＜問 3＞ スマートフォンアプリケーションの試験

■設問 1

〔試験センターによる解答例〕

(1) a：S サーバ

(2) b：試験用 Web サーバ

(3) c：試験の実施よりも前の日時（12 字）

(4) d：S アプリがサーバ認証エラー画面を表示する。(21 字)

(1), (2)図 2 に，「S アプリ内に，S サーバの FQDN が組み込まれている」とあり，図 3 の

サーバ証明書の検証試験環境では，S サーバに代わって試験用 Web サーバが接続先となることから，［ a ］には「**S サーバ**」，［ b ］には「**試験用 Web サーバ**」が入る。

(3)表 2 の項番 2 では，サーバ証明書が有効期間内でないことの検出を行う。したがって，サーバ証明書の「有効期間の終了」には，**試験の実施よりも前の日時**を設定する必要がある。

(4)表 2 の各試験において期待される結果は，「S アプリがサーバ証明書を認証できない」である。図 2 にあるように，S アプリが S サーバを認証できなかった場合は，サーバ認証エラー画面を表示する仕様になっている。したがって，［ d ］には「**S アプリがサーバ認証エラー画面を表示する。**」が入る。

■設問２

〔試験センターによる解答例〕

(1) e : 1, 2, 3, 4

f : 3

g : 1

(2) SSID，暗号化方式と事前共有鍵に，公衆無線 LAN で使用されているものを設定する。（41 字）

(1)

e：発行者の検証不備があると，表 3 で発行者が「攻撃者が準備するプライベート認証局」であっても認証が成立する。さらにサブジェクトのコモンネームの検証不備があると，表 3 でサブジェクトのコモンネームが「攻撃者が所有しているドメインを使用した FQDN」や「上記二つ以外の FQDN」であっても認証が成立する。したがって，表 4 の項番 1 では，表 3 の **1，2，3，4** の全ての証明書で中間者攻撃が成功する。

f：発行者の検証不備があると，表 3 で発行者が「攻撃者が準備するプライベート認証局」であっても認証が成立するが，サブジェクトのコモンネームの検証不備がなければ，サブジェクトのコモンネームが「S サーバの FQDN」の場合のみ認証が成立する。したがって，表 4 の項番 2 では，表 3 の **3** の証明書のみ中間者攻撃が成功する。

g：サブジェクトのコモンネームの検証不備があると，表 3 でサブジェクトのコモンネームが「攻撃者が所有しているドメインを使用した FQDN」や「上記二つ以外の FQDN」であ

っても認証が成立するが，発行者の検証不備がなければ，発行者が「スマートフォンに対応している商用認証局」の場合のみ認証が成立する。したがって，表 4 の項番 3 では，表 3 の 1 の証明書のみ中間者攻撃が成功する。

(2)無線 LAN に自動的に接続するためには，アクセスポイントの SSID を認識しており，かつ，使用している暗号化方式（WEP，WPA，WPA2 など），そして各々の暗号化方式で使用する事前共有鍵を設定しておく必要がある。したがって，W-AP の **SSID，暗号化方式，事前共有鍵に，公衆無線 LAN で使用されているものを設定**すれば，公衆無線 LAN の利用者のスマートフォンを自動的に W-AP に接続させることができてしまう。