通信情報保護學會誌
第 10 券 第 1 號, 2000. 3

취약성 평가에 의한 정보보호지표의 계량화: 정보자산가치가중치법

김 기윤*, 나 관식**

요 약

본 연구의 목적은 취약성을 보안대책의 결핍으로 정의해서 정보보호지표의 개념을 도출한 후에, 정보자산가치에 따라서 가중치를 부여하는 정보자산가치가중치법에 의해서 정보보호지표를 계량화하는 절차를 제시하는 것이다. 이와 같은 정보보호지표에 근거해서 정보보호를 위한 기본적인 보호 대책(관리적, 기술적, 물리적 대책을 포함하는 기본통제)을 구현하고 특정 응용시스템을 위한 특수한 보호 대책을 구현함으로써, 조직 내외의 위협으로부터 안정적이고 신뢰성 있는 정보서비스를 제공할 수 있다.

Ⅰ. 서 론

일반적으로 지표(Index 혹은 Indicator)란 어떤 사회적 현상을 계량적, 수치적으로 표현하는 방법을 일컫는 것으로 특정한 사회현상에 대한 대표성을 위하여, 또는 국가 간, 지역 간, 조직 간 등의 비교를 위하여, 또는 정책적인 의미를 도출하기 위하여, 또는 지표의 생성에 관한 계량분석을 통한 추후 연구의 기초자료로서의 이용가능성을 위하여 만들어진다. 현재 정보기술과 관련된 지표에 대한 국내외 연구는 주로 정보화 지표에 관한 연구가 대부분을 차지하고 있다. 1960년대부터 미국에서는 거시경제학적 관점에서 정보부문의 비중이 얼마나 되는가를 평가할 수 있는 분석의 틀을 개발했으며, 일본에서는 독자적으로 정보화 지표, 네트워크화 지표 등을 사용해 왔다. 기존 연구가 사회경제학적인 접근방법에 치중한 정보화현상의 대표성 기술 및 국가 간 비교의 측면에 치중하고 있다. 지표의 목적 별로 정보설비 지표, 정보이용 지표, 정보화투자 지표, 자치단체 정보화지표 등의 지표를 구하여 정보화 진전 정도를 측정하려고 했다[1,2].

정보보호와 관련되어 있는 개체들과 그들의 이해관계가 상이하고, 이에 따라 측정되는 지표 또한 다양할 수 있기 때문에, 이들을 모두 포함할 수 있는 모형개발이 필요하다. 모형개발에 있어 우선적으로 고려해야하는 점은 정보보호의 개념을 적절히 반영할 수 있고, 또한 지표개발의 궁극적인 목적이 그 자체보다는 정확한 현황 파악에 기초하여 정책수립에 반영됨으로써, 그 의미를 가지기 때문에, 정보보호수준의 현황 파악과 정책의 추진방향에 대한 충분한 검토가 필요하다는 점이다.

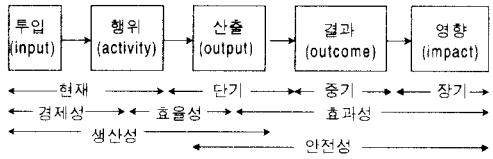

그림 1. 시스템 성과의 흐름

과거 연구를 통해 본 정보보호를 위한 모형은 상당히 다양하게 존재하고 있다. 정보보호 모형을 크게 나누어 보면 4가지로 분류할 수 있다. 첫째, 정보 시스템 보안 관리를 위한 모형으로서, 정보보호 시스템 구축을 위한 생명주기, 위험관리, 정보보호

* 광운대학교 경영학과(min1203@daisy.kwangwoon.ac.kr)
** 서원대학교 경영정보학과(ksna@dragon.sewon.ac.kr)
※ 본 연구는 1999년도 광운대학교 교내학술연구비로 수행되었습니다.

요구사항, 정보보호 조직의 관리 기능 파악을 위한 모형들이 존재한다. 둘째, 접근 제어를 위한 모형로서, 참조모니터모형(Reference Monitor Model)을 대표로 하는 단일수준모형, 정보의 기밀성 수준과 사용자의 인가 수준을 고려한 군사 환경에 적합한 격자모형(Lattice Model), 상이한 보안 수준간의 정보의 흐름을 서술하는 정보흐름모형(비밀성을 위한 Bell-LaPadula Model, 무결성을 위한 Bida Model)이 있다. 셋째, 정보보호시스템 구축 기술에 관한 모형으로서, ISO의 보안참조모형, 분산시스템 보안모형 등이 있고, 마지막으로 정보시스템의 보안성 평가 및 인증을 위한 모형으로 미국방부의 TCSEC(Trusted Computer System Evaluation Criteria), 미 연방지침인 FC (Federal Criteria), 유럽의 정보기술 보안평가기준인 ITSEC (Information Technology Security Evaluation Criteria), 영국의 정보보안관리 지침(BS7799, Code of Practice for Information Security Management) 등이 있다.

정보보호지표의 여러 유형을 도출하기 위해서는 시스템 사고로 접근해야 올바른 해결책을 제시할 수 있다. 즉 정보보호를 위해서는 여러 개념들이 존재하며 이들 간의 관계에 대한 명확한 이해가 우선되어야 한다. 본 연구의 목적은 취약성을 보안대책의 결핍으로 정의해서 정보보호지표의 개념을 도출한 후에, 정보자산가치에 따라서 가중치를 부여하는 정보 자산가치 가중치법에 의해서 정보보호지수를 계량화하는 절차를 제시하는 것이다. 이와 같은 정보보호지표에 근거해서 정보보호를 위한 기본적인 보호 대책(관리적, 기술적, 물리적 대책을 포함하는 기본통제)을 구현하고 특정 응용시스템을 위한 특수한 보호 대책을 구현함으로써, 조직 내외의 위협으로부터 안정적이고 신뢰성 있는 정보서비스를 제공할 수 있다.

II. 정보보호지표의 개념

정보보호란 크게 다음과 같은 세 가지 위험으로부터의 보호를 의미한다. 세 가지 위험이란 정보의 비인가된 공개(조직의 비밀정보가 비인가된 자에 의해 노출되는 것으로 비밀성(Confidentiality)이 침해되는 경우), 정보의 불법적인 변조 및 파괴(고의나 실수로 인해 정보의 변조, 파괴 등 정보의 무결성(Integrity)이 침해되는 경우), 정보서비스의 이용 불가(언제든지 필요한 정보나 정보서비스를 필요한 때에 얻을 수 없는 경우로서 정보의 가용성(Availability)이 침해되는 경우)이다. 그러므로, 정보보호의 정의를 "데이터 및 시스템을 고의적 혹은 실수에 의한 불법적인 공개(노출), 변조, 파괴 및 지체로부터의 보호"라고 할 수 있다. 이것을 다른 말로 표현하면, 데이터 및 시스템의 보안성, 무결성, 가용성을 확보하는 것이며, 바로 이것이 정보보호의 속성 또는 목표가 될 수 있다.

