PKI Day 2011 <番号制度時代のPKI> 開催報告

セコム株式会社 IS 研究所
水戸　和

去る 9 月 26 日（月）、赤坂の山王健保会館にて PKI 相互運用技術 WG 主催 PKI Day 2011 が開催されました。今年で 7 回目を迎える PKI Day ですが、今回は副題を“番号制度時代の PKI”として、現在法制化の議論が行われている「社会保障・税に関わる番号制度」を本格的なデジタル社会への移行のための社会基盤の整備と捉え、そのようなデジタル社会における PKI の方向性を議論しようという趣旨で開催されました。これまでの PKI Day を振り返ってみると、第 1 回目の副題が“PKI 最新動向”となっていたものが、今回は“番号制度時代の PKI”となっているように、PKI Day で扱う題材が技術としての PKI から、社会的な問題に対するソリューションとしての PKI へと変化を迎えているようにも見受けられます。このことを裏付けるかのように、午後のパネルディスカッションでは経済産業省 CIO 補佐官の満塩尚史氏や弁護士の宮内宏氏といった、幅広い肩書きの方が参加され、熱い議論を繰り広げられました。

■講　演

最初の発表は“セキュリティ＆プライバシーの課題とマイクロソフト U-Prove”と題してマイクロソフトの渡辺清氏から、オンラインサービスの普及に伴い生じているセキュリティ・プライバシ・スケーラビリティの 3 要件を満たす新しい認証技術として Microsoft 社の推進する U-Prove 技術の紹介が行われました。この U-Prove を認証に用いることにより、ユーザーは問い合わせに対し必要とする情報のみ開示することが可能であり、Privacy by Design を実現した技術となっているとのことでした。

二人目は“楕円曲線暗号における PKI”と題し、筑波大学助教の金岡晃氏より RSA と並ぶ公開鍵暗号アルゴリズムとして知られる楕円曲線暗号（以下、ECC）の普及の背景、暗号強度を決定する複数のパラメータの紹介から OpenSSL に実装された ECC のパフォーマンスの評価まで、ECC 全般に亘る発表が行われました。

質疑では、ECC 関連の多くの特許を抑えている Certicom 社について言及され、金岡氏からは”実装にあたって特許問題で苦労している人も多いはずで、そろそろ（ECC 関連の特許マップなどを）まとめる動きがあってもいいはず”との発言がありました。また、金岡氏から会場への逆質問への回答として電子パスポートでの ECC 使用実態の解説がなされるといった一幕もありました。

小休憩を挟み、三人目の発表は PKI Day 初参加の NTT 情報流通プラットフォーム研究所の武藤健一郎氏から“SSL における暗号危殆化サンプル調査の報告”と題し、実際に稼動している SSL サーバーの証明書の署名アルゴリズム、サーバーの対応する SSL コネクション、そしてクライアント（OS・Web ブラウザ）における暗号・ハッシュアルゴリズムの対応状況といったものの調査報告が行われました。

サーバー証明書の調査では、危殆化が懸念されている RSA1024 と MD5 の組み合わせを用いるサーバーは昨年度の調査でほぼ無くなるなど、順調に移行が進んでいるようにも見受けられましたが、一方でサーバーが受け入れ対応している暗号・ハッシュアルゴリズムでは古いデバイスへの接続対応のため未だに RC4-MD5 の接続に対応しているサーバーが大部分を占めているという事実も示されました。また、クライアント側で使用する OS、ブラウザの違いによっても、SSL 接続において用いられる暗号・ハッシュアルゴリズムに違いが出るため、サーバー側、クライアント側双方で危殆化の対策が必要であるとの見解を示されました。質疑では、

サーバー側でRC4-MD5を利用した接続を許可しない設定にすることの可能性について言及され、業務系や組み込み系といったデバイスへの対応が問題となるとの見解が示されました。また、会場からのコメントとして、“ベンダーとしてはクライアントにベネフィットを示すことが出来ないと移行を促しにくい、各ベンダーのコツコツとした努力が不可欠である”との見解が示されていました。

