問 I　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。

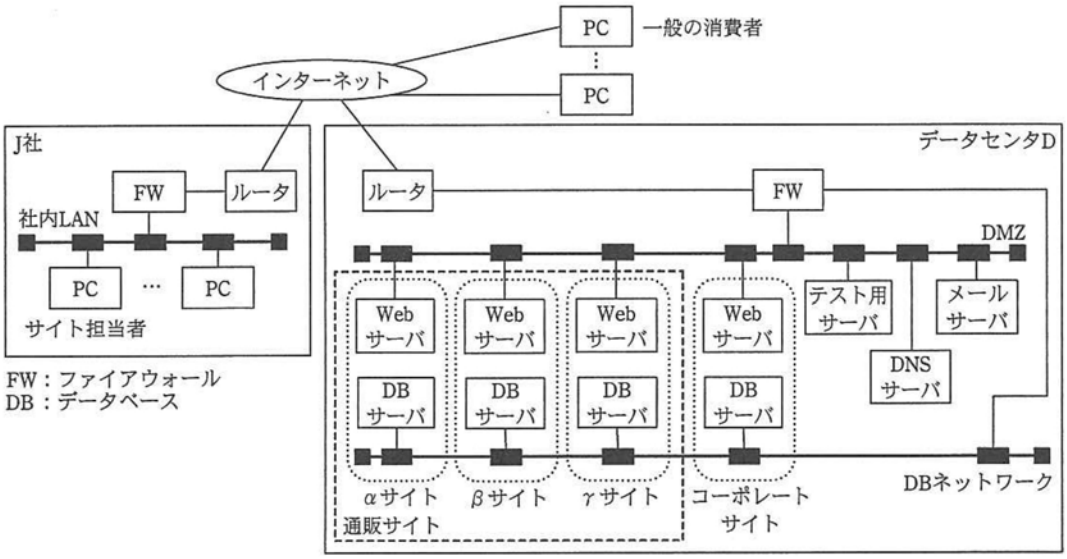


図 1　J 社のシステム構成

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年前からサイト解説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-Contro1 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-Contro1: max-age＝10800`
イ `Cache-Contro1: no-store`
ウ `Cache-Control : no-transform`
エ `Cache-Contro1: 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。

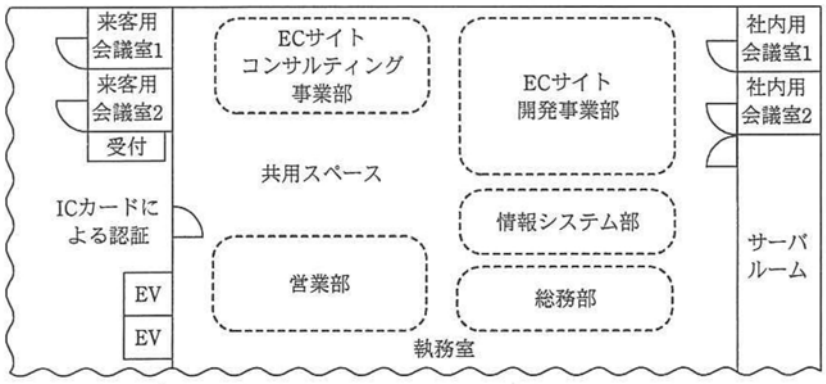
(2) γサイトでチェックシートを利用したにもかかわらず，エスケープ処理に漏れがあった。製造工程をどのように改善すればよいか，35 字以内で述べよ。

問 2　無線 LAN の構築に関する次の記述を読んで，設問 1～4 に答えよ。

T 社は，商品やサービスをインターネット上で販売するための Web サイト（以下，EC サイトという）の開発，構築及び構築支援を主力事業とする企業であり，従業員数は 150 名である。T 社には，EC サイト開発事業部，EC サイトコンサルティング事業部，情報システム部，営業部及び総務部の五つの部署がある。EC サイト開発事業部と EC サイトコンサルティング事業部では，顧客から預かった機密資料や機密データを扱うケースが多い。

