通信情報保護學會誌
第 10 券 第 3 號, 2000. 9

정보보호시스템 평가기준 보안기능 요구사항 분석

조 규 민*, 황 영 석*, 이 경 구*

요 약

정보보호시스템을 평가하기 위한 기준은 보안기능 요구사항 및 보증요구 사항으로 이루어진다.[1] 본고에서는 미국의 TCSEC(Trusted Computer System Evaluation Criteria)과 유럽의 ITSEC(Information Technology Security Evaluation Criteria), 국제표준(ISO/IEC 15408)으로 제정된 CC(Common Criteria for Information Technology Security Evaluation)의 보안기능 요구사항을 비교, 분석하고, 국내에서 개발된 침입차단시스템과 침입탐지시스템 평가기준, 현재 개발 중인 사용자인증용 스마트카드 평가기준의 보안기능 요구사항을 소개한다.

Ⅰ. 서 론

정보통신 기술의 발달로 정보시스템 사용이 급속도로 증가되고 있다.

이러한 정보통신 기술의 발달과 급속한 정보화는 곧 정보유출, 파괴, 위·변조, 바이러스, 서비스 방해, 불건전 정보 유통, 해킹 등의 컴퓨터 범죄 및 정보화 역기능이 날로 확산되어가고 있다. 체계적인 총체적 정보보호 대책은 이러한 정보화 역기능으로부터 정보시스템과 통신망을 보호하고 안전한 운영을 가능하게 한다.

따라서, 정보보호 기술을 일반 사용자가 신뢰하며 안전하게 사용할 수 있도록 보증하는 정보보호시스템 보안기능의 신뢰도에 대한 평가는 그 중요성이 날로 증대하고 있다.[2]

본고에서는 미국의 TCSEC(Trusted Computer System Evaluation Criteria)과 유럽의 ITSEC (Information Technology Security Evaluation Criteria), 국제표준(ISO/IEC 15408)으로 제정된 CC (Common Criteria)의 보안기능 요구사항을 비교, 분석하고, 국내에서 개발된 침입차단시스템과 침입탐지시스템 평가기준, 현재 개발 중인 사용자인증용 스마트카드 평가기준의 보안기능 요구사항을 고찰하고자 한다.

Ⅱ. 국외 정보보호시스템 평가기준의 요구사항

1. TCSEC 보안기능 요구사항

미국은 1983년에 오렌지 북으로 불리는 안전한 컴퓨터 시스템 평가 기준인 TCSEC 초안을 제정하고, 이에 대한 약간의 수정을 가한 후 1985년에 미국방성의 표준(DoD STD 5200.28)으로 채택하였다. 미국방성은 안전성 및 신뢰성이 입증된 컴퓨터 시스템을 국방 기관 및 정부 기관에 보급하기 위하여 TCSEC을 6가지 등급(C1, C2, B1, B2, B3, A1)으로 분류하고 각 기관별 특성에 맞는 컴퓨터 시스템을 도입 운영하도록 권고하고 있다.

TCSEC의 기본적인 보안요구사항은 다음과 같다.[10]

1.1 보안정책

- 요구조건 1 : 보안 정책(Security Policy)
  - 시스템에 의해 실행되는 명확하고 잘 정의된 보안 정책이 존재하여야 함
  - 식별된 주체와 객체가 주어지면 주체가 특정 객체에 대한 접근 취득을 허가 받을 수 있는지를 결정하기 위해 시스템이 사용하는 몇 개의 규칙들의 집합이 있어야 함

* 한국정보보호센터 평가기준팀 (gmcho@kisa.or.kr, galatici@kisa.or.kr, kglee@kisa.or.kr)

· 대상 컴퓨터 시스템은 비밀, 즉 분류된 정보의 처리를 위한 접근 규칙을 효과적으로 구현할 수 있는 강제적 보안정책을 실행, 이러한 규칙들은 정당한 개인 비밀인가를 갖지 않은 어떤 사람도 분류된 정보에 접근을 취득할 수 없고 임의적 보안 통제는 선택된 사용자나 사용자의 그룹들만이 자료에 대한 접근을 취득할 수 있도록 하는 요구사항을 포함

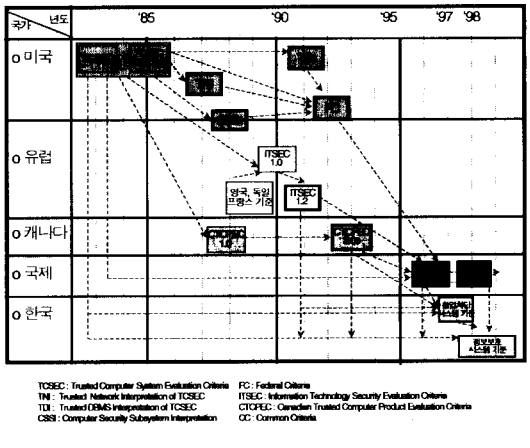


그림 1. 국가별 평가기준 개발 연혁

- 요구조건 2 : 표식(Marking)
  · 접근통제 레이블이 관련된 객체가 있어야 함
  · 강제적 보안 정책 규칙들에 따라 컴퓨터에 저장된 정보에 대한 접근을 통제하기 위해 모든 객체에 대해 그 객체의 보안 등급을 신뢰성 있게 식별하는 레이블을 표시할 수 있어야 하며, 접근 모드가 그 객체를 접근할 수 있는 주체들과 합당해야 함

