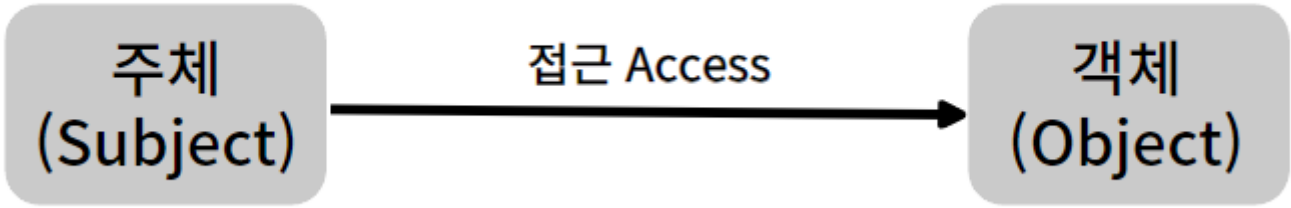
접근 제어

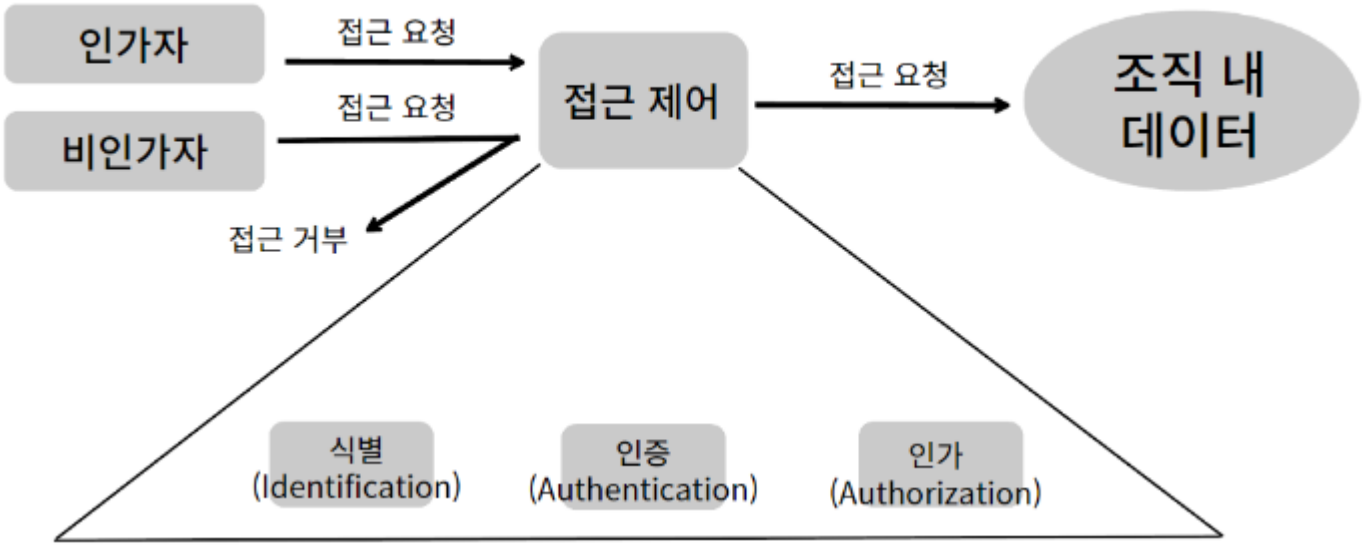
접근 제어

- 접근 제어란?
  - 적절한 권한을 가진 인가자만이 특정 시스템이나 정보에 접근할 수 있도록 통제하는 것
    - 접근 통제와 동의어
  - 접근 제어의 구성요소: 주체(Subject), 객체(Object), 접근(Access)



접근 제어

- 접근 제어의 과정
  - 식별: 자신이 누구인지 밝히는 것
    - 사용자 명, 계정 번호
  - 인증: 자신의 신원이 올바른지 증명하는 활동 또는 과정
    - 패스워드, 생체 인증
  - 인가: 사용자의 특정 객체에 대한 접근을 허용하는 과정
    - 보안 등급



접근 제어

- 인증
  - 지식: 주체는 그가 알고 있는 것을 보여줌
    - 패스워드, 핀(PIN)
  - 소유: 주체는 그가 가지고 있는 것을 보여줌
    - 토큰, 스마트 카드
  - 존재: 주체는 그가 나타내는 것을 보여줌
    - 생체 인증
  - 행위: 주체는 그가 하는 것을 보여줌
    - 서명, 움직임, 음성

