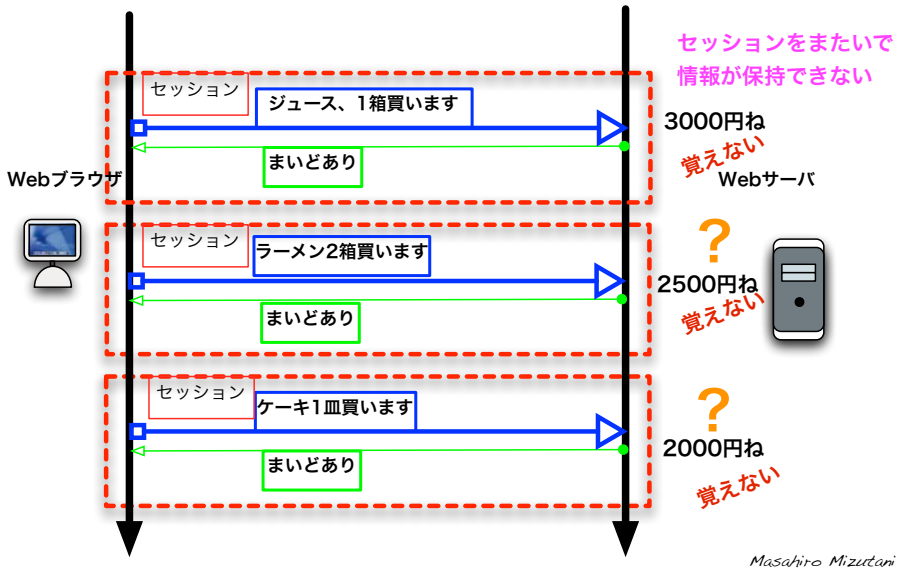
Cookieの周辺
と
Webアプリケーション

水谷正大

*HTTP*の特徴と問題点

- 非常に単純
  - HTTP要求とその応答が１つのセッション
- ステートレス（stateless）
  - 次の通信は前のセッション結果と何ら関係を持たない
    - 処理結果は残さずに、その都度廃棄される
- トランザクション処理では工夫が必要
  - 状態を維持できないために、関連する複数の処理を一つの処理単位としてまとめることができず工夫が必要
    - ユーザ認証をした上でのページ移動
    - 複数選んだ商品の購入決算

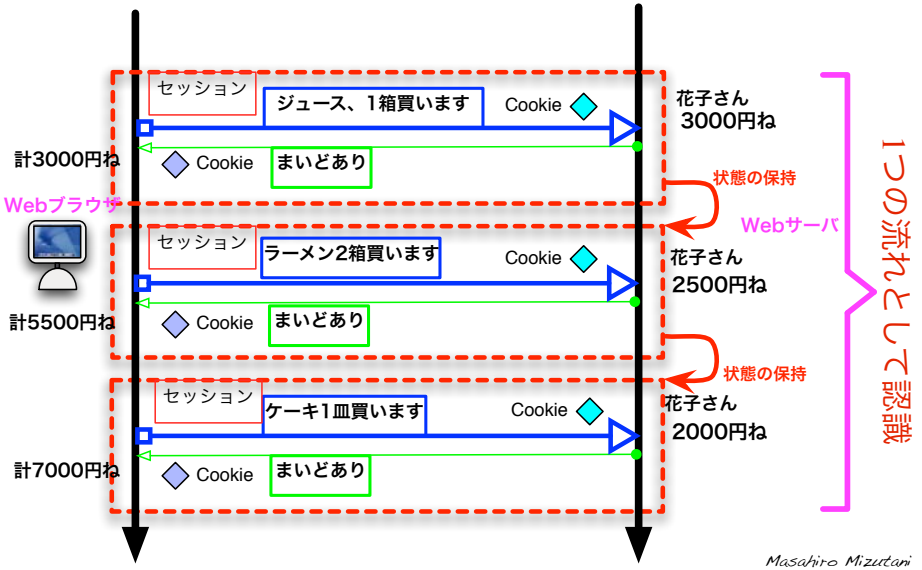
ステートレスなHTTP通信



クッキー（cookie）の利用

- トランザクション処理を可能
  - クッキーを使って状態を維持
- クッキーの仕組み (RFC2965/6265)
  - サーバからクッキーをブラウザに渡す
    - HTTPヘッダに埋め込むかJavascriptで利用
  - ユーザ情報をクッキーに書き込む
  - 同じURL（やサーバ）に接続するときはクッキー情報をサーバに送信
  - WebクライアントとWebサーバ間でお互いを認識し、継続的なデータ交換を可能にする

Cookieを使ったHTTP通信



Cookieを使う

1) Webサーバは応答ヘッダで指定してブラウザにCookieを渡す(Set-Cookie)

