IE Interfaces
Vol. 16, No. 4, pp. 421-431, December 2003.

업무 프로세스 중심의 정보기술 보안 위험분석 적용 사례 —클라이언트/서버 시스템 중심으로

안춘수† · 조성구

동국대학교 산업시스템 공학부

A Case Study of Business Process Centered Risk Analysis for Information Technology Security

Choon-Soo, Ahn · Sung-Ku, Cho

Department of Industrial System Engineering, Dongguk University, Seoul, 120-728

Due to the increasing complexity of the information systems environment, modern information systems are facing more difficult and various security risks than ever, there by calling for a higher level of security safeguard. In this paper, an information technology security risk management model, which modified by adopting the concept of business processes, is applied to client/server distributed systems. The results demonstrate a high level of risk-detecting performance of the model, by detecting various kinds of security risks. In addition, a practical and efficient security control safeguard to cope with the identified security risks are suggested. Namely, using the proposed model, the risks on the assets in both of the I/O stage(on client side) and the request/processing stage(on server side), which can cause serious problems on business processes, are identified and the levels of the risks are analyzed. The analysis results show that maintenance of management and access control to application systems are critical in the I/O stage, while managerial security activities including training are critical in the request/processing stage.

Keywords: information technology security risk management. client/server system, business process

1. 서 론

1980년대 이후 컴퓨터와 통신의 결합체인 정보기술의 발달로 우리 사회 및 개인의 삶의 질이 높아지는 등 자유로운 정보의 교환이라는 풍요로운 정보화 사회를 이룩하고 있다. 이에 따라 정보기술은 어느 산업이든지 불문하고 기업 경영의 근간을 이루고 있다. 하지만 정보화의 부정적 측면인 정보의 남용 및 악용 등과 같은 정보화의 역기능이나 컴퓨터 범죄 등으로부터 정보를 보호해야 할 필요성이 증가되고 있다.

또한 1990년대 이후 분산시스템, 최종사용자, 네트워크의 급진전, 인터넷과 인트라넷의 급속한 보급 등으로 정보시스템 환경이 중앙 집중 처리방식에서 분산 처리방식으로 변화되고 있으며 이에 따른 정보시스템의 위험도 증가하고 그 유형도 다양해지고 있다.

전통적인 메인 프레임을 이용한 중앙 집중 처리시스템보다 클라이언트/서버 분산시스템의 위험이 더 높다는 것을 제대로 인식하지 못하고 이에 대한 관리가 소홀히 이루어지고 있으며 (Fried, L. 1995), 실제로 최근에 행하여진 설문조사 결과에 의하면 기업들은 중앙 집중 시스템보다 클라이언트/서버 분산시스템에서 보안위험의 인식 부족으로 정보시스템을 보호할 수 있

†연락저자 : 안춘수, 120-728 서울시 중구 필동 3가 26번지 동국대학교 산업시스템 공학부, Fax : 02-2273-9522, E-mail: sooahn@dongguk.edu
2003년 8월 접수, 1회 수정 후 2003년 9월 게재 확정.

는 적절한 보안대책을 수립하지 못하고 있다(Ryan and Bordoloi, 1997).

즉, 정보시스템의 환경이 하드웨어 중심에서 소프트웨어 및 사용자 중심으로 발전함으로써 발생할 수 있는 위험도 물리적인 위험보다는 관리적이고 기술적인 위험이 증가하게 된다. 그러나 기존의 정보기술 보안 관리는 현 정보시스템의 환경에 대응하는 위험수준도 모른 체 중앙 집중 처리방식에서의 개념으로 아직까지도 하드웨어 차원에서의 물리적인 위험을 분석함으로써 현실적인 보안대책 수립을 어렵게 하여 효율적인 정보기술 보안관리가 이루어지지 않고 있다(NCA, 1998).

정보화의 역기능 및 위험요소는 우연히 발생하는 사고라고 하기 보다는 위협, 취약성, 보안사고, 자산손실, 영향 등 위험 구성요소의 조합에 의해서 발생이 된다. 이러한 구성요소들을 분석 정보자산에 대한 정확한 위험분석을 통해서 위험을 감소 또는 제어할 수 있도록 기술적, 관리적, 물리적 요소를 고려한 보안대책 기준을 마련할 필요가 있다.

이에 본 논문에서는 정보보호의 필요성과 현 시스템에 적용할 수 있는 정확한 위험분석의 필요성에 의해 국내 환경에 효율적인 기존의 정보기술 보안 위험관리 모형을 현 정보시스템의 환경에 적합하도록 수정 혼합하였다. 또한 수정모형을 현재 가장 많이 보편화된 정보시스템인 클라이언트/서버 분산방식 시스템에 적용할 수 있는 효율적인 보안대책의 기준을 제시하고자 한다.

다시 말하면, 국내외 정보기술 보안 위험관리 모형의 장단점을 분석하고 국내 정보시스템 환경 및 위협을 분석하여 개발된 정보기술 보안위험관리 모형(Ahn, C. S., Cho, S. K., 2002)을 시스템의 업무 프로세스 개념을 도입하여 수정하였다. 또한 기존연구에서의 정보자산 위주의 위험분석이 아닌 자산손실로 인한 업무수행의 중단 및 지연과 관련된 위험을 분석하고자 사례적용을 하였다.

2. 정보기술 보안 위험관리

2.1 정보기술 보안 위험관리 구성요소

정보화 사회는 정보의 양이 아니라 정보의 질이 강조되는 사회로서 정보시스템의 위험으로 인해 정보화의 역기능 및 정보기술의 부작용이 증가하고 있다. 이에 따라 정보기술 보호에 대한 많은 연구가 진행되고 있는데 정보기술을 보호해야 할 필요성은 다음과 같다(NCA, 1998; Kim, J. P., Park, D. S., Lee, S. J., 2003).

첫째, 정보의 기능유지 측면에서 정보는 고유한 사용목적과 기능을 유지해야 하고 필요한 장소, 사람, 시점에 정확히 전달되어야 한다. 그러나 정보의 무결성 및 비밀성 등을 보장하지 못하면 정상적인 정보의 기능유지를 할 수 없다.

둘째, 자산의 보호 측면에서 정보는 모든 자산의 손실과 왜곡으로 막대한 재정적 손실을 유발한다. 따라서 정상적인 통신망 운영과 정보에 관련된 모든 재산권 보호를 위해 필요하다.

셋째, 개인정보보호 측면에서 개인정보의 침해 가능성으로 개인의 프라이버시 보호를 위해 필요하다.

