위험관리의 체계(framework) 연구

신동익
한국전산원

Risk Management Frameworks - review and direction

Shin, Dong-Ik
National Computerization Agency

<요약>
많은 정보시스템이 점차적으로 전산망으로 연결되므로서, 보안성에 대한 위협이 더욱 증대되고 있다. 적절한 보안성을 유지하기 위해서는 시스템이 어느정도 위험한지를 파악하여 이를 관리하는 노력이 필요하다. 이와같은 노력의 가장 중심이 되는 것은 위험관리의 체계를 세우고 이에 따른 방법론을 개발하는 것이다. 본 논문은 기존의 위험관리 체계를 검토하고 분석하여, 이를 기초로 단순하면서도 실용적인 위험관리의 체계를 제시하고자 한다.

1. 위험관리의 목적 및 중요성

위험관리는 매우 강력한 개념적 보안 도구일 수 있다. 선진국의 경우 대부분의 정부 조직과 일반 기업들은 이런 사실을 인식하고 정보시스템의 보안 위험을 주기적으로 측정하도록 요구하고 있다. 이와같은 노력에 있어 가장 큰 문제점은 위험 측정을 수행하는 표준화된 방법이 없다는 것이다.

본 논문은 위험관리의 표준화를 위한 첫번째 단계인 위험관리의 체계를 정립하고자 하는 노력의 산출물이다. 우선 기존의 위험관리 체계에 관한 연구를 분석하고, 이를 기초로 실용적이며, 단순한 위험관리의 체계를 제시하고자 한다.

■ 위험분석의 목적 및 중요성
- 조직내에서 효과적인 정보기술 보안 프로그램의 초석
- 보안 안전장치의 구현에 선행해서 수행해야 할 중요한 작업
- 정보시스템의 무결성, 비밀성, 가용성의 상실이 사업에 주는 영향 이해
- 보안 안전장치의 식별과 정당화
- 노출된 위험의 분석과 관리

■ 위험분석이 사용되지 않은 이유
- 위험분석의 유익성 인식 부족
- 잘못된 분석 방법의 사용으로 인한 나쁜 경험
- 요구사항의 정의와 선택 기준 수립의 어려움
- 평가의 비용
- 적절한 지침의 부족

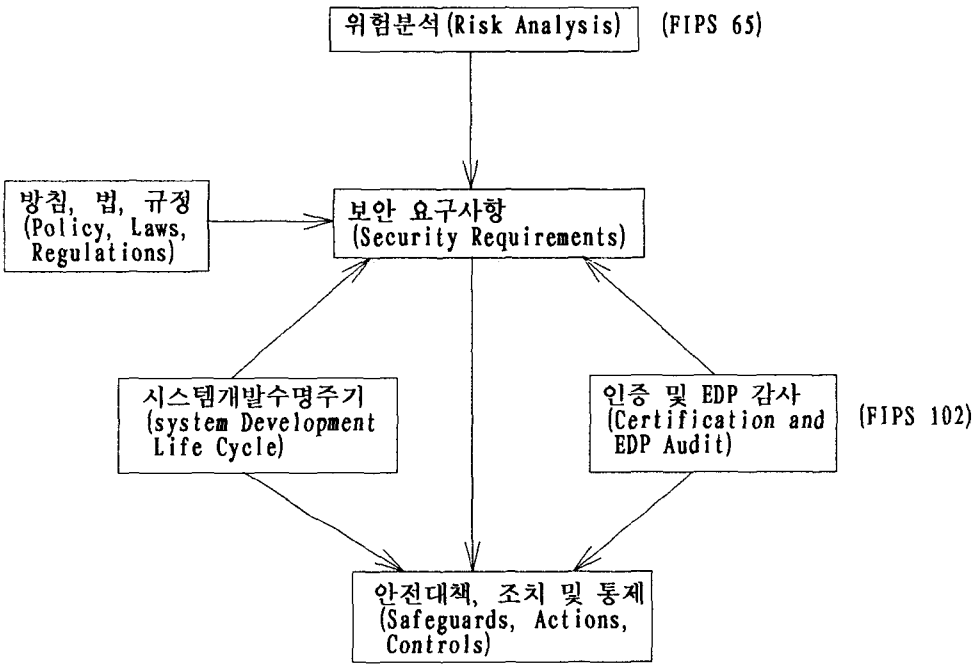
2. 기존의 위험관리 체계

2.1 미국 NIST의 위험관리 체계 (Stuart W. Katzke)

