CC RI 처리절차 및 Final Interpretation 분석

김선미, 김상호, 김태훈, 노병규
한국정보보호진흥원

CC RI processing and Final Interpretation Analysis

Sun-Mi Kim, Sang-Ho Kim, Tai-Hoon Kim, Byung-Gyu No
Korea Information Security Agency

요 약

공통평가기준(CC: Common Criteria)은 1999년에 국제표준(ISO/IEC 15408)으로 채택되어 우리나라를 포함한 미국, 캐나다, 영국, 프랑스, 독일, 네덜란드 등에서 사용되고 있는 IT제품 및 시스템의 보안성 평가기준이며, Interpretation 과정을 통하여 지속적으로 수정 및 보완되고 있다.

본 논문에서는 공통평가기준의 문제점 요청 및 Interpretation 제정 절차를 소개하고 현재 발표된 공통평가기준 버전 2.1의 Final Interpretation을 분석하였다.

I. 서론

공통평가기준(Common Criteria, CC)은 CTCPEC, FC, TCSEC, ITSEC 등 각국이 서로 다른 평가 기준을 사용하여 평가를 시행함으로써 발생하는 비용과 시간의 과다 소모 등의 문제점을 없애기 위해 미국, 캐나다, 영국, 프랑스, 독일, 네덜란드 등 선진 6개국을 중심으로 독립된 각 평가기준을 널리 이용될 수 있는 단일 IT 보안성 평가기준으로 통합한 것이다.

공통평가기준 개발을 위한 '공통평가기준 프로젝트'의 목적은 기존 평가기준들의 기술 및 개념상의 차이를 해결하고 ISO에 결과를 제출하여 국제표준화에 기여하기 위한 것이며 개발 참여기관의 대표자들은 공통평가기준 개발을 위하여 CCEB(CC Editorial Board)를 구성하였다. 이후 CCEB와 ISO/IEC JTC 1/SC 27/WG 3간의 교섭이 이루어졌고 그 결과로 1996년에 공통평가기준 버전 1.0이 개발 완료되어 CD(Committee Draft)로 승인되었다.

공통평가기준 프로젝트에서는 공통평가기준 버전 1.0을 기준으로 시험평가를 여러 번 수행하였고, 공통평가기준에 대한 광범위하고 공개적인 검토를 진행하였다. 공통평가기준 개정작업은 CCEB의 후임단체인 CCIB(CC Implementation Board)를 통해 수행되었고, 이 작업의 결정체가 1998년 5월에 발표된 공통평가기준 버전 2.0이며, 이후 버전 2.0을 수정 및 보완한 공통평가기준 버전 2.1이 발표되었고 ISO/IEC JTC 1은 1999년 6월 공통평가기준 버전 2.1을 국제 표준(ISO/IEC 15408)으로 채택하였다.

CCIB는 CCIMB(Common Criteria Interpretation Management Board)로 이관하여 공통평가기준 개정작업등을 수행하고 있다.

본 논문에서는 CCIMB의 역할과 공통평가기준 버전 2.1의 문제점 요청 및 Interpretation 제정 절차를 소개하고, 현재 발표된 공통평가기준 버전 2.1의 Final Interpretation을 분석하고자 한다.

II. Interpretation 요청 및 처리절차

1. CCIMB

CCIMB는 CC 집행위원회에 속하는 CC 해설서 관리 위원회이다. CCIMB는 CCRA(Common Criteria Recognition Arrangement, CC 상호인정협정)에 가입한 국가간의 평가 일관성을 유지하고, CC를 보다 일관성 있게 적용하기 위해 CC 및 CEM(Common Evaluation Methodology, 공통평가방법론)의 해설서 개발을 목적으로 하고 있다. 각 국의 평가 스킴 또는 일반인은 CCIMB에 RI(Request for Interpretation)를 제출할 수 있다. 제출된 RI는 CCIMB에서 논의를 거쳐 CC 및 CEM 해설서 개발에 사용하며, 필요시 CC와 CEM 개정에 사용한다.

2. RI

CC 또는 CEM의 해석에 대하여 CCIMB에 문제를 제기하는 요청을 RI라 한다. 제출된 RI의 유형은 다음을 포함할 수 있다.

- CC/CEM에서 수정이 요구되는 오류
- CC/CEM에 식별된 필요사항 추가
- CC/CEM에 적용하기 위한 방법 제안
- CC/CEM의 이해를 돕기 위한 정보

RI는 입력, 처리, 결과의 과정을 거쳐 Interpretation에 포함되거나 채택되지 않은 경우 요청자에게 피드백된다.

