SC

令和４年度　春期
情報処理安全確保支援士試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1 時間 30 分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問１～問３
選択方法	２問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。3 問とも○印で囲んだ場合は，はじめの 2 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問１，問３を選択した場合の例〕

選択欄	
２問選択	(問１)
	問２
	(問３)

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　Webアプリケーションプログラム開発のセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

H社は，Webアプリケーションプログラム（以下，Webアプリという）を開発する従業員200名の会社である。H社では，開発部がWebアプリを開発し，情報セキュリティ部が，表1に示す方法に従って，脆弱性検査を実施する。

表1　脆弱性検査の方法（抜粋）

項番	脆弱性	検査の方法	脆弱性が検出された場合の対策方法
1	HTTP ヘッダインジェクション	利用者の入力を基にHTTPレスポンスヘッダを生成する処理において，①改行コードを意味する文字列を入力したときに，HTTP ヘッダフィールドが追加されないことを確認する。 （省略）	（省略）
2	SQL インジェクション	（省略）	SQL 文の組立てにおいて，SQL 文のひな形の中に②変数の場所を示す？記号を置く技法を利用する。
3	メールヘッダインジェクション	（省略）	次のいずれかの対策を実施する。 (1)　メールヘッダを固定値にする。 (2)　外部からの入力を適切に処理するメール送信用APIを使用する。 (3)　外部からの入力の全てについて，［　a　］を削除する。

開発部では，自部で開発したSシステムというWebシステムを利用して，コーディングルールなどの社内ルールを含む各種の情報を共有している。Sシステムの利用者は，ログイン後に情報の投稿と表示を行うことができる。投稿された情報はデータベースに格納される。

ログインから情報表示までのSシステムの画面遷移を表2に示す。

表2　ログインから情報表示までのSシステムの画面遷移

項番	利用者の操作	操作の結果
1	Sシステムのログイン画面にアクセスし，利用者IDとパスワードを入力する。	ログインが成功すると，次の画面がWebブラウザに表示される。なお，下線はリンクであることを示している。 URL　https://（省略）/menu ・情報の投稿 ・情報の表示 （省略）
2	表示された画面の“情報の表示”をクリックする。	“情報選択機能”が呼び出され，次の画面がWebブラウザに表示される。プルダウンには，表示できる情報の情報番号と情報名がリストされる。 URL　https://（省略）/select 表示したい情報の情報番号，情報名を選んでください。 ▼ 番号1001　コーディングルール ⋮ 表示
3	プルダウンから表示したい情報を選択し，“表示”ボタンをクリックする。	“情報表示機能”が呼び出され，次の画面[1)]がWebブラウザに表示される。 URL　https://（省略）/show?no=1001 番号1001 コーディングルール （省略）

注記　利用者のログイン後，セッションIDでセッション管理を行っている。セッションIDは，ログイン時に発行される推測困難な値であり，secure属性が付与されたcookieに格納される。

注[1)]　プルダウンから，表示したい情報として“番号 1001 コーディングルール”を選択した場合を示している。

〔Sシステムの改修におけるアクセス制御要件の追加〕

開発部で新しいプロジェクトを立ち上げることになり，開発部の各プロジェクト内の情報共有を強化することにした。開発部は，次のようにSシステムを改修する方針とした。

・社内ルールだけでなく，各プロジェクトの計画書や各種の設計情報を各プロジェ

クト内で共有できるようにする。

・各プロジェクトの計画書や各種の設計情報については，情報が表示できる利用者を，情報の作成者と同じプロジェクトに参加する利用者に限定できるようにする。

なお，開発部員は，一時期には一つのプロジェクトだけに参加する。同時に複数のプロジェクトには参加しない。

開発部のDさんが，Sシステム改修の担当者に任命され，利用者のアクセス制御を次のように設計した。

・プロジェクトを識別するプロジェクトIDを連番で採番する。

・利用者 ID それぞれに対して，その利用者が参加するプロジェクトのプロジェクトIDを登録しておく。

・S システムに格納される各情報に，作成者の参加するプロジェクトを示すプロジェクトIDをあらかじめ付与しておく。

・プロジェクトIDを次に示す方法で取得し，そのプロジェクトIDを用いてアクセス制御する。

方法1：ログイン時にその利用者IDに対して登録されているプロジェクトIDを取得し，GET リクエストのクエリ文字列に，“id=プロジェクト ID”の形式で指定する。情報選択機能は，クエリ文字列からプロジェクト ID を取得する。

