커널에 의해 할당되고 커널만이 제어 가능한 커널 영역의 메모리 블록.

일반 - Process, Thread, Job

동기화 전용 - Mutex, Semaphore, Event, Waitable Timer

입출력 - File, Communication Device(COM, LPT…), Console, Mailslot, Pipe, Socket, IOCP, File Mapping, File Change Notification

보안 - Access Token, Window Station, Desktop

기타 - Heap, Moudule-DLL, Event log, Registry Key,...

커널 객체: 공통 헤더 + 개별 바디.

헤더: 객체 이름, 보안 기술자(액세스 토큰과 비교), 사용 계수(열린 핸들/객체 참조 카운트),...

동기화 여부: 객체 타입 멤버 필드. 커널 객체 자체가 동기화에 사용 될 수 있는지.

주요 API 일반적인 공통 사항

{

CreateXXX

커널객체 생성

PSECURITY\_ATTRIBUTE: 보안 기술자, NULL 이면 프로세스의 속성.

PCTSTR: 객체 이름

프로세스와 스레드는 이름 대신 ID로 식별해서 PCTSTR 없음.

프로세스간 공유가 되지 않는 커널 객체(IOCP 등)은 둘다 없음.

HANDLE 리턴.

~Ex: 접근 권한 설정 등. 기본 Create는 권한 기본값은 ALL\_ACCESS

OpenXXX

이미 생성된 객체 열기(공유)

성공할 때마다 사용계수 1 증가.

대부분이 Create와 같이 이름과 보안 접근 권한 지정 매개 변수 등을 받음.

HANDLE 리턴.

CloseHandle

매개변수

HANDLE: 닫을 커널 객체의 핸들.

호출마다 사용계수 1 감소. 0이 되면 커널 객체를 메모리에서 해제.

사용계수가 맞지 않아 해제가 안되면 메모리 누수가 발생 될수 있음.

기타 개별 커널 객체에 알맞은 전용 API

Suspend/ResumeThread, Read/WriteFile, SetEvent 등.

GetLastError()

}

HANDLE

어떤 커널 객체에 대한 HANDLE은 프로세스 마다 고유함. (같으면 우연)

프로세스 커널 객체 내의 커널 객체 핸들 테이블의 인덱스 값.

리턴값이 NULL 이면 실패. GetLastError()