Journal of the Korean Institute of Industrial Engineers
Vol. 28, No. 1, pp. 44-56, March 2002.

효율적 국내 정보기술 보안을 위한 위험관리 모형

안춘수† · 조성구

동국대학교 산업시스템공학과

A Risk Management Model for Efficient Domestic Information Technology Security

Choon-soo Ahn · Sung-Ku Cho

Department of Industrial Engineering, Dongguk University, Seoul, 100-715

For the risk analysis and risk assessment techniques to be effectively applied to the field of information technology (IT) security, it is necessary that the required activities and specific techniques to be applied and their order of applications are to be determined through a proper risk management model. If the adopted risk management model does not match with the characteristics of host organization, an inefficient management of security would be resulted. In this paper, a risk management model which can be well adapted to Korean domestic IT environments is proposed for an efficient security management of IT. The structure and flow of the existing IT-related risk management models are compared and analysed, and their common and/or strong characteristics are extracted and incorporated in the proposed model in the light of typical threat types observed in Korean IT environments.

Keywords: risk management, risk analysis & assessment, information technology security management

1. 서 론

사회전반에 걸쳐 정보화가 급진전되면서 조직의 정보체계에 대한 의존도가 갈수록 높아지고 있으며, 정보체계는 효율적인 조직활동의 수행에 있어 필요 불가결한 요소로 인식되어 가고 있다. 이에 따라 정보보호의 필요성은 정보시스템환경에서 특히 중요해 지고 있으며, 정보자산이 조직에서 차지하는 비중이 증대됨에 따라 고의 혹은 실수로 인한 정보자산의 변경, 파괴, 불법적 공개 등으로 인한 손실로부터 정보를 보호할 필요성이 대두되고 있다.

따라서 많은 조직들은 정보시스템에 대한 각종 보안 솔루션을 도입하거나 추진중에 있으나, 이들 대부분은 정보시스템에 대한 보안관리 체계없이 운영되고 있다.

즉, 효율적인 정보기술 보안관리를 하기 위한 핵심적 기능인 위험분석 및 위험관리가 제대로 이루어지지 않고 있는 실정이다. 또한 정확한 위험분석 및 관리기법을 사용하더라도 전반적인 위험분석 모형이 조직의 특성에 맞게 구성되어 있지 않다면, 시간과 비용의 비효율성은 물론 분석결과의 신뢰도가 떨어지는 결과를 초래한다. 이로 인하여 위험수준 감소를 위한 대응책의 적용 및 평가에 영향을 끼치고, 이는 보안정책의 수립으로 이루어지는 보안관리 주기의 연속성을 저해한다 (Lee and Lee, 1999; NCA, 1996).

따라서 본 논문에서는 정보기술 보안대책 중 관리적 대책의 핵심인 정보기술 보안 위험관리 모형을 개발하고자 하였다. 먼저 국외의 대표적인 위험분석 및 관리모형들과 국내의 한국정보통신 기술협회에서 제시한 위험분석 모형을 비교하여 각 모형들의 특징과 흐름, 구조 등을 분석하고 공통분모를 도출하였다.

그리고 각 모형들의 비교분석 결과와 장점들을 수용하고, 국내외의 위협유형을 비교 분석한 결과를 토대로 국내의 환경에 적합한 정보기술 보안 위험관리 모형을 제시하였으며, 본 연구에서 제시된 모형을 통해서 국내 정보기술 보안위험분석 방법론을 개발하여 적용하는 데 밑거름이 될 수 있게 하고자

† 연락저자 : 안춘수, 서울시 중구 필동 3가 26번지 동국대학교 산업시스템공학과, Fax : 02-2273-9522, e-mail : sooahn@dongguk.edu
2001년 4월 접수, 1회 수정(7주 소요) 후, 2001년 12월 게재 확정.

하였다.

2. 정보기술 보안 위험관리

2.1 정보기술 보안관리와 위험관리

정보기술 보안관리란 정보시스템이 제공하는 정보와 서비스에 대해 적절한 수준의 비밀성, 무결성, 가용성 및 인증성과 책임추적성을 유지하는 과정이며, 보안 위험분석 및 관리 기능은 정보기술 보안관리의 핵심적인 기능으로서 자산에 대한 보호를 체계적으로 수행하기 위해 자산을 식별하고 이 자산이 위협으로부터 어느 정도 위험에 처해 있는가를 측정하여 위험수준을 적절한 정도로 낮추기 위한 보안대책을 선정하는 활동이다(BSI, 1998; ISO/IEC, 1996; NIST, 1994). 일반적인 정보시스템 보안관리 모형은 <그림 1>과 같다(CCTA, 1998; ISO/IEC, 1996; ISO/IEC 1997).

일반적으로 보안 위험관리는 위험분석과 위험평가로 구분이 된다. 위험분석은 정보시스템과 관련된 자산, 위협, 취약성, 영향을 조사하여 어느 정도의 위험이 존재하는지를 측정하는 분석기술로서, 구축 대상 시스템에 영향을 미칠 수 있는 다양한 위협, 취약점을 식별하고 이로 인해 예상되는 손실 및 영향을 분석하여 목표 보호수준에 도달하기 위한 적절한 보호 메커니즘을 선택하는 과정이다.

그리고 위험평가는 위험의 수준을 낮추려는 활동으로 어느 정도 위험수준이 완화되었는지, 보안대책 구현 후에도 잔류위험을 감당할 수 있는 수준인지를 평가한다(Kang, 1998; Lee and Lee, 1999; ISO/IEC, 1996; NIST, 1999).

2.2 정보기술 보안 위험분석 요소

위험분석을 수행하는 데 있어서 주요한 요소로는 자산, 위협, 취약성, 영향, 위험, 대응책 등이 있다. 보안관리의 전체 흐름에 핵심이 되는 위험분석 요소들의 상관관계는 <그림 2>와 같으며 이를 정리하면 다음과 같다(ISO/IEC, 1996; ISO/IEC, 1997).

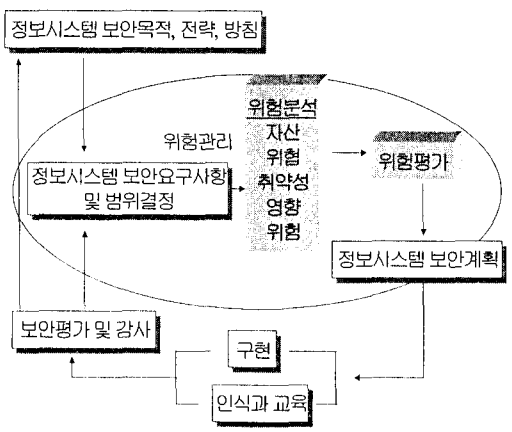

그림 1. 정보시스템 보안관리 모형.

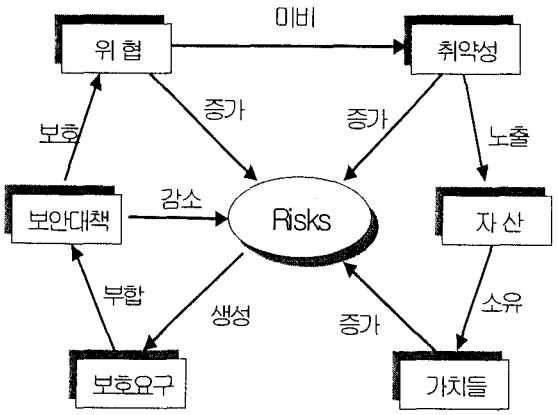

그림 2. 위험분석 요소들의 상관관계.

(1) 수많은 위협요소는 위험의 원천으로 취약성을 이용하여 전산자원에 손상을 입힌다.
(2) 취약성은 자산이 잠재적으로 갖고 있는 약점 또는 위협의 공격을 방지할 수 있는 보안대책의 미비로서 위험을 증가시키고 전산자원의 결함을 유발한다.
(3) 전산자원의 결함에 의해 정보기술 보안 목적에 손상을 입히는 경우에 대한 대응조치는 보안대책이다.
(4) 위험은 보안대책이 존재하지 않는 취약성으로 인해 발생하는 기대 손실이다.
(5) 보안대책은 위험을 감소시킨다.
(6) 보안대책은 하나 이상의 취약성을 감소시키며 위협요소로부터 자산을 보호한다.
(7) 보안대책은 그 자체가 내부적으로 취약성을 지니고 있으며 효율적이지 못할 수도 있다. 이때 남아 있은 위험을 잔여위험이라 한다.

3. 정보기술 보안 위험관리 모형

3.1 기존의 정보기술 보안 위험관리 모형

위험관리 모형은 위험관리의 전반적인 흐름을 나타내는 위험관리 구조도이다. 이 모형을 통하여 분석 작업들의 적용순서, 필수적인 작업 요소, 적용될 위험분석 기법들이 결정된다.

(1) ISO/IEC에서 제시한 위험분석 모형(ISO/IEC, 1996; ISO/IEC, 1997; ISO/IEC, 1998; ISO/IEC, 2000)
이 위험분석 모형은 정보시스템 보안을 위한 일반적 모형으로서 위험분석의 기법을 사용자가 자유롭게 채택할 수 있도록 하였다. 자산의 가치 산정 및 자산간의 관계와 현 대응책 조사, 취약성 분석, 위협분석을 동시에 수행하도록 되어 있고, 위험분석 전략 선택으로 기본통

제 접근, 공식적 접근, 상세 위험분석, 혼합접근을 제시하여 사용자가 자유롭게 선택하도록 하였다.

