SC

平成29年度　秋期
情報処理安全確保支援士試験
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　ランサムウェアへの対策に関する次の記述を読んで，設問1～4に答えよ。

B社は，従業員数300名の建築資材販売会社であり，本社，営業店10か所の他に倉庫がある。本社，各営業店及び倉庫のネットワークはIP-VPNで接続されており，インターネットとの接続は本社に集約されている。本社と営業店では，それぞれ，本社用PCと営業用PCから情報共有サーバ（以下，Gサーバという）を利用し，Windowsのファイル共有機能を使って資料を共有している。本社用PC及び営業用PCでは，一般利用者権限でログオンすると，自動的にGサーバへもその権限でログオンされ，Gサーバ上の共有フォルダが各PCのGドライブとして自動的に割り当てられる。Gサーバ上の共有フォルダの利用者データ，本社用PCの利用者データ及び営業用PCの利用者データは，それぞれ，各コンピュータのローカルディスク上に設けられた一般利用者権限ではアクセスできない領域に1時間に1回，毎時0分に開始されるジョブによって，バックアップされる。ジョブのログには，バックアップの開始と終了の時刻，総ファイル数，ジョブ実行結果などが記録される。

B社は，販売及び在庫管理を行うソフトウェアを独自に開発し利用している。受注から出荷までの業務を管理するWebアプリケーションソフトウェア（以下，業務APという）は，販売及び在庫管理用のWindowsサーバ（以下，Dサーバという）上で稼働している。B社の全てのPCは，ログオン時に，Dサーバへも一般利用者権限で自動的にログオンされ，Dサーバ上の共有フォルダがWindowsのファイル共有機能を使って各PCのDドライブとして自動的に割り当てられる。出荷業務は，倉庫に設置された作業用PCに，無線ハンディターミナル（以下，HTという）を接続して行う。各PCで用いるB社のWindowsアプリケーション（以下，Aアプリという）は，業務APにHTTP over TLSで接続する機能，及び出荷指示情報が記載されたファイル（以下，出荷指示ファイルという）を読み書きする機能をもっている。

B社のシステム構成を図1に，受注から出荷までの業務の流れを図2に示す。

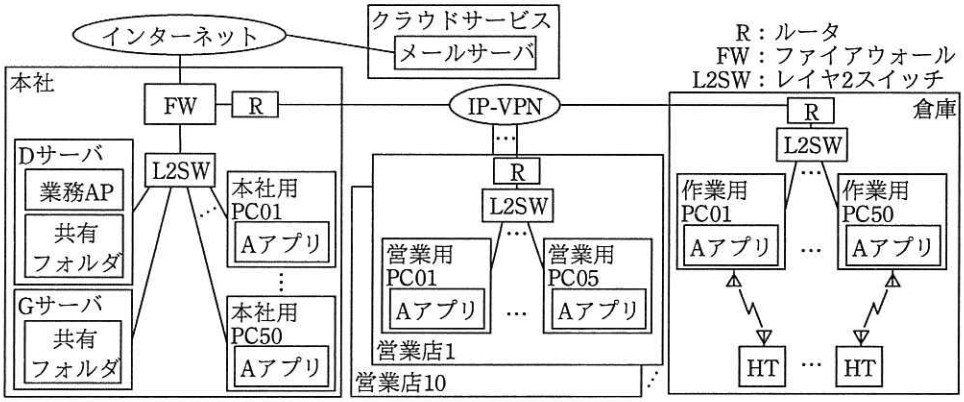

図 1　B 社のシステム構成

1. 営業担当者が，自分の利用者 ID で営業用 PC にログオンし，A アプリを使って業務 AP に接続し，受注情報を登録する。
2. 本社スタッフが，自分の利用者 ID で本社用 PC にログオンし，A アプリを使って業務 AP に接続し，受注情報を基に出荷指示情報を登録する。
3. 業務 AP では，出荷指示情報が登録されると D サーバ上の共有フォルダに，出荷指示 1 件につき，CSV 形式による出荷指示ファイルを 1 ファイルとして出力する。全ての出荷指示ファイルは，出荷担当者が内容の確認と更新をすることができる。
4. 出荷担当者が，自分の利用者 ID で作業用 PC にログオンする。
5. 出荷担当者が，作業用 PC に HT を接続し，A アプリを使って D ドライブ上の自分が担当する出荷指示ファイルを“出荷処理中”にステータス更新した上で，出荷指示情報を HT に取り込む。倉庫内の商品に貼ってあるバーコードを HT で読み取りながら出荷を行う。
6. 出荷担当者は，出荷が完了すると，A アプリを使って D ドライブの該当する出荷指示ファイルを“出荷完了”にステータス更新する。
7. 営業担当者及び本社スタッフが，A アプリを使って D ドライブ上の出荷指示ファイルを閲覧し，最新の出荷状況を確認する。ただし，内容を確認するだけで更新はしない。