〔オフィス及びネットワークの構成〕

T 社のオフィスは，都内のビルの 1 フロアにある。執務室では，座席を部署ごとに集めて配置し，その他に来客用の会議室を二つ，社内用の会議室を二つ用意している。T 社のフロアのレイアウトの概要を図 1 に示す。



EV：エレベータ

注記　波線から左と下のレイアウトは省略

図 1　T 社のフロアのレイアウトの概要

各従業員には，ノート PC 1 台と，入退室の認証に使用する IC カードが貸与されている。入退室で通常使用する執務室のドアは 1 か所で，非接触型の IC カードによって認証し，開錠を行っている。受付担当者は，来客があると，担当者を呼び出し，来客を来客用会議室に案内する。

T 社のネットワーク構成の概要を図 2 に，社内サーバの機能一覧を表 1 に示す。

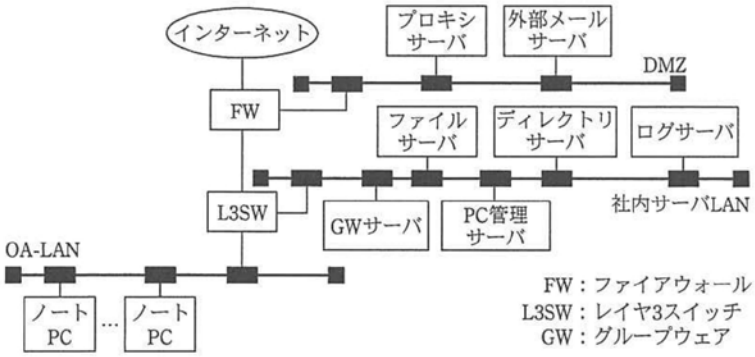


図２　Ｔ社のネットワーク構成の概要

表１　Ｔ社の社内サーバの機能一覧

項番	サーバ名	機能	備考
1	プロキシサーバ	・インターネット上の Web サイトにアクセスする際の利用者認証 ・ウイルスチェック ・URL フィルタリング	利用者 ID とパスワードによる利用者認証をディレクトリサーバで行う。認証にはベーシック認証を利用する。
2	外部メールサーバ	・インターネットから受信した T 社宛てのメールの，GW サーバへの中継 ・GW サーバから受信したメールの，インターネット上のメールサーバへの中継 ・添付ファイルのウイルスチェック ・スパムメールのフィルタリング	
3	ファイルサーバ	・ファイルの共有	次のフォルダが用意されている。 ・全従業員がアクセス可能な，全社共通のフォルダ ・各部の従業員だけがアクセス可能な，部ごとのフォルダ ノート PC とファイルサーバとの通信は暗号化されていない。
4	ディレクトリサーバ	・各利用者の氏名，所属（部署），メールアドレス及び認証情報の一元管理	
5	GW サーバ	・従業員及び社内リソースのスケジュール管理 ・Web メールサーバ	ブラウザから HTTP を利用してアクセスする。SSL は利用しない。 利用者 ID とパスワードによる利用者認証をディレクトリサーバで行う。
6	ログサーバ	・各サーバ上の OS，ソフトウェア及びネットワーク機器のログの収集・保管	ログ閲覧用の管理画面をもつ。
7	PC 管理サーバ	・ノート PC の OS のポリシ設定の強制適用 ・ノート PC にインストールされたソフトウェアのポリシ設定の強制適用	OA-LAN に接続されたノート PC を一元管理している。

ノート PC から社内サーバ及びインターネットへの通信の可否は，次のとおりである。

・社内サーバ LAN 上の全てのサーバとの通信は許可されている。

・インターネットへの通信は，FW で禁止されている。ただし，OA-LAN に接続されたノート PC 上のブラウザから，プロキシサーバを経由したインターネット上の Web サイトへのアクセスは許可されている。

