# 平成 30 年度 春期 情報処理安全確保支援士

## ＜午後Ⅱ 解答・解説＞

＜問 1＞ セキュリティ対策の評価

■設問 1

(1) 脆弱性の有無によってサーバからのレスポンスに違いがないから（29 字）
(2) スクリプトを分析し，フラグメント識別子の値の変化による挙動を確認する。(35 字)
(3) R ポータルが利用しているスクリプトが Cookie の値を利用している場合（35 字）

(1) DOM-based XSS は，Web ページに含まれる正規のスクリプトにより，動的に Web ページを操作した結果，意図しないスクリプトを Web ページに出力してしまうタイプの XSS 脆弱性。Web ページを構成するオブジェクトを操作する仕組みを DOM と呼ぶことから，DOM-based XSS と呼ばれる。DOM-based XSS では，攻撃者の不正なスクリプト等が Web サイトからの応答中に出力されず，脆弱性の有無によってサーバからのレスポンスに違いがない。そのため，検知方法 1 では検知できない。

(2) 図 4 にあるように，DOM-based XSS の脆弱性があると，攻撃者は"#"から始まるフラグメント識別子に攻撃コードを記述できる。

例えば，"http://www.example.jp/domxss.html"に，次のようなスクリプトを含む HTML がある場合を想定する。

■"http://www.example.jp/domxss.html"の HTML の例

```
<html>
<body>
<script>
 document.write(decodeURIComponent(location.hash));
</script>
</body>
</html>
```

ここで，攻撃者が次のような URL を含むメールを利用者の PC に送り付け，それがクリックされた場合，HTML の 4 行目のスクリプトにより，URL の"#"から始まるフラグメ

©2018 Takayuki Uehara

ント識別子の"#"以降の部分が利用者の PC で実行される。

■攻撃者が送り付ける URL の例

http://www.example.jp/domxss.html#<script>alert(1)</script>

攻撃者が R ポータルサイトで DOM-based XSS 脆弱性の有無を分析する場合，まず，R ポータルにアクセスし，"#"から始まるフラグメント識別子を使うスクリプトの存在を確認する。その後，確認されたスクリプトを分析し，フラグメント識別子の値の変化による挙動を確認することで，当該脆弱性を検知することが可能である。

(3) HttpOnly 属性を付与することにより，Cookie の適用範囲を HTTP/HTTPS 通信だけに限定し，ブラウザ等で実行されたスクリプトが"document.cookie"を用いて Cookie にアクセスすることを禁止する。これにより，XSS 攻撃によって Cookie が窃取されるのを防ぐことが可能となる。しかし，R ポータルが利用しているスクリプトが Cookie の値を利用している場合，HttpOnly 属性を付与することにより，スクリプトから Cookie にアクセスできなくなるため，R ポータルの動作に影響が出ることになる。

■設問 2

**踏み台サーバの操作記録機能によって，ログインした利用者のデスクトップ画面，実行したコマンド，及びキーボード入力を記録する。(61 字)**

図 3 の検出事項 2 にあるように，R 団体では，踏み台サーバを除く全てのサーバの管理者アカウントに共通管理アカウントが使用されている。問題文にあるように，共通管理アカウントを使用する際には，まず PC からリモートデスクトップ機能で踏み台サーバに接続し，職員ごとに発行された管理 ID でログイン後，さらに踏み台サーバからリモートデスクトップ機能で目的のサーバにアクセスし，共通管理アカウントでログインする，という仕組みとなっている。

また，「踏み台サーバには操作記録機能があり，ログインした利用者のデスクトップ画面が数秒間隔で画像データとして記録され，実行したコマンドやキーボード入力がテキストで記録される」とあることから，これを証跡として，共通管理アカウントが正しく利用されていることを確認することが可能である。

