情 報 保 護 學 會 誌
第 13 券 第 2 號, 2003. 4

# 키 복구 에이전트 시스템 보호프로파일에 관한 고찰

이 용 호*, 이 임 영**, 김 춘 수***, 채 수 영***, 나 학 연***

요 약

국제공통평가기준(Common Criteria)은 현재 고려되고 있는 모든 정보보호시스템 유형을 포괄할 수 있는 보안 요구사항의 집합체라 할 수 있다. 특정 형태의 정보보호시스템을 대상으로 하는 평가기준이 되기 위해서는 사용환경이나 보안목적에 적합한 보안 요구사항이 도출되어야 한다. 정보보호시스템을 사용하고자 하는 보안환경 및 보안목적을 정의하고, 이에 적합한 보안 요구사항을 국제공통평가기준에서 채택하여 제품별 평가기준으로 작성한 것이 보호프로파일(Protection Profile)이다. 보호프로파일은 미국의 국가안보국(NSA)과 국립표준기술원(NIST)에서 중점적으로 개발하고 있으며, 현재 다양한 제품에 대한 보호프로파일이 개발되고 있다.

본 고에서는 미국의 국가안보국에서 개발한 키 복구 에이전트 시스템 보호프로파일에 대하여 해당 TOE의 보안 환경과 보안 요구사항에 대하여 깊이있게 고찰하고자 한다.

## Ⅰ. 서 론

정보화 사회가 발전하면서 다양한 보안 제품들이 개발되고 있다. 선진국들은 이러한 보안 제품들에 대해 자국의 환경에 맞는 정보보호시스템 평가기준을 제정하고 이를 평가에 적용하고 있다. 정보보호시스템 평가 및 인증 제도의 목적은 정보보호시스템에 대한 안전성과 신뢰성을 보증하기 위해 신뢰된 제 3자로부터 객관적이고 공정한 평가를 통하여 검증된 정보보호시스템 사용을 권장하고, 정보의 유출과 해킹 그리고 바이러스와 같은 문제점들을 해결하고자 하는 것이다.

현재 사용되고 있는 평가기준으로는 미국의 TCSEC (Trusted Computer System Evaluation Criteria)과 캐나다의 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria) 그리고 유럽 국가에서 사용하는 ITSEC(Information Technology Security Evaluation Criteria) 등이 있으며, 국제적으로는 국제공통평가기준인 CC(Common Criteria)가 있다.

국제공통평가기준은 ISO/IEC에서 국제표준(ISO 15408)으로 제정되었고, 보안기술 평가에 관련한 표준제정 작업을 담당하고 있는 ISO/IEC JTC 1/SC 27 WG 3에서는 국제공통평가기준의 활용을 원활하게 하기 위해서 국제공통평가기준과 관련된 표준문서 초안을 개발 중에 있다. 선진국들은 국제공통평가기준을 이용하여 국가별로 평가받은 제품에 대하여 효력을 상호 인정하는 CCRA(Common Criteria Recognition Arrangement) 협정을 체결하고, 평가 결과를 국가간 상호 인정하여 정보보호제품의 수출·입 및 다양한 평가제품의 활용이라는 측면에서 소비자의 욕구를 만족시키고 있다. 우리 나라도 개별 제품 평가기준의 국한된 평가 한계를 극복하고 다양한 제품을 평가할 수 있도록 국제공통평가기준 기반 평가제도 도입을 준비중에 있으며, 상호인정협정의 가입을 검토하고 있다.

국제공통평가기준은 모든 정보보호시스템 유형을 포괄할 수 있는 보안 요구사항을 제시한 평가기준으로 정보보호시스템 보안 요구사항의 집합체라 할 수 있다. 특정한 형태의 정보보호시스템을 대상으로 하

* 한국정보통신기술협회(abysskey@yahoo.co.kr)
** 순천향대학교 정보기술공학부
*** 한국전자통신연구원 부설 국가보안기술연구소

는 평가기준이 되기 위해서는 사용환경, 보안목적에 적합한 보안 요구사항이 도출되어야 한다. 즉, 정보보호시스템을 사용하고자 하는 보안환경 및 보안목적을 정의하고, 이에 적합한 보안 요구사항을 국제공통평가기준에서 선택하여 단일제품별 평가기준으로 작성한 것이 보호프로파일이다. 보호프로파일이나 보안목표명세서의 대상이 되는 정보보호제품이나 시스템을 TOE(Target of Evaluation)라고 한다. 보호프로파일의 작성목적은 정보보호시스템의 구현기술을 서술하고자 하는 것이 아니라 보안환경에 의해서 정의한 보안목적을 만족하도록 보안대책을 체계적으로 세우고 이에 합당한 보안 요구사항을 도출하여 정보보호시스템을 논리적으로 평가하고자 하는 것이다.

본 고에서 설명하고자하는 보호프로파일은 키 복구 제품시스템의 한 부분인 키 복구 에이전트 시스템이다. 2장에서 키 복구 에이전트 시스템 보호프로파일의 내용에 대해 설명하고, 3장에서 결론을 맺도록 한다.

## Ⅱ. 키 복구 에이전트 시스템 보호프로파일

다음은 키 복구 에이전트 시스템 보호프로파일의 구성과 내용에 대해 설명한다.

