情 報 保 護 學 會 誌
第 13 券 第 6 號, 2003. 12

정보보호시스템 공통평가기준 기반의 평가제출물 작성 방법 연구

박 진 완*, 신 화 종**, 박 동 규***, 류 재 철****

요 약

정보보호시스템 공통평가기준(정보통신부고시 제2002-40호)에 의해 정보보호시스템을 평가받기 위해 개발자는 해당 평가보증등급의 보증패키지에 속하는 보증컴포넌트에서 요구하는 평가제출물을 작성하여야 한다. 공통평가기준에서는 평가제출물에 대한 작성방법을 제공하고 있지 않으므로 개발자가 평가제출물을 작성하는데 어려움이 있다. 본 고에서는 개발자가 공통평가기준에 기반한 평가제출물을 용이하게 작성할 수 있도록 적용될 수 있는 평가제출물 작성 방법론(순차방식, 병행방식)을 제시한다.

Ⅰ. 서 론

사회전반에 IT 제품 또는 시스템이 널리 활용되면서 IT 제품 또는 시스템에 대한 보안성 평가가 중요한 이슈로 등장하게 되었다. 국내 정보보호시스템 평가제도는 1998년에 고시한 침입차단시스템 평가기준과 2000년에 고시한 침입탐지시스템 평가기준과 같이 제품별로 평가기준이 개발되어 있으며, 다양한 정보보호시스템의 평가를 원활히 하고 국내 정보보호시스템의 수출 활성화를 지원하기 위하여 지난 2002년 8월 5일에 국제표준인 공통평가기준(Common Criteria, CC)을 수용하여 정보통신부고시 제2002-40호 - '정보보호시스템 공통평가기준'을 제정·고시하여 시행하고 있다.

공통평가기준에 의한 평가를 수행하기 위해 개발자는 보안목표명세서(ST, Security Target)와 더불어 공통평가기준에서 등급별로 요구하는 보증요구사항을 문서화하여 평가자에게 제출하여야 하고, 평가자는 이를 기반으로 평가대상제품(TOE, Target of Evaluation)의 평가를 수행하게 된다. 그러나, 공통평가기준에서는 평가제출물에 대한 작성방법을 제공하지 않고 있으므로 개발자가 평가제출물을 작성하는데 어려움이 있다. 개발자는 평가대상제품이 개발이 완료된 후에 평가를 위해 평가제출물을 작성할 수도 있고, 또는 평가대상제품의 개발과 병행하여 평가를 수행하기 위해 평가제출물을 작성할 수도 있다. 평가제출물은 평가대상의 형상을 나타내며 개발자와 평가자들간의 공식적인 대화수단이라고 할 수 있으나 공통평가기준은 특정 개발방법론이나 생명주기 모델을 따르도록 강요하지 않는다. 따라서 공통평가기준에서는 두 경우에 대한 평가제출물 작성순서를 규정하고 있지 않기 때문에 개발자가 평가제출물을 작성하는데 많은 어려움을 야기한다.

본 고에서는 개발자에게 평가제출물 작성시에 활용할 수 있는 평가제출물 작성 방법론으로 순차방식과 병행방식을 제시하여, 개발자가 실제적으로 평가제출물을 작성하는데 참조할 수 있도록 하고자 한다.

본고의 구성은 다음과 같다. 제 2장에서는 정보보호시스템 공통평가기준을 기반으로 EAL4 등급에서 요구하는 평가제출물을 먼저 기술한다. 제 3장에서는 보증컴포넌트간 종속관계를 분석하며 제 4장에서 평

* 한국정보보호진흥원 산업지원단 지원기획팀(jwpark@kisa.or.kr)
** 한국정보보호진흥원 산업지원단 평가2팀(shinhj@kisa.or.kr)
*** 순천향대학교 정보기술공학부(dgpark@sch.ac.kr)
**** 충남대학교 정보통신공학부(jcryou@home.cnu.ac.kr)

가제출물 작성 방법론으로 순차방식과 병행방식을 제시한다. 그리고 마지막으로 제 5장에서 결론을 정리한다.

Ⅱ. 공통평가기준 기반의 평가제출물

공통평가기준의 평가보증등급은 EAL1~EAL7으로 구성된다. 개발자는 해당 평가보증등급에서 요구하는 보증요구사항을 충족시키도록 평가제출물을 작성하여야 한다. 평가자는 평가제출물을 통해 TOE의 형상을 정확히 파악할 수 있으며 평가가 용이해진다. 공통평가기준을 기반으로 EAL4 등급에서 요구하는 평가제출물은 아래와 같다. 보안목표명세서는 평가의 기초가 되며, 평가보증등급에 무관하게 적용되므로 본 고에서는 작성되어 있음을 전제로 하여 평가제출물 작성 방법론에서는 고려하지 않는다.

1. 형상관리문서

TOE 및 관련 정보를 세분화하고 변경하는 과정에서 규칙적이고 체계적인 관리를 통해 TOE의 무결성이 유지됨을 보장하기 위한 문서로, 형상관리(ACM) 클래스의 부분적인 형상관리 자동화(ACM_AUT.1) 컴포넌트와 생성지원 및 수용절차(ACM_CAP.4) 컴포넌트, 형상관리 범위(ACM_SCP.2) 컴포넌트를 포함한다. 형상관리문서는 TOE 버전과 레이블, 형상항목 식별 방법, 형상항목, 형상관리 계획, 수용계획, TOE 구현표현의 자동화된 접근통제 수단과 자동화된 TOE 생성수단을 서술하여야 한다.

2. 배포문서

TOE를 사용자에게 배포하는 과정에 다양한 보안위협요소가 존재할 수 있으므로, TOE가 사용자에게 배포되는 동안에 보안성이 유지됨을 보장하기 위한 문서로, 배포 및 운영(ADO) 클래스의 변경의 탐지(ADO_ DEL.2) 컴포넌트를 포함한다. 배포문서는 배포방법, 배포절차, TOE 식별절차, 전송시 보안유지 절차, 변경이나 불일치 탐지 절차, 위장시도 탐지절차를 서술하여야 한다.

