＜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

させる機構である。メールサービスPにはHSTSは実装されておらず、HTTPでアクセスした場合はHTTP over TLSのURLにリダイレクトされる仕様となっていた。これらのことから、Sさんは日頃からメールサーバPにアクセスする際にHTTPでFQDNを入力していたため、攻撃者が用意したWebサーバとHTTPで接続が開始され、サーバ証明書が信頼できない旨のエラーが表示されなかったと考えられる。

●設問2

[試験センターによる解答例]

(1) OTPの入力を要求し、OTPを認証サーバXに中継する処理（28字）

(2) c：ウ
d：ア
e：エ
f：イ

(3) 認証サーバXでオリジンbとオリジンsの一致を確認しているから（30字）

(1) 要求 2 は、手口 G に限らず、偽サイトにアクセスしてしまったときにフィッシングの手口によるメールサービス P への不正アクセスを防ぐことである。図 4 の OTP 認証方式の認証処理において、攻撃者が利用者と認証サーバ X との間に介在して OTP の入力を要求し、利用者が入力した OTP を認証サーバ X に中継した場合、メールサーバ P への不正アクセスが成立する可能性がある。

(2) c：図 5 の注 1 に「オーセンティケータには，搭載されたデバイスごとにユニークな公開鍵 A，秘密鍵 A，及び証明書 A が組み込まれている」とあることからわかるように、オーセンティケータの登録処理において署名 L を生成する際には、秘密鍵 A を用いる。

d：秘密鍵 A を用いて生成された署名 L を検証するには、公開鍵 A を用いる。

e：図 5 中に「利用者 ID とドメインの組みに対して IDc を発行」「IDc ごとの公開鍵 K，秘密鍵 K を生成」とあることからわかるように、図 6 のパスワードレス認証方式の認証処理においては、オーセンティケータでは利用者 ID とドメインの組みに対する IDc 及び秘密鍵 K を取得後、秘密鍵 K を用いて署名 M を生成する。

f：秘密鍵 K を用いて生成された署名 M を検証するには、公開鍵 K を用いる。

(3) 図 6 にあるように、パスワードレス認証方式では、認証サーバ X で、Web ブラウザがアクセスした Web サイトのオリジンであるオリジン b と、認証サーバ X の Web サイトのオリジンであるオリジン s の一致を確認している。利用者が攻撃者のフィッシングサイトなどにアクセスした場合には、オリジン b とオリジン s が一致しなくなるため、攻撃者によるメールサーバ P への不正アクセスを防ぐことが可能と考えられる。

＜問３＞　IoT 機器の開発

●設問 1

［試験センターによる解答例］

エ