通信情報保護學會誌
第2卷, 第1號, 1992. 3

# 안전한 컴퓨터 시스템 개발동향

박 태 규*

## 1. 서 론

컴퓨터 및 네트워크 시스템의 보급이 활발해짐에 따라서 제공되는 서어비스도 다양해지고 있으며, 이 서어비스를 통해 유통되는 정보는 개인 및 기업의 정보로부터 국가의 정보에 이르기까지 실로 다양하고, 그 정보의 중요성이 점점 증대 되고 있는 추세이다. 그러나 현재 국내에서 개발되어 보급되고 있는 컴퓨터 및 네트워크 시스템은 이러한 중요한 정보의 보호라는 측면에서 보면 취약점이 많으며 이에 대한 대책이 거의 전무한 실정이다. 정보의 중요도에 따라 컴퓨터 및 네트워크 시스템도 보안기능을 갖추도록 하는 컴퓨터 및 네트워크 보안 연구는 미국, 유럽 등 선진국에서 부터 이미 시작되었으며 최근들어 상용화 단계에까지 이르고 있는 추세이다. 이에 본고에서는 '80년대 미국 및 전세계의 관심사인 미국의 안전한 컴퓨터 시스템 평가기준의 탄생배경 및 구성요소를 살펴보고, 이후에 이에 대처하기 위한 유럽의 정보기술보안평가 기준인 ITSEC(Information Techndogy Security Evaluation Criteria)의 발간 배경 및 구성요소를 살펴보았다. 또한 미국의 안전한 컴퓨터 시스템 평가기준과 유럽의 정보기술보안 평가 기준을 비교하여 그 차이점을 알아보고자 한다. 아울러 미국의 안전한 컴퓨터 시스템 평가기준에 따라 개발된 최근의 실용화 제품들을 살펴보고자 한다.

## 2. 미국의 안전한 컴퓨터 시스템 평가기준

1981년 미 국방부에서는 군기관, 정부기관 및 민간기업체를 위한 컴퓨터 보안기준 작성과 안전한 컴퓨터 시스템개발 및 평가를 담당하도록 하는 기관으로 Computer Security Center(1985년에 NCSC : National Computer Security Center로 바뀜)를 설립하였는데 이 NCSC의 설립목적은 안전한 컴퓨터 시스템의 광범위한 이용을 촉진시키는데에 있었다. 이런 목적의 일환으로 1983년에 NCSC는 기존에 개발된 Software Tool과 Multics(운영체제의 이름)를 기술적 기반으로 하여 TCSEC(Trusted Computer System Evaluation Criteria)이라는 안전한 컴퓨터 시스템 평가기준을 발간하였는데 일명, 표지의 색깔이 Orange 색이어서 Orangebook 이라고 부른다. 이 기준은 컴퓨터 시스템의 보안성을 효과적으로 평가하기 위한 기본적 요건을 정하여 그 요건에 따른 평가 등급을 부여하고 있다. 그러므로 이 기준에 따라 어떤 조직에서 어떤 등

* 정회원, 한서대학교 전산정보학과 조교수

급의 컴퓨터 시스템이 필요한지를 결정할 수 있게 하였다. 이 TCSEC에서 기준이 되는 기본적인 요건은 다음과 같다.

- policy : 컴퓨터 시스템 보안에 관한 정책 수립.
- Marking : 컴퓨터 시스템의 취급대상인 객체에 대한 액세스 레이블 정의
- Identification : 컴퓨터 시스템의 각 사용자는 사용자 신분 식별자를 가져야 함.
- Accountability : 각 행위에 대한 명백한 책임의 한계를 정함.
- Assurance : 상기 각 요건의 평가기준을 컴퓨터 시스템이 만족하는지를 H/W, S/W적으로 보증.
- Continuous Protection : 계속적인 컴퓨터 시스템 보안의 유지

이러한 요구사항들을 기반으로 하여 평가등급을 A1, B3, B2, B1, C2, C1, D급의 7등급으로 나타내고 있는데 등급에 따른 요건은 그림 1과 같으며, 그 주요한 특성을 살펴보면 다음과 같다.

