국가 정보보안 이슈 및 정책방안에 관한 연구

김정덕†

National Information Security Agenda and Policies

Jungduk Kim†

요 약 새로운 정보통신기술 변화에 따른 신규 보안위협의 등장, 사이버 공격의 증가, 국내외 정보보안 관련 법규 제정 및 시행 강화 등 제반 환경 변화에 따라 정보보안에 대한 대응방법의 변화를 요구하고 있다. 본 논문에서는 디지털 경제주체로서 정부, 기업/산업, 개인, 환경 등 네 가지 측면에서 국가 정보보안을 위해 해결해야 할 이슈를 도출하고 해결방안을 제시하였다. 구체적으로 국가 정보보안 거버넌스 체계 개선 방안, 정보보안 산업 육성 및 기업보안 수준 제고 방안, 정보보안 전문인력 양성 방안, 정보보안 법·제도 정비 및 문화 형성 등 네 가지 관점에서 현황 및 문제점 분석과 주요 이슈 해결을 위한 정책 방안을 제시하였다.

주제어 : 정보보안, 정보보안 정책, 정보보안 거버넌스, 정보보안 산업, 인력 양성, 정보보안 법, 정보보안 제도, 문화형성

Abstract This study is to propose national information security policies based on the policy framework, which has four components: government, industry/company, individual, and environments. According to the framework, the four policy agenda are derived: national information security governance scheme, information security industry competitiveness and corporate security level enhancement, eco-system for security professionals, and finally related laws & regulations modification and security culture movement. Specific issues and policies in each agenda are proposed.

Key Words : national information security policy, governance, industry, professionals, laws & regulations, culture

1. 서론

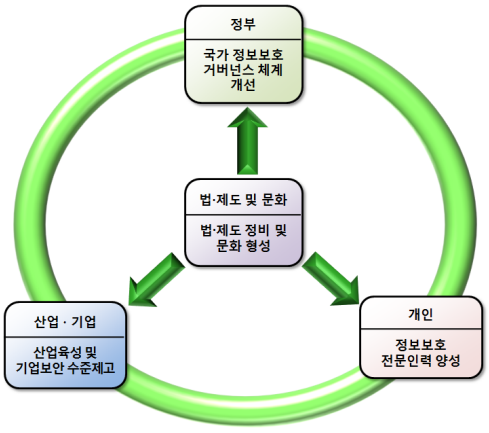
최근 모바일, 클라우드 컴퓨팅, SNS 환경 등 신규 서비스로 인한 보안위협 및 공격대상이 확대되고 공격 기법이 지능화되고 있다. 최근 2년간 75%이상의 기업이 사이버 공격을 경험 하였고, 사이버공격으로 인한 기업의 손실(피해)액은 연평균 약 23억원으로 추산되고 있다[3]. 또한, SOX, BaselⅡ, HIPPA, 개인정보보안법 등의 국내외 정보보안 관련 법규 제정 및 시행 강화 등 제반 환경이 변화함에 따라 국가 정보보안을 위한 접근방법도 달라질 필요가 있다.

국가 정보보안의 주체 별 주요 이슈는 크게 네 가지로 구분하여 접근할 수 있다. 첫 번째는 정부의 정보보안 업무처리의 중복성・비효율성 이슈를 해결해야 한다. 국가적 차원의 컨트롤 타워(Control Tower) 부재로 인한 국가 정보보안체계 기획 및 조정 기능이 저하됨을 방지하기 위한 국가 정보보안 거버넌스 체계를 개선해야 한다. 두 번째는 선진국과의 정보보안 기술 격차를 극복하고 대외 경쟁력을 보유하기 위한 정보보안 전문업체의 역량을 제고시켜야 하는 이슈이다. 또한 공공기관 및 민간 기업에서의 자율통제적인 보안관리 활동을 유도하여 보안수준을 제고할 필요가 있다. 세 번째는 정보보안 전문인력 수급간의 격차가 계속 커지고 있는 문제를 해결해야 하며 또한 전문인력의 역량도 지속적으로 개선시켜야 하는 이슈이다. 마지막으로 정보보안 관련 법률의 적용 대상 및 범위의 혼재, 정보보안 관련 평가제도의 중복, 청소년의 인터넷 오남용 및 윤리의식 희박에 따른 법・제도 정비 및 정보보안 문화 형성에 관한 이슈를 해결해야 한다.

