미국과 우리나라의 정보보안관리 활동 비교연구

김 소 정†

요 약

미국 연방정부는 정부의 정보 및 정보시스템에 대한 연방정보보안관리법을 적용하여 각 기관의 정보보안을 강화하기 위한 프레임워크를 제시했다. 동 법에 따라 NIST 주관으로 연방정보보안관리법 실행 프로젝트를 실행하여 미국 연방정부의 정보 및 정보시스템을 보호해 안전한 미국연방정부 설립이라는 목적을 달성하고자 한다. 이를 위해 각 연방기관의 정보보안강화를 위한 근거를 마련하고 관리예산처 및 인반회계감사원 등 이를 관리·감독할 수 있는 체계를 구성하고 있다. 우리나라의 경우 국가사이버안전관리규정을 통해 국가차원의 사이버안전 관리강화를 위해 노력하고 있으며 특히 국가사이버안전매뉴얼에서는 각급기관이 평시에 자신의 정보시스템에 대한 관리를 수행할 수 있도록 평시 안전점검 체크리스트를 만들었다. 본 논문에서는 미국의 연방정보보안관리법에 따른 보안관리체계를 분석해 우리나라의 사이버안전 관리체계 강화 시 참고하고자 한다.

키워드 : 연방정보보안관리법, 국가사이버안전관리규정, 국가사이버안전매뉴얼, 보안관리

A Comparative Study on Information Security Management Activity of Public Sector in USA & Korea

So-Jeong KIM†

ABSTRACT

USA is strengthening the information security by managing federal agency's information and information system systematically. For this purpose, US government put the Federal Information Security Management Act into the E-Government Act of 2002. According to the FISMA, it is required to have information security management plan for all federal agencies. In addition that, Inspector Generals of these agencies should assess the status of their agency and report the result to the Office of Management and Budget. Collecting all the reports from each agency, OMB should report to GAO on general status of information security of federal agency. It is helpful to provoke the information security as a necessary activity to realize the E-government. Comparing these efforts with our system will give us good implications to get more idea to secure our information system.

Key Words : FISMA, NIST SP 800-53, FIPS 200, Security Controls

1. 서 론

미국은 전자정부법(E-Government Act) 제3편에 연방정보보안관리법(FISMA : Federal Information Security Management Act of 2002)을 삽입 통과시켰다. 연방정보보안관리법은 연방정부의 IT 시스템에 대한 적절한 보안 수준을 유지하고 연방기관과 국립표준기술원(NIST) 및 관리예산처(OMB)에 정보시스템의 보안을 강화하도록 하고 있다. 특히 각 연방기관의 장이 비용 효율적으로 IT보안위험을 줄여 감내할 만한 수준으로 위험을 최소화할 수 있는 정책과 절차를 실행할 것을 요구한다. 또한 NIST 주관으로 연방정보보안관리법 실행 프로젝트를 실행하여 미국 연방정부의 정보 및 정보시스템을 보호해 안전한 미국연방정부 설립이라는 목적을 달성하고자 한다.

본 논문에서는 미국의 연방정보보안 관리체계와 우리나라의 국가 및 공공영역의 보안관리체계를 비교해 보고자 한다. 이를 위해 미국의 연방정보보안관리법, NIST SP 800-53, FIPS 200 및 2004 OMB 의회보고서 등을 분석하고자 한다. 또한 우리나라의 국가사이버안전관리규정 및 국가사이버안전매뉴얼을 살펴보고 매뉴얼에서 제시하고 있는 평시 안전점검 체크리스트에 대해서도 살펴보고자 한다.

