정보보호관리 분석 프레임워크를 활용한 국외 정보보호관리 제도 및 정책 분석

정재훈*, 최명길**
*중앙대학교 경영대학
**중앙대학교 사회과학대학
e-mail : selpine@naver.com

An Analysis of Foreign Information Security Management system and policy using Information Security Management analysis framework

Jae-Hun Jeong*, Myung-Gil Choi**
*College of Business Adminstration, Chung-Ang University
**College of Social Sciences, Chung-Ang University

요 약

정보기술에 대한 투자규모는 날로 증가하고 있다. 국내 공공 부문의 경우에도 전자정부 구현 등을 위한 다양한 사업으로 인해 투자가 지속적으로 증가하고 있다. 이런 정보화 투자의 증대에도 불구하고 정보화의 효과에 대해서는 아직도 많은 의문이 제기되고 있다.

특히 S/W 취약성으로 인해 보안 침해사고가 발생하고, 정보화 관련 법제도 미흡으로 보안강화 노력이 강구되지 못하였으며 국가정보화의 새로운 틀이 마련되는 시점에서 법제도의 정비가 필요해졌다. 이러한 부분을 보완하고자 정보보호관리(Information Security Management : ISM)라는 제도를 분석한 프레임워크가 개발되었고, 본 논문은 이를 활용하여 국외 정보보호관리 제도 및 정책을 분석하고자 한다.

ISM은 주체별로 역할과 책임을 명확하게 하고, 정보화의 목표를 조직목표에의 기여로 정하여 체계적으로 추진하되, 정보보호 보안 프로그램의 적합성과 구현 및 평가/개선을 하려는 핵심추진 노력이 필요하고, 아울러 이런 노력은 현재의 모습에 만족하지 말고 보다 나은 대안과 효과적 수단을 지속적으로 강구하려는 자세 등이 주요한 특징에 속한다. 본 논문을 통하여 분석된 국외 정보보호관리 제도 및 정책은 향후 우리나라의 정보보호관리 제도 및 정책에 상당한 영향을 미칠 것으로 기대된다.

1. 서론

우리나라의 정보시스템은 현재 S/W취약성으로 인한 보안침해사고 발생의 증가 및 정보화 관련 법제도의 미흡으로 인한 보안강화 노력이 강구되지 못하고 있다. 또한, 국가정보화의 새로운 틀이 마련되고 있는 시점에서 법제도의 정비가 이루어지고 있다. 이러한 상황에서 정보시스템 개발 프로세스 전반에 대한 S/W 프로그램 내의 취약성 점검의 필요성이 등장하게 되었다. 이에 본 연구에서는 정보시스템 보안강화체계 적용을 위한 국외 정보보호관리 제도 및 정책을 분석하려고 한다.

컴퓨터 기술의 발달과 S/W 취약성으로 인하여 정부·공공기관에 대한 해킹시도와 사고발생이 지속적으로 이루어지고 있다. 또한 전자정부 서비스의 고도화에 따라 사이버 위험도가 증가하고 있다.

기존의 많은 연구조사에서 나타나듯이, 정보시스템 S/W의 취약성이 이러한 보안침해사고의 공격대상이 되고 있다. 이에 S/W 개발 프로세스 전반에 걸친 취약성 점검의 중요성이 대두되고 있다.

2. 정보보호관리제도 분석을 위한 프레임워크

정보기술에 대한 투자규모는 날로 증가하고 있다. 국내 공공 부문의 경우에도 전자정부 구현 등을 위한 다양한 사업으로 인해 투자가 지속적으로 증가하고 있다. 이런 정보화 투자의 증대에도 불구하고 정보화의 효과에 대해서는 아직도 많은 의문이 제기되고 있다.

특히 앞서 언급한 바와 같이 S/W 취약성으로 인해 보안 침해사고가 발생하고, 정보화 관련 법제도 미흡으로 보안강화 노력이 강구되지 못하였으며 국가정보화의 새로운 틀이 마련되는 시점에서 법제도의 정비가 필요해졌다. 이러한 부분을 보완하고자 정보

보호관리(Information Security Management : ISM)라는 제도를 분석하고자 한다. ISM은 주체별로 역할과 책임을 명확하게 하고, 정보화의 목표를 조직 목표에의 기여로 정하여 체계적으로 추진하되, 정보보호 보안 프로그램의 적합성과 구현 및 평가/개선을 하려는 핵심추진 노력이 필요하고, 아울러 이런 노력은 현재의 모습에 만족하지 말고 보다 나은 대안과 효과적 수단을 지속적으로 강구하려는 자세 등이 주요한 특징에 속한다.

