韓國情報敎育學會論文誌
第2卷 第1號 pp.57~66.

# 안전한 접근 경로를 보장하기 위한 접근 제어

김 현 배

부산교육대학교 컴퓨터교육과

# Access Control for Secure Access Path

Kim, Hyun-Bae

Pusan National University of Education, Dept. of Computer Education

## Abstract

The primary purpose of security mechanisms in a computer systems is to control the access to information. There are two types of access control mechanisms to be used typically. One is discretionary access control(DAC) and another is mandatory access control(MAC). In this study an access control mechanism is introduced for secure access path in security system. The security policy of this access control is that no disclosure of information and no unauthorized modification of information. To make this access control correspond to security policy, we introduce three properties; read, write and create.

## Ⅰ. 서 론

컴퓨터 기술의 급속한 발전과 함께 현대 사회는 산업 사회에서 정보화 사회로 급속히 전환되고 있다. 정보화 사회의 특징인 정보의 공유, 정보 서비스의 다양화 등으로 인하여 정보에 대한 여러 가지 위협 요소들이 산재하여있는 현 시점에서는 중요 정보에 대한 보호가 큰 문제점으로 대두되고 있다.

보안이란 시스템에서 중요 정보에 대한 원하지 않는 노출, 변경, 파괴로부터 보호하는 것이다. 시스템의 보안 요구 사항은 정보의 불법적인 노출을 방지하기 위한 비밀성, 정보의 불법적인 변경을 방지하기 위한 무결성, 적법한 접근은 방해받지 않기 위한 가용성으로 요약할 수 있다[8][11]. 비밀 취급이 많은 정부 기관이나 군대는 비밀성을 강조하는 것이 적절하며 읽기 접근에 대한 제어를 중요시한다. 그러나 금융 기관 같은 상업용에서는 정보의 부적절한 변경을 방지하기 위한 무결성을 강조하며 쓰기 접근 제어를 중요시한다. 그리고 데이터 처리 업체와 같은 곳에서는 적법한 접근이 항상 방해받지 않도록 하기 위한 가용성이 강조되는 것이 타당하다.

시스템이 특정 목적에 한정되어 사용되는 전용 시스템은 시스템의 이용 권한이 없는 사용자는 시스템의 외부적 접근을 통제하여 보안을 유지할 수 있다. 그러나 여러 사용자에게 시스템의 접근을 허용하는 다중 프로그래밍에서는 시스템의 외부적 접근 통제만으로는 보안을 유지할 수 없으므로 내부적인 보안 메커니즘이 필요하다.

본 연구는 안전한 접근 경로를 확보하기 위하여 비밀성과 무결성을 보장할 수 있는 접근 경로를 정의하여 정보의 접근 권한이 없는 사용자에게 접근을 불허한다.

# Ⅱ. 접근 제어

시스템에서 보안 메커니즘의 기본 목표는 정보에 대한 접근을 통제하는 것이다. 정보의 접근을 통제하기 위한 수단으로서 접근 제어는 임의적 접근 제어와 강제적 접근 제어로 구별한다.

## 1. 임의적 접근 제어

임의적 접근 제어는 아주 일반적으로 사용하는 방법으로서 사용자는 자신이 소유한 파일을 접근할 수 있는 이들을 임의대로 지정할 수 있다. 임의적 접근 제어는 사용자 또는 그들이 속해있는 그룹들의 식별자(ID)에 근거하여 파일에 대한 접근을 통제하는 방법으로서 패스워드, 능력 리스트, Unix의 허가 비트, 접근 제어 리스트 등이 있다[7][8].

임의적 접근 제어에서 사용자는 자신이 소유한 파일에 대한 접근 제어 정보를 자유롭게 변경할 수 있으며, 사용자 자신이 소유한 접근 권한을 다른 사용자에게 넘겨주는 것이 가능하다. 따라서 운영체제는 접근 제어 정보를 변경할 때 사용자의 합법적인 요구와 합법적인 요구를 가장한 요구를 구별할 수 없다.

## 2. 강제적 접근 제어

임의적 접근 제어와는 달리 강제적 접근 제어는 특별한 보안 등급을 사용자와 파일 각각에 할당한다. 사용자가 파일을 접근하려 할 때 시스템은 사용자와 파일의 보안 등급을 비교하여 접근 허가를 결정한다[1][8][7]. 이때 사용자와 파일의 보안 등급은 임의로 변경될 수 없다.

