情報保護學會論文誌
第19卷 第5號, 2009. 10

전자정부 정보보호관리체계(G-ISMS) 적용 정책

한 근 희†‡
행정안전부

Adaptation Policy of ISO 27001 ISMS (Information Security Management System) for e-Government

Keun-hee Han†‡
MOPAS

요 약

우리나라 전자정부는 UN 전자정부 참여지수 2위, 미국 브루킹스연구소(전 브라운대학) 평가에서 3년 연속 1위를 차지할 정도로 잘 구축되어 있으나, 반면에 세계경제포럼(WEF)에서 2007년 조사한 정보보호 순위는 51위로서 인터넷 이용자수와 서비스 환경에 비해서 상대적으로 열악한 수준이다.

2008년 한 해 동안에만 옥션 정보유출, GS 칼텍스 정보 유출 등 크고 작은 보안 사고들이 끊임없이 발생하여 국민들이 사이버위협에 노출되고 주요 정보들이 유출되자 점차 정보보안, 개인정보보호의 필요성과 중요성에 눈을 뜨게 되어 정보보호에 대한 요구가 점차 늘어나고 있는 추세이다.

본고에서는 주요 국가들의 전자정부 서비스 수준과 정보보호를 위한 투자·제도·정책 등을 벤치마킹하여, 우리나라에서 이를 효율적으로 활용할 수 있는 방안을 찾아보고, 중앙행정기관 및 지방자치단체에서 제공하고 있는 전자정부 서비스의 안전성과 보안성을 향상시킬 수 있도록 국제적으로 표준화된 정보보호 관리체계인 ISO 27001 ISMS를 적용할 수 있는 정책을 발굴하여 국가 정보보호 수준을 더욱 높이고자 한다.

ABSTRACT

Korea ranked 2nd in the UN Global e-Participation Index and ranked number one as the leader in e-Government for the third consecutive year. However, Korea ranked 51 in the level of information security published by WEF(World Economic Forum), relatively a low level comparing with its great number of users and excellent environments for the Internet service.

A series of critical hacking accidents such as the information leak at Auction and GS Caltex emerged consecutively in 2008 year, resulting in the leak of personal & critical information. This led to a strong interest in the necessity and importance of information security and personal information so that demand for IT security is growing fast.

In this paper, we survey to benchmark information security in the perspective of service level, system, investment and policy about major foreign countries. Then we research on an effective way to make the most of the benchmark result to Korea e-Government. In addition, the purpose of this paper is to improve national information security index by developing a policy for ISO 27001 ISMS, an international standard for Information Security Management System, and elevate safety and security of the e-Government serviced by central administrative organizations and local authorities.

Keywords: G-ISMS, ISO 27001 ISMS, IT Security, e-Government

접수일(2009년 4월 22일), 수정일(1차: 2009년 6월 30일), 2차: 2009년 7월 20일), 게재확정일(2009년 8월 15일)

† 주저자, hankeunhee@nate.com
‡ 교신저자, hankeunhee@nate.com

I. 서 론

사회 환경은 갈수록 유비쿼터스 사회로 진화되어 와이브로, DMB , RFID/USN 등 유·무선 융·복합 기술이 날로 발전되고 있으며, 개방·참여·공유를 내세운 매쉬업 기반의 시맨틱 웹 혹은 웹 2.0 사회로 급변하고 있고, 행정 환경 또한 누구나 참여 가능한 전자정부 기반의 공개서비스로 진화되고 있다.

더구나, 우리나라의 인터넷 환경은 세계적으로 뛰어나서 '09.5월 기준 초고속 인터넷 보급률 96%로서 1,587만명이 사용 중이고[1], '08.12월 기준 인터넷 이용자 수는 3,536만명으로 6세 이상 인구의 77.1%가 사용 중이다[2].

우리나라 전자정부는 UN 전자정부 참여지수 2위, 미국 브루킹스연구소(전 브라운대학) 평가에서 3년 연속 1위를 차지할 정도로 잘 구축되어 있으나, 반면에 세계경제포럼(WEF)에서 2008년 조사한 정보보호 순위는 51위로서 인터넷 이용자수와 서비스 환경에 비해서 상대적으로 낮은 수준이다[3].

2008년 한 해 동안 옥션 해킹으로 개인정보 1,081만건이 유출된 사건을 비롯하여 KT, 다음 등 9개 업체 해킹, GS 칼텍스의 개인정보 CD 유출 등 민간에서의 개인정보 유출이 크게 증가하였고, 병무청 등 공공기관과 기업의 웹 사이트에 대한 사이버 공격 등 크고 작은 보안 사고들이 끊임없이 발생하여 국민들이 사이버활동에 불안감을 한층 더 느끼게 되었다.

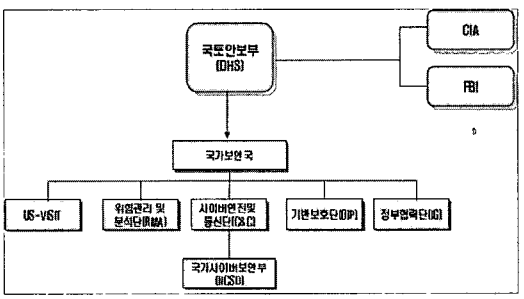
본고에서는 주요 선진국들의 전자정부 서비스 수준과 정보보호 환경 등을 분석하고, 국내에서 시행되고 있는 여러 가지 보안수준 실태조사 방법들(개인정보보호 분야 포함)과 정보보호 관리체계에 대한 국제 표준인 ISO 27001 ISMS(Information Security Management System)[4,5]를 국내 전자정부 환경에 적용할 수 있는 통합 방안을 도출하여, 전자정부 서비스에 대한 보안수준을 향상시킬 수 있도록 실용적인 활용방안을 제안하고자 한다.

II. 주요 국가의 정보보호 정책

안전한 유비쿼터스 사회를 구현하기 위하여 국가마다 다양한 정책들이 추진되고 있으며, 미국, 일본, EU 등 주요 국가의 정보보호 정책[6]을 비교·분석하여 우리나라 전자정부 정보보호 환경에 도입·적용할 방안을 찾고자 한다. 안전한 유비쿼터스 사회를 구현하기 위하여 국가마다 다양한 정책들이 추진되고 있으며, 미국, 일본, EU 등 주요 국가의 정보보호 정책을 비교·분석하여 우리나라 전자정부 정보보호 환경에 도입·적용할 방안을 찾고자 한다.

2.1 미국의 정보보호 정책

미국은 9.11 테러 이후 국토안보부(DHS, 2002. 11)를 신설하여 국가사이버보안부에서 사이버안전 업무를 총괄하여 사이버위협 정보 분석 및 경보 정보 제공, 연방 차원의 사이버위협 대응활동 조정, 금융 등 산업분야별로 민간이 자체 운영하는 ISAC과 긴밀한 협력을 통해 기반시설 보호 활동 전개 등을 수행하며, 정보보호개혁법(2000), 연방정보보안관리법(FISMA, 2002.1)[7] 등을 제정하여 각 부처의 모든 정보자원을 대상으로 '위험기반 정보보호 관리계획'을 수립하도록 하고 평가 시행 및 결과를 주기적으로 보고하도록 하였다. 또한 국토안보부에서는 연방차원의 사이버위협 대응활동으로 '국가사이버공간 보호전략(2003. 3)'을 수립하여 국가 사이버보안 대응시스템 구축, 정보보호 위협·취약점 감소, 정보보호 인식 제고 및 교육, 정부의 사이버공간 보호 및 국제협력 강화 등 정보보호정책을 적극적으로 추진하였으며 '국가기반보호계획(2006. 6)'을 통해 국가기반구조와 주요 자원을 안전하게 보호하도록 추진하였다.



