CC기반 생명주기 지원 클래스 요구사항 분석에 관한 연구

신호준*O 김행곤* 김태훈** 김상호**
*대구가톨릭대학교 컴퓨터정보통신공학부, **한국정보보호진흥원 평가인증사업단
*{g98521002O, hangkon}@cuth.cataegu.ac.kr, **{taihoon, shkim}@kisa.or.kr

A study on the Requirement Analysis for Lifecycle based on Common Criteria

Ho-Jun Shin*O Haeng-Kon Kim* Tai-Hoon Kim** Sang-Ho Kim**
Dept. of Computer Information Communication, Catholic University of Daegu
IT Security Evaluation & Certification Authority, Korea Information Security Agency

요 약

웹 기반의 응용시스템 개발이 보편화되면서 보안은 특히 인터넷과 같은 네트워크 환경에서 정보처리에서 매우 중요한 요소로 대두되고 있다. 공통평가기준은 보안을 중요시하는 시스템의 평가를 위해서 표준화된 요구사항들의 목록이다. 공통평가기준을 사용하여 시스템 자체와 시스템 개발에 많은 보안 요구사항 정의는 가능하지만, 방법론 지원은 제공하지 않는다.

본 논문에서는 보안 클래스를 중심으로 소프트웨어공학 생명주기에서 보안측면을 분석하고 적용하는 방법을 제시한다. 공통평가기준에서의 행위와 문서는 개발된 시스템의 품질을 개선하며, 높은 보안 요구사항을 만족하기 위해 부가적 비용과 노력을 감소시키는 시스템 개발에서 가장 중요한 요소이다. 이를 기반하여 프로세스, 자원, 생명주기 분석 모델과 프레임워크를 정의하고 생명주기 지원 클래스의 적용에 대해서 논한다.

1. 서론

소프트웨어 개발과 응용 패러다임이 분산 환경을 두면서 보안 문제가 중요시되고 있다. 정보통신 제품이나 시스템을 개발할 경우 보안에 대한 평가를 위해서 표준화된 요구사항들의 목록으로 공통평가기준이 정의되어 있다. 공통평가기준을 사용하여, 시스템 자체와 시스템 개발에 많은 보안 요구사항을 정의 가능하지만, 공통평가기준으로 모든 개발에 대한 요구사항 분석이 힘들며, 구체적인 항목을 통한 방법 지원을 제공하지 않는다[1].

본 논문에서는 소프트웨어공학 생명주기동안의 프로세스에서 보안측면을 고려하여, 공통평가기준에서의 행위와 문서 등의 자원과 생명주기 지원을 위한 클래스의 적용 및 분석을 위한 방법으로 분석 모델과 프레임워크를 정의한다. 이는 생명주기 지원 클래스를 통한 개발과 평가를 지원하고, 개발자와 평가자에게 고려해야할 기준 이외에 생명주기상에서의 자원 처리의 유무나 중요도를 제공 가능하다. 따라서, 생명주기 지원 클래스의 적용에 대한 부가적인 비용과 노력을 감소시키고 시스템 개발로 밀접하게 연관되어 시스템의 중요한 부분의 모델링과 검증을 위한 시스템 명세와 시스템의 신뢰성을 증가시키고자 한다.

2. 관련 연구

2.1 국제공통평가기준

국제공통평가기준(CC : Common Criteria)은 국가마다 다른 정보보호시스템 평가기준을 연계시키고 평가결과를 상호인증하기 위해 제정된 평가기준으로, 1999년 8월 국제표준(ISO/IEC 15408) 버전 2.1로 승인됐다. 이는 정보보호제품의 평가에 관한 기준을 국제적으로 단일화 한 것으로써 세계 각국의 평가 기준이 상이하여 평가에 소요되는 비용과 시간이 많이 소요되는 요구사항을 해결하였다. CC는 크게 세 가지 부분으로 구성되어 있으며, CC의 핵심은 제2부와 제3부로써 정보보호시스템이 구비해야 하는 기능 및 보증 요구사항을 기술하고 있으며 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발하고 있다[2].

