通信情報保護學會誌
第 10 券 第 3 號, 2000. 9

CC보안기능 요구사항과 PP에서의 해석

김 석 우*

요 약

국제 공통평가기준(CC)은 정보보호제품의 개발·평가·사용을 위한 ISO 15048 국제 표준이다. 국제 공통평가기준의 제 2부 보안기능 요구사항은 정보보호제품의 보안 기능을 11개 클래스로 분류하였고, 13개국 인증제품 상호승인 협정(MRA)에 의하여 교차 사용이 가능한 평가된 보안제품을 해설할 수 있는 공통 언어로써 사용할 수 있다. 보호프로파일(PP)은 특정형태의 제품군이 지녀야 할 보안 목적을 사용자 그룹에서 요구한 명세서이다. 보호프로파일은 제품군의 운영환경, 위협요소를 분석하고 보안기능 요구사항의 부분 집합들을 모아서 제품군이 목표로 하는 보안 목적들을 주장할 수 있다.

Ⅰ. 서 론

인터넷 정보화사회에서 정보보호의 필요성은 대단히 중요하다. 1980년대 국가 보안을 중심으로 시작되었던 국내정보보호기술이 2000년 현재에는 일반적으로 사용되는 정보시스템의 중요기술로 자리하고 있다. 국가기관 외에 일반기업체에서도 보안의 필요성을 절감하고 있기에, 기관의 정보시스템 구축에 정보보호제품의 도입은 당연한 기본전략으로 채택되고 있다. 정보보호 분야의 활성화와 더불어 그 동안 연구·개발된 국내외 기술이 1997년도를 기점으로 제품화에 돌입하게 되었고, 이제 평가기준에 부합된 제품으로 구현되고, 평가되고, 사용되고 있다. 국내에서도 현재 5개 평가 인증된 침입차단 시스템을 비롯하여 하반기까지 침입탐지, 스마트 카드, 인증 시스템의 3개 분야의 평가기준이 한국 정보보호센터 주도로 개발공표되거나 예정이다[13]. 국외 정보보호 연구 개발 분야 역시 1999년 11월 국제공통평가 기준인 CC(Common Criteria)가 ISO/IEC 15048 국제 표준으로 공표되었다[1][2][3].

이러한 제품개발 표준을 기반으로 국내외 정보보호산업이 급속히 발전되고 있으며 2000년을 기준으로 전세계적으로 500억불 규모이며, 국내의 경우 약 10억불로 예상하고 있다. 정보보호제품 중 평가된 제품의 비율은 미국의 경우 약 18%로 추산하고 있다[11].

정보보호 제품의 개발·평가·사용을 염두에 두고 개발된 국내외 표준 및 관련 가이드라인은 실제로 제품을 구현하고 평가한 기술과 경험으로 바탕으로 추상적으로 작성된다. 국제 공통평가 기준의 내용을 살펴보면 제1부 일반모델, 제 2부 보안기능 요구사항[2]은 제품에서 필요로 하는 보안기능을 11개 클래스로 분류하고 있으며, 제 3부 보증기능요구사항[3]은 제품을 사용하는 환경 및 제품의 성능까지 포함한 평가자가 보증하기 위한 7가지 보증클래스와 보증유지 클래스를 분류하고 있다. 국제 평가 기준에서 명시하고 있는 내용은 제품의 기능과 운영보증에 관한 기본적인 원칙을 보안기술 전체적인 관점에서 기술하고 있다. 반면에, 보호프로파일(Protection Profile)과 보안목표명세서(Security Target)은 CC에 기반하여 개발되는 제품을 보다 구체적인 관점으로 해석하고 설명한 표준과 매뉴얼 중간수준의 명세서이다[4]. 보호프로파일은 CC 평가 기준 2등급의 운영체제, 응용계층 방화벽 등과 같은 특정 형태의 정보보호제품 군이 갖추어야 할 보안 목적들과 이를 달성하기위한 기능 및 환경에 대해 정의한다.

따라서, 보호프로파일은 정보보호제품을 동일한 목적에 사용코자 하는 사용자그룹에서 요구하는 것

* 한세대학교 정보통신공학

이 이상적이다. 반면에, 보안목표명세서는 보호프로파일에 기반하여 개발업체가 개발한 특정 제품에 대한 설명 및 업체의 주장을 담은 명세서이다. 본 논문은 국제공통평가 기준의 보안기능 요구사항과 보호프로파일에서의 해석에 관하여 사용자 및 개발자 관점에서 간략하게 기술한다. 제 2장에서는 보호프로파일을 2등급 OS 보호프로파일인 CS-2[5]를 중심으로 기술하고, 제 3장은 CC part2 보안기능요구사항을 기술한다. 제 4장에서는 보호프로파일에서 보안기능요구사항의 사용에 대하여 해석, 정리한다.

II. CC 보호 프로파일 (Protection Profile)

보호프로파일은 분류된 TOE (Target of Evaluation)들의 보안목적(security objectives)을 표현하기 위해 사용되는 기능(function)과 보증(assurance) 요구사항 들의 모음이다. 보호프로파일은 비슷한 보안기능을 필요로 하는 사용자들의 요구조건을 명시하게 되는데, 우선 보호프로파일이 필요한 사용자를 분류해 보면, 크게 일반소비자, 정부기관, 기업체의 3분류로 나눌 수 있으며, 각각의 환경에서 필요한 제품군의 요구사항을 기술한다[14].

