전산망보안을 위한 위험관리기술지원서 개발 연구[1)]

° 임채호*, 박태완**, 이경석***[2)]
* 대전실업전문대학, ** I.S.K., *** 산업연구원

A Study on Developing Technical Guideline of Risk Management for Computer Network Security

Chae-Ho Lim*, Tae-Wan Park**, Kyung-Seok Lee***
* Taejon Vocational Junior College, ** ISK, *** KIET

1. 배경 및 필요성

국내에서 최근 빈발하고 있는 전산시스템에서의 범죄나 보안사고들은 정보화사회로의 발전에 가장 문제가 되는 걸림돌이 되는 것이다. 은행에서의 온라인시스템에서의 범죄는 자주 발생되는 컴퓨터범죄의 하나이며, 국가기간전산망인 행정전산망에서의 국민의 개인정보에 대한 프라이버시 침해 등이 심각하게 우려되고 있다. 또한 최근 모 백화점에서의 고객정보가 임의로 누출되어 범죄의 대상으로 비화된 사건은 컴퓨터보안의 중요성을 잘 일깨워주는 사례라고 보겠다.

하지만 이러한 사례에서 드러나듯이 현재 국내에서는 전산망 보안을 위한 여러 대책을 제대로 세우고 있지 않고 있으며, 보다 체계적인 관리적, 기술적인 방법을 잘 알지 못하는 경우가 허다한 것으로 파악되고 있다. 그리고 자신의 조직에서 시스템이 보안상 어떤 부분이 취약하고 또 이러한 취약성으로 인해 어떤 위험이 도사리고 있는지 그 위험으로 인해 얼마나 손실을 볼 수 있는지 적절하게 파악할 수 없으로 더욱 문제의 심각성이 있다고 보겠다. 조직의 최고 경영자는 전산시스템과 전산망의 보안위험이 어떻게 얼마나 자신의 조직에 손실을 줄수 있다는 사실을 정확하게 인식할 수 없으므로 보안대책에 대한 투자는 인색하기 마련이며, 전산시스템 관리자는 보안위험 분석 방법론을 몰라 최고경영자의 투자 결정을 지원할 수가 없어 계속적으로 체계적인 보안대책을 만들지 못하는 것이다.

어떠한 조직에서 보안관리를 위해 맨 처음 선행되어야 할 것은 위험분석이다. 위험분석은 다음과 같은 목적을 위해 진행된다.

① 전산시스템 취약성 발견과 확인
시스템의 결함이나 이용자의 잘못에 대비하여 전산시스템은 나름의 보안기능을 가지고 있다. 그러나 어디에 위험이 있는지 모른다면, 시스템 보안의 존재를 우선 백지화된 상태로 생각하는 입장에서 위험을 확인하는 것이 중요하다. 위험분석은 시스템템에서의 손실이 어떠한 측면에서 발생할 수 있는지 취약성의 발견·확인에 도움이 된다.

② 컴퓨터 범죄에 대응
컴퓨터범죄가 시스템의 보안이 파괴됨에 따라 발생하는 것이라고 볼때 위험분석은 컴퓨터 범죄를 방지하는데 유용한 기본 방법제시할 것이다.

③ 조직에 주는 손실확인과 대응
위험분석 결과로서, 어떠한 손실의 형태로 어느 정도의 손실규모가 발생할 수 있는지, 또 어떻게 대응하면 좋은가를 제시할 수 있다.

1. 본 논문은 OSIA 를 통해 한국전산원의 "전산망보안을 위한 위험관리 기술지원서" 과제로 진행되고 있습니다.
2. 그밖에 위 과제에 참가한 분들의 성명은 다음과 같습니다. 김기윤(장운대), 김정덕(원광대), 김종기(국방체계연), 김현배(경인여전), 남길현(국방대학원), 류재철(충남대), 이성만(포항공대), 이재권(세동회계법인), 이필중(포항공대), 신동익(한국전산원)

④ 조직과 전산시스템파악
위험분석을 통해 그 조직의 취약성과 손실등을 파악함으로서 조직이 얼마나 전산시스템을 의존하는지 전산규모가 적당한지등이 파악된다.

