情報保護學會論文誌
第 22 卷 第 4 號, 2012. 8

스마트시대 정보보호정책에 관한 연구*

김 동 욱,† 성 욱 준‡
서울대학교

A Study on Information Security Policy in the era of Smart Society*

Kim Dongwook,† Sung Wookjoon‡
Seoul National University

요 약

본 연구는 정보보호 전문가를 대상으로 한 AHP(Analytic Hierarchy Process) 설문 분석을 통하여 우리나라 정보보호 정책 및 전략에 관한 우선순위를 제안하는 것을 목적으로 한다. AHP 설문에서는 안전한 정보사회 구현을 위한 정보보호 정책을 정보보호 기반분야, 정보보호 정책활동 분야로 나누었다〈계층 1〉. 이 중 정보보호 기반분야는 법제도기반, 인적기반, 기술적 기반, 사회적 인식으로 나누고, 정보보호 정책활동은 주요기반시설보호, 개인정보보호, 정보보호 산업진흥, 국가안보활동의 각 4가지로 나누었으며〈계층 2〉, 〈계층 3〉을 다시 총 16개의 정보보호 정책 대안으로 세분하였다. 정보보호정책의 우선순위에 대한 분석 결과 정책중요도 측면에서는 법제도정비의 순위가 가장 높았고, 전문인력 처우개선과 추진체계 정비에 대한 정책요구가 높았다. 정책시급성 측면에서는 추진체계정비가 가장 높은 순위로 나타났고 법제도 기반정비, 전문인력 처우개선, 사이버침해대응 활동에 대한 순위가 높게 나타났다. 중요성과 시급성을 종합적으로 고려한 분석에서는 정보보호 관련 법제정비, 추진체계정비, 전문인력 처우개선 등이 중요도와 시급성이 모두 높은 최우선 정책과제로 나타났다. 최근 정보보호 관련 사고로 정보보호에 대한 우려가 높아짐에 따라 정보보호 분야의 보다 체계적인 대응과 정책적 연구가 필요할 것으로 보인다.

ABSTRACT

This study will propose the policy priorities of cyber information security by AHP(Analytic Hierarchy Process) survey. The policy categories for AHP survey consist in the foundation of information security and activity of information security(1st hierarchy). In the second hierarchy, the foundation of information security was classified into laws-system, human resources, h/w-s/w technology and sociocultural awareness. And the activity of information security was divided into infrastructure protection, privacy protection, related industry promotion, and national security. Information policy alternatives were composed of 16 categories in the third hierarchy. According to the AHP result, in the perspective of policy importance, the modification of related laws was the first agenda in the policy priority, better treatment of professionals was the second, and the re-establishment of policy system was the third. In the perspective of policy urgency, the re-establishment of policy system was the first item, the modification of related laws was the second, and better treatment of professionals is the third.

Keywords: cyber security, information security, information security policy, AHP(Analytic Hierarchy Process)

접수일(2011년 12월 14일), 수정일(2012년 2월 28일), 게재확정일(2012년 4월 12일)

* 이 논문은 2011년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2011-330-B00205)

† 주저자, dong@snu.ac.kr
‡ 교신저자, side91@snu.ac.kr

I. 서 론

제3의 물결이라 불리는 정보화 변혁이 시작된 이후 정보화는 빠른 속도로 사회 전반에 영향력을 확대하고 있다. 특히, 2009년 후반기부터 한국에 본격적으로 도입되기 시작한 스마트폰의 등장과 각종 스마트 기술의 발전 속도는 이전의 정보사회와는 또 다른 스마트 사회로의 이행을 촉진하고 있다. 스마트폰, 스마트패드 등의 기기는 물론 소셜네트워크(Social Network Service), 위치기반 서비스(Location Based Service), 증강현실(Augmented Reality), 소셜커머스(Social Commerce), 스마트워크(Smart Work), 스마트TV(Smart TV), 클라우드 컴퓨팅(Cloud Computing), N-Screen, 스마트그리드(Smart Grid) 등 스마트 관련 기술과 서비스들이 홍수처럼 쏟아지면서 산업·경제 부문은 물론 우리의 일상생활 전체가 네트워크를 통해 언제(anytime) 어디서나(anywhere) 연결되는(connected) 스마트 사회로 빠르게 변화하고 있다.

우리가 정보통신 기술과 스마트 기술에 힘입어 네트워크에 연결되면 될수록 그에 따르는 잠재적 위험도 증가하고 있다. 우리를 편리하게 이끌 것으로 생각했던 스마트 혁명은 기술에 대한 인간의 민감성(sensitivity)과 취약성(vulnerability)을 심화시켜 기술이 붕괴되는 순간 대규모 위험에 노출될 가능성도 커지고 있다. 해킹에 의한 전기·통신·발전소 등 국가기반시설의 마비가 실제로 일어날 지도 모른다는 우려가 커지고 있으며, 개인정보나 기업비밀, 국가기밀 유출과 같은 보안사고의 위험이 증가하고 있다.[2] 또한 불법적으로 이루어지는 보안사고 외에도 기술의 발전으로 인해 원하지 않는 정보유출의 위험에 상시적으로 노출되는 상황을 맞고 있다. 미국의 에셜론(Echelon)이 전 세계적으로 위성통신을 통한 정보를 감청한다는 사실이 공개되었고, 스마트폰이 확산되면서 전 세계 스마트폰 사용자의 이동경로와 소비이력 정보, 생활과 생각에 대한 개인기록을 수집하는 구글(Google), 애플(Apple), 페이스북(Facebook)과 트위터(Twitter) 등 미국의 거대 통신사업자의 과도한 영향력이 확인되면서 전자감시와 프라이버시 침해에 대한 우려가 심화되고 있다.[3] 국내에서도 최근 농협전산망 마비(2011.4)나 현대캐피탈 고객정보 유출(2011.4) 등의 금융권 해킹, 네이트·싸이월드의 3500만건 개인정보유출(2011.7), (주)넥슨 해킹으로 인한 1300만명 개인정보 유출(2011.11) 등 대형 해킹사고와 개인정보 유출사건이 끊임없이 이어지고 있으며, 인터넷과 SNS 상에서 특정인에 대한 불법적인 개인정보 노출이나 해킹을 통한 집단적 인신공격이 자살로 이어지는 등 스마트사회의 보안에 관한 문제는 특정 영역이나 집단에 대한 문제가 아니라 우리 생활 각 분야에 깊숙이 자리 잡은 일부분이 되고 있다.

우리나라에서도 정보보호문제에 대한 중요성을 인지하고 다양한 기관에서 정보보호정책들을 발표하여 시행하고 있다. 정보보호와 관련된 정부부처로서 방송통신위원회. 행정안전부. 지식경제부, 국가정보원, 국가정보화전략위원회 등이 다양한 정보보호 정책을 통해 역할을 분담하고 있다. 공공기관으로서 국가보안기술연구소(NSRI), 한국인터넷진흥원(KISA), 한국전자통신연구원(ETRI) 등도 정보보호와 관련된 기술적 예방과 대응은 물론 인력 양성·교육 세부정책들을 계획·집행하고 있다. 특히, 2011년 9월 30일 개인정보보호법의 시행을 통해 그동안 문제점으로 지적되어온 정보보호 통합법제 논의에 대한 전환의 계기를 맞게 되었다.[4] 개인정보보호법을 통해 그동안 의료, 교육,

2) 교통시스템이 마비돼 순식간에 도심 사거리가 주차장으로 변하고 교통사고가 이어진다. 금융·통신·전기·가스·수도·원자력 등 기간시설 시스템 전체가 순차적으로 마비된 후 통제 불능의 상태에서 누군가의 의도에 따라 폭주한다. 지난 2007년 개봉한 헐리우드 영화 '다이하드 4.0'에서 테러리스트인 토마스 가브리엘은 컴퓨터만으로 역대 그 어떤 무기보다 더 강력한 미국의 위협이 된다. (서울신문, 2011년 6월 13일, "지구촌은 사이버 전쟁 중")

3) 2010년 "구글의 스트리트 뷰 사건"은 대표적인 예다. 구글은 인터넷 지도를 통해 특정 위치의 영상정보를 제공하는 스트리트 뷰를 서비스 중인데, 2009년 10월부터 2010년 5월까지 정보수집과정에서 무선기기 및 개인 정보 및 통신 내용 등 60만 명의 개인정보를 무단 수집한 혐의로 한국에서 구글 본사를 입건한 사건을 말한다. 애플이 아이폰이 사용자의 위치정보를 'consolidated.db'라는 이름의 숨겨진 파일에 저장한다는 사실이 드러나면서 미국에서는 애플을 상대로 민사소송은 물론, 미국 의회 차원에서 공개 질의와 청문회 조사가 착수되었다. 한국에서도 2011년 4월에 애플을 상대로 한 집단 소송이 제기되었다.

4) 이전의 개인정보보호에 관련된 법률을 살펴보면, 공공부문에서는 "공공기관의 개인정보보호에 관한 법률"이, 민간부분에서는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률", 의료분야에서는 "생명윤리및 안전에 관한 법률", "장기등 이식에 관한 법률", "응급의료에 관한 법률"이, 금융부문에서는 "신용정보의 이용 및 보호에 관한 법률"이, 교육부문에서는 "초중등 교육법"이 해당 분야들을 분산적으로 규율하여 왔다.

금융, 민간부문, 공공부문에서 각각의 개별법으로 다루어지던 개인정보 관련 사항들을 통합적으로 관리할 수 있게 되었으며, 개인정보 영향평가제도의 의무적용이나 개인정보 관리책임자(Chief Privacy Officer) 지정, 대통령 소속기구로서 개인정보보호위원회가 출범 등의 변화를 통해 정보보호의 제도화에 큰 진전이 있을 것으로 기대된다. 하지만, 정보보호 정책의 경우 유사한 정책이 관련 기관들에서 중복적으로 제안되고 있을 뿐 아니라, 각 정책들이 큰 변화 없이 매년 반복되고 있는 것이 아닌가하는 우려의 목소리가 지속적으로 제기되고 있다. 현실적으로도 정책문제의 해결을 위해서는 관련된 정책을 한꺼번에 검토하여 단기간 내 문제 모두를 해결하는 것은 부처의 시간이나 인력, 정책자원의 배분 등을 고려할 때 한계가 있을 수밖에 없다. 바람직하다고 생각되는 모든 정책대안들에 똑같은 중요도를 부여하여 자원과 인력을 분산하기 보다는 좀 더 중요하고 해결의 필요성이 높은 정책에 대해 우선순위를 부여하여 순차적으로 정책문제를 해결해 나가는 것이 바람직할 수도 있는 것이다.

