정보보안 지표 개발에 관한 탐색적 연구

김 현 수* · 정 해 철**

An Exploratory Study on the development of Information Security Index

Kim, Hyunsoo · Jung, Haechoul

요 약

본 연구는 정보보안 수준을 효과적이고 효율적으로 측정할 수 있는 간편한 지표를 개발하는 목적으로 수행되었다. 기존 관련연구 및 지표를 분석하여 문제점을 도출하고 개선 방향을 설정한 후, 관련 전문가들에게 예비조사를 실시하여 후보지표 항목을 선정하였다.

선정된 후보지표 항목에 대한 타당성 검증을 위해 보안 전문가 집단에게 설문조사를 실시하였다. 요소로서의 타당성, 상대적 중요성, 항목 결여시 보안사고 발생확률, 사고의 심각성 등 4가지 기준에 의한 설문조사 결과를 분석하여 각 후보 지표 항목에 대한 요소로서의 타당성을 도출하였다. 대부분의 후보 항목이 바람직한 항목인 것으로 나타났다. 향후 요인 분석과 상관 분석 등을 추가로 수행하고, 보안 수준을 계량화하는 연구로 발전시킬 필요가 있다.

1. 서론

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. 또한 우리사회에서는 정보보안에 대한 각 부문의 인식이 제고되어 정보보안의 수준을 파악하려는 요구가 증대되고 있다.

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 환경적 측면과 사용자 의식의 측면에서 함께 기반이 갖추어져야 한다.

*: 국민대학교 정보관리학부

**: 국민대학교 정보관리학과 대학원

예를 들어 전자상거래에서의 디지털 서명의 법적 효력, 해커에 대한 법적인 제재, 보안사고 발생시 법적인 책임소재 규명과 손해보상 제도 정착 등에 대해서도 적정한 수준이 무엇인지를 평가할 수 있어야 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 나타낸 수치라고 정의할 수 있다.

정보보안 지표에 대한 연구는 기존 연구 사례가 거의 없으므로 본 연구에서는 정보보안 요소의 분류부터 시작하여 체계 정립을 위한 노력을 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 정보화 지수나 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 선정하여 제시하였다.

2. 정보보안 지표 항목과 수준 연구

정보보안 지표 연구는 직접적인 지표개발 목적으로 수행된 경우는 극소수이고, 정보시스템 감사 등의 목적으로 개발된 체크리스트 개발 연구가 대부분이다. 국내의 관련 연구로는 정보보호 지표 계량화에 관한 선행 연구[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.

기존의 연구에서 도출된 정보보안 지표 항목과 계량화 방식은 대체로 물리적보안, 논리적보안, 관리적보안 등 3가지 관점에서 지표 항목을 분류하고, 단순가중치법을 사용하여 정보보안 수준을 지수화한다. 대표적인 보안 지표 점검목록의 내용과 본 연구의 예비조사 결과를 대비시킨 비교표는 [표 1]과 같다.

이와 같은 기존의 연구는 크게 3가지 관점에서 문제점이 있다. 우선 보안시스템 자체의 완전성을 주 목적으로 보안 지표 항목이 설계되어 있다. 이는 기업이나 국가의 관점에서 보안시스템을 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/제도 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, 바이러스 대책 등과 같은 신규 분야를 지표에 편입시키는 것이 필요하다.

본 연구에서는 이와 같은 기존 지표 구성의 문제점을 인식하고, 최종결과중심의 목적지향적인 지표 시스템을 개발하는 탐색적 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 취업구조접근방법이 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 비즈니스 차원, 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. 지표 개발 과정과 결과는 다음과 같다.

