通信情報保護學會誌
第3卷 第4號, 1993. 12

미국의 새로운 보안 평가 기준서 FC 분석

An Analysis on the U.S. Federal Criteria

윤이중* · 홍주영* · 이대기**

요 약

미국은 안전한 시스템에 대한 평가를 위하여 TCSEC(Trusted Computer System Evaluation Criteria)을 1985년에 발표하였고, 이는 안전한 시스템의 구매자, 개발자, 평가자 들에 의해 사용되었다. 그러나 TCSEC의 적용 경험에서 발견된 문제점의 보완, 상용의 보안 정책의 수용, 각국 평가 기준서들과의 상호 연동성 등의 고려 등 새로운 요구조건들이 제기됨에 따라 NIST와 NSA가 TCSEC을 대치할 새로운 보안 평가기준서를 제작하기 위한 공동의 프로젝트를 수행하게 되었고 1993년 FC(Federal Criteria)의 첫번째 작업 초안을 발표하였다.

본 고에서는 FC의 추진동기, 목적, 구성의 특징 등을 분석하고 현재 시도되고 있는 국제 보안평가 기준서의 작성동향등을 파악함으로써 국내 보안평가 기준서 작성 필요성과 작성시 필요한 사항들을 검토하였다.

1. 서 론

정부와 민간 분야에서의 정보처리 시스템 사용은 계속 증가되고 있다. 이러한 정보처리 시스템 사용의 증가는 정보에 대한 훼손, 불법누출, 절도로 인한 피해 범위를 심화시키는 부정적인 측면도 가지고 있다. 이때문에 선진 각국에서는 이미 시스템의 정보보호에 대한 표준화 및 연구 개발에 많은 노력을 기울이고 있으며 현재 상당한 정도로 발전되어 있다. 일반적으로 정보보호에 대한 요구는 주로 국방 분야에서 있어 왔고 이들이 주요 재원을 지원했기 때문에 국가용, 특히 국방용의 보안 정책을 위주로 하는 작업들이 주류를 이루어 온것이 사실이다. 그 대표적인 예로서 1985년 발표된 다수 사용자 운영체제에 대한 보안 평가 기준서인 TCSEC은 국가/국방용 보안 정책인 분류 정보(classified information)의 불법유출 방지를 기본으로 하여 작성되었다.

TCSEC발간 이후 민간용 보안 요구의 증가, 유럽등 다른 국가 보안 평가 기준서와의 호환성, 정보처리 시스템 기술 발전 등의 변화를 반영하기 위한 새로운 보안 평가 기준서 제정에 대한 요구가 제기되어왔다. 예를 들어 일반 행정 기관을 비롯 금융, 상용의 각 분야마다 정보처리 시스템에 대한 중요정보(sensitive information)처리 요구가 계속 증가하면서 자연히 중요 정보 처리에 대한 보안 요구의 증가를 유발하였다. 그러나 국가/국방용 보안 정책을 기반으로 작성된 TCSEC은 상용 분야의 보안 개념을 포함시키지 못하고 있어 이들의 요구를 수용할 수 없었다. 이러한 이유들로 인하여 1991년 NIST(Na-

* 한국전자통신연구소 연구원
** 한국전자통신연구소 부호기술부 부장

tional Institute of Standards and Technology)와 NAS(National Security Agency)는 새로운 보안평가 지침서를 만들기 위한 공동 프로젝트를 시작하였고 1993년 1월 FC버젼 1.0을 발표하였고 이는 향후 수정 보완 작업을 거쳐 FIPS로 만들어 질 예정이다[2][7].

본 논문에서는 이 FC가 만들어지게 된 배경과 이력, FC의 구성과 특징, 국제 공통 평가서 제작 활동과의 관련성 등을 고찰하여 보안평가서의 국제적인 동향파악은 물론 국내의 보안 평가, 지침서에 대한 이해와 필요성을 강조하고자 한다.

2. FC의 개발 배경

2.1. 평가 기준서의 목적과 역할

평가 기준서의 목적은 이 기준서를 이용하는 사람들의 관점에서 살펴보면 명확해 진다. 기준서를 사용하는 사람들은 사용자, 공급자, 평가자의 세부류로 나누어진다. 사용자측면에서의 필요성은 요구 시스템의 보안기능 및 수준을 정의할 기준의 필요성과 기존에 사용하고 있거나 새로 구매한 시스템의 보안 기능 및 수준의 평가를 위한 기준의 필요성 등이다. 공급자 측면에서의 필요성은 사용자 요구사항과 개발된 보안 기능 및 평가 수준사이에 발생할 수 있는 불일치 제거를 위한 공인된 요구사항 정의 명세서 필요성과 공인 기관의 평가를 받기위한 평가 항목의 지침 필요성 등이다. 평가자 측면에서는 사용자와 공급자가 평가 결과를 신뢰할 수 있는 객관적이고 정확한 평가 절차에 대한 지침이 필요하다. 이러한 관점에서 평가 기준서의 목적을 정리하면 아래와 같다[3].

- 보안 시스템의 보증수준(assurance level)을 평가하는 도구
- 보안 요구 조건 및 수준을 명세하기 위한 근간
- 보안시스템 제작시 보안 기능의 가이드
- 공식승인, 평가, 테스트, 기관들의 지원 도구

2.2. FC의 개발 동기와 이력

가) 개발 동기

TCSEC의 확장 및 대치를 요구하게 된 동기는 아래의 네가지로 집약될 수 있다.

- 융통성(Flexibility)의 요구 : TCSEC은 6개의 평가 계층으로 구성된 매우 엄격한 구조로 구성되어 있어 각 환경에 맞는 보안 요구사항과 평가 수준을 작성할 수 없다.
- Modern Stucture의 적용 요구 : TCSEC개발 당시에 비해 보안의 역할과 환경이 서비스 중심 및 개방 환경에 적합하도록 요구하고 있다.
- 평가 기준의 상호 인정(Mutual Recognition) 요구 : 업계 입장에서는 국제적으로 너무 많은 기준을 상대해야 하는 어려움에 처하게 되어 이러한 기준들을 동일하게 고려하여 상호 인정될 수 있는 적절한 스킴의 새로운 평가 기준서를 요구하게 되었다.
- 상용성(Cermmerciality)의 요구 : 기존 평가서는 무결성과 가용성측면이 결여되어 있으며 상용환경 보다는 국가 보안 요구 중심적이다.

