산업기술연구(강원대학교 산업기술연구소 논문집), 제31권 A호, 2011.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 31 A, 2011.

FISMA의 국내 도입에 따른 문제점 예측

Prediction of the Problems from Domestic Introduction of FISMA

김 상 균*
Kim, Sangkyun

Abstract

Federal Information Security Management Act emphasizes the importance of information security to the economic and national security interests of the United States. This paper provides a brief review on FISMA which is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002, and predicts the possible problems which might be caused from domestic introduction of FISMA. The domestic introduction of FISMA could improve the average level of information security of government agencies. Whereas, the government agencies and the government officials might face with many problems such as the increased government budget, lack of social awareness and security professionals, and the effectiveness of penalty on non-compliance.

키워드 : *연방정보보안관리법, 정보보호, 위험관리*
Keywords : *FISMA, information security, risk management*

1. 서론

국가정보원의 보고에 따르면 국내 공공기관에서 발생하고 있는 정보보호 침해사고는 매년 증가하고 있으며, 최근에는 한 해에 두 배 수준으로 증가하기도 하였다. 이와 같은 상황에서 국내 정부기관의 정보보호 수준 향상을 위한 제도적 장치의 보완이 필요하다.

현재 국내의 정보보호 관련 법제도는 미국의 법제도와 유사한 면이 많다. 아직 국내의 정보보호 관련 법제도는 미국에 비하여 그 포괄성과 세분화에서 부족한 면도 있으나, 법제도의 전반적인 틀은 미국과 유사한 면이 많다. 또한 국내의 정부기관에서 사용하고 있는 정보보호 관련 표준, 가이드라인 및 절차서 등은 미국의 DoD, NIST 및 기타 연구기관들의 자료를 기반으로 개발된 것들이 많다. 미국은 9.11이후 연방정부기관의 정보보호를 위해 FISMA(Federal Information Security Management Act of 2002)를 제정하여 운영하고 있다. FISMA를 기반으로 정부기관의 정보보호 라이프사이클에 대한 전체적인 틀을 정립하고, 정보보호 수준을 보장하고자 한다.

국내의 정보보호 관련 법과 기준들이 미국의 것과 유사한 상황에서 본 논문은 국내 정부기관의 정보보호 수준 향상을 위하여 미국의 FISMA를 국내에 도입할 경우 발생할 수 있는 문제점들을 예측한다. 본 논문은 FISMA의 개요를 설명하고, FISMA 시행에 참여하는 미국 정부기관별 역할을 소개한다. 또한 FISMA시행 시 미국에서 나타난 문제점을 고찰하고, 이를 바탕으로 FISMA와 유사한 제도가 국내에서 시행될 경우 발생할 수 있는 문제를 예측한다.

* 강원대학교 산업공학과 교수, 공학박사

2. FISMA의 개요 [1][2]

2.1 제정 배경

미국 일반 회계원(General Accountability Office: 이하 GAO)은 1996년부터 연방 시스템들이 전산적 공격에 대한 보호 대책을 적절하게 구비하지 못하고 있음을 지속적으로 지적했다. 1998년과 2000년의 24개 연방 부처에 대한 감사결과에서 24개 전 부처의 정보보호 문제가 심각한 수준으로 나타났으며, 이에 대한 대응으로 연방정보보안을 위한 활동들에 대한 종합적 전략 개선이 요구 되었다. 미국 연방정부는 정부정보보안 개혁법을 통과시켜 연방 각 부처들로 하여금 컴퓨터 시스템과 그에 의하여 처리되는 정보 및 관련 기술자원의 보호를 의무화 하였다.

미국의 정부정보보안개혁법은 컴퓨터 보호법(Computer Security Act of 1987)과 OMB Circular A-130를 바탕으로 정부 부처의 정보보호를 위한 기본적 틀을 제시하는 것으로 당초에는 2002년 11월 29일까지 한시법으로 공표되었으나 2002년 말에 전자정부법(E-Government Act of 2002)에 FISMA로 이름이 바뀌며 지속적으로 운영되게 되었다.