3. 정보보안 지표 항목 개발

3.1 지표 항목 개발 과정

[표 1] 지표항목 비교

대분류	중분류	소분류(항목)	BS 7799	김정덕	금융결제원	이형원	SAFE	보안평가	AFIPS	LLNL
물리적 보 안	물리적인 접근통제	물리적 보안 경계(보안구역) 설정	v			v	v	v	v	v
		2선(건물 출입구)에서의 물리적 출입 통제			v					
		3선(보안구역 출입구)에서의 물리적 출입 통제	v	v	v	v				
		데이터 센터와 컴퓨터실의 보안	v		v	v				
		깨끗한 책상 정책(퇴근/이석 시 책상위 서류정리정돈 등)	v							
		문서의 보관/이전/폐기/복사 등에 대한 통제의 적절성	v		v					
		통신용 배선의 보호	v		v					
		보안구역을 벗어난 정보자산에 대한 보호	v							
		보안관련 장비의 처분 시 적절한 보호조치 수행	v							
		관리되지 않는 보안관련 장비에 대한 접근 통제 실시	v							
		출입 시 인가자 여부 확인	v	v	v	v				
		방문자 수행(escort) 여부		v		v				
	환경위험에 대한 대책	화재,수해,지진 등의 비상사태 대비계획 수립 여부		v	v	v	v	v	v	v
		비상계획 메뉴얼의 상세함 정도		v	v					
		비상사태 대비훈련의 정기적 실시		v	v					
		비상계획 유지관리의 적절성		v	v					
	업무 계속성 확보 계획	시스템 운용상황의 지속적 감시			v	v	v	v	v	v
		장애의 검출 및 장애부분의 차단과 복구 기능 존재 여부			v	v				
기술적 보 안	시스템 접근통제	시스템 접근 통제 정책의 문서화 수준	v		v	v	v	v	v	v
		시스템 접근 시 사용자 등록 및 해지 절차 존재	v	v		v				
		사용자 접근 권한 부여의 적절성	v	v	v	v				
		사용자 암호의 적절한 관리 및 주기적 갱신	v	v		v				
	감사추적	시스템 수준의 감사추적 적절성		v	v			v	v	
		사용자 수준의 감사추적 적절성		v						
	응용 프로그램 보안	부정 프로그램 감지 대책의 수립 및 실시	v		v	v		v	v	v
		부정 프로그램 방어 대책의 수립 및 실시	v		v	v				
		시스템 유틸리티 사용에 대한 통제	v	v						
		프로그램 소스 라이브러리에 대한 접근통제절차의 수립 및 실시	v	v						
		보안상 중요한 응용시스템의 격리(접근제한)	v		v					
		입력 데이터 검증 여부		v						
		데이터 암호화 지침 수립	v	v	v	v				
	데이터베이스 보안	데이터베이스 접근통제의 적절성		v		v	v			v
		데이터베이스 복제/갱신 통제의 적절성		v		v				
	하드웨어 보안	운영절차 수립과 책임자 권한 명시			v			v	v	
		시스템 관리계획 수립과 검수 실시			v	v				
	네트워크 보안	사용자 인증(본인확인 기능)의 적절성	v	v	v	v	v	v	v	v
		서비스 제한(사용영역 제한 기능)의 적절성	v	v	v					
		사용자 로그 관리의 적절성		v						
		데이터와 S/W 전송 시 보안조치 수행의 적절성	v	v	v	v				
		터미널 보안의 적절성	v		v					
	PC 및 바이러스 보안	바이러스 보안 대책 수립 및 실시			v					
		디스크 등 물리적 저장장치에 대한 보안 통제 실시		v	v	v				
관리적 보 안	보안 조직	보안관리 부서의 독립성 여부	v	v						v
		보안 교육 및 테스트 실시의 적절성	v	v						
		정보 보안 책임의 할당 여부	v	v		v				
		보안 시설/장비에 대한 권한 부여 절차 존재 여부	v	v		v				
		보안에 대한 부서간 협조의 적절성	v							
		사용자 업무 분장의 명확성 정도		v						
	보안 정책	정보 보안 정책의 문서화 여부		v						
		정보 보안 정책의 적절성	v	v						
	보안 계획						v		v	
	자산 파악	정보자산 목록의 존재 여부 및 적절성	v	v		v				
		정보자산 분류 지침의 적절성(등급별 보안제 실시 등)	v	v		v				
	위험 분석	정보자산에 대한 위험분석 실시의 적절성		v				v	v	
		위험분석 결과에 의한 보안조치 수행의 적절성		v						
	인사 보안	직무 기술서 상의 보안 역할과 책임 명시	v	v						
		채용 시 보안 서약 여부	v				v	v		v
		보안조치 위반 시 징계절차의 적절성	v							
	유지 보수 점검	유지보수 시 데이터 백업 관리	v	v	v					
		유지보수에 대한 기록 관리	v	v	v	v	v			
		유지보수 시 보안대책 시행	v							
정보보안 환경		보안 관련 법/제도/표준/규정의 수량(갯수)		v				v		

본 연구에서는 정보보안 수준 계량화 지표를 6단계에 걸쳐 개발하였다. 각 단계별 수행내용은 다음과 같다. 우선 제 1단계에서는 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 전문가 면담을 통하여 후보 지표에 대한 파일럿 테스트를 실시하였다. 4단계에서는 각 분야에 종사하는 보안 전문가 100명을 선정하여, 지표항목의 타당성과 가중치 등에 대한 전문가 의견을 수집하였다. 5단계에서는 지표항목의 타당성, 중요성, 확률, 심각성, 가중치 등에 대한 통계 분석을 수행하였다. 마지막으로 6단계에서는 바람직한 지표요소 후보 항목을 제시하였다.

