제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

CCRA 가입을 위한 정보보호시스템 평가·인증제도 개선 방안에 대한 연구

김수연*, 김근옥*, 이승우*, 김춘수**, 원동호*
*성균관대학교 컴퓨터공학과
**국가보안기술연구소
e-mail : sykim@dosan.skku.ac.kr

A Study on the Improvement of IT System Security Evaluation and Validation Program for joining CCRA

Sooyeon Kim*, Keunok Kim*, Seungwoo Lee*, Choonsoo Kim**, Dongho Won*
*Dept. of Computer Science & Engineering, Sungkyunkwan University
**National Security Research Institue

요 약

각국의 평가·인증제도는 안전성과 신뢰성을 보증하는 우수한 정보보호시스템 개발을 촉진하여 정보보호산업 육성에 기여해 왔다. 이와 같은 산업 육성 측면과 안전한 제품을 공급하여 신뢰할 수 있는 정보사회를 구축한다는 면에서 국제 표준인 CC 기반의 정보보호제품 평가의 국제 상호인정협정인 CCRA 에 대한 국내의 신속한 대응이 요구된다. 본 고에서는 CCRA 체제의 특징을 고찰하여, 국내 정보보호시스템 평가·인증제도의 개선 사항과 대응 방안을 제안하고자 한다.

1. 서론

정보기술의 발달과 정보화의 확대로 인하여 국가 및 사회, 개인간의 정보경쟁이 치열해짐에 따라 정보보호의 중요성이 더욱 높아지고 있다. 이에 정보를 보호하기 위한 정보보호시스템의 사용이 증가하고 있다. 선진국에서는 이와 같은 제품의 신뢰성 확보를 위한 제도적 장치로서 평가기준 및 평가·인증제도를 개발하여 정보보호시스템에 대한 평가를 시행하고 있다.

1999 년 국제공통평가기준인 CC(Common Criteria)가 ISO/IEC 15408 표준[1]으로 승인되어 평가에 활용되고 있다. 미국, 영국 등의 선진국들은 CC 를 이용하여 국가별로 평가 받은 제품의 효력을 상호인정하는 CCRA(Common Criteria Recognition Arrangement)를 체결하여 정보보호제품의 수·출입 및 다양한 평가제품의 활용이라는 측면에서 소비자 및 개발자의 욕구를 만족시키고 있다[2]. 국내에서는 초기의 정보보호 제품 평가를 위한 기준이 개별 제품에 대한 기준으로 국한되었으나, 현재는 평가의 한계를 극복하고 다양한 제품을 평가할 수 있도록 CC 기반의 평가를 시행 중에 있으며, CCRA 가입에 대하여 적극 검토하고 있다.

정보보호시스템 평가·인증제도는 검증된 정보보호시스템을 공급하기 위한 목적으로 운영되고 있지만, 국내 평가·인증제도는 민간분야에서 요구하는 다양한 제품의 평가가 이루어지고 있지 않고, 제품평가에 소요되는 시간과 비용이 많으며, 평가된 제품이 국제적으로 상호인정 되지 않는다는 문제점을 가지고 있다.

이에 위의 문제점을 해결하고 CCRA 가입에 대응을 하기 위해, 국제 환경에 적합하고 신뢰할 수 있는 국내 정보보호시스템 평가·인증제도의 개선이 요구된다.

따라서 본 고에서는 2 장에서 CCRA 가입효과 및 요구사항에 대해 알아보고, 3 장에서는 국내 평가·인증제도의 현황에 대해 분석한다. 4 장에서는 CCRA 가입을 위한 국내 평가·인증제도의 개선 방안을 제안하고, 마지막 5 장에서는 결론 및 향후 연구과제에 대해 설명한다.

2. CCRA

CCRA 란 가입국의 정보보안기관에서 행한 CC 등급에 준하는 평가결과를 각 가입국간에 상호인정하는 협정이다. CC 가 확대 수용되고, CCRA 에서 보다 많은 국가의 참여를 위해 복잡한 가입 요구사항을 완화했다는 점을 고려할 때, 향후 CCRA 의 참가국이 크게 증가할 것으로 예상된다.