여기에서는 국가기간전산망에 속한 기관을 대상으로 위험관리 및 위험 분석이란 무엇이며 위험관리와 위험분석을 어떻게 할 것이며, 어떻게 하면 효율적으로 손쉽게 위험분석을 할 수 있을지 제시하는 문서(안)을 보이기로 한다.

2. 요구사항 분석

2.1 기술지원서의 요구사항

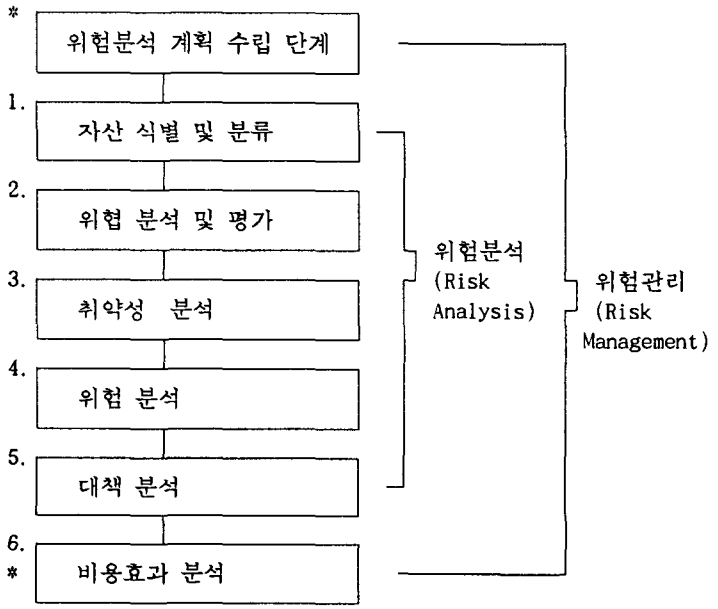
기술지원서의 사용자는 "국가기간 전산망 가입기관"으로서 주로 국가기관을 대상으로 하며, 이는 사용자들이 이 지원서를 참고하여 자신의 조직에서 비교적 손쉽고 효율적인 보안 위험분석과 관리를 할 수 있도록하는 것이다. 그러므로 위험관리와 위험분석에 대한 이해를 쉽게 해주고 또한 따라야 해야할 업무와 절차를 정확하게 명시하여 무엇때문에 어떤 절차로 해야한다는 사실을 잘 일깨워야 한다. 또한 보다 손쉽고 단순한 위험분석 방법을 제시하여 큰 수고를 치르지 않더라도 자신의 조직과 전산시스템의 취약성을 파악하고 예상되는 손실과 영향을 파악함으로서 적절한 보안대책을 강구하도록 도와 주어야 한다.

2.2 해외 관련 표준 분석

생략, "해외 보안위험방법론 현황 및 분석" 및 "위험분석 방법론 : 분류와 선택기준" 참고

3. 기본 모델

위험관리를 위한 기본적인 개념과 체계는 "위험관리의 체계 연구"를 참고하기 바라며 여기에서는 우선 일반적인 절차에 의한 모델을 간단하게 소개한다. 우선 [그림 1]은 일반적인 위험분석과 관리에 대한 절차를 보여주고 있다.



[그림 1] 위험분석/관리 단계별 구성요소

1) 자산 식별 및 분류: 보호해야할 전산자원들의 체계적인 분류를 통해 소유하고 있는 자산들의 가치를 평가하고 이는 정량화된 가치를 추출한다면 위험분석 과정을 통해 보호해야 할 기준이 마련되고 에에 대한 대책도 강구되므로 가장 기본적인 단계이다.