2. 미국의 정보보안 강화 노력

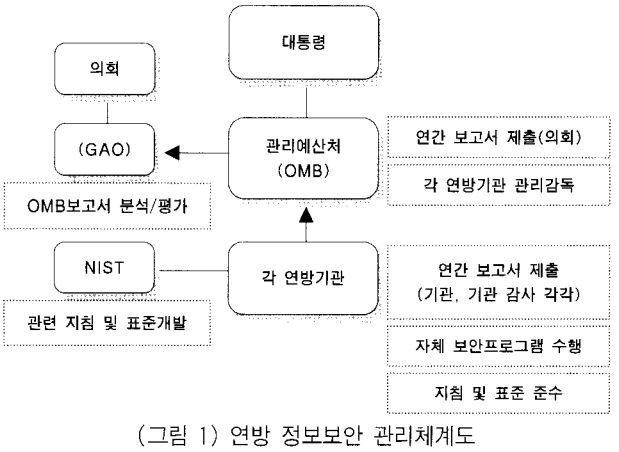
2.1 법적근거 : 연방정보보안관리법

연방정보보안관리법은 미국 전자정부법 제3편에 해당하며

† 정 회 원 : 국가보안기술연구소 정책연구실 연구원
논문접수 : 2005년 11월 25일, 심사완료 : 2006년 1월 5일

각 연방기관의 정보보안 강화를 위한 법제도적 근거가 되고 있다. 동 법에 따라 각 연방기관은 자신의 정보 및 정보시스템에 대한 보안관리를 강화해야 하고, 관리예산처 및 일반회계감사원 등은 이를 관리 감독해야 한다. 同 법의 목적은 1)연방정부의 운영 및 자산에 대한 정보보안 통제항목의 효율성을 강화하기 위한 총괄적인 프레임워크 제공, 2)연방 컴퓨터 환경이 네트워크화 되어 있음을 자각하고 민간, 국가보안 및 법집행기관 전반에 걸친 관련 정보의 보안 위험에 대한 효율적인 관리 및 통제방안 제공, 3)연방 정보 및 정보시스템 보호를 위한 최소한의 통제 및 유지 방안 개발, 4)연방기관의 정보 보안 프로그램의 관리를 강화하는 메커니즘을 제공한다.

연방정보보안관리법은 정보보안 통제의 정확성과 효율성을 보장하기 위해 각 기관별 프로그램 담당자와 최고정보화 담당관(CIO) 및 감사(Inspector Generals)가 해당 기관의 정보보호 프로그램에 대한 연간 검토를 수행하도록 하고 이를 OMB에 보고하도록 했다. OMB는 이 데이터를 사용해 의회에 주요 내용을 매년 보고하고, 각 기관의 정보보안 프로그램에 대한 관리를 하고 있다. 또한 OMB는각 부처와 독립감사관들이 제공한 보고서에 기초하여 각 부처의 연방정보보안관리법 실행에 대하여 매년 의회에 보고서를 제출하고 있다. 이와 동시에 연방정보보안강화를 위해 NIST 주관으로 연방정보보안 실행 프로젝트(FISMA Implementation Project)를 추진하고 있다. 연방정보보안관리법 체계에 따른 연방 정보보안 관리 체계도를 도식화하면 (그림 1)과 같다.



(그림 1) 연방 정보보안 관리체계도

이러한 체계적인 연방정보보안 강화 활동을 통해 1)정보시스템에 적용 가능한 보안 통제 항목이 좀 더 일관되고 비교가능하며 반복적으로 수행할 수 있는 평가 체계를 갖추고, 2)정보시스템 운영에 따른 기업 임무의 위험에 관한 이해를 돕고, 3)상위 관료들이 신뢰할 수 있는 경쟁력 있는 정보를 전달함으로써 보안 인증 절차를 위한 확실한 정보를 제공하고, 4)미국 주요기반보호시설을 포함한 미 연방정부의 정보시스템을 더욱 안전하게 하는 것을 목표로 한다. 연방정보보안관리법 실행 프로젝트는 다음의 3단계로 추진된다.

- 1단계 : 보안 표준 및 지침 개발
- 2단계 : 조직적인 인증(Accreditation) 프로그램
- 3단계 : 보안 툴(Tool) 검증 프로그램

미국 정부는 2005년 말까지 1단계를 마무리하고 2006년부터 2단계를 추진하고자 한다.

2.2 표준 및 지침개발

국립표준기술원(NIST)은 위험 수준별 적절한 정보보안을 제공할 목적으로 연방 정부 부처들이 정보와 정보시스템을 범주화할 수 있는 표준을 제공하기 위해 노력하고 있다. 또한 각 범주에 포함될 수 있는 정보와 정보시스템의 유형을 권고하는 지침을 개발하고 각 범주의 정보와 정보시스템을 위한 관리, 운용 기술적 통제와 같은 최소한의 정보보안 요구조건을 수립하기 위해 노력하고 있다.

