情 報 保 護 學 會 誌
第17卷 第3號, 2007. 6

국내 정보보호 시스템 평가기관 승인 자격기준 개발*

유다혜,** 윤신숙,** 오수현,** 김환구**

요 약

정보보호 시스템 평가제도는 안정성과 신뢰성이 검증된 시스템사용을 권장하고 이를 통해 정보보호 제품 개발을 유도하며 정보보호 산업 육성을 기여하기 위한 것이다. 최근 정보보호 제품의 해외 경쟁력 증대를 위하여 인증된 평가기관 설립의 필요성이 대두되고 있어 본 논문에서는 국내 환경에 적합한 국내 정보보호 시스템 평가·인증 제도의 평가기관 자격 기준을 제안하고자 한다. 이를 위하여 본 논문에서는 해외 각 국의 인증 요구사항 및 절차를 항목별로 상세히 비교·분석하였으며, 이를 토대로 국내 실정에 맞는 국내 정보보호 시스템 평가기관 승인 요구사항을 도출하였다. 적절히 제안된 평가기관 설립 기준안은 평가가기관의 추가 설립을 위한 기준안으로 활용될 수 있을 것으로 기대한다.

Ⅰ. 서 론

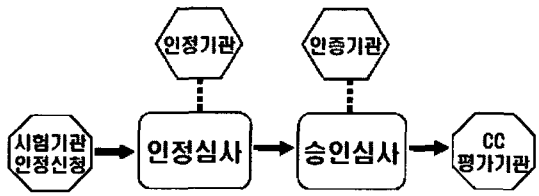
CC(Common Criteria) 인증은 국제적으로 통용되는 정보보호 제품에 대한 평가 기준으로 국내에서는 CC 인증이 정보보호 솔루션에 국한된 것으로 인식되어 왔다. 하지만, 이미 선진국들은 CC인증을 정보보호 솔루션을 넘어 IT와 관련된 모든 제품의 보안성과 신뢰성을 보증하는 인증으로 인식하기 시작했다.

CC평가기관의 경우 인정기관으로부터 심사를 받은 후, 인증기관의 평가기관 요구사항에 대하여 별도의 심사를 받아야 하며, 이것이 통과되면 공식적으로 CC 평가기관으로 인정이 된다. 이러한 절차는 〔그림 1〕과 같다.

CC인증은 CCRA(Common Criteria Recognition Arrangement : 국제공통평가기준 상호인정협정)에 따라 인증서 발행국(CAP) 중 한곳에서 정보보호 제품에 대한 평가 인증서를 받게 될 경우, 다른 회원국에서 평가 인증서를 그대로 사용할 수 있게 된다.

우리나라는 2006년 5월 CAP국이 되면서 국내에서 평가 인증한 CC 인증서를 해외에서 모두 인정받을 수 있게 되어, 국내 보안 기업은 물론 IT기업들의 해외 수출에 든든한 지원 체제를 갖출 것으로 예상하고 있다.

현재 우리나라가 CAP국에 참여하게 됨으로써 국내에도 인증된 평가 기관 설립의 필요성이 대두되고 있으며, 평가기관 설립을 위한 국내 평가기관 인정 및 승인을 위한 자격기준 개발이 필요한 실정이다.



〔그림 1〕 CC 평가기관 승인절차

정보보호 시스템 평가기관 자격기준 개발은 국가적, 경제적 중요성을 지니고 있으며, 이러한 중요성을 인식하여 본 논문에서는 CCRA 인증서 발행 국가를 중심으로 IT 보안성 평가기관의 자격 기준을 분석하고, 이를 토대로 국내 평가기관 자격 기준을 제안하고자 한다.

Ⅱ. 국외 평가기관의 요구사항 및 승인절차

각 국에서 예비 평가기관은 일정한 자격기준을 만족하여 평가기관으로서 승인을 받은 후, 정보보호 제품에 대한 인증을 실시하고 있다.

본 장에서는 CCRA의 인증서 발행국(CAP)중 미국, 영국, 스웨덴, 일본, 캐나다 5개국의 평가기관 승인 기

* 본 논문은 정보통신부의 출연금 등으로 수행한 정보보호체계 강화사업의 결과입니다.
** 호서대학교(yfresh99@nate.com, yss28@hanmail.net, shoh@office.hoseo.ac.kr, hkkim@office.hoseo.ac.kr)

준에 대하여 평가기관 요구사항, 평가기관 승인 절차로 분류하여 분석한 결과를 기술한다.

2.1. 미국

미국의 승인 기본 요구사항은 NIST 핸드북 150과 150-20의 절차 및 요구사항을 충족해야 한다고 규정하고 있다. 평가기관의 경영 구조 및 책임자에 대한 구조는 NVLAP(National Voluntary Laboratory Accreditation Program) 요구사항을 이행하도록 지명된 평가기관 이사, 대표이사, 승인된 서명자, 평가팀 팀장, 선임평가자, 경영·품질시스템에 대한 전체 책임 직원, 품질 경영자 직원을 유지해야 한다.

평가기관으로 승인 받기위해 첫 번째로 평가기관은 충분히 실행되어온 관리 시스템, 품질 메뉴얼, 연계된 문서, 신청서 양식을 NVLAP로 송부한다. 송부 된 문서를 검토한 후, NVLAP는 현장심사를 거쳐 평가기관으로서의 승인을 결정한다.

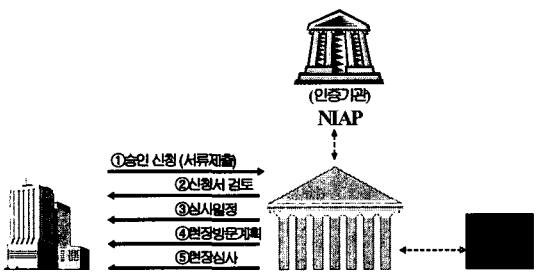
평가기관 승인을 유지하기 위해서는 CCEVS(Common Criteria Evaluation Validation Scheme) 요구사항을 매년 재확인을 통하여 승인을 평가하고 NVLAP는 2년에 한 번 현장평가를 수행하여 재평가를 한다. 평가기관이 CCEVS와 NVLAP의 요구사항을 준수하지 않았을 경우 평가기관의 자격은 보류 또는 철회될 수 있다.

