情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

공통평가기준 v2.3과 v3.1 비교 분석

조혜숙*, 전웅렬*, 정한재*, 이성진*, 유연정**, 김승주*, 원동호*‡

요 약

미국, 독일 등 선진국을 중심으로 개발된 공통평가기준(Common Criteria, CC) 3.1이 공식 문서로 등재되어 2009년 9월부터는 기존의 CC v2.3을 완전히 대체할 것으로 예상됨에 따라 현재 우리나라 평가 완료된 CC v2.3 기반 보호프로파일은 CC 3.1 기반 보호프로파일로 개정이 필요하다. 따라서 본 논문은 CC v2.3과 v3.1에서의 보호프로파일 요구사항을 비교 및 분석하고, 보안기능 및 보증요구사항의 평가업무량 및 제출물 작성수준을 분석한다. 이러한 미국, 영국, 캐나다, 프랑스, 네덜란드 등 선진국의 주도하에 개발되고 있는 CC v3.1에 대한 분석을 통하여 국제적으로 새롭게 정립되고 있는 평가기준 및 평가방법에 대한 기술을 확보할 수 있으며, 향후 CC v3.1에 의한 평가 기반을 마련하는데 기여 할 것이다.

Ⅰ. 서 론

공통평가기준(Common Criteira, CC)은 보안기능이 있는 IT 제품이나 시스템의 보안성을 평가하기 위한 공통의 요구사항을 제시한 기준으로써 미국, 영국, 프랑스 등 선진국이 참여하여 각국의 보안평가기준을 하나로 통합 및 일원화하여 개발하였다. CC는 1993년 개발이 시작된 이래 현재의 v2.3 및 v3.1에 이르기까지 지속적으로 개선 및 개정되어 왔으며, 주요 개발 연혁은 다음과 같다.

- 1998년 5월 : CC 2.0
- 1999년 12월 : CC 2.1 (ISO 15408:1999)
- 2004년 1월 : CC 2.2 (ISO FCD)
- 2005년 6월 : CC 3.0 (Draft)
- 2005년 9월 : CC 2.3 (ISO 15408:2005)
- 2005~2006년 8월 : CC 3.0 개발 및 공개 검토
- 2006년 9월 : CC 3.1 (공식 평가기준)

우리나라는 이와 같은 국제적 추세에 발맞추어 2005년 1월부로 국내 평가기준을 CC로 일원화 하였으며, 현재 공통평가기준 관리위원회(CCMB, Common Criteria Management Board)에서 발행한 공식문서인 CC v2.3을 기반으로 정보보호제품의 보안성 평가를 수행하고 있다. 현재 CC v3.1은 미국, 독일 등 선진국을 중심으로 역할을 분담하여 개발 중에 있으며 클래스의 통합 및 간소화, 새로운 패밀리 추가, ADV 요구사항 상세화 등 기존의 CC v2.3에 비해 많은 변화가 예상됨에 따라서 CC v3.1 기반 보안기능 및 보증요구사항의 평가 업무량 및 제출물 작성수준 분석을 통해 보호프로파일을 개정하고 또한 보안목표명세서 개정을 위한 분석이 필요하다.

특히, CC v3.1이 공식 문서로 등재되면서 2009년 9월부터는 기존의 CC v2.3을 완전히 대체할 것으로 예상됨에 따라 현재 우리나라 평가 완료된 CC v2.3 기반 보호프로파일(국가기관용 침입차단시스템, 국가기관용 침입탐지시스템, 국가기관용 가상사설망, 국가기관용 등급기반 접근통제시스템, 네트워크 침입방지시스템 등 10종 이상)과 여러 업체에 의해 작성되고 평가된 보안목표명세서(네트워크정보보안제품군, 정보보호기반제품군, 컴퓨터정보보호제품군 등 80종 이상)는 CC v3.1 기반으로 개정이 필요하다.

따라서 본 논문에서는 CC v2.3과 CC v3.1의 보호프로파일의 요구사항을 분석하고, 보안기능 및 보증요구사항의 평가 업무량 및 제출물 작성 수준을 분석함으로써 CC v2.3과 CC v3.1을 비교 분석한다. 특히 본 논문은 보호프로파일의 구성을 예로 들어 비교 분석을 진행

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성·지원 사업과 정보보호진흥원의 공통평가기준 3.1 기반 보호프로파일 개발의 연구결과로써 수행되었습니다.

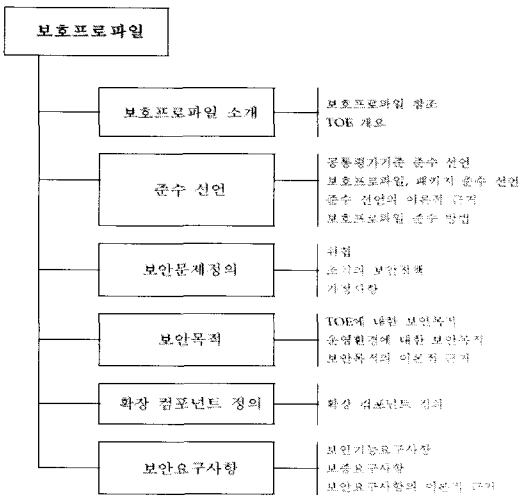
* 성균관대학교(hsjo@security.re.kr(주저자), wrjeon@security.re.kr, hjjeong@security.re.kr, sjlee@security.re.kr, skim@security.re.kr)
** 한국정보보호진흥원(yjyu@kisa.or.kr)
‡ 교신저자, 성균관대학교(dhwon@security.re.kr)

한다. 이와같은 분석을 통하여 기존 보호프로파일 및 보안목표명세서 개정 시 활용 가능하고, 또한 향후 CC v3.1을 적용하는 새로운 보호프로파일 및 보안목표명세서 개발과 평가 시 활용이 용의할 것으로 예상된다.

