【解答例＆解説】令和6年度 春期 情報処理安全確保支援士試験 午後 問４

まさ@情報処理技術者試験研究家
2024年6月8日 16:09

情報処理安全確保支援士試験の、解答例とオリジナル解説を公開します。
あくまでも解答例ですので、正解はIPAのサイト（2024年7月2日正午公開）で確認してくださいね。
この記事の最終更新日は、2024年6月8日です。
皆さまの解答例、ご意見も参考にしたいので、コメントお待ちしております。

目次

設問２（４）g ソースコードまたは処理内容

すべて表示

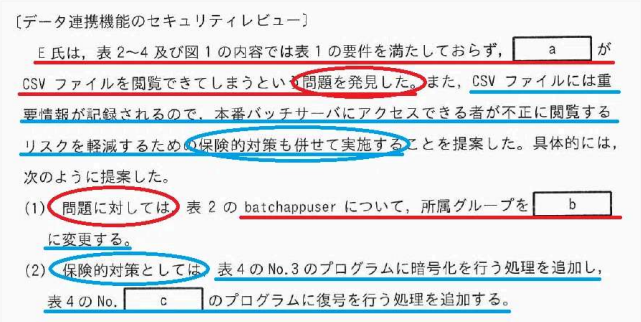
■解答例

設問１（１）a　ア
設問１（２）b　personal
設問１（３）c　4
設問２（１）d　5
設問２（２）e　チェック例外　又は　NoSuchAlgorithmException
設問２（３）システム運用担当者
　　情報　氏名、住所、電話番号、メールアドレス
　　場所　エ
設問２（３）システム開発者
　　情報　氏名、住所、電話番号、メールアドレス
　　場所　オ
設問２（４）f　SHA-256
設問２（５）g ソースコード　？
　　又は
　　処理内容　処理を異常終了させる
設問２（６）h　finally
設問２（７）　ア

■解説

設問１（１）a

解答：ア
解説：問題文のヒントから考える問題
重要情報が記録されているCSVファイルを閲覧できてはいけない人〔 a 〕が閲覧できてしまう。〔 a 〕は誰？という設問です。
問題文〔 a 〕の前後にヒント（解答への制約）が無いか確認します。


〔データ連携機能のセキュリティレビュー〕
E 氏は，表 2～4 及び図 1 の内容では表 1 の要件を満たしておらず，［ a ］が CSV ファイルを閲覧できてしまうという問題を発見した。また，CSV ファイルには重要情報が記録されるので，本番バッチサーバにアクセスできる者が不正に閲覧するリスクを軽減するための保険的対策も併せて実施することを提案した。具体的には，次のように提案した。
(1) 問題に対しては，表 2 の batchappuser について，所属グループを［ b ］に変更する。
(2) 保険的対策としては，表 4 の No.3 のプログラムに暗号化を行う処理を追加し，表 4 の No.［ c ］のプログラムに復号を行う処理を追加する。

よく読むと「問題に対する対策」と「保険的対策」の2つの対策を行っています。〔ａ〕がcsvファイルを閲覧できてしまう対策として「表2のbatchappduserのグループを変更する」と書いてあるため、〔ａ〕の解答には、batchappduserのグループ変更が関係することがわかります。

解答群は５個用意されています。

解答群

ア　システム運用担当者

イ　システム運用担当者とシステム開発者

ウ　システム開発者

エ　システム開発者と重要情報取扱運用者

オ　重要情報取扱運用者

そもそも、重要情報を見てもいい人といけない人を確認しましょう。
問題文表１のNo.18ですね。

18	システムのユーザーと役割	(1)　個人顧客 Web 受注システムの AP サーバで注文，決済などを行う。 (2)　システム運用担当者 本番 AP サーバ及び本番バッチサーバの稼働を監視する。バッチ処理が異常終了したときは，手動で再実行する。これら以外のサーバについては，統合監視システムの画面から死活監視だけを行う。重要情報にアクセスしてはならない。 (3)　重要情報取扱運用者 本番環境に保管されている重要情報を参照し，個人顧客からの問合せに対応する。 (4)　システム開発者 開発環境においてプログラムの開発・保守を行う。障害発生時は，本番ログサーバにアクセスして障害原因を調査する。重要情報にアクセスしてはならない。 (5)　システム管理責任者 各サーバの OS，ミドルウェアの脆弱性修正プログラムの適用などのメンテナンス作業を行う。各サーバの OS アカウントを管理する。各 DB のアカウント管理を行う。

