JNSA 西日本支部主催セキュリティセミナー

株式会社サイロック　松原　裕正

日本ネットワークセキュリティ協会西日本支部主催の第 8 回セキュリティセミナーが近畿経済産業局、大阪商工会議所、財団法人関西消費者協会、社団法人関西経済連合会の後援のもと、3 月 16 日（木）に大阪市北区にあるコンベンションルーム・アクスネッツにおいて開催されました。
当日は残念ながら雨天でしたが、約 100 人（～ 120 人）の方にご来場いただきました。
今回は「コーポレートガバナンス強化に直面する中小企業のセキュリティ対策について」をテーマとした、今後の中小企業における新たなセキュリティ対策の方向性が示されるセミナーとなりました。

初めに

まずJNSA西日本支部中台芳夫氏より、JNSAの各部会が行っている様々な調査活動や、ワーキンググループの活動内容のご紹介をいただきました。

アメリカではSOX法の導入によって、情報セキュリティ対策を核としたITガバナンスの見直しが進められています。そして日本でもアメリカと取引のある会社を中心に、セキュリティ対策の見直しが始まってきています。

それに対し中台氏は「この動きはひょっとすると2008年3月からの日本版SOX法の導入が予定されていることを考えますと、今後の企業活動に影響するというふうに考えられます。またこの5月施行が予定されている新会社法においても内部統制システムの構築に関する方向性が示されるということで、今後中小企業に対し大きな課題をもたらすものと考えられます」と語られました。そしてコーポレートガバナンス、SOX法の概要についてふれられました。

「今回のセミナーでは関西圏に多い中小企業において企業の内部統制強化がどのような影響をもたらすか、そしてどのようなセキュリティ対策が新たにクローズアップされるかを明らかにしていきます」と話されました。

講演 1

中小企業向け個人情報保護対策 WG 活動報告

最初は「中小企業向け個人情報保護対策WG活動報告」と題し、WGメンバー 嶋倉 文裕氏(富士通関西中部ネットテック株式会社)より、一年間の活動報告及び今後の課題に関してご発表いただきました。

嶋倉氏はまず、個人情報保護法施行後一年が経過した現在、関心が高まってきているにも関わらずファイル交換ソフト(Winny等)のソフトを介して情報漏えい事故が多発しており、中小企業の間で個人情報をめぐって混乱があるのではないかと指摘されました。

「個人情報保護対策法の施行で中小企業はどんな状態に陥るのか。大企業と比較してできる対策はあるのか」という疑問を追及することがWG発足のきっかけでした。2005年2月に発足後、6月からモニタ企

業による実地検証を開始し、10月に中間発表、そして12月に2社目のモニタ企業のコンサルティングを行い、そして本日の結果発表となりました。

環境や規模も違う、扱っている情報内容も違う、それぞれの中小企業が、「個人情報保護体制の構築(Plan)、安全管理の実装(Do)、監査(Check)、対策の見直し(Act)」の一連のPDCAの仕組みを自分たちで運営できるようなものを作成したいという思いのもと、モニタ企業へのコンサルティングを通じた実地検証や、JNSA提供の雛形も参考にした中小企業の運用に適した形のテンプレートを検討し、様々なフィードバックを通じてテンプレートの完成度をブラッシュアップしてまいりました。

また昨年10月に行われたJNSAセミナーのアンケート結果報告と分析が行われました。

個人情報の趣旨は「個人情報をうまく使う」為のものであったはずなのに、経済活動の足かせになっているのではないか?と言う指摘や、個人情報保護法の施行を逆風とせず、個人情報保護の意識を高める事によって顧客評価が上がったところもあるという結果がありました。個人情報は使う為に持っている資産でありながら、守る事に一生懸命になって、使いにくくしている、自分で自分の肩身を狭くしているのではないだろうか、そのためにどうすればいいのかを考える事が課題だろう、と語られました。

情報管理の対策が担当者任せになっていること、個人情報に対して過剰な反応をしたり、なんでも個人情報として一括りにしたり、個人情報保護の対策が解らないという現状もまた見えてきました。

中小企業の現状として、個人情報に対する意識はあるが、どこまですればよいのか分からない所がまだまだ多く、技術的･物理的対策は重視されているが、組織的・人的な対策が軽視されている状態であることが分かりました。

