PKI Day 2007 - ＜PKIの過去、現在、未来＞

PKI相互運用技術WGリーダ
セコム株式会社IS研究所　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 2007 - ＜PKIの過去、現在、未来＞」が6月25日(月)に、南青山の東京ウィメンズプラザホールにおいて170名余りの参加者のもと開催されました。PKI Dayというタイトルでのセミナーの開催は今回で3回目ですが、それなりに定着してきた感があります。本稿では、PKI Dayの目標とするところをご紹介し、今回のPKI Day 2007の報告を行います。

PKI Day 2007

「PKI Day」について

「PKI Day」というタイトルでのセミナーの開催は、今回で3回目となります。第1回の「PKI Day」以前にも、半日のセミナーを何度か行ってきましたが、こうした一連のセミナーのひとつの目的は、PKI相互運用技術WGのIETFでの活動を始めとしたPKIの相互運用技術に関連した活動を広くご紹介するということがあります。更に、我々が意図するところの本質的な目標として、単に最新技術の紹介というだけではなく、相互技術などの課題の解決に向けた共通の認識の醸成を行っていきたいとうことがあります。

PKIは、基盤技術としての宿命みたいなとことがあります。社会の複雑さが基盤技術としてのPKIへの要求となり、これが、PKIの(相互運用)技術の複雑さになっているところがあります。PKIを真に社会の基盤技術するためには、この複雑なPKIの相互運用技術が広く理解される必要があります。エンドユーザがこれらを分かる必要はないのですが、やはりPKIに関連した技術者や政策担当者には、これらの課題についての正確な理解が求められます。こうした中、PKIの相互運用技術に関する課題の解決は、閉鎖的な活動で成しえるはずもなく、オープンな幅広い技術情報の共有や人脈つくりが欠かせません。

以上の目的、目標を踏まえこれまでのPKI Dayのプログラム等は、以下のようなことを念頭に企画してきました。

(1) 内容としては、特定の製品紹介などでなるべく控え、技術中心の内容とする
(2) 最小限のコストで質の高い技術セミナーとする
(3) 問題点や課題の共有を意識したプログラム構成を考慮する

コスト面などでは、紙での資料配布は一切行わず、事前公開とし、また講演者に関しては、なるべくボランティアでお願いできる方に依頼しています。こうした条件の中でバランスのよいプログラムを考慮するといった方針で企画してきました。講演者の半数程度は、PKI相互運用技術WGのメンバーが行っていますが、十分に質の高い情報を提供できていると考えています。これまでの3回のPKI Dayの開催日とタイトルを以下に示します。各URLからは、これまでのPKI Dayの講演のほぼ全てのプレゼン資料がダウンロードできます。これまでPKI Dayに参加されたことがない方にも一度ご参照して頂ければ幸いです。

第1回「PKI Day PKI技術最新事情」
2005年10月28日(金)
http://www.jnsa.org/seminar/2005/seminar_20051028.html

第2回「PKI Day – PKIの展開と最新技術動向」
2006年6月7日(水)
http://www.jnsa.org/seminar/2006/20060607.html

第3回「PKI Day 2007 - ＜PKIの過去、現在、未来＞」
2007年6月25日
http://www.jnsa.org/seminar/2007/070625/index.html

PKI Day 2007

今回の「PKI Day 2007」

今回の「PKI Day 2007 - PKIの過去、現在、未来」は、以下の主旨で開催しました。

IT技術、ネットワーク技術が深く社会に浸透し行くなか、IT社会、ネットワーク社会における信頼関係を確立するための基盤が求められています。PKIは、こうしたことに対応する技術ですが、広くIT社会の基盤となるためには、まだ、多くの課題があります。「広くIT社会の基盤」の課題の解決のたには、組織や業界を超えて、PKI技術や相互運用に関する共通の課題などを共有する必要があるのではないでしょうか。PKI Day 2007では、PKIの過去から現在までの状況、標準化などの最新状況などを踏まえた上で、共通課題の認識とその解決策、そして将来の方向性を議論します。

今回のPKI Day 2007では、より多くの技術情報を1日で提供するという観点から、前回までに比べ、ひとつの講演時間を短くして(30分から40分)、多くの方に講演をお願いしました。朝10:00から19:00近くまでビッシリのプログラムで、セミナーが終わった時には、おなか一杯といったところでした。一方、個々の講演時間が短いところから消化不良の面も多々あったかもしれません。今回のPKI Day 2007のプログラムを示します。

