경영정보학연구
제9권 제4호
1999년 12월

정보보안수준 계량화 연구*

김 현 수**

A Study on the Quantification of Information Security Level

Kim, Hyun-Soo

This study presents an information security level index and a quantification scheme. A comprehensive survey on previous researches in information security checklists has been performed. A candidate indicator list for information security level has been developed. Desirability of each indicator has been tested by 4 criteria. They are general validity, relative importance, probability of accident and impact of accident. 67 experts' opinion has been collected and analysed. The result shows that selected indicators are a very good candidate set for the determination of information security level. A factor analysis shows indicators are well structured. There exists strong correlations between validity and probability, validity and impact, and importance and probability. A quantification scheme of information security index has been developed by experts' judgement and statistical tests.

* 이 연구는 한국학술진흥재단의 1998년 연구비 지원에 의하여 연구되었음.
** 국민대학교 정보관리학부

Ⅰ. 서 론

최근 빠르게 진행되고 있는 우리사회 각 부문의 정보화는 정보보안의 필요성을 급속히 증대시키고 있다. 정보시스템 구축이 활발해지고, 그 기능이 증대되면서 정보시스템의 건전하고 효율적인 운용의 중요성이 더욱 높아지고 있으며, 정보 보안이 필요한 정보시스템 개발이 증가되고 있다. 정보시스템의 구축효과를 극대화하기 위해서는 각종 위험으로부터 정보시스템을 보호해야 한다. 따라서 정보보안에 대한 각 부문의 인식이 제고되어 정보보안의 수준을 파악하려는 요구가 증대되고 있다.

보안은 위협(threat)으로부터 자산을 보호하는 것이며, 여기서 위협이란 보안대상 자산의 오용(abuse)을 의미한다. 또 정보시스템의 보안은 '정보시스템의 자료와 자원의 무결성, 기밀성, 가용성을 관리하기 위하여 수립되는 통제구조'라고 정의된다[김기범 외, 1997]. 여기서 무결성(integrity)은 자료가 의도적이나 비의도적으로 변경 또는 파괴되지 않는 특성을 의미한다. 또한 기밀성(confidentiality)은 정보가 비인가된 개인, 개체, 처리들에게 누설되거나 공개되지 않는 특성을 의미하며, 가용성(availability)은 인가된 실체가 요구할 때 정보기술 자원에의 접근과 사용을 가능하게 하는 특성을 의미한다.

보안의 개념도 정보화가 진전됨에 따라 많은 변화를 거치고 있다. 1970년대에는 데이터보안(data security)중심의 개념에서, 1980년대에는 컴퓨터보안(computer security), 1990년대에는 정보보안(information security)의 개념으로 사용하고 있다.정보보안에 대한 위협은 조직의 내부자 및 외부자, 인가자 및 비인가자등 다양한 원천으로부터 올 수 있다. 통계에 의하면 외부자보다 내부자에 의한 정보 범죄가 많으며, 인가자에 의한 범죄가 비인가자에 의한 범죄보다 많은 것으로 나타나고 있다. 따라서 정보보안은 위협의 원인별로 별도의 대책을 수립할 필요가 있다.

즉 정보보안은 보안의 기술과 전략, 보안 대상 및 범죄 원인 등의 차원에서 포괄적으로 정의되는 것이 바람직하다.

이러한 관점에서 볼 때 정보보안은 과거와 같이 단순히 정보통신 분야의 기술 또는 서비스로 인식되는 차원을 벗어나서, 기업경쟁력 또는 국가경쟁력 강화차원에서 논의되어야 하며, 전체 산업의 경쟁력 차원에서 논의되어야 한다. 정보보안의 실현은 기술적 측면이 기본 전제가 되지만 법/제도적인 환경적인 측면과 사용자의 식의 측면에서 함께 기반이 갖추어져야 한다.

정보보안 지표는 정보보안의 여러측면을 고려하여 수준을 판단하는 기준으로서 기업 또는 국가의 정보보안 수준을 측정하고 정보보안 전략 및 정책 수립에 활용될 수 있다. 비교적 오래전부터 국내에서 연구된 정보화지표의 경우와 같이, 정보보안 지표는 정보보안의 각 부문에 대해 수치화된 자료를 이용하여 평가하고, 이를 종합적으로 점수화하여 나타내는 수치라고 정의할 수 있다. 정보보안 지표에 대한 연구는 기존 연구 사례가 거의 없으므로 본 연구에서는 정보보안 요소의 분류부터 시작하여 체계 정립을 위한 노력부터 시작하였다. 즉 정보보안의 환경적 요소, 기술적 요소, 관리적 요소, 산업적 요소 등 거시적인 차원의 분류에서 시작하여 각 부문별로 세부 요소를 도출하는 과정을 수행하여 정보보안의 전체 체계 모델을 먼저 정립하였다.

정보보안의 경우, 기존의 관련 연구인 정보화지수나 정보인프라 지수와는 달리 정보보안상의 취약성과 위협을 용이하게 발견할 수 있는 지표 구성이 되어야 한다. 즉 기술적 측면, 조직적 측면, 사회적 측면의 각각에 대해 위험과 취약성이 복잡하게 존재하므로 시스템의 위험분석을 병행하는 차원에서의 지수 설정과 진단평가가 수행되어야 한다. 단순히 비교가능한 수치의 수준을 넘어서서 절대적으로 나온 수치가

위험의 가능성을 어느정도 내포하고 있는지를 알려 줄 수 있어야 하며, 위험으로 인한 손실은 어느 정도인지 예측가능한 모델이 되어야 한다.

본 연구는 이러한 필요성에 입각하여 정보보안 수준 지표 작성을 위해 정보보안 지표의 개념을 정립하고, 지표를 구성하는 기준항목을 선정하며, 선정된 항목 및 지표의 계량화 방안에 대해 대안을 제시하였다. 다음 제 2 장에서는 기존의 보안수준 측정 관련 연구와 그 문제점을 요약하여 제시하고, 제 3 장에서는 전문가 조사에 대한 통계분석 결과를 토대로, 본 연구의 지표모델을 제시한다. 제 4 장에서는 정보보안 수준 계량화 모델을 제시하며, 제 5 장에서는 결론과 향후 연구방향을 제시한다.

Ⅱ. 정보보안 지표 항목과 계량화 연구

정보보안 수준을 계량화하는 연구는 직접적인 계량화 목적으로 수행된 경우는 극소수이고, 정보시스템 감사 등의 목적으로 개발된 체크리스트 개발 연구가 대부분이다. 이들 방법은 자산가치에 의해서 가중치를 부여하는 모형을 사용하거나, 취약성 평가(vulnerability assessment)에 의해 지표의 계량화를 시도하였다. 그러나 위험을 빈도(frequency)와 강도(severity:손실액 등)의 곱인 기대손실(expected loss)로 정의하여 측정하게 되는데, 수치화된 과거의 손실자료가 대부분 없기 때문에, 이 방법을 적용하기 어렵다. 한편 BS7799에서는 물리적보안, 기술적보안, 관리적보안 차원의 지표를 비교적 포괄적으로 제시하고 있어 기초 지표의 설정에는 좋은 참고가 될 수 있다.

국내의 관련 연구로는 정보보호 지표 계량화에 관한 선행 연구[김종석, 1994; 김정덕과 김기윤,1998]가 있다. 이들은 관련 연구를 참조하여, 기본통제에 관한 항목을 도출하였다. 도출된 지표는 산출지표, 결과지표, 영향지표로 분류되었다. 산출지표는 보안장치의 생산성 및 효율성을 측정하고, 결과지표는 정보자산의 효과성을 측정하며, 1차적 영향지표는 내부업무의 효율성을, 2차적 영향지표는 정보통신인프라의 효과성을 측정한다. 정보 보안 요구가 높은 금융결제원의 점검목록은 환경위험 대책을 보다 강조하고 있다.

기존의 연구에서 도출된 정보보안 지표 항목과 계량화 방식은 대체로 물리적보안, 논리적보안, 관리적보안 등 3가지 관점에서 지표 항목을 분류하고, 단순가중치법을 사용하여 정보보안 수준을 지수화한다. 이와 같은 대표적인 보안 지표 점검목록의 내용을 비교하면 아래 <표 1>과 같다. 이 표는 본 연구의 예비조사 결과로 도출된 예비 지표 항목을 기준으로 기존 연구의 점검 목록을 정열하여 비교한 표이다. 항목의 분류와 항목의 명칭은 각 연구결과마다 상이하므로, 일관되는 명칭이나 기준을 찾기 어렵다. 따라서 본 연구에서는 비교가능성을 높이기 위하여 본연구의 예비조사 결과를 활용하여 분류와 명칭을 설정하였다. 표에서 사용된 보안의 분류는 일반적으로 통용되는 물리적보안, 기술적보안, 관리적보안 등의 구분을 사용한 것이며, 법/제도/표준 항목은 환경 항목으로 별도로 구분하였다. 지표개발을 위한 보안의 분류체계에 대해서는 본 연구의 제 3 장에서 상세하게 논의한다.

계량화에 대해서는 대표적인 접근법이 LLNL (Lawrence Livermore National Laboratory) 체크리스트이다. 이 체크리스트는 13개 부문의 854개 질문으로 구성되어 있으며, '예', '아니오', '해당없음'으로만 표시하게 되어있다. 각 항목에 대한 가중치는 매우높음, 높음, 보통, 낮음, 매우낮음 등 5단계 척도로 중요도의 정도를 주관적으로 부여하였다. 소프트웨어 접근법으로는 BDSS (Bayesian Decision Support System) 등의 정량적 소프트웨어와, CRAMM(CCTA Risk Analysis and Management Methodology), LAVA(Los Alamos Vulnerability/Risk Assessment Method) 등의 정성적 소프트웨어가 있다.