2) 위협분석 및 평가: 분류되고 가치가 평가된 자산들이 어떤 위협요소가 있는지 알아내는 단계인데, 여기에는 그 위협적인 요소가 얼마나 발생할 확률이 있는지를 분석하는 것도 포함된다.

3) 취약성 분석 : 취약성은 정보 시스템이나 조직 목표에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어등의 약점을 확인하고 분류하여 위협을 감소시키도록 하는 것이다.

4) 위험 분석 : 자산분석과, 위협요소분석, 취약성분석을 거쳐 자산에 대한 손실을 평가 분석하는 과정으로서 위험분석의 정량적, 정성적, 혼합등의 방법론으로 나누어진다.

5) 대책 분석 : 평가된 각각의 위협요소 및 취약요소에 대한 대책(Safeguard)를 선정하는 과정으로서 이를 구현하였을때 드는 비용계산등이 이과정에서 필요하다.

6) 비용효과 분석 : 비용효과분석 과정은 위험분석과정을 거쳐 대책 선정을 할때 논리적 근거를 마련하는 과정으로서 이는 위험을 줄이기위한 결과를 정량적으로 혹은 정성적으로 보이기도 한다.

위험분석 계획 수립단계에서는 보안위험 분석을 실행하기 전에 사전 단계로서 프로젝트 참여 인원들과 위험분석 범위, 일정등을 결정하는 것이다. 이 프로젝트에 참여하는 인원은 프로젝트를 책임질 보안전문가, 위험분석을 잘 알고있는 관리자를 포함하여, 운영요원, 시스템 프로그래머, 응용 프로그래머, 시스템 사용자등을 포함시키며, 다음과 같은 내용의 프로젝트 기획문서들을 모두 숙지시킨다.

1) 개발 목적
2) 연구의 필요성
3) 관련 인원 확인
4) 기대하는 효과

그 밖에 프로젝트의 개시일과 종료일등을 명기하는데 이는 프로젝트에 참여하는 구성원의 숙련도, 대상 범위등에 의해 결정한다. 그리고 위험분석 계획수립단계와 위 위험 분석의 6)단계인 비용효과 분석 단계는 보통 위험관리에는 포함되지만 위험분석단계에는 포함하지 않는다.

4. 위험관리의 각 단계

4.1 자산 식별 및 평가

자산의 식별과 분류에 의하여 무엇을 보호해야 할지와 보호되어야 할 자산의 가치를 결정할 수 있다. 과거에는 위험분석 작업이 물리적인 하드웨어에 한정되었으나, 요즈음은 전산망을 통하여 송수신되는 데이타가 가장 중요한 자산으로 취급되기도 할만큼 전산망에서의 위험분석이 절실히 요구되고 있다.

위험분석은 전산시스템의 자산 목록작성에서 부터 시작한다. 이것이 전산망과 관련된 전체시스템의 목록이며, 하드웨어등의 유형자산에 대해서 매년 자산의 재평가를 위하여 그 잔존가치를 산정하기도 한다. 경우에 따라서는 데이타나 인적자원에 대한 항목이 이러한 자산의 평가항목에 포함되기도 한다. 즉, 자산은 컴퓨터나 가치있는 정보등의 물리적인 것에 국한되지 않고, 경우에 따라서는 인적자원, 회사평판, 사업능력, 종업원의 사기 등의 무형자산도 포함된다. 자산을 식별하고 분류하는 방법은 여러가지가 있으나 여기에서는 일반적인 방법에 따라 다음과 같이 8가지로 분류한다.

