

# 平成26年度「Webアプリケーション」定期試験問題

2015-02-09 国島丈生

## 第1問

次について、簡潔に説明しなさい。(各5点)

1. URIスキーム
2. HTTPのステートレス性
3. クッキー
4. Webブラウザのキャッシュ

## 第2問 (HTML, Webアプリケーション)

次の文章中の空欄に、適切な用語を埋めなさい。(2点×7)

Webブラウザで表示されるWebページは、通常HTMLと呼ばれる形式で記述される。HTMLでは、プレインテキスト中に、<p>や</p>などの[ a ]を用いてテキストの意味が表されている。例えば、テキスト中の「例」という文字列からhttp://example.com/へのリンクを張るためには、<[ b ]>と</[ b ]>という[ a ]を用いて、<[ b ] [ c ]="http://example.com/">例</[ b ]>というように記述する。

Webブラウザは、HTMLで書かれたページを読み込むと、内部データ構造として木を構築する。この木を[ d ]という。[ e ]というプログラミング言語で書かれたプログラムをWebブラウザ内で実行させて、この木を操作すると、Webページの表示が変更される。このことを応用すると、Webブラウザ内でプログラムからネットワークアクセスを行ってデータを取得し、そのデータを用いてWebページの表示を変更することができる。この技術を[ f ]と呼ぶ。

この技術を用いると、最初にWebページを読み込むだけで、以降は別ページへの遷移をすることなく動作するWebアプリケーションが構築できる。このようなWebアプリケーションを、Webクライアントで主に動作するという意味で[ g ]、または単一Webページで動作するという意味でSPA (Single Page Application) という。

## 第3問 (HTTP)

次の文章中の空欄に、適切な用語を埋めなさい。(2点×18)

Webで最も広く用いられている通信プロトコルであるHTTPは、TCPの上位層である[ a ]層に属するサーバ・クライアント型の通信プロトコルであり、デフォルトのTCPポート番号は[ b ]番である。また、[ c ]暗号を利用したTCP/IP通信路の暗号化技術である[ d ]を用いてセキュアな通信を実現する[ e ]というプロトコルもWebで用いられている。

HTTPの通信は必ず[ f ]から始まる。つまり、最初に[ f ]から[ g ]に対して処理の要求

([ h ]メッセージ) が送られ、[ g ]は対応する処理を行った後、結果 ([ i ]メッセージ) を[ f ]に送信する。

HTTPでは、URIで表される[ g ]上のリソースに対しておこないたい処理の種類を[ j ]という。現在最も普及しているHTTPバージョン[ k ]では、[ j ]として[ l ],[ m ],[ n ],[ o ], HEAD, OPTIONS, TRACE, CONNECTの8種類が用意されている。

またHTTPでは、[ g ]側の処理結果を[ f ]に伝える仕組みとして、処理結果の種類を番号で[ g ]から[ f ]に返す。これを[ p ]という。[ p ]のうち、正常に処理が終了した場合は[ q ]番台の番号が、サーバ側の原因で処理が正常に終了しなかった場合は[ r ]番台の番号がそれぞれ使われている。

## 第4問 (Webアプリケーションのセキュリティ)

以下の問に答えなさい。

1. 通信に関わるセキュリティ上の脅威として、盗聴、改ざん、なりすましの3つがある。これらについて、どのような脅威なのか、説明しなさい。(15点)
2. Webアプリケーションで注意しなければならないセキュリティ上の脅威の一つにHTMLインジェクションがあります。どのような脅威なのか説明しなさい。説明の中には、どのような状況で発生しやすいのか、どうやって防ぐのか、などについて述べるようにしてください。(15点)

# 平成26年度「Webアプリケーション」定期試験問題解答例

## 第1問

1. (URIスキーム) インターネット上の資源の所在を表すURIの先頭部分で、資源に到達するための手段(プロトコル)を表したもの。
2. (HTTPのステートレス性) サーバがクライアントのアプリケーション状態を保存しないプロトコルをステートレスという。HTTPはステートレスなプロトコルであり、リクエストメッセージには、そのリクエストを処理するのに必要な情報をすべて含める。
3. (クッキー) HTTPにおいてアプリケーション状態を管理するために、Webブラウザに保存される情報。
4. (Webブラウザのキャッシュ) ブラウザがアクセスしたWebページなどのデータを一時的にクライアントコンピュータ上に保存する機能。

## 第2問

a. タグ b: a c: href d: DOM e: JavaScript f: Ajax g: クライアントサイドアプリケーション

## 第3問

a: アプリケーション b: 80 c: 公開鍵 d: TLS (SSL) e: HTTPS f: クライアント g: サーバ h: リクエスト i: レスポンス j: HTTPメソッド k: 1.1 l: GET m: PUT n: POST o: DELETE p: ステータスコード q: 200 r: 500

## 第4問

1. 盗聴は、通信路を流れるデータを第三者が盗み聞きすること。改ざんは、通信路を流れるデータを第三者が不正に書き換えること。なりすましは、第三者が、正規の通信相手になりすまして通信内容を不正に取得したり、偽の通信データを送りこむこと。
2. HTMLインジェクションは、ユーザのブラウザで表示されるHTMLに、サーバ管理者の意図しないHTMLコードを混入させられてしまうことである。これにより、サーバ管理者の意図しないJavaScriptプログラムをブラウザ上で実行させられるなどの被害が起こる。SNS、ブログ、掲示板など、サーバ管理者以外の人に起因するデータをWebページ上に表示する場合に多く発生する。主な原因は、サーバ管理者以外の人に起因するデータ中にHTMLの特殊な文字が含まれていた場合に、これらのエスケープ処理を怠っていることである。