넷째, 기업 또는 조직 안전의 측면에서 통신망을 통한 기업 비밀 정보 유출, 파괴, 훼손 등 통신망의 보안 허점으로 인해 기업의 경쟁력 약화를 유발하므로 기업 및 조직의 안전보장을 위해 필요하다.

이에 본 논문에서는 자산의 보호 측면을 중심으로 접근하고자 한다. 자산에는 물리적 자산, 소프트웨어 자산, 무형자산, 조직의 직원, 정보자산 등이 포함된다.

자산에 대한 보호를 체계적으로 수행하기 위해서는 중요자산을 식별하고, 이 자산이 위협으로부터 어느 정도 위험에 처해있는 지를 측정하여, 위험수준을 적절한 정도로 낮추기 위해 보안대책을 선정하는 활동, 즉 위험관리가 필요하다.

정보기술 보안 위험관리는 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).

정보기술 보안 위험관리의 핵심적인 활동은 위험분석과 평가로서, 위험분석은 자료수집과 분석을 하는 단계이며 위험관리의 80%를 차지한다. 위험평가는 분석된 결과물을 기초로 현황을 평가하고 적절한 방법을 사용하여 효과적으로 위험수준을 낮추려는 활동을 하는 단계이다(Kim, H. B., 2000).

즉, 위험분석은 위험의 식별과 분석을 하는 단계이고, 위험평가는 위험의 평가와 보안대책을 결정하는 단계이다. 또한 조직의 효과적 정보기술 보안을 위해서는 위험관리 외에도 IT 보안의 목적, 전략과 방침과 같은 활동들이 필요하다. 위험분석 및 관리를 수행하는 데 있어서 주요한 요소로는 자산, 위협, 취약성, 영향, 위험, 대책 등이 있다(BSI, 1998).

2.1.1 자산

조직의 성공을 위해서는 자산을 적절하게 관리하는 것이 필수적이다. 보안의 관점에서 볼 때, 조직의 자산이 식별되지 않으면 성공적인 보안 프로그램을 수립하여 구현하는 것이 불가능하며, 자산을 식별하기 위해서는 많은 비용과 시간이 요구될 수도 있다. 일반적으로 자산을 항목별로 분류하면 <표 1>과 같다.

각 자산별로 고려해야 할 사항은 그들의 가치와 잠재적으로 포함하고 있는 보안대책, 그리고 특정 위협에 대한 취약성이다. 조직이 처해 있는 환경과 문화에 따라서 자산의 가치와 자산의 취약성에 대한 중요도는 매우 다를 수 있다.

표 1. 자산의 항목별 분류(BSI, 1998)

분류	내용	세부 항목
하드웨어	데이터를 각종 방식으로 처리할 수 있는 능력을 가진 자산	CPU, 하드디스크(내장/외장), System Terminal, 광파일 서버, Disk Array, 프린터 등
시스템 소프트웨어	중앙처리장치를 운영하는 소프트웨어	UNIX, DOS, Windows, WindowNT, LINUX 등
네트워크	데이터를 서로 다른 시스템 간에 공유할 수 있는 기능을 제공할 수 있는 하드웨어 및 소프트웨어	Management OS, HUB, Router, Repeater, Gateway, TX(교환기), Interface Card, Protocol Types, LAN Types, WAN Types 등
데이터	정보시스템에 저장, 처리, 연산될 수 있는 전자적 정보	User's Data, Employee Data, Financial Data, System Data 등
응용 소프트웨어	중앙처리장치를 이용 사용자에게 특정 작업기능을 제공하는 프로그램	Security S/W, Word Processing 등
사용자	정보시스템을 사용하는 모든 인력	System Administrator, Risk Analyst, System Operator, DataBase Administrator, Security Manager, System Programmer 등
환경	정보시스템과 간접적 관계를 갖는 유·무형 자산	UPS, 차폐벽, Clent/Server DataBase System, 화재통제 시스템, 습도조정 시스템 등

2.1.2 위협

위협은 자산에 해를 줄 수 있는 위험의 원천이다. 이런 손상은 정보기술 시스템이나 서비스가 취급하는 정보의 분실 또는 이용 불가능성, 직/간접적으로 비인가된 파괴, 누설, 수정 등과 같은 결과를 초래한다. 위협은 자산이 지니고 있는 취약성을 이용하여 자산에 손상을 입힌다.

위협은 일반적으로 그 원천이 자연적인가 또는 인위적인가로 구별될 수 있으며, 인위적 위협은 다시 고의적 또는 우연적 위협으로 구분될 수 있다.

표 2. 위협원천에 의한 분류(ISO/IEC, 1996)

인위적		자연적
고의적	우연적	
도청, 시스템 해킹, 정보변조, 바이러스, 도난 등	자료 입력 실수, 접근통제의 실수, 파일삭제 실수 등	지진, 벼락, 화재, 전력 과부하 등

BSI 7799에서는 위협을 하드웨어, 소프트웨어, 환경, 인적요소, 저장장치, 통신으로 구분하고 있다.

2.1.3 취약성

취약성은 조직, 물리적 배치, 절차, 직원, 관리, 하드웨어, 소프트웨어, 정보 등과 같은 자산이 잠재적으로 갖고 있는 약점을 말한다. 취약성의 또 다른 정의는 위협의 공격을 방지할 수 있는 보안대책의 미비이다. 어떤 정의를 사용하던 취약성은 위협과 관련되어 있다.

즉, 화재의 위협은 부적절한 화재방지의 취약성과 연관되어 있고, 비인가된 접근은 부적절한 접근통제와 연관되어 있다. 이러한 취약성은 위협에 의해 공격을 당해, 원하지 않는 사건을 초래하여 정보기술 시스템에 손상을 줄 수 있다.

그러나 취약성 자체가 손상을 초래하지는 않는다. 취약성은 단순히 위협이 자산에 영향을 줄 수 있는 조건을 제공할 뿐이며, 자산에 대해서 취약성이 존재하지 않는다면 위협의 발생 여부에 대해서 위험을 분석할 필요는 없다.

취약성은 일반적으로 물리적 취약성, 관리적 취약성, 기술적 취약성으로 구분하며, 취약성 분석은 환경과 기존의 보안대책을 고려하여 현존하는 위협의 공격대상이 될 수 있는 자산의 약점을 검사하는 것이다. 즉 특정 시스템 또는 자산의 취약성이란 시스템 또는 자산이 얼마나 쉽게 손상될 수 있는가를 말한다.