2.2 목적 및 정의

FISMA 원문 '제 3541조'에서는 목적을 다음과 같이 규정하고 있다. FISMA의 제정 목적은 연방정부의 보안 강화에 두고 있다. 이를 위해 효과적인 정보보안 통제를 위한 프레임워크를 설정하고 네트워크화 된 컴퓨팅 환경에 필요한 정보보안 리스크의 관리감독을 하며, 연방정보와 정보시스템을 보호하기 위한 최소한의 통제 수단을 제공한다. 또한 기관 정보보호 프로그램 감독기능 향상을 위한 메커니즘을 명문화 하며 상업적 정보보안 제품의 우수한 솔루션을 제공하는 것을 인정하고 정보보안 제품의 선택을 각 기관에 일임하는 것을 인식하기 위한 것이다.

FISMA 원문 '제 3542조'에서는 정의를 다음과 같이 규정하고 있다. '정보보안'이란 승인되지 않은 접근, 사용, 노출, 방해, 변경, 파괴로부터 정보와 정보 시스템을 보호하는 것이다. 정보보안은 컴퓨터 시스템과 네트워크, 소프트웨어로 구성되는 정보시스템을 보호하고 정보 시스템에 기록, 진행, 소통, 저장, 공유, 분배, 전송, 접수되는 데이터와 메시지 그리고 정보의 보호에 중점을 둔다.

2.3 관련 기관별 역할

FISMA에 관여하는 연방 정부기관별 역할은 다음의 표 1과 같다.

표 1 FISMA관련 기관별 역할

행정기관	역할
예산 관리처 (Office of Management and Budget: 이하 OMB)	● 정보보안 정책수립 ● 정책, 원칙, 표준 및 지침 개발/감독 ● 정보보안대책을 강구함을 정부기관에 요구 ● 연방 컴퓨터시스템의 보안과 관련한 상무부의 표준과 지침의 개발과 집행을 감독
상무부 (United States Department of Commerce: 이하 US. Commerce)	● 연방정부시스템의 보안을 위한 표준과 지침 개발 및 보급/검토/개정 ● 각 정부부처의 정보보안 정책 수립 지원 및 정보보안 위협 기술평가에 대한 책임을 부담
국방부 (United States Department of Defense: 이하 DoD)/ 중앙정보국 (Central Intelligence Agency: 이하 CIA)	● 정보시스템의보안정책, 표준 및 지침의 개발 및 보급, 수행을 점검 ● 보안정책, 표준 및 지침의 공표
법무부 (Department of Justice: 이하 DOJ)	● 정보보안사고와 관련한 법적인 조치 및 보고 지침 검토/개정
총무청 (General Services Administration: 이하 GSA)	● 연방 정부부처들이 새로운 정보 기술을 도입하는 경우 발생되는 정보보안 문제를 검토하여 개선 ● 각 부서의 보안제품 확보를 위한 지원과 정보보안 기술 도입의 비용 효과적인 제품과 서비스를 도입
인사 관리국 (Office of PersonnelManagement: 이하 OPM)	● 연방 공무원을 대상으로 컴퓨터 보안교육과 관련한 법규를 재검토 및 개선 ● 컴퓨터 보안교육 지침에 대해서 상무부와 협력 ● 정보보안 교육내용 및 교육 강사와 관련하여 국립과학재단 및 기타 기관과 협력

2.4 표준 및 지침의 제공 [3]

FISMA에 대한 정부기관의 이해 제고와 수행 용이성을 위하여 NIST는 FISMA와 연관된 정보보호 표준과 지침들을 개발했다. NIST는 제시하는 표준과 지침들을 전체적으로 통합하고 설명하기 위하여 위험 관리 체계(RMF, Risk Management Framework)를 개발하였다. 위험 관리 체계(RMF)는 위험을 관리하기 위한 활동들을 6단계의 구조로 분류하여 제시하고 있다. 그림 1은 RMF의 단계별 특징을 설명한다.

