情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

IT 보안 평가 스킴에 관한 고찰

서 대 희*, 이 덕 규*, 이 임 영**, 나 학 연***

요 약

세계 각국에서는 산업 및 정보의 의존성에 의해 전세계의 모든 정보를 한눈에 볼 수 있는 시대가 도래하였으며, 사이버 공간 그 자체가 정치, 경제사회, 문화 등의 기본적인 생활 공간으로 자리매김 하고 있다. 따라서 이를 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.

본 고에서는 정보보호 제품을 평가하기 위해 단일화된 국가 평가 기준을 기반으로한 국외 평가 스킴 중에서 미국의 평가 스킴을 예로 들어 그에 대한 분석하고자 한다. 분석된 내용은 국내 정보보호 관리체계를 위한 국내 평가 스킴 개발을 위한 바람직한 추진 방향과 향후 발전방향에 대하여 살펴보고자한다.

Ⅰ. 서 론

컴퓨터 기술의 발달과 인터넷의 확산으로 인하여 전 세계를 하나로 잇는 정보화 사회 구축이라는 꿈을 현실화시키게 되었다. 하지만 정보통신 기술의 발달과 급속한 정보화는 정보의 유출, 파괴, 위·변조, 바이러스, 서비스 방해, 불건전 정보 유통, 해킹 등의 컴퓨터 범죄 등 정보화 역기능이 급속히 증가하여 국가 기반 구조 등 사회 전반에 큰 위협이 되고 있다.

이에 대한 대책으로 미국, 영국, 독일, 프랑스, 캐나다 등의 국가들은 IT 제품의 보안성 평가를 자체적으로 수행하여 왔다. 하지만 세계적으로 개발되는 제품의 수적 증가와 다양성으로 인하여 자체적으로 모든 제품을 평가하기에는 역부족이었다. 따라서 이들의 국가들은 평가결과를 국가들 간에 상호인정하기 위한 국제 표준인 단일의 평가기준 개발에 합의하였다. 이렇게 개발된 공통평가기준은 현재 버전 2.1이 사용되고 있으 며 이는 ISO/IEC JTC 1/SC 27/WG 3를 통하여 ISO/IEC 국제표준으로 등록되었다.

따라서 본 고에서는 국내 공통 평가 체계 수립을 위해 국외의 사례 중 미국의 평가 체계를 중심으로 분석하고 미국의 평가 체계에서 정의하고 있는 보호 프로파일에 대한 개요와 구성에 대해 알아보고자 한다.

Ⅱ. CC와 보호 프로파일의 목적

세계 각국에서는 다가오는 산업 및 사회 일반에서 정보의 의존성을 한층 가속화되고 있다. 현대 사회의 정보화는 컴퓨터의 보급 확산과 공용 네트워크의 발전을 통해 그 범위 또한 확대되고 있으며, 정보가 독점되고 개방되지 않았던 과거와는 달리 현대 사회는 일반인 누구나 인터넷을 통해 세계 곳곳의 정보를 값싸고 편리하게 이용하고 있다. 특별한 관련 지식이 없더라도 누구나 컴퓨터와 모뎀이 있으면 전세계의 모든 정보를 한눈에 볼 수 있는 시대가 온 것이다.

그러나 어느 사회이든 사회가 안정되지 못하면 국민의 경제 활동은 물론 삶의 불편을 초래하게 된다. 현대의 정보 사회에서는 사이버 공간 그 자체가 정치, 경제 사회, 문화 등의 기본적인 생활공간이다. 따라서 이를 보호하지 않으면 안되며 안정된 정보사회 구축은 불가능하다. 정보보호의 대상이 특정 국

* 순천향대학교 정보기술공학부 (1636711@hitel.net), (hbrhcdbr@catholic.or.kr)
** 순천향대학교 정보기술공학부 부교수(inylee@sch.ac.kr)
*** 한국전자통신연구원 부설 국가보안기술연구소(hyna@etri.re.kr)

가기밀에 국한되지 않고 국민의 개인 정보, 사생활 보호, 기업정보, 주요 사회 기반에 대한 정보 등으로 확대되었다. 막대한 보호의 대상을 효율적으로 보호하기 위해서는 국민 각자와 기업 등의 적극적인 참여가 필요할 뿐만 아니라 종래의 보안에 관한 인식과 조직, 법/제도의 틀을 벗어나 국민의 생활과 기업의 경제 활동을 보호하면서 국가안보를 지키는 민간과 공조하는 새로운 제도와 조치가 마련되어야 한다.

국제공통평가기준(CC - Common Criteria)는 선진 각국의 정보보호 제품 평가기준을 국제적으로 단일화하려는 움직임의 결과물이다. 즉, 국제적으로 활용되고 있는 다양한 평가 기준의 단일화를 통하여 상호인증 기반을 구축하고 정보보호 시장확대의 기반을 마련하며, 국자간 정보보호시스템의 평가 결과를 상호인정협정(CCRA)의 기반을 마련하는데 그 목적이 있다.

1993년, 미국(NSA, NIST), 영국(CESG), 독일(BSI), 프랑스(SCSSI), 캐나다(CSE), 네덜란드(NL-NCSA)등 6개국 7개 기관이 합의하여 국제공통평가기준(CC)개발에 착수한 이후, 1996년 1월 버전 1.0을 발표하고, 1998년 5월 버전 2.0이 발표되었고, 1999년 9월 국제표준(ISO/IEC 15408)으로 제정되면서 현재의 버전 2.1이 발표되었다.

CC개발에서부터 주도적인 역할을 해온 미국은 정보보호시스템에 대한 평가/인증 제도를 가장 먼저 실행해온 국가이지만, 국가기관에서 활용하는 정보보호시스템에 한하여 평가/인증제도를 시행해 왔으며, 1998년 들어서 비로소 민간부분에까지 평가/인증 제도를 확대 적용하였다. 또한 국제공통평가기준은 보안요구사항에 유연성을 부여하기 위해 "보호프로파일 (Protection Profile)"이라는 제품 구현에 독립적인 문서를 제공한다. 개발자나 사용자는 보호프로파일을 이용하여 정보보호시스템 개발시 예상되는 보안기능이나 사용자 자신의 조직에 적합한 정보보호제품 보안요구사항을 쉽게 나타낼 수 있다. 국내에서는 국제공통평가를 기준으로 정보보호시스템을 평가할 경우 평가신청인이 제품의 사용 환경을 명확히 하기 위해 보호 프로파일을 작성하여 제출하거나 특정 보호 프로파일을 준수하도록 할 예정이다.

Ⅲ. 미국의 평가 인증 체계 검토

이 장에서는 국외의 평가 프로그램 중에서도 미국에의 보안 평가 및 인증 체계에 대해 살펴보고자 한다.

1. 미국의 평가 인증 체계 개요

CCTP(Common Criteria Testing Program)는 국제공통평가기준(CC)에 기반한 평가·인증 체계를 정립하기 위하여 NIAP(National Security Agency)에서 개발하고 있는 프로그램이다. 국제공통평가기준(CC)에 의한 평가체계는 민간평가기관(CCTL-Common Criteria Testing Laboratory)을 승인하는 인정기관의 역할과 평가결과를 심사하고 확인하는 인증기관의 역할은 NIAP이 수행하며 제품에 대한 실제 평가는 민간평가기관에서 수행한다.