重要情報取扱運用者は重要情報を参照するため、解答群エとオは除外。
正解はア、イ、ウのいづれかになる。
次に、「システム運用担当者」と「システム開発者」と問題文のヒントの「batchappuser」のアカウント設定を表２と表3で確認します。

表２　OS アカウントの一覧

No.	ユーザーID	所属グループ	OS アカウントが定義されるサーバ	説明
1	root	root	(省略)	システム管理責任者が利用する。
2	operator	operation	(省略)	システム運用担当者が利用する。
3	personal	personal	(省略)	重要情報取扱運用者が利用する。
4	developer	develop	(省略)	システム開発者が利用する。
5	batchappuser	operation	本番バッチサーバ	データ連携機能 注1)の各プログラムの実行に利用される。
6	webappuser	personal	本番 AP サーバ	AP サーバのプログラムの実行に利用される。

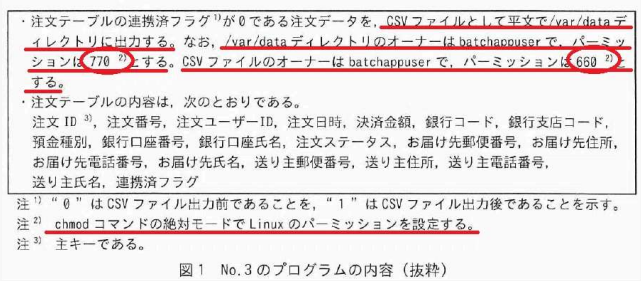
注記　root，operation，personal，develop という所属グループは各サーバに定義されている。
注 1)　業務システムと Web 受注システムがデータ連携を行うための機能である。

表３　所属グループとその権限

No.	所属グループ	権限
1	root	特権ユーザーである。全てのアクセス権がある。
2	operation	一般ユーザー権限である。本番 AP サーバと本番バッチサーバへのアクセス権がある。
3	personal	一般ユーザー権限である。本番環境へのアクセス権がある。
4	develop	一般ユーザー権限である。開発環境と本番ログサーバへのアクセス権がある。

注記　Web 受注システムでは，OS アカウントの権限を所属グループ単位で管理する。

システム開発者は、データ連携機能が動作する本番バッチサーバへアクセス権が無いため、解答はアになりそうです。
さらに問題文ヒントの「batchappuser」についてヒントを探します。
図１に、ヒントになりそうなことが書いてあります。
Linuxを知らない人には、意味がわかりませんね。
わからない場合は、解答は「ア」にして次の設問に進みましょう。


・注文テーブルの連携済フラグ[1]が0である注文データを，CSVファイルとして平文で/var/dataディレクトリに出力する。なお，/var/dataディレクトリのオーナーはbatchappuserで，パーミッションは770[2]とする。CSVファイルのオーナーはbatchappuserで，パーミッションは660[2]とする。
・注文テーブルの内容は，次のとおりである。
注文ID[3]，注文番号，注文ユーザーID，注文日時，決済金額，銀行コード，銀行支店コード，預金種別，銀行口座番号，銀行口座氏名，注文ステータス，お届け先郵便番号，お届け先住所，お届け先電話番号，お届け先氏名，送り主郵便番号，送り主住所，送り主電話番号，送り主氏名，連携済フラグ
注[1] “0”はCSVファイル出力前であることを，“1”はCSVファイル出力後であることを示す。
注[2] chmodコマンドの絶対モードでLinuxのパーミッションを設定する。
注[3] 主キーである。
図１　No.３のプログラムの内容（抜粋）

