次の問1は必須問題です。必ず解答してください。

問1　Webサイトのセキュリティに関する次の記述を読んで，設問に答えよ。

F社は，日用雑貨を製造・販売する中堅企業である。このたび，販路拡大を目的として自社製品を販売するWebサイト（以下，本システムという）を新規に開発した。本システムは，D社クラウドサービス上に構築しており，Webサーバとデータベース（以下，DBという）サーバから成り，D社クラウドサービスが提供するファイアウォール（以下，FWという）及びWebアプリケーションファイアウォール（以下，WAFという）を経由してインターネットからアクセスされる予定である。

本システムの開発環境のネットワーク構成（抜粋）を図1に示す。なお，本システムはリリース前であり，F社開発環境の特定のIPアドレスからだけアクセスできるようにFWで制限している。

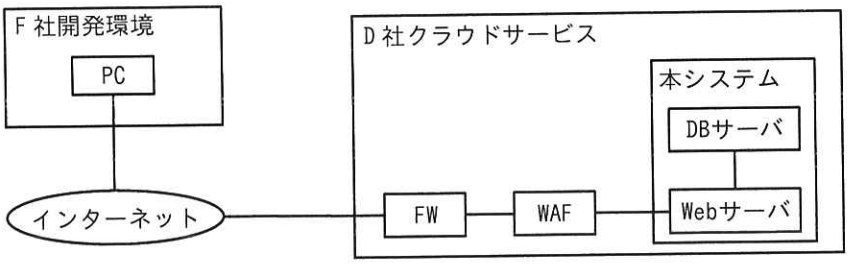


図1　本システムの開発環境のネットワーク構成（抜粋）

本システムの主な仕様を次に示す。

・会員登録時に自動で発行される会員番号と会員が設定したパスワードをログインフォームに入力してログインする。商品の購入はログイン後に行う。
・パスワードとして使用できる文字は，英数字に一部の記号を加えた70種類である。
・パスワードは，6字以上16字以下で設定する。
・会員テーブルは，会員番号，メールアドレス，パスワードのハッシュ値，姓，名，住所，電話番号の7フィールドで構成されている。①パスワードのハッシュ値は，会員が設定したパスワードをハッシュ関数によってハッシュ化したものである。

F社情報セキュリティ部のG部長は，本システムのリリース前にペネトレーションテストを実施することを決定し，H主任をリーダーに任命した。H主任は，セキュリ

ティベンダーであるU社に本システムのペネトレーションテストの実施を依頼した。ペネトレーションテストは，U社内のPCからインターネット，FW及びWAFを経由して本システムにアクセスする経路で実施した。

ペネトレーションテスト期間中は，FW及びWAFに対して次の変更を行った。

・FWに対する変更

通信を許可するアクセス元IPアドレスとして，ペネトレーションテストに用いるU社のIPアドレスを追加する。

・WAFに対する変更

攻撃を検知した際には，通信の遮断は行わず，検知したことだけを記録する。

〔ペネトレーションテストの結果〕

ペネトレーションテストの結果，次の手順（以下，本シナリオという）で会員のパスワードが推測されて，不正にアクセスされてしまうことが確認された。

1. ②SQL インジェクション攻撃によって会員テーブルのデータを取得する。このとき取得した会員テーブルのデータ（抜粋）を表1に示す。
2. レインボーテーブル攻撃によって，手順1で取得した会員テーブル中のパスワードのハッシュ値から元のパスワードを推測する。
3. 推測したパスワードを利用して，会員になりすまして本システムにログインする。

表1　取得した会員テーブルのデータ（抜粋）

| 会員番号 | パスワードのハッシュ値 | 姓 | 名 |
|---|---|---|---|
| 21717202 | 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 | T中 | T郎 |
| 21717203 | 2597a7caf656e89e9ab35e12326d557ebfe9b7b5dcbe4c564e74070fa5cfcbe5 | S藤 | H子 |
| 30781985 | 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 | S藤 | J郎 |
| 36150833 | ac9689e2272427085e35b9d3e3e8bed88cb3434828b43b86fc0596cad4c6e270 | S木 | H子 |
| 45905900 | ac9689e2272427085e35b9d3e3e8bed88cb3434828b43b86fc0596cad4c6e270 | Y田 | J郎 |
| 45917046 | d82494f05d6917ba02f7aaa29689ccb444bb73f20380876cb05d1f37537b7892 | T中 | T郎 |

