정보 보호를 위한 위험 분석 방법: 분류와 선택 기준을 중심으로

김 정덕(원광대학교 정보관리학과)
김 기윤(광운대학교 경영학과)

Risk Analysis Methods for Information Security: Classification and Selection Criteria

Jungduk Kim(WonKwang University)
Kiyoon Kim(KwangWoon University)

1. 서론

위험과 이에 따른 잠재적인 손실에 대한 의사결정은 사실 개인이나 조직에서 항상 직면하는 문제이다. 비지니스, 특히 보험이나 투자결정 분야와 원자력 등 손실의 대가가 상당한 분야에서는 손실을 감소시키기 위해 오래 전부터 위험관리에 관심을 갖고 있었다. 최근에는 컴퓨터 네트워크의 확산과 정보화에 따른 정보 의존도가 심화됨에 따라 시스템의 안정적 운영과 보호가 중요한 문제로 대두되고 있다. 그러나 비교적 새로운 정보 기술에 대한 위협 요인을 파악하기 어려우며 정보 기술 관리자의 위험 관리에 대한 인식 및 전문 지식의 결여, 적절하지 못한 위험 분석 방법의 사용으로 인한 잘못된 경험, 오랜 시간 및 자금의 소요 등의 원인으로 정보 기술에 대한 위험 분석이 회피되거나 무시되어 왔다.

따라서 시스템적 접근방법에 의한 체계적인 대책 구현보다는 직감이나 주관적인 판단에 의한 부분적인 보안용 하드웨어나 소프트웨어의 구입으로 만족하고 있다. 또는 다른 경쟁 기업이나 타 업종에서 성공한 기업이 사용하는 정보 보호 설비나 대책을 그대로 수정없이 적용하는 경향이 있다. 그러나 개별 기업이 처한 위협요인, 기업 문화나 환경, 전산 수준 등이 상이하기 때문에 타 기업에서의 성공사례와 같은 정도의 효과성이나 효율성을 거둘 수 있는지에 대한 의문이 일고 있다. 따라서 각 조직이 처한 상이한 환경을 고려하면서 각 조직이 투자할 수 있는 비용에 적절한 정보 보호 대책을 선정, 구현하는 방법론이 먼저 제공되어야 한다. 이러한 방법론을 위험 관리(Risk Management)라고 말하고 있으며 이는 정보 시스템 보안을 위한 계획 수립에서 가장 우선되면서 중요한 작업이라고 할 수 있다.

본 논문에서는 여러 기관에서 보고된 위험 관리 모델을 근거로 독자적인 위험 관리 모델을 개발하고 위험 관리 과정의 핵심이라고 할 수 있는 위험 분석 기법을 분류하여 각각의 장단점을 분석한 후 조직의 특정 상황에 적합한 위험 분석 기법을 선정할 수 있는 기준을 제시하고자 한다.

2. 위험 관리 모델과 위험 분석

2.1 외국의 위험 관리 연구 동향

70년대 중반 이전에는 국외에서도 정보 기술을 보호하기 위한 대책을 결정하기 위해 위험 분석 및 관리를 사용하였지만, 이것은 주로 내부 보안 담당관이나 감리인 등의 주관적인 판단 하에 이루어 졌거나 일반적인 환경에서의 위협요인에 기초해서 필요한 보호 대책을 기술한 일종의 규칙서(rule book)를 근거로 이루어 졌다. 이와 같은 접근방법 사용결과, 일부 성공적인 사례도 있었으나 이는 근본적인 문제를 안고 있다. 즉, 기존의 구현된 정보 보호 대책은 무조건 필요한 것으로 간주되고 정당성에 대한 평가는 전혀 의문시되지 않았다. 이는 어떤 경우에는 시스템이 과소 보호되어 허용될 수 없는 위험에 방치될 수도 있으며, 다른 경우에는 과대 보호되어 자원의 낭비를 초래할 수 있다.

70년대 중반 이후에서야 비로소 체계적이고 분석적인 방법론에 대한 연구가 시작되었다. 1979년에 미국 상무성 산하 NIST(National Institute of Standards and Technology)에서 발간한 'FIPS Pub(Federal Information Processing Standards Publication) 65; Guideline for Automatic Data Processing Risk Assessment'에서 데이터 처리에서의 위험을 자연재해와 그 결과로서 발생하는 사고의 처리 계획 요건에 초점을 두고 서술하고 ALE(Annual Loss Exposure)를 근거로 자료처리에서의 위험에 대해서 기술한 바 있다. 1990년에 미국 법무성의 보안 및 비상기획국에서 준비한 위험 분석지침으로서 'SRAG(Simplified Risk Analysis Guidelines)'는 NIST에서 다른 기관에서도 활용할 수 있도록 공포한 보안지침이다. 여기서는 위험 분석단계를 7단계로 구분하고, 위험 분석대상을 개인용 컴퓨터, 응용시스템, 주전산기와 원격접근이 가능한 자동화된 시스템별로 구분하고, 이들을 다시 정보의 비밀성 여부와 민감성(sensitivity)에 따라서 구분해서 기술했다.