細かい説明は省略しますが、パーミッションとは、権限設定のことです。
「770」の各数値は、オーナー、グループ、その他ユーザの各権限を表します。
パーミッション770とは、
7 オーナーは、読む・書く・実行、全て権限あり
7 グループも、読む・書く・実行、全て権限あり
0 その他ユーザ、読む・書く・実行、全て権限なし
パーミッション660とは、
6 オーナーは、読む・書く、権限あり。実行権限なし
6 グループも、読む・書く、権限あり。実行権限なし
0 その他ユーザ、読む・書く・実行、全て権限なし
です。

すなわち、表2に戻ると、「batchappuser」が所属する「operation」に同じく所属している「システム運用担当者」は、csvファイルを閲覧する権限があることがわかります。やっぱり答えは「ア」です。

設問１（２）b

解答：personal
解説：問題文のヒントから考える問題
設問１（１）で確認したことより、「batchappuser」が所属するグループの変更先は、「operation」より権限が低く、本番環境へのアクセス権は必要な「personal」になります。

表２　OS アカウントの一覧

No.	ユーザーID	所属グループ	OS アカウントが定義されるサーバ	説明
1	root	root	（省略）	システム管理責任者が利用する。
2	operator	operation	（省略）	システム運用担当者が利用する。
3	personal	personal	（省略）	重要情報取扱運用者が利用する。
4	developer	develop	（省略）	システム開発者が利用する。
5	batchappuser	operation	本番バッチサーバ	データ連携機能 注1)の各プログラムの実行に利用される。
6	webappuser	personal	本番 AP サーバ	AP サーバのプログラムの実行に利用される。

注記　root，operation，personal，develop という所属グループは各サーバに定義されている。
注 1)　業務システムと Web 受注システムがデータ連携を行うための機能である。

表３　所属グループとその権限

No.	所属グループ	権限
1	root	特権ユーザーである。全てのアクセス権がある。
2	operation	一般ユーザー権限である。本番 AP サーバと本番バッチサーバへのアクセス権がある。
3	personal	一般ユーザー権限である。本番環境へのアクセス権がある。
4	develop	一般ユーザー権限である。開発環境と本番ログサーバへのアクセス権がある。

注記　Web 受注システムでは，OS アカウントの権限を所属グループ単位で管理する。

設問１（３）c

解答：4
解説：問題文から抜粋問題
表４のNo.3でcsvファイルを暗号化して、そのcsvファイルを読み込むのはNo.4です。読み込んでDB更新しているので、復号が必要です。

表４　データ連携機能のプログラム一覧

No.	プログラム名	実行するサーバ	概要
1	バッチ処理管理 1	Web 受注システムのバッチサーバ	Web 受注システムの各バッチ処理のプログラムの起動，監視などを行う。
2	バッチ処理管理 2	業務システムのバッチサーバ	業務システムの各バッチ処理のプログラムの起動，監視などを行う。
3	注文データ CSV 出力バッチ処理	Web 受注システムのバッチサーバ	Web 受注システムの DB 内の注文テーブルから注文データを取得し，CSV ファイルに出力する。
4	注文データ CSV 取込みバッチ処理	業務システムのバッチサーバ	保存された CSV ファイルを読み込んで，業務システムの DB を更新する。
5	在庫データ CSV 出力バッチ処理	業務システムのバッチサーバ	業務システムの DB 内の在庫テーブルから在庫データを取得し，CSV ファイルに出力する。
6	在庫データ CSV 取込みバッチ処理	Web 受注システムのバッチサーバ	保存された CSV ファイルを読み込んで，Web 受注システムの DB を更新する。
7	データ送信 1 バッチ処理	Web 受注システムのバッチサーバ	CSV ファイルを業務システムのバッチサーバに HTTPS で送信する。
8	データ送信 2 バッ	業務システムのバ	CSV ファイルを Web 受注システムのバッチサーバ

