□ 기술해설 □

보안 제품 평가 기준 및 평가 제도의 현황과 추세†

한국과학기술원 차성덕*·김태호**·윤광식**
한국전산원 김홍근**

● 목 차 ●

1. 서 론

정보화 사회로 가는 피할 수 없는 거대한 흐름 속에서, "정보력은 국력"이라는 구호가 점점 현실로 나타나고, 따라서 정보화 사회에서의 피할 수 없는 문제로 보안의 중요성이 날로 더해 가고 있다. 이러한 추세는 앞으로도 더욱 빠른 속도로 진행될 것이 확실하다.

컴퓨터 보안(computer security)에도 여러 가지 측면이 있을 수 있겠으나, 보안성에 중점을 둔 소위 말하는 보안 제품(trusted products)의 개발 및 보안 성능 평가작업도 중요한 요소이다. 미국은 일찍부터 국방산업 또는 국방관련 정보처리에 있어서 보안의 중요성을 인식하고 이에 대한 연구를 시작하였다. 그리하여 83년에는 Trusted Computer System Evaluation Criteria(TCSEC) 즉 보안성 평가를 위한 국가기준을 마련하였고, 1985년에는 이를 개정하여 미 국방성 표준으로 채택하였다. 또한 미 국가 안전 보장국(National Security Agency, NSA)의 주관으로 미 국방성에서 비밀을 요구하는 정보처리의 보안성 향상을 위하여 보안성 평가제도인 Trusted Product Evaluation Program(TPEP)을 실시하여 오고 있다. 유럽 연합 및 카나다에서도 이와 유사한 보안성 평가의 필요를 인식하여, 자체의 평가 기준을 마련하여 각종 상용 보안 제품의 평가 및 인증 작업을 수행해 오고 있으며, 세계 표준화 작업도 또한 진행중이다. 본 글에서는 각국의 평가 기준과 평가 제도와 이에 관련된 기술 동향을 살펴보겠다.

2. 정보 시스템 보안 평가 기준

정보 시스템 보안성을 평가하는 기준을 만드는 목적은 다음과 같다.

- 보안 신뢰성을 측정할 수 있는 평가기준으로 사용되어 질 수 있다.
- 제작자가 보안제품을 개발하는 경우에 있어서 어떤 특성을 가져야 하는지 알려 준다.

† 본 연구는 한국전산원 위탁과제 연구 결과의 일부임.
*종신회원
**비 회 원

- 신뢰성 있는 시스템을 구매하려는 사람들에게 기준을 제공한다.

본 절에서는 각 국의 보안 평가 기준을 평가 기준 항목과 평가 등급의 관점에서 살펴보겠다.

2.1 TCSEC의 소개[1]

1960년대 말부터 미국에서는 정보 보호를 위한 조직을 만드는 등 많은 연구가 있었다. 80년대 초반 NCSC(National Computer Security Center)를 구성하여 83년에는 평가기준으로 TCSEC을 만들었는데, 이것은 이후 유럽 및 카나다의 보안 평가 기준을 마련하는데 기준으로 쓰여졌으며, 많은 보안 제품들이 이 기준에 의해서 평가되었다. 반면에 평가 등급이 고정되어 있기 때문에 융통성이 없어서 필요한 요구사항만 모아 만족시켜야 하는 경우, 이들을 적절히 선택 또는 조합할 수 없는 등 융통성이 거의 없다.

2.1.1 TCSEC의 평가기준 항목

TCSEC의 보안 요구사항은 보안 정책, accountability, 보장(assurance), 문서화(documentation)로 나눠 생각할 수 있다.

[보안 정책]

보안 정책은 정보를 보호하려는 조직을 위한 기본적인 요구사항을 포함하고 있다.

- DAC(Discretionary Access Control) : 소유자(subject) 또는 소유자가 속한 그룹을 기반으로 해서 object를 제한적으로 접근하게 하는 방법이다. 소유자는 자신과 자신이 속한 그룹에 대하여 접근 모드(읽기, 쓰기, 지우기 등)를 임의로 설정할 수 있다.
- MAC(Mandatory Access Control) : object에 포함된 sensitivity label과 그 정보에 접근하려는 자의 재량(clearance)에 따라서 object에 접근을 통제하는 방법이다. 즉 사용자는 단지 그가 접근할 수 있는 재량을 가진 정보에 한해서만 접근할 수 있다. sensitivity label에는 계층적인 분류(1급 비밀, 2급 비밀 등)와 종류에 의한 분류(군사문제, 원자력문제, 개인정보 등)의 분류가 있다.
- Label : 각각의 시스템의 자원(예를 들어 사용자, 기억장소 object, ROM등)과 관련된 sensitivity label은 자원의 보안 측면에서의 중요도를 나타내며, 이는 MAC에서 이용된다.
- Object 재사용 : 이전 사용자가 기억장소의 부분(disk sector, memory page등)에 남긴 정보를 다른 사용자가 접근할 수 없게 하기 위해서, 다른 사용자에게 할당하기 이전에 깨끗하게 지워야 한다.

[Accountability]

접근 제어를 위해 다음 기능을 제공해야 한다.

- I&A(Identification and Authentication) : identification은 사용자가 시스템이 인식하고 있는 사용자인지 아는 것이다. 이것은 사용자 이름, 사용자 ID등을 이용해서 구별된다. 그리고, authentication은 사용자가 시스템이 인식하고 있는 사용자라는 것을 검증하는 것이다. 여기에는 password가 가장 많이 사용된다.
- Audit : 보안에 관련된 사건(login, read 등의 화일 연산)의 발생을 함부로 수정될 수 없는 화일에 기록하게 한다. 이러한 정보들로 침입 시도와 시스템 보안 정책의 위반 시도를 분석한다.
- 신뢰성 있는 통로(Trusted path) : 터미널 앞에 있는 사람이 믿을 수 없는 것을 거치지 않고, 시스템과 직접 대화할 수 있는 방법이 제공 되야 한다. 이것이 사람과 시스템에 사이에 믿을 수 없는 소프트웨어에 의해서 모방되어질 수 없어야 한다.

[보 장]

보장을 위해서 만족되어야 하는 요구사항은 다음과 같다. 첫째, 괜찮은 공학적 방법을 이용하여 시스템이 만들어져야 한다. 둘째, 보안 정책, accountability의 보안특성과 통제가 잘못되지 않고, 올바르게 작동을 계속하는 것을 보여야 한다.

