SC

平成25年度　春期
情報セキュリティスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

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. **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。**
4. 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2
選択方法	1問選択

5. 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，**生年月日欄**に**受験票の生年月日**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。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **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。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 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。
   (5) 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2を選択した場合の例〕

選択欄	
1問選択	問1
	問2 ○

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　業務パッケージの開発に関する次の記述を読んで，設問1～4に答えよ。

U社は，従業員数100名のソフトウェア開発会社で，以前は受託開発を主に行っていたが，数年前から業務パッケージの開発も手がけるようになり，業績を伸ばしている。今回，新たに美容室向けの自社製品として，表1の機能を備えた美容室管理システム（以下，HSSという）を開発することが決まり，M専務が開発責任者になった。M専務は，美容室がHSSを運用することは難しいと考え，U社がHSSを運用し，インターネット経由で美容室へサービスを提供する，いわゆるSaaS型の商品とすることにした。また，美容室間の情報の独立性を高めるために，美容室ごとに仮想サーバを用意し，その上でHSSを運用することにした。

表1　HSSの機能

機能名称	機能概要
顧客管理	美容室の顧客の氏名，住所，注文履歴などの管理
予約管理	来店予約の管理
従業員管理	美容室の従業員の氏名，役職，勤務シフト，勤怠などの管理
売上管理	売上の管理

〔機能要件の定義〕

M専務は，HSSの要件定義から詳細設計までを担当するグループ（以下，Sグループという）を編成し，T主任をリーダに任命した。Sグループは，HSSの想定契約先に関する調査などを行い，機能要件の定義を行った。そのうち，顧客管理と予約管理に関する機能要件は，それぞれ図1，図2のとおりである。

・顧客データは，データベース内に格納する。
・顧客データのメンテナンスは，美容室内の管理端末から美容室の従業員が行う。ただし，一部の顧客データについては，Webサイトで顧客が変更できる。
・顧客データのうち，顧客から取得するものは次のとおりとする。取得は対面で行う。
　- 氏名，住所，生年月日，性別，電話番号，メールアドレス，美容室に対する要望
・顧客データのうち，システムが付与するものは次のとおりとする。
　- 顧客ID，パスワードの初期値
・顧客は，Webサイトで，自分の顧客データを閲覧できる。
（以下，省略）

図1　顧客管理の機能要件

・美容室の従業員は，美容室内の管理端末から，全ての顧客の来店予約ができる。
・顧客は，Web サイトで，自分の来店予約ができる。
・予約データはデータベース内に格納し，内容は次のとおりとする。
　- 予約年月日，予約時刻，担当美容師，顧客 ID，注文メニュー，美容室へのメッセージ
・予約に当たっては，担当美容師を指定する。
・予約に当たっては，注文メニューを指定する。
（以下，省略）

図２　予約管理の機能要件

なお，HSS では美容室の従業員及び顧客の利用時に認証を行う。

〔システム・ソフトウェア要件定義〕

S グループは，システム方式設計及びソフトウェア要件定義を開始し，まず図 3 のとおり，ソフトウェア構成を決定した。

なお，図 3 中の太線枠内が，今回 HSS として開発する Web アプリケーションである。

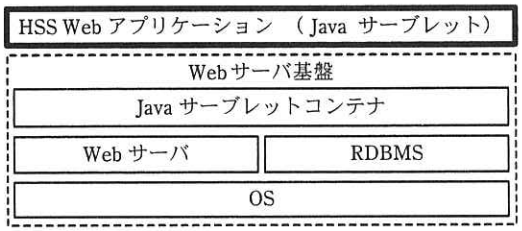


図３　ソフトウェア構成

〔リスクアセスメント〕

M 専務は，HSS では，美容室が顧客から取得した個人情報を含む情報資産を取り扱うことから，情報の漏えいや滅失の可能性を評価するためにリスクアセスメントを実施し，その結果に基づきソフトウェア要件の中でセキュリティ仕様を定めることにした。この作業を，ソフトウェア要件定義の他のタスクと並行して行うために，S グループとは別のグループ（以下，R グループという）を編成した。

R グループでは，次の(1)～(3)の手順に従ってリスクアセスメントを実施した。

(1) 表2のように，美容室における情報資産の分類を定義した。

(2) 表3のように，HSSで取り扱う情報資産を特定し，情報セキュリティの3要素に照らして情報資産の分類を行った。

(3) 各情報資産に対する脅威と脆弱性を特定し，それぞれについてリスク分析を行い，その結果を取りまとめた。そのうち，顧客データに対する結果を表4に示す。

表2　美容室における情報資産の分類の定義

分類	定義
Ⅰ	・美容室の顧客に直接被害が及ぶ。 ・美容室の存続に関わるほどの被害が発生する。
Ⅱ	・従業員や取引先に直接被害が及ぶ。 ・美容室の営業に支障が発生する。
Ⅲ	・直接的には大きな被害や影響は発生しない。

表3　HSSで取り扱う情報資産（抜粋）

情報資産	概要	a に係る分類	完全性に係る分類	可用性に係る分類
顧客データ	顧客の氏名，顧客ID，パスワードなど	Ⅰ	Ⅰ	Ⅰ
予約データ	予約状況に関する情報	Ⅰ	Ⅰ	Ⅰ
従業員データ	従業員の氏名，従業員ID，パスワードなど	Ⅱ	Ⅱ	Ⅰ
売上データ	販売状況に関する情報	Ⅲ	Ⅱ	Ⅲ

表4　顧客データに対するリスク分析の結果（抜粋）

リスクNo.	脅威	脆弱性	被害	発生確率[1]	深刻度[2]	対応要否[3]
1	インターネット経由のHSSへの不正アクセス	b	情報漏えい	高	高	要
2		Webアプリケーションのセキュリティホール	情報漏えい	中	高	要
3		Webサーバ基盤のセキュリティホール	情報漏えい	中	高	要
4		脆弱な認証とアクセス権管理の仕組み	情報漏えい	低	高	要
5	美容室従業員による物品持ち去り	物品管理の不備	情報へのアクセス不能	低	中	不要
6		c	情報へのアクセス不能	低	中	不要
7	美容室従業員による不正アクセス	b	情報漏えい	中	高	要
8		脆弱な認証とアクセス権管理の仕組み	情報漏えい	低	高	要
9	不正プログラムによる管理端末からの情報窃取	ウイルス対策ソフトの停止	情報漏えい	低	中	不要
10		未知のウイルスへの未対応	情報漏えい	低	中	不要