NIAP의 인원은 NIST(National Institute of Standards and Technology)와 NSA(National Security Agency)가 공동으로 구성하는데 공동 감독자, 기술전문가, 관리자, 계약담당자로 이루어진다. NIAP에서 제공하는 활동과 서비스는 다음과 같다.

- 국제공통평가기준(CC) 평가·인증 체계와 평가기관 인정프로그램 개발
- 국제공통평가기준(CC) 기반 시험평가 및 국제상호인정 체계 구축
- 인정된 평가기관, 평가결과 보고서 및 평가제품 목록 관리
- 인정된 평가기관에 대한 전반적인 전문 기술 및 자원 서비스 제공
- 표준, 정보보호제품군에 대한 시험 및 검증 프로그램을 구축하고자 하는 기관 지원
- IT 제품 개발자와 평가시험소에서 사용할 툴 개발
- 정보보호시스템 평가 기술개발을 위하여 산업체와 평가기관 간의 협력 지원
- 국제공통평가기준(CC)을 기반으로 한 보호프로파일 및 시험 방법 개발
- 정보보호제품 시험평가 관련 워크샵 및 교육 프로그램 개발 및 제공
- 성공적인 평가 완료 제품에 국제공통평가기준(CC) 평가인증서 발급

미국은 1996년 CC 표준화를 추진하던 평가방법론(CCEB-Commom Criteria Editiorial Board)에 의해 발표된 "Network/Transport Layer

Packet Filter Firewall" 보호프로파일을 모델로 하여 1997년 "US Government Traffic-Filter Firewall Protection Profile for Low Risk Environ- ment V1.0"을 개발한 이후 NSA와 NIST등 정부기관 주도로 다른 나라들에 비해 가장 많은 보호프로파일을 개발 중이다.

미국에서 개발된 보호프로파일들의 특징은 크게 두 가지로 나눌 수 있다. 첫째로는 대부분이 국가기관 활용을 위해 개발되었다는 것이며, 두 번째로는 OSD(Office of the Secretary of Defense) GIG(Global Information Grid)의 정보보증(IA-Information Assurance) 정책에 따라 조직의 정보가치와 위협수준에 적절한 보안강도 및 보증요구사항을 만족하도록 보호프로파일이 3단계(High, Medium, Basic)로 나뉘어져 있다는 점이다[3,4].

미국 내에 보호프로파일을 개발하는 주체로는 NSA가 후원하는 포럼인 IATFF(Information Assurance Technical Framework Forum)와 정보 보호 시스템 인증기관인 NIAP, 국립표준기술원인 NIST등이 있다. 이들의 보호프로파일 개발 프로젝트 현황을 살펴보면 다음과 같다.

가. NIAP

9.11 테러사건 이후 Firewall, VPN, OS, DB 등 9종의 정보보호시스템에 대한 연방정부용 보호 프로파일 개발 프로젝트와 연방정보처리표준인 FIPS140-1, FIPS140-2를 국제공통평가기준에 적합하도록 하기 위한 Cryptographic Module 보호 프로파일 개발 프로젝트를 진행 중이다.

나. NIST

Biometric Interoperability, Performance and Assurance Working Group 운영을 통해 Biometric에 대한 보호 프로파일를 개발 중이며, 스마트카드 사용자 그룹을 지원 SCSUG-SC보호프로파일을 개발하였고 보호 프로파일 개발을 위한 지침도 제공하고 있다. 현재 NIST 웹 사이트에 공개되어 있는 Biometric의 버전은 버전 0.01이다.

다. NSA

NIAP 및 정보보호업체와의 연계를 통해 보호 프로파일을 개발 중이며, Information Assurance Directorate를 운영하면서 사이버 시스템을 위한 정보보증 솔루션을 개발 중이다.

라. 기타

이외 NIST 산하 Intelligent System Division에서는 Process Control Security Requirements Forum(PCSRF)을 운영하면서 진행 제어를 위한 보호 프로파일을 개발 중이고, US National Information System Security Conference에서는 보호프로파일 개발을 위한 워크샵을 개최하였다. 또한 보호프로파일 개발에 참여한 바 있는 SPARTAR사는 보호프로파일 개발 자동화 도구인 CC-Toolbox를 제공하고 있다.

Ⅳ. 국제 상호인정협정

미국, 영국, 프랑스, 캐나다, 독일, 네덜란드 6개국은 각국의 평가 기준이 상이함에 따라 각국의 평가에 소요되는 노력, 비용과 시간의 중복 소비를 절감하기 위하여 1993년 국제공통평가기준 개발에 합의하였으며 1996년 1월 국제공통평가기준인 버전 1.0을 발표하였다. 또한 1998년 5월 국제공통평가기준 버전 2.0을 발표하였으며 ISO의 국제표준화를 통하여 버전 2.1이 최종 발표되었다.

정보보호 평가기준은 정보보호시스템 신뢰도를 보증하기 위하여 정보보호시스템의 보안기능과 보증요구사항에 대한 등급 기준을 정의한 기술기준이다. 국외의 정보보호시스템 평가기준으로는 1985년 제정된 미국의 TCSEC(Trusted Computer Security Evaluation Center), 1991년에 유럽 4개국(영국, 프랑스, 독일, 네덜란드)이 공동으로 개발한 ITSEC (Information Technology Security Evaluation Criteria), 1993년에 개발된 캐나다의 CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)이 있다.

독일, 미국, 영국, 캐나다, 프랑스 5개국은 자국의 평가기준을 사용하여 정보보호제품을 평가하여 왔으며 평가받은 제품을 다른 평가기준을 활용하는 국가에 판매하기 위해서는 그 국가가 사용하는 평가기준을 활용하여 재평가 받아야만 수출을 할 수 있었다. 이러한 문제점들을 해결하기 위하여 국가들은 국제공통평가기준 국제공통평가기준 개발에 합의하

였으며 아래의 평가원칙을 항시 준수할 수 있도록 평가방법론(CEM-Common Evaluation Methodology for Information Technology Security)을 개발하여 평가자 들의 평가수행에 사용할 수 있도록 하였다.

- 평가의 적절성 : 평가자 들이 대상 보증평가등급(EAL: Evaluation Assurance Level)의 요구사항에 정확하게 일치하는 평가행위만을 수행하여야 한다.
- 평가의 공정성 : 모든 평가는 편견을 배제하여 수행되어야 한다
- 평가의 객관성 : 평가결과는 주관적인 판정이나 견해가 최소화되어 얻어져야 한다.
- 평가의 반복성 및 재생산성 : 동일한 평가증거를 제시한 평가대상물 또는 보호 프로파일에 대한 반복적인 평가는 항상 동일한 결과를 산출하여야 한다.
- 평가의 완전성 : 평가결과는 완전하여야 하며 기술적으로 정확하여야 한다.