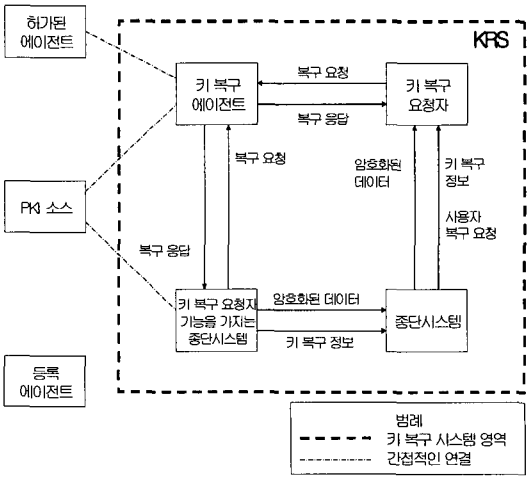
### 1. 보호프로파일 개요

키 복구 에이전트 시스템(KRAS : Key Recovery Agent System) 보호프로파일은 키 복구 에이전트를 구현 또는 개발하기 위한 지침서로서 제공되고 기술되었다. 이 보호프로파일은 키 복구 에이전트에 대한 보안 요구사항을 정의하고 있으며 정보 시스템 보안 엔지니어, 상점, 시스템 개발자, 그리고 일반적으로 통용되는 키 복구 에이전트 제품들의 취약점을 식별하는데 유용하게 사용될 것이다.

키 복구 에이전트 시스템 보호프로파일은 다음과 같이 구성되어 있다.

- 세션 1 : 보호프로파일에 대한 요소들의 개요를 제공한다.
- 세션 2 : TOE 명세와 일반적 목적을 제공한다.
- 세션 3 : TOE를 위한 예상된 환경의 안건을 제공하고, TOE 하드웨어나 소프트웨어 또는 환경 설정을 통해서 수행된 기술에 의해 나타나는 위협들의 집합을 정의한다.
- 세션 4 : TOE와 TOE 환경을 위한 보안 목적을 정의한다.
- 세션 5 : 공통평가기준 Part 2, Part 3에 의해 다루어진 기능과 보증 요구사항을 다룬다.
- 세션 6 : 정책과 위협을 해결하는 정보기술 보안 객체의 명시적 논증에 대한 이론적 근거를 제공하고, 논점은 각 정책과 위협의 범위를 제공한다. 그리고 하나 또는 그 이상의 구성요소 요구사항에 의해 표시된 각 보안 목적과 객체에서 상대적으로 완성된 요구사항의 집합에 대하여 설명하고 종속관계 분석, 기능강도 문제, 보호프로파일 요구사항의 상호 유지 관계 그리고 내부 견고성에 대한 논점들의 집합을 제공한다.

이 보호프로파일은 키 복구 시스템 구성요소를 묘사하고 있는 보호프로파일의 시리즈 중 하나이다. 키 복구 시스템은 기밀성을 가진 보호된 데이터 또는 기밀성을 위해 사용된 키의 복구 기능을 제공한다. 키 복구 시스템 구성요소는 종단 시스템 구성요소, 요청자 기능을 가지는 종단 시스템 구성요소, 요청자 구성요소, 그리고 키 복구 에이전트 구성요소를 포함하고 있다. 허가된 에이전트, PKI 소스, 그리고 등록 에이전트와 같은 다른 구성요소들은 키 복구 시스템과 상호작용이 고려된다. 그러나 시스템의 한 부분은 아니다. [그림 1]은 키 복구 시스템의 구성요소에 대해 설명하고 있다.




[그림 1] 키 복구 시스템 구성요소

이 보호프로파일의 TOE는 키 복구 에이전트 시스템이다. 키 복구 에이전트는 승인된 키 복구 요청에 대한 응답으로서 키 복구 서비스를 수행한다. 키 복구 응답의 결과(기밀성을 가지는 데이터 또는 암호화 연계에서 사용된 키의 반환)는 유용한 키 복구 기술에 의존한다. 여기서 포함하는 두 가지 기술은 다음과 같다.

- 키 캡슐화 기술 : 키나 키 부분 또는 키와 관련된 정보는 키 복구 에이전트를 통해 암호화되고, 암호화된 데이터와 연계된다. 이렇게 구성됨으로써 추후에 키 복구가 가능하게 된다.
- 키 위탁 기술 : 복구되는 비밀, 개인키, 키 부분들, 또는 키와 관련된 정보가 하나 또는 그 이상의 키 복구 에이전트와 연계되어 위탁됨으로써 추후에 키 복구가 가능하게 된다.

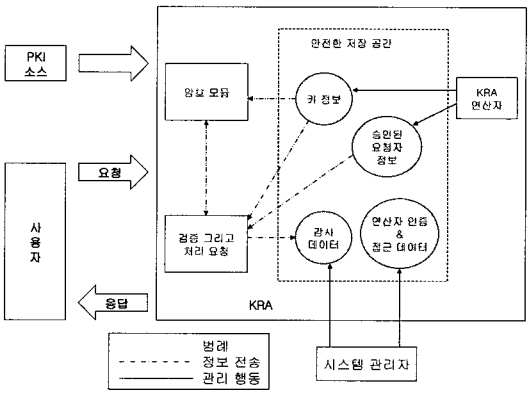
이 보호프로파일은 상기 두 가지 키 복구 기술에 모두 적용할 수 있고, 이와 관련된 보호프로파일은 다음과 같다.