시스템 보안을 위한 접근 제어 정책은

임의적 접근 제어와 강제적 접근 제어를 각각 독립적으로 사용하거나 두 방법을 혼합하여 사용할 수 있다. 임의적 접근 제어와 결합하여 사용되어지면 사용자는 임의적 접근 제어와 강제적 접근 제어로부터 모두 허가를 얻어야 파일에 대한 접근 권한을 획득하게 된다. 사용자는 강제적 접근 제어의 보안 등급을 직접 조작할 수 없으므로, 자신만의 임의적인 보호를 위하여 임의적 접근 제어를 사용할 수 있다.

단순히 다른 사용자의 파일에 대한 접근을 통제하려 한다면 임의적 접근 제어만으로도 충분하다. 반면에 임의의 파일에 대해서 임의적 접근 제어를 가진 어떤 사용자가 그 파일을 다른 사용자에게 주는 것을 통제하려 한다면 임의적 접근 제어만으로는 충분하지 못하다. 어떤 파일에 대한 읽기 접근이 가능한 임의의 사용자가 파일을 읽어서 다른 사용자에게 파일의 내용을 전달하는 것은 언제나 가능하기 때문이다.

강제적 접근 제어는 임의적 접근 제어 권한을 가진 사용자가 파일을 읽어서 접근 권한이 없는 다른 사용자에게 전달하는 것을 막으려는 목적이다. 강제적 접근 제어가 일단 구축되면 정보를 다른 사용자에게 전달하는 방법은 문서를 통하여 전달하거나 아니면 자신의 패스워드를 알려주는 방법뿐이다. 강제적 접근 제어는 여러 가지 방법으로 제안되어 있지만 이들은 모두 미국방성의 다단계 보안 정책의 변형들이다.

## III. 다단계 보안

다단계 보안의 개념은 1960년대 컴퓨터에 저장된 정보를 보호하기 위한 미국방성의 군사 보안 정책을 바탕으로 한다. 미국방성의 군사 보안 정책은 일반적으로 모든 정보가 똑같은 수준으로 보호될 필요가 없다는 점에 착안하여 정보를 보안 등급에 따라 분류한다. 모든 정보에는 보안 등급을 부여하고 사용자에게는 인가 등급을 부여한다. 사용자가 정보를 열람할 때에 그 허가를 결정하기 위하여 사용자의 인가 등급과 정보의 보안 등급을 비교한다.

보안 등급은 비밀 등급과 구획의 두 가지 요소로 구성된다. 비밀 등급은 정보의 비밀 정도에 따라 상위 등급으로부터 top secret, secret, confidential, unclassified 등의 이름으로 분류한다. 또한 동일한 비밀 등급의 정보라도 그 정보를 사용할 수 있는 사용자의 업무에 따라 이용할 수 있는 정보의 이용 범위를 제한하여 보다 높은 정보의 분류가 가능하도록 하였다. 정보의 이용 범위는 구획의 집합으로 정의하며, 그 구성은 NATO, atomic, USSR, cryptographic 등과 같이 미국방성에서 사용하는 여러 이름들 중에서 선택하도록 하였다[8][9][11].

보안 등급은 정보의 비밀 등급과 구획 집합을 결합하여 (비밀 등급, 구획 집합)과 같이 표현하며, 정보의 이용자와 비밀성을 가진 정보에 각각 부여된다. 접근 제어는 사용자의 보안 등급이 정보의 보안 등급을 지배할 때 접근을 허가한다. 사용자를 주체로 하고 정보를 객체라 할 때, 주체 S와 객체 O의 보안 등급 사이의 지배 관계 "≥"는 다음과 같다.

정의 : 지배 관계 S ≥ O

S ≥ O 와 동격 관계는

비밀 등급(S) ≥ 비밀 등급(O) 이고,

구획 집합(S) ⊇ 구획 집합(O)일 때 성립한다.

군사 보안 정책은 많은 연구가 거듭되었고 그 의미가 잘 정돈되어 있으므로 군사 목적이 아닌 상업용에 적용이 쉽게 이루어질 수 있다. top secret, secret와 같은 비밀 등급은 1급 비밀, 대외비 등과 같이 일반적으로 사용하는 비밀 등급으로 변환이 가능하고, 구획 집합도 회계, 인사 등과 같은 부서의 이름으로 변환이 가능하다.