図 2　受注から出荷までの業務の流れ

〔セキュリティインシデントの発生〕

ある日の 9:50 に，出荷担当者の V さんから，IT システム担当者の L 君に A アプリの障害の連絡が入った。L 君が D サーバ上の共有フォルダを確認したところ，出荷指示ファイルが破損しており，A アプリで読込みエラーが発生していた。L 君は，原因究明よりも，業務の再開を優先するため，業務 AP の管理機能を使って出荷指示ファイルを再出力して復旧させた。このとき，L 君は，①破損した出荷指示ファイルを削除せず，別のフォルダに移動しておいた。後に，このファイルが，調査に役立った。

復旧させた直後，10:30 に，営業担当者の S さんから L 君に，暗号化されたファイ

ルを取り戻したければ手順に従うよう指示する脅迫文が，営業用 PC05 のデスクトップ画面に表示されているという連絡が入った。また，営業用 PC05 で一部のファイルを開くことができなくなっていた。L 君は，営業用 PC05 がマルウェアに感染したと判断し，営業用 PC05 をネットワークから切り離すよう S さんに指示した。

L 君は，D サーバの出荷指示ファイルも営業用 PC05 と同じように開くことができなくなっていたことから，D サーバも同じマルウェアに感染した可能性があると考え，一連の事象を上司に報告した。上司と相談した結果，業務を一時停止し，D サーバをネットワークから切り離し，従業員に注意喚起をした後，セキュリティ専門会社 U 社の J 氏に協力を依頼して，調査を行うことにした。

〔セキュリティインシデントの調査〕

L 君と J 氏は，感染経路と影響範囲を特定するために，営業用 PC05 と D サーバからログファイルやメモリダンプなどを収集して，表 1 のタイムラインを作成した。

表 1　セキュリティインシデントのタイムライン

No	時刻	事象	対象機器
1	7:50	PC が起動された。	営業用 PC05
2	7:51	営業利用者 05 でログオンされた。	営業用 PC05
3	7:51	営業用 PC05 から営業利用者 05 でログオンされた。	D サーバ
4	8:25	A アプリが実行された。	営業用 PC05
5	8:29	メール閲覧ソフトが実行された。	営業用 PC05
6	8:30	invoice.fdp.exe が実行された。	営業用 PC05
7	8:32	提案書.docx ファイルが暗号化された。	営業用 PC05
以降，9:11 までファイルの暗号化が繰り返された。			営業用 PC05
8	9:11	出荷指示_01_00001.csv ファイルが暗号化された。	D サーバ
以降，9:40 までファイルの暗号化が繰り返された。			D サーバ
9	10:10	脅迫文のファイルが作成され，画面に表示された。	営業用 PC05

受信した電子メールを調査したところ，PDF ファイルに偽装したマルウェアが添

付されていた。ファイル名に Unicode 制御文字の［ a ］が使われていたので，実際のファイル名は invoice.fdp.exe であるが，表示上は invoice.exe.pdf となっていた。S さんは PDF ファイルだと思って添付ファイルを開いたとのことで，開いたときにマルウェアのプログラムが実行されたと考えられた。差出人は B 社従業員になっていたが，メールヘッダの［ b ］フィールドで，経由したメールサーバを調べたところ，社外から送信されていたことが分かった。

S さんに割り当てられている営業利用者 05 に与えられているのは，一般利用者権限なので，営業用 PC05 では，OS のシステムファイルは暗号化されず，S さんが作成したファイルだけが暗号化されていた。L 君は，管理者権限を使って営業用 PC05 にログオンし，マルウェアを除去した上で，②複数世代のバックアップデータの中から，暗号化される直前の世代のバックアップデータを選択し，それを使ってファイルを復元した。

次は，マルウェアに関する，L 君と J 氏の会話である。

L 君：営業用 PC05 が感染したマルウェアはどのようなものなのでしょうか。

J 氏：今回のマルウェアは，ランサムウェア X と呼ばれるものです。ランサムウェア X は，アクセス可能なドライブをドライブレターのアルファベット順に探し，見つけたドライブ内のファイルを暗号化して上書き保存します。内蔵ドライブ，外付けドライブ，ネットワークドライブが対象です。暗号化の対象となるファイルは，文書ファイルなど約 60 種類の拡張子をもつファイルです。対象となるファイルを全て暗号化した後で，脅迫文を画面に表示します。