©2018 Takayuki Uehara

■設問 3

(1) a：WebAP サーバ
b：DB サーバ
c：ODBC
ルール：9

(2) 人事総務課の職員が踏み台サーバを経由して DB サーバに共通管理者アカウントでログインする行為

(3) d：2

(1) 問題文の冒頭に，「WebAP サーバと DB サーバは ODBC を用いて特定のポート間で通信している」とある。したがって，DB サーバをサーバセグメントに移動した場合，表 5 の追加する FW のフィルタリングルールは，送信元 [ a ] が「WebAP サーバ」，宛先 [ b ] が「DB サーバ」，サービス [ c ] が「ODBC」である。

また，「利用者セグメントから DB サーバへのアクセスは，FW によって運用管理 PC の IP アドレスからのアクセスだけが許可されている」とあり，表 4 の項番 9 のルールがこれに該当するが，DB サーバがサーバセグメントに移動することにより，このルールは不要となる。

(2) 問題文の冒頭にあるように，R 団体のセキュリティ対策基準では「DB サーバには，システム運用課員によるログインと，WebAP サーバからの接続だけが許可されている」とある。ところが，DB サーバがサーバセグメントに移動すると，表 3 の項番 3，4 にあるように，踏み台サーバ及び利用者セグメントの全ての PC からのアクセスが許可されてしまう可能性がある。ただし項番 4 については，表 3 の「アクセス制御方法」にある IP アドレスによるフィルタリングを行うことで，運用管理 PC からのアクセスのみで制限することが可能である。一方，項番 3 の踏み台サーバを経由したアクセスについては，運用管理 PC 以外に，項番 1 で人事総務課の一部の職員の PC からも可能となっており，これを行うと R 団体のセキュリティ対策基準違反となる。したがって解答は，「人事総務課の職員が踏み台サーバを経由して DB サーバに共通管理アカウントでログインする行為」となる。

(3) 図 3 の中で，上記(2)のセキュリティ対策基準違反を発生させる原因の一つとなっているのは，検出事項 2 の「踏み台サーバを除く全てのサーバの管理者用アカウントに，共

©2018 Takayuki Uehara

通管理アカウントが使用されている」ことである。そのため，案 2 を採用する場合は，共通管理アカウントを廃止するなど，検出事項 2 の対策と併せて実施する必要がある。

■設問 4

(1) e：製作パートナに渡す CCI の数（14 字）
(2) f：CC をインストールした PC を協力者宛てに輸送（22 字）
(3) g:DRM サーバへの通信を製作パートナのグローバル IP アドレスからだけに制限する(38 字)

(1) 図 7 のコンテナ方式の利用イメージを見ると，2 つ目の項目に「R 団体は，必要な数の CCI を製作パートナにメディアで渡す」とある。このことから，製作パートナに事前に確認しておくべき事項として「製作パートナに渡す CCI の数」が挙げられる。他に，図 7 の末尾の項目に「仮想デスクトップ環境には CC をインストールすることはできない」とあることから，製作パートナにおける仮想デスクトップ環境の導入状況等についても事前に確認しておく必要があると考えられる。

(2) 図 7 にあるように，コンテナ方式では，CCI で CC をインストール後，認証ダイアログにあらかじめ R 団体から利用者の人数分だけ与えられた CC 用の利用者 ID，パスワードを入力することでコンテナドライブにアクセス可能となる。また，最初にコンテナドライブにアクセスする際，CC の識別情報と PC の端末情報の組がコンテナサーバに登録され，仮に同一の CC を複数台の PC にインストールしても，最初にコンテナドライブにアクセスした 1 台だけがコンテナドライブにアクセスできる仕組みとなっている。そのため，海外の協力者に有効期限内の S 図面を渡そうとした場合には，CC をインストールした PC を協力者宛てに輸送した上で，CC 用の利用者 ID とパスワードを協力者に伝える必要がある。

(3) DRM 方式では，海外の協力者が入手した S 図面を開く場合，協力者の PC 上の DRM 対応の図面アプリを用いるが，その際に協力者の PC と DRM サーバとの間で通信が行われ，認証ダイアログが表示される仕組みとなっている。DRM サーバは R 団体の DMZ 上に設置されているため，FW を用いて，DRM サーバへの通信を必要最小限に制限すればよい。具体的には，FW で DRM サーバへの通信を製作パートナのグローバル IP アドレスからだけに制限することで，海外の協力者による S 図面の不正利用を防ぐことが可能となる。

