情 報 保 護 學 會 誌
第 13 券 第 3 號, 2003. 6

미국 전자정부 정보보안 법제 동향

김 대 호*, 오 일 석**

요 약

미국은 전자정부 구현을 위하여 각종 법규를 제정하였고 이를 통합하여 2002년에 전자정부법을 제정하였다. 그리고 동 법을 제정하면서 전자정부의 성공이 정보보안에 있다는 사실을 인식하고 전자정부법에 연방정보보안관리법을 삽입하여 통과시켰다. 이를 통하여 전자정부의 실현과 관련하여 연방 각 부처로 하여금 정보보안의 이행을 실질적으로 추진하고 보고하도록 하는 연방 정부의 체계적인 정보보안 정책을 확립하였다. 이러한 미국의 전자정부에 대한 정보보안 정책 확립은 우리나라 전자정부의 구현과 실행에 있어 체계적인 정보보안 정책 수립의 필요성과 중요성을 다시금 일깨우고 있다고 할 것이다.

Ⅰ. 서 론

미국 부시 대통령이 2002년 12월 17일 전자정부법(Electronic Government Act of 2002)에 서명함으로써 관리예산처내에 전자정부국을 신설하고 정보화책임관 회의에 대한 법적 근거를 마련하였으며 전자정부 기금을 조성할 수도 있게 하는 등 전자정부의 실질적 구현을 위한 법적 장치를 확립하게 되었다. 이와 동시에 동 법에 연방정보보안관리법을 삽입하여 제정함으로써 전자정부 정보보안을 위한 연방 정부의 노력을 결집시켰다. 본 논문에서는 이러한 미국의 전자정부의 구현과 전자정부 정보보안을 위한 법제 동향을 살펴봄으로써 향후 우리나라 전자정부에 대한 체계적인 정보보안 정책 수립을 위한 토대를 마련하고자 한다.

본 논문의 구성은 다음과 같다. 제2장에서는 미국의 전자정부 추진 배경을 살펴보고 제3장에서는 미국의 전자정부 관련 각종 법규를 살펴본 후, 제4장에서는 전자정부 정보보안을 위한 각 종 법들을 고찰 한 후 제5장에서 결론을 내리고자 한다.

Ⅱ. 미국 전자정부 배경

미국의 전자정부 구현을 위한 노력이 어느 정도 가시화된 것은 신보수주의와 세금 감면을 주요 정책으로 한 레이건과 부시 정부에 의한 엄청난 재정적자를 줄이면서 동시에 공공서비스 개선을 주장한 클린턴 정부의 등장과 함께였다. 클린턴 정부는 출범과 더불어 국가정보기반(National Information Structure: NII) 구축사업과 국가행정성과평가(National Performance Review) 사업을 중심으로 행정개혁 작업에 착수하여 재정적자의 축소와 공공서비스 개선을 시도하였다. 엘고어 부통령의 주도로 시작된 국가정보기반 구축사업은 미 국민들이 정부와 각종 기관의 데이터에 접근할 수 있는 시스템을 확립함으로써 국민들에게 디지털 형태의 정부 서비스를 제공받을 수 있는 전자정부를 구축하려고 하였다. 국가행정평가 사업은 기존의 행정과정과 절차에 대한 근본적인 개혁을 통하여 연방 정부의 낭비적 요소를 줄이고 성과 지향적인 전자정부를 이룩하려고 하였다.

이러한 미국 정부의 노력은 정부업무수행관리법(Government Performance Results Act of 1993(GPRA), Pulic Law 103-62), 정부문서감축법(Government Paperwork Reduction Act), 정보기술관리개혁법(Information Technology Management Reform Act of 1996, Public Law 104-106) 등 관련 법률들의 제정과 개정을 통하여 체계적으로 정비되었으며, 지난 2002년 12월 17일 부시

* 국가보안기술연구소 소장
** 국가보안기술연구소 연구원

대통령이 전자정부법(e-Government Act of 2002)에 서명함으로써 전자정부의 실질적 구현을 위한 법제의 결실을 보게 되었다.