보호프로파일은 CC 평가그룹이 평가하여 등록기관에 기록되어 공표된 후, 개발자에 의해 제품으로 개발하게 된다. 보호프로파일은 특정 사용자들이 필요로 하는 보안 요구사항 들이며, 이러한 요구사항을 반영하여 개발된 정보보호 제품의 보안기능을 기술한 것이 보안목표 명세서이다[1]. 보호프로파일은 사용자 입장에서 특정한 TOE가 지녀야 하는 보안요구 사항들을 나타내기 때문에 일반 사용자가 이해하기 힘든 기술 자료 참조를 최소화하도록 그 내용과 표현이 문서로 나타내야 한다. 아래 그림 2 .1에 보호프로파일의 구성을 보인다.

1. 보호프로파일 구조

보호프로파일의 처음 시작은 보호프로파일의 식별자, 개요로써 TOE에 대한 제품유형, 제품이 지녀야 할 특성을 기술한다

1.1 보호프로파일 소개(PP Introduction)

보호프로파일을 등록할 수 있는 식별자 및 요약 기술하고 있다. 식별자에는 PP의 제목, 보증레벨, 등록번호를 기술하며, 개요에는 TOE의 목적, 범위, 사용법외 간략한 요약설명을 담고 있다.

1.2 TOE 설명서

평가를 위한 운영환경을 제시한다. TOE가 stand alone과 네트워크 환경에서 보안 기능이나, TOE가 지녀야 하는 보안기능(접근제어, 신분확인, 감시추적 등)등을 기술한다. PP는 ST와 달리 특정 제품에 대한 설명이 아니므로, 가정 사항이므로 TOE를 적용할 수 있는 폭 넓은 응용환경을 서술하는데 사용된다.

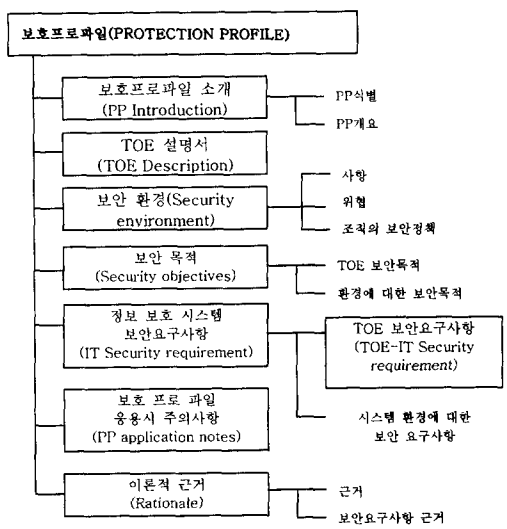


그림 2.1 보호프로파일

1.3 보안환경(Security Environment)

TOE를 사용하려는 환경상의 보안관점과 TOE를 사용하는 방법상의 보안관점을 설명한다. 표 2.1 에 TOE 보안 제품이 추구하고 있는 보안기능을 중심으로 이를 사용하려는 사용자나 조직의 보안정책이 지녀야 할 조건을 가정하고 발생 가능한 위협을 설명한다.

1.4 기관 보안 정책(Organizational Security Policies)

표 2.2 에 평가 2등급 일반 운영체제를 사용하려는 기관이 필요한 세분화된 보안정책을 보인다.

1.5 보안 위협 요소(Threats to Security)

제품의 보안기능은 위협요소에 대한 기술적 방어 대책이다. CC평가 2등급을 목표로 하는 일반 운영체제 CS-2의 대응 위협요소는 다음의 2가지 그룹으로 구분한다.

- 비인가 된 사용자의 정교하진 않지만 악의적인 공격
- 인가된 사용자가 악의적인 의도는 아니지만 미승인된 액세스(호기심의 단계를 벗어난 공격)

표 2.3에서 보인 TOE 자체 위협요소 외에 운영환경 상에서의 위협 중 일부를 표 2.4 에 보인다.

1.6 보안목적 (Security Objectives)

- TOE는 여러 가지 세분화된 보안목적을 가진다. PP는 특정 형태의 보안 제품이 필요로 하는 사용자 측면의 요구 사항을 일반적으로 기술한다. 표 2.5 에 전술한 보안 위협에 대응하기 위한 기능과 기관의 보안 정책을 준수하도록 하는 기능이 모두 TOE의 보안 목적이 된다. 표 2.6 에 CS-2의 환경 보안 목적 중 일부를 보인다. TOE가 운용되는 환경에서 IT 보안목적을 달성하기 위한 것으로써 TOE와 연동된 보안 목적이다.

표 2.1 가정사항(Assumption)

형 태	명 칭	가 정	비 고
물리적	A.PHYSICAL	TOE는 인가되지 않은 물리적 액세스로부터 보호될 수 있도록 HW기반의 물리적 보호환경 내에 위치한다.	물리적으로 최소한의 보호 벽이 설치되지 않은 곳에서는 제품의 보안기능을 보장할 수 없다.
인원적	A.USER-NEED	인증된 사용자는 안전한 IT환경의 필요성을 공감한다.	안전한 IT환경을 공감하지 못하는 사용자는 보안기능을 우회하려고 노력할 수도 있다.
	A.USER-TRUST	인증된 사용자는 보안정책에 부합되는 임의적 행동을 취한다.	훈련과 동기부여를 통해 이해할 수 있는 IT활용을 기대한다.
	A.ADMIN	TOE의 보안기능이 사건별로 관리된다.	기술적이고 통제되는 보안관리 기능이 수행되어야 한다.

