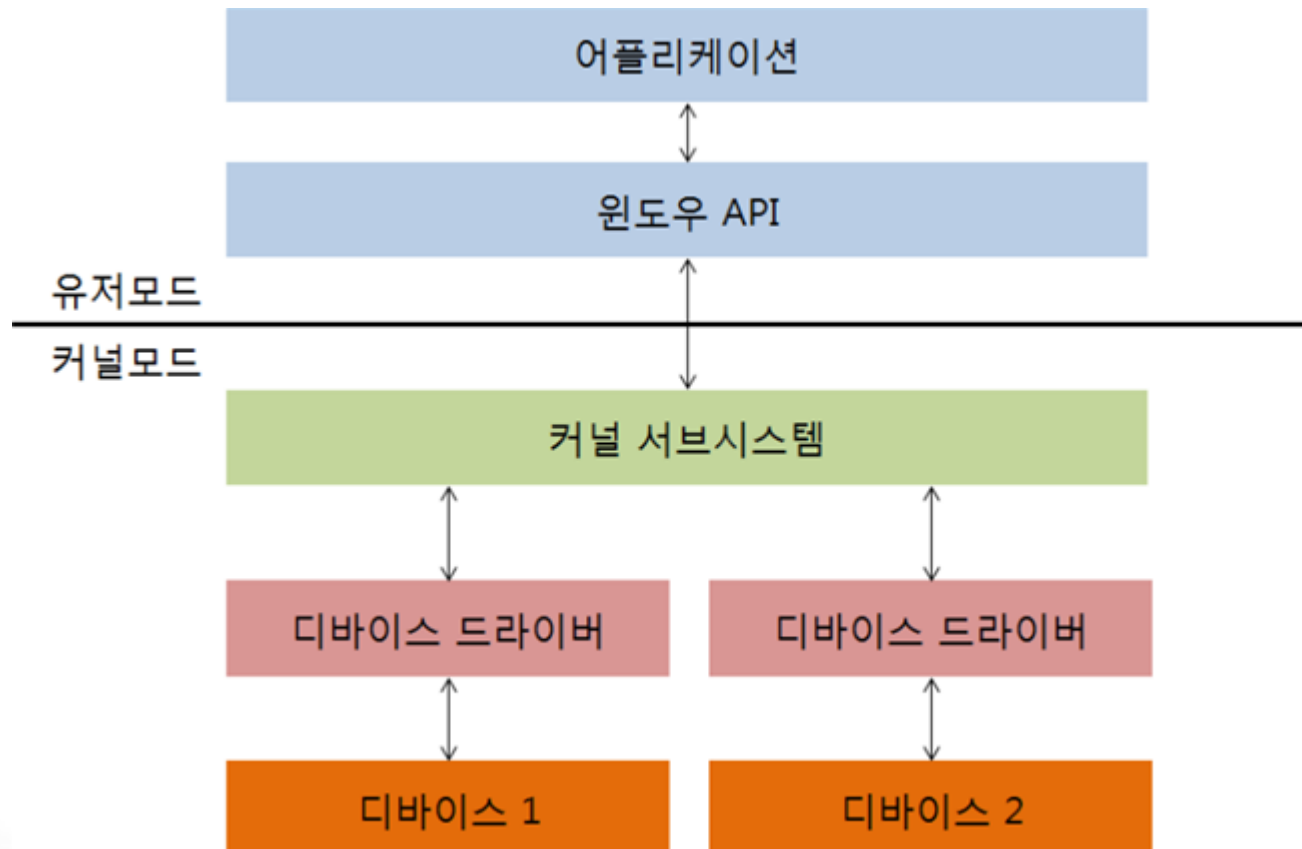

주간 보고

Finger Keyboard - Keyboard Filter Driver

프레C맨 

윈도우 디바이스 드라이버 계층구조

윈도우 핵심 운영체제 아키텍처 – 2장 드라이버의 기본



윈도우 디바이스 드라이버 계층구조

윈도우 핵심 운영체제 아키텍처 – 2장 드라이버의 기본

1) 유저모드와 커널모드

어플리케이션과 어플리케이션에서 사용되는 API의 경우 유저모드에서 작동
드라이버는 일반적으로 커널 모드에서 실행

2) 어플리케이션과 윈도우 API

어플리케이션은 커널 모드 구성 요소에 대해 직접적으로 접근 할 수 없다.
윈도우 API를 이용해서 I/O를 발생시켜 디바이스로부터 필요한 정보 획득



