問１　Webサイトの診断と対策に関する次の記述を読んで，設問1～4に答えよ。

Ｊ社は，従業員数1,000名の衣料品販売会社であり，店舗での販売を主としている。12年前に開設したWebサイト（以下，サイトという）は企業紹介を目的としたコーポレートサイトであったが，8年前に一般の消費者がαブランドの商品を検索したり，Ｊ社に問合せしたりすることができるサイト（以下，αサイトという）を開設した。現在では，他の商品ブランドβ及びγの通販サイト（以下，βサイト，γサイトという）も立ち上げており，新商品の宣伝，キャンペーンを積極的に行っている。

Ｊ社では，サーバをデータセンタＤに設置している。OS，ミドルウェア及びWebアプリケーションは通販事業部が所管し，データセンタＤとの契約やネットワーク，サーバ，機器などのシステム基盤は情報システム部が所管している。通販事業部にはサイトごとにサイト担当者がいて，サイト担当者は，それぞれ担当の通販サイトの開発業者を選び，OSのインストール及び要塞化，必要なミドルウェアのインストール及び設定並びにWebアプリケーションの開発を委託している。Webアプリケーションの簡単な修正などのメンテナンスはサイト担当者が行っている。情報システム部には品質チームがいて，各サイトのセキュリティチェックを行っている。Ｊ社のシステム構成を図１に，Ｊ社の通販サイトに関する情報を表１に示す。

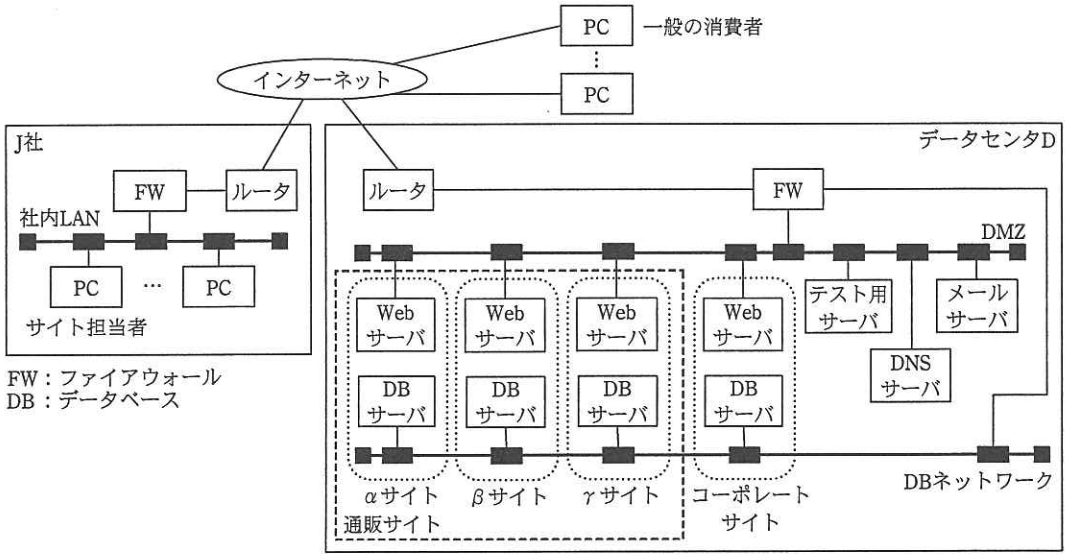

図１　Ｊ社のシステム構成

表１　Ｊ社通販サイトに関する情報

項目＼サイト名	αサイト	βサイト	γサイト
サイトの機能	商品検索 メールマガジン登録 問合せ	新規会員登録 ログイン 会員専用ページ 商品検索 商品購入 問合せ	新規会員登録 ログイン 会員専用ページ 商品検索 商品購入 問合せ
決済機能	なし	決済代行業者のシステムを利用	決済代行業者のシステムを利用
開設・再構築した時期	８年前に開設し，３年前に再構築	７年前に開設	今年開設
セッション管理の有無	セッション管理なし	クッキーによるセッション管理あり	クッキーによるセッション管理あり
開発業者	Ｌ社	Ｍ社	Ｎ社