(2) 미국 NIST의 위험분석 모형(NIST, 1994)
사용자의 환경이나 목적에 상관없이 적용할 수 있는 일반적인 위험분석 모형으로서 위험분석 수행시 필요한 절차와 순서, 유의점 등 전반적 흐름을 제시하였다.

(3) 영국 CCTA의 위험관리 모형(CCTA, 1998)
위험분석과 위험관리를 서로 독립된 영역으로 구분한 대표적 정성적 위험분석 방법론으로 보안 시스템 설계시 위험분석을 적용하도록 하였으며 크게 시스템 모델화, 위험분석, 위험관리로 구분하였으며 적절한 보안대책을 식별할 때 보호체계의 유형을 회피, 이전, 위험의 감소, 취약점의 감소, 영향의 감소, 탐색, 복구로 나누어 보호체계를 선택하게 하였다.

(4) 한국 TTA의 보안 위험분석 모형(TTA, 2000)
국내 공공정보시스템 보안 위험분석의 표준이 되는 모형으로서 정량적 분석과 정성적 분석 모두를 활용하였으며 위험분석시 업무처리절차를 고려할 수 있도록 함으로써 정보시스템 환경이 업무의 관점에서 고려되고 있는 현실을 반영한 위험분석 모형이다.

(5) 미국 에너지성(DoE)의 위험분석 모형(NIST, 1989)
이 모형은 수작업을 위주로 구현하였으며 정량적 분석 방법을 배제한 모형으로서 위험분석의 경험이 없는 조직에서 적용하기 용이하다. 그러나 정성분석을 위한 각종 변수(상, 중, 하) 등으로 주관적 평가를 한다는 단점이 있으며 자산의 파악시 증거자료의 검토가 요구된다.

(6) 미국 법무성(DoJ)의 SRAG(NIST, 1990)
위험분석 수행시 간단히 수행할 수 있는 단순화된 위험분석 모형으로서 조직의 특성에 맞게 위험분석 방법론이 이미 구성되어 있어, 모형이 이러한 방법론에 근거한다. 이 모형은 특정 위험분석 기법을 사용하지 않으며 시스템의 위협과 손실에 대한 평가만 수행하여, 법무성 정보시스템에 적용할 수 있는 최소 보안 요건이 만족하는지를 신속하게 알아내도록 하였다.

(7) Sergio의 위험분석 모형(LRAM)(Sergio B. Guarro, 1987)
이 모형은 대형 및 통합 정보시스템의 보호설계와 관리를 위한 포괄적인 의사결정 및 위험관리 지원 방법론으로, 다른 모형과 다른 점은 총위험수준을 도출하지 않고 단일 사건 손실의 발생과 관련된 개별 위협요소에 의해 야기된 위험만을 도출한 모형이다.

3.2 기존 위험분석 및 관리 모형의 비교분석

위험분석 및 관리 모형의 흐름면에서 비교하여 보면 앞에서 기술한 7가지의 모형 중 NIST와 ISO/IEC, CCTA, 한국정보통신 기술협회(TTA)의 위험분석 및 관리모형은 사용자의 특성이나 목적에 상관없이 일반적인 위험분석 및 관리모형의 전체적 흐름을 잘 제시하고 있다. 그러나 위험분석의 범위가 광범위하고 모형의 구조가 복잡하여 시간과 비용의 증가로 위험분석의 경험이 없는 조직에서의 적용이 어렵다. 특히, NIST, CCTA 모형은 세부적인 분석기술이 나타나 있지 않으므로 적용할 조직에서 자기 조직의 위험분석 흐름(process)을 표준에 맞추어 재정립해야 한다.

반면에 DoJ와 DoE의 위험분석 모형은 조직의 최소 보안 요구조건이 잘 만족되고 있는지를 알아보기 위한 모형으로 흐름을 단순화함으로써 시간과 비용의 감소로 적용이 쉬우나 위험관리를 하기 위한 필수작업 요소들이 많이 생략됨으로써 분석결과에 대한 정확성을 신뢰하기가 어렵다는 단점이 있다.

위험분석시 필수 작업 요소인 자산분석, 위협분석, 취약성분석, 위험분석, 보안대책 등의 반영 여부 면에서는 ISO/IEC, CCTA, 한국 TTA의 위험분석 및 관리 모형은 필수작업 요소들이 잘 반영되고 있으나, NIST의 모형은 ISO/IEC 모형과 달리 기존대응책 조사와 제약조건에 대한 조사활동이 빠져 있다. 대응책에 관한 조사와 정상작동 여부에 관한 확인은 추후 대응책을 선택할 때 불필요한 작업과 추가비용을 줄이기 위한 것으로 반드시 확인해야 할 작업 요소이다. 적용중인 대응책이 동작 안 될 경우, 취약성의 원천이 될 수 있으며 또한 적용중인 대응책이 있는 줄 모르고 대응책을 중복 구현한다면 자원의 낭비를 초래할 수 있기 때문이다.

Sergio의 LRAM 모형은 조직의 총위험수준 도출과정이 빠져있으며 DoJ의 모형은 조직 시스템의 위협분석과정만 반영함으로써 시스템 손실에 대해서만 평가하였다. 또한, DoE의 모형은 위협분석, 취약성분석 과정만을 반영하여 조직의 보안요구사항을 만족하는 보안대책을 선택한 모형이다. CCTA 모형은 보안시스템을 설계할 경우에 적용가능한 모형으로서 필수요소들이 잘 반영되고 있으나 위협분석 및 취약성 분석, 보안대응책 도출 과정이 복잡하다는 단점이 있다.

모형의 적용 규모면에서 ISO/IEC, NIST, CCTA, LRAM 모형은 대형 정보시스템 위험분석 및 관리에 적용가능하며 DoE, DoJ 모형은 위험분석 경험이 없는 조직에서 적용시 유리하다. 특히, CCTA, TTA, NIST 모형은 설계목적을 국가기관, 대학, 연구소 등과 같은 공공기관을 적용대상으로 하였다. 이는 기업에서의 정보기술 목적과 공공 정보기술에서의 정보기술의 목적이 다르기 때문에 일반 기업에서 적용시 모형의 구조도를 조직에 맞도록 각 정보시스템에 대한 보안 위험관리가 따로 이루어져야 할 것이다.

위험분석 방법면에서 정량적인 방법과 정성적인 방법을 혼합하여 사용하는 것이 가장 효율적이지만, 과거자료 부재 등으로 인한 이유로 CCTA, LRAM, DoE의 모형은 정성적인 방법위주의 분석 방법을 사용하고 있다. 반면에 ISO/IEC, NIST, DoJ, TTA의 모형은 두 분석 방법을 혼합하여 사용하고 있다.

표 1. 기존의 위험분석 및 관리 모형의 특징

위험분석모형	특 징 및 장 단 점
ISO/IEC	· 전체적인 흐름은 명확 · 세부적 기술은 자유롭게 선택 · 자산 간의 관계와 적용중인 대응책 조사, 취약성분석, 위험분석을 동시에 수행
NIST	· 일반적 흐름을 제시, 범용모델로 사용 · 기존 보안정책의 조사과정과 제약조건에 대한 조사활동이 없다
DoJ	· 위험분석 방법론이 이미 구성 · 시스템의 위협과 손실에 대한 평가만 수행 · 최소보안여건의 만족도 확인 모형 · 과거데이터 불필요, 비용절감과 시간단축의 효과가 크다. · 정확성이 낮으며 필수위험요소 없음
DoE	· 수작업 위주로 구현, 정량분석 방법을 배제 · 간단하고 이해하기 쉬운 모형, 정성적 위험 분석 기법 사용 · 많은 분석 시간 요구
CCTA	· 정성적 위험분석 기법사용 · 자동화 도구사용으로 비용절감, 시간 단축 · 정성적 표현에 대한 해석 중요 · 보안 시스템 설계시 적용 가능
LRAM	· 포괄적 의사결정에 대해 근거를 제시 · 단일 손실에 대한 위험 도출 · 총위험수준 파악 불가능
한국 TTA	· 정성적 위험분석 방법 위주의 모형 · 필수작업 요소들이 잘 반영 · 위험분석시 업무처리 절차를 고려함

각 모형들을 비교 분석하여 도출된 공통분모와 장점들을 정리하면 <표 1>과 같다. 일반적으로 위험분석과정은 자산분석, 위협분석, 취약성분석을 거치며 잔존위험의 평가와 보안대응책 결정과정을 위험평가로 구분하였다. 또한 위험분석과 관리를 독립된 영역으로 제시한 모형도 있었으나 일반적으로는 위험관리 과정 안에 위험분석 과정을 포함시켰으며 특수상황에 따른 모형보다는 일반적인 상황에 적용할 수 있는 모형들이 공통분모로 도출되었다.