1) 하드웨어 : CPU, 주기판, 키보드, 모니터, 터미날, 개인용컴퓨터, 테이프장치, 프린터, 디스크장치, 통신회선, 접속장치, 통신제어장치, 통신매체

[표 1] 위협의 분류

분류기준	분 류	사 례
위협 원천	자연 재해	자연재해, 정전
	사람(의도적)	물리적공격(하드웨어파괴, 절도), 기술적 공격(불법사용, 불법접근, 통신선로공격, 사용방해, 사용부인, 위조, 위장등)
	사람(비의도적)	조작미숙, 조작실수, 데이타 누출등
	시스템 결함	운영체제나 프로그램 결함, 과부하, 하드웨어 고장
보안요구사항	기 밀 성	자연재해, 정전, 하드웨어파괴, 절도, 불법사용, 선로공격, 사용방해 사용부인, 위조, 위장, 유해프로그램 삽입, 망분석, 조작미숙, 실수, 데이타누출, 운영체제/프로그램결함, 과부하, 하드웨어 고장
	무 결 성	
	가 용 성	
공격대상	물리적피해	상동(단지, 각 사례들이 어느 분류에 해당되는지 식별)
	정보/데이타 피해	
	SW/프로그램 피해	
	무형자산 피해	

2) 소프트웨어 : 소스프로그램, 목적프로그램, 구입 프로그램, 자체개발 프로그램, 응용 프로그램, OS, 시스템 프로그램(컴파일러), 유지보수 프로그램
3) 데이타/데이타베이스 : 처리용 데이타, 저장 자료(디스크, 테이프,...), 출력자료, 보관용 자료, 갱신추적 자료, 감사용자료, 문헌 DB, 통계 DB등
4) 사용자/전산요원 : 사용자, 시스템이나 특정 프로그램 운용에 필요한 인원(프로그램머, 시스템 분석가, 기기운영요원, 시스템 설계자, 관리자,...)
5) 시스템 관련문서 : 프로그램 개발용, 하드웨어용, 시스템용, 일반 소프트웨어용, 전체 시스템용, 행정절차용
6) 전산자료 저장매체 : 자기디스크, 광디스크, 디스켓, 자기테이프,... 등
7) 통신망 및 관련장비 : 통신장비, 접속기, 통신회선, 교환기,... 등
8) 부대설비 : 전원장치, 항온항습기, 공기정화장치, 방재장치, 방범장치,... 등

전산망 자산에 대하여 직접적으로 자산의 가치를 산정하는 것은 매우 복잡한 일이다. 그러나 자산의 가치산정과 범위의 확정은 기관측면에서 반드시 필요하다. 자산의 가치산정 방법과 조직의 전분야에 미칠 잠재적인 영향등을 사용한 비교표를 만들어 보관하여야하며 자산의 가치산정에는 정성적 가치산정과 정량적 가치산정을 병행하여야 한다.

4.2 위협분석 및 평가

위험분석 및 관리(risk analysis and management)의 최종목적은 자산을 여러 위협(threat)으로부터 안전하게 보호하고자 하는 것이므로 위험분석은 한 조직 또는 자산에 해를 끼칠 수 있는 가능한 모든 위협들을 찾아내고 그것의 발생확률 및 그것이 미칠 수 있는 피해정도를 평가하는 것, 즉 위협분석을 포함해야 한다. 위협(threat)이란 위험분석을 위해 재고하고 있는 자산(asset)에 해를 줄 수 있는 위험의 원천 또는 잠재적인 공격을 말하는 것으로 자산가치 평가 다음으로 수행해야할 위험분석요소이다. 각 위협들은 위협원천에 따라 크게 자연재해에 의한 것과 인간에 의한 것일 수 있으며 인간에 의한 위협은 다시 의도적인 위협과 비의도적인 위협으로 나눌 수 있다. 위협분석(threat analysis)이란 자산에 해를 입힐 수 있는 가능한 모든 위협들을 규정하고 적절한 방법으로 분류하여 각 위협들의 성질을 파악하는 것이며 위협평가(threat assessment)는 이러한 위협들의 발생확률(probability of occurrence)또는 발생빈도(frequence)와 자산에 해를 입히는 정도(severity)를 평가하는 것을 말한다. 그리고 위협분석은 취약점 분석과 함께 시스템 자산을 보호하기 위한 보안수단 (security countermeasure)에 대한 요구 정도를 판단하는데 기초가 된다.

