問1　Webアプリケーションプログラム開発のセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

H社は，Webアプリケーションプログラム（以下，Webアプリという）を開発する従業員200名の会社である。H社では，開発部がWebアプリを開発し，情報セキュリティ部が，表1に示す方法に従って，脆弱性検査を実施する。

表1　脆弱性検査の方法（抜粋）

項番	脆弱性	検査の方法	脆弱性が検出された場合の対策方法
1	HTTP ヘッダインジェクション	利用者の入力を基にHTTPレスポンスヘッダを生成する処理において，①改行コードを意味する文字列を入力したときに，HTTP ヘッダフィールドが追加されないことを確認する。 （省略）	（省略）
2	SQL インジェクション	（省略）	SQL 文の組立てにおいて，SQL 文のひな形の中に②変数の場所を示す？記号を置く技法を利用する。
3	メールヘッダインジェクション	（省略）	次のいずれかの対策を実施する。 (1)　メールヘッダを固定値にする。 (2)　外部からの入力を適切に処理するメール送信用APIを使用する。 (3)　外部からの入力の全てについて，［　a　］を削除する。

開発部では，自部で開発したSシステムというWebシステムを利用して，コーディングルールなどの社内ルールを含む各種の情報を共有している。Sシステムの利用者は，ログイン後に情報の投稿と表示を行うことができる。投稿された情報はデータベースに格納される。

ログインから情報表示までのSシステムの画面遷移を表2に示す。

表2　ログインから情報表示までのSシステムの画面遷移

項番	利用者の操作	操作の結果
1	Sシステムのログイン画面にアクセスし，利用者IDとパスワードを入力する。	ログインが成功すると，次の画面がWebブラウザに表示される。なお，下線はリンクであることを示している。 URL　https://（省略）/menu ・情報の投稿 ・情報の表示 （省略）
2	表示された画面の“情報の表示”をクリックする。	“情報選択機能”が呼び出され，次の画面がWebブラウザに表示される。プルダウンには，表示できる情報の情報番号と情報名がリストされる。 URL　https://（省略）/select 表示したい情報の情報番号，情報名を選んでください。 ▼ 番号1001　コーディングルール ⋮ 表示
3	プルダウンから表示したい情報を選択し，“表示”ボタンをクリックする。	“情報表示機能”が呼び出され，次の画面[1)]がWebブラウザに表示される。 URL　https://（省略）/show?no=1001 番号1001 コーディングルール （省略）

注記　利用者のログイン後，セッションIDでセッション管理を行っている。セッションIDは，ログイン時に発行される推測困難な値であり，secure属性が付与されたcookieに格納される。

注[1)]　プルダウンから，表示したい情報として“番号 1001 コーディングルール”を選択した場合を示している。

〔Sシステムの改修におけるアクセス制御要件の追加〕

開発部で新しいプロジェクトを立ち上げることになり，開発部の各プロジェクト内の情報共有を強化することにした。開発部は，次のようにSシステムを改修する方針とした。

・社内ルールだけでなく，各プロジェクトの計画書や各種の設計情報を各プロジェ

クト内で共有できるようにする。

・各プロジェクトの計画書や各種の設計情報については，情報が表示できる利用者を，情報の作成者と同じプロジェクトに参加する利用者に限定できるようにする。

なお，開発部員は，一時期には一つのプロジェクトだけに参加する。同時に複数のプロジェクトには参加しない。

開発部のDさんが，Sシステム改修の担当者に任命され，利用者のアクセス制御を次のように設計した。

・プロジェクトを識別するプロジェクトIDを連番で採番する。

・利用者 ID それぞれに対して，その利用者が参加するプロジェクトのプロジェクトIDを登録しておく。

・S システムに格納される各情報に，作成者の参加するプロジェクトを示すプロジェクトIDをあらかじめ付与しておく。

・プロジェクトIDを次に示す方法で取得し，そのプロジェクトIDを用いてアクセス制御する。

方法1：ログイン時にその利用者IDに対して登録されているプロジェクトIDを取得し，GET リクエストのクエリ文字列に，“id=プロジェクト ID”の形式で指定する。情報選択機能は，クエリ文字列からプロジェクト ID を取得する。

〔情報選択機能の脆弱性〕

S システム改修後の脆弱性検査で，情報セキュリティ部は，プロジェクトの情報番号と情報名を，そのプロジェクトには参加していない利用者が，③そのプロジェクトに参加しているかのように偽ってリスト可能であるという脆弱性を指摘した。これは，情報選択機能においてクエリ文字列で受け取ったプロジェクト ID をチェックせずに利用していることに起因していた。この指摘を受けて，Dさんは，プロジェクトIDの取得方法として，次に示す別の方法を提示した。

