위험분석모델의 정보시스템 구축방법론 적용에 관한 연구

박 동 석* 안 성 진* 정 진 욱*
* 성균관대학교 컴퓨터교육과

요 약

조직의 정보시스템이 직면한 위험을 분석할 수 있는 위험분석모델을 정보시스템구축 방법론에 적용하여 정보시스템 구축을 진행하면서 위험분석 결과를 반영할 수 있도록 하였다. 위험분석은 조직의 정보자산에 대한 위협과 취약성, 그리고 대응책간의 함수관계를 활용하는 방법으로 조직이 보유한 정보자산에 내재한 취약성의 영향범위와 이에 대응하고 있는 위협의 빈도와 강도 그리고 위협에 대한 대응책의 적용정도를 분석해 종합적인 정보위험수준을 평가하는 방법이다.

The Study of Developing an Index for Evaluating

Park Dong Suck*Ahn Seong Jin*Chung Jin wook*

ABSTRACT

The purpose of this study is to reflect the risk analysis results acquired while building an information system of an organization by applying a risk analysis model capable of analyzing the confronted risk, on the information system build methodology. Risk analysis, a method of utilizing the functional relation between risk, vulnerability and countermeasure of information assets, is used to evaluate the overall information risk level by analyzing the influence range of vulnerability imposed in the information asset of an organization, and the applications of the countermeasures on the frequency and intensity of the corresponding risk.

1. 서 론

본 연구의 목적은 조직의 정보시스템이 직면한 위험을 분석할 수 있는 위험분석모델을 정보시스템구축 방법론에 적용하여 정보시스템 구축을 진행하면서 위험분석 결과를 반영할 수 있도록 하기 위한 것이다. 위험분석은 조직의 정보자산에 대한 위협과 취약성, 그리고 대응책간의 함수관계를 활용하는 방법으로 조직이 보유한 정보자산에 내재한 취약성의 영향범위와 이에 대응하고 있는 위협의 빈도와 강도 그리고 위협에 대한 대응책의 적용정도를 분석해 종합적인 정보위험수준을 평가하는 방법이다. 위험분석을 위한 기존의 연구사례는 ISO/IEC TR 13335 GMITS(Guidelines for the Management of IT Security) 표준을 바탕으로 한 정보보호진흥원의 CI2RAM(주요정보통신기반시설 취약성분석 평가 방법론), NIST의 Risk Management Guide for IT System, BS7799(ISO/IEC 17799-1), IAM(INFOSEC Assessment Methodology), VAF(Vulnerability Assessment Framework), IPAK(Information Protection Assessment Kit) 등이 있다. 정보시스템 구축방법론은 정보시스템 구축의 기획/분석/설계/구현 및 이의 유지보수와 관련된 사항의 성공적인 수행과 구축에 따른 시행착오를 감소시키기 위한 도구로서 정보시스템 구축방법론을 위한 기존연구는 ISO/IEC 12207, Method1 방법론, 객체지향방법론, 삼성 SDS의 Innovator, ISACA의 CobIT 등이 있다. 위험분석 모델과 정보시스템구축방법론은 각각 독자적으로 연구가 진행되어 왔으나 위험분석 모델을 정보시스템 구축방법론에 적용하는 적용성에 대한 연구사례는 찾아볼 수 없다. 위험분석모델을 정보시스템 구축 방법론에 적용한 것은 정보시스템을 구축하여 운영하기 전에 정보시스템의 위험을 인식하고 대처함으로써 예방적 차원에서 접근하여 정보시스템이 구축된 사후에 정보보안 위험분석을 실시함에 따른 시간과 경제적인 손실을 최소화하기 위한 것이다. 본 연구에서 참조된 위험분석 모델은 ISO/IEC TR 13335 GMITS(Guidelines for the Management of IT Security) Parts1,2,3,4,5 표준과 NIST의 Risk Management Guide for IT System, 정보보호진흥원의 CI2RAM(Critical Infrastructure Information & Communication Risk Analysis Model, 주요정보통신기반시설 취약성분석 평가 방법론) 이며 정보시스템 구축방법론은 삼성SDS의 Innovator를 참조하였다.