設問２（１）d

解答：5
解説：知識問題
プログラミング知識の必要な問題ですね。
プログラミング知識が無くても正解できるように、ヒントを探します。

・今後，メンテナンスなどで実行環境を変更した場合に，［　d　］行目で［　e　］が発生すると，25，26 行目では，パスワードが平文でユーザーマスターテーブルに保存されてしまう。

［ｅ］が発生すると、パスワードが平文で～と記載されています。
ということは、［ｅ］が発生しなければ、パスワードは暗号化されていると考えられます。図３の中で暗号化に関係しそうな箇所を探すと、5行目に"SHA-1"が見つかります。（"SHA-1"がハッシュ関数

だという知識は必要）
プログラミングがわからなければ「５」で解答しましょう。

次に図３ソースコードの解答に関連する部分を確認しましょう。

```
   (省略)  //package 宣言, import 宣言など
 1: public UserData(HttpServletRequest request) {
 2:   this.userId = request.getParameter("userId");
 3:   this.password = request.getParameter("password");
      (省略)  //入力値チェックなど
 4 ① try {
 5:     MessageDigest mdObj = MessageDigest.getInstance("SHA-1");
 6:     byte[] hashByte = mdObj.digest(this.password.getBytes());
 7:     this.password = String.format("%x", new BigInteger(1, hashByte));
 8:   } catch (NoSuchAlgorithmException e) {
 9:     log.debug("error:" + e);    ②
10:   }
      (省略)
11: }
    //引数 conn は DB コネクションオブジェクトを示す。    ④
12: public void addUser(Connection conn) {
13:   PreparedStatement psObj;
14:   String sql = "INSERT INTO USER_MASTER" +
15:                "(USER_OID, USER_ID, PASSWORD, USER_NAME, ZIP_CODE" +
                   (省略);
16:   try {
17:     psObj = conn.prepareStatement(sql);
18:     psObj.setString(1, this.userOid);
19:     psObj.setString(2, this.userId);
20:     psObj.setString(3, this.password);
        (省略)
        //次の２行はデバッグログの出力
21:     System.out.println("SQL:" + sql);
22:     System.out.println("InsertData:" + this.toString());
        //次の２行はログサーバへの AP ログの出力
23:     log.debug("SQL:" + sql);
24:     log.debug("InsertData:" + this.toString());
25:     psObj.execute(); ③
26 ④   conn.commit();
27:   } catch (SQLException e) {
        (省略)  //例外処理
28:   }
      (省略)
29: }
    (省略)
```

注記　log.debug()は，引数の文字列をログサーバに送信するメソッドである。

図３　UserData クラスのソースコード（抜粋）

必要な知識①　try とは？

例外処理を行うにはtry文を使用します。基本的な書式は次の通りです。

```
try{
  例外が発生しているかどうか調べる文1;
  例外が発生しているかどうか調べる文2;
  ...
}
catch (例外クラス1 変数名1){
  例外クラス1の例外が発生した時に行う文;
  ...
}
catch (例外クラス2 変数名2){
  例外クラス2の例外が発生した時に行う文;
  ...
}
```

まずプログラムの中で例外が発生するかどうかを調べる対象の文をtryの後の「{」から「}」までのブロック内に記述します。そして例外が発生した時に行いたい処理をcatchの後の「{」から「}」までのブロック内に記述します。

引用：Java入門 try文
https://www.javadrive.jp/start/exception/index2.html

必要な知識②　NoSuchAlgorithmException　とは？
指定されたアルゴリズムが使用できない場合に発生するチェック例外です。

必要な知識③　execute　とは？
「呼び出す」とか「実行する」ですね。

必要な知識④　DBコネクションオブジェクト　とは？
データベース接続を管理するオブジェクトです。プログラムからデータベースに接続するときに必要です。データベースへの接続から切断までの手順を管理・実行します。

必要な知識①と②の組み合わせで、以下のように考えて解答します。
5行目のSHA-1ハッシュ値生成が正常に行われたのかのチェックで、
チェック例外が発生（NoSuchAlgorithmException）した場合、パスワードが平文でユーザマスタに登録されてしまう。
［ｄ］５
［ｅ］チェック例外　又は　NoSuchAlgorithmException