† 중앙대학교 정보시스템학과 교수(교신저자)
논문접수 : 2012년 2월 1일, 1차 수정을 거쳐, 심사완료 : 2012년 2월 17일

따라서 본 연구에서는 국가 정보보안 정책을 [그림 1]과 같이 네 가지 관점에서 다음과 같은 정책 아젠다를 제시하였다. 즉, 정부, 산업/기업, 그리고 개인 등 경제주체 차원에서의 정책 개발과 법 제도 및 문화 등 정보보안 환경 및 인프라 차원의 정책이 필요하다. 정책 아젠다로서는 국가 정보보안 거버넌스 체제 개선, 정보보안 산업육성 및 기업보안 수준제고, 정보보안 전문인력 양성, 정보보안 법·제도 정비 및 문화 형성 등 네 가지를 포함하고 있다.

본 연구에서는 위에서 제시한 4가지 정보보안 정책 아젠다를 기반으로 각 아젠다별 현황과 문제점을 분석하고 이를 개선시킬 수 있는 정책 대안 및 실행 방안을 제시하였다. 결론부분에서는 정보보안 정책 개발을 위한 토론회의 의견수렴을 바탕으로 향후 정보보안 정책 개발에 대한 고려사항 및 향후 과제를 제시하였다.



[그림 1] 정보보안 정책 개발을 위한 프레임워크

2. 국가 정보보안 거버넌스 체계 개선방안

2.1 현황 및 문제점

현재 국가 정보보안 거버넌스 체계의 현황 및 문제점은 정부의 정보보안 업무처리의 중복성·업무영역의 모호성 등으로 인해 효과성 및 효율성이 저하되고 있다. 즉 국가 차원의 컨트롤 타워(Control Tower)의 부재로 인한 국가 정보보안 체계의 기획 및 조정 기능이 제 역할을 수행하지 못하는데 있다.

현재 정부의 정보보안 거버넌스 체계는 분권형이라고 볼 수 있다. 국가 정보보안에 대한 기획 및 조정 업무를 국가정보원이 수행하는 것을 되어 있으나, 국가보안업무 특성상 폐쇄적이고 비공개적인 업무처리 성격으로 인해 제대로 역할 수행을 하고 있다고 보기 어렵다. 특히 정부기관을 포함한 공공기관에 대해서는 국정원과 행정안전부간의 업무 중복이 발생하여 이중 규제, 중복 평가 등 공공기관에 이중 부담을 주고 있다. 또한 정보통신 관련 민간 분야를 방송통신위원회에서 담당하며, 정보보안 산업의 경쟁력 육성 및 기타 산업에서의 보안수준 제고는 지식경제부가 담당하고 있어 업무 및 책임 범위가 중복되거나 불분명한 부분이 있다.

