情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

정보보호시스템 평가·인증체계 모델 제안

김 수 연*, 오 동 규*, 이 승 우*, 최 희 봉**, 원 동 호***

요 약

최근, 정보통신 기술의 발달로 국가간의 정보 경쟁이 치열해지고 이와 더불어 개인, 사회 간의 정보경쟁 역시 치열해짐에 따라 정보 보안의 중요성이 더욱 높아져 가고 있다. 이에 선진국들은 정보보호시스템 평가·인증체계를 통해 안전성과 신뢰성을 보증하는 우수한 정보보호시스템 개발을 촉진하여 정보보호산업의 육성에 기여해 왔다. 우리나라의 경우 1998년에 처음으로 정보보호시스템 평가를 위한 기준을 고시했으나, 산업육성의 측면과 안전한 제품을 공급하여 신뢰할 수 있는 정보사회를 구축하기 위해서 국가보안시스템 평가·인증체계 모델의 보완 및 개선이 요구된다. 따라서, 본 논문에서는 국내·외 평가인증체계 관련기관 및 스킴, 절차 등을 연구 분석하고, 평가·인증체계의 요구사항을 도출하여 정보보호시스템 평가·인증체계를 제안한다.

Ⅰ. 서 론

정보기술의 발달과 정보화의 확대로 인하여 국가 및 사회, 개인간의 정보경쟁이 치열해짐에 따라 정보보호의 중요성이 더욱 높아지고 있으며, 이에 정보보호시스템의 사용이 증가하고 있다. 선진국에서는 이와 같은 제품의 신뢰성 확보를 위한 제도적 장치로서 평가기준 및 평가·인증제도를 개발하여 정보보호시스템에 대한 평가를 시행하고 있다. 1999년 국제공통평가기준인 CC(Common Criteria)는 ISO/IEC 15408 표준[1]으로 승인되어 평가에 활용되고 있으며, 미국, 영국 등의 선진국들은 국가별로 평가받은 제품의 효력을 상호 인정하는 CCRA(Common Criteria Recognition Arrangement)를 체결[2]하여 정보보호시스템의 수·출입 및 다양한 평가제품의 활용이라는 측면에서 소비자 및 개발자의 욕구를 만족시키고 있다. 국내에서는 정보보호시스템 평가·인증제도 시행 초기에 개별 제품에 대한 평가기준에 국한하여 평가를 시행하였으나, 현재는 평가의 한계를 극복하고 다양한 제품을 평가할 수 있도록 CC 기반의 평가를 시행[3] 중에 있다.

국내 정보보호시스템 평가·인증제도는 검증된 정보보호시스템을 공급하기 위한 목적으로 운영되고 있지만, 민간분야에서 요구하는 다양한 제품의 평가가 이루어지고 있지 않고, 제품평가에 소요되는 시간과 비용이 많으며, 평가된 제품이 국제적으로 상호인정되지 않는다는 문제점을 가지고 있다. 이에 이런 문제점을 해결하고 CCRA 가입에 대응을 하기 위해, 국제 환경에 적합하고 신뢰할 수 있는 국가 보안시스템 평가체계의 개선이 요구된다.

본 논문에서는 급변하는 국내·외 환경에 대처할 수 있는 국가 보안시스템 평가체계를 제안한다. 2장에서는 기존 평가체계의 문제점을 분석하여, 국가 보안시스템 평가체계 개선의 필요성에 대해서 설명하고, 국가 보안시스템 평가체계에 적합한 요구사항을 도출한다. 다음 3장에서는 평가·인증과정의 관련기관 개선과 평가·인증스킴 개발, 정보보호시스템 평가·인증절차의 제안, 평가관련 기술력 확보 등에 관한 새로운 국가 보안시스템 평가체계를 제안하며, 마지막 제4장에서 결론을 통해 이 논문을 맺는다.

Ⅱ. 기존 평가·인증체계의 분석

본 논문에서는 국가 보안시스템 평가체계를 제안하

* 성균관대학교 정보통신공학부 정보통신보호연구실 ({sykim, dkoh, swlee}@dosan.skku.ac.kr)
** 국가보안기술연구소 (hbchoi@etri.re.kr)
*** 성균관대학교 정보통신공학부 정교수 (dhwon@dosan.skku.ac.kr)

기 위해 CCRA 국가 중에서도 인증서 발행국인 CAP(Certificate Authorizing Participants)[4] 대표국인 미국과 영국을 분석하여, 현 우리나라 평가·인증체계와 비교한다. 우선, 국외의 평가·인증체계 관련 기관의 현황을 알아보고, 각 기관별 요구사항에 대해 조사하며, 다음으로 평가방법, 제도 등 평가에 대한 자세한 설명서라고 할 수 있는 국외의 평가·인증스킴을 알아본다. 또, 평가관련 기술력의 필요성을 기술하며, 분석결과에 의거하여 국가 보안시스템 평가체계 개선의 당위성을 서술한다.

1. 국내·외 평가·인증체계 관련기관 분석

1.1 평가·인증체계 관련기관 현황

미국은 평가·인증체계 실행 초기에는 국가기관의 정보보호제품에 대한 책임을 NSA(National Security Agency)[5]에 부여하였지만, 1987년 컴퓨터 보호법이 통과하면서 정부부처를 포함한 국가기관은 NSA, 민간분야는 NIST(National Institute of Standards and Technology)[6]가 책임을 지며 상호 지원하였다. 현재, 미국의 민간용 정보보호시스템의 평가는 NSA와 NIST가 공동으로 설립한 인증 및 인정기관인 NIAP(National Information Assurance Partnership)[7]에 의해 인정받은 8개의 민간평가기관이 실행하고 있다. 인정기관은 NVLAP(National Voluntary Laboratory Accreditation Program)[8]와 정부표준인 FIPS(Federal Information Processing Standards) 150-20을 개발하여 평가기관을 인정하는데 활용하고 있다.

영국도 미국과 마찬가지로, 인증기관, 인정기관, 평가기관이 조직되어 국가기관용과 민간용이 분리된 정보보호시스템 평가·인증체계를 구성하고 있다. 영국의 인증기관은 CESG(Communications Electronics Security Group)이며, 인정기관은 UKAS (United Kingdom Accreditation Service), 평가기관은 국가용은 CESG, 민간용은 5개의 민간평가기관이 맡아 평가를 시행하고 있다[9].

우리나라의 현재 국내 평가·인증체계는 정보통신부가 정보보호시스템 평가·인증관련 정책을 지원하고, 한국정보보호진흥원이 평가기관의 역할을 수행하며, 국가정보원이 인증기관의 역할을 담당하여 인증서를 발급하고 있다[10]. 그러나 선진 평가국처럼 다수의 민간평가기관이 존재하지 않으며, 평가기관을 인가해 주는 인정기관도 없는 상태이다.

〔표 1〕 각 국의 평가·인증체계 관련기관

국가	평가기관		인증기관	인정기관
	정부기관	민간기관		
미국	NSA	• Booz Allen Hamilton CCTL • COACT • Cable and Wireless CCTL • Computer Science Corp. • CygnaCom Solutions • Infogard Laboratories, Inc. • Science Applications International Co. • Netigy Corporation	NIAP	NIAP
영국	CESG	• Admiral Management Services Ltd. • EDS Ltd. • IBM Global Services • Logica UK Ltd. • Syntegra	CESG	UKAS
한국	NIS	• KISA	NIS	없음

1.2 각 기관별 요구사항

CC 평가를 기반으로 하고 있는 평가·인증체계 관련 기관인 평가기관, 인증기관, 인정기관은 공통의 요구사항을 만족해야 하는데, CCRA 가입국들을 위한 CCRA 협정서[11]에서 설명하는 각 기관의 요구사항은 다음과 같다.