이에 FISMA Implementation Project 1단계에서는 법률 제정 및 연방정보보안관리법 관련 세부 발간물을 통해 보안과 관련된 표준 및 지침을 개발하는 것을 목적으로 한다. 이는 정보 보안 프로그램을 더욱 안전하게 하고 연방기관의 운영과 자산의 위험을 최소화해 효율적으로 관리할 수 있게 된다. 아래에서는 1단계에서 개발된 표준 및 지침 중 보안통제항목 설정과 관련된 NIST SP 800-53 및 FIPS 200에 대해서 살펴보고자 한다.

2.3 NIST SP 800-53

NIST SP 800-53(Recommended Security Controls for Federal Information Systems, Feb. 2005)은 연방정부의 행정기관의 정보시스템에 대한 보안 통제항목을 구체화하고 이를 지정하기 위한 지침이다. 여기서 보안통제라 함은 정보시스템 및 그 정보의 기밀성, 무결성, 가용성을 보장하기 위해 해당 정보시스템에 설치되거나 운영되는 관리적, 운영적, 기술적 세이프가드나 대응책을 말한다.

즉, 연방정보보안관리법 및 관련 지침이 규정하는 적정한 수준의 보안 상태(adequate security)를 모든 연방정부기관에 실현하는 것이 동 지침의 궁극적 목표이다. 따라서 각 기관의 정보보안프로그램과 병행 및 이에 포함되어 실시되어야 그 효율을 극대화 할 수 있다. 정보보안프로그램에는 다음 사항이 포함되어야 한다.

- 주기적 위험 평가
- 도출된 위험을 줄이는 정책 및 절차 수립
- 위험 평가 결과에 따른 세부 정보시스템 보안 강화 계획 수립
- 직원에 대한 보안 인식 교육
- 보안 정책의 주기적 테스트
- 보안 정책, 절차, 실행을 보완하는 과정
- 보안 사고 탐지, 보고 및 대응 절차
- 업무 연속성 보장 계획

800-53은 연방정부의 정보시스템에 대한 보안 통제항목을 구체화하고 이를 지정하기 위한 지침이다. 동 지침은 연방 정부 내의 안전한 정보시스템 구현을 목표로 개발되었으며 주요목표는 아래와 같다.

- 정보시스템의 보안 통제항목 구체화 및 선정에 있어서 일관되고 비교 가능하며 반복 가능한 방법 제공
- FIPS 199에 따른 정보시스템 분류에 사용될 최소한의 보안 통제항목 추천
- 정보시스템에 대한 보안 통제항목의 가변적이며 확장 가능한 카탈로그를 만듦으로써 변화하는 기술 및 요구사항의 수요를 만족시키고자 함
- 보안 통제의 효율성을 결정할 수 있는 평가 방법 및 절차 개발 기초 수립

동 지침은 미국 헌법 3542조에서 규정하고 있는 국가보안시스템을 제외한 모든 연방 정보시스템에 적용가능하다. 동 지침은 강제사항은 아니지만 미국의 주요기반 시설을 구성하는 주 및 지방 정부, 민간 영역의 조직들도 동 지침에 따라 줄 것을 촉구하고 있다.

800-53의 보안 통제항목은 NIST SP 800-25, 국방부 Policy 8500, DCID[2] 6/3, ISO/IEC 표준 17799, GAO 연방정보시스템 통제감사메뉴얼(FISCAM), 건강 및 인력서비스(Health and Human Services)[3]의 메디케어와 메디케이드 서비스 센터(Centers for Medicare and Medicaid Services)의 핵심보안요구사항(Core Security Requirements)을 기반으로 각계의 의견을 수렴하여 작성되었다.

각 기관은 FIPS 199를 기반으로 각 기관의 정보시스템의 등급을 구분하고 등급에 따른 보안통제항목을 800-53을 참고해 수립한다. 800-53은 최소한의 가장 기본적인 보안통제항목만을 포함하고 있으므로, 각 기관은 기관의 특성을 고려한 보안 관리정책을 각자 수립해야 한다. 안전한 정보시스템을 구축하기 위해서는 아래의 요건을 모두 갖추어야 한다. 이 외에도 지속적인 예산 투자 등의 관리적 노력도 필요하다.

- 시스템 수준의 보안 요구사항 및 보안 명세서 정의
- IT 제품에 대한 상세 설계
- 부속품을 전체 정보시스템에 효율적으로 통합하기 위한 안전한 시스템 및 보안 기술 원칙 및 실행
- 제품 및 시스템에 대한 적절한 테스팅 및 평가
- 총괄적인 시스템 보안 계획 및 생명주기 관리

800-53의 보안통제항목은 크게 관리적, 운영적, 기술적 측면에서 고려되고 있다. 동 지침에서 다루고 있는 보안 통제 항목은 <표 2>와 같다.