2.1.4 영향

영향은 보안사고가 자산에 미치는 결과로서 자산에 대한 직/간접적 피해를 유발하는 원하지 않은 사건의 결과이다. 같은 위협이라도 피해자산의 종류에 따라 위협에 의한 피해규모는 다를 수 있다. 위협에 의한 보안사고 발생시 자산에 미치는 영향은 거부, 변조, 파괴, 폭로 등으로 나뉜다(BSI, 1998).

영향의 측정은 보안사고로 인한 손실과 이러한 손실을 완화하는 보안대책에 대한 비용간의 균형을 맞출 수 있게 하며, 위험수준의 결정 및 위험의 평가와 보안대책의 선정에 있어서 매우 중요한 요소이다.

2.1.5 위험

위험은 특정 위협이 취약성을 이용하여 자산을 공격해서 손상을 초래할 수 있는 잠재력이다. 일반적으로 위험 = 위협 발생 빈도 × 위협 발생시 자산에 미치는 손실로 정의한다. 즉, 위험은 위협 발생 가능 확률과 영향 두 가지 요소의 결합에 의해 특징지어진다.

2.1.6 보안대책

보안대책은 위험을 감소시키는 행위, 절차, 또는 방법으로서 대책의 기본 기능은 감지, 예방, 제한 또는 통제, 수정, 복구, 교육 또는 인식 등이 있다.

일반적으로 보안대책은 크게 물리적·기술적·관리적 보안대책으로 분류하며 <표 3>과 같다.

표 3. 보안대책의 분류(ISO/IEC, 1997)

물리적 보안대책	관리적 보안대책	기술적 보안대책
물리적인 시설물 보호, 지역적 특성에 의해 야기되는 위협 최소화 등	내·외부자에 의한 정보의 오남용을 방지하기 위한 보안 등.	컴퓨터 기술을 통해서 시스템을 보호 등

2.2 정보기술 보안 위험관리 적용시 문제점

정보기술 보안 위험관리의 목적은 위험 측정 및 비용효과적인 통제 선택의 두 가지 기능을 수행함으로써 보안을 증대시키는 것이다. 위험은 완전히 제거될 수 없다는 가정하에 가능한 한 비용효과적인 방법을 수용할 수 있는 수준으로 위험을 감소시켜야 한다.

NIST에서는 위험관리의 목적을 단지 IT 자산을 보호하는 것이 아니라 조직과 IT 자산의 미션을 수행하는 조직의 능력을 보호하는 것이라 정의하였다.

위험분석이란 구축대상 시스템에 영향을 미칠 수 있는 다양한 위협, 취약점을 식별하고 이로 인해 예상되는 손실 및 영향을 분석하여 목표보호 수준에 도달하기 위한 적절한 보호 메커니즘을 선택하는 과정이다(Rex Kelly Rainer. JR., Charies A. Snyder, and H.H. Carr, 1991).

위험분석의 활동으로는 자산분석, 위협분석, 취약점분석, 위험도분석, 비용효과분석, 최적보호대책의 선정 등이 있으며, 위험분석은 시스템 개발 전 단계에 걸쳐 수행되는 지속적이고 반복적인 과정으로 시스템 개발 초기부터 수행하는 것이 더욱 경제적이며 보다 뛰어난 효과를 발휘한다.

정보기술 보안 위험분석 및 관리는 정보기술 보안관리시 매우 중요한 단계임에도 불구하고 다음과 같은 문제점으로 인해 많은 조직들은 위험분석 및 관리를 수행하지 않거나 수행하더라도 체계적이지 못하여 보안관리에 있어서 매우 취약한 실정이다(NCA, 1998).

첫째, 위험분석의 첫 단계인 자산분석은 모든 자산 중에서 중요한 자산 또는 중요 시스템을 도출하여 가치를 측정하는 것이다. 하지만 조직의 모든 자산을 고려한다는 것은 불가능한 일이며 시간과 비용이 기하급수적으로 증가하므로 위험분석을 적용하기 어렵다는 단점이 있다.

둘째, 위험관리 프로세스 중 가장 기반이 되는 프로세스는 시스템 평가 프로세스로서, 현 정보시스템의 상태에 대한 평가가 적절히 이루어지지 않은 상태에서 이에 따른 후속 계획이나 관리과정이 제대로 이루어질 수 없다. 이러한 평가 수행시 고려되어야 할 기본적인 요소는 평가의 기준을 무엇으로 할 것인가이다. 현 상태의 문제점이나 취약성을 도출하기 위해서 무엇인가 비교할 기준이 필요하다. 하지만 정보 보안관리에서 절대적인 기준이란 존재하지 않으며 존재하더라도 적용성 측면에서 바람직하지 않을 수 있다.

셋째, 기존의 위험관리 방법들은 중앙집중 처리방식의 정보시스템을 기준으로 하여 연구된 모형으로서 최근의 정보시스템 환경인 클라이언트/서버 분산방식 정보시스템의 적용에 어려움이 있다. 클라이언트/서버 분산방식은 중앙 집중 처리방식 시스템에 비해서 유연성을 가지고 생산성을 향상시키기 때문에 사용자 만족을 증가시키며 최근 급속히 보편화되어가고 있다. 이 방식은 중앙집중 처리방식에 비해 보안상의 위험이 대체로 증가함에도 불구하고 많은 조직들은 중앙집중 처리방식에서의 위험에 대해서만 보안대책을 수립하고 있다. 즉, 이 방식은 공급자들이 제공한 플랫폼, 운영체제, 프로토콜, 응용시스템 등 복잡한 플랫폼으로 구성되어 있어 위험에 대한 정확하고 다양한 분석을 필요로 한다.

넷째, 정보시스템의 궁극적 목적은 원활한 정보 서비스의 수행에 있다. 정보시스템에서 자산의 가치도 중요하지만 업무의 흐름에 따라 시스템의 성공여부가 결정된다(KISA, 2001). 즉, 업무 프로세스 상의 중단 및 지연이 없이 업무가 원활히 수행될 수 있는 위험을 감소시킬 수 있는 보안대책이 필요하다.

3. 적용할 정보기술 보안 위험관리 모형

3.1 정보기술 보안 위험관리 모형의 수정

위험관리 모형은 위험관리의 전반적인 흐름을 나타내는 위험관리 구조도이다. 이 모형을 통하여 분석작업들의 적용순서, 필수적인 작업요소, 적용될 위험분석기법들이 결정된다.

본 논문에서는 대표적인 위험관리 모형들의 특징 및 장단점을 분석하여 공통분모를 도출하고, 정보기술 보안 위험관리의 필수 구성요소들을 중심으로 쉽게 적용할 수 있게 개발한 기존의 위험관리 모형을 수정하여 모형 적용시의 문제점을 해결하면서 현 정보시스템 환경에 적용 가능하도록 하였다.

