情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

정보보안관리 평가방법론 고찰: BS7799를 중심으로 한 운영적 접근법

이 철 원*, 김 종 기**, 이 동 호***, 박 춘 식*

요 약

다양한 정보보안 평가 방법론들 중에서 BS7799는 정보시스템을 운영하는 조직 전반의 보안 상태를 평가하는데 유용한 방법론으로서, 여러 나라에서 활용하고 있으며 최근에는 국제표준으로 채택되었다. 본 고에서는 BS7799에서 제시하고 있는 보안통제 항목과 정보보안관리시스템의 구축 및 이의 객관적인 평가를 위한 인증 방법을 살펴본다. BS7799는 전자상거래를 수행하는 기업들 사이에 보안 수준에 대한 상호 신뢰를 확인하기 위한 방법으로 활용될 수 있으며, 최근에 제정된 정보통신기반보호법에서 요구하고 있는 취약성 평가에도 적용될 수 있을 것이다.

Ⅰ. 서 론

사회 전반에 걸쳐 정보화가 급속히 진행되면서 정보보안의 중요성에 대한 인식도 높아지고 있다. 정보보안은 단순히 정보시스템이나 정보기술에 국한된 문제가 아니라, 조직 전반에 걸쳐 포괄적으로 검토되어야 하는 문제로 대두되고 있다. 이러한 맥락에서 정보보안과 관련된 관리 활동은 다양한 기법과 방식으로 수행되고 있다.

보안 관리의 방법론들이 다양하게 제시되어 있는데, 그 중에서 영국의 BSI에서 개발된 BS7799는 영국은 물론 여러 국가에서 활용되고 있으며, 나아가 국제적인 표준으로 자리잡고 있다.

본 연구에서는 이러한 BS7799의 보안관리 지침과 적용 방법을 살펴보고, 전반적인 보안 통제와 관리에 대한 내용을 다루고자 한다.

BS7799는 크게 두 부분으로 나뉘어 지는데, 한 부분은 보안 통제 목록이며, 다른 부분은 보안 관리를 위한 표준에 대한 내용이다. 이 두 부분에 대한 고찰을 통해서 표준으로 자리잡고 있는 BS7799에 대한 정확한 이해를 돕고, 또한 이 방법론을 바탕으로 효과적인 관리방법이나 절차 그리고 적용단계와 과정의 응용에 대한 이해를 돕고자 한다.

1. BS7799의 개요

정보 사회에 접어든 오늘날 정보기술(IT)은 어느 산업이든지 불문하고 기업 경영의 근간을 이루고 있다. 정보보안은 이제 더 이상 정부기관이나 높은 수준의 보안을 요하는 한정된 분야의 업체에서만 관심을 가지는 문제가 아니라 모든 기관과 기업체에서 반드시 짚고 가야하는 문제로 인식되고 있다.

정보보안관리는 보안위험을 식별하고 이러한 위험을 효과적으로 관리할 수 있는 대책을 다룬다. BS7799는 기업이 고객 정보의 비밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는데 초점을 둔다. BS7799는 BT, HSBC, Marks and Spencer, Shell International, Unilever 등 주요 업체와 더불어 영국의 상무성 주관으로 "정보보안관리 실무 규범(A Code of Practice for Information Security Management)"이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 개발되었으며, 조직의 보안 표준의 기반이 되도록 고안되었다.

BS7799의 개발 배경은 기업들이 직면하고 있는 대부분의 상황에 필요한 통제를 식별하기 위한 단일

* 국가보안기술연구소 ({cheolee, csp@etri.re.kr})
** 부산대학교 경영학부 조교수 (jkkim1@hyowon.pusan.ac.kr)
*** 부산대학교 경영학부 박사과정 (dghlee@hyowon.pusan.ac.kr)

한 참조점을 제공하고, 중소기업은 물론 대기업까지 광범위한 범위에 적용될 수 있도록 하여 공통적인 정보보안관리 문서를 참조함으로써 기업들간의 네트워킹에 있어서 상호 신뢰가 가능하도록 한다. 물론 이 표준에서 제시하고 있는 통제들 모두가 모든 상황에 적용될 수 있는 것은 아니며, 개별적인 환경적 또는 기술적 제약조건을 고려하여 선택하여야 할 것이다. 따라서 BS7799 표준은 지침과 권고안의 성격을 가진다.

BS7799는 1995년에 처음 제정되어 1999년에 개정되었으며, 영국 이외에 호주, 브라질, 네덜란드, 뉴질랜드, 노르웨이, 핀란드, 인도 등에서 사용되고 있고, 1999년 10월에 ISO 표준으로 제안되어 ISO/IEC 17799-1이 되었다. 영국 정부에서는 전자정부를 향한 노력을 뒷받침하기 위하여 2001년 3월까지 대부분의 정보시스템에 대하여 BS7799 인증을 받도록 하여 국가 핵심 정보 기반구조를 보호하기 위한 수단으로 활용하고 있다. 산업계에서는 정보보안이 국제시장에서 경쟁 우위를 제공하는 경영전략이 될 수 있다고 인식하고 있으며, 유럽, 북미, 환태평양권 등 전세계적으로 BS7799에 대한 높은 관심을 보이고 있다.