Ⅲ. 미국 전자정부 관련 법규

1. 정부업무수행결과법(Government Performance Result Act of 1993(GPRA), Public Law 103~62)

정부업무수행결과법은 연방 행정기관으로 하여금 업무수행에 있어 낭비와 비효율을 제거하기 위하여 전략적 계획을 수립하고 이를 관리예산처장(Director of the Office of Management and Budget)과 연방 의회에 제출하도록 하고 있다. 정부업무수행결과법은 정부문서감축법의 주된 수행기관인 관리예산처를 동법의 시행과 관련한 주무부서로 하고 있다. 또한 관리예산처장은 각 행정기관으로 하여금 업무수행 성과 목표를 확립하고 이러한 목표를 정량적이고 계량적인 형태로 명시하며 성과목표를 달성하기 위한 운영 절차, 인적 물적 자원, 업무수행 성과지표의 확립 및 실제 결과와 목표와의 비교 등을 포함한 연례업무수행계획을 준비할 것을 요구할 수 있도록 하고 있다.

2. 정보기술관리개혁법(Information Technology Management Reform Act of 1996, Public Law 104~106): 일명 Clinger-Cohen법

정보기술관리개혁법은 미국 연방정부의 정보기술관리에 관하여 규정할 목적으로 IT 관련 조달, IT 투자 계획, 정보화담당관(Chief Information Officer)제의 확립 및 IT 성과 측정의 요건을 기술하고 관리예산처장으로 하여금 연방 정부가 획득한 IT의 검토와 관리에 대하여 궁극적인 책임을 지도록 하였다. 즉, 정부문서감축법을 수정하여 행정기관의 정보기술 관리 실태를 개선하기 위하여 관리예산처장에게 상당한 권한과 책임을 부여한 것이다.

3. 정부문서감축법(Government Paper Reduction Act)

정부문서감축법은 1980년에 제정되어 연방 정보자원 관리(Imformation resource Management : IRM)에 대한 단일 정책틀을 확립하였다. 즉, 대통령 직속의 관리예산처를 중심으로 각 기관의 문서감축과 범 정부적 정보관리의 효율성을 목표로 제정되어 전자정부 구현을 위한 중요한 법적 기틀을 확립하였다.

이후 정부문서감축법은 1986년 개정되어 문서활용과정에서 일반 대중의 접근을 가능하게 하고 관리예산처로 하여금 정보관리정책을 개발하고 유지하도록 하였으며, 정보자원 관리에 대하여 별도의 정의(定議) 규정을 두었으며, 각 기관에 대하여 정보자원관리에 대한 책임을 부과하였다.

1995년 개정법에서는 관리예산처내에 정보규제국(Office of Information and Regulatory Affairs)을 신설하였다. 또한 관리예산처장으로 하여금 연방 정보자원관리 정책과 지침을 개발, 시행 및 감독하고, 정보의 공개와 공유 및 보안과 정보기술의 습득과 사용을 감독하고 이에 관한 지침을 제정할 권한을 부여하였다. 동 법에 의하여 1996년 관리예산처는 OMB Circular A-130을 발표하여 연방정부 공통의 단일 정보자원관리 정책을 도입하였다.

1998년 정부문서감축법은 전자서명을 사용하여 정보전송자의 신원과 그 내용의 진실성을 확인할 수 있도록 하였으며 미국 통신정보청(National Telecommunications and Information Administration)과의 협력으로 문서감축과 전자상거래상의 전자서명의 사용, 프라이버시 보호 및 정보 보안과 신뢰성 확보에 대한 연구를 수행하며 이를 의회에 보고하도록 하고 있다.