2.1 CCRA 가입을 위한 요구사항

기존의 CC-MRA(Common Criteria-Mutual Recognition Arrangement) 체제에서 2000 년 새롭게 출범한 CCRA 의 협정서는 서문, 18 개의 본 조항, 11 개의 부록 조항으로 구성되어 있다[3]. CCRA 협정서에는 CCRA 가입을 위한 목적, 범위, 인정조건, 평가기관 및 인증기관의 요구사항 등의 내용이 기술되어 있다.

■ 가입자격

CCRA 는 CCRA 에 의해 인정 받은 평가·인증기관을 가지고 있는가의 유·무에 따라 두가지 가입자격[4]을 제시하는데, 다음 [표 1]은 CCRA 가입국 및 가입자격에 대한 설명이다.

[표 1] CCRA 가입국 및 가입자격

구분	가입국	가입자격
CAP (Certificate Authorizing Participants)	미국, 캐나다, 영국, 독일, 프랑스, 호주, 뉴질랜드	CCRA 에서 요구하는 적법한 인정을 받은 평가 및 인증기관을 소유한 국가 - 평가인증서를 발급 - 다른 참가국이 발급한 적법한 평가인증서를 인정
CCP (Certificate Consuming Participants)	네덜란드, 이탈리아, 그리스, 핀란드, 노르웨이, 스페인, 이스라엘, 스웨덴, 오스트리아	CCRA 에 의해 인정받은 평가 및 인증기관을 소유하지 않은 국가 - 평가인증서를 발급할 수 없음 - 다른 참가국이 발급한 평가인증서를 인정하여 자국에 적법한 평가인증서로 활용

■ 인증기관의 요구사항

인증기관은 유럽기준인 EN 45011(General Criteria for Certification Bodies Operating Product Certification)이나 국제 표준인 ISO Guide 65(General Requirements for Bodies Operating Product Certification Systems), CCRA 협정서의 부록 C(Requirements for Certification/Validation Body)에 구체화된 요구사항을 최소한 만족시키는 해석에 의거해야 한다. 또, 인정기관에 의해 각국에서 인가 받는 조건, 각국의 법 혹은 행정절차에 의해 설립되어야 한다. CCRA 협정서 부록 B.3(Accreditation and Licensing of Evaluation Facilities)의 모든 요구조건을 충족해야 하며, 평가기관이 CC 와 CEM(Common Evaluation Methodology)을 평가·인증스킴간에 일관성 있게 적용하고 있는지를 옳게 판단할 수 있는 능력이 있어야 한다.

■ 평가기관의 요구사항

평가기관은 유럽기준인 EN 45001(General Criteria for the Operation of Testing Laboratories)이나 국제 표준인 ISO Guide 25(General Requirements for the Competence of Calibration and Testing Laboratories)를 만족하거나, 공인된 해석에 의거하여 허가된 인정기관에 의해 인가되고, 각국의 법, 법적 수단, 혹은 행정절차에 의해 설립되며, CCRA 협정서 부록 B.3 의 모든 조건을 충족되도록 요구하고 있다.

■ 평가관련 전문가 필요

CCRA 에 가입하기 위해서는 평가기준인 CC 의 기능 컴포넌트에 대한 이해를 통해 PP(Protection Profile)와 ST(Security Target)를 개발하고 작성할 수 있는 기술을 보유하며, 이를 분석 및 이해할 수 있는 능력을 구비한 전문가가 요구된다.

■ 선진국의 평가기술과 방법론을 습득

CCRA 신청국의 평가능력 검증시, CAP 에서 평가전문가를 직접 신청국에 파견하여 On-Site 평가를 실시하기 때문에 선진국의 평가기술과 방법론을 우선적으로 습득해야 한다.

■ 국제협력체제 구축

CCRA 의 가입은 회원국의 만장일치를 요구하고 있으므로 CCRA 회원국들과의 신뢰구축이 CCRA 가입의 기본이 되므로 국제협력체제 구축을 위해 노력해야 한다.

2.2 CCRA 가입효과

CCRA 에 가입함으로써 얻을 수 있는 긍정적 효과는 다음과 같다.

■ 정보보호제품의 국제경쟁력 향상

정보보호제품을 여러 국가에서 다시 평가해야 하는 번거로움을 덜어주게 되어 글로벌 시장형성을 촉진하게 되며, 자국에서 개발된 정보보호제품을 평가하여 신뢰성이 입증된 제품을 수출함으로써 각국의 정보보호제품의 국제경쟁력 향상이라는 기회를 제공한다.