そこでWGは「自分たちの課題・問題点が把握できていないのは、技術ではなくマネジメントに問題がある為」と考え、組織的対策を各々に分類する等、セキュリティヒアリングシートを工夫しました。具体的事例として台帳作成を挙げながら、中小企業における対策推進方法として、目標時期と成果を具体的に盛り込み、セキュリティヒアリングシートを個人情報保護体制のチェックシートとして加工し利用する、そしてチェックシートそのものが規定集の原案も兼ねるようになる事を発表しました。

対策と今後の課題について、「現状を把握しましょう。目標として何をして言いか分からないという声もありましたが、問題を把握していないのに目標はたてられません。次に共通意識を持ちましょう。これは中小企業の強みです。人数が少ないからこそできる。どういうことをしないといけないのかが、はっきり分かる。そして対策を検討しましょう。セキュリティヒアリングシートをベースにして、それを個人情報保護体制のチェックシートに加工し、いつまでに何をするのか目標時期と成果をはっきり書いて、PDCAサイクルをスパイラルアップしていきましょう。」と話されました。

情報セキュリティを大きな変化として、個人情報保護法の次に「日本版SOX法」「不正競争防止法改正」等が今後の課題として控えています。

最後にコンプライアンスルールを守る事が中小企業だからこそ大切であり、企業価値を高める事になるのではないか、とまとめられました。

講演２

企業価値の向上に向けた情報セキュリティ対策：目に見えない資産の重要性と内部統制

「企業価値の向上に向けた情報セキュリティ対策:目に見えない資産の重要性と内部統制」と題し、東京大学大学院情報学環の田中 秀行氏よりご講演いただきました。田中氏は情報セキュリティに対し経済的、経済学的な側面に立って話をされました。

田中氏はまず、情報セキュリティ対策には、ITに

イベント開催の報告

直接関係するソフトウェアやハードウェアだけではなく､｢目に見えない資産｣が重要であると語られました。実際に実証分析を確認すると｢目に見えない資産｣にどれだけ取り組んでいるかが情報セキュリティの水準を上げるという事が確認できましたので報告いたしますと述べられました。

IT技術が上がっても必ずしも情報システムのセキュリティ水準は上がっていないこと、組織のあり方も含む経済的動機付けについて考える事が重要であることについてふれられました。｢目に見えない資産｣として、ビジネスプロセスや組織内での意思決定権、情報共有や組織文化、人と人との関係、人材を挙げ、これらが、IT投資成功の鍵と述べられました。

また、セキュリティ水準を定めるものは｢取り組みの総和であり、最も弱い所であり、最も強い所である｣と説明され、相互依存性があり様々な例と共に問題点を喚起しました。

企業価値とセキュリティ対策について、情報漏えい事件や不正アクセス事件の報道後、情報セキュリティ・インシデントがあると短期的な株価の下落につながる事を話されました。

情報セキュリティ対策は企業価値を下げない為の、ネガティブな努力になりがちですが、日本企業を対象にした実証分析からすると｢セキュリティ対策をすると、企業価値が高くなる。むしろポジティブな評価がもらえる面がある｣と言う話をされました。情報セキュリティは、相互依存性があり、自分だけではなく相手にも一緒にやってもらうのが情報セキュリティである事、目に見えない資産は投資家も評価していると語られました。

そして｢国内情報セキュリティ調査の別冊で平成16年情報処理実態調査を用いた情報セキュリティ対策の実証分析に関する調査研究｣(JNSA調査)の結果から内容の分析が行われました。

2004年3月末のデータで情報通信機械製造業は8割がセキュリティトラブルを経験しており、金融・保険業・医療業の企業4割とやや低いものの、全業種平均で6割以上の企業がなんらかのセキュリティトラブルを経験しており、ウィルス感染は半数以上の企業が経験しています。

セキュリティ対策の実態に関して、4分の3の企業は何らかのセキュリティ対策をしているが、残りの4分の1の企業が対策をしていない。単一の対策しか導入していない企業が1割以上であると言う実態がアンケートの結果より分かりました。

また、企業の規模に関わらず、情報セキュリティ対策を投資額で把握できているのは一部の企業に過ぎませんでした。情報セキュリティ対策の費用対効果についても把握できているかという現状が示されました。企業の情報システムの状態とセキュリティトラブル経験の関係においてシステムの使用範囲が広いほどトラブル経験率は高く、電子メールID数が多いほどトラブル経験率が多く、電子メールIDあたりのIT経費が多いほどトラブル経験率は低い可能性があるという､面白い結果が得られたと報告されました。

セキュリティへの認識度合いとトラブル経験率の関係においては、セキュリティ・トラブルを重要と認識する度合いが高ければ高いほど、トラブル経験率は低いと言うことがいえそうです。

