情 報 保 護 學 會 誌
第23卷 第5號, 2013. 10

국외 정보보안관리 동향

최 명 길*, 정 재 훈**

요 약

본 연구는 정보보안관리의 중요성에 대해 지적하고, 적절한 정보보안관리에 대해 알아보기 위해 국외의 정보보안관리 현황에 대해 조사연구하였다. 미국, 일본, 영국, 독일은 각각 정부기관에 의해 정보보안관리가 체계적으로 수행되고 있으며, 그 효과에 대해 면밀히 검토하여 우리나라에 적용할 수 있는 방안을 모색해보고자 한다.

Ⅰ. 서 론

정보는 그 자체로도 유용하나, 해당 정보를 제대로 관리하는 것은 정보보안의 무결성, 기밀성, 가용성의 특성상 매우 어렵고, 정보에 대한 침해가 발생할 경우 개인, 조직, 사회에 심각한 위협이 되기도 한다.

최근에는 정보 유출의 심각성이 미디어 매체를 통해 알려짐에 따라, 정보보안 관리의 심각성이 크게 주목받고 있다.

특히 현재 분단 상태인 우리나라의 특수한 환경에 맞추어, 우리나라는 북한 및 외부의 보안위협에 대처하기 위하여 '사이버안전센터'를 신설하고, 운영하고 있다.

'사이버안전센터는' 북한의 사이버공격의 가능성 고조에 따라 사이버 공격 대응방안 수립 및 관계기관 협의체를 구성하고, 정보보호 관련 지침 적용·관리 등과 같은 정책·기획 업무 등을 수행하고 있다.

이러한 사이버 공격 대응방안을 수립하고, 정보화 및 사이버 보안 개선을 위해서 국외 정보화 및 사이버 보안 현황을 고찰할 필요가 있다.

국외 선진 정보화 및 사이버 보안 현황을 살펴보는 것은 보안에서 앞선 상태인 선진국의 보안 현황을 통해 우리나라의 보안 상황을 되짚어볼 수 있으며, 주요 보안 프레임워크를 적용하는 방안을 통해 보다 수준 높은 보안 환경을 구축하는데 도움이 된다.

따라서 본 논문에서는 미국, 일본 및 영국의 정보보안관리 현황을 살펴보고, 특히 국외의 정보보안관리 프로세스인 FISMA와, 정보화 및 정보보안 프로세스 개선방안을 고찰해보고자 한다.

Ⅱ. 미국의 정보보안관리 현황

2.1 FISMA 현황 및 제정 목적

FISMA은 2002년도 제정된 전자정부법(e-Government Act) 중 3편(Title III)의 SEC.301(Information Security)에 포함된 법률이다.

US Code Title 44(Public printing and documents)의 Chapter 35(Coordination of federal information policy)의 Sub-chapter III(Information security)에 포함된다.

연방 정부의 정보와 운영 및 자산을 보호하기 위한 포괄적인 기본 프로임웍 수립하고, 정부기관이 정보와 정보시스템 보호를 위해 전사적 정보보호 프로그램을 개발, 문서화, 구현을 요구하고, 연방정부 기관의 정보보안 강화를 위해서 제정된다.

의회는 한시법으로 2002년 만료 폐기되는 정부정보보안개혁법(Government Information Security Reform Act of 2000)의 한시법 조항을 삭제하고, 이를 연방정보보안관리법(the Federal Information Security Management Act of 2002; FISMA)로 이름을 변경한다.

연방 정부에 관한 정보보안활동의 관리, 감독권은 국토안보부에 부여 : 국토안보부의 미국컴퓨터비상대응팀

* 중앙대학교 경영학과 교수 (mgchoi@cau.ac.kr)
** 중앙대학교 일반대학원 경영학과 박사과정 (selpine@naver.com)

(United States Computer Emergency Readiness Team; US-CERT)을 사이버 보안에 대한 침해사고 대응센터로 승인하고, 컴퓨터 보안표준과 관련하여 국립표준기술원(NIST)와 관리예산처(OMB)의 역할을 강화한다.