이러한 원칙을 사용하여 네덜란드를 제외한 국제공통평가기준 개발에 참여한 독일, 미국, 영국, 캐나다, 프랑스 5개국은 국제공통평가기준과 평가방법론을 사용하여 평가된 제품 중 EAL 1 ~ EAL 4까지의 모든 평가 결과를 상호 인정해 준다는 국제상호인정협정을 체결하였다. 따라서 개발된 정보보호제품이 미국에서 평가를 받았으며 유럽의 영국 또는 프랑스에 수출될 경우 그 나라의 평가기준에 의해 재평가 받을 필요가 없어 재평가에 소요되는 시간, 노력 및 비용을 절약할 수 있게 되었다.

1999년 10월에는 호주와 뉴질랜드가 국제상호인정협정에 사인함으로 인하여 기존의 5개 국가를 포함하여 총 7개 국가가 현재 국제상호인정협정에 가입하였다. 유럽의 경우 ITSEC을 이용한 평가결과에 대한 상호인정협정이 체결되어있었으며 EEA(Europe Economic Area)의 모든 국가가 이에 가입되어있다. 이들 국가들 역시 빠른 시일 내에 국제공통평가기준을 이용한 국제상호인정협정에 가입할 것으로 분석된다. 또한 국내뿐만 아니라 일본을 비롯한 러시아, 우크라이나, 중국 등도 국제공통평가기준에 많은 관심을 가지고 있으며 국제상호인정협정 가입을 추진하고 있는 상황이다.

1. 국제상호인정협정 가입 효과

인정된 평가시험소에서 평가를 받은 민간용 정보보호제품에 대한 상호인정을 합의한 5개국 어디에서나 평가받은 정보보호제품으로 인정받을 수 있다. 따라서 같은 정보보호제품을 여러 국가에서 평가해야 하는 번거로움이 없어졌다. 또한 사용자가 정보보호제품을 구입하고자 할 경우 여러 평가기관에서 많은 정보보호제품을 평가할 수 있으므로 다양한 평가제품목록에서 구입하고자 하는 정보보호제품을 선택할 수 있다. 단시일 내에 평가를 받아야 하는 정보보호제품은 다른 나라의 인정된 평가기관에서라도 급히 평가를 받을 수 있으며 평가 경험이 많은 평가시험소와 계약을 맺음으로써 평가시간을 단축할 수 있다. 또한 저가에 평가를 받을 수 있는 평가시험소에서 평가를 받을 수도 있다.

국제상호인정협정 가입은 이와 같은 장점 외에 국내에서 개발된 정보보호제품을 평가하여 신뢰성이 입증된 제품을 수출함으로써 국내 정보보호제품의 국제경쟁력 향상이라는 기회를 제공하여 주기도 하지만 너무 이른 시기에 가입할 경우 외국의 정보보호제품이 국내 정보보호시장을 장악할 수도 있다는 가능성을 내재하고 있다. 따라서 가입시기에 대한 심도 있는 분석이 필요하다.

2. 국제상호인정협정 가입을 위한 준비

국제상호인정협정에 가입하기 위해서는 사전에 여러 준비가 있어야 하겠지만 우선 국제공통평가기준을 이용하여 정보보호제품을 평가할 수 있는 기술이 필요하다. 먼저 국제공통평가기준은 단일의 평가기준으로 여러 다양한 제품을 평가할 수 있는 기준이다. 따라서 국제공통평가기준은 백과사전과 같으며 특정 제품의 평가를 위해서는 국제공통평가기준을 이용하여 사용자의 요구사항을 정의한 보호프로파일(보호 프로파일: Protection Profile) 또는 제품 개발자가 작성하는 보안목표명세서(ST-Security Target)가 필요하다. 이러한 특정 제품에 대한 보호 프로파일나 ST를 작성할 수 있는 기술을 확보하여야 하며 이러한 기술을 관련 실무자에게 전달할 수 있는 교육 과정이 확보되어야 한다.

또한 국제공통평가기준 기반의 평가·인증체계를 구축하기 위한 법·제도의 정비가 이루어져야 한다.

평가·인증체계에서는 외국의 사례와 같이 평가결과를 인증하는 인증기관, 제품을 평가하는 평가기관, 평가기관을 인정하는 인정기관 등의 역할과 임무가 명확하게 구분되어야 한다. 외국에서는 여러 개의 민간평가기관을 확보하여 정보보호제품 평가의 수요를 충족하고 있으며 민간평가기관은 ISO Guide 25의 요구사항을 기본적으로 만족하여야만 평가기관으로서의 역할을 수행할 수 있다. 특히, 국제상호인정협정에 가입하기 위해서는 정보보호제품 수출·입 관련 국내 법·제도의 정비가 있어야 한다.

국제공통평가기준은 국내 평가기준 개발 방법과는 다르게 다양한 환경에 존재할 수 있는 위협을 고려하여 보안기능을 선택 할 수 있으므로 평가기준의 유연성 및 국제적인 범용성을 갖추고 있다고 할 수 있다. 특히 국제적으로 활용되고 있는 모든 평가기준의 조화(Harmonization)를 이룬 공통의 평가기준을 개발하겠다는 것은 궁극적으로 평가의 상호인증을 위한 골격을 제시함으로 국가간의 상호인정의 틀을 구축하겠다는 것이라고 본다. 전자상거래 및 사이버스페이스에서의 활동이 증대되면 될수록 신뢰구축을 위한 평가된 정보보호제품의 활용이 증대되리라 예측되므로 이와 같은 국제간의 정보보호제품 상호인정에 대한 요구도 높아지리라 생각된다. 더욱이와 같은 정보보호제품 상호인정은 정보보호제품의 국제간의 수출입을 촉진하고 MRA에 가입한 국가들에 대한 국내 정보보호제품 수출 시 무역장벽으로 활용될 수 있다고 예측된다. 그러므로 이러한 MRA 관련 국외 동향에 적절하게 대처하기 위한 관련 전문가들의 의견 수렴을 통한 국내 정보보호산업을 위한 최선의 정책을 개발하여야 한다고 본다.

V. 미국 공통 평가 스킴

1. 인증기관

인증기관은 미국 공통 표준들 평가와 인증을 이행하는 것을 위한 정보 기술 보안에 대하여 계획을 세우기(CCEVS) 위해서 책임 있는 정부 존재이며, 다음의 관리자들에 의해 설립되었다.

- Public Law 100-235, Computer Security Act of 1987.
- National Information Assurance Partnership (NIAP) Letter of Partnership National Security Agency and National Institute of Standards and Technology, dated 22 August 1997.
- NIAP Letter, Establishment of National Voluntary Laboratory Accreditation Program (NVLAP) Laboratory Accreditation Program (LAP) for Information Technology (IT) Security Testing, dated 5 August 1998.
- Common Criteria Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of Information Technology Security, dated 5 October 1998.

인증기관은 국가 정보기술보안을 위해 국가평가인증스킴의 개발 책임을 갖는 조직으로서 국가평가인증체계 하에서 적절한 법적, 행정적 근거 하에 설립되어야 하며, 그 근거에 대한 내용을 명확히 문서화해야 한다. 국가평가인증스킴의 구현에 있어, 인증기관은 국가평가인증체계의 정책 및 국제공통표준상호인정조약의 운영 요구사항을 따라야 한다. 인증기관의 주요 임무는 다음과 같다.