[그림 1] 미국의 정보보호 조직

정보보호를 강화하기 위하여 예산도 2006년 8.3%에서 2007년 9.1%, 2008년 9.7%로 증가하였고 2009년에는 10.3%의 예산을 요구하였으며, 해가 갈수록 대폭적으로 증가하고 있는 것을 알 수 있다[6].

미국의 정보보호 관련 예산은 테러방지, 자국민 보호, 사이버 시큐리티 및 중요 인프라 보호 관련 연구개발이 주를 이루고 있으며, 국방 부문은 정보보호에 있어서 최대의 지출기관으로 국방 관련 예산이 전체

〔표 1〕 미국의 정보화 대비 정보보호예산
(단위: 100만 달러)

구 분	'06년	'07년	'08년	'09년 요구액
IT예산(A)	66,215	64,911	68,314	70,914
정보보호 예산(B)	5,512	5,905	6,631	7,278
정보보호 예산 비율(B/A)	8.3%	9.1%	9.7%	10.3%

주) 2006, 2007년의 경우, IT예산은 실적액, 정보보호 예산은 성립(Enacted)액이며, 2008년은 성립액, 2009년은 요구액임
출처) OMB(행정관리예산국)

정보보호 예산의 약 60%를 차지(IT대비 11.8%)하고 있다.

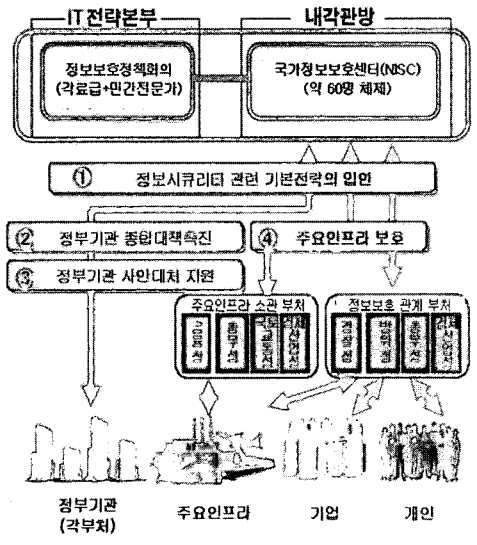
2.2 일본의 정보보호 정책

일본은 IT전략본부에서 고도 정보통신 네트워크사회 형성기본법(200 정보1)을 제정하여 내각관방을 중심으로 총무성과 경제산업성이 양대 축이 되어 각 부처의 정보보호 정책 총괄 조정하고 정보보호 기본 전략의 입안 및 홍보, 정부의 통일된 안전기준 책정 및 평가 등 정보보호 정책을 추진하고 있으며, 유비쿼터스 사회에 대한 비전으로 'u-Japan' 정책(2004. 12)을 수립하여 2010년까지 안전하고 안심할 수 있는 사회를 실현하고자 노력하고 있다

특히, 경제산업성에서는 정보통신기반 위협 대응 및 정보경제기반 안정을 위해 정보보호 종합전략(2003. 10)을 마련하였고, 총무성에 국가정보보호센터(2005. 4)를 설치하여 제1차 정보보호기본계획(2006-2008)을 발표(2006. 2)하여 정부, 주요 인프라, 민간 대상 정보보호 기본계획을 수립·추진하였으며, 경제산업성에서 정보보호 선진국 실현, 정보보호 정책의 글로벌화, 국내외 변화에 대응하는 메커니즘 확립 등을 위한 글로벌 정보보호 전략('07)을 수립·추진하였다. 또한, 개인정보보호를 위해 개인정보보호법(2005. 4)을 통한 개인정보의 유출방지와 부정액세스 행위금지에 관한 법률(1999. 8)에 의한 해킹, 바이러스 등의 사이버침해를 방지하도록 규정하였다.

정보보호를 위한 예산으로 2006년 2.43%, 2007년 2.4%, 2008년 2.49% 책정하였지만, 내각법제국(20%), 내각관방(18.1%)에서는 정보보호 예산을 대폭 증액하여 정보보호 분야를 중요한 핵심사업으로 추진하고 있다〔6〕.

일본의 정보보호예산은 전자정부 관련 예산에 집중되고 있으며 개인정보보호 관련 예산은 부족한 실정으로 내각관방 정보보호센터(NISC)를 중심으로 「제1차 정보보호 기본계획」 및 「시큐어 제팬 2006」을 통해 정보보호 관련 정책 및 예산을 편성하고 있다.



〔그림 2〕 일본의 정보보호 조직

〔표 2〕 일본의 정보화 대비 정보보호 예산
(단위: 억엔, %)

구 분	'04년	'05년	'06년	'07년	'08년
IT 관련예산(A)	13,315	13,016	13,115	12,484	13,580
정보보호 관련예산(B)	267	288	319	300	338
비중(B/A)	2.01	2.21	2.43	2.40	2.49

주) · IT관련예산은 내각관방의 IT담당실이 집계한 고도정보통신네트워크사회의 형성에 관한 예산임
· 정보보호예산은 내각관방 정보보호센터가 집계한 자료로, 정보보호관련 예산이라고 단정하기 어려운 것은 제외한 것임
출처) 내각관방의 IT담당실 및 정보보호센터

2.3 EU의 정보보호 정책

U는 유럽 네트워크 및 정보보호기구(ENISA, 2004.3)를 설치하여 유럽 공동체 네트워크 및 시스템 보호를 강화하고 있으며 정보보호 문화 구현 및 사이버 위협에 대한 공동 대응 등을 위해 회원국 간 유기적인 정보보호 협력체계를 구축하여 운용하고 있다.

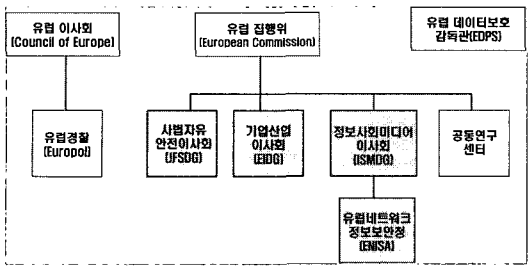
네트워크와 정보보안계획(2001 .6)을 수립하였고, 정보사회 확립을 위해 'eEurope2005'의 우선과제로 정보보호를 선정하여 안전한 정보인프라 구축을 위한 4대 중점과제를 도출하였고, 인터넷에서의 이용자 보호를 위한 'Safer Internet' 프로젝트(2005)를 추진하였다. 또한, 2012년까지의 중장기 정보보호 연구개발 계획을 수립하여 안전한 지능기반 사회 구현을 위한 연구개발 과제를 선정하여 추진하고 있다.

ENISA는 미래사회에서의 사이버공격에 대한 위험성을 지적하고, 유비쿼터스 환경에서 사이버범죄가 만연할 것이라고 예측하였다. 이에 EU는 데이터보호 지침(1995.10), 전자서명지침(1999. 12), 전자상거래지침(2000. 6), 정보보호 프레임워크 지침(2002. 3) 등과 같이 정보보호를 위한 지침들을 제공하고, 안전한 정보사회를 위한 전략을 수립하여 중장기액션플랜(2006.5)을 마련하였다.

EU의 기업산업 이사회는 정보보호에 관한 연구를 위하여 2006년 1,900만 유로를 지출하였으며, 2008년까지 총 3,560만 유로를 배정하였으며, 사법자유안전이사회는 정보보호를 포함한 대테러대책을 위해 3년간 1,200만 유로(2006)를 지원할 예정이다[6].

