HANSUNG UNIVERSITY

클라우드컴퓨팅

AWS Service - IAM

Sung-Dong Kim,
School of Computer Engineering,
Hansung University

What to study

- AWS Identity and Access Management (IAM)
- IAM 그룹
- IAM 정책
- IAM 권한
- IAM 역할
- Root 사용자 vs IAM 사용자

AWS Identity and Access Management (IAM)

AWS IAM

- IAM을 사용하여 AWS 리소스에 대한 액세스 관리
  - 리소스는 사용자가 작업을 수행할 수 있는 AWS 계정의 엔터티 (entity)
  - 리소스 예: Amazon EC2 instance, Amazon S3 bucket, ...
- 예: EC2 인스턴스를 종료할 수 있는 사용자 제어
- 세분화된 액세스 권한 정의
  - 리소스에 액세스할 수 있는 사용자
  - 액세스할 수 있는 리소스와 사용자가 리소스에 수행할 수 있는 작업
  - 리소스에 액세스 하는 방법
- 무료

AWS IAM: 필수 구성 요소

IAM 사용자

AWS 계정으로 인증할 수 있는 사람 또는 애플리케이션입니다.

IAM 그룹

동일한 권한 부여를 허락받은 IAM 사용자의 모음입니다.

IAM 정책

액세스할 수 있는 리소스와 각 리소스에 대한 액세스 수준을 정의하는 문서입니다.

IAM 역할

AWS 서비스 요청을 위한 권한 세트를 부여하는 유용한 메커니즘입니다.

AWS IAM: 액세스 유형

- IAM 사용자 정의 시 사용자가 사용할 수 있는 액세스 유형 선택
- 프로그래밍 방식 액세스
  - 인증 방법
    - access key ID
    - 보안 액세스 키
  - AWS CLI 및 AWS SDK 액세스 제공

AWS CLI

AWS 도구 및 SDK

- AWS Management Console 액세스
  - 인증 방법
    - 12자리 계정 ID 또는 별칭 (alias)
    - IAM 사용자 이름
    - IAM 암호
  - MFA (Multi-Factor Authentification): 인증 코드 필요

