情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

국내 · 외 정보보호관리 모델에 관한 고찰

이 강 신*, 김 학 범*, 이 홍 섭*

요 약

정보화의 급진전에 따라 역기능의 문제도 대폭적으로 증가되고 있는 추세 속에서 이를 극복하고정보화의 급진전에 따라 역기능의 문제도 대폭적으로 증가되고 있는 추세 속에서 이를 극복하고자 하는 노력이 국제적으로 활발하게 전개되고 있다. 보다 체계적이고 비용 효과성을 고려하여 미국, 유럽, 호주 등 많은 선진국가에서는 지난 수년동안 정보를 보호하는 기준이나 지침 등을 학계, 산업계, 연구기관, 정부기관과 공동 또는 자체적으로 개발하여 활용하고 있거나 활용 예정에 있다. 국내에서도 이러한 접근 방식의 중요성을 인식하고 정보통신망이용촉진및정보보호등에관한법률을 개정하여 정보보호관리체계에 대한 인증 제도를 2001년 7월 1일부터 시행하기에 이르렀다.

이에 따라 국내에서도 동 법에 근거하여 인증업무를 수행하게 될 한국정보보호센터에서 국내의 현실에 맞는 정보보호관리기준 마련 작업을 1년여 동안 추진하여 왔으며, 각고의 노력을 기울이고 있는 상태이다. 이에 따라 본 고에서는 정보보호관리체계에 대한 구체적인 소개와 더불어 각 국에서 노력을 기울이고 있는 정보보호 관리를 위해 마련하여 온 지침과 절차 및 기준 등의 내용을 소개하고, 각각이 가지고 있는 특성들을 프레임워크 수준에서 살펴보기로 하며, 제시하고 있는 통제사항들을 간략하게 비교함으로써 정보보호관리체계의 수립과 인증 제도의 효과성에 대하여 많은 관련자들의 인식을 제고하고자 한다.

그리고, 향후 정보보호관리체계 수립 및 인증제도의 도입과 운용이 활발하게 이루어지고 활성화될 경우를 미리 준비하기 위하여 정보보호관리를 위한 성숙도의 측정에 대한 연구 방향을 나름대로 제시하고자 한다.

Ⅰ. 서 론

정보화의 거센 물결은 전 지구촌에 새로운 문화적인 충격을 주고 있다. 많은 국가들은 정보화가 국가 생존의 가장 강력한 수단이라는 공통적인 생각을 가지고 앞다투어 이를 자국의 경쟁 수단으로 채택하여 활용하는 노력을 적극적으로 전개하고 있다. 산업사회에서도 그러하였듯이 정보화 사회에서는 사이버 상에서 범죄가 정보화의 속도와 규모에 비례하여 사회문제로 나타나고 있으며, 이를 방어하고 예방하기 위한 노력도 다양한 형태로 전개되고 있다.

산업화에 늦어 많은 어려움을 겪어야 했던 우리나라의 경우는 정보화에는 가장 앞선 나라가 되기 위하여 정부 및 민간차원에서 많은 노력을 하여 왔고, 그로 인하여 지금은 인터넷 인구가 2,000만(2001. 3 기준)이 넘고 정보화의 성장률도 가장 높은 나라가 되는 개가를 이룩하게 되었다.

그러나, 서구의 합리적인 사고방식에 비하여 국내의 경우는 그에 미치지 못하고 있는 것이 현실이다. 정보화의 역기능을 체계적으로 방지하거나 대응하는 방법을 도입하기 위하여 선진 각 국에서는 부단한 노력을 기울이고 있다. 정보보호관리를 위한 모델이나 기본 틀을 제시하는 것이 바로 이러한 예들이라고 할 것이다.

먼저, 이러한 노력들을 살펴보면 크게 전사적 차원에서 접근하는 방식과 IT를 기초로 접근하는 방식으로 분리할 수 있다. 우선, 전사적 차원에서 접근하는 방식은 국내의 정보보호관리지침과 영국의 표준기구인 BSI(British Standard Institute)가 제정한 BS 7799이며, 나머지는 대부분이 IT를 기반으로 하여 접근하고 있다. 그리고 SSE-CMM (System Security Engineering - Capability Maturity Model)은 정보보호관리 수준에 대한 성숙도를 측정할 수 있도록 모델을 제시하고 있어 타

* 한국정보보호센터(kslee@kisa.or.kr, hbkim@kisa.or.kr, hslee@kisa.or.kr)

관리방식과는 차별화 되어 있다고 하겠다.

본 고에서는 바로 이러한 체계적인 정보보호관리를 위한 노력들을 국내 및 국외로 나누어 소개하며, 비교 및 분석하고 향후 발전 방향을 제시하면서 끝을 맺고자 한다.

Ⅱ. 국내의 정보보호관리기준

국내에서는 정보를 보호하기 위한 체계적 관리의 중요성을 인식하여 국가 차원의 대응을 하고 있다. 정보통신이용촉진및정보보호등에관한법률에 정보보호관리체계인증(제47조) 시행을 추가하는 등 정보보호를 강화하는 방향으로 개정하여 2001년 7월 1일 시행을 앞두고 있다. 이에 따라 정보보호관리를 희망하는 조직 또는 기관들이 관리체계를 수립할 경우 참고로 활용할 수 있도록 한국정보보호센터에서는 정보보호관리기준을 작성하고 있다.

정보보호관리기준의 기본적인 사상은 정보기술이 아닌 조직이나 환경 측면에서의 관리적 방식을 기초로 하였다는 것이다. 이는 전 세계적으로 발생되고 있는 각종 해킹 등의 발생 건수들을 분석하여 보면 알 수 있듯이 실제 네트워크에 침투하여 컴퓨터시스템에 저장되어 있는 정보 등 자산을 악의적인 목적으로 접근하여 피해를 발생시키는 사례는 전체 정보보호 관련 문제 발생 유형 중 매우 작은 부분이라고 할 수 있을 것이다. 대부분은 내부자의 소행이거나 조직적 관리의 소홀함으로부터 기인하고 있기 때문이다.

다음은 범용성을 고려하였다. 많은 조직 또는 기관들은 다양한 형태의 환경과 관리방식 그리고 비즈니스 모델을 가지고 있다. 이러한 다양한 환경에 전체적으로 적용할 수 있는 것은 단지 IT 관점에서가 아닌 종합적인 차원에서 접근되어야 하고 본 지침을 활용하여 누구나 정보보호관리체계를 수립할 수 있어야 하는 것이다. 따라서 조직과 조직이 보유하고 있는 업무의 특수성 등을 모두 고려하여 적절하게 보완하여 활용할 수 있도록 작성하였다.

그리고 국내 실정을 최대한 반영하기 위하여 노력하였다. 본 지침은 BS 7799의 내용을 기본으로 하였으나 문서의 작성 작업을 상당부분 줄였으며, 정보보호관리체계의 도입단계라는 점을 고려하여 관련자들에 대한 인식의 확산을 위한 교육과 훈련 내용을 보강하였다. 또한 보안사고가 발생할 경우 신속한 보고 및 대응에 대한 내용을 새로운 분야로 추가하기도 하였다.

본 기준은 기본 틀로 4개의 과정을 거치도록 하였다. 4개의 과정이란 1단계 정보보호관리체계(framework) 수립, 2단계 통제사항별 대책의 구현, 3단계 문서관리(변경관리 포함), 4단계 운영상의 내용을 기록 및 유지관리이며, 본 과정을 거치면서 구현할 통제 대책을 13개 분야에 걸쳐 131개로 구성하였다.