3. 기능명세서

TOE에 의해 제공되는 모든 보안기능과 외부인터페이스를 서술함으로써, 보안목표명세서에 서술된 모든 보안기능요구사항이 TOE에 의해 실체화됨을 보장하기 위한 문서로, 개발(ADV) 클래스 기능명세(ADV_FSP) 패밀리의 완전하게 정의된 외부인터페이스(ADV_FSP.2) 컴포넌트와 표현일치성(ADV_RCR) 패밀리의 비정형적인 표현일치성 시연(ADV_RCR.1) 컴포넌트를 포함한다. 기능명세서는 TOE 보안기능, 외부인터페이스를 서술하고, 보안목표명세서의 TOE 요약명세에 서술된 모든 보안기능과 기능명세서의 보안기능간의 [1]완전함을 보증하는 표현일치성 검증을 서술하여야 한다.

4. 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) 패밀리의 보안기능과 비보안기능을 분리한 기본설계(ADV_HLD.2) 컴포넌트와 표현일치성(ADV_RCR) 패밀리의 비정형적인 표현일치성 시연(ADV_RCR.1) 컴포넌트를 포함한다. 기본설계서는 보안 서브시스템, 기타 서브시스템, 인터페이스를 서술하고, 기능명세서의 보안기능과 기본설계서의 서브시스템간의 완전함을 보증하기 위한 [2]표현 일치성 검증을 서술하여야 한다.

5. 상세설계서

기본설계를 프로그래밍이나 하드웨어 구축시 사용할 수 있도록 상세한 수준(예, 모듈수준)으로 세분화하는 설계 문서로, 상세설계(ADV_LLD) 패밀리의 서술적인 상세설계(ADV_LLD.1) 컴포넌트와 표현일치성(ADV_RCR) 패밀리의 비정형적인 표현일치성 시연(ADV_RCR.1) 컴포넌트를 포함한다. 상세설계서는 보안 모듈, 기타 모듈, 인터페이스를 서술하고, 기본설계서의 서브시스템과 상세설계서의 모듈간의 완전함을 보증하기 위한 표현 일치성 검증을 서술하여야 한다.

---

1 완전한(Complete) - 실체의 모든 필요한 부분이 제공되는 것을 말한다. 문서에서 "완전한"의 의미는 해당 추상화 수준에서는 더 이상의 설명이필요 없는 상세한 수준으로 모든 관련된 정보가 문서에 포함된 것을 말한다.

2 표현 일치성 - TSF의 다양한 표현(즉, TOE 요약명세, 기능명세, 기본설계, 상세설계, 구현표현)간의 일치성은 제공된 가장 구체적인 TSF 표현에 대하여 요구사항이 정확하고 완전하게 실체화 되는지에 대해 다룬다.

6. 구현검증명세서

구현표현이 보안목표명세서의 보안기능요구사항들을 만족하기에 충분하고, 상세설계의 정확한 실체임을 보장하기 위한 문서로, 구현표현(ADV_IMP) 패밀리의 TOE 보안기능의 구현표현 부집합(ADV_IMP.1) 컴포넌트와 표현일치성(ADV_RCR) 패밀리의 비정형적인 표현일치성 시연(ADV_RCR.1) 컴포넌트를 포함한다. 구현검증명세서는 구현표현의 부집합을 서술하고, 상세설계서의 모듈과 구현검증명세서의 구현표현간의 완전함을 보증하기 위한 표현 일치성 검증을 서술하여야 한다.

7. 보안정책모델명세서

TOE 보안정책에 기반한 보안정책모델을 개발하여 기능명세, 보안정책모델간의 일치성을 입증함으로써, 기능명세의 보안기능이 TOE 보안정책을 수행함을 추가적으로 보증하기 위한 문서로, 보안정책모델(ADV_SPM) 패밀리의 비정형적인 보안정책모델(ADV_SPM.1) 컴포넌트를 포함한다. 보안정책모델명세서는 보안정책모델을 서술하고, 기능명세서의 모든 보안기능과 보안정책모델명세서의 보안정책 모델간의 완전함을 서술하여야 한다.

8. 관리자설명서

TOE 보안을 위해 안전하고, 정확한 방식으로 TOE를 구성, 유지, 관리하는데 책임 있는 관리자에게 TOE의 안전한 설치, 생성, 시동 및 안전한 운영을 보장하기 위한 문서로, 배포 및 운영(ADO) 클래스의 설치·생성·시동 절차(ADO_IGS.1) 컴포넌트와 설명서(AGD) 클래스의 관리자 설명서(AGD_ADM.1) 컴포넌트를 포함한다. 관리자 설명서는 안전한 설치·생성·시동절차, 보안기능, 인터페이스, 안전한 운영 방법을 서술하여야 한다.

9. 사용자설명서

관리자가 아닌 TOE 사용자 또는 TOE의 외부인터페이스를 사용하는 사용자에게 TOE의 안전한 사용을 보장하기 위한 문서로, 설명서(AGD) 클래스의 사용자 설명서(AGD_USR.1) 컴포넌트를 포함한다. 사용자 설명서는 보안기능, 인터페이스, 안전한 운영 방법을 서술하여야 한다.

10. 생명주기지원서

TOE 개발 및 유지하는 동안에 TOE에 대한 규칙 및 통제를 수립하여 TOE의 보안성을 보장하기 위한 문서로, 생명주기지원(ALC) 클래스의 보안대책 식별(ALC_DVS.1) 컴포넌트와 개발자가 정의한 생명주기모델(ALC_LCD.1) 컴포넌트, 잘 정의된 개발도구(ALC_TAT.1) 컴포넌트를 포함한다. 생명주기지원서는 물리적·절차적·인적·기타 보안대책, 생명주기 정의, 잘 정의된 개발도구를 서술하여야 한다.

