

PKI Day 2008 レポート

富士ゼロックス株式会社 横田 智文

JNSA PKI相互運用技術WG主催セミナー
【PKI-Day 2008ー

<PKIの標準から実装まで最新動向>】

■日時：2008年7月3日(木)10時～18時半

■場所：東京ウィメンズプラザホール

■主催：JNSA PKI相互運用技術WG

PKI Day 2008は、京都大学の岡部氏の基調講演「全国大学電子認証基盤 (UPKI) とその先にあるもの」から始まりました。氏の講演では、国立7大学と国立情報学研究所等が共同で構築しているUPKIの現状として、UPKIが用途に応じた3つのPKI (PKI オープンドメインPKI、キャンパスPKI、グリッドPKI) から構成されていることやそれぞれのPKIの役割、UPKIを使ったシングルサインオン等の実証実験、キャンパスPKI間の相互運用性確保、CP/CPSのテンプレート化などを含むキャンパスPKI導入促進のためのUPKI共通仕様などが紹介されました。また講演の最後では、UPKIの先にあるものとして、もっと誰でも簡単にPKIを利用できるようにしていきたいという方向性が示されました。

続いての講演は、富士ゼロックスの稲田氏の「標準化の一側面 - IETFにおけるPKIの状況」でした。講演では、IETFのPKIX-WGで議論されている主要な話題と現状が紹介され、PKIX-WGの活動報告として、RFC 3280の後継であるRFC 5280が公開されたことや暗号アルゴリズムの移行 (世代交代) について議論がされていることが紹介される一方、暗号アルゴリズムの移行に考慮されていないプロトコルも存在し、これらのプロトコルに関してはさらに多くの議論が必要になると説明されていました。

午前最後の講演は、セコム株式会社IS研究所の島岡氏の「日本発のPKI国際標準を目指して」でした。講演では、氏が標準化を目指すきっかけとなったJNSAのChallenge PKIという活動や標準化活動から学んだ標準化活動の難しさといったことが紹介さ

れました。標準化文章というものは、バックグラウンドが違う人にも正確にその内容を理解してもらう必要があるため、非常に緻密な論理構造、内容が求められるということが、英語以上に苦勞したと説明されていました。また氏のRFCである「マルチドメインPKIの相互運用性に関するメモ」は、RFC 5217として近日中に公開されることが紹介されました (2008/07/04公開)。

午後最初の講演は、JPNICの木村氏の「電子認証プラクティスフォーラム」でした。講演では、電子認証技術を使うためには、技術だけではなく運用やノウハウも重要であるが、今のPKIはこの部分が足りていないため、適切な普及が図りにくい状況であると説明されていました。このノウハウを電子認証技術に携わる人々で共有できるように、電子認証プラクティスフォーラムでは、電子認証に関わるノウハウをBCPとして文書化する活動を行っていると紹介されました。また本活動においてBCP化を目指しているいくつかのドキュメントも紹介されていました。

続いての講演は、日本電気株式会社の木村氏の「電子署名JIS制定の背景と今後の展望」でした。講演では、2008年3月20日に制定された電子署名に関する初のJIS規格である「JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル」および「JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル」を制定するまでの経緯と電子署名文書の安全性を長期間保証するための長期署名技術



について紹介されました。またこの長期署名技術を使ったソフトウェアは、相互に長期署名を検証できなければならないため、ETSI(欧州電気通信標準化機構)と共同でソフトウェアの相互接続テストを行っている」と説明されていました。

続いての講演は、セコム株式会社IS研究所の松本氏の「PKI対応IDカードの相互運用とHPKI対応ICカードガイドライン」でした。講演では、PKI対応IDカードの相互運用の難しさと相互運用を行うために策定したICカードガイドラインが紹介されました。ICカードは安全性の確保のため多くの仕様が非公開となっているが、ICカードを広く利用(相互運用)していくためには仕様を公開する必要がある、この非公開部分と公開部分のバランスが相互運用を行っていく上で難しいところであると説明されました。そして相互運用を行うためには「特定のベンダー等に依存しないデータモデル」、「特定のベンダー等に依存しないカードエッジI/F」が必要であり、JAHIS(保健医療福祉情報システム工業会)が策定した「HPKI対応ICカードガイドライン」では、こうした仕様をカバーしていることが説明されました。

続いての講演は、有限会社ロボックの伊藤氏の「オープンなPKI対応ICカードを扱うオープンソースソフトウェアの紹介」でした。講演では、公開されている標準仕様に準拠しているICカードを使い、ICカードを利用するために使用するソフトウェアとそのICカードをPKIアプリケーションから利用できるようにするための手順が紹介されました。講演タイトルにもある通り紹介されたソフトウェアはオープンソース、つまり無料で利用できるものであり、標準仕様に準拠しているICカードを購入するだけで、ICカードを利用することができると説明されました。