BS7799는 두 부분으로 구성된다. 제1부는 표준적인 실무 지침이며 종합적인 보안 통제 목록을 제시하고, 제2부는 정보보안관리시스템 (Information Security Management System; ISMS)에 대한 표준적인 명세이다. 또한 ISO9000과 유사하게 운영되는 "c:cure"라는 인증 스킴이 있다. ISO9000과 BS7799사이에는 많은 유사성이 있는데, 예를 들어 ISO9000에서의 품질 정책과 품질관리시스템 대신에 BS7799에는 정보보안 정책과 ISMS가 존재한다.

2. BS7799의 역사

BS7799의 원래의 목적과 개발취지는 영국내의 보안과 관련된 표준을 만들어 전반적인 틀을 작성하는 것이었다. 이러한 목적에서 인증체계의 개발과정은 다음과 같은 흐름으로 이어져 왔다.

- 1987년:
  영국 상무성의 상업용 컴퓨터 보안센터의 프로젝트 시작
  개발 방침 수립
  Users code of practices 발행
- 1995년:
  PD0003 구현 기준 개발
  1995년도 판 BS7799의 출시
  ISO에 상정되었으나 표준 채택 실패
  영국외의 지역에서 유사한 표준들이 태동되게 됨
- 1998년:
  BS7799 제2부 추가
  인증 스킴인 c:cure가 공식적으로 시작됨
  제1부에 대한 국제적인 표준적용을 위해서 개정작업 착수
- 2000년:
  1999년 판 BS7799의 발행
  최초의 c:cure 인증 시행
  제1부가 ISO에서 정식 표준인 ISO17799-1로 채택됨
  제2부의 표준인증을 위한 프로젝트가 개발중
- 2001년 이후:
  제2부의 ISO 인증 완료 예정

3. 국내 동향

세계적인 보안 표준 지침 준수의 경향에 따라서 국내에서도 이러한 BS7799에 대한 관심이 높아지고 있으며, 국가적인 차원에서 시행을 위한 구체적인 절차가 계획된 상태이다.

향후 국내에서의 추진과정은 2001년 5월 중 시범 인증기관을 지정하여, 인증에 대한 실제 업무를 7월부터 수행할 예정이다.

최근에 제정된 정보통신기반보호법에서 규정하고 있는 취약성 평가에 있어서도 BS7799의 방법론이 원용될 수 있을 것이다. 향후 산업전반에 걸친 전자상거래의 확대와 금융산업에서의 온라인 거래의 확산을 계기로 이러한 BS7799의 표준에 대한 관심과 인증을 위한 노력은 앞으로 급속하게 진행될 것으로 예상된다.

II. 표준 내용

1. 제1부: 보안통제항목 - Part1 : Code of practice for information security management

제1부는 전체 10개의 주요한 부분으로 구성되어 있으며, 36개의 통제 목적, 그리고 전체 127개의

〔표 1〕 BS7799의 분야와 통제항목

분야	세부분야	통제항목
보안정책	정보보안 정책	정보보안정책 문서, 검토 및 평가
보안조직	정보보안 기반구조	정보보안 관리 포럼, 정보보안 조정, 정보보안 책임 배정, 정보처리시설의 권한부여 프로세스, 전문가의 정보보안 조언, 조직간 협력운영, 정보보안의 독립적인 검토
	제3자 접근 보안	제3자 접근에 대한 위험 식별, 제3자 계약에 대한 보안 요구사항
	아웃소싱	아웃소싱 계약의 보안 요구사항
자산분류 및 통제	자산에 대한 책임	자산목록
	정보 분류	분류지침, 정보 등급화 및 취급
인적보안	직무정의 및 자원배정 보안	직무기술서에 보안책임 정의, 인적 검열 및 정책, 기밀 협정, 채용 약정 및 조건
	사용자 교육훈련	정보보안 교육 및 훈련
	보안사고 및 오류의 대응	보안사고 보고, 보안취약성 보고, 소프트웨어 오류 보고, 사고로부터 교훈 획득, 징계절차
물리적 및 환경적 보안	보안지역	물리적인 보안경계, 물리적인 출입 통제, 사무실, 룸 및 시설 보안, 보안지역 내에서의 작업, 격리된 배달 및 적재 영역
	장비보안	장비 위치 및 보호, 전원 공급장치, 선로보안, 장비 유지보수, 영외 장비 보안, 장비의 안전한 폐기 및 재사용
	일반적인 통제	청결한 책상 및 화면 정책, 소유물의 제거
의사소통 및 운영관리	운영 절차 및 책임	문서화된 운영절차, 운영환경의 변경 통제, 사고관리절차, 직무 분리, 개발과 운영 시설의 분리, 외부시설관리
	시스템 계획수립 및 인수	능력계획, 시스템 수락
	악성 소프트웨어에 대한 보호	악성 소프트웨어에 대한 통제
	운영	정보 백업, 운영자 로그, 결함 기록
	네트워크 관리	네트워크 통제
	매체의 취급 및 보안	이동 가능한 컴퓨터 매체의 관리, 매체의 폐기, 정보 취급 절차, 시스템 문서 보안
	정보 및 소프트웨어의 교환	정보 및 소프트웨어 교환 협정, 운송중인 매체 보안, 전자상거래 보안, 전자우편 보안, 전자사무시스템 보안, 일반에 공개된 시스템, 기타 정보교환 형태

통제항목을 통한 보안 지침을 제공하고 있다. 이러한 통제항목들을 통해서 보안관리에 대한 전반적인 사항을 확인할 수 있으며 보안관리의 참조기준으로 활용할 수 있다.

제1부에서는 위험관리(risk management)의 중요성을 강조하고 있으며, 공식적인(formal) 관리의 절차와 방법, 그리고 문서화를 상대적으로 중요시하고 있다.

