問1　Web システムのクロスサイトスクリプティング対策に関する次の記述を読んで，設問 1，2 に答えよ。

E 社は，提携店舗数 100 店の賃貸不動産仲介業者である。E 社では，3 年前に開設した Web システム（以下，E システムという）を用いて賃貸物件情報を提供している。E システムの運用はシステム部が担当し，E システムの保守とコンテンツの開発は E システムの開発を担当した B 社に委託している。

E 社は，E システムをインターネットに公開することを踏まえて，IPA が公表している“安全なウェブサイトの作り方”のチェックリストを参考にしてセキュリティ対策の実施項目を作成し，その実施項目に従って Java で開発するよう B 社に依頼していた。対策の実施項目のうち，クロスサイトスクリプティング（以下，XSS という）対策の実施項目を，表 1 に示す。

表 1　XSS 対策の実施項目

項番	実施項目
①	HTML テキストの入力を許可しない仕様とする。
②	Web ページに出力する全ての要素に対して，エスケープ処理を施す。
③	URL を出力するときは，“http://” 又は “https://” で始まる URL だけを許可する。
④	スクリプト要素の内容（“<script>…</script>” の “…” 部分）を動的に生成しない。
⑤	スタイルシートを任意のサイトから取り込めるようにしない。
⑥	HTTP レスポンスヘッダの Content-Type フィールドに文字コード（charset）を指定する。

〔社内検査〕

E システム開発後，他社の Web サイトで XSS 対策漏れが原因の事故が多発したことから，E システムにも問題が潜在していることが懸念された。そこで容易に検査できる方法はないかと探していたところ，基本的な XSS 対策を実施しているかどうかを診断する“ウェブ健康診断仕様”（以下，Web 健康診断という）が，“安全なウェブサイトの作り方”の別冊として IPA から公表されているとの情報を得た。表 2 は Web 健康診断に基づいて作成した XSS 対策の判定基準である。システム部の C 部長は，表 2 の内容であれば，社内で検査できると考え，若手の D 君を担当に指名した。

表 2 の判定基準では，“対象画面”の“検査文字列を入力する場所”に“入力する検査文字列”を入力した場合に，“脆弱性ありと判定する基準”で示された基準で脆弱性ありと判定する。

表 2　Web 健康診断に基づいて作成した XSS 対策の判定基準

検出パターン	対象画面	検査文字列を入力する場所	入力する検査文字列	脆弱性ありと判定する基準
1	・入力内容確認画面 ・エラー画面	GET パラメタ及び POST パラメタ	`'>"><hr>`	HTTP レスポンスボディに検査文字列がエスケープ処理などを行われずに出力される場合，脆弱性ありと判定
2			`'>"><script>alert(document.cookie)</script>`	
3		URL 中最後の “/” に続く文字列	`<script>alert(document.cookie)</script>`	同上。例えば，URL が “http://www.aaaa.jp/bbbb/index.html” で，“index.html” の部分に検査文字列をエンコードせずに挿入したときエスケープされずに出力される場合，脆弱性ありと判定
4		GET パラメタ及び POST パラメタ	`javascript:alert(document.cookie);`	HTTP レスポンスボディの特定の URI 属性（src, action, background, href, content）に検査文字列が出力される場合，脆弱性ありと判定

図 1 は E システムのうち，賃貸物件の選択結果を表示するプログラムである。D 君が表 2 の判定基準に基づいて検査をしたところ，検出パターン [a] の検査で脆弱性ありと判定された。その原因箇所は図 1 のプログラムの [b] 行目であった。図 1 に，他の脆弱性ありと判定されたものはなかった。

```
（省略）    〔package，import 宣言など〕
 1 public class SelectWin extends HttpServlet {
 2    public void doGet(HttpServletRequest request, HttpServletResponse response)
 3        throws IOException, ServletException
 4    {
 5        response.setContentType("text/html; charset=¥"UTF-8¥"");
 6        request.setCharacterEncoding("UTF-8");
   /* パラメタ name（物件名称），loc（地区名）及び url（URL 情報）を取得 */
 7        String rqName = request.getParameter("name");
 8        String rqLoc = request.getParameter("loc");
（省略）    〔rqName，rqLoc の文字化け対策〕
 9        String rqUrl = request.getParameter("url");
   /* 画面の HTML を出力 */
10        PrintWriter out = response.getWriter();
11        out.println("<html>");
12        out.println("<head>");
13        out.println("<title>賃貸物件の選択結果</title>");
14        out.println("</head>");
15        out.println("<body>");
16        out.println("<h3>詳細表示を開く</h3>");
17        out.println("<p>");
   /* 選択された賃貸物件の詳細を開くリンクを作成 */
18        out.print  ("<a href=¥"" + escapeHTML(rqUrl) + "¥">");
19        out.print  (" 【" + escapeHTML(rqLoc) + "】 ");
20        out.println(escapeHTML(rqName) + "</a>");
21        out.println("</body>");
22        out.println("</html>");
23    }
（省略）    〔その他の必要なメソッドなど〕
```