2. 정보시스템 구축 방법론의 위험분석 모델 적용

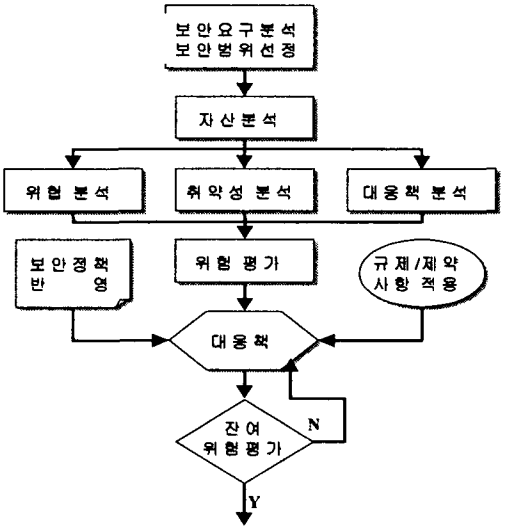


그림 2-1 위험분석모델

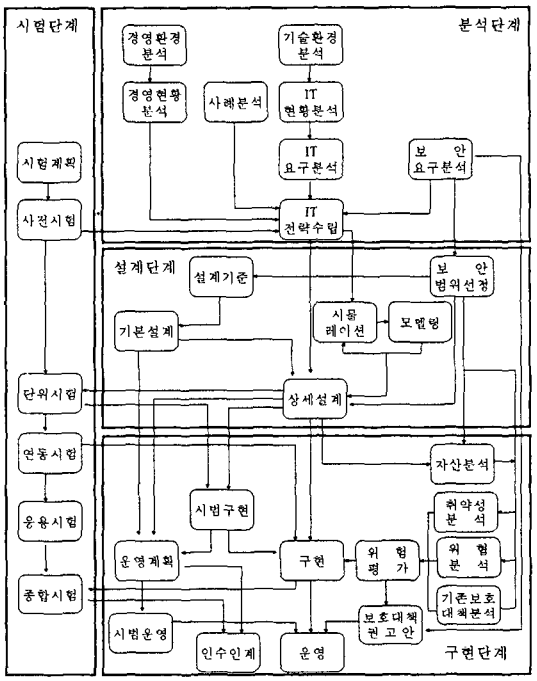


그림 2-2 위험분석모델의 적용

삼성SDS의 SI를 위한 방법론인 Innovator에 따르면 정보시스템구축은 4단계 (분석단계, 설계단계, 구현단계, 시험단계)로 구성되어 있으며 정보보호진흥원의 CI2RAM(Critical Infrastructure Information & Communication Risk Analysis Model, 주요정보통신기반시설 취약성분석 평가방법론)에 따르면 위험분석은 보안요구분석, 보안범위선정, 자산·위협·취약성·기존보호대책분석, 위험평가, 보호대책권고안 마련으로 구성되어 있다. 정보시스템 구축방법론에 위험분석모델을 적용하기 위해 분석단계에 보안요구분석프로세스 적용하였으며 설계단계에 보안범위선정 프로세스를 적용하였고 구현단계에 자산·위협·취약성·기존보호대책분석, 위험평가, 보호대책권고안 프로세스를 적용하였다

2-1 분석단계

분석단계에서는 정보시스템 구축 방법론의 환경분석(경영환경분석과 기술환경분석)과 현황분석(경영현황분석과 IT현황분석) 활동에 위험분석을 위한 보안요구분석 프로세스를 추가하였다. 추가된 보안요구분석 프로세서에서는 조직의 현황을 파악하고 담당자들과의 면담을 통하여 요구사항 명세서를 작성하는 활동을 한다. 이 프로세스에서 도출한 기초 자료들이 IT 전략수립과 함께 위험분석 각 프로세스들의 기본 자료로 사용되므로 요구사항을 정확히 도출해야 된다.

(가) 자료분석

자료 분석 활동에서는 조직의 현황을 파악하기 위해 설문지, 질문서 및 담당자 회의를 통해서 필요자료를 수집한 다음 수집된 자료를 관계자 면담 직전에 분석하고 미흡한 세부적인 내용은 관계자면담을 통해서 수집할 수 있도록 준비한다.

(나) 관계자면담

관계자 면담 활동에서는 조직의 상위 관리자부터 실무 책임자까지의 면담을 통해서 이전 자료분석 태스크부분에서 부족한 부분을 보완하고 해당 조직이 요구하는 요구명세를 작성하기 위해 준비하는 과정이다.