접근 제어

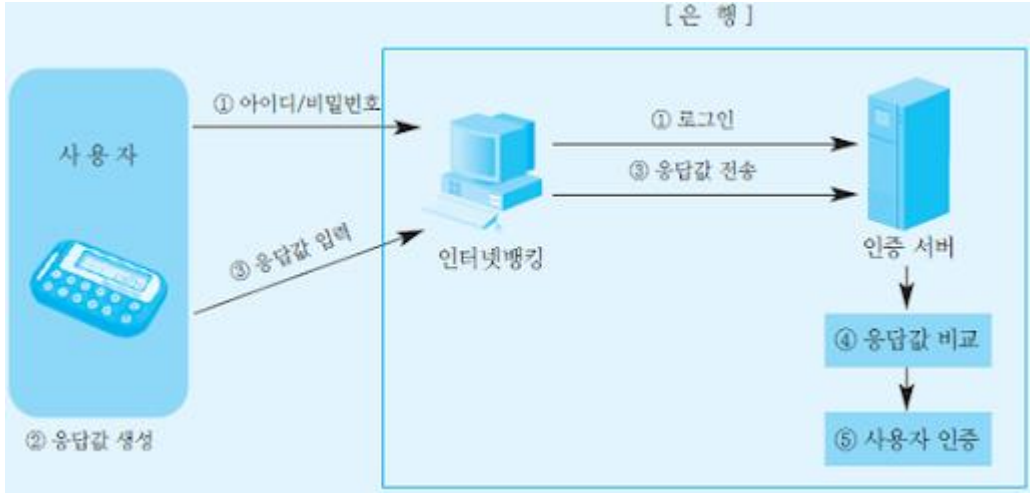
- 지식 기반 인증
  - 사용자가 알고 있는 정보에 의존하는 인증 기법
    - ID, 패스워드를 입력하여 인증하는 것이 이에 해당
    - 사용자의 신원 정보와 기존에 등록되어 있는 참조 지식을 비교하는 일대일 검증 사용
    - 편리하고 확실하며 관리 비용 또한 저렴한 편
    - 패스워드를 평문으로 저장 시 패스워드의 유출 가능성 있음
  - 패스워드 해시 저장
    - 실제 패스워드 추측 불가, 보안성 우수
    - 무차별 공격에 취약
  - 솔팅된 패스워드 해시 저장
    - 패스워드에 덧붙일 랜덤 문자열인 솔트(Salt)를 생성하고 이를 패스워드 해시 값 계산에 사용
    - 보안성 강화

접근 제어

- 소유 기반 인증
  - 사용자가 가지고 있는 인증 수단으로 인증하는 방식
    - 열쇠, 운전면허증 등
    - 도용의 위험성 때문에 지식 기반 기반 인증, 존재 기반 인증 방식과 함께 사용
      - ex) 신분증 얼굴 확인
    - 저렴한 비용으로 높은 신뢰성을 보장
    - 복제의 위험성이 있고 고장, 분실, 파손 등의 이유로 인증이 불가능할 수 있음
  - 스마트 카드
    - 고유한 식별 정보 저장, 이 정보를 처리할 하드웨어와 소프트웨어도 장착
    - 메모리, CPU, 카드 운영 체제 등도 포함
      - IC칩이 부착된 은행 카드
    - 정보 처리가 불가능 한 카드는 메모리 카드 또는 토큰이라고 함
      - 마그네틱 카드는 메모리 카드

접근 제어

- 소유 기반 인증
  - 일회용 패스워드(OTP: One – Time Password)
    - 인터넷 뱅킹 등 전자금융 거래를 할 때 무작위로 비밀번호를 생성하는 매체
      - 매우 높은 보안성
    - 인증 서버와 사용자의 OTP 생성기는 같은 시간을 시드(Seed)로 하여 같은 알고리즘을 통해 난수 생성하는 것으로 토큰 생성
    - 시간이 같도록 동기화하는 것이 중요
      - 주로 1분 단위



접근 제어

- 존재 기반 인증: 생체 인증
  - 지문, 망막, 홍채, 목소리, 얼굴 등
  - 생체 정보 리더기를 이용하여 생체 템플릿(Biometric template)이라고 불리는 자신의 생체 정보를 데이터베이스에 등록

