5. 접근통제 정책

접근통제는 비인가자의 불법적인 접근으로 변조, 파괴 등의 행위를 차단하기 위한 것이다.

- **임의적** 접근통제(DAC, discretionary access control) – 자율적인, 자유재량에 의한 통제
- **강제적** 접근통제(MAC. mandatory access control) – 의무적인, 법에 정해진 통제
- **역할기반** 접근통제(RBAC, role based access control) – 업무, 직무, 하는 일에 의한 통제

◈ DAC / MAC / RBAC 요약

	정책 기본 원리	특징	장단점
DAC	신분-기반 접근통제 정책	• 정보 **소유자**가 사용자나 사용자가 속한 그룹에 임의적 접근제어를 설정한다. • 대부분의 OS에서 채택(유닉스 등)	• 객체단위 권한설정 가능 • 유연성이 있다. • 트로이 목마에 취약 • id가 도용되면 DAC는 파괴
MAC	규칙-기반 접근통제 정책	• **관리자만** 사용자에게 접근권한을 부여할 수 있다. • 시스템 사용자들은 자신의 정보에 대한 어떠한 접근권한도 설정할 수 없다. • 정부, 군 같은 복잡한 시스템에 사용된다.	• 객체단위 권한설정 불가 • 강력한 통제를 부여 • DAC에 비해 안전 • 일반적인 환경에서 사용하기 어렵다.
RBAC	역할-기반 접근통제 정책	• **조직의 변화에 따른 보안 관리**에 용이하다. • 사용자와 자원을 직접 연관시키지 않고, 사용자가 속한 그룹에 부여된 역할을 통해 자원에 접근하도록 하는 방식이다. • 정부, 금융, 통신, 의료 등 다양한 분야에 최근 적용되고 있다.	• 직무 순환이 빈번하게 발생하고, 보호해야 할 자산과 사원수가 많은 대규모 조직에 적합하다. • 보안 관리가 단순하다.

	DAC	MAC	RBAC
보안 주체	소유자	시스템	역할
통제 주체	권한 위임	보안 등급	참조 모니터
사용자 통제	복잡, 유연	단순	유연
적용하는 곳	운영체제	군, 정부 기관	(대)기업

1. 임의적 접근통제(DAC, discretionary access control) - 자율적인, 자유재량에 의한

① DAC는 자원에 대한 **소유권**과 자원에 대한 접근 요청은 **사용자 계정(ID)에 기반**을 한다.
- 소유자가 사용자의 신분에 근거하여 임의로 접근을 제어하는 방식이다.(융통성 있다)
- 각 객체에 대하여 접근권한을 추가하거나 철회할 수 있다.(임의적)
- DAC는 **자율적 정책**이라고도 한다.

② 사용자는 자원 관련 접근통제목록(ACL)에 의해 자원 대한 접근권한을 부여 받을 수 있다.
- ACL은 Access Control List 약어이다.
- 쉽게 말하면, ACL은 각 사용자의 권한을 관리하기 위한 테이블이다.
- ACL을 통해 파일에 대한 읽기, 쓰기, 실행 등이 수행된다.

③ DAC에서 사용자가 객체의 소유자일 때는 다른 사용자에게 권한을 부여할 수 있다.
- 용어 "임의적"은 객체 소유자의 판단에 의해 다른 사용자에게 권한을 부여하는 것이다.

④ DAC는 **객체를 복사하여도 객체의 접근통제 정보가 전파되지 않는다.**
- 허가권이 전파되지 않는다.
- 하나의 주체(사용자)와 객체(자원)에 대한 관계를 정의하므로

⑤ 하나의 주체, 객체 단위로 접근권한을 설정할 수 있다.
- 모든 주체, 객체에 대한 접근권한은 일정하지 않다.
- 주체가 소속된 그룹의 ID에 근거하여 객체에 대한 접근을 제한한다.