미국의 평가기관 승인절차를 요약하면 [그림 2]와 같다.

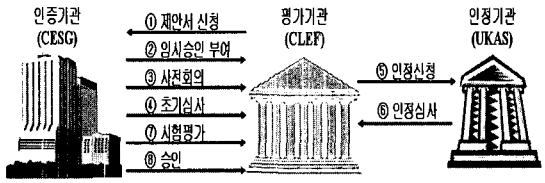
2.2. 영국

영국의 평가기관 기본 요구사항은 임원, 조직구조, 평가기관에서 갖춰야할 설비, 인증 감독관등 상세한 내용을 언급하고 있다.

영국에서 평가기관으로 승인 받기위해서는 CLEF (Commercial Licensed Evaluation Facility)를 설치·관



[그림 2] 미국의 평가기관 승인절차



[그림 3] 영국의 평가기관 승인절차

리하는 방법에 대하여 상세히 서술하여 인정기관에 제출해야 하고, 이 제안서를 인증기관이 인정할 경우 임시승인 부여가 이루어진다.

임시승인 부여가 이루어진 후 사전회의를 거쳐 초기심사에 들어가면 상세한 평가를 거치고 인증기관의 시험 평가 완료 후, 인증기관으로부터 최종 승인을 받는다.

승인에 대한 갱신은 현장감사와 재평가로 나눌 수 있는데, 현장 감사는 인정 후 6개월 이내에 실시하고 차후로는 1년 간격으로 수행한다. 재평가는 인정 후 3년 6개월 이내에 한번 실시하고 차후로는 4년 간격으로 수행한다. 만약 UKAS 인정이 경과되거나 승인조건을 위반한 사실이 발견된 경우 승인을 철회 할 수 있다.

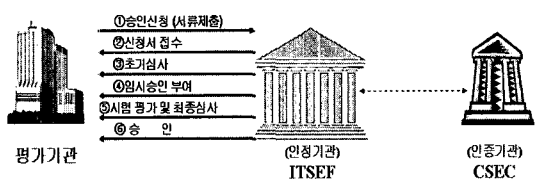
영국의 평가기관 승인절차를 요약하면 [그림 3]과 같다.

2.3. 스웨덴

스웨덴은 평가기관 기본요구사항으로 기밀성 유출 방지를 강조하고 있고, 조직구조, 문서화 요구사항, 인증감독관에 대해서도 명시하고 있다.

스웨덴의 평가기관은 승인을 받기위해 인증기관에 승인을 신청해야 하며 신청서를 제출할 때에는 조직에 관한 기본적 사항, ITSEF(IT Security Evaluation Facility) 부서장의 서명 등 부가적인 서류의 첨부가 필요하다. 초기심사 이전에 사전회의를 거치며 초기심사가 완료되면 임시승인을 부여 받고 시험평가를 받을 수 있는 자격이 주어진다.

시험평가를 성공적으로 완료하고 평가기관 요구사항을 충분히 만족한다면 승인을 부여받는다.



[그림 4] 스웨덴의 평가기관 승인절차

ITSEF의 승인 기간은 4년이며, 승인 갱신을 위한 새로운 심사를 수행해야 한다. 승인유지를 위해서는 ITSEF 요구사항과 승인유지 요구사항을 이행해야 한다.

스웨덴의 평가기관 승인절차를 요약하면 〔그림 4〕와 같다.

스킴 절차 요구사항이 불이행 되었을 경우 또는 불이행 조건이 6개월 이내 해결되지 않았을 경우에 승인은 보류상태가 되며, 보류조건이 기간 내 해결되지 않았거나 승인조건을 심각하게 위반했을 경우 승인을 철회, 종료한다.

2.4. 일본

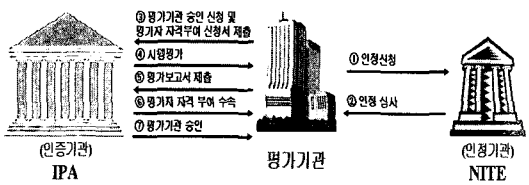
일본의 평가기관 기본 요구사항은 평가기관의 조직구조에 대해 간단하게 기술하고 있으며, 문서화 요구사항과 인증 감독관에 대해서는 언급하고 있지 않다. 일본의 평가기관 승인절차는 인정기관으로부터 인정서를 부여 받은 후 인증기관에 신청서와 함께 인정서와 기타 서류를 제출하는 과정을 거쳐 평가기관 승인을 받는다.

문서가 접수되고 확인이 이루어지면 평가자 심사의 평가를 통하여 시험평가를 치루고 평가기관으로서 승인을 받게 된다. 평가기관의 승인은 4년 동안 유지되며, 갱신은 승인을 받은 뒤 4년 후 재심사를 수행해야 한다. 일본은 보류에 대한 사항을 언급하지 않고 있으며, 철회에 대한 사항으로 평가기관에 평가 가능한 평가자가 없거나, 더 이상 평가를 수행할 능력이 없는 경우, 홈페이지에 기재되어 있는 승인 요구사항에 적합하지 않은 경우, 그리고 평가기관이 승인 철회를 요청 한 경우에는 평가기관 승인을 철회하게 된다.

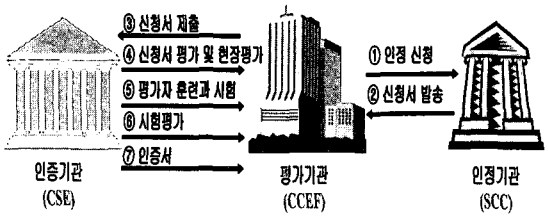
일본의 평가기관 승인절차를 요약하면 〔그림 5〕와 같다.