11. 시험서

명세된 TOE 보안기능요구사항과 서브시스템 및 모듈을 그 명세에 따라 시험함으로써, TOE가 최소한의 보안기능요구사항과 적절한 TOE 내부구조를 만족함을 보장하기 위한 문서로, 시험(ATE) 클래스의 시험범위의 분석(ATE_COV.2) 컴포넌트와 기본설계시험(ATE_DPT.1) 컴포넌트, 기능시험(ATE_FUN.1) 컴포넌트를 포함한다. 시험서는 시험계획, 시험절차, 시험결과, 시험분석을 서술하여야 한다.

12. 오용분석서

TOE가 안전하기 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 설명서 분석의 검증(AVA_MSU.2) 컴포넌트를 포함한다. 오용분석서는 관리자 설명서의 오용가능성 분석, 사용자설명서의 오용가능성 분석을 서술하여야 한다.

13. 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) 패밀리의 TOE 보안기능 강도에 대한 평가(AVA_SOF.1) 컴포넌트와 취약성 분석(AVA_VLA) 패밀리의 독립적인 취약성 분석(AVA_VLA.2) 컴포넌트를 포함한다. 취약성분석서는 TOE 보안기능강도 분

석, 개발자에 의한 취약성 분석을 서술하여야 한다.

Ⅲ. 컴포넌트간 종속관계

평가제출물간 일관성 등 공통평가기준에 의한 평가 제출물을 효과적으로 작성하기 위한 작성 방법론 설정 위해서는 보증컴포넌트간 종속관계 분석을 통한 평가 제출물간 연관관계를 도출이 필요하다. 공통평가기준에서 보증 컴포넌트간의 종속관계는 특정 컴포넌트가 독립적으로 충분하지 않아서 다른 컴포넌트에 의존하는 경우에 발생한다. 그러므로 두 개의 컴포넌트가 종속관계에 있다는 표현은 하나의 컴포넌트는 수행 선행조건으로 다른 하나의 컴포넌트가 만족되야 한다는 것을 의미한다. 예를 들면, EAL4 등급에서 요구하는 ADV_HLD(기본설계) 패밀리의 ADV_HLD.2(보안기능과 비보안기능을 분리한 기본설계) 컴포넌트는 ADV_FSP(기능명세) 패밀리의 ADV_FSP.1(비정형화된 기능명세) 컴포넌트와 ADV_RCR(표현일치성) 패밀리의 ADV_RCR:1(비정형화된 일치성 입증) 컴포넌트와 종속관계를 갖는다. 이는 ADV_HLD.2 컴포넌트를 만족하기 위해서는 ADV_FSP.1 컴포넌트와 ADV_RCR.1 컴포넌트가 선행되어 만족되어야 함을 의미한다. 따라서 보안기능과 비보안기능을 분리한 기본설계(ADV_HLD.2)를 하기 위해서는 TOE에 대한 비정형적인 형태의 기능명세(ADV_FSP.1)가 이루어져야 하고, 기능명세에 서술된 보안기능과 보안목표명세서의 TOE 요약명세에 서술된 TOE 보안기능간의 비정형적인 형태의 일치성 시연이 이루어져야 한다.

특정 컴포넌트와 종속관계에 있는 컴포넌트들도 역시 다른 컴포넌트와 종속관계를 가질 수 있으므로 특정 컴포넌트와 종속관계에 있는 컴포넌트들은 하나 또는 그 이상이 될 수 있다. 하나 이상일 경우에 특정 컴포넌트와 종속관계에 있는 보증 컴포넌트들의 집합을 종속관계 목록이라 한다.[1]

종속관계 목록에 제시된 컴포넌트와 계층관계를 가지는 컴포넌트들도 특정 컴포넌트에 대한 종속관계를 만족시키기 위해 사용될 수 있다. 같은 보증 패밀리에 속하는 컴포넌트간에는 하위 레이블을 갖는 컴포넌트는 상위 레이블을 갖는 컴포넌트와 계층관계를 갖기 때문에, 상위 레이블을 갖는 컴포넌트가 하위 레이블을 갖는 컴포넌트를 포함한다. 그러므로 상위 레이블을 갖는 컴포넌트와 종속관계를 가지면 하위 레이블을 갖는 컴포넌트와도 종속관계를 만족한다고 할 수 있다. 예를 들어 EAL4에서 ADV_HLD.2 컴포넌트는 ADV_FSP.1 컴포넌트와 종속관계를 갖는다. ADV_FSP.2 컴포넌트와 ADV_FSP.1 컴포넌트는 계층관계를 이루고 있으므로, ADV_FSP.2 컴포넌트가 ADV_FSP.1 컴포넌트를 포함한다. 그러므로 EAL4 등급에서 ADV_HLD.2 컴포넌트의 종속관계에 의해서 ADV_FSP.1 컴포넌트를 요구하지만, EAL4 등급에서 ADV_FSP.2를 요구하기 때문에 별도로 ADV_FSP.1 컴포넌트를 요구할 필요는 없다.