표 1. CC 보증 요구사항 클래스

클래스명	클래스 제목	역할
ACM	형상관리(Configuration Management)	TOE의 무결성이 유지되고 있는지를 확인
ADO	배포와 운영(Delivery and Operation)	TOE의 안전한 배포, 설치, 운영에 필요한 수단, 절차 및 표준을 확인
ADV	개발(Development)	TOE 개발 과정의 일치성 및 완벽함을 확인
AGD	설명서(Guidance Documents)	TOE의 안전한 운영을 위한 지침서를 확인
ALC	생명주기 지원 (Life Cycle support)	TOE의 생명주기와 관련된 사항을 확인
ATE	시험(Tests)	TOE가 기술요구사항을 만족하는지를 확인
AVA	취약성 분석 (Vulnerability Analysis)	TOE의 개발과정 중에 발견되지 않은 취약성, 사용자에 의한 오용등 잠재적인 취약성을 확인
APE	보호프로파일평가(Protection Profile Evaluation)	PP가 완전하고 모순이 없으며 기술적으로 충분함을 보임
ASE	보안목표명세서평가(Security Target Evaluation)	ST가 완전하고 모순이 없으며, 기술적을 충분함을 보임
AMA	보증의 유지(Maintenance of Assurance)	TOE나 보안환경이 변화에도 ST를 지속적으로 만족시킴을 보임

제3부에서는 보증컴포넌트, 보증패밀리, 보증클래스로 분류되고 보호프로파일(PP : Protection Profile)과 보안목표명세서(ST : Security Target)에 대한 평가기준을 정의하며 평가대상(TOE : Target of Evaluation) 평가를 등급별로 나누어 7등급의 평가등급을 소개하고 있다. 10개 클래스의 보증 요구사항을 요약하면 표 1과 같다.

2.2 표준 소프트웨어 생명주기 프로세스

ISO12207은 소프트웨어 생명주기 프로세스 표준이다. 기존의 방법론이나 표준과는 달리 소프트웨어 개발주기에 대한 기본공정이외에도 지원공정과 조직공정을 추가함으로써 정보시스템 전체를 어떻게 하면 포괄적으로 적용할 수 있을 지에 대한 전체적인 프레임워크를 제공한다[3].

다음 (그림 1)은 ISO12207의 전체 구성도이며, 기본공정, 지원동정, 조직공정으로 구분되는데 기존의 소프트웨어 품질 및 개발주기 관련 표준과 달리 조직공정에 기반구조 공정을 포함함으로써 정보시스템 아키텍처가 정보시스템을 구축하는데 반드시 다루어야할 필수요소임을 제시하는 최초의 국제표준이다. 소프트웨어를 포함한 시스템, 단독형 소프트웨어 및 서비스의 획득 동안에, 그리고 소프트웨어 제품의 공급, 개발, 운영 및 유지보수 동안에 적용될 수 있는 공정(process), 활동(activity) 및 세부업무(task)를 포함한다.

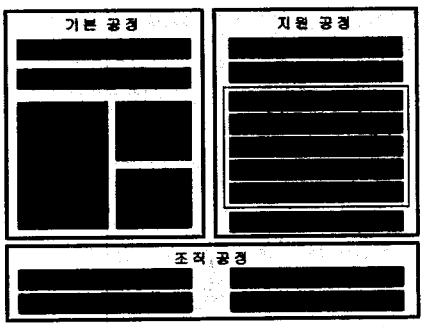

그림 1. ISO/IEC 12207 국제표준의 구성도

3. CC 기반의 생명주기 지원 클래스

IT 시스템의 부분이나 CC에 기반하여 평가되어야 하는 생산품은 평가 목표(TOE : Target of Evaluation)라고 불리고 평가 권한에 의해 검증되는 다른 보안 요구사항을 수행해야 한다. CC의 보안 요구사항은 보안 기능 요구사항(생산품상의 요구사항)과 보안 보증 요구사항(프로세스상의 요구사항)으로 분할되며, 클래스 내에 구조화된다. 기능적인 요구사항은 TOE의 보안 목표를 달성하기 위한 시스템의 기능에서 실체화되며, 보증 요구사항의 수와 엄격함에 따라 TOE를 위해 선택한 평가 보증등급(EAL : Evaluation Assurance Level)에 의존하여 수행된다.

TOE에 대한 적절한 평가 보증등급을 부여하기 위해서는 <표 1>에서 제시된 요구사항의 고수준을 만족해야한다. 특히, 본 논문에서는 CC의 생명주기 지원 보증 요구사항 클래스는 TOE 개발을 위한 생명주기 모델에 관한 보증요구사항으로 정의하고, 생명주기 지원 영역에 요구사항을 분석을 하고자 한다. 다음 (그림 2)은 제시된 생명주기 지원 클래스에 대한 적절한 요구사항들의 클래스, 패밀리, 컴포넌트의 구조를 도식화하였다.

