

CC와 CEM의 평가요구사항 분석

강 연 희*, 방 영 환*, 최 성 자*, 이 강 수*

요 약

정보보호 수준을 향상시키기 위해 정보보호시스템 평가·인증에 대한 필요성이 높아지고 있으며 선진국에서는 정보화 역기능 위험 방지를 위해 제도적 일환으로 자국의 환경에 적합한 평가·인증제도를 마련하여 정보보호시스템을 평가해 오고 있다. 그러나 상이한 평가기준의 적용으로 인한 시간 및 비용 소모의 문제점이 발생되었으며 이를 해결하기 위한 노력으로 현재 정보보호 시스템 평가를 위한 상호인증을 위해 공통평가기준(CC : Common Criteria)과 공통평가방법론(CEM : Common Evaluation Methodology)을 사용하고 있다. 선진화된 평가제도의 조기 정착과 효율적인 평가 준비 및 수행방법을 위한 정보보호시스템 평가 참여자들의 평가기준 및 방법론에 대한 유연하고 능동적인 해석이 필요하다.

Analysis of Evaluation Requirement for CC and CEM

Yeon-Hee Kang*, Young-Hwan Bang*, Sung-Ja Choi*, Gang-Soo Lee*

ABSTRACT

For improve level of information security, the necessity of evaluation and certification of Information Security System(ISS) is increasing. Evaluation and Certification Institution have evaluated ISS for risk prevention of information dysfunction in an advanced countries. But, the problem of the time and cost occurred when it is caused by with application of unlike evaluation criteria each other. The result of effort to solution, Common Criteria(CC) and Common Evaluation Methodology(CEM) is using for evaluation of ISS and mutual recognition. Evaluation participant is needed flexible and active interpretation of CC and CEM for an efficient evaluation preparation and performance.

Key words : CC, CEM, Evaluation Requirement

1. 서론

최근 국가주요기관에 대한 국제적인 해킹 사례가 발생하는 등 정보통신기술의 발달로 인해 정보보호시스템의 안전성 확보의 필요성이 증대되고 있다. 이러한 정보보호시스템의 안전성과 신뢰성 검증을 위해 선진 각국에서는 평가와 인증을 위한 기준(예 : TCSEC., ITSEC 등)들을 개발하고, 공정하고 객관적인 평가를 시행할 수 있는 평가체계를 구축하여 왔다[1,2]. 그러나 서로 다른 평가기준을 적용하여 평가를 수행함으로써 이중의 비용 및 시간 소모가 발생하며 이러한 문제점을 해결하기 위해 평가결과의 상호인증을 고려하게 되었다. 이러한 평가기준 조화를 위한 노력 하에 1993년도

CC v0.6 문서개발을 시작으로 1999년 6월 ISO/IEC에서 CC Version 2.1(15408)을 국제표준으로 채택하였다[3]. 현재 공식적으로 발표된 문서로서 CC v2.2가 있으며 드래프트 문서인 CC v2.4를 개발 중에 있다. 또한 CC를 기반으로 평가수행 골격을 제시함으로써 등급유지 및 평가결과의 상호인증을 목적으로 하는 CEM 역시 1997년도를 시작으로 CC와 발맞추어 개정작업이 계속되어오고 있다. 이러한 CC와 CEM을 평가에 적용하기 위한 분석과 변화를 정확히 파악하고 대처할 필요성이 존재한다.

비용 효과적인 평가를 수행하기 위해서는 평가치침의 변화에 능동적으로 대처하기 위한 요구사항의 파악이 우선적으로 요구되므로 본 논문에서는 평가를 수행하기에 앞서 평가요구사항을 분석 및 검토하고자 한다.

※ 제일저자(First Author) : 강연희, 주소 : 대전광역시 대덕구 오정동 133번지 한남대학교 컴퓨터공학과,
접수일 : 2004년 4월 26일, 완료일 : 2004년 6월 19일

본 논문의 2장에서는 CC와 CEM의 개념 및 현재동향에 대하여 조사하였으며 3장과 4장에서는 각각 CC와 CEM의 평가적용을 위한 요구사항 제시, 변화 양상에 대한 특징과 향후 평가적용 방향에 대하여 제시하였다. 마지막으로 5장에서 결론을 맺는다.

