

국가정보보호수준 평가지표 개선 및 지수 산출에 관한 연구*

임규건** · 배순한*** · 이대철**** · 지상호***** · 백승익*****

A Development of a Framework for the Measuring National Information Security Level*

Gyoo Gun Lim** · Soon han Bae*** · Dae Chul Lee****
지상호 영문명***** · Seung Ik Baek*****

■ Abstract ■

In this study, we developed a comprehensive model to measure the National Information Security Level based on PRM framework. The proposed model reflected a rapidly changing technology environments such as social network service, mobile devices, and etc. This new model consists of three layers : Infrastructure Layer, the Action Layer and the Performance Layer, and there are 16 sub-indexes under the 3 layers.

To develop new model and sub-indexes for measuring the National Information Security Level, much amounts of documents related to security indexes or deliberation criteria and security guidelines from international organization were reviewed and then most probable index pool were composed. The Index pool were verified by expert group consisting of professors and specialists. Through five times of screening and having an evaluation review, 16 sub-indexes were deduced and then Delphi and AHP have been conducted to obtain validity and objectiveness of the indexes. Thus the new proposed national information security index will show more exact national information security level and we expect that the indexes give much implications for establishing information protection policy

Keyword : Information Protection, Security, NISI(National Information Security Indicators),
Informatization Index, Performance Evaluation

논문투고일 : 2013년 04월 29일 논문수정완료일 : 2013년 12월 10일 논문게재확정일 : 2013년 12월 16일

* 본 연구의 데이터와 결과를 논문화하는데 협조해 준 한국인터넷진흥원 지상호 박사께 감사드린다.

** 한양대학교 경영대학 교수

*** ㈜Opentide Korea 컨설턴트

**** ㈜창의컨설팅 ICT전략경영그룹 그룹장

***** 한국인터넷진흥원 정보보호관리 팀장

***** 한양대학교 경영대학 교수, 교신저자

1. 서 론

초고속 인터넷과 이동통신의 보급을 통해 우리나라는 정보화 수준에 있어 최상위 국가로 인정받고 있다. 정보화와 관련된 여러 국내·외 지수들이 이를 증명하고 있다(<표 1> 참조). 특히 이들 지수에서 우리나라는 정보 인프라와 인터넷 이용률 측면에서 가장 우수한 나라로 평가 받고 있으며, 이를 반증하듯 현재 우리 생활 깊숙이 초고속네트워크 망이 설치되어 있어, RFID, 스마트카드, 스마트폰과 같은 새로운 기술과 서비스를 일상 생활에서 용이하게 이용할 수 있게 되었다.

이와 같이 정보화의 진전으로 인해 기업과 개인은 고도로 정비된 IT 인프라 환경에 적응하고 다양한 정보 기기들을 이용하고 있다. 특히 우리나라의 인터넷 이용자수는 [그림 1]과 같이 2003년에 2,922만 명에서 2013년 약 4,008만 명으로 약 1,000만 명 가량 증가하였으며 이용율은 65.5%에서 82.1%

로 증가하였다[12].

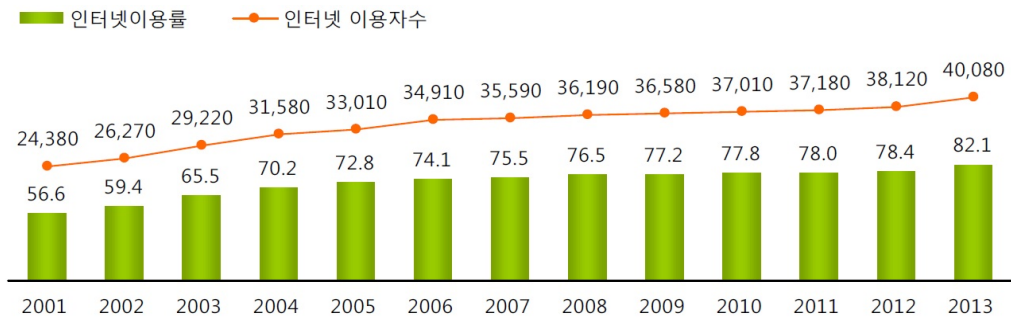
최근에는 무선 인터넷을 기반으로 스마트폰, 테블릿 PC, 넷북 등 다양한 제품 및 서비스가 폭발적으로 증가 하였으며 사회전반에 걸쳐 정보의 검색과 공유가 그 어느 때 보다 자유로워 졌다. 그러나 이 같은 정보화 수준의 외형적 성장과는 달리 현재의 IT 환경은 결코 안전한 것만은 아니다. 개인정보유출, 프라이버시 문제 등 다양한 정보화의 역기능 현상들이 사회 문제화 되고 있다.

실제로 2012년 해킹사고 신고건수는 총 19,570건으로 전년도(11,690건) 대비 67.4%나 증가하였고, 2011년 개인정보 침해신고 상담건수는 총 166,801건으로 2011년 대비 26.7%나 증가한 것으로 나타났다[32]. 2009년 DDos 공격으로 국내 11만대 이상의 PC가 악성코드에 감염되고 PC 손상 피해접수는 총 1,353건에 이르기기도 하였다[13]. 이와 같이 정보보호 관련 피해사례 및 피해액은 지속적으로 증가하는 추세이며 관계 기관을 중심으로 정보보

<표 1> 국제정보화 지수별 우리나라 순위

지수명 (작성기관)	우리나라 순위(조사대상 국가 수)										
	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
전자정부발전지수 (UN)	15 (190)	13 (191)	5 (191)	5 (191)	-	-	6 (192)	-	1 (192)	-	1 (193)
온라인참여지수 (UN)	-	12 (191)	6 (191)	4 (191)	-	-	2 (192)	-	1 (192)	-	1 (193)
ICT 발전지수 (ITU)	-	-	-	-	-	-	-	2 (159)	1 (159)	1 (152)	-
네트워크 준비지수 (WEF)	20 (75)	14 (82)	20 (102)	24 (104)	41 (115)	19 (122)	9 (127)	11 (134)	15 (133)	10 (138)	12 (142)
국가경쟁력지수 (기술준비도 부분) (WEF)	19 (80)	11 (102)	18 (104)	11 (117)	12 (125)	7 (131)	13 (131)	15 (133)	19 (139)	-	-
국가경쟁력지수 (기술인프라 부분) (MD)	17 (49)	24 (51)	8 (51)	2 (51)	6 (53)	6 (55)	14 (55)	14 (57)	18 (58)	14 (59)	-
디지털경제지수 (구 e-비즈니스 준비도) (BU)	21 (60)	16 (60)	14 (64)	18 (65)	18 (68)	16 (69)	15 (70)	19 (70)	13 (70)	-	-
IT산업 경쟁력 지수(BU)	-	-	-	-	-	3 (64)	8 (66)	16 (66)	-	19 (66)	-

출처 : 한국정보화진흥원(2012), '2012 국가정보화백서'[16, 22, 31],



출처 : 미래창조과학부 · 한국인터넷진흥원, '2013년 인터넷이용실태조사[12].

[그림 1] 인터넷 이용자수와 이용률

호 관련 법령 제정 및 정책 수립노력이 수행 되고 있다. 예를 들어 방송통신위원회는 2008년 6월 '주민등록번호 외 회원 가입방법의 제공'을 의무화하는 '정보통신망법' 개정을 통해 i-PIN 활성화를 위한 법적 기반을 마련하여 개인정보 유출방지에 노력하고 있으며, 적절한 정보보호 정책 수립 및 현재 정보보호 수준을 확인하기 위한 다양한 정보보호 체계 및 평가 지표들이 개발되었다. 주로 정부 주도로 개발된 관리체계 및 평가지표로 국가정보원(NIS)/방송통신위원회/한국인터넷진흥원(KISA)의 '국가정보보호지수', 국가정보원(NIS)의 '정보보안 관리수준 평가', 행정안전부의 '전자정부서비스 보안수준 실태조사'와 '공공기관 개인 정보보호 수준진단' 등이 있다. 이와 같이 다양한 기관에서 수행된 정보보호 수준의 평가 체계 개발 노력은 사회 전반의 정보침해 위협이 가중되고, 정보보호와 관리의 중요성이 재고되는 시점에서 의미있는 노력이며, 정보보호 정책을 효과적으로 추진하기 위해 반드시 선행되어야 하는 것이다.