EU에서는 IT 예산 및 정보보호 예산 집계액을 별도로 공표하고 있지 않으며, 참고로 ENISA의 2006년 예산은 680만 유로(기준 환율을 1유로에 1,200원으로 산정하였을 때 약 81억원)였다.

주요 국가의 정보보호 추진 정책을 [표 4]와 같이 요약 비교하였다.



[그림 3] EU의 정보보호 조직

[표 3] ENISA 연도별 예산

(단위 : 유로)

구 분	'04년	'05년	'06년
인건비	1,620,000	3,060,000	4,463,000
설비비	1,380,000	2,430,000	1,027,000
운영비	500,000	1,310,000	1,310,000
합 계	3,500,000	6,800,000	6,800,000

출처) Rand of Europe 보고서

[표 4] 주요국의 정보보호 추진정책 비교

구분	미 국	일 본	유 럽 연 합
주요 정책	· 국가사이버 공간 보호전략('03)	· 정보보호 종합 전략('03) · 글로벌 정보 보호 전략('07)	· Safer Internet Project('05) · 중장기 정보보호 연구개발 (FP7 ICT Security R&D) 프로그램('07)
공공 부문 정책	· DHS를 중심으로 CERT, ISAC등 인터넷 침해사고 대응, 보안기술에 대한 표준, 권고안 개발 등	· 정보보호 센터 중심의 표준 안전기준 개발 및 평가 추진	· 단일 기구 (ENISA)를 중심으로 침해정보 공유 및 모범사례 발굴 등을 통한 예방 활동 주력
민간 부문 정책	· 인식제고를 위한 인증마크 제도 운영 · 민간 자율 규제 중심	· 기업 측면의 정보보호는 경제산업성, 이용자 보호는 총무성 중심	· 회원국 별 이용자 인식제고를 위한 정보보호 문화 운동 (culture of security) 추진
특 징	· 주요 국가 시설에 대한 안보 측면의 정보보호 강조	· 총무성 중심의 공공, 민간 정보보호 정책일원화를 통한 추진력과 효율성 제고	· 유럽 사이버범죄 조약 등 범 유럽 차원의 통합된 정보보호 접근방법
정보보호 R&D 정책	· 국가 사이버 공간 보호전략, · 연방 사이버 보안 및 정보보증 연구개발 계획	· 내각관방 기술전략전문위원회 보고서	· 2010년 이후의 미래 정보보호 연구개발 전략

III. 행정기관의 정보보호 현황 및 문제점

앞에서 살펴 본 바와 같이 주요 선진 각국들은 정부의 정보화(전자정부)를 추진하면서 정보보호를 위한 정책·연구 개발 등을 함께 적극적으로 추진하고 있으며, 전자정부 구축 및 서비스 사업을 추진할 때 초기 기획 단계부터 정보보호 계획 및 정책을 수립·적용하고 있고, 이에 대한 예산계획이 포함되어 있어야만 사업을 추진할 수 있도록 제도화되어 있다. 미국의 경우 연방정보보안관리법(FISMA)에서 연방정부 각 부처에서 정보화사업을 계획수립·추진할 때 정보보호를 포함하여한 계획을 수립하고 이를 실질적으로 이행하고 있는지 여부를 엄격하게 확인 점검하고 있으며, 서비스 제공 이후에는 각 부처별로 정보보호 수준을 평가하여 평가 점수를 공개하고 있으며, 이를 국회 및 예산처에 정기적·의무적으로 보고하도록 하고 있다[7].

국내의 경우, "전자정부 대민서비스 보안수준 실태조사 및 개선방안 연구"[8]를 통해 중앙행정기관 및 지방자치단체 273개 기관 1600개 정보서비스를 대상으로 전반적인 정보보호 환경을 조사·분석하였고, 지방자치단체의 정보보호 현황을 파악하기 위하여 93개 기관에 설문서를 배포하여 분석한 결과[9]를 활용하였다.

3.1 기반 환경

중앙행정기관이나 지방자치단체에 정보보호를 추진하는 전담기관이나 조직·인력 등이 턱없이 부족하고 아예 없거나 하여 정보보호를 위해 적극적인 대응을 하지 못하고 있다. 2006년 공공부문의 정보보안 전담조직 구성 비율은 23.9%이며, 2007년은 20.7%로 나타나 별로 늘어나지 않았고, 정보보안 전담조직이 없는 경우 대부분(96.88%) 정보화 담당부서에서 정보보호 업무를 같이 수행하고 있는 실태이다. 또한,

[표 5] 정보보호 전담조직 및 인력 현황

(단위 : %, 명)

구 분	'07년	'08년	증감율
· 정보보호 전담조직 설치율	11.7%	22.6%	10.9% ↑
행정기관	22.0%	38.4%	16.4% ↑
공공기관	11.8%	16.6%	4.8% ↑
민간기업	1.4%	12.7%	11.3% ↑
· 정보보호 전담인력수	1명	1.76명	76% ↑

[표 6] 정보화 대비 정보보호 예산

(단위 : 백만원)

구분	'07년	'08년	'09년
정보보호 예산총액(A)	101,827	160,755	174,245
정보화 예산총액(B)	3,410,400	3,396,000	3,155,100
A/B(%)	2.99%	4.73%	`5.52%

※주요국 규모('08년 기준): 미국 약 66억달러(9.7%), 일본 338억엔(2.5%)

정보보호 부서가 있는 경우라도 정보보안 담당인력은 평균 1~2명이고 정보보안 관련 학위를 취득한 인력은 11%이며 정보보호 관련 자격증을 보유한 인력은 20%로 정보보호 업무 추진 인력의 전문성이 미흡한 실정이다[8,10].

우리나라도 최근 정부에서 정보보호에 관해 많은 관심을 갖고 정보보호 분야에 투자를 확대하고 있는 상태이나 선진국 수준의 절반 수준에 그치고 있는 실정으로, 2008년에 정보보호 중기 종합계획을 처음 수립하여 2010년까지 정보화예산대비 10%까지 정보보호 분야 예산을 확충할 계획이다. 국가정보화 전체예산 대비 정보보호 예산은 2005년 1.93%에서 2007년 2.9%, 2008년 4.73%까지 증가하였으나 미국 연방정부의 정보화 예산대비 9% 수준에는 미치지 못하고 있으며, 일본과 비교하였을 경우 우리나라가 상대적으로 매우 높은 것 같이 보이나 이는 일본의 정보보호예산은 내각관방 정보보호센타가 집계한 자료를 기반으로 산정하면서 정보보호관련 예산으로 확인하기 어려운 것은 제외하여 그런 것으로 보이는 면이 있다[3].

3.2 정책 환경

우리나라는 공공기관의 개인정보보호에 관한 법률(1994)을 제정하면서 본격적인 정보보호정책을 추진하였으나 정보보호 분야에 대한 종합적인 법·제도가 수립되지 못하고 전자정부법, 정보화촉진기본법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등에서 정보보호에 관한 법규가 산재되어 있는 상태이다.

조직·인력·예산 문제 이외에 중앙행정기관 및 지방자치단체에서 정보보호 관련 업무를 수행하면서 개선 및 보완이 필요한 요소들을 분석한다[8,9].