(1) 평가기관 요구사항

평가기관은 EN 45001(General Criteria for the Operation of Testing Laboratories)이나 ISO Guide 25(General Requirements for the Competence of Calibration and Testing Laboratories) 혹은 이들에 대한 참가주체들에 의해 공인된 해석에 의거하여 인정된 인정기관에 의해 각 국에서 인정되고, CCRA 협정서의 부록 B.3에 의해 허가받거나 공인 받는 조건, 각 국의 법, 법적 수단, 혹은 행정절차에 의해 설립되고, 그리고 CCRA 협정서 부록 B.3의 모든 요구조건을 충족해야 한다.

(2) 인증기관 요구사항

인증기관은 EN 45011(General Criteria for Certification Bodies Operating Product Certification)이나 ISO Guide 65(General Requirements for Bodies Operating Product

Certification Systems) 혹은 이들에 대한 각 국의 해석 중 부록 C에 구체화된 요구사항을 최소한도로 만족시키는 해석에 의거하여 인정된 인가기관에 의해 각 국가에서 인가받는 조건, 각 국의 법, 법적 수단, 혹은 행정절차에 의해 설립되고, CCRA의 모든 요구조건을 충족한다는 조건을 만족해야 한다. 인증기관은 CC와 CEM(Common Evaluation Methodology)[12]을 일관성 있고 신뢰성 있게 적절히 적용하겠다는 목표를 위해 인증기관은 평가·인증스킴 내에서 진행중인 모든 종류의 평가를 적정 수준에서 감시하는 책임을 가진다.

(3) 인정기관 요구사항

CCRA 가입국의 경우, 민간평가기관의 자격을 심사하여 평가기관으로 지정하는 임무를 수행하는 인정기관을 두고 있다. CCRA의 가입국들은 추가적으로 평가기관이 만족시켜야 할 요구사항을 제시하고, 인정기관의 체계적인 실사를 통하여 실제 평가기관으로서의 자격을 갖추고 있는지 평가한 후 민간평가기관으로 최종 승인한다. 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.

2. 국내·외 평가·인증스킴 분석

2.1 평가·인증스킴 현황

미국의 초기 평가·인증스킴인 TPEP(Trusted Product Evaluation Program)[13]은 TCSEC (Trusted Computer System Evaluation Criteria)[14] 기반으로써 국가용 정보보호시스템 평가를 위한 것으로, 개발자가 자체적으로 평가신청을 할 수 있는 것이 아니라, 정부기관에서 제품을 도입하기 이전 단계에 평가를 의뢰함으로 평가 대상 제품이 선정되었다. 따라서 평가 대상 제품으로 선정되었다 하더라도 우선순위에 의해 오랜 기간을 대기해야 하는 문제점이 있었다. TPEP의 문제점을 해결하는 동시에 민간분야에서의 정보보호 마인드 확산으로 인한 평가수요의 증가를 해결하기 위하여 TTAP(Trust Technology Assessment Program)[15]를 개발하였다. TTAP에서는 C2 등급 이하의 정보보호시스템을 민간평가기관에서 평가하는 것을 전제로 하였으나, 그 등급을 상향조정하여 B1 등급까지 확대하였다. 현재는, TTAP를 대체하는 CC 기반의 CCEVS(Common Criteria Evaluation and Validation Scheme)[16]를 개발하여 시행하고 있다.

영국에는 ITSEC(Information Technology Security Evaluation and Certification Scheme)[17] 기반의 ITSEM(Information Technology Security Evaluation Manual)[18]이 있으며, CC 기반의 평가·인증스킴인 UKSP (United Kingdom Scheme Publication)가 제정되어 시행되고 있고, 이는 미국의 스킴에 비해 매우 세부적으로 기술되어 있다. 특히, 암호알고리즘 평가방법 등 평가기준의 세부 분야에 대한 평가방법론을 기술하고 있으나 스킴 전체가 공개되어 있지는 않으며, 그 일부만이 공개되어 있다.

한국은 인증기관인 국가정보원과 정책기관인 정통부, 그리고 평가제도에 관한 연구를 병행하고 있는 한국정보보호진흥원이 주축이 되어 스킴문서를 개발중에 있으나, 아직 문서가 공개되지 않았다. 2002년 정보통신부가 고시한 정보보호시스템 평가·인증지침이 있지만, 각 단계별로 구분한 세부적인 평가·인증절차나 각 평가·인증관련 기관의 요구사항들에 대해 자세히 기술하고 있지 않으며, 대략적인 조건만을 설명하고 있으므로 평가·인증스킴이라고 볼 수 없다. 그러므로 CC를 기반으로 한 국내 평가·인증스킴의 개발 및 보완이 요구된다.

정보보호 평가·인증제도를 설명하기 위해 개발된 평가·인증스킴 문서 목록은 다음 표 2와 같다.

2.2 평가·인증스킴 요구사항

정보보호시스템 평가·인증스킴을 개발하는 목적은 정보보호시스템 평가·인증과 관련된 조직의 체계적인 구성과 관리로 평가·인증의 공정성을 유지하고 일관성을 확보하는 것이다. 평가·인증스킴 문서의 구성은 국가별로 상이하지만, 대체로 평가·인증체계 관련기관을 지원하기 위한 문서가 요구된다.

이러한 스킴은 평가·인증제도를 운영하는 국가별로 평가·인증결과에 대한 상호신뢰를 가능하게 하며, CCRA 가입요건의 하나로도 스킴문서를 요구하고 있다. 스킴문서는 문서의 초안작성, 다양한 통로를 통한 의견수렴, 문서초안의 개정, 최종심의 그리고 문서 최종본의 완성 등의 절차를 위해서 많은 물적, 인적 자원과 긴 시간이 요구된다. 평가·인증스킴의 개발이라

〔표 2〕 각 국의 평가·인증스킴 문서

국가	평가·인증스킴 문서
미국	• NIAP Common Criteria Evaluation and Validation for - IT Security Organization, Management and Concept of Operation - IT Security Validation Body Standard Operating Procedures - IT Security Technical Oversight and Validation Procedures - IT Security Guidance to Common Criteria Testing Laboratories - IT Security Guidance to Sponsors of IT Security Evaluations - IT Security Certificate Maintenance Program
영국	• Description of the Scheme • The Appointment of Commercial Evaluation Facilities - CLEF Requirements Part 1. Start up and Operation - CLEF Requirements Part 2. Conduct of an Evaluation • Sponsor's Guide Role of Sponsor in IT Security Evaluation and Certification • Developer's Guide - Part 1. Roles of Developer in ITSEC - Part 2. Reference for Developers - Part 3. Advice to Developers • Manual of computer Security Evaluation - Part 1. Evaluation Procedures - Part 2. Standard Evaluation Work Programmes - Part 3. Evaluation Techniques and Tools • UK Certified Product List • Certifiers' Guide • Scheme Information Notices • UK IT Security Evaluation Scheme • Evaluation Work Programmes • Relationship between accreditation document set and security targets for evaluation • UK Certification Maintenance Scheme - Part 1. Description of the CMS - Part 2. Impact Analysis and Evaluation Methodology - Part 3. DSA Reference Manual
한국	• 없음

는 것은 단순한 문서의 작성이 아니라, 한 나라의 공정하고 신뢰할 수 있는 평가·인증의 체계를 세우는 것이므로 평가·인증과 관련된 기관과 전문가들의 많은 참여와 관심이 요구된다.