[그림 2] 정부의 정보보안 조직 현황

또한 보안관제 중심의 사이버 침해대응 업무에 관한 국가사이버안전관리체계도 재 정비할 필요가 있다. ([그림 2] 참고). 국가 및 공공영역의 보안관제는 국가정보원의 국가사이버안전센터(NCSC)가 총괄적 책임을 지고 민간영역의 보안관제는 방통위의 인터넷침해대응센터(KISC), 전자정부영역은 행안부의 정부통합전산센터(NCIA), 국방영역은 국방부의 사이버사령부가 담당하며 기타 20여개의 주요부터 보안관제센터가 관제업무를 수행하고 있다. 그러나 NCSC와 민간분야 (ISP, 보안전문업체, 금융기관 등)과의 정보공유체계가 부실하고 이로 인해 사이버 침해에 대한 책임회피 현상이 발생하고 있다. 또한 행안부의 영역과 국가정보원의 영역이 중복됨에 따라 대상기관의 불만이 증가하고 보안업무 효율이 저하되는 문제가 발생하고 있다. 사이버 침해 발생시 검찰, 경찰의 수사 개시되는 시점에 민관 합동조사반의 조사권이 중단되는 사태가 발생하여 침해에 대한 신속한 대응에 제한이 있다. 사이버전에 대한 위협이 점차 증대되는 현 시점에서 민, 관, 군 별로 독립된 대응체계로는 한계가 있으며 전 국가적 차원의 사이버전 대응체계가 필요하다.

[그림 3] 정부의 정보보안 조직 현황

2.2 정책대안과 실천방안

위의 문제를 해결하기 위한 정책대안과 실천방안은 크게 연반형(Federal) 거버넌스 체계 구축 및 보안 분야 간 통합·조정이다. 연방형 거버넌스 체계 구축을 위한 방안은 세 가지로 들 수 있다. 첫 번째로 청와대나 국무총리실 산하에 정보보안 기획, 조정 및 통제 기능을 수행하는 상근 조직을 신설하는 것이다. 상근 조직의 주요 역할은 정보보안 관련 활동의 심의 의결, 조사·감독 등 실행력을 보유하며, 민·관·군을 모두 포함하는 국가적 차원의 정보보안 컨트롤 타워 역할을 수행하도록 해야 할 것이다.

두 번째로는 국가 사이버 대응체계의 통합을 통해 효율적인 사이버 침해사고와 사이버전(cyber war)에 대처해야 할 것이다. 즉 NCSC, KISC, NCIA(일부)에 분산되어 있는 사이버 대응체계를 일원화하여 효율성을 극대화하고 사이버전에 대한 대응체계는 국방부와 국정원의 협력 하에 사이버 작전체계를 구축하는 것이다. 물론 이 두 체계는 앞에서 언급한 국가 정보보안 컨트롤 타워의 통제하에서 협력과 조정이 되어야 할 것이다.

국가 정보보안 거버넌스 체계를 해결하기 위한 구체적 실천 방안으로 다음과 같은 두 가지를 제안할 수 있다.

먼저 정보보안 분야의 중복성 제거하고 통합 및 융합을 통한 효과성 및 효율성을 극대화하는 방안으로서 물리보안과 정보(사이버)보안의 통합과 정보보안과 개인정보보호와의 융합이 필요하다. 특히 최근 주요 위협으로 대두되고 있는 국가 기반시설보호를 효과적으로 수행하기 위해서는 물리보안과 사이버보안이 분리될 수 없기 때문이다. 또한 개인정보보호와 정보보안의 업무는 상호 중복되는 부분이 상당부분 존재하므로 이를 융합적으로 추진할 수 있는 체계가 필요하다.

다음으로 정보보안과 개인정보를 포함하는 정보보안 전문기관을 재편성 하는 방안인데 현재 개인정보보안 담당 전문기관이 NIA와 KISA로 구분되어 개별 수행되고 있는데 이에 대한 단일화 작업을 고려할 필요가 있다.

위의 정책대안 및 실천방안으로 국가 정보보안 거버넌스 체계를 개선한다면, 국가 정보보안 자원의 효율적 사용, 정보보안 업무 기능의 효과성 증대 및 정보보안 사이버침해 대응능력 증대 등의 효과가 기대된다.