이 연구는 정보통신기술의 발전과 스마트사회로의 전환에 따른 잠재적 위험으로서 정보보호 문제에 대한 정책 대응방안을 모색하는 것을 목적으로 한다. 연구방법으로 정보보호 전문가를 대상으로 한 AHP 설문조사를 사용하였다. AHP 설문은 기존의 방안들이 개선사항을 병렬적으로 나열하는 것을 보완하여, 스마트시대의 정보보호 정책에서 우선적으로 고려해야 할 과제들을 파악할 수 있는 유용한 방법이 될 것이다. 이를 위하여 기존의 정보보호 정책에 대한 선행연구와 전문가의 의견을 토대로 AHP 설문을 작성하고, 다양한 분야에 종사하는 정보보호 전문가들을 대상으로 AHP 설문조사를 실시하였다. AHP 설문의 분석은 정보보호정책 중요도와 시급성 양 측면의 분석과 함께 양 기준을 함께 고려한 종합적인 분석을 통해 최우선 정책과제 및 단기·장기정책에서 고려해야 할 정책과제들을 도출하였다.

II. 정보보호에 대한 이론적 논의와 선행연구

2.1 정보보호의 개념과 분류

먼저 정보보호의 개념과 관련하여 OECD는 1992년 11월에 발표한 보안가이드라인(Guideline for the Security of Information Systems)에서 "정보시스템 보안(security)의 목적은 정보시스템에 의존하는 자를 가용성, 기밀성, 완전성의 결여로 인한 위험으로부터 보호(protection)하는 것"이라고 정의하고 있고, 미국의 「연방정보보안관리법」 제3542조와 「컴퓨터보안법(Computer Security Act of 1987)」에서는 각각 'information security'와 'computer security'라는 용어를 사용하여 개념을 정리하고 있다[1]. 우리나라 「국가정보화 기본법」 제3조 제6호는 '정보보호'를 "정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것"으로 정의하고 있다[2]. 오흥룡 외(2005)는 정보보호와 관련된 개념으로 정보보호기술은 인터넷 등의 컴퓨터 통신망을 통하여 전달되거나 정보시스템에 저장되어 있는 정보에 대한 위조, 변조, 유출, 무단침입 등을 비롯한 각종 불법 행위로부터 조직 혹은 개인의 컴퓨터와 정보를 안전하게 보호하는 기술로 정의하고 있으며, 정보통신용어 사전에 따르면 정보보호란 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단, 또는 그러한 수단으로 이루어지는 행위로 정의하고 있다[3][4]. 김성태(2010)는 정보보호를 데이터 및 시스템을 고의적 혹은 실수에 의해 불법적인 공개, 변조, 파기 및 지체로부터 보호하는 것으로 정의하고, 협의의 정보보호를 정보통신망과 관련한 기술적 측면에서의 정보보호로, 광의의 개념으로 프라이버시 및 지적재산권 보호 등 행정·관리적 정보보호, 인적정보보호, 법률적 정보보호 등 사용자 및 이용자를 보호하는 개념으로 확대하고 있으며, 최광의로는 사이버범죄와 같은 응용프로그램에서 발생할 수 있는 행위로부터의 정보의 내용을 보호하는 것을 포함하는 개념으로 사용하고 있다. 일련의 개념정의에 따르면 정보보호란 기본적으로 정보의 생애주기나 처리과정·방법에 상관없이 정보가 가진 원래의 형태와 내용을 유지하는 것과 관련된 기술적·관리적 과정 혹은 상태라고 할 수 있을 것이다[5].이 글에서의 연구대상과 관련하여 정보보호의 범위를 사이버 상에서 발생하는 전자적 침해행위, 즉 사이버보안(cyber security)을 포함하는 최광의의 개념으로 사용하도록 한다.[5)]

정보보호는 구체적으로 정보의 기밀성(confidentiality)과 무결성(integrity), 가용성(availability) 유지를 목표로 한다. OECD(1992)의 안정성요건에

5) 사이버보안의 개념은 정보통신기반법 제2조 제2호의 '정보통신기반시설을 대상으로 전자적 수단을 활용하여 침해를 하는 행위'라는 '전자적 침해행위'와도 밀접하다.

따르면 기밀성(confidentiality)이란 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것으로 원치 않는 정보의 공개를 막는 것이다. 무결성(integrity)은 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것으로, 수신자가 정보를 수신했을 때 또는 보관된 정보를 꺼내 보았을 때 그 정보가 중간에 수정 또는 첨삭되지 않았음을 확인할 수 있도록 하는 것이다. 가용성(availability)은 허락된 사용자 또는 객체가 정보에 접근하려 하고자 할 때 이것이 방해받지 않도록 하는 것을 의미하는데, 최근의 분산서비스거부공격이 이러한 가용성을 해치는 공격의 대표적 예라 할 수 있다[6].

정보보호에 대한 다양한 개념정의에도 불구하고 정보보호 분야의 빠른 기술 변화로 인하여 정보보호 분야의 명확한 범위설정이나 하위분류 규정에 어려움이 존재한다. 정보보호의 하위 기술·기능의 분류, 직위·직무에 대한 구분이 아직 세분화되지 않은 상태이며, 최근 직무 세분화를 위한 연구들이 시도되고 있으나(김기윤 외, 2000; 전효정 외, 2009; 유혜원, 2009) 주로 기술을 중심으로 한 분류가 주를 이룬다[7][8][9]. 기술적 분류를 기준으로 할 때, 정보보호 기술은 암호·인증·생체인식 기술 등을 포함하는 공통기반기술, PC·서버·무선이동단말 등의 시스템 및 네트워크 보호기술, 웹·이메일·전자정부 보호 등의 응용서비스 보호기술, 보안성평가·정보보호정책/관리 등의 정보보호 평가 및 관리 기술의 4가지 영역으로 크게 구분된다[10].

2.2 한국의 정보보호 정책현황

2008년 옥션의 1800만 명에 이르는 개인정보 유출, 2009년 각종 정부기관과 포탈 등을 마비시킨 7.7 DDoS(Distributed Denial of Service) 사건, 2010년 3월 중국 해커 등에 의한 2000여만 건의 개인정보 불법 유출, 2011년 주요 정부기관 등을 대상으로 한 3·3 DDoS 사건, 최근의 현대캐피털과 농협과 같은 금융권의 보안사고, 네이트·싸이월드, (주)넥슨의 개인정보 유출(2011.11) 사고에 이르기까지 해킹에 따른 정보보호 침해사고의 규모와 파장이 점점 더 심각한 수준으로 커져가고 있다.[6][7][8] 2009년 한해 방송통신위원회에서 접수·처리한 민간부문 침해사고 통계에 따르면, 웜·바이러스 신고건수는 총 10,395건으로 2008년 8,469건에 비해 22.7% 증가하였으며, 해킹사고 접수·처리 건수는 총 21,230건으로 2008년 15,940건에 비해 33.2% 증가하는 등 양적으로 확대되고 있다[11].

우리나라의 경우, 정보통신 기술의 발달과 사이버상의 정보보호의 중요성이 증가함에 따라 핵심 기반이 되는 정보보호 정책이 지속적으로 이루어져왔다. 중앙행정기관 차원에서는 행정안전부, 방송통신위원회, 지식경제부, 국가정보원이 상호 간 역할 분담 및 조정 등을 통해 협력하고 있다. 행정안전부는 관련 법률에 의해 소관 정보보호 및 개인정보보호 정책임무를 담당하고 있으며, 지방자치단체의 정보보호 정책 임무와 정부통합전산센터(NCIA, National Computing Information Agency)의 국가정보자원의 관리와 운영에 관여하고 있다. 방송통신위원회는 방송통신 분야의 사이버 위협 대응과 정보보호 관련 업무를 담당하고 있으며, 한국인터넷진흥원(KISA)의 인터넷침해대응센터를 관장하고 있다. 지식경제부는 관련 법률에 의거해 지식정보보안산업의 육성 및 전문인력 양성 업무를 수행하고 있다. 또한 지식경제부는 소관 공공 기관의 통신기반시설을 보호하기 위하여 지식경제 사이버안전센터를 운영 중이며 지식정보보안산업지원센터, 바이오인식정보시험센터, KISA 아카데미를 지원하고 있다. 그 외 정보보호 관련 전문기관으로서 국가보안기술연구소(NSRI), 한국인터넷진흥원(KISA), 한국전자통신연구원(ETRI), 금융보안 연구소(FSA), 금융결제원(금융부문 정보공유·분석 센터), 코스콤(증권부문 정보공유··분석 센터), 2011년 1월에 창설된 사이버 사령부 등이 전문기관으로서 역할하고 있다[11].

6) 7·7 DDoS 공격은 2009년 7월 7일을 기점으로 대한민국과 미국의 주요 정부기관, 포털 사이트, 은행 사이트 등을 분산 서비스 거부(DDoS, 디도스) 공격하여 서비스를 일시적으로 마비시킨 사건이다.

7) 2010년 대한민국 개인정보 대량유출사건은 대한민국의 주요 사이트가 해킹을 당해 2,000만 건이 넘는 개인정보가 유출된 사건을 말한다. 이 사건은 수 년 전부터 계속 진행되었던 범죄이나, 2010년 3월에 일당이 검거됨으로 인해 큰 이슈로 번졌다. 개인정보를 팔아넘기려던 3명의 해커그룹이 2010년 3월 경찰에 검거되었으며, 이들의 진술에 따르면 직접 해킹을 하거나 중국의 해커 등으로부터 개인정보를 사들이는 등으로 자료를 획득했다고 밝혔다. 이로 인해 대한민국 국민 5명 중 2명꼴로 개인정보가 유출되었다(www.ko.wikipedia.org)

8) 3·3 분산 서비스 거부 공격은 2011년 3월 3일을 기점으로, 대한민국의 주요 정부기관, 포털 사이트, 은행 사이트 등을 분산 서비스 거부(DDoS) 공격하여 두 차례 서비스를 일시적으로 마비시킨 사건이다. 이는 2010년에 일어난 7 · 7 분산 서비스 거부 공격보다 진화된 형태이다.

정보보호와 관련된 주요 법제로는 국가정보화기본법, 전자정부법, 정보보호통신기반보호법, 정보통신산업 진흥법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등이 있으며 2011년 3월 개인정보보호법이 제정되어 시행령과 시행규칙을 거쳐 9월 30일 시행되었다.

2.3 정보보호에 대한 선행연구의 검토

정보보호 정책에 관한 연구들은 개별 쟁점이나 분야에 집중하여 접근한 연구들과 정보보호에 대한 포괄적인 정책방안이나 전략적 접근을 다룬 연구들로 나눌 수 있다.