3) 커널 서브 시스템

핵심 윈도우 기능을 처리하는 부분

4) 드라이버와 디바이스

드라이버는 커널 서브 시스템과 디바이스 간의 인터페이스 제공,

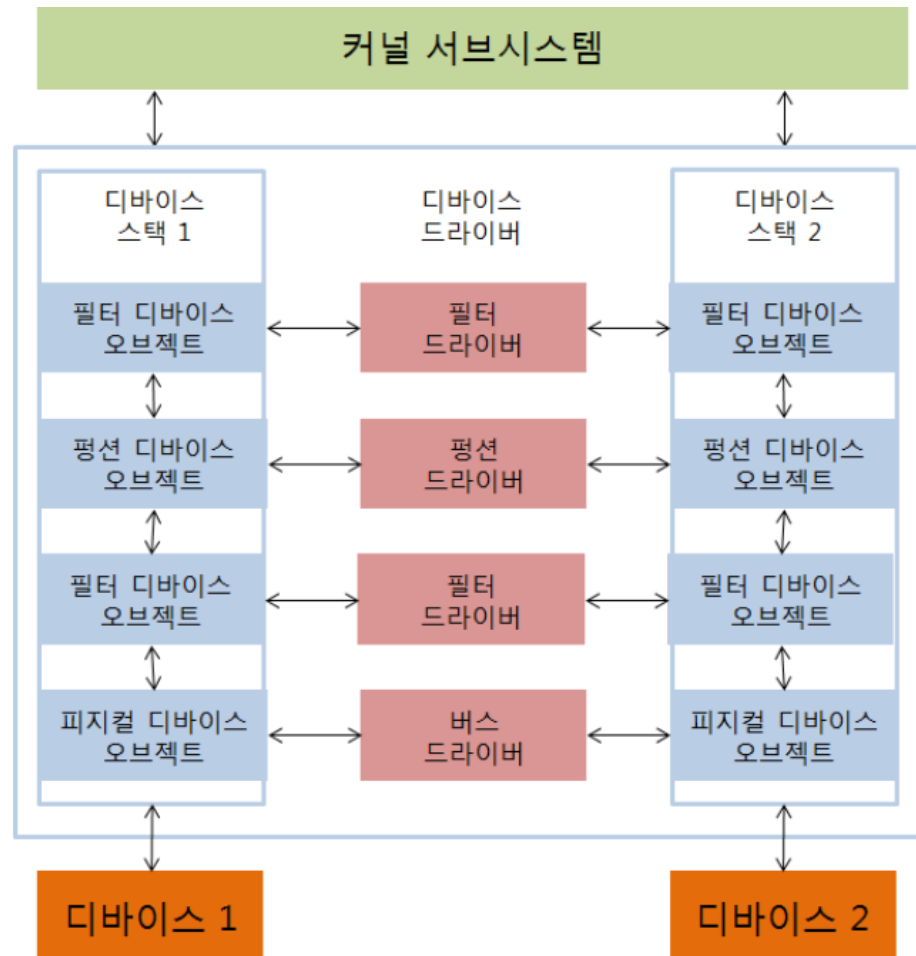
커널 서브 시스템이 I/O를 특정 디바이스에 대해 요청

드라이버는 요청을 처리, I/O를 생성한 커널 서브 시스템에게 데이터를 돌려줌



윈도우 디바이스 드라이버 계층구조

디바이스 스택



커널 서브 시스템이 특정 디바이스에 대한 I/O를 요청할 경우
하나 이상의 드라이버가 I/O를 처리
각각의 드라이버는 처리과정 참여여부를 나타내는
디바이스 오브젝트를 가지고 있음
각각의 디바이스 오브젝트는 드라이버가 해당 I/O를 처리하기 위한
디스패치 함수들의 포인터를 포함하고 있고 각각을 처리 함



디바이스 스택은 이러한 처리과정을 위해 필요

디바이스는 각각의 디바이스 스택을 가지고,

각각의 디바이스 스택은 디바이스 오브젝트를 정렬하여 가지고 있음

하나의 디바이스는 하나의 디바이스 스택만을 가질 수 있으며

드라이버들은 여러 디바이스 스택에 참여 할 수 있음.



1) DriverEntry : 디바이스 드라이버가 메모리에 상주

```
// 드라이버가 메모리에 상주할때 호출됩니다
NTSTATUS
DriverEntry
(
    IN PDRIVER_OBJECT DriverObject,
    IN PUNICODE_STRING RegistryPath
)
```



2) AddDevice : 디바이스 스택에 포함될 디바이스 오브젝트 생성

```
NTSTATUS  
SIMPLE_AddDevice  
(  
    IN PDRIVER_OBJECT DriverObject,  
    IN PDEVICE_OBJECT PhysicalDeviceObject  
)
```



3) PlugNPlayDispatch : PnP IRP를 처리

```
/*  
Pnp Manager로 부터 전달되는 PnP Event IRP를 받습니다  
*/  
NTSTATUS  
SIMPLE_PnpDispatch  
(  
    IN PDEVICE_OBJECT DeviceObject,  
    IN PIRP Irp  
)
```



4) PowerDispatch : 문맥 보관, 복원

```
/*
Power Manager로 부터 전달되는 Power Event IRP를 받습니다
특별한 처리는 하지 않고 받은 모든 명령어를 다음 계층으로 전달하도록 합니다
*/
NTSTATUS
SIMPLE_PowerDispatch
(
    IN PDEVICE_OBJECT DeviceObject,
    IN PIRP Irp
)
{
    ,
}
```



5) DriverUnload : 디바이스 드라이버 메모리에서 제거

```
// 드라이버가 메모리에서 해제될 때 호출됩니다
```

```
VOID
```

```
SIMPLE_Unload
```

```
{
```

```
    IN PDRIVER_OBJECT DriverObject
```

```
}
```

```
[  
{  
}
```



- 1) 사용자가 키보드를 누르면 입력된 키보드 데이터를 읽기 위한 읽기 요청 발생
- 2) 이 요청에 대한 IRP(I/O request packet)가 생성
- 3) 생성된 IRP는 디바이스 체인을 타고 내려가서 8042controller에 도착
- 4) 8042 드라이버가 키보드 버퍼에서 키보드 데이터를 가져오면
그에 해당하는 scan code를 IRP에 넣음
- 5) IRP는 다시 디바이스 체인을 거슬러 상위 계층으로 이동