設問２（２）e

解答：チェック例外　又は　NoSuchAlgorithmException
解説：知識問題
解説は、設問２（１）ｄ　参照。

設問２（３）

解答：システム運用担当者
　　情報　氏名、住所、電話番号、メールアドレス
　　場所　エ
解答：システム開発者
　　情報　氏名、住所、電話番号、メールアドレス
　　場所　オ
解説：問題文から抜粋問題
・情報について
アクセスが禁止されている情報は、図２と表１No.5を比較して確認します。
ユーザマスタテーブルのパスワードは、ハッシュ値のためアクセスできないと考えます。

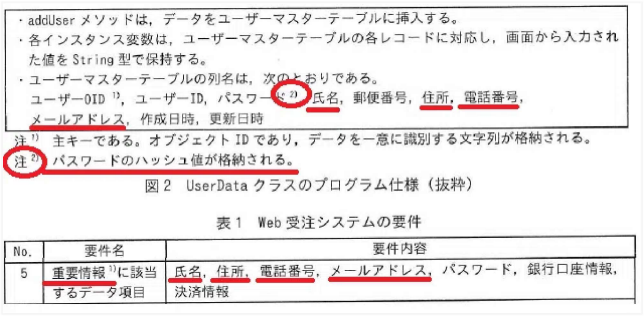

・addUser メソッドは，データをユーザーマスターテーブルに挿入する。
・各インスタンス変数は，ユーザーマスターテーブルの各レコードに対応し，画面から入力された値を String 型で保持する。
・ユーザーマスターテーブルの列名は，次のとおりである。
ユーザーOID 注1)，ユーザーID，パスワード 注2)，氏名，郵便番号，住所，電話番号，
メールアドレス，作成日時，更新日時
注1) 主キーである。オブジェクト ID であり，データを一意に識別する文字列が格納される。
注2) パスワードのハッシュ値が格納される。

図２　UserData クラスのプログラム仕様（抜粋）

表１　Web 受注システムの要件

No.	要件名	要件内容
5	重要情報 1)に該当するデータ項目	氏名，住所，電話番号，メールアドレス，パスワード，銀行口座情報，決済情報

・場所について
プログラム実行に関するデータ保存場所を表１で確認します。

No.1　プログラムは、APサーバに実装される。
No.15　APサーバのプログラムは、APログをログサーバに転送する。
　　ログサーバはAPログをテキストファイルで保存する。

No.16　APサーバの標準出力はAPサーバの/var/log/serverlog配下の
　　テキストファイルに出力する
・APサーバの/var/log/serverlog
　オーナーはwebappuser
　パーミッション　774
パーミッション774とは、
7 オーナーは、読む・書く・実行、全て権限あり
7 グループも、読む・書く・実行、全て権限あり
4 その他ユーザ、読む・実行、権限あり。書く権限無し
・APサーバの/var/log/serverlog配下のテキストファイル
　オーナーはwebappuser
　パーミッション　664
パーミッション660とは、
6 オーナーは、読む・書く、権限あり。実行権限なし
6 グループも、読む・書く、権限あり。実行権限なし
4 その他ユーザ、読む・実行、権限あり。書く権限無し
つまり、参照は誰でもできるということですね。

次に、システム運用管理者とシステム開発者がアクセスできる場所を確認します。再び、表２を確認。

表２　OS アカウントの一覧

No.	ユーザーID	所属グループ	OS アカウントが定義されるサーバ	説明
1	root	root	（省略）	システム管理責任者が利用する。
2	operator	operation	（省略）	システム運用担当者が利用する。
3	personal	personal	（省略）	重要情報取扱運用者が利用する。
4	developer	develop	（省略）	システム開発者が利用する。
5	batchappuser	operation	本番バッチサーバ	データ連携機能 注1)の各プログラムの実行に利用される。
6	webappuser	personal	本番 AP サーバ	AP サーバのプログラムの実行に利用される。