2) Director of Central Intelligence Directive

3) GAO의 연방정보시스템 통제감사 매뉴얼(Federal Information System Controls Audit Manual)로 GAO 감사 및 기관 감사들이 기관 평가 시 사용한다.

〈표 1〉 NIST SP 800-53 보안통제항목 분류표

No.	대분류	중분류	식별기호
1	관리	위험평가	RA
2		계획	PL
3		시스템 및 서비스 획득	SA
4	운영	인증, 인정 및 보안 평가	CA
5		개인 보안	PS
6		물리적 및 환경적 보호	PE
7		연속성 계획	CP
8		Configuration 관리	CM
9		유지	MA
10		시스템 및 정보 무결성	SI
11		Media 보호	MP
12		사고 대응	IR
13		인식 및 훈련	AT
14	기술	Identification and authentication	IA
15		접근통제	AC
16		감사 및 책임	AU
17		시스템 및 통신 보호	SC

각각의 통제항목은 부록F 보안통제항목 카탈로그(Appendix F Security Control Catalog)에서 세부적으로 기술되고 있다. 각각의 통제항목은 집약된 통제 명제를 제시하고 있는 통제(control) 섹션, 관련 법률 및 통제 섹션과 연계해 수행되어야 할 항목을 설명한 관련지침(supplemental guidance) 섹션과 통제항목 강화(control enhancement) 섹션으로 구성되어 있다. 통제항목 강화 섹션은 1)기본 통제항목에 관련되었지만 부수적인 기능 첨가, 2)기본 통제항목의 강화를 목적으로 하는 내용이 기술된다.

각 기관의 자신의 정보시스템에 맞는 기본 보안 통제항목을 800-53을 참고해 설정하고 이를 공통 보안 통제항목(common security controls)이라 부른다. 이 외에도 각 기관의 특성에 맞는 보안 요구사항을 첨가하는데 이는 시스템 특성을 고려한 통제항목(system-specific controls)이라 부른다. 이렇게 구분해서 적용하는 시스템은 비용 효율적이며, 일관된 정책을 보유할 수 있고, 인증 및 인정 절차의 비용 절감 및 효율성 증대 효과를 가져 올 수 있다.

low baseline을 위한 보안 통제항목에서는 보안 관리가 실행되고 있으며, 특별한 실행 미완이나 결점이 드러나지 않고, 결점이 드러난다고 해도 정해진 절차에 따라 빨리 해결될 수 있는 상태를 말한다. moderate baseline은 결점이 발견되었을 때 빨리 기능 및 목적에 맞는 역할을 할 수 있도록 수정할 수 있는 상태를 말한다. high baseline은 업무 연속성을 해치지 않을 수 있는 지속적인 통제 기능 및 지원이 가능한 상태를 말한다.

동 통제항목들은 1)통제항목 실시의 경험에 따른 개정 필요성이 제기되거나, 2)조직 내 보안 요구사항이 변경된 경우, 3)적용 가능한 새로운 보안 기술이 있는 경우에 변경되거나 확장될 수 있다.

조직의 위험 관리를 위해서는 1)위험 평가, 2)비용대효율 분석, 3)보안 통제항목 선택, 실행, 평가, 4)정보시스템 운영을 공식적으로 승인하는 과정을 따른다.

- 분류 : 정보시스템 및 시스템 내부에 있는 정보를 FIPS 199의 영향력 분석을 통해 분류
- 선택 : FIPS 199 보안 분류에 기반해 기본이 되는 정보시스템 보안 통제항목(예, baseline) 선택
- 조정 : 위험 평가에 기반한 보안 통제항목과 조직 특성을 반영한 보안 요구사항, 특정 위협 정보, 비용대비효과 분석, 대체 통제항목의 활용 가능성, 특정상황 등을 수용해 보안통제항목 조정
- 문서화 : 합의 및 조정된 보안통제항목 문서화
- 실행 : 정보시스템에 보안통제항목 적용
- 평가 : 실행된 보안통제항목이 적절한 방법과 절차를 통해 실행되고 있는지, 의도된 목적대로 운영되고 있는지, 시스템이 요구하는 보안 요구사항을 충족시키는 등의 좋은 결과를 내놓고 있는지 등에 대해 평가
- 결정 : 조직 운영 및 자산의 위험 식별
- 승인 : 조직의 운영 및 자산에 대한 위험 정도가 감내할 만한 수준인 경우 정보시스템 처리절차 승인
- 감시 : 지속적으로 정보시스템에 대한 보안통제항목 감시 및 평가. 필요한 경우 시스템 변화 기록, 관련 변화에 따른 보안 영향 분석, 시스템 실태를 해당 관리자에게 주기적으로 보고