<표 1> 보안 점검항목 비교

대분류	중분류	소분류(항목)	BS 7799	김정덕	금융결제원	이형원	SAFE	보안펀랄	AFIPS	LLNL
물리적 보 안	물리적인 접근통제	물리적 보안 경계(보안구역) 설정	✓			✓	✓	✓	✓	✓
		2선(건물 출입구)에서의 물리적 출입 통제			✓					
		3선(보안구역 출입구)에서의 물리적 출입 통제	✓	✓	✓	✓				
		데이터 센터와 컴퓨터실의 보안	✓		✓	✓				
		깨끗한 책상 정책(퇴근/이석 시 책상위 서류정리정돈 등)	✓							
		문서의 보관/이전/폐기/복사 등에 대한 통제의 적절성	✓		✓					
		통신용 배선의 보호	✓		✓					
		보안구역을 벗어난 정보자산에 대한 보호	✓							
		보안관련 장비의 처분 시 적절한 보호조치 수행	✓							
		관리되지 않는 보안관련 장비에 대한 접근 통제 실시	✓							
		출입 시 인가자 여부 확인	✓	✓	✓	✓				
		방문자 수행(escort) 여부		✓		✓				
	환경위험에 대한 대책	화재,수해,지진 등의 비상사태 대비계획 수립 여부		✓	✓	✓	✓	✓	✓	✓
		비상계획 메뉴얼의 상세함 정도		✓	✓					
		비상사태 대비훈련의 정기적 실시		✓	✓					
		비상계획 유지관리의 적절성		✓	✓					
	업무 계속성 확보 계획	시스템 운용상황의 지속적 감시			✓	✓	✓	✓	✓	✓
		장애의 검출 및 장애부분의 차단과 복구 기능 존재 여부			✓	✓				
기술적 보 안	시스템 접근통제	시스템 접근 통제 정책의 문서화 수준	✓		✓	✓	✓	✓	✓	✓
		시스템 접근 시 사용자 등록 및 해지 절차 존재	✓	✓		✓				
		사용자 접근 권한 부여의 적절성	✓	✓	✓	✓				
		사용자 암호의 적절한 관리 및 주기적 갱신	✓	✓		✓				
	감사추적	시스템 수준의 감사추적 적절성		✓	✓			✓	✓	
		사용자 수준의 감사추적 적절성		✓						
	응용 프로그램 보안	부정 프로그램 감지 대책의 수립 및 실시	✓		✓	✓		✓	✓	✓
		부정 프로그램 방어 대책의 수립 및 실시	✓		✓	✓				
		시스템 유틸리티 사용에 대한 통제	✓	✓						
		프로그램 소스 라이브러리에 대한 접근통제절차의 수립 및 실시	✓	✓						
		보안상 중요한 응용시스템의 격리(접근제한)	✓		✓					
		입력 데이터 검증 여부		✓						
		데이터 암호화 지침 수립	✓	✓	✓	✓				
	데이터 베이스 보안	데이터베이스 접근통제의 적절성		✓		✓	✓			✓
		데이터베이스 복제/갱신 통제의 적절성		✓		✓				
	하드웨어 보안	운영절차 수립과 책임자 권한 명시			✓			✓	✓	
		시스템 관리계획 수립과 검수 실시			✓	✓				
	네트워크 보안	사용자 인증(본인확인 기능)의 적절성	✓	✓	✓	✓	✓	✓	✓	✓
		서비스 제한(사용영역 제한 기능)의 적절성	✓	✓	✓					
		사용자 로그 관리의 적절성		✓						
		데이터와 S/W 전송 시 보안조치 수행의 적절성	✓	✓	✓	✓				
		터미널 보안의 적절성	✓		✓					
	PC 및 바이러스 보안	바이러스 보안 대책 수립 및 실시			✓					
		디스크 등 물리적 저장장치에 대한 보안 통제 실시		✓	✓	✓				

<표 1> 보안 점검항목 비교 (계속)

대분류	중분류	소분류(항목)	BS 7799	김정덕	금융 결제원	이형원	SAFE	보안 편람	AFIPS	LLNL
관리적 보안	보안 조직	보안관리 부서의 독립성 여부	✓	✓						
		보안 교육 및 테스트 실시의 적절성	✓	✓						
		정보 보안 책임의 할당 여부	✓	✓		✓				✓
		보안 시설/장비에 대한 권한 부여 절차 존재 여부	✓	✓		✓				
		보안에 대한 부서간 협조의 적절성	✓							
		사용자 업무 분장의 명확성 정도		✓						
	보안 정책	정보 보안 정책의 문서화 여부		✓						
		정보 보안 정책의 적절성	✓	✓						
	보안 계획	정보 보안 계획 수립 및 내용의 적절성					✓		✓	
	자산 파악	정보자산 목록의 존재 여부 및 적절성	✓	✓		✓				
		정보자산 분류 지침의 적절성(등급별 보안제 실시 등)	✓	✓		✓				
	위험 분석	정보자산에 대한 위험분석 실시의 적절성		✓				✓	✓	
		위험분석 결과에 의한 보안조치 수행의 적절성		✓						
	인사 보안	직무 기술서 상의 보안 역할과 책임 명시	✓	✓						
		채용 시 보안 서약 여부	✓				✓	✓		✓
		보안조치 위반 시 징계절차의 적절성	✓							
	유지 보수 점검	유지보수 시 데이터 백업 관리	✓	✓	✓					
		유지보수에 대한 기록 관리	✓	✓	✓	✓	✓			
		유지보수 시 보안대책 시행	✓							
정보보안 환경	정보보안 법/제도/표준	보안 관련 법/제도/표준/규정의 수량(갯수)		✓				✓		
		보안 관련 법/제도/표준/규정의 내용(충실성)		✓						

이와 같은 기존의 연구는 크게 3가지 관점에서 문제점이 있다. 우선 보안시스템 자체의 완전성을 주 목적으로 보안 지표 항목이 설계되어 있다. 이는 기업이나 국가의 관점에서 보안 시스템을 조직의 목적에 맞게 활용하려 할 때, 정확한 정책방향을 제공하는데 문제가 있다. 즉 목적지향적인 지표항목의 개발이 필요하다. 보안 역량을 정의하고 이를 보다 정확하게 측정하여 조직의 보안 목적을 달성할 수 있도록 지표 설계 시스템을 개발할 필요가 있다.

다음으로 기존의 지표구성은 환경요소의 반영이 미흡하다. 구성원의 마인드(인식), 관련 규정/법/재도 등이 보안시스템의 평가에 중요한 변수가 될 수 있다.

마지막으로 보안은 정보시스템의 발전과 함께 지속적으로 발전되는 분야이다. 기존의 보안 지표 항목은 신기술의 반영이 미흡하다. 예를 들어 방화벽 등 네트워크 보안, PC보안, 바이러스 대책 등과 같은 신규 분야를 지표에 편입시키는 것이 필요하다.

본 연구에서는 이와 같은 기존 지표 구성의 문제점을 인식하고, 최종결과중심의 목적지향적인 지표시스템을 개발하고, 이를 계량화하는 연구를 수행하였다.

목적중심적인 정보보안 지수 설정의 방향을 구체화하기 위해 기존 관련 연구의 진행방향과 연구에 함축된 의미를 분석하였다. 정보화 지수에 관한 연구는 국가의 정보화 수준을 측정하기 위해 수행되어 왔다. 정보화 지표의 접근방법은 크게 나누어 거시경제적 접근방법, 사회경제지표 접근방법, 정보유통량 측정방법 등으로 구분할 수 있다. 또한 거시경제적 접근방법은 산업관련표상의 산업분류를 이용하여 정보부문이 전체산업에서 차지하는 비중으로 정보화의

성숙도를 측정하는 산업구조적 접근방법과, 고용구조상에서 정보노동이 차지하는 비중으로 정보화를 측정하는 취업구조 접근방법이 있다.

정보인프라 지수에 관한 연구는 기업집단 및 개별기업의 정보화 수준을 측정하기 위해 수행되어 왔다. 기업집단의 정보화에 대한 수준 평가는 미시적 차원과 거시적 차원, 기술적 차원과 비즈니스차원, 내부적 차원과 외부적 차원 등 다양한 관점에서 정보시스템을 평가할 수 있고, 평가 목적에 따라 이들 차원의 지표를 적절히 조합하여 사용하게 된다. 미시적 차원은 개별 정보시스템의 성능 및 기능에 관련되는 내용이고, 거시적 차원은 조직 전체의 목표 달성과 관련되는 차원이다. 기술적 차원은 하드웨어, 소프트웨어, 네트워크 등의 기술의 적정성을 포함하여 기술적인 충분성을 평가하는 관점이고, 비즈니스적 차원은 정보통신기술 및 정보시스템이 조직의 핵심 프로세스를 얼마나 잘 지원하는지를 평가하는 관점이다.

미국 등의 선진국에서 가장 많이 사용하는 평가의 관점은 균형점수카드(Balanced Scorecard: BSC) 방법에서 제시하는 4가지 관점이다. BSC 방법에서는 혁신 및 학습관점, 재무적관점, 내부사업 관점, 고객 관점 등 4개의 관점으로 평가의 관점을 제시한다 [Kaplan and Norton, 1996].