표 2.2 CS-2 운영체제를 사용하는 기관의 보안정책 예

명 칭	정 책	설 명
P.ACCESS	정보에 대한 액세스는 기관의 보안 정책에 따라 주체와 객체(정보)에 부여된 보안속성(객체보안등급, 주체보안 속성, 환경조건)에 기반하여 결정된다.	주체보안속성(사용자 신분, 그룹 등)과, 객체 보안속성(permission bit), 액세스형태(rwex), 환경조건(Time-of-day)에 따라 액세스 규칙이 적용된다. 액세스의 결과는 승인 또는 거부로 나타난다.
P.ACCOUNT	보안 관련 사건을 유발시킨 사용자는 확인(accountable)될 수 있어야 한다.	CS2는 부적절한 행위를 유발시킨 사용자를 사건 베이스로 추적하기를 원하는 기관의 보안 정책을 수행할 수 있도록 기능을 제공해야 한다.
P.KNOW	정해진 일련의 작업 (Web processing등) 외에 TOE액세스는 사전에 규명되고 인증(authenticated) 되야 한다.	웹 서버의 읽기 액세스는 조건 없이 허용되며 공개된 보안정책에 부합되지 않는 TOE액세스는 배제된다.

표 2.3 CS-2 TOE 자체위협

명 칭	위 협
T.ACCESS	사용자라도 사용시스템에러를 이용하여 인가되지 않은 비 악의적인 액세스 권한을 얻을 수 있다. 또한 기술적인 공격을 통하여서도 위와 같은 액세스를 얻을 수 있다.
T.CRASH	TOE의 안전한 상태(secure state)가 시스템 크래쉬 때문에 붕괴될 수 있다.
T.OBSERVE	TOE결함이 아닌 IT보안 취약성 때문에 유능한 사용자나 보안 관리자라도 실제로는 안전치 못한 상태를 안전하다고 믿을 수 있다. 이러한 상황은 TOE의 설계규격, 구 현상의 결점 때문에 발생할 수 있다.
T.RECORD-EVENT	보안관련 이벤트가 기록되지 않을 수가 있다.
T.DENIAL	TOE는 가공되지 않은 (unsophisticated)서비스거부(Denial-Of-Service)공격을 허용할 수 있다.

표 2.4 CS-2 TOE의 운영환경상의 위협

명 칭	위 협
T.INSTALL	TOE는 보호되지 않은 상황에서 배포되고 설치될 수 있다.
T.OPERATE	TOE의 부적합한 동작(인가된 특권의 남용 등)으로 인해 보안 실패가 유발될 수 있다.
T.ENTRY_SOPHISTICATED	인증된 사용자가 아닌 자가 정교한 기술적 공격을 사용하여 자원과 정보를 처리할 수 있는 액세스 권한을 얻을 수 있다.
T.DENIAL-SOPHISTICATED	정교한 기술적 서비스 거부(Denial-Of-Service) 공격을 허용할 수 있다.
T.ACCESS_MALICIOUS	인증된 사용자가 악의적 목적으로 승인되지 않은 액세스를 얻을 수 있다.
T.ENTRY-NON-TECHNICAL	인증되지 않은 사용자가 기술적 방법 외의 수단으로 정보자산을 처리할 수 있는 권한을 얻을 수 있다.
T.ACCESS-NON-TECHNICAL	인증되지 않은 자가 기술적 방법 외의 수단으로 악의적 이진 않지만 미 승인된 액세스 권한을 가질 수 있다.

표 2.5 CS-2 TOE 보안 목적

IT 보안 목적		대 응 위 협	대응 보안정책
명 칭	설 명		
O.ACCESS	TOE는 공개된 Web 액세스와 승인된 TOE 정보자산 액세스를 허용한다.		P.ACCESS
O.INFO-FLOW	TOE 컴포넌트 사이, TOE 외부 인터페이스에서 정보흐름을 통제해야만 한다.		P.INFO-FLOW
O.KNOWN	잘 정의된 인가된 액세스 행동 외에 모든 사용자를 인증하여야 하며, 모든 액세스를 사용 전에 제어해야 한다.		P.KNOWN
O.AUTHORIZE	TOE는 기관의 액세스 정책에 부합되도록 사용자 및 시스템 프로세스 액세스 권한을 제어해야만 한다.		P.ACCESS
O.ACCOUNT	TOE는 모든 사용자의 보안관련 사건을 추적(accountable)할 수 있어야 한다.	T.TRACEABLE T.RECORD-EVENT T.AUDIT-CORRUPTED	P.ACCESS
O.BYPASS	TOE는 인가된 사용자나 시스템 SW가 실수 또는 비악의적인 bypass나 우회를 방지하여야 한다.	T.ACCESS	