시스템 관점에서 측정대상이 되는 성과(Performance)의 흐름에는 투입 -> 행위 -> 산출 -> 결과 -> 영향 등이 있다[3,4,5]. 정보보호 관점에서 투입(Input)이란 위협(혹은 위협의 공격)을 의미하며, 행위(혹은 과정)는 이러한 위협으로부터 자산을 보호하기 위한 보안대책이며, 산출(Output)은 보안대책에 의한 정보자산의 보호이다. 결과(Outcome)는 정보자산에 대한 산출의 효과이다. 영향(Impact)은 결과의 장기적인 효과이다. 장기적인 결과와 영향의 의미를 구별하기는 어렵다. 정보보호의 성과측정은 투입, 행위, 산출, 결과 등에서 평가되는 수준으로 이루어진다. 그러므로, 정보보호의 성과란 투입, 행위, 산출, 결과 등의 평가된 수준이라고 정의 할 수 있다.

정보보호 관점에서 위협의 투입에 대해서 정보보호 원인지표가 측정되어야 하며, 보안대책의 행위에 대해서 정보보호 실행지표가 측정되어야 하고, 자산보호 측면에서 정보보호 산출지표, 정보보호 결과지표, 정보보호 영향지표가 측정되어야 한다. 투입의 수준과 산출의 수준간에는 직접적인 인과관계가 있지만, 산출과 결과간에는 투입/산출보다는 직접적인 인과관계가 많지 않다. 산출(예로써, 하드웨어 손상)로 인한 결과(예로써, 업무중단)가 장기적으로는 영향(예로써, 기업 이미지 손상)을 이끌어내지만, 그 관련성은 가끔 무시할 정도이며, 관련성이 있다 할지라도 파악하기가 어렵다.

측정대상이 되는 성과의 개념에는 6가지 - 생산성, 효과성, 효율성, 품질, 적시성, 안전성 - 가 있다[6,7]. 여기서 생산성(Productivity)이란 산출된 부가가치를 소비된 투입가치로 나눈 것이다. 효과성(Effectiveness)이란 산출이 시스템의 목표에 일치하는 정도를 나타내는 시스템의 특성이고, 효율성(Efficiency)이란 최소한의 자원비용으로 시스템이 목표로 한 산출을 출력시킨 정도를 나타내는 시스템의 특성이다. 품질(Quality)이란 제품과 용역이 고

객의 욕구와 기대를 만족시키는 정도이다. 적시성(Timeliness)이란 작업의 단위가 정확하게 그리고 적시에 이루어진 정도이다. 여기서 작업단위에 대한 기준은 항상 고객만족에 근거를 두어야 한다. 안전성(Safety)이란 조직과 조직구성원들의 작업환경에 대해서 전반적으로 안전한 정도이다.

투입되는 자원을 행위로 변환하는데는 자원투입의 경제성이 중요하고, 바람직한 산출의 수준을 얻기 위한 행위에서는 자원의 효율성이 중요시된다[5]. 또한, 효과성은 행위와 영향간의 관련성에 부여된 가치이다. 효과성은 산출, 결과, 영향 등 3가지 측면에서의 관련성이 있기 때문에, 이에 대한 측정 및 통제가 어렵다. 운영수준에서는 효율성과 생산성이 중요하고, 관리수준에서는 조직 및 관리의 효과성이 중요하고, 전략적 수준에서는 기업의 경쟁력이 중요하다[8]. 이와 같이 조직계층 관점에서 각 수준마다 서로 다른 척도를 적용해야 한다. 측정을 옳게 하는 효율성보다는 옳은 것을 측정하는 효과성이 보다 더 중요하다[6]. 효율성은 정보시스템 기능의 내적 요구사항에 관심을 두지만, 효과성은 외적 요구사항에 관심을 두고 있다.

정보보호 관점에서는 안전성을 나타내는 정보보호 지표를 개발해야 한다. 안전성 역시산출, 결과, 영향 등 3가지 측면에서 관련성이 있으며, 자산의 보호 관점에서 산출지표, 결과지표, 영향지표 등 3가지를 도출할 수 있다. 산출지표는 여러 위협의 공격들에 대해서 보안장치가 방어한 보안장치의 생산성 혹은 효율성만을 나타낸다. 이와 같이 보안설비의 효율성을 분석하는 것을 설비효율분석이라고 한다. 결과지표는 위협에 의한 정보자산의 손실액으로 나타낸다. 이와 같이 정보자산에 큰 영향을 주는 위협들을 파악하고, 이러한 위협과 관련된 조직의 취약성을 분석하는 것을 위험분석 이라고 한다.

1차적 영향지표는 재해로 인한 업무중지를 비용으로 추정해서 나타낸다. 이와 같이 조직 내의 중요한 업무기능을 파악하고, 업무기능의 중지로 인한 영향을 분석하는 것을 업무영향분석(BIA: Business Impact Analysis)이 라고 한다. 2차적 영향지표는 초고속 정보통신기반계층인 정보의 전달, 유통, 응용, 사회 등 관련계층에 대한 재해의 영향을 분석해서 사회적 비용으로 추정해서 나타낼 수 있다.

본 연구에서는 보안관리 관점에서 위협분석에 연구초점이 있으므로, 정보보호 결과지표만을 고려하고자 한다. 이와 같이 정보보호수준은 원인지표 -> 실행지표 -> 결과지표로 진행되므로, 정보보호 결과지표는 실행지표의 영향을 직접적으로 받고, 원인지표의 영향을 간접적으로 받는다. 그러므로, 결과지표는 다음과 같은 조건부 함수의 형태로 표현할 수 있다.

결과지표=f(실행지표 | 원인지표)

실행지표는 정보시스템의 취약성에 반비례한다. 즉 물리적 대책, 기술적 대책, 관리적 대책 등 보안대책에 의한 보호수준이 높을수록 정보 시스템의 취약성은 낮아진다. 또한, 원인지표는 위협빈도에 반비례한다. 즉 위협의 발생확률이 높을수록 보안대책을 뚫고 손실을 일으킬 가능성이 커지므로, 결과지표(효용 개념으로 측정되는 경우)의 보호수준은 낮아진다.

효용개념에 의한 결과지표=f{(1/정보시스템의 취약성) | (1/위협빈도)}

표 1. 정보보호 산출/결과/영향 지표의 비교

	산출지표	결과지표	1차적 영향지표	2차적 영향지표
측정영역	보안대책	정보시스템	조직시스템	정보통신망
측정대상	보안장치	정보자산	업무	정보통신기반계층
성과흐름	생산성, 효율성	효과성	효과성	효과성
측정척도	입출력비율	정보자산 손실액	업무중단비용	사회적 비용
시간흐름	단기	중기	장기	장기
관리차원	설비관리	보안관리	업무지속성관리	정보통신망관리
분석방법	설비효율분석	위험분석	업무영향분석	재해분석

정보보호 결과지표는 정보자산 혹은 조직 내의 자산에 대한 손실크기로 측정되고, 궁극적으로 손실액으로 측정된다. 이와 같이 비효용(Disutility) 개념으로 측정되는 경우에는 역수를 취하므로 결과지표는 다음과 같이 표현하게 된다.

