PKI Day － PKI技術最新事情

セコム株式会社　金岡　晃

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－PKI技術最新事情」が10月28日(金)にセコムホールにおいて開催されました。会場は満員の盛況で、100名以上の方がセミナに参加されました。今回はPKIにおける「技術最新事情」をテーマとして、標準化の動向やPKIの利用法、運用における検討点などの広範にわたる講演があり、多数の参加者がPKIの理解を深めることができたセミナとなりました。

基調講演ではIPAセキュリティセンターの宮川氏が「経営幹部にPKIを理解してもらうためには…」と題して、技術者が非技術者、とりわけ経営幹部にPKIを理解してもらうことの困難さと、その解決法を示しました。最初に「PKIは正直難しい」としながらも、実は技術が難しいのではなく、利用技術が複合的であり、さらに利用目的も複数であることが難しさとなっていると指摘。そもそも複数の目的も許容する社会基盤であるPKIを単一の目的に絞って話そうとすると理解を妨げさせる原因になることから「まず『複雑』で『複合的』であることから話すべき」と示されました。PKIを説明する場合、公開鍵暗号技術の説明から始めることが多く見られますが、それではPKIの全体像までたどりつかなくなってしまいます。公開鍵暗号技術はPKIの要素技術でしかないことを考慮すべきで、その上でお勧めする説明方法として『信頼関係(trust)モデル』から説明し、デジタル証明書に関しても技術仕様の用語よりも、関係者が何をしなければならないかを示す証明書ポリシ(CP)を説明するという方法を示されました。信頼関係モデルの説明は、いわばPKIをトップダウンで説明するものであり、それは社会的なモデルを説明することでもあるから、公開鍵暗号技術の説明から始めるボトムアップの説明よりも、こちらの方が経営幹部に説明するには望ましいと述べられ、また専門用語を正しく使うことや無理のある比喩表現を避けることも重要であることを強調されました。

続いてのセッションでは、富士ゼロックスの稲田氏が「PKI標準化最新動向」と題してPKI関連標準の最新動向を紹介されました。まず稲田氏はSSL/TLSに焦点を当て「Amazon、楽天などのサービスを使ったことがある人」とセミナ参加者に投げかけました。ほぼ全員の人が挙手した結果を見て、稲田氏は「PKIはもはやすぐ隣に存在する技術」とした上で、インターネットは車や火と同じく利用法によっては非常に危険なものであり、その中でPKIが提供する機能が注目されている、と述

べられました。PKIの標準化について証明書自身のプロファイルはほぼ完成しているということを紹介されるとともに、証明書の検証やその応用系については標準化が現在も進んでいるという現状を紹介されました。また、証明書の検証については検証をクライアント側でやるのには相当な労力が必要であると指摘し、その回避策としてサーバサイドで検証プロセスを代行するためのプロトコル、SCVPやOCSPについて図解されました。最後に証明書の応用系の標準化として長期署名とタイムスタンプについて触れ、その最新動向を解説していただきました。

午後に入り、実際にPKIが利用されていくなかで現れてきた問題点や、運用上での注意点などに関して、PKIがどう使われているか、どう使われていこうとしているか、というセッションが続きました。

まず、「マルチドメインPKIと相互運用性のBCP(Best Current Practice)」がセコムの島岡氏より発表されました。あるポリシ下で運用されているPKIの単位「PKIドメイン」に対し、複数のPKIドメインをまたぎ、信頼関係を築く「マルチドメインPKI」がこれからのPKIが進んでいく方向であろうとした上で、自身がPKIの相互運用で苦慮された経験を、同じく米国で政府系のマルチドメインPKIのノウハウを持つNISTの方との共著で文書化しIETFへと標準化を提案していることを紹介されました。またこういった相互運用性のBCP策定にあたってのコンセンサス作りとして、海外での活動なども紹介されました。

続いてのセッションではNECの奥野氏による「グリッドコンピュータとPKI」の発表が行なわれました。グリッドコンピューティングで多く利用されているGlobus Tool Kit（GTK）や、グリッドコンピューティングの全機能をWebサービス技術によりサービス化するOGSA（Open Grid Services Architecture）を中心に解説を行い、その中でPKIが利用されている場面を説明されました。OGSAのセキュリティアーキテクチャの中では、複数の組織が資源を共有するために構築するVO（Virtual Organization）を紹介、ここでも組織間のポリシなどの相互運用性がポイントになっていることが伺えました。最後に、奥野氏が認証局ソフトの開発などで参加しているNAREGI（超高速コンピュータ網形成プロジェクト）の説明があり、認証局ソフトNAREGI-CAの構成図や運用概要が紹介されました。