さらに、ファイヤーウォールだけをセキュリティ対策にしている会社ほどトラブル経験率は高いと言う結果より､｢安易にファイヤーウォールに頼っている所にトラブルが多い｣と言う指摘をされました。防御措置を単一手段に頼らず、ファイヤーウォールと、何かを組み合わせたり、またインフォメーションセキュリティポリシー等のセキュリティ・マネジメントや責任・教育体制と組み合わせる事により安全性が高まり、セキュリティ対策の効果が現れる。セキュリティ管理者を置く時に全社での管理者ではなく、部門ごとにセキュリティ管理者を置く場合にトラブル経験率が低いと話されました。

そして、個人情報保護法が成立されてから残業が多くなり生産性が落ちるという現象が起こっていて、セキュリティ水準を上げながら生産性も上げる為には

技術力が不可欠である事、また効果的なセキュリティ対策はハードウェアやソフトウェアに頼るのではなく、マネジメントや人材教育のような「目に見えない資産」への対策と補完的に行う事が重要であります。

内部統制においてIT関連パッケージを導入する事にとらわれることなく、むしろビジネスプロセス、目に見えない資産の見直しをする事が重要であり、そうする事で、内部統制が有効的に機能しはじめ企業価値を高めると述べられました。

企業活動は従来の組織の境界を越えつつあり、組織が異なっても一つのプロセスとしてまとまりを持つ「プロセス・エンタープライズ」へ移行しています。サプライチェーンマネージメントがわかりやすい例ですが、組織を越えたつながりが一連のプロセスとして把握できるようなEAやSOAはその動きを加速しています。例として自治体の電子化構想を述べられ、組織の境界を越えた動きが加速していると述べられました。

内部統制は、非公開の中小企業であってもプロセス・エンタープライズを前提とすると、内部統制は組織の境界内にとどまらず密接に関係している可能性が高くなってきている為にSLAやSLMの対応が求められるようになる。内部統制の構築についても「目に見えない資産」に効果的投資が重要であり、IT投資を通じて業務を効率化できる面や生産性を上げる面もあるのではないか、「守り」の話になってしまいがちですが、ビジネス環境に応じて積極的なIT戦略は残されているのではないかと最後に話されました。

質疑応答部分で、目に見えない部分への投資はどれぐらい掛ければいいかについて、ハードウェア、ソフトウェア部分より教育部分をしっかり考えておくことと、しっかり最初に計画しておく事が重要で、資料としてセキュリティ対策設計段階での投資を1としてメンテナンス運用部分でのセキュリティ投資が60倍もコストが掛かるということが言われていると述べられ締めくくられました。

講演３

内部統制のためのIT フレームワーク

最後に「内部統制のためのITフレームワーク」と題して、弁護士であり、また宇都宮大学工学部講師をされている高橋郁夫氏よりご講演をいただきました。高橋氏はアメリカのSOX法との比較等を通し、日本版SOX法の位置づけを行われました。そして内部統制のチェックリストを提示され、内部統制のあるべき姿、そしてITフレームワークの構築に関しての話をされました。

まず、日本の現状として、日本の政府がここ数年で取り組んできた会社法改正や改正監査基準などがあり、金融商品取引法に関しては全体像が見えてきたところです。「監査品質の向上」を実現するために内部統制の構築に関する企業努力をどのように評価するかが仮題です。

COSOフレームワークといわれているものは、資産保全等の観点から内部統制が考えられており、経営者はきちんと評価を行った上で外部に向けて報告をせねばならず、また公認会計士等が監査を行い、それを担保しなくてはなりません。これが金融商品取引法案の要旨として平成１８年3月１０日に閣議決定されました。これをマスコミは日本版SOX法と呼んでいます。

また日本とアメリカ版SOX法との比較では、訴訟制度が非常に違う点が指摘されました。日本版SOX法が施行されるにあたり、社会に対する影響は少ないのではないかと考えられますが、取引先との間で「信頼性を確保して、きちんと問題が起きないように、ビジネスも継続します、情報を預かっても守っていけます。」と宣言することが、内部統制を構築するということである、と問題提起されました。

業務プロセスの改善を前提としなければ、内部統制の構築が役に立つかどうかは微妙です。なぜならSOX法は新しい概念というわけではないからであり、日本版SOX法がどのレベルを要求するのかの合意はこれからの課題なので、早く対応することが目的ではないのではないかと考えられます。

