JNSA 西日本支部主催セキュリティセミナー
NSF2005 in OSAKA

JNSA 西日本支部 セミナー運営 WG リーダー
西日本電信電話株式会社　中台　芳夫

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 6 回セキュリティセミナー「NSF2005 in OSAKA」が、経済産業省、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、10月27日(木)に大阪市にある天満研修センターにおいて開催されました。当日は好天にも恵まれ、約90名の方にご来場頂きました。

今回は企業における「情報セキュリティガバナンス」をテーマとし、経済産業省からの基調講演、法曹界からの個人情報保護対策のあり方をそれぞれご講演頂いたほか、JNSA の各部会の WG から、最新の研究成果について報告し、本格的な情報セキュリティ対策を目指している企業等のお客様に対し、今すぐ着手すべき情報セキュリティ対策のポイントを明らかにするセミナーとなりました。

プログラムは最初に井上支部長から、「４月に個人情報保護法がスタートし、『日本版SOX（Sarbanes-Oxley）法』の導入の動きも見られる中、適切な情報セキュリティ対策を打つことが企業の価値に結びつく、と注目を浴びています。今回のセミナーを機に『情報セキュリティ・ガバナンス』に対する知識・研鑽を深めて頂きたいと思います」とご挨拶を頂き、あわせてJNSA、各部会・WGの調査研究活動状況、および西日本支部の取り組みについてもご紹介を頂きました。

続いて基調講演として、「企業における情報セキュリティガバナンスのあり方」と題し、経済産業省・商務情報政策局・情報セキュリティ政策室課長補佐の村野正泰様からご講演を頂きました。村野様からはまず、「政府では、世界最高水準の高信頼性社会の実現のため、しなやかな事故前提社会システムの構築、高信頼性を強みとするための公的対応の強化、内閣機能強化による統一的推進、の３つの戦略からなる情報セキュリティ総合戦略を掲げ、これに基づいて内閣官房の機能強化を図り、政府機関の総合対策促進として『情報セキュリティ基準』をまもなく策定予定です」と、政府全体的な動きについてご紹介頂き、関連して、企業等の情報セキュリティにおける組織的対策の推進、早期警戒体制の整備など、経済産業省として推し進めている各種事業についてご紹介頂きました。続いて今回のセミナーのメインテーマである「情報セキュリティ・ガバナンス」への取り組みについてご紹介頂きました。企業等における近年のIT事故は経営を左右し、社会的にも大きな影響が出ることになります。このため企業自身が情報セキュリティを自律的・継続的に改善するための組織的かつ包括的アプローチが求められます。また米国のSOX法の成立過程にも見るように、事業継続計画(BCP)を策定しておくことも、大規模な事件に遭遇した場合でも企業経営を健全に維持するための必須条件として求められつつあります。村野様はこれらの状況に端的に触れ、「情報セキュリティ・ガバナンス」の必要性を訴求されました。一方で、適正なセキュリティ投資の判断の難しさ、セキュリティ対策の企業価値への評価の反映等が、日本では適切に判断されていない問題点として存在しています。経済産業省では、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル、事業継続計画策定ガイドラインの３つを、

西日本支部長 井上陽一氏

イベント開催の報告

情報セキュリティ・ガバナンスの確立を促進するツールとして策定し展開を行っています。村野様からはツールを利用した取り組みについて詳しくご紹介を頂きました。講演後の質問では「今回のツールが今後の日本版SOX法における企業の取り組みの指標として継続的に利用可能なのか」などの質問があり、企業でも日本版SOX法を意識した取り組みが少しずつ始まっていることがうかがわれました。

午後からは、JNSAの代表的なワーキンググループの調査活動報告を行いました。報告内容の選定にあたっては、セキュリティ対策の不備によって生じるインシデントによる被害額の算定、その対策の代表例としての個人情報保護対策、そして今年度上期に著しく話題を集めたマルウェアの動向と対策と言う形で、リスク分析と対策の双方の重要性を受講者に認識して頂く形式を取りました。

最初の報告は「2004年度個人情報漏えい事件の分析と想定被害額の算出による評価」と題し、JNSA政策部会・セキュリティ被害調査WGメンバーの山本匡様(株式会社損保ジャパン・リスクマネジメント)から発表頂きました。山本様からは「日本でセキュリティインシデントに対する被害額が端的に判るものがないか、とJNSA事務局で議論されたのがWG発足の契機であり、インシデント被害調査を2001年度から着手しました。2004年度は警察庁からの委託事業としてのインシデント被害調査(『不正アクセス行為対策等の実態調査』)と、JNSAの活動として個人情報漏えいにおける被害考察と分析を実施しました。前者のインシデント被害調査では、632の回答の中からインシデント被害に遭ったと言う回答が230事業体あり、被害後は技術的対策をとる例が多数見られました。また従業員1人あたりの被害額と対策費用との相関関係は明確ではないものの、2～3万円の対策費用で被害はある程度抑えられていると想定されます。後者の個人情報漏えいによる被害想定の調査においては、2004年度になって小さな『漏えい等事故』も報告されるようになって、調査対象件数も大きく増加しています。想定損害賠償額算定式のモデル化から、2004年度の想定損害賠償額総額は4,666億円以上に達すると想定されています。個人情報漏えいの被害が株価へ影響する点も分析を続けています」と、2004年度の調査報告の要点を講演して頂きました。講演後には、個人情報保護の賠償請求額の具体的な算出式についての質問などが寄せられていました。