3.2 지표 요소 개발

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

목표지향적인 정보보안 지표를 도출하기 위해서는 보안의 계층적 구조를 발전시켜 활용할 필요가 있다. 정보보안 지표는 정보보안 요소, 서비스, 역량의 세 가지 차원으로 구성된다. 이중 요소(elements)는 정보보안활동과 관련된 제반 기술, 조직, 제도 및 절차, 인식 요인들로 평가의 대상이 된다. 서비스는 정보보안 구성 요소들이 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 크게 거시적 측면과 미시적 측면으로 구분하여 평가 영역을 구분해 볼 수 있다. 이 경우 거시적 측면은 조직의 정보보안 비전이나 목표, 이를 달성하기 위한 전략 등이 해당되고, 미시적 측면에서는 개인 및 조직의 정보보안 업무를 수행하는 프로세스가 중심이 된다.

정보보안 수준을 계량화하기 위해서는 먼저 보안 수준에 영향이 큰 지표 항목을 개발해야 한다. 본 연구에서는 정보보안의 분야와 정보보안의 목적 적합성 관점에서 지표 항목을 도출한다. 우선 정보보안은 크게 나누어 정보보안 기술, 정보보안 의식, 정보보안 제도 및 표준 등의 분야로 나누어 생각할 수 있다.

이 중에서 정보보안 기술은 정보보안의 관리적 요소, 물리적 요소, 기술적 요소를 포함한다. 일반적인 사항으로서 정보보안 관련 법규 및 표준 등과 사용자의 정보보안 의식 수준 분야가 있다.

정보보안 기술의 기술적 요소는 식별과 인증 등의 시스템 접근통제, 감리추적 등이 포함되며, 구매, 영업 등의 응용프로그램 보안, 미들웨어 보안, 데이터베이스 보안, 운영체제 보안, 하드웨어 보안 등을 주요 대상으로 포함한다. 이들 요소의 기반은 네트워크이므로 네트워크 보안도 중요한 기술적 요소 항목이 된다.

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

보안, 암호, 인증 분야 등의 정보보안 산업 관련 통계항목은 최근에 급성장하고 있는 분야이므로 기존의 정보관련 산업 분류 통계로서는 정확히 규모와 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(한국정보산업연합회), 전산업무 보안관리지침(국가안전기획부) 등을 비롯하여 많은 법 및 규칙의 질적 양적인 수준을 측정하는 항목이 된다.

대분류 항목으로서, 전통적인 보안 요소인 물리적 보안, 기술적 보안, 관리적 보안 등 3가지 범주를 설정하였다. 물리적 보안의 세부요소로는 물리적인 접근통제, 환경위험에 대한 대책, 업무계속성 확보계획 등이 도출되었고, 기술적 보안 항목은 시스템 접근통제, 감사추적, 응용프로그램보안, 데이터베이스보안, 하드웨어보안, 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 단위 항목(소분류 항목)을 도출하였다. 전체적인 보안요소 항목을 계층적인 표로 나타내면 [표 2]와 같다.

도출된 후보 항목에 대해 대기업 SI계열사에서 보안업무를 전담하고 있는 전문가들을 대상으로 항목의 타당성과 중요성에 대한 1차 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.

[표 2] 보안 요소 항목의 계층적 구조

대분류	중분류	소항목수
물리적 보안	물리적 접근통제	14
	환경위험에 대한 대책	5
	업무계속성 확보 계획	3
기술적 보안	시스템 접근통제	4
	감사추적	3
	응용 프그램 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

파일럿테스트(pilot test)를 거쳐 완성된 보안수준 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 보안 항목을 선별하는 가장 보편적인 기준인 위험의 크기를 측정하였다. 즉 위험의 크기는 발생확률과 발생시 사고의 심각성(크기)로 측정할 수 있으므로, 전문가 판단에 의한 발생확률과 사고의 심각성 정도를 조사하였다.