비효용개념에 의한 결과지표=f{(정보시스템의 취약성)|(위협빈도)}

그러므로, 정보시스템의 취약성을 나타내는 정보보호 실행지표는 (실행하고 있는 보안대책)/(기본통제를 위해 필요한 보안대책) 이고, 위협빈도는 위협의 발생확률이다. 비효용개념에 의한 결과지표인 보안위험에 의한 손실크기는 정보시스템의 취약성을 기본통제에 대한 보안대책의 결핍으로 정의할 때, 다음과 같이 표현 할 수 있다.

보안위험의 손실크기=f{(실행하고 있는 보안대책)/(기본통제를 위해 필요한 보안대책)|(위협발생확률)}

III . 위험분석에서의 취약성 평가

위험관리란 불확실한 사건의 피해를 식별, 통제, 최소화하는 전반적인 절차에 관계된 경영과학의 한 분야로서, 정보시스템의 위험관리는 측정 및 평가된 위험에 대한 보안대책을 일정 수준까지 유지관리하는 것이다. 위험관리의 목적은 위험분석의 결과에 의해서 현재의 보안수준을 허용된 수준까지 높이기 위해서 보안대책을 마련하는 것이다[9,10]. 다시 말해서, 정보기술보안을 위한 위험관리는 경영층이 받아들일 수 있는 수준까지 위험을 감소시킬 수 있는 보안대책을 선택하는 것이다. 위에서 기술한 여러 기관의 보고서(NIST, 미법무성, 국제표준화기구 등)를 근거로 위험분석절차는 다음과 같다[11,12,13].

1. 자산 분류 및 평가

보호해야 할 전산자원들을 식별하고, 체계적인 분류를 해서, 소유하고 있는 자산들의 가치를 평가하는 기본적인 단계이다. 여기서 자산이란 하드웨어, 소프트웨어, 데이터 및 데이터베이스, 사용자 및 전산요원, 시스템 관련문서, 전산자료 저장매체, 통신망 및 관련장비 등을 말한다.

2. 위협평가

위협(Threat)은 자산(Asset)에 해를 줄 수 있는 위험의 원천이다. 이와 같은 위협을 식별하고 분류해서, 발생빈도와 손실크기(Severity)를 측정하는 것을 말한다. 위협에는 위협원천에 따라, 자연재해로 인한 위협들(화재, 수재, 정전, 등), 사람에 의한 의도적 위협들(단말기, 디스켓, 등의 파괴 및 절취와 같은 물리적 공격, 그리고 시스템 자원의 불법사용, 허가되지 않은 자원의 불법접근, 타인으로 위장하여 권한사용, 바이러스, 벌레 등 유해프로그램 삽입과 같은 기술적 공격), 사람에 의한 비의도적 위협들(명령어 혹은 프로그램의 조작미숙 및 조작실수), 정보시스템의 결함(운용체제 결함, 응용프로그램의 결함, 통신 프로토콜의 결함, 통신 소프트웨어의 결함) 등이 있다.

3. 취약성평가

취약성(Vulnerability)이란 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어의 약점을 뜻한다. 이와 같은 약점을 확인하고 분류하여 위협을 감소시키는 것이 취약성을 평가하는 목적이다. 취약성에는 관리적 취약성(보안관리, 인원관리, 절차상관리, 사고대책관리, 등에 대한 취약성), 기술적 취약성(하드웨어, 응용소프트웨어, 운영체계, 데이터베이스, 네트워크, 등에 대한 취약성), 물리적 취약성(출입통제, 환경관리, 등에 대한 취약성)이 있다.

4. 위험분석전략 선택

자산에 대한 기대손실을 분석하는 과정으로서 위험분석에 대한 전략은 다음과 같이 네 가지 접근방법으로 구분할 수 있다.

첫째, 기본통제 접근방법(Baseline Approach)은 모든 조직에 대해서 기본적인 보안요구사항을 충족시키는 표준적인 보안대책의 집합을 구축하는 것이다. 기본통제의 장점은 시간과 비용을 많이 들이지 않고 모든 조직에서 기본적으로 필요한 보안대책을 선택할 수 있다는 것이다. 단점은 조직의 특성을 고려하지 않았기 때문에, 조직 내에 부서별로 적정 보안수준보다도 높게 혹은 낮게 보안통제가 적용된다는 것이다.

둘째, 비공식적인 접근방법(Informal Approach)은 조직 내부에 보안전문가가 없을 때, 외부 전문가의 지식과 경험을 이용하는 것이다. 장점은 별도의 기

술을 습득할 필요가 없기 때문에, 작은 조직인 경우에는 비용 효과적이라는 것이다. 단점은 구조화된 접근방법이 없기 때문에, 위험을 제대로 평가하기 어렵고 보안대책의 선택 및 소요비용을 합리적으로 도출하기 어렵다. 또한, 계속적으로 반복되는 보안관리의 보안감사 및 사후관리가 어렵다는 것이다.

셋째, 상세 위험분석(Detailed Risk Analysis)은 자산의 식별 및 평가, 자산에 대한 위협 및 취약성 평가를 근거로 위험의 발생확률과 손실크기를 곱해서 기대손실을 가능하면 계량적으로 계산하는 것이다. 손실크기를 화폐가치로 계산할 수 없으면, 정성적인 위험분석법을 이용한다. 장점은 조직 내에 부서 별로 적절한 보안수준을 마련할 수 있다는 것이다. 단점은 전문적인 지식과 시간과 노력이 많이 소요된다는 것이다.

넷째, 복합적인 접근방법(Combined Approach)은 기본통제 접근방법과 상세 위험분석의 장점을 이용하는 것이다. 즉 조직 내에 특정 부서가 높은 위험에 직면해 있거나 매우 중요한 부서인 경우에는 상세 위험분석을 하고, 그렇지 않은 경우에는 기본통제 접근방법을 이용한다. 장점은 보안전략을 빠르게 구축할 수 있고, 상대적으로 시간과 노력을 효율적으로 활용할 수 있다는 것이다. 단점은 두 가지 방법의 적용대상을 명확하게 설정하지 못 함으로써, 자원의 낭비가 발생될 수도 있다는 것이다.