1993년 EC(European Communities)에서 '위험 분석'이라는 보고서를 발행했다. 여기서는 기존 55개 위험 분석방법들을 분석하여 유럽 전체에서 공동으로 활용될 수 있는 분석방법을 개발하기 위해서 '요구구조(claim structure)'라는 도구를 개발하여 유럽표준 뿐만 아니라 국제표준으로 발전시키려 하고 있다. 1994년 현재 국제표준화기구(ISO; International Organization for Standardization)의 ISO/IEC(International Electrotechnical Commission) JTC1/SC27에서 '정보기술보안관리지침(GMITS; Guidelines for the Management of IT Security)'으로 위험 분석에 관한 표준화를 진행시키고 있다.

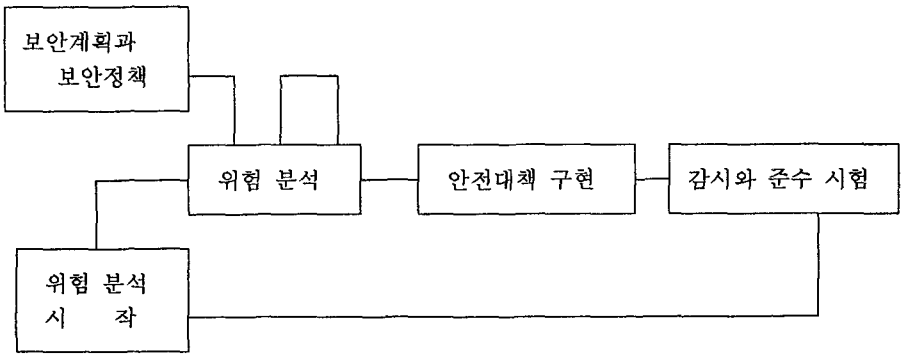
일본에서는 일본정보처리 개발협회(JIPDEC)의 주관 하에 실용적인 분석방법을 연구개발한 결과 JRAM(JIPDEC Risk Analysis Method)을 제시하였다. 이의 특징은 질문서(questionnaire)를 이용한 현 시스템 취약성에 관한 주관적 평가와 동시에 업무일지/장해보고/장해복구 종료보고/손실보고 등에서 얻어진 사고나 손실 경험을 데이터로서 작업표상에 명시하고 정량적 평가를 하는 실태 분석을 행한다는 점이다.

2.2 위험 관리와 위험 분석과의 관계

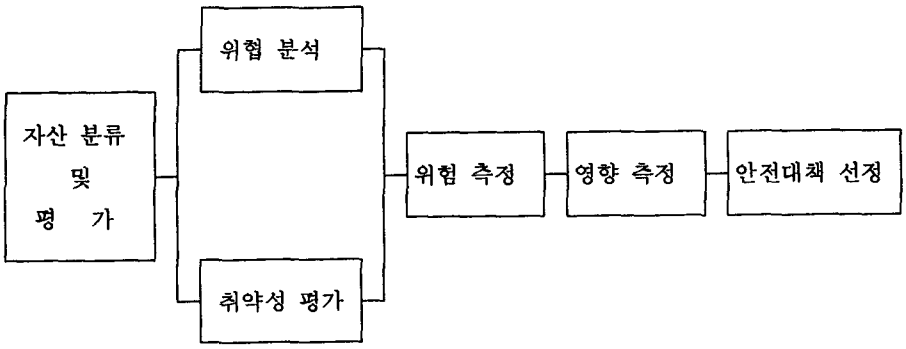
그림 1에서 나타나듯이 위험 관리란 불확실한 사건의 피해를 식별, 통제, 최소화하는 전반적인 절차에 관계된 경영 과학의 한 분야로서, 정보 시스템 위험 관리는 보안 계획과 정책에 기초하여 측정/평가된 위험에 대한 안전대책을 일정 수준까지 유지/관리하는 전체 과정을 포함한다. Robin Moses(1992)에 의하면, 위험 관리의 목적은 위험 분석 결과에 의해서 현재의 보안수준을 허용된 수준까지 높이기 위해서 보안대책을 선정/유지보수하는 것이다. 다시 말해서, 정보 시스템 위험 관리는 경영층이 받아들일 수 있는 수준까지 위협의 빈도와 영향을 감소시킬 수 있는 보안대책을 선택하고 이의 효과성, 효율성 등에 대한 감시와 준거 검사를 포함하는 것이다. 한편, 위험 분석이란 정보 시스템과 그 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대해서 시스템이 취약함을 인식하고, 이로 인해서 예상되는 손실을 분석하는 것이다.

