IT 시스템 개발현장실사 절차에 관한 연구

김태훈° 김재성 김행곤*
한국정보보호진흥원, *대구가톨릭대학교
{taihoon°, jskim}@kisa.or.kr, *hangkon@cu.ac.kr

A Study on the Evaluation Procedures for IT System Development Site

Taihoon Kim°, Jaesung Kim, *Haengkon Kim
KISA, *Catholic University of Daegu

요 약

IT 시스템 평가과정은 시스템의 보안기능과 이에 적용된 보증수단이 요구사항들을 만족하는지에 대한 신뢰도를 확인하는 것이며, 평가결과는 소비자가 IT 제품이나 시스템이 주어진 환경에 적용하기에 충분히 안전한지, 사용상 내재하는 보안위험이 허용가능한지를 결정하는데 도움이 될 수 있다. 평가를 통하여 평가보증등급(EAL: Evaluation Assurance Level) 3 이상으로 인증받기 위해서는 ALC_DVS.1 컴포넌트의 요구사항을 만족하여야 하며, 이들 요구사항은 개발현장에 대한 실사를 요구하게 된다. 본 논문에서는 ALC_DVS.1 컴포넌트에서 요구하는 현장 실사의 중요성을 파악하고, 국내에 적용가능한 ALC_DVS.1 컴포넌트 패밀리를 제안하고 실사 준비에 필요한 절차를 도출하였다.

1. 서 론

공통평가기준의 생명주기 지원 보증 클래스(ALC)는 결함교정 절차 및 정책, 도구 및 생명주기 방법론의 정확한 이용, 개발 환경을 보호하기 위해 사용되는 보안대책 등을 포함하여 TOE 개발의 모든 단계에 대하여 잘 정의된 생명주기 모델을 채택하도록 보증요구사항을 정의하고 있으며, ALC_DVS.1 컴포넌트만이 EAL 3 등급에서 요구된다.

개발환경 보안은 IT 제품 및 시스템의 개발 환경에 적용된 물리적, 절차적, 인적, 기타 보안수단을 검토함으로써 평가될 수 있다. 개발환경에 대한 보안은 제품 개발 장소의 물리적 보안과 개발인력의 선정 및 고용에 대한 통제 요소를 포함하며, 이에 대한 요구사항은 공통평가기준(정보통신부 고시 제2002-40호)의 ALC_DVS 패밀리에 기술되어 있다[1].

현재 등재되어 있는 국가기관용 보호프로파일들의 평가보증등급이 EAL 3+임을 감안하여 볼 때, 이들 보호프로파일을 준수하여 개발된 제품들을 평가하는 경우에 ALC_DVS.1 컴포넌트의 요구사항 만족 여부를 검토하여야 하며, 대부분의 경우에는 개발현장에 대한 실사를 통하여 만족 여부를 평가하게 된다. 하지만 공통평가기준은 개발현장에 대한 실사를 수행할 수 있다는 의미를 나타내면서도 구체적인 실사 방법론에 대한 언급은 하고 있지 않다. 따라서 개발현장에 대한 실사가 갖는 중요한 의미를 고려할 때, 적절한 절차에 따라 실사가 진행되어야만 요구사항의 만족 여부를 합리적으로 파악할 수 있을 것으로 사료된다.

본 논문에서는 ALC_DVS.1 컴포넌트에서 요구하는 현장 실사의 중요성을 파악하고, 국내에 적용가능한 ACL_DVS.1 컴포넌트 패밀리를 제안하고 실사 준비에 필요한 절차를 도출함으로써, 평가자의 개발환경 보안 실사에 대한 준비 및 개발자의 개발환경 보안에 대한 보완을 지원하고자 한다.

2. ALC_DVS 패밀리

공통평가기준 3부 보증요구사항에 명시되어 있는 개발보안(ALC_DVS, Development security) 패밀리는 TOE를 보호하기 위하여 개발 환경에 적용될 수 있는 물리적, 절차적, 인적, 기타 보안대책에 관한 요구사항을 명시한 것이다. 이들 보안 대책은 IT 제품 개발 장소의 물리적 보안 및 인적 보안을 위한 선택 방법 등에 적용되는 절차를 포함하고 있다.