注[1]　脅威が脆弱性を悪用し被害が発生する確率
[2]　被害が発生した場合の，被害の深刻さ
[3]　リスクに対応するために，HSSに管理策を施す必要性の有無

〔セキュリティ仕様の決定〕

R グループはリスク分析の結果から，Web アプリケーションに係るセキュリティ仕様と HSS の運用管理に関する要件を取りまとめた。そのうち，顧客管理機能に関するセキュリティ仕様を表5に，HSS の運用管理に関する要件を表6に示す。

表5　顧客管理機能に関するセキュリティ仕様（抜粋）

機能	仕様	リスク No.[1)]
顧客の認証	・顧客の認証用パスワード設定時に，次の条件を強制する。 － 長さ：8 文字以上 － 文字種：英字，数字，記号の 3 種類の全てを含む。 － 別途指定する禁止文字列を含まない。 ・パスワードの入力を所定回数連続して誤った場合，［ d ］	1，4
美容室の従業員の認証	・美容室の従業員の認証では，顧客の認証と同様の認証に加えて，クライアント証明書によるクライアント認証を実装する。	7，8
Web 画面入出力	・Web 画面からの入力については，全て値チェックを行う。 ・Web 画面の出力時には，エスケープ処理を行う。 （以下，省略）	［ e ］
権限管理	・次のロールを定義し，最小権限を与える。 － HSS のシステム管理者 － HSS のデータ管理者 － 美容室の従業員 － 顧客	1，4，7，8

注[1)]　リスク No.は，表 4 中のリスク No.のうちで，該当するものを示す。

表6　HSS の運用管理に関する要件（抜粋）

適用対象	要件	リスク No.[1)]
インターネットからのアクセスを受け付ける回線	・ファイアウォールを設置し，最小限のアクセスだけを許可する。 ・IPS を設置し，不正アクセスの検出と，自動遮断を行う。 ・Web アプリケーションファイアウォールを設置し，不正な HTTP アクセスを遮断する。	［ f ］
インターネットからのアクセスを受け付ける Web サーバ	・［ g ］	3

注[1)]　リスク No.は，表 4 中のリスク No.のうちで，該当するものを示す。

R グループは，検討したセキュリティ仕様と運用管理に関する要件を M 専務に報告し，その承認を受けた。

〔予約管理機能の不具合〕

その後，HSS の開発は順調に進み，予約管理機能のうち，顧客が操作する画面の機能テストを開始した。予約管理機能の画面遷移を図 4 に示す。

画面1　ログイン

顧客 ID　[　　]
パスワード　[　　]
[ログイン]

・顧客 ID とパスワードを入力して，“ログイン”ボタンを押す。
・ログインが成功したら，メインメニュー（画面省略）が表示される。
・メインメニューで予約を選択すると，予約日選択画面（画面省略）が表示される。
・予約日選択画面で予約希望日を選択すると，画面 2 が表示される。

画面2　予約状況

4/22(月)	10:00	10:30	11:00	11:30
美容師 A	○	○	○	○
美容師 B	○	○	○	×
美容師 C	×	○	×	○

[予約日選択画面へ戻る]

注記 12:00 以降の予約枠も表示されるが，この図では省略している。

・各予約枠内で，○は仮予約状態又は空き状態を，×は予約済状態を示す。
・○を選択すると，サーブレット“WakuClick”が呼び出される。
・その予約枠が空き状態であれば仮予約状態とした後に，画面 3 が表示される。
・予約枠が仮予約状態の場合，仮予約の有効期間（10 分間）を確認し，有効期間を過ぎていれば，この顧客の仮予約に置き換えた後に，画面 3 が表示される。有効期間内の場合は，予約失敗の画面（画面省略）が表示される。

画面3　本予約

予約日時：　4/22(月)　11:00　美容師 B

注文メニュー　[　　▽]
美容室への
メッセージ　[　　]

[予約する]

・注文メニュー項目は，所定の選択肢から一つを選択する。
・美容室へのメッセージ項目は，400 字まで自由に入力できる。
・“予約する”ボタンを押すと，サーブレット“KakuteiClick”が呼び出されて予約確定になり，画面 4 が表示される。

画面4　予約確定

ご予約ありがとうございました。予約内容は以下のとおりです。下記のメールアドレス宛てに予約確定メールをお送りしました。

氏名	○○ ○○ 様
メールアドレス	yyyyyy@xxxx.zzz
予約日時	4/22(月) 11:00
担当美容師	美容師 B

[戻る]

・予約確定の画面が表示される。
・“戻る”ボタンを押すと，メインメニューに戻る。

図 4　予約管理機能の画面遷移（抜粋）

機能テストの結果，複数の予約を同時に処理した場合，画面上では正常に予約が完了したように見えるにもかかわらず，データベースには反映されていないことがあるという不具合が発見された。不具合の原因と思われるプログラムは，図 5，図 6 のとおりである。また，データベースのテーブルは，図 7，図 8 のとおりである。

```
 1: package jp.co.u_sha.hssystem;
 2:
 3: import java.io.IOException;
 4: import javax.servlet.ServletException;
 5: import javax.servlet.http.*;
 6: import java.sql.Connection;
 7: import java.sql.PreparedStatement;
 8: import java.sql.ResultSet;
 9: import java.util.Date;
10:
11: public class WakuClick extends HttpServlet {
12:     （省略）〔init メソッド内に適切な初期化処理を記述〕
13:
14:     static final int RSV_AKI = 0;
15:     static final int RSV_KARI = 1;
16:     static final int RSV_KAKUTEI = 2;
17:     static final long TIMEOUT_KARI = 600000;
18:
19:     protected void doPost(HttpServletRequest request, HttpServletResponse response) throws
    ServletException, IOException {
20:         Connection conn;
21:         PreparedStatement psSel, psUp;
22:
23:         （省略）〔DriverManager から Connection インスタンスを取得し，その参照を conn に代入する〕
24:         psSel = conn.prepareStatement("SELECT * FROM rsvList WHERE rsvDate=? AND rsvTime=? AND
    Biyoshi=?");
25:         psUp = conn.prepareStatement("UPDATE rsvList SET Status=?, CustID=?, Messages=?, Menu=?,
    LastUpdate=? WHERE rsvDate=? AND rsvTime=? AND Biyoshi=?");
26:
27:         // サーブレットのセッション情報から，顧客 ID 情報を取得する
28:         HttpSession session = request.getSession(false);
29:         if (session == null) {
30:             （省略）〔ログイン未処理のエラーの HTML 出力を行って終了する〕
31:         }
32:         String loginUserID = (String)session.getAttribute("userID");  // ログイン時の顧客 ID
33:         // 選択された予約枠の情報を取得する
34:         String rsvDate = request.getParameter("rsvDate");  // 予約枠（予約年月日）
35:         String rsvTime = request.getParameter("rsvTime");  // 予約枠（予約時刻）
36:         String rsvBiyoshi = request.getParameter("Biyoshi");  // 予約枠（担当美容師）
```