RI는 여러 가지 동기에서 발생하게 되고 몇 가지 유형으로 나뉘어 요청을 하게 된다. 또한, RI가 Interpretation으로서 의미를 갖기 위해 세부적인 단계를 거친다.

1) 동기부여

CC 또는 CEM의 Interpretation을 요청하는 이유는 다음과 같다.

- TOE 평가에 영향을 주는 경우 - TOE를 평가하기 전 계획 단계 또는 평가 중에 발생할 수 있다.
- IT 제품 및 시스템의 보안성 평가를 지원하는 자료 개발에 영향을 주는 경우 - 스킴 문서, CC 또는 IT 보안 설명서, 습득한 자료, CC(또는 CEM)와 관련된 문서를 개발하는 중에 발생할 수 있다.
- PP 개발에 영향을 주는 경우 - 사용자가 CC 및 CEM의 개념을 특정 기술분야에 적용하여 PP 개발 시 Interpretation을 필요로 할 때 발생할 수 있다.
- 학구적인 관심 - CC에 관심이 있는 사람이 CC 관련 자료를 읽다가 오류를 발견할 수도 있다.

2) 요청유형

Interpretation을 요청하는 유형은 다음과 같이 분류할 수 있다. 요청에 따라서는 Interpretation 유형과 직접적으로 관련되지 않을 수도 있고, 하나의 이상의 유형으로 요청될 수도 있다.

- 오류 인식 - CC 또는 CEM의 내용에 명백한 오류가 발생하여 수정 필요
- 누락된 자료 - CC 또는 방법론에서 필요한 추가 자료 식별
- 확인/동의 - 특별한 상황에서 CC 또는 CEM을 적용하기 위한 방법 제시
- 설명 - CC 또는 방법론을 이해하는데 필요한 자료 요청. 이 요청 유형은 자료를 추가하기 위해 반드시 요청할 필요는 없지만, 요청하지 않을 경우 나중에 이해 부족을 초래할 수 있음

3) RI 해석 절차

CCIMB에 제출된 RI를 수용하고 그에 맞는 응답을 제공하기 위해서는 다음 절차를 따라야 한다.

- Step 1 : RI 코디네이터에 의한 중재

RI 코디네이터는 RI를 요청한 사람(예: 개발자)과 RI를 수용하는 쪽(예: CCIMB)에서 요청절차가 원활하게 등록되도록 중간 역할을 하는 사람이다. 요청하는 절차가 더 자동화 될수록 그 역할은 감소하겠지만, 관리적인 지원을 위해서는 항상 필요하다.

- Step 2 : RI 접수

RI 요청은 CCIMB 회원이나 요청자(예, RI 코디네이터)로부터 웹사이트를 통해 받게 된다. 접수된 RI는 어떤 정보도 포함하지 않은 그 상태를 'RI 등록부'에 등록시킨다. CCIMB 회원은 요청을 처리하기 전에 각자의 스킴과 관련하여 선처리 할 요청을 선택하게 된다.

- Step 3 : 요청 할당

CCIMB 의장은 해당 RI에 대한 모든 토론 및 결정의 핵심 역할을 하는 CCIMB 회원(RI 챔피온)에게 RI를 할당한다. RI 챔피온은 요청이 완료되었는지를 결정하고 추가적인 정보가 필요하다면 요청자와 접촉한다. 이것은 CC 프로젝트 문서가 요청에 따라 영향을 받는지, 다른 CC 프로젝트 그룹(예: CEMEB)의 포함이 필요한지 여부를 결정하는 것이다. 새로운 챔피온은 의장의 재량으로 요청을 처리하는 시간을 할당받게 된다.

- Step 4 : RI 챔피온 처리 시작

RI 챔피온은 'RI 등록부'의 요청에 대한 모든 정보 교환을 캡처할 책임이 있고, 수행된 작업에 대한 기록을 남겨야 한다. RI 코디네이터는 웹사이트를 통해 받은 어떤 제안이라도 RI 챔피온에게 안전하게 전달되도록 지원한다. 언제라도 요청자가 추가적인 정보 제공을 요청하는 동안은 보류 상태가 된다.