[표 1]은 이 정보보호관리의 특성을 보다 세부적으로 묘사한 것이다. 여기서 제시된 정보보호관리의 특성은 차후 국외 관련 법, 제도의 분석 및 운영체계의 분석에도 그대로 활용될 예정이다.

[표 1] 정보보호관리 제도의 특성

ISM 요소	ISM세부 요소	내 용
역할과 책임의 명확화	감독 및 조정기관의 역할과 책임	* 정보보호 강화를 위해 어느 기관이 감독 및 조정 역할을 수행하여야 하는가?
	보안에 관한 기관장의 책임과 역할	* 정보보호 보안에 관련하여 해당 기관장은 어떤 책임과 역할을 수행하여야 하는가?
	개별 기관 보안 조직의 역할과 책임	* 해당 기관이 정보보호관리를 수행할 때 지원과 협력 역할을 수행할 전문가와 조직의 어떤 역할이 필요한가?
보안 프로그램	보안 프로그램의 적합성	* 정보보호관리 노력은 어떠한 적합성을 지녀야 하고, 특히 어떤 보안 위험의 대응책을 마련해야 하는가?
	보안 프로그램의 구현	* 정보보호 보안 프로그램은 어떠한 절차를 담고 구현되어야 하는가?
	보안 프로그램의 평가 및 개선	* 정보보호관리 노력은 어떤 단계별로 평가되어야 하고, 또한 더 나은 방향으로 개선하려는 노력이 담겨져 있는가?
효과적 수단	표준 및 가이드라인 활용	* 정보보호의 관리에 어떤 일정한 기준과 표준을 적용함으로써 기술과 업무처리 방식의 변화에도 체계적으로 대응할 수 있는가?
	tool 및 도구의 활용	* 정보보호관리에 해당 보안 프로그램을 효과적으로 사용하기 위하여 어떤 tool 및 도구를 활용할 수 있는가?
	기술 센터 활용	* 정보보호 관리를 위해 기술 센터를 조직·운영하여 정보보호관리 노력을 수행하는가?

이러한 정보보호관리 노력은 보안 침해사고를 체계적으로 극복하기 위한 노력으로 작용할 수 있다고 본다. 또한 [표 나-1]를 이용해서 정보보호 법제도 미흡과 정보보호관리 주요 요소의 관계를 보여줄 수 있을 것이다.

3. 국외 정보시스템 보안 관련 제도 및 정책 분석

위에서는 보다 나은 정보보호를 위해 새롭게 등장한 정보보호관리의 개념과 특성을 소개하였다. 공공부문에서는 어떤 새로운 방안이라 하더라도 이를 제도화하려는 노력이 중요하다. 즉, 이런 방향으로 추진하게끔 하는 법적 제도적 기반 마련이 필요하다. 이에 여기서는 미국과 일본의 정보보호 관련 제도와 정책을 분석한다. 특히 이 정보보호관리를 법률에 가장 체계적으로 반영한 미국의 사례를 토대로 미국의 정보보호 관련 법·제도를 자세히 분석하기로 한다.

3.1. 미국의 정보보호관리 법·제도 분석

미국은 정보보호관리를 제도화하기 위해 오래전부터 다양한 법적 장치를 강구해왔다. 특히 2002년 FISMA(Federal Information Security Management Act)를 전자정부법(e-Government Act)에 포함시키면서 정보보호관리를 크게 반영하였다. 여기서는 이러한 미국의 정보보호 관련 법률과 이와 관련된 위원회 활동 및 행정명령 등을 정보보호관리의 관점에서 분석하기로 한다.

미국의 정보보호 관련 법률은 집행의 대상에 따라 국민(민간주체)과 공공기관으로 나누어 분석할 수 있다[표 2].

[표 2] 정보시스템 보안관련 법률의 성격에 따른 분류

국민(민간주체)	공공기관
* Computer Fraud and Abuse Act * Digital Millenium Copyright Act * Electronic Communication Protection Act	* Computer Security Act * Federal Information Security Management Act

위의 국민을 대상으로 하는 정보보호 관련 법률은 본 논문에서는 다루지 않기로 한다.

