韓國 OA學會 論文誌
第7卷 第3號, 2002. 9.

2002-7-3-2-5

정보시스템 보안을 위한 위험분석 모델

김 강* 박진섭** 김봉회***

A Risk Analysis Model for Information System Security

Kang Kim* Jin-sub Park** Bong-hoi Kim***

요 약

정보화 시대의 역기능으로서 존재하는 정보시스템에 대한 보안 위협은 날로 증가하고 있으며 이에 대한 체계적인 보안관리가 중요시되고 있다. 보안관리에 있어서 가장 중요한 것은 위협의 근원을 파악하여 대책을 수립하기 위한 위험분석이다. 따라서 제안모델은 보안성향상을 위하여 보안정책수립을 조언하도록 하고 경제적인 보안대응책 수립을 위하여 위험산출단계에 대하여 신뢰성을 향상 시켰다. 특히 대응책 단계에서 자산에 대하여 보안등급을 부여하여 자산간의 상호의존도를 검사하게 하고, 제시된 대응책의 구현은 표준모델과 다르게 제안모델에서는 자산별 제약사항을 식별하도록 하여 불필요한 대응책을 구현하지 않도록 하여 경제적인 대응책의 구현이 이루어질 수 있도록 모델을 개선하였다.

Abstract

Existing as a reverse function in the information age, the security threats against the information system is increasing day by day and a systematic security management to this is being considered more and more important. The most important thing on security management is a risk analysis to understand the cause of the threat and to set up a countermeasure. Therefore, to increase security the proposed model will advise on the set up of the security policy and for a set up of an economic security countermeasure we have increased the reliability on the risk calculation stage. Especially, on the countermeasure stage we have requested a security level on the asset in order to examine the mutual reliance between assets, and differing from the standard model, we have improved the proposed model so that the materializing of the proposed countermeasure has been made to identify the restricted items for each asset and in order to not materialize superficial countermeasures and to make sure to materialize an economic countermeasure.

* 강원관광대학 컴퓨터정보계열 부교수
** 대전대학교 컴퓨터공학부 교수
*** 대전대학교 박사수료

논문접수 : 2002. 6. 24
심사완료 : 2002. 9. 14

Ⅰ. 서론

현대 사회는 정보화 시대로 컴퓨터기술과 통신기술의 발달로 컴퓨터를 이용한 정보통신분야가 급속히 발전하고 있다. 이와 함께 정보시스템에 대한 보안 사고도 점차 증가하고 있어 사회적으로 많은 문제가 야기되어 공공기관, 기업 등 정보시스템을 운영하는 조직들은 보안점검도구, 방호벽 등 각종 보안솔루션을 도입하여 정보시스템보안을 강화하는데 노력을 기울기고 있다. 그러나, 대부분의 조직들은 정보시스템에 대하여 보안관리체계 없이 정보시스템을 운영하고 있으며, 기업의 경우에도 보안정책을 만들어서 운영하는 기업이 거의 없는 실정이다. 특히 조직에서 운영하고 있는 망을 외부와 접속할 경우에 조직의 내부에서 가지고 있는 자원을 보호하기 위해서 보안대책 수립이 되어야만 한다.

구미 선진국에서는 보안관리를 체계화 할 수 있는 기능인 위험분석에 대해서 많은 연구가 꾸준히 진행되어 최근에는 ISO/IECJTCI/SC27/W

G1의 정보기술 보안관리 지침(Guideline for Management of IT Security)[ISO97]중에서 위험관리 방법론에 대한 지침이 출간되었고, 미국(DOC80), 캐나다(CSE96)의 관련 기관에서는 위험관리 및 분석에 대한 방법론을 자체적으로 개발하여 자국의 정보시스템 보안에 대한 효율적인 위험분석을 위해 열심히 연구개발하고 있다. 국내에서는 한국정보통신기술협회에서 1998년 국내 위험분석 표준모델을 제정하였으나, 보안에 대하여 인식과 비용 등 여러 가지 이유로 일반 조직에 적용하기에는 많은 무리가 따른다. 따라서 본 논문에서는 국내정보통신기술협회의 표준으로 제정된 위험분석 표준 모델을 바탕으로 요구사항을 적용하여 일반 조직에서 실제적으로 활용이 가능한 위험분석 모델을 제시함으로 국내 보안 수준향상에 기여 하고자 한다.