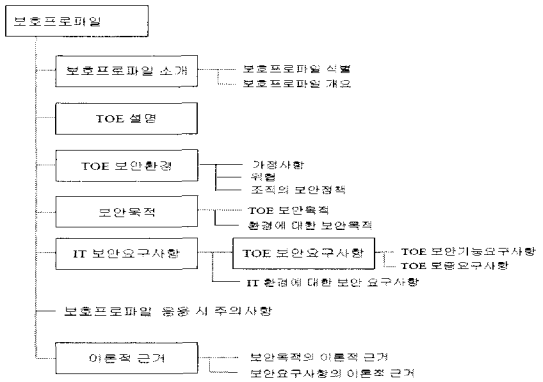
본 논문의 2장에서는 CC v2.3과 v3.1의 보호프로파일 요구사항을 비교 분석하고 3장에서는 평가보증등급 변경사항에 대해서 보증컴포넌트 별로 비교 분석한다. 4장에서는 보호프로파일의 소개, 보안문제정의, 보안목적의 변경사항에 대해서 자세히 설명하고 5장에서는 CC v3.1에서 새로 추가된 준수방법의 요구사항 분석과 준수방법 결정 방법에 대해서 설명한다. 6장에서는 확장 컴포넌트의 정의를 서술하고, 7장에서는 보안요구사항의 보안기능요구사항과 보증요구사항의 변경사항에 도출하고 8장에서는 결론을 맺는다.

Ⅱ. CC v2.3과 CC v3.1의 보호프로파일 요구사항 비교

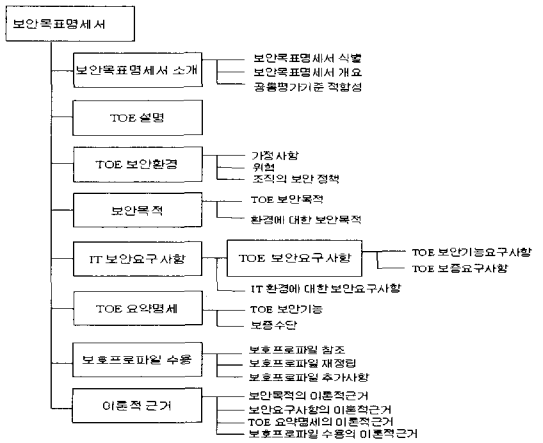
보호프로파일은 소비자 그룹과 이해집단이 그들의 보안 요구를 표현할 수 있도록 하고 보안목표명세서 작성을 용이하게 하기 위해 CC가 제공하는 문서로 CC v3.1에서 그 구조가 상이하게 변경이 되었다. 전체적은 구조의 변경은 단순·일관성·명료함 추구, 합리성 및 중복의 제거, 개발자 사용 편이성 향상을 목적으로 추진되었다. [그림 1]과 [그림 2]는 CC v2.3과 CC v3.1의 보호프로파일 구조와 보안목표명세서 구조를 나타낸다.



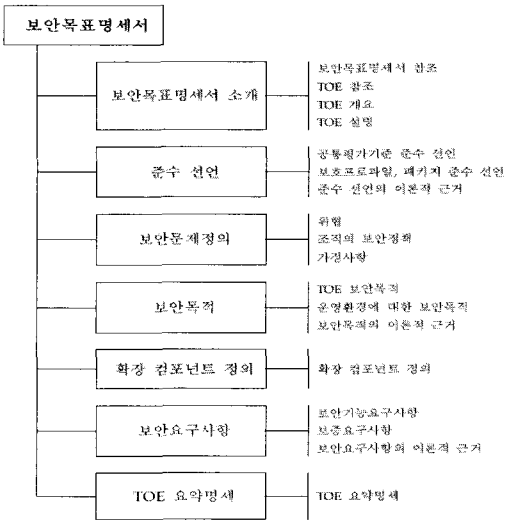
〔그림 1〕 공통평가기준 v3.1의 보호프로파일 구조



〔그림 2〕 공통평가기준 v2.3의 보호프로파일 구조



〔그림 3〕 공통평가기준 v3.1의 보안목표명세서 구조

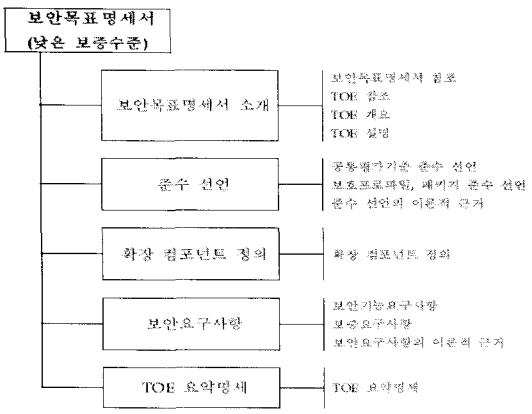


〔그림 4〕 공통평가기준 v2.3의 보안목표명세서 구조

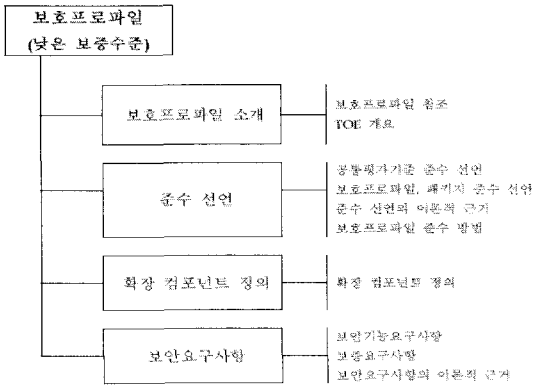
위 그림에서 보는 바와 같이 CC v3.1은 기존 CC v2.3 보호프로파일의 TOE 설명(TOE Descryption)을 보호프로파일 소개에 포함하고, 이론적 근거(Rationale)는 보안목적(Security Objectives)과 보안요구사항(Security Requirements)에 포함된다. 그리고 준수 선언(Conformance Claim)이 새로이 추가되었다. 그 외에도 TOE 보안환경(TOE Security Environment)은 보안문제 정의(Security Problem Definition)로 명칭이 변경되었고, IT 환경에 대한 보안요구사항이 삭제되었다. 그리고 보안목표명세서에서는 보호프로파일과 비슷한 변경 구조를 갖는 것을 볼 수 있다.