- Step 5 : RI의 우선순위 결정

CCIMB는 항상 RI를 접수받지만, 중요한 요청인 경우 우선순위를 주어 첫 번째로 처리한다. 초기 처리과정에서 CCIMB 의장(또는 위임된 RI 코디네이터)은 요청의 출처와 동기에 기반하여 요청의 우선순위를 결정하게 된다.

- Step 6 : 의견을 합의하기 위한 RI 토론

CCIMB(아마 CEMEB와 협동으로)는 요청에 대한 응답의 합의점에 도달하기 위해 요청과 관계된 토론에 참여하게 된다. 복잡한 문제를 가진 요청에 대해 여러 달이 소요되는 동안은 토론 상태를 유지하게 된다. 토론은 CC 및/또는 CEM에 대한 변경이 필요한지에 대한 결정을 포함하게 된다. 또한, 결정은 공개하거나 요청자에게 피드백되어 다시 요청하게 된다.

- Step 7 : Interpretation 초안

CCIMB가 해결법에 동의한 경우, Interpretation 초안을 작성한다. 이 단계에서 요청은 중지되고 Interpretation으로 변경된다. CCIMB는 웹사이트 게시판을 통해 검토한 Interpretation 초안을 공개한다. 공개된 내용은 약 두 달 가량 초안을 논의하게 되고, 토론을 마치게 된다. 하지만, 중요한 논평이 있다면 초안을 다시 논의하게 되고, CCIMB가 Interpretation에 동의할 때까지 초안은 공개되어 진다.

- Step 8 : Final Interpretation

CCIMB는 잠재된 문제에 대해 충분히 검토된 Interpretation 초안을 Final Interpretation으로 공개한다. 여기에서, Interpretation은 본질적으로 CC(또는 CEM)의 일부가 되고, 스킴에 의해 사용되어야 한다. Interpretation은 웹사이트의 초안 섹션에서 최종 목록으로 옮겨지고, Final Interpretation의 형태로 표시된다.

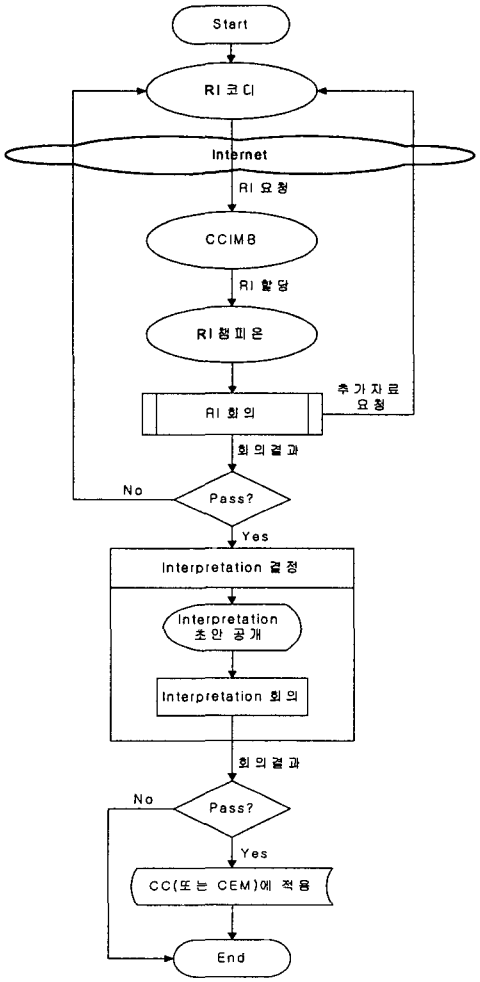
- Step 9 : Interpretation을 다음 버전에 적용

Final Interpretation은 CC(또는 CEM)의 다음 버전의 기초로 사용되며, 다음 버전이 발표되었을 때, Final Interpretation을 적용 및 표시하여 웹사이트로 옮긴다. 이 시점에서 Interpretation은 기존 평가기준에

서 삭제할 하나 또는 그 이상의 CC 문서를 고려하게 된다.

4) RI 해석 절차 흐름도

앞에서 설명한 RI 해석 절차 내용을 도식화하여 나타내면 [그림1]과 같다.



[그림 1] RI 해석절차 흐름도

III. RI 현황 및 Final Interpretation

1. RI 현황

현재 CCIMB에 제출된 RI는 242개이고, 각 RI의 상태는 [표 1]과 같다.