- 시스템 구조 : 시스템 개발 단계와 운영

단계에서 시스템 구조의 요구사항이 언급되야 한다. 개발 단계에서는 모듈화 설계, 계층화, 데이터 추상화, 정보 은닉(information hiding) 등이 행해져야 하고, 운영 단계에서는 사용자의 process와 신뢰도가 필요한 부분을 분리시켜야 한다.

- 시스템의 무결성 : 시스템의 하드웨어와 펌웨어가 올바른 작동을 해야 하고, 이것은 보통 소프트웨어로 주기적인 진단을 함으로써 만족되어 진다.
- 시스템의 시험 : 보안 특성을 전체적으로 충분히 시험했음이 보장되어야만 한다.
- 설계 요구사항과 검증 : 시스템 보안 정책에 맞는 시스템의 설계와 구현을 언급해야 한다. 시스템 보안 정책은 보안 원칙과 일관성을 가지고 쓰여지고, 증명되어야만 한다.
- Covert 채널 분석 : 다수 사용자 환경에서는 어떤 변수, 속성 혹은 object 정보 등이 MAC 정책을 위반한 채 언제나 일정하게 공유되어 지는데, 그것들이 covert 채널을 구성한다. 예를 들어 사용자는 일급 비밀 정보를 읽을 수 없다 하더라도 일급 비밀 정보 화일이 존재하는지, 언제 만들어 졌는지 등을 알 수 있다. 따라서 이 채널의 전송률을 낮추고, 이 채널을 감시할 수 있는 방법이 요구되어진다.
- 신뢰성에 관한 기능 관리 : 시스템의 운영 관리자와 보안 관리자의 역할을 분리하면, 정보누출의 범위와 가능성을 줄일 수 있다.
- 신뢰성 있는 복구 : failure나 crash로부터 시스템을 복구한 이후에 보안 기능의 작동이 올바르게 되어야 한다.
- 신뢰성 있는 분배 : 시스템의 하드웨어, 펌웨어, 소프트웨어가 제공자로부터 사용자로 전송되는 정보를 허가 받지 않고 고칠 수 없도록 해야 한다.
- 형상 관리(configuration management) : 개발과정중의 변화를 기록 관리하는 것이다.

[문서화]

문서를 만드는 것은 매우 어렵고 시간이 많이 걸리는 작업이기는 하지만, 평가를 위해서 꼭 필요한 작업이다.

- 사용자를 위한 보안 지침서 : 관리자가 아닌 일반 사용자를 위한 지침서이다. 이것에는 시스템 보안 기능에 관한 내용과 그것을 어떻게 이용하여 보안을 강화시킬 수 있는 지에 대하여 쓰여져 있다. 전형적으로 시스템으로의 login, 화일과 다른 정보의 보호. 다른 시스템에 있는 화일의 읽기와 쓰기, 시스템에서의 제약 등에 대해서 쓰여져 있다.
- 관리자를 위한 보안 지침서 : 시스템 관리자, 보안 관리자를 위해 쓰여진 문서이다. 이것은 시스템 보안을 위해, 보안을 강화하기 위해, 사용자의 요구에 맞추기 위해 또 최적화를 위해서 어떻게 하여야 하는 지를 나타낸 문서이다.
- 시험 문서 : 실제로 잘 작동되는지 시험해 봐야 한다. 이 문서는 어떤 방식으로 보안 기능이 시험되었는지(시험 계획, 환경에 대한 가정, 시험절차), 결과는 어떠한지를 나타내야 한다.
- 설계 문서 : 이것의 주된 개념은 시스템의 내부를 문서화한 것이다. 주된 목적은 개발자의 보안 철학은 어떠한데. 이것이 어떻게 구현이 되었다는 것을 나타내는 것이고, 주된 목표는 평가자에게 시스템이 평가기준을 만족한다는 것을 판단할 수 있게 해주고, 개발자에게 시스템이 어떤 보안정책을 정의했고 잘 구현되었는가 하는 것을 알려준다.

2.1.2 TCSEC의 평가 등급

TCSEC는 앞 절의 요구사항을 근거로 해서 등급을 계층적(D, C, B, A)으로 구성하고 있다. 각각의 계층은 하나이상의 세부 계층으로 구성되어 있다. 즉. D(최소한의 보호; minimal protection), C(재량에 의한 보호; discretionary protection), B(강제적인 보호; mandatory protection), A(검증된 보호; verified protection)로 나눠지고, C등급은 C1(재량에

의한 보안 보호; discretionary security protection), C2(통제된 접근 보호; controlled access protection)로, B등급은 B1(라벨을 이용한 보안 보호; labeled security protection)과 B2(구조화된 보호; structured protection), B3(보호 영역;security domain)로, A등급은 A1(검증된 설계; verified design)으로 나뉘어 진다. 보통 D, C1, C2, B1 등급은 낮은 보장 시스템이고, B2,B3,A1 등급은 높은 등급의 보장 시스템으로 분류한다. 그림 1에서 알 수 있듯이 상위 등급은 하위 등급의 요구사항을 모두 포함해야 한다.

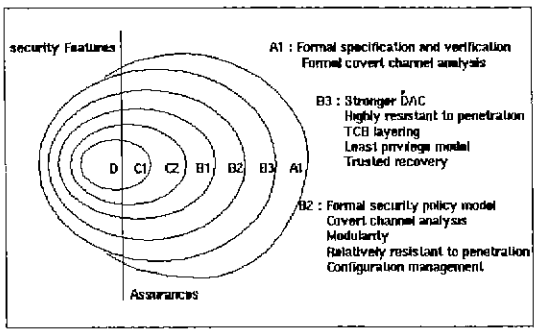


그림 1 TCSEC의 평가 등급

2.2 ITSEC의 소개[2]

ITSEC이전에도 TCSEC뿐만 아니라 유럽 각국에도 여러 가지 기준들이 존재하고 있었다. 그러나 이것들을 통합하려는 움직임이 생겨서 프랑스, 영국, 네덜란드, 독일이 모여 유럽 각국의 기준뿐만 아니라 미국의 TCSEC의 내용을 모두 합하여 Information Technology Security Criteria(ITSEC)을 만들어 냈다. 이것은 비록 유럽에 한정된 것이지만, 국제적인 표준으로서는 최초의 것이었다.

