# 令和６年度　秋期　情報処理安全確保支援士試験　解答例

午後試験

問１

| 出題趣旨 |
|---|
| サイバー攻撃はエンドポイントへの侵入から始まることが多い。攻撃者は，マルウェアを仕掛けた後に，より高い権限の奪取を試みたり，ほかのエンドポイントを探索したりする。そのため，エンドポイントのセキュリティ対策としてログの分析が重要になってきている。<br>インシデント発生時に迅速に対応するためには，どのような攻撃を受けているのかをログから推測・確認する対応力が必要となる。本問では，ソフトウェア開発会社の社内システムの運用及びインシデント対応を題材として，ログを解析する能力及び技術的対策を立案する能力を問う。 |

| 設問 | | 解答例・解答の要点 | | 備考 |
|---|---|---|---|---|
| 設問１ | (1) | a | PC-C | |
| | (2) | b | filesv | |
| | (3) | c | ad01¥user019 | |
| | (4) | d | 無効化 | |
| | (5) | 全てのドメインユーザーに対して，https://△△△.com/，https://□□□.com/及び https://○○○.com/を管理者拒否リストに登録する。 | | |
| | (6) | https://○○○.com/，https://△△△.com/又は https://□□□.com/に通信したＬ社内ホストがないか調査する。 | | |
| | (7) | タスク名が install であるタスクが登録されている L 社内ホストがないか調査する。 | | |
| | (8) | マルウェア対策サービスのログから，マルウェア対策ソフトが停止した L 社内ホストを検出する。 | | 順不同で二つ解答 |
| | | ドメインサーバのログから，RDP 接続をくり返しているＬ社内ホストを検出する。 | | |
| 設問２ | | e | 仮想 PC への RDP 接続に対して，IP アドレスによる接続元制限を行う | |
| | | f | Ｌ社内に DLP を導入し，ファイルの持出しを制限する | |

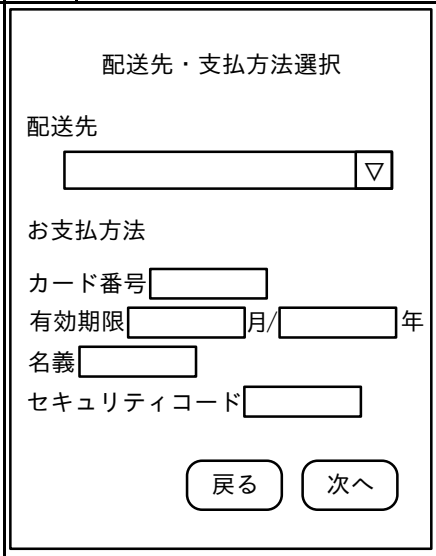
問２

| 出題趣旨 |
| --- |
| 電子メール（以下，メールという）の送信者メールアドレスを詐称したフィッシングが多くなっている。送信者メールアドレスの正当性を判定する対策として DMARC の導入が進んでいる。<br>本問では，メールのドメイン名の変更を機とした新たなメールサービスの導入を題材として，メールサービスの設定及び DMARC の導入を問う。 |

| 設問 | | 解答例・解答の要点 | | 備考 |
| --- | --- | --- | --- | --- |
| 設問１ | (1) | a | A 社ドメイン名 | |
| | (2) | b | 全て | |
| 設問２ | | c | SMTPS | |
| 設問３ | (1) | エ | | |
| | (2) | d | イ | |
| 設問４ | (1) | ソフトウェア修正プログラムに見せかけたマルウェアをダウンロードさせる。 | | |
| | (2) | メール | 社外サービスのパスワード再設定画面の URL が書かれたメール | |
| | | 攻撃 | 任意のパスワードを設定し，アカウントを乗っ取る。 | |
| | (3) | e | ア | |
| 設問５ | (1) | SPF レコードに，T サービスのメール送信元 IP アドレスを追加する。 | | |
| | (2) | SPF | SPF レコードに Y サービスの情報が登録されていないのに，メールが Y サービスから送られる。 | |
| | | DKIM | DKIM レコードの h タグに Subject が含まれているのに，Y サービスでメールの Subject が変わる。 | |

問３

| 出題趣旨 |
| --- |
| Web サイトの改ざんが発生したときには，悪用された脆弱性，影響を受けた利用者及びデータの範囲などを特定し，再発防止策を講じる必要がある。<br>本問では，EC サイトの Web スキミングによるクレジットカード情報の漏えいを題材として，HTML の仕様，ECMAScript の仕様，Web サーバの動作及び Web アプリケーションプログラムの脆弱性に関する知識及び影響を受けた利用者を特定する能力を問う。 |

