인증서발행국(CAP)들의 스킴 분석을 통한 우리나라의 평가, 인증 제도의 문제점과 시사점

강장묵*, 유의상**, 박광철***
서경대학교 컴퓨터공학과*, 소프트웨어공제조합**, (주)한국전자인증***

The Suggestion and problem of Korea Skim looking into through the CCRA-CAP Analysis

Kang Jang Mook**, Yoo eui sang**, Park Kwang Cheol***
Seokyeong University*, Software Financial Cooperative**, CrossCert, Inc.***

E-mail : wseoul@bcline.com, yes@ksfc.or.kr, kcpark@crosscert.com

Key Words : 국제공통평가인정협정(CCRA), 국제공통평가기준(CC), CCRA-CAP, CC-MRA, Common Criteria, Common Criteria Recognition Arrangement

요 약

국제공통평가기준(Common Criteria)2.1을 기반으로 한 국제공통평가인정협정(Common Criteria Recognition Arrangement)은 21세기 정보보호 산업 전반에 수출입 장벽 및 국제적 표준으로 자리매김 할 것이다. 이미 국제공통평가상호인정협정(CC-MRA)에서부터 적극적으로 기술을 축적하고 세계적 표준을 선도한 미국, 캐나다, 영국, 독일, 프랑스 등의 주요 선진국들은 국제공통평가인정협정 인증서발행국(CCRA-CAP)으로서의 우월적 지위를 확보한 상태이다. 이에 본 연구는 CCRA-CAP국가들에 대한 스킴(Skim) 분석을 통하여 우리나라의 스킴 개발이 국제적인 선도국과 비교하여 어떤 차이를 보이는지와 우리나라의 문제점을 도출해보고자 한다. 이를 통하여 향후, CCRA-CAP국가로 세계적 평가, 인증체계의 선도국이 되기 위한 준비과정에서 얻을 수 있는 통찰력과 시사점을 제공하고자 한다. 본 연구에서는 여러 스킴 중 정보보호시스템 평가, 인증 제도 관련 기관 책임 및 임무에 관한 1번 스킴을 주요 논의의 대상으로 하여 분석 연구한다.

목 차

1. 서론

2003년 1월 25일 발생한 인터넷 대란은 IT선진국에 비하여 피해수준이 상대적으로 컸던 우리나라에 많은 교훈을 주었다. 1.25대란은 특히 IT기반의 정보사회에서 안정성이 입증되지 않은 정보시스템의 구축과 허술한 관리는 오히려 그 취약성을 증가시키는 위험성을 내포하고 있으며, 지속적인 관심과 관리가 얼마나 중요한지를 다시 한번 일깨워주었다. 이제, 우리나라도 초고속 통신망 등 하드웨어적인 시설구축에서 진정한 정보화 사회를 만들기 위한, 정보보호 시설과 정보보호 관련 제품에 대한 표준화된 관리 그리고 현실성 있는 법제도 마련을 위해 노력해나가야 할 때이다. 이에 본 연구는 최근 정보보호시스템 평가·인증 체계연구에 있어, 현실적으로 중요시 되고 있는 국제공통평가인정협정(CCRA - Common Criteria Recognition Arrangement)에 대하여 살펴보고자 한다. 이는 향후, 국제공통평가기준(CC)기반의 CCRA가 정보보호시장에서의 정보보호제품의 새로운 무역장벽으로 과거 우르과이 라운드, 도쿄 라운드 등과 같은 시큐리티 라운드(Security Round)의 성격을 띠게 될 것이기 때문이다. 따라서 미리 철저한 준비와 대응전략 그리고 주도적인 참여를 통하여, "시장개방화"내지 "규제개혁"의 자국보호수단으로 활용할 수 있는 정보보호시스템 평가·인증 체계 연구를, 정보보호 산업의 육성과 보호라는 우리나라의 이익을 최대한 극대화하는 방향으로 진행하여야 한다.

이에 본 연구는 CCRA협정에서 주도적인 역할을 하고 있는 국제공통평가인정협정의 인증서발행국(CCRA-CAP)들에 대한 스킴(Skim) 연구를 통하여 CCRA가입에 필요한 한국의 효과적인 스킴 개발방안을 모색하고 문제점을 도출해 보고자 한다. 또한 본 연구를 결과를 통하여 향후, 한국의 CCRA가입에 필요한 준비과정에 많은 시사점과 통찰력을 얻을 수 있을 것으로 기대한다.

1.1 국제공통평가기준(CC)의 개요

(1) 국제공통평가기준(CC)의 내용

2003년도에 미국, 영국, 독일, 프랑스 등 평가 선진국들이 참여하는 국제공통평가기준 해설관리위원회(CCIMB - Common Criteria Interpretation Management Board) 에서는 2003년도에 CC버전을 3.0으로 개발하고 ISO에서 CC 3.0을 국제표준으로 채택할 예정이다. 하지만, 아직까지의 국제공통평가인정협정(CCRA)은 국제공통평가기준(CC) 2.1기반이다. 따라서 가장 최근에 발표된 CC 2.1의 고찰은 CCRA-CAP국가의 스킴 분석을 위해서는 반듯이 고찰해야 할 선행연구라고 볼 수 있다. 우선 국제공통평가기준은 크게 1부, 2부, 3부로 구분되어졌으며, 각 부분은 유기적으로 연관되어 있다.[1] 아래 <표 1-1>은 국제평가기준(CC)를 크게 3개 세부 내용으로 구분하여 기술한 것이다.

<표 1-1> 국제평가기준의 구성과 내용

구 성	내용	비고
1 부 :소개 및 일반모델	IT 보안성 평가의 원칙과 일반개념을 정의하고 평가의 일반적인 모델을 설명하는 공통평가기준의 소개 부분이다. 1부는 IT 보안목적을 표현하고 IT 보안요구사항을 선택·정의하며, 제품 및 시스템의 상위수준 명세를 작성하기 위한 구조를 소개한다. 또한, 공통평가기준 각 부의 유용성을 각 활용주체 측면에서 서술한다.	
2 부 :보안기능 요구사항	TOE의 기능요구사항을 표준화된 방법으로 표현한 것으로 기능 컴포넌트들의 집합으로 이루어져 있다. 2부는 기능 클래스, 기능 패밀리, 기능 컴포넌트의 집합으로 분류된다.	
3 부 :보증요구 사항	TOE의 보증요구사항을 표준화된 방법으로 표현한 것으로 보증 컴포넌트들의 집합으로 이루어져 있다. 3부는 보증 클래스, 보증 패밀리, 보증 컴포넌트의 집합으로 분류된다. 또한, 보호프로파일 및 보안목표명세서에 대한 평가기준을 정의하고 있으며, TOE의 보증수준을 정하기 위한 공통평가기준에서 미리 정의된 척도를 소개하는데 이를 평가보증등급이라 한다.	