- 국가평가인증스킴의 운영에 대한 정책과 절차 구현 및 수립
- 국가평가인증스킴에 대한 정보의 일반 공개. 이 정보에는 국가평가인증스킴 관련 정보, 검증된 제품 목록, 승인된 평가기관 목록, 스킴 활동 참여와 관련된 각종 양식, 안내서 등이 포함됨.
- 차별이나 지나친 재정적 부담을 지우지 않고, 자격이 있는 모든 조직에 인증기관 서비스를 동등하게 제공. 국가평가인증스킴에 참여하는 모든 이해 당사자들에게 대한 적절한 고려 제공.
- 평가기관의 승인, 시험 방법·기술적 안내·각 평가에 대한 국가 감독(Government Oversight) 제공, 평가기관 활동의 감시 기능
- 평가에 대한 결과가 제시된 증거와 모순이 없는가를 검증하기 위해 평가기관의 평가기술보고서(ETR)를 검토하며, 스킴의 틀에서 수행된 각 평가에 대해서 검증보고서(Validation Report)를 작성
- 국가평가인증스킴의 틀에서 CC에 대한 적합

성을 평가받은 IT 제품 또는 보호프로파일에 대한 인증서를 평가신청인(Sponsor)에게 인증서를 발급
- 인증기관에 위임된 소유권(Proprietary) 정보가 비인가자에게 유출되지 않는 것을 보증하기 위한 대책 수립
- 발행된 인증서의 무결성, CC와 인증기관 로고의 올바른 사용을 촉진
- 국가평가인증스킴에서 발생하는 모든 논쟁에 대한 조정을 수행하며, 불만 및 이의 제기에 대한 절차를 제공
- 인증기관 활동을 문서화하는데 이용하는 인증기관 기록의 생성(Creating), 저장(Storing), 접근(Accessing), 보관(Archiving), 처리(Disposing)를 위한 기록시스템(Record System)의 유지

인증기관은 최종적으로 국제 공통 평가 기준을 기반으로 하여 IT 제품 및 시스템에 관하여 보안 목적을 효과적으로 만족시키고 정책적인 구현을 보장하도록 구성하여야한다. 다음의 〔그림 1〕은 기본적인 인증 기관 조직의 구성이다.

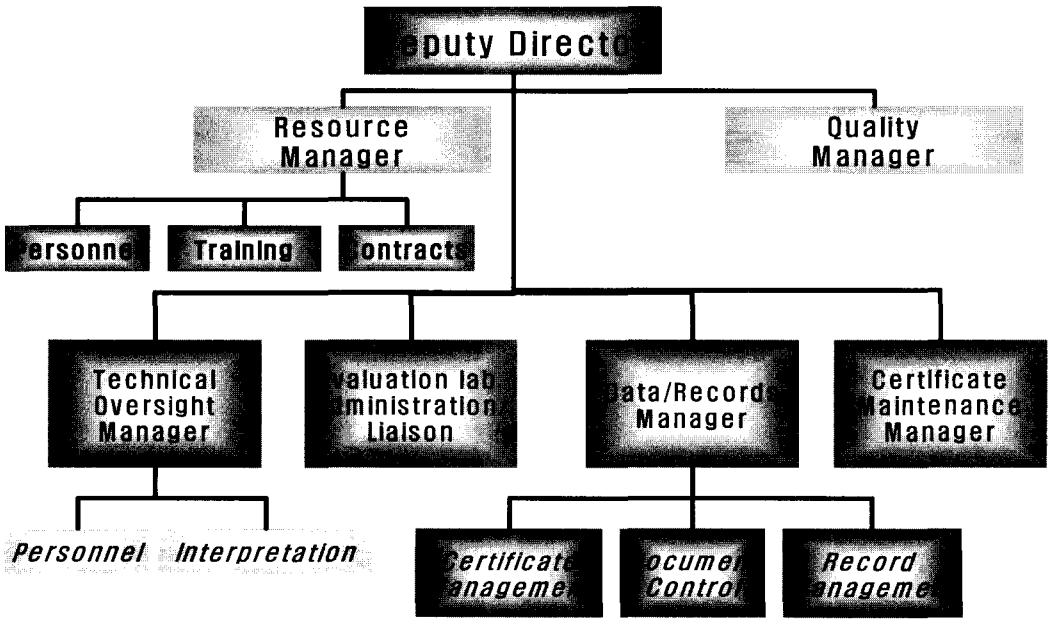
2. CCEVS(Common Criteria Evaluation and Validation Scheme) 인증 절차

평가(예를 들면 제품의 개발자 혹은 보호 프로파일의 개발자)의 스폰서는 계획된 접근법을 통하여 공통 평가에 의한 공통 평가 인증서를 얻는 것에 목적이 있다. 평가에 대한 가격, 지불의 상태 그리고 평가 계획에 대한 토론은 CCTL과 평가 스폰서에게 부여된다.

이와 더불어 CCTL은 보호 프로파일 혹은 IT 시스템의 제안된 내용과 실제적인 관련 내용이 올바른지 결정한다. 스폰서는 인증서 획득을 목적으로 고객과 합의서를 체결할 때 평가 기관과 이해 관계가 없음을 보증해야 한다.

일단 평가 후원자가 CCTL을 선택하면 CCTL 계획의 승인에 대한 평가를 제출하여야 할 동의를 가지고 있다. 신청된 IT 제품 혹은 시스템을 위한 계획은 CCTL이 인증기관에 다음의 사항을 보고해야 한다.

- 평가의 대상(TOE)
- 평가 제품의 설명



〔그림 1〕 기본적인 인증기관 구조

- 판매자나 평가기관 POCs의 이름
- 평가를 위한 평가 계획 계획서

제출된 자료는 인증기관에서 세밀하게 조사해야 하며 2일 내에 제출된 정보를 검토하여 필요한 검증 요구사항을 도출한다. 검증된 결과가 올바르다면 ST, 보호 프로파일, EAL, TOE와 보호프로파일의 복잡성에 대한 초기 검토 결과에 근거하여, 한 명 또는 그 이상의 검증 인력과 책임 검증자(lead validator)가 임명된다. 필요시 검증자의 요구에 따라 추가적인 선임 검증자의 조언 및 지원을 제공될 수 도 있다. 인증기관의 책임 검증자는 모든 정보에 대한 검토를 끝내고, ST 또는 보호프로파일, 평가작업계획(evaluation workplan)을 수립하여, 평가를 위한 검증계획서(Validation Plan)를 작성하며, 책임 검증자는 동시에 기술 감독 관리자에게 검증계획서를 제출한다.

할당된 검증 담당자는 평가와 검증 계획을 검토하고, 일반적인 예상 사항들을 관리하기 위해 평가기관, 평가신청인과의 회의를 갖는다. 이 회의에서 모든 참석자들이 동의하게 되면, 인증기관, 평가기관, 평가신청인은 평가가 공식적으로 평가 스킴에서 수용되었다는 것을 나타내는 평가동의서에 서명하고 모든 활동을 시작한다.

