# 1 접근 통제 종류

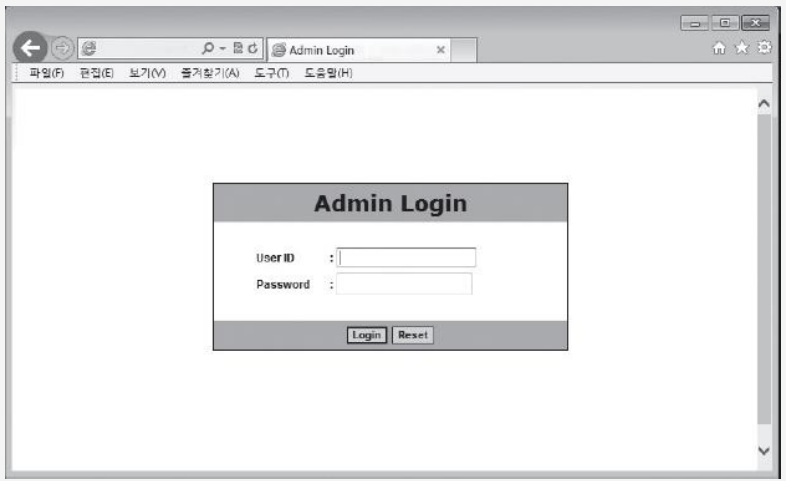
# 1 | 접근 통제 종류

## 1 수직적 접근 통제

- 특정 정보에 대한 접근 권한을 수준별로 상이하게 설계한 통제
- 대부분의 웹 사이트는 일반 사용자가 접근할 수 있는 기능 외에 일반 사용자가 접근할 수 없는 관리자 기능을 만들어 놓음(보안 레벨)

## 1 수직적 접근 통제

[수직적 접근 통제의 대표적인 예인 관리자 페이지]




관리자 페이지를 잘못 만들 경우?

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 수평적 접근 통제

- 웹 애플리케이션 내에 여러 사용자가 존재할 때
  상대방의 정보를 볼 수 없도록 통제하는 것(같은 레벨)
- 수평적 접근 통제에 대한 공격은 주로 URL에 노출되는
  자신의 식별 코드(Get Method)를 다른 사람의 것으로
  변경하거나 쿠키 또는 세션 값을 다른 사람의 것으로
  대체함으로써 이루어짐(Cookie Injection, 세션 하이재킹)

  - 예) 이메일, 인터넷 뱅킹

## 3 비즈니스 로직 접근 통제

- 사용자 권한에 종속되지 않고 민감하거나 중요한 자원에 대한 접근과 관련된 것(역할, 행위)

  - 예) 일반 사용자가 관리자 권한을 전부 획득하지 못했더라도 관리자만 접근할 수 있는 메뉴에 접근하는 경우

# 2 접근 통제 방법

## 1 접근제어

### 접근제어의 동기(접근통제)

- 컴퓨터의 발전으로 말미암아 문서, 혹은 물리적인 형태로 존재하던 많은 정보, 정보자원 들이 컴퓨터 안에 **디지털 데이터**의 형태로 존재하게 됨(아날로그)

- 이에 따라 조직의 민감한 정보들이 권한이 없는 사용자들에 의해 외부로 **누출, 변조, 파괴될 위험성**이 증가함(접근통제)

## 1 접근제어

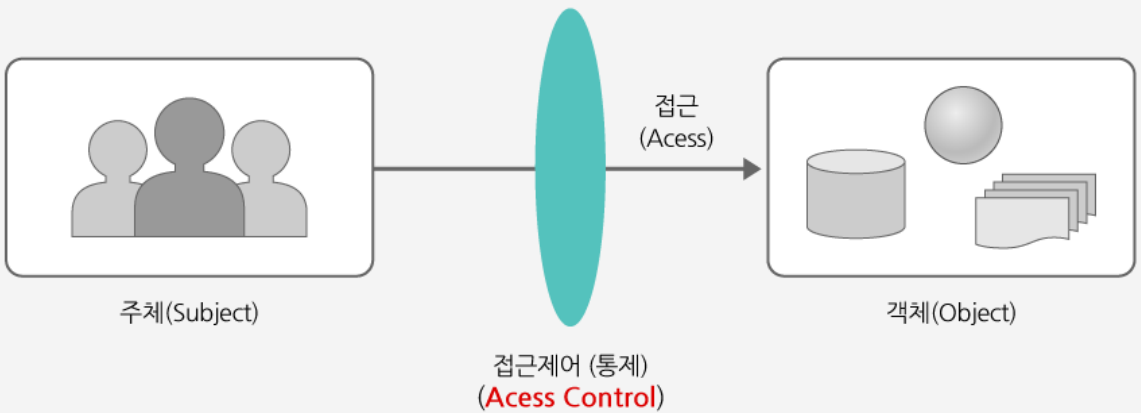
### 접근제어의 동기(접근통제)