1.1 주요 통제항목

제1부는 앞서 설명하였듯이 보안통제에 대한 전반적인 목록으로 구성되어 있으며, 보안관리의 실행을 위한 기본적인 내용을 다루고 있다. 이러한 통제항목들에 대한 내용은 표 1과 같은 주요한 10개의 통제항목과 세부적인 통제내용으로 요약할 수 있다.

1.2 1999년 판의 최신개정 내용

1995년도 판에서는 주요 통제항목(key controls)이라는 용어를 통해서 다음과 같은 10개의 중요한 통제항목들을 명시하고 있었다.

- 정보보안 정책 문서
- 정보보안 책임 배정
- 정보보안 교육 및 훈련
- 보안 사고 보고
- 바이러스 통제
- 업무 지속성 계획 절차

〔표 1〕 BS7799의 분야와 통제항목 (계속)

접근통제	접근통제 업무 요구사항	접근 통제 정책
	사용자 접근 관리	사용자 등록, 권한 관리, 사용자 패스워드 관리, 사용자 접근 권한의 검토
	사용자 책임	패스워드 사용, 관리하지 않는 사용자 장비
	네트워크 접근 통제	네트워크 서비스의 사용 정책, 강제된 통제, 외부접속에 대한 사용자 인증, 노드 인증, 원격점검포트 보호, 네트워크 분리, 네트워크 접속 통제, 네트워크 라우팅 통제, 네트워크 서비스 보안
	운영체제 접근통제	자동화된 터미널 식별, 터미널 로그온 절차, 사용자 식별 및 인증, 패스워드관리 시스템, 시스템 유틸리티의 사용, 비인가 사용자에 대한 경고, 터미널 종료, 접속 시간 제한
	어플리케이션 접근 통제	정보 접근 제한, 민감한 시스템 격리
	시스템 접근과 사용의 감시	사건 기록, 시스템 사용 감시, 시계 동기화
	이동 컴퓨팅 및 텔레워킹	이동컴퓨팅, 텔레워킹
시스템 개발 및 유지보수	시스템 보안요구사항	보안 요구사항 분석과 명세화
	응용시스템의 보안	입력데이터 확인, 내부처리 대한 통제, 메시지 인증, 출력 데이터 확인
	암호통제	암호통제의 적용 정책, 암호화, 디지털 서명, 부인봉쇄 서비스, 키 관리
	응용시스템 파일의 보안	운영 소프트웨어의 통제, 시스템 시험 데이터 보호 , 프로그램 소스라이브러리의 접근 통제
	개발 및 지원 프로세스 보안	변경 통제 절차, 운영시스템 변경에 대한 기술적 검토, 소프트웨어 패키지 변경 제한, 은닉 채널 및 트로이안 코드, 외주 소프트웨어 개발
업무지속성 관리	업무지속성 관리 측면	업무지속성 관리 프로세스, 업무지속성 및 영향 분석, 지속성 계획의 작성 및 구현, 업무지속성 계획수립을 위한 프레임워크, 업무지속성 계획의 시험, 유지, 재평가
준수	법적 요구사항 준수	적용 법률의 식별, 지적자산권, 조직 기록의 보호, 데이터 보호 및 개인정보의 프라이버시, 정보처리시설의 오용 방지, 암호화 통제 규정, 증거수집
	보안정책과 기술적 준수 검토	보안 정책 준수, 기술상의 준수 점검
	시스템 감사 고려사항	시스템 감사 통제, 시스템 감사 도구 보호

- 소프트웨어 복제 통제
- 조직 기록의 보호
- 데이터 보호
- 보안 정책 준수

1999년 판에서도 이러한 맥락은 그대로 이어지고 있으나, 주요통제항목이라는 명칭을 사용하지 않고 있다. 특히 1995년 판이 ISO에서 표준으로 인정받지 못한 이후 1999년도 판에서는 다음과 같은 부분들이 개정되어 표준으로 적용되었다[3][5][13].

- 정보기술과 관련된 정보를 대폭 변화하고, 정보 전송과 저장과 관련된 다양한 과업을 포괄하도록 소개하였음.
- 도입부분에 위험평가에 대한 보다 상세한 정보를 기술함.
- BS7799를 보다 기술 독립적인 것으로 변환됨.
- 영국 산업과 국제적인 산업에 응용가능 하도록 내용이 수정되었음.
- 아웃소싱과 제3자 계약을 포함하는 제3자 접근 위험을 설명하는 내용을 추가하였음.
- 자산의 가치와 중요성이 추가되었으며, 무결성과 가용성을 포함하는 정보 등급화의 일반적인 관점을 포함하도록 정보 분류의 개념을 확장하였음.
- 컴퓨터와 네트워관리라는 명칭이 커뮤니케이션과 운영관리로 변화되었으며, 정보 처리의 보다 광범위한 해석을 포함하도록 함.
- 이동 컴퓨팅과 텔레워킹에 대해 기술함.
- 암호화 정책, 디지털 서명과 키 관리를 포함하는 암호화 기술에 대한 내용이 추가되었으며, 출력 검증과 채널 은닉과 트로이안 코드에 대한 내용을 추가하였음.