3. 평가관련 기술력 분석

3.1 국내·외 평가관련 기술력 현황

현재 미국에서 IT 보안 평가 활동을 수행하는 민간 평가기관의 직원은 컴퓨터 공학과 관련된 기술적인 분야의 석사학위 이상이나 이와 동등한 경험을 가지고 있어야 한다. 민간평가기관 직원에 대한 훈련은 평가 보고서의 생성을 포함한 시험 방법들에 대한 일반적인 요구사항이나 컴퓨터 공학의 개념, 컴퓨터 보안, CC와 CEM에 대한 작업 지식 등과 같은 분야에 대해 집중적으로 수행된다.

영국의 평가관련 기술력의 확보를 위한 평가자 훈련은 ITSEC에 기초를 둔 원리를 완전히 이해하며, 모든 기준을 선정 조건에서 지정된 임의의 평가 레벨에 적용할 수 있도록 평가자를 양성한다. 영국의 평가·인증스킴은 상급 평가자에 의해 훈련받는 평가자, 자격이 있는 평가자, 상급 평가자 이렇게 3단계의 자격을 인정하며, 평가자 훈련프로그램으로 M1-기본보안컨셉, M2-평가기술접근, M3-계획과 업무, M4-외부의 기관 등 4개 모듈을 설명하고 있다. 평가 후보자가 모듈 M1과 M2를 만족하게 완성하면, 그들은 훈련받은 평가자로 간주되며, 자격을 갖춘 평가자가 되기 위해서는 관련 OJT 경험과 함께 모든 모듈의 완료가 요구된다. 자격을 갖춘 평가자는 그들의 평가업무를 통하여 경험을 계속적으로 얻게 될 것이고, 그런 경험의 축적으로 상급 평가자로서의 승인을 얻게 된다.

국내 평가·인증관련 인력은 국외 평가·인증관련 인력에 비해 현저히 부족하며, 특별히 인력 양성을 위한 홍보나 교육의 기회가 거의 없는 상황이다. 이에 정보보호시스템 평가·인증의 인적기반 조성을 위해서 정보보호시스템 평가·인증분야의 고급 전문인력 양성 교육을 지원해야 하며, 국외 관련 기관의 협조를 통해 평가·인증 기술력을 습득할 기회를 마련해야 한다.

3.2 평가관련 기술력 요구사항

CCRA의 평가기관 인정을 위한 조건에서는 평가자에 대한 요구사항으로 '각각의 스킴의 공인 정책에는 평가자의 보안 요건과 훈련 요건의 세부항목이 포함되어 있다'라는 내용이 명시되어 있다. 그러므로 평가자의 자격, 훈련 프로그램, 평가자의 등급구분, 등급별 자격 등의 평가자를 위한 스킴문서가 요구되며, 평가자 양성을 위한 교육 및 자격부여 프로그램이 필요하다. 또한, CCRA 신청국의 평가능력 검증시, CAP에서 평가 전문가를 직접 신청국에 파견하여 현장 평가를 실시하기 때문에 평가자는 선진국의 평가기술과 방법론을 우선적으로 습득해야 한다. CCRA 체제에는 복수의 민간평가기관의 설립이 필수적인데, 이에 능동

적으로 대응하기 위해서는 평가기관의 업무수행에 필요한 교육, 훈련, 기술적 지식 및 경험을 갖춘 충분한 수의 평가인력의 확보가 중요하다. 그리고 CC 평가의 근간이 되는 PP(Protection Profile)의 경우 사용자 그룹 외에도 보안제품 개발업체가 작성해서 이를 다른 기관이 평가할 수 있도록 되어 있고, 평가신청인도 평가를 위해 ST(Security Target)를 작성해야 하므로 PP과 ST를 이해하고 작성할 만큼 실력을 갖춘 개발자나 일반인을 위한 평가관련 교육 프로그램이 반드시 필요하다.

Ⅲ. 국가 보안시스템 평가체계 제안

앞에서 살펴본 바와 같이, 국내에서는 1998년부터 정보보호시스템 평가·인증제도를 시행하여, 국내에 적합한 평가·인증제도를 구축하는데 주력하여 왔다. 하지만, 평가 수요의 대부분이 아직은 국가용 제품에 있으며, 민간용 제품에서는 그 수요가 크지 않은 것으로 판단되어 현재까지 민간평가기관이 지정되지 않은 상태이다. 국내 정보보호산업은 지난해 500억원 규모에서 올해는 1500억~2000억원 규모로 빠르게 성장할 것으로 예측되며, 정부는 인터넷 기반의 IT 인프라를 구축하여 정보화 사회 건설을 국가적인 지상 과제로 삼고 있다. 즉, 정보보호산업은 인터넷 서비스에 대한 안전과 신뢰성 제고를 통해 국내의 산업경쟁력을 높이는 밑거름이 될 뿐 아니라 국가 안보와도 직결된다. 국내 정보보호업체들은 정보보호시스템 평가에 많은 관심을 가지고 있으며, 특히 경쟁업체보다 빨리 평가를 받아야 시장확보에 유리한 위치를 선점할 수 있기 때문에 신속히 평가를 받기 위하여 노력하고 있다. 그러나 현재의 정보보호시스템 평가·인증체계로는 다양한 정보보호시스템의 개발과 평가수요를 충족시킬 수 없으며, CCRA에 가입하기 위한 요구사항 부족의 문제 등 아직 미흡한 점을 가지고 있다. 그러므로, 국제적으로 확산되고 있는 CC를 이용한 정보보호시스템 평가·인증제도를 수행하기 위해서는 현재 국가 보안시스템 평가체계의 개선이 요구되며, 다음에서 새로운 국가 보안시스템 평가체계에 관해 제안한다.

1. 평가·인증 관련기관 개선

국가 보안시스템 평가체계를 위한 첫 번째 제안 사항으로 평가·인증과정에 연관된 각 기관들에 대한 개선점을 제시한다.

1.1 평가기관

국내 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 역부족이다. 국내 평가기관은 민간 평가수요의 확대와 CCRA 가입의 요구사항에 맞게 개선되어야 하는데, 국가용 정보보호시스템의 평가의 경우에는 국가보안사항에 대한 공개되지 않는 기밀사항을 평가·인증해야 하므로 평가기관과 인증기관을 분리하지 않고, 한 기관에서 평가와 인증의 역할을 동시에 수행하도록 한다. 또한, 민간용 정보보호시스템의 평가의 경우, 정보보호시스템 평가에 대한 민간업체의 관심도가 높아지고 있어, 독립적으로 한 기관에서 모든 제품평가의 수요를 감당하기에는 어려움이 따르므로 국내의 평가수요를 만족시키고, 평가기간을 단축시킬 수 있는 방안으로 복수의 민간평가기관을 운영한다.

앞으로 CCRA 체제를 위한 국내 평가기관은 평가자격에 대한 일반적 요구사항을 기술한 EN 45001이나 ISO Guide 25에 의거하여, 공정하고 객관적으로 평가를 수행할 수 있는 기술과 조건을 갖춘 민간기업으로 선정해야 한다. 즉, 높은 보안성을 요구하는 국가용 제품에 대해서는 따로 평가를 수행할 수 있는 기관이 요구되며, 공정하고 객관성 있게 평가를 수행할 수 있는 기술과 조건을 갖춘 민간평가기관을 선정하여 문제점을 보완하고 복수 평가기관을 둠으로써 시장의 독점을 막도록 한다.