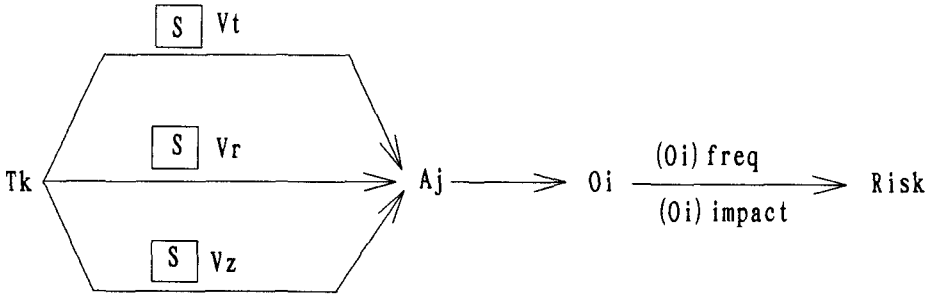
미국의 표준화 기관인 NIST(National Institute of Standards and Technology)는 NBS(National Bureau of Standards)의 후신이다. NIST는 1972년 처음으로 정부기관의 정보시스템에 대한 보안프로그램을 수립하였다. 이 보안프로그램은 국가적 기밀사항이 아닌 일반 행정정보를 처리하는 정보시스템에 대한 위험관리를 지원하는 것을 포함하고 있다. NIST는 위험관리에 대한 다양한 표준과 지침서(guideline)을 제정하였고, 미국 상무성(Department of Commerce)의 산하기관이므로 상업부문의 기업들과도 긴밀히 협조하여 표준개발을 지원하는 연구를 수행해 왔다. Katzke는 NIST의 security division manager로서 위험관리 프로그램에 주도적 역할을 수행하고 있다. 이 곳에서는 Katzke가 제시하는 위험관리 체계를 소개한다.

<그림 1>은 위험관리의 과정을 그림으로 보여주고 있으며, 이 과정을 설명하면 다음과 같다. 즉 위험관리는 다음과 같은 과정을 포함하고 있는 것으로 제시되고 있다. 첫째, 정보시스템 기술을 사용하므로서 야기되는 잠재적 손해(loss)의 측정, 둘째, 손해의 측정을 위한 시스템 취약성(vulnerability)의 분석, 마지막으로 위험을 승인할 수 있는 수준으로까지 감소시키는 비용효과적인 안전대책의 선택 및 구현이다. 위험관리의 개념은 <그림 2>와 같이 보여질 수 있다.

<그림 1> 위험관리의 과정



<그림 2> 위험관리의 개념



Tk = 특정 위협 k
S = 안전대책
Vt, Vr, Vz = 특정 취약성 t, r, z
Aj = 특정 자산 j
Oi = 특정 손상결과 i
(Oi) freq = 특정 손상결과 i의 빈도수
(Oi) impact = 특정 손상결과 i의 금전적 또는 비금전적 영향
Risk = 잠재적 손해의 측정치 (e.g., annual loss expectancy = (Oi) freq * (Oi) impact)

특정 위협, Tk, 는 특정 자산, Aj, 의 취약성 Vt, Vr, Vz를 공격하여 Oi의 영향을 주고, 이는 Risk로 측정된다. 취약성 Vt, Vr, Vz는 안전대책의 일부분인 $(S)_{Vt}$, $(S)_{Vr}$, $(S)_{Vz}$를 이용하여 취약성을 제거할 수 있다. 여기서 $(S)_{Vt}$는 취약성 Vt를 제거하는 안전대책들을 말한다. 흔히 취약성 Vt, Vr, Vz에 대응하는 안전대책인 $(S)_{Vt}$, $(S)_{Vr}$, $(S)_{Vz}$는 서로 상호간 완전히 다르지 않다. 즉 하나의 안전대책은 여러개의 취약성을 제거할 수 있기 때문이다. 이런 관계는 안전대책의 선정 및 비용효과분석을 복잡하고 어렵게 만든다.

Katzke는 위험관리의 일반적 모델을 구성요소들과 구성요소들 간의 관계를 설정하여 제시하고 있다. 이 모델은 흔히 strawman model로 불린다. 구성요소로는 아래와 같은 것들이 제시되고 있다.

