情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

정보보호관리체계 인증 제도 소개 및 추진 방향

장 상 수*, 김 학 범*, 이 홍 섭*

요 약

인터넷이 급속하게 확산되면서 그 동안 오프라인 환경에서만 가능하던 많은 일들을 사이버 상에서도 가능하게 해 준 반면에 해킹이나 바이러스 등 새로운 보안위협도 증가하게 되었다. 이제까지 국내기업이나 기관의 정보보호에 대한 투자는 기술적인 대응책 위주로 진행되어 왔으나 정보보호 관련 사고는 여전히 증가세를 보이고 있다. 이것은 기술적 대응만으로는 정보보호 관련 사고를 줄일 수 없다는 것을 나타내는 것이다. 최근 기업이나 조직에서는 산발적인 보안관리에서 종합적이고 체계적인 정보보호관리체계가 요구되고 있으며 이용자 보호 및 B2B, B2C간 전자상거래에 의한 상호 안전성, 신뢰성 등 사회적 요청과 전자정부 구현, 지식정보화 사회 기반 조성을 위한 국가적 요청 등 정보보호관리에 관하여 제3자에 의한 독립적이고 객관적인 점검 및 평가를 통하여 적정 여부를 확인시켜주는 인증제도의 필요성이 대두되고 있다. 본 고에서는 국내외 정보보호관리체계 인증 제도의 동향 및 국내 실정에 맞는 바람직한 인증제도 추진 방향과 향후 발전 방향에 대하여 살펴보고자 한다.

Ⅰ. 서 론

우리 사회도 정보통신 기술의 급격한 발달에 힘입어 정보화 사회에 접어든 것은 부정할 수 없는 사실이다. 그리고 우리 눈앞에서 현실화되고 있는 각종 뉴미디어는 여러가지로 유익하고 편리한 삶을 제공해주며, 인간들 사이의 커뮤니케이션을 원활하게 해줄 뿐만 아니라 IT 분야에 새로운 비즈니스를 창출해 주는 것도 사실이다. 그러나 세계는 지금 컴퓨터 해킹 및 바이러스, 도청 등 독버섯 같은 신종 하이테크 범죄가 날뛰고 있어 사이버공간 이용자들에게 불안감을 주고 있다. 이처럼 그 발전을 악용하는 사람들로 인해 미래를 부정적인 시각으로 바라볼 수도 있으나 철저한 대비책을 세우고 지속적인 보안관리를 한다면 안전하리라 확신한다. 그러면 정보보호를 책임지고 있는 정부나 연구기관 또 일반 조직에서는 무엇을 해야 할까? 다가올 예측하지 못할 사이버테러나, 정보통신시스템의 마비, 개인정보유출, 기업의 사업연속성 문제 등에 강력 대응 할수 있는 사후조치가 아닌 예방을 해야 한다. 현대 기업에 있어서 자원의 효율적인 활용과 기업목적의 효과적인 달성에 있어 정보시스템이 결정적인 역할을 하고 있음은 주지의 사실입니다. 정보사회에 있어서 컴퓨터와 통신의 역할이 비약적으로 증대되고 있는 반면에, 컴퓨터 범죄 및 보안 사고 등 그에 대한 역기능을 억제하고 대응할 수 있는 것이 중요한 문제로 대두되고 있으며 기업 경영에 있어서 보안관리(Information Security Management)를 하나의 경영단계로 인식되하 있다. 이러한 보안관리에 대한 외부의 독립적인 평가 또는 인증의 필요성도 점차 강조되고 있다. 본고에서는 정보보호관리체계 인증제도 동향과 금년 7월부터 시행 예정인 정보보호관리체계 인증제도 추진 방향에 대하여 살펴본다.

Ⅱ. 해외 정보보호관리체계 인증 제도 동향

ISMS(Information Security Management System) 즉 보안관리 문제가 정보화시대에 있어서 기업 경영의 한 축으로서 대두되고 있으며 이를 체계적으로 접근하기 위한 보안관리시스템에 대한 인증의 필요성이 요구되고 있다. 이를 위하여 영국의 BSI가 BS7799-Part 1을 ISO에 상정하여 ISO/IEC17799로 국제 표준화하였고, 인증규격인 Part 2도 현재 국제 표준으로 추진 중이며 유럽을 중심으

* 한국정보보호센터(ssjang@kisa.or.br)

로 현재 BS7799-Part 2를 기반으로한 인증 제도를 시행 중에 있어 이에 대한 고찰과 함께 기타 국가에서 시행하는 인증제도에 대하여 살펴본다.

1. 유 럽

세계의 여러 곳에서 인증제도가 구축되어지고 있는데 유럽에서는 Testing and calibration, Inspection, certification of management systems, Certification of products등 적합성 판정을 다루기 위해서 조직된 EA(European co-operation for Accreditation)에서 EA-7/03 (Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems)을 통해 정보보호관리체계 인증에 관한 내용을 다루고 있다.

EA는 2000년 6월 26일 인증기관(Certification Body)들과 Laboratory들과 관련되어서 서로 분리되어 운영되던 EAC(European Accreditation of Certification)와 EAL(European co-operation form Accreditation of Laboratories)를 합병하여 EA를 설립하였다. 네덜란드에 본사를 두고 있으며 Calibration, Certification, Inspection 과 Testing에 관한 일관성을 세워 무역장벽을 줄이는데 그 목적을 가지고 있다.

EA-7/03은 ISMS를 심사하기 원하는 인증기관을 위한 국가 인정기관에게 지침을 제공하고 있다. 전 세계의 다양한 국가 인정기관은 한 국가에서 발급된 인증서를 다른 국가의 인정기관에서 인정하는 프로세스를 운영하고 있다.

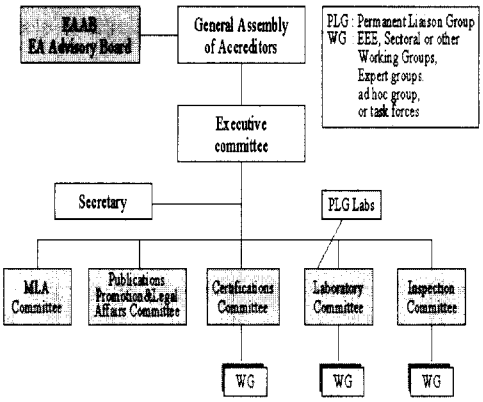
2. 영 국

2.1 개 요

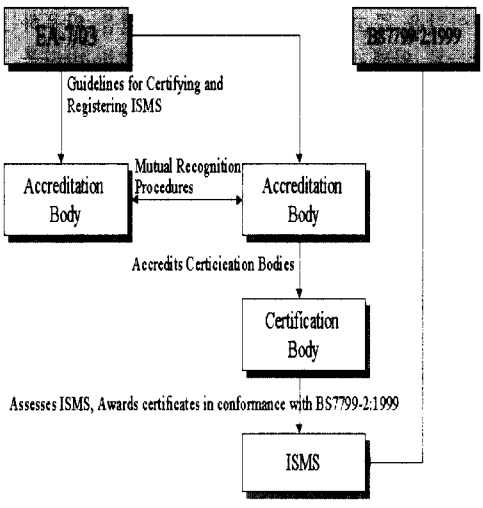
EA에서 인정을 받은 대표적인 Accreditation Body는 영국의 UKAS(UK Accreditation Service)이다. UKAS는 영국의 인증업무를 담당하고 있는 유일한 기구로서 각종 측정실험, 조사, 테스트 기관의 인정을 위하여 1995년에 설립된 상무성(Department of Trade and Industry) 산하의 비영리기관이다.

UKAS는 EA의 회원기관이며 UKAS의 승인을 받은 인정기관은 국제적인 승인을 받은 것과 같은 인정을 받는다. 승인 받는 평가자들은 매년 모니터 받고 4년마다 재평가 받는다. 평가자는 요구되는 기준을 항상 만족시켜야 하며 적당한 재교육을 받거나 승인취소가 되기도 한다.