첫째, 정보보호 관련 책임자·담당자들의 순환근무 정책에 따른 잦은 인사이동으로 업무에 대한 이해도가 낮고, 기술 습득 및 축적이 이루어지지 않아 전문성

및 숙련성을 확보하지 못하고 있다. 정보보호 업무의 성격상 지속적으로 전문 기술에 대한 동향과 최신 기술을 습득하고 축적하여야 하나 단기간 근무하고 다른 부서로 이동함에 따라 관련 기술과 업무 속성이 담당자와 해당 조직에 축적되지 못하고 업무 연속성이 결여되는 것이 커다란 문제이다.

더욱이, 정보화사업 추진시 사이버위협 및 해킹공격 방지를 위한 기술을 도입하고자 할 때 전문성 부족에 따른 기술력 부족으로 외부 업체에 의존하여 사업 기획을 함에 따라 업무 종속과 더불어 자칫하면 특정 기업과의 유착관계가 발생할 수 있어 이를 시급히 해결해야 할 문제이다.

둘째, 매년 정보화 분야 인력 충원의 기회가 있을 때마다 정보보호 분야에 우선적으로 인력을 배치하도록 독려하고 있으나 〈표 5〉에서 보듯이 전담 조직조차 설치하지 못하고, 보안 전문가를 확보하는 경우는 더욱 없는 실정이어서 전자정부 서비스를 제공하는 과정에서 안전성과 신뢰성을 향상시키고 강화하기에 한계가 있는 상황이다.

셋째, 개인정보보호를 포함한 정보보호 업무를 담당하는 부서에 배치되는 것을 꺼려한다는 것이다. 자발적으로 원해서 보안업무를 담당하는 사례는 많지 않고, 어쩔 수 없이 배치되었을 경우에도 가능한 한 단기간 근무한 후에 다른 부서로 옮겨 가는 경우가 많다. 따라서, 보안기술 수준이 낮음에 따라 정보시스템을 안전하게 보호하고 유지하기 위한 전문성이 떨어지고 조직 내부에 정보보호 역량이 취약한 실정이다. 이런 상태에서 정보시스템을 관리하면서 사이버 공격을 당하거나 사고가 발생하였을 경우 적기에 절적한 기술을 활용하여 대처하기에는 한계가 있게 되고, 사고 내용이 중차대할 경우 정보보호 업무 담당자가 처벌을 받게 되어 더욱 동 분야에 근무하기를 기피하게 된다.

넷째, 정부와 행정서비스의 정보화는 세계 각국의 추세로서 모든 정부 업무가 전산화되고 있는 환경으로 전산 담당자가 더욱 필요한 상태이다. 대개의 경우, 전산 담당자 혹은 통신 담당자 중에서 정보보호 담당자를 선임하고 있는 환경이나 반면에 정보화를 담당하는 전산·통신 직렬이 승진 기간에서 행정 직렬에 비해서 더 오래 소요되어 전산 직렬 기피 현상이 발생하고 있다.

더구나, 전산·통신 직렬의 경우 최신 기술을 도입 적용하고 전문성을 확보하기 위해서는 해당 정보통신·정보보호 분야에 대한 대학원 진학, 연수 등 학습을 하여야 하나, 이보다 승진에 도움이 되는 분야로 직렬 변경 혹은 학습과목 선택을 하는 경우가 많아 더욱 전문성이 결여되고 있다.

다섯째, 인력과 전문가의 부족에 따라 전자정부에서 사용하는 정보시스템은 거의 대부분 민간 전문업체에 외주 의뢰하여 개발하고 있고 개발 후 운영할 때에도 정보시스템 전체를 아웃소싱하여 관리하는 상황이어서 외주용역 개발 및 운영업체에 대한 관리를 효율적으로 수행해야 할 필요가 있다. 개발 과정중에서 프로그램이 오류나 결함이 없이 잘 만들어졌는지, 전문기술자를 투입해서 체계적으로 관리하고 있는 지, 운영·유지보수가 적절하게 이루어지고 있는 지 등을 확인하는 방안이 있어야 하나, 외주 용역업체에 의존하여 전적으로 맡겨 놓고 있는 경우가 대부분이다. 더구나, 외주용역 발주, 의뢰 혹은 계약시 정보보호 분야에 대한 내용이 계약에 포함되어 있지 않아 사이버 공격이나 위협에 신속하게 대응하지 못하고 있으며, 정보보호 분야 업무 수행에 대한 관리·감독·점검 능력이 부족하여 대응이 제대로 되지 않고 있다.

3.3 서비스 환경

김대중 대통령 시절의 DJ 정부에서 추진된 전자정부 11대 과제와 노무현 대통령 시절의 참여정부에서 추진된 전자정부 31대 로드맵 과제에서 구축된 전자정부 서비스는 모두가 웹 서비스 환경을 기반으로 만들어졌는데, 여기서 우리가 더욱 고려해야 하는 것은 최근 발생하고 있는 사이버 위협의 80% 이상이 웹 서비스를 대상으로 하는 해킹 공격으로 웹 서비스에 대한 보안대책 마련이 중요한 요소로 부각되었다[11].

웹 서비스가 공격자의 수단이 된 이유는 의외로 간단하다. 첫째로 해커가 공격하고자 하는 거의 모든 대상이 웹 서비스를 운영했다. 둘째로 웹 서비스를 제공하는 웹 서버와 웹 애플리케이션 서버에서 많은 취약점이 지속적으로 발견되어 해킹에 이용당하고 있다. 세 번째로는 웹 서비스를 제공하기 위해 제작된 애플리케이션이 짧은 역사와 급격한 발전으로 인해서 속도, 기능, 디자인만을 고려해 제작함에 따라 보안을 전혀 고려하지 않아 웹 서비스를 대상으로 한 사이버 공격이나 해킹에 매우 취약하다는 점이다.

웹 해킹이란 웹 서비스와 관련된 웹 서버, 웹 애플리케이션 서버, 데이터베이스 시스템 그리고 CGI, ASP, JSP 등과 같은 웹 애플리케이션을 대상으로 불법적인 권한과 정보를 획득하는 것이다. 특히 불법적인 권한과 정보라는 것이 기존의 해킹과 달리 사이

버 머니나 회원 정보와 같은 개인 정보 그리고 웹 애플리케이션의 사용자/관리자 권한 획득 등과 같이 기존의 해킹과는 달리, 최근에는 금전적인 목적성을 가지고 있는 것이 대부분이다. 또한 이러한 추세는 웹이란 매체에 인터넷 뱅킹을 비롯한 다양한 금전 관련 정보들이 웹에 집중됨에 따라서 가속화되고 있다.

웹은 현재 우리의 생활에 중심이 됐으나 이를 사용하고 있는 다수의 사용자를 충분히 보호할 수 있을 만큼 안전하지 않다. 공격자는 웹 애플리케이션을 통해 기관의 내부 시스템에 접근할 수 있으며, 취약점이 존재한다면 이를 통해 손쉽게 내부로 침투하여 주요 정보를 탈취할 수 있다.

공격자에 의해서 침투를 당했다면 같은 네트워크 대역에 존재하는 모든 시스템에서의 정보 유출을 의심해봐야 하며, 더 이상 신뢰할 수 없게 되는 것이다. 또한 모든 정보를 보유하고 있고 가장 핵심적인 데이터베이스의 경우 전자정부 서비스의 웹 애플리케이션을 통해서 제공되고 있기 때문에 모든 정보가 공격자에게 노출될 수 있다. 다음으로 공격자는 장악한 시스템을 이용해서 내부 시스템 사용자가 존재하는 곳에 침투할 수 있으며 악성 프로그램을 실행시킬 수도 있다.

