情 報 保 護 學 會 誌
第 14 券 第 1 號, 2004. 2

복합 기능을 갖는 정보보호 제품의 보호 프로파일 개발을 위한 평가 방법론 고찰

서 대 희*, 이 임 영*, 정 지 훈**, 채 수 영**

요 약

세계 각국은 산업 및 정보의 의존성에 의해 모든 정보를 한눈에 볼 수 있는 시대로 변모하였으며, 사이버 공간 그 자체가 정치, 경제사회, 문화 등의 기본적인 생활 공간으로 자리매김 하고 있다. 따라서 사이버 공간을 보호하지 않을 경우 안정된 정보사회 구축은 불가능하다. 특히, 정보보호의 대상이 특정 국가적인 정보 보안에 국한되지 않고 기업 및 사회의 정보등으로 확대되고 있어, 국가적으로 국가 안보 뿐만 아니라 개인의 정보보호를 위한 새로운 제도와 조치가 절실히 요구되는 시점이다.

따라서 본 고에서는 복합 기능을 갖는 정보보호 제품의 보호 프로파일 개발을 위한 기반 연구로 요구되는 대체 평가 방법론에 대해 고찰해 보고자한다. 특히 북미를 중심으로 표준화가 진행중에 있는 CEM을 기준으로, 영국을 중심으로 유럽의 적합성 표준으로 추진중에 있는 SCT와 ISO/IEC에서 제시되고 있는 적합성 테스트 방법론인 ISO/IEC 9496 및 보증 프레임워크인 ISO/IEC 15443에 대한 자체 취약성 분석을 수행하고, 각각의 평가 방법론간의 상호 연관성과 비교 분석을 통해 복합 기능을 갖는 정보보호 제품의 보호 프로파일 개발의 가이드라인을 제시하고자 한다.

Ⅰ. 서 론

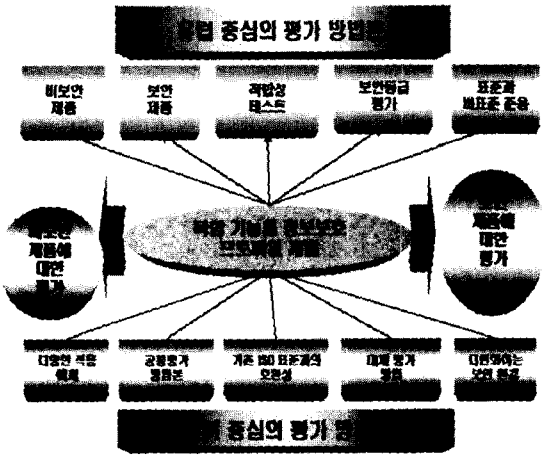
최근 정보보호에 대한 인식이 제고되는 상황에서, 정보보호 제품이 관련 표준에 적합하게 구현되었는지를 확인하는 적합성 시험의 중요성이 커지고 있다. 적합성 시험이란 관련 표준에 따라서 설계되고 구현되었는지를 확인하는 시험으로, 구현물이 표준에 규정된 대로 기능하고 동작한다는 것을 보증해준다. 이러한 적합성은 시스템의 확장시 상호운용을 위한 전제조건이 되어, 시스템의 도입 시에 반드시 고려하여야 하는 항목중의 하나가 되고 있다.

그러나 적합성 시험의 경우에는 대상 제품이 표준을 얼마나 정확하게 구현하였는지를 확인하기 때문에, 보안성이나 표준 자체의 취약성, 설계 및 구현 시에 발생 가능한 오류에 대해서는 확인할 수 없다는 한계를 가진다.

복합 보호프로파일의 경우 보안성에 대한 시험 평가뿐만 아니라 컴포넌트 자체의 표준 적합성에 대한 시험이 반드시 요구되는 실정이다. 이는 보안 제품이 제공하고 있는 보안 서비스뿐만 아니라 사용자가 요구하는 보안 서비스의 만족도를 충족시켜야 하기 때문이다. 따라서 유럽 평가기준인 ITSEC(Information Technology Security Evaluation Criteria), 미국이 주도적인 표준화를 추진하고 있는 CEM(Common Evaluation Methodology) 보안 보증평가에 관련된 내용뿐만 아니라 각각의 컴포넌트에 대한 표준 적합성 테스트가 반드시 요구되는 실정이다. 이는 보안 보증 평가만을 수행할 경우 보안성 시험 평가에만 한정하지 않고 정보보호 제품에 대한 컴포넌트 테스트를 동시에 수행함으로써 보다 사용자 중심의 안전한 서비스를 제공할 수 있다.

따라서 이 두 가지 방법을 적절히 보완하여 표준 적합성을 시험하고, 시험절차에서 표준 자체의 취약성이나 설계, 구현 시 발생 가능한 오류, 보안 취약성을

* 순천향대학교 정보기술공학부({patima, imylee}@sch.ac.kr)
** 국가보안기술 연구소({jihoon, sychae}@etri.re.kr)



〔그림 1〕 대체 평가 방법 분석의 필요성

찾으려는 노력이 필요하다. 또한 이렇게 발견된 오류나 취약성을 해당 표준에 반영되고, 이 표준에 따라 제품이 개발되면, 결국에는 보다 높은 신뢰성을 가지는 정보보호 제품과 해당 표준을 얻을 수 있게 된다.

따라서 본 고에서는 보증 평가 방법론인 CEM, ISO/IEC 9496, SCT(Strict Conformance Test) 뿐만 아니라 보증 프레임워크를 기반으로 기존 평가 제품에 대한 다양한 평가 방식을 채택한 ISO/IEC 15443의 분석을 통해 보증 평가 방법론과 컴포넌트 평가 방법론의 연관성을 분석하고 복합 보호 프로파일 개발을 위한 평가 방법론 및 대체 평가 방법론의 취약성을 분석하고자 한다.

II. 본 론

본 장에서는 국제적으로 연구되고 있는 평가 방법론중 국제 공통 평가 방법론을 비롯하여 ISO/IEC 9496, SCT, ISO/IEC 15443에 대한 개요를 살펴보고, 각 방법론에 대한 분석을 통해 복합 기능을 갖는 정보보호 프로파일을 평가하기 위한 기반 연구를 수행한다.

1. 적합성 시험의 개요

일반적으로 적합성 시험은 구현물이 표준이나 명세를 얼마나 충실하게 따르고 있는가를 알아내는 시험으로 정의된다. 적합성에 대한 요구사항이나 기준은 표준 또는 명세에 정의되어 있으며, 이는 적합성 조항(Conformance Clause)이나 적합성 명세서(Conformance Statement)등의 형태로 표현된다.

적합성에 대한 일반적인 정의는 특정 표준마다 다르게 정의되어 왔으며, "적합도(Conformity)"가 적합성과 같은 의미로 사용되고 있다. 1991년 ISO/IEC DIS(Draft International Standard) 10641에서는 적합성 시험을 "구현된 실체 즉 구현물의 표준에 대한 충실도(Fidelity)를 평가하는 시험"으로 정의하였으며, ISO/IEC TR(Technical Report) 13233에서는 적합도를 "적합성에 대한 요구사항이 의미 있게 명시된 모든 프로세스나 서비스를 만족시키는 것"으로 정의하고 있다. 1996년에 발행된 ISO/IEC 가이드 2에서는 적합성 분야에서 사용되는 3개의 주요 용어들에 대하여 다음과 같이 정의하고 있다.

- 적합도 (Conformity) : 명시된 요구사항에 대한 프로세스나 서비스에 대한 제품의 충실도
- 적합도 평가(Conformity Assessment) : 관련 요구사항들이 직/간접적으로 만족되는가를 판단하는 것과 관련된 활동
- 적합도 시험(Conformity Testing) : 시험에 의한 적합성 평가

적합성 시험은 개발자들이 개발 초기 단계에서부터 그들의 구현물에 대한 품질개선에 이르기까지의 전 절차에서 사용하고, 또 시험 및 인증 프로그램을 주관하는 협회에서도 사용한다. 이는 적합성 시험을 이용하는 이용자들이 그들의 제품이 적합성을 가진다는 것을 확신하거나 제품이 예측한 대로 동작하고 알려진 방법대로 기능을 수행하거나, 알려진 인터페이스 또는 형식을 가지고 있음을 보장하는데 사용한다. 적합성 시험은 해당 제품이 다른 것에 비하여 우수하다는 것을 판단하는 방법이 아니라, 제품이 표준이나 명세의 기준을 따르는가를 판단하는 수단이다. 따라서 적합성 시험의 결과는 시험 목적에 따라서 다양한 의미로 해석될 수 있다.