図 5　サーブレット “WakuClick”

```
37:          （省略）〔前出の四つの変数の入力値チェックを行う〕
38:          （省略）〔入力値チェックで問題があったら，エラーの HTML 出力を行って終了する〕
39:
40:          // 選択された予約枠の予約状況を参照する
41:          psSel.setString(1, rsvDate); psSel.setString(2, rsvTime); psSel.setString(3, rsvBiyoshi);
42:          ResultSet rs = psSel.executeQuery();
43:          rs.next();
44:          long lastDateTime = rs.getLong("LastUpdate");
45:          // 現在の時刻を取得する
46:          long nowDateTime = new Date().getTime();
47:          // 既に仮予約状態であった場合，仮予約の最終更新日時を確認し，TIMEOUT_KARI 経過後なら空きにする
48:          int rsvStatus = rs.getInt("Status");
49:          if (rsvStatus == RSV_KARI) {
50:              if ((nowDateTime - lastDateTime) > TIMEOUT_KARI) {
51:                  rsvStatus = RSV_AKI;
52:              }
53:          }
54:          // 予約状況が空きであることを確認し，仮予約処理を行う
55:          if (rsvStatus == RSV_AKI) {
56:              psUp.setInt(1, RSV_KARI); psUp.setString(2, loginUserID); psUp.setString(3, "");
57:              psUp.setString(4, ""); psUp.setLong(5, nowDateTime);
58:              psUp.setString(6, rsvDate);
59:              psUp.setString(7, rsvTime); psUp.setString(8, rsvBiyoshi);
60:              psUp.executeUpdate();
61:              （省略）〔図 6 の処理に引き継ぐために，選択した予約枠の情報をサーブレットのセッション情報に保存する〕
62:              （省略）〔画面 3 の HTML 出力を行う〕
63:          } else {
64:              （省略）〔予約失敗の画面の HTML 出力を行う〕
65:          }
66:          （省略）〔後処理を行う〕
67:      }
68:      （省略）〔その他の必要なメソッド〕
69: }
```

注記 1 SQL 例外を含め，例外処理については省略している。省略した部分で必要とするクラスに関わる import の記述も省略している。

注記 2 （省略）〔･･･〕は，その位置に〔 〕内に示す処理が記述されているが，省略していることを示す。

図 5　サーブレット“WakuClick”（続き）

```
 1: package jp.co.u_sha.hssystem;
 2:
 3: import java.io.IOException;
 4: import javax.servlet.*;
 5: import javax.servlet.http.*;
 6: import java.sql.Connection;
 7: import java.sql.PreparedStatement;
 8: import java.sql.ResultSet;
 9: import java.util.Date;
10:
11: public class KakuteiClick extends HttpServlet {
12:     （省略）〔init メソッド内に適切な初期化処理を記述〕
13:     static final int RSV_AKI = 0;
14:     static final int RSV_KARI = 1;
15:     static final int RSV_KAKUTEI = 2;
16:
17:     protected void doPost(HttpServletRequest request, HttpServletResponse response) throws
   ServletException, IOException {
18:         Connection conn;
19:         PreparedStatement psSel, psUp;
20:
21:         （省略）〔DriverManager から Connection インスタンスを取得し，その参照を conn に代入する〕
22:         psSel = conn.prepareStatement("SELECT * FROM rsvList INNER JOIN custMaster ON
   rsvList.CustID=custMaster.CustID WHERE rsvDate=? AND rsvTime=? AND Biyoshi=?");
23:         psUp = conn.prepareStatement("UPDATE rsvList SET Status=?, CustID=?, Messages=?, Menu=?,
   LastUpdate=? WHERE rsvDate=? AND rsvTime=? AND Biyoshi=?");
24:
25:         // サーブレットのセッション情報から，選択された予約枠の情報を取得する
26:         HttpSession session = request.getSession(false);
27:         if (session == null) {
28:             （省略）〔ログイン未処理のエラーを表示して終了する〕
29:         }
30:         String rsvDate = (String)session.getAttribute("Date");  // 予約枠（予約年月日）
31:         String rsvTime = (String)session.getAttribute("Time");  // 予約枠（予約時刻）
32:         String rsvBiyoshi = (String)session.getAttribute("Biyoshi");  // 予約枠（担当美容師）
33:         String loginUserID = (String)session.getAttribute("userID");  // ログイン時の顧客 ID
34:         // 本予約画面で入力された情報を取得する
35:         String serviceMenu = request.getParameter("Menu");  // 選択されたメニュー
36:         String toShop = request.getParameter("Message");  // 入力されたメッセージ
37:         （省略）〔前出の六つの変数の入力値チェックを行う〕
38:         （省略）〔入力値チェックで問題があったら，エラーの HTML 出力を行って終了する〕
39:         // 指定日時の予約状況を参照する
40:         psSel.setString(1, rsvDate); psSel.setString(2, rsvTime);
41:         psSel.setString(3, rsvBiyoshi);
42:         ResultSet rs = psSel.executeQuery();
43:         rs.next();
```