1.2 책임성

- 요구조건 3 : 신분확인(Identification)
  · 각 주체들은 식별되어야 함
  · 정보에 대한 각 접근은 누가 정보에 접근하고, 어떤 부류의 정보가 허가되는가에 기초하여 허용되어야 함
  · 이 신분확인과 허가에 관련된 정보는 컴퓨터 시스템에 의해 안전하게 유지되어야 하며 시스템 내에서 보안 관련 행위를 수행하는 모든 작동중인 요소들과 관련되어야 함
- 요구조건 4 : 책임성(Accountability)
  · 감사자료는 보안에 영향을 주는 행위가 책임질 수 있는 측까지 추적될 수 있도록 선별적으로 유지되고 보호되어야 함
  · 보안 시스템은 감사 기록 내에 보안 관련 사건들의 발생을 기록할 수 있어야 함
  · 기록되기 위한 감사사건을 잘 선택하는 능력은 감사에 드는 비용을 최소화하며, 효율적인 분석을 가능케 함
  · 감사자료는 수정과 허가되지 않은 삭제로부터 보호되어야 하며, 이는 보안 위반의 감지와 사후 조사를 가능케 함

TCSEC에서는 안전한 컴퓨터 시스템이 지녀야 하는 기능을 보안 정책, 보안 정책을 지원하는 책임성(Accountability), 그리고 보증 및 문서 부분으로 나누어서 각 등급별로 요구사항을 정의해 놓고 있다. 각각의 요구사항은 다음과 같다.

- 임의적 접근통제 : 주체의 신분을 기반으로 하는 접근통제이다.
- 객체 재사용 : 시스템 저장 영역 내에 남아 있는 데이터가 없도록 모든 저장 영역을 우선적으로 재 할당한다.
- 레이블 : 비밀 등급을 표현한다.
- 레이블 무결성 : 비밀 레이블은 주체 및 객체의 비밀 등급과 정확하게 부합되어야 한다.
- 레이블 부착 정보의 전송 : TCB(Trusted Computing Base)[1]와 통신 채널 혹은 TCB와 장치 사이의 정보 교환은 TCB가 다중 등급과 단일 등급장치를 구분하여 허용한다. TCB는 보안 정책의 시행을 책임지는 하드웨어, 펌웨어, 소프트웨어 및 이들의 조합을 포함하는 컴퓨터 시스템 내의 모든 보호 메커니즘을 의미한다.
- 다단계 보안 장치로의 전송 : TCB는 객체의 비밀 등급이 허용된 범위 내인지를 확인한 후 객체와 비밀 등급을 함께 전송한다.
- 단일 등급 보안 장치로의 전송 : 객체만 전송한 다.
- 판독 가능한 출력물에 대한 레이블 : 출력물에 객체의 비밀 등급을 표현한다.
- 강제적 접근통제 : 비밀 등급의 비교에 의한 접근 통제이다.
- 주체의 보안 레이블 : TCB는 단말 사용자의 "현

1) TCB(Trusted Computing Base) : 신뢰받는 컴퓨팅 기반

표 1. TCSEC의 등급별 요구사항 요약

요구사항	C1	C2	B1	B2	B3	A1	기능
임의적 접근통제							보안정책
객체 재사용							
레이블							
레이블 무결성							
레이블 부착 정보의 전송							
다단계 보안 장치로의 전송							
단일 등급 보안 장치로의 전송							
판독 가능한 출력물에 대한 레이블							
강제적 접근통제							
주체의 보안레이블							
장치 레이블							
신분 확인							책임성
감사 추적							
안전한 경로							

: 본 등급에서 추가적인 요구사항은 없다.
: 본 등급에 대하여 새로운 혹은 개선된 요구 사항이 존재한다.
: 본 등급에 대하여 요구사항이 존재하지 않는다.

재 비밀 등급"의 변화를 유지한다.

- 장치 레이블 : TCB는 물리적으로 접속된 장치에 지정된 최고 및 최저 비밀 등급을 유지한다.
- 신분 확인 : 사용자의 신분을 식별하고 인증한다.
- 감사 추적 : TCB는 모든 보안 관련 사건의 기록을 TCB 보호 영역에 유지하여야 한다
- 안전한 경로 : TCB는 사용자에게 TCB 자신을 식별하기 위한 수단을 제공하여야 한다.