Ⅱ. 모델 및 위험분석의 개념

2.1 모델에 대한 개요

2.1.1 접근제어 모델

1) Take - Grant 모델

Take - Grant모델은 행렬에 의해서 이루어지므로 행렬의 모든 상태를 예측하기 어렵다는 문제점을 극복하기 위해서 Jones에 의해 제안된 Take - Grant 모델은 행렬 모델의 확장형으로 볼 수 있다. 이 모델은 시스템에서 권한 부여를 나타내기 위해서 그래프 구조를 사용한다.

그래프 G는 G = (S, O, E)로 정의하며, 정점(Vertex)의 집합 V는 V = SYO(S I O = ϕ이고, E는 간선(Arc)의 집합이다. $x \xrightarrow{r} y$ 는 x가 y에 대하여 접근 허가 r를 갖는다는 것이다.

2) BLP 모델

Bell Lapadula에 의해서 개발된 모델로서 정부기관이나 국방조직에서 가장 널리 사용되고 있는 최초의 수학적 모델이고, 강제적 정책하에서 자료 보호를 위한 참조 모델이다. BLP모델의 허용등급은 TS(Top Secret), S(Secret), C(Confidential), U(Unclassified)의 네 가지 요소로 구성된 집합이며, 등급 순위는 TS 〉 S 〉 C 〉 U 이다.

보안 등급의 집합은 지배관계(≥)에 따라서 부분적으로 순서화 될 수 있다. 보안 등급은 L_1 = (C_1, S_1)은 다른 보안 등급 L_2 = (C_2, S_2)에 대하여 다음과 같은 관계를 가질 경우에 우세하고, : $C_1 \geq C_2$, $S_1 \supseteq S_1$.

한편, 주어진 두 개의 등급 L_1과 L_2가 $L_1 \geq L_2$ 또는 $L_2 \geq L_1$의 관계를 갖지 않는다면 비교할 수 없도록 되어있다.

3) Biba 모델

Biba 모델은 정보의 무결성 보호를 위한 BLP 모델과

비슷한 원리를 적용한다. Biba 모델은 낮은 무결성 정보가 높은 무결성 정보에 흘러가지 못하도록 하는 모델로서, 하나의 무결성 등급이 다른 무결성 등급을 지배하는 경우에만 정보의 흐름이 발생할 수 있도록 하고 있는 모델이다.

4) Lattice 모델

Lattice 모델은 Denning에 의해서 제안된 것으로서 BLP 모델의 확장된 형태이다. 이 모델은 수학적 구조(Lattice)를 이용하여 보안 등급 집합 C와 보안범주 집합 S에 대하여 정의된 보안 수준이 주어졌을 때 격자(Lattice)는 다음과 같이 기술된다.

(C1, S1) ≤ (C2, S2) ⇔ C1 ≤ C2, S1 ⊂ S2

(C1, S1) $\oplus$ (C2, S2) = (max ((C1, S1), S1 Y S2) : 최소 상한 값

(C1, S1) $\otimes$ (C2, S2) = (max ((C1, S1), S1 I S2) : 최대 하한 값

L = (Unclassified, {}), H = (Top Secret, S).

5) Clark - Wilson모델

Clark - Wilson(CW) 모델의 목적은 상용 시스템에서 회사의 재산이나 계정 기록에 상실 또는 변형을 가져오지 못하도록 무결성을 제공하고 정당한 사용자의 권한을 통제하는 모델이다.

2.1.2 위험분석 모델

1) NIST 위험분석모델

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

2) ISO/IEC JTC1 SC27 모델

국제표준화 기구인 ISO/IEC JTC1 SC27에서 보안관리 표준지침인 정보기술 보안관리지침(GMIT)에서 위험분석을 하기 위한 방법론을 기본통제방식, 비공식적 방식, 상세 위험분석방식, 혼합방식으로 구분한 모델이다.

3) CRAMM모델

영국의 CCTA에서 영국정부기관들의 정보시스템 위험분석을 위하여 자동화 도구로 개발되어 사용하고 있다. 자동화 도구는 분석과정 및 검정과정을 자동화하고 위험관리기능도 추가하여 위험분석 효과를 극대화하는 모델이다.