4. 국내 정보기술 보안 위험관리 모형의 제시

4.1 국내의 정보시스템 환경

최근 정보시스템에 대한 보안사고가 국내에서도 점차 증가하고 있으며 사회 문제화되자 각 조직들은 방화벽 등 보안 솔루션을 도입하거나 정부 지침에 의거 보안을 강화하는 노력을 기울이고 있다. 그러나 통제위주의 관리이거나 보안관리를 하더라도 너무 광범위하고 포괄적인 지침으로 인해 체계적이고 효과적인 보안관리가 이루어지지 않고 있는 실정이다. 또한 보안관리의 핵심인 정보시스템의 위협을 막기 위한 위험분석을 운용하는 기업도 많지 않은 실정이다.

즉, 국내의 정보시스템 현실은 정보시스템 보안 위협에 대한 유형과 새로운 정보기술에 대한 위협요인을 파악하기 어려우며, 오랜 시간 및 자금 소요 등의 원인으로 정보기술에 대한 위험분석 및 관리가 회피되거나 무시되어 왔으며 보다 정확한 위험분석을 수행하기 위해서는 해당 조직에서 발생한 보안사고에 관한 과거자료가 있어서 이를 기초로 정량적인 분석방법을 사용해야 하지만 이러한 과거 자료가 부실한 실정이다 (NCA, 1996; NCA, 1998).

또한 국내에서의 위험관리에 대한 연구가 미비한 실정으로 인해 많은 조직에서는 국외의 위험분석 및 관리 모형을 적용하고 있으나 정보기술 환경에 따른 차이로 인해 분석 결과의 정확성을 인정하기 어려우며, 국내 조직의 정보자산에 대한 정보유출의 위험성이 크고 비용증가의 원인이 되므로 적용하기 곤란한 상황이다.

4.2 국내 정보시스템 위협의 분석 및 분류

4.2.1 일반적인 정보기술 보안 위협

시스템이 안고 있는 구조적 문제인 정보시스템 위협은 정보기술의 역기능으로서 컴퓨터 범죄, 컴퓨터 자체의 결함, 운영자의 실수 등이 있으며 정보시스템 운영상의 위험을 통제하기 위해서는 시스템의 취약성과 그것을 교묘히 이용하는 위협에 대해 알고 있어야 한다. 즉, 정보기술 보안 위험분석 과정에서 가장 중요한 처리과정 중 하나가 위협분석이다(NIST, 1999).

위협은 조직, 시스템, 자산에 예상치 못한 피해를 초래할 잠재성을 갖고 있다. 이러한 피해는 위협이 정보기술 시스템이나 서비스가 처리하는 정보를 직 · 간접적으로 공격하기 때문에 발생한다.

4.2.2 국내의 정보기술 보안 위협

국내 정보시스템 조직들은 위협에 대한 유형피해를 발견하지 못하거나 대외적인 평판이 나빠지는 것을 우려하여 조직내에서 발생한 정보시스템 손실을 숨김으로서 위협으로 인해 발생하는 손실에 대한 예측이 불가능한 실정이다.

위협은 일반적으로 의도적 · 비의도적 · 환경적 위협으로 크게 나누어진다. 비의도적인 위협이나 환경적 위협은 국외와 국내 간에 차이가 없으므로 본 연구에서는 의도적인 위협에 대해서만 조사를 하였다. 의도적인 위협이란 정보시스템을 변경하여 재산을 부정한 방법으로 획득하거나 귀중한 정보를 파괴 또는 불법으로 취득하는 컴퓨터 범죄에 해당하는 위협으로서 다른 위협보다 정보시스템의 역기능을 주도하는 중요한 문제점으로 대두되고 있다(Kim and Nam, 1994; NCA, 1996; ISO/IEC, 1997).

국내에서 발생된 정보시스템 위협의 현황은 <표 2>와 <표 3>, <표 4>, <표 5>와 같다. <표 2>는 1973~1994년, <표 3>은 1995~1996년까지의 위협유형을 나타내었으며, <표 4>는 1998년 1/4분기 동안에 발생한 위협유형으로 전체 40건 중에서 내부자에 의한 정보 오남용은 14건으로 약 35 %를 차지하였다(NCA, 1996; KISA, 1998). 그리고 <표 5>는 1999~2000년도에 발생된 위협유형을 나타내었다(KISA, 1999; KISA, 2000).

표 2. 국내 정보기술 위협사례 유형별 분석(1973~1994)

사례유형	1973.1.1~1992.10.23	1992.10.24~1994.12.31	계
자료유출		12	12
자료 및 프로그램 변조	5	5	10
자료 부정 입력	38	17	55
컴퓨터 부정 사용		10	10
시스템 파괴 및 절도		3	3
자료 및 프로그램 절도		4	4
CD 범죄	4	2	6
기타(소프트웨어 불법 복제 및 바이러스)		65	65
자료부정 입수	3		3
콘솔 부정 조작	1		1
합 계	51	118	169

표 3. 국내 정보기술 위협사례 유형별 분석(1995~1996)

분류기준	사례유형	1995	1996	계
컴퓨터 주변 역기능 행위	자료유출	14	15	29
	정보기기관련	9	2	11
컴퓨터 처리과정 역기능 행위	내부자료 변조 및 파괴	14	17	31
	부정 정보처리	2	1	3
컴퓨터 활용 역기능 행위	해킹	17	14	31
기타 컴퓨터 관련 역기능 행위	금융관련	8	4	12
	비윤리적 행위	20	31	51
	컴퓨터 바이러스	6	26	32
	기타	10	8	18
	합 계	100	118	218

1970 · 80년대에는 은행이나 금융기관에서 단말기나 콘솔을 통한 데이터 조작이나 자료 부정 입력 등의 위협이 주를 이루었으나 1990년대에는 금융관련 범죄와 더불어 자료 유출, 해킹 사례가 발생하였다.

표 4. 국내 정보기술 위협사례 유형별 분석(1998 1/4분기)

사례유형	건 수	빈 도(%)
내부자 오남용	14	35
불건전 정보	8	20
불법복제	2	5
통신사기	8	20
바이러스	6	15
외부자 오남용	2	5
합 계	40	100

표 5. 국내 정보기술 위협 사례 유형별 분석(1999~2000)

위협유형	발생빈도	
	1999년	2000년
개인정보 및 프라이버시 침해	99.7%	95.4%
바이러스로 인한 시스템 손상	72.6%	52.6%
정보시스템의 불법 침입 및 파괴(해킹)	18.0%	20.1%
불건전 정보 유통	82.3%	81.0%
스팸메일	99.7%	46.1%
불법복제 및 지적 재산권 위협	66.8%	52.2%
전자상거래 관련 위협	22.6%	23.5%
기타(정보격차 및 인터넷 중독)	54.8%	77.3%

컴퓨터와 관련된 의도적 위협의 유형이 다양해짐에 따라 새로운 분류기준을 적용한 '95년과 '96년 사례들을 보면 PC통신을 이용한 비윤리적 행위가 가장 많았으며 해킹의 발생비율도 과거에 비해 많이 증가하였다. 또한 개인정보나 중요자료들이 쉽게 유출되는 사례가 빈번하였으며 자료유출 외에도 이를 조작하거나 변조하는 등의 사례도 증가하고 있다.

1990년대 후반부터는 정보통신기술의 발달과 인터넷의 발달로 인해 정보화 사회가 급속하게 발전함에 따라 전자상거래와 관련된 위협 등 새로운 형태의 위협들이 조합되어 나타나고 있는 실정이다.

또한 1998년도 후반부터는 내부자 오남용과 관련된 위협이 줄어든 반면 외부자와 관련된 위협과 더불어 개인정보 유출에 의한 프라이버시 침해 위협이 날로 증가하고 있다. 개인정보와 관련된 위협은 조직에서의 정보시스템과 별도로 생각할 수 있으나 개인정보의 보호는 스팸메일, 컴퓨터 바이러스, 해킹, 인터넷 사기 등 여러 가지 정보기술 위협의 방지를 위해 반드시 필요한 일이기도 하다. 기타 정보소외, 정보격차, 인터넷 중독, 언어오염 등의 위협들이 앞으로 심각한 위협이 될 것으로 예상된다.

반면, 미국의 경우 <표 6>에서의 결과에서 볼 수 있듯이 1998년 후반부터 정보통신기술의 발달과 인터넷의 보편화에

표 6. 미국의 정보기술 위협사례 유형별 분석(1999~2000)

위협유형	발생빈도	
	1999년	2000년
루트 침해(네트워크 침해, 해킹)	19.3 %	26.3 %
사용자 침해	3.6 %	17.1 %
정보절도 및 불법접근	13.8 %	23.1 %
바이러스	5.8 %	5.3 %
비인가 접근	7.9 %	12.4 %
잘못된 경보	0.7 %	3.9 %
서비스 거부	5.8 %	6.0 %
정보자원 오남용	2.0 %	3.2 %
사기	0.5 %	1.1 %
기타(알려지지 않은 위협)	10.6 %	1.6 %

따른 현상으로 각 조직이나 기관이 다른 조직과의 개방형 시스템으로 전환함으로써 내부자에 의한 위협보다는 외부자에 의한 위협사례가 날로 증가하는 현상을 볼 수 있다. 또한 새로운 양태의 위협 발생 가능성이 높아지고 있는 것으로 분석된다.