표준 명세에는 적합성에 대한 조항들이 명시되어 있다. 각 조항은 구현자와 응용 개발자들에게 요구하고 있는 내용들을 서술하며, 임의의 기능에 대한 최소한의 요구사항과 구현에 관련된 값들에 대한 최소의 요구사항들을 프로파일과 같은 형태로 명시한다. 프로파일은 특정 사용자 집단의 요구사항들을 만족시키는데 필요한 기능들을 포함하고 있다. 명세는 여러 기준에 의하여 여러 개의 부분집합으로 분류될 수 있으며, 각 부분집합은 프로파일이 될 수 있다. 표준의 내용은 필수적인 것(Mandatory)과 선택적인 것(Optional)

〔표 1〕 ISO/IEC 9646과 X.290 표준문서의 관계

ISO/IEC	ITU-T	내용
9496-1	X.290	General concepts
9496-2	X.291	Abstract Test Suite Specification
9496-3	X.292	The Tree and Tabular Combined Notation
9496-4	X.293	Test Realization
9496-5	X.294	Requirements on test laboratories and clientes for the Conformance Assessment

으로 구분될 수 있다. 구현물 이 명시된 기능들을 제공하고자 할 경우에 반드시 따라야만 하는 명세들을 지칭할 때는 "필수적이라는 것"이라는 용어가 사용된다.

2. ISO/IEC 9496

ISO/IEC 9496은 ISO/IEC에서 적합성 테스트를 위해 제시된 평가 방법론으로써 내부 컴포넌트에 대한 표준 준수성을 평가하는 방법이다.

2.1 ISO/IEC 9496의 개요

ISO/IEC 9646은 OSI(Open Systems Interconnection) 7 계층을 기반으로 한 통신 프로토콜의 적합성 시험 방법론에 대한 국제 표준이다. 통신 프로토콜의 적합성 시험(Conformance Test)이란 구현된 프로토콜이 기준 프로토콜(Base Protocol) 혹은 참조 프로토콜(Reference Protocol)의 규정을 준수하는지를 확인하는 시험으로, 프로토콜 구현 과정이나 혹은 구현이 완료된 시점에 시행된다. 적합성 시험은 정보통신제품의 요구사항이 복잡하고 다양해짐에 따라서 발생할 수 있는 문제를 조기에 해결하고, 제품 생산 및 수요자의 신뢰성을 높이기 위해서 최근에 사용이 증가하고 있다. 또한 장비간의 상호운용을 위해서 표준 적합성은 필요조건의 하나이다. 시험 비용의 감소 및 시험의 공정성, 객관성, 반복성, 재생성을 보장하기 위해서 자동화된 시험 도구(Test Tool)가 선호되며 ISO/IEC 9646에서는 표준 문서에서 이러한 시험 스위트(Test Suite)를 어떻게 생성하는지에 대해서 상세히 설명하고 있다.

ISO/IEC 9646의 적합성 시험은 크게 다음의 세 가지로 구성된다.

- 추상 시험스위트의 명세(Specification of Abstract Test Suite) : 시험 스위트 구조(Test Suite Structure)와 시험 목적(Test Purpose)의 작성 포함
- 시험 수단의 실현(Realization of a Means of Testing) : 추상 시험 케이스(Abstract Test Cases)에서 실행가능 시험(Executable Tests)으로의 변환 포함
- 시험 캠페인 수행(Conducting the test campaign) : 구현물에 대해서 실행가능 시험 수행

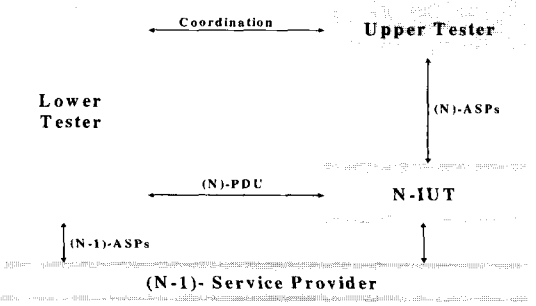
ISO/IEC 9646은 총 7개의 문서로 구성되어 있다. 이 7개의 문서는 각각 X.290에서 X.296까지의 권고와 대응된다. 각각의 대응되는 관계는 〔표 1〕과 같다.

2.2 적합성 시험 모델과 시험 기법

부분의 구현 제품은 사용자(UT : Upper Tester)와 IUT(Implementation Under Test), IUT와 제공자(LT : Lower Test), 그리고IUT와 동등 개체(peer entity) 간의 상호 동작으로 이루어진다.

따라서 특정한 IUT의 시험은 IUT와 LT, UT, 동등 개체간의 상호 동작을 제어하고 관찰함으로써 이루어질 수 있다. 이러한 상호 동작을 어떻게 제어하고 관찰할 것인가는 시험 스위트에서 기술된다 〔그림 2〕에서 N-ASP를 제어하고 관찰하는 모듈이 UT이고, N-PDU(Protocol Data Unit) 및 (N-1)-ASP(Abstract Service Primitive)를 제어하고 관찰하는 모듈을 LT라하며, 일반적인 시험 모델은 〔그림 2〕와 같다.

적합성 시험 방법은 시험기와 시험 대상이 동일 시스템 내부에 위치하는 지역적 시험 방법(Local Test Methods)과 시험기와 시험 대상이 별도의 시스템으로 존재하는 외부 시험 방법(External Test Methods)의 두 가지로 분류할 수 있다. 또한, 외부 시험 방법은



〔그림 2〕 IUT의 개념적 시험 모형

시험기와 시험 대상 사이에서 시험을 위하여 교환되는 PDU(Protocol Data Unit)들을 제어하고 관찰하는 제어 및 관찰점(PCO : Point of Control and Observation) 수와 그 위치에 따라 분산 시험 방법(Distributed Test Methods), 조정 시험 방법(Coordinated Test Methods), 원격 시험 방법(Remote Test Methods)으로 분류된다. 또한 각각의 시험 방법은 단일 계층을 독립적으로 시험하는 단일 계층 시험 방법(Single-layer Test Methods)과 다중 계층 내부에 삽입되어 있는 계층을 시험하는 방법인 내장 시험 방법(Embedded Test Methods)으로 구분되기도 한다.

2.3 ISO/IEC 9496 취약성 분석

ISO/IEC 9496을 기반으로 복합 기능을 갖는 정보보호 프로파일에 대한 평가를 수행할 경우 예측되는 취약성은 다음과 같다.

① 보안 연계성 : ISO/IEC 9496은 OSI 7계층을 기반으로 통신 프로토콜의 적합성 시험 방법론에 대한 국제 표준이다. 그러나 ISO/IEC 9496이외의 보안 평가 표준과의 호환성에 문제성이 지적된다. ISO/IEC 9496으로 평가받은 보호 프로파일이나 제품에 대한 평가가 다른 표준과의 호환성 때문에 재평가되어야 하는 취약성을 내포하고 있다. 특히 복합 보호 프로파일의 경우에는 동일한 제품에 대해 독립된 형태로 평가될 경우와 복합된 제품이나 프로파일의 평가가 상이할 경우 이와 관련된 문제점이 지적될 수 있다.

② OSI 표준을 따르는 취약성 : ISO/IEC 9496은 OSI 7계층을 기반으로 평가되어지는 평가 방법론이다. 그러나 OSI 7계층을 기반으로 평가되었다 할지라도 정보보호 제품이나 보호 프로파일에 대한 안전성을 보장해 줄 수 없다. 이는 네트워크 보안 제품에서 그 예를 찾아볼 수 있다. 침입 차단이나 탐지 시스템의 경우 로그 포맷 교환이 서로 다른 표준을 따르더라 할지라도 실제 보안성에는 전혀 영향을 미치지 못하기 때문이다.

③ 수정 불가능성 : ISO/IEC 9496은 프로토콜 표준 자체에 대한 평가를 수행하는 평가 방법론이다. 따라서 프로토콜 이외의 암호 알고리즘이나 암호 키에 대한 안전성을 보장해 줄 수 없다. ISO/IEC 9496의 평가 방법론을 따를 경우제품에 대한 암호 알고리즘이나 암호 키에 대한 안전성에 대한 평가 방법론이 추가되어야 한다.

④ 표준이 없는 정보보호 제품에 대한 평가 : ISO/IEC 9496의 경우 표준이 없는 정보보호 제품이나 보호 프로파일에 대한 평가가 불가능하다. 이는 ISO/IEC 9496이 OSI 표준을 따르기 때문이다. 특히, 네트워크 제품과 관련된 침입 차단이나 탐지 및 바이러스와 같은 제품의 평가에는 이와 같은 문제점이 발생된다.

따라서 ISO/IEC 9496에서는 단일 제품뿐만 아니라 복합 보호 프로파일이나 제품에 대한 평가에도 동일한 취약성을 내포하는 단점을 갖고 있다.

⑤ 구현에 따른 취약성 검증 불가 : 제안된 보호 프로파일에 대한 평가를 수행한다 할지라도, 실제 구현 과정에서 나타날 수 있는 취약성 평가를 추출해 낼 수 없는 단점이 있다. 이는 복합 기능을 갖는 보호 프로파일 개발에 따른 구현에도 같은 취약성이 지적될 수 있다.

3. SCT

SCT(Strict Conformance Test)는 유럽을 중심으로 정보보호 제품에 대한 표준 적합성을 평가하는 방법론으로써 기존 ISO/IEC 9496에 보안적 평가 내용을 추가적으로 도입함으로써 보다 향상된 방식의 유럽 평가 방법론 표준이다.