NIST는 NIST 산하 정보기술연구소의 컴퓨터 보안과를 중심으로 법령에 규정된 책임- 연방정보 및 정보시스템의 보안강화를 위한 관련 지침과 표준을 개발, 제정한다.

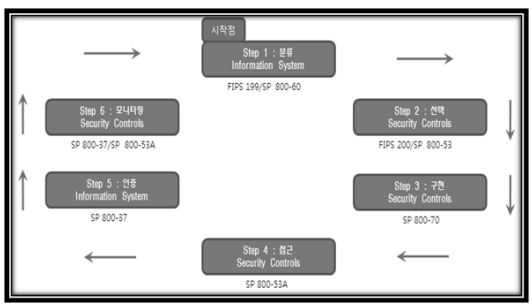
각 연방 정부기관의 정보시스템의 보안 강화를 위한 프로그램 개발, 문서화, 집행을 의무화하고 있으며, 시행 및 감독은 OMB가 담당하고 있고, 준수 등급에 따라 연방정부기관의 정보화 예산을 지급한다.

2.2 FISMA 운용을 위한 표준 문서 구성

NIST는 FISMA에 대한 정부기관의 이해 제고 및 수행 용이성을 위해 FISMA 관련 정보보호 표준과 지침을 개발하고, 해당 표준과 지침을 전체적으로 통합하고 설명하기 위해 위험관리체계(Risk Management Framework; RMF)를 개발하였다.

위험관리체계는 위험을 관리하기 위한 활동을 정보시스템 분류, 보안통제 선택, 보안통제 구현, 보안통제 평가, 정보시스템 인증, 보안통제 모니터링의 6단계로 분류하여 제시한다.

[그림 1]은 FISMA의 위험관리체계를 도식화한 것이다.



〔그림 1〕 FISMA의 위험관리체계

2.3 FISMA 위험관리체계 단계

NIST의 FISMA는 위험관리체계를 총 6단계로 구분하고 있다. 다음은 각각의 단계를 설명한 것이다.

Step 1 : 정보 시스템 분류(Information System Categorize): 특정 사건 또는 위험이 기밀성, 무결성, 가용성 관점에서 정보와 정보 시스템에 잠재적(impact)으로 미치는 영향력에 기반하여 정보와 정보 시스템을 분류

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 선택

Step 3 : 보안 통제 구현(Security Controls Implement): 선택한 보안 통제를 보안 환경 설정에 맞게 구현

Step 4 : 보안 통제 평가(Security Controls Assess): 보안 통제가 시스템의 보안요구사항에 기반 하여 적절한 방법을 사용하였는지, 구현이 정확한지, 운영이 올바른지, 원하는 결과를 도출하는지를 평가

Step 5 : 정보 시스템 인증(Information System Authorize): 정보 시스템 운영에 있어 조직 운영, 조직 자산 또는 개별적인 결과와 관련하여 위험을 판단하고, 위험이 용인될 수 있는지 결정하여 정보시스템 운영을 인증(authorize)

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

Ⅲ. 일본의 정보보안관리 현황

3.1 JISMS 적합성 평가제도

‘ISMS(Information Security Management System) 적합성 평가제도’는 일본정보처리개발협회 JIPDEC (Japan Information Processing Development Corporation)이 운영하는 국제 표준규격 ISO/IEC 27001에 준거한 정보보안 매니지먼트 시스템에 대한 제3자 적합성 제도이다.

JISMS 적합성 평가제도는 국제적인 정합성을 맞춘 정보보안 매니지먼트에 대한 제3자 적합성 평가제도로 일본의 정보보안 수준 전체의 향상에 공헌하며, 해외에

서도 신뢰를 얻을 수 있는 정보보안 수준의 실현을 목적으로 한다.