4. 전자정부법 2002(e-Government Act of 2002)

4.1 제정 배경 및 경과

미국 정부는 정보기술을 이용한 정부혁신과 국민을 정부의 고객으로 지향하는 열린 정부의 구현을 위하여 앞에서 살펴본 것과 같이 법 제도를 정비하여 전자정부의 구현을 위한 기틀을 확립하였다. 미국 정부는 이러한 법 제도에 기초하여 그동안 구축한 국가정보인프라를 실질적인 행정 효율화 및 대민서비스 제고로 연결시키기 위하여 각 정부 부처의 전자정부 관련 정책 및 시스템의 연계를 강화하고 전자정부 구축을 위한 조직체계 개편에 역점을 둔 전자정부법의 입법을 추진하게 되었다. 2001년 5월

민주당 리버만 상원의원이 전자정부 구축을 위한 전담기관으로서 전자정부국을 신설하고 정부 기금을 조성하는 것을 주요내용으로 하는 법안(S.803)을 상원에 제출하였다. 동 법안은 2002년 6월 상원을 통과하고, 하원의 수정을 거쳐(H.R. 2458) 2002년 11월 하원을 통과하여 12월 17일 대통령의 서명으로 법률로 제정되었다.

4.2 주요내용

동 법에 의하면 관리예산처내에 전자정부국을 신설하고 대통령으로 하여금 전자정부국 국장을 선임하도록 하고 있다. 또한 향후 4년간 약 3억4천5백만 달러의 예산을 들여 전자정부 기금을 조성하도록 하고 있으며 관리예산처 차장을 의장으로 하고, 전자정부 국장, 정보규제국장, 기타 동 법이 정한 각 기관과 중앙정보국, 미 육·해·공군의 정보화책임관으로 구성된 정보화책임관회의를 신설하였다. 그리고 각 기관으로 하여금 전자정부기금의 운용실태 및 전자정부법의 준수여부 등을 포함한 보고서를 관리예산처에 제출하도록 하고, 관리예산처가 이를 매년 2회 하원 정부개혁위원회(the Committee on Government Reform of the House of Representatives)와 상원 정부위원회(the Committee on Governmental Affairs of the Senate)에 제출하도록 하고 있다. 또한 연방 정보기술인력양성, 연방인터넷 포털 사이트의 설치, 인터넷 이용격차에 대한 연구 및 프라이버시 보호 등을 규정하고 있다.

나아가 동 법은 정보보안의 중요성을 인식하고 제3장에 연방정보보안관리법(the Federal Information Security Management Act of 2002)를 삽입하여 통과시켰다. 동 법은 한시법으로 2002년 11월 29일 만료 폐기되는 2001년 국방권한법의 정부정보보안개혁법(Government Information Security Reform Act of 2000) 조항들을 대거 수용하였다.

Ⅳ. 미국 전자정부 정보보안 관련 법규

1. 개 요

인터넷의 급격한 확산으로 미국 정부는 자신들의 컴퓨터 시스템과 컴퓨터 시스템이 지원하는 통신, 공중 보건, 국방 등과 같은 국가기간업무에도 중대한 위험이 있다는 사실을 심각하게 인식하였다[1]. 따라서 미국 정부도 효과적인 정보보안이 전자정부의 확대에 불가결하다고 인식하고 있다. 나아가 정보보안 없이는 전자정부를 통한 전자조달 등에 있어 전통적인 문서기반 거래에서 보다 오용이나 범죄에 취약할 수 있다고 인식하고 있다. 이러한 인식을 바탕으로 미국 연방 정부는 컴퓨터보호법(Computer Security Act of 1987), OMB Circular A-130, 정부정보보안개혁법(Government Information Security Reform Act of 2000) 및 전자정부법 2002에 연방정보보안관리법(the Federal Information Security Management Act of 2002)을 삽입하여 통과시키는 등 전자정부 정보보안 관련 법규를 제정 시행하고 각 기관들로 하여금 컴퓨터시스템과 그에 의하여 처리되는 정보 및 관련 기술자원의 보호를 의무화하고 있다.