[표 2] 보안 통제의 인식에 대한 전통적인 접근법

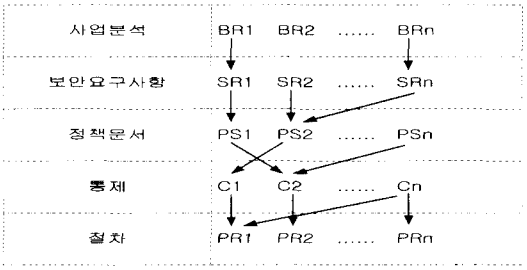
위험분석(risk analysis)		위험관리(risk management)
사업분석(business analysis) 위험평가(risk assessment) 위험순위화(risk prioitization) 보안요구사항(security requirements)	→	통제 제안(proposal of control) 통제 구현(implementation of controls)

- 업무 지속성 관리가 어떠한 업무 지속성 계획의 기본으로 사용가능 하도록 재구성되고 확장되었음.
- 영국에 국한된 준수의 부분이 국제적인 적용이 가능하게 하였으며, 지적자산권, 감사, 증거와 암호와 규제에 대한 내용을 수정하였음.

2. 제2부: 관리 표준 - Part2 :Specification for information security management

제2부는 제1부에서 설명한 내용의 구체적인 보안관리 프레임워크를 제공하며, 구축과 관련된 절차와 방법을 설명한다. 즉, ISMS에 대한 세부적인 규격으로 문서화의 실행에 대한 요구사항과 각 조직의 필요성에 따라 실행 될 수 있는 보안관리의 항목들을 규정하고 있다.

BS7799는 ISMS를 수립하도록 명백하게 요구하고 있다. 즉, ISMS 수립을 통해서 조직은 그들의 환경과 상황에서 정보자산을 보호할 수 있는 통제목적을 선택하고 이러한 것을 관리할 수 있는 체계를 만들도록 한다는 것이다. 한편, BS7799에서는 위험관리의 중요성을 강조하며, 제1부에 수록된 모든 통제 항목들을 구현할 필요는 없다는 점을 명확히 강조하고 있다. 관리적인 차원에서 보안은 통제요소를 고려하며 모든 항목들이 필수적인 것은 아니며, 조직적 혹은 상황적인 여건에 따라서 유동적이다. 제2부에서는 ISMS를 어떻게 구축하는지를 제시하며, 이러한 관리 절차의 순서는 먼저 모든 정보자산과 조직에 있어서 그들의 가치를 분석하고, 어떤 정보가 왜 중요한지를 식별하는 정책을 고안하도록 한다. 다음 단계에서는 낮은 가치를 가진 정보를 제외하여 관리 대상의 범위를 정의한다. 다음으로, 정보자신의 가치를 상실하는데 따른 위험을 분석하며, 그 위험을 어떻게 관리할지를 결정한다. 여기에는 물리적, 인적, 절차적인 측면을 고려하여야 하며, 효과적인 업무 지속성 계획의 개발도 포함된다. 그 후에는 위험을 관리하기 위한 보안대책을 선정한다. BS7799에는 이러한 보안대책이 열거되어 있다. 그러나 BS7799의 목록은 완전한 것이 아니며, 원하는 경우에는 추가적인 보안대책이 포함될 수 있다. 적용성보고서(Statement of Applicability)에는 특정한 보안 통제가 선택된 이유를 기술할 뿐만 아니라 BS7799에서 열거한 보안 통제 중에서 제외된 항목이 특정 조직에 관련이 없는 이유를 명시한다. 이 적용성보고서(SoA)에는 ISMS의 적용 통제 항목과 기업의 상황적인 맥락에서 기술된 내용으로 BS7799 최종심사 수립시에 고려가 되는 문서이다.



[그림 1] 사업분석, 보안요구사항, 정책문서, 통제 및 절차간의 관계

2.1 BS7799의 정형적 보안통제 접근방식

전통적인 보안 통제인식을 위한 접근방식은 위험분석과 위험관리의 두 단계를 가진다. 이러한 두 단계는 표 2와 같이 표현된다. 즉, 사업과 관련된 정보자산의 위험분석을 기반으로 위험관리를 위한 토대가 작성되는 것이다.

한편 정형적인 접근법은 사업분석 (business analysis), 보안 요구사항 (security requirement), 보안 정책 (security policy), 그리고 BS7799의 보안 통제 (security controls from BS7799)로 구성된다[2]. 이러한 정형적인 접근법은 보안 통제의 절차와 관계를 명시하고 있는 것으로 그림 1과 같이 도해될 수 있다.

즉, 사업분석을 통해서 보안요구사항이 결정되고, 결정된 보안요구사항은 정책문서로 작성되며, 정책

문서를 기반으로 통제가 선정되고, 선정된 통제는 절차에 의해서 수행되는 과정을 설명하고 있다[1].

이러한 구현단계는 BS7799를 기준으로 선택된 통제는 모두 구현되어야 함을 명시하고 있으며[6], 관리는 이러한 통제가 모두 적절하게 제대로 수행되고 있는지를 평가해야한다.

2.2 정보시스템 관리 시스템의 구축 단계

BS7799의 제2부는 정보보안관리시스템(ISMS)의 구축, 문서화 및 구현을 위한 요구사항을 정의한 것이다. 이것은 각 개별조직의 요구에 따라 구현될 보안통제에 대한 요구사항을 정의한 것이다.

이러한 조직의 요구에 따라 적용할 수 있는 정보보안 통제목표 및 방안은 적용성보고서로 문서화가 된다.

2.3 정보보안관리시스템 요구사항 (ISMS requirements)

조직은 문서화된 ISMS를 구축, 유지하여야 한다. 이는 보호대상 자산, 위험관리에 대한 조직의 접근, 통제목표 및 방안, 요구되는 보증수준을 언급하여야 한다.