기본 통제항목에 각 기관이 요구하는 보안 범위를 설정하고 통제항목을 구체화한 뒤, 대체 가능한 통제항목이 있는지 등에 대해 고려한 다음 보안통제항목을 재구성하고, 이를 보안계획 안에 문서화한다.

보안대체항목은 기술 측면, 인프라 측면, 대중의 접근 가능성 측면, 범위 측면, 공통 보안 통제 측면 및 위험 측면의 다각적인 면에서 고려해야 한다.

각 기관은 FIPS 199를 기반으로 각 기관의 정보시스템의 등급을 구분하고 등급에 따른 보안통제항목을 NIST SP 800-53을 참고해 수립한다. NIST SP 800-53은 최소한의 가장 기본적인 보안통제항목만을 포함하고 있으므로 각 기관은 기관의 특성을 고려한 보안 관리정책을 각자 수립해야 한다.

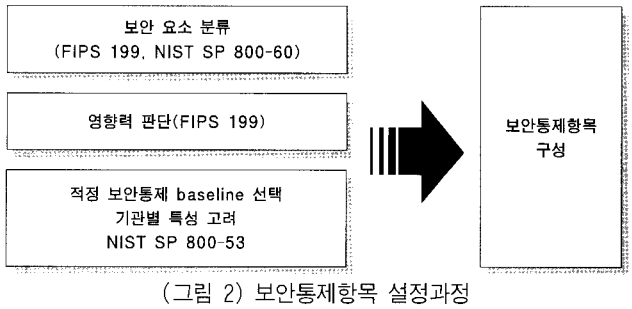
2.4 FIPS 200

FIPS Publication 200 연방정보 및 정보시스템에 대한 보안 최소 요구사항(Minimum Security Requirements for Federal Information and Information Systems)은 NIST SP 800-53과 함께 기관의 보안 통제항목을 설정하는 기준이 된다.

FIPS 200은 1)연방정보 및 정보시스템에 대한 보안 최소 요구사항 명시, 2)보안 분류 표준인 FIPS 199를 활용한 표준화된 보안 통제 선택, 3)최소 보안 요구사항을 반영하여 보안 통제항목을 설정하는데 NIST SP 800-53과의 연계 활용방안을 제시함으로써 각 기관의 최소한의 보안통제항목 선택의 기준이 된다.

- 접근 통제 강화
- 인식 및 훈련 실시
- 정보보안 시스템에 대한 감사를 실시하고 개별 사용자는 자신의 컴퓨터 사용 활동에 대해 추후에도 책임을 지고 이를 설명할 수 있어야 하며
- 인증, 인정 및 보안평가 실시
- configuration 관리
- 연속성 계획 수립
- 식별 및 인증 체계 수립
- 사고 대응 절차 마련
- 정보시스템의 주기적인 업데이트 및 유지관리 실시
- 출력물 형태 혹은 디지털 미디어 형태의 정보에 대한 보호대책 수립
- 물리적 및 환경적 보호
- 정보보안 계획의 수립, 실행, 문서화 등에 관한 주기적인 업데이트 및 관리체계 마련
- 개별 직원의 보안의식 강화
- 위험 평가
- 시스템 및 서비스 획득에 관한 절차 수립
- 시스템 및 통신 보호 대책 수립
- 시스템 및 정보 무결성 보장 등의 영역에 대한 최소 보안요구사항 명시

각 기관은 NIST SP 800-53의 보안통제항목을 설정하는데 있어 FIPS 200의 보안 최소 요구사항을 반영하고 이에 따른 영향 정도를 판단해야 한다. 보안 분류 및 통제항목을 통해 각 연방부처는 기관별 요구사항을 반영한 보안 통제항목을 설정할 수 있다. 이를 도식화하면 아래 그림과 같다.