■ 평가기간 단축 및 평가비용 감소

단시일 내에 평가를 받아야 하는 제품은 다른 나라의 인정된 평가기관에서도 평가를 받을 수 있으며, 평가 경험이 많은 평가기관에 평가를 의뢰함으로써 평가기간을 단축할 수 있다. 중복되는 평과 과정을 제거함으로써 생기는 평가비용의 절감과 평가의뢰자가 저가의 수수료로 평가 받을 수 있는 평가기관을 선택할 수 있다는 장점도 있다.

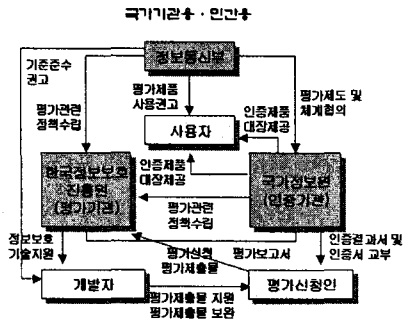
■ 수요자 선택 폭 향상

수요자 측면에서 보다 좋은 제품을 보다 싼 가격에 사용할 수 있도록 선택의 폭을 넓혀줄 수 있는데, 각국의 수요자는 일반적인 시장개방의 논리와 같이 가격과 질의 양 측면에서 직접적인 도움을 받을 수 있다.

3. 국내 평가·인증제도 현황

국내에서는 1997 년 정보통신망 침입차단시스템 평가기준과 침입차단시스템 평가·인증지침이 고시되면서 국내 평가·인증제도가 시행되었으나, 아직 선진국에 비해 많은 보완이 요구된다.

현재 국내 평가·인증제도에서는 정보통신부가 정보보호시스템 평가·인증관련 정책을 지원하고, 한국정보보호진흥원이 평가기관의 역할을 수행하며, 국가정보원이 인증기관의 역할을 담당하여 인증서를 발급한다[5]. 국가기관용과 민간용 평가의 명시적 구분은 없으나 2002 년 국내에서 CC 를 이용한 평가가 시행되면서 인증기관인 국가정보원에서 국가기관용 보호프로파일을 개발하여 보급하고 있다. 다음 [그림 1]은 국내 정보보호시스템 평가·인증제도를 설명한 것이다.



[그림 1] 국내 정보보호시스템 평가·인증제도

4. 국내 평가·인증제도 개선 방안

현재의 정보보호시스템 평가·인증제도로는 다양한 정보보호제품의 개발과 평가수요에 대한 대비가 미흡한 실정이다. 장기적으로 국내에서 평가받은 정보보호제품의 평가인증서가 국외에서도 인정받기 위해서는 CCRA 에 가입할 수 있는 기반을 구축하는 것이 중요하다. 따라서 앞에서 살펴본 것과 같이 CCRA 의 표준화된 평가기준이나 평가방법론, 평가기관 및 인증기관의 요구사항 등을 고려하여 국제환경에 맞는 국내 정보보호시스템 평가·인증제도의 수정이 절실히 요구된다.

4.1 정보보호시스템 평가·인증제도 관련기관의 개선

▣ 인증기관

CCRA 가입을 위한 국내 정보보호시스템 평가·인증제도를 구축할 때 가장 먼저 요구되는 사항은 정보보호시스템의 평가·인증을 위한 인증기관의 구축이다. CCRA 가입을 위해서는 실사를 받아야 하는데, CCRA 가입을 신청하면 CCRA 관리위원회에서 전문 위원들을 가입국에 파견하여 제품을 선정하여 평가를 의뢰하며 이 과정을 평가한다. 이는 평가기관의 평가 기술력을 평가한다는 점도 있으나, 실제로는 인증기관의 인증과정이 공정하고 신뢰할 수 있으며 객관적인가를 평가하는 것이다. 따라서 인증기관은 평가기관보다 훨씬 더 많은 평가 기술력을 확보하여 평가기관의 평가결과가 정확한지를 판단할 수 있어야 한다.

이러한 현실을 종합하여 볼 때, 국내 인증기관은 EN 45011 및 ISO Guide 65 규정을 만족하고, 평가 기술력을 더욱 확충하여 인증 및 평가경험의 노하우를 가진 발전된 형태의 운영이 요구된다.