1) http://csrc.nist.gov/cc/CC-v2.1.html
2003년 3월 19일 방문, 영문으로 CC2.1의 원본을 다운로드 할 수 있으며, 3개 부분으로 나누어져 있다.

(2) 국제공통평가기준(CC)의 개발 연혁

1993년 6개국 7개 기관이 합의하여 국제공통평가기준(CC)을 개발하기 시작하여, 1999년 9월 국제표준(ISO/IEC 15408)으로 제정[3]되었다. 아래 <표 1-2>은 국제공통평가기준(CC)에 대하여 요약하여 설명한 것이다.

년 도	당담 기관	내 용	비 고
1993년	미국(NSA,NIST),영국(CESG),독일(BSI),프랑스(SCSSI),캐나다(CSE),네덜란드(NL-NCSA)	6개국 7개 기관 개발 합의, 국제공통평가기준(CC: Common Criteria) 개발 시작	
1994년 4월	CCEB(Common Criteria Editional Board)	CC Version 0.6	
1994년 11월	CCEB	CC Version 0.9	
1996년 1월	CCEB	CC Version 1.0	
1996년 12월 ~ 1997년 3월	CCIB(Common Criteria Implementation Board)	CC Version 1.0 수정 보완	
1997년 7월	CCIB	CC Version 1.02 (Alpha) CC Version 2.0(Beta)	
1997년 12월	CCIB	CC Version 2.0(Draft)	
1998년 4월	CCIB	CC Version 2.0(Semi-Final)	
1998년 5월	CCMB(Common Criteria Maintenance Board)	CC Version 2.0(Final)	CC Version2.0 개발 완료된 후 CCIB에서 CCMB로 이관
1999년 9월	CCIMB (CC Interpretation Management Board)	CC Version 2.1(Final)	국제표준 (ISO/IEC 문서번호15408)으로 제정(1999.9) CC는 1999년6월8일표준화승인투표(승인29표,기권2표)국제표준승인 CC Version 2.1개발 완류 이후 CCIMB로 이관 "August 1999, Version 2.1, CCIMB-99-031"를 정보통신부에서 2002년 7월 "정보보호시스템 공통평가기준"으로 고시(국문/영문)[2]
2002년 2월	CCIMB (CC Interpretation Management Board)	Interpretation 반영 결과 발간	CCIMB(CC해설서관리위원회:CC 및 공통평가방법론(CEM)의 해설서 개발)

<표 1-2> 국제공통평가기준(CC)의 연혁

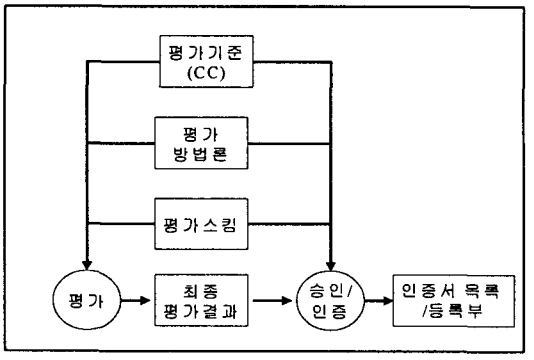
(3) 국제공통평가기준(CC)의 평가, 인증 절차

(가) 평가결과간의 비교가능성을 높이기 위하여 평가는 평가 스킴(Skim)의 틀에 따라 수행되어야 한다. 평가 스킴은 규범을 수립하고 평가의 신뢰도를 검증하며, 평가기관과 평가자가 지켜야 하는 규정을 관리 감독한다.

(나) 공통평가기준은 규정 체제에 대한 요구사항을 언급하지 않는다. 그러나 평가결과를 상호인정하려는 목표를 달성하기 위해 서로 다른 인증기관의 규정 체제간의 일관성이 필요하다. 아래 <그림 1-1>은 평가, 인증절차에 대한 주요 요소들을 나타내고 있다.

(다) 공통평가방법론을 사용하는 것은 평가결과의 반복성과 객관성에 기여하지만 이것만으로는 충분하지 않다. 평가기준 적용 시 일관성을 확보하기 어려운 많은 부분에서 평가자의 전문적인 판단과 배경 지식을 활용할 것을 요구한다. 평가 결과의 일관성을 높이기 위하여, 최종 평가결과에 대한 인증절차를 요구할 수 있다. 인증절차는 제품의 인증 또는 승인을 이끌어내는 과정으로, 평가결과에 대해 독립적으로 정밀 검사한다. 일반적으로 인증서는 공개된다. 인증절차는 IT 보안성 평가기준의 적용 시 더 향상된 일관성을 얻기 위한 방법이다.

(라) 평가스킴, 평가방법론, 인증절차는 평가스킴을 운영하는 인증기관의 책임이며, 공통평가기준의 범위에 포함되지 않는다.



<그림 1-1> 평가, 인증절차의 주요 요소[4]

2) http://www.mic.go.kr/jsp/mic_d/d100-0001-1-1.jsp?gubun=2&id=14, 2003년 3월 17일 방문 확인, 정보통신부 정보화정책관련 고시 자료 참조

3) http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf "Common Criteria for Information Technology Security Evaluation User Guide", p7., 1999년 10월, 2003년 3월 27일 방문 확인

4) 정보보호시스템공통평가기준, 2002년 7월, 정보통신부

1.2 국제공통평가인정협정(CCRA)의 개요

(1) 국제공통평가인정협정(CCRA)의 연혁

(가) 국제공통평가상호인정협정(CC-MRA)의 연혁

국제공통평가인정협정(CCRA)의 전신으로서 국제공통평가상호인정협정(Common Criteria Mutual Recognition)이 1998년 10월 5일에 주요 5개국(6개 기관)의 서명으로 체결되었다. 과정을 간략히 도표화하면, 아래 <표 1-3>과 같다.

[illegible]	[illegible]	[illegible]
1998년 3월	CC-MRA Draft작성	미국, 캐나다, 영국, 독일, 프랑스, 네덜란드 6개국에 의한 CC-MRA의 기반 구축
1998년 10월	CC-MRA 공개	미국, 캐나다, 영국, 독일, 프랑스 (5개국 참가)

<표 1-3> 국제공통평가상호인정협정의 연혁

(나) 국제공통평가인정협정(CCRA)의 연혁

국제공통평가인정협정(CCRA)의 연혁을 간략히 도표화하면, 아래 <표 1-4>와 같다.