⑥ DAC는 **트로이 목마 공격에 취약점**이 있다.
- DAC는 신분에 근거하므로 데이터(악성코드)의 의미에 대한 지식이 없으므로

⑦ DAC는 Windows, 유닉스, 리눅스 등에서 적용되고 있다.
- 리눅스의 방화벽인 TCP Wrapper, iptables 등에서 네트워크 서비스에도 적용할 수 있다.
- TCSEC의 등급 C는 신분-기반 접근통제 정책으로 DAC를 적용한다.
- TCSEC는 미국의 정보보호제품 평가기준이다.(뒤이서 구체적으로 다룬다)

2. 강제적 접근통제(MAC. mandatory access control) - 의무적인, 법에 정해진

① MAC는 주어진 **규칙에 기반**하여, 자동적으로 수행되는 접근통제 방법이다.
- MAC는 원래의 **객체에 부여된 허가권은 복사된 객체에서도 동일하게 유지**된다.**(전파)**

② MAC에서는 사용자들의 자원에 대한 접근권한은 관리자로 부터 부여받는다.
- 오직, 관리자만 설정된 보안 정책에 따라 사용자에게 접근권한을 부여할 수 있다.
- 관리자만이 시스템 객체의 **보안레벨**과 사용자의 보안등급을 수정할 수 있다.

③ MAC에서는 강제적인 정책에 의해 주체와 객체가 갖는 **보안등급**을 정의한다.
- 하나의 주체, 객체 단위로 접근권한을 설정하기 어렵다.

④ MAC는 높은 보안을 요구하는 객체가 낮은 보안수준의 주체에게 노출되지 않도록 한다.
- 소장이 취급하는 고급 비밀문서는 낮은 보안수준의 소령에게 노출되지 않도록 한다.
- 어떤 객체(자원)에 접근하려 할 때 양자의 보안레이블 정보에 기초한다.

⑤ 최상위 **보안등급**을 가졌다 하더라도 모든 자료를 다 볼 수 없도록 차단한다.
- **알 필요성의 원칙**에 의거하여 필요한 사용자에게만 자료를 볼 수 있도록 한다.
- 그룹 a의 정보는 그룹 b의 top secret 권한을 가진 사용자가 접근할 수 없다.

⑥ 분류(classification)된 자원에 대하여 보안을 한층 더 강화한다.
- 분류된 자원에 대해 각자 별도로 관련된 정보를 모아 보관한다.(category)

⑦ MAC는 정부, 군 같은 복잡한 조직에 적용한다.

◈ 알 필요성의 원칙(need to know)

- 시스템 주체들이 업무 수행에 필요한 최소량의 정보를 사용하도록 한다.
- 최소권한정책(minimum privilege policy)이라고도 한다.
- 시스템 주체들의 객체 접근에 강력한 통제를 부여하게 된다.
- 단점으로, 정당한 주체에게 불필요하게 과한 접근통제를 부여하게 된다.

---

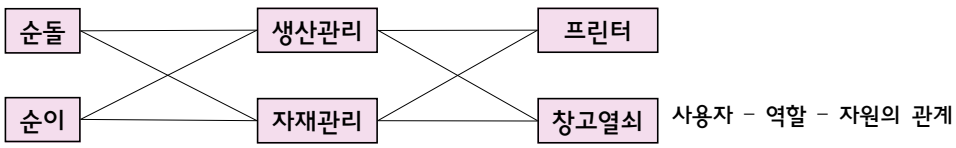
3. 역할기반 접근통제(RBAC, role based access control) - 업무, 직무, 하는 일

① RBAC는 조직 내에서 **역할(직무)**을 기반으로 하는 접근통제이다.
- 비임의적 접근통제(non-discretionary access control)라고도 한다.
- 각 사용자의 접근권한은 사용자가 속한 **그룹**에 할당된 역할에 기초한다.
- RBAC는 임의적 또는 강제적 접근제어 방식으로 구현 가능하다.

② 관리자는 각 사용자에게 직접 접근권한을 부여하지 않는다.
- 관리자는 **그룹에 권한을 부여**하고, 사용자를 그룹별로 분류한다.**(계정 그룹이 중요)**
- 그룹이 수행해야 할 역할(업무)을 정의한다. 역할에 따라 권한이 부여된다.
- 접근통제 관리에 부담을 줄일 수 있다.

