6. 강제적 접근통제 모델

1. BLP 모델 - Bell Lapadula(벨 라파듈라) 모델

BLP의 개념	• 1973년, 미국의 Bell과 Lapadula가 개발한 **최초의 수학적 모델**이다. • **군사용 보안** 구조의 요구를 충족시키기 위하여 개발된 잘 알려진 모델이다. • 정보의 불법적 변조보다는 **기밀성 유지**에만 중점을 두고 있다. • 보안 등급을 이용한 **강제적** 보안 정책에 의한 접근통제 모델이다. • 정보가 높은 보안 레벨로부터 낮은 보안 레벨로 흐르는 것을 차단한다. • 정보를 "극비(top secret), 비밀(secret), 미분류(unclassified)"로 분류한다. • No-read-up 정책과 No-write-down 정책이 적용된다.
BLP의 정책	**① 상위레벨 읽기금지 정책(No-read-up policy, NRU) : [단순 보안 속성]** • 보안 등급이 낮은 주체는 보안 등급이 높은 객체를 읽을 수 없다. • 정보의 기밀성 보호는 가능, 무결성 보호는 불가능 • 읽기 행위는 할 수 없으나 쓰기 행위는 할 수도 있다는 뜻이 된다. • 주체는 사용자(프로세스 등), 객체는 파일(데이터베이스 등)을 지칭한다. **② 하위레벨 쓰기금지 정책(No-write-down policy, NWD) : [*-속성]** • 보안 등급이 높은 주체는 보안 등급이 낮은 객체에 쓰기(기록)를 할 수 없다. • 인가 받은 보안 등급 이하의 정보를 수정하지 못하게 하는 보안정책이다. • 읽기는 가능, 쓰기는 불가능 **• 정보의 기밀성 보호** **높은 보안 등급의 주체가 자신이 접근 가능한 비밀정보를 낮은 등급으로 복사(쓰기)하여 정보를 유출시키는 행위를 금지한다.**
BLP의 문제점	• BLP 모델은 정보의 기밀성만을 최대로 고려하였다. • BLP 모델은 정보의 불법적인 변조에 대한 해결책을 제시하지 못했다.**(무결성 결여)** • 즉, 접근통제의 관리적인 측면이 고려되지 않았다. • 기밀성 보호를 위해 No-read-up과 No-write-down 정책만을 제시하였다. • BLP 모델은 No-read-down과 No-write-up에 대한 내용은 없다. • BLP 모델에서는 낮은 보안등급의 주체가 높은 보안등급의 객체에 읽기 행위는 할 수 없으나 쓰기 행위는 할 수도 있다는 뜻이 된다. • BLP 모델은 정보의 무결성이 보호되지 못할 수도 있다. • 이러한 행위를 Blind write라고 하며, • 이러한 BLP의 문제점을 해결한 모델이 Biba integrity 모델이다.

2. Biba 모델

Biba 개요	• Biba integrity**(무결성)** 모델이라고도 한다. • 정보의 **불법 변조 방지**를 정의한 최초의 상업적 모델이다. - BLP 모델의 문제점 해결 • 낮은 보안 등급에서 높은 보안 등급으로 쓰기(기록)하지 못하도록 한다. • 예를 들면, **소령은 소장**이 취급하는 문서에 쓰기를 할 수 없다. • 높은 무결성 정보가 낮은 무결성 정보와 결합되는 무결성 훼손 방지 • No-write-up 정책과 No-read-down 정책이 적용된다.
Biba 의 정책	**① 상위레벨 쓰기금지 정책(No-write-up policy) : [*-무결성 원리]** • 주체는 자신의 무결성 접근등급보다 높은 객체에 쓰기를 할 수 없다. • 높은 무결성을 가진 정보의 훼손을 방지하기 위한 것이다. • 자신의 무결성 접근등급보다 높거나 같은 수준의 객체만 읽을 수 있다. **② 하위레벨 읽기금지 정책(No-read-down policy) : [단순 무결성 원리]** • 주체는 자신의 무결성 접근등급보다 낮은 객체는 읽을 수 없다. • 낮은 수준의 문서가 인용되는 것을 방지한다.