経済産業省 林野正泰氏

続いて「中小企業に必要な個人情報保護対策の策定に向けて」と題し、JNSA西日本支部・中小企業向け個人情報保護対策WGメンバーの西村祥様(伊藤忠テクノサイエンス株式会社)から発表頂きました。西村様からは「当WGは、大企業とは異なった位置づけで個人情報保護が求められる中小企業の現状の取り組みについて調査し、具体的な対策･対応方法を運用マニュアルとして取りまとめ、各種中小企業での利用に役立てて頂けるものを策定したいと考えています。WGはコンサルティングチームと研究チームに分かれ、月1回のミーティングを基本として活動しています。モニタ企業様をチェックした現状報告としては、セキュリティに対する文書化の不徹底や、システム対策と運用とのバランス不足がみられています。またモニタ企業様の生の声として、保護法対策している企業としてのアピールの展開方法や、企業規模に応じたセキュリティ対策の指標化を模索している

点が課題として挙がっています」と報告が寄せられました。本WGの課題として、モニタ企業が1社に限定されている点、WGメンバが不足している点にあり、早急な対応が必要となっています。講演後はWG参画に興味を持った受講者からの問い合わせがあるなど、WG活動の活性化に向けて受講者からの反応を頂いた点が印象的でした。

三番目には「多様化するマルウェアの実態と対策」と題し、JNSA技術部会の渡辺章様(株式会社アークン)から発表頂きました。不正プログラム調査WGのリーダでもいらっしゃる渡辺様からは、最近著しく話題を呼んでいるスパイウェア、不正プログラム、ウェブアプリケーションへの攻撃等について詳しい解説を頂きました。渡辺様は「スパイウェアの定義はまだ曖昧であって、多種多様なものが分類されています。米国ではアドウェア等のスパイウェアモジュールを作成・配布しているソフトウェア会社もいて、ユーザはフリーウェア等のインストール時に、これらのモジュールを知らずに取り込んでしまっているケースもあります。国内でもネット銀行のユーザ等を標的としたスパイウェアの活動も報道されるようになりました。米国では、広告表示のプログラムがスパイウェア対策ソフトによる駆除対象と扱われて訴訟になったことをきっかけに、業界を主体に2つのスパイウェア規制法案が検討され、採決待ちになっています。国内でも問題が大きくなれば同様の動きになると想定されるでしょう」と語られ、パソコン上で自己修復機能・ステルス機能を仕掛けるマルウェアの実演も交え、マルウェアの現状について報告されました。またウェブアプリケーションへの攻撃についても、「2004年からSQLインジェクション攻撃が急激に増加していますが、悪用の危険性は旧来から言われていたもので、未だに事件が生じています」と、ウェブアプリケーションプログラム作成の陥穽について指摘され、網羅的な対策の必要性についても詳しくコメントを頂きました。

そして最後に「情報セキュリティ対策における実務上の法的課題について」と題し、きたおか法律事務所の北岡弘章弁護士にご講演頂きました。北岡様は、「企業において漏えいリスクの高い情報は多種ありますが、多数の相談を受けていることを背景に、個人情報保護関連で一般企業の懸念事項となっている点について解説します。個人情報の漏えいリスクを考えた場合、クレームや訴訟による金銭的な損害賠償を生じる例は少なく、むしろ信用喪失のリスクが大きく存在します。小額のお見舞い金を配布するかどうかは企業の姿勢であって必ず生じるリスクとは言えません。その他にもサービスの停止・解約やサイトの閉鎖による損害、株価への影響、行政処分等のリスクが存在します。その対策としての安全管理措置の中で、ここでは従業者の監督について詳説します。情報漏えいは内部からの犯行が多いものですが、従業者の管理を厳しくし過ぎた場合には人権侵害の問題になりえるため、法的には悩ましい部分です。『モニタリング』は従業者の個人情報を収集し、プライバシー侵害の問題にも関わってくるため、省庁の個人情報保護ガイドライン等に沿った形で実施する必要があります。また誓約書の提出は範囲の明確化と自覚を促す意味としての存在に留まると考えられるため、従業者の秘密保持義務については就業規則で明確化しておく必要があります。競業避止義務については職業選択の自由との関係で有効性が問題と思われます。情報を守るための社内規則等について、守れないルールは止めて合理的なルールを策定すべきであり、実行不可能と判明したルールはどんどん改訂していくことが大事です。内部犯行の特定のためにはアクセスログを記録することが重要ですが、今後は日本版SOX法の出現により、内部統制を行う上でのモニタリング、アクセスログ記録が不可欠になってきます。また財務情報の正確性の確保も求められるため、情報セキュリティの三要素のバランスを取ることが法的にも要求される傾向が想定されます」と講演され、従業者の立場も配慮した人的安全管理措置のあ

り方と、今後のセキュリティ対策の方向性について明確化して頂きました。

情報セキュリティ対策は、個人情報保護法が本格的な定着期に入ろうとする中で、3つの観点からの変容の時期を迎えようとしています。一つ目は「情報セキュリティ・ガバナンス」の観点からの組織的対策のシフト、二つ目は「システム防衛型」から「情報漏えい対策型」への技術的対策のシフト、三つ目は「予防偏重型」から「事故前提型」へのリスク管理のシフトです。すなわち、企業の発展に帰する「あるべき姿」を意識し、来たる「日本版SOX法」の到来も視野に入れ、情報セキュリティ対策機能をコーポレート・ガバナンス(企業統治)における内部統制機構に如何に取り込んで、どう運用していくかが、今後の情報セキュリティ対策のキーポイントになると言えるでしょう。今回のセミナーはその変革の前段階の時期にあって、今後の取り組みのありかたに対して一石を投じるものになりました。