〔Ｊ社通販サイトのセキュリティ対策状況〕

３年前からＪ社では，脆弱（ぜい）性を防ぐために，開発時にセキュリティチェックシート（以下，チェックシートという）でセキュリティ対策状況を確認するよう開発業者に依頼している。チェックシートを表２に示す。

表２　チェックシート

項番	項目	内容	確認済
1	通信の安全性確保	重要な情報を含む通信を暗号化する	
2	アクセス制御	ログインのパスワードを，英字と数字の両方を含む８文字以上にする	
		特定の利用者だけ利用する画面はアクセス制御を行う	
3	情報の漏えい，改ざん及び破壊の防止	セキュアプログラミングを行う	
		OS やミドルウェアの最新バージョンを利用し，提供済みの全ての修正プログラムを適用する	
		OS やミドルウェアのセキュリティに関する設定を行う	
		不要なファイルを公開しない	
4	サービスの可用性確保	サービス妨害攻撃対策を行う	
5	ログ取得	ログを取得する	

注記　詳細は省略

また，Ｊ社では，３年前からはサイト開設時及び再構築時に品質チームが自動診断ツ

ールを用いて，OS 及びミドルウェアに対する診断（以下，PF 診断という）と Web アプリケーションに対する診断（以下，Web アプリ診断という）を行い，脆弱性の有無を確認している。品質チームが利用している自動診断ツールの仕様を図 2，図 3 に示す。

1. 診断項目の設定（省略）
2. ポートスキャンの実行（省略）
3. オープンポートに対する診断（省略）
4. レポート出力（省略）

（以下，省略）

図 2　PF 診断用自動診断ツールの仕様

1. 診断対象 URL の設定
   (1) 自動探査：起点になる URL（以下，開始 URL という）から順に画面に含まれるリンクをたどりながら自動で巡回し，それらのリンク先の URL を診断対象として設定する。自動探査では，次の制限を設けること（以下，自動探査制限設定という）ができる。
      i．冗長なパスの制限：同一 URL の探査回数の制限
      ii．深さ制限：開始 URL からたどるリンク数の制限
      iii．探査制限：探査する URL の上限数の制限
   (2) 手動探査：特定の URL を診断対象として設定できる。
2. 診断項目の設定（省略）
3. 設定した診断対象 URL に対する診断（省略）
4. レポート出力（省略）
5. 診断可能画面
   次の a）と b）を満たす画面
   a）巡回できる画面
   b）同じ処理が繰返しできる画面
6. パラメタについての条件
   診断対象画面に存在する全てのパラメタのうち，入力した値が次画面で取り扱われるものだけ診断可能

（以下，省略）

図 3　Web アプリ診断用自動診断ツールの仕様

Web アプリ診断では，診断対象の URL を自動探査で設定し，診断項目を設定した後，診断している。自動探査でたどれない画面は，手動探査で設定している。

サイトによっては，診断を行うと大量の問合せメールがサイト担当者に送られたり，大量のテスト注文が発生したりするおそれがある。また，他サイトと連携している場合には，他サイトに意図しないデータが大量に送られるおそれもある。そのため，診断の実施を関係者に連絡し，許可を得てから診断を実施している。

〔専門家によるセキュリティ診断〕

ある日，同業他社の通販サイトで，Web アプリケーションの脆弱性を狙った攻撃によって，個人情報が漏えいする事件が発生した。強い危機感をもったＪ社経営陣は，Ｊ社通販サイトの安全性を改めて確認するように指示した。そこで情報システム部では，Ｊ社通販サイトに対して，専門家による詳細な診断を行うことにした。情報システム部のセキュリティ担当者の Q 主任が専門業者 R 社に依頼して，診断を行った。診断実施後，R 社の Y 氏がＪ社を訪問し，診断結果の説明を行った。

