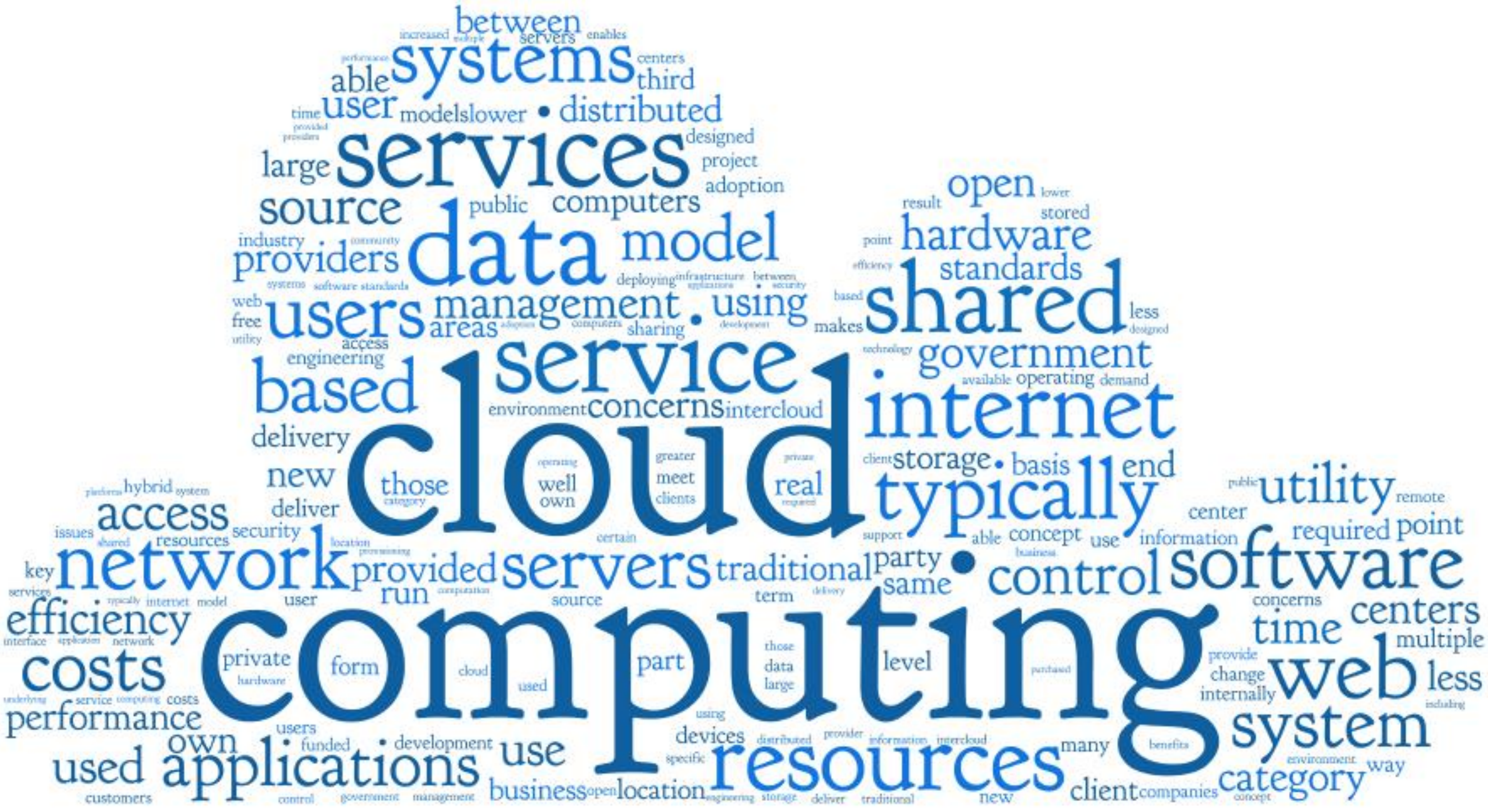
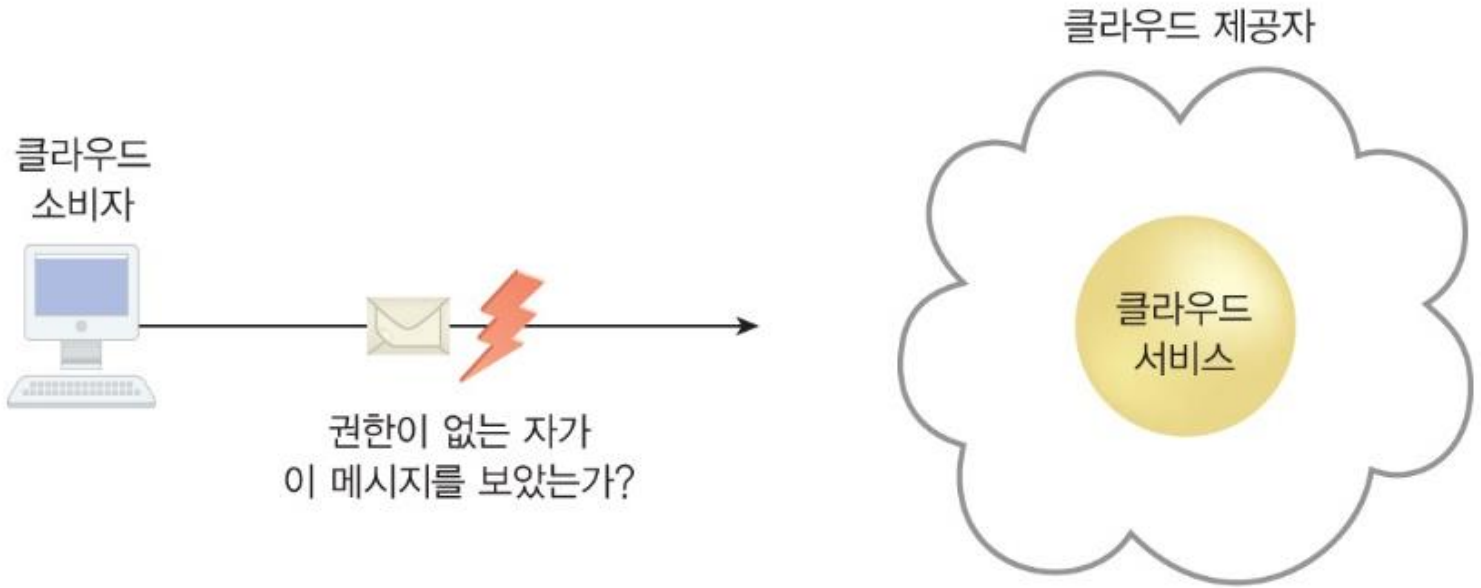