생명주기 지원 클래스는 결함 교정 절차 및 정책, 도구와 기법의 정확한 이용, 개발 환경을 보호하기 위해 사용되는 보안 대책 등을 포함한 TOE 개발의 모든 단계에 대하여 잘 정의된 생명주기 모델을 채택함으로써 보증 요구사항을 정의한다. 또한, 개발 및 유지하는 동안 TOE의 상세화 과정에서 규칙 및 통제를 수립한다. 보안 분석 및 증거 생성이 개발 과정과 운영지원 활동의 한 부분으로서 정기적으로 수행될 때, TOE와 TOE 보안 요구사항 간의 일치성에 대한 신뢰는 증가한다.

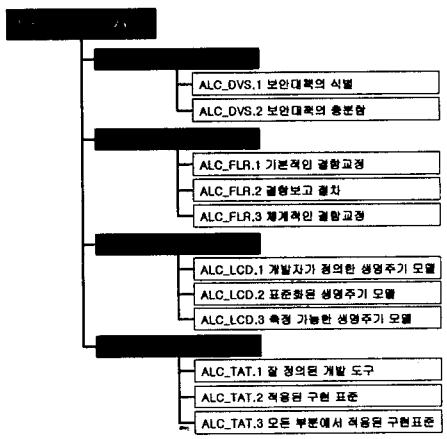

그림 2. CC에서의 생명주기 지원 클래스의 구성

4. 생명주기 지원 클래스 요구사항 분석

CC의 보증 요구사항 클래스 및 패밀리에 해당하는 각 관련 보증방법론의 항목 도출을 위하여 프로세스와 세부적인 활동을 중심으로 하고, 평가 기준을 중심으로 하는 요구사항 분석을 한다. (그림 3)에서와 같이 생명주기 지원 클래스를 통한 개발 및 평가를 반복적으로 수행하고 컴포넌트에 포함된 보증 엘리먼트의 속성들 즉, 개발과 평가 프로세스가 병행으로 이루어진다.

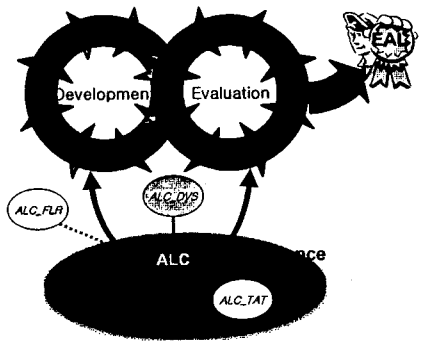

그림 3. 생명주기 지원 클래스를 통한 개발 및 평가

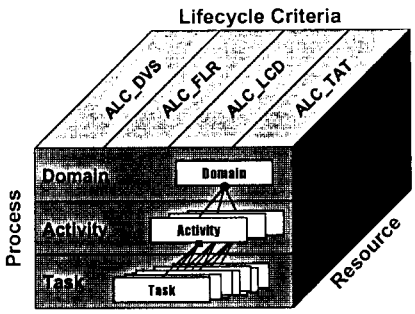

그림 4. 생명주기 지원 클래스 분석 모델

생명주기 지원 클래스는 개발과 평가의 상호작용 및 관계성을 가진다. 일반적인 개발 프로세스 단계에서 생명주기 지원 클래스는 단지 높은 평가 보증등급 영역에서 요구되어지는 행위들로 구성되어 있다. 요구사항들은 개발자, 증거, 평가자 요구사항의 3가지 측면으로 나누어지며, 개발자 측면에서는 생명주기 지원 클래스의 결함 교정 패밀리는 고려되어야 하지만, 평가보증 등급을 부여하기 위해서는 고려되지 않는다.

IT 제품이나 시스템을 CC를 기반으로 개발과 평가할 경우 분석해야할 많은 부분이 존재한다. 본 논문에서는 (그림 3)에서 제시한 개발과 평가 방법을 지원하고 분석을 하기 위해 자원, 프로세스, 생명주기 기준의 3가지 영역의 모델을 제안한다. 즉, 보안 평가 모델에서는 생명주기 지원 요구사항, 자원, 프로세스간의 상호작용을 중요시하며, 이 세 가지 요소간의 상호작용을 기반으로 하여 3차원 모델을 분석의 기본 틀로 하고 있다. 생명주기 기준은 정보시스템이나 IT 관련 프로세스가 갖추어야 하는 특성들로 개발 보안, 결점교정, 생명주기 정의, 도구와 기법으로 분류되며, 총 11개의 컴포넌트와 보증 앨리먼트로 세분화되어 있다. 자원은 평가의 대상물로서 크게 기술, 자산, 도구, 모델, 문서 등으로 분류하였다. 프로세스는 기존의 표준으로 제시된 프로세스의 구조로써 프로세스, 단계, 행위의 계층적인 구조로 파악하고 있다.