L 君：ファイルが暗号化されていたので，A アプリで読込みエラーが発生したわけですね。しかし，D サーバは，どのようにして感染したのでしょうか。

J 氏：ランサムウェア X によって，③D サーバ上のファイルが暗号化されたと考えられますが，D サーバ自体が感染した形跡はありません。

L 君：G サーバ上のファイルへの影響はどうでしょうか。

J 氏：D サーバ上のファイルの暗号化が完了した後で，G サーバ上のファイルを暗号化している可能性があるので調査が必要です。

G サーバを調査したところ，共有フォルダのファイルが暗号化されていることが分

かった。しかし，Gサーバ上に取得しているバックアップデータを使って，ファイルを復元することができたので，大きな影響はなかった。

〔被害拡大防止策の実施〕

L君は，PCがランサムウェアに感染した場合に備えて，サーバへの被害を最小限にする対策を講じることにした。Dサーバ上の出荷指示ファイルを格納しているフォルダのアクセス権限が必要最小限になるよう，表2のとおりに見直しを行った。

表2　Dサーバ上の出荷指示ファイルを格納しているフォルダのアクセス権限設定（抜粋）

利用者のグループ	見直し前		見直し後	
	読み	書き	読み	書き
出荷担当者グループ	可	可	c	d
営業担当者グループ	可	可	e	f
本社スタッフグループ	可	可	g	h

L君は，Gサーバについても，ファイルの被害が最小限になるように，Gサーバ上の共有フォルダのアクセス権限を見直した。

L君は，ランサムウェアによって暗号化されたファイルを，バックアップから復元する以外に元に戻す方法はないかJ氏に質問した。J氏によると，ランサムウェアには，ファイルの暗号化に共通鍵暗号だけを使っているタイプと，共通鍵暗号と公開鍵暗号を組み合わせて使っているタイプが発見されている。それぞれファイルを復号可能なケースが報告されているとのことであった。共通鍵暗号だけを使うタイプでは，ランサムウェアのプログラム内にその鍵がハードコードされていれば，ランサムウェアの検体を解析することによって，その鍵を入手してファイルを復号できる可能性がある。一方，共通鍵暗号と公開鍵暗号を組み合わせて使うタイプでは，PCのメモリ上に一時的に作成する共通鍵で対象ファイルを暗号化した後，その共通鍵をプログラム内にハードコードされた公開鍵で暗号化した上で，メモリ上からは共通鍵を消去するので，④このタイプでは，検体を解析しても，ファイルを復号することは難しい。ただし，ランサムウェアXの場合，暗号化に使用した共通鍵をメモリ上から消去しないため，⑤PCをハイバネーション機能によって休止状態で保管しておくことによって，セキュリティベンダから復号ツールが提供されたときに，

復号できる場合があるとのことであった。

L 君は，ランサムウェアに感染した場合の対応手順やツールの整備を上司に進言した。

数日後，J 氏から，OS の新たな脆弱性を悪用する新たなランサムウェア Y が発見されたので，至急，セキュリティパッチ P を適用した方がよいという連絡があった。L 君が確認したところ，B 社のサーバと PC に影響する脆弱性であることが分かった。ランサムウェア Y は，⑥ファイルを暗号化するとともに，他のサーバや PC の OS の脆弱性を悪用し，管理者権限で次々と感染を広めるとのことであった。

L 君は，ランサムウェア Y に対処するために，全てのサーバと PC にセキュリティパッチ P を適用するとともに，セキュリティパッチ適用に関する運用の見直しを検討することにした。

設問 1　本文中の下線①のファイルについて，タイムラインを作成する際に用いたタイムスタンプ情報を解答群の中から選び，記号で答えよ。

解答群

ア　アクセス日時　　イ　更新日時

ウ　削除日時　　エ　作成日時

設問 2　〔セキュリティインシデントの調査〕について，(1)～(4)に答えよ。

(1)　本文中の［　a　］，［　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　BOM　　イ　Content-Type　　ウ　CRLF

エ　Received　　オ　RLO　　カ　X-Mailer

(2)　本文中の下線②について，復元に利用するバックアップデータを選択する際，感染開始時刻と，何の時刻を比較すべきか。15 字以内で答えよ。

(3)　本文中の下線③について，感染していない D サーバも，ランサムウェア X によってファイルが暗号化された。その原因となる，営業用 PC の設定とランサムウェア X の特徴を，それぞれ 35 字以内で述べよ。

