利用環境に対応できる情報リスクアセスメントの分析の考察

浅原　慎哉　　渥美　清隆
静岡大学

1.はじめに

情報セキュリティマネイジメントシステムを構築する上で情報リスクアセスメントは必須であるが，その方法はまだ十分に確立しているとはいえない．ノート PC のような移動ができる装備などの場合，屋内や屋外といった利用環境毎に情報資産におけるリスクは異なってくる．システムの一部を変更した時，他のシステムに影響を及ぼす場合リスクアセスメント全体を見直さなくてはならない．このような方法では利用していく上で不便である. 本研究では，情報リスクマネイジメント特有の現象に対応するリスクアセスメントを実施するために情報リスクアセスメントの分析について考察する．

2.定義

情報リスクアセスメントの分析(以下リスク分析)とは組織などが守るべき情報資産を明らかにして，個々の情報資産に関わるリスクを明らかにして数値化する作業を指す[1]. 情報リスクアセスメントは分析結果を元にリスク評価を行い反映させていくが，ここでは分析についてのみ触れている．情報セキュリティにおける一般的な要素を以下に定義する[1].

- 機密性：アクセスを許可された者だけが情報にアクセスできることを確実にすること．
- 完全性：情報及び処理方法が，正確であること及び完全であることを保護すること．
- 可用性：認可された利用者が，必要なときに情報及び関連する資産にアクセスできることを確実にすること．

3.リスク分析の方法

リスク分析は通常，重要度，脅威，脆弱性の各値が計算される．これについては文献[2]等を用いることとしてここでは取り扱わない．脅威は情報資産の機密性，完全性，可用性に危害を与える原因となる事象を考える．脅威には地震や火災などの災害や停電，静電気などによる故障，不正アクセスや盗聴，入力ミスなどの人的要因が考えられる．

通常の情報リスク分析は情報資産毎に考えられる全ての脅威に対して評価を行うが，今回は情報資産毎ではなく，情報資産が置かれている環境の属性毎にまず評価を行う．

3.1 評価方法

まず環境属性毎の評価を行う．環境属性の全体集合を $E=\{e_1,e_2,e_3,\cdots,e_n\}$とおく．$e_i$ は環境属性の要素とする．必要な要素だけを取り出した集合を部分集合 E_k とする．また脅威の全体集合を $T=\{t_1,t_2,t_3,\cdots,t_m\}$とおく．脅威の要素 $t_j=(t_j[0],t_j[1],t_j[2],t_j[3])$は 4 つの組からなる．配列部分 $t_j[0]$には脅威の種類が入り，以降の配列部分には脅威の機密性，完全性，可用性に対応する値が入る．これらは $t_j[1]$，$t_j[2]$，$t_j[3]$ のそれぞれをアクセスすることとする．脆弱性は脅威と環境属性から決まる．関数 f は，ある環境 e_i の脅威 t_j に対する脆弱性を求めるためのものとする．$f(e_i,t_j[0])$と示すことにする．

情報資産の重要度を $V_l=(V_l[1],V_l[2],V_l[3])$と表す．それぞれ機密性，完全性，可用性についての重要度を示している．情報資産の機密性に関する評価式を以下に示す．

$$V_l[1]\times\sum_{e_i\in E_k}\sum_{t_j\in T}(t_j[1]\times f(e_i,t_j[0])) \quad (1)$$