3. 정보보안 산업육성 및 기업보안 수준 제고 방안

3.1 현황과 문제점

산업 또는 기업 차원에서의 정보보안 정책은 크게 공급측면에서 정보보안 산업의 경쟁력 제고와 수요측면에서 기업의 보안수준 제고로 요약할 수 있다. 국내 정보보안 산업의 경쟁력은 컨텐츠 보안 분야의 기술 경쟁력은 어느 정도 우위를 보이고 있으나, 네트워크 보안 및 보안관리 기술 분야는 선진국에 비해 열세를 보이고 있다[4]. 그리고 물리보안 분야에서는 CCTV, 바이오 인식 제품 등의 전반적인 기술 경쟁력은 우위이나 미래 핵심원천기술 분야의 보완이 필요하다.

이러한 기술경쟁력 외에 국내 보안시장의 협소로 인해 해외시장으로의 진출이 산업육성을 위한 주요 정책으로 대두되고 있다. 문제는 대외경쟁력을 가지고 있는 분야를 선택하고 이에 대한 적극적 지원이과 역량강화가 필요하다.

일반 민간 기업이나 공공 조직에서의 정보보안 수준 제고를 위해서는 새로운 패러다임의 변화가 필요하다. 기업이나 조직의 정보보안을 위한 자발적 노력이 아직도 상당히 미흡하다. 국내 기업의 85.5%가 정보보안 전담조직 미 운영과 같은 지속적인 정보보안관리를 위한 점담부서가 부족하다[5]. 또한 정보보안 업무를 책임지는 CSO나 CISO가 형식적으로 운영되거나 임명조차 안 된 기업도 상당부분 있다. 즉, 기업에서의 정보보안 지시 및 통제를 담당하는 거버넌스 체계가 아직 구축되지 않아 보안투자 및 성과평가 등 비즈니스와 연계된 보안활동이 수행되고 있지 않으며 아직도 대부분의 기업이 임시방편

적인 기술적 대응활동으로 보안관리 활동을 수행하고 있다. 또한 기업 정보보안을 지원하기 위한 정부의 정책에도 많은 부분 수정 보완되어야 할 필요가 있다. 즉 관련 평가 및 인증제도 상에서 중복 규제가 존재하며 또한 제도의 효과성에 대한 면밀한 검토로 제도 개선의 노력이 필요하다. 특히 기업의 자율통제(self-control) 역량을 함양하고 보안수준 제고를 위한 당근과 채찍 정책에 대한 재검토가 필요하다.

3.2 정책대안과 실천방안

국내 정보보안 산업의 대내외 경쟁력 강화를 위한 정책대안으로는 '선택과 집중' 전략을 채택하여 기업의 역량을 제고하고 또한 해외시장 진출에 도움을 주어야 할 것이다. 국내 보안산업의 경쟁력에 대한 보다 면밀한 평가가 있어야 하나, 국내 기술여건을 고려해 볼 때 보안 원천기술에 대한 경쟁력보다는 상대적으로 경쟁력이 높은 SI(Security Integration)산업에 보다 집중적인 지원과 기술개발 정책이 요구된다. 특히 국제적으로 인정받고 있는 전자정부 보안 등 과 같은 분야를 육성하고 지원해야 할 것이다. 또한 급속한 시장 성장이 예견되는 보안관제, 보안컨설팅, 보안운영 등 제3의 전문업체기관에서 보안서비스를 제공하는 MMS(Managed Securirty Service) 또는 ISaaS(Information Security as a Service) 분야에 대한 지원 정책을 검토할 만하다.

또한 글로벌 보안기업과 경쟁하기 위해 M&A를 통한 산업구조의 전문화・대형화를 유도할 수 있는 제도적 지원방안도 고려할 필요가 있다. 물론 M&A는 업계의 필요성과 자발적 의지로 수행되어야 하나, 인센티브 제공, 입찰 조건 제한 등 정책적으로 이를 유도할 수 있는 방안 개발이 필요하다.