3.1 SCT의 개요

정보보호 제품은 특성상 표준 적합성 시험을 통과하더라도, 설계 및 구현상의 오류나 표준에 내재되어 있는 오류로 인해 안전성과 신뢰성에 악영향을 미칠 수 있다. 이러한 언급은 일반적으로 잘 알려지거나, 경미한 보안 취약성(Vulnerability) 등으로 인해 정보보호 제품의 안전성이 떨어질 수 있음을 의미하며, 제품 전반의 신뢰성이 훼손(Compromise)될 수 있음을 지적하고 있다. 이러한 ISO/IEC 9646 표준적합성 시험 방법론의 문제점을 고려하여 영국 NPL (Nation Physical Laboratory)에서 제안한 방법론이 SCT이며, ITSEC/ITSEM의 몇몇 아이디어를 적용하고 있다. ISO/IEC 9646에서 제시한 적합성 시험 방법론은 IT 제품 또는 시스템의 안전성을 목적으로 하는 정보보호 표준을 포괄하지 못하므로, 정보

보호제품을 시험하는 데는 적절하지 못한 것이 사실이었다. SCT 방법론은 이러한 문제점들을 해결할 뿐만 아니라, 상용 정보보호제품 또는 시스템이 포함하고 있는 보안 기능에 대해 보안 목표(Security Target)를 대상으로 평가를 수행함으로서 표준적합성 이외에 보안성과 관련된 보증(Assurance)을 함께 제공할 수 있다. 이렇듯 SCT 시험은 시스템이나 제품에 대한 평가에서 시간 소모를 줄이고, 개발자가 평가 과정을 잘 준비하게 함으로써 보다 높은 목표량 달성을 통해 비용 절감 효과 및 신뢰도를 향상시킬 수 있다.

3.2 SCT에 적용되는 시험 기법

SCT는 개발 제품 및 시스템이 외부로부터 특정 요인에 의한 기능, 트랩도어, 트로이 목마 등을 내포하는지 확인하고 보증하게 된다. 이를 위해 SCT에서는 정보보호 제품을 시험하는 활동을 기술하고 있으며, 다음의 시험 기준들을 통하여 개발 제품 및 시스템을 시험하고 분석한다.

① 표준의 필수요구사항들을 올바른 방법으로 정확하게 구현함
② 적합성 명세서에서 기술되고 있는 바와 같이 선언된 표준의 선택적 요구사항을 구현하였으며 또한 올바르게 구현함
③ 구현물의 올바른 운용을 침해하거나 아니면 보안상의 가능한 결함을 야기하는 특정 기능을 내포하지 않음

적합성 시험과 관련된 SCT의 정의를 통해 다양한 시험 결과들을 처리할 수 있다. 물론 위의 정의에서 기준 ①과 ②는 OSI 적합성 시험을 위한 기준의 단순한 재선언으로 규정되기도 한다. 그러나 SCT와 OSI 적합성 시험 모두는 어떤 구현물이 해당 표준의 적합한지를 판별한다는 측면에서 그 의미와 목적을 같이하고 있다. 기준 ③은 평가의 목적을 요약함과 동시에 개발 제품 및 시스템에 대한 보안성 검증 및 보증의 필요성을 언급한 것이다. 이는 시스템이 잠재적인 오류를 범할 수 있는 코드를 포함할 수 있음을 지적한 것으로써, 해당 표준에서 필수적으로 규정된 것 이외에 발생할 수 있는 역기능을 설명하고 있다. 이러한 역기능은 정보보호관련 구현물의 규정된 산출물에 영향을 미치며, 외부적으로는 정상적인 동작을 하는 것처럼 보이지만 보안상의 취약성을 가질 수 있음을 의미한다.

〔표 2〕 화이트박스 레벨 등급

화이트박스 레벨	레벨별 범위
C0	모든 문장 범위
C1	모든 부분 범위
C2	모든 사항 범위
C3	모든 연합 사항 범위
C4	모든 패치 영향 범위
C5	모든 패치 영향의 반복
C6	모든 유리한 패치의 반복
C7	모든 패치 범위

표준문서의 시스템 구현시 발생될 수 있는 모호함이나 불완전성에 대한 분석과 오류 발견을 쉽게 할 수 있는 기법으로 정형기법을 적용할 수 있다. 정형화 기법은 수학적인 기호를 통해 시스템 동작 시 발생할 수 있는 오류 및 잠재된 오류에 대한 검사를 시스템 개발 단계 이전에 수행함으로써 보다 안전하고 정확한 시스템을 개발 할 수 있다. 그러나 전체 시스템에 수학과 논리학을 기반으로 하는 정형기법을 적용하기에는 현실적으로 많은 문제점들이 있다. 따라서 SCT에서는 표준문서 구현의 적합성을 시험하는 기법으로 비정형기법 중 하나인 그레이 박스(Grey-box) 시험 위주로 실행하며, 보다 완전한 시스템을 위해 선택적으로 정형기법을 도입하도록 권고하고 있다.

3.3 SCT 보증 방법

SCT에서 제공하는 보증 방법은 다양한 레벨 시험에 의해서 제공되는 보증 정도 측정에 대한 방법을 제공한다. SCT의 시험 테스트에서 TAL(Test Assurance Level)에서 기반이 되는 시험은 화이트 박스 시험과 블랙 박스 시험으로 나눌 수 있으며, 이는 다음과 같다.

(1) 블랙 박스 테스트

블랙 박스의 테스트는 제품의 기능 명세를 기본으로 한다. 블랙 박스의 테스트는 제품의 접속과 각각의 함수의 증명으로 모든 사용과 일반적인 입력과 각각의 제품의 출력 값이 올바른지 확인 한다. 제품의 클래스의 입력으로 동등한 분배는 테스트 케이스로 동등한 분할 분배이다. 제품의 분할 테스트 방법을 기초로 하여 분석을 제공해 준다. 일련의 그래프 결과를 나타내는 것으로 유사한 집합의 정의를 할 수 있다. 상태의 변화 측정의 테스트는 상태에서의 변화에 대한 정의를 나타낼 수 있다.

(2) 화이트 박스의 테스트

화이트 박스의 테스트는 제품의 내부의 활동을 기초로 한다. 화이트 박스의 테스트는 제품의 명세서에 대해 내부적인 기능의 문서를 처리한다. 소프트웨어의 논리적인 테스트의 집합은 상태와 루프와 제품의 상태를 시험한다. 테스트의 기본으로 논리적인 패치로 복합성을 이용한다. 프로그램의 모든 문장을 테스트로 실행한다. 외형 테스트 운영은 논리적인 모듈의 집합의 정의로 패치를 실행한다. 화이트박스 테스트는 데이터 흐름의 테스트로 모듈의 집합에 대한 정의와 사용자의 변화를 정의하며, 테스트로 모듈의 집합 정의를 이용한다. 화이트 박스는 레벨8로 C0에서 C7을 이용하고 있다([표 2] 참조).

이상의 내용을 기반으로 SCT에서는 다음과 같은 4개의 레벨 단계로 이루어지며 각각의 내용은 다음과 같다.

- TAL1 (시스템 시험) : 블랙 박스시험을 이용해서 보안 목표(Security Target)에 기반한 시스템 레벨에서의 적합성 검증 시험
- TAL2 (통합 시험) : TAL1 + 단계적으로 시스템에 모듈을 통합하는 동안 통합모듈 인터페이스 시험 위주의 블랙 박스 시험
- TAL3 (모듈 시험) : TAL2 + 모듈 인터페이스 행위 위주의 저 수준 설계 정보에 기반한 화이트 박스 시험
- TAL4 (단위 시험) : TAL3 + 내부 모듈 경로 행위 위주의 소스코드 레벨 정보에 기반한 화이트 박스 시험

3.4 SCT의 취약성 분석

SCT의 경우 정보보호 제품의 적합성 및 보안성을 평가하기 위한 방법론이다. 이러한 방법론이 복합 보호 프로파일 개발을 위해 적용되기 위해서는 다음과 같은 고려사항과 취약성을 지적할 수 있다.

① 그레이 박스 시험의 실현 불가능성 : 그레이 박스 시험에 대한 정확한 예가 없을 뿐만 아니라 개념적인 설명으로 실제 SCT 평가를 위해 구현하거나 개발되는 정보보호 프로파일이나 제품의 개발에 어려움이 예측된다. 따라서 복합 보호프로파일도 같은 취약성을 내포하게 된다.

② SCT ATS(Abstract Test Suite) 추출의 어려움 : 추상 보안 목표에서 SCT 추상 시험 스위트를 추출하는 것에 대한 정확한 예가 없어는 취약성을 갖게 된다. 이는 개념적인 설명으로 그치고 있어 실제 환경에 적용하기에는 어려움을 갖게 된다.

③ 보안 전문가의 필요 : 그레이 시험 기법을 적용하거나 추상 보안 목표에서 SCT 시험 스위트를 추출하기 위해서는 구현 경험을 가지고 있고 구현 코드 분석이 가능한 숙련된 보안 전문가가 필요하다.

