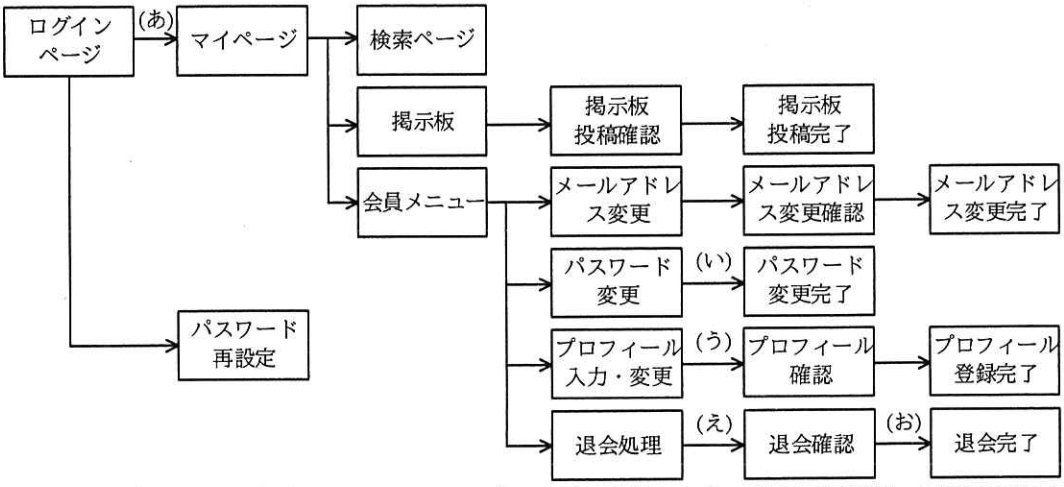
問2　Webサイトのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

E社は，従業員数200名の情報サービス事業者である。E社は，3年前からWebサイトα（以下，サイトαという）を利用して，次のような機能をもつ会員制の飲食店情報提供サービスを行っている。

・飲食店情報の検索
・飲食店情報に関する掲示板での投稿
・新規登録情報の，会員への電子メール（以下，メールという）による通知

サイトαに対する脆弱（ぜい）性修正プログラムの適用や，コンテンツ作成などの日々の作業は，情報提供サービス担当チームが行っている。チームはリーダのQさんと5名のメンバで構成されている。サイトαで稼働しているWebアプリケーションソフトウェアは，情報提供サービス担当チームがベンダに開発と保守を委託している。サイトαの画面遷移図を図1に，画面遷移の仕様を表1に示す。



注記1　ログインページ以外からのマイページへの画面遷移，エラー時の画面遷移，画面を戻るための遷移，ログアウトの画面遷移は省略している。
注記2　全画面とも同一ドメイン（www.e-sha.co.jp）で提供されている。

図1　サイトαの画面遷移図（抜粋）

表1　サイトαの画面遷移の仕様（抜粋）

画面遷移	PCでの操作例，URL及びPOSTデータ	操作の結果
(あ)	操作例：利用者ID（例：user0302）とパスワード（例：aBcD1234）を入力し，ログインボタンを押す。 URL：https://www.e-sha.co.jp/login POSTデータ：action_id=login&user_id=user0302&passwd=aBcD1234	・user_idと，passwdのハッシュ値がサイトαに登録されたものと同じ場合，新しいセッションID（JSESSIONID）とセッションオブジェクトが取得され，マイページが表示される。JSESSIONIDはCookieに格納される。それ以外の場合，セッションIDとセッションオブジェクトは取得されず，ログインページに戻る。 ・ログイン記録（利用者IDと時刻）が取得される。
(い)	操作例：現在のパスワード（例：aBcD1234）と新しいパスワード（例：aBcD5678）を入力し，変更ボタンを押す。新しいパスワードは確認のために，2回入力する。 URL：https://www.e-sha.co.jp/member/changepasswd POSTデータ：action_id=submit&old_passwd=aBcD1234&new_passwd1=aBcD5678&new_passwd2=aBcD5678	・次を全て満たす場合はパスワードがnew_passwd1の値に変更され，次画面が表示される。 - old_passwdのハッシュ値が，サイトαに登録された現在のセッションをもつ利用者のパスワードのハッシュ値と同じである。 - old_passwdとnew_passwd1の値が異なる。 - new_passwd1とnew_passwd2の値が同じで，かつ，定められた複雑さを満たす。 ・それ以外の場合はパスワードが変更されず，エラー画面が表示される。
(う)	操作例：名前（例：Bob）とコメント（例：よろしく）を入力し，確認ボタンを押す。 URL：https://www.e-sha.co.jp/member/profile POSTデータ：action_id=confirm&nickname=Bob&comment=%E3%82%88%E3%82%8D%E3%81%97%E3%81%8F [1]	・nicknameとcommentに入力された値がセッションオブジェクトに格納され，次画面が表示される。profile_tokenが生成されてセッションオブジェクトに格納され，profile_token（例：CACC321A638BBC11DE9352EB8D5E56A3）がプロフィール確認画面のhiddenに格納される。 ・プロフィール入力・変更画面では一部のHTMLの要素の入力が許可されている。（許可されている要素：b，font，i，s，sub，sup，u） ・コメントにURLを記載するとリンクとして表示される。
(え)	操作例：退会理由（例：特になし）を入力し，退会確認ボタンを押す。 URL：https://www.e-sha.co.jp/member/taikai POSTデータ：action_id=confirm&taikai_message=%E7%89%B9%E3%81%AB%E3%81%AA%E3%81%97 [2]	・taikai_messageに入力された値がセッションオブジェクトに格納され，次画面が表示される。taikai_token（例：B582DF03524FBB9DBCCE0BA0610F2EA1）が生成されてセッションオブジェクトに格納され，退会確認画面のhiddenに格納される。[3]

