韓國 컴퓨터情報學會 論文誌
第8卷 第2號, 2003. 6.

2003-8-2-2-2

IT시스템 보안관리 위험분석 시뮬레이션 모델

김 강* 조 경 식**

A Risk Analysis Simulation Model for Security Management of IT System

Kang Kim* Kyoung Sik Cho**

요 약

현재 국내표준으로 제시된 모델은 공공시스템에 적용하도록 만들어진 일반 모델로서 비용과 보안관리 능력 등 여러 가지 측면에서 볼 때 일반 기업체에는 적용하기가 어렵다.

본 논문에서는 국내위험분석 모델을 바탕으로 보안관리 위험분석 시뮬레이션모델을 제안하여 일반 기업체에서 실제 적용, 운영이 가능하도록 하였다.

본 모델은 위험분석 특성상 임의적, 주관적으로 도출하게 되는 많은 기준들을 가능한 객관적이고 보편 타당한 기준을 제시하려고 하였고, 대응책 분석 및 제시에서도 현실성 있고 실제 운영 가능한 대응책을 도출하도록 하였다.

Abstract

The Korea standard model is not fitted to general company in many faces because it is made for the public institution.

This report suggests the risk analysis Simulation model of Security Management based on korea standard model, to apply and operate for general companies possibly.

This model tries to show many standards, come subjectively in the character of the risk analysis, objectively and generally, and tries to give you the possible countermove, which can be operated and actual, for the countermove analysis and presentation.

* 강원관광대학 컴퓨터정보계열 조교수
** 강원관광대학 컴퓨터정보계열 전임강사

Ⅰ. 서론

외국에서는 보안관리를 체계화하여 내·외부의 위협으로부터 보호하기 위하여 1970년부터 위험분석을 추진하여 왔으며, 근래에는 ISO/IEC JTCI/SC27/WGI[1. 2. 3. 4]의 정보기술 보안관리 지침(Guideline for the Management fo IT Security)에서 위험관리 방법론에 대하여 상세한 지침이 제시되고 있으며, 국내에서는 정보보호센타에서 1998년 국내 위험분석 모델이 제정되었으나[5] 보안에 대한 인식, 비용 등 여러 가지 면에서 일반기업체와는 매우 다른 공공정보 시스템의 위험분석 수행을 돕기 위해서 만들어진 것으로 일반 기업체에 적용하기가 어렵도록 모델이 제시되었다. 현재 일반기업체에서 위험분석에 대한 작업이 이루어지고 있으나 과정 및 결과에 대해서 충분한 의사결정권자의 신뢰를 얻지 못하고 있는 실정이다. 따라서 본 논문에서는 정보통신단체 표준으로 제정된 위험분석 표준을 기준으로 요구사항을 적용하여 일반기업체에서 실제적용 가능한 보안테스트를 위한 시뮬레이션모델 설계와 취약성, 공격, 대책의 데이터베이스 등에 대한 위험분석 시뮬레이션 모델을 제안함으로 국내 기업들의 보안에 대한 수준을 높이고자 자산에 대한 평가 시뮬레이션 모델을 구현하였다.

Ⅱ. 위험분석의 개념

2.1 정보보호관리 모델에 대한 개요

(1) BS7799 모델

정보보호관리를 위하여 IT차원이 아닌 전사적 차원에서 접근하고 있다. 즉 정보의 보호는 단지 정보차원을 통해서가 아니라 전사적 차원에서 관리하는데 중점을 두고 있다[6].

BS7799는 10개의 주요분야로 나누어진 127개의 통제사항으로 구성되어 있으며, 현재 사용되고 있는 최선의 보안실무들로 구성된 종합적인 통제사항목록을 제공하고 있다.