④ 보안 환경의 고려 : 표준에 근거하여 한번 작성하면 반복성을 갖는 운용 시험스위트가 나오는 ISO/IEC 9496 적합성 시험과는 달리 SCT에서는 변화하는 보안환경을 고려하여 주기적으로 시험 스위트가 갱신되어야 한다.

⑤ 정형 기법적용의 어려움 : 정보보호 제품의 개발 시에 명세나 검증의 수단으로 정형 기법을 적용하려면 많은 시간 및 비용이 소모되기 때문에 현실적으로 적용하기에 어려움이 예측된다.

4. CEM(ISO/IEC 15408)

CEM은 북미를 중심으로 정보보호 분야에서 기술적 평가를 위주로 하는 제품/시스템에 대한 평가 방법론중의 하나로 현재 국제 공통 평가 기준인 CC(Common Criteria)의 평가 방법론으로 연구가 진행중이다.

4.1 개요

안전한 정보보호 시스템에 대한 평가자의 능동적인 조사를 통한 평가에 기반한 보증을 제공하기 위해 미국, 영국, 프랑스, 캐나다, 독일, 네덜란드는 정보보호시스템을 위한 국제 공통 평가 기준인 CC v2.0을 1998년 5월에 공표하였으며, 국제 표준화 기구인 ISO/IEC 15408로 표준을 제정하였다. ISO/IEC 15408은 크게 정보보호시스템의 기능 요구사항과 보증 요구사항으로 구성된다. 기능 요구사항에는 사용자 식별과 인증, 데이터나 자원의 보호, 보안 감사 등 정보기술 보안에 중요시되는 모든 기능을 망라하고 있다. 그리고 보증 요구사항에는 개발 사양서의 내용, 시험 실시 내용, 취약성/오용에 관한 저항력, 형상관리, 개발 환경, 배포 절차 및 운영 등 여러 가지 측면에서 확인 항목을 포함하고 있다. 이 확인 작업들을 "평가"라고 한다. 평가를 받기 위해서는 개발자가 준비해야 하는 사항에 대해서도 상세히 서술되어 있다. 또한 제품이나 시스템이 기능요구사항을 어디까지 보증하고 있는가를 나타내는 척도

로써 7단계의 보증 요구사항의 부 집합을 정의하고 있다. 이것을 보증 등급(EAL : Evaluation Assurance Level)이라 한다. 또한 보안에 관한 기본적인 개념의 설명과 함께 평가 대상인 제품이나 시스템의 보안 기본 조건을 기술한 보안 목표 명세(ST : Security Target)와 ST의 기본이 되는 보호 프로파일(PP : Protection Profile)에 대해서 설명하고 있다. ISO/IEC 15408은 정보기술을 이용한 제품이나 시스템의 보안 기능을 대상으로 하고 있다. 소프트웨어뿐만 아니라 하드웨어, 펌웨어(IC카드 등), 혹은 시스템 전체도 평가 대상이 된다. 제품의 형태는 방화벽과 같이 직접 보안에 관련한 기능을 제공하는 제품뿐만 아니라 사용자에 대해서 패스워드 입력을 요구하는 운영 체제나 데이터 베이스, 업무상의 역할마다 접근 관리를 수행하는 그룹웨어 등 보호해야 하는 자원을 보유하는 제품이나 시스템 전반이 대상이 된다. 규격에서 취급되는 내용에는 보안 기능의 기술적인 대책뿐만 아니라, 이와 같은 제품이나 시스템을 이용하기 위한 보안 교육이나 보안 감사 등의 조직적인 보안 운영이나 관리 등의 대책도 포함된다. 단, 이것은 어디까지나 이들 제품이나 시스템이 평가의 대상이지 ISO 9000이나 ISO 14000과 같은 조직을 평가하기 위한 기준은 아니다.

4.2 CEM의 보증 등급

CEM의 평가 등급(EAL : Evaluation Assurance Levels)은 보증을 위한 비용과 보증 수준간의 단계적인 등급을 제공한다. 보증 등급은 제품이나 시스템이 기능 요구사항을 어느 수준까지 보증하고 있는가를 나타내는 척도로써 각 보증 요구사항의 부 집합의 형태로 계층적으로 등급을 분류하고 있다. CC에서는 7개의 계층으로 EAL을 정의하고 있으며 만족해야 하는 보증 요구사항이 규정되어 있다. 이는 평가 대상의 제품이나 시스템의 성격, 사용 형태 등에 따라 구분될 수 있으며, EAL1에서 EAL 5까지는 상용 제품이나 시스템이 갖추어야 하는 보증 등급이며, EAL5 이상은 군용 혹은 그에 준하는 용도로 활용이 가능하나 금융 및 상용 등급에서도 EAL5 이상되는 보증 등급이 적용 될 수 있다. 각각의 EAL 등급별 보증 내용 및 SCT에서 제시되는 평가 레벨 TAL과 매핑은 다음과 같은 표 3으로 정리할 수 있다.

4.3 CEM의 취약성 분석

CEM은 국제 공통 평가 기준으로 보호 프로파일이나 정보 보호 제품을 평가하기 위한 평가 방법론으로써 복합된 보호 프로파일의 개발에 대한 적용에 따른 취약성은 다음과 같이 분석할 수 있다.

① 단일 제품의 평가와 복합 제품의 평가의 불분명 : 단일 제품으로 평가한 보호 프로파일이나 정보보호 제품에 대한 평가와 복합 제품으로 포함된 단일 제품의 평가가 서로 상이한 결과를 초래할 경우 발생되는 문제점을 지적할 수 있다. 이는 특히 네트워크 제품에서 많은 문제점을 제기할 수 있다. (침입 감내 시스템의 경우 국내외적으로 서로 다른 정의를 내리고 있다. 국외적으로는 순수 감내 서비스를 침입 감내라고 하지만, 국내에서는 침입 차단 시스템과 결합된 형태의 침입 감내 서비스를 개발하고 있다. 따라서 국내에서 평가된 침입 감내 시스템을 국외적으로 평가받을 경우침입 차단 시스템을 기준으로 해야 하는지 침입 감내시스템을 기반으로 해야 하는지에 대한 기준이 없다.)

② 국제 공통 평가 기준에만 적용할 수 있는 한정성 : 시험 평가 방법론을 비롯하여 많은 평가 기준과의 호환성을 지적할 수 있다. 이는 CEM이 국제 공통 평가 기준을 위해 개발되어 있어 보호프로파일이나 정보보호 제품에 대한 평가를 수행함으로써 발생한다. 따라서 이를 보완하기 위해서는 다양한 평가 기준과의 호환성을 유지할 수 있는 새로운 형태로의 전환이 필요하며, 보안 조직에 대한 평가도 대상에 포함되어야 할 것으로 예측된다.

③ 개념적인 이론 정의 : CEM의 경우 개념적인 이론 정의로 인해 실제 적용했을 시 검증자의 주관적인 내용이 추가 될 수 있다. 이는 평가 방법론을 기준으로 평가를 수행했다 할지라도 그에 해당되는 실질적인 예시가 없어 취약성으로 평가 될 수 있다.

5. ISO/IEC 15443

ISO/IEC 15443의 목적은 여러가지 보증 방법을 언급하고, 주어진 IT 보안 제품, 시스템, 서비스, 과정 그리고 주위 요인에 대한 보안 보증 필요 조건을 만족시켜 IT 보안 제품에 대한 신용을 이루기 위한 적합한 보증 방법(또는 방법의 결합)의 선택 과정에서 나타날 수 있는 다양한 방법들을 제공한다.

〔표 3〕 EAL 보증 등급의 개요 및 TAL 매핑

보증 등급	보증 등급 내용	TAL과 매핑
EAL 1 : 기능적인 시험의 보증	평가자 설명서에 따른 기능적 분석과 시험	TAL 1
EAL 2 : 구조적 시험의 보증	상위 수준 설계서에 기반한 프로그램 구조의 검증 및 샘플링 시험	TAL 2
EAL 3 : 체계적인 시험 및 확인에 대한 보증	계통적 시험의 실시 및 분석, 개발 환경, 개발 생성물의 관리 상태에 대한 평가	
EAL 4 : 체계적인 설계, 시험, 검토의 보증	하위 수준 설계서와 중요 원시코드에 대한 이용과 처리 내용을 검증하고 평가 감독자의 시험 수행	TAL 3
EAL 5 : 준정형적인 설계 및 시험의 보증	전체 원시 코드의 분석 및 정보 유출 루트 분석 수행	TAL 4
EAL 6 : 준정형적인 설계의 검증 및 시험의 보증	정형적인 검증 이외의 소프트웨어 공학적인 검증 수행	
EAL 7 : 형식적인 설계의 검증 및 시험의 보증	정형적인 기술 언어를 이용한 검증 방식에 기반한 설계 및 시험 확인	

5.1 ISO/IEC 15443의 개요

ISO/IEC 15443의 경우 다양한 경우에 의해 신청된 보증 방법과 평가 방법에 대한 접근 방법을 제공한다.