(다) 요구명세 작성

요구명세서 작성 활동에서는 위험분석의 첫 산출물로서, 앞으로 진행될 정보시스템구축을 위한 IT전략 수립과 보안범위선정 단계에서 반드시 고려해할 요구명세서를 작성하는 것이며 이 내용은 위험분석의 보호대책 권고안 수립 단계에서 반드시 반영되어야 한다.

2-2 설계단계

설계단계에서는 정보시스템 구축방법론의 기본설계와 상세설계를 진행하는 활동에 위험분석의 보안범위선정 활동을 추가하였다. 추가된 보안범위선정 프로세스에서는 업무현황 파악활동과 핵심업무 선정활동, 업무 구성도 작성활동, 경계 확정활동, 평가계획 수립활동을 하게된다. 보안범위선정 프로세스에서 도출한 결과가 설계기준에 반영되며 상세설계의 기본자료가 된다 또한 위험평가를 위한 자산분석과 취약성·위협·기존보호대책 분석의 기준이 된다

(가) 업무현황 파악

업무현황 파악 활동에서는 정보시스템구축 방법론의 IT전략수립 결과를 바탕으로 조직의 업무영역별 현황 목록을 분석한다. 목록에는 업무명, 사용 부서명, 타 업무와 연관되는 업무명 등을 포함할 수 있도록 하고 요구사항 분석 결과를 토대로 업무별로 임무는 무엇인지에 대해서 파악하는 활동이다.

(나) 핵심업무 선정

업무현황 목록을 기반으로 위험 분석 대상이 되는 조직의 핵심업무들을 선정한다. 핵심업무의 대상이 될 수 있는 것은 국가적으로 중요성을 가져야 하며, 경제 사회적인 파급효과가 큰 것이다.

(다) 업무 구성도 작성

핵심업무별로 업무 구성도, 구축예정인 물리적인 시설에 해당하는 네트워크 구성도, 이들이 모두 포함된 아키텍처를 수립하도록 한다. 그리고 조직도 구성현황을 작성할 때 조직과 업무 흐름에서의 역할 등이 잘 나타날 수 있도록 한다.

(라) 평가 계획 수립

요구명세서, 업무 구성도, 네트워크 구성도 및 조직의 구성현황 등을 이용하여 위험분석을 위한 투입인력, 시간 등의 일정관리계획을 수립하는 활동이다.

2-3 시험단계

정보시스템구축 방법론의 시험단계에서는 장비시험과 응용시험 그리고 종합시험을 실시하게 되는데 응용시험에서 모의해킹 등 위협에 대한 취약성시험을 병행 할 수 있다

2-4 구현단계

정보시스템구축 방법론의 구현단계에서는 제품선정과 시공을 통한 구현, 그리고 운영을 하게 되는데 위험분석 모델의 자산·위협·취약성분석 프로세스와 위험평가결과를 바탕으로 한 보호대책 권고안 프로세스를 추가하였다. 자산·위협·취약성분석에 따른 위험평가 결과를 정보시스템 구현에 반영하고 보호대책 권고안을 마련하여 운영에 반영토록 한다.

(1) 자산분석 프로세서

자산 분석 프로세스는 상세설계와 보안범위선정을 바탕으로 보호해야 할 대상인 자산을 식별하고 자산의 중요도에 따라 자산의 가치를 평가하는 프로세스이며 자산분류와 자산가치산정 활동을 한다.

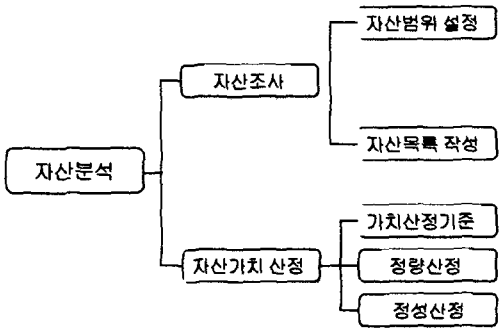


그림 2-3 자산분석 프로세스

(가) 자산 조사

자산 조사 활동은 중요 자산에 대한 적절한 보호가 취해질 수 있도록 상세설계를 바탕으로 자산을 체계적으로 조사하는 것을 의미한다. 자산을 조사한 그림 2-4의 Hawk의 자산분류방법 등을 이용해 자산목록을 만든다.