[illegible]	[illegible]	[illegible]
2000년 5월	CCRA 체계 출범	기존의 CC-MRA체계를 대체하는 새로운 CCRA체계 출범 제 1차 ICCC회의(미국 볼티모어) 총 13개국 협정서에 서명 (MRA 가입국 7개국 + 신규가입 6개국)
2002년 9월	신규가입	이스라엘, 스웨덴 추가 가입 (총 15개국 16개 기관)

<표 1-4> 국제공통평가인정협정의 연혁

(2) CCRA체제의 주요 특징

상호인정협정(CCRA)체제가 기존의 상호인정합의(CC-MRA)체제와 가장 큰 차이점은 인증서 발행자와 인증서 수용자라는 이원화된 체제로 바뀐 것에 둘 수 있다. 아래 <표 1-5>는 CCRA체계의 주요 특징인 인증서발행자(CAP : Certificate Authorizing Participants)와 인증서수용자(CCP : Certificate Consuming Participants)에 대하여 간략히 정리하였다.

CAP	평가인증서의 생산자인 동시에 소비자 국가 CCRA에 의해 인증 받은 평가 및 인증기관을 보유한 국가 평가 인증서를 발급하는 동시에 다른 참가국이 발급한 평가인증서를 인증해주는 국가	미국 캐나다 영국 프랑스 독일 호주 뉴질랜드
CCP	평가인증서의 소비국 CCRA에 의해 인정받은 평가 및 인증기관을 보유하지 않은 국가 평가 인증서를 발급할 수는 없고, 다만 다른 참가국이 발급한 평가 인증서를 인정해 주는 국가	네덜란드 이탈리아 그리스 핀란드 노르웨이 스페인 이스라엘 스웨덴

<표 1-5> CAP와 CCP 비교 분석

(3) CCRA가입에 필요한 스킴(Skim)의 개요

CCRA에 가입하기 위해서는 국가스킴의 개발이 필요하다. 본 연구는 CCRA-CAP 주요 5개국에 대한 국가 스킴 분석을 통하여, CCRA 가입을 준비 중인 우리나라의 국가 스킴 도출과 시사점을 얻고자 하는 연구이다. 따라서, CCRA가입에 요구되어지고 개발되어야 할 국가 스킴의 전반적인 내용을 살펴보고자 한다. 아래, <표 1-6>은 CCRA 가입에 필요한 국가 스킴에 대한 제목과 세부 내용이며, 본 연구에서는 1번 스킴-즉 "정보보호시스템 평가, 인증 제도 관련 기관 책임 및 임무"에 관하여 주요 연구 대상으로 하여 스킴을 분석할 것이다. 또한 아래 소개한 내용 이외에도 필요에 따라 더 많은 스킴이 요구되어질 수 있으며, 또는 적은 스킴으로도 CCRA에 가입되는 다른 나라의 선례도 있다.

[illegible]	[illegible]	[illegible]
# 1	평가인증 스킴 관련 기관 및 역할	관련법으로 정하는 경우가 많음
# 2	평가 및 인증 절차	지침의 수준
# 3	인증서 유지 프로그램	지침의 수준
# 4	평가기관 운영지침	지침의 수준
# 5	평가신청인을 위한 지침	지침의 수준
# 6	기타 사항에 대한 지침	지침의 수준

<표 1-6> CCRA가입에 필요한 스킴의 개요

2. 본론

2.1 국제공통평가인정협정 인증서 발생국(CCRA-CAP)국가 스킴(Skim) 분석(주요 5개국)

2000년 5월 13개국(Australia and New Zealand, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, The United Kingdom, The United States of America)이 CCRA에 참가하여 "ARRANGEMENT on the Recognition of Common Criteria Certificates In the field of Information Technology Security"이라는 협정서를 체결하였다.[5] 그 후, 2002년 9월, 이스라엘, 스웨덴이 참가하여, 현재 총 15개국이 국제공통평가인정협정(CCRA)에 협정하였다. 본 연구에서는 국제공통평가인정협정 인증서발행국(CCRA-CAP)-7개국 중 5개국(미국, 캐나다, 영국, 독일, 프랑스)에 대하여 연구하고자 한다.

(1) 미국

(가) 배경 및 평가 인증제도 개요

NSA(National Security Agency)와 NIST(National Institute of Standards and Technology)는 미국 정부를 대표하는 IT 보안 관련 기관이다. 그간 NSA와 NIST는 미국 정부를 대표하는 IT 보안기관이 되기 위하여 지속적인 업무 영역분쟁을 벌여왔다. 하지만 2000년 1월 개정된 Computer Security Act에 의하여 NSA와 NIST의 업무 영역이 명확하게 구분되었다.[6] NSA는 미국 정부의 국가 보안시스템을 포함한 군사 외교상 목적에 사용되는 시스템에 대한 지침 및 표준을 개발하고, NIST는 그 외 SBU(Sensitive But Unclassified, 대외비)를 포함한 정부의 IT 시스템과 민간분야에 대한 지침 및 표준 개발을 담당하는 것으로 업무를 명확히 나누게 되었다.

IT 제품의 평가 인증제도에 있어서는 NSA와 NIST가 NIAP(National Information Assurance Partnership)이라는 독립기관을 설립하여 인증기관의 역할을 수행하도록 하였으며 NIAP의 역할은 다음과 같다.

NIAP은 3가지의 업무를 수행하며 그 업무는 다음과 같다.

- 정부 및 사용자를 대신하여 요구되는 IT제품의 보안 요구사항 제시
- IT 제품의 보안기능에 대한 평가 및 인증 업무를 총괄하며 평가 인증제도 관련 규정 수립
- IT 제품 평가 인증 관련 기술 개발 및 연구 수행

NIAP의 가장 중요한 업무가 바로 국제공통평가기준(CC) 기반의 평가 · 인증제도 관련규정인 평가 ·인증 스킴(Common Criteria Evaluation and Validation Scheme)을 개발하는 것이다. 스킴의 목적은 미국의 평가 · 인증제도에 제 3자의 민간 평가기관을 지정하여 참여하도록 하며, 그 결과를 국가적 차원에서 활용하도록 권장하고 국제공통평가인정협정을 체결한 국가들로부터 인정받을 수 있도록 하는 것이다.

미국은 1998년 국제공통평가상호인증협정(CC-MRA)에 가입한 후 현재까지 12개의 제품과 5개의 보호프로파일을 평가하였으며 15개의 제품과 7개의 보호프로파일을 평가하고 있다.