(4)　ランサムウェア X が起動した直後に感染を検知し，営業用 PC05 をネットワークから切り離していれば，今回の被害を一部防ぐことができたと考えら

れる。どのような被害を防ぐことができたか。25字以内で述べよ。

設問3　〔被害拡大防止策の実施〕について，(1)～(3)に答えよ。

(1)　表2中の［　c　］～［　h　］に入れる適切なアクセス権限を，業務要件を踏まえて，可又は不可で答えよ。

(2)　本文中の下線④について，検体を解析してもファイルの復号が困難である理由を，30字以内で述べよ。

(3)　本文中の下線⑤のように，PCを休止状態で保管しておけばファイルを復号できる可能性があるが，シャットダウンしてしまうとその可能性が低くなる。可能性が低くなる理由を，ランサムウェアXの動作を踏まえて35字以内で述べよ。

設問4　本文中の下線⑥について，セキュリティパッチPを適用せずに放置した場合，営業用PCがランサムウェアYに感染すると，他のサーバやPCに感染が広がり，甚大な被害が生じるおそれがある。Gサーバにおいて，ランサムウェアXでは起きないが，ランサムウェアYでは起きる被害を，40字以内で述べよ。

問2　Web アプリケーション開発における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。

A 社は，Web マーケティングを支援する従業員数 40 名の企業である。A 社では，現在，Web マーケティング分析システム（以下，W システムという）を Web アプリケーションとして独自に開発し，クラウドサービス事業者 S 社のクラウドサービス上で顧客にサービスとして提供している。W システムでは，A 社独自の分析アルゴリズムを用いて，顧客の Web サイトを分析する。顧客の評価は高く，販売も好調である。

〔W システムの概要〕

W システムの開発は，役員 T 氏とシステム担当の K 氏が行っている。T 氏がアルゴリズムなどの基本的な仕様を決め，K 氏が，Java，サーブレットや開発フレームワークなどを用いて開発している。また，ブラウザ側での機能性向上のために JavaScript も用いている。開発は K 氏が管理する PC（以下，開発用 PC という）上で行い，完成したプログラムをシステム管理者の F 氏が本番システムにデプロイし，運用している。

W システムの画面構成は，次のようになっている。

・総ページ数は 8 である。
・“ログインページ”で利用者を認証し，認証が成功すると，“ダッシュボードページ”へ遷移する。
・“ダッシュボードページ”からは，“分析キーワード入力ページ”などへ遷移できる。

W システムのシンプルなページの構成は，顧客にも好評である。

〔W システムの実装に関する脆弱(ぜい)性〕

A 社では，W システムのセキュリティ検査を，あらかじめ定められた手順に従い K 氏がブラウザを用いて手動で実施している。しかし，昨今の他社のセキュリティインシデント増加を受け，念のために，先月実施した社内のセキュリティ検査とは別に，今月になり初めて，外部の専門家にセキュリティ検査を依頼することにした。

そこで，セキュリティ専門会社 L 社の情報処理安全確保支援士である N 氏が，W システムのセキュリティ検査を担当することになった。

まず，N 氏が脆弱性検査ツールを使って本番システムを検査したところ，図 1 の Java コードで書かれたサーブレット SearchServlet に，SQL インジェクション脆弱性及びクロスサイトスクリプティング（以下，XSS という）脆弱性があることが判明した。図 2 は，図 1 の SearchServlet を呼び出す HTML コードである。