(나) 자산 가치 산정

자산 가치 산정 활동은 분류된 자산을 사업과 업무의 중요도 및 요구사항에 따라 가치를 평가하는 활동이다. 자산의 중요도 및 특성을 파악하여 중요 자산 목록을 작성하고 보안 요구사항 등을 고려하여 자산 분류기준을 수립하여 자산 가치를 평가한다. 자산의 가치 산정으로 중요자산의 영역을 재분류하여 대상 영역을 줄인다. 평가하는 방법은 보안 요구사항을 기반으로하여 계량화 단위로 나타낼 수 있는 정량적인 분석과 정성적인 분석 중 선택하여 적용할 수 있다.

구분	내용	세부항목
하드웨어 (H/W)	전산시스템에서 기계적, 전자적, 전기화학적인 물리적 특성을 갖는 자산 (데이터를 작성·입력(연산, 저장, 출력 등)으로 처리할 수 있는 능력을 가짐	시스템 본체, HDD(내/외장), Catridge Tape, CD-ROM, Disk Array, System Terminal, 광파일 서버, Juke Box, 프린터, 프린터 서버
운영체제 (O.S)	컴퓨터 H/W를 효율적으로 운영하기 위한 일종의 S/W 자원의 관리 및 사용 / 처리능력의 자동화로 운영의 능률과 신뢰성을 높임	UNIX, DOS, Windows3.1/95/98/2000/NT, LINUX, MVS, MacOS, BeOS
네트워크 (Network)	데이터를 서로 다른 시스템간에 공유할 수 있는 기능을 제공할 수 있는 H/W 및 S/W	Network OS, OS Application, DSU, HUB, Router, Repeater, Bridge, Gateway, ESS(교환기), Modem, Interface Card, Cabling, Protocol Types, LAN Types, WAN Types, Firewall, Access Control S/W
데이터 (Data)	전산 시스템에 저장, 처리, 연산될 수 있는 전자 정보	User's Data, Employee Data, Financial Data, Contract Data, Project Data, System Data
응용S/W (Application S/W)	컴퓨터 시스템을 문서편집, 금융계산, 정보처리, 계산 등 사용자가 필요한 특정 분야에 사용하기 위하여 작성된 소프트웨어	Word Processor, DBMS, Spread Sheet, Office
사용자 (User)	정보시스템을 사용하는 운영자, 개발자, 분석가, 이용자 등의 모든 인력	System Administrator, Risk Analyst, Risk Manager, Security Manager, System Operator, Application Programmer, Project Manager, IS Auditor, Product Vendor, System Programmer, Data Base Administrator
환경 (Environment)	정보 시스템과 간접적 환경을 가지고 있는 위협, 무형 자산	Security Controller for external device(Robot,), 무정전전원장치(UPS), CO2 화재진압 시스템, 항온항습기, 자폐벽, Fax machine 등

그림 2-4 Hawk의 자산분류방법

(2) 취약성 분석 프로세스

취약성 분석 프로세스는 위협 시나리오에 의해 중요 자산의 취약성을 식별하고 취약성을 평가하는 활동을 한다

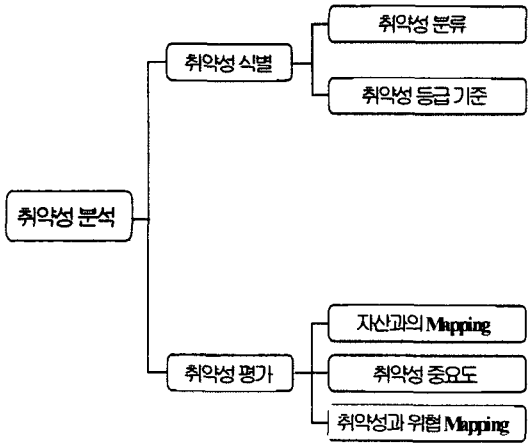


그림 2-5 취약성분석 프로세스

(가) 취약성 식별

취약성 식별 활동은 조직 내부 혹은 정보시스템을 사용하는 환경 등에 내재된 약점으로 인한 위협 시나리오에 기준한 취약성을 분류하고 취약성의 등급을 나눈다.

(나) 취약성 평가

취약성 평가활동은 자산과의 매핑과 취약성 중요도 취약성과 위협 매핑을 통해 취약성의 수준을 평가한다.

(3) 위협분석 프로세스

위협 분석 프로세스는 시스템 및 조직, 조직의 자산을 손상시키는 잠재성을 가지고 있는 위협을 인간과 비인간 측면에서 식별하고 이를 통해 위협 위협의 빈도와 강도를 분석하여 위협의 순위를 정하는 프로세스이다.