- 종단 시스템을 위한 키 복구 보호프로파일
- 제 3의 요청자를 위한 키 복구 보호프로파일

## 2. TOE 명세

키 복구 에이전트는 요청자에 의해 만들어진 승인된 요청에 대한 응답으로 키 복구 서비스를 수행하는 신뢰된 개체이다. 키 복구 서비스는 요청자에 의해 키 복구 에이전트로부터 제공되는 키 복구 정보를 처리하고 검증하는 것으로 구성된다. 그리고 요청자에게 키 또는 복호화된 데이터를 반환한다. 이러한 절차가 진행되기 전에, 키 복구 에이전트는 요청자의 신원과 요청된 키 복구 서비스가 올바른지를 검증한다.

이 보호프로파일은 키 위탁 그리고 키 캡슐화 기술 모두에 적용 가능하다. [그림 2]는 키 복구 에이전트 기능의 개요를 보여주고 있다. 키 복구 에이전트는 주로 요청자나 다른 키 복구 에이전트들과의 인터페이스를 수행한다. 또한, 키 복구 에이전트는 받은 키 또는 키 요소를 PKI(Public Key Infrastructure) 소스(만약 키 복구 에이전트와 PKI 소스가 분리되어 있다면)와 상호 동작한다. 키 복구 에이전트의 기능을 수월하게 하기 위해, 키 복구 에이전트 시스템은 안전한 데이터 저장 공간을 포함해야 한다. 이 공간은 인증 요청시에 키 복구 에이전트를 도와주고 키 또는 데이터의 접근을 통제하는 등의 정보를 포함하고 있다. 감사 데이터 그리고 키 정보 또한 이 영역에 위치된다.




[그림 2] 키 복구 에이전트 시스템

내부 키 복구 에이전트는 키 복구 요청을 처리하고 모든 암호학적 기능을 위한 FIPS 140-1 단계 3에 해당하는 암호모듈에 일치하는 응답을 생성한다. 추가적으로, 내부 처리에서는 진행 또는 생성하는 키 복구 요청에 대한 결정을 하기 위해서 안전한 저장 장소에서 정보를 이용한다.

TOE에서의 동작은 두 가지, 시스템 관리자와 키 복구 에이전트 연산자, 역할을 수행한다. 키 복구 에이전트 연산자는 사용자, 종단 시스템, 키 복구 에이전트 키, 그리고 리스트 및 기능에 요청자의 접근 통제를 수행하는 관리자와의 연계를 통하여 키 복구를 수행한다.

만약 키 복구 에이전트 시스템이 키 복구 에이전트 연산자 역할을 사람에게 요구한다면, 이 역할은 TOE의 부분으로 고려된다. 키 복구 에이전트의 시스템 관리자는 설치, 유지보수, 감사, 관리, 그리고 TOE 사용자 계정 관리 등을 고려해야 한다. TOE에 저장된 데이터는 TOE 보안 기능(TSF) 데이터와 사용자 데이터이다. TSF 데이터는 감사 데이터, 관리자 인증, 접근 데이터, 그리고 승인된 요청자 정보로써 구성되고, 사용자 데이터는 사용자 키 또는 키 복구 에이전트에 의해서 얻어지는 키 정보로써 구성된다.

TOE 형태는 아래 3개의 문서에 평가기준 그리고 요구사항을 부분적으로 기초한다. 3개의 문서는 다음과 같다.

- "키 복구 제품을 위한 요구사항"이라고 명명된 TAC (Technical Advisory Committee) 리포트
- IATF(Information Assurance Technical Framework) Release 2.0
- KREC(Key Recovery Evaluation Criteria)

이 보호프로파일은 키 복구 에이전트에 의해 구현된 IT(Information Technology) 보안 요구사항의 최소 집합을 묘사하고 있다.

## 3. TOE 보안 환경

여기서는 안전한 사용을 위한 전제와 보안 위협 그리고 보안 정책에 대해 설명한다.

### 3.1 안전한 사용을 위한 전제 사항

이 보호프로파일에서 기술하고 있는 TOE를 사용하기에 앞서 전제로 하는 4가지 사항에 대해 설명한다. 다음은 이 문서에서 기술하고 있는 전제 사항이다.

- A.CRYPTO : 암호학적 연산은 FIPS 140-1 단계 3에 해당하는 암호모듈을 사용하는 TOE에 대해 내부적으로 수행된다.
- A.FACILITY : TOE는 통제된 접근 시설하에서 수행된다. 시설은 여기에 포함된 정보의 감도에 대해서는 인가되고, 비인가된 물리적 접근이나 변경에 대응하는 보호 기능을 제공한다.
- A.NO_EVIL : 인가된 사용자들 그리고 관리자는 우호적이고 보안 정책 그리고 절차를 제공한다. 그러나 그들 또한 오류 능력을 가지고 있다고 가정한다.
- A.OS : 기본적인 운영체제는 서비스를 포함해서 수행하는 TOE에 의지하게 된다. 그러나 식별 및 인증, 다른 응용과 데이터로부터 TOE 응용과 데이터의 분리 등은 제한되지 않는다.

### 3.2 TOE에 대한 보안 위협

이 보호프로파일에서 기술하고 있는 TOE에 대한 보안 위협 16가지를 설명한다. 여기서, 공격자는 전문기술, 리소스 그리고 동기에 대한 다양한 단계를 가지고 있다고 가정한다. 관련된 전문기술은 소프트웨어 공학, 해킹 기술 또는 TOE 명세일 수 있다. 리소스는 값싼 장치인 개인 컴퓨터부터 값비싼 장치인 세련된 공학 테스트 그리고 측정 장치일 수 있다. 그들은 아마도 소프트웨어 처리 순서, 인터넷상에서 이용할 수 있는 것들을 모두 포함할 수 있다. 동기는 경제적 보수 또는 만족 그리고 전문 보안 파괴의 평판을 포함할 수 있다.