따라서 ISO/IEC 15443은 현재 보증 방법을 적당한 장소에 놓고 그들의 관계를 보인 모델에 대해 기술하고 보증 방법의 수집, 그들의 설명 그리고 참조 모델에 대해 설명하다. 또한 보증 방법의 부분일 수 있거나 개별적으로 보증에 기여할지도 모르는 보증 요소의 수집 및 보증 방법 그리고 요소에 일반적이고 독특한 특성 부여하고 현재의 보증 방법과 요소의 질적으로 비교가 가능한 경우와 보증 계획들의 동일하다는 증명은 현재 보증 방법을 가지고 교환에 대해 설명한다. 마지막으로 다른 보증 방법과 요소 사이의 관계 및 적용에 안내, 보증 방법의 구성과 인식을 제시함으로써 다양한 형태의 보증에 대한 프레임워크를 제시하고 있다.

ISO/IEC WD 15443은 총 3개의 파트로 이루어져 있으며 이에 대한 간략한 개요는 다음과 같다.

- 파트1 (개요 및 프레임워크) : 파트1은 보증방법과 보증요소에 대한 일반적인 설명과 기본 개념에 대한 소개를 제공한다. 파트2, 파트3의 이해를 위한 장으로, IT 보안 관리자 및 보안보증 프로그램(예 : ISO 9000, SSE-CMM, ISO/IEC 15408), 또는 다른 보증 행위들에 대한 책임이 있는 사람들을 대상으로 한다.
- 파트2 (보증 방법) : 파트2는 보증 방법, 접근법에 대해서 설명하며, 그러한 것들을 파트1의 보증 모델과 연관시킨다. 이 장은 제품 또는 서비스의 생명주기(Life Cycle)에서 보증을 얻는 방법을 이해하는 IT 보안전문가를 대상으로 한다.
- 파트3 (보증 방법 분석) : 파트3은 필요한 자원, 관계, 효과, 동등성의 관점에서 다양한 보증 방법에 대해서 분석한다. 이러한 분석은 보증 접근법을 결정하는 기본이 된다. 이 장은 보증 방법 및 접근법을 선택해야 하는 IT 보안전문가를 대상으로 한다.

5.2 ISO/IEC 15443 적용의 다양성

ISO/IEC 15443은 다양한 평가 방법들에 대한 상호 연관성을 분석하고 다양한 형태의 적용성을 제시하고 있다. 현재 ISO/IEC 15443에서 제시되고 있는 보증에 대한 구성과 보증에 대한 인가에 대한 내용은 이러한 상호 연관성과 적용성을 위해 활용 될 수 있다.

- 보증 구성 : 보증 구성으로 컴퓨터 또는 외형 보증 방법의 차이점은 비슷한 외형의 보증 방법에서 차이점을 발견할 수 있다. 따라서 보증 구성을 기본적으로 블록단위를 통해 보증해야 한다. 각각 보증의 구성은 보증의 전반적인 활동으로 제공되어야하며, 보증의 방법은 다른 보증의 구성 또는 특정 관점으로 포함 될 수 있다. 보험 구성은 보증의 원시코드로 작성되어 제공해야 하며, 비용과 효과에 대한 의문점과 의문점으로 인해 발생되는 보증 방법의 외관 및 신뢰에 대한 의문이 있을 제기할 수 있어야 한다.
- 보증인가 : 보안 목적으로 보증인가의 체크는 효과적으로 IT 제품의 보안 함수를 평가하는 것이다. 이러한 평가 활동은 인가에 대한 평가로 전형적인 채널 분석, 강한 보안 함수 분석, 오용 분석, 인가 실패의 가정과 강도 테스트가 있다. 외형적으로 형성되는 시스템은 항상 높은 레벨을

목적으로 정확한 검증만을 요구하지는 않지만, 인증이 요구되는 경우도 발생한다. 보안 시스템에 대한 보증의 정당성은 결과를 확인 할 수 있는 논의에 대해 시스템의 보안 목적으로 실행되지 못한 경우의 명세화가 필요하다.

Ⅲ. 대체 평가 방법론의 연관성 및 비교 분석

본 장에서는 북미 표준으로 자리잡고 있는 CEM을 기반으로 하여 대체평가 방법론으로 제시되었던ISO/IEC 9496, SCT, ISO/IEC 15443에 대한 연관성과 SCT와 CEM의 보증등급에 대해 ISO/IEC 15443에 매핑과정을 제시함으로써 안전한 복합 보호프로파일 개발을 평가 방법론의 적용성을 제시하고자 한다.

1. 대체 평가 방법론의 연관성 분석

기존에 제시된 다양한 형태의 대체 평가 방법론들에 대해 연관성을 분석함으로써 복합 기능을 갖는 정보보호 제품에 대한 평가를 위한 기반 연구를 수행하고자 한다.

1.1 CEM과 ISO/IEC 9496의 연관성

ISO/IEC 9496은 IT 보안 제품이 아닌 일반적인 네트워크 제품을 OSI 7계층을 기반으로 표준 적합성을 테스트하는 대체평가 방법론이다. CEM은 IT 보안 제품에 대한 보안 보증 평가 방법론으로써 각국마다 다양한 방법론이 적용되기 때문에 공통적인 제품 개발을 위해서는 CEM에 고려되지 않았던 일반적인 제품에 대한 평가 방법론이 요구된다. CEM의 경우 보증 엘리먼트를 기반으로 하여 패키지 및 클래스로 처리되는 보증 평가가 수행되고 ISO/IEC 9496 역시 같은 개념으로 평가가 수행되지만 사건 이벤트를 통해 아이템을 생성하고 아이템에 기반한 케이스 및 그룹, 스위트를 제공한다. 따라서 CEM과 ISO/IEC 9496은 서로 공통성이 없는 방법론이나 같은 개념의 처리과정을 통해 상호 연관성을 유지할 수 있다 할 수 있다.

1.2 CEM과 SCT의 연관성

SCT는 기존 ISO/IEC 9496의 취약성을 보완하면서 정보보호 제품에 대한 보안 평가를 수행함으로써 ISO/IEC 9496과는 차별화된 서비스를 제공하는 유럽 표준이다. 특히, SCT는 정보보호 제품이 표준을 준수하고 있는지에 대한 적합성 테스트와 업체가 IT 시스템에서 제공하고자 하는 보안 요구사항 뿐만 아니라 소비자가 요구하는 보안 요구사항의 비교를 통해 평가가 테스트되는 특징이 있다. 그러나 CEM의 경우 일반적인 표준 적합성 테스트 시험에 대한 방법론을 제시하고 있지 않기 때문에 SCT와는 차별화 된 서비스일 수 있다. 그러나 보증 평가 방법론 부분에서는 SCT의 보증 레벨과 CEM의 보증 레벨간의 상호 매핑을 통해 그 연관성을 지적할 수 있다.

1.3 CEM과 ISO/IEC 15443의 연관성

ISO/IEC 15443의 경우 보증 프레임워크를 기반으로 기존 평가 제품에 대한 다양한 평가 방식을 채택한 대체 평가 방법론이다. 특히, 파트 3은 SCT에 영향을 미쳤으며, CEM의 확장된 적용을 위해서는 반드시 고려되어야 하는 표준이 ISO/IEC 15443이다.

이는 기존 CEM이 북미 표준으로 전세계적인 공통성을 제공한다 할지라도 유럽 표준으로 자리잡고 있는 SCT와의 공통성을 유지하기 위하여 다양한 형태의 평가 방식이 필요하게 되었으며, 이러한 필요성으로 인해 제기된 대체 평가 방법이 ISO/IEC 15443이다.

1.4 ISO/IEC9496과 SCT의 차별성

NPL(National Physical Laboratory)의 SCT 연구는 IT 보안과 관련된 프로젝트에서부터 출발하였다. 이 프로젝트 중 일부는 다양한 IT 보안 표준에 근거하여 대상 제품이나 시스템이 어느 정도의 정확성을 가지고 구현되었는지 시험할 수 있는 방법을 개발하였다.

초기 적합성 시험 연구 과정에서는 IT 보안 표준의 주요 시험 요소가 무엇인지에 대해서 별도의 검토를 수행하지는 않았다. 또한 기존의 IT 보안 표준은 시스템 또는 제품이 표준을 준수하는데 필요한 요구사항이나 적합성 요구사항이 어떻게 시험을 통하여 검증되는지에 대한 방법에 대해서는 명시하고 있지 않다. 그러나 SCT 프로젝트가 진행됨에 따라 IT 보안 표준의 중요한 특성들과 이들의 시험 방법을 제시함으로써 IT 보안 표준 및 시험에 대한 새로운 접근방법(New Approach)을 개발하였다. 본 절에서는 SCT가 기존의 표준적합성 시험들과 비교하여 차별화 되는 특성들을 기술한다.