AWS Management Console

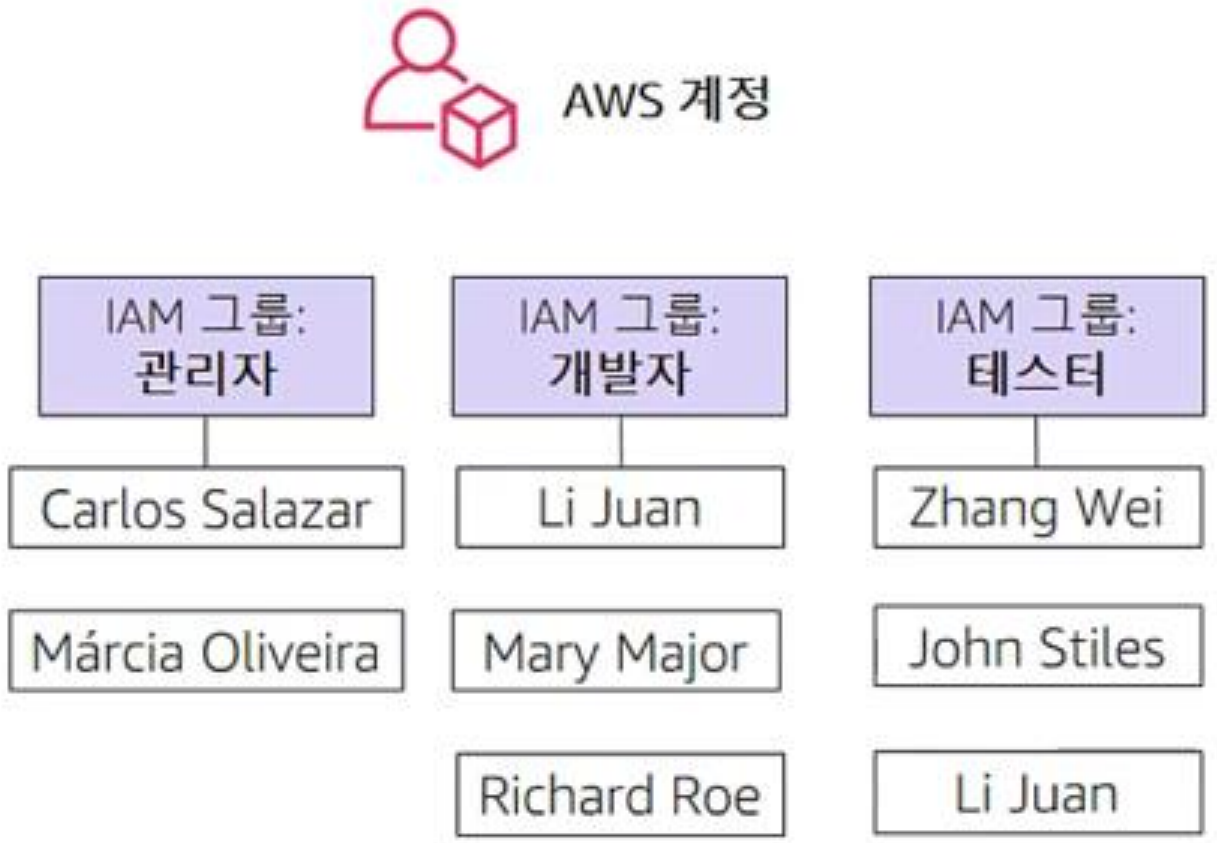
MFA

- 보안 향상
- 사용자 이름, 암호 + 인증 코드

IAM 그룹

IAM 그룹

- IAM 사용자의 모음
- 여러 사용자에게 동일한 권한을 부여하는 데 사용됨
  - IAM 정책을 그룹에 연결하여 권한 부여
- 한 사용자가 여러 그룹에 속할 수 있음
- 기본 그룹은 없음
- 그룹을 중첩할 수 없음



IAM 정책

IAM 정책 (policy)

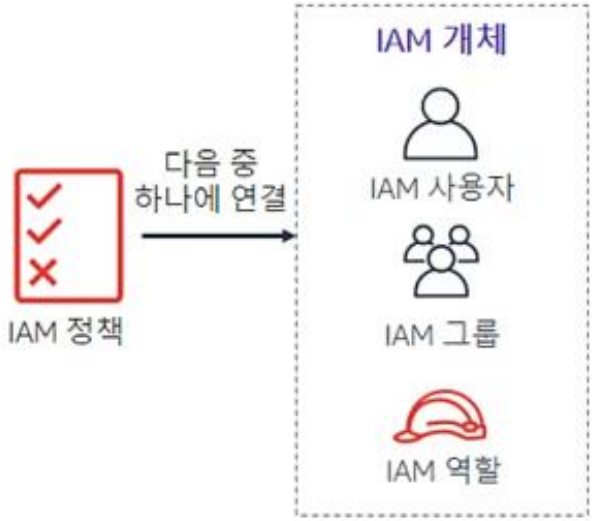
- 정책은 권한을 정의하는 문서
  - 세분화된 액세스 제어 가능
- 2가지 유형의 정책 - 자격 증명 기반 / 리소스 기반

IAM 정책 (policy)

HANSUNG UNIVERSITY

자격 증명 기반 정책

- 정책을 모든 IAM 엔터티에 연결: IAM 사용자, IAM 그룹, IAM 역할
- 정책은 다음을 지정
  - 엔터티가 수행할 수 있는 작업
  - 엔터티가 수행할 수 없는 작업
- 단일 정책을 여러 엔터티에 연결할 수 있음
- 단일 엔터티에 여러 정책을 연결할 수 있음