첫째, 정보기술 보안관리를 수행하기 위해서는 일반적으로 보안정책, 위험관리, 보안대책, 사후관리의 4단계로 이루어지며, 위험관리는 보안관리에 있어서 가장 핵심이 되는 과정이다. 즉, 위험관리 과정이 보안관리에 포함되어 있으며 위험관리의 궁극적 목적이 보안관리이므로 위험관리 부분만을 따로 구분하지 않고 보안관리의 4단계 과정에 따랐다. 또한 자산, 위협, 취약성, 위험, 영향 등 필수적인 보안 위험관리 구성요소들을 포함시켰으며 쉽게 적용할 수 있도록 개념적인 흐름보다는 모형 각 단계마다 상세히 설명하였다. 보안관리의 주기에 맞게 구성된 정보기술 보안 위험관리 프레임워크 틀은 <그림 1>과 같다.

둘째, 클라이언트/서버 분산방식은 중앙집중 처리방식보다 복잡한 구조로써 다양한 위험이 발생하며 보안 위험에 대한 정확한 분석을 필요로 한다. 따라서 정보시스템에서 수행하는 핵심 업무를 파악하고 업무프로세스에 따라 각 자산과 위험을 분석하였다.

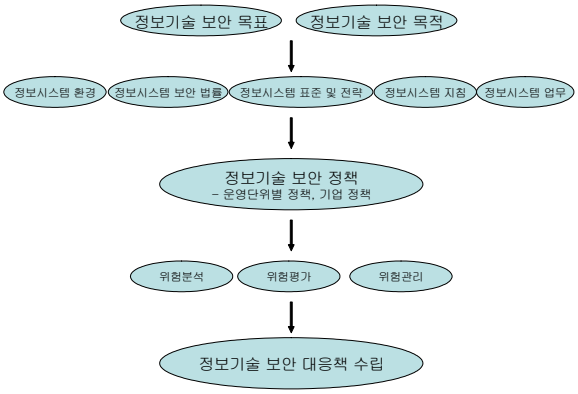

그림 1. 정보기술 보안 위험관리 프레임워크 틀.

즉, 정보시스템은 자산도 중요하지만 정보시스템의 핵심은 업무의 흐름에 따라 시스템의 성공여부가 결정된다(KISA, 2001). 정보시스템의 구성에 근거하여 각 주요 데이터의 흐름을 입출력, 처리/요구 등으로 구분하고, 각 흐름별로 자산 및 위험을 분석하였다. 이 방법은 간단하면서도 포괄적인 체계를 제공하고 위험분석 단계 초기의 범위 설정 및 중요 자산의 도출 단계가 쉬워지며 업무 프로세스 측면을 고려함으로써 정보시스템의 목적인 업무 서비스를 효율적으로 수행할 수 있는 보안대책 설정에 효과적 기준이 된다.

셋째, 위협이 자산에 어떠한 영향을 주는지를 분석하는 자산에 대한 영향도 중요하지만 궁극적으로는 자산에 대한 영향으로 인해 정보시스템 업무의 중단 및 지연이 발생한다. 따라서 원활한 업무수행을 위한 보안 대책을 도출할 수 있도록 자산 손실로 인해 업무 프로세스에 어떠한 영향을 주는지를 파악하도록 하여 수행 업무의 지속성에 악영향을 주는 심각상의 정도를 분석하여 정확한 위험을 분석할 수 있게 하였다.

넷째, 일반적으로 위험은 자산의 취약성으로 인해 발생되는 기대손실로 정의한다. 본 논문에서는 적용시 보안 담당자 및 사용자의 이해를 돕기 위해 위험의 정의를 위험발생 주기에 맞게 상세히 설명하였다. 위험 정의와 보안대책(S)의 기본 개념은 <그림 2>와 같다.

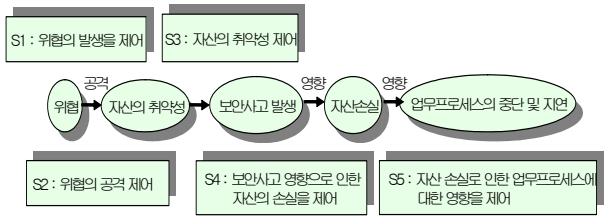

그림 2. 위험의 정의 및 보안대책의 의미.

3.2 클라이언트/서버 분산방식 정보시스템

최근의 정보시스템 환경은 개인의 컴퓨터가 근거리 통신망에 편성되고, 워크스테이션급 컴퓨터와 통합되는 개방형 시스템으로 변모하고 있다. 중앙집중 처리방식에 비해 유연성 및 생산성의 향상이라는 특징으로 인해 1990년대 이후 많은 기업 및 공공기관들의 정보시스템 환경은 클라이언트/서버 분산방식으로 전환되고 있는 실정이다.

클라이언트/서버 분산 시스템은 네트워크를 통해 연결된 컴퓨터 간에 업무를 분산시키고 정보를 공유시키는 분산화된 처리 시스템이다. 클라이언트는 서비스를 요청하고 서버는 이러한 서비스 요청을 수신하여 처리한다. 주요 특징은 <표 4>와 같다.

표 4. 클라이언트/서버 시스템의 특징

장 점	단 점
· 자원의 공유를 통한 효율적 사용 · 기능형 분산 시스템 · 개방시스템으로 멀티 벤더 환경 구축 · 시스템 규모와 조정의 유연성 · 최종 사용자 컴퓨팅 위주의 시스템 구축	· 시스템 관리 및 유지가 복잡

클라이언트/서버 시스템은 다양한 공급자들이 제공한 플랫폼, 운영체제, 프로토콜 및 응용시스템 등 복잡한 플랫폼으로 구성되어 위험을 발견하고 해결하기가 어려워졌으며, 데이터 및 응용 프로그램에 불법적으로 접근할 수 있는 경로와 가능성이 높아졌다(Lee, S. J., 2000).

다양한 하드웨어와 소프트웨어로 구성된 클라이언트/서버 시스템은 보안정책을 표준화하고 보안대책을 도출하여 일관되게 적용시키는 데 어려움이 따른다(Ryan and Bordoloi, 1997). 따라서 클라이언트/서버 시스템의 효과성 및 안전성과 생산성 있는 업무수행을 위해 현실적인 위험을 분석하고 위험수준에 따른 보안대책에 대한 연구가 필요하다.