ITSEC 또한 TCSEC의 영향을 받아 만들어 졌으므로 중복되는 내용이 많이 존재한다. 그러나, ITSEC의 특징 중 하나는 각 등급에 전체 요구사항을 일률적으로 적용하는 TCSEC과는 달리 필요한 기능에 대해서 다양한 종류의 평가 등급을 만들었다는 것이다.

또한, 새로 필요한 기능을 정의하는 것이 용이하다. 이는 ITSEC 자체에서도 어떤 구체적인 한계를 명확히 만들지 않고, 기능에 의한 기준에서는 정의 정도만을 내리고 있고(간혹 예를 드는 경우도 있다), 보장, 효과에 의한 기준에서는 도입, 설명과 접근방법, 시스템과 제품, 몇 가지 기준, 평가자의 행동, 만들었어야 되는 문서 정도만을 설명하고 있기 때문이다. 물론 보장 – 올바름 기준에서는 E1등급에서 E6등급까지 나눈 것은 TCSEC과 비슷하나 항목들을 살펴보면 매우 다른데, TCSEC은 어떤 조건을 만족시켜야 한다고 하는 것에 반하여, ITSEC은 각 단계에 나온 문서들이 어떤 특성(예를 들면 formal, informal등)을 만족시켜야 한다는 식으로 서술하고 있다. 이것의 예는 뒤 2.2.2절에 설명하였다.

2.2.1 ITSEC의 평가 기준 항목

평가 기준에 대해서는 기능에 의한 기준, 보장 – 효과에 의한 기준, 보장 – 올바름에 의한 기준으로 나뉘는데, 각각에 대해 간단히 설명하겠다.

[기능에 의한 기준]

- 시스템의 보안 정책과 product rationale : 보안 조직 안에서 보안이 필요한 정보를 포함한 재산을 어떻게 관리하고, 보호하고, 분배할 것인지를 규정한 '단체의 보안 정책', 보안 목적을 만족시키는 수단을 정의한 '시스템 보안 정책'. 정보의 처리와 자원의 이용을 규정한 '기술적인 보안 정책'이 있다. product rationale는 보안 제품이 보안 목적을 만족시키는데 도움을 줄 것인가를 결정하는 정보를 제공한다.
- 보안 강화 기능의 요구사항 : 보안 강화 기능은 명백하게 언급되거나 정의된 것을 이용해야 한다. 'I&A', '접근 제어(access control)', 'accountability', 'audit', 'object 재사용', 자료간의 관계가 유지되고 변경되지 않고 넘겨 줄 수 있어야 하는 '정확성(accuracy)', 시간 제약을 지키는 '서비스의 믿을 만함(reliability of service)', 통신을 통해 전송되는 동안 보안 요구사항을 만족시켜야 하는 '자료 교

환(data exchange)'이 있다.

[보장 – 효과(effectiveness)]

이것은 보안 강화 기능과 방법에 언급된 보안 목적을 실제로 만족시킬 수 있는지 평가한다. 이 부분의 문서의 내용은 항목에 대한 정의, 내용과 표현을 위한 요구사항, 평가자의 행동 순으로 정의되어 있다.

- 효과 평가 기준-구축 : 올바름을 평가하기 위한 문서와 다음 문서가 필요하다. 보안 기능이 보안에 위협을 잘 대처하는지를 분석하는 데 사용되는 '적합성 분석', 보안 기능과 방식이 서로 지원하면서, 통합적이고 효과적으로 잘 작동하는지를 분석하는 데 사용되는 '일치 분석', 보안 위협에도 얼마나 버텨낼 수 있는지를 보이는 데 사용되는 '강도 분석', 구축 중에 발견된 약점을 평가하는 데 사용되는 '약점 목록' 등이 필요하다.
- 효과 평가 기준-운영 : 이것 역시 올바름을 평가하기 위한 문서와 함께 '사용의 용이성', 운영 중에 발견된 약점을 평가하는 데 사용되는 '약점 목록' 등이 필요하다.

[보장 – 올바름(correctness)]

보안 강화 기능과 방법이 올바르게 구현되었는지 평가한다. 개발 공정 각 단계에서 나오는 문서들이 어떤 특성을 만족시켜야 한다는 식으로 기준이 만들어져 있다.

- 구축-개발 단계 : 보안 목표에 대한 내용을 기술하고, 평가를 위한 기준이 되는 '요구 분석', 보안 목표에 대한 정의와 설계를 내용으로 하는 '구조 설계', 설계를 향상시키고, 구현을 위한 기초를 마련하는 '세부 설계', 실제 제품을 구현하고, 각각의 부분과 전체가 시험된 것을 보이는 '구현'에 관한 문서가 필요하다.
- 구축-개발 환경 : 개발자에 의해서 이용된 방법, 절차, 표준에 대하여 쓰여 있다. '형상관리', '프로그래밍 언어와 컴파일러', '개발자 보안'등에 관한 문서가 있다.
- 운영-운영 문서 : 개발자와 사용자간의 의사소통 창구로, '사용자를 위한 보안 지침서'와 '관리자를 위한 보안 지침서'가 있다.
- 운영-운영 환경 : 보안성을 유지한 채 운반되어 install하는 것에 대한 '설치(delivery)와 설정(configuration)'에 관한 문서와 '운영 시작과 운영 중'에 보안을 유지하고 작동시켜야 하는 지에 대한 문서가 있다.

2.2.2 ITSEC의 평가 등급

[기능에 의한 등급]

기능에 의한 등급은 기능에 대한 요구사항을 여러 개 모아서 만들어지며, 몇 개의 예만을 draft형태로 정의하고 있다. 부록에 TCSEC과의 호환성을 유지하기 위한 등급을 정의하였고, 데이터 베이스에 적합하도록 무결성 요구사항을 높인 F-IN, 암호화 장치에 적합하도록 자료의 비밀 요구사항을 높인 F-DC, 중요한 정보를 보안이 되지 않는 통신망을 통해서 전송하는 경우에 적합하도록 교환되는 자료의 비밀과 무결성 요구사항을 높인 F-DX는 계층적이지 않은 등급을 구성한다. 물론 이외에도 얼마든지 등급을 만들 수 있다.

[보장 – 효과에 의한 등급]

효과에 의한 등급은 만든 사람에 의해서 제공된 문서와 올바름을 평가한 문서에 의해서 평가된다. 문서가 얼마나 엄격하게 만들어 졌는가에 기반으로 해서 약점 분석 결과를 기반으로 보장을 평가하게 된다.