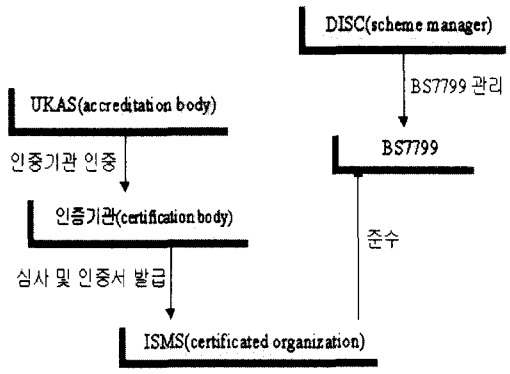
1997년에 상무성은 BS7799에 근거한 정보보호 관리체계에 관한 스킴을 만들기로 하여 BSI(British Standard Institute)의 표준관련 부서 중의 하나인 DISC(Delivering Information Solutions to Customers)에 그 체계의 개발과 관리를 위탁하였다. 1998년 4월에 정식으로 시작된 c:cure 인증체계는 'scheme manager'인 DISC에서 무결성(integrity)과 시장의 필요에 따라 그 체계를 유지하였으나 2년도 안되어, c:cure 인증체계는 EA-7/03의 폭넓은 인정의 관점에서 2000년 10월 2일 상무성에서 c:cure에 대한 지원을 철회·종료되었다.



〔그림 1〕 EA의 구조



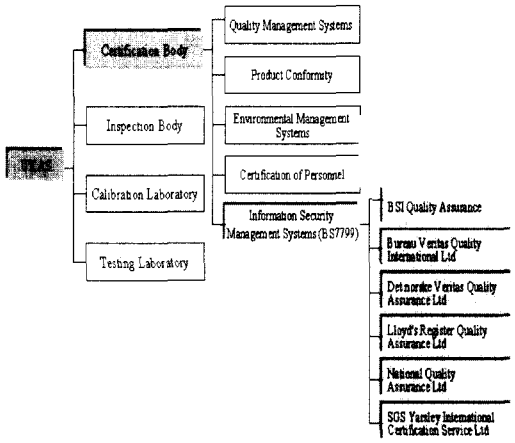
〔그림 2〕 EA의 ISMS인증 구조



〔그림 3〕 c:cure scheme

2.2 ISMS 인증기관 현황

UKAS에서 ISMS 부문과 관련하여 인정을 받은 인증기관은 BSI, BVQI, DNV Certification Limited, Lloyd's Register Quality Assurance Ltd, National Quality Assurance Ltd, SGS Yarsley International Certification Service Ltd와 2001년 4월에 인증기관으로 지정된 KPMG Certification Services까지 7개 기관이 있다.



〔그림 4〕 BS7799관련 Certification Body 조직도

영국의 UKAS로부터 인정을 받은 Certification Body는 영국 이외에 스웨덴, 독일, 네덜란드 등에서도 BS7799과 관련하여 인증업무를 하고 있으며, 각 Certification Body의 지사가 한국에도 진출해 있지만 현재까지 BS7799 인증과 관련한 실적은 없는 상태이다.

〔표 1〕 BS7799관련 인증기관의 URL

인증기관	URL	인증
BSI	http://www.bsi-global.com	BS7799
BVQI	http://www.bvqi.com	BS7799& c:cure
DNV Certification Limited	http://www.dnv.com	BS7799& c:cure
KPMG Certification Services	http://www.kpmg.com	BS7799
Lloyd's Register Quality Assurance Ltd	http://www.lrqa.com	BS7799& c:cure
National Quality Assurance Ltd	http://www.nqa.com	BS7799& c:cure
SGS Yarsley International Certification Service Ltd	http://www.sgs.com	BS7799

3.3 BS7799 인증 사례

영국에서 BS7799관련해서 인증기관으로부터 인증을 받은 사업장 수는 BSI로부터 13업체, DNV로부터 10업체, SGS Yarsley International

〔표 2〕 BS7799 인증현황

인증업체	영 국 내	영 국 외
BSI (18)	- The internet Bank from the Co-operative Bank, - Camelot Group Plc, - Glaxosmithkline, - Cadweb Ltd, Dai-Ichi Kangyo Bank Ltd, - Volex Group Plc, - DBI Associates Ltd, - Midas-Kapiti International, - Business Coach IT Management, - Property Search Agency Ltd, - NETSTORE Plc, Serco Consultancy, - Total Network Solutions Ltd	- Vodafone, - Glaxo Welcome Manufacturing, - The University of Texas, - Amoun Pharmaceutical Co, - TQM Consultants Co Ltd (독일, 싱가포르 미국, 이집트, 홍콩)
DNV (10)	- BSC Consulting, - Foreign and Colonial Management Ltd, - Idetica Limited, - Insight Consulting, -Logica UK Limited, -Marconi Secure Systems	- ABB Facilities, - Gesab Engineering, - PICC-Xiamen branch, - C2 Management, - Folksam, - Computer Sciences Corporation (스웨덴, 중국)
SGS (4)	- L.E.D.U., - Brite Voice Systems Group, - Terrington Systems Limited, - Terrington Systems Ltd	-

Certification Service Ltd로부터 4업체, BVQI로부터 2업체 등 약 30~40여 업체로 추산되며, 그 외 기관은 다수 있는 것으로 파악된다.

3. BS7799

3.1 개 요

정보보호에 대한 인증이 필요한 조직들의 요청에 의해 지난 영국 BSI에서 98년 2월15일 제정한 정보보호관리체계 인증규격인 BS7799는 현재 정보보호를 위한 유일한 영국 국가표준으로 최상의 실행을 위한 포괄적인 일련의 관리방법에 대해 요건별로 해석해 놓은 규격이다. 이미 BS7799 : 1999 Part 1은 국제규격인 ISO/IEC 17799로 채택(2000년 12월1일)되었으며, 인증규격인 Part 2도 Part 1과 마찬가지로 국제표준으로 검토하고 있으나 채택 여부 와 시기는 아직 불확실한 상태이다. BS7799는 전세계 많은 나라에서 표준으로 채용되고 있으며 스웨덴의 경우 이 표준들을 그들 나름대로 SS627799라고 재명명해 놓았으며 호주와 뉴질랜드에서는 ANZ4444로 명명되어 있다. 이 표준은 또한 여러 국가에서 중국어, 독일어, 핀란드어, 프랑스어, 네덜란드어, 일본어, 노르웨이어, 포르투갈어, 스웨덴어, 그리고 한국어까지 전 세계에 걸쳐 수많은 언어로 번역되어 출간되고 있다.

(1) 영국 BSI의 정보보호관리 표준
(2) 1999년 개정판은 ISO/IEC17799로 표준화
(3) 정보보호관리체계를 효율적으로 수립, 수행, 감시하기 위한 방법론을 제시
(4) 조직상호간의 신뢰성 있는 거래를 위한 기준

3.2 BS7799 구성요소

- Part 1(Code of practice for information security management)은 정보보호관리에 대한 실행지침으로 총 10개의 주요세션으로 구성되어 있으며, 127가지의 보안 지침을 제공함으로써, 정보보호관리에 대한 포괄적인 세트를 제공하고 있고, 참조문서로 사용할 수 있다. ISO/IEC17799의 목적은 관련 회사가 공식적으로 고객 정보에 대한 비밀성, 무결성, 가용성을 보장할 수 있도록 하는데 있다. ISO/IEC 17799 : 2000은 실질적인 업무 또는 책임을 맡고 있는 사람들이 특별한 지역에 적합한 실질적인 세이프가드를 식별할 수 있도록 10개의 주요 섹션하에 127가지의 보안 통제항목을 정의하고 있다. 또한 이 규격은 위험관리(Risk management)의 중요성을 강조하고 있으며 관련된 지침만 실행하면 되는 것으로 하고 있다. 규격의 범위는 음성과 그래픽 그리고 휴대폰과 팩스와 같은 매체를 포함한 모든 형태의 정보에 대해서 다루고 있다. 신 규격은 전자상거래, 인터넷, 아웃소싱, 텔레워킹 그리고 이동컴퓨팅과 같은 업무를 수행하는 새로운 방식을 감안하고 있다.

- Part 2(Specification for information security management)는 정보보호관리체계(ISMS)에 대한 규격으로 정보보호관리체계 문서화 수립·실행에 대한 요구사항과 개별조직의 필요성에 따라 실행될 수 있는 정보보호관리 요건을 규정하고 있다. 여기에서는 "조직은 문서화된 ISMS를 구축하고 유지해야 한다"고 명시하고 있으며, 이는 보호대상의 자산과 위험관리에 대한 조직의 접근과 통제목표 및 방안, 그리고 요구되는 보장수준을 언급해야 한다는 것을 의미한다.