〔αサイトの診断結果と検出された脆弱性への対応〕

αサイトでは，脆弱性が二つ検出された。αサイトで検出された脆弱性を表 3 に示す。

表３　αサイトで検出された脆弱性

項番	脆弱性	概要
1	サービス妨害の脆弱性（以下，DoS 脆弱性という）	Web サーバで使用しているミドルウェアでは，HTTP リクエストヘッダの処理に問題があり，DoS 脆弱性が存在する。この脆弱性が悪用されると，サービスを提供できなくなる可能性がある。
2	管理者用ログイン画面でのログイン試行可能	ミドルウェアの管理者用ログイン画面がインターネットから誰でもアクセス可能になっている。攻撃者が ID とパスワードを推測してログインし，サイトを不正に利用する可能性がある。

項番 1 の“DoS 脆弱性”は，数か月前に公表された脆弱性であった。Ｊ社では脆弱性情報を入手しておらず，ミドルウェアに修正プログラムを適用していなかった。

Q 主任がαサイトのサイト担当者に修正プログラムを適用するよう依頼したところ，“①修正プログラムの適用にはリスクがあるので，適用前に実施しておくべき作業がある”という回答であった。しかし，長期間対策せずにいるのは好ましくないと考えて，暫定的に Web サーバの設定変更を行うようサイト担当者に依頼した。

項番 2 の“管理者用ログイン画面でのログイン試行可能”について，サイト担当者に確認したところ，“ミドルウェアの管理者用ログイン画面は ID とパスワードによる認証によってアクセス制限を行っており，チェックシートに準拠しているので問題ないと思う”という回答であった。

しかし，ID とパスワードによる認証を行っていても，このようなログイン画面が攻

撃者によって見つけられた場合，ID を固定して，考えられる全てのパスワードを試行する，［　a　］が行われる可能性がある。この攻撃によって，管理者権限が奪われると大きな被害になるので，Q 主任はサイト担当者と検討し，インターネットから管理者用ログイン画面にアクセスする場合は，SSH を利用することにした。SSH 利用時には公開鍵認証でログインするので，［　b　］がなければ，Web サーバへの［　a　］を成功させることは困難である。

なお，サイト担当者がミドルウェアの管理画面にアクセスする際には，サイト担当者の PC から Web サーバへの SSH 接続時に，②サイト担当者の PC の任意の通信ポートとミドルウェアの管理画面が動作している通信ポートとの間を暗号通信させることにした。

〔βサイトの診断結果と検出された脆弱性への対応〕

βサイトでは脆弱性が三つ検出された。βサイトで検出された脆弱性を表 4 に示す。

表 4　βサイトで検出された脆弱性

項番	脆弱性	概要
1	セッション ID の固定化	攻撃者があらかじめ用意したセッション ID を，利用者がログイン後に使ってしまうという問題である。攻撃に成功すると，攻撃者がそのセッション ID を利用し，利用者になりすまして Web サイトにアクセスする可能性がある。
2	クロスサイトスクリプティング（以下，XSS という）	新規会員登録画面や検索画面などで，入力内容を検査する処理や出力内容を構成する処理に問題があり，レスポンスにスクリプトを埋め込まれてしまうという問題である。本物サイト上に偽の画面が表示されたり，利用者のブラウザが保存しているクッキーを攻撃者に取得されたりする可能性がある。
3	キャッシュへのコンテンツ残留	サイト利用時に閲覧した個人情報などのコンテンツがブラウザのキャッシュに保存されてしまうという問題である。インターネットカフェなどの共用 PC を利用した場合，ブラウザのキャッシュに保存された情報を他人に閲覧される可能性がある。

診断時の HTTP リクエストとレスポンスのうち，検出された脆弱性に関連したものを図 4～図 9 に示す。

図 4 と図 5 は診断のために URL にセッション ID を含めた，ログイン画面表示時の

リクエストとそのレスポンスである。

```
1  GET /brandbeta/login;jsessionid=65H38O9KCGO30CPGCDHJ4PJ369H62OP7  HTTP/1.1
2  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, (省略)
3  Accept-Language: ja
4  Accept-Encoding: gzip, deflate
5  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; (省略)
6  Host: www.j-sha.jp
```