정보시스템에 대한 위협들의 매우 다양하므로 위협평가를 하기위해서는 먼저 여러 위협들을 적절한 방법으로 분류해야 하는데 다음 [표 1]과 같이 분류하였다.

앞서 설명된 각 위협들은 공격대상인 자산과 자산에 미치는 충격의 정도가 각기 다르며 발생빈도 역시 다르다. 물론 동일한 위협일지라도 시스템의 종류나 업무의 성격에 따라 위협의 정도는 다르게 평가될 수 있다. 위협평가는 각 위협들의 발생빈도(frequency) 및 위협정도(severity)를 측정하는 것으로 이 위협평가는 위협요소의 발생빈도, 충격을 주는 자산의 범위, 그리고 시스템에서 평가된 자산가치와 위협이 발생하였을 때 입는 자산의 손상률에 위해 결정되며 이 평가의 결과는 보안대책의 수립에 기초가 된다. 다음은 산출하는 방법이다.

- 발생빈도(F_j) : j 번째 위협이 일정기간 동안 발생할 횟수를 예상, $1 \le i \le n$
- 성공률 (Sj) : j 번째 위협이 성공할 확률, $1 \le i \le n$
- 위협대상의 가치(V_i) : i 번째 위협대상이 되는 자산의 가치를 평가, $1 \le i \le k$
- 위협대상의 손상비율(R_{ij}) : j 번째 위협에 의해 입을 수 있는 i번째 위협대상의 손상비율 j 번째 위협에 대한 평가는 다음의 식으로 산출될 수 있다.
  T_j는 일정기간 동안 j번째 위협에 의한 자산피해액을 나타낸다.

$$T_j = \sum_{i=1}^{k} F_j * S_j * V_j * R_{ij}$$

그리고 일정기간 동안 모든 위협들에 의해 입을 수 있는 위협대상의 피해액(T)은 다음과 같이 나타낼 수 있다.

$$T = \sum_{j=1}^{n} T_j$$

위에서 평가된 각 위협요소들의 평가값들은 정보시스템의 보안정책결정자로 하여금 적절한 보안대책을 수립할 수 있게 해줄 것이다.

4.3 취약성 분석

취약성은 정보 시스템이나 조직 목표에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어등의 약점을 뜻한다. 취약성이 있다고 해서 곧바로 손해을 입는다고 볼 수는 없으나 위협요소들이 침입할 수 있는 근거를 제공한다. 취약성 분석은 이와 같은 약점을 확인하고 분류하여 위협을 감소시키도록 하는 것이 목적이다. 따라서 취약성은 위협과 밀접한 관계가 있다. 예를 들어 화재라는 위협은 화재에 대한 부적절한 방재 대책이라는 취약성과 연관되어 있다. 또한 하나의 취약성은 하나 이상의 자산에 영향을 줄수 있다.

취약성 분석은 기존의 보호대책들과 환경을 감안하여 함께 이루어져야하며, 보호대책들이 적용되더라도 그대로 남아있거나 근본적으로 내재되어 있는 취약성에 대한 분석이 되어야 한다. 가능한 취약성을 평가함에 있어서는 전산 보안의 목적인 Confidentiality, Integrity, Availability등을 고려하여야 할 것이다.

취약성은 경영조직이 위협에 노출될 때 시스템내에 존재하는 약점으로 취약성이 발생하는 과실에 기초하여 분류할 때 다음과 같이 3개의 유형으로 나눌 수 있으며 다음 [표 2]에서 요약하였다.