새로 추가된 준수 선언은 보호프로파일이 수용하는 CC의 버전과 보호프로파일에 사용된 보안요구사항이 확장되었는지 아닌지 등을 설명한다. 준수 선언은 보호프로파일 및 보안목표명세서에 모두 적용된다. 단, 준수 선언에서 준수 방법(Conformance Statement)은 보호프로파일에만 포함되는 내용으로 보안목표명세서 또는 다른 보호프로파일이 어떻게 본 보호프로파일을 만족해야 하는지를 기술한다.

또, CC v3.1에서 낮은 보증 수준의 보호프로파일과 보안목표명세서가 새로 추가되었다. 추가된 보호프로파일과 보안목표명세서는 EAL1에서만 선택적으로 사용할 수 있다. EAL1 등급의 경우 보호프로파일 개발자는 낮은 보증 수준의 보호프로파일을 선택할 수 있다. 그리고 낮은 보증 수준의 보호프로파일을 준수하는 보안목표명세서는 낮은 보증 수준의 보안목표명세서야만 한다. [그림 5]와 [그림 6]은 낮은 보증 수준의 보호프로파일과 보안목포명세서를 나타낸 것이다.



〔그림 5〕 낮은 보증 수준의 보안목표명세서



〔그림 6〕. 낮은 보증 수준의 보호프로파일

2.1. CC v2.3과 CC v3.1에서의 보호프로파일 요구사항 분석

[표 1]은 보호프로파일의 구조 비교를 도식화 한 것이다.

CC v3.1에서는 보호프로파일 소개와 TOE 설명이 보호프로파일 소개라는 하나의 장으로 통합되었다. 주요 내용 변경사항은 TOE 설명에서 TOE가 필요로 하는 하드웨어/소프트웨어/펌웨어의 식별을 요구한다는 점이다. 그 외 사항은 CC v2.3과 CC v3.1이 상이하게 차이나지는 않는다.

준수 선언은 CC v3.1에서 새로 추가된 장으로 보호프로파일의 준수와 준수 방법, 준수 패키지 등을 서술한다. 또한 보호프로파일이 준수하는 다른 보호프로파일

〔표 1〕 CC v2.3과 v3.1의 보호프로파일 구조 비교

CC v2.3의 보호프로파일	CC v3.1의 보호프로파일	CC v2.3과의 차이점
보호프로파일 소개 TOE 설명	보호프로파일 소개	TOE 설명이 보호프로파일 소개에 포함
-	준수 선언	CC v3.1에서 새로 추가된 장
TOE 보안환경	보안 문제 정의	제목 및 내용의 변경
보안목적	보안목적	보안목적의 이론적 근거를 포함
-	확장컴포넌트 정의	CC v3.1에서 새로 추가된 장
IT 보안요구사항	보안요구사항	보안요구사항의 이론적 근거를 포함
이론적 근거	-	이론적 근거라는 장 삭제

〔표 2〕 CC v2.3과 v3.1의 EAL4 등급 비교

CC v2.3		CC v3.1	
ACM_AUT.1	부분적인 형상관리 자동화	ALC_CMC.4	생산지원, 수용절차 및 자동화
ACM_CAP.4	생성지원 및 수용절차		
ACM_SCP.2	문제추적 형상관리 범위	ALC_CMS.4	문제추적 형상관리 범위
ADO_DEL.2	변경의 탐지	ALC_DEL.1	배포 절차
ADO_IGS.1	설치, 생성, 시동 절차	AGD_PRE.1	준비 절차
ADV_FSP.2	완전히 정의된 외부 인터페이스	ADV_FSP.4	완전한 기능명세
ADV_HLD.2	보안기능과 비보안기능을 분리한 기본설계	ADV_TDS.3	기본적인 모듈화 설계
ADV_LLD.1	서술적인 상세설계		
ADV_IMP.1	TSF 일부에 대한 구현의 표현	ADV_IMP.1	TSF에 대한 구현의 표현
ADV_SPM.1	비정형화된 TOE 보안정책모델		
AGD_ADM.1	관리자 설명서	AGD_OPE.1	사용자 운영 설명서
AGD_USR.1	사용자 설명서		
ALC_DVS.1	보안대책의 식별	ALC_DVS.1	보안대책의 식별
ALC_LCD.1	개발자가 정의한 생명주기 모델	ALC_LCD.1	개발자가 정의한 생명주기 모델
ALC_TAT.1	잘 정의된 개발 도구	ALC_TAT.1	잘 정의된 개발 도구
ATE_COV.2	시험범위의 분석	ATE_COV.2	시험범위의 분석
ATE_DPT.1	기본설계 시험	ATE_DPT.2	보안-수행 모듈 시험
ATE_FUN.1	기능 시험	ATE_FUN.1	기능 시험
ATE_IND.2	독립적인 시험	ATE_IND.2	독립적인 시험
AVA_MSU.2	설명서 분석의 검증	AVA_VAN.3	강화된 취약성 분석
AVA_SOF.1	TOE 보안기능 강도에 대한 평가		
AVA_VLA.2	독립적인 취약성 분석		
		ADV_ARC.1	보안 구조 설명
		ASE_CCL.1	준수 선언
		ASE_ECD.1	확장 컴포넌트 정의
		ASE_INT.1	보안목표명세서 소개
		ASE_OBJ.2	보안목적
		ASE_REQ.2	도출된 보안요구사항
		ASE_SPD.1	보안문제정의
		ASE_TSS.1	TOE 요약명세

을 소개하고, 본 보호프로파일이 CC 2부와 3부의 요구사항을 준수하는 방법을 설명하며, 준수 방법에서 다른 보호프로파일 및 보안목표명세서가 본 보호프로파일을 준수할 경우 준수방법을 설명한다.

기존 CC v2.3까지는 CC 2부의 요구사항을 확장하여 사용하는 것에 제한이 없었으나 CC v3.1부터는 2부 및 3부의 요구사항을 확장하는 경우, 확장 근거를 반드시 서술해야 하며, 2부 컴포넌트 확장의 경우 확장하는 컴포넌트를 CC와 동일한 수준으로 정의하고 사용해야 한다.