2.2 보안관리에서 위험분석의 역할

정보기술의 자산은 어떠한 방법으로든 보호를 필요로 한다. 자산에서는 물리적 자산, 소프트웨어, 무형의 자산, 조직의 인원, 정보자산 등이 포함된다. 자산에 대한 보호를 체계적으로 수행하기 위해서는 자산을 식별하고, 이들 자산이 어떠한 형태의 위협으로부터 어느 정도 위험에 처하여 있는지를 측정하여, 위험 수준을 낮추기 위하여 보안대책을 선정하는 것이 필요하다. 이러한 활동을 위험관리라 하며, 위험관리는 보안관리에 있어 가장 핵심적인 활동이다.

2.3 위험분석의 요소

① 자산 : 자산의 분석범위는 시간과 비용 등의 제약조건을 고려하여 구체적인 분석수준에 맞게 결정해야한다.

② 위협 : 자산에 해를 줄 수 있는 위험의 원천이고, 잠재적인 공격을 말하는 것이다.

③ 취약성 : 자산을 손상시켜 위험을 일으키는 시스템의 약점으로 자산, 위협, 대응책간의 함수 관계를 갖는 실체이다.

④ 영향 : 보안사고가 자산에 미치는 결과를 말한다.

⑤ 위험 : 특정 위협이 취약성을 이용해서 자산을 공격하여 피해를 줄 수 있는 잠재력이며, 발생가능성과 영향의 결합에 의해 특정 지어진다.

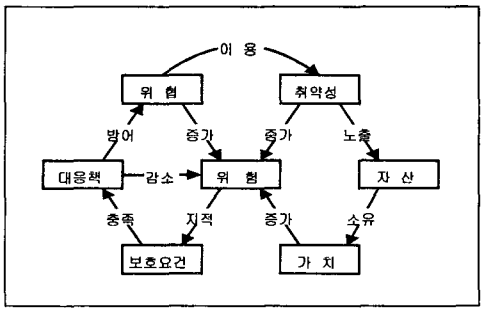

그림 2-1 위험분석 상관관계도

2.4 위험분석 접근 방법

2. 4. 1 정성적 위험분석 방법

SRI(Stan ford Research Institute)의 Donn

Parker가 제안한 조직의 환경에 대하여 중요한 영향을 미치는 위협을 고, 중, 저와 같은 설명변수에 따라 지정하는 것이며, 정성적 위험분석은 점수 또는 상/중/하 등으로 적정수준을 평가하고 그 합계를 구하여 전체 위험수준을 평가하는 방법도 정성적 분석의 하나이다.

2.4.2 정량적 위험분석 방법

정량적 방법은 위협발생 확률과 손실크기에 대하여 기대가치분석이며, 자산가치를 산출함에 있어서 가시적이고 구체적인 수치를 제공함으로 위협정도에 따라서 보안 대응책의 요소를 구체적으로 산정 할 수 있도록 한다.

※ 기본적인 정량적 위험분석 방법

① 비용대 효과 가치 계산

비용대 효과 가치 = 현재 가치(PV : Present Value)

PV = 총 이익(PV Benefit) - 비용(PV Costs)

② 연간손실액(ALE : Annual Loss Estimate)계산

$ALE = T \times L$ ($T = 1/3 \times 10^{(t-3)}$, $L = 10^{I}$)

(T : 위협의 기대빈도, L : 위협이 발생한 한 건당 손실크기)

(t, 1 : 발생빈도와 손실액에 관련된 파라미터)

2. 4. 3 체크리스트 방법

체크리스트 방법의 목적은 자산에 대한 특정 위협의 공격에 대해서 취약성을 평가하는 것이며, 보안대책의 유·무를 묻는 질문들로 구성되어 있으므로 보안대책이 가능해 진다.

Ⅲ. 위험분석 모델

3.1 기존 모델의 비교 기준

위험분석을 수행하는데 있어서 무엇을 어떻게 해야하는 것에 대해서는 적용분야와 조직의 업무분야의 대상에 따라 여러 가지 모델들이 있다.

