**[19] Trusted Computing이 무엇인지, ARM의 TrustZone을 예를 들어 설명합니다.**

Trusted Computing이란 컴퓨터가 의도된 대로 동작 할 수 있도록 신뢰성을 부과하는 기술이다.

Trusted Computing에서 하드웨어와 소프트웨어가 함께 움직인다. 소프트웨어만으로 보완을 하는 게 아니고 하드웨어가 도움을 줘야 한다는 뜻이다.

스마트폰으로 예를 들면, Trusted zone과 non-Trusted zone이 있는데, 하드웨어와 소프트웨어가 전부 똑같이 존재하는 2개의 스마트폰이 사실 동작하고 있는 것이다. 논리적으로는 하나이지만 정확하게 서로 다른 운영체제, 서로 다른 하드웨어를 쓸 수도 있고, 그 위에 서로 다른 어플리케이션이 들어가게 된다.

Trusted zone은 보호받고 있는 영역으로서 변경금지이고, 접근시 사용자가 허가를 해야한다. 보안에 민감한 것들은 Trusted zone과 거의 같은 개념인 secure world에서 통제하고 있다고도 볼 수 있다.