# 네트워크 보안제품 평가기준(안) 연구

서정택°, 박종운, 이규호, 장준교, 이상하, 김동규
아주대학교 컴퓨터공학과

# Study on the Evaluation Criteria of Network Security Product

Jung-Taek Seo°, Jong-Woon Park, Kyu-Ho Lee, Jun-Kyo Jang, Sang-Ha Yi, Dong-Kyoo Kim
Department of Computer Engineering, Ajou University

요 약

오늘날 전세계를 하나로 잇는 정보화사회는 보다 신뢰성 있는 네트워크 보안제품을 요구하며 이들 제품을 객관적으로 평가하기 위한 평가기준을 필요로 한다. 따라서 본 논문에서는 국내 네트워크 보안제품 관련 평가기준(안) 제정을 위해 국제공통평가기준인 CC(Common Criteria)와 미국의 네트워크 보안제품 관련 평가기준인 TNI(Trusted Network Interpretation of TCSEC)를 비교/분석하여 필요한 보안기능 요구사항을 도출하여 향후 평가기준(안) 제정을 위한 방향성을 제시한다.

## 1.서론

전 세계적으로 정보화 시대를 이끌고 있는 선진 국가들은 앞선 노력으로 정보보호 시스템을 계속적으로 개발하고 있으며, 표준의 제정으로 선진기술 확보 및 국가이익에 이바지하고 있다. 또한 개발된 정보보호 시스템들을 인증하고 평가하기 위한 평가방법을 만들어 나감에 따라 개발자의 입장에서는 개발할 대상의 목표를 명확히 해줄 뿐 아니라 평가를 통해 얻는 평가등급은 이익 창출과 개발 노력을 더욱더 활성화 시키는 효과를 발휘할 수 있다. 사용자 입장에서도 정보보호에 대한 전문지식이 없다 하더라도 필요한 정보보호 제품을 선정할 수 있는 기준을 마련해주며, 신뢰하고 사용할 수 있는 여건을 만들어 나간는데 많은 기여를 하고 있다.[1] 그 첫째 예로 국제공통평가기준(CC : Common Criteria)이 있다. 이는 국가간의 상호 인증과 ISO/IEC JTC1/SC27/WG3 를 통한 국제 표준으로 정착시키기 위한 평가기준 이다. 또한 TCSEC을 네트워크 시스템에 적용하여 해석한 것으로 1987 년에 개발되어진 TNI(Trusted Network Interpretation of TCSEC)가 있다.

위의 국제 추세에 반해 현재 국내에서는 다수의 네트워크 보안제품들이 개발되고 있으나, 이 제품들에 대해서 일관성 있고 객관적인 평가를 할 수 있는 기준 및 근거가 부족하여, 사용자가 적합한 보호수준을 제공하는 정보보안 제품을 신뢰하고 선택할 수 있는 환경이 조성되어 있지 않다. 또한 개발된 제품에 대해 검증이 이루어지지 않았으므로 국외 제품과의 경쟁력에 치명적인 손실을 가져오게 된다. 본 논문에서는 네트워크 보안제품의 평가기준에 대한 연구결과를 도출해내기 위해, 우선 국제평가기준으로 국제공통평가기준(CC)과 TNI 를 비교 분석하여 필요한 보안기능 요구사항을 도출해내고 결론 및 향후 연구과제로 국내실정에 적합한 형태의 네트워크 보안제품의 평가기준(안) 제정을 위한 방향성을 제시한다.

## 2. 국제평가기준

### 2.1 국제공통평가기준(Common Criteria)

CC(Common Criteria for Information Technology Security Evaluation)는 세계 각국의 정보보호 시스템에 대한 평가기준이 상이함을 해결하기 위해 1993 년 미국, 캐나다, 프랑스, 독일, 네덜란드, 영국 6 개국의 합의에 따라 개발 시작 되었고,1996 년 1 월에 CC V1.0 이 발표되고, 마침내 CC V2.0 이 1999 년 6 월 ISO IS 15408 로 확정되었다.[7]

(1) 국제공통평가기준의 구성

Part 1 는 소개 및 일반 모델을 제시하며,Part 2 는 보안기능 요구사항, Part 3 는 보증 요구사항, Part 4 는 이미 정의된 보호 프로파일을 기술하고,Part 5 는 보호 프로파일을 등록하는 절차를 포함한다.[2] CC 의 핵심 요소는 Part 2 와 Part 3 로 정보보호시스템이 구비하여야 하는 기능 및 보증 요구사항을 기술하고 있으며 개발자는 기술된 요구사항을 참조하여 정보보호 시스템을 개발할 수 있다.[4]

(2) 보안기능요구사항

보안기능 요구사항은 TOE 의 보안행동을 설명하기 위한 보안기능 컴포넌트를 세분화 한 것이다.