그러나 지금까지의 국가정보보호 수준을 측정하고자 하는 연구는 대체로 다음과 같은 한계점을 지니고 있다. 첫째 기술적 접근 중심이며, 정보보호와 관련하여 관리적 요인과 환경적 요인에 대한 연구가 매우 부족했다. 둘째 공공기관이나 일반 기업 등 특정 분야에만 적용할 수 있도록 개발되어 다른 분야에 적용하기 어려워, 국가 전체의 정보보호 수준을 대표하기 어렵었다. 셋째 평가 체

계 및 지표들은 서로간의 지표 항목이 유사하여 동일한 평가 분야의 중복이 발생하고, 유사한 인증 제도가 운영됨으로써 그 실효성이 저하되는 문제가 발생한다. 마지막으로 측정 항목이 지속적으로 개선되지 않는 문제가 있는데, 최근에 개발된 지표가 아니라면 최근 정보보호 이슈에 대한 점검과 평가 항목이 없는 경우가 있다. 이러한 문제로 인해 지속적으로 발생하는 보안 이슈를 파악하고 평가하여 그 결과를 정책에 반영할 수 없게 된다.

따라서 본 연구는 이와 같은 기존의 정보보호 연구들의 한계점을 개선하고, 국가정보보호 수준을 평가하기 위한 방법론으로 계량적인 국가정보보호 지수 모델을 제시하고자 한다. 근래 급변하는 ICT 환경에 따라 국가 정보보호의 체계적이고 효과적인 관리를 위해 기존 국가 정보보호지수 모델의 보완과 개선의 필요성이 부각되고 있는 실정이다. 이에 본 연구에서는 정보보호 기술, 환경의 인프라 요인뿐만 아니라 관리측면에서 정보보호의 효과를 인과적으로 제시할 수 있는 프레임워크(framework)를 개발하여 최근의 정보보호 환경을 반영하는 새로운 국가 정보보호지수 모델을 제시하고 그 지수를 산출하고자 한다. 그리고, 도출된 모델을 바탕으로 실제 2007~2009년의 실제 데이터에 적용해 보고자 한다. 본 연구의 구체적인 목적은 다음과 같다.

첫째, 최근의 IT 환경을 고려하고, 원인과 대응의 인과적 관계와 관리적 측면이 제시되는 국가

정보보호지수 모델을 제시하고자 한다.

둘째, 국내외 다양한 정보보호 관련 문헌 고찰을 통해 정보보호 평가 지표 Pool을 구성하고, 전문가들의 타당성 검증을 통한 객관적인 지표 체계를 수립하고자 한다.

셋째, 개선된 지표 체계를 통해 정량적인 현재 국가정보보호지수를 산출하고, 향후 국가정보보호지수 모델의 활용 방안을 제시하고자 한다.

본 논문의 구성은 제 2장에서 국가정보보호 지표 및 지수의 개념을 살펴보고, 제 3장에서 국내외 정보보호 수준 평가에 관한 기존연구들을 살펴보고 기존 정보보호평가 모델의 한계 및 시사점을 도출한다. 제 4장에서 국가정보보호 측정지표를 개발하고 제 5장에서 결론과 향후 연구의 방향을 제시한다.

2. 국가정보보호 지표 및 지수의 개념

2.1 지표(Indicator)와 지수(Index)

지표란 일정한 방향이나 목표를 가지고 어떤 현상이나 사물을 측정할 수 있게 해주는 수단으로 목표의 달성 정도를 측정하기 위한 기준 혹은 척도의 역할을 한다. 즉 지표(indicator)란 우리의 가치와 목표에 비추어 우리가 어디에 있고, 어디로 가고 있는가를 판단할 수 있는 통계, 통계 계열 및 그 외의 모든 형태의 증거로 우리가 바라는 욕구 수준에 비교한 현재 상태의 반영이라고 할 수 있다[10]. 이와 관련하여 Land[27]는 변화를 측정하는데 도움을 주는 변수를 지표라고 설명하면서 시스템의 조건과 변화에 대해 판단을 제공하는 규범적 통계라고 설명하고 있다. 따라서 지표는 추상적인 현상이나 개념을 일정한 속성을 가진 변수로 변환 하고 측정 가능하게 구체화 하는 기준이나 척도(측정항목)의 역할을 하며 지표가 특정 개념의 상태와 변화를 타당하게 구체화하고 신뢰성을 확보하기 위해서는 올바른 평가와 검증을 거쳐야 할 것이다. 일반적으로 지수와 지표는 혼용되어

사용하는 경우가 많다. 그러나 지표(indicator)는 앞에서 언급한바와 같이 변화를 측정하는데 도움을 주는 변수라 할 수 있으며 반면에 지수(index)는 다양한 지표들을 종합하여 산출된 단일한 값이다[18]. 통상적으로 지수(index)란 어떠한 사회적 현상을 계량적, 수치적으로 표현하는 방법을 일컫는 것으로 특정한 사회현상에 계량적인 의미를 부여하고 설명하기 위하여, 또는 국가 간, 지역 간, 조직 간 등의 비교를 위하여, 또는 정책적인 의미를 도출하기 위하여 만들어진다. 국가 정보보호 수준 측정사례를 보여준다.

2.2 국가 정보보호 지표와 지수의 개념

특정한 사회 현상과 그 영향력을 설명하고 향후 그 변화를 예측하기 위해서는, 먼저 그 현상에 대한 현재 수준을 계량화하는 것이 가장 바람직한 방법일 것이다. 즉 사회 현상을 대표하는 측정 가능한 지표(indicator)를 구성하고 이를 통해 현재 수준의 단일한 값인 지수(index)를 도출 하는 것이 정책 결정 등과 같은 의사결정 수립에 시사점을 줄 수 있을 것이다. 따라서 국가정보보호 지표의 구성과 지수의 산출은 현재의 정보보호 수준 측정과 더불어 향후 정책수립에 앞서 선행되어야 하는 것이다. 그러나 현재까지 국가정보보호 수준에 대한 평가와 측정에 관련된 연구에서 만족할 만한 연구 결과를 찾기는 어렵다. 국가정보보호의 수준을 측정하는 것이 어려운 이유는 정보보호의 영역이 계속 확장됨에 따라 개념 자체를 정의하기가 어렵기 때문이다. 정보보호의 개념은 여러 가지의 형태로 정의되어 있는데, 국내의 정보화 촉진법 제2조의 정의를 살펴보면, ‘정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강구하는 것’으로 명시되어 있고, 미국 및 영국을 중심으로 하는 유럽에서 통용되는 정의를 살펴보면, ‘전자적인 형태의 정보를 처리, 저장 및 통신의 모든 단계에서 고의적 혹은 실수에 의한 불법적인 공개, 변조, 파괴 및 지체로부터 보호하는 것’으로

정의한다. 한편 일본에서는 ‘정보와 정보시스템의 안전성을 말하는 것으로 이용자가 정보나 정보시스템을 안심하고 사용하는 상황’을 지칭한다[15]. 이와 같이 정보보호의 정의는 정보통신망을 통해 발생하는 문제를 해결하는 정보통신 네트워크 및 시스템에 국한한 협의의 개념에서 이루어졌다. 즉 “데이터 및 시스템을 고의적 혹은 실수에 의해 불법적인 공개, 변조, 파괴 및 지체로부터의 보호”를 위하여 신뢰성, 무결성, 가용성을 포함한 안정성이 보장하고, 모든 정보대상을 보호하도록 규정하고 있다[14]. 그러나 점차 그 범위가 확대되어 하드웨어 또는 소프트웨어를 포함한 시스템과 데이터, 네트워크 등에 국한하지 않고 사이버공간에서 침해되어지는 프라이버시, 지적재산권, 저작권 등 보호범위가 확대되었다. 또한 사이버공간이 새로운 ‘법행 장소’로 이용되면서 정보통신기술이나 컴퓨터프로그램을 이용한 전산망 침해행위, 컴퓨터에 저장된 정보의 절도, 부정조작 및 부정사용, 암호해독, 컴퓨터 바이러스의 배포, 음란물의 유통이나 국가의 군사기밀, 비밀무기를 통제하는 시스템의 파괴 행위 등 국가 위기를 해결하기 위한 보호까지 확대되고 있다. 이와 같이 정보보호대상이 국가차원으로 확대됨에 따라 국가정보보호의 개념 정립과 이를 대표하는 국가정보보호 지표 개발 및 지수 산출이 필요하게 된 것이다. 따라서 본 연구에서 다루고자 하는 국가정보보호의 개념은 국가를 구성하는 다양한 정보보호 대상(개인, 기업, 공공)을 포함하는 정보보호의 개념이며, 그 수준을 측정하는 객관적 기준을 국가정보보호 지표로 정의하며 지표를 통해 산출되어 단일 값으로 합산된 수치를 국가정보보호 지수로 정의하고자 한다.