[보장 – 올바름에 의한 등급]

위에서 언급했듯이 이 단계는 개발 및 운영 단계에서 나타나는 문서를 기반으로 해서 가장 낮은 등급인 E1부터 E6까지로 나뉘게 된다. 각각의 등급은 제공되어야 하는 문서의 종류와 내용, 형식이 다르다. 예를 들어 E4 등급의 경우 구축 – 요구분석에 있어서 시스템의 보안 목표, 기본이 되는 formal하게 지정된 보안 모델에 대한 정의와 참조, 보안 목표의 관점에서 모델의 informal한 설명, 시스템의 구조에 대한 semiformal한 기술, 세부적인 설계의 semi-

formal한 기술 등의 요구내용이 있다.

2.3 CTCPEC의 소개[3]

1988년 CSSC(Canadian System Security Center)를 구성하여 1989년에 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)를 만들었다. 그후 1993년에 version 3.0e의 개정 기준을 만들어 내었다. 이것의 특징으로는 기능에 관한 기준을 service별로 수준에 따라 나누고, 이것을 평가를 위하여 처음으로 사용하였다는 것이다. covert channel의 경우 4개의 등급으로 나누어지는데, CC-0는 현재 평가받고 있는 제품과 더 높은 등급을 받는 데 실패한 경우, CC-1은 최대 전송률 같은 covert 채널 분석을 한 경우, CC-2는 covert 채널을 audit할 수 있을 경우에 수여된다. 또한 CC-3은 covert 채널이 제거되었을 때 수여된다.

또한 TCSEC처럼 특정한 시스템에 한정되지 않고, 다양한 시스템에 적용할 수 있는 기준을 만들려고 했다. 따라서 기능과 보장 면에서 나눈 점, 각각에 대해 등급을 나눈 점 등에서 ITSEC의 형식을 많이 따랐다.그러나, 기능 면에서 세부적인 분류, 기준 등의 내용 면에서는 TCSEC과 거의 흡사하다.

2.3.1 CTCPEC의 평가 기준 항목

이것은 기능적인 측면과 보장의 측면으로 나누어져 있다. 기능은 보안 정책에 관한 내용들로 이루어져 있고, 보장은 보안 정책이 얼마나 잘 구현되었는가 하는 것을 나타내고 있다.

[기 능]

크게 '기밀성', 승인되지 않은 수정을 할 수 없게 하는 '무결성', '이용가능성', 'accountability'로 나뉘어 지고, 각각에 대해서 3-7개의 항목이 존재한다.

[보 장]

믿을 수 있는 정도에 대해 등급을 평가해야 한다. 이것은 구조, 개발환경(개발 과정, 형상관리), 증명(evidence)을 위한 문서, 운영 환경, 보안환경(사용자를 위한 보안 지침서, 관리자를 위한 보안 특성 지침서), 보안 시험으로 구성되어 있다. 이 문서를 근거로 해서 평가하며, 이 내용은 ITSEC과 유사하다.

2.3.2 CTCPEC의 평가 등급

기능에 관해서는 각각에 서비스에 대해서 몇 개의 계층으로 나눠있다. 분류의 일부를 보면 표 1과 같다.

이와 같은 방식으로 평가 기준항목 각각에 대해서 3-6등급으로 나누어져있다. 여기서 각각의 서비스에 등급을 정하는 방식은 이미 간단히 설명을 하였다. 각각의 서비스의 등급의 모임이 하나의 평가 등급을 형성하게 된다. 예를 들면 CC-2, CD-3, CM-1, IB-2, ID-2, IM-4, ...T-3 이런 식으로 하나의 등급을 만든다. 기능적 측면에서 각각의 서비스가 계층으로 나뉘어져 있기 때문에 여러 개의 서비스의 등급을 모아서 functional profile을 만들어서 하나의 기준으로 만들기도 한다.

표 1 CTCPEC 평가 등급의 일부

범 주	약 자	서 비 스 명	범 위
Confidential	CC	Covert Channel	CC-0~CC-3
	CD	Discretionary Confidential	CD-0~CD-4
	CM	Mandatory Confidential	CM-0~CM-4
	CR	Object Reuse	CR-0~CR-1
Assurance	T	Levels of Assurance	T-0~T-7

2.4 CC의 소개[4]

보안에 대한 중요성이 커지고 있는데 반해 세계 각국에서 사용되는 기준이 달라서 비용과 시간이 많이 소모되는 등 문제점이 발생되기 시작하였다. 이에 FC(Federal Criteria; 한때 TCSEC를 개정하려는 움직임이 있었으나 CC가 진행되면서 흡수되었다)를 포함한 TCSEC, CTCPEC, ITSEC등의 기준을 통합하여 하나의 기준으로 만들려는 움직임이 생겨서 나온 것이 CC(Common Criteria for Information Technology Security Evaluation)이다. CC도 CTCPEC처럼 하나의 서비스를 여러 개의 수준으로 나누고 그것을 모아서 profile을 구성하는 방식을 취하고 있다. 이것은 계층적인 구조를 가지게 되는데, 그림 2와 같이 구성되어진다. 즉, class는 family로, component로, element로 구성되는 데, 이 element 들을 모아서 functional package 또는 assurance level를 만들고, 이것을 모아서 protection profile을 구성한다. 이러한 protection profile을 구성하면 이걸 하나의 등급으로 삼을 수 있다. CTCPEC와 이런 점에서는 같은 장점을 가진다. 그러나, CTCPEC은 구조자체가 CC만큼 계층적이지 않다. 반면 CC는 중간 단계를 두어 활용도를 높였다. 따라서 다른 기준들에 비해 매우 융통성 있게 구성할 수 있다.

