권한

- 윈도우 서버에서 권한은 파일/폴더에 접근하는 권한, 시스템을 제어하는 권한으로 구분

> 파일/폴더에 접근하는 권한 : permission

시스템을 제어한 권한 : user righ

permission(접근 권한)

- 파일이나 폴더에 지정

> 허가 or 거부 권한 설정 가능

- 보안 주체(사용자나 그룹, 컴퓨터 객체)를 접근 제어 목록에 추가하고 권한을 설정하여 사용

> 보안주체를 운영체제가 식별하기 위해 SID를 사용한다

\* SID

Security ID

사용자, 컴퓨터, 보안 그룹이 생성될 때 부여되는 식별 값

Domain ID와 RID로 구성

- 객체에 대한 접근을 허가하거나 거부하기 위해 사용되는 규칙

> 접근을 제어하기 위해 사용

- 로컬이나 도메인 계정에 권한이 설정될 수 있다

- 권한은 직접적으로 부여하거나 상속 받을 수 있고 암시적인 권한 설정을 이용할 수도 있다.

접근 제어 목록

- 권한을 부여하여 접근을 할 수 있도록 만드는 목록

> 권한 설정 화면

- ACE와 DACL 로 구분

> ACE : 적용되는 권한 값

> DACL : 보안 주체의 목록

기본 권한

- 읽기 및 실행 : 파일이나 폴더의 내용을 볼 수 있는 권한

- 쓰기 : 파일이나 폴더의 내용을 수정하는 권한

- 폴더 내용 보기 : 폴더 내용을 미리 볼 수 있게 하는 권한

- 읽기 : 속성을 읽을 수 있는 권한

- 수정 : 속성을 변경할 수 있는 권한

\* 특수 권한은 기본 권한을 세분화 시킨 권한이다

\* 읽기 및 실행, 폴더 내용 보기, 읽기 권한은 같이 적용 된다.

권한 상속

- 기본적으로 권한은 상속 된다.

> 폴더 안에 파일/폴더를 만들면 상위 폴더의 각종 속성들이 생생한 파일/폴더에 적용

- 상속된 권한 값은 수정할 수 없다.

- 필요에 따라 상속을 차단할 수 있다

> 상속을 차단하면 ACL을 유지하고 권한만 수정하거나 ACL을 초기화 할 수 있다.

허용 권한 & 거부 권한

- 허용은 작업을 허가해주는 권한, 거부는 작업을 하지 못하게 만드는 권한

- 허용과 거부가 함께 적용되면 거부가 우선

> a 사용자가 b 그룹과 c 그룹에 소속되어 있을때

b그룹에는 허용권한, c 그룹에 거부권한을 부여하면 a는 거부권한을 적용받는다.

- ACE에 없으면 기본적으로 거부권한 적용

> 단, 그룹에 구성원으로 들어가 있는 사용자가 ACE에 없고 그룹만 등록되어 있으면

그 사용자는 그룹의 권한을 적용받는다.

파일 복사/이동 작업 시 권한 상속

- 같은 파티션 (드라이브) 간의 복사/이동

복사를 할 경우 목적지 폴더의 권한이 상속된다.

이동을 할 경우 원래의 권한이 유지된다.

- 다른 파티션 (드라이브) 간의 복사/이동

복사/이동 전부 목적지 폴더의 권한이 상속된다.

\* 복사는 새로운 대상을 만들고 기존 내용을 읽어서 그대로 넣어주는 작업

> 새로운 항목이 생성되기 때문에 목적지의 권한을 상송

이동은 다른 파티션의 경우에는 복사 + 원본 삭제 작업이 진행

> 복사 작업에서 새로운 항목이 생성되기 때문에 목적지의 권한을 상송

같은 파티션의 경우에는 목적지 폴더에 아이콘만 새로 생성 후 기존 아이콘 삭제

> 아이콘은 실제 데이터가 위치한 저장 매체의 주소값을 갖고 있는 파일

목적지 폴더에 새로 생성한 아이콘에 주소값만 저장하기 때문에 자료가 새로 만들어지지 않음