〔표 3〕 BS7799-Part 2 구성 체계

4.1	보안방침	정보보호에 대한 경영방침과 지원사항을 제공하기 위함
4.2	보안조직	조직내에서 보안을 효과적으로 관리하기 위해서는 보안에 대한 책임을 배정
4.3	자산분류 관리	조직의 자산에 대한 적절한 보호책 유지
4.4	인사보안	사람에 의한 실수, 절도, 부정 수단이나 설비의 잘못 사용으로 인한 위험을 감소
4.5	물리적 보안	비 인가된 접근, 손상과 사업장과 정보에 대한 영향을 방지하기 위함
4.6	운영관리	정보처리 설비의 정확하고 안전한 운영을 보장하기 위함
4.7	접근통제	정보에 대한 접근통제를 하기 위함
4.8	시스템 개발 및 유지	정보 시스템내에 보안이 수립되었음을 보장하기 위함
4.9	사업지속성 관리	사업활동에 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업활동을 보호하기 위함
4.10	부합성	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보안 요구사항의 불일치를 회피하기 위함

BS7799-2:1999는 어떻게 ISO/IEC 17799를 적용하고 ISMS를 구축하는지 알려주고 있다. 또한 6단계 프로세스를 정의하고 있다. 정보보호 관리체계 프레임워크를 수립하는 단계로 1단계는 정보보호정책을 정의하고, 2단계는 정보보호관리 체계의 범위를 정의, 3단계는 적절한 위험평가를 실시, 4단계는 관리해야 하는 위험영역을 조직의 정보보호정책과 요구되는 보장수준을 토대로 식별, 5단계는 적절한 통제목표 및 방안의 선정과 그 선정을 정당화하고, 6단계에서 적용성 보고서를 설정한 통제목표 및 방안과 그것의 설정 사유는 적용성 보고서로 문서화하는 단계를 정의하고 있다.

4. 기타 국가

4.1 스웨덴 (SS627799)

스웨덴은 정보보호관리체계인증에 관련된 ISO 17799-1 표준을 그들 나름대로 SS627799라 재명명하여 국가표준으로 만들어 인증을 시행하고 있다. 정보보호관리체계인증을 수행할 인증기관을 ISO Guide 62(EN 45012)에 따라 선정하여 인증기관이 정보보호관리체계인증 신청 업체의 ISMS를 SS627799에 따라서 인증을 해주게 된다. 인증과 관련된 다국적기업인 DNV에서는 스웨덴의 SS627799를 이용하여 스웨덴에서 처음으로 인증을 받은 ABB Facilities을 비롯하여, Gesab Engineering, PICC-Xiamen branch, C2 Management를 인증한 실적이 있으며, 위의 실적 이외에도 1999년과 2001년에 Folksam과 Computer Sciences Corporation이 pre-assessment를 받은바 있다.

4.2 호주, 뉴질랜드

호주와 뉴질랜드에서는 정보보호관리체계에 대하여 호주/뉴질랜드 표준위원회 IT/12를 공동으로 구축하여 AS/NZS4444를 발표하였다.

AS/NZS4444는 호주와 뉴질랜드의 표준기구에서 검토하여 영국의 정보보호관리기준인 BS7799와 동일하게 만들어졌다. 따라서 AS/NZS4444도 BS7799와 마찬가지로 Part 1 : Code of practice for information security management와 part 2 : Specification for information security management systems으로 나뉘어져 있다.

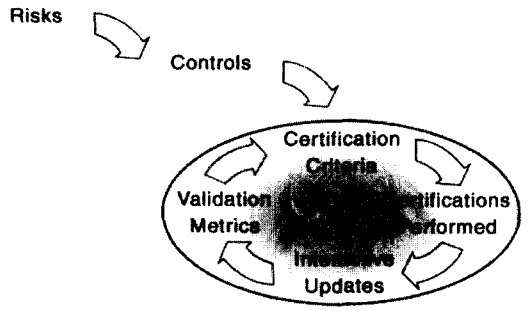
이 표준은 BS7799와 마찬가지로 조직의 관리자와 구현, 이행, 정보보호의 유지에 책임이 있는 직원에 유용하게 이용 된다.

정책과 절차문서들 그리고 모든 관련된 기록들로 구성된 적용명세서에 기록된 통제목적과 통제항목들이 조직의 ISMS이다. 호주/뉴질랜드 표준을 인정받기 위해서는 ISMS가 구축되어지고 유지되는 것을 제3자 인증기관으로부터 인정을 받아야 한다. 또한 호주/뉴질랜드 표준을 따른 것으로 법적인 의무를 면제받을 수 없다.

5. 기타 해외 유사 인증 제도

5.1 미국 (TruSecure 인증)

TruSecure는 1989년 미국에서 보안 전문 그룹으로 설립된 가트너의 협력 자회사로, 범 세계적으로 보안 솔루션에 대한 제품 인증 및 각종 보안관련 멤버쉽과 학술기고 컨소시엄의 세계적인 리더 역할을 수행하고 있으며 NCSA(National Computer Security Association)과 ICSA.net(International Computer Security Association)의 명칭을 거쳐, 지난 1989년부터는 인터넷 관련 보안 서비스를 제공하고 있다.



[그림 5] 인증 라이프사이클 (BodyGuard Service)

TruSecure 관리체계 인증 서비스는 프로세스 개념의 순환 반복적인 BodyGuard Service 형태의 보안 서비스로 11년간의 풍부한 경험과 120여 소프트웨어 벤더와의 깊은 유대 및 각종 인증을 통한 지식기반을 바탕으로 인터넷 관련 시스템, 애플리케이션 등에 대해 보안 적용 가이드 및 on-site visit을 통한 컨설팅, 원격 기반 진단 및 솔루션 제

시 등을 통한 종합적인 보안 서비스 솔루션으로, 고객은 TruSecure Service의 진단 및 솔루션 제시에 따라 보안 상태가 적정 수준에 오르게 되면 정보보호관리체계 인증과 유사한 TruSecure 인증을 부여하고 있다.

5.2 일본의 프라이버시마크제도

1997년 일본 통상산업성은 '민간부문에 있어서 전자계산기처리에 관계된 개인정보의 보호에 관한 지침'(통상산업성 고시 98호, 이른바 '개인정보보호지침')을 제정하여, 민간부문에 있어서 개인정보 관리의 가이드라인을 제시한 바 있다. 이 가이드라인이 제정되고 난 뒤, 민간사업자가 이 가이드라인에 따라 개인정보관리를 하도록 유도하기 위해서는 인증마크 제도의 도입이 필요하다는 논의가 제기되었다. (재)일본정보처리개발협회가 이러한 논의를 구체화하여 도입한 제도가 1998년 4월부터 시행한 '프라이버시마크제도'이다. 1999년 11월말 현재 이 프라이버시마크를 부여받은 업체는 총 81개 업체에 달한다.

5.3 미국의 TRUSTe

TRUSTe마크제도는 인터넷에서도 신뢰의 상징으로서 UL마크나 Good Housekeeping과 같은 인증마크(Seals of approval)의 필요에 의해 생겨나게 되었다. TRUSTe의 프라이버시 원칙에는 프라이버시보호대책(privacy policy)의 채택과 이행, 개인정보의 수집과 사용에 대한 통지와 공시(notice and disclosure), 선택과 동의(choice and consent), 즉 이용자에 자신의 정보를 통제할 수 있는 기회 부여, 정보보안과 품질 및 접근(data security and quality and access), 즉 개인 식별 정보의 보안성과 정확성을 보호하기 위한 수단으로 강구되고 있다.

5.4 미국의 BBB Online마크제도

미국 경영개선협회 이사회(Council of Better Business Bueaus)가 운영하는 BBB 온라인마크는 신뢰성마크(reliablity seal)과 프라이버시마크(privacy seal) 등 두 개의 마크로 구성된다.

BBB는 민간사업자의 회비로 운영되는 비영리단체로서, 소비자가 구매를 하기 전에 도움이 되도록 회원사에 대한 자료를 작성하여 제공하고, 자선단체에 관한 정보를 제공하며, 조정 및 중재제도를 통하여 소비자의 불만을 해결하는 등의 사업을 수행한다.

- 신뢰성마크

신뢰성마크는 1997년 4월에 시작되었으며 일정한 자격이 되는 업체에게 해당 업체가 BBB의 회원사이며, 믿을 수 있는 업체임을 표시하는 마크이다. 소비자가 이 신뢰성마크를 클릭하면 BBB에 저장되어 있는 회사에 관한 데이터 베이스에 접근할 수 있다. 1999년 8월 현재 3,600개 업체가 신뢰성마크를 부착하고 있다.

- 프라이버시마크

프라이버시마크는 1999년 3월에 시작되었다. 이 마크는 해당 업체가 엄격한 수준의 개인정보보호원칙(privacy principles)에 따라 개인정보를 관리하고 있으며, 공신력 있는 기관으로부터 정기적으로 개인정보 관리 상태에 대해 점검을 받고, 소비자불만처리 절차를 갖추고 있음을 표시한다.