ALC_DVS 패밀리는 개발자 측에 존재하는 위협을 제거하거나 줄이기 위한 대책을 다루는 것이며, 이것은 TOE 사용자 측에 존재하는 위협을 줄이기 위한 대책과는 차이가 있다(TOE 사용자 측에서 대응해야 하는 위협은 일반적으로 보호프로파일 또는 보안목표명세서의 보안환경 절에서 다룬다).

평가자는 ALC_DVS 패밀리의 요구사항이 만족되는지를 확인하기 위하여 개발자 측을 방문할 필요가 있는지를 결정해야 하며, 개발환경 내에서의 TOE 보호에 대하여 비밀성은 쟁점이 되지 않을 수도 있음을 인식할 필요가 있다.

현재 국가기관용 보호프로파일에서 요구하고 있는 평가보증등급은 EAL 3+이며, 이 경우 ALC_DVS.1 컴포넌트가 적용된다.

2.1 ALC_DVS.1 컴포넌트의 요구사항

ALC_DVS.1 컴포넌트의 요구사항은 크게 세 가지로 구성되어 있으며, 각각 개발자 요구사항, 증거 요구사항, 평가자 요구사항으로 이루어진다. 개발자 요구사항은 다음과 같다.

ALC_DVS.1.1D 개발자는 개발보안 문서를 작성해야 한다.

개발자는 개발현장의 보안을 위하여 개발보안 문서를 작성하도록 요구받게 되며, 이 개발보안 문서 안에 포함되어야 하는 내용은 다음과 같은 증거 요구사항에 명시되어 있다.

ALC_DVS.1.1C 개발보안 문서는 개발환경 내에서 TOE 설계 및 구현 과정의 비밀성과 무결성을 보호하기 위하여 필요한 모든 물리적, 절차적, 인적 및 기타 보안대책을 서술해야 한다.

ALC_DVS.1.2C 개발보안 문서는 TOE를 개발 및 유지하는 동안 이러한 보안대책이 준수된다는 증거를 제공해야 한다.

이와 같은 증거에 대하여 평가자는 평가를 통하여 다음의 항목을 확인하도록 요구받는다.

ALC_DVS.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ALC_DVS.1.2E 평가자는 보안대책이 적용되고 있는지 확인해야 한다.

3. IT 제품 개발현장실사 절차

제품 개발현장실사는 공통평가기준에 정의된 ALC_DVS 패밀리의 요구사항을 기반으로 하여 이루어지며, 제품 개발현장에 적용되고 있는 물리적, 절차적, 인적 및 기타 보안 대책에 대하여 평가하는 것이다.

IT 제품 개발현장실사의 주요 목적은 IT 제품 개발환경의 안전성 확인과 개발환경 안전성 확보를 위한 다양한 보안 대책 수립이 가능하다. 또한, 물리적, 절차적, 인적 및 기타 보안측정요소에 대한 보안 대책 확인을 통해 개발 제품의 평가 등급 부여가 가능하다.

개발현장실사 진행 절차는 현장실사단 구성, 현장실사 준비, 현장실사 수행, 현장실사 결과보고 등으로 그림 1과 같이 크게 4 단계로 정의할 수 있다.

3.1 현장실사단 구성

현장실사를 하기 위해 먼저 실사단의 규모와 인력을 확보해야 한다. 실사할 대상 업체의 규모와 인원에 따라서 실사단 인원을 결정한다. 또한, 대상 업체의 분야에 평가 능력을 가진 전문가를 확보한다.

3.2 현장실사 준비

현장실사단이 구성되면 실사 일정을 계획하고, 해당 업체의 기본 정보를 확보한다. 결정된 실사 일정을 해당 업체에 통보하며, 구비해야할 문서와 자원, 인력 등을 미리 준비할 수 있도록 한다.

현장실사단은 TOE에 대한 정보와 실사 대상 업체의 정보를 숙지하고, 이에 따른 인터뷰 노트 및 실사 항목 체크리스트를 준비한다.

모든 실사 절차와 방식에 대한 협의 및 준비 사항을 점검한 후 일정에 따라 실사를 진행한다.