続いて N 氏が本番システムのソースコードを確認し，次の指摘をした。

・SQL インジェクション脆弱性への対処としては，図 1 の［　ア　］行目から［　イ　］行目までを①適切なコードに置き換える必要がある。

・XSS 脆弱性への対処としては，XSS 脆弱性を招く可能性の否定できない箇所について，HTML 形式での出力時に処置するよう改修することとする。

今回指摘された脆弱性は，検査すべき項目の中に含まれており，K 氏によるブラウザを用いた手動のセキュリティ検査によって発見され，開発用 PC 上のコードでは先月に修正されていた。しかし，K 氏からファイルを受け取った F 氏が，本番システムに修正版をデプロイし忘れたので，本番システムに脆弱性が残存したままとなっていた。

```
   (省略)   //package, import宣言など
 1:public class SearchServlet extends HttpServlet {
     (省略)   //変数やメソッドの定義など
 2:
 3:  protected void doPost(HttpServletRequest request, HttpServletResponse response) thr
  ows ServletException, IOException {
 4:    Connection conn = null;
 5:    String cname = request.getParameter("cname");
 6:    response.setContentType("text/html; charset=UTF-8");
 7:    PrintWriter out = response.getWriter();
 8:    try {
         (省略) //データベースにアクセスするためにconnを初期化など
 9:      String sql = "SELECT * FROM companylist WHERE cname = '" + cname + "'";
10:      Statement stmt = conn.createStatement();
11:      ResultSet rs = stmt.executeQuery(sql);
12:      if (cname != null && rs != null) {
13:        out.println("<html>");
14:        out.println("<head>");
15:        out.println("<title>分析結果</title>");
           (省略) //その他，JavaScriptの読込みなど
16:        out.println("</head>");
17:        out.println("<body>");
```

図 1　分析結果を表示するページを出力する Java コード（抜粋）

```
18:         out.println("<table border=1>");
19:         out.println("<tr><th>キーワード</th><th>アクセス</th><th>売上げ</th></tr>");
20:         while (rs.next()) {
21:           out.println("<tr><td>" + rs.getString(1));
22:           out.println("</td><td>" + rs.getString(2));
23:           out.println("</td><td>" + rs.getString(3));
24:           out.println("</td></tr>");
25:         }
26:         out.println("</table>");
            (省略) //その他
27:         out.println("</body>");
28:         out.println("</html>");
29:       }
30:     } catch (SQLException e) {
          (省略) //例外処理
31:     } finally {
          (省略) //データベースへのアクセスを終了する処理など
32:     }
        (省略) //その他，エラー処理など
33:   }
34:
      (省略)    //その他のメソッドの定義など
35:}
```

図 1　分析結果を表示するページを出力する Java コード（抜粋）（続き）

```
1:<form action="SearchServlet" method="post">
2:  分析キーワードを入力してください：<input type="text" name="cname" />
3:  <input type="submit" value="検索" />
4:</form>
```

図 2　SearchServlet を呼び出す HTML コード（抜粋）

〔W システムの設計に関する脆弱性〕

以前の W システムは，ログイン状態で 30 分間操作しないと，サーバ側で自動的にログアウトする仕様であった。自動的にログアウトした場合，ログアウト直前のページを閲覧するには，再度ログインをして，ダッシュボードページから所望のページを選択する必要があるので，不便だとの指摘が顧客からあった。これを改善するため，自動的にログアウトした場合に，ログアウト直前のページの閲覧を試みると，一旦はログインページに遷移するが，認証が成功すると，閲覧を試みたページへリダイレクトする機能（以下，リダイレクタ機能という）を導入した。例えば，W システムの URL である https://w-system.a-sha.jp/ で動作する Web アプリケーションにおいて，W システムにログインしていない状態で，https://w-system.a-sha.jp/dashboard.jsp という URL にアクセスすると，図 3 のように生成された URL へリダイレクトされる。

```
https://w-system.a-sha.jp/LoginServlet?redirect_url=https://w-system.a-sha.jp/dashboard.jsp
```

図3　リダイレクタ機能によって生成されたURL

認証用サーブレット LoginServlet で認証が成功すると，https://w-system.a-sha.jp/dashboard.jsp へリダイレクトされる。

リダイレクタ機能を含めて W システムの設計に関して検査を実施したところ，N 氏から幾つかの指摘があった。主な指摘は次の3点であった。

指摘1：W システムの認証後のリダイレクタ機能は，オープンリダイレクタの問題を招く。修正する必要がある。

指摘2：W システムからの Cookie 発行の際，TLS 通信時だけ Cookie をブラウザから送信する［　a　］属性を設定する必要がある。

指摘3：JavaScript から Cookie を操作できないようにする［　b　］属性を設定する方がよい。

K 氏は，指摘 1 に対しては，W システムの特性を考慮して，②ホワイトリスト方式によるリダイレクタ機能を採用することにした。指摘 2 と指摘 3 については，N 氏の指摘どおりに改修することにした。

〔脆弱性対策の強化〕

脆弱性が残存した原因も踏まえ，脆弱性対策の強化として，次のとおり提案と指摘を N 氏は行った。

・変更管理プロセスを改善すべきである。

・③脆弱性検査手順を改善すべきである。

・K 氏によるブラウザを用いた検査には問題がある。W システムに XSS 脆弱性があったとして，適当な検査用文字列を入力しても，④一部のブラウザでは XSS 攻撃の試みを完遂できないことがある。

