제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

정보보호시스템 평가 · 인증스킴에 관한 연구

오동규*, 이승우*, 최희봉**, 원동호*
*성균관대학교 컴퓨터공학과
**국가보안기술연구소
e-mail : dkoh@dosan.skku.ac.kr

A Study on Evaluation and Validation Scheme of IT Security System

Dongkyu Oh*, Seungwoo Lee*, Heebong choi**, Dongho Won*
*Dept of Computer Engineering, Sungkyunkwan University
**National Security Research Institute

요 약

정보보호를 위한 보안 제품의 필요성과 그에 대한 평가가 요구되면서, 미국과 영국 등의 선진국을 중심으로 정보보호시스템의 보안성에 대한 평가가 시작되었다. 국내에서는 1990 년대 중반에 보안 제품에 대한 평가가 시작되었고, 공통평가기준을 도입하여 국내 평가제도와 체계를 정비하고 있으며, 관련된 연구가 계속 진행되고 있다. 그러나, 평가 수행에 필요한 절차, 방법 및 문서가 정의된 평가 · 인증스킴에 대한 연구가 미흡한 실정이다. 따라서, 본 논문에서는 외국의 평가 · 인증스킴을 살펴보고, 현재 국내에 제정된 평가절차와 비교하여, 국내 평가 · 인증스킴의 제정에 바람직한 대안을 제시한다.

1. 서론

1980 년대부터 미국, 영국, 프랑스, 독일 등의 선진국을 중심으로 정보보호시스템과 제품 등을 평가하기 위한 평가 · 인증제도를 운영하여 왔다.

초기에는 국가기관의 공공용 제품을 중심으로 평가가 진행되어 왔다. 그러나, 정보통신의 급속한 발전으로 개인정보와 기업정보의 유출 및 파괴 등 정보화 역기능이 발생하면서, 민간용 제품과 시스템에 대한 평가의 요구와 수요가 증가하게 되었고, 평가의 범위가 공공용에서 민간용으로 확대되었다.

민간 보안제품이 수출되면서, 각 국가들간에 제품에 대한 상호인정을 위해 평가기준의 필요성이 대두되었고, 이에 공통평가기준인 CC(Common Criteria)를 개발하였다. CC 는 하나의 기준으로 다양한 정보보호 제품과 시스템을 평가할 수 있으며, 현재 국제 표준(ISO/IEC 15408)로 지정되어 있다. 정보보호시스템 및 제품을 평가하고 있는 국가들은 CC 를 도입하여 평가 · 인증제도를 재정비하여 운영하고 있다.

국내에서는 1998 년 정보통신망 침입차단시스템 평가기준이 고시되면서 정보보호제품에 대한 평가가 시작되었고, 2000 년 CC 를 수용하여 정보보호시스템 평가 · 인증지침을 고시하면서, 국내 평가 · 인증제도를 재정비했다.

그러나, CC 를 이용한 평가활동은 시행 초기 단계이므로 크게 활성화 되지 않았고, 추후 국제적인 상호인정협정에 가입하기 위해서 국내 정보보호 시스템 평가 · 인증스킴이 마련되어야 한다.

평가 · 인증스킴이란 자국의 평가 · 인증과정을 수행하기 위한 절차와 문서 등을 정의하고 있는 것으로, 현재 국내에도 평가 · 인증 절차가 정의되어 있으나, 정형화된 평가방법론과 평가절차상의 상세한 설명 등의 부족으로 평가 · 인증스킴으로 제정되기에는 부족한 상황이다.

본 논문에서는 평가 · 인증스킴 내에 평가절차를 분석하여 현재 국내 평가 절차와 비교 분석을 통해, 평가 · 인증스킴을 제정하기 위한 바람직한 대안을 제시한다.

본 논문의 구성은 다음과 같다. 2 장에서 대표적인 평가 · 인증스킴인 미국의 CCEVS 와 영국의 UKSP 의 평가절차와 국내 평가절차에 대해 알아보고, 3 장에서는 국내 · 외 평가절차를 비교하여, 4 장에서 대안을 제시하고, 마지막 5 장에서 결론 및 향후 연구과제를 제시한다.

