通信情報保護學會誌
第 10 券 第 3 號, 2000. 9

국제공통평가기준(CC)기반의 상호인정협정(MRA) 동향 분석

이 유 신*, 이 경 구**

요 약

인터넷을 통한 기업간(B2B) 전자상거래 시장규모가 올해 17조원대에 이르고, 기업과 소비자간(B2C) 전자상거래 시장규모 또한 1조원을 넘어서는 등 전체 국내 전자상거래 시장규모가 18조원을 넘어 설 전망이다. 이는 정보통신시스템에 대한 사회 전반의 의존도가 한층 증대하고 있음을 보여주는 단적인 예라 할 수 있다. 오늘날 인터넷 사용이 보편화되고 전자상거래의 규모가 커져 갈수록 정보보호시스템에 대한 신뢰성 및 안전성에 대한 입증 노력 또한 더 강하게 요구되고 있는게 사실이다. 특히, 안전성이 입증되지 않은 취약한 정보보호시스템을 사용한 시스템 구축은 오히려 그 위험성을 증가시킬 수 있음을 최근의 많은 해킹사례를 통해 경험한바 있다. 향후 예견되는 이러한 엄청난 사회적 손실을 막기 위한 제도적 노력의 일환으로 미국, 영국, 독일, 프랑스 등 선진국에서는 10여년 전부터 자국의 환경에 적합한 평가기준을 마련하여 정보보호시스템을 평가해 오고 있다. 본고에서는 정보보호시스템 평가제도와 관련하여 최근의 국제동향과 그에 따른 국내 대응방안을 모색해 보고자 한다. 특히, 정보보호시스템 평가를 위한 국제기준인 CC(*Common Criteria*)와 이를 기반으로 맺어진 MRA(*Mutual Recognition Arrangement*)의 전개과정을 살펴보고, 유럽의 상호인정협정인 ITSEC-MRA의 출범배경과 올 5월에 새롭게 출범한 CC-RA체제의 특징적인 모습을 고찰해 보고자 한다.

Ⅰ. 서 론

오늘날 정보통신기술의 발달로 사회 각 분야에서 구축·운영되는 공공 및 민간분야 정보통신시스템의 안전성 확보의 필요성 증대와 정보통신시스템에 의하여 전자적으로 처리되는 정보량이 증가함에 따라 주요 정보통신시스템에 대한 사회 전반의 의존도 또한 이에 상응하여 증대하고 있다. 특히, 주요 정보통신시스템의 안전운영에 문제가 발생할 경우 국가사회의 주요 기능마비로 이어져 막대한 손실 및 혼란이 초래될 것은 불을 보듯 뻔하다. 인터넷 사용이 보편화되고 전자상거래의 규모가 커져갈수록 정보보호시스템에 대한 신뢰성 및 안전성에 대한 평가는 그래서 더욱 요구된다.

올해 초 발생한 세계 최대 인터넷 포털사이트인 Yahoo를 비롯한 CNN, 아마존닷컴 등 유명사이트들의 해킹사건에서 알 수 있는 바, 안전성이 입증되지 않은 취약한 정보보호시스템을 사용한 정보시스템 구축은 오히려 그 취약성을 증가시키는 위험성을 내포하고 있음을 의미하고 있어 정보시스템의 안전성 및 신뢰성 검증이 새삼 중요해 지고 있다. 특히, 전 세계적으로 전자상거래의 비중이 날로 높아지고 있는 현 상황에서 불안전한 시스템 구축은 그 기반마저 무너질 수 있다는 불안감을 가중시키고 있다.

그 위험으로부터의 예방 노력을 위한 제도적 일환으로 미국, 캐나다, 영국, 독일, 프랑스 등 선진국에서는 10여전부터 자국의 환경에 적합한 평가기준을 마련하여 정보보호시스템을 평가해 오고 있다[1].

* 한국정보보호센터 평가기준팀 연구원(yueshin@kisa.or.kr)
** 한국정보보호센터 평가기준팀 팀장 (kglee@kisa.or.kr)

향후 다자간 국제무역에서만 불어온 개방화의 물결이 머지않아 정보보호산업에서도 예외 없이 적용되어 이른바 'Security Round'가 거칠게 휘몰아칠 것으로 예상되고 있다. 아울러, 전자상거래와 사이버스페이스 상에서의 활동이 증대되어 가면서 정보보호제품의 활용이 늘어나고 이에 따른 정보보호제품의 국가간 교역이 촉진될 것으로 전망되고 있다. 한편, 국내 정보보호산업은 초창기 보안 솔루션의 수입 제품 의존 형태에서 현재는 자체 개발의 비중이 점점 늘어나는 추세로, 통합 보안솔루션업체로의 지향 및 전략적 제휴 등으로 국내 보안 솔루션 제공뿐만 아니라 글로벌화에도 박차를 가하고 있다.

96년부터 형성되기 시작한 국내 정보보호시장은 바이러스백신 분야를 제외하고는 외국산제품들이 주종을 이루며 판매되었으나, 98년 9월 이후 한국정보보호센터(KISA)로부터 침입차단시스템(Firewall) 평가를 받은 제품이 출시되면서 보안솔루션 제품들이 다양하게 등장하였으며, 현재는 통합 보안솔루션 시장으로 확대되어 가고 있는 추세이다[2]. 정보보호시스템 평가제도가 안전성과 신뢰성을 지닌 우수한 정보보호제품 개발을 유도함으로써 정보보호산업 육성에 기여하고, 안전한 정보보호시스템 구축에 일조하여 궁극적으로는 '건강한 정보사회'를 이룩하는 유용한 제도로서의 큰 틀을 형성한다는 점에서 정보보호시스템 평가제도와 관련된 최근의 국제적 흐름 및 국내 대응방안을 분석하는 것은 중요하며, 향후 정보보호제품과 관련된 국가간 상호인정의 중심 축이 될 국제공통평가기준(CC)기반의 상호인정협정(MRA) 동향은 국내 정보보호시스템 평가제도에 큰 영향을 미친다는 점에서 의미 있다 할 것이다.

이러한 흐름을 바탕으로 본고에서는 우선 제2장에서 정보보호시스템 평가를 위한 국제기준인 국제공통평가기준(CC) 개발연혁을 살펴보고, 제3장에서는 1998년 5월, 5개국 6개 기관간 CC 버전 2.0을 기반으로 맺어진 상호인정협정을 파악해 볼 것이다. 이어 제4장에서는 유럽의 상호인정협정인 ITSEC-MRA의 출범배경 및 주요내용을 살펴보고, 제5장에서는 올 5월에 출범한 새로운 체제의 CC-RA에 대해 분석한 후, CC-RA출범에 따른 국내 대응방안과 그 결론을 제6장과 제7장에 각각 제시하고자 한다.

II. 국제공통평가기준(CC) 개발 연혁

1. CC 개발 필요성

국제공통평가기준(CC : Common Criteria)은 정보보호제품의 평가에 관한 기준을 국제적으로 단일화하려는 노력의 산물이라 할 수 있다. 이러한 단일화의 움직임은 일반적인 국제표준화 활동과 유사하다. 즉, 정보보호 기술의 시장성 확보의 기초적인 작업으로 기술개발의 방향성을 제공하면서 시장의 규모를 세계적으로 확대하기 위한 토대 마련 역할을 한다. 아울러, 수요자 측면에서는 제품에 대한 불확실성을 감소시키는 효과를 가져옴과 동시에 정보통신시장 기반이 네트워크라는 점에서, 국제적인 정보통신시장에서의 균일화된 정보보호의 필요성이 더욱 요구된다고 할 수 있다.