3.1.1 FISMA(Federal Information Security Management Act)

FISMA는 2002년도 제정된 전자정부법(e-Government Act) 중 3편(Title III)에 속하는 법으로서 정부기관으로 하여금 정보와 정보시스템 보호를 위해 전사적 정보보호 프로그램을 개발, 문서화, 구현하도록 요구하고 있다. 정보보호 통제의 효과성과 충분성을 보장하기 위해, FISMA는 기관의 CIO와 정보보호 책임자로 하여금 정보보호 프로그램을 매년 검토하여 그 결과를 관리예산국(Office of Management and Budget: OMB)에게 보고하도록 요구하고 있다. FISMA에 의하면 연방정부기관은 매년 정보보호 프로그램에 대해 독립적인 평가를 수행하도록 요구되어진다. 또한 FISMA에서는 정보 및 정보시스템에서 보장해야 할 3가지 정보보호 목표로 기밀성(개인정보보호 포함), 무결성(부인방지 및 진정성 포함), 가용성을 정의하고 있다.

[표 3] FISMA F/W분석

법안명	Federal Information Security Management Act(2002), FISMA		
입법취지	연방정부 기관의 정보보안을 강화하는 것을 의무화하기 위해 제정. 구체적으로 각 연방 정부기관의 정보시스템에 보안을 강화하기 위한 프로그램 개발, 문서화, 집행을 의무화함.		
ISM과의 관계			비고
역할과책임의명확화	감독 및 조정기관의 역할과 책임	● 기관의 정보보호 정책 및 업무의 감독 - 정책, 기준 등의 수립 및 실행의 감독 - 기관의 정보 및 정보시스템 보호를 위한 기준 준수 여부 확인 - NIST를 통한 표준/가이드라인의 수립과 관련된 조정 - 1년에 한번 기관 보안노력에 대한 평가 - 기관 보안노력 평가결과를 의회에 보고 ● 국방 및 중앙정보부 관련 보안은 국방장관 또는 중앙정보부장에게 일임	
	보안에 관한 기관장의 책임과 역할	● 정보보호 제공 의무 ● 정보보호 정책, 기준 등의 준수 의무 ● 정보보호 프로세스가 기관 전략 및 운영계획 프로세스에 통합되어 있어야 함	
	개별 기관 보안 조직의 역할과 책임	● 담당조직이 정보보호 제공 의무 - 위험의 식별, 영향도 평가 - 필요 정보보호 수준의 결정 - 정보보호 정책 및 절차의 실행 - 정기적인 정보보호 통제 점검 및 평가 ● CIO에게 정보보호 관련 역할을 부여 - 고위 정보보호관리관을 지명하여 CIO 책무를 수행하게 함 ● 기관의 정보보호 프로그램 수립 및 관리 ● 직원의 보안 훈련 제공	
보안프로그램	보안 프로그램의 적합성	● 보안 위험의 정기적 평가 ● 정보보호 정책 및 절차의 수행 ● 네트워크, 시설 등에 대한 정보보호 대책 강구 ● 관련 주체 모두에게 정보보호 인식 재고 ● 정보보호 정책, 대책, 절차 등의 정기적 시험 및 평가 ● 정보보호 개선 계획, 실행 ● 정보보호 사건(Incident)의 발견, 보고, 대응책 마련	
	보안 프로그램의 구현	● 정보시스템 라이프 사이클(Life Cycle) 전 단계에 정보보호 대책이 담겨 있어야 함	
	보안 프로그램의 평가 및 개선	● 매년 독립적인 정보보호 프로그램 평가 ● 감사 또는 외부 전문 감사인에 의한 평가 수행	
효과적수단	표준 및 가이드라인 활용	● NIST에서 정보보안 규격, 표준, 가이드라인을 개발하게 함 ● FIPS와 SP 800 Series 가이드라인을 제정하고 다음과 같은 내용을 명시하고 있음 - 개발된 규격, 표준, - 정보자산 등급, 보안대책 선택, - 문서화, 감시, 평가 - 인증과 인가(C&A)	
	tool 및 도구의 활용	NIST에서 보안 구성 점검표의 개발을 용이하게 하고 2002년 실행된 Cyber Security Research and Development Act을 충족시키기 위해 아래와 같은 목표를 가진 프로그램을 개발 - 프레임워크 제공을 통해 개발 및 보안 구성 점검표 공유의 용이 - 공통 운영환경을 준수하는 점검표 개발자에 대한 지원 - 점검표에 대한 검토, 갱신, 유지를 위한 관리 프로세스 제공 - 사용하기 쉬운 점검표 저장소의 제공 SP 800-70에서는 현재 및 향후의 점검표 사용자를 위해 NIST 점검표 프로그램의 개요와 점검표의 사용 방법 등을 기술하고 제품군, 제조사 등을 통해 특정 IT 제품에 대한 점검표 획득	
	기술 센터 활용	정보보호 사건(Incident) 센터의 운영	

