平成 31 年度 春期 情報処理安全確保支援士

＜午後 I 解答・解説＞

＜問 1＞ Web サイトのセキュリティ

●設問 1

［試験センターによる解答例］

(1) a：Same-Origin

(2) b：イ
c：キ
d：ク
※b～d は順不同

(3) Web サイト B へのログイン（13 字）

(1) 悪意のあるサイトに対し、不用意に個人情報や機密情報を送ってしまわないようにするなど、セキュリティ上の理由から、ブラウザの標準的な仕様により、FQDN、スキーム（http、https など）、ポート番号のいずれかが異なるサイトに対してリクエストを送信（クロスドメインリクエスト）できないように制限されている。これを「Same-Origin ポリシ」あるいは「同一生成元ポリシ」と呼ぶ。

(2) 上記のとおり、FQDN、スキーム、ポート番号が入る。

(3) 問題文にあるように、Web サイト B はブランド B の商品を扱う EC サイトであり、10 万名の会員情報を管理している。攻撃者が会員情報を窃取するには、被害者を Web サイト B にログインさせた上で、攻撃者の Web サイトのページにアクセスさせればよい。

●設問２

［試験センターによる解答例］

e：（v）

図２で XMLHttpRequest プロパティの withCredentials の値が true に設定されていた場合、(iii)のプリフライトリクエストが test2.example.com へ送られた後、(iv)で Cookie の送信許可が返され、(v)のメインリクエストの際に、test2.example.com から発行された Cookie が送られる。

●設問３

［試験センターによる解答例］

(1) f：https://site-a.m-sha.co.jp

(2) g：**売れ筋商品情報配信の申込ページのオリジン**（20 字）

(3) h：**Origin ヘッダフィールドの値**（16 字）
i：**許可するオリジンのリスト**（12 字）
j：**一致**（2 字）

(1) Access-Control-Allow-Origin ヘッダフィールドには、Web サイト B が許可するオリジンが設定される。表 1 の No.3 で、プリフライトリクエストの Origin ヘッダフィールドには“https://site-a.m-sha.co.jp”が設定されている、とあることから、Access-Control-Allow-Origin ヘッダフィールドの値は、“https://site-a.m-sha.co.jp”である。

(2) 表 1 にあるように、Web ブラウザは No.1 で Web サイト A の売れ筋商品情報配信の申込ページにアクセスしている。その後 No.3 で Web サイト B にプリフライトリクエストを送信している。したがって、No.5 では、Web ブラウザは、売れ筋商品情報配信の申込ページのオリジンと Access-Control-Allow-Origin ヘッダフィールドの値を照合し、アクセスが許可されていることを確認する。

(3) 問題文に複数のオリジンからのアクセスを許可するために、許可するオリジンのリストを用意しておくことが示されていることから、リクエストの内容と許可するオリジンのリストを突合させることがわかる。プリフライトリクエスト又はメインリクエストにおいて突合する対象となるのは Origin ヘッダフィールドの値であり、リストに一致した値があれば、その値を Access-Control-Allow-Origin ヘッダフィールドに設定する。したがって、［ h ］には「Origin ヘッダフィールドの値」、［ i ］には「許可するオリジンのリスト」、［ j ］には「一致」が入る。

＜問２＞　クラウドサービスのセキュリティ

●設問 1

［試験センターによる解答例］

(1) ホテル Wi-Fi と同じ SSID と事前共有鍵（21 字）

(2) a：メールサービス P
b：攻撃者が用意した Web サーバ

(3) HTTP で接続が開始されたから（15 字）

(1) S さんはホテル Wi-Fi を利用するつもりで攻撃者が用意した無線 LAN に接続させられていた。図 1 に「ホテル Wi-Fi の SSID は、宿泊客で共通であり、その SSID と事前共有鍵はロビーなどの共有スペースに張り出されていた」とあることから、攻撃者はホテル Wi-Fi と同じ SSID と事前共有鍵を設定した偽の無線 LAN アクセスポイントを用意することで、S さんを騙して接続させることに成功したと考えられる。

(2) 図 1、図 2 にあるように、S さんはメールサービス P を利用するために Web ブラウザのアドレスバーにメールサービス P の FQDN を手入力したが、実際には攻撃者が用意した Web サーバに接続させられ、入力した利用者 ID とパスワードを盗まれてしまったと推測される。攻撃者がこれを成功させるには、メールサーバ P の FQDN と攻撃者が用意した Web サーバの IP アドレスを関連付ける A レコードを、自身が用意した DNS サーバに設定していたと考えられる。

(3) HSTS は、Web サイトが、HTTPS でアクセスしたブラウザに対し、次回以降のアクセスにおいて、「max-age」で指定した有効期限（秒単位）まで、HTTP over TLS の使用を強制