4.2.3 국내외 정보기술 위협간의 비교, 분석

위협의 분석은 정보기술 보안 위험분석의 핵심이 되는 과정으로서 위협의 발생빈도를 고려하여 분석하여야 하며, 아무리 치명적인 위협이라도 발생하지 않은 위협에 대해서는 고려하지 않는다. 국내에서는 자료 부족으로 인하여 선진국에서 발생한 위협을 이용하여 위협분석을 하고 있는 실정이다.

그러나 국내의 정보기술 환경과 선진국에서의 정보기술 환경이 다르고 위협 발생빈도나 발생하지 않는 위협에 대한 차이로 인해 효율적인 위협분석이 될 수 없다. 또한 효율적인 정보시스템 보안대응책 결정을 위해서는 국내 정보기술 환경에서의 정보기술 위협의 파악 및 분류가 선행되어야 한다.

따라서 국내 정보기술과 관련하여 최근에 발생한 위협을 유형별로 조사하고, 국외의 위협유형과 비교, 분석하여 본 연구에서 제시한 위험관리 모형에 적용하고자 정보기술 보안의 목적에 맞게 분류하고자 하였다.

미국 NIST에서는 현재의 컴퓨팅 환경과 앞으로 발전될 것으로 예상되는 위협의 유형 및 중요성에 바탕을 두고 폭넓은 관점에서 실수와 태만, 위조와 절도, 고용인의 파괴 행위, 기반구조 지원 및 물리적 손실, 악의적 해커, 산업스파이, 악성코드, 외국정부 스파이, 개인 프라이버시 침해 등으로 위협의 유형을 구분하여 분류하고 있다(TTA, 2000; NIST, 1999).

ISO/IEC에서는 위협을 138가지로 세분화하였으며 자산 분류기준에 맞추어 하부구조(infrastructure), 하드웨어, 저장, 소프트웨어, 통신, 인력 등으로 위협을 구분하였다(ISO/IEC, 1996). 영국 BS7799에서는 정보, 정보시스템 및 네트워크와 네트워크 서비스의 사용과 비인가된 접근, 사고를 유발하는 의도적인 소프트웨어, 소프트웨어 실패, 정보와 메시지의 비인가된 수정, 메시지의 전달, 화재, 절도, 스태프 실수 등으로 위협을 구분하고 있다(BSI, 1998).

국내에서 발생된 의도적 위협의 유형을 살펴보면 1970년대부터 1990년대 초기까지는 하드디스크 도난, 정보의 유출 등의 자료 유출 위협과 정보 기기의 도난 등의 정보 기기 관련 위협, 내부자료 변조 및 파괴 위협, 부정 정보처리 위협, 해킹 위협, 컴퓨터 바이러스 위협 등 개별적으로 발생하는 경향이 짙었으나, 1990년도 후반부터는 정보화가 진전되면서 정보기술 위협 유형은 좀더 다양해지고 광범위해 지고 있는 실정이다.

정보화가 진행되는 과정에서 나타나는 여러 양태 중 우리 생활을 방해하거나 정보화의 진전을 막는 유형을 몇 가지 범주로 나눠 볼 수 있는데, 본 연구에서는 일반적으로 정보화 역기능에 적용되는 정보시스템의 불법침입을 통한 정보 및 자료의 유출과 파괴 등을 유발할 수 있는 해킹, 바이러스 위협을 비롯하여 개인정보의 유출로 인한 프라이버시와 관련된 위협, 불건전정보의 유통, 지적재산권 위협, 생산성 저하 및 시간의 낭비를 초래할 수 있는 스팸메일 위협, 전자상거래시 발생하는 위협, 정보소외, 정보격차, 인터넷 중독 등의 기타 위협으로 분류하여 분석하였으며 분석결과를 정리하면 다음과 같다.

① 자료유출 위협 및 개인 프라이버시와 관련된 위협
이 위협의 대부분은 개인정보 유출과 관련된 것이며 금융기관에서 주로 나타난 위협으로 자료가 담긴 디스켓의 관리 및 자료 폐기처분의 책임을 명확히 해야 한다.
또한 1990년대 후반 정보통신 기술의 비약적인 발전과 인터넷 사용이 보편화됨으로써 개인 사생활의 노출 및 프라이버시 위협 등 사이버 범죄의 위험을 초래하고 있다.

② 정보기기관련 위협
물리적 보안과 관련된 위협으로 출입제한 및 통제 등의 관리적인 요소의 강화가 필요하다.

③ 내부자료 변조 및 파괴 위협
정보시스템 내부 관리자 및 정보처리자에 의해 발생되는 위협으로서 아직까지 국내에서는 금융기관에서 주로 발생되었으나 사실상 알려지지 않은 사례로 인하여 더 많은 조사가 필요하며 자료 사용자별로 물리적 접근 제한을 두어 신뢰할 수 있는 특정 사용자만 데이터 변경 및 삭제를 할 수 있도록 관리적인 대책이 시급하다.

④ 부정 정보처리 위협
전산망과 연결된 정보시스템에서 정확한 정보를 처리하지 못하여 생기는 위협으로서 정보의 정확한 검증에 대한 대책이 필요하다.

⑤ 해킹 위협
ID의 도용과 패스워드의 누설로 인해 전산망에 부당한 방법으로 접속하여 정보를 삭제, 변경하는 등의 사례가

대표적이며 백업과 파일의 접근통제 관리 등의 주기적인 사전보안을 실시해야 한다. 1990년대 후반에 발생한 사례를 보면 호기심 등에 의한 단순해킹에 그치지 않고 개인의 정보 및 회사의 정보를 이용한 사이버 범죄의 성향이 짙어지고 있는 실정이다.

⑥ 컴퓨터 바이러스 위협

인터넷의 발달과 전산망의 확대로 인해 PC통신을 이용한 바이러스의 유포나 소스코드를 공개한 사례로 인해 그 피해가 날로 증가하고 있다. 1973년부터 1992년 10월 23일까지 발생한 위협들 중에서 1992년 10월 24일 이후에 발생되지 않은 위협은 치명적이라 하더라도 발생되지 않았으므로 고려하지 않았다. 1990년대 후반 이후 해킹과 마찬가지로 호기심에 의한 단순 바이러스에 의한 위협이 아닌 타인의 정보 유출과 관련된 금전적 이익을 취하려는 경향이 증가하고 있다.

⑦ 전자상거래와 관련된 위협

전자상거래는 유형 및 무형의 상품에 대한 판매자와 구매자 사이의 온라인 거래로서 점차 일상생활의 수단으로 자리잡고 있다. 따라서 이와 관련된 위협이 새롭게 등장하였으며 개인정보 유출 및 사이버 사기 등의 위험이 증가하고 있다.

⑧ 기타 위협

19900년대 후반부터는 정보소외, 정보격차, 인터넷 중독 등의 위협이 발생하였으며, 이는 앞으로 심각한 사회문제가 될 것으로 예상된다. 이외에도 시간의 낭비 및 시스템의 부분 마비를 야기하는 스팸메일이 새롭게 등장하였다.

국내에서 발생된 위협을 정보기술 보안의 목적에 따라 분류함으로써 본 모형에서 제시한 단계 4의 위협분석과 단계 6의 초기 보안대응책 결정이 효율적으로 이루어 질 수 있다. 또한 정보기술 보안 목적에 따라 자산 및 위협의 중요도가 결정이 되며 더불어 위험의 순위도 결정이 된다. 그러므로 위협원천이나 자산분류 기준에 따라 위협을 분류하기보다는 조직에서 정보기술 보안 목적의 중요도에 따라 위협을 분류하는 것이 정보기술 목표를 반영한 효율적 위험분석이 될 것이다.

분석된 위협들과 정보기술 보안의 목적인 가용성, 무결성, 비밀성, 책임추적성, 인증성과의 관계를 정리하면 <표 7>과 같으며 추후 이 분류에 대한 검증이 필요하다.

국외에서 발생된 위협의 발생빈도와 국내에서 발생된 위협의 발생빈도를 비교, 분석한 결과는 <그림 3>과 <그림 4>와 같으며 이를 정리하면 다음과 같다.