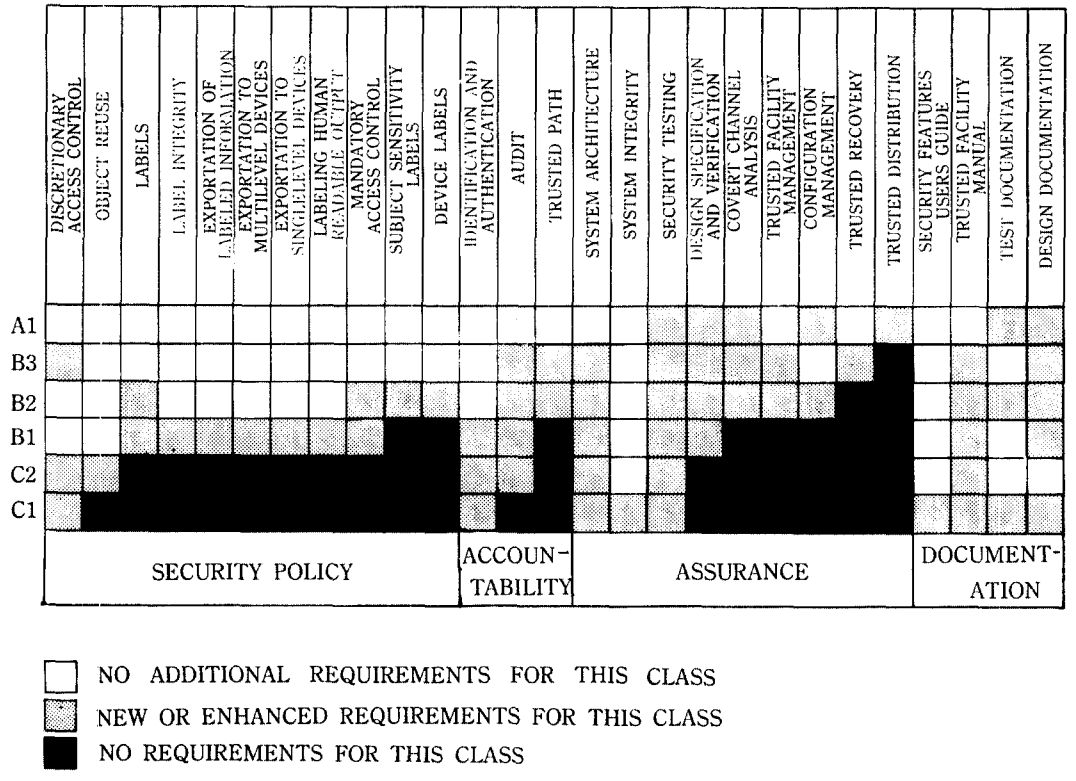


그림 1. TCSEC의 평가 등급

D급은 최소 비밀보호를 의미(Minimal Protection)하며, C급은 임의적 액세스제어(Discretionary Access Control) 수준을 말하는데 C1과 C2급으로 나누어진다. C1급은 사용자와 데이타를 분리하여 같은 등급의 데이타를 여러 사용자가 공유하며, C2급은 C1급 기능을 만족하는 동시에 로그인(Login) 기능 및 감사(Audit) 기능을 강화했으며 자원의 분리에 따른 각 사용자의 책임을 부여한 것이다. B급은 강제적 액세스제어(Mandatory Access Control) 수준으로 B1, B2, B3 등급으로 나누어진다. B1급은 보안정책에 대한 비정형화 보안 모델을 요구하며, 데이타에 비밀등급을 표시하는 레이블을 부여하여 주체(user 등) 및 객체(file 등)에 대한 강제적 액세스 제어를 시행한다. B2급은 보안정책에 대한 정형화보안 모델을 요구하며 보다 강화된 사용자 식별 및 신분확인 기능을 요구한다. B3급은 객체에 대한 주체의 모든 액세스를 제어하고 TCB (Trusted Computing Base ; 보안정책을 실행하는 컴퓨터 시스템내의 보호구역)가 외부로 부터 수정되는 것을 방지해야 하며, 비밀에 관련된 처리사항을 기록하는 감사 및 시스템 복구 기능을 제공하여야 한다. A급은 검증된 보호(Verified Protection) 수준을 제공하는 것으로 B3급을 만족하는 동시에 정형화한 설계 사양, 정형화한 설계검증 즉, 수학적인 증명 및 이러한 기능들에 대한 문서화를 요구하는 A1급으로 이루어져있다. 이러한 평가기준에 기반을 두고 컴퓨터 시스템의 보안을 검증 및 보증하는 연구도 활발히 진행되고 있으며 그 대표적인 검증방법으로는 HDM(Hierarchical Development Methodolgy), FDM(Formal Development Methodology), GIPSY, Affirm 등이 있다. 그리고, 미국의 TCSEC에서는 컴퓨터 시스템의 기술적 보안요소로서 통상 분류하는 Confidentiality, Integrity, Availability의 3가지로 볼 때 주로 confidentiality 만을 강조하여 평가를 하고 있다.