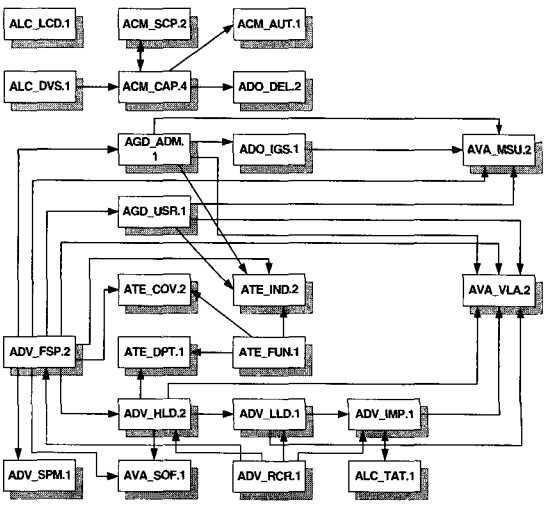
EAL 등급에서 컴포넌트간의 종속관계는 개발자가 별도로 고려하지 않아도 된다. EAL 등급은 등급에 적합한 보증요구사항들을 패키지로 묶은 집합이므로, 등급별 패키지는 컴포넌트간의 종속관계를 모두 고려하여 구성되어 있다. 그러나 등급 외로 새로운 컴포넌트가 추가되었거나, 등급에서 요구하는 컴포넌트 수준보다 높은 컴포넌트 수준을 요구할 경우에 추가(Augmentation)된 컴포넌트에 대한 종속관계는 완전하게 만족시켜야 하기 때문에 참조되어야 한다.

컴포넌트간의 종속관계를 분석 시에 고려해야할 사항은 다음과 같다.

첫째, 보증컴포넌트는 동일 패밀리내에서 상위 보증컴포넌트가 하위 보증컴포넌트를 계층관계에 의해 포함한다.

둘째, 표현일치성(ADV_RCR) 패밀리의 비정형적인 일치성 시연(ADV_RCR.1) 컴포넌트는 관련된 기본설계, 상세설계, 구현표현 패밀리에 포함시킨다.

〔그림 1〕은 앞에서 설명된 고려사항이 포함된 EAL4 등급의 컴포넌트간 종속관계를 도식화한 그림이다.



〔그림 1〕 EAL4 등급의 컴포넌트간 종속관계

1. 형상관리 클래스

1.1 부분적인 형상관리 자동화(ACM_AUT.1)

부분적인 형상관리 자동화(ACM_AUT.1) 컴포넌트는 형상관리 능력(ACM_CAP) 패밀리의 권한 통제(ACM_CAP.3) 컴포넌트와 종속관계를 갖는다.

1.2 생성지원 및 승인절차(ACM_CAP.4)

생성지원 및 승인절차(ACM_CAP.4) 컴포넌트는 형상관리 범위(ACM_SCP) 패밀리의 문제추적 형상관리 범위(ACM_SCP.2) 컴포넌트와 생명주기지원(ALC) 개발 보안(ALC_DVS) 패밀리의 보안대책의 식별(ALC_DVS.1) 컴포넌트와 종속관계를 갖는다.

1.3 문제추적 형상관리 범위(ACM_SCP.2)

문제추적 형상관리 범위(ACM_SCP.2) 컴포넌트는 형상관리 능력(ACM_CAP) 패밀리의 권한 통제(ACM_CAP.3) 컴포넌트와 종속관계를 갖는다.

2. 배포와 운영 클래스

2.1 변경의 탐지(ADO_DEL.2)

변경의 탐지(ADO_DEL.2) 컴포넌트는 형상관리 능력(ACM_CAP) 패밀리의 권한 통제(ACM_CAP.3) 컴포넌트와 종속관계를 갖는다.

2.2 설치 · 생성 · 시동 절차(ADO_IGS.1)

설치 · 생성 · 시동 절차(ADO_IGS.1) 컴포넌트는 관리자설명서(AGD_ADM) 패밀리의 관리자설명서(AGD_ADM.1) 컴포넌트와 종속관계를 갖는다.

3. 개발 클래스

3.1 완전하게 정의된 외부인터페이스(ADV_FSP.2)

기능명세(ADV_FSP) 패밀리의 완전하게 정의된 외부인터페이스(ADV_FSP.2) 컴포넌트는 표현일치성(ADV_RCR) 패밀리의 비정형적인 일치성 시연(ADV_RCR.1) 컴포넌트와 종속관계를 갖는다.

3.2 보안기능과 비보안기능을 분리한 기본설계(ADV_HLD.2)

기본설계(ADV_HLD) 패밀리의 보안기능과 비보안기능을 분리한 기본설계(ADV_HLD.2) 컴포넌트는 기능명세(ADV_FSP) 패밀리의 비정형적인 기능명세(ADV_FSP.1) 컴포넌트와 표현일치성(ADV_RCR) 패밀리의 비정형적인 일치성 시연(ADV_RCR.1) 컴포넌트와 종속관계를 갖는다.

3.3 TOE 보안기능의 구현표현 부집합(ADV_IMP.1)

구현표현(ADV_IMP) 패밀리의 TOE 보안기능의 구현표현 부집합(ADV_IMP.1) 컴포넌트는 상세설계(ADV_LLD) 패밀리의 서술적인 상세설계(ADV_LLD.1) 컴포넌트와 표현일치성(ADV_RCR) 패밀리의 비정형적인 일치성 시연(ADV_RCR.1) 컴포넌트와 생명주기지원(ALC) 클래스 도구와 기법(ALC_TAT) 패밀리의 잘 정의된 개발도구(ALC_TAT.1) 컴포넌트와 종속관계를 갖는다.

3.4 서술적인 상세설계(ADV_LLD.1)

상세설계(ADV_LLD) 패밀리의 서술적인 상세설계(ADV_LLD.1) 컴포넌트는 기본설계(ADV_HLD) 패밀리의 보안기능과 비보안기능을 분리한 기본설계(ADV_HLD.2) 컴포넌트와 표현일치성(ADV_RCR) 패밀리의 비정형적인 일치성 시연(ADV_RCR.1) 컴포넌트와 종속관계를 갖는다.

3.5 비정형적인 일치성 시연(ADV_RCR.1)

표현일치성(ADV_RCR) 패밀리의 비정형적인 일치성 시연(ADV_RCR.1) 컴포넌트는 종속관계를 갖는 컴포넌트가 없다.