同じノート PC を屋内と屋外で使い分ける場合には環境属性の部分集合 E_k を変えることで計算ができる．

3.2 物理的な環境の場合

物理的な環境の場合，以下に示すような属性を考える．評価は情報資産毎に行うのではなく環境属性毎，屋内や屋外，ハードや媒体ごとにあらかじめ行っておく．また全ての評価を同じ人物が行う必要はなく，各管理者が行えば良い．情報資産の評価者は行われた環境属性の結果を利用して求めたい情報資産のリスク分析を行う．

e_1:ある部屋
e_2:屋外
e_3:ノート PC
e_4:デスクトップ PC　　など

属性はノート PC のように屋内や屋外など様々な環境で使用するものの場合，同時に異なる環境では使用しないので 1 度の評価では行はず別の評価をすることになる．

3.3 ネットワーク上の場合

ネットワーク上にある情報資産のリスク分析を行う場合は，物理的な場合と環境属性は異なってくる．

e_5:インターネット
e_6:イントラネット
e_7:有線 LAN
e_8:無線 LAN　　など

3.4 脅威の例

脅威の例を以下に示す. t_j=(脅威の種類, 機密性の値, 完全性の値，可用性の値)として表す.

t_1=(盗聴，3，2，2)
t_2=(盗難，3，3，3)
t_3=(地震，1，3，3)
t_4=(操作ミス，2，3，2)　　など

3.5 計算例

脅威により生じる影響度をその脅威に対する重みとして 3.4 節で説明したように機密性，完全性，可用性に対して 0~3 までで点数化する．0 の場合は機密性，完全性，可用性に脅威が影響を与えない場合となる. 点数の大きい方が影響度が高いと考える. 脅威の種類などは文献[2]等が参考になる. 脆弱性は脅威を引き起こす可能性で考える．脆弱性に対する重みは 0~3 までそれぞれ点数化する．脅威による影響が全くない場合は 0 を与え点数が高いほど影響を受ける可能性が高くなる．脅威と脆弱性は情報資産毎に機密性，完全性，可用性について評価する．情報資産の脅威に対する評価は機密性，完全性，可用性毎に(1)式に従い計算を行う．情報資産が置かれている環境を“ある部屋，ノート PC ”とすると環境属性の部分集合は $E_1=\{e_1,e_3\}$となる．脅威を上に述べた t_1~t_4 だとする．脅威の部分集合は $T_1=\{t_1,t_2,t_3,t_4\}$となる．脆弱性は表 1 より求まる．同じ脅威でも環境によって脆弱性は変わってくる．リスク値を求めると，機密性の場合リスク値は“ 33 ”となる．つぎに環境を“ 屋外，ノート PC ”としてリスク値をもとめる場合，環境属性の部分集合は $E_2=\{e_2,e_3\}$となり，リスク値は“ 39 ”となる. 完全性，可用性の場合も同様に行うことができる.

表 1　関数 f(抜粋)

		環境属性		
		e_1	e_2	e_3
脅威	t_1	2	2	3
	t_2	2	3	3
	t_3	1	1	1
	t_4	0	2	0

4.結び

今回の方法で情報リスク分析を行うと，評価者は自分の管理している環境だけの評価を行うだけですむ．部屋やネットワークなど個人で評価しにくいものはそれを管理している人の評価を利用できるため評価者による同じ環境属性に対する評価の違いはさ抑えられると考えられる. 環境属性に関する評価は，今までの方法では情報資産毎に部屋や使用ハードなどの同じ評価でも何度も行わなければならなかったが，それを行わなくてすむためリスク分析が容易になる．また，一部のシステムを変化させそれにより他のシステムに対して影響を及ぼす場合でも，変化させたり影響を受けた環境属性を変えてリスク分析を行うことで変化後のリスク分析も容易に行うことができる．一方，屋外と屋内といった場合のリスク分析を別々のものとして取り扱う場合，同時には取り扱わないようにしなくてはならない．また，金庫などの環境を追加した場合, リスクが増えてしまい，安全の為に導入したのに導入後の方がリスク値が高くなってしまうことが考えられる．その場合その環境を追加しなかった場合起こりうるリスク又は，追加することでリスクが減少するなどを考慮しなくてはならないなど課題が残る.

参考文献

[1]日本規格協会著：〝情報セキュリティマネジメントの実践のための規範”，JIS X5080:2002
[2]中野明著：〝よくわかる最新 ISMSver.2 の基本と仕組み”，2003，秀和システム