1) 분석결과의 정확도 : 위험분석의 결과를 신뢰할 수 있어야 대응책 구현을 위한 의사결정에 이용될 수 있으며, 이것이 정확할수록 대응책 구현으로 인한 비용이 절감되므로 이것은 가장 중요한 기준이라 할 수 있다.
2) 과거 데이터의 유무 : 국내에는 위협이나 위험분석 결과의 과거 데이터가 존재하지 않기 때문에 국내에 적용하기 어려운 단점이 있다.
3) 설계목적 : 위험분석의 모델이 어떠한 조직을 대상으로 설계하는지 검증하는 단계가 필요하다.
4) 위험분석의 전체흐름 제시 유무 : 실무적인 분석에 치중하여 취약성, 위험분석 등의 방법론에 매달릴 경우 위험분석과 위협분석과 위험관리와의 관계가 불명확해지고 위험분석 결과를 준수시험(Compliance Evaluation) 등에 적용하는데 문제가 될 수 있다.
5) 필수요소의 반영 유·무 : 위험분석 조직의 업무의 위험분석 모델에 반드시 반영되어야 할 분석 단계가 빠져 있는지 검증할 필요가 있다.
6) 분석비용과 분석 시간의 단축 유·무 : 대응책 수행의 검증 등에 위험분석 결과가 관리층에 전달되지 않은 경우 분석비용과 시간의 증가를 가져올 수 있다. 따라서 질문의 방법(Survey)또는 정보습득(Information Gathering)의 단순화의 전문화가 되어 있는지를 확인할 필요가 있다.
7) 자동화 분석도구의 적용 유·무 : 위험분석모델은 자동화분석도구를 사용하여 분석비용과 시간을 단축함은 물론 지식기반 시스템의 도움을 받아 분석의 정확도를 높이고 있으므로 이것에 대한 검토를 해야 한다.

3.2 비교분석

위험분석모델은 사용자의 특정환경이나 목적에 상관없이 일반적인 위험분석에 대하여 기술하고 있다. 일반적인 위험분석 모델인 NIST, ISO, CRAMM의 모델들은 위험분석에 관한 전체적인 흐름이 잘 제시되어 있으며, 그동안 문제가 되어 온 정량적 분석을 보완하기 위해 정성적인 방법을 자산가치 산정부분에 적용하고 있다. 또한 모델의 전체의 흐름이나 상세한 분석기술은 다양한 조직 및 정보시스템 환경에서 적용하기 어려운 위험분석 모델을 쉽게 적용할 수 있게 하였다.

표 3-1. 모델 비교

구 분	NIST	ISO	CRAMM
정확도	- 일반적인흐름 제시 - 정량(기대손실치)부분의 정확도 낮음.	- 일반적인 흐름 제시	- 결과부분의 정성적 표현(상, 중, 하)에 대한 해석 중요
과거 데이터의 유무	- 위험분석기법의 종속적	- 위험분석기법의 종속적	- 데이터 있을시 유리 - 자산가치 산정시 유리
설계목적	- 공공기관, 기업대상 - 위험분석 실시기관에 표준으로 제공	- 국제표준 - 세계가 각 조직에서 사용될 수 있게 설계	- 영국정부 - 유럽에서 사용
위험분석의 전체흐름 제시 유무	- 제시함.	- 제시함.	- 제시함.
필수요소의 반영 유·무	- 기존대응책 조사과정 없음.	- 반영되어 있음.	- 반영되어 있음.
분석비용과 분석 시간의 단축 유·무	- 기법종속	- 기법종속	- 자동화도구 분석 - 시간단축
자동화 분석도구의 적용 유·무	- 기법종속	- 기법종속	- 100% 자동화 도구사용
위험분석 기법	- 정량/정성	- 정량/정성	- 정성

Ⅳ. 제안 모델

위험분석모델의 유형은 사용자의 목적과 환경에 관계없이 일반적인 환경에 적용할 수 있는 일반모델과 사용자의 환경에 맞게 개발되어 그 환경에서 최적의 위험분석을 수행할 수 있는 특수목적 모델이 있다.

본 논문에서 제안하는 위험분석 모델은 조직의 업무별로 중요성을 고려할 때 일반적인 위험분석 모델이 더욱 적합하며, 이미 개발된 국내 위험분석 표준모델을 따르되 다양한 외국모델의 장점을 수용하여 조직에 쉽게 적용할 수 있게 하고자 한다. 제안된 위험분석 모델은 위험관리 모델에서 제시한 것과 같이 대응책 구현과 잔류위험 평가를 제외한 순수위험분석 만을 위주로 구현하였으며, 현재 운영 중인 시스템의 위험요소만을 식별하고자 할 때 비용대 효과의 측면에서 다른 과정을 생략하고 위험분석만을 실시할 수 있도록 독립적인 프로세스로 분리하였다.

이는 전산망 관리자의 업무공백을 방지하고, 위험분석의 일부단계에서도 전산망의 현황을 파악하고 자산에 따른 위험의 정도를 파악하는데 용이하도록 하기 위함이다.