표 7. 보안 목적에 따른 위협의 분류

정보기술 보안목적	위 협
가 용 성	컴퓨터 부정사용, 시스템 파괴 및 절도, 자료 및 프로그램 절도, 정보기기 관련,
무 결 성	자료 및 프로그램 절도, 자료 부정 입력, 시스템 파괴 및 절도, 컴퓨터 바이러스, 내부 자료 변조 및 파괴, 해킹, 부정정보처리, 개인정보 및 프라이버시 위협, 지적 재산권 위협, 전자상거래 관련 위협
비 밀 성	자료 유출, 자료 및 프로그램 절도, 해킹, 개인정보 및 프라이버시 위협, 지적 재산권 위협, 전자상거래 관련 위협
책임추적성	전자상거래 관련 위협, 스팸메일
인 증 성	정보기기관련, 해킹, 전자상거래 관련 위협, 개인정보 및 프라이버시 위협

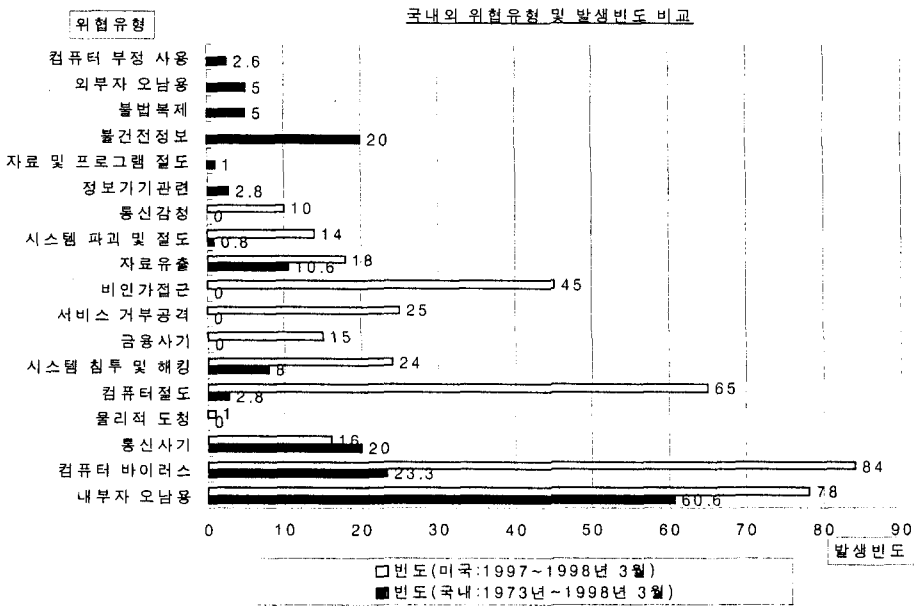

그림 3. 국내외 위협의 유형 및 발생빈도.

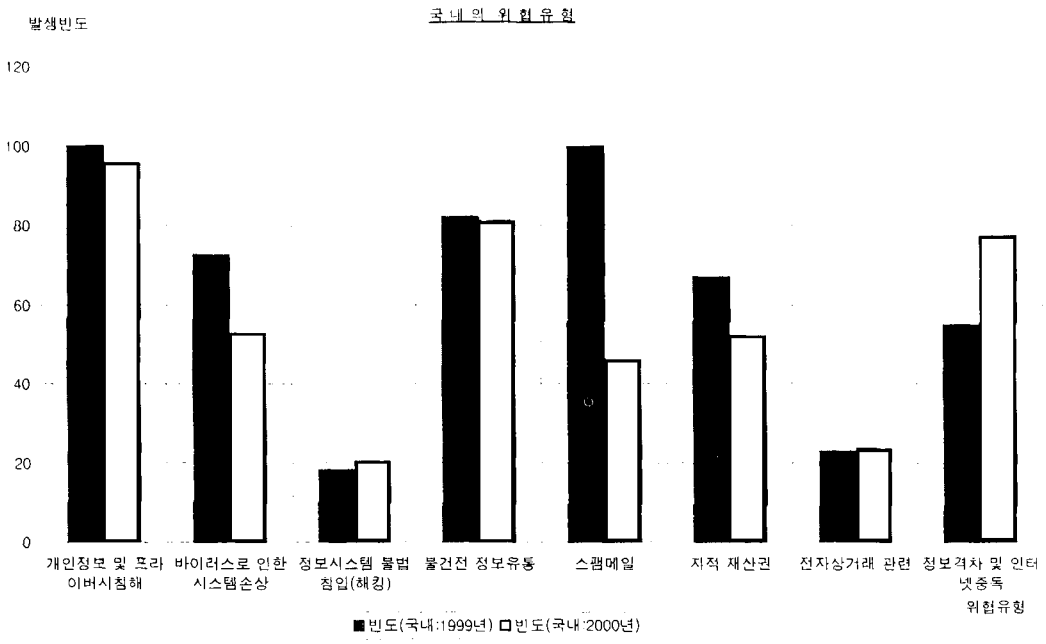

그림 4. 국내의 정보기술 위협의 유형 및 발생빈도.

① 정보시스템의 규모면에서 많은 차이를 보이고 있다. 즉, 위협발생 조직의 수에서 많은 차이가 나는데 미국 내에서 조사된 위협발생 조직은 1997년부터 1998년 3월까지 458개가 되는 데 비해 국내에서 조사된 발생건수는 1973년 1월 1일부터~1998년 3월까지 427개가 된다(NCA, 1996; KISA, 1998).

이는 국내의 많은 조직들이 각 조직에서 발생한 위협에 대해서 공개를 하지 않아서 생긴 현상이며 위협분석시 자료부재로 인해 효율적인 위협분석이 어렵다는 것을 나타내고 있다. 또한 국외의 정보기술환경이 국내의 환경보다 복잡하고 대규모 정보기술을 이용하고 있다는 것을 알 수 있다.

② 국내에서 발생된 위협과 국외에서 발생된 위협의 유형에 있어서도 많은 차이가 난다. 1990년도 초기까지 국내에

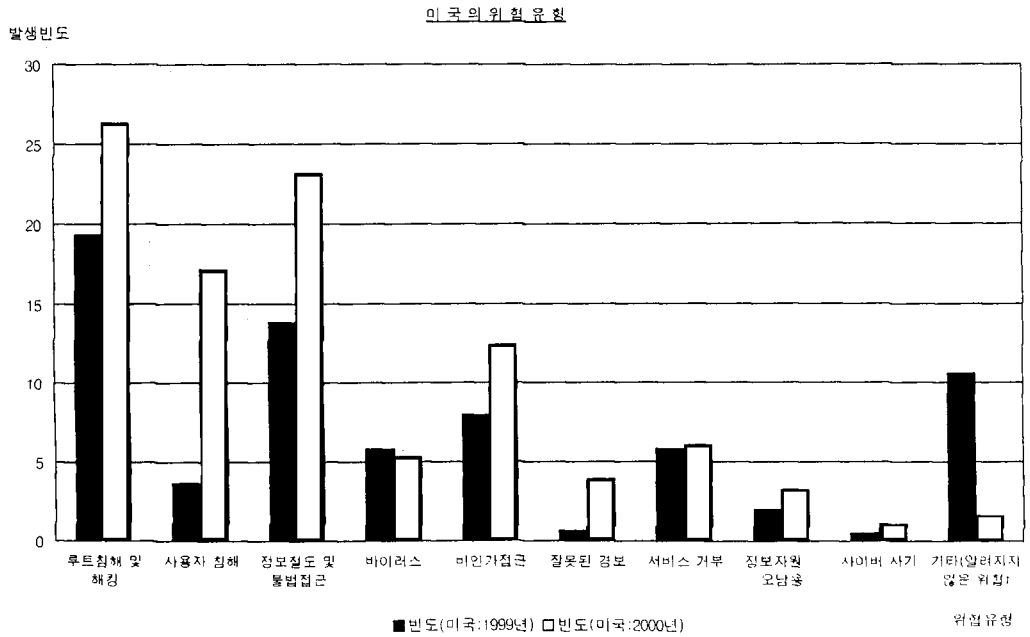

그림 5. 외국의 정보기술 위협유형 및 발생빈도.

서 발생된 위협은 내부자 오남용에 대한 발생빈도가 가장 높았으며 이는 국외의 현황과 비슷한 결과를 보이고 있다. 그러나 1990년도 후반부터 국내의 경우는 불건전 정보 유통 위협, 전자상거래 관련 위협, 정보격차 및 인터넷 중독 등의 위협 등이 새롭게 등장하였으나 미국의 경우는 잘못된 경보, 서비스 거부, 기타 알려지지 않은 위협에 대한 빈도가 높은 것으로 나타났다. 이는 축적된 과거 자료를 토대로 정보기술 위협에 대한 상세한 분류가 이루어져 있어 보다 효율적인 위협의 분석이 이루어지고 있음을 의미한다. 따라서 국내에서 발생한 정보기술 보안 위협과는 현실적으로 많은 차이가 난다는 것을 시사하고 있다.

③ 반면에 불건전 정보, 불법복제, 컴퓨터 부정사용, 외부자 오남용 등은 국내에서만 발생하는 위협으로 나타나고 있으며 특히 내부자 오남용과 관련된 위협 및 개인 프라이버시와 관련된 위협은 날로 증가하고 있는 실정이다. 이것은 아직까지 국내에서는 철저한 정보기술 보안시스템을 구체적으로 도입하지 않고 있는 데 반해 국외에서는 철저한 보안시스템의 적용으로 외부의 접근에 대한 보안면에서 많은 성과를 거두고 있다는 것을 의미한다.

④ 국외 정보시스템의 위협 유형들은 오랜 시간 동안 축적된 위협을 기초로 정리된 결과로서 환경이 다른 국내에서 이와 같은 위협이 발생되리라고는 볼 수가 없다. 또 발생빈도뿐만 아니라 발생되지 않은 위협에 대해서는 고려할 필요가 없으므로 자료가 부족한 국내 정보시스템에 외국의 위협유형을 적용하기에는 너무 광범위하며 효율적이지 못하다.

