JNSA 西日本支部主催セキュリティセミナー

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
富士通関西中部ネットテック株式会社　嶋倉　文裕

個人情報保護法施行１年を経過！
迫りくる「中堅・中小企業に求められる内部統制への対応」

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９回セキュリティセミナー　個人情報保護法施行1年を経過！　迫りくる「中堅・中小企業に求められる内部統制への対応」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、財団法人ひょうご情報教育機構、NPO滋賀県情報基盤協会、NPOなら情報セキュリティ総合研究所、NPO情報セキュリティ研究所、NPO GIS総合研究所の後援のもと､7月21日（金）に大阪市にある大阪国際会議場において開催されました。当日は、あいにくの雨模様でしたが108名の方にご来場頂きました。
今回は「内部統制」をテーマとし、監査法人の立場から、また法曹界の立場から、およびJNSA研究員の立場からそれぞれご講演頂いたほか、フォレンジック調査を通じ、組織内部の情報セキュリティ事故発生時における現状と将来についてのご講演、および中小企業における個人情報保護対策WGから成果の報告がありました。本セミナーは、関西圏に多い中堅・中小企業にとって､「企業の内部統制強化」がどのように影響を及ぼすのか、また、その結果として、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ていくのかを明らかにすることとなりました。簡単に内容をご紹介します。

まずプログラムの最初に井上JNSA西日本支部長から､「関西圏に多い中堅・中小企業にとって､「企業の内部統制強化」がどのように影響を及ぼすのか、また、その結果として、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ていくのか、を明らかにすること」と本セミナーへの期待の挨拶があり、あわせてJNSA、各部会・WGの調査活動状況、および西日本支部の取り組みについても紹介がされました。

続いて最初の講演として、監査法人の立場から「財務報告に係る内部統制の評価と監査制度　IT部門におけるポイント」と題し、監査法人トーマツ パートナー 公認会計士 丸山満彦様からご講演を頂きました。丸山様からはまず、内部統制が注目されている背景と、いわゆるJ-SOXとはなにを指しているか、についてご説明を頂きました。さらに制度概要、内部統制の定義、重要なポイント、範囲、評価について説明を頂き、さらにIT統制の位置づけ、その概要についてご紹介して頂きました。その中で重要なポイントとして、自ら評価し管理体制に問題がないことを報告書にすること、また外部監査人はその報告書を監査し、結果の正しさのみならずプロセスも含めてその適正を保証することであり、結果適正ではないとの指摘がありました。これは今までの会社が経験したことがないことだという、説明がありました。さらに評価の対象は連結対象のみならず委託先にも及ぶことも指摘されています。これは、非上場の中小企業にとってもJ-SOXが他人事ではない、ということを指します。また最後にＩＴ部門への期待として、IT全般統制が信頼できると、IT業務処理統計のサンプル数が減少でき、評価コストも減少できる、との紹介がされました。本法律は平成20年4月1日以降に開始する事業年度から適用されることとなりますが、２年弱の間でやるべきことが本講演でいろいろ明確になり、中小企業にとってもこの期間に準備すべき方向が見えてきた、と期待されます。

イベント開催の報告

「監査法人トーマツ」丸山氏のご講演

2番目の講演は、「組織内部のフォレンジック調査における現状と将来」と題し、ネットエージェント株式会社 取締役の伊原秀明様からご講演を頂きました。フォレンジックは、まだ馴染みの薄い分野ではありますが、不正アクセスなどのハイテク犯罪に遭遇したときに必要な行動について、貴重な指摘、紹介を頂きました。その中で、情報システム部門の担当者がどこを調べれば良いかが判らないにも拘らず、いろいろ手探りで調査を行ってしまい、かえって証拠が残らなくなってしまうことがあるということの指摘がありました。必要な行動としては、まず現状保全する、ということでした。また、被害が発生しているにも拘らず業務に重要なサーバのため停止できない、という理由により稼動し続けるサーバが多い、との指摘がありました。これは、被害にあっているにも関わらずサーバを稼動し続け、より被害を拡大する、例えば個人情報などの重要情報の漏洩が拡大する危険性よりも、目の前の自分たちの業務を優先している、ということの指摘でした。伊原様からは、事故の発生を前提とし、発生時における体制の構築、および被害にあっているにも拘らずサーバを稼動し続け被害を拡大するような誤った判断を防ぐ体制や教育が必要、との貴重な提言を頂きました。また、常日頃から事故発生直後から調査に着手可能な体制、連絡先の確保も重要、との指摘も頂きました。内部統制の運用、事業継続という観点からもフォレンジックを通して見えてきたこれらの課題への対応の重要性を強く感じることができた内容でした。