2. 정보보호시스템 평가인증 절차

본 장에서는 대표적인 평가 · 인증 스킴의 예로

미국의 CCEVS(Common Criteria Evaluation and Validation Scheme)과 영국의 UKSP(United Kingdom Scheme Publication)의 평가절차와 국내의 정보보호 시스템 평가 · 인증 지침의 평가절차에 대해 설명한다.

2.1 CCEVS

미국의 평가 · 인증스킴인 CCEVS 는 1999 년 NSA 와 NIST 가 공동으로 개발했고, CC 에 기반한 평가 · 인증체계를 정립하기 위한 프로그램이다. CCVES 는 평가활동에 대해 6 개의 문서로 구성되어 있다.

다음 [표 1]는 CCEVS 를 구성하는 문서를 나타낸 것이다.

[표 1] CCEVS 문서

구분	내 용
1	Organization, Management and Concept of Operations
2	Validation Body Standard Operating Procedure
3	Guidance to Validation of IT Security Evaluation
4	Guidance to CCEVS Approved Common Criteria Testing Laboratories
5	Guidance to Sponsors of IT Security Evaluation
6	Certificate Maintenance Program

(1) CCEVS 의 평가·인증 절차 참여자

평가인증절차의 참여자는 평가스폰서, 평가기관, 인증기관으로 구성된다.

평가스폰서는 평가인증을 얻기 위해서 평가신청인(고객)의 역할을 대신하는 대리인으로 예를 들면, 제품의 개발자 또는 보호 프로파일(Protection Profile: PP)의 작성자 등이다.

평가기관은 평가를 수행하는 기관으로 국가용을 평가하는 평가기관인 NSA(National Security Agency)와 다수의 민간평가기관이 있다. 민간평가기관을 CCTL(Common Criteria Testing Laboratory)이라고 하는데, CCTL 은 NVLAP(National Voluntary Laboratory Accreditation Program)로부터 인정을 받아, NIAP(National Information Assurance Partnership)내에 인정기관의 승인된 시험연구소 목록에 등재되어 있는 시험소(Testing Laboratory)를 말한다.

인증기관은 평가기관의 평가업무 감독, 인증서 발급, 인증 받은 제품에 대한 등록 및 관리, 인증제품에 대한 사후관리 등을 수행하는 기관이다. 인증기관은 각각의 평가마다 인증담당자를 선임하여 기술적, 절차적인 문제에 대해 감독 및 조언을 한다. 그리고, 인증기관은 평가기관을 인정하는 역할도 담당하여 NIST Handbook 150-20 을 만족하고 평가 · 인증스킴에서 CCTL 요구사항을 만족 하는 평가기관에 대해 승인을 한다.

(2) CCEVS 의 평가·인증 절차

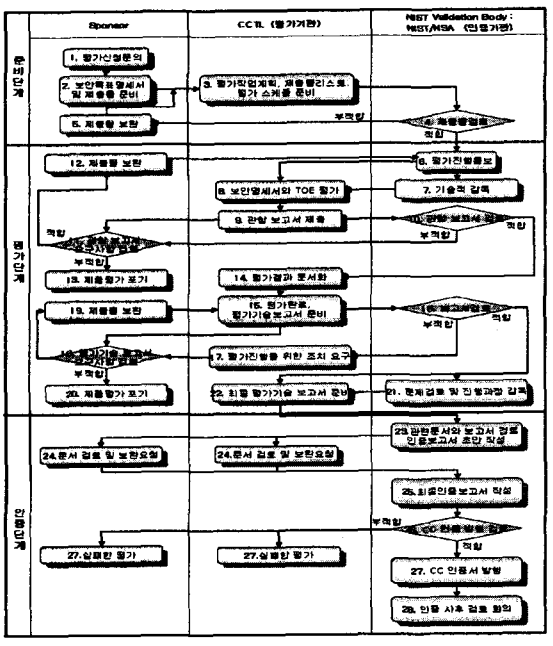
평가인증절차는 크게 사전평가단계, 평가단계, 인증단계의 3 단계로 구성한다.