日本ネットワークインフォメーションセンター(JPNIC)の木村氏からは「JPNIC認証局～IPアドレス認証局(認証)～」と題して、JPNIC CAの紹介、またご自身の経験などから得られたいくつかのポイントについて講演がありました。電子証明書を簡単に利用してもらう点として「本人性確認」と「手続きの複雑さ」を挙げ、それらの解決手段の1つとして商用サービスなどで多く適用されているRA（登録機関）を外部に持つモデルを示し、同モデルを提供しているJPNICの認証局が紹介されました。また、ご自身の経験からのCA構築時の検討ポイントや、整備されていると便利である事項などを示し、「こういったBCPを皆で持ち寄ることが大事」とセッションを締められました。

休憩を挟んだ午後の後半では2つのセッションがありました。1つ目はマイクロソフトの渡辺・鈴木両氏による「WS-FederationとPKI」。Federation（連携）は、PKIなどの認証基盤が整備されたあとに出てくる注目度の高い話であり、司会をされたJNSA安田氏や2つ目のセッションで講演されたセコム松本氏は「次回はFederationをキーワードにしてセミナを開催したい」という意向を持っており、今回の渡辺・鈴木両氏の発表は

イベント開催の報告

それに先駆けてのものとなりました。

発表ではまず渡辺氏が、現状持っている認証の基盤を利用して他の組織との柔軟なシステム間接続を可能にするFederationが今後重要になってくると強調。PKIとWS-Federationの連携方法の違いの解説などがされました。続いて鈴木氏が、マイクロソフトの取り組み詳細を紹介。WS-FederationやADFS（Active Directory Federation Service）の説明を頂きました。利用シナリオをいくつか紹介後、事例として、イラク戦争などにおける同盟国間のインターオペラビリティ実証実験「CWID2005」の紹介もあわせて行なわれました。

最後のセッションは本セミナを主催したPKI相互運用技術WGリーダであるセコムIS研究所の松本氏より「Challenge PKIプロジェクトとPKI技術最新事情」と題して、JNSAのChallengePKIプロジェクトの紹介と、最近のPKI関連トピックや今後の課題についての解説がありました。PKIの業界において、アイディアから仕様、仕様から標準、実装から標準という一連の標準化の流れにそれぞれプレーヤーがいる一方で、実際に標準・実装から展開し相互運用を行なう部分を担うプレーヤーがいないことを指摘しました。さらに、標準と呼ばれる文書は山のようにあるが、相互運用が可能なものはわずかであることも問題とし、解決していくにはベストプラクティスが重要である、と述べられました。これらを目標とし2001年よりスタートしたChallenge PKIプロジェクトの活動報告をされ、現在までの活動内容を振り返られました。成果はIPAの報告書や、Web上でのテストケースの公開、得られた知見のIETFへのフィードバックなどが挙げられます。PKIの最新事情としては、危殆化が指摘されたSHA-1からいかにしてSHA2ファミリーに移行していくかというSHA-1問題について、また近年IT化の動きが活発になってきた医療福祉分野へのPKI整備の動向という内容で医療PKIについて、さらに来年度に現状の問題点から改正がさけばれる電子署名法の改正についても解説されました。そして最後のまとめとして「PKIの本質的な問題とは相互運用性に集約されるが、同時に、ますます社会基盤として重要性も深まっていくだろう」と述べられて講演を終えられました。

PKIは情報社会における「信頼の拠りどころ」を提供するものであり、それ自身が社会基盤にもなれば、別の基盤における信頼性を保つ機構として利用される非常に重要な技術でもあります。PKIはすでにさまざまな分野で利用されており、今後の社会で浸透していくほどにその相互運用性の重要性が高まると言えます。またPKIはその複雑さや困難さが指摘される場面が多くありますが、本セミナの発表者はPKIの導入・利用においてさまざまな困難を経験されてきた方々であり、それらの方々からの発表による有用な事例や導入・利用における指針などが広く示された今回のセミナとなりました。

※当日のプレゼンテーション資料はJNSAのホームページより参照可能です。
http://www.jnsa.org/seminar/2005/seminar_20051028.html

IPA 宮川寧夫氏