위협 (threats) : $T = \{t_1, t_2, t_3, \ldots, t_n\}$
자산 (assets) : $A = \{a_1, a_2, \ldots, a_m\}$
안전대책 (safeguards) : $S = \{s_1, s_2, \ldots, s_k\}$
결과 (outcomes) : $O = \{o_1, o_2, \ldots, o_p\}$
영향 (impact) : $I = \{i_1, i_2, \ldots, i_j\}$
결과 빈도 (outcome frequency) : O_f, 모든 o_p에 대해서
위협 빈도 (threat frequency) : t_f, 모든 t_n에 대해서
안전대책 효과성 (safeguard effectiveness) : S_{eff}, 모든 S_n에 대해서
위협 정도 (threat severity) : T_{sev}, 모든 t_n에 대해서
위험 (risk) : R
안전대책 비용 (safeguard cost) : SC, 모든 s_k에 대해서
결과 영향 (outcome impact) : OI, 모든 o_p에 대해서

위험관리 요소들간의 함수 관계(functional relationship)는 다음과 같다.

$S = f(A, T, V)$ $\quad V = g(T, S, S_{eff})$

$t_f = h(A, T, V, I)$

$O_f = k(t_f, V)$

$I = l(A, T, S, V, S_{eff}, t_{sev})$

$R = t(I, e_f, t_f, t_{sev}, S, V, A, T, \ldots)$

$SC = y(\text{initial} + \text{ongoing} + \ldots)$

SSF = w(R, SC) such that if SSF_0 is some initial state, then SSF converges (i.e., you are done) when:

a) $|SSF_n - SSF_{n-1}| <$ some value

or

b) $|R_n - R_{n-1}| < e$ and $|SC_n - SC_{n-1}| < d$ and $SC_n < R_n$

or

c) $R_n <$ value and $SC_n <$ $ value and $SC_n < R_n$

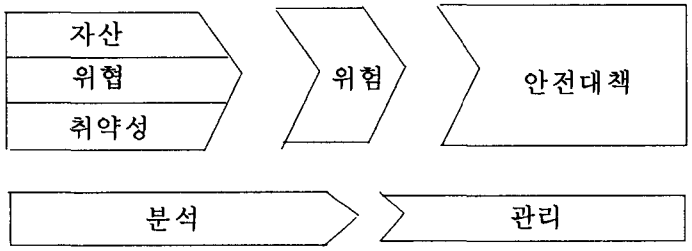
or

d) some other condition for convergence

2.2 영국 CCTA의 위험관리 체계 (Robin Moses)

영국의 표준화 기관인 CCTA(Central Computer and Telecommunications Agency)는 영국 정부기관 정보시스템의 위험관리를 위하여 CRAMM(CCTA Risk Analysis and Management Model)을 개발하여 사용할 것을 권고하고 있다. CRAMM은 전통적인 위험분석과 관리 모델에 기초하여 개발되었다. CRAMM의 모델은 <그림 3>과 같다.

<그림 3> CRAMM의 모델



CCTA의 CRAMM은 자산, 위협 및 취약성 분석을 하여 위험을 측정하는 단계까지를 위험분석으로 보고, 측정된 위험으로 분터 적절한 안전대책을 선정하여 구현하는 것은 위험관리로 보았다. CRAMM에서는 우선 자산을 파악하고 분석 범위를 결정하게 된다. 자산에는 하드웨어, 소프트웨어, 문서, 환경 장비, 자료 등이 포함되나, 크게는 물리적 장비와 자료 자산(소프트웨어를 포함한)으로 구분될 수 있다. 자료 자산은 입력, 처리, 출력을 위해서는 물리적 장비를 이용해야 하므로 물리적 장비에의 의존관계를 갖고 있다. 다음 단계에서는 의도적 및 비의도적 위협들이 파악된다. 의도적 및 비의도적 위협은 물리적 장비와 자료 모두에 영향을 줄 수 있으며, 특히 물리적 장비에 대한 위협은 간접적으로 자료에 대한 위협도 되므로 의존관계를 명시하게 된다. 위협이 실질적으로 영향을 미치기 위해서는 특정 사건(e.g., 내부요원의 실수)이 일어나야 하며, 또한 위협에 의해 공격당할 수 있는 취약

성이 있어야 한다. 의도적 위협의 경우 행동을 하기 위한 동기가 있어야 한다. 위협에 대한 영향은 누설, 수정, 비가용성 및 파괴 등 이다. 영향의 경우에 있어서도 물리적 장비에 대한 영향은 자료에 대해 2차적 영향을 주게된다.