또한 침해를 당했을 경우, 현실적인 환경에서 대부분의 서스템 관리자는 시스템의 속도가 저하되거나 메인 페이지가 공격자에 의해서 변조되거나 시스템을 업그레이드 또는 재 구동하는 과정에서 침해 사실을 인지하게 되어 적시에 적절하게 대응할 수가 없는 경우가 많다.

따라서, 침해 상황을 분석할 수 있는 로그 파일이나 공격자의 흔적들이 삭제되거나 변조된 이후이고 웹의 특성상 엄청난 로그의 양으로 인해 공격의 흔적을 찾는 것이 어렵기 때문에 공격자가 어디까지 침해를 했는지 알 수 없게 된다.

IV. 행정기관 정보보호 역량강화

"전자정부 대민서비스 보안수준 실태조사 및 개선방안 연구"[8] 및 "정보보호관리체계 도입방안 연구"[12]를 수행하면서 11개 주요 전자정부 서비스 및 제공기관(전자민원 G4C, 서울시청 등)을 대상으로 '08.9월 2주간 현장방문으로 "정보보호관리체계 인증제도 취지 설명 및 도입 타당성 의견 청취", "중요 정보보호관리 현황 8개 영역 25개 항목 파악", "정보보호 애로사항 및 요구사항 수렴" 등을 통해 중앙행정기관 및 지방자치단체에서 전자정부 대민서비스를 안전하게 제공하고 국민들이 안심하고 사용할 수 있도록 신뢰성과 보안성을 향상시키기 위한 방안을 도출하였다.

앞장에서 살펴 본 행정기관의 정보화 및 정보보호 업무 정책상 문제점들에 대해서 이를 개선할 방안에 대해서 제안한다.

4.1 정책 개선

"전자정부 대민서비스 보안수준 실태조사 및 개선방안 연구"[8] 및 "지방자치단체의 정보보호 관리체계 구축방안"[9]에서 조사한 자료를 살펴보면; 정보보호 조직(과, 팀 혹은 계)이 독립적으로 설치되어 있는 기관이 11% 로서 대부분 기관이 전담조직이 없는 상태이고, 정보보호 담당자도 중앙행정기관이 평균 2명, 지방자치단체가 평균 1.5명으로 전담인력이 턱없이 부족하고, 정보보호담당자의 현업 부서 평균 근무기간이 1년도 채 되지 않아 해당 업무에 대한 전문성 및 숙련도를 확보하기가 무척 어려운 상태이다. 따라서, 무엇보다도 먼저 인사정책 및 제도에 대한 개선작업이 시급한 상태이다.

첫째, 순환근무제도에 의한 잦은 인사이동에 대해서는 문제점도 있지만 나름대로 장점(다양한 직무 경험으로 관리능력 향상, 중앙-지방간 인사교류, 유착관계 형성 차단, 부정 발생소지 사전 제거 등)도 있기 때문에 이를 무조건적으로 폐지하는 것 보다 문제점을 다소나마 줄일 수 있는 방안으로 해결책을 찾는 것이 필요하다. 인사제도에서 발생하는 것을 조직 혹은 제도에 의해서 보충하는 방안을 제안한다.

기업의 품질향상을 위해서 제품을 생산하는 단위마다 표준화를 적용하여 사람과 조직 모두가 엄격한 품질관리를 시행할 수 있도록 국제표준 품질인증 제도인 ISO 9001 을 활용하듯이, 잦은 인사이동에도 불구하고 조직 내부에 정보보호에 대한 노하우가 쌓이고 정착될 수 있도록, 정부 업무 수행 조직 내부에 표준화된 국제표준 정보보호관리체계인 ISO 27001 ISMS를 우리나라 전자정부 대민서비스 환경에 알맞도록 수정·적용하여 업무가 지속적이고 효율적으로 관리될 수 있도록 하고, 사람이 바뀌더라도 각각의 단위 조직(총무, 인사, 예산, 행정, 정책 등)에서 표준화된 정보보호 절차 및 프로세스를 자연스럽게 수행하여 정보보호 업무가 물 흐르듯 수행되도록 시스템화하는 방안을 제안한다.

국제 표준화 기구인 ISO/IEC JTC1 (IT 국제표준화조직) SC27(정보보안기술 표준화그룹), WG1

(ISMS 표준화 워킹그룹)에서는 정보보안경영시스템(ISMS: Information Security Management System)에 대한 국제표준화 작업을 수행하고 있으며 관련 국제표준을 ISO 27000 시리즈라는 문서체계로 발표하고 있다.

ISO 27000 시리즈는 정보보호를 단순히 기술적 이슈로 보는 것이 아니라 관리적, 기술적, 물리적 통제들을 포함하는 전사적 차원의 정보보호를 구현하기 위한 체계화된 일종의 경영시스템으로 보는 것이다. 즉 ISO 9000 시리즈 (품질경영시스템)나 14000 시리즈 (환경경영시스템)와 같이 하나의 경영시스템으로서 정보보호를 계획, 구현, 유지보수 및 검토, 지속적 개선 등과 같은 일련의 프로세스로서의 활동을 중요시 하는 점이 기존의 기술적 솔루션 중심의 정보보호 체계와 차이를 보이는 것이다.

둘째, 전자정부서비스가 활성화될수록 정보보호분야 전문가의 확보가 중요한 과제이므로 인력 확보 방안으로, 개인정보보호를 포함한 정보보호 분야의 연간 필수이수 학점을 부여하여 최소한 일정시간 이상 의무적으로 교육을 이수하게 하고, 국내외 정보보호 분야 전문자격을 취득할 경우 승진 가산점을 부여하고, 우선적으로 정보보호 업무를 담당케 하는 것이 필요하다.

셋째, 정보보호 업무 담당 부서 근무를 권장하기 위해서, 정보보호 분야의 교육 훈련을 정해진 기간 이상 받았을 경우 정보보호 부서 배치에 우선권을 부여하고, 정보보호 업무를 일정 기간(수년간) 이상 담당하였을 때 타 부서 이동시 우선적인 선택권을 제공하는 방안을 제안한다.

넷째, 정보화 업무 및 정보시스템 개발·관리 등을 전산·통신직렬 공무원이 직접 수행하던 추세에서 외주용역 개발과 관리 아웃소싱 등으로 변화하여 행정 직렬에서 업무를 담당하는 경우가 더 많은 상태이므로 행정 직렬과 전산·통신 직렬을 통합하여 운영하는 것이 바람직하다. 이럴 경우, 인사 불이익을 우려한 전산·통신 직렬의 불만을 없애는 효과도 부수적으로 얻을 수 있을 것이다.

다섯째, 전자정부에서 사용하는 정보시스템은 거의 대부분 외주용역에 의해서 개발되고 있고 개발 후 운영할 때에도 정보시스템 관리 전체를 아웃소싱하는 상황이어서, 자칫하면 보안에 허점이 발생할 우려가 높다. 따라서 정보시스템 담당자와 외주용역업체가 맡은 바 업무를 적확하게 수행하고 있는 지, 표준과 절차에 따라서 수행하고 있는 지 등등을 효율적으로 관리할 수 있는 프로세스, 제도, 방법론 등을 체계적으로 마련하는 것이 필요하며, 이를 위해 ISO 27001 ISMS를 전자정부 환경에 알맞도록 응용하여 행정기관 정보보호관리체계(G-ISMS)를 개발·적용할 것을 제안한다.

이는 최근의 전자정부서비스 대부분이 웹 서비스를 근간으로 하여 구축되고 있어서 웹서비스 보안요소를 확실하게 적용하기 위해서도 표준화된 프로세스와 절차에 따라서 보안요소를 체계적으로 관리하는 것이 필요하기 때문이다.