4. 적용 사례

4.1 적용 시스템의 특징

제시한 위험관리 모형의 적용 가능성과 클라이언트/서버 시스템에서의 정확한 위험분석을 위해 D대학의 클라이언트/서버 분산방식의 정보시스템에 적용하여 보았다. 적용시킨 정보기술 보안 위험관리 모형은 Ahn, C. S., Cho, S. K.의 위험관리 모형에 업무 프로세스 개념을 도입하여 업무분석 및 위험발생으로 인한 업무의 영향 정도를 추가하여 수정된 모형으로서 <그림 3>과 같다.

적용시 보안의 특수성, 즉 보안이란 남에게 공개하지 않는다 라는 특징으로 인해 D대학의 보안대책 수립 및 평가가 어려웠으며 본 논문에서는 정보기술 보안 위험분석까지 적용범위로 정하였다. 조직의 보안정책상 보안대책에 대한 내용의 공

개를 꺼리는 이유로 인해 본 연구에서는 적용대상 시스템에서의 위험수준 측정을 주 범위로 결정하여 업무 프로세스 중심으로 어떤 자산의 위험수준이 가장 높고, 어떤 유형의 위협 및 취약성이 존재하는가를 식별하여 분석하였다.

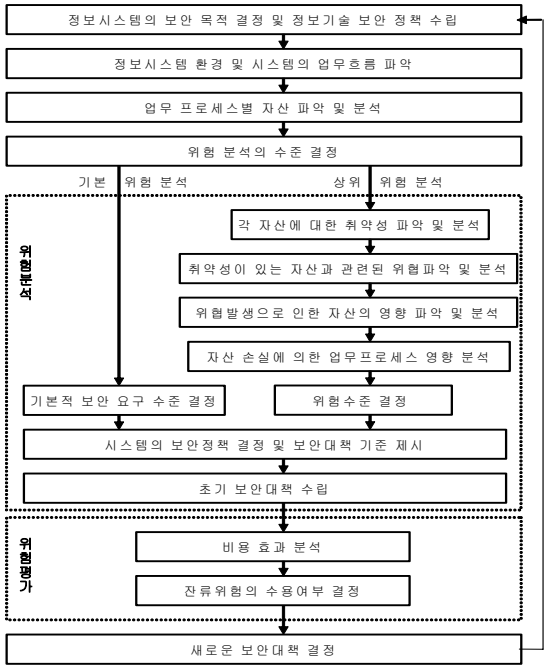

그림 3. 수정된 정보기술 보안 위험관리 모형.

사례 적용방법으로는 보안에 대한 자료의 미공개 및 과거자료의 부재 등으로 인하여 통계적 분석방법의 적용에 어려움이 있어 시스템 보안 담당자를 대상으로 BSI에서 국제 표준으로 제시하고 있는 정성적 방법인 면담분석 방법을 사용하였으며, 위협 및 취약성은 국제표준과 국내표준에서 제시되고 있는 목록과 국내 정보기술 위협 유형별 사례를 분석한 자료(Ahn, C. S., Cho, S. K., 2002)를 참조하였다.

적용대상 DRIMS 종합 정보시스템 개념도와 구현절차는 <그림 4>, <그림 5>와 같다.

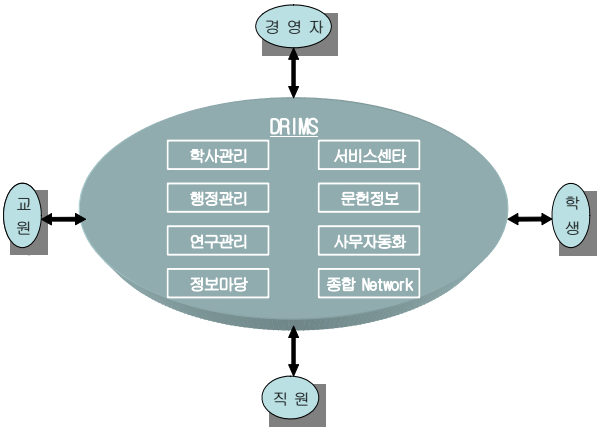

그림 4. 종합 정보시스템 개념도.

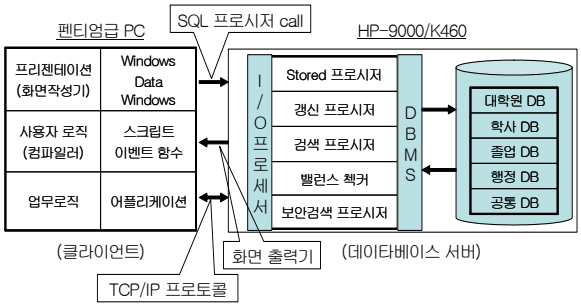

그림 5. DRIMS 구현절차.

조직의 보안 요구사항은 학교와 관련된 기밀 정보, 해당부서의 대외비 정보, 학생 및 교직원과 관련된 신상 정보, 학교의 학사관리 업무 정보, 행정 서비스 관련 정보 등의 보안이었으며 핵심 업무는 학사관리로서 시스템의 특징은 다음과 같다.

① D대학 통합 정보시스템인 DRIMS는 기존의 호스트 컴퓨터를 중심으로 한 중앙 집중식 처리방식에서 최신의 클라이언트/서버 방식으로 설계하였다.

② 학부 학사행정용인 5개의 데이터베이스(학사, 졸업, 행정, 입시, 공통)를 연계하여 유지, 관리한다.

③ 메인 서버로 UNIX에서 구동한다.

④ LAN 상에 접속된 PC라면 학내 어느 곳이든지 사용이 가능하다.

시스템의 목표는 학적 정보의 온라인 전산 데이터베이스화, 관련 정보 공유로 사무생산성 대폭 개선, 업무 흐름 간소화 및 자료의 실시간 처리이다.

4.2 위험관리 모형의 사례 적용 결과

정보기술 보안 위험관리 모형에 따라 각 단계별로 적용한 사례 분석 결과는 다음과 같다.

(1) 정보시스템의 보안 목적에 대한 가중치는 가용성 0.3, 비밀성 0.3, 무결성 0.4이고 보안정책은 국내표준인 전산보안정책 수립을 위한 지침에 따라 수립되어 있었다. 보안 목적 가중치는 보안대책 우선순위 결정의 기준이 된다.

(2) 업무분석을 통한 업무 흐름도는 <그림 6>과 같다.

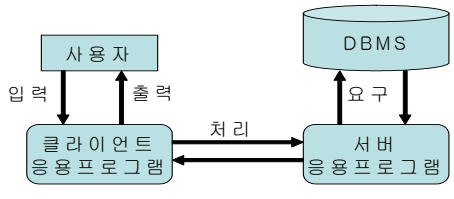

그림 6. 업무 흐름도.