위험 관리 과정에서 가장 중요한 과정이 위험분석 과정으로서 그림 2에서 위험 분석의 모델을 보여주고 있다. 위험 분석 절차에 대한 간략한 설명은 다음과 같다.

1) 자산 분류 및 평가: 보호해야 할 전산자원들을 식별하고, 체계적인 분류를 해서, 소유하고 있는 자산들의 가치를 평가하는 기본적인 단계이다. 여기서 자산이란 하드웨어, 소프트웨어, 데이터/데이터베이스, 사용자/전산요원, 시스템 관련문서, 전산자료 저장매체, 통신망 및 관련장비, 등을 말한다.



[그림 1] 위험 관리의 모델



[그림 2] 위험 분석 모델

2) 위협 평가: 위협(threat)은 자산(asset)에 해를 줄 수 있는 위험의 원천이다. 이와 같은 위협을 식별하고 분류해서, 발생빈도와 손실크기(혹은 강도(severity))를 측정하는 것을 말한다. 위협에는 위협원천에 따라, 자연재해로 인한 위협들(화재, 수재, 정전, 등), 사람에 의한 의도적 위협들(단말기, 디스켓, 등의 파괴 및 절취와 같은 물리적 공격, 그리고 시스템 자원의 불법사용, 허가되지 않은 자원의 불법접근, 타인으로 위장하여 권한사용, 바이러스, 벌레 등 유해프로그램 삽입과 같은 기술적 공격), 사람에 의한 비의도적 위협들(명령어 혹은 프로그램의 조작미숙 및 조작실수), 정보시스템의 결함(운용체제 결함, 응용프로그램의 결함, 통신 프로토콜의 결함, 통신 소프트웨어의 결함)이 있다.

3) 취약성 평가: 취약성(vulnerability)이란 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어의 약점을 뜻한다. 이와 같은 약점을 확인하고 분류하여 위협을 감소시키는 것이 취약성을 평가하는 목적이다. 취약성에는 관리적 취약성(보안관리, 인원관리, 절차상관리, 사고대책관리, 등에 대한 취약성), 기술적 취약성(하드웨어, 응용소프트웨어, 운영체계, 데이터베이스, 네트워크, 등에 대한 취약성), 물리적 취약성(출입통제, 환경관리, 등에 대한 취약성)이 있다.

4) 위험 분석: 자산에 대한 손실을 분석하는 과정으로서, 위협의 발생확률과 손실크기를 곱해서 기대손실을 가능하면 계량적으로 계산한다. 손실크기를 화폐가치로 계산할 수 없으면, 정성적인 위험 분석법을 이용한다.

5) 보안대책 선택: 평가된 위협요소와 취약요소에 대해서 보안대책(safeguard)을 선택하는 단계이며, 여기서 선택해서 추진하는 비용까지 계산해야 한다. 발생가능한 위험요소에 대응해서 보안대책을 수립했을 경우 감소되는 위험수준을 화폐가치로 측정/평가한다.

3. 위험 분석 접근방법

정보기술에 대한 위험 분석 방법에는 정량적 분석법과 정성적 분석법이 있다. 여기서 정량적 분석법이란 위협발생 확률과 손실크기를 곱해서 계산하는 '기대가치분석(expected value analysis)'인 경우이며, 정성적 분석법이란 손실크기를 화폐가치로 측정할 수 없어서 위험을 기술변수(descriptive variables)로 표현하는 경우이다.

정량적 분석법에는 수학공식접근법, 확률분포추정법, 점수법, 몬테칼로 시뮬레이션 등이 있고, 정성적 분석법에는 델파이법, 시나리오법, 순위결정법, 퍼지행렬법(fuzzy metrics), 질문서법(questionnaires) 등이다.

3.1 정량적 위험 분석방법

3.1.1 수학공식 접근법

수학공식접근방법은 위협의 발생빈도를 계산하는 식을 이용하여 위험을 계량화하는 것이다. 이 방법은 자료를 획득하기 어려울 때, 위협발생빈도를 추정하기 위해서 이용된다. 우선 위험분석팀을 편성한 후 위협변수들을 식별한다. 위험 분석 팀은 위협에 영향을 받는 자원을 식별해서 위협으로 인한 최대 손실 액을 추정하기 위해서 자동화된 장비의 형태, 컴퓨터 시스템의 특성, 사용자 수, 거래 수, 거래 당 평균 가치, 등에 관한 정보를 수집한다. 그 다음 단계는 위협의 발생빈도를 추정한다. 위험 분석 팀은 위협에 영향을 받는 각 자원에 대한 손실 발생의 기대 빈도 값을 추정해야만 한다. 가장 많이 알려진 방법이 IBM의 Robert Courtney 공식에 의한 것이다. 이를 기초로 년간 기대손실액(ALE; Annual Loss Expectancy)을 추정/계산한다.

