情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

CC 평가인증 문서 작성법

이완석*, 유연정**

요 약

공통평가기준 기반으로 정보보호제품 평가를 수행하기 위해 개발자는 해당 평가보증등급에서 요구하는 평가제출물을 작성해야 한다. 본 고에서는 개발자가 실제적으로 평가제출물을 작성하는데 참조할 수 있도록 CC에서 요구되는 평가제출물을 살펴보고, 간략하게 CC V2.3과 CC V3.1간의 평가제출물 차이점을 제시하고자 한다.

Ⅰ. 서 론

공통평가기준(CC, Common Criteria)을 기반으로 정보보호제품을 개발 및 평가할 때, 개발자는 보안목표명세서(ST, Security Target)와 더불어 CC에서 평가보증등급별로 요구하는 보증요구사항을 문서화하여 평가자에게 제출하여야 하고, 평가자는 이를 기반으로 평가대상(TOE, Target of Evaluation)에 대한 평가를 수행하게 된다. 개발자는 평가대상 제품 개발이 완료된 후에 평가제출물을 작성할 수도 있고, 또는 평가대상 제품의 개발과 병행하여 평가제출물을 작성할 수도 있다.

평가제출물은 TOE의 형상을 표현하며, 개발자와 평가자간의 공식적인 대화수단으로, 규정화되고, 최적의 양식과 내용을 필요로 한다. 하지만, CC는 특정 개발방법론이나 생명주기 모델을 따르도록 강요하지 않는다. 이는 개발자에게 유연성을 제공하지만, 평가제출물에 대한 구체적인 작성방법을 제공하지 않기 때문에 많은 어려움을 야기하기도 한다.

본 고에서는 개발자가 실제적으로 평가제출물을 작성하는데 참조할 수 있도록 CC에서 요구되는 평가제출물을 살펴보고, 간략하게 CC V2.3과 CC V3.1간의 평가제출물 차이점을 제시하고자 한다. 그리고 마지막으로 결론을 정리한다.

Ⅱ. CC 기반의 평가제출물

CC의 평가보증등급은 해당 보증등급 획득 가능성 및 비용의 균형을 고려해서 EAL1~EAL7으로 구성된다. 각 평가보증등급은 모든 하위의 평가보증등급보다 더 높은 보증을 표현하고 있으므로, 계층적으로 순서화되어있다. EAL1 등급에서 EAL4 등급까지는 일반적으로 기존에 사용하고 있는 제품과 시스템을 재정비하기 위한 관점에서 적용될 수 있으며, EAL5 이상의 등급은 위험 수준 및 자산의 가치가 높은 상황에서 사용하기 위한 TOE 개발에 적용 가능하다.

보증요구사항은 정보보호제품의 보안기능에 대한 신뢰성을 보증하기 위해 9개의 클래스로 표현된다. 이는 보호프로파일 평가(APE), 보안목표명세서 평가(ASE), 형상관리(ACM), 배포 및 운영(ADO), 개발(ADV), 설명서(AGD), 생명주기지원(ALC), 시험서(ATE), 취약성 평가(AVA)에 대한 요구사항이다. 보호프로파일 평가(APE), 보안목표명세서 평가(ASE)를 제외한 각 보증요구사항이, 평가보증등급별로 패키지화 되어 있다.

개발자는 해당 평가보증등급에서 요구하는 보증요구사항을 충족시키도록 평가제출물을 작성하여야 한다. 공통평가기준을 기반으로 EAL4 평가보증등급에서 요구되는 평가제출물은 일반적으로 다음 [표 1]과 같다.

2.1. 보안목표명세서(ST)

ST는 보호프로파일 또는 패키지에 근거해서 작성되거나, 다른 문서에 근거하지 않고 독립적으로 작성될

* 한국정보보호진흥원 IT기반보호단 U-IT서비스보호팀(wsyi@kisa.or.kr)
** 한국정보보호진흥원 보안성평가단 평가기획팀(yjyu@kisa.or.kr)