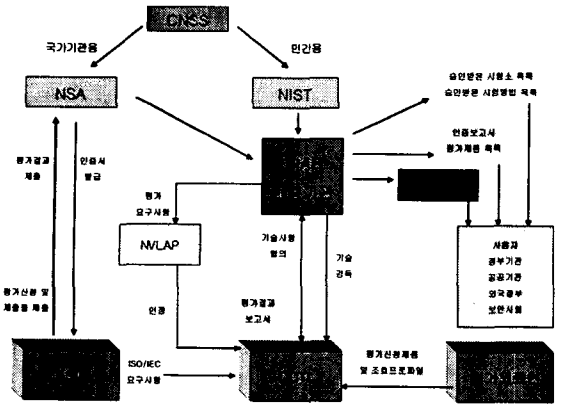
(나) 평가 인증체계

미국의 평가 ·인증체계의 참여자들은 인증기관인 NIAP, 인정기관인 NVLAP, 민간평가기관(CC Testing Laboratory, CCTL)과 평가신청인으로 구성되며 이들의 관계는 아래 <그림 2-1>과 같다.

---

5) "ARRANGEMENT on the Recognition of Common Criteria Certificates In the field of Information Technology Security, May 2000 http://www.commoncriteria.org/registry/ccra-may00.pdf, 2003년 3월 17일 방문 확인

6) http://www.niap.nist.gov 2003년 3월 17일 방문 확인. 우측의 "About NIAP"에서 상세히 설명하고 있음.



<그림 2-1> 미국의 평가 인증 체계

(2) 캐나다

(가) 평가 인증제도 구축

캐나다 정부는 평가 인증제도 품질과 평가기관의 기술력 향상을 위하여 노력하고 있으며 국제공통평가기준(CC) 기반의 국제공통평가인정협정(CCRA) 요구사항 보다 훨씬 더 높은 수준의 요구사항들을 참여기관들에게 요구하고 있다. 캐나다 정부는 인증된 제품의 사용을 권장하기 위하여 인증제품 목록(Information Technology Security Product Pre-qualification List, IPPL)을 작성하여 정부의 IT제품 획득과정에 활용할 수 있는 제도를 마련하였다. 또한 새로운 평가기술 개발을 위하여 생체특징을 이용한 사용자 인증 제품 평가기술, 스마트카드 평가기술 및 암호제품 평가기술 등 다양한 분야의 평가기술을 개발하였다. 또한 평가기관의 공정성 및 숙달된 평가자 양성을 위하여 정부는 평가자 교육과정을 개설하여 운영하고 있다. 또한 평가전문가 육성을 위하여 평가자 인증절차를 개발하여 교육과정 이수 후 등급별 시험을 통하여 등급별 평가전문가 인증서를 발급하여 평가기관의 품질을 보증하는 제도를 마련하였다. 이는 다른 어떠한 국가의 평가 인증제도보다 평가기관에게 높은 수준의 요구사항을 제시하는 것이다.

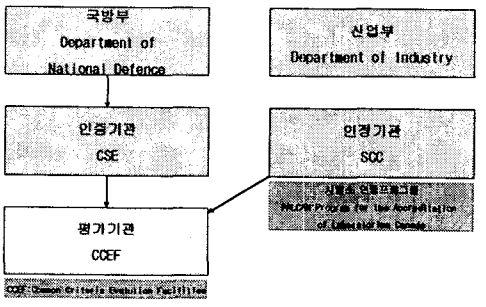
(나) 정부의 인증제품 활용

캐나다 정부는 인증제품의 활용을 극대화하기 위하여 정부차원의 정책을 수립하여 고시한 바 있다. 캐나다 정부는 인증제품 목록을 작성하여 정부기관에서 IT 제품을 획득하고자 할 경우, 이 목록에 명시된 제품을 구매할 것을 권장하고 있다. IPPL은 캐나다 IT 제품 평가 인증 스킴에 의하여 평가를 받은 제품과 CC 기반의 상호인정협정 인증서발행국가에서 인증서를 발행한 제품, 그리고 CMVP(Cryptographic Module Validation Program)에 의하여 인증된 제품을 포함한다.

캐나다 정부는 보안기능이 검증된 제품의 획득을 권장함으로써 신뢰할 수 있는 IT 시스템 구축과 안전한 컴퓨팅 환경의 구축을 목적으로 한다.

(다) 평가기술력 확보

통신 보안국(CSE :Communications Security Establishment)는 국제공통평가기준(CC) 기반의 신 평가기술 확보를 위하여 생체특징을 이용한 사용자인증제품 평가, 스마트카드 평가[7] 및 암호제품 평가기술 확보를 위한 연구를 진행 중이다.



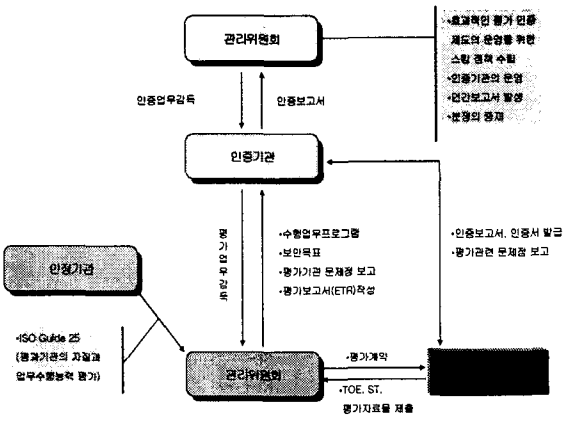
<그림 2-2>캐나다의 평가, 인증 체계

7) http://www.cse-cst.gc.ca/en/services/common_criteria/protecti 2003년 3월 27일 방문 확인, 위 사이트에 가면, 스마트 카드에 대한 평가 결과를 볼 수 있다.

(3) 영국

(가) 개요

7개 대륙의 39개국에 위치하고 있으며, 32만명에 연간 228억불의 예산을 사용하고 있는 영국 국방성의 IT 제품에 대한 안전성을 보장하기 위한 일환으로 시작되었다. 하지만 그 범위는 영국 정부 및 업체, 유럽 그리고 CC 기반 평가, 인증 제도를 마련하면서 세계적으로 확대되었다. 영국 정부의 IT 보안을 책임지고 있는 조직도는 다음과 같다. 8)



<그림 2-3> 영국의 평가, 인증 체계9)

(나) 연 혁

영국의 IT 제품 평가 인증제도는 크게 4단계로 구분할 수 있다. 그 구분은 평가 인증제도가 확대되는 범위에 따라서 단계별로 구분하였다.

