問9　Webアプリケーションのセキュリティ対策に関する次の記述を読んで，設問1～4に答えよ。

W社は，インターネット上で日用雑貨品の会員制通信販売システムを運営する会社である。この通信販売システム（以下，本システムという）は，商品検索，注文，会員管理，会員掲示板などの機能を提供する。

本システムの機能を利用するには，あらかじめ会員管理機能を使って，会員登録しなければならない。

図1は，会員掲示板機能を使った会員掲示板画面の例である。

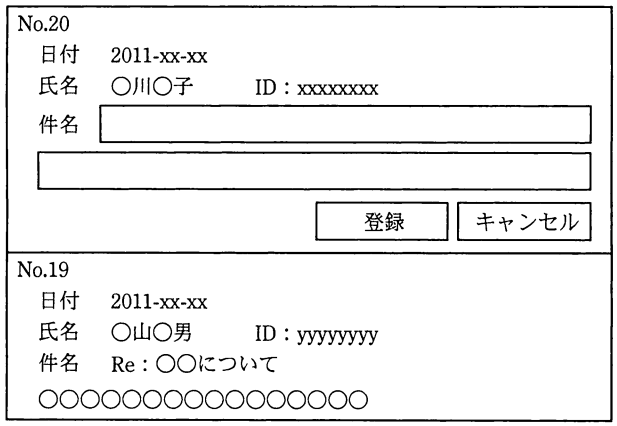

図1　会員掲示板画面の例

ある日，会員情報が知らぬ間に書き換わっていたり，覚えの無い商品が届いたりしたとのクレームが複数の会員から寄せられた。情報システム部門で本システムを調べたところ，クレームに該当する登録情報の変更処理や商品の注文処理が確認された。

情報システム部門の責任者であるA部長は，セキュリティ事故が発生したと判断して，本システムの利用を直ちに停止し，外部のセキュリティ専門会社の支援を受けながら対策をとることを指示した。

後日，外部のセキュリティ専門会社から，今回のセキュリティ事故に関する調査報告書が届けられた。調査報告書に記載された内容は，次のとおりである。

〔セキュリティ事故の経過〕

(1) 会員 X は，本システムのトップ画面から，会員ログインページへのボタンを押した。

(2) 本システムは，ログイン画面を表示した。

(3) 会員 X は，ログイン画面で，自身のアカウント名とパスワードを入力した。

(4) 本システムは，アカウント名とパスワードを確認して，セッション ID を発行し，cookie を利用して会員のブラウザに戻した。

(5) 会員 X は，会員メニュー画面で，会員掲示板機能を選択した。

(6) 本システムは，会員掲示板画面を表示した。

(7) 会員 X が，特定の会員掲示板ページを参照したときに，悪意のあるコードが自動的に実行され，会員 X の登録情報を書き換える処理と，注文処理が行われた。

〔想定される原因〕

(1) 会員掲示板ページを出力する処理に問題があり，この問題を悪用した<script>タグを用いた悪意のあるコードが，会員掲示板ページに埋め込まれた形跡があった。

(2) ログインした会員が，この悪意のあるコードが埋め込まれた会員掲示板ページを参照すると，そのコードが自動的に実行され，会員の登録情報を書き換える処理や特定の商品の注文処理が行われるようになっていた。

〔原因から想定される脅威〕

(1) 登録情報や会員掲示板情報に対して，ログインした会員が予期しない処理を勝手に実行させられることによって起こる情報の改ざん

(2) ログインした会員が予期しない注文処理を勝手に実行させられることによって起こるサービスの悪用

〔対策の提言〕

(1) 入力された文字列は，そのままではなく，エスケープ処理を適切に施してからブラウザに表示する。入力データに “<”，“>”，“&” などの HTML の特別な記号文字が存在した場合，その記号文字が有する特別な働きを無効にする文字や文

字列に置き換える。例えば，“>”は“>”，“<”は“<”，“&”は“&”とする。これによって，タグの文字列“<script>”は，文字列“<script>”に置き換わる。

(2) 特に，会員情報の登録処理や注文処理のような重要な処理を実行するページには［ a ］メソッドでアクセスするようにし，その hidden パラメタに秘密情報（ページトークン）が挿入されるように，前のページを自動生成する。実行ページでは，その値が正しい場合だけ処理を行う。もし［ a ］メソッドの代わりに［ b ］メソッドでアクセスすると，秘密情報を URL に付加して送信することになるので，ここでは利用を避けるべきである。また，HTML フォームで<form>タグを用いる場合，メソッド属性の指定を省略すると［ b ］メソッドと解釈されるので，適切に指定する必要がある。

今回のように，ログインした会員だけが，予期しない処理を実行させられてしまうセキュリティ攻撃は，クロスサイトリクエストフォージェリーと呼ばれている。

この攻撃が成功する主たる要因は，会員の正しい要求と悪意のあるコードの要求を区別できないことである。

この後，A 部長は，外部のセキュリティ専門会社の提言に従い，今回のセキュリティ攻撃の根本的な原因を解消すべく，本システムの改善を行うことにした。

提言された対策(1)を本システムの全てのプログラムに適用し，その上で重要な処理を行う注文機能と会員管理機能に対して，提言された対策(2)を適用した。会員登録時における本システムと会員のブラウザとの間の情報の流れは，図2のとおりである。

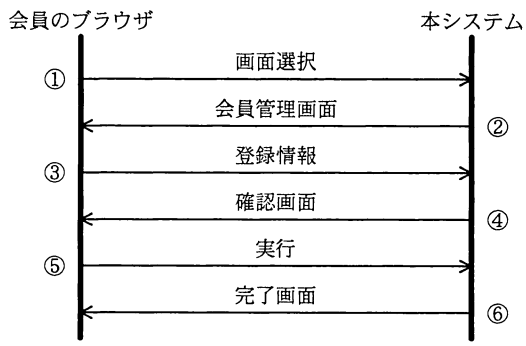

図2　会員管理機能の流れ

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　GET　　イ　HEAD　　ウ　OPTION

エ　POST　　オ　PUT　　カ　RESET

設問2　〔対策の提言〕(1)について，今回の場合，<script>タグを用いたコードにエスケープ処理を適切に施す目的は何か。20字以内で述べよ。

設問3　図2において，秘密情報（ページトークン）を送受信する適切な箇所の組合せを解答群の中から選び，記号で答えよ。

解答群

ア　①，②，③　　イ　②，③，④　　ウ　③，④

エ　④，⑤　　オ　⑤　　カ　⑤，⑥

設問4　今回のセキュリティ攻撃を防ぐ対策として〔対策の提言〕(1)，(2)を実施した上で，この攻撃を検出する対策をとることにした。この攻撃を検出するために有効な対策として適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　悪意のあるコードを埋め込まれた特定の会員掲示板ページを直ちに削除する。

イ　会員情報の登録や変更，注文処理などの重要な処理を行うページでは，HTTPSによって，途中経路を暗号化する。

ウ　会員情報の登録や変更，注文処理などの重要な処理については，必ずログを記録する。

エ　本システムで利用するセッションIDとして会員ごとに一意の固定値を割り当て，常にそれを利用する。