3. 정보보호 수준평가에 관한 기존연구

3.1 국내의 연구

정보보호 수준 측정을 위한 객관적인 기준을 마련하기 위해 정보보호 지표 개발 및 정보보호 평

가에 관한 연구는 국내·외에서 지속적으로 이뤄지고 있다. 먼저 국내의 관련 연구로는 정보보호 지표 계량화에 관한 연구로서 김기윤 외[3]와 김정덕[4]의 연구에서는 통제 항목을 도출하고, 도출된 지표는 산출지표, 결과지표, 영향지표로 분류하였다. 이때 산출 지표는 보안 장치의 생산성 및 효율성을 측정하고, 결과지표는 정보자산의 효과성을 측정하며, 1차적 영향지표는 내부업무의 효율성을, 2차적 영향지표는 정보통신 인프라의 효과성을 측정하였다. 또한, 김현수[5]는 균형성과표(Balanced Scorecard : BSC)를 기반으로 최종 결과 중심의 목적 지향적 지표 시스템을 개발하여 이를 계량화하는 연구를 수행하였으며, 정희조 외[9]는 정보보호수준을 종합적이고 체계적으로 평가하기 위한 방법론으로 정보보호와 관련된 기술적 요소와 관리적 요소를 기본으로 하는 정보보호 지표체계를 구성하였다. 이와 같은 연구 이외에도 국가정보원을 비롯한 한국인터넷진흥원, 방송통신위원회 및 행정안전부와 같은 주요 정부 기관이 주도적으로 정보보호 지표 개발 연구를 지속적으로 수행하고 있다. 아래 <표 2>는 최근 이들 기관들이 개발한 정보보호 평가 지표명과 그 연구 내용들을 분류한 것이다.

3.2 국외의 연구

국외에서의 연구로는 국가 차원으로 미국 및 영국을 중심으로 한 유럽 국가들이 제품 및 시스템의 정보보호 위한 평가 체계를 구축하고 있다. 미국은 1985년에 TCSEC(Trusted Computer Systems Evaluation Criteria)를 제정하여 컴퓨터 시스템의 보안성을 효과적으로 평가하고 안정성 및 신뢰성이 입증된 컴퓨터 시스템을 각 기관에 보급하기 위해 보안의 요구사항에 따라 보안 등급을 6 등급으로 분류하고 있다[30]. 또한 영국, 독일, 프랑스 및 네덜란드 등 자국의 정보보호시스템 평가 기준을 제정하여 시행하던 4개국 이 평가제품의 상호인정 및 평가기준이 상이함에 따른 정보보호제품의 평가에 소요되는 시간, 인력 및 소요 비용을

〈표 2〉 정부 기관의 정보보호 지표 개발 연구

평가 지표명	내용	기관
정보보안관리 수준 평가	<ul style="list-style-type: none"> 국가사이버 안전 관리 규정을 바탕으로 각급 기관의 안정성 수준을 평가 기관별 등급을 분류, 가중치 적용 	국가 정보원[2]
국가정보 보호지수	<ul style="list-style-type: none"> 개인, 정부, 기업을 대상으로 종합적 정보보호수준 결정 정보보호지수와 역기능 지수로 나누어 측정 	한국 인터넷 진흥원 [11, 14]
국내 ISMS	<ul style="list-style-type: none"> 전체 경영시스템 대상 정보보호관리 수준 인증 물리적, 기술적, 관리적 보호조치 수준 평가 	방송통신위원회 (구 : 정보통신부)[7]
전자정부서비스 보안수준실태조사	<ul style="list-style-type: none"> 중앙행정 및 지방행정 기관의 전자정부서비스의 보안수준 평가 	행정 안전부[17]
공공 기관 개인정보보호수준진단	<ul style="list-style-type: none"> 중앙행정기관, 지방자치체의 개인정보 관리 수준 평가 	행정 안전부[17]

절감하기 위해 1992년 ITSEC(Information Technology Security Criteria)를 제정하였다[20]. 이후에 영국은 조직의 정보보호를 구현하고 유지하는 관리자리의 참조 문서인 “BS7799”를 고안했고, 이는 호주, 브라질, 네덜란드, 뉴질랜드, 노르웨이 등에서 사용되어, 1999년에는 ISO 표준으로 제안되어 “ISO/IEC 17799-1”이 되었다[24, 29]. 이외에도 독일은 기관의 적절한 어플리케이션, 인력, 기반 구조와 기술적인 표준 보안대책을 통해 IT 시스템에 대한 보안 수준의 표준 보호요구사항을 권고하는 “IT Baseline protection Manual”을 고안하였다[26]. 이와 같이 정보보호 기준 마련 및 평가에 관한 국가 차원의 연구 뿐만 아니라 민간차원에서도 정보보호 수준 평가와 관련된 다양한 연구가 지속적으로 이뤄져 왔다. Ernst and Young[21]은 정보보호관리, IT 보호기술 개발 등을 중심으로 정보보호 수준을 평가하고 있고 그 외에 인터넷 보안 연합(In-

ternet Security Alliance), 국가 생산협회(National Association of Manufacture), RedSiren Technology는 공동으로 무역협회 9.11 테러 사건 이후 미국 정보보호 수준에 대해 세계 전문가들의 인식 수준을 조사 하였다[23]. 이상과 같은 민간차원에서 정보보호 수준을 평가한 평가 기준은 다음 <표 3>와 같다.

이와 같이 민간단체에서 조사한 정보보호 지표들은 정보보호 전문가를 대상으로 한 설문조사나 일부 조직에 대한 실태조사로 이루어져 국가차원의 정보보호 수준을 평가하는데 한계가 있다. 따라서 국제 환경에서 이루어지는 국제기구들의 정보보호 접근방법들을 살펴볼 필요가 있는데, 경제협력개발기구(OECD : Organization for Economic Cooperation and Development)는 정보보호 수준을 네트워크 보안, 시스템 보안, 응용보안, 최종이용자보안으로 구분하여 정보보호 방향을 제시하고 있다

〈표 3〉 국외 민간 기관의 정보보호 기준

정보보호 기준	민간 기관명
기술, 관리	Ernst and Young[21]
전문가 인식도	인터넷 보안 연합(Intenet Security Alliance), 국가 생산협회(National Association of Manufacture), RedSiren Technology
정보침해건 수	Riptech(2003), Symantec(2003), CERT/CC[19]
예산, 산업, 서비스 침해	Information Week and Pricewaterhouse Coopers LLP(1999)
인적, 예산, 정책, 계획	Internet Security Magazine(2002)

출처 : 신영진(2005), 정보보호정책의 지표개발과 국가간 수준비교, 한국행정논집, 17(1) 발췌수정[6].

[28]. 또한 국제표준화기구(ISO : International Organization for Standardization)는 개인정보보호를 위한 실행지침 ISO/IEC 27001, 27002을 제정하였고, 국제전기통신연합(ITU : International Telecommunication Union)은 보안 인프라에 대한 기술 인증 및 사이버보안 지수(Cyber Security Index) 개발을 제안하였다[25].

3.3 기존 정보보호 평가 모델의 한계 및 시사점

본 연구에서 언급한 기존의 정보보호 평가 모델들은 특정 기관에서 정보보호 상태를 규정하는 표준안과 보안 등급을 제시하고 있다. 그러나 이와같은 지표 또는 표준안을 이용하여 국가정보보호수준을 평가하기에는 다음과 같은 문제들이 존재한다.