cloud
computing
services
data
service
network
shared
internet
typically
software
resources
applications
systems
users
model
management
servers
based
access
costs
efficiency
web
system
control
utility
hardware
government
source
providers
between
distributed
user
able
third
large
open
standards
using
concerns
intercloud
environment
delivery
new
those
real
storage
basis
end
provided
traditional
party
same
time
centers
multiple
less
category
client
location
business
use
used
own
performance
private
form
part
level
devices
security
deliver
hybrid
key
run
required
point
concept
information
center
remote
change
internally
many
way
companies
computers
public
adoption
project
designed
hardware
engineering
areas
sharing
deploying
makes
less
operating
demand
well
meet
clients
greater
development
funded
customers
issues

02
클라우드 컴퓨팅 보안

02 Cloud Computing Security

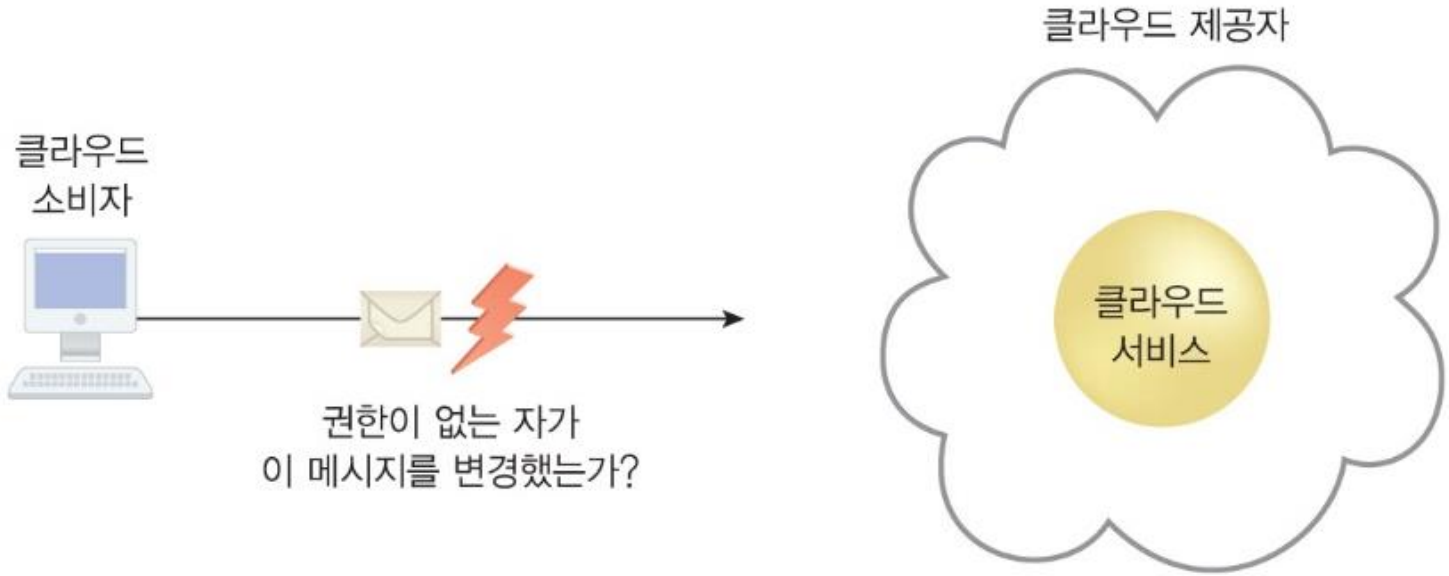
클라우드 컴퓨팅 보안 ①

- 기밀성
  - 권한이 부여된 자에게만 접근이 허용되는 특징
  - 클라우드 환경에서의 기밀성은 주로 이동 중인 데이터와 스토리지 내의 데이터에 대한 접근을 제한하는 방식으로 유지



클라우드 컴퓨팅 보안 ②

- 무결성
  - 권한이 없는 주체에 의해 변경되지 않았다는 특징
  - 클라우드에서 데이터 무결성을 고려할 때 중요한 점은 클라우드 소비자가 클라우드 서비스에 보낸 데이터와 클라우드 서비스가 받은 데이터가 일치하는지를 보증할 수 있는지의 여부
  - 무결성은 데이터가 어떻게 저장되고 처리되며 클라우드 서비스와 클라우드 기반 IT 자우너에 의해 추출되는지까지를 포함



클라우드 컴퓨팅 보안 ③

- 진실성
  - 인증된 출처에서 제공된 것이라는 특징
  - 상호작용의 인증을 부정하거나 반박할 수 없는 부인 방지를 포함
  - 부인방지가 되는 상호작용에서의 인증은 인증된 출처와 유일하게 연결되었다는 증거 제공
  - 만약 사용자가 접속기록 생성 없이 부인 방지되는 파일을 받았다면 파일에 접근 불가
- 가용성
  - 특정 시간 동안 접속 및 사용이 가능한 특징
  - 클라우드 서비스의 가용성은 클라우드 제공자와 클라우드 전달자가 책임을 공유
  - 클라우드 소비자는 클라우드 서비스 소비자에게 미치는 클라우드 기반 솔루션의 가용성을 공유