- 보안 목표를 고려한 추상 시험 스위트 : SCT와 개방형 시스템의 적합성 시험 방법론(ISO/IEC 9646)

의 가장 큰 차이점으로는 보안 표준(Security Standard)에 근거한 "실제 구현물"을 대상으로 "구현 독립" 및 "구현 종속" 시험이 가능하다는 점이다. 이를 위해 보안 표준에 기초하여 생성된 추상적 보안 목표(AST : Abstract Security Target)를 구성하게 되며, 이것은 추상 시험스위트(ATS : Abstract Test Suite)로 표현된다. ATS는 적합성 시험 스위트 와함께 구현 독립 시험 시 사용되는 SCT 시험 스위트의 요소가 될 뿐 아니라, 구현 종속 시험을 위해 개발자들이 작성하는 보안 목표(Security Target)의 기준 요소가 된다. 프로젝트 초기에는 단지 설계문서에 대한 평가만 가능하였으나, ATS를 이러한 문서와 비교함으로써 중요한 결함들을 밝혀 내었다. 제조업체는 개발과정에서 이러한 중요한 결함을 조기에 발견함으로써 개발비용을 10% 절감시킨 것으로 추정하고 있으며, 이것은 SCT 개념의 견실성을 입증한 사례가 되었다.

- 적합성 시험 결과의 표준 피드백 : SCT의 시험 기준 구성시 3가지의 시험 스위트(적합성 시험 스위트, SCT 시험 스위트, 운용 시험 스위트)가 구성되게 된다. 전반 2개의 스위트는 구현 독립 시험을 위해서 사용되며, 마지막 스위트는 구현 종속 시험을 위해 구성된다. 구현 독립 시험을 위한 SCT 시험 스위트는 적합성 시험 스위트와 시험 목적을 기술한 AST를 기반으로 개발되며, 구현 종속 시험을 위해 SCT 시험 스위트 와 보안 목표(ST)를 기반으로 운용 시험 스위트 가개발된다. 이들을 통한 시험 결과들은 각각에 대한 개별적인 검토를 통해 다시 표준에 피드백 됨으로써 기존의 적합성 시험보다 표준문서에 적극적 기여를 하게 된다. 이러한 과정을 거치면서 표준 문서 자체에 내재되어 있는 논리적 오류의 발견이나, 개발자가 표준문서를 임의적으로 해석함으로써 발생할 수 있는 문제점들을 표준문서에 적극적으로 반영할 수 있게 된다. 취약성 예시 방법론(VIM : Vulnerability Instanitation Methodology)은 보안 검증 도구로부터 출력을 받고 그 출력을 대상 시스템과 더욱 높은 연관성을 가지도록 만드는 기능을 가지고 있는데 적합성 시험 결과의 표준 피드백에 도움을 줄 수 있다.
- 취약성 고려를 통한 SCT 추상 시험 스위트의 최적화 : SCT를 기존의 적합성 시험과 가장 크게 차별 지을 수 있는 요소로 보안 취약성을 고려하는 것을 들 수 있다. 보안 취약성을 고려하는 측면에서 SCT 프로젝트의 일환으로 구획 모드 워크스테이션(CMW : Compartmented Mode Workstation)으로 알려져 있는 워크스테이션에 대한 보안요구사항 문서를 구성하여 보안 취약성 부분에 적용하였다. 여기에서는 시스템이나 제품을 사용한 후에 발견되는 취약성까지 고려해야 한다는 의견이 개진되었으며, 이러한 취약성들에 대한 시험이 SCT 시험 스위트에 최적화될 수 있는 방법을 제시하였다.
- 취약성 고려를 통한 SCT 추상 시험 스위트의 최적화 : ISO/IEC 9646이 시험 스위트에 대한 자동화 과정의 난해함으로 구현된 예들이 극히 적은데 반해, SCT는 실제 구현 경험을 활용하여 추상 시험스위트를 개발할 수 있다. SCT 프로젝트에서 개발된 EDI(Electronic Data Interchange) 시험 스위트 중 하나를 시험 모듈로 개발하여 실행 가능하게 하고, 표준에 근거한 참조 구현을 개발한 다음, 시험 모듈을 이들 참조 구현과 상용 제품 양쪽에 장착하여 수행하였다. 이 프로젝트에서는 참조 구현 및 제품과 시험 스위트 모두에서 오류를 발견했으며, 시험 스위트의 오류들을 수정하여 Secure EDIFACT(Electronic Data Interchange for administration, Commerce and Transport)를 위한 개량된 시험 스위트를 만들 수 있게 되었다. 이런 과정들과 SCT 방법론의 표준화를 통해 SCT의 인지도가 확산되었다.

2. 보증 등급의 매핑

TAL과 EAL간의 매핑은 다음과 같이 비교 분석할 수 있다.

- TAL1은 EAL1에 적용될 수 있다. EAL1은 가장 낮은 단계의 기능 명세 ADV_FSP.1 (비정형화된 기능명세)같은 개발 문서를 제공하며, 독립 시험 ATE_IND.1(독립적인 시험 : 기능 확인)을 필요로 한다.
- TAL2는 EAL2 및 EAL3에 적용될 수 있다. EAL2는 상위 레벨 설계 ADV_HLD.1(서술적인 기본설계)같은 개발 문서를 제공하며, 독립 시험 ATE_IND.2(독립적인 시험 : 표본 시험), ATE_FUN.1(기능 시험), ATE_COV.1(시험

〔표 4〕 TAL1과 EAL1의 세부 엘리먼트 매핑

	CEM의 세부 엘리먼트	ISO/IEC 15443의 적용성을 위한 TAL 매핑
세부 엘리먼트	기능 명세의 평가(ADV_FSP.1)	독립적인 시험의 평가(ATE_IND.1)
목적	개발자가 TOE의 모든 보안 기능들의 적절한 서술을 제공하고 TOE에 의해 제공하는 보안 기능이 ST의 기능 요구사항을 만족하기에 충분한지를 결정하기 위함	TSF의 부 집합을 독립적으로 시험함에 의해 TOE가 기술된 대로 행동하는지를 결정하기 위해 수행되는 세부 엘리먼트
평가 증거 자료	ST, 기능명세, 사용자 설명서, 관리자 설명서	ST, 기능명세, 사용자 설명서, 관리자 설명서, 안전한 설치, 생성, 시동 절차, 시험에 적합한 TOE
평가자 동작	ADV_FSP.1.1.E ADV_FSP.1.2.E	ATE_IND.1.1E ATE_IND.1.2E
분석	TAL1의 적용을 위해서는 높은 테스트 레벨에서는 ATE_IND.1에 의존되는 테스트가 요구된다. 이는 TAL 1 시스템이 보안 목적의 정보를 이용하여 수행되는 블랙박스 테스트로 요구되기 때문이다. 따라서 TAL을 위해서는 테스트 계획 및 테스트 순서, 테스트 도구와 테스트 케이스를 포함해야 한다.	

범위의 증거)을 필요로 한다. EAL3은 상위 레벨 설계 ADV_HLD.2(보안기능과 비보안기능을 분리한 기본설계)같은 개발 문서를 제공하며, 독립 시험ATE_IND.2(독립적인 시험 : 표본 시험), ATE_FUN.1(기능 시험), ATE_COV.2(시험범위의 분석), 상위 레벨 설계 시험 ATE_DPT.1(기본설계 시험)을 필요로 한다.

- TAL3은 EAL4에 적용될 수 있다. EAL4는 하위레벨 설계 ADV_LLD.1(서술적인 상세설계)같은 개발 문서를 제공하며, 독립 시험ATE_IND.2(독립적인 시험 : 표본 시험), ATE_FUN.1(기능 시험), ATE_COV.2(시험범위의 분석), 상위 레벨 설계 시험 ATE_DPT.1(기본설계 시험)을 필요로 한다.
- TAL4는 EAL5, EAL6, EAL7에 적용될 수 있다. EAL5, EAL6은 가장 낮은 레벨의 TSF (TOE Security Function) 구현문서 ADV_IMP.2/3(TSF에 대한 구현의 표현/TSF의 구현 표현의 구조화)을 제공하며, 하위레벨 설계 ATE_DPT.2(상세설계 시험)에 대한 가장 높은 시험을 요구한다. EAL7은 가장 낮은 레벨의 TSF 구현문서 ADV_IMP.3(TSF의 구현 표현의 구조화)을 제공하며, ATE_DPT.3(구현표현 시험)에 대한 가장 높은 시험을 요구한다.

2.1 TAL1과 EAL1의 매핑

EAL1은 기본 보증 수준을 제공한다. 보안 기능은 보안 행동을 이해하기 위해 기능 명세와 설명서를 이용하여 분석된다. EAL1은 TOE 보안 기능 부 집합의 독립적인 시험이 수행된다. 따라서 개발 문서로 낮은 레벨의 함수는 ADV_FSP.1에 명세되어 있다(〔표 4〕 참조).

2.2 TAL2와 EAL2의 매핑

TAL2의 경우 EAL2와 매핑이 가능하다. TAL2에서는 블랙박스 테스트를 기초로 하여 추가로 높은 레벨의 테스트에서 시스템의 모듈에 대한 단계적인 통합 인터페이스를 테스트하는데 그 목적이 있다(〔표 5〕 참조).