또한 전문가의 소속집단과 경력년수에 의한 의견차이도 함께 분석하였다.

3.3 지표 검증 결과

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

3.3.1 자료수집절차 및 표본의 특성

본 연구의 조사 대상은 정부/공공기관 및 일반 보안/SI업체, 그리고 금융권의 보안관련 전문가를 중심으로 하였으며, 설문배포는 전화로 통화한 후 E-mail를 통해 이루어졌다. 전체 배포된 설문의 수는 100건 이였으며, 회수된 설문의 수는 67건으로 설문의 회수률은 67%였다.

응답자 분포는 정부 및 공공기관이 26건, 금융업체가 18건, SI/보안업체가 23건이었으며, 보안관련 경력은 5년 미만이 38건, 5년 이상이 29건이였다.

3.3.2 정보 보안 지표의 타당성 분석

본 연구에서 후보요소로 도출된 물리적 보안요소와 기술적 보안요소 그리고 관리적 보안요소와 정보보안 의식/투자/환경 요소 지표에 대해 타당성과 중요성 그리고 발생확률과 심각성을 조사하였다. 척도는 5점 척도를 사용하였으며,5점이 가장 높거나 가장 바람직한 수준이고, 1점이 가장 낮거나 가장 바람직하지 않은 수준을 나타낸다. 타당성과 중요성 그리고 발생확률과 심각성에 기준에 대한 기초 통계량은 다음의 [표 3]~[표 6]과 같다.

표에서 보는 바와 같이 후보로 선정된 모든 항목에서 평균치가 3.0 이상으로 나타났으며, 대부분의 항목에서 높은 타당성과 중요성, 그리고 발생확률과 심각성을 가지는 것으로 나타났다.

본 연구에서는 정보보안 지표 항목의 도출을 위해 보안 항목요소로서의 일반적 타당성과 상대적 중요성, 해당항목 결여시 보안사고 발생 확률과 해당항목 결여로 인한 보안사고 발생의 심각성 등의 개별 기준과 함께 다음과 같은 2가지 복합기준을 사용하였다. 즉 보안 항목요소로서의 타당성과 상대적 중요성을 동시에 고려하였을 경우와, 보안사고 발생확률과 결여로 인한 보안사고 발생의 심각성을 동시에 고려하였을 경우에 대한 지표 항목의 바람직한 수준을 기준으로 사용하여 분석하였다.

'타당성 × 중요성', '발생확률 × 심각성의 크기'의 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, 항목으로서의 적합성이 낮은 지표요소로는 1선에서의 물리적 출입통제, 2선에서의 물리적 출입통제, 깨끗한 책상정책, 보안구역을 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 위반시징계절차의 적절성, 1인당 보안투자액 수준, 보안관련

법/제도/표준/규정의 수량(갯수) 등이 있는 것으로
나타났다.

[표 3] 물리적보안 지표항목의 평균 비교표

대분류	중분류	소분류(항목)	전체 평균	타당성 평균	중요성평균	발생 확률 평균	심각성 평균
물리적 보 안	물리적인 접근통제	물리적 보안 경계(보안구역) 설정	4.14	4.45	4.15	3.95	4.02
		1선(정문)에서의 물리적 출입통제	3.03	3.16	3.03	2.97	2.97
		2선(건물 출입구)에서의 물리적 출입 통제	3.30	3.45	3.25	3.30	3.19
		3선(보안구역 출입구)에서의 물리적 출입 통제	4.51	4.63	4.48	4.42	4.51
		데이터 센터와 컴퓨터실의 보안	4.74	4.82	4.73	4.63	4.78
		깨끗한 책상 정책(퇴근/여석 시 책상위 서류정리정돈 등)	3.08	3.19	2.99	3.06	3.07
		문서의 보관/이전/폐기/복사 등에 대한 통제의 적절성	3.66	3.78	3.64	3.60	3.63
		정보자산의 이동시 승인	3.75	3.88	3.69	3.69	3.75
		통신용 배선의 보호	3.74	3.82	3.67	3.63	3.82
		보안구역을 벗어난 정보자산에 대한 보호	3.42	3.48	3.37	3.34	3.48
		보안관련 장비의 처분 시 적절한 보호조치 수행	3.56	3.73	3.57	3.43	3.52
		관리되지 않는 보안관련 장비에 대한 접근 통제 실시	3.29	3.33	3.22	3.30	3.31
		출입 시 인가자 여부 확인	4.04	4.12	3.97	4.03	4.04
		방문자 수행(escort) 여부	3.52	3.60	3.48	3.46	3.55
	환경위험에 대한 대책	화재,수해,지진 등의 비상사태 대비계획 수립 여부	3.98	4.10	3.99	3.57	4.24
		비상계획 메뉴얼의 상세함 정도	3.53	3.75	3.64	3.21	3.51
		비상사태 대비훈련의 정기적 실시	3.46	3.60	3.48	3.27	3.48
		비상계획 유지관리의 적절성	3.44	3.64	3.48	3.25	3.40
		테러 및 내부직원의 파괴와 같은 인위적 위협에 대한 대책 수립 여부	3.68	3.76	3.60	3.43	3.94
	업무 계속성 확보 계획	시스템 운용상황의 지속적 감시	4.16	4.27	4.18	3.97	4.23
		장애의 검출 및 장애부분의 차단과 복구 기능 존재 여부	4.05	4.18	4.09	3.82	4.12
		보안사건 발생 시 처리절차 수립 여부 및 절차의 적절성	3.93	4.22	3.96	3.64	3.89
평 균			3.73	3.86	3.71	3.59	3.75
표준편차			0.43	0.44	0.44	0.42	0.46