먼저 개별 정보보호 정책에 관한 연구들은 개인정보보호와 관련된 연구들이 대부분을 차지하고 있다. 개인정보보호와 관련된 연구들은 기술개발 및 기술정책에 관한 연구(임종인, 2004)에서부터 개인정보보호를 위한 법률·제도적 방안(강신원, 2003; 최상호 외, 2005), 전자정부 환경과 유비쿼터스 환경으로의 변화에 따른 개인정보보호 방안(나종연 외, 2009; 윤상오, 2009; 정충식, 2010)에 이르기까지 다양한 관점에서 연구들이 진행되고 있다[12][13][14][15][16][17]. 정보보호 전문인력의 중요성 관점에서 인력의 양성방안을 제시한 연구들도 다수 있는데, 나현미 외(2003)는 정보보호 전문인력의 양성을 위해 국외 정보보호 자격제도 검토하고 국내 자격제도 활성화 방안을 모색하였으며, 김태성 외(2006)는 AHP를 통한 정보보호 인력의 양성방안을 살펴보았고, 김동욱 외(2011)는 공공부문 정보보호 전문인력 직무이탈 동기를 살펴봄으로써 정보보호인력의 정착과 양성을 위한 방안을 모색하였다[18][19][20].

둘째, 정보보호 정책이나 전략 연구들을 통해 정보보호 정책의 기본적인 유형이나 큰 틀을 파악할 수 있다. 신영진 외(2004)의 연구는 정보보호 정책의 우선순위를 분석하기 위한 범주로서 법률·제도적 정책, 물적·기술적 정책, 조직·관리적 정책의 세 범주로 구분하였다. 법률·제도적 정책의 경우 프라이버시 보호, 지적재산권 보호, IT 이용확산을 위한 보호로 나누고, 물적·기술적 정책은 정보보호를 위한 정보통신기반 확충, 정보보호기술기반확보, 정보보호를 위한 통신응용·관리로 나누었다. 조직·관리적 정책은 정보보호조직을 위한 운영체계 강화, 정보보호를 위한 예산확보, 행정서비스를 위한 정보보호 강화로 구분하고 있다[21]. 한국인터넷진흥원(2006)은 유비쿼터스 정보보호 기본전략 연구에서 정보보호정책을 안전한 정보 인프라 구축, IT 서비스의 신뢰기반확보, 이용자의 프라이버시 보장, 깨끗하고 건전한 정보이용환경 조성, 정보보호 기반 조성으로 나누었다[22]. 임종인(2008)은 사이버보안 강화를 위한 쟁점으로 사이버 위험과 보안에 대한 중요성의 인식, 사이버 위험관리체계의 마련, 사이버 보안 법제 및 조직의 정비, 개인정보보호제도 강화의 4가지를 들고 있다[23]. 국가정보화전략위원회의 국가정보화기본계획(2008) 중 정보보호와 관련된 건강한 사이버 구현 부문은 정보화 정책을 관리체계 구축, 사이버범죄대응, 개인정보보호, 정보문화의 4범주로 분류하고 있다. 이 중 관리체계 구축은 모니터링 기관(센터)의 설계, 사이버 신뢰도 제고 기반 및 환경 마련, 사전보안진단제 실시로 나누었으며, 사이버범죄대응은 정보보호 지원, 예방 및 대응체계 구축, 협력체계 확립으로 분류하였다. 개인정보보호는 개인정보 수집제한, 개인정보오남용 책임 및 처벌 강화, 개인정보 관리체계 개선으로 나누고, 정보문화 부문은 사이버 정의 확립, 정보보호 인식 개선, 사이버 경제 질서 확립으로 세분류하였다[24]. 부처 수준의 정보보호 정책을 살펴보면 행정안전부(2008)는 정보보호 중장기 추진방안을 통해 주요추진과제로 법제도 개선, 정보보호 종합계획 추진, 사이버침해 대응력 강화, 정보보호 기반 조성, 정보보호 인식 제고, 자치단체 사이버침해대응센터 구축, 전자정부서비스 보안수준 실태조사 및 개선대책 추진으로 나누었다[25]. 방송통신위원회의 국가사이버종합대책(2009)에서는 사이버위기 대응 주요정책으로 위해 국가기관 간 사이버관리 기능 명확화, 민간분야 사이버안전 수준 제고를 위한 사이버보안 교육 강화와 사이버 보안관 양성, 보안관제센터(ISAC) 설립을 강조하였다[26]. 유은재 외(2009)는 주요국의 사이버 보안 추진전략을 소개하면서 국가 총괄 조정기능 강화, 사이버 보안 법제도 개선, 사이버보안 기술혁신 및 연구개발 고도화, 사이버보안문화 확산의 4개의 범주를 사용하여 설명하였다[27]. 김희정(2009)은 인터넷 환경의 변화에 따른 한국인터넷진흥원의 정보보호 선진국을 위한 중점 추진과제를 정리하면서, 인터넷 기술 고도화를 통한 역량 강화, 인터넷 문화 선진화, 선진법제도 기반조성, 방송통신·인터넷의 국제화의 4가지로 분류하였다[28]. 한국인터넷진흥원(2010)의 국가정보보호백서에서는 정보보호 분야를 정보보호활동과 정보보보기반조성 분야로 나누고 있다. 정보보호활동분야로는 전자정부 정보보호활동, 주요정보통신기반시

설 보호 활동, 개인정보보호활동, 정보통신서비스제공자 등의 정보보호, 국민생활 정보보호활동, 정보보호 협력활동으로 나누고 있으며, 정보보호 기반조성 분야로는 정보보호 법제도 정보보호 교육 및 인력, 정보보호산업, 정보보호 원천기술 개발로 나누고 있다[11]. 신영진(2010)은 유비쿼터스 사회에서의 국가정보보호에 관한 연구에서 정보보호 정책에 대한 추세분석과 SWOT 분석을 통해 정보보호를 위한 관심과 투자, 정보보호 산업을 육성하는 R&D, 정보보호인력 및 정보보호인식 수준 향상을 강조하였다. 또한 정보보호수요자들을 대상으로 한 설문조사를 통해 정보보호를 위한 중장기 계획 및 미래전략의 수립, 통합적인 정보보호법의 제정과 국가 간 협력체계 구축, 대국민서비스 안전기반 마련을 정책과제로 선정하였다[29]. 서종렬(2010)은 스마트시대로의 환경변화에 따른 정보보호 부문의 중점 추진과제로서 인터넷 정책 개발과 활성화 기반 마련, 건전한 인터넷 문화와 이용환경 조성, 신속한 침해사고 대응과 선순환 구조 마련, 커뮤니케이션 패키지를 통한 국제협력 활동, 사회적 공감대 형성과 적극적인 참여를 들고 있다[30]. 김성태(2010)는

〔표 1〕 선행연구에 나타난 정보보호 정책 분류와 내용

정책	세부분류	내용	연구자
정보보호 기반 확립	법제도 기반 정비	기본 법제 정비(정보보호통합법제 마련, 정보보호관련 법제 정비, 중장기 정보보호정책 비전 및 로드맵 작성, 정보보호 예산확보), 추진체계 정비(사이버 위험 관리체계 구축, 정보보호 컨트롤타워 마련, 정보보호 리더십 강화, 부처간 조정 협의체·기구 추진)	신영진(2004), 임종인(2008), 국가정보화전략위원회(2008), 행정안전부(2008), 방송통신위원회(2009), 유은재 외(2009), 김희정(2009), 신영진(2010), 서종렬(2010), 정충식(2010), 김성태(2010), 한국인터넷진흥원(2010)
	인적 기반 정비	교육·연구 기관의 확충 및 지원(정보보호학과 확대·지원, 핵심 연구기관의 설립, 교육 커리큘럼의 강화, 학-석사 연계, 산·학·연 연계, 정보보호영재 특성화), 전문인력 처우 개선(보수의 개선, 인센티브 제도, 경력관리개선, 병역특례제도 활용, 정보보호 인력 고용 의무화, 정보보호 기능·직위 분류)	나현미(2003), 김태성 외(2006), 방송통신위원회(2009), 신영진(2010), 김성태(2010), 한국인터넷진흥원(2010), 김동욱 외(2011)
	기술적 기반 확충	H/W 기반 기술(가용성·생존성·신뢰성 높은 네트워크·시스템 기술 개발), S/W 기반 기술(보안백신 개발, 보안패치 개선, 암호화기술등 기반기술 강화)	신영진(2004), 한국인터넷진흥원(2006, 2010), 유은재 외(2009), 김희정(2009), 김성태(2010)
	사회 문화적 인식 개선	정보보호 중요성 인식(각종 홍보 강화, 민간 자정활동, 사이버 신뢰지수 등 개발, 정보보호 인식 및 문화 개선), 전문가주의인식(정보보호에 대한 전문성 인정, 전문가 우대 문화, 용어 재인식(ex. 해커->정보보호전문가))	한국인터넷진흥원(2006, 2010), 임종인(2008), 국가정보화전략위원회(2008), 행정안전부(2008), 방송통신위원회(2009), 유은재 외(2009), 김희정(2009), 신영진(2010), 서종렬(2010)
정보보호 정책 활동	주요 기반 시설 보호 활동	안전한 정보보호 인프라 구축(DDoS 대응시스템 구축, 정보보호 시설 사전진단제도, 사이버침해 대응센터 확대), 사이버 침해 사전 예방 및 대응(침해에 대한 공격탐지·차단·정비 모의훈련 및 대응 프로세스 마련, 모니터링 강화, 취약성 리포트)	국가정보화전략위원회(2008), 행정안전부(2008), 신영진(2010), 서종렬(2010), 김성태(2010), 한국인터넷진흥원(2010)
	개인 정보 보호 활동	개인정보수집제한(주민번호 대체수단 확대, 개인정보 수집절차 엄격화, 개인정보처리자 사전통지의무), 개인정보 오남용 책임 및 처벌강화(오남용에 대한 책임범위 규정, 불법 사용에 대한 형사고발 등 처벌 강화)	강신원(2003), 최상호 외(2003), 한국인터넷진흥원(2006, 2010), 임종인(2008), 국가정보화전략위원회(2008), 행정안전부(2008), 나종연 외(2009), 윤상오(2009), 신영진(2010), 정충식(2010)
	정보 보호 산업 진흥	R&D 및 사업화 지원(핵심기술에 대한 연구 지원, 기술의 제품·솔루션·서비스로 개발 지원) 표준 및 인증제 등 제도 지원(정보보호 각종 표준 마련 및 각종 보안성 평가 인증제 마련, 정보보호 투자 의무화)	신영진(2010), 김성태(2010), 한국인터넷진흥원(2010)
	국가 안보 활동	사이버전 등 대비(테러단체·북한·개인으로부터의 불법적인 사이버 위협 대비), 국가간 협력 강화(사이버 보안을 위한 국가간 협의체 구성 및 협력강화, 국제기구의 참여,)	신영진(2010), 서종렬(2010)

정보보호를 위한 대응방안을 정보보호관련 법제 및 기관, 정보보호 산업 및 인력양성, 네트워크관리 및 시스템 대책 분야로 나누어 검토하고 있다[5]. 이상의 선행연구들을 정보보호활동이 이루어지는 정책대상의 수준과 정책을 촉진시키는 기반의 종류에 따라 [표 1]과 같이 정리하였다. 먼저, 정보보호정책 활동은 정책대상의 수준에 따라 국가안보, 사회기반보호, 산업활성화, 개인정보보호의 4가지 수준으로 나눌 수 있을 것이다. 구체적 정책 활동을 촉진시키는 기반여건의 경우 법제도, 인적기반, 기술기반, 사회인식기반으로 나누어 기존의 연구들과 정책들을 재분류하였다.