추가적으로, 정보보호 교육에 대한 중요성을 절대적으로 강조한다[13,14]. 선진 각국의 정보보호 정책을 살펴보면 대부분의 국가에서 교육과 훈련의 중요성을 인식하고 막대한 자금과 시간을 투자하여 꾸준하게 인력을 양성하나, 우리나라의 경우 예산을 조정해야 할 필요성이 있을 경우 우선적으로 교육 및 훈련 예산을 삭감하는 경우가 대부분이어서 전문 인력의 양성에 어려움이 많다.

4.2 제도 개선

전자정부의 정보보호 수준을 근본적으로 제고하기 위하여 사전 예방 및 지속적인 정보보호수준 관리방안으로써 각급 행정기관에서 국제표준인 ISO 27001 ISMS를 기반으로 한 행정기관 정보보호관리체계(G-ISMS) 인증제도의 도입을 제안한다.

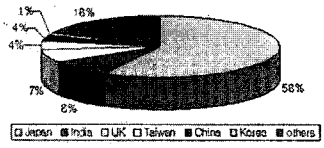
정보보호관리체계 인증제도란 행정기관이 정보보호를 위해 필요한 관리적·기술적·물리적 기준에 적합한 정보보호관리체계를 갖추었는지 심사하여 인증기준에 따라 적절히 운영되고 있는 경우 인증서를 부여하고 지속적으로 사후관리를 수행하는 제도를 말한다[15,16].

대외적인 측면에서 정보보호 관리 능력에 대한 보증은 민원 서비스, 전자 거래, 개인정보보호 등의 분야[17]에서 서비스의 안전성과 신뢰성을 확보하는데 중요한 요소가 될 수 있으나 기관 내부뿐만 아니라 외부에 정보시스템 및 서비스의 정보보호 수준에 대한 신뢰를 제공하기란 더욱 힘들다. 특히 협력업체 운용, 업무의 아웃소싱 등 긴밀한 관계를 맺고 협업할 경우 상대 조직의 정보보호 수준을 확인하기를 원할 수 있지만 그런 요구를 만족시켜주기 위해 내부의 통제나 세부사항을 상대방에게 공개하기는 어렵다.

따라서 이러한 의문을 해소하고 조직의 정보보호 수준에 대한 대내외적 신뢰도를 높이기 위해서 전문적이고 객관적인 제3자에 의한 평가가 필요하다.

이러한 특성으로 인해 세계 각국에서는 자체적인

Japan	2,994
India	440
England	374
Taiwan	210
Korea	74
USA	85
Others	1,663
Total	5,190



※ 2009.2 현재

〔그림 4〕 ISO 27001 ISMS 인증현황
(한국은 민간기관에서 인증받은 사례)

ISMS 인증 제도를 수립하고 이러한 인증의 활성화를 통해 조직의 정보보호 수준을 제고하며 객관적이고 올바른 정보를 제공하여 상호 신뢰를 제고하기 위하여 노력하고 있다[16,18].

세계 각국에서 ISO 27001 기반 ISMS 인증서 발급 현황(한국은 민간기관 인증 현황)을 살펴보면, 일본은 인증을 받을 경우 다양하고 혜택많은 인센티브를 제공하여 발급 1위이고, 가장 두드러지는 성장세는 인도로서 2006년 12월 369개 기관에서 인증서를 발급받았으나 최근 급속한 인도로의 해외투자로 인해 상대방에게 자국 기관의 신뢰도를 높이고자 인증서 발급이 대폭(70여개 기관) 늘어났다.

행정기관에서 정보보호관리체계 인증제도의 도입을 통하여 사후적 사고 대응, 타율적인 규제 중심의 단편적, 일회적, 부분적 보안을 시행하던 방식에서, 각 기관의 정보시스템 혹은 서비스 담당자가 스스로 체계적, 지속적, 균형적으로 관리하도록 변화시킴으로써, 행정기관 및 공공기관의 정보보호 수준이 지속적으로 개선될 수 있는 기반이 마련될 것이며, 장기적으로는 정보보호 수준의 획기적 개선이 이루어 질 것이다.

4.3 인증기준 모델

행정기관에서 제공하고 있는 전자정부서비스에 ISMS 적용방안을 수립하기 위하여 노동부, 행안부, 교육과학기술부, 국민권익위, 국세청, 경찰청, 방위사업청, 서울시, 경기도, 대전시 등의 11개 주요 서비스에 대해서 설문과 현장방문(2008. 9. 4 - 2008. 9. 17)을 병행하여 핵심 정보보호관리 현황 8개 영역 25개 항목을 중심으로 정보보호관리체계 실태 및 애로사항을 파악하고 개선방안을 도출하여 인증기준 모델을 제안한다[12,19-21].

행정기관 ISMS 인증기준을 개발하기 위하여 참조한 기준은 다음과 같다 [12] .

〔표 7〕 현장방문 조사항목

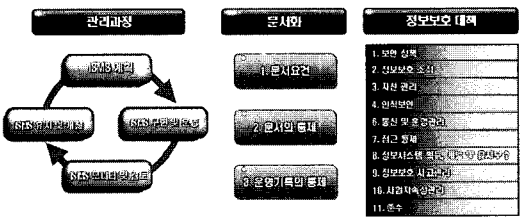
영역	질의 항목
1. 보안 규정 지침 절차	- 정보보호(보안) 활동의 기준이 되는 귀 조직의 보안 관련 규정/지침의 성격을 갖는 문서들은 어떠한 것들이 있는지 나열해 주십시오. - 위의 문서들의 제정/개정의 절차 및 주기는 어떻게 이루어지 기술해 주십시오. - 귀 기관의 보안 규정/지침의 제정/개정 시 직,간접 영향을 주는 보안관련 규정/지침(예: 상위기관으로 부터의 공문 등)의 문서를 나열해 주십시오.
2. 조직	- 귀 기관의 정보보호 관련 업무를 수행하는 사람들을 업무별로 나열하고 정보보호 업무량이 자신의 전체 업무량에 어느 정도를 차지하고 있는지를 기술해 주십시오. - 귀 기관의 전체 조직도와 그 조직도 상에 보안업무 조직(또는 역할과 책임을) 표시해 주십시오 - 귀 기관의 보안 조직과 대외 보안관련 조직간의 역할과 책임을 명시한 상관관계도를 작성해 주십시오 - 조직원 각각의 역할과 책임을 명시한 문서에 보안 관련 내용이 어느 정도 명시되어 있는지를 기술해 주십시오 - 정보보호의 세가지 분야인 물리적 보안/관리적 보안/기술적 보안에 대한 귀 기관내에서의 역할과 책임을 간략히 기술해 주십시오
3. 정보자산 관리	- 정보보호(보안)의 대상이 되는 귀 기관의 정보자산을 파악해 보신 적이 있으십니까? 파악하셨으면, 그 리스트를 제공해 주십시오 - 정보자산외에 보안관리의 대상이 되는 것들을 나열해 주십시오 혹은 보안 관리의 대상을 어떻게 파악하고, 관리하고 계시는지를 간략히 기술해 주십시오 - 자산의 등급 분류 및 취급 방법을 기술해 주십시오.
4. PC 보안	- 귀 기관의 PC 구매에서부터 사용/폐기까지의 절차를 서술해 주십시오 - 위 절차상에서 보안과 관련되어 어떠한 활동이 일어나고 있는지 기술해 주십시오
5. IT (정보시스템) 보안	- 귀 기관의 IT 시스템 도입, 개발, 운영의 절차에 대하여 간략히 서술해 주십시오 - 위 절차상에서 일어나는 보안 활동을 기술해 주십시오 - 귀 기관은 전체 IT업무의 어느 정도를 외부 전문 IT회사에 의존하고 계십니까? - 귀 기관은 전체 보안 업무의 어느 정도를 외부 전문 보안 회사에 의존하고 계십니까?
6. 정보보호 예산	- 귀 기관의 정보보호(보안)을 위한 연간 예산의 규모는 어느정도입니까? - 정보보호 예산의 수립에서 승인/집행시까지의 흐름을 간략히 기술해 주십시오
7. 정보보호 사건/사고	- 귀 기관에서 정보보호(보안)사고가 지난 1년에 발생하였습니까? - 발생하였다면 몇건이 발생하였습니다. (전체 건수만 표시) - 위 발생건수 중 대외적으로 알려진 것은 몇건입니까? - 보안사고 처리 프로세스를 간략히 기술해 주십시오.
8. 보안 업무 애로 사항	- 보안 업무 수행 중 가장 어려운 점은 어떤 것이 있습니까? - 보안 수준 제고를 위해 가장 중요한 측면은 어떤 것이라고 생각하십니까? 중요한 순서대로 3가지만 나열해 주십시오.