2. 컴퓨터보호법(Computer Security Act of 1987, Public Law 100-235)

컴퓨터보호법은 연방 컴퓨터 시스템에 있는 기밀정보(sensitive information)의 안전과 프라이버시 보호를 위하여 기존의 보안 조치내에서 최소한의 보안관행(security practices)을 확립하려고 하였다. 동 법은 국가표준국(National Bureau of Standard)으로 하여금 연방 컴퓨터시스템에 대한 표준과 지침을 개발하도록 하며 보안 정보를 소유한 연방 컴퓨터시스템 운영자에게 안전계획의 수립을 요구하도록 하고 있다. 그리고 동 법은 상무부 장관으로 하여금 국가표준법(National Bureau of Standards Act)에 의하여 국가표준국에서 개발한 표준과 지침이 연방 컴퓨터 시스템의 운영에 활용되도록 표준과 지침을 공표하도록 하고 있다. 대통령은 동 표준과 지침을 수정하거나 거부할 수 있으며 각 연방 정부의 장은 상무부 장관이 공표한 표준이나 지침을 그대로 수용할 수도 있으나 필요한 경우 비용 효과적인 보안 표준이나 지침을 채택할 수 있다. 또한 동 법은 각 연방 기관들로 하여금 컴퓨터 보안과 컴퓨터 보안 절차를 인식시키기 위해 일정한 훈련을 실시할 것을 의무화하고 있다.

1) 미국 일반회계원(GAO)가 연방 기관들의 정보보안 실태를 분석한 결과 연방 정보 시스템들이 컴퓨터 관련 위협으로부터 적절하게 보호받지 못하고 있다는 사실도 발견하였다 U.S. General Accounting Office, Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets, GAO-02-231T

3. 관리예산처(OMB) Circular A-130

3.1 개 요

전자정부의 구축과 관련한 핵심기관은 앞에서도 살펴본 바와 같이 관리예산처이며, 동 기관은 전자정부 정보보안관 관련해서도 중심적인 역할을 수행하고 있다. 전자정부 구축과 관련한 법규들에 의하여 관리예산처는 OMB Circular A-130을 발표하여 정보자원의 관리와 정보보안에 있어 요구되는 임무를 수행에 필요한 사항들을 기술하였다.

3.2 주요내용

OMB Circular A-130의 부록Ⅲ 연방정보자원 보안(Security of Federal Automated Information Resources)은 연방 정보보안정책에 필요한 최소한의 통제장치들을 수립하고 있으며, 각 기관들로 하여금 정보보안에 대한 책임을 지도록 하면서 각 기관들의 정보보안프로그램과 기관관리통제시스템을 상호 연계시키고 있다.

OMB Circular A-130은 정보의 손실, 오용, 비인가된 접근 및 수정의 위험을 제거하여 각 기관의 시스템 및 응용프로그램들의 효과적인 운영은 물론 정보의 기밀성, 무결성 및 가용성을 확보하려고 하였다. 이를 위하여 정보 자원을 일반지원시스템(general support system)과 주요 응용자원(major application)으로 구분하고 각각에 대하여 각 기관들로 하여금 정보보안 담당 지정, 보안계획수립 및 보안통제평가 등을 수행하도록 하고 있다.

3.3 주요기관의 역할

OMB Circular A-130에 의하여 관리예산처는 연방정보자원 보안정책을 총괄하고 감독하며 상무부 특히 국립기술표준원(National Institute of Standard and Technology: NIST)는 보안관련 표준 및 지침을 개발하고, 인사관리처(Office of Personnel Management: OPM)와의 협력하에 정보보안 교육·훈련을 위한 지침을 검토 및 개정하며, 연방기관들의 보안계획 수립에 필요한 지침과 지원을 제공하고, 각 기관의 침해사고 대응 및 취약성 정보 공유 및 조정을 담당하며 국방부 특히 국가보안국(NSA)의 기술적 지원을 받아 새로운 정보기술의 보안 취약성 평가와 공표를 담당한다. 국방부, 특히 국가보안국(National Security Agency: NSA)은 상무부에 적정한 기술 자문 및 지원을 제공하고 새로운 정보기술의 취약성 평가과 관련하여 상무부를 지원하며, 법무부는 보안침해사고에 대한 법적 절차 및 보고에 관한 지침을 제공하고 보안침해사고가 일어날 경우 적절한 법적 조치를 수행한다. 총무청(General Services Administration : GSA)은 정보처리장치 관련 장비 구입시 고려해야 할 보안지침을 제공하고 연방 기관들이 필요로 하는 적절한 보안서비스를 제공하며, 인사관리처는 연방 공무원들에 대한 컴퓨터 보안 훈련을 지원하고, 보안정책위원회(Security Policy Board)는 정보기술보안 관련 연방 정부의 활동을 조정하는 역할을 담당한다.