하지만 정보보호 문제에 대한 다양한 정책 제안과 연구들이 이루어져 왔음에도 불구하고, 기존의 연구들은 연구의 시점이나 연구자·정책기관에 따른 큰 차이 없이 비슷한 정책들을 나열식으로 제안하고 있다는 점에서 한계를 갖는다. 따라서 이 연구는 선행연구에서 도출된 정보보호정책에 대한 분류를 토대로 전문가들의 의견을 수렴하여 각각의 정보보호정책에 가중치를 부여하여 정보보호 정책의 우선순위를 도출하고자 한다. 이를 통해 정보보호 분야에서의 현안 및 문제점을 명확히 진단하고, 나열식 정책제언의 한계를 극복할 수 있을 것이다. 구체적 연구방법으로 AHP 설문조사를 사용하여 정책중요도 및 정책시급성의 기준에 따라 정책 우선순위를 도출하였다.

III. 연구방법과 절차

3.1 AHP 개요

1970년대 초반 T.Satty에 의해 개발된 계층분석적 의사결정방법(Analytic Hierarchy Process, AHP)은 의사결정의 계층구조를 구성하고 있는 요소간의 쌍대비교에 의한 판단을 통하여 평가자의 지식, 경험 및 직관을 포착하고자 하는 하나의 새로운 의사결정방식이라 할 수 있다[31]. 그 동안 AHP 기법은 다기준 의사결정 방식으로서 OR (Operations Research)에서부터 시작하여 이후 계획과 자원배분, 갈등해소, 예측 등의 다양한 연구목적을 위해 사용되어 왔으며, 그 적용분야도 공학, 경제, 경영, 사회, 정치, 행정 등 다양한 영역에서 폭넓게 적용되어 왔다. AHP 기법은 첫째, 평가요소간의 가중치를 체계적인 계량적 절차를 통해 결정할 수 있으며, 최적대안의 선택에 있어 기존의 효용이론 혹은 통계적 의사결정에 비하여 이해가 쉽고 전문가의 주·객관적인 정보를 종합적으로 사용할 수 있다는 점, 둘째, 의사결정자들의 일관성을 판단할 수 있는 지표를 제공하며, 분석절차가 합리적 의사결정 절차와 부합한다는 장점으로 다차원 의사결정 문제에 널리 활용되어 왔다[32].

3.2 연구절차 개관

본 연구는 정보보호 정책의 우선순위에 대한 분석을 위해 AHP 설문 분석을 실시하고, AHP 설문결과를 기반으로 우리나라의 정보보호 정책의 문제점 및 앞으로의 정책 방향에 대한 대안들을 제안하고자 한다. 먼저, 본 연구는 문헌조사를 통한 자료 수집과 정보보호 전문가들의 인터뷰를 통해 AHP 설문조사를 위한 설문내용을 구성하였다. 특히, 현행 정보보호 정책의 주요현안과 문제점을 맵핑(mapping)하기 위하여 국내외 선행연구와 국내 전문가 인터뷰를 통해 설문 체계도를 구성하였다. 문헌조사는 행정안전부, 방송통신위원회, 지식경제부, 국가정보원, 한국정보화진흥원, 한국인터넷진흥원, 한국방송통신전파진흥원 등 정보보호와 관련된 기관의 정책자료, 연구논문, 보고서, 신문기사, 국외 정보보호 관련 정책자료 등을 참조하였다. 또한 정보보호 분야 전문가 5인(공무원 1인, 정보보안 실무자 2인, 정보보호학 연구자 2인)과 우리나라 정보보호 정책의 현황과 문제점들에 대한 심층인터뷰 및 회의를 진행하여 설문의 구성에 반영하였다. AHP 설문과 동일한 시기에 설문 대상자들을 상대로 개별 방문을 통한 심층 인터뷰를 실시하여 정보보호 정책에 대한 구체적인 정책 대안을 논의하였다.

설문조사는 2010년 7월 12일부터 2010년 9월 10일까지 직접방문 및 이메일을 통한 전자조사방식을 혼용하여 이루어졌다. 조사대상자 35명으로부터 35부의 설문을 회수하였으며, 그 중 설문 답변에 결측치가 있거나 일관성지수(Consistency Ratio)가 0.1을 초과하는 12부를 제외한 23부를 설문의 분석에 사용하였다. 설문분석에 사용된 대상자의 구성은 학계 4명, 언론 1명, 정보보호산업 현직종사자 2명, 국방 분야 1명, 정보보호 관련 공공기관 전문가 2명, 지방자치단체 공무원 1명, 중앙부처 공무원 12명으로 이루어졌다. 이 중 학계, 언론, 현직종사자, 공공기관 전문가의 경우 정보보호 분야에서만 10년 이상을 활동한 전문가로 구성하였으며, 공무원의 경우 현재 정보보호 정책을 주임무로 하고 관련 직무에서 10년 이상을 근무하고 있는 사무관 급 이상 국장급 고위공무원 이하 공직자를 대상으로 하였다.

이에 따라 본 연구는 다음의 절차에 따라 이루어진다. 첫째, 각종 문헌조사를 통한 이론적인 논의와 정보보호 전문가 심층인터뷰를 통해 정보보호 부문의 주요 정책쟁점을 도출한다. 둘째, 안전한 정보사회 구현이라는 정보보호 정책의 목표를 달성하기 위한 정책들을 대분류, 중분류, 소분류의 3계층으로 구분하고, 각 정책에 대해 9점 척도의 AHP 설문지를 작성하였다.[9] 단, 본 설문은 정보보호 정책의 우선순위에 있어 정보보호 정책의 정책중요도(정책이슈 및 트렌드의 사회적 파급력)와 정책시급성(해당분야의 신속한 대응 또는 지원이 필요한 이슈 및 트렌드)의 두 가지 측면으로 설문지를 구성하였다. 이는 정보보호 정책의 중요도와 현재의 정책시급성이 일치하지 않을 수도 있다는 가정에서 비롯한 것이다. 셋째, 정보보호 정책의 전략적 우선순위를 위해 학계, 산업계, 언론, 국방, 공공기관, 지자체 및 중앙부처의 정보보호 전문가들에게 AHP 설문에 대한 설명과 설문지 쌍대비교를 통해 설문지를 작성하게 하고 이를 회수하였다. 넷째, 설문분석 단계로 회수된 설문지를 엑셀 2010을 이용해 일관성 지수(Consistency Index, C.I.)를 계산하고, CI에 무작위지수(Random Index, R.I.)를 나눈 값으로 일관성비율(Consistency Ratio, C.R.)을 계산하여, CR이 0.1 이하인 설문지를 분석하였다.[10] 개별 설문지의 합산을 위해 기하평균을 사용하였고 이러한 기하평균값을 사용하여 전체 가중치를 계산하였다. 다섯째, 설문분석을 통해 우리나라 정보보호 정책의 추진 전략의 우선순위를 선정하여 도출하고, 이를 기반으로 현재 우리나라의 정보보호 정책의 우선과제를 제언하였다.

9) 9점 척도의 점수기준은 1점을 같음, 3점은 약간 중요함, 5점은 중요함, 7점은 매우 중요함, 9점은 절대 중요함으로 명기하고, 2, 4, 6, 8점은 중간척도 값으로 사용하였다.

10) AHP 기법은 의사결정요소들 간에 상대적 가중치를 추정하여 사용한다.
A·w = λmax·w. 여기서 A는 쌍대비교로 얻어진 정방행렬식으로부터 고유벡터 값을 구한 후 고유벡터 W의 각 요소를 ∑Wi로 나눔으로써 표준화된 가중치를 구한다.
일관성 지수 (Consistency Index, C.I) 공식: C.I=(λ-N)/(N-1), N은 쌍대비교의 대상수
일관성 정도 (Consistency Ratio, C.R.) 공식: C.R.=C.I/R.I
무작위 지수 (Random Index, R.I.): 경험적 자료로 얻어진 행렬의 차원별 평균무작위 지수

행렬수	1	2	3	4	5	6	7	8	9
R.I	0	0	0.58	0.90	1	1.12	1.32	1.41	1.45

3.3 AHP 구조도 작성 및 설문

3.3.1 분석의 틀

이 연구에서의 AHP 설문 구조도 작성은 선행연구를 통해 정보보호활동이 이루어지는 정책대상의 수준과 정책을 촉진시키는 기반의 종류로 대분류한 후 정보보호 정책의 쟁점과 과제들을 다룬 연구들과 전문가들의 의견을 토대로 작성하였다. 이에 따라 안전한 정보사회 구현이라는 목적을 실현하기 위한 정보보호 정책의 구성은 정보보호 기반정책과 정보보호활동정책으로 대분류할 수 있다.

정보보호 기반정책은 법제도 및 인적 기반 정비, 기술적 기반 확충, 사회적 인식 개선의 4가지 중분류로 나눌 수 있다. 먼저, 법제도 기반정비는 관련 법제의 정비와 정보보호 추진체계 정비 정책의 두 분야로 나누었다. 구체적으로 관련 법제 정비와 관련된 내용들은 중장기정보보호 정책 비전 및 로드맵의 마련, 개인정보보호법을 비롯한 기본 법제의 정비, 정보보호 업무 및 직위의 분류 세분화, 정보보호를 위한 투자·고용의 의무화 제도 등을 포함한다. 추진체계정비는 정보보호 컨트롤 타워(control tower)의 마련, 정보보호 조정협의체·기구의 구성, 강력한 리더십 발휘를 위한 정책적 방안 노력들을 포함한다. 둘째, 인적기반정비는 새로운 인력의 양성 및 기존 인력의 재교육을 위한 교육·연구기관의 확충 및 지원과 현재 정보보호 부문에 종사하고 있는 인력의 처우개선을 통한 정보보호 능력 함양 부분으로 세분하였다. 이 중 교육·연구 기관의 확충 및 지원은 정규대학교육기관에 정보보호학과의 확대·지원, 정보보호 인력의 교류, 공동 연구를 위한 핵심연구기관의 설립, 정보보호 교육 커리큘럼의 강화, 학사-석사과정의 연계, 산학연계를 통한 인턴십 강화의 정책들이 포함된다. 정보보호 업무에 종사중인 인력의 처우개선에 관한 정책은 열악한 보수체계의 개선, 각종 인센티브제도의 도입, 경력관리 개선, 실무 보안전문가 인력에 대한 병력특례제도의 활용 등을 들 수 있을 것이다. 셋째, 기술적 기반 확충과 관련된 정책은 하드웨어 부문과 소프트웨어 부문으로 나눌 수 있다. 하드웨어 기반 정책은 정보보호 관련 시스템과 네트워크의 가용성·생존성·신뢰성을 유지할 수 있게 하는 일련의 정책들을 의미하며, 소프트웨어 기반정책은 보안 백신 및 패치의 개발, 암호화 기술 등의 정책을 포함할 것이다. 넷째, 사회적 인식 개선과 관련된 정책은 정보보호 중요성의 인식 확산과 함께 전문가주

