Web を支える情報通信技術（１）
――授業紹介――

2007 年 4 月 16 日
情報基盤センター
佐藤周行・中山雅哉・西村健

１．はじめに

このゼミナールは、高校を出たて、または Web を使いこなして勉強しているが、その仕組についてはこれまであまり気にしてこなかった学生を対象にして、Web とは何ものか、Web はどういうソフトウェア技術に支えられているのか、ということを実感してもらうために開講するものである（気宇壮大）。

現在の IT 技術がインターネット技術に支えられていることは関係する技術に携わっていない人でも感覚的に理解していると思うが、ではその「インターネット技術」とは何？といわれると、これが多岐にわたっていて、一言では説明しづらい。そこで、このゼミナールでは、Web という、われわれと一番なじみの深いものを題材にとって、具体的な技術を解説し、実感してもらうという方法をとることにした。

Web といっても、これまた関係するものが多すぎて、一言で「これ」とはいいがたい。一言で言い表せないけれど、われわれの身近にあって役に立っているのである。これを少しずつ解剖していこう。解剖には、少しの知識と、少しの実験が必要である。「教えてこられなかっただろうな」と判断した点は、われわれが解説しよう。実験については、手を動かすことが必要である。その実験を解釈するのには、解説された知識を使って、頭を使うことが必要になる。暗号のようなデータの並びに一定の解釈を与えられるようになり、自分で何か別のこと（情報科学を本格的に学ぶことでもかまわないし、プログラミングをはじめることでもかまわない）をはじめようと思うようになることが、このゼミナールのもうひとつの目的である（大言壮語）。

この文書は、授業の第一回目に配布され、授業選択の材料として使われることを想定している。

２．このゼミナールの目的

このゼミナールの目的は、シラバスでは以下のように書かれている。

今やインターネット上でのデータ通信の主流となった Web は、情報科学的にさまざまな技術によって支えられている。この授業では、Web を支える技術としてデータの表現形式、データの通信方式（プロトコル）を中心に、セキュリティに関する機能までを講義と実験をとおして解説、実感する。

今日の目標は、この話がある程度（ぼんやりと）わかるようになることである。

３．Web とは何か

そもそも、Web とはなんだろうか？

「インターネットのことでしょう？」

「えと、契約したプロバイダにつなぐと、ホームページがまず出ますね。直感的なイメージを大切にすることはとても大切です。」

「あの IE のことじゃないんですか？」

「Windows で Web のページを見るときにはたいていこれですね（本当は他にもいろいろあるんですが）。これが最初に出てくるということは、よく使いこなしてるんでしょうね。」

「ホームページは作ったことがあるよ」

「うん。最近は便利なツールがたくさんありますから作るのは簡単ですよね。一昔前までは、ホームページ作成代行業がお金儲けになったって知ってます？今も、プロが作るのはデザインが違いますよね」

「ブログで情報発信だぁ」

「炎上しないように気をつけてね。」

「最近は何でも検索できるようになって便利ですね。Google のことじゃないんですか？」

「Web でほしい情報を得るのに検索は必須ですね。検索結果に一喜一憂する人たち（主にビジネスで）もいるそうです。Web につなげるときはまずここ、というものをポータルといいますが、Google は、自分もポータルになれるし、他のポータルにも検索バーを同居させていることがよくあります。で、Google はわれわれの首根っこを押さえ込もうとしている感じがしませんか？」