L3SW 及び FW は必要最低限の通信だけを許可するよう設定されている。また，各

サーバ及びネットワーク機器で取得したログは，ログサーバに転送し，保管している。

T 社の情報セキュリティ管理規程（以下，規程という）を図 3 に示す。

1.適用範囲
1-1. 本規程は，当社の従業員と，当社のシステム及びネットワークの利用者を対象とする。
（省略）
9. ネットワーク管理ルール
9-1. 社内ネットワークと社外ネットワークを接続する場合は，情報セキュリティ管理委員会の許可を得なくてはならない。
9-2. 当社のネットワークに接続する機器は，当社所有のものに限る。
（省略）
11. PC 管理ルール
11-1. 業務データはファイルサーバ上に保存することとし，PC への保存は禁止する。ただし，打合せを目的とした場合など，一時的な保存はその限りではない。
11-2. 個人所有の PC 及びその他の機器への社内情報の保管は禁止する。
11-3. 社内及び社外における次の行為は禁止する。
－当社所有の PC 及びその他の機器を業務以外で使用すること
（省略）
14. ログ管理ルール
14-1. 次のログを取得しなければならない。
－インターネットとの通信のログ
－情報共有サーバ（ファイル共有，スケジュール共有などを目的としたサーバ）へのアクセスのログ
14-2. 取得対象の各種ログにアクセスできるのは，その管理権限をもつ者に限定しなければならない。
14-3. 異常又は不正行為を発見するために，ログの確認を行わなければならない。
（省略）
20. 改定
20-1. 本規程の改定には，情報セキュリティ管理委員会の承認を必要とする。

図３　T 社の規程（抜粋）

〔オフィス効率化委員会〕

T 社では，IT を活用した働きやすいオフィス作りを推進するために，オフィス効率化委員会を月次で開いている。オフィス効率化委員会は，情報システム部の U 部長を委員長とし，メンバは各部から従業員 1 名を選出して構成しており，全社的にメリットがあると判断した要望について改善策を検討している。

最近，オフィス効率化委員会には次のような要望が多く寄せられている。

（1）EC サイト構築プロジェクトに関する要望

・EC サイト構築プロジェクトでは，EC サイトコンサルティング事業部と EC サイト開発事業部からメンバを集めて案件ごとにチームを編成する。ミーティングを行う機会が多いので，プロジェクトメンバの座席はまとめて配置してほしい。

（2）会議室利用環境に関する要望

・社内用会議室と来客用会議室（以下，会議室という）には LAN がないので，会議中に資料が必要なときは，必要なファイルをあらかじめノート PC に保存した上で会議室内で参照・編集している。会議室から社内のファイルサーバにアクセスして，ファイルを参照・編集できるようにしてほしい。

・会議中に疑問点を調べるために，インターネット上の Web サイトを閲覧できるよ

うにしてほしい。

U 部長は，次の改善策についてオフィス効率化委員会で検討することにした。
・EC サイト構築プロジェクトの効率を向上させるために，座席を柔軟に移動できるようにする。
・会議室利用環境の改善を行う。

オフィス効率化委員会では，“EC サイト構築プロジェクトの開始・終了時に，座席移動を行ったり，レイアウトを変更したりするとき，有線 LAN だと，その都度，LAN ケーブルを配線し直さなければならないので，社内関連部署に負荷が掛かる”という意見が出た。また，今後はスマートフォンを社内業務に導入していきたいという M 社長の意向があった。そうした背景を踏まえ，今回は無線 LAN の導入を検討することにした。対象エリアは執務室の一部と会議室とすることを決めた。U 部長は，情報システム部の C 君に，無線 LAN の方式を検討するように指示した。