보호프로파일에서 기술하고 있는 보안 요소를 갖추고 있다면 TOE는 아래에 정의된 위협에 대항하는 방어 기능을 가지게 될 것이다. 다음은 이 문서에서 기술하고 있는 보안 위협이다.

- T.ACCESS_CONTROL : 만약 TOE 소프트웨어 그리고 데이터에 대한 접근 통제가 수행되지 않을 경우 비 인가된 사용자는 보안 함수를 손상 및 변경할 수 있다.
- T.AUDFAIL : 시스템 변경, 절충, 또는 전체 감사 파일은 감사 데이터 분석 실패의 결과이다.
- T.AUDMOD : 비인가된 사용자는 악의있는 행동으로 감사 기능을 손상 또는 감사 데이터를 변경할 수 있다.
- T.AUDREV : 감사 데이터의 번역 그리고 검사에 대해 실패할 수 있다.
- T.BACKUP : 시스템 관리자는 TOE의 비가용성 또는 타협의 결과로써 TSF 데이터의 시스템 백업에 실패할 수 있다.
- T.COMPROMISE : 키 복구 에이전트 시스템 또는 키 복구 에이전트 연산자는 아이템의 타협의 결과로써 사용자의 개인키 또는 기밀 데이터를 보호하는데 실패할 수 있다.
- T.ERROR : 인가된 사용자 또는 관리자는 사용자 또는 시스템 리소스에 대해 비인가된 것 또는 잘못된 액션의 수행을 시도할 수 있다.
- T.IMPERSONATE : 비인가된 사용자는 키 복구 에이전트 연산자 또는 관리자 TOE에 접근하려는 시도를 할 수 있다.
- T.KRA_ROGUE : 부정한 키 복구 에이전트는 기밀성을 가지는 보호된 데이터에 대응하는 복호화가 아닌 비인가된 사용자가 허락한 비인가된 방식에 의해 키가 노출될 수 있다.
- T.MALICIOUS : 악의적인 소프트웨어는 키의 부주의한 노출과 같이 TOE의 키 복구 정책 시행 메커니즘의 연산이 손상 또는 변경될 수 있다.
- T.MEDIA : 저장 미디어의 적당한 보호의 실패는 아마도 저장된 데이터의 비가용성의 원인 또는

공격자의 타협으로 인한 결과일 것이다.

- T.MODIFY : TSF 데이터의 무결성은 공격자에 의해 TSF 데이터의 비인가된 변경 또는 파괴하는 것을 타협할 수 있다.
- T.PHYSICAL : 인가된 그리고 비인가된 사용자는 TOE의 물리적인 공격 보안 평가 부분이다.
- T.SPOOF : 비인가된 사람은 인가된 요청자로 가장하여 사용자 키 또는 데이터의 접근 권한을 획득할 수 있다.
- T.UNDETECT : 비인가된 사용자에 의한 시스템 리소스의 타협은 시간의 긴 주기 동안 발견되지 않을 지도 모른다.
- T.UNSECURED : TOE는 사용자 키 또는 데이터의 비인가된 노출, 서비스 단절 또는 악의 있는 행동과 같은 위험한 상태에 처할 수 있다.

### 3.3 보안 정책

이 보호프로파일에서 기술하고 있는 TOE에 대한 보안 정책 5가지를 설명한다. 다음은 이 문서에서 기술하고 있는 보안 정책이다. TOE는 아래에 정의된 정책에 기반하여 보호를 제공해야 한다.

- P.ACCOUNTABLE : 사용자 활동은 부정행위가 일어날 경우, 그리고 시스템 통제들이 적당히 적용되는 것을 확실히 하기 위하여 적용된 허가를 모니터할 것이다.
- P.MANAGE : TOE는 생명주기 동안 연산을 통하여 보존되고 구현된 TSF와 같이 관리될 것이다.
- P.PROTECT : TOE는 접근 통제 그리고 시스템 리소스의 무결성을 제공할 것이다.
- P.TRAINING : 모든 TOE 사용자들 그리고 관리자들은 사용할 수 있는 TOE에 접근하는 것에 앞서 TSF에 적당히 훈련될 것이다.
- P.KRA_POLICY : 키 복구 에이전트는 키 복구 에이전트 정책 구조에 기반한 문서화된 정책을 가지고 있다. 그리고 그것은 이 정책에 따라 연산된다.

## 4. 보안 목적

다음은 이 보호프로파일에서 기술하고 있는 보안 목적에 대해 설명한다. 보안 목적은 TOE를 위한 보안 목적과 TOE 환경에 대한 보안 목적으로 나누어 설명한다.

### 4.1 TOE를 위한 보안 목적

여기서는 이 보호프로파일에 기술되어 있는 보안 목적 중에서 TOE를 위한 보안 목적에 대해 설명한다. 다음은 TOE를 위한 보안 목적을 설명한 것이다.