昼休み前最後の発表は、産業技術総合研究所（AIST）の山口利恵氏から“日本におけるRSA1024・SHA-1の移行に関する施策”と題し、先の武藤氏の発表にもあったRSA1024・SHA-1の危殆化に合わせて行われる公的個人認証サービス（JPKI）、政府認証基盤（GPKI）、地方公共団体組織認証基盤（LGPKI）といった国や自治体の運用しているPKIでの暗号移行について説明が行われました。2014年度に移行開始を予定しているこれらのシステムですが、国や自治体のような複数の運営者の問題や、e-Taxのようなアプリケーションやハードウェア（ICカードや利用端末）の移行問題といった複合的な問題を抱えているという事実が紹介されていました。

午後の部の講演では日本情報経済社会推進協会（JIPDEC）の木村道弘氏から“最近の欧州PKI事情”と題し、欧州におけるPKI標準化体制の歴史的推移から欧州各国の電子署名法の要件になっているAdES（Advanced Electronic Signature）を例にとり実際に標準化された技術の紹介、そして直近の欧州PKI標準化組織の動向の紹介がなされました。

欧州におけるPKI標準化体制については、欧州標準化委員会（CEN）が要求仕様を作成、欧州電気通信標準化機構（ETSI）が対応する技術仕様を策定という形を目指していたが、十分に機能していなかったため、EC指令によって規格そのものも含めた再編成が取り組まれているとのことでした。質疑では欧州でのタイムリーな話題としてDigiNotarにおける適合性評価の問題について扱われ、ETSIによる基準はあくまで最低限の認定（クオリファイ）であり、実際は運用によってレベルに大きな差が生まれてしまっているという問題点が指摘されていました。

■ パネルディスカッション

パネルディスカッションでは「社会保障と税に関わる番号制度」における法人番号の扱いを主な題材に、JNSA PKI相互運用技術WGのリーダーで、内閣官房で番号制度検討を行う情報連携基盤技術WG、社会保障分野SWGの委員も勤めるセコムの松本泰氏をモデレーターとして、同様に情報保護評価SWG委員を勤める宮内宏法律事務所の宮内宏氏、情報連携基盤技術WGの委員である東京工科大学教授の手塚悟氏、経済産業省CIO補佐官の満塩尚史氏、そして日本ベリサインの佐藤直之氏の5名という番号制度を語るにはこれ以上ないメンバーによるディスカッションが繰り広げられました。

まず、松本氏からこれまで技術的な問題にフォーカスしていたPKIにおける議論は今後、証明書が「何を証明するのか」といった制度的な側面についても行っていく必要があるという提言が行われ、そのケーススタディとしての番号制度に関する検討状況の解説と、付番・本人確認・情報連携という番号制度の実現する3つの機能についての説明がありました。その中でPKIの証明書は、従来からの人が紙の書類を読むことを前提とした本人確認ではない、曖昧性のないデジタル技術を前提とした番号制度の様な制度、すなわち「デジタル時代の社会基盤としてのアイデンティティ管理」に基づいて発行されるべきものであると指摘し、これが実現することにより番号制度がデジタル社会の社会サービスプラットフォームとして機能するとの見解が示されました。一方で、現在の番号制度に関する検討では法人番号に関する検討が不十分であり、法人の意思がどのように確認されるかが不明

瞭であるとの指摘がなされました。

これを受け、手塚氏からは現在の番号制度の中で行われている法人番号について、「個人」のライフサイクルと「法人」のライフサイクルの違いに言及し、個人に対して行われるのと同様のフレームワークを適応するのは困難であると指摘し、同時にこれら境界にある個人事業主の存在に関しても検討が必要との見解が示されました。