표 2.6 CS-2의 환경 보안 목적

환경 보안 목적		상 대 위 협	상대보안정책
명 칭	설 명		
O.OPPERATE	TOE책임자는 IT(정보기술)보안 정책을 유지하는 TOE 배포, 설치, 운영을 확인하여 한다.	T.INSTALL T.OPERATE	P.TRAINING
O.ACCESS-MALICIOUS	TOE환경은 인증된 사용자의 악의적인 위협을 저지할 수 있어야 한다.	T.ACCESS-MALICIOUS	
O.ENTRY-SOPHISTICATED	TOE환경은 고도의 기술적 공격을 통하여 얻은 비인가된 액세스 위협을 저지할 수 있어야 한다.	T.ENTRY-SOPHISTICATED	
O.DETECT-SOPHISTICATED	TOE환경은 고도의 기술적 공격 및 공격의 결과(예: 붕괴된 시스템 상태)를 감지할 수 있는 능력을 제공하여야 한다.	T.SYSTEM-CORRUPTED	P.SURVIVE

III. 보안기능 요구사항

국제 공통 평가 기준의 제 2부는 보안기능 요구사항을, 제3부는 보증요구사항을 기술하고 있다. 보안기능 요구사항은 TOE의 기능 요구사항을 표준화된 방법으로 표현한 것으로써 기능 컴포넌트들의 집합을 모아 놓았다. 보안기능 요구사항은 보안 감사 기능 외 11개 기능들로 대 분류되어 있으며, 이를 클래스(class)라고 부른다. 클래스는 다시 패밀리, 컴포넌트로 세분화된다.

1. 클래스(Class)

표 3.1 에 기능 클래스를 요약 정리한다. 각 기능 클래스에는 클래스 명, 소개와 소 분류된 기능 패밀리가 하나 이상 존재한다.

클래스는 기능클래스를 식별 및 분류할 수 있도록 고유의 이름을 가지며 분류정보에 해당하는 3글자짜리 이름으로 구성된다.

패밀리의 약식 명칭을 명시할 때 클래스의 약식 명칭을 함께 사용한다.

클래스명	클래스 제목	설 명
FAU	보안감사(Security Audit)	보안활동과 관련된 정보로 감지, 기록, 저장, 분리
FCO	통신(Communication)	데이터를 교환하는 주체의 신원을 감지
FCS	암호지원(Cryptographic Support)	암호 운용 및 키 관리
FDP	사용자 데이터 보호(User Data Protection)	사용자 데이터의 보호
FIA	식별 및 인증(Identification & Authentication)	사용자의 신원 확인 및 인증
FMT	보안관리(Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR	프라이버시(Privacy)	허가되지 않은 사용자에 의한 개인의 신원 및 정보의 도용방지
FPT	TOE 보안기능의 보호(Protection of Trusted Security Function)	TSF 데이터의 보호 및 관리
FRU	자원활용(Restore Utilization)	TOE의 가용자원을 확보
FTA	TOE 접근(TOE Access)	TOE에 대한 사용자 세션의 보호
FTR	안전한 경로/채널(Trusted Path/ Channel)	사용자와 TSF간 혹은TSF간의 안전한 통신채널 확보

2. 패밀리 (Family)

패밀리는 고유의 이름을 가지며 총 7자리로 구성된다. 이중 처음 3글자는 클래스 명이며 나머지 3글자가 패밀리 명이며 가운데 한자는 언더 바로 두개의 3글자를 연결한다. 예를 들면 보안감사 클래스(FAU)의 보안감사 자동응답 패밀리(ARP)는 FAU_ARP로 표현된다. 이 패밀리 이름은 컴포넌트를 참조할 때의 이름으로 사용된다. 패밀리의 행동은 기능 패밀리에 대한 서술적 설명이며 보안 목적과 기능 요구사항이 상세하게 기술된다. 컴포넌트 패밀리의 "보안 목적"은 패밀리내의 컴포넌트들이 해결할 수 있는 보안 문제를 간결하고 명확하게 설명한 것이다.

"기능 요구사항" 설명에서는 컴포넌트에 포함된 요구사항을 요약해 보여준다. 이것은 패밀리가 요구사항과 관련되는지를 평가하려는 보호 프로파일, 보안목표개요 및 기능 패키지의 작성자들을 위한 것이다.

3. 컴포넌트 (Component)

기능 패밀리들은 1개 이상의 컴포넌트를 가지며 이들은 보호 프로파일, 보안목표개요 및 기능 패키지 내에 포함(선택)될 수 있다. 컴포넌트들을 등급화 하는 목적은, 일단 어떤 패밀리가 필요하거나 유용한 보안 요구사항으로 식별된 경우, 사용자에게 적절한 기능 컴포넌트를 선택할 수 있는 정보를 제공하는 것이다. 기능 패밀리 서술 부분에서는 사용가능한 컴포넌트, 그들의 해석 및 컴포넌트들간의 관계를 기술한다. 기능 패밀리 내의 컴포넌트들간의 관계는 계층적이거나 아닐 수도 있다. 이러한 관계를 보이는 것이 컴포넌트 등급화의 부분이다.

3.1 개 요

컴포넌트 개요는 컴포넌트 이름과 컴포넌트들의 계층도를 포함한다. "FAU_GEN.1 감사데이타 생성"의 좌측 9자는 패밀리 이름 7자 + "." + 번호 1 로 구성되는 약식이름(Short name)이며 우측의 7자는 컴포넌트 목적을 나타내는 고유이름(Unique name)이다.