4.4 위험분석

"생략", "위험분석 방법론: 분류와 선택기준" 참조

4.5 대책분석

대책은 안전대책(Safeguards), 통제(Controls) 또는 대응책(Countermeasures)등으로 불리우고 있으나 여기서는 대책이라는 용어를 사용한다. 대책은 위험을 감소시키기 위한 보호조치를 의미하며 이는 장치, 절차, 기법, 행위 등을 포함한다. 앞 장에서 논의된 여러단계의 분석을 통하여 예상되는 손실 혹은 위험이 높을시는 이에 대한 새로운 대책을 고려 하여야 한다. 예를들면, 만약 불법적인 접근의 위험이 높을시는 이에 대비한 접근 통제를 위한 하드웨어, 소프트웨어 그리고 절차등을 평가하여 대책을 수립 하여야 한다.

한가지 위협에 대해 여러 대책을 수행할 필요도 있으며, 그 반대로 한 대책은 여러 위협에 대해 보호 조치의 역할을 할 수 있다. 정보 보호를 위한 대책은 여러가지가 있으며 따라서 대책의 적절한 분류 체계를 설정하는 것이 중요하다. 여기서는 대책에 대한 과거 연구 결과를 조사 분석하여 국내 실정에 적합한 분류 체계를 설정하고 이 분류체계에서 제시하고 있는 대책이 제공하는

[표 2] 취약성의 분류와 과실요소

분류기준	과 실 요 소	설 명
관 리 적 취 약 성	보안 관리	경영층은 보안담당 업무가 적절히 되도록 해야함
	요원/이용자 관리	전산자원에 접근하는 요원/사용자의 관리
	보안정책 문서화	보안정책, 규정, 표준, 교육등의 문서화
	사고대책 관리	우발적인 사고에 대비하는 능력
기 술 적 취 약 성	하드웨어	정해진 요원에게만 하드웨어상의 행동 보장
	운영체제	상호 침해 방지, 자원보호 기능 등
	응용 소프트웨어	프로그램의 가용성, 무결성, 신뢰성, 내부적 감사 가능
	네트워크	안전한 통신선로, 암호, 인증등이 요구됨
	데이타베이스	데이타의 무결성을 위한 특별한 기능이 요구됨
물 리 적 취 약 성	출 입 통 제	승인된 요원만이 시설 영역에 접근토록 함
	환 경 관 리	화재,누수경보기, 정화기, 습도/온도 감시등이 요구됨

정보 보호 서비스와 매가니즘을 중심으로 기술한다.

대책을 대상에 기초하여 크게 3 분류할 수 있다: 논리적, 물리적, 관리적 대책. 논리적 대책은 소프트웨어와 데이터를 대상으로 불법적이고 의도적인 접근이나 비의도적인 실수나 오용으로 부터 보호하기 위한 조치로서 인증, 암호화 등 접근제어나 통신 보안을 위한 기법을 의미한다. 물리적 대책은 전산실이나 통신실 등의 시설물과 정전압/무 정전 설비, 공기 정화 설비, 집진 장치 등 물리적 시설 과 장비에 대한 물리적 침입과 파괴, 자연재해 등의 위협요인으로 부터 보호하기 위한 조치로 정보 통신 시설 및 설비의 위치 설정 및 기계적 기준 등을 명시하는 대책이다. 관리적 대책은 논리적, 물리적 자산을 다루는 사람과 조직 그리고 행정 행위에 관한 대책으로 인간에 의한 의도적 /비의도적 위협으로 부터 보호하기 위한 조치이다. 다음 [표 3]은 대책을 3가지로 분류한 내용을 요약하고 있다.