③ 사용자가 속한 그룹에 할당된 **역할**과 연관성을 가진다.
- 사용자 역할에 의해 자원에 접근할 수 있고, 아울러 특정한 작업들을 수행할 수 있다.
- RBAC는 500명 이상의 직원이 있는 기업에서 많이 사용하고 있다.
- RBAC는 사용자가 자주 변경되는 환경에는 적합한 모델이다.
- 역할은 환경 변화에 따라 자연스럽게 생성 및 재구성될 수 있다.

④ RBAC 특징
- RBAC는 직무 기반 접근통제 정책으로 초기 관리의 오버헤드를 줄일 수 있다.
- RBAC는 인사담당자, 영업담당자 등과 같이 권한 그룹을 통해 접근을 제어한다.
- RBAC에서 사용자(users)와 역할(roles)의 관계는 **다 대 다** 관계이다.
- RBAC에서 역할과 자원(resources)도 **다 대 다** 관계이다.



사용자 - 역할 - 자원의 관계

◈ **접근통제 정책 정리**

정책	모델	특징
DAC	• 접근제어행렬 • 접근가능목록 • 접근제어목록	• 주체가 객체에 대한 접근권한을 자율적으로 결정 • 자율적으로 다른 주체에게 권한을 부여하거나 철회 가능 ↓ ↓ **보안 취약점** ↓ • 악의적인 목적에 이용 가능**(트로이 목마)**
MAC	• BLP 모델 : 기밀성 • Biba 모델 : 무결성	• 관리자에 의한 **보안 등급** 결정 ↓ ↓ **엄격한 보안 제한** ↓ • 다중사용자 보안요구사항 표현에 부적절 • 일반적인 분야 적용은 부적절
RBAC	• T-RBAC (Task-RBAC)	• 객체에 대한 접근권한은 사용자 역할(업무)에 기반 ↓ ↓ **상업적 측면이 강화된 정책** ↓ • 직원 500명이상의 기업에 사용

• RBAC는 설정에 따라 임의적 또는 강제적 접근제어 요소를 가질 수 있다.(중립적)

◈ **접근제어에서 전파(propagate) 유무 - 상속**

임의적 접근제어(DAC)	• 객체를 복사하여도 객체의 접근통제 정보가 전파되지 않는다. • 허가권이 전파되지 않는다.
강제적 접근제어(MAC)	• 객체에 부여된 허가권은 복사된 객체에서도 동일하게 유지된다. • 허가권이 전파된다.
역할기반 접근제어(RBAC)	• 역할에 대한 계층을 두어 허가권 전파가 가능하다. • 역할기반은 임의적 또는 강제적 접근제어 방식으로 구현 가능하다.

기출문제 분석

1. 자원의 접근제어 방법 중 강제적 접근제어(MAC)에 해당하는 것으로 옳은 것은? [2016년 국회 9급]

① 자원마다 보안 등급이 부여된다.
② 사용자별로 접근권리를 이전할 수 있다.
③ UNIX 운영체제의 기본 접근제어 방식이다.
④ 조직의 역할에 따라 접근권한을 부여하는 방식이다.
⑤ 자원의 소유자가 자원에 대한 접근권한을 설정한다.

♤ **접근제어**

① 자원마다 보안 등급이 부여된다. → 강제적 접근제어(MAC)
② 사용자별로 접근권리를 이전할 수 있다. → 임의적 접근제어(DAC)
③ UNIX 운영체제의 기본 접근제어 방식이다. → 임의적 접근제어(DAC)
④ 조직의 역할에 따라 접근권한을 부여하는 방식이다. → 역할기반 접근제어(RBAC)
⑤ 자원의 소유자가 자원에 대한 접근권한을 설정한다. → 임의적 접근제어(DAC)

정답 : ①

2. 다음 설명에 해당하는 접근제어 정책은? [2014년 국가 7급]

한 개체(entity)가 자신의 의지로 다른 개체의 자원에 접근할 수 있는 권한을 승인받을 수 있다.