3.6 비정형적인 TOE 보안정책 모델(ADV_SPM.1)

보안정책 모델링(ADV_SPM) 패밀리의 비정형적인 TOE 보안정책 모델(ADV_SPM.1) 컴포넌트는 기능명세(ADV_FSP) 패밀리의 비정형적인 기능명세(ADV_FSP.1) 컴포넌트와 종속관계를 갖는다.

4. 설명서 클래스

4.1 관리자 설명서(AGD_ADM.1)

관리자 설명서(AGD_ADM) 패밀리의 관리자 설명서(AGD_ADM.1) 컴포넌트는 개발(ADV) 클래스 기능명세(ADV_FSP) 패밀리의 비정형적인 기능명세(ADV_FSP.1) 컴포넌트와 종속관계를 갖는다.

4.2 사용자 설명서(AGD_USR.1)

사용자 설명서(AGD_USR) 패밀리의 사용자 설명서(AGD_USR.1) 컴포넌트는 개발(ADV) 클래스 기능명세(ADV_FSP) 패밀리의 비정형적인 기능명세(ADV_FSP.1) 컴포넌트와 종속관계를 갖는다.

5. 생명주기지원 클래스

5.1 보안대책 식별(ALC_DVS.1)

개발보안(ALC_DVS) 패밀리의 보안대책 식별(ALC_DVS.1) 컴포넌트는 종속관계를 갖는 컴포넌트는 없다.

5.2 개발자가 정의한 생명주기모델(ALC_LCD.1)

생명주기정의(ALC_LCD) 패밀리의 개발자가 정의한 생명주기모델(ALC_LCD.1) 컴포넌트는 종속관계를 갖는 컴포넌트는 없다.

5.3 잘 정의된 개발도구(ALC_TAT.1)

도구와 기법(ALC_TAT) 패밀리의 잘 정의된 개발도구(ALC_TAT.1) 컴포넌트는 구현표현(ADV_IMP) 패밀리의 TOE 보안기능의 구현표현 부집합(ADV_IMP.1) 컴포넌트와 종속관계를 갖는다.

6. 시험 클래스

6.1 시험범위 분석(ATE_COV.2)

시험범위(ATE_COV) 패밀리의 시험범위 분석(ATE_COV.2) 컴포넌트는 기능명세(ADV_FSP) 패밀리의 비정형적인 기능명세(ADV_FSP.1) 컴포넌트와 기능시험(ATE_FUN) 패밀리의 기능시험(ATE_FUN.1) 컴포넌트와 종속관계를 갖는다.

6.2 기본설계 시험(ATE_DPT.1)

시험깊이(ATE_DPT) 패밀리의 기본설계 시험(ATE_DPT.1) 컴포넌트는 기본설계(ADV_HLD) 패밀리의 서술적인 기본설계(ADV_HLD.1) 컴포넌트와 기능시험(ATE_FUN) 패밀리의 기능시험(ATE_FUN.1) 컴포넌트와 종속관계를 갖는다.

6.3 기능시험(ATE_FUN.1)

기능시험(ATE_FUN) 패밀리의 기능시험(ATE_FUN.1) 컴포넌트는 종속관계를 갖는 컴포넌트는 없다.

6.4 샘플링을 통한 독립시험(ATE_IND.2)

독립시험(ATE_IND) 패밀리의 샘플링을 통한 독립시험(ATE_IND.2) 컴포넌트는 기능명세(ADV_FSP) 패밀리의 서술적인 기능명세(ADV_FSP.1) 컴포넌트와 관리자 설명서(AGD_ADM) 패밀리의 관리자 설명서(AGD_ADM.1) 컴포넌트와 사용자 설명서(AGD_USR)의 사용자 설명서(AGD_USR.1) 컴포넌트와 기능시험(ATE_FUN) 패밀리의 기능시험(ATE_FUN.1) 컴포넌트와 종속관계를 갖는다.

7. 취약성 평가 클래스

7.1 분석 검증(AVA_MSU.2)

오용분석(AVA_MSU) 패밀리의 분석 검증(AVA_MSU.2) 컴포넌트는 배포와 운영(ADO) 클래스 설치·생성·시동(ADO_IGS) 패밀리의 설치·생성·시동 절차(ADO_IGS.1) 컴포넌트와 개발(ADV) 클래스 기능명세(ADV_FSP) 패밀리의 서술적인 기능명세(ADV_FSP.1) 컴포넌트와 설명서(AGD) 클래스 관리자 설명서(AGD_ADM) 패밀리의 관리자 설명서(AGD_ADM.1) 컴포넌트와 사용자 설명서(AGD_USR) 패밀리의 사용자 설명서(AGD_USR.1) 컴포넌트와 종속관계를 갖는다.

7.2 TOE 보안기능강도 평가(AVA_SOF.1)

보안기능강도분석(AVA_SOF) 패밀리의 TOE 보안기능강도 평가(AVA_SOF.1) 컴포넌트는 기능명세

(ADV_FSP) 패밀리의 서술적인 기능명세(ADV_FSP.1) 컴포넌트와 기본설계(ADV_HLD) 패밀리의 서술적인 기본설계(ADV_HLD.1) 컴포넌트와 종속관계를 갖는다.

7.3 독립적인 취약성 분석(AVA_VLA..2)

취약성 분석(AVA_VLA) 패밀리의 독립적인 취약성 분석(AVA_VLA.2) 컴포넌트는 개발(ADV) 클래스 기능명세(ADV_FSP) 패밀리의 서술적인 기능명세(ADV_FSP.1) 컴포넌트와 기본설계(ADV_HLD) 패밀리의 보안기능과 비보안기능을 분리한 기본설계(ADV_HLD.2) 컴포넌트와 구현표현(ADV_IMP) 패밀리의 TOE 보안기능의 구현표현 부집합(ADV_IMP.1) 컴포넌트와 상세설계(ADV_LLD) 패밀리의 서술적인 상세설계(ADV_LLD.1) 컴포넌트와 설명서(AGD) 클래스 관리자 설명서(AGD_ADM) 패밀리의 관리자 설명서(AGD_ADM.1) 컴포넌트와 사용자 설명서(AGD_USR) 패밀리의 사용자 설명서(AGD_USR.1) 컴포넌트와 종속관계를 갖는다.