구 분		인식원리	장점	단점
생체적	지문	• 개인의 지문 특성을 DB와 비교	• 편리하며 안전함 • 위조 불가능	• 땀, 먼지 등에 의한 인식률 저하
	홍채	• 망막 모세혈관 분포 패턴 분석 • 홍채 무늬, 형태 색깔 분석	• 낮은 오인식률 • 고도의 보안성 • 위조 불가능 • 분실위험 없음	• 불편(눈을 계속 뜨고 있어야 함) • 비위생적(안구질환 우려)
	얼굴	• 얼굴 요소의 특징 분석 • 눈, 코, 입 거리/얼굴의 열상/3차원 얼굴 영상 분석	• 위생적(비접촉식)이며 편리 • 시스템 비용 저렴	• 빛의 세기, 촬영 각도, 자세 등으로 인한 인식률 저하
	정맥	• 혈관 패턴의 특징을 파악 비교	• 편리, 복제 불가능	• 구축 비용 높음
행동적	음성	• 음성 특징을 DB와 대조해 개인 인증	• 편리, 전화나 인터넷으로 원격지에서 이용 가능	• 녹음을 통한 도움 가능성 • 목소리 상태에 따른 오인식
	서명	• 서명 과정(펜의 움직임, 속도, 압력) 모양 특징 분석	• 분실, 도난 위험 없음	• 서명 복제, 위조 가능

접근 제어

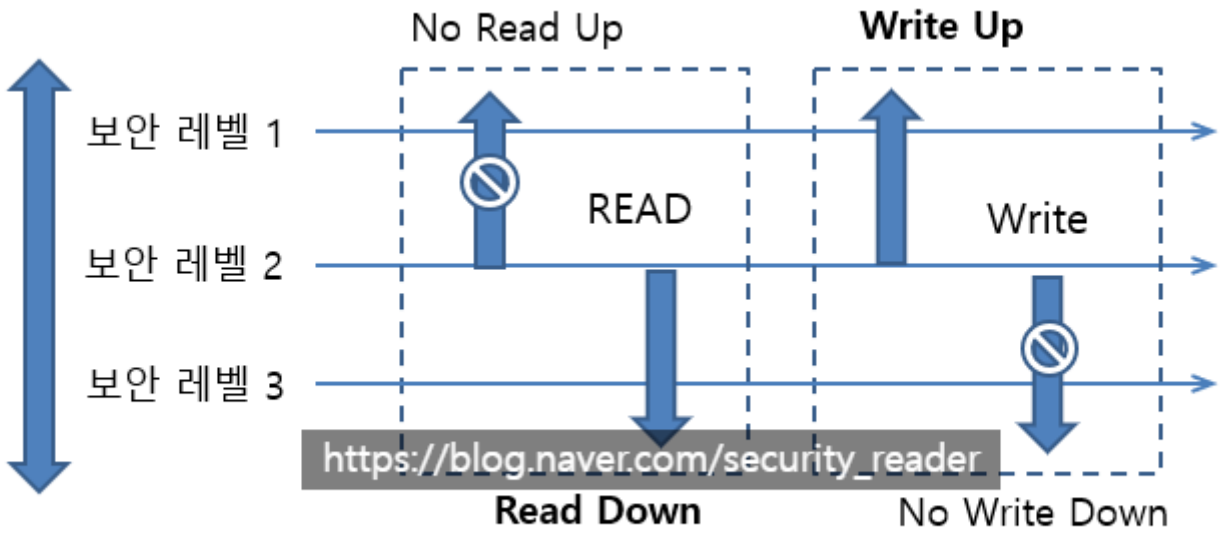
- 접근 제어의 모델
  - 강제적 접근 제어(MAC: Mandatory Access Control)
    - 벨-라파둘라(Bell-LaPadula)
    - 비바(Biba)
  - 임의적 접근 제어(DAC: Discretionary Access Control)
  - 비임의적 접근 제어(Non-Discretionary Access Control)
  - 그 외의 보안 모델들
    - 클락-윌슨(Clark-Wilson)
    - 만리장성(Chinese Wall)

접근 제어

- 강제적 접근 제어(MAC: Mandatory Access Control)
  - “모든 데이터에 레이블을 붙여서 통제하겠다.”
  - 조직에서 사용되는 데이터를 분류하여 각각 레이블을 붙이고, 각 레이블별로 정책을 설정
  - 보안 레이블 = 보안 수준 X 카테고리
    - 보안수준: 1급 비밀, 2급 비밀, 3급 비밀, 대외비, 평문
  - 매우 높은 보안 수준을 요구하는 군대에서 주로 사용