① MAC(Mandatory Access Control)
② DAC(Discretionary Access Control)
③ ACL(Access Control List)
④ RBAC(Role Based Access Control)

♤ **임의적 접근통제**

• DAC는 사용자가 객체의 소유자일 때는 다른 사용자에게 권한을 부여할 수 있다.

정답 : ②

3. 다음 설명에서 제시하는 접근제어 정책은? [2020년 국회 9급]

----<보기>----------

주체 또는 소속 그룹의 아이디(ID)에 근거하여 객체에 대한 접근 제한을 설정한다.
객체별로 세분화된 접근제어가 가능하고,
유연한 접근제어 서비스를 제공할 수 있어 다양한 환경에서 폭넓게 사용되고 있다.

---

① 강제적 접근제어(mandatory access control)
② 규칙 기반 접근제어(rule based access control)
③ 역할 기반 접근제어(role based access control)
④ 임의적 접근제어(discretionary access control)
⑤ 래티스 기반 접근제어(lattice based access control)

♤ **접근제어 – DAC / MAC / RBAC 요약**

	정책 기본 원리	특징	장단점
DAC	신분-기반 접근통제 정책	• 정보 **소유자**가 사용자나 사용자가 속한 그룹에 임의적 접근제어를 설정한다. • 대부분의 OS에서 채택(유닉스 등)	• 객체단위 권한설정 가능 • 유연성이 있다. • 트로이 목마에 취약 • id가 도용되면 DAC는 파괴
MAC	규칙-기반 접근통제 정책	• **관리자만** 사용자에게 접근권한을 부여할 수 있다. • 시스템 사용자들은 자신의 정보에 대한 어떠한 접근권한도 설정할 수 없다. • 정부, 군 같은 복잡한 시스템에 사용된다.	• 객체단위 권한설정 불가 • 강력한 통제를 부여 → DAC에 비해 안전 • 일반적인 환경에서 사용하기 어렵다.
RBAC	역할-기반 접근통제 정책	• **조직의 변화에 따른 보안 관리**에 용이하다. • 사용자와 자원을 직접 연관시키지 않고, 사용자가 속한 그룹에 부여된 역할을 통해 자원에 접근하도록 하는 방식이다. • 정부, 금융, 통신, 의료 등 다양한 분야에 최근 적용되고 있다.	• 직무 순환이 빈번하게 발생하고, 보호해야 할 자산과 사원수가 많은 대규모 조직에 적합하다. • 보안 관리가 단순하다.

• DAC는 자원에 대한 소유권과 자원 접근을 요청하는 **사용자 계정(ID)에 기반**을 한다.
• DAC는 소유자가 사용자의 신분에 근거하여 임의로 접근을 제어하는 방식이다.(융통성 있다)
• DAC는 소유자가 각 객체에 대하여 접근권한을 추가하거나 철회 할 수 있다.(임의적)

정답 : ④

4. 역할기반 접근제어(RBAC)에 대한 설명으로 옳은 것은? [2020년 국가 7급]

① 정보의 소유자가 특정 사용자와 그룹에 특정 권한을 부여한다.
② 사용자에게 부여된 권한에 따라 사용자를 역할로 분류하여 각 사용자에게 하나의 역할만 할당되도록 한다.
③ 역할 및 역할이 수행할 권한을 정의하고, 사용자를 역할에 할당하는 방식이다.
④ 기밀문서가 엄격히 다루어져야 하는 군이나 정보기관 등에서의 중앙집중형 보안 관리에 적합하다.

♤ **역할기반 접근제어(RBAC)**

① **정보의 소유자**가 특정 사용자와 그룹에 특정 권한을 부여한다.**(×)**
→ **관리자**가 그룹에 권한을 부여하고, 사용자를 그룹별로 분류한다.
② 사용자에게 부여된 권한에 따라 사용자를 역할로 분류하여 각 사용자에게 하나의 역할만 할당되도록 한다.**(×)**
→ 각 사용자의 접근권한은 사용자가 속한 그룹에 할당된 역할에 기초한다.
④ 기밀문서가 엄격히 다루어져야 하는 군이나 정보기관 등에서의 중앙집중형 보안 관리에 적합하다.**(×)** → 정부, 군 같은 복잡한 조직에는 강제적 접근통제(MAC)를 적용한다.