만약, 평가기관이 스킴의 공식적인 승인 없이 평가를 시작하였다면, 인증기관은 그 특정 평가에 대한 검증 서비스를 거부할 수 있다. 대안으로, 인증기관은 모든 스킴의 절차 단계가 수행되는 것을 요구할 수도 있으며, 검증자의 기능 수행을 위해 평가 프로세스가 처음부터 재 시작할 것을 요구할 수도 있다.

평가가 평가 스킴의 틀 안에서 공식적으로 승인되면, 검증과 평가 활동이 시작되는데, 평가기관은 CEM, 평가작업계획, 스킴 프로세스에 따라서 모든 평가 활동을 수행한다. 검증 담당자는 평가기관의 활동을 감독하는 동시에 검증계획에 따라 검증 작업을 수행하는 한편, 검증계획에 따라 검증상태보고서를 준비하고 제출하고, 평가기관이 인증기관에 제출하는 모든 OR(Observation Report)를 조정하고, 인증기관과의 지속적인 인터페이스 역할을 수행한다.

평가가 종결되면, 평가기관은 검증자에게 평가기술보고서(Evaluation Technical Report), 모든 평가 OR 그리고 이에 대응하는 OD(Observation Decision), VPL(Validated Products List) 요약 초안을 제출한다. 검증자는 모든 정보들의 자세한 검토 후, 검증보고서와 권고문을 작성한다. 검증보고서와 VPL 기입 요약문은 작성된 문서의 배포 승인을 위해 평가기관과 평가신청인에게 동시에 전달된다. 또한 검증자는 문서 배포 승인의 동의를 얻기 위해 기술감독관리자에게 최종 권고문을 제출하며 인증기관 국장에게 프리젠테이션을 제출한다.

최종 권고 사항을 이용하여 인증기관 국장은 다음 사항에 대해 최종 결정을 한다.

- CC 인증서 준비 및 VPL을 발간하고 국제상호인정협정 참가국에 통지
- 실패 사실과 이유를 평가기관과 신청자에 통지

가. 평가기관 승인 요구사항

인증기관은 후보 평가기관이 국가평가인증스킴의 틀에서 평가기관으로 등록되는 것을 승인하며, 그에 해당하는 승인 조건 2가지는 다음과 같다.

- 스킴의 평가기관 세부 요구사항 만족
- 인정기관의 인정

인증기관은 인정기관에 평가기관의 인정 여부에 대한 책임을 위임하며, 인증기관은 스킴에서 요구하는 추가 요구사항들에 대한 적합성을 검토한다. 승인을 위한 위의 두 조건들이 충족되면, 후보 평가기관은 인정기관이 인정한 특정 시험 방법으로 IT 보안 평가를 수행할 수 있도록 승인되고, 국가평가인증스킴의 평가기관 목록에 등록되며, 세부 요구사항은 다음과 같이 3가지로 요약해 볼 수 있다.

- 평가기관은 국내에 존재하며, 법적 존재이고, 정당한 법인 조직이고, 유효한 존재이고, 국내 법률 하에 있어야 함.
- 평가기관은 정부의 기술 감독과 스킴에서 수립한 절차와 정책에 따라 평가 관련 활동에 대한 인증을 수용하겠다고 동의.
- 평가기관은 스킴에 의해 수립된 절차와 정책에 따라 평가기관에 의해 수행하는 CC 평가에 있어 국가평가인정체계가 지정한 평가에 국가의 참가를 수용하는 것에 동의.

인증기관은 평가기관의 승인 내용과 관련하여 후보 평가 기관이 제출한 "의향서"를 제출하여 평가 기

관의 승인을 위한 요구사항을 검증하고, 검증 과정의 발견 사항을 문서화한 뒤 인증기관의 문서 및 기록 통제 절차에 따라 5년 동안 보관한다. 또한 발견 사항에 따라 후보 평가기관에 통지하고 인증기관에서 후보 평가 기관이 인정되었을 경우 평가기관과의 합의서를 문서화한다.

나. 평가보증등급(EAL) 5에서 7까지의 평가

현재, 국제상호인정협정에서 상호 인정이 보장되는 평가보증등급은 EAL 4 이하까지이며, 국가평가인증스킴의 절차 및 지침은 이 영역에 대한 평가, 인증에 초점을 맞추고 있다.

그러나, 평가신청인과 평가기관은 인증기관과의 공동 협력을 통해 평가보증등급 5 이상의 평가를 수행할 수 있다. 인증기관은 평가신청인과 평가기관과의 협력을 통해 평가보증등급 5 이상의 평가를 개별적으로(case-by-case) 처리할 것이다. 평가에 요구되는 기술이나 환경에 따라서, 국가는 정부 평가자를 선택하여 작업을 수행하고 그 결과를 평가기관에 전달할 수도 있으며, 평가기관 평가 팀에 정부 평가자를 포함시킬 수도 있으며, 추가적인 평가 방법을 제공하여 평가기관이 평가를 수행하도록 할 수도 있으며, 또는 이러한 것들이 조합될 수도 있을 것이다.

다. 정부의 역할(Government Roles)

평가기관은 평가 팀의 일원으로 임명된 정부평가자(GE, Government Evaluators(s), 평가를 감독하기 위해 임명된 정부검증자(Government Validators)와 정기적인 접촉을 가져야 한다. 다음은 이와 같은 국가평가인증 스킴의 대리인들의 책임에 대해 설명한다.

1) 정부평가자(Government Evaluators)

정부평가자는 평가에 있어 팀 구성원로서 개별적으로 임명된다. 정부평가자는 평가기관과의 조정을 통하여, 훈련 또는 평가 관련 이유 등으로 국가에서 재량적으로 임명하며, 평가기관은 이것을 거부할 수 없다.

평가 팀의 구성원으로, 정부 평가자는 분석, 시험, 평가관련 기록(예: 평가기관 품질 시스템에서 요구되는 문서화, 평가 특유의 작업 계획 또는 개별적인 작업 패키지), 평가 보고서 내용을 포함한 평가 결과의 일정 부분을 작성할 수 있다. 정부평가자는 비록 국가의 피고용인이지만, 개인의 기술, 흥미, 능력 등을 고려하여 평가기관 팀 리더가 할당한 평가 작업을 수행하며, 평가기관 팀 리더의 관리를 받는다.

정부평가인은 평가기관의 프로세스와 절차를 따라야 한다. 정부평가인은 평가기관의 품질 절차를 개발하여서는 안되지만, 평가기관의 품질 절차에 따른 평가자 활동에 대한 증거 서류 작성을 요청 받을 수는 있다. 정부평가자는 검증 활동 작업이나 어떠한 검증 권고문의 번역 작업에 관여하여서는 안된다.

평가기관은 정부평가자를 비용 절감의 목적으로 이용하여서는 안된다. 평가기관이 평가 신청인에게 제출하는 입찰 가격은 평가 팀에 정부 평가자가 추가되는 것이 영향을 미치지 않는다.

2) 검증자(Validators)

검증자는 인증기관과 평가기관 사이의 연결점으로서 역할 및 평가가 국가평가인증스킴 표준을 충족시키며 국제상호인정협정의 요구사항을 만족시키는 것을 보장하기 위해 각 평가마다 임명된다.

검증자는 평가기관에 기술적, 절차적인 문제에 대해 조언을 하지만, 평가 보고서 부분이나 시험 보고서와 같은 평가 증거들을 만들지는 않는다.