5.5 영국의 Hall마크제도

Hall마크는 IMRG(Interactive Media in Retail Group)가 회원사를 대상으로 IMRG의 전자상거래 영업규정 (IMRG Code of Practice for Electronic Commerce)에 적합한 영업활동을 하는 업체를 대상으로 부여하는 마크제도로서 1997년 10월 14일부터 시행되었다. IMRG는 쌍방향미디어를 이용해 소매를 하는 회사(Interactive Media in Retail)들의 단체로 1990년 영국에서 설립되었다. 현재 20개 국가에 걸쳐 400개의 회원사가 참여하고 있으며, 주기적인 시장조사와 보고서의 발간, 업계 자문, 공동프로젝트의 수행과 같은 임무를 수행한다.

6. 기타 국내 유사 인증 제도

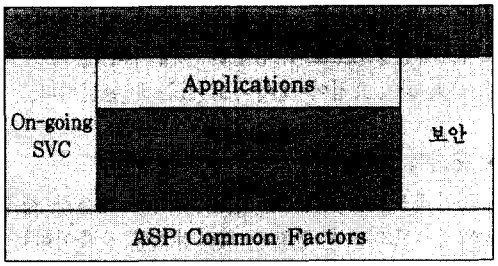
6.1 인터넷 안전마크제도

소비자의 건전한 소비활동 보장과 전자상거래에 따르는 피해의 최소화와 21세기 핵심산업 기반인 인터넷의 활성화를 위해 공급자와 이용자, 사업자와 소비자간 신뢰관계를 형성하고자 한국정보통신진흥협회에서 민간 자율적으로 2000년에 인터넷사이트

안전마크제도를 도입하여 그에 대한 일환으로 "이용자가 믿을 수 있는 인터넷 사이트(SAFE SITE)"에 대해 인터넷사이트안전마크를 부여하고 있으며 또한 이용자 보호를 위한 안전한 사이트 관리 모델 및 지침 등을 개발 보급하고있다. 2001년 현재 인증 부여 기관은 삼성전자외 27개 기관이 있다.

6.2 ASP(Applications Service Provide) 인증제도

ASP 서비스 제공자와 이용자 양측에 신뢰성, 안정성 확보를 통해 ASP 산업이 원활하게 수행되도록 지원하는 제3자의 진단, 평가, 인증, 감리 활동으로 2000년도부터 한국정보통신진흥협회에서 민간 자율적으로 실시하는 인증제도로 인증의 대상은 5개의 Layer로 구분하여 데이터센터(Data Center), 네트워크 서비스(Network Service), 애플리케이션 서비스 (Application Service), 보안 서비스 (Security Service), 지원서비스(On-going SVC)에 대하여 5개 등급으로 구분 평가 심사하여 인증을 주고 있다.



〔그림 6〕 ASP 인증의 대상

6.3 전산감리 제도

● 감리제도 정의

현재 한국전산원을 주축으로 민간 감리법인에서 시행하고 있는 정보시스템 감리제도는 그 성격은 인증제도와는 다르나 효율성, 효과성, 안전성을 추구하는 감리 목적과 인증과는 상당한 유사성이 있다고 하겠으며, 정보시스템 감리에 대한 정의는 국가의 특성에 따라 달리 해석할 수 있는데, 정리요약하면 표 4와 같다.

〔표 2-4〕 정보시스템 감리의 정의

구분	정보시스템 감리 정의	강조점
ISACA 정의 (미국)	자동화된 정보처리시스템의 모든 측면 또는 특정부문을 검토하고 평가하는 각종활동	상호접속성, 신뢰성 유용성 및 합법성
시스템 감사기준 (일본,1995)	감리대상으로부터 독립된 객관적인 입장에서 컴퓨터를 중심으로 하는 정보시스템을 종합적으로 점검, 평가하여 관계자에게 조언, 권고하는 것으로 정보시스템의 유효이용 촉진과 폐해제거를 동시에 추구하며 건전한 정보화를 도모하는 것	유효성 신뢰성
정보시스템 감리기준 (한국전산원)	정보시스템 감리인이 전산망의 효과성, 효율성, 보안성 및 준거성의 관점에서 자료의 수집 및 분석을 통해 전산망을 점검, 평가해 감리의뢰인 등 관계자에게 조언, 권고하는 것	

● 정보시스템 감리의 목적

(1) 효율성(Efficiency) : 제한된 자원으로 최대의 산출물을 제공하는 속성

(2) 효과성(Effectiveness) : 사전에 정의하고 요구된 목적을 달성하는 속성

(3) 안정성(Security) : 각종 위험의 차단정도의 속성

● 정보시스템감리제도 현황

국내 정보시스템감리는 전산망보급확장과 이용촉진에 관한 법률(1986년)에 의거 국가전산기간망사업 중 행정전산망 선투자사업에 대한 사업비정산목적으로 1987년3월에 한국전산원이 회계 및 기술분야의 감리를 시행하면서 시작하였는데, 미국·일본 등 외국과 같이 정보시스템의 내부통제검토에 역점을 두고 운영과정에서의 부정적발을 주목적으로 하는 데 비해, 국내의 정보시스템감리는 공공부문의 기술감리에 중심을 두고 진행되어 오다 1996년부터 민간감리법인에서도 감리업무를 시행하고 있다. 전산원을 포함한 민간 감리법인에서 시행한 실적과 최근에 회계법인에서 시행한 전산감리 수까지 포함한다면 표 5의 현황보다 더 많을 것으로 추산된다.

〔표 5〕 연도별 전산감리 시행 현황

구 분	'93	'94	'95	'96	'97	'98
감리요청	11	16	33	67	83	99
한국전산원 시행	11	16	33	65	74	65
민간감리법인 이양				2	9	34

〔출처 : 한국전산원〕

Ⅲ. 국내 정보보호관리체계 인증 제도 시행

오늘날 정보의 가치가 기업의 발전 및 연속성을 결정할 수 있는 중요한 요소로 대두되었으며 사업에 필수적인 정보자산의 보호, 경쟁력 유지, 법규에 일치, 상업적 이미지의 제고, 위험의 감소, 취약부분에 대한 보안을 위해서는 정보보호관리체계의 조직 내 정착 및 인증을 획득하고 유지·관리함으로써 조직 내부에서 정보보호관리체계(ISMS)의 독립적인 검토를 수행할 수 있으며, 취약부분을 식별하고 개선을 할 수 있는 기획을 가질 수 있고 관리자는 정보를 소유 및 위험에 따른 손실을 최소화할 수 있다. 국내에서도 이미 정보 시스템을 갖고 있는 기업이나 기관들에서 체계적인 위험분석 및 보안관리에 대한 요구가 늘어나고 있으며, 보안 서비스 업체의 컨설팅 내역에서도 변화의 바람이 불고 있다. 이러한 정보보호관리체계의 인증 제도 시행에 관한 필요성 과 효과 등에 대하여 살펴보기로 하겠다.

1. 인증제도 필요성

조직의 최고 책임자나 정보보호책임자 입장에서 정보보호관리체계에 대한 인증의 필요성은 보안관리에 대한 그들의 몇 가지 질문에 답변으로 인증에 대한 필요성을 역설할 수 있겠다.

(1) 과연 우리 기업은 보안에 안전한가 ?
(2) 정보보호관리체계가 합리적이고 비용 효과적인가 ?
(3) 현재의 보안 대책들이 적정한 방법으로 구현·이행되고 있는가 ?

라는 이 세가지 질문은 다시 두가지 문제로 축소할 수 있다. 하나는 인증을 받는 입장에서 생각해보면 관련 정말 우리가 정보보호관리체계의 유효한가? 라는 것이고 또 다른 하나는 이용자의 입장에서 생각해 보는 것으로서, 정보보호관리체계에 대한 신뢰성에 대한 문제이다.

● 조직내부의 요청

현대 조직에 있어서 정보시스템에 대한 침해사고 등 예기치 못한 사고의 발생 과 내부인의 보안 사고 등으로 인한 피해는 조직 사활에 걸려 있을 수 있는 큰 위험에 직면할 가능성이 있다. 조직에 내재하고 있는 이러한 위험(risk)은 기업에 막대한 손실을 끼칠 수도 있는데 대부분의 최고경영자나 일반관리자들은 이것에 대한 이해가 충분하지 못한 것이 현실이다. 다만 어떤 재해가 구체적으로 발생했을 때 비로소 그것이 미치는 영향을 이해하는 경향이 있다. 예를 들면, 1999년 국내 증권회사의 증권시스템이 침수하여 증권업무가 마비되는 사태가 발생할 당시에만 해도 이러한 사태에 대비하여 시설에 대한 신뢰성 및 안전성에 대하여 또는 재해 복구시스템 등을 고려하게 된다. 조직의 자사을 보호하고 침해사고에 대한 대응책 등 이러한 불의의 사태에 대비할 장치를 갖고 있어야 한다는 조직 내부에서의 요청이 있다.