Set-Cookie: Customer="Taro_Jirou"; expires="25 Nov 2015 08:36:20 GMT"; path=/Shopping; domain=happy-shopping-town; secure

2) ブラウザが同じWeb サーバと通信する時に、CookieをサーバにCookie送信(Cookie)

Cookie: Customer=" Taro_Jirou"; PartItem="Lemon_0987",Shipping="Post";

3) サーバをCookieを受け取ると、DBに問い合わせてユーザを特定、ブラウザに渡す情報をカスタマイズして送信

以降は、2, 3 を繰り返して通信する

Cookieの条件

- 有効期限（expires属性）内のCookieは保存
- Cookieの数は最大300個まで
- 1つのCookieは最大4KBまで
- 1つのサーバにつき、Cookieは最大20個まで

HTML を用いて Cookie の値を記録させることができる

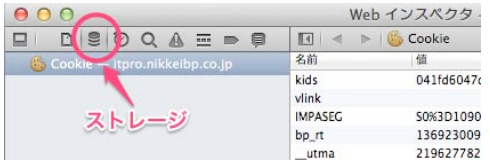
```
<meta http-equiv="Set-Cookie" content="〜">
```

〜の部分に *NAME*=値; expires=値; domain=値; path=値; secure

Cookieを表示する（1）

Internet Explorer　テキストファイルなのでエディタで開くだけ

Safari　(a) [環境設定]/[詳細]/メニューバーに"開発"メニューを表示



[開発]Webインスペクタを表示
[ストレージボタン]

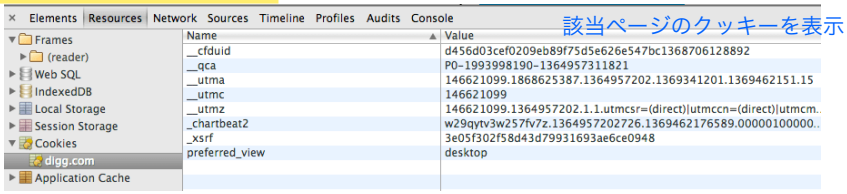
該当ページのクッキーを表示

(b) Safari Cookieを使う(MacOS)　http://sweetpproductions.com/safaricookies/

クッキーを管理できて便利

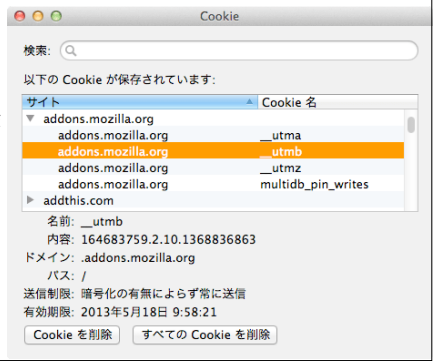
Cookieを表示する（2）

Google Chrome　[表示]/[開発/管理]/デベロッパーツール



Firefox

(a) [環境設定]/[プライバシー]Cookieを個別に削除



(b) アドオン Firebug を使って編集

Cookieの課題

- セッション・ハイジャック
  - 第三者にセッションIDを読み取られる
- トラッキング・クッキー
  - ユーザのアクセス履歴の追跡
  - Web広告業者、マーケティング
    - 第三者への情報開示

Cookieの信頼性=Cookieの管理者の信頼

サイト内容が信頼できないとき
はCookieも信頼すべきでない

Masahiro Mizutani

Weサイト側の不手際による危険性

Cookieが盗まれたら

成りすまし

サーバーはクッキーの内容を見てクライアントを判別するだけで、送信されてきたクッキーが盗まれたものであるか否かは判断できない

別サイトで発行されたCookieは受け取らない

セッションフィクセーション

取得したセッションIDをセットして新規ユーザー登録画面へ誘導する罠をしかける

クロスサイト・リクエスト・フォージェリ（CSRF）

カートへの追加リクエストを対象としたCSRF攻撃を受けると、セッション変数が上書きされてしまい、結果としてカートの中身が書き換えられて意図しない商品を購入させられてしまう

Masahiro Mizutani

Cookieは危険なのか？（1）

決められたサーバーや指定のディレクトリにあるHTMLファイルを要求したときにのみ、Cookieをサーバーへ送信

ユーザが管理方法を間違えない（パソコンを盗まれない）限りCookieは外部へは出ない

Cookieファイルはテキストファイルなので、すぐさまプログラムとして動作させることは不可能（ウイルスでない）

Webサーバーのソフトの欠陥 または管理者によるCookieの設定ミスによるクロスサイトスクリプティングなどの脆弱性があり得る

Masahiro Mizutani

Cookieは危険なのか？（2）

Cookieを利用した個人の行動監視　**トラッキング**

元々、Web サーバはどのIPアドレスからどのページが何回呼び出されたか把握・記録している（Webの仕組み）。誰がどのページを見たのかを知るためにCookieを使って識別番号を誰がどう閲覧したかは分かるようになる。