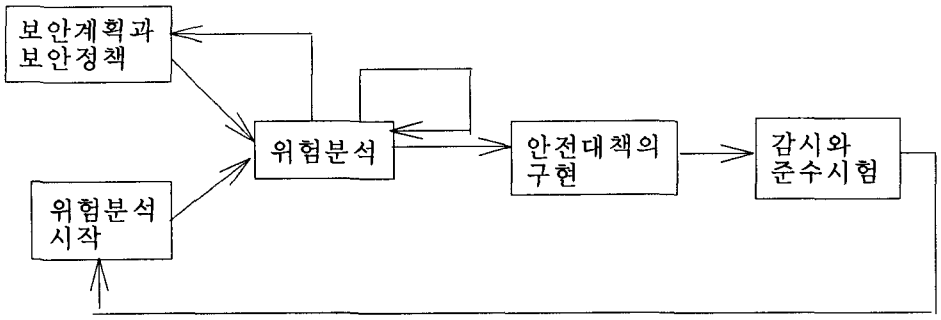
CRAMM은 자산평가와 위협 및 취약성 수준의 측정, 의도적 위협들의 동기들을 고려하여 위험의 측정을 하게 된다. 위험의 측정은 위험을 관리할 수 있게 하는 중요한 관리수단이 된다. 위험의 수준을 적절한 수준으로 감소시키고자 할때는 필요한 안전대책을 선정하여 실행하는 것이다. CRAMM은 7가지 종류의 안전대책을 제시하고 있다

A : avoidance (예 : 자료의 분리처리)
T : transfer (예 : 보험)
RT : reduction of threat (예 : 다이알업 라인의 제거)
RV : reduction of vulnerability (예 : 자산의 분리 배치)
RI : reduction of impact (예 : 화재 대비한 소방기구 구입)
R : recovery (예 : 비상계획)

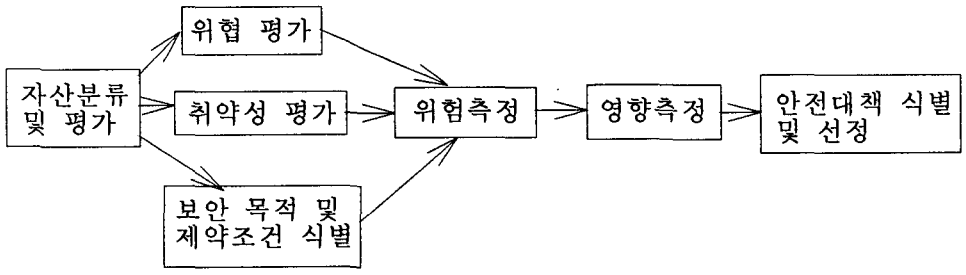
2.3 INFOSEC

CEC(*Commission of the European Communities*)는 위험분석의 프로젝트를 통해 위험관리와 분석의 모델을 도출하였다. <그림 4>와 <그림 5>는 각각의 모델을 보여주고 있다.

<그림 4> INFOSEC의 위험관리 모델



<그림 5> INFOSEC의 위험분석 모델



■ Risk analysis model components
- assets
- threat
- vulnerability
- risk
- impact
- safeguard

■ Risk analysis model characteristics

(1) Assets
- hardware
- firmware
- communications
- environmental
- system software
- application software
- DBMS
- office automation
- other software
- data/information
- processes
- business functions
- documentation
- people
- real estate
- money
- other

(2) Extent of impact analysis
- availability
- destruction
- confidentiality
  . internal
  . external
- integrity
  . accidental
  . deliberate
- metrics
  . qualitative
  . quantitative
  . likelihood
  . other

(3) Extent of threat and vulnerability analysis
- accidents
  . physical
  . failures
  . natural

  . loss of services
  . staff shortage
  . other
- errors
  . logical
  . design
  . other
- malicious attach
  . theft
  . fraud
  . sabotage
  . viruses
  . hacking
  . misuse of resources
  . other