- O.ACCESS : TSF는 TOE에 대한 보안 정책을 우회할 수 없는 타당한 개인적인 식별에 기초하여 TOE에 대해 접근 통제를 수행하게 된다.
- O.ANTIVIRUS : TOE는 유효한 악의 있는 코드를 검출하고 치료하는 기능을 제공할 수 있게 된다.
- O.AUDIT : TOE는 가능한 공격들의 검출 또는 TOE 보안 형태의 관리자를 원조하기 위해 어떠한 보안과 관련된 이벤트들을 기록하는 방법을 제공할 것이다. 그리고 어떠한 사용자들의 보안과 관련된 행동에 대한 증거와 같은 역할 또한 수행하게 된다.
- O.CONFIDENTIAL : TOE는 전송 또는 저장하는 기밀 데이터 또는 사용자 개인키의 기밀성과 무결성을 확보하기 위한 메커니즘을 제공할 것이다.
- O.INTEGRITY : TOE는 인가되지 않은 변경으로부터 TOE 보안 데이터를 보호하기 위한 메커니즘을 제공할 것이다.
- O.KRA_ROGUE : TOE는 키 또는 기밀 데이터의 비인가된 공개의 보호를 제공할 것이다.
- O.MANAGE : TOE는 보안 기능들에 대하여 충분한 관리 특징을 제공할 것이다.
- O.MODIFY : 모든 변경 TSF 데이터는 감사 데이터 표기의 결과이다.
- O.POLICY_ENFORCE : TSF는 TSP와 TOE를 위한 어떠한 다른 연산 정책을 시행할 것이다.
- O.POWERUP : TOE는 전원이 유지되는 경우 보안 단계에서 연산될 것이다.
- O.PROOF : TOE는 신원 요청자들, 그리고 키 복구 연산을 위한 영수 또는 원본의 증거를 생성하는 메커니즘을 제공할 것이다.

### 4.2 TOE 환경을 위한 보안 목적

여기서는 이 보호프로파일에 기술되어 있는 보안 목적 중에서 TOE 환경을 위한 보안 목적에 대해 설명한다. 다음은 TOE 환경을 위한 보안 목적을 설명한 것이다.

- OE.INSTALL : TOE는 시스템의 보안을 유지하기 위한 방법으로써 전달, 설치, 관리 그리고 연산될 것이다.
- OE.OS : TOE는 식별 그리고 인증된 모든 관리자와 연산자, 다른 응용 그리고 데이터로부터 TOE 응용의 세분화에 대해 운영체제에 의지할 것이다.
- OE.PHYSICAL : TOE를 위한 이러한 책임은 물리적인 공격으로부터 보호되는 보안 정책 시행의 평가기준인 TOE의 부분에 의해 보증되어야 한다.
- OE.REVIEW : 시스템 관리자는 정기적으로 감사 데이터를 검토할 것이다.
- OE.TRAIN : 관리자들은 TOE 보안 기능의 적당한 운영에 대해 훈련한다. 또한, 관리자들은 보안 정책들과 연습들에 따라서 TOE 보안 파라미터들을 설립한다.

## 5. IT 보안 요구사항

본 절에서는 이 보호프로파일에서 기술하고 있는 TOE 보안 기능 요구사항과 TOE 보안 보증 요구사항에 대해 설명한다.

### 5.1 TOE 보안 기능 요구사항

여기서는 이 보호프로파일에서 기술하고 있는 보안 기능 요구사항에 대해 설명한다. 보호프로파일에서는 CC Part 2에 있는 요구사항들 중에서 해당하는 TOE가 가져야 하는 요구사항만을 기술한 것이다. [표 1]은 TOE를 위한 기능 요구사항들을 나타낸 것이다.

### 5.2 TOE 보안 보증 요구사항

여기서는 이 보호프로파일에서 기술하고 있는 보안 보증 요구사항에 대해 설명한다. 이 보호프로파일은 키 복구 에이전트 시스템을 위한 보증 요구사항에 대해 기술하고 있다. 키 복구 에이전트 시스템을 위한 보안 보증 요구사항은 기본적인 결함교정(ALC_FLR.1)의 보증 단계 EAL 3에서 보증한다. 이들은 CC Part 3에서 있는 요구사항들 중에서 해당하는 TOE가 가져야 하는 요구사항만을 기술한 것이다. [표 2]는 이 보호프로파일에서 기술하고 있는 보안 보증 요구사항을 나타낸 것이다.

[표 1] TOE를 위한 기능 요구사항들

| 클래스 | 구성요소 |
|---|---|
| 보안 감사 | 감사 데이터 생성(FAU_GEN.1)<br>사용자 신원 연관(FAU_GEN.2)<br>감사 검토(FAU_SAR.1)<br>감사 검토 권한 제한(FAU_SAR.2)<br>감사 데이터의 가용성 보장(FAU_STG.2) |
| 통신 | 강제적인 발신증명(FCO_NRO.2)<br>강제적인 수신증명(FCO_NRR.2) |
| 암호 지원 | 암호 키 분배(FCS_CKM.2)<br>암호 키 접근(FCS_CKM.3)<br>암호 연산(FCS_COP.1) |
| 사용자 데이터 보호 | 부분적인 접근통제(FDP_ACC.1)<br>보안속성에 기반한 접근통제(FDP_ACF.1)<br>기본적인 데이터 인증(FDP_DAU.1)<br>보안속성을 포함한 사용자 데이터 유출(FDP_ETC.2)<br>부분적인 정보흐름 통제(FDP_IFC.1)<br>단일 계층 보안 속성(FDP_IFF.1)<br>보안속성을 포함한 사용자 데이터 유입(FDP_ITC.2)<br>기본적인 내부전송 보호(FDP_ITT.1)<br>무결성 검사(FDP_ITT.3)<br>저장된 데이터의 무결성 검사(FDP_SDI.1)<br>전송 데이터 무결성(FDP_UIT.1) |
| 식별 그리고 인증 | 모든 행동 이전에 사용자 인증(FIA_UAU.2)<br>모든 행동 이전에 사용자 식별(FIA_UID.2) |
| 보안 관리 | 보안기능 관리(FMT_MOF.1)<br>보안속성 관리(FMT_MSA.1)<br>안전한 보안속성(FMT_MSA.2)<br>정적 속성 초기화(FMT_MSA.3)<br>TSF 데이터 관리(FMT_MTD.1)<br>보안 역할(FMT_SMR.1) |
| TSF 보호 | 추상기계 시험(FPT_AMT.1)<br>내부전송 TSF 데이터의 기본적인 보호(FPT_ITT.1)<br>TSP의 우회불가성(FPT_RVM.1)<br>신뢰할 수 있는 타임스탬프(FPT_STM.1)<br>TSF간 전송되는 TSF 데이터의 일관성 (FPT_TDC.1)<br>TSF 자체 시험(FPT_TST.1) |
| 안전한 경로/ 채널 | TSF간 안전한 채널(FTP_ITC.1) |