3.2 JISMS 개발배경

JISMS 적합성 평가제도 이전에는 정보처리 서비스업의 컴퓨터 시스템이 충분한 안전 대책을 실시하고 있는지를 인정하는 '정보 시스템 안전 대책 실시 사업소 인정제도'가 수행되었다.

1981년 일본 통상산업성이 정한 안전 대책에서는 집중 관리되고 있는 정보 시스템의 시설·설비 등 물리적 대책에 중점을 두었으나, 기술적 대책만으로는 안전보안 대책을 포함한 조직전체의 매니지먼트를 확립할 필요성이 대두되었다.

이러한 기존 제도 폐지와 더불어 기술적인 보안 외에도 인간계의 운용·관리 면을 균형 있게 도입하고, 시대의 요구에 맞는 새로운 제도로 2002년 JISMS 적합성 평가제도가 운영되기 시작하였다.

3.3 JISMS 적합성 평가제도 프로세스

JISMS 프로세스는 ISO/IEC 27001의 PDCA 모델을 채용하여 정리되며, 조직의 정보보안 관리체계에 지속적인 학습과 개선 기회를 제공하고, ISO/IEC 27001의 'Plan-Do-Check-Act(계획-실시-평가-개선)'모델을 채용하여 이것을 JISMS 프로세스 모두에 적용하였다.

ISO/IEC 27001의 PDCA 모델을 통해 확립된 JISMS 단계는 다음 [그림 2]와 같다.

JISMS는 총 10단계를 거치게 된다. 다음은 각 단계를 서술한 것이다.

Step 1: JISMS를 실시하는 범위와, JISMS가 미치는 영향의 경계를 결정하며, 산출물은 JISMS 적용 범위를 결정한다.

Step 2: JISMS에 대한 조직의 보안 방침을 결정하며, 산출물은 기본방침 문서

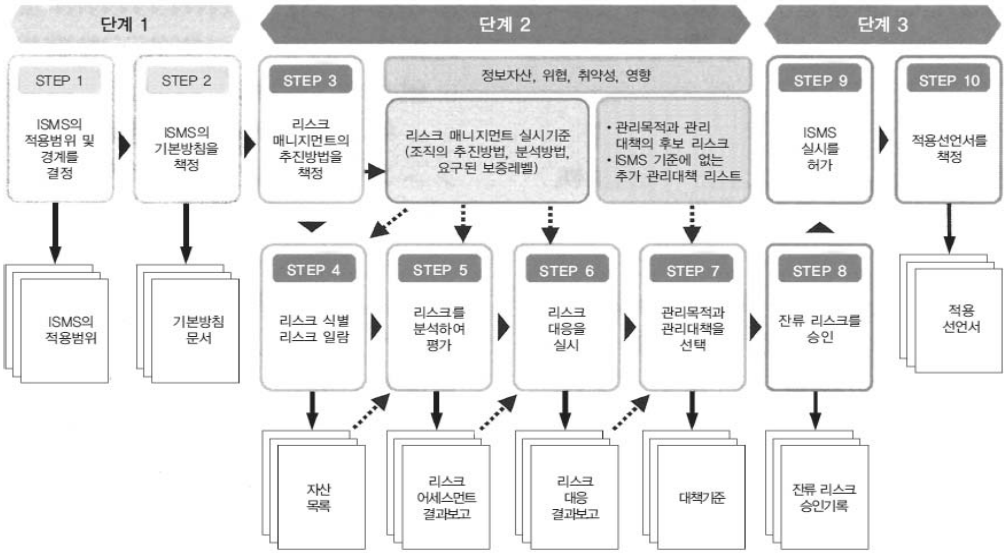
Step 3: 위험 관리의 추진 방법을 책정하며, 산출물은 위험 관리 실시기준가 수립되며, 결정된 추진방법을 바탕으로 Step 4 및 위험 관리 실시기준이 결정된다.