〔情報選択機能の脆弱性〕

S システム改修後の脆弱性検査で，情報セキュリティ部は，プロジェクトの情報番号と情報名を，そのプロジェクトには参加していない利用者が，③そのプロジェクトに参加しているかのように偽ってリスト可能であるという脆弱性を指摘した。これは，情報選択機能においてクエリ文字列で受け取ったプロジェクト ID をチェックせずに利用していることに起因していた。この指摘を受けて，Dさんは，プロジェクトIDの取得方法として，次に示す別の方法を提示した。

方法2：情報選択機能の利用時に，セッション情報から利用者情報を取得する。情報選択機能は，当該利用者情報からプロジェクトIDを取得する。

情報セキュリティ部は，④方法1の脆弱性が方法2で解決されることを確認した。Dさんは，プロジェクトIDの取得方法を方法2に修正した。

情報選択機能及び情報表示機能が参照するデータベースのE-R図を図1に，修正後の情報選択機能のソースコードを図2に示す。

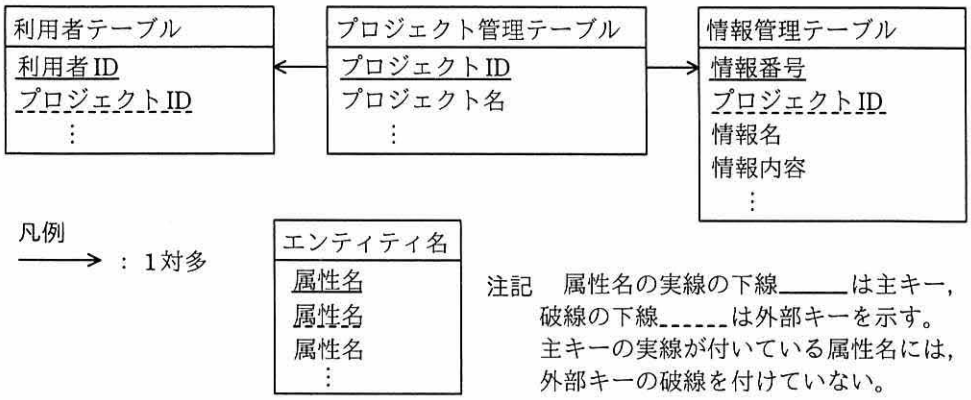

図1　参照するデータベースのE-R図

```
   （省略）  // package宣言，import宣言など
 1: public class SelectServlet extends HttpServlet {
     （省略）  // 変数の宣言やメソッドの定義など
 2:    protected void doGet(HttpServletRequest request, HttpServletResponse response)
   throws ServletException, IOException {
 3:       java.sql.Connection con = null;
 4:       try {
          （省略）  // 初期化処理など
 5:          con = java.sql.DriverManager.getConnection( （省略） );  // データベースに接
   続する処理
 6:          int projectId = （省略）;  // 利用者の参加プロジェクトのプロジェクトIDを利用
   者テーブルから取得し，代入する処理
 7:          String sql = "SELECT 情報番号，情報名 FROM 情報管理テーブル WHERE プロジェ
   クトID = ?";
 8:          java.sql. [ b ] stmt = con.prepareStatement(sql);
 9:          [ c ].setInt(1, projectId);
10:          java.sql.ResultSet rs = stmt.executeQuery();
          （省略）  // 例外処理やその他の処理
```

図2　修正後の情報選択機能のソースコード

〔情報表示機能の脆弱性〕

情報セキュリティ部は，情報表示機能にも情報選択機能と同様の脆弱性があることを指摘した。D さんは，情報表示機能にも同様の修正を行った。修正後の情報表示機能のソースコードを図 3 に示す。

```
   (省略)  // package宣言, import宣言など
 1: public class ShowServlet extends HttpServlet {
     (省略)  // 変数の宣言やメソッドの定義など
 2:   protected void doGet(HttpServletRequest request, HttpServletResponse response)
   throws ServletException, IOException {
 3:      int documentNo = Integer.parseInt(request.getParameter("no"));
 4:      java.sql.Connection con = null;
 5:      try {
          (省略)  // 初期化処理など
 6:        con = java.sql.DriverManager.getConnection( (省略) );  // データベースに接
   続する処理
 7:        int projectId = (省略);  // 利用者の参加プロジェクトのプロジェクトIDを利用
   者テーブルから取得し，代入する処理
 8:        String sql = "SELECT 情報番号, 情報名, 情報内容 FROM 情報管理テーブル WHERE
     [ d ] ";
 9:        java.sql.[ b ] stmt = con.prepareStatement(sql);
          (省略)  // SQL文のひな型に変数を代入する処理
10:        java.sql.ResultSet rs = stmt.executeQuery();
          (省略)  // 例外処理やその他の処理
```

