このドキュメントは
Interpretation and Semantics on the Semantic Web
http://www.w3.org/DesignIssues/Interpretation.html
の和訳です。
このドキュメントには和訳上の誤りがありえます。
内容の保証はいたしかねますので、必ず W3C Web サイトの正式版ドキュメントを参照して下さい。

Tim Berners-Lee
Date: 1998, last change: $Date: 2000/01/18 20:03:25 $
状態:個人的見解. 編集状態:最初のドラフト.
(残念ながらここで用いている用語は、慣習的な哲学用語に従っていないと思う)
Design Issues へ

ウェブ アーキテクチャ の公理 :n

セマンティック ウェブの解釈と意味論

私たちは電子署名(digital signature)とセマンティックウェブのアーキテクチャのために基礎としていくつかの哲学を必要とする。
セマンティックウェブはコンピュータシステムであり、社会的に有益なタスクを実行するように機能すべく分散配置された機構である。商品の物理的配達や人に対するドキュメントのプレゼンテーションのように、セマンティックウェブ (SW) 世界と人々の社会的な世界の間に様々な署名のためのインタフェースがあるだろう。しかしながら、一般には、これらの重要な例外を除くと、セマンティックウェブは自己完結したループを形成するだろう。従って、SW にある何かの意味論は、SW 上あるいは現実世界との接点との関係から定義されるだろう。だから例えば、チェックを最初は、Fed が銀行のブラックボックスへ行ったとき何かするものと定義するかもしれない。その後で、SW の中で、ドルや転送(transfer)はチェックのためにすべて定義しなおして、自己完結したシステムにすることができる；それでもチェックを銀行に送るなど必要なリソースがあるけれども、それも、e-通貨、e-送り状、e-配達票、なんかを使う e-トレードにしてもいい。
これは、現実世界で、初期での通貨(coin)と金や請求書(bill)と通貨の関係に似ている。(英ポンドには、“ 私は署名され求めに応じて 1 ポンドの金額(the sum of pound)を運搬人に支払う約束をする　署名：イングランド銀行 ” と書かれていたものだ。)　その時から、ポンド紙幣は人々がそれをポンドと見なすようになり、元来の「the sum of pound」とは無関係になり、紙のお金は自己完結する。だから、我々がコンピュータシステム上に作ろうとしているマシン上の機能も（もっと、パリっと(crisply)定義されるだろうけど）トレードや裏書といった社会のプロセスと全く同等の役割を果たすだろう。
SW に結びつくアプリケーションは、以下の 3 つの理由を現在、考慮しようと考えている

1. SW と現在の社会システムのインタフェースが必要である、即ち、SW が少なくとも初期的にどのように動くのか
2. 我々が開発したい、立法的に支持された（そして皆に理解されている　など）の社会システム
3. 現在稼動しているシステムで、徐々にマシンに変更してゆきたいもの

我々の理由は、現在の定義は基本的であるとか、それらの仕様が内在的に美しい（実際本当に多くの現存するシステムは本当に crufy だよね）というものではない。重要なのは、SW 上で閉じている（自己完結の）ループを壊すような現実世界の意味論を定義しようとしているのではないってことだ。例えばセマンティックウェブのループとしては、

- a. Web サーバが要求への応答として許すリソース d へのアクセスは鍵 k1 で署名されている。
- b. 鍵 k1 がリストされている　[employee list] ドキュメントは、鍵 k2 で署名されている
- c. 鍵 k2 がリストされている　[w3c member] リストは、鍵 k3 で署名されている
- d. 鍵 k3 は、信用のために Web サーバが設定した鍵である。

この小さなシステムは、我々の Web サイトをご機嫌にコントロールすることができる。そしたら、実際、以下のような社会システムのモデルを設定できる。

- A. 人 P1 はメンバーサイトを読むのを許される
- B. 人 P1 は会社 C2 の従業員である
- C. C2 は、Hugo に関するコンソーシアムの会員である
- D. Hugo はメンバーアクセスを定義する責任がある

ここで、SW の a-d のループは非常に単純である。状態は数学的に記述され証明することが可能である。A-D の社会的ループは、大概が複雑な Web の信頼関係を非常にラフな近似的に書いており、しばしば単純な SW ほども頼りにならない。