클라우드 컴퓨팅 보안 ④

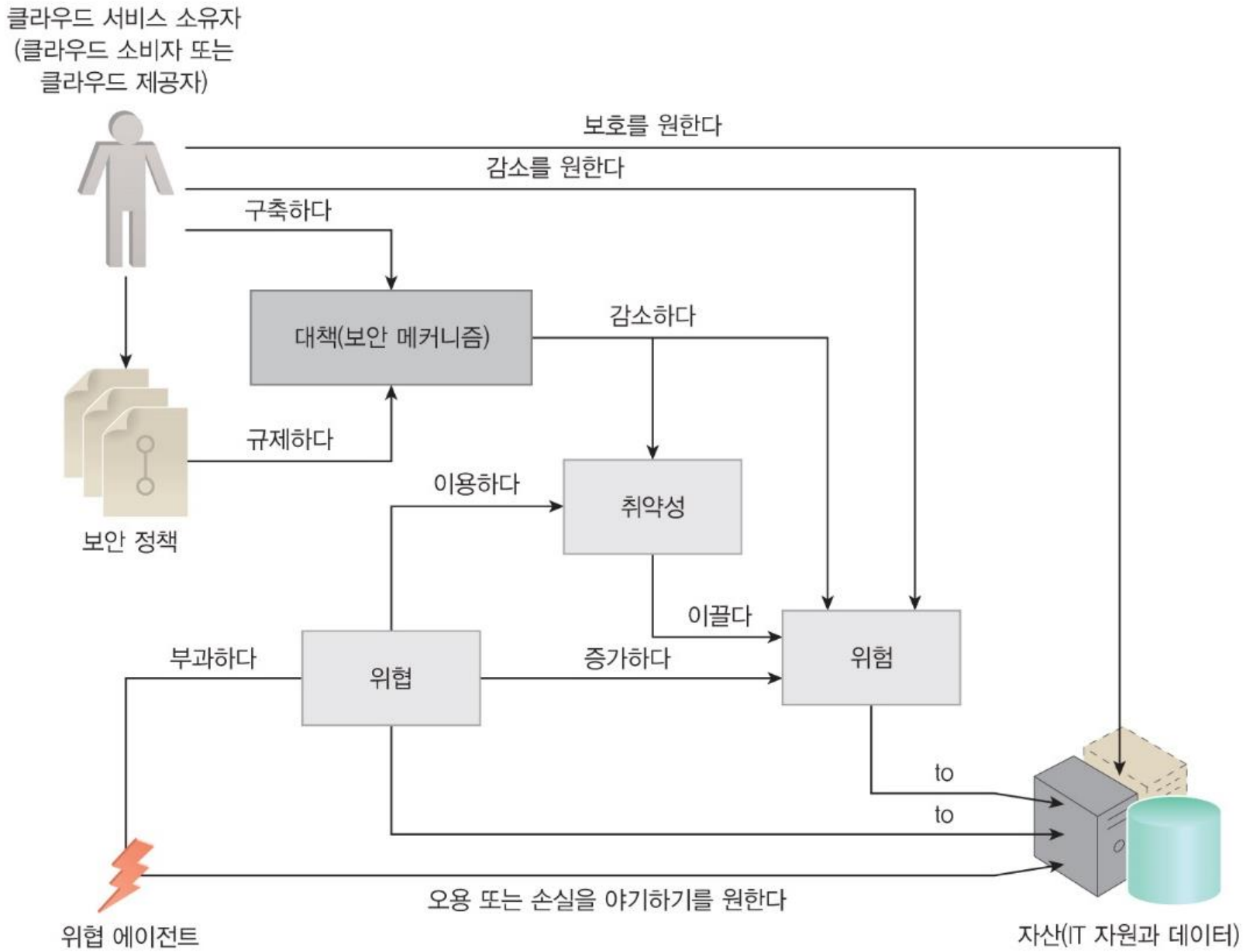
- 위협
  - 프라이버시를 침해하거나 손상을 일으키려는 시도에 대한 방어에 대해서 도전하는 잠재적인 보안 침해
  - 수동적, 자동적으로 조장된 위협은 모두 취약점을 이용하도록 설계되며 위협이 수행되면 곧 공격이 시작
- 취약성
  - 불충분한 보안 통제에 의해 보호나 기존의 보안 통제를 능가하는 공격으로 인해 침해될 수 있는 약점
  - IT 자원 취약성에는 설정의 부족, 보안 정책 약점, 사용자 실수, 하드웨어나 펌웨어의 약점, 소프트웨어 버그, 취약한 보안 아키텍처 등 다양한 원인이 존재

클라우드 컴퓨팅 보안 ⑤

- 위험
  - 어떤 행위로 인해 발생할 수 있는 손실이나 손상의 가능성
  - 위험은 대개 위험 수준과 알려진 취약성의 수를 기준으로 측정
  - IT 자원의 취약성을 파고드는 위협의 확률
  - 구성하고 있는 IT 자원 손실의 기대값
- 보안 통제
  - 보안 위협을 예방하거나 대응하고 위험을 줄이거나 피하기 위해 사용되는 대책
  - 민감하고 중요한 IT 자원을 최대한 보호하기 위해 시스템이나 서비스, 보안 계획을 어떻게 구현할지에 대한 일련의 규칙과 지침 등을 보안 정책에 기술
- 보안 메커니즘
  - IT 자원 정보, 서비스를 보호하는 방어 프레임워크를 구성하는 컴포넌트
- 보안 정책
  - 일련의 보안 규칙과 규제를 수립
  - 보안 통제와 보안 메커니즘의 배치와 사용을 결정

위협 에이전트

- 공격을 수행하는 능력이 있어 위협을 부과하는 주체
- 취약성, 위협, 위험과 관련되어 수행되는 역할과 보안 정책 그리고 보안 메커니즘에 의해 구축된 안전 장치가 필요