注記　escapeHTML は HTML の特殊文字 5 文字（<，>，&，"，'）のエスケープ処理を行うメソッドとして別途定義されている。

図 1　賃貸物件の選択結果を表示するプログラム

〔詳細な診断の受診〕

表 2 の判定基準に基づいた社内検査で脆弱性が検出されたことから，C 部長は詳細な診断を受ける必要があると判断し，セキュリティ専門会社の F 社に詳細な診断を依頼した。F 社では，インターネット経由でのアクセスによる E システムの診断とサーバプログラムのソースコードレビューを行った。F 社による診断結果を，図 2 に示す。

XSS 対策に関する診断結果

この脆弱性は，表 1 の実施項目①～⑥が全て正しく実施済みであれば発生しない。
確認した範囲で現状の実施状況をまとめると次のとおりである。

実施項目	実施状況	備考
①	合格	画面からの入力で HTML テキストを必要としているものも，許可しているものもない。
②	一部不合格	社内検査の検査対象に関してはエスケープ処理が施されている。しかし，社内検査の検査対象以外に，対策漏れがある。
③	不合格	URI 属性出力に対しては制限が必要である。
④	不合格	スクリプト要素の内容を動的に生成している。命令として解釈される可能性がある。
⑤	合格	E システム以外のスタイルシートは使用されておらず，任意のサイトから取り込めるようになっていない。
⑥	合格	文字コードは全て指定されている。

図２　Ｆ社による診断結果（抜粋）

〔プログラムの修正〕

図 3 の賃貸物件の検索画面を表示するプログラムでは，賃貸物件を検索するキーワードと地区名を設定するための画面を表示する。その次に呼び出される図 4 の賃貸物件の検索結果を表示するプログラムでは，そのキーワードと地区名を用いて賃貸物件を検索し，その結果をオプションメニューで表示する。オプションの選択が変更された際に，表示用に用意されているテキスト領域に，賃貸物件の情報を“【地区名】説明”の形式で表示する。選択ボタンが押下されると，図 1 のプログラムが呼び出される。

F 社による診断結果に基づき，図 3 と図 4 のプログラムを詳しく検討し，次のとおり問題点を整理して修正することとした。

(1)図 3 の賃貸物件の検索画面を表示するプログラムの問題点と修正

問題点：［ c ］行目と［ d ］行目では，表 1 の実施項目［ e ］に該当する対策が行われていなかった。社内検査では，検査対象を［ f ］に限定しているので D 君はこの脆弱性を検出できなかった。

修正　：エスケープ処理が必要であり，定義されているメソッド［ g ］を適用すべきである。

```
（省略）　〔package，import 宣言など〕
 1 public class SelectKey extends HttpServlet {
 2    public void doGet(HttpServletRequest request, HttpServletResponse response)
 3        throws IOException, ServletException
 4    {
 5        String rsKey, rsLoc;
   /* rsKey にデータベースに登録されたキーワードで検索回数が一番多いものを取得
      rsLoc にデータベースに登録された選択候補地区名を取得，選択候補地区名の値は運用者が設定 */
 6        response.setContentType("text/html; charset=¥"UTF-8¥"");
 7        request.setCharacterEncoding("UTF-8");
   /* 画面の HTML を出力 */
 8        PrintWriter out = response.getWriter();
 9        out.println("<html>");
10        out.println("<head>");
11        out.println("<title>賃貸物件の検索</title>");
12        out.println("</head>");
13        out.println("<body>");
14        out.println("<h3>検索キーワードの設定</h3>");
（省略）　〔データベースに登録されたキーワードで検索回数が一番多いものを rsKey として取得〕
15        out.println("<br>");
16        out.println("<form action=¥"SelectURL¥" method=¥"GET¥">");
17        out.println("よく用いられるキーワード：" + rsKey);
18        out.println("<br>");
19        out.println("検索に用いるキーワードを入力してください：");
20        out.println("<input type=¥"text¥" size=¥"20¥" name=¥"key¥">");
21        out.println("<br>");
22        out.println("物件の地区名を選択してください：");
23        out.println("<select name=¥"loc¥">");
（省略）　〔データベースから選択候補地区名を検索
            検索結果から選択候補地区名を rsLoc として繰返し取得〕
24            out.println("<option value=¥"" + rsLoc + "¥">" + rsLoc + "</option>");
（省略）　〔繰返しはここまで〕
25        out.println("</select>");
26        out.println("<br>");
27        out.println("<input type=¥"submit¥" value=¥"選択¥">");
28        out.println("</form>");
29        out.println("</body>");
30        out.println("</html>");
31    }
（省略）　〔その他の必要なメソッドなど〕
```