첫째, 각각의 지표들이 만들어진 환경이나 의도가 서로 다르기 때문에 적용할 수 있는 대상이 서로 다르다. “TCSEC”, “ITSEC”의 경우, 정보보호 평가 대상이 제품 및 시스템에 한정되어 있으며, “BS7799”의 경우는 시스템에 대한 평가가 미흡하여 정보보호 수준 반영이 어렵다는 한계점이 있다. 또한 “ISO27001”의 경우, 정보보호 수준 측정에서 통제항목의 적용시, 심사원 주관적 의견 및 심사환경에 따라 결과가 다를 수 있기 때문에 객관적이고 정량적인 정보보호 수준 도출이 어렵다. 둘째, 대부분의 지표들이 기관이나 기업체를 대상으로 삼았기 때문에 개인 간의 데이터 이동이나 전자상거래시의 프라이버시 보호에 대한 부분 등이 미흡하다. 셋째, 정보보호 환경변화 측면을 고려하지 않고 있다. 최근 스마트폰으로 인한 무선망의 사용이 급증하였지만 이에 따른 정보보호 위협요소를 고려한 정보보호 지표는 개발되어 있지 않다. 특히 정보보호 환경변화 측면을 지속적으로 고려하기 위해서는 정보보호 환경변화를 측정하는 항목이 지속적으로 개선되어야 할 것이다. 넷째, 정보보호 지표 및 지수의 타당성 측면으로, 지표의 중요도에 따른 가중치가 부여 되어 산출된 지수의 타당성이 확보 되어야 할 것이다. 마지막으로 정보보호를 위한 시스템의 구축뿐만 아니라 관리적

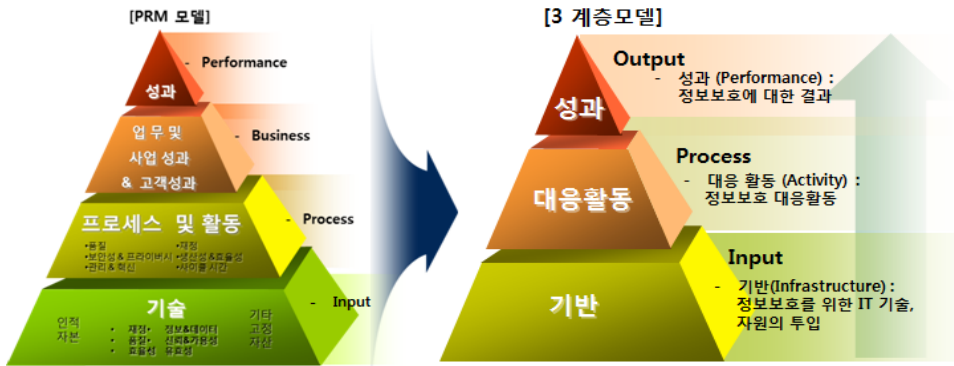
요인이 고려된 지표가 추가 되어야 할 것이다.

본 연구에서는 이와 같은 한계점을 개선하여, 기존의 국가정보보호 지수 모델을 개선하고 우리나라의 국가정보보호 수준을 체계적 그리고 객관적으로 대표하는 새로운 국가정보보호 지수 모델을 개발하고자 한다.

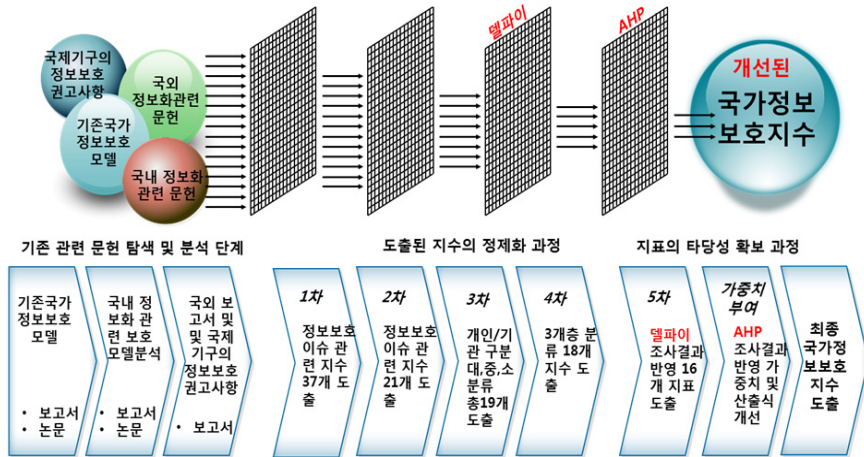
4. 국가 정보보호 측정 지표 개발

4.1 연구 프레임워크

국가의 정보보호수준을 대표하는 지표를 결정하기 위해서는 개인과 기관 등의 정보 및 정보 기술 이용자를 대상으로 정보보호를 위한 IT 기술 및 자원과 같은 인프라(Infrastructure)의 투입과 정보이용자들의 정보보호 대응활동(Activity) 그리고 정보보호의 결과를 나타내는 성과(Performance) 측면이 모두 고려되어야 할 것이다. 따라서 본 연구에서는 다음 [그림 2]와 같이 ‘기반(Infrastructure)-대응활동(Activity)-성과(Performance)’의 3계층으로 구성된 프레임워크를 제안하고자 한다. 이는 미연방의 대표적인 성과체계 방법론인 PRM (Performance Reference Model)을 기반으로 한 것으로 ‘Input-Process-Output’의 인과적 메커니즘을 정보보호 지수 모델 개발에 적용한 것이다. 이러한 프레임워크는 공공 정보화 성과 측정 및 지표 개발에 주로 활용 되고 있으며, 특히 공공 기관의 건축행정 정보화, 행정 정보화, 특히 검색 정보화 및 성과 지표 개발에 적용되었다[8]. 본 연구 또한 이와 같은 프레임워크를 기준으로 국가정보보호 지표를 선정하고 국가 정보보호 수준을 측정하고자 한다. 여기서 기반(Infrastructure)-이란 정보보호 인프라를 구축하는 IT기술과 자원의 투입을 의미한다. 이러한 투입으로 인하여 개인 또는 기업의 기존 프로세스가 정보보호 프로세스로 변화할 것이다. 정보보호에서는 정보보호 활동 또는 대응이 되므로 이 계층을 대응활동(Activity) 계층으로 정의 하였다. 이러한 정보보호 활동들은 궁극적으로 보안사고의 절감 등의 성과를 나타낼 것이다. 이



[그림 2] PRM 모델과 국가정보보호지수 프레임워크



[그림 3] 국가정보보호지수 지표 선정 및 산출 과정

부분을 성과(Performance) 계층으로 정의 하였다.

4.2 지표 선정 과정

국가 정보보호 지수를 구성하는 세부 지표의 선정은 [그림 3]과 같은 4차의 지수 정제화 과정과 2차례의 지표 타당성확보 과정을 포함하였다. 첫째 정보보호 지수를 구성하는 세부 지표를 도출하기 위해 기존 자료에 대한 조사와 정보보호를 둘러싼 국내의 분석 가능한 모든 지표를 취합하여 지표 Pool 을 구성 하였다. 이후 정보보호 기관연구원과 학계 전문가(교수) 그리고 정보보안 업체 담당자로 구성된 총 13인의 전문가들로 구성된 연구반의

검토를 거쳐 세부 지표를 도출하였다.

위 [그림 3]과 같이 지표 Pool 선정 이후 첫째 대표성이 뛰어나고, 둘째 계량화가 가능하고, 셋째 정보보호에 있어 중요성이 높은 지표들을 4차에 걸쳐 정제화 하였으며, 마지막으로 정보보안 전문가들을 대상으로 각 예비 지표들에 대해서 ‘지표 대표성’, ‘측정 가능성’, ‘지표 중요도’등에 대해서 델파이 조사를 실시하고 그 결과를 반영하여 총 16개의 지표를 도출하였다. 이때 총 16개의 지표 중 기존 지표와 비교하여 개선된 지표의 내용은 아래 <표 4>와 같으며, 결론적으로 최종 도출된 국가정보보호지표와 개별 지표의 정의는 아래 <표 5>와 같다. 특히 세부 지표에 사용되는 통계데이터는 한

국인터넷진흥원(2009)의 ‘정보보호 실태조사’[13], 지식경제부, 방송통신위원회의 ‘2009 국가정보보호 백서’[1]에 의존하였으며, 보안서버이용률에 있어서는 경제개발협력기구(OECD : Organization for Economic Cooperation and Development)의 Communication outlook을 참조하였다. 본 연구에서 도출한 각 계층의 성격을 살펴보면, 먼저 기반 계층은 정보보호를 위한 시스템의 구축정도와 보안인력 및 자본의 투입 정도를 대표하여 정보보호의 직접적인 수준을 나타낸다. 둘째 대응활동계층은 정보기술 및 정보 사용자의 활동에 주목한 것으로 신기술 환경에서 초래된 정보위협에 대응정도와 백업, 업데이트, 패스워드, 공인인증서, 보안서버와 같은 정보보호 장치의 적극적인 활용 정도를 측정할 것이다. 마지막으로 성과 계층은 정보보호 기반과 대응활동의 결과로 해킹, 바이러스 및 스파와 개인정보침해 신고율 그리고 개인정보 노출률과 악성 봇 감염율을 통해 정보 보호 수준을 나타낸다. 특히 본 연구에서 제안하고자 하는 국가 정보보호지수는 16개 지표 값의 합으로 산출된다. 이때 각 개별 지표 값이 산출되는 과정에서 특정

지표가 우선순위와 그 중요성에 비해 적은 비중으로 산출될 위험이 있다. 이러한 한계를 보정하기 위하여 개별 지표의 가중치를 산출하여 국가 정보보호지수 산출에 적용하고자 하였으며, 이를 위해 AHP 조사를 수행 하였다.