3.2 기능 엘리먼트

컴포넌트는 또다시 엘리먼트들로 구성된다. 기능 엘리먼트는 보안기능 요구사항에서 존재하는 가장 적은 단위 기능을 표현한다. 따라서, 보호 프로파일 / 보안 목표개요를 작성할 때 한 컴포넌트로부터 1개 이상의 엘리먼트만을 선택할 수는 없다. 한 컴포넌트의 엘리먼트 집합이 보호 프로파일/보안목표 개요 내에 포함될 수 있다. 기능 엘리먼트 이름은 유일하고 짧아야 한다. 예컨대, 기능 컴포넌트명인 "FDP_IFF.4.2"에서 "F"는 기능 요구사항, "DP"는 "사용자 자료보호" 클래스, "_IFM"은 "정보 흐름 제어 기능" 패밀리, ".4"는 4번째 컴포넌트 명 즉, "특정 정보흐름 제한"을 나타내며 ".2"는 컴포넌트의 2번째 엘리먼트를 각각 나타낸다.

3.3 종속성

각 기능 컴포넌트마다 다른 기능 및 보증 컴포넌트와의 종속성 목록이 포함된다. "종속성이 없음"도 유효한 목록이다. 기능 컴포넌트들간의 종속성은 컴포넌트가 자기 충족적이 아니며 타 컴포넌트의 기능에 의존하여야 하는 경우에 발생한다. 종속성 목록은 컴포넌트와 관련된 보안 요구사항을 만족시키기에 필요한 최소한의 기능 및 보증 컴포넌트를 식별하여야 한다. 또한 식별된 컴포넌트에 계층적인 컴포넌트들은 부가적인 잠재적 취약성의 위험과의 종속성을 만족하기 위해 사용된다.

3.4 컴포넌트 연산자

엘리먼트의 설명시 정의되지 않은 또는 보다 상세한 목록의 실증을 보이기 위하여 값을 부여하거나 (할당) 목록으로부터 1개 이상의 엘리먼트들을 선택하거나 내용을 상세히 기술할 수 있는 정제의 3가지 연산자를 사용한다. 5 절의 FCO_NRO에 할당, 선택의 예와 설명을 보인다.

4. 클래스별 보안기능 요구사항

4.1 클래스 FAU : 보안감사(Security Audit)

보안감사는 보안 관련 활동(즉, TSP에 의해 통제되는 모든 활동)에 관련된 정보의 인식, 기록, 저장 및 분석을 포함한다. 감사 기록 결과는 어떤 보안 관련 활동이 발생했으며, 누가 이에 대한 책임이 있는가를 결정할 때 활용될 수 있다.

4.2 클래스 FCO : 통신(Communication)

통신 클래스는 자료 교환 시에 참여하는 파트의 식별을 보증하는 것에 관련된 2개의 패밀리를 제공한다. 이들 패밀리는 전송된 정보의 생성자와 수신자의 신분을 보증하고 증명하는 것이다.

또한, 생성자는 (Originator) 메시지의 송신(Send)을 부인할 수 없으며, 수신자(Recipient)도 수신(receive)을 거부할 수 없음을 보증한다.

4.3 클래스 FDP :사용자 자료보호(User Data Protection)

사용자 자료보호 클래스는 사용자 자료의 보호와 관련된 TOE 보안기능 및 보안기능 정책을 위한 요구사항을 기술하는 패밀리들을 포함한다.

FDP는 입력(import), 출력(export) 및 저장 동안의 TOE내의 사용자 자료의 기술과 사용자 자료와 직결되는 보안 속성의 기술을 포함하여 자료보호의 형태(Forms of Data Protection), 자료보호 보안기능정책(Data Protection Security Function Policies), 보안 속성 관리(Security Attribute Management), 오프라인 저장 및 통신(Off-line Storage and Communication), TSF간 통신(Inter-TSF Communication)의 5개 패밀리 그룹으로 분리된다.

4.4 클래스 FIA : 식별 및 인증(Identification and Authentication)

본 클래스내의 패밀리들은 요구된 사용자 신분의 개설 및 검증 기능에 대한 요구사항을 기술한다. 식별과 인증은 사용자들이 진정한 보안속성(예:신분(identity), 역할, 보안 또는 무결성 수준)과 연관된다는 것을 확신(ensure)하기 위해 요구된다. 인가된 사용자를 애매하지 않게 식별하는 것과 사용자와 주체간의 보안 속성의 연관을 올바르게 하는 것은 의도된 보안정책의 강화에 있어서 핵심적이다.

본 클래스내의 패밀리들은 사용자의 신분 검증 및 결정, TOE에 대화하기 위한 권한의 결정 및 각 인가된 사용자에 대한 보안 속성의 올바른 연관과 관련된다. "사용자 자료보호", "보안감사" 등과 같은 다른 클래스의 요구사항이 효과적이기 위해서는, 사용자의 올바른 식별 및 인증에 달려있다.

4.5 클래스 FPR : 프라이버시(Privacy)

본 클래스는 프라이버시 요구사항을 포함한다. 이들 요구사항은 사용자에게 다른 사용자가 자신의 신분을 발견 및 잘못 사용하는 것에 대한 보호를 제공한다. 본 클래스는 프라이버시 기술에 관한 현재의 가용 지식을 바탕으로 한다.

4.6 클래스 FPT : 안전한 보안기능의 보호 (Protection of the Trusted Security Function)

본 클래스는 TSF를 제공하는 매커니즘의 관리와 무결성에 관련되고 TSF자료의 특정 내용과 독립적인 TSF 자료의 관리와 무결성에 관련된 기능 요구사항의 패밀리를 포함한다. 본 클래스내의 패밀리들은 FDP(사용자자료보호)내의 컴포넌트와 중복된다. 이들은 동일한 매커니즘을 사용해 구현된다. 그러나, FDP는 사용자 자료의 보호에 중점을 두지만, FPT는 TSF자료의 보호에 중점을 둔다.