## 1. 안전한 정보 흐름 경로

안전한 정보 흐름 경로란 파일을 읽어서 쓰기를 할 때에 정보의 흐름이 보안 요구 사항을 위반하지 않는 경로를 말한다. 다음에 비밀성을 보장하기 위한 접근 경로와 무결성을 보장하기 위한 접근 경로를 보인다.

### (1) 비밀성 보장을 위한 접근 경로

D. Bell과 L. LaPadula는 비밀성을 강조한 군사 보안 정책인 다단계 보안 정책을 수용하여 강제적 접근 제어로 안전한 정보 흐름 경로를 형식적으로 표현하였다[2][9][10]. 이때 안전한 정보 흐름 경로는 상위 보안 등급의 정보가 하위 보안 등급으로 흐르지 않는 접근 경로를 말한다.

비밀성을 보장하기 위한 안전한 접근 경로를 정의하기 위하여 사용자(이하 주체)와 파일(이하 객체)은 보안 등급에 따라 분류하고, 읽기에 관련한 성질과 쓰기에 관련한 성질을 정의한다.

읽기 성질에서 주체는 주체가 지배하지 못하는 상위 보안 등급의 객체는 읽지 못하도록 하여 상위 보안 등급의 객체가 하위 보안 등급으로 흐르는 것을 차단한다. 그러나 읽기 성질만으로는 비밀성을 보장할 수 없다. 상위 보안 등급의 주체가 그 주체와 같은 보안 등급의 객체를 읽어서 하위 보안 등급의 객체에 쓰기를 시도한다면 비밀성은 유지될 수 없으므로 쓰기 성질로 보완한다.

쓰기 성질에서 주체는 하위 보안 등급의 객체에 쓰기를 금지하여 상위 보안 등급의 객체가 그 객체보다 하위 보안 등급을 획득하는 것을 차단한다. 안전한 정보 흐름 경로를 확보하기 위하여 읽기 성질과 쓰기 성질을 각각 단순 보안 성질과 *-보안 성질의 두 가지 보안 성질로 정의한다.

다음에 S를 주체의 집합, O를 객체의 집합, C(s)를 주체 s의 보안 등급, 그리고 객체 o와 p의 보안 등급을 각각 C(o), C(p)라 할 때 단순 보안 성질과 스타 보안 성질을 다음과 같이 정의한다.

단순 보안 성질

주체 S는 객체 O에 대하여 C(s) ≥ C(o) 일 때 읽기 허가

*- 보안 성질

객체 O에 대하여 읽기 접근이 있는 주체 S는

C(p) ≥ C(o) 인 객체 p에 쓰기 허가

단순 보안 성질은 읽기에 관련한 보안 성질로서 하위 보안 등급의 주체는 상위 보안 등급의 객체를 읽지 못하도록 하여 상위 보안 등급의 정보가 하위 보안 등급의 주체로 노출되는 것을 차단한다. 스타 보안 성질은 쓰기에 관련한 보안 성질로서 임의의 객체에 대해서 읽기 접근을 시도한 주체는 지금까지 읽은 객체보다 보안 등급이 낮은 객체에 쓰기를 금지하는 보안 성질이다.

스타 보안 성질은 상위 보안 등급의 주체가 고의적으로 혹은 무의식적으로 상위 보안 등급의 객체를 읽어서 보다 낮은 보안 등급으로 내려놓는 것을 차단하는 보안 성질이다.

### (2) 무결성 보장을 위한 접근 경로

Biba는 주체와 객체를 무결성 등급으로 분류하고, 낮은 무결성 등급의 정보가 높은 무결성 등급으로 흐르지 못하도록 하는 안전한 정보 흐름 경로를 정의하였다[4]. 무결성을 보장하기 위한 안전한 접근 경로를 정의하기 위하여 Biba는 주체와 객체를 무결성 등급으로 분류하고, 주체와 객체에 대하여 쓰기에 관련한 성질과 읽기에 관련한 성질을 정의한다.

쓰기 성질에서 무결성이 낮은 주체는 주체가 지배하지 못하는 상위 무결성 등급의 객체에 쓰기를 금지하여 무결성이 낮은 주체에 의한 객체의 변경을 차단한다. 상위 무결성 등급의 주체가 하위 무결성 등급의 객체를 읽어서 읽은 객체보다 상위 무결성 등급의 객체에 쓰기를 시도한다면 무결성은 유지될 수 없으므로 읽기 성질로 보완한다.