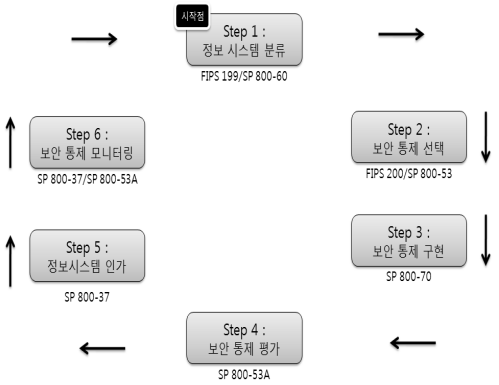

그림 1 RMF의 6단계 모델

RMF의 단계별 상세 내용은 다음과 같다.

o Step 1 : 정보 시스템 분류(Information System Categorize)

특정 사건 또는 위험이 기밀성, 무결성, 가용성 관점에서 정보와 정보 시스템에 잠재적(impact)으로 미치는 영향력에 기반 하여 정보와 정보 시스템을 분류한다. “FIPS 199”, “NIST SP 800-60 Revision 1(Volume 1, Volume 2)”를 참고한다.

o Step 2 : 보안 통제 선택(Security Controls Select)

“FIPS 199”의 보안 분류와 “FIPS 200”의 보안 요구사항, 그리고 위험 정보, 비용 분석, 조직의 사정 등 기타 요소들에 기반 하여 정보 시스템의 최소 보안 통제를 선택한다. “FIPS 200”, “NIST SP 800-53 Revision 3”를 참고한다.

o Step 3 : 보안 통제 구현(Security Controls Implement)

실제로 Step2에서 선택한 보안 통제를 보안 환경 설정에 맞게 구현한다. “NIST SP 800-70”을 참고한다.

o Step 4 : 보안 통제 평가(Security Controls Assess)

보안 통제가 시스템의 보안요구사항에 기반 하여 적절한 방법을 사용하였는지, 구현이 정확한지, 운영이 올바른지, 원하는 결과를 도출하는지를 평가한다. “NIST SP 800-53A”를 참고한다.

o Step 5 : 정보 시스템 인가(Information System Authorize)

정보 시스템 운영에 있어 조직 운영, 조직 자산 또는 개별적인 결과와 관련하여 위험을 판단하고, 위험이 용인될 수 있는지 결정하여 정보시스템 운영을 인가(authorize)한다. “NIST SP 800-37”을 참고한다.

o Step 6 : 보안 통제 모니터링(Security Controls Monitor)

선택한 보안 통제가 시스템 변경에 따른 문서화, 보안 영향력 분석, 보안 상태 보고 등의 기본 사항을 계속해서 효율적으로 수행하고 있는지 재평가하고 모니터링 한다. “NIST SP 800-37”와 “NIST SP 800-53A”를 참고한다.

3. FISMA관련 미국내 현황 및 문제점

3.1 미국내 현황 [4][5]

FISMA 시행 이후 미국정부는 정부기관의 정보보호 수준 향상을 위해 초 년도에 42억불을 투자하였고, 그 규모를 지속적으로 증가시켜, 최근에는 한 해에 70억불 정도의 예산을 투자하고 있다.

미국의 25개 주요 정부기관에 대한 2002년부터 2009년까지의 FISMA와 관련된 주요 실적은 다음의 표 2와 같다.

표 2 2002년~2009년의 FISMA 주요 실적

년도	인증 & 인가	테스트된 위기대처 계획	테스트된 정보보호 통제	보고된 전체 시스템 수
FY 2002	47%	35%	60%	7,957
FY 2003	62%	48%	64%	7,998
FY 2004	77%	57%	76%	8,623
FY 2005	85%	61%	72%	10,289
FY 2006	88%	77%	88%	10,595
FY 2007	92%	86%	95%	10,304
FY 2008	96%	92%	93%	10,679
FY 2009	95%	86%	90%	12,930

미국 정부기관에서 고용하고 있는 정보보호 관련 인력의 숫자는 현재 6만여명으로 추산되고 있다. 주요 정부기관별 정보보호 인력의 고용 규모는 다음의 그림 2와 같다.