위험 분석의 공식접근법으로 가장 많이 쓰이는 것은 Robert H. Courtney, Jr의 분석 방법으로 미국 NIST(National Institute of Standards and Technology)에서 발간하는 FIPS65(Federal Information Processing Standards Publication Number65)에서 채택되었다. 이 분석방법의 특징은 위험의 정량화(금액화)를 매우 간결하게 나타낸 것이다. R. Courtney는 모든 위협은 여섯 개의 속성(우연적인 폭로, 의도적인 폭로, 우연적인 변경, 의도적인 변경, 우연적인 파괴, 의도적인 파괴)에 포함된다고 가정했다. 그리고, 여섯 개의 위협 구분에 대하여 년간 기대 손실액(ALE; Annual Loss Expectancy)을 계산한다. 위협의 기대빈도 P는 다음과 같은 식으로 추정했다.

$$P = 1/3 * 10^{(p-3)}$$

위협 발생 한 건당 손실크기 V는 다음과 같은 식으로 추정했다.

$$V = 10^{v}$$

그러므로, 년간 기대 손실액 E는 다음과 같이 계산된다.

$$E = P * V = 1/3 * 10^{(p-3)} * 10^{v} = 1/3 * 10^{(p+v-3)}$$

여기서, 소문자로 표시된 p와 v는 발생 빈도와 손실 액과 관련된 파라메타로서 (표 1)과 같은 상수가 공식에서 사용된다. 각 각의 v와 p의 경우에 E의 값을 계산한 것이 (표 2)이다.

수학공식접근법으로서 년간 기대 손실액(ALE; Annual Loss Expectancy)을 계산하는 방법은 미국 NIST의 FIPS65 뿐만 아니라, RISKCALC, BDSS(Bayesian Decision Support System)와 같은 위험 분석 소프트웨어에서도 사용되었다. 수학공식접근법의 장점은 위험추정과정을 단순화시키면서 체계적인 절차를 제시해준다는 것이다. 그러나, 공식에서 사용되는 변수간의 관계에 대한 수학적인 증명이 없고, 손실을 계량화하는데 어려움이 있다. 특히 년간을 기준으로 년간 기대 손실액(ALE)을 계산하는데 모순이 있다. 예로써, 100년에 한번 $1,000,000 손실이 발생된 것은 년간 $10,000 손실이 발생된 것이다. $10,000손실은 큰 재난(catastrophic)은 아니지만, $1,000,000손실은 큰 재난이며, 위험의 특성이 전혀 다른 것이다.

(표 1) p와 v에 대한 값

추정된 발생 확률 p			1회 예상 손실액, $ v	
300년에	1회	p=1	10	v=1
30년에	1회	p=2	100	v=2
3년에	1회	p=3	1,000	v=3
100일에	1회	p=4	10,000	v=4
10일에	1회	p=5	100,000	v=5
1일에	1회	p=6	1,000,000	v=6
1일에	10회	p=7	10,000,000	v=7
1일	100회	p=8	100,000,000	v=8

(표 2) 년간 기대 손실액 E

	p의 값								
		1	2	3	4	5	6	7	8
v의 값	1					$300	$3K	$30K	$300K
	2				$300	3K	30K	300K	3M
	3			$300	3K	30K	300K	3M	30M
	4		$300	3K	30K	300K	3M	30M	300M
	5	$300	3K	30K	300K	3M	30M	300M	
	6	3K	30K	300K	3M	30M	300M		
	7	30K	300K	3M	30M	300M			

3.1.2 확률분포 추정법

미지 사건을 추정하는데 흔히 사용되는 방법 중에 하나가 PERT(Program Evaluation and Review Technique)에서 베타분포를 가정해서 시간추정 하는 방법과 동일한 방법이다. 다점 확률분포 추정법은 다점 추정치로 부터 도출된 분포로 부터 가중치를 계산하기 위해서 다음과 같은 표준분포식(Standard Distribution Equation)을 이용한다.

$$E_v = \frac{a + K * m + b}{K + 2}$$

여기서, E_v = 단위 기간당 기대(가중)값, a = 위협발생에 대해 가장 비관적 추정치, b = 위협발생에 대해 가장 낙관적 추정치, m = 모든 다른 추정 치의 산술평균, K = 표준화시키는 인자(normalizing factor)로서 파라메터(parameter)이며, 4가 가장 적당하다. 표준분포식은 최대값과 최소값 사이의 분산 혹은 편차가 유의적일 경우만 이용될 수 있으며, 유의적이지 못할 때는 산술평균을 이용하는 것이 바람직하다. 이용하기 위한 전제조건으로는 (1) m값은 a나 b값과 같으면 안된다. (2) K가 4일때 3점추정법과 같다. (3) m값이 0이면 K와 m값을 공식에서 제거시키고, a와 b의 평균값 = (a+b) / 2를 사용한다. 계산된 기대값은 단위 시간당 기대 빈도이므로, 여기에 사건 당 손실 액을 곱해서 전체 기대 손실 액을 구하게된다. 위 공식을 발생빈도에 대한 추정은 물론 손실 액을 추정하는데도 사용할 수 있다. PERT에서와 같이 베타분포를 근거로 한 3점 추정법보다도 우수한 추정법으로는 Extended Pearson-Tukey 추정법, Extended Swanson-Megill 추정법, 등이 있다.

