

イベント開催の報告

PKI Day 2009

＜様々な分野に展開される PKI の最新動向＞

セコム株式会社 IS 研究所
PKI 相互運用技術 WG リーダー
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 2009 が6月24日（水）に、南青山の東京ウィメンズプラザホールにおいて158名の参加者のもと開催されました。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と考えています。今回のPKI Day 2009「様々な分野に展開されるPKIの最新動向」は、様々な分野における「信頼(Trust)」の確立への努力の紹介ということになります。



■ 「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5回目であり、また5年目でもあります。これまでの一連のセミナーの目的は、PKI相互運用技術WGのIETFでの活動を始めた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でした。また、回を重ねるごとに、PKIの展開への課題解決を意識するようになりました。以下に、これまでの5回のPKI Dayの開催日とタイトルを以下に示します。この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(月)

<http://www.jnsa.org/seminar/2007/070625/index.html>

第4回 「PKI Day 2008 - 〈PKIの標準から実装まで最新動向〉」 2008年7月3日(木)

<http://www.jnsa.org/seminar/2008/0703/index.html>

第5回 「PKI Day 2009 - 〈様々な分野に展開されるPKIの最新動向〉」 2009年6月24日(水)

<http://www.jnsa.org/seminar/2009/0624/index.html>

PKI Dayの目的ですが、過去においても、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きたいという狙いがありました。現在は、更に一步進め、展開への課題の共有が目標となっています。PKI技術は、法制度まで含めた社会システムとして取り込まれる傾向がありますが、それが故既存の法制度等との整合も求められることになり、これが大きな課題となっている面があります。PKIを理解する重要なキーワードに、信頼関係モデル(Trust model)、信頼点(Trust point)などがありますが、この「信頼」自体は、IT技術により実現できるというものではありません。PKIの場合、信頼関係をマシンリーダブルな標準化された証明書で表しコンピュータによる自動処理等を可能にしますが、この場合、社会において何が信頼できるかと言ったことは、既存の制度や慣習等に大きく左右される訳です。こうしたこともあり「様々な分野に展開」というのは、様々な分野における信頼関係を理解し、これを如何に技術と融合させることを考えるのかという意味を含んでいます。

■ 今回の「PKI Day 2009」

今回の「PKI Day 2009 - 〈様々な分野に展開されるPKIの最新動向〉」は、以下の主旨で開催しました。

PKIは、デジタル社会のインフラとなるべき技術です。PKI Day 2009では、インターネット、学術分野、医療分野、電子政府分野、企業内など、様々な分野においてデジタル社会のインフラとして展開されているPKIの最新動向をお届けします。

今回のPKI Day 2009のプログラムを示します。

「PKI Day 2009」の各講演者と講演のタイトル

◇「PKIの展開状況の概観」

セコム株式会社 IS研究所/PKI相互運用技術WGリーダー 松本 泰 氏

◇「PKIの標準化動向とリソースPKI」

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

◇「長期署名フォーマットの欧州実証実験ETSI Remote XAdES/CAAdES Plugtests について」

欧州通信規格協会(ETSI) スペシャリストタスクフォース(STF)351 メンバー
次世代電子商取引推進協議会(ECOM) 客員研究員
エントラストジャパン株式会社 漆寫 賢二 氏

イベント開催の報告

◇「大学のサーバ証明書自動発行を目指して」

国立情報学研究所 客員准教授 島岡 政基 氏

◇「日本におけるヘルスケアPKI(HPKI)の最新動向」

保健医療福祉情報システム工業会 セキュリティ委員会 委員長 茗原 秀幸 氏

◇「欧州の政府系PKIとID管理」

セコム株式会社 IS研究所/PKI相互運用技術WGリーダー 松本 泰 氏

◇「政府機関及び金融機関のSSLサーバ暗号設定に関する調査結果について」

NTT情報流通プラットフォーム研究所 神田 雅透 氏

◇「Windows 7とWindows 2008 R2で実現するPKI」

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

GMOグローバルサイン株式会社 グループ技術開発部部長 浅野 昌和 氏

司会 JNSA主席研究員/株式会社ディアイティ 安田 直 氏

今回は、最初に「PKI Day 2009」の概観を示すことも含め、私(松本)が、「PKIの展開状況の概観」という短い講演と行いました。その後、午前中は、標準化関係のトピックを二人の講演者にお話して頂きました。一つ目は、IETFにおける標準化動向と新しいPKIの適応領域であるリソース証明書に関して木村氏にお話して頂き、二つ目は、欧州と日本でのコラボレーションが進んでいる「長期署名フォーマット」の実証実験について漆島氏にお話して頂きました。双方とも、標準化に対する日本からの貢献が重要な分野だと認識を新たにしました。

午後は、「学術分野」「医療分野」「電子政府分野」「インターネットのSSL」「企業内」と「様々な分野に展開されるPKI」を意識した講演をお願いしました。

「学術分野」に関しては、島岡氏に国立情報学研究所が進めているUPKIの活動の中での動きとして「大学のサーバ証明書自動発行」への試み、「医療分野」に関しては、保健医療福祉情報システム工業会で活動されている茗原氏に、それぞれの分野で活動されているお二方に「展開」をお話して頂きました。電子政府に関しては、欧州における展開を私(松本)がID管理の視点も含めて説明しました。「インターネットのSSL」に関しては、展開というよりは、既に広く展開されているSSLの現状、それから暗号アルゴリズムの移行の問題ということも合わせて神田氏にお話して頂きました。これは、PKI Day 2008でのパネルディスカッション/「暗号アルゴリズム移行問題」の延長上の話でもあり、非常に興味深い内容でした。最後に渡辺氏と浅野氏に、企業内で幅広く利用されつつあるWindowsでのPKIについてお話し頂きました。