본 연구에서의 위험분석은 기본통제를 전제로 한 정보보호지표를 도출하고자 한다. 즉 모든 조직에 대해서 기본적인 보안요구사항을 충족시키는 표준적인 보안대책의 집합을 전제로 해서 취약성의 정도를 정보보호지표로 나타내고자 한다. 본 연구에서는 정보보호의 기본통제에 대한 표준적인 분류체계를 물리적 보안, 논리적 보안, 관리적 보안으로 분류하고, 이에 대한 하위요소를 다음과 같이 구분하였다.

4.1 물리적 보안(Physical Security)

물리적 보안은 전산실이나 통신실 등의 시설물과 정전압 및 무정전 설비, 공기정화설비, 집진장치 등 물리적 시설과 장비에 대한 물리적 침입과 파괴, 자연재해 등의 위협요인으로부터 자산을 보호하기 위한 정보통신시설, 설비의 위치설정, 기계적 기준 등을 말한다. 첫째, 환경보안(Environment Security)은 정보시스템의 자산이 설치되어 있는 건물과 관련된 모든 위험에 대한 보호이다. 둘째, 물리적 접근보안(Physical Access Security)은 권한 있는 사람의 물적 접근통제와 관련된 모든 위험에 대한 보호이다. 셋째, 물적가용보안(Physical Availability Security)은 하드웨어를 항상 사용하지 못하는 위험에 대한 보호이다.

4.2 논리적 보안(Logical Security)

논리적 보안은 소프트웨어와 데이터를 대상으로 불법적이고 의도적인 접근 또는 비의도적인 실수나 오용으로부터 보호하기 위해서 인증, 암호화 등 접근통제나 통신보안을 하는 것을 말한다. 첫째, 소프트웨어 보안(Software Security)은 모든 응용 및 운영 시스템의 정확하고 연속적인 운영장애에 대한 보호이다. 둘째, 자료보안(Data Security)은 모든 자료항목에 대해서 권한 없는 자의 접근변경에 대한 보호이다. 세째, 통신보안(Communication Security)은 통신시스템의 보안과 관련된 위험에 대한 보호이다.

4.3 관리적 보안(Management Security)

관리적 보안은 물리적 및 논리적 자산을 다루는 사람과 조직 그리고 행정에 관한 것으로 인간에 의한 의도적 및 비의도적 위협으로부터 보호하는 것을 말한다. 첫째, 행정적 보안(Administrative Security)은 최고경영층 측면에서 보안정책과 관련된 모든 위험에 대한 보호이다. 둘째, 조직적 보안(Organizational Security)은 조직적 측면 특히 중간관리층의 보안관리의 실행과 관련된 모든 위험에 대한 보호이다. 셋째, 인적 보안(Personnel Security)은 조직구성원 개개인의 보안과 관련된 모든 위험에 대한 보호이다.

취약성 개념은 정보시스템에 대한 위험을 모형화하는데 중요한 역할을 한다. 취약성 모형은 정보보호 분야에서 현재 가장 많이 사용되는 모형으로서, 이에 기초하여 많은 위험분석 소프트웨어, 위험관리에 관한 정책이나 지침들이 개발되어 왔다. 취약성이 있다고 해서 곧 바로 손실을 입지는 않지만, 위협요소들이 침입 할 수 있는 근거를 제공하게된다. 취약성 개념에는 일반적으로 다음과 같이 3가지가 있다.

첫째, 취약성을 '자산의 속성' 으로 파악하고 있다. 취약성을 "자산을 손상시켜서 위험을 일으키는 시스템의 성질", 보다 구체적으로 "시스템 내에서 불법적 상태로 변화되는데 소요되는 노력의 양에 대한 부적인 측정치(Inverse Measure)" 라고 정의했다[14]. 또한, 취약성을 "기존 시스템의 약점"이라고도

했다[10].

둘째, 취약성을 '자산과 위협의 관계'로 파악하고 있다. 취약성을 "자산, 위협, 보안대책, 보안대책 효과간의 함수관계를 갖는 실체" 라고 정의했다[15]. 또한, 취약성을 "위협영향과 자산의 대응관계"로 파악하고, 취약성을 도출하기 위해서 다음과 같은 3가지 고려사항을 제시했다. 첫째는 자산이 위협받을 가능성, 둘째는 자산이 위협에 의해 손상되는 정도, 셋째는 보안대책 효과이다[16].

셋째, 취약성을 '보안대책의 결핍(Absence of Safeguards)'으로 파악하고 있다. 취약성을 "위협공격에 대한 통제 실패확률"이라고 했다[17]. 또한, 취약성을 "위협공격에 노출되어 있는 시스템의 상태", 그리고 "보안대책시스템 내에 약점, 혹은 보안대책의 결핍"이라고 했다[18]. 이러한 취약성 개념 측면에서 위험모형을 나타낸 것이 〈그림 2〉이다.

위협 T1이 자산 A1을 공격했을 때, 자산 A1은 보안대책 S1에 의해서 보호되었다. 위협 T4가 자산 A4를 공격했을 때는 보안대책이 없어서 손실이 발생되는 경우이다. 그러나, 위협 T2이 자산 A2를 공격했을 때, 자산 A2는 보안대책 S2에 약점이 있어서 보호되지 못했다. 이와 같은 실패 확률을 실제 정량적으로 추정하기는 어렵다. 그러므로, 본 연구에서는 취약성 개념을 보안대책의 약점으로 보호 실패되는 경우는 제외하고, 단지 보안대책의 결핍상태라고 정의한다.

취약성 평가의 목적은 자산에 손실이 발생될 수 있는 약점을 식별하고 분류하여 위협을 감소시키는데 있다. 취약성 평가란 "식별된 위협원천에 의해서 손상될 수 있는 기존 시스템의 약점에 대한 심각성 수준을 식별하고 평가하는 것" 이라고 했다[10]. 취약성 평가는 취약성에 대한 정의에 따라 그 방법이 달라질 수 있다. 단순히 '자산의 속성'으로만 정의하면, 취약성을 정성적 혹은 정량적으로 평가하기가 어렵다. '자산과 위협의 관계'로 정의하면, 관계에 대한 구체적 모형이 제시되어야 한다. 계량적인 평가모형을 도출해도 실증적으로 적용하는데는 위협발생 혹은 손실발생에 대한 확률추정을 해야하는데, 이에 대한 과거자료를 확보한다는 것은 사실상 어려운 문제이다.

IV. 정보자산가치가중치법에 의한 정보호지표의 계량화

1. 취약성 평가에 의한 정보보호지표의 개념 도출

본 연구에서는 취약성이란 보안대책의 결핍상태로 정의한다. 또한, 취약성 평가란 보안대책의 유무를 식별하여, 보안대책이 결핍상태에 있는 경우 위협발생을 감소시킬 수 있는 보안대책을 제시하는 것이라고 정의한다.