〔無線 LAN 導入の検討〕
次は，C 君が無線 LAN 導入の検討結果を U 部長に報告したときの会話である。

U 部長：無線 LAN を導入する上で，盗聴・不正利用を防止する対策が必要になるが，それは当社の無線 LAN 上を流れる情報の特性や無線 LAN の利用可能エリアを考えると，どのようにすべきだろうか。
C 君　：まず，盗聴を防ぐためには①通信を暗号化する必要があります。そのための規格としては WPA2 を利用します。
U 部長：では，不正利用を防ぐにはどのようにすべきだろうか。
C 君　：無線 LAN を利用するノート PC の認証が必要だと考えています。その方式には，無線 LAN 用のアクセスポイント（以下，AP という）とノート PC との間で事前共有鍵を設定しておく方式と，動的に鍵を交換する［ a ］という方式があります。事前共有鍵を各従業員が設定する場合，②鍵を知る者の退職時などに必要なことがあります。一方，［ a ］を利用する場合は，認証サーバが必要ですが，ディレクトリサーバに認証サーバの機能をもたせることもできます。
U 部長：それなら，［ a ］を採用することにしよう。
C 君　：それから，より強固な認証を行うために，［ a ］の中でもクライアント証明書を用いる EAP-TLS を採用すべきです。
U 部長：なるほど。では EAP-TLS を採用しよう。クライアント証明書はどのように配布するのかな。
C 君　：クライアント証明書は，全て情報システム部がノート PC にインストールするのがよいと思います。

U 部長と C 君は，不正利用を防止する対策について更に検討を行った。次は，U 部長と C 君の会話である。

C 君　：無線 LAN の不正利用対策としては，他にも③ノート PC のネットワークインタフェースがもつ MAC アドレスによるフィルタリングや，AP が定期的に送信している［ b ］を停止する④SSID のステルス化，［ c ］応答

の禁止がありますが，これらの対策も実施してはどうでしょうか。
U 部長：確かにそういう対策があるね。でも，それらの対策は，もし実施するとしても限定的な効果しかないことを踏まえておくべきだと思うよ。

〔会議室への無線 LAN 導入の検討〕

続いて，C 君は会議室への無線 LAN の導入について検討を進めた。まず，C 君は，1 台の AP では安定した通信を提供できないことから，執務室，社内用会議室，来客用会議室のそれぞれに AP を設置する方針とした。そして，次のようにすることにした。

・会議室用の LAN（以下，会議室 LAN という）を L3SW 配下に新設し，そこに会議室用の AP（以下，会議室 LAN 用 AP という）を設置する。
・執務室用の AP（以下，OA-LAN 用 AP という）は，OA-LAN 上に設置する。
・AP で取得するログは，その他のネットワーク機器と同様にログサーバへ転送する。
・従業員が接続先の無線 LAN を識別できるように，執務室用の無線 LAN と会議室用の無線 LAN とで SSID を分ける。
・接続先の無線 LAN を各従業員が設定できるように，ノート PC のネットワーク設定を変更する権限を，PC 管理サーバで各従業員に付与する。
・会議室 LAN からアクセスできるサーバや機器は必要最小限に絞る方針とし，OA-LAN からアクセスできるサーバのうち，一部のサーバについては，会議室 LAN からのアクセスを禁止するよう L3SW を設定する。
・会議室に導入する無線 LAN の暗号化方式や認証方式などは，執務室に導入予定の無線 LAN と同じにする。

C 君は，会議室への無線 LAN の導入についての検討内容を U 部長に報告した。

C 君　：以上のように検討しましたが，いかがでしょうか。
U 部長：会議室 LAN を新設するとなると，⑤アクセスコントロールについては，L3SW の設定だけでなく FW の設定も変更する必要があるね。
C 君　：承知しました。

C 君は U 部長の意見を踏まえ，無線 LAN の導入を進めることにした。

〔無線 LAN の導入〕

C 君は執務室と会議室への無線 LAN の導入を進め，無事導入を終えた。無線 LAN 導入後の T 社のネットワーク構成の概要を図 4 に，T 社のネットワーク接続ポリシを表 2 に示す。