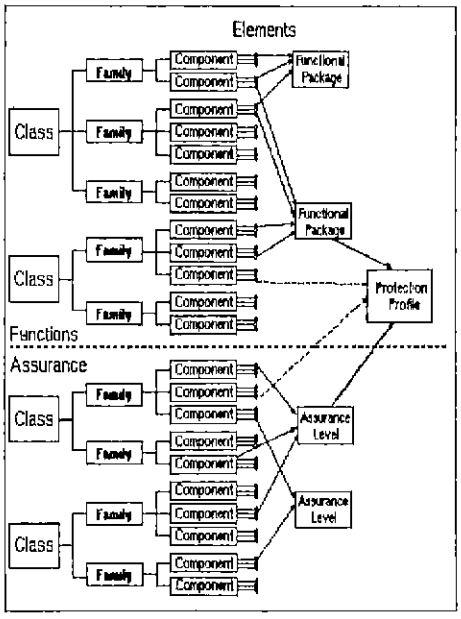


그림 2 CC 요구사항의 구조와 등급을 만드는 방법

2.4.1 CC의 평가 기준 항목

기능 요구사항으로는 I&A, 신뢰할 수 있는 통로, 보안 audit, 평가 대상 entry(사용자 session의 설정을 제어), 사용자 정보 보호, 자원 utilization, 신뢰할 수 있는 보안 기능의 보호, 개인 정보(privacy), 통신이 있다. 여기에 나열한 것은 각 class이다. 내용은 다른 평가방법과 크게 다르지 않다. 이 class의 실제 예로써 Class FIA(Identification과 Authentication)을 살펴보면, 그림 3과 같다.

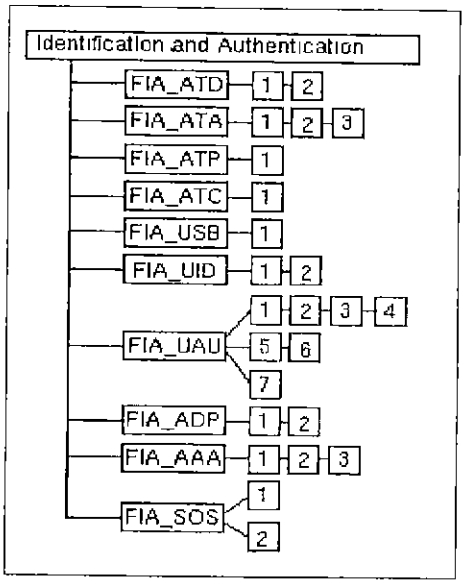


그림 3 CC의 FIA class 구조

여기서 FIA-ATD은 사용자 속성 정의이고, family이다. 이 family는 사용자의 identify로부터 구별되는 보안 속성의 집합이다. FIA-ATD.1은 최소한의 사용자 속성 정의이고, FTA-ATD.2는 FTA-ATD.1을 포함한 기초적인 사용자 속성 정의이다.

[보장 요구사항]

이것의 내용은 개발, 시험, 약점 평가, 형상관리, 생명 주기(life cycle) 지원, 안내 문서, 설치(delivery)와 운영으로 나누어져 있다.

2.4.2 CC의 평가 등급

위의 도입부에 설명했듯이 각각의 element를 모아 만들어진 functional package또는 assurance level(AL0-AL7)과 element를 모아서 하나의 protection profile을 구성하고 이것을 기준으로 평가한다.

2.5 세계의 추세

위에서도 언급되었듯이 정보 선진국들은 다들 자국의 기준을 가지고 있었다. 그러나 공통적인 기준을 만들려고 하고 있는데, 그 이유는 다음과 같다.

첫째, 다양한 나라들에서 이미 많은 경험들이 축적되어 있다. 따라서 다른 나라의 경험들을 공유함으로써 많은 이익을 얻을 수 있다.

둘째, 시스템을 구축하는 산업계에서는 다른 기준이 운영되는 것을 원하지 않는다. 왜냐하면, 기준이 다를 경우에는 각각의 기준에 따라서 여러 번 재 평가를 하여야 하기 때문에 돈과 시간이 많이 들게 되기 때문이다.

셋째, 보안의 특성상 기본 개념과 방법에 있어서 국가간의 차이가 있지 않기 때문에 국가만의 특정한 요구사항이 꼭 필요하다고 보여지지 않는다.

따라서 평가기준에 통합이 이루어지고 있는 것이다. 이것이 CC이다. CC는 94년 12월 draft version 0.9부터 시작하여 개정을 계속하여 현재 version 0.91까지 나와 있다. 이 기준은 금년 말쯤이면 어느 정도 틀을 다 갖추게 되고 그때부터 1년 반 내지 2년 간의 시험 운영을 거쳐서 확정이 될 것으로 예상되어진다. 따라서 CC가 확정될 때까지는 각국이 기존에 존재하는 평가 기준에 의해서 보안 제품을 평가하다가, 기존의 기준을 CC가 점진적으로 대체하게 될 것을 예상할 수 있다.

3. 정보시스템 보안성 평가 제도 및 절차 연구

지금까지 각국의 정보 시스템 보안성 평가 기준 연구의 현황을 대략적으로 살펴보았다. 각국의 정보 시스템 보안성 평가 기준은 그 자체로서도 중요하지만 그와 함께 모든 보안 제품의 평가 기준이 된다는 점에서도 매우 중요하다.

보안제품에 대한 평가기준을 보유하고 있는 미국, 캐나다, 유럽 중에서 캐나다는 평가 활동이 그다지 활발하지 못하며, 유럽의 평가활동은 그리 널리 알려져 있지 못하다. 반면에 미국의 평가 활동은 매우 활발한 편이며 많은 사실들이 알려져 있다. 따라서 이 장에서는 미국에서 실행중인 정보시스템 보안성 평가기준에 따른 평가제도의 개요와 앞으로의 변화방향을 살펴본다.

3.1 Trusted Product Evaluation Program

TPEP은 미국 NSA 산하의 NCSC에서 주관하는 프로그램으로써, 이 프로그램을 통하여 NCSC는 trusted operating systems등을 포함한 여러 보안제품을 평가한다. TPEP은 이전의 NCSC의 평가 프로그램이었던 Commercial Products Evaluation Program을 대체하는 것으로서, 다음과 같은 목적을 가지고 있다[5].

...(TPEP은) 상업적으로 생산되고, 지원되는 컴퓨터 시스템의 보안 성능의 기술적인 면들을 TCSEC에서 제시된 기준에 대하여 평가하는 것에 중점을 두고 있다.

3.2 TPEP의 과정

보안 시스템의 평가를 위해서는 vendor proposal이후에 다음의 4단계를 거치게 된다[6].

- Preliminary Technical Review(PTR)
- Vendor Assistance Phase(VAP)
- Design Analysis Phase(DAP)
- Formal Evaluation Phase(FEP)

이 외에도 일단 평가를 마쳐 등급을 부여받은 제품이 성능 향상, 오류 수정 등을 위해서 어떤 변화를 겪게 될 때, 같은 등급을 유지하기 위한 방법으로 Rating Maintenance Phase (RAMP)가 정해져 있다.