나) 개발 이력과 향후 계획

- 1991년 중반 NIST/NSA 공동 프로젝트로 시작
- 1993년 1월 21일 첫번째 draft 배포
- NIST/NSA FC 설명회 : all-day 세미나, 200여명 참석
- 1993년 3월 31일까지 NIST로 검토 의견 수렴
- 수렴된 의견들을 가지고 4월 초청 워크숍 개최
- 1993년 2월 2일 Brussel FC Workshop : 100여명 참석
- 두번째 draft는 93년 12월로 예정
- 1994년 최종판 출간 예정 : Trusted IT 제품들의 설계, 개발, 평가를 위한 요구 조건으로 FIPS로서 출간될 것이다.
- FCWG(FC Working group)의 향후 연구는 프로화일의 초기 집합들을 분석, 채택하며 다양한 방식으로 비교, 출간하며 새로운 보호 프로화일들의 모범안을 개발할 것이다.
- 이후 부가적인 지침서들과 프로화일들이 FIPS 시리즈로 발간될 것이다.

다) 참여 인원

이 프로젝트의 공동 의장은 NIST의 Gene Troy와 NSA의 Lt.Col.Ron Ross가 맡고 있으며 기타 관련기업 및 연구소, 정보보호 분야의 전문가들이 참여했다.

- NIST/NSA
- MITRE
- IDS(Institute for Defence Analysis)
- Aerospace Corp.
- Galaxy Corp.
- James P. Anderson
- David Bell
- Virgil Gliger(U.of Maryland)
- 카나다 관계자

라) 카나다와의 공동 작업 내용

- CCSE(Canadian Computer Security Establishment)
- 1990년 10월 기준서에 대한 두 정부간의이해의 메모랜덤에 비공식 협정
- 1992년 3월 공식 협정
- 92년 12월 북미 기준서 개발을 위한 원칙에 동의가 있었고 FC프로젝트는 이를 위한 기초가 될 것이다.

마) FC가 근간으로 한 기준서들

- TCSEC
- 유럽의 ITSEC(IT Security Evaluation Criteria)
- 카나다의 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)
- NIST의 MSFR(Minimum Security Functionality Requirements)
- NIST의 요구사항 연구 패널, NIST/NSA의 공동 TTAP(Trusted Technology Assessment Program)작업그룹의 결과물들.

바) 일반용 보안 정책에 관련된 연구

미국의 두개 일반회사인 Bellcore와 American Express Travel Related services(TRS)에서는 그들의 보안 정책에 맞는 보안 요구 사항을 정의 하였다. Bellcore에서는 Bellcore Standard Operating Environments Securty Requirement를 만들었고, TRS에서는 C2-Plus Company Security Standard를 발표하였다. Bellcore 문서에 기술된 보안 요구 사항은 Bellcore상의 보안 평가팀의 경험으로 부터 얻어진 자체 보안 요구사항과 고객 회사들로 부터 제기되는 보안 요구를 기반으로 만들어졌다. TRS사는 C-Plus문서를 작성할 때 TCSEC의 C2레벨의 요구사항이 상용 분야의 요구사항을 상당 부분 포함하고 있음을 파악했다. 따라서 이들은 C2레벨을 기반으로 C2-Plus를 작성하였다. TRS사의 문서를 이용해서 International Information Integrity Instituts(I-4)에서는 CISR(Commercial International Security Requirements)을 작성하여 1992년에 발표하였다. 이 문서에서는 정부 특히 국방분야를 중심으로 한 보안 요구사항(TCSEC)으로는 상용 분야의 보안 요구 사항을 많은 측면에서 수용할 수 없음을 발표하였다.

이렇게 상용 부문에서 보안 시스템과 제품에 대한 수요가 증대되고 기타 여러 요구 사항들이 대두되면서 새로운 평가서의 제작의 필요성이 제기되었다. 미국 정부 기관인 NIST에서는 1992년 MSFR을 발표하였는데 이는 NIST와 NSA가 정부 및 상용의 다수 사용자 운영 체제에서도 적용 가능하다고 생각되는 보안 요구 사항의 최소 단계를 정의한 것이다. MSFR[8]은 TCSEC의 C2레벨과 Bellcore Standard Operating Environment Security Requirements, CISR, DARPA(Defense Advance Research Projects Agency)의 시스템 보안 연구 위원회(National Research Council)에서 발표한 Computers at Risk 등을 참조하여 작성되었다. FC는 이상과같은 정부와 민간 분야에서 이루어진 연구 결과물들을 기반으로 민간용 보안 정책을 수용하였다.

3. FC 구성

FC는 보호 프로화일들을 만들기 위한 요구사항들을 포함한 제1권과 이들 요구사항들의 집합으로 생성된 보호 프로화일을 포함한 제 2권의 두개의 볼륨으로 구성되어 있다. 요구사항들로만 1권을 만든

이유는 기존의 TCSEC이 보안 정책의 변경 및 보안 요구사항의 변경 등을 반영할 수 있는 정립된 방법이 없다는 점을 보완하기 위한 것이다. 즉 어떤 조직에서 기존의 보호 프로화일이 자신들의 환경에 적용될 수 없다고 판단되면 그 조직은 1권의 요구사항들을 이용하여 새로운 보호 프로화일을 만들 수 있다는 것이다. 이와 같은 관점에서 1권은 평가서를 만들기 위한 지침서이고 2권은 이 지침서를 이용해서 만든 평가서라할 수 있다. 그림 1은 FC문서의 구성과 보호 프로화일의 생성관계를 나타내고 있다.