・S 社のクラウド型 WAF サービス（以下，S サービスという）を導入することを推奨する。S サービスでは，Web システムに脆弱性が発見された際，短時間で適切なシグネチャが WAF に追加される。したがって，S サービスを利用していれば，WAF を利用せずに W システムを改修するケースと比較して，⑤Web アプリケーションサーバへのリスクの低減を期待できる。

A社では，N氏のこれらの提案と指摘を検討し，適切に対処することにした。

設問1　〔Wシステムの実装に関する脆弱性〕について，(1)～(3)に答えよ。

(1)　本文中の［　ア　］，［　イ　］に入れる，適切な行番号を答えよ。また，本文中の下線①について，必要な全てのコードを解答群の中から選び，適切な順序に並べ替えて解答欄の左から順に記号で答えよ。

解答群

ア　PreparedStatement pstmt = conn.prepareStatement(sql);

イ　pstmt.setString(1, cname);

ウ　ResultSet rs = pstmt.executeQuery();

エ　ResultSet rs = pstmt.executeQuery(sql);

オ　String sql = "SELECT * FROM companylist WHERE cname = '" + cname + "'";

カ　String sql = "SELECT * FROM companylist WHERE cname = ?";

(2)　図1には，XSS脆弱性を招く可能性を否定できないコードがある。N氏の指摘に従い，改修すべき行番号を全て答えよ。

(3)　XSS脆弱性に対する修正を，N氏の指摘に従い，解答群の中から選び，記号で答えよ。

解答群

ア　CSRF対策トークンを使う。

イ　Refererヘッダの値のURLのドメイン名がWシステムのものであることを確認する。

ウ　出力時に<，>，&，"，'の各文字をエスケープする。

エ　同一生成元ポリシを適用する。

オ　バインド機能を使う。

設問２　〔W システムの設計に関する脆弱性〕について，(1)，(2) に答えよ。

(1)　本文中の［　a　］，［　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　Expires　　イ　HttpOnly　　ウ　Max-Age

エ　Secure　　オ　Secured

(2)　本文中の下線②について，W システムで採用するホワイトリスト方式の適切な仕様を，40 字以内で具体的に述べよ。

設問３　〔脆弱性対策の強化〕について，(1)～(3) に答えよ。

(1)　本文中の下線③について，どのように改善すべきか。改善された検査手順を 30 字以内で述べよ。

(2)　本文中の下線④について，XSS 攻撃の試みを完遂できないことがある理由を 30 字以内で述べよ。

(3)　本文中の下線⑤について，低減できるリスクを 50 字以内で述べよ。

問3　SSL/TLS を用いたサーバの設定と運用に関する次の記述を読んで，設問 1～3 に答えよ。

C 社は，衣服のデザイン，製造及び販売を行う中堅の衣料品製造会社である。近年は，C 社の複数の販売チャネルのうち，EC モールに出店したオンラインショップでの販売量が増えており，C 社の社名も比較的知られるようになった。C 社では，事業を更に拡大するために，新たに独自のドメイン名を取得し，C 社専用の販売サイト（以下，EC サイトという）を立ち上げることにした。

EC サイトの構築，運用及び管理は，C 社のシステム部が担当することになった。システム部は開発会社の協力を得て構築を進め，当初の計画どおり運用が開始された。

〔社外からの通報〕

運用開始から 3 か月が経過した頃，C 社の問合せ窓口に，EC サイトで利用されている一部のサーバ証明書に対応する秘密鍵が，サーバ証明書と一緒に，ある Web サイト（以下，Q サイトという）に掲示されているという通報があった。そこで，システム部の M 部長は，EC サイトの管理を担当する B さんに，セキュリティ専門会社である E 社の支援を得て本件を調査し必要な措置を講じるよう指示した。

E 社のセキュリティコンサルタントである H 氏のアドバイスを受けて B さんが確かめたところ，Q サイトに掲示された秘密鍵は自社のものと一致していた。B さんは鍵が危たい化したと判断した。

次は，H 氏と B さんの会話である。

H 氏　：サーバ証明書に対応する秘密鍵が公開された影響について，順に説明していきましょう。サーバ証明書は認証局サービス事業者から発行されます。サーバ証明書には，サーバの FQDN と公開鍵が記載されます。サーバ証明書の作成とその検証には公開鍵暗号方式を利用した［ a ］技術を利用します。サーバ証明書は SSL/TLS で利用されます。SSL/TLS は複数の暗号技術を用います。データの送受信時は，暗号化と復号のために［ b ］を利用します。また，データの送信者と受信者が［ b ］で使用する鍵