2. 개념 및 현재 동향

2.1 공통평가기준 (CC)

CC는 미국의 TCSEC, 유럽의 ITSEC, 캐나다의 CTCPEC기준을 통합한 표준으로써 평가기준의 상호인증을 위한 골격체제를 위해 개발되었으며, 정보보호시스템을 위한 평가기준의 국제표준일 뿐 아니라 우리나라의 정보통신부 표준이다. CC기반 상호인정 협정인 CCRA에는 현재 호주, 뉴질랜드, 오스트리아 등 19개국이 가입하였으며 우리나라도 가입 진행중이다. CC는 모든 정보보호제품 및 시스템에서 필요로 하는 보안기능요구사항의 전체집합을 클래스-패밀리-킴포넌트를 통해 계층적으로 분류하고 있다. 또한, 보안기능 구현의 정확성에 대한 보증요구사항의 전체집합을 계층적으로 분류하였고 7단계의 보증수준별로 요구하는 보증요구사항(킴포넌트)을 정의하고 있다. 보증요구사항에 대해서 EAL1~EAL7과 같이 7단계의 보증수준으로 정의하고 있으며 해당등급에 추가적인 요구사항이 포함될 경우 Augmentation을 사용한다(예:EAL3+). 상위의 보증수준은 하위의 보안수준보다 완전하고, 엄격하며 정형적이므로 보증수준간에는 완전성, 엄격성 및 정형성 관계를 갖는다[2,3,12].

정보보호시스템(TOE: Target of Evaluation, 평가대상물)의 제품유형에 따라 CC보안기능요구사항의 일부를 선택하고 7단계의 보안수준 중 하나를 택하여 보호프로파일(PP: protection profile) 또는 보안목표명세서(ST: security target)를 구성한다. PP는 정보보호제품의 유형(방화벽, 스마트카드, 운영체제 등)의 특성에 따라 CC의 보안기능요구사항과 보증요구사항으로부터 선택한 제품 유형별 공통 보안요구사항명세서에 해당하며 ST는 특정 제품(예: Oracle 9i)의 보안요구사항명세서에 해당한다.

2.2 공통평가방법론 (CEM)

CEM은 IT 보안평가를 위한 CC를 위한 지침문서로써 적절하고 비용 효과적인 평가를 수행할 수 있는 골격을 제시하여 효율적인 평가결과를 도출할 수 있도록 하며 평가받은 제품의 등급유지 및 평가결과의 상호인증을 목적으로 한다. CEM은 CC에 정의된 기준과 평가증거를 사용하여, CC 평가지침에 따른 평가자가 수행해야하는 최소한의 행동을 기술하고 있다. CC구조와 CEM의 구조사이에는 직접적인 관계가 있으며 클래스, 킴포넌트, 평가자 행동요소의 CC 구성과 CEM의 활동, 하부활동, 행동 구조가 대응된다[3,12]. 그러나, 몇몇의

CEM 작업단위는 CC 개발자행동, 내용과 표현요소의 주된 요구사항으로부터 생성될 수 있다. CEM은 1997년도 CEM 파트1 v0.6 발표를 시작으로 현재 CC의 버전을 따라 v2.2가 개발되어 현재 EAL1~EAL4의 정보보호제품평가에 활용하고 있으며 비공식문서로서 v2.4가 개발 중에 있다.

2.3 현재 동향

현재 정보보호제품 및 시스템을 평가하기 위해서 평가기준으로 적용하고 있는 것은 CC v2.1 또는 v2.2이며 CC와 함께 CEM 역시 v2.2를 따른다.

CC와 CEM v2.2를 분석함으로써 실제평가에 적용할 수 있는 평가스킴으로 사용하고자 한다. 또한 CC와 CEM의 변화에 대한 이해를 도우며 정보보호제품 및 시스템의 평가동향에 유연하게 대처하고자 한다. 앞으로 CC와 CEM은 국제동향에 맞추어 계속해서 변화가 예상되며 그에 따른 평가참여자의 역할도 CC와 CEM의 기준에 맞추어 시대의 흐름에 대응해야 할 필요가 존재한다.