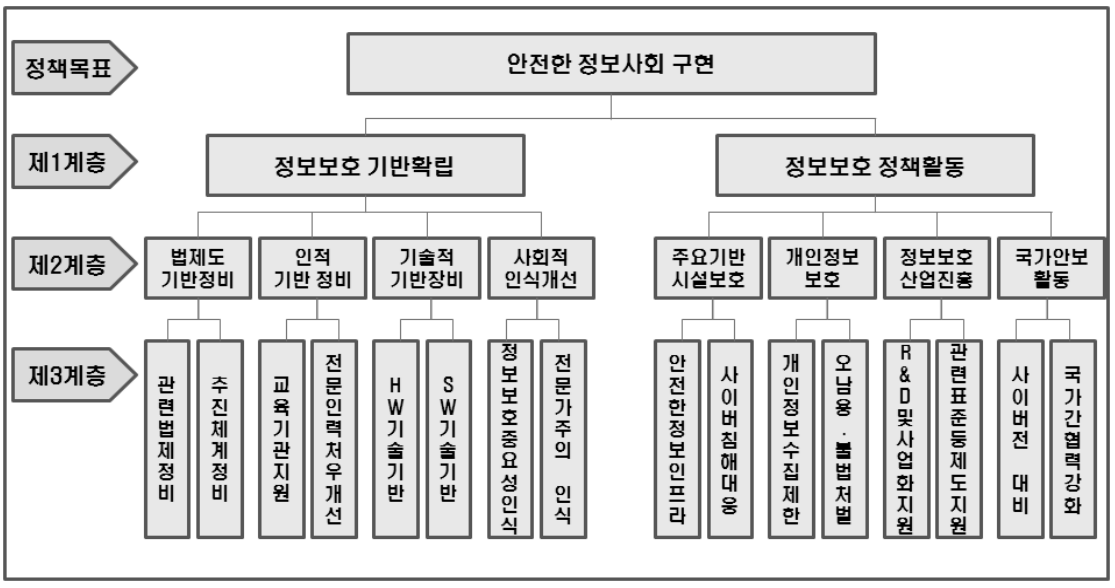
의에 대한 인식 전환을 들 수 있을 것이다. 사회적 인식 개선에 대한 정책은 정보보호의 중요성에 대한 각종 홍보 강화, 민간의 자정활동 지원, 사이버 신뢰 지수 등과 같은 객관적 지표를 통한 정보보호의 중요성 확산을 들 수 있으며, 전문가주의에 대한 인식 전환 관련 정책은 정보보호 분야의 전문성에 대한 인정과 전문가 우대 문화의 정착을 포함한다.

안전한 정보사회 구현을 위한 정보보호 정책 활동은 주요 기반시설 보호활동, 개인정보보호 활동, 정보보호산업 진흥활동, 국가안보 활동의 4가지 중분류로 나누었다. 먼저, 주요 기반시설 보호활동은 안전한 정보보호 인프라 구축 활동과 사이버 침해에 대한 사전 예방·대응 관련 정책으로 나눌 수 있을 것이다. 이 중 안전한 정보보호 인프라 구축 정책은 정보보호 시설의 설치 감리 문제, DDoS 대응 시스템의 구축 등을 포함하며, 사이버 사전 침해 예방과 대응에 관련된 정책은 침해에 대한 공격탐지·차단·정비, 대응 모의훈련 및 대응 프로세스 개발 등을 들 수 있다. 둘째, 개인정보보호 활동은 사전적 개인정보 수집 제한과 사후적 개인정보의 불법·오남용에 대한 책임 및 처벌강화로 나누었다. 사전적 개인정보 수집제한 정책은 I-Pin 등 주민번호 대체 수단의 제공, 개인정보 수집절차의 강화, 자기정보통제권의 강화, 개인정보 처리자 사전 통지 의무 등을 포함하며, 사후적 개인정보 오남용·불법처벌은 불법·오남용 행위자에 대한 처벌 및 피해자에 대한 구제방안을 담고 있다. 셋째, 정보보호산업 진흥 정책은 R&D 및 사업화 지원의 직접적 지원정책과 정보보호 관련 표준 등의 간접적 지원정책으로 나눌 수 있다. 전자에는 핵심기술에 대한 연구지원, 기술을 제품화·솔루션·서비스 등 구현하도록 하는 개발지원 정책 등이 있으며, 후자의 경우 정보보호 제품·서비스 등에 대한 표준 마련 및 각종 보안성 평가 인증제 지원을 들 수 있다. 넷째, 국가안보에 관련된 정책 활동은 사이버전에 대한 대비와 국가 간 협력 강화로 세분화시킬 수 있을 것이다. 전자는 테러단체나 북한, 블랙 해커로부터의 불법적인 사이버 위협이나 테러에 대한 대비 정책 등을 포함하며, 후자는 사이버 보안을 위한 국가 간 협의체 구성 및 협력, 국제기구 참여, 개도국과의 협력 강화 정책 등을 포함한다.

IV. 분석결과

4.1 정보보호정책 우선순위 분석: 정책중요도 측면

안전한 정보사회 구현을 위한 정보보호정책 우선순위를 정책중요도(정책이슈 및 트렌드의 사회적 파급력) 측면에서 비교 분석하였다. 먼저 〈계층 1〉을 비교한 결과 정보보호 기반확립이(0.67)이 정보보호 정책활동(0.33)보다 훨씬 더 중요한 사안이라고 전문가들은 평가하고 있다. 즉, 우리나라 정보정책에 있어 본질적인 중요성이나 향후 파급력이 큰 정책과제는 개별 분야에서 시행되고 있는 정보보호 대응 활동보다는 정



〔그림 1〕 AHP 설문 계층도

보보호기반의 정비 및 수준 향상이라고 전문가들은 판단하고 있다. 〈계층 2〉에서 먼저 정보보호 기반확립과 관련된 정책 우선순위를 살펴보면, 법제도 기반의 정비(0.39)가 가장 중요한 정책이라고 답하였으며, 인적기반 정비(0.31)와 기술적 기반확충 정책(0.152), 사회적 인식개선 정책(0.146)의 순서대로 정책우선순위를 인식하고 있다. 이는 우리나라의 정보보호 부문의 발전수준과 관련이 있는 것으로 보인다. 즉, 우리나라의 경우 ICT 기술의 발전과 정보화의 진전에 따라 시스템적 기반을 갖추는 정보화 초기 단계를 넘어, 관련 제도나 인적 기반의 재정비가 필요한 질적 심화 및 재정비의 단계라고 볼 수 있다. 정보보호 정책활동과 관련된 순위를 보면 주요기반시설보호활동(0.35)이 가장 중요한 정책으로 분석되고 있으며, 국가안보활동(0.25), 개인정보보호(0.23), 정보보호 산업진흥(0.17)의 순서로 나타나고 있다. 〈계층 3〉의 정보보호 기반확립 부분을 살펴보면, 첫째, 법제도 기반정비에서는 관련 법제정비(0.52)가 추진체계 정비(0.48)보다 약간 더 중요하다고 평가하고 있으며 둘째, 인적기반정비에서는 전문인력 처우개선(0.61)이 전문교육 기관지원(0.39)보다 더 중요하다고 제안하고 있다. 셋째, 기술적 기반확충에서는 S/W 기술기반(0.75)이 H/W 기술기반(0.25)보다 훨씬 중요하다고 평가하고, 넷째, 사회적 인식개선에서는 정보보호 인식의 확산이(0.74)이 전문가주의 인식의 확산(0.26)보다 중요한 정책으로 판단하고 있다. 〈계층 3〉의 정보보호 정책활동과 관련된 중요도를 살펴보면 먼저, 주요기반시설 보호활동 중에는 사이버 침해대응(0.54)이 안전한 정보보호 인프라 구축(0.46)보다 중요하다고 평가하고 있으며, 둘째, 개인정보 보호활동 중에는 개인정보 수집제한활동(0.60)이 개인정보 오남용책임 및 처벌 강화(0.40)보다 중요하다고 생각하고 있었다. 셋째, 정보보호산업 진흥활동 중에서는 R&D 및 사업화 지원(0.67)이 정보보호 관련표준 등의 지원(0.33)보다 중요하며, 넷째, 국가안보활동 중에서는 국가간 사이버전 대비(0.75)가 국가 간 협력 강화 활동(0.25)보다 훨씬 더 중요한 정책으로 평가하고 있다.

종합하면, 안전한 정보사회 구현이라는 정보보호정책의 정책적 중요도에 따른 정책 우선순위는 정보보호 관련 법제의 정비(0.137), 전문인력의 처우 개선(0.127), 추진체계정비(0.126)를 중요한 정책과제로 전문가들은 인식하고 있었다. 이러한 정책과제들은 주로 법제나 인적기반정비와 관련된 정책들로 정보보호 정책에 미치는 파급력이나 중요도를 고려할 때, 물적 기반을 운영·관리하는 인력이나 기본 법제, 추진체계의 정비가 우선적으로 요구된다 하겠다. 이외에도 전문교육·연구기관 지원이 4순위(0.08),

〔표 2〕 안전한 정보사회 구현을 위한 정책 우선순위: 정책중요성 기준

계층1 (대분류)	가중치	계층2 (중분류)	가중치	계층3 (소분류)	가중치	최종가중치	정책우선순위
정보보호 기반확립	0.67	법제도 기반정비	0.39	관련 법제정비	0.52	0.137	1
				추진 체계정비	0.48	0.126	3
		인적 기반정비	0.31	교육·연구기관지원	0.39	0.080	4
				전문인력 처우개선	0.61	0.127	2
		기술적 기반확충	0.15	H/W 기술기반	0.25	0.025	13
				S/W 기술기반	0.75	0.077	5
		사회적 인식개선	0.15	정보보호 인식확산	0.74	0.073	6
				전문가주의 인식전환	0.26	0.025	14
정보보호 정책활동	0.33	주요기반시설 보호활동	0.35	안전한정보보호 인프라구축	0.46	0.053	9
				사이버 침해대응	0.54	0.0615	8
		개인정보 보호활동	0.23	개인정보 수집제한	0.60	0.046	10
				개인정보 오남용책임 및 처벌강화	0.40	0.030	12
		정보보호 산업진흥	0.17	R&D 및 사업화 지원	0.67	0.037	11
				정보보호 관련표준등지원	0.33	0.018	16
		국가 안보활동	0.25	사이버전 등 대비	0.75	0.0623	7
				국가 간 협력 강화	0.25	0.021	15

S/W 기술기반(5순위, 0.077), 민간부문 인식개선(6순위, 00.73), 사이버전 대비(7위, 0.0623), 사이버 침해대응(8위, 0.0615), 안전한 정보보호인프라(9위, 0.053), 개인정보수집제한(10위, 0.046), R&D 및 사업화 지원(11위, 0.037), 개인정보 오남용 및 불법사용 처벌(12위, 0.030), H/W 기술기반(13위, 0.025), 공공부문인식개선(14위, 0.025), 국가 간 협력 강화(15위, 0.021), 정보보호 관련 표준 등 지원(16위, 0.018)의 순서로 정책우선순위가 나타나고 있다.