● 사회적 요청

B2B, B2C간 전자상거래가 활성화 되면서 이용자의 개인정보보호 및 상호 안전성, 신뢰성 확보가 사이버 거래에서 정보보호 만큼 해결해야 할 가장 큰 과제로 대두 된 것이다. 기업의 효율성을 높이고 타기업에 비해 전략적인 우위를 확보하기 위해서 정보시스템의 안전성, 신뢰성이 얼마나 중요한 것인가는 최고 경영자나 일반관리자들도 모두 인식하고 있을 것이다. 이와같이 최근의 정보시스템의 전략적인 중요성에 대한 인식과 함께 정보보호에 대한 인식이 일반 이용자들에게 까지관심을 불러 일으키키고 있으며, 개인정보보호나 안전한 금융거래 등으로 인한 범 사회적인 요청이 일어나고 있는게 현실이다.

● 국가적 요청

국가적으로는 대 국민 민원 서비스 개선과 행정정보화 등 전자정부 구현과 지식정보화 구축이라는 대명제하에 기업, 학교, 연구계, 이용자 등 각계 각층에서 편리한 대 정부 민원서비스 및 행정의 효율화를 요구하고 있다. 이러한 정보화의 기반 구조에는 정보시스템, 정보통신망 등이 안전성과 신뢰성이 확보 없이는 실패하고 말 것이다. 최근의 불법 소프트웨어의 단속이라든가 음란사이트 단속은 그 단면을 보여주고 있는 것이다. 이용자나 서비스제공자가 모두 관련 법규를 준수하고 내부 조직의 기준이나 절차, 지침을 제대로 이행하고 철저한 교육 훈련과 정보보호에 대한 윤리 등을 이행하고 있다면 외부의 불법 접근이나 으로 보안사고를 최소로 줄일 수 있을 것이다. 조직의 자산에 대한 적절한 보안대책이 강구되지 않는 한 그렇지 않을 때와 비교하여 보다 많은 여러 가지 위협에 노출 될 가능성이 크다 하겠

다. 최근의 법제도 제정 및 개정에 따른 주요정보통신기반시설에 대한 보호 대책 수립과 정보통신서비스 제공자 및 IDC 등 정보통신시설제공자 등이 준수하도록 요구하고 있으며, 이용자보호 및 개인정보보호, 불법 정보 유출에 대한 정보보호관리 강화를 더욱 요구하고 있다.

2. 인증제도 영향 분석

정보보호관리체계 인증 제도가 근본적으로 조직이나 기업에 어떤 영향을 미칠 것인가 하는 것이다. 이런 측면에서 정보보호관리체계 인증 제도를 도입하기에 앞서서 이것이 기업에 미치는 여러가지 영향에 대해서 살펴보는 것은 의의가 있는 일이라 하겠다. 왜냐하면 정보보호관리체계 인증 제도의 실시에 따른 영향을 살펴보는 것은 이러한 조치가 가져올 수 있는 긍정적인 면을 살리고 부정적인 면을 최소화할 수 있는 방안을 자연스럽게 유도할 수 있기 때문이다. 이처럼 정보보호관리체계 인증 제도가 기업에 미치는 조직내부의 요청, 사회적 요청, 국가적 요청 등 그 영향과 중요성, 이에 따른 최고 경영자의 관심 등을 고려 해 볼 때 정보보호관리체계에 대한 평가 및 인증은 일반 조직에서 당연한 귀결이고 필수적이라고 할 수 있겠다. 하지만 현재 국내에 실제로 정보보호관리체계 인증를 받을 수 있도록 요건을 갖추고 지속적으로 유지·관리 하고 있는 기업이 몇 없다는 것이다. 인터넷이 보급된지 10년이 넘었으나 여전히 보안에 문제 없다고 자신있게 말할 수 있는 조직이나 기업은 없다고 본다. 이제부터라도 국내 기업이나 일반 조직들이 종래의 무계획적인 보안관리에서 보다 효율적이고 통합적인 입장에서 보안관리를 하고 그에 따른 객관적이고 독립적인 제3의 기관에서 평가하고 검증을 걸쳐 인증을 받아야 할 시기가 되었다고 본다.

〔그림 7〕 정보보호관리체계 인증

3. 인증제도의 기대효과

- 현재의 정보 시스템 운영상에 처해있는 위협으로부터 발생할 수 있는 손실 가능성을 정량적으로 예측 대처 하고 위험의 수준을 관리자나 사용자가 이해하고 위험 가능성을 줄일 수 있도록 한다.
- 조직의 자산에 대한 안전성, 효과성, 효율성, 신뢰성을 향상시킬 수 있다.
- 위험 분석 및 평가를 통한 위험수준의 가시적 표현으로 관리자와 사용자의 보안의식 고취를 할 수 있다.
- 위험 발생 가능성이 높은 부분에 대해 우선 순위와 비용/효과적인 측면을 고려하여 보안대책을 선정할 수 있도록 의사결정을 지원한다.
- 정보보호관리기준에 적절하게 합치되는지 검증함으로써, 해당 조직의 보안수준을 높이고 고객 또는 고객사 들로부터 신뢰감을 확보 할 수 있다.
- 정보보호관리를 제대로 하고 있다는 것을 국가인증기관으로부터 인정받게 되는 것이므로 대외적인 신뢰도와 경쟁력을 제고 할 수 있다.
- 관련 법규나 절차, 지침 등을 준수하고 있다는 것을 이용자 또는 거래 당사자에게 기업의 이미지 제고를 할 수 있다.
- 기업 경영의 목표를 실질적으로 지원 할 수 있다.

위에서 살펴 본바와 같이 많은 인증을 취득한 조직에게는 여러가지 효과를 가져오지만 대부분의 효과는 눈에 보이지 않기 때문에 정보보호관리체계 인증 제도를 통한 전통적인 비용/효과 분석방법으로 정당화하기는 매우 어렵지만 부가적으로 얻을 수 있는 무형이든 유형이든 것들을 가치로 환산하기란 쉽지 않다. 국내에서는 아직 이런 제도를 시행하지 않았기 때문에 실증적 효과를 분석하기가 매우 어려운 실정이나 영국에서 실시한 인증제도에 대하여 설문조사한 표 6, 7에서 보여 주는 것처럼 주요 자산을 보호하고 기업내의 정보보호관리 프레임워크 구축하고, 사업연속성을 보장해주며, 무역거래 당사자간의

안전성을 보장한다는 것을 알수 있다.

〔표 6〕 BS7799 인증의 이점

Protection of Business Information	40.5%
Internal Information Security Framework	34.6%
Business Continuity	14.9%
Safe Information Transfer to Trading Partners	10%

〔표 7〕 BS7799 인증의 추진 이유

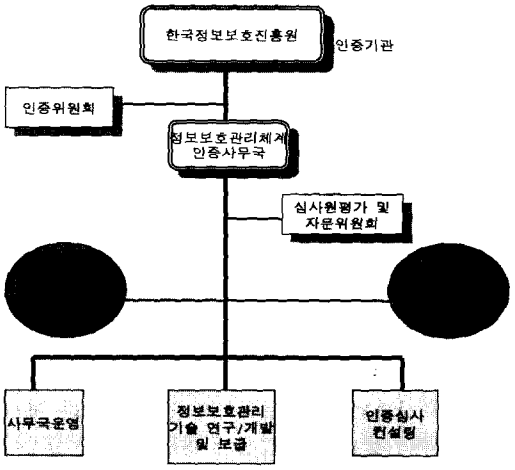
Business Practice	38.3%
Business Security	35.3%
Competitive Advantage	17.6%
Demand Customers	8.8%

Ⅳ. 국내 정보보호관리체계 인증 제도 추진 방안(안)

1. 정보보호관리체계 인증 제도란

조직의 자산에 대한 안전성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리·운영하고 정보보호 목표인 정보의 비밀성, 무결성, 가용성을 실현하기 위한 일련의 과정 및 활동을 정보보호관리체계라고 하며, 또한 기업(조직 또는 사업장의 일부 또는 전체)이 수립하여 운영하고 있는 이러한 정보보호관리체계가 일정한 인증심사기준에 적합한지 여부를 제3자인 인증기관이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도를 정보보호관리체계 인증제도라고 할 수 있다. 우리나라에서는 올 7월부터 시행 예정인 「정보통신망이용촉진및정보보호등에관한법률(안)」 제47조에 〔정보보호관리체계의 인증〕 이라는 법적 근거를 통하여 기술적·물리적 보호조치를 포함한 종합적 관리체계가 당해 서비스에 적합한지에 대하여 한국정보보호진흥원(현 센터)이 인증할 수 있도록 하고 있다.