2. ITSEC 보안기능 요구사항

ITSEC에서는 기본적으로 보안 기능에 대한 정의는 하고 있지 않으며, TCSEC과의 호환을 위한 F-C1, F-C2, F-B1, F-B2 및 F-B3등 다섯 가지와 독일의 ZSIEC의 보안 기능을 이용한 F-IN (무결성), F-AV(가용성), F-DI(전송 데이터 무결성), F-DC(비밀성) 및 F-DX(전송 데이터 비밀성)등 총 10가지의 보안 기능을 제공하고 있다.[10]

- ITSEC의 기능은 크게 3개의 기능으로 구분할 수 있다.
  - 보안목적 - 보안기능이 필요한 이유
  - 보안기능 - 실제 제공되는 보안기능 내용
  - 보안매커니즘 - 보안기능이 제공되는 방법

- 식별 및 인증(Identification and authentication)
  - 요청한 사용자의 신분을 설정하고 신분확인을 요청한 사용자에 대하여 이를 식별하여 검증하는 기능
  - TOE[2]는 식별 및 인증을 위해 사용자가 제공한 신분확인 관련 정보를 유지
  - 식별 및 인증 데이터의 추가, 삭제, 변경 등을 할 수 있어야 함

- 접근통제(Access control)
  - 접근을 허가받지 못하거나 접근할 필요가 없는 사용자나 프로세스가 정보나 자원에 대한 접근 허가를 얻는 것을 막기 위한 요구사항
  - 더불어 허가받지 않은 자원의 생성, 갱신, 삭제도 막을 수 있도록 하여야 함
  - 접근통제 기능은 정보흐름에 대한 통제를 수행하여야 하며 사용자, 프로세스 및 객체가 정보를 사용하는 것에 대해서도 통제하여야 함
  - 객체에 대한 접근권한의 전파(propagation) 통제 및 데이터의 조각모음으로 인한 추론 통제 등의 기능도 포함

- 책임성(Accountability)
  - 보안 관련된 권한을 사용하는 경우 이를 기록하는 기능
  - 사용자 및 프로세스의 행동을 기록하여 이들 행동 결과로 문제가 발생하는 경우 책임소재를 가릴 수 있는 연결고리를 유지하는 것
  - 정보에 대한 수집, 보호 및 분석 기능을 수행하여야하고 다른 보안기능에서는 책임성의 요구사항을 만족하여야 함

- 감사(Audit)
  - TOE는 일상사건 및 예외사건에 대한 정보를

2) TOE(Target of Evaluation) : 평가대상이 되는 정보보호시스템과 이에 연관된 관리자설명서 및 사용자설명서

기록하고 있어야 함
- 후에 보안위반 사건이 실제로 발생하였는지 판단하고 이로 인해 정보나 다른 자원의 손해정도를 알아내기 위한 기초자료로 이용
- 감사기능은 감사정보에 대한 수집, 보호 및 분석 기능을 포함하여야 하며 이러한 분석을 통하여 보안위반 사건이 실제로 일어나기 전에 위반 잠재성을 탐지하여 사전에 알려줄 수 있도록 함

● 객체재사용(Object Reuse)
- TOE는 보호대상인 주기억장치나 디스크 저장장소와 같은 자원들이 재 사용할 수 있도록 보장
- 객체재사용 기능에서는 데이터 재사용을 위한 통제기능까지 포함하고 있으며 이를 위해서 데이터의 초기화, 릴리즈, 재 할당의 기능을 수행

● 정확성(Accuracy)
- TOE는 서로 다른 데이터 조각사이의 특정관계가 정확하게 유지되어야 하고 프로세스간에 데이터가 이동되는 경우 변경이 되지 않음을 보장
- 데이터가 비 인가된 방법에 의해 수정될 수 없도록 하여야 하며 연관된 데이터 사이의 관계를 정확 하에 결정, 설정 및 유지할 수 있는 기능이 제공되어야 함

● 서비스에 대한 신뢰성(Reliability of Service)
- TOE는 시간이 중요한 요소로 작용하는 작업(Task)에 대해서는 정확한 시기에 수행되도록 보장하여야 하며 자원에 대한 접근이 요청 될 때만 이에 대한 접근이 가능하도록 함
- 오류 검출 및 오류 복구 기능까지 제공하여서 서비스에 대한 중단이나 손실을 최소화하도록 하여야 하며 외부사건과 이에 대한 결과를 시간내에 응답 할 수 있도록 스케줄링을 할 수 있어야 함

● 데이터 교환(Data Exchange)
- 통신채널을 통하여 데이터가 전송되는 동안 이 데이터에 대한 보안기능을 제공
- 이러한 기능을 제공하기 위해서는 인증, 접근통제, 데이터 비밀성, 데이터 무결성, 부인방지 등 의 보안서비스가 뒷받침되어야 함

3. 국제공통평가기준(CC) 보안기능 요구사항

CC는 정보보호시스템의 보안기능 요구사항과 이를 평가하는 동안 적용하는 보증요구사항에 대한 공통의 집합을 정하여 서로 독립적으로 수행한 평가결과들을 호환할 수 있도록 하기 위한 것이다. CC는 크게 3부분으로 구성되어 있는데 제 1부에서는 소개 및 일반 모델을 제시하고 있으며 제 2부는 보안기능 요구사항, 제 3부는 보증 요구사항을 기술하고 있으며 제 2부의 부록에서는 보안기능 요구사항에 대한 부연 설명을 기술하고 있다. CC의 핵심은 제 2부와 제 3부로 정보보호시스템이 제공해야 하는 보안기능 및 보증 요구사항을 기술하고 있으며, 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발할 수 있다.[2]