이 요구사항들은 기능 구성요소 15개, 개발보증 구성요소 23개, 평가 보증 구성요소 6개로 총 44개의 항목이 있다. 이들 각각의 구성요소들은 다시 자체적인 기준에 의해서 최대 여섯 단계의 요구수준으로 분류된다. 이러한 요구수준의 분류는 TCSEC의 분류 방법과 동일하다. 예를 들어 TCSEC의 감사(audit)는 다섯 단계로 분류되는데 가장 낮은 최소 감사로부터 기본 감사, 감사 도구, 감사 경고, 실시간 침입 감지 등으로 분류된다. 높게 분류된 것은 하위분류의 요구사항을 포함한다. FC의 2권은 1권에 정의된 구성 요소들의 집합으로 만들어진 일반용 보안 정책을 중심으로한 CS1, CS2, CS3와 정부용 보안 정책을 중심으로한 LP1, LP2, LP3, LP4의 일곱개 보호 프로화일들을 포함하고 있다. 이들 보호 프로

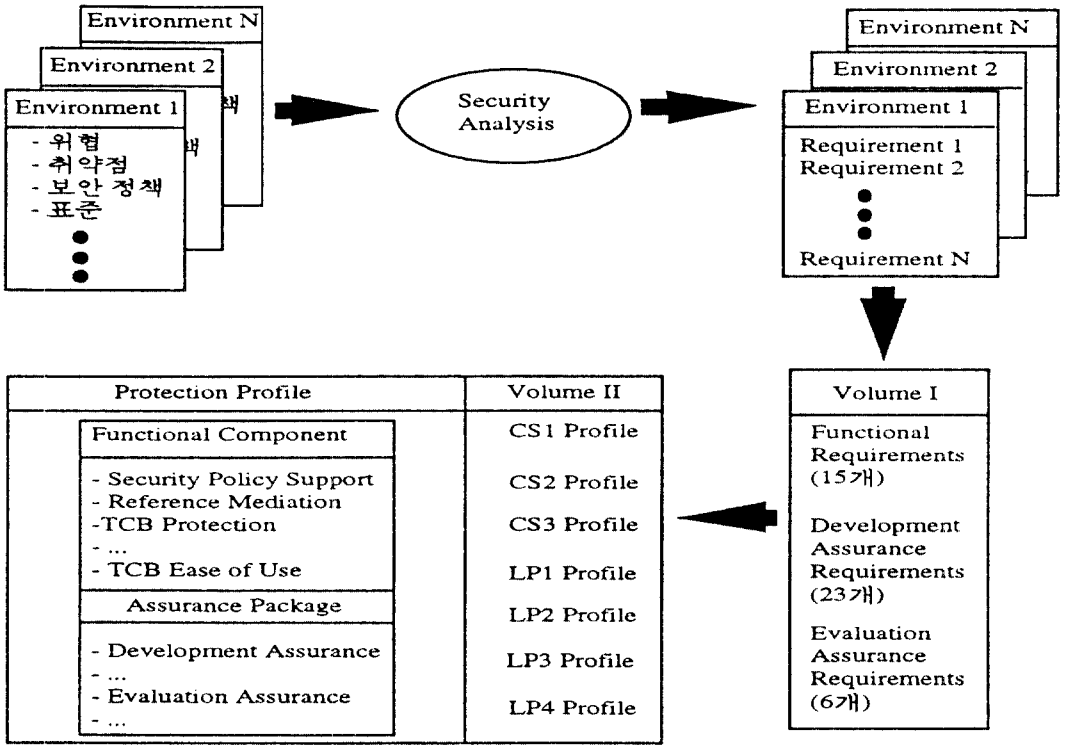


그림 1. FC 구성과 보호 프로화일의 생성 관계

FC			CS1	CS2	CS3	LP1	LP2	LP3	LP4
TCSEC	D	C1	C2			B1	B2	B3	A1

그림 2. FC와 TCSEC 등급의 비교

화일을 TCSEC과 비교해 보면 그림 2와 같다.

3.1. 보호 프로화일

FC의 구성중 가장 특이한 것은 보호 프로화일의 개념이다. 보호 프로화일은 보안 시스템에 대한 보안기능 요구사항과 보증성 요구사항을 정의한다. 보증성 요구사항은 개발 보증성 요구사항과 평가 보증성 요구사항으로 나누어진다.

보호프로화일은 다섯개의 부분으로 나누어진다.

1. 서술적 요소
2. 기본 정책
3. 기능 요구 사항
4. 개발 보증 요구 사항
5. 평가 보증 요구 사항

보호 프로화일 내의 기능 요구사항, 평가 보증 요구사항들은 1권에 기술된 구성요소로 부터 나온다. 이들 구성요소들은 특정 변수들에 의해서 세부적인 요구수준들로 분류된다. 보호 프로화일은 보안 시스템을 구매하려는 사용자나 또는 생산자에 의해서 만들어지며 생성, 분석, 채택, 등록의 과정을 거친다. 그러나 분석, 채택, 등록에 대한 절차는 현재 정의되지 않았다.

3.2. 기능 요구사항(Functional Requirements)

여기서 언급된 요구사항들은 보안시스템의 각기 다른 사용 환경과 위협에 따라 적용할 수 있는 보호 프로화일을 생성할 수 있게 해준다. 또한 이들은 기술의 발달과 경험들로 부터 발생한 변화를 반영하기 위해 보호 프로화일을 확장또는 재구성할 수 있게 해주며 CTCPEC, ITSEC, TCSEC 등 기존의 평가서와 조화를 이룰 수 있게 해준다. 이들 구성요소들은 그림 3과 같이 15개의 부류로 나눌 수 있고 이들은 TCB(Trusted Computing Base)의 구성요소가 되며 일반용과 비일반용 환경 모두를 고려하여 만든 것이다. 이들 요구사항들은 적용 개체 범위(scope), 지원 범위(coverage), 적용 개체 어트리뷰트 범위(granularity), 강도(strength) 등 네가지 요소에 의하여 최대 여섯 단계로 분류된다.