2.3.1 관리프레임워크의 구축 (Establishing management framework)

통제 목표 및 방안을 식별하고 문서화하기 위하여 그림 2와 같은 단계를 밟아야 한다.

① 1단계: 정보보안정책을 정의한다
② 2단계: 정보보안관리시스템의 범위를 정의한다. 경계는 조직 특성, 위치, 자산 및 기술 등의 용어로서 정의한다
③ 3단계: 적절한 위험평가를 실시한다. 위험평가는 자산에 대한 위협, 취약점 및 조직에 대한 영향을 식별하고 위험수준을 결정한다
④ 4단계: 관리하여야 하는 위험영역은 조직의 정보보안정책과 요구되는 보증수준을 토대로 식별하여야 한다
⑤ 5단계: 적절한 통제 목표 및 방안을 선정하고, 그 선정을 정당화한다. 통제 목표 및 통제방법의 선정을 위한 지침은 BS 7799 제1부에 정의되어있다. 정의한 통제 목표 및 통제방법은 완전한 것이 아니며 추가적인 통제가 필요할 수 있음을 나타낸다.
⑥ 6단계: 적용성보고서를 작성한다. 설정한 통제 목표 및 방안과 그것의 설정 사유는 적용성보고서로 문서화하여야 한다. 이 문서는 정의한 통제 방안중에서 제외된 것을 전부 기록하여야 한다.

그림에 나타나 있는 각 단계는 주기적으로 재검토하여야 한다. 즉, 일회적인 것이 아니라, 반복적이고 지속적으로 검토되어야 한다는 것이다.

2.3.2 구현 (Implementation)

조직은 선정한 통제 목표 및 방안을 효과적으로 구현하여야 한다. 통제를 위해 채택한 절차의 효율성은 보안정책과 기술적 준수의 검토에 따라 검토하여 검증하여야 한다.

2.3.3 문서화 (Documentation)

ISMS문서화는 다음과 같은 정보로써 구성된다.

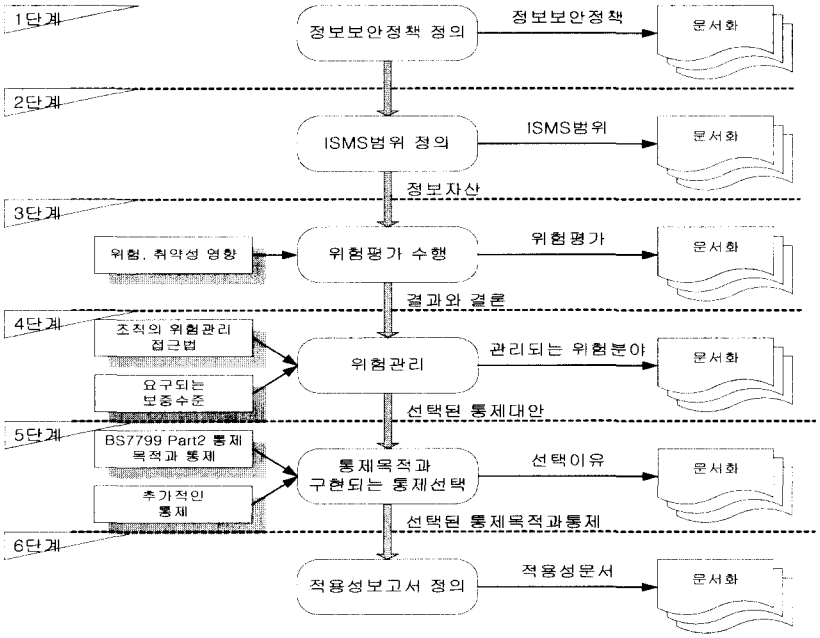
① 정의한 활동의 실행 증거
② 관리프레임워크의 요약, 정보보안정책 및 통제목표, 적용성보고서에 정의한 통제방법을 포함
③ 정의한 통제방법을 구현하기 위한 책임 및 관련 활동을 기술한 절차서
④ ISMS의 관리 및 운영을 위한 책임 및 관련 활동을 기술한 절차서

2.3.4 문서통제 (Document control)

조직은 요구되는 모든 문서의 통제절차를 수립, 유지하여야 한다. 문서통제는 다음사항을 보장하여야 한다.

① 편리한 유용성
② 조직의 보안정책과 부합하는지를 주기적으로 검토하고 수정
③ 버전의 통제 및 효과적으로 ISMS 기능이 실행될 수 있는 모든 분야에서 유용하도록 함
④ 구본은 즉시 제거
⑤ 법적, 지식보존의 목적으로 보관하는 구본을 식별하고 유지

문서는 읽기 쉽고, 날짜와 버전을 기록하고, 쉽게 식별할 수 있게끔 정해진 방식에 따라 유지하여야 하며 정해진 기간동안 보관하여야 한다. 절차와 책임은 다양한 형태의 문서를 제정하고 수정하기 위해



〔그림 2〕 보안관리 프레임워크

수립, 유지하여야 한다.

2.3.5 기록 (Record)

ISMS 운영결과로 생성된 증거인 기록은 조직에서 BS 7799의 요구사항에 부합함을 실증할 수 있도록 적절한 시스템으로서 유지하여야 한다.

조직은 준수를 실증할 수 있는 기록을 식별, 유지, 보관, 폐기하는 절차를 수립, 유지하여야 한다.