우선 혁신 및 학습관점(innovation and learning perspective)에서는 시스템이 조직의 혁신 및 학습 능력을 증진시키는가에 초점을 두고 있다. 재무적 관점(financial perspective)에서는 시스템이 조직의 재무적 목표 달성에 성공적으로 기여하고 있는지를 평가한다. 또한 내부사업관점(internal business perspective)에서는 시스템이 조직의 업무 수행을 얼마나 잘 지원하고 있는지 평가하는 것이며, 고객관점(customer perspective)은 시스템의 내부 및 외부고객이 시스템의 서비스를 어떻게 평가하는지를 측정하는 관점으로서 내외부 고객 만족도로서 이를 측정할 수 있다.

본 연구에서는 이들 관련 연구의 접근법을 참조하여 포괄적인 목적중심적 지표를 개발한다. 지표개발 과정과 결과는 다음과 같다.

Ⅲ. 정보보안 지표 항목 개발

3.1 지표 항목 개발 과정

본 연구에서는 정보보안 수준 계량화 지표를 6단계에 걸쳐 개발하였다. 각 단계별 수행내용은 다음과 같다. 우선 제 1 단계에서는 정보보안의 각 차원과 구성 요소를 파악하였다. 여기에서는 기존의 관련연구를 분석하여 포괄적인 지표 후보를 도출하였다. 2단계에서는 1단계에서 도출된 후보요소에 대해 개념적 정의를 하고, 소분류 항목을 도출하였다. 3단계에서는 전문가면담을 통하여 후보 지표에 대한 파일럿 테스트를 실시하였다. 4단계에서는 각 분야에 종사하는 보안 전문가 100 명을 선정하여, 지표항목의 타당성과 가중치 등에 대한 전문가 의견을 수집하였다. 5 단계에서는 지표항목의 타당성, 중요성, 확율, 심각성 등에 대한 통계 분석을 수행하고, 항목구성의 타당성을 조사하기 위한 요인분석과 상관분석을 실시하였다. 마지막으로 6 단계에서는 바람직한 지표요소 후보항목을 제시하고, 가중치 분석 결과를 제시한다.

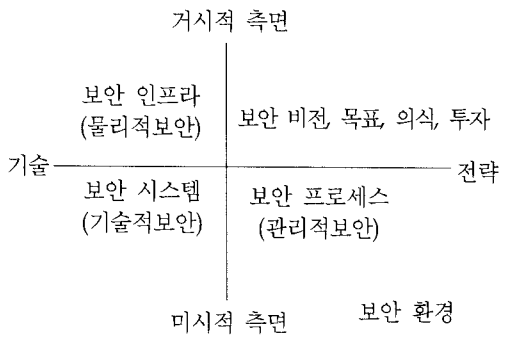
3.2 지표 요소 개발

제 2 장에서 분석한 결과를 토대로 지표 후보 항목을 도출 하였다. 지표 후보항목 도출과정은 다음과 같다.

목적지향적인 정보보안 지표를 도출하기 위해서는 보안의 계층적 구조를 발전시켜 활용할 필요가 있다. 정보보안 지표는 정보보안 요소, 서비스, 역량의 세가지 차원으로 구성된다. 이중 요소(elements)는 정보보안활동과 관련된 제반 기술, 조직, 제도 및 절차, 인식 요인들로 평가의 대상이 된다. 서비스는 정보보안 구성 요

소들이 상호 결합되어 창출하는 다양한 정보보안 서비스를 의미하여, 이러한 서비스들은 상호 결합되어 특정한 정보보안 역량(capabilities)들을 생성해낸다. 정보보안 역량은 정보보안 수준을 나타내는 지표가 된다. 이 개념을 본 연구에서는 계층적인 수준으로 표현하여, 대분류, 중분류, 소분류로 보안 항목을 구분하여 나타낸다.

정보보안의 지표 영역은 보안의 관점을 중심으로 개발할 수 있다. 대표적인 관점으로는 보안구현방법 차원과 보안수준 차원이 있다. 우선 수준 차원으로서 보안은 거시적 수준과 미시적 수준으로 구분할 수 있다. 즉 조직전체 차원의 거시 수준과 개별적인 미시수준으로 구분할 수 있다. 또한 보안구현방법 차원으로서 보안은 기술과 전략으로 나눌 수 있다. 즉 기술로 구현되는 보안과 전략으로 구현되는 보안으로 구분할 수 있다. 이 경우 거시적이고 전략적인 측면에는 조직의 정보보안 비전이나 목표, 조직원의 의식, 투자 등이 해당되고, 미시적이고 전략적인 측면은 개인 및 조직의 정보보안 프로세스가 중심이 된다. 보안환경은 외부적인 차원으로 존재한다. 이러한 차원을 그림으로 도시하면 다음과 같다.



<그림 1> 정보보안 지표 구성 프레임워크

위의 <그림 1>의 지표 프레임워크는 일반적인 보안 분류체계에 대응시킬 수 있다. 즉 보안인프라는 기존 분류의 물리적 보안으로, 보안시스템은 기술적 보안에, 보안프로세스는 관리적 보안으로 대응시킬 수 있다. 그리고 거시적이고 전략적인 측면으로 정보보안 의식/투자/환경을 하나의 영역으로 설정할 수 있다.

기술적 보안에는 식별과 인증 등의 시스템 접근통제, 감사추적 등이 포함되며, 구매, 영업 등의 응용프로그램 보안, 미들웨어 보안, 데이터베이스 보안, 운영체제 보안, 하드웨어 보안 등을 주요 대상으로 선정한다. 이들 요소의 기반은 네트워크이므로 네트워크 보안도 중요한 기술적 요소 항목이 된다.

물리적 보안은 정보시스템에 대한 물리적인 접근통제와 환경위험 및 재난에 대한 대책, 보안 사건 처리 및 업무 계속성 확보 계획, 보안성 평가, 준거성 점검, 보안대책의 관리/유지보수 점검, 시스템 개발 및 유지보수시 보안 설계 등을 포함하고 있으며, 관리적 보안에는 보안조직, 보안정책, 보안계획, 자산파악, 위험분석, 인사보안(직무정의 및 사용자 훈련등) 등이 포함된다.

보안, 암호, 인증 분야 등의 정보보안 산업 관련 통계항목은 최근에 급성장하고 있는 분야이므로 기존의 정보관련 산업 분류 통계로서는 정확히 규모와 데이터의 품질을 평가하기 어려운 문제점이 있다. 따라서 본 연구에서는 이를 향후 연구과제로 남겨둔다.

정보보안 의식은 정보보안의 필요성에 대한 조직원의 의식 수준, 정보의 가치 및 유료화에 대한 의식, 프라이버시의 보안에 대한 개인의 의식 수준 등을 포함한다. 정보보안 법/제도/표준은 정보보안을 위한 공식적인 환경 수준을 나타내는 지표항목으로서 컴퓨터 안전관리지침, 전산업무 보안관리지침 등을 비롯하여 많은 법 및 규칙과 기업의 내규 등에 대한 질적 양적인 수준을 측정하는 항목이 된다.

따라서, 기존 연구결과와 예비조사 결과를 반영하여 본 연구에서는 대분류 항목으로서, 전통적인 보안 요소인 물리적 보안, 기술적 보안, 관리적 보안과 정보보안 의식/투자/환경 등 4가지 범주를 설정하였다. 물리적 보안의 세부요

소로는 물리적인 접근통제, 환경위험에 대한 대책, 업무계속성 확보계획 등이 도출되었고, 기술적 보안 항목은 시스템 접근통제, 감사추적, 응용프로그램보안, 데이터베이스보안, 하드웨어 보안, 네트워크보안, PC 및 바이러스보안 등의 요소가 도출되었다. 관리적 보안 요소에는 보안조직, 보안정책, 보안계획, 자산파악, 위험분석, 인사보안, 유지보수점검 등을 포함하였다.

최근에 들어 강조되고 있는 정보보안 의식, 정보보안 투자수준, 법/제도/규정 등의 정보보안 환경 등은 하나의 대분류 항목으로 설정하여, 전반적인 균형을 이룸으로서 BSC 방법 등의 관련 평가지표의 프레임워크와 호환적인 체계를 유지하였다.

도출된 요소를 중분류 항목으로 설정하고, 중분류 항목 변수의 조작적 정의에 해당하는 단위항목(소분류 항목)을 도출하였다. 전체적인 보안요소 항목을 계층적인 표로 나타내면 <표 2>와 같다.

<표 2> 보안 요소 항목의 계층적 구조

대 분 류	중 분 류	소항목 수
물리적 보안	물리적 접근통제	14
	환경위험에 대한 대책	5
	업무계속성 확보 계획	3
기술적 보안	시스템 접근통제	4
	감사추적	3
	응용 프로그램 보안	7
	데이터베이스 보안	2
	하드웨어 보안	2
	네트워크 보안	6
	PC 및 바이러스 보안	3
관리적 보안	보안 조직	7
	보안 정책	2
	보안 계획	2
	자산 파악	2
	위험 분석	2
	인사 보안	3
	유지보수 점검	3
정보보안 의식/투자/환경	정보보안 의식	3
	정보보안 관련 투자	2
	정보보안 법/제도/표준	2
	보안상태 점검목록 및 수행	4

도출된 후보 항목에 대해 대기업 SI계열사에서 보안업무를 전담하고 있는 전문가들을 대상으로 항목의 타당성과 중요성에 대한 1 차 검증을 실시하였다. 그 결과 정보보안 의식 부분을 강화하여 CEO의 의지 및 마인드, 임원/부서장의 의지 및 마인드, 직원의 의지 및 마인드로 세분하여 측정할 필요가 있는 것으로 조사되었다. 또한 물리적 접근통제에서 1선, 2선, 3선 보안으로 세분하여 조사하여 중요도를 측정할 필요가 있는 것으로 나타났다.