읽기 성질에서 주체는 하위 무결성 등급와 객체를 읽지 못하도록 하여 무결성 등급의 객체가 그 객체보다 상위 무결성 등급을 획득하는 것을 차단한다.

무결성을 보장하기 위한 안전한 접근 경로를 정의하기 위하여 Biba는 쓰기 성질과 읽기 성질을 각각 단순 무결성 성질과 *-무결성 성질의 동치인 무결성 성질로 정의한다.

다음에 S를 주체의 집합, O를 객체의 집합, 주체의 무결성 등급을 I(s), 그리고 객체 o와 p의 무결성 등급을 각각 I(o), I(p)라 할 때, 단순 무결성 성질과 스타 무결성 성질을 정의한다.

**단순 무결성 성질**

주체 S는 객체 O에 대하여 I(s) ≥ I(o)인 경우

객체에 쓰기 허가

***- 무결성 성질**

객체 O에 대하여 읽기 접근이 있는 주체 S는

I(o) ≥ I(p)인 객체 p에 쓰기 허가

단순 무결성 성질을 하위 무결성 등급의 주체는 상위 무결성 등급의 객체에 쓰기를 금지하여 상위 무결성 등급의 객체가 하위 무결성 등급의 주체에 의하여 변경되는 것을 차단한다.

스타 무결성 성질은 읽기에 관련한 성질로서 상위 무결성 등급의 주체는 하위 무결성 등급의 객체를 읽지 못하도록 한다. 상위 무결성 등급의 주체가 하위 무결성 등급의 객체를 읽어서 주체와 같은 등급의 객체에 써넣는다면 주체와 같은

등급의 객체는 하위 무결성 등급의 객체에 의하여 변경될 수 있다. 스타 무결성 성질은 하위 무결성 등급의 객체가 보다 높은 상위 무결성 등급을 얻지 못하도록 하는 성질이다.

## Ⅳ. 안전한 접근 경로

본 연구에서 정의하는 안전한 접근 경로는 시스템의 모든 상태는 주체와 객체로 구별하고, 주체와 객체에는 (비밀 등급, 구획 집합)으로 구성된 보안 등급을 부여한다. 주체와 객체의 보안 등급은 지배 관계가 성립하고, 각 주체와 객체의 보안 등급은 반순서 관계를 유지하도록 한다.

안전한 정보의 흐름은 비밀성을 보장하기 위하여 상위 보안 등급의 객체가 그보다 하위 보안 등급의 주체나 객체에 흐를 수 있는 경로를 허가하지 않고, 무결성을 보장하기 위하여 하위 보안 등급의 객체가 그보다 상위 보안 등급의 주체나 객체에 흐르는 경로를 허가하지 않는다. 안전한 접근 경로를 정의하기 위하여 읽기, 쓰기, 그리고 생성의 세 가지 성질을 정의한다.

### 1. 읽기 성질

비밀성을 보장하기 위해서는 상위 보안 등급의 객체가 하위 보안 등급의 주체나 객체로 흐르는 경로를 차단하여야 한다. 상위 보안 등급의 객체가 하위 보안 등급으로 흐르는 경우는 하위 보안 등급의 주체가 상위 보안 등급의 객체를 읽는 경우이다. 따라서 비밀성을 보장하기 위한 읽기 성질은 주체가 객체를 지배하는 경우만 읽을 수 있도록 허가한다.