実際にITが関わる部分を含む内部統制を考える場合、COSOキューブと呼ばれる、ビジネスの全般をコントロールするモデルがあります。一方、ITセキュリティで必要とされる要素はどのようなものがあるか、各要素に対する制御機能を考え、ビジネスの目的、IT資源等との情報をうまくリンクさせるための橋渡しが「COBIT」というモデルです。これはIT資源に関する色々な観点(計画と組織、調達と導入、サービス提供とサポート、モニタリング)からビジネス目標や到達目標など、いろいろな項目ごとのチェックを行うアーキテクチャーとなります。

リスクを減らして機会を増やしていく、そのために利益や効率を上げ、制御機能として内部統制を考えていくことが、企業文化を根付かせます。内部統制の基礎として重要なのは企業文化なのです。
内部統制をいろいろな業務ごとに構築し、IT化するとERPパッケージという形になります。ERPパッケージを導入しようとする時、元々のプロセスの見直しが重要であり、なかなかうまくいかない場合があります。この時は、ITを離れてコーポレートガバナンスを考え直す必要があります。

内部統制は不正を防ぐものとして、自分たちの企業の立脚点と、構成員で押し進めていこうとする文化、何が正しく何が間違っているということを理解していこうとする構成員全員の意思と共通の方向性が必要です。内部統制のキーワードはtransparency(透明性)を保持し、何か問題が起こったときに「自分たちはこうしていましたよ」というaccountability(説明責任)、監査証拠を示す考え方が非常に重要であると締めくくられました。

終わりに

個人情報保護法の施行後、個人情報の取り扱いに対する戸惑い、一種の空気のこわばりがあるようです。個人情報の価値が叫ばれているにもかかわらず、winnyなどのソフトを介して個人情報が漏えいしている事件が新聞に載ることは、もはや珍しくありません。

企業に対して、ITセキュリティ対策やコーポレートガバナンスの見直し等、内部統制に関する要求は日々高まっています。

今回のセミナーにおいては内部統制の構築、ITフレームワークという形で取れる対策について、経済学的な視点から、また法律的、学術的な視点からの分析が行われました。またアンケート結果を通して、現在の企業が直面している問題が見えてきたと考えられます。

「企業はどこまで内部統制を、セキュリティ対策を行うべきなのか?」という問いに対して、「それはそれぞれの企業によって違ってきます」という答えが返りました。

内部統制の構築がネガティブな努力ではなく、企業価値の向上につながるポジティブなものになりえるということが、中小企業のコーポレートガバナンスのひとつの指標となりえるのではないでしょうか。

JNSA 2005 年度 ワーキンググループ成果報告会

JNSA 主席研究員　安田　直義
JNSA 研究員　松田　剛

2006 年 5 月 30 日、大手町サンケイプラザに於いて、2005 年度日本ネットワークセキュリティ協会成果報告会と定時総会が開催されました。ここでは、成果報告会の内容についてご紹介します。尚、当日のプレゼン資料などは下記の URL で公開されていますので、合わせてご覧ください。

http://www.jnsa.org/2006/seminar/20060530.html

成果発表会は下記のプログラムのように、2 部屋に分かれて平行して報告されました。今年度は、昨年の両方聞きたかった、というご意見を参考にし、発表の長さを揃え、トラック間の休憩時間を合わせることで、相互に行き来できるように配慮してみました。

2 トラックの 1 トラック目は、教育部会と技術部会、2 トラック目は政策部会と西日本支部が担当しました。次に報告内容について順を追ってご紹介して行きましょう。

303 号室		304 号室	
教育部会（10:30-12:00）		政策部会（10:30-12:00）	
10:30-11:00	CISSP WG NTT コミュニケーションズ 大河内 智秀氏	10:30-11:00	セキュリティ会計ガイドライン検討 WG 凸版印刷 佐野 智己 氏
11:00-11:30	情報セキュリティ推奨教育検討 WG セキュリティ・エデュケーション・アライアンス・ジャパン 持田 啓司氏	11:00-11:30	スパイウェア対策啓発 WG アークン 蛭間 久季 氏
11:30-12:00	情報セキュリティ教育実証実験プロジェクト JNSA 研究員 松田 剛氏	11:30-12:00	セキュア・システム開発ガイドライン WG ラック 丸山 司郎 氏
12:00-13:00 昼休み			
技術部会（13:00-15:20）		政策部会（13:00-14:00）	
13:00-13:30	脆弱性定量化に向けての検討 WG セコム 金岡 晃 氏	13:00-13:30	セキュリティ市場調査 WG リコー・ヒューマン・クリエイツ 勝見 勉 氏
13:30-14:00	PKI 相互運用技術 WG セコム 松本 泰 氏	13:30-14:00	セキュリティ被害調査 WG ディアイティ 山田 英史 氏
14:00-14:20 休憩			
14:20-14:50	WEB アプリケーションセキュリティ WG 住商情報システム 二木 真明 氏	西日本支部（14:20-14:50）	
		14:20-14:50	中小企業向け個人情報保護対策 WG 伊藤忠テクノサイエンス 市川 順之 氏
14:50-15:20	不正プログラム調査 WG アークン 渡部 章 氏		