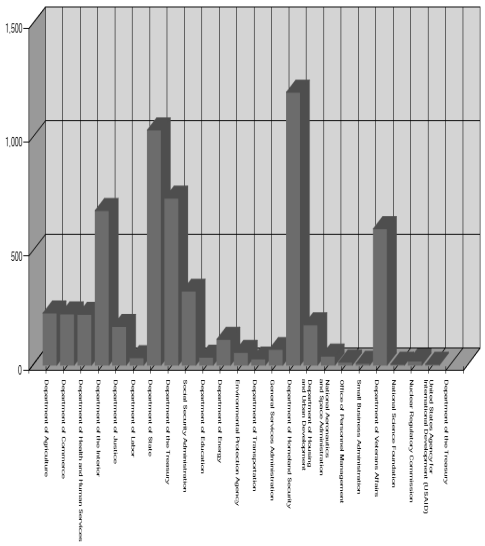

그림 2 미국의 정부기관내 정보보호 관련 인력

미국 정부기관의 고용인력 중 정보시스템 접근권한을 가진 직원들을 대상으로 정보보호 관련 교육 이수 현황을 조사한 결과는 다음의 그림 3과 같다. 전반적으로는 90%이상의 직원들이 FISMA와 관련하여 정보시스템에 대한 정보보호 교육을 이수한 상태이다.

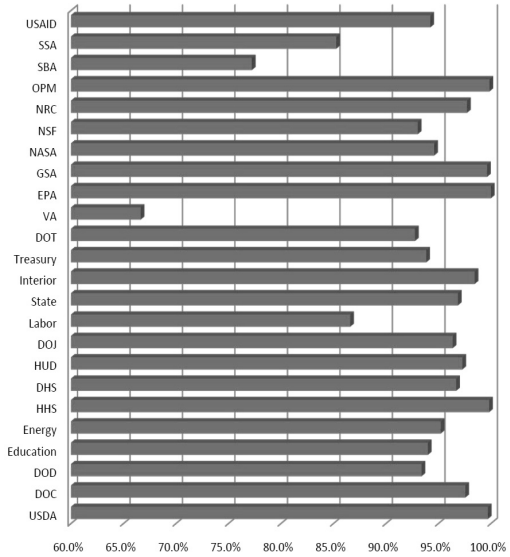

그림 3 정부기관 직원의 정보보호 교육이수 현황

미국 하원에서 FISMA와 관련된 보고서를 기반으로 분석한 정부기관의 정보보호 수준은 다음의 표 3과 같다.

표 3 미국 주요 정부기관의 정보보호 수준

FEDERAL COMPUTER SECURITY REPORT CARD			May 2008		
GOVERNMENTWIDE GRADE 2007: C (2006: C-)					
	2007	2006		2007	2006
DEPARTMENT OF JUSTICE	A+	A-	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	C	D-
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+*	A+	DEPARTMENT OF STATE	C*	F
ENVIRONMENTAL PROTECTION AGENCY	A+	A-	DEPARTMENT OF EDUCATION	C-	F
NATIONAL SCIENCE FOUNDATION	A+*	A+	DEPARTMENT OF COMMERCE	D+	F
SOCIAL SECURITY ADMINISTRATION	A+*	A	DEPARTMENT OF TRANSPORTATION	D	B
HOUSING AND URBAN DEVELOPMENT	A	A+	DEPARTMENT OF LABOR	D	B-
OFFICE OF PERSONNEL MANAGEMENT	A-	A+	DEPARTMENT OF DEFENSE	D-	F
GENERAL SERVICES ADMINISTRATION	B+	A	DEPARTMENT OF THE INTERIOR	F	F
DEPARTMENT OF ENERGY	B+	C-	DEPARTMENT OF TREASURY	F	F
DEPARTMENT OF HOMELAND SECURITY	B+	D	NUCLEAR REGULATORY COMMISSION	F	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	B	DEPARTMENT OF VETERANS AFFAIRS	F	N/A
SMALL BUSINESS ADMINISTRATION	B	B+	DEPARTMENT OF AGRICULTURE	F	F

앞의 표는 2006년과 2007년에 대한 수준을 보여주고 있는데, 대부분의 기관이 2006년과 대비하여 2007년의 정보보호 수준이 향상된 것을 볼 수 있다. 2006년의 전반적 수준이 “C-등급”이었던 것이, 2007년에는 “C등급”으로 향상되었다.