2.5. 캐나다

캐나다는 평가기관 인정을 받기 위하여 인정기관에



〔그림 5〕 일본의 평가기관 승인절차



〔그림 6〕 캐나다의 평가기관 승인절차

신청서와 양식을 제출한다. 인증기관의 승인과 인정기관의 인정은 동시에 수행될 수 있다.

인증기관은 초기심사로 신청서 평가, 평가자 훈련 및 검사, 시험 평가를 받은 후 평가기관 승인을 받는다. 인증에 관한 철회조건은 다른 국가와 마찬가지로 요구사항을 만족하지 못하거나, 결함이 기간 내 교정되지 않았을 경우로 제시하고 있다.

캐나다의 평가기관 승인절차를 요약하면 〔그림 6〕과 같다.

Ⅲ. 국외 평가기관 자격기준 비교·분석

본 장에서는 평가기관 요구사항에 대해서 각 국의 승인 요구사항을 비교·분석하여 기술한다. 기본 요구사항은 조직구조와 문서화 요구사항 그리고 인증 감독관으로 나누어 이를 세부적으로 분석한다. 또한 승인절차와 승인유지, 승인종료 방법에 대해서도 상세히 비교하여 우리나라에 적절한 평가기관 요구사항을 도출한다.

3.1. 평가기관 요구사항 비교·분석

기본 요구사항은 세부적으로 조직구조와 문서화 요구사항 그리고 인증 감독관으로 나뉘어 진다.

〔표 1〕 기본요구사항 비교표

공통 요구사항	스웨덴	- CCRA 요구사항을 만족해야함 - 인정기관에 의한 평가기관 승인 - 인증기관과의 협력
	영국	
세부 요구사항	영국	- 기록보관시설
	일본	- 평가기관 독립성, 비밀자료 유지
	미국	- NIST 핸드북 150 요구사항 만족
	캐나다	- CAN_P_4D & CAN_P_1591B 요구사항 만족

〔표 2〕 조직구조 비교표

공통 요구사항	스웨덴	- 물리적 보안, 고객정보 기밀성 - 기밀성을 위해 직원변동을 최소 - 한사람이 여러 역할을 위임 가능 - 책임자 역할의 세분화
	영국	
세부 요구사항	스웨덴	- 역할은 한 사람이 맡아서 책임
	영국	- 소그룹의 평가자 팀으로 수행 - 기술책임자에게 보고
	미국	- 1인 다 직책 이상의 업무

〔표 3〕 문서화 요구사항 비교표

공통 요구사항	스웨덴	- 보안 매뉴얼의 문서화
	영국	
세부 요구사항	영국	- 품질 매뉴얼 보유
	미국	- 문서의 주기적 검토 및 개정 - 컴퓨터시스템 관리문서의 관리 방안 및 절차

〔표 4〕 인증감독관 비교표

공통 요구사항	스웨덴	- 인증감독관 임명
	영국	
세부 요구사항	영국	- 인증감독관에게 모든 권한 부여
	스웨덴	- 이미지에 손상이 될 수 있는 일은 삼가야 함

기본요구사항은 각 국의 특성에 맞게 기술하고 있으며, 그 중 스웨덴과 영국에서 CCRA 요구사항 만족 및 인증기관과의 협력에 대한 내용을 공통 요구사항으로 서술하고 있다. 우리나라 평가기관이 인정기관의 승인을 취득하기 위해서는 국제적 인식을 고려하여 〔표 1〕의 공통 요구사항을 기본으로 준수하도록 하는 것이 적합하다.

〔표 2〕는 각 국가별 조직구조에 대하여 비교한 표이다. 표의 요구사항을 살펴보면 스웨덴과 영국은 조직구조의 요구사항으로 물리적 보안, 고객정보의 기밀성 등을 공통으로 정의하고 있다.

우리나라 평가기관의 적절한 조직구조 형성을 위해서는 자격을 갖춘 직원의 유지와 조직구조를 통해 역할을 분배하고 책임자를 세워야 한다.

평가기관으로 승인 받기위해서는 적절한 문서화 요구사항을 만족해야 한다. 스웨덴과 영국은 절차 및 책임에 관한 설명을 보안 메뉴얼에 문서화 시키도록 요구하고 있으며, 미국에서는 컴퓨터시스템 관리 문서의 관리 방안 및 절차를 수립해야 한다고 정의하고 있다. 〔표 3〕은 국가별 문서화 요구사항에 대하여 비교해 놓은 표이다.

우리나라는 미국과 같이 전산화가 널리 이용되고 있기 때문에 전산 시스템 문서의 관리가 중요하게 정의되어야 한다고 판단된다.

인증감독관은 인증기관과 연락을 취하는 역할자로, 그 이외에도 평가기관의 신청사항을 처리하고, 스킴에 참여하는 인원으로서 평가기간 동안 기술지원과 지도활동을 수행 할 수 있는 능력을 가진 사람을 임명하여 평가활동에 편의를 제공해야 한다.

3.2. 평가기관 승인절차 비교·분석

평가기관 승인 절차는 초기 승인, 승인 유지, 승인 종료 과정으로 구성된다. 초기 승인에서는 각 국의 승인 절차와 승인신청, 임시승인 부여, 사전 회의, 초기심사, 시험 평가, 인증기관 최종심사로 과정으로 이루어져 있다. 승인 유지에서는 갱신주기와 승인유지 절차에 대하여 비교·분석하였으며, 승인 종료에서는 보류와 철회로 나누어 비교 · 분석한다.

3.2.1 승인

미국의 경우 인정기관에 승인 신청을 시작으로 평가기관 승인에 대한 평가를 수행한다. 미국은 영국과 달리 인정기관에서 신청기관이 평가기관으로서 자격을 갖추었는지 평가한다.

