イベント開催の報告

PKI Day 2010 ＜社会基盤としてのPKI/PKIの10年＞

セコム株式会社 IS 研究所
PKI 相互運用技術 WG リーダ
松本　泰

日本ネットワークセキュリティ協会PKI相互運用技術WGが主催する「PKI Day 2010」が6月29日（火）に、南青山の東京ウィメンズプラザホールにおいて184名の参加者のもと開催されました。今回の「PKI day 2010」のテーマは「社会基盤としてのPKI／PKIの10年」としました。これは、社会基盤としてのPKI、例えば政府認証基盤（GPKI）や電子署名法等の制度の検討や構築が始まって10年が経過しましたが、この10年を振り返った上で、次のやるべきことを見極めるがテーマになります。

今回の「PKI Day 2010」は、以下の主旨で開催しています。

> インターネットが急激に普及し社会基盤となったと言われ久しいものがあります。その中で、ネット社会における信頼（TRUST）の仕組み、すなわち信頼のおけるリモート認証や、電子署名、これらがネット社会の基盤として必要だと思われてきました。しかし、現実には、「ネット社会における信頼（TRUST）の仕組み」が定着し、社会基盤化していると感じている人は少ないでしょう。「PKI day 2010」では、過去からの現在までの取り組みや社会の変化も議論した上で、「ネット社会における信頼（TRUST）」を担うべき社会基盤としてのPKIの方向性を議論します。

今回は、午後半日４時間以上のパネルディスカションという暴挙？に出ました。これまでのPKI dayでも何度かパネルディスカションを行って来ましたが、そのたびに時間切れで消化不良の多いディスカッションだったということがあります。

次に今回の「PKI day 2010」のプログラムを示します。

PKI day2010 のプログラム
「PKI day 2010」の各講演者と講演のタイトル

午前のセッション
◇「社会基盤としてのモバイル PKI の動向」 東京工科大学 教授　手塚 悟 氏
◇「電子署名の技術的問題点と電子署名法」 ひかり総合法律事務所　弁護士　宮内 宏 氏
◇「MS Crypto の 10 年」 マイクロソフト株式会社 コンサルティングサービス統括本部 Security Center of Excellence (SCOE)　渡辺 清 氏
◇「OpenSSL 1.0.0 のリリースについて」 富士ゼロックス株式会社　漆嶌 賢二 氏

午後のセッション
◇パネルディスカッション 「社会基盤としての　PKI/PKI の 10 年」
＜モデレータ＞ セコム株式会社 IS 研究所 PKI 相互運用技術 WG リーダ　松本 泰 氏 ＜パネリスト＞ 社団法人 日本ネットワークインフォメーションセンター (JPNIC) 技術部 / インターネット基盤企画部 セキュリティ事業担当　木村泰司 氏 富士ゼロックス株式会社　稲田 龍 氏 クロストラスト株式会社 代表取締役／日本電子認証協議会 代表理事　秋山卓司 氏 日本ベリサイン株式会社　主席研究員　佐藤直之 氏 株式会社イマーディオ　パートナー 満塩尚史 氏 東京工科大学 教授　手塚 悟 氏

○ 午前中のセッション

午前中は４人の講演者にお話して頂きました。一人目の東京工科大学の手塚先生には、今回の「社会基盤としてのPKI／PKIの10年」の基調講演とも言える内容を講演して頂きました。二人目の宮内弁護士には、2001年施行の電子署名法の問題点を再確認しようといった内容を講演して頂きました。宮内弁護士は2001年当時、大手ＩＴ企業の研究所において暗号技術等の研究に従事されており、電子署名法の施行にも関与されていましたが、その後、弁護士に転身されたという異色の経歴の持ち主です。

３人目、４人目は、PKI Dayでは何度か講演をお願いしている渡辺氏と漆嶌氏に、それぞれ技術的なトピックでお二人しか話せない内容を講演して頂きました。

○ 午後のセッション(パネルディスカッション)

午後は、６名のパネリストをお迎えして「社会基盤としてのPKI／PKIの10年」、具体的には、以下の様なお題目を設定してマラソンパネルディスカッションを行いました。

（1）「PKIの標準と相互運用性の課題」	（3）「電子署名法等の課題」
（2）「暗号アルゴリズムの移行問題」	（4）「番号制度とPKI」

社会基盤としてのPKI、例えば政府認証基盤（GPKI）や電子署名法等の制度の検討や構築が始まって10年が経過しましたが、現在の状況は、図１に示すように、技術と制度が噛み合っていないという現状認識があります。この状況を図２に示すような状況にするためにはどうすればよいかということがあります。この10年議論されてきたことは、技術として「How」の話が中心であり、技術と制度が噛み合うためには、何のための公開鍵証明書なのか（Why）、公開鍵証明書は何を証明するべきなのか（What）といった本質的なことがもっと議論されるべきといった内容のディスカッションが行われました。