表1　サイトαの画面遷移の仕様（抜粋）（続き）

画面遷移	PCでの操作例，URL及びPOSTデータ	操作の結果
(お)	操作例：退会ボタンを押す。 URL：https://www.e-sha.co.jp/member/taikai POSTデータ：action_id=submit&taikai_token=B582DF03524FBB9DBCCE0BA0610F2EA1	・taikai_tokenの値がセッションオブジェクト内の値と同じ場合，退会処理が行われ，次画面が表示される。違う場合，退会処理が行われず，エラー画面が表示される。 ・退会処理時にセッションIDとセッションオブジェクトが無効にされ，ログアウトされる。

注[1]“よろしく”をURLエンコードした値
注[2]“特になし”をURLエンコードした値
注[3] taikai_tokenの値が0になることはない。

〔利用者からの問合せ〕

ある日，サイトαの利用者L氏から，“今朝9時にログインし，サイトαを利用していたら，10時に急にログアウトさせられ，その後ログインできなくなった。パスワードを再設定しようとしたが，エラーが表示され，再設定できない。”という内容のメールがE社宛てに届き，他にも同様の問合せが数件来た。

情報提供サービス担当チームのXさんがサイトαの会員情報データベースにアクセスし，L氏の情報を確認したところ，退会処理が完了していた。Xさんは，誰かが嫌がらせ目的でL氏のアカウントで不正ログインし，退会処理を行った可能性を疑った。①Xさんは，L氏に詳細な利用状況を確認し，その確認内容とログイン記録を照合した結果から，L氏のアカウントは少なくとも今日は不正ログインされていないとの結論に至った。

Xさんが，ログインできなくなる前にどのような操作をしたかをL氏に聞いたところ，サイトα内の掲示板に投稿していた人のプロフィール画面を見て，そこに記載されていたリンクをクリックしたとのことであった。リンク先は，別サイトのURLであり，かつ，Xさんが確認した時点ではリンク先は既に削除されていた。

Xさんは，今回の事象が起きたのはサイトαに脆弱性があるからかもしれないと考え，セキュリティ専門業者J社にWebアプリケーションソフトウェアの脆弱性検査（以下，WebAP検査という）を依頼することにした。WebAP検査の結果，脆弱性が二つ（以下，脆弱性1，脆弱性2という）検出された。

〔脆弱性1について〕

脆弱性1は [a] の脆弱性であった。脆弱性1を確認した手順を表2に示す。

表2　脆弱性1を確認した手順

項番	手順	画面遷移（お）を試みる際のPOSTデータ	表示された画面
1	画面遷移（え）を行った後，画面遷移（お）を試みる	action_id=submit&taikai_token=B582DF03524FBB9DBCCE0BA0610F2EA1 [1]	退会完了
2	画面遷移（え）を行った後，画面遷移（お）を試みる	action_id=submit&taikai_token=0	エラー画面
3	画面遷移（え）を行った後，画面遷移（お）を試みる	action_id=submit	退会完了
4	画面遷移（え）を経ずに，ログイン後すぐに画面遷移（お）に相当するアクセスを試みる	action_id=submit&taikai_token=0	エラー画面
5	画面遷移（え）を経ずに，ログイン後すぐに画面遷移（お）に相当するアクセスを試みる	action_id=submit	エラー画面