(3) 업무흐름과 관련된 자산을 입출력, 처리/요구로 구분한 뒤 일반적인 자산항목 하드웨어, 시스템 소프트웨어, 응용 소프트웨어, 데이터, 네트워크, 사용자, 환경의 7가지로 분류하여

업무 프로세스에서의 기여도, 전체 업무에서의 자산의 가치, 잔존가치, 비용을 파악하였다.

파악된 자산 항목에 대해 자산 속성 중 보안 담당자 및 사용자의 주관적 판단을 통해 자산가치에 대한 중요도는 프로세스 자산가치 > 업무기여도 > 비용 > 잔존가치 순이었으며 속성별 제거방법과 사전식 방법을 혼합한 발견적 방법으로 중요자산의 순위를 결정하였다. 결정된 중요자산의 순위는 <표 5>, <표 6>과 같다. 즉, 전체 업무에서의 자산가치와 업무와의 기여도가 보통 이하인 경우는 사용자의 주관적 판단에 의해 고려하지 않기로 하였다.

표 5. 입출력 단계 자산의 가치

순위	자산
1	학사관리 자료
2	LAN types, 교학과 직원
3	Sybase client module
4	TCP/IP 네트워크
5	펜티엄급 PC
6	교수
7	Windows 98
8	경리과 직원, 정보관리실 직원

표 6. 처리/요구 단계 자산의 가치

순위	자산
1	학사관리 자료
2	HP 9000 V2600
3	Sybase 12
4	Router
5	UPS
6	LAN types
7	UNIX, 시스템 관리자, DB 관리자
8	HP 9000 RP7400
9	프로그램 개발자
10	보안매니저

(4) 취약성에는 관리적, 기술적, 물리적 취약성이 존재하며 어느 하나의 취약성 수준이 낮거나 존재하지 않더라도 전체 취약성 수준에 영향을 주지 않는다. 즉, 관리적 취약성이 0이고 기술적 취약성이 10인 경우 승법으로 취약성 수준을 계산한다면 취약성은 존재하지 않는 것으로 나타나게 된다. 그러나 관리적 취약성만 존재하지 않을 뿐 다른 부분에서의 취약성은 존재하므로 가법의 형태로 자산에 대한 취약성 수준 = 관리적 취약성 정도 + 기술적 취약성 정도 + 물리적 취약성 정도로 구하였으며, 각 자산에 대한 취약성 수준을 분석한 결과는 <표 7>, <표 8>과 같다.

표 7. 입출력 단계 자산의 취약성 수준

순위	자산	취약성 수준
1	Sybase client module	78
2	User	61
3	학사관리 자료	54
4	TCP/IP 네트워크	51
5	LAN Types	48

표 8. 처리/요구 단계 자산의 취약성 수준

순위	자산	취약성 수준
1	HP 9000 V 2600, HP 9000 RP 7400	68
2	UNIX	58
3	시스템 관리자	56
4	Router	55
5	학사관리 자료	54
6	DB 관리자	52
7	LAN Types	51
8	보안 담당자	49
9	Sybase 12	45
10	UPS	36

(5) 발생한 적이 있거나 발생할 가능성이 있는 위협에 대한 발생빈도를 ISO/IEC 17799 위협목록과 국내표준에서의 위협목록을 기본으로 140가지의 위협 목록을 작성하였다. 위협에 대한 발생빈도를 발생하지 않는다(0), 매우 낮다(1), 낮다(2), 보통(3) 높다(4), 매우 높다(5)로 구분하여 분석한 결과는 <표 9>, <표 10>과 같으며 발생하지 않은 위협에 대해서는 고려하지 않았다.

표 9. 입출력단계 자산의 위협 발생빈도 수준

자산	위협 발생빈도						순위
	매우낮다	낮다	보통	높다	매우높다	합계	
Sybase client module	2	2	18	24	30	76	1
User	3	6	24	4	10	47	2
LAN types	7	10	12	4	5	38	3
TCP/IP 네트워크	3	2	6			11	4
학사관리 자료	4	4				8	5

표 10. 처리/요구 단계 자산의 위협 발생빈도 수준

자산	위협 발생빈도						순위
	매우 낮다	낮다	보통	높다	매우 높다	합계	
시스템 관리자	5	8	15	12	10	50	1
DB 관리자	1	8	12	12	10	43	2
Router	6	4	9	4	10	33	3
보안 담당자	1	12	9	8		30	4
Sybase 12	1	6	9	4		20	5
LAN types	12	6				18	6
UNIX	1	6	9			16	7
HP 9000 V2600	5		9			14	8
UPS	11	2				13	9
HP 9000 RP 7400	5		6			11	10
학사관리 자료	4	4				8	11

(6) 취약성 수준이 아주 낮더라도 위협 발생이 빈번하면 위험의 발생 가능성은 높아지며 그 반대의 경우도 마찬가지이다. 위험은 취약성이 있는 자산에 위협이 공격을 함으로써 발생하는데 위협이나 취약성이 존재하지 않는다면 위험발생 가능성은 0이 되며, 발생되지 않는 위험에 대한 자산은 보안대책을 고려할 필요가 없다. 따라서 취약성 수준과 위협 발생빈도의 곱으로 위험발생 가능성을 결정하였으며 결과는 <표 11>, <표 12>와 같다.

표 11. 입출력 단계 자산의 위험발생 가능성

자산	취약성 수준	위협 발생빈도	위험 발생 가능성	순위
Sybase client module	73	76	5548	1
User	61	47	2867	2
학사관리 자료	54	38	2052	3
TCP/IP 네트워크	51	11	561	4
LAN Types	48	8	384	5

(7) 같은 위협이라도 피해자산의 종류에 따라 위협에 의한 피해규모는 다를 수 있으며, 위협에 의한 자산에 미치는 영향은 파괴, 변조, 폭로, 거부로 나누어진다(BSI). 따라서 위협에 의한 보안사고 발생시 업무 및 자산에 미치는 영향을 파악하였다.

먼저 위협의 공격으로 인해 자산에 미치는 영향의 정도를 영향이 없다(0), 영향이 매우 낮다(1), 영향이 낮다(2), 영향이 보통(3), 영향이 높다(4), 영향이 매우 높다(5)로 분석하였다. 또한 취약성 수준에서와 같이 어떤 영향 정도가 존재하지 않더라도 다른 영향 정도는 존재하므로 각 자산의 손실 정도 = 거부 영향 정도 + 변조 영향 정도 + 파괴 영향 정도 + 폭로 영향 정도로 구하였다. 결과는 <표 13>, <표 14>와 같다.