〔표 1〕 EAL4 평가제출물

평가제출물		기여도
제품 규격	보안목표 명세서	사용자에게 정확하고 완전한 제품규격을 제공하며, 제품 선택 시 기초 자료로 사용
문서 증거	형상관리 문서	개발자가 제품 개발에 필요한 ST, 문서증거, 소스코드 등의 버전관리 및 변경통제를 효율적으로 수행하기 위한 도구 및 절차에 대한 지침 제공
	설치지침서	사용자에게 안전한 방식으로 제품을 설치하는 지침 제공
	배포문서	사용자가 개발자로부터 제품 수령 시 배송 단계에서 제품이 훼손되지 않았음을 보장
	기능명세서	제품기능 사용수단인 외부 인터페이스 분석을 통해 제품규격에 따라 개발자가 효율적으로 제품 설계를 관리할 수 있는 개발 방법 제공
	기본설계서	복잡한 기능설계를 논리적으로 단순화하여 표현한 기본설계 분석을 통해 개발자가 안전하고 견고하게 제품을 설계할 수 있는 개발 방법 제공
	상세설계서	구현 가능한 수준으로 기능을 표현한 상세설계 분석을 통해 개발자가 실제 안전하고 견고한 제품 개발에 사용할 수 있는 설계문서 제공
	구현검증 명세서	상세설계와 정확하게 일치하도록 제품을 개발했는지 개발자가 소스코드/하드웨어도면 등을 분석하는 방법 제공
	보안정책 모델명세서	보안정책에 따라 제품기능을 설계했는지 개발자가 분석하기 위한 가이드 제공
	관리자 설명서	관리자 역할을 수행하는 사용자에게 정확하고 명료한 제품 관리기능 사용방법 제공
	사용자 설명서	일반 사용자에게 정확하고 명료한 일반기능 사용방법 제공
	생명주기 지원서	개발자가 생명주기에 따라 제품을 생산·관리하기 위한 지침 및 개발환경의 물리적·인적·절차적 보안대책 수립을 위한 지침, 제품 개발에 사용된 도구의 신뢰성을 검토할 수 있는 지침 제공
제품	시험서	개발자가 제품규격에 맞게 제품이 구현되었음을 확인하기 위한 제품 기능시험 수행 방법 제공
	오용분석서	개발자가 제품오용으로 인한 취약점 내재 가능성을 조사하는 방법 제공
	취약성 분석서	개발자가 제품에 취약성이 존재하는지 분석하고 침투시험 하는 방법 제공

수 있다. ST는 평가이전과 평가 과정 중에는 개발자와 평가자간에 합의를 이끌어 내기 위해, TOE의 보안특성과 평가 범위에 대한 기술적인 정확성 및 완전성이 중점사항이 되며, 평가 완료 후에는 개발자 또는 판매자와 소비자 간에 사용되므로, ST의 이해 가능성을 높이는 것이 중점사항이 된다. 그러므로 ST는 이해 가능성이 용이해야 하며, 기술적인 정확성 및 완전성을 모두 고려해서 작성되어야 한다.

ST에 포함되어야 하는 필수 구성요소는 다음과 같다.

- ST 소개 : ST 및 TOE에 관한 목적, 주요 보안특성 등 서술적인 설명문을 포함한다.
- 보안환경 : TOE 및 운영환경에 의해 대응되어야 하는 위협, 조직의 보안정책, 가정 사항을 서술한다.
- 보안목적 : 보안환경에서 정의된 보안문제의 해결책이 어떻게 TOE 및 운영환경에서 다루어지는지 서술적으로 기술한다.
- 보안요구사항 : TOE 보안목적이 만족될 수 있도록 CC 2부, 3부에 기반해서 보안기능요구사항(SFR), 보증요구사항(SAR) 형태로 표현한다.
- TOE 요약명세 : SFR이 TOE에서 어떻게 구현되는지 서술한다.

2.2. 형상관리문서

TOE 및 관련 정보를 세분화하고 변경하는 과정에서 규칙적이고 체계적인 관리를 통해 TOE의 무결성이 유지됨을 보장하기 위한 문서로, 형상관리(ACM) 클래스의 형상관리 자동화(ACM_AUT)와 형상관리 능력(ACM_CAP), 형상관리 범위(ACM_SCP)로 구성된다. 형상관리문서는 TOE 버전과 레이블, 형상항목 식별 방법, 형상항목, 형상관리 계획, TOE 구현표현의 자동화된 접근통제 수단과 자동화된 TOE 생성수단 등을 서술하여야 한다.