영국은 인증기관이 평가를 수행한다. 시험평가 이전에 인정기관에 인정신청을 하여 시험평가 후반에 인정을 부여 받고 시험평가를 완료하여 인증기관에 최종 승인을 받는다.

스웨덴의 경우 인정기관에 승인신청을 하고 신청서 접수 완료시 승인 ID를 부여 받는다. 초기심사 이전에 사전회의를 거치며 초기심사가 완료되면 임시승인을 부여 받고 시험평가를 받을 자격이 주어진다. 시험 평가를 성공적으로 완료하고 평가기관 요구사항을 충분히 만족한다면 승인을 부여받는다.

일본은 인정기관으로부터 인정서를 부여 받은 후 인증기관에 신청서와 함께 인정서와 기타 서류를 제출하는 과정을 거쳐 평가기관 승인을 받는다.

캐나다는 인정을 받기위하여 인정기관에 인정신청을 하여 신청서와 양식을 제출 후 인증기관의 신청서 평가, 평가자 훈련 및 검사, 시험 평가를 받은 후 평가기관 승인을 받는다.

각 국의 평가기관 승인절차를 비교하면 일반적으로 평가기관에서 일정한 양식을 갖춘 신청서를 인증기관에 제출하고, 적절한 절차를 밟게 된다. 단, 미국의 평가기관은 인정기관에게 승인신청을 한다.

〔그림 2〕부터 〔그림 6〕는 각 국가별 평가기관 승인절차이다.

국내 평가기관 승인절차는 일반적 사항을 고려하여 인증기관에 일정 양식을 갖춘 신청서를 제출하는 방법을 제시하였다.

3.2.2 승인신청

승인신청 과정에서 5개국 모두 신청서 양식을 제출해야하며 영국과 미국, 일본, 캐나다는 품질 메뉴얼을 추가로 제출하도록 요구하고 있다.

스웨덴은 접수한 신청서가 적절하다면 승인 ID를 부여하여 승인 취득과정을 식별한다. 영국은 신청서 제출 시 품질 메뉴얼과 보안 메뉴얼을 제출해야 한다. 일본은 평가기관 관련 준수사항 서약서, 품질 메뉴얼, 교육·훈련과 관련된 서류, 시험 평가의 대상과 관련된 서류, 평가 업무 실시 계획서, 평가 공평성 및 독립성 대조표, 인정서 사본 또는 인정신청서 사본을 제출해야한다. 미국의 경우 품질 메뉴얼과 관리 시스템을 보유해야 한다고 규정하고 있다.

캐나다는 독립성과 설비의 요구사항 충족 여부를 증명해야 하며 평가자 증명서와 예비 평가자 기술/경험 기록표를 인증기관에 제출하여야 한다. 인증기관의 승인과 인정기관의 인정은 동시에 실행 할 수도 있다. 하지만 최종심사는 인정과정을 모두 통과해야 가능하다.

만약 우리나라가 영국, 스웨덴, 일본 또는 캐나다의 절차를 따를 경우 영국과 같이 품질 메뉴얼과 보안 메뉴얼을 같이 제출하도록 하는 것이 적합하다.

3.2.3 임시승인 부여

평가기관의 승인을 위해 임시 승인을 부여하는 국가는 스웨덴과 영국이다. 스웨덴은 초기 심사 후 요구사항이 만족할 경우 임시 승인을 부여한다. 영국은 이와 달

〔표 5〕 승인신청 요구사항 비교표

공통 요구사항	영국	- 신청서 양식 제출 - 품질 매뉴얼 제출
	일본	
	미국	
	캐나다	
세부 요구사항	영국	- 보안 메뉴얼도 추가 제출
	일본	- 관련 서약서 및 서류 추가제출
	미국	- 관리 시스템 보유
	캐나다	- 독립성 설비의 요구사항 충족여부 증명
	스웨덴	- 신청서만 제출 - 신청접수 인정 시 승인 ID 부여

〔표 6〕 임시승인부여 비교표

공통 요구사항	영국	- 임시 승인 부여
	스웨덴	
세부 요구사항	영국	- 초기심사 후 임시 승인 부여
	미국	- 제안서를 인증기관이 허용할 경우 임시 승인 부여
	스웨덴	- 경영시스템과 NIST 핸드북 150을 만족하는지 검토

〔표 7〕 사전회의 비교표

공통 요구사항	스웨덴	- 승인 취득 과정에 대한 정보 제공
	미국	
	영국	
세부 요구사항	미국	- 초기 현장 방문 일정 계획 - 본격적인 현장 방문 일정 계획 - 요구사항들의 개선기회 제공
	스웨덴	- 승인 취득 과정의 기본 계획 및 승인 합의에 대한 회의

〔표 8〕 초기심사 비교표

세부 요구사항	영국	- 초기 훈련 프로그램은 관련 직원이 담당
	미국	- 초기방문은 두 명의 평가자가 이틀반 동안 진행
	캐나다	- 인증기관에 제출한 신청서의 통과여부 확인 - 설비와 독립성 요구사항 확인
	스웨덴	- 인증기관은 품질 및 보안 시스템 문서와 평가자 자격에 관한 문서 심사 - 평가기관에 현장 방문 실시, 초기심사 시행

리 신청 시 제출한 제안서를 인증기관이 인정할 경우 임시 승인을 부여한다. 일본은 임시 승인 부여에 대한 내용은 언급하고 있지 않으며, 미국의 경우 임시 승인을 부여 하지 않으며 단지 경영시스템, NIST 핸드북 150을 만족하는지 검토한다.

우리나라의 경우에도 영국과 스웨덴과 같이 평가를 받고 있는 평가기관의 현 평가 상태를 파악하기 위해, 임시 승인 절차를 도입하는 것이 필요하다. [표 6]은 각 국가별 임시승인 부여에 대하여 비교한 표이다.