- 어떻게 하면 사용자들이 자신의 권한에 맞는 정보만 접근할 수 있도록 통제할 수 있을까?
  (1,000명의 사용자와 100,000개의 파일이 있다면?)

- 접근제어는 외부 침입자가 아닌 **내부 사용자**에 대한 보안관리 분야임

## 1 접근제어

### 접근제어의 요소




※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 1 접근제어

### 접근제어의 요소

- 주체(Subject) : 사용자(User), 프로세스(Process)
- 객체(Object) : 파일(레코드, 필드),
  데이터베이스(테이블, 뷰-view,..),
  프로그램
- 접근(Access) : 읽기(Read), 쓰기(Write),
  변경(Update), 삭제(Delete),
  실행(Execute), 등등

## 1 접근제어

### 접근제어의 요소

- 접근제어(Access Control)
  : 주체가 객체에 접근을 요구했을 때
  이 요구를 수락할지, 거절할지를 결정하는 행위

  - 예) 사용자 ID가 ‘ S01 ’ 인 사용자가
    인사기록에 있는 주소를 변경하려고 할 때,
    이를 허용해야 하는가, 거절해야 하는가?

## 1 접근제어

### 접근제어의 요소

- 사용자의 접근을 허용할지 말아야 할지를 결정하는 근거는 그 **사용자에게 부여된 권한**이 어떤 것인가에 달려 있음

## 1 접근제어

### 접근제어의 요소

- 권한 관리를 어떻게 하느냐에 따라 여러 **접근제어 모델**이 있음(접근제어 보안모델)
  - 접근제어 표(ACM)/접근제어 리스트(ACL)
  - 강제적 접근제어(MAC : Mandatory Access Control)
  - 자율적 접근제어(DAC : Discretionary Access Control)
  - 역할기반 접근제어(RBAC : Role-Based Access Control)
  - 기타(ABAC : Activity-Based Access Control)

## 2 접근 통제 공격 기법

### ACM

Access Control Matrix(**ACM**)

| 객체 / 주체 | 성별코드 | 인사기록 | 주소정보 | … |
|---|---|---|---|---|
| Jane | R,W | | R | |
| John | R | R,W | R | |
| Sam | | R | R,W | |
| … | | | | |

(R:read, W:write)

※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### ACL

- Access Control List(**ACL**)

| | |
|---|---|
| Jane | 급여정보[R,W], 주소정보[R] |
| Jojn | 급여정보[R], 인사기록[R,W], 주소정보[R] |
| Sam | 인사기록[R], 주소정보[R,W] |

