IT 시스템 개발현장 보안점검항목 추출에 관한 연구

김선미, 김태훈, 김상호, 김재성, 김행곤*
한국정보보호진흥원, *대구가톨릭대학교
{smkim, taihoon, shkim, jskim}@kisa.or.kr, *hangkon@cu.ac.kr

A Study on the Extraction of Security Check Lists for IT System Development Site

Sun-Mi Kim, Tai-hoon Kim, Sang-ho Kim, Jae-sung Kim,
*Haeng-kon Kim
Korea Information Security Agency, *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. 공통평가기준(정보통신부 고시 제2002-40호)에 기반한 평가를 통하여 평가보증등급(EAL) 3 이상의 등급을 인증받기 위해서는 ALC_DVS 패밀리의 요구사항을 고려하여야 하며, 국가기관에서 요구하고 있는 EAL 3+ 등급을 획득하기 위해서는 ALC_DVS.1 컴포넌트의 요구사항을 만족하여야 한다. ALC_DVS.1 컴포넌트의 요구사항 만족 여부를 확인하기 위해서는 개발현장에 대한 실사가 필요할 수 있으나, 공통평가기준에는 이에 관하여 세부적인 요구사항이 명시되어 있지 않다. 본 논문에서는 평가자 및 개발자가 ALC_DVS.1 컴포넌트에서 요구하는 인적, 물리적, 절차적 보안 요소를 확인하는 데 도움을 줄 수 있는 점검항목들을 도출하였다.

1. 서 론

개발현장 보안은 IT 제품 및 시스템의 개발 환경에 적용된 물리적, 절차적, 인적, 기타 보안수단을 검토함으로써 평가될 수 있다. 개발현장에 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 침입탐지시스템 보호프로파일, 국가기관용 침입차단시스템 보호프로파일, 국가기관용 가상사설망 보호프로파일 등의 평가보증등급이 EAL 3+임을 감안하여 볼 때, 이들 보호프로파일을 준수하여 개발된 제품들을 평가하는 경우에 ALC_DVS.1 컴포넌트의 요구사항 만족 여부를 검토하여야 한다. 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 평가자 및 개발자가 ALC_DVS.1 컴포넌트에서 요구하는 인적, 물리적, 절차적 보안 요소를 확인하는 데 도움을 줄 수 있는 점검항목들을 도출하였다.

2. 현장실사 점검항목 구조

공통평가기준 3부 보증요구사항에 명시되어 있는 개발 보안(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.

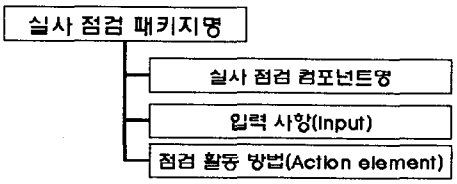

그림 1. 실사 점검 항목 구조

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).

정보보호 제품의 현장실사 항목의 구조는 그림 1과 같이 CC의 클래스 및 패키지 구조를 기반으로 작성되었으며, 내용은 ALC_DVS에서 정의한 개발환경에서 사용가능한 인적, 물리적, 절차적, 기타 보안 요소를 고려한다.

2.1 실사 점검 패키지명

실사 점검 패키지 구성은 다양하게 구성될 수 있으나, 본 논문에서는 다음과 같이 ALC_DVS에서 중점을 두고 있는 3가지 요소로 분류하여 연구를 진행하였다.

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

2.2 실사 점검 컴포넌트명

실사 점검 컴포넌트는 각 패키지별로 식별된 보안 컴포넌트로써 하나 이상의 하위 실사 점검 컴포넌트 요소를 가질 수 있다. 이 경우 하위 요소들의 분류 코드는 .(점)을 기준으로 하나씩 레벨 하강한다.

2.3 입력 사항(Input)

입력 사항(Input)은 해당 컴포넌트에 대해 실사를 진행하기 위해 요구되는 자원이며, 이를 통해 점검 활동을 한다. 입력 사항은 기업의 지침이나 관리용 문서뿐만 아니라 전산 처리된 정보등 그 범위가 폭넓게 적용된다. 또한, 입력 사항은 점검 활동의 기반이 됨으로 정확하고 신뢰성 있는 정보이어야만 한다. 현장 실사 결과 도출의 기본이 됨으로 매우 중요한 사항이다.