3.2.4 사전회의

평가기관의 승인과정에서 일본과 캐나다를 제외한 스웨덴, 영국, 미국에서는 사전 회의를 실시한다. 사전 회의는 승인 취득 과정에 대한 정보를 제공하며 스웨덴은 추가로 승인 취득 과정의 기본 계획과 승인 합의에 대해서 회의를 실시한다. 미국은 사전 회의에서 초기 현장방문 일정을 계획하고 현장방문에 대해 의견을 조정하여 심사할 요구사항들의 변경 및 개선의 기회를 갖는다. 그 후 성공적으로 모든 기타 인정 요구사항을 충족하면 본격적인 현장방문 일정을 계획한다. [표 7]은 국가별 사전회의에 대하여 비교한 표이다.

우리나라의 경우에도 신청서를 접수하여 초기 심사를 수행하기 전, 앞으로의 승인 취득 과정과 조언을 얻을 수 있는 사전 회의를 실시하는 것이 적합하다.

3.2.5 초기심사

초기 심사 과정에 대한 각 국가의 세부 요구사항은 다음과 같다. 먼저 스웨덴의 경우 인증기관은 품질 및 보안시스템 문서와 ITSEF 요구사항에서 서술한 평가자 자격에 관한 문서를 심사하고 평가기관에 현장방문을 실시하여 초기 심사를 수행한다. [표 8]은 각 국가별 초기심사에 대하여 비교한 표이다.

우리나라는 스웨덴과 영국의 초기심사를 접목하여 평가자에 대한 훈련 및 감시를 수행하고, 평가기관에 대한 현장 방문을 통해 평가기관이 요구사항들을 적절히 이행하는지 심사하도록 하는 것이 적합하다.

3.2.6 시험평가

시험평가의 시행 목적은 평가기관이 보안성 평가 수행 능력을 인증기관에 입증하기 위한 것으로 [표 9]를 살펴보면 영국, 스웨덴에서는 실제 평가 시 사용될

[표 9] 시험평가 비교표

공통 요구사항	영국	- EAL4 또는 ITSEC E3 수준에서 수행 - 시험 평가는 인증기관에 의해 엄격한 감독 하에 수행 - 평가자를 최소한 한명 배치해야 함
	스웨덴	
세부 요구사항	영국	- 3~4개월 동안 시험 평가를 실시
	일본	- 평가자 심사를 통과해야 함
	캐나다	- CCS 기술 감독의 평가 요구사항을 만족해야 함 - IT제품은 평가기관이 평가를 통과하였다면 평가를 받지 않아도 됨
	스웨덴	- 기술 감독 외 한 명 이상의 승인 부여자를 지명하여 엄격한 감독 하에 수행 - ITSEF 승인은 평가한 제품의 인증서 없이도 진행 가능

[표 10] 승인 비교표

세부 요구사항	스웨덴	- 심사결과를 평가기관에 승인 합의 보고서로 보고
	영국	- 승인 부여자는 시험 평가에서 얻어진 평가보고서를 고려하여 승인여부 판단
	미국	- 품질시스템 검토, 현장방문, 시험에서 얻어진 정보를 기준으로 NVLAP가 인정을 최종 결정
	캐나다	- 인증기관은 인수 서한을 평가기관에 제공
	일본	- 평가기관 승인을 받기위한 요구사항을 충족하는지 심사

[표 11] 갱신유지 비교표

세부 요구사항	일본	- 4년에 한번 갱신
	스웨덴	
	캐나다	- 갱신주기를 명시하지 않고, 승인 등급 유지를 명시함
	영국	- UKAS 감시 및 재평가 - 인증기관 감시 및 재평가
	미국	- CCEVS 승인과 NVLAP 인정에 대해 재평가 - NVLAP 절차는 2년에 한번 현장평가를 수행 - CCEVS는 승인을 매년 재확인을 통해 수행

제품의 수준과 인원에 대해서 같은 내용을 제시하고 있다.

우리나라는 스웨덴과 영국의 시험평가를 참조하여 시행, 심사, 완료 단계로 구성하여 도입하는 것이 효과적이다.

3.2.7 승인

인증기관 승인단계에서 각 나라의 세부 요구사항을 살펴보면 〔표 10〕과 같다. 스웨덴의 경우 심사 결과를 평가기관에 승인 합의 보고서로 보고한다. 영국의 경우 승인 부여자가 시험 평가에서 얻어진 평가보고서를 심사하여 승인여부를 결정하며, 미국의 경우 NVLAP가 최종결정을 하게 된다. 대체적으로 승인에 대한 통보는 평가기관이 제출한 평가보고서를 검토하여 인증기관이 최종승인을 부여하는 방식을 채택하고 있다.

〔표 12〕 승인 보류 비교표

공통 요구사항	영국 스웨덴 미국	- 승인 요구사항을 불이행 시 인증 보류
세부 요구사항	영국	- UKAS 인정의 경과되었을 경우 승인을 철회하기 전 통보로 권리를 유보 - CLEF 모회사가 인수됐을 경우 재검토
	미국	- CCEVS와 NVLAP의 모든 요구사항을 준수하지 않을 경우 CCTL 자격을 보류 또는 철회 - CCTL 철회 또는 보류 시 30일 전에 CCTL에게 통보
	스웨덴	- 불이행 조건이 6개월 이내에 정당한 노력으로 해결

〔표 13〕 승인 보류 비교표

공통 요구사항	영국 스웨덴	- 진행 중인 평가 업무에 대해 계약상의 의무를 이행시킬지 결정
세부 요구사항	영국	- 인증기관이 최소 6개월 전에 철회 승인 기간 변경에 대한 무갱신 또는 무의사에 관한 통보
	일본	- 승인의 범위를 넘어선 인증마크를 첨부한 평가보고서를 발행한 경우 - 계약검사 또는 능력 평가의 결과 IT 보안성 평가의 기술적 능력이 없음으로 판명되는 경우
	캐나다	- 평가기관이 인증기관의 요구사항을 충족시키지 못하는 경우 - 인증기관이 명시한 문제점을 기간 내 시정하지 않은 경우
	미국	- 보류의 내용과 동일
	스웨덴	- 보류 조건이 합의된 기간 내에 해결되지 않은 경우 철회 - 승인 조건을 심각하게 위반한 경우 철회나 보류 없이 승인 합의를 종료

3.3. 승인유지 및 승인종료 비교·분석

평가기관이 최종 승인을 획득 하였어도 평가기관으로써의 자격과 능력을 유지하기 위해서는 갱신이 필요하다. 〔표 11〕은 갱신을 유지하기 위한 각국의 요구사항을 비교한 표이다.