(2) GMITS 모델

IT보호관리를 중심으로 기술되어 있는 표준모델이라 할 수 있다. IT보호관리라는 개념은 조직에서 보유하고 있는 IT자산 모두에 대하여 IT보호정책을 개발하고, 조직 내 역할과 책임의 정의 및 부여, 위험의 관리, 형상관리, 변화관리, 비상계획, 통제사항의 선택과 구현, 보호에 대한 인식제고, 사후관리 등을 수행하는 일련의 관리적인 차원의 활동을 의미한다. 그리고 요구하는 수준의 기밀성, 무결성, 가용성, 책임성, 인증성, 신뢰성에 도달하고 관리하는 일련의 절차를 구현한 모델이다[1. 2. 3. 4].

(3) COBIT 모델

COBIT(Control Objectives for Information and Related Technology)모델은 IT보안 및 통제를 위한 모범적인 자료를 모아 구성한 일반적인 수준으로 작성된 모델이며, 전반적인 프레임워크 및 개별 통제목적을 기존의 산업 및 공인, 국제표준 및 규정과 연계하여 다양한 활동과 작업들을 세밀하게 검토하여 정보시스템의 감사 수행의 지침서를 개선하도록 한 모델이다[7].

(4) SSE-CMM 모델

SSE-CM은 소프트웨어 생명주기(Software Life Cycle)에 관한 국제표준인 ISO/IEC 12207에 기초를 한 모델이며, 조직이 구현한 IT 정보보호 프로세스를 맵핑시켜 성숙도를 측정하는 모델이다. 따라서, 정보보호관리와 관련된 지침 등에 보조적으로 사용할 수 있다. 즉 이 지침들에 의하여 구현된 체계가 얼마나 성숙되어 있는지를 확인하고 조직에서 성숙도를 높이는데 활용할 수 있기 때문이다. 구성을 살펴보면 2차원 메트릭스 형태로 구성되어 있는 모델이M다[8].

(5) NIST 모델

NIST는 보안분야에서 많은 표준 및 관련연구를 수행하였으며, NIST는 전반적인 흐름을 제시하고 사용자에게 위험분석 기법의 선택을 자유롭게 함으로 다양한 환경에서의 적용이 가능한 모델이다[9].

2.2 위험분석의 요소

① 자산(Asset) : 조직내의 가치를 갖고 있는 모든 것을 말한다.

② 위협(Threat) : 시스템이나 조직에 피해를 끼칠 수 있는 원치 않는 사고의 잠재적인 원인이다.

③ 취약성(Vulnerability) : 위협이 가해질 수 있는 자산 또는 자산 집합의 약점을 포함한 것이다.

④ 위험(Risk) : 자산 또는 자산 집합의 취약한 부분에 위협 요소가 발생하여 자산의 손실, 손상을 유발할 잠재성을 말한다.

⑤ 영향(Impact) : 원하지 않는 사건의 결과이다.

⑤ 보호대책(Safeguard) : 위험을 줄이기 위한 실천, 절차 또는 메커니즘이다.

⑦ 잔여위험(Residual Risk) : 대책을 구현한 후 남아 있는 위험이다.

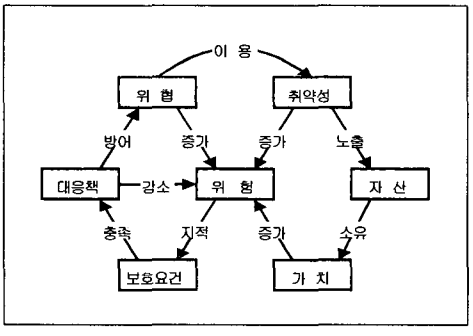

그림2-1. 위험분석 연관관계도
Fig. 2-1 Risk Analysis Diagram

Ⅲ. 제안 모델 비교 분석

3.1 제안 시뮬레이션 모델

보안관리 위험분석 시뮬레이션 모델은 정보보호관리를 위하여 보편타당성 있게 기준을 제시하고 보안사고 시 발생되는 IT자산의 손실을 정량적으로 산출하여 기업에 미치는 유·무형의 손실을 사전에 예방하기 위한 것이다.