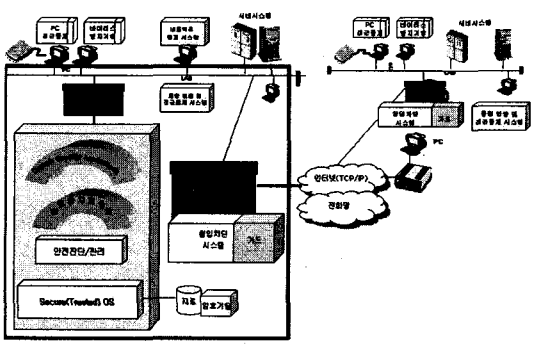

그림 2. ALC_DVS 컴포넌트 정의를 위한 시스템 구조도

2.4 점검 활동 방법(Action element)

점검활동 방법(Action element)은 입력된 사항을 기반으로 실사를 진행하는 방법과 활동 내용을 기술하며, 이는 인터뷰 내용 및 질의문 작성에 기본이 된다. 즉, 입력 사항을 처리하는 과정이 구체적이고 상세하게 기술되어 있으며, 평가자가 진행해야할 실사 방법을 단계별로 정의한다.

3. 현장실사 점검 항목 정의

정보보호제품의 현장실사 절차의 표준(안)을 제정하기 위해서는 먼저 TOE의 도메인 정의가 요구된다. 즉, 정보보호제품에 대한 개발환경이나 시스템 구조 정의 없이는 ALC_DVS에서 언급된 인증 컴포넌트에 따른 실사 항목들의 정의는 어렵다.

본 논문에서는 ALC_DVS 컴포넌트 정의를 위한 시스템 구조를 그림 2와 같이 제시한다. PC 접근 통제, 바이러스 방지 기술, 네트워크 탐지 시스템이 존재하는 네트환경과 방화벽을 통해 인터넷 망과 연결되며, 신뢰성이 인증된 운영체제 상에서 안전 진단/관리 서비스를 제공하고 특정 도메인 응용과 침입탐지 및 추적이 가능한 개발환경을 대상으로 한다. 시스템은 개발환경 네트워크 및 정보보호 시스템으로써 개발, 시험, 업무를 위한 물리적인 자원으로 정의된다.

패키지 항목과 각각의 보안 컴포넌트는 그림 3과 같이 크게 세 가지 패키지에 해당하는 실사 점검 컴포넌트가 기본적으로 정의되어 있다. 이 현장 실사 점검 항목 패키지를 기반으로 구체적인 입력 사항과 점검 활동 방법을 다음과 같이 간략하게 기술한다. 기술된 내용은 세 가지 범주에서 추출 및 식별된 내용으로써 전체내용 중에 일부분만 소개한다.

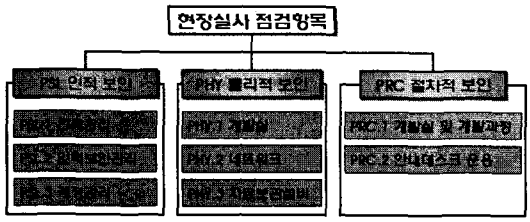

그림 3. 현장실사 점검 항목 패키지

3.1 인적 보안(PSL)

인적 보안은 개발에 참여한 신규, 내부, 외부, 재택근무자 모두를 대상으로 하여 인력 관리, 인력 보안 관리, 계정 관리를 한다.

3.1.1 인력 관리

PSL.1.1 신규 개발 인력 채용 관련 기준/절차 수립 및 운용

Input: PSL.1.1.1I 이력서
PSL.1.1.2I 신규 직원 채용에 관한 지침
PSL.1.1.3I 신규 직원 채용 공고문

Action element:
PSL.1.1.1A 체계적인 신입 직원 채용기준 및 절차에 의거하여 개발 인력을 채용하는지 입력 사항을 검토
PSL.1.1.2A 채용기준의 이행 여부의 입력 사항을 토대로 확인

3.1.2 인력 보안 관리

PSL.2.1 개발인력의 보안교육 정책 수립 및 운용

Input: PSL.2.1.1I 보안 교육 지침
PSL.2.1.2I 보안 교육 자료
PSL.2.1.3I 보안 교육 일지

Action element:
PSL.2.1.1A 체계적인 보안교육 정책에 의거하여 개발인력에 대한 보안교육을 실시하는지 검토
PSL.2.1.2A 교육자료를 통해 보안 교육 내용의 타당성 검사
PSL.2.1.3A 보안 교육이 주기적으로 이루어지는지를 검사

3.1.3 계정 관리

PSL.3.1 개발인력 계정 생성/유지/폐기를 위한 절차 수립 및 운용

Input: PSL.3.1.1I 계정 정책 지침
PSL.3.1.2I 계정 발급과 폐기 근거 문서

Action element:
PSL.3.1.1A 신규 및 퇴사자 개발 인력의 계정 발급과 폐기까지에 대한 관련 문서와 절차가 확립되어 있는지 검토
PSL.3.1.2A 개발 인력의 직급과 역할에 따른 개발 자료 접근 권한이 올바르게 결정되었는지 검토
PSL.3.1.3A 개발 인력 계정에 대한 암호는 안전한지의 여부 확인

3.2 물리적 보안(PHY)

물리적 보안은 개발실, 네트워크, 자료 보관 설비 등으로 나누어 보안관리 한다.