◈ **접근통제 정책 정리**

정책	모델	특징
DAC	• 접근제어행렬 • 접근가능목록 • 접근제어목록	• 주체가 객체에 대한 접근권한을 자율적으로 다른 주체에게 부여하거나 철회 가능 ↓ ↓ 보안 취약점 ↓ • 악의적인 목적에 이용 가능(트로이 목마)
MAC	• BLP 모델 : 기밀성 • Biba 모델 : 무결성	• 관리자에 의한 보안 등급 결정 ↓ ↓ 엄격한 보안 제한 ↓ • 다중사용자 보안요구사항 표현에 부적절 • 일반적인 분야 적용은 부적절
RBAC	• T-RBAC (Task-RBAC)	• 객체에 대한 접근권한은 사용자 역할(업무)에 기반 ↓ ↓ 상업적 측면이 강화된 정책 ↓ • 직원 500명이상의 기업에 사용

정답 : ③

5. <보기>에서 설명하는 접근제어 모델로 가장 옳은 것은? [2020년 서울 7급]

----<보기>----------

시스템 자원이 얼마나 민감하고 중요한지를 나타내는 보안 레이블과 어떤 시스템 개체가 특정 자원에 접근할 수 있는지를 나타내는 보안 허가에 기반하는 접근제어 방식이다.

---

① 강제 접근제어(mandatory access control)
② 임의 접근제어(discretionary access control)
③ 역할기반 접근제어(role-based access control)
④ 속성기반 접근제어(attribute-based access control)

♤ **접근제어**

	정책 기본 원리	특징	장단점
DAC	신분-기반 접근통제 정책	• 정보 **소유자**가 사용자나 사용자가 속한 그룹에 임의적 접근제어를 설정한다. • 대부분의 OS에서 채택(유닉스 등)	• 객체단위 권한설정 가능 • 유연성이 있다. • 트로이 목마에 취약 • id가 도용되면 DAC는 파괴
MAC	규칙-기반 접근통제 정책	• **관리자만** 사용자에게 접근권한을 부여할 수 있다. • 시스템 사용자들은 자신의 정보에 대한 어떠한 접근권한도 설정할 수 없다. • 정부, 군 같은 복잡한 시스템에 사용된다.	• 객체단위 권한설정 불가 • 강력한 통제를 부여 → DAC에 비해 안전 • 일반적인 환경에서 사용하기 어렵다.
RBAC	역할-기반 접근통제 정책	• **조직의 변화에 따른 보안 관리**에 용이하다. • 사용자와 자원을 직접 연관시키지 않고, 사용자가 속한 그룹에 부여된 역할을 통해 자원에 접근하도록 하는 방식이다. • 정부, 금융, 통신, 의료 등 다양한 분야에 최근 적용되고 있다.	• 직무 순환이 빈번하게 발생하고, 보호해야 할 자산과 사원수가 많은 대규모 조직에 적합하다. • 보안 관리가 단순하다.

① MAC는 주어진 **규칙에 기반**하여, 자동적으로 수행되는 접근통제 방법이다.
→ MAC는 원래의 객체에 부여된 허가권은 복사된 객체에서도 동일하게 유지된다.**(전파)**
② MAC에서는 사용자들의 자원에 대한 접근권한은 관리자로 부터 부여받는다.
→ 오직, 관리자만 설정된 보안 정책에 따라 사용자에게 접근권한을 부여할 수 있다.
→ 관리자만이 시스템 **객체의 보안레벨과 사용자의 보안등급을 수정**할 수 있다.
③ MAC에서는 강제적인 정책에 의해 주체와 객체가 갖는 보안등급을 정의한다.
→ 하나의 주체, 객체 단위로 접근권한을 설정하기 어렵다.

