平成 31 年度　春期　情報処理安全確保支援士試験　採点講評

午後 I 試験

問 1

問 1 では，Web サイト間の情報連携を題材に，Same-Origin ポリシと CORS（Cross-Origin Resource Sharing）を用いた実装について出題した。

設問 1(1)，(2)は，正答率が低かった。Web サイト A と Web サイト B のオリジンが異なるので，Same-Origin ポリシによって，アクセスは制限される。用語とその意味を適切に理解しておいてほしい。

設問 1(3)は，正答率が低かった。攻撃者が被害者の会員情報を窃取する流れを理解できれば，解答できる問題であった。

設問 3(1)は，CORS の仕組みを理解していない解答が散見された。異なる Origin のリソースにアクセスを許可する際には，CORS を使う場合があるので，理解しておいてほしい。

設問 3(3)は，正答率が高かった。複数のオリジンからのアクセスを許可する場合に，どのように実装すればよいかを，本文から正しく読み取り解答されていた。

問 2

問 2 では，クラウドサービスのセキュリティを題材に，通信を攻撃者に中継され得る環境下での認証方式の強化について出題した。

設問 1(1)，(2)は，全体的に正答率が高かった。攻撃者の用意した無線アクセスポイントに誘導される仕組みについて十分理解されていた。

設問 2(1)は，正答率が低かった。通信を攻撃者に中継され得る環境下では，ネットワーク上を流れる情報は，ワンタイムパスワードのような毎回変わる情報であっても，攻撃者に悪用され得ることを理解しておいてほしい。

設問 2(2)は，正答率が低かった。公開鍵と秘密鍵を取り違えている解答が散見された。ディジタル署名の仕組みについて理解しておいてほしい。

設問 2(3)は，正答率が低かった。中間者攻撃では偽装できない情報が何かを考えれば，解答できる問題であった。被害者が署名したデータを攻撃者がそのまま悪用することを想定していない，“攻撃者が入手できないオーセンティケータの秘密鍵で署名しているから”といった解答が一部に見られた。

問 3

問 3 では，IoT 機器を題材に，サーバ間での認証連携，及び IoT 機器への物理的な不正アクセスへの対策について出題した。

設問 2(1)は，正答率が高かった。本問のような認証連携方式では，利用を許可するリソースの範囲を認証トークンに含める必要があることについて，よく理解されていた。

設問 2(4)は，正答率が高かったが，公開鍵と秘密鍵を取り違えている解答が一部に見られた。公開鍵暗号方式やディジタル署名はセキュリティ技術の基礎なので，よく理解しておいてほしい。

設問 3 は，ハッシュ値リストを保護するために TPM（Trusted Platform Module）を用いる解答を期待したが，ディジタル署名の付与についてだけ記述し，秘密鍵の保護を考慮していない解答が散見された。ハッシュ値リストにディジタル署名を付与した場合，秘密鍵が盗まれてしまうと，不正にディジタル署名を付与され，データの改ざんを検出できなくなってしまうおそれがある。IoT 機器では特に物理的な不正アクセスへの対策が重要になるので，TPM 及び設問 2(6)で出題した耐タンパ性についてよく理解しておいてほしい。