第１０２回月例研究会報告

ＮＯ．５６２　森本　哲也

日　時：平成１６年1月１５日（木）１８：３０～２０：２０
場　所：中央大学駿河台記念館６１０号室
講　師：(株）損害保険ジャパン　事務・IT 企画部　リスク管理グループリーダー　飯田　憲　氏
演　題：損保ジャパンにおける情報セキュリティ監査の取組み
参加者：７６人（理事１１人を含む）

情報セキュリティ監査制度施行後の初事例となる外部監査を受けられた（株）損害保険ジャパンの事務・ＩＴ企画部　リスク管理グループリーダー飯田氏に監査受診の概要を講演いただいた。
（株）損害保険ジャパンは、旧安田火災、旧日産火災、旧大成火災、旧第一ライフ損保が経営統合し、平成１４年７月に誕生した損害保険会社である。また、事務・ＩＴ企画部は、今回の外部監査の事務局を担当された。

Ⅰ．情報セキュリティ監査導入の背景

１．　損害保険と個人情報

１）　当社は、１，４００万人の顧客分と多数の個人情報を保有している。
２）個人情報保護法の成立は、管理の焦点を個人情報の中の機密部分、取扱い注意部分だけの管理の是非から、個人を識別する情報自体の管理へ移したとの認識がある。

２．　情報セキュリティを巡る問題意識

１）　損保では、紙ベースの上記情報は従来から扱ってきている。従来と違うのは、ＩＴ時代に入り、大量の個人情報が電磁データ化されている点である。
２）　扱いを誤って、個人情報が外部に流出した場合、企業が負担する損害は軽く数億円に達してしまう可能性がある。
３）　ミスによる漏洩は限りなくゼロにする。故意による漏洩は完全に防ぐことは困難であるが、機会を減少させることは可能である。
４）　自社の仕組みはどうか。第三者の眼で客観的にチェックする手だてはないか。それも押しつけられてからではなく自発的に、と考えていた。

３．　当社の監査（検査）体制

１）当社の監査（検査）は、コンプライアンス検査、内部監査、外部監査より成る。
２）コンプライアンス検査では、業務管理室が営業店の法令遵守状況をチェックする。
３）内部監査では、業務監査部が本社各部門と保険金支払い部門の業務実施状況を検証する。
４）外部監査では、公認会計士による会計監査の関連で、財務諸表作成システムの数字の連続性等を検証する。

４．　当社におけるシステムの外部監査

１）基本的に毎年度１回、システムの外部監査を受けている。
２）平成１５年度の監査テーマ選定に当たっては、個人情報保護法成立の動向を見て、情報セキュリティを大きなテーマとした。

Ⅱ．情報セキュリティ監査の実際

５．　監査分野の設定

１）　情報セキュリティ監査制度では、対象組織の監査分野の設定は任意としている。
２）　一方、ＩＳＭＳでは管理基準は情報セキュリティと同じだが、監査分野を選択することは不可で、全分野（１３１の管理策に区分）に亘って審査を受けねばならない。
３）　当社では、次の４点を「監査分野」と設定した。
①情報セキュリティ管理の組織体制
②業務継続に関する緊急時対応体制
③個人情報保護法に対する準備状況
④外部委託業務のセキュリティ管理状況

６．　情報セキュリティ管理基準（例）

１）外部委託に関して、前述の両制度を見ると以下になる。結論として、両者は項番の振り方が異なるだけで、殆ど同じである。

２）情報セキュリティ管理基準において、２．３．１のような３桁部をコントロールと称し、２．３．１．１のような４桁部をサブコントロールと称す。

３）情報セキュリティ管理基準と情報セキュリティ監査基準との違いは、前者が監査人が監査を行う際の判断尺度であるのに対し、後者は監査人の行為規範である相違。

７．　適用する管理基準の選定

監査分野に応じて、適用する管理基準の項目（コントロール、サブコントロール、および情報セキュリティ管理基準以外の基準等）を選定するステップであるが、監査人がドラフトを作り、当社でそれをレビューする方法を採った。実施例を見ると以下である。

