問3　スマートフォン向けQRコード決済サービスの開発に関する次の記述を読んで，設問1～3に答えよ。

L社は，様々なWebサービスを提供している従業員8,000名の企業である。市場環境の変化に合わせ，L社は，QRコードを利用した実店舗向けの決済サービス（以下，Qサービスという）を提供することを決め，Qサービス用のサーバプログラムと，Qサービスを利用するためのスマートフォン向けアプリケーションプログラム（以下，Qアプリという）を開発することになった。

システム開発部門のBさんは，Qサービス用のサーバプログラム及びQアプリの開発責任者に任命された。

〔Qサービス用のサーバプログラム及びQアプリの概要〕

Qサービス用のサーバプログラム及びQアプリの機能ごとの概要を表1に示す。

表1　Qサービス用のサーバプログラム及びQアプリの機能ごとの概要

機能	概要
アカウント作成	・Qサービスのアカウント情報として，利用者IDとパスワード，氏名，生年月日，携帯電話番号を登録する。
Qサービスへのログイン	・利用者IDとパスワードでQサービスにログインする。ログインに連続して5回失敗すると，アカウントが一時的にロックされる。
銀行口座とのひも付け	・利用者の銀行口座とのひも付けを行う。手順を次に示す。 (1)　Qアプリ上では，Qサービスの連携先としてあらかじめL社と契約した銀行がリストされている。利用者は，そのリストから銀行を一つ選択する。選択された銀行には，利用者を認証するために，Qサービスを介してアカウント情報の氏名が提供される。 (2)　次に，当該銀行が運用する口座振替登録用のWeb画面が開かれるので，利用者は，口座番号，キャッシュカードの数字4桁の暗証番号を入力する。 (3)　(1)で提供された情報と(2)で入力された情報が共に正しければ認証に成功し，アカウントと利用者の銀行口座とのひも付けが完了する。連続して認証に5回失敗すると，当該口座とのひも付けができなくなる。
チャージ	・ひも付けた銀行口座から，指定した金額をQサービスのアカウントに入金する。
決済	・利用者がQアプリでQRコードを表示する。コンビニエンスストアなどの店舗は専用機器を使って当該QRコードを読み取り，決済する。支払には，Qサービスのアカウントの残高が利用される。 ・Qアプリ上のQRコードは，Qサービスが自動的に生成する。

表1　Qサービス用のサーバプログラム及びQアプリの機能ごとの概要（続き）

機能	概要
利用者間の送金[1)]	・送金する相手の携帯電話番号と送金する金額を指定して送金する。送金には，Qサービスのアカウントの残高が利用される。

注記　銀行口座とのひも付け，チャージ，決済，利用者間の送金を行うには，Q サービスへのログインが必要である。

注[1)]　将来追加予定の機能である。

〔本人確認〕

Bさんは，上司である情報処理安全確保支援士（登録セキスペ）のC課長に表1をレビューしてもらった。C課長は，Qサービス及びQアプリが他人名義で利用されたり，他人のアカウントで不正にログインされたりすることを防ぐためには，表1のアカウント作成と Q サービスへのログインの方法では本人確認が不十分であると指摘した。

C 課長は，経済産業省が 2020 年に公表した“オンラインサービスにおける身元確認手法の整理に関する検討報告書”を確認するように指示した。当該報告書では，本人確認の構成要素は，身元確認と当人認証であると整理されている。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”と定義されている。また，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”と定義されている。したがって，Qサービスにおいては，表1の［　a　］時に身元確認を，表1の［　b　］時に当人認証を実施することになる。

〔身元確認〕

B さんは，身元確認についてどのような方法があるのかを調査したところ，“犯罪による収益の移転防止に関する法律施行規則”（以下，犯収法規則という）に規定があることが分かった。犯収法規則の規定を参考にすると，銀行側が利用者の身元確認を行い，かつ，銀行がその記録を保存していることをL社が確認すれば，Qサービスの［　a　］時の身元確認を実施したとみなせるとBさんは考え，C課長に相談した。

C課長は，表1の銀行口座とのひも付けでは，キャッシュカードの所持が確認されず，暗証番号で照合されるだけなので，攻撃者が他人の氏名でアカウント作成を行

い，①他人の銀行口座とのひも付けを行うリスクを低減するためには，L社が表1の［ a ］時に身元確認を実施する必要があると指摘した。

L社には対面で身元確認できる店舗がなく，身元確認の手続を郵送で行うことになると，利用者がQサービスを利用するまでに時間が掛かる。Bさんは，身元確認をオンラインで行う方法をC課長に相談した。