리소스 기반 정책

- 리소스(예: S3 버킷)에 연결됨
- 리소스에 액세스할 수 있는 사용자와 해당 사용자가 수행할 수 있는 작업 지정
- 일부 AWS 서비스에서만 지원됨

IAM 정책 (policy)

정책 (policy): 예


```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action":["DynamoDB:*","s3:*"],
    "Resource":[
      "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

명시적 허용은 사용자에게 특정 DynamoDB 테이블과...

...Amazon S3 버킷에 대한 액세스 권한을 부여합니다.

명시적 거부 는 사용자가 테이블과 해당 버킷을 제외하고 다른 AWS 작업 또는 리소스를 사용할 수 없게 합니다.

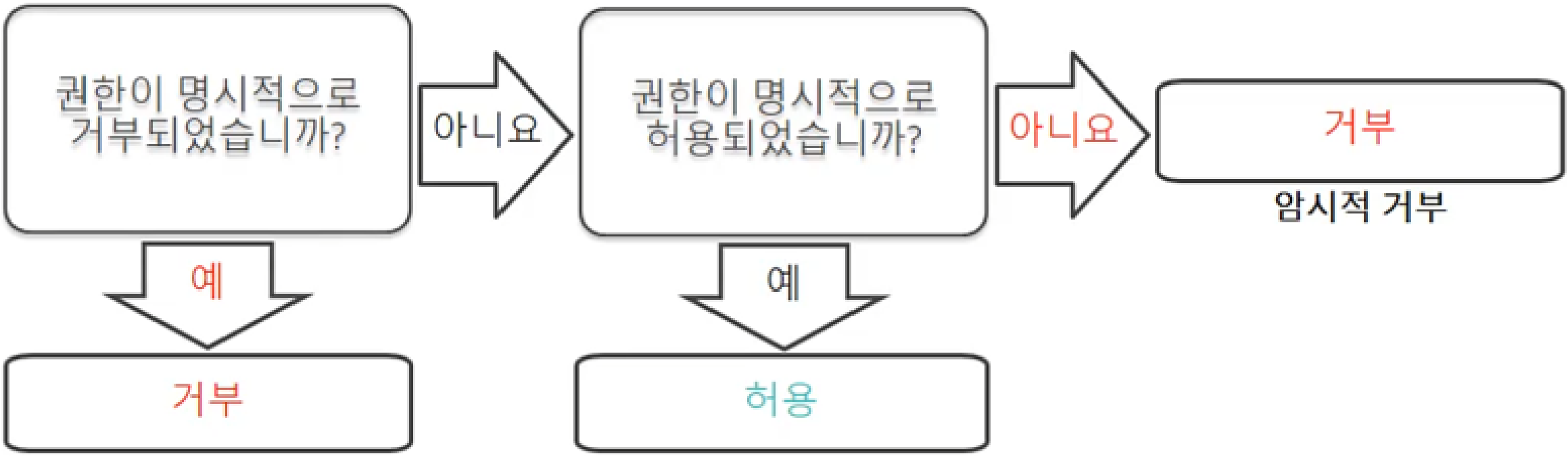
명시적 거부문은 허용문보다 **우선** 적용됩니다.

IAM 권한

권한

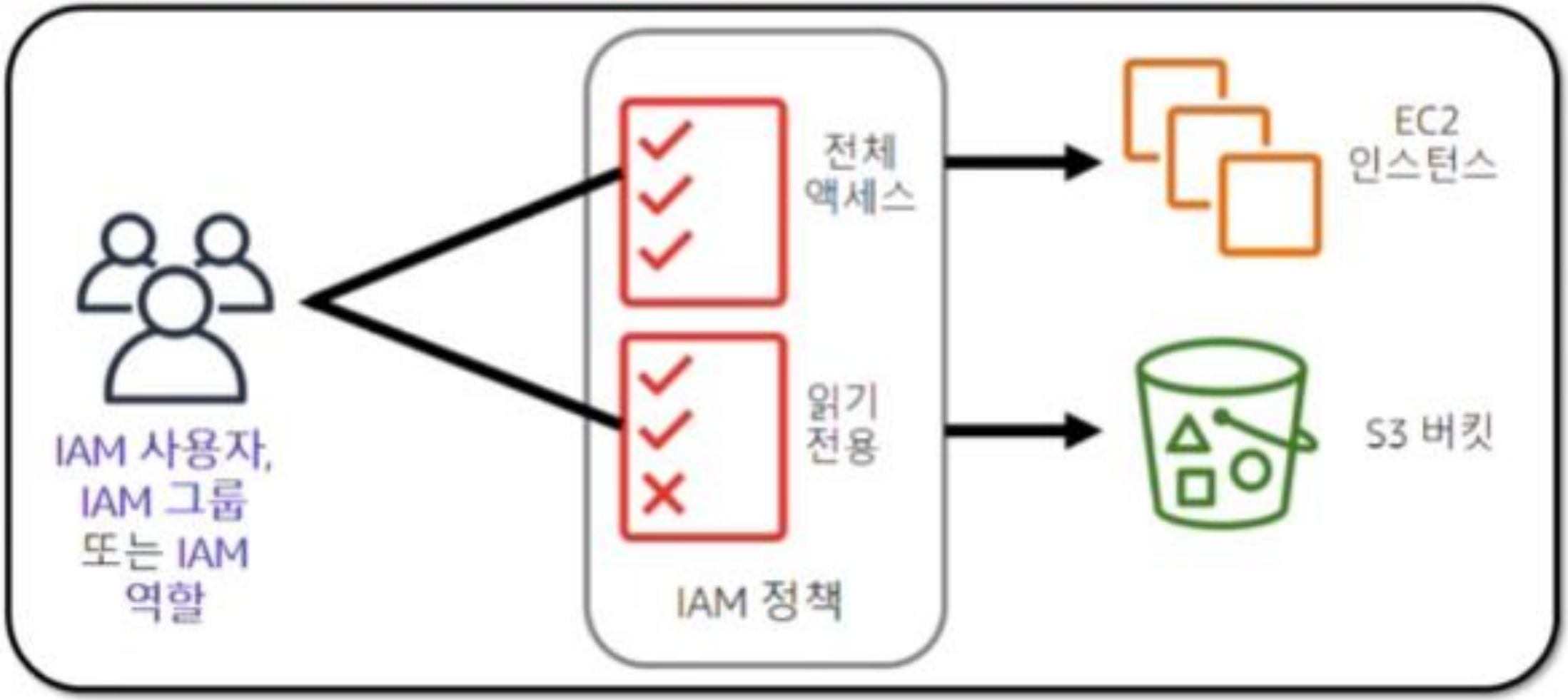
- IAM 정책을 생성하여 권한 할당
- 권한은 허용되는 리소스와 작업을 결정
  - 기본적으로 모든 권한은 암시적 (default, implicit)으로 거부됨
  - 명시적으로 거부된 항목은 절대 허용되지 않음
- 모범 사례: 최소 권한의 원칙 따르기

권한 결정 방법



권한

AWS 계정에 연결한 사용자 또는 애플리케이션에 허용되는 작업은 무엇입니까?