稼働中のシステムのログインフォームに対してパスワードを総当たりで試行する［ a ］攻撃では，システム側で試行回数に制限を設けて対策することができるが，レインボーテーブル攻撃ではそれができない。

H主任は，本システムの修正方針を整理するために，SQL インジェクション攻撃及

びレインボーテーブル攻撃への対策を検討することにした。なお，ペネトレーションテスト期間中にWAFでSQLインジェクション攻撃が検知できていたが，③仮に対策の一つが破られても他の対策で攻撃を防ぐという考え方に基づき，攻撃への対策をWAFだけに頼らず本システム自体でも行うことにした。

〔SQLインジェクション攻撃への対策の検討〕

本システムのソースコードを調査したところ，一部の処理で外部からの入力値をそのままSQL文に埋め込んでいる箇所が存在していた。そこで，対策として，［ b ］を利用する方式を採用することにした。この方式では，外部からの入力値が埋め込まれる箇所を専用の記号に置き換えたSQL文の雛形(ひな)をあらかじめ作成しておき，専用の記号で置き換えた箇所にDB管理システム側で外部からの入力値を割り当てる。

〔レインボーテーブル攻撃への対策の検討〕

本システムでは会員のパスワードをハッシュ化して保存しているが，パスワードそのものにハッシュ関数を1回適用しただけであったので，レインボーテーブル攻撃に対して脆弱(ぜいじゃく)であった。そこで，パスワードをハッシュ化する際に，次の三つの処理を組み合わせて実施することにした。

1. ソルトを用いた処理
   - パスワードをハッシュ化する際に，ソルトを付加した上でハッシュ化する。
   - ソルトとして，会員ごとに異なるランダムな文字列を用意し，会員テーブルに格納する。
2. ④ペッパーを用いた処理
   - パスワードをハッシュ化する際に，ペッパーを付加した上でハッシュ化する。
   - ペッパーとして，全ての会員に共通のランダムな文字列を用意し，Webサーバ内の外部からアクセスできない安全な領域に格納する。
3. ストレッチング
   - ハッシュ関数を複数回適用する。

さらに，ハッシュ化処理の変更に加えて，会員が設定可能なパスワード長を10字

以上 64 字以下に変更した。本システムにおいて，パスワード長が 10 字の場合，6 字の場合と比べてパスワードとして使用可能な文字列のパターン数が［ c ］倍になるのでレインボーテーブル攻撃がより困難になる。

H 主任は，これらの対策を取りまとめて G 部長に報告し，承認された。

設問 1　本文中の下線①について，会員のパスワードをハッシュ関数でハッシュ化して保存することは，情報漏えいの脅威に対してメリットがある。それは，ハッシュ値にどのような特性があるからか。25 字以内で答えよ。

設問 2　本文中の下線②について，会員テーブルのデータが漏えいした場合，情報セキュリティの 3 要素のどれが直接的に侵害されたといえるか。漢字 3 字で答えよ。

設問 3　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　エスケープ　　イ　許可リスト　　ウ　サニタイズ

エ　中間者　　オ　ブルートフォース　　カ　プレースホルダ

キ　リプレイ

設問 4　本シナリオによって，表 1 に示す会員テーブルのデータが窃取され，会員番号“21717202”の会員のパスワードが推測され不正アクセスを受けたとすると，推測されたパスワードを利用して不正アクセスを受けるおそれが最も強い他の会員は誰か。該当する会員の会員番号を解答群の中から選び，記号で答えよ。

解答群

ア　21717203　　イ　30781985　　ウ　36150833

エ　45905900　　オ　45917046

設問 5　本文中の下線③の考え方を，漢字 4 字で答えよ。

設問 6　〔レインボーテーブル攻撃への対策の検討〕について答えよ。

(1)　本文中の下線④について，ペッパーを付加してハッシュ化することで本シナリオにおいてレインボーテーブル攻撃が困難になる理由を，ソルトを用いた処理との違いに着目して 35 字以内で答えよ。

(2)　本文中の［ c ］に入れる適切な数を，$x^y$ のような指数を用いた表記で答えよ。