Ⅳ. 평가제출물 작성 방법론

위에서 분석한 EAL4 등급에서 컴포넌트간의 종속관계를 고려하여 다음과 같은 두 개의 평가제출물 작성 방식을 제안한다.

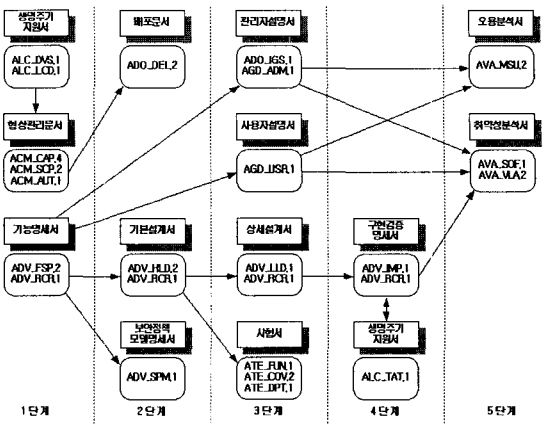
첫째, TOE가 개발된 후에 평가제출물을 작성할 경우에 적용되는 순차방식으로 컴포넌트간의 종속관계에 의한 평가제출물을 작성한다.

둘째, TOE 개발과 동시에 평가제출물을 작성할 경우에 적용되는 병행방식으로 컴포넌트간의 종속관계와 소프트웨어 생명주기를 고려하여 평가제출물을 작성한다.

1. 순차 방식

순차 방식은 정보보호시스템을 개발한 후에 평가를 받기 위해 개발자가 평가제출물을 작성할 경우에 적용할 수 있는 방식이다. 이 방식은 정보보호시스템의 개발 공정과는 무관하게 평가제출물이 작성되므로, 결정된 등급에서 요구하는 보증 컴포넌트들간의 종속관계에 의해 평가제출물 작성 순서가 결정된다.

〔그림 2〕는 평가제출물 작성을 위한 순차 방식을 표현한다. 순차방식은 다섯 단계로 구성되어 있고, 각 단계별로 작성되어야 할 요구사항은 다음과 같다.



〔그림 2〕 순차 방식

첫째, 1단계에서는 생명주기지원의 ALC_DVS.1 컴포넌트, ALC_LCD.1 컴포넌트와 형상관리의 ACM_CAP.4 컴포넌트, ACM_SCP.2 컴포넌트, ACM_AUT.1 컴포넌트와 기능명세의 ADV_FSP.2 컴포넌트, ADV_RCR.1 컴포넌트에 대한 요구사항을 작성한다. 생명주기지원은 TOE 설계 및 구현 과정에서의 비밀성 및 무결성을 보호하기 위해 개발 환경에서 사용될 수 있는 물리적, 인적, 절차적, 기타 보안대책과 개발자가 TOE 개발에 사용한 생명주기 모델에 대해 요구한다. 형상관리는 평가 시 모호함이 없도록 TOE 버전과 레이블을 요구하고, 형상관리계획, 형상관리를 수행해야 하는 형상항목, TOE 생성(Generation) 및 형상항목이 변경되거나 새로 생성될 경우에 TOE 일부로 수용하는데 사용된 절차를 요구한다. 또한 TOE 구현표현에 인가된 변경만이 일어날 수 있도록 하는 자동화된 접근통제수단과 TOE 생성을 지원하는 자동화된 도구를 요구한다. 기능명세는 TOE에 의해 제공되는 TOE 보안기능과 완전하게 정의된 외부인터페이스를 요구한다.

둘째, 2단계에서는 배포의 ADO_DEL.2 컴포넌트와 기본설계의 ADV_HLD.2 컴포넌트, ADV_RCR.1 컴포넌트와 보안정책모델의 ADV_SPM.1 컴포넌트에 대한 요구사항을 작성한다. 배포는 TOE를 안전하게 배포할 수 있는 모든 과정을 요구하고, 배포에서 발생할 수 있는 변경이나 불일치를 탐지하기 위한 다양한 절차와 기술적인 수단을 요구하며, 개발자로 위장된 배포 시도를 탐지하기 위한 다양한 절차를 요구한다. 기본설계는 1단계에서 작성된 기능명세를 바탕으로 TOE를 보안 서브시스템과 비 보안 서브시스템으로 분리하여 서술하고, 각 서브시스템이 제공하는 보안기

능성과 인터페이스를 서술한다. 보안정책모델은 1단계에서 작성된 기능명세를 바탕으로 모델링 가능한 TOE 보안정책의 규칙과 특성을 비정형화된 방식으로 작성할 것을 요구한다.