図４　ログイン画面表示時のリクエスト

```
1  HTTP/1.1 200 OK
2  Date: Mon, 18 Jun 2012 02:55:40 GMT
3  Content-Type: text/html;charset=UTF-8
4  Set-Cookie: JSESSIONID=65H38O9KCGO30CPGCDHJ4PJ369H62OP7; Domain=www.j-sha.jp;
   Path=/brandbeta/; Secure
5  Content-Length: 1200
6  Connection: close
7
8  <HTML>
9  <HEAD>
10 <TITLE>ログイン</TITLE>
11 </HEAD>
12 <BODY>
 (以下, 省略)
```

図５　ログイン画面表示時のレスポンス

図６と図７はテスト用 ID（test1）によるログイン時のリクエストとそのレスポンスである。

```
1  POST /brandbeta/login HTTP/1.1
2  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, (省略)
3  Referer: https://www.j-sha.jp/brandbeta/login
4  Accept-Language: ja
5  Content-Type: application/x-www-form-urlencoded
6  Accept-Encoding: gzip, deflate
7  Cookie: JSESSIONID=65H38O9KCGO30CPGCDHJ4PJ369H62OP7
8  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; (省略)
9  Host: www.j-sha.jp
10 Content-Length: 29
11
12 userid=test1&passwd=password1
```

図６　ログイン時のリクエスト

```
1  HTTP/1.1 200 OK
2  Date: Mon, 18 Jun 2012 03:00:49 GMT
3  Content-Type: text/html;charset=UTF-8
4  Content-Length: 3400
5  Connection: close
6
7  <HTML>
8  <HEAD>
9  <TITLE>会員トップ画面</TITLE>
（以下，省略）
```

図７　ログイン時のレスポンス

図 8 と図 9 は test1 でログインした後の会員情報変更画面の入力時のリクエストとそのレスポンスである。このとき，“名”（name2）を入力せずに送信しているので，エラーになり，エラーメッセージを含む入力画面が表示されている。

Y 氏は図 9 を見て XSS の脆弱性があるかもしれないと思い，あるパラメタの値に“a onmouseover=alert(document.cookie);”を指定し，そのレスポンスを確認して実際に XSS の脆弱性があることを確認した。また，“キャッシュへのコンテンツ残留”の脆弱性についても図 9 を見た後，診断で用いた PC 内のキャッシュを確認して実際に脆弱性があることを確認した。

```
1  POST /brandbeta/user.jsp HTTP/1.1
2  Accept: image/gif, image/x-xbitmap, image/jpeg, (省略)
3  Referer: https://www.j-sha.jp/brandbeta/user.jsp
4  Accept-Language: ja
5  Content-Type: application/x-www-form-urlencoded
6  Accept-Encoding: gzip, deflate
7  Cookie: JSESSIONID=65H38O9KCGO30CPGCDHJ4PJ369H62OP7
8  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; (省略)
9  Host: www.j-sha.jp
10 Content-Length: 182
11
12 user=test1&name1=%E9%88%B4%E6%9C%A8&name2=&birth=1970%2F01%2F01&sex=1&zip=112-
   0000&address=%E6%9D%B1%E4%BA%AC%E9%83%BD%E6%96%87%E4%BA%AC%E5%8C%BA&mail=taro@xx.yy
   &mbmail=taro@mb.xx.yy
```