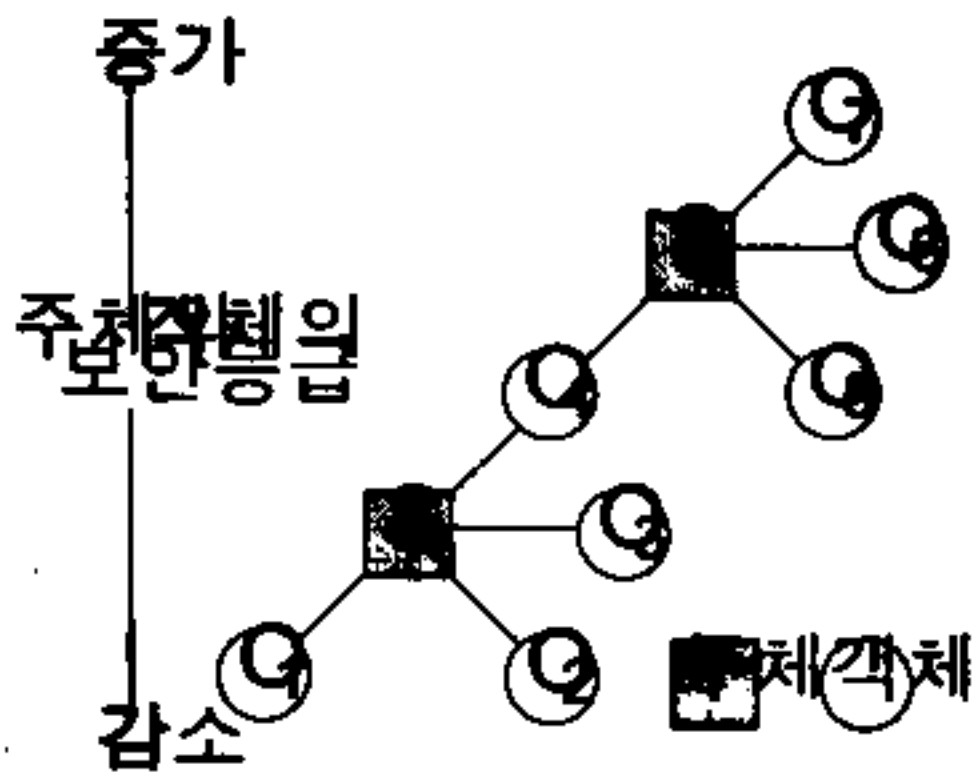
무결성의 위반은 하위 등급의 주체가 상위 등급의 객체에 쓰기를 시도할 때 발생하므로 주체가 객체를 지배하는 경우에만 읽기를 허가하면 읽기에 관련한 무결성은 보장할 수 있다.

<그림 1>에서 주체 S1은 O1, O2, O3, 을 지배하므로 읽기 권한이 있지만 O4는 S1이 지배하지 못하므로 읽기 접근을 허가하지 않는다. O5는 S2에게 지배당하지만 S1과는 관계가 없으므로 읽기 접근을 허가하지 않는다. 주체의 집합을 S, 객체의 집합을 O, 주체의 보안 등급을 SC(s), 객체 p, q의 보안 등급 각각 SC(p), SC(q)라 할 때 읽기 성질을 다음과 같이 정의한다.

읽기 성질
주체 S는 객체 O를 SC(s) ≥ SC(o)
일 경우
읽기 허가.

### 2. 쓰기 성질

읽기 접근을 시도한 어떤 주체가 지금까지 읽은 객체보다 하위 보안 등급의 객체에 쓰기를 시도한다면 상위 보안 등급의 객체가 하위 보안 등급으로 유출되어 비밀성을 보장할 수 없다. 비밀성을 보장하기 위한 읽기 성질은 보완되어야 한다.




<그림 1> 주체와 객체와의 관계

<그림 1>에서 주체 S1은 O1, O2, O3을 지배하므로 읽기 권한이 있다. 이때 S1이 O3을 읽어서 O1이나 O2에 쓰기를 시도한다면 상위 보안 등급의 정보 O3의 내용이 하위 보안 등급의 객체 O1이나 O2로 흘러 들어가게 되어 비밀성을 보장할 수 없게 된다. 따라서 비밀성을 보장하기 위한 쓰기 성질은 읽기 접근을 시도한 주체는 지금까지 읽은 객체보다 하위 보안 등급의 객체에 쓰기를 할 수 없도록 한다.

무결성을 보장하기 위한 읽기 성질 또한 보완되어야 한다. 읽기 접근이 있는 어떤 주체가 지금까지 읽은 객체보다 상위 보안 등급의 객체에 쓰기를 시도한다면 상위 보안 등급의 객체는 무결성을 잃게 된다.

<그림 1>에서 S1이 객체 O1, O2를 읽어서 O3에 쓰기를 시도한다면 상위 등급 O3은 하위 등급의 O1, O2에 의해서 오염될 가능성이 있으므로 무결성을 유지할 수 없다. 무결성을 보장하기 위한 쓰기 성질은 읽기 접근은 시도한 주체는 지금까지 읽은 객체보다 상위 보안 등급의 객체로 쓰기를 허가하지 않는다. 따라서 비밀성과 무결성을 유지하기 위한 쓰기 성질은 읽은 객체와 같은 보안 등급으로만 허가한다.