따라서 이러한 Confidentiality를 강조하는 군·정부기관 등에서는 비밀에 대한 취급이 많아 적절할지라도 Integrity가 강조되는 금융기관과 Availability가 강조되는 데이타처리업체에는 적절한 평가기준이 될 수 없다는 비판이 제기됨에 따라 미국 국가표준국인 NIST(National Institute of Standardization Technology)에서는 민간, 상업용을 위한 Civil Orange Book을 만들기 위해 1992년 초에 Draft를 만들어 각국에 배포하여 의견수렴을 하고 있는 단계이다. 그리고, 1988년 3월에 발표된 미국방성 Directive 5200.28의 지침중 비밀로 분류된 데이타 또는 중요한 데이타를 처리하는 모든 컴퓨터는 최소한 1992년까지는 C2급 이상을 충족시켜야 하며 장기적으로 2003년까지는 B3급 이상을 충족시켜야 한다는 규정에 따라 미국의 컴퓨터 개발업체에서는 안전한 컴퓨터 시스템 개발에 박차를 가하고 있다. 그러나 최근 이 규정에 대한 반발이 일어나고 있다. 이상의 TCSEC이 컴퓨터 시스템 자체를 위한 기준인 관계로 Network이나 Data Base 시스템에 이를 적용하기가 어려워 이 TCSEC을 Network에 적용시키기 위해서 1987년에 TNI(Trusted Network Interpretation)를 발간하였으며, Data Base 시스템에 적용하기 위한 TDI(Trusted Data Base Interpretation) Draft가 1988년에 발간되었다.

## 3. 유럽의 정보기술 보안 평가 기준

미국의 TCSEC에 맞서 유럽에서도 영국, 독일, 프랑스 등의 국가에서 안전한 컴퓨터 시스템 평가기준의 필요성이 대두되어 각자 자국의 평가기준(그림 2참조)을 발간하였으나 널리 이용이 되지 않았으며 보안성 평가에 대한 경험도 각국에 분산, 축적되어 있다는 판단과 유럽 각국의 산업체에서도 서로 다른 보안기준을 원치 않아 국가(정부·군) 및 상업용일지라도 기본개념과 접근방법이 같다는 인식하에 1990년 5월에 유럽 합동기준 Draft인 ITSEC(Information Technology Security Evaluation Criteria)을 영국, 독일, 프랑스, 네덜란드 등 4개국이 주축이 되어 발간하였으며, 1990년 9월 브뤼셀에서 Commission of the European Community 후원하에 2일간 Conference가 개최되어 미비점을