● 감사(FAU : Security Audit)
- 보안감사 클래스는 보안활동에 관련되는 정보를 인식, 기록, 저장 및 분석할 수 있도록 FAU_ARP(Security Audit Automatic Response),FAU_GEN(Security Audit Data Generation), FAU_SAA(Security Audit Analysis), FAU_SAR(Security Audit Review), FAU_SEL (Secuirty Audit Event Selection), FAU_STG(Security Audit Event Storage) 6개의 패밀리로 구성
- 이들 패밀리에서 정의되고 있는 요구사항들은 보안관련사건 발생시 감사대상사건에 부합하는 시스템 활동을 감사레코드에 기록 저장하여 관리자나 인가된 사용자가 필요시에 감사관련 자료들을 검토할 수 있게 함

● 암호(Cryptographic Support : FCS)
- TSF가 암호기능을 지원할 경우 FCS클래스의 요구사항이 포함되어야 함
- FCS는 암호키관리에 대한 요구사항을 정의하며 FCS_CKM(Cryptographic Key Management), FCS_COP(Cryptographic Operation)의 패밀리로 구성

● 통신(Communication : FCO)
- 통신클래스는 데이터교환시 송수신자의 신원을 보증 및 확인할 수 있는 요구사항을 정의하는

두 개의 패밀리, 즉 FCO_NRR(Non-Repudiation of Receipt), FCO_NRO(Non-Repudiation of Orign)가 있음

- 사용자데이터 보호(User Data Protection : FDP)
  - 사용자데이터를 보호하기 위해 요구되는 컴포넌트들로 패밀리를 구성
  - 사용자데이터가 유입, 유출 및 저장되는 동안 이와 직접적으로 관련되는 보안속성을 다루는 패밀리들로 구성

- 식별 및 인증(Identification and Authentication : FIA)
  - FIA클래스는 사용자의 신원확인을 요청할 경우를 위하여 사용자의 신분을 설정하고 이를 검증할 수 있도록 요구사항들을 제공
  - 또한, 사용자가 가지는 권한이 TOE와의 상호작용을 허용하는 것인지를 판단하기 위하여 인가된 사용자의 명확한 신분을 보증하고 보안속성과 사용자간의 정확한 연결을 보증하도록 해줌

- 보안관리(Security Management : FMT)
  - 이 클래스는 3가지 관점에서 관리를 정의하고 있는데 TSF 기능에 관한 관리, TSF 데이터 관리, 보안속성의 관리로 나누어 컴포넌트를 설명
  - TSF 기능 관리에서는 기능자체의 활동상태에 관한 관리를 다루며, 보안속성 관리는 TOE의 자원에 대한 접근시 이에 관련되는 보안속성에 관한 관리와 더불어 보안속성의 제한을 정의하는 컴포넌트에서는 보안속성의 유효기간에 대해 설명
  - 마지막으로 TSF 데이터 관리는 보안속성을 제외한 TSF가 다루는 데이터에 관한 관리를 정의

- 비밀성(Privacy : FPR)
  - 비밀요구사항은 다른 사용자가 인가된 사용자의 ID를 도용하는 것을 막도록 요구사항을 정의
  - 이 클래스의 패밀리는 익명성, 가명성 (pseudonymity), 연결불가성(unlinkability) 및 관찰불가성(unobservability)를 중점적으로 다루고 있음

- 안전한 보안기능 보호(Protection of the Trusted Functions : FPT)
  - FDP는 사용자데이터 보호를 위한 클래스이지만 FPT클래스는 보안기능에 관련된 데이터를 보호하기 위한 요구사항들로 이루어짐
  - TSFs(TOE security functions)을 실제 구현하는 메커니즘의 유지보수를 다루도록 컴포넌트를 정의하며 TSF를 위해 사용되는 데이터에 대한 무결성과 관련하여 컴포넌트를 정의

- 자원활용(Resource Utilization : FRU)
  - FRU 클래스는 TOE 자원의 가용성 즉, 처리능력과 저장 용량 등의 가용성을 지원하기 위한 패밀리들을 가지고 있고 이들 패밀리들은 고장내인성, 서비스 우선순위, 자원할당의 관점으로 구성

- TOE 접근 (TOE Access : FTA)
  - 원격지에 있는 사용자가 TOE를 이용할 경우 TOE로 접근하기 위하여 세션을 설정하여야 하는데 이 과정에서 요구되는 신분확인과 인증을 위한 요구사항을 서술
  - TOE 접근 클래스에서 정의되는 요구사항은 사용자 세션수와 세션의 범위를 제한하고 접근내역과 접근 매개변수의 수정내역을 화면으로 출력할 수 있도록 하는 것

- 안전한 경로/채널(Trusted Paths/Channels : FTP)
  - 이 클래스는 사용자-TSF, TSF-TSF간의 안전 한 통신을 보장하기 위해 통신경로에 대한 요구사항을 가짐
  - 안전한 채널에 의한 경로는 안전한 경로를 이루게 하며 이 경로로 TSF간 통신의 안전성을 보장
  - 사용자는 TSF와 직접적으로 상호작용을 하여 보안기능을 수행
  - FTP 클래스에서 정의되는 컴포넌트들로 안전하지 않은 응용계층에 의한 수정을 막는지 보증할 수 있어야 함