5. 국가정보보호수준 측정

5.1 지수의 산출 과정

본 연구에서 산출한 국가정보보호 지수는 아래 식 (1)과 같이 계산된다.

$$\text{국가정보보호지수}(NISI) = C_1I + C_2R + C_3P \quad (1)$$

where, $C_1 + C_2 + C_3 = 1$

위 식 (1)과 같이 국가정보보호 지수(National Information Security Index : NISI)는 각 계층별 지수를 통합한 것이다. 이때 각 기반(I), 대응활동(R), 성과(P) 계층의 중요도에 따라 가중치($C_1 \sim C_3$)가 부여된다. 또한 각 개별 계층의 지수는 계

〈표 4〉 기존 지표와 신규 지표 비교

항목	기존 지표 세부항목	수정된 지표	개선 사항	
정보 보호 수준	정보 보호 기반	백신보급률	보안소프트웨어 설치율	에드웨어, 백신, 통합 보안 S/W으로 확대
		패치보급률	업데이트 관리율	개인의 정보보호 수준 측정에 있어 OS패치뿐만 아니라 백신업데이트가 중요함으로 본 지표에 포함
		PKI 보급률	공인인증서 발급률	유지
		Firewall 보급률	정보보호시스템 도입률	Firewall, IDS 등 13개의 정보보호 시스템 설치 목표 값을 고려
		IDS 보급률		
	보안서버 보급률	보안서버 이용률	유지	
	정보 보호 환경	정보보호 관련 예산비율	정보보호 투자 비율	유지
		정보보호 전문인력 비율	정보보호 전문인력 비율	유지
국민의 보안의식 수준 비율		삭제	정성적 지표로서 객관성이 부족하여 삭제	
역기능 수준	정보화 역기능	해킹·바이러스 신고비율	해킹 바이러스 신고율	(기존) 신고건수/PC 보급 대수 분모를 ‘인터넷 사용자 수’로 수정
		개인정보 침해 신고비율	개인정보침해 신고율	유지
		스팸메일 수신비율	스팸신고율	기존에는 개인별 스팸수신율을 측정했으나 객관성을 높이기 위해 개인당 신고비율로 수정

<표 5> 도출된 국가정보보호지수 세부지표 및 정의

계층	세부지표	정의	산출 데이터 출처
성 과	16 개인정보 노출률(신규지표)	Kr 도메인에서 주민번호가 노출되어 있는 웹 페이지 비율	◦ KISA, ISIS 인터넷통계 정보시스템 ITU
	15 개인정보침해 신고율	인터넷 사용자의 개인정보 침해 신고의 비율	◦ 당해년도 신고건수 : KISA 통계자료, 2010, 10; 개인정보침해 구제현황, p.14. ◦ 인터넷 사용자 수 : KISA, ISIS 인터넷통계 정보시스템 ITU
	14 악성 봇감염률(신규지표)	악성 봇에 감염된 국내 IP의 비율	◦ KISA, ISIS 인터넷통계 정보시스템 ITU
	13 스팸신고율	당해 년도 인터넷 사용자의 스팸 신고 비율	◦ 당해년도 신고건수 : KISA 통계자료, 2010, 10; 개인정보침해 구제현황, p.14. ◦ 인터넷 사용자 수 : KISA, ISIS 인터넷통계 정보시스템 ITU
	12 해킹 바이러스 신고율	연간 인터넷 사용자의 해킹 바이러스 신고 비율	◦ 당해년도 신고건수 : KISA 통계자료, 2010, 10; 개인정보침해 구제현황, p.14. ◦ 인터넷 사용자 수 : KISA, ISIS 인터넷통계 정보시스템 ITU
대 응 활 동	11 신기술 환경 대응률 (신규지표)	IT신기술을 통한 위협에 대한 대응 정도	◦ KISA 자료-기관 정보보호 실태조사 ◦ KISA 자료-개인 정보보호 실태조사
	10 보안서버 이용률	인터넷에서 보안서버의 보급률	◦ 당해년도 신고건수 : KISA 통계자료, 2010, 10; 개인정보침해 구제현황, p.14. ◦ 인터넷 사용자 수 : KISA, ISIS 인터넷통계 정보시스템 ITU
	9 정보보호관리체계 인증률(신규지표)	전체 기업 중 정보보호 관리체계 인증(ISMS)을 받은 기업의 누적 비율	◦ ISMS 인증업체(누적) : KISA 통계자료, 2010, 10 ; 직원 10인 이상 기업수 : 통계청, 시도·산업·종사자규모별 사업체수, 종사자수(2008)
	8 업데이트 관리율	개인의 OS와 백신의 주기적인 업데이트 실행 정도	◦ KISA 자료, 2009 개인정보보호 실태조사
	7 백업 관리율 (신규지표)	개인과 기관의 백업 실시 정도	◦ KISA 자료, 2009 개인정보보호 실태조사 ◦ 기업에 대한 백업주기 산출 값은 신규지수임에 따라 추정치임
	6 공인인증서 발급률	개인 및 기관의 공인인증서 발급자의 비율	◦ 공인인증서 발급자 수 : KISA 개인 인터넷 이용자 정보보호실태조사. ◦ 인터넷 사용자 수 : KISA, ISIS 인터넷통계 정보시스템 ITU
	5 패스워드 관리율(신규지표)	패스워드의 안전성과 복잡성을 확보하고 주기적인 변경을 실시하는 사용자 수의 비율	◦ KISA, 패스워드 관리 가이드라인 ◦ KISA, 2009 정보보호 실태조사-개인편, p.190-191
	4 정보보호시스템 도입률	기관의 정보보호시스템 도입 비율	◦ 당해년도 신고건수 : KISA 통계자료, 2010, 10; 불법스팸 조치현황, p.24. ◦ 인터넷 사용자 수 : KISA, ISIS 인터넷통계 정보시스템 ITU
기 반	3 보안소프트웨어 설치율	개인의 PC에 보안 소프트웨어가 설치된 비율	◦ KISA 자료, 2009 개인정보보호 실태조사
	2 정보보호 투자비율	공공과 민간기관의 총 정보화 예산에서 정보보호 예산이 차지하는 비율	◦ 공공 부문 (정보화 및 정보보호 예산); “국가정보화사업 평가” 국회예산정책처, NABO, 2010. 8. 104 ◦ KISA자료-관 정보보호 실태조사
	1 정보보호 전문인력 비율	전체 IT 종사인력 1천명 당 정보보호 전문가 인력의 수	◦ 정보보호 전문가 인력 수 : KISA 자료-2009 국내지식 정보보안산업 시장 및 동향조사 ◦ IT 인력 수 : 지식경제부, 방송통신위원회, ISIS 2008년 정보통신부분 인력동향 보고서, 2009. 4

층 내부가중치 세부지표의 통합으로 아래 식 (2) ~ 식 (4)와 같다. 여기서 $n_1 \sim n_{16}$ 은 각 개별 지표 값이며 $w_1 \sim w_{16}$ 각 개별 지표에 부여된 가중치 값으로 각 계층내의 가중치합은 1이다.

• 기반 (I) = $w_1n_1 + w_2n_2 + w_3n_3 + w_4n_4$ (2)

• 대응활동 (R) = $w_5n_5 + w_6n_6 + w_7n_7 + w_8n_8 + w_9n_9 + w_{10}n_{10} + w_{11}n_{11}$ (3)

• 성과 (P) = $w_{12}n_{12} + w_{13}n_{13} + w_{14}n_{14} + w_{15}n_{15} + w_{16}n_{16}$ (4)

where, $w_1 + w_2 + w_3 + w_4 = 1$
 $w_5 + w_6 + w_7 + w_8 + w_9 + w_{10} + w_{11} = 1$
 $w_{12} + w_{13} + w_{14} + w_{15} + w_{16} = 1$

이때 $n_1 \sim n_{16}$ 의 개별 지표 값은 델파이 조사 결과로부터 얻은 목표값을 기준으로 표준화되고 최종 국가정보보호지수는 표준화된 세부 지표값에 계층별, 계층내 가중치를 적용한 후 산술 평균하여 계산되어 진다.