さらにユーザー登録という形で付加サービスを利用するときに、実名や住所を入力すると、利用者が完全に特定できる

トラッキングを利用したターゲット広告

広告にCookieを埋め込むことで、広告企業は誰がどのサイトでどの広告を見たのか把握することができる。広告マーケティングにCookieが利用されている（この是非は議論すべきだ）。

ただし、現在閲覧しているページ以外の第三者サーバーがCookieを要求しても送信しないようにできるWebブラウザ機能がある

Masahiro Mizutani

Cookieファイルは定期的にチェック

ユーザの知らない間にクッキーが使われている

- Webサイト上の**行動履歴**
  - プライバシの問題も生じ得る
  - 信頼できないサイトによるCookieの悪用
- Webブラウザは最新版を使う
- 定期的にCookieファイルのチェックと削除
  - 各種ブラウザを使い分けて、その設定や特長を把握
  - Windows：IEの[ツール][インターネットオプション][全般]から「Cookieの削除」

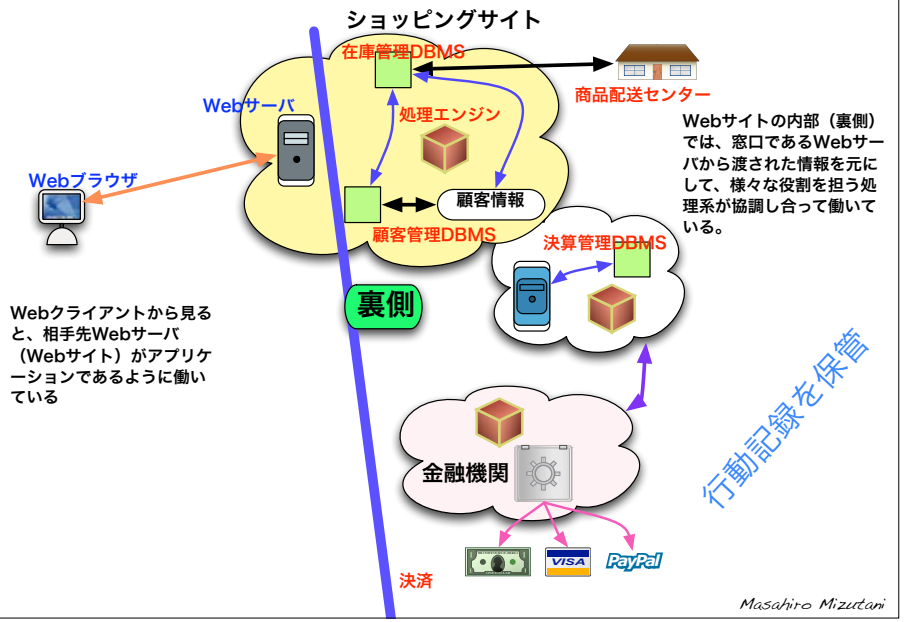
Masahiro Mizutani

Cookieにさえ気をつければ行動履歴の追跡から安全か？

まったくNO！

Masahiro Mizutani

Webアプリケーション



Masahiro Mizutani

アプリケーションの変遷

- デスクトップアプリケーション
  - ローカル端末内にインストール
- Webアプリケーション
  - 同等な処理をWebを通じて実現する
    - 写真管理
      - Flicker/Picasa
    - 文書・表計算・プレゼン
      - Google Doc/Office Web Apps
  - 窓口であるWebサーバを通じてさらに多様なサービスを提供

Masahiro Mizutani

Webアプリの利点

- 端末アプリの管理から開放される
  - 端末側にはWebブラウザだけがあればよい
  - Webサイトの内側でなされている複雑な処理はマスクされてユーザからは見えない
- 端末側の負担を小さくできる
  - 要求ハードウエア仕様が低い
- Webサービスの充実
  - サービスを提供するWebサイトにアクセスできれば多様なサービスを享受できる

Masahiro Mizutani

Webアプリケーションの活況

- 多様な複数デバイスの利用が浸透
- クラウドサービスの拡大
  - メール、ショピング、バンキング/トレード、ブログ、SNS、twitterなど全方面で
  - ユーザは処理をネットワーク経由でサービスとして受け取る
    - 情報共有サービスの活況（Google Docs等）
- 新しいビジネスを牽引
  - ソフトでなくサービスに課金

Masahiro Mizutani

クラウドの問題点

- ユーザの都合でサービス内容を変更できない
- クラウド提供側の機器障害、倒産などの事由によりサービスが停止する
- クラウド側に全データが集中している情報管理上の問題
  - 情報流出のリスク
    - 攻撃対象になりやすい
    - クラウドの破壊や政治的利用の影響が甚大