続いての講演は、マイクロソフト株式会社の渡辺氏の「Windows Server 2008のPKI機能」でした。講演では、マイクロソフトのPKIに対する考え方と

Windows Server 2008のPKI機能について紹介されました。マイクロソフトのPKIに対する考え方は、ただ動くことだけを狙っており、囲い込み等は考えていない。そしてよく誤解されているが、マイクロソフトのPKIはマイクロソフト専用ではなく標準と同じものなので、安心して使って欲しいと説明されていました。またWindows Server 2008のPKIの機能については、Windows Vistaと同様にNSAのSuite-Bのアルゴリズムが実装済みであり、それらの暗号を使った証明書を発行することができること、証明書検証機能としてOCSPに対応したことが紹介されました。

最後はセコムIS研究所の松本氏をモデレーターとし、IPAセキュリティセンターの山岸氏、松下電工株式会社の福田氏、日本クロストラスト株式会社の秋山氏、富士ゼロックスの稲田氏により「暗号アルゴリズム移行問題」についてのパネルディスカッションがありました。パネラーは暗号研究者、製品を作る人、証明書を発行する人、標準化に携わる人とそれぞれ全く立場が違うため非常に興味深いパネルディスカッションでした。パネラーの共通認識として、近年騒がれているRSA1024bitやSHA-1はアルゴリズムの脆弱化ではなく、世代交代の時期に来たということである。しかし世代交代と言うと強制力が弱く、脆弱と言うと過敏に反応されてしまうため、暗号アルゴリズムの移行に関してその進め方が難しいということが説明されていました。

今年のPKI Dayは、PKIが広く使われて来ているという印象を強く感じることでできたセミナーでした。JPNICの木村氏の電子認証プラクティスフォーラム、セコムIS研究所の松本氏のICカードの相互運用、そして最後のパネルディスカッションなどは、PKIが使われているからこそ問題になる話題であり、このPKI Dayのような有益なセミナーによって、PKIに携わる多くの人たちの共通認識となり、これらの問題が解決に向かうことを期待するばかりです。

中小企業情報セキュリティ対策支援セミナー開催結果

西日本支部長 井上 陽一

日 時	2008 年 11 月 26 日 (水) 13 時～ 17 時 50 分 (開場 12 時 30 分)
場 所	大阪国際会議場 10 階 1008 号室 (大阪市北区中之島 5-3-51)
主 催	NPO 日本ネットワークセキュリティ協会 西日本支部
共 催	NPO 日本システムインテグレーションパートナーズアソシエーション (JASIPA) 関西支部
後 援 (申請中)	近畿経済産業局、大阪商工会議所、社団法人 関西経済連合会、財団法人 関西情報・産業活性化センター、 社団法人 組込みシステム技術協会近畿支部

年の瀬も近づき慌ただしさが漂う多忙な時期のため、セミナーへの参加人数が気にかかりましたが、申込者の留保率が高かった事と JASIPA メンバーの参加で会場はほぼ満杯の状況であり、13 時から 18 時までの時間を熱心に静聴いただいたと思います。今回は JNSA 西日本支部としては第 11 回目のセミナーでした。これまでの単独開催から、JASIPA との共催という、ある意味で節目に当たる意義あるセミナーであったと思います。

システムインテグレータ等に大きく依存している中小企業には、情報セキュリティチェックシートの開発は JNSA が行い、JASIPA がチェックシートを顧客に適合する形にアレンジを行う (特に、技術的対策部分について、サポートする企業の特性を捉え、チェックシートで求める対策の具体的な実施策を提案・紹介願ひ、チェックシートと具体的実施策を紐付けていただく) 事が望ましいとの確信が得られたことで、今後も、関西でがんばる同種の団体とのジョイントセミナーをやらねばと感じさせてくれた今回のセミナー開催でした。

以下に、各テーマの講演者が主張された記憶にとどめたい内容を簡記します。

1. 【基調講演】

中小企業の情報セキュリティ対策に活用するツール類

IPA セキュリティセンター普及グループ・グループリーダの石井氏よりご講演いただきました。

説明資料は 70 ページに及ぶものであり、1 時間ではとても説明しきれないボリュームを判り易く説明いただくと共に、語りきれない部分については、提供いただいたツール類で補足をされました。

提供されたツール類は次の通りです。

- ・CD-ROM: 情報セキュリティ対策の基礎知識
- ・小冊子 (6 種)
- ・パンフレット: 中小企業経営者の皆様へ

昨年から中小企業における情報セキュリティ対策に関する研究会を立ち上げ、対策主体を 4 つに分類して研究を進めていますが、現在、検討結果の取りまとめの段階にあり、その成果を紹介出来ないため、