- 1단계(국방성) : 초기에는 영국의 국방성내에서 지금의 인증기관인 CESG를 중심으로 시작하였으며 국방성내에만 적용되었다. 당시 세계적으로 유일하게 평가 인증 제도를 도입한 국가는 TCSEC을 사용한 미국이 전부였다.

- 2단계(영국정부) : 국방성에서 확대되어 영국 정부 전체에 적용할 수 있는 영국의 평가 인증 스킴을 개발하고 발표하면서 시작되었다. 국방부내에서는 'DCI GEN 125/92' 문서를 근거로 하였으며 기타 정부에서는 'HMG Compusec Memo 10 Issue 1'를 근거로 하였다. 당시 미국은 TCSEC(Orange Book), 독일 ZSIEC, 프랑스 SCSSI(Blue-White-Red Book)를 활용하였으며 영국은 DTIEC(Green Book)를 이용하여 IT 제품을 평가하였다.

- 3단계 (Information Technology Security Evaluation Criteria, ITSEC) : 영국, 독일, 프랑스, 네덜란드 등 4 개국은 각 국에서 사용하는 3개의 평가기준을 조화시킨 ITSEC이라는 단일의 평가기준을 개발하였다.
ITSEC 버전 1.0이 1990. 5월에 발표되었으며 버전 1.2가 1991. 6월에 발표되었고 ITSEC을 이용한 평가방법론인 ITSEM이 1993년 발표되었다. 단일의 평가기준과 평가방법론이 발표되면서 IT 제품의 평가결과를 상호 인정할 수 있는 기반이 마련되었다. CC 기반의 상호인정협정은 EALI에서 EAL4등급의 평가결과를 상호 인정하는데 반해, ITSEC 기반의 상호인정협정은 E1에서 E6의 모든 등급에 적용된다. 유럽의 국가들은 각 국가에서 ITSEC을 이용한 평가 결과를 상호 인정하기 위한 ITSEC 기반의 상호인정 협정을 체결하였으며 현재 12개의 유럽 국가들이 참여하고 있다.

- 4단계(CC) : 3단계에서는 단순히 유럽의 국가들간의 상호인정협정을 체결하였으나 4단계에서는 미국, 영국 등 평가 선진국들이 세계적인 상호인정협정을 체결하기 위하여 국제공통평가기준(CC)를 개발하였다. 현재 국제공통평가기준(CC)는 ISO 표준으로 제정된 버전 2.1를 사용하고 있으며, EALI에서 EAL4등급까지의 평가 제품만을 상호 인정한다.

영국은 약 10여년이 넘도록 평가, 인증 제도를 운영하면서 250여개의 IT 제품을 평가하였다. 2000년에서 2001년 7월 현재까지 5개의 제품과 2개의 보호프로파일을 국제공통평가기준(CC) 기반으로

8) 상호인정협정 관련 국외 동향 분석, 한국정보보호진흥원, 2001.12.

9) http://www.cesg.gov/uk/assurance/iacs/itsec/documents/formal-docs/index.html
2003년 3월 27일 방문 확인, 위 사이트에서 UK스킴을 다운 받아 읽어보면, 그림과 같은 틀을 얻을 수 있음.

평가, 인증하였다.

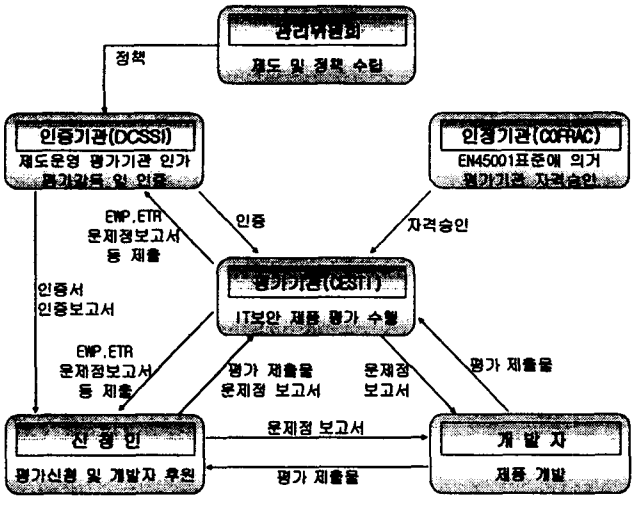
(4) 프랑스

(가) 평가 인증 체계

프랑스의 IT 제품 평가를 담당하고 인증기관의 역할을 수행하던 SCSSI가 정보시스템보안센터(DCSSI-Direction centrale de la securite des systems d information)[10]로 명칭이 수정되었으며 이에 따른 세부 조직 개편이 진행되었다.

민간평가기관 인정 절차는 크게 둘로 나뉜다. 하나는 COFRAC에서 시행하는 시험실 인정절차로 유럽의 표준인 EN 45001 또는 ISO 가이드 25를 사용하여 시험실의 기본 자격을 갖추고 있는지를 시험한다. 예를 들어 시험실이 재정적으로 안전하며, 평가자들이 경제적으로 안정되어 있어 어떠한 압력에도 평가결과에 영향을 미치지 않는다는 등의 심사를 하게 된다.

인증기관은 시험실로 인정받은 기관이 IT 제품의 보안기능 안전성 평가를 시행할 수 있는 기술을 보유하고 있는지를 심사한다. 이러한 심사에 통과한 시험실만이 평가 인증제도에서의 IT 제품 보안기능을 평가할 수 있는 민간평가기관으로서의 면허증을 부여받는다.



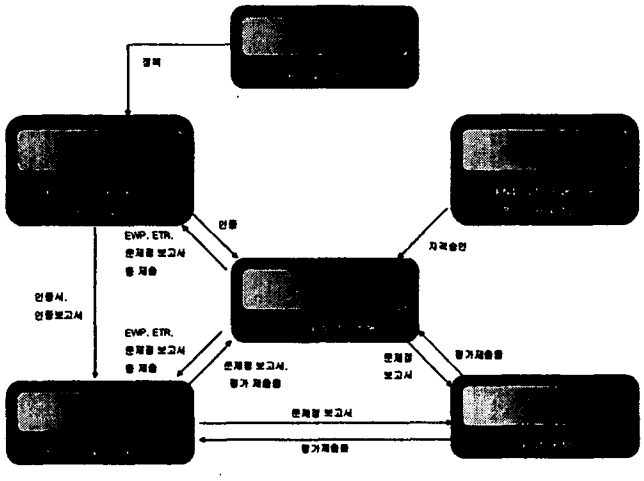
<그림 > 프랑스의 평가, 인증 체계

(나) 민간평가기관

프랑스에는 Algoriel, AQL, CEACI(CNES-SOREP), CEA/LETI, SERMA Technologies 등 5개의 민간평가기관이 있다. 프랑스에서는 특별히 스마트카드를 평가할 수 있는 평가기관을 별도로 지정하여 운영하고 있으며, 이들은 CEACI, CEA/LETI, SERMA Technologies 등 3개 민간평가기관이다.