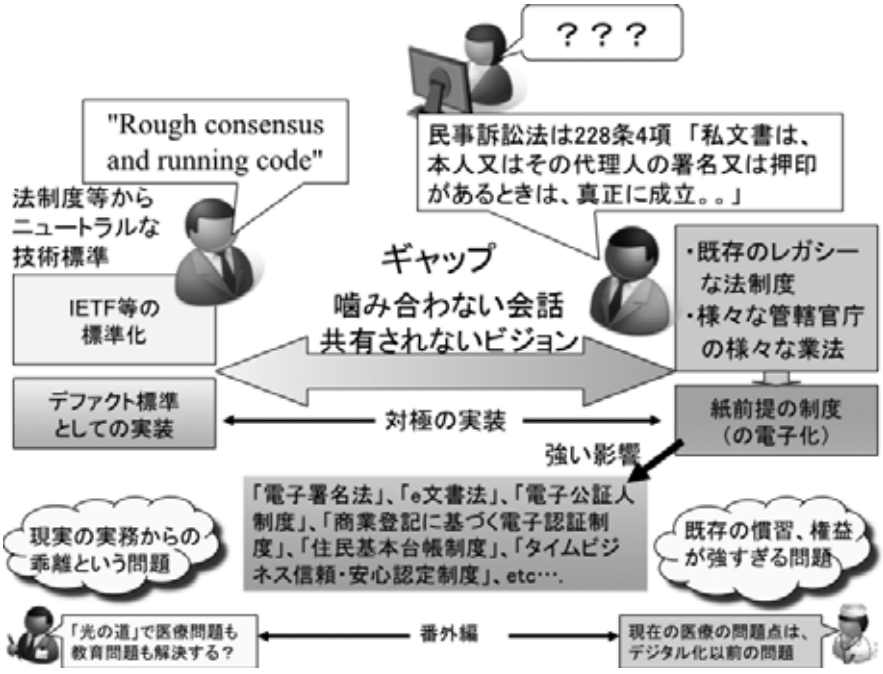

図１　技術標準と法制度の関係

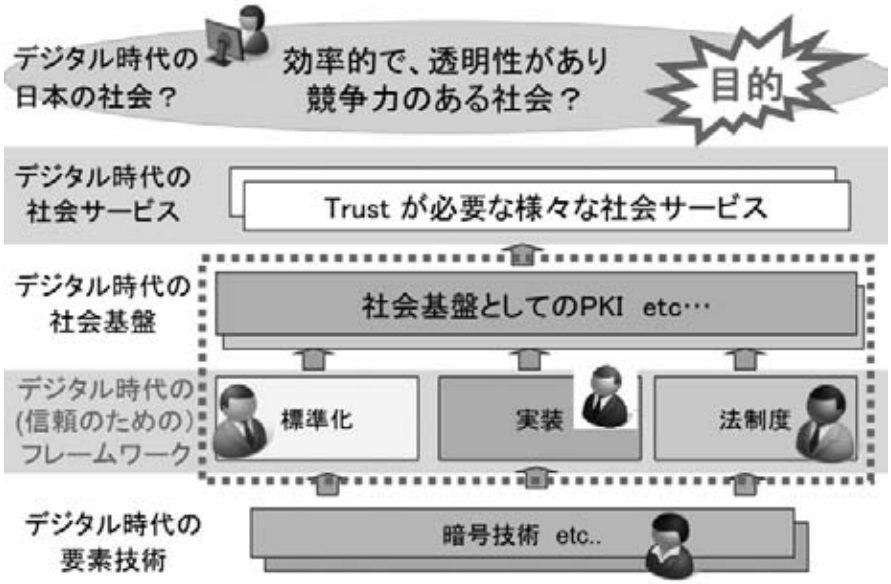

図２　今後のデジタル社会

○ おわりに

「PKI day 2010」の開催が6月29日で、同時期に、当時の国家戦略室から「社会保障・税に関わる番号制度に関する検討会　中間取りまとめ」が公表され、その後パブリックコメントの募集がありました。そして、この原稿を書いている最中の2010年11月11日に、このパブリックコメントの募集の結果が公表されています。パブリックコメントでは、番号制度等に対する様々な意見が提出されています。これらは、本質的には「社会基盤としてのPKI／PKIの10年」以前に検討されるべき内容だったとも言えます。なぜなら「番号制度等に対する様々な意見」にある番号等の識別子は、社会基盤としてのPKIとして扱われる公開鍵証明書等において、プライバシーも配慮した上で何らかの関連性が証明されるべきだからです。つまり社会基盤としてのPKI以前に「社会基盤としてのアイデンティティ管理」があるべきということが言えます。「PKI day」では、今後とも最新の技術動向を紹介すると共に、こうした制度と技術の関係に関する本質的な課題を取り上げていきたいと考えています。

参　考

PKI day 2010
http://www.jnsa.org/seminar/pki-day/2010/index.html
JNSA／PKI相互運用技術ワーキンググループ
http://www.jnsa.org/result/pki/
「社会保障・税に関わる番号制度に関する実務検討会」 第１回
http://www.cas.go.jp/jp/seisaku/bangoseido/dai1/gijisidai.html