＜解説＞

(1) GET メソッドでは、リクエストされた文字列は URL に含まれるため、アクセスログに記録される。一方、POST メソッドを用いた場合は、リクエストされた文字列は HTTP のメッセージボディにセットされ、URL には含まれない。そのため、実行された OS コマンドをアクセスログから確認することはできない。

(2) 問題文より、tar コマンドには任意の OS コマンドを実行できるオプションがあるが、ファームウェアのアップデート時にはこのオプションは使用していないことがわかる。したがって、sudo コマンドの設定ファイルで、このオプションを受け付けないように設定することで、悪用されるのを防ぐのが有効な対策となる。

●設問４

［試験センターによる解答例］

h：・noindex（7 字）
　　・none（4 字）

＜解説＞

検索エンジンに登録する Web サイトの情報を収集する自動巡回（ロボット）型のプログラムをクローラと呼ぶ。検索エンジンで検索されないように設定するには、対象となる Web ページの <head> セクションに <meta name="robots" content="noindex"> を記載する。これにより、設定したページが検索結果に表示されないようになる。また、"noindex"の部分を"nofollow"にすると、クローラに対してリンクをたどらせないようにすることができる。そして、同じ部分を"none"にすると、"noindex"と"nofollow"の両方を設定することができる。したがって、"noindex"か"none"が解答となる。

＜問３＞　スマートフォン向け QR コード決済サービスの開発

●設問１

［試験センターによる解答例］

a：イ
b：ア

＜解説＞

a：身元確認は、"登録する氏名・住所・生年月日等が正しいことを証明／確認すること"であるから、アカウント作成時に実施する。

b：当人認証は、"認証の 3 要素のいずれかの照合で、その人が作業していることを示すこと"であるから、Q サービスへのログイン時に実施する。

●設問２

［試験センターによる解答例］
(1)・漏えいしている口座番号と暗証番号を悪用する方法（23 字）
　・口座番号と暗証番号をだまして聞き出し、悪用する方法（25 字）
(2) c：写真（2 字）
(3) d：ウ
　 e：イ
(4) f：・署名用電子証明書の有効性（12 字）
　　・署名用電子証明書の失効の有無（14 字）
(5) g：そのランダムな数字を紙に書き、その紙と一緒に容貌や本人確認書類を撮影（34 字）

＜解説＞

(1) 表 1 の「銀行口座とのひも付け」にあるように、口座番号とキャッシュカードの数字 4 桁の暗証番号で Q サービスとのひも付けができる。この仕組みを使って攻撃者が他人の銀行口座とのひも付けを行う方法としては、既に何らかの理由で漏えいしている口座番号と暗証番号を入手し、悪用することが考えられる。または、フィッシング詐欺などの手口で口座番号と暗証番号を当人から聞き出し、悪用することも考えられる。

(2) 本人確認を行う際に通常用いられているように、[c]には"写真"が入る。なお、「犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概要」において、本人確認書類を用いた方法として表 2 の項番 1～4 が挙げられている。

(3) d：デジタル署名を行う際に使用するのは秘密鍵である。
　 e：デジタル署名の検証に用いるのは公開鍵である。なお、Q サービス利用者の公開鍵は Q サービスに送付された署名用電子証明書に含まれている。

(4) 電子証明書を用いた認証システムやデジタル署名を利用する際には、使用する電子証明書の有効性（期限切れや失効等が発生していないか）について確認する必要がある。IPA が公開している採点講評に記載されているが、公的個人認証サービスでは、電子証明書の失効有無の確認について、地方公共団体情報システム機構（J-LIS）が OCSP による方法と CRL による方法を提供している。

(5) 事前に準備した他人の画像を用いられないようにするには、認証時に撮影された利用者の容貌が確認できる画像を用いる必要がある。その際に、Q アプリが表示したランダムな数字を利用者が紙に書き、その紙と利用者の本人確認書類を合わせて撮影するようにすれば、第三者によるなりすましのリスクを低減することができる。

●設問３

［試験センターによる解答例］
(1) スマートフォンを盗まれた場合（14 字）
(2) Q アプリの起動時に、PIN コードで利用者を認証する機能（27 字）

＜解説＞

(1) Q サービスにログインした状態で、スマートフォンの画面ロックを設定していなかったとすれば、そのスマートフォンが盗まれた場合には Q サービスが不正利用される可能性が高い。

(2) Q サービスにログインした状態を保持した上で、Q アプリの不正利用を防ぐには、アプリの起動時にサービス利用者しか知らない情報等を入力させる方法が考えられる。4～8 桁程度の PIN コードであれば、利用者の利便性に大きく影響を及ぼすことなく、スマートフォン盗難時等の不正利用を防ぐ効果が期待できる。