익명 공격자

- 클라우드의 허가를 받지 않은, 신뢰할 수 없는 클라우드 서비스 소비자
- 대부분 퍼블릭 네트워크를 이용해 네트워크 수준의 공격을 하는 외부 소프트웨어 프로그램의 형태로 존재
- 익명 공격자가 보안 정책과 방어에 대한 제한된 정보만 가지고 있을 경우, 효율적인 공격을 감행할 가능성이 적음
- 종종 사용자 계정을 바이패싱하거나 사용자 자격 증명을 훔치는 식의 방법을 사용

악성 서비스 에이전트

- 클라우드 내에 흐르는 네트워크 트래픽을 가로채 전송 가능
- 대부분 손상을 가하거나 악의적인 로직을 보유한 서비스 에이전트(또는 서비스 에이전트인 척 하는 프로그램) 형태로 존재
- 메시지 컨텐츠를 원격에서 가로채고 잠재적으로 메시지 컨텐츠를 파괴시킬 수 있는 외부 프로그램 형태로도 존재

신뢰할 수 있는 공격자

- 클라우드 소비자로서 동일 클라우드 환경에 있는 IT 자원을 공유하면서 클라우드 제공자와 클라우드 테넌트를 목표로 부당하게 이용하려는 시도를 함
- 익명 공격자와 달리 신뢰할 수 있는 공격자는 대게 합법적인 자격을 오용하거나 민감하고 은밀한 정보를 도용하여 클라우드 신뢰 경계 내에서 공격을 수행
- 신뢰할 수 있는 공격자는 취약한 인증 처리를 해킹하거나 암호를 해독하거나 이메일 계층 스팸, 서비스 캠페인 부정과 같은 일반거인 공격 등을 위하 클라우드 기반 IT 자원을 사용