한편, 이러한 국제 표준화의 움직임은 정보보호산업이 상대적으로 시장규모가 작다는 제약을 극복하는데 중요한 돌파구가 되기도 한다. 국제적으로 공통의 평가기준을 마련하고, 이에 기초하여 평가를 통과한 제품에 대하여 국가간에 상호인정해줌으로써 협소한 국내시장을 확대해 나갈 수 있는 것이다. 평가기준의 단일화 움직임이 유럽에서 제일 먼저 시작하게 된 배경 또한 이러한 이유에 근거한다고 할 수 있다. 수요자 입장에서 볼 때도, 글로벌 네트워킹으로 국제적 공통기준의 필요성을 제공하는 동시에 국제공통기준을 전 세계적으로 급속하게 확산시키는 요인이 되기도 한다. 다른 산업의 글로벌화와는 달리 정보산업의 기반인 네트워크의 특성은 일단 국제표준으로 채택되면, 이를 전 세계적으로 급속하게 확산시키는 동인으로 작용하는 것이다.

결과적으로, 각 국의 서로 상이한 평가기준을 단일화하고자 하는 요인은 근본적으로 정보의 글로벌화에 기인한다고 할 수 있다. 한 국가내의 정보화를 촉진하기 위해서 정보보호제품의 평가제도가 중요한 것처럼, 글로벌 네트워킹을 중요한 특징으로 하고 있는 범 지구적 정보화를 촉진시키기 위해서는 평가기준의 국제적 단일화는 필수적으로 요청된다 할 것이다.

2. CC 개발 연혁

정보보호시스템을 평가하기 위한 평가기준 개발 역사는 1983년 일명 "Orange book"으로 불리는 미국의 국방성(DoD)표준인 TCSEC에서 찾을 수 있다. 이후 1990년 영국, 독일, 프랑스, 네덜란드 등 유럽 4개국의 ITSEC 버전 1.0 개발, 1993년 캐나다의 CTCPEC 버전 3.0 개발 순으로 전개되었다[3].

이러한 평가기준의 개발 노력은 정보보호시스템을 직접 평가하기 위한 사전단계로서 그 의미를 지니지만, 한편 각국의 서로 다른 평가기준의 시행은 비용과 시간의 과다 소모 등의 문제점을 야기시켰고, 이를 타개하기 위한 노력의 일환으로 1993년 6월 선진 6개국을 중심으로 국제공통평가기준(CC) 개발을 시작하여 CC 버전2.0을 1998년 5월에 제정하였다.

이후 개정 작업이 계속되어 1999년 6월 8일 CC 버전2.1이 ISO/IEC 15408 국제표준으로 채택되었으며, 이 과정에서 기존의 CC버전 2.0의 체계가 서론 및 일반모델(Introduction and general model), 보안기능 요구사항(Security functional requirements), 보증요구사항(Security assurance requirements), 부록(Annexes) 등 네 파트에서 서론 및 일반모델(Introduction and general model), 보안기능요구사항(Security functional requirements), 보증요구사항(Security assurance requirements) 등 세 부분으로 변경되어 CC버전 2.1로 모습을 바꾸었다[4].

내용상 CC버전 2.1과 CC버전 2.0의 차이점은 거의 없으나, ISO/IEC 15408 획득 과정에서 표준 문서로의 수정이 가해져 국제표준으로 채택되었다.

이러한 개발과정을 통해 완성된 국제공통평가기준(CC) 버전 2.1은 2000년 5월 새롭게 출범한 CCRA체제에서의 평가기준으로서 뿐만 아니라, 현재의 정보보호시스템 평가를 위한 국제기준으로서 그 역할을 하고 있다[5].

3. CC 주요 구성

국제공통평가기준 버전2.1은 크게 세 부분으로 구성되어 있다. 제1부에서는 개요 및 일반모델, 제2부에서는 보안기능 요구사항, 제3부에서는 보증 요구사항을 다루고 있다. CC의 핵심은 제2부와 제3부로써 정보보호시스템이 구비해야 하는 기능 및 보증 요구사항을 기술하고 있으며 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발하고 있다.

제2부에서 다루고 있는 11개 클래스의 보안기능 요구사항을 살펴보면 표 1과 같다[6][7].

표 1. CC 보안기능 요구사항

클래스명	클래스 제목	역 할
FAU	보안감사(Security Audit)	보안활동과 관련된 정보를 감지, 기록, 저장, 분리
FCO	통신(Communication)	데이터를 교환하는 주체의 신원을 감지
FCS	암호지원(Cryptographic Support)	암호 운용 및 키관리
FDP	사용자 데이터 보호 (User Data Protection)	사용자 데이터의 보호
FIA	식별 및 인증 (Identification & Authentication)	사용자의 신원확인 및 인증
FMT	보안관리(Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR	프라이버시(Privacy)	허가되지 않은 사용자에 의한 개인의 신원 및 정보의 도용방지
FPT	TOE 보안기능의 보호 (Protection of Trusted Security Functions)	TSF 데이터의 보호 및 관리
FRU	자원활용(Resource Utilization)	TOE의 가용자원을 확보
FTA	TOE 접근(TOE Access)	TOE에 대한 사용자 세션의 보호
FTP	안전한 경로/채널 (Trusted Path/Channel)	사용자와 TSF간 혹은 TSF간의 안전한 통신채널 확보

표 2. CC 보증 요구사항

클래스명	클래스 제목	역 할
ACM	형상관리 (Configuration Management)	TOE의 무결성이 유지되고 있는지를 확인
ADO	배포와 운영 (Delivery and Operation)	TOE의 안전한 배포, 설치, 운영에 필요한 수단, 절차 및 표준을 확인
ADV	개발(Development)	TOE 개발 과정의 일치성 및 완벽함을 확인
AGD	설명서 (Guidance Documents)	TOE의 안전한 운영을 위한 지침서를 확인
ALC	생명주기 지원 (Life Cycle Support)	TOE의 생명주기와 관련된 사항을 확인
ATE	시험(Tests)	TOE가 기술요구사항을 만족하는지를 확인
AVA	취약성 분석 (Vulnerability Analysis)	TOE의 개발과정 중에 발견되지 않은 취약성, 사용자에 의한 오용 등 잠재적인 취약성을 확인
APE	보호프로파일 평가 (Protection Profile Evaluation)	PP가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
ASE	보안목표명세서 평가 (Security Target Evaluation)	ST가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
AMA	보증의 유지 (Maintenance of Assurance)	TOE나 보안환경이 변화에도 ST를 지속적으로 만족시킴을 보임

제3부는 보증컴포넌트, 보증패밀리, 보증클래스로 분류되고 보호프로파일(PP)과 보안목표명세서(ST)에 대한 평가기준을 정의하며 TOE 평가를 등급별로 나누어 7등급의 평가등급을 소개하고 있다. 10개 클래스의 보증 요구사항을 요약하면 표 2와 같다.

Ⅲ. CC-MRA(1998) : 제1기 국제공통평가기준 기반의 국제상호인정협정

1. CC-MRA 출범배경

1998년 10월 5일 미국, 영국, 캐나다, 프랑스, 독일 등 5개국 6개 기관이 국제공통평가기준(CC) 평가인증서에 대한 국제상호인정 협정서에 서명함으로써 각국에서 실시한 정보보호시스템에 대한 평가결과를 상호 인정하게 되었다. 협정서에 의하면 5개국은 국제공통평가기준(CC) 버전 2.0과 국제공통평가방법(CEM : Common Evaluation Methodology)을 사용하여 정보보호시스템을 평가하기로 합의하였으며, EAL 4등급(TCSEC : B1등급) 이하만을 상호인정하기로 하였다[8].