1단계인 정보보호관리체계수립에서는 정보보호관리를 위한 전체적인 틀을 제시하고 있는데, 첫 번째로, 조직이 선택하는 정보보호관리 방향을 제시하기 위한 상위개념의 정보보호정책을 수립하는 것이다. 두 번째로, 결정된 정보보호정책에 기초하여 보호할 대상 범위를 조직, 위치, 자산, 기술의 특성을 고려하여 결정하는 것이다. 범위의 개념이란 업무프로세스 단위가 될 수도 있으며, 물리적 경계일 수도 있다. 또한, 기관이 다르다고 하여도 업무간 또는 물리적으로 상호 연계성 등이 있을 경우에는 이들을 하나의 범위로 결정할 수도 있다. 세 번째, 범위 내에 있는 자산들에 대하여 위험분석을 실시하는 것이다. 위험분석을 위하여 결정된 범위 내의 정보자산 등을 모두 조사하고 이들의 업무 프로세스 상에서의 가치를 결정하며, 각 자산들에 대한 위협을 열거하고, 위협이 발생될 수 있는 취약점을 점검하게 된다. 취약점을 점검한 후 취약점으로 인해 발생될 수 있는 위험을 측정하게 된다. 네 번째는 위험관리단계로, 위험을 측정한 결과는 조직에서 채택한 정보보호정책에 근거하여 조직이 보유하고 있는 예산, 현실성 등을 고려하여 조직에서 받아들이기 어려운 통제사항과 미치는 영향이 비용효과성 측면에서 무시하여도 되는 통제사항으로 분리한다. 통제사항을 구현하여야 하는 이러한 위험들의 집합을 위험영역(risk domain)이라고 한다. 그리고 위험영역 내의 위험에 대해서는 총 131개의 통제사항 중에서 대상을 선정하는 작업을 하게 된다. 물론 필요하다면 131개 이외의 통제사항도 추가할 수 있다. 그리고 위협 또는 취약점의 신규 추가 등 변화가 있을 경우에도 이에 대한 지속적인 위험의 관리를 한다. 다섯 번째는, 이러한 선택과 무관하게 통제사항을 선택한 사유를 함께 기록하는 통제사항적용명세서(statement

of Applicability)를 작성하여 관리한다.

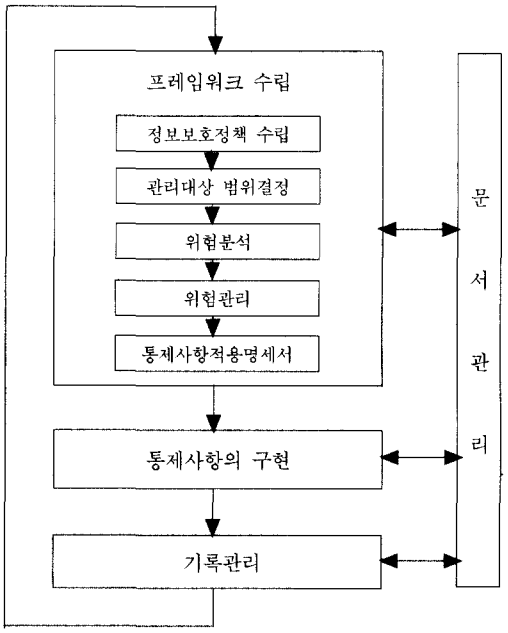
2단계인 통제사항의 구현은 선택한 통제사항을 실 환경에 적용하는 것으로 조직적인 측면 뿐만 아니라 기술적인 측면까지 세부적으로 실 환경에 구현하는 것이다. 내부의 관련자간에 충분한 의견 수렴을 통하여 구현 절차를 마련하여 이에 따라 절차적 구현을 한다. 가령, 교육을 실시하고 정보보호를 위한 조직을 만들어야 한다는 통제사항을 선택하였을 경우 정보보호를 위한 조직을 위원장에 CEO 또는 CIO로 하고, 위원들은 부서장으로 하는 조직을 설치할 수 있을 것이다. 그리고 임직원들에 대하여 주기적 또는 수시로 교육 정책에 따라 교육을 실시하는 것을 하나의 예로 들 수 있다.

3단계인 문서관리에서는 조직의 정책 또는 통제사항을 구현하는 과정에서 필요하다고 인정한 사항에 대하여 문서를 작성하도록 하며, 운영과정에서 발생된 변화를 실시간으로 운영환경에 반영하여 문서화를 하는 것이다. 각각의 부서에서는 부여된 보안 수준을 고려하여 접근통제를 하여야 한다. 문서가 더 이상 사용 필요성이 없을 때에는 자체적으로 정한 절차에 따라 신속하게 폐지하도록 하여야 하며, 보존 대상이 되는 문서는 신속한 절차를 거쳐 보존할 수 있도록 하여야 한다.

4단계인 운영상의 내용 기록 및 유지관리는 통제사항을 구현한 이후 지속적인 운영을 하면서 발생된 각각의 기록을 유지하는 것이다. 컴퓨터시스템의 경우는 이를 위해서 로그 증적을 운영할 수도 있다. 그래서 주기적 또는 필요시 수시로 기록된 내용에 대한 검토를 실시하여 반영할 사항이 있으면 반영하도록 하며, 조직의 정보보호 정책의 변경, 범위의 변경이나, 받아들이기 어려운 위험영역에서 위협이 발생된 경우 이에 대한 보완을 하도록 한다.

본 기준은 프레임워크 수립, 통제사항의 구현, 기록관리, 문서관리라는 4개의 과정으로 구성되어 있으며 그림 1과 같다

그리고 정보보호관리 과정에서 선택하여 적용할 수 있는 13개의 통제분야란 정보보호정책, 정보보호조직, 아웃소싱및제3자접근, 자산분류와 통제, 인적보안, 교육 및 훈련, 접근통제, 물리적보호, 운영관리, 개발보안, 업무연속성관리, 보안사고대응 및 복구, 요구사항준수이다. 분야별 통제사항들의 분포는 표 1과 같다.



〔그림 1〕 정보보호관리 과정

〔표 1〕 통제사항 분야별 통제사항

번호	통제분야	통제대책 수
1	정보보호정책	6
2	정보보호조직	5
3	아웃소싱및제3자접근	5
4	자산분류와 통제	3
5	인적보안	8
6	교육 및 훈련	5
7	접근통제	29
8	물리적보호	13
9	운영관리	21
10	개발보안	17
11	업무연속성관리	6
12	보안사고대응 및 복구	7
13	요구사항준수	6
합 계		131

정보보호정책분야는 정보보호에 대한 관리방향과 지원에 대한 사항을 주로 다루고 있다. 조직전반에 대한 정보보호관리 방향을 제시하는 상위개념에서 정책을 수립하여 최고관리층이 이를 승인함은 물론 모든 임직원들이 이를 이해하고 있어야 한다.

정보보호조직 분야는 정보보호를 위한 구체적인 실천과 유지관리를 위하여 조직 내부에서 운영하여야 할 조직의 구조를 의미한다. 정보보호조직은 조

직간 또는 부서간 의견조율과 상호 협력을 위하여 상위관리자로 구성하는 방법이 있고, 실무적인 사항에 대한 협력을 위해서는 실무책임자급 중심으로 구성할 수도 있으며, 이를 병행할 수도 있다. 다만, 조직의 규모와 보호하여야 할 규모 및 범위에 따라 탄력적으로 운영할 수 있다.

아웃소싱및제3자접근 분야는 조직 내의 업무 등에 관하여 제 3자가 접근할 경우 또는 업무를 위탁하여 관리할 경우 조직의 업무 등에 대한 보안사항을 지켜야 할 의무사항으로 다루고 있다. 위탁 또는 제3자의 출입 또는 업무의 수행에 있어서 계약서를 작성할 경우에는 정보의 보호를 위한 방침, 의무사항 등을 포함하도록 하고 있다.

자산분류와 통제 분야는 정보보호관리를 위한 위험분석 과정에서 대상 통제사항들을 중심으로 다루고 있다. 조직이 소유하거나 관련되어 있는 정보자산 등에 대하여 이에 대한 전반적인 현황을 파악하고 책임자를 지정하며, 이에 대한 보안수준을 정의 및 관리하는 사항들을 서술하고 있다.

인적보안 분야는 조직의 내부 직원과 조직에 업무상 또는 기타 관련사항으로 출입할 경우와 직원을 신규로 채용, 근무, 퇴직 시에 정보의 보호를 위하여 준수하여야 할 사항 등을 기술하고 있으며, 제3자의 경우라도 출입 시에 지켜야 할 사항들을 기술하고 있다. 채용 시에는 신용의 조회와 정보보호의 의무에 대한 서약 등이 있으며, 근무중인 직원이 조직의 정보보호 정책에 따라 준수하여야 할 사항, 그리고 관리자는 이들에 대한 감시를 하는 것을 주요 내용으로 하고 있다.