(4) Method of measuring threat levels
- qulaitative
- quantitative
- likelihood
- other

(5) Method of measuring vulnerability levels
- qualitative
- quantitative
- likelihood
- other

(6) Method of expressing risks
- qualitative
- quantitative
- likelihood
- other

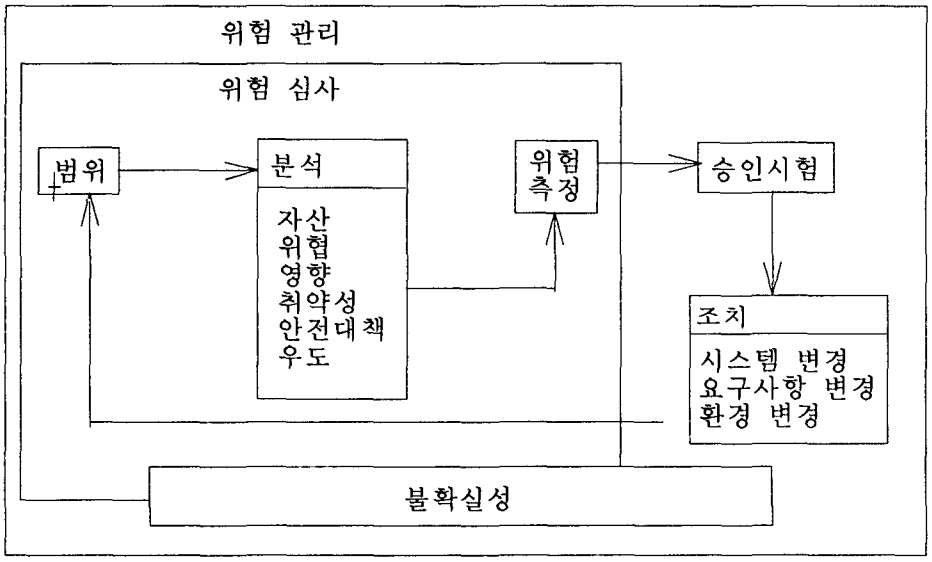
(7) Coverage of security safeguards
- physical
- personnel
- hardware
- software
- communications
- procedural
- organizational
- tempest
- other

2.4 NRMM(NIST Risk Management Model)

NRMM은 NIST straw-man 모델에 수명주기(life-cyle) 개념을 첨가하여 만들어 졌다. 위험관리의 모델에 수명주기의 개념이 첨가되었다는 것은 개발의 수명주기의 각가 다른 시점에 있어서 위험분석의 변수들이 다양한 다른 모습으로 사용된다는 것을 의미한다. 즉 수명주기의 각각의 다른 단계에서 발생되는 특정문제에 더욱 적절하게 대응하는 유일한 방법이 있을 수 있다는 것이다. 예를 들면 시스템 개발의 시작단계에서 사용되는 위험심사 모델은 구현이 완료된후 유지보수 단계에서 사용되는 위험심사 모델과는 다를수 있다는 것이다. 기본 원칙과 변수는 동일하나, 변수들에 대한 강조의 정도와, 구체성의 수준, 모델링 기법 등이 다를 수 있다.

NRMM은 <그림 6>에서 보여지고 있다. NRMM에서 분석되는 변수는 6개로서, 자산, 위협, 영향, 취약성, 안전대책, 우도이다. 이 6개의 변수는 위험측정치를 계산하는 기본을 이루며, 계산된 위험측정치는 시스템 보안성의 적절성을 결정하는데 사용된다.

<그림 6> NRMM



3. 실용적 위험관리 체계

지금까지 여러 종류의 위험관리 체계를 검토해 보았다. 이들은 일반적인 위험관리의 모델을 제시하고 있으며, 다양한 시각에서 위험관리를 이해하고 있음을 알수 있다. 우리는 이런 일반론에서 부터 좀더 실용적이며 우리나라의 상황에 적합한 체계를 수립할 필요성이 있다. 위험관리의 체계에 대해 설명하기 전에 먼저 일반적인 보안과 보안관리 및 위험관리의 연결성을 생각해 보기로 한다.