(5) 독일

독일의 평가 인증제도가 유럽에서는 가장 짧은 역사를 가지고 있으며 알려진 정보가 거의 없는 상태이다. 1989년 IT 제품 보안기능 평가기준을 처음으로 발표하였으며, 1990년에 평가 메뉴얼을 발표하였다. 그 후 1991년 BSI 법에 의하여 현 인증기관인 BSI(GISA-German Information Security Agency가 BSI의 영문 공식 명칭)[11]가 내무부 산하에 설립되었다. BSI는 6개의 부서로 구성되어 있으며 약 360여명의 직원이 근무하고 있다. BSI의 임무는 크게 3개로 구분되며 보안위험 연구, 평가기준 개발 및 BT 제품 평가 등이다. 독일은 1995년 영국과 처음으로 인증된 제품의 국가간 상호인정협정을 체결하였으며 1997년 프랑스와 국가간 상호인정협정을 체결하였다. 1998년에는 ITSEC 기반의 상호인정협정을 체결하였다.



<그림 2-5>독일의 평가, 인증 체계

10) http://www.ssi.gouv.fr/fr/dcssi/index.html 2003년 3월 27일 방문 확인

11) http://www.bsi.bund.de/english/index.htm 2003년 3월 27일 방문 확인

2.2. CCRA-CAP 준비국인 한국의 분석과 문제

(1) 우리나라의 CCRA관련 평가, 인증 제도 연혁

1995년 8월	정보화촉진기본법 제정 공고 - 제14조 : 한국정보보호센터의 설립·운영 - 제15조 : 정보보호시스템에 관한 기준고시 등
1995년 12월	정보화촉진기본법 시행령 제정 공포 - 제15조 : 한국정보보호센터의 임무제4항 : 정보보호시스템의 연구·개발 및 시험·평가제5항 : 평가기준의 제정 - 제16조 : 정보보호시스템 보완 등
1998년 2월	침입차단시스템 평가기준 및 지침서 고시(정보통신부 고시 1998-20) 침입차단시스템 평가제도 시행
1998년 5월	침입차단시스템 평가기준 보안기능 해설서 발간
1998년 11월	침입차단시스템 평가기준 보증 해설서 발간
2000년 2월	정보보호시스템 침입차단시스템 평가기준 개정·고시(정보통신부 고시 2000-14) 정보보호시스템 평가·인증지침 고시(정보통신부 고시 2000-15)
2000년 7월	정보보호시스템 침입차단시스템 평가기준 고시(정보통신부 고시 2000-62)
2001년 4월	정보보호시스템 평가·인증지침 개정·고시(정보통신부 2001-24)
2002년 8월	정보보호시스템 공통평가기준 고시(정보통신부 고시 2002-40) 정보보호시스템 평가·인증지침 개정·고시(정보통신부 2002-41)
2003년 진행	CC 3.0 버전을 한글화하여 국내 정보보호시스템 공통평가기준에 반영 CC 3.0 버전에 추가 또는 수정된 내용을 이미 개발된 공통평가기준 해설서에 반영 등의 연구 과제를 진행 할 예정임[12]

<표 2-1> 우리나라의 평가, 인증 제도 연혁

(2) CCRA-CAP 주요국과 우리나라의 평가, 인증 제도 비교

CCRA관련 주요 선진국인 미국, 캐나다, 영국, 독일, 프랑스는 일찍이 관련법규를 근거로 인증기관, 인정기관, 평가기관을 담당할 기관을 선별하고 각 기관별 스킴 및 체계를 갖추어 나가고 있다. 이에 반하여, 우리나라는 아직 이렇다할 명확한 기관의 역할 구분 등이 이루어지지 않고 있다. 특히, 관련 법제를 통한 제도적 뒷받침이 부족한 현실이다. 아래 < 표 2-2>는 CCRA관련 선진 5개국과 우리나라의 평가, 인증 체계에 대한 비교를 통하여, 오늘날 우리나라가 시급히 준비해야할 과제에 대한 시사점을 얻을 수 있다.

<표 2-2> CCRA-CAP주요국과 한국의 평가, 인증 체계

국가	인증기관	인정기관	평가기관
미국	-NSA (정부), NIAP (민간)	-NIAP	- 정부기관 NSA(National Security Agency) - TTAP하의 민간기관 ·Arca Systems Inc.(www.arca.com) ·Computer Sciences Corp.(www.csc.com) ·Cygnacom Solutions(www.cygnacom.com) ·National Software Testing Laboratories (www.nstl.com) ·Science Applications International Co. (www.saic.com) ·Booz, Allen, Hemilton(www.bah.com) ·CoAct Incorporated(www.coact.com) - 국제공통평가기준기반의 민간평가기관(CCTL) ·Arca Systems Inc.(http://www.arca.com) ·Computer Sciences Corp.(www.csc.com) ·Cygnacom Solutions(www.cygnacom.com) ·Science Applications International Co. (www.saic.com) ·Booz, Allen, Hemilton(www.bah.com)
캐나다	-CSE(Communications Security Establishment)	-SCC(Standards Council of Canada)	- 정부기관 ·CSE(Communications Security Establishment) - 민간기관 ·CGI Information Systems and Management Consultants Inc. ·DOMUS IT Security Lab. ·EWA-Canada

12) http://www.kisa.or.kr/admin_bulletin/2003_enterprise_03.html 2003년 3월 19일 방문 확인

13) 국내정보보호시스템 평가, 인증 제도 관련 기관 역할 분석 보고서, 한국정보보호진흥원, 2002.12.