図３　賃貸物件の検索画面を表示するプログラム

(2)図 4 の賃貸物件の検索結果を表示するプログラムの問題点と修正

問題点: [h] 行目では，表 1 の実施項目 [i] に該当する対策が不十分であった。

修正　: [h] 行目を [j] に修正すべきである。

```
（省略）　〔package, import 宣言など〕
 1 public class SelectURL extends HttpServlet {
 2    public void doGet(HttpServletRequest request, HttpServletResponse response)
 3        throws IOException, ServletException
 4    {
 5        response.setContentType("text/html; charset=¥"UTF-8¥"");
 6        request.setCharacterEncoding("UTF-8");
   /* パラメタ key（キーワード）と loc（地区名）を取得 */
 7        String rqKey = request.getParameter("key");
 8        String rqLoc = request.getParameter("loc");
（省略）　〔rqKey, rqLoc の文字化け対策〕
   /* データベースから物件名称（rsName），URL 情報（rsUrl）及び説明（rsText）を取得
      これらの値は運用者が設定 */
 9        String rsName, rsUrl, rsText;
（省略）　〔データベースから rqLoc と rqKey の値を用いて賃貸物件を検索〕
   /* 画面の HTML を出力 */
10        PrintWriter out = response.getWriter();
11        out.println("<html>");
12        out.println("<head>");
13        out.println("<title>賃貸物件の検索結果</title>");
14        out.println("<script type=¥"text/javascript¥">");
15        out.println("<!--");
   /* 選択ボタン押下時に選ばれている select オプションの値を変数 url と name の値に設定 */
16        out.println("function setValue() {");
17        out.println("  var index = document.form1.menu1.selectedIndex;");
18        out.print  ("  document.form1.url.value = ");
19        out.println("document.form1.menu1.options[index].value;");
20        out.print  ("  document.form1.name.value = ");
21        out.println("document.form1.menu1.options[index].label;");
22        out.println("}");
   /* オプションの選択が変更された際に msg1 のテキスト領域に “【地区名】説明” として表示 */
23        out.println("function onSet() {");
24        out.println("  var index = document.form1.menu1.selectedIndex;");
25        out.print  ("  document.form1.msg1.value = ¥"【¥" + ");
26        out.print  ("¥"" + escapeHTML(rqLoc) + "¥"");
27        out.println(" + ¥"】¥" +  document.form1.menu1.options[index].text;");
28        out.println("}");
29        out.println("// -->");
30        out.println("</script>");
31        out.println("</head>");
32        out.println("<body>");
33        out.println("<h3>詳細を表示する物件の選択</h3>");
34        out.println("<br>");
35        out.println("キーワード【" + escapeHTML(rqKey) + "】");
36        out.println("<br>");
37        out.println("<form name=¥"form1¥" action=¥"SelectWin¥" method=¥"GET¥">");
38        out.println("<input type=¥"text¥" size=¥"50¥" name=¥"msg1¥" readonly>");
39        out.println("<br>");
40        out.println("<select name=¥"menu1¥" onChange=¥"onSet()¥">");
（省略）　〔検索結果から物件名称（rsName），URL 情報（rsUrl）及び説明（rsText）を繰返し取得〕
41          out.print  ("<option label=¥"" + escapeHTML(rsName) + "¥" value=¥"");
42          out.println(escapeHTML(rsUrl) + "¥">" + escapeHTML(rsText) + "</option>");
（省略）　〔繰返しはここまで〕
43        out.println("</select>");
44        out.println("<br>");
45        out.println("<input type=¥"hidden¥" name=¥"url¥" value=¥"¥">");
46        out.println("<input type=¥"hidden¥" name=¥"name¥" value=¥"¥">");
47        out.print  ("<input type=¥"hidden¥" name=¥"loc¥" value=¥"");
48        out.println(escapeHTML(rqLoc) + "¥">");
49        out.println("<input type=¥"submit¥" value=¥"選択¥" onclick=¥"setValue()¥">");
```

図４　賃貸物件の検索結果を表示するプログラム

```
50        out.println("</form>");
51        out.println("</body>");
52        out.println("</html>");
 (省略)     〔検索に使用したキーワード rqKey の値をデータベースに登録〕
53    }
 (省略)     〔その他の必要なメソッドなど〕
```

図 4　賃貸物件の検索結果を表示するプログラム（続き）

E 社は，今回の XSS 対策以外の対策も含めて E システムの修正を B 社に依頼し，修正後，再度 F 社の診断を受診し，問題が解決していることを確認した。

設問 1　〔社内検査〕について，(1)～(4)に答えよ。

(1)表 2 の検出パターン 1～4 は，それぞれ表 1 の②～⑥のどの実施項目の不備を検出できるものか。それぞれに該当する最も適切な項番を答えよ。

(2)本文中の [a] に入れる適切な検出パターンを 1～4 から選び答えよ。

(3)本文中の [b] に入れる適切な行番号を答えよ。

(4)図 1 のプログラムの [b] 行目に対して実施する XSS 対策を 40 字以内で述べよ。

設問 2　〔プログラムの修正〕について，(1)～(7)に答えよ。

(1)本文中の [c] , [d] に入れる適切な行番号を答えよ。

(2)本文中の [e] に入れる最も適切な実施項目を表 1 の②～⑥から選び答えよ。

(3)本文中の [f] に入れる適切な字句を，表 2 中の字句を用いて 20 字以内で述べよ。

(4)本文中の [g] に入れる適切なメソッド名を答えよ。

(5)本文中の [h] に入れる適切な行番号を答えよ。

(6)本文中の [i] に入れる最も適切な実施項目を表 1 の②～⑥から選び答えよ。

(7)本文中の [j] に入れる適切な修正後の 1 行のソースコードを答えよ。

問 2　スマートフォンアプリケーションに関する次の記述を読んで，設問 1～3 に答えよ。

R 社は，従業員数 1,000 名の飲食店情報提供サービス会社である。R 社では，会員制 Web サイトで飲食店情報や割引クーポンを提供してきた。今回，会員数を更に増やすために，新たに R 社スマートフォンアプリケーション（以下，スマホアプリという）を利用したサービスを提供することを決め，プロジェクトを立ち上げた。プロジェクトリーダには，会員制 Web サイトの運用チームのメンバである B さんが任命された。