3. 평가요구사항 분석

CC v2.1과 CC v2.2는 큰 차이점이 존재하지 않으며 CC v2.2가 2004년 1월 공식적으로 발표되었으므로 본 논문에서는 CC v2.2를 중심으로 CEM v2.2와 함께 평가요구사항에 대하여 제시한다.

3.1 CC v2.2와 CEM v2.2의 요구사항

요구사항 분석은 평가준비, 평가실행, 평가결과 승인 의 3단계로 분류하여 실제 평가에서 주요한 최소한의 요구사항만을 분류해 놓았다.

평가참여자의 역할은 평가신청자, 개발자, 평가자, 감독자로 분류될 수 있으며 각각의 역할에 따라 평가의 3 단계에 참여하게 된다. 단계에 해당하는 각 사항은 CC v2.2와 CEM v.2.2에 명시되어 있는 평가요구사항을 근거로 한다[4,11,12].

3.1.1 단계1 : 평가준비(문서준비 및 제출)

- (1) 입력단계 : 평가에 필요한 TOE에 대한 전달물 및 평가를 위한 문서 등을 입력해야 한다.
- (2) 전달물 제출 : 평가신청자(또는 개발자)는 평가자에게 보호프로파일 및 보안목표명세서, TOE를 증명할 자료 전체(전달물), 평가가 요구된 TOE 등을 제출해야 한다.
- (3) 평가를 위한 문서준비 : 평가를 위해서는 평가기준, 평가방법론, 평가스킴, 그 밖의 참고자료가 필요하므로 평가자는 평가를 위한 문서를 준비해야 한다.

3.1.2 단계2 : 평가시행(TOE 평가)

(1) 예비 평가

평가자는 신속하고 간략한 예비평가를 초안 평가증거로 다음과 같은 문서를 이용할 수 있으며 이는 평결을 위한 기준으로 사용되지는 않는다.

- a) 평가자가 테스트와 테스트 절차의 빠른 평가를 하도록 허용하는 테스트 문서
- b) TOE 설계이해를 위해 배경을 제시하는 설계문서
- c) 평가자가 평가자지침의 응용을 평가하도록 허용하는 소스코드나 하드웨어 도면

(2) 실제 평가

- ① 평가 초기화 : 모든 평결은 'pass(통과)' 또는 'fail(실패)' 평결이 나기 전까지 'inconclusive(유보)'로 초기화된다.
- ② 평가근거 정보 목록 제공 : 평가자는 평가 근거의 각 항목에 대해 발행자(예: 개발자, 보증인), 제목, 유일한 참조(예: 발행일, 버전 번호) 등의 정보를 보고해야 한다.
- ③ 배타적인 평가구조 : 최종평결은 배타적인 평가구조를 가지며 하나라도 'fail(실패)'나 'inconclusive(유보)'가 존재할 때 최종평결 또한 '실패'나 '유보'가 된다. (그림 1)은 CEM구조와 평결규칙을 나타낸다.

(3) 보고서 작성

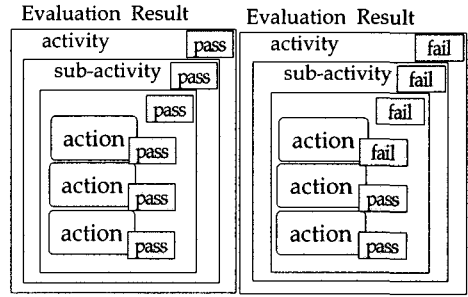
평가자는 보고서의 정보내용에 대한 요구사항을 충족하기 위해 관찰보고서와 평가기술보고서에 대한 부업무를 수행하여야 한다.

- ① 출력 단계 : 평가 중간단계에서 문제점이 발생하거나 필요한 명시를 표현하는 방법으로 "관찰보고서(OR)"가 발행되며 최종적으로는 "평가기술보고서(ETR)"가 발행된다. 관찰보고서와 평가기술보고서는 평가신청자 또는 개발자에게 전달할 수 있는 스키마가 요구되며 관찰보고서와 평가기술보고서에 대한 요구사항은 다음과 같다.