- 클래스 : 공통내용을 지닌 패밀리들의 그룹
- 패밀리 : 공통된 보안목적의 컴포넌트들의 그룹
- 컴포넌트 : 실제 보안 요구사항
- 패키지 : TOE 에서 같은 보안목적을 만족하는 요구사항들을 모은 컴포넌트들의 집합

# 국제공통평가기준 보안기능 요구사항 클래스[7]

FAU(보안감사) : 보안활동과 관련된 정보를 감지, 기록, 저장, 분리
FCO(통신) : 데이터를 교환하는 주체의 신원을 감지
FCS(암호지원) : 암호 운용 및 키 관리
FDP(사용자 데이터 보호) : 사용자 데이터 보호
FIA(식별 및 인증) : 사용자의 신원확인 및 인증
FMT(보안관리) : TSF 데이터, 보안속성, 보안기능 관리
FPR(프라이버시) : 허가되지 않은 사용자에 의한 개인의 신원 및 정보의 도용 방지
FPT(TOE 보안기능의 보호) : TSF 데이터 보호 및 관리
FRU(자원활용) : TOE 의 가용자원을 확보
FTA(TOE 접근) : TOE 에 대한 사용자 세션의 보호
FTP(안전한 경로/채널) : 사용자와 TSF 간 혹은 TSF 간의 안전한 통신채널 확보

(3) 국제공통평가기준 분석 결과

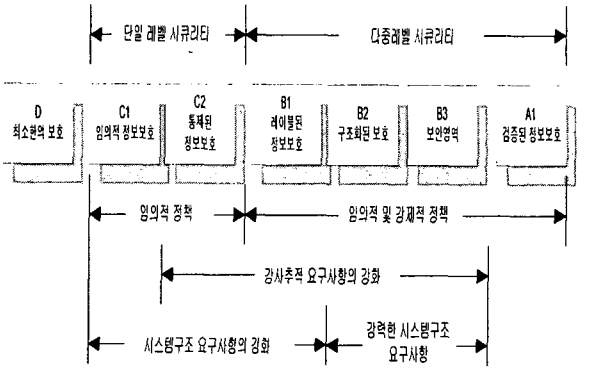
국제공통평가기준의 보안기능요구사항에서 실제 보안요구사항을 정의하는 컴포넌트들은 계층적인 관계와 함께 종속성을 가진다. 만일 컴포넌트가 추가적인 보안기능을 제공할 경우에 이 컴포넌트는 다른 컴포넌트에 계층적인 관계를 가지게 된다. 따라서 네트워크 보안제품에 대한 평가기준을 작성할 경우 기능 컴포넌트 각각이 제공하는 기능과 더불어 계층관계와 종속관계에 있는 기능 컴포넌트를 고려하여 작성되어야 한다.

## 2.2 TNI (Trusted Network Interpretation of TCSEC)

TNI 는 기존의 TCSEC 을 네트워크 시스템에 적용하여 해석한 것으로 1987 년에 개발되었다. Part I 는 기존의 TCSEC 을 네트워크 시스템에 맞게 해석한 내용을 가지고 있으며 구성상 TCSEC 의 기본구조를 따르면서 네트워크의 문맥을 이해하는데 꼭 필요한 부분에만 새로운 개념을 도입하였다. Part II 는 단일한 컴퓨터에서는 나타나지 않거나 네트워크 환경에서 중요성이 높아지는 추가적인 네트워크 보안에 관한 고려사항을 다룬다.[3]

(1) TNI 의 Part I 등급체계

TNI 의 등급체계는 [그림 2.1]과 같이 기존의 TCSEC 의 등급체계와 마찬가지로 A, B, C, D 등급으로 크게 구분된다. D 등급은 평가가 수행되었지만 평가등급의 요구사항을 만족하지 못한 등급이다. C 등급은 임의적 보호를 제공하며 감사기능을 통하여 주체와 그들의 행위에 대한 책임추적을 제공한다. B 등급에서는 중요한 요구사항으로 보안 레이블의 무결성을 보장하고 강제적 접근통제 규칙들의 집합을 적용하기 위하여 보안 레이블을 사용하는 TCB 의 개념을 네트워크에 적용하였다. A 등급은 정형화된 검증방법을 사용하는 것이 특징이다. 이 정형화 보안 검증방법은 시스템에서 채택된 강제적, 임의적 보안통제가 시스템에서 저장되고 처리되는 비밀 혹은 기타 중요 정보를 효과적으로 보호함을 보증하기 위해 사용된다.[5]