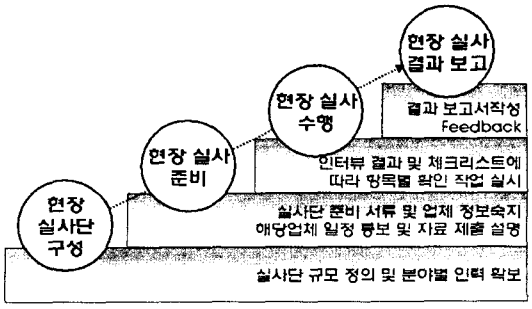

그림 1. IT 제품개발 현장실사 절차

3.3 현장실사 수행

현장실사 수행은 ALC_DVS의 요구사항을 기반으로 작성된 실사 점검 항목을 기반으로 수행된다. 평가 수행은 질의식과 확인식으로 진행할 수 있다.

3.3.1 질의식

질의식은 인터뷰 방식으로써, 주로 인적, 물리적, 절차적 보안 요소를 담당하는 관리자에 대한 면담을 통해 이루어진다. 미리 항목별 질의 내용을 작성한 후 평가 대상자를 중심으로 인터뷰를 실시하며, 긍적적 응답과 부정적 응답에 따른 질의 절차를 미리 설계하는 것이 가능하다. 인터뷰 진행시 그림 2의 예와 같은 인터뷰 노트에 면담 내용 등을 기록할 수 있으며, 이를 평가 결과로 활용하는 것이 가능하다.

3.3.2 확인식

확인식은 체크 리스트를 이용하는 방식으로써, 정의된 실사 항목들을 입력되는 자원과 시연되는 과정 등을 통해 확인하는 방식으로 진행된다. 미리 모든 실사 항목에 대해 질문식 문장을 체크리스트 형식으로 작성하도록 하며, 수치적인 결과를 얻는 정량적인 평가라기 보다 어느 정도의 개발환경을 마련하고 있으며, 보안성을 제시하는 가의 정성적인 평가이다. 주로 물리적, 절차적, 기타 보안요소의 만족도를 확인하는 수준의 평가에 적용할 수 있다.

3.4 현장실사 결과 보고

실사 결과물은 질의식, 확인식 실사 진행을 통해 생성된 인터뷰 결과 문서와 실사 항목 체크리스트, 그리고 이들 자료를 기반으로 실사단이 작성한 실사 결과 보고서이다.

인터뷰 결과					
업체명		직책		대상자	
기록자		진행자		작성일	
항목	질문사항		응답 및 요구사항		
PSY.1.1	1. 2. 3.		1. 2. 3.		

그림 2. IT 제품 개발현장실사용 인터뷰 노트의 예

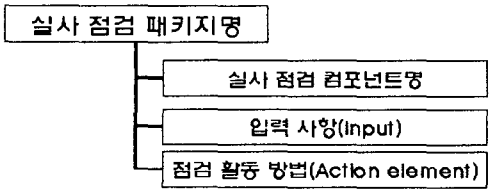

그림 3. 현장실사 점검 항목 구조

보고서는 평가 주관 기관과 대상 업체에 각각 피드백 되어야 하며, 실사단은 자체 평가회를 통해 개선점을 파악하여 차후 실사에 반영할 수 있다. 실사 결과는 업체의 신뢰도, 개발 제품의 신뢰도 평가에 활용하는 것이 가능하다.

4. 현장실사 점검 항목

정보보호 제품의 현장실사 항목의 구조는 그림 3과 같이 CC의 클래스 및 패키지 구조를 기반으로 작성되었으며, 내용은 ALC_DVS에서 정의한 개발환경에서 사용가능한 인적, 물리적, 절차적, 기타 보안 요소를 고려한다. 실사 점검 패키지의 구성은 다음 4가지로 분류한다.