〔スマホアプリの概要〕

スマホアプリは，専用 Web サーバに設置する Web アプリケーション（以下，WebAP という）と通信する。WebAP は各飲食店の予約システムと通信して，予約を

行う。スマホアプリを利用したサービスのシステム構成を図1に，スマホアプリとWebAPの動作概要（案）を表1に示す。

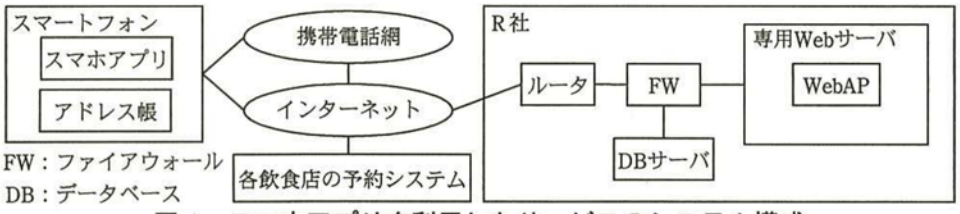


図1　スマホアプリを利用したサービスのシステム構成

表1　スマホアプリとWebAPの動作概要（案）

サービス	スマホアプリ	WebAP
(1) 情報配信	新しい飲食店情報をWebAPに定期的に確認し，受信	新しい飲食店情報を送信
(2) 飲食店検索	地域，料理ジャンル，その他条件を選択してWebAPに送信し，検索結果を受信	検索条件に合致する飲食店情報を送信
(3) 予約確認	会員が予約した情報（以下，予約情報という）をWebAPから受信し，表示	予約情報を送信
(4) 予約案内	パーティ開催のために会員が予約した日時，店舗情報をパーティ参加予定者に案内するために，スマートフォン内のアドレス帳の全件データをWebAPに送信	アドレス帳の全件データの中からパーティ参加予定者を選択して，そのメールアドレスに予約情報を記載した電子メール（以下，メールという）を送信
(5) 新規予約	WebAPに予約要求を送信し，予約結果をWebAPから受信	スマホアプリからの予約要求を飲食店の予約システムに送信し，予約結果をスマホアプリに送信
(6) 会員管理	会員情報を受信して表示し，変更情報をWebAPに送信	DBに登録している会員情報を送信し，変更情報を受信

〔スマホアプリの利用者認証〕

Bさんは，スマホアプリを開発するに当たり，利用者認証について情報システム部のC課長に相談した。次は，そのときの会話である。

Bさん：スマホアプリを繰返し利用してもらうために，面倒なログイン操作は初回だけにして，2回目以降は自動的に利用者が認証されるようにしたいと考えています。

C課長：2回目以降はどんな情報を用いて利用者を認証するのかね。

Bさん：スマートフォンには，IMEI（International Mobile Equipment Identity）などの固有の端末識別番号が付与されていますので，これを用いて利用者を認証することを考えています。

C課長：確かに端末識別番号は端末の固有コードにはなるね。しかし，端末識別番号の特性を考えると，自分の端末識別番号を別の端末で利用されて，サービスを不正利用されるおそれがあるから、①端末識別番号の値をそのまま利用者認証に使うわけにはいかないな。

Bさん：そのまま使うのが問題であれば，端末識別番号を基にスマホアプリ内で②鍵付きハッシュ関数で算出したハッシュ値を使うという方法はどうでしょう。このスマホアプリ専用の鍵を一つ用意して，スマホアプリ内に格納しておけば，不正利用を防ぐことができるのではないかと思います。

C 課長：しかし，③鍵を秘密にしておくことが難しいので，その方法を採用してはいけないと思うよ。スマートフォンサイトでの利用者認証は，一般的な PC サイトと同じように考えた方がいいのではないかな。
B さん：分かりました。

〔予約案内サービスの問題〕
予約案内サービスは，利用者がパーティの参加予定者を利用者のスマートフォンのアドレス帳から選択すると，予約した日時，店舗の情報が参加予定者にメールで通知されるサービスである。具体的には次のような手順で行われる。
(1) 利用者が，スマホアプリの画面で“友達に案内する”ボタンを選択すると，図 2 のような予約案内の確認画面が表示される。
(2) 確認画面の“はい”ボタンを選択すると，WebAP にアドレス帳の全件データが送信され，友達の選択画面が表示される。
(3) 選択画面で参加予定者を選択すると，WebAP から参加予定者宛てにメールが送信される。