교육 및 훈련 분야는 임직원들에 대하여 정보보호를 위한 정책 및 지침 등을 준수하도록 하는 업무의 절차, 책임성 등을 포함하며, 기본적으로 정기적인 교육을 실시하되 필요시 중대 사안 등이 발생될 경우 수시로 시행할 수 있다는 내용을 담고 있다.

접근통제 분야는 가장 많은 비중을 두어 다루고 있는 분야이다. 결국, 대부분의 정보보호를 위한 활동은 접근에 대한 통제에서 비롯되기 때문이다. 접근통제의 주요분야로는 접근통제를 위한 상위 또는 상세 수준의 정책, 시스템에 접근할 경우 적절한 사용자인지를 인증하는 사용자에 대한 식별과 인증, 내부 또는 외부와의 시스템간에 연계되어 있어 네트웍을 통하여 접근할 경우 연결노드, 접속 포트, 네트워크의 논리적 및 물리적 분리 등 네트워크 서비스 제공 시에 발생될 수 있는 정보의 오용 및 유출 등을 방지하기 위한 네트워크에 대한 접근통제, 최종적으로 정보의 보호를 담당하고 있는 시스템의 운영체제에 대한 로그온 절차, 패스워드 관리, 시스템 유틸리티의 보안 준거성 등을 다루는 운영체제에 대한 접근통제, 각종 트로이목마나 은닉채널 등의 문제를 방지하기 위한 응용프로그램 접근통제, 접근통제 메커니즘을 적용한 후 적절하게 보안이 유지되고 있는지를 지속적으로 점검하는 접근 및 사용에 대한 모니터링, 점차적으로 정보의 흐름이 개인화와 이동성을 갖추고 있는 점을 고려하여 원격으로 조직의 정보에 접근하는 경우 이에 대한 통제 방법을 서술하고 있는 이동컴퓨팅 및 원격작업으로 분류하여 다루고 있다.

물리적 보호 분야는 주로 건물, 사무실, 전산실 등 물리적으로 분리되어 있는 곳에 대한 통제사항을 다루고 있다. 정보의 보호를 위하여 제한구역의 설치, 제3자의 방문에 대응하기 위한 접견실의 별도 운영, 정보자산의 적재와 하역 장소의 통제 등을 들 수 있으며, 전산실에 대한 출입통제, 장비의 보호, 전력선의 보호, 항온·항습 유지 등을 다루고 있다.

운영관리 분야는, 운영 전반에 대한 절차 등을 문서화하고 관련자들이 알 수 있도록 하는 운영절차와 책임, 시스템의 도입 및 이를 인수하는데 있어서 적용하여야 할 사항을 서술하고 있는 시스템 도입계획 및 인수, 시스템의 안정적인 운영을 위한 성능 및 용량에 대한 지속적인 측정을 통하여 관리하는 성능 및 용량관리, 악성소프트웨어의 탐지 및 예방을 위한 악성소프트웨어 통제, 정보 및 데이터의 백업 및 장애관리를 위한 관리, 데이터 및 정보를 저장하는 매체 및 시스템 문서의 관리, 네트워크를 이용하여 정보의 전달 등을 안전하게 관리할 수 있도록 하는 정보와 소프트웨어 교환 시 보안관리 등으로 구성되어 있다.

개발보안 분야는 응용시스템의 개발에 따른 생명주기 단계별로 보안을 위한 활동을 기술하였다. 소프트웨어의 생명주기에 대하여 권고하는 국제표준인 ISO/IEC 12207에 따라 개발단계에서 정보보호를 위한 정책 및 메커니즘 등을 적용하고 확인하는 것이 비용 효과성이 매우 높기 때문에 이에 대한 사항도 비중 있게 다루고 있다.

업무연속성관리 분야는 인공 또는 자연재해로부터 위협에 대하여 최소한의 업무 수행이 지속될 수 있도록 하기 위한 절차를 마련하고 이를 시험하며 지속적인 갱신을 하도록 하기 위한 사항들을 기술하였다.

보안사고대응 및 복구 분야는 외부 또는 내부 침입자가 악의적인 침입 등으로 각종 정보를 오용하거나

남용하는 행위에 대하여 대응 절차를 수립·준수하고 신속히 보고하여 업무에 중대한 지장을 주지 않도록 즉각적 조치사항들을 기술하였다. 또한, 업무의 조직간 또는 부서간 연계성 등을 고려하여 상호 협의 또는 조정할 수 있는 통제사항들도 기술하였다.

끝으로, 요구사항준수 분야는 법·제도적인 측면에서 이를 준수할 수 있도록 하는 사항을 다루고 있으며, 조직에서 설정한 정보보호정책, 표준, 절차 등에 대해서도 이를 준수하여야 한다는 사항들을 기술하였다.

Ⅲ. 국외의 정보보호관리기준

1. BS 7799

BS 7799는 영국의 BSI(British Standard Institute)의 DISC에서 운영하는 위원회 BDD/2에서 주도하여 개발한 것으로, 2부(part1, part2)로 구성되어 있다.

1부 : Code of practice for information security management
2부 : Specification for information security management systems

이 중 1부는 조직에서 정보보호관리체계를 수립하기 위한 지침으로 활용하게 하는데 목적이 있고, 2부에서는 정보보호관리체계의 규격(specification)을 제시하는 것으로 인증심사시 활용하는데 목적이 있다. 현재 1부는 "ISO/IEC 17799 part1"으로 2000년 12월에 국제표준으로 채택된 상태이나, 2부는 영국 국가표준으로 남아있는 상태이다.

1부에는 프레임워크를 제시하지 않음으로써 활용하는 조직에서 결정하도록 하고 있다. 다만, 2부에서 프레임워크를 제안하여 놓은 상태여서 BS7799를 수용하는 대부분의 기관에서는 이 프레임워크를 따르고 있다.

기본적으로 두 문서 공히 정보보호관리를 위하여 IT 차원이 아닌 전사적 차원에서 접근하고 있다는 사실이다. 즉, 정보의 보호는 단지 정보자원을 통해서가 아니라 전사적인 차원에서 관리하는 것이 더 중요하다는 기본적인 사상을 내포하고 있다.

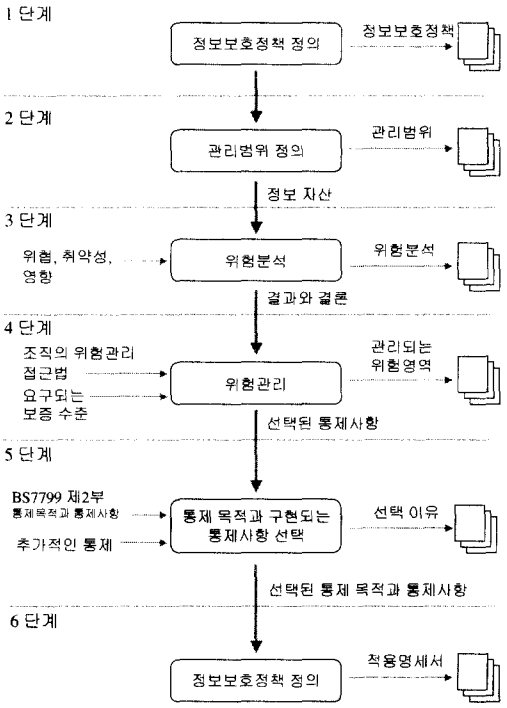
BS7799는 1995년에 처음 제정되어 1999년에 개정되었으며, 영국 이외에 호주, 브라질, 네덜란드, 뉴질랜드, 노르웨이 등에서 사용하고 있다. 영국 정부에서는 전자정부를 향한 노력을 뒷받침하기 위하여 2001년 3월까지 대부분의 정보시스템에 대하여 BS7799 인증을 받도록 하여 국가 핵심 정보 기반 구조를 보호하기 위한 수단으로 활용하고 있다.