トラック1（303号室）

教育部会

午前中は教育部会からの発表が3件ありました。

CISSP-WG

NTTコミュニケーションズの大河内智秀氏から、CISSPに関する活動の報告がされました。CISSP-WGは2006年度からISSJP-WGとして活動していますが、2005年度の活動として、CISSPの上位資格として日本の状況、特に地方自治体などを念頭に置いたISSJPのCBK（Common Body of Knowledge）作成や問題作成などの活動チーム、作業ドメインについて説明されました。ISSJPのドメインは、法ドメイン、制度・政策ドメイン、技術ドメイン、倫理その他ドメインの4つで構成されており、2007年より試験開始の予定だそうです。

CISSPは世界で5万名くらいが取得しているITセキュリティに関する代表的な資格ですが、日本でのセキュリティ意識の啓発のためにももっと普及させたいとのことでした。

情報セキュリティ推奨教育検討WG

セキュリティ・エデュケーション・アライアンス・ジャパン（SEA/J）の持田哲司氏から、情報セキュリティ推奨教育に関する活動報告がありました。教育の必要性はどの組織でも8割は認識しているが、実装は難しい。ともすると売れるという観点だけから教育プログラムを作ってしまう。組織の中で必要かどうかではなく、対症療法的な教育になりやすいという現状認識の下、どのような教育が実際に行われていて、またどのような教育を行えばよいのかを整理するという目標で活動され報告書がまとめられているそうです。

一例として、内部統制に関するITへの対応例を考えるとき、IT成熟度診断や、ERP、BPM系ツールが利用されることもあるが、これらでカバーしきれない部分の限界についての対策として、教育が重要な役割を持ち、これをIT担当者、全スタッフばかりではなく、経営者の教育も重要だとの指摘がありました。また、キャリアパス形成についてのロードマップについての考え方の説明があり、これらは報告書として公開される予定とのことでした。

情報セキュリティ教育実証実験プロジェクト

JNSA研究員の松田剛氏から、東京電機大学、工学院大学、岡山理科大学で行われた、ITセキュリティの専門家育成コースの実施について報告されました。高等教育機関でも、ITセキュリティに関するコースは解説されていますが、どちらかというと暗号教育などの理論研究に偏っている節があるので、もう少し実践的な教育内容があってよいのではないか、という即戦力への期待が発端となっています。

教えられる側、教える側の意識調査結果や、地方の問題として、対応できる講師がいないという事案に対する問題提起と解決の提案がされ、2006年度の活動として解決案の実践が予定されているとのことでした。

技術部会

午後は技術部会からの発表が4件ありました。

脆弱性定量化に向けての検討WG

WGメンバーのセコムの金岡晃氏に発表していただきました。本WGの目的は、サーバーマシンを運用管理する現場技術者がパッチ情報などを当てるに際して、どのくらいの重要度があるかを定量的に評価しようというところから始まっています。このために、攻撃が発生するメカニズムをモデル化するにあたって、CVSSやMSの脆弱性評価とは異なる検証可能なモデルを作るアプローチを採っています。

モデル化を考える際に検討したのは、脆弱性とは何か？のコンセンサスを取ることであり、脆弱性の構

成要素を整理し、攻撃が発生した時の主体(エンティティ)をオブジェクトとし、オブジェクト間の関連(リレーション)について、良い影響／悪い影響を評価する方法論を取っています。このように、攻撃発生のメカニズムの解析を基にした数式モデルを作成し、Excelシートで数値計算ツールを試作しているそうです。観測可能な属性値を適用して、メンバー内でレビュウを行っているそうです。2006年度活動として、引き続き数値化の確定やツールの公開、報告書の作成を行う予定とのことでした。