기업의 보안수준 제고를 위해서는 과거의 일률적인 체크리스트 방식의 평가제도에서 기업의 특성을 반영한 위험관리에 기초하고 자율적 통제 활동을 유도할 수 있는 정보보안관리체계 구축 및 인증제도를 확대할 필요가 있다. 이를 위해 인센티브 제공을 포함한 활성화 정책과 관련 교육 및 지침 제공 등 자체 역량을 함양할 수 있도록 지원 정책이 요구된다. 특히 평가 제도를 수행하는 정부기관 입장이 아닌 평가대상 기관이나 기업 입장에서 효과적이고 효율적인 제도 개선을 위한 노력이 필요하다. 즉 보안 관련 제 평가나 인증제도에 대한 전반적인 재 검토와 개선 노력이 요구된다. 또한 최고 경영층의 정보보안에 대한 역할과 책임을 강조하는 정보보안 거버넌스 지침 개발 및 보급을 통해 자율적 보안활동을 가능하게 해야 한다. 참고로, 일본은 이미 2008년 관련 지침을 개발 보급하여 자율통제 환경을 조성하고 있다[8].

4. 정보보안 전문인력 양성을 위한 생태계 구축 방안

4.1 현황과 문제점

양질의 정보보안 전문인력 부족은 매우 시급하며 중대한 이슈라고 할 수 있다. 관련 현황 및 문제점으로는 정보보안 전문인력 수급간의 격차 존재, 국가공인 정보보안 자격 제도 미비, 국내 정보보안 교육 프로그램 미흡 등 세 가지 측면에서 분석할 수 있다.

첫째, <표 1>과 같이 정보보안 전문인력의 수급간의 격차는 향후 계속 벌어지고 있음을 알 수 있다. 정보보안 분야의 다양화 및 규모의 성장이 이루어짐에 따라, 관련 업무를 수행할 정보보안 전문인력에 대한 수요가 증가하고 있다. 또한 정보보안 전문인력의 신규 공급은 점차 늘어나지만 수급간의 격차가 여전히 존재하여 공급 부족으로 인한 어려움이 계속될 것이라 예측 된다 [6].

〈표 1〉 정보보안 인력 수요 및 공급 전망

연도	취업자수	신규수요	신규공급	수급차
2010	6,221명	533명	264명	-269명
2011	6,688명	532명	284명	-248명
2012	7,151명	533명	308명	-225명
2013	7,766명	689명	333명	-356명
2014	8,397명	712명	367명	-345명
2015	9,046명	737명	405명	-332명
2016	9,715명	764명	447명	-317명
2017	10,407명	793명	496명	-297명
2018	11,123명	825명	550명	-275명

* 출처 : 지식정보보안분야 인력현황 및 중장기 인력수급 전망 분석(2010)

둘째, 국가공인 정보보안 자격제도가 존재하고 있지 않다. 정보보안관련 자격 제도는 국내 자격증으로 정보보안전문가(SIS), 산업보안관리사 등 다수가 존재하며 국제 자격증으로 정보시스템보안전문가(CISSP), 정보시스템감리사(CISA), 정보보안관리자(CISM) 등이 있으나

국가 자격증은 아직 존재하지 않고 있다. 전문인력에 대한 국가 자격증의 미비로 자격증에 대한 공신력 부족과 함께 전문인력 공급 창출에도 기여하지 못하고 있다. 따라서 민간 자격제도가 아닌 국제공인 자격 제도 설립의 필요성이 증대되고 있다.

셋째, 국가적인 정보보안 전문인력 양성을 위한 교육 프로그램이 부재하다. 전문인력이 공통적으로 습득해야 하는 지식분야에 대한 정의도 없으며, 이를 교과과정으로 연계할 수 있는 표준적 방안도 미흡한 상황이다. 또한 교육기관도 수도권 인구 억제 정책으로 인해 정보보안학과는 대부분 지방에 소재하고 있으며 전문 대학원은 수도권 소재 1~2개에 편중되어 있어 인력체계 공급 상 구조적 문제가 있다.