2.3 TAL2와 EAL3의 매핑

TAL2의 경우 EAL2와 매핑이 가능하다. TAL2에서는 블랙박스 테스트를 기초로 하여 추가로 높은 레벨의 테스트에서 시스템의 모듈에 대한 단계적인 통합 인터페이스를 테스트하는데 그 목적이 있다(〔표 6〕 참조).

2.4 TAL3와 EAL4의 매핑

TAL3는 EAL4와 매핑이 가능하다. TAL3는 모듈 테스트로써 화이트 박스 시험을 기반으로 이루어진다. 이는 기본적인 낮은 레벨의 외형 정보에 대한 관점으로 인터페이스의 내부 모듈 테스트를 수행한다(〔표 7〕 참조).

2.5 TAL4와 EAL5의 매핑

TAL4는 EAL5와 매핑이 가능하다. TAL4는 화이트 박스와 소스코드 테스트에 부과되어 내부의 모듈의 작동의 테스트 정보에 대한 관점을 두어 수행되는 테스트이다(〔표 8〕 참조).

2.6 TAL4와 EAL6의 매핑

TAL4는 EAL6와 매핑이 가능하다. TAL4는 화이트 박스와 소스코드 테스트에 부과되어 내부의 모듈의 작동의 테스트 정보에 대한 관점을 두어 수행되는 테

〔표 5〕 TAL2와 EAL2의 매핑

	CEM의 세부 엘리먼트	ISO/IEC 15443의 적용성을 위한 TAL 매핑
세부 엘리먼트	서술적인 기본 설계(ADV_HLD.1) 독립적인 표본 시험(ATE_IND.2) 기능 시험(ATE_FUN.1) 시험범위의 증거(ATE_COV.1)	시스템 테스트에서 정당성의기본으로 보안의 목적 레벨 정보를 이용하여 블랙박스 테스트 방법으로 시스템의 필요 조건을 제공하는 논증을 기반으로 하여 높은 레벨의 외형 정보에 대한 테스트를 결부하여 점차적으로 시스템의 측정을 위함
목적	개발자가 TOE의 모든 보안 기능들의 적절한 서술을 제공하고 TOE에 의해 제공하는 보안 기능이 ST의 기능 요구사항을 만족하기에 충분한지를 결정하기 위함	TAL1 시스템 테스트 + 외부 시스템 측정의 인정을 위한 매핑
평가 증거 자료	ST, 기능명세, 사용자 설명서, 관리자 설명서	제품의 접속과 각각의 함수의 증명으로 모든 사용과 일반적인 입력 및 각각의 출력 값이 올바른지 확인을 위한 입력과 출력 값에 대한 테이블
평가자 동작	CC 파트 3에 포함된 EAL2 보증 요구사항으로부터 유도된 평가 활동을 수행	제품의 분할 테스트 방법에 기초한 테이블을 작성 및 변화에 대한 그래프 작성
분석	TAL2의 경우 TAL1에서 매핑 과정을 수행한 EAL1과는 별도로 TAL1을 기반으로한 입력과 출력값에 대한 테이블 작성을 통해 입력과 출력의 비교를 수행한다. 그러나 EAL1과 EAL2의 수행은 EAL1을 기반으로 이루어지는 추가적인 보증 레벨이 아니므로 관계성 측면에서는 별개로 이루어진다.	

〔표 6〕 TAL2와 EAL3의 매핑

	CEM의 세부 엘리먼트	ISO/IEC 15443의 적용성을 위한 TAL 매핑
세부 엘리먼트	상위 레벨 설계(ADV_HLD.2) 독립적인 표본 시험(ATE_IND.2) 기능 시험(ATE_FUN.1) 시험범위의 분석(ATE_COV.2) 기본설계시험(ATE_DPT.1)	외부적인 시스템의 정보를 기반으로 테스트를 수행한다.
목적	적당한 보증 수준을 제공하기 위한 EAL3는 보안 기능을 이해하기 위해 기능 명세, 설명서, TOE 상위 수준 설계를 이용하여 분석된다.	TAL2의 기본 통합 테스트를 기반으로 하여 외형 정보의 관점에서 수행되는 테스트 레벨
평가 증거 자료	ST의 평가, 형상 관리의 평가, 배포 및 운영서의 평가, 개발서의 평가, 설명서의 평가, 생명주기 지원의 평가, 시험의 평가, 시험, 취약성 판단의 평가	외부적인 정보 테이블을 기반으로 보증 엘리먼트들에 대한 확인 과정을 수행하기 위한 방법(내부 설계서, TAL2의 외부 입출력 테이블, 세부 모듈 설계서, 동작 설명서)
평가자 동작	ST가 어떠한 부수적 활동을 수행하기 위한 근거와 구문을 제공하므로 ST에 대한 평가는 어떤 TOE 평가 활동보다 우선적으로 수행된다.	보증의 방법으로 측정된 보증의 원소 테스트를 보증 제품으로 제공하기 위한 제품의 내부 테스트 수행
분석	EAL3는 TAL2와 매핑이 가능하며 이는 EAL3가 TOE의 부수적인 활동을 수행하기 위한 근거와 구문 제공을 통해 취약성 평가를 수행하게 되므로 TAL2에서 제시되고 있는 외부 테스트를 통해 제품 외형 테스트는 취약성 평가와 동일한 수행 결과를 예측할 수 있다.	

스트이다(〔표 9〕 참조).

2.7 TAL4와 EAL7의 매핑

TAL4는 EAL7과 매핑이 가능하다. TAL4는 화이트 박스와 소스코드 테스트에 부과되어 내부의 모듈의 작동의 테스트 정보에 대한 관점을 두어 수행되는 테스트이다(〔표 10〕 참조).

이상의 연관성과 세부 엘리먼트 매핑을 통해 복합 기능을 갖는 정보보호 제품에 대한 보호 프로파일을 위한 대체 평가 방법론의 추가적인 요구사항과 보안적 제품과 비보안 제품에 대한 평가를 〔표 11〕과 같이 정리할 수 있다.

Ⅳ. 결 론

본 고에서는 정보통신 기술 및 정보매체의 발전, 그리고 인터넷 통신 환경의 변화에 따라 많은 연구와 다양한 접근이 시도되고 있는 정보보호 제품의 대체 평가방법론에 대해 살펴보았다. 이는 국내의 평가 방법론의

〔표 7〕 TAL3와 EAL4의 세부 엘리먼트 매핑

	CEM의 세부 엘리먼트	ISO/IEC 15443의 적용성을 위한 TAL 매핑
세부 엘리먼트	서술적인 상세설계 (ADV_LLD.1) 독립 시험 (ATE_IND.2) 기능 시험 (ATE_FUN.1) 시험범위의 분석 (ATE_COV.2) 기본 설계 시험 (ATE_DPT.1)	외부적인 시스템의 측정 뿐만 아니라 내부적으로 낮은 레벨의 정보를 기반으로 모듈 테스트를 수행한다. (화이트 박스 시험 테스트의 기본 테스트)
목적	최소의 평가 노력을 정의하고 평가를 달성하기 위한 방법과 수단을 제공	TAL2의 기본 통합 테스트를 기반으로 하여 모듈간의 인터페이스를 외형 정보의 관점에서 수행되는 테스트 레벨
평가 증거 자료	ST의 평가, 형상 관리의 평가, 배포 및 운영서의 평가, 개발서의 평가, 설명서의 평가, 생명주기 지원의 평가, 시험의 평가, 취약성 판단의 평가, 평가 출력 작업	외부적인 정보 테이블을 기반으로 보증 엘리먼트들에 대한 확인 과정을 수행하여 내부 모듈에 대한 인터페이스 테스트를 수행하기 위한 방법(화이트 박스 테스트 방법에 필요한 자료: 내부 설계서, TAL2의 외부 입출력 테이블, 세부 모듈 설계서, 동작 설명서)
평가자 동작	ST가 부활동을 수행하기 위한 근거와 구문을 제공	보증의 방법으로 측정된 보증의 원소 테스트를 보증 제품으로 제공하기 위한 제품의 내부 테스트 수행
분석	EAL3는 TAL2와 매핑이 가능하며 이는 EAL3가 TOE의 부수적인 활동을 수행하기 위한 근거와 구문 제공을 통해 취약성 평가를 수행하게 되므로 TAL2에서 제시되고 있는 내부 테스트를 통해 제품 모듈의 인터페이스 테스트는 취약성 평가와 동일한 수행 결과를 예측할 수 있다.	

〔표 8〕 TAL4와 EAL5의 세부 엘리먼트 매핑

	CEM의 세부 엘리먼트	ISO/IEC 15443의 적용성을 위한 TAL 매핑
세부 엘리먼트	TSF에 대한 구현의 표현 (ADV_IMP.2) 상세 설계 시험 (ATE_DPT.2)	TAL4의 경우 화이트 박스 시험을 통해 소스 코드 테스트에 대한 내부의 모듈의 작동 테스트의 정보에 목적을 두어 수행된다.
목적	None	소스 코드에 대한 내부 모듈의 작동 테스트
평가 증거 자료	None	화이트 박스 시험에 요구되는 소스 코드 테스트 설명서
평가자 동작	None	블랙 박스 시험은 기본으로 수행되고 TAL3에서 수행된 모듈 시험과 소스 코드에 대한 모듈의 동작 정보에 대한 수행 테스트를 수행
분석	TAL4와 EAL5의 매핑을 위한 세부 엘리먼트는 설계시 작성되는 소스 코드와 설계 명세서가 요구되며 이는 ISO/IEC 15443에서 같은 형태의 수행 테스트로 기술된다.	

