제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

정보보호 제품의 결함 추적 및 교정에 관한 연구

신호준*, 김행곤*, 김태훈**
*대구가톨릭대학교 컴퓨터정보통신공학부
**한국정보보호진흥원
e-mail:{g98521002, hangkon}@amare.ac.kr, taihoon@kisa.or.kr

A Study on Flaw Track and Remediation of Information Security Product

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

요 약

소프트웨어 개발 응용 패러다임이 분산 환경 기반을 두면서 보안 문제가 매우 중요시되고 있다. 정보통신 제품이나 시스템을 개발할 경우 보안에 대한 평가를 위해서 표준화된 요구사항들의 목록으로 공통평가기준이 정의되어 있다. 공통기준에서 고려되어야할 결함 교정에서 구체적인 절차와 결함 항목의 식별, 속성, 행위 정의가 필요하다.

본 논문에서는 소프트웨어공학 프로세스에서 보안측면을 고려하여, 생명주기의 자원과 프로세스에서 결함 추적 및 교정을 위한 기능적, 비기능적인 엔티티와 이를 기반으로한 프로세스를 제안한다. 즉, 생명주기를 통한 개발과 평가를 지원하고, 개발자와 평가자에게 고려해야할 기준 이외에 생명주기상에서의 자원 처리의 유무나 중요도 제공이 가능하다. 결함 추적과 교정을 위한 엔티티 적용에 대한 부가적인 비용과 노력을 감소시키고 정보보호 제품 개발과 밀접하게 연관된 결함을 검증하고 교정함으로써 제품의 개발과정의 신뢰성을 제공하고 생명주기 관리의 효율성을 증가시키고자 한다.

1. 서론

정보보호에 대한 관심이 높아지고 있는 가운데 정보보호 관련 정부조직과 정보보호 업체들에 대한 직·간접적인 지원과 운영의 확대가 이루어지고 있다. 정보보호 영역에서의 소프트웨어 개발과 관리는 보안 표준의 준수와 보안 요소들의 고려를 매우 중요하게 여기고 있다. 현재 IT 보안성 평가를 위한 CC(Common Criteria : 공통평가기준)를 통해 보안에 대한 위협과 조직의 보안 정책을 명확하게 표현하고, 제안된 보안수단이 본래 의도된 목적을 만족시키는데 충분함을 입증하고자 한다. 하지만 입증된 정보보호 제품에 대한 개발 과정 및 생명주기 유지 방법이 무척 미흡한 상태이다. 또한, 개발과 관리 영역에서 식별될 수 있는 결함에 대한 정책이나 절차가 형식적인 수준에 머물고 있다.

본 논문에서는 정보보호 제품의 개발과 유지과정에서 제공되어야할 결함에 대한 추적과 식별된 결함에 대한 교정을 위한 결함 요소를 정의하고 이를 통한 추적 및 교정을 위한 프로세스를 제안한다. 제안된 결함요소들은 소프트웨어 생명주기를 기반으로 정의되며, 기능적인 요소뿐만 아니라, 정책적으로 요구되는 비기능적인 요소도 고려하여 정의하였다. 또한, 제안된 프로세스에서 처리 절차를 명세하고 이 절차에 기준하여 정의된 요소를 기술하였다.

2. 관련연구

2.1 공통 평가 방법론

CEMEB(Common Evaluation Methodology Editorial Board)는 CC(Common Criteria) 작성에 참여한 미국, 캐나다, 영국, 독일, 프랑스, 네덜란드가 CC에 적용할 수 있는 평가방법론인 CEM(Common Evaluation Methodology for Information Technology Security)을 작성하기 위하여

구성한 위원회이다.

CEM은 적절하고 비용·효과적인 평가를 수행할 수 있도록 하는 골격을 제시함으로써 효율적인 평가결과를 도출할 수 있도록 하며 평가받은 제품의 등급유지 및 평가결과의 상호인증을 목적으로 한다.

CEM은 평가자를 주 대상으로 하여 작성되어 있으나 개발자, 평가신청인, 감독자 및 평가결과를 이용하는 다른 조직에서도 그 내용을 유용하게 사용할 수 있도록 기술되어 있다. CEM에서 제시하고 있는 평가절차는 위와 같은 평가주체의 참여하에 평가준비, 평가시행, 평가결과 승인의 세 단계로 구성된다. 이에 따른 평가인증체계도는 다음 그림 1과 같다.