3.2 미국내 문제점 [2][6][7]

표 2의 수치가 보여주듯이 FISMA의 시행 초기에는 FISMA의 추진 주체와 시행 대상 기관 모두 실효성 있는 확산에 큰 어려움을 겪었다. 당시의 문제점을 일부 문헌에서는 혼돈, 잘못된 목표, 책임추궁성의 부재로 요약하고 있다.

2002년 이후 지금까지 미국내에서는 FISMA가 시행되면서 다양한 가이드라인이 개발되었으며, 행정적인 지원 규모도 큰 폭으로 증가하였다. 현재 시점에서 OMB와 하원에서 직접적으로 언급하고 있는 FISMA와 관련된 구체적 문제점은 발견하기 어렵다.

본 논문에서는 FISMA 시행 초기에 제시되었던 문제점을 다음과 같이 요약한다.

o 예산의 부족

FISMA 시행 대상인 기관들의 대부분이 자체적으로 확보한 다른 예산을 재편하여 FISMA와 관련된 투자를 수행해야 함을 토로하였으며, 이는 이후 재정적 지원 확대를 통해 일부 해소되었다.

o 정보보호 목표 및 범위 설정의 주관성

FISMA 의 법조문은 정부기관의 정보보호 목표를 세분화하여 제시하지 않고 있다. 또한 NIST에서 제시한 RMF문서들은 일부 표준적인 역할도 있으나 통상적으로 가이드라인의 성격을 가지고 있다. 따라서 FISMA 시행 대상 기관들은 FISMA의 목표 및 범위를 가급적 축소하여 해석하고 실행하는 경향이 있었다.

o 대중적 공감대 부족

FISMA 시행 대상기관의 대부분은 직접적으로 대민 서비스를 제공하거나, 대중의 요구에 따라서 기관의 정책방향을 수립하는 경향이 있다. 그러나 OMB주도로 FISMA를 시행하면서 대중의 FISMA에 대한 인지도 향상과 의식 개선 활동이 제대로 제공되지 않아서, 시행 대상기관들은 대중의 직접적인 인식과 요구가 낮은 FISMA에 대한 투자에 더욱 소극적일 수밖에 없었다.

o 미준수 기관에 대한 패널티 부재

OMB에서 재정적인 권한을 가지고 FISMA를 추진했으나, 실제 FISMA와 관련된 실적이 부족한 정부기관을 재정적 수단으로 압박하거나 패널티를 부과하기에는 현실적인 어려움이 크다는 지적이 많았다.

o 대상 범위의 모호성

정부기관의 대부분은 정보시스템과 관련하여 다양한 종류와 규모의 아웃소싱을 활용하고 있다. 이 경우 FISMA의 적용대상이 정부기관의 범위를 넘어서는 상황이 발생하여, 아웃소싱 공급자의 FISMA 준수 의무에 대한 모호성이 발생했다. 또한 이를 확대하자면 아웃소싱 공급자가 100% 독자적으로 시스템이나 서비스를 공급하는 것이 아니라 개별적 협력이나 제휴의 네트웍으로 아웃소싱 시스템이나 서비스를 제공할 경우 FISMA 준수 의무에 대한 범위는 더욱 모호해진다.