Step 4: Step 3의 추진 방법을 바탕으로 위험을 식별하고 조직의 자산을 목록화하며, 산출물은 자산 목록을 작성한다.

Step 5: 식별된 위험을 분석하여 평가하며, 산출물은 위험 평가 결과서이다.

Step 6: 평가된 위험에 대해 적절한 대응을 실시하며, 산출물은 위험 대응 결과보고서이다.

Step 7: 관리 목적과 관리 대책을 선택하며, 산출물은



〔그림 2〕 JISMS 단계

관리 대책 기준과 JISMS 이외의 추가적인 관리대책을 수립한다.

Step 8: 식별되어 관리되는 위험 이외의 잔류 위험을 승인하며, 산출물은 잔류 위험 승인기록이다.

Step 9: JISMS 실시를 허가한다.

Step 10: JISMS 적용선언서를 책정하며, 산출물은 적용선언서이다.

Ⅳ. 영국의 정보보안관리 현황

4.1 ISO/IEC 27000 패밀리

1998년 영국에서 수립된 BS7799-2(정보보호관리 규격)를 기초로 하여, ISO(국제표준기구)와 IEC(국제전기기술위원회)를 통해 ISO/IEC 27001로 2005년 10월 15일 국제표준이 된다.

현재는 ISO/IEC 27001 규격을 인증심사 기준으로 사용하여 ISO 인증이 제공되고 있다.

ISO/IEC 27000 패밀리의 보안통제는 통제영역 11개, 통제항목 39개, 세부통제항목 133개로 구성되며, 보안통제 유형으로 구분하는 경우, 세부통제항목: 관리적 보안 47개, 물리적 보안 13개 기술적 보안 73개로 분류된다.

〔표 1〕 ISO/IEC 27000 보안통제 구성

보안통제 구분	통제영역	통제항목	세부통제항목	합계
관리적 보안	보안 정책	1	2	47
	조직 보안	2	11	
	자산 관리	2	5	
	인적자원 보안	3	9	
	정보 보안사고 관리	2	5	
	업무 연속성 관리	1	5	
	준거성	3	10	
물리적 보안	물리적 보안 및 환경적 보안	2	13	13
기술적 보안	통신 및 운영 관리	10	32	73
	접근 통제	7	25	
	정보시스템 획득, 개발 및 유지보수	6	16	
합계	11	39	133	

4.2 ISO/IEC 27000 보안통제 분석

4.2.1 보안 정책(Information security policy)[ISO/IEC 27001 A.5.1]

통제 목표: 사업 요구사항과 관련 법규에 부합하는 정보보안 관리 방향과 지원을 제공하기 위함. 경영자는 사업목표와 일맥상통하는 명확한 정책 방향을 설정하고 조직에 대해 정보보안 정책을 공표하고 유지하여 정보보안에 대한 실행의지와 지원을 입증하여야 함

세부통제항목

① 정보보안정책 문서[ISO/IEC 27001 A.5.1.1]: 정보보안정책 문서는 경영자가 승인,공표하고 직원들과 관련 외부조직에게 전달하여야 함

② 정보보안정책의 검토[ISO/IEC 27001 A.5.1.2] : 계획된 간격 또는 적합성, 타당성과 효과성을 지속적으로 보장하기 위해 중요한 수정이 발생한 경우에 정보보안정책을 검토하여야 함

4.2.2 내부 조직(Internal organization) [ISO/IEC 27001 A.6.1]

통제목표 : ① 조직 내부의 정보보안을 관리하기 위함 ② 관리 골격은 조직 내의 정보보안 구현을 착수, 통제하기 위해 수립됨

세부통제항목

① 정보보안 경영자 실행의지[ISO/IEC 27001 A.6.1.1]: 경영자는 명확한 방향, 증명된 실행의지, 정보보안 책임을 정확하게 배정, 주지시켜 조직 내의 보안을 적극적으로 지원함

② 정보보안 조정[ISO/IEC 27001 A.6.1.2]: 보안활동을 적절한 역할과 업무기능 가진 조직의 다른 파트의 대표자가 조정하여야 함

4.2.3 자산에 대한 책임 (Responsibility for assets) [ISO/IEC 27001 A.7.1]

통제 목표

① 조직 자산을 적절히 보호하고 유지하기 위함.