초기 CC 개발에 참여한 국가중 네덜란드는 자체 평가·인증체계가 아직 완벽하게 구축되지 않아 MRA에 가입을 하지 않았고, 이후 1999년 10월 NISSC에서 호주와 뉴질랜드가 MRA에 가입하였다. 이 두 나라는 이미 가입 신청 전에 유럽의 ITSEC을 이용한 평가·인증체계를 구축하여 다년간의 평가 경험을 소지한 평가·인증체계의 선진국이라 할 수 있다. MRA는 CC와 CEM에 기반을 두고 있으므로, MRA의 전개과정은 CC 및 CEM의 발전과 거의 일치한다고 할 수 있다. 따라서 CC 프로젝트의 주체와 MRA의 주체는 동일하고 특히, CC 버전 2.0기반의 MRA는 CC 프로젝트의 주체들에 의해 주도적으로 추진되었다. 향후 CC 버전 2.1을 기반으로 하는 MRA는 MRA의 주체들에 의해 CC와 CEM이 지속적으로 발전될 것으로 예상된다.

2. 국제상호인정협정서(CC-MRA) 주요내용

1998년 출범한 CC-MRA 관련 협정서는 형식상 서문, 본문 17조, 부록 10항으로 이루어져 있다.

본 협정서의 주된 내용을 살펴보면 다음과 같다. 각 국가에서 평가된 정보보호제품 중 EAL1에서 EAL4 등급까지의 정보보호제품을 상호 인정하는 것을 주된 내용으로 하고 있다. 다만 정보보호제품의 보호프로파일(Protection Profile)이 국가, 국제법이나 정책과 상충하는 경우 그 정보보호제품에 대한 평가인증서 또는 제품의 사용을 인정하지 않을 수 있도록 하고 있다. 상호 인정될 수 있는 정보보호시스템은 관리위원회에서 명시한 버전의 국제공통평가기준(CC)과 국제공통평가방법(CEM)에 의해 평가된 것을 말한다. 평가기관은 각국의 인정기관(Accreditation Body)에 의해 EN 45001 또는 ISO Guide 25의 요구사항을 만족하는 시험소이어야 하고, 보증 및 인증기관(Assurance/Validation Body)은 각국의 인증 기구에 의해 EN 45011 또는 ISO Guide 65의 요구사항을 만족한다고 정부 기관으로부터 인정받은 기관으로 구성된다. 인증서의 구성요소에는 평가한 나라의 특정 표시, 로고, 상호인정합의 마크 및 표준 용어를 사용한 평가인증서 내용이 포함되어 있다. 각 국은 평가한 정보보호제품의 목록을 제시하여야 하며 보호프로파일과 평가한 정보보호시스템의 특성에 대한 설명을 포함하도록 하고 있다.

Ⅳ. ITSEC-MRA : 유럽의 상호인정협정

1. ITSEC-MRA 출범배경

ITSEC 기반의 MRA는 1996년 영국과 독일간의 양자 협정(Bilateral Agreement)에서부터 시작되어, 1997년 영국과 프랑스간의 양자협정으로 이어졌다. 1997년 ITSEC 기반의 MRA가 SOG-IS(Senior Officials Group for Information Security of the European Commission)에 의해 인준되었고, 1998년 영국, 프랑스, 독일, 핀란드, 그리스, 이탈리아, 네덜란드, 노르웨이, 포르투갈, 스페인, 스웨덴 그리고 스위스 등 12개국이 가입하였다[9]. 현재 영국과 프랑스 그리고 독일이 공인받은 인증기관(SOG-IS Qualifying Certification Bodies : QCB)을 가지고 있으며, 이들 기관이 발행한 인증서가 이 MRA에 의해 이들 가입 국에서 인정받게 되었으며 CC 등급 EAL7까지 상호인정하기로 결정하였다. 협정서의 내용이 CC 버전 2.1기반의 MRA와 흡사하다. 다만, CC 버전2.1기반의 MRA에서는 협정서 Title이 'Arrangement'라고 표현하고 있지만, ITSEC기반의 MRA는 'Agreement'

라는 표현을 사용하고 있다는 점이 다르다. 이는 단순한 표현의 차이가 아닌 아마도 참여주체의 차이에 의한 것으로 판단된다.

2. ITSEC-MRA 주요내용

1998년 영국, 독일, 프랑스를 중심으로 출범한 ITSEC기반의 MRA협정은 유럽 12개국간 정보보호제품 평가결과에 대한 상호간 인정을 도모하고자 출범하였다. ITSEC-MRA의 평가기준인 ITSEC (Information Technology Security Evaluation Criteria)은 영국, 독일, 프랑스, 네덜란드 등 자국의 정보보호시스템 평가기준을 제정하여 시행하던 4개국이 평가제품의 상호인정 및 평가기준이 상이함에 따른 정보보호 제품의 평가에 소요되는 시간, 인력 및 소요비용을 절감하기 위하여 소위 "Harmonized Criteria"를 작성하기로 합의하고 1991년 ITSEC 버전 1.2를 제정하였다. ITSEC은 미국의 TCSEC과는 달리 단일기준으로 모든 정보보호 제품을 평가하고 있다. 따라서 보안기능은 개발자가 제품이 사용될 환경을 고려하여 설정하거나 TCSEC 혹은 독일의 ZSIEC에서 미리 정의한 보안 기능을 사용토록 하였으며 제품에 대한 평가는 보증부분만 가지고 수행하였다. 한편, 1998년 3월 SOG-IS(Senior Officials Group-Information Security)협정인 ITSEC-MRA에 가입한 12개국 중 이른바 '자격을 구비한 인증기관'인 QCB(Qualified Certificate Body)를 보유한 국가는 영국, 프랑스, 독일 등 3개국밖에 없고 나머지는 이른바 '인증서 사용국가'로 가입되어 있다[10].

ITSEC-MRA의 평가기준 역할을 하고 있는 ITSEC의 개략적인 내용을 살펴보면 다음과 같다.

기본적으로 ITSEC에서의 보안기능 요구사항은 정의되어 있지 않으며, 평가신청인이 작성한 보안목표명세서(ST)에 의해 평가를 수행하고 있다. 그렇지만 TCSEC과의 호환을 위한 F-C1, F-C2, F-B1, F-B2 및 F-B3 등 다섯 가지와 독일의 ZSIEC의 보안 기능을 이용한 F-IN(무결성), F-AV(가용성), F-DI(전송 데이터 무결성), F-DC (비밀성) 및 F-DX(전송 데이터 비밀성) 등 총 10가지의 보안기능을 제공하고 있다. ITSEC의 보증 요구사항은 효용성 기준(Effectiveness)과 정확성 기준(Correctness)으로 나누어진다. 우선, 효용성 기준은 다시 적절성 분석, 바인딩 분석, 메커니즘의 강도 분석, 개발시의 취약성 분석, 사용의 용이성, 운영 중의 취약성 분석 등이 있다. 정확성 보증기준은 요구사항, 구조 설계, 상세 설계, 구현, 구성관리, 프로그래밍 언어 및 컴파일러, 개발자 보안, 운영문서, 배달절차 및 구성, 시동 및 운영에 대한 요구사항과 같은 구현된 보안 기능의 신뢰성을 소프트웨어 공학적인 측면에서 평가하는 것이다.