を共有するために，公開鍵暗号方式を用いて［　c　］を行います。現在，世の中で発行されているサーバ証明書には複数の種類があり，代表的なものはドメイン認証証明書と［　d　］です。サーバ証明書の種類によって，認証局サービス事業者が発行時に行う審査の内容が異なります。

秘密鍵を知った者は，御社の EC サイトと利用者との通信パケットを入手できれば，それを復号して内容をのぞき見できる可能性があります。また，御社の EC サイトを複製して偽の EC サイトを立ち上げ，①DNS キャッシュポイズニング攻撃と組み合わせて，不正を行うかもしれません。

H 氏は，DNS キャッシュポイズニング攻撃について説明した。

B さん：分かりました。でも，なぜ鍵が他者に知られてしまったのでしょうか。

H 氏　：経緯はまだ分かりません。Q サイトには，サーバ証明書のうち，ある古い暗号ソフトウェア（以下，Z ソフトという）を用いて鍵ペアが生成されたものを対象に秘密鍵の推定を試み，推定に成功したものを掲示している旨の説明がありました。御社は Z ソフトを利用していませんか。②鍵ペアの生成に用いる擬似乱数生成器に必要な条件を，Z ソフトは，満たさないことが分かっています。

〔鍵の危たい化への初動対応〕

H 氏は，次の二つの措置をとるように B さんにアドバイスした。

・当該鍵に関わるサーバ証明書の［　ア　］停止

・当該鍵に関わるサーバ証明書の［　イ　］申請

H 氏は，今後，再び鍵の危たい化が起きた場合に備えて，あらかじめ検討して準備しておくことが望ましい事項について，B さんに説明した。その事項を図 1 に示す。

・鍵の危たい化に対応するための体制，及びその役割と責任（認証局サービス事業者との連携を含む。）
・鍵が危たい化した又はそのおそれがあると判断する基準
・鍵が危たい化した又はそのおそれがあると判断した場合の実施事項
(1) 当該鍵に関わるサーバ証明書の［ア］停止
(2) 当該鍵に関わるサーバ証明書の［イ］申請
(3) 原因の調査
(4) 影響範囲の調査
(5) 原因の除去
(6) ③当該鍵を使用していたサーバの利用者が，自身の被害の可能性を判断できるようにするための情報の公表
(7) その他の必要な是正処置
・システムを復旧させる際の遵守事項
(1) 危たい化した鍵に関わる証明書署名要求（CSR）の再利用禁止
(2) ［e］の生成と，その利用

図1　あらかじめ検討して準備しておくことが望ましい事項

〔H氏による調査及び問題の指摘〕

Bさんは，秘密鍵が他者に知られてしまった原因と，SSL/TLSの利用に関してECサイトの設定などに改善すべき問題がないかについて，H氏に調査を依頼した。

H氏による調査の結果を図2に，暗号スイートの名前の構成を図3に示す。

1. ECサイトの設定など基本情報
・ECサイトのサーバ数：5台
・社外からアクセスできる全てのサーバでSSL/TLSを利用
利用可能なプロトコルのバージョン：SSL 3.0，TLS 1.0，TLS 1.1，TLS 1.2
・サーバの鍵ペアは，Zソフトを利用して生成
鍵ペアは，特定の機器で生成されていた。当該機器にZソフトがインストールされていた。
・SSL/TLSの暗号スイートに，次のものを設定
(1) TLS_RSA_WITH_AES_128_CBC_SHA
(2) TLS_RSA_WITH_AES_128_CBC_SHA256
(3) TLS_RSA_WITH_AES_128_GCM_SHA256
(4) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
(5) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
(6) TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
(省略)
・サーバ証明書は，認証局サービス事業者Y社が発行するドメイン認証証明書を採用
2. 秘密鍵が他者に知られてしまった原因
・鍵ペアの生成にZソフトを利用していたので，Qサイトが推定に成功したと推測
3. SSL/TLSの利用に関して改善すべき問題
問題1　POODLE攻撃に対して脆弱(ぜい)であること
問題2　Perfect Forward Secrecy（以下，PFSという）に対応していないこと
問題3　サーバ証明書にドメイン認証証明書を用いていること

図2　H氏による調査の結果（抜粋）

TLS_RSA_WITH_AES_128_CBC_SHA
(a) (b) (c)