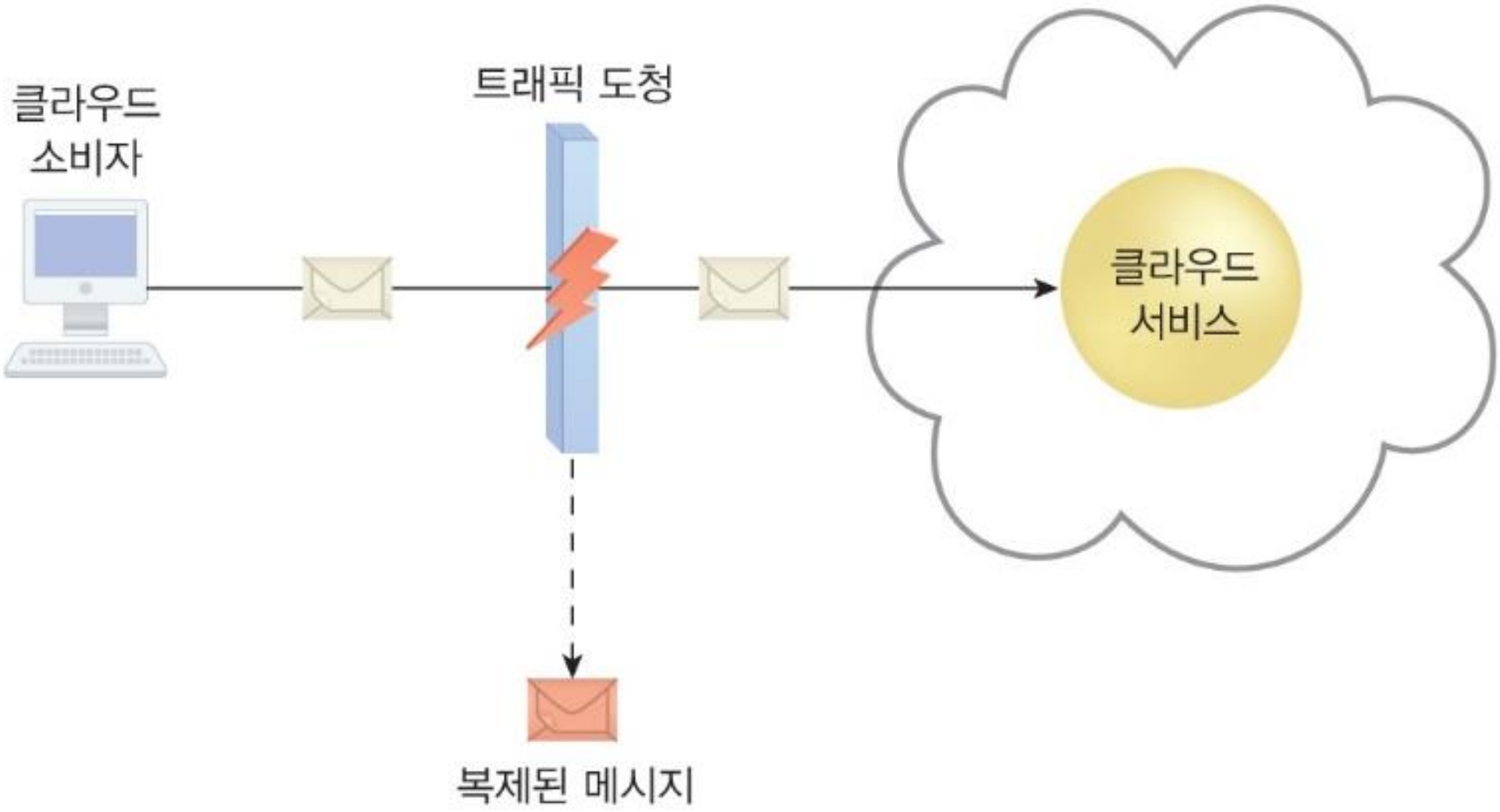
악성 내부자

- 클라우드 제공자처럼 행동하거나 클라우드 제공자와 관계된 인간 위협 에이전트
- 현재 또는 이전에 직원이었거나 클라우드 제공자의 구역에 접근할 수 있는 제3자
- 악성 내부자는 클라우드 소비자의 IT 자원에 접근하는 관리자 권한을 가지기 때문에 이러한 형태의 위협 에이전트는 막대산 손상 잠재력을 가짐

