* 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
- 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

* AWS KMS Keys(예전 이름 Customer Master Key)
- 데이터를 암호화하는데 사용하는 데이터 키의 생성에 관여하는 키
- AWS 서비스가 암호화를 시작할 때 KMS Key의 생성을 요청한 후 데이터 암호화를 시작
- KMS Key를 생성한 후에 데이터 키를 생성하고 데이터 암호화를 시작함
- 위의 3가지 유형 키는 KMS Key를 누가 관리하느냐에 따라 달라짐

* 데이터 키
- 데이터를 암호화하는데 사용되는 대칭키
- 데이터 키만을 활용해 암호화할 수는 없고 OpenSSL 또는 AWS Encryption SDK 같은 암호화 라이브러리를 사용해 암호화 가능

* 데이터 암호화 과정(봉투 암호화)
1. 먼저 암호화를 시작하고자 하는 서비스가 KMS Key의 생성을 요청함
2. KMS Key가 생성되고 KMS 키를 통해 데이터를 암호화할 데이터 키를 생성
3. KMS는 "평문 데이터 키"와 "암호화한 데이터 키" 두 개를 서비스에 전달함
4. 두 개의 키를 전달받은 서비스는 "평문 데이터 키"를 통해 데이터를 암호화하고 "평문 데이터 키"를 폐기함
5. 암호화된 데이터와 "암호화한 데이터 키"를 동봉하여 저장함(봉투 암호화)
6. 서비스가 데이터를 복호화하고자 할 경우, "암호화된 데이터키"를 KMS에 전달하고 KMS는 KMS Key를 통해 복호화된 평문 데이터 키"를 서비스에 전달함
7. 서비스는 "평문 데이터 키"를 이용해 데이터 복호화

* AWS 관리형 키(AWS KMS Keys)
- AWS가 직접 KMS Key를 생성, 관리하는 서비스
- 사용자가 KMS Key에 대한 제어 권한이 없음
- AWS가 주기적으로 KMS Key를 변경하여 사용함(1년 주기)
- 대칭키가 사용됨
- 고객 관리형 키를 쓰고 있지 않는데, 암호화를 사용중이라면 AWS 관리형 키를 이용해 암호화하고 있는 것

* 고객 관리형 키(Customer Master Key)
- 고객이 직접 KMS Key를 생성하고 관리하는 서비스
- 키의 활성화, 비활성화, 삭제 등 제어 권한을 가짐
- IAM을 이용하여 KMS Key에 접근할 주체를 정할 수 있음

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