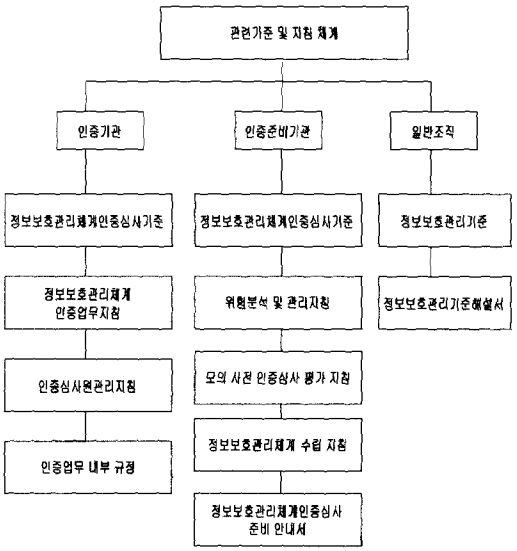
2. 정보보호관리체계인증 조직 구성(안)



〔그림 8〕 정보보호관리체계 조직 체계

3. 관련 기준 및 지침 개발 현황

정보보호관리체계인증과 관련된 기준 및 지침은 크게 인증기관, 인증준비기관, 일반조직에서 유용하게 사용할 것이다.



〔그림 8〕 인증심사관련 기준 및 지침 체계

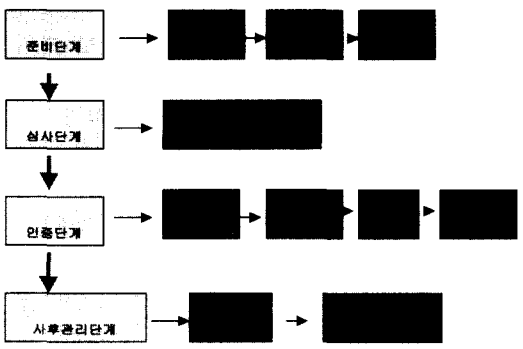
- 정보보호관리기준 : 일반조직에서 보안관리 모델로 활용할 수 있는 포괄적인 정보보호관리 지침
- 정보보호관리체계 인증심사기준 : 인증기관과 인증준비기관에서 정보보호관리체계 수립 및 인증심사용으로 활용
- 정보보호관리체계 인증업무지침 : 인증기관에서 인증심사 업무 지침으로 활용하며 인증 절차 및 방법, 수수료 등을 규정한 업무 지침서
- 인증심사원관리지침 : 인증기관에서 인증심사원의 양성 및 관리에 활용코자 개발한 규정
- 인증업무 내부 규칙: 인증심사업무에 관한 내부 규정을 담고 있는 인증기관용 내규 (심사원 윤리 강령 포함)
- 수수료산정기준 : 인증심사수수료를 결정하는 기준

4. 인증범위 및 대상

인증의 범위는 조직단위별, 지역별, 건물별 또는 조직 전체 등으로 구분하여 인증 받을 수 있다. 일반적으로 정보보호관리체계 수립 범위 내로 정할 수 있으며, 제품 및 서비스 등은 제외된다. 인증의 범위가 적절한 지에 대해서는 인증심사 준비단계에서 인증기관과 신청기관과의 협의에 의해 조절할 수 있다.

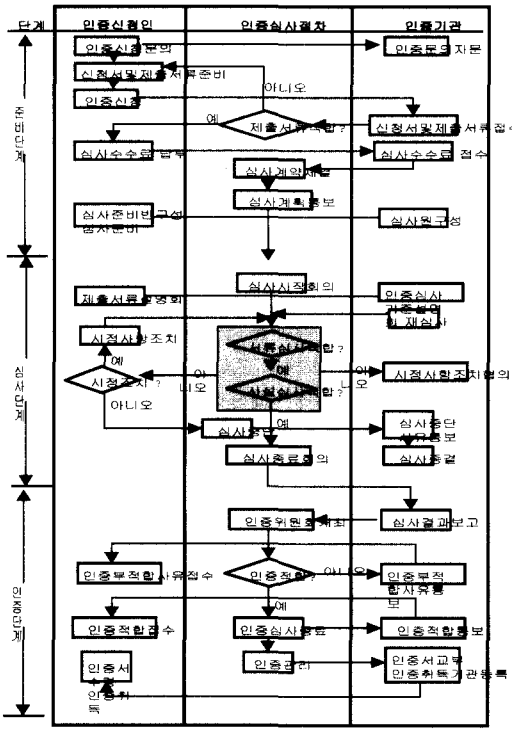
법률에서 정하는 인증의 대상은 정보통신망이용촉진및정보보호등에관한법률에 의한 정보통신서비스제공자 및 정보통신서비스를 제공하기 위한 물리적 시설을 제공하는 자로 한정하고 있으나 이는 포괄적 의미로 전기통신기본법에서 규정하고 있는 정보통신서비스 제공자를 모두 포함하고 있으며 구체적인 인증의 대상은 시행 세칙이나 업무지침에 명시할 계획이다.

5. 인증심사 절차 및 방법(안)



〔그림 9〕 정보보호관리체계 인증심사 단계

- 준비단계 : 인증신청서류 접수 및 계약이 이루어지고 인증심사계획이 통보된다.
- 심사단계 : 최초심사는 신청기관이 최초로 인증을 신청한 경우 행하는 심사이며 모든 심사는 서류심사와 사실심사로 이루어진다.
  - 서류심사 : 인증심사기준에 준한 관리체계 수립 및 이행 여부 확인을 위한 문서검토 단계로 정보보호정책, 위험분석자료, 범위, 생략된 부분 등 사실심사 전에 준비 상태를 점검한다.
  - 사실심사 : 현장실사로 정책, 절차, 목표들에 대한 효과성 검토와 서류심사에 대한 사실 확인 및 검증 작업 등이 포함된다.
- 인증단계 : 인증위원회의 인증심의·의결 과정으로 심사결과에 따라 인증서가 교부되며 인증심사가 종료된다.
- 사후관리단계 : 갱신심사는 인증취득 후 인증범위 등에 변경이 있는 경우나 인증 유효기간이 만료에 따른 재 인증을 받기 위하여 실시하며, 사후관리심사는 인증 취득 후 인증의 유지·관리 차원 및 유효 여부를 확인하기 위하여 주기적으로 실시된다.



〔그림 10〕 정보보호관리체계 인증 심사 절차

6. 정보보호관리체계 인증 준비

인증심사는 인증을 신청한 기관이 정보보호관리체계를 수립하고 구현하여 지속적인 유지·관리를 이행하고 있는지를 인증심사기준에 따라 확인하는 절차이다. 이를 위해서 인증을 받고자 준비하는 기관은 다음 4가지의 관리과정을 모두 수행하여야 하며, 통제사항 등에 대한 적용 방법을 자체적으로 결정하여 준수하여야 한다. 이를 위해 현재 자체적으로 준비를 하는 기관에서는 정보보호책임자를 임명하고 전담반을 구성 또는 외부의 전문가 (컨설팅)의 도움을 받아 구현할 수 있을 것이다.

- **정보보호관리체계 수립**

먼저 조직에 적합한 정보보호정책을 정의하여야 하며, 조직의 특성과 지리적 위치, 자산 및 기술 등을 고려하여 적용 범위를 설정하고, 적절한 위험 평가를 실시하여야 한다. 보증의 수준에따라 위험관리를 하여야 하며, 통제목적과 통제사항을 결정한다. 마지막으로 통제사항 결정 사유 등을 통제사항 적용 명세서로 문서화한다.