② 모든 자산은 책임을 갖는 소유자(Owner)를 가져야 함

③ 소유자는 모든 자산에 대해 식별하고 적절한 통제

의 유지보수를 위한 책임이 배정되어야 함

세부통제항목

① 자산의 목록[ISO/IEC 27001 A.7.1.1]: 모든 자산은 명확하게 식별하고, 중요한 자산의 모든 목록을 기록하고 유지하여야 함

② 자산의 소유권[ISO/IEC 27001 A.7.1.2]: 정보처리설비와 관련된 모든 정보와 자산은 조직이 지정한 조직이 소유하여야 함

③ 자산의 수용 가능한 사용[ISO/IEC 27001 A.7.1.3]: 정보처리설비와 연관된 정보와 자산의 사용을 수용하는 규칙을 식별, 문서화, 이행하여야 함

4.2.4 고용 이전 (Prior to employment) [ISO/IEC 27001 A..8.1]

통제 목표

① 직원, 계약자, 제3의 사용자가 그들의 책임을 이해하고, 도난+사기+설비 오용 위험을 줄이기위해 고려된 그들의 역할이 적합하다는 것을 보장하기 위함

② 보안책임은 직무기술서와 고용 계약의 조항 및 조건에 고용이전에 적절히 다루어야 함

세부통제항목

① 역할과 책임[ISO/IEC 27001 A..8.1.1]: 조직 정보보안정책에 따라 직원, 계약자, 제3의 사용자의 보안 역할과 책임을 정의하고 문서화하여야 함

② 선발[ISO/IEC 27001 A..8.1.2]: 직원, 계약자, 제3의 사용자 등 모든 지원자의 검증은 연관 법률과 규제, 윤리, 사업요구사항과의 조화, 접근되어야 하는 정보의 분류, 지각된 위험에 따라 이행함

4.2.5 정보보안 사건과 취약점 보고 (Reporting information security events and weaknesses)[ISO/IEC 27001 A.13..1]

통제 목표

① 정보시스템과 관련된 정보보안 사건과 취약점이 적시에 시정조치가 취하는 것이라는 방식으로 전파되는 것을 보장하기 위함

② 공식적인 사건 보고와 승격 절차가 이행되어야 함

세부통제항목

① 정보보안 사건 보고[ISO/IEC 27001 A.13.1.1]: 정보보안 사건은 가능한 빠르게 적절한 관리 경로를 통하여 보고하여야 함

② 보안 취약점 보고[ISO/IEC 27001 A.13.1.2]: 정보시스템과 서비스에 대한 모든 직원, 계약자, 제3의 사용자는 시스템과 서비스에서 관찰되었거나 의심되는 모든 보안 취약점들을 기록하고 보고함

4.2.6 사업 연속성 관리의 정보보안 관점(Information security aspects of business continuity management) [ISO/IEC 27001 A.14.1]

통제 목표

① 업무 활동의 중단을 해소하고, 정보시스템의 중요 고장이나 재난의 영향으로부터 중요 업무 프로세스를 보호하고, 그들을 적시에 재개하는 것을 보장하기 위함

② 사업연속성관리 프로세스는 예방과 복구 통제의 조합을 통해 수용할만한 수준으로 정보자산의 손실을(자연재해+돌발사고+장치고장과 고의적 행동) 복구하여 조직에 영향을 최소화하기 위해 구현하여야 함