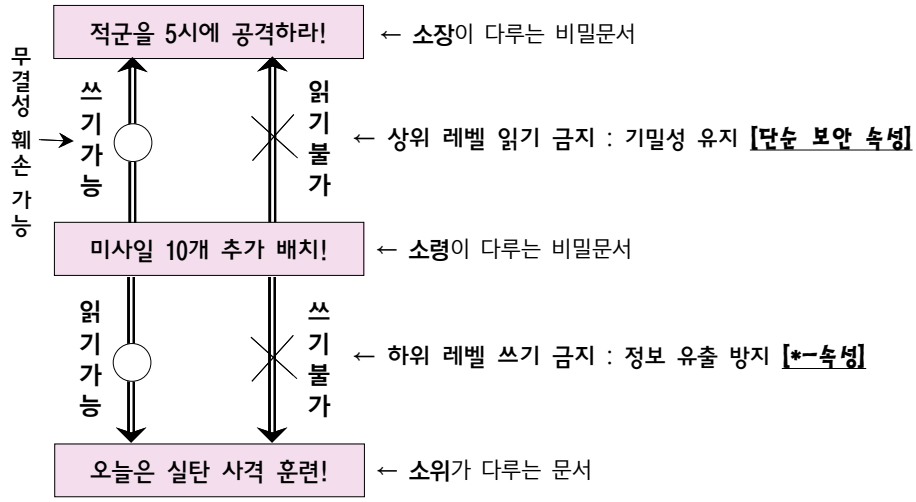
• 높은 보안 수준을 유지하려면,

• BLP(기밀성)와 Biba(무결성) 모델을 동시에 구현해야 한다. ← BLP/Biba **융합** 접근통제모델

3. Clark-Wilson 모델

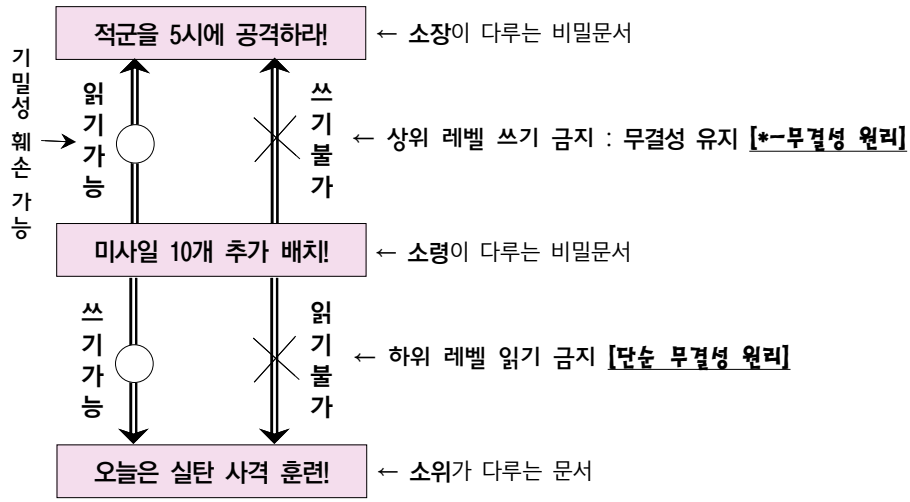
Clark-Wilson 의 개념	• **불법적인 정보 변조를 방지**하기 위한 접근통제 모델이다. • **상업 환경**에 적합하게 개발된 접근통제 모델이다. • 금융자산 관리 및 회계 분야에 주로 사용한다.**(무결성 중심)** • Biba Integrity 모델보다 더 진화한 **무결성 강조** 모델이다. • 주체는 직접 객체에 접근할 수 없고, • 주체는 허가된 프로그램을 통하여 객체에 접근할 수 있다.
Clark-Wilson 의 정책	**① 정형 거래(well-formed transaction)** • 체계화된 거래를 위한 접근통제 모델이다. • 모든 거래 사실을 철저히 기록하여 **불법적인 거래를 방지**한다. • 거래 사실을 완전하게 관리할 수 있는 자료처리 정책이다. **② 임무 분할(separation of duty)** • 인가자의 부적절한 정보 변조를 방지하는 **직무분리**를 반영한다. • 어느 한 사람만이 한꺼번에 모든 정보를 처리하지 않고 • 여러 사람이 각 부문별로 나누어 처리하는 정책이다. • 정당한 사용자의 **비인가된 행동을 예방**한다.

◉ BLP 모델 – 기밀성 위주



• 상위 레벨 문서에 쓰기가 가능하면, 보안 등급이 높은 문서의 무결성이 훼손될 수 있다.
• [*-속성] = star property = confinement property 라고도 한다.

◉ Biba 모델 – 무결성 위주



기출문제 분석

1. 접근통제(access control) 모델에 대한 설명으로 옳지 않은 것은? [2016년 지방 9급]

① 임의적 접근통제는 정보 소유자가 정보의 보안 레벨을 결정하고 이에 대한 정보의 접근 제어를 설정하는 모델이다.
② 강제적 접근통제는 중앙에서 정보를 수집하고 분류하여, 각각의 보안 레벨을 붙이고 이에 대해 정책적으로 접근제어를 설정하는 모델이다.
③ 역할 기반 접근통제는 사용자가 아닌 역할이나 임무에 권한을 부여하기 때문에 사용자가 자주 변경되는 환경에서 유용한 모델이다.
④ Bell-LaPadula 접근통제는 비밀노출 방지보다는 데이터의 무결성 유지에 중점을 두고 있는 모델이다.