4.6 비용효과 분석

비용/효과 분석은 발생가능한 위험요소와 이에 대한 대책수립 결정을 위한 논리적 근거를 제공하는 방법론이다. 비용과 효과는 복잡한 산술계산식에 의해서 계산될 수도 있고, 직관적인 방법을 이용하여 추정할 수도 있다. 비용/효과 분석의 최종 결과는 발생가능한 위험요소에 대응하여 대책을 수립하였을 경우 감소되는 위험수준으로 나타난다. 이를 위하여 위험수준과 효과는 비교가 가능한 가치로 표현되어야 하고, 위험수준과 효과의 가치를 산정하기 위한 방법은 일반적으로 납득할 수 있어야 한다. 가능한 위험에 대한 대책수립은 전산망에 속한 여러 사용자에게 동시에 영향을 미칠 수 있으므로 비용/효과 분석은 다수의 사용자에게 미치는 영향을 고려하여야 한다.

비용과 효과의 가치산정은 현재가치(Present Value)로 산정하기로 가정한다. 따라서 위험과 이에 대한 대책수립에 관련한 모든 비용과 효과는 정확하게 산정할 수 있고 시간 경과에 따른 불확실성을 제거할 수 있다. 현재 시점에서의 실질 가치는 다음과 같은 식으로 표현될 수 있다.

$$\text{Net PV} = \text{PVBenefits} - \text{PVCosts}$$

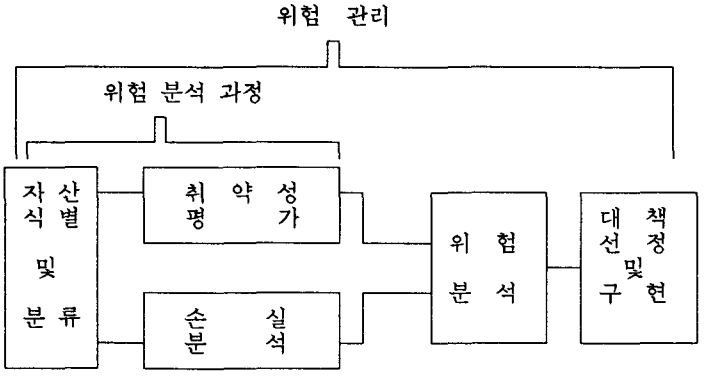
이때 PV는 Present Value를 의미한다.

[표 3] 대책의 분류

대 분 류	대 책 분 류	대 책
논리적 대책	소프트웨어 접근제어	- 사용자 인증, - 로깅
	소프트웨어개발/변경 통제	- 바이러스예방, 치료복구, - 소프트웨어 개발시 특권 폐지, - 버전관리, 변경통제 - 개발 및 유지보수 방법론의 표준화
	데이타 보안	- 데이타 민감도분류, - 민감정보의 접근, 보관, 복사, 폐기, - 비상계획수립, 훈련, 시험, - 백업, 저장, - 무결성 체크
	통신 보안	- 암호화, - 키관리, - 통신보안 프로토콜
물리적 대책	시설물에 대한 접근 통제	- 빌딩/사무실 - 정보시스템 접근 통제
	시설/설비의 입지 환경	- 시설물 위치, 주위 구조 - 부대설비의 구비 및 운영
관리적 대책	행정 관리	- 교육 및 훈련, - 사고보고 체계 - 정보보호 정책, 표준 절차 수립등
	인사 관리	- 임무분리, - 신원조회, - 퇴사/파면시 절차및 규정
	조직 관리	- 최고 경영자의 역할 및 책임, - 보안 담당부서의 역할 및 책임, - 사용자 부서의 역할 및 책임, - 보안 감사부서의 역할 및 책임

5. 적용방법

본 위험관리 기술 지원서는 실제 사용자들이 손쉽게 자신의 조직에 활용하여 사용케하는데 목적이 있으므로 위에서 기술적으로 나열되고 설명된 내용은 실제로 적용하는 데는 매우 어려움이 있을 것이다. 그러므로 이 기술 지원서에서는 새로운 간편하고 단순한 방법에 의한 위험관리/위험분석 체계를 제안하려고 준비중에 있으며 이러한 방법에 의한 적용사례를 제공하여 사용자의 적용성을 높이고자 준비 중인 것이다. 다음 [그림 2]는 간단한 모델을 보여주고 있으며, 이러한 방법과 절차에 의해 실제 적용사례를 준비중에 있다.