- ② 관찰 보고서 (OR : Observation Report) : 관찰 보고서는 평가 시 필요할 때에만 작성되며 "실패" 평결의 경우 평가자는 평가결과를 반영하기 위한 관찰보고서를 제공해야 한다. 또한 평가자는 필요한 명시를 표현하는 한 방법으로 관찰보고서를 사용하며 개발자에게 문서 수정을 요구할 때 발행 가능하다. 관찰보고서에 식별 가능한 목록으로서 관찰보고서 식별자, 간단한 요약, 제목이 필요하며 포함 내용으로는 (그림 2)와 같다.

- ③ 평가기술보고서(ETR : Evaluation Technology Report) : 평가기술보고서를 작성하기 위해서는 단위업무에 관련한 평가업무 패키지(Evaluation Work Packages)가 필요하며, 오직 하나의 ST, PP, TOE 에 대해서 평가기술보고서는 하나만 존재한다[14]. 작성된 평가기술보고서는 표준에 의거하고 평가 권위를 증명하는 출력물로서 효력을 발

휘하며 문서 결과에는 모든 필요 정보를 제공하지는 않는다. 또한 특별히 요청되는 부가적인 정보에 관하여 내용이 추가될 수



- 배타적인 평가 구조를 가짐.
- 평가자행동(Action)을 기준으로 평가를 내림
- 평가자행동의 지침은 "평가자는 제공된 정보가 모든 증거요구사항을 만족하는지 확인해야 한다"이므로 하부활동(Sub-activity)에 속하는 모든 증거요구사항에 대해서 만족해야 함.
- 각 증거요구사항에 대해서도 배타적인 평가 구조를 적용시킴.

그림 1. 공통평가방법론(CEM)의 구조와 평결 규칙[12]

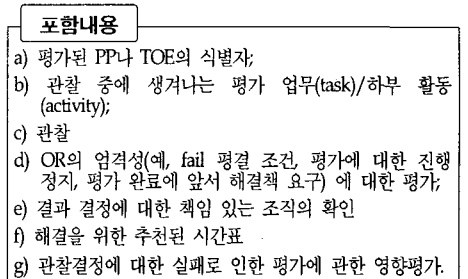


그림 2. 관찰보고서(OR)에 포함되어야 할 내용

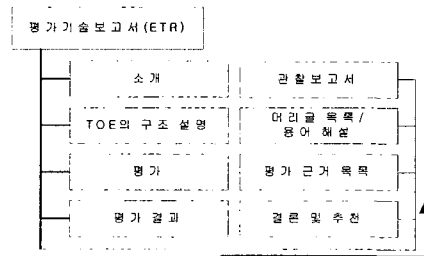


그림 3. PP 및 TOE에 대한 평가기술보고서(ETR) 정보 내용

있으며 평가기술보고서는 기밀 사항 또는 소유자의 정보를 포함해야 하며 유출이 되지 않도록 보안을 철저히 해야 한다. (그림 3)은 PP 및 TOE 평가에 대한 평가기술보고서 정보 내용을 나타낸다. 이는

목적은 개발자가 TOE 사용자에게 보안결함의 추적 및 교정행위의 식별, 이에 대한 배포를 기술하는 결함교정 절차를 확립했는지에 대해 결정하는 것이다.

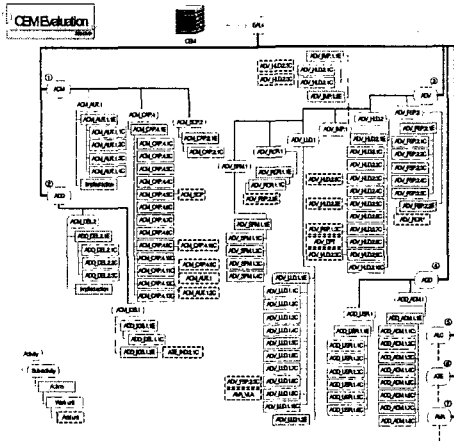


그림 5. EAL4등급에 대한 평가 업무

각 평가보증등급에 따른 평가업무 이외에도 필요하다면 “ALC_FLR(결함 교정)”패밀리에 대한 부가적인 평가업무를 수행해야 한다. CEM 또한 “ALC_FLR(결함교정)” 패밀리에 관한 평가 부활동을 따로 정의하고 있다. 평가자가 TOE의 평가를 수행할 때 “ALC_FLR(결함교정)” 부활동에 대한 업무는 평가보증등급과 관계없이 CC와 CEM의 기준에 따라 수행되어야 할 것이다.