3. CC-MRA(1998)와 ITSEC-MRA(1998) 비교

1998년 출범한 CC기반의 MRA와 유럽국가간의 ITSEC-MRA를 비교하여 살펴보면 다음과 같다. 우선 참가국 수를 비교 해보면 CC-MRA는 미국, 캐나다, 영국, 독일, 프랑스 등 5개국 6개 기관으로 이루어 있는데 반해, ITSEC-MRA는 영국, 프랑스, 독일, 핀란드, 그리스, 이탈리아, 네덜란드, 노르웨이, 포르투갈, 스페인, 스웨덴, 스위스 등 12개국으로 구성되어 있다. 평가의 근간이 되는 기준으로는 CC-MRA에서 CC버전 2.0을, ITSEC-MRA에서는 ITSEC 버전 1.2을 기반으로 하고 있는 점이 차이가 난다. 이를 요약해서 비교해 보면 표 3과 같다.

표 3. CC-MRA(1998)와 ITSEC-MRA(1998)비교

구 분	CC-MRA	ITSEC-MRA
출범시기	1998. 10	1998. 3
참 여 국	5개국 (미국, 캐나다, 영국, 독일, 프랑스)	12개국 (영국, 프랑스, 독일, 핀란드, 그리스, 이탈리아, 네덜란드, 노르웨이, 포르투갈, 스페인, 스웨덴, 스위스)
평가기준	CC V2.0	ITSEC V1.2
보안기능 요구사항	11개 보안기능 클래스	TCSEC과 ZSIEC기반으로 정의된 10개의 보안기능 클래스를 제시하여 선택 가능토록 함
보 증 요구사항	10개 보증 클래스	정확성기준과 효용성기준
등급체계	7등급체계 (EAL 1-7)	7등급체계 (E0-6)

V. CC-RA(2000) : 제2기 국제공통평가기준 기반의 국제상호인정협정

1. CC-RA 출범배경

2000년 5월 23일부터 25일까지 미국 Baltimore에서 열린 제1차 ICCC회의에서 기존의 CCMRA체제가 새로운 CCRA체제로 출범하였다[11]. 정보보호시스템 평가를 위한 국제기준인 CC(Common Criteria)가 지난해 6월 국제표준(ISO/IEC 15408)으로 승인되어, 이제는 국내에서도 사실상(de facto)의 국제규범으로 자리 매김하고 있다.

제1차 ICCC(International Common Criteria Conference)는 기존의 98년 10월 5개국 6개 기관간 맺어진 CC기반의 상호인정협정체제를 대체하는 이른바 CCRA(Common Criteria Recognition Arrangement)체제를 태동시키는 계기를 마련하였다[12]. 종전의 상호인정협정 가입 7개국과 신규가입 6개국이 합쳐 총 13개국 13개 기관이 협정서에 서명하였다. 이번 ICCC 회의는 최근의 CC관련 각국의 활동 소개, 평가·인증스킴 소개, 정보보호제품 전시 등 정보보호시스템 평가·인증과 관련된 처음으로 열린 국제회의라는 점에서 그 의의를 찾을 수 있다.

CCRA는 국제공통평가기준 기반의 상호인정협정을 말한다. 정보보호제품을 상호인정(Mutual Recognition)하자는 논의는 정보보호제품의 국가 간 교역장벽을 낮추고자 하는 이른바 「시장개방화」 내지 「규제개혁」의 수단이라 할 수 있다. 이는 상호인정협정 가입국간에 평가·인증 받은 제품은 협정에 참여한 어떤 국가에서도 재평가절차를 거치지 않고 동일한 효력을 가질 수 있도록 하자는 것으로 정보보호제품을 여러 국가에서 평가해야 하는 부담감을 덜어주게 되어 글로벌 시장형성을 촉진케 하는 작용을 한다.

CCRA체제의 주요 특징으로는 참가국 형태가 기존의 일원화된 체제에서 인증서발행자 (CAP : Certificate Authorizing Participants)와 인증서수용자(CCP : Certificate Consuming Participants)로 이원화되어 회원국 수가 배 가까이 증가한 점을 들 수 있다. 본 협정의 법적 성격은 신사협정으로 협정 조건을 위반했을 경우에 제재조치에 관한 규정이 없으며, 가입을 위하여 국가간 협정체결의 경우와 같은 복잡한 법적 절차를 필요로 하지 않는다.

2. CC-RA협정서 주요내용

2000년 5월에 출범한 CC-RA 협정서는 서문, 18개의 본 조항 그리고 11개의 부록 조항으로 구성되어 있다. 협정서상에 나타난 목적은 다음과 같다.

정보기술(Information Technology)제품과 보호 프로파일(Protection Profile)의 평가가 고도의 일관성 있는 기준에 따라 수행되게 함으로써 이들 제품과 PP의 보안성에 대한 신뢰성을 현저히 높일 수 있도록 하며, 평가를 통과한 보안성이 향상된 IT제품과 PP의 가용성을 높이고, IT제품과 PP 평가가 불필요하게 반복되는 것을 방지하며, IT제품과 PP의 평가 및 인증(certification/validation) 과정의 효율성과 비용 경제성을 향상시킬 수 있도록 한다.

각 국간의 행정체계의 차이점은 별도의 양자간 혹은 다자간 협정에 의해 유지되고, 인정될 수 있도록 하고 있다. 신뢰성 있는 인증을 할 수 있는 CB로는 정부기관과 비정부기관이 가능하며, 이러한 양 기관에 대한 조항을 만든다. 그러나 다른 국가에서 발행된 인증서를 인정하는 것은 각국 정부의 고유 업무사항이므로 본 협정에서는 인증서를 발행하는 것과 인정하는 기능은 구분되어 있다.

본 협정의 참가주체는 국가를 대표하는 정부조직이나 정부기관이다. 참가주체는 평가인증서를 발급하는 주체 또는 평가인증서를 수용하는 주체이거나, 양 기능을 모두 가진 주체들로 구성된다. '인증서수용자(Certificates consuming Participants : CCP)'는 정보보호 평가능력을 가지지 않을 수도 있지만 인증된 IT제품과 PP를 받아들이겠다는 명시적 의사를 표현한 주체를 말하고, '인증서발행자(Certificates authorizing Participants : CAP)'는 그들의 국가에서 활동 중인 '준수하는 인증기관(Compliant CB : CCB)'의 후원자이면서 이들 CB에서 발행한 인증서를 공인해 주는 주체이기도 하다.

본 협정은 평가보증 등급(EAL) 1 - 4까지 요구되는 모든 국제공통평가기준 보증 컴포넌트의 이행사항에 대하여 규정하고 있다. 이러한 범위를 확대하는 것(보증등급이나 보증 컴포넌트의 확대)은 제14조의 조항에 의거하여 이 협정의 참가주체들에 의해 언제라도 동의될 수 있다. 어떤 참가주체가 특정

국제공통 평가기준 인증서를 인정하는 것이 그들의 국내법과 규정, 국제 및 유럽연합의 법과 규정에 상충한다면 그 주체는 인증서를 인정하지 않을 수 있다.

특히, IT제품이나 PP가 참가 주체의 국내법, 부속법규, 행정조례 혹은 공공의무 조항에 의해 요구되는 비밀 등급이나 혹은 보호표시와 같은 정보보안과 관련되어 있다면, 그 참가주체는 이러한 경우에 한하여 인증서를 인정하지 않을 수 있다.

본 협정에 규정되어 있는 것을 제외하고는 각 참가주체는 다른 어떤 CAP가 발행한 국제 공통 평가기준 인증서를 인정해야 한다. 인증서 발행은 평가 및 인증과정이 정당하고 전문적 방법에 의해 수행되었음을 확인하는 것이다. 인정된 IT 보안 평가기준에 의해서 인정된 IT 보안 평가방법을 사용하고 CAP 국가의 CCB에 의해 관리되어지는 평가 및 인증 스킴에 따라 발행된 국제공통평가기준 인증서와 발간된 인증보고서가 본 협정의 목표들을 충족시키는 방법 등 모든 조건들을 충족시키는 인증서들은 본 협정서 상의 인증서와 동일한 것이 된다.