4.2. 정책대안과 실천방안

위의 문제를 해결하기 위한 정책대안과 실천방안은 크게 정보보안 필수요구지식(EBK: Essential Body of Knowledge) 개발을 통한 정보보안 융합전공 인증 프로그램 도입과 정보보안 인력양성을 위한 생태계 구축 등 두 가지 정책대안을 제시한다.

정보보안은 융합적 학제간 학문 분야로서 접근해야 한다. 즉 정보보안을 정확히 이해하고 구축하기 위해서는 보안기술 이해 및 개발을 위한 컴퓨터 공학분야 지식이 필요하며, 또한 기업 내 보안관리 업무를 수행하기 위한 기획, 성과평가 등 경영/경제학 분야의 지식과 더불어, 관련 법, 규정에 대한 이해를 위한 법학 분야의 지식까지 요구된다. 따라서 융합학문으로서 정보보안에 대한 교육 프로그램이 개발되어야 하며 그 결과 균형 잡힌 전문인력을 양성할 수 있을 것이다. 참고로 미국에서는 국가안보국(NSA)과 국토안보부(DHS)가 중심이 되어 학제간 성격을 갖는 정보보안 교육 프로그램을 개발하고 이를 인증함으로써 인력양성을 위한 기반구조를 구축하고 있다. 현재 이러한 인증프로그램에 가입된 140여개의 대학/대학원 재학생과 졸업생에게 장학금 지급, 공공기관 우선 채용 등 많은 인센티브를 제공하고 있다[7].

정보보안 융합전공은 대학 내 연계전공과 유사한 형태로 정원 확보에 대한 부담이 없으며 따라서 수도권정비계획법 등 수도권 내 정보보안학과의 신설에 따른 정원 확보의 어려움을 해결할 수 있다. 대학 내 정보보안 융합전공 구축 및 운영을 활성화하기 위해서는 객관적 전문기관이 교육/연구 프로그램을 인증하고 주기적으로 재평가함으로써 지속적으로 양질의 전문인력 양성을 유도할 수 있는 시스템을 구축해야 할 것이다. 이를 위한 전제조건으로 정보보안 전문인력의 필수요구지식(EBK)을 개발하여 보급할 필요가 있다[1].

정보보안 전문인력 양성을 위해서는 공급 측면에서의 노력만으로는 부족하며 수요 측면까지 포함하여 자생적으로 수급 격차를 조정할 수 있는 생태계 구축이 필요하다. 즉 수요 측면에서의 인력수요 확대에도 노력해야 한다. 이를 위해서는 민간기업이나 공공기관에서 CSO/CISO 임명을 의무화 또는 권고하고 전담인력으로 구성된 정보보안팀이 활동하는 경우, 제반 평가에서 높은 평점을 받을 수 있도록 유도하는 것이 필요하다. 또한 전문인력의 지속적 역량 개선을 위한 교육기관, 민간 업체 또는 전문기관에서 운영하는 교육 프로그램에 대한 지원도 고려해야 한다. 기존 관련 자격증제도를 통합 발전시켜 국가자격증제도로 승격하는 것도 필요하다

5. 정보보안 법·제도 정비 및 문화 형성 방안

5.1 현황과 문제점

정보보안 법・제도와 정보보안 문화 등 환경적 차원에서의 현황 및 문제점은 관련 법률의 적용 대상 및 범위의 혼재, 정보보안 관련 평가제도의 중복, 기업의 정보보안에 대한 부정적 인식 등 세 가지 이슈로 요약할 수 있다.