3.2.1 Preliminary Technical Review

PTR수행을 위해서 NCSC는 senior TPEP evaluator 2-3인으로 구성된 평가팀을 제품 생

산회사에 보내 약 2주정도에 걸쳐 회사측에서 제공한 기술적 문서들에 대한 검토를 실시하도록 한다. 이 검토의 결과로써 평가팀은 preliminary technical report(PTR)을 작성하게 된다. PTR은 제품의 high-level 구조가 얼마나 보안 관련 요구사항들을 만족시킬 수 있는가에 관한 점을 중점적으로 다루게 되며 이 보고서에서 내려진 평가에 따라 NCSC는 그 제품을 정식 평가 프로그램에 포함시킬 것인가를 결정한다. 이 단계는 제품 계획단계나 개발의 초기에 행해지는 것이 가장 바람직하다.

3.2.2 Vendor Assistance Phase

PTR에서 계속해서 평가를 하기로 결정이 된 제품은 VAP를 거치게 된다. 이 과정이 행해지는 동안 회사측은 제품에 대한 디자인과 구현을 수행하게 되며 NCSC측은 3-5명의 전문가 팀을 파견하여 design decision에 대한 조언과 평가를 하게 된다. 파견된 evaluation team은 실질적으로는 그 제품에 대한 TCSEC에 대한 해석을 제공하게 되며 평가에 필요한 high-level documentation에 대한 검토도 수행한다. 전문가 팀이 모든 필요한 문서들이 완성되었다고 판단을 내리면 TPEP의 다음 단계로 이행하게 된다. 이 단계는 대상 시스템의 디자인, 구현과 함께 이루어지는 것이 바람직하다.

3.2.3 Design Analysis Phase

DAP단계에서는 제품의 복잡도와 목적 등급에 따라 5-8명의 평가팀이 구성된다. 회사측에서는 이 팀원들에 대하여 제품의 내부 디자인과 구현에 대한 훈련을 제공하며 평가팀은 시스템의 이해를 위해 주어진 문서들을 재검토하게 된다. DAP를 거치면서 평가팀은 시스템의 보안 관련 요소에 대한 이해를 주요한 내용으로 하여 Initial Product Assessment Report (IPAR)를 작성하게 된다. IPAR에는 또 제품의 보안 관련 기능 설명 외에도, 평가대상 시스템이 어떻게 TCSEC에서 정의하고 있는 목적등급의 요구사항들을 만족할 수 있을 것인가에 평가팀의 판단도 포함된다.

이 단계에서는 평가대상의 다양성과 평가팀간의 차이 때문에 일관성의 유지가 중요한 문제가 되며 NCSC는 일관성을 제공하기 위해 컴퓨터 보안의 전문가들로 구성된 Technical Review Board(TRB)를 두고 있다. TRB는 평가팀이 작성한 IPAR을 검토하고 IPAR이 필요한 모든 보안 기능을 빠짐없이 분석하고 또 같은 TCSEC에 의거해 수행되는 다른 제품들에 대한 평가들과 일관성을 유지할 수 있도록 완전성(completeness)과 일관성(consistency)측면에 관해서 평가팀에게 조언을 한다. TRB의 검토와 조언이 이루어진 후 평가팀은 TRB에 의해 제기된 문제에 대한 해결책을 중심으로 TRB에게 briefing을 하게 된다.

TRB와 평가팀의 건의에 따라 NCSC는 평가대상을 정식 평가 과정에 받아들일 것인가여부를 결정하게 된다. 이 단계는 대상 시스템에 대한 알파테스트나 베타테스트가 행해지는 동안, 즉 디자인이 결정된 상태에서 이루어지는 것이 바람직하다.

3.2.4 Formal evaluation Phase

평가 대상이 FEP에 접어들게 되면 그 제품이 특정 등급을 위한 평가에 접어 들었다는 사실이 Product Bulletin(PB)를 통해 일반에게 알려지게 된다. 이 과정동안 평가팀은 DAP도중에 나타난 모든 질문들에 대한 해답을 찾게 되며 이 과정에서 발견된 내용들과 IPAR의 내용들이 Final Evaluation Report(FER)를 구성하게 된다.

먼저 평가팀은 테스트계획을 작성하게 된다. 이 테스트 계획은 크게 회사측에서 제공하고 평가팀에 의해 검증된 테스트, 팀에서 만든 테스트, 팀 penetration scenario로 구성된다. 이 테스트 계획은 TRB의 검토와 조언을 통해 수정, 보완된다. 평가팀은 TRB의 조언을 받아 완성된 테스트 계획을 실행에 옮기게 되며 테스트 결과를 기록하게 된다. 이 기간동안 발견된 보안 관련 결점들은 수정과 재 테스트과정을 거치게 된다.

모든 테스트의 결과는 그 효용성을 TRB에 의해 검증 받게 된다. 모든 테스트와 검증과정이 끝난 후 NCSC는 TRB와 평가팀의 제안에 따라 평가대상 시스템에 등급을 수여하게 된다. 평가가 끝난 시스템은 보안 관련 요소들에

대한 요약과 함께 Evaluated Products List (EPL)에 실리게 되며 FER도 일반에게 공개된다.

3.2.5 Rating Maintenance Phase(RAMP)

모든 다른 시스템과 마찬가지로 보안 관련 시스템들도 기능의 보완, 세부적인 사항의 수정 등을 거치게 된다. 하지만 TPEP를 통해 결정된 등급은 evaluated configuration으로 불리는 특정한 hardware에서 수행되는 특정한 software release에 대한 것이므로 어떤 시스템이 수정을 거치게 된다면, 등급을 유지하기 위한 재 평가가 필요하게 된다.

NCSC는 이러한 재평가에 따른 부담을 줄이기 위해 C1-B1등급 제품들에 대해 RAMP 프로그램을 제공한다. RAMP는 Configuration Management(CM), 회사측 스태프에 의한 보안요소 분석, 보안 요소 테스팅등에 중점을 두고 있다.