셋째, 3단계에서는 상세설계의 ADV_LLD.1 컴포넌트, ADV_RCR.1 컴포넌트와 관리자 설명서의 ADO_IGS.1 컴포넌트, AGD_ADM.1 컴포넌트와 사용자 설명서의 AGD_USR.1 컴포넌트와 시험의 ATE_COV.2 컴포넌트, ATE_DPT.1 컴포넌트, ATE_FUN.1 컴포넌트에 대한 요구사항을 작성한다. 상세설계는 2단계에서 작성된 기본설계를 바탕으로 서브시스템을 보안 모듈과 비 보안 모듈로 분리하여 서술할 것을 요구하고, 각 모듈이 제공하는 보안기능성과 인터페이스를 요구한다. 관리자 설명서는 기능명세서에 서술된 TOE 보안기능 중 TOE의 안전한 운영을 위해 관리자가 사용할 수 있는 보안기능과 인터페이스를 요구하고, TOE를 안전한 방식으로 관리하는 방법을 요구한다. 또한 관리자가 TOE를 안전하게 설치·생성·시동할 수 있는 절차를 요구한다. 사용자 설명서는 기능명세에 서술된 TOE 보안 기능 중 사용자가 TOE를 안전하게 사용하기 위해 필요한 보안기능과 인터페이스를 요구하고, 또한 TOE를 안전한 방식으로 사용하는 방법을 요구한다. 시험은 기능명세에 서술된 모든 TOE 보안기능이 명세된 대로 수행됨을 보이기 위해 시험을 수행하고, 시험을 수행하기 위한 시험계획, 시험절차, 예상 시험결과와 실제 시험결과를 요구하고, 기능명세에 서술된 모든 보안기능이 시험되었는지를 분석하고, 기본설계에 서술된 TOE 서브시스템이 올바르게 구현되었음을 보증하기 위해 기본설계에 서술된 모든 서브시스템이 시험되었는지에 대한 분석을 요구한다.

넷째, 4단계에서는 구현표현의 ADV_IMP.1 컴포넌트, ADV_RCR.1 컴포넌트와 생명주기지원의 ALC_TAT.1 컴포넌트에 대한 요구사항을 작성한다. 구현표현은 3단계에서 작성된 상세설계를 바탕으로 개발자가 실제 구현한 소스코드, 하드웨어 도면 등을 부분적으로 요구하고, 생명주기지원은 TOE 개발을 위해 사용된 잘 정의된 개발도구를 요구한다.

다섯째, 5단계에서는 오용분석의 AVA_MSU.2 컴포넌트와 취약성 분석의 AVA_SOF.1 컴포넌트, AVA_VLA.2 컴포넌트에 대한 요구사항을 작성한다. 오용분석은 3단계에서 작성된 관리자 설명서, 사용자 설명서를 바탕으로 설명서에 오용 가능한 부분이 있는지를 분석할 것을 요구하고, 취약성분석은 보안기능을 구현하기 위해 사용된 보안 메커니즘의 강도에 대한 분석을 요구하고, TOE의 명백한 취약성이 악용될 수 없음을 분석한다.

2. 병행 방식

병행 방식은 개발자가 정보보호시스템의 개발과 병행하여 평가를 수행하기 위해 평가제출물을 작성할 경우에 적용될 수 있는 방식이다. 공통평가기준은 설계를 하는데 있어 특정 표현방식을 강요하지는 않지만 보증 기준은 기능명세, 기본설계, 상세설계, 구현 등으로 설계의 추상화 단계를 식별한다. 따라서 보증등급에 따라 개발자는 개발방법론이 공통평가기준 보증요구사항을 어떻게 만족시키는지 보여야 한다. 이 방식은 정보보호시스템의 생명주기에 속하는 개발 공정의 각 단계와 보증 컴포넌트간의 관계를 고려하고, 또한 보증 컴포넌트간의 종속관계를 고려하여 평가제출물을 작성하는 방식으로, 이런 두 가지 요인을 분석하여 평가제출물 작성 순서가 결정되고, 개발자는 정보보호시스템 개발과 병행하여 평가제출물을 작성한다.

소프트웨어 생명주기 모델 중에서 폭포수 모형은 개발자에 의해 수행되는 개발 공정을 크게 5단계로 분류하고 있다. 폭포수 모형의 개발 공정은 요구사항 분석, 설계, 구현, 시험, 유지보수이다.[2] 개발자가 정보보호시스템 개발에 폭포수 모형과 같은 일반적인 소프트웨어 개발 공정을 사용한다고 가정하고, 각 개발 공정단계와 공통평가기준에서 요구하는 보증 요구사항과의 관계를 분석하면 다음과 같다.

첫째, 요구사항 분석단계에서 개발자는 정보보호시스템을 개발하기 위하여 보호프로파일에서 사용자 요구사항(보안환경, 보안목적, 기능요구사항)을 인식하고, 보안목표명세서에서 사용자 요구사항에 맞는 정보보호시스템의 보안기능과 보증수단을 정의한다. 이를 기반으로 실질적으로 정보보호시스템이 구현하여야 하는 보안기능을 나열하는 기능명세를 수행한다. 그러므로 요구사항 분석단계에서는 공통평가기준의 기능명세(ADV_FSP)를 포함한다.

둘째, 설계 단계에서 개발자는 전체적인 구조를 파악할 수 있는 기본설계를 수행한다. 기본설계는 논리적인 서브시스템 단위로 정보보호시스템 구조를 설계한다. 또한 개발자는 기본설계를 바탕으로 모듈단위의 설계를 수행한다. 그러므로 설계 단계에서는 공통평가기준의 기본설계(ADV_HLD)와 상세설계(ADV_LLD)를 포함한다.

셋째, 구현 단계에서 개발자는 설계단계에서 도출된 논리적인 산출물을 가지고 잘 정의된 프로그래밍 언어를 통해 정보보호시스템을 구현한다. 그러므로 구현 단계에서는 공통평가기준의 구현표현(ADV_IMP)을 포함한다.

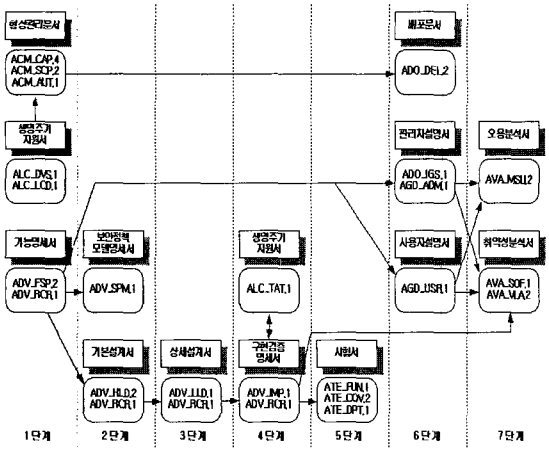
넷째, 시험 단계에서 개발자는 구현된 정보보호시스템이 기능명세에서 정의한 모든 보안기능을 수행하는지, 기본설계 및 상세설계에서 서술된 부분과 동일하게 구현되었는지를 시험한다. 그러므로 시험 단계에서는 공통평가기준의 시험(ATE)을 포함한다.