「Web2.0 というのはこのゼミナールに関係あるんですか？」

「Web をビジネスや社会的な点から論じることはぜひ必要ということは理解していますが、われわれはとりあえずこれにふれません。で、Web2.0 って何？」

「Web ってのは、HTML で書くんですよね。」

「ブログはどういう形式で保存されるか知ってます？」

「HTTP とか、HTTPS とか、TCP/IP とか、」

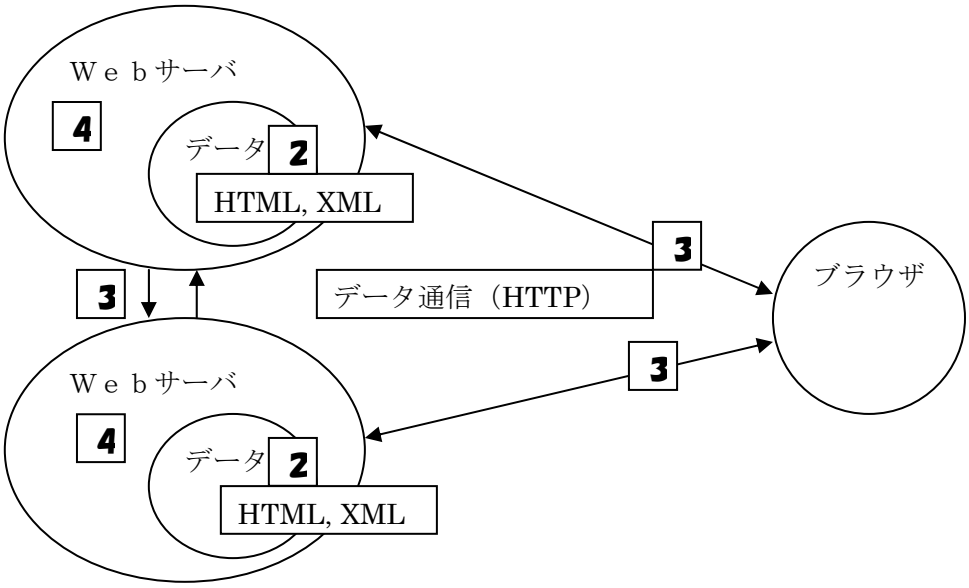
「キーワードだけ並べてもだめです。」

それで、Web っていったい何？

３．１　現代的なサービス[1]の仕組

われわれは、まず「多数のコンピュータが分散して存在している」ことを前提にしよう。そして、その前提となるもろもろのこと（一般的に環境ともいう）の上で、個々のコンピュータが連動して情報を処理し、全体としてひとつの処理を行っていることを想像してみよう。このような計算の環境を「分散計算環境」という。現代的な情報サービスは、この分散計算環境の上に提供されている。さて、Web である。Web とは、分散計算環境の上での情報処理を考えるときのデータの表現方式と通信方式を含めた処理の枠組のことだと思い込むことにしよう。

もちろん、このような抽象的なことばに満足してはいけない。実体として何があるのかを押さえておくのは重要である。Web を考えるとき、データの表現形式としては HTML と XML がある。通信方式としては HTTP がある。本体としての Web サーバのソフトウェアが動いていないと、そもそもがはじまらない。そしてブラウザがある。ブラウザは、われわれの一番近くにあるものである。



[1] 「サーバ」は、とりあえずなじみがあると思うが、ここで「サービス」に対する違和感を覚える人はいると思う。ここでは、デパートやレストランに限った話ではない。ここではより一般的に「ある要求に対して、その処理を行うこと」と考えてほしい。サービスを行うことが「サーブ」であり、それを行うシステムが「サーバ」である。「要求を出すもの」は「クライアント」というが、これも広告業界だけの用語ではない。

３．２　Web の特徴

Web を考えるときに HTML というデータ表現形式を抜きには語れない。HTML という形でデータ表現形式を統一したことで、今のように HTML で表現された膨大な Web の世界が作り上げられ、ブラウザを通してアクセスができるようになった。対人間では HTML は便利だが、対サーバでは XML というデータ表現形式が新たに出てきた。これは、Web サーバが人間だけでなく、他のサーバと語らってより大きなサービスを提供することが現実的になってきたことを意味する。

分散計算環境上で情報サービスを作り上げるためには、いくつかの流儀がある。Web を使った場合はどうだろうか。Web を使った場合、サーバどうしの結合度をゆるくとるのが一般的である。「結合度」とは、ここでは、処理を進める場合に互いに依存する度合いを小さく取る程度のことだと思うことにしよう。そんなわけだから、サーバの提供するサービスは、ある程度失敗してもやり直しが聞くとか、他に（機械の部品のように）取替えが容易にできるとか、という利点がある（ことになっている)。また、一度の通信ごとに処理が完結するように作り上げるのも一般的である（Cookie なんて言葉はとりあえず忘れる)。このように相互に通信を行う Web サーバが全体としてひとつのサービスを提供するようになっている。