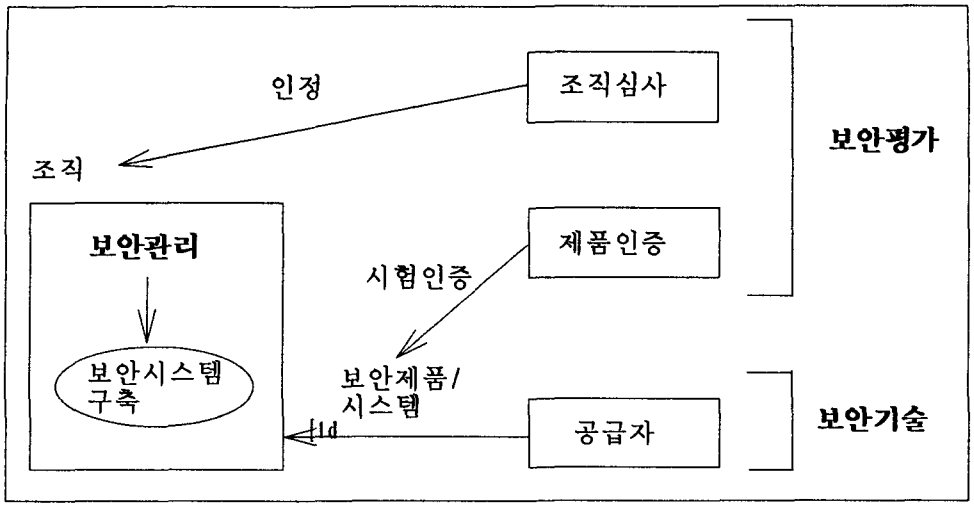
3.1 보안의 체계

보안이라하면 여러가지 시각에서 이해하고 모델화 할 수 있을 것이다. 이 논문에서는 보안을 보안관리, 보안평가 및 보안기술의 세가지 부분으로 구별하여 이해하기로 한다. 보안관리란 조직에서 보안의 필요성을 인식하고 보안을 유지하기 위해 기울이는 노력을 말한다. 흔히 보안은 사람의 문제로 또는 기술의 문제로 치우쳐서 이해하기 쉽다. 사람의 문제로 이해하는 경우에는 "열사람의 경비원이 하나의 도둑을 못막는다"라는 말로 보안은 사람의 문제로 말한다. 기술의 문제로 치우치는 경우에는 도둑이 감히 이길수 없는 기술적으로 탁월한 보안시스템을 구축하면 보안의 문제가 해결된다고 한다. 그러나 보안은 사람과 기술의 문제 둘다이며 중요한 것은 이 둘의 적절한 균형을 맞추는 것이다.

보안관리는 보안 제품 또는 시스템이 제공하는 보안기능을 고려하고 사람들에 대한 적절한 통제를 사용하여, 보안 체계를 구축하고 관리하는 것을 말한다. 보안제품과 시스템은 보안기술을 구현하여 생산된다. 보안제품의 공급자는 적절한 보안기술들의 조합을 통해 고유한 보안제품을 생산하여 판매할 것이다. 이렇게 생산되는 보안제품은 기준이되는 관련표준이나 또는 구매자의 규격에 적합한지를 시험하여 보증하는 것이 필요할 것이다. 경우에 따라서는 보안제품의 품질까지도 보증할 수 있을 것이다. 이런 일들은 제3자나 또는 구매자를 대신하는 제2자가 시험하고 인증하게 된다.

인증된 제품을 구매하여 보안시스템을 구축하면 조직은 보안시스템을 더욱 쉽게 구축할 수 있을 것이며, 또한 보안시스템에 대해 더욱 자신감을 가질수 있을 것이다. 적절한 보안을 유지하는 것은 보안시스템의 구축만 갖고는 어렵다. 즉 보안은 사람의 문제이기도 하기 때문이다. 적절한 보안을 유지하는 것은 사람과 보안시스템을 적절히 편성하여 관리할 때에 가능하다. 어떤 조직이 이와같은 편성을 잘하여 적절히 보안을 유지하고 있는지를 심사하여 인정해 주는 제도가 필요할 수 있다. 최근 각각의 조직내의 정보시스템은 홀로 사용되는 것이 아니라 전산망으로 연결되어 공동으로 사용되는 추세이다. 초고속 통신망이 구축되게 되면 이런 추세는 더욱 가속화 될것이다. 이런 경우 자기 조직의 보안이 잘 구축되어 관리되고 있다하여도, 전산망으로 연결되는 조직의 보안이 취약하다면 이것은 큰 위협이 될수 있다. 따라서 전산망으로 연결되는 조직들은 최소한의 보안을 유지하여야 하며 이를 제3자의 입장에서 심사하여 인정하는 제도가 필요하다. 이런 제도는 전산망을 위협하는 많은 종류의 위협요인들로 부터 전산망과 연결하는 조직들의 보안을 유지하는데 큰 도움이 될것이다.