1.2 인증기관

인증기관에 대한 개선방향은 우선, 인증기관을 국가용과 민간용 제품평가에 대한 두 개의 인증기관으로 분류해야 하고, 이원화 된 두 기관이 서로 다른 인증정책을 수행하지 않도록 상호 협의하고 관리 할 수 있는 기구의 신설이 필요하다. 또한, 인증기관의 역할, 규정, 절차 등에 대해 명확하게 문서화해야 한다. 국내 인증기관을 국가용과 민간용 제품의 평가에 대한 두 개의 인증기관으로 분류하여 얻을 수 있는 효과는 첫째, 국가용으로 사용하는 EAL4 등급 이상의 제품의 보증결과를 얻기 위한 평가·인증비용과 소요되는 기간을 줄이고 평가에 대한 인증 결과의 효율성을 높일 수 있다. 둘째, 국가용과 민간용 제품이 만족해야 하는 보증요구사항이 다르므로 각 기관이 주로 인증하

는 사항에 대한 기술력을 집중 투자 및 보완하여 인증결과의 신뢰성을 높일 수 있다. 셋째, 민간평가기관을 도입함에 따라 민간평가기관에 대한 관리 및 평가결과에 대한 보증을 해주는 기관이 요구되는데, 이를 국가용과 민간용 제품평가의 인증을 구별하지 않고 하나의 인증기관에서 단독으로 수행한다면, 인증기관의 역할과 책임이 편중되는 문제점이 있다.

CCRA에 가입할 경우, CCRA 관리위원회에서는 평가기관의 평가기술력을 평가하는 것 뿐만 아니라, 실제로는 인증기관의 인증과정이 공정하고 신뢰할 수 있으며 객관적인지를 평가한다. 그러므로, 인증기관은 평가기관보다 훨씬 더 많은 평가기술력을 확보하여야 하고 평가기관의 평가결과를 정확하게 판단할 수 있어야 한다. 이러한 현실을 종합하여 볼 때, 국내 인증기관은 CCRA의 요구사항인 EN 45011 및 ISO Guide 65 규정을 만족하고, 평가 기술력을 더욱 확충하여 인증 및 평가경험의 노하우를 가진 발전된 형태의 운영이 요구된다.

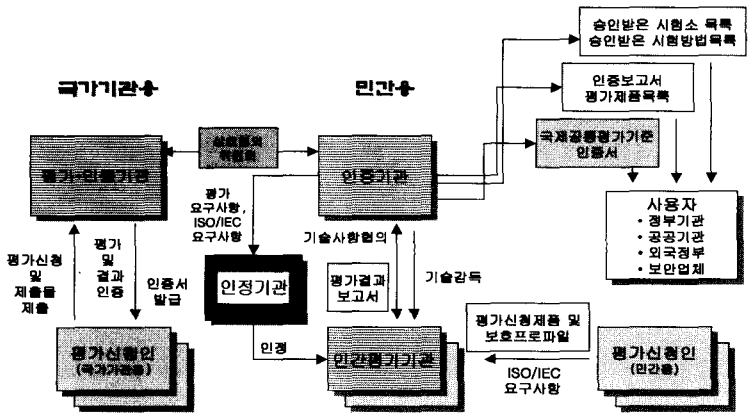
1.3 인정기관

복수의 민간평가기관을 지정하기 위해서는, 민간평가기관이 공정하고 객관적으로 평가할 수 있는 능력을 보유하였는지 심사 해야한다. 미국의 NIAP, 영국의 UKAS 등 선진 각 국은 별도의 기관을 지정하여 평가기관의 자격을 심사하는 임무를 수행하고 있으며, 이들 인정기관들은 ISO/IEC 17025와 이를 기반으로 하는 평가기관 자격 요건을 정하여 평가기관 지정심사를 하고 있다. 인정기관은 평가기관을 평가하는데 있어서, 공정성(평가기관이 평가자의 편견을 배제), 객관성(평가자의 주관적 요소 및 개인적 견해를 최소화), 반복성(동일한 평가기관에서 같은 제품을 평가하여도 동일한 평가결과 발생), 재생성(여러개의 평가기관에서 하나의 평가대상물을 평가하여도 동일한 평가결과 발생)을 만족시키는지에 대한 심사과정이 포함되어 있어야 한다. 그러므로, 평가기관의 공정한 심사와 CCRA 가입을 위한 필수 조건으로 국가차원의 인정기관이 필요하며, 인정기관은 평가기관 인정프로그램을 이용하여 평가기관등록의 심사를 주관해야 한다.

평가·인증관련 기관에 대한 개선안을 종합하였을 때, 제안하는 평가·인증체계 관련기관의 구성도는 다음 그림 2와 같다.

2. 평가·인증스킴 개발

현재 국내에는 평가·인증체계를 위한 구체적인 평가방법론이나 평가절차 등에 대한 문서가 없기 때문에 새로운 국가 보안시스템 평가체계를 위해서는 평가·인증스킴의 개발이 요구된다. 평가·인증스킴이란 평가신청자나 사용자에게 정보보호시스템 평가·인증제도에 대한 신뢰를 높이기 위해 평가·인증제도, 평가기준, 평가방법론, 평가관련 기관의 임무 등을 설명한 문서들이다. 평가·인증스킴은 단순하게 자국의 평가·인증제도를 설명하는 것이 아니라, 실제로 다른 국가에게 평가·인증제도에 대한 신뢰를 얻기 위해 필요하며, CCRA 가입시 요구되는 가장 중요한 도구라고 할 수 있다. 이에 미국, 영국, 캐나다 등은 자국의 평가·인증스킴 문서를 공개하여 정보보호시스템 평가·인증제도를 설명하고 있다.



〔그림 1〕 제안하는 평가·인증체계 관련기관

현재 국내에서 정보보호시스템 평가·인증체계와 관련하여 공식적으로 발표된 문서는 정보보호시스템 평가·인증지침, 국가기관용 PP, 정보통신망 침입차단시스템 평가기준, 정보통신망 침입탐지시스템 평가기준, 정보보호시스템 공통평가기준 등이 있다. 그러나, 이 문서들은 평가방법이나 절차에 대한 개략적인 내용이 기술되어 있으므로 새로운 평가·인증스킴은 평가·인증관련 전문가를 통해 자세한 과정 및 방법을 설명하고, 국내 평가·인증제도를 누구나 이해할 수 있도록 쉽게 작성되어야 한다.

다음 표 3은 본 논문에서 제안하는 국가 보안시스템 평가체계를 위한 평가·인증스킴이다.

〔표 3〕 제안하는 평가·인증스킴 문서

총 론	• 조직구성 • 관련 조직들의 임무 • 관련 조직들의 자격 요건 (기준과 자격 부여 방법 및 절차) • 관련 조직들의 상호관계 • 평가기준과 평가방법의 개요 • 스킴 문서의 전체 구성에 대한 소개
인 증	• 인증기관의 자격요건 • 인증기관의 자격 부여 방법 및 절차의 세부적 설명 • 인증기관의 관리와 운영 • 인증의 방법과 기준 • 인증절차
평 가	• 평가기관의 자격요건 • 평가기관의 자격부여 방법 및 절차의 세부적 설명 • 평가기관의 관리와 운영 • 평가의 방법과 기준 • 평가절차
평가기관 인정	• 인정기관의 자격요건 • 인정기관의 관리와 운영 • 인정의 방법과 기준 • 평가기관 인정절차
평가신청인	• 평가신청인의 자격 • 평가신청을 위한 준비사항과 신청절차 • 평가신청인의 권리와 의무
인증서 유지	• 인증서 유지의 주체 • 인증서 유지방법과 절차

3. 평가기관 인정기준 개발

새로운 국가 보안시스템 평가체계를 위해서는 평가기관을 인정하기 위한 구체적인 인정기준이 개발되어야 한다. 국내 평가수요가 증가하면서 평가시간을 단축시킬 방법은 복수의 평가기관을 인정하여 제품을 평가하는 것이다. 즉, 복수의 평가기관을 지정하기 위한 구체적인 기준이 있어야 하는 것이다. 현재 미국의 경우, NVLAP과 FIPS 150-20을 개발하여 평가기관을 인정하는데 사용하고 있고, 캐나다 영국 등 평가선진국의 경우에도 평가기관이 갖출 요건을 개시하여 민간평가기관 인정에 활용하고 있다. 그러므로, 국내에서도 평가기관의 자격을 알아볼 수 있는 요구사항을 명시한 인정기준을 개발하여야 하고, 평가·인증스킴에 그 절차를 명시해야 한다.

