* Cloudfront의 개요와 Edge Location
- CDN(Content Delivery Network)
- 간단히 말하여 HTTP / HTTPS를 이용하여 S3 및 ELB, EC2, 외부 서버 등을 캐시하고 보다 빠른 속도로 콘텐츠를 전달하는 캐시 서버
- 전 세계 각지에 퍼져 있는 Edge Location의 주변 Origin Server의 콘텐츠를 Edge Location에 캐싱하고 각 Edge Location간 공유를 통해 콘텐츠를 전달
- Distribution은 Edge Location의 집합을 의미
- 각 Edge Location간에는 아마존의 백본 네트워크를 통하기 때문에 매우 빠른 속도로 전달 가능
- 위에서 언급한 것처럼 S3, ELB, EC2 등의 AWS 서비스뿐만 아니라 외부의 서버도 캐싱 가능(이를 Custom Origin이라 함)
- TTL을 조절하여 캐시 주기를 통제할 수 있음

* 콘텐츠 제공 방법
1. 사용자가 웹 사이트 혹은 앱에 액세스하고 이미지 혹은 HTML 파일을 요청함(정적 데이터)
2. DNS가 요청을 최적으로 서비스할 수 있는 Cloudfront Edge Location으로 요청을 라우팅함
3. Edge Location에서 해당 캐시에 요청된 파일이 있는지 확인하고 없으면 오리진 서버에 요청하여 확보 후 전달, 그리고 캐시 적재

* OAI(Origin Access Identity)
- S3를 오리진 서버로 사용시, Cloudfront를 제외하고 다른 경로로 S3를 접근하는 것을 막는 방법
- OAI를 설정하게 되면 각각의 Distribution이 별도의 Identity를 갖게 되며, S3의 버킷 정책을 수동 혹은 자동으로 수정할 수 있음
- OAI가 적용된 S3의 버킷정책은 다음과 같이 수정됨

```
{
     "Version": "2008-10-17",
     "Id": "PolicyForCloudFrontPrivateContent",
     "Statement": [
         {
             "Sid": "1",
             "Effect": "Allow",
             "Principal": {
                 "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
Identity xxx"
             },
             "Action": "s3:GetObject",
             "Resource": "arn:aws:s3:::bucket-name/*"
         }
     ]
 }
```

* Presigned URL
- 인증된 사용자만이 해당 Distribution를 사용할 수 있도록 제어하는 기능
- 만료 날짜 및 시간까지 설정 가능
- Cloudfront 설정시 Presigned URL 사용과 Cloudfront Key Pair를 계정의 보안자격증명에서 생성해야 함
- 이를 조합하여 URL 서명을 생성하고 해당 URL을 통해 Cloudfront에 접근할 수 있음