사전평가단계에서는 평가시행 이전의 평가를 위한 준비단계이다. 평가스폰서는 제품의 보안평가를 위해 보안목표명세서(Security Target: ST)와 평가에 필요한 제출물을 준비하여, CCTL 을 선택 후 접촉한다. CCTL 은 ST 와 제출물을 검토 후, 성공적인 평가의 가능성이 있다고 판단되면, 평가작업계획서(Evaluation Work Plan), 평가스케줄(Evaluation Schedule), 제출물 목록(Deliverable List)을 준비한다. 인증기관은 CCTL 에서 제출 받은 평가대상(Target Of Evaluation: TOE), 평가제품의 설명서, 평가계획서, 평가 스케줄의 자료를 초기 검토하여 한 명 이상의 실무 인증자와 책임 인증자를 선임한다. 책임 인증자는 평가계획서, 인증계획서(Validation Plan)를 작성한다. 책임 인증자는 평가스폰서와 평가기관과의 회의를 통해 토의하여, 모든 참석자들이 동의하면, 평가동의서에 모두 서명하고 평가활동을 시작한다.

평가단계에서는 신청이 제출한 제품이 평가기준에 부합하는지 여부를 확인하는 단계이다. CCTL 은 CC 에 명시된 요구사항들을 만족하는지 여부를 ST 와 TOE 를 통해 평가한다. 인증기관은 평가기관의 평가활동을 감독하고 인증계획에 따라 인증 작업을 수행한다. 평가작업이 진행되는 동안 관찰보고서(Observation Report)를 작성하여 인증기관에 제출하고 인증기관은 관찰보고서를 조정하고 평가기관과 계속적인 인터페이스를 유지한다. 평가가 종료되면 평가기술 보고서(Evaluation Technical Report: ETR)와 인증된 제품 리스트(Validated Product List: VPL)의 초안을 작성하여 인증기관에 제출한다.

인증단계에서는 평가기관에서 제출 받은 보고서를 검토 후, 인증보고서(Validation Report)를 작성한다. 인증보고서와 VPL 요약문을 평가기관과 평가신청인에 동시에 전달한다. 인증자는 문서 배포의 승인 동의를 위해 기술감독 관리자에게는 최종 권고문을 제출하고, 인증기관 국장에게 프리젠테이션을 준비하여 제출 발표한다. 인증기관 국장의 검토를 통해서 인증이 실패인 경우 이유를 평가기관과 평가스폰서 에게 통지하고, 인증이 성공한 경우, CC 인증서 및 VPL 발간하고 CCRA 참가국에 통지한다.

다음 [그림 1]은 평가인증절차를 나타낸 것이다.



[그림 1] CCEVS 평가인증절차

2.2 UKSP

영국의 평가·인증스킴인 UKSP 는 1991 년 영국 정부 및 민간부문에 활용되는 정보보호시스템을 평가·인정하기 위하여 영국정부의 상공부와 CESG (Communication Electronics Security Group)라는 보안 평가기관에서 공동으로 개발하였다.

UKSP 는 전체 10 개의 카테고리로 구분된 문서로 구성되어 있고, 개발자와 컴퓨터 보안 평가 매뉴얼 및 인증서 유지 스킴에 대해서는 3 개의 문서로 구성되어 모두 17 종류의 문서가 개발되어 있다. 모든 문서가 공개되어 있지 않다. 다음 [표 2]는 UKSP 를 구성하는 문서 일부를 나타낸 표이다.

[표 2] UKSP 문서

구분	내 용
1	Description of the Scheme
2	CLEF Requirement Part 1 - Start Up and Operation Part 2 - Conduct of an Evaluation
3	Sponsor's Guide (Role of Sponsor in IT Security Evaluation and Certification)
4	Developer's Guide Part 1. Roles of Developers in ITSEC Part 2. Reference for Developers Part 3. Evaluation Techniques and Tools
5	Manual of Computer Security Evaluation
12	UK IT Security Evaluation Scheme
16	UK Certification Maintenance Scheme Part 1. Description of the CMS Part 2. Impact Analysis and Evaluation Methodology Part 3. DAS Reference Manual

(1) UKSP 의 평가·인증 절차 참여자

평가·인증과정에 대한 구성원은 평가신청인, 평가기관, 인증기관, 인정기관으로 구성되어 있다.