Ⅲ. 국내 정보보호시스템 평가기준의 요구사항

1. 침입차단시스템 평가기준 보안기능 요구사항

보안기능 요구사항은 신분확인, 접근통제, 무결

성, 비밀성, 감사기록 및 추적, 보안관리의 여섯 가지 요구사항으로 이루어진다.[5]

- 신분확인 : 침입차단시스템을 이용하여 내, 외부의 자원에 접근하고자 하는 사용자 및 관리자의 신분을 식별하고 확인하는 기능으로 향후의 기술추세를 고려하여 상호인증에 대한 요구사항을 포함

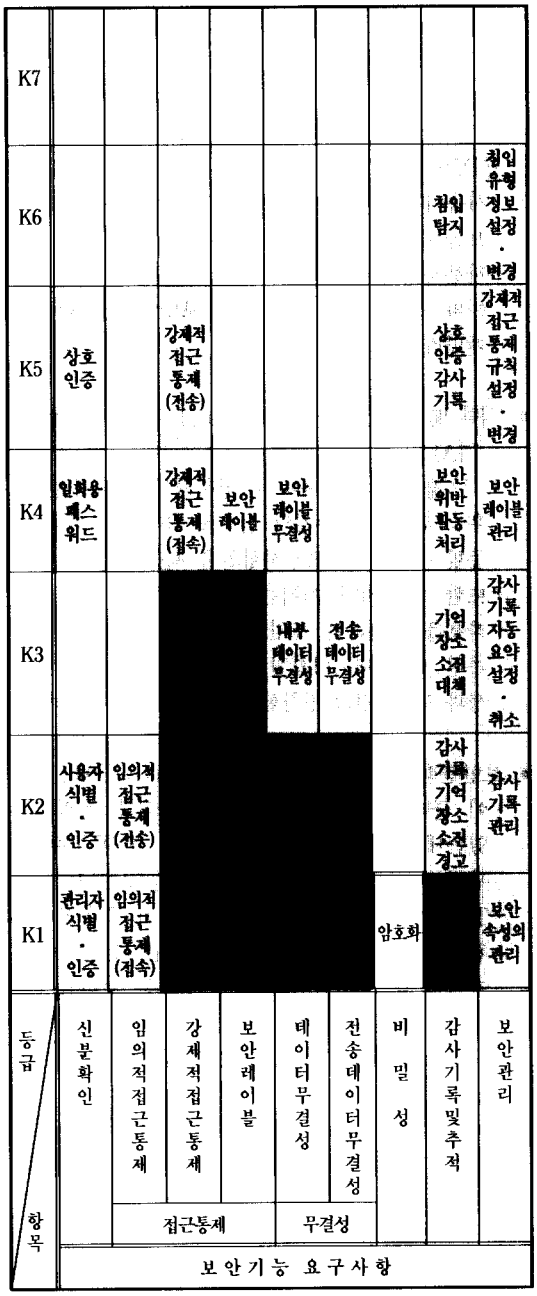
- 접근통제 : 접근통제 기능은 일정한 규칙에 따라 정보시스템 접속 및 사용범위를 통제하는 기능으로써 임의적 접근통제와 강제적 접근통제로 분류하여 등급이 높아질 수록 더욱 강력한 접근통제가 이루어지도록 함

- 무결성 : 무결성은 데이터에 대하여 부당한 변조가 발생하였을 시 이를 감지해내는 기능
  - 무결성 요구사항은 침입차단시스템이 가지고 있는 중요 내부 데이터에 대한 무결성과 침입차단시스템 사이에 전송되는 데이터에 대한 무결성 요구사항으로 나뉨

- 비밀성 : 비밀성이란 데이터가 불법적으로 노출되었을 경우 데이터의 내용이 비인가된자에게 알려지는 것을 방지하는 기능
  - 암호학적인 기법을 이용하여 전송되는 데이터를 암호화하고 정당한 사용자만이 복호화하여 데이터를 사용할 수 있는 기능
  - 우리나라의 경우 비밀성 기능은 사용자 조직에 따라서 사용되지 않을 수도 있으므로 이 기능의 제공은 개발자의 선택에 맡겨 모든 등급에서 이 기능을 제공하거나 제공하지 않을 수 있도록 함

- 감사기록 및 추적 : 해커 등과 같은 불법적인 사용자의 침입행위가 발생하였을 경우 추후 그 침입행위를 추적할 수 있는 기능을 제공하는 것이 감사기록 및 추적기능임
  - 사용자의 모든 행위를 기록하여 추후 문제점이 발생할 경우 감사기록을 근간으로 언제, 어디서, 누구에 의하여 침입행위가 발생하였는지를 추적할 수 있어야 하며 현재의 기술추세를 반영하여 침입으로 판단되는 행위가 발생하면 이를 감지하여 보고할 수 있는 기능을 요구

표 2. 침입차단시스템 평가기준 기능 요구사항



: 추가 요구사항 없음

: 추가 또는 확장된 요구사항

: 선택사항

: 요구사항 없음

● 보안관리 : 보안관리는 정보시스템의 보안관련 기능 및 데이터를 관리자가 안전하게 관리할 수 있도록 지원하는 기능으로써 ◦접근통제 규칙 설정, 변경, ◦감사기록 대상사건의 설정, 조회, 변경, 추가 및 삭제 ◦사용자 신분확인관련 데이터의 설정, 조회, 변경 및 삭제 등 등급별 요구되는 기능에 따라 안전한 관리기능을 요구

2. 침입탐지시스템 평가기준 보안기능 요구사항

● 축약감사데이터 생성

데이터를 수집하고 변환, 축약하는 기능은 일반적으로는 보안기능으로 분류되지 않지만, 침입탐지시스템에서는 가장 중요한 분석기능의 근거를 제공하기 때문에 보안기능으로 분류되어야 한다. 축약감사데이터 생성은 보안위반 분석을 위한 데이터 수집과 분석을 효율적으로 수행하기 위한 데이터의 축약 및 변환을 요구하고 있으며, 축약감사데이터에 기본적으로 포함되어야 하는 정보에 대한 요구사항도 포함하고 있다.