## 6. 이론적 근거

본 절에서는 이 보호프로파일에서 기술하고 있는 이론적 근거에 대해 설명한다. 보호프로파일은 이론적 근거를 보안 목적, 보안 요구사항, 종속관계, 기능강도로 나누어 설명한다.

〔표 2〕 TOE를 위한 보증 요구사항

| 클래스 | 구성요소 |
|---|---|
| 형상관리 | 인가통제(ACM_CAP.3)<br>TOE 형상관리 범위(ACM_SCP.1) |
| 배달 및 운영 | 배달 절차(ADO_DEL.1)<br>설치, 생성 시동 절차(ADO_IGS.1) |
| 개발 | 비정형화된 기능명세(ADV_FSP.1)<br>보안기능과 비보안기능을 분리한 기본 설계(ADV_HLD.2)<br>비정형화된 일치성 입증(ADV_RCR.1) |
| 설명서 | 관리자 설명서(AGD_ADM.1)<br>사용자 설명서(AGD_USR.1) |
| 생명주기 지원 | 보안대책의 식별(ALC_DVS.1)<br>기본적인 결함교정(ALC_FLR.1) |
| 시험 | 시험범위의 분석(ATE_COV.2)<br>기본설계 시험(ATE_DPT.1)<br>기능 시험(ATE_FUN.1)<br>독립적인 시험 : 표본 시험(ATE_IND.2) |
| 취약성 평가 | 설명서에 대한 조사(AVA_MSU.1)<br>TOE 보안기능 강도에 대한 평가(AVA_SOF.1)<br>개발자에 의한 취약성 분석(AVA_VLA.1) |

### 6.1 보안 목적의 이론적 근거

여기서는 각 정책, 위협에 대한 매핑 테이블 그리고 개별적인 인수들을 포함하고 있다. 〔표 3〕은 1번째 칼럼에 요구된 범위상에서 기관의 기밀 보호 정책 혹은 위협들을 나열했다. 관련되고 적용할 수 있는 가정들은 2번째 칼럼에 나열했고, 적용할 수 있는 가정들이 주어진 각 정책과 위협을 포함한 객체는 3번째 칼럼에 나열했다.

### 6.2 보안 요구사항의 이론적 근거

#### 6.2.1 기능적 보안 요구사항의 이론적 근거

여기서는 각 객체를 위한 개인적인 인자 그리고 매핑 테이블을 포함하고 있다. 〔표 4〕의 1번째 칼럼은 TOE 또는 환경 객체를 나열하고 있고, 각 객체에 대한 TOE 또는 환경 요구사항은 2번째 칼럼에 나열하고 있다.

#### 6.2.2 보증 보안 요구사항의 이론적 근거

보증 보안 요구사항은 EAL 3에 기초하고 있다. 기본적인 결함교정은 건전한 개발 실습에 있어서 현재의 수정은 요구되지 않는 보안 기술자의 최대 보증 제공을 선택한다. 추가적으로, 이 보호프로파일의 단 하나의 목표는 이용 가능한 키 복구 에이전트 시스템을 획득하도록 도와주는 것이다. 이것은 특별한

〔표 3〕 TOE보안 환경상의 보안 목적의 흐름

| 정책/위협 | 가정 | 객체 |
|---|---|---|
| P.ACCOUNTABLE | A.NO_EVIL | O.AUDIT<br>OE.OS |
| P.MANAGE | A.NO_EVIL | O.MANAGE<br>OE.TRAIN |
| P.PROTECT | A.FACILITY | O.ACCESS<br>O.INTEGRITY |
| P.TRAINING | | OE.TRAIN |
| P.KRA_POLICY | A.NO_EVIL | O.POLICY_ENFORCE |
| P.KRA_POLICY | A.NO_EVIL | O.POLICY_ENFORCE |
| T.ACCESS_<br>CONTROL | | O.ACCESS<br>O.MODIFY<br>OE.OS |
| T.AUDFAIL | | O.AUDIT |
| T.AUDMOD | | O.INTEGRITY<br>O.MODIFY |
| T.AUDREV | | OE.REVIEW<br>OE.TRAIN |
| T.BACKUP | | O.POLICY_ENFORCE<br>OE.TRAIN |
| T.COMPROMISE | A.CRYPTO | O.CONFIDENTIAL |
| T.ERROR | | O.ACCESS<br>O.POLICY_ENFORCE<br>OE.TRAIN |
| T.IMPERSONATE | | OE.OS |
| T.KRA_ROGUE | A.FACILITY | O.KRA_ROGUE |
| T.MALICIOUS | | O.ANTIVIRUS<br>O.AUDIT<br>OE.REVIEW |
| T.MEDIA | A.NO_EVIL<br>A.FACILITY | O.ACCESS<br>OE.INSTALL<br>OE.TRAIN |
| T.MODIFY | A.NO_EVIL<br>A.FACILITY | O.ACCESS<br>O.AUDIT<br>O.INTEGRITY<br>O.MODIFY<br>OE.INSTALL<br>OE.REVIEW |
| T.PHYSICAL | A.NO_EVIL<br>A.FACILITY | OE.PHYSICAL |
| T.SPOOF | A.NO_EVIL<br>A.FACILITY | O.PROOF |
| T.UNDETECT | | O.AUDIT<br>O.MODIFY<br>OE.REVIEW |
| T.UNSECURED | | O.POWERUP |