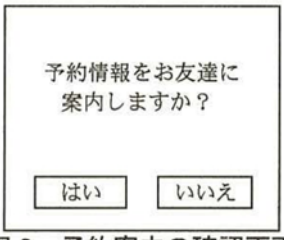


図 2　予約案内の確認画面

予約案内サービスについてプロジェクトのメンバが検討している際に，“図 2 の確認画面は，メールで予約情報を案内することについて同意確認を行っているが，アドレス帳の全件データが R 社に送信されることについては利用者に説明していないので問題である”という意見が多くのメンバから出た。
この意見に対して，“アドレス帳の全件データが送信されることについて確認画面で明確に説明し，同意確認を行う”という改善案が出た。しかし，説明しただけでは不十分であるとして，“アドレス帳の全件データの送信”が行われない別の案（以下，A 案という）が提示され，A 案を採用することになった。
B さんは A 案に基づき，仕様を策定した。また，スマホアプリの機能や動作を利用者に理解してもらえるよう，スマホアプリの導入時に表示される利用規約に，サービスについて詳細に記述することにした。B さんは仕様書を渡して開発業者にスマホアプリと WebAP の実装を依頼した。

〔WebAP の問題〕
開発後，スマホアプリと WebAP に関して第三者のセキュリティ評価を受けることが決定された。そこで B さんは，この分野で実績がある S 社を選んでセキュリティ評価を受けることにした。S 社によるセキュリティ評価の結果，WebAP の予約確認サービスには他人の予約情報を取得できてしまうという問題があるとの指摘を受けた。予約確認サービスのリクエストに含まれるパラメタの概要と，WebAP の予約確認サービスの動作概要を図 3 に示す。

この問題は，ある利用者（以下，利用者 V という）が，数日前に自分が発した予約確認のリクエスト中に含まれるパラメタのうちの二つのパラメタの値を変更して送信することによって，別の利用者（以下，利用者 W という）の予約情報を取得することができるというものであった。つまり，④利用者 V が予約憤報膏表示した際のリクエストである図 4 で使われるパラメタのうちの二つの値を変更して送信すると，利用者 W が予約情報を表示した際のリクエストである図 5 に対する応答を得られるというものである。セキュリティ評価では，仕様書などを参考にして，図 4 のリクエストに操作を加えた上で，WebAP に送信し，その応答を確認した。予約確認サービスについて，図 4 のリクエストに対して行った操作内容，及びリクエストに対して WebAP から受信した応答を表 2 に示す。

1. 予約確認サービスのリクエスト中のパラメタの概要
   - LANG：言語を指定する値
   - AppID：アプリケーション名
   - AuthKey：初回ログイン時に発行される利用者認証用のキー
   - YoyakuCode：年月と予約番号で構成された予約明細コード（予約番号は月ごとに全利用者の予約を 000001 から順番に割り振る）
   - DateTime：スマートフォンの年月日及び時刻

2. WebAP の予約確認サービスの動作概要
   (a) LANG の値が条件に含まれる文字以外の場合はアプリケーションエラーを返し，ja の場合は日本語，en の場合は英語で該当するコンテンツを返す。
   (b) AppID の値が URL に含まれていなければアプリケーションエラーを返す。
   (c) AuthKey の値が WebAP に保持されている利用者認証用の値と一致しない場合は認証エラーを返す。
   (d) YoyakuCode の値が DB サーバに保持されている予約明細コードと一致しない場合はアプリケーションエラーを返す。
   (e) DateTime の値とサーバ側の時刻とのずれが 5 分以上の場合はアプリケーションエラーを返す。
   (f) (a)～(e)でエラーを返さない場合は該当の予約情報を返す。

図 3　WebAP の予約確認サービスのパラメタと動作概要

表 2　リクエストに対して行った操作内容，及び WebAP から受信した応答（抜粋）

リクエストに対して行った操作内容	WebAP から受信した応答
LANG パラメタを削除	アプリケーションエラー
LANG パラメタの値を削除	アプリケーションエラー
LANG パラメタの値を 0 に変更	アプリケーションエラー
AppID パラメタを削除	アプリケーションエラー
AppID パラメタの値を新規予約サービス（ShinkiYoyaku）に変更	アプリケーションエラー
AuthKey パラメタを削除	認証エラー
AuthKey パラメタの値を削除	認証エラー
AuthKey パラメタの値を別利用者の値に変更	YoyakuCode が 201310000034 の予約情報の表示
YoyakuCode パラメタを削除	アプリケーションエラー
YoyakuCode パラメタの値を 201310000071 に変更	YoyakuCode が 201310000071 の予約情報の表示
DateTime パラメタを削除	アプリケーションエラー
DateTime パラメタの値を現在から 4 分前の時刻に変更	YoyakuCode の値に該当する予約情報の表示
DateTime パラメタの値を現在から 5 分前の時刻に変更	アプリケーションエラー