파일럿테스트를 거쳐 완성된 보안 수준 측정지표 후보에 대해 타당성을 체계적으로 검증하기 위한 기준을 설정하였다. 우선 항목 요소로서의 일반적인 타당성을 조사하고, 항목의 상대적인 중요성을 조사하였다. 상대적인 중요성은 소수의 요소로서 보안수준을 측정하려할 경우 유용한 항목 집합을 도출하기 위하여 조사하였다. 그리고 보안항목을 선별하는 가장 보편적인 기준인 위험의 크기를 측정하였다. 즉 위험의 크기는 발생확율과 발생시 사고의 심각성(크기)로 측정할 수 있으므로, 전문가 판단에 의한 각 해당항목의 보안 조치 결여시 보안사고의 발생확율과 사고가 발생할 경우, 해당 사고의 심각성 정도를 조사하였다.

보안지수 계량화를 위해 대항목 및 중항목을 기준으로, 바람직한 가중치 비율에 대해 전문가 견해를 조사하였다. 전문가의 소속집단과 경력년수에 의한 의견 차이를 분석하여 가중치의 타당성을 검증하였다.

3.3 지표 검증 결과

지표 항목의 타당성을 검증하고, 효과적이고 효율적인 보안수준 계량화 지표를 개발하기 위해 통계분석을 수행한 결과는 다음과 같다.

3.3.1 자료수집절차 및 표본의 특성

본 연구의 조사는 정부/공공기관 및 보안/SI 업체, 그리고 금융권의 보안관련 전문가를 대상으로 하였으며, 설문배포는 전화로 통화한후 E-mail

를 통해 이루어졌다. 전체 조사대상 전문가 수는 100명 이었으며, 회수된 설문의 수는 67건으로 설문의 회수률은 67%였다.

응답자는 정부 및 공공기관 소속이 26명, 금융업체가 18명, SI/보안업체가 23명이었으며, 보안관련 경력은 5년 미만이 38명, 5년 이상이 29명이였다.

3.3.2 정보 보안 지표 항목의 종합적 타당성 분석

본 연구에서 제시한 정보보안 지표항목은 크게 물리적 보안요소와 기술적 보안요소 그리고 관리적 보안요소와 정보보안 의식/투자/환경 요소로 구분되며, 구분된 보안 지표에 대해 타당성과 중요성 그리고 발생확률과 심각성을 조사하였다. 사용된 척도는 5점 척도이며, 5점이 가장 높거나 가장 바람직한 수준이고, 1점이 가장 낮거나 가장 바람직하지 않은 수준을 나타낸다. 이들 타당성과 중요성 그리고 발생확률과 심각성에 대한 기초 통계량은 전체평균이 3.78로서, 대부분의 항목에서 보통 이상의 타당성과 중요성, 그리고 발생확률과 심각성을 가지는 것으로 나타났다. 전체적으로 '기술적 보안'과 '정보보안 의식/투자/환경'의 타당성이 상대적으로 높은 것으로 나타났다. 요약표는 <표 3>과 같다.

본 연구에서는 정보보안 지표 항목의 계량화를 위한 보안 지표 항목의 도출을 위해 보안 항목요소로서의 일반적 타당성과 상대적 중요성, 해당항목 결여시 보안사고 발생 확률과 해당항목 결여로 인한 보안사고 발생의 심각성 등 4가지 주요기준과 두가지 복합 기준을 사용하여 요소의 종합적인 타당성을 판단하였다. 즉, 보안 항목요소로서의 타당성과 상대적 중요성을 동시에 고려하였을 경우와, 보안사고 발생확률과 보안조치 결여로 인한 보안사고 발생의 심각성을 동시에 고려하였을 경우에 대한 지표 항목의 바람직한 수준을 중심으로 종합적인 타당성을 판단하였다. 복합기준으로 2가지 기준만을 채택한 이유는 다음과 같다. 우선 확률과 심각성의 곱은 전통적으로 위험의 크기를 측정하는 수치이므로 채택되었으며, 타당성과 중요성의 곱은 바람직함의 정도를 대표하는 수치이므로 채택되었다. 나머지 항목들의 결합은 의미적으로 타당성이 낮으므로 제외하였다.

지표항목의 바람직한 수준은 절대적인 수준과 상대적인 수준을 동시에 사용하였다. 절대적인 수준은 3.0을 기준으로 사용하였다. 분석결과 각 기준에 의한 응답값의 평균이 3.0 이

<표 3> 평가기준별 항목 평균

대분류	구분	전체 평균	타당성 평균	중요성평균	발생확률 평균	심각성 평균
물리적보안	평균	3.73	3.86	3.71	3.59	3.75
	표준편차	0.43	0.44	0.44	0.42	0.46
기술적보안	평균	3.93	4.03	3.93	3.83	3.90
	표준편차	0.29	0.27	0.29	0.30	0.30
관리적보안	평균	3.60	3.75	3.66	3.48	3.50
	표준편차	0.25	0.25	0.23	0.25	0.31
정보보안의식/투자/환경	평균	3.83	4.01	3.91	3.70	3.72
	표준편차	0.29	0.31	0.28	0.28	0.31
전체 평균		3.78	3.91	3.81	3.66	3.73
전체 표준편차		0.34	0.34	0.34	0.34	0.38

<표 4> 물리적 보안 항목 분석

중분류	소분류	타당성	중요성	확률	심각성	타당성×중요성	확률×심각성
물리적인 접근통제	물리적 보안 경계(보안구역) 설정	◎	◎	○	○	◎	○
	1선(정문)에서의 물리적 출입 통제	×	×	×	×	×	×
	2선(건물 출입구)에서의 물리적 출입 통제	×	×	×	×	×	×
	3선(보안구역 출입구)에서의 물리적 출입 통제	◎	◎	◎	◎	◎	◎
	데이터 센터와 컴퓨터실의 보안	◎	◎	◎	◎	◎	◎
	깨끗한책상 정책(퇴근/이석시 책상위 서류정리정돈 등)	×	×	×	×	×	×
	문서의 보관/이전/폐기/복사 등에 대한 통제의 적절성	△	△	△	△	△	△
	정보자산의 이동시 승인	△	△	○	○	△	○
	통신용 배선의 보호	△	△	△	○	△	○
	보안구역을 벗어난 정보자산에 대한 보호	×	×	△	△	×	△
	보안관련 장비의 처분 시 적절한 보호조치 수행	△	△	△	△	△	△
	관리되지 않는 보안관련 장비에 대한 접근 통제 실시	×	×	×	×	×	×
	출입 시 인가자 여부 확인	○	○	◎	○	○	○
	방문자 수행(escort) 여부	△	△	△	△	△	△
환경위험에 대한 대책	화재,수해,지진 등의 비상사태 대비계획 수립 여부	○	○	△	◎	○	○
	비상계획 메뉴얼의 상세함 정도	△	△	×	△	△	△
	비상사태 대비훈련의 정기적 실시	△	△	×	△	△	△
	비상계획 유지관리의 적절성	△	△	×	△	△	×
	테러 및 내부직원의 파괴와 같은 인위적 위협에 대한 대책 수립 여부	△	△	△	○	△	○
업무 계속성 확보 계획	시스템 운용상황의 지속적 감시	◎	◎	○	◎	◎	◎
	장애의 검출 및 장애부분의 차단과 복구 기능 존재 여부	○	○	○	◎	○	○
	보안사건 발생 시 처리절차 수립 여부 및 절차의 적절성	○	○	△	○	○	○

[범례] ◎ : $\mu+\sigma$이상 ○ : $\mu \sim \mu+\sigma$ △ : $\mu-\sigma \sim \mu$ × : $\mu-\sigma$미만

하인 항목은 전혀 나타나지 않았다. 즉 본 연구의 예비조사 결과 항목은 모두 절대적인 기준에서는 보안 지표 항목으로 타당한 것으로 나타났다.

따라서 본 연구에서는 효율적인 지표 구성을 위한 상대적인 타당성 분석에 주력하였다. 항목의 상대적인 타당성 분석을 위해 4 단계의 구분을 사용하였다. 즉, '평균치+표준편차'이상의 항목, '평균치' 이상 '평균치+표준편차'미만의 항목, '평균치-표준편차'이상 '평균치'미만의 항목, '평균치-표준편차'미만의 항목 등 4단계 구분을 사용하였다. 타당성, 중요성, 발생확율, 심각성의크기, '타당성×중요성', '발생확율×심각성의크기'등 6가지 기준으로 분석한 종합적인 항목 분석결과는 다음 <표 4> ~ <표 7>과 같다.