4.2 정보보호정책 우선순위 분석: 정책시급성 측면

안전한 정보사회 구현을 위한 정보보호정책 우선순위를 정책시급성 측면에서 분석해 본다. 먼저, 〈계층 1〉을 비교한 결과 정책시급성에 있어서도 정보보호 기반확립(0.54)이 정보보호 정책활동(0.46)보다 시급한 것으로 전문가들은 평가하고 있다. 그러나 그 차이의 정도는 중요도에 비해 상대적으로 작은 것으로 나타난다. 이것은 현재 각종 정보침해나 해킹과 같은 각종 사건들의 발생으로 인해 긴급하게 대응할 필요성이 높아지는 것과 밀접한 관련이 있을 것이다. 〈계층 2〉의 정보보호 기반확립과 관련된 정책들을 시급성 측면에서 살펴보면, 법제도 기반정비(0.40)가 가장 시급한 것으로 평가되고, 다음으로 인적 기반정비(0.29)가 시급한 것으로 제안되고 있다. 사회적 인식개선(0.17)과 기술적 기반확충(0.14)은 상대적으로 시급성 측면에서 낮은 평가를 받는데, 둘 중에는 사회적 인식개선이 보다 시급한 것으로 나타났다. 〈계층 2〉의 정보보호 정책활동 중에서 순위를 살펴보면 역시 주요기반시설 보호활동(0.34)이 가장 시급하게 필요하다고 평가하고 있으며, 다음으로 개인정보 보호활동(0.29), 국가 안보활동(0.23)이 시급하다고 평가하고 있다. 상대적으로 정보보호산업 진흥활동(0.15)은 이상의 정책 사안들보다는 덜 시급한 것으로 평가하고 있다. 특징적인 것은 중요도 측면에서는 국가 안보활동(0.25)이 개인정보 보호활동(0.23)보다 중요하다고 평가하였으나, 시급성 측면에서는 개인정보 보호활동이 국가 안보활동보다 중요하다고 제안하고 있다. 〈계층 3〉의 정보보호 기반확립 분야에서 정책 우선순위를 살펴보면, 첫째, 법제도 기반정비에서는 추진체계정비(0.54)가 관련 법제정비(0.46)보다 시급한 것으로 평가되고 있다. 이는 정책중요도 측면에서의 우선순위와 반대로 나타나는데, 현재 추진체계에서의 기능 중복이나 조정체계의 미흡과 같은 부정적 인식에서 비롯한 것으로 보인다. 둘째, 인적기반정비에서는 전문인력 처우개선(0.55)이 전문교육·연구기관 지원(0.45)보다 시급한 것으로 평가된다. 기술적 기반확충에서는 역시 S/W 기술기반(0.72)이 H/W 기술기반(0.28)보다 훨씬 시급한 것으로 평가되고 있으며, 사회적 인식개선에서는 민간부문 인식개선(0.70)이 공공부문 인식개선(0.30)보다 더 시급한 것으로 평가하고 있음을 알 수 있다. 〈계층 3〉의 정보보호 정책활동 부문의 정책시급성 순위를 살펴보면, 먼저, 주요기반시설 보호활동 중에서는 사이버 침해대응 활동(0.52)이 안전한 정보보호인프라 구축(0.48)보다 시급하다고 평가하고 있다. 개인정보 보호 정책과 관련해서는 개인정보수집제한(0.59)이 개인정보 오남용 책임 및 처벌 강화(0.41)보다 시급한 것으로 나타났다. 정보보호 산업진흥에서도 정책중요도 측면에서와 같이 R&D 및 사업화 지원활동(0.67)이 정보보호 관련표준 등 지원활동(0.33)보다 우선되어야 한다고 평가하고 있으며, 국가안보활동의 경우 사이버전 등에 대비(0.71)하는 것이 국가 간 협력을 강화하는 활동(0.21)보다 훨씬 시급하다고 평가하고 있다.

종합하면, 안전한 정보사회 구현이라는 정보보호정책의 정책적 중요도에 따른 정책 우선순위는 추진체계정비(0.116), 정보보호 관련 법제의 정비(0.097), 전문인력의 처우 개선(0.086)을 중요한 정책과제로 전문가들은 인식하고 있었다. 정책중요성 측면의 우선순위와 비교하여 추진체계정비가 현재 시급한 과제이며, 추진체계에 대한 정비가 최우선 과제임을 보여주고 있다. 이외에도 사이버 침해대응(4위, 0.081), 개인정보수집제한(5위, 0.078), 안전한 정보보호인프라(6위, 0.076), 사이버전 대비(7위, 0.074), 전문교육·연구기관 지원(8위,0.070), 민간부문 인식개선(9위, 0.063), S/W 기술기반(10위, 0.056), 개인정보 오남용 및 불법사용 처벌(11위, 0.055), R&D 및 사업화 지원(12위, 0.047), 국가 간 협력 강화(13위, 0.030), 공공부문인식개선(14위, 0.027), 정보보호 관련 표준 등 지원(15위, 0.023), H/W 기술기반(16위, 0.022)의 순으로 정책시급성에 따른 우선순위가 제안되고 있다.

4.3 정책중요도 및 정책시급성 종합 분석

안전한 정보사회 구현을 위한 우선적 정책을 정책중요도와 정책시급성 두 가지 기준을 종합하여 살펴보

〔표 3〕 안전한 정보사회 구현을 위한 정책 우선순위: 정책시급성기준

대분류	가중치	중분류	가중치	소분류	가중치	최종가중치	정책순위
정보보호 기반확립	0.54	법제도 기반정비	0.40	관련 법제정비	0.46	0.097	2
				추진 체계정비	0.54	0.116	1
		인적 기반정비	0.29	전문교육 기관지원	0.45	0.070	8
				전문인력 처우개선	0.55	0.086	3
		기술적 기반확충	0.14	H/W 기술기반	0.28	0.022	16
				S/W 기술기반	0.72	0.056	10
		사회적 인식개선	0.17	정보보호 인식확산	0.70	0.063	9
				전문가주의 인식전환	0.30	0.027	14
정보보호 정책활동	0.46	주요기반시설 보호활동	0.34	안전한 정보보호 인프라구축	0.48	0.076	6
				사이버 침해대응	0.52	0.081	4
		개인정보 보호활동	0.29	개인정보 수집제한	0.59	0.078	5
				개인정보 오남용책임 및 처벌강화	0.41	0.055	11
		정보보호 산업진흥	0.15	R&D 및 사업화 지원	0.67	0.047	12
				정보보호 관련표준 등 지원	0.33	0.023	15
		국가 안보활동	0.23	사이버전 등 대비	0.71	0.074	7
				국가 간 협력 강화	0.29	0.030	13

았다. 정보보호정책을 위해 더 큰 파급력을 가지는 정책과 현재 신속한 대응 및 지원이 필요한 정책 사이에는 차이가 있을 수 있으며, 특히 양자 간에 다른 정책 우선순위를 가질 경우 양 기준을 고려한 종합적인 고찰이 필요하기 때문이다.[11] 본 연구에서는 양 기준을 종합적으로 고려하여 정책의 우선순위를 판별하기 위하여 〔표 4〕와 같이 2x2 matrix를 구성하였다.

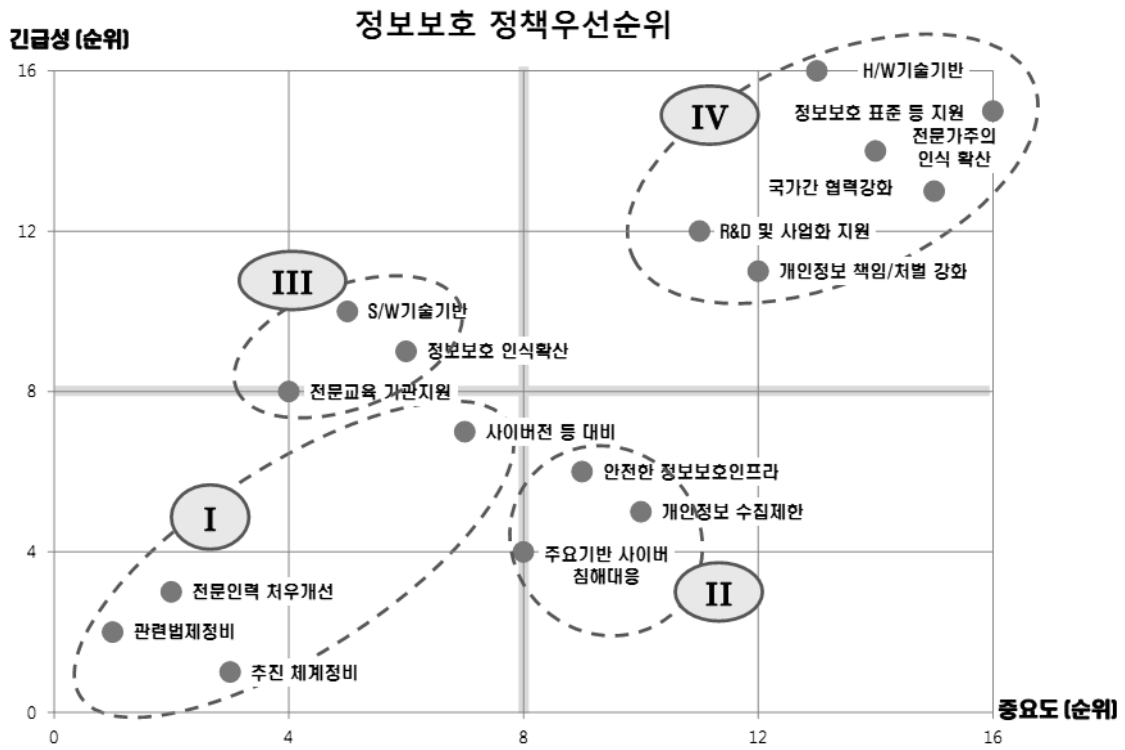
영역 I에 위치한 대안은 중요도와 시급성이 모두 높으며 장·단기 정책대안에서 가장 우선적으로 고려되어야 한다. 영역 II에 위치한 대안은 중요도는 낮으나 시급성이 높은 정책대안이다. 정보보호 정책에 있어 파급력은 낮으나 긴급한 대응이나 지원의 필요성이 높은 정책들로써 단기적 정책방안에 우선적으로 고려되어야 한다. 영역 III에 위치한 대안은 정보보호 정책 영역에서 매우 파급력이 큰 중요한 정책이나 현재 신속한 대응이나 지원의 순위는 상대적으로 낮은 정책이 해당한다. 단기적 해결의 시급성은 떨어지나 정보보호 정책에 있어 핵심적 요소로써 중장기 정책에 필수적으로 고려되어야 한다. 영역 IV의 경우 중요도와 시급성이 모두 낮은 정책들이다. 이것은 이 영역의 정책들이 필요없다는 의미보다는 다른 분야에 비해 비교적 높은 수준의 준비가 되어 있거나 앞으로도 현재와 같은 수준을 유지할 수 있도록 지속적인 노력이 필요하다는 의미로 해석될 수 있을 것이다.