영국	-CESG(Communications-Electronics Security Group)	-CESG(Communications-Electronics Security Group)	- 정부기관 ·CESG(Communications-Electronics Security Group) - 민간기관 (CLEF : Commercial Licensed Evaluation Facility) ·Admiral Management Services Ltd. ·EDS Ltd. ·IBM Global Services ·Logica UK Ltd. ·Syntegra
독일	-정부기관: BSI -민간기관 ·T-Systems ISS GmbH ·TUViT(TV Information-stechnik GmbH)	-BSI	- 정부기관 ·GISA(Germen Information Security Agency) - 민간기관(ITSEF : Information Technology Security Evaluation Facility) ·IABG(Industrieanlagen-Betriebsgesellschaft mbH Abeteilumg ITE) ·CCI(Competence Center Informatik GmbH Prufstelle IT-Sicherheit) ·debis Systemhaus Information Security Services GmbH ·Tele-Consulting GmbH ·TUV Informationstechnik GmbH ·TUV Nord e.V. ·Vossloh System-Technik GmbH
프랑스	-DCSSI(Direction centrale de la securite des systems d'information)	-COFRAC	- 정부기관 ·DCSSI(Direction Center for Security of Systeme Information) ·CELAR/CASSI - 민간기관(ITSEF) ·CEA-LETI ·AQL(Alliance Qualite Logiciel) ·SERMA Technologies ·ALGORIEL Consulting ·CEACI(CNES-SOREP) ·Oppida
한국	-국가정보원(NIS:National Intelligen- ce Service)		- 정부기관 ·한국정보보호진흥원(KISA:Korea Information Security Agency)[13]

(3) 인증서 발행국(CAP)가입을 위한 개선안 도출

첫째로 인력 부분을 들 수 있다. 인증서 발행국(CAP)으로 가입하기 위해서는 국내에 국제공통평가인증협정(CCRA)관련 전문가가 필요하다. 특히, 현재는 국제공통평가인증협정(CCRA)관련 배경지식을 습득하고 오랜 시간동안 국제공통평가인증협정(CCRA)관련 일에만 종사해온 전문가 양성과 국제 회의(ICCC 등)에 계속적인 참석을 통한 국제공통평가인증협정(CCRA)관련 외국 전문가와의 대화 채널을 확보한 전문가 발굴과 확보 그리고 교육이 가장 시급한 현실이다. 그럼에도 불구하고 최근 우리나라에서는 전문가의 양성보다는 관련 기관의 전문가들을 교체하는 관례를 따라 인력을 재배치하여, 국제공통평가인증협정(CCRA)관련 기관 등 에서도 국제공통평가인증협정(CCRA)관련 연구와 대외 협력을 해온 전문가를 만나기가 쉽지 않은 현실이다. 또한 인증서 발행국(CAP)가입에 있어서는 기술적인 이해뿐만 아니라 국가 체계의 구축과 함께 국제 협력과 협상의 전문가도 중요하다. 2000년 이후 국제공통평가인증협정(CCRA)에 가입한 국가 중, 인증서 수용국(CCP)에서 인증서 발행국(CAP)으로 전환한 국가는 하나도 없다. 따라서 인증서 수용국(CCP)으로서 국제공통평가인증협정(CCRA)에 가입조차 하지 않은 우리나라의 경우, 그 어느 때보다 대외협상력이 강조된다고 생각된다. 그럼에도 국제공통평가인증협정(CCRA)가 가지고 있는 기술적인 특성으로 현재 기술 중심적인 엔지니어들의 연구가 주를 이루어왔다. 하루빨리 국제공통평가인증협정(CCRA)가입을 준비하는 인적구성을 기술인과 대외 교섭력을 가진 사람으로 적절히 배치하여 함께 지혜를 모아야 한다.

둘째, 국제공통평가인증협정(CCRA) 가입에 따른 각 이해 당사자들의 이견을 좁히고 국익을 우선으로 하는 정책이 준비되어야 한다. 국제공통평가인증협정(CCRA)의 조기 가입은 정보보호 산업에 대한 경쟁력이 없는 국내 산업의 시장 잠식과 경쟁력 약화 등을 가져올 수 있다. 또한 국제공통평가인증협정(CCRA)의 더딘 가입은 국내 정보보호 산업의 글로벌 스탠다드와 국제적인 경쟁력 구축이라는 국익을 저해하는 요소로 작용될 수 있다. 따라서 현재 국제공통평가인증협정(CCRA)관련하여 다양한 이견을 가지고 있는 국가 기관과 기업체 등에서 책임있는 담당자들을 중심으로 하루빨리 국제공통평가인증협정(CCRA)관련

스킴 1번에 대한 확립과 이를 근거로 할 수 있는 관련 법규의 정비 및 체계 구축이 시급한 실정이다.

셋째, 스킴 1번의 도출을 위해서는 해외 사례를 충분히 검증하는 과정을 거쳐야 할 것이다. 본 연구에서는 우리나라의 특성상 각 기관의 협력과 견제 그리고 균형을 위하여, 미국과 같이 관련법규를 근거로 국제공통평가인증협정(CCRA)의 대표기관으로 NIAP와 같은 기관을 설립하는 스킴안을 제안한다. 이는 조속한 인증서 발행국(CCRA-CAP)으로의 지위 확보라는 국익을 위하여, 각 기관의 장점을 최대한 수용하는 스킴 구조란 점과 현재 각 기관들과 이해 당사자들의 이견으로 국익과 무의미한 논쟁만이 무성한 점 등을 고려하여 각 기관의 협력체를 구축하여야 한다고 판단하였기 때문이다. 특히, 미국의 경우, 1997년 8월 22일 PL 100-235(Computer Security Act of 1987)에 근거하여 NIST와 NSA가 공동으로 국가정보보증협의체(NIST-National Information Assurance Partnership)를 구성하여 현재 모범적으로 운영하고 있다. 우리나라는 각 기관의 전문성을 살리고 각 기관의 장점을 통한 시너지를 확보하기 위하여 NIAP와 같은 형태의 국가 스킴을 도출하는 것이 효과적일 것으로 사료된다. 또한, 한 기관이 평가기관, 인증기관, 인정기관의 모든 역할을 단일 기관으로 맡을 것이 아니라, 국가의 인프라적 성격을 가지는 정보보호제품에 대해서는 관련 기관이 맡고, 개인 등 민감도가 덜한 정보보호제품에 대해서는 다른 관련 기관이 맡는 식의 이원화 정책도 효과적인 것으로 판단된다. 특히, 이부분에서는 평가기관(정부, 민간)에서 고려대 볼 수 있을 것으로 사료된다. 아직, 국내에 관련 법규에 근거한 각 기관의 명확한 정의와 역할이 결정나지 않은 여건에서 미국의 예를 중심으로 하나의 시나리오적인 접근으로서 국제공통평가인증협정(CCRA)에 가입하기 위한 국내 관련 기관의 역할과 정의 등에 관한 국내 스킴 1을 도출해보았다.