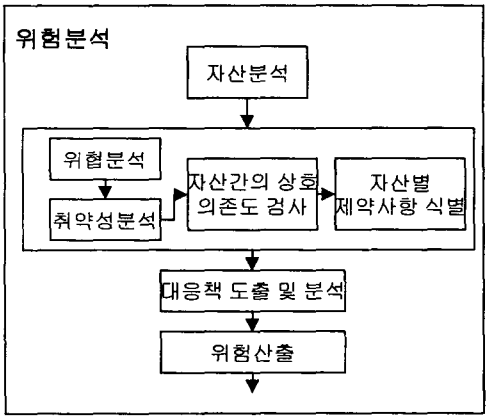

그림 4-1. 위험분석모델

1) 자산분석 모델

방법론과 분석기준이 마련되면 자산분석을 수행해야 한다. 자산분석을 통하여 조직의 자산을 파악하고, 자산의 가치와 중요도를 산출하며, 자산과 업무처리와 관계도 알 수 있다. 자산가치산정은 자산을 화폐가치를 이용하여 정량적으로 산출하는 방법과 화폐가치로 산출이 어려운 자산들을 정해진 정수나 설명변수(Descriptive Variable : 상, 중, 하) 등을 부과하여 간접적으로 산출하는 방법을 적용한다.

2) 위협분석 모델

위협분석은 자산의 피해(Impact)를 줄 수 있는 잠재적인 요소인 위협을 파악하고, 발생 가능성 등을 분석하는 과정으로 위험을 산출하는데 중요한 단계이다. 특히 자산과 취약성간의 관계를 정의함으로 앞으로 발생할 수 있는 위협이 미칠 대상을 고려하게 된다. 위협분석은 크게 사고에 의한 위협평가, 고의적인 위협평가로 나누어지며, 위협파악에서는 위협을 유형별로 분류하고, 조사하며, 각 위협의 주기를 산출한다. 위협속성에서는 위협과 자산, 취약성, 대응책의 상호관계를 파악하고, 위협순위에서는 파악된 위협주기를 바탕으로 위협의 정도에 따라 고려해야할 위협부터 순위를 결정한다.

3) 대응책분석 모델

대응책 분석모델은 기존 대응책, 보안정책 및 요구사

항 검토로 나눌 수 있으며, 대응책 파악에서는 대응책을 유형별로 분류하고, 조사하는데 현재 사용중인 대응책도 파악한다. 대응책 속성에서는 대응책과 자산, 취약성, 위협과의 관계를 파악하기 위한 대응책의 속성을 파악한다.

특히 대응책 분석은 정보시스템을 새로이 구축하는 경우와 현재 사용하고 있는 정보시스템의 2가지 경우로 나누어 적용할 수 있다. 정보시스템을 새로이 구축하는 경우에는 필요한 대응책을 조사하는 정도면 충분하다. 하지만, 운영중인 정보시스템에 대하여 대응책 분석은 운영중인 대응책들을 파악하고 이들 대응책들이 기본기능(감지, 금지, 제한, 수정, 복구, 교육, 홍보 등)을 적절히 수행하고 있는지를 파악 해야한다.

4) 위험산출 모델

위험분석 모델에서는 위험산출 시 위협분류에서 구분된 장애에 대한 위협과 보안지침에 대한 위협으로 구분하여 각각의 연간예상 기대손실을 산출하여 조직의 업무별 보안관리 뿐만 아니라 장애관리도 가능하게 하여 경영계획 수립에 도움을 주고자 한다.

위험산출을 하기 위해 자산(A : asset)의 가치를 자산 파괴 시 나타나는 손실액(A_d)으로 산정 하였다. 위협(T : threat)은 발생가능성(T_f) 및 위협과 자산에 따른 서로 다른 이용 용이도($V_{d(T,A)}$)와 영향의 범위($V_{S(T,A)}$)값을 갖게 된다. 또한 보호대책(S : safeguard)은 구현의 정도(S_i)에 따라 보호수준에 영향을 미치며, 각 위협에 대하여 서로 다른 정도의 보호($S_{d(T)}$)를 제공한다. 어떤 위협이 특정 자산에 발생하였을 때, 보호대책이 존재하지 않는다면 이때의 피해는 자산의 가치 X 취약성 이용 용이도 X영향이 미치는 범위로 나타난다. 즉, SLE(Single Loss of Expectancy) =($A_d \times V_{d(T,A)} \times V_{S(T,A)}$)이고 이에 대하여 연간 발생 가능성 T_f를 곱하면 연간 해당 위협에 의하여 해당 자산에 발생할 예상손실을 산출할 수 있다.