접근 제어

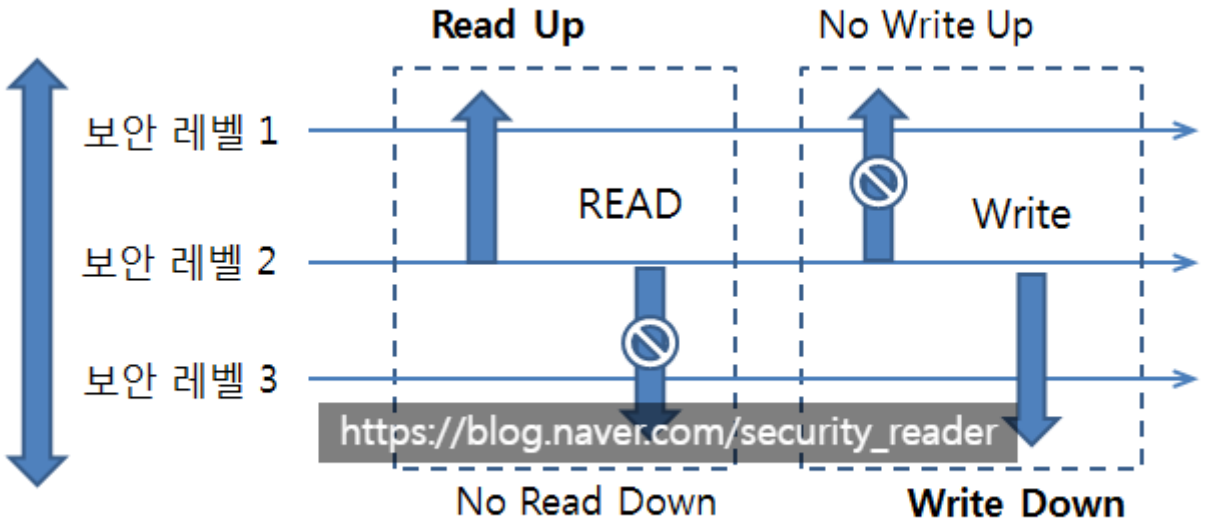
- 강제적 접근 제어(MAC: Mandatory Access Control)
  - 벨-라파둘라(Bell-LaPadula) 모델
    - 첫 번째로 제시된 수학적 보안 모델
    - NRU(No Read-Up), NWD(No Write-Down)
      - 보안 수준이 높은 데이터가 낮은 보안 수준으로 전파되는 것을 방지



BLP의 동작원리

접근 제어

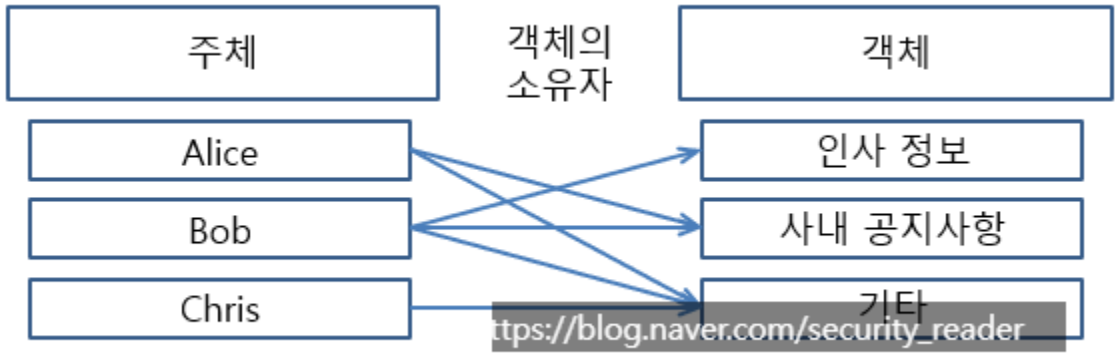
- 강제적 접근 제어(MAC: Mandatory Access Control)
  - 비바(Biba) 모델
    - 벨-라파둘라 모델과는 달리 데이터의 부적절한 변조 방지에 목적을 두고 있으며 보안 수준 대신에 무결성 수준(Integrity Level)이라는 용어 사용
    - NRD(No Read-Down), NWU(No Write-Up)
      - 높은 무결성 수준의 데이터가 낮은 무결성 수준의 데이터에 의해 손상되는 것을 방지