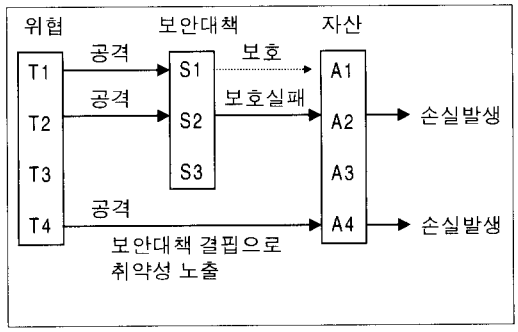

그림 2. 위협, 보호대책, 손실간 관계

그러므로, 정보보호 실행지표란 취약성 평가를 정보보호 의사결정을 위한 지표로 만든 것으로 다음과 같이 정의한다.

정보보호지표=실행하고 있는 보안대책/기본통제를 위한 보안대책

기본통제에 필요한 보안대책이 결핍되어 있을수록, 정보보호지표는 낮아져서 취약성이 많은 것을 나타낸다. 이와 같이 정보보호지표는 정보시스템의 정보보호 구현수준을 나타낸다. 이와 같이 정보보호지표를 계량적으로 지수화 했을 경우, 0 〈 정보보호지수 〈 1 이다. 여기서 정보보호지수가 0 이란 것은 기본통제를 위해 필요한 보안대책이 하나도 없다는 것이고, 정보보호지수가 1 이란 것은 기본통제를 위해 필요한 보안대책을 모두 갖추고 있다는 것을 말

한다. 문제는 기본통제를 위해 필요한 보안대책들의 항목분류체계와 계량화 방법이 문제이다.

정보보호지표는 정보보호지수 혹은 경우에 따라서는 손실액으로도 나타낼 수 있다. 산출지표, 결과지표, 영향지표에 대한 정보보호지수는 전체 정보보호지수 혹은 개별 정보보호지수(물리적 정보보호지수, 논리적 정보보호지수, 관리적 정보보호지수, 생존력지수)로 나타낸다. 구체적으로 설문지 질문내용의 중요도를 감안하여 가중치를 감안한 점수법에 의해서 정보보호지수를 계산하여 지수로 도출하게 된다. 정보보호지수는 전체항목수 중에서 보안대책이 있어서 Yes라고 대답한 항목수의 비율에 상대적 가중치를 곱한 정보보호분야별 점수를 합한 것이다.

정보보호지수(SI) = 가중점수의 합 = {정보보호분야별 점수*상대적 가중치)의 합 = {(Yes 항목 수/전체 항목 수)*상대적 가중치)}의 합

정보보호지표를 손실액으로 나타내는 경우에, 손실액은 3가지 형태의 손실 - 유형의 직접손실, 유형의 간접손실, 무형손실 - 을 추정한다. 유형의 직접손실은 계산하기가 쉽다. 또한, 쉽게 측정될 수 있으므로 유형손실이라고 한다. 기업의 경우 매출을 창출하는 기능을 추적함으로써 추정할 수 있다. 유형의 직접손실에는 매출손실, 제조손실, 납기손실, 그리고 기타 기회손실 등이 포함된다. 유형의 간접손실은 추정하기가 다소 어려운 편이다. 유형의 간접손실에는 벌금, 수수료, 시장지분, 기타 간접적으로 계산되는 손실이 포함된다. 무형손실은 계산하기가 가장 어렵다. 무형손실에는 추락한 공공신용, 고객의 불만족, 불이행된 약속, 손상된 평판, 기타 쉽게 계산할 수 없는 손실이 포함된다. 때때로 이러한 손실은 회계학적 손실로 추정할 수 없기 때문에 비용으로 계산되지 않는 경우가 있다. 이러한 경우에는 손실 을 계량화하지 못하더라도 추가적인 설명을 기술해야 한다.

이러한 손실추정은 활동기준원가계산에 의해서 하는 것이 바람직하다. 활동기준원가계산(ABC: Activity-Based Costing)이란 기업의 중요한 활동들과 관련된 재무 및 운영성과 정보의 집합체이며, 여기서 활동이란 기업내의 각 집단이 기업목표의 달성을 위하여 수행하는 일체의 반복적인 과업으로 정의된다. 원가계산의 대상은 제품이 아니라, 지연 혹은 정지된 특정 업무기능의 프로세스이므로, 프로세스 가치분석(PVA: Process Value Analysis)에 근거한 총괄적 원가관리(TCM: Total Cost Management)가 이루어져야 한다.

2 정보자산가치평가에 의한 가중치 측정

정보자산의 분류는 속성, 위험지대(혹은 위치), 형태 등의 측면에서 다양하게 분류될 수 있다. 자산은 속성에 따라 유형자산과 무형자산으로, 그리고 위치에 따라 물리적 위험지대와 논리적 위험지대로, 그리고 형태에 따라 하드웨어, 소프트웨어, 데이타/데이타베이스, 사용자/전산요원, 시스템 관련문서, 전산자료 저장매체, 통신망 및 관련장비, 기타 부대설비 등으로 구분할 수 있다. 우선 자신이 가진 자산들을 일반적인 위험관리에서의 방법에 따라 분류하는 과정으로서, ①하드웨어, ② 소프트웨어, ③ 데이터/데이터베이스, ④ 사용자/전산요원, ⑤ 시스템 관련문서, ⑥ 전산자료 저장매체, ⑦ 통신망 및 관련장비, ⑧ 부대설비 의 8가지로 분류할 수 있다. 혹은 보다 간략하게 하려면 논리적대책을 위한 자산(①데이터, ②소프트웨어, ③ 통신), ④ 물리적대책을 위한 자산, ⑤ 관리적 대책을 위한 자산으로 분류하기도 한다.

표 2. 정보자산의 분류

자산분류		자산항목
물리적 자산		소스/목적/OS/응용/시스템 프로그램 등
논리적 자 산	소프트웨어	처리, 저장, 출력, 보관, DB 데이터 등
	데이터	터미널, 메세지, 통신장비 등
	통신	하드웨어, 부대설비, 전산실 출입문 등
관리적 자산		인원, 문서, 조직등

기본통제분석과정에서 자산에 대한 대책들의 검사항목목록에서 작성된질문표의 분류에 따라 자산을 분류하는 것이 좋다. 다음의 적용 사례에서는 자산에 대한 대책으로 5가지로 분류하였으므로 이러한 방법으로 나눈다면 표 2. 와 같다. 자산분석은 정보시스템 내에 모든 자산을 식별하고 분류해서, 그 가치를 평가하는 것이다. 자산분류를 논리적, 물리적, 관리적 자산으로 분류했을 때, 논리적 자산가치는

파괴된 소프트웨어, 데이터, 통신을 재복구시키는데 소요되는 비용을 추정해야 하고, 물리적 및 관리적 자산가치는 대체비용을 추정해야 한다.