주체의 집합을 S, 객체의 집합을 O, 주체의 보안 등급을 SC(s), 객체 p, q의 보안 등급 각각 SC(p), SC(q)라 할 때 쓰기 성질을 다음과 같이 정의한다.

쓰기 성질

객체 O에 대해서 읽기 접근이 있는 주체 S는

SC(o) = SC(p)인 객체 p에 쓰기 허가

## 3. 생성 성질

읽기 접근이 있는 어떤 주체가 읽은 객체들을 처리하여 새로운 파일을 생성한다면 이때 생성된 파일은 지금까지 읽은 파일보다 비밀성이 더 높아진다. 비밀성과 무결성을 보장하기 위한 쓰기 성질은 보완되어야 한다.

<그림 1>에서 주체 S1이 객체 O1과 O2를 읽어서 기존의 O3에 쓰기를 허가하면 무결성을 보장할 수 없지만, 새로운 파일 O4로 생성하도록 한다면 무결성을 위반하지 않으며, 보안성도 위반하지 않는다. 따라서 읽은 객체보다 상위 보안 등급으로 쓰기는 허가하지 않지만 읽은 객체보다 상위 보안 등급으로 새로운 파일을 생성하는 것은 허가한다.

주체의 집합을 S, 객체의 집합을 O, 주체의 보안 등급을 SC(s), 읽은 객체를 p, 새로 생성하는 객체 'o의 보안 등급 각각

SC(p), SC('o)라 할 때 생성 성질을 다음과 같이 정의한다.