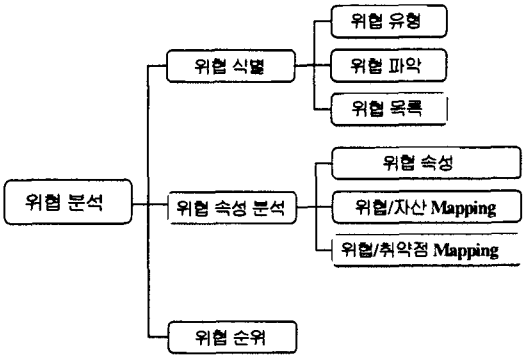


그림 2-6 위협분석 프로세스

(가) 위협 식별

위협 식별 활동은 중요 자산에 대한 위협을 인간(고의적, 비고의적)과 비인간(자연, 시스템 오류 등)의 측면을 분류하여 유형을 식별하고 위협 목록을 만든다.

(나) 위협 속성 분석

위협 속성 분석 활동은 위협 속성을 정의하고 위협과 자산을 매핑하며 위협과 취약성 매핑을 통하여 정의된 위협 유형 식별 후, 자산의 취약성을 이용할 수 있는 가능성을 확인할 수 있는 활동이다. 이 활동에서 위협이 실제 중요 자산의 취약성을 이용할 수 있는지 여부를 확인하고 새로운 형태의 위협을 검증할 수 있는 단계이다.

(다) 위협 순위

위협 순위 활동은 자산 가치 산정을 통하여 분류된 중요 자산에 대하여 식별된 위협의 유형을 토대로 위협의 빈도와 영향을 계산하는 방법으로 위협을 평가한다. 이때 위협의 빈도는 정성적인 방법을 이용하여 사용하나, 점차적으로 정량적인 방법으로 변환해 가는 방향을 권장하며, 위협의 영향 역시 빈도와 동일한 방법으로 평가를 한다.

(4) 위험 평가 프로세스

위험 평가 프로세스에서는 요구사항 분석, 범위 선정, 자산 분석, 위협 분석, 취약성 분석, 기존 보호대책의 분석을 통해서 도출된 자료를 기반으로 위험을 산정하고 위험 순위를 결정하여 우선 순위를 결정한 후에 위험 평가의 영역을 결정하는 프로세스이다.

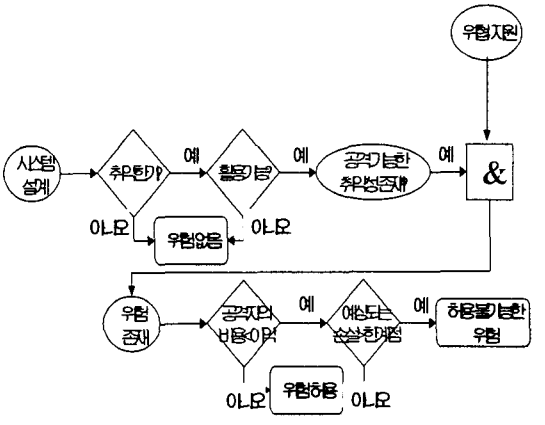


그림 2-7 위험평가 프로세스

(가) 위험 산정

위험산정 수행기법에는 결과성격에 따른 분류와 요구사항(수준)에 따른 분류로 나뉠 수 있다. 결과성격에 따른 위험산정구현방법에는 정량적 접근방법(Quantitative Approach)과 정성적 접근방법(Qualitative Approach)이 있으며 요구사항(수준)에 따른 위험산정 구현방법에는 기본통제선 접근방법(Baseline Approach)과 위험분석 접근방법(Risk Analysis Approach)이 있다. 조직에 적합한 위험산정 방법을 선택하도록 한다.