평가신청인은 제품에 대한 평가 요청과 결과를 받는 대상으로 개발자가 대신하여 TOE 를 작성하고, 스폰서가 대신하여 평가신청을 지원한다.

평가기관은 영국 정부기관인 CESG 와 CLEF(Commercial Licensed Evaluation Facility)라고 불리는 6 개의 민간 평가기관으로 구성되어 있다. 민간평가기관은 CLEF 관리위원회가 정한 스킴의 규정을 준수하고, 평가 활동에 대한 인증기관의 사전승인이 필요하다.

인증기관은 인정기관의 승인 하에 평가기관에 대한 업무감독 및 평가기관이 제출한 평가기술보고서를 검토하여 평가등급을 인증하는 역할을 담당한다.

인정기관은 인정서 발급과 평가자의 자격 및 능력을 평가하여 승인하는 역할을 담당하는 기관으로 유일한 인정기관인 UKAS(United Kingdom Accreditation Service)가 있다.

(2) UKSP 의 평가·인증 절차

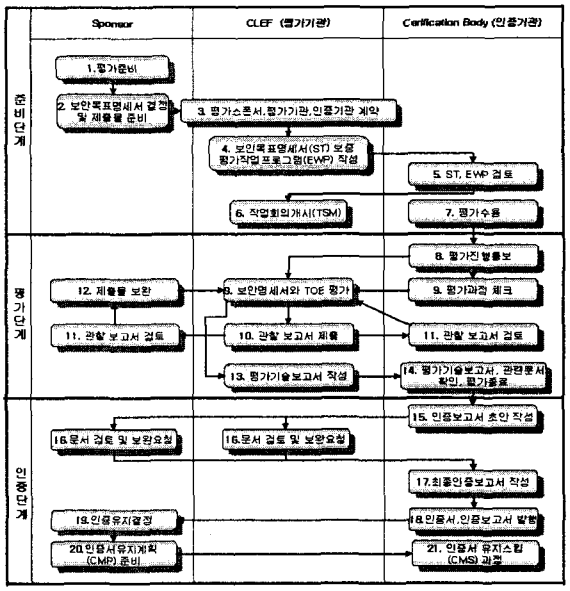
평가·인증절차는 크게 사전평가단계, 평가단계, 인증단계의 3 단계로 구성되어 있다.

사전평가단계는 평가와 인증이 이루어지기 전에 필요사항 및 제출물 등의 평가·인증을 위한 준비 단계이다. 평가신청인은 TOE 평가와 인증을 위한 제출물을 준비하고 보안목표명세서를 결정한다. 평가기관을 선택하고 평가 시작을 위해 인증기관, 평가기관과 계약을 맺는다. 평가기관은 평가신청인(스폰서)에게서 받은 제출물을 검토하여 보안 목표 명세서를 보증하고 평가 작업 프로그램(Evaluation Work Program)을 작성하여 인증기관에 제출하여 동의를 얻는다. 평가기관은 평가신청인, 인증기관과 함께 TOE 평가에 대해 논의하는 평가작업 개시회의를 개최한다. TOE 가 인증기관이 인정할 수 있는 범위 내에 것이고, 평가신청인이 평가·인정활동에 대한 비용을 지불하고 인정기관이 모든 활동을 지원한다는 것에 동의하여 계약한 경우 정식으로 평가를 수용하게 된다.

평가단계는 평가기관에 의해 실제적으로 평가가 수행되는 단계로 제출물이 평가기준에 충족되는지 결정하는 단계이다. 평가기관은 평가신청인이 제출한 제출물을 바탕으로 보안 목표 명세서에 대한 TOE 평가를 실시한다. 인증기관은 모든 평가를 감독하고, 사전에 평가기관과 함께 동의한 기준과 절차를 따라 평가가 이루어지는지 확인한다. 평가기관은 평가종료 후 인증기관과 평가신청인에게 평가기술보고서를 작성하여 제출하여 평가를 종료한다.