今回のPKI Day 2009では、ひとつの講演の時間を50分から60分と長めに設定しました。技術情報を詰め込むというよりは、消化不良にならないセミナーをイメージしてプログラムを構成しました。それでも、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だったかと思います。



■ おわりに

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、すなわち信頼におけるリモート認証、サービスの認証、電子署名等、これらは、ネット社会の基盤として必然だと思われてきました。しかし、現時点において、「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。安全で安心なネット社会の実現、そして効率的で透明性の高い社会の実現に向けて、様々な分野における「信頼(Trust)」の確立への努力が望まれます。PKI Dayでは、こうした取り組みを今後とも紹介していきたいと考えています。

イベント開催の報告

広げよう!! インターネット安全教室 第2回全国情報セキュリティ啓発シンポジウム in 宮崎

【日時】 2009年10月24日(土)13:40~17:00(開場 12:30)

【会場】 宮崎公立大学 交流センター 多目的ホール

【主催】 経済産業省、NPO日本ネットワークセキュリティ協会(JNSA)

【共催】 宮崎公立大学

【後援】 警察庁、宮崎県警察本部、宮崎県、宮崎市、宮崎県教育委員会、宮崎市教育委員会、
宮崎県ソフトウェアセンター、宮崎銀行、MCN宮崎ケーブルテレビ、宮崎日日新聞社、MRT宮崎放送

【協力】 (財)みやざき観光コンベンション協会



2009年10月24日(土)に宮崎公立大学交流センターにて「第2回全国情報セキュリティ啓発シンポジウム」を開催いたしました。あいにく小雨模様のお天気でしたが、この日のために宮崎に集まっていた全国の共催団体メンバーとJNSAのメンバー約30名に加え、宮崎県内の参加者と運営をお手伝いいただいた宮崎公立大学の学生さんなどを含め、合計約60名の方にご参加いただきました。

このシンポジウムは各地域で情報セキュリティ普及啓発活動に携わる方々を対象にしていますが、全国の「インターネット安全教室」共催団体の方々にも参加していただき、地域の現状を知り対応策を考えると共に、それを各地の普及啓発活動の参考にしよ

うという趣旨で始まり、2008年10月に福井で開催した第1回に引き続き開催されました。また、今回は各地の「インターネット安全教室」の様子のパネル展示やパソコンによるデモ展示も行いました。

第1部では「今、インターネット社会では何が問題なのか!」というテーマのもと、まず熊本県阿蘇郡南小国町立南小国中学校教頭の桑崎剛先生に「子供とインターネット・その現状と課題」というタイトルでお話いただきました。引き続き、「インターネットの光と影」というタイトルで、株式会社アークン代表取締役渡部章氏にご講演いただきました。今は日常生活に必要不可欠となったインターネットですが、

大変便利な反面、出会い系サイト・学校裏サイト・プロフなどの様々な問題点もあります。そのあたりをお二方に大変わかりやすくご説明をしていただきました。特に桑崎先生のお話では、フィンランドと日本の携帯電話普及率の比較なども取り上げられ、大変興味深いお話でした。最後に宮崎県警察本部サイバー犯罪対策室一元氏より県警の窓口のご紹介とサイバー犯罪の現状についてのご説明をしていただきました。

第2部は、「みんなで考えよう! 地域で・家庭で・企業でできること」と題して会場参加型のパネルディスカッションを行いました。第1部の冒頭で、パネルディスカッションのテーマとして取り上げて欲しい内容についてのアンケートを参加者から集め、そのテーマを参加者も含めて討論するという方法をとりました。

まずはパネラーの宮崎公立大学の金子先生に自己紹介を兼ねて小学校での出前講座などご自身のお話をしていただき、引き続き水居徹氏の自己紹介の後、本題のディスカッションに入りました。

桑崎先生から、親の知識不足が問題であるという意見が出され、それを受けて渡部氏からは知識不足だけでなくモラル不足もあるのではないかという意見がありました。特に桑崎先生が話された、携帯電話購入のきっかけが、日本の場合は「テストの点が良かったから」「進級したから」「誕生日だから」などが多く、「必要だから買い与える」という理由付けがなされていないという意見が印象的でした。何事にも危険はありますが、危険性を明確にしようとしな(危険性の宣伝はしない)という日本人の社会体質があり、「自分で自分の危機管理をする」という意識が低いのではないか、という意見もあり、黒田氏からは、経済産業省としては賢い消費者がメーカーを教育して欲しいという意見もありました。

また、教師の知識不足が問題であるという意見もあり、一般的な「先生」の知識レベルは現状どうなのか?という問いかけもありました。宮崎市では、



100%の教師が情報モラルの指導ができるようになるように、教師対象に情報モラル研修を行っているそうです。

後半は、法による規制についてのディスカッションとなりました。規制は最小限にすべきであり、危険を冒して行動するかどうかは自分たちで判断すべきである、という意見が出る一方で、日本のインターネット社会を免許制にすべきであり「インターネットだと何割安い」をPRするのなら、不正を行った際の罪は1.5倍重くするべきだ、というような過激な意見もありました。

今回のパネルディスカッションでは、最終的に明確な1つの「解決策」を呈示することはできませんでしたが、いろいろなお立場の方の多種多様な意見を聞くことができ、大変有意義なものだったと思います。現実社会では、小学生は歩ける範囲、中学生は自転車移動できる範囲、高校生はもう少し広く、と自然と行動範囲が決まっているように、インターネット社会もそのように分けできればよい、という意見がとても印象的でした。そのようなことが必要であるし大切なことだと感じました。