ALE(Annual Loss of Expectancy) = SLE × T_f

또한 보호대책이 설치되어 있을 경우, 하나의 위협에 작용하는 여러 가지 보호대책이 있을 수 있고, 각각의 대책 값이 반영되어야 하는데 보호대책의 효과는 100%가 없으므로 다음과 같이 계산한다.

보호대책의 효과 = $\Pi_{i=1\sim n}[(1-S_{d(T)\times S_i})]$

기하평균($\Pi_{i=1\sim n}$) = $\sqrt[n]{a_1, a_2, \ldots a_n}$

이에 따라 보호대책이 구현될 경우 연간 예상손실은 다음과 같이 줄어들게 된다.

ALE(Annual Loss of Expectancy) = SLE × $T_f \times \Pi_{i=1\sim n}[(1-S_{d(T)\times S_i})]$

모든 자산과 가능한 모든 위협, 그리고 설치되어 있는 보안대책을 고려함으로 분석 대상 시스템에 발생할 수 있는 연간예상손실액(ALE)을 계산하고 이에 따라 자산의 위험도를 정한다.

위 과정을 자동화 도구를 이용하여 적용할 경우 많은 시간을 절약할 수 있다.

한편, 제안모델에서는 다음과 같이 구한다.

ALE = Value(자산가치) × Exposure Factor(위협에 노출정도) × T_f(위협주기)

자산이 위협에 어느 정도 노출되었는지를 나타내는 EF는 취약성 수준산출과 마찬가지로 위험 시나리오의 자산 - 취약성 - 위협 - 대응책의 관계에서 자산 - 위협을 기준으로 관련 있는 대응책과 시행하고 있는 대응책 및 미 수행 대응책의 비율로부터 산출한다.

$$E \cdot F = V = \left(\sum_{i=1}^{i=m} CiW - \sum_{i=1}^{i=n} C \cdot iW\right) \div \sum_{i=1}^{i=m} CiW$$

- CiW : 자산, 위협별 전체대응책의 중요도합
- $C \cdot iW$:자산, 위협별 실시 대응책의 중요도합

4.3.1 제안 모델 분석

국내 표준 위험분석 모델과 외국의 위험분석 모델을 분석하여 장점을 수용하고, 필수 작업요소들을 포함한 위험분석의 전체흐름을 제시하여 일반적인 환경에 적용하기 쉬운 일반적인 모델을 제안하였다. 이 모델은 보안정책 수립에 조언하도록 하고 경제적인 보안대응책 수립을 위하여 위험산출 단계를 강화하였다. 또한 각 단계마다 의사결정권자의 참여를 유도하고 위험분석 산출물에 대한 신뢰성을 향상시켰다. 그리고 조직의 정보시스템 중 일부를 대상으로 국내 표준 위험분석 모델을 적용하여 주요단계의 산출물을 분석하고, 제안모델을 이용한 위험분석 주요단계에서 산출물과 비교하여 제안모델의 장단점을 분석하는데 이용하였다.

표 4-1. 표준모델과 비교분석

분 류	국내표준모델	제안모델
설계목적	- 국내표준 (광범위한 시스템에 적용)	- 일반전산망에 적합
위험분석 전체흐름	- 위험분석의 범위가 큼	- 위험분석의 범위 축소
보안정책 반영	- 위험관리 초기에 반영	- 도출된 대응책 반영
대응책 제시	- 위험분석 마지막 단계에 제시	- 위험분석 다음 단계에서 제시
보안등급 분류	- 데이터에 대한 등급 분류 - 등급분류 없음.	- 보안정책 분석 단계에 등급 분류 - 자산분류단계에서 다시 등급 분류
분석범위	- 분석초기에 기본, 상세위험분석으로 분류	- 잔류위험평가 후 범위 재설정
자산분석	- 정량적, 정성적 자산분석	- 영역별 자산분류 추가 가능
위협분류	- 자산별 위협 파악	- 자산별 위협의 중복성 배제
대응책 반영	- 운영 중인 대응책과 필요한 대응책 파악	- 자산별 제약사항에 따른 대응책 파악과 실제 운영 가능 대응책 반영
자동화 도구적용	- 적용가능	- 적용가능

4.3.2 제안 모델 적용

1) 자산분석

S대학의 정보시스템 중 중요도가 높고 정량적 자산가치 측정이 가능한 서버를 대상으로 하였다

표 4-2. 자산조사표

자산의 종류	자산	위치	자산가치(원)	도입시기	영역
H/W	서버	강원	100,000,000	2002. 2	H/W

2) 자산위협 평가

자산위협 평가는 위협발생 빈도 및 자산에 대한 위협의 취약성 이용 용이성 ISO/IEC JTCI/SC27의 정보기술 보안관리 지침에 따라 지수적으로 증가하는 빈도 간격과 기준 값을 적용하였다.