BS7799 제1부는 10개의 주요 분야로 나누어진 127개의 통제사항으로 구성되어 있으며, 현재 사용되고 있는 최선의 정보보안 실무(Best Practice)들로 구성된 종합적인 통제사항 목록을 제공하고 있다. 아래의 표 2는 이들에 대한 구성 현황을 보여주고 있다.

〔표 2〕 BS7799의 분야별 통제사항 현황

분야	세부 분야	통제사항 갯수
보호정책	정보보호정책	2
보호조직	정보보호 기반구조	7
	제3자 접근 보호	2
	위탁	1
자산분류와 통제	자산의 책임성	1
	정보 분류	2
인적보안	직무 정의와 고용 보안	4
	사용자 훈련	1
	사고 대응	5
물리적 및 환경적 보안	보안 영역	5
	장비 보호	6
	일반통제	2
통신과 운영관리	운영 절차와 책임	6
	시스템 계획과 수락	2
	악성 소프트웨어 보호	1
	시스템 운영	3
	네트워크 관리	1
	매체 처리와 보호	4
	데이터와 소프트웨어 교환	7
접근통제	접근통제에 대한 업무 요구사항	1
	사용자 접근 관리	4
	사용자 책임	2
	네트워크 접근 통제	9
	운영시스템 접근 통제	8
	애플리케이션 접근 통제	2
	시스템 접근과 사용 감시	3
	이동통신과 텔레워킹	2
시스템개발 및 유지보수	시스템 보호 요구사항	1
	응용 시스템 보호	4
	암호통제	5
	시스템화일 보호	3
	개발과 지원 공정 보안	5
업무연속성계획	업무연속성관리 측면	5
준수	법적 요구사항 준수	7
	보호정책의 검토와 기술적 준수	2
	시스템 감사 고려사항	2

제2부에서는 정보보호관리체계를 구축하는 절차를 제시하며, 〈그림 2〉와 같이 여섯 단계로 구성된다. BS7799에서는 위험관리의 중요성을 강조하며, 제1부에 수록된 모든 통제사항들을 구현할 필요는 없다는 점을 명확히 강조하고 있다.



〔그림 2〕 BS7799 적용 단계

먼저, 모든 정보 자산과 조직에 있어서 그들의 가치를 분석하고, 어떤 정보가 왜 중요한지를 식별하는 정책을 수립하도록 한다. 2단계에서는 낮은 가치를 가진 정보를 제외하여 관리 대상의 범위를 정의한다. 다음으로, 가치를 상실하는데 따른 위험을 분석하며, 그 위험을 어떻게 관리할지를 결정한다. 여기에는 물리적, 인적, 절차적인 측면을 고려하여야 하며, 효과적인 업무연속성계획의 개발도 포함한다. 그 다음 단계는 위험을 관리하기 위한 통제사항을 선정한다. BS7799에는 이러한 통제사항이 열거되어 있다. 그러나 BS7799의 목록은 완전한 것이 아니므로, 원하는 경우에는 통제사항을 추가 또는 삭제하여 사용할 수 있다.

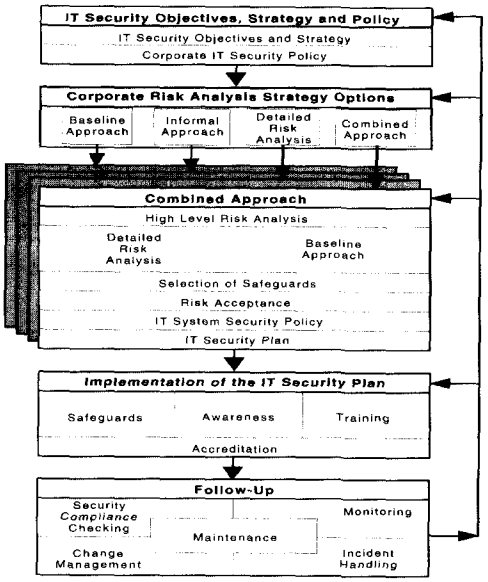
2. GMITS

정보보호관리를 위한 표준으로 ISO/IEC 13335, "Guidelines for the Management of IT Security(GMITS)"는 5부로 구성되어 있다. BS 7799가 전사적 차원의 보호를 위해 출발한 반면 GMITS은 기본적으로 IT 보호 관점에서 다루고 있다. 즉, GMITS은 조직이 보유하고 있는 정보자산이 주요 대상이라고 할 수 있다.

GMITS의 1부에서는 정보보호관리를 서술하기 위하여 기본 개념과 모델들에 대하여 개략적으로 소개하고 있으며, 2부에서는 관리와 계획의 관점에서 동 모델 등에 대하여 기술하고 있다. 3부에서는 IT 보호관리에 대한 전체 과정을 제시하고 이에 대한 기술적인 설명을 하고 있다. 4부에서는 통제사항을 설명하고 보안요구사항과 조직의 특정 환경에 따라 통제사항을 선정하는 과정을 기술하고 있다. 5부에서는 인터넷과 같은 외부 네트워크와 연결된 상황에서의 통제사항을 선정하는 방법을 기술하고 있으나 아직 표준화 작업을 진행 중에 있어 계속 관심을 가져야 할 사항이다.

ISO/IEC TR 13335-1 : Information Technology - Concepts and Models of IT Security (1996-12-15)
ISO/IEC TR 13335-2 : Information Technology - Managing and Planning IT Security (1997-12-15)
ISO/IEC TR 13335-3 : Information Technology - Techniques for the Management of IT Security (1998-06-15)
ISO/IEC TR 13335-4 : Information Technology - Selection of Safeguards (2000-03-01)
ISO/IEC PDTR 13335-5 : Information Technology - Safeguards for external connections

GMITS의 정보기술 보호관리의 모델은 목적과 전략 및 정책을 수립하고 위험분석을 실시한 후 정보기술 보호계획을 수립한 다음 구현을 하며, 구현 후에는 철저한 사후관리를 실시하는 것이 주요 골자이다. 이러한 과정에 대하여 GMITS 3부에서 IT 보호를 위한 관리 틀을 그림 3과 같이 제시하고 있다.



〔그림 3〕 IT 보호 관리를 위한 기본 틀

통제사항을 선택하는 가장 중요한 과정중의 하나인 위험분석(Risk Analysis) 방법을 타 정보보호관리 관련 지침이나 기준 등과 다르게 Baseline Approach, Informal Approach, Detailed Approach, Combined Approach 4가지로 제시하고 있다. 그리고 위험분석의 방법에 따라 통제사항을 선택하는 방법도 각각 상이하게 제시하고 있다. 제시하고 있는 통제사항은 조직적 및 물리적 분야에서 7개의 세부 분야에 걸쳐 40개, IT 시스템 분야에서 5개 세부 분야에 걸쳐 23개를 합하여 63개로 구성되어 있다.

〔표 3〕 GMITS의 통제사항 현황

구 분	세부분야	통제사항 갯수
조직적 및 물리적 통제사항 (40개)	IT Security Management and Policy	7
	Security Compliance Checking	2
	Incident Handling	4
	Personnel	4
	Operational Issues	12
	Business Continuity Planning	4
	Physical Security	7
IT 시스템 중심의 통제사항 (23개)	Identification and Authentication (I&A)	3
	Logical Access Control and Audit	5
	Protection against Malicious Code	4
	Network Management	6
	Cryptography	5

그리고 이러한 통제사항을 선택하는 3가지 방식은 다음과 같다.

첫 번째는 IT 시스템 타입별로 접근하여 통제사항을 선택하는 방법(Baseline Approach : Selection of Safeguards according to the Type System)으로, 워크스테이션, 서버, 응용프로그램 등 유사 유형으로 분류하여 주제별로 통제사항을 선택하여 이를 구현하는 방법이다.

두 번째는 위협에 따른 접근방법(Selection of Safeguards according to Security Concerns and Threats)으로 비밀성, 무결성, 가용성, 책임성, 인증성, 신뢰성에 영향을 줄 수 있는 위협으로 인한 위험을 최소화하기 위하여 필요한 통제사항을 선택 및 구현하는 방법이다.

세 번째는 상세분석에 따른 접근방법(Selection of Safeguards according to Detailed Assessment)으로 세부적인 위험분석을 통하여 위협과 취약성으로 인한 위험을 평가하여 해당되는 통제사항을 선택하는 방법이다.