3-2-1. 요구수준 측정 변수

가) 적용 개체 범위(scope)

개체는 사용자, 주체, 객체, TCB 함수, 응용프로그램 인터페이스 등이며, 각 요구사항들은 이들 각개체의 전체 또는 특정 부분 집합에 적용될 수 있다. 즉 각 구성요소의 기능은 모든 개체들에 적용되지 않는다. 예를 들어 신뢰 경로(trusted path)는 로그인시에만 적용되고 패스워드의 변경등에는 적용되지 않는다.

나) 적용 개체 어트리뷰트 범위(granularity)

각 구성요소의 기능은 특정 개체의 어트리뷰트 부분 집합에 적용된다. 예를 들어 액세스 제어는 주체와 객체의 액세스 권한 어트리뷰트에는 적용되지만 그들의 상태정보에는 적용되지 않는다.

다) 지원 범위(coverage)

지원 범위란 각 구성요소의 기능 요구수준을 의

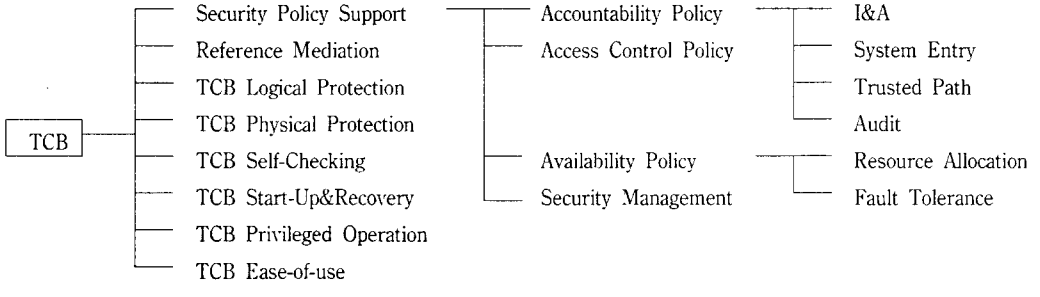


그림 3. 기능 요구사항의 구성요소

미한다. 예를 들어 구성요소 중의 하나인 감사 기능에서 최소 감사 요구 수준과 실시간 침입 감지 요구 수준 사이에서 어느 요구수준의 감사 기능을 제공하느냐 하는 문제이다.

라) 강도(strength)

강도란 예상되는 공격들에 대한 방어 능력을 말한다. 예를 들어 패스워드를 정하는 규칙은 사람의 추측에 의한 공격은 막을 수 있으나 컴퓨터를 이용한 공격에는 취약하다.

3-2-2. 기능 구성요소

가) 보안 정책 지원(Security Policy Support)

이 항목은 그림 3에서 보는 바와 같이 네가지로 분류되고 그 각각은 다시 세부적인 기능 구성요소로 이루어진다. 이들 기능 구성요소는 위에서 설명한 네가지 변수로 요구수준을 나누며 TCB 인터페이스를 통해 지원 된다. TCB에 구현되어야 하는 기능 구성요소의 요구 수준은 제품의 보안 목적과 위협 환경에 따라서 결정된다. 그리고 상기 기능 구성요소가 구현된 TCB의 보안 목적 달성 여부는 다음과 같은 세가지 항목에 의해서 영향을 받는다.

- TCB 기능으로 구현된 제품 보안 정책과 조직 보안 정책 사이의 일관성
- 시스템 관리자에 의한 시스템의 운영과 입력자료 정확성
- 패스워드 선택과 같은 일반 사용자들의 행위

나) 참조 조정(Reference Mediation)

객체, 자원, 서비스에 대하여 TCB 외부의 모든 주체가 행하는 액세스는 TCB 기능을 통하여 보안 정책에 맞는지 검사되어야 한다. 이 요구사항을 만족하기 위해서는 참조 조정 기능이 제공되어야 한다.

다) TCB 논리적 보호(TCB Logical Protection)

외부의 방해 또는 간섭으로 부터 TCB를 보호하는 것은 보안시스템의 가장 기본적인 구성요소이다. 이 구성요소는 TCB 기능 수행을 위해 사용 가능한 최소한 하나의 도메인을 확보하여 TCB를 권한 없는 주체에 의한 외부 방해, 간섭으로 부터 보호하여야 한다는 것이다. 이를 위해 TCB는 자체 보호기능(self-protecting)을 이용하여 권한 없는 주체가 TCB를 변경 또는 파손하는 것을 방지하여야 한다.

라) TCB 물리적 보호(TCB Physical Protection)

TCB는 물리적 방해나 간섭으로 부터 보호되어야 하고 보호된 환경에서 운영되어야 한다. 이를 위해 TCB는 패키지화 되어야 하고 물리적 변경과 간섭의 감지 및 이들 위협에 대한 저항력의 측정이 가능하도록 운영되어야 한다.

마) TCB 자체 검사(TCB Self-Checking)

TCB가 보안정책에 따라 운영되는지의 여부와 보호 기능에 연관된 데이타 구조가 일관성을 가지고 운영되어짐을 확인할 수 있는 하드웨어, 소프트웨어 또는 펌웨어등으로 지원되어야 한다. 이를 위하여 여러가지 오류로 부터 발생하는 보호 기능 연관 코드와 데이타 구조의 훼손 감지 및 수정 작업의 실시 등이 필요하다.

바) TCB 가동과 복구(TCB Start-up and Recovery)

TCB는 보안시스템의 보호 기능을 훼손시키지 않고 가동되고, 오류 발견 후에 보호 기능의 훼손 없이 복구될 수 있어야 한다. 이 요구를 만족하기 위해서 TCB의 최초 및 복구후 상태는 보안 정책, 참조 조정, TCB 보호 요구 사항을 만족해야 한다.

사) TCB 최소 권한 운영(TCB Privileged Operation)

TCB 함수들은 그들 목적을 수행하기 위해 필요한 최소한의 권한만을 소유하여야 한다. 이를 통하여 TCB 메카니즘의 오류로 부터 발생할 수 있는 피해를 최소한으로 줄일 수 있다.