注記　10 行目より後の（省略）に，projectId，documentNo を用いた処理はない。

図 3　修正後の情報表示機能のソースコード

情報セキュリティ部による脆弱性検査に合格後，S システムの改修版がリリースされ，各プロジェクト内の情報共有が強化された。

設問 1　表 1 について，(1)～(3)に答えよ。

(1) 表 1 中の下線①について，適切な文字列の例を，解答群の中から選び，記号で答えよ。

解答群

ア　%0D%0A　　イ　%20　　ウ　
　　エ　<p>

(2) 表 1 中の下線②について，名称を，10 字以内で答えよ。

(3) 表 1 中の [a] に入れる適切な字句を，5 字以内で答えよ。

設問２　〔情報選択機能の脆弱性〕について，(1)～(4)に答えよ。

(1) 本文中の下線③について，未参加のプロジェクトに参加しているかのように偽るための操作を，40 字以内で具体的に述べよ。

(2) 本文中の下線④について，方法 1 の脆弱性が方法 2 で解決されるのはなぜか。30 字以内で述べよ。

(3) 図 2 中及び図 3 中の［ 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 Connection　　イ DriverManager

ウ PreparedStatement　　エ Statement

(4) 図 2 中の［ c ］に入れる適切な字句を答えよ。

設問３　図 3 中の［ d ］に入れる適切な字句を，図 1 中の属性名を含めて答えよ。

問2　セキュリティインシデント対応に関する次の記述を読んで，設問1～4に答えよ。

Z社は，Network Attached Storage（NAS）製品，ルータ製品などのネットワーク機器を開発，保守している従業員200名の会社であり，国内の中小企業の顧客を中心に事業を展開している。NAS製品である製品Xは，ファイル共有の用途で利用され，ルータ製品である製品Yは，インターネット接続の用途で利用されている。製品X及び製品Yは，Linuxをベースとした OS を搭載している。

Z社では，インターネットドメイン名 z-sha.co.jp を取得している。製品Xの利用者は，インターネットから Web インタフェース経由で自身の製品Xにアクセスするに際して，Z社が提供しているダイナミック DNS サービス（以下，DDNS-Zという）を利用することができる。

〔障害の発生〕

ある日，製品Xと製品Yを利用しているA社から，Z社の保守サポート窓口に障害の報告が入った。製品X（以下，A社に設置された製品Xを NAS-A という）上のファイルにおいて，ファイル名は表示されるがファイルを開くことができないとのことであった。

障害報告によると，A社は，オフィス環境のデザイン及び施工を行う従業員30名の会社であり，デザインデータのファイルを NAS-A に保存して社内で共有している。在宅勤務者の増加に伴い，7日前に，NAS-A及び製品Y（以下，A社に設置された製品Yをルータ-Aという）の設定を変更して，A社の従業員の自宅から NAS-A 上のファイルにアクセスできるようにしていた。

〔NAS-A及びルータ-Aの調査〕

Z社の保守サポート課のK氏は，A社の障害調査を担当することになった。

NAS-Aは，DDNS-Zを使用して，https://nas-a.z-sha.co.jp/ の URL でアクセスできるようになっていた。ルータ-A のグローバル IP アドレスが変更された場合，Z社の DNS サーバの設定でホスト名 nas-a に割り当てている IP アドレスを変更するために，［　a　］レコードを更新する。そのレコードの［　b　］は，300秒に設定されていた。