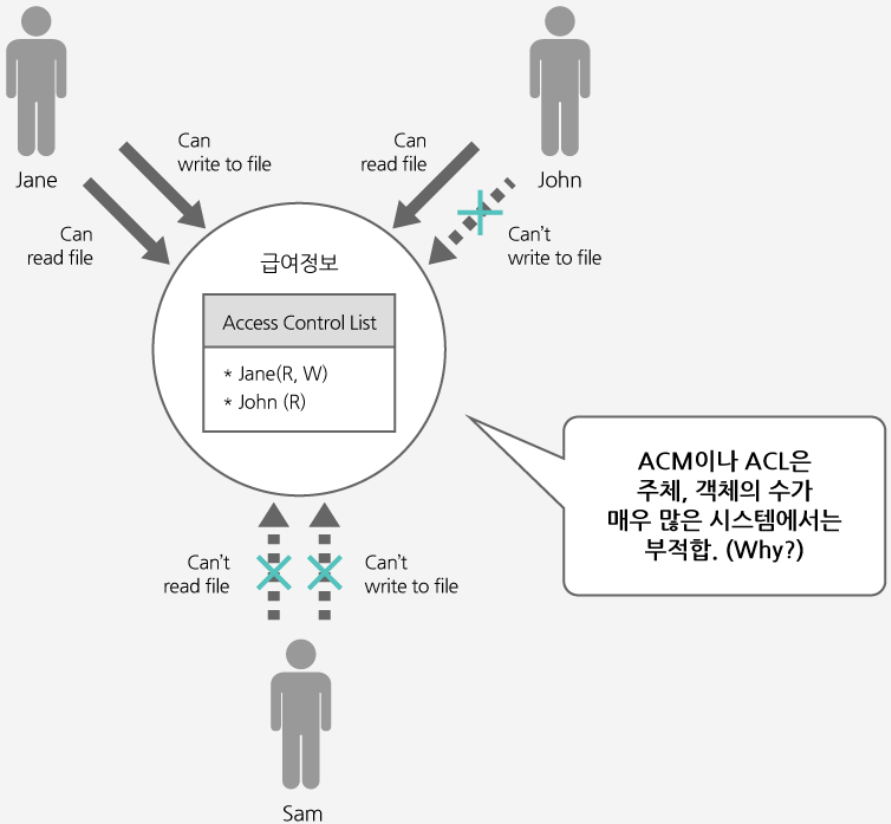
| | |
|---|---|
| 급여정보 | Jane[R,W], John[R] |
| 인사기록 | John[R,W], Sam[R] |
| 주소정보 | Jane[R], John[R], Sam[R,W] |

※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### ACL

- ACL을 이용한 접근제어의 예 (기하급수적 증가)




※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### ACL

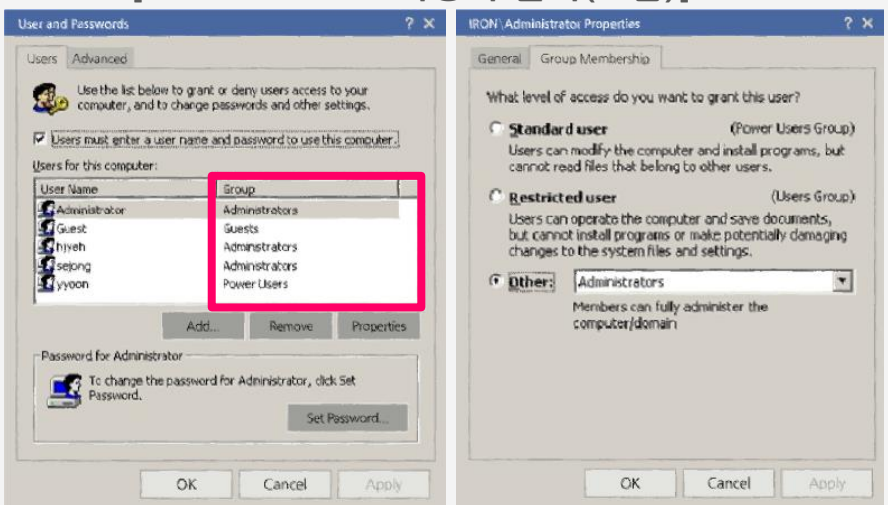
- ACL을 이용한 접근제어의 예
  - 일반적으로 서버급 OS 에서는 접근제어 리스트(ACL)를 사용함 (Unix, Window NT 계열) (복합 접근제어)
  - 접근제어 리스트의 약점을 보완하기 위해 그룹(Group) 개념을 추가하여 사용(vs. others)
  - 그룹(Group) : 비슷한 성격의 사용자들을 하나로 묶어서 그룹으로 지정하고, 개별 사용자에게 권한을 부여하는 대신 그룹에 권한을 지정(ex. admin., developer,..)