3.1.3 점수법

점수법(scoring)에서는 기대가치를 추정하기 위해서 가치측정행열을 이용한다.

(표 3) 위협강도 추정을 위한 가치측정행열의 예

위협발생요인	가중치	4	3	2	1	0	가중치*점수
표준의 결여	5		x				15
규칙제정의 결여	3		x				9
문서화의 결여	4	x					16
훈련절차의 취약	2		x				6
기타	1						

우선 위험 분석가는 가치측정행열의 왼쪽 행에 위협발생을 야기시키는 요인(혹은 조건/상황)을 기술한다. 표 3과 같이, 점수를 0점-4점까지 5점 척도로 측정할 수 있다. 가능하면, 기

술된 요인들에 대한 상대적 중요도인 가중치를 이용할 수도 있다. 그 다음, 각 요인에 대한 점수에 가중치를 곱한 값이 강도지수(severity index)이고, 개별 강도지수들을 합한 값이 전체 강도지수(ASI; Aggregate Severity Index)이다. 예에서는 ASI = 15 + 9 + 16 + 6 = 46 이다. 이론적 최대값(예로써, 0점-4점까지 측정된 값 중 4점)으로 측정된 모든 요인들을 근거로 최대 강도지수를 계산한다. 예에서 최대강도지수는 4 * (5 + 4 + 3 + 2 + 1) = 60 이다.

다음 단계는 발생빈도에 대해서 구간추정(예로써, 0-15 회/년)을 한다. 위험 분석가는 계산된 강도지수(ASI)에 대해서 발생빈도를 추정한다. 예로써, 위협발생이 년간 0회 내지 15회이고, 전체 강도지수가 최대값 60에서 46으로 계산된 경우에, 발생빈도를 추정하라고 질문하면, 어떤 사람은 년간 5회, 또 다른 사람은 년간 8회라고 대답할 것이다. 기대값을 계산하기 위해서 여러 사람들이 추정한 값을 다점 추정법에 의해서 평균값을 구한다.

주관적 가중치를 부여하는 방법은 MAUT(Multi-Attribute Utility Theory), AHP(Analytic Hierarchy Process), Borda-Kendall 법, Minimum-Variance 법, Geometric-mean consensus matrix 법, 등 다양한 방법이 있다.

3.1.5 시뮬레이션법

시뮬레이션은 위험을 평가하는데 매우 유용한데, 그 이유는 의사결정자가 예상가능한 결과들뿐만 아니라 다양한 결과와 관련된 확률들을 관찰하도록 하기 때문이다. 몬테칼로 시뮬레이션(Mote Carlo simulation)은 시스템이 확률적 요소를 내포하고 있을 때 사용할 수 기법이며, 무작위 표본추출법을 통한 확률에 근거를 두고 있다. 시뮬레이션의 핵심적인 절차는 세 가지 기본단계를 거친다. 첫째, 스프레드쉬트(spreadsheet)나 시뮬레이션 언어로 문제나 상황을 정의하는 모형을 세운다. 둘째, 불확실하기 마련인 모형에서 변수들을 확인하고 가능치들의 확률분포를 명시한다. 셋째, 모형의 핵심변수에 대한 가능한 결과의 확률분포를 생성하기 위해서 시뮬레이션 모형을 실행한다.

시뮬레이션의 장점은 수리적 모형으로 분석할 수 없는 복잡하고 동적인 현상을 모형 화하도록 해준다. 또한, 모형의 구성요소들과 변수들 간의 상호작용 효과를 분석할 수 있으므로 중요한 구성요소와 변수를 파악할 수 있다. 단점은 시뮬레이션은 최적화기법이 아니고 비용이 많이 들며, 표본오류(sampling error)가 확률적 시뮬레이션 모형들로부터 나온 모든 결과에 존재한다는 것이다. 또한, 시뮬레이션 모형은 스스로 해를 제공하는 것이 아니므로 의사결정자가 검토하고자 하는 해를 위한 조건이나 제약을 만들어야 한다.

3.2 정성적 위험 분석방법

3.2.1 델파이법

델파이 기법의 목적은 전문가들의 견해를 일치시키는 것이다. 델파이 팀으로서 위험 분석 팀은 정보시스템이 직면한 다양한 위협과 취약성을 토론하고 우선 순위를 결정하는 방법이다. 델파이법의 주요 장점은 위험 분석을 짧은 시간 내에 할 수 있으므로 비용을 절약할 수 있다는 점이다. 이 방법은 단독으로 사용되기 보다는 이 장에서 서술하는 여러 기법과 동시에 사용된다. 예를 들면, 델파이법에 의해 인식된 위협의 심각성에 대한 우선순위를 결정하기 위해 비교 위험 순위결정법을 사용하기도 한다.