１．１　セキュリティ基本方針には、コントロールのみ使用

２．１　情報セキュリティ基盤には、サブコントロールを含めて使用

２．２　第三者によるアクセスのセキュリティには、サブコントロールを含めて使用

２．３　外部委託には、コントロール、サブコントロールの他、（財）金融情報システムセンター（FISC）「金融機関等コンピュータシステムの安全基準」のいくつかの基準を追加

上記の基準を元に、具体的に何をチェックするかが、外部監査人のノウハウである。

８．　監査スケジュール

１）契約締結と報道機関へのニュースリリースを平成１５年６月２日

２）事前準備（計画フェーズ）が６月６日～６月２４日　監査方法を①資料閲覧、と②インタビューと決めた。

３）監査キックオフを７月１日

４）非監査部門のヒヤリングを７月１日～７月１７日　２７回の計画されたヒヤリングと４回の追加ヒヤリングと、合計３１回のヒヤリングを行った。

５）まとめ（報告フェーズ）を７月３１日～１０月９日　監査報告会は１０月９日に行った。報告会は当初９月上旬であったが、１ヶ月延びた。

９．　閲覧資料の選定

適用する管理基準の項目毎に、監査人が事前閲覧すべき資料を選定するステップである。以下の順で行った。

１）監査人から必要資料の一覧表を提出してもらう。

２）監査人と当社で打合わせをし、最も相応しい資料に特定する。最終的に提出した資料は１４種であった。この中には、インタビュー後に追加提出したものもある。

１０．インタビュー内容・スケジュールの決定

１）監査人がインタビュー対象部門とインタビュー内容を作成するが、以下の観点から事務局と摺り合わせる。

①対象部門は適正か。監査人は、前もって渡してある組織図等の部署の名称から判断して、ドラフトを作成するが、誤解を招いているケースが多い。これを調整して最適なインタビュー対象部門とする。

②インタビュー内容は確か。監査人は外部の人なので、社内の人と意志の疎通を欠くことがある。事務局が監査人の質問内容を社内の人に分かるよう翻訳する。

③インタビューを受ける部門の回答者を決める。決定には事務局の人脈をフル活用。

④インタビューの内容確認、回答者の決定、それを踏まえてのスケジュール調整は非常に手間がかかる。最大の課題は会議室の確保であった。

Ⅲ．情報セキュリティ監査の総括

１１．事務局の役割

１）情報セキュリティ監査における事務局は、社内に強制権限を持たないので、資料の提出、役

職員との面談等を協力依頼するのみ。幸い拒まれることはなかった。
2）社内的なやりとりを全て取り仕切る。
3）監査報告書のドラフトが提出された後でヒヤリング先と事実確認をするが、この作業に時間がかかった。このことが、監査報告が遅れた理由である。今後は、工程管理の対象とすべき。

１２．監査に対する社内の受け止め方

どこかに漏れがあるはずだ。だから外部の目で見て貰おうとの基本的考え方で始めた。その考えはかなり理解されたが、問題意識の程度により監査に対する温度差が生じている。事実、監査→不備（要改善）事項の指摘→個人的不名誉という感覚は根強い。

１３．他の監査との相違点

他の監査、社内監査および公認会計士監査と比較すると、情報セキュリティ監査は以下の相違点がある。講師の個人的解釈は、外部監査人に委託した自主チェックあり、実施に当たっては監査と云う言葉を使わないようにしたとのことである。

	社内監査	公認会計士監査	情報ｾｷｭﾘﾃｨ監査（今回のもの）
監査の種類	内部監査	外部監査	外部監査
担当部署	業務監査部	経理部	事務・IT 企画部
監査のタイプ	助言型	保証型	助言型
法令の根拠	なし	商法・証取法	なし
社内強制権限	あり	あり	なし
監査の周期	原則毎年	決算期（四半期）	任意