세부통제항목

① 사업연속성 프로세스에 정보보안을 포함[ISO/IEC 27001 A.14.1.1]: 조직의 사업연속성을 위해 필요한 정보보안 요구사항을 다루는 조직을 통해 사업연속성을 위하여 관리되는 프로세스를 개발하고 유지하여야 함

② 사업연속성과 위험 평가[ISO/IEC 27001 A.14.1.2]: 업무 프로세스의 중단을 유발할 수 있는 사건들을 그러한 중단의 발생가능성과 중단으로 인한 영향, 정보보안에 대한 중단의 결과와 함께 식별함

4.2.7 법적 요구사항과 준거성 (Compliance with legal requirements) [ISO/IEC 27001 A.15.1]

통제 목표

① 모든 법률, 법령, 규제 또는 계약적 의무와 모든

보안 요구사항 위반을 피하기 위함
② 정보시스템의 설계, 운영, 사용, 관리는 모든 법률, 법령, 규제 및 계약적 보안 요구사항에 영향을 받을 수 있음

세부통제항목
① 적용 가능한 법률의 식별[ISO/IEC 27001 A.15.1.1]: 관련 모든 법률, 법령, 규제 및 계약적 요구사항과 그 요구사항을 충족시키기 위한 조직의 접근을 명확히 정의하고 문서화하여 각 정보시스템과 조직을 위해 최신으로 유지하여야 함
② 지적 재산권[ISO/IEC 27001 A.15.1.2]: 지적재산권이 될 수 있는 자료의 사용과 소프트웨어 제품의 소유권을 사용하는 데 있어 법률, 규제 및 계약 요구사항에 부합함을 보장하기 위한 적절한 절차를 이행하여야 함

4.2.8 보안 지역 (Secure areas) [ISO/IEC 27001 A.9.1]

통제 목표
① 조직의 재산과 정보에 대한 비 인가 물리적 접근, 훼손, 방해하는 것을 예방하기 위함
② 중요하거나 민감한 정보처리설비는 안전한 지역에 위치하여야 하며, 적절한 보안 장벽과 출입통제를 실시하는 보안구역으로 보호되어야 함

세부통제항목
① 물리적 보안 경계[ISO/IEC 27001 A.9.1.1]: 보안경계(카드로 통제하는 입구나 안내 데스크와 같은 방책들)이 정보와 정보처리설비를 포함하는 지역을 보호하기 위해 사용하여야 함
② 물리적 출입 통제[ISO/IEC 27001 A.9.1.2]: 보안지역은 오직 인가된 사람들만 접근이 가능하도록 적절한 출입 통제를 통해 보호하여야 함

4.2.9 운영 절차와 책임 (Operational procedures and responsibilities) [ISO/IEC 27001 A.10.1]

통제 목표
① 정보처리설비의 정확하고 안전한 운영을 보장하기 위함
② 모든 정보처리설비의 관리와 운영을 위한 책임과 절차가 수립되어야 함. 이는 적절한 운영절차를 수립하는 것을 포함함

세부통제항목
① 문서화된 운영 절차[ISO/IEC 27001 A.10.1.1]: 운영 절차를 문서화하여 유지하고 필요로 하는 모든 사용자에게 사용 가능하도록 하여야 함
② 변경 관리[ISO/IEC 27001 A..10.1.2]: 정보처리설비와 시스템의 변경을 통제하여야 함

4.2.10 접근통제를 위한 업무 요구사항 (Business requirement for access control) [ISO/IEC 27001 A.11.1]

통제 목표
① 정보의 접근을 통제하기 위함
② 정보와 정보처리설비, 프로세스에 대한 접근을 사업 및 보안 요구사항을 기초로 통제하여야 함

세부통제항목
① 접근통제 정책[ISO/IEC 27001 A..11.1.1]: 접근통제 정책을 수립, 문서화하고 접근에 대한 사업과 보안 요구사항을 기반으로 검토하여야 함