4.7 클래스 FRU : 자원 활용(Resource Utilization)

본 클래스는 처리 능력 및 저장 용량과 같은 요구된 자원의 가용성을 지원하는 3개의 패밀리를 제공한다. "고장 허용(Fault Tolerance)" 패밀리는 TOE의 고장에 의해 야기된 기능의 불가용성에 대한 보호를 제공한다. "서비스 우선순위(Priority of Service)"는 자원은 중요하고 시간-임계적인 태스크에만 할당되어야 하며, 이보다 낮은 우선순위의 태스크에는 할당하지 않음을 보증하여야 한다. 자원 할당(Resource Allocation)은 가용 자원의 사용상의 한계를 제공한다. 따라서, 사용자가 자원을 독점하지 못하게 한다.

4.8 클래스 FTA : 평가대상물 접근(TOE Access)

본 클래스는 사용자 세션의 개설을 제어하기 위한 식별 및 인증 요구사항의 상위인 기능 요구사항을 기술한다.

4.9 클래스 FTP : 안전한 경로/채널(Trusted Path/Channel)

본 클래스는 사용자들과 TSF간의 안전한 통신

경로와 TSF들 사이의 안전한 통신 경로에 대한 요구사항의 제고하며 다음과 같은 일반 특징을 갖는다.

통신 경로는 TSF자료의 식별된 부분집합을 분리하는, 컴포넌트에 대해 적절한 내외부 통신 채널과 TSF와 사용자 자료의 나머지로부터의 명령을 이용해 구성된다. 통신 경로의 사용은 사용자 및 컴포넌트에 대해 적절한 TSF에 의해 시작될 수 있다.

또한 통신 경로는 사용자가 올바른 TSF와 통신함을 보증하고, TSF가 올바른 사용자와 통신함을 보증할 수 있는 능력을 가진다.

5. FCO_NRO.1 선택적 송신증명 컴포넌트 예

본 절에서는 보안기능 요구사항의 한 사례로서 "FCO_NRO.1 선택적 송신증명"에 대한 설명 예시를 보인다. 사각형 박스로 둘러싸인 부분은 컴포넌트를 나타내며 박스 아래쪽에 설명과 예시를 보였다.

FCO_FAM1

송신 부인방지(FCO_NRO, No-requdiation of origin)패밀리는 정보의 송신자가 정보의 송신사실을 부인하지 못하게 함을 보장한다. TSF는 데이터 교환 시 전송된 정보를 수신한 주체에게 정보의 송신에 대한 증거가 제공됨을 보장하는 방법을 제공해야 한다. 이 증거는 이 주체나 혹은 다른 주체에 의하여 증명될 수 있어야 한다.

〈해설〉 사용자나 주체에게 정보생성자가 누구인가를 증명하는 증거(예: 디지털 서명)를 제공한다. 수신자나 제 삼자는 이 증거를 검증함으로써 생성자가 누구인가를 알 수 있다.

〈기술〉 사용하는 증거로는

1) 무결성 체크의 MAC 알고리즘에 의해 생성된 값
2) 공개키 기반의 전자서명
3) 토큰형태
4) 기타

사용방법으로는

1) 수신자가 요구한 유효성 검사
2) 제 3자가 개입하는 저장 후 유효성 체크 방식
3) 제 3자가 인 라인 저장 후 분쟁 시 검증 방식 등이 있다.

〈적용〉 PP의 functional requirement 및 제품

FCO_FAM2

FCO_NO.1 선택적 송신증명(Selective proof of origin)은 TSF가 주체에게 정보의 송신에 대한 증거를 요청할 수 있는 능력을 제공할 것을 요구한다.

선택적 송신방법은 *송신측 그룹(예: 전자 수표의 전송환경에서 송신측 은행)/기관의 보안관리자(domain security manager)/제 삼자*가 시스템 내 임의의 주체가 정보를 송신시 송신했다는 증거생성을 요구할 때, TSF 가 이를 생성 할 수 있도록 시스템이 보안기능을 가질 것을 의미한다.

FCO_FAM3

FCO_NRO.2 강화된 송신증명(Enforced proof of origin)은 TSF가 항상 전송된 정보의 송신에 대한 증거를 생성할 것을 요구한다.

선택적 송신증명이 송신시 증거생성을 요청하는 주체를 선택적으로 지정하는 것에 비해, 지정자가 존재하지 않는다. 이는 어떤 정보이던지 송신시에는 증거가 생성됨을 의미하는 강화된 보안 정책의 실행을 뜻한다.

FCO_FAM4

관리 : FCO_NRO.1, FCO_NRO.2

FCO_FAM5

FMT의 관리 기능에 다음과 같은 행동이 고려되야 한다. 1) 정보 유형, 필드, 송신자 속성 및 증거의 수신에 대한 변경 관리

관리기능에서는 송신증거가 생성되는 대상 정보유형(예: 전자우편, 화일.doc), 송신자 속성(예:송신자 id/호스트명), 수신환경(수신자명)에 대한 변경이 관리되어야 한다.