注記　操作するパラメタ以外の値はエラーにならない値を送るものとする。

```
POST /coupon/YoyakuKakunin HTTP/1.0
Host: www.r-sha.jp
Content-Type: text/xml
Content-length: 254

<?xml version="1.0" encoding="utf-8"?>
<XML>
    <LANG>ja</LANG>
    <AppID>YoyakuKakunin</AppID>
    <AuthKey>f3c7b48aac2da10596271a460fb317ac</AuthKey>
    <YoyakuCode>201310000034</YoyakuCode>
    <DateTime>2013 10 16 18:08:10</DateTime>
</XML>
```

図４　利用者Ｖが予約情報を表示した際のリクエスト

```
POST /coupon/YoyakuKakunin HTTP/1.0
Host: www.r-sha.jp
Content-Type: text/xml
Content-length: 254

<?xml version="1.0" encoding="utf-8"?>
<XML>
    <LANG>ja</LANG>
    <AppID>YoyakuKakunin</AppID>
    <AuthKey>6h4Y4io98Uy3q2rfbghyy45ecRyH44po</AuthKey>
    <YoyakuCode>201310000071</YoyakuCode>
    <DateTime>2013 10 16 20:17:14</DateTime>
</XML>
```

図５　利用者Ｗが予約情報を表示した際のリクエスト

〔指摘された問題への対応〕

B さんは S 社から指摘された問題について対応を検討し，開発業者に依頼して必要な修正を行った後，再度 S 社のセキュリティ評価を受けた。その結果，問題が解消されていることが確認できたので，スマホアプリを利用したサービスの提供を開始した。

設問 1　〔スマホアプリの利用者認証〕について，(1)～(3)に答えよ。

(1)C 課長が本文中の下線①のように判断したのは，端末識別番号のどのような特性からか。 20 字以内で述べよ。

(2)本文中の下線②の鍵付きハッシュ関数を解答群の中から選び，記号で答えよ。

解答群

ア　AES　　イ　HMAC　　ウ　RIPEMD　　エ　SHA-256

(3) 本文中の下線③について，どのような手法で鍵を知られてしまうか。30 字以内で述べよ。

設問 2　〔予約案内サービスの問題〕について，A 案の実現方法を，40 字以内で述べよ。

設問 3　〔WebAP の問題〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，利用者 V はどのパラメタの値を変更することによって利用者 W の予約情報を取得できたか。値を変更したパラメタを，図 4 から選び，二つ答えよ。また，それぞれ，どのような値にすることで予約情報を取得できたか。予約情報を取得できたパラメタの内容を答えよ。

(2) 他人の予約情報を取得できてしまう問題の対策として，図 3 の 2.にどのような仕様を追加すればよいか。追加する仕様を 55 字以内で述べよ。

問 3　パブリッククラウドサービスの安全な利用に関する次の記述を読んで，設問 1～3 に答えよ。

P 社は，経営コンサルティングを行っている，従業員数 60 名の会社であり，オフィスは東京にある。P 社には，オフィスに常勤している従業員と，主に客先や自宅で作業を行い，打合せのときだけオフィスに出社する従業員がいる。

社内にファイルサーバを設置して利用していたが，容量は十分であるものの検索の機能が不十分なことから，高機能のファイル共有サービス（以下，C サービスという）を提供している C 社と契約し，C サービスを利用し始めた。C サービスは，ブラウザ経由でアクセスできる SaaS 型パブリックグラウドのサービスである。P 社は，C サービスのサーバ内に P 社専用の領域を確保して，使用履歴，作成者名，メモなどの情報を添えた上でプロジェクト資料を保管している。P 社では，C サービスを活用することで，検索を高速に行えるようになり，業務効率が格段に向上するものと見込んでいる。

客先や自宅で作業を行う従業員には，社外で利用するための PC（以下，リモート PC という）を貸与しており，リモート PC をインターネットに接続できれば，リモートアクセスサーバ（RAS）経由で社内に接続し，社内システムにアクセスできる。客先や自宅から C サービスへのアクセスは，P 社ネットワークを経由せずに直接行う。ネットワーク構成の概要を図 1 に示す。

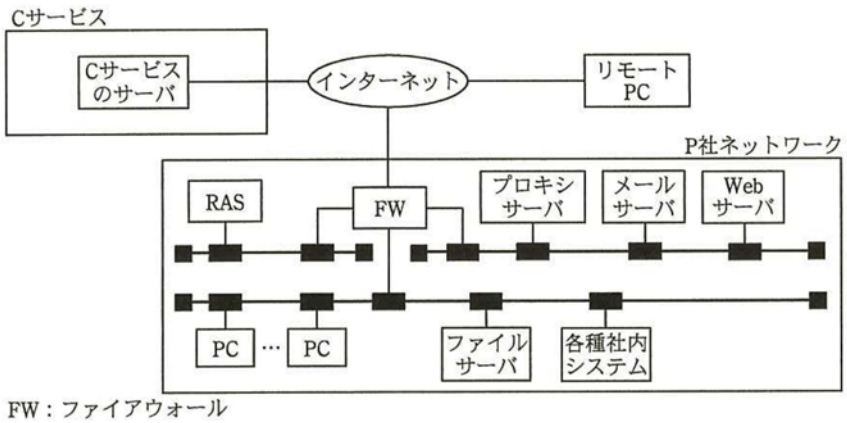


図 1　ネットワーク構成の概要

〔C サービスの認証の強化〕

C サービスの契約と利用者管理については，総務部の X 課長が管理責任者を務めている。C サービスの採用については，C サービスが停止するような事態が発生した場合の事業継続について具体的対策を 1 年以内にまとめることを条件に社長の了承を得ていた。