- **통제사항별 대책의 구현**

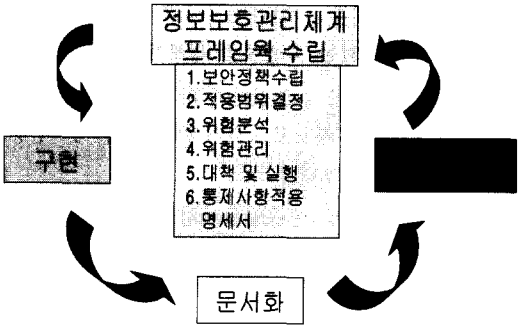
통제사항별로 적절한 대책을 실 환경에 적용하여 대상 자산을 보호하여야 한다. 이 때는 내부의 관련 자간에 충분한 의견수렴을 통하여 구현절차를 수립하여야 한다.

- **관리체계 수립과정의 문서화와 지속적인 변경관리를 통한 통제**

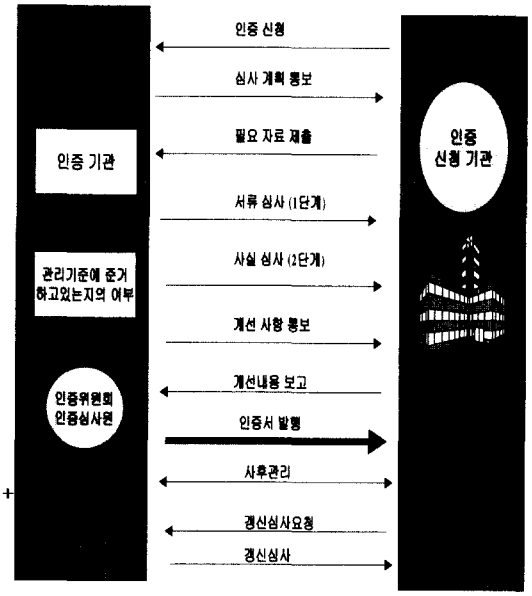
정보보호관리체계 활동을 문서화하여 관리하여야 하며, 위험분석 보고서를 포함한 관리체계 수립과 관련한 문서, 정보보호 메뉴얼, 정보보호관리체계 운영절차 및 절차별 책임과 관련한 문서들이 포함될 수 있으며 이들 문서는 접근 권한에 따라 관리하고, 조직의 필요에 따라 검토·관리되어야 한다.

- **운영상의 내용을 기록 및 유지관리**

정보보호관리체계 운영상에 발생되는 사항들은 기록하고 유지하여야 하며 여기에는 방문자 기록이나 감사기록, 접근인가 등이 포함될 수 있다.



〔그림 11〕 정보보호관리 과정



〔그림 12〕 정보보호관리체계 인증 프레임워크

7. 정보보호관리체계의 효과적인 수립·운영 방법

일반 조직에서 인증심사기준이나 내부 지침에 따라 정보보호관리체계을 수립하고 운영하게 될 때 접할 수 있는 어려움을 슬기롭게 대처할 수 있어야 정보보호관리체계의 지속적인 유지·관리를 통해 조직의 경영 목표를 달성 할 수 있는 것이다. 정보보호관리체계를 수립코자 하거나 수립하여 기 운영 중인 최고경영층이나 정보보호책임자 또는 모든 정보보호관리체계에서 정한 범위에 속하는 이용자들이 효과적으로 정보보호관리체계를 수립·운영하기 위한 고려 사항에 대하여 살펴보고자 한다.

- 조직이 정보보호관리체계 수립시에 사후 처리의 예방 중심에서 적극적으로 파악하여 대처하는 능동적 예방중심 정보보호관리체계로 구축해야 한다. 정보보호관리체계는 수동적으로 보안사고 등에 대하여 사후에 처리하는 수비적 시스템이 아니고, 능동적으로 파악하여 미리 대처하는 적극적 시스템이며, 보안사고후 투자비용은 실패 비용이고, 사전에 파악하여 처리하는 투자비용은 예방 비용이라 할 수 있다. 처음부터 올바른 정보보호관리체계를 수립하여 사후 비용을 줄임으로서 이윤극대화를 지향해 나가야 한다
- 정보보호관리체계 수립후 인증을 취득하고자 하는 목적이외부용 인증필요 수단에서 내부용 경영목적 달성수단으로 활용하여야 한다. 정보보호관리체계는 우선 내부 경영 목적을 달성하기 위한 수단으로 설계되고 적용되어야 한다. 내부 경영목적 달성 없이는 거래 당사자나 이용자에게 신뢰감이나 만족도 가 있을 수 없다.
- 정보보호관리체계를 수립 운영시에 일반 경영시스템에서 분리된 별도의 시스템이 아닌 일반 경영시스템과 통합된 일상적인 경영시스템으로 정착시켜야 그 효과를 높일 수 있다. 정보보호관리체계 요건은 기존의 경영시스템에 접목하여야 더 효과적이고 효율적이며, 일반 경영 시스템과 함께 생활화 습관화 될 때 정보보호관리체계가 목표하는 성과를 거둘 것이다.
- 정보보호관리체계를 단지 인증을 받기 위하여 인증심사기준에 따라 수립하는 방식을 지양하고 기업의 경영 목표에 준하게 설계 구현하여야 한다. 일반 경영시스템이 경영 목표라는 것에 기초하고 있는 것처럼 기업의 정보보호목표가 경영 목적을 달성하기 위하여 있다는 것도 잊어서는 안된다.
- 정보보호관리체계의 운영에 있어 단지 인증을 유지하기 위한 문서나 기록을 유지해서는 안되며 지속적인 문제점을 개선하고 실천하는 기회로 삼아야 한다. 정보보호관리체계에 대한 인증은 그 기업의 최고경영자가 신뢰할 만한 경영개선으로 이어져야 지속성을 확보할 수 있는 것이다.
- 위험분석을 통하여 통제사항의 선택시에 형식적인 대책보다는 효율과 효과적인 우선순위 방식으로 추진해야 한다. 위험분석을 통한 자산에 대한 가치와 중요도가 구분되고 요약되어 우선순위를 결정하고 추진하는 것이 정보보호관리체계 수립의 기본이며 다양한 대책을 나열하기 보다는 통제 방법을 하나로 통합하고 단순화하는 것이 효과적이고 효율적이다.
- 문서에 의존한 운영 방식보다는 기록 위주의 운영 방식이 정보보호관리체계의 능력을 향상시키는 방법이다. 정보보호관리체계의 수립·이행에 대한 문서의 양은 그 시스템의 능력을 저하시키는 핵심적인 요소로 작용 할 수 있다.
- 경제적인 관리 방식으로 추진해야 한다.
  정보보호관리체계를 단순화시키고 통합하여 효과적으로 운영할 때 시간, 노력, 비용도 줄여나갈 수 있는 것이다. 추가하고, 증가시키고, 덧붙여 보완해 가는 인식과 관행은 시스템의 특성에 적합하지 못한 것이다.
- 위험분석 및 위험평가 등을 통한 정량적인 관리 방식을 적극 활용하여 손실 가능성을 예측하고 현재의 정보보호관리체계 수준을 자체적으로 인식하여 지속적인 개선이 이루어지도록 해야 한다.

V. 국내 정보보호관리체계 인증 제도 향후 발전 방향

정보보호관리체계 인증 제도는 정보시스템에 대한 역기능을 예방하고 조직의 자산을 보호함으로써 비밀성, 무결성, 가용성을 확보하는 것을 기본목표로 하고 있다. 이 두 가지 목표는 조직의 경영목표 와 호환성을 유지해야 하며 나아가 효율적이고 효과적인 자산의 관리로 정보시스템의 안전성 및 신뢰성을 제고하기 위한 길잡이가 될 수 있다. 정보보호관리체계 인증 제도를 위해 필수적인 것으로 인증을 받기를 원하는 인증 준비 기관이나 인증심사원이 인증심사 수행 과정에서 준수해야 할 가장 기본적인 사항을 규정해 놓은 인증심사기준 및 인증심사지침 등 인증 준비에 필요한 기준이나 지침 등을 요소 기술별로 지속적으로 제정 보완 해 나 갈 예정이다. 또한 정보통신부장관이 고시하는 인증심사기준은 최근 급증하고 있는 정보보호컨설팅 수요와 함께 인증 수요의 요구사항을 반영하여 국제적인 규격에 준하도록 개발 완료 단계에 있으며, 인증심사의 객관성, 독립성 확보와 인증의 품질 향상을 위하여 필수적인 인증심사원 양성 방안에 대하여 기본 계획을 수립하고 양성 프로그램에 의한 교육을 실시할 예정이다.