C課長は，将来，Qサービスには利用者間の送金機能などが追加されることを考慮し，金融庁が公表している“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”の個人顧客向けの本人確認方法が採用できると考えた。そこで，表2のように整理してBさんに説明した。

表2　個人顧客向けの本人確認方法

項番	分類	方法
1	本人確認書類を用いた方法	次の2点を用いた方法 ・［ c ］付き本人確認書類の画像 ・容貌の画像
2		次の2点を用いた方法 ・［ c ］付き本人確認書類のICチップ情報 ・容貌の画像
3		次の2点を用いた方法 ・本人確認書類の画像又はICチップ情報 ・銀行等への顧客情報の照会
4		次の2点を用いた方法 ・本人確認書類の画像又はICチップ情報 ・顧客名義口座への振込み
5	電子証明書を用いた方法	公的個人認証サービスの署名用電子証明書[1)]を用いた方法
6		民間事業者発行の電子証明書を用いた方法

注[1)]　マイナンバーカードに記録された署名用電子証明書

次は，表2についてのBさん及びC課長の会話である。

Bさん：項番5のセキュリティが強固だと思うので，項番5をQサービスに導入する場合の本人確認方法について詳しく教えてください。

C課長：マイナンバーカードには，地方公共団体情報システム機構が発行した署名用電子証明書などが格納されている。Q サービスの利用者は，NFC 機能のあるスマートフォンを利用して，マイナンバーカードを読み取り，署名用

電子証明書のパスワードを Q アプリに入力する。入力されたパスワードが正しい場合，マイナンバーカード内の［ d ］で Q サービスの申込用のデータにデジタル署名し，当該デジタル署名，当該データ本体，署名用電子証明書を Q サービスに送付する。Q サービス側で，デジタル署名が利用者本人のものであり，改ざんされていないことを Q サービスの利用者の［ e ］を用いて確認した後，地方公共団体情報システム機構に［ f ］を確認する。

B さん：項番 5 の方法では，利用者が NFC 機能のあるスマートフォンとマイナンバーカードを用意する必要があるのですね。それならば，項番 1 の方が，利用者にとっては利用しやすい方法と言えそうです。項番 1 では，注意点はありますか。

C 課長：項番 1 では事前に準備した他人の画像を用いられないようにする必要がある。

B さん：どうすればよいでしょうか。

C 課長：完全な対策はないが，政府が犯収法規則の改正において意見公募を実施した際の“警察庁及び共管各省庁の考え方”に記載されている方法を採用すると，“Q アプリが毎回ランダムな数字を表示し，利用者が［ g ］して，直ちに送信することによって，L 社では提出された画像が事前に準備されたものではないことを確認する”という方法が考えられる。この方法で身元確認しよう。

B さん：分かりました。

〔当人認証〕

B さんは，Q サービスの当人認証を強化する方法を検討し，利用者 ID とパスワードによる認証後に SMS で認証コードを利用者に送り，入力させる方法を実装することを考えた。

一方，利便性を向上させるために，ログインが成功した場合は，1 か月間，ログイン状態を保持することを考えた。しかし，②Q 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いと，Q サービスが不正利用されることがある。そこで，Q サービスにログインした状態を保持することにした上で，③Q アプリに不正利用を防ぐための機能を追加することにした。

これまでの検討を踏まえ，Bさんは，Qサービス用のサーバプログラムとQアプリの開発を進めた。

設問1　本文中の［　a　］，［　b　］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　Qサービスへのログイン　　イ　アカウント作成

設問2　〔身元確認〕について，(1)～(5)に答えよ。

(1) 本文中の下線①について，攻撃者はどのようにして他人の銀行口座とのひも付けを成功させるか。その方法を二つ挙げ，それぞれ30字以内で述べよ。

(2) 表2中の［　c　］に入れる適切な字句を，5字以内で答えよ。

(3) 本文中の［　d　］，［　e　］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　共通鍵　　イ　公開鍵　　ウ　秘密鍵

(4) 本文中の［　f　］に入れる適切な字句を，15字以内で述べよ。

(5) 本文中の［　g　］に入れる適切な字句を，40字以内で述べよ。

設問3　〔当人認証〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，スマートフォンの画面ロックを設定していないと，どのような場合に不正利用が行われるか。20字以内で具体的に述べよ。

(2) 本文中の下線③について，どのような機能が考えられるか。30字以内で具体的に述べよ。