A 社のネットワーク構成を図 1 に，NAS-A の設定内容を表 1 に，ルータ-A の設定内容を表 2 に示す。

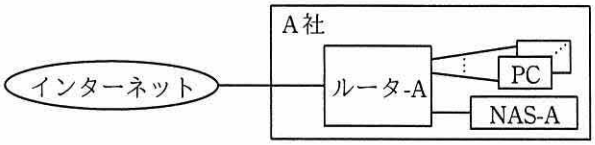

図 1　A 社のネットワーク構成（抜粋）

表 1　NAS-A の設定内容（抜粋）

設定項目	設定値	説明
ファイル共有機能	・SMB：有効 ・NFS：無効	有効に設定したプロトコルで，ファイルを共有する。
UPnP [1] 設定要求機能	・有効 ・製品 Y の WAN 側 TCP ポート：443 ・NAS-A の TCP ポート：443	左記の設定にすると，製品 Y の WAN 側ポート宛てのパケットを NAS-A のポートにフォワードする設定を製品 Y に要求する。
Web 操作機能	・有効	Web ブラウザから HTTPS で，一般利用者権限のアカウントで本機能にログイン後，ファイルの操作ができる。
Web 管理機能	・有効	Web ブラウザから HTTP で，管理者権限のアカウントで本機能にログイン後，NAS-A の設定変更などができる。

注 [1]　Universal Plug and Play の略称。認証なしでリクエストを受け付ける仕様のプロトコルである。

表 2　ルータ-A の設定内容（抜粋）

設定項目	設定値	説明
ファイアウォール機能	・インバウンド通信：全て拒否 [1] ・アウトバウンド通信：全て許可	ステートフルパケットインスペクション型である。
UPnP 機能	・LAN 側：有効	LAN 側の機器から受け付けたリクエストの内容で，ポートフォワーディングの設定とファイアウォール機能の設定を行う。①WAN 側は，本機能を有効にできない仕様になっている。

注記　ルータ-A がインターネットに接続するための ISP 回線では，グローバル IP アドレスが動的に割り当てられる。

注 [1]　UPnP 機能による設定が優先される。

K 氏が NAS-A を調査した結果，次のことが分かった。

・デザインデータのファイルが暗号化され，ファイル名の拡張子が変更されていた。

・A 社では身に覚えのない，英語で書かれた脅迫文のテキストファイルが，NAS-A に

保存されていた。

・ファイル共有機能でも Web 操作機能でもアクセスできない /root ディレクトリ配下のファイルも暗号化されていた。

K 氏は，今回の障害がランサムウェアに起因するものであり，さらに，②A 社の PC がランサムウェアに感染したのではなく，NAS-A 自体がランサムウェアに感染したことによって NAS-A のファイルが暗号化された可能性が高いと判断した。そこで，脆弱性，アクセスログ，DDNS-Z の三つの観点から更に調査を進めることにした。

〔脆弱性の調査〕

NAS-A における脆弱性修正プログラムの適用状況を確認したところ，数週間前にリリースされた製品 X の脆弱性修正プログラム（以下，パッチ M という）が未適用であった。パッチ M は，Web 管理機能に関する二つの脆弱性（以下，脆弱性 1 と脆弱性 2 という）について対策したものである。脆弱性 1 及び脆弱性 2 の概要を図 2 に示す。

脆弱性 1

製品 X では，除外リスト[1)]に次のディレクトリが指定されている。

```
/css
/images
/js
```

認証なしアクセスの処理に脆弱性があり，除外リストに指定されていないディレクトリ配下のファイルにも認証なしでアクセスできてしまう。例えば，http://192.168.0.1/images/..%2fstatus.cgi の URL にアクセスすると，http://192.168.0.1/status.cgi に認証なしでアクセスできてしまう。これは，URL に“..%2f”を使用した［ c ］と呼ばれる攻撃手法である。

脆弱性 2

製品 X には，Web 管理機能の一つとして，IP アドレスを指定して ping を実行する機能がある。この IP アドレスの処理に脆弱性があり，任意の OS コマンドを実行できてしまう。次は，その脆弱性を悪用した例であり，“ping 127.0.0.1;whoami”というコマンドが実行される。

```
POST /ping.cgi HTTP/1.0
Content-Length: 21

addr=127.0.0.1;whoami
```

図 2　脆弱性 1 及び脆弱性 2 の概要

これは，［ d ］と呼ばれる攻撃手法である。脆弱性1と脆弱性2を組み合わせると，認証なしで任意のOSコマンドの実行が可能になる。次は，その例である。

```
POST /images/..%2fping.cgi HTTP/1.0
Content-Length: 21

addr=127.0.0.1;whoami
```

注 1) 除外リストに指定されたディレクトリ配下のファイルには，認証なしでアクセスできる。除外リストは，利用者が変更できない。

図2 脆弱性1及び脆弱性2の概要（続き）

パッチMでは，脆弱性1の対策として，認証なしアクセスの処理の流れにパス名の正規化の処理を加え，さらに，図3に示す順序にした。パス名の正規化とは，相対パスで記述されたパス名を，相対パス記法を含まない形式に変換することである。