최소한의 조건으로서 다음의 두 조건을 충족시킨다면 평가 및 인증은 정당하고 전문적인 방법에 의해 수행되었다고 판단한다. 평가기관의 조건은 EN45001이나 ISO Guide 25 혹은 이들에 대한 참가주체들에 의해 공인된 해석에 의거하여 인정된 인정기관(Accreditation Body : AB)에 의해 각국에서 인가되고, 부록 B.3에 의해 허가받거나 공인받는 조건, 각국의 법, 법적 수단, 혹은 행정절차에 의해 설립되고, 부록 B.3의 모든 조건을 충족되도록 요구하고 있다.

인증기관의 조건은 EN45011이나 ISO Guide 65 혹은 이들에 대한 각국의 해석 중 부록 C에 구체화된 요구사항을 최소한도로 만족시키는 해석에 의거하여 인정된 인정기관(Accreditation Body : AB)에 의해 각국에서 인가 받는 조건, 각국의 법 혹은 행정절차에 의해 설립되고, 부록 B.3의 모든 요구 조건을 충족한다는 조건, CC와 평가·인증스킴간에 일관성 있게 적용하기 위해서, 참가주체들은 현재의 CC와 CEM의 단일 해석 안을 만들 계획으로 있다. 이를 위하여 참가주체들은 해석에 관한 정보를 정기적으로 교환하고 해석상의 차이를 해결하기 위한 논의를 계속할 계획이다.

나아가 CC와 CEM을 일관성과 신뢰성 있도록 하고 적절하게 적용하겠다는 목표를 위하여, CB는 평가와 인증 스킴내에서 진행중인 모든 종류의 평가를 적정 수준에서 감시하는 책임을 갖게 될 것이며, 동시에 CB와 제휴되어 있는 모든 평가기관이 다음의 세 가지를 준수할 수 있도록 하는 다른 절차도 수행한다.

공정하게 평가하고, 바르고 일관적으로 CC와 CEM을 적용하며, 보호되어야 할 정보의 기밀성을 적절하게 준수하도록 하고 있다. 신규 참여주체는 기존 참여주체들의 만장일치의 조건으로, 본 협정의 원칙에 동의하는 국가의 대표기구가 협정 참여 주체가 된다.

3. CC-MRA(1998)와 CC-RA(2000) 비교

CC 버전2.0을 기반으로 한 기존의 MRA는 모든 참가국이 기본적으로 MRA에 의해 공인된 평가 및 인증기관을 갖추도록 되어 있었지만, 새로운 CCRA 체제에서는 타국의 인증서를 인정해 주는 동시에 자국내 CCRA에 의해 공인된 평가 및 인증기관을 보유하는 인증서 발행국과 타국의 인증서를 상호 인정해 주지만 자국 내에 CCRA에 의해 공인된 평가 및 인증기관을 보유하지 않은 인증서 수용국으로 구분할 수 있다.

2000년 5월에 발효된 CCRA협정서인 '정보보호분야 국제공통평가기준 인증서 인정협정(Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security)'상에서 변화된 주요 특징을 살펴보면 다음과 같다.

먼저, 1998년 CCMRA에는 없던 회원제(Membership)규정이 제1조에 신설되어 인증서발행자(CAP)와 인증서수용자(CCP)로 구분되어 있는 점 둘째, 협정서 제2조 인정범위(Scope)에 관한 규정으로 보증등급이나 보증컴포넌트의 인정범위의 확장(Extension)이 필요한 때는 협정참가자의 동의를 받도록 한 점 셋째, 제8조 정보공유(Sharing of Information)에 관한 규정으로 각 참가국의 정보공유를 의무화한 점 마지막으로, 제15조 협정의 효력에 관한 존속기간(Duration) 규정 중 협상개시 3년경과 후 재검토한다는 사항을 삭제한 점등을 들 수 있다.

표 4. CC-MRA(1998)와 CC-RA(2000) 비교

구 분	CCMRA(1998)	CCRA(2000)
협정서 형식	서문, 본문 17조, 부록 10항	서문, 본문 18조, 부록 11항
회원제 구성	근거조항 없음	회원구성조항 신설 (제1조) CAP와 CCP로 이원화
인정 범위	근거조항 없음	인정범위 확장(Extension) 조항 신설(제2조)
정보 공유	정보공유의 자율규제	정보공유의 의무화 (제8조)
효력 존속기간	본 협정의 효력존속기간 3년 경과시 재검토	존속기간 재검토 조항 삭제(제14조)
참가국가	5개국 6개 기관	13개국 13개 기관

Ⅵ. CC-RA 출범에 따른 국내 대응방안

1. 평가제도 관련 법·제도 정비

국내 정보보호제품 평가와 관련된 근간이 되는 현행법으로는 정보화촉진기본법을 들 수 있다. 동법 제14조 제2항에서 정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 강구하여야 한다고 규정하여 정보보호 제품에 국가가 관여할 수 있는 근거를 마련하고 있다. 이에 근거하여 제15조(정보보호시스템에 관한 기준고시 등)에서는 정보통신부장관이 관계기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 이를 고시하고, 정보보호시스템을 제조하거나 수입하는 자에 대하여 이 기준의 준수를 권고할 수 있도록 하고 있다. 또한 정보통신부장관은 유통중인 정보보호시스템이 동법 제1항의 규정에 의한 기준에 미치지 못할 경우에 정보보호시스템의 보완 및 기타 필요한 사항을 권고할 수 있다고 규정하고 있다. 이에 근거하여 정보통신부장관은 '정보통신망 침입차단시스템 평가기준(정보통신부 고시 2000-14)'과 '정보보호시스템 평가인증지침(정보통신부 고시 2000-15)'을 고시한 바 있다[13]. 그러나 이 규정들은 정부에 대해 권고할 권한만을 부여한 것이어서 정부가 제정한 기준이 어떤 법적 강제력을 가질 수는 없는 실정이다.

이러한 상황에서 CCRA의 대응에 필요한 입법사항을 제시하면 다음과 같다. 우선 CAP의 인증서를 획득한 제품은 국내 평가기준에 합치하는 것으로 보는 규정이 제정되어야 한다. CAP의 인증서를 인정하기 위해서는 법률 또는 명령에 이를 명시적으로 규정해야 하는데, 이에 관한 몇 가지 입법 방안으로는 우선 기준 자체와 관련하여 기준의 형식을 유지하는 방법과 이를 포기하는 방법을 생각할 수 있다.

아울러, 기준의 형식은 유지하되 그 내용을 독자적으로 정하는 방법과 CC를 그대로 수용하는 방법을 생각할 수 있다. 다른 하나는 외국에서 발급한 인증서를 인정하는 규정의 위치를 법률에 두는 방법과 시행령에 두는 방법을 고려할 수 있을 것이다.