方法2：情報選択機能の利用時に，セッション情報から利用者情報を取得する。情報選択機能は，当該利用者情報からプロジェクトIDを取得する。

情報セキュリティ部は，④方法1の脆弱性が方法2で解決されることを確認した。Dさんは，プロジェクトIDの取得方法を方法2に修正した。

情報選択機能及び情報表示機能が参照するデータベースのE-R図を図1に，修正後の情報選択機能のソースコードを図2に示す。

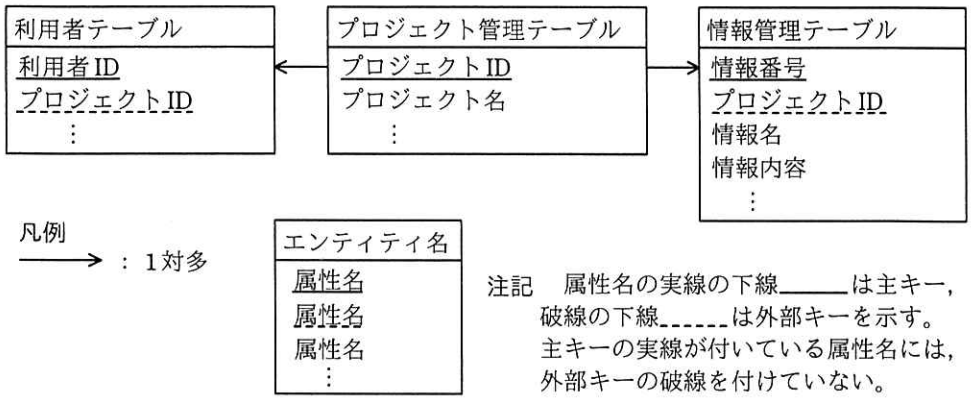

図1　参照するデータベースのE-R図

```
   （省略）  // package宣言，import宣言など
 1: public class SelectServlet extends HttpServlet {
     （省略）  // 変数の宣言やメソッドの定義など
 2:    protected void doGet(HttpServletRequest request, HttpServletResponse response)
   throws ServletException, IOException {
 3:       java.sql.Connection con = null;
 4:       try {
          （省略）  // 初期化処理など
 5:          con = java.sql.DriverManager.getConnection( （省略） );  // データベースに接
   続する処理
 6:          int projectId = （省略）;  // 利用者の参加プロジェクトのプロジェクトIDを利用
   者テーブルから取得し，代入する処理
 7:          String sql = "SELECT 情報番号，情報名 FROM 情報管理テーブル WHERE プロジェ
   クトID = ?";
 8:          java.sql. [ b ] stmt = con.prepareStatement(sql);
 9:          [ c ].setInt(1, projectId);
10:          java.sql.ResultSet rs = stmt.executeQuery();
          （省略）  // 例外処理やその他の処理
```

図2　修正後の情報選択機能のソースコード

〔情報表示機能の脆弱性〕

情報セキュリティ部は，情報表示機能にも情報選択機能と同様の脆弱性があることを指摘した。D さんは，情報表示機能にも同様の修正を行った。修正後の情報表示機能のソースコードを図 3 に示す。

```
   (省略)  // package宣言, import宣言など
 1: public class ShowServlet extends HttpServlet {
     (省略)  // 変数の宣言やメソッドの定義など
 2:   protected void doGet(HttpServletRequest request, HttpServletResponse response)
   throws ServletException, IOException {
 3:      int documentNo = Integer.parseInt(request.getParameter("no"));
 4:      java.sql.Connection con = null;
 5:      try {
          (省略)  // 初期化処理など
 6:        con = java.sql.DriverManager.getConnection( (省略) );  // データベースに接
   続する処理
 7:        int projectId = (省略);  // 利用者の参加プロジェクトのプロジェクトIDを利用
   者テーブルから取得し，代入する処理
 8:        String sql = "SELECT 情報番号, 情報名, 情報内容 FROM 情報管理テーブル WHERE
     [ d ] ";
 9:        java.sql.[ b ] stmt = con.prepareStatement(sql);
          (省略)  // SQL文のひな型に変数を代入する処理
10:        java.sql.ResultSet rs = stmt.executeQuery();
          (省略)  // 例外処理やその他の処理
```

注記　10 行目より後の（省略）に，projectId，documentNo を用いた処理はない。

図 3　修正後の情報表示機能のソースコード

情報セキュリティ部による脆弱性検査に合格後，S システムの改修版がリリースされ，各プロジェクト内の情報共有が強化された。

設問 1　表 1 について，(1)～(3)に答えよ。

(1) 表 1 中の下線①について，適切な文字列の例を，解答群の中から選び，記号で答えよ。

解答群

ア　%0D%0A　　イ　%20　　ウ　
　　エ　<p>

(2) 表 1 中の下線②について，名称を，10 字以内で答えよ。

(3) 表 1 中の [a] に入れる適切な字句を，5 字以内で答えよ。

設問2　〔情報選択機能の脆弱性〕について，(1)～(4)に答えよ。

(1) 本文中の下線③について，未参加のプロジェクトに参加しているかのように偽るための操作を，40字以内で具体的に述べよ。

(2) 本文中の下線④について，方法1の脆弱性が方法2で解決されるのはなぜか。30字以内で述べよ。

(3) 図2中及び図3中の［ b ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア Connection　　イ DriverManager

ウ PreparedStatement　　エ Statement

(4) 図2中の［ c ］に入れる適切な字句を答えよ。

設問3　図3中の［ d ］に入れる適切な字句を，図1中の属性名を含めて答えよ。