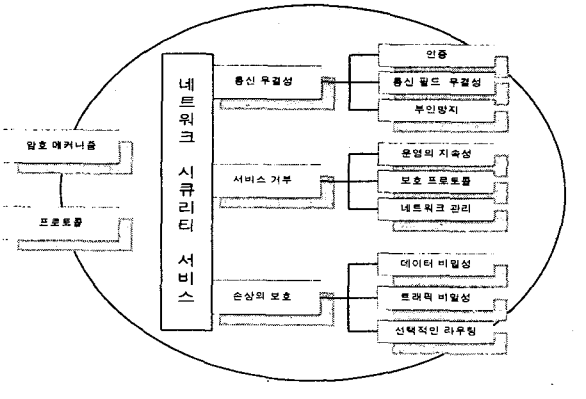



[그림 2.1] TNI 의 등급별 특성

(2) TNI 의 Part II 의 등급체계

TNI 의 Part II 에서 제시하고 있는 서비스들의 구조를 살펴보면 [그림 2.2]와 같이 구성된다. 이렇게 제공되어질 수 있는 시큐리티 서비스들은 크게 두 가지 형태로 평가할 수 있다.[6]

- 기능성 평가 : 서비스가 제공되지 않으면 not offered 또는 none 으로 표현되며 인증, 부인방지, 데이터 비밀성, 트래픽 비밀성, 선택적 라우팅의 경우에는 서비스가 존재하는지 아닌지의 유/무( none / present ) 두 개의 값만을 갖는다.
- 메커니즘의 강조 : none 에서 good 까지의 값으로 나타나지만 비밀성을 위한 기능의 경우는 그 서비스로 안전하게 보호할 수 있는 비밀 정보의 등급으로 표현한다.




[그림 2.2] TNI Part II 의 구조

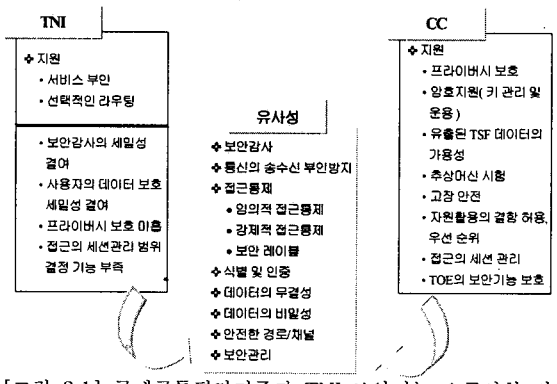
## 3. 네트워크 보안제품 평가기준(안) 연구

국제공통평가기준은 정보보호시스템에 필요한 모든 보안기능 요구사항을 담고 있어 특정 유형의 보안 제품에 대해 요구되어지는 요구사항들을 선택적으로 제공할 수 있다. 이에 반해 TNI 는 네트워크 보안제품이라는 특정 대상에 필요한 보안기능 요구사항들만 담고 있다. 이들의 일반적인 특징을 비교한 것은 [표 3.1]에 나타난다.

[표 3.1] 국제공통평가기준과 TNI 특징 비교

| 국제공통평가기준 | TNI |
|---|---|
| • 모든 정보보호 시스템(제품)에 적용 가능한 평가기준 | • 네트워크 정보보호 시스템(제품)에 적용 가능한 평가기준 |
| • 모든 정보보호 제품에 관련된 보안 요구사항을 클래스별로 분류 | • 정보보호 제품에 공통적인 보안기능 요구사항 - Part I<br>• 네트워크 정보보호 제품에 관련된 부가적인 보안기능 요구사항 - Part II |
| • 보안기능 요구사항에 따른 평가등급체계 미 설정 | • 평가등급체계 따라 정보보호 시스템에 공통적인 보안기능 요구사항 분류 - Part I<br>• 네트워크 정보보호시스템에 필요한 보안기능 요구사항을 정성적으로 분류 - Part II |
| • TOE 의 다양한 기능에 필요한 보안기능 요구사항을 선택하여 도출 | • 대상 제품을 보안기능 요구사항으로 평가 |
| • 평가대상 제품의 보안기술 변화에 따른 유연하고 확장성 있는 평가 가능 | • 평가대상 제품의 보안기술 변화에 CC 보다 유연하지 못함 |