수행 작업과 팀 활동의 관여 정도는 매 평가마다 매우 다양하지만, 높은 평가 등급의 경우 시, 작업량과 관여도는 커진다고 할 수 있다.

평가기관이 아닌 검증자의 재량 하에 선택적인 활동들이 수행될 수 있다. 검증자는 팀 훈련에 참여하거나, 팀 미팅을 참관하거나, 시험소의 프로세스와 절차를 관찰하거나 평가 증거들을 검토할 수 있다.

검증자의 주된 산출물은 평가 시 발생하는 문제점에 대해서 평가팀에 제공하는 조언(advise)과 평가 진행 사항에 대해서 인증기관에 제공하는 식견(insight)으로, 검증자는 평가 증거를 작성하지 않는다.

평가 기간 동안, 검증자는 매월 활동 보고서를 작성해서 적절한 포럼에 고시하며, 평가, 이슈, 문제점들의 상태, 진행사항들에 대한 기록을 위해 검증자 웹 페이지 또는 다른 통신 수단에 정보를 제공해야 한다. 평가 작업 종결 시, 검증자는 평가 절차와 평가 팀에 대한 검증 작업을 요약한 검증보고서를 작성한다.

Ⅵ. 보호 프로파일

본 장에서는 평가 스킴에서 기술하고 있는 보호 프로파일에 대한 내용을 논하고자 한다.

1. 보호 프로파일 개요

보호프로파일은 특정 조직이나 사용자가 IT 환경을 분석하여 이에 발견된 취약점들을 제거하기 위한 목적을 달성하는데 필요한 보안 요구사항을 공통평가기준 2부의 보안기능 요구사항과 3부의 보증 요구사항을 추출하여 기술한 문서를 의미한다. 보호프로파일의 완전성 및 완벽성에 대한 평가는 공통평가기준 3부의 APE 클래스를 사용하여 평가한다.

2. 보호프로파일의 구성요소

가. 구성 및 표현

보호프로파일 구성은 [그림 2]에 나타내었다. 보호프로파일은 IT 제품 사용자나 개발자가 작성할 수 있다. 보호프로파일은 필요한 정보보호제품에 포함되어야 하는 보안 요구사항을 기술한 것으로써 어느 누구나 쉽게 이해할 수 있도록 작성되어야 이를 기반으로 요구사항을 만족하는 제품을 개발할 수 있다.

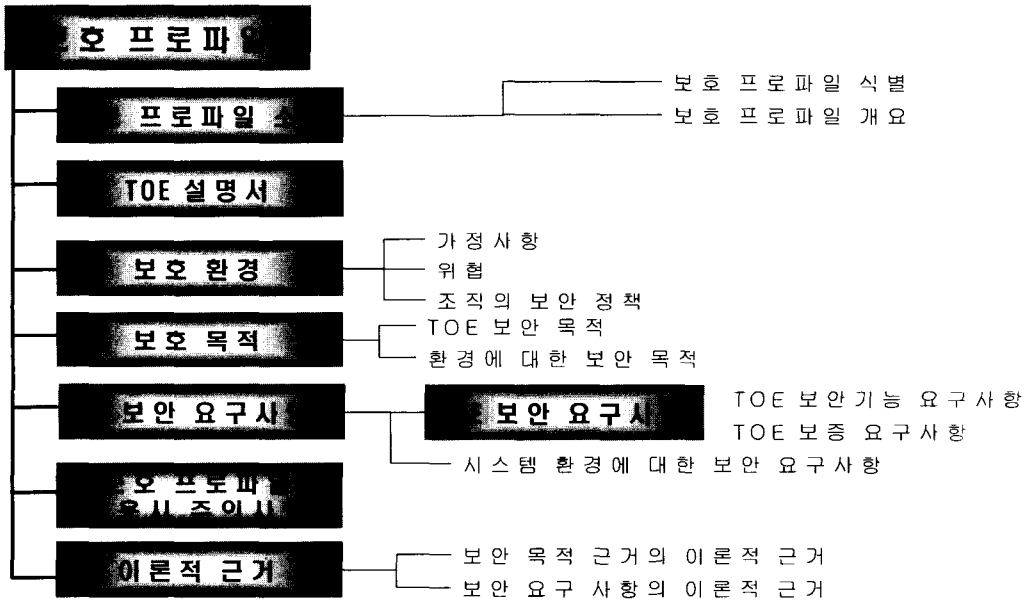
주로 보호프로파일 개발에 있어 가장 많은 시간이 요구되는 부분이 이론적 근거를 작성하는 것이다. 이는 보안 요구사항이 어떠한 이류로 선택되었으며 어떠한 기능을 의미하며 어느 정도의 강도를 가져야 하는지 등 다양한 내용을 작성할 수 있다. 하지만 서술의 깊이와 범위에 대해 특별히 언급한 작성법은 없다.

나. 보호프로파일 소개

보호프로파일은 평가·인증 후 인증기관이 관리하는 인증제품목록에 추가되며 보호프로파일의 소개 절에 포함되어 있는 내용이 보호프로파일을 등록하는데 사용된다. 따라서 보호프로파일 소개 절은 보호프로파일 등록을 위해 필요한 다음과 같은 문서관리와 개요 정보를 포함해야 한다.

보호프로파일 식별은 보호프로파일을 식별, 분류, 등록, 상호 참조하는데 필요한 레이블 및 설명정보가 포함되어야 한다.

보호프로파일 개요는 보호프로파일의 내용을 요약하여 서술한다. 개요는 보호프로파일의 잠재적인 사용자가 보호프로파일에 관심이 있는지를 결정할 수 있도록 상세하게 설명되어야 하며, 보호프로파일 목록과 등록부에 사용될 수 있어야 한다.



[그림 2] 보호 프로파일 구성도

다. TOE 설명

TOE 설명 절은 TOE 보안요구사항의 이해를 돕기 위해 TOE를 서술해야 하며, TOE의 제품 유형 및 일반적인 IT 특성에 대해서도 다루어야 한다.

보호프로파일은 일반적으로 특정 구현에 독립적이기 때문에, 서술된 TOE 특성은 가정사항이 될 수도 있다. TOE가 보안기능을 주요기능으로 갖는 시스템이나 제품이라면, 보호프로파일의 TOE 설명은 이러한 TOE에 적합한 포괄적인 응용환경을 서술하는데 이용될 수 있다.

라. TOE 보안환경

TOE 보안환경 절은 TOE를 사용하려는 환경상의 보안성과 적용하고자 하는 방법상의 보안성을 설명해야 한다. 이 절은 다음을 포함해야 한다.

가정사항은 TOE가 사용될 환경에 대한 보안성을 설명해야 한다. 이는 다음을 포함해야 한다.

- 정해진 용도, 잠재적인 자산 가치, 사용상의 제약사항 등을 포함한 TOE의 정해진 사용법에 관한 정보
- 물리적, 인적, 연결성 측면 등을 포함한 TOE 사용환경에 대한 정보

위협은 TOE나 TOE 환경 내에서 구체적인 보호가 요구되는 자산에 대한 모든 위협을 포함해야 한다. 주의할 점은 사용환경에서 발생 가능한 모든 위협을 열거할 필요는 없고, TOE의 안전한 운영과 관련된 사항만을 서술한다.

