第ニ回 IT マネジメント研究会 初心者編（東京） 議事録	
日時：	**2010/11/18（木）15:00～17:30**
会場：	**クオリティ(株) 本社 6F 会議室**
テーマ：	**我々は情報リスクにどう立ち向かうべきか**
講師：	**橋本 純生 様** **日本セキュリティマネジメント学会理事**
司会・進行：	**IT マネジメント研究会 初心者編 座長** **月島食品工業株式会社　総務部 情報システム室 室長代理　吉原 徹 氏** **IT マネジメント研究会 初心者編 副座長** **株式会社リコー　IT/S 本部 IT/S 技術センター サーバーグループ リーダー** **中俣 幸二 氏**

※当研究会の運営方針により、個人/会社名を特定できる発言、および発表者から公開の許可を得られなかった内容は 議事録より削除されています。あらかじめご了承ください。

今回は情報セキュリティをテーマに、参加者の方々から、課題に対する相談や自社で行っている対策法など、活発な意見交換が行われました。

◆”情報”リスクをテーマにした理由について

【講師から】

セキュリティとは何を守るかが一番重要となる。講師依頼が来たときは、ネットワークセキュリティや C.I.A を中心に話をしようかと考えていた。しかし、振り返ってみると、情報をハンドリングするリスク、情報に振り回されるリスクのほうが、はるかに怖いものなのではないかと考えた。情報を鵜呑みにするのは恐ろしいこと。自分で考えて再構築しなければならない。

【副座長から】

今回の情報リスクをテーマにしたきっかけについて。PCNW のミーティングの際、セキュリティやハードウェア、ソフトウェアに関する焦点を絞った話はよく耳にするが、ウイルス対策や PC 管理、ドキュメント管理など細かな部分ではなく、その上の全体を捉えた話はあまり聞かないという話題になった。本来は全体を理解してから細かい部分のセキュリティ対策をするのではないか、というところから今回のテーマが決まった。なかなか、そういった話を聞く機会はなく、開催することになった。

◆参加者からの質問

Q:自社は情報漏えいに関するリスクを被害総額に変えてしまう傾向にある、皆さんの会社ではどうか？

A(参加者）:情報が漏れた場合の被害総額によって重要度がランク付けしている。

Q(講師):セキュリティ対策に投資をする場合、その被害総額から対策コストを考えるのはよいこと。しかし、担当部署が所有する情報の価値がないと判断された場合、現場のモチベーションをどう維持するのか？　あれも重要、これも重要と被害総額では測れないという評価になると、会社のすべての情報を守ることになってしまい、セキュリティが維持できない。ほかにコストとリスクを紐付けているケースはあるか？

A(参加者)：私の会社では、情報とシステムでリスクの考え方を分けている。システムが停止した場合の損害は、その担当者の決済権で重要度を決める。情報が漏洩した場合は、会社や個人への被害度によってランク付けしている。当然、個人情報が最もリスクが高いと設定している。

Q(参加者)：メール誤送信の対策について、実施されていますか？　セキュリティレベルとコストのバランスについて、重大な事故は起きていないが、誤送信はなくならない。自社では誤送信した場合の報告と、誤送信対策ソフトを導入している。

A(参加者)：

- システム的には添付ファイルは全て暗号化している。社内規定として外部に送信する場合は、CC や BCC を必ず入れる。ツールによって 5 分間メールは送信されない。
- ノーツでメール誤送信対策を行っている。送信する前に宛先がポップアップ表示される。添付ファイルの場合は、暗号化等の警告が表示される。
- Groupmax を使っている。CC に部長以上を入れないと送信できない仕組み。とどメールという、送信バッファーを設定できるツールがある。
- 同じようなメール誤送信対策ソフトを使っている。バッファーを何分にするのかでアンケートをとった。5 分間の設定にしているが、送った瞬間に気づかなければ、10 分後はもう忘れている。誤送信対策では、送信されないストレスよりも、添付ファイルを暗号化する処理のほうがクレームが多い。
- WEB 上でドキュメントを閲覧、パスワードをメールで送るシステムを使っている。しかしお客様は添付ファイルのほうが便利なので、添付ファイルも使っている。暗号化した添付ファイルのパスワードもメールで送るのでセキュリティが甘くなってしまう。

Q(講師)：誤送信の反対に、なりすましメールに対する対策はされているか？　昔はウイルスによるなりすましメールが流行した。ウイルス送信元が自社名になっていて、よくクレームが会社に届いた。電子署名は良い対策だが、コストがかかる。ところで、メールのフッターに「メールの複製・転載禁止」の説明文を挿入している会社はありますか？ メール誤送信からの二次災害を防ぐための対策だと思われるが。

A（参加者）：

- 「送信者だけに送ることを意図しています」といったものをいれている。
- 「受信者本人ではない場合破棄してくださいという」文面を海外からのメールで多く見かける。

Q(参加者)：情報セキュリティポリシ等の策定はしっかりやっているが、運用にコストがかかるので社員のPCにアドミン権限を持たせている。アドミン権限を持たせている会社はありますか？

A(参加者)：

- 毎回、利便性と運用コスト、リスクの観点で議論になるが、自社もアドミン権限を与えています。
- 業務アプリケーションでアドミン権限でなければ動作しないものがあるため、アドミン権限を与えています。
- ユーザー権限で行っています。アドミン権限がある場合のリスクについて議論したわけではないが、システムのリテラシーが高くなく、設定を自分で変更させないために行っている。操作を間違っておかしくなる方が多いので、統制で対応したほうがメリット。
- セキュリティについて、アドミン権限で自由にソフトをインストールできるようになるが、Winny などはファイヤーウォールでアプリケーションを禁止できるので、ネットワーク監視を充実させたほうがセキュリティ上は効果があり、運用性も高いと思う。
- フリーソフトのインストールについてはどうか？　無料で便利になるが、業務システムとぶつかってシステムが壊れて修理対応というリスクがある。

Q(参加者)：セキュリティリスクを経営陣にどう説得するか？セキュリティリスクをシステム側で説明しても理解出来ないということでNGになる。経営陣が納得しそうなキーワードはないか？

A(参加者)：

- 業務優先と言われると、対応してしまう。経営陣は漏洩の仕方がわからない。
- 仕事が取れなくても首にはならないが、個人情報が漏れたら社長が首になる可能性を上司に訴える。
- 社内/社外で起きた情報セキュリティ事故の事例を社内告知する。名前は伏せるが具体的に紹介することで事例を学ぶ。
- 大きな企業では委託先に情報セキュリティ教育のビデオ等を配布している。

◆参加者の感想

- マネジメント層のリテラシーと現場のギャップについて、システムにかかわらない関係者に対するセキュリティのリテラシーについて。1 年前に警告をしていたがウイルス感染被害が起きた。起こってからの対応になってしまった。セキュリティに対する誤解を解いていかなければ、根本的な解決にならないと感じた。
- セキュリティと輸出管理を一元管理している。輸出の場合、相手国によって輸出許可の決済が変わる。アメリカやドイツなどのホワイト国は部長レベルでいいが、イランやイラク等はとても厳しくなる。輸出管理とセキュリティ管理は大枠では同じような考えの元にできる。