● 보안위반 분석

보안위반 분석 기능은 침입탐지시스템의 가장 핵심적인 부분이다. 시스템 보안영역에서 침입탐지시스템의 분석 및 탐지는 보안감사 분석을 담당하는 중요한 보안기능이다. 보안위반 분석부분은 다양한 방법이 이미 제공되고 있고, 새로운 방법에 대한 연구도 활발히 진행하고 있는 부분으로 객관적으로 분석방법을 비교할 수 있는 공인된 시범방법도 제시되고 있지 않기 때문에 특정 분석방법에 대한 요구를 명시하지는 않는다. 알려진 침입에 대한 기본적인 탐지방법을 K1등급에서 요구하고 있고, K5등급에서 알려지지 않은 침입에 대한 대응 기능을 요구하고 있다.

● 보안감사 대응

보안감사 대응은 침입을 탐지한 후 수행하는 기능에 대한 요구사항이다. 관리자에게 통보하는 기능과 침입관련 정보를 저장하는 기능을 K1등급에 1.서, 시스템 보호를 위한 대응행동 수행기능을 K3등급에서, 별도의 기능을 통한 침입관련 상세정보의 수집과 저장을 K4등급에서 요구하고 있다.

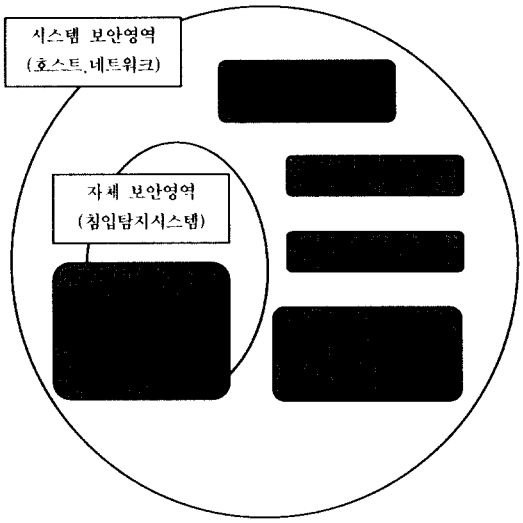


그림 2. 침입탐지시스템 보안영역과 보안기능의 관계

● 신분확인

신분확인은 침입탐지시스템 관리자를 식별하고 인증하는 기능이다. 침입탐지시스템에서는 일반 사용자에 대한 서비스는 제공되지 않으므로 사용자에 대한 신분확인은 요구되지 않는다. 관리자 ID와 호스트주소에 의한 식별 및 기본 인증기능(K1), 인증실패 관리기능(K2), 인증데이터 재사용 공격에 방지기능(K4), 상호인증(K5) 등이 등급별로 요구된다.

● 데이터 보호

데이터 보호는 시스템의 운영 과정에서 발생하는 시스템 관리 데이터에 대한 보호를 요구하는 항목으로 침입탐지시스템에서는 보안위반 분석을 위한 감사데이터, 침입을 탐지하였을 때 기록하는 침입관련 정보, 자체 운영을 기록한 자체 감사기록, 침입탐지시스템 실행파일 및 환경설정 파일등을 대상으로 무결성 기능(K3)이 요구된다. 네트 워크를 통해 관리데이터를 주고받아야 하는 다중 호스트 기반 시스템이나 네트워크 기반 시스템의 경우에는 전송데이터에 대한 무결성 기능(K3)과 비밀성 기능(K4)이 요구된다.

표 3. 침입탐지시스템 평가기준 등급별 보안기능 요구 사항

	축약 감사 데이터 생성	알려진 공격 탐지	관리자 통보 기반 정보 저장	식별 및 인증		감사 데이터 보호	보안 관리	
K7								
K6								
K5		알려지지 않은 공격 탐지		상호 인증				타임 스탬프 제공
K4			상세 정보 저장	재시도 공격 방지	전송 데이터 보호			
K3					데이터 무결성			안전한 경로
K2			대응 행동 수행	인증 실패 관리		감사 데이터 보호		
K1	축약 감사 데이터 생성	알려진 공격 탐지	관리자 통보 기반 정보 저장	식별 및 인증		감사 데이터 생성 및 검토	보안 관리	
	축약 감사 데이터 생성	보안 위반 분석	보안 감사 대응	식별 및 인증	데이터 보호	보안 감사	보안 관리	보안 기능 보호

: 본 등급에서 추가적인 요구사항은 없다.