회사측은 기본 평가과정 중에 Rating Maintenance Plan을 제출하도록 요구되며 평가 대상 제품과 컴퓨터 보안에 관한 전문가를 지정하여 훈련시키도록 요구된다. NCSC는 강연, 독해물, 수업 등을 통해 회사측 전문가들을 보안 시스템 평가에 대해 훈련시킬 수 있는 프로그램을 제공한다. 회사측의 보안 분석 전문가들은 평가 대상 시스템에 발생한 변화를 검토하고 이 변화들이 보안 등급과 보안 관련 요소들에 미치는 영향에 대한 평가를 하며 이러한 변화에 대응하는 테스트 자료를 작성하고 수행한다. 그 결과는 TRB에서 검증을 받게 된다.

TRB에 대한 브리핑의 결과에 따라서, 변화된 시스템의 등급 유지 여부가 결정되며 이 과정에서 등급의 변화는 허용되지 않는다. 등급의 변화를 위해서는 TPEP과정 전체를 새로이 거쳐야만 한다.

3.3 TPEP의 지원

앞에서 살펴보았듯이 평가 과정 자체는 거의 대부분 사람에 의해서 이루어지고 또 긴 시간 동안 이루어지기 때문에 비용이 많이 드는 과정이다. 실제로 한 제품이 TPEP를 통해 인증을 받는데는 수년이 걸리기도 하였다. 또 DAP와 FEP과정동안에는 평가 자체의 효율성이 평가팀의 효율성에 전적으로 의존하기 때문에 평가팀의 효율적인 활동이 필수적이다.

이에 따라 NCSC에서는 평가팀의 효율을 높이고 여러 평가들 간에 서로간의 일관성을 유지하기 위해서 가이드 라인, 정보수집 도구, 자동화 도구, process-oriented 도구와 재도 등을 마련하였다,

- TCSEC는 독립적이고 일반적인 다중수행 데이터 프로세싱 시스템을 위하여 작성되었다. 하지만 TCSEC를 여러 다른 관련분야에 대해 새롭게 해석할 필요가 생겼고 이에 따라 NCSC는 가이드 라인들("rainbow series")를 발표하게 되었다. Trusted Network Interpretation과 Trusted DBMS Interpretation이 이러한 가이드 라인중 대표적인 것이다.
- 평가팀을 위해서 평가에 필요한 도구들과 도구들의 유용성, 평가 과정에 관한 평가자들의 관찰과 의견을 수집하기 위한 질문집과 제품의 보안 기능에 관계된 기술적인 사항들에 대한 질문집을 제공한다.
- 평가자들과 회사관계자들간의 의사소통을 도와주기 위해 DOCKMASTER를 제공한다. DOCKMASTER는 multics를 기반으로 한 B2 시스템으로 전자 우편, 게시판등의 기능을 제공한다. 각각의 평가 대상에 대해서는 평가자들이 이용할 수 있는 "팀 포럼"과 평가자, 회사관계자들 모두가 이용할 수 있는 "Vendor 포럼"이 제공되며 이 포럼을 통해 정보와 의견을 교환할 수 있다.
- 또 이와는 별도로 평가과정 전반에 걸친 일관성을 유지하기 위해 평가자들을 위한 3개의 포럼이 제공된다. 해석(Interpretation)포럼은 평가자들간에 특정한 TCSEC 요구사항에 관한 해석을 공유하고 그에 대한 타당성을 논하는데 이용되며, 결정(Decisions)포럼은 해석포럼에서 논의된 사항에 대한 결정을 공식화하는 포럼으로 평가과정 전반에 영향을 미치게 된다. 이 두 포럼이 주로 평가의 기술적인 사항들을 위한 포럼인 반면 Evaluation Issue

포럼은 평가 과정 자체에 대한 의견을 위한 포럼이다.

- 평가의 수준을 일정하게 유지하고 일관성을 보장하기 위해서 TRB를 제공한다. TRB는 컴퓨터 보안의 전문가들, 특히 senior TPEP evaluator들로 구성되어 있으며 IPAR, 테스트 계획, FER등을 검토하며 평가팀들은 TRB에게 평가의 중요 사항들에 대하여 브리핑을 하여야 한다. TRB는 이들에 대하여 조언과 비판을 하게 되며 이 조언과 비판을 통해 평가의 일관성, 완전함, 질등을 보장하게 된다.
- 해석의 일관성 유지와 각 평가팀들에게 특정 TCSEC항목에 대한 조언을 해주기 위해 Interpretation Working Group (IWG)가 존재한다. TRB를 구성하는 senior evaluator들이 주 구성원이다.
- B2이상의 시스템에 요구되는 정형적 검증, 정형적 모델링 대한 평가의 일관성을 위해서 정형적 방법론에 대한 전문가들로 구성된 Verification Working Group (VWG)을 구성하였으며 이 그룹의 도움을 받아 정형적 검증, 모델링에 이용될 때 유용성을 인정받을 수 있는 Endorsed Tools List(ETL)을 제공한다.
- 이 외에도 평가 도중에 작성하여야 하는 보고서들을 위한 LaTex 시스템과 마크로등을 제공하며 PTR, IPAR, FER에 관한 개요도 제공하며 evaluator들에게 지속적인 교육과 토론의 기회를 제공하기 위해 workshop을 1년에 한두차례 제공한다.

3.4 TPEP의 평가 및 개선 방향

앞에서 살펴보았듯이 TPEP과정은 많은 사람들이 함께 참여하고, 또 많은 시간이 걸리는 복잡한 과정이다. 보통 이렇게 복잡한 프로그램들은 모든 평가대상에 대해 공정하다는 평가를 받기가 어렵다. 그러나 TPEP은 기업의 이익에 좌우되는 상업적인 목적을 갖고 있지 않고 또 미국 정부의 자금으로 운영되기 때문에 공정한 평가제도라는 면에서는 좋은 평가를 받고 있다[7]. 또, TPEP를 효율적이고 일관성 있는 프로그램으로 만들기 위해 많은 사람들이 오랜 시간동안 노력한 결과 객관적이고 고신뢰도의 보안 분석을 행한다는 긍정적인 평가를 얻을 수 있었다.

하지만 다음에 설명할 여러가지 이유로 하여 문서에 대한 검토과정과 그에 따른 개정과정이 느려지는등 전체과정의 진행 자체가 느리다는 비판이 있다. 또 일부에서는 평가를 받은 제품들 자체가 그다지 유용하지 못하며, 그 제품들이 평가받은 configuration도 그다지 유용하지 못하다는 비판을 하기도 한다.