図 6　サーブレット “KakuteiClick”

```
44:         int rsvStatus = rs.getInt("Status");
45:         String rsvUserID = rs.getString("CustID");
46:         // 現在の時刻を取得する
47:         long nowDateTime = new Date().getTime();
48:         // 予約状況が仮であり，自分の予約であることを確認する
49:         if (rsvStatus == RSV_KARI && rsvUserID.equals(loginUserID)) {
50:             // 予約状況を予約確定に変更する
51:             psUp.setInt(1, RSV_KAKUTEI); psUp.setString(2, loginUserID);
52:             psUp.setString(3, toShop); psUp.setString(4, serviceMenu);
53:             psUp.setLong(5, nowDateTime); psUp.setString(6, rsvDate);
54:             psUp.setString(7, rsvTime); psUp.setString(8, rsvBiyoshi);
55:             psUp.executeUpdate();
56:             psSel.setString(1, rsvDate); psSel.setString(2, rsvTime);
57:             psSel.setString(3, rsvBiyoshi);
58:             rs = psSel.executeQuery();
59:             （省略）〔rs 内のデータを基にして図 4 の画面 4（予約確定）の HTML 出力を行う〕
60:         } else {
61:             （省略）〔予約失敗画面の HTML 出力を行う〕
62:         }
63:         （省略）〔後処理を行う〕
64:     }
65:     （省略）〔その他の必要なメソッド〕
66: }
```

注記 1 SQL 例外を含め，例外処理については省略している。省略した部分で必要とするクラスに関わる import の記述も省略している。

注記 2 （省略）〔･･･〕は，その位置に〔 〕内に示す処理が記述されているが，省略していることを示す。

図 6 サーブレット“KakuteiClick”（続き）

rsvList[予約リスト]（rsvDate[予約年月日]，rsvTime[予約時刻]，Biyoshi[従業員 ID]，CustID[顧客 ID]，Status[予約状態]，Menu[注文メニュー]，Messages[美容室へのメッセージ]，LastUpdate[最終更新日時]）

custMaster[顧客マスタ]（CustID[顧客 ID]，Name[氏名]，Address[住所]，Birth[生年月日]，Gender[性別]，Tel[電話番号]，Mail[メールアドレス]，Password[パスワード]，LastUpdate[最終更新日時]）

注記 表記ルールは次のとおり。下線は，主キーを表す。
テーブル名[注釈]（列名 1[注釈]，列名 2[注釈]，列名 3[注釈]，…，列名 n[注釈]）

図 7 主なテーブルの構造

・rsvList テーブルには，毎月最初の営業日に，翌々月の予約枠に相当する行が全て空き状態として追加される。
・Status に“0”が設定されている行は，空き状態を表す。その場合，CustID には空文字列が設定される。
・Status に“1”が設定されている行は，仮予約状態を表す。その場合，CustID には仮予約を行った顧客の顧客 ID が設定される。
・Status に“2”が設定されている行は，予約済状態を表す。その場合，CustID には予約を行った顧客の顧客 ID が設定される。
・Biyoshi には，顧客が指定した美容師の従業員 ID が設定される。
・ある行のいずれかの列に更新があった場合，その時刻を LastUpdate に設定する。時刻の単位はミリ秒であり，LastUpdate の型は long 型である。
・LastUpdate には初期値として“0”が設定される。

図 8　予約リストテーブルの仕様

不具合の発見を受けて，図 5 及び図 6 について，顧客 α と顧客 β がそれぞれのブラウザから操作を行うことを想定して，ソースコードレビューを行った。

その結果，顧客 α と顧客 β が，画面 2 で空き状態であった同一の予約枠をほぼ同時に選択した場合，表 7 に示す順序で各処理が完了すると，顧客 α の仮予約がデータベースに反映されないことが確認できた。

表 7　仮予約が無効になる処理の順序

順序	対象の顧客	処理
1	α	図 5 の 42 行目
2	β	図 5 の [h] 行目
3	[i]	図 5 の [j] 行目
4	[k]	図 5 の [ℓ] 行目

さらに，①空き状態であった予約枠を，顧客 α が画面 2 で選択して画面 3 に進むのと並行して，同一の予約枠を顧客 β が画面 2 で選択した場合，表 8 に示す順序で各処理が完了すると，顧客 β の個人情報が顧客 α の画面 4 に表示されてしまうことが確認できた。

表 8　個人情報の漏えいにつながる処理の順序

順序	対象の顧客	処理	備考
1	α	図 5 の 60 行目	
2	α	図 6 の 42 行目	順序 1 の処理が完了し，10 分以上経過してから実行される。
3	β	図 [m] の [n] 行目	
4	α	図 [o] の [p] 行目	
5	β	図 [q] の [r] 行目	
6	α	図 6 の 58 行目	

〔予約管理機能における不具合の修正〕

S グループのリーダとしてソースコードレビューに参加していた T 主任は，この不具合を修正するために，executeUpdate メソッドで UPDATE 文を実行したとき，更新した行数が戻り値になることに着目した。そして，図 5 の 25 行目のパラメタ付き SQL 文の WHERE 句を修正した上で，図 5 の 60 行目の executeUpdate メソッドの実行時に異常の発生を検知する仕組みを提案した。この提案に基づき修正されたプログラムは図 9 のとおりである。

```
1～23: （省略）〔図 5 の 1～23 と同じ〕
24:         psSel = conn.prepareStatement("SELECT * FROM rsvList WHERE rsvDate=? AND rsvTime=? AND
    Biyoshi=?");
25:         psUp = conn.prepareStatement("UPDATE rsvList SET Status=?, CustID=?, Messages=?, Menu=?,
    LastUpdate=? WHERE rsvDate=? AND rsvTime=? AND Biyoshi=? AND CustID=? AND [ s ] ");
26:
27～46: （省略）〔図 5 の 27～46 と同じ〕
47:         int rsvStatus = rs.getInt("Status");
48:         String rsvCustID = rs.getString("CustID");
49:         if (rsvStatus == RSV_AKI) {
50:             // 予約状況が空きであることを確認し，仮予約処理を行う
51:             （省略）〔予約リストを適切に更新し，仮予約処理を行う〕
52:         } else if (rsvStatus == RSV_KARI && ((nowDateTime - lastDateTime) > TIMEOUT_KARI)) {
53:             // 既に仮予約状態であっても，TIMEOUT_KARI 経過後なら，自分の仮予約に変更する
54:             psUp.setInt(1, RSV_KARI); psUp.setString(2, loginUserID); psUp.setString(3, "");
55:             psUp.setString(4, ""); psUp.setLong(5, nowDateTime);
56:             psUp.setString(6, rsvDate);
57:             psUp.setString(7, rsvTime); psUp.setString(8, rsvBiyoshi);
58:             psUp.setString(9, rsvCustID); [ t ] ;
59:             if (psUp.executeUpdate() == [ u ] ) {
60:                 （省略）〔図 6 の処理に引き継ぐために，選択した予約枠の情報をサーブレットのセッション情報に保存する〕
61:                 （省略）〔画面 3 の HTML 出力を行う〕
62:             } else {
63:                 （省略）〔予約失敗画面の HTML 出力を行う〕
64:             }
65:         } else {
66～71: （省略）〔図 5 の 64～69 と同じ〕
```