: 본 등급에 대하여 새로운 혹은 개선된 요구사항이 존재한다.

: 본 등급에 대하여 요구사항이 존재하지 않는다.

- 보안감사
  보안감사는 일반적인 제품이나 시스템이 운영될 때 기본적으로 요구되는 보안기능으로 침입탐지시스템에서도 운영상에서 발생하는 모든 보안관련 사건들을 기록하도록 요구된다. 이러한 보안감사기록의 범위는 등급별로 요구되는 보안기능에 따라 구분하여 요구된다.

- 보안관리
  보안관리는 다른 보안기능이 요구되면 부가적으로 요구되는 기능으로 침입탐지시스템에서도 관리자에 의한 보안속성 설정이나, 다른 보안기능의 운영에 필요한 사항들이 요구된다. 보안관리 기능도 등급별로 요구되는 보안기능에 따라 구분하여 요구된다.

- 보안기능의 보호
  보안기능의 보호는 침입탐지시스템의 보안기능을 보호하기 위해 요구되는 것으로 원격지에서 관리자에 의한 시스템관리를 지원할 경우 안전한 경로 기능과 신뢰성 있는 시간과 일자에 대한 시점 확인 기능이 요구된다.

3. 사용자인증용 스마트카드 평가기준 보안기능 요구사항

사용자 인증용 스마트카드에 대한 보안기능 요구사항은 식별 및 인증, 사용자 데이터 보호, 암호기능, 보안관리, 보안기능의 보호, 안전한 채널의 6가지 사항으로 이루어진다.

- 식별 및 인증
  식별 및 인증에 대한 요구사항에서는 사용자의 신분을 증명하거나 스마트카드의 접근통제 정책을 적용하기 위한 식별자를 유지하는 식별, 카드 소지자와 스마트카드에 접근하는 외부실체에 대한 신분을 증명하는 사용자 인증, 사용자를 인증하기 위한 다양한 인증 메커니즘을 제공하는 인증방식, 스마트카드의 중요 자원을 보호하기 위해 접근조건에 따라 사용자를 다시 인증하는 재인증, 연속적인 인증시도 실패에 대한 횟수를 제한하는 인증 실패에 대한 요구사항으로 이루어진다.

- 사용자 데이터 보호
  사용자 데이터 보호에 대한 요구사항에서는 스마트카드에서 저장·처리되는 사용자의 데이터를 보호하기 위하여 주체의 스마트카드 내부 자원접근에 대해서 미리 정해진 접근통제규칙을 적용하여 접근을 통제하는 접근통제, 스마트카드에 할당한 객체가 논리적으로 삭제되는 경우에 이 객체의 데이터를 사용하지 못하도록 하는 삭제된 객체의 데이터 유출방지, 사용자 데이터의 무결성을 보장하기 위해 스마트카드의 동작을 취소하는 복귀, 스마트카드에 저장된 사용자 데이터에

대한 변경을 확인하는 저장된 데이터의 무결성, 스마트 카드와 외부실체 사이에서 전송되는 데이터에 변경이 발생한 경우에 이를 확인할 수 있는 전송데이터 무결성, 스마트카드와 외부실체 사이에서 전송되는 데이터가 인가되지 않은 사용자에게 노출되는 경우 그 내용이 알려지는 것을 방지하는 전송 데이터 비밀성에 대한 요구사항으로 이루어 진다.

- 암호기능
  암호기능에 대한 요구사항에서는 스마트카드의 보안기능에서 암호기능을 사용하는 경우 암호키에 대한 저장 및 속성을 관리하는 암호 키 관리, 스마트카드의 보안기능이 암호기능을 올바르게 사용할 수 있도록 검증된 암호 알고리즘을 수행하는 암호연산에 대한 요구사항으로 이루어진다.

- 보안관리
  보안관리에 대한 요구사항에서는 인가된 사용자가 스마트카드의 보안관련 데이터와 보안기능을 안전하게 유지하기 위하여 수행하는 기능에 대한 요구사항으로 이루어진다.

- 보안기능의 보호
  보안기능의 보호에 대한 요구사항에서는 스마트카드의 보안기능이 고장난 경우 이를 확인하고 스마트카드의 보안정책을 유지하는 고장안전, 스마트카드 보안 관련 중요 데이터에 변경이 발생하는 경우 이를 확인하는 보안기능 데이터 무결성, 스마트카드 보안 관련 중요 데이터가 인가되지 않은 사용자에게 노출되는 경우 그 내용이 알려지는 것을 방지하는 보안기능 데이터 비밀성, 스마트카드 내부 모듈사이로 전송되는 보안관련 중요 데이터를 보호하는 보안기능 데이터의 내부 전송 보호, 비인가된 물리적 접근으로부터 스마트 카드 보안기능의 안전성을 유지하는 물리적 보호, 고장으로 인한 스마트카드 운영중단이 발생할 경우 스마트카드의 안전한 초기상태로 돌아갈 수 있도록 하는 안전한 복구, 스마트카드 중요 자원에 대한 재사용 시도를 탐지하는 재사용 공격 탐지, 외부 간섭공격으로부터 스마트카드의 보안기능을 보호하는 보안영역 분리, 보안기능의 올바른동작을 보장하기 위하여 스마트카드의 보안기능 데이터에 대한 무결성을 확인하는 보안기능 자체 시험에 대한 요구사항으로 이루어진다.