(그림 2) 보안통제항목 설정과정

2.5 대통령 현안관리보드

미국의 경우 전자정부사업 추진 시 정보보안을 대통령 관리 사업(PMA : President's Management Agenda)[4] 보드에 포함시켜 그 책임을 최고 관리자급으로 끌어 올렸다. 즉 정보통신보안은 전자정부확대 보드에서 녹색[5]을 받기 위해 필

4) PMA는 2001년 8월에 연방정부의 업무 효율을 개선시키기 위한 전략으로 시작되었다. PMA 5개 주요 프로젝트 중 전자정부확대(Expanded Electronic Government) 프로그램이 있는데 동 프로그램은 연방정부의 연간 정보통신에 대한 투자를 확대해 국민에게 봉사하고 시스템을 안전하게 하며, 정확한 시간에 서비스를 전달하고 예산을 효율적으로 사용하는 것이다. OMB, Federal Information Security Management Act 2004 Report to Congress, 2005. 3.

5) 매 분기마다 각 기관은 OMB에 목표 달성을 위한 기관의 노력 결과를 보고해야 한다. 이 보고를 통해 목표 성취 여부를 적색(심각한 결함을 단 하나라도 갖고 있는 경우), 황색(모든 기준에서 중간 수준 이상을 달성한 경

수적으로 만족시켜야 할 요소 중의 하나로 구성함으로써 보안 기준이 충분하지 않으면 다른 전자정부관련 기준에 대한 성취도가 높을지라도 좋은 결과를 받을 수가 없도록 했다. 이를 위해 각 기관은 아래의 보안 기준을 만족시키기 위해 노력해야 했다.

- 보안 취약점 개선을 위한 지속적인 노력을 보여줄 것
- 기관 OS의 90% 이상을 인증 및 인정받기
- 감사가 평가하고 검증한 POA&M 유지
- 모든 시스템에 대한 인증 및 인정받기
- 보안 통제항목에 따른 시스템 설치 및 유지
- 운영상의 연속성 보장이 가능한 형태로 기관의 모든 인프라 통합 및 최적화

미국의 경우 정부차원의 활동을 통해 기관 관리자의 동기를 부여하고 개선 영역을 더욱 더 강화함으로써 긍정적 요인을 줌으로써 보안강화를 기관장의 차원에서 적극적으로 실시하도록 고무시킨 것이다.

3. 우리나라의 정보보안 강화 노력

3.1 국가사이버안전관리규정

우리나라는 사이버위협과 관련한 국가차원의 대응체계 구축을 위해 국가사이버안전관리규정을 제정하였다. 동 규정과 국가위기관리기본지침(대통령훈령 제124호), 국가정보보안기본지침, 사이버안전분야 위기관리표준매뉴얼 등의 관련 내용을 준용해 국가사이버안전매뉴얼을 개정하였다.

국가사이버안전관리규정에 따라 국가사이버안전전략회의, 국가사이버안전대책회의 등의 관련 업무 수행체계와 조직 및 기구의 역할을 정립하였다. 이를 통해 사이버안전 활동 역량을 통합하고 피해 발생 시 체계적이고 유기적 대응을 함으로써 정보통신망의 안전을 확보하고자 한다.

동 규정 및 국가사이버안전매뉴얼에 따라 각급기관은 기관 수준에 맞는 보안점검 기준을 충족시킬 수 있도록 지속적으로 노력해야 하며, 특히 사고 발생 시 이를 민첩하고 노련하게 대응 및 복구하기 위한 절차를 숙지하도록 하고 있다.

이외에도 국가사이버안전센터의 역할을 규정하였으며 사이버안전대책의 수립·시행에 있어서의 관련기관간 정보협력을 의무화하고 있다. 이러한 정보를 바탕으로 사이버위협에 대해 4단계로 경보를 발령하고 있으며 사고 발생 시 통보 및 복구, 조사 및 처리 등의 절차를 마련함으로써 체계적이고 즉각적인 대응이 가능하도록 하고 있다.

이를 위한 전문 인력의 양성, 교육 및 홍보와 관련 기술의 연구개발에 관해 규정하고 있으며 이를 위한 예산에 대해 규정하고 있다.