<표 5> 기술적 보안 항목 분석

중분류	소분류	타당성	중요성	확률	심각성	타당성 × 중요성	확률 × 심각성
시스템 접근통제	시스템 접근 통제 정책의 문서화 수준	△	△	△	△	△	△
	시스템 접근 시 사용자 등록 및 해지 절차 존재	○	○	○	◎	○	○
	사용자 접근 권한 부여의 적절성	◎	◎	◎	◎	◎	◎
	사용자 암호의 적절한 관리 및 주기적 갱신	◎	◎	◎	◎	◎	◎
감사추적	시스템 수준의 감사추적 적절성	○	○	○	○	○	○
	응용프로그램 수준의 감사추적 적절성	△	△	△	△	△	△
	사용자 수준의 감사추적 적절성	△	△	△	△	△	△
응용 프로그램 보안	부정 프로그램 감지 대책의 수립 및 실시	△	△	○	○	△	○
	부정 프로그램 방어 대책의 수립 및 실시	△	○	○	○	○	○
	시스템 유틸리티 사용에 대한 통제	△	△	△	△	△	△
	프로그램 소스 라이브러리에 대한 접근 통제 절차의 수립 및 실시	○	○	○	○	○	○
	보안상 중요한 응용시스템의 격리(접근제한)	◎	◎	◎	◎	◎	◎
	입력 데이터 검증 여부	△	△	△	△	△	△
	데이터 암호화 지침 수립	○	○	○	○	○	○
데이터 베이스 보안	데이터베이스 접근통제의 적절성	◎	◎	◎	◎	◎	◎
	데이터베이스 복제/갱신 통제의 적절성	○	◎	◎	◎	○	◎
하드웨어 보안	운영절차 수립과 책임자 권한 명시	○	△	△	△	△	△
	시스템 관리계획 수립과 검수 실시	△	△	△	△	△	△
네트워크 보안	사용자 인증(본인확인 기능)의 적절성	◎	◎	◎	◎	◎	◎
	서비스 제한(사용영역 제한 기능)의 적절성	○	○	○	○	○	◎
	사용자 로그 관리의 적절성	○	○	○	○	○	○
	방화벽 설치 여부 및 방화벽의 성능 수준	◎	◎	◎	◎	◎	◎
	데이터와 S/W 전송 시 보안조치 수행의 적절성	○	○	○	○	○	○
	터미널 보안의 적절성	△	△	△	△	△	△
PC 및 바이러스 보안	PC 보안 대책의 수립	△	○	○	△	△	○
	바이러스 보안 대책 수립 및 실시	○	◎	◎	○	◎	◎
	디스크 등 물리적 저장장치에 대한 보안 통제 실시	△	△	△	△	△	△

[범례] ◎ : $\mu+\sigma$이상 ○ : $\mu \sim \mu+\sigma$ △ : $\mu-\sigma \sim \mu$ × : $\mu-\sigma$미만

<표 6> 관리적 보안 항목 분석

대분류	소분류	타당성	중요성	확률	심각성	타당성×중요성	확률×심각성
보안 조직	보안관리 부서의 독립성 여부	×	×	×	×	×	×
	보안 교육 및 테스트 실시의 적절성	△	△	△	△	△	△
	정보 보안 책임의 할당 여부	△	△	△	△	△	△
	보안 시설/장비에 대한 권한 부여 절차 존재 여부	△	△	△	△	△	△
	보안에 대한 부서간 협조의 적절성	○	○	△	○	○	△
	보안사고에 대응하기 위한 최신 기술 확보	×	×	△	×	×	×
	사용자 업무 분장의 명확성 정도	×	×	△	×	×	×
보안 정책	정보 보안 정책의 문서화 여부	○	△	△	△	△	△
	정보 보안 정책의 적절성	○	△	△	△	○	△
보안 계획	보안계획 수립 및 유지보수의 적절성	△	△	△	△	○	△
	보안계획 내용의 적절성	△	△	△	△	△	△
자산 파악	정보자산 목록의 존재 여부 및 적절성	△	△	△	△	△	△
	정보자산 분류 지침의 적절성(등급별 보안제 실시 등)	△	△	△	△	△	△
위험 분석	정보자산에 대한 위험분석 실시의 적절성	△	△	△	△	△	△
	위험분석 결과에 의한 보안조치 수행의 적절성	△	△	△	△	△	△
인사보안	직무기술서 상의 보안 역할과 책임 명시	△	△	×	×	△	×
	채용 시 보안 서약 여부	×	×	×	×	×	×
	보안조치 위반 시 징계절차의 적절성	×	×	×	×	×	×
유지보수점검	유지보수 시 데이터 백업 관리	◎	◎	◎	◎	◎	◎
	유지보수에 대한 기록 관리	○	△	△	○	△	○
	유지보수 시 보안대책 시행	○	○	○	○	○	○

[범례] ◎ : $\mu+\sigma$이상 ○ : $\mu \sim \mu+\sigma$ △ : $\mu-\sigma \sim \mu$ × : $\mu-\sigma$미만

위 표에서 보는 바와 같이 '타당성×중요성'과 '발생확율×심각성의크기'의 종합적 기준에서 가장 바람직한 지표요소로는 물리적 보안경계설정, 3선에서의 물리적 출입통제, 데이터센터와 컴퓨터실의 보안, 시스템 운영상황의 지속적 감시, 사용자 접근권한 부여의 적절성, 사용자 암호의 적절한 관리 및 주기적 갱신, 보안상 중요한 응용시스템의 격리, 데이터베이스 접근통제의 적절성, 데이터베이스 복제/갱신통제의 적절성, 사용자인증(본인확인기능)의 적절성, 서비스제한(사용영역제한기능)의 적절성, 방화벽 설치여부 및 방화벽의 성능수준, 바이러스 보안대책 수립 및 실시, 유지보수시 데이터 백업 관리, CEO의 정보보안 필요성 인식정도, 임원/부서장의 정보보안필요성 인식정도, 직원의 정보보안 필요성 인식정도, 직원의 정보가치에 대한 인식정도 등이 있는 것으로 나타났다.

상대적으로 지표항목으로서의 적합성이 낮은 지표요소로는 1선에서의 물리적 출입통제, 2선에서의 물리적 출입통제, 깨끗한 책상정책, 보

<표 7> 보안의식/투자/환경 항목 분석

대분류	소분류	타당성	중요성	확률	심각성	타당성 × 중요성	확률 × 심각성
CEO의 의지 및 마인드	정보보안의 필요성 인식 정도	◎	◎	○	○	◎	○
	정보보안 의지 정도	○	○	○	○	○	○
	정보의 가치에 대한 인식 정도	○	○	○	○	○	○
임원/부서장의 의지 및 마인드	정보보안의 필요성 인식 정도	◎	◎	○	○	◎	○
	정보보안 의지 정도	○	○	○	○	○	○
	정보의 가치에 대한 인식 정도	○	○	○	○	○	○
직원의 의지 및 마인드	정보보안의 필요성 인식 정도	◎	◎	◎	◎	◎	◎
	정보보안 의지 정도	○	○	◎	○	○	○
	정보의 가치에 대한 인식 정도	◎	○	◎	○	○	◎
정보보안 관련 투자	매출액 대비 보안 투자액 수준	×	△	△	×	△	△
	1인당 보안 투자액(정보보안 설비 비용 등)수준	×	△	△	×	×	×
정보보안 법/제도/표준	보안 관련 법/제도/표준/규정의 수량(갯수)	×	×	×	×	×	×
	보안 관련 법/제도/표준/규정의 내용(충실성)	○	○	△	△	○	△
보안상태 점검 목록 및 수행	보안 상태의 정기적 점검(체크리스트 이용 등)	○	○	○	○	○	○
	보안 상태의 수시적 점검(우발상황 대처 훈련 등)	○	○	○	○	○	○
	보안 상태 점검 목록 존재 및 갱신의 적절성	△	△	△	△	△	△
	보안 상태 점검 목록 내용의 적절성	△	△	△	△	△	△

[범례] ◎ : $\mu+\sigma$이상 ○ : $\mu \sim \mu+\sigma$ △ : $\mu-\sigma \sim \mu$ × : $\mu-\sigma$미만

안구역을 벗어난 정보자산에 대한 보호, 관리되지 않는 보안관련 장비에 대한 접근통제 실시, 비상계획 유지관리의 적절성, 보안관리부서의 독립성 여부, 보안사고에 대응하기 위한 최신기술 확보, 사용자 업무분장의 명확성 정도, 직무기술서상의 보안 역할과 책임 명시, 채용시 보안 서약 여부, 보안조치 위반시 징계절차의 적절성, 1인당 보안투자액 수준, 보안관련 법/제도/표준/규정의 수량(갯수) 등이 있는 것으로 나타났다. 그러나 이러한 항목들은 상대적인 바람직함의 정도가 낮기는 하지만, 절대적인 관점에서는 평균치가 3.0이 넘는 보통 이상의 항목들이므로, 이들 항목을 포함하여 보안 수준 지표를 구성하는 것이 타당할 경우가 많다.

따라서 이 결과를 활용하여 정보보안 수준 측정을 위해 지표 항목을 선정하는 조직에서는 평가의 목적과 예산을 고려하여 항목을 선별하여 사용할 수 있을 것이다. 즉 가장 바람직한 요소에 포함되는 항목만을 사용하여 간결한 지표 집합을 구성할 수도 있고, 상대적으로 바람직한 정도가 낮은 항목까지 포함하여 포괄적인 지표 항목의 집합을 구성할 수 도 있다.

또한 본 연구에서는 중분류를 중심으로 타당성, 중요성, 발생확율, 심각성의크기, '타당성×중요성', '발생확율×심각성의크기'등 6가지 기준에 대해 분석하였다. 분석 결과는 다음 <표 8>과 같다.