표 4. 스마트카드 평가기준 등급별 보안기능 요구사항

	식별 및 인증	사용자 데이터 보호	암호기능	보안관리	보안 기능의 보호	안전한 채널
K7						
K6	영지식 증명					
K5	생체인증 다중인증			인증 메커니즘 관리		
K4		삭제된 데이터 유출 방지, 복구		응용 프로그램 관리	보안 기능 복귀	안전한 채널
K3	상호 인증 인증시 암호화 재인증	삭제된 데이터 유출방지 전송 데이터 무결성/ 비밀성	암호키 관리 암호연산	암호키 속성 설정 자체 실험 실행 조건 관리	고장안전 (일부) 보안기능 데이터 무결성/ 비밀성 복구 자체실험	
K2	실체인증				재사용 공격탐지	
K1	사용자 및 관리자 식별 및 인증	접근 통제		인증 데이터 관리 접근통제 관리	고장안전 (일부) 카드동작 중지 보안영역 분리	

: 본 등급에서 추가적인 요구사항은 없다.
: 본 등급에 대하여 새로운 혹은 개선된 요구사항이 존재한다.
: 본 등급에 대하여 요구사항이 존재하지 않는다.

- 안전한 채널
  안전한 채널에 대한 요구사항에서는 스마트카드

와 외부실체간에 안전하게 통신할 수 있는 채널을 개설할 수 있도록 하는 기능에 대한 요구사항으로 이루어진다.

Ⅳ. 결 론

앞에서 TCSEC(Trusted Computer System Evaluation Criteria)과 유럽의 ITSEC(Information Technology Security Evaluation Criteria), 국제표준(ISO/IEC 15408)으로 제정된 CC(Common Criteria for Information Technology Security Evaluation)의 보안기능 요구사항을 비교, 분석하고, 국내에서 개발된 침입차단시스템과 침입탐지시스템 평가기준, 현재 개발중인 사용자인증용 스마트카드 평가기준의 보안기능 요구사항을 살펴보았다.

현재의 국제적인 추세는 자국의 평가기준을 국제공통평가기준(CC)으로 통합하는 방향으로 가고 있으며, 국제공통평가기준(CC)은 TCSEC이나 국내 평가기준과 같이 하나의 정보보호 제품에 대한 보안기능 요구사항과 보증 요구사항이 정의되어 있는 것이 아니라 제품의 사용 목적 및 환경에 따른 다양한 기능에 필요한 요구사항을 분류하여 기준으로 제시하고 보증 요구사항에 따른 등급별 평가를 하고 있다.

참 고 문 헌

[1] 한국정보보호센터 "정보보호 평가기준 개발", *정보통신부 연구개발결과보고서*, 1999. 12.

[2] 한국정보보호센터 "정보보호시스템 국제공통평가방법 연구", *정보통신부 연구개발결과보고서*, 1999. 11.

[3] 한국정보보호센터 "정보보호시스템 평가기준(안) 및 평가지침서(안)", *정보통신부 연구개발결과보고서*, 1997. 12.

[4] "정보통신망 침입차단 시스템 평가기준", *한국정보보호센터*, 2000. 2.

[5] "정보통신망 침입탐지 시스템 평가기준", *한국정보보호센터*, 2000. 7.

[6] http://csrc.nist.gov

[7] http://www.itsec.gov.uk

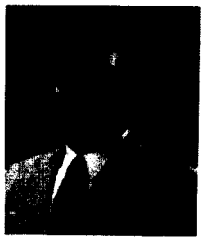
[8] http://www.bsi.bund.de

[9] http://www.kisa.or.kr/sysevaluation

[10] "국내,외 정보보호시스템 평가 가이드", *한국정보보호센터*, 1998. 11.

〈著者紹介〉

조 규 민(Gue-min Cho)
1993년 2월 : 서울대학교 자연과학대학 계산통계학과 졸업 (이학사)
2000년 2월~현재 : 동국대학교 국제정보대학원 정보보호학과 석사과정
1999년 8월~현재 : 한국정보보호센터 평가기준팀 연구원
〈관심분야〉 정보보호 및 네트워크 보안



황 영 석(Young-suk Hwang)
1999년 2월 : 한국방송대학교 컴퓨터공학과 졸업(학사)
1999년 2월~현재 : 동국대학교 국제정보대학원 정보보호학과 석사과정
2000년 4월~현재 : 한국정보보호센터 평가기준팀 연구원
〈관심분야〉 전자, 통신공학, 컴퓨터 및 네트워크 보안, 전자상거래 보안

이 경 구(Koung-goo Lee)
1975년~1982년 : 한양대학교 무기재료공학과 졸업(공학사)
1984년~1986년 5월 : University of central arkansas 전산학과 졸업(이학사)
1986년~1988년 5월 : University of arkansas 전산학과 졸업(이학석사)
1989년~1996년 5월 : Kent State University 전산학 졸업(이학박사)
1996년~현재 : 한국정보보호센터 평가기준팀 팀장
〈관심분야〉 정보보호, 시스템 성능분석, 네트워크 프로토콜