- 평가준비 : 평가신청인은 평가자에게 보호 프로파일 또는 보안목표명세서(Security Target)를 제공한다. 평가자는 성공적인 평가 가능성 여부를 분석하고 관련 정보를 평가신청인에게 요구한다. 평가신청인 또는 개발자는 요구받은 제출물을 평가자에게 제출하여야 한다.
- 평가시행 : 평가시행단계는 평가절차의 핵심부분으로 이 단계에서 평가자는 평가제출물을 검토하고 CC에서 정의한 평가자 활동을 수행한다. 평가를 수행하는 동안 평가자는 평가보고서(Observation Report)를 작성하며 감독자에게 평가보고서에 대한 설명을 하여야 한다. 평가자는 평가를 수행하면서 발견한 취약성 혹은 결점을 평가보고서에 명시하여야 하며 평가보고서를 작성하기 위하여 평가신청인 혹은 개발자에게 부가의 정보를 요구할 수 도 있다.

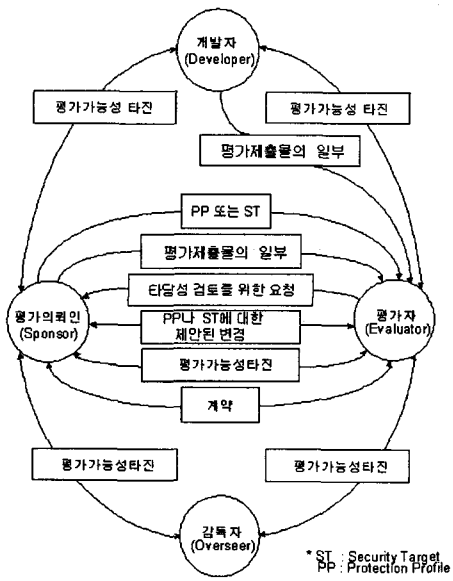

그림 1. 평가 절차

감독자는 평가체계에서 요구한 바대로 평가를 감독하며 평가자는 평가결과 및 평가결과의 정당성을 입증하는 내용이 포함되어 있는 평가기술보고서를 작성하여야 한다.

- 평가결과 승인 : 이 단계에서 평가자는 평가기술보고서를 감독자에게 제출한다. 평가기술보고서를 처리하는 절차 및 평가기술보고서를 개발자 및 평가신청인에게 전달하는 절차는 각 국가별 평가체계에서 정의된다.

2.2 결함 교정

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 보증 등급(EAL : Evaluation Assurance Level)에 의존하여 수행된다[2].

TOE에 대한 적절한 평가 보증등급을 부여하기 위해서는 보증 요구사항의 고수준을 만족해야한다. 특히, 본 논문에서는 결함 추적과 교정을 위해 CC의 생명주기 지원 보증 요구사항 클래스에서 결함 교정 패밀리를 기반으로 한다. 다음 그림 2는 제시된 생명주기 지원 클래스에서의 결함교정 패밀리의 컴포넌트 구조를 도식화하였다.

결함교정(ALC_FLR, Flaw remediation) 패밀리는 발견된 결함을 개발자가 추적하고 교정하도록 한다. TOE 평가 시에는 결함교정 절차가 향후 준수될지는 결정할 수 없지만, 개발자가 결함을 추적 및 교정하고 결함 정보와 교정본을 배포하기 위한 적절한 정책과 절차에 대해서는 평가할 수 있다.

이 패밀리의 컴포넌트는 결함교정 절차의 범위와 결함교정 정책의 엄밀성에 기반하여 계층화되어 있다. 이 패밀리는 TOE 개발자에게 TOE의 결함을 추적하고 교정하도록 요구함으로써 TOE가 계속해서 유지되고 지원될 것이라는 보증을 제공한다. 또한, 결함교정본의 배포에 대한 요구사항을 포함한다. 그러나, 이 패밀리는 현재의 평가범위를 벗어나는 평가 요구사항을 포함하지 않는다.

결함교정 절차는 발생하는 모든 유형의 결함을 다루기 위한 방법을 서술해야한다. 일부 결함은 즉시 교정되지 못할 수도 있다. 결함이 교정될 수 없어서 다른 대책이 필요한 경우도 있다. 제공되는 문서는 운영자 측에 교정을 제공하기 위한 절차 및 교정이 지연되거나 불가능한 경우 결함에 대한 정보를 제공하기 위한 절차를 다루어야 한다.

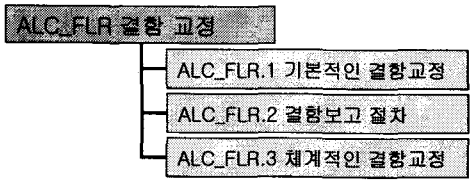

그림 2. 결함 교정 패밀리

3. 결함 추적 및 교정을 위한 엔티티 정의

CC에서는 결함에 관련해서 기본적인 결함 교정, 결함보고 절차, 체계적인 결함 교정 3가지 범주에 기준을 마련해 놓고 있다. 하지만 이것에 대한 구체적인 방법과 적용 절차에 대한 것은 없다. 따라서, 개발자와 평가자가 스스로 평가기준을 기반으로 적절한 방법을 마련해야한다.