3.4 OMB Circular A-130에 대한 평가

전자정부 구축과 관련한 정보보안을 위하여 OMB Circular A-130을 중심으로 한 미국의 노력은 급증하고 있는 새로운 보안침해 및 기술에 대하여 충분하지 못했다는 인식하에서 국가 주요기반보호 정책 논의와 더불어 정보보안 정책 강화의 필요로 이어져 2000년 10월 30일 정부정보보안개혁법을 제정하게 되었다.

4. 정부정보보안개혁법(Government Information Security Reform Act of 2000)

4.1 개 요

정부정보보안개혁법(Government Information Security Reform Act of 2000)은 비기밀(unclassified) 시스템과 국가안보(national security)시스템 모두를 적용대상으로 하고 있다. 비기밀시스템인 경우 1995년 정부문서감축법(Government Paperwork Reduction Act of 1995)와 Clinger-Cohen Act of 1996에 의하여 관리예산처가 부여받은 권한과 책임을 유지하도록 하고 각 기관의 정보보안프로그램에 대한 감사관의 평가 역할을 제외하고는 기존 OMB Circular A-130을 법규화 한 것으로 볼 수 있다. 그러나 국가안보시스템의 경우 정보보안과 관련한 관리예산처의 권한을 국방부, 중앙정보국 및 대통령이 지정한 다른 기관에 위임하도록 하고 있으며 국방부의 비기밀시스템에 대한 관리예산처의 권한도 국방부 장관에게 일부 위임하도록 하고 있다.

4.2 목 적

정부정보보안개혁법은 1) 연방정부가 가진 정보자원을 효과적으로 통제하기 위한 총체적인 틀을 제공하고, 2) 연방정부의 네트워크 컴퓨팅 환경을 인식하여 연방정부 정보처리의 상호운용성(interoperablity)의 필요성과 철저한 보안관리의 필요성을 인식하며, 3) 연방정부의 정보보안 위험성을 점검하여 정부 차원에서 효과적인 수단을 제공하고, 4) 연방정부의 정보나 정보시스템을 보호하기 위한 최소한의 통제수단을 제공하며 5) 연방정부의 정보보안프로그램을 효괴적으로 통제하기 위한 메카니즘을 제공하는 것을 목적으로 하고 있다.

4.3 각 기관의 권한과 책임

4.3.1 관리예산처장

관리예산처장은 범 정부차원의 정보보안 정책을 수립하여야 한다. 즉, 관리예산처장은 1) 연방정보시스템의 비용효과적인 보안, 2) Clinger-Cohen 법에 제시된 정보기술아키텍쳐, 3) 정보시스템 위험의 확인 및 평가를 통한 위험관리사이클 구축, 4) 위험의 적절한 통제, 5) 정보보안 위험에 대한 인식 제고 및, 6) 정보보안 절차의 효과성 감시 평가 등을 포함하는 것을 내용으로 하는 정책을 수립하여야 한다. 관리예산처장은 연방정부의 정보나 정보자원을 효과적으로 관리하기 위한 정책, 원칙, 표준 및 지침을 개발하고 감독할 뿐만 아니라 수집된 정보의 분실, 오·남용, 불법접근, 변조 등에 따라 발생되는 손실과 위험에 대비한 정보보안 대책을 강구할 것을 연방 정부기관들에게 요구할 수 있다.