기록은 읽기 쉽고, 식별하기 쉽고, 관련 활동을 추적할 수 있어야 한다. 기록은 쉽게 검색할 수 있고 파손, 질의 저하 또는 분실로부터 보호할 수 있는 방식으로 저장, 유지하여야 한다.

2.4 세부통제방안 (Detailed controls)

세부통제 방안은 제1부에서 제시한 통제 목표 및 통제방법에서 도출한 것이므로, 제1부의 내용과 일치한다 (표 1 참조).

Ⅲ. 인증 체계

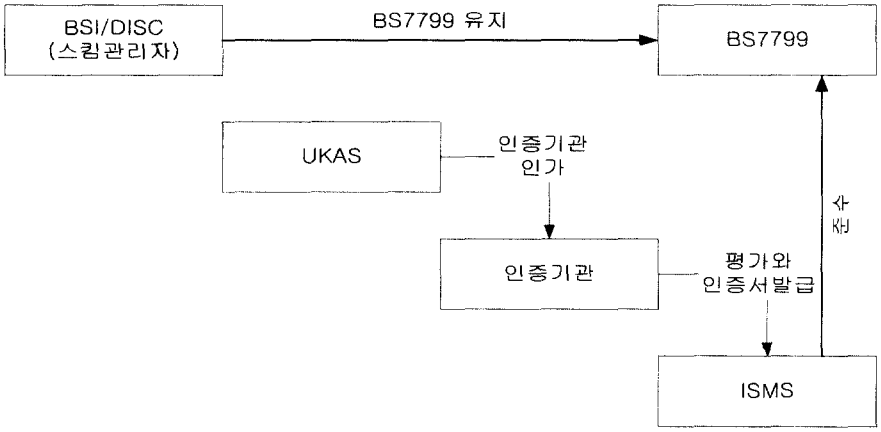
1. BS7799 인증 스킴: c:cure

c:cure는 평가가 적절하다는 것을 보증하기 위한 BS7799의 확장으로 볼 수 있으며, 독립적인 감사 등록을 실시한다는 점이 차이가 있다. 그러나 이러한 독립적인 감사는 2000년까지는 영국에서만 이루어지고 있으며, 향후 자질이 있는 기관이나 요원에 대한 훈련과 교육이 이루어질 것이라고 명시하고 있다[14].

이러한 인증스킴은 다음에 설명되는 인증기관에서 수행하는 것으로 현재 다수의 인증을 받은 감사자가 이러한 업무를 수행하고 있다. 실제 우리나라의 경우에도 외국의 독립적인 감사자의 국내법인이 들어와 있으며, 앞서 언급한 국가적인 추진 방안에 따라서 인증 서비스를 실시하고 있다.

2. 인증절차와 인증기관

BS7799에 대한 인증 관리는 영국의 상무성을 대리하여 영국표준협회(BSI/DISC)에서 수행하고 있다. 인증서를 발급받기 위해서는 해당 ISMS는 독립된 제3자인 BS7799 평가자(assessor)에 의한 감사를 받아야 한다. 평가자의 자격에 대해서는 엄격한 규칙이 적용된다. 이러한 엄격한 규칙은 평가자가 소속된 평가기관이 영국인증서비스(UK Accreditation Service: UKAS)의 인가를 받아야 한다는 조건으로도 명시가 되어 있으며, 평가자는 해당 ISMS가 적절히 운영되고 있는지 주기적으



〔그림 3〕 c:cure 인증 스킴

로 확인해야만 함을 명시하고 있다. 이러한 과정은 그림 3과 같이 나타낼 수 있다[13].

그림에 나타나 있듯이, 해당 조직은 그들의 정보자산 관리를 설명하고 있는 개별 ISMS를 문서화를 통해서 수립하고 이렇게 수립된 ISMS에 대해서 평가자를 통해서 구체적인 인증을 받게 된다. 이러한 인증은 일회적인 것이 아니라 지속적인 관리체계가 유지되고 있는가와 문서화가 영속적으로 이루어지고 있는가를 확인하는 절차를 거친다.

Ⅳ. 참고문서: PD3000 series

실제 BS7799의 인증을 받기 위한 단계에 대한 설명은 인증스킴에 서술되어 있다. 그러나, 이러한 인증을 받는데 있어서 해당조직은 자체적으로 현재 인증을 받기에 타당한가에 대한 평가를 수행할 수 있다. 즉, 평가수행을 위해서 기본적으로는 BS7799를 참조할 수 있으며, 몇 가지의 추가적인 지침을 통해서 현재의 상황판단과 보안통제와 관련된 전반적인 평가를 수행할 수 있게 된다.

따라서, PD3000 씨리즈 문서들은 기존의 조직이 가지고 있는 보안 정책과 위험관리에 대한 사항과 항목들이 BS7799의 표준에 합당한 지를 자체적으로 평가할 수 있는 문서라고 볼 수 있다. 물론 부분적으로 몇몇의 PD 3000 씨리즈의 문서들은 인정을 받는 조직만이 아니라 감사를 수행하는 심사원에게도 참조가 될 수 있는 항목들이 기술되어 있다. BS7799 제2부에 따른 인증을 받는데 있어서 참고할 지침 자료의 내용과 항목들은 표 3과 같다.

Ⅴ. BS7799의 목적과 중요성공요인

이상에서 BS7799와 관련된 전반적인 내용을 설명하였다. 여기서는 BS7799의 근본적인 목적을 정리하고 이러한 BS7799의 성공적인 수행에 있어서 중요한 성공요인에 대하여 살펴본다.