本日は「ここにこういった役立つ情報、ツールがあります」とご紹介いただきました。

2. 【JNSA セッション】

中小企業の情報セキュリティ対策について

JNSA 西日本支部情報セキュリティチェックシートWGリーダー(富士通関西中部ネットテック)の嶋倉氏より、前身の個人情報保護対策チェックシートWGから進化させた同WGの活動成果についてご紹介いただきました。IPAの講演資料と同様に50ページを超えるボリュームを45分間で説明されました。

3. 【JASIPA セッション】

(テーマ1)

JNSA チェックシートの利活用報告

JNSAのWGが作成した情報セキュリティ対策チェックシートを高く評価いただいております、実際にシステムインテグレータであるJASIPA関西のメンバー企業が体験した結果をご報告いただきましたが、システムインテグレータの20%強が情報セキュリティ対策に関心である事がアンケートから確認されました。この事から、中小企業をサポートするIT企業を対象とした啓発が必要との認識を強く持つと共に、IT事業者への警鐘としたいとのJASIPA関西副支部長のシステム・ファームズ代表取締役の上森 茂氏からの説明が補足されました。

(テーマ2-1)

製造業における情報セキュリティ対策の実情について

製造業向けITパートナーとして活躍をされている(株)フエムト代表取締役の梅谷氏より、製造業の現場における情報セキュリティ対策の実情をご紹介いただくと共に、「賢い管理」でも、「システム管理

責任者は絶対必要」とご講演いただきました。WGの金型、鞆の団体を訪問しヒアリングで得られたデータと相似した製造業における“特に重要な機密情報”が網羅されており、業界特有の表現、説明文等の必要を改めて感じさせられました。

(テーマ2-2)

製造・生産業務の標準化と過剰在庫の削減成功事例について

化粧品・医薬品製造業向けのITパートナーとして活躍されているシステム・ファームズ(株)部長の大上誠一氏から、IT活用事例をご紹介いただくと共に、システム面から見た情報セキュリティ対策についてご講演いただきました。情報セキュリティ対策を可用性の視点に立って、ビジネスと連動している活用事例をご紹介いただき、これまでのCI偏重のアプローチとは違ったアプローチ策となる内容でした

4. 【BoF】

なぜ進まない中小企業における情報セキュリティ対策

(1) BoF開催の目的

中小企業の情報セキュリティ対策の実情を把握するために実施したアンケート・ヒアリングの結果を総括し、情報セキュリティ対策を必要としている企業にはJNSA西日本支部が作成した情報セキュリティチェックシートを活用し、自社の実施状況を診断、さらなる改善・PDCAに役立てていただき、一方、守るべき情報資産があり、守らねばならない必要意識があるが、費用対効果の面が見えず躊躇・逡巡し対策が伴わない企業には、対策することへの義務化・切迫感を感じていただくために引き続きワークを継続し、情報セキュリティ対策の入口と考えられる情報資産管理台帳ワークシートの活用を推奨する事とし、台帳への記載を支援するサンプルモデル等を用意して、アンケート調査を行いました。

イベント開催の報告

その結果は、従前同様に回答率は低かったものの、製造業の業種団体の協力を得てより現場に近づいたものと評価できることから、再度総括し、情報セキュリティ対策のさらなる飛躍に向けての課題、対策へのステップとすべく開催したものです。

(2) B o F の実施

パネルディスカッション方式で、情報セキュリティ対策を啓発・支援する側、対策を実践する上でサポートする側・ユーザ側の代表者を配し、それぞれの立場からの知見による議論が期待できるものとなりました。

モデレータ:

元持 哲郎 氏(アイネット・システムズ株式会社)

パネラー:

石井 茂 氏(IPAセキュリティセンター)

嶋倉 文裕 氏(富士通関西中部ネットテック株式会社)

梅谷 康子 氏(株式会社フェムト)

林 道彦 氏(三星ダイヤモンド工業株式会社)

中小企業の情報セキュリティ対策につながる現実的な解とは何か、中小企業に共通的に感じられる費用対効果への不満、さらに、中小企業が実際に実践できるアプローチ手法をテーマに議論が進み、会場からは常識が守れない場合の内部・外部の反応がはっきりしました。セキュリティ対策を行ったことで儲かった事例、信頼が営業成約につながった等の事例集を作り、もっと啓蒙すべきでは、等の意見も出され、活発な討議が行われました。今後のセミナー活動継続に勇気を与えてくれたセミナーでした。