표 12. 처리/요구 단계 자산의 위험 발생 가능성

자산	취약성 수준	위협 발생빈도	위험 발생 가능성	순위
시스템 관리자	56	50	2800	1
DB 관리자	52	43	2236	2
Router	55	33	1815	3
보안 담당자	49	30	1470	4
HP 9000 V2600	68	14	952	5
UNIX	58	16	928	6
LAN Types	51	18	918	7
Sybase 12	45	20	900	8
HP 9000 RP7400	68	11	748	9
UPS	36	13	468	10
학사관리 자료	54	8	432	11

표 13. 입출력 단계 자산의 영향 정도

자산	자산 피해 영향				자산 영향 정도	순위
	거부	변조	파괴	폭로		
Sybase client module	68	77	69	69	283	1
User	57	62	62	57	238	2
LAN Types	46	50	51	46	193	3
TCP/IP 네트워크	17	19	19	17	72	4
학사관리 자료	15	19	18	17	69	5

표 14. 처리/요구 단계 자산의 영향 정도

자산	자산 피해 영향				자산 영향 정도	순위
	거부	변조	파괴	폭로		
시스템 관리자	61	64	64	60	249	1
DB 관리자	44	50	52	47	193	2
LAN Types	39	44	43	43	169	3
보안 담당자	40	40	40	40	160	4
Router	30	32	39	29	130	5
UPS	22	30	36	29	117	6
Sybase 12	29	28	29	28	114	7
UNIX	18	31	31	22	102	8
학사관리 자료	25	19	24	21	89	9
HP 9000 RP7400	12	17	17	25	71	10
HP 9000 V2600	14	14	18	15	61	11

자산의 피해로 인해 업무 프로세스에 악영향을 주는 정도를 없다(0), 미미하다(1), 보통이다(2), 심각하다(3), 매우 심각하다(4)로 파악하여 각 자산으로 인한 업무상의 피해에 미치는 심각도를 <표 15>, <표 16>과 같이 분석하였다.

표 15. 입출력 단계 자산 피해로 인한 업무 심각성

자산	자산 피해로 인해 전체적인 업무 프로세스에 미치는 심각성						순위
	없다	미미	보통	심각	매우 심각	합계	
Sybase client module		1	14	36	4	55	1
LAN Types			10	39		49	2
User		1	12	24	8	45	3
학사관리 자료			4	9	4	17	4
TCP/IP 네트워크			6	6	4	16	5

표 16. 처리/요구 단계 자산 피해로 인한 업무 심각성

	자산의 피해로 인해 전체적인 업무 프로세스에 미치는 심각성						순위
	없다	미미	보통	심각	매우 심각	합계	
시스템 관리자		1	4	39	12	56	1
LAN Types			2	30	16	48	2
DB 관리자		1	8	18	12	39	3
Router			6	33		39	3
보안 담당자		1	4	27		32	4
UNIX			4	9	16	29	5
Sybase 12			2	15	8	25	6
학사관리 자료			2	6	12	20	7
UPS		5	6	9		20	7
HP 9000 V2600		4	8			12	8
HP 9000 RP7400		5	2	3		10	9

(8) 위험수준을 결정한다. 위험수준은 위험발생 가능성이 크고 자산이 입는 피해 정도가 크며 자산 피해로 인해 업무 프로세스에 미치는 심각성의 정도가 큰 것이 위험수준이 높다. 즉, 위험발생 가능성이 없다면 자산이 입는 피해도 없으며 자산 피해가 없으므로 업무 프로세스에 미치는 심각성도 없게 된다. 따라서 위험수준 = 위험발생 가능성 × 자산 영향 정도 × 업무 프로세스에 미치는 심각성 정도를 이용하여 순위를 결정하였으며 결과는 <표 17>, <표 18>과 같다.

보안 담당자와의 면담을 통해 입출력 단계에서의 자산의 위험수준에서는 Sybase client module 자산이 다른 자산에 비해 위험수준이 가장 큰 것으로 나타났으며, 처리/요구 단계에서의 자산에 대한 위험수준에서는 시스템 관리자, DB 관리자 자산이 가장 위험수준이 높다고 평가되었으며, 위험수준이 높은 자산에 대해서 위험수준을 줄일 수 있는 보안대책을 마련하여야 할 것이다.

표 17. 입출력 단계 자산에 대한 위험수준

자산	위험값	위험 순위
Sybase client module	86,354,620	1
User	30,705,570	2
LAN Types	19,405,764	3
학사관리 자료	658,053	4
TCP/IP 네트워크	442,368	5

표 18. 처리/요구 단계 자산에 대한 위험수준

자산	위험값	위험 순위
시스템 관리자	39,043,200	1
DB 관리자	16,830,372	2
Router	9,202,050	3
LAN Types	7,300,800	4
보안 담당자	4,751,360	5
UNIX	2,715,444	6
Sybase 12	2,131,800	7
HP 9000 V2600	1,076,040	8
UPS	1,010,880	9
학사관리 자료	833,040	10
HP 9000 RP7400	675,920	11

4.3 사례 적용 결과에 대한 분석

위험도가 높은 자산의 유형을 분석해 보면 정보시스템 환경이 중앙집중 처리방식에서 분산 처리방식으로 바뀌면서 위험에 대한 종류도 하드웨어 중심에서 응용 소프트웨어 및 사용자 중심으로 바뀌고 있다는 것을 알 수 있으며 이와 같은 결과를 고려하여 보안대책 설정시 기준으로 삼아야 할 것이다.

또한 입출력 단계에서 위험도가 높은 자산인 Sybase client module은 자산 피해 영향과 업무 프로세스에 미치는 심각성보다도 취약성이나 위협발생으로 인한 위험발생 가능성이 훨씬 높게 나타났다. 이는 위험발생 가능성을 제어만 한다면 다른 자산의 위험수준보다도 더욱 큰 효과를 볼 수 있는 자산이 될 수 있다. 즉, 다른 자산에 비해 자산 피해 영향과 업무 프로세스

에 미치는 심각성 정도는 차이가 나지 않으나 위험발생 가능성은 <표 11>에서와 같이 다른 자산과 많은 차이를 보여주고 있다.

Sybase client module과 관련된 위협은 프로그램 개발 및 변경으로 인한 위협, OS의 문제점으로 인한 위협, 접근통제 권한 부여 및 사용자의 운영상 부주의, 악성 프로그램을 보유하고 있는 소프트웨어 사용으로 인한 위협 등이 발생빈도가 높았으며, 이는 클라이언트/서버 분산방식의 개방형 시스템으로서 데이터나 시스템에의 부적절하고 비합법적인 접근과 연관된 위협으로서 응용시스템에 대한 유지 관리 및 접근통제에 대한 위협을 억제할 수 있는 보안대책이 시급하다.