유형자산에 대한 재복구비용 혹은 대체비용은 취득원가 혹은 감가상각기초가액으로 평가할 수 있다. 취득원가란 구입의 경우에는 구입에 소요된 구입원가가 되고, 자기제작의 경우에는 제작에 소요된 제작원가가 된다. 감가상각기초가액이란 감가상각할 때에 기준이 되는 금액으로 상각할 수 있는 최고한도액이라고 할 수 있다. 기초가액은 취득원가로부터 잔존가액을 차감한 금액으로 이 금액이 감가상각할 수 있는 금액이다. 즉 감가상각기초가액 = 취득원가 - 잔존가액 이다. 유형자산이외에 무형자산에 대한 재복구비용은 추정하는 것이 매우 어렵다. 무형자산이란 물적실체가 없는 고정자산으로서, 이 자산을 소유함으로써 미래의 경제적 효익을 얻을 수 있는 것이다. 논리적 자산 중 특히 데이터 자산의 재복구비용은 이러한 무형자산과 관련되어 있다.

산업화 사회의 재무자본 관점에서 발달된 기존의 회계개념으로는 정보화 사회의 지적자본을 평가하는 데는 한계가 있다. 여기서 지적자본은 유형자산을 대표하는 재무자본에 대응되는 개념으로 조직이 보유하고 있는 무형자산을 총칭하는 개념이다. 지적자본과 관계된 경영활동에는 지식창조 측면과 지식축적, 활용, 평가 측면이 있다. 이러한 지적자본은 지식자본으로서, 비재무적 자산이며, 무형의 보이지 않는 자산이지만, 전략목표 달성에 핵심이 되는 자산이다. 지적자본을 시장자산(브랜드, 고객규모, 로열티, 유통경로 등), 인간중심자산(리더쉽, 직원의 문제해결능력, 경영기술 등), 지적소유자산(상표권, 특허권, 노하우, 등), 인프라자산(정보기술시스템, 업무처리과정, 기업문화, 재무구조 등) 네가지로 구분하기도 한다. 인프라자산에 속하는 정보자산 평가방법으로는 보유수준조사, 투자수익율평가, 기업목표와의 부합도, 부가가치평가, 고객면담조사, 종업원면담조사, 자산평가기준 등이 있다.

표 3. 정보자산가치평가에 의한 가중치의 계량화

자 산	용 도	가용성 가치	무결성 가치	기밀성 가치	가중치
데이터베이스	자료보관	중	대	중	0.67

지적자본은 크게 인적자본(human capital)과 구조적자본(structural capital)으로 구성된다. 인적자본은 조직구성원들이 가지고 있는 지식, 기술, 능력의 결합물이다.

계량화하는데는 3가지 척도가 있다. 첫째, 서수(Ordinal)로 평가치를 서열 혹은 순서로 표시하는 것이다. 둘째, 구간(Interval)으로 평가치들 사이의 동등한 정도를 구간으로 나타내며, 동시에 임의의 원점으로부터의 평가치들 사이의 차이를 나타낸다. 셋째, 비율(Ratio)로 미리 정해진 원점으로부터 평가치들 사이의 차이를 나타낸다. 그러므로, 정보자산가치는 반드시 비율척도인 화폐가치로 평가하지 않고, 등간척도로서 평가할 수도 있다. 즉 3점척도(대, 중, 소: 1, 0.5, 0) 혹은 5점(1, 0.75, 0.5, 0.25, 0)척도로 측정할 수 있다.

상대적 가중치의 합은 1이 되도록 정규화(Normalization)한다. n개 요소가 있을 때, 가중치의 집합은 벡터의 형태로 다음과 같이 표시된다.

$$wT=(w1, ..wj, ..wn), \sum_{j=1}^{n} wj=1$$

단순가중치법(Simple Additive Weighting Method)에서는 가중치를 다음과 같이 계산한다. 여기서, xij 는 대안 i 가 요소 j에서 기수로 나타난 비교가능한 척도에서의 평가치이다.

$$\sum_{j=1}^{n} wjxij \; / \sum_{j=1}^{n} wj$$

예로서, 어떤 지역의 전산망에 컴퓨터시스템에서 특정 데이터베이스 중에 매년 해커에 의해서 침입된다는 사실이 통계조사의 결과로 밝혀졌다. 이 지역에서 정보에 대한 보안요구사항으로서 가용성, 무결성, 기밀성 측면에서 특정 데이터베이스에 대한 정보기술전문가의 평가 예가 (표3)과 같다. 가중치는 0 보다 크거나 같고 1보다 작거나 같으므로, 가중평균해서 {중(0.5)+대(1.0)+중(0.5)}/3=0.67으로 계량화 될 수 있다.

대부분의 의사결정문제는 대체안 평가를 위한 속성이 여러 개로 구성되어 있으며, 질적 그리고 양적

특성을 갖고 있다. 정보보호지표와 관련 있는 여러 가지 항목들을 고려하여 측정 가능한 속성들에 대해서 선호가중치를 평가하여야 한다. 효과적으로 속성들의 선호도를 평가하기 위해서는 무엇보다도 선호 예측력과 실용성 있는 선호모형이 필요하다. 지금까지 설명한 정보보호지표 계량화모형은 정보자산가치에 따라서 가중치를 주는 단순가중치모형으로서 다속성 효용이 개별속성의 효용으로 분리될 수 있다는 가정 하에 속성들 간의 한계가치를 평가하는 것이다.

이와 같은 점수모형(Scoring Model)에는 단순가중치법 이외에, 계층가중치법(Hierarchical Additive Weighting Method), 교호단순가중치법(Interactive Simple Additive Weighting Method) 등이 있다. 또한, 가중치 산출방법에는 Eigenvector방법, 가중최소자승법(Weighted Least Square Method), 엔트로피(Entropy)방법, LINMAP (Linear Programming Technique for Multi -dimensional Analysis of Preference) 등이 있다. 위와 또 다른 접근방법에는 다속성효용함수모형(MAUT: Multi-Attribute Utility Model), AHP모형(AHP: Analytic Hierarchy Process), 동적태도모형(ADAM: Attribute-Dynamic Attitude Model) 등이 있다. 여러 가지 다속성 선호모형의 근본적인 차이는 일차적으로 중요도 가중치 도출방법에 있다. 속성의 가중치 도출방법으로는 Schoemaker-Waid가 제시한 MR(Multiple Regression), AHP (Analytic Hierarchy Process), DT(Direct Tradeoff), PA(Point Allocation), UW(Unit Weighting) 등이 있고, 서수적 선호의 총괄방법으로는 Jensen이 제시한 BK(Borda-Kendall), MV(Minimum Variance), MR(Mean of Ranks), ME(Mean of Eigenvector), GM(Geometric-Mean Matrix Eigenvector) 등이 있다.