더욱이 관리예산처장은 연방 정부기관의 장에 대하여 적절한 보안 대책의 수립, 사용 및 공유와 범부처 차원의 정보보안 계획 수립, 정보시스템의 라이프사이클에 적합한 정보보안 원칙 및 절차의 마련 등을 지시할 수 있다. 또한 Clinger-Cohen법과 국립표준기술원법(National Institute of Standards and Technology Act)에 근거하여 연방컴퓨터시스템의 보안과 관련한 상무부의 표준과 지침의 개발과 집행을 감독한다.

4.3.2 상무부 장관

상무부 장관은 연방정부시스템의 보안을 위한 표준과 지침을 개발하고 보급 검토하며 개정할 책임을 부담하며, 정보보안 훈련을 위한 표준과 지침의 개발, 각 정부 부처의 정보보안 정책 수립 지원 및 정보보안 위협 기술 평가 등에 대한 책임을 부담한다.

4.3.3 국방부 장관 및 중앙정보국장

국방부 장관과 중앙정보국장은 정보시스템의 보안정책, 표준 및 지침의 개발과 보급 및 그 수행을 점검하여야 하며 국방부 장관과 중앙정보국장이 마련한 정책, 원칙, 표준 및 지침의 모든 내용이 공개되도록 하여야 한다.

4.3.4 법무부 장관

법무부 장관은 정보보안 사고와 관련한 법적인 조치 및 보고 지침 등을 검토하고 개정해야 한다.

4.3.5 총무청

총무청은 연방 정부 부처들이 새로운 정보기술을 도입하는 경우 발생되는 정보보안 문제를 검토하고 개선해야 하며, 각 부서의 보안제품 확보를 위한 지원과 정보보안 기술의 도입에 있어서 비용 효과적인 제품과 서비스 등이 도입되도록 하여야 한다.

4.3.6 인사관리국

인사관리국은 연방 공무원을 대상으로 컴퓨터 보안 교육과 관련한 법규를 재검토하고 개선하여야 하며, 컴퓨터 보안 교육 지침에 대해서는 상무부와 협력하여야 한다. 또한 정보보안 교육의 내용 및 교육강사와 관련하여 국립과학재단(National Science Foundation) 및 기타 다른 기관들과 협력하여야 한다.

결국 연방 각 정부 부처는 관리예산처와 상무국이 작성한 정보보안 정책, 원칙, 표준 및 지침의 범위내에서 각자의 정보보안 정책, 원칙, 표준 및 지침을 작성하고 채택하여야 한다.

4.4 연방 부처의 정보보안 정책에 대한 평가

4.4.1 연방 각 정부 부처 정보보안 정책 내용과 평가

연방정부의 모든 부처는 i)정보시스템의 안전성과 위협에 대비한 정기적인 위험평가, ii)관리예산처장이 지시한 내용을 수용하며 정책 대상집단이 순응할 수 있는 동시에 비용 효과적이며, iii)정보보안 위험이나 책임의식 고취와 관련한 정보보안 의식의

제고 및 iv)심각한 취약점이 발견된 경우의 대처를 위한 제반 과정과 정보보안 사고 발생시 발견, 보고 및 대응절차 등을 포함한 정보보안 정책을 개발하고 수행하여야 한다.

또한 연방 정부 부처의 이러한 정보보안 정책은 i) 연간 예산, ii) 정보자원관리정책, iii) Clinger-Cohen법에 의한 정보보안 성과 및 결과, iv) 재정관리 정책 및 v) 정책관련 중요한 개선사항 등을 포함하여야 한다.

이러한 연방 각 부처의 정보보안 정책들은 정보화책임관협의회를 거쳐 정책담당관에 의해 최소한 1년에 1회 검토 받아야 하며 관리예산처장의 승인을 받아야 한다.

4.4.2 연방 각 부처의 정보보안 정책 평가

연방정부의 모든 부처는 매년 자신들의 정보보안 정책을 평가하여야 한다. 이 경우 정보시스템의 정보보안 통제기법의 효과성, 관련된 정보보안 프로그램 및 관련 정책과의 일치성에 대한 평가 등이 포함되어야 한다. 각 부처의 정보보안 정책에 대하여 관련 평가기관이나 감사관(inspector general)의 감사, 평가를 받아야 한다.