우), 녹색(성공적으로 모든 기준을 만족시킨 경우)으로 구분한다. 각 기관은 공개적으로 해당 목표를 달성할 의무가 있으며 그 결과는 아래 홈페이지에 공개된다. http://results.gov/agenda/scorecard.html

3.2 평시 안전점검 체크리스트

우리나라는 국가사이버안전관리규정 제9조 제4항에 의거하여 정보통신망에 대한 안전성 확인을 위한 정보시스템 중요도에 따른 보안대책 수준을 평가하고 있다. 특히 기관별로 운영하고 있는 정보통신망의 중요도가 상이함에도 불구하고 동일한 보안관리 기준을 적용하여 보안대책을 강구함에 따른 불합리한 면을 개선하여 각급기관 스스로 정보보안 수준을 진단하고 이에 따른 정보보안대책을 수립함으로써 정보보안 사각지대를 해소하였다.

국가사이버안전매뉴얼에 따르면 대상기관을 수행업무의 중요도(수행업무의 국가사회적 중요도, 인원 및 서버규모), 정보시스템 및 정보중요도(정보 중요도, 정보시스템 의존도, 대외업무연계 정도), 피해분석(위협발생 가능성, 피해영향 정도) 등의 방법을 통해 대상 기관을 '가'급, '나'급, '다'급으로 분류하고('가'급기관의 중요도가 가장 높음) 기관의 등급에 따른 점검항목을 적용하고 있다.

또한 각급기관이 자체적으로 보안관리 상태를 평가하는데 활용할 수 있는 보안관리 기준을 마련하고 평시 안전점검 체크리스트를 만들었다. 체크리스트에는 9개 대분류, 33개 중분류, 81개 소분류, 254개 소소분류로 구성되어 있다. 254개 소소분류 체크리스트는 모두 'A', 'B', 'C' 급으로 나누어져 있는데 가장 기본적인 보안이 되는 부분이 'A'급이고, 'C'급은 가장 강력한 보안을 유지해야 하는 기관인 경우 체크 관리해야 할 체크리스트 항목이다.

〈표 2〉 체크리스트 대분류 및 중분류 내용

No.	대분류	중분류	No.	대분류	중분류
1	정보보안 관리체계	정보보안정책	17	접근 보안대책	정보시스템 보안
2		정보보안조직	18		사용자 인증 및 계정관리
3	정보보안 계획 및 활동	정보보안계획	19		응용프로그램 접근통제
4		사용자정보보안 활동	20	운영관리	운영상의 변경통제
5		정보보안사고 예방 및 대응	21		서비스 관리
6		정보보안감사	22		상용 정보보호시스템 보안
7	정보자산 통제	정보취급 절차	23		악성코드 관리
8		정보자산 도입 및 폐기	24		PC보안 관리
9		매체관리	25		로그 및 모니터링
10	인적 보안	인원 보안	26		백업
11		정보보안교육 및 훈련	27	시스템 개발 및 유지보수	시스템 개발 및 정보보안 요구사항
12		정보보안의식 및 환경조성	28		운영소프트웨어 보안
13	물리적 보안	시설보안	29		외주관리
14		재난복구대책	30	보안 시스템	암호사용
15	접근 보안대책	접근 보안지침	31		암호장비
16		네트워크 보안	32		암호자재
			33		암호논리

254개 체크리스트 중 'A'급은 140개, 'B'급은 82개, 'C'급은 32개이다. 즉 대상기관별 보안 중요도가 높은 '다'급 기관

인 경우 254개 체크리스트를 모두 만족시켜야 한다.

각급기관은 평시 안전점검 체크리스트를 준용해 각 기관별 수준에 맞는 정보보안대책을 수립하고 이를 유지할 수 있도록 노력해야 한다.

4. 결 론

미국 연방정부는 정부의 정보 및 정보시스템에 대한 연방정보보안관리법을 적용하며 각 기관의 정보보안을 강화하기 위한 프레임워크를 제시했다. 아울러 이를 보다 구체적으로 실행하기 위해 NIST로 하여금 연방정보보안관리법 실행 프로젝트를 실시하도록 했다. 즉 상위법인 연방정보보안관리법을 통해 원칙을 제시하고, FIPS 199 및 FIPS 200을 통해 보안 항목을 분류하고 이에 요구되는 최소 보안 요구사항을 정의함으로써 NIST SP 800-53의 수준별 보안통제항목을 설정하고 기관의 특성을 고려해 각 기관의 보안 수준을 결정하고 필요한 보안 통제항목을 설정하는데 기초가 될 수 있도록 하고 있다.