4.3 국내 정보기술 위험관리 모형의 제시

본 연구에서는 국내외의 각 위험분석 및 관리 모형들의 특징과 장 · 단점을 비교 분석하여 공통분모를 도출하였고, 국내 정보기술 위협과 국외 정보기술 위협의 비교분석을 통해 국내 정보시스템 위협환경에 적합한 위협분류기준을 제시하였다. 따라서 기존 위험분석 및 관리 모형들의 장점을 수용하고, 국내 정보시스템의 위험유형 조사 결과를 토대로 국내 정보시스템 환경에 적합한 위험분석 및 관리 모형을 개발하였다.

본 연구에서 제시한 정보기술 보안 위험관리 모형의 패러다임은 다음과 같다.

첫째, 조직의 정보시스템 환경에 맞는 보호 서비스를 제공하기 위해서는 정보기술 보안 시스템이 시스템 개발 과정과 통합하여 초기단계에서부터 수행하는 것이 중요하게 고려되어야 훨씬 경제적이므로(Lee and Lee, 1999; CCTA, 1998) 보안시스템 설계시 적용될 수 있도록 초기 보안정책 수립, 초기 위험분석을 통한 초기 보안대응책 선정, 새로운 보안대응책의 선정을 포함하는 위험평가 단계 등의 작업 요소 등을 추가하였다.

둘째, 정보기술 보안 위험분석 및 관리는 결국은 정보기술 보안관리의 한 부분(NIST, 1990; ISO/IEC, 1996)이므로 본 연구에서 제시한 모형도 정보기술 보안관리의 주기에 따르도록 설계하였다.

셋째, 정보기술 위험관리에 대한 연구가 미비한 국내 실정을 감안하여 특수한 상황에서의 위험관리보다는 일반적 상황하에서 적용될 수 있도록 전체적 흐름이 제시되면서 경험이 부족한 조직에서도 적용 가능하도록 모형의 흐름을 위험분석 단계와 위험평가 단계로 상세하게 설계하였다.

넷째, 정보기술 보안 위험분석 및 관리란 결국은 현 정보시스템의 효율성을 극대화하고자 하는 것이다. 따라서 본 모형에서는 위험분석과 위험관리를 따로 분리하지 않고 하나의 모형으로 통합하여 구조를 단순화함으로써 적용이 쉽도록 설계하였다.

다섯째, 조직 내의 정보시스템은 다양하고 복잡한 시스템을 가지고 있다. 따라서 위험분석 수행시 많은 시간과 비용으로 인해 위험관리가 회피되는 등 비효율적으로 운영되고 있는 실정이다. 이와 같은 단점을 극복하고자 조직 내의 정보시스템을 규모와 중요도에 따라 파악하여 위험관리의 효율성을 높일 수 있도록 설계하였다.

여섯째, 각 조직은 최상의 보안관리를 목표로 하지만 비용의 제한이라는 제약조건이 존재한다. 따라서 예산의 제약으로 인한 제한된 비용하에서 최적의 효과를 얻을 수 있도록 하기 위해 비용효익분석 단계를 포함시켰다.

일곱째, 정보기술 보안 위협에 대한 과거자료의 부재로 인한 국내 정보시스템 환경을 고려하여 정성적 분석 방법 위주의 위험분석 중심으로 모형을 설계하였다.

위에서 언급한 7가지의 패러다임을 토대로 제시된 위험관리 모형의 전체적인 흐름도는 다음과 같다

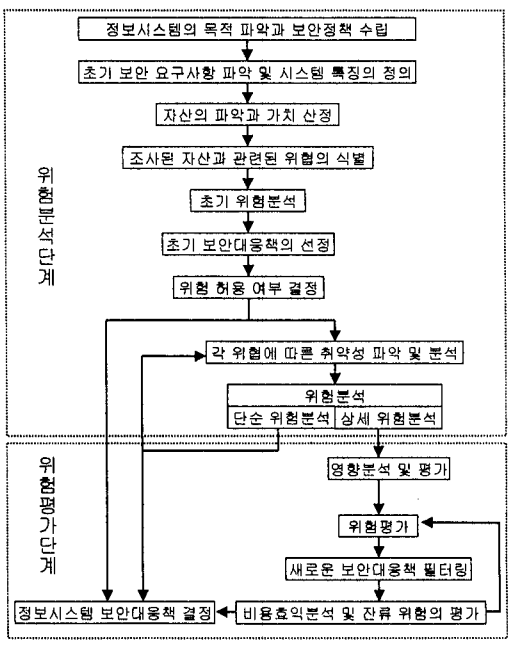

그림 6. 제시된 위험관리 모형의 흐름도.

(1) 단계 1 : 정보시스템의 목적 파악 및 보안정책 수립

정보시스템의 목적은 대량 데이터의 신속·정확한 처리, 서로 다른 업무나 프로세스의 다양한 데이터 처리, 양질의 데이터 처리 등 다양하다. 이와 같은 목적 중 어디에 초점을 맞추느냐에 따라 정보시스템의 역할 및 유형이 달라지며 정보기술 보안관리 및 보안정책이 결정된다(BSI, 1998).

보안정책이란 시스템 보안 개발시 첫 단계로서 조직의 정보자산을 어떻게 관리하고 보호할 것인가에 대한 지침과 규약을 기술해 놓음으로써 위험관리를 통해 보안대응책을 결정할 때 표준자료로 제공된다.

따라서 단계 1을 통해 위협 및 위험 분석의 범위를 결정할 수 있으며, 시스템의 중요도를 결정할 수 있는 기초 자료의 제시는 보안시스템 개발의 초기단계이다.

(2) 단계 2 : 초기 보안 요구사항 파악 및 시스템 특징의 정의

정보시스템 사용자들을 대상으로 초기 보안 요구사항을 식별한다. 효과적인 요구사항 수집을 위해 현 시스템의 운영환경 및 정보보안 특성의 파악 등 시스템의 특징을 정의함으로써 보안 시나리오 작성의 기초가 될 수 있다.

이 단계도 단계 1에서와 같이 보안시스템 설계시 위험관리를 적용하기 위한 기초적인 단계로서 기 구축된 정보보안 시스템에서도 적용할 수 있다는 특징이 있다. 또한 시스템의 운영환경 및 조직의 보안 특성 파악 등 시스템의 특징을 정의함으로써 단계 1에서의 결과와 더불어 위험분석의 범위 및 분석방법을 결정하는 데 중요한 단계가 된다.

(3) 단계 3 : 자산의 파악과 가치의 산정

자산의 분석은 정보기술 보안 위험분석의 핵심으로 조직의 자산이 식별되지 않는다면 성공적인 보안 위험관리가 이루어질 수 없으며 더불어 효율적인 보안정책이 수립될 수 없다.

따라서, 본 단계에서는 조직에서 가치가 있는 모든 자산을 파악함으로써, 즉 자산별로 조직에서의 정보기술 목적과 초기 보안 정책 간의 관계를 토대로 자산의 가치를 고려함으로써 초기 위험분석의 범위를 결정할 수 있는 자료를 제공한다. 또한 현재의 자산가치를 파악하여 위협분석의 범위를 결정할 수 있다. 자산의 파악 및 분석의 수준은 단계 1과 2의 결과에 기초하여 결정되어야 한다.

(4) 단계 4 : 자산과 관련된 위협의 식별

단계 3에서 파악된 자산분석 결과를 토대로 가치가 있는 자산과 관련된 위협을 식별함으로써 초기 위험분석의 기초 자료를 제공한다. 위협의 식별 및 분석에는 현 조직에서 발생했던 과거 자료 또는 다른 조직에서 발생한 적이 있는 자료가 필요하다.

따라서 본 연구에서는 국내외 정보기술 위협 중 정보기술과 관련된 의도적 위협분석에 대한 비교분석 결과를 토대로 국내 환경에 적합한 위협분석을 제시하였다.

(5) 단계 5 : 초기 위험분석

단계 3과 4에서의 결과를 토대로 위험분석의 시간과 비용을 줄이기 위한 초기 위험분석을 실시한다. 즉, 조직에서 세운 최소 보안 요구사항을 만족하고 있는지에 대해서 자산의 손실과 시스템 위협의 손실 크기를 측정하여 초기 보안대응책 결정의 자료를 제공해 준다.

이 단계는 보안시스템을 설계하고자 하는 경우나 위험분석의 경험이 없는 조직에서 시간과 비용을 줄이고 위험분석의 범위를 최대한 줄여 조직의 보안 요건에 만족하는지에 대한 평가를 하는 단계이다.

(6) 단계 6 : 초기 보안대응책의 선정

초기 위험분석을 통해 산출된 결과를 토대로 초기 보안대응책을 선정한다. 즉, 위협의 손실 및 자산의 손실 크기를 예측하여 초기 보안대응책을 선정하고 기존의 보안대응책과 비교하여 최소한으로 만족할 수 있는 보안관리를 결정하는 단계이다.

즉, 이 단계는 가장 간단하고 기본적인 위험분석을 실시하는 단계로서 단계 5와 더불어 처음 위험분석을 실시하거나 보안시스템 설계시에도 필요한 단계라고 할 수 있다.

(7) 단계 7 : 위험허용여부 결정

단계 6에서 도출된 보안대응책이 현 조직의 위험을 허용할 수 있는 수준인지 아닌지 위험허용여부 평가를 통해 허용될 수 있는 수준의 보안대응책이라면 단계 14로 이동하여 현 조직의 정보시스템 보안대응책으로 결정을 한다. 만약 허용될 수 없는 수준의 보안대응책이라면 새로운 보안대응책을 결정하기 위하여 위험분석을 하기 위한 단계 8로 이동한다.