우리나라는 각 국에서 제시한 갱신 요구사항을 비교하여 적절한 기간을 결정하여 갱신을 수행하도록 해야 할 것이다. 이를 위하여 평가기관은 각 년도마다 감사를

〔표 14〕 각국의 승인 요구사항 비교·분석

승인 요구사항		미국	영국	일본	스웨덴	캐나다
평가기관 요구사항	기본 요구사항	○	○	○	○	○
	조직 구조	○	○	○	○	×
	문서화 요구사항	○	○	×	○	×
	인증 감독관	×	○	×	○	×
평가기관 승인절차 (초기인증)	인증절차	○	○	○	○	○
	인증신청	○	○	○	○	○
	임시승인 부여	×	○	×	○	×
	사전 회의	○	○	×	○	-
	초기심사	○	○	×	○	○
	시험 평가	×	○	○	○	○
	인증기관 최종심사	○	○	○	○	○
인증유지	갱신 주기	○	○	○	○	×
	인증 유지 절차	○	○	×	○	×
인증종료	보류	○	○	×	○	×
	철회	○	○	○	○	○

수행하여 자격을 갱신하도록 해야 할 것이다. 또한 승인 유지절차에 대해서는 스웨덴과 같이 평가기관 내부 감사를 실시하고 승인 유지절차를 초기 심사와 시험 평가 과정으로 심사하는 것이 적절하다.

승인 종료는 보류와 철회로 나뉜다. 보류는 일정한 승인 요구사항 불이행 시 평가기관의 승인을 잠시 보류하는 것으로써 일정기간동안 문제에 대한 해결이 되지 않을 경우 자동으로 승인 철회로 이어질 수 있다.

철회의 경우 분석결과 스웨덴과 영국이 진행 중인 평가 업무에 대해 계약상의 의무를 이행시킬지 결정해야 한다는 것이 공통적으로 명시되어 있다. 우리나라에서도 승인 조건에 대하여 위반할 시 승인을 철회하는 것이 적합할 것이다.

지금까지 기술한 평가기관 승인 요구사항 비교·분석 결과를 토대로, 각 국에서 명시하고 있는 항목을 요약하면 〔표 14〕와 같다.

평가기관 및 평가자의 자격 기준에 대한 요구사항을 각 국의 문서에서 명시하고 있는 경우 ○로 표기하였으며, 명시하고 있지 않을 경우 ×로 표기하였다.

각국의 승인 요구사항을 비교·분석한 본 논문의 내용은 국내 평가기관 설립 기준 제안에 자료로 활용될 수 있을 것으로 예상된다.

Ⅳ. 국내 평가기관 승인 요구사항 제안

본 장에서는 앞 장에서 분석한 각 국의 승인 요구사항을 토대로 개발한 국내 평가기관 승인 요구사항을 제안한다. 제안된 평가기관 승인 요구사항은 기본 요구사항과 평가기관 승인 절차 그리고 승인 유지로 나누어 기술한다.

4.1. 평가기관 기본 요구사항

우리나라에서 평가기관이 인정기관의 승인을 취득하기 위해서는 국제적 인식을 고려하여 각 국에서 공통으로 언급하고 있는 요구사항을 기본으로 준수하는 것이 적합할 것이다.

공통 요구사항을 기준으로 우리나라의 승인 요구사항을 제안하면 다음과 같다.

(1) 평가기관이 되기 원하는 신청기관은 국내에 위치해야 하며, 법인 기업이어야 한다. 또한 신청기관은 인증기관의 승인을 부여받기 위해 기본 요구사항을 만족하고 공통평가기준과 공통평가방법론을 만족하며, 스킴 원칙을 만족하는 능력이 있음을 입증하고 적합성, 공정성, 객관성, 기밀성, 독립성을 만족해야 한다.

(2) 기본적으로 인증기관의 승인을 부여받기 위해 평가기관은 CCRA 요구사항을 만족해야 하며 인정기관에 의해 공인된 평가기관으로 인정되어야 한다.

(3) 인증 절차나 규칙에 관한 요구사항을 이행해야하며 정보제공을 위한 질문, 인원구성, 심사, 문서, 기록, 열람 등에 관하여 인증기관과 협력하고 인증기관과 연락, 협력하기 위한 사무 공간, 통신시설, 기록 보관실 등을 갖추어야 한다.

(4) 운영 및 행정적 관점에서 모회사와 별개로 자발적이고 자체부서로 운영해야 한다. 또한 평가기관은 인증기관 및 평가 신청인과의 의사소통을 위한 통신 시설을 보유해야 하며 인정기관 요구사항에 만족하는 기록 보관 시설을 갖추어야 한다.

(5) 평가기관의 직원은 IT장비를 사용하여 업무 평가를 지원할 수 있는 능력을 갖춘 자 이어야 하며 그밖에 적합한 자격을 갖고 경험이 많은 직원이어야 한다.

(6) 평가기관은 운영을 위해 총 책임자를 지정해야 하고, 총 책임자는 스킴 절차에 만족하는 인원을 임명하거나 인증기관과 연락하고 협력하는 일을 맡으며 품질, 경영, 보안책임을 총괄한다.

(7) 평가기관은 문서화 요구사항을 이행함으로써 문서의 변경, 수정, 갱신을 수행하고 변경된 부분은 명확한 식별표시를 하고, 주기적으로 문서를 검토, 개정, 관리한다.