인증단계에서 인증기관은 제출된 평가기술보고서를 검토하여 인증보고서를 작성하여 제품에 대한 인증서 발급과 인증보고서를 간행한다.

다음 [그림 2]는 평가인증 절차를 나타낸 것이다.



[그림 2] UKSP 평가인증절차

2.3 국내 평가 절차

2000 년 2 월 CC 를 국내 평가에 수용하기 위해 정보보호시스템 평가·인증 지침을 고시하여, 공공기관용과 민간용의 구분이 없는 일원화된 정보보호시스템 평가·인증체계가 구축되었다. 2002 년 8 월 정보보호시스템 평가·인증지침을 개정하였다.

(1) 정보보호시스템 평가 · 인증지침

정보보호시스템 평가 · 인증지침은 크게 총칙, 평가 · 인증체계, 평가절차, 인증절차, 평가 · 인증 사후관리, 보호프로파일 평가 · 인증절차로 구성되었다.

(2) 정보보호시스템 평가 · 인증지침 참여기관

평가 · 인증을 위한 구성원은 평가신청인, 평가기관, 인증기관 3 가지로 구분한다. 평가신청인은 평가 · 인증에 필요한 제출물 작성, 평가수행에 필요한 추가자료를 제출하고, 평가수수료를 납부한다.

평가기관은 한국정보보호진흥원(KISA)으로 평가 계약체결 및 평가수행 등의 업무를 담당한다.

인증기관은 국가정보원으로 평가기관의 평가업무 감독과 인증서 발급 및 인증제품에 대한 사후관리 등을 담당한다.

(3) 정보보호시스템 평가 · 인증절차

평가절차는 평가신청 준비, 평가신청 및 평가계약 체결과 평가로 구성되어 있다. 평가신청 준비과정에서 평가기관의 자문을 통해 보안목표명세서와 제출물을 준비한다. 평가신청 및 평가계약 체결과정은 평가신청인이 평가신청서와 제출물을 구비하여 평가 기관의 장에게 신청하면, 제출물을 검토하여 평가 계약서를 작성하고, 평가신청인은 계약서에 서명하여 평가 수수료를 납부한다. 평가기관은 평가팀을 구성하여 평가 수행 계획서를 인증기관의 장에게 제출하고 평가를 수행한다. 평가가 종료되면, 평가보고서 및 최종제출물을 인증기관의 장에게 제출한다.

인증절차에서 인증기관의 장은 최종제출물과 평가보고서를 검토한 후, 평가과정의 공정성과 객관성 여부를 확인하여 적합하다고 판단한다. 인증기관의 장은 공정성과 객관성에 대한 심의 · 의결 및 신청인과 평가기관의 분쟁 조정을 위해 인증위원회를 구성, 운영할 수 있다. 위원회의 심의 결과에 따라 부적합 등급을 부여하거나 평가등급을 부여하고, 심의결과를 평가기관의 장과 신청인에게 통보한다. 그리고, 결과에 따라 인증서를 발급한다.

3. 국내 · 외 평가 절차 비교

정보보호시스템을 평가하기 위한 국내 · 외 평가 절차에 대해 살펴보았다. 이 내용을 토대로 공통점과 차이점을 비교해 보면, 공통적으로 평가기관, 평가 신청인, 인증기관의 3 가지 기관으로 구성되어 있고, 각 기관들도 유사한 역할을 담당하고 있다. 그리고, 평가절차 면에서도 평가 이전에 준비하는 사전평가 단계와 실제적인 평가가 이루어지는 평가단계 평가결과에 대해 인증을 해주는 인증단계로 구성되어 있다.