RI 중 CCIMB의 논의가 끝난 Final Interpretation은 CC V2.1 이후 버전인 CC V3.0에 반영될 예정이다. 미국, 캐나다, 영국, 프랑스, 독일, 네덜란드 등 상호인정협정(CCRA) 가입국은 향후 정보보호제품 평가의 핵심이 될 CC에 자국의 평가기준 및 평가방법을 적극적으로 반영하기 위해 CCIMB에서 적극적으로 활동하고 있다.

[표 1] CCIMB에 제출된 RI

상태	갯수
Received(접수)	34
Assigned(할당)	22
Discussion(논의)	53
Draft(초안)	11
Superceded(교체)	7
Closed(종료)	69
Incorporated(적용)	11
Final(최종)	35
합계	242

2. Final Interpretation 분석

본 논문에서는 현재까지 CCIMB에서 발표한 Final Interpretation을 분석하여 추가, 수정, 삭제로 분류 및 공통평가기준의 1부(소개 및 일반모델), 2부(보안기능요구사항), 3부(보증요구사항)에 [표 2]와 같이 적용하였다.

[표 2] Part별 분류표

부 / 분류	1부	2부	3부
추가	2	1	7
수정	5	2	9
삭제	1	3	4
총계	8	6	20

1) 추가

주요 추가사항으로는 분석된 내용에서 보듯이 컴포넌트의 추가, 연관된 패밀리간의 불일치로 인한 내용 추가, 클래스에 기능을 제공하기 위한 새로운 패밀리 추가 등이 있다.

1부에서는 위협이 TOE(Target of Evaluation) 뿐 아니라 TOE의 환경에 의해 만족되도록 위협의 범위 확대, 보호프로파일과 보안목표명세서간에 일치해야할 보안목표명세서의 응용 시 주의사항이 추가되었다.

2부에서는 보안관리 클래스(FMT: Security management) 중 관리할 수 있는 기능명세 패밀리가 추가되었다.

3부에서는 유일하지 않은 형상항목 식별, 단일 TOE에서 다중 영역에 대한 다중 SOF(Strength of Function) 선언, TOE가 제품의 일부분일 경우에 대한 형상관리 클래스(ACM: Configuration management) 적용, TOE에 의해 제공된 보안기능 관리를 명세하기 위한 컴포넌트 등이 추가되었다.

다음은 추가에 해당하는 예이다.

- 단일 TOE에서 다중 영역에 대한 다중 SOF 선언

CC는 TOE를 위해 하나의 최소 강도를 수용하지만 TOE가 다중 영역을 수행하는데는 부적당하므로, 보호프로파일 또는 보안목표명세서에서 정의된 각 영역의 최소 강도 계층을 수용하여 다중 영역에서 수행한다.

● 위협은 환경에 대한 하나 또는 그 이상의 보안목적의 결합으로 대응

위협은 TOE에 대응하지 못하는 자산뿐 아니라 TOE환경에서 요구되는 자산까지 보호가 필요하므로, 위협의 범위에 TOE 및 TOE환경을 포함시켜야 한다.

● TOE에 의해 제공된 보안기능관리를 명세하기 위한 컴포넌트 부재

FMT(보안관리) 클래스는 보안관리기능을 제한하여 수행하지만, 이 기능을 적용한 TSF(TOE의 보안정책)에 보안관리기능을 명세하기 위한 컴포넌트가 없다. 이를 제공하기 위해서 FMT 클래스에 보안 기능 관리를 호출하는 새로운 패밀리의 추가가 필요하다.

2) 수정

주요 수정사항은 기능 컴포넌트의 오퍼레이션 중 반복과 정교화의 사용에 관한 정의, 사용 범위 및 사용 방법에 관한 것과 정교화의 제약사항 등이 있으며 기존 공통평가기준의 둘 이상 부분에 연관되는 내용이 많다. 불명확한 정의에 따른 혼란 및 제약사항, 단순한 오류, 목적과 내용의 불일치, 중복된 내용 등이 수정되었다.

1부에서는 평가결과의 '추가'와 '준수'의 중복사용, 정교화를 사용함에 있어 혼란을 초래하는 내용 등이 수정되었다.

2부에서는 컴포넌트 복사 중 오류 및 정교화의 혼란이 수정되었다.

3부에서는 용어의 정의가 부정확함, 결함교정(ALC_FLR: Flaw remediation) 설명서 오류, 명백하지 않은 요구사항, 목적에 부합되지 않는 내용 등이 수정되었다.

다음은 수정에 해당하는 예이다.