(8) 단계 8 : 취약성 파악 및 분석

취약성은 위협에 의해 야기될 수 있는 자산 내의 약점으로서 위험분석시 고려되어야 할 필수요소 중 하나이다. 또한 취약성은 위협의 공격을 방지할 수 있는 보안대응책의 미비한 정도를 나타내므로 기존의 보안정책에서의 문제점을 파악하여 새로운 보안정책 결정시 기초자료로서 활용이 된다.

단계 8에서의 취약성 분석 결과와 단계 4에서의 위협분석 결과를 토대로 보안 시나리오를 작성한다. 보안 시나리오는 대상 시스템에서 발생할 수 있는 다양한 위협 및 취약성을 스토리로 체계화한 것(TTA, 2000)으로 가상적인 위협환경을 설정하고 발생 가능한 위협을 유추하여 위협을 찾아내어 취약성과의 관련성을 통해 조직에 나쁜 결과를 어느 정도 끼치는지를 알아내는 방법이다. 이 시나리오를 통하여 단순 위험분석과 상세 위험분석의 방법이 결정이 된다

(9) 단계 9 : 위험분석-단순 위험분석과 상세 위험분석 방법

이 단계는 실질적인 위험분석을 하기 위한 단계로서 단계 5에서의 결과와 취약성분석을 통해 얻어진 위험분석 수준을 토대로 단순 위험분석과 상세 위험분석 중 하나를 결정한다. 즉, 위협의 손실이 크지 않거나 이로 인해 자산의 손실 및 가치가 크지 않다면 단순 위험분석을 실시함으로써 시간과 비용이 많이 드는 상세 위험분석을 수행할 필요가 없을 것이다. 또한 초기 위험분석을 통해서 정보기술의 조직 규모가 크고 중요시스

템에 대한 자산 및 위협의 손실이 클것으로 예측된다면 보다 정확한 상세 위험분석을 실행해야 할 것이다.

위험분석은 조직의 자산이 위협으로부터 얼마나 취약한지 위험의 수준을 측정하는 방법이다. 초기 위험분석과 초기 보안정책의 평가 결과를 통해 최소한의 정보기술 보안 요구사항을 토대로 보안 정책을 결정할 것인가 아니면 시스템의 중요성과 조직의 정보보안 수준에 따라 보다 정확하고 상세한 위험분석을 할 것인가를 결정하여야 한다. 즉, 초기 위험분석을 통해 도출된 보안대응책이 조직의 위험을 허용할 수 없는 수준이라면 보다 구체적인 위험분석을 실시해야 할 것이다.

따라서 본 연구에서는 위험분석의 단계를 초기 위험분석단계를 거친 후 단순 위험분석과 상세 위험분석단계로 세분화하였다. 즉, 대부분의 조직에서는 많은 정보시스템이 존재하며 조직 내의 모든 정보시스템을 대상으로 위험분석을 수행한다면 너무 많은 시간과 비용이 소요되어 효율적이지 못하기 때문이다. 이에 본 연구에서는 조직의 규모와 시스템 중요도, 보안정책에 따라 위험분석 수준을 3단계로 세분화함으로써 보다 유연하고 효율적인 위험관리를 할 수 있도록 하였다.

본 모형은 위험에 많이 노출된 정보시스템과 사업측면에서 매우 중요한 시스템을 파악하기 위해서 초기 위험분석을 먼저 수행 · 평가하여, 이 결과에 따라 단순 위험분석 또는 상세 위험분석 방식을 선택하도록 하였다.

단순 위험분석 방식과 상세 위험분석 방식은 국내에서 가장 많이 사용하고 있는 기본 통제 방식을 확장한 개념으로 기본 통제 방식은 정보기술 보안에 대한 전반적인 체계가 조직 내에 구축되어 있지 않은 경우, 즉 정보 보안대응책이 구현되어 있지 않거나 단기간 내에 조직에서 필요한 최소한의 보안 요구에 맞는 보안대응책을 구축하고자 할 때 이용될 수 있는 방법(ISO/IEC, 1997)으로써 정보기술 위험관리가 미비한 국내실정에 가장 적합한 실용적 위험분석 방법이다.

그러나 이 방법은 조직 내의 다양한 시스템과 각각의 시스템에서의 위험 및 다양한 보안 요구사항을 고려하지 못하고 있다. 즉, 각각의 시스템에 대한 정보 보안정책의 구축에는 적용하기 어려운 단점이 있다. 이러한 단점을 해결하기 위해 단순 위험분석 방식과 상세 위험분석 방식을 제안하였다. 이들 방식들은 자산과 관련된 위협식별을 통해 발생 가능한 위협을 도출하고, 이의 영향을 측정함으로써 초기 위험분석 방식보다는 좀더 포괄적인 위험분석 방식이 될 수 있다. 즉, 단계 5에서 설명하였듯이 각각의 시스템 중요도와 정보 및 데이터의 보안수준에 따라 단순 위험분석 방식을 적용할 것인지 또는 상세 위험분석 방식을 적용할 것인지 결정이 된다.

단순 위험분석 방식은 현 조직에서 요구하는 최소 보안 수준에만 적합하도록 함으로써 위험분석 절차를 단순화하여 보안 시스템 설계시 위험분석의 효과를 극대화하고 시간과 비용을 줄이고자 하거나 경험이 부족한 정보기술 환경하에서 필요한 분석 방식이라 할 수 있다. 상세 위험분석 방식이 단순 위험분석 방식과 다른 점은 위험평가 단계와 비용효익 분석단계를 별도로 분리함으로써 더욱 중요한 시스템에 대해서는 보다 세밀한 위험분석을 하도록 한 점이다. 그러나 시간과 비용이 많이 소요된다는 단점이 있다.

단계 9에서는 각각의 위협 발생빈도와 시스템의 취약성에 따른 손실에 대한 결과를 토대로 각 위험요소별로 확률분포가 도출될 수 있을 것이다.

(10) 단계 10 : 영향분석 및 평가

이 단계는 상세 위험분석을 통해 도출된 위험수준을 평가하는 위험평가의 첫 단계이다. 영향이란 보안사고가 자산에 미치는 예기치 않은 나쁜 결과로서 자산의 파괴, 가용성, 인증성, 비밀성, 무결성, 이용성의 상실, 조직의 이미지 손실 등을 말하며 이러한 손실 등을 분석 평가하여 감소시킬 수 있는 보안대책 선정의 기초자료로 활용된다. 즉, 위험의 가능성이 있는 자산의 피해를 분석하여 평균 기대손실 비용, 기대 효용 등의 기존의 위험평가방법들을 결정하여 어떠한 안전대책을 세울지를 검토하는 단계이다.

(11) 단계 11 : 위험평가

단계 11은 영향분석 및 평가를 통해 도출된 여러 가지의 보안대응책을 전체적으로 평가하는 단계로서 측정된 위험의 수준을 조직에서 원하는 수준으로 낮추기 위한 보안대응책을 선정하는 단계이다. 즉, 위험평가 단계에서는 정보기술 보안계획 수립시 기초가 되는 보안대응책의 프로파일을 제공한다.

정보기술 위협의 식별과 각 위협에 따른 취약성의 발생 가능성을 토대로 위협 및 취약성의 수준과 자산의 손실비용 및 기대 효용 등을 토대로 위험의 수준을 평가하고 각 조직 환경에 맞는 위험수준을 결정해야 한다. 또한 각 조직의 환경에 따라 위협의 발생빈도나 시스템의 취약성 수준이 다르고 위험에 따른 손실에 있어서도 많은 차이를 보이므로 본 모형의 사용자는 자신의 조직 환경에 맞는 위험평가 방법을 결정해야 할 것이다.

기존의 위험관리 모형에서는 이 단계를 위험분석 단계에 통합시켰으나, 본 모형에서는 독립된 프로세스로 분리함으로써 위험관리를 상세히 기술하였다. 이 단계는 기존의 보안대응책뿐만 아니라 새로운 보안대응책들을 전체적으로 고려하여 위험의 수준을 낮추기 위한 보안대응책을 평가하는 단계이다.

(12) 단계 12 : 새로운 보안대응책 도출

본 단계에서는 단계 11에서 구해진 많은 보안대응책에 대해서 조직에서의 정보기술 목적과 보안정책을 만족할 수 있는 조직에 적합한 새로운 보안대응책을 필터링 한다.

(13) 단계 13 : 비용효익 분석 및 잔류 위험의 평가

단계 12에서 제시된 보안대응책에 대해서 비용효과분석을 통하여 조직에 적합한 보안대응책인가를 평가한다. 또한 도출된 보안대응책이 남아 있은 잔류위험에 대해서 어느 정도 감당할 수 있는 대책인지를 평가하여 경영진의 정보기술 보안정책 의사결정시 관련 자료로 활용한다. 즉, 도출된 보안대응책

표 8. 제시된 모형에서의 위험분석 방식들의 특징

위험관리 방식	특 징
초기 위험분석	자산분석, 위협분석
단순 위험분석	자산분석, 위협분석, 취약성 분석
상세 위험분석	자산분석, 위협분석, 취약성분석, 영향분석
위험관리	위험분석, 위험평가, 보안대응책 결정

이 위험감소에 끼치는 공헌도를 제한된 비용하에서 비용효익 측면에서 평가하고 남아 있은 잔류 위험에 대해 보안대응책이 어느 정도 감당할 수 있는 수준인지를 평가하는 단계이다.