자) TCB 가용성(TCB Ease-of-Use)

TCB에 대한 일반사용자, 시스템 관리자, 응용 프로그램의 사용이 활발히 그리고 적극적으로 사용될 수 있도록 하기위한 기능을 제공해야 한다.

3.3. 개발 보증 요구사항(Development Assurance Requirements)

개발 보증이란 특정 보안 시스템이 보호 프로화일의 기능 요구 사항을 만족하는지 보이는 것이다. 개발 보증 요구사항은 개발자가 제품의 설계, 구현, 문서화, 지원, 유지보수 시에 따라야 하는 의무사항들로 이루어진다. 개발자는 이 요구사항을 따름으로서 제품의 보안 기능이 보호 프로화일의 기능 요구 사항을 만족한다는 구매자와 평가자의 신뢰를 향상시킬 수 있다. 개발 보증 요구사항들의 조합에 의해서 다양한 신뢰 등급이 설정되고, 이들 각 구성요소들은 기존의 평가서 내용을 포함하고 지난 10여년간의 실제 적용에서 발생한 문제점들을 반영했다. 이들 구성요소들은 특정 제품에 독립적인 방식으로 정의하여 적용 범위를 확장시켰다. 개발 보증 요구사항의 구성요소들은 기능 요구 구성요소들과 동일한 방식인 적용범위(scope), 정확성(precision), 지원범위(coverage), 강도(strength)의 네가지 변수에 의해서 요구수준이 분류된다.

2-1-1. 개인식별 프로토콜

가) 적용 범위(Scope)

적용 범위란 제품의 개발, 지원, 유지보수 등의 보증 방법이 모든 기능 요구사항에 적용되었는지의 여부와 제품 개발, 유지보수, 운영절차의 모든 단계에 적용되었는지의 여부를 의미한다. 예를 들어 covert-channel 식별 방법은 디자인 스펙 단계에 적용되고 구현 단계에는 적용되지 않는다.

나) 정확성(Precision)

보증 방법의 정확도는 제품의 개발, 유지보수, 운영에 적용 될때의 상세 단계를 의미한다. 예를 들어 분석 방법이 기능 구성요소의 서술, 비정형 스펙, 정형화 스펙에 적용될 때의 정확도가 다르다.

다) 지원 범위(Coverage)

보증 방법이 기능 구성요소에 전체적 또는 부분적으로 적용되는 지의 범위를 결정한다. 예를 들어 보안 검사는 모든 검사 조건을 사용할 수 있고 또는 그중 일부분 만을 사용할 수 있다.

라) 강도(Strength)

보증 방법의 강도는 대상 방법의 특성에 따라 정해진다. 예를 들어 자동적인 구성 관리 방법 또는 도구는 당연히 운영자 제어 방법 보다 강하다.

3-3-2. 개발 보증 구성요소

가) 개발 과정(Development Process)

개발 단계에서 개발자가 보안 제품의 분석, 설계, 구현시 꼭 수행해야 하는 행위가 네가지 범주로 정의되어 있다. 개발 단계의 구성요소들은 보호 기능의 정확한 구현에 대한 주요한 보증 요구사항들이기 때문에 대부분의 보호 프로화일에 포함되어 있다. 프로화일 내에서의 구성요소의 요구수준 선택은 프로화일 내의 보증 구성요소들 사이와, 기능 구성요소와 보증 구성요소들 사이의 의존도에 의해서 결정된다.

나) 운영 지원(Operational Support)

개발자는 사용자가 제품을 안전하게 사용할수 있도록 그림 4의 네가지 구성요소를 따라야 한다. 이들 구성요소는 개발자가 TCB 생성, 설치, 운영에 대한 절차를 명확히 알려 줄 것을 요구한다. 또한 제품의 설치나 구성을 할 수 있는 도구나 절차를 제공할 것을 요구한다. 그림 4의 처음 두개의 구성요소는 모든 보호 프로화일에 다 포함되는 것이고 나중 두 개의 처음 것은 중간 정도의 보증단계 후자는 높은 수준의 보증을 요구하는 경우에 포함된다. 프로화일 내의 구성요소 요구수준 선택은 보증 목표와 보증 구성요소들 사이의 의존성에 따라 결정된다.

다) 개발 환경(Development Environment)

개발 환경 요구사항은 보안 제품에 대한 배포 제어절차, 유지보수, 개발의 질에 대한 보증 구성요소로 구성된다. 이들 구성요소는 개발자가 제품의 개발과 유지보수시 공학적 절차에 따르고, 제품구성에 대한 제어를 설정하고, 제품 배포시에 발생하는 TCB 불법 변조의 방지와 감지할 수 있는 기술적 수단을 채택할 것을 요구한다. 이의 가장 중요한