우리나라의 경우 국가사이버안전관리규정을 통해 사이버안전 관리체계를 구축해 나가고 있다. 국가사이버안전관리규정의 경우 우리나라의 사이버안전체계를 구축하는데 필요한 가장 큰 그림이며 각 기관의 정보보안을 강화할 수 있는 밑거름이 되고 있다. 하지만 미국의 FISMA와 비교했을 때는 몇 가지 차이점을 갖고 있다. 첫째, 국가사이버안전관리규정 및 체크리스트에는 FISMA의 OMB나 GAO와 같은 관리감독 기관의 역할이 규정되어 있지 않고, 이러한 관리활동의 결과에 대해 환류(feedback)해 주는 기능이 없다. FISMA에 따른 각 기관 감사들의 자체 감사활동, 이를 OMB에 보고하고 OMB가 이를 다시 의회에 보고함으로써 객관적 실태 파악이 가능하도록 한 점, 同 보고서를 의회의 GAO가 다시 검토하는 과정을 거쳐 이를 평가하고 향후 발전하는 원천으로 삼고 있는 데 반해 우리나라의 관련 규정은 관리활동의 향후 활용에 대한 내용이 언급되지 못하고 있다.

둘째, FISMA의 경우 NIST에서 보안관리활동과 관련한 규칙 및 지침을 개발하여 각 연방기관의 보안관리활동을 지원할 수 있도록 해주는데 비해 우리나라의 경우 이러한 역할에 대한 명시적 언급이 없어 각 기관이 실질적으로 보안관리활동을 수행하는데 있어 지원받을 수 있는 근거가 없다.

셋째, FISMA는 FIPS 199를 통해 보안 관리 활동 대상을 국가보안시스템 및 일반보안시스템 등으로 구분하고 보안시스템의 등급별 보안 활동을 유도하고 있는데 반해 우리나라의 경우 기관별 등급에 따른 보안관리 활동을 요구하고 있다.

이러한 차이점에도 불구하고 본문에서 언급한 규정 및 체크리스트는 보안관리 활동 사이버테러 대응 체계를 구축하는 첫 출발점이 되었다는 점에서 큰 의의를 지니고 있다. 다만 우리나라도 각급기관장의 인식을 제고하고 의사결정시 정보보안을 중요시할 수 있는 제도적 뒷받침을 둠으로써 국가 전체의 정보 및 정보시스템의 안전성 강화를 유도하는 것이 바람직할 것이다. 따라서 향후 국가 사이버안전 관리를 강화할 수 있도록 하기 위해 관련법을 비교분석하여 제안하는 것이 바람직할 것으로 판단된다. 본 논문을 통해 미국의 연방정보보안관리법 및 이에 따른 정보보안통제항목에 대한 분석을 통해 우리나라의 정보보안 관리체계 개선을 위한 참고자료로 활용하고 이를 적용해 정보보안관리 부분에서 Best Practice가 될 수 있도록 진일보한 정보보안 관리체계를 구축하는데 도움이 되었으면 한다.

참 고 문 헌

[1] Federal Information Security Management Act of 2002.

[2] ISO 17799, A Code of Practice for Information Security Management (British Standard 7799).

[3] NIST SP 800-53 *Recommended Security Controls for Federal Information Systems.*

[4] FIPS Publication 200 *Security Controls for Federal information Systems.*

[5] Office of Management and Budget, "FY 2004 Report to Congress on Federal Government Information Security Reform", 2005. 4.

[6] GAO, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, 1999. 1.

[7] 대통령훈령 제141호 국가사이버안전관리규정

[8] 국가정보원, *국가사이버안전매뉴얼*, 2005. 10.

[9] 김소정 외, "미국 FISMA Implementation Project 소개," WISC2005, 2005. 9.

[10] 국가보안기술연구소 정책연구실, Security Issue 2005-2 미국 연방정보보안관리법 체계 및 동향, 2005. 10.

김 소 정

e-mail : sjkim@etri.re.kr

1994년 부산대학교 사학과(학사)

2001년 경희대학교 평화복지대학원 동북아학과(석사)

2005년 고려대학교 정보보호대학원 정보보호정책학과(박사)

2001년~2002년 한국전파진흥협회 ITU-WRC 담당 연구원

2004년~현재 국가보안기술연구소 정책연구실 연구원

관심분야 : 정보보호정책, 정보보안관리체계, 개인정보보호 등