©2018 Takayuki Uehara

## ＜問 2＞ Web サイトのセキュリティ

### ■設問 1

(1) 攻撃に使われる文字列が POST データ内に含まれている場合（28 字）
(2) a：Web サイト Y の全ファイルと比較（16 字）
(3) 公開鍵認証方式（7 字）

(1) 表 1 にあるように，攻撃手法 K は，特定の文字列を含む HTTP リクエストを送信すると，Web アプリの実行権限で任意のファイルの読出しと書込みができる可能性がある，というものである。攻撃手法 K の HTTP リクエストが GET メソッドで行われている場合には，攻撃に使われる文字列が URL パラメタに含まれるため，Web サーバ X のアクセスログで確認することができる可能性が高い。一方，POST メソッドで行われている場合には，攻撃に使われる文字列が POST データ内（HTTP メッセージボディ）に含まれているため，Web サーバ X の標準設定ではアクセスログに残らないと考えられる。

(2) 問題文にあるように，A 社では，Web サイト X とシステム構成が全く同じ Web サイト Y を，別のデータセンタ Y に設置している。表 1 の No.5 にあるように，Web サイト Y は今回のセキュリティインシデントの影響を受けておらず，改ざんされていないことが確認されている。したがって，Web サイト X の全ファイルを Web サイト Y の全ファイルと比較することで，Web サイト X の改ざんされた箇所を漏れなく確認することができる。

(3) SSH では，パスワードによる認証方式の他に，公開鍵暗号技術を用いた公開鍵認証方式がある。公開鍵認証方式では，あらかじめクライアント側で公開鍵，秘密鍵の鍵ペアを生成し，公開鍵を接続先の SSH サーバに登録しておく。認証に際しては，サーバが乱数を生成した後，クライアントの公開鍵で暗号化し，クライアントに送付する。続いてクライアントが受け取った乱数を自身の秘密鍵で復号した後，サーバ，クライアントで結果を照合し，認証が成立する。

パスワード認証方式では，辞書攻撃によって Web サイト Y に不正にログインされる可能性がある他，認証プロセスにおいてパスワードがネットワーク中を流れるため，パケット盗聴によって攻撃者にパスワードが盗まれ，Web サイト Y に不正にログインされる可能性がある。一方公開鍵認証方式では，辞書攻撃による不正なログインを防げることに加え，認証プロセスにおいてパスワードがネットワーク中を流れないため，パケット盗聴によってパスワードが盗まれるのを防ぐことができる。

©2018 Takayuki Uehara

■設問 2

| |
|---|
| Web サイトで使用している OS，ミドルウェア及び WF の名称並びにそれぞれのバージョン情報（44 字） |

WF 及びプラットフォーム（OS，ミドルウェア）の脆弱性対策として，情報システム部が効率的に脆弱性情報を収集するためには，各 Web サイトで使用している OS，ミドルウェア，WF の名称とそれぞれのバージョン情報を把握しておく必要がある。そのため，各 Web サイトの担当者に当該情報を報告させるとともに，変更が生じた場合にはその都度報告させることにしたのである。

■設問 3

| |
|---|
| c：ディレクトリ（6 字）<br>d：クロスサイト（6 字）<br>e：HTTP（4 字）<br>f：ジャッキング（6 字） |

いずれも典型的な Web アプリケーションの脆弱性を突いた攻撃の名称である。

c：該当するのはディレクトリトラバーサルであるであるため，「ディレクトリ」が入る。
d：該当するのはクロスサイトリクエストフォージェリであるため，「クロスサイト」が入る。
e：該当するのは HTTP ヘッダインジェクションであるため，「HTTP」が入る。
f：該当するのはクリックジャッキングであるため，「ジャッキング」が入る。