3. IT Baseline Protection Manual

독일의 BSI(Bundesamt Für Sicherheit in der Informationstechnik)에서 개발한 BSI IT Baseline Protection Manual 은 IT 시스템 차원에서 접근하고 있으며, 조직구조, 인력, 기반구조와 기술적인 차원을 적절하게 조화시켜 IT시스템에 대하여 정보보호 수준을 3단계로 분류하여 선택할 수 있도록 구성되어 있다.

가장 최근 것은 2000년 10월에 발간한 매뉴얼로 파악되고 있다. 본 매뉴얼의 기본적인 구조는 기본적으로 IT 자산에서 출발한다고 할 수 있다. 즉, 조직 전체 차원에서 접근하는 방식이 아니고 자산별로 세부적인 설명을 하고, 자산별로 가능한 위협들의 명세를 나열하였으며, 이러한 위협에 따른 위험을 줄이기 위한 가능한 통제사항들을 3단계 수준별로 구분하여 목록을 제시하고 있다. 따라서 조직에서는 본 매뉴얼에 따라 기 제시하고 있는 통제사항들을 세부적으로 기술한 별도 통제사항을 보면서 구현하면 되며, 정보보호의 수준을 조절할 수도 있다.

본 매뉴얼은 총 9장으로 구성되어 있으며, 추가로 위협의 시나리오와 통제사항(safeguards), 그리고 보조적인 설명자료와 형식 및 툴 등을 소개한 첨부로 구성되어 있다. 본 매뉴얼은 아래와 같이 5개의

영역으로 나누어져 있다.

첫 번째, 1장과 2장으로 본 매뉴얼의 전반적인 소개와 사용방법을 소개하고, 전제적인 수행절차를 제시

두 번째, 3장부터 9장까지로 정보기기 또는 자산 등 주제별로 서술한 총 7개 분야에 걸쳐 47개의 모듈 소개

세 번째, 위협 시나리오를 각각 소개하고 있으며, 5개 분야에 걸쳐 262개를 제시하는 위협사전(Dictionary)임

네 번째, 통제사항 각각에 대하여 실제 구현하는 방법과 내용까지도 제시하고 있으며, 6개 분야에 걸쳐 544개를 제시한 통제사항사전(Dictionary)임

다섯 번째, 기타 보조적인 설명자료로서 각종 서식과 관련 툴 들을 소개

즉, 임의의 조직에서 정보보호 정책을 결정하고 개략적인 위험분석을 실시하며, 정보자산에 대한 모델링 과정을 거쳐 파악된 자산 중 소유하고 있는 유닉스 시스템이 있다고 가정할 경우, 이에 대한 두 번째 영역의 유닉스시스템이라는 모듈을 찾아가서 이미 이곳에서 제시하고 있는 위협들이 무엇이며 통제사항들이 무엇인지를 확인한다. 위협들에 대하여 세부적으로 이해하기를 원할 경우 세 번째 영역에서 제시하는 세부적인 위협시나리오를 참조하면 된다. 그리고 본 조직에서 취하고자 하는 정책이 3단계 중 어느 단계를 택할 것인지 결정하였거나 결정하지 않았으면 정책을 결정한다. 그리고 그에 상응하는 통제사항들을 구현하면 된다. 구현할 경우 통제사항들을 세부적으로 설명하고 있는 네 번째 영역을 참조하면 된다.

영역별로 보다 세부적으로 살펴보면,

첫 번째 영역인 전반적인 소개 부분의 경우 IT 정보보호 구축방법으로 정보보호책임자가 IT 시스템에 정보보호를 위한 통제사항을 구현하기 위한 전체적인 프레임워크를 구성하는 과정을 아래와 같이 정의하고 있다

○ IT 정보보호절차의 수립
  - 정보보호 정책수립
  - IT 정보보호관리 설정
○ IT 정보보호 개념의 개발
  - 정보기술 구조분석
    · IT와 관련 응용에 대한 정보의 수집
    · 항목들에 대한 그룹핑
  - 정보보호요구사항의 평가
    · IT baseline protection modeling("basic to moderate", "high", "very high")
    · Basic security check with actual versus target comparison
  - Supplementary security analysis
    · 위험분석
    · High protection requirement
    · 필요한 추가적인 분석
  - 구현계획의 수립
    · 통제사항의 통합정리
    · 구현계획 수립
○ 구현 : infrastructure, organisation, personnel, technology, communications, contingency planning 6개 분야에서의 미비된 통제사항을 구현
    · IT 정보보호문제에 대한 인식 제고
    · IT 정보보호 교육/훈련 제공
○ 운영/유지보수 : 구현된 통제사항을 운영하면서 발생되는 문제점의 보완 과정

두 번째 영역인 모듈분야는 총 7개 분야에 걸쳐 47개를 소개하고 있으며, 그 현황은 표 4와 같다.

〔표 4〕 BSI IT Baseline Protection Manual의 모듈분류 현황

대분류	소분류	갯수
Generic Components (공통 적용 일반항목)	- IT security management - Organisation - Personnel - Contingency Planning concept - Data Backup Policy - Data Privacy Protection - Computer virus protection Concept - Crypto-concept - Handling of Security Incidents	9
Infrastructure (기반시설)	- Buildings - Cabling - Rooms(office, server room, storage media archives, technical infrastructure room) - Protective Cabinets - Working Place At Home (Telecommuting)	8

Non-Networked Systems (독립된 시스템)	- DOS PC(Single User) - Unix System - Laptop PC - PCs With a Non-Constant User Population - PC Under Windows NT - PC with Windows 95 - Stand-Alone IT Systems Generally	7
Networked Systems (네트워크시스템)	- Server-Supported Network - Unix Server - Peer-to-peer network - Windows NT Network - Novell Netware 3.x - Novell Netware 4.x - Heterogenous Networks - Network and system management	8
Data Transmission Systems (데이터 전송 시스템)	- Exchange of Data Media - Modem - Firewall - E-Mail - WWW server - Remote Access	6
Telecommunications (통신)	- Telecommunications system (Private Branch Exchange, PBX) - Fax Machine - Answering Machine - LAN connection of an IT system via ISDN - Fax Servers - Mobile Telephones	6
Other IT components (기타사항)	- Standard Software - Databases - Telecommuting	3
계		47

세 번째 영역인 위협시나리오의 카탈로그에서는 5개 분야에 걸쳐 262개의 위협시나리오를 제시하고 있는데, 표현방식은 "T 4.1 Disruption of power supply"와 같이 하고 있다. 여기서 T는 위협을 말하고, 4는 5개 분야에 대한 순차적인 번호를, 1은 해당 분야 중 첫 번째 위협을 말한다. 개략적인 분포 현황은 표 5와 같다

〔표 5〕 위협의 분야별 분포 현황

번호	분야	기본설명	갯수
1	Force Majeure	조명, 화재, 수해, 먼지, 인력손실, 시스템고장 등	10
2	Organization Shortcomings	조직(기관)에서의 지원미비 등	66
3	Human Error	관리자(이용자)의 관리 및 사용 오류 등	45
4	Technical Failure	기술적 미비 및 오류 등	42
5	Deliberate Acts	기타 사항	99

네 번째 영역인 통제사항은 구현을 할 경우 세부적으로 참고할 수 있도록 상세하게 구현하는 방법과 절차를 기술하고 있다. 본 매뉴얼에서는 "S 2.18 (3) Inspection rounds(optional)"로 표현하고 있는데 여기에서 S란 대책을 의미하고, 2란 2번째 분야를 의미하며, 18이란 해당분야의 18번째 통제사항을 의미한다. (3)의 경우 security priority를 의미하는 것으로 1은 기본사항이면서 가장 높은 우선순위를 말하며, 2는 중요하므로 가능하면 빨리 구현하도록 하는 것이고, 3은 마무리하기 위해서 중요하나 어려운 상황이라면 미룰 수도 있음을 의미한다. 그리고 *optional* 이란 비용효과 측면에서 적절하지 않을 경우 다른 통제사항으로 대체할 수 있음을 의미한다. 통제사항의 내용의 기본적인 구성은 다음과 같다.