3. 정보보호지수의 도출

취약성 평가란 식별된 위협원천에 의해서 손상될 수 있는 기존 시스템의 약점에 대한 심각성 수준을 식별하고 평가하는 것이므로, 취약성 평가는 취약성에 대한 정의에 따라 그 방법이 달라질 수 있다. 단순히 '자산의 속성'으로만 정의하면, 취약성을 정성적 혹은 정량적으로 평가하기가 어렵다. '자산과 위협의 관계'로 정의하면, 관계에 대한 구체적 모형이 제시되어야 한다. 계량적인 평가모형을 도출해도 실증적으로 적용하는데는 위협발생 혹은 손실발생에 대한 확률추정을 해야하는데, 이에 대한 과거자료를 확보한다는 것은 사실상 어려운 문제이다. 위험분석에서 위험이 측정 가능하다는 전제하에, 위험을 빈도와 강도(손실액)의 곱인 기대손실로 정의해서 측정하게 된다. 그러나, 대부분의 경우 계량화된 과거 손실자료가 충분치 않기 때문에, 취약성 평가를 위한 검사항목목록의 정보보호항목을 보안관리 영역별로 점수화해서 지표로서 계량화시킨다.

기본통제분석은 일반적인 기관에서 갖추어야 할 위험관리를 위한 통제 수단이 마련되어 있는지 검사항목목록으로 작성하여 조직의 위험 취약요소들을 분석하려는 방법이다. 보통 작성된 질문표를 통해 받은 회답지를 통계 분석하여 자산식별 분류에 의한 각종대책들의 현재 보안상태를 분석하게 된다. 기본통제는 모든 기관에서 공통적으로 정보 보호를 위해 구축해야 할 기본적인 통제 수단을 목록형식으로 작성한 후, 이를 이용하여 조직의 취약성을 분석하고 미비된 대책 보완하도록 하게 된다. 검사항목 목록은 질문서법을 이용하며, 질문내용의 중요도를 감안하여 가중치를 감안한 점수법 또는 표준화를 통해서 정보보호지수(SI: Security Index)를 계산하여 취약성을 평가하게 된다. 여기서 Ni 는 정보보호분야 별 항목수이고, Yi 는 보안대책이 있어서 Yes라고 대답한 항목수이고, wj 는 상대적 가중치 이다.

정보보호지수(SI)=가중점수의 합=(정보보호분야별 점수*상대적 가중치)의 합={(Yes 항목 수/전체 항목 수)*상대적 가중치)}의 합

$$= \sum_{j=1}^{n} \{(Yi/Ni)*wj\}$$

검사항목목록에 포함될 내용은 위에서 기술한 보안관리의 분류체계와 같이 크게 3 분야로 구분하는 것이 일반적이다. 정보시스템 전체 정보보호지수는 분야별로 물리적 정보보호지수, 논리적 정보보호지수, 관리적 정보보호지수로 구분 할 수 있다. 특히 백업 및 복구를 물리적 보안영역에 포함시키지 않고 별도의 분야로 취급하는 경우가 많다. 그래서 백업 및 복구에 관한 항목만으로 계산한 백업/복구 정보

보호지수를 정보시스템의 생존력지수(Survivability Index)라고 정의할 수도 있다. 그러므로, 정보시스템 전체 정보보호지수는 물리적/논리적/관리적 정보보호지수와 생존력지수로 나눌 수 있다.

여기서 생존력(Survivability)이란 용어의 정의가 학자들마다 서로 다르지만, 일반적으로 백업 및 복구와 관련된 신뢰성(Reliability), 고장방지능력(Fault -tolerance), 안전성(Safety), 가용성(Availability) 등의 개념들을 포함하고 있다. 생존시스템(Survivable Systems)의 주요 특징은 공격, 고장, 사고에 직면해서도 본질적인 서비스를 제공할 수 있는 능력이다. 생존력 서비스의 일반적인 영역에는 저지(Resistence), 인식(Recognition), 복구(Recovery), 적응 및 진화(Adaptation and Evolution) 등 4가지가 있다. 일반적으로 생존력의 영역은 비유계(unbounded) 네트워크 환경이다. 유계(bounded) 시스템이란 모든 하위 시스템이 단일화된 관리체계에 의해서 통제되는 시스템이고, 비유계 시스템이란 단일화된 관리통제가 없는 시스템이다.

정보시스템의 전체 정보보호를 물리적/논리적/관리적 정보보호 3가지 영역으로만 구분한 경우에, 전체 정보보호지수를 계산하는 절차는 다음과 같다. 이러한 기본통제 분석 방법에 의한 검사항목 목록에 의해 질문문항을 자산의 대책을 위한 5가지 분류 방식에 의해 질문표를 가상의 모 기관을 대상으로 회답지를 받아 이를 분석한 결과가 아래 표와 같다. 여기의 통계치는 가상적으로 데이터를 만들어 보았으며, 이 질문은 일반적으로 Y(Yes), N(No), N/A(Not Available)로 답할 수 있도록 되어있으며, N/A에 대한 답은 전체 통계에서 제외시켰다.

자산가치 평가에 의한 가중치가 소프트웨어, 데이터, 통신, 물리적 보안, 관리적 보안에 대해서, 각각 0.50, 0.50, 0.50, 0.75, 0.25 이라면, 소프트웨어의 상대적 가중치는 0.50/(0.50 + 0.50 + 0.50 + 0.75 + 0.25) = 0.2 가 된다. 정보시스템에 대한 전체 정보보호지수(SI)는 다음과 같은 기준에 의해 의미를 해석할 수 있다.

.0 〈SI〈 .25 --〉 전반적인 보호시스템 재구축 필요(D등급)

.25〈SI〈 .50 --〉 상당부문 보호시스템 수정 및 보완 필요(C등급)

.50〈SI〈 .75 --〉 부분적인 보호 대책 보완 필요(B등급)

.75〈SI〈1.00 --〉 새로운 위협 요소에 대한 대비 필요(A등급)

표 4. 정보보호지표의 계량화

대분류		소분류	Yes 항목수	No 항목수	전체 항목수	항목별점수	상대적가중치	가중점수
논리적 보안	소프트웨어	소프트웨어 접근제어	25	14	39	25/39=0.64	0.2	0.128
		소프트웨어개발과 변경통제						
	데이터	데이터 민감도 분류	15	17	32	15/32=0.47	0.2	0.094
		백업,저장,보관,복사,폐기						
		무결성 체크						
	통신	암호화, 키관리	2	9	11	2/11=0.18	0.2	0.036
		통신보안 프로토콜						
물리적 보안		시설물에 대한 접근통제	5	4	9	5/9=0.56	0.3	0.168
		시설/설비의 입지 조건						
관리적 보안		인사정책,훈련/인식,	7	12	19	7/19=0.37	0.1	0.037
전체점수			54	56	110	54/110=0.49	1.00	SI=0.463

본 예에서는 전체 시스템의 취약성 정도를 나타내는 정보보호지수(SI)는 0.463 으로, 상당부문 보호시스템 수정 및 보완 필요한 상태로 나타났다. 부문별 가중점수는 물리적 보안이 상대적으로 양호하고, 이에 반해 통신 보안은 가장 취약한 부문으로 나타나 상당부문 보호시스템을 재구축 할 필요가 있다. 이와 같이 정보보호지수(SI)를 정보시스템 별로 A, B, C, D로 등급화해서 보안감사 결과에 대한 인증을 제도화 할 수도 있다.