2.3. 설치지침서

개발자가 의도한 안전한 방식으로 TOE가 설치, 생성, 시동되고 있음을 보장하기 위한 문서로, 배포 및 운영(ADO) 클래스의 설치, 생성, 시동(ADO_IGS) 요구사항을 포함한다. 설치지침서는 TOE의 안전한 설치, 생성, 시동 절차와 단계 등을 서술하여야 한다. 설치지

침서는 독립된 문서로 존재하거나, 관리자 설명서의 일부로 존재할 수도 있다. 그러나, 설치지침서는 자주 사용되지 않고 일회적으로 사용된다는 점에서 관리자 설명서(AGD_ADM)의 요구사항과 차이가 있다.

2.4. 배포문서

TOE를 사용자에게 배포하는 과정에 다양한 보안위협 요소가 존재할 수 있으므로, TOE가 사용자에게 배포되는 동안에 보안성이 유지됨을 보장하기 위한 문서로, 배포 및 운영(ADO) 클래스의 배포(ADO_DEL) 요구사항을 포함한다. 배포문서는 배포 방법 및 절차, 전송시 보안유지 절차 등을 서술하여야 한다.

2.5. 기능명세서

TOE에 의해 제공되는 모든 보안기능과 외부인터페이스를 서술함으로써, 보안목표명세서에 서술된 모든 보안기능요구사항이 TOE에 의해 실체화됨을 보장하기 위한 문서로, 개발(ADV) 클래스 기능명세(ADV_ FSP) 요구사항을 포함한다. 기능명세서는 TOE 보안기능, 외부 인터페이스를 서술하고, 보안목표명세서의 TOE 요약명세에 서술된 모든 보안기능과 기능명세서의 보안기능 간의 완전함을 보증해야 한다.

2.6. 기본설계서

사용자의 요구사항에 적합한 TOE를 개발하기 위한 중요한 단계로, TOE 보안기능을 TOE 보안기능의 주요 구성성분(예, 서브시스템)으로 세분화하여 서술하는 최상위 수준의 설계문서로, 기본설계(ADV_HLD) 요구사항을 포함한다. 기본설계서는 보안 서브시스템, 기타 서브시스템, 인터페이스를 서술하고, 기능명세서의 보안기능과 기본설계서의 서브시스템간의 완전함을 보증해야 한다.

2.7. 상세설계서

기본설계를 프로그래밍이나 하드웨어 구축 시 사용할 수 있도록 상세한 수준(예, 모듈수준)으로 세분화하는 설계 문서로, 상세설계(ADV_LLD) 요구사항을 포함한다. 상세설계서는 보안 모듈, 기타 모듈, 인터페이스를 서술하고, 기본설계서의 서브시스템과 상세설계서의 모듈간의 완전함을 보증해야 한다.

2.8. 구현검증명세서

구현표현이 보안목표명세서의 보안기능요구사항들을 만족하기에 충분하고, 상세설계의 정확한 실체임을 보장하기 위한 문서로, 구현표현(ADV_IMP) 요구사항을 포함한다. 구현검증명세서는 구현표현의 일부분을 서술하고, 상세설계서의 모듈과 구현검증명세서의 구현표현 간의 완전함을 보증해야 한다.

2.9. 보안정책모델명세서

TOE 보안정책에 기반한 보안정책모델을 개발하여 기능명세, 보안정책모델간의 일치성을 입증함으로써, 기능명세의 보안기능이 TOE 보안정책을 수행함을 추가적으로 보증하기 위한 문서로, 보안정책모델(ADV_ SPM) 요구사항을 포함한다. 보안정책모델명세서는 보안정책모델을 서술하고, 기능명세서의 모든 보안기능과 보안정책모델명세서의 보안정책 모델간의 완전함을 서술하여야 한다.

2.10. 관리자설명서

TOE 보안을 위해 안전하고, 정확한 방식으로 TOE를 구성, 유지, 관리하는데 책임 있는 관리자에게 TOE의 안전한 운영을 보장하기 위한 문서로, 설명서(AGD) 클래스의 관리자 설명서(AGD_ADM) 요구사항을 포함한다. 관리자 설명서는 TOE의 안전한 운영을 위한 방법 및 절차 등을 서술하여야 한다.

2.11. 사용자설명서

관리자가 아닌 TOE 사용자 또는 TOE의 외부인터페이스를 사용하는 사용자에게 TOE의 안전한 사용을 보장하기 위한 문서로, 설명서(AGD) 클래스의 사용자 설명서(AGD_USR) 요구사항을 포함한다. 사용자 설명서는 TOE의 안전한 운영을 위한 방법 및 절차 등을 서술하여야 한다.