〈 통제사항의 구성 〉

S 2.11 Provisions Governing the Use of Password
Initiation responsibility : Head of IT Section, IT Security Manager
Implementation reponsibility : IT Security Management, users
〔Text of the safeguards ....〕
Additional controls:
- Have the users been briefed on the correct handling of password
〔...〕

6개 분야별로 544개의 통제사항 분포 현황을 살펴보면 〔표 6〕과 같다.

〔표 6〕 분야별 통제사항 분포 현황

번호	분야	기본설명	갯수
1	Infrastructure	기반 구조적 대책 중심	46
2	Organization	조직관리 대책 중심	205
3	Personnel	인력관리 중심	23
4	Hardware & Software	하드웨어 및 소프트웨어 대책 중심	115
5	Communication	통신관련 대책	83
6	Contingency Planning	비상계획 대책 중심	72

다섯 번째 영역은 기타 보조적인 설명 자료로서 각종 서식을 담고 있으며, 본 매뉴얼을 적용하는데 있어 용이성과 효율성을 제고하기 위하여 제시된 각종 툴에 대한 개략적인 설명을 담고 있다.

4. SSE-CMM

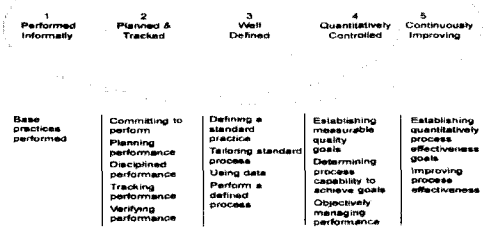
카네기멜론대학의 소프트웨어공학연구소 주관으로 40개 이상의 정부기관과 업체가 참여하는 프로젝트 그룹을 1995년 1월에 결성하여 제품과 서비스의 품질 향상을 위하여 SSE-CMM(Systems Security Engineering Capability Maturity Model) 개발을 시작하였다. 이후 1996년 10월에 1.0 버전을 발표하였으며, 1999년 4월 1일에 2.0 버전을 비 이익단체인 ISSEA(International Systems Security Engineering Association)에서 지원하여 발간되었다. 참고로 ISSEA는 시스템 보안공학과 관련되어 ISO/IEC JTC 1의 Liason으로 실질적인 표준화 작업을 하는 기관이다.

SSE-CMM은 기본적으로 정보보호관리기준, BS7799, GMITS 등의 보안관리를 위한 지침 등의 성격과는 다르다. 우선 적용 대상이 정보기술에 대한 사항으로 전체적인 구조는 소프트웨어 생명주기(Software Life Cycle)에 관한 국제표준인 ISO/IEC 12207에 기초하되, 조직이 구현한 IT 정보보호 프로세스를 맵핑시켜 성숙도를 측정하는 수단이기 때문이다. 따라서, 이들 정보보호관리와 관련된 지침 등에 보조적으로 사용할 수 있다. 즉, 이들 지침들에 의하여 구현된 체계가 얼마나 성숙되어 있는지를 확인하고 조직에서는 성숙도를 높이는데 활용할 수 있기 때문이다.

본 모델의 구성을 살펴보면, 2차원 메트릭스 형태로 구성되어 있다. 크게 능력(capability)과 영역(domain)으로 구성되어 있다. 본 모델의 기본적인 특성은 각각의 영역에서의 프로세스를 결정하고 이에 대한 능력 수준을 평가하고 개선하기 위해 사용하는 것을 제시하고 있다.

능력은 잘 작성된 실무(Best Practices)로 generic practices라고 하고, 5개의 단계로 구성되어 있으며 단계가 높을 수록 성숙도가 높은 것이다. 이러한 단계의 정의는 다음과 같이 하고 있다.

- 1(Performed Informally) : 비공식적인 수행으로 기본 실무를 수행하는 수준을 말함
- 2(Planned and Tracked) : 계획되고 추적 가능한 단계로 성과계획, 성과통제, 성과추적, 성과확인이 되어야 함
- 3(Well Defined) : 잘 정의된 단계로 표준공정의 정의, 정의된 공정의 수행, 보안 실무의 조정이 이루어짐
- 4(Quantitatively Controlled) : 계량적으로 통제되는 단계로 측정 가능한 품질목표를 수립하고 성과의 객관적인 관리가 이루어짐
- 5(Continuously Improving) : 지속적으로 향상되는 단계로 조직 능력의 향상과 공정 효과성의 향상이 이루어짐



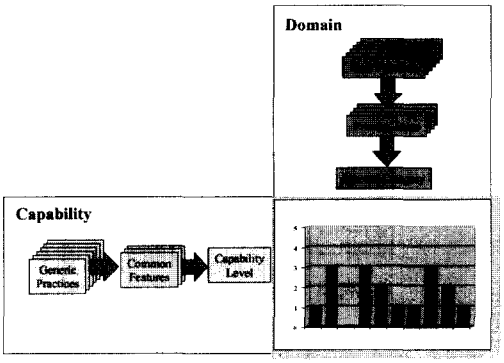
〔그림 4〕 Generic Practices

영역은 가장 잘 작성된 실무사항을 기본적으로 수행하여야 할 대상으로 base practices라고 하며, security base practices와 project and organizational base practices로 구성되어 있다. Base practices는 11개의 process areas에 걸쳐 61개 통제사항과 11개의 project and organizational process areas에 걸쳐 62개 통제사항으로 총 123개로 구성되어 있다. 이들의 구성을 세부적으로 살펴보면 표 7과 같다.

〔표 7〕 프로세스 분야별 통제사항 현황

구분		공정분야(process area)	통제 항목 수
기본		Administer Security Controls	4
		Assess Impact	6
		Assess Security Risk	6
		Assess Threat	6
		Assess Vulnerability	5
		Build Assurance Argument	5
		Coordinate Security	4
		Monitor Security Posture	7
		Provide Security Input	6
		Specify Security Needs	7
		Verify and Validate Security	5
프로젝트/조직	프로젝트	Ensure Quality	7
		Manage Configurations	5
		Manage Project Risk	6
		Monitor and Control Technical Effort	6
		Plan Technical Effort	10
	조직	Define Organization's Systems Engineering Process	4
		Improve Organization's Systems Engineering Processes	4
		Manage Product Line Evolution	5
		Manage Systems Engineering Support Environment	7
		Provide Ongoing Skills and Knowledge	8
		Coordinate with Suppliers	5

SSE-CMM에 대한 전체적인 구조를 살펴보면 그림 5와 같다.



〔그림 5〕 SSE-CMM의 구조

SSE-CMM은 결국 영역이 가지고 있는 22개의 프로세스들에 대하여 정보보호의 성숙도 수준을 평가하여 지속적인 개선을 하자는 취지에서 작성이 되었다. 여기에서 영역에 있는 프로세스는 조직의 특성에 따라 추가하거나 삭제하여 사용할 수도 있다.

5. 기 타

정보보호관리를 위한 기준이나 지침 등은 앞에서 다룬 이외에도 다양하게 나와 있다. NIST에서는 컴퓨터보호 소개라는 책자를 발간하였는데, 관리통제, 운영통제, 기술통제 3개분야로 분류하고는 있으나, 전체적인 프레임워크를 제시하고 있지는 않다.

유럽전기통신표준협회(ETSI)에서 제시하고 있는 Baseline Protection Manual의 경우 독일의 Baseline Protection Manual과 유사한 형태로 되어있다.

미국 예산회계국(GAO)의 경우도 Best Practices로서 정보보호관리를 위한 기준으로 미 연방기관들에 권고하고는 있으나 이의 활용 현황은 그리 활발하지 않은 것으로 파악되고 있다.

미 회계감사협회인 ISACA의 ISACF의 경우도, 2000년 10월에 COBIT(Control Objectives for Information and Related Technology) 3판을 출간하였는데, 기존의 2판과는 기본 철학이 바뀌는 완전히 상이한 접근법을 제시하였다. 즉, 기존의 정보기술 중심으로 시스템의 생명주기에 입각하여 통제사항을 제시하였으나, 3판에서는 "IT Governance"라는 개념을 도입하고, 이를 관리할 수 있도록 관리자용 지침을 새로이 제시하고 있다.