차이점은 정보보호시스템을 평가하기 위한 국내 평가 · 인증절차에는 미국의 NVLAP 나 영국의 UKAS 와 같은 인정기관이나 인정프로그램을 갖고 있지 않다. 그리고, 국내 평가기관은 국가용과 민간용 제품에 대한 평가가 단일 기구에 의해 수행되고 있으나, 미국과 영국의 경우, NSA(미국)와 CESG(영국)에서 국가용 제품을 평가하고, 인정 받은 민간평가기관에서 민간용 제품에 대한 평가를 담당하고 있다. CCEVS 나 UKSP 의 평가 · 인증절차에서는 평가 · 인증과정에서 각 기관의 활동과 역할에 대해 구체적으로 명시하여 제시하고 있으나, 정보보호시스템 평가 · 인증 체계에서는 문서상으로 개괄적인 역할을 제시하기는 했으나, 어떤 단계에 어떤 일을 수행해야 하는지는 구체적으로 명시되어 있지는 않다.

4. 대안

국내 평가 · 인증스킴의 제정에 바람직한 대안을 제시하면, 첫째, 평가 · 인증절차에 인정기관이나 인정프로그램을 제정해야 한다. 평가제품이 다양해지고 수요가 늘게 되면 제품을 평가하기 위한 평가기관이 증가하게 되므로, 다수의 민간 평가기관을 관리, 감독하고 인정하기 위한 인정기관 및 인정프로그램이 필요하다.

둘째, 평가 · 인증절차에서 인증기관의 구체적인 활동이 고시되어야 한다. 인증기관은 평가기관과 계속적인 인터페이스를 통해 기술적, 절차적인 문제에 감독과 조언의 역할을 수행해야 한다. 그러나, 현재 국내 인증기관이 평가과정에서 어느 단계에 어떤 활동을 수행해야 하는지 구체적으로 고시되어 있지 않다. 평가의 신뢰성과 질적 향상을 위해 인증기관의 활동을 구체적으로 명시할 필요가 있다.

셋째, 높은 보안성을 요구하는 국가용 제품을 평가하기 위한 평가기관이 마련되어야 한다. 국내 평가기관은 한국정보보호진흥원으로 단일 평가기관의 체계를 갖고 있다. 미국, 영국, 독일 등 국외의 사례의 경우, 보안성이 낮고 수요와 수량이 많은 민간용 제품에 대해서는 다수의 민간평가기관을 두고 평가를 수행하도록 하고, 높은 보안성이 요구되는 국가용 제품에 대한 평가는 국가기관을 정하여 평가를 수행하고 있다. 국내에서도 민간용과 국가용을 구분하여 평가진행의 효율성과 신뢰성을 높이기 위해 민간용과 국가용 평가기관을 이원화할 필요가 있다.

5. 결론 및 향후 연구

국제적으로 CC 를 도입하는 국가들이 증가하고 있고, 국내에서도 CC 를 도입하여 기준 및 체계를 제정하였다. CC 의 도입은 국가간의 상호인정을 목적으로 한 것이기 때문에 상호인정에 맞는 평가체계, 제도 등이 있어야 하고, CC 를 갖고 와서 쓰기만 하는 것이 아니라, 우리나라 실정에 맞는 평가체계로 정비해야 한다. 즉, 상호인정협정 가입과 국내환경에 적합한 평가 · 인증스킴의 제정이 필요하다.

향후, 정보보호시스템의 세계시장 확보와 국제적인 기술을 선점하기 위해 CC 에 따른 평가절차 및 평가체계의 개선 및 수립을 위한 연구와 국제 상호인정협정 가입을 위한 많은 연구가 필요하다.

참고문헌

[1] Common Criteria Evaluation and Validation Scheme for Information Technology Security. Organization, Management and Concept of Operations. Scheme Publication #1

[2] Common Criteria Evaluation and Validation Scheme for Information Technology Security. Guidance to Validators of IT Security Evaluations. Scheme Publication #3

[3] UK Scheme Publication No 1. Description Of the Scheme

[4] UK Scheme Publication No 12. Relationship between accreditation document set and security targets for evaluation

[5] 정보통신부고시 제 2002-41 호. 정보보호시스템 평가 · 인증지침개정. 정보통신부