▣ 평가기관

국외의 평가·인증제도는 초기에 공공기관을 위하여 구축되었으며, 국가기관에서 제품의 신뢰성에 대한 평가를 수행하였다. 하지만 정보보호의 중요성과 마인드가 확산되고 민간분야에서의 수요가 급증함에 따라 공공기관에서 민간분야에 요구되는 모든 제품을 평가하기에는 역부족이었다. 이에 CCRA 에 가입되어 있는 국가들은 평가능력이 인정된 민간평가기관에 평가를 일임하여 평가를 시행하고 있다.

국내에서도 정보보호시스템 평가에 대한 민간업체의 관심도가 높아지고 있어, 독립적으로 한 기관에서 모든 제품평가의 수요를 감당하기에는 어려움이 따른다. 그러므로 국내의 평가수요를 만족시키고, 평가기간을 단축시킬 수 있는 방안으로 복수의 민간평가기관을 운영하는 것이 요구된다.

앞으로 CCRA 체제를 위한 국내 평가기관은 평가자격에 대한 일반적 요구사항을 기술한 EN 45001 이나 ISO Guide 25 에 의거하여, 공정하고 객관적으로 평가를 수행할 수 있는 기술과 조건을 갖춘 민간기업으로 선정해야 한다. 또한, 복수의 평가기관을 둠으로써 시장을 독점하지 않도록 해야 한다.

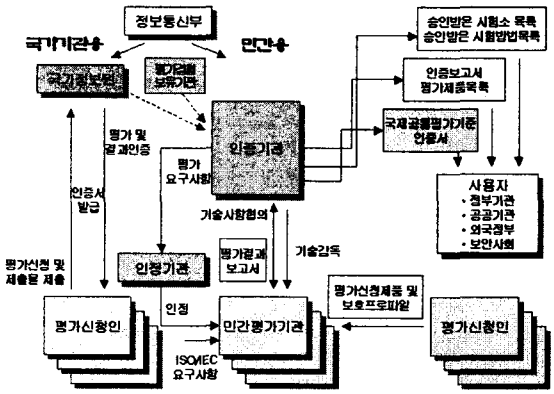
▣ 인정기관

CCRA 가입국의 경우, 민간평가기관의 자격을 심사하여 평가기관으로 지정하는 임무를 수행하는 인정기관을 두고 있다. 또, CCRA 의 가입국들은 추가적으로 평가기관이 만족시켜야 할 요구사항을 제시하고, 인정기관의 체계적인 실사를 통하여 실제 평가기관으로서의 자격을 갖추고 있는지 평가한 후 민간평가기관으로 최종 승인한다. 미국의 경우, NVLAP(National Voluntary Laboratory Accreditation Program)와 정부표준인 FIPS 150-20 을 개발하여 평가기관을 인정하는데 활용하고 있다[6]. 국내에서도 정보보호제품 평가를 위한 평가기관의 자격요건을 갖추고 있는지를 알아볼 수 있는 요구사항들을 명시한 인정기준을 반드시 제정해야 하며, 평가기관으로 인정하기 위한 절차를 명시한 프로그램을 개발해야 한다.

현재 국내에는 CCRA 에서 요구하는 인정기관의 조건을 만족하는 정보보호제품에 대한 개별적인 인정기관이 없으므로, 인정기관은 평가기관을 인정하는 기구의 운영조건을 명시하고 있는 ISO/IEC Guide 58(Calibration and Testing Laboratory Accreditation Systems

- General Requirements for Operation and Recognition) 요건에 따라 인정제도의 구축 및 운영이 필요하며, 이는 CCRA 가입시 평가하게 되는 기준이다. 인정기관의 심사과정은 실제 평가과정을 심사하는 것이 바람직하므로, 국내 평가·인증제도 개선을 위해 새로 개설되어야 하는 인정기관은 국내 현실을 반영한 인정프로그램을 개발하여 평가과정을 공정히 심사할 수 있어야 한다.

앞의 내용들을 종합하여 본 논문에서 제안하는 국내 정보보호시스템 평가·인증제도 개선안은 다음 [그림 2]와 같다.