<table>
<tr><th colspan="2">設問</th><th colspan="3">解答例・解答の要点</th><th>備考</th></tr>
<tr><td colspan="2" rowspan="5">設問１</td><td>a</td><td colspan="2">5</td><td></td></tr>
<tr><td>b</td><td colspan="2">クロスサイトスクリプティング</td><td></td></tr>
<tr><td>c</td><td colspan="2">格納</td><td></td></tr>
<tr><td>d</td><td colspan="2">2</td><td></td></tr>
<tr><td>e</td><td colspan="2">SQL インジェクション</td><td></td></tr>
<tr><td rowspan="4">設問２</td><td>(1)</td><td colspan="3"> 
</td><td></td></tr>
<tr><td rowspan="2">(2)</td><td>パラメータ名</td><td colspan="2">order[Payment]</td><td></td></tr>
<tr><td>値</td><td colspan="2">1</td><td></td></tr>
<tr><td>(3)</td><td colspan="3">addEventListener メソッドで配送先・支払方法選択画面の form 要素にイベントリスナーを登録し，submit 時にクレジットカード情報をクエリパラメータとして i-sha.com に送信する。</td><td></td></tr>
<tr><td rowspan="2">設問３</td><td>(1)</td><td colspan="3">Web サーバのアクセスログのリクエスト URI から情報を取得する。</td><td></td></tr>
<tr><td>(2)</td><td>f</td><td colspan="2">配送先・支払方法選択画面にアクセスしたアカウント名</td><td></td></tr>
</table>

問４

| 出題趣旨 |
|---|
| 脆弱性は一つ一つが軽微でも，複数組み合わせて悪用されると，重大な被害につながることがある。また，診断ツールで検出される脆弱性以外にも，想定される攻撃に対して，セキュリティ対策が不足しているといった脆弱性もある。診断者がこういった脆弱性も報告に含めることで，その後，システムのセキュリティが大きく向上することがある。<br>本問では，個人情報を取り扱う Web サイトに対するセキュリティ診断を題材に，診断ツールで検出された脆弱性について，悪用された場合の被害を想定する能力及び被害を低減するための対策を立案する能力を問う。 |

| 設問 | | | 解答例・解答の要点 | 備考 |
|---|---|---|---|---|
| 設問１ | (1) | a | (イ) | |
| | (2) | b | https://test.△△△.jp/ | |
| | (3) | c | メール受信者によるログイン | |
| | (4) | d | 使用済みの sessionID を無効にした上で，新しい sessionID を発行 | |
| | (5) | e | M サイトへの接続を HTTPS に強制することができる。 | |
| | | f | M サイトのコンテンツに対して，Content-Type ヘッダーで指定した MIME タイプを強制的に適用することができる。 | |
| 設問２ | | g | 画面 09 で，会社名に，図 C の abc@example.com を攻撃者のメールアドレスに変更した文字列を入力して変更ボタンをクリックする。 | |
| | | h | 画面 04 からの一連の操作において，画面 05 又は画面 07 で再設定後のパスワードを入力して，WebAPI キーを確認又は発行する。 | |
| 設問３ | ① | i | 求職者 ID が推測困難なものになるように，求職者 ID の生成方法を変更する。 | ①～③に限らず，WebAPI に関する被害を軽減する仕様の改善方針案が記述されていること |
| | | j | APIkey が窃取された場合，当該求人企業への問合せ又は応募をした求職者の情報漏えいだけに被害を軽減することができるから | |
| | ② | i | WebAPI のアクセス元 IP アドレスを限定して接続を許可するように変更する。 | |
| | | j | WebAPI への第三者による不正なアクセスを防ぐことができるから | |
| | ③ | i | WebAPI で取得できる求職者属性情報は，個人を特定できないものだけに限定するように変更する。 | |
| | | j | 不正に WebAPI が利用されても，個人を特定できない情報の漏えいだけに被害を軽減することができるから | |
| | ④ | k | ログインの認証を，多要素認証に変更する。 | ④～⑥に限らず，Web アプリケーションプログラムに関する被害を軽減する仕様の改善方針案が記述されていること |
| | | l | アカウントの乗っ取りを防ぐことができるから | |
| | ⑤ | k | 利用者ごとにアクセス元 IP アドレスを限定して接続を許可するように変更する。 | |
| | | l | 第三者による不正なアクセスを防ぐことができるから | |
| | ⑥ | k | 求人企業プロパティ変更において，メールアドレス以外を変更した場合でも，メールを送信するように変更する。 | |
| | | l | 不正に求人企業プロパティが変更された場合に気付くことができるから | |