注記 1 SQL 例外を含め，例外処理については省略している。
注記 2 下線は，修正した部分を表す。
注記 3 （省略）〔…〕は，その位置に〔 〕内に示す処理が記述されているが，省略していることを示す。

図 9　修正されたサーブレット“WakuClick”

〔販売の開始〕

U 社はその後も HSS のテストを続け，更にいくつかの不具合を発見し，プログラムの修正を行った。その結果，テストを完了し，予定どおりに発売日を迎えることができた。発売後，HSS は順調に契約数を伸ばしており，U 社の業績向上に寄与している。

設問1　〔リスクアセスメント〕について，(1)，(2) に答えよ。

(1)　表3中の［ a ］に入れる適切な字句を答えよ。

(2)　表 4 中の［ b ］，［ 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　管理端末の保守体制の不備　　イ　推測可能なパスワード

ウ　耐震性能の不足　　エ　データセンタの施錠管理不良

オ　美容室の施錠管理不良　　カ　防火体制の不備

設問2　〔セキュリティ仕様の決定〕について，(1)～(4) に答えよ。

(1)　表5中の［ d ］に入れる適切な字句を 30 字以内で述べよ。

(2)　表5中の［ e ］に入れる適切なリスク No.を一つ答えよ。

(3)　表6中の［ f ］に入れる適切なリスク No.を二つ答えよ。

(4)　表6中の［ g ］に入れる適切な字句を 40 字以内で述べよ。

設問3　予約管理機能の不具合について，(1)～(4) に答えよ。

(1)　表 7 を完成させるために，［ h ］～［ ℓ ］に入れる適切な字句又は数字を答えよ。

(2)　表 8 を完成させるために，［ m ］～［ r ］に入れる適切な数字を答えよ。

(3)　図 9 を完成させるために，［ s ］～［ u ］に入れる適切な文字列を答えよ。

(4)　本文中の下線①の事象をテストにおいて再現させるための方法を 60 字以内で具体的に述べよ。

設問4　今回のような予約管理機能の不具合を未然に防止するためには，データベースを利用した Web アプリケーションの開発における規約が必要である。特に，データベースから読み込んだデータの更新処理に必要な規約について，Web アプリケーションの特性を考慮した上で，80 字以内で述べよ。

問2　技術情報の管理に関する次の記述を読んで，設問1～5に答えよ。

W社は，従業員数3,000名の機械部品メーカである。東京に本社，国内8か所に営業所，関西地区1か所に工場がある。本社には，経営管理部，人事総務部，営業部及び情報システム部があり，営業部は各営業所を統括する。工場には，開発部及び製造部がある。

〔特許取得の推進〕

W社では，国内での特許取得を推進しており，経営管理部，開発部及び製造部は，合同で特許検討会を月1回開催している。従業員は，発明の内容及び実施計画を説明した技術報告書を特許検討会に提出する。特許検討会では，技術報告書について審議し，議事録を作成する。審議の結果には，“特許庁に出願”，“ノウハウとして秘匿”及び“発明者への差戻し”の3種類がある。W社の知的財産管理規程では，技術報告書及び議事録（以下，技術報告書と議事録を合わせて，検討会文書という）は，紙のほか，電子ファイルとしても30年間保管することになっている。

特許として登録された場合は，通常，出願から20年間，特許権を保持できる。しかし，特許検討会に提出された技術報告書を全て出願するわけではない。仮に出願すれば，出願の内容が，全て一定期間後に公開されるので，特許として登録されなかった場合は，技術が流出してしまうからである。

一方，W社が特許庁に出願せずに実施した技術に関して，他社の特許が登録された場合は，損害賠償などを請求される可能性がある。

特許検討会では，“ノウハウとして秘匿”と決定した審議案件の紙の検討会文書については，先使用による通常実施権（以下，先使用権という）を確保するために，“公証人の確定日付の付与”を得ている。

特許検討会のメンバが送受信する電子メール（以下，メールという）に添付されている電子ファイルやファイルサーバに保存されている電子ファイルのような日常的にやり取りしている技術情報は，“公証人の確定日付の付与”を得ていない。