■設問 4

| |
|---|
| (1) g：30<br>　　h：0<br>(2) i：イ |

©2018 Takayuki Uehara

(3) j：（う）の操作を実行するときに，code の値を限定商品の値に書き替える（34 字）
(4) k：権限が異なる複数の（9 字）
　　l：許可されている操作の違い（12 字）

(1)
g：表 4 の No.4 で keyword の値が bag であった場合，SQL 文の WHERE 句の内容はシングルコーテーションが付加されて「WHERE keyword = 'bag'」のようになると考えられる。これを実行した結果，該当商品数は 30 件となっている。

同様に，表 4 の No.1 では，SQL 文の WHERE 句の内容は「WHERE keyword = 'bag' and '1'='1'」のようになる。この条件は No.4 と同じ条件であるため，該当商品数は 30 件になる。

一方，表 4 の No.2 では，SQL 文の WHERE 句の内容は「WHERE keyword = 'bag' and '1'='2'」のようになるが，この条件は常に偽となるため，該当商品数は 0 件である。

したがって，［ g ］には 30 ，［ h ］には 0 が入る。

(2) ［ i ］には，警告ダイアログに"NG"を表示されるためのスクリプト文字列が入る。図 9 でこれを実行している行は"<script>"，"</script>"タグで囲まれた中にあるため，解答群ア，エは誤りであることが分かる。また，解答群ウの場合，図 9 の 2 行目は次のようになり，警告ダイアログは表示されない。

```
var returnobj = window.opener.document.getElementById("alert('NG');");
```

一方，解答群イの場合には図 9 の 2 行目は次のようになり，警告ダイアログが表示される。

```
var returnobj = window.opener.document.getElementById('');alert('NG');
```

(3) 表 5 は，有料会員だけが購入できることになっている限定商品を一般会員が購入できてしまう脆弱性を，セキュリティ専門業者が確認した方法である。表 2 の画面遷移を見ると，通常の商品購入時の操作が（う）であり，POST データで code の値をセットし，処理を実行している。一方，限定商品購入時の操作が（え）だが，code の値が異なるのみで，（う）と同じ処理を実行していることが分かる。したがって，セキュリティ専門業者は，（う）の操作を実行するときに，code の値を限定商品の値に書き替えることで，当該脆弱性の存在を確認したと考えられる。

©2018 Takayuki Uehara

(4) 表 5 では，セキュリティ専門業者が一般会員アカウントでログインした後，商品一覧画面で，本来は有料会員にのみ許可されるはずの操作を行い，脆弱性の存在を確認している。このように，図 10 の診断においても，事前に権限の異なる複数のアカウントを用意し，許可されている操作の違いを確認する必要がある。したがって， k には「権限が異なる複数の」， l には「許可されている操作の違い」が入る。

■設問 5

**作業の妥当性を確認できる詳細なレビュー記録を委託先が提出していること（34 字）**

図 11 の「Web セキュリティガイド第 3 版」では，各工程においてレビューポイントが示されている。開発を外部の業者に委託する場合には，詳細なレビュー記録を提出させることで，作業の妥当性を確認する必要がある。したがって，外部に開発を委託する契約の検収条件に追加すべき記載内容は，「作業の妥当性を確認できる詳細なレビュー記録を委託先が提出していること」である。

■設問 6

**脆弱性の作り込原因を調査して，注意すべきポイントを追加する。(31 字)**

問題文にあるように，図 1 の「Web セキュリティガイド第 1 版」では，記載が抽象的であったために実装を誤り，XSS の脆弱性を作り込んでしまったことが分かった。そこで，図 3 の「Web セキュリティガイド第 2 版」では，具体的な実装方法を追加した。また，Web サイト Z で検出された脆弱性が作り込まれた原因はいずれも確認不足であったことから，図 11 の「Web セキュリティガイド第 3 版」では，各工程でのレビューポイントを追加した。このように，診断で見つかった個々の脆弱性から，その作り込原因を調査し，注意すべきポイントを追加することで，Web セキュリティガイドを改善することができる。

©2018 Takayuki Uehara