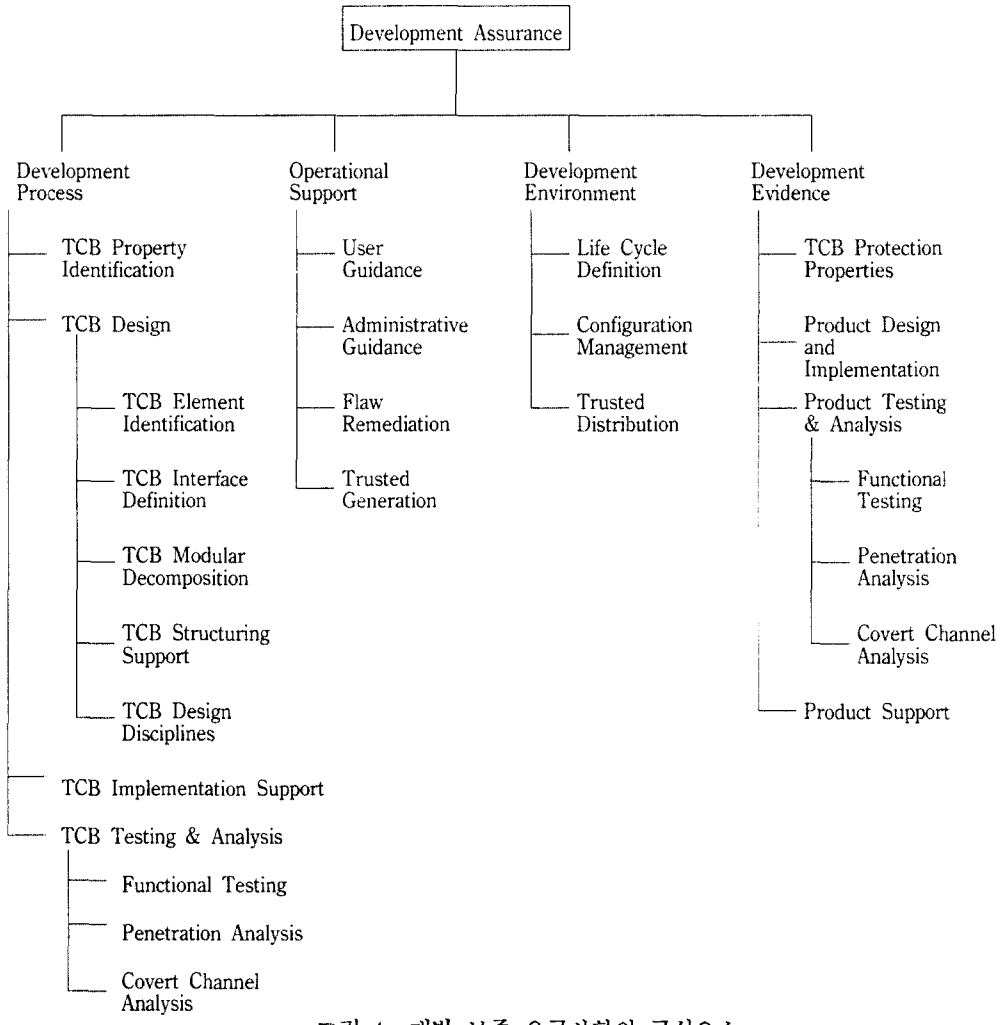


그림 4. 개발 보증 요구사항의 구성요소

개념은 개발 단계와 운영 지원 요구사항이 개발자의 공학적 절차로 통합되었다는 것이다. 이 항목은 중간 또는 상위의 보증을 요구할때 보안 프로화일에 포함된다. 프로화일 내의 구성요소 요구수준 선택은 보증 목표와 보증 구성요소들 사이의 의존성에 따라 결정된다.

라) 개발 증거(Development Evidence)

개발 증거 요구사항은 개발자가 위의 세가지 보안 요구사항이 만족되었음을 보이기 위해 작성 유지 해야하는 문서에 관한 것이다. 이 문서에는 TCB 보호 특성, 개발과정, 제품 검사와 분석, 제품 개발 지원 사항 등 네가지가 정의된다.

3.4. 평가 보증 요구사항(Evaluation Assurance Requirements)

제품 평가는 보안 제품이 보안 프로화일의 요구사항을 만족하는 지를 확인하는 과정이다. 실질적으로 위협에 대한 방어는 제품의 보호 기능과 품질이다. 사용자는 이들에 대한 평가 정보를 대부분

개발자의 자료에 의존한다. 그러나 이러한 정보가 개발자와는 독립적인 방법으로 제공된다면 소비자는 일반적으로 개발자가 제시한 평가 자료보다 더 많은 신뢰를 하게 된다. 여기에서 품질이라는 것은 기능 요구사항 측면에서의 정확성과 타당성, 설계 측면서의 구현의 정확성, 효과, 효율성들을 의미한다. 보안 프로화일 내의 평가 보증 요구사항은 평가 절차중 따라야 하는 최소한의 요구 사항을 포함한다. FC의 평가 보증 요구사항은 향후 특히 많은 논의를 거쳐야할 부분이다.

가) 검사(Testing)

이들은 TCB가 기능 보안 요구사항을 만족하는지를 검사하고, TCB 특성 정의를 위한 요구사항과 TCB 검사와 분석 검증이 이루어 졌는지를 확인하는 두가지로 이루어져 있다.

나) 조사(Review)

개발환경 조사와 운영지원 조사로 나누어지며 개발 보증 요구사항의 운영지원과 개발 지원 측면을 따랐는지를 확인한다.

다) 분석(Analysis)

설계 분석과 개발분석으로 나누어지고 보호 프로화일에 정의된 개발 보증 요구사항인 TCB 설계와 TCB구현 요구사항을 따랐는지 확인한다.

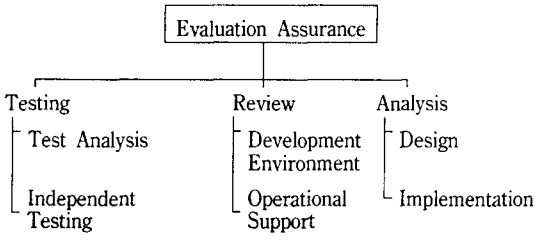


그림 5. 평가 보증 요구사항의 구성요소

4. FC의 개선점과 논의 사항

4.1. FC의 개선점

FC 1권은 평가 기준서의 논리와 체계를 개발한 것으로 기존의 Rainbow 문서의 개념을 확장, 보완하였고 개발 및 평가에 대한 보증(assurance) 개념은 기능성에 대한 요구조건들 보다 효과성(effectiveness)에 많은 비중을 둔 유럽의 ITSEC의 영향을 받아 발전하였다. TCSEC과 MSFR로 부터 얻어진 감사와 신분확인 및 신분 인증 분야에 상당한 보강이 이루어졌다. 특히 accountability와 감사 부분은 상용 시스템이 수용 하게된 기능과 보안 메카니즘이 무엇인가에 대해 상당히 상세히 제공하고 있다. 또 다른 개선점은 각 보안 레벨에 대해 예견되는 위협들을 명확하게 정의 한것이다. 이러한 개선 사항은 제안된 어떤 평가 기준서보다도 좋은 점이며 사용자를 교육하는데 도움이 되며 시스템 운용시 더 나은 보안 관습(security practice)들을 적용하도록 할 것이다.