〔표 4〕 보안 객체 매핑에서의 기능적 구성요소

| 객체 | 요구사항 |
|---|---|
| O.ACCESS | FAU_SAR.1, FAU_SAR.2, FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FPT_RVM.1 |
| O.ANTIVIRUS | FDP_ITT.3, FDP_SDI.1, FDP_UIT.1, FPT_ITT.1, FPT_TST.1 |
| O.AUDIT | FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.2, FPT_STM.1 |
| O.CONFIDENTIAL | FCS_CKM.2, FCS_CKM.3, FCS_COP.1, FDP_DAU.1, FDP_ETC.2, FDP_ITC.2, FDP_ITT.1, FDP_ITT.3, FDP_SDI.1, FDP_UIT.1, FTP_ITC.1 |
| O.INTEGRITY | FAU_STG.2, FCS_CKM.3, FCS_COP.1, FMT_MSA.1, FMT_MTD.1 |
| | FPT_ITT.1 , FPT_TST.1 |
| O.KRA_ROGUE | FAU_GEN.1, FAU_GEN.2, FDP_IFC.1, FDP_IFF.1, FPT_RVM.1 |
| O.MANAGE | FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1 |
| O.MODIFY | FAU_GEN.1, FAU_GEN.2, FAU_STG.2, FPT_ITT.1, FPT_TST.1 |
| O.POLICY_ENFORCE | FDP_ACC.1, FDP_ACF.1, FDP_ETC.2, FDP_IFC.1, FDP_IFF.1, FDP_ITC.2, FDP_ITT.1, FDP_ITT.3, FDP_UIT.1, FMT_MSA.1, FMT_MSA.3, FPT_RVM.1 |
| O.POWERUP | FPT_AMT.1, FPT_TST.1 |
| O.PROOF | FCO_NRO.2, FCO_NRR.2, FPT_TDC.1 |
| OE.INSTALL | ADO_DEL.1, ADO_IGS.1, FPT_AMT.1, FPT_RVM.1 |
| OE.OS | FDP_ACC.1, FDP_ACF.1, FIA_UAU.2, FIA_UID.2, FMT_SMR.1, FPT_AMT.1 |
| OE.PHYSICAL | 이론적 근거를 참조 |
| OE.REVIEW | AGD_ADM.1, FAU_SAR.1, FAU_SAR.2 |
| OE.TRAIN | AGD_ADM.1, AGD_USR.1, FMT_MOF.1, FMT_MSA.2 |

지식, 기술 또는 리소스를 필요로 하는 개발자를 필요로 하지 않고, 충분한 관리자와 연산자 지침서와 함께 독립적으로 보증된 시스템을 제공한다.

### 6.3 종속성의 이론적 근거

다음 요구사항은 CC Part 2의 보안 기능 요구사항에 종속성으로써 포함되어 있다. 〔표 5〕는 기능적 요구사항 종속성을 나타낸 것이다.

### 6.4 기능 강도의 이론적 근거

IATF 문서에서, 기능강도는 SML(Strength of Mechanism Level)과 같이 참조된다. 이 보호프로파일의 요구사항을 만족하는 키 복구 에이전트는 최소한 SML-2의 메커니즘 단계의 강도를 가져야 한다. 다음은 IATF에 나와있는 SML에 대한 설명이다.

- SML1 : "기본" 강도 또는 좋은 상업적 실습으로 정의된다. 이것은 간단한 위협을 보호할 수 있고, 저가의 데이터를 보호하기 위해 사용된다.
- SML2 : "중간" 강도로써 정의된다. 이것은 복잡한 위협을 보호할 수 있고, 중간 정보의 비용이 드는 데이터를 보호하기 위해 사용된다. 이것은 일반적으로 많은 노력을 통한 위협에 대해 방어할 수 있다. 예로써, 해커 그룹의 공격을 들 수 있다.
- SML3 : "높음" 강도로써 정의된다. 그것은 국영 연구소 또는 국가적 차원의 위협에 대항할 수 방어를 할 수 있고, 높은 가치의 데이터를 보호하는데 사용된다. 예로는 매우 강력한 핵심 기반 기술을 가진 연구소 또는 국가 차원의 상대가 될 수 있다.

## Ⅲ. 결 론

기존에 나와있는 키 복구 시스템과 관련된 보호프로파일은 총 3가지로 나누어져 있다. 이들 중에서 우리는 키 복구 에이전트 시스템에 대한 보호프로파일의 내용을 살펴보았다. 이 보호프로파일들은 특정 목적의 키 복구 시스템에 대해 언급하지 않고 전반적인 내용에 대해 다루고 있다. 이것은 어떤 특정한 목적을 가지는 키 복구 시스템이 필요할 경우 이에 알맞은 보호프로파일을 생성하는데 기초자료가 될 수 있을 것이다.