<표 8> 중분류 항목 분석

대항목	중항목	타당성	중요성	확 률	심각성	타당성 × 중요성	확률 × 심각성	Cronbach's Alpha
물리적 보안	물리적 접근통제	△	△	△	△	△	△	.8817
	환경위험에 대한 대책	△	△	△	△	△	△	.6160
	업무계속성 확보 계획	○	○	○	○	○	○	.8281
기술적 보안	시스템 접근통제	○	○	○	○	○	○	.7204
	감사추적	△	△	△	△	△	△	.7713
	응용프로그램 보안	○	○	○	○	○	○	.8361
	데이터베이스 보안	◎	◎	◎	◎	◎	◎	.8683
	하드웨어 보안	△	△	△	△	△	△	.7484
	네트워크 보안	○	○	○	○	○	○	.8308
	PC 및 바이러스 보안	○	○	○	○	○	○	.7621
관리적 보안	보안 조직	△	△	△	△	△	△	.8280
	보안 정책	○	△	△	△	△	△	.8086
	보안 계획	△	△	△	△	△	△	.8524
	자산 파악	△	△	△	△	△	△	.7751
	위험 분석	△	△	△	△	△	△	.8459
	인사 보안	×	×	×	×	×	×	.8804
	유지보수 점검	○	○	○	○	○	○	.7244
정보보안 의식/투자 /환경	CEO의 의지 및 마인드	○	◎	○	○	○	○	.8746
	임원/부서장의 의지 및 마인드	○	○	○	○	○	○	.9108
	직원의 의지 및 마인드	◎	○	◎	◎	◎	◎	.9220
	정보보안 관련 투자	×	△	△	×	×	△	.8943
	정보보안 법/제도/표준	△	△	△	×	△	×	.6008
	보안상태 점검 목록 및 수행	○	△	△	△	○	△	.8996

[범례] ◎ : $\mu+\sigma$이상 ○ : $\mu \sim \mu+\sigma$ △ : $\mu-\sigma \sim \mu$ × : $\mu-\sigma$미만

위 표에서 보는 바와 같이 중항목내의 요소들간의 신뢰도를 분석한 결과 모든 중분류 요소에 대해 크론바하 알파(Cronbach's Alpha) 계수가 0.6이상으로 모두 높게 나타났다.

3.3.3 지표 구조 및 평가기준 분석

본 연구에서는 항목 분류의 구조적 타당성을 검증하기 위해 요인분석을 실시하였다. 그러나 요소들의 수가 적정 수준 이상인 경우에만 요인분석이 적절하게 수행될 수 있기 때문에 본 연구에서는 일부 중분류와 대분류를 중심으로 요인 분석을 수행하였다.

중분류 내의 요소들이 5개 이상인 경우와 모든 대분류 항목에 대해 요인분석을 실시한 결과, 후보 요소들의 응집도가 매우 높은 것으로 나타났다. 요인분석은 타당성, 중요성, 확율, 심

각도 모두에 대해 수행하였으며, 결과는 대동소이하게 나타났다. 논문의 제한된 지면관계로 여기에서는 가장 중심이 되는 기준인 타당성에 대한 요인분석 결과만을 제시한다. 물리적 접근통제에 대한 14개 항목에 대한 요인분석 결과는 다음과 같다. 아이겐 값 1 이상에서 3개의 요인이 추출되었으며, 본 요인분석에서의 KMO 값은 0.826이므로 요인분석의 의미가 크다고 할 수 있다. 또한 구상검정치는 366.617로서 유의도는 0.0000 이다. 따라서 요인분석의 사용이 적합하며, 공통요인이 존재한다고 결론지을 수 있다. 요인의 신뢰도를 나타내는 Cronbach's α 값은 모두 0.7 이상으로서 추출된 요인은 신뢰도가 높다고 할 수 있다.

'환경위험에 대한 대책' 항목의 요인은 단일 요인으로 나타나, 현재 상태가 바람직함을 보여주었다. 기술적보안 중 '응용프로그램 보안'에 대한 요인분석 결과 다음 두가지 요인이 도출되었다. 본 요인분석에서의 KMO 값은 0.767이므로 요인분석의 의미가 크다고 할 수 있다. 또한 구상검정치는 178.141로서 유의도는 0.0000 이다. 요인의 신뢰도를 나타내는 Cronbach's α 값은 모두 0.7 이상으로서 추출된 요인은 신뢰도가 높다고 할 수 있다.

<표 9> 물리적 접근통제에 대한 요인분석

요 인 명	요인내 상세 항목	요인계수	신뢰도계수
접근통제	보안구역을 벗어난 정보자산에 대한 보호	.815	0.8047
	정보자산의 이동시 승인	.768	
	관리되지 않는 보안관련장비에 대한 접근통제 실시	.654	
	보안관련장비 처분시 적절한 보호조치수행	.632	
	방문자 수행(escort)여부	.577	
출입통제	1선(정문)에서의 물리적 출입통제	.791	0.7751
	2선(건물 출입구)에서의 물리적 출입통제	.745	
	3선(보안구역 출입구)에서의 물리적 출입통제	.681	
	데이터센터와 컴퓨터실의 보안	.582	
	통신용 배선의 보호	.490	
기본 통제	문서의 보관/이전/폐기/복사 등에 대한 통제의 적절성	.806	0.7465
	깨끗한 책상정책(퇴근/이석 시 책상위 서류정리정돈 등)	.766	
	물리적 보안경계(보안구역)설정	.620	
	출입시 인가자 여부 확인	.544	

<표 10> 응용프로그램 통제에 대한 요인분석

요 인 명	요인내 상세 항목	요인계수	신뢰도계수
프로그램 일반 통제	입력 데이터 검증 여부	.798	0.7842
	보안상 중요한 응용시스템의 격리(접근제한)	.738	
	프로그램 소스 라이브러리에 대한 접근 통제 절차의 수립 및 실시	.676	
	데이터 암호화 지침 수립	.648	
	시스템 유틸리티 사용에 대한 통제	.642	
부정프로그램 감지/방어	부정 프로그램 감지 대책의 수립 및 실시	.932	0.8949
	부정 프로그램 방어 대책의 수립 및 실시	.897	

<표 11> 정보보안 의식/투자/환경에 대한 요인분석

요 인 명	요인내 상세 항목	요인계수	신뢰도계수
정보보안 의식	임원/부서장의 의지 및 마인드	.928	0.8619
	CEO의 의지 및 마인드	.897	
	직원의 의지 및 마인드	.770	
투자 및 환경	정보보안 법/제도/표준	.855	0.6320
	정보보안 관련 투자	.774	
	보안상태 점검목록 및 수행	.562	

<표 12> 전문가의 소속 및 경력에 의한 차이분석

대분류	소분류	요소의 타당성		요소의 중요성		사고발생 확률		보안사고의 심각성	
		경력차이 Sig.	소속차이 Sig.	경력차이 Sig.	소속차이 Sig.	경력차이 Sig.	소속차이 Sig.	경력차이 Sig.	소속차이 Sig.
물리적 보안	1선(정문)에서의 물리적 출입통제	.148	.093	.110	.112	.015*	.077	.014*	.736
	통신용 배선의 보호	.585	.059	.150	.012*	.783	.016*	.479	.042*
	비상계획 유지관리의 적절성	.409	.040*	.801	.020*	.711	.340	.032*	.104
	테러 및 내부직원의 파괴와 같은 인위적 위협에 대한 대책 수립여부	.198	.636	.661	.760	.049*	.748	.672	.728
	장애의 검출 및 장애부분의 차단과 복구기능 존재 여부	.218	.481	.020*	.561	.166	.780	.295	.794
기술적 보안	부정프로그램 감지 대책 수립 및 실시	.174	.868	.161	.643	.063	.342	.030*	.067
	부정프로그램 방어 대책의 수립 및 실시	.074	.591	.032*	.781	.137	.184	.006*	.304
	시스템 유틸리티 사용에 대한 통제	.035*	.644	.301	.889	.477	.389	.216	.906
	입력데이터 검증여부	.738	.006*	.805	.036*	.899	.238	.684	.060
	PC 보안대책의 수립	.426	.957	.735	.972	.659	.685	.200	.995
	바이러스 보안 대책 수립 및 실시	.213	.316	.650	.417	.138	.176	.030*	.419
	디스크 등 물리적 저장장치에 대한 보안통제실시	.193	.018*	.335	.149	.550	.211	.092	.432
관리적 보안	정보보안 책임의 할당 여부	.018*	.685	.133	.324	.136	.280	.052	.738
	보안시설/장비에 대한 권한 부여 절차 존재여부	.943	.616	.139	.319	.644	.050*	.514	.888
	보안사고에 대한 부서간 협조의 적절성	.619	.190	.192	.364	.882	.032*	.472	.101
	정보보안 정책의 문서화 여부	.101	.162	.021*	.521	.172	.528	.023*	.862
정보보안 의식/투자/환경	정보의 가치에 대한 인식정도	.036*	.802	.035*	.711	.113	.868	.082	.724
	임원/부서장의 정보보안 의지정도	.255	.468	.204	.823	.243	.859	.232	.936
	직원의 정보보안 의지정도	.021	.719	.335	.359	.033*	.804	.104	.786

'네트워크 보안' 항목과 '보안 조직' 항목의 요인은 단일 요인으로 나타나, 현재 상태가 바람직함을 보여주었다.

