6R－08　情報セキュリティポリシーの実践的な作り方

坂巻　修
あさひ銀総合システム　株式会社

1.研究の背景と目的

本格的なオープンネットワーク時代を迎え、利便性が急速に高まる反面、情報の漏洩、改ざん、破壊といったリスクも急増している。また、EC など企業間電子商取引の広まりにより、欧米企業から情報セキュリティポリシーの保持を求められるケースもあり、全社的な情報セキュリティポリシーが企業にとって必要不可欠であることは明らかである。

富士通ユーザ研究会であるリーディングエッジシステム研究会（以下 LS 研）では、オープンネットワーク時代における実践的な情報セキュリティポリシーの策定をテーマに研究を進めた。本稿ではその研究成果の概要を報告する。

2.研究の進め方

研究を進めるにあたり LS 研には業種の異なる 15 社から参加があり各企業の事情も異なる為、参加者それぞれが描くポリシーのイメージが異なっていた。異なるイメージを合わせるため、モデル企業を想定し、全員がモデル企業の社員（各部門代表）としてポリシー策定をロールプレイングにより進めた。

策定の手法であるが「情報セキュリティポリシーの作り方」の手法は確立されておらず、公表されている事例も少ない。ISO/IEC TR13335 によれば、ポリシー策定には次の 4 つの手法が存在している。

1.Baseline　Approach	既存の標準またはガイドラインに従う手法
2.Informal　Approach	担当者の知識と経験に従う手法
3.Detailed Risk Analysys	リスクなどを詳細に分析する手法
4.Combined Approach	1 と 3 を組合わせる手法

一般的には Baseline Approach が現実的な工数負担でポリシーを構築できると考えられており、特に国内ではこの手法により構築された事例が大半を占めると考えられる。しかし、企業内の情報セキュリティーに合致したポリシーが構築されたかの判断が（なぜそれを守らなければならないのか納得させる事が）難しいと考え本研究では、Detailed Risk Analysys を取上げた。

3.研究成果

ロールプレイングでは情報セキュリティポリシーを作成し、実際の運用に至るまでをおこなったが、本稿では特に研究成果として、企業にとって最も重要なセキュリティに対する投資の判断基準の元となるリスク分析から対策決定に至るプロセスについて述べる。

3.1 リスク分析とリスク算出

リスクを分析するためには、次の要素が必要である。

(1)保護対象資源の決定と被害金額の想定
(2)セキュリティ要件（機密性:アクセス制御、完全性:更新許可、可用性:障害復旧時間）の明確化
(3)保護対象資源への脅威の洗い出し
(4)保護対象資源の脆弱性

これらの要素をモデル企業の中で設置した仮想情報セキュリティ委員会洗い出し、それぞれの脅威に対するリスク R（円/年）を以下のように定量化した。

R = Ct × Lt

Ct：脅威による被害金額（円）

Lt：脅威の発生頻度（回/年）

留意すべき点は、各リスク間で大きな差がでるので精度をあまり求める必要ない。ここでは被害金額を 1 億、1 千万、百万といった桁数レベルで想定した。

3.2 発生頻度の定量化

脅威の発生頻度を（「誰が（行為者）」「何を（資産）」「どうやって（脆弱性）」「どうする（漏洩・改ざん・破壊）」について検討した。ここでの組み合わせは膨大な量となり、詳細を把握する作業は非常に困難であった（モデル企業では 12,000 通りになった）。しかし、脅威の実行人数や発生頻度を把握するためには必要であり省くことのできない作業である。

Lt は次のように定量化した。

Lt＝Ns×(Ct×Ka×α)

Ns：推定実行者数（人）

Ka：魅力・脆弱性係数

α：発生頻度換算係数（1/円・年）

ここでαは被害金額から発生頻度を導き出すための変換係数であり、利益当たりの不正実行確率である。これは、1億円ならば30年に1回不正を実行する人が10％は存在すると想定し、α＝(0.1/1億（円）)/30（年）とした。

また、Kaは目的の資産がどの程度犯罪・誤操作を誘発するかを示す無次元の係数であり、企業にとっての価値と行為者にとっての価値の差を補正するものである。ここでは営利目的:1/100、嫌がらせ:1/1000、過失：1/1000として定義した。

この算出式を用いた例を次に示す。

『社内から技術を持たない人(1000人と想定)が、顧客情報を印刷物からの入手により営利目的にデータを漏洩する場合』

R ＝Ct×(Ns×Ct×Ka)×α

＝1億×(1000×1億×0.01)×α＝333万（円/年）

となる。これらを全ての脅威に対してこのロジックを適用し「リスク分析算出表」をスプレッドシートとして作成した。

3.3 セキュリティ対策方針の検討

3.2項でで求められたリスクを大きい順に並べ替え、リスクが一定の大きさ（たとえば100万円／年）を超えるものについて、4つの観点（抑止、予防、検出、回復）からセキュリティ対策方針を立案した。

3.4 セキュリティ対策の決定

3.3項で立案した対策方針に対する具体的な対策案を洗い出し、そのコストを求める。ここでは、対策コストを使い勝手と効果を補正するための補正コストCo（円）を求めた。

Co ＝ Cm × 10/Ke × 10/Ko

Cm：対策案の実現コスト（円）

Ke：効果係数

Ko：使い勝手係数

ここで、Keは対策の効果を補正する係数であり、効果が十分ならば10、効果が少ない場合は1とした。また、Koは対策による利便性の低下を補正する係数であり、使い勝手が従来通りなら10、使い勝手が相当悪くなる場合は1とした。

洗い出した対策ごとの補正コストと、それにより回避可能となるリスクの総和を比較・検討し、対策の採否を決定する。一般的には、企業ごとにセキュリティ対策に使用できるコストには制限があるため、それに従うように対策を選定しなければならない。今回は、（補正コストの総和）≦(リスクの総和)/2を満たすように対策を決定した。なお、ソーシャルエンジニアリング（非技術的方法による不正行為）や内部要員による不正・不用意な漏洩などのリスクに対応するため、ITだけではなく、教育・啓発などが対策としてかならず必要になる。

4.おわりに

Detailed Risk Analysys手法にてセキュリティ企業においてポリシーを構築する場合、ともすれば考え方が発散し収集がつかない状況に陥ると考えられている。しかし、実際に仮想企業の中ではあるが構築が可能であることが証明できた。また、企画（ポリシーの作成）／実施（システム構築、教育・管理・啓発）／追跡調査（監査、レビュー）のサイクルを繰り返すことにより企業内で極めて有効なポリシーへと育てることが出来ることを確信した。

最後に本研究の成果物である各種定量化手法について、精度の向上と情報セキュリティポリシーの効果的な運用・展開を今後の課題としたい。

以上

The Practical Way to Make Information Security Policies.
Osamu Sakamaki　Asahigin Systems Co.,Ltd.
3-1-43 Minamiaoyama,Minato,Tokyo,107-8605,Japan　(e-mail) o-sakamaki@ags.co.jp