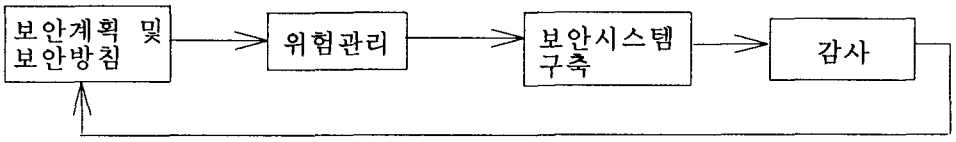
<그림 7> 보안의 체계



3.2 보안관리 체계

이제는 보안관리의 체계에 대해 구체적을 알아볼 차례이다. 보안관리는 크게 보안계획과 방침을 수립하는 단계와, 이를 기초로 위험을 관리하는 단계, 선정된 안전대책을 구현하여 보안시스템을 구축하는 단계, 마지막으로 조직내에 구축된 시스템이 적절하게 운영되고 있는 자를 사후 시험하는 보안감사가 있게 된다.

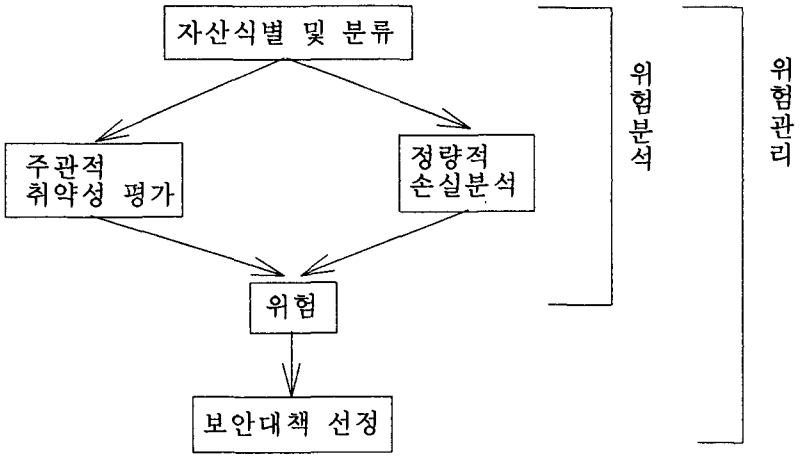
<그림 8> 보안관리 체계



3.3 실용적 위험관리 체계

이곳에서는 간단하나 매우 효과적일 수 있는 위험관리의 방법을 도출할 수 있는 위험관리의 체계를 제시한다. 실용적 위험관리 체계는 우선 자산을 식별하고 분류하는 작업부터 시작한다. 다음 단계는 설문지를 사용한 주관적인 취약성을 평가하고, 동시에 과거의 장애나 사고에 대한 기록을 토대로한 정량적 손실분석을 한다. 이 두가지 활동으로 부터 나온 산출물은 조직의 위험수준을 결정하게 된다. 계산된 위험수준은 조직의 방침으로 결정된 위험수준, 또는 유사업종의 위험수준 등과 같은 기준치와 비교하여 승인될 수 있는 위험과 승인될 수 없는 위험으로 구분된다. 승인될 수 없는 위험은 안전대책을 선정하여 위험수준을 낮추게 된다.

<그림 9> 실용적 위험관리 체계



<참고문헌>

1. Katzke, Stuart, "A Government Perspective on Risk Management of Automated Information Systems," Risk Analysis Symposium, The Research Foundation of the Institute of Internal Auditors, Oct. 4-5, 1987.

2. CEC Security Investigations Projects - Risk Analysis, Final and Strategy Report, 1993.

3. Jackson, K. and Hruska, J., Computer Security Reference Book, CRC Press, Inc., 1992.

4. NIST and CSE, Proceedings of 5th International Risk Management Workshop, 1993.

5. William, Perry and Kuong, Javier, EDP Risk Analysis and Controls Justification, Management Advisory Publications, 1981.