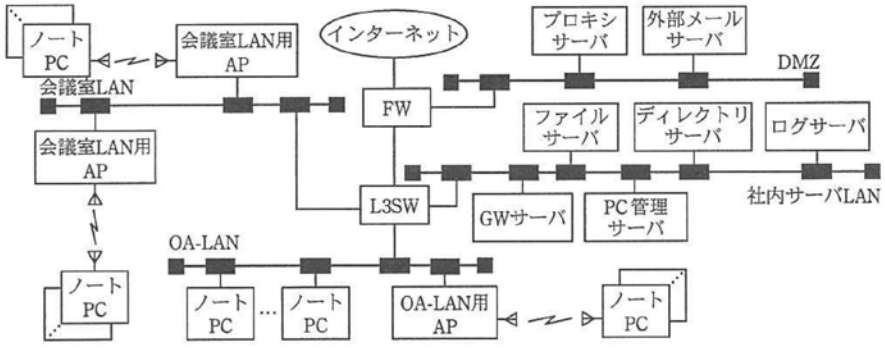


図 4　無線 LAN 導入後の T 社のネットワーク構成の概要

表２　無線 LAN 導入後の T 社のネットワーク接続ポリシ

利用者＼接続先	OA-LAN（有線 LAN）	OA-LAN 用 AP	会議室 LAN 用 AP
EC サイトコンサルティング事業部員 EC サイト開発事業部員	接続不可	接続可	接続可
営業部員 情報システム部員 総務部員 役員	接続可	接続不可	接続可

〔内部監査での指摘〕

T 社では半年に一度，自社の情報セキュリティ上の問題点を洗い出すために内部監査を実施している。前回の内部監査以降に無線 LAN を導入したことで，オフィス環境が大きく変わっている。そこで，T 社では，今回の内部監査において無線 LAN の導入後のセキュリティ対策が適正かどうかを重点的に確認する方針とした。

内部監査の結果，2 件の問題が指摘された。次は，内部監査報告会での M 社長，U 部長，及び内部監査を担当した EC サイトコンサルティング事業部の K 部長の会話である。

K 部長：今回の内部監査の結果として 2 件の指摘事項を報告いたします。1 件目の重要度の高い指摘事項は，私物のデータ通信カード及び私物の携帯型無線 LAN ルータを社内に持ち込んで，ノート PC をインターネットに直接接続している従業員がいるというものです。⑥セキュリティ対策のうち，幾つかは機能の実効性が損なわれてしまいます。この点については至急改善策を検討することを推奨します。

M 社長:それは問題だね。規程の周知徹底と技術的な対策とを併せて検討してほしい。技術的な対策としてはどのようなものが考えられるのだろうか。

U 部長：本指摘事項については，既存の仕組みを利用して対応可能であると考えています。ノート PC のログインアカウントを各従業員に割り当てていますが，⑦そのアカウントに応じて，OS のネットワーク設定のうち一部だけを許可し，それ以外を禁止します。

K 部長：2 件目の指摘事項は，来客用会議室内での従業員のノート PC の扱いが不適切な場合，⑧従業員以外の者が T 社のネットワークに不正にアクセス可能になる，というものです。

U 部長：本指摘事項については，新たなルールを規程に追加すればよいと考えています。

M 社長：了解した。では，進めてくれ。

内部監査報告会での指示を受け，情報システム部で改善を進めることにした。

〔来客用無線 LAN の準備〕

T 社では無線 LAN の利用が進み，“メンバが集まって座れるようになり，EC サイト構築プロジェクトメンバ間でのコミュニケーションがとりやすくなった”，“会議が効率よく行えるようになった”などの声がオフィス効率化委員会に寄せられるようになった。特に，会議中にインターネット上の Web サイトを閲覧できるようになったことは好評であった。

一方で，最近は来客が小型のノート PC やタブレット（以下，この二つをデバイス

という）を持ち込むことが多く，プロジェクトによっては来客との会議でインターネット上の Web サイトを閲覧するケースも増えている。そのような来客用会議室の利用状況を踏まえて，来客用会議室を利用する来客にも無線 LAN を提供し，来客がインターネット上の Web サイトにアクセスできるようにしてほしいとの要望が出るようになつた。オフィス効率化委員会では，来客用に無線 LAN を準備することにし，その検討を C 君が行うことになった。