위협은 식별된 위협원, 공격, 공격대상이 되는 자산에 대해 서술해야 한다. 위협원은 전문지식, 가용자원, 동기와 같은 측면을 서술해야 하고, 공격은 공격 방법, 취약성, 공격기회와 같은 측면을 서술해야 한다.

보안목적이 조직의 보안정책 및 가정사항에서만 도출된다면 위협에 대한 설명은 생략될 수 있다.

조직의 보안정책은 TOE가 따라야 하는 조직의 보안정책 또는 규칙을 식별해야 하며,L 필요하다면 이를 설명해야 한다. 명백한 보안목적을 설정할 수 있도록 한다는 의미에서도 개별적인 보안정책을 표현하는데 설명과 해석이 필요할 수 있다.

TOE가 물리적으로 분산되어 있는 경우, 보안환경(가정사항, 위협, 조직의 보안정책)을 TOE 환경의 독립된 영역별로 분리하여 설명할 필요가 있다.

마. 보안목적

보안목적 절은 TOE 보안목적 및 환경에 대한 보안목적을 정의해야 한다. 보안목적은 식별된 보안환경의 모든 관점을 다루어야 한다. 보안목적은 보안목적의 의도를 반영하고 식별된 모든 위협을 대응하는데 적합해야 하고, 식별된 모든 보안정책 및 가정사항을 다루어야 한다. 다음과 같은 범주의 보안목적이 식별되어야 한다. 주의할 점은 하나의 위협 또는 조직의 보안정책이 부분적으로 TOE와 TOE 환경에서 모두 다루어지는 경우에 관련되는 보안목적은 각 범주에서 반복되어야 한다는 것이다.

TOE 보안목적은 명확하게 설명되어야 하고 TOE에 의해 대응되는 식별된 위협 및/또는 TOE에 의해 만족되는 조직의 보안정책을 연관시킬 수 있어야 한다.

환경에 대한 보안목적은 명확하게 설명되어야 하고 TOE에 의해 완전하게 만족되지 못하는 조직의 보안정책 또는 가정사항을 연관시킬 수 있어야 한다.

환경에 대한 보안목적은 전체 또는 부분적으로 TOE 보안환경 절의 가정사항 부분에 대한 반복적인 서술이 될 수 있다.

바. IT 보안요구사항

IT 보안요구사항 절은 TOE 또는 TOE 보안환경에서 만족되어야 하는 IT 보안요구사항을 상세하게 정의한다. IT 보안요구사항은 다음과 같이 설명되어야 한다.

TOE 보안요구사항은 TOE의 보안목적을 만족시키기 위해 TOE 및 TOE 평가를 위한 증거 제출물에서 요구되는 보안기능 및 보증요구사항을 정의해야 한다. TOE 보안요구사항은 다음과 같이 설명되어야 한다.

TOE 보안기능요구사항은 TOE에 대한 기능요구사항을 2부에서 도출된 적용 가능한 기능 컴포넌트들로 정의해야 한다.

동일한 요구사항을 다른 측면(예 : 여러 유형에 대한 사용자 신원 식별)에서 다루어야 하는 경우에는 각 측면을 다루기 위하여 2부의 동일한 컴포넌트를 반복적으로 사용(즉, 반복 오퍼레이션의 적용)할 수도 있다.

AVA_SOF.1이 TOE 보증요구사항(예 : EAL2

이상)에 포함되어 있는 경우, TOE 보안기능요구사항은 확률 또는 순열 메커니즘(예 : 패스워드 또는 해시함수)으로 구현된 TOE 보안기능에 대하여 최소 강도 수준을 서술해야 한다. 이러한 모든 기능은 최소한의 수준을 만족해야 한다. 수준은 기능강도-기본, 기능강도-중간, 기능강도-높음으로 구성된다. 수준의 선택은 TOE에 대한 식별된 보안목적과 모순되지 않아야 한다. 또한, TOE의 특정 보안목적을 만족시키기 위하여, 선택된 기능요구사항에 대하여 구체적인 기능강도 측정기준을 정의할 수도 있다.

TOE 보안기능 강도 평가(AVA_SOF.1)는 개별적인 TOE 보안기능에 대해 선언된 강도와 전체적인 최소 강도 수준이 TOE에 의해 만족되는지를 사정할 것이다.

TOE 보증요구사항은 3부의 보증 컴포넌트로 구성된 평가보증등급들 중의 하나로 보증요구사항을 명시해야 한다. 보호프로파일은 3부에 포함되지 않는 추가 보증요구사항을 별도로 명시함으로써 평가보증등급을 확장할 수도 있다.

선택사항인 IT 환경에 대한 보안요구사항은 실제로는 유용하지만, TOE 구현에 직접적으로 관련이 없기 때문에 보호프로파일 구성의 한 부분으로 요구되지 않는다.

다음의 공통조건은 TOE 및 TOE의 IT 보안환경을 위한 보안기능요구사항 및 보증요구사항을 표현할 때 동일하게 적용되어야 한다.

모든 IT 보안요구사항은 2부와 3부에서 도출된 적용 가능한 보안요구사항 컴포넌트를 참조하여 명시해야 한다. 2부와 3부의 컴포넌트 중 어떤 컴포넌트도 전체 또는 일부 보안요구사항에 적용이 불가능하다면, 보호프로파일은 공통평가기준과 관계없이 이들 요구사항을 별도로 명시할 수 있다.

별도로 명시된 TOE 보안기능 또는 보증요구사항은 일치성에 대한 평가와 증명이 가능하도록 명백하고 모호하지 않게 표현되어야 하며, 공통 평가기준에서 제시하고 있는 보안기능 또는 보증요구사항의 상세 수준 및 표현방법에 따라 사용되어야 한다.

오퍼레이션(할당 또는 선택)이 명세되어 있는 요구사항 컴포넌트를 선택하는 경우, 보호프로파일은 보안목적이 만족함을 보이기 위해 필요한 수준으로 요구사항을 보다 상세히 서술하는데 이들 오퍼레이션을 사용해야 한다. 보호프로파일 내에서 수행되지 않은 오퍼레이션은 별도로 식별되어야 한다.

TOE 보안요구사항은 요구사항 컴포넌트에 오퍼레이션을 수행함으로써 필요한 경우 특정 보안 매커니즘의 사용을 선택적으로 규정하거나 금지할 수 있다.

IT 보안요구사항간의 모든 종속관계는 만족되어야 한다. 종속관계는 TOE 보안요구사항 내에 관련 요구사항을 포함시키거나 환경상의 요구사항으로써 만족될 수 있다.

아. 응용 시 주의사항

응용 시 주의사항 절은 선택사항으로, TOE에 관한 구성, 평가, 사용에 대해 유용하거나 관련된 추가정보를 제공한다.

자. 이론적 근거

이론적 근거 절은 보호프로파일의 평가에 사용되는 증거를 서술한다. 이러한 증거는 보호프로파일이 요구사항들의 완전하고 응집된 집합이며, 해당 TOE가 보안환경 내에서 효과적인 IT 보안대책을 제공한다는 사실을 지원해 준다. 이론적 근거는 다음을 포함해야 한다.