1. BS7799의 목적

BS7799의 목적은 다음과 같다.

- 보안관리의 개발, 구현 그리고 측정에 있어서 표준과 지침으로 활용: 효과적인 개발과 구현 그리고 측정을 가능하게 한다.
- 기업간 거래에 있어서 확신을 제공: 기업간의 신뢰구조를 강화하여, 거래의 무결성, 기밀성, 정확성을 보장하도록 한다.
- 정보기술 제품과 서비스를 조달하게 되는 경우 참조할 수 있는 표준과 지침으로 사용: 아웃소싱이나 조달(procurement)과 같이 외부 조직에 의해서 개발되는 경우, 해당 제품과 서비스를 평가할 수 있는 준거로써 사용할 수 있다.

2. 성공요인에 대한 실증연구

1996년에 실시된 BS7799 구현에 대한 실증적인 조사에서는 상당수의 기업이 구현에 어려움을 겪고 있거나, 인지하지 못하고 있는 것으로 나타나 있다[11]. 영국의 기업을 대상으로 한 이 연구에서는 80%이상

〔표 3〕 BS7799 보안지침 문서

문서번호	제목	내용
PD 3000	Information Security Management: An introduction	인증제도와 절차 및 지침 문서들의 개요를 소개 - ISMS의 개발, 평가 및 인증 - BS7799 인증의 중요성에 대한 이해
PD 3001	Preparing for BS7799 Certification-Guidance on implementation requirements to organisations preparing for certification	인증심사를 위해 준비해야 하는 사항들을 나타내고 있으며, BS7799의 각 요구사항 별로 준비되어야 할 증거를 산업의 Best Practice를 기반으로 제공
PD 3002	Guide to BS7799 Risk Assessment and Risk Management-Guidance aimed at those responsible for carring out risk management	위험을 평가하고 관리하기 위한 전체적인 프로세스와 용어의 정의를 포함하여 BS7799의 기본적인 개념을 설명 - 위험 평가와 관리 절차에 대한 이해 - BS7799 ISMS의 개발, 평가, 인증 획득에 대한 지침
PD 3003	Are you ready for a BS7799 Audit?	인증심사에 앞서 조직 내에서 점검을 수행하기 위한 지침을 소개
PD 3004	Guide to BS7799 Auditing	심사지침 - 심사원이 심사를 수행하는 경우의 안내서 - 내부감사자가 내부감사를 위한 참조문서로 활용가능
PD 3005	Guide on the selection of BS7799 controls	BS 7799 Part 2의 관리항목 중에서 조직이 선택적으로 사용할 수 있는 지침을 제공

의 기업이 BS7799에 대한 명확한 인식을 못하고 있거나, 구현을 고려하고 있지 않은 것으로 나타나 있다. 그러나, 이러한 문제는 향후 영국정부의 강력한 주도로 개선될 것으로 보이며, 현재 상당수의 기업이 기업간 거래의 상호인증의 한 수단으로 BS7799를 활용하고 있는 것으로 나타나 있다[4].

또한, 앞서 서론에서 지적한 10개의 주요한 통제의 구현에 대한 조사에서는 BS7799를 적용한 대부분의 기업이 통제를 구현하고 있지만, 상대적으로 차이가 존재하고 있음을 나타내고 있다. 즉, 바이러스 보호, 보안 정책, 자료처리, 소프트웨어 감사, 자산보호, 정책 준수가 상대적으로 높은 80%이상의 구현을 나타내고 있으며 교육과 훈련의 부분은 40% 정도로 낮게 나타나 있다.

이러한 결과에서 BS7799는 제2부에서도 언급되었듯이 반드시 구현해야한다거나, 동등한 상황이 아니라 조직의 상황이나 사업의 환경 등에 따라서 차별적으로 이루어질 수 있음을 내포하고 있다고 할 수 있을 것이다. 요약하면, BS7799의 성공적인 구현에 있어서 중요한 요인은 다음과 같은 5개의 항목으로 제시될 수 있다[7][9].

- 보안 목표와 활동은 업무 목표와 요구사항에 반드시 기반되어야 하고 업무 관리에 의해서 주도되어야 한다.
- 최고경영층으로부터 가시적인 지원과 적극적인 참여가 있어야 한다.
- 기업 자산에 대한 보안 위험에 대한 명확한 이해가 있어야 하며, 조직내부의 보안 수준에 대한 이해가 필요하다.
- 보안은 모든 관리자와 종업원들에게 효과적으로 인식되어야 한다.
- 보안 정책에 대한 지침과 표준이 모든 종업원과 계약자에게 배포되어야 한다.

즉, 본 연구에서 논의한 BS7799의 핵심적인 이해뿐만이 아니라, 조직적인 차원과 관련된 모든 조직구성원의 인식과 이해 그리고 무엇보다 업무와 직접적인 연관성을 확보하여야 BS7799의 구현이 성공적으로 이루어질 수 있게 된다는 것이다.

Ⅵ. 결 론

BS7799는 기본적으로 두 부분으로 구성되어 있는데, 제1부는 조직의 보안 구축을 위한 참조와 지침으로 사용될 수 있으며, 제2부는 구체적인 구현에 있어서 그 방법론과 절차를 명확하게 기술하였으며, c:cure라는 인증체계에 대한 내용을 서술하였다.