１４．情報セキュリティ監査の効用

1）　要改善項目の客観性
2）　関連部門の連携強化
①個人情報保護対応の関連各部と、今後の対応がスムーズに行くようになった。
②事務・IT 企画部内で旧の２組織が協業したことにより、内部の連携が上手く行くようになった。

１５．おわりに

1）現場の重要性

情報セキュリティを守るのは、情報資産を扱う現場の動きである。現場で自律的に情報セキュリティを推進する仕掛けが必要である。例としてポスター掲示による啓蒙活動。

2）何のために個人情報を守るのか？

従来の、漏れたら企業の信用を失墜するから、今後はそれにプラスして、「企業防衛のため」という視点が必要である。もし事態が発生すれば、億単位の金がかかることを認識する。

＜質疑応答＞

Q1:被監査部門から感謝されたことはあるか。
A1:お礼を言われたことはない。ただ、事務局として、各部門との今後取り組むべき課題が明らかになったことは、受診部門にとっても受診のメリットであると認識。

Q2:従来から個人情報の取り扱いの重要性は云われてきた。今回個人情報保護法が制定されて何が変わったのか。
A2:従来は、情報自体が機密であるとか、プライバシーであると認識されていたが、同法制定後は、個人情報の扱い方如何により法令違反となることを明確に意識。

Q3:マネジメントシステムに係わる点、特に経営者に関することは何か。
A3:個人情報の扱いに、経営者のコミットメントがいかに反映されているかがチェックされる。

Q4:個人情報と云う中で、法人と自然人との扱いを分けているか。

A4:個人情報保護法では自然人を意識しているが当社では分けていない。顧客情報として同じ扱い。

Q5:受診に対する満足度は。
A5:満足している。受診に当たり、当社の管理は万全ではない、管理レベルを知りたいから受けるとの認識があった。指摘された事項は予想されたものであったが、外部の意見として客観性のあるものとなり、社内への説得力が向上した。

Q6:改善提案は納得できるものであったか。
A6:改善の方向性は示されたが、具体的な改善提案までは受けていない。各論で改善を考えるのは自分たちの役割と認識。

Q7:監査人がこうしてくれていれば、もっとやり易かったと云う点はないか。
A7:やりにくかったことはなかった。外部の監査人の限界は初めから覚悟していた。

Q8:監査人を選択した基準は。
A8:従来から知っているところで、信頼できるところ。結果として会計監査法人とは別法人となった。

Q9:業務継続に関する緊急時対応体制を選んだ理由。
A9:情報セキュリティ監査基準に含まれている。また緊急時にどうやって情報資産を守るかをチェックするため。

Q10:個人情報保護法の細則がない状況下で監査を受けたとのことであるが、細則の予測をどのように行ったのか。
A10:特に深い読みはない。個人情報の扱いにおいて準備する点を考えると以下になる。即ち、開示、訂正要求の扱い、どこにどのような個人情報があるかの掌握、等々。

Q11:ISMS,プライバシーマークへの認識は。
A11:存在を知っているとの認識レベルである。会社として認証を取得するかどうかは、今後検討することになる。

＜感想＞

何事も一番にやるということは、リスクもあるが大きな成果が期待できるものです。今回の情報セキュリティ監査制度の成立を、社内体制のチェックに巧みに利用された飯田氏の戦略性の高さにまず敬服いたしました。これは、日頃から問題意識を持たれていて、それをいかに実行に移すかを常日頃から考えておられる証と感じます。監査ですから、当然社内には抵抗勢力があるでしょう。しかしながら、本邦一番、業界一番との誘因は多大であったことと思います。その誘因を梃子に上手くことを進めたのが、今回の監査を成功させた鍵と思います。

業界の然るべき立場の方がこのように、情報資産の扱いに高い見識を持っておられることは、一保険契約者として安心すると共に、日本企業の健全性に希望を持ちました。

また、事務局しての苦労話は、同種の経験を持つ者には納得を覚えさせ、未経験の者には大いに先行指標となるものでありました。

貴重な体験を披露いただいたことに深く謝意を表します。ありがとうございました。