이 두 가지를 고려하면 다음과 같은 경우의 수를 생각할 수 있는데 이 방법들의 장단점을 비교하면 다음과 같다. 우선, 기준 자체를 폐기하고 CC를 수용하는 방법은 수요자의 입장에서 규범이 명확하고 입법적인 작업량이 줄어든다는 장점이 있지만, 내국법의 입법권을 포기하는 것으로 보일 수 있다. 아울러, CC의 변화가 그대로 국내에서 효력을 갖기 때문에 효율적이기는 하지만 내국에서의 여과 장치가 없는 단점 또한 있다. 기준의 형식 속에 CC와는 다른 독자적인 내용을 담는 것은 단기적으로는 의미가 있으나, 장기적으로 CC의 수용이 바람직하다면 CC와 현재의 기준의 내용이 융합해 가는 과정이 필요한데 단기적으로 두 기준을 병행하는 것도 하나의 방법일 수 있다. 이 방법은 기존의 규범 내용이 유지됨에 따른 법적 안정성이 장점이지만 규범의 이용자나 운영자의 입장에서 번잡함을 피할 수는 없을 것이다. 기준의 내용으로 CC를 도입하는 방법에는 두 가지 방법을 고려할 수 있는데, 하나는 기존의 기준의 내용을 CC로 대치하는 것이고 다른 하나는 시행령에서 CC를 기준으로 한다고 규정하는 방법이다. 전자는 CC의 변화에 맞추어 개정작업을 계속해야 하는 어려움이 있지만 CC의 의미를 명확히 정립하고 CC 중에서 수용하기가 어려운 내용이 있는 경우 이를 걸러낼 수 있는 장점이 있다. 반면 후자는 반대의 장단점을 가진다. 외국에서 발급한 인증서를 인정하는 규정을 법률에 두면 법적 효과라는 측면에서 부족함이 없지만 개정작업이 번잡한 단점이 있다. 그런데 법리적으로 보면 CCRA가 조약의 형태이므로 당연히 국내법과 같은 효력을 지니기 때문에 굳이 법률에 규정을 두어야 하는 것은 아니다. 반면 그러한 규정을 시행령에 두면 개정작업이 상대적으로 수월한 장점은 있지만 CCRA의 법적 성격과 관련하여 법리적인 모순이 있다는 지적은 피할 수 없을 것이다. 종합적으로 보면 기준의 형식을 유지하면서 그 내용을 CC로 담고 시행령에서 CAP가 발

급한 인증서를 인정하는 규정을 두는 것이 바람직하다고 판단된다.

2. 국제협력체제 구축

정보보호제품에 대한 평가능력을 개발하고 보호프로파일(PP) 및 보안목표명세서(ST) 개발능력 향상을 위해서는 국제공동협력체제 구축과 국외기관간 공동개발 노력이 요구된다. 이러한 노력의 선행작업의 일환으로 먼저 CCRA의 최근 동향을 살펴보면 다음과 같다. 올 5월에 개최된 ICCC회의에서 미국 NSA (National Security Agency)의 Louis Giles는 내년까지 CCRA에 최소한 4-5개국이 더 참가할 것으로 전망하고 있다. 이러한 상황이 현실로 나타난다면 회원국이 20개국에 육박하게 될 것이다.

이들 국가 중 특히, 제1차 ICCC회의에 참석한 스웨덴, 스위스는 조만간 CCP로의 참여가 확실시되며, 정보보호강국인 이스라엘 또한 CAP가입 준비단계로서 CCP로의 조기참여를 강력히 희망하고 있다[14].

아시아권에서는 일본이 최종 목표를 CAP가입으로 잡고 98년 3월부터 통산성(MITI : Ministry of International Trade and Industry)산하 정보처리진흥사업협회(IPA:Information-technology Promotion Agency)의 보안센터(Security Center)에서 9명의 전담인력으로 구성된 CCTF (Common Criteria Task Force)를 운영하면서 200여명 이상의 평가자(Evaluator)를 양성하고 있는 등 CCRA가입을 위한 노력을 적극 펼치고 있다[15]. 최근 발표에 따르면 일본은 CC를 자국의 국가표준(JIS)으로 7월에 편입(JISX5070) 시켰으며, 내년 4월에 현재의 「제품평가 기술센터」를 「보안평가인증체제」로 명칭을 변경하여 새롭게 창설하고, 2003년까지 CCRA 가입 목표를 천명하는 등 발빠르게 움직이고 있는 점은 시사하는바가 크다할 것이다[16].

각 국의 이러한 준비 노력들은 IT기반의 정보시스템 네트워킹 추세가 전 세계적으로 강화되면 될수록 더욱 확산될 것으로 판단된다. 특히, CC는 정보보호제품에 대한 상호인정협정의 기초가 되는 것으로 CCRA의 참여국 수의 증대는 자동적으로 CC의 수용 확대를 의미하며, CCRA 미참가국이라 할지라도 참가를 위한 준비과정으로 CC를 수용하는 국가가 확대될 것으로 예상되어 그 폭은 더욱 클 것으로 판단된다. CCRA에 대하여 수동적이고 중립적인 국가의 경우에도 세계적인 표준화의 큰 흐름에 순응할 수밖에 없으며 적극적으로 국제표준을 인정할 수밖에 없는 상황 또한 자국내 CC수용의 촉매제로 작용할 것이다[17].

향후 CC와 CCRA는 상호보완적으로 발전되어, CCRA 가입국 수와 구성이 확대되어감에 따라 CC의 내용 변화 또한 더 빈번히 일어날 것으로 예상된다[18]. CC가 CC버전 2.1까지 개정되어 오면서 많은 수정을 거쳐온 것처럼 향후에도 정보보호 환경변화에 발맞추어 끊임없이 변화할 것으로 예상된다.

아울러, CC와 ISO와의 연계를 포함한 다른 국제기구 및 국제활동과의 연계과정에서 CC의 부단한 변화는 계속 나타날 것이며, 정보화의 세계적 확산, 기술의 발전과 융합, 수요의 질적 변화 등을 적절하게 반영하기 위한 CC의 내용상의 변화 또한 지속되리라 예상된다. 특히, CC수용의 확대와 CCP자격조건이 자국내 추가적인 비용을 수반하는 평가제도를 구비하지 않고도 CCRA에 참여할 수 있다는 점에서 CCRA의 확산이 가속화 될 것으로 예상된다.

WTO나 OECD-ICCP, APEC-TEL 등과 같은 국제기구에서 정보보호 및 상호인정에 관한 의제가 아직은 초보수준으로 논의되고 있지만, 정보보호제품의 평가·인증을 현행의 '자율적'인 방법이 아닌 '강제화'된 형태로 변화시킨다면, 이는 결국 또 다른 통상협상의 모습을 띈 뉴라운드인 이른바 'Security Round'로 귀결될 것이며, 이때에는 기존의 CCRA 참가국 주도의 연계적 논의가 본격적으로 펼쳐질 것이다.

이러한 여러 가지 상황을 종합해 볼 때 CCRA참가국 및 참가준비국 간의 국제협력체제 및 공동개발 노력은 전략적인 차원에서 긴요하다 할 것이다.

3. 평가기술 개발 및 평가자 양성을 위한 제도 확립

향후 국내 평가기관이 CC를 수용하고 CC기반의 상호인정협정 가입을 할 때, 아마도 가장 먼저 해결해야 할 부분이 평가기술력 확보와 평가자 양성일 것이다. CCRA체제에 능동적으로 대응하기 위해서는 평가기관의 업무수행에 필요한 교육, 훈련, 기술적 지식 및 경험을 갖춘 충분한 수의 평가요원 확보가 필수적이라 할 것이다. 평가기관은 평가요원이 항상 최신 지식을 습득하도록 훈련시키며, 평가요원의 자격, 교육/훈련, 기술 및 경험에 관한 기록을

유지하고, 평가 툴 개발 및 민간평가기관의 평가 기법 및 기술 전수, 평가인력 양성을 위한 평가교육과정 개설 등이 우선적으로 확립되어야 할 것이다.