4.2. FC의 논의사항

FC가 배포된 이후 관련 기관 및 민간 회사, 연구소, 학교 등에서 이에대한 논의가 활발히 진행되고 있다. 이 논의문 가운데는 FC 역시 일반용 보안개념을 만족하지 못한다는 것과 현재 요구되고 있는 보안 기능들 중 포함되지 않은 것들이 많다는 것이 주류를 이루고 있다. 본 절에서는 FC에 대한 비판들을 정리하였다[6].

가) No networking

현재 컴퓨터들이 그저 stand-alone 상태로 운영되지 않는 것이 실제 상황임에도 FC는 TCSEC과 마찬가지로 웍스테이션, 소형, 대형컴퓨터의 다수 사용자 운영체제에 대해서만을 언급하고 있다.

나) No data confidentiality

패스워드의 암호를 명세하는 것을 제외한 기타 정보에 대한 비밀성 요구사항이 포함되어 있지 않다.

다) No data integrity

이는 일반용 보안 정책에서 매우 핵심적인 문제로 제기되고 있음에도 FC는 이를 충분히 반영하지 않았다.

라) No message nonrepudiation

부인 봉쇄 기능은 특히 네트워크 환경에서는 매우 중요한 보안 서비스이다. 92년의 MSFR의 3분의 2 정도의 특성들이 이에 관해 중점적으로 다루어 있으나 FC에서는 자료 정확성과 유용성 측면에서 이러한 항목들이 필요함에도 불구하고 언급하지 않았다.

마) Nothing about viruses or other malicious software

TCSEC에서 C등급을 얻기 위해서는 제품은 서브시스템이나 부속품이 아닌 하나의 완전한 시스템이어야 한다. 이러한 특성은 오랜 동안 논쟁의 대상이 되어 왔다. 대부분의 업체들은 하나의 단독 시스템보다는 기존의 컴퓨터나 운영체제에 올려질 보드나 소프트웨어 형태의 서브시스템들을 제작하고 있다. 이러한 패키지들이 컴퓨터에 올려지면 주어지는 보안 레벨은 TCSEC기준으로 서브시스템에 대한 D레벨(D1, D2, D3)이 된다. 그러나 대부분의 제품들은 C2 요구조건들 이상을 만족시키는데 이로 인해 C2-functonality라는 용어까지 나오게 되었다. 이러한 문제점이 있음에도 FC 역시 서브시스템에 대한 언급을 하고 있지 않다. 이는 실제의 상이한 환경들의 관계성들을 거의 고려하지 않았다는 것을 의미한다. FC는 운영체제의 개발자들이 이 평가서에 맞는 자신들의 새로운 버젼의 제품들을 만들 것으로 가정하고 있는 것으로 보이는데 사실 다양한 운영체제들을 동작시키는 많은 다른 시스템들이 공존하고 있으며 제삼자로써 보안 강화 제품들을 만들어 내는 것이 흔한 일이다. 따라서 시스템 통합자들은 동종의 통일적인 한 시스템을 이질적인 방식으로 조작 하게 될지도 모른다.

5. FC와 각국의 보안 평가서의 비교

국제적인 평가 기준서 작성에 대한 기업들의 요구가 카나다, 미국, 일본, 유럽 등에서 제기되었고, 이러한 요구에 의해 국제 통합 보안평가 기준서의 작성 작업이 ISO와 북미 연합 등을 중심으로 진행되고 있다. 기존에 발간되어 있는 미국의 TCSEC, 카니다의 CTCPEC, 유럽의 ITSEC등 각국의 각국의 보안평가 기준서들을 분석해보면 공통적으로 기능 요구사항과 보증 요구사항의 주요한 두가지 요구사항들로 구성되어 있다. 국제 통합 보안 평가서에 대한 요구사항을 고려하여 작성된 FC를 기능 요구사항과 보증 요구사항 측면에서 각국의 보안 평가 기준서들과 비교해 본다[1].

5.1. 기능 요구사항의 비교

기존의 대표적인 네개의 보안 평가서들은 각기 다양한 방식으로 기능 요구사항을 표현하고 있다. 이들중 FC는 카나다의 CTCPEC과 상당히 비슷한 방법으로 정의되어 있다. ITSEC은 그림 6에서 보이는 것과 같이 요구하고 있는 기능 요구사항이 극히 적지만 반면에 보증 요구사항을 강조했다. 기능 요구사항의 빈약으로 인한 문제점은 ITSEC으로 평가받은 제품들 상호간에 서로 쉽게 비교가 되지 않는다는 것이다. 즉 제품들에 구현된 기능들이 각각 다르기 때문이다. 반면에 FC와 CTCPEC은 기능요

보안 평가 지침서 / 보안서비스	TCSEC	ITSEC	CTCPEC	FC
Functional Component	0	–	0	0
Discretionary Access Control	0	–	0	0
Mandatory Access Control	0	–	0	0
Object Reuse	–	–	0	0
Integrity Access Control	0	–	0	0
Least Privilege	0	–	0	0
Self-test	0	–	0	0
Physical Integrity	–	–	0	0
Rollback	–	–	0	0
Containment	–	–	0	0
Robustness/Fault Tolerance	0	0	0	0
Trusted Recovery	0	–	0	0
Audit	0	–	0	0
Identification/Authentication	0	–	0	0
Trusted Path	0	–	0	0
Covert Chanenels	–	0	–	0
Ease of Safe Use	0	–	0	0
Reference Mediation	0	–	0	0
TCB Protection	0	0	0	0
Physical Protection	0	0	0	0

그림 6. 각국 보안 평가 기준서의 기능 요구사항 비교표

구사항에 거의 동일하고 TCSEC역시 fault tolerance 등과 같은 몇가지 기능을 제외하면 많은 기능 요구사항을 정의하고 있다[1][5][9].