그룹에 권한을 지정하게나 삭제하면 그 그룹에 속한 모든 사용자에게 권한을 지정하거나 삭제하는 것과 동일한 효과

## 2 접근 통제 공격 기법

### ACL

[window 2000 사용자 관리(그룹)]




※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### MAC

- MAC 개요
  - Bell-LaPadula의 이론(**BLP 모델**)에 기초
  - 1970년대 초 미국 정부는 MITRE Corporation에 정보 누출위협에 대한 연구를 의뢰
  - 이 연구소의 연구원이었던 Elliott Bell과 Leonard LaPadula에 의해 보안 모델 발표(접근제어 모델, 접근제어 보안모델)

## 2 접근 통제 공격 기법

### MAC

- MAC 개요
  - 핵심 아이디어
    : **주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어 시 이 등급을 비교함으로써 접근의 허용여부를 판단 하게 됨**
  - 주로 **군사 환경**과 같은 엄격한 보안이 요구되는 분야에 적합

## 2 접근 통제 공격 기법

### MAC

- 보안레이블(**Security Label**)
  - 보안 레이블이란 컴퓨터 안에 존재하는 개체(Entity)들이 얼마나 보안상 중요한 가를 나타내는 속성을 말함
  - 보안 레이블들은 계층적인 등급을 이룸(위아래에 쓰거나 읽을 수 있는가?)

## 2 접근 통제 공격 기법

### MAC

▶ 보안레이블(Security Label)

- 군사 환경에서 보안 레이블의 예)
  - Top Secret
  - Secret
  - Confidential
  - Unclassified

- 상업 환경에서 보안 레이블의 예)
  - Restricted
  - Proprietary
  - Sensitive
  - Public

## 2 접근 통제 공격 기법

### MAC

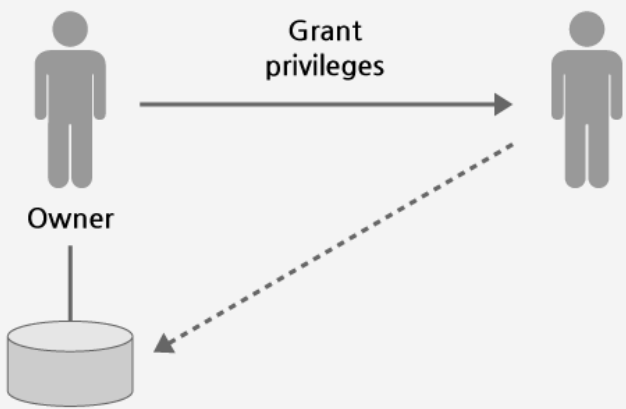
- 강제적 접근제어 모델의 적용 사례
  - DBMS 제품들
    : Trusted Oracle, Sybase secure SQL server, Informix Online/secure 5.0
  - UNIX system V/MLS 운영체제
  - Linux 보안 커널
  - 기타 보안 시스템 S/W

강제적 접근제어 모델은 '다단계 보안(MLS; Multi Level Security)' 으로도 불림

## 2 접근 통제 공격 기법

### DAC

- DAC 개요
  - 객체에 대한 소유권(Ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부, 혹은 일부를 다른 주체에게 부여(Grant)함
  - 적용 사례 : 관계형 데이터베이스(**RDBMS**) (레거시, 객체)

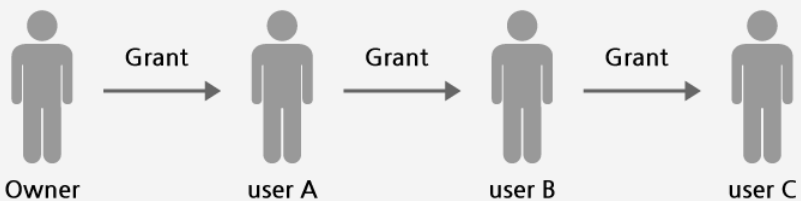



※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### DAC

- 자율적 접근제어에서의 이슈
  - 내가 제 3자로부터 부여 받은 권한을 다른 사용자에게 부여할 수 있는가? (옵션)
  - 권한이 여러 사용자에게 연이어 부여 됐을 때 이를 회수하면 어떤 일이 일어나야 하는가?




※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### RBAC

- RBAC 개요
  - 기업 환경으로부터 아이디어가 만들어짐
  - 기업 환경에서는 사용자가 기업 내에서 어떤 역할(**Role**)을 수행하고 있는가에 따라 권한이 정해짐
  - 이를 모델화 한 것이 역할기반 접근제어