3番目の講演は昼休み後の最初の講演で、法曹界の立場から「中堅・中小企業の個人情報保護・情報セキュリティと内部統制」と題し、稲垣隆一法律事務所 弁護士　稲垣隆一 様からご講演を頂きました。

講演の冒頭から稲垣先生の「真剣に考えていますか？」、「今日、何人の経営者のかたがこのセミナーに参加されていますか？」という厳しく、また非常に印象的なご発言がありました。本講演では、過去の情報漏洩事件を例にそれぞれの本質的な問題について掘り下げてご説明を頂きました。そのなかで稲垣先生が一番言いたかったものとして感じられたのが、冒頭にもあった「真剣に考えているのか」ということでした。例えば、宇治市の個人情報漏洩事件における委託先から個人情報が漏洩した原因のひとつに、再委託・再々委託における誤った判断を指摘されています。情報漏洩が発生する過程における誤った判断をした人の存在、その人はなぜそのような判断をくだしたのか、それ以前に判断を任せるに足る人材だったのか、セキュリティ教育を十分にうけ理解をしている人であったのか、ヒューマンエラーの要因を為す人間の不安定行動にまで言及されました。情報セキュリティ対策を考えるうえで、どこまで「真剣に考えているのか」という問題の貴重な事例でした。さらに、中小企業が抱える現在の情報セキュリティ対策の課題についても触れて戴きました。中小企業の情報セキュリティ対策は、まだまだ脆弱であり、経営者にとって情報セキュリティや個人情報保護が経営課題になっていません。そのような中小企業はまず、自らの力で対策を構築する組織体制、実現可能なスケジュールをたて、そのための体制、業務の振り分けを行うこと、経営課題とするために基本方針の確認、リスクの把握の必要性、などを明確化する必要がある、との提案を戴きました。

「稲垣隆一法律事務所」弁護士 稲垣先生のご講演

続いて､「内部統制とセキュリティのルール」と題し、日本ネットワークセキュリティ協会 研究員・独立行政法人情報処理推進機構 研究員の園田道夫様からご講演を頂きました。情報セキュリティは、ISMS、15408、個人情報保護、Ｐマークといろいろ対応してきたなかで、今度は内部統制が法制化されるということになったが、いったい何をどうして、どう棲み分け使い分けたらいいのか、そもそも棲み分けなければならないのか、などについて説明を頂きました。J-SOXの目的は会計上の不正行為の防止、翻れば正しいことの証明であり、不正行為を防ぐには単独処理をなくす、相互チェックの仕組みが大前提になる､という解説がありました。不正行為の検出には、ISMSやＰマークの管理項目としての従来から実施している対策のアクセスコントロールやログの取得を行うことであり、大きく変わることではない、ということの説明がありました。そして、会計における不正行為は、一従業員の行為よりむしろ経営層の行為であることから、これまでの情報セキュリティ対策として行われきた従業員の行動の監視、監査ではなく経営者の行動の監視、監査が必要、という指摘がありました。

最後に、中小企業向け個人情報保護対策WGから「個人情報保護法から1年、中小企業の対策と実情」と題し、ＷＧリーダー・伊藤忠テクノサイエンス株式会社　市川 順之様から講演を戴きました。個人情報保護法が施行されてから、この一年の状況についての説明と、昨年10月のJNSA西日本支部主催セミナーNSF in Osakaで来場者の皆さんに回答して頂いた個人情報保護に関するアンケート結果の報告、WGの活動を通してみえてきた中小企業の問題についての説明がありました。さらに、成果物としてのヒアリングシートの紹介が行われるとともに、本講演では来場者の方とのディスカッションの時間を設けました。大きな会場で、公の場での発言される来場者のかたは少なかったのですが、その中で「経営者の理解の乏しさ」という訴えがありました。稲垣先生のご講演にもありましたが、経営者にとって情報セキュリティが経営課題になっていない現実を垣間見ました。最後に井上ＪＮＳＡ西日本支部長からは、今回のようなセミナーに加えて、来場者を経営者に絞ってのインターアクティブな小セミナーも開催して見たいとの提案もさせて戴きました。

おわりに

非上場の中小企業にとってもJ-SOXは無関係ではなく取引企業の上場企業から同等なことは求められるという現実を認識したセミナーだったのではないか、と思います。J-SOXが適用される平成20年４月１日以降に開始する事業年度までには、まだ一年半ほどの時間がありますが、中小企業にとってこの期間はJ-SOXへの対応を検討、実施する貴重な時間であり、けっして余裕のある時間ではない、と感じました。また、これまでは情報セキュリティが経営課題として取り上げ難い現状にありましたが、今後は中小企業においてもJ-SOX対応に取り組む上で健全な情報セキュリティ対策こそが必須不可欠なものとして認識されるのでは、という期待を抱くことのできたセミナーになった、と感じました。