COBIT을 좀 더 살펴보면, 기본 시각이 기존의 IT 시스템 중심에서 광범위한 IT 차원으로 범위를 확대하였다는 것이다. 이는 모든 정보기술은 경영과 관리상에 있어서 매우 중요한 수단으로 IT와의 관계는 이제 거의 동일하여, 시각을 넓혀야 한다는 것이다. 그러나, COBIT은 아직까지는 정보보호 중심으로 접근하고 있지는 않다. COBIT은 정보기술 중심으로 통제사항을 다루면서 정보보호의 중요성이 보다 강화되는 사회적인 추세를 반영하여 정보보호 관련 통제사항을 대폭 강화하고 있다.

이 밖에도 다양한 관리적인 기준과 지침 등이 있으나, 본 고에서는 이 정도로 살펴보기로 한다.

Ⅳ. 정보보호관리를 위한 기준간 비교

많은 국가가 지역적인 특성과 문화적인 특성 등을 고려하여 정보보호 관리를 위한 지침이나 기준 등을 활발하게 연구하고 있다. 따라서, 이들 지침이나 기준 등은 전혀 다르다고는 할 수 없으나 나름대로 추구하는 목적, 범위, 방법, 절차 등을 서로 상이하게 제시하고 있다. 이들에 대한 특성들을 살펴보면 표 8과 같다.

〔표 10〕 정보보호관리체계와 BS 7799 1부와 비교

구분	관리기준(국내)	ISO/IEC 13335	BS 7799	IT Baseline Protection Manual	SSE-CMM
작성기관	한국정보보호센터	ISO/IEC JTC1	영국 BSI	독일 BSI	미국 ISSEA
작성연도	2001	1996부터 구성	1999	2000. 10.	1999. 4.
표준화 현황	단체표준 예정	part1 - part 4 까지 TR, part 5는 작업중	국가표준 (2000.10 ISO/IEC 17799 part 1)	-	국제표준 작업 중
작성목적	정보보호관리 체계 수립/인증	IT 보호관리	정보보호 관리체계 수립/인증	IT 시스템 보호관리	IT 시스템 보호관리
적용범위	전사적	IT	전사적	IT 시스템	IT 시스템
기본 틀 제공여부	제공	제공	제공 안함	제공	제공
통제사항 분류	13개 분야	조직적및물리적 7개분야, IT 시스템 5개 분야	10개 분야	6개 분야	기본/프로젝트 및 조직 22개 분야
통제 사항 수	131	63	127	544	123

< 정보보호관리기준과 BS 7799 >

정보화 역기능의 발생 사례를 보면 70퍼센트 이상이 기술적인 부분이 아닌 물리적 및 환경적인 부

분에서 발생된다고 한다. 따라서 정보를 보호하기 위한 방편으로 기술적인 부분도 중요하지만 그 이외의 인적, 물리적, 환경적인 관점에서 접근하여야 하는 것도 매우 중요하다. 따라서 국내의 정보보호관리를 위한 기준은 전사적인 관점에서 출발한 BS 7799를 근간으로 하고 있다.

국내에 적용하게 될 정보보호관리기준은 BS 7799의 내용 중에서 국내 실정에 맞도록 문서화의 양을 최소화하는 방향으로 접근하였으며, 법·제도적인 준거성 부분도 일부 가감을 하였다. 그리고 정보보호 정책의 경우 필요시 IT 시스템 수준에서도 작성할 수 있도록 항목을 추가하였다. 정보보호를 위해서는 무엇보다도 이에 대한 올바른 인식이 있어야 하는 점을 고려하여 교육 및 훈련부분을 보다 구체화하였으며, 전산실이라는 물리적인 공간에 대해서도 정보를 보호하기 위한 통제사항을 추가하였다.

또한, 다양한 산업 분야에서 활용할 수 있도록 전사적인 차원에서 접근함으로써 범용성을 확보하고 있다. 그리고, 부분적으로는 IT 시스템에 적용할 수도 있도록 세부적인 통제사항을 추가하기도 하였다.

국내의 정보보호관리기준과 BS 7799에 대한 세부 통제사항들을 비교하여 보면 표 9와 같다.

〔표 8〕 정보보호관리기준과 BS 7799 통제사항 비교

구분	정보보호관리기준		BS 7799 part 2		통제사항	
					추가	삭제
정보보호관리과정	관리체계 수립		Establishing a management framework			
	구현		Implementation			
	문서관리		Documentation Document Control			
	기록관리		Records			
세부통제분야(13개)	정보보호정책	6	Security Policy	2	3	
	정보보호조직	5	Security Organization	10	1	2
	아웃소싱 및 제3자접근	5			2	
	자산분류와 통제	3	Asset classification and Control	3	0	
	인적보안	8	Personal Security	10	3	
	교육 및 훈련	5			3	
	접근통제	29	Access Control	31	2	1
	물리적보호	13	Physical and Environmental Security	13	5	3
	운영관리	21	Comunication and operations	24	0	4
	개발보안	17	Systems development and maintenance	18	1	1
	업무연속성관리	6	Business Continuity Management	5	0	0
	보안사고대응및복구	7			5	3
	요구사항준수	6	Compliance	11	0	4
합 계		131		127	25	18

< 정보보호관리기준과 GMITS >

GMITS은 기본적으로 전사적 관리, 전사적 정보보호 관리, 전사적 IT 보호관리, IT 시스템 보호관리 중 전사적 IT 보호관리에 초점을 맞추어 제작되었다. 전사적인 IT 보호관리부터 출발하여 파악된 정보자산들에 대하여 통제사항의 선택 등 세부 접근을 할 수 있도록 하고 있다. 그리고 추가적으로 SSE-CMM에서 처럼 IT 시스템별로 수준을 측정할 수 있는 프레임워크를 제시하고 있기도 하다. 여기서 국내에 적용하게 될 정보보호관리지침은 전사적 정보보호관리 수준에서 작성되었으나 수준 측정에 대한 방안은 제시되어 있지 않다.

정보보호관리기준은 13개 분야로 나누어 131개의 통제사항을 제시하고 있는 반면에 GMITS은 12개 분야에 63개의 통제사항을 제시하고 있다. 통제사항들의 내용을 비교하여 보면 대부분은 같거나 유사하다. 물론, 접근하는 수준 차이가 나는 것은 기본 철학이 상이하기 때문이다. GMITS은 정보보호관리기준에 비하여 다음과 같은 부분이 미약하다.

- ○ 제3자접근 및 아웃소싱
- ○ 장비보관실에 대한 보호
- ○ 장비의 재사용 또는 폐기
- ○ 작업책상의 정리
- ○ 운영관점의 변화관리
- ○ 개발장비와 운영장비의 분리
- ○ 외부로부터 들여오는 장비의 관리
- ○ 정보 및 소프트웨어의 상호 교환 관리
- ○ 전송매체의 관리
- ○ 전자상거래 및 전자메일
- ○ 공개시스템에 대한 관리
- ○ 이동컴퓨팅
- ○ 정보보호요구사항 분석
- ○ 입출력데이터 및 메시지 인증
- ○ 기타 운영관련 사항 등

< 정보보호관리기준과 IT Baseline Protection Manual >

IT Baseline Protection Manual의 가장 큰 특징 중의 하나는 일종의 위협과 통제사항에 대한 사전이라고 볼 수 있는 262개의 위협과 544개의 통제사항을 제시하고 있다는 점이다. 특히, 통제사항은 구현 절차까지도 다루고 있을 정도로 매우 세부적으로 기술되어 있다. 그리고 IT 시스템을 중심으로 접근하도록 되어있는 절차에 맞게 시스템 유형별

로 잘 정리하여 놓았다는 것이다.

뿐만 아니라 시스템별로 관리수준을 조정하여 정리할 수 있도록 3단계의 측정 모델을 제시함으로써, 조직의 특성에 따라 자율적으로 선택함은 물론, 향후 정보보호 관리의 수준을 향상시킬 수 있는 방법을 제시하고 있기도 하다.