［ e ］ → ［ f ］ → ［ g ］

図3 パッチM適用後の認証なしアクセスの処理の流れ

〔アクセスログの調査〕

NAS-Aのアクセスログを調査したところ，外部からHTTPSリクエストを使用してOSコマンドを実行する攻撃ツール（以下，WebShellという）がNAS-Aに配置されており，OSコマンドが実行されたことが分かった。NAS-Aのアクセスログから WebShellに関連するものを抽出した結果を表3に示す。

表3 WebShellに関連するNAS-Aのアクセスログ

No.	時刻	リクエスト	ステータスコード	応答バイト数
1	13:01	GET /images/..%2fstatus.cgi HTTP/1.1	200	634
2	13:02	POST /images/..%2fping.cgi HTTP/1.1	200	418
⋮	⋮	⋮	⋮	⋮
18	13:05	GET /images/shell.cgi?cmd=whoami HTTP/1.1	200	1418
⋮	⋮	⋮	⋮	⋮
89	13:18	POST /images/shell.cgi HTTP/1.1	200	2490

注記 一部の項目は省略している。

表 3 からは，GET メソッドを使用して実行された OS コマンドの内容は分かったが，③POST メソッドを使用して実行された OS コマンドの内容は分からなかった。WebShell が配置されたディレクトリは，書込み不可であるが，root アカウントを用いれば書込み可能に変更できる。製品 X では，sudo コマンドの設定ファイルが図 4 のようになっている。

```
www ALL=NOPASSWD: /bin/tar
```

図 4　sudo コマンドの設定ファイル（抜粋）

tar コマンドは，標準の OS コマンドであり，複数のファイルを一つのアーカイブファイルにまとめたり，アーカイブファイルを展開したりできる。製品 X では，ファームウェアのアップデート時，www アカウントの権限で sudo コマンドを使用して tar コマンドを実行することで，root アカウントの権限でアーカイブファイルを展開している。この 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。ただし，ファームウェアのアップデート時にこのオプションは使用していない。当該オプションを悪用する例を図 5 に示す。

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=whoami
```

図 5　tar コマンドのオプションを悪用する例

K 氏は，“攻撃者が，Web 管理機能の脆弱性と tar コマンドのオプションを悪用し，書込み不可のディレクトリを書込み可能に変更して WebShell を配置した後，WebShell を使用してランサムウェアを実行した”と推測した。そこで，④製品 X で tar コマンドのオプションが悪用されるのを防ぐ対策を検討することにした。

〔DDNS-Z の調査〕

DDNS-Z を使用して製品 X にアクセスするための URL は，インターネットの検索エンジンで特定のキーワードを検索すると容易に見つけることができてしまい，攻撃対象になりやすいことが分かった。インターネットの検索エンジンで検索されないようにするために，各 Web ページの<head>セクションに<meta name="robots" content="［　h　］">を記載することを検討した。

これまでの検討を踏まえ，A 社及び Z 社は必要な対策に着手した。

設問 1　〔NAS-A 及びルータ-A の調査〕について，(1)～(3)に答えよ。

(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　A　　イ　MX　　ウ　TLS

エ　TTL　　オ　TTY　　カ　TXT

(2) 表 2 中の下線①について，WAN 側で UPnP 機能を有効にできる仕様とした場合，ルータ-A が操作されることによって，どのようなセキュリティ上の問題が発生するか。発生する問題を，30 字以内で述べよ。

(3) 本文中の下線②のように判断した理由を，40 字以内で述べよ。

設問 2　〔脆弱性の調査〕について，(1)～(3)に答えよ。

(1) 図 2 中の［ c ］に入れる適切な字句を，15 字以内で答えよ。

(2) 図 2 中の［ d ］に入れる適切な字句を，15 字以内で答えよ。

(3) 図3中の［ e ］～［ g ］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　URL デコード　　イ　除外リストとの比較

ウ　パス名の正規化

設問 3　〔アクセスログの調査〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，実行された OS コマンドの内容が分からなかった理由を，35 字以内で述べよ。

(2) 本文中の下線④について，対策を，50 字以内で具体的に述べよ。

設問 4　本文中の［ h ］に入れる適切な字句を，英字 10 字以内で答えよ。

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。

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。
なお，試験問題では，™ 及び ® を明記していません。

©2022　独立行政法人情報処理推進機構