♤ **Bell-LaPadula 접근통제**

- Bell-LaPadula 접근통제는 비밀노출 방지 모델이다. - **기밀성**

정답 : ④

2. Bell-LaPadula 보안 모델의 *-속성(star property)이 규정하는 것은? [2016년 국가 9급]

① 자신과 같거나 낮은 보안 수준의 객체만 읽을 수 있다.
② 자신과 같거나 낮은 보안 수준의 객체에만 쓸 수 있다.
③ 자신과 같거나 높은 보안 수준의 객체만 읽을 수 있다.
④ 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있다.

♤ **보안 규칙**

단순 보안 속성 (ss-property)	• 상위레벨 읽기금지 정책(No-read-up policy, **NRU**) • 주체는 자신보다 높은 보안 등급의 객체를 읽을 수 없다.
***-속성 (star property)**	• 하위레벨 쓰기금지 정책(No-write-down policy, **NWD**) • 주체는 자신보다 낮은 보안 등급의 객체에 정보를 쓸 수 없다.
강한 *-속성 (strong star property)	• star property를 더욱 강화한 보안 규칙 • 주체는 자신과 보안 등급이 다른 객체에 대해 읽거나 쓸 수 없다.

- 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있다.**(*-속성)**

↓ **다르게 말하면**

- 자신보다 보안 등급이 낮은 보안 수준의 객체에 쓸 수 없다.**(*-속성)**

정답 : ④

3. BLP(Bell & La Padula) 모델에 대한 설명으로 가장 옳지 않은 것은? [2018년 서울 9급]

① 다단계 등급 보안(Multi Level Security) 정책에 근간을 둔 모델이다.
② 기밀성을 강조한 모델이다.
③ 수학적 모델이다.
④ 상업용 보안구조 요구사항을 충족하는 범용 모델이다.

♤ **접근통제정책 모델**

• 상업 환경에 적합하게 개발된 접근통제 모델로 Clark-Wilson 모델이 있다.

정답 : ④

4. 컴퓨터 보안의 형식 모델에 대한 설명으로 옳은 것은? [2017년 법무부 9급]

① Bell-LaPadular 모델은 다중 수준 보안에서 높은 수준의 주체가 낮은 수준의 주체에게 정보를 전달하는 것을 다루기 위한 것이다.
② Biba 모델은 데이터 무결성을 위한 것으로, 사용자 자신과 같거나 자신보다 낮은 무결성 수준의 데이터에만 쓸 수 있고, 자신과 같거나 자신보다 높은 무결성 수준의 데이터만 읽을 수 있도록 한 것이다.
③ Bell-LaPadular 모델은 이해 충돌이 발생할 수 있는 상업용 응용프로그램을 위해 개발되었으며, 강제적 접근 개념을 배제하고 임의적 접근 개념을 이용한 것이다.
④ Clark-Wilson 모델은 강력한 기밀성 모델을 제안하며, 데이터 및 데이터를 조작하는 트랜잭션에 높은 수준의 기밀성을 제공한다.

♤ **접근통제**

---

① Bell-LaPadular 모델은 다중 수준 보안에서 높은 수준의 주체가 낮은 수준의 주체에게 정보를 전달하는 것을 다루기 위한 것이다.**(×)**
→ Bell-LaPadular 모델 : 하위레벨 쓰기금지 정책(No-write-down Policy, NWD)
→ 보안 등급이 높은 주체는 보안 등급이 낮은 객체에 쓰기(기록)를 할 수 없다.
③ Bell-LaPadular 모델은 이해 충돌이 발생할 수 있는 상업용 응용프로그램을 위해 개발되었으며, 강제적 접근 개념을 배제하고 임의적 접근 개념을 이용한 것이다.**(×)**
→ Bell-LaPadular 모델 : 강제적 접근 개념 사용하고, 상업용 위한 개발이 아님
④ Clark-Wilson 모델은 강력한 기밀성 모델을 제안하며, 데이터 및 데이터를 조작하는 트랜잭션에 높은 수준의 기밀성을 제공한다.**(×)**
→ Clark-Wilson 모델 : 강력한 무결성 모델을 제안