4. v2.2와 v2.4의 변화 특징

CC v2.4는 CC의 구성 면에서 파트 2만 그대로 유지하며 파트 1과 파트 3에서 괄목할만한 변화를 보인다. CC v2.2와 CC v2.4의 큰 차이는 PP와 ST의 평가 구성요소의 변경과 ST가 평가보증등급의 상관관계에 포함된다는 것이다. 이에 따라 AVA_SOF(보안기능강도) 패밀리가 삭제되었으며 이외에도 AVA_VLA(취약성평가) 패밀리의 중속성 삭제, 추상적인 “일관성”요구사항 삭제 및 축소화한 특징을 보인다.

CEM v2.4는 CEM v2.2까지 파트1과 파트2로 분류되어 있는 문서를 하나로 통합하여 작성되었다. CC에서 ST 평가 패밀리가 평가보증등급에 관여함에 따라 CEM에서도 역시 ST평가의 부활동이 평가보증등급에 관계하여 포함된다. 또한, CEM v2.2에서는 PP와 ST, EAL1~4의 부활동이 명시되어 있으나 CEM v2.4에서는 PP와 EAL1, 4 부분의 부활동만이 존재하며 EAL2와 EAL3등급에 관한 사항은 특별한 평가활동으로 분류해놓고 있다[12,13]. 또한, CEM v2.4에 추가된 사항

은 다음과 같으며 현재 평가수행 시 참고 가능한 요구사항이 된다. CEM v2.4에서 “평가프로젝트 생성 시 평가자(평가책임자 포함)를 3명으로 구성한다.”라고 직접적으로 제시하므로 평가를 할 때 가장 적정 평가인원으로 3명으로 구성할 수 있다. 또한 ETR과 관련하여 입력작업과 출력작업에 관련된 식별자 및 관련된 사항을 보고서 자체나 평가프로젝트 정보에 포함하도록 명시하고 있다. 그리고 평가참여자의 역할 중 “감독자(Overseer)”가 “평가 권위자(evaluation authority)”로 명칭이 바뀌며 증명/검증보고서를 발행하는 업무가 부가된다.

CC v2.2에서 CC v2.4로의 변화는 ST가 평가보증등급(EAL)과 관계되었으며 PP 및 ST의 보증패밀리 목록이 변경되었고, ST가 평가보증등급(EAL)에 관계되면서 AVA_SOF(보안기능강도)가 삭제되는 등 이전의 변화 특징보다 큰 변화를 보이고 있다. 이렇듯 보안기능에 중점을 둔 CC v2.2에 비해 CC v2.4는 TOE의 요구사항에 관련한 기능에 초점을 맞추고 있다. CEM의 경우 추상적이고 주관적인 내용의 간소화 및 명확화, 그리고 실례를 적용한 평가방법을 제시함으로써 개발자 및 평가자가 평가에 대해 좀더 쉽게 이해할 수 있도록 상세화된 특징을 보인다.

5. 결론

본 논문은 CC와 CEM의 개념과 문서에 명시된 평가요구사항에 관하여 논하였으며 개정중인 지침문서의 변화된 사항에 대하여 살펴보았다. CC기반 평가는 국제적으로 정보보호제품 및 시스템의 평가에 관한 일원화, 효율성, 그리고 관리의 표준화를 위한 방향제시를 하고 있다. 국내뿐만 아니라 국제적으로 정보보호시스템의 사용도는 증가하고 있으며 이러한 정보보호시스템의 신뢰성 확보와 상호인증을 위해 CC는 필요불가결한 존재가 되고있다. 현재 CC v2.4와 CEM v2.4는 비공식문서이지만 변화된 사항을 분석 및 예측하여 효율적이며 유연한 평가를 수행할 수 있는 이점을 가지고 있다. 앞으로도 계속 CC와 CEM의 변화를 예측 및 분석하여 평가요구사항을 정확히 파악할 수 있어야 하며 이를 실제 평가에 적용 및 반영한 자동화된 도구로 발전시킬 수 있을 것이다.