PKI 技術と私
講師：東京電機大学教授／ JNSA 会長　佐々木　良一 氏

「PKI Day 2007」の各講演者と講演のタイトル

PKI技術と私
講師:東京電機大学教授／ JNSA 会長
佐々木 良一 氏

我が国におけるPKIの不幸-ネットワーク社会における信頼関係の基盤上で
独立行政法人情報処理推進機構(IPA)セキュリティセンター
宮川 寧夫 氏

PKIドメインを確立するには
セコム株式会社 IS研究所
島岡 政基 氏

IPアドレスの使用権を示すリソース証明書の動向
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

Windows VISTAでのスマートカード
マイクロソフト株式会社 コンサルティング統轄本部
プリンシパルコンサルタント
香山 哲司 氏

長期署名フォーマットの標準化と日欧相互運用実験
ECOM長期署名フォーマット相互運用実証実験プロジェクトリーダー
エントラストジャパン株式会社
漆嶌 賢二氏

東京大学におけるキャンパスPKIの配備に向けて
東京大学情報基盤センター PKIプロジェクト 准教授
佐藤 周行氏

パネルディスカッション／ PKIの過去、現在、未来

パネリスト:
日本電気株式会社　小松 文子 氏
富士ゼロックス株式会社　稲田　龍 氏
セコム株式会社ＩＳ研究所　松本　泰 氏
東京大学　佐藤 周行 氏

司会
JNSA主席研究員／株式会社ディアイティ
安田　直 氏

イベント開催の報告

今回の「PKI Day 2007」では、今年の6月にJNSAの会長に就任された佐々木良一東京電機大学教授に基調講演をお願いしました。佐々木先生のご講演「PKI技術と私」では、古代文明における印鑑の歴史から始まって、公開鍵暗号の歴史、その中で公開鍵暗号が人類の最も重要な発明の一つだという説など非常に示唆に跳んだお話でした。改めて「なぜ電子署名が重要なのか」「今後の社会において電子署名が持つ本質的な役割」等を認識されられました。過去から現在をふりかえり、将来のあるべき姿を考えてみようという、今回の「PKIの過去、現在、未来」の主旨に相応しいご講演でした。

2番目の基調講演のIPAの宮川氏のご講演は、電子署名よりも認証(Authentication)の重要性を説いた内容でした。この宮川氏の基調講演だけではなく、午後のセッションのマイクロソフトの香山氏の「Windows VISTAでのスマートカード」や、東京大学の佐藤先生の「東京大学におけるキャンパスPKIの配備に向けて」においてもPKIによる保証レベルの高い認証(Authentication)の重要性が強調されていました。

標準化動向ということに関しては、セコムの島岡氏の「PKIドメインを確立するには」、JPNICの木村氏の「IPアドレスの使用権を示すリソース証明書の動向」、エントラストジャパンの漆嶌氏の「長期署名フォーマットの標準化と日欧相互運用実験」などのご講演があり、どれも質の高い内容でした。「IPアドレスの使用権を示すリソース証明書の動向」などは、今後のPKIの新しい利用の方向性を示しているように思いました。

パネルディスカッション／ PKI の過去、現在、未来

今回初めての試みとして、最後にパネルディスカッションを行いました。「 電子署名法の功罪」「PKIが利用されるべき領域」「複雑さの克服」の3つのお題目をパネルディスカッションのネタとして取り上げ議論しました。短い時間でこれらを深く議論できた訳ではありませんが、会場からの活発な質疑もあり、PKI Dayの目的とする「相互技術などの課題の解決に向けた共通認識の醸成」がなされつつあり、目標とする課題の解決に向けて少し前進したのかなと感じられました。

おわりに

JNSAが設立された2000年頃から、情報セキュリティに関連した様々な課題は、かなり整理されてきたように思います。こうしたことに関しては、JNSAも様々な貢献を行ってきました。一方、PKIに要求されている「IT社会、ネットワーク社会における信頼関係を確立するための基盤」は、ネットワークセキュリティなどの個別の課題よりも少し上位の概念である「信頼(Trust)」が重要なキーワードになるのかなと思います。この「信頼(Trust)」の確立、実現のために、JNSA、並びに、PKI相互運用技術WGが果たすべき役割はまだ多く、「PKI Day」も、まだしばらくは、続ける必要があると考えています。