준수 방법에는 크게 두 가지 방법으로 입증 가능한 준수와 엄격한 준수가 있다. 입증 가능한 준수는 보안

목표명세서 혹은 보호프로파일이 한 보호프로파일을 준수하고자 할 때, 기존 보호프로파일의 보안문제정의와 보안목적, 보안기능요구사항을 수정할 수 있는 준수 방법이다.

엄격한 준수는 보안목표명세서가 보호프로파일을 준수할 때 TOE에 대해서는 최소한이며, 운영환경에 대해서는 최대한 명세 한다. 이는 보안목표명세서 개발자가 보호프로파일의 보안문제정의 및 보안목적을 모두 포함해야 함을 의미하며, 보안요구사항의 경우 추가적, 계층적으로 보다 강력한 보안요구사항을 추가할 수 있음을 의미한다.

요약하면 입증 가능한 준수 방법은 보안목표명세서 개발자가 환경에 대해 추가적인 가정사항 및 운영환경에 대한 보안목적을 추가할 수 있으며, 엄격한 준수는 이같은 수정이 불가능한 준수 방법이다.

CC v3.1에서 TOE 보안환경이 보안 문제 정의로 변경되었다. CC v3.1은 TOE와 TOE의 환경을 엄격히 분리할 것을 요구한다. 보안 문제 정의는 위협, 조직의 보안정책, 가정사항 순으로 기술할 것을 요구하며, CC v2.3보다 상세한 수준으로 서술할 것을 요구한다. CC v2.3의 이론적 근거 장은 CC v3.1에서 삭제되었지만 각각 보안목적과 보안요구사항 장 뒤에 포함된다.

확장 컴포넌트 정의는 CC v3.1에서 추가된 장으로 CC 2부나 3부에 포함되지 않은 새로운 컴포넌트를 정의한다. 개발자는 반드시 확장의 근거를 확장 컴포넌트의 이론적 근거에서 설명해야 한다.

Ⅲ. 평가보증등급 변경사항 도출

본 장에서는 평가보증등급의 변경사항에 대해 언급한다. CC v2.3과 CC v3.1의 가장 큰 차이점은 보증요구사항에 있다. CC v3.1에서 보증요구사항은 통합 및 삭제, 간소화 등 많은 부분이 수정되었으며, EAL 등급도 기존 CC v2.3과 다른 컴포넌트로 구성되어 있다. 기존 보호프로파일 및 개정 보호프로파일의 대부분이 EAL4 등급으로 보증등급을 설정하고 있기 때문에, 본 장에서는 CC v2.3과 CC v3.1의 EAL4 등급을 비교 및 분석한다.

EAL4 등급은 CCRA에 기인한 상호인증의 등급 중 가장 높은 등급이다. EAL5 등급 이상은 상호인증에 포함되지 않으며 평가를 받은 제품 및 시스템이라 해도 납품하고자 하는 기관의 요구에 맞춰 재평가를 받아야 한다.

그리고 EAL4 등급은 EAL 1~3 등급과 확연한 차이를 지니고 있다. 보다 상세한 평가를 위해 요구되는 보증요구사항의 컴포넌트들이 EAL4부터 등장하기 때문이다. 예를 들어 개발(ADV) 클래스의 상세설계(LLD) 패밀리나 구현의 표현(IMP) 패밀리같이 구현에 대한 직접적인 정보를 요구하는 컴포넌트가 EAL4 등급에서 처음 등장한다.

이와 같은 이유로 본 절은 CC v2.3과 CC v3.1의 EAL4 등급을 비교 및 분석하고자 한다. [표 2]는 CC v2.3과 CC v3.1의 EAL4 등급 보증컴포넌트를 연관관계에 맞게 도식화한 것이다.

증거요구사항에서 차이가 생기는 보증컴포넌트 별로 비교 및 분석한 결과는 다음과 같다.

3.1. ADO_DEL.2 - ALC_DEL.1

기존 배포(ADO) 클래스가 삭제되고 생명주기(ALC) 클래스에 배포와 관련된 내용이 흡수 통합되었다. ADO_DEL.2 컴포넌트가 배포 시 버전의 변경 및 불일치를 탐지하기 위한 모든 보안절차와 위장배포를 탐지하기 위한 시도에 대한 대책 기술을 요구하고 있는 반면, ALC_DEL.1은 단지 배포 시 보안을 유지하기 위한 모든 절차만 요구한다. 즉, 요구사항이 CC v2.3에 비해 완화되었다.

3.2. ADV_HLD.2, ADV_LLD.1 - ADV_TDS.3

CC v2.3의 개발 클래스, 기본설계(HLD) 패밀리와 상세설계(LLD) 패밀리가 CC v3.1에 이르러 TOE 설계(TDS) 패밀리로 통합되었다. 전체적으로 TDS 패밀리가 이전 HLD, LLD 패밀리에 비해 TOE 구성 및 설계에 대한 보다 높은 수준의 분석과 설명을 요구한다. 따라서 본 컴포넌트 간의 요구사항의 차이는 EAL4 등급에서만 나타나는 것이 아니며 CC v3.1에 이르러 TOE 설계에 대한 설명의 중요성이 보다 부각되었음을 의미한다.

3.3. ATE_DPT.1 - ATE_DPT.2

시험(ATE) 클래스는 본 컴포넌트의 차이를 제외하면 크게 달라진 점이 없다. 상세수준(DPT) 패밀리가 CC v2.3에서는 3개의 컴포넌트를 포함하는데 비해 CC

v3.1에서는 4개의 좀 더 세분화된 컴포넌트를 포함한다. CC v2.3의 ATE_DPT.1이 서브시스템 단위의 시험을 요구하는 반면, CC v3.1의 ATE_DPT.2는 모듈 단위의 시험을 요구한다. 이는 CC v2.3에 비해 CC v3.1이 상세수준 시험을 조금 더 정교하게 수행할 것을 요구함을 의미한다.