여기에서는 정보통신 분야의 특급기술자 이상의 자격을 갖춘 지원자를 선발하여 수일간의 인증심사이론교육 및 실무교육를 실시한 후 각계 전문가로 구성된 심사원평가및자문위원회에서 심사를 거쳐 최종적으로 정보보호관리체계 인증 심사원 인정서를 수여하게 된다. 이를 통하여 인증을 받은 인증 취득기관에서는 전직원이 참여하는 실천적 정보보호관리체계의 방법을 제시할 것이며 정보보호에 대한 마인드와 인식 제고를 도와 줄 것입니다. 그러므로써 보안관리 역량의 개선 활동이 촉진되도록 할 것이며 무리한 투자, 중복, 낭비, 불합리 등에 대한 개선기회가 창출되도록 할 것이다. 전직원이 보안관리에 교육·훈련이 이루어지므로서 중점관리 할 자산 항목이 합리적으로 도출되고 보안관리체계의 수준 평가기법이 적용 가능하도록 해야 할 것이다. 국내에서 실시하게될 정보보호관리체계 인증 제도는 정보보호관리체계의 이행여부, 자산의 위험과 이에 대한 통제상태의 점검 및 정보보호관리체계의 수준을 평가하여 개선이 필요한 사항을 권고하는 방향으로 수행되야 한다. 이와 같이 어떤 시점을 중심으로 단속적으로 이루어지고 인증을 준비하기 위해 많은 인원이 참여해야하는 비효율적이고 요식행위의 인증보다는 지속적인 사후관리로 사후적인 성격에서 사전적 내지는 동시적인 것으로 추진해야 할 것이다.

Ⅵ. 결 론

국내에서 시행하게될 정보보호관리체계 인증 제도는 앞에서 해외 인증제도와 유사 인증 제도를 살펴본 바와 같이 국내 실정에 맞는 인증심사기준안을 만들고 수요자들이 쉽고 편하고 이해하기 쉽도록 각종 기준이나 지침을 개발 보급해 나갈 것이다. 또한 외국의 각종 관련 사례들을 분석하여 장단점을 보완하고 국제적 인증제도와 호환성을 유지하며 명실상부한 국가 인증제도로 정착시키고 현재 해외에서 시행되고 있는 보안관리 분야의 인증 제도의 단점을 보완하고 인증의 효과를 높일 수 있도록 지속적인 연구와 관련 기준이나 지침서 등의 개발 보급할 계획이다. 또한 피 인증기관들에게 유용한 국가인증제도로 활성화와 인증의 품질제고를 위해 필요한 기준, 지침 등의 연구가 또한 지속적으로 할 것이다. 인증을 준비하는 조직이나 기업들을 위하여 정보보호관리체계 수립 방법론을 제시하고 준비를 도와 줄 예정이며 인증 취득기관의 자산을 효과적으로 보호할 수 있도록 지속적으로 사후관리를 통하여 인증을 유지·관리토록 해야 할 것이다. 또한 변화하는 현실에 적극 대응하고 국제적인 인증제도로의 발전을 위해 인증심사원의 철저한 교육 및 훈련을 통해 양질의 인증서비스를 제공할 것이며 심사원의 자질향상과 보다 현실적인 인증심사에 대한 기준 및 지침의 마련을 위해 각각의 요소 기술별로 지침을 보완하고 통합해 나갈 것이다. 또한 정보보호관리체계 인증심사에 대한 효과를 극대화하기 위한 방안이 꾸준히 연구되어야 하며, 기업별로 정보보호관리체계의 수준을 평가하여 개선을 할 수 있는 평가 방법론의 개선도 적극적으로 이루어져야 한다. 이를 위해 금년도에 시행예정인 정보보호관리체계 인증 제도를 명실상부한 국가인증제도로 정착시키기 위해서는 철저한 준비와 수요기관들의 의견을 충분히 반영하여 인증의 효과성을 높이고 인증심사원에 대한 철저한 관리 프로그램 개발로 국내 일반 조직들이 정보보호관리체계에 대한 수준을 한 단계 높일 수 있도록 많은 노력을 다하여야 할 것이다.

참 고 문 헌

[1] NIST Technology Administration, An Introduction to Computer Security: The NIST Handbook, NIST USA 1998

[2] ISO/IEC TR 13335, Information Technology-Guidelines for the Management of IT Security, ISO/IEC, 1996

[3] Information Systems Audit and Control Association, COBIT-Governance, Control and Audit for Information and Related Technology, ISACA International, 1999

[4] Information System Audit and Control Association, Certified Information Systems Auditor Review Technical Information Manual, ISACA International, 1999

[5] S. Rao Vallabhanen:, CISSP Examination Textbooks-Volumel Theory, SRV Professional Publications I1, 2000

[6] 한국정보보호센터, 정보보호표준교재, 정보보호센터, 1999

[7] 한국정보보호센터, 컴퓨터 보안 입문, 정보보호센터, 1999

[8] 한국정보보호센터, 2000정보시스템 해킹, 바이

러스 현황 및 대응, 2000
[9] 한국정보보호센터, 정보보호 평가 기준개발, 1999
[10] 한국전산원, 전삼감리 효과 연구, 전산원, 1995
[11] 한국정보통신진흥협회, 인터넷모범상점인증제도 연구보고서, 1999
[12] 교우사, 정보보호개론, 정보보호센터, 1999
[13] 한국정보보호센터, 정보보호평가체계, 한국정보보호센터, 1997
[14] 정보통신부, 정보통신망이용촉진및정보보호등에관한법률, 2000.
[15] 한국정보보호센터, 정보보호관리기준(안), 2001
[16] BSI(U.K.), BS 7799 part1 : Information Security Management - Code of Practice for Information Security Management, 1999
[17] BSI(U.K.), BS 7799 part2 : Specification for Information Security Management SYstemss, 1999
[18] http://www.iso17799software.com/presentation/index.htm
[19] http://www.iso.ch/iso/en/ISOOnline.frontpage
[20] http://www.ukas.org/
[21] http://www.trusecure.co.kr/
[22] http://www.bsi-global.com/Information+Security/04_Standards_infosec/index.xhtml
[23] http://athena.fit.qut.edu.au/security/as4444.htm
[24] http://www.kab.or.kr/index_k.html
[25] http://www.isoeasy.org/

〈著者紹介〉

장 상 수 (Sangsoo Jang) 정회원
1989년 2월 : 한국항공대학교 정보통신공학과 졸업(학사)
2000년 8월 : 동국대학교 정보보호학과 석사과정
1989년 ~ 2000년 : 대한항공 정보시스템실 과장 네트워크 설계 및 네트워크 보안 담당
2000년 ~ 현재 : 한국정보보호센터 선임연구원, 과제책임자
관심분야 : 네트워크보안, 정보보호관리

김 학 범(Hakbeom Kim) 종신회원
1990년 8월 : 중앙대학교 전자계산학과 졸업(석사)
2001년 2월 : 아주대학교 컴퓨터공학과 졸업(박사)
1991년 10월 ~ 1996년 6월 : 한국전산원 주임연구원
1996년 7월 ~ 현재 : 한국정보보호센터 기술표준팀장
2000년 1월 ~ 현재 : TTA 시스템보안 연구반 의장
2000년 1월 ~ 현재 : TTA 정보보호 기술위원회 간사
2000년 6월 ~ 현재 : 인터넷보안기술포럼 간사
관심분야 : 정보보호 표준화, 정보보호 관리, 컴퓨터·네트워크 보안, 접근통제

이 홍 섭(Hongsub Lee) 종신회원
1979년 : 한양대학교 전자공학과 졸업(학사)
1985년 : 한양대학교 전자공학과 졸업(석사)
1999년 : 대전대학교 컴퓨터공학과 졸업(박사)
1980년 ~ 1996년 : 한국전자통신연구원, 연구원 책임연구원, 실장
1996년 ~ 현재 : 한국정보보호센터 기술부장
1996년 ~ 현재 : 한국통신정보보호학회 상임이사
1997년 ~ 현재 : 정보통신기술협회 정보보호기술위원회 의장
2000년 : NETSEC-KR 행사 조직위원장
2000년 ~ 현재 : 전자거래분쟁조정위원회 조정위원(산자부), 금융분쟁조정위원회 조정위원(금감원), 개인정보분쟁조정위원회 조정위원(정통부), 인터넷보안기술포럼 초대 의장, 한국ASP인증위원회 인증위원
2001년 ~ 현재 : 인터넷사이트 안전마크위원회 위원, 대한전자공학회 회지편집위원회 위원, 국가과학기술표준분류전문위원회 위원, 사이버범죄 민간자문위원회 위원(서울지방경찰청)
관심분야 : 정보보호 관리, 정보보호기술 표준화, PKI, 시스템 및 네트워크 보안 등