따라서 본 모델은 대응책 구현과 잔류위험 평가를 제외한 순수한 위험분석을 기준으로 구현할 수 있고, 현재 사용하는 IT시스템의 위험요소만을 식별할 수 있게 독립된 프로세스로 분리 구성하였다.

또한, 대응가능수준 단계에서는 위험분석 할 대상 범위의 분류와 위협수준에 따라서 자산가치를 분석하고, 분석된 자산은 등급별로 분류하여 위협수준에 따라 틀려지는 자산의 피해정도를 보안등급으로 분류하여 자산의 가치를 보다 정확하고 신속하게 분석할 수 있게 하였다.

특히, IT시스템 자산에 대한 제약사항을 식별하고 취약성을 분석하여 자산별 가치정도에 따라서 자산간의 의존도를 고려하여 IT시스템의 위험에 대한 대응책을 도출하고 위험에 대하여 기존에 구축되어있는 대응책을 분석하여 위험의 정도와 가치정도를 산출할 수 있게 하였다.

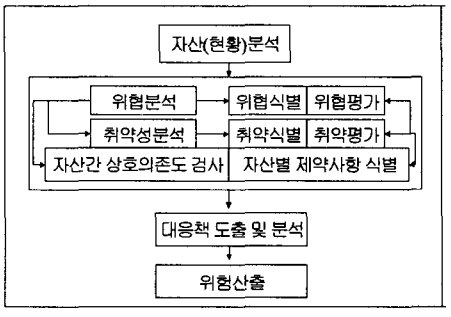

그림 3-1. 위험분석 시뮬레이션 모델
Fig. 3-1 Risk Analysis Simulation Model

3.2 국내 표준모델과 비교

국내 표준 위험분석 모델과 비교하여 장점을 수용하고 필수작업요소들을 포함한 위험분석의 전체흐름을 제시하여 일반환경에서 적용하기 쉬운 모델을 제안하였다. 본 시뮬레이션 모델은 보안 정책 수립 시 조언과 경제적인 보안대응책 수립을 위하여 위험산출 단계를 강화하여 의사결정권자의 참여를 유도하고 위험분석 산출물에 대한 신뢰성을 향상시켰다. 그리고 기업의 IT시스템을 대상으로 위험분석 시뮬레이션 모델을 적용하여 주요단계를 분석하고, 국내표준모델과 제안모델을 단계별로 장·단점을 비교분석 하였다.

표 3-1. 국내 표준 모델과 비교
Table. 3-1 Compare to Korea Standard Model

구 분	국내표준모델	제안모델
설계 목적	공공기관정보시스템에 적용	일반기업체 적합
위험분석의 전체흐름 제시 유무	위험분석의 전체 흐름제시	위험분석의 전체 흐름제시

분석결과의 정확성	방법론에서 정확	정확
대응책의 경제성	정성적 분석위주	정량적분석 위주로 적용용이
분석 비용과 시간	상세위험분석으로 시간 및 비용 과다	미확인
분석범위의 적절성	기본 및 상세위험분석 분류	기본 및 상세위험분석 분류
자산분석의 효율성	정량 및 정성적 자산분석	- 정량 및 정성적 자산분석 - 영역별 자산분류
위협분류의 적절성	자산별 위협의 중복	위협의 중복성 제거
대응책 분석결과 반영여부	운영중인 대응책과 필요한 대응책 파악	- 자산별 제약사항에 대한 대응책 파악 - 실제 운영 가능한 대응책 적용
자동화도구 적용 여부	적용가능	적용가능

Ⅳ. 제안 시뮬레이션 모델의 적용 및 분석평가

4.1 자산분석

IT정보시스템 중 자산의 가치가 높고 정량적 자산가치 측정이 가능한 자산을 대상으로 하였다. 자산의 가치는 해당 자산이 파괴되거나 보안요구사항이 충족되지 않았을 때 발생할 수 있는 비용으로 환산하였다.