PKI相互運用技術WG

セコムの松本泰氏からハッシュアルゴリズムの危殆化等に関して、SHA-1問題の背景と現状について解説されました。最近話題になっているSHA-1というハッシュ関数が事実上解読可能となってしまったことを踏まえ、一番弱いところが狙われるのは必定なので、ある時点で下位互換性を断ち切る大きな転換が必要であることが説明されました。しかし、多くのアプリケーション等の実装は、暗号アルゴリズムに依存した仕様になっている場合が多く、移行が難しい問題点が指摘されました。タイムスタンプはSHA-1からSHA-2に移行できましたが、広く普及する前だったので移行ができた面と、移行できたのは文書のハッシュのみで、時刻証明のハッシュはSHA-1のままという問題点があります。

米国の政府調達基準を作っているNISTでは2010年までしかSHA-1を許しておらず、SuiteB基準ではSHA-1, RSAを認めていないのは重要な点であることが説明されました。

WEBアプリケーションセキュリティ WG

住商情報システムの二木真明氏から、Webアプリケーションのセキュリティを確保するための技術的な活動についての報告がありました。2005年度は、啓発コンテンツ、受発注ガイドライン、技術分科会に分かれて活動していました。

受発注ガイドライン分科会の奥原雅之氏(富士通)から、絶対人が死なない自動車です、というような契約内容が横行しているという点が上げられ、瑕疵だ、欠陥だ、仕様だ、などの水掛け論を避けるにはどうすればよいか、という問題提起がされ,「Webリスクモデルのツリーモデル」について説明がありました。

2005年度は、メンバーが技術系の中核を担っているため多忙で思うような成果が出せなかったという反省を踏まえて、2006年度はテーマを絞り込んで活動する予定だそうです。また、WGリーダーの二木氏が技術部会長になるのに伴い、新WGリーダーとしてIIJテクノロジーの加藤雅彦氏に交代し、技術的な背景を持った経営層に働きかけられるようなコンテンツを作成する方向で活動を予定しているとのことです。

不正プログラム調査WG

最後にアークンの渡部章氏から、不正プログラム全般に対しての対策ガイドラインの改定版について説明がありました。不正プログラムを分類化し、タイプ別、進入経路別に対策ソリューションをわかりやすくまとめたものになっています。不正プログラム対策の3要素である、予防、検出、復旧について、企業規模ごとに対策の考え方をイラストで説明されており、不正プログラム対策10か条や、具体的なチェックシートとともに解かりやすいガイドラインになっています。

(安田)

イベント開催の報告

トラック 2（304 号室）

2トラック目には、政策部会から5件、西日本支部から1件の発表をしていただきました。

政策部会

午前中と午後の前半は政策部会からの発表が5件ありました。

セキュリティ会計ガイドライン検討WG

凸版印刷の佐野智己氏に冒頭の発表をしていただきました。「セキュリティ会計」とはまだあまり聞きなれない言葉ですが、環境会計に倣って企業のセキュリティ確保における取組みを適切に把握、評価そして伝達する仕組みを示すもので、2004年度から研究に着手しました。情報セキュリティの確保や評価が難しいのは、定量化すなわち「費用対効果」が明確化できないといった問題は以前から指摘されていましたが、セキュリティ会計WGではこうしたセキュリティが抱える本質的な問題に正面から取り組んでいることから、筆者も注目するWGの一つです。

スパイウェア対策啓発WG

アークンの蛭間久季氏にご報告していただきました。一般的には 情報漏えいといえばWinny事件が注目されていますが、キーロガーやワンクリウェア（ワンクリック詐欺）などの危険性は十分に認識されているとは言えません。蛭間氏はスパイウェアを「利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム」と定義づけたうえで、一般のPC利用者にそうした危険性と対策方針を普及する取組みを紹介しました。スパイウェア問題に関する取組みはいまだ各国で統一した動きが見られず、今後は北米、欧州、中国、韓国などの事情を調査し、日本独自の対策方針を提言することを目標としています。

セキュア・システム開発ガイドラインWG

ラックの丸山司郎氏にご報告いただきました。セキュア・システム開発ガイドラインとは、「システムオーナー（ユーザ側企業）が、RFPに記載すべきセキュリティ要件」を整理したものを示します。その目的はユーザ側企業とITベンダー側のコミュニケーションギャップ解消を目指したものです。安全なシステムを作りたいというユーザ側とITベンダーの思いは共通なのに、方法論や成果物の評価をめぐって対立してしまう残念なケースも少なからず存在します。「リスク」という抽象概念を扱うことからこうした問題が発生するのだと思いますが、調達側と供給側双方の共通尺度が存在すれば実務的な効果は計り知れないでしょう。

セキュア・システム開発ガイドラインとは共通尺度、いうならばコミュニケーションツールのようなもので、パターン1：対策視点のRFP、パターン2：現象視点のRFP、パターン3：脅威視点のRFPといくつかの視点に分類して開発を目指しています。