이러한 비판들에 대하여 NSA에서는 TPEP 과정을 좀더 효율적으로 운영하기 위하여 TPEP내부의 전문가들과 외부의 컴퓨터 보안 전문가들에게 개선 방향을 모색하도록 의뢰하였다. 외부와 내부의 TPEP에 대한 검토 결과로써 다음과 같은 사항들이 지적되었다[8].

- 평가를 위한 객관적인 기초가 없다. : 평가를 마쳤다고 결정내릴 수 있는 객관적인 기준이 없고, 평가기준에 대한 해석이 고정되어 있지 않기 때문에 평가과정이 자꾸 늦어진다.
- 산업체의 현실에 적합하지 못한 점들이 있다. : TPEP의 기준을 따라 평가를 수행하게 되면 평가의 주요활동들이 평가대상이 고정된 이후에 이루어 지게 된다. 하지만 이미 시스템이 완성되어 있기 때문에 사소한 부분에서의 변화라도 무척 힘들게 된다. 이런 점은 부분적으로 평가가 등급에 맞는가에 관해 이루어 지기 때문에 발생하는 문제로써 만약 시스템의 부분에 대한 평가로 등급이 세분화 될 수 있다면 마지막 단계에서의 수정이 개발과정 전체를 되풀이 하여야 하는 결과로 나타나지는 않을 것이다. 반면에 이러한 점은 개발자측에서 평가과정을 가볍게 생각하고 충분한 준비없이 평가를 받기 때문이라는 지적도 있다.
- TPEP자체의 integrity : CMW를 평가받고자 한 몇몇 특정 회사의 경우 다른 회사의 경우에는 요구되었던 사항들이 요구되지 않는등 평가팀들의 활동이 공평하지

못하다는 지적이 있었다.

이외에도 평가자들의 능력에 관한 문제, 개발자들의 준비 부족,평가를 완료하는 것에 대한 평가자들의 의지의 부족, 평가과정을 돕기 위한 도구들의 부족등이 지적되었으며 Trusted System자체에 대한 정부의 구매 부족에 따른 시장의 협소등도 문제로 지적 되었다.

이러한 문제점들을 해결하기 위해서는 먼저 TPEP에 참여하는 평가자들, 프로젝트 관리자들에 대한 매니저로서의 소양 교육, 평가기관원들의 역할에 대한 전문적인 지식의 배양, 평가 과정에 고위 관리자의 참석등의 적극적인 참여, 개발자들의 성실한 참여를 유도할 수 있는 방법등이 모색되어야 할 것으로 지적되었다[8].

4. 결 론

보안 기능 평가 기준에 관한 최근의 동향은 여러 독립된 평가 기준들간에 상호 호환성을 부여하고, 좀 더 유연한 평가를 가능하게 하는 Common Criteria에 관한 연구를 중심으로 이루어지고 있다. 비록 CC가 아직 draft상태이고 아직 어떠한 평가제도에 대한 언급은 없지만 앞으로 CC에 기반한, 여러 국가간에 상호 인정가능한 평가제도가 연구될 것이다. 이를 위하여 미국 NSA에서는 TPEP를 어떻게 CC에 적용할 수 있을까에 관한 연구를 95년부터 자체적으로 수행중에 있다.

이러한 경향은 우리나라에서 필요한 보안 시스템 평가 기준 및 평가 제도의 구축시에도 고려 되어야 할 것이며, 외국에 비해 보안 평가 제도에 대한 경험이 전무한 우리의 입장을 고려한다면 현재의 격차를 극복하고 또 Common Criteria및 이에 의거한 CC Evaluation Methodology에 대한 연구와 CCEB에의 참가를 포함한, 외국의 발전 사항들을 예의 주시하기 위한 노력이 시급한 실정이라 하겠다.

참고문헌

[1] Department of Defense standard, 'Department of Defense Trusted Computer System Evaluation Criteria", Dec. 1985.

[2] European Communities, 'Information Technology Security Evaluation Criteria ver 1.2", Jun. 1991.

[3] Canadian System Security Centre, 'The Canadian Trusted Computer Product Evaluation Criteria ver 3.0e", Jan. 1993.

[4] "Common Criteria for Information Technology Security Evaluation ver 0.9", Oct. 1994

[5] Deborah Russell, G. T. Gangemi Sr.,"Computer Security Basics", O'Reilly & Associates, Inc. Jul.1992.

[6] Santosh Chokhani, 'Trusted Products Evaluation", CACM Vol. 35, pp. 64-76 Jul. 1992.

[7] 차 성덕, "Trusted System 설계 및 평가 방법", NETSEC-KR'95 Jun. 1995.

[8] James P.Anderson Co., Clark Weissman Consulting, 'TPEP Process Review" May. 1994.

[9] 한국전산원 표준연구본부, "전산망 보안성 평가 기준에 관한 연구", Dec. 1993.

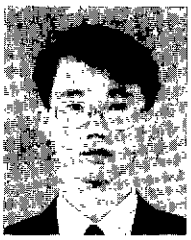
차 상 덕

1983 University of Calfornia at Irvine 전산학 학사
1986 University of Calfornia at Irvine 전산학 석사
1991 University of Calfornia at Irvine 전산학 박사
1990~1991 Hughes Aircraft Co. 연구원
1991~1994 The Aerospace Corp. 연구원
1994.9 ~ 현재 한국과학기술원 전산학과 조교수

김 태 호

1995 성균관 대학교 공과대학 정보공학과 학사
1995~현재 한국과학기술원 전산학과 석사과정
관심분야 : Software safety, Formal methods, Network security

윤 광 식



1995 한국과학기술원 전산학과 학사
1995~현재 한국과학기술원 전산학과 석사과정
관 심 분 야 : Safety - critical system, Formal methods, Parallel program testing과 debugging

김 홍 근

1981~1985 서울대학교 컴퓨터공학과 학사
1985~1987 서울대학교대학원 컴퓨터공학과 석사
1989~1994 서울대학교 대학원 컴퓨터공학과 박사
1994.5~현재 한국전산원 전산망보안실 선임연구원
관심분야 : 컴퓨터 보안, 암호알고리즘, 병렬처리

● 제13회 정보산업리뷰 심포지움 ●

- **주 제 : 국가 경쟁력 강화를 위한 정보산업의 역할**
- 일 자 : 1995년 12월 12일(화)
- 장 소 : KOEX 4층 대회의실
- 내 용 : 주제발표 및 질의 등
- 주 최 : 한국정보과학회
- 문 의 : 한국정보과학회 사무국
  T. 02-588-9246