5.1.1 가중치 및 목표값 산출

본 연구에서 제안한 국가정보보호 지수의 산출 식에는 각 계층과 세부 지표에 따라 각기 다른 가중치가 부여 된다. 이와 같은 가중치는 각 계층 간, 지표 간 상대적 중요도를 도출하는 방법론인 AHP

(Analytic Hierarchy Process) 방법론을 적용하여 도출한 것이다. AHP는 여러 속성을 두 개의 쌍으로 묶어 비교함으로써 의사결정 과정에 참여하는 여러 전문가들의 의사결정 판단 자료를 기반으로 보다 쉽고 체계적으로 개별 속성의 상대적 중요도를 도출 할 수 있는 방법이다. 따라서 본 연구에서는 최종 도출된 3개 계층과 계층 내 16개 지표를 대상으로 [그림 4]와 같은 AHP 설문지를 구성하고 내부의 위촉 연구위원을 대상으로 설문을 실시하였다. 또한 본 연구에서는 지수 값의 표준화를 위해서 위촉된 연구위원을 대상으로 델파이를 실시하여, 정보 보안이 가장 이상적인 상태 일 때 개별 지표들이 가져야 할 목표 수치를 도출하였다. 그 결과, 아래 <표 6>과 같이 가중치와 개별 지표 값의 목표치가 도출되었다.

5.2 국가정보보호 지수 산출

5.2.1 지수의 표준화

기존의 국가 정보보호지수 모델에서는 산출된 지표 값이 표준화 되지않아 산출된 개별 지표 값을 통해 국가정보보호 수준을 판단하기 어렵고, 개별 지표 간 상대적 비교 또한 어렵다는 단점이 있었다. 따라서 본 연구에서는 앞에서 언급한 바와 같이 보안 전문가 그룹을 대상으로 델파이 조사를 실시하였으며 이를 통해 도출한 목표값을 산

[응답 예시]

각 문항은 비교대상을 A와 B로 구분하였으며, 양자를 대상으로 더 중요하다고 생각하는 곳에 V를 표기해 하면 됩니다. 예를 들어 다음 설문 중 A와 B 중 더 중요하다고 생각하는 쪽에 V를 표시한 예입니다

	더 중요함 <-----									같음	-----> 더 중요함									
	9	8	7	6	5	4	3	2	1		2	3	4	5	6	7	8	9		
1. 정보보호전문인력비용																				2. 정보보호투자비용
1. 정보보호전문인력비용																				3. 보안소프트웨어설치율
2. 정보보호투자비용																				3. 보안소프트웨어설치율

- [1.정보보호 전문 인력비용]이 중요도 측면에서 [2.정보보호투자비용] 보다 4배 정도 더 중요하다고 생각되면 [1.정보보호전문인력비용] 방향의 4에 체크(V)
- [3.보안소프트웨어설치율]보다 [1.정보보호 전문인력비용]이 중요하다고 생각하는 정도가 6배 정도라고 생각되면 [3.보안소프트웨어 설치율] 방향에 6에 체크.
- [3.보안소프트웨어 설치율]과 [2.정보보호투자비용]이 중요도 측면에서 같은 수준이면 1에 체크

[그림 4] AHP 응답 예시

〈표 6〉 계층별, 지표별 가중치

분류			세부 지표		가중치		목표치
계층	가중치						
성과 (P)	C ₃	0.160	n ₁₆	개인정보 노출률	w ₁₆	0.084	2.920
			n ₁₅	개인정보침해 신고율	w ₁₅	0.234	0.660
			n ₁₄	악성 봇감염율	w ₁₄	0.128	0.590
			n ₁₃	스팸신고율	w ₁₃	0.160	74.000
			n ₁₂	해킹 바이러스 신고율	w ₁₂	0.393	4.280
대응 활동 (R)	C ₂	0.464	n ₁₁	신기술 환경 대응률	w ₁₁	0.038	63.111
			n ₁₀	보안서버 이용률	w ₁₀	0.058	92.500
			n ₉	정보보호 관리체계 인증률	w ₉	0.147	2.272
			n ₈	업데이트 관리율	w ₈	0.100	95.453
			n ₇	백업 관리율	w ₇	0.189	53.167
			n ₆	공인인증서 발급률	w ₆	0.189	56.667
			n ₅	패스워드 관리율	w ₅	0.280	67.273
기반 (I)	C ₁	0.376	n ₄	정보보호 시스템 도입률	w ₄	0.097	55.170
			n ₃	보안소프트웨어 설치율	w ₃	0.113	97.091
			n ₂	정보보호 투자비율	w ₂	0.347	1.341
			n ₁	정보보호 전문인력비율	w ₁	0.443	9.090

출하고(〈표 7〉 참조), 이를 기준으로 세부 측정 지표값을 표준화 하였다.

식 (5)와 같이, 개별 지표의 목표 값을 100점으로 설정하고 목표값에 대한 당해 연도의 측정값의 비율을 개별 지표의 표준화 값으로 계산 하였다.

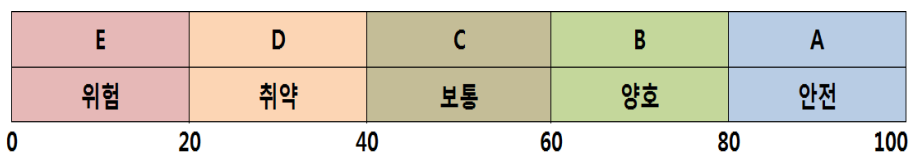
$$\text{표준화 값} = \frac{\text{측정값}}{\text{목표값}} \times 100 \quad (5)$$

이와 같이 표준화 된 측정 지표 값은 개별 지표의 가중치와 계층별 가중치가 각각 부여되고 통합

되어 국가정보보호지수가 산출이 된다. 그리고 그 산출된 값의 범위는 0과 100사이에 있게 되는데, 각 점수의 범위에 따라 위험(0~20), 취약(20~40), 보통(40~60), 양호(60~80), 안전(80~100)으로 그 수준을 아래 [그림 5]과 같이 구성하였다.

5.2.2 지수 산출

본 연구에서 도출된 지표 정의 및 산출식에 2009년 데이터를 적용하여 아래 〈표 7〉과 같이 국가정보보호 지수를 도출하였다. 먼저 지표 정의 및 산출식에 따라 세부 지표별 측정값을 도출하고,



[그림 5] 국가 정보보호지수의 수준

〈표 7〉 국가정보보호 지수 산출

계층	세부 지표	측정값	목표값	표준화값	가중치				계층 산출값	국가정보보호 지수값
					계층별	세부지표				
성과 (P)	n_{16}	4.94	2.92	59.12	C_3	0.160	w_{16}	0.084	60.53	76.38
	n_{15}	0.96	0.66	69.06			w_{15}	0.234		
	n_{14}	1.00	0.59	59.00			w_{14}	0.128		
	n_{13}	96.66	74.00	76.56			w_{13}	0.160		
	n_{12}	0.09	0.04	49.87			w_{12}	0.393		
대응 활동 (R)	n_{11}	58.25	63.11	92.30	C_2	0.464	w_{11}	0.038	76.55	
	n_{10}	89.30	92.50	96.54			w_{10}	0.058		
	n_9	0.27	2.27	11.87			w_9	0.147		
	n_8	92.44	95.45	96.85			w_8	0.100		
	n_7	50.57	53.17	95.12			w_7	0.189		
	n_6	47.59	56.67	83.97			w_6	0.189		
	n_5	53.25	67.27	79.16			w_5	0.280		
기반 (I)	n_4	36.46	54.92	66.38	C_1	0.376	w_4	0.097	82.91	
	n_3	95.73	97.09	98.59			w_3	0.113		
	n_2	1.03	1.34	76.75			w_2	0.347		
	n_1	0.78	0.91	86.10			w_1	10.443		

이를 목표값으로 나누어 세부 지표의 표준화된 값을 도출하였다. 이후에 계층별 가중치와 세부 지표별 가중치를 부여하고 통합하여 계층별 지수값을 산출하고 이를 다시 산술 평균하여 최종 국가정보보호지수 값을 도출 하였다. 그 결과 최종 국가정보보호 지수는 76.38점으로 산출 되었으며, 계층별로 기반은 82.91점, 대응활동은 76.55점, 성과는 60.53점으로 산출 되었다.