수행절차는 GMITS와 유사하다. 자산 현황을 조사하여 유사한 유형별로 분류한 후 해당 모듈을 찾아 기술되어 있는 위협과 통제사항, 그리고 보호수준에 따라 구현할 수 있도록 되어 있다. 즉, 자산에 대하여 위험분석을 수행한 후 위험을 받아들이는데 비용효과성이 있다고 판단되면, 매뉴얼 방식으로 순차적으로 접근하여 대처하면 된다.

따라서, 국내 적용하고자 하는 정보보호관리기준의 철학과는 많은 차이를 보이고 있음을 알 수 있다. 그러나 정보보호관리기준을 국내 적용하고자 하는 자는 IT Baseline Protection Manual의 위협사전과 통제사항사전을 활용할 수는 있을 것이다. 본 매뉴얼의 통제사항 사전에는 기술적인 부분을 포함하여 세부적으로 구현하는 절차와 방법까지도 제시되어 있기 때문이다.

< 정보보호관리기준과 SSE-CMM >

SSE-CMM의 기본 목적은 정보보호를 위한 관리의 성숙도를 측정할 수 있는 모델을 제시하고 있다는데 있다. 대부분의 정보보호관리에 관한 지침 등이 비록 관리의 수준을 조절할 수 있는 모델을 제시하고 있기는 하나 대상 항목을 제시하고 항목별로 성숙도를 높일 수 있는 평가체계를 뚜렷하게 제시하고 있는 SSE-CMM과는 차이가 있다고 하겠다.

국내에 적용할 예정에 있는 정보보호관리기준은 이러한 성숙도 또는 수준에 대한 모델을 제시하고 있지는 않다. 이는 아직까지 국내에 수준을 측정할 수 있을 만큼의 분위기가 성숙되어 있지 않기 때문이다.

V. 결 론

정보보호관리를 위한 체계의 수립과 이에 대한 보증의 수단으로 인증제도가 2001년 7월 1일 부터 국내에 처음으로 도입이 된다. 본 제도의 시행을 위하여 정보통신부, 한국정보보호센터 및 관련 전문가들과 그 동안 많은 준비와 노력을 기울여 왔다. 그러나 좋은 제도라고 하여도 공감대가 형성되지 않으면 실패할 가능성이 높다고 하겠다. 따라서 본 제도의 성공적인 정착과 활성화를 위하여 조금이나마 기여할 수 있기를 기대하는 마음으로 본 고를 작성하게 되었다.

정보의 보호를 위한 이러한 기준과 지침 등의 도입은 비록 완벽하게 비밀성, 가용성, 무결성을 보장할 수는 없을 것이다. 그러나, 조직의 특성에 맞게 비용 효과성 측면에서 체계적이며 효율적으로 접근하는 여지를 제공하여 해당 조직에서 이를 활용함으로써 보호하고자 하는 중요한 전사적 자원 또는 정보자산에 대한 위험을 최소화한다는 점에서 그 의미가 크다고 하겠다. 현재 국내에 도입하고자 하는 정보보호관리기준도 이러한 점들을 감안하여 국내 실정에 가장 잘 맞도록 각계 전문가들의 의견을 반영하여 작성하였다.

제도의 시행을 준비하는 시간이 그리 많이 주어지지 않은지라 충분한 연구 작업을 수행하지 못한 감이 없지 않아 있다는 점에 대하여 아쉬움을 가지고 있으나, 본 제도의 도입 취지는 정보를 신뢰성 있게 활용하는데 최소한의 기준을 제시하여 정보에 대한 비 인가된 사용과 오·남용 등을 최소화하자는 데 있다.

지금은 이러한 정보보호를 위한 관리적 개념이 도입단계로, 정보보호관리기준의 국내 적용은 소기의 성과를 달성할 것으로 판단이 되나, 국내의 정보보호관리를 위한 인식과 환경이 성숙된 이후도 대비를 하여야 할 것이다. 즉, 현재의 기준을 가지고 국내 환경이 성숙되었을 경우에는 적용하는데 다소 무리가 따를 수도 있기 때문이다.

따라서, 이러한 앞으로의 방향에 대해서도 많은 준비를 하여야 할 것이다. 구체적으로 향후 연구 가능한 방향에 대하여 제시하여 보면 다음과 같은 것들이 있을 수 있다.

- ○ 현재 제시되어 있는 SSE-CMM의 성숙도 측정을 위한 모델을 국내의 정보보호관리기준에 적용하는 것으로, SSE-CMM의 프로세스 분야를 정보보호관리기준의 13개 영역으로 대체하고 프로세스별로 성숙도 측정을 위한 수준을 제시하거나 SSE-CMM의 성숙도 수준을 수용하는 방법
- ○ IT 시스템 중심으로 적용하는 독인 BSI의 IT Baseline Protection Manual에서 각각의 유사한 시스템별로 제시된 모듈 부분에 대하여 기 제시된 수준 분류를 보다 구체화하며 국내 실정

에 적합하도록 하는 방법. SSE-CMM의 성숙도 수준을 참고할 수 있음

○ GMITS에서 제시하는 미약하지만 정보보호 수준 측면을 구체화하고, 국내 실정에 적합하도록 보완하는 방법

등이 있을 수 있을 것이다. 이 외에도 다양한 많은 방법이 있을 것이며, 많은 연구를 통하여 가장 효율적이고 우리 실정에 맞는 접근 방법을 도출하여 적용하는 노력을 기울여야 할 것이다.

참 고 문 헌

[1] 정보통신부, "정보통신망이용촉진및정보보호등에 관한법률", 2000.

[2] 한국정보보호센터, 정보보호관리기준(안), 2001

[3] BSI(U.K.), "BS 7799 part1 : Information Security Management - Code of Practice for Information Security Management", 1999

[4] BSI(U.K.), "BS 7799 part1 : Specification for Information Security Management Systems", 1999

[5] Carnegie Mellon University, "Systems Security Engineering Capability Maturity Model, version 2.0", April 1, 1999

[6] BSI(Bundesamt Für Sicherheit in der Informationstechnik)(독일), "IT Baseline Protection Manual", October 2000

[7] ISACA, "COBIT:Executive Summary, 3rd Ed.", July 2000

[8] ISACA, "COBIT:Management Guidelines, 3rd Ed.", July 2000

[9] ISACA, "COBIT:Framework, 3rd Ed.", July 2000

[10] ISACA, "COBIT:Control Objectives, 3rd Ed.", July 2000

[11] ISACA, "COBIT:Audit Guidelines, 3rd Ed.", July 2000

[12] ISO/IEC, "ISO/IEC TR 13335-1:1996(E) : Information Technology - Guidelines for the Management of IT Security part 1", 1996

[13] ISO/IEC, "ISO/IEC TR 13335-2:1997(E) : Information Technology - Guidelines for the Management of IT Security part 2", 1997

[14] ISO/IEC, "ISO/IEC TR 13335-3:1998(E) : Information Technology - Guidelines for the Management of IT Security part 3", 1998

[15] ISO/IEC, "ISO/IEC TR 13335-4:2000(E) : Information Technology - Guidelines for the Management of IT Security part 4", 2000

[16] John P. Hopkinson, "The Relationship between the SSE-CMM and IT Security Guidance Documentation", 1999, EWA-Canada Ltd.

[17] NIST, "An Introduction to Computer Security: The NIST Handbook", 1996.

〈著者紹介〉

이 강 신 (KangShin Lee)

1987년 2월 : 한양대학교 수학과 졸업(학사)
1989년 8월 : 한양대학교 수학과 졸업(석사)
1990년 7월 ~ 1992년 6월 : (주)데이콤 종합연구소 연구원
1992년 7월 ~ 2000년 8월 : 한국전산원 정보화 표준부장
2000년 9월 ~ 현재 : 한국정보보호센터 선임연구원
관심분야 : 정보보호관리, 소프트웨어공학, 정보기술아키텍처

김 학 범 (Hakbeom Kim)
종신회원

본 호의 "정보보호관리체계 인증 제도 소개 및 추진 방향" 저자소개 참조

이 홍 섭 (Hongsub Lee)
종신회원

본 호의 "정보보호관리체계 인증 제도 소개 및 추진 방향" 저자소개 참조