〔표 9〕 TAL4와 EAL6의 세부 엘리먼트 매핑

	CEM의 세부 엘리먼트	ISO/IEC 15443의 적용성을 위한 TAL 매핑
세부 엘리먼트	TSF에 대한 구현의 표현 (ADV_IMP.3) 상세 설계 시험 (ATE_DPT.2)	TAL4의 경우 화이트 박스 시험을 통해 소스 코드 테스트에 대한 내부의 모듈의 작동 테스트의 정보에 목적을 두어 수행된다.
목적	None	소스 코드에 대한 내부 모듈의 작동 테스트
평가 증거 자료	None	화이트 박스 시험에 요구되는 소스 코드 테스트 설명서
평가자 동작	None	블랙 박스 시험은 기본으로 수행되고 TAL3에서 수행된 모듈 시험과 소스 코드에 대한 모듈의 동작 정보에 대한 수행 테스트를 수행
분석	TAL4와 EAL5의 매핑을 위한 세부 엘리먼트는 설계시 작성되는 소스 코드와 설계 명세서가 요구되며 이는 ISO/IEC 15443에서 같은 형태의 수행 테스트로 기술된다.	

〔표 10〕 TAL4와 EAL7의 세부 엘리먼트 매핑

	CEM의 세부 엘리먼트	ISO/IEC 15443의 적용성을 위한 TAL 매핑
세부 엘리먼트	TSF에 대한 구현 표현의 구조화(ADV_IMP.3) 구현 표현 시험(ATE_DPT.3)	TAL4의 경우 화이트 박스 시험을 통해 소스 코드 테스트에 대한 내부의 모듈의 작동 테스트의 정보에 목적을 두어 수행된다.
목적	None	소스 코드에 대한 내부 모듈의 작동 테스트
평가 증거 자료	None	화이트 박스 시험에 요구되는 소스 코드 테스트 설명서
평가자 동작	None	블랙 박스 시험은 기본으로 수행되고 TAL3에서 수행된 모듈 시험과 소스 코드에 대한 모듈의 동작 정보에 대한 수행 테스트를 수행
분석	TAL4와 EAL5의 매핑을 위한 세부 엘리먼트는 설계서 작성되는 소스 코드와 설계 명세서가 요구되며 이는 ISO/IEC 15443에서 같은 형태의 수행 테스트로 기술된다.	

〔표 11〕 복합 기능을 갖는 정보보호 제품의 보호 프로파일 개발을 위한 대체 평가 방법론의 비교 분석

평가 방법론	보안 제품 평가	비보안 제품 평가	복합 제품의 평가	추가적 요구사항
ISO/IEC 9496	X	O	X	보안 평가를 위한 방법론
SCT	O	O	△	정확한 적용 예시
CEM	O	X	X	비보안적 평가 적용
ISO/IEC 15443	다양한 평가 방법론의 적용성을 위한 보증 프레임워크 제시			

〈X : 평가 불가능, O : 평가 가능〉

기반으로 제시되고 있는 CEM에서 고려되지 않았던 표준에 따른 적합성 평가에 대한 한계성과 CEM으로 평가가 수행된 제품의 다양한 수출 활로 개척에 어려움이 있었다. 특히, 복합 보호 프로파일을 개발하기 위해서는 보안 보증 평가뿐만 아니라 표준 적합성 테스트를 추가적으로 만족할 수 있는 평가 방법론을 제시함으로써 IT 보안 제품에 대한 신뢰성을 높일 수 있는 방안에 대한 연구는 매우 미흡한 실정이다. 따라서 본 고에서는 다양화된 환경의 변화에 따라 사용자의 요구가 급증하고 있는 복합 보호 프로파일 개발을 위한 대체 평가 방법론의 기술 분석을 통해 기존 국내 표준 개발의 기반이 되는 CEM과 대체 평가 방법론의 연관성을 제시하고 이에 대한 취약성을 분석하였다. 따라서 복합 기능을 갖는 정보보호 제품에 대한 보호 프로파일 개발을 위해서 기반 연구로 제시되고 있는 다양한 대체 평가 방법에 대한 기술 분석을 수행하고 이를 기반으로 복합 기능을 갖는 정보보호 제품에 대한 보호 프로파일 개발을 위해서 상이한 평가 방법론간의 연관성과 대체 가능성을 분석하였다.

따라서 본 고에서는 다변화하는 IT 보안 제품 뿐만 아니라 기존의 일반 IT 제품에 대한 평가를 위한 방법론을 다각적인 각도로 분석하여 향후 복합 보호프로파일 개발을 위한 평가 방법론의 신뢰성과 안전성을 제공할 수 있을 것으로 사료된다.

참고문헌

〔1〕 Common Criteria Editorial Board, Common Criteria for information Technology Security Evaluation,1996

〔2〕 ISO/IEC, ISO/IEC WD 15443 Information technology - Security techniques - A framework for IT security assurance, 2001

〔3〕 ISO/IEC 10025-2 : Information technology - Telecommunication and information exchange between systems - Transport conformance testing for connection-mode transport protocol operating over connection mode network services - Part 2 : Test suite structure and test purposes

〔4〕 ISO/IEC 8073 : 1992, Information technology - Telecommunications and information exchange between systems - Open Systems Interconnection - Protocol for providing the connection-mode transport service

〔5〕 ISO/IEC 9646-1 : 1994, Information technology - Open Systems Interconection -

Conformance testing methodology and framework - Part 1 : General concepts
[6] ISO/IEC 9646-2 : 1994, Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2 : Abstract Test Suite specification
[7] ISO/IEC 9646-3 : 1992, Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 3 : The Tree and Tabular Combined Notation
[8] NIST, Conformance testing, 2001
[9] NIST, Conformance Requirements Guideline, 2001
[10] NPL, Strict Conformance Testing, 1996
[11] NSA, Key Recovery Agent System Protection Profile, 2000.1.14
[12] NSA, Key Recovery Third Party Requestor Protection Profile, 2000.2.21
[13] NSA, Key Recovery End System Protection Profile, 2000.1.14
[14] Office for Official Publications of the European Communities, Information Technology Security Evaluation Criteria(ITSEC), 1991
[15] Office for Official Publications of the European Communities, Information Technology Security Evaluation Manual(ITSEM), 1993
[16] http://csrc.nist.gov/cc/ccv20/cc2list.htm, The Common Evaluation Methodology (CEM) Editorial Board (CEMEB), Common Criteria for Information Technology Security Evaluation Version 2.0, May, 1998.
[17] http://csrc.nist.gov/cc/cem/cem-p2v06-992.pdf, The Common Evaluation Methodology(CEM) Editorial Board(CEMEB) Common Methodology for Information Technology Security Evaluation, Version 0.6, Jan., 1999.
[18] http://csrc.nist.gov/cc/cem/cem-p2v06-992.pdf, The Common Evaluation Methodology(CEM) Editorial Board(CEMEB) Common Methodology for Information Technology Security Evaluation, Version 1.0, Aug., 1999.
[19] http://www.wiis.co.kr/lab/standardization1.htm
[21] http://eagle.kisa.or.kr/edu/edu2002/edu_20020819/edu_20020823_013.pdf
[22] http://www.npl.co.uk, The UK's national Standards Laboratory for Physical Measurement
[23] http://okpos.com/docs/rfcs/rfc/html/rfc1708.html

〈著 者 紹 介〉

서 대 희(Dae-Hee Seo)
학생 회원

2003년 2월 : 순천향대학교 전산학과 석사
2003년 3월~현재 : 순천향대학교 전산학과 박사과정
〈관심분야〉 암호 프로토콜, 키 관리, 정보보호

이 임 영 (Im-Yeong Lee)
종신회원

1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학전공 석사
1989년 3월 : 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 : 순천향대학교 정보기술공학부 부교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안

정 지 훈 (Ji-Hoon Jeong)
정회원

1981년 2월 : 전북대학교 컴퓨터공학과 졸업
1983년 2월 : 전북대학교 컴퓨터공학과 석사
1993년 2월~2001년 12월 : 한국전자통신연구원 선임연구원
2002년 1월~현재 : 한국전자통신연구원 부설 국가보안기술연구소 선인연구원
〈관심분야〉 정보보호, 보안 평가

채 수 영 (Soo-Young Chae)
일반회원

1982년 2월 : 전북대학교 전산통계과 졸업
1999년 8월 : 숭실대학교 정보통신공학과 석사
1989년 3월~2000년 3월 : 포항종합제철(주), 교보정보통신(주) 시스템 개발
2000년 4월~2001년 9월 : 한국정보보호진흥원 정보보호팀
2001년 10월~현재 : 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호 응용, 보안 평가