개발자가 결함을 추적 및 교정하기 위해 사용할 수 있는 정책 및 절차 연구로는 관련 단체의 협의 기구가 있어야 한다. 또한, 전략을 세우기 위해서는 오류 보고에 의해서 결함을 추적할 수 있으며, 자동적인 결함 추적을 위해서는 결함추적의 계획과 결함 결정 요소를 정의하여 이를 개발 단계에 적용, 개발해야만 한다. 이러한 결함에 밀접한 관련성을 가진 엔티티를 정의한다.

결함 추적과 교정을 위한 엔티티 분류에 의해서 소프트웨어 개발의 생명주기를 중심으로 자료와 정보를 조직한다. 결함 식별은 자원을 식별하는 과정으로 그 분류 구조는 응용을 위한 분류기반 질의와 애플리케이션에 대한 프로세스로 구성된다.

엔티티들은 그림 3과 같이 클래스, 패밀리, 컴포넌트의 세 수준으로 CC의 분류에 준해서 소프트웨어 개발 결함을 구성한다. 또한, 클래스와 하위 분류 항목들은 소프트웨어 생명주기에 기준을 둔 결함 요소로써 제한한다. 결함 추적의 기준이 될 엔티티를 표 1과 같이 식별하여 정의한다.

4. 결함 추적 및 교정을 위한 프로세스

결함을 관리하는 주요 목적은 소프트웨어 품질에 부정적인 영향을 줄 가능성이 있는 잠재적 요소를 식별, 분석, 해결하기 위한 체계적인 프로세스이다. 결함 관리의 궁극적인 목표는 결함 요소를 파악하고, 해결 및 감소할 수 있는 프로세스와 전략을 개발하는데 있다. 이는 고객, 프로젝트, 이익, 자사 및 고객사의 신뢰를 위해 개발 및 유지 실패 가능성의 원인적 요소와 확률을 최소화하고, 실천적이고 바람직한 결론과 결함으로 인한 치명적인 손실 가능성을 최소화하는데 그 의미가 있다.

결함 추적 및 교정은 정보보호제품의 개발뿐만 아니라 제품의 유지되는 부분과도 다음 그림 4와 같이 밀접한 관련성을 가진다. 개발 단계에서는 결함의 발생을 최소화하기 위해 결함 요소를 결정하여 분석, 설계 단계를 포함한 전 단계에 대해서 결함 요소 평가를 해야한다. 또한, 이러한 요소에 대한 자료를 선정하여 정보보호제품의 보안

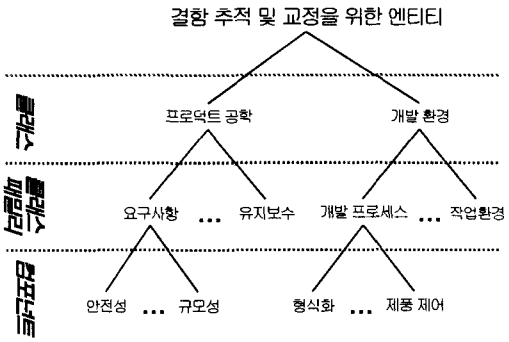

그림 3. 결함 추적 및 교정을 위한 엔티티 분류

표 1. 결함 추적 및 교정을 위한 엔티티

카테고리	생명주기	주요 엔티티
프로덕트 공학	요구 분석	안전성
		완전성
		명료성
		정당성
		타당성
		연계성
		규모성
	설계	기능성
		난해성
		인터페이스
		효율성
		테스팅
		하드웨어 제약
	코딩 및 유닛 테스팅	타당성
		테스팅
		코딩/구현
	통합 테스팅	환경
		프로덕트
		시스템
	공간적 측면	유지보수
		신뢰성
		안정성
		인적 요소
		명세
개발 환경	개발 프로세스	형식성
		적합성
		프로세스 제어
		그룹성
		프로덕트 제어
	개발 시스템	용량성
		안전성
		사용성
		구룹성
		신뢰성
		시스템 지원
		양도성
	관리 프로세스	계획
		프로젝트 조직
		관리 경험
		프로그램 인터페이스
	관리 방법	감시성
		개인 관린
		품질 보증
		형상 관리
	작업 환경	품질 요소
		협동
		통신
		도덕성

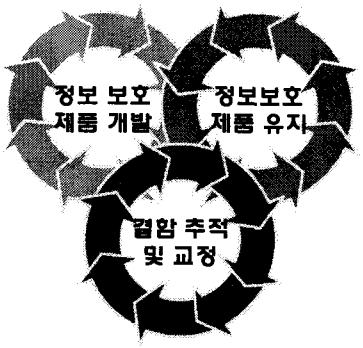

그림 4. 제품 개발-결함 추적-제품 유지 상호 관련성

평가가 이루어진 후에도 유지 단계에서의 결함 관리는 계속적으로 이루어져야한다.