● 평가결과의 추가와 준수 중복 사용

CC 3부 보증패키지의 의미를 보면 패키지에 대한 평가 요구사항 없이 "추가" 및 "준수"의 정의가 서로 포함되었다. 보증패키지의 내용이 임의적이기 때문에, 하나의 보증패키지에 다른 보증 컴포넌트를 더한 경우는 추가라 할 수 있지만, 다시 보면 새로운 보증 패키지로서 정의되므로 "준수"이다.

● '배포의 목적'에 적합하지 않은 내용

ADO_DEL(배포)의 목적은 TOE 무결성을 보호하는데 참조하는 내용을 다루어야 하지만, 실제 내용은 일반적인 보안에 관한 내용을 다룬다. 배포의 목적은 분배하는 동안 TOE의 보안(예: 비밀성, 무결성, 가용성)을 유지하는 것이므로, 무결성을 요구하는 ADO_DEL.2와 ADO_DEL.3에 무결성을 다루는 내용으로 수정하고 있다.

● 정교화의 혼란

IT 요구사항은 TOE가 아닌 IT환경에서 그 요구사항이 만족됨을 명시하므로 "TOE 보안기능"이 "IT환경"으로 변경되는 것은 확장이 아니라 정교화이다.

3) 삭제

주요 삭제사항은 불필요한 용어 및 내용, 중복적으로 사용되는 항목 등이 삭제되었다.

1부에서는 본문 내용 중 '최소한'이란 단락을 삭제되었다.

2부에서는 본문 내용 중 '최소한'이란 단락을 삭제 및 오퍼레이션 사용의 불필요한 내용을 삭제되었다.

3부에서는 '분명하게 명시된다'는 중복적인 내용 및 오퍼레이션 사용의 불필요한 내용을 삭제되었다.

다음은 삭제에 해당하는 예이다.

● 이미 포함된 증거요구사항에서 '최소한'의 사용

엘리먼트의 증거요구사항에서 "최소한"의 사용은 추가적인 정보인 '보안기능은 적어도 하나의 TOE 보안기능요구사항을 만족시켜야 한다'에 포함되므로, 따로 사용하는 것이 불필요하다.

● 보호프로파일/보안목표명세서에서 '분명하게 명시된다'의 의미

ASE_OBJ.1.2/3C와 APE_OBJ.1.2/3C의 내용 중 "분명하게 명시된다."는 ASE_OBJ.1.2E와 APE_OBJ.1.2E에서 이중으로 요구하므로 그 부분을 삭제한다.

IV. 결론

본 논문에서는 공통평가기준의 개발 배경 및 연혁을 알아보았고, RI 요청 절차 및 평가 중에 발생하는 문제에 대해 CCIMB에 요청하여 처리하는 과정을 분석하였다. 또한, Final Interpretation을 분석하여 공통평가기준에서 추가, 수정, 삭제되는 부분에 대해서 알아보았다.

Final Interpretation은 단순히 현재의 CC버전에서 변경되는 내용으로써의 의미뿐만 아니라 향후 수정된 공통평가기준 버전에 반영되어 평가에 적용되므로 관련 동향 파악 및 분석이 중요하다. 하지만 Interpretation은 수시로 발생되고 있으므로 CCIMB의 경우, Interpretation을 웹사이트에 게시하여 이를 평가에 적용할 수 있도록 하고 있으며, 이를 반영한 공통평가기준 버전 변경 및 버전 개정을 계획하고 있다. 공통평가기준을 수용한 국내에서도 수시로 Interpretation을 기준에 반영하여 기준을 개정·고시하는 것은 번거로울 수 있으므로 정보보호시스템 평가관련 규정에 Interpretation 적용 사항을 명시하여 신규로 해석되어 수정된 공통평가기준의 항목이 적용되도록 하는 것이 바람직하다 사료된다.

공통평가기준은 정보기술이 급속하게 발전됨에 따라 최신의 기술에 적합하게 해석 및 수정되고 있으며, RI 절차를 통한 Interpretation에 의해 반영 및 적용되고 있으므로 이에 대한 지속적인 동향 파악 및 분석이 필요하다.

참고문헌

[1] 정보통신부고시 제2002-40호, 정보보호시스템 공통평가기준, 2002. 8. 5

[2] 정보보호시스템 평가·인증 가이드, 정보보호진흥원, 2002. 12

[3] CCIMB Interpretation, CCIMB, 2002. 2. 15

[4] http://www.commoncriteria.org