(14) 단계 14 : 정보기술 보안대응책 결정

위험분석과 위험평가로부터 측정된 위험과 보안대응책의 비용과 효과를 비교하여 조직의 정보기술 목적에 잘 부합되는 정보기술 보안대응책을 결정한다. 즉, 결정된 보안대응책이 위험의 잠재적 영향정도와 조직에서의 잔류위험에 대해 얼마나 감당할 수 있는 위험수준인가를 고려하여 조직의 정보기술 보안대응책으로 최종 결정하여야 한다.

본 연구에서 제시된 위험관리 모형에서 위험분석 방식들의 특징을 정리하면 <표 8>과 같다. 위험관리를 하기 위한 필수 작업 요소들의 포함여부에 따라서 위험분석의 수준을 결정하였으며 위험관리의 과정은 위험분석과 위험평가를 거쳐 보안대응책 결정까지를 포함하였다.

4.4 제시된 모형의 분석

본 모형은 국내 정보기술환경이 외국에 비해 열악한 데 따른 위험분석 적용의 어려움을 해소하기 위해 다양한 환경에서 수용이 가능하고, 객관적이면서 보편 타당한 위험관리 모형을 제시하는 것을 목표로 작성되었다. 이에 따라, 외국의 위험분석 및 관리 모형들을 분석하여 장점을 수용하고 공통분모를 추출하여 위험관리의 전체적 흐름을 제시하였고 자산분석, 위협분석, 취약성분석, 위험분석, 위험평가 등의 필수 작업 요소들을 포함시켰다.

또한 대응책 선정과 위험허용 수준을 결정하기 위한 비용효과 분석의 중요성을 감안해 타 모형에서 일반적으로 위험분석에 포함시키는 위험평가 부분을 독립적인 프로세스로 분리하였으며 정보기술 보안관리의 주기에 맞춰 통합적인 위험관리 모형이 되도록 하였다. 그리고 ISO의 제안모형에서 제시됐던 기본통제방식과 상세 위험분석 방식을 위험분석작업의 효율화를 기하기 위해서 확장하여 본 모형에 응용하였다.

본 모형은 특정 사용자 환경을 고려하지 않은 일반적 위험관리 모형으로 구성했으면서도 매우 상세한 과정을 기술하여 되도록 손쉽게 적용할 수 있도록 한 점이 특징이다. 또한 위험분석 경험이 없는 조직에서의 적용을 쉽도록 하였으며 조직의 다양한 정보기술 범위에 따라서 유연하게 본 모형을 적용할 수 있도록 하였다.

5. 결 론

정보화에 따른 정보 의존도가 심화됨에 따라 여러 위협에 의한 정보시스템의 심각한 피해를 방지하기 위한 보안대책이 필요하게 되었다. 이에 따라 보안관리를 체계화할 수 있는 핵심 기능인 위험관리에 대한 연구가 진행되고 있으며 다양한 위험관리 모형이 제시되고 적용되고 있다.

국내에서는 정보시스템에 대한 위험분석의 필요성이 겨우 인식되고 있는 실정으로 국내환경에 맞는 위험관리 모형의 제시와 이것을 적용한 위험분석도구의 개발과 적용이 시급한 상황이다.

따라서 본 연구에서는 현재 외국에서 개발되었거나 제안된 위험분석 및 관리 모형에 대한 특성, 흐름, 구조 등을 검토하였으며, 위험분석 각 모형별로 비교분석을 하였다. 이것을 토대로 외국 위험분석 모형의 공통분모와 장점을 수용하여 다양한 환경에서 수용이 가능하고 이해하기 쉬운 위험관리 모형을 제안하였다. 또한 국내외의 정보기술 위협을 비교, 분석하여 국내 환경에 적합한 위험관리 모형을 개발하였다.

본 모형은 조직 내의 많은 정보시스템 중 위험에 많이 노출된 정보시스템이나 매우 중요한 시스템을 파악하기 위해서 위험분석 수준을 초기 · 단순 · 상세 위험분석으로 분류하여 수행하도록 함으로써 위험분석의 효율화를 기하였다. 또한 구축되어 있는 정보 보안시스템에서 뿐만 아니라 정보 보안시스템 설계시에도 적용 가능하도록 상세하게 위험관리의 흐름을 제시한 것 등이 본 모형의 특징이라 할 수 있겠다.

다만, 본 위험관리 모형은 하나의 제안모형으로서 검증되지는 않았으며 앞으로 위험분석 및 관리방법론을 개발하여 본 연구에서 제시한 모형의 적용시 모형의 각 프로세스에 대한 정확성, 효율성, 시간, 비용, 자동화 도구 적용가능성 측면에서 검토하고 공공기관, 기업, 연구소를 대상으로 조직규모와 시스템 환경별로 다각도로 검증하는 것이 필요하다.

추후 위험분석 방법론을 개발하여 본 모형을 기반으로 실제 적용하면서 도출되는 문제점과 국내 정보시스템 환경에 쉽게 적용할 수 있는 특성화된 모형에 대한 연구가 지속적으로 수행되어야 할 것이다. 또한 위험관리의 효율화를 위한 위험분석 소프트웨어 개발에 대한 연구도 이루어져야 한다.

참고문헌

Ahn, J-H. (1998), *Information System for Management* Hongmoonsa, Seoul, Korea.

BSI. (1998), *Guide to Risk Assessment and Risk Management*, BS7799, British Standard Institute, Great Britain.

CCTA. (1998), *The CCTA Risk Analysis and Management Method:*

CRAMM, Central Computer and Telecommunications Agency, Great Britain.

CSI. (2001), *CSI/FBI Computer Crime & Security Survey Analysis*, Computer Security Issues & Trends, **V1**(1), San Francisco, USA.

ISO/IEC. (1996), *Information Technology-Guidelines for the Management of IT security-Part 1*, ISO/IEC TR 13335-1, ISO/IEC, Switzerland.

ISO/IEC. (1997), *Information Technology-Guidelines for the Management of IT security-Part 2*, ISO/IEC TR 13335-2, ISO/IEC, Switzerland.

ISO/IEC. (1998), *Information Technology-Guidelines for the Management of IT security-Part 3*, ISO/IEC TR 13335-3, ISO/IEC, Switzerland.

ISO/IEC. (2000), *Information Technology-Guidelines for the Management of IT security-Part 4*, ISO/IEC TR 13335-4, ISO/IEC, Switzerland.

Kang, D-S. (1998), Risk Analysis and Management in Public Project Selection, *The Journal of Information*, **5**(1), 16-29.

Kim, Y-C. and Nam, G-H. (1993), Information System Security and Auditing Mechanisms, *Korea Institute of Information Security & Cryptology Review*, **3**(3), 67-79

KISA. (1998), *Information Dysfunction Analysis in the First Quarter of The Year 1998*, Korea Information Security Agency, Seoul, Korea.

KISA. (1999), *Information Dysfunction Analysis of The Year 1999*, Korea Information Security Agency, Seoul, Korea.

KISA. (2000), *Information Dysfunction Analysis of The Year 2000*, Korea Information Security Agency, Seoul, Korea.

Lee, Y-H. and Lee, N-Y. (1999), The Study for Security Engineering Methodology, *Korea Institute of Information Security & Cryptology Review*, **9**(2), 69-81.

NCA.(1996), *Development of Automated Risk Analysis Software (V.1.0) for Information Systems Security*, NCA III-RER-9653, National Computerization Agency, Gyonggi-do, Korea.

NCA. (1996), *Analysis of Computer Crime and Misuse Cases*, NCA III - RER - 96099, National Computerization Agency, Gyonggi-do, Korea.

NCA. (1998), *A Study on Audit Guideline for the Information Systems Management*, IV-AUER-98061, National Computerization Agency, Gyonggi-do, Korea.

NIST. (1989), *DoE Risk Assessment Instruction*, National Institute of Standards Technology, Washington, USA.

NIST. (1990), *U.S. Department of Justice Simplified Risk Analysis Guidelines*, NISTIR 4387, National Institute of Standards Technology, Washington, USA.

NIST. (1994), *Guidelines for the Analysis of Local Area Network Security*, FIPS PUB 191, National Institute of Standards Technology, Washington, USA.

NIST.(1999), *An Introduction to Computer Security: The NIST Handbook*, NIST Special Publication 800-12, National Institute of Standards Technology, Washington, USA.

Sergio B. Guarro. (1987), Principles and Procedures of the LRAM Approach to Information System Risk Analysis and Management, *Computers & Security*, **6**, 493-504.

TTA. (2000), *Risk Analysis and Management Standards for Public Information System Security-Risk Analysis Methodology Model*, TTA. KO-12.0007, Telecommunications Technology Association, Seoul, Korea.

Vlasta Molak.(1997), *Fundamental of Risk Analysis and Risk Management*, CRC Lewis, New York, USA.