FCO_FAM6

감사 : FCO_NRO.1 만일 FAU_GEN(보안감사데이터 생성) 패밀리가 보호 프로파일/보안목표명세서에 포함되면 다음 행동을 감사할 수 있어야 한다. 1) 최소 : 송신자 증거 생성을 요구한 사용자의 신분 2) 최소 : 부인방지 서비스의 호출 3) 기본 : 정보, 목적지, 그리고 제공된 증거의 사본에 대한 식별 상세 : 증거의 검증을 요구한 사용자의 신분

선택적 송신증명 패밀리에서 부인 방지 서비스는 누군가에 의해서 요구되어 진다. 감사기록의 생성시 포함되어야 하는 데이터 내용은

1) 최소 : 송신증거 생성을 요구한 누군가와 부인방지 서비스가 호출된 사실은 적어도 포함한다.
2) 기본 : 송신증거가 생성된 대상정보, 수신자, 증거의 ID
3) 상세 : 송신증거는 정보의 송신측 또는 제삼자에 의해 검증될 수 있다. 시스템내의 주체이던지 외부의 요청이던지 증거의 검증을 요구한 사용자의 신분이 기록되어진다.

FCO_FAM7

감사 : FCO_NRO.2 만일 FAU_GEN(보안감사데이터생성) 패밀리가 보호프로파일/보안목표명세서에 포함되면 다음 행동을 감사할 수 있어야 한다. 1) 최소 : 부인방지 서비스의 호출 2) 기본 : 정보, 목적지, 제공된 증거의 사의 식별 상세 : 증거의 검증을 요구한 사용자의 신분

Ⅳ. 보호프로파일에서 보안기능요구사항

제 2장과 3장에서 보호프로파일(PP)와 보안기능요구사항(CC part2)을 각각 설명하였다. 여기서는 보안기능요구사항이 PP의 어느 보안목적을 만족시키는 가를 CS2 보호프로파일의 감사추적 클래스에서 설명하고, 일반적으로 사용하는 보안기능에서 필요로 하는 CC part2의 보안기능요구사항을 신분확인과 인증기능(I &A)에서 예시 설명한다.

1. PP에서 보안기능 요구

감사추적은 감사데이터를 감지하고, 생성하고, 감사데이터를 기록저장한 후, 기록된 감사데이터를 가공하여 관리자에게 보이며, 관리자는 이를 검토하고, 분석하게 된다. 이러한 각각의 패밀리는 FAU_ARP, FAU_GEN, FAU_STG, FAU_SEL, FAU_SAR, FAU_SAA에 대응된다.

감사추적의 컴포넌트는 제품의 보안 목적들을 만족시키는 제품의 보안기능으로 역할 한다. 표 5.1에 CS-2의 예시와 설명을 보인다.

1.2 신분확인과 인증에서 보안기능요구사항

정보보호 기능을 구현하기 위해 필요한 CC part2 패밀리들의 사용을 ISO 가이드[4]로부터 기본적인 정보보호기능을 분류해 보면다음의 7가지로 구성된다[4].

1) 신분확인과 인증(Identification and Authentication)
2) 액세스 제어 (Access Control)
3) 감사 (Audit)
4) 무결성 (Integrity)
5) 가용성 (Availability)
6) 프라이버시 (Privacy)
7) 데이터 교환 (Data Exchange)

여기서는 신분확인과 인증 중 로그온 제어 내용을

표 5.1 CS-2 기능요소

컴포넌트 명	보안 목적	설 명
FAU_GEN.1 감사데이터 생성	O.ACCOUNT	보안위반 감사데이터를 발생시킨 사용자 추적
	O.RECOVER	안전하지 않은 시스템 상태를 감지하여 감사 데이터를 발생하고 시스템을 안전한 상태로 복구
	O.DETECT	안전하지 않음을 감지하였을 때는 감사 데이터를 생성.
	O.OPERATE/ O.MANAGE	TOE 관리자는 TOE를 안전하게 운영하여 하므로 감사 데이터가 생성되어 활용되어야 한다.
	O.DUE-CARE	TOE 관리자는 조심스럽게 운영하여 위험정도를 낮추어야 하므로 감사 데이터를 활용한다.
FAU_GEN.2 사전 생성자 신분확인	O.ACCOUNT	보안 위반 감사 데이터를 발생시킨 사용자 추적
FAU_SAR.1 보안감사 검토	FAU_SAR.2 FAU_SAR.3	SAR.1은 감사 레코드로부터 데이터를 읽는 사항과 감사자 레코드의 이해가능여부를 명시한다. SAR.2와 3은 SAR.1의 내용을 더 잘게 세분화하여 세분화된 내용을 선택한다. 따라서, SAR.2와 3은 SAR.1모집합의 부분집합 이므로 종속된다.

소개한다.

사용자가 로그 인하고, TOE가 이를 인증하여, TOE정보를 액세스 할 수 있도록 하는 절차 중 사용자 신분, 사용자 인증, 로그인 실패제한, 안전한 경로(Trusted Path), 로그인 가능시간의 5가지 보안 이벤트가 아래 표와 같이 발생된다.