표 4-1. 자산조사표
Table. 4-1 Asset Investigation Table

자산의 종류	자산	위치	자산가치 (원)	도입시기	영역
S/W	DB	강원	1억	2003. 2	S/W

4.2 자산위협 평가

자산위협 평가는 정보기술 보안관리 지침(ISO/IEC JTCI/SC27)을 적용하여 지수적으로 증가하는 빈도 간격과 기준 값을 적용하기 위하여 위협의 발생 빈도와 자산에 대한 위협의 취약성 이용 용이성을 적용하였다[6].

표 4-2. 위협 용이성 기준 값
Table. 4-2 Basis Value of Threat Facility

무관	0	위협이 해당 자산에 영향을 미치지 않음. 자산이 위협에 대한 취약성이 없음.
낮음	0.1	위협이 해당 자산에 미미하게 영향을 줌. 자산에 위협에 대한 취약성이 약간 있음.
중간	0.5	위협이 해당자산에 영향을 줌. 자산에 위협의 취약성이 존재함.
높음	0.85	위협이 해당 자산에 쉽게 영향을 가함. 자산이 위협에 매우 취약함.

특히 자산위협 평가 단계에서 표준모델은 먼저 모든 자산의 취약성을 파악한 후에 자산의 위협에 대한 영향을 평가하였으나, 제안 시뮬레이션모델에서는 자산이 위협과 Mapping 될 때에만 자산의 위협에 대한 영향을 평가하여 분석단계를 단축시켰다.

표 4-3. 위협테이블
Table. 4-3 Threat Table

항 목	빈도 값	취약성 이용 용이도	영향의 범위
전력공급기 고장	1년 1회	중간	75%이하
사용자실수	월 1회	낮음	10%이하

그리고 위협 영향범위 산정의 단계를 두어 자산분포 및 해당자산의 양에 따라서 자산의 침해정도를 계산하도록 하여 위협에 대한 침해정도가 과다하게 평가되지 않게 하여 분석의 정확도를 높였으며, 자산조사 시 제안 시뮬레이션모델에서 제시 된 4개의 영역은 위협범위 산정단계에서 위협영향에 대한 구체적인 기준을 제시하였다.

4.3 자산별 제약사항 식별

제안 시뮬레이션모델에서는 대응책분석에 있어 사전에 자산별 제약사항을 식별하여 기존 보안 대응책이 얼마나 정확하게 산출되었는지를 판단하는데 중요한 역할을 하게 하였으나 본 제안 시뮬레이션모델에서는 제약사항을 파악할 수 없었다.

4.4 대응책 분석

일반적인 보호대책을 알아보기 위해서 국제표준인 ISO/IEC 17799의 대책 목록을 참조하여 127개의 보호대책을 산정 하여[4], 이들의 구현 수준을 정보보호 성숙도 모델[7. 8]에 따라 다음과 같이 6단계로 구분 적용하였고,

표 4-4. 대책 구현 수준
Table. 4-4 A Counter Move Embodiment Level

대책 구현 정도	값
필요성에 대한 인식이 전혀 없음	0
문제를 인식하고 임기응변으로 대처함	0.1
대책 도입이 있으나 사안별로 큰차이기 있음	0.3
절차가 정의되어있으나 확인이 어려움	0.5
절차를 모니터링하고 반영하고 있음	0.7
최상의 프로세스로 업무를 수행하고 있음	0.9

또한, 정보보호대책과 위협과의 관련도를 정보기술 보안관리 지침(ISO/IEC JTCI/SC27)에 따라서 4단계로 나누어 분석하였다[9. 11].

표 4-5. 보호대책과 위협과의 관련도
Table. 4-5 Relation Diagram Safeguard and Risk

보호대책과 위협과의 관련 내용	기준 값
무관(보호대책이 위협을 막지 않음)	0
해당 위협과 간접적으로 관련	0.1
해당 위협과 (직접적)관련	0.5
해당 위협으로부터 보호를 목적으로 설계됨.	0.85

4.5 위험산정

보호대책의 효과는 조직에서 대책 구현정도(Si)에 따라서 보호수준에 영향을 주며, 하나의 대책이 각 위협에 대해서 서로 다른 정도의 보호 $Sd(t)$를 제공함으로 구현정도 X의 보호 정도를 나타낸다.