[그림 2] 국내 정보보호시스템 평가·인증제도 개선안

4.2 정보보호시스템 평가·인증스킴 개발

평가·인증스킴은 CCRA 가입 신청시에 제출해야 하는 문서들 중 하나이다. CCRA 에 가입하기 위해서는 모든 사전 가입국의 동의를 얻어야 하는데, 이 때 평가·인증스킴은 자국의 정보보호시스템 평가·인증제도를 설명해 주는 역할뿐만 아니라, 신뢰를 얻기 위한 중요한 문서이다. CCRA 가입국들의 경우, 자국의 정보보호시스템 평가인증제도에 대한 신뢰도 및 홍보를 위하여 정보보호시스템 평가·인증스킴 문서를 공개하고 있다. 국내의 경우 국가 차원에서의 평가방법론이나 평가절차 등을 상세하게 설명하고 있는 문서는 전무한 상태이므로 국내 정보보호시스템 평가·인증제도를 설명할 수 있는 평가·인증스킴의 개발이 시급하다.

4.3 정보보호시스템 평가수수료의 현실화

국외의 경우에는 제품 평가에 필요한 인원 및 평가기간을 고려하여 평가수수료를 책정하고 있다. 하지만 국내의 경우 국가보안정책상 국내업체 육성이 필요하고, 평가제도 정착을 위해 평가수요 창출이 필요하기 때문에 평가서비스 원가를 낮게 책정했다. 국내에 민간평가기관이 지정되어 정보보호제품을 평가한다면, 현재의 평가수수료만으로는 평가기관을 운영할 수 없다. 그러므로 보다 능률적이고 효율적인 평가 활동을 위해서는 제품 평가에 투입되는 인원 및 기간을 고려하여 평가수수료를 책정할 수 있도록 하고, 평가수수료의 현실화를 위한 많은 공청회와 토론이 필요하다.

4.4 평가관련 기술력 확보를 위한 교육 및 홍보

CCRA 체제에는 복수의 민간평가기관의 설립이 필수적인데 이에 능동적으로 대응하기 위해서는 평가기관의 업무수행에 필요한 교육, 훈련, 기술적 지식 및 경험을 갖춘 충분한 수의 평가인력의 확보가 중요하다. 경쟁력을 보유하지 않은 상태에서의 CCRA 가입은 국내시장을 국외업체에게 완전히 개방하는 것이 된다. 또한 CC 평가의 근간이 되는 PP 의 경우 사용자 그룹 외에도 보안제품 개발업체가 개발해서 이를 다른 기관이 평가할 수 있도록 되어 있고, 평가신청인도 평가를 위해 ST 를 작성해야 하므로 PP 와 ST 를 이해하고 작성할 만큼 실력을 갖춘 개발자나 일반인을 위한 평가관련 교육 프로그램이 반드시 필요하다.

5. 결론 및 향후 연구과제

본 논문에서는 향후 정보보호시스템 평가·인증제도의 국제적 흐름을 결정하게 될 CC 기반의 CCRA 출범과 관련한 국내 정보보호시스템 평가·인증제도의 개선방안에 대해 제시하였다. 선진국은 CC 기반의 평가체제로 전환하며 국가 보안기관 주도의 평가업무를 대부분 민간평가기관에 이양함으로써 평가기술과 업무를 상업화하고, 자국의 정보보호제품에 대한 시장을 확보하려고 노력하고 있다. 또한 CCRA 에 가입하여 자국에서 평가·인증된 정보보호시스템을 상호인정하기로 회원국간 합의하여 표준화된 정보보호시스템 평가·인증제도에 대한 관심이 고조되고 있는 실정이다.

따라서 국내 정보보호시스템 평가·인증제도 역시 국제 환경에 맞는 평가·인증제도로의 전환이 절실히 요구되며, CCRA 가입을 위한 사전 준비에 필요한 사항들의 방향제시가 필요하다. 이에 본 고에서 제안하는 국내 정보보호시스템 평가·인증제도에 대한 연구가 계속되어야 하며, 이는 시기 적절한 CCRA 가입의 초석이 될 것으로 기대된다.

참고문헌

[1] ISO/IEC 15408, "Information technology-Security techniques-Evaluation criteria for IT security-", 1999. 12

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

[3] Common Criteria, "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security", 2000. 5

[4] Louis Giles, "The Common Criteria Recongnition Arrangement", 1st International Common Criteria Conference, 2000. 5

[5] 한국정보보호진흥원, "정보보호시스템 평가·인증 가이드", 2002. 12

[6] NIST, "Guidance to CCEVS Approved Common Criteria Testing Laboratories", 2001. 3