정보보호 정책의 중요도와 긴급성 순위를 종합적으로 고려한 결과를 〔그림 2〕에 표시하였다. 중요도와 시급성이 함께 높은 순위를 나타낸 최우선 정책과제(영역 I)로는 관련법제정비(1위, 2위), 추진체계정비(3위, 1위), 전문인력처우개선(2위, 3위), 사이버전 등 국가보안정책(7위, 7위)이 있었다. 중요도는 낮으나 시급성이 높은 단기적 정책 과제(영역 II)로는 사이버침해대응(8위,4위), 안전한 정보보호인프라구축(9위, 6위), 개인정보 수집제한(10위, 5위)로 나타났다. 중요도는 높으나 시급성은 낮은 중장기적 정책과제(영역 III)로는 전문교육기관지원(4위, 8위), 정보보호인식확산(6위, 9위), S/W기술기반 확충(5위, 10위)이 있다. 중요도와 시급성이 모두 낮은 정책 영역 IV에는 R&D 및 사업화 지원(11위, 12위), 개인

〔표 4〕 중요도와 시급성에 따른 정보보호정책 영역 구분

시급성 낮음	영역 III 중장기적 정책과제	영역 IV 현상유지
시급성 높음	영역 I 최우선 정책 과제	영역 II 단기적 정책 과제
	중요도 높음	중요도 낮음

11) 이를 위하여 포트폴리오 분석을 사용하였다. Portfolio 분석은 세부항목에 두 가지 이상의 기준에 대한 관계를 Matrix(Portfolio map)상에 좌표로 나타내는 기법으로 전략적인 관점에서 중점 개선과제를 도출하기 위하여 다양한 분야에서 활용될 수 있다.



〔그림 2〕 정보보호정책 중요도-시급성의 종합

정보 오남용 책임 및 처벌 강화(12위, 11위), SW기술기반 강화(13위, 16위), 정보보호 표준 등 지원(16위, 15위), 전문가주의 인식확산(14위, 14위), 국가간 협력강화(15위, 13위)가 있다.

중요도와 시급성을 종합적으로 고려한 결과 다음의 몇 가지 특징이 나타난다. 먼저, 중요도와 시급성의 정책우선 순위가 비슷하게 나타나고 있다. 중요도의 순위가 높은 경우 대체로 시급성도 같이 높은 것으로 나타났다. 이는 〔그림 2〕의 경우 세부정책들의 분포가 전체적으로 우상향하는 모양을 나타내는 것으로부터 확인할 수 있다. 둘째, 정보보호 분야에 있어 전문가들이 최우선 정책으로 고려하는 사항 및 단기·중장기적으로 고려해야 할 정책의제들이 비교적 뚜렷하게 나타나고 있다. 특히 관련 법제정비, 추진체계정비, 전문인력 처우개선의 3가지 정책대안의 경우 중요도와 시급성 양 기준에서 다른 정책대안과는 비교되지 않을 정도로 높은 순위를 나타내고 있다. 따라서 정보보호의 해당 정책분야에 대해 단기정책은 물론 중장기 정책에 있어 각별한 관심이 필요하다.

V. 결론 및 제언

5.1 연구의 요약

이 연구는 최근 정보통신기술의 발전과 스마트사회의 도래에 따라 관심이 높아져 가고 있는 정보보호 분야의 정책우선순위를 전문가 대상의 AHP 분석을 통해 살펴보았다.

AHP 분석의 결과를 정리하면 다음과 같다. 정책 중요도 측면에서 정책우선순위는 정보보호 관련 법제의 정비, 전문인력의 처우 개선, 추진체계정비, 전문교육·연구기관 지원, S/W 기술기반, 민간부문 인식개선, 사이버전 대비, 사이버 침해대응, 안전한 정보보호인프라, 개인정보수집제한, R&D 및 사업화 지원, 개인정보 오남용 및 불법사용 처벌, H/W 기술기반, 공공부문인식개선, 국가간 협력 강화, 정보보호 관련 표준 등 지원 순으로 정책우선순위가 제안되고 있다. 정책시급성 측면에서는 추진체계정비, 정보보호 관련 법제의 정비, 전문인력의 처우 개선, 사이버 침해대응, 개인정보수집제한, 안전한 정보보호인프라, 사이

버전 대비, 전문교육·연구기관 지원, 민간부문 인식개선, S/W 기술기반, 개인정보 오남용 및 불법사용 처벌, R&D 및 사업화 지원, 국가간 협력 강화, 공공부문인식개선, 정보보호 관련 표준 등 지원, H/W 기술기반의 순으로 정책순위가 평가되고 있다. 정책중요도와 시급성의 종합적인 분석을 통해 중요도와 시급성이 높은 최우선 정책과제로서 정보보호 관련 법제정비, 추진체계정비, 전문인력 처우개선 등을 도출하였다. 시급성이 높은 단기적 과제로서 사이버침해대응, 안전한 정보보호인프라구축, 개인정보 수집제한을, 중요도가 높은 중장기 정책과제로서 전문교육기관지원, 정보보호인식확산, S/W기술기반 확충으로 분석되었다.

5.2 정책 제언

AHP 설문과 분석을 토대로 정보보호 부문 우선정책과제로서 정보보호 추진체계 정비, 정보보호 법제정비, 정보보호 전문인력 양성에 관한 몇 가지 정책적 제언을 하고자 한다.

먼저, 정보보호 정책 추진체계에 대한 정비가 필요하다. 지금의 행정안전부, 방송통신위원회, 지식경제부, 국가정보원의 역할 분담 체계 하에서는 일관되고 강력한 정보보호 정책이 추진되어야 할 시점에 오히려 공공조직은 물론 민간 분야에서도 정책협조의 미비로 인한 정책적 중복과 혼선을 가져올 수 있다는 비판이 높다.[12] 국가정보원이 담당하는 국가안보에 관한 부문과 나머지 행정안전부 등이 담당하는 일반 정보보호 부문과의 교류와 협력이 정보의 특성 등의 문제로 인해 기관 간 협조에 어려움을 겪고 있다. 일반 정보보호 부문에서도 부처 간 업무 협조와 역할 조정에 대해 지속적으로 논의는 되고 있지만 여전히 대대적인 정보보호 사건 등의 대응에 있어서 협조 문제가 지적되고 있는 실정이다. 특히, 2011년 개인정보보호법의 시행과 함께 설립된 개인정보보호위원회의 위상과 관련하여 위원회가 행정안전부, 방송통신위원회, 국가정보원 등 관련 부처 간의 역할·기능들에 대해서 실질적인 조정 역할을 수행할 수 있느냐가 개인정보보호법의 효과적 집행을 위해 중요한 문제가 될 것이다. 위원회 내부적으로도 간사부처 역할을 맡은 행정안전부가 실질적인 총괄기능을 맡을 경우 생길 수 있는 위원회의 독립성과 중립성 훼손 문제에 대해서는 행정안전부가 스스로 개인정보보호 평가대상 기관의 위치와 감시부처로서의 기능을 엄격히 구분하려는 노력이 필요할 것이다. 추진체계의 경우 완성된 형태가 있다기보다는 정보보호 분야 기술 발전의 속도와 폭을 고려하여 환경의 변화에 적극적이고 선제적으로 대응할 수 있도록 지속적 재정비 노력을 경주하여야 할 것이다. 미국의 경우 2009년 오바마 대통령의 취임과 함께 사이버보안에 대한 정책 검토를 통해 백악관 주도로 미래전략에 대한 추진방향의 제시와 부처별 활동 조정 업무의 수행을 명시한 바 있다[11].

둘째, 정보보호 관련 법제의 경우 국내적으로는 2011년 9월 30일 개인정보보법이 시행되면서 개인정보보호 분야의 통합적 법제가 마련되는 등 큰 성과를 거두었다. 하지만 대외적으로 정보통신 부문의 개방과 개방형 스마트 환경으로의 변화가 촉진되면서 국제 표준(global standard)을 고려한 정보보호법제 정비 필요성이 더욱 커지고 있다. 특히, 최근 스마트폰의 등장과 함께 가속화되고 있는 무선인터넷의 활성화, 소셜네트워크(SNS), 클라우드 컴퓨팅, 위치정보서비스(LBS), 스마트워크와 같은 새로운 스마트기술의 도입이나 구글, 애플과 같은 국외 사업자의 국내 진출로 인해 규제의 사각지대가 나타나고 있다. 구글의 스트리트 뷰 사건이나 애플의 개인정보수집 사건, 소니의 PSN(PlayStation Network) 사건에서 보듯 정보침해와 보호의 문제는 국경을 넘어서고 있으며, 그 침해의 불법성은 국내법으로 다루기 쉽지 않다는 문제를 안고 있다. 따라서 외국사업자의 국내 서비스 사업 과정에서 발생하는 정보보호의 문제들을 국내규범에서 어떻게 다룰 것인가를 염두에 두고 지속적인 제도개선을 해야 하며, 나아가 국내법규가 국내사업자에게만 엄격하게 적용될 경우 발생할 수 있는 국내기업과 외국기업의 역차별 문제에 대한 보완이 필요할 것이다.

셋째, 정보보호 인력의 양성에 있어 다음의 사항이 고려되어야 한다. 먼저 정보보호 인력과 관련된 기본적 제도 정비가 필요하다. 정보보호 전문인력의 수요과 공급에 대한 정확한 현황 파악, 정보보호 전문 인력의 기능·직무·등급에 대한 분류 체계 마련, 효율적

12) 방송통신위원회는 방송통신 분야의 정보보호 업무와 정보보호 침해사고 예방·대응 업무를, 행정안전부는 국가정보화와 전자정부, 공공기관의 개인정보보호, 지자체의 사이버침해 대응에 관련된 통합 업무를, 지식경제부는 지식정보보안사업 육성과 전문인력 양성 업무, 국가정보원은 국가보안과 관련된 업무 및 비상시 국가정보보호에 관한 총책 임무를, 사이버사령부는 군에서의 정보보호와 관련된 업무를 수행하고 있다. 하지만, 정보보호 분야가 가진 정보의 기밀성으로 인해 서로 간 원활한 정보 교류가 이루어지지 못하고 있다.