3.2.1 개발실

PHY.1.1 출입 통제 설비의 운영/관리 체계 구축 및 운용

Input: PHY.1.1.1I 출입 통제 설비의 운영/관리 지침
PHY.1.1.2I 설비 운영/관리 매뉴얼
PHY.1.1.3I 설비 현장 상황 및 관리자 지정 문서
PHY.1.1.4I 정기점검 기록 문서
PHY.1.1.5I 유지보수 기록 문서

Action element:
PHY.1.2.1.1A 출입통제설비의 운영/관리에 적절한 체계가 수립되어 운용되는지 문서검토
PHY.1.2.1.2A 수립된 체계에 의한 자료 확인
PHY.1.2.1.3A 수립된 체계에 의해 출입통제설비를 운영/관리하는지 출입통제설비 관리자 면담 및 시연 확인

3.2.2 네트워크

PHY.2.1 개발환경 네트워크 보호 관련 정책의 수립 및 운용

Input: PHY.2.1.1I 개발환경 네트워크 보호 관련 정책 지침
PHY.2.1.2I 네트워크 구성도

Active element:
PHY.2.1.1A 개발환경 네트워크 보호화 관련된 정책문서 검토
PHY.2.1.2A 입력 자료 및 실물확인을 통해 정책 시행여부 확인

3.2.3 자료 보관 설비

PHY.3.2 출입통제 설비의 물리적 특성에 대한 기준 수립 및 운용

Input: PHY.3.2.1I 출입통제 설비의 강도, 내구성,

화재, 충격 등과 같은 물리적 특성에 대한 기준 지침

PHY.3.2.2I 출입통제 설비 실물의 물리적 특성에 대한 자료

Action element:

PHY.3.2.1A 출입통제설비의 물리적 특성에 대한 지침 검토

PHY.3.2.2A 출입통제설비가 지침에 따르는지 실물 확인

3.3 절차적 보안(PRC)

절차적 보안은 개발실 및 개발과정에 관한 보안과 외부방문자의 기업 방문에 의한 정보 유출 등을 고려하여 안내 데스크 운용에 관한 실사 점검 항목으로 구성될 수 있다.

3.3.1 개발실 및 개발과정

PRC.1.2 개발인력의 직급/역할별 권한 및 책임 규정

Input: PRC.1.2.1I 개발인력의 직급/역할별 권한 및 책임 규정 지침

Action element:

PRC.1.2.1A 개발직원의 직급/역할별 권한 및 책임 규정 검토

PRC.1.2.2A 개발직원이 부여된 역할에 따라 업무를 수행하는지 확인

3.3.2 방문자 출입통제

PRC.2.4 방문자 출입통제 내역 보고체계 정의 및 운용

Input: PRC.2.4.1I 방문자 출입통제 내역 보고 지침

PRC.2.4.2I 방문자 출입통제 명부 및 보고일지

Action element:

PRC.2.4.1A 방문자 출입통제에 대한 내역 보고체계 검토

PRC.2.4.2A 출입통제 명부 및 보고일지를 통해 시행여부 확인

4. 결론 및 향후 과제

개발환경보안 실사는 IT 제품 및 시스템의 개발환경에 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. 하지만 공통평가기준의 ALC_DVS.1 컴포넌트에서는 이러한 보안대책이 있어야 한다는 것을 암시하고 있을 뿐, 실제로 어떠한 내용을 고려하여야 한다는 내용을 포함하고 있지는 않으며, 따라서 대부분의 경우 개발현장 실사는 개발자의 경험에 의한 보안 절차 운영 및 평가자의 경험에 의한 점검 항목 작성에 의존하는 경우가 많은 실정이다.

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.

본 논문에서 언급하고 있는 보안대책들이 자칫 반드시 따라야 하는 강제적 요구사항이 변질될 우려가 있으므로, 이러한 점검 항목들을 사용하고자 하는 개발자, 평가가 및 평가기관의 유연한 의미 해석이 반드시 고려되어야 할 것이다.

참고 문헌

[1] 정보통신부고시 제2002-40호, 정보보호시스템 공통평가기준, 2002. 8. 5

[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. 26

[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.