정답 : ①

6. 다음 중 역할기반 접근제어(role-based access control)에 대한 설명으로 옳은 것은 몇 개인가? [2022년 군무원 9급]

ㄱ. 다중사용자 및 프로그래밍 환경에서의 접근제어를 위하여 사용자의 역할에 기반을 두고 통제하는 방식으로 강제적 및 임의적 접근제어를 보완한 방식이다.
ㄴ. 접근대상 정보를 보안등급을 지정하여 분류한다.
ㄷ. 접근제어 목록을 이용하여 각 객체에 대한 권한을 명시한다.
ㄹ. 사용자의 역할이 변경되면 이에 따른 접근제어 권한을 변경한다.

---

① 0개 ② 1개
③ 2개 ④ 4개

♤ **역할기반 접근제어**

ㄱ. 다중사용자 및 프로그래밍 환경에서의 접근제어를 위하여 **사용자**의 **역할**에 **기반**을 두고 통제하는 방식으로 강제적 및 임의적 접근제어를 보완한 방식이다. ← **역할기반 접근제어(1)**
ㄴ. 접근대상 정보를 **보안등급**을 지정하여 분류한다. ← **강제적 접근제어**
ㄷ. **접근제어 목록**을 이용하여 각 객체에 대한 권한을 명시한다. ← **임의적 접근제어**
ㄹ. **사용자**의 **역할**이 변경되면 이에 따른 접근제어 권한을 변경한다. ← **역할기반 접근제어(2)**

정답 : ③

7. 다음 중 접근제어 원칙으로 옳지 않은 것은? [2022년 군무원 9급]

① 통신규약 ② 최소 권한 ③ 알 필요성 ④ 직무 분리

♤ **접근제어 원칙**

// 알 필요성의 원칙(need to know)
- 시스템 주체들이 업무 수행에 필요한 **최소량의 정보**를 사용하도록 한다.
- **최소권한정책**(minimum privilege policy)이라고도 한다. - 강력한 통제 부여

// 직무분리(separation of duty)
- 인가자의 부적절한 정보 변조를 방지하는 **직무분리**를 반영한다. - **비인가된 행동을 예방**
- 어느 한 사람만이 한꺼번에 모든 정보를 처리하지 않고
- 여러 사람이 각 부문별로 나누어 처리하는 정책이다.

정답 : ②

8. 접근제어 모델에 대한 설명으로 옳지 않은 것은? [2022년 국가 9급]

① 접근제어 모델은 강제적 접근제어, 임의적 접근제어, 역할기반 접근제어로 구분할 수 있다.
② 임의적 접근제어 모델에는 Biba 모델이 있다.
③ 강제적 접근제어 모델에는 Bell-LaPadula 모델이 있다.
④ 역할기반 접근제어 모델은 사용자의 역할에 권한을 부여한다.

♤ **접근제어 모델**

· **임의적** 접근제어 모델에는 **Biba** 모델이 있다.(×)
→ **Biba**는 **강제적** 접근제어 모델이다.

정답 : ②

9. 접근제어 모델에 대한 설명으로 옳지 않은 것은? [2022년 국회 9급]

① 임의적 접근제어 기법은 자원의 소유자가 접근 주체를 결정한다.
② 강제적 접근제어 기법은 자원이 소속된 조직의 관리자가 접근권한을 결정한다.
③ 임의적 접근제어 기법은 보안 레이블을 기반으로 접근 가능 여부를 판단한다.
④ 강제적 접근제어 기법은 원래의 객체에 부여된 허가권이 복사된 객체에서도 동일하게 유지된다.
⑤ 임의적 접근제어 기법은 대부분의 운영체제에서 파일의 접근규칙을 정의할 때 활용한다.

♤ **접근제어 모델**

· 임의적 접근제어 기법은 **보안 레이블**을 **기반**으로 접근 가능 여부를 판단한다.(×)
→ **보안 레이블 기반**은 강제적 접근제어이다.
· 임의적 접근제어는 **접근제어 목록**을 이용하여 각 객체에 대한 권한을 명시한다.

정답 : ③