３．３　Web を支えるもの　――ゼミナールの具体的なテーマ

では、このような Web は何に支えられているのだろうか。まずはデータ表現の方式と、その処理方式である。HTML や XML がキーワードになるだろう。

次が、それらをやりとりする通信方式である。HTTP はこのためのプロトコルの一つである。HTTP も、その下にいくつかもとになる通信方式があって、それらに支えられていることがわかる。インターネットで使われている通信方式一般の理解はとても重要である。この理解はこのゼミナールの最大の目的である。これらが理解できれば、Web サーバのソフトウェアの全体像の理解ができるようになるだろう。

もうひとつ、考えるべきことがある。サービスを提供するための技術である。コンテンツを通信技術で互いにやりとりして、何を提供したいのか？広報でも、検索でも、オークションでも、提供されるのは、「サービス」である。「サービス」の提供は Web の登場以前から行われていた。インターネットと Web は、それを大々的に行う枠組みを提供したのである。この時に、現実社会で提供されているサービスの「質」として重要なプライバシー保護や、必要に応じて情報を秘密にできることは、Web を使わないサービスでは、いろいろな方法で保証されてきた。実は、Web という枠組みでも、これらの質の保証ができるようになっている。このゼミナールでは、Web の上でこれらがどのように実現されているかをみることにしよう。このゼミナールでは特に「セキュリティ」というキーワードで論じられる。インターネットそのものは「安全に利用できる」ようなものではないことを実感し、ではどうしたらよいかについて、現在の技術を解説し、実験することで実感しよう。

実は、Web の世界でもサーバ証明書と HTTPS という形でセキュリティ技術が日常的に使われていること、それが現代的な暗号技術に立脚していること、それを社会基盤として提供する体制の構築が大切なこと、などについて解説する。

４．予備知識と、講義と演習の計画

とりあえず、意味不明の略語は、はじめはわからなくてもかまわない。また、「プロトコル」、「セキュリティ」などの（なんとなくわかっていても）説明を求められると窮してしまうような言葉についても最初は気にする必要はない。ゼミナールが終わるころにはきちんと理解できるようになる（ようにするのが教師の責任）。

講義とともに、演習を積極的に行う。演習はプログラミングをするというよりは、いろいろなツールを使って、Web が動作するときに何が起こっているかを観察することのほうが多いだろう。プログラミングが（現時点で）できないことは、このゼミナールの障害にはならない（たぶん）。

教科書であるが、特に指定しない。必要なプリントは教員側で用意して配布する。もっとも、参考書があると、いろいろ予習しやすいということはあるだろう。参考書がほしくなったら、教員側にアドバイスを求めてほしい。できるだけ親切（？）に対応したいと思う。

授業の評価は最終的に提出されるレポートでするとシラバスには書いたが、授業の中間でレポートを求めることがある（2 回程度）。これは、評価をマイナス側に倒すためには使わない。だから、積極的に提出して、自分の途中での理解度を深めるために利用してほしい。

さて、授業としては以下（次ページ）を計画している。今回が１．である。次回は２．である。３．については 5 月いっぱいを使う。5 月のおわりには Web サーバの実際の構築（インストールや設定）をしてみよう。6 月からは 5.1 にはじまり、7 月にかけて５．を取り扱う。６．はおまけである。3 ページの図中にある番号は、各章が現実の Web のシステムのどこに対応するかを示している。５．と６．がどこに対応するかは、ゼミナールが進行していく途中であらためて示すことにしよう。

1．授業導入：Web とその重要性
2．Web 上でのデータ表現
  2.1 HTML
  2.2 XML
3．Web のプロトコル
  3.1 HTTP
  3.2 TCP
  3.3 IP
4．Web サーバ構築
5．Web のセキュリティ
  5.1 インターネットにおける「安全」とは
  5.2 HTTPS と SSL
  5.3 公開鍵暗号技術
  5.4 サーバ証明書
  5.5 PKI
6．Web のこれから
  6.1 Web サービス

5．このゼミナールの Web ページ

http://www-sato.cc.u-tokyo.ac.jp/PKI-project/Komaba/にこのゼミナールの Web ページを用意している。教材を適宜置くので利用してほしい。

6．とりあえずのおわり

今回は授業紹介をした。次回から、上の授業予定にしたがって進行することになる。