契約後に，“あるパブリッククラウドサービスから，パブリッククラウドサービス会

社の管理が不十分であったのでパスワードが大量に漏えいし，保存されていたデータが漏えいしだとの報道があった。漏えいがあったパブリッククラウドサービス会社はC社ではなかったが，報道を聞いたP社の社長は，Cサービスで保管している情報が漏えいして多大な損害が発生することを懸念し，X課長に，Cサービスを利用する際の認証の強化を検討するように指示した。X課長は，部下のQさんに，認証の強化策を調査するよう指示した。

Qさんはまず，Cサービスのセキュリティに関する機能を表1にまとめた。

表1　Cサービスのセキュリティに関する機能（抜粋）

番号	項目	機能	備考
1	利用領域へのアクセス制御	契約会社ごとに割り当てられた領域だけにアクセスできる。	P社が契約している領域は，200Gバイトである。
2	利用者管理	契約会社内の管理責任者が，Cサービスの利用者管理機能を使って自社の利用者IDを管理する。	管理責任者は，アクセス履歴も確認できる。
3	通信路暗号化	通信路は，サーバ認証によるSSLで暗号化される。	
4	利用者認証	Web画面で入力された利用者ID（会社が利用者に付与したメールアドレスを利用者IDとして使用）とパスワードを，Cサービス内で照合し，利用者認証を行っている。認証情報は，利用者IDとパスワードが必須である。 追加オプションとして，ログイン手続中に，利用者のメールアドレスに送信したワンタイムパスワードも入力する方式（以下，追加認証方式という）が用意されている。	全ての契約会社の利用者が，同じURLのWeb画面からログインする。

Qさんは，利用者が個人所有の携帯電話メールアドレスを活用することも視野に入れて，追加認証方式の利用について検討した。検討結果を(1)～(3)に示す。

(1)業務上の支障の有無

次の理由から，業務上の支障はないと判断した。

・P社では，P社が契約した携帯電話を多くの従業員に貸与しており，個人所有を含めると全従業員が携帯電話を利用できる。
・携帯電話の故障，紛失などが年に数件発生しているが，個人所有の場合も含めて，携帯電話業者に依頼すれば速やかに同一電話番号かつ同一メールアドレスで利用が再開できる。

なお，P社貸与の携帯電話は，盗難，紛失があった場合には必ず総務部に連絡することになっている。盗難届，紛失届を受けると総務部は，速やかに対応している。

（2）認証強度

他のパブリッククラウドサービスで利用者のパスワードが漏えいした事件を踏まえ，Cサービスの利用者H）とパスワードが漏えいした場合であってもなりすましが困難であるかどうかを評価することにした。