생성 성질
객체 O에 대해서 읽기 접근이 있는
주체 S는
SC(o) < SC('o)인 새로운 객체 'o에
생성 허가

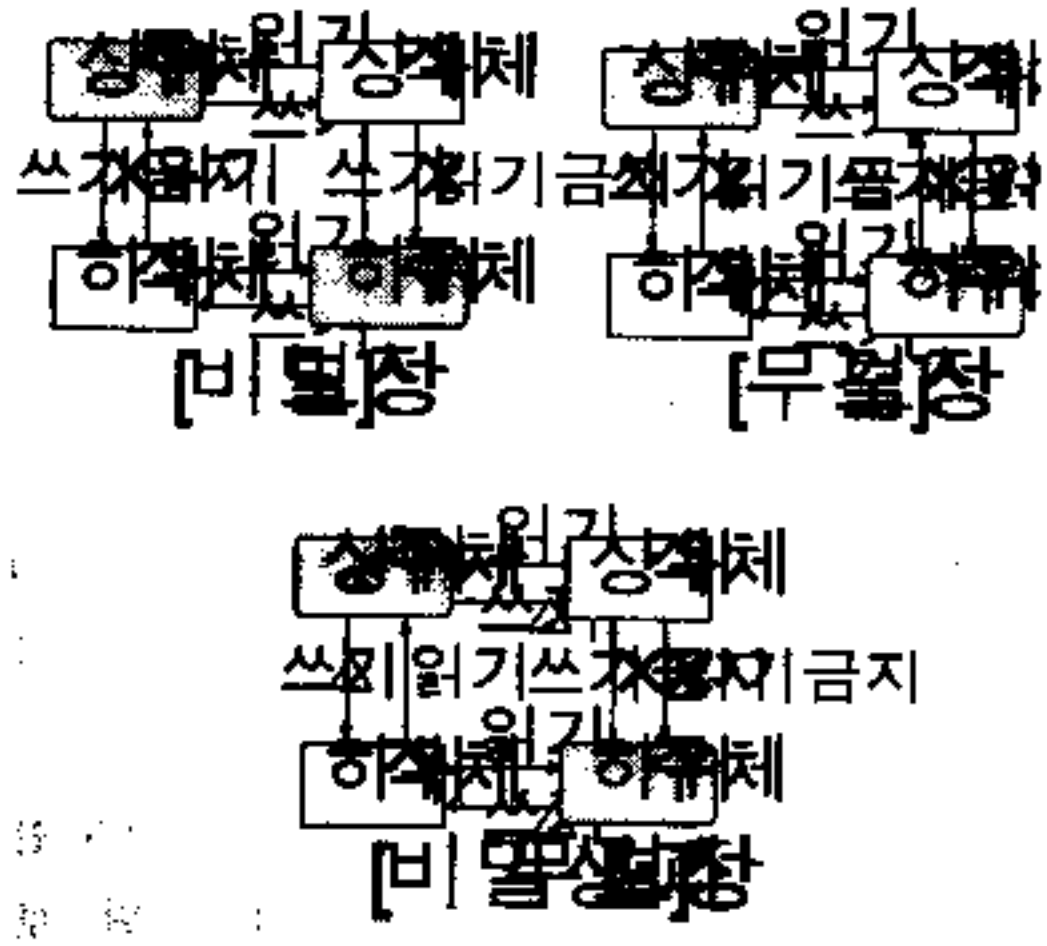
## V. 토 론

D. Bell과 L. LaPadula는 비밀성을 보장하기 위하여 상위 보안 등급의 객체가 하위 보안 등급의 객체로 흐르는 접근 경로를 차단하였다. 읽기 성질을 정의하여 하위 보안 등급의 객에는 상위 보안 등급의 객체를 읽을 수 없도록 하였다. 읽기 접근이 허가된 주체가 읽은 객체보다 하위 보안 등급의 객체에 쓰기를 금지하기 위하여 D. Bell과 L. LaPadula는 주체의 관점에서 주체보다 하위 보안 등급의 객체에 쓰기를 금지하였다.

하위 보안 등급의 주체가 상위 보안 등급의 객체를 읽을 수 없으므로 정보의 불법적인 노출을 막을 수 있다. 그러나 하위 보안 등급의 주체가 상위 보안 등급의 객체에 쓰기를 허가하므로 하위 보안 등급의 주체에 의해서 상위 보안 등급의 객체가 변경될 수 있다.

Biba는 무결성을 보장하기 위하여 하위 무결성 등급의 주체가 상위 무결성 등급의 객체를 변경하는 접근 경로를 차단하였다. 쓰기 성질에서 Biba는 하위 무결성 등급의 주체는 상위 무결성 등급의 객체에 쓰기를 금지하였다.

하위 무결성 등급의 주체가 상위 무결성 등급의 객체에 쓰기를 허가하지 않으므로 무결성 등급이 낮은 의심스러운 주체에 의한 변경을 방지할 수 있다. 그러나 Biba는 하위 무결성 등급의 주체가 상위 무결성 등급의 주체를 읽을 수 있도록 허가하므로 상위 무결성 등급의 객체가 하위 무결성 등급의 주체에 노출될 수 있다.




<그림 2> 접근 제어 비교

<그림 2>에서 비밀성을 보장하기 위한 접근 제어는 상위 보안 등급의 객체가 보다 하위 보안 등급으로 떨어지는 경로를 차단한다. 그리고 무결성을 보장하기 위한 접근 제어는 하위 무결성 등급의 객체가 상위 무결성 등급을 갖게 되는 경로를 차단한다.

본 연구에서 정의한 접근 제어에서 하위 보안 등급의 주체가 상위 보안 등급의 주체를 읽지 못하도록 하여 상위 보안 등급의 정보가 하위 보안 등급의 주체로 노출되는 것을 차단한다. 주체가 지금까지

읽은 객체의 보안 등급에 대한 정보를 바탕으로 제한적인 쓰기를 허가한다.

주체의 보안 등급과 같은 보안 등급의 객체를 읽었을 때는 쓰기를 허가하고 읽은 객체의 보안 등급이 주체의 보안 등급보다 낮은 때에는 생성을 허가한다. 이때 생성된 객체는 이미 읽은 객체보다는 높은 보안 등급을 갖도록 한다. 또한 주체와 같은 보안 등급의 객체를 읽지 않은 객체는 하위 등급으로 쓰기를 허가한다.