3.4. AVA_VLA.2 - AVA_VAN.3

CC v3.1에서는 취약성 분석(AVA) 클래스의 오용분석(MSU) 패밀리와 TOE 보안기능강도(SOF) 패밀리, 그리고 CC v2.3 EAL4에는 포함되지 않지만 비밀채널 분석(CCA) 패밀리가 삭제되었다. 그리고 개발자에 의한 취약성 분석이 삭제되고 EAL1 등급도 가장 낮은 수준의 평가자에 의한 취약성 분석을 수행하도록 하였다. AVA_VLA.2가 낮은 공격 성공 가능성을 지닌 공격자를 가정하고 취약성 분석을 실시하는 것에 비해 AVA_VAN.3은 강화된-기본 공격 성공 가능성을 지닌 공격자를 가정하고 취약성 분석을 실시할 것을 요구한다. 공통평가방법론의 부록에 따르면 낮은 공격 성공 가능성은 10~17 사이의 취약성 등급을 의미하고, 강화된-기본 공격 성공 가능성은 14~19 사이의 취약성 등급을 의미한다. 즉, CC v3.1이 보다 깊은 수준의 취약성 분석을 요구하고 있다.

3.5. 비교 및 분석 결과

앞서 살펴본 바와 같이 CC v3.1은 CC v2.3에 비해 전체적으로 높은 수준의 보증요구사항을 포함하고 있다. 이는 EAL4 등급에서만 나타나는 현상이 아니라 CC v3.1의 보증요구사항이 전체적으로 CC v2.3에 비해 강화되었기 때문이다. 예를 들어 TDS 패밀리와 AVA 패밀리의 경우 전체적으로 보증요구사항이 좀 더 상세한 수준의 제출물을 요구하는 형태로 조정되었다.

즉, CC v3.1의 EAL4 등급은 CC v2.3의 EAL4 등급에 상응하는 혹은 보다 높은 수준의 보증요구사항을 포함하고 있으며, 보증요구사항에 미묘한 차이는 있으나 CC v2.3과 CC v3.1의 EAL4 등급을 동등한 수준으로 대응하는 것에는 큰 무리가 없다. 왜냐하면 강화된 보증요구사항은 CC v3.1의 기조에 의한 것으로 EAL4에서만 나타나는 특성이 아니고, 이를 제외하면 대부분 동등한 수준의 보증을 요구하고 있기 때문이다.

Ⅳ. PP 소개, 보안문제정의, 보안목적 변경사항 도출

4.1. 보호프로파일 소개 변경사항

보호프로파일 소개의 변경사항은 [표 3]과 같다.

〔표 3〕 CC v3.1의 보호프로파일 소개

CC v2.3	CC v3.1
1. 보호프로파일 소개 - 보호프로파일 식별 - 보호프로파일 개 2. TOE 설명	1. 보호프로파일 소개 - 보호프로파일 참조 - TOE 개요

CC v3.1은 CC v2.3의 1장 보호프로파일 소개와 2장 TOE 식별을 통합하여 1장 보호프로파일 소개를 서술한다. TOE 개요는 CC v3.1에 의거, 비-TOE 및 TOE에 포함된 하드웨어, 소프트웨어 및 펌웨어를 모두 식별해야 한다. 보호프로파일은 운영환경에 대한 설명을 구체적으로 기술하지는 않는다. 왜냐하면 보호프로파일은 특정 제품에 대한 운영환경을 다루는 것이 아니기 때문에, 운영환경은 가변적이며 보안목표명세서 개발자가 구체적으로 서술할 수 있다.

4.2. 보안문제정의 변경사항

기존 TOE 보안환경이 CC v3.1에서 보안문제정의로 명칭이 변경되었다. 그리고 서술의 순서도 가정사항, 위협, 조직의 보안정책에서 위협, 조직의 보안정책, 가정사항으로 변경되었다.

〔표 4〕 CC v3.1의 보안문제정의

CC v2.3	CC v3.1
3. TOE 운영환경 - 가정사항 - 위협 - 조직의 보안정책	3. 보안문제정의 - 위협 - 조직의 보안정책 - 가정사항

CC v3.1은 CC v2.3보다 상세한 수준의 위협, 조직의 보안정책, 가정사항을 서술할 것을 요구하며, 그 외 눈에 띄는 변경사항은 없다. 본 과제는 CC v3.1 기반 보호프로파일을 개발함에 있어 위협을 위협원, 자산, 공격방법으로 구분하여 서술하였다.

특이사항으로는 CC 2부의 FPT_RVM.1, FPT_SEP.1이 CC v3.1에서는 삭제되었는데, 기존 두 컴포넌트와 연관된 보안문제정의로는 T.우회접근과 O.자체기능보호가 있다. 삭제된 두 컴포넌트는 보안과 관련된 개념이 완전히 배제된 것이 아니라, 보증요구사항에서 이를 대체하므로, 본 과제는 CC v3.1 기반에서 T.우회접근과 O.자체기능보호를 삭제하고, 보안목적의 이론적 근거를 일관성 있게 수행하는 방향으로 과제를 진행한다.

4.3. 보안목적 변경사항

CC v3.1 기반 보호프로파일은 이론적 근거 장이 삭제되고 보안목적과 보안요구사항의 장 뒤에 각각 보안목적의 이론적 근거와 보안기능요구사항, 보증요구사항의 이론적 근거를 포함한다. 또, IT 환경에 대한 보안요구사항이 완전히 삭제됨으로써, 환경에 대한 언급은 운영환경에 대한 보안목적에서 마무리를 짓는다.

〔표 5〕 CC v3.1의 보안목적

CC v2.3	CC v3.1
4. 보안목적 - TOE 보안목적 - IT 환경에 대한 보안목적	4. 보안목적 - TOE 보안목적 - 운영환경에 대한 보안목적

IT 환경에 대한 보안요구사항이 삭제되면서 이를 보완하기 위해 운영환경에 대한 보안목적을 보다 상세히 기술하였다. 또, CC v3.1이 TOE와 운영환경을 엄격히 구분하기 때문에, IT 환경에 대한 보안요구사항과 관련된 보안요구사항을 삭제하면서 상세한 설명이 부족하다 판단되는 경우 부록을 통해 요구사항을 권고하는 방향으로 개정을 진행한다.