セキュリティは、(A-D のような)社会的な機械へのアクセスの各段階で、(a-d のような) SW への接続を行おうとしている人を常に悩ませている。例えば、鍵 k1 で人 P1 をどうやって識別(identify)するかというときに、全く不必要な x.500　directory system を、これは信頼のループに本来入っていないものだが、使ってたりすると、セキュリティホールの原因になるので、不必要に“ 信用できる ”第三者を導入する必要がでてきてしまう。それはとにかく「同一性(Identity)」って一体何なのかという尽きない疑問にぶち当たる。Hugo だろうか Webmaster だろうか k3 に関連した何か（が与えるものなの）だろうか悩ましい。同一性の議論を終える前に、「信念」の議論もしておこう。Hugo が本当にその人がその会社のメンバーかどうか信じられるだろうかを考えてみたい - 多分 Hugo はそうする必要はないけれど Webmaster の役割がそうさせるだろう。ほら、穴があった。（人々はただ信じているわけではなく、程度に応じて信じていたり、特定の目的について特定の情報源を信頼したりする。）従って、現実世界と意味論(the Semantic)の間をマッピングするには、違う用語（“ 解釈 ”？）を用いるのがよさそうである。（私はもしかしたら哲学用語を正しく理解していなかったかもしれない）

それで、電子署名に基づくアクセスプロトコルを Web サーバにインストールした後、起こったことはそれに関連している。招待された専門家は、与えられたリストの鍵を持っているとした。セマンティックウェブは definitive machine となって動作し、我々は端(edge)で、メンバーシップと支払いなどとの関係を規則の形で持つだけである。招待された専門家は鍵が与えられたリストにある誰かと定義するようになる。

電子署名の仕様から我々が探していることは、書名とビットのストリングの間の関係で、セマンティック Web ツールボックスから探しているのは a-d の条件を記述する言語である。我々は a-d や A-D の関連の言語を提供したり解釈したりするものでも、A-D のステップを記述する法律上の言語を探しているわけでは決してない。

大変よく尋ねられる質問として、上記 a-d における電子署名の“ 意味 ”は何かというのがある。SW の視点からするとそれらの規則はシステムの意味である。マシンからすれば“ アクセスを与える ”ということを理解しなければならない端っこ(edge)を除き、全ては自己完結している、一方人間は要求やリストに署名を行う。セマンティックウェブの偉大なところは、これらがちゃんと動くってことであって、*“招待 ”ってどういう意味かとか、誰にされたのとか、*あるいは*これは招待が受け入れられたってことか？*といったものに答えられるようにすることでは決して無い。何を言っているかとそれをどこに格納するかを混乱しないよう気をつけなければならない。基本的にアクセスマシンを定義する４つの規則がある。我々はそれをどこにでも格納することができる。HTTP の要求に従い転送することもできるし、いくつもの異なる Web サイトに置くこともできるし、Java ring　や Smartcard に入れてもいいし、電子メールで送ってもいいし、なんなら大理石に彫ってもかまわない。SW のデザインは、それらの格納場所の制約を受けてはならない。

で、どこに、“ 署名の意味論 ”はあるの？

私にとって SW の意味論は a-d の全体のループであり、従って、任意の処理を許可するために結局、鍵が試されなければならないということである。鍵による署名の基本的事項の何かを議論し始めるときに、次のステップとしてあるのは鍵に関する知識だけだろう。セマンティックウェブでは、それは鍵で証明されたものに関する処理規則である。しかしながら、それは、鍵　として／とともに／に関して　格納した署名が意味論を持つということではない。実際、“ 署名の意味論 ”を語ることに意味があるとは思わない。

ドキュメントは意味を持つ。署名それ自体は意味論を持たない。

したがって、署名の意味論がなんであるかを尋ねるのは有益ではない。そうであっても、鍵に関する宣言の集合と文書があり、署名は信用を伝える。社会はさまざまな状況で、署名により信用を伝える規則が社会には多く存在する。セマンティックウェブの基本的基盤を構築するとき、我々はそれらのモデル化を試みるべきではない。

初版作成 1999/12/01
Tim BL

参考資料のメモ

[14:31] DanC は BAN logic のためにサーフィンをしに行って ietf – tls で以下を見つけた Oct 1996
http://lists.w3.org/Archives/Public/ietf-tls/msg02632.html
[14:33] < DanC> 次も参照：「 Authentication の論理」(所謂 BAN logic)
http://gatekeeper.dec.com/pub/DEC/SRC/research-reports/abstracts/src-rr-039.html