3.2.2 이야기식 시나리오법

이야기식 시나리오(Narrative Senario) 접근법은 실제로는 어떤 사건도 기대했던 대로 정확하게 발생하지 않는다는 사실을 근거로, 일정 조건하에서의 위협에 대한 발생가능한 결과들을 추정하는 것이다. 이 방법에서는 전문가 집단이 자산과 잠재적인 위협을 식별하고, 이와 같은 자산이 위협에 의해서 어떻게 손실이 발생되는지를 기술한 다양한 시나리오들을 도출해낸다. 이러한 시나리오들을 중요도에 따라서 순위를 정한 후에는, 보안 프로그램 중에서 가장 취약한 부분을 빠르게 식별해 낼 수 있다. 시나리오 접근법은 특히 내부적 위협에 대한 취약성을 식별하는데 유용하다.

이야기식 시나리오 접근법에 의해 위협의 결과로 발생될 수 있는 상황에 대한 서술, 발생될 수 있는 사건에 대한 확률 추정, 위협으로부터 조직이 보호되는데 소요되는 비용을 추정 등을 산출해 낼 수 있다. 시나리오법의 장점은 아주 적은 정보를 가지고 있는 경우에도 전반적인 가능성을 추론할 수 있고, 위험 분석 팀과 경영층간의 원활한 의사소통을 가능케 한다는 것이다. 단점은 시나리오 법은 결국 발생가능한 사건의 이론적 추측에 불과하다는 것이다. 시나리오란 비현실적이고 실용적이지 못하므로, 이를 채택한 조직으로서는 가능성이 많지 않은 것에 대해서 상당한 비용 부담을 감수해야 한다.

3.2.3 순위결정법

비교 위험 순위결정(comparison risk ranking)은 비교 위험 순위결정표에 위험 항목들의 서수적 순위(ordinal ranking)를 결정하는 기법이다. 비교 위험 순위결정은 각 위협을 모든 다른 위협과 비교할 수 있기 때문에, 전문가 견해를 아주 단순하게 통합시킬 수 있다. 두 위협만을 비교하고 있는 동안, 나머지 다른 위협들은 전부 무시되고 있다.

Jerry FitzGerald & Associates가 생산한 RANK-IT은 델파이법을 이용한 위험 분석 소프트웨어이다. 이를 이용하여, "어떤 위협이 급료 지급 시스템에 보다 더 큰 위험인가 ? "라는 질문에 대한 5명의 델파이 위원들의 대답 자료를 예로 설명하고자 한다.

7.5	불법접근	불법접근			
10.0	가짜와 도난	2 : 3	가짜와 도난		
1.5	사생활 침해	1.5:3.5	0 : 5	사생활 침해	
11.0	자료손실	4 : 1	2 : 3	5 : 0	자료손실

(그림 4) RANK-IT을 이용한 위험 순위결정 표의 예

단계1: 델파이 팀의 구성원들은 "어떤 위험이 보다 더 발생될 가능성이 많은가 ?" 라는 질문을 가지고 두 가지 위협을 쌍비교 한다. 이에 대한 대답은 예로써, 1 : 0, 0.8 : 0.2, 0 : 1, ..., 혹은 0.5 : 0.5 (두 위협의 가중치가 동일한 경우), 등 합이 1 이되는 수많은 비율로 표현될 수 있다.

단계2: 한번에 두 가지 위협만을 비교하면서 의견 차이를 서로 토론/조정한다. 그러나, 일치된 견해를 도출하기 위해서 구성원들을 강압하지 않고, 다양한 견해를 표현하게 한다.

단계3: 두 가지 위협에 대해서 각 구성원들이 제시한 값을 합산한다. 예로써, 5명인 경우 2 : 3, 1.5 : 3.5, 0 : 5, 등의 값이 나올 수 있다.

단계4: 단계3에서 제시된 값들을 각 위협별로 합산한다. 예로써, 불법접근인 경우, 3 + 3 + 1 = 7.5 이고, 가짜와 도난인 경우는, 2 + 5 + 3 = 10 이고, 사생활 침해인 경우는 1.5 + 0 + 0 = 1.5 이고, 자료손실인 경우는 4 + 2 + 5 = 11 이 된다.

단계5: 단계4에서 합산된 값을 근거로 위협 우선순위표를 작성한다. 예에서는 자료손실, 가짜와 도난, 불법접근, 사생활 침해 순이다.