注[1] 画面遷移（え）で生成されたtaikai_tokenの値とする。

次は，Xさんが J社の情報処理安全確保支援士K氏から，脆弱性1についての報告を受けた時の会話である。

Xさん：開発委託時の要件に [a] の脆弱性への対策を含めていたので，脆弱性1の対策はできていると思っていました。

K氏　：対策を試みたけれど，プログラムの実装に不備があったようです。プロフィール確認画面についても脆弱性1が確認されています。

Xさん：そうですか。退会処理が行われてしまった利用者がクリックしたリンク先はどのようなものだったのでしょうか。

K氏　：例えば，図2のようなHTMLです。このHTMLは，表2中の項番 [b] のような動作をWebブラウザにさせます。

Xさん：変更操作がある画面のうち，パスワード変更画面は，そもそも [a] の脆弱性への対策をしていませんが，問題ありませんか。

K氏　：パスワード変更画面では表1にあるように，[c] を入力させる仕様

です。[c]は攻撃者が[d]情報であることを前提としてよいので，問題ありません。画面遷移（お）のような実装の不備もないようでした。

```
 1 <html>
 2 <head>
 3 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
 4 </head>
 5 <body>
 6 <iframe src="ifrm1.html" width="1" height="1" name="ifrm1"></iframe>
 7 <iframe src="ifrm2.html" width="1" height="1" name="ifrm2"></iframe>
 8 <form target="ifrm1" method="POST" action="https://www.e-sha.co.jp/member/taikai">
 9 <input type="text" name="action_id" value="[ e ]">
10 <input type="text" name="taikai_message" value="OK">
11 <input type="submit">
12 </form>
13 <form target="ifrm2" method="POST" action="https://www.e-sha.co.jp/member/taikai">
14 <input type="text" name="action_id" value="[ f ]">
15 <input type="submit">
16 </form>
17 <script>setTimeout('document.forms[0].submit()',0);</script>
18 <script>setTimeout('document.forms[1].submit()',1000);</script>
19 </body>
20 </html>
```

図２　退会処理が行われてしまう HTML

〔脆弱性２について〕

脆弱性 2 は“クロスサイトスクリプティング”であった。脆弱性 2 を確認したのはプロフィール入力・変更画面であった。次はＫ氏とＸさんとの会話である。

Ｋ氏　：プロフィール入力・変更画面は，利用者が入力できる HTML の要素が制限されています。しかし，例えば“<b>”タグ中に，②特定の属性を指定することによってスクリプトの実行が可能です。スクリプト実行の結果，Cookie の属性の設定によっては，Cookie の情報が盗まれます。これを用いて，[g]が行われ，勝手にプロフィールを閲覧されたり，変更されたりするおそれがあります。

Ｘさん：そういうことですか。では，利用者が入力できる HTML の要素の制限は変

えずに，[h]という仕様に変更したいと思います。

K 氏　：それで問題ありません。

X さんは，二つの脆弱性について，対策をベンダに依頼した。対策後，J 社に WebAP 検査を依頼し，問題がないことを確認した。X さんは，リリース前の WebAP 検査の義務化を Q さんに提案し，採用された。

設問 1　本文中の下線①について，L 氏のアカウントが不正ログインされていないとの結論に至るには，L 氏に確認した内容から分かる何の値と，ログイン記録から分かる何の値を抽出して，一致していることが確認できればよいか。それぞれ 25 字以内で述べよ。

設問 2　〔脆弱性 1 について〕について，(1)～(4)に答えよ。

(1)　本文中の[a]に入れる脆弱性の名称を，カタカナ 20 字以内で答えよ。

(2)　本文中の[b]に入れる表 2 中の項番を 1～5 から選び，数字で答えよ。

(3)　本文中の[c]，[d]に入れる適切な字句を，それぞれ 10 字以内で答えよ。

(4)　図 2 中の[e]，[f]に入れる適切な文字列を，それぞれ 10 字以内で答えよ。

設問 3　〔脆弱性 2 について〕について，(1)～(3)に答えよ。

(1)　本文中の下線②に該当する属性を解答群の中から全て選び，記号で答えよ。

解答群

ア　accesskey	イ　class	ウ　hidden	エ　id
オ　lang	カ　onclick	キ　onmouseover	ク　title

(2)　本文中の[g]に入れる攻撃の名称を 15 字以内で答えよ。

(3)　本文中の[h]に入れる仕様を 25 字以内で具体的に述べよ。