또한 국제공통평가기준과 TNI 에서 제공하는 네트워크 보안제품 기능 요구사항들을 각 평가기준이 제공하는 독창적인 요구사항들과 서로 공통적으로 제공하는 요구사항들, 그리고 상호보완이 필요한 요구사항들을 중심으로 분류하면 [그림 3.1]과 같고 이 요구사항들을 조합하여 네트워크 보안제품을 위한 기능 요구사항들을 도출할 수 있다. 여기서 유사성에 나타난 요구사항들은 대부분의 네트워크 보안제품에서 요구되어지는 공통적인 보안기능 요구사항이고 국제공통평가기준, TNI 측의 개별적인 요구사항들은 보안제품 유형에 따라 첨가되거나 제공되지 않는다.

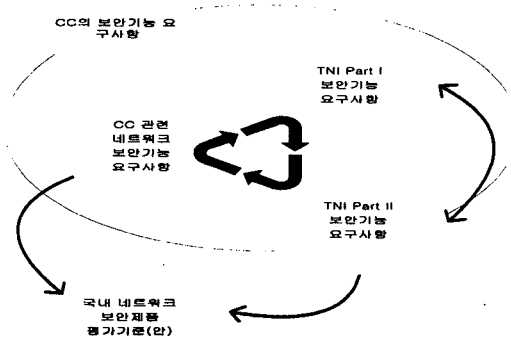



[그림 3.1] 국제공통평가기준과 TNI 보안기능 요구사항 비교

## 4. 결론 및 향후 연구방향

네트워크 보안제품 평가기준(안)을 제정하기 위해서는 우선적으로 네트워크 보안제품의 범주가 확정되어야 한다. 현재 평가를 받은 대부분의 제품들이 운영체제, 네트워크 컴포넌트, DBMS, 침입차단시스템 등에 한정되어 있으며 실제 네트워크를 구성하고 있는 라우터, 스위치, 허브, 랜 카드 등의 독립적인 장비에 대해서는 평가 사례가 없다. 또한 네트워크의 연결 및 인터넷의 연동은 LAN, WAN 등의 개념을 허물고 있으며, 다양한 네트워크 보안제품이 응용계층에서의 개발되고 있다. 따라서 평가기준(안)에 적용시킬 대상의 범주를 명확하게 설정하는 것이 우선되어져야 한다.

평가대상의 범주가 설정되었다면, 실제 이 네트워크 보안제품의 기능 요구사항을 [그림 4.1]과 같은 과정으로 도출해야 한다. 실제로 TNI 는 네트워크 보안기능 요구사항을 담고 있으므로 이를 기반으로 하되 미약한 부분을 국제평가기준 및 상용화 제품에서 요구되어지는 기능에서 보완하여 사용자, 개발자, 평가자 모두가 만족할만한 요구사항을 도출해야 한다.




[그림 4.1] 네트워크 보안기능 요구사항 도출 과정

또한 급변하는 정보보호 패러다임을 수용할 수 있도록 평가기준(안)에 융통성을 부여해야 한다. 즉 현재의 네트워크 보안제품에는 필요치 않은 기능들이 미래에는 요구될 수 있으며, 현재 제공되어지는 기능이 미래에는 사라질지 모르므로 평가기준(안)의 보안기능 요구사항은 유연성과 확장성을 지녀야 한다.

향후과제로 현재 도출된 모든 네트워크 보안제품 기능 요구사항을 기반으로 국제기준에 상호호환이 가능한 등급체계를 설정하여 등급별 보안기능 요구사항을 분류하는 작업이 수행되어야 한다. 이 작업은 실제 평가결과가 타당성 있고 신뢰성이 부여되어야 하므로 충분한 검증을 통하여 확인작업이 이루어져야 한다.

## [ 참고 문헌 ]

[1] 김동규외, 분산통신망 환경 통합 정보보호 소프트웨어기술, 3 차년도 보고서, 정보통신부, 1999.01
[2] [ITSEC] Information Technology Security Evaluation Criteria, Version 1.2 Office for Official Publications of the European Communities, June 1991.
[3] [TCSEC] Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985.
[4] 한국정보보호센터, 국제공통평가기준, 1998.11
[5] 한국정보보호센터, 국내외 정보보호시스템 평가 가이드, 1998.11
[6] http://www.Radium.ncsc.mil/tpep/
[7] http://csrc.nist.gov/cc