来客用に準備する無線 LAN について，C 君は次のように検討結果をまとめた。

・LAN を新設して（以下，来客 LAN という），AP（以下，来客 LAN 用 AP という）を新たに設置する。
・無線 LAN を利用するデバイスの認証方式は，導入済の無線 LAN で採用している［ a ］では運用上の負荷が高いので，事前共有鍵方式を利用する。事前共有鍵は来客に設定してもらう。
・来客のデバイスから T 社内の各サーバには通信する必要がないことから，インターネット接続のための回線を新たに準備し，既存のネットワーク環境とは独立したネットワークを構築する。
・来客は，プロキシサーバを経由せずに直接インターネットにアクセスする。
・その際，通信のログは取得しない。

次は，C 君の検討結果についての U 部長と C 君の会話である。

U 部長：来客用のネットワークであるので，当社のネットワークから独立させる方法もある。しかし，設置する AP のメンテナンスやシステムログの取扱いの観点からは，既存のネットワークに AP を設置した方がよいのではないだろうか。そうすることで，通信費用や機器購入のコストを抑えられるメリットもある。
C 君　：そうですね。ネットワーク構成を見直します。
U 部長：それから，現行の規程とネットワーク接続ポリシでは，来客が無線 LAN を利用することを想定していない。⑨来客への無線 LAN の提供によって，規程とネットワーク接続ポリシを見直す必要がありそうだね。ただし，セキュリティリスクが増大しないように，留意する必要がある。
C 君　：承知しました。規程とネットワーク接続ポリシを見直します。

見直し後の T 社のネットワーク構成の概要を図 5 に，見直し後の T 社のネットワーク接続ポリシを表 3 に示す。

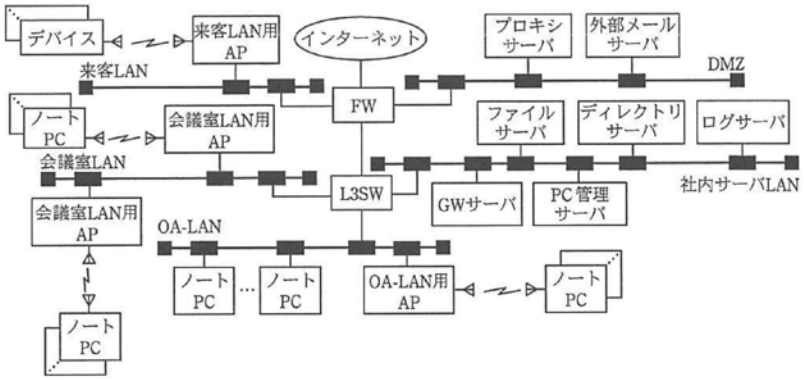


図５　見直し後のＴ社のネットワーク構成の概要

表3　見直し後のT社のネットワーク接続ポリシ

利用者＼接続先	OA-LAN（有線 LAN）	OA-LAN 用 AP	会議室 LAN 用 AP	来客 LAN 用 AP
EC サイトコンサルティング事業部員 EC サイト開発事業部員	接続不可	接続可	接続可	接続不可
営業部員 情報システム部員 総務部員 役員	接続可	接続不可	接続可	接続不可
来客	接続不可	接続不可	接続不可	接続可

オフィス効率化委員会の検討結果を受けて，情報システム部は，来客 LAN の構築を行った。

設問 1　〔無線 LAN 導入の検討〕について，(1)～(3)に答えよ。

(1)本文中の［ a ］～［ 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　802.11i　　イ　802.1X　　ウ　ALL　　エ　ANY プローブ
オ　PSK　　カ　SHA-1　　キ　SHA-2　　ク　WPS
ケ　ビーコン

(2)本文中の下線①について，C 君が，通信を暗号化する必要があると判断した理由を，T 社の無線 LAN 上を流れる情報の特性の観点，及び無線 LAN の利用可能なエリアの観点から，それぞれ 30 字以内で述べよ。