2.12. 생명주기지원서

TOE 개발 및 유지하는 동안에 TOE에 대한 규칙 및 통제를 수립하여 TOE의 보안성을 보장하기 위한 문서로, 생명주기지원(ALC) 클래스의 개발보안(ALC_DVS)과 생명주기 정의(ALC_LCD) 컴포넌트, 도구와 기법(ALC_TAT) 요구사항을 포함한다. 생명주기지원서는 물리적 · 절차적 · 인적 · 기타 보안대책, 생명주기 정의, 잘 정의된 개발도구를 서술하여야 한다.

2.13. 시험서

명세된 TOE 보안기능요구사항과 서브시스템 및 모듈을 그 명세에 따라 시험함으로써, TOE가 최소한의 보안기능요구사항과 적절한 TOE 내부구조를 만족함을 보장하기 위한 문서로, 시험(ATE) 클래스의 범위(ATE_COV), 상세수준(ATE_DPT), 기능시험(ATE_FUN) 요구사항을 포함한다. 시험서는 시험계획, 시험절차, 시험결과, 시험분석을 서술하여야 한다.

2.14. 오용분석서

TOE가 안전하지 않은 방식으로 구성되거나, 사용되었음에도 TOE 관리자나 사용자가 타당한 이유로 TOE가 안전하다고 믿을 수 있는 부분, 즉 오용가능한 부분이 설명서에 없음을 보장하기 위한 문서로, 취약성 평가(AVA) 클래스의 오용(AVA_MSU) 요구사항을 포함한다. 오용분석서는 관리자설명서의 오용가능성 분석, 사용자설명서의 오용가능성 분석을 서술하여야 한다.

2.15. 취약성분석서

확률 메커니즘과 순열 메커니즘에 의해 구현된 TOE 보안기능의 강도가 선언된 일정수준이나 허용정도를 만족함을 보장하고, 식별된 보안 취약성이 TOE의 예상된 환경 내에서 악용될 수 없음을 보장하고, TOE가 명백한 침투공격에 내성이 있음을 보장하기 위한 문서로, TOE 보안기능강도(AVA_SOF), 취약성 분석(AVA_VLA) 요구사항을 포함한다. 취약성분석서는 TOE 보안기능강도 분석, 개발자에 의한 취약성 분석을 서술하여야 한다.

〔표 2〕 CC V2.3-V3.1 EAL4 요구사항 비교

보증 클래스	CC 2.3	CC 3.1	비고
개발		ADV_ARC.1	추가
	ADV_FSP.2	ADV_FSP.4	
	ADV_HLD.2	ADV_TDS.3	통합
	ADV_LLD.1		
	ADV_IMP.1	ADV_IMP.1	
	ADV_RCR.1	-	각 컴포넌트에 통합
	ADV_SPM.1	-	삭제
설명서 (배포 및 운영 포함)	AGD_ADM.1	AGD_OPE.1	통합
	AGD_USR.1		
	ADO_IGS.1	AGD_PRE.1	
생명주기 지원 (배포 및 운영, 형상관리 포함)	ADO_DEL.2	ALC_DEL.1	
	ACM_AUT.1	ALC_CMC.4	통합
	ACM_CAP.4		
	ACM_SCP.2	ALC_CMS.4	
	ALC_DVS.1	ALC_DVS.1	
	ALC_TAT.1	ALC_TAT.1	
	ALC_LCD.1	ALC_LCD.1	
시험	ATE_COV.2	ATE_COV.2	
	ATE_DPT.1	ATE_DPT.2	요구사항 강화 (모듈시험 요구)
	ATE_FUN.1	ATE_FUN.1	
	ATE_IND.2	ATE_IND.2	
취약성 평가	AVA_MSU.2	-	AGD_OPE로 이동
	AVA_SOF.1	-	AVA_VAN으로 이동
	AVA_VLA.2	AVA_VAN.3	공격 성공 가능성 변경 (낮음 →강화된-기본)

Ⅲ. CC V2.3과 V3.1의 평가제출물 차이점

CC V2.3과 CC V3.1에서 EAL4 요구사항 변경내용은 다음 [표 2]과 같다.