続いて満塩氏からは、ユーザーとしての観点から番号制度の目的・効果に注目して番号制度について論じる必要性が指摘されました。その一例に氏の私見として、番号制度による法人認証が導入されることにより、申請者の存在確認・申請事実の確認・申請内容の確認のうち前者2点の仕事を自動化できるというワークフロー削減の可能性を示しました。一方で、申請内容の確認のような人手によって実現するほうが効率的な仕事も依然として存在するため、番号制度により実現される機能と人手による仕事のバランスをとることが大事との見解が示されました。

宮内氏は、法務上の観点から、現状の法人の電子認証制度やその証明書の内容の紹介に続いて、法人の意思表示がどのように行われているかという点に関して「代理方式」と「機関方式」の2つの方式を紹介し、代理方式の必要性が求められる認証（Authentication）と異なり、電子署名においては機関方式と同様の運用が望ましいと示す一方で、従来の法人印と同様に法人の中の個人に電子署名に用いる私有鍵やパスワードを預けることがあってよいのか？という問題点を指摘していました。

最後に、佐藤氏からはPKIと電子署名法について、現状の電子署名法において企業の電子認証行為は管轄外となっており、署名実施者個人から見ても電子署名法における認証認定業務では企業との所属関係などは取り扱われないため、企業としての機関による意思表示や、企業人としての個人による代理での意思表示が出来ておらず、商業登記に基づく電子認証制度用いた企業の代表者による個人の認証しか行えていない事実が指摘され、番号制度の制定にあわせ電子署名法の改正も含めた検討が必要との見解が示されていました。

そして、自由討論ではこれらの発表を題材にして法人格による電子署名の法令化可能性と、その署名管理を民間事業者が行う可能性を題材に、議論が行われました。満塩氏からは法人番号を含んだ証明書の可能性について、証明書にとって「修正」という概念が存在しないことを指摘し、代表者名のような比較的高い頻度で変更される情報を入れるのは不適当であるとの指摘がされていました。

最後の質疑では会場から「こういった制度があると何が出来るか、と言った議論だけではなく、Trustと言う視点に立って、何を”信じて”こういった制度が機能するのか、といった点について考えることも必要」と言う指摘がなされました。松本氏からも、Trustが崩壊してしまったオランダのDigiNotarの事例から様々学ぶことも多いのではないかと言う返答がなされるなどの意見交換がなされていました。

今年のPKI Dayは、プライバシー問題等に対応するU-Prove、組み込み機器に対する楕円暗号、そして、パネルディスカッションでのTrustという観点など、技術としてのPKIから、社会的な問題に対するソリューションとしてのPKIと言う方向性が強く出ていたように思われました。タイトルにある「番号制度」の導入はそういったソリューションとしてのPKI時代の嚆矢として大いに期待したいと思うと同時に、PKIの可能性を示すマイルストーンとして十分な検討がなされてほしいと感じました。

参考URL：http://www.jnsa.org/seminar/pki-day/2011/index.html
http://www.jnsa.org/result/pki/index.html

西日本支部主催　セキュリティセミナー「NSF 2011 in Kansai」

株式会社インターネットイニシアティブ
関西支社技術部　齋藤　聖悟

JNSA西日本支部では地域のセキュリティレベルの向上を目的としてNSF 2011 in Kansaiを下記の要領で開催しました。

日　時: 2011年10月5日(水)9時50分～17時20分
会　場: 大阪国際会議場グランキューブ大阪
主　催: NPO 日本ネットワークセキュリティ協会 西日本支部
定　員: 150名
概　要: 中小企業における情報セキュリティの現場にあったクラウド、スマートフォンの運用のポイントについて
料　金: 無料

2011年に入ってクラウドやスマートフォンの企業への導入が本格化する中、中小企業の情報セキュリティ対策の現状に、これらの最新トレンドをどのように組み込んで行けばよいかを探ることを目的に開催しました。

開催挨拶

西日本支部の井上支部長がJNSAおよび西日本支部の発足以降の歩みと現状、これからのJNSAについて紹介を行ないました。

基調講演

奈良先端科学技術大学院大学 山口英教授からは「クラウドやスマホとの付き合い方」と言う題名で、これまでのコンピュータシステムと何が違い、何がメリットなのかを解説戴きました。