표 2. 생명주기 지원 클래스의 분석 프레임워크의 예

Domain			기본 공정					
Activity			...	개발				
Task			...	공정 구현	시스템 요구 분석	시스템 구조 설계	SW 요구 분석	SW 구조 설계	...
Life cycle Criteria	ALC_DVS	ALC_DVS.1		V	V	V	V	V	
		ALC_DVS.2				V		V	
	ALC_FLR	ALC_FLR.1							
		ALC_FLR.2							
		ALC_FLR.3							
	ALC_LCD	ALC_LCD.1		V					
		ALC_LCD.2							
		ALC_LCD.3							
	ALC_TAT	ALC_TAT.1	...	V				V	...
		ALC_TAT.2							
		ALC_TAT.3							
Resource	Technology			V	V	V	V	V	
	Property			V	V	V	V	V	
	Tool			V	V	V	V	V	
	Model					V		V	
	Document			V	V	V	V	V	

생명주기 기준은 다른 CC의 보안 보증 요구사항으로 대체 하여 모든 클래스에 대한 기본 분석에 사용가능 하며, 평가 모델로써 재사용 가능하다.

생명주기 지원 클래스 분석 모델을 기반으로 12207 소프트웨어 생명주기 프로세스에 적용하여 작성한 프레임워크를 <표 2>와 같이 나타내었다. 본 논문에서는 12207의 3가지 도메인 중에서 기본공정을 선택하여 각각의 액티비티와 태스크를 제시하였고, 생명주기 지원 클래스의 컴포넌트와 자원 항목들이 어떤 태스크에 존재하고 보증을 하기 위해 요구되는 지의 여부를 예를 들어 정의한다. 생명주기에 필요한 부분과 필수적으로 검증이 되어야할 항목을 선택 가능하며, 이는 생명주기 관점에 포함된 프로세스 단계를 중심으로 작성한다.

5. 결론 및 향후 연구

정보기술 영역에서 유연성 높은 전산시스템을 구축할 수 있는 서비스 지향 아키텍처가 요구되면서, 소프트웨어 인프라와 보안에 대한 중요성이 인식되고 있다. 공통평가기준은 보안을 중요시하는 시스템의 평가를 위해서 표준화된 요구사항들의 목록이다. 공통평가기준을 사용하여, 시스템 자체와 시스템 개발에 많은 보안 요구사항 정의는 가능하지만, 이를 통해 모든 개발에 대한 보안 요구사항 분석이 어렵고, 방법론 지원을 하지 않는다.

본 논문에서는 소프트웨어공학 프로세스에서 보안요소를 고려하고, 공통평가기준에서의 행위와 문서 등의 자원과 생명주기 지원을 위한 클래스의 적용 및 분석을 위한 방법으로 분석 모델과 프레임워크를 정의하였다. 이는 생명주기 지원 클래스를 통한 개발과 평가를 지원하고, 개발자와 평가자에게 고려해야할 기준 이외에 생명주기 상에서의 자원 처리의 유무나 중요도를 제공 가능하다. 따라서, 생명주기 지원 클래스의 적용에 대한 부가적인 비용과 노력을 감소시키고 시스템 개발로 밀접하게 연관되어 시스템의 중요한 부분의 모델링과 검증을 위한 시스템 명세와 시스템의 신뢰성의 이해를 증가시킨다. 향후 연구는 CC기반 생명주기 지원 개발 프로세스와 평가 프로세스 모델 작성 및 도구에 대한 연구가 필요하다.

참고 문헌

1. Jonathan Stephenson, "Web Services Architectures for Security," CBDi Journal, http://www.cbdiforum.com/, Feb. 2003.
2. Common Criteria Project/ISO, "Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408)," http://www.commoncriteria.org/cc/, 1999.
3. "Information Technology-Software Life cycle Process, (ISO/IEC 12207)," http://standards.ieee.org/ reading/ieee/std/, 1998.
4. Monika Vetterling , Guido Wimmel and Alexander Wisspeintner, "Requirements analysis: Secure systems development based on the common criteria: the PalME project," Proceedings of the tenth ACM SIGSOFT symposium on Foundations of software engineering, pp. 129 - 138, Nov. 2002.
5. "정보보호시스템 공통평가기준," 정보통신부 한국정보보호진흥원, 2002.