〔표 8〕 주요 서비스 실태조사 결과

영역	조사 결과
1. 보안 규정/지침/절차	11개 기관 중 8개 기관이 보안관련 규정 보유 대부분 국정원 국가정보보안기본지침 준용
2. 조직	11개 기관 중 4개 기관만이 보안 전담 인력 보유 대부분 정보보호 역할 및 책임을 별도 문서로 규정하지 않음
3. 정보자산 관리	11개 기관 모두 정보자산을 관리하고 있으나, 자산의 등급 분류는 2개 기관만 수행
4. PC 보안	11개 기관 모두 PC 보안 제품을 활용하고 있음.
5. IT (정보 시스템) 보안	11개 기관 중 7개 기관이 IT 도입 시 보안활동을 수행하고 있음 11개 기관 중 3개 기관은 외부위탁을 통해 관제서비스 등을 수행함
6. 정보보호 예산	11개 기관 중 2개 기관은 5천~6천만원, 4개 기관은 5~10억, 1개 기관은 20억 이상 예산 보유
7. 정보보호 사건/사고	11개 기관 중 5개 기관이 사이버위협, 해킹공격 등 사건 처리 프로세스를 보유
8. 보안 업무 애로 사항	정보보호 관련 유사 점검/감사 등의 업무 가중 인력, 예산 부족

- ISO 27001 인증기준 : 정보보호관리체계 인증을 위한 국제 표준으로 PDCA (Plan-Do-Check-Act) 사이클에 따라 정보보호 위험을 평가하여 11개 분야 151개 통제항목 중에서 필요한 통제를 선정, 구축하고 문서화하여 운영하고 정기적으로 평가 개선할 것을 요구한다.
- 행정안전부의 전자정부 대민서비스 보안수준 실태조사 항목 : 12개 분야 77개 항목에 대한 지표로 이루어져 있다. 평가를 위한 기준이라기보다는 행정기관의 정보보호 현황을 파악하는데 중점이 있다.
- 행정안전부의 개인정보보호 수준진단 지표 : 공공기관의 개인정보보호에 관한 법률에 기초하여 18개 분야 85개 항목에 대하여 만족 여부를 점검한다. 법적 요구사항이므로 반드시 만족해야 하는 사항들이다.
- KISA ISMS 인증기준 : '정보통신망이용촉진및정보보호등에대한법률'에 따라 한국정보보호진흥원(KISA)으로부터 정보보호관리체계 인증을 받고자 할 때 적용되는 인증기준을 말한다. 5단계 관리과정에 따라 정보보호 위험을 평가하여 15개 분야 455개 통제항목 중에서 필요한 통제를 선정, 구축하고 문서화하여 운영하고 사후관리 할 것을 요구한다〔15,16〕.

ISO 27001 ISMS는 국제표준으로 범용적인 환경을 고려하여 통제항목들이 선정된 결과, 이를 우리나라 전자정부서비스 환경에 그대로 적용하기에는 다소 보완해야할 부분들이 있다. ISO와 KISA의 인증기준은 통제항목의 구성이나 점검항목의 수는 차이가 나나, 내용적으로는 유사하며 장기적으로 국제 표준화를 지향하므로 ISO의 구조를 따르되 국내 실정을 반영하여 점검항목을 작성하였다. 또한 행정안전부의 개인정보보호 수준진단 지표 항목은 법 규정적 요건으로서, 조사 대상기관의 응답에서 유사한 조사에 대한 통합요구가 많은 점을 고려하여 단일 심사로 통합할 수 있도록 상응하는 통제항목에 점검 항목으로 포함하였다〔12,17,19-21〕.



〔그림 5〕 행정기관 G-ISMS 인증기준 구조

행정기관 G-ISMS 인증기준은 기존 ISO 27001 ISMS와 같이 관리과정, 문서화, 통제항목(정보보호 대책)의 3개 부문으로 나누어 구성하였다.

최종적으로 관리과정은 ISO의 PDCA 사이클(Plan-Do-Check-Act, 계획-실행-검토-개선)에 따라 4개 관리과정에 대하여 15개 요구사항을 구성하였으며, 이 요구사항의 달성 여부를 점검하기 위한 39개 점검항목을 제시하였다.

문서화는 3개 요건에 대하여 12개 점검항목을 제시하였다. 통제항목은 일반적인 정보보호 대책을 나열한 것으로서 ISO 27001과 같이 11개 분야로 나누어 135개 통제항목, 즉 정보보호 대책을 제공하였다. 이 통제항목들은 모두 구현해야 하는 것은 아니며 관리과정에서 위험분석을 통해 해당 기관에 필요한 대책을 선정하여 구현하여야 한다.

통제항목 즉, 정보보호 대책의 수립 여부를 점검하기 위한 355개의 점검항목을 제시하였다. 이 점검항

목에는 행정안전부의 개인정보보호 수준진단 지표 84개 항목을 포함하고 있다. 개인정보보호 수준진단의 경우 총 85개 항목으로 이루어져 있으나 처리 정보의 이용·제공 시 제공하는 경우와 제공받는 경우의 안전성 검토 요건을 묶어서 하나의 항목으로 작성하였으므로 84개 항목이 되었다.

행정기관용 정보보호관리체계 인증제도는 먼저 전자정부서비스에 적용하고 이후 중앙행정기관에서 정보보호관리체계를 수립하여 운영하는 경우를 고려하여 작성되었으며, 동일한 법 제도의 적용을 받거나 조직문화를 공유하는 중앙행정기관 외에도 지방 자치단체와 소속기관에게도 적용될 수 있다.

그러나 인증제도가 적용된다고 하더라도 기관 단위로 인증을 받게 되는 것은 아니며, 정보보호관리체계는 특별히 보호하여야 할 범위를 정하여 수립하는 것으로서 IT 시스템 단위, 업무 시스템 단위, 또는 조직 단위로 수립할 수 있으며, 해당 정보보호관리체계의 범위에 따라 인증을 받게 된다.