IAM 역할

IAM 역할 (role): 예

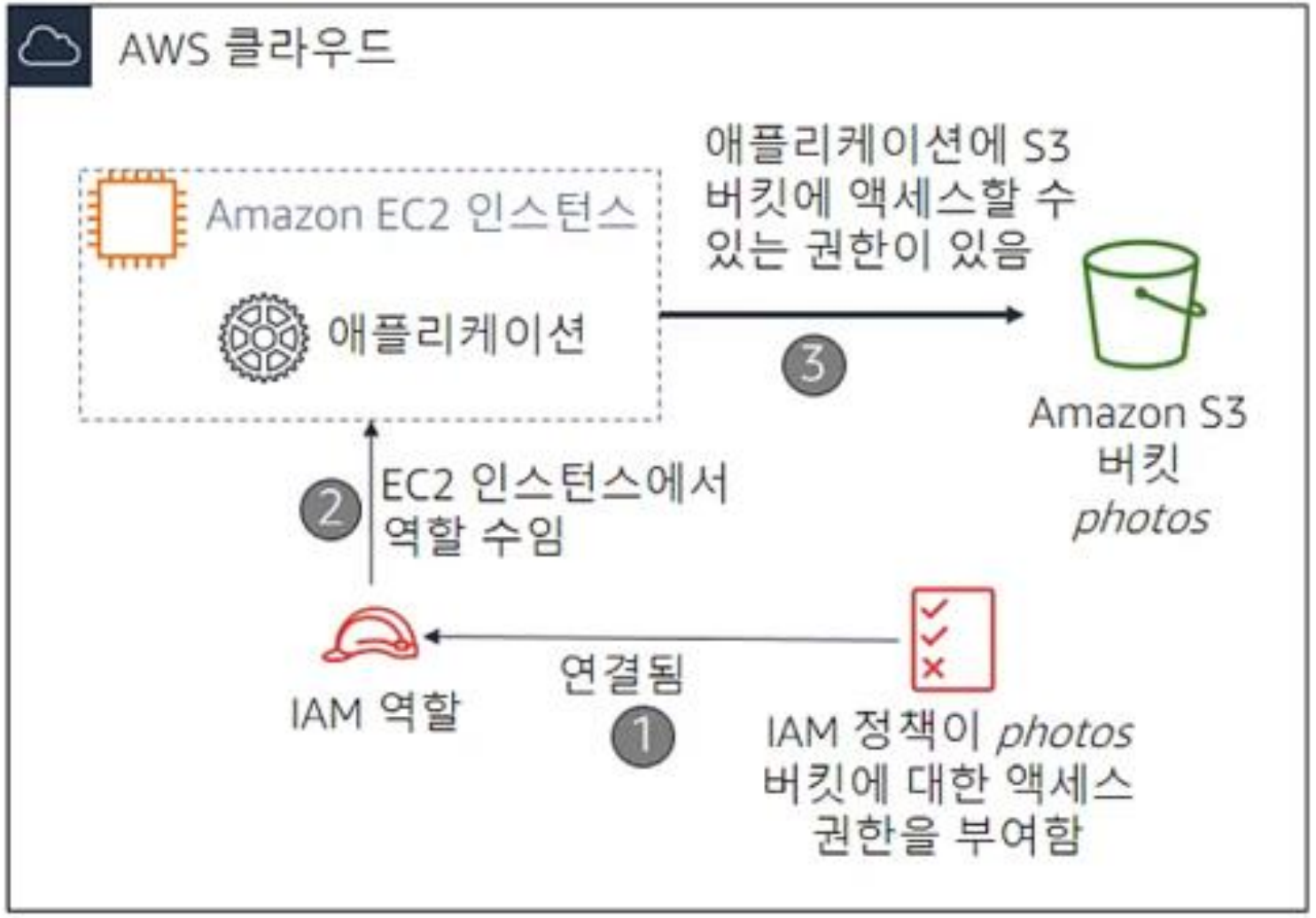
HANSUNG UNIVERSITY

시나리오

- EC2 인스턴스에서 실행되는 애플리케이션에 S3 버킷에 대한 액세스 권한이 필요한 경우

솔루션

- S3 버킷에 대한 액세스 권한을 부여하는 IAM 정책 정의
- 정책을 역할에 연결
- EC2 인스턴스가 이 역할을 수임하는 것을 허용



Root 사용자 vs IAM 사용자

root 사용자와 IAM 사용자 비교

모범사례

- 필요한 경우를 제외하고 루트 사용자를 사용하지 않음

루트 사용자

- 루트 사용자 암호 변경
- AWS support plan 변경
- IAM 사용자 권한 복원
- 계정 설정 변경