図８　会員情報変更画面の入力時のリクエスト

```
1  HTTP/1.1 200 OK
2  Date: Mon, 18 Jun 2012 03:55:40 GMT
3  Content-Type: text/html;charset=UTF-8
4  Cache-Control: private
5  Content-Length: 3850
6  Connection: close
7
8  <HTML>
9  <HEAD>
10 <TITLE>利用者情報入力</TITLE>
11 </HEAD>
12 <BODY>
13
 (省略)
32 <font color="red">名が入力されていません。</font>
33 <form method="post" action="/brandbeta/user.jsp" autocomplete="off">
34 <B>利用者情報入力</B>
35 <table width="80%" border="3">
36 <tr bgcolor="#CCCCFF">
37 <td align="center">項目</td>
38 <td align="center">利用者情報</td>
39 </tr>
40 <tr bgcolor="#FFFFFF">
41 <td align="left">ID</td>
42 <td align="center">test1<input type="hidden" name="user" value="test1"></td>
43 </tr>
44 <tr bgcolor="#F3F3F3">
45 <td align="left">姓</td>
46 <td align="center"><input type="text" name="name1" value="鈴木"></td>
47 </tr>
48 <tr bgcolor="#FFFFFF">
49 <td align="left">名</td>
50 <td align="center"><input type="text" name="name2" value=""></td>
51 </tr>
 (省略)
68 <tr bgcolor="#F3F3F3">
69 <td align="left">メールアドレス</td>
70 <td align="center"><input type="text" name="mail" value="taro@xx.yy"></td>
71 </tr>
72 <tr bgcolor="#FFFFFF">
73 <td align="left">携帯メールアドレス</td>
74 <td align="center"><input type=text name=mbmail value=taro@mb.xx.yy></td>
75 </table>
 (以下，省略)
```

図９　会員情報変更画面の入力時のレスポンス

Q 主任は，β サイトのサイト担当者 H さんを呼び，表 4 の各脆弱性について確認した。

Q 主任：項番 1 の“セッション ID の固定化”については，ログイン時に新たなセッション ID が発行されていないことが図 6 と図 7 から確認できます。さらに，

図4と図5からはWebサーバの好ましくない挙動が確認できます。つまり，攻撃者が利用者になりすますことができるという脆弱性がありました。

Hさん：開発時に考慮していなかったようです。

Q主任：項番2のXSSについては，出力にスクリプトが挿入可能でした。

Hさん：ブラウザから送られる各パラメタの値に対し，<，>，"，'，&などの特定の記号をそれぞれ<，>，"，'，&などに変換するエスケープ処理を出力時に行っていましたが，別のミスがありました。

Q主任：項番3の“キャッシュへのコンテンツ残留”については，Cache-Controlヘッダでの制限が不適切なことが図9から確認できます。その結果，姓，名，メールアドレスなどの情報がブラウザのキャッシュに残るような状況でした。

Hさん：この問題については意識していませんでした。

Q主任：今回検出された3種類の脆弱性を，すぐに修正してください。

Hさん：分かりました。

〔γサイトの診断結果と検出された脆弱性への対応〕

γサイトでは脆弱性が一つ検出された。γサイトで検出された脆弱性を表5に示す。

表5　γサイトで検出された脆弱性

項番	脆弱性	概要
1	XSS	表4の項番2と同様

XSSの脆弱性は，新規会員登録機能において検出された。新規会員登録機能の画面遷移を，表6に示す。

表６　γサイトの新規会員登録機能の画面遷移

項番	PC での操作	操作の結果
1	新規会員仮登録画面（下記の URL）にアクセスする。 https://www.j-sha.jp/brandgamma/signup	ブラウザに下記の画面が表示される。 新規会員仮登録（1） ユーザID メールアドレス 次へ
2	表示された画面にユーザ ID（taro）とメールアドレス（taro@xx.yy）を入力し，“次へ”ボタンを押す。 ブラウザから送られる POST データ: action=input&ID=taro&mail=taro@xx.yy	ブラウザに下記の画面が表示される。 新規会員仮登録（2） ユーザID　taro メールアドレス　taro@xx.yy 仮登録
3	“仮登録”ボタンを押す。 ブラウザから送られる POST データ: action=submit&c_token=37sneesy78fe	ブラウザに下記の画面が表示される。 新規会員仮登録が完了しました。 本登録に必要な URL（下記の URL）が記載された電子メールが送られる。 https://www.j-sha.jp/brandgamma/touroku?key=3dk45ttfeUesYdde3Juqaz312y00Pe4W
4	電子メール中に記載された本登録に必要な URL（項番 3 の操作結果中の URL）にアクセスする。	ブラウザに下記の画面が表示される。 新規会員本登録（1） 名前 住所 電話番号 次へ
5	表示された画面に名前（鈴木太郎），住所（東京都）及び電話番号（03-XXXX-XXXX）を入力し，“次へ”ボタンを押す。 ブラウザから送られる POST データ: action=input&name=鈴木太郎&address=東京都&tel=03-XXXX-XXXX	ブラウザに下記の画面が表示される。 新規会員本登録（2） ユーザID　taro メールアドレス　taro@xx.yy 名前　鈴木太郎 住所　東京都 電話番号　03-XXXX-XXXX 登録
6	内容を確認し，“登録”ボタンを押す。 ブラウザから送られる POST データ: action=submit&c_token2=t33x30salh2s	ブラウザに下記の画面が表示される。 新規会員登録が完了しました。