<표 1> 비밀성과 무결성을 보장하는 접근 제어

| 허용 정책 / 접근 구분 | | 비밀성 | 무결성 | 비밀성/무결성 |
|---|---|---|---|---|
| 읽기 | 상위 등급 읽기 | × | | × |
| | 하위 등급 읽기 | | × | |
| 쓰기 | 하위 등급으로 쓰기 | × | | △ |
| | 같은 등급으로 쓰기 | | | △ |
| | 상위 등급으로 쓰기 | | × | × |

(×:허가하지 않음, △:제한적 허가)

<표 1>에서 보듯이 본 연구의 접근 제어는 비밀성을 보장하기 위여 주체는 상위 등급의 객체를 읽지 못하도록 하였고, 상위 등급의 객체를 읽어서 하위 등급의 객체에 쓰지 못하도록 하기 위하여 쓰기는 상위 등급의 객체를 읽지 않은 경우만 허가하였다.

무결성을 보장하기 위한 성질은 쓰기에 관련한 성질로서 상위 등급의 객체로 쓰기를 금지한다. 그러나 읽은 객체 보다 상위 등급의 새로운 객체를 생성하는 것은 허가한다. 따라서 읽은 객체와 같은 등급으로 쓰기를 허가하고, 읽은 객체보다 상위 등급과 하위 등급으로 쓰기는 제한적으로만 허가한다.

## VI. 결 론

본 연구는 다중 프로그래밍을 지원하는 시스템에서 비밀성과 무결성을 보장할 수 있는 안전한 접근 경로를 위한 접근 제어를 정의하였다. 안전한 접근 경로란 정보의 불합리한 노출과 변경이 허가되지 않는 경로를 말한다.

본 연구에서 정의한 접근 제어는 비밀성을 보장하기 위하여 읽기 성질에서 하위 등급의 주체는 상위 보안 등급의 객체를 읽을 수 없도록 하였다. 쓰기 성질에서 상위 등급의 주체를 읽어서 하위 등급으로 쓰기를 허가하지 않았다.

무결성을 보장하기 위하여 하위 등급의 주체는 상위 등급의 객체에 쓰기를 금지하였다. 그러나 새로운 파일을 생성할 때 새로운 파일은 이미 읽은 파일보다 비밀성이 높아지도록 하였다. 주체가 읽은 객체의 보안 등급에 따라 읽은 객체와 같은 등급으로의 쓰기 성질과 읽은 객체보다 상위 등급으로의 생성 성질로 구별하여 상위 보안 등급으로 쓰기는 허가하지 않지만 상위 보안 등급으로 새로운 파일을 생성하는 것은 허가하였다.

본 연구에서 정의한 접근 제어는 보안 커널을 구성하기 위한 시스템 함수로 작성되어 비밀성과 무결성을 보장하기 위한 보안 시스템을 구축할 수 있을 것이다.

## 참고 문헌


[1] 차성덕, Trusted System 설계 및 평가 방법, NETSEC-KR95, Tutorial No.2, Jun 1995.

[2] Bell, D. E. and La Padula, L. J. Secure Computer Systems: Methemetical Foundations and Models, MITRE Report MTR 2547, 1973.

[3] D. Elliott Bell, Secure Computer Systems : A Retrospective, IEEE Symposium on Security and Privacy, pp.161-162, 1983.

[4] Biba, K. J. Integrity Considerations for Secure Computer System, US Air Force Electronic System Division, 1977.

[5] Anthony Boswell, Specification and Validation of a Security Policy Model, IEEE Transactions on Software Engineering. Vol.21, No.2, pp.63-68, Feb 1995.

[6] John E. Dobson and John A. McDermid, A Framework for Expressing Models of Security Policy, IEEE Symposium on Security and Privacy, pp.229-239, 1989.

[7] Deborah D. Downs, Jerzy R. Rub, Kenneth C. Kung and Carole S. Jordan, Issues in Discretionary Access Control, IEEE Symposium on Security and Privacy, pp.208-218, 1985.

[8] Morrie Gasser and Van Nostrand Reinhold, BUILDING A SECURE COMPUTER SYSTEM, 1988.

[9] Carl E. Landwehr, Formal Models for Computer Security, ACM Computing Survey, Vol13, No,3, pp. 247-278, Sept, 1981.

[10] J. Landaur and T. Renmond, A Framework for Composition of security Models, IEEE Symposium on Security and Privacy, pp.157-166,1992.

[11] Chales P. Pfleeger, SECURITY IN COMPUTING, Prentice-Hall, 1989.

[12] Ben L. Di Vito, Paul H. Palmquist, Eric R. Anderson, and Michael L. Johnston, Specificatiion and Verification of the ASOS Kernel, IEEE Symposium on Security and Privacy, pp.61-73, 1990.