4. 정보보호시스템 평가·인증절차 개선

본 논문에서 제안하는 국내 정보보호시스템 평가·인증절차는 평가신청인과 인정기관 사이에 평가를 진행하는 국가용 정보보호시스템에 대한 평가·인증절차와 평가신청인과 평가기관, 인증기관이 필요한 민간용 정보보호시스템에 대한 평가·인증 절차로 구분한다.

4.1 국가용 정보보호시스템 평가·인증절차

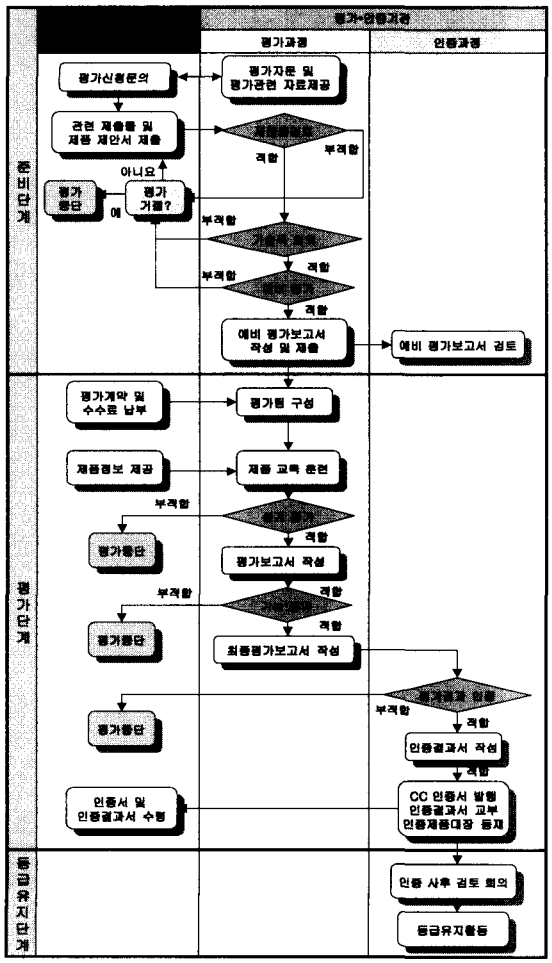
제안하는 국가용 정보보호시스템의 평가·인증절차의 경우, 국가보안사항에 대한 공개되지 않는 기밀사항을 평가·인증해야 하고, 평가·인증비용과 소요되는 기간을 줄일 수 있으며, 인증결과의 효율성 및 신뢰성을 증대시키기 위해 평가기관과 인증기관을 분리하지 않고, 한 기관에서 평가와 인증의 역할을 동시에 수행한다. 국가용 정보보호시스템에 대한 평가는 높은 등급의 보안성이 요구되며, 평가결과는 보안 제품 활용에 대해 특정 지침을 제공한다. 그리고, 국가용 정보보호시스템에 대한 평가·인증과정은 국가보안 및 IT 산업발전의 조화를 위해 필요하다.

국내에서 CC에 따른 평가가 2002년 8월부터 시행되면서, 인증기관인 국가정보원에서는 국가기관에 조달을 목적으로 하는 정보보호시스템의 안전성 및 신뢰성을 확보하기 위해 국가기관용 PP을 개발하여 보급하고 있다. 그리고, CC 평가를 받은 상용제품 및 CCRA의 인정제품을 각 국가기관에 보급하기로 방침을 세우고 있다. 그러나, 이는 정보보호시스템의 제한적인 사용과 제품 사용에 따른 추가적인 평가가 요구되기 때문에, 환경 적용 평가 등 부분적으로만 시행될 수 있다. 그러므로, 국가용 정보보호시스템을 인증하는 평가·인증기관은 국가보안정책을 수립하여 국가암호논리를 적용하고, 국가용 정보보호시스템을 보증

할 수 있는 평가·인증절차를 수립해야 한다.

국가용 정보보호시스템 평가·인증절차는 평가준비단계, 평가단계, 등급유지단계로 이루어져 있으며, 국가기관에서 사용 가능한 높은 등급의 보안을 요구하는 제품을 평가하기 때문에 준비단계에서 민간용 제품 평가보다 치밀한 평가과정을 수행하게 된다. 국가용 정보보호시스템 평가·인증절차는 준비단계에서 평가계약 수락 여부를 결정할 수 있는 세 번의 평가단계를 수행하며, 평가단계에서는 설계평가와 기능평가를 수행하여 준비단계에서 이루어졌던 평가보다 체계적이고 실질적인 보안요구사항을 평가한다. 마지막 등급유지단계에서는 인증사후검토회의를 통하여 인증된 제품의 등급유지를 위한 활동을 한다.

다음 그림 3은 제안하는 국가용 정보보호시스템 평가·인증절차에 대한 설명이다.



〔그림 2〕 제안하는 국가용 평가·인증절차

(1) 준비단계

제안하는 국가용 정보보호시스템 평가·인증절차의 준비단계는 본 평가를 시작하기 전, 준비단계 과정에서 평가신청인이 제출한 제출물이나 제안서 등에 대한 검토를 여러번 수행하여 평가결과를 더욱 확실히 보증할 수 있다는 점을 특징으로 한다.

준비단계는 평가신청인이 국가용 정보보호시스템의 평가를 수행하는 국가용 평가·인증기관에 신청을 문의하고, 신청 문의를 받은 평가·인증기관은 평가에 대한 자문 및 평가관련 자료를 신청인에게 제공하면서 시작된다. 평가관련 자료에는 국가용 정보보호시스템 평가 과정의 간단한 기술과 평가신청시에 평가신청인이 제출해야 할 제품 제안서의 요구사항, 평가기준, 문의사항, 예제문서 등의 내용이 포함된다. 평가신청인은 평가를 진행하기 원한다면, 제품개요, 제품질문서에 대한 답변서, 간단한 회사의 약력 등이 포함된 제품 제안서와 제출물 등을 평가·인증기관에 제출한다. 국가용 제품 평가·인증기관은 평가신청인으로부터 시장성, 재정적인 면과 CC 요구사항을 만족하기 위한 적당한 보안 메커니즘을 제공하는지 등을 판단하기 위해 제품 제안서와 제출물을 검토한다.

국가용 제품 평가·인증기관은 검토 후에 요구사항이 만족되면, 평가후보로 받아들이고 평가준비를 돕는다. 평가검토시에 평가·인증기관은 추가적인 자료를 요청할 수 있고, 기술적인 부분이 부족하거나, 시장성이 없는 경우에는 제안을 거절하고 거절한 배경에 대해 설명한다. 제안서 및 제출물이 적합한 경우, 기술적 회의를 갖는다. 기술적 회의는 제품에 대한 첫 번째 조사로써, 제품 공급자의 시연, 질의응답, 정보교환 등으로 구성된다. 기술적 회의를 토대로 평가여부를 결정하여, 평가가 가능할 것으로 결정한 경우, 기술적 회의보다 더욱 체계적이고 자세한 내용을 평가하는 예비 평가 일정을 세운다. 만약 평가 불가 결정이 내려지면, 평가신청인에게 평가 불가 결과와 사유를 고지하며, 평가신청인은 관련 제출물이나 제품 제안서를 보완하여 다시 평가를 의뢰할 수 있다. 예비 평가는 제품과 평가증거물의 완전성을 정확히 검토하고 제품 공급자의 평가준비 상태를 점검하는 것으로 설계문서와 시험문서를 바탕으로 진행하게 된다. 예비 평가는 실제 평가단계는 아니지만, 민간용 제품의 평가단계와 비슷한 과정을 수행하게 되는데, 이는 국가용 보안제품이 민간용 제품에 비해 만족해야 하는 보안요구사항이 더 많으므로 실제 평가단계에 앞서 최소한의 요구사항을 미리 평가하는 것이다. 국가용 평가·인증