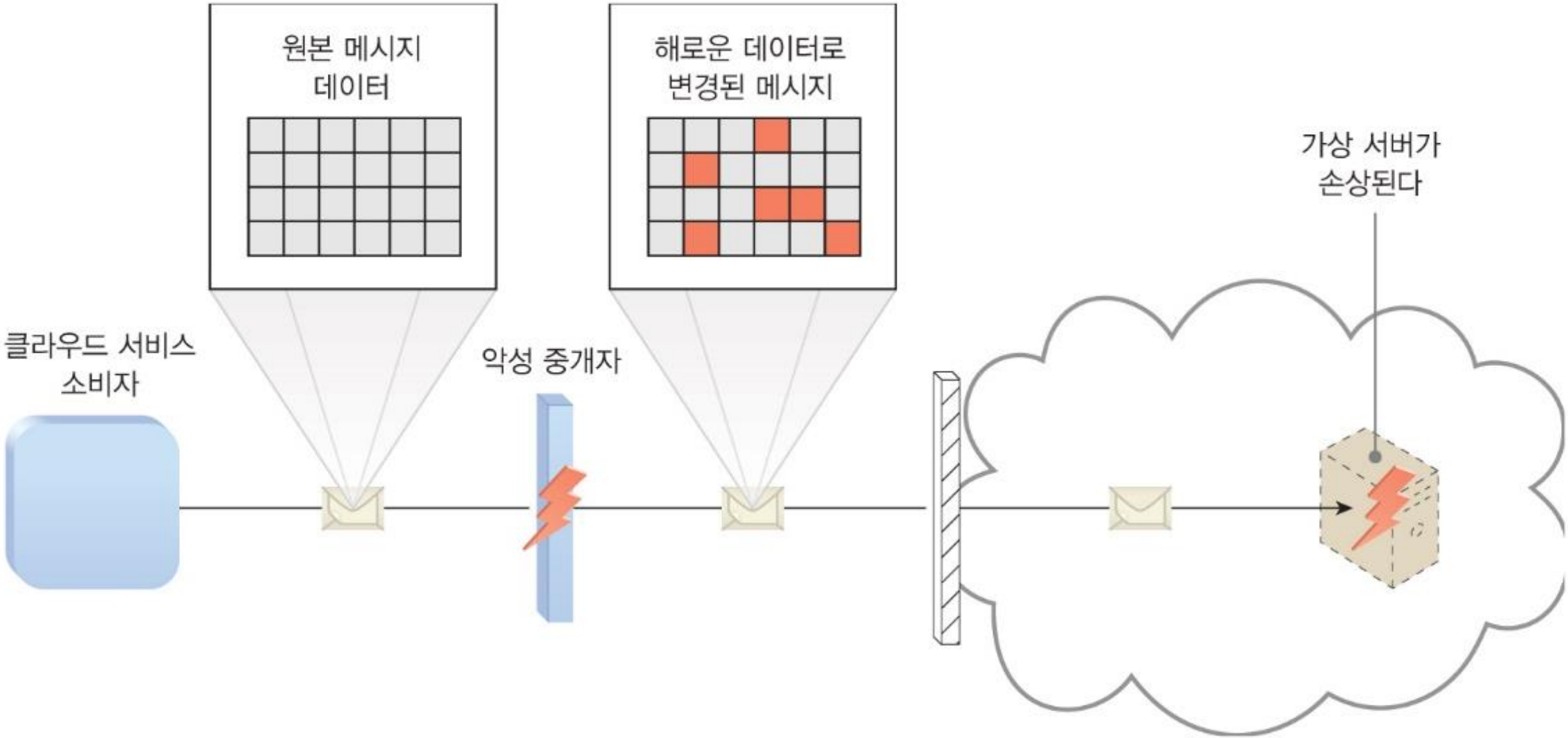
클라우드 보안 위협

- 트래픽 도청
- 악성 중개자