현재 정보보안에 관한 법률로서 정보통신망 이용촉진 및 정보보안 등에 관한 법률, 정보통신기반보호법, 신용정보의 이용 및 보호에 관한 법률, 전자서명법, 위치정보의 보호 및 이용 등에 관한 법률 등 여러 개별법이 있으나 국가 전체에 적용되는 일반법이 부재함에 따라 법률 적용의 사각 지대가 발생할 수 있으며 개별법 간의 상이한 기준으로 인한 충돌이 발생되기도 한다. 현재 개인정보보호법은 일반법으로서 2011년에 제정됨에 따라 비교적 위와 같은 문제는 상쇄되었다고 하나 정보보안에 있어서는 일반법이 없으므로 새로운 국가 정보보안 거버넌스 체계를 반영한 일반법 제정을 고려할 필요가 있다.

둘째, 정보보안 관련 유사 평가 및 인증제도의 중복에 따라 대상 기관의 혼란과 업무 부담 가중 등 부작용을 해결해야한다. 정보보안관리체계(ISMS), G-ISMS, 개인정보관리체계(PIMS) 등 유사한 인증제도가 존재하나 상호

다른 인증체계를 가지고 있어 대상 기관에 혼란을 발생시키고 있으며 부담을 가중시킬 우려가 있다.

마지막으로 기업의 정보보안에 대한 부정적 인식이나 오해가 아직도 상당부분 존재한다고 할 수 있으며, 일반 개인도 정보보안에 대한 책임 의식 등이 아직도 미흡하다고 할 수 있다. 정보보안을 관련 법률이나 제도에 대한 컴플라이언스 이슈로만 간주하여 조직 특성에 맞는 정보보안 체계 구축 등 자발적인 노력이 미흡하며 최고 경영층의 정보보안활동에 대한 투자 및 관심이 부족하다는 것이다.

5.2. 정책대안과 실천방안

위의 문제를 해결하기 위한 정책대안과 실천방안은 크게 정보보안 일반법 제정, 정보보안 평가제도의 정비, 인터넷윤리 등 정보보안 문화 확산 등으로 구분할 수 있다.

정보보안 일반법 제정은 적용범위를 국가 전체를 대상으로 하고 새로운 국가 정보보안 거버넌스 체계를 반영하며 필수적인 평가제도 등을 포함함으로써 국가적 정보보안 수준 제고를 목적으로 해야 할 것이다.

정보보안 평가제도의 정비는 평가제도간의 중복되는 분야에 대해 평가 및 심사 기준을 통일하고 동일한 항목에 대한 면제조치 등을 통해 상호 운영성 등을 보장하고 비효율성을 해소해야 할 것이다. 또한 일회성 평가나 인증으로 보안수준 측정을 하는 인증제도가 아닌 지속적인 정보보안 관리를 유도할 수 있는 평가제도 설계 및 재정비 작업이 요구된다.

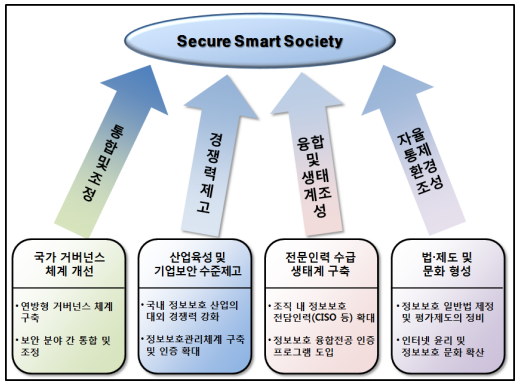
마지막으로 대국민 또는 대기업에서의 정보보안 문화 확산을 위한 실천방안으로는 강제적·의무적 준수가 아닌 자발적 준수와 정보보안 인식제고를 위한 홍보활동 강화가 필요하다. 또한 인터넷 사용과 관련된 청소년의 희박한 윤리의식을 제고할 수 있는 교육에 대한 지원도 필요하다. 특히 대학에서 인터넷 윤리에 대한 교양 교육을 권고하도록 유도하는 방안을 강구할 필요가 있다.