特許検討会は情報システム部に対して，次の二つの要望を出した。

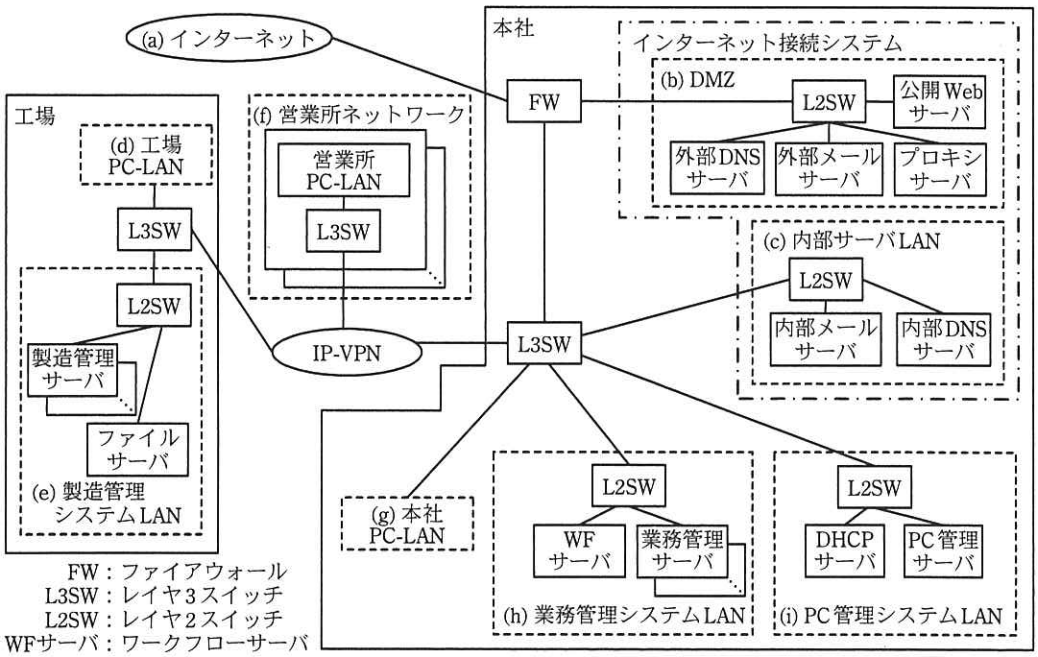
・先使用権を確保するために，検討会文書の電子ファイルは，経営管理部の特許責任者の押印に相当するディジタル署名を付与し，署名日の証明機能をもたせ

たい。

・従業員が送信したメールに添付された技術報告書の電子ファイルを検索できるようにしたい。

〔W社の情報システム〕

W社の情報システムには，インターネット接続システム，製造管理システム，業務管理システム及びPC管理システムがある。情報システムの各サーバは，導入後，5年をめどに更新している。情報システムの全てのサーバは，全ての電子ファイルのウイルススキャンを1日に1回行っている。W社のネットワーク構成を図1に示す。



注記　W社のPCは全て，いずれかのPC-LANに接続されている。PCの記載は省略している。

図1　W社のネットワーク構成

FWでは，拒否した通信をログとして記録している。情報システムの各サーバでは，サーバへのアクセス及びプログラムの動作をログとして記録している。FW上及びサーバ上でのログの保存期間は6か月である。

外部DNSサーバは，インターネット上の時刻サーバとの間で，［　a　］を用いて時刻同期を行っている。FW及び情報システムの各サーバは，外部DNSサーバとの

間で，［ a ］を用いて時刻同期を行っている。

〔PC の利用状況〕

W 社の PC は全て会社が貸与している。各部門における，PC の貸与状況を表 1 に示す。

表 1　PC の貸与状況

部門名	貸与状況
経営管理部，人事総務部，営業部，情報システム部	1 名につき，1 台のノート PC（以下，NPC という）を貸与
営業所	1 名につき，1 台の NPC を貸与
開発部	1 名につき，1 台のデスクトップ PC（以下，DPC という）を貸与
製造部	5 名のメンバで構成される作業グループごとに，1 台の共用 DPC を貸与

W 社では，全ての PC にウイルス対策ソフトを導入している。ウイルス対策ソフトは，PC の起動時及び起動後は 2 時間ごとに PC 管理サーバからウイルス定義ファイルをダウンロードし，更新する。

PC 管理サーバは，1 時間ごとにプロキシサーバ経由でウイルス対策ソフトのベンダの Web サーバからウイルス定義ファイルをダウンロードし，更新する。

全ての PC は，起動時に，PC 管理サーバとの間で時刻同期を行っている。

PC の IP アドレスは，DPC には固定的に割り当て，NPC には，L3SW の DHCP リレーエージェント機能によって動的に割り当てている。

PC の利用者 ID は，従業員ごとに割り当てている。

〔W 社におけるメールの利用〕

従業員は，PC のメールソフトを用いて，他の従業員との間及びインターネットとの間でメールの送受信を行っている。表計算ソフトを使って作成した注文票など，第三者に秘匿したい電子ファイルを送信する場合は，暗号化した上で，メールに添付している。メールソフトの受信フォルダと送信済フォルダの管理は，従業員に任されている。

W 社のメールアドレスのドメイン名には，W 社が取得したドメイン名（以下，W 社

ドメイン名という）を用いている。

情報システムのサーバのうち，メールを扱うのは，外部メールサーバ，内部メールサーバ及び WF サーバである。各サーバのメールに関する機能及び動作概要を表 2 に示す。

表 2　各サーバのメールに関する機能及び動作概要

サーバ名	機能	動作概要
外部メールサーバ	メール転送	SMTP を使用し，インターネットと内部メールサーバとの間でメールを転送する。
	送信ドメイン認証	ディジタル署名を利用する［　b　］を用いた機能及び SPF（Sender Policy Framework）検証機能によってメールの送信ドメインを認証する。
	迷惑メール対策	メールの転送時に迷惑メールのスキャンを行う。迷惑メール定義ファイルを迷惑メール対策ソフトのベンダの Web サーバから 1 時間ごとにダウンロードし，更新する。情報システム部の運用担当者は，送信者メールアドレスや受信者メールアドレスを，それぞれの拒否リストに登録できる。
内部メールサーバ	メール転送	SMTP を使用し，外部メールサーバとの間でメールを転送する。
	メールボックス格納	受信者メールアドレスのドメイン名（以下，受信者ドメイン名という）が W 社ドメイン名であるメールを，従業員用メールアドレスごとのメールボックスに保存する。
	WF サーバ及び PC からのメール送信要求受付	SMTP を使用し，WF サーバ及び PC 上のメールソフトから送信されたメールを受け付ける。
	PC からのメール受信要求受付	POP3 を使用し，PC 上のメールソフトから内部メールサーバのメールボックスへのアクセスを受け付ける。PC のメールソフトの設定によって，メールの受信後に内部メールサーバのメールボックスからメールを削除することもできる。
	ウイルス対策	メール転送，並びに WF サーバ及び PC からのメール送信要求受付で，ウイルススキャンを行う。プロキシサーバ経由でウイルス定義ファイルをウイルス対策ソフトのベンダの Web サーバから，15 分ごとにダウンロードし，更新する。
WF サーバ	メール送信	SMTP を使用し，内部メールサーバにメールを送信する。WF サーバでは，申請及び承認が行われたときにだけメールを従業員用メールアドレス宛てに送信する。
	メール転送拒否	WF サーバにメールが転送されてきた場合は，転送を拒否する。