3) 대응책 분석

일반적인 보호대책을 알아보기 위해서 국제표준인 ISO/IEC 17799의 대책 목록을 참조하여 127개의 보호대책을 산정하여, 이들의 구현 수준을 정보보호 성숙도 모델에 따라 6단계로 구분하였다.

4) 위험산출

특정자산에 위협에 발생하였을 때 보호대책이 존재하지 않는다면 이때의 피해는 자산의 가치 X 취약성 이용 용이도 X영향이 미치는 범위로 나타낸다.

표 4-3. 보안 대책 적용 후 Server 총 ALE

항 목	기존 대책값	ALE (적용 전)	ALE (적용 후)
공중의 먼지	0.6060	2,500,000	1,515,000
네트워크 구성요소 고장	0.0457	500,000	22,850
통신망을 통한 침투	0.0699	0	0

5) 대응가능 수준분석

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

V. 결론

정보화에 따른 정보의 의존도가 심화됨에 따라 여러 위협에 의해 정보시스템의 심각한 피해를 방지하기 위한 보안대책이 요구되고 있다. 이에 따라서 보안관리를 체계화할 수 있는 국내환경에 적합한 위험분석 모델을 제안하였다.

본 모델은 초기시스템 구축 시에는 전체위험분석을 실시하도록 하였고, 이후 재분석이 필요할 시에는 잔류위험평가 이후의 피드백 단계로부터 위험관리를 실시하여 경제적인 분석에 효율화를 기하였다. 특히 대응책 도출단계에서 자산에 대하여 보안등급을 부여하여 자산간의 상호의존도를 검사하고, 자산별 제약사항을 식별하도록 하여 불필요한 대응책을 구현하지 않도록 하여 경제적인 대응책의 구현이 이루어 질 수 있도록 모델을 개선하였다. 하지만, 본 모델은 제한적인 검증만 이루어 진 것이므로 앞으로 다각적인 환경과 구체적인 검증이 필요하다. 또한 충분한 검토를 통하여 위협이나 대응책의 산출 시 필요한 다양한 체크리스트의 개발이 필요하며, 효율적인 자동화 방안이 연구되어야 할 것이다.

참고문헌

[1] "정보보호관리체계 모델", KISA, 2001.

[2] "공공정보시스템 보안을 위한 위험분석 표준-위험분석방법론 모델", 한국정보통신기술협회,정보통신단체표준, 2000.

[3] "BS7799 PD3002 : Guide to BS7799 Risk Assessment and Risk Management".

[4] Bell D.E., LaPadula L. J., 'Secure Computer Systems : Unified Exposition and Multics Interpretation", The MITER Corp., 1975.

[5] Edward Rarkely, NISTIR 4325, Risk Asses-sment Methodology, 1990.

[6] NISTIR 4387, " Simplified Risk Analysis Guideline", NIST,1990.

[7] "IT Baseline Protection Manual", GISA, 2000.

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

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

[10] Biba K. J., "Integrity Considerations for Secure Computer Systems", ESD-TR-76-372, The MITRE Corp., 1977.

[11] Donald L. Pipkin, "Information Security Protecting the Global Enterprise", HP, 2000.

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

[13] "SSE-CMM : Model Description Documen-t Chapter Ⅲ", 1999.

저 자 소 개

김 강

OA학회 논문지 제6권 제4호 참조

현재 강원관광대학 컴퓨터정보계열 부교수

박 진 섭

1987년 중앙대학교 전자계산학과(학, 석, 박사)

현재 대전대학교 컴퓨터공학부 교수

관심분야 : 시스템 보안

김 봉 희

1984년 중앙대학교 전자계산학과(석사)

1999년 대전대학교 컴퓨터공학부 박사수료

2002년 한남대학교 전산원교수