기관은 평가신청인이 제출한 서류에 추가하여, CC에 의해 요구되는 평가증거물인 상세 설계문서나 매뉴얼, 사후관리계획 등을 제공받아 평가할 수 있다. 예비 평가의 결과로 예비 평가보고서를 작성하고, 평가의 결과 외에 앞으로 필요한 사항이나 CC의 각 요구사항에 대한 제품의 대략적인 평가, 기술적인 문제와 관리적인 문제점 등을 기술한다. 예비 평가에 대한 최종결정이 내려지면, 실제적인 평가가 시작되며, 예비 평가 결과는 본 평가에서 평가보고서를 작성할 때 이용하며, 그 결과를 인증한다.

(2) 평가단계

제안하는 국가용 정보보호시스템 평가·인증절차의 평가단계는 앞에서 진행한 준비단계의 기술적 회의와 예비 평가에서 기본적으로 요구되는 1차적 평가를 미리 수행한다. 민간용 제품 평가단계는 대략적인 사항에 대한 관찰보고서를 작성하고 구체적인 평가를 진행하지만, 국가용 제품 평가단계는 준비단계의 평가보다 좀더 구체화된 사항인 보안제품의 설계부분이나 기능을 시험하는 것을 중점으로 둠으로써, 세부 보안요구사항들을 평가할 수 있는 특징이 있다. 평가신청인이 국가용 정보보호시스템 평가·인증기관과 평가계약을 맺고 평가수수료를 납부하면, 평가단계가 개시된다. 평가계약서가 체결되면 평가·인증기관은 평가팀을 구성하고, 평가신청인은 평가팀의 훈련을 준비할 수 있도록 제품에 대한 정보를 제공한다. 평가·인증기관은 시스템의 하드웨어와 소프트웨어 구성요소를 포함하는 제품설계, 개발업체의 설계문서, 사용자 문서, 테스트 문서, 사후관리 문서 등을 분석을 통해 설계평가를 수행한다. 만약, 평가결과가 부적합하면 평가는 중단되고, 평가가 적합한 경우, 평가·인증기관은 설계문서에 대한 평가 결과를 평가보고서에 작성한다. 평가보고서를 작성한 후, 평가결과가 적합하다면 국가용 정보보호시스템 평가·인증기관은 평가관련 요구사항에 대한 기능시험과 침투시험등의 기능평가를 수행하고, 부적합하다면 평가는 중단된다. 국가용 정보보호시스템 평가·인증기관은 기능평가가 완료한 후에, 시험결과에 대한 문서와 평가보고서를 수정하여 최종평가보고서를 작성하며, 작성한 최종평가보고서를 검토하여 CC 인증서의 발행여부를 결정한다. 검증결과, 평가를 의뢰한 정보보호시스템의 평가결과가 성공적으로 완료된 것으로 결정되면, 제품은 인증제품대장에 등재되며, 인증결과서가 교부된다. 최종평가보고서의 인증과정의 수행 결과, 평가의 결과를 인증할 수 없으면 평가는 중단된다.

(3) 등급유지단계

국가용 정보보호시스템 평가·인증절차의 마지막 과정은 등급유지단계이다. 민간용 정보보호시스템 평가·인증절차의 인증과정에서 수행되는 인증사후검토회의가 국가용 정보보호시스템 평가·인증절차에서는 하나의 단계로 분리되면서, 국가용으로 사용되는 제품의 사후관리 및 등급유지활동을 더욱 신뢰하며, 보증할 수 있다는 특징이 있다. 등급유지단계는 평가신청인이 자격요구사항, 평가계약서의 조건과 규칙을 만족시키는 경우에만 계속적으로 인정하게 된다. 인증받은 제품의 사후관리를 위해 평가신청인과 평가·인증기관은 검토회의를 가지게 되며, 등급유지프로그램에 따른 등급유지활동을 시작한다.

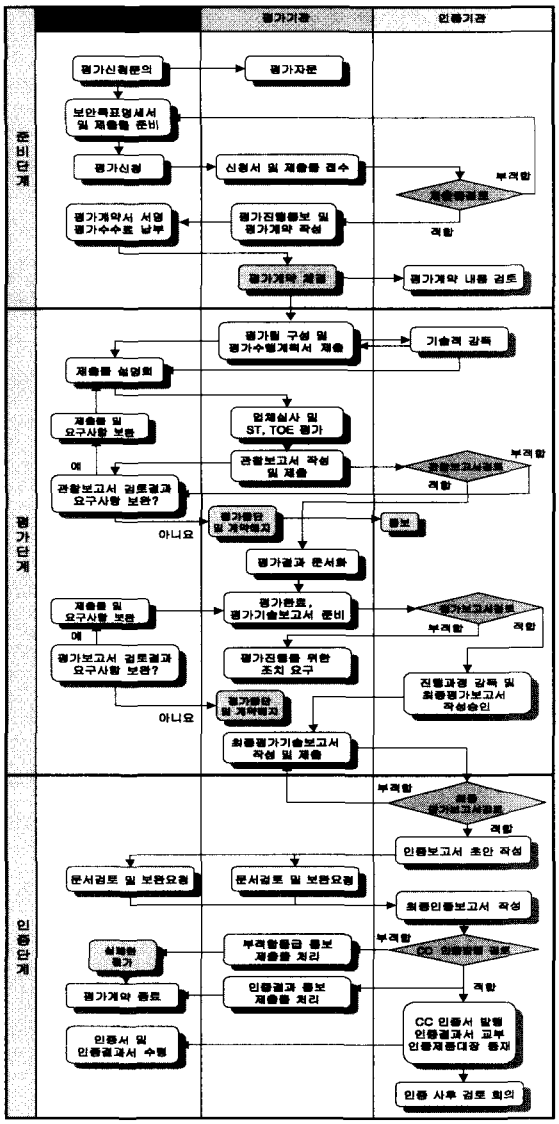
4.2 민간용 정보보호시스템 평가·인증절차

국내 평가·인증관련 기관 개선안에서 민간용 정보보호시스템의 평가를 위해서는 다수의 민간평가기관이 필요하며, 민간평가기관은 평가의 역할만을 전담하고, 민간평가기관의 평가결과를 인증해 주는 역할은 민간용 평가의 인증의 임무를 수행하는 인증기관이 한다고 제안하였다. 그러므로, 제안하는 민간용 정보보호시스템 평가·인증절차는 평가신청인, 평가기관, 인증기관 사이에서 이루어지는 CC 기반의 평가로써, 평가절차는 크게 준비단계, 평가단계, 인증단계의 3부분으로 나뉜다. 제안하는 민간용 정보보호시스템 평가·인증절차는 기존의 평가·인증 절차보다 준비단계 및 평가단계의 인증기관의 검토 과정이 많으며, 평가신청인과 평가기관, 인증기관이 평가·인증결과를 상호협의를 통해 보완하는 과정이 추가된다. 또한, 평가·인증단계의 마지막 수행과정에 인증사후검토회의를 통해 인증결과를 지속시키는 과정이 포함된다.

다음 그림 4는 제안하는 민간용 정보보호시스템 평가·인증 절차이다.

