第 112 回　月例研究会報告

1. タイトル

講演テーマ：「システム監査で押さえておくべき情報セキュリティ技術のポイント」
講　師：エヌ・ティ・ティコムウエア株式会社　木村　歳修　氏
会　場：中央大学　駿河台記念館 280 号会議室

報告者　No. 851　大野　勇進

2. はじめに

今回の講師、NTT コムウェア㈱セキュリティコンサルタント木村歳修（きむらとしなが）氏は、ISMS 審査員、IT コーディネータ、システム監査技術者／プロジェクトマネージャ／情報セキュリティアドミニストレータ情報処理技術者、MCP、BS7799 Specialist 等の資格を保有しておられ、現在、情報セキュリティポリシー策定支援、ISMS 認証取得支援をはじめ、個人情報保護関連のセキュリティコンサルタントを中心に、ISMS 審査員、セミナー講師としても活動中です。

本日は、最新情報セキュリティ技術のポイントを解説していただき、知識の整理とポイントを習得できると期待しているという紹介で、講演が始まりました。

3. 講演概要

3.1. アジェンダ

下記のアジェンダにそって、まずは、最新技術動向を説明し、次に本日のメインテーマを説明しますということで、解説をいただきました。

【アジェンダ】

Ⅰ．最新の情報セキュリティ技術の動向
　１．安全管理措置のポイント（個人情報保護法 20 条）
　２．最新ウイルス・ハッカー対策
　３．生体認証
　４．暗号化
　５．e-文書法
　６．IC タグのセキュリティ
　７．IP 電話のセキュリティ

Ⅱ．情報セキュリティ技術の組合せや選択のポイント

Ⅲ．情報セキュリティ技術に対する監査のポイント

3.2. 最新の情報セキュリティ技術の動向

システム監査と情報セキュリティ監査は目的が違うので並立できます。

・システム監査
　情報システム構築・運用の全体最適化の観点からの監査
・情報セキュリティ監査
　情報セキュリティ確保の観点からの監査

本日は情報セキュリティ管理基準にそった情報セキュリティ技術の説明が主になります。

情報セキュリティ規格・基準の説明があり、特に ISMS 認証基準 2003 の構成を説明いただきました。

3.2.1. 安全管理措置のポイント（個人情報保護法 20 条）

事業者は、個人情報保護法第 20 条安全管理措置により、リスクに応じた、必要かつ適切な措置を講じなければならない。

事業者を所管する各省庁において、審議会の議論等を経て、20 分野について 30 のガイドラインが策定され事業者はそれぞれの所轄省庁のガイドラインを精査し実施することが必要です。

安全管理措置のポイントは①組織的安全管理措置②人的安全管理措置③技術的安全管理措置④物理的安全管理措置の、以上４分野にわたってバランスよく情報セキュリティ対策を実施することです。

最近の事例に見るように個人情報はお金になると認識され、顧客情報の漏洩が今後も危惧されます。

情報漏洩の主原因は、①アクセス管理が不十分②データの持ち出し手段の制限措置が不十分の２点が考えられます、この２点を事前にチェックすることがリスクマネジメントです。こうしたセキュリティ事件からの教訓として、下記の 3 点がいえます。

教訓１：あらゆる業種で流出事件が多発
　　明日は我が身
教訓２：経営者の意識の甘さ
　　顧客拡大戦略で顧客保護意識が薄れた
　　痛い目に合わないとわからない
　　リスクマネジメントの欠如
教訓３：性悪説で対策を打つ必要がある

3.2.2. 最新ウイルス・ハッカー対策

ホームページ改ざん、情報漏えい、データ破壊、消去、サービス妨害（DOS）、迷惑メール中継、フィッシング詐欺のような多発する情報セキュリティ事件・事故による有形無形の損失が発生しています。

事業者が情報漏えいした場合の影響は、

・ 情報資産の損失
ハードの復旧、ソフトの修復、データの再作成費用、再発防止のためのセキュリティ改善費用等が発生します。

・ 社会的信用の失墜
賠償損害、慰謝料、謝罪広告費用、顧客離れ、株価暴落が考えられます。

また、米企業が懸念する IT セキュリティの脅威は下記の通り。
（参考）ウイルスおよびワーム
外部からのハッキングまたはクラッキング
身分詐称およびフィッシング
スパイウエア
サービス拒否（DoS）攻撃
スパム
無線／モバイル・デバイスのウイルス
内部者による攻撃
未公表の脆弱性を突くゼロ・デイ・アタック
ソーシャル・エンジニアリング
サイバー攻撃