즉, 선진화된 평가제도의 조기 정착과 효율적인 평가 준비방법을 위한 정보보호시스템 개발자 및 신청인을 위한 평가제도 및 교육과정이 요구된다.

아울러, 국외 선진 평가기관과 공동협력체계를 통한 평가전문인력 양성을 위한 노력 또한 필요한데, 이를 위해 유럽 및 미국 등의 선진 평가기관과 평가업무관련 협력을 맺어 공동평가 등 평가기술 교류를 통한 평가자 양성을 하고 평가기술 확보를 통한 평가절차 및 방법 매뉴얼화 등을 개발하여야 할 것이다. 특히, 미국, 영국 등 해외 선진평가기관 교육훈련을 통해 선진 평가기술 확보 및 실무를 국내에 적용할 수 있는 기틀을 마련해야 할 것이다.

한편, 국내 산·학·연간 평가전문인력 양성 프로그램 운영을 통해 정보보호 관련학계 및 산업체 전문가로 구성된 평가기술 전문가 그룹을 구성하여 국제공통평가기술 등 공통연구를 통한 기술을 공유하는 노력 또한 필요하다. 이러한 일련의 노력을 위한 제도적 장치가 국내에서도 조속히 마련되어 정보보호시스템 평가기술력 확보 및 평가자 양성에 기여할 수 있도록 하여야 할 것이다.

4. 정보보호산업 육성

CCRA가입을 함으로써 인증서 인정에 대한 가장 큰 우려는 국내 시장에서 외국제품이 경쟁력을 갖게 되어 결국 국내 정보보호산업이 좌초할지도 모른다는 점이다[19]. 이러한 염려를 불식시키기 위해서는 국내 정보보호산업의 육성 전략이 다양한 형태로 수립되어져야 할 것이다. 이를테면, 공공부문에서의 정보보호제품 수요기반 창출, 정보보호 전문인력 확보, 기술개발 지원 확충, 전문업체들의 실질적인 경쟁력 확보를 위한 해외 마케팅 지원, 정부 각 부처를 비롯한 사회전반의 정보보호 필요성에 대한 인식 확산을 위한 대 국민 홍보작업 등 여러 가지 정책방안을 들 수 있다. 국내 정보보호산업의 경쟁력 강화 방안을 전략적 관점에서 제시하면 다음과 같다[20].

먼저, 정보보호 기술연구개발의 특화전략이 필요하다. WTO체제의 출범으로 기술개발과 관련된 국책연구개발과 기업보조금의 범위가 제한 받게 되는 것은 기술개발정책을 변화시키는 주요 원인으로 작용하고 있다. WTO체제 하에서는 연구개발에 대한 보조금을 상용제품개발분야에 전면 금지시키고 있어 기술개발보조금을 전략적인 분야를 선택하여 신속하게 상품화 될 수 있는 핵심기술개발분야를 집중적으로 지원하는 등 종전의 기술개발정책에 변화가 요구된다. 즉, 대규모 연구소의 연구프로젝트에 국가가 직접적으로는 상용제품을 개발하기보다는 민간의 위탁연구나 공동연구 형식을 활용하는 연구개발 운영방식의 전환이 필요하며, 세계 정보보호산업을 주도할 수 있는 최첨단 수준의 정보보호기술을 단계적으로 확보하는 노력이 요구된다. 타 분야에 비하여 상대적으로 기술력이 취약한 정보보호분야의 기술개발 능력의 조기 향상 추진을 위하여 정보통신 기술개발 계획 수립 시 정보보호분야에 매년 일정비율 이상의 기술개발비를 지속적으로 투입하고 기술개발의 효율성 제고를 위해 연구분야별 전문화를 유도하는 노력이 요구된다.

둘째, 정보보호 전문인력 양성 프로그램 운영의 내실화가 필요하다. 정보보호 산업현장에서 필요로 하는 현장감 있고 창의적인 전문기술인력을 꾸준히 양성하는 노력이 요구된다. 산업체가 당장 필요로 하는 실무적인 인력을 조기에 확충하기 위해서는 한국정보보호센터와 정보통신대학원대학교 부설 정보통신교육원의 교육과정에 정보보호에 관한 교육프로그램을 신설 또는 증설하여 정보보호기술에 관한 교육을 실시하는 방안을 들 수 있을 것이다. 교육내용 또한 현재의 지나친 이론적인 교육보다는 실무위주의 커리큘럼 운영으로 인력수급의 내실화를 기하는 노력이 필요하며, 국내 대학(원)의 정보보호분야 교육 활성화를 위해 정보보호학과 또는 과정의 신·증설 및 전문연구센터의 설치를 위한 정부의 지원이 필요하고, 정보보호 전문가의 저변확대를 위한 여건조성으로 대학 내 정보보호 관련 동아리 활동이 활성화 될 수 있도록 지원하는 방안을 확대·운영할 필요가 있다. 아울러 지난해부터 실시하고 있는 정보통신부의 '정보통신 해외장학프로그램' 지원사업에 선발인원의 일정부분을 정보보호분야 전공자에 우선 배분하여 정보보호 우수인력의 조기 확보를 위한 노력을 적극적으로 전개할 필요가 있다.

셋째, 정보보호 관련 지원산업 육성을 서둘러야 한다. 우수제품 개발이 가능하고 국내외 시장규모 확대가 예상되는 정보보호 관련 지원산업을 지정하고 이를 전문적으로 생산하는 유망 중소기업을 다양한 제품 구성군으로 선정하여 자금, 기술개발, 판로 등의 지원을 통해 정보보호 벤처기업을 적극 육성할

필요가 있다. 한편, 내년 3월에 개소 예정인 '정보보호산업육성지원센터'를 주축으로 창업활동, 투자유치 및 제품 판매 등을 지원하고 고가의 장비 및 시스템을 공동 활용하는 등 기술 관련 중요 정보 공유 촉진에 이바지 할 수 있도록 기반시설 정비를 위한 노력에도 박차를 가해야 할 것이다.

마지막으로, 정보보호 업체의 해외진출을 적극 추진할 필요가 있다. 종전의 정보산업체의 전략은 주로 국내 위주의 정책과 규제 구도로 인하여 국내 투자에만 집중하고 해외사업에는 소홀하여 왔으며, 대외개방에 대해서도 방어 위주의 대응에만 치중하여 온게 사실이다. 하지만, 이제는 시장 개방의 추세에 따라 국제 경쟁력 제고를 위해 공격적인 해외사업 진출이 필요한 시점에 와 있다.

매우 역동적인 산업으로 인식되고 있는 정보보호산업은 본질적으로 세계시장을 무대로 한 경쟁만이 의미를 가질 수 있다고 할 것이다. 기업들은 더 이상 국내시장에서만 안주할 수 없을 뿐만 아니라 독자적인 표준이나 내수 중심의 기업전략으로는 기업의 생존자체가 어려워지고 있는 형편이다. 세계시장에서 무차별적인 기업간의 전략적 제휴·합병의 증가에 따라 국내기업들간의 경쟁에서 우위를 점하는 것이 무의미할 뿐만 아니라 인터넷의 사용 등으로 전 세계가 네트워크화 되어감에 따라 중소기업도 세계시장을 무대로 사업을 전개할 수 있고, 가상공간에서의 교역이 크게 증가할 것으로 예상됨에 따라 국경 없는 경제가 가속화되어 경쟁 자체가 세계화될 수밖에 없는 실정에 놓여 있다.