이와 같이 서수적 순위결정(ordinal ranking)은 순위가 일련의 순서로 표현된 것이다. 서수적 서열은 위협, 취약성, 등을 가장 위험한 혹은 가장 민감한 위험 항목에서 가장 덜 위험한 혹은 가장 덜 민감한 위험 항목 순으로 나열한 것이다. 이와는 달리 기수적 순위결정(cardinal ranking)은 각 위협에 대해서 정확하게 숫자로 표현된 값을 부여한 것이다. 이러한 것에는 각 위협에 대해서 항상 발생 건당 손실 액과 발생확률을 추정하는 과정이 포함되어 있다.

이 이외에 정성적인 위험 분석방법으로 질문서법(questionnaires)이 있다. 질문서법에서 질문들은 컴퓨터 공급업자, 보안회사, 컴퓨터 보안 관련 자료로부터 구할 수 있다. 질문들은 항상 입/

출력, 처리, 등 기능적인 영역에 따라 구분되어 있고, 하드웨어, 소프트웨어, 사람, 등과 같은 자산별로 기술되어 있다. 질문서로 부터 최근 보안대책이 소홀히 취급되는 취약성을 파악할 수 있다는 장점이 있다. 그러나, 질문들이 대부분 너무 일반적이고 포괄적이므로, 잠재적 손실에 대한 발생 확률이나 크기를 구체적으로 고려하지 못하는 단점이 있다.

여기서 기술한 정량적 및 정성적 위험 분석방법 이외에도 상대적 영향척도법(RIM; Relative Impact Measure), Citibank 방법, Fuzzy Metrics 등 다양한 방법들이 있다. 이와 같은 위험 분석방법은 미국의 NIST(National Institute of Standards and Technology)와 NCSC(National Computer Security Center)에서 위험 관리와 방법론에 관해서 많은 연구를 하고 있으며, 위험 분석방법의 선택 및 사용을 지원하는 지침서를 발간하고 있다.

4. 위험 분석방법의 선택기준과 적용

위험 분석방법을 선택할 경우에는 비용, 복잡성, 적용성, 타당성, 등을 고려하여 장/단점을 검토해야 한다. 위험 분석방법들의 장/단점을 비교한 후에, Perry & Kuong(1981)이 제안한 다음과 같은 기준을 고려해서 그 분석방법을 선택하되 가능하면 여러 방법을 복합적으로 사용하는 것이 바람직하다.

(1) 정확성; 위험 분석방법에 의한 추정의 정확성 정도.
(2) 완전성; 분석/평가 과정 중 가능한 모든 위협속성을 포함시킨 정도.
(3) 노력; 위험을 분석하는데 소요되는 시간과 자원의 량.
(4) 실행성; 위험 분석 결과를 경영층이 받아들여 실행시키는 정도.
(5) 이용기술; 위험 분석방법을 효과적으로 이용하는데 소요되는 훈련과 지식의 량.
(6) 지원가능성; 기대 손실을 추정하는 위험 분석방법을 지원하는 명시적인 자료의 량.
(7) 측정가능성; 실제 손실과 추정 손실을 비교해서 추정 손실의 신뢰도를 높이는 손실 추정의 정확도.

분석방법들을 선택기준에 따라 정성적으로 높음, 보통, 낮음으로 평가한 것이 (표 4)이다. 높음은 선택기준의 목표에 아주 잘 도달된 것이고, 낮음은 그 반대이다. 보통은 선택기준의 목표에 적절하게 도달된 것이다. 이와 같은 여러 가지 선택기준들과 분석방법들의 장/단점을 고려해서 위험 분석가 혹은 경영자는 특정 상황에 적절한 분석방법을 선택해야 한다.

분석방법에서 과거자료접근법은 미래 사건의 발생가능성을 예측하는 방법으로 사건에 대한 과거 자료를 이용하는 일상적인 기술통계분석을 의미하는 것으로 기대손실을 계산하고, 보안대책에 대한 비용효과에 따라 통제를 조정하는 방법이다. 정량적 분석법이 정성적인 분석법보다도 우수한 것은 당연하며, 특히 위협의 발생빈도와 손실크기에 대한 과거자료가 있는 경우에는 과

거자료접근법에 의해서 위험측정이 가능하므로 대부분 선택기준에서 높게 평가되었다. 또한, 위에서 기술한 확률분포추정법, 점수법, 델파이법, 순위결정법, 시나리오접근법, 등은 모두 주관적 접근법이므로 낮게 평가되었다.