시장 신호기능으로서 정보보호 자격제도에 대한 정비, 고급인력의 지속적 양성을 위한 경력개발제도(CDP) 개선 등은 명확한 분류나 체계적 제도화가 부족하다. 특히, 정보보호에 기본적인 분류나 역할·기능 구분, 직무에 대한 상세한 분류기준이 없다는 점은 인력의 수준이나 수요에 대한 실질적인 논의보다는 고급인력의 부족과 인재 양성의 필요성이라는 추상적인 논의만 되풀이하게 하는 주요한 원인이 된다. 이것은 우리나라 뿐 아니라 미국 등의 정보보호 선진국에서도 겪고 있는 비슷한 문제라고 할 수 있지만 외국에 비해서 실제적인 논의수준은 상대적으로 부족하다. 미국의 경우 이러한 정보보호 인력의 수준과 기능을 체계적으로 분류하기 위한 백악관 중심의 CSIS위원회 보고서(2010), 미 연방 CIO 협의회 & 인사관리처(OPM)의 정보보보 기능 분류(2009), 국토안보부(Homeland Security)의 EBK(Essential Body of Knowledge) 분류(2008)들이 다양하게 발표되어 왔다.[13)][33][34][35]. 둘째, 전문인력의 양성에 있어 정보보호 부문의 특성을 고려한 육성 체계가 필요하다. 현재 정보보호 부문의 전문적 지식 습득과 고급화의 과정은 대학 등의 정규교육보다는 주로 자기 학습이나 폐쇄적인 소규모 그룹 활동을 통해 이루어지고 있다.[14)] 정보보호 분야 기술 변화 속도가 빨라 직업 수명도 상대적으로 짧은 반면, 암호학·네트워크·시스템·소프트웨어 지식 등 일반적인 IT 직종보다 폭넓은 종합적 지식을 요구하고 있어 육성에 걸리는 시간은 더 길다. 더구나 정보보호 시스템이나 기기의 취약성을 분석하고 관련된 프로그램 및 도구 제작까지 가능한 고급 정보보호 전문인력의 경우 그 수가 매우 제한적이며 10대 후반이나 20대 초반의 젊은 나이에 두각을 나타나게 된다.[15)] 따라서 이러한 특수한 환경에 있는 정보영재의 경우 대학 입학 등에서의 특기 인정, 군복무 기간 동안의 경력관리, 장기적인 관점에서 기술과 관리자 능력의 균형적 발전을 이룰 수 있도록 하는 교육과 경력관리가 필요할 것이다. 이와 함께 현재 해커(hacker)를 정보보호 전문가보다는 언제든 범법의 가능성이 있는 크래커(cracker)와 구분하지 않는 사회적 인식문제의 개선, 2011년 개설한 카이스트 사이버 보안연구센터와 같은 정보보호 전문가들의 연구와 교류를 지원할 맞춤형 연구공동체가 지속적으로 확대되어야 한다.

13) CSIS위원회의 경우 사이버보안 역할을 시스템보안, 네트워크 보안, 보안시스템 평가, 위협분석, Forensic 분석, s/w 보안, 시스템 개발, 전반적 시스템의 관리의 8가지로 나누고 있다. CIO 협의회 & 인사관리처(OPM)는 정보보호기능 분야를 중요도에 따라 최우선(High Priority), 중간(Medium Priority), 하위(Low Priority)로 나누고 11개의 세부 정보보호 업무를 분류하였다. 국토안보부(Homeland Security)의 EBK(Essential Body of Knowledge)의 경우 사이버 보안 관련 기본 기능을 관리, 개발, 실행, 평가의 가지로 구분하고 정보보호 직무 12가지를 4가지 기본기능을 중심으로 역할 분류하였다.

14) 정보보호전문인력 교육과 양성에 관련된 제도화가 성숙한 이후에는 정규교육을 통한 전문인력의 지속적 양성이 고급인력 양성의 주요한 통로가 될 것이다. 하지만, 정보화 전문인력 양성의 제도화가 초기 단계에 있는 현재에는 정규교육을 통한 장기적 육성과 자기학습을 통한 정보영재의 효과적 관리를 통한 양성이라는 두가지 경로(two track)를 동시에 고려하는 것이 바람직하다.

15) 우리나라 정보보호 전문인력은 그 전문성에 따라 3등급으로 구분될 수 있다. 시스템이나 기기의 취약성을 스스로 찾아내고, 창의적 신종기법을 연구가능한 A급 정보보호인력, 시스템의 공격 및 방어 기법을 알고 분석가능한 B급 전문인력, A급과 B급에서 제작된 도구와 프로그램을 사용이 가능한 C급 인력으로 분류할 수 있다. 이 중 A급은 국내 50-100명 정도, B급의 경우 2-300명 내외 C급은 약 1000명 내외로 파악된다. 이 중 A급과 B급 인력의 대부분은 자기 학습을 통해 능력을 획득하며, C급의 경우에도 정보보호에 관한 정규기관의 교육보다는 전국의 대학 동아리 활동을 통해 지식을 획득하고 있다[36]

참고문헌

[1] 이준호, "스마트모바일의 발전과 정보보안," 방송통신정책, 22(13), pp. 17-33, 2010년 7월.

[2] 법률정보시스템, "국가정보화 기본법," 2011년 7월.

[3] 오흥룡, 오세순, 김선, 염흥열, "정보보호 표준화 항목 정의 및 로드맵," 한국정보보호학회, 정보보호학회지, 15(5), pp. 67-82, 2005년 10월.

[4] 정보통신기술협회,정보통신용어사전, www.word.tta.or.kr

[5] 김성태. 신 정보정책론: 이론과 전략. 법문사. 2010년 3월.

[6] OECD, "정보시스템보안에 관한 가이드라인(OECD Guidelines for the Security of Information Systems)," 1992년.

[7] 김기윤, 나현미, "정보보호관리자에 대한 직무분석," 정보보호학회논문지, 10(3), 2000년 9월.

[8] 전효정, 김태성, 유진호, 지상호, "정보보호 분야 직무체계 개발," 정보보호학회논문지, 19(3),

2009년 6월.
〔9〕 유혜원, 김태성, “정보보호 전문인력의 경력에 따른 지식 및 기술 수요 특성,” 정보보호학회논문지, 19(4), 2009년 8월.
〔10〕 한국인터넷진흥원, 정보보호기술 표준화 로드맵, 2004년 7월.
〔11〕 한국인터넷진흥원, 국가정보보호백서, 2010년 4월.
〔12〕 임종인, “개인정보보호를 위한 기술개발 및 기술정책에 관한 연구,” 한국정보화진흥원, 2004년.
〔13〕 강신원, “개인정보보호제도와 정책이슈,” 정보통신연구진흥원〔IITA〕 학술정보 주간기술동향 1081호, 2003년 2월.
〔14〕 최상호, 이은옥, 정미란, “유비쿼터스 환경의 개인정보보호를 위한 법률, 제도적 방안,” 한국정보과학회 2005 한국컴퓨터종합학술대회 논문집(A), pp. 121-123, 2005년 7월.
〔15〕 나종연, “유비쿼터스 환경에서의 개인정보 활용 및 보호방안 연구,”한국인터넷진흥원, 2009년 9월.
〔16〕 윤상오, “전자정부 구현을 위한 개인정보보호 정책에 관한 연구,” 한국지역정보화학회지, 제12(2), pp. 1-29, 2009년 6월.
〔17〕 정충식. 2009 전자정부론, 서울경제경영. 2009년 6월.
〔18〕 나현미, 한호현, 김종배, “국외 정보보호 자격제도에 대한 현황 및 분석,” 정보보호학회지, 제13(2), 2003년 4월.
〔19〕 김태성, 전효정, “AHP를 이용한 정보보호인력 양성 정책 분석,” 한국통신학회논문지, 31(5B), , pp. 486-493, 2006년 5월.
〔20〕 김동욱·성욱준, “공공부문 정보보호전문인력의 직군이탈에 대한 연구,” 한국정책학회 2011 춘계 학술대회, pp. 237-256, 2011년 4월.
〔21〕 신영진, 김성태, “정보보호 정책의 전략적 우선순위 분석 -AHP기법을 이용한 정책비교를 중심으로-,” 한국정책학회보, 13(3), pp. 29-63, 2004년.
〔22〕 한국인터넷진흥원, “유비쿼터스 정보보호 기본전략연구,” 2006년 12월.
〔23〕 임종인, “사이버 보안 정책 및 법제도 현황,” 한국정보통신기술협회(TTA), TTA Journal, 118호, pp. 39-46, 2008년 7월.
〔24〕 국가정보화전략위원회, “국가정보화 추진계획,” 2008년 12월.
〔25〕 행정안전부, “정보보호 중장기 추진방안,” 2008년 7월.
〔26〕 방송통신위원회, “국가사이버위기 종합대책,” 2009년 9월.
〔27〕 유은재, 윤미영, “주요국의 사이버 보안 추진전략과 시사점,” 한국인터넷진흥원 CIO REPORT 제15호, pp. 2-20, 2009년 8월.
〔28〕 김희정, “인터넷 최강국, 정보보호 선진국을 위한 중점 추진과제,” 한국통신학회지(정보와통신), 27(1), pp. 28-34, 2009년 12월.
〔29〕 신영진, “유비쿼터스사회에서의 국가정보보호에 관한 연구,” 한국지역정보화학회지, 13(3), pp. 65-90, 2010년 9월.
〔30〕 서종렬, “스마트 시대의 인터넷과 정보보호 과제,” 한국통신학회, 한국통신학회지(정보와통신), 28(1), pp.29-35, 2010년 12월.
〔31〕 조근태, 앞서가는 리더들의 계층분석적 의사결정, 동현출판사, 2003년.
〔32〕 고길곤, 하혜영, “정책학 연구에서의 AHP 분석기법의 적용과 활용,” 한국정책학회보 17(1), pp.287-313, 2008년.
〔33〕 CSIS, A Human Capital Crisis in Cybersecurity: A White Paper of the CSIS Commision on Cybersecurity for the 44th Presidency, July. 2010.
〔34〕 CIO Council, Federal Information Security Workforce Development Matrix: Roles Identifications, Definitions and prioritization, Apr. 2009.
〔35〕 국토안보부(Department of Homeland Security), “Information Techology(IT) Security Essential Body of Knowledge (EBK),” Sep. 2008.
〔36〕 보안뉴스 Trusted Security Research Center(TSRC), 정보보호 전문인력에 대한 설문조사, 2010년.

〈著者紹介〉

김 동 욱 (Kim Dongwook) 정회원
1982년 2월: 서울대학교 경제학 학사
1984년 2월: 서울대학교 행정대학원 행정학 석사
1993년 9월: Ohio State University 정책학 박사
1994년 3월~현재: 서울대학교 행정대학원 교수
2011년 9월~현재: 정보통신정책연구원(KISDI) 원장
〈관심분야〉 정보화정책, 통신방송정책, 정책분석평가

성 욱 준 (Sung Wookjoon) 학생회원
1999년 8월: 고려대학교 정치외교학 학사
2008년 8월: 서울대학교 행정대학원 행정학 석사
2011년 8월: 서울대학교 행정대학원 행정학 박사과정 수료
〈관심분야〉 정보화정책, 통신방송정책, 정책과정론