V. PP 준수 방법 도출

앞 장에서 기술하였듯이 CC v3.1의 보호프로파일에는 보호프로파일/보안목표명세서에서 요구되는 해당 보호프로파일 준수 방법을 서술해야 한다. 준수 방법은 '엄격한 준수'와 '입증 가능한 준수'로 나뉜다. 보호프로파일의 준수 방법을 결정하기 위해 각 준수 방법에 대한 요구사항 분석이 필요하다. 즉, 보안목표명세서가 보호프로파일을 각 준수 방법에 따라 준수하기 위해 만족해야 할 사항들을 분석해야 한다. 또한 기존의 보안목표명세서가 보호프로파일에 대해 '보안문제정의'와 '보안목적', '보안요구사항'을 준수하는 정도를 파악하여 적절한 준수 방법을 결정하기 위한 근거로 사용해야 한다.

5.1. 준수 방법의 요구사항 분석

보호프로파일에 명시할 준수 방법을 결정하기 위해 CC v3.1에서 처음으로 도입된 '엄격한 준수'와 '입증 가능한 준수' 방법의 보안목표명세서에 대한 요구사항을 분석하였다.

5.1.1. 엄격한 준수

'엄격한 준수'는 보안목표명세서가 보호프로파일 내에 있는 모든 서술문을 포함해야 하며, 별도의 서술을 포함할 수도 있다고 정의될 수 있다. '엄격한 준수'에서 보안목표명세서는 보호프로파일을 실체화한 것으로 보호프로파일보다 광범위할 수 있다. 따라서 보안목표명세서는 보호프로파일을 TOE에 대해서는 최소한으로, 운영환경에 대해서는 최대한으로 명세할 수 있다. '엄격한 준수'의 적용은 정해진 한 가지 방법으로 준수되어야 하는 엄격한 요구사항을 필요로 하는 상황에 적합하다. 보호프로파일에 대한 보안목표명세서의 '엄격한 준수' 요구사항은 다음과 같다.

(1) 보안문제정의
- 보호프로파일의 '보안문제정의'를 포함
- 보호프로파일의 '보안문제정의'에서 추가적인 위협 및 조직의 보안정책 명세 가능
- 보호프로파일의 '보안문제정의'에서 추가적인 가정사항 명세는 불가

(2) 보안목적
- 보호프로파일의 'TOE 보안목적'을 모두 포함
- 추가적인 'TOE 보안목적' 명세 가능
- 보호프로파일의 '운영환경에 대한 보안목적'이 보안목표명세서의 'TOE 보안목적'이 될 수 있음

(3) 보안요구사항
- 보호프로파일의 '보안기능요구사항'을 모두 포함
- 추가적인 또는 계층적으로 더 강력한 '보안기능요구사항' 및 '보증요구사항' 명세 가능
- 오퍼레이션은 보호프로파일과 같거나 더 제한적인

형태로 명세

5.1.2. 입증 가능한 준수

'입증 가능한 준수'는 보안목표명세서가 보호프로파일과 동등하거나 더 제한적이어야 한다. '입증 가능한 준수'를 요구하는 보호프로파일은 일반적인 보안문제에 대해 해결책이 한 가지 이상의 방법이 있다는 것을 전제로 그 해결에 필요한 요구사항을 포괄적으로 서술한다. 따라서 보안목표명세서가 몇몇 존재하는 비슷한 보호프로파일을 준수하기 위한 경우에 '입증 가능한 준수'를 적용하는 것이 적합하다. 보호프로파일에 대한 보안목표명세서의 '입증 가능한 준수' 요구사항은 다음과 같다.

(1) 보안문제정의
- 보호프로파일의 '보안문제정의'와 동등하거나 더 제한적
- 보안목표명세서의 '보안문제정의'는 보호프로파일의 '보안문제정의'를 만족시킴

(2) 보안목적
- 보호프로파일의 '보안목적'과 동등하거나 더 제한적
- 보안목표명세서의 TOE와 운영환경에 대한 '보안목적'은 보호프로파일의 TOE와 운영환경에 대한 '보안목적'을 만족시킴

(3) 보안기능요구사항
- 보호프로파일의 '보안기능요구사항'과 동등하거나 더 제한적
- 보안목표명세서의 '보안기능요구사항'은 보호프로파일의 '보안기능요구사항'을 만족시킴

(4) 보증요구사항
- 보호프로파일의 '보증요구사항'을 모두 포함
- 추가적인 또는 계층적으로 더 강력한 '보증요구사항' 명세 가능
- 오퍼레이션은 보호프로파일과 같거나 더 제한적인 형태로 명세

5.2. 준수방법 결정 방법

기존의 보호프로파일을 준수하는 보안목표명세서를 분석한 결과 가정사항과 환경에 대한 보안목적, 보안기능요구사항을 추가적으로 명세한 보안목표명세서가 많았다. 이를 통해 기존의 보호프로파일을 준수한 보안목표명세서가 '입증 가능한 준수' 방법을 적용하는 것이 적절하다는 결론을 내릴 수 있다. 또한 12종의 보호프로파일은 정해진 한 가지 방법으로 준수될 수도 있지만, 동시에 여러 보호프로파일들이 준수 가능하기 때문에 '입증 가능한 준수' 방법이 12종의 보호프로파일에 적합하다.

Ⅵ. 확장 컴포넌트의 정의 서술

CC v3.1의 보호프로파일에서는 보안요구사항에서 CC 2부 또는 3부에 기초하지 않은 요구사항에 대해 새로운 컴포넌트를 정의하도록 되어있다. 새로운 컴포넌트는 보호프로파일의 '확장 컴포넌트의 정의' 절에서 정의해야 한다. 확장 컴포넌트에 기반하는 확장 요구사항은 '확장 컴포넌트의 정의' 절이 아닌, '보안요구사항' 절에 포함되어야 한다.