보완한 Draft를 발간하기로 하였다. 1990년 5월에 발간된 Draft를 대상으로 분석해 본 이 기준은 IT (Information Technology) Security 제품에 대한 시장개발을 지원하기 위하여 IT관련 보안제품과 시스템 보안성평가를 위한 기준임을 목적으로 하고 있으며, 유럽공동체(EC) 구성과 때를 같이하여 유럽공동체의 보안성 평가, 승인제도를 채택하기 위한 출발로 향후에 국제 표준안(최근 ISO SC27의 working Group 3의 작업시 ITSEC을 제안하고 있음)으로 추진할 것으로 판단된다.

| 국 가 | 년 도 | 제 목 | 작 성 기 관 |
|---|---|---|---|
| 영 국 | 1989. 2 | Security Functionality Manual (Green Book) | DTI의 Commercial Computer Security Center |
| 독 일 | 1989. 7 | IT Security Criteria for the evaluation of trustworthiness of Information Technology system (Green Book) | German Information security Agency |
| 프 랑 스 | 1989. 9 | Blue-White-Red Book | Service Central de la securite des systems D'Information |

그림 2. 유럽 각 국의 보안성 평가 기준

ITSEC 기준은 기능(Functionality)과 보증(Assurance)의 두가지 요소로 분리되어 있다. 기능은 10개의 구분(F1, F2, …, F10)으로 나뉘어져 있으며, 보증은 7개 level(E0, E1, …, E6)의 Correctness 보증과 5개 과정을 평가하는 Effectiveness 보증으로 다시 구분된다. 그러나 ITSEC은 보안제품이나 시스템을 설계하는 지침서가 아니라 스폰서(산업체, 기업)가 보안 목표를 결정하여 이를 행할 보안기능을 선택하기 위한 것으로 이때 보증 기준은 체크리스트와 같으며, 모든 시험과 분석에 대한 책임은 스폰서에게 있다. 자세한 보안기능(Security Functionality), 보증, Correctness, Effectiveness, Rating에 관한 설명은 본 통신정보보호학회지 제 1 권 제 2 호(1991. 8)의 "컴퓨터 시스템의 보안평가를 위한 기술적 기준"(저자, 신장균)을 참조하기 바란다.

## 4. TCSEC과 ITSEC의 비교

지금까지 설명한 TCSEC과 ITSEC과의 비교는 표 1과 같다.

표 1. TCSEC과 ITSEC의 비교

| ITSEC | TCSEC |
|---|---|
| E0 | D |
| F1, E2 | C1 |
| F2, E2 | C2 |
| F3, E3 | B1 |
| F4, E4 | B2 |
| F5, E5 | B3 |
| F5, E6 | A1 |

여기에서 중요한 점은 ITSEC에서 TCSEC으로의 관계는 설립하지만 TCSEC에서 ITSEC으로의 관계는 어려우며 ITSEC 자체의 비현실적인 문제도 발생되고 있다. 즉 등급관계에서 TCSEC은 7개의 등급으로 고정되어 있는 반면 ITSEC에서는 가능한 등급수가 1344개(6×7×2×2×2×2×2)로 Many-to-one의 관계(예, F4/E3과 F3+7/E3 모두가 B1과

일치)가 성립되는 경우 및 F5+6+7+8+9/E0과 F1/E6와 같은 극단적인 경우는 비현실적이기 때문이다. 그리고, 두 기준의 평가측면에서도 TCSEC의 중요한 부분이 참조 모니터(Reference Monitor ; 주체가 객체를 액세스할때 보안통제) 개념에 기인하지만 ITSEC은 특정 메카니즘을 강요하지 않고 있다. 또한 TCSEC은 기능과 보증이 합쳐져 있지만 ITSEC은 기능과 보증이 분리되어 있다. TCSEC에서는 Integrity, Availability에 관한 것과 분산 네트워크에 관한 것이 미비 되어 있는데 TCSEC에서의 미지정을 TNI, TDI에서 정의하고 있다. 상기와 같은 두 기준의 차이점은 있으나 그 기본적 내용은 TCSEC의 범주를 벗어나지 못하고 있는 실정이다.