注記　root，operation，personal，develop という所属グループは各サーバに定義されている。
注 1)　業務システムと Web 受注システムがデータ連携を行うための機能である。

表３　所属グループとその権限

No.	所属グループ	権限
1	root	特権ユーザーである。全てのアクセス権がある。
2	operation	一般ユーザー権限である。本番 AP サーバと本番バッチサーバへのアクセス権がある。
3	personal	一般ユーザー権限である。本番環境へのアクセス権がある。
4	develop	一般ユーザー権限である。開発環境と本番ログサーバへのアクセス権がある。

注記　Web 受注システムでは，OS アカウントの権限を所属グループ単位で管理する。

システム運用管理者は、APサーバにアクセスできます。
システム開発者は、本番ログサーバにアクセスできます。
これらのことより、
システム運用管理者がデータにアクセスできる場所は「エ」
システム開発者がデータにアクセスできる場所は、「オ」

設問２（４）f

解答：SHA-256
解説：知識問題
SHA-1に変わるものと言えば、SHA-256という知識問題。

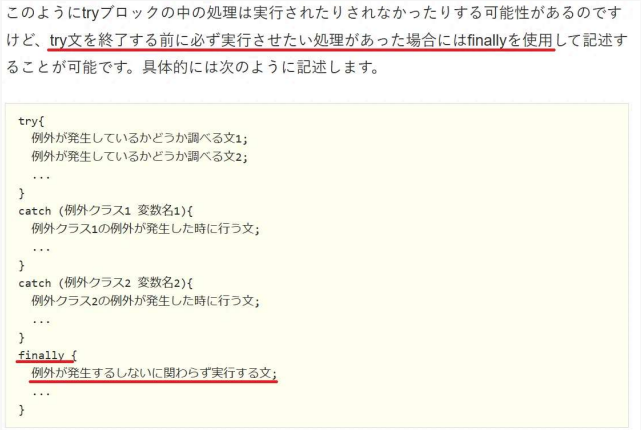
SHA-256は、ハッシュ関数の中で、実装のしやすさ、処理速度、安全性などの面で優れており、最も普及しています。

設問２（４）g ソースコードまたは処理内容

解答：処理を異常終了させる
解説：知識問題
［ｇ］の上に「//回復不能な例外発生」のコメントがあるため、これ以上処理できないため、異常終了ですね。プログラミングの知識問題です。

設問２（６）h

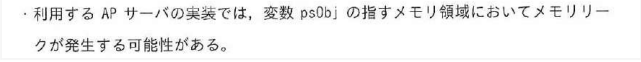
解答：finally
解説：知識問題
設問２（１）の「必要な知識①　try とは？」で説明した、try,
catch,に続く［ｈ］が空欄になっています。
tryでのチェック結果に関係なく、必ず実行する処理の記述が考えられます。


このようにtryブロックの中の処理は実行されたりされなかったりする可能性があるのですけど、try文を終了する前に必ず実行させたい処理があった場合にはfinallyを使用して記述することが可能です。具体的には次のように記述します。

```
try{
  例外が発生しているかどうか調べる文1;
  例外が発生しているかどうか調べる文2;
  ...
}
catch (例外クラス1 変数名1){
  例外クラス1の例外が発生した時に行う文;
  ...
}
catch (例外クラス2 変数名2){
  例外クラス2の例外が発生した時に行う文;
  ...
}
finally {
  例外が発生するしないに関わらず実行する文;
  ...
}
```