<표 2-1> 위험산정 수행기법 분류]

구분	내 용	비 고
결과성격	정량적 접근방법 (Quantitative Approach)	위협의 영향, 빈도, 가능성 등을 수리적으로 평가하는 방법 종류 : 수학공식 접근법, 확률분포, 확률지배, 몬테카를로 시뮬레이션, 과거자료 분석법 비용/가치분석, 예산계획, 자료분석이 쉬운 반면 분석의 시간, 노력, 비용이 큰 단점이 있다
	정성적 접근방법 (Qualitative Approach)	손실크기를 화폐가치로 측정할 수 없을 때 분석가의 경험 및 지식에 기초하여 위험을 분석하는 방법 종류 : 델파이법, 시나리오법, 순위결정법, 퍼지행렬법, 질문서법 금액화하기 어려운 정보의 평가가 가능하고 분석시간이 짧고 이해가 쉬운 장점이 있는 반면 평가 결과가 주관적이어서 사용자에 따라 달라질 수 있는 단점이 있다
요구사항(수준)	기본통제 접근방법 (Baseline Approach)	일반조직에서 공통적으로 사용되는 최소한의 정보보호대책으로서 널리 알려진 위협요인에 대한 통제수단을 제시 분석, 대응책 선정이 용이하고 경제적이나 새로운 위협에 대처가 곤란하며 조직의 실질적인 정보보호수준을 정량적으로 드러내기는 어려운 단점이 있음
	위험분석 접근방법 (Risk Analysis Approach)	정보시스템 종류의 다양성과 환경의 특수성으로 인해 각 조직 고유의 위협을 식별하고 이의 영향을 측정하여 비용효과적인 보호대책을 수립하고자 하는 접근방법 자체적으로 적용하기 위해서는 높은 수준의 전문가와 위험분석의 효율성을 제고해 줄 수 있는 자동화툴이 필요하며 상당한 노력이 요구되어 일반적으로 복잡하고 비용이 많이 드나 조직의 상태를 파악하고 새로운 위협에 대한 대처방법에 적합함

(나) 위험 순위 결정

위험 순위 결정 활동은 위험 산정 활동에서 나온 결과치를 이용하여 우선 순위를 결정한다. 위험의 크기는 표 2-2 위험순위 계산방법에 따라 높음(50~100), 중간(10~50), 낮음(1~10) 단계로 나눌 수 있으며 높은단계는 즉시조치가 필요하며 중간단계는 적절한 기일내에 조치를 취하기 위한 계획을 수립하여야 하며 낮은 단계는 수용가능 여부와 조치필요를 판단하게 된다

<표 2-2> 위험순위 계산방법

	낮음 (10)	중간 (50)	높음 (100)
높음(1.0)	낮음(10*1.0=10)	중간(50*1.0=50)	높음(100*1.0=100)
중간(0.5)	낮음(10*0.5=5)	중간(50*0.5=25)	높음(100*0.5=50)
낮음(0.1)	낮음(10*0.1=1)	중간(50*0.1=5)	높음(100*0.1=10)

※ 위험의 크기 : 높음(50~100), 중간(10~50), 낮음(1~10)

(다) 위험 영역 결정

위험 영역 결정 활동은 산정된 위험도를 토대로 우선 위험 순위를 결정하고 시간, 비용, 기술, 사회, 환경과 법률 등의 규제사항과 조직의 정책과 업무규정 등을 고려하여 위험 영역을 결정하는 활동이다.

(5) 보호대책 권고안 프로세스

보호대책 권고안 프로세스는 기술적, 물리적, 관리적 측면에서 위험 평가의 결과를 토대로 작성된 보호대책 권고(안)을 정보시스템 구축 운영 프로세스에 제공하여 정책으로 결정되게 한다.

(가) 보호 대책 분류

보호 대책 분류 활동은 위험 평가의 결과를 이용하여 위험을 회피, 전이, 감소, 허용 등의 결정

단계에 대해 기술적, 물리적, 관리적 보호 대책으로 분류하고 단기/장기성을 고려하여 분류한다.

(나) 보호 대책 권고(안) 작성

보호 대책 권고안 작성 활동은 정보시스템의 자산 및 업무의 중요도에 따라 비용 효과적인 대응 권고안을 선정하고 정책으로 활용되도록 하는 활동이다.