Sybase client module의 취약성은 관리적 취약성과 기술적 취약성의 대책이 시급한 것으로 나타났으며, 특히 복잡해진 시스템으로 인한 패스워드 및 접근통제로 인한 기술적 취약성이 심각한 것으로 나타났다. 따라서 위협과 취약성을 감소 및 제어할 수 있는 보안대책이 필요하다. 보안대책이 모든 위협을 다 해결할 수 있는 것은 아니며 한 가지 위협만 해결되는 것도 아니다. 그러므로 보안대책 결정시 많은 위협과 취약성을 해결할 수 있는 보안대책을 도출하여야 할 것이다.

처리/요구 단계에서 위험수준이 높게 도출된 자산은 시스템 관리자와 DB 관리자이다. 이 자산들은 데이터의 분산화나 처리 분산화에 기여하는 사용자로서 관련된 위협으로는 보안에 대한 부족한 인식, 관리 실수로 인한 미흡한 대처, 인력부족으로 인한 위협, 부족한 교육 등이었으며 취약성은 관리적 취약성이 심각하게 나타났다. 특히 취약성 분석에서도 보안인식 부족이나 접근통제에 관련된 취약성이 높게 나타났다.

시스템 관리자와 DB 관리자 자산은 사용자로서 인적요소를 고려한 보안대책인 보안관리에 대한 철저한 교육 및 홍보, 보안 전문가의 인력 보충 등의 관리적 측면의 보안대책이 시급한 것으로 평가된다.

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 핵심기능인 위험관리에 대한 연구가 진행되고 있으며, 다양한 위험관리 모형이 제시되고 적용되고 있다.

또한 복잡한 구조로 변화되고 있는 정보시스템 환경에 적합한 위험관리 모형에 대한 연구가 필요하며 다각도로 많은 정보시스템에 대한 사례 적용을 통해 국내 환경에 맞는 위험관리 모형 및 위험분석 도구의 개발과 적용이 시급한 상황이다.

본 논문에서는 빠르게 변모되고 있는 정보시스템의 환경에 대응하고 정보시스템의 궁극적 목적인 정보시스템 업무를 지속적으로 수행할 수 있도록 정보기술 보안 위험을 식별하고 이러한 위험에 대한 특징 및 위험의 수준을 사례 적용을 통하여 분석하였다.

자산위주의 분석방법보다는 자산으로 인해 정보시스템 업무 수행에 어떠한 영향을 주는지 업무 프로세스 중심으로 위험을 분석, 위험수준을 도출하였으며, 클라이언트/서버 분산방식의 특성으로 인해 생길 수 있는 위험의 유형을 분석하여 현실적인 보안대책 결정의 기준 자료로 제시하였다.

사례 분석을 통해 D대학의 클라이언트/서버 시스템은 입출력 단계에서 응용시스템의 관리, 접근통제 및 권한 부여 등이 문제점으로 나타났고, 처리/요구 단계에서는 사용자에 대한 보안 중요성 인식 부족 등으로 인한 위험이 심각한 것으로 나타났다. 주로 물리적인 위험보다는 관리적, 기술적 위험이 중요시되고 있으며, 아직까지는 사용자로 인한 위험으로 심각한 재해를 가져오지는 않았으나 향후 사용자에게 보다 많은 전산 업무능력과 통제권한을 부여하는 클라이언트/서버 시스템의 특징으로 인해 학사관리 업무의 마비 또는 개인의 프라이버시 침해 등 심각한 위험을 초래할 수 있으며 이에 대한 효율적인 보안대책이 시급하다고 할 수 있다.

다만, 본 적용 사례는 적용시 모형의 각 프로세스에 대한 정확성, 효율성, 시간, 비용, 자동화 도구 적용 가능성 측면에서 검토하고 공공기관, 기업, 연구소 등을 대상으로 조직규모와 시스템 환경별로 다각도로 검증하는 것이 필요하다. 또한 위험분석 방법론을 개발하여 본 모형을 기반으로 실제 적용하면서 도출되는 문제점과 국내 정보시스템 환경에 쉽게 적용할 수 있는 특성화된 모형에 대한 연구가 지속적으로 수행되어야 하며 위험관리의 효율화를 위한 소프트웨어의 개발에 대한 연구도 이루어져야 할 것이다.

참고문헌

Ahn, C. S., Cho, S. K., (2002), A Risk Management Model for Efficient Domestic Information Technology Security, *Journal of the Korea Institute of Industrial Engineers*, **28**, 44-56.

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

CCTA. (1998), *The CCTA Risk Analysis and Management Method : CRAMM,* Central Computer and Telecommunications Agency.

Fried, L.(1993), Distributed Information Security, *Information Systems Management*, summer, 56-65.

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

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

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

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

Ken Otwell, Bruce Aldridge.(1990), The Role of Vulnerability in Risk Management, *IEEE*, 32-38.

Kim, H. B., (2000), Risk Analysis and Management Standards for Public Information Systems Security : Risk Analysis Methodology Model, *Journal*

of Telecommunications Technology Association, **69**, 62-73.

Kim, J. P., Park, D. S., Lee, S. J.,(2003), *The point of Information Security Knowledge*, Jungil.

Korea Information Security Agency,(2001), *Concept of Information Security*, Kyowoo.

Lee, S. J., (2000), The controls of Client-Server System : Case Studies of Bank, *Korean Management Science Review*, **17**, 97-113.

NCA.(1998), *A Study on the Contingency and Disaster Recovery Plan for the Public Information System*, National Computerization Agency.

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

Park, T. G., Kang, C. K., Kim, D. H., .(1996), Security Management of Network System, *Korea Institute of Information Security & Cryptology Review*, 6, 95-114, *Journal of MIS*. 129-147.

Ryan, S.D., B. Bordoloi.(1997), Evaluating Security Threats in Mainframe and Client/Server Environments, *Information & Management*, **32**, 137-146.

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

안춘수
경일대학교 산업공학 학사
동국대학교 산업공학 석사
동국대학교 산업공학 박사 과정 수료
현재: (주)투이정보기술 연구소 선임연구원
관심분야: 의사결정, 정보기술 보안 위험관리

조성구
서울대학교 산업공학 학사
한국과학원 산업공학 석사
프랑스 Aix-Marseille Ⅲ 대학 경영과학 박사
현재: 동국대학교 산업시스템공학부 교수
관심분야: 의사결정, 위험관리, 프로젝트관리