(3) 本文中の下線②について，C 君が必要なこととしている内容を 10 字以内で答えよ。

設問 2　無線 LAN 環境におけるセキュリティ対策について，(1)，(2) に答えよ。

(1) 本文中の下線③及び下線④の対策は，必ずしも効果が得られない。その理由を，それぞれ 20 字以内で述べよ。

(2) 本文中の下線⑤について，FW の設定はどのように変更すべきか。30 字以内で述べよ。

設問 3　〔内部監査での指摘〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線⑥について，ノート PC を直接インターネットに接続する場合に，実効性が損なわれてしまう機能とは何か。二つ挙げ，それぞれ 10 字以内で答えよ。

(2) 本文中の下線⑦について，従業員のアカウントに応じて許可する OS のネットワーク設定とは何か。ネットワーク接続ポリシを踏まえ，EC サイトコンサルティング事業部員及び EC サイト開発事業部員のアカウントの場合と，それ以外の場合の二つに分けて，それぞれ 45 字以内で述べよ。

(3) 本文中の下線⑧の状況を招くノート PC の不適切な扱いとは何か。20 字以内で述べよ。

設問 4　〔来客用無線 LAN の準備〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線⑨について，規程のうち，見直す必要があるとしている項目を二つ挙げ，図 3 中の番号で答えよ。また，各項目について，来客の無線 LAN 利用が抵触する内容を，35 字以内で述べよ。

(2) 無線 LAN のデバイスの認証方式を検討する上で C 君が考慮した，運用上の負荷とは何か。 30 字以内で述べよ。

(3) 来客がインターネット上の Web サイトにアクセスできるようにするために，FW に追加すべき通信許可ルールを，送信元ネットワーク，宛先ネットワーク，通信プロトコルの三つの組で答えよ。

なお，送信元ネットワーク，宛先ネットワークについては図 5 中の字句を用いてそれぞれ一つ答え，通信プロトコルについては二つ答えよ。

解答例

問 1

出題趣旨

Web サイトのセキュリティ対策については，ここ数年対応がとられてきているが，必ずしも万全とは言えない状況である。本問では，Web サイトの診断結果からセキュリティ対策の状況を確認し，見つかった脆弱性の修正方法，診断ツールの適切な利用方法，開発プロセスの改善方法を問う。

設問 1　(1) サーバが正常に動作しなくなるリスク

(2) **検知**　サーバ停止などの異常を検知するための監視体制の整備

回復　サーバを元の状態に戻すための必要なファイルのバックアップ

(3) a　ブルートフォース攻撃

(4) b　秘密鍵

(5) ポートフォワーディング

設問 2　(1) リクエストの URL に含まれていたセッション ID を，レスポンスでクッキーとして発行していた。

(2) **行番号**　74

理由　value 値が二重引用符で囲まれていなかったから

(3) イ

設問 3　(1) ①　・ID

②　・mai1

(2) パラメタについては入力した値が次画面で処理される場合にだけ診断可能である点

設問 4 (1) ①　・システムで利用している OS やミドルウェアの脆弱性情報を定期的に収

②　集し，必要な対応を行う。

・自動診断ツールを最新のものに更新し，定期的に診断を実施し，必要な対応を行う。

(2) チェックシートに基づきコーディング規約を整備する。

問 2

出題趣旨

無線 LAN を経由したインターネット接続形態が，昨今のスマートフォンやタブレットといった携帯可能デバイスからの接続をはじめ増えていることを踏まえ，本問では無線 LAN を題材とし，無線 LAN の導入及び，それに伴う社内ネットワークの構成変更が，情報セキュリティ管理規程や既に講じているセキュリティ対策へどのような影響を与えるのか，またその影響に対してどのように対応すべきかを問う。