따라서 인증의 범위는 행정기관이 자율적으로 정하되, 초기 도입 시기에는 기관 내 중요 서비스 단위로 정보보호관리체계를 수립할 것을 제안한다. 즉, 초기에는 전자정부서비스와 중앙행정기관의 서비스 중 국민 생활에 밀접한 대국민 서비스를 중심으로 인증을 받도록 하고 차차 정보보호관리체계의 신뢰도 및 인지도를 높여가면서 인증 대상이 되는 서비스 범위를 확장하고, 최종적으로는 기관전체에 대한 인증을 목표로 확산하며, 소속기관 및 산하기관으로 확산, 연계하는 방식을 제안한다.

이를 적용하는 방안에 있어서는 기관의 규모와 정보시스템의 특징에 따라 355개 항목중에서 적정한 수준을 선택 적용하는 것이 필요하고, 각 항목에 대해서도 깊이와 수준에 차이를 두고 적용하는 것이 바람직하다고 생각하며, 행정기관에서 이를 적극 수용할 수 있도록 다양한 인센티브를 제공하는 방안이 필요할 것이다.

V. 결 론

구슬이 서말이라도 꿰어야 보배라고 하듯이 좋은 시스템, 정책, 제도가 있다 해도 현장에서 이를 활용하지 못하거나 적용할 수 없다면 소용없다.

행정기관에서 정보보호관리체계가 효율적으로 실행되기 위해서는 쉽고 간편하게 적용할 수 있는 제도·절차·프로세스 등이 실용적으로 만들어져야 하고 이를 현장에서 운용할 수 있는 구축 방법론과 해설 가이드 등에 대한 추가 연구가 필요하고, 현장에서 적극적으로 수용할 수 있도록 다양한 인센티브 제도가 뒷받침된다면 활성화에 많은 도움이 될 것이다.

현장 업무를 수행하고 있는 행정기관의 담당자들에게서 나온 의견으로 시급성을 요하는 것이 유사한 정보보호 수준 평가 및 실태 조사 등의 제도에 대한 통폐합이 우선적으로 필요하다. 정보보호 인력이 부족함에도 불구하고 여러 부처에서 제각각 평가나 실태조사 등을 중복적으로 실시함에 따라 현장에 있는 실무자들이 유사한 업무에 중복적으로 답하느라 정작 필요한 업무를 수행하기 어려운 상황을 토로하고 있다. 그러나 이와 같은 통폐합을 한 부처에서 주도하기에는 현실적으로 한계가 있어, 전향적인 자세로 협동하여 실마리를 풀어 나가는 것이 필요할 것이다.

어느 조직에서나 최고책임자가 관심을 갖는 분야에 대해서는 조직원 누구나가 관심을 갖게 되므로, 행정기관의 정보화 및 정보보호 업무를 개선하기 위해서는 무엇보다도 위정자, 최고책임자의 절대적인 관심이 중요하다.

앞에서 제안한 여러 가지 문제점과 개선 방안들을 잘 운용할 수 있도록 우리나라 전자정부서비스 환경에 알맞게 통제항목을 선정하여 적용하고자 한 것으로, 이를 행정조직에 잘 응용하여 실용적으로 수행할 수 있게 하는 것이 작금의 숙제로 남아 있는데, 표준화된 정보보호관리체계를 행정기관에서 잘만 운용한다면 기관의 보안수준을 한층 향상시킬 수 있고 안전성을 용하 사이버 위협을 다소나마 줄일 수 있을 것으로 보며 이를 통해 국가 전체의 보안 수준이 향상되기를 기원한다.

참 고 문 헌

[1] 방송통신위원회, "유·무선 통신서비스 가입자 현황(2009.5월말)," pp. 5-6, 2009년 7월.

[2] 서재철, 조찬형, 김주영, 안인회, 나은아, 박수미, "2008 인터넷이용실태조사," 방송통신위원회, 한국인터넷진흥원, 2008년 11월.

[3] 행정안전부, "정보보호 중기 종합계획," 국무회의 보고자료, pp. 11-14, 2008년 8월.

[4] ISO/IEC 27001, "standard for the establishment, implementation, control and improvement of the Information Security Management System," ISO, Oct.

2005.
[5] ISO/IEC 27002, "code of practice providing good practice advice on ISMS," ISO, Oct. 2005.
[6] 행정안전부, "주요국가 정보보호 정책 및 예산," 2008년 4월.
[7] 국가보안기술연구소, "미국 연방정보보안관리법 체계 및 동향," pp. 15-24, 2005년 10월.
[8] 한국정보보호진흥원, "전자정부 대민서비스 보안 수준 실태조사 및 개선방안 연구," 2008년 12월.
[9] 차광승, "지방자치단체의 정보보호 관리체계 구축 방안," 석사학위논문, 경원대학교 소프트웨어대학원, 2007년 8월.
[10] 국가정보원, 방송통신위원회, "2009 국가정보보호백서," 2009년 4월.
[11] J. Pescatore, R. Mogull, E. Ouellet, J. Girard, R. Wagner, J. Heiser, P.E. Proctor, A. Litan, V. Wheatman, A. Hallawell, M. Nicolett, N. MacDonald, P. Firstbrook, Joseph, Feiman, and G. Young, "Hype Cycle for Data and Application Security," Gartner Group, Dec. 2006.
[12] 오경희, 김정덕, 박태완, 권헌영, 김지연, 한근희, "정보보호관리체계 인증제도 도입방안 연구," 한국정보보호학회, 2008년 12월.
[13] 서동현, "A기업의 정보보호와 『정보보호인증제도의 발전방향』에 관한 연구," 석사학위논문, 동국대학교 국제정보대학원, 2007년 2월.
[14] 신영수, "중·소 기업 정보보호 수준 향상을 위한 모델 제안 및 적용," 석사학위논문, 건국대학교 정보통신대학원, 2006년 2월.
[15] 한국정보보호진흥원, "ISMS 인증제도 소개," pp. 6-19, 2007년 8월.
[16] 이강신, 이병욱, 이재로, 김종원, 이재호, "정보보호관리체계 인증준비 가이드," 한국정보보호진흥원, 2002년 9월.
[17] 오경희, 김호진, 김기홍, 이준택, 윤명훈, 박의원, "개인정보보호 등을 위한 ISMS 모델 및 보호대책 개발," 한국정보보호진흥원, 2007년 11월.
[18] 오경희, 김정덕, 박태완, 김지연, 한근희, "전자정부 대민서비스 정보보호관리체계 구축가이드," 한국정보보호진흥원, 2009년 6월.
[19] 고규만, 김재성, 장상수, "정보보호관리체계(ISMS) 구축 시 일반적으로 나타나는 결함사례에 관한 분석," 정보보호학회논문지, 17(4), pp. 34-41, 2007년 8월.
[20] 전용준, 조기환, 김원규, "공공기관의 정보보호관리체계 감사시스템의 설계 및 구현," 인터넷정보학회논문지, 7(5), pp. 81-93, 2006년 10월.
[21] 허순행, 이광우, 조혜숙, 정한재, 전웅렬, 원동호, 김승주, "정보보호 수준평가 적정화 방안 연구," 정보처리학회논문지C, 15(3), pp. 173-190, 2008년 6월.

〈著者紹介〉

한 근 희 (Keun-hee Han) 종신회원
1986년: 서울산업대학교 컴퓨터학과 학사
1988년: 한양대학교 공과대학원 컴퓨터학과 공학석사(정보보안 전공)
2006년: 고려대학교 대학원 컴퓨터학과 이학박사(정보보안 전공)
2006년 3월 ~ 현재: 행정안전부 정보보호정책과 근무
2002년 9월 ~ 현재: 건국대학교 정보통신대학원 겸임교수
〈관심분야〉 인터넷 보안, 통합보안관리, 모바일 보안, 차세대 인터넷 등