- 서비스 거부
- 불충분한 권한 부여
- 가상화 공격
- 신뢰 경계의 중복
- 구현 결함

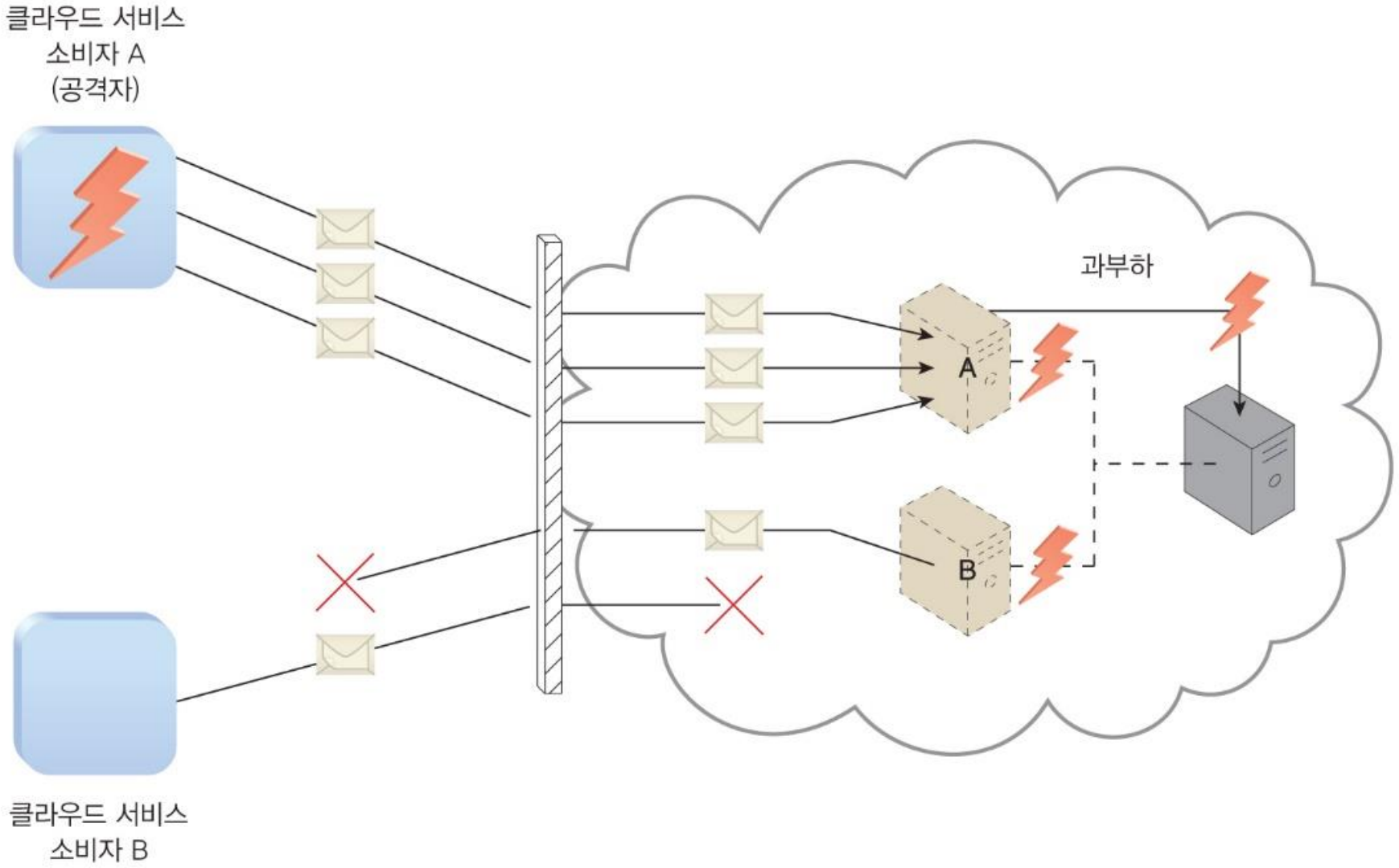