(표 4) 위험 분석방법의 선택기준

선택 기준 / 분석 방법	정확성	완전성	노 력	실행성	이 용 기 술	지 원 가능성	측 정 가능성
과거자료접근법	높음	높음	높음	높음	보통	높음	높음
수학공식접근법	보통	보통	보통	보통	보통	낮음	높음
확률분포추정법	낮음	보통	낮음	보통	보통	보통	보통
점 수 법	낮음	보통	낮음	보통	보통	보통	보통
델 파 이 법	낮음	보통	낮음	보통	보통	보통	보통
순위 결정법	낮음	보통	낮음	보통	보통	보통	보통
시나리오접근법	낮음	낮음	낮음	보통	낮음	보통	낮음
몬테칼로시뮬레이션	낮음	높음	높음	보통/낮음	높음	높음	보통/높음

5. 결론

위험 분석이란 정보시스템과 그 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대해서 시스템의 취약성을 인식하고, 이로 인해서 예상되는 손실을 분석하는 것이다. 위험 분석과정은 자산, 위협, 취약성, 보안대책, 그리고 손실을 계산하는 여러 요소들 간에 관계를 분석하는 것이다.

위험 분석방법에는 위협발생확률과 손실크기를 곱해서 계산하는 '기대가치분석(expected value analysis)'인 정량적 분석법과, 손실크기를 화폐가치로 측정할 수 없어서 위험을 기술변수(descriptive variables)로 표현하는 정성적 분석법이 있다. 정량적 분석법에는 수학공식접근법, 확률분포추정법, 점수법, 몬테칼로 시뮬레이션, 과거자료접근법, 등이 있고, 정성적분석법에는 델파이법, 시나리오법, 순위결정법, Fuzzy Metrics, 질문서법, 등이 있다.

위험 분석방법들은 정확성, 완전성, 노력, 실행성, 이용기술, 지원가능성, 측정가능성, 등 선택기준들과 분석방법들의 장/단점을 고려해서 위험 분석가 혹은 경영자는 특정 상황에 적절한 분석방법을 선택해야 한다. 위와 같은 위험 분석과정에서 정량적 분석법이 정성적 분석법보다도 선택기준 측면에서 우수한 방법이지만, 별로 이용되지 않은 이유는 주관적 성질을 갖고 있는 위험을 계량화하는데는 한계가 있기 때문이다. 위협의 발생빈도가 매우 작은 경우나 손실크기를 화폐 가치로 추정해야하는 경우 충분한 과거자료가 없는 경우가 대부분이다. 무엇보다도 위험 분석방법의 불완전성과 의사결정자의 제약된 합리성이 위험을 분석하는데 가장 큰 한계점이 된다. 그러므로, 선택기준을 고려해서 그 분석방법을 선택하되 가능하면 여러 방법을 복합적으로 사용하는 것이 바람직하다.

참 고 문 헌

Commission of the European Communities Security Investigations Projects, Risk Analysis Methods Database, Project S2014 - Risk Analysis, Report Number 19744(S2014/WP08), Version 1.0, Jan. 1993.

Commission of the European Communities Security Investigations Projects, Final and Strategy Report, Project S2014 - Risk Analysis, Report Number 9744 (S2014/WP08), Version 1.0, Feb. 1993.

FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis, U.S. Department of Commerce/National Bureau of Standards, Aug. 1979.

FIPS PUB 73, Guidelines for Security of Computer Applications, U.S. Department of Commerce/National Bureau of Standards, Jun. 1980.

ISO/IEC JTC1/SC27 N689, Guidelines for the Management of IT System Security: Part3-Techniques for the Management of IT Security, ISO, Mar. 1993.

ISO/IEC JTC1/SC27 N720, Guidelines for the Management of IT Security(GMITS): Part2-Managing and Planning IT Security, ISO, May. 1993.

ISO/IEC JTC1/SC27 N777, Guidelines for the Management of IT System Security (GMITS): Part1-Concepts and Models for IT Security, ISO, Oct. 1993.

Keefer, Donald L. & Bodily, Samuel E., "Three-Point Approximations For Continuous Random Variables," Management Science, Vol.29, No.5, May 1983, pp.595-609.

Moses, Robin., "Risk Analysis and Management," Computer Security Reference Book edited by Jackson, K. M. & Hruska, J. & Parker, Donn B., CRC Press, Inc., 1992, pp.227-263.

_____ , "CCTA Risk Analysis and Management Methodology(CRAMM)," Datapro Reports on Information Security, December 1992, pp.101-110.

NIST, U.S. Department of Justice Simplified Risk Analysis Guidelines, NISTIR 4387, Aug. 1990.

Ozier, Will., "Issues in Quantitative Versus Qualitative Risk Analysis," Datapro Reports on Information Security, March 1992, pp101-107.

Perry, William E. & Kuong, Javier F., EDP Risk Analysis and Control Justification, Management Advisory Publications 1981.

Rainer, Rex Kelly, Jr. & Snyder, Charles A. & Carr, Houston H., Risk Analysis for Information Technology, Journal of Management Information Systems, 1991, Vol.8, No.1, pp.129-147.

Robak, Edward. & Security and Emergency Planning Staff, U.S. Department of Justice Simplified Risk Analysis Guidelines(SRAG), National Institute of Standards and Technology, 1990.