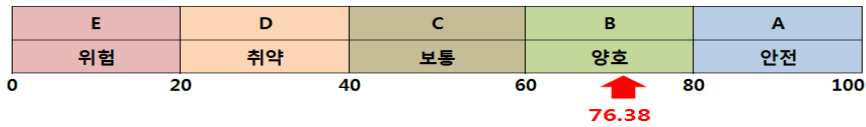
이와 같이 각 계층별, 지표별 도출된 값을 통해, 2009년도 최종 국가 정보보호 지수의 수준을 나타내면 아래 [그림 6]과 같이 76.3점, 양호한 수준임 판정할 수 있다.

각 계층별로 국가 정보보호 수준을 살펴보면 다음 [그림 7] 같이 성과는 60.53점, 양호수준 대응활동 또한 76.55점으로 양호, 마지막으로 기반은 82.91점으로 안전에 해당하는 수준으로 나타났다. 이러한 분석으로 볼 때 정보보호와 관련된 기반부분의 투자와 보호활동이 상대적으로 잘 추진되고 있다고

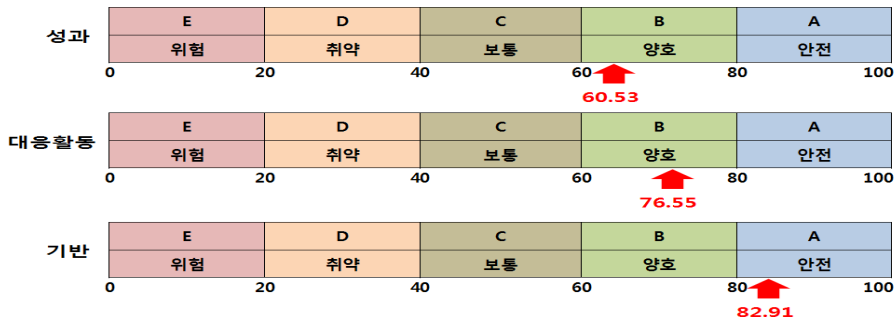
볼수 있고 이러한 투자가 대응활동과 성과에 점증적으로 반영되고 있는 상황이라고 분석할 수 있다.

5.2.3 국가정보보호 지수의 추세 분석

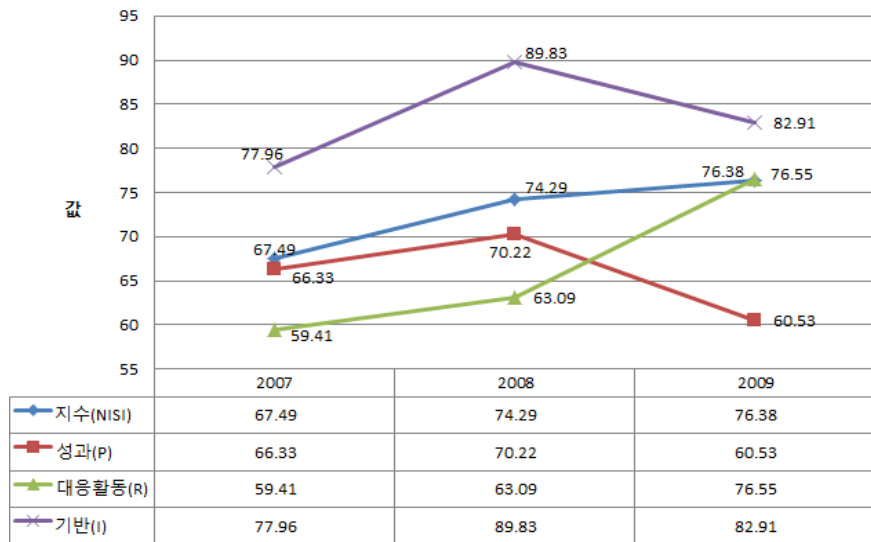
본 연구에서 도출한 국가 정보보호지수 모델을 통해, 2007년~2009년의 3년간 연도별 국가 정보보호지수 값을 산출하였다. 그 결과 아래 [그림 8]와 같이 국가정보보호 수준은 2007년에는 67.49, 2008년에는 74.29 그리고 2009년에는 76.38로 국가정보보호 수준은 양호한 수준에서 해마다 조금씩 개선되는 추세를 나타냈다. 본 모델의 적용으로 3개년에 대한 계층별 비교분석이 가능하다. 추이를 보면 전반적으로 우리나라의 정보보호 인프라 부분은 다른 계층에 비해서 탄탄함을 보여주고 있다. 지속적인 정보보호에 대한 홍보와 지원을 통해 대응활동들은 점차 증가하고 있음을 알 수 있다. 그러나, 성과부분은 상대적으로 낮아지고 있는 것으로 나타나 정보보호 피해가 늘어나며 그 심각성이 더



[그림 6] 국가정보보호지수 수준



[그림 7] 계층별 국가정보보호지수 수준



[그림 8] 개선된 모델이 적용된 2007년~2009년의 국가정보보호지수

욱 증대되고 있음을 알 수 있다. 이렇듯 본 모델을 통해서 계층별로 또 인과성을 연계해서 정보보호 수준 및 대응방향을 설정할 수 있는 장점이 있다.

6. 결 론

본 연구에서는 국가정보보호 지수 및 지표를 도출

하기 위하여 국내외 정보보호 및 정보화지수모델 관련문헌 및 보고서를 비롯한 국제기구의 권고 기준을 바탕으로 지표 Pool을 구성하고 5차의 지표 정제 과정과 델파이, AHP 분석 방법을 활용하여 지표 및 그 산출 방법의 타당성을 확보하였다. 특히 지표 선정을 위해 PRM 모델의 ‘투입(Input)-프로세스(Process)-결과(Output)’의 인과적 메카니즘

을 기반으로 ‘기반(Infra)-대응활동(Activity)-성과(Performance)’의 3계층의 프레임워크가 고안되었다. 본 연구에서는 국가정보보호 지수를 구성하는 3 계층별 산출값 뿐과 개별 지표를 목표치를 기준으로 표준화되었기 때문에 상호 비교가 가능하여, 지표의 우선순위 결정시 시사점을 제공할 수 있다. 또한 개별 지표와 계층에 가중치가 부여되어 국가정보보호 수준을 측정하는 지수 값이 산출 되어 현재의 국가 정보보호 수준을 보다 객관적으로 가늠할 수 있는 수치로 활용 될 수 있을 것이다. 실제로 2009년 데이터를 기준으로 국가 정보보호지수를 산출한 결과, 76.38점으로 양호한 수준을 나타내고 있으며, 추가적으로 2007년~2009년의 국가 정보보호 수준의 추세를 분석한 결과 추세적인 일관성을 보여주고 있으며 계층별 비교 분석이 가능함을 보였다.

국가 정보보호 지수 모델 개선을 수행한 본 연구는 지속적인 연구반 회의와 델파이, AHP 분석 기법을 통해 최종 국가 정보보호지수 모델을 도출하였으며, 지표와 가중치의 타당성을 높여 국가 정보보호지수를 산출하였다. 본 연구에서 개발된 국가 정보보호지수 모델의 특징은 다음과 같다.

첫째 본 연구는 국가 정보보호 지수 모델 개선을 위해 3개 계층 ‘기반-대응활동-성과’의 인과적 과정을 적용하였다. 이는 기술적 측면과 인프라 투자만을 고려한 기존 모델과 차별되는 점으로, 도출된 3계층의 산출 값 비교를 통해 정보보호 투자의 정책적 시사점을 제시 할 수 있다. 본 연구의 이러한 계층 구조는 향후 인과적 관계의 증명이나 기반 → 대응활동 → 성과까지 나타나는데에 걸리는 시차(time-lag)의 요인들에 대한 추가적인 연구가 이루어 진다면 더욱 의미있는 국가정책을 수립할 수 있을 것이다.

둘째, 본 연구에서 제시한 국가 정보보호 지수 모델은 델파이, AHP를 통해 각 지표의 타당성이 확보되었다. 특히 각 지표별 목표치가 고려되고, 각 지표별, 각 계층별 가중치가 고려되어 도출된 표준화된 값이기 때문에 지표별, 계층별 우선순위를 비교할 수 있다. 이는 투자의 우선순위를 결정하기 위한

정책결정과정에 합리적 시사점을 제시할 수 있다.

셋째, 본 연구에서는 국내의 정보보호 지수를 탐색하여 지표 Pool을 구성하고 전문가들의 의견 수렴을 통해 최종 지표를 선정하였으며, 선정한 지표 중 신기술 환경을 고려한 지표를 추가 하였다. 이 지표는 환경변화에 맞게 수정과 보안이 가능한 유연성 있는 지표로 설정하여 신기술 환경으로부터의 정보보호 위협을 즉각적으로 반영할 수 있게 한 것이다.