(8) 인증감독관으로 임명받은 직원은 인증기관이 진행 중에 있는 모든 스킴 평가에 대해 알고 협의할 수 있어야 하며, 스킴, 인증기관의 이미지 손상이나 공익성에 위배되는 활동 및 참여, 서비스 하는 일을 삼가 해야 한다.

(9) 인증기관은 동일 인증 감독관에게 전권을 승인하고, 평가기관 신청 사항을 처리하며 책임을 지고 스킴 참여 인원으로 평가기간 동안 기술 지원과 지도 활동을 수행한다.

(10) 인증 감독관은 평가기관 평가 시 사전 회의를 위해 신청기관을 방문하여 평가에 대한 자문을 제공한다. 또한 인증 감독관은 회의를 주관하며 회의 내용을 문서화하여 보관해야하며, 보통 인증기관에 의해 승인 부여자로 임명되며 평가를 감시하고 승인 보고서를 작성하여 제출한다.

4.2. 평가기관 승인절차

우리나라의 기존 평가체계를 고려하면, 인증기관은 미국 보다는 영국과 스웨덴 그리고 일본의 평가기관 승인절차에 보다 더 적합하므로, 우리나라 평가기관 승인은 인증기관에 의해 수행하는 방법을 제안한다.

제안된 우리나라 평가기관 승인절차를 살펴보면 승인은 평가기관이 인정기관에 의해 심사를 받아 인정서를 받은 상태에서 추가로 인증기관에 의해 보안성 평가에 있어 평가기관이 자격을 갖추었는지 심사하여 승인을 부여한다.

본 논문에서 제안하는 국내 평가기관의 승인절차는 〔그림 7〕과 같다.

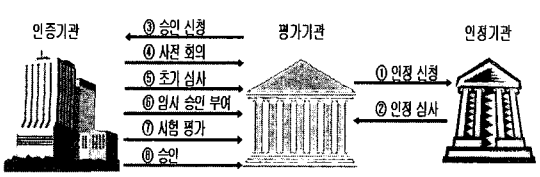
(1) **인정신청** : 신청기관이 평가기관으로서 승인을 받기 위해서는 먼저 인정기관에 인정신청을 한다.

(2) **인정심사** : 인정 신청되면 인정기관은 일정한 심사를 통해 신청기관에 인정서를 부여한다.

(3) **승인신청** : 신청기관은 인정기관에서 인정을 부여 받고 인정서와 품질 메뉴얼, 보안 메뉴얼을 보유해야 하며, 승인 신청 접수 시 신청서와 함께 제출해야 한다. 신청서에는 평가기관이 되기 원하는 신청기관의 요구사항 및 평가기준 그리고 스킴 규칙에 따라 평가기관을 설치하고 관리한다는 제안을 상세히 작성해야 한다.

(4) **사전방문** : 신청기관이 제출한 신청서가 적절할 경우 인증 감독관은 신청기관을 사전 방문하여 인증기관 평가를 준비 중인 신청기관에 자문을 제공한다.

(5) **사전회의** : 사전 회의는 인증기관이 신청기관에게 평가기관을 구성하는데 있어서 조언을 주기 위한 것으로 일본과 캐나다를 제외한 스웨덴, 영국, 미국에서는 사전 회의를 실시하고 있다. 우리나라의 경우에도 신청서를 접수하여 초기 심사를 수행하기 전, 사전 회의를 실시하는 것이 적합할 것이다. 회의는 인증감독관의 주관으로 소개, 설치단계, 평가기관 품질 메뉴얼 및 보안 메뉴얼의 중대성 설명, 승인 부여 과정에 대한 계획 검토, 스킴의 요구사항 및 서비스에 대한 정보가 주요 안건으로 진행된다. 회의는 수시로 개최되며 이 회의 내용은 문서화 시킨다.



〔그림 7〕 국내 평가기관 승인 절차

(6) **초기심사** : 초기 심사에서는 인증기관이 평가기관에 현장 방문을 실시하여 평가기관 직원들과 면담을 통하여 평가기관의 운영절차, 품질 시스템 그리고 보안 안전 감시, 절차서 이행 등에 대해 적절히 이행하는지 검증한다. 초기 심사 단계에서 인증 감독관은 평가자 신청자에 대한 예비 평가자 훈련 프로그램을 수행하고 성공적으로 이 프로그램을 이수한 신청자에게 예비 평가자 상태를 부여한다.

(7) **임시승인부여** : 인증기관은 신청기관이 초기심사를 적절히 수행하였고, 시험 평가를 수행 할 자격이 있을 경우 신청기관에게 임시 승인을 부여한다. 임시 승인은 단지 시험 평가를 수행할 자격이 있다는 것을 판별하기 위해 부여되는 것이다.

(8) **시험평가** : 임시 승인을 부여한 뒤 평가기관은 보안성 평가를 적절히 수행할 능력이 있다는 것을 인증기관에게 입증하기 위하여 시험평가를 시행한다. 시험평가의 세부항목으로는 시행, 심사, 완료의 단계가 있다.

(9) **승인** : 인증기관은 시험평가 완료 후 평가기관이 제출한 평가 보고서를 검토하여 최종 승인을 부여하며, 승인을 유지하기 위해서는 평가기관이 승인을 받은 날로부터 4년 이내에 인증기관에게 갱신을 받아야 한다. 갱신 신청은 갱신 만료일 6개월 이전에 신청해야하며 이 기간에 신청하지 않을 경우 평가기관의 자격은 철회된다.

4.3. 평가기관 승인유지

4.3.1 갱신

매년 평가기관 변동 사항과 평가기관 내부감사 및 기록을 이용해 감사를 수행하지만 인증기관, 인정기관 갱신연도와 중복될 경우 감사를 수행하지 않는다. 승인 유지 절차는 3년에 한번 초기 심사를 수행하여 승인 요구사항을 검토하며, 인정기관 갱신평가에 대한 결과도 인증기관에서 검토를 수행한다.