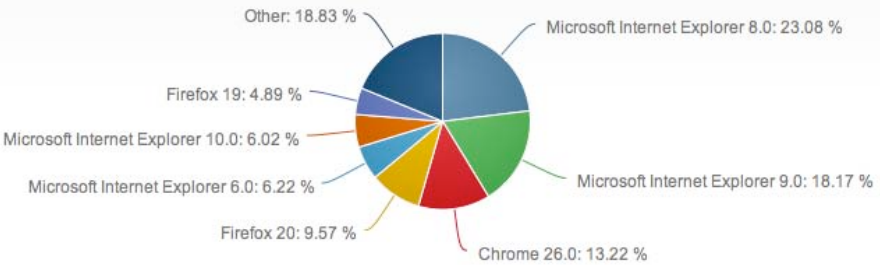
Masahiro Mizutani

ブラウザ戦争

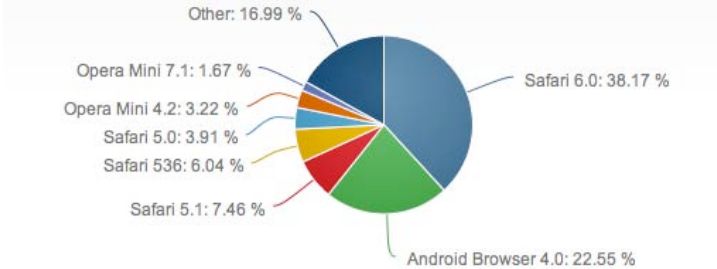
- ブラウザはクラウドサービスの最前線に位置
- 早く、軽い高機能Webブラウザの開発競争
  - Firefox, Google Chrome
  - Internet Explore, Safari
  - Operaなど
- プラグイン＋拡張機能の提供
- Apple iPhone/iPadでのAdobe Flash非採用
  - HTML5+CSS3の登場

http://www.netmarketshare.com/browser-market-share.aspx

パソコンWebブラウザシェア 2013年4月



Mobile/Tablet Webブラウザシェア 2013年4月



http://jp.techcrunch.com/archives/20120625chromebooks-education-500-school-districts/

GoogleのChromebookを合衆国とヨーロッパの500の校区が採用-その"ノー管理"が魅力

by Frederic Lardinois on 2012年6月26日

学校は、GoogleのChromebookがある程度成功している市場のようだ。今日（米国時間6/25）のGoogleの発表では、今合衆国とヨーロッパで500の校区がChromebookを積極的に利用しているそうだ。最近はノースカロライナ州のRockingham郡とTransylvania郡、ウィスコンシン州のFond du Lac校区の計3地区がChromebookを採用した。

Chromebookがこのように学校で採用され始めている理由の一つとして、Smarter Balanced Assessment Consortiaと Partnership for Assessment of Readiness for College and Careers(PARCC)が新たに定めたハードウェアとオペレーティングシステムに関するガイドラインに合っていることが挙げられる。

Googleはさらに、今日行われているInternational Society for Technology in Education(ISTE)の会議で、児童生徒と管理者向けの新しいツールとWebアプリケーションをいくつか発表した。Googleによればそれらのツールにより、"Webアプリケーションを全校向けに見つける、利用する、インストールする、そして管理することが一層容易になる"そうだ。Chromebookの管理コンソールから一つの学年全体向けのアプリケーション集をインストールでき、アプリケーションはGoogle Apps for Educationと緊密に連携利用できるものが提供される。また管理者は、Chrome Web Storeから適切と思われるアプリケーションをピックアップして、児童生徒や教師、スタッフなどに推奨できる。

今日のISTEの会議では、ST MathやVoiceThreadやAchieve3000など数社が、Chrome向けの教育アプリケーションを紹介し売り込んでいた。

今日の発表文の中でGoogleは、"学校では、必要なものはWebだけである"と豪語している。言い過ぎかもしれないが、一面の真理はあるかもしれない。ChromebooksのOS/ハードウェアの仕様は最近やや変わってきたとはいっても、当面はニッチにとどまるだろう。でも学校では、これまでのラップトップよりはChromebooksのほうが魅力的だ。ウィルスと無縁、アップデートはアプリケーション側で勝手に行われるなど、管理コストが格安だから。

Googleの挑戦と身勝手

- オープンソースとして無償で提供
- Chrome OS
  - Webの閲覧とWebアプリケーションの動作に適したコンピュータ環境(Linux OS+Chrome), 2011年にChromebookとして販売開始
- Android
  - スマートフォン携帯端末のための環境
- サービスの停止 http://digg.com/reader
  - Google Readerの停止を宣言