5.2. 보증 요구사항의 비교

보증 요구사항측면에서 보안 평가 기준서들은 그림 7에서 보는 바와 같이 상당한 정도의 상호 호환성을 유지하고 있다. ITSEC은 다른 보안 평가 기준서들보다 보증 요구사항이 매우 엄격하지만 전체적인 기본 개념 측면에서는 ITSEC의 E-레벨과 CTCPEC, FC의 T-레벨은 동일하다 할 수 있다.

TCSEC	ITSEC	CTCPEC	FC
-	-	T-7	-
A1	E6	T-6	T-7
B3	E5	T-5	T-6
B2	E4	T-4	T-5
-	-	-	T-4
-	-	T-3	T-3
B1	E3	T-2	T-2
C2	E2	T-1	T-1
C1	E1	-	-
D	E0	-	-

그림 7. 각국 보안 평가 기준서의 보증요구 등급 비교표

6. 결 론

본 고에서는 FC의 발간 동기를 TCSEC의 실제 적용 과정에서 발생한 문제점들과 환경의 변화를 중심으로 분석하였고, FC구성에 대한 기본 개념과 개선 사항, 미비점 등에 대하여 연구하였다. FC는 기존의 평가 기준서가 가지고 있는 구조적 엄격함에서 발생한 융통성의 결여를 보완하기 위하여 보호 프로화일 개념을 도입하였고, 이를 통하여 특히 민간 분야의 보안 요구 사항을 포함하였다. 이러한 융통성의 도입으로 각 환경에 맞는 보안 요구사항 및 평가 수준을 정할 수 있는 잘 정립된 방법들 제공 받을 수 있게 되었다. 또한 현재 보안 시스템 개발자들이 안고 있는 국가간 평가 기준서들의 불일치를 감소시키기 위하여 FC는 ITSEC, CTCPEC, TCSEC 등을 기반으로하여 만들어졌다. 현재 FC는 네트워킹 환경의 포함여부, 민간용 보안 요구사항의 확장, 시스템 통합에 대한 관심, 컴퓨터 바이러스 분야의 누락 등에 대한 비평을 받고 있다. 이러한 문제점들은 향후 광범위한 논의를 거쳐 개선될 것이다. 또한 국제적으로 추진하려고 하는 통합보안 평가 기준서의 토대가 될 것이다.

앞으로 국내 보안 평가서의 제작을 위하여 FC의 세부적인 구성요소들에 대해 면밀한 검토와 분석, 외국 평가 기준서들의 작성시 기초가 된 기본 사상, 통합 평가 기준서 작성을 위한 각국의 활동 등에 꾸준한 관심을 기울여야 할 것이다.

참고 문헌

[1] CSE, The Canadian Trusted Computer Product Evaluation Criteria, January 1993,

[2] Data Security Letter, No. 38, January/February 1993.

[3] ECMA/TC36-TC1, Secure Information Processing Versus the Concept of Product Evaluation, 1st Draft, Feb. 1993.

[4] Eugen Mate Bacic, The Canadian Criteria, Version 3.0& The u.S.Federal Citeria, Verson 1.0, Proceedings on Fifth Annual Canadian Computer Security Symposium. May 1993.

[5] Information Technology Security Evaluation Criteria, May 1990.

[6] Info Security News, Vol.4, MIS Press, July/August 1993.

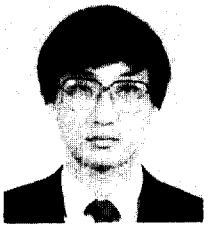
[7] NIST &NSA Federal Criteria, Version 1.0, December 1992.

[8] NIST, Minimum Security Functionality Requirements For Multi-User Operating System, January 1992.

[9] NCSC, The DoD of Trusted Compter Security Evaluation Criteria, 1985.

[10] NCSC, The 16th NCSC Conference Proceeding, September, 1993.

□ 著者紹介



윤 이 중

1988년 2월 인하대학교 전산학과 졸업(학사)
1990년 2월 인하대학교 전산학과 졸업(석사)
1990년 2월～현재 한국전자통신연구소 연구원
관심분야 : Computer Security, DBMS, Network Security

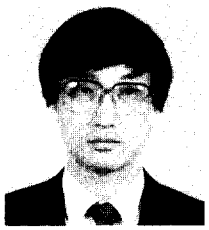
홍 주 영

1990년 2월 홍익대학교 전산학과 졸업(학사)
1990년 2월～현재 한국전자통신연구소 연구원
관심분야 : Computer Security, Network Security

이 대 기

1962년 2월 한양대학교 전자공학과 졸업(학사)
1987년 2월 한양대학교 전자공학과 졸업(석사)
1980년 4월～1992년 11월 한국전자통신연구소 산업기술개발부 부장,
지상시스템연구부 부장
1992년 12월～현재 한국전자통신연구소 부호기술부 부장

□ 著者紹介

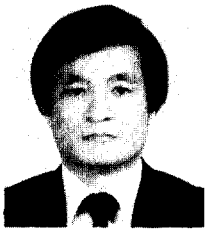


윤 이 중

1988년 2월 인하대학교 전산학과 졸업(학사)
1990년 2월 인하대학교 전산학과 졸업(석사)
1990년 2월～현재 한국전자통신연구소 연구원
관심분야 : Computer Security, DBMS, Network Security

홍 주 영

1990년 2월 홍익대학교 전산학과 졸업(학사)
1990년 2월～현재 한국전자통신연구소 연구원
관심분야 : Computer Security, Network Security



이 대 기

1962년 2월 한양대학교 전자공학과 졸업(학사)
1987년 2월 한양대학교 전자공학과 졸업(석사)
1980년 4월～1992년 11월 한국전자통신연구소 산업기술개발부 부장,
지상시스템연구부 부장
1992년 12월～현재 한국전자통신연구소 부호기술부 부장