外部メールサーバ及び内部メールサーバでは，オープンリレー対策を実施している。オープンリレー対策では，SMTP の転送元又は送信元と，エンベロープの受信者ドメイン名の組合せで，転送と送信の許可又は拒否を判定する。判定条件は，図 1，従業員用 PC の使用状況及び表 2 を考慮して決めている。外部メールサーバのオープンリ

レー対策設定を表3に，内部メールサーバのオープンリレー対策設定を表4に示す。

表3　外部メールサーバのオープンリレー対策設定

項番	転送元又は送信元	受信者ドメイン名	設定
1	インターネット	W社ドメイン名	許可
2	c	社外のドメイン名	許可
3	全て	全て	拒否

注記　項番が小さいものから順に，最初に一致したルールが適用される。

表4　内部メールサーバのオープンリレー対策設定

項番	転送元又は送信元	受信者ドメイン名	設定
1	外部メールサーバ	W社ドメイン名	許可
2	WFサーバ	W社ドメイン名	許可
3	d	全て	許可
4	全て	全て	拒否

注記　項番が小さいものから順に，最初に一致したルールが適用される。

表2の“PCからのメール受信要求受付”では利用者認証が行われる。しかし，表2の“WFサーバ及びPCからのメール送信要求受付”では利用者認証（以下，“WFサーバ及びPCからのメール送信要求受付”での利用者認証を，送信利用者認証という）が行われておらず，送信利用者認証の実現が課題になっている。

〔送信利用者認証と特許検討会の要望の実現に関する検討〕

情報システム部のG部長は，送信利用者認証及び特許検討会の要望の実現を検討するように，H主任とJさんに指示した。

H主任とJさんは，G部長の指示について検討し，実現すべき機能を表5のようにまとめた。

表5　実現すべき機能

項番	課題又は要望	実現すべき機能
1	送信利用者認証	送信利用者認証機能
2	メールの検索	メールの保管及び検索機能
3	電子提出	次の機能をもつ電子提出機能 ・電子ファイルによる提出機能 ・電子ファイルへのディジタル署名の付与機能 ・電子ファイルの署名日の証明機能

Jさんは，表5の実現すべき機能について検討した。

〔送信利用者認証機能に関する具体的な検討〕

Jさんは，送信利用者認証機能について，表6に示す具体案をH主任に説明した。

表6　送信利用者認証機能を実現するための具体案

比較項目	X案	Y案
名称	POP before SMTP	SMTP Authentication
利用者ID	送信者メールアドレス	送信者メールアドレス
パスワード	POP3用パスワード	POP3用パスワード
方式	POP3の認証が行われたIPアドレスから内部メールサーバへのメール送信を，認証後，一定時間だけ許可する。	PCから内部メールサーバへのメール送信時に，利用者IDとパスワードによる認証を行う。認証が成功した場合は，メール送信を許可する。

Jさんは，PCからのメール送信方法が現在と変わらないX案を採用したいと，H主任に説明した。H主任は，W社におけるPC及びメールの利用状況を考慮すると，X案では，POP3の認証を実行しなくてもメールを送信できる場合があり，課題が解決できないことを指摘した。H主任の指摘を踏まえて，Y案が採用されることになった。

〔メールの保管及び検索機能に関する具体的な検討〕

Jさんは，内部サーバLANにアーカイブサーバを導入してメールの保管及び検索機能を実現することとし，図2に示すアーカイブサーバの機能及び運用案を作成した。

1. 技術情報の電子ファイルを添付したメールの送信ルール
　経営管理部，開発部及び製造部の主任以上による技術情報の検索を可能にするために，従業員が技術情報の電子ファイルを添付したメールを送信する場合は，内部メールサーバ上の技術情報同報専用のメールアドレス（以下，専用メールアドレスという）にも同報する。
2. メールの複製及び保存
　2.1 内部メールサーバは，受け取ったメールを，ウイルススキャン後に複製する。複製したメールにエンベロープなどの情報を付加し，アーカイブサーバに転送する。
　2.2 アーカイブサーバに転送されたメールは，全て次のように保存する。
　メールは，ハードディスクに一時的に保存する。保存したメールは，定期的に，一度だけ書込み可能な媒体（以下，WORM（Write Once Read Many）媒体という）に保存した後，ハードディスクから削除する。これらの処理は自動的に実行する。
　2.3 WORM 媒体の保存期間は，10 年間とする。
3. メールの検索と検索したメールのダウンロード
　3.1 Web によるアーカイブサーバの検索機能を提供する。検索を行う場合は，WORM 媒体からハードディスクにメールを一時的に書き戻す。
　3.2 従業員は，自身のメールアドレスから送信したメール及び自身のメールアドレス宛てに届いたメールの検索を行うことができる。
　3.3 経営管理部，開発部及び製造部の主任以上は，3.2 に加えて，1.の専用メールアドレス宛てに同報されたメールの検索も行うことができる。
　3.4 3.2，3.3 以外のメールを検索する場合は，人事総務部長の承認を必要とする。
　3.5 人事総務部長は必要に応じて，全メールの検索を行うことができる。
　3.6 検索したメールは，必要に応じてダウンロードできる。
4. アーカイブサーバの機能周知
　4.1 アーカイブサーバの運用を開始する前に，全従業員にアーカイブサーバの機能を説明する。
（以下，省略）

図２　アーカイブサーバの機能及び運用案

J さんは，H 主任に図 2 の案を説明した。次は，その時の会話である。

H 主任：図 2 の 3.1 と 3.6 について，社内メールサーバの機能を考慮すると，保管されているメールの添付ファイルからウイルスが検知される可能性がありますね。