3.1.2 ITMRA(Information Technology Management Reform Act)

ITMRA는 행정의 효율성과 효과성을 증진시키기 위하여 정보기술의 효과적인 활용을 도모하기 위하여 1996년에 제정되었으며, 이는 연방획득혁신법(Federal Acquisition Reform Act)와 함께 Clinger-Cohen Act로 불리어졌다. ITMRA는 정보기술의 효과적인 활용을 위하여 자본계획과 투자 통제, 정보기술 조달, 정보자원관리, 정보기술에 대한 성과 평가를 중심으로 OMB, 기관장, CIO 등의 역할 및 책임에 대하여 규정짓고 있다. ITMRA는 주로 정보자원관리에 중점적인 규정을 하고 있으며 정보보호관리에 관한 것은 FISMA로 이양된 상태이다.

[표 4] ITMRA법 F/W분석

법안명	Information Technology Management Reform Act (1996), ITMRA		
입법취지	행정의 효율성과 효과성을 증진시키기 위하여 정보기술의 효과적인 활용을 도모하기 위하여 1996년에 제정.		
ISM과의 관계			비고
역할과책임의명확화	감독 및 조정기관	● IT 표준 제정 ● 보안 예산 편성 ● IR관리를 위한 의회에 정보제공	* 프로세스 통합 전략에 관한 언급 없음
	기관장	● 보안 재정 및 프로그램 관리에 대한 절차 통합 ● 정보시스템 투자를 위한 기준(수량적으로 표시된 수익, 투자 이익 비교) 마련	
	기관 보안 조직	● 정보자원관리 교육에 대한 책임 ● 기관 책임자에게 정보시스템 투자 과정에 대한 관련 정보 제공	
보안프로그램	보안 프로그램의 적합성	● 정보보호 시범 사업 - 정보보호 시범 사업을 위한 실시 권한 규정 - 정보보호시범 사업에 대한 평가 기준 및 계획 확립	* 주로 정보관리 사업에 관한 내용 다룸
	보안 프로그램의 구현	● 정보보호의 효율성 확인을 위한 예산절차를 통하여 정보관리에 대한 정기적 심사 ● 정보보호 관리를 위한 행정 절차 개선, 정보보안 유지	
	보안 프로그램의 평가 및 개선	● 성과 평가 - 성과 측정 기준을 바탕으로 프로그램의 성과 평가 - 정보관리에 대한 추진 목표 달성을 위한 적정성 평가 - 정보기술 프로그램의 성과 조사	
효과적수단	표준 및 가이드라인 활용	● 임무관련절차 및 행정절차의 평가와 개선 및 정보시스템에 대한 기관의 투자성과에 대한 성과 측정을 위한 정책 절차 제공	
	tool 및 도구의 활용		
	기술 센터 활용	● Office of Federal Procurement Policy(OFPP)와의 공조로 IT 구매와 IT의 조달에 관한 정책 개발 및 심사를 담당하는 정보기술 활용(utilization) 센터 운영	

3.2 일본의 정보보호관리 법·제도 분석

일본은 2000년 11월에 고도 정보통신 네트워크 사회 형성 기본법(IT기본법)을 마련하고 e-japan 전략(2001년~2005년)을 통해 국가정보화를 가속해왔다. 그리고 2001년 1월부터 내각관방(총리실) 직속의 IT 전략본부가 국가정보화 전략을 전담해왔다. 그리고 2004년 12월, 정보보호 문제에 대한 정부의 역할과 기능을 재검토하여 정보보호문제에 관한 정부의 중심적인 역할 강화를 위한 기능, 체제를 정비하여 2005년 4월 25일 정보보호센터를 설치하게 되었다. 그리고 정보보호센터 내의 "정보보호 기본문제 위원회"의 정책제언을 통해 정보보호 정책회의 설립되고 9월 15일 개최된 제2차 정보보호 정책회의에서 정부기관 통일기준 마련이 의제로 올라 정보보호 대책강화에 관한 기본방침 및 통일 기준 제정을 하게 되었다.

