* Key Management System란?
- Key Management System는 말그대로 'key'를 관리하는 시스템으로 데이터를 암호화하고 복호화하는 기능을 담당함
- EBS, S3, RDS, EFS, SNS 등의 서비스에서 데이터 암/복호화 기능을 제공
- 즉 다른 서비스와 통합되어 사용됨
- KMS를 사용하여 암호화를 관리할 경우 키가 외부로 유출되는 위험이 적으며, AWS가 직접 키의 안전을 책임짐
- 다음 3가지 유형의 키로 나뉨
    - AWS 관리형 키
    - 고객 관리형 키
    - 사용자 키 스토어

* 고객 마스터 키(Customer Master Key, CMK)
- 데이터를 암호화하는데 사용하는 데이터 키의 생성에 관여하는 키
- AWS 서비스가 암호화를 시작할 때 CMK의 생성을 요청한 후 데이터 암호화를 시작
- 즉, CMK를 생성한 후에 데이터 키를 생성하고 데이터 암호화를 시작함
- 위의 3가지 유형 키는 CMK를 누가 관리하느냐에 따라 달라짐

* 데이터 암호화 과정
- 먼저 암호화를 시작하고자 하는 서비스가 CMK의 생성을 요청함
- CMK가 생성되고 이를 통해 데이터를 직접적으로 암호화할 데이터 키(대칭키) 생성
- 데이터를 데이터 키(대칭키)로 암호화한 후, 데이터 키를 폐기
- 그리고 데이터 키(대칭키)를 마스터 키로 암호화하여 암호화한 데이터와 같이 동봉함
    - 이를 봉투 암호화라 함
- 서비스가 암호화된 데이터를 다시 복호화하여 사용하고자 할 경우 고객 마스터 키를 가지고 데이터 키를 복호화 한 뒤 이 데이터 키를 가지고 데이터를 복호화함
    - 즉, CMK에 대한 접근권한이 없다면 데이터를 복호화할 수 없음
    - CMK를 삭제하게 되면 데이터를 복호화할 길은 전혀 없음

* AWS 관리형 키(CMK)
- AWS가 직접 CMK를 생성, 관리하는 서비스
- 사용자가 CMK에 대한 제어권한이 없음
- AWS가 주기적으로 CMK를 변경하여 사용함
- 고객 관리형 키를 쓰고 있지 않는데, 암호화를 사용중이라면 AWS 관리형 키를 이용해 암호화하고 있는 것

* 고객 관리형 키(CMK)
- 고객이 직접 CMK를 생성하고 관리하는 서비스
- 키의 활성화, 비활성화, 삭제 등 제어 권한을 가짐
- IAM을 이용하여 CMK에 접근할 주체를 정할 수 있음

* 사용자 지정 키 스토어
- CMK를 KMS가 아닌 CloudHSM에 저장하여 사용하는 방식
- CloudHSM 클러스터가 생성되어 있어야 사용 가능