다섯째, 유지보수 단계에서 개발자는 구현된 정보보호시스템에 대해 유지보수를 수행한다. 이 부분은 공통평가기준 요구사항으로 보증유지(AMA)가 존재하지만 평가보증등급에 실제적으로 적용되고 있지는 않다.

이런 소프트웨어 개발 공정을 통해 정보보호시스템이 개발되면, 개발자는 개발된 정보보호시스템의 배포, 설명서, 오용분석, 취약성 분석에 대한 사항을 고려하여 평가제출물을 작성한다.

〔그림 3〕은 평가제출물 작성을 위해 보증컴포넌트 간의 종속관계 분석과 소프트웨어 생명주기를 고려한 병행 방식을 표현한 것으로, 일곱단계로 구성되어 있고, 각 단계별로 작성되어야 할 요구사항은 다음과 같다.

첫째, 1단계에서는 생명주기지원의 ALC_DVS.1 컴포넌트, ALC_LCD.1 컴포넌트와 형상관리의ACM_CAP.4 컴포넌트, ACM_SCP.2 컴포넌트, ACM_AUT.1 컴포넌트와 기능명세의 ADV_FSP.2 컴포넌트, ADV_RCR.1 컴포넌트에 대한 요구사항을 작성한다. 각 해당 컴포넌트에서 요구하는 자세한 사항은 순차 방식의 내용을 참조한다.



〔그림 3〕 병행 방식

둘째, 2단계에서는 기본설계의 ADV_HLD.2 컴포넌트, ADV_RCR.1 컴포넌트와 보안정책모델의 ADV_SPM.1 컴포넌트에 대한 요구사항을 작성한다.

셋째, 3단계에서는 상세설계의 ADV_LLD.1 컴포넌트, ADV_RCR.1 컴포넌트에 대한 요구사항을 작성한다.

넷째, 4단계에서는 구현표현의 ADV_IMP.1 컴포넌트, ADV_RCR.1 컴포넌트와 생명주기지원의ALC_TAT.1 컴포넌트에 대한 요구사항을 작성한다.

다섯째, 5단계에서는 시험의 ATE_COV.2 컴포넌트, ATE_DPT.1 컴포넌트, ATE_FUN.1 컴포넌트에 대한 요구사항을 작성한다.

여섯째, 6단계에서는 배포의 ADO_DEL.2 컴포넌트, 관리자설명서의 ADO_IGS.1 컴포넌트, AGD_ADM.1 컴포넌트와, 사용자설명서의 AGD_USR.1 컴포넌트에 대한 요구사항을 작성한다.

일곱째, 7단계에서는 오용분석의 AVA_MSU.2 컴포넌트, 취약성분석의 AVA_SOF.1 컴포넌트, AVA_VLA.2 컴포넌트에 대한 요구사항을 작성한다.

V. 결론 및 향후 연구방향

본 고에서는 정보보호시스템의 평가를 수행하기 위해 개발자가 작성하는 평가제출물에 대한 작성방법론을 순차방식과 병행방식으로 제시하였다. 순차방식은 평가대상제품이 개발된 후에 수행하는 방법이며, 병행방식은 평가대상제품의 개발과 병행하여 수행하는 방식이다.

향후, 제시된 방법론을 기반으로 각 단계별로 요구하는 보증 컴포넌트의 요구사항 분석을 바탕으로 개발자가 효율적으로 평가제출물을 작성할 수 있도록 평가제출물에 대한 탬플릿 개발이 필요하다.

참고문헌

〔1〕 정보통신부고시 제2002-40호, 정보보호시스템 공통평가기준, 2002. 8. 5
〔2〕 윤청, 성공적인 소프트웨어 개발 방법론, 2002. 2. 1, 생능 출판사
〔3〕 정보보호뉴스 2002년 9월호 통권 60호
〔4〕 공통평가기준 기반의 평가제출물 작성지침, 한국정보보호진흥원, 2002.12.
〔5〕 한국정보보호진흥원, 산업지원, http://www.kisa.or.kr

〈著 者 紹 介〉

박 진 완 (Jin-Wan Park)

1999년 2월 : 한국항공대학교 항공통신정보공학과(공학사)
2001년 2월 : 한국항공대학교 항공통신정보공학과(공학석사)
2001년~현재 : 한국정보보호진흥원 지원기획팀 연구원
〈관심분야〉 네트워크 보안, 공통평가방법론, 프로세스 기반 보증성 평가

신 화 종 (Hwa-Jong Shin)
정회원

1999년 2월 : 세종대학교 전산과학과(이학사)
2001년 2월 : 세종대학교 전산학과 (이학석사)
2001년~현재 : 한국정보보호진흥원 평가2팀 연구원
〈관심분야〉 네트워크 보안, 소프트웨어 공학, 무선 통신 보안

박 동 규 (Dong-Gue Park)
종신회원

1988년 2월 : 한양대학교 전자공학과 (공학석사)
1992년 2월 : 한양대학교 전자공학과 (공학박사)
1992년~현재 : 순천향대학교 부교수
〈관심분야〉 시스템 보안, 공통평가 방법론, ubiquitous 보안

류 재 철 (Jae-Cheol Ryou)
종신회원

1985년 2월 : 한양대학교 산업공학과 졸업
1988년 5월 : Iowa State Univ. 전산학 석사
1990년 8월 : northwestern Univ. 전산학 박사
1991년 2월~현재 : 충남대학교 정보통신공학부 교수
관심분야 : 인터넷 보안