仮想化・集中の技術をベースとするクラウドについては運用のプロフエッショナルの知見を活用した利用を推奨するという立場で、保有から利用、独占から共有へのメリットによりTCO削減以上のメリットはあるが、パブリッククラウドについてはベンダーロックインや適正なトラブル対応がされるかなどサービス事業者の選定には注意が必要との指摘がありました。

スマートフォンについてはBOYD対策の視点から、どのような業務で使用するのか？ビジネスプロセスを明らかすることが大切であり、クラウドに比べるとStepByStepでのアプローチが大切と言う解説でした。

日本ではこれから本格的な導入活用が始まるが、諸外国では相当に活用が進んでおり、見習うべきところが沢山あると言うメッセージには多くの参加者が考えさせられたのではと思います。

中小企業セキュリティ

西日本支部からは富士通関西中部ネットテック株式会社 嶋倉文裕氏が「中小企業セキュリティ」と題し、現状の中小企業セキュリティ対策としてJNSA 西日本支部が作成した「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」の活用方法について解説頂きました。また中小企業でクラウドやスマートフォンなど新たな技術や新デバイスへの対応のための考慮すべき点について問題提起をして頂き、その後のクラウドセッションとスマートフォンセッションへの導入付けになったと思います。

クラウドセキュリティ

クラウドセキュリティのセッションでは二人の方に講演頂きました。

株式会社インターネットイニシアティブ 加藤雅彦氏は3月11日東北地方太平洋沖地震直後に実際に行ったクラウドでの震災支援について実際のtwitterでのやり取りを交えながら発表されました。またその体験から中小企業がクラウドを利用する場合には緊急時と平常時のセキュリティを分けて考えたほうがいいのでは、という提起がなされました。

株式会社ディアイティ 河野省二氏からは経済産業省が発行したクラウドセキュリティの活用について紹介頂きました。

クラウドコンピューティングに対する漠然とした不安を整理解説しそれらを「見える化」するためにクラウドサービス利用のための情報セキュリティマネジメントガイドラインの活用方法を解説頂きました。

後半では「最近気になるクラウドに関する思い込みセキュリティってありますか？」「セキュリティの強度と可用性のバランス」をテーマに加藤氏と河野氏の思いを語って頂きました。

スマートフォンセキュリティ

スマートフォンセキュリティのセッションでは株式会社カスペルスキー 前田典彦氏からスマートフォンのマルウェア検知状況について解説頂きました。

特に2011年に入って急激にその利用が増加しているスマートフォンのセキュリティ対策の必要性を強調されていました。

引き続きラックホールディングス株式会社 山城重成氏からスマートフォンのプラットフォームによるマルウェアの違いやウィルスの基本構造を解説頂き、遠隔操作でカメラを使用した盗撮や盗聴でAndroid端末がマルウェアに感染する様子のデモを交えながら、最後にキャリアによる対策・個人による対策についてまとめて頂きました。

パネルディスカッション

パネラーとして嶋倉氏、河野氏、前田氏、「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」の取りまとめを担当したアイネット・システムズ株式会社 元持哲郎氏に加わって頂き、最新の事例を元に複数の視点から中小企業におけるクラウドやスマートフォン導入時・運用時の問題点や対策のポイントについてディスカッションを行って頂きました。

その結果、クラウド・スマートフォンについては導入が本格化、特にクラウドについては活用事例やセキュリティガイドラインなどが整備されつつあり、中小企業での導入も積極的に行い得る状況にあるとの共通認識に至りました。しかし、スマートフォンについては利用者視点を踏まえたセキュリティ対策がまだまだ途上にあり、慎重な対応が必要との意見が大勢を占め、基調講演の山口教授の「スマートフォンの活用にはビジネスプロセスの構築と業務の改善が必須」と言う指摘に呼応した形で、スマートフォン単体のセキュリティだけではなく、業務プロセス全体を考えてのセキュリティ対策が必要との警鐘でまとまりました。