設問 1　(1) a　イ

b　ケ

c　エ

(2)　**情報の特性**　顧客から預かった機密データを扱うから

利用可能なエリア　T 社オフィス外でも通信を傍受できる可能性があるから

(3) 事前共有鍵の変更

設問 2　(1) ③ MAC アドレスは偽装可能だから

④ SSID は傍受可能だから

（2）会議室 LAN からプロキシサーバへの通信を許可する。

設問 3　（1）①　・ウイルスチェック

②　・URL フィルタリング

（2）**EC サイトコンサルティング**　執務室用の無線 LAN と会議室用の無線 LAN

事業部員及び EC サイト開発　のどちらかを選択して接続できるようにする。

事業部員のアカウント

それ以外　会議室用の無線 LAN と OA-LAN のどちらかを選択して接続できるようにする。

（3）ノート PC をロックせずに放置すること

設問 4　（1）①　**項目**　9-2

内容　来客所有のデバイスが無線 LAN に接続されること

②　**項目**　14-1

内容　来客のインターネットアクセス時の通信ログが取得されないこと

①と②は順不同

（2）来客のデバイス用のクライアント証明書を発行する負荷

（3）**送信元ネットワーク**　来客 LAN

宛先ネットワーク　インターネット

通信プロトコル　①・HTTP

②・HTTP Over TLS

採点講評

問 1

問 1 では Web サイトのセキュリティ対策について出題した。全体としては正答率が高く，対策についておおむね理解されているようであった。

設問 1（4），（5）は，正答率が低かった。技術用語を問う問題だが，正確に記憶できていない受験者が多かった。

設問 2（1）は，正答率が低かった。“セッション ID の固定化”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”と“利用者に攻撃者があらかじめ用意したセッション ID を使わせること”の二つの条件がそろった場合に脆弱性となる。後者の条件をログイン時のリクエストとレスポンスから確認できれば，正解を導けるはずである。

設問 2（2）理由は，問題文中に“エスケープ処理を出力時に行っていましたが”という記述があるにもかかわらず，“エスケープ処理がされていなかったから”といった誤った解答が多かった。また，“二重引用符”だけは書かれていたが，具体的な理由が記載されていない解答も散見された。

設問 3（1）は，正答率が低かった。表 6 の項番 5 の“PC での操作”に記載のパラメタ，“操作の結果”，そして，図 3 の入力した値が次画面で取り扱われるものだけ診断可能という仕様を確認できれば，正解を導けるはずである。（2）の自動診断ツールの仕様と限界についても関連性を的確に解答してほしかった。

設問 4（1）は，脆弱性情報の入手についての改善案を問う問題である。今回，専門業者の診断で脆弱性を発見できたので，同様の効果が得られる運用を解答として期待していた。しかし，問題文中で修正プログラムの適用にはリスクがあるとしているにもかかわらず，

“自動アップデート機能を利用する”という誤った解答が散見された。
日頃からセキュリティに関する知識を理解しておくことと，問題文をしっかりと読むことを期待する。

問 2

問 2 では，無線 LAN の導入を例にとり，社内ネットワークの構成変更が情報セキュリティ管理規程や既存のセキュリティ対策へ与える影響について出題した。全体として，正答率は高かった。

設問 2（2）では，“ノート PC からインターネットへの直接の通信を許可する”といった誤った解答が多かった。 OA-LAN からインターネットへのアクセスと同様に，会議室 LAN からインターネットへのアクセスに対しても利用者認証や URL フィルタリングが必要である。そのため，会議室 LAN からインターネットへのアクセスもプロキシサーバを経由する必要があるということを，問題文から読み取ってほしかった。

設問 3（3）は正答率が低かった。単に“ノート PC を放置する”といった解答が多かったが，リスクの認識という点では不完全なので，第三者が操作可能な状態であることが具体的に分かるような説明を記述してほしかった。

設問 4（2）も正答率が低かった。プロキシサーバでの利用者認証を行うために，“ディレクトリサーバ上で利用者 ID を登録する”といった誤った解答が散見された。来客のデバイスがインターネットにアクセスする際はプロキシサーバを経由しないとなっていたので，問題文の設定をよく読み，解答してほしかった。