4.3.2 보류

평가기관의 승인이 보류 상태로 되는 경우는 두 가지가 있다. 첫 번째로 평가기관의 모회사가 다른 회사로

인수됐을 경우에 평가기관의 승인은 자동으로 보류 상태가 되고 인증기관은 평가기관이 평가를 적절히 수행할 수 있는지 다시 심사한다.

두 번째로 평가기관이 스킴 요구사항을 이행하지 않은 경우 평가기관의 상태는 보류가 된다. 불이행 조건이 있을 경우 6개월의 보류 기간을 주어야 한다.

평가기관 승인이 보류되면 인증기관은 스킴에 준해 진행 중인 평가업무를 평가기관이 고객과 계약상의 의무를 이행시키기 위해 평가를 진행 또는 중단할 것인지 결정한다.

4.3.3 철회

평가기관이 부도 또는 부도 위기에 있을 경우, 불이행 조건의 시정조치가 기간 내에 완료하지 못할 경우, 철회 신청이 있을 경우, 스킴 규칙을 위반했을 경우, 인증범위 밖의 평가를 수행하여 제품을 인증할 경우 철회의 대상이 되며 평가기관 승인이 철회되면 평가기관은 즉시 모든 스킴 평가 활동을 중지하고, 해당 평가기관을 평가기관 목록에서 삭제해야 한다.

V. 결 론

본 연구에서는 CCRA 인증서 발행 국가인 미국, 영국, 스웨덴, 일본, 캐나다 5개국을 중심으로 IT 보안성 평가기관의 자격 기준을 분석하였다. 이를 토대로 국내 평가 기관 설립을 위한 자격 기준을 제시하였고, 우리나라에 맞는 평가기관 승인 요구사항을 도출 하였다.

본 논문의 결과는 국제적으로 인정받을 수 있는 평가기관 설립 기준과 해외 평가기관 기준 동향에 관한 자료 확보에 도움이 될 것으로 기대한다. 또한 국내에 인증된 정보보호 제품 평가기관의 추가 설립을 위한 평가기준으로 활용될 수 있을 것이다.

참고문헌

[1] C. D. Faison외, "*National Voluntary Laboratory Accreditation Program*", NIST HANDBOOK 150, February 2006

[2] Jeffrey Horlick, "*National Voluntary Laboratory Accreditation Program*", NIST HANDBOOK 150-20, October 2005

[3] CSEC, "*Swedish Certification Body for IT Security : 004 Licensing of Evaluation Facilities*", 2005. 12

[4] CESG, "*UK IT Security Evalution and Certification Scheme Publication UKSP 02 Part 1, CLEF REQUIREMENTS : Start up and Operation*", 2003. 4

[5] CESG, "*UK IT Security Evalution and Certification Scheme Publication UKSP 02 Part 2, CLEF REQUIREMENTS : Conduct of Evalution*", 2005. 12

[6] Standards Council of Canada, "*PALCAN Policy on the Use of Information Technology in Accredited Laboratories*", 2005.9

[7] Standards Council of Canada, "*PALCAN Policy on the Use of Information Technology Security Evaluation and Testing Facilities CAN-P-1591B*", 2003.2

[8] Communications Security Estavlishment, *Evaluation Facility Approval*, 2005.8

[9] DCSSI, "PRUCEDURE", *Licensing of Evaluation Facilities,Direction Centrale de la Securite des Systemes d'information*, 2003.12

[10] Anders assta Staaf, Dag Stroman, CSEC, "*Licensing of Evaluation Facilities 004*", IT 보안을 위한 스웨덴 인증기관 FMV/CSEC, 2005.12

[11] 上木 鷲見 외 2명, *認証業務の品質を維持向上させるためのマニュアル*, 獨立行政法人情報處理推進機構, 平成１７年７月

[12] 上木 鷲見 외 2명, *評価機關承認手續規程*, 獨立行政法人情報處理推進機構, 平成１７年７月

[13] 上木 鷲見 외 2명, *評価機關承認業務取扱規程*, 獨立行政法人情報處理推進機構, 平成１７年７月

[14] 남지희, "*KOLAS 품질보증시스템 구축을 위한 ISO/IEC 17025의 요건분석*", 2000.12

[15] 한국정보보호진흥원, "*정보보호 시스템 평가·인증 가이드*", 2004.12

[16] 성윤기, "*미국과 영국의 CC평가기관 승인 절차 차이점 분석*", 한국정보보호진흥원, 2005.12

〈著者紹介〉

유 다 혜 (Da-hye Yoo) 학생회원
2006년 2월: 호서대학교 컴퓨터공학과 졸업
2006년 3월~현재: 호서대학교 컴퓨터공학과 정보보호전공 석사과정
<관심분야> 정보보호, 시스템보안, 정보보호 표준

윤 신 숙 (Sin-sook Yoon) 학생회원
1994년 2월: 단국대학교 화학과 졸업
2006년 3월~현재: 호서대학교 컴퓨터공학과 정보보호전공 석사과정
<관심분야> 정보보호, 유비쿼터스 보안, 정보보호 표준

오 수 현 (Soo-hyun Oh) 종신회원
1998년 2월: 성균관대학교 정보공학과 졸업
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업(공학박사)
2004년 3월~현재: 호서대학교 정보보호학과 교수
<관심분야> 정보보호, 암호 알고리즘/프로토콜, 유비쿼터스 보안

김 환 구 (HwanKoo Kim) 종신회원
1987년 2월: 경북대학교 수학과 졸업
1991년 2월: 경북대학교 대학원 수학과 이학석사
1998년 5월: U. of Tennessee-Knoxville, 수학과, Ph. D.
2002년 3월~현재: 호서대학교 정보보호학과 교수
<관심분야> 평가 및 인증, 암호학