NSF 2011 in Kansaiを終えて

3年ぶりとなる大阪でのセミナー開催で、色々と不安要素がありましたが、関心の高い内容だったためか多数の申し込みを頂き、事前受付は満席となり、当日は129名の参加者を集め、盛況なセミナーとなりました。アンケート結果も“大変有益であったが44%”、“有益であったが55%”と好評で成功したと思います。

アンケート一部抜粋

- 基調講演、クラウド、スマホの内容が良く理解できた。
- 最新の動向や、本質的な課題は何なのか、といった点で、非常に勉強になりました
- スマートフォンセキュリティについては、マルウェアのトレンドが具体的に紹介されており、有意義でした。デモもよかったです。
- クラウドセキュリティ等のパネルディスカッションで有益な情報も聞けてよかった。

ただ、予想よりも多くの方に申し込みいただいたため、参加できなかった方がいらっしゃったのも事実で、またアンケートの中では関西でのセキュリティに関連したイベントが少ないという指摘もありました。

- 関西でのセミナーが少ないので増やしてほしい
- 西日本支部での勉強会やセミナーの回数を増やしてほしい

今回のセミナーでは企業ブースコーナーを併設すると共に出社してから退社するまでソリューションマップを配布するなど積極的な取組みを行いましたが、これからも関西圏のセキュリティレベル向上のためJNSA 西日本支部としてセミナー・勉強会を継続していきますのでご期待ください。

「2011 日韓情報セキュリティシンポジウム」の報告

【日　程】　2011年11月10日(木)13：00～18：45

【場　所】　五反田ゆうぽうと

【主　催】　特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)
特定非営利活動法人日本セキュリティ監査協会(JASA)
韓国知識情報保安産業協会(KISIA)

【後　援】　総務省、経済産業省、情報セキュリティ政策会議、独立行政法人情報処理推進機構(IPA)、
JPCERTコーディネーションセンター、Telecom-ISAC Japan

【参加人数】　合計148名
＜内訳＞韓国側：36名、日本側：112名(一般参加者：91名　関係者16名　事務局5名)

「2011日韓情報セキュリティシンポジウム」は、2011年11月10日(木)、五反田ゆうぽうとにて開催いたしました。当シンポジウムは、日韓の情報セキュリティの向上を目指す企業と人の交流を図り、グローバルな体制が必要とされる情報セキュリティに関して両国に共通の課題を議論し、共通の理解を得る目的で、日本ネットワークセキュリティ協会(JNSA)、日本セキュリティ監査協会(JASA)、韓国の知識情報セキュリティ協会(KISIA)が協力して開催したものです。

今回は、本年1月に韓国ソウルで開催した「第1回日韓情報セキュリティシンポジウム」を受けて第2回目として日本で開催いたしました。

プログラムは、JASA土居会長、JNSA田中会長、KISIA李会長の挨拶に始まり、「大規模インシデントの予防と対応」というテーマでJNSA副会長中尾康二氏とアンラボ張氏の講演、「スマートフォンと情報セキュリティ」というテーマで株式会社ラック西本逸郎氏とFasoo.com李氏の講演、「クラウドコンピューティングと情報セキュリティ」というテーマで伊藤忠テクノソリューションズ株式会社佐藤元彦氏とSECUI.COM南氏の講演、そして、IPAとKISA(韓国インターネット振興院)による取り組み紹介のあと、最後に「情報セキュリティ産業のアジア展開と日韓連携」というテーマでモデレータに日本側は中尾氏、韓国側は韓国情報保護学会長Dr. Youmを迎え、パネルディスカッションを行いました。当日は総勢148名(内韓国側36名)の参加者を集め、パネルディスカッションでは日韓の連携の具体化についても討議されました。また、別室で韓国企業による展示会も開催され、こちらも多くの方々にご参加いただきました。次回は2012年11月に韓国ソウルで第3回シンポジウムを開催予定です。