트래픽 도청



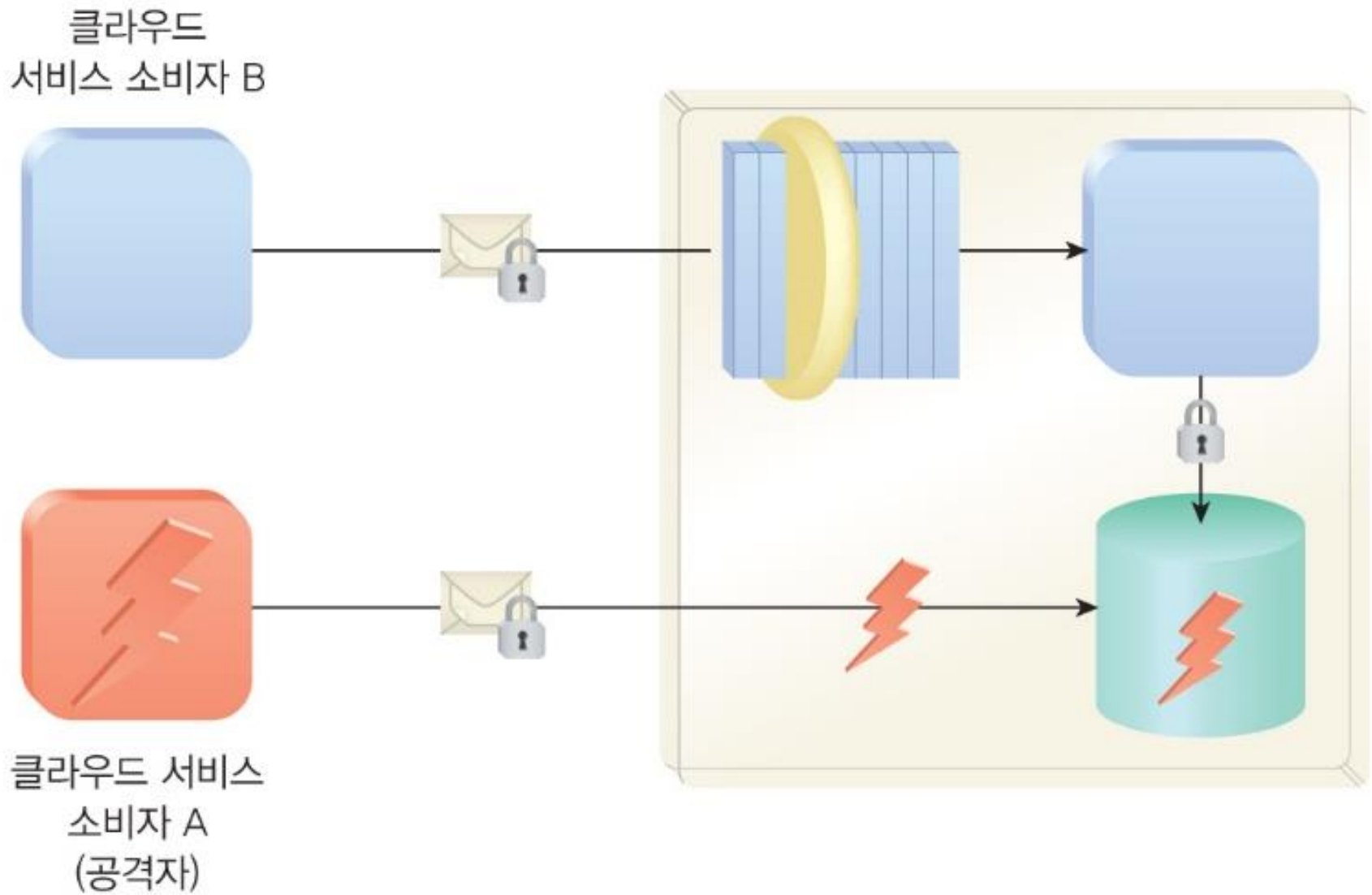
악성 중개자