Biba의 동작원리

접근 제어

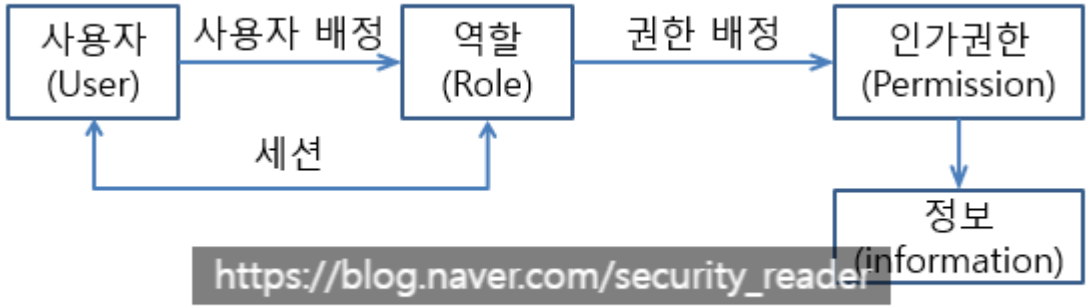
- 임의적 접근 제어(DAC: Discretionary Access Control)
  - 접근을 요청하는 사용자가 접근하려는 데이터(객체)에 대해서 접근 권한이 있는지 확인하여 접근 여부를 결정하는 접근 제어 방식
    - 특정 데이터에 대한 사용자가 접근 권한을 임의로 추가하거나 제거 가능해서 '임의적'이라는 용어 사용
  - 중앙 집중적인 관리가 어려워 엄격한 접근 제어가 어려움



DAC의 개념도

접근 제어

- 비임의적 접근 제어(Non-Discretionary Access Control)
  - 1970년대 다중 사용자, 다중 프로그래밍 환경에서의 보안 처리 요구를 만족하게 하려고 제안된 접근 제어 모델로 사용자의 역할에 기반을 두고 접근을 통제하는 모델
  - 기업 내의 잦은 부서 이동 등의 이유로 조직이 동적으로 변화하는 구조에 적합
  - RBAC(Role Based Access Control)와 동의어



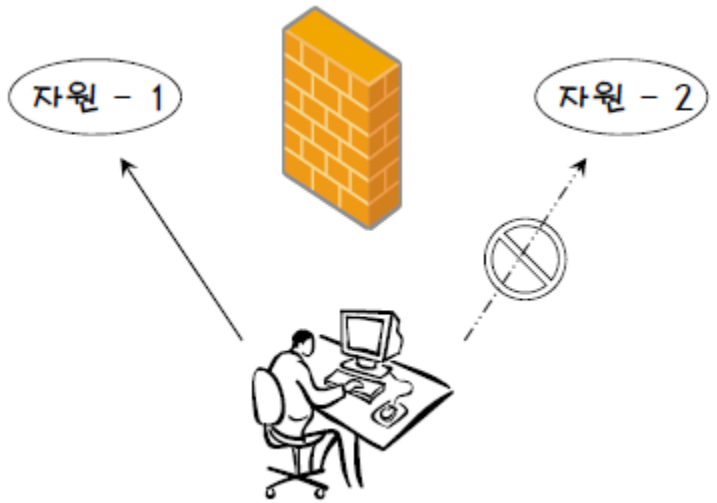
RBAC의 개념도

접근 제어

- 클락-윌슨(Clark-Wilson) 모델
  - 무결성의 3가지 목표를 모두 만족하는 접근 제어 모델
    - 비인가자들의 데이터 변형 방지: 비바 모델이 해결
    - 내/외부의 일관성 유지
    - 합법적인 사람에 의한 불법적인 수정 방지
  - 클락-윌슨 모델의 3가지 요소
    - 잘 구성된 트랜잭션
      - 모든 거래(Transaction) 사실을 구조화하고 예측 가능하며 안전한 방식으로 기록하는 것
    - 직무 분리
    - 사용자(주체)의 응용 프로그램을 통한 데이터 접근
      - 사용자가 직접 객체로 접근하는 것을 금지

접근 제어

- 만리장성(Chinese Wall) 모델
  - 브루어-나쉬(Brewer Nash) 모델과 동의어
  - 비즈니스 영역의 한 회사에 최근 일을 한 적이 있는 파트너는 동일한 영역에 있는 다른 회사의 자료에 접근해서는 안 된다는 개념이 핵심인 접근 제어 모델
  - 사용자의 이전 활동에 근거하여 동적으로 접근 제어 수행




Any Questions?