これらの脅威に対する対策を事前に打っておくことが重要です、それでもさまざまなリスクが残っていますたとえば未知のウイルス対策、Bot にも注意が必要です。

3.2.3. 生体認証

さて、そんな脅威の中、認証技術が重要性を増しています。
認証技術は下記の場面で必要です。

１．ネットワークノードの認証（対向の IP-VPN 装置の認証等）
２．業務アプリアプリケーション利用時の認証（グループウェア、勤怠管理ソフトウェア等）
３．ファイルサーバ等のフォルダ・ファイル単位でのアクセス制御
４．利用者の識別及び認証（端末認証、ドメイン認証等）

本人認証の種類は記憶（パスワード）、持ち物（専用カード）、生体認証（指紋、虹彩、声紋、静脈等）がありますが、最近生体認証が注目されています。
生体認証も万全ではありません、他の認証技術との複合化が重要です。

3.2.4. 暗号化

暗号化技術の利用局面は、通信経路の暗号化、記憶媒体の暗号化がありますが、暗号化ツールには、いろいろ問題点があり使ってみなければわからない点があるので、全社導入の前にチェックが必要です。

3.2.5. e-文書法

「個人情報保護法」と同じく H17.4.1 に施行された e- 文書法とは、簡単に言えば「紙以外での保存は認めない」と規定している多くの法令を、「スキャナで読み取った電子文書も条件つきで原本としていいですよ」という法令に一括改正してくれる法令です。
注目点は下記のとおりです。
・ 保管コストの削減効果は経済界全体で年間約 3,000 億円です。
・ 電子文書は「カラー文書はカラーで、モノクロ文書はモノクロで」が原則です。
・ 電子署名やタイムスタンプ等が技術要件として求められます。
・ 具体的な技術要件は、これから法令毎に決められることになるため、事業者の本格的な対応は H18 年度以降になりそうです。

3.2.6. IC タグのセキュリティ

IC タグとは大きさが 1 ミリ角以下というゴマ粒大の IC（集積回路）チップに ID を記録し、無線電波で読み出しを行う小さなタグ（荷札）で下記のような特徴があります。
・ バーコードが数十桁に対して、IC タグは数千けたの情報を保存できます。
・ 小さな取り付けスペースがあれば容易に導入でき、複製・偽造が困難で、書き換えができます。
・ IC タグが付けられた複数の対象物の情報を一括読み取りできます。
・ 電波で交信するために汚れ・ほこり等の影響を最小限に抑えることができます。
・ アンテナ側からの非接触電力伝送で動作するため電源が不要です。

また、今後の利用が期待される分野は、①医薬品や患者に IC タグを付けて安全を管理する医療・薬品分野、②産地や賞味期限、流通経路等を IC タグに記録し、トレーサビリティを実現する食品分野、②在庫管理の分野等です。
但し、技術の問題もあります。

(1) どの無線電波を使うか？
・ 使う電波によって届く距離が違う
・ 無線 LAN のセキュリティ対策
Wi-Fi Protected Access (WPA) 方式
暗号化技術 Wired Equivalent Privacy (WEP)
Extensible Authentication Protocol (EAP) 等

(2) IC タグの低コスト化の問題
バーコードコスト：2 円
vs ＩＣタグコスト：100 円

(3) プライバシーの問題
自分の個人情報が自分でコントロールできない恐れがある。
購入した品物に取り付けられていた IC タグが、気づかないうちにさまざまな場所で読み取られ、個人の行動が追跡されてしまう恐れがある。
リアルタイムで存在がわかる。
⇒個人監視やストーカーに使われたら・・・・心配？

上記の問題を認識しながら活用することが必要であるが、今後活用が期待され、また確実に普及していくでありましょう。

3.2.7. IP 電話のセキュリティ

IP 電話とは電話をかける相手との間の通信経路を、インターネットで使用されている IP プロトコルベースで構築した電話ネットワークのこと。
1 つの回線を多数の会話で併用できるなどの点で従来の電話よりも回線の使用効率がよく、その分従来の電話よりも低いコストで利用できる。
IP 電話と一口で言っても、IP 化する場所によって様々な種類があります。
・ 通信事業者内のネットワーク、インターネット経由等
・ 電話機、IP 電話機、パソコン（IP テレビ電話）等
但し IP 電話のセキュリティは基本的にパソコンと同じ、脅威としては、DoS 攻撃、不正利用、盗聴等です。
LAN ポートに「パケット・キャプチャ・ソフト」をインストールしたパソコンを接続することで盗聴される恐れがあります。
無線 IP 電話も盗聴に弱く、IP 電話にもセキュリティ・ホールがあるので、セキュリティパッチを適用する必要があるが、対応が不十分になっています。
DoS 攻撃を受けるとほとんどの IP 電話サーバがダウンします。
セキュリティパッチは、手作業で一台一台対応しなければいけないケースが多いが
“Windows Update”のようにネットワーク経由でセキュリティパッチをダウンロードできる機器もあります。