[표 5] 일본 정부기관의 정보보호 대책을 위한 통일기준 F/W분석

법안명	정부기관의 정보보호 대책을 위한 통일기준(2007)		
입법취지	정부기관의 정보보호 대책을 위한 통일기준은 각 부처별로 운영되는 정보보호대책을 통일하고 각 부처가 적용하기 쉬운 형태의 구체적인 대책을 제시하기 위해 제정되었다. 또한 기술, 환경변화에 따른 정보보호 대책 요구사항의 고도화에 신속한 대응이 가능하도록 하는 내용이 담겨져있다.		
ISM과의 관계			비고
역할과책임의명확화	감독 및 조정기관의 역할과 책임	● 정보보호에 대한 승인·허가 - 정보에 대한 접근 승인 및 허가 규정 - 통일기준에 대한 예외 사항 발생시 충분한 검토를 하고 승인 및 허가 - 기관의 보안노력 평가결과를 내각관방의 정보보호센터에 보고 ● 년도감사계획에 따라서, 정보보안감사책임자에 대해서, 감사의 실시	
	보안에관한 기관장의 책임과 역할	● 정보보안에 관한 장해·사고가 발생한 경우를 대비한 복구 체제 정비 ● 매년 최저 1회 정보보안대책의 교육에 관한 계획 수립 ● 년도자기점검계획을 책정하여 정보보호센터에 보고	
	개별 기관 보안 조직의 역할과 책임	● 정보보안관계규정에의 위반이 있는 경우에 위반의 사실을 최고정보보안책임자에게 보고. - 내용, 결과, 업무에 영향, 사회적 평가를 포함 ● 정보보안관계규정의 중대한 위반에 정보보안 유지를 위한 조치를 강구 - 기밀성, 완전성, 가용성이 훼손되는 경우 ● 정보보안대책 교육의 실시	
보안프로그램	보안 프로그램의 적합성	● 정보시스템의 문서 및 대장정비 ● 정보보안 프로그램의 선정기준을 정비	
	보안 프로그램의 구현	● 정보처리와 정보시스템에 대한 정보보호 대책 수립	
	보안 프로그램의 평가 및 개선	● 정보보호센터내의 정보보호위원회에 의한 평가 수행	
효과적수단	표준 및 가이드라인 활용	● 암호와 전자서명의 표준절차 시행	
	tool	●	
	기술 센터	●	

4. 결론

향후 정보시스템에 대한 침해는 더욱 심해질 것으로 보인다. 따라서 기존 정보보호시스템의 보안성 및 안전성을 강화할 필요가 있고, 그에 대한 다양한 평가제도 및 평가기술이 존재하고 있다. 그리고 현재 우리나라도 정보보호관리 강화를 위한 제도 및 정책을 시행하고 있다.

하지만 본 연구에서 살펴본 국외 정보보호관리 제도 및 정책과 같이 심도 깊고 다방면에 걸친 제도 및 정책은 아직 우리나라에 존재하지 않는다. 따라서 현존하는 국외 정보보호관리 제도 및 정책을 분석하고, 우리나라 실정에 맞는 제도 및 정책 도입이 시급하다. 구체적으로는, 이러한 정보보호관리에 있어 선진국인 미국의 FISMA와 같은 제도가 필요할 것으로 예상된다. 위에서 연구한 바와 같이, FISMA는 ISM에서 요구하는 역할과 책임의 명확화, 보안 프로그램, 효과적 수단을 모두 갖추는 완성된 정보보호관리 제도라고 할 수 있다.

본 연구는 정보시스템 보안강화체계 확립을 위해 국외 정보보호관리 제도 및 정책, 특히 미국과 일본의 제도를 조사, ISM 프레임워크를 통해 분석하여 국내 정보보호관리 제도 및 정책에 어떠한 요구사항이 필요할지 조사하였다. 본 연구에서 제기된 내용을 참조하여 향후 국내 정보보호관리 제도 및 정책에 기여할 수 있을 것이다.

참고문헌

[1] 김명룡, 박광진, 박정현, "국내외 정보보호관련 법제도 현황", 한국정보보호센터 정책연구, 96-1, 1996.

[2] 임혜경, "정보자원관리를 위한 미국의 관련법 및 프로세스 분석", 정보통신정책 제18권 1호, 2005.

[3] 한국소프트웨어산업협회, "공공기관 S/W 발주체계관련 현행 법제도 조사 및 분석 연구", 한국소프트웨어산업협회, 2003.

[4] 한국전산원, "한·미 법제도 및 추진 체계비교", 정보화이슈분석 05-02, 2005.

[5] 한국정보보호진흥원, "통합시스템 보안성 평가체계 및 방법연구", 한국정보보호진흥원, 2006.

[6] Cenzic, "Cenzic Web Application Security Trends Report Q1-Q2", Cenzic Inc, 2009.

[7] McGraw, G., "Software Security", THE IEEE COMPUTER SOCIETY, 2004

[8] OWASP Foundation , "OWASP TOP 10 2007", OWASP Foundation, 2007.

[9] Simpson, S., "Fundamental Practices for Secure Software Development 2008", Software Assurance Forum for Excellence in Code, 2008.

[10] US FISMA(Federal Information Security Management Act of 2002), 2002.