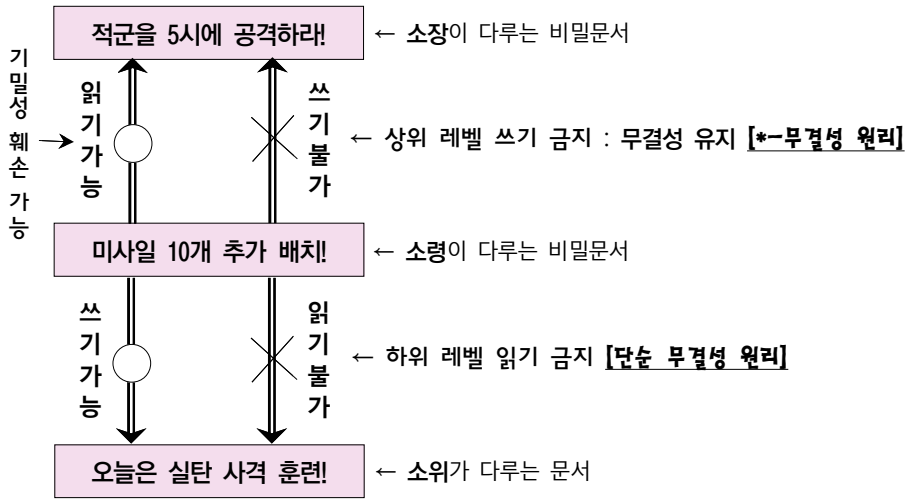
정답 : ②

5. Biba 보안 모델에 대한 설명으로 옳은 것은? [2019년 국가 7급]

① 이해가 상충되는 회사들 간의 정보흐름이 일어나지 않도록 고안되었다.
② 자신의 보안 수준보다 낮거나 같은 수준의 객체만 읽을 수 있다.
③ 자신의 보안 수준보다 높거나 같은 수준의 객체에만 쓸 수 있다.
④ 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.

♤ Biba 보안 모델 - 무결성 위주

- Biba 보안 모델은 **Biba integrity**(무결성) 모델이라고도 한다.
- Biba 보안 모델은 정보의 불법 변조 방지를 정의한 모델이다. - BLP 모델의 문제점 해결



① 상위레벨 쓰기금지 정책(No-write-up Policy) : [*-무결성 원리]
- 주체는 자신의 무결성 접근등급보다 높은 객체에 쓰기를 할 수 없다.
- 높은 무결성을 가진 정보의 훼손을 방지하기 위한 것이다.
- 자신의 무결성 접근등급보다 높거나 같은 수준의 객체만 읽을 수 있다.

② 하위레벨 읽기금지 정책(No-read-down Policy) : [단순 무결성 원리]
- 주체는 자신의 무결성 접근등급보다 낮은 객체는 읽을 수 없다.
- 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.
- 낮은 수준의 문서가 인용되는 것을 방지한다.

정답 : ④

6. 다음에서 설명하는 접근제어 모델은? [2019년 지방 9급]

군사용 보안구조의 요구사항을 충족시키기 위해 개발된 최초의 수학적 모델로 알려져 있다. 불법적 파괴나 변조보다는 정보의 기밀성 유지에 초점을 두고 있다. '상위레벨 읽기금지 정책(No-Read-Up Policy)'을 통해 인가받은 비밀 등급이 낮은 주체는 높은 보안 등급의 정보를 열람할 수 없다. 또한, 인가받은 비밀 등급 이하의 정보 수정을 금지하는 '하위레벨 쓰기금지 정책(No-Write-Down Policy)'을 통해 비밀 정보의 유출을 차단한다.

---

① DAC(discretionary access control) 모델
② Bell-LaPadula 모델
③ Biba 모델
④ RBAC(role-based access control) 모델

♤ **Bell-LaPadula 모델**

• 주어진 설명은 Bell-LaPadula 모델에 대한 설명이다.
• Bell-LaPadula 모델은 최초의 수학적 모델로 알려져 있다.

정답 : ②

7. 접근제어(access control)에 대한 설명으로 옳지 않은 것은? [2022년 국가 7급]

① 임의적 접근제어(discretionary access control)는 정보 소유자가 정보의 보안 수준을 결정하고 그에 대한 접근제어까지 설정한다.
② BLP(Bell-LaPadula) 모델과 Biba 모델은 강제적 접근제어(mandatory access control) 모델에 해당한다.
③ 역할기반 접근제어(role-based access control)는 사람이 아닌 역할 또는 직책에 권한을 부여한다.
④ BLP 모델에서는 낮은 수준의 보안 권한을 가진 사람이 자신의 권한보다 높은 보안 수준의 문서에 쓸 수 없다.

♤ **접근제어 – BLP 모델**

• BLP 모델에서는 **낮은** 수준의 보안 권한을 가진 사람이 자신의 권한보다 **높은** 보안 수준의 문서에 **쓸 수 없다.(×) → 쓸 수 있다.**
① 상위레벨 읽기금지 정책(No-read-up policy, NRU) : 단순 보안 속성, 쓰기는 가능
② 하위레벨 쓰기금지 정책(No-write-down policy, NWD) : *-속성

정답 : ④