[표 4] 기술적보안 지표항목의 평균 비교표

대분류	중분류	소분류(항목)	전체 평균	타당성 평균	중요성평균	발생 확률 평균	심각성 평균
기술적 보 안	시스템 접근통제	시스템 접근 통제 정책의 문서화 수준	3.52	3.67	3.66	3.34	3.42
		시스템 접근 시 사용자 등록 및 해지 절차 존재	4.11	4.24	4.12	3.94	4.13
		사용자 접근 권한 부여의 적절성	4.37	4.45	4.37	4.30	4.34
		사용자 암호의 적절한 관리 및 주기적 갱신	4.33	4.45	4.38	4.23	4.27
	감사추적	시스템 수준의 감사추적 적절성	3.84	4.00	3.87	3.72	3.78
		응용프로그램 수준의 감사추적 적절성	3.73	3.87	3.73	3.61	3.69
		사용자 수준의 감사추적 적절성	3.62	3.70	3.64	3.52	3.62
	응용 프로그램 보안	부정 프로그램 감지 대책의 수립 및 실시	3.81	3.86	3.74	3.73	3.89
		부정 프로그램 방어 대책의 수립 및 실시	3.83	3.88	3.83	3.75	3.86
		시스템 유틸리티 사용에 대한 통제	3.71	3.82	3.70	3.63	3.69
		프로그램 소스 라이브러리에 대한 접근통제절차의 수립 및 실시	4.02	4.17	4.06	3.91	3.94
		보안상 중요한 응용시스템의 격리(접근제한)	4.30	4.44	4.29	4.20	4.25
		입력 데이터 검증 여부	3.55	3.64	3.48	3.50	3.58
		데이터 암호화 지침 수립	3.86	3.99	3.82	3.83	3.79
	데이터 베이스 보안	데이터베이스 접근통제의 적절성	4.25	4.27	4.28	4.16	4.27
		데이터베이스 복제/갱신 통제의 적절성	4.17	4.22	4.15	4.12	4.18
	하드웨어 보안	운영절차 수립과 책임자 권한 명시	3.73	3.94	3.75	3.54	3.70
		시스템 관리계획 수립과 검수 실시	3.58	3.76	3.63	3.40	3.52
	네트워크 보안	사용자 인증(본인확인 기능)의 적절성	4.30	4.36	4.33	4.21	4.31
		서비스 제한(사용영역 제한 기능)의 적절성	4.08	4.18	4.04	3.99	4.10
		사용자 로그 관리의 적절성	3.86	4.00	3.96	3.70	3.78
		방화벽 설치 여부 및 방화벽의 성능 수준	4.44	4.46	4.39	4.42	4.48
		데이터와 S/W 전송 시 보안조치 수행의 적절성	3.92	3.99	3.91	3.79	3.97
		터미널 보안의 적절성	3.58	3.66	3.58	3.57	3.51
	PC 및 바이러스 보안	PC 보안 대책의 수립	3.77	3.84	3.81	3.72	3.69
		바이러스 보안 대책 수립 및 실시	4.13	4.22	4.19	4.04	4.06
		디스크 등 물리적 저장장치에 대한 보안 통제 실시	3.58	3.69	3.51	3.52	3.60
평 균			3.93	4.03	3.93	3.83	3.90
표준편차			0.29	0.27	0.29	0.30	0.30