o FISMA에 대한 투자와 정보보호 수준의 불확실한 연관성

FISMA는 근본적으로 정보보호 수준을 관리하지 않는다. FISMA는 정부에서 정한 절차를 준수하여 정부기관이 정보보호의 목표를 수립하고, 그에 따라 시스템을 구축하고, 평가하며 운영하는 것을 요구한다. 이러한 정보보호 라이프사이클을 준수하는 것이 정보보호 수준의 절대적인 개선을 보장하는 것은 아니라는 점이 문제로 지적된다. 정보보호에 대한 투자가 다양한 영역에서 2002년부터 2009년까지 증가했으나, 이러한 규모의 증가가 정보보호 수준 개선에 직접적인 영향을 주는가는 명확하지 않다는 점이다. 반면에 하원의 평가자료를 보면 미국 정부기관의 정보보호 수준이 전반적으로 향상되고 있는 것을 볼 때 FISMA와 관련된 다양한 영역의 투자 확대가 정보보호 수준의 개선과 어느 정도 연관성이 있다고 추측할 수 있다.

4. 국내 도입에 따른 문제점 예측 [2]

본 장에서는 FIMSA 체계를 국내에 도입할 경우에 예상되는 문제점들을 미국내 FISMA도입 시 발생했던 문제점, 진행 경과, 국내의 관련 법체계 현황 등을 고려하여 제시한다. FISMA 체계를 국내에 도입할 경우 예상되는 문제점 및 관련된 제언은 다음과 같다.

o 예산 확보

· 문제점: 크게 두 분류의 예산이 필요하다. 첫째는 FISMA와 관련된 체계를 관리하기 위한 예산이며, 둘째는 개별 정부기관의 FISMA준수를 위한 정보보호 투자 예산이다. 소요되는 예산의 규모가 현재보다 대폭으로 증가할 것이며, 장기적으로 안정적인 확보가 필요한데, 현재 국내 정부기관의 정보보호 관련 예산과 같이 매해 예산을 수립하고, 승인받는 구조는 적절하지 못하다.

· 제 언: FISMA와 관련된 체계를 관리하기 위한 예산은 최소 5년치 이상이 미리 확보되어야 한다. 또한 개별 정부기관의 정보보호 예산도 현재 보다 대폭으로 증액되어야 한다.

o 평가 결과에 대한 보상

· 문제점: FISMA 추진 결과에 대한 평가가 필수 요소의 이행 여부에 대한 평가에만 집중될 경우, 정보보호 수준 향상이라는 목적과는 거리가 생길 수 있다.

· 제 언: 연단위로 정보보호 수준 향상도를 평가하고, 평가결과에 따른 재정적인 인센티브를 기관별로 제공해야 한다.

o 수행 결과에 대한 제재

· 문제점: FISMA 체계를 국내에 도입할 경우 최소한의 필수 요소만을 수동적으로 이행하고, 정보보호 수준 향상이라는 목적 달성에는 소극적인 기관들이 발생할 수 있다.

· 제 언: FISMA의 필수 요소 이행도와 정보보호 수준 향상도를 평가하여, 이행도가 낮거나 수준 향상도가 부족한 기관에 대해서는 재정적인 제재를 가할 수 있어야 한다.

o 정보보호 책임관 및 기관내 전문가

· 문제점: CIO 제도에 대한 준수수준도 높지 않은 상태에서 FISMA제도를 도입할 경우 개

별 정부기관들은 내부에 정보보호 책임관 및 전문가 부족으로 인하여 업무상 많은 혼선을 빚게 된다.

· 제 언: CIO가 정보보호 책임관을 겸하게 하거나, CIO를 보좌할 정보보호 보좌관을 둘 것을 제안한다. 아울러 개별 기관별로 국가에서 인정하는 자격요건을 가진 정보보호 전문가를 기관의 특성이나 규모에 따라서 일정 수준이상 확보하도록 유도해야 한다.

o 관련 지침 및 절차서 개발

· 문제점: 미국의 경우 FISMA와 관련된 표준, 지침 및 절차서 등이 법 시행 이후에 순차적으로 개발되고, 제공되는 과정(2003년~2009년)에서 개별 정부기관들의 FISMA에 대한 구체적 수행기준 해석 및 실행에 많은 혼선이 있었다. 이러한 문제점은 국내에서도 동일하게 발생할 것이다.