引用：Java入門 必ず実行する処理の記述(try..catch..finally)
https://www.javadrive.jp/start/exception/index3.html

tryでのチェック結果に関係なく、必ず実行する処理とは何か？
下記問題の対策ですね。


・利用する AP サーバの実装では，変数 psObj の指すメモリ領域においてメモリリークが発生する可能性がある。

設問２（７）

解答：ア
解説：知識問題
これもプログラミングの知識問題。

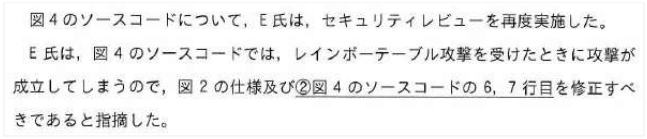
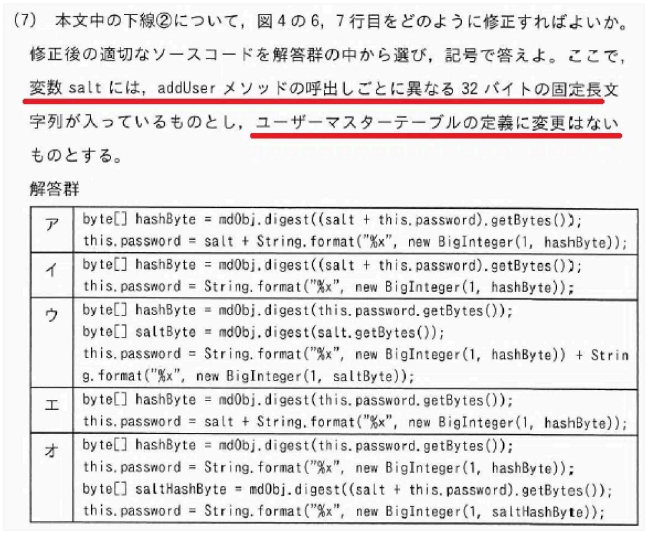


図４のソースコードについて，E氏は，セキュリティレビューを再度実施した。
E氏は，図４のソースコードでは，レインボーテーブル攻撃を受けたときに攻撃が成立してしまうので，図２の仕様及び②図４のソースコードの６，７行目を修正すべきであると指摘した。

レインボーテーブル攻撃とは、ハッシュ値から元の平文を解読する攻撃のひとつです。あらかじめハッシュ値と平文候補を準備しておき、ハッシュ値の総当たり攻撃を行う手法です。



(7) 本文中の下線②について，図４の６，７行目をどのように修正すればよいか。修正後の適切なソースコードを解答群の中から選び，記号で答えよ。ここで，変数saltには，addUserメソッドの呼出しごとに異なる32バイトの固定長文字列が入っているものとし，ユーザーマスターテーブルの定義に変更はないものとする。

解答群

ア
```
byte[] hashByte = md0bj.digest((salt + this.password).getBytes());
this.password = salt + String.format("%x", new BigInteger(1, hashByte));
```

イ
```
byte[] hashByte = md0bj.digest((salt + this.password).getBytes());
this.password = String.format("%x", new BigInteger(1, hashByte));
```

ウ
```
byte[] hashByte = md0bj.digest(this.password.getBytes());
byte[] saltByte = md0bj.digest(salt.getBytes());
this.password = String.format("%x", new BigInteger(1, hashByte)) + Strin
g.format("%x", new BigInteger(1, saltByte));
```

エ
```
byte[] hashByte = md0bj.digest(this.password.getBytes());
this.password = salt + String.format("%x", new BigInteger(1, hashByte));
```

オ
```
byte[] hashByte = md0bj.digest(this.password.getBytes());
this.password = String.format("%x", new BigInteger(1, hashByte));
byte[] saltHashByte = md0bj.digest((salt + this.password).getBytes());
this.password = String.format("%x", new BigInteger(1, saltHashByte));
```

ソルト(salt)は元の平文に任意の文字列を追加してハッシュ化する手法です。 ハッシュ値から平文を解読されにくくなるため、レインボーテーブル攻撃対策になります。
設問のヒント
①saltは32バイト固定長
②ユーザーマスターテーブルの定義に変更はない
から解答を考えます。
が、ヒントだけからは答えは出せません.....。

プログラミングのわかる方へ、解説をお願いします。m(_ _)m

最後までお読みいただきありがとうございました。
少しでも参考になれば幸いです。

■更新履歴

2024/4/21(日)　試験日
2024/6/8(日)　作成・公開