（3）追加認証方式の手順

Qさんは，追加認証方式について，次の手順案を作成した。

・Cサービスの利用者ID登録手順案（図2）
・Cサービスの利用者ID変更手順案（図は省略）
・認証の手順案（図3）

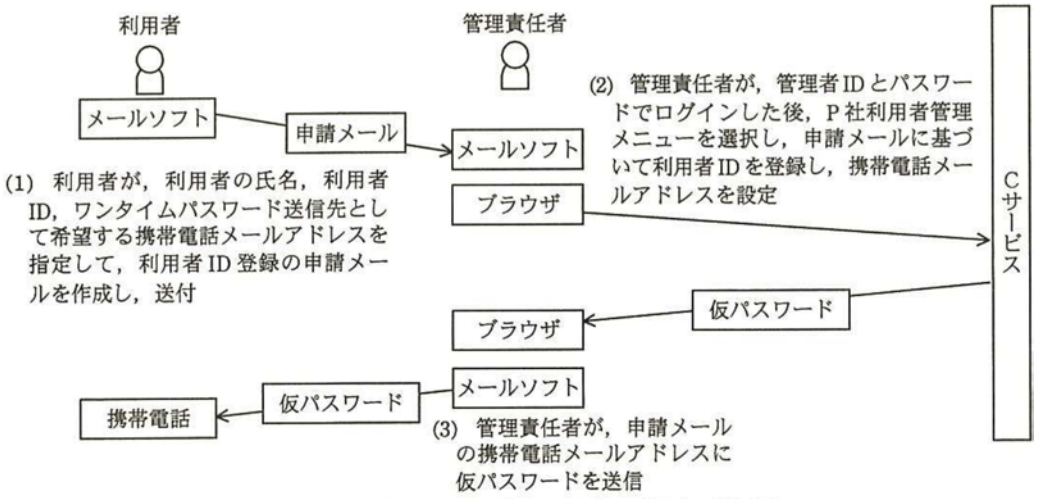
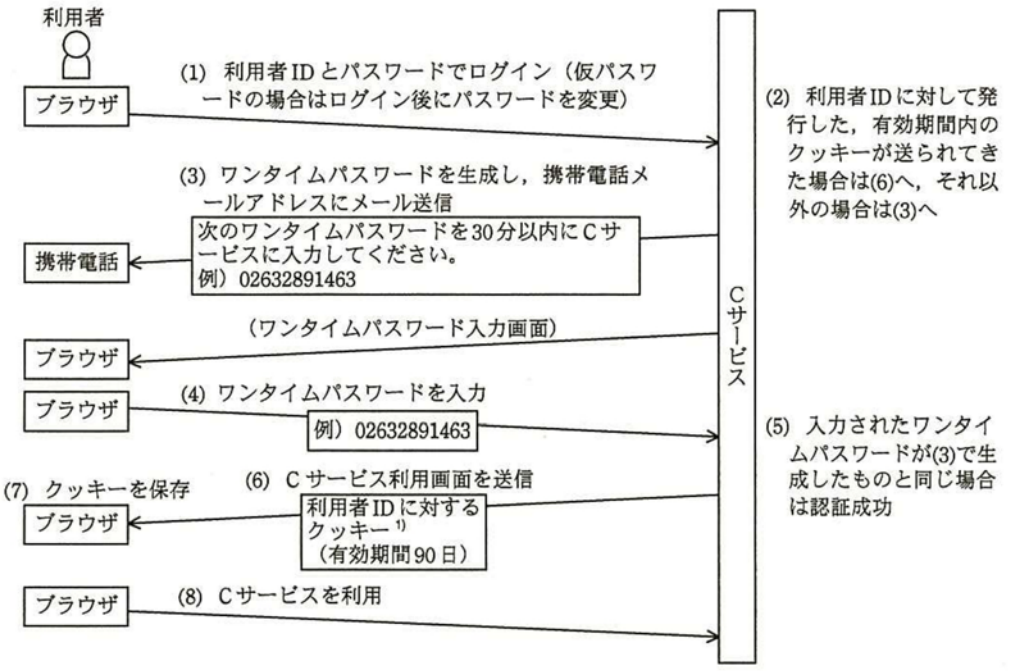


図２　Ｃサービスの利用者 ID 登録手順案（抜粋）



注 1) (5)で認証が成功した場合だけ新たにクッキーが生成され，ブラウザに保存される。
同じ利用者IDに対してさらに他のクッキーが生成された場合でも，このクッキーは90日間有効である。

注記　ログイン状態が 24 時間以上継続すると，自動的にログアウトされ，再度(1)から認証を行う。

図３　認証の手順案（抜粋）

Q さんが手順案を X 課長に提示したところ，“図 2 の手順では，①第三者が利用者になりすまして，仮パスワードを簡単に入手できてしまう”と指摘された。
さらに，“個人の携帯電話が盗まれ，かつ，利用者 ID とパスワードが推測されてしまったときに，②C サービスが不正使用され，しかも、それが長期間続くおそれがあ

る”と指摘された。Q さんは，それらの指摘に対応するため，手順を修正し，対策を追加した。
修正後，追加認証方式は，十分な認証強度をもっていると判断され，P 社では追加認証方式を採用することになった。

〔C サービスを利用できない場合の対応〕
Q さんは，C サービスが停止するような事態が発生した場合の具体的な対策を検討し，表 2 にまとめた。

表 2　C サービスが停止するような事態が発生した場合の具体的な対策

想定シナリオ	求められる業務レベル	事前準備として実施すること	想定シナリオが現実化してから実施すること
C サービスのサーバが被災し，停止するが，2 週間後に元どおり再開する。	業務効率の低下は許容するが，C サービス停止の 24 時間後にはプロジェクト資料を使う業務を再開できる。	[a] しておく。	ファイルサーバを用いて，[b] する。ただし，C サービス復旧後は，C サービスの利用を再開する。
C 社が，1 か月後に C サービスの提供を終了すると通知し，実際に 1 か月後にサービス終了となる。	業務効率を低下させることなく業務を継続できる。	C サービスに代替可能なサービスを選定しておく。 C サービスからの [c] を確認しておく。	代替サービスと契約する。 代替サービスのセットアップ（ID 登録や設定）を行う。 C サービスのデータを代替サービスに移行する。 代替サービスの利用方法を従業員に周知する。

表 2 の内容は承認され，P 社の事業継続計画に盛り込まれた。定期的に訓練が実施されることになり，その後，新しい手順で C サービスの利用が開始された。

設問 1　本文中の下線①について，どのような方法で第三者が仮パスワードを入手することができるか。また，その対策としてどのように本人確認すればよいか。それぞれ 25 字以内で述べよ。
設問 2　本文中の下線②について，不正使用が長期間続く理由を 3O 字以内で，対策を 70 字以内で具体的に述べよ。
設問 3　表 2 中の [a] ～ [c] に入れる実施事項を，[a] は 35 字以内で，[b] は 25 字以内で，[c] は 15 字以内で述べよ。