표 5.2 신분확인과 인증/로그온과 CC part2 컴포넌트

보안 요구조건	CC part2	설 명
사용자 신분	FIA_UID.1-2	사용자를 인증하기 전에 사용자를 식별 할 수 있어야 한다. 사용자의 식별 시기가 매우 중요한데, 식별 전에는 시스템의 어떤 help 동작 허용 여부를 명시
사용자 인증	FIA_UAU.1-2	사용자를 인증하기 전에 login help 등의 중재 역할의 허용여부, 허용된다면 지정된 목록에 의해서만 수행된다.
로그인 실패회수 제한	FIA_AFL.1	지정된 인증 횟수 감지, 감사 후 지정된 행동목록 수행(터미널 폐쇄, 관리자 경보 등) 안전한 채널
안전한 채널	FTP_TRP	E-E 원격 프로세서간 안전한 채널, 안전한 통신상대방 지정, 초기 사용자 인증 시 안전한 채널 연결
TOE 액세스 시간제한	FTA_TSE.1	연결시도 위치(remote terminal), 액세스 시간(일과 외 시각), 액세스 방법 등의 액세스 제한 중 시간 제한

V. 결 론

국제 공통평가 기준은 국제 표준규격으로 정보보호 제품개발의 가장 기본적인 가이드라인으로 사용되고 있다. 국가간 상호인정프로그램 MRA(Mutual Recognition Agreement)이 1988 년 10월 미·영·불·독·캐 5개국 사이에 최초로 맺어진 이후 2000년 현재 13개국으로 확장되어 제품의 상호인정 사용이 가능하게 되었다. 이제 정보보호 제품은 명실공히 산업의 한 부분으로 중요한 위치를 점하고 있으며, 모든 제품의 개발평가사용은 국제공통평가 기준과 PP및 ST에 기반하여야 가능하다.

이와 관련한 국내 기술개발은 제품의 평가기관은 매우 활발하게 주도하고 있으나, 개발자 및 사용자의 관점은 제품 그 자체의 개발 및 사용에 그치고 있다. 만일, 국내 제품의 국외 수출 시 13개국이 상호 인정한 국제 표준 규격에 의거 개발평가되지 않았다면 불리한 경우에 봉착 할 수도 있다.

본 논문은 평가기준의 중요성에 비추어, CC 제2부 보안기능요구사항을 중심으로 보호프로파일에서 해석을 기술하였다. 보안제품의 개발, 평가기술 들은 매우 광범위하고 폭 넓은 관계로 어느 한 분야의 기술로 모든 문제를 해결하기 힘든 종합 분야이다.

보안기능 요구사항을 다른 분야로 해석하기 위한 연구·개발이 향후 필요한 연구 과제라 생각된다.

특히, 보안기능을 보증기술/보안목표 명세서/평가기술에서의 해석 등을 시급히 연구한 후, 세계적 경쟁력을 지닌 국내 보안제품 개발에 기반을 다져야 하겠다고 판단된다.

참 고 문 헌

[1] Common Criteria Editorial Board, Common Criteria For Information Technology Security Evaluation, part 1 : Introduction and General Model, Version 2.1, Aug., 1999

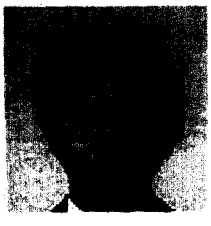
[2] Common Criteria Editorial Board, Common Criteria For Information Technology Security Evaluation, part 2 : Security Functional Requirements, Version 2.1, Aug., 1999

[3] Common Criteria Editorial Board, Common Criteria For Information Technology Security Evaluation, part 3 : Security Assurance Requirements, Version 2.1, Aug., 1999

[4] Murray G., *Guide for Protection Profile of PPs and STs*, v0.6, ISO/IEC JTC 1/SC27/WG3 N452, Jul., 1998

[5] Garry Stoneburner, *CS2-Protection Profile Guidance for Near-Term COTS*, NIST, Jul. 13,1998
[6] 한국정보보호센터, *국내·외 정보보호시스템 평가가이드*, 1998.11
[7] 한국정보보호센터 정보통신부, *정보보호 평가기준 개발*,1998.12.
[8] 김석우, *정보보호시스템 CC 활용방안*, 1998. 12
[9] 김석우, *정보보호체계 구성 방식 연구*, 한국전자통신 연구소, 1991.2
[10] 김석우, 정보보호시스템 평가기준 현황, 정보보호심포지움 SIS '99, 한국교육회관, 1999. 4, pp. 519-569
[11] 길인수, 정보보호시스템 평가 인증 정책, 정보보호심포지움 SIS '99, 한국교육회관, 1999. 4, pp. 115-161
[12] 이경구, 정보보호시스템 평가기준 개발 추진 현황, 정보보호심포지움 SIS '99, 한국교육회관, 1999.4, pp. 415-474
[13] http://www.kisa.or.kr 국내 정보보호 제품 평가 기준
[14] http://www.commoncriteria.org/protection_profiles/pp.html CC,PP,ST 등

〈著者紹介〉



김 석 우(Seok-woo Kim)
'79년 2월 : 한국항공대학 통신정보공학과(학사)
'89년 10월 : 뉴저지 공대 전자계산학과(석사)
'95년 2월 : 아주대학교 컴퓨터공학과 정보통신전공(박사)
'79년 1월~'80년 5월 : 삼성전자 특수사업부(현 삼성 HP)
'80년 8월~'97년 3월 : 한국전자통신연구소 책임연구원,부호5실장
'87년 1월~'89년 1월 : AT&T Bell Lab. 방문연구원
'97년 3월~현재 : 한세대학교 대학원 정보보호공학과, 한국통신정보보호학회 이사 논문 편집위원, TTA SC10 부의장
〈관심분야〉 정보보호제품 개발.평가, 사이버테러