## 2 접근 통제 공격 기법

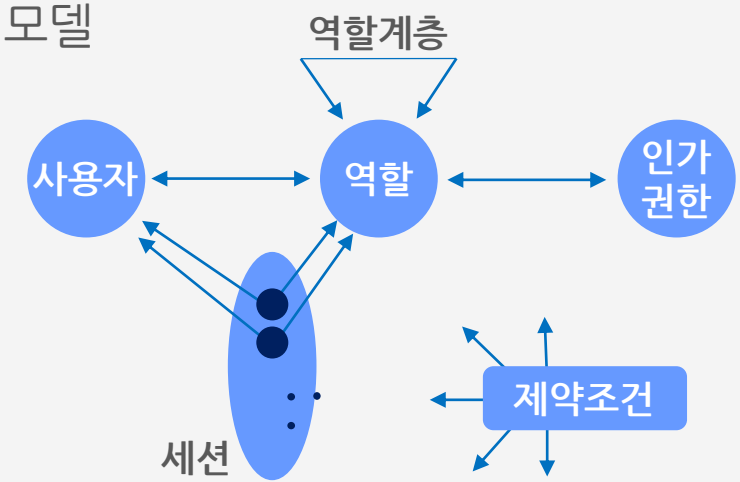
### RBAC

- RBAC 개요
  - 역할(**Role**)에 대한 개념은 컴퓨터 분야에서 오래 전부터 사용되었으나 본격적인 이론화는 90년대 이후에 이루어짐
  - 상용 제품 들에서 구현하는 사례가 점차 증가

## 2 접근 통제 공격 기법

### RBAC

RBAC 모델




※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### RBAC

- RBAC 모델
  - 사용자(**User**)
    : 시스템을 사용할 수 있도록 ID가 부여된 사람
  - 인가권한(**Permission**) : 사용자들이 쓸 수 있는 권한
    예) file 1 [r,w], file 2 [r]
  - 역할(**Role**)
    : 사용자들이 조직 내에서 부여 받은 직무, 위치
    예) 영업부장, 경리, 프로그래머, 제1팀장,..

## 2 접근 통제 공격 기법

### RBAC

- RBAC 모델
  - 세션(Session)
    : 사용자가 시스템에 로그인 함으로써,
    자신에게 부여된 권한들을 사용할 수 있는 상태를 유지하는 것(집에서 부장?)

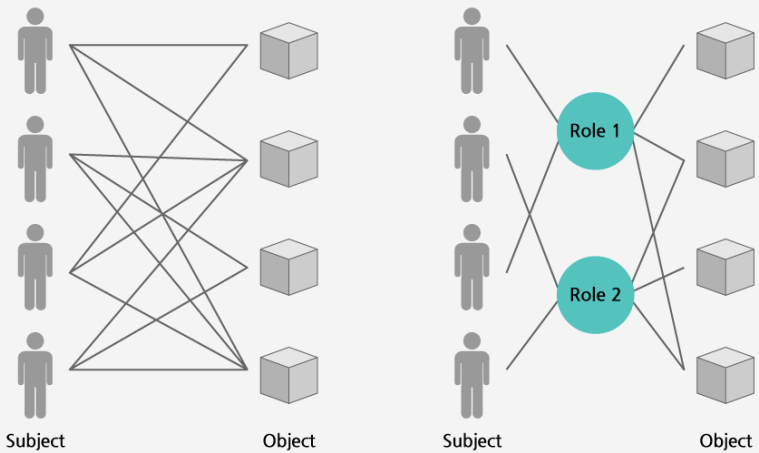
✓ RBAC에서는 권한을 직접 사용자에게 부여하는 대신 역할에 부여하고, 사용자들을 적절한 역할에 할당

✓ 결국 사용자들은 자신에게 부여된 역할을 통해 권한을 행사

## 2 접근 통제 공격 기법

### RBAC

#### RBAC 모델

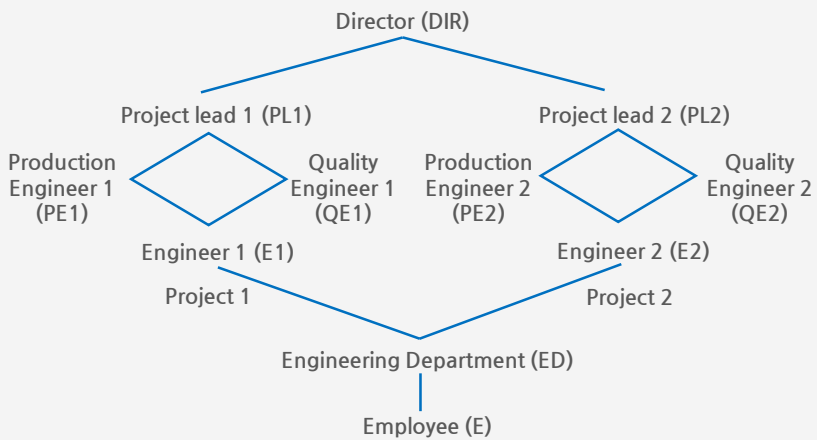



※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### RBAC

- RBAC 모델 - 역할 계층(Role Hierarchy)(기업)