보안목적의 이론적 근거는 명시된 보안목적이 TOE 보안환경에서 식별된 모든 측면으로 연관될 수 있으며, 보안목적이 이들을 다루는데 적합한지를 보여야 한다.

보안요구사항의 이론적 근거는 일련의 보안요구사항(TOE 및 TOE 환경)이 보안목적을 만족시키는데 적합하며, 보안목적으로 연관될 수 있는지를 보여야 한다.

보안요구사항들이 전체적으로 상호보완적이며 내부적으로 일관성을 갖는지를 보여야 한다.

보안요구사항의 선택이 정당한지를 보여야 한다. 다음의 경우는 모두 구체적으로 정당화되어야 한다.

- 2부나 3부에 포함되지 않은 요구사항을 선택한 경우
- 평가보증등급에 포함되지 않은 보증요구사항을 선택한 경우
- 종속관계를 만족하지 않는 경우

명시된 기능강도 선언과 함께 보호프로파일에서 선택한 기능강도 수준이 TOE의 보안목적에 일치하는지를 보여야 한다.

Ⅶ. 현재 국내 평가 체제 수립을 위한 고려사항

본 장에서는 국내 평가 체제 수립을 위한 고려사

항을 살펴보고자 한다.

1. 국내 민간 평가 시험소

- 현재의 국내 평가 체제 수립을 위해서는 민간 시험소의 선정과 민간 시험소 인력 확보가 시급하다. 민간 시험소의 선정과 교육은 인증기관에서 반드시 책임 영역에 이루어져야 하지만 현재의 국내에서 이와 관련된 노력이 소극적이다. 따라서 국내 민간 시험소의 설치와 관련된 법규와 선정 과정을 거쳐 이를 교육할 수 있는 프로그램과 인증기관의 능동적인 노력이 필요하다.

2. IT 제품, 시스템 평가 금액의 현실화

- 국내 IT 보안 제품, 시스템을 평가하는 인증기관에서 이루어지고 있는 평가 금액은 현실화 되지 못하고 있다는 것이 일반화된 견해이다. 이는 국내 민간 평가 시험소의 구축과도 관계되며, 보다 능률적 효율적인 평가 활동을 위해 평가 금액 현실화를 위한 많은 공청회와 토론이 필요하다.

3. 보호 프로파일 개발자 및 일반인들을 위한 교육 프로그램 실시

- 국내 평가 체제 수립은 개발자나 일반인들을 대상으로 제출되는 TOE를 대상으로 이루어진다. 따라서 이들에게 CC에 기반한 평가에 적합한 평가 제출물을 작성할 수 있는 능력을 이해하고 적용시킬 수 있는 지속적인 교육 프로그램이 시급한 실정이다. 이러한 프로그램은 국외 사례를 분석하면서 먼저 개발된 국외 보호 프로파일이나 평가 제출물에 관한 내용에 대해 토론할 수 있는 프로그램으로써 국내 정보 보호 제품 시장의 확대와 더불어 많은 평가 제출물을 제출할 수 있는 능력을 함양할 수 있을 것이다.

4. 국제적인 평가 활동에 참여

- 세계 각국에서 독립적으로 자국의 평가 체계를 가지고 IT 보안 제품을 평가하지만, 궁극적으로 개발된 보호 프로파일이나 IT 제품을 전 세계적으로 판매 및 인증 받아 시장을 확대하는데 목적이 있다. 따라서 국내에서도 국제적인 평가 활동에 적극적인 참여를 통해 국제적인 흐름에 맞는 발빠른 대응과 조치로 국내에서 개발된 보안 제품들에 대한 판로 확장 및 기술의 적용을 위한 국제적인 평가 활동의 적극적인 참여가 절실히 필요하다.

Ⅷ. 결 론

정보통신 기술과 정보매체의 발전과 인터넷 통신 환경의 변화에 따라 현재 많은 연구와 다양한 접근이 시도되고 있는 공통평가기준과 보호 프로파일에 대해 살펴보았다. 그러나 아직까지 국내에서 미흡한 연구일 뿐만 아니라 독자적인 활동을 시작하는 측면에서 볼 때 정보보호시스템 시장의 세계적인 확보와 판로개척을 위해 매우 중요한 연구일 뿐만 아니라 향후 국제적인 기술 선점을 위해 반드시 필요한 연구이다. 따라서 이러한 결과를 만족시키기 위해서는 국제공통 평가기준을 선진 도입한 나라의 평가 스킴을 분석하고 해당 보호 프로파일을 분석함으로써 향후 국내 공통평가기준과 보호 프로파일 개발을 위한 기초자료로 활용 될 수 있을 것으로 사료된다.

참 고 문 헌

[1] Guideline for Federal Organization on Security Assurance and Acquisition/Use of Tested/Evaluated Products, US Department of Commerce, NIST Special Publication 800-23, 1998.

[2] 정보보호시스템 평가 인증 가이드 , 한국정보보호진흥원, 2000.

[3] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCIMB, 1999.

[4] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirement, CCIMB, 1999.

[5] Common Criteria for Information Technology Security Evaluation, Part 3 : Security Assurance Requirement, CCIMB, 1999.

[6] 정보보호시스템 평가기준 보안기능 요구사항

분석, 정보통신학회논문지, 2000.
[7] 정보통신부, 정보통신망이용촉진 및 정보보호 등에 관한 법률, 2000.
[8] 정보통신부, 정보통신망이용촉진 및 정보보호 등에 관한 법률 시행규칙, 2000.
[9] 정보통신부 제2002-22호, 정보보호관리체계 인증심사 기준, 2002.
[10] 한국정보보호진흥원, 정보보호관리체계 인증업무 지침, 2002.
[11] ISO/IEC 17799:2000, Information Security Management Code of Practice for Information Security Management, 2000.
[12] 진성우, 국내외 정보보호시스템 보호프로파일 개발 동향, 정보보호심포지움 SIS 2002, 2002.
[13] 이완석, CC기반 평가 시행 실무, 정보보호심포지움 SIS 2002, 2002.
[14] 이병욱, 정보보호관리체계 인증제도 추진현황, 정보보호심포지움 SIS 2002, 2002.
[15] 한국정보보호진흥원, CC기반 평가준비과정, 2002.

〈著 者 紹 介〉

서 대 희 (Dae-Hee Seo)

2001년 2월 : 동신대학교 전기전자공학부(학사)
2001년 3월~현재 : 순천향대학교 전산학과 석사과정
관심분야 : 근거리무선통신, 보안평가체계

이 덕 규 (Deok-Gyu Lee)
학생회원

2001년 2월 : 순천향대학교 컴퓨터공학과 졸업
2001년 3월~현재 : 순천향대학교 전산학과 석사과정
관심분야 : IMT-2000, PKI, DRM

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

나 학 연 (Hac-Yun Na)

1999년 2월 : 숭실대학교 컴퓨터학과 학사
2001년 2월 : 숭실대학교 컴퓨터학과 석사
2001년~현재 : ETRI 부설 국가보안기술연구소 연구원
관심분야 : 정보이론, 보안평가 체계