특히 하나의 위협에는 여러 가지 보호대책이 있으므로 각각의 대책 값이 반영되어야 하는데 보호대책의 효과는 실제 100%가 없으므로 다음과 같이 계산 할 수 있다.

보호대책의 효과 =

$$\Pi_{i=1\sim n}\{(1-S_{d(T)}\times S_i)\} \cdots\cdots (1)$$

ALE(Annual Loss of Expactancy) = SLE × T_f

$$\times \Pi_{i=1\sim n}\{(1-S_{d(T)}\times S_i)\} \cdots\cdots (2)$$

특히, 모든 조건을 동일 조건으로 보기 위해서

n개의 양수 a_1, a_2, ... a_n이 있을 때, 이들 수의 곱의 n제곱근 $\sqrt[n]{a_1\ a_2 \ldots\ a_n}$ ..... (3)의 값을 상승평균이라고 한다. 이를테면, 1개의 직육면체의 가로, 세로, 높이가 각각 a, b, c일 때, 이 직육면체와 같은 부피의 정육면제의 한 모서리의 길이는 3개의 수 a, b, c의 기하평균과 같다. n개의 양수 a_1, a_2, ... a_n의 기하평균은 이들 수의 산술평균보다 크지 않다.

즉,

$$\sqrt[n]{a_1\ a_2 \ldots\ a_n} \le \frac{a_1+a_2+\ldots+a_n}{n}$$

(n = 1, 2, 3, ...) ..... (4)

또한, 식

$$\sqrt[n]{a_1\ a_2 \ldots\ a_n} \cdots\cdots (5)$$

은 도수가 1일 때의 변량 a_1, a_2, ..., a_n의 기하평균이지만, 각 변량의 도수가 f_1, f_2, ..., f_n 이면 그 기하평균은,

$$\sqrt[n]{f_{1a1}\cdot f_{2a2}\cdot \ldots\ f_{nan}}\ [N=\sum_{i=1}^{n} f_i]$$

으로 주어진다.

이에 따라서 보호대책이 구현될 경우에는 연간예상손실액(ALE)은 [표4-6]과 같이 줄어들게 된다.

표 4-6. 보안 대책 적용 후 총 ALE
Table. 4-6 Total ALE after Security Countermove Application

항 목	ALE (적용 전)	ALE (적용 후)
전력공급기 고장	37,500,000	16,443,375
사용자실수	850,000	244,460

4.6 대응가능 수준분석

기업의 DB의 위험분석 결과 연간기대손실이 계산 될 수 있다. 자산가치의 1/2 수준으로 위험허용 기준치를 넘으면 보안대책이 필요한 자산으로 분석된다.

기업의 집행 가능한 보안예산은 2천만원으로 파악되었으며, 위험허용 기준치는 CSO(Chief Sec-urity Office)의 판단에 근거하여 자산가치의 1/4 수준인 2천5백만 원으로 결정되었다.

대응책 도출 시 대응가능 한 수준 분석단계에서 파악된 조직의 운영 능력이 고려되어 표준모델에서 도출되었을 항목을 운영 가능한 대응책이 제시 되도록 하였다.

표 4-7. 위협순위에 따른 대책
Table. 4-7 Countermove by Risk Order

항 목	대 책
전력공급기 고장	물리적인 통제구역, 장비유지보수, 보안사고보고, 사무실, 설비보안
사용자실수	물리적인 통제구역, 사무실, 연구실 및 설비보안

4.7 대응책 제시 및 잔류위험 분석

잔류위험은 대응가능 수준을 참고로 하여 미 시행된 대응책을 도출하고, 대응책이 구현되었을 경우의 효과를 분석하여 대응책의 효율성을 검증하였다. 새로운 대응책의 필요성은 비용을 적게들이고 위험수준을 낮출 수 있는 항목과 연간 손실액에 대한 효과가 큰 항목부터 적용하였다.