J さん：アーカイブサーバに保存された時点のウイルス定義ファイルにないウイルスが検知されるということでしょうか。

H 主任：はい。図 2 の 3.1 についてはそうですね。しかし，アーカイブサーバに保存された時点のウイルス定義ファイルにあるウイルスであっても，図 2 の 3.6 で検知される可能性があります。①具体的には，アーカイブサーバから PC にダウンロードしたメールの添付ファイルにアクセスしたときに，ウイルスが検知される可能性があります。

Jさん：そのほかに，PC のメールソフトで受信したメールの添付ファイルにアクセスしたときに，同じようにウイルスが検知される可能性がありますね。利用者への説明事項を作成するようにします。

H主任：図2の3.2について，どのように検索の範囲を限定しますか。

Jさん：ヘッダにある From，To，Cc のメールアドレスと従業員のメールアドレスを比較し，限定します。

H主任：それでは不十分ですね。従業員宛てに届いたメールを例に説明します。②ヘッダのメールアドレスと従業員のメールアドレスとの比較では，従業員宛てに届いたメールであっても，検索できないことがあります。図2の3.3も同様です。

Jさん：はい，分かりました。比較方法を修正します。

H主任：専用メールアドレスに届くメールは，従業員が社内から送信したメールに限定すべきです。どのように実現しますか。

Jさん：③表2に示したメールに関する機能で実現します。

H主任：分かりました。それから，④アーカイブサーバの導入によって，メール利用に関する抑止的な効果が期待できますね。

最後に，Jさんは，図2の4.についてH主任に説明した。H主任は説明内容を了承した。

〔電子提出機能に関する具体的な検討〕

Jさんは，図3に示す電子提出機能に関する案をH主任に説明した。

1. 電子ファイルによる検討会文書の提出
WF サーバに，検討会文書の提出フローを追加する。
2. 電子ファイルへのディジタル署名付与
経営管理部の特許責任者が，提出された検討会文書の電子ファイルに秘密鍵を用いてディジタル署名を付与するためのソフトウェアを導入する。ディジタル署名の第三者による検証を可能にするために，認証事業者から公開鍵証明書を購入し，ディジタル署名に使用する。公開鍵証明書の有効期間は 2 年間である。
3. 電子ファイルの署名日の証明
経営管理部の特許責任者は，ディジタル署名を付与した検討会文書の電子ファイルを直ちに DVD-R に保存する。

図3　電子提出機能に関する案

H 主任は，図 3 の 3.の DVD-R では，第三者に署名日を証明できないことを指摘した。J さんが検討したところ，TSA（Time Stamping Authority）が発行するタイムスタンプを付与すれば，タイムスタンプの有効期間中は，電子ファイルが［ e ］及び［ f ］を証明可能であることが分かった。

Z 社のタイムスタンプサービスの導入を前提に調査したところ，TSA 証明書の有効期間は 10 年間であった。

そこで，H 主任は，検討会文書の保管が必要な期間を考慮し，長期署名サービスの導入を行うように指示した。長期署名とは，電子ファイルのディジタル署名値とそのタイムスタンプの検証に必要な公開鍵証明書や失効情報などの情報を加えたタイムスタンプ（以下，アーカイブタイムスタンプという）を付与し，そのアーカイブタイムスタンプの有効期間内に，再びアーカイブタイムスタンプの付与を繰り返す方式である。J さんは，更に検討を行い，図 3 を修正した。

続いて，長期署名の検討を踏まえて，J さんは，図 4 に示す DVD-R の保管方法案を作成した。

1. DVD-R の読取確認
   DVD-R の読取確認を 1 年ごとに実施する。
2. アーカイブタイムスタンプの付与，並びに DVD-R の作成及び保管
   アーカイブタイムスタンプの付与及び DVD-R の作成の手順，並びに⑤災害対策としての DVD-R の作成及び保管の手順を作成し，5 年ごとに実施する。

図 4　DVD-R の保管方法案

H 主任と J さんは，⑥情報セキュリティ技術の観点から，アーカイブタイムスタンプについての事項を確認する手順を図 4 の 2.に追加した。

H 主任は，DVD-R の保管方法案を特許検討会に提示した。特許検討会では，検討の結果，提示された DVD-R の保管方法案を採用することにした。

H 主任と J さんは，これまでの検討結果を踏まえ，表 5 の機能の導入計画を作成し，G 部長に報告した。計画は経営会議で報告され，承認された。そこで，H 主任と J さんは，計画を実行に移した。

設問1　本文中の［　a　］，表2中の［　b　］に入れる適切な字句を，それぞれ英字5字以内で答えよ。

設問2　〔W社におけるメールの利用〕について，(1)～(3)に答えよ。

(1)　メール転送時のウイルススキャンを，外部メールサーバではなく内部メールサーバで行う目的を40字以内で述べよ。

(2)　表3中の［　c　］に入れる適切なサーバ名を，図1中の字句を用いて答えよ。

(3)　表4中の［　d　］に入れる適切なネットワークを，図1中の(a)～(i)から全て選び，記号で答えよ。

設問3　〔送信利用者認証機能に関する具体的な検討〕について，X案で，POP3の認証を行わなくてもメールを送信できる状況を55字以内で具体的に述べよ。

設問4　〔メールの保管及び検索機能に関する具体的な検討〕について，(1)～(4)に答えよ。

(1)　本文中の下線①について，ウイルスが検知される可能性がある理由を50字以内で具体的に述べよ。

(2)　本文中の下線②について，検索できないメールの例を一つ挙げ，25字以内で具体的に述べよ。また，修正後のメールアドレスの比較方法を40字以内で述べよ。

(3)　本文中の下線③について，実現した内容を図1中のサーバ名を含めて50字以内で述べよ。

(4)　本文中の下線④について，どのような行為を抑止する効果が期待できるか。その行為を25字以内で述べよ。

設問5　〔電子提出機能に関する具体的な検討〕について，(1)～(3)に答えよ。

(1)　本文中の［　e　］，［　f　］に入れる証明可能なことを，それぞれ30字以内で述べよ。

(2)　図4中の下線⑤の手順を，60字以内で具体的に述べよ。

(3)　本文中の下線⑥について，確認する手順を40字以内で具体的に述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 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	15:10 ～ 16:20

7. **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。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，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，ポケットティッシュ，目薬
   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 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。
12. 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。