6.1. 확장 컴포넌트의 사용

확장 컴포넌트는 다음과 같은 경우에만 허용될 수 있다.
- CC 2부의 보안기능요구사항으로 표현될 수 없는 TOE 보안목적
- CC 3부의 보증요구사항으로 표현될 수 없는 개발환경에 대한 보안목적
- 보안목적이 2부 및/또는 3부에 근거하여 표현될 수 있지만, 매우 난해하거나 복잡한 경우

확장 컴포넌트가 '확장 컴포넌트의 정의' 절에서 정확하게 정의되면 그에 근거하는 하나 이상의 보안요구사항을 설정해야 한다. '확장 컴포넌트의 정의' 절에 새롭게 정의된 컴포넌트는 CC 2부 또는 3부에서 제공되는 보안요구사항처럼 사용될 수 있다. 사용되는 확장 요구사항은 CC 2부 또는 3부에 기초하는 다른 요구사항들과 같은 목적을 가져야 한다.

확장 컴포넌트는 기존 CC의 컴포넌트와 유사한 형태로 정의 되어야 한다. 즉, 명확하고 모호하지 않게 평가 가능한 형태이어야 한다. 따라서 확장 컴포넌트는 기존의 CC 컴포넌트와 유사한 레이블, 표현 방식, 상세 수준을 갖추어야 한다. 종속관계는 기존의 CC 컴포넌트들의 종속관계에 기반하여 확장 컴포넌트 정의에 포함

되어야 한다. 확장 컴포넌트가 오퍼레이션을 사용하는 경우에는 CC 1부 부록 C.4의 '오퍼레이션'과 일관성 있게 사용해야 한다.

확장 기능 컴포넌트는 CC 2부의 컴포넌트와 유사한 형태로 적용 가능한 감사 및 관련 오퍼레이션 정보를 포함해야 한다. 확장 보증 컴포넌트는 공통평가방법론에 제시된 것과 유사한 형태로 해당 컴포넌트에 대한 방법론을 제시해야 한다.

확장 컴포넌트가 기존의 패밀리에 적합할 경우, 기존의 패밀리에 포함되어 정의 될 수 있다. 이러한 경우 변경된 기존의 패밀리를 서술해야 한다. 확장 컴포넌트가 기존의 패밀리에 적합하지 않은 경우에는 새로운 패밀리를 정의하여 확장 컴포넌트가 포함되도록 해야 한다.

새로운 패밀리가 기존의 클래스에 적합할 경우, 기존의 클래스에 포함될 수 있다. 이러한 경우 변경된 기존의 클래스를 서술해야 한다. 새로운 패밀리가 기존의 클래스에 적합하지 않은 경우에는 새로운 클래스를 정의하여 새로운 패밀리가 포함되도록 해야 한다.

새로운 패밀리나 클래스는 기존의 CC의 패밀리나 클래스와 유사한 형태로 정의되어야 한다.

Ⅶ. 보안요구사항 도출

CC 2부 보안기능요구사항에 대한 CC v3.1과 CC v2.3의 차이점은 CC v2.3의 'FPT_RVM 참조 모니터에 의한 중재'와 'FPT_SEP 영역분리'가 CC v3.1에서는 보안기능요구사항에서 삭제되고, 그 개념은 CC 3부 보증요구사항의 'ADV_ARC 보안 구조'에서 다루고 있다.

CC 3부 보증요구사항은 CC v3.1로 개정되면서 많은 사항들이 변경되었다. 특히 개발 평가(ADV)에 많은 변경사항이 나타났다. '우회불가성', '영역 분리', '자체 보호' 기능을 다루는 보안 구조(ADV_ARC)가 추가되고, 상세설계(ADV_LLD)와 기본설계(ADV_HLD) 개념이 TOE 설계(ADV_TDS)로 결합되었다. 또한 표현의 일치성(ADV_RCR)은 CC v3.1에서 삭제되었다. 이외에도 기존의 개념들이 변경되거나, 결합, 추가, 삭제되었다.

CC v3.1의 2부와 3부의 변경 사항들에 대한 분석을 통해 CC v2.3 기반의 보호프로파일의 보안요구사항을 CC v3.1에 적합하도록 변경해야 한다.

7.1. 보안기능요구사항

보안기능요구사항은 CC v3.1의 요구사항에 맞게 기존의 보호프로파일에서 'FPT_RVM 참조 모니터에 의한 중재'와 'FPT_SEP 영역분리'를 모두 삭제해야 하며, 'FAU_STG.1'의 레이블은 '감사 증적 보호'에서 '감사 증적 저장소 보호'로 변경한다. 이 외에 각 컴포넌트에서 정의한 요구사항은 표현한 단어 상의 차이점 외에 의미상의 차이점이 없기 때문에 기존의 컴포넌트를 동일하게 사용할 수 있다.

'FAU_SAR 보안감사 검토'와 'FAU_STG 보안감사 사건 저장', 'FPT_AMT 하부 추상기계 시험', 'FPT_ITC 외부전송 TSF 데이터의 비밀성', 'FPT_STM 타임스탬프'에 대한 기능은 주로 운영환경에서 지원받고 있다. 따라서 해당 요구사항의 '응용 시 주의사항'에 TOE에서 완전히 구현할 수 없는 경우, 운영환경에서 지원받을 수 있음을 서술해야 한다.

CC v2.3 보호프로파일의 'IT 환경에 대한 보안기능요구사항'은 CC v3.1 보호프로파일에서 삭제되었지만, 해당 보안기능요구사항이 TOE의 운영에 필요하기 때문에 분석을 통해 반영 여부를 결정해야 한다. 기존의 'IT 환경에 대한 보안기능요구사항'의 기능이 TOE에서 구현 가능할 경우 '보안기능요구사항'에 추가하고, '응용 시 주의사항'에 TOE에서 완전히 구현할 수 없는 경우, 운영환경에서 지원 받을 수 있음을 서술하는 것으로써 반영될 수 있다. TOE에서 구현할 수 없는 기능은 '보안문제 정의'의 '가정사항'으로 서술함으로써 반영될 수 있다.