① 자산식별 및 분류 : 자산 분석 과정
② 취약성 분석 : 질문표에 의한 취약성 검토
③ 손실 분석 : 실제 일어난 보안사고에서의 손실 파악
④ 위험분석 : 손실분석에 의한 취약요소의 검토 및 보안영역의 수준 파악
손실분석 자료가 없다면 취약성평가의 결과로 수준 파악

[그림 2] 보안분석 방법/모델

6. 결론

이상에서 현재 진행되고 있는 전산망 보안을 위험관리 기술지원서에 대한 내용을 살펴 보았다. 위험관리와 위험분석은 해외에서도 많은 표준들과 방법론이 존재하고 있으며 조직의 보안과 위험관리를 위해 구체적이고 상세한 위험관리의 지원서를 우리의 표준으로 만들기에는 어렵고도 무리한 점이 있으므로 여기에서는 다음과 같은 점에 중점을 두고 추진 중이다.

① 간단하고 일반적인 절차와 방법론을 사용한다.
② 적용하기에 까다롭지 않은 방법을 제시 한다.

위험관리의 일반적인 절차인 6단계를 제시하고 설명하였으나, 지원서 사용자들의 적용성을 중시하여 [그림 2]와 같은 간단한 모델과 절차를 만들어 내게 되었으며 이러한 모델에 근거하여 사례를 들어 제시함으로서 사용자들의 이해를 도울 예정이다.

이러한 위험관리를 위한 지원서를 발간하고 배포함으로서 다음과 같은 효과를 기대하고 있다.

① 국내에서 위험과 보안에 대한 인식의 확산
② 국가조직의 취약성과 위험요소의 인식과 대처 방안 제고
③ 컴퓨터 범죄 대책과 방지
④ 국가조직의 전산화 수준과 전산의존도의 파악을 통한 조직의 활성화 및 안전도 제고

참고문헌

[1] JTC1/SC27/WG1, JTC1/SC27/WG1 N394(Risk Ananysis Tecnique)
[2] Pfleeger, Security in Computing, 1989
[3] NIST/DoJ, "NISTIR 4387: Simplified Risk Analysis Guidelines", 1990
[4] NIST/NTIS, "NIST Special Publication 800-4, Computer Security Considerations in Feral Procurements, 1991
[5] NIST, "FIPS PUB 65, Guidelines for ADP Risk Analysis", 1979
[6] David J. Stang, Sylvia Moon, Network World: Network Security Secrets, IDG Books, 1993
[7] Robin Moses, "Risk Analysis and Management", ?
[8] Deborah J. Bedeau ,"A Conceptual Model for Computer Security Risk Analysis", 1992
[9] Robin Moses, "INFOSEC Project S2014: Risk Analysis,Final and Strategy Report", 1993
[10] Robin Moses, "INFOSEC Project S2014: Risk Analysis, Final and Strategy Report, Appendix A: Claim Structure for Selection and Development of Risk Analysis Methods", 1993
[11] Robin Mose, "INFOSEC Project S2014: Establish Database of Risk Analysis and Management Methods", 1993
[12] W. Timothy Polk, "Automated Tools for Testing Computer System Vulnerability", 1992
[13] NIST/NCSL, "Guide for Selecting Automated Risk Analysis Tools",
[14] 日本情報處理開發協會, 컴퓨터시큐리티에 관한 리스크分析 - JRAM Approach, 1992
[15] K Bhaskar, "Computer Security : Threats and Countermeasures"
[16] K.M.Jackson, J.Hruska, Donn B.Parker, "Computer Security Reference Book"
[17] Deborah J.Bodeau, "A Conceptual Model for Computer Security Risk Analysis," in Computer Security Applications Conference, 1992