セキュリティ市場調査WG

リコー・ヒューマン・クリエイツの勝見勉氏にご報告いただきました。セキュリティ市場調査WGは経済産業省の委託と支援を受け、国内の全情報セキュリティ事業者を対象に市場調査を行いました。報告のなかで興味深かったことは、「以前にこうした調査を行った際は事業者がセキュリティに特化した数値管理していたが、今日ではこれらはITシステムのなかの必要条件として組み込まれており、独立した数値

を有していないケースが多く、調査活動の難しさを再認識した」という点です。

こうした状況は調査ないしは統計的にはやっかいな側面があるかもしれませんが、安全意識がITシステムのなかにビルトインされつつあることを如実に示しており、セキュリティの面からは極めて歓迎できそうな傾向ではないでしょうか。

セキュリティ被害調査WG

政策部会の最後は、ディアイティの山田英史氏に発表していただきました。注目度の高いセキュリティ被害調査WGは、セキュリティ会計WGと同様にリスクの数値化・定量化を目的に設立され、主として情報漏えいに係わる損害賠償請求額を調査研究アプローチとして設定しています。様々な事件・事故の分析結果から山田氏は、「現在の企業・病院・学校などが施す個人情報保護対策は、情報の保護にナーバスな顧客や患者を基準に考えられており、普通の人にはむしろデメリットなのではないか。また本来であれば対策の目的は本人を守ることのはずなのに、どちらかと言うと企業側を守るために行っているような印象を受ける。法律の趣旨に従って、もっと本人の方を向いて考えるべき」との提言を行っていただきました。筆者も同法のもつ真の理念が社会に誤解されているという思いから、山田氏の提言には考えさせられるものを感じています。

西日本支部

中小企業向け個人情報保護対策WG

伊藤忠テクノサイエンスの市川順之氏に発表していただきました。西日本支部では、中小企業向け個人情報保護対策WGが精力的な活動を展開しています。このWGは、個人情報の保護やその対策手段の普及に力点を置いている点は他のWGと同様ですが、中小企業にターゲットを絞り込んでいるところがユニークです。2005年4月に同法が施行されたのちの中小企業の動向や大企業部門との比較などを通じて、課題を明確化していただきました。とくに中小企業部門では、技術対策の目標レベルを単独では決めにくい環境にあることを強く念頭におき対策ツールを策定、その紹介を行っていただきました。こうしたツールはこれまで大企業ユースを前提に作られているものが多く、中小企業部門のユーザ企業あるいはこのセグメントをマーケティング対象とするITベンダーの方には魅力的なものと思います。

（松田）

最後に

2005年度のJNSA活動報告会は多彩な内容でした。教育部会、技術部会、政策部会、西日本支部と、それぞれの内容も興味深いもので、多くの方々に参考となるものだったと思います。JNSAではこのほかにもマーケティング部会が中心になっている「インターネット安全教室」の活動もありますが、こちらは別稿でご紹介します。

JNSAの活動にご興味があれば、まずは参加してみてください。また、新しいテーマでの活動を起こされたい場合もぜひご相談ください。ご質問やご相談はご遠慮なく事務局までご連絡くださるようお願い申し上げます。

第２回 PKI Day －PKIの展開と最新技術動向

セコムIS研究所　新野　賢央

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の展開と最新技術動向」が6月7日（水）に、南青山の東京ウィメンズプラザホールにおいて開催されました。「PKI Day」というタイトルを掲げてのセミナーは今回が2回目の開催となりますが、昨年10月に行われた第1回を上まわる250名以上の申し込みがあり、実際の参加者も190名という盛況でした。冒頭の主催者側挨拶の「ニッチなインフラ技術であるPKIが、確実に盛り上がりを見せている」という言葉も、にわかに実感できる雰囲気で始まりました。

まず午前の最初の講演では、セコムIS研究所の松本氏より「PKIの展開と最新技術動向」というタイトルでご講演いただきました。冒頭では、この相互運用技術WGのリーダーであるという立場から、現在までのChallenge PKI プロジェクトに関する経緯や活動報告を説明されました。続いて、電子署名法の改正議論、電子署名の展開という内容で、現行の電子署名法やPKIの展開に対する問題点を示しながら、今後どうなるべきかというビジョンを“松本キューブ”なる概念図を用いてわかりやすく解説されました。

