス権の付与状況を一覧表で管理できるようにした。ただし，投資システムのアクセス権管理については，Z 社の統制状況についても確認の必要な項目が存在する。しかし，Z 社は，データセンタへの取引先の立入りを認めていない。そこで，Q 社は，Z 社に対して，①Q 社としての確認が必要な項目を含む，Z 社の統制状況に関する報告書を［ f ］の立場の専門家に作成してもらい，提出するよう依頼した。

その後，Z 社から報告書が提出され，Q 社は，Y 社のコンサルタントからの指摘に対応して，無事に上場の準備を整えることができた。

設問 1　本文中及び図 3 中の［ a ］に入れる適切な字句を答えよ。

設問 2　表 2 中の［ b ］～［ e ］に入れる適切な字句を，［ b ］，［ c ］については 10 字以内で，［ d ］については 15 字以内で，［ e ］については 20 字以内で答えよ。

設問 3　〔IT 全般統制に関する指摘〕について，(1)～(3) に答えよ。

(1) 指摘 1 は，どのようなリスクに対する対策の不備を指摘しているか。解答群の中から一つ選び，記号で答えよ。

解答群

ア　DDoS　　イ　ウイルス感染　　ウ　改ざん

エ　盗難　　オ　漏えい

(2) 指摘 1 について，どのような技術的対策が効果的か。30 字以内で述べよ。

(3) 指摘 1 について，悪意をもった事務担当者による不正行為を防止できない。このためにどのような管理的対策が効果的か。情報セキュリティガイドラインの改定を前提として 30 字以内で述べよ。

設問 4　〔Z 社の統制状況〕について，(1)，(2) に答えよ。

(1) 本文中の［ f ］に入れる適切な字句を 10 字以内で答えよ。

(2) 本文中の下線①について，図 2 中の 5. (2) に関して確認が必要な，具体的な項目を一つ挙げ，30 字以内で述べよ。

7. 退室可能時間に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，黒鉛筆及びシャープペンシル（B 又は HB），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，目薬
    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。