表 6 の項番 5 の“新規会員本登録 (2)”画面の出力で二つのパラメタにスクリプト及びタグが挿入可能であると指摘された。

この脆弱性について，Q 主任がγサイトのサイト担当者に確認したところ，“開発業者にチェックシートの利用を要求していたが，プログラマがそれぞれの解釈でコーディングしたため，エスケープ処理に一部漏れがあるプログラムが作られてしまったという話だった。また，リリース前に品質チームが，新規会員本登録の画面も含む全ての画面の診断を自動診断ツールで行ったようだが，脆弱性は指摘されなかった”とのことであった。Q 主任は，すぐに脆弱性の修正をサイト担当者に依頼した。後日，R 社に，J 社通販サイトについて再度診断を依頼し，指摘された脆弱性が全て修正されたことを確認した。

〔サイトのセキュリティ向上〕

Q 主任は，今回の診断結果を参考に，チェックシート，システム開発手法，及び既存サイトの診断について改善すべき事項を検討した。

これらの対応によって，J 社はサイトのセキュリティをより向上させた。

設問 1　〔αサイトの診断結果と検出された脆弱性への対応〕について，(1)～(5)に答えよ。

(1)　本文中の下線①の修正プログラムの適用に際して考慮すべきリスクは何か。20 字以内で述べよ。

(2)　(1)のリスクに対する対策として，検知及び回復の観点から修正プログラム適用前に実施しておくべき作業は何か。それぞれ 30 字以内で述べよ。

(3)　本文中の [a] に入れる攻撃手法の名称を 15 字以内で答えよ。

(4)　本文中の [b] に入れる適切な字句を 5 字以内で答えよ。

(5)　本文中の下線②は，SSH の何と呼ばれる機能を示しているか。15 字以内で答えよ。

設問 2　〔βサイトの診断結果と検出された脆弱性への対応〕について，(1)～(3)に答えよ。

(1)　図 4 と図 5 から読み取れる Web サーバの好ましくない動作を 50 字以内で述べよ。

(2)　Y 氏が XSS の脆弱性があるかもしれないと判断したのは，図 9 の何行目か。行番号で答えよ。また，その理由を 30 字以内で述べよ。

(3)　ブラウザのキャッシュにコンテンツが残留しないようにするためには，どの Cache-Control ヘッダを出力すればよいか。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　`Cache-Control: max-age=10800`

イ　`Cache-Control: no-store`

ウ　`Cache-Control: no-transform`

エ　`Cache-Control: public`

設問 3　〔γサイトの診断結果と検出された脆弱性への対応〕について，(1)，(2)に答えよ。

(1)　XSS の脆弱性が存在していたと考えられるパラメタを，表 6 中の字句を用いて二つ答えよ。

(2)　リリース前の診断で XSS の脆弱性を検出できなかったのは，自動診断ツールの機能に限界があったからである。その限界を 40 字以内で具体的に述べよ。

設問 4　サイトのセキュリティ向上について，(1)，(2)に答えよ。

(1)　表 3 の項番 1 の脆弱性が，今回の R 社の診断で発見されるまで残存していたのは，新たに発見される脆弱性への対策の遅れが原因であった。今後，このような遅れを防ぐためにセキュリティ対策の運用をどのように改善すべきか。改善点を二つ挙げ，それぞれ 50 字以内で述べよ。

(2)　γサイトでチェックシートを利用したにもかかわらず，エスケープ処理に漏れがあった。製造工程をどのように改善すればよいか，35 字以内で述べよ。