보안기능요구사항으로 확장 컴포넌트를 사용할 경우, '확장 컴포넌트 정의' 절에 정의된 확장 컴포넌트에 적절한 오퍼레이션을 적용하여 보안기능요구사항으로 명시한다. 확장 컴포넌트의 사용은 기존의 CC 2부 보안기능요구사항의 컴포넌트를 적용하는 방법과 동일한 방법을 사용해야 한다.

7.2. 보증요구사항

CC v3.1의 3부 보증요구사항은 모든 컴포넌트에 대해 변경되었기 때문에 각 컴포넌트에 따른 변경 사항의 분석을 통해 기존의 보증요구사항에 대응되는 적절한 컴포넌트를 결정해야 한다.

'추가'가 적용되지 않은 평가보증등급에 대해서는 유사한 수준의 신뢰도 수준을 보장하기 위해 동일한 평가보증등급을 적용하는 것이 적합하다. 이러한 경우 CC v3.1에서 정의된 보증패키지에 따라 보증요구사항을 적용할 수 있다.

'추가'가 적용된 평가보증등급에 대해서는 '추가'된 보증요구사항을 분석해야 한다. '추가'된 보증요구사항에 대응되는 보증 컴포넌트가 존재 할 경우 해당 보증 컴포넌트를 반영한다. 만약, 해당 보증 컴포넌트가 지나치게 높은 보증 수준을 요구한다면 평가보증등급에 대한 적절한 조정이 필요하다. 평가보증등급에 대한 조정은 평가에 소요되는 비용과 전체적인 보증 수준, TOE의 특징을 통해 이루어져야 하며, '제 2 절 평가보증등급 변경사항 도출'의 평가보증등급과 보증 컴포넌트의 분석을 이용할 수 있다.

Ⅷ. 결 론

2006년 9월 CC v3.1이 공식 평가 기준이 되면서 우리나라 국제상호인정협정(CCRA) 결정사항에 따라 정보보호제품 평가·인증 신청제품에 대한 CC v3.1 적용에 대비하여 기존 CC v2.3과 CC v3.1의 개정이 필요한 시점이다. 또한 2009년 9월부터는 기존의 CC v2.3을 완전히 대체 할 것으로 예상됨에 따라 개정을 위한 분석이 더욱 시급하다. 따라서 본 논문에서는 CC v2.3에서 CC v3.1로의 개정을 위한 CC v3.1의 변경사항을 비교 및 분석하였다. CC v3.1 보안기능 및 보증요구사항의 평가 업무량 및 제출물 작성수준 분석하기 위해 평가보증등급 변경사항, PP 소개, 보안문제 정의, 보안목적, PP 준수 방법 등의 변경사항을 분석하여 개정사항을 도출하였다.

본 분석을 통하여 기존 보호프로파일 및 보안목표명세서 개정 시 활용 가능하고, 또한 향후 CC v3.1 적용 시 새로운 보호프로파일 및 보안목표명세서 개발과 평가 시 활용이 용의할 것으로 예상된다.

참고문헌

[1] 정보보호시스템 공통평가기준, 정보통신부 고시 2005-25호, 2005. 5. 21

[2] 정보보호시스템 평가·인증 지침, 정보통신부 고시 2007-31호, 2007. 8. 22

[3] 보호프로파일 및 보안목표명세서 작성법, 정보통신단체표준 TTAR-0011, 한국정보보호진흥원, 2002. 12. 11

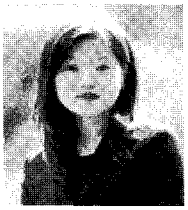
[4] Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB, 2006. 9.

[5] Common Methodology for Information Technology Security Evaluation, Version 3.1, CCMB, 2006. 9.

[6] Common Criteria for Information Technology Security Evaluation, Version 2.3, CCMB, 2005. 8.

[7] Common Methodology for Information Technology Security Evaluation, Version 2.3, CCMB, 2005. 8.

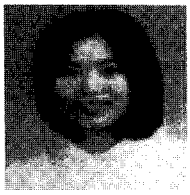
〈著者紹介〉



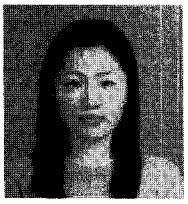
조 혜 숙(Hea-suk Jo)
학생회원
2003년 2월 : 한성대학교 멀티미디어정보처리과 학사 졸업.
2005년 2월 : 성균관대학교 전자전기컴퓨터공학부 석사 졸업.
2006년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 박사과정
<관심분야> 정보보호, 보안성평가, 무선네트워크

전 웅 렬(Woong-ryul Jeon)
정회원
2006년 2월 : 성균관대학교 컴퓨터공학과 졸업
2006년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 보안성평가, 데이터베이스 보안

정 한 재(Han-jae Jeong)
정회원
2006년 2월 : 성균관대학교 컴퓨터공학과 졸업
2006년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 정보보호, 보안성평가, 무선네트워크

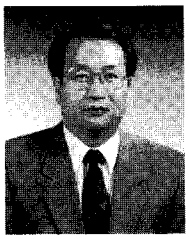


이 성 진(Sung-jin Lee)
학생회원
2007년 2월 : 성균관대학교 정보통신공학부 졸업
2007년 3월 ~ 현재 : 성균관대학교 휴대폰학과 석사과정
<관심분야> 정보보호, 모바일 통신 보안, 보안성평가



유 연 정(Yeon-jung Yu)
2000년 2월 : 서울시립대 전산통계학과 졸업
2000년 2월~현재 : 한국정보보호진흥원 평가기획팀 주임연구원
<관심분야> 정보보증, 소프트웨어 공학

김 승 주 (Seung-joo Kim)
종신회원
1994년 2월~1999년 2월 : 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월~현재 : 성균관대학교 정보통신공학부 교수
2001년 1월~현재 : 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 6월~현재 : 교육인적자원부 유해정보차단 자문위원
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET



원 동 호 (Dong-ho Won)
종신회원
1976년~1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~2003년 : 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재: 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장
<관심분야> 암호이론, 정보이론, 정보보호