4.2.11 정보시스템의 보안 요구사항 (Security requirements of information systems) [ISO/IEC 27001 A.12.1]

통제 목표
① 보안이 정보시스템의 필수 불가결한 파트임을 보장하기 위함
② 정보시스템은 운영 시스템, 기반구조, 업무 어플리케이션, 패키지 제품, 서비스, 사용자 개발 어플리케이션을 포함함

세부통제항목
① 보안 요구사항 분석 및 명세화[ISO/IEC 27001 A.12.1.1]: 신규 시스템 또는 기존 시스템의 개선에 대한 업무 요구 사항에 보안 통제 요구사항을 적시하여야 함

Ⅴ. 독일의 정보보안관리 현황

5.1 IT Protection Baseline Manual

독일은 BSI, GISA(German Information Security Agency)의 IT Baseline Protection은 정보보호수준을 차등적으로 적용하고, 가장 하위 수준을 기본적인 보안 기준으로 설정하는 것을 반영한다.

정보보호수준을 "중간/낮음" 수준, "높음" 수준, "아주높음" 수준으로 분류하였다. 여기에서는 "중간/낮음" 수준을 기준으로 위험자산에 대하여 알려진 위협들과 취약점들을 기반으로 추정한다.

목적 달성을 위하여 적합한 대책 항목들을 매뉴얼 형식으로 개발하여 사용자들이 중간수준보호 요구사항을 가진 IT 정보보호를 적은 인건비로 달성하도록 도와준다.

권고된 대책만으로 "높음" 수준의 정보보호를 요구하는 IT 시스템의 정보보호는 달성할 수 없다. 이런 경우는 비용/효과적인 측면에서 개별적인 정보보호분석을 전제로 하며, 여기에서 제공하는 IT의 기본적인 보호대책은 "높음" 수준의 보호대책구축에 포함된다.

5.2 IT Baseline Protection 영역

IT Baseline Protection Manual은 3개의 영역으로 분류하여 표준화시키고 있으며 새로운 사항은 추가 작업이 진행 중이다.

제1영역은 IT 정보보호 구축방법으로 정보보호책임자가 IT 시스템에 대한 정보보호 대책을 수립하기 위한 제반 단계와 계획과정, 구현과정, 관리유지과정으로 구분하여 서술하고 있다.

계획과정: IT 정보보호 정책수립, 정보보호수준의 결정, 정보보호 관리팀의 구성, 정보보호 정책문 작성, IT 정보보호 개념(대상)정립, IT 안전대책의 구현, 인식제고와 교육 계획, 운영 및 적용

제2영역은 IT Baseline Protection을 위한 정보보호 대상 모듈을 분류하고, 권고되는 세부 위협대상을 서술하고있으며, 각 모듈에 대하여 예상되는 위협 시나리오 요소 각각을 제시하고 있다.

제 3 영역은 각 정보보호대상에 따른 예상되는 위협요소의 대상 분류와 함께 항목별 해설을 포함하고 있으며, 또한 위협요소에 따른 표준 안전대책을 6종으로 분류하고 각 세부 항목에 대한 해설을 포함하고 있다.

GISA에서는 IT Baseline Protection 매뉴얼을 통하여 IT 보안의 개념을 인식시키고, 표준 IT 구성에서 중간수준의 보안이 성취될 수 있는 권고대책을 제시하고 있다.

1992년 온수파이프의 파손(물리적 보안)으로 시스템에 고장이 발생한 이래로 1993년에는 미켈란젤로 바이러스에 의한 자료손실, 해커에 의한 신용정보유출, 1994년부터는 인터넷을 통하여 손실의 정도를 파악할 수 없는 침해사고가 발생함에 따라 보안대책수립의 동기가 된다.

1996년 최초로 "낮음수준"의 보안대책 수립을 위한 매뉴얼 개발이 부분적으로 완료되어, 매년 그 내용을 보충하고 보안정도의 수준을 향상시키고 있다.