[표 5] 관리적보안 지표항목의 평균 비교표

대분류	중분류	소분류(항목)	전체 평균	타당성 평균	중요성평균	발생 확률 평균	심각성 평균
관리적 보 안	보안 조직	보안관리 부서의 독립성 여부	3.28	3.52	3.37	3.13	3.1
		보안 교육 및 테스트 실시의 적절성	3.59	3.67	3.67	3.48	3.52
		정보 보안 책임의 할당 여부	3.56	3.58	3.64	3.53	3.5
		보안 시설/장비에 대한 권한 부여 절차 존재 여부	3.53	3.61	3.6	3.43	3.48
		보안에 대한 부서간 협조의 적절성	3.83	4.03	3.93	3.63	3.73
		보안사고에 대응하기 위한 최신 기술 확보	3.37	3.51	3.45	3.33	3.19
		사용자 업무 분장의 명확성 정도	3.40	3.46	3.46	3.33	3.33
	보안 정책	정보 보안 정책의 문서화 여부	3.59	3.91	3.7	3.37	3.39
		정보 보안 정책의 적절성	3.69	3.93	3.79	3.51	3.54
	보안 계획	보안계획 수립 및 유지보수의 적절성	3.69	3.85	3.7	3.61	3.58
		보안계획 내용의 적절성	3.60	3.73	3.59	3.56	3.52
	자산 파악	정보자산 목록의 존재 여부 및 적절성	3.54	3.7	3.62	3.44	3.38
		정보자산 분류 지침의 적절성(등급별 보안제 실시 등)	3.61	3.81	3.66	3.49	3.46
	위험 분석	정보자산에 대한 위험분석 실시의 적절성	3.54	3.75	3.58	3.42	3.39
		위험분석 결과에 의한 보안조치 수행의 적절성	3.66	3.84	3.72	3.55	3.52
	인사 보안	직무 기술서 상의 보안 역할과 책임 명시	3.42	3.6	3.48	3.3	3.3
		채용 시 보안 서약 여부	3.23	3.33	3.36	3.07	3.15
		보안조치 위반 시 징계절차의 적절성	3.35	3.55	3.43	3.25	3.18
	유지 보수 점검	유지보수 시 데이터 백업 관리	4.42	4.45	4.39	4.3	4.52
		유지보수에 대한 기록 관리	3.78	3.91	3.76	3.64	3.82
		유지보수 시 보안대책 시행	3.85	3.94	3.87	3.79	3.81
평 균			3.60	3.75	3.66	3.48	3.50
표준편차			0.25	0.25	0.23	0.25	0.31

[표 6] 정보보안 의식/투자/환경 보안 지표항목의 평균 비교표

대분류	중분류	소분류(항목)	전체 평균	타당성 평균	중요성평균	발생 확률 평균	심각성 평균
정보 보안 의식 / 투자 / 환경	CEO의 의지 및 마인드	정보보안의 필요성 인식 정도	4.08	4.28	4.18	3.9	3.96
		정보보안 의지 정도	3.95	4.18	4.12	3.75	3.76
		정보의 가치에 대한 인식 정도	3.94	4.19	4.13	3.67	3.75
	임원/부서장의 의지 및 마인드	정보보안의 필요성 인식 정도	4.03	4.31	4.15	3.81	3.85
		정보보안 의지 정도	3.94	4.16	4.07	3.76	3.76
		정보의 가치에 대한 인식 정도	3.98	4.16	4.06	3.85	3.85
	직원의 의지 및 마인드	정보보안의 필요성 인식 정도	4.25	4.37	4.21	4.16	4.24
		정보보안 의지 정도	4.08	4.18	4.07	4.01	4.06
		정보의 가치에 대한 인식 정도	4.11	4.26	4.09	4.05	4.05
	정보보안 관련 투자	매출액 대비 보안 투자액 수준	3.45	3.55	3.52	3.39	3.33
		1인당 보안 투자액(정보보안 설비 비용 등)수준	3.41	3.5	3.48	3.34	3.3
	정보보안 법/제도/표준	보안 관련 법/제도/표준/규정의 수량(갯수)	3.22	3.36	3.27	3.13	3.1
		보안 관련 법/제도/표준/규정의 내용(충실성)	3.72	3.97	3.84	3.52	3.55
	보안상태 점검목록 및 수행	보안 상태의 정기적 점검(체크리스트 이용 등)	3.99	4.17	4	3.89	3.91
		보안 상태의 수시적 점검(우발상황 대처 훈련 등)	3.82	3.97	3.82	3.7	3.8
		보안 상태 점검 목록 존재 및 갱신의 적절성	3.61	3.77	3.7	3.47	3.48
		보안 상태 점검 목록 내용의 적절성	3.59	3.8	3.68	3.45	3.42
평 균			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

