20160209 WEBアプリケーション定期試験問題

2015年度「WEBアプリケーション」定期試験問題

2016-02-09, 国島丈生

第1問

1. URIにおいて、URIスキーム、ホスト名、パス、クエリパラメータ（GETパラメータ）とはどの部分を指し、どういう意味を持っているのか、URIの例を自分で示した上で、その例を用いながら説明しなさい。（15点）
2. WebブラウザでURI http://example.jp/sample.html を表示させる状況を考えます（ユーザが手でURIを入力する、リンクをクリックするなど）。このページが表示されるまでにブラウザ内で行われる処理を、順を追って説明しなさい。このページは、内部で次のリソースだけを参照しているものとします。（15点）
   - http://example.jp/sample.js（JavaScriptファイル）

第2問

1. 主にサーバとクライアントとで行われる通信の観点から、HTTP Cookieの仕組みを説明しなさい。（10点）
2. Webアーキテクチャスタイルの観点から、HTTP Cookieがなぜ必要なのか、説明しなさい。（10点）

第3問

1. インターネットにおけるセキュリティ上の脅威には、盗聴、改ざん、なりすましの3つがあります。このうち2つを各自で選び、SSL/TLSがそのセキュリティ上の脅威に対してどのように対策しているのかを説明しなさい。（各20点、計40点）
2. セキュリティ上の脅威を軽減するため、Webブラウザ内でJavaScriptプログラムを実行する場合には、いくつか制限がかけられます。どのような制限がかけられるか、列挙しなさい。（10点）

解答例、ポイントなど

第1問

1. 例として、次のURIを考える。
   http://example.jp/blog/search?date=20160209&category=web
   このとき、
   - ”http” の部分をURIスキームと言い、リソースにアクセスするプロトコルなどを表す。
   - “example.jp” の部分をホスト名と言い、リソースを提供するサーバ名（またはサーバのIPアドレス）を表す。
   - “/blog/search” の部分をパスと言い、サーバ上でのリソースの識別子を表す。
   - “date=20160209&category=web” の部分をクエリパラメータと言い、サーバに渡すパラメータをあらわす。この例では、パラメータ date として 20160209 を、パラメータ category として web をそれぞれ指定している。
2. 次のような手順になる。
   1. サーバ example.jp に対しHTTPリクエストを行い、リソース /sample.html へ HTTPメソッド GET を実行する。
   2. サーバからのレスポンスを解析し、得られた HTML データを構文解析して DOM と呼ばれる内部データ構造をブラウザ内に構築し、ブラウザで表示（レンダリング）する。
   3. DOMから外部リソースのURIをすべて抽出し、これらを取得する。この例では、http://example.jp/sample.jsの取得、すなわちサーバ example.jp に対しHTTPリクエストを行い、リソース /sample.js へ GETメソッドを実行する。
   4. サーバからのレスポンスを解析し、得られたJavaScriptプログラムをブラウザ内で逐次実行する。

順番は多少前後しても良い（ブラウザごとに挙動が異なる可能性があるため）。ポイントは、sample.htmlの取得→DOMの構築→sample.jsの取得→JavaScriptの実行、という流れが書けているかどうかである。

第2問

1. Webクライアントからのリクエストに対してサーバがレスポンスを返す時、ヘッダに Set-Cookie フィールドをつけて返信することがある。これがHTTP Cookieであり、この後、このWebクライアントが同一サーバに対してリクエストを行う時は、サーバから送られてきたHTTP Cookieをリクエストヘッダに Cookie フィールドとして付与する。
2. HTTPはステートレスの通信プロトコルであり、原則としてサーバはクライアントの状態を保存しない。しかし実際には、ユーザのログインなど、サーバでクライアント状態を保存したい場合がある。このような場合にHTTP Cookieが使われる。ユーザのログインでいうと、ユーザ認証が成功すると、サーバから、認証したユーザの情報がHTTP

Cookieとしてクライアントに渡され、以降ログインした状態でHTTP通信が行われることになる。

ポイントは、1ではサーバからクライアントにCookieが渡されることと、以降は渡されたCookieがクライアントからサーバへのリクエストに付与されること、この2点です。2では、ステートレスな通信プロトコルであるHTTPでクライアント状態を扱うときに必要である、という点です。

第3問

1. 以下の通り。
   - 盗聴：通信内容の暗号化には共通鍵暗号が用いられる。共通鍵をクライアントとサーバで安全に共有する手段として、公開鍵暗号が用いられる。1. クライアントはサーバの公開鍵Pを取得 2. クライアントが共通鍵Cを生成してPで暗号化し（E(P, C)）、サーバに送信 3. サーバはPとペアになる秘密鍵Sで受信内容を復号し、Cを取得する
   - 改ざん：一方向ハッシュ関数を用いたデータダイジェストを用いる。1. 送信側で、送信したいデータDのダイジェストF(D)を計算し、DとF(D)を共に送信 2. 受信側は、送られてきたデータD'からダイジェストF(D')を計算し、F(D)と比較する。F(D) = F(D')なら改ざんはないと考えられる。
   - なりすまし：公開鍵暗号を用いた電子署名を用いる。 1. サーバは、あらかじめ公開鍵Pを認証局に送り、認証局の秘密鍵S'で暗号化しておいてもらう（E(S', P)） 2. サーバは公開鍵Pの代わりに 1. の結果 E(S', P)を公開 3. クライアントは E(S', P)を取得すると、認証局の公開鍵P'をさらに取得し、これで復号を試みる。成功すればPは信用できる（なりすましがない）と考えられる。
2. 次の通り。
   - ローカルファイルへのアクセス禁止
   - プリンタなどの資源の利用禁止
   - JavaScriptによるサイトをまたがったアクセスの禁止（同一生成元ポリシー）

1は、上の例のようにデータの流れまで書いてはじめて十分な解答であるとみなします。