- 물리적 보안 패키지 (Phy : Physical security)
- 인적 보안 패키지 (Psl : Personnel security)
- 절차적 보안 패키지 (Prc : Procedural security)
- 기타 보안 패키지 (Oth : Other security measures)

실사 점검 컴포넌트는 각 패키지별로 식별된 보안 컴포넌트로써 하나 이상의 하위 실사 점검 컴포넌트 요소를 가질 수 있다. 이 경우 하위 요소들의 분류 코드는 .(dot)을 기준으로 하나씩 레벨 하강한다. 입력사항(Input)은 해당하는 컴포넌트에 대해 실사를 진행하기 위해 요구되는 자원이며, 이를 통해 점검 활동을 한다.

점검 활동 방법(Action element)은 입력된 사항을 기반으로 실사를 진행하는 방법과 활동 내용을 기술하며, 이는 인터뷰 내용 및 질의문 작성에 기본이 된다.

패키지 항목과 각각의 보안 컴포넌트는 그림 4와 같이 크게 세 가지 패키지에 해당하는 실사 점검 컴포넌트가 정의되어 있다.

5. 결론 및 향후 과제

제품 자체의 안전성 평가와 함께 해당 제품의 개발환경에 대한 보안 평가를 수행하는 것은 제품의 신뢰성 향상에 많은 영향을 미칠 수 있다. 정보보호제품의 경우와 함께 일반적인 IT 제품의 경우에도 개방적인 환경에서의 제품 개발은 자칫 제품의 무결성에 대한 심각한 위협을 초래할 가능성을 내포하고 있기 때문이다.

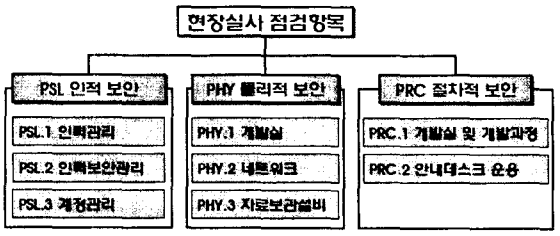

그림 4. 현장실사 점검 항목 패키지

개발환경보안 실사는 IT 제품 및 시스템의 개발 환경에 적용된 물리적, 절차적, 인적, 기타 보안대책을 검토하고 현장에서 개발자 및 관리자의 의견을 들어봄으로써 진행될 수 있으며, 이를 기반으로 하여 공통평가기준의 요구사항 만족 여부를 평가할 수 있다.

본 논문에서는 현재 등재되어 있는 국가기관용 보호프로파일들의 평가보증등급이 EAL 3+임을 감안하여 ALC_DVS.1 컴포넌트의 요구사항을 다루었으나, 고등급의 경우에는 이보다 높은 요구사항을 만족할 수 있도록 하여야 할 것이다.

공통평가기준은 개발현장에 대한 실사를 수행할 수 있다는 의미를 나타내면서도 구체적인 실사 방법론에 대한 언급은 하고 있지 않으며, 이러한 형식은 다양한 활용을 위한 근거가 됨과 동시에 모호함으로 인한 혼란을 야기할 수 있다. 따라서 개발현장에 대한 실사를 위한 어느 정도의 절차가 마련되고 일정 정도 개발환경에서 갖추어야 하는 요소들을 언급함으로써 기준을 제시하는 것이 가능할 것이다. 하지만 이와 같은 절차와 방법론은 자칫 반드시 따라야 하는 강제적 요구사항으로 변질될 우려가 있으므로, 이 절차와 방법론을 적용하는 평가자와 평가기관의 유연한 의미 해석이 또한 중요할 것이다.

[참고 문헌]

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

[2] ISO/IEC 15504 - Information Technology - Software Process Assessment, 1998.

[3] ISO/IEC 15443-3 - Information Technology - Security techniques - A framework for IT security assurance - Part 3: Analysis of assurance methods, 2001. 2.

[4] 김태훈, 이태승, 조규민, 이경구, "프로세스 평가 모델 등급과 정보보호시스템 공통평가기준 평가보증등급 비교", 한국사이버테러정보전학회 정보보증논문지 제2권 제2호, pp.137~142, 2002. 12.

[5] 정보통신부고시 제1999-104호, "정보시스템 감리기준", 1999. 12.

[6] 정보통신부고시 제2002-22호, "정보보호관리체계인증심사기준", 2002.5.

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