그러나 이러한 항목들은 상대적인 바람직한 정도가 낮기는 하지만, 절대적인 관점에서는 평균치가 3.0이 넘는 보통 이상의 항목들이므로, 이들 항목을 포함하여 보안 수준 지표를 구성하는 것이 타당할 경우가 많다.

다음으로 각 항목에 대해 전문가 집단별 분석을 수행하였다. 즉 전문가의 소속집단에 따른 견해 차이와 경력년수에 따른 견해차이를 분석하였다. 대부분의 항목에 대해 집단별 차이는 나타나지 않았으며, 아래의 [표 7]과 같은 일부 항목에 대해서만 약간의 의견차이를 나타내었다.

따라서 이 결과를 활용하여 정보보안 수준 측정을 위해 지표 항목을 선정하는 조직에서는 평가의 목적과 예산을 고려하여 항목을 선별하여 사용할

[표 7] 전문가의 소속 및 경력에 의한 견해차이

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
기술적보안	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
관리적보안	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

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 수도 있다.

4. 토의 및 결론

본 연구는 정보보안 수준을 효과적이고 효율적으로 측정할 수 있는 간편한 지표를 개발하는 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 타당성, 상대적 중요성, 항목 결여시 보안사고 발생확율, 사고의 심각성 등 4가지 기준에 의한 설문조사 결과를 분석하여 각 후보 지표 항목에 대한 요소로서의 타당성을 도출하였다.

도출된 결과 대부분의 후보 항목이 바람직한 항목인 것으로 나타났으며, 물리적 보안경계설정, 3선에서의 물리적 출입통제, CEO의 정보보안 필요성 인식정도, 임원/부서장의 정보보안필요성 인식정도, 직원의 정보가치에 대한 인식정도 등을 비롯한 다수의 요소가 특히 중요하고 바람직한 항목으로 나타났다.

본 연구는 요인 분석과 상관 분석 등을 수행하여 요소간의 관계와 항목평가기준간의 관계를 조사하여 보완할 필요가 있다. 또한 정보보안 수준을 계량화하기 위한 바람직한 가중치 수준을 도출하여 수치화된 보안수준을 제시할 수 있도록 발전시킬 필요가 있다.

이렇게 하여 계량화된 지표가 완성되면, 정부 및 공공기관과 대표적인 민간기관을 중심으로 각 조직의 정보보안 수준을 조사하여, 전체적으로 우리나라의 정보보안 수준을 진단하고, 문제점과 개선방안을 제시할 필요가 있다.

참 고 문 헌

[1] 김기범, 박학수, 이강수, 정보보호 시스템의 품질(보안성) 평가 스킴, *제 1 회 소프트웨어 품질관리 심포지움 논문집*, 한국정보처리학회/한국소프트웨어산업협회, 1997.11, pp. 209-214

[2] 김정덕, 김기윤, 정보보호 지표항목개발 및 계량화 연구, 한국정보보호센터 연구보고서, 1998.12

[3] 김종석, 정보시스템 취약성 평가:체크리스트 접근방법, 광운대학교 석사학위논문, 1994.2

[4] 김현수, 정보시스템 진단과 감리, 법영사, 1999.6

[5] European Communication, "Information Security Evaluation Criteria(ITSEC)", Ver1.2, June. 1991

[6] Information Technology Security Evaluation Manual(ITSEM), Commission of the European Communities, 1993

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

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

[9] 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://audit.nca.or.kr/mainstudy03_06.shtml

http://www.itpolicy.gsa.gov/mkm/pathways/

http://www.kisa.or.kr/sysevaluation/menu1/sub2/itsem.html

http://www.itsec.gov.uk/info/about.htm

http://csrc.ncsl.nist.gov/cc/info/projsum.htm