(a) 認証及び鍵交換のアルゴリズム
(b) データ暗号化のアルゴリズム
(c) MAC又はPRF（Pseudorandom Function）のアルゴリズム

図3　暗号スイートの名前の構成（概要）

問題1中のPOODLE攻撃の概要を図4に示す。H氏は，④問題1を解決するために各サーバに施すべき措置を提案した。

・POODLE攻撃によって，攻撃者は，暗号化された通信データの一部を解読し，取得できる。
・中間者攻撃が可能であり，かつ，攻撃対象に大量のデータを送信できることなどの一定の条件を満たす場合に，攻撃が成功する。
・SSL 3.0 プロトコルのパディングチェックの脆弱性を利用して攻撃する。ソフトウェアの開発時に起こり得る実装上のミスによる脆弱性を利用するものではない。
・TLS 1.0 以降のプロトコルについて，同様のパディングチェックの仕組みを突いた攻撃の可能性はあるが，実装上の問題がなければ成功は困難と考えられている。

図4　POODLE攻撃の概要

問題2は，C社がSSL/TLSのハンドシェイクにおいて，⑤PFSの性質をもつ鍵交換方式を利用せず，代わりに，⑥セッション鍵を共有するための秘密情報をクライアントがサーバ証明書に記載されたRSAの公開鍵を用いて暗号化して送信する方式を用いていたことである。

問題3は，サーバ証明書の種類についてである。H氏は，⑦ECサイトが新たに立ち上げたサイトであることを考慮すると，ドメイン認証証明書の選択は妥当でないと指摘した。

〔対策実施と運用見直し〕

Bさんは，H氏の支援を受け，各問題について解決策を検討した。また，M部長の承認の下，図1の事項の検討も進めた。C社は，Qサイトに関わる通報を受けた1か月後には，各問題を解決し，今後起こり得る鍵の危たい化に備えた態勢を整えた。

設問1　〔社外からの通報〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］～［ d ］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　CA 証明書	イ　EV 証明書	ウ　エンコード方式
エ　エンティティ認証	オ　鍵交換	カ　共通鍵暗号
キ　公開鍵	ク　自己解凍	ケ　相互認証証明書
コ　ディジタル署名	サ　ハッシュ関数	シ　メッセージ認証
ス　ルート証明書		

(2) 本文中の下線①について，DNS キャッシュポイズニング攻撃は偽の EC サイトと組み合わせた不正の中でどのような役割を果たすか。40 字以内で具体的に述べよ。

(3) 本文中の下線②について，擬似乱数生成器が生成する乱数列に求められる性質として，適切なものを，解答群の中から選び，記号で答えよ。

解答群

ア　一様分布でない。	イ　規則性がある。
ウ　周期が短い。	エ　予測不可能である。

設問2　〔鍵の危たい化への初動対応〕について，(1)～(3)に答えよ。

(1) 本文中及び図 1 中の［ ア ］，［ イ ］に入れる適切な字句を，それぞれ5字以内で答えよ。

(2) 図 1 中の下線③について，公表すべき情報として，重要なものを二つ挙げ，それぞれ 20 字以内で具体的に述べよ。

(3) 図1中の［ e ］に入れる適切な字句を，7字以内で答えよ。

設問3　〔H 氏による調査及び問題の指摘〕について，(1)～(4)に答えよ。

(1) 本文中の下線④について，H 氏が提案した措置を，20 字以内で述べよ。

(2) 本文中の下線⑤について，SSL/TLS の利用において，PFS の性質をもつ鍵交換方式を解答群の中から全て選び，記号で答えよ。

解答群

ア　AES	イ　CFB	ウ　DHE	エ　DSA
オ　ECDHE	カ　ECDSA	キ　PKCS	ク　RSA

(3) 本文中の下線⑥について，RSA の鍵が危たい化した場合に，当該鍵を用いてハンドシェイクを行った通信に関するリスクは何か。そのリスクの説明として，最も適切なものを解答群の中から選び，記号で答えよ。ここで，攻撃者は，Web ブラウザと Web サーバの通信経路上におり，危たい化前後における通信データを取得していたものとする。

解答群

ア 取得された通信データのうち，鍵が危たい化した時点より前の通信データだけを，復元されるおそれがある。

イ 取得された通信データのうち，鍵が危たい化した時点で通信中だった通信データだけを，復元されるおそれがある。

ウ 取得された通信データのうち，鍵が危たい化した時点より後の通信データだけを，復元されるおそれがある。

エ 取得された通信データの全てを復元されるおそれがある。

(4) 本文中の下線⑦について，妥当でないと指摘した理由を，40 字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 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。ただし，問題冊子を切り離して利用することはできません。
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。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。
なお，試験問題では，™ 及び ® を明記していません。

©2017　独立行政法人情報処理推進機構