3. 결론

국제공통평가인증협정(CCRA)에 가입하여 빠른 시간 안에, 인증서 발행국(CAP)의 지위를 확보하여야 국내 평가 인증 기술력과 국내 기업의 해외 판로 그리고 국제 경쟁력 확보에 긍정적인 요인으로 작용할 수 있을 것이다. 하지만, 현재 2000년 이후 국제공통평가인증협정 인증서 수용국(CCRA-CCP)으로 가입한 8개국(네덜란드, 이탈리아, 그리스, 핀란드, 노르웨이, 스페인, 이스라엘, 스웨덴) 중 한 나라도 인증서 발행국(CAP)으로 지위를 확보하지 못한 것으로 미루어, 우리나라의 인증서 발행국(CCRA-CAP) 지위 확보는 단기간에 얻기 어려운 과제임을 알 수 있다. 따라서, 현재 국제공통평가인증협정(CCRA)가입을 위한 기술적 제도적 국내 스킴 개발 및 관련 법제 마련의 중요성은 우리가 인증서 발행국(CCRA-CAP)으로 가기위해 기본적으로 이행하여야 할 요구사항이다. 따라서 국제공통평가인증협정(CCRA) 가입 후, 빠른 시간안에 인증서 발행국(CAP) 지위를 확보하기 위해서는 가입을 위한 선제조건 보다 더 중요한 것으로 국제공통평가인증협정의 실질적인 운영과 내부 사정에 밝은 전문가의 양성이라고 사료된다. 그 이유로는 국제공통평가인증협정이 가입국들의 만장일치로 의견조정이 이루어지며, 실질적인 투표권(Voting Power)의 영향력이 클 것이 여겨지기 때문이다. 따라서 국제공통평가기준(CC)과 관련한 국제회의(ICCC 등) 등에 꾸준한 참석과 해외 관련 전문가들과 대화 채널을 확보한 국제협력 전문가의 발굴과 양성을 위해 관련 기관이 힘써야 한다. 그럼에도 불구하고, 공무원들의 정기적인 자리이동과 관련 연구기관 등의 담당자의 이동 등으로 업무 공백이 예상되어지는 우리나라는 현재, 국내의 국가 스킴 개발 등에 참여한 엔지니어 중심의 국제회의 참석과 국제공통평가인증협정(CCRA) 가입 준비 등으로 인하여 대외 협력을 통한 국익 추구에 허점이 발견되고 있다. 이를 시정하기 위하여서는, 대외 교섭력 등 국제무대에서 국익을 위해 활동한 경험이 있는 국가 기관 및 담당 전문가와 기술적으로 국제공통평가인증협정을 연구한 담당자간의 협의체 등을 통해, 시너지를 얻을 수 있도록 하여야 한다. 이를 위하여서는 국제공통평가인증협정(CCRA)의 창구 역할을 할 기관의 확정이 필요하며, 미국의 예와 같이 NSA와 NIST에서 각 전문가 들이 모인 NIAP의 설립과 같은 예도 충분히 검증하여, 우리나라의 국가 스킴 개발에 반영할 만한 사례라고 여겨진다.

본 연구는 인터넷을 통하여 국제공통평가인증협정(CCRA)에서 투표력과 대외 교섭력 등에서 막강한 힘을 보유하고 있을 것으로 예상되는, 국제공

통평가인증협정인증서발행국(CCRA-CAP) 중 미국, 캐나다, 영국, 독일, 프랑스와 같은 주요 5개국의 국가 스킴을 살펴보고, 현재 우리나라의 국가 스킴과 비교함으로 우리나라에 국가 스킴 개발에 시사점과 국가 스킴 개발의 시나리오적인 개발안을 모색해 볼 수 있었다는 점에서 그 의미가 있다고 사료된다. 보다 구체적으로 우리나라의 국가정보원과 정보통신부 그리고 한국정보보호진흥원이 현재 주도적으로 국제공평평가인증협정에 대한 연구를 수행하고 있으나, 산업자원부, 외교통상부 등의 대외협력전문가들의 의견과 조언을 수렴하는 과정이 추가된다면 보다 효과적일 것으로 여겨진다. 또한, 한 기관만이 평가기관, 인정기관, 인증기관을 맡기보다, 자국의 보안 등 국가 인프라적 성격인 공공 기관에 설치될 정보보호제품에 대해서는 국가정보원이, 일반적인 국민이 사용하는 정보보호제품에 대해서는 정보통신부 등이 이원화하여 평가를 담당할 수도 있다. 다양한 시나리오와 현실적인 여건(기술적 평가 인력 확보 등)을 감안하여, 하루 빨리 각 기관의 역할 분담이 이루어져야 할 것으로 사료되며, 본 연구를 통하여서는 각 기관의 전문가들의 참여를 통한 미국의 NIAP와 같은 형식의 국가 스킴이 다양한 이해집단간의 의견조정과 빠른 시간안에 국제공통평가인증협정 인증서발행국(CCRA-CAP)으로 진입을 희망하는 여건에서 최대한의 시너지 효과를 얻기 위함 등을 감안하여 국가 스킴이 개발되었으면 하는 방안을 도출해 보았다.

[참고문헌]

1. 국내 문헌

"국내외 정보보호시스템 평가 가이드", 한국정보보호센터, 2002.12.

"국내정보보호시스템 평가, 인증 제도 관련 기관 역할 분석 보고서", 한국정보보호진흥원, 2002.12.

"상호인정협정 관련 국외 동향 분석", 한국정보보호진흥원, 2001.12.

"정보보호시스템공통평가기준", 정보통신부, 2002. 7.

"CCRA 최근동향 및 향후 전망", 정보보호뉴스(통권 35호), 한국정보보호센터, 이유신, 2000.8.

"CyberSpace의 법과 기술", 고려대학교 CIST 정보보호 정책연구회, 북카페, 2003. 1.

2. 해외 문헌

"The Common Criteria Recognition Arrangement",1st International Common Criteria Conference, Louis Giles, May,2000

"Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security", CCRA, May, 2000

"German IT Security Certificates ITSEC", BSI, March, 2000

"Common Criteria for Information Technology Security Evaluation User Guide", p7.

3. 웹 사이트

http://www.commoncriteria.org

http://www.niap.nist.gov/

http://www.itsec.gov.uk

http://csrc.nist.gov/cc/CC-v2.1.html

http://www.cesg.gov.uk/assurance/iacs/itsec/documents/formal-docs/index.htm

http://www.ssi.gouv.fr/fr/dcssi/index.html

http://www.bsi.bund.de/english/index.htm