이러한 운영적인 보안프레임워크는 추상적인 보안 모형이나 이론이 아닌 보다 현실에 적합한 운영적인 부분이며, 이러한 BS7799의 적용은 기업에서 발생하는 활동들에 대한 제3자의 객관적인 인증을 통해서 신뢰를 보장받게 되는 것이다. 즉, 보안의 객체인 거래나 자료들에 대한 보증만이 아니라, 기업간 거래의 주체가 되는 각 해당기업에 대한 보증을 통해서 기업이 다른 기업을 신뢰할 수 있는 근본적인

토대를 제공하게 되는 것이다.

이러한 토대는 향후 기업활동 영역의 확장에 따른 국제적인 기업간의 상호신뢰를 구축하는 데에도 상당한 기여를 하게 될 것이며, 기업이 다른 기업과의 업무제휴나 시장에서의 활동에 있어서 필수적인 요건으로 인식될 수도 있을 것이다.

현재, 정보시스템의 보안성 평가에 관련하여 TCSEC, ITSEC, CC 등의 제품/시스템 중심의 평가 기준에 대하여 활발한 연구개발이 되어 국내외에서 적용되고 있고, SSE-CMM과 같은 시스템 개발 프로세스에 대한 평가 프레임워크에 대한 관심이 서서히 일어나고 있다. 정보보안은 기술적, 운영적 환경의 변화에 따라 매우 동태적인 특성을 지니고 있으므로, BS7799와 같은 조직의 운영적 측면을 고려한 정보보안 평가 프레임워크의 중요성도 간과할 수는 없을 것이다.

참 고 문 헌

[1] Barnard, Lynette and Solms, von Rossouw, "A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls", Computer & Security, Vol.19, NO.2, 2000, pp.185-194.

[2] Barnard, Lynette and Solms, von Rossouw, "The Evaluation and Certification of Information Security against BS7799", Information Management & Computer Security, Vol. 6, No. 2, 1998, pp.72-77.

[3] BSI, BS7799: Code of Practices for Information Security Management, United Kingdom, 1995 & 1999.

[4] BSI corporate press and PR department, PR Week, November, No. 17, 2000.

[5] Pounder, Chris, "The Revised Version of BS7799-So What's New", Computer & Security, Vol.18, 1999, pp.307-311.

[6] Elof, M.M. and Solms, von S.H., "Information Security Management: A Hierarchical Framework for Various Approaches", Computer & Security, Vol.19, 2000, pp.243-256.

[7] Institute for Certification of Information Technology(ICIT), Scheme for Self Assessment and Certification of Information Security against BS7799, 1997.

[8] Solm, von Rossouw, "Information Security Management(1): Why Information Security Is So Important", Information Management & Computer Security Vol. 6, No. 4, 1998, pp.174-177.

[9] Solm, von Rossouw, "Information Security Management(2): Guidelines to The Management of Information Technology Security(GMITS)", Information Management & Computer Security Vol. 6, No. 5, 1998, pp.221-223.

[10] Solm, von Rossouw, "Information Security Management(3): The Code of Practice for Information Security Management(BS7799)", Information Management & Computer Security Vol. 6, No. 5, 1998, pp.224-225.

[11] White, Kearvell Brian, "National(UK) Computer Security Survey 1996," Information Management & Computer Security, Vol. 4, No. 3, 1996, pp.3-17.

[12] 전자신문, 2001년 01월 12일.

[13] http://www.bsi-global.com/index.html

[14] http://www.c-cure.org

[15] http://www.dnv.com/mngsyscert/Services/BS7799.htm

〈著者紹介〉

이 철 원 (Cheol Won Lee)

1987년 : 충남대학교 수학과(이학사)

1989년 : 중앙대학교 전자계산학과(이학석사)

1989년 ~ 1996년 : 한국전자통신연구원 선임연구원

1996년 ~ 2000년 : 한국정보보호센터 선임연구원/통신모델링 과제책임자

2000년 ~ 현재 : ETRI부설 국가보안기술연구소 팀장

관심분야 : 컴퓨터 및 네트워크 보안, 정보통신기반보호, 정보보호시스템 평가기준

김 종 기 (Jongki Kim)

1987년 : 부산대학교 경영학과 학사
1988년 : Arkansas State University, MBA
1992년 : Mississippi State University, Ph.D. in MIS
1993년 3월 ~ 1998년 12월 : 국방정보체계연구소 선임연구원
1999년 3월 ~ 현재 : 부산대학교 경영학부 조교수
관심분야 : 정보시스템 보안관리, 전자상거래, 프로젝트 관리

이 동 호 (Dongho LEE)

1996년 : 부산대학교 경영학과 학사
1998년 : 부산대학교 경영학과 석사
1999년 5월 ~ 2000년 5월 : 부산대학교 경영경제 연구소 전임연구원
2001년 : 부산대학교 경영학과 박사과정 재학중
관심분야 : 그룹의사결정지원시스템, 정보시스템 보안, 전자상거래, 웹어플리케이션

박 춘 식 (Choon Sik Park)

광운대학교 전자통신공학과 졸업(학사)
한양대학교 대학원 전자통신공학과(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 : 9월 일본 동경공업대학 객원연구원
1989년 ~ 현재 : ETRI 부설 국가보안기술연구소 책임연구원, 정보보증연구부장
1999년 ~ 현재 : 한국통신정보보호학회 편집(논문지)이사, 논문지 편집위원장, 종신회원
관심분야 : 암호이론, 이동통신보안, 정보전