· 제 언: FISMA와 같은 제도를 국내에 도입할 경우 관련 표준, 지침 및 절차서를 조기에 개발하고, 적극적으로 보급 및 홍보하여 개별 정부기관들의 해석 및 실행에 대한 혼선을 최소화해야 한다.

o 사회적 의식수준

· 문제점: 미국내 FISMA도입 시 나타났던 문제점 중의 하나는 사회적으로 FISMA에 대한 인지도와 필요성에 대한 공감대 형성이 부족하여, 개별 기관들의 수동적인 대응을 유도했다는 점이다.

· 제 언: FISMA에 대한 대국민 인지도 향상 및 필요성에 대한 공감대 형성을 위한 홍보 및 의식개선 활동을 추진하여, 개별 정부기관들이 수동적인 해석과 대응에서 탈피하여 적극적으로 나설 수 있도록 해야 한다.

5. 결론

본 논문에서는 미국이 연방정부기관의 정보보호를 위해 운영 중인 FISMA의 배경, 목적, 관련 지침 등을 소개하고, FISMA에 대한 추진 현황 및 추진 과정 중에 도출된 문제점들을 설명하였으며. 이를 바탕으로 국내에 FISMA와 유사한 제도를 도입할 경우 발생할 수 있는 문제점을 예측하고 이를 해결하기 방법을 간략하게 제안하였다.

본 논문에서 제시한 내용의 한계점 및 향후 추진 방향은 다음과 같이 요약된다.

o 미국내 현황에 대한 세부적 분석

미국의 경우 2002년부터 현재까지 연간 수 십억불 이상을 투자하여 FISMA를 추진해왔으며, 이와 관련하여 다양한 정부기관이 관련되어 있다. 따라서 미국내 현황 및 문제점을 깊이 있게 분석하기 위해서는 보다 체계적인 연구가 필수적으로 추진되어야 한다.

o 국내 도입 문제점에 대한 구체적, 장기적 예측

본 논문에서는 FISMA와 관련되어 미국에서 발생했던 문제점을 중심으로 국내의 문제점을 간략하게 예측하고 있다. 향후에는 미국내 정치, 제도, 경제적 현황과 국내 정치, 제도, 경제적 현황의 차이점을 세부적으로 분석하여, 문제점을 깊이 있고 현실적으로 예측하는 작업이 필요하다.

o 국내 도입 시 문제점에 대한 대응방안 수립

본 논문에서는 FISMA의 국내 도입 시 예견되는 문제점에 대하여 간략한 제언을 하고 있다. 그러나 이는 분석의 깊이와 관점의 다양성에서 제한적인 것이다. FISMA와 같은 제도의 도입과 정착을 위해서는 많은 제도가 개선되어야 하고, 정부기관의 내부 조직구조와 업무 프로세스에도 많은 변화가 요구된다. 또한 이를 지원하기 위한 다양한 지침이 개발되고, 의식개선 작업 및 교육 프로그램 등도 개발되어야 한다.

참 고 문 헌

[1] 김대호, 오일석, “미국 전자정부 정보보안 법제 동향”, *정보보호학회논문지,* 제13권, 제3호, 2003.

[2] 박완규, “정보보안 법제의 개선 방향에 관한 연구 :미국 연방정보보안관리법 문제점과 시사점”, *행정법연구*, 통권22호, 2008.

[3] 한국정보보호학회, *미 연방정부 정보시스템 안전성 보증체계 분석 보고서*, 한국인터넷진흥원, 2009.

[4] Office of Management and Budget, *Fiscal Year 2009 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002,* Office of Management and Budget, 2009.

[5] Robert Silers, *Rethinking FISMA and Federal Information Security Policy*, Vol.81 N.Y.U. L. Rev, 1844, 2006.

[6] General Accountability Office, *Information Security: Serious weakeness Place Critical Federal Operations and Assets ant Risk*, General Accountability Office, 1998.

[7] General Accountability Office, *Information Security: Serious and Widespread Weaknesses Persist at Fedral Agencies*, General Accountability Office, 2000.