## 5. 시스템 개발 동향

1970년대에는 보안제품 연구개발을 기존 컴퓨터 시스템에 암호화, 액세스제어, 감사 등의 H/W, S/W를 Add-on하는 방식으로 연구·개발되어 왔으나 이러한 방식으로는 새로운 문제점(예로, 트로이 목마, 신종 시스템 범죄)을 해결할 수 없다는 연구결과와 더불어 문제점 발생시마다 보안제품을 계속적으로 Add-on 하는데 드는 비용과 번거로움에 따라 미니급 이상의 컴퓨터 시스템에서는 1980년대부터 시스템 내부 커널(Kernel)에 보안기능을 탑재시키는 보안커널 시스템(Security Kernel System) 접근방법이 활발히 연구되어 왔다. 이러한 연구방향에 기본 지침을 준것이 앞서 설명한 TCSEC이며 이 지침에 따라 주로 정부기관과 군기관에서 이러한 보안제품(시스템)을 연구·개발하여 사용하고 있었다. 그러나 이러한 시스템 내부 보안에 대한 범국가적인 필요성이 증대된 것은 1987년부터 전세계적으로 파급되어 큰 경각심을 불러일으킨 컴퓨터 바이러스에 의해서이며 그 피해의 심각성에 비추어 안전한 컴퓨터 시스템의 연구개발은 당연한 것이었다. 1990년초까지 미국에서 TCSEC에 따라서 개발완료된 제품 중 미국 정부의 공인 평가기관인 NCSC에서 평가가 완료된 제품은 표 2에서 보는바와 같이 17개 제품이 있으며 평가중에 있는 제품은 24개인데 이중 21개가 B급 이상의 등급으로 평가를 의뢰하고 있다는 점에서 볼 수 있듯이 향후개발될 컴퓨터 시스템에 대한 보안 등급이 상향추세임을 짐작할 수 있다.

최근 이런 추세에 따라 DEC사는 VMS운영체제를 B1급, IBM사는 MVS운영체제의 RACF를 B1급, AT&T사는 UNIX System V Release 4. 1 운영체제를 B2급으로 개발하고 있다.

그리고, 기존의 운영체제 수준에서의 Security Kernel의 구현으로 인해 발생되는 문제점인 성능저하, 운영체제의 변경에 따른 응용프로그램 등의 호환성 그리고 S/W 오동작에 의한 전체 보안매카니즘의 정확성 결여 등의 문제점을 해결하기 위한 새로운 접근방법으로 Security Kernel을 H/W level에서 구현하기 위하여 DOD와 Honeywell Systems에서 1988년부터 LOCK(Logical Coprocessor Kernel) 프로젝트를 수행하고 있는데 이것은 Host를 안전하게 하기 위하여 Host 내에 부가의 Coprocessor와 bus device를 이용하는 것이며 A1급으로 평가될 것으로 예상된다. 또한, 현재 국제적으로 표준운영체제로 되어가고 있는 UNIX 운영체제를 기반으로 하여 어떤 시스템에서도 서로 호환성이 있도록 하는 표준화 작업도 활발히 진행되고 있는데 그 대표적인 표준화 그룹으로는 IEEE의 POSIX, X/OPEN 그리고 OSF 등이다. OSF에서는 UNIX의 Secure Version을 개발하고 있으며, IEEE의 POSIX.6 Working Group에서는 4개의 보안소위원회(DAC, MAC, Privilege, Audit 그룹)를 구성하여 보안 표준화에 힘을 쏟고 있다. X/OPEN에서도 이미 X/OPEN Security Guide를 발간한 바 있으며, NCSC에서도 trusted UNIX 시스템을 개발하기 위한 Vendor들의 모임인 TRUSIX (Trusted UNIX Organization)를 구성하여 진행중에 있으며, 이 밖에도 OSF, AT&T, SUN Microsystems, 그리고 Santa Cruz Inc.들은 각각 Secure UNIX Version을 표준화된 UNIX로 채택하고자 많