V. 결 론

정보보호지표란 특정 집단의 정보보호 특성을 가장 간단하고 명확하게 나타내주는 통계수치로서, 각종의 통계 자료와 함께 정보보호 정책을 결정하는데 매우 유용하게 사용된다. 그러나, 정보보호지표는 지표 산출방법이나 데이터 수집상의 문제로 인해 현실적인 어려움을 수반하고 있다. 정보보호지표는 시스템 관점에서 위협의 투입에 대한 정보보호 원인지표가 있고, 보안대책의 행위에 대한 정보보호 실행지표가 있고, 자산의 보호 측면에서 정보보호 산출지표, 정보보호 결과지표, 정보보호 영향지표가 있다.

정보보호 결과지표는 위협과 관련된 조직의 취약성을 분석하는 위험분석에 의해서, 정보자산에 대한 위협의 손실액으로 나타내므로, 조직 내에 정보자산의 가치를 파악해야 한다. 정보자산가치의 중요도를 감안하여 가중치를 고려한 단순가중치모형에 의해서 정보보호지수를 도출하였다. 이와 같은 정보보호지표를 단일 수치로 계량화한 정보보호지수는 물리적/논리적/관리적 정보보호지수와 생존력지수로 나눌 수 있다. 이러한 정보보호지표를 이용해서 보안관리를 단계적으로 ①보안정책, ②보안조직의 역할과 책임, ③위험분석전략(기본적인 접근방법, 비공식적인 접근방법, 세밀한 위험분석, 복합적인 접근방법의 선택, ④보안위험평가, ⑤시스템보안의 정책 및 계획, ⑥보안대책의 설치 및 보안의식, ⑦보안감사 및 사후관리 등을 효율적으로 실행할 수 있다.

본 연구의 정보자산가치가중치법은 다속성선호모형으로서 속성간의 독립성을 전제로 하고 있다. 그러나, 정보보호지표 항목 속성간의 독립성 조건을 완전하게 만족시키지 못한 상태에서, 단순가중치모형의 타당성을 어디 정도 논할 수 있는지 의문이 있다. 그럼에도 불구하고, 기존의 체크리스트 접근방법은 물론 CRAMM, BDSS 등 대부분의 위험분석 소프트웨어에서는 단순가중치모형을 채택하고 있다. 속성들간의 완벽한 독립성을 유지하고 있는 경우는 많지 않다는 점을 감안하여, 앞으로의 연구과제는 독립성 조건을 완화한 모형의 개발이 필요하다.

참 고 문 헌

[1] 한국전산원, 국가정보화백서, 1998.

[2] 황병천, 오정훈, 박민구, *지방자치단체 정보화 수준측정을 위한 지표개발*, 행정자치부 자치정보화지원재단, 1998. 11.

[3] GSA(General Services Administration), "Performance-Based Management: Eight Steps to Develop and Use Information Technology Performance Measures Effectively," *GSA Report*, 1997.

[4] Barzelay, M., "Performance Auditing and the New Public Management: Changing Roles and Strategies of Central *Audit Institutions*," *in the Performance Auditing and the Modernisation of Government*, PUMA of the OECD, 1996.

[5] Bouckaert, G., *Performance Management in Government: Performance Measurement and Results-Oriented Management No.3*, Public Management Occasional Papers, PUMA of the OECD, 1994.

[6] DOD(Department of Defense), "Information Management Performance Measures," *Report by a Panel of the National Academy of Public Administration*, 1996.

[7] DOE(Department of Energy), *How to Measure Performance: A Handbook of Techniques and Tools*, 1995.

[8] Myers, B. L., Kappelman, L. A., and Prybutok, V. R. (1997), "A Comprehensive Model for Assessing the Quality and Productivity of the Information Systems Function: Toward a Theory for Information Systems Assessment," *Information Resources*

Management Journal, 10(1), 6-25.

[9] Moses, R., "Risk Analysis and Management," *Computer Security Reference Book* edited by Jackson, K. M. & Hruska, J. & Parker, Donn B., CRC Press, Inc., pp.227-263, 1992.

[10] ____ , "CCTA Risk Analysis and Management Methodology (CRAMM)," Datapro Reports on Information Security, *Risk Analysis*, December, pp.101-110, 1992.

[11] ISO/IEC JTC1/SC27 N689, *Guidelines for the Management of IT System Security: Part3- Techniques for the Management of IT Security*, ISO, Mar. 1993.

[12] ISO/IEC JTC1/SC27 N720, *Guidelines for the Management of IT Security (GMITS): Part2 -Managing and Planning IT Security*, ISO, May. 1993.

[13] ISO/IEC JTC1/SC27 N777, *Guidelines for the Management of IT System Security(GMITS): Part1-Concepts and Models for IT Security*, ISO, Oct. 1993.

[14] Otwell, K. and Aldridge, B., "The Role of Vulnerability in Risk Management," *Computer Security Journal*, Vol.VI, No.1, pp.15-21, 1989.

[15] Katzke, S., "A Government Perspective on Risk Management of Automated Information Systems," *Proceedings of the 1988 Computer Security Risk Management Model Builders Workshop*, pp.3-20, 1988.

[16] Schmit, E., "Conceptual Model of the Risk Management Process," *Proceedings of the 1988 Computer Security Risk Management Model Builder Workshop*, pp.89-102, 1988.

[17] Guarro, S., "Analytical and Decision Models of the Livermore Risk Analysis Methodology (LRAM)," *Proceedings of the 1988 Computer Security Risk Management Model Builders Workshop*, pp.49-72, 1988.

[18] Gilbert, I. A.,"Risk Analysis: Concepts and Tools," Datapro Reports on Information Security, *Risk Analysis*, pp.101-112, Sep. 1991.

〈著者紹介〉

김 기 윤 (Ki-Yoon Kim)
1976년 : 고려대학교(공학사)
1979년 : 고려대학교(경영학 석사)
1985년 : 고려대학교(경영학 박사)
1980년 - 현재 : 광운대학교 경영학과 정교수
〈관심분야〉 정보시스템 보안/위험관리

나 관 식 (Kwan-Sik Na)
1986년 : 광운대학교(경영학사)
1988년 : 광운대학교(경영학석사)
1992년 : 광운대학교(경영학 박사)
1993년 - 현재 : 서원대학교 경영정보학과 조교수
〈관심분야〉 정보시스템 보안/위험관리