〔표 5〕 기능적 요구사항 종속성

| 색인 | 요구사항 | 의존성 | 범위 |
|---|---|---|---|
| 1 | FAU_GEN.1 | FPT_STM.1 | 33 |
| 2 | FAU_GEN.2 | FAU_GEN.1, FIA_UID.1 | 1, 22 |
| 3 | FAU_SAR.1 | FAU_GEN.1 | 1 |
| 4 | FAU_SAR.2 | FAU_SAR.1 | 3 |
| 5 | FAU_STG.2 | FAU_GEN.1 | 1 |
| 6 | FCO_NRO.2 | FIA_UID.1 | 22 |
| 7 | FCO_NRR.2 | FIA_UID.1 | 22 |
| 8 | FCS_CKM.2 | No FCS_CKM.1, no FCS_CKM.4, FMT_MSA.2 | 25 |
| 9 | FCS_CKM.3 | No FCS_CKM.1, no FCS_CKM.4, FMT_MSA.2 | 25 |
| 10 | FCS_COP.1 | No FCS_CKM.1, no FCS_CKM.4, FMT_MSA.2 | 25 |
| 11 | FDP_ACC.1 | FDP_ACF.1 | 11 |
| 12 | FDP_ACF.1 | FDP_ACC.1, FMT_MSA.3 | 10, 26 |
| 13 | FDP_DAU.1 | None | N/A |
| 14 | FDP_ETC.2 | FDP_IFC.1 | 10 |
| 15 | FDP_IFC.1 | FDP_IFF.1 | 15 |
| 16 | FDP_IFF.1 | FDP_IFC.1, FMT_MSA.3 | 14 ,26 |
| 17 | FDP_ITC.2 | FDP_ACC.1, FDP_IFC.1, FTP_ITC.1, FPT_TDC.1 | 10, 34 |
| 18 | FDP_ITT.1 | FDP_ACC.1, FDP_IFC.1 | 10 |
| 19 | FDP_ITT.3 | FDP_ACC.1, FDP_IFC.1, FDP_ITT.1 | 10, 17 |
| 20 | FDP_SDI.1 | None | N/A |
| 21 | FDP_UIT.1 | FDP_IFC.1, FTP_ITC.1 | 14, 16 |
| 22 | FIA_ATD.1 | None | N/A |
| 23 | FIA_UAU.2 | FIA_UID.1 | 22 |
| 24 | FIA_UID.2 | None | N/A |
| 25 | FIA_USB.1 | FIA_ATD.1 | 21 |
| 26 | FMT_MOF.1 | FMT_SMR.1 | 28 |
| 27 | FMT_MSA.1 | FDP_ACC.1, FDP_IFC.1, FMT_SMR.1 | 10, 28 |
| 28 | FMT_MSA.2 | No ADV_SPM.1, FDP_ACC.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1 | 10, 24, 28 |
| 29 | FMT_MSA.3 | FMT_MSA.1, FMT_SMR.1 | 24, 28 |
| 30 | FMT_MTD.1 | FMT_SMR.1 | 28 |
| 31 | FMT_SMR.1 | FIA_UID.1 | 22 |
| 32 | FPT_AMT.1 | None | N/A |
| 33 | FPT_ITT.1 | None | N/A |
| 34 | FPT_RVM.1 | None | N/A |
| 35 | FPT_STM.1 | None | N/A |
| 36 | FPT_TDC.1 | None | N/A |
| 37 | FPT_TST.1 | FPT_AMT.1 | 29 |
| 38 | FTP_ITC.1 | None | N/A |

향후 나머지 2개의 보호프로파일에 대한 분석과 함께, 이들 모두를 연계하여 국내 환경에 적합한 새로운 키 복구 시스템 보호프로파일의 연구가 진행되어야 할 것이다.

## 참 고 문 헌


[1] NSA, Key Recovery Agent System Protection Profile, 2000.1.14

[2] NSA, Key Recovery Third Party Requestor Protection Profile, 2000.2.21

[3] NSA, Key Recovery End System Protection Profile, 2000.1.14

[4] 정보통신부 고시 제2001-24호, 정보보호시스템 평가·인증 지침, 2001.4.24

[5] CCIMB-99-031, Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, 1999.8.1

[6] CCIMB-99-032, Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, 1999.8.1

[7] CCIMB-99-033, Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, 1999.8.1

[8] ISO/IEC 15408-1, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, 1999.12.1

[9] ISO/IEC 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements, 1999.12.1

[10] ISO/IEC 15408-3, Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements, 1999.12.1

[11] NIST, Common Criteria Protection Profile Development Workshop Student Handbook V2.0. 2000.8.1


## 〈著 者 紹 介〉


**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

**김 춘 수 (Choon-Soo Kim)**
**정회원**

1987년 2월 : 숭실대학교 전기공학과 졸업
1989년 2월 : 숭실대학교 전기공학과 석사
1998년 2월 : 숭실대학교 전기공학과 박사
1990년 2월~1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월~현재 : 한국전자통신연구원 부설 국가보안기술연구소 팀장
관심분야 : 전자화폐, 정보보호응용

**채 수 영 (Soo-Young Chae)**

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

**나 학 연 (Na-Hac Yun)**

1999년 2월 : 숭실대학교 컴퓨터학과 학사
2001년 2월 : 숭실대학교 컴퓨터학과 석사
2001년 3월~현재 ETRI 부설 국가보안기술연구소 연구원
관심분야 : 평가 체계, 정보보호이론