향후 국가 정보보호 지수 모델은 정교화 객관화가 지속적으로 확보되어야 할 것이다. 특히 산출식과 목표치 그리고 가중치의 정교화는 정보보호 지수의 개발에 필수적인 요소임을 상기하여야 할 것이다. 또한 국가 정보보호 지수 모델 개발과 더불어 그 체계적인 운영전략 또한 마련되어야 할 것이다. 본 연구에서는 다음과 같은 지수의 운영 전략을 제언한다.

첫째 ‘국가 정보보호지수 위원회’를 구성하여 지속적인 지수 검토가 이뤄져야 할 것이다. 이와 같은 위원회를 통해 지표의 목표치, 가중치가 정기적으로 설정되고, 모델보완 및 개선안에 대한 토의와 인준이 이뤄진다면 국가 정보보호 수준을 보다 객관적으로 가늠할 수 있게 될 것이다.

둘째, 자동적으로 국가 정보보호지수의 패널 정보 입력 및 가중치 선정과 지수 산출이 가능한 시스템 구축이 필요하다.

셋째, 국가간 비교를 위한 표준화 노력이 이뤄져야 할 것이다. 이를 위해서는 국외의 보고서에 의존하는 문헌 연구가 아니라 지수비교를 위한 국제적 협조 네트워크 구축이 필요 할 것이다.

참 고 문 헌

- [1] 국가정보원·방송통신위원회·행정안전부·지식경제부, 『2009 국가정보보호백서』, 2009.
- [2] 국가정보원·정보통신부, 『2007 국가정보보호백서』, 2007.
- [3] 김기윤, 나관식, 김종석, “LLNL 체크리스트를 이용한 정보시스템 취약성 평가”, 『통신정

- 보보호학회지」, 제6권, 제4호(1996), pp.1-20.
- [4] 김정덕, 김기윤, “정보보호지표 항목개발 및 계량화 연구”, 연구보고서(98-10), 한국정보보호센터, (1998), pp.1-120.
- [5] 김현수, “정보보안수준 계량화 연구”, 『경영정보학연구』, 제9권, 제4호(1999), pp.181-201.
- [6] 신영진, 김성태, “정보보호 정책의 지표개발과 국가간 수준비교”, 『한국행정논집』, 제17권, 제10호(2005), pp.131-163.
- [7] 정보통신부, “정보보호관리체계 인증심사 기준”, 정보통신부 고시 제2002-22호, 2002.
- [8] 정국환, 안재민, 홍필기, 『공공정보화 성과 평가방법론 연구』, 정보통신 정책 연구원, (2008), pp.35-37.
- [9] 정희조, 김진영, 임춘성, “기업의 정보보호 수준 및 성숙도 진단을 위한 정보보호 수준 통합 평가 시스템 개발에 관한 연구”, 『정보보호학회지』, 제14권, 제4호(2004), pp.37-44.
- [10] 최승담, 박기홍, 『국민관광지표개발 연구 보고서』, 한국관광연구원, 1996.
- [11] 한국인터넷진흥원, 『2006년 국가정보보호 수준 평가지수 산출과 시사점』, 한국정보보호진흥원, 2006.
- [12] 한국인터넷진흥원, 『2013 인터넷 이용실태조사』, 한국인터넷진흥원, 2013.
- [13] 한국인터넷진흥원, 『2009 정보보호 실태조사 : 개인편』, 한국인터넷진흥원, 2009.
- [14] 한국정보보호진흥원, 『국가정보보호 수준 평가모델 개발』, 한국정보보호진흥원, 2004.
- [15] 한국정보보호진흥원, 『주요 국가의 개인정보보호 동향조사』, 고려대학교 산학협력단, 2009.
- [16] 한국정보화진흥원, 『2012 국가정보화백서』, 한국정보화진흥원, 2012.
- [17] 행정 안전부, 전자정부 서비스보안 수준 개선 대책, 행정안전부, 2008.
- [18] 황철중, 주용완, 민경식, 정경호, “국가정보보호수준 측정 및 활용에 관한 연구”, 『정보화 정책』, 제13권, 제3호(2006), pp.121-135.
- [19] CERT/CC, *CERT/CC Overview Incident and vulnerability trends*, CERT/CC, 2002.
- [20] EC, *Information Technology Security Evaluation Criteria*, The European Commission, 1992.
- [21] Ernst and Young LLP, *Global Information Security Survey*, Published in the UK by Presentation Services, 2002.
- [22] IMD, *World Competitiveness Yearbook*, 2010.
- [23] ISSA(Information System Security Association), *Ernst and Young Global Information Security Survey*, 2002.
- [24] ISO/IEC, *ISO/IEC 17799 : Information Technology-Code of Practice for Information Security Management*, 2000.
- [25] ITU(International Telecommunications Union), *Radio Regulations*, Vol.1(1998).
- [26] Karin Höne and J. H. P. Eloff, “Information security policy-what do international information security standards say?”, *Computers and Security*, Vol.21, No.5(2002), pp.402-409.
- [27] Land, K. C., “Theories, Models and Indicators of Social Change”, *International Social Science Journal*, Vol.27, No.1(1975), pp.7-8.
- [28] OECD, *Overview OECD Communications Outlook : Edition*, 2003.
- [29] Pounder, C., “The revised version of BS 7799-so what’s new?”, *Computers and Security*, Vol.18, No.4(1999), pp.307-311.
- [30] US DoD, *Trusted Computer System Evaluation Criteria. US Department of Defence*, 1985.
- [31] WEF, *The Global Competitiveness Report*, 2009-2010.
- [32] URL : e-나라지표 : <http://www.index.go.kr>.

◆ 저 자 소 개 ◆



임 규 건 (gglim@hanyang.ac.kr)

KAIST 전산학 학사, POSTECH 전자계산학 석사, KAIST 경영공학 박사학위를 취득하였고, 삼성전자, KT 연구개발본부 전임연구원, 국제전자상거래 연구센터(ICEC)의 연구위원, 세종대학교 경영학과 교수로 재직하였으며 현재 한양대학교 경영대학 교수로 재직하고 있다. 한국지능정보시스템학회, 한국IT서비스학회, 한국전자거래학회, 한국경영정보학회 등 주요학회 임원 및 UCI 운영위원 등의 활동을 하고 있다. 주요 저서로는 경영을 위한 정보 기술(2007, 교보문고), e-비즈니스 경영(2005, 이프레스) 등이 있으며, 관심분야는 e-Business, 기술경영, Intelligent IT Service 등이며, 다수의 프로젝트 참여 경력과 Electronic Commerce Research and Applications, Journal of Organizational Computing, 한국전자거래학회지, 한국IT서비스학회지, 경영정보학회지 등의 논문과 관련 특허가 있다.



배 순 한 (ifsleeping@naver.com)

한국외국어대학교 신문방송학과와 경영정보학과 박사수료후 한양대학교 경영학과에서 박사학위를 취득하였다. 관심분야는 IT 서비스 전략, IT 산업 및 시장분석, 소셜 미디어, 사회네트워크 분석 등이다.



이 대 철 (dclee@creativeconsulting.kr)

평택대학교 전산통계학과를 졸업하고, 세종대학교에서 e-Business학 전공으로 경영학 석사학위, 한양대학교 경영학 박사학위를 취득하였으며, 현재 ㈜창의컨설팅의 그룹장으로 재직하고 있다. 다수의 프로젝트 참여 경력과 Electronic Commerce Research and Applications, Journal of Information Technology Applications and Management, Information System Review, 한국전자거래학회지, 한국IT서비스학회지, 경영정보학회지 등의 논문이 있다. 주요 관심분야는 공공정보화사업 성과분석, e-Business, MIS, Intelligent Service 등이다.



지 상 호 (jsh@kisa.or.kr)

현재 한국인터넷진흥원 정보보호관리 팀장으로 재직 중으로 정보보호, 국가정보보호지수 등이 관심연구영역이다.

**백 승 익 (dclee@khu.ac.kr)**

미국 George Washington University에서 경영학 석사 (MBA)와 박사 학위 (Ph.D.)를 취득하였으며, 현재 한양대학교 경영대학 교수로 재직 중이다. 한양대학교에 부임하기 전에 미국 Georgia State University와 Saint Joseph's University에서 조교수를 역임하였다. 주요 연구관심 분야로는 Business Intelligence, Service Science, Service Innovation, HCI 등이다.