続いての講演として、「わが国の保健医療福祉分野PKIの動向」というタイトルで、東京大学大学院・学際情報学府の山本氏にご講演いただきました。講演内容としては、行政の立場から医療情報がどう変革を遂げてきたのか、を示す年表に沿いながら、平成6年の医療画像の電子媒体への保存から始まり、最近の取り組みとしてIT新改革戦略におけるレセプトオンライン化、EHR-DB、HPKIの3点についてそれぞれ説明されました。

午前中最後の発表では、国立情報学研究所の島岡氏より、「大学間連携のための全国共同電子認証基盤UPKI構想と米国学術PKIの動向」というタイトルでご講演いただきました。講演内容としては、冒頭では簡単に米国学術PKIプロジェクトを紹介され、学術情報基盤UPKIの現状に関する話題を紹介されました。UPKIについては、3つのPKI、オープンPKI、キャンパスPKI、グリッドPKIをうまく連携させて機能させていくことが重要であると同時に、明確な保証レベルを定義してそれを共有して運用していくことが必要であると主張され、また、大学有志がUPKIに関してバーチャルに意見交換できるコミュニティ作りを進めていく予定であることも紹介されました。

午後最初の発表として、産業技術総合研究所グリッド研究センターの田中氏より「グリッドにおけるセキュリティの概要と動向」というタイトルでご講演いただきました。前半ではGSIというProxy証明書やDelegateを用いたグリッドセキュリティ技術を紹介され、これらの技術によりグリッドの普及面に関して大きく貢献した点、今後のビジネス展開にはセキュリティ上若干の問題があるProxy証明書に代替する技術が必要である点を示されました。また後半では、国をまたいでグリッドのポリシーや運用を調整するPAMと呼ばれる機関とその活動を紹介され、加えてIGTFと呼ばれるPAMを統括する上位機関が設立されたことについても紹介されました。

続いての発表として、三菱電機・情報技術総合研

究所の宮崎氏より「長期署名フォーマットとECOMにおける相互運用実証実験について」というタイトルでご講演いただきました。宮崎氏がWGリーダーを勤めるECOMの長期署名保存フォーマット普及SWGでは、前年度にECOMプロファイルに基づいた長期署名フォーマットの相互運用実験を行っており、今回はこの結果報告の内容を中心にお話いただきました。報告内容としては、この実験により参加企業数社内での相互運用性はある程度実証されたという反面、以前、不明確な仕様があり更なる議論が必要という部分も見つかったという報告もありました。また、現在直面している大きな問題として、推進すべき国際標準が実は国税要件の電子文書に対応しているとは言いがたい現状がある点をあげられました。

続いての発表としては、富士ゼロックス株式会社の稲田氏より「標準はどのように実装されているのか?～OpenSSLにおけるSSL/TLSの実装に関して～」というタイトルでご講演いただきました。冒頭ではSSL/LTSに関する技術的概要や歴史などを、続くスライドでOpenSSLに関する生い立ちや特徴などを紹介されました。その中で、OpenSSLは事実上この分野におけるデファクトスタンダードツールとなっており、単純なSSL/TLSスタックとして利用するのに問題はないが、証明書の失効検証機能としては不十分な実装が見られるという点を説明されました。

最後の発表では、「Windows VistaのPKIとIE7」というタイトルでMicrosoftの渡辺氏よりご講演いただきました。冒頭では、今秋以降リリース予定である最新OS、Windows Vistaに新たに搭載される証明書の失効機能の紹介をされました。従来から悩みの種であった失効機能に対して、Vistaではデフォルトオンという設定を試みており、その背景にはどのような技術でもって数々の問題に対処してきたかという点について説明されました。また、発表後半ではVista搭載予定の最新セキュリティ機構である、

BitLocker、Microsoft Certificate Lifecycle Managerや、最新版IEであるバージョン7でのサイト認証の扱い方などについても示されました。

将来的にPKIはインフラとして私たちの生活に深くかかわってくる技術です。未来の生活には印鑑というものは古き時代の遺物となり、現実世界でもオンラインの世界でもICカードなどをかざして自分を他人に認証してもらう時代がすぐそこまで来ています。しかし、そこにはインフラとして備えるべき、相互運用性問題という大きな壁が存在しています。この大きな壁を乗り越えるには、まずはPKIを導入できるあらゆるドメインの人々が、「PKIはいかなる技術か」をしっかりと理解し、みなで議論しながら普及・啓発していくことが大切ではないでしょうか。こうした試みの一端を担うことを目的とし、今回のように有益なセミナーが多く開催され、多くの方々がPKIに興味を抱いてもらえることを期待するばかりです。