조사된 각 대응책에 대해 DB의 40개 위협에 대한 ALE의 일부를 나타내었다. 이러한 추가 대응책의 실시로 DB의 총 ALE는 허용 수준에 접근한 것을 볼 수 있다. 본 논문에서는 잔류위험을 평가한 후 총 ALE가 허용수준 이하로 낮아지지 않을 경우에는 다시 대응가능수준 분석 단계로 피드백 되도록 하여 일반 조직의 역량 등을 감안하여 새로운 대응책이 도출될 수 있도록 하였다.

V. 결론

위험분석 모델은 국내에서는 1998년에 한국정보통신기술협회에서 공공정보시스템 보안을 위한 위험분석모델을 제시하여 공공분야에 적용하고 있는 실정이다.

본 논문에서는 이미 제시된 국내표준 위험분석 모델에 대하여 특성, 구조 등을 검토하여, 이를 기초로 일반 기업에서 적용이 가능한 위험분석 시뮬레이션 모델을 제안하였다. 제안 모델은 위험분석을 특성상 임의적, 주관적으로 적용하는 많은 기업들을 가능한 객관적이고 보편 타당한 기준으로 만들어 제시하였다.

특히, IT시스템 보안사고 시 발생되는 자산에 대한 피해정도를 정량화하여 기업에 미치는 유·무형의 자산의 손실을 금액으로 표현하였고, 또한 본 모델을 실질적으로 IT시스템 환경에 적용하여 본 결과 모델 각각의 프로세스에 대한 정확하고, 효율적이고, 현실성 있는 결과를 얻었다. 하지만 제한적인 IT시스템에 대하여 검증만 이루어진 것이며, 앞으로 기업의 규모나 환경면에서 다각도로 검증할 필요가 있고 위험분석 시뮬레이션 모델 평가에 대한 자동화 방안이 연구되어야 할 것이다.

참고문헌

[1] ISO/IEC TR 13335-Ⅰ, "Guidelines for the Management of IT Security Part Ⅰ : Concepts and models for IT Security", 1996.

[2] ISO/IEC TR 13335-Ⅱ, "Guidelines for the Management of IT Security Part Ⅱ : Management and Planning IT Security", 1997.

[3] ISO/IEC TR 13335-Ⅲ, "Guidelines for the Management of IT Security Part Ⅲ : Techniques for the management of IT Security", 1998.

[4] ISO/IEC TR 13335-Ⅳ, "Guidelines for the Management of IT Security Part Ⅳ : Selection of Safeguards", 2000.

[5] "공공정보시스템 보안을 위한 위험분석 표준-위험분석방법론 모델", 한국정보통신기술협회, TTAS. KO-12.0007, 2000. 3.

[6] "BS7799 Part Ⅰ, Ⅱ, PD3001, 3002, 3003, 3004".

[7] ISACA, "COBIT : Executive Summary, Management Guideline, Framework, Control Objectives, Audit Guideline, 3rd Ed.", July 2000.

[8] Jone P. Hopkinson, "The Relationship between the SSE-CMM and IT Security Guidance Documentation", 1999, EWA-Canada Ltd.

[9] NIST, FIPS PUB 191, "Guideline for the Analysis of Local Area Network Security", NIST, 1994.

[10] Alberts, Chistopher J., Audrey Dorofee, *OCTAVE*^{sm} Threat Profiles, Software Engineering Institute, Carnegie Mellon University

[11] Carnegie Mellon University, "Systems Security Engineering Capability Maturity Model, version 2.0", April 1, 1999.

저 자 소 개

김 강

1992 숭실대학교 정보산업학과 (석사)

2003 대전대학교 컴퓨터공학과 (박사)

현 재 강원관광대학 컴퓨터정보계열 조교수

조경식

1993 단국대학교 전산통계학과 (석사)

2001 단국대학교 전산통계학과 (박사수료)

현 재 강원관광대학 컴퓨터정보계열 전임강사