(1) 준비단계

평가준비단계는 평가기관이 평가할 제품에 대한 설명과 향후 진행될 평가 수행에 따른 방법과 결과물, 절차 및 스케줄 등에 대해 인증기관에 설명하는 단계이다. 기존의 국내 평가·인증절차의 준비단계에서는 평가기관이 제출물을 검토하여 평가수행 여부를 결정하였으나, 제안하는 민간용 정보보호시스템 평가·인증 절차의 준비단계에서는 인증기관이 평가 제출물 검



〔그림 3〕 제안하는 민간용 평가·인증절차

토의 역할을 담당하도록 하여 민간평가기관의 부담을 줄여주고, 인증기관이 결과를 승인하는 역할을 하도록 한다. 평가신청인은 평가를 받기 위해 승인된 다수의 민간평가기관 중 적합한 평가기관을 선택하는데, 평가기관의 평가경험, 평가비, 평가스케줄, 다른 부수적인 요소 등을 통해 신중히 판단한다. 평가신청인은 보안목표명세서 및 평가관련 제출물을 준비하여 선택한 평가기관에 평가를 신청하고, 평가 수행에 대한 검토를 받기 위해서 평가기관은 평가신청인에게 받은 신청서와 제출물 및 평가기관에서 작성한 평가계획서 등의 문서를 첨부하여, 인증기관에 제출한다. 평가계획서는 ST 또는 PP, 평가계획, 평가준비단계와 관련된 사항을 기록한 것으로 예를들어, 신청인, 평가자 등의 이름 등을 말한다. 인증기관이 평가기관에서 받은 문서가 적합하다고 판단될 경우, 인증기관은 평가기관에 평가진행을 통보하고, 부적합하다고 판단될 경우에는 평가신청인에게 제출물에 대한 보완을 요청해야 한다. 즉, 인증기관은 평가수락 여부를 결정하는 권한을 갖고 있다. 신청인이 제출물을 보완하지 않을 경우, 평가신청서 접수를 거부한다. 평가진행을 통보받은 평가기관은 평가신청인과 평가계약을 맺고 평가수수료가 납부되면, 평가과정을 수행한다.

(2) 평가단계

제안하는 민간용 정보보호시스템 평가·인증절차의 평가단계에서는 평가신청인이 제출한 제출물을 평가신청인, 평가기관, 인증기관이 서로 검토하는 과정을 추가하고, 평가기관의 평가결과를 인증기관이 인증함에 따라 평가결과를 신뢰할 수 있다. 기존 국내 평가단계에서는 평가보고서를 한번만 작성하지만, 제안하는 평가단계에서는 평가기관이 평가한 결과를 관찰보고서와 평가보고서를 통해 두 번 인증기관에 보고하여 평가의 신뢰도를 높인다.

평가 준비단계에서 평가자의 제출물에 대한 검토와 회의결과에 평가에 적합한 판정이 나오면, 인증기관은 평가를 진행할 것을 평가기관에 통보하는 것과 동시에 인증기관은 정확한 평가를 위해 기술적 감독을 제공한다. 인증기관은 평가기관이 평가팀을 구성하고, 평가수행계획서 등의 내용을 평가 과정을 모니터하며, 인증계획에 따라 인증 활동 과정을 문서화한다. 실제적인 평가에 들어가기 전에 평가신청인은 평가기관 및 인증기관과 제출물 설명회를 갖게 된다. 제안하는 민간용 정보보호시스템 평가·인증 절차에서 실제 평가는 민간평가기관이 수행하게 되는데, 민간평가기관은 보안명세서와 TOE를 평가하고, 인증기관은 인증계획에 따라 평가기관의 활동을 감독한다. 평가후, 평가기관은 인증기관에 관찰보고서를 제출하게 되며, 인증기관은 관찰보고서를 검토하여 그 결과를 평가기관에 보낸다. 인증기관에서 관찰보고서 검토후에는 제출물 보완이 필요한 경우, 평가신청인에게 관찰보고서 검토결과를 통보하고 제출물 보완을 요구한다. 평가신청인은 이를 확인하여 합당하거나 평가를 계속 이행하기를 원한다면, 제출물을 보완한다. 만약, 평가신청인이 응하고 싶지 않다면, 제품에 대한 보안 평가를 포기하고 이를 평가기관에 통보하면 평가의 중단 및 계약을 해

지할 수 있다. 평가완료 후 평가기술보고서의 양식에 따라 보고서를 작성 후 인증기관에 제출한다. 평가기술보고서는 TOE 또는 PP 평가와 평가수행 방법을 기술한 것과 평가결과에 대해 요약한 문서이다. 평가자 활동보고서 또는 평가 작업 단위에 의해 이루어진 판단에 대한 증거가 확실하다는 것을 증명하기 위해 인증기관은 평가기술보고서를 검토하고, 이 과정에서 증거가 만족스럽지 못한 경우, 평가에 대한 분과 판단을 확증할 수 있는 평가증거물을 검토한다. 인증기관은 평가기관이 작성한 평가기술보고서를 검토하여 적합할 경우, 평가기관이 최종 평가기술보고서를 작성하도록 하고, 문제를 검토하고 계속 진행과정을 감독한다. 만약 보고서 검토 결과 부적합하다고 판단되면, 평가를 중단하고 일정기간 안에 평가기관에 평가의 진행을 위한 조치를 요구하고, 평가기관은 평가신청인에게 시정을 요구한다. 평가기관의 평가절차 검토는 인증기관에서 허가한 평가와 평가절차에 따라 평가를 수행하는 지를 판단하는 것이다. 평가를 위한 절차 중에 평가시작단계에서 문서화되지 않은 것이 있고, 새로운 단계가 있다면, 인증기관은 새롭게 바꾼 절차를 검토해야 한다. 평가기관은 평가기술보고서의 수정사항을 참조하여 최종 평가기술보고서를 작성하며, 이는 인증기관에만 제출한다. 인증기관은 보고서를 검토하고 다음 과정인 인증단계를 준비한다.

(3) 인증단계

인증기관은 최종평가기술보고서를 접수한 후에 평가준비단계에서 검토한 결과와 최종평가기술보고서를 이용하여 인증보고서의 초안을 만들고, 평가기관과 평가신청인에게 문서 검토 및 보완을 요청한다. 평가신청인과 평가기관의 검토에 의해 변화된 사항은 인증기관에 보완을 요청한다. 인증기관은 평가신청인과 평가기관의 동의를 얻어 최종 인증보고서를 작성하고, 인증기관 최상위 관리자에게 제출하여 CC 인증서의 발행 여부를 결정한다. 이 때 부적합 판정을 받으면, 실패한 평가가 되며 평가가 종료된다. CC 인증서의 발행이 결정하게 되면, 인증기관은 CC 인증서와 인증결과서를 교부하며 인증제품 대장에 제품을 등재한다. 그리고 CCRA에 가입 했을 경우, CCRA 기관에 제품의 인증 사실을 알린다. 인증서의 발급한 후에는, 인증기관과 평가기관 절차의 끊임없는 개선을 위해 효율적인 평가과정 및 인증과정에 대해 토론하고, 추후 재인증시에 절차를 향상시킬 수 있는 방법에 대해 추천을 받는 사후 검토회의가 열리게 된다.