표 2. 보안 평가 완료 제품

(1990년 1월 현재)

| 등급 / 개발회사 | C1 | C2 | B1 | B2 | B3 | A1 | 승인날자 |
|---|---|---|---|---|---|---|---|
| AT&T | | | SVR/MLS (UNIX) | *SVR4.1 | | | 89.9 |
| BOEING | | | MLS LAN | | | | |
| UNISYS | | InfoGuard Security | OS1100 Security | | | | 87.8<br>89.8 |
| CDC | | NOS2.2 | | | | | 86.5 |
| CAI | | CA-TOP SECRET/MVS | | | | | |
| DEC | | VMS | | | *VMS50 | | 86.7 |
| DATA GENERAL Corporation | | AOS/VS | | | | | 88.12 |
| GEMINI | | | | | | | |
| Encore Computer System | | UTX/32S | | | | | 88.12 |
| SUN | | | *SunOS MLS | | | | |
| Honeywell Information. Inc. | | | | MULTICS | | SCOMP | |
| IBM | | RACF/MVS RACF/VM | | *Trusted XENIX | | | 88.6<br>89.9 |
| PRIME | | PRIMOS | | | | | 88.6 |
| SKK | | ACF2/MVS | | | | | |
| WANG | | *SVS/OS | | | | | |
| Hewlett Packard Company | | MPE V/E | | | | | 88.10 |

*평가 중

은 노력을 기울이고 있다.

## 6. 결 론

컴퓨터 및 네트워크 시스템의 많은 보급으로 정부·군·민간기업·개인 등에 이르기까지 정보의 중요성이 높아지고 있어 컴퓨터 시스템의 보안연구·개발은 필수적이라 하겠다. 신종 컴퓨터 범죄나 컴퓨터 바이러스와 같은 지능적이며 시스템의 대량 피해를 유발시키는 역 기능적인 문제점을 미연에 방지하기 위해서도 차근 차근히 안전한 컴퓨터 시스템에 대한 연구가 필요함을 다시 강조하고자 한다.

현재 국내에서 이 분야의 연구·개발은 각 정부부처, 금융기관, 연구소, 대학 등에서 소규모적 일시적으로 실시되고 있는 것이 현실이며 이 분야의 전문가의 수와 연구수준, 투자비용 등을 고려해 볼때 초창기 단계임에 틀림이 없다. 그러므로 적은 자원으로 최적의 보안기술을 개발하기 위해서는 선진외국의 안전한 컴퓨터 시스템에 대한 면밀한 분석을 토대로 관 및 학·연·산이 공동대처해야 될 것으로 판단된다.

## 참 고 문 헌

1. DOD NCSC, "Trusted Computer System Evaluation Criteria", DOD 5200. 28-STD, NCSC, Dec, 1985.

2. M. Gasser, "Building A Secure Computer System", Van Nostrand Reinhold Company Inc., 1988.

3. "Information Technology Security Evaluation Criteria(ITSEC)", version 1, May, 1990.

4. "Conference Proceedings of The 7th International Conference & Exhibition on Information Security", IFIP TC-11, May, 1991.

5. "Proceedings of The 6th Annual Computer Security Applications Conference", IEEE Computer Society Press, Dec, 1990.

6. 박태규, 이형수, 신종태, "컴퓨터·네트워크 시스템 보안 표준화 동향분석", 제 2 회 정보보호와 암호에 관한 워크숍 논문집, 한국전자통신연구소, 1990, 9.

7. 신장균, "컴퓨터 시스템의 보안평가를 위한 기술적 기준", 통신정보보호학회지 제 1 권, 제 2 호, 1991. 8

8. 이형수, 이철원, 박태규, "안전한 컴퓨터 시스템 연구개발 동향", 제 3 회 정보보호와 암호에 관한 워크숍 논문집, 한국전자통신연구소, 1991. 10.

## □ 著者紹介

朴 泰 奎(正會員)

本 學會誌 第 1 卷 第 2 號 參照