3. 결 론

이 논문에서는 정보시스템이 직면한 위험을 분석할 수 있는 위험분석모델을 정보시스템구축 방법론에 적용하기 위한 방안을 제안하였다. 분석단계에서는 보안요구사항분석프로세스를 추가하여 구축대상 정보시스템의 보안요구사항을 사전에 인지하고 IT전략수립에 반영토록 하였으며, 설계단계에서는 보안범위선정 프로세스를 추가하여 정보시스템에서 보안이 필요한 부분을 설계기준과 상세설계에 반영하도록 하였다 또한 구현단계에서는 자산·위협·취약성분석결과에 따른 위험평가결과를 정보시스템 구현에 반영토록 하여 본격적인 운영을 실시하기 전에 보안위험에 대비할 수 있도록 하였다. 정보시스템 구축 방법론에 위험분석 모델을 적용함에 따라 얻을 수 있는 효과는 정보보안활동을 정보시스템을 구축과 병행토록 하여 정보보안시스템 구축의 과다투자 및 이중투자를 사전에 방지하고 예방적 차원의 정보보안 정책을 수립할 수 있으며 향후 정보시스템을 변경하거나 증설할 경우 정보보안이 자동으로 연동될 수 있도록 한 것이다. 본 방법론은 정보시스템을 구축하고 있거나 구축예정인 대다수 프로젝트에 적용할 수 있을 것으로 보인다. 본 연구는 정보시스템 구축 전문가가 정보시스템 구축 업무를 수행함에 있어 함께 고려하고 검토해야할 위험분석의 기본적인 프로세스를 추가하여 정리한 것이므로 이해를 요하는 관련 종사자에 도움이 될 수 있을 것으로 보인다

참고문헌

[1] ISO/IEC TR 13335 GMITS(Guidelines for the Management of IT Security) (Parts1,2,3,4,5) (www.iso.org)

[2] Risk Management Guide for IT System(www.nist.gov)

[3] 한국정보보호진흥원 CI2RAM(Critical Infrastructure Information & Communication Risk Analysis Model, 주요정보통신기반시설 취약성분석 평가 방법론)(www.kisa.or.kr)

[4] 한국정보통신인력개발센터, 삼성SDS, "SI를 위한 방법론 innovator",2001.

[5] 정보기술교육원, NETWORK 설계기법, 1998.

[6] 정진욱, 컴퓨터네트워크, 희중당, 1999.

[7] 한국정보통신인력개발센터, "IT-Networker", p212-214, 2001.

[8] 김동윤, "근거리통신망(LAN) 구축 지침서",http://ccl.chungnam.ac.kr/QosIP/LANcont/LAN/guide.htm, 1998.

[9] 박동석, The Study of Developing an Index for Evaluating the Quality of The Network, 2000 성균관대학교 석사학위 논문

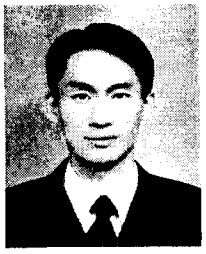
[10] 한국정보보호진흥원, 보호프로파일 개발을 위한 위험분석, p17-24, 2000.

[11] 한국정보보호센터, 정보보호표준교재, p292-296, 1999. 1

[12] Donald R. Peeples, Inforsec Risk Management:Focused, Integrated & Sensible, NSA,

[13] Joan Fowler and Robert C. Seate III, Threats

and Vulnerabilities for C4I in Commercial Telecommunications:A Paradigm for Mitigation, Data Systems Analysts, Inc.



박 동 석

1995년 서울산업대학교 전자공학과(공학사)

2001년 성균관대학교 정보통신공학과(공학석사)

1999년 정보통신 기술사

1995년 ~ 현재 서울시청 DMC(디지털미디어시티) 추진단

2001년 ~ 현재 성균관대학교 컴퓨터교육과 겸임교수

관심분야 : 네트워크 보안, 도시계획과 정보통신인프라, 미디어스트리트, 유비쿼터스

안 성 진

1988년 성균관대학교 정보공학과 졸업 (학사)

1990년 성균관대학교 대학원 정보공학과 졸업 (석사)

1998년 성균관대학교 대학원 정보공학과 졸업 (박사)

1990년 ~ 1995년 시스템공학연구소 연구 전산망 개발실 연구원

1996년 정보통신 기술사 자격 취득

1999년 ~ 현재 성균관대학교 컴퓨터교육과 조교수

관심분야 : 네트워크 관리, 트래픽 분석 ,보안 관리

정 진 욱

1974년 성균관대학교 전기공학과 학사

1979년 성균관대학교 대학원 전자공학과 석사

1991년 서울대학교 대학원 계산통계학과 박사

1982년 ~ 1985년 한국과학기술 연구소 실장

1981년 ~ 1982년 Racal Milgo Co. 객원연구원

1985년 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 교수

관심분야 : 컴퓨터 네트워크, 네트워크 관리, 네트워크 보안