4.4.3 평가 결과의 보고

연방정부 각 부처는 정부정보보안개혁법에 제시된 정보보안 평가결과 및 정보보안 감사결과를 동 법 발효 후 1년 이내에 관리예산처장에게 보고하여야 하며 관리예산처장은 이러한 제반 보고를 요약하여 의회에 제출하여야 한다.

4.5 정부정보보안개혁법에 대한 평가

미국 정부는 정부정보보안개혁법을 통하여 연방정부 부처의 정보보안 관련 업무에 대한 철저한 통제시스템을 구축하여 그 이행과정을 감독하려고 하였다. 즉, 정보보안관 관련하여 연방 정부 부처의 장, 정보화책미관 등의 업무와 책임을 명확히 하고, 각 정부 부처가 관리예산처, 국립표준기술원 등의 지침을 기반으로 자체적으로 수행한 정보보안업무에 대하여 감사관의 감사 및 관리예산처와 의회에 대한 보고절차를 명확히 하여 각 부처의 정보보안 정책 및 프로그램을 철저히 감독하고 그 이행을 독려하고자 하였다. 특히 OMB로 하여금 각 부처의 정보보안 정책에 대한 총괄 감독을 수행하도록 하였을 뿐만아니라 각 부처의 자체 정보보안 평가 및 감사관의 보고서 등을 종합적으로 검토하여 기관의 업무성과 평가에 반영되도록 하여 각 부처의 정보보안 정책 및 프로그램의 실행을 강화하는 절차를 확립하였다. 결국, 정부정보보안개혁법은 연방 각 부처로 하여금 정보보안 정책과 프로그램을 개선하고 정보보안의 중요성에 대한 인식을 제고하였을 뿐만 아니라, 정보보안 관련 취약점과 허점들을 개선하는 중요한 역할을 수행한 법률로 평가되었다.

그러나 정부정보보안개혁법은 2002년 11월 29일에 그 기한이 만료되는 한시법으로 규정되어 있다. 따라서 미국 정부는 정보보안 관련 문제점을 파악하고, 정보보안 업무의 수행을 지속하며, 미국 정부와 의회가 전자정부 정보보안을 효과적으로 관리 감독할 수 있도록 정부정보보안개혁법의 계속적인 시행을 요구하였다. 나아가 정부정보보안개혁법을 1년여 시행한 후 미국은 정보보안과 정보시스템에 대한 최소한의 관리 통제 요건 등과 같은 연방 정부의 전자정부 정보보안 구현과 감독을 한층 더 강화하기 위한 관련 법안을 제안하였다.

5. 연방정보보안관리법(Federal Information Security Management Act of 2002)

연방정보보안관리법은 한시법으로 2002년 11월 29일 만료 폐기되는 정부정보보안개혁법(Government Information Security Reform Act of 2000)의 한시법 조항을 삭제하고, 이를 연방정보보안관리법(the Federal Information Security Management Act of 2002)으로 이름을 바꾸어 전자정부법 2002의 제3장 정보보안에 삽입 통과되었다. 또한 동 법은 국토안보부의 연방컴퓨터사고대응센터(Federal Computer Incident Response Center : FedCIRC)를 사이버 보안에 대한 침해사고 대응 센터로 승인하였으며, 컴퓨터 보안표준과 관련한 국립표준기술원(NIST)과 상무부의 역할을 강화하였다.

V. 결 론

이상에서 미국의 전자정부 구현을 위한 법제와 전자정부 정보보안을 위한 법제에 대하여 개략적으로 살펴보았다. 미국은 전자정부 구현을 위하여 각 종 법규를 제정하였고 이를 통합하여 2002년에 전자정부법을 제정하였다. 그리고 전자정부법을 제정하면

서 전자정부의 성공이 정보보안에 있다는 사실을 확실히 인식하고 전자정부법에 연방정보보안관리법을 삽입하였다. 동 법은 그동안 전자정부와 관련된 각종 법규를 시행하면서 미국 정부가 정보보안의 중요성을 강하게 인식하고 연방 각 정부 부처에서 정보보안의 이행을 추진하기 위해 시행하였던 각 종 법규의 결정체라고 할 것이다.