3.3. 情報セキュリティ技術の組合せや選択のポイント

多くの企業や組織では、事業を行うに当たって情報システムが広範に用いられ、組織の戦略や目的達成に大きく関わっています。
そのため、組織の経営戦略と IT 戦略を整合させ、IT 投資を適切に管理し、IT 要員やその体制、IT に関するリスクのコントロールなどフレームワークを確立すること、すなわち「IT ガバナンス」「セキュリティガバナンス」が極めて重要となってきています。

3.3.1. リスクアセスメントに基づく対策

脅威と脆弱性が結びつくと、リスクが顕在化し、情報資産に損失が発生する、この点を注意しバランスの取れたセキュリティ対策を行うことが重要です。
「脅威の例」
不法侵入による盗難、破壊
不正アクセスよる情報漏えい、改ざん、破壊
内部関係者による不正参照、不正持出、紛失
災害（地震、火災、水害、風害、停電等）
不正ソフト、ウイルスによるデータの改ざん・消去
機器故障、操作ミスによるデータ等の消失
「脆弱性の例」
物理的、技術的な弱点
セキュリティ対策が未実施又は不十分
社員等の意識やモラルが低い

セキュリティ対策機能とは、抑止、防止、検知、回復の 4 種類をいう、リスクアセスメントに基づく対策としてはこれらをバランスよくおこなうことです。
●「抑止」人に対して、故意によるセキュリティ犯罪や違反を思い止まらせる等、脅威が発生する可能性を低減することを主目的として法令や組織内ルールの整備を行う。
具体例→不正アクセス禁止法による罰則、組織内の懲戒手続による懲戒処分
●「防止」脅威が顕在化した場合に被害の発生を未然に防ぎ、被害拡大を防止することを主目的として予め対策を行う。
具体例→ファイアウォール、ウイルス対策ソフト、ユーザ認証、ファイル・ネットワーク経路の暗号化、役職員、システム管理者の教育・訓練等
●「検知」脅威が実際に発生した場合にその発生を迅速に発見し、脅威に対してすばやく対応を可能とすることを主目的として予め対策を行う。
具体例→システムのアラーム監視、ログ解析、侵入検知システム(IDS) の導入等
●「回復」脅威の顕在化により発生した被害を正常状態に復元することを主目的として対策を行う。
具体例→事業継続計画、証拠となるログの管理、バックアップツールの導入等

3.3.2. 情報セキュリティ管理の成熟度

組織の ISMS の成熟度とは下記の 5 段階と定義している

0. 情報セキュリティポリシーが作成されていない
1. ポリシーはあるが、実行されていない
2. ポリシーを策定し、行動を起こしている
3. 全体のマネジメントサイクルが回っている
4. 見直しが定期的に行われている
5. 全てのサイクルが有機的に結合している

3.3.3. 情報セキュリティ実施の重要成功要因

下記が重要である。

1. 事業目的を反映したセキュリティ基本方針、目的、活動
2. 組織文化に合ったセキュリティの実施方法
3. 目に見える形での経営陣の支持及び責任
4. セキュリティ要求事項、リスクアセスメント及びリスクマネジメントの十分な理解
5. 管理者・従業員に対するセキュリティの効果的な普及
6. 全従業員・請負業者への情報セキュリティ手引の配布
7. 適切な教育及び訓練の実施
8. ISMS の実施状況評価、改善提言のフィードバック

情報セキュリティ管理の成熟度により要求されるセキュリティレベルが違うので、人的対策、技術的対策、物理的対策、組織的対策を実施し、序々にレベルを高度化していくサイクルを実現することが重要です。

3.4. 情報セキュリティ技術に対する監査のポイント

監査のポイントは下記のとおりです。

・企業の成熟度に見合った指摘をする。
・情報セキュリティマネジメントシステム（管理のしくみ）が有効かつ効率的に機能しているかという視点が必要です。
　→個別最適より全体最適
・情報セキュリティ技術の監査する側にも IT ＋セキュリティの知識がなければ指摘ができない。
　→ IT の知識が無い場合、被監査部門の人に操作してもらい、必要な監査証跡を見せてもらう。
・その他の法令・制度等の知識も必要！
　IT コーディネータのフレームワークとシステム監査のフレームワークの違い、ISMS プロセスにおける PDCA モデル、個人情報保護法とプライバシーマークの違い、プライバシーマークと ISMS の違いのポイントを知ることも重要です。

4. 感想

短時間のセミナーにこれだけの内容を解説していただきありがとうございました。

短時間であったので、表面的な内容になってしまったのが残念でありましたが、情報セキュリティ技術の整理になり、知識の確認ができました。

資料の不備があり質問もその点の確認にとどまったのも残念でした。

主題の情報セキュリティ技術に対する監査のポイントだけについて、もう一度解説していただきたいと感じました。

今後も技術面での進歩は急速に起こると考えられますので、常に技術面の理解を監査に反映する努力が求められ、監査人としてのスキルアップの必要性を感じた研究会でありました。

以上