※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD

## 2 접근 통제 공격 기법

### RBAC

- RBAC 모델
  - 제약조건(**Constraints**)

- 예)
  ‘경리’ 역할에는 3 인 이상의 사용자를 할당할 수 없음
  ‘경리’ 역할을 포함하는 세션은 오후 6:00 이후에는 사용할 수 없음

## 2 접근 통제 공격 기법

### RBAC

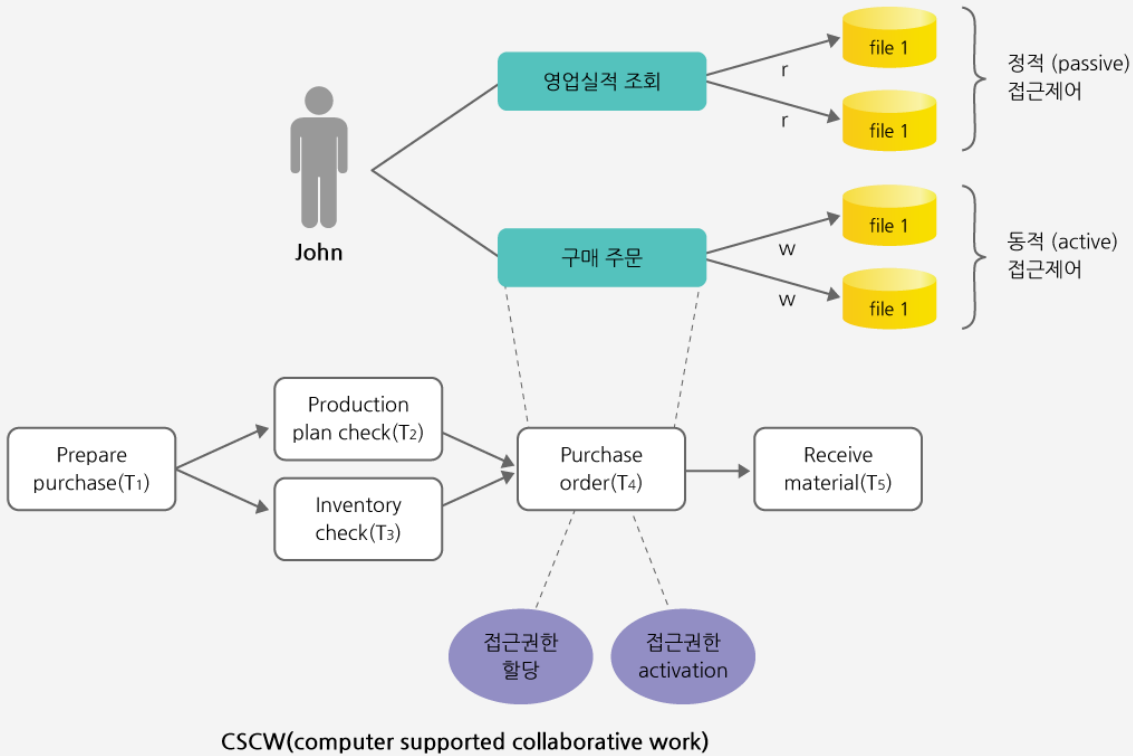
- RBAC 모델
  - 중요한 제약 조건 : 임무 분리(Separation Of Duty)
  - 권한이 한 사람에게 집중되었을 때 발생할 수 있는 권한 남용의 위험을 막기 위해 권한을 여러 사람에게 분산(실제 예?)

- 예)
  세금고지서 발행 ↔ 세금징수
  프로그램 개발 ↔ 프로그램 검수

## 2 접근 통제 공격 기법

### ABAC

- 행동기반(**Activity-Based**) 접근제어(정적, 동적)




※출처: cfile208.uf.daum.net/attach/110DBF344DBFD4D90B03DD