우리나라도 전자정부의 구현을 위하여 2001년 7월 1일부터 전자정부법을 제정 시행하고 있다. 우리의 경우도 전자정부의 성공이 전자정부 정보보안에 달려 있다는 인식이 확산되고 있으나 현행 전자정부법은 제27조 제1항에서 "국회·법원·헌법재판소·중앙선거관리위원회 및 행정부는 전자정부의 구현에 요구되는 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다"고 하고 제2항에서 "행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다"고 선언적으로 규정하고 있을 뿐 그 구체적인 절차나 시행에 대해서는 언급하지 않고 있다. 다만 동 법 시행령 제34조에서 행정정보가 유출되지 않도록 적절한 조치를 취할 것과 동 조 제5항에서 전자문서의 유통 보관 등과 관련하여 국정원장이 안전성을 확인한 조치를 취하도록 요구하고 있을 뿐이다.

이는 전자정부의 성공을 위한 체계적인 정보보안에 대한 입법적 불비로 생각되며, 조속한 시일 내에 미국의 전자정부법과 같이 정보보안에 대한 체계적인 입법이 시도되어 안전하고 신뢰할 수 있는 전자정부가 구현되도록 하여야 할 것으로 생각된다.

참 고 문 헌

[1] Government Performance Results Act of 1993(GPRA) Public Law No: 103-62.

[2] Clinger-Cohen Act of 1996 Public Law No: 104-208.

[3] Government Paperwork Elimination Act of 1998(GPEA) Public Law No: 105-277.

[4] The E-Government Act of 2002 Public Law No: 107-347.

[5] Computer Security Act of 1987, Public Law 100-235.

[6] OMB Circular A-130.

[7] Government Information Security Reform Act of 2000.

[8] Federal Information Security Act of 2002.

[9] http://www.whitehouse.gov/omb/egov/about_leg.htm.

[10] http://www.whitehouse.gov/omb/egov/pres_state.htm.

[11] http://www.whitehouse.gov/omb/egov/pres_state2.htm.

[12] U.S. General Accounting Office, Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets, GAO-02-231T.

[13] U.S. General Accounting Office, Information Security: Comments on the Proposed Federal Information Security Management Act of 2002, GAO-02-677T.

[14] 임지봉, 미국의 전자정부 관련 법제 동향, 전자정부구현을 위한 법제동향과 과제(II), 법제연구원, pp. 33-49, 2001. 4. 25.

[15] 국가보안기술연구소, 전자정부 정보보안 대응체계에 관한 연구, 2001. 11.

[16] 국가보안기술연구소, 한국 정보보안 정책방향에 관한 연구, 2002. 11.

[17] 한국전산원, 미국의 전자정부 입법동향 분석, 2002. 11.

〈著 者 紹 介〉

김 대 호 (Dae-ho Kim)
종신회원

1977년 2월 : 한양대학교 전자공학과 학사
1984년 8월 : 한양대학교 전자공학과 석사
1993년 : University of Maryland 방문 연구원
1995년 : 전기통신기술사, 정보통신기술사
1977년 3월~1999년 12월 : 한국전자통신연구원 본부장
2000년 1월~현재 : 국가보안기술연구소 소장

오 일 석 (Il-seok Oh)

1994년 2월 : 한국외국어대학교 영어과 졸업
1997년 2월 : 고려대학교 일반대학원 법학과 석사
1997년 3월~1997년 12월 : 고려대학교 비교법연구소 연구원
2001년 3월~현재 : 한국전자통신연구원 부설 국가보안기술연구소 연구원
관심분야 : 정보보호 정책, 정보전 정책, 기본권 보장과 제한