대분류에 대한 요인분석, 즉 중항목 단위의 요인분석 결과 '정보보안 의식/투자/환경' 범주만이 복수개의 요인을 나타내고 있다. 이 분석에서의 KMO 값은 0.724이므로 요인분석의 의미가 크다고 할 수 있다. 또한 구상검정치는

<표 13> 상관분석표 (계수 0.5 미만 항목)

중 분 류	소 분 류	타당성 확률	타당성 심각성	중요성 확률	중요성 심각성
물리적인 접근통제	물리적 보안 경계(보안구역) 설정	.576	**.453**	.731	.629
	3선(보안구역 출입구)에서의 물리적 출입 통제	.692	**.485**	.649	**.490**
	데이터 센터와 컴퓨터실의 보안	.505	**.404**	.656	**.361**
환경위험에 대한 대책	화재,수해,지진 등의 비상사태 대비계획 수립 여부	**.385**	.504	.652	**.472**
	비상계획 메뉴얼의 상세함 정도	**.483**	.554	.559	.534
	테러 및 내부직원의 파괴와 같은 인위적 위협에 대한 대책 수립 여부	**.440**	**.421**	.710	.605
업무 계속성 확보 계획	시스템 운용상황의 지속적 감시	.536	**.425**	.725	.642
시스템 접근통제	시스템 접근 통제 정책의 문서화 수준	.558	**.458**	.550	.542
	사용자 접근 권한 부여의 적절성	**.456**	**.470**	.569	.714
감사추적	시스템 수준의 감사추적 적절성	.598	**.469**	.613	.568
	응용프로그램 수준의 감사추적 적절성	.569	**.492**	.542	.602
하드웨어 보안	운영절차 수립과 책임자 권한 명시	.621	**.473**	.715	.510
네트워크 보안	데이터와 S/W 전송 시 보안조치 수행의 적절성	.606	**.494**	.710	.614
보안 조직	보안 교육 및 테스트 실시의 적절성	**.467**	**.377**	.650	.516
	정보 보안 책임의 할당 여부	**.367**	**.385**	.686	.623
자산 파악	정보자산 목록의 존재 여부 및 적절성	.552	**.464**	.797	.707
	정보자산 분류 지침의 적절성(등급별 보안제 실시 등)	**.478**	.520	.656	.740
유지보수점검	유지보수에 대한 기록 관리	**.478**	**.440**	.676	.674
CEO의 의지 및 마인드	정보보안의 필요성 인식 정도	**.376**	**.458**	**.491**	**.408**
	정보보안 의지 정도	**.425**	.513	.530	.560
	정보의 가치에 대한 인식 정도	**.467**	**.458**	.601	.647
임원/부서장의 의지 및 마인드	정보보안 의지 정도	**.474**	.574	.574	.608

147.137로서 유의도는 0.0000 이다. 요인의 신뢰도를 나타내는 Cronbach's α 값은 모두 0.6 이상으로서 추출된 요인은 신뢰도가 높다고 할 수 있다.

이상의 요인분석 결과를 통해볼 때, 본 연구에서 설정된 지표의 항목 분류는 상당히 바람직한 것으로 볼 수 있으며, '물리적보안대책'과 '응용프로그램보안'만 하위항목으로 세분할 필요가 있는 것으로 나타났다.

다음으로 각 항목에 대해 전문가 집단별 분석을 수행하였다. 즉 전문가의 소속집단에 따른 견해차이와 경력년수에 따른 견해차이를 분석하였다. 대부분의 항목에 대해 집단별 차이는 나타나지 않았으며, 아래와 같이 '통신용 배선의 보호', '비상계획 유지관리의 적절성', '입력데이터 검증여부', '보안 시설/장비에 대한 권한부여 절차 존재 여부', '보안사고에 대한 부서간 협조의 적절성' 등과 같은 일부 항목에 대해서만 약간의 의견차이를 나타내었다.

본 연구에서 채택된 지표 항목 평가기준간의 상관관계를 분석하였다. 보안사고의 발생확율과 항목 요소로서의 일반적인 타당성, 확율과 상대

적인 중요성, 보안사고의 심각성과 타당성, 심각성과 중요성 등 4가지 주요 관계에 대한 상관 분석 결과는 다음과 같다. <표 13>에서는 피어선 상관계수가 0.5 미만인 항목만을 나타내었다. 이 표에서 보는 바와 같이 타당성과 확율, 타당성과 심각성, 중요성과 확율, 중요성과 심각성은 거의 대부분의 항목에서 높은 상관관계를 보이는 것으로 나타났다. '화재, 수해, 지진 등의 비상사태 대비 계획 수립 여부', '정보보안 책임의 할당 여부', 'CEO의 정보보안 필요성 인식정도' 등 0.5 이하의 상관관계를 가지는 부분은 강조체로 나타내었다.

이러한 상관 분석 결과는 보안 사고의 발생 확율과 사고의 심각성이 주요한 원인이 되어 지표 항목의 타당성과 중요성이 결정된다는 가설을 설정할 수 있게 한다.

타당성이 검증된 지표항목을 이용하여 보안 수준을 계량화하는 방식과 가중치에 대한 분석 결과를 아래에 제시한다.

Ⅳ. 정보보안 수준 계량화

정보보안 수준 계량화는 여러개의 항목을 계층적으로 사용하여 총량 지표화하는 방식으로 수행된다. 따라서 항목간의 가중치 부여 방법에 대해 전문가의 의견을 수집하고 분석하였다.

지표의 총량화 작업은 평가 영역별로 점수를 계산하고 각 영역별로 평가목적에 따라 가중치를 주어 총량지표를 계산하는 작업이다. 평가항목이 많은 경우 항목이 대분류, 중분류, 소분류 등으로 계층화하게 된다. 이 경우 각 분류의 수준에서 평가항목의 중요도에 따라 가중치를 달리 주어 소분류 -> 중분류 -> 대분류 수준으로 합산을 하게 된다. 일반적인 경우, 가중치 부여에 너무 많은 융통성을 가지도록 하는 것은 바람직하지 않기 때문에, 중분류와 대분류 수준에서만 가중치가 조정되도록 한다. 본 연구에서도 대분류와 중분류 수준에서 가중치를 부여하는 방안을 채택하였다.

전문가의 가중치에 대한 판단의 종합 분석 결과와 전문가 집단간의 의견차이 분석 결과는 다음 <표 14>와 같다.

위 표에서 보는 바와 같이 기술적 보안에 대해 31% 정도의 가중치를 주고, 관리적 보안과 정보보안 의식/투자/환경에 대해서는 23% 정도씩의 가중치를 주고, 물리적보안에 대해 22% 내외의 가중치를 주는 것이 바람직한 것으로 나타났다. 물리적 보안 중 '시스템 접근통제'는 10.2%, '환경위험에 대한 대책'은 5.5%, '업무계속성 확보계획'은 6.9% 정도의 가중치가 바람직한 것으로 나타났다. 기술적 보안 중 '시스템 접근통제'는 6.3%, '감사추적'은 3.6%, '응용프로그램 보안'은 3.7%, '데이터베이스보안'은 4.5%, '하드웨어보안'은 3.1%, '네트워크 보안'은 6.8%, 'PC 및 바이러스 보안'은 3.5% 등이 적정한 것으로 나타났다. 관리적 보안 중 '보안조직'은 3.6%, '보안정책'은 4.2%, '보안계획'은 3.4%, '자산파악'은 2.6%, '위험분석'은 4.1%, '인사보안'은 2.7%, '유지보수 점검'은 2.8% 로 나타나 보안정책과 위험분석이 상대적으로 중요한 것으로 분석되었다. 정보보안 의식/투자/환경의 'CEO의 의지 및 마인드'는 6.1%, '임원/부서장의 의지 및 마인드'는 3.7%, '직원의 의지 및 마인드'는 4.3%, '정보보안관련 투자'는 3.9%, '정보보안법/제도/표준'은 2.3%, '보안상태 점검목록 및 수행'은 2.7% 등으로 나타나, 조직원의 의지 및 마인드가 높게 평가되고, 관련 표준의 중요성은 낮게 평가되었다.

전문가 집단의 견해 차이 분석의 경우, 경력 차이에 의한 의견 차이는 '데이터베이스 보안', '보안상태 점검목록 및 수행' 등 소수의 항목에서만 유의한 차이가 나타났고, '물리적 접근통제'와 '위험분석', '보안계획'등 일부항목에 대해서는 전문가의 소속 집단별로 견해 차이가 있는 것으로 나타났다.