5. 평가관련 기술력 확보

CC를 기반으로 한 국가 보안시스템 평가·인증체계를 구축하기 위해서는 평가·인증 관련 기술력이 요구된다. CC 평가의 근간이 되는 PP의 경우 사용자 그룹 외에도 보안제품 개발업체가 작성해서 이를 다른 기관이 평가할 수 있도록 되어 있고, 평가신청인도 평가를 위해 ST를 작성해야 한다. 그러나 PP나 ST의 개발은 제품의 운영환경에 따라 도출될 수 있는 위협을 나열해야 하고, 이로부터 시스템 또는 데이터를 보호하기 위해 보안기능 요구사항과 보증 요구사항을 포함한 요구사항들을 도출해 내야 하므로 개발이 쉽지 않다. 그러므로 현재 평가가 잘 이루어지는 국가에서 실제적인 교육을 통해 관련 기술을 확보하거나, PP 또는 ST를 개발하는 프로젝트를 국외의 평가관련 선진국과 함께 수행함으로써 기술을 전수 받는 등의 방법 등의 방법을 고려하여 평가관련 기술력을 확보해야 한다. 또한, 평가자의 자격, 훈련 프로그램, 평가자의 등급구분, 등급별 자격 등의 평가자를 위한 국내 스킴 문서가 요구되며, 평가자 양성을 위한 교육 및 자격부여 프로그램을 개발해야 한다. 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.

Ⅳ. 결 론

본 논문에서는 향후 정보보호시스템 평가·인증체계의 국제적 흐름을 결정하게 될 CC 기반의 CCRA 요구사항을 만족하는 국가 보안시스템 평가체계를 제안하기 위해서, 선진국의 평가·인증체계를 분석하여 우리나라 실정에 맞는 평가·인증체계를 제안했다. 선진국은 CC 기반의 평가체계로 전환하며 국가 보안기관 주도의 평가업무를 대부분 민간평가기관에 이양함으로써 평가기술과 업무를 상업화하고, 자국의 정보보호제품에 대한 시장을 확보하려고 노력하고 있다. 또한 CCRA에 가입하여 자국에서 평가·인증된 정보보호시스템을 상호인정하기로 회원국간 합의하여 표준화된 정보보호시스템 평가·인증체계에 대한 관심이 고조되고 있는 실정이다. 따라서 국내 정보보호시스템 평가·인증체계 역시 국제 환경에 맞는 평가·인증체계로의 전환이 절실히 요구되며, CCRA 가입을 위한 사전 준비에 필요한 사항들의 방향제시가 필요하다.

본 논문에서는 제안한 국가 보안시스템 평가·인증 체계는 다음과 같다. 우선, 국가 보안시스템 평가체계를 위한 첫 번째 제안 사항으로 평가·인증과정에 연관된 기관에 대한 개선점을 제시했다. 평가기관은 현재의 단일 기관에서 공정하고 객관성 있게 평가를 수행할 수 있는 기술과 조건을 갖춘 복수의 민간평가기관으로의 변경이 요구되며, 높은 보안성을 요구하는 국가용 제품의 경우에 대해서는 독립적으로 평가를 수행할 수 있는 전문기관이 설립되어야 한다. 인증기관은 인증기관의 역할, 규정, 절차 등에 대해서 정확히 문서화하고, 국가용과 민간용 제품으로 분류하여 인증기관을 이원화해야 하며, 이렇게 이원화된 두 인증기관을 관리하고 상호 교류하기 위한 기구가 설치되어야 한다. 또한, 공정하고 객관적으로 평가할 수 있는 능력을 보유한 민간평가기관을 심사하기 위한 역할을 하기 위해 인정기관의 설립이 요구된다. 둘째, 현 국내 평가체계에는 구체적으로 평가방법론이나 평가절차 등에 대한 상세한 내용을 담은 문서가 없으므로 이에 대한 구체적인 문서인 스킴의 작성이 필요하다. 즉, 평가신청자나 사용자에게 정보보호시스템 평가·인증제도에 대한 신뢰를 높이기 위해 평가·인증제도, 평가기준, 평가방법론, 평가관련 기관 및 사용자의 임무 등을 설명한 문서를 개발해야 한다. 셋째, 인정기관이 평가기관을 인정하기 위한 구체적인 민간평가기관 인정기준을 개발해야 한다. 민간평가기관의 자격에 대한 요구사항을 명시한 인정기준의 개발을 통해 공정성과 반복성, 재생성 등의 평가자격을 갖춘 민간평가기관이 인정될 수 있을 것이다. 넷째, 평가관련 기술력을 확보해야 한다. 실제 제품에 대한 평가를 위해서는 CC를 이해하고, PP와 ST를 개발할 수 있는 기술을 갖춘 평가인력이 요구된다. 이에 실제적인 교육과 홍보를 통한 관련 기술력의 확보가 필요하다.

본 논문은 국내 정보보호시스템 평가·인증체계의 활성화를 위한 요구사항을 분석하여, 평가의 인프라에 대비할 수 있는 자료로 활용될 수 있으며, 향후 국가간 정보보호시스템에 대한 상호인정에 관한 협정인 CCRA에 가입을 위한 기초 방안을 제공할 것으로 기대된다.

참 고 문 헌

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

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

[3] 정보통신부고시 제 2002-40호, "정보보호시스템공통평가기준", 2002. 8.

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

[5] http://www.nsa.gov

[6] http://ts.nist.gov

[7] http://niap.nist.gov

[8] Department of Commerce U.S., "National Voluntary Laboratory Accreditation Program v1.1", April 1999.

[9] http://www.cesg.gov.uk

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

[11] Common Criteria, "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security", May 2000

[12] Common Criteria, "Common Methodology for Information Technology Security Evaluation, Part2 : Evaluation Methodology", August 1999.

[13] http://www.radium.ncsc.mil/tpep/tpep.html

[14] Department of Defense Standard, "Department of Defense Trusted Computer System Evaluation Criteria", December 1985.

[15] http://www.radium.ncsc.mil/tpep/ttap/

[16] http://niap.nist.gov/cc-scheme/index.html

[17] Michael Gehrke, Andreas Pfitzmann, and Kai Rannenberg, "Information Technology Security Evaluation Criteria (ITSEC)", Proc. IFIP 12th World Computer Congress Madrid, 1992.

[18] Commission of the European Communities, "Information Technology Security Evaluation Manual(ITSEM)", 1993.

〈著 者 紹 介〉

김 수 연 (Soo-Yeon Kim)
학생회원

2003년 2월 : 서울여자대학교 컴퓨터공학과 졸업(공학사)
2003년 3월~현재 : 성균관대학교 정보통신공학부 석사 과정
〈관심분야〉 정보보호시스템 평가 및 인증, 공통평가방법론, 정보보호

오 동 규 (Dong-Kyu Oh)
학생회원

2002년 2월 : 성균관대학교 정보공학과 졸업(공학사)
2003년 3월~현재 : 성균관대학교 정보통신공학부 석사 과정
〈관심분야〉 정보보호, 무선통신 보안, 정보보호 평가

이 승 우 (Seung-Woo Lee)
학생회원

2001년 2월 : 강남대학교 전자계산학과 졸업(공학사)
2003년 3월 : 성균관대학교 대학원 전지전자 및 컴퓨터 공학부 졸업(공학석사)
2003년 3월~현재 : 성균관대학교 정보통신공학부 박사 과정
〈관심분야〉 정보보호, PKI, 정보보호 평가

최 희 봉 (Hee-Bong Choi)
정회원

1984년 2월 : 부산대학교 전기공학과 졸업(공학사)
1987년 3월 : 부산대학교 대학원 전기공학과 졸업(공학석사)
2002년 2월 : 성균관대학교 대학원 전기전자 및 컴퓨터 공학부 졸업(공학박사)
1987년 2월~2000년 1월 : 국방과학연구소 선임연구원
2000년 1월~현재 : 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 보안시스템 설계 및 평가

원 동 호 (Dongho Won)
정회원

성균관대학교 전자공학과 졸업 (학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~1999년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
2002년~2004년 : 성균관대학교 연구처장
현재 : 성균관대학교 정보통신공학부 교수, 정통부 지정 정보보호 인증기술 연구센터장
〈관심분야〉 암호이론, 부호이론, 공개키 기반구조