6. 결 론

본 연구에서 도출한 국가 정보보안 정책대안의 타당성 검토를 위해 정성적 연구방법 중 하나인 포커스 그룹 인터뷰를 실시하였다. 정부 및 공공기관과 산업계 등 관련 전문가들로 구성된 정책대안 토론회를 거쳐 의견수렴 과정을 거쳤다. 회의 중재자(김정덕 교수)의 진행 하에 도출된 방안에 대한 다양한 의견을 수렴하였으며 이를 반영하여 새롭게 정책대안을 추가 및 수정하였다. 전문가들은 제시된 정보보안 정책대안에 대하여 모두 동의하였으나 실제 정책을 수립하고 구현하기 위하여 구체적인 계획 및 정책 대상자로부터의 폭 넓은 의견수렴이 필요하다는 의견이 있었다. 더불어 정보보안 정책대안을 홍보하고 추진하는 전담 기구 설립의 필요성에 대한 의견을 도출하였다.

본 연구에서는 정보보안 정책 개발 프레임워크를 기반으로 국가 정보보안 거버넌스 체계 개선, 정보보안 산업 육성 및 기업보안 수준 제고, 정보보안 전문인력 양성을 위한 생태계 구축, 정보보안 법·제도 정비 및 문화형성의 정책 개발 방안을 구체적으로 제시하였다.

즉, 연방형(Federal) 거버넌스 체계 구축 및 보안 분야간 통합 및 조정을 통하여 국가 정보보안 거버넌스 체계를 개선해야 한다. 그리고 국내 정보보안 산업의 대외 경쟁력 강화와 기업 내 정보보안관리체계 구축 및 인증 확대를 통하여 정보보안 산업 육성 및 기업보안 수준 제고를 해야 할 것이다. 또한 조직내 정보보안 전담인력 확대 및 정보보안 융합전공 인증프로그램 도입을 통하여 정보보안 전문인력 양성을 위한 생태계 구축을 해야 한다. 마지막으로 정보보안 일반법 제정 및 평가 제도의 정비와 인터넷 윤리 및 정보보안 문화 확산을 통하여 보다 안전하고 스마트한 지식정보화 사회를 달성해야 할 것이다([그림 4] 참고).



[그림 4] 정보보안 정책대안

본 논문에서 제시한 정책대안에 대한 실효성을 얻기 위해서는 제시된 정책대안에 대한 심층연구와 이해관계

자간의 이해조정 및 의견수렴 과정이 필요하다. 둘째, 정보보안 정책 제안을 구체화하기 위한 세부 추진계획이 보완되어야 할 것이다.

참 고 문 헌

[1] 김정덕, 백태석(2011). 정보보호 전문인력 양성을 위한 필수요구지식 및 교육인증 프로그램, 디지털정책연구, pp. 113-121.

[2] 김태성, 전효정(2003). 정보보안인력 양성정책 분석. 한국디지털정책학회. pp 8

[3] 시만텍(2010), 2011년 기업현황 보고서..

[4] 한국기술산업편가관리원(2010), IT산업원천 기 술수준조사.

[5] KISA(2010). 2010년 정보보안 실태조사

[6] KISA(2010). 지식정보보안분야 인력현황 및 중장기 인력수급 전망 분석. pp. 36-41.

[7] NICE(2011),"National Initiative for Cybersecurity Education Strategic Plan"

[8] ISO/IEC 27014(2011), Governance of Information Security, DIS

김 정 덕

· 1979년 2월 : 연세대학교 정치외교학과 학사
· 1981년 8월 : 연세대학교 경제학과 석사
· 1986년 5월 : University of South Carolina, MBA
· 1990년 12월 : Texas A&M University, Ph. D. in MIS
· 1995년 3월 ~ 현재 : 중앙대학교 정보시스템학과 교수
· 관심분야 : 정보보호관리/거버넌스, 시스템감리, IT 전략/관리
· E-mail: jdkimsac@cau.ac.kr