개발 클래스에서는 ADV_ARC.1이 추가됨에 따라 별도의 보안구조를 설명한 제출물이 요구되며, ADV_HLD와 ADV_LLD는 ADV_TDS로 통합되었으므로, 기본설계서, 상세설계서로 구분하던 것을 설계문서로 통합해서 제공할 수 있게 변경되었다. 또한, ADV_RCR은 삭제되고, 각 개발 패밀리에서 해당 요구사항을 수행하도록 변경되었으며, ADV_SPM.1은 삭제되어, 별도의 제출물을 제공하지 않아도 된다. 단, 보안정책모델은 EAL6 이상에서 정형화 명세를 요구하는 것으로 변경되었다.

설명서와 생명주기지원 클래스와 관련된 요구사항은

CC V2.3과 거의 유사하므로, 관련 제출물 작성에서도 거의 변경사항이 없다

시험 클래스에서는 시험의 상세수준과 관련된 요구사항 ATE_DPT 요구사항이 변경되어, CC V2.3에서는 기본설계에 대한 시험내용만 문서화 하였지만, CC V3.1에서는 SFR 수행과 관련된 모듈에 대한 시험내용까지 제출하도록 요구사항이 강화되었다.

취약성 평가 클래스에서는 AVA_MSU와 AVA_SOF를 삭제하고, 해당 내용은 설명서와 취약성 분석의 다른 컴포넌트를 통해서 수행하도록 변경되었다. 제출물 작성시 별도의 오용분석서를 제출하지 않아도 된다. 취약성 분석서에 기술하는 내용과 관련해서는 공격 성공 가능성이 낮음에서 강화된-기본으로 변경되었다

Ⅳ. 결 론

국내의 정보보호제품 개발 환경에서 개발 및 유지보수단계별로 도출될 수 있는 문서화에 대한 체계적 관리는 매우 취약한 실정이며, 제품 개발에 여념이 없는 업체에게 평가에 필요한 제출물 작성은 상당한 인력 및 시간, 비용 측면의 노력이 요구되므로 부담으로 작용할 수도 있다. 하지만, 신뢰성을 제공하지 못하는 제품은 결국 사용자로부터 선택받을 수 없게 되므로, 제품 평가는 필수적으로 요구된다고 할 수 있겠다.

본 고에서 제시된 CC 기반 15종의 평가제출물 작성을 통해 개발자는 기능명세, 기본설계, 상세설계 등 제품 개발 프로세스의 정확성을 보장하고, 운영 및 유지보수를 체계적으로 수행할 수 있게 된다. 또한 제품을 구성하는 모든 문서, 모듈, 개발 도구 등을 형상 관리함으로써 제품의 버전 관리 및 모든 변경을 효율적으로 통제할 수 있다. 이러한 방법을 통하여 최종 완제품에 포함될 수 있는 취약점이나 오류를 사전에 방지함으로써 완성도를 한층 더 높일 수 있게 된다.

결론적으로 평가제출물을 작성하고, CC 평가인증을 수행하는 것이 국내·외적으로 증가하고 있는 평가제품의 수요로 인하여 국내 시장은 물론 해외 시장을 선점하고 개척해 나갈 수 있을 뿐 아니라, 개발된 제품의 품질 및 안전성을 한층 더 향상시킴은 물론, 자체 개발 프로세스를 점검하고 개선할 수 있는 기회로 활용할 수 있을 것이다.

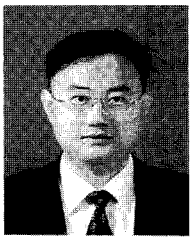
참고문헌

[1] "정보보호시스템 공통평가기준", 정보통신부 고시 2005-25호, 2005

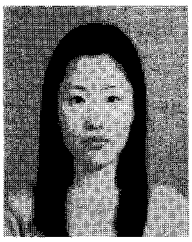
[2] "정보보호제품 평가제출물 작성가이드", 한국정보보호진흥원, 2005

[3] "Common Criteria for Information Technology Security Evaluation, Version 3.1", CCMB, 2006

〈著者紹介〉



이 완 석 (Wan S. Yi)
정회원
1991년 5월 : Va. Tech. 전산과학과 학사 졸업
2001년 2월 : 동국대학교 정보보호학과 석사 졸업
2004년 9월~현재 : 성균관대학교 전자공학과 박사과정
1996년 7월~현재 : 한국정보보호진흥원 u-IT서비스보호팀장
<관심분야> 정보보증, 주요정보통신 기반시설보호



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