참 고 문 헌

- [1] Information Technology Security Evaluation Manual (ITSEM), Commission of European Communities, <http://www.cesg.uk>, 1993.
- [2] DoD, “Department of Defense Trusted Computer System Evaluation Criteria (TCSEC),” Dec. 1985.
- [3] 한국정보보호진흥원, “정보보호시스템 평가·인증 가이드

- 드," KISA, pp.52-68, 2002. 12.
- [4] Part 1 : Introduction and General Model, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-01-001, Version 2.2 : ISO/IEC 15408, Jan. 2004.
 - [5] Part 2 : Security Function Requirements, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-01-002, Version 2.2 : ISO/IEC 15408, Jan. 2004.
 - [6] Part 3 : Security Assurance Requirements, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-01-003, Version 2.2 : ISO/IEC 15408, Jan. 2004.
 - [7] Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), US Dod 5200.28-STD, Dec. 1985.
 - [8] 김광식, 남택용, "정보보호시스템 공통평가기준 기술동향," <http://kidbs.itfind.or.kr>, pp.2-15, Oct. 2002.
 - [9] Part 1 : Introduction and General Model, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-03-001, Version 2.4 : ASE/APE Trial Use version, Mar. 2004.
 - [10] Part 3 : Security Assurance Requirements, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-03-003, Version 2.4 : ASE/APE Trial Use version, Mar. 2004.
 - [11] Part 1 : Introduction and general model, Common Evaluation Methodology for Information Technology Security(CEM), CEM-97/017, Version 0.6, Jan. 1997.
 - [12] Part 2 : Evaluation Methodology, Common Evaluation Methodology for Information Technology Security(CEM), CCIMB-2004-01- 04, Version 2.2, Jan. 2004.
 - [13] Evaluation Methodology, Common Evaluation Methodology for Information Technology Security(CEM), CCIMB-2004-03-04, Version 2.4 : ASE/APE Trial Use version, Mar. 2004.
 - [14] Reuse of Evaluation Results and Evidence, 2002-08-009-002, CCRA, Version 1 Final, pp.1-2, Oct. 2002.
 - [15] Ruben Prieto-Diaz, "The Common Criteria Evaluation Process," CISC, pp.24-33, Dec. 2002.

강 연 희



2003년 한남대학교 컴퓨터멀티미디어 공학과 졸업(학사)
 2003년~현재 한남대학교 컴퓨터공학과 석사 과정
 관심분야 : 소프트웨어공학, 정보보호시스템 평가, 보안공학

방 영 환



1997년 한남대학교 컴퓨터공학과 졸업(학사)
 2002년 대전대학교 대학원 컴퓨터공학과 졸업(석사)
 2002년~현재 대전보건대학 컴퓨터정보처리과 프로그래밍 전문강사

2002년~현재 한남대학교 대학원 컴퓨터공학과 박사과정
 관심분야 : 소프트웨어 품질 평가 및 보증, 소프트웨어 표준화, 보안공학

최 성 자



1991년 한남대학교 컴퓨터공학과 졸업(학사)
 1997년 한남대학교 대학원 컴퓨터공학과 졸업(석사)
 2002년~현재 한남대학교 컴퓨터공학과 박사과정

관심분야 : 소프트웨어공학, 자바, 워크플로우 모델링, 보안평가 EDI 보안, 패턴리넷 등

이 강 수



1981년 홍익대학교 전자계산학과 학사
 1983년 서울대학교 대학원 전산학과(석사)
 1989년 서울대학교 대학원 전산학과(박사)
 1985년~1987년 국립한밭대학교 전자계산학과 전임강사

1992년~1993년 미국일리노이대학교 객원교수
 1995년 한국전자통신연구원 초빙연구원
 1998년~1999년 한남대학교 멀티미디어학부장
 1987년~현재 한남대학교 컴퓨터공학과 정교수
 관심분야 : 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