본 논문에서는 그림 5와 같이 결함 추적과 교정을 위한 프로세스에서 정보보호 제품 개발 과정뿐만 아니라, 유지 단계에서의 결함 추적 및 교정을 가능케 한다. 결함 관리를 위한 프로세스는 크게 결함 반응 계획, 추적, 결함 식별, 분석 , 교정으로 구분할 수 있다.

- 식별 : 결함을 관리하기 이전에 식별되어야만 하며, 결함이 문제시되기 전에 식별을 통해 가시화 시켜야 한다.
- 분석 : 결함 데이터를 결정을 위한 정보로 변형시키며, 결점의 우선순위와 분류를 한다. 또한, 결함 요소의 평가와 요소 선정 작업이 이루어진다.
- 교정 : 계획된 결함 행위에 대한 잘못된 부분을 바로 잡는 것이다. 결함의 회피 및 완화 계획 수행과 추적 활동 수행과 교정 활동 식별이 요구된다. 또한, 결함 요소가 실제화 되었을 때 위험 발생 대책 수행을 하게된다.
- 계획 : 결함 정보를 결정과 교정시킬 수 있는 행위로 변형하며 구현한다. 이는 결함 회피 및 완화계획 수립과 결함 위험 발생 대책 수립을 포함한다. 또한, 위험 상황 모니터링 및 보고 계획 수립, 개별 결함 요소 담당자 정의, 위험관리 문서화 계획과 같은 전략적이고 비기능적인 행위를 포함한다.

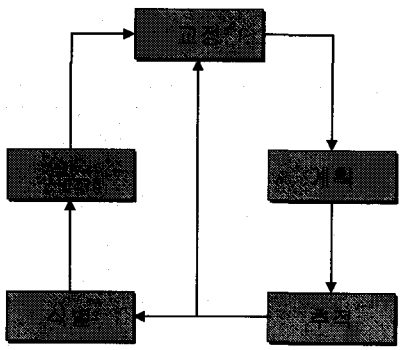

그림 5. 결함 추적 및 교정 프로세스

- 추적 : 결함의 상태에 대한 모니터와 결점을 고치기 위한 행위로 구성된다. 결함 메트릭스는 결함 해결 계획뿐만 아니라 결함 상태의 평가를 가능하게끔 식별되어지고 모니터 되어진다. 추적은 관리 기능으로써 제공된다.

5. 결론 및 향후 연구

정보통신 제품이나 시스템을 개발할 경우 보안에 대한 평가를 위해서 표준화된 요구사항들의 목록으로 공통평가기준이 정의되어 있다. 본 논문에서는 공통기준에서 고려되어야할 결함 교정에서 구체적인 절차와 결함 항목의 부재를 해결하고자 제안되었다.

본 논문에서는 소프트웨어공학 프로세스에서 보안측면을 고려하여, 공통평가기준에서의 행위와 문서 등의 자원과 생명주기를 고려한 결함 추적 및 교정을 위한 엔티티와 이를 기반으로한 프로세스를 제안하였다. 이는 생명주기를 통한 개발과 평가를 지원하고, 개발자와 평가자에게 고려해야할 기준 이외에 생명주기상에서의 자원 처리의 유무나 중요도를 제공 가능하다. 따라서, 결함 추적과 교정을 위한 엔티티의 적용에 대한 부가적인 비용과 노력을 감소시키고 시스템 개발로 밀접하게 연관되어 시스템의 중요한 부분의 결함을 검증하고 교정함으로써 정보보호 제품의 개발 과정과 생명주기 유지의 신뢰성을 증가시킬 수 있다. 향후 연구로써는 결함 추적 및 교정 프로세스의 상세한 활동을 정의하고, 자동화된 도구의 지원이 요구된다.

참고문헌

[1] 정보통신부 한국정보보호진흥원, "공통평가방법론", http://www.kisa.or.kr/, 2001.

[2] "정보보호시스템 공통평가기준," 정보통신부 한국정보보호진흥원, 2002.

[3] Common Criteria Project/ISO, "Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408)," http://www.commoncriteria.org/cc/, 1999.

[4] "Information Technology-Software Life cycle Process, (ISO/IEC 12207)," http://standards.ieee.org/reading/ieee/std/, 1998.

[5] Ruben Prieto-Diaz, "The Common Criteria Evaluation Process," Commonwealth Information Security Center Technical Report, 2002.

[6] 김세헌, 정보보호 관리 및 정책, 생능출판사, 2002.