국내 정보보호산업의 해외진출은 그 동안 비교적 경쟁이 심하지 않은 개도국 위주로 전개해 왔으나, 이제는 해외시장의 블록화 내지는 완전 개방화 추세로 세계 어느 곳에서나 무한경쟁에 직면하고 있으며, 막강한 자금력과 첨단기술로 영향력을 행사하고 있는 외국 기업체와의 경쟁에서 이겨내기란 결코 쉬운 일이 아니다. 따라서 국내 정보보호업체도 그 동안 축적한 경험과 기술을 바탕으로 개도국에 대한 시장진출을 계속 추진하되 국내 업체간의 공동 진출 방안을 모색하는 전략과 외국 선진업체와의 컨소시엄 구성 등의 형태로 선진국 시장에 진출하는 노력이 병행되어 이루어 져야 할 것이다. 아울러, 업체의 해외 진출에 필요한 해외시장 동향파악, 관련업체 정보수집, 해외 현지법인 설립, 해외 전시회 참가 등 해외시장 진출을 위한 기반 조성 노력이 선행적으로 이루어 져야 할 것이다.

Ⅵ. 결 론

이상 국제공통평가기준 기반의 상호인정협정과 관련된 최근동향 및 대응방안을 살펴보았다. 향후 정보보호시스템 평가제도의 국제적 흐름을 결정하게될 CCRA출범이라는 새로운 환경을 맞이하여 무엇보다도, 정부와 시장간의 새로운 관계 설정이 요구되고 있다. "정부는 환경조성, 성장은 기업책임"이라는 명제로, 국제공통평가기준(CC) 수용 및 상호인정협정(MRA)가입을 위한 제도적 정비에 정부의 노력이 한층 더 필요하다. 특히, 정보보호 수출입 관련정책, WTO, OECD-ICCP, APEC- TEL 등 국제기구와의 정책수립에 있어 명확한 입장을 정보보호산업계에 전달하여 향후 예상되는 'New Round'에 확실한 대책과 방법을 강구할 수 있도록 해야 할 것이다.

정보보호산업은 애초에 국가안보와 관련된 기술이 일반화된 것이기 때문에 정부가 가장 큰 사용처 일 수밖에 없다. 따라서 그 어떤 산업보다도 정부 정책에 민감하게 반응하는 것은 당연하다할 것이다. 선진국을 필두로 대부분의 국가들이 정보보호산업에 대한 구체적이고 때로는 타협할 수 없는 정책을 가지고 구매와 판매에 영향을 끼치고 있는 것 또한 이러한 연유에서 근거한다 할 것이다. 아울러, 자국의 정보보호산업 기반을 구축하는 것이 국가안보 뿐만 아니라 산업적 수익에도 엄청난 영향을 미치기 때문이라 할 수 있다. 이러한 정책들은 각 국의 정보보호 제품에 많은 영향을 미치며 제품의 국제적 판매에 진입장벽의 역할을 하고 있기도 하다. 국내 정보보호산업이 국제경쟁력을 갖기 위해서는 이러한 난관을 극복해야 하는데, 이것은 정부가 자국의 정책과 타국에 대한 정책을 적절하게 조화시킴으로서 가능하다 할 것이다.

한편, 새로운 표준형성을 위한 선도국가로의 지향을 통해 국제표준(IS)을 수용하고 선도하는 자체가 이젠 그야말로 중요한 '경쟁 핵심'이 되고 있다는 사실을 인식해야 할 것이다. 향후 예상되는 국제적 흐름은 우리에게 위협인 동시에 기회로 작용할 것이다. 국내에서만 통하는 국지적(Local)발상으로는 개방된 사회에서의 생존은 불가능할 것이다. 과거의 법과 제도를 어떻게 수정할 것이 아니라, 국제화(global)에 비추어 무엇부터 먼저 바꾸어야 하는가를 검토하는 것이 우선적으로 고려되어야 할 것이다. 국제사회에 통용되면서 우리 실정에 맞는 법과 제도를 설계하는 노력이 선행적으로 이루어져 함은

두말할 필요가 없다. 이를 위해 글로벌 스탠더드를 수용할 수 있는 역량을 배양함은 물론, 향후 CCRA 가입시 예상되는 충격을 최소화하기 위한 노력 또한 병행하여 추진되어야 할 것이다. 결국, 국내에 CCRA를 수용한다는 것은 단순히 CC기반의 MRA가입 그 이상의 의미를 지닌다고 할 것이다.

참 고 문 헌

[1] 한국정보보호센터, "국내외 정보보호시스템 평가가이드", 1998. 11

[2] 한국정보보호센터,"국내외 정보보호산업 현황", 1999. 12

[3] Robert Morey, "The Canadian Common Criteria Evaluation and Certification Scheme(CCS)", 1st International Common Criteria Conference, May, 2000

[4] Gene Troy, "Introduction to the Common Criteria for IT Security(ISO 15408)", 1st International Common Criteria Conference, May, 2000

[5] Thomas E. Anderson, "Common Criteria Evaluation & Validation Scheme-CCEVS", 1st International Common Criteria Conference, May, 2000

[6] 한국정보보호센터, "정보보호 평가기준 개발", *정보통신부 연구개발결과보고서*, 1999. 12

[7] CommonCriteria,http://www.commoncriteria.org

[8] "Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of Information Technology Security", *CC-MRA*, October, 1998

[9] BSI,"German IT Security Certificates-ITSEC", March, 2000

[10] ITSEC, http://www.itsec.gov.uk

[11] Louis Giles, "The Common Criteria Recognition Arrangement", *1st International Common Criteria Conference*, May, 2000

[12] "Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security", *CC-RA*, May, 2000

[13] 정보통신부, "정보보호시스템 평가·인증지침", *정보통신부고시 제 2000-15호*, 2000. 2

[14] David Guttman, "Standard Institution of Isra/el", *1st International Common Criteria Conference*, May, 2000

[15] Yoshitaka Toui, "Japanese Evaluation and Certification Scheme", *1st International Com-mon Criteria Conference*, May, 2000

[16] MITI,http://www.miti.go.jp/kohosys/press/0000931/0/itsecurity.htm

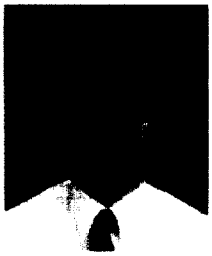
[17] Ian Bryant, "Implementing the CC via Government Policy", *1st International Common Criteria Conference*, May, 2000

[18] 이유신,"CCRA 최근동향 및 향후 전망", *정보보호뉴스*(통권35호),한국정보보호센터, 2000. 8

[19] 디지털타임즈,"보안업계, 정보보호시스템 국제상호인정협정 가입 놓고 찬반 팽팽" 2000. 7/24

[20] 이유신,"정보보호산업육성 시급하다", *인터넷 eConomy*, (주)리딩컴, 2000. 7

〈著者紹介〉



이 유 신(Yue-Shin Lee)
1986년~1994년 2월 : 경희대학교 경제학과 졸업(경제학사)
1995년~1997년 2월 : 경희대학교 행정학과 졸업(행정학석사)
1997년~현재 : 경희대학교 행정학과 박사과정
2000년~현재 : 한국정보보호센터 평가기준팀 연구원
〈관심분야〉 정보정책, 정보통신산업, 정보보호시스템 평가·인증제도

이 경 구(Koung-Goo Lee)
1975년~1982년 2월 : 한양대학교 무기재료공학과(공학사)
1984년~1986년 5월 : University of Central Arkansas 전산학과 졸업(이학사)
1986년~1988년 5월 : University of Arkansas 전산학과 졸업(이학석사)
1989년~1996년 5월 : Kent State University 전산학 졸업(이학박사)
1996년~현재 : 한국정보보호센터 평가기준팀장
〈관심분야〉 정보보호, 시스템 성능분석, 네트워크 프로토콜