<표 14> 대분류 및 중분류별 계량화 가중치

대분류		평균(%)	표준편차	경력집단차이 (2개집단 Sig.)	소속집단차이 (3개 집단 Sig.)
물리적 보안		22.5510	9.7960	.448	.592
	물리적 접근 통제	10.2245	7.6008	.375	.036**
	환경위험에 대한 대책	5.4694	2.6876	.933	.105
	업무계속성 확보 계획	6.8980	3.8689	.864	.064*
기술적 보안		31.3265	8.7664	.859	.634
	시스템 접근 통제	6.2916	3.1383	.262	.995
	감사 추적	3.6080	1.9192	.848	.221
	응용 프로그램 보안	3.6794	1.5847	.066*	.612
	데이터베이스 보안	4.4651	2.0090	.016**	.418
	하드웨어 보안	3.0722	1.7031	.788	.517
	네트워크 보안	6.7508	4.2120	.213	.593
	PC 및 바이러스 보안	3.4600	1.9371	.532	.653
관리적 보안		23.0612	8.0245	.872	.071*
	보안 조직	3.5867	2.2358	.343	.789
	보안 정책	4.2041	2.1721	.826	.374
	보안 계획	3.4286	1.9284	.099*	.022**
	자산 파악	2.6480	1.6249	.375	.198
	위험분석	4.1020	2.2661	.935	.012**
	인사 보안	2.6735	2.0655	.147	.249
	유지보수 점검	2.7551	1.7857	.097*	.356
정보보안 의식/투자/환경		23.0612	10.7924	.506	.834
	CEO의 의지 및 마인드	6.0510	6.2185	.792	.845
	임원/부서장의 의지 및 마인드	3.7245	2.2869	.821	.949
	직원의 의지 및 마인드	4.3367	2.8475	.711	.277
	정보보안 관련 투자	3.9082	3.1634	.140	.153
	정보보안 법/제도/표준	2.3163	1.5602	.968	.471
	보안상태 점검 목록 및 수행	2.7245	1.6958	.025**	.909

*: 유의수준 0.10 **: 유의수준 0.05

V. 토의 및 결론

본 연구는 정보보안 수준을 효과적이고 효율적으로 측정할 수 있는 간편한 지표를 개발하고, 계량화하는 목적으로 수행되었다. 먼저 기존 관련연구 및 지표를 분석하여 문제점을 도출하고 개선 방향을 설정하였다. SI업체 보안담당자 등 관련 전문가들에게 예비조사를 실시하여 개선 방향의 타당성을 검증하고, 그들의 의견을 반영하여 후보 지표항목을 선정하였다.

선정된 후보지표 항목에 대한 타당성 검증을 위해 보안 전문가 집단에게 설문조사를 실시하였다. 요소로서의 일반적인 타당성, 상대적 중요성, 항목 결여시 보안사고 발생확율, 사고의

심각성 등 4가지 기준에 의한 전문가 의견 조사 결과를 분석하여 각 후보 지표 항목에 대한 요소로서의 타당성을 도출하였다.

도출된 결과 대부분의 후보 항목이 바람직한 항목인 것으로 나타났으며, 특히 중요하고 바람직한 항목으로는 3선에서의 물리적 출입통제, 데이터센터와 컴퓨터실의 보안, 시스템 운영상황의 지속적 감시, 사용자 접근권한 부여의 적절성, 사용자 암호의 적절한 관리 및 주기적 갱신, 보안상 중요한 응용시스템의 격리, 데이터베이스 접근통제의 적절성, 사용자인증(본인확인기능)의 적절성, 방화벽 설치여부 및 방화벽의 성능수준, 바이러스 보안대책 수립 및 실시, 유지보수시 데이터 백업 관리, CEO의 정보보안 필요성 인식정도, 임원/부서장의 정보보안필요성 인식정도, 직원의 정보보안 필요성 인식정도, 직원의 정보가치에 대한 인식정도 등이 있는 것으로 나타났다.

또한 요인 분석과 상관 분석을 수행하여 요소간의 관계와 항목평가기준간의 관계를 조사하였다. 그 결과 본 연구에서 설정한 요소 구분이 적절한 것으로 나타났으며, 물리적 접근통제와 같이 소분류 항목이 많은 경우에는 복수개의 요인이 있는 것으로 분석되었다. 4가지 중요한 관계인 타당성과 확율, 타당성과 심각성, 중요성과 확율, 중요성과 심각성의 관계에 대해 각각 분석한 결과 거의 대부분의 항목에서 높은 상관관계를 보이는 것으로 나타났다. CEO의 정보보안 필요성 인식정도 등은 0.5 이하의 비교적 낮은 상관관계를 가지는 것으로 나타났다. 이러한 상관 분석 결과는 보안 사고의 발생확율과 사고의 심각성이 주요한 원인이 되어 지표 항목의 타당성과 중요성이 결정된다는 가설을 설정할 수 있게 한다. 가설 검증은 향후 연구과제로 남겨둔다.

정보보안 수준을 계량화할 때 바람직한 가중치 수준은 기술적 보안에 대해 31% 정도의 가중치를 주고, 관리적 보안과 정보보안 의식/투자/환경에 대해서는 23% 정도씩의 가중치를 주고, 물리적보안에 대해 22% 내외의 가중치를 주는 것이 바람직한 것으로 나타났다. 전문가 집단의 차이 분석에 관해서는 경력 차이에 의한 의견 차이는 데이터베이스 보안, 보안상태 점검목록 및 수행 등 소수의 항목에서만 유의하게 나타났고, 물리적 접근통제와 위험분석, 보안계획등 일부항목에 대해서는 전문가 소속 집단별로 견해 차이가 있는 것으로 나타났다.

본 연구의 기대성과는 다음과 같이 여러가지 측면에서 제시할 수 있다. 우선 정보보안 수준의 개념을 정립하고, 정보보안 수준 측정을 위한 지표 항목을 도출하였다. 또한 정보보안 수준을 계량화할 때 총량화 방법과 가중치 수준에 대한 결과를 도출하였다.

본 연구의 결과는 기업이나 국가에서 정보보안 수준을 계량적으로 측정하고 수준을 파악하고, 조직간 비교분석을 수행할 때 유용하게 활용될 수 있다. 또한 지표 항목의 상대적인 유용함의 수준을 제공함으로써 지표항목집합을 조직의 목적에 맞게 구성할 수 있도록 하였다. 예를 들어, 간편하게 정보보안 수준을 측정하기 위해서는 각 항목 평가기준에서 '평균'이상 또는 '평균+표준편차'이상의 점수를 획득한 항목을 선별적으로 채택하여 조사서로 구성할 수 있으며, 일반적인 보안수준을 측정하기 위해서는 '평균-표준편차'이상을 획득한 항목을 사용할 수 있다.

향후 연구과제로는 본 연구의 결과를 활용하여 국내 기업의 정보보안 수준을 진단하고 문제점을 분석하는 연구가 필요하다. 특히 업종별로 또는 조직의 특성별로 정보보안 수준의 차이가 있는지 분석하고, 보안의 각 부문별로 취약점이 무엇인가를 분석할 필요가 있다. 이러한 결과를 반영하여 보안 수준 지표항목과 계량화 방법을 지속적으로 개선하여 정보보안 수준을 효과적이고 효율적으로 제고하는 시스템을 정착시킬 필요가 있다.

〈참 고 문 헌〉

[1] 권근하, 김치용, 주요지표를 통한 한국과 선진국의 정보화 수준 비교연구, 한국과학기술연구원, 1992. 12

[2] 김기범, 박학수, 이강수, 정보보호 시스템의 품질(보안성) 평가 스킴, *제 1회 소프트웨어 품질관리 심포지움 논문집*, 한국정보처리학회/한국소프트웨어산업협회, 1997. 11, pp. 209-214

[3] 김정덕, 김기윤, 정보보호 지표항목개발 및 계량화 연구, 한국정보보호센터 연구보고서, 1998. 12

[4] 김종석, 정보시스템 취약성 평가:체크리스트 접근방법, 광운대학교 석사학위논문, 1994. 2

[5] 김현수, 정보시스템 진단과 감리, 법영사, 1999. 6

[6] 박태완, *정보시스템 보안감리*, 정보시스템 감리, 한국전산원 교육교재, 1997. 10, pp. 815-837

[7] 이형원 편저, *정보시스템 안전대책*, 영진출판사, 1993

[8] 전성현, 정보기술 영향연구의 개념적 모형, *경영정보학 연구*, 제 6권 제 2호, 1996. 12, pp. 201-220

[9] 정보통신정책연구원, 국가정보화 측정지표 개발에 관한 연구, 1989. 12

[10] CCEB, "Common Criteria for Information Technology Security Evaluation(CC)," Ver. 1.0, Jan. 1996

[11] U.S. Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria(TCSEC)," Dec. 1995

[12] U.S. Department of Defense, "Information Management Performance Measures," Report by a Panel of the National Academy of Public Administration, 1996

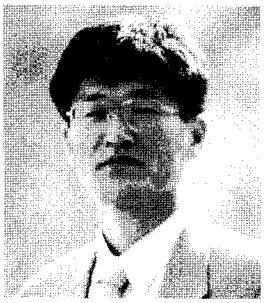
[13] Kaplan, R.S. and Norton, D.P., "Using the Balanced Scorecard as a Strategic Management System," Harvard Business Review, pp. 75-85, Jan. -Feb. 1996

Internet site

http://csrc.ncsl.nist.gov/cc/
http://www.itsec.gov.uk/
http://audit.nca.or.kr/mainstudy03_06.shtml
http://www.gvnfo.state.ut.us/planning/
http://www.itpolicy.gsa.gov/mkm/pathways/
http://www.kisa.or.kr/sysevaluation/menu1/sub2/

◈ 이 논문은 1999년 9월 13일 접수하여 1차 수정을 거쳐 1999년 11월 5일 게재확정되었습니다.

◆ 저자소개 ◆



김현수 (Kim, Hyun-Soo)

서울대 공대에서 학사, 한국과학기술원에서 경영과학으로 석사, 미국 University of Florida에서 경영정보학 박사를 취득한후, 현재 국민대학교 경상대학 정보관리학부 교수로 재직하고 있다. (주)데이콤의 주임연구원, 한국정보문화센터의 정책연구부장으로 재직한바 있으며, 주요관심분야는 정보시스템 진단과 감리, 프로젝트관리 및 소프트웨어공학, 정보시스템계획, 전문가시스템 등이며, Omega, European Journal of Operational Research, Intelligent Systems in Accounting, Finance and Management, 경영정보학연구, 한국경영과학회지, 경영과학, 한국정보처리학회논문지 등의 학술지에 논문을 발표한 바 있다.