새로운 IT 개념(통신기술의 발전)이 도입됨에 따라 내용(취약성 보완)이 갱신되고 있으며, 보안정도도 현재 "중간수준"을 위한 보안 권고대책 수립을 위한 내용으로 발전하였다. 향후에는 이에 대한 추가적인 권고대책의 개발과 아울러 "높음"수준의 보안 권고대책이 포함 될 것으로 예측되며, "높음"수준의 보안 권고대책은 별도의 적용기술에 따라 개별대책으로 발전 될 가능성이 높다.

Ⅵ. 결 론

사이버 환경 및 사이버 테러 환경의 급격한 변화는 정보에 대한 위협을 제거하는 것 뿐만 아니라, 정보보안에 대한 관리도 함께 이루어져야 함을 시사하고 있다. 하지만 많은 조직과 기관에서는 단순히 개인정보보호에만 집중하며, 그마저도 제대로 관리되지 못하여 여러 가지 보안사고가 발생하고 있다.

본 연구에서는 정보보안관리의 중요성을 고찰하고, 정보보안관리에 있어서 우리나라보다 선진화된 국외의 정보보안관리 동향을 소개 및 연구 분석하여 보다 향상된 정보보안관리 방법의 일환을 제공하고자 했다.

본 연구에서는 미국, 일본, 영국, 독일의 정보보안관리 프레임에 대하여 소개하고, 각각의 정보보안관리 프레임을 분석하였다. 향후 연구에서는 더 많은 국외의 정보보안관리 동향을 살펴봄과 동시에, 국외 정보보안관리의 프레임에 대하여 면밀한 분석이 필요할 것이다.

참고문헌

[1] *김정태, 이현우(2004), 미국의 사이버보안 분야 기술정책 및 투자 동향, 전자통신동향분석, 제19권, 제5호, pp. 177~184*

[2] *박상돈, 박현동, 홍순좌(2011), 미국 사이버보안 입법의 신경향 연구, 정보·보안 논문지, 제11권, 제4호, pp. 19~29*

[3] *박청수, 이동범, 곽진(2011), 정보보호관리체계를 통한 기업 및 정부 정보보안 강화 방안에 관한 연구, 한국행정학회, 제15권, 제6호, pp. 1220~1227*

[4] *오철호(2009), 정보화평가연구의 경향, 정보화정책, 제16권, 제4호, 겨울호, pp. 3~26*

[5] *NIST SP 800-37 rev 1(Aug 2008)*

[6] *FIPS 199 (Feb 2004)*

[7] *FIPS 200 (Mar 2006)*

[8] *Public Law 107-296, Critical Information Infrastructure Act of 2002, §§211-215, November 25, 2002.*

[9] *United States Office of Management and Budget, Circular No. A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000.*

[10] *교육과학기술부(2011), 국가 사이버보안 대응체계 혁신에 관한 연구, 연구보고서*

[11] *한국인터넷진흥원, 미 연방정부 정보시스템 안전성 보증체계 분석, 2009*

〈著者紹介〉

최 명 길 (Myeonggil Choi)
종신회원

2004년 9월: 한국과학기술원 박사
1995년 9월~2000년 1월: 국방 과학연구소 연구원
2000년 2월~2005년 8월: 한국 전자통신연구원 선임연구원
2005년 9월~2008년 2월: 인제대학교 조교수
2008년 3월~현재: 중앙대학교 조교수
<관심분야> 보안성 평가, 정보보호정책 및 관리

정 재 훈 (Jaehun Jeong)
학생회원

2009년 2월: 인제대학교 시스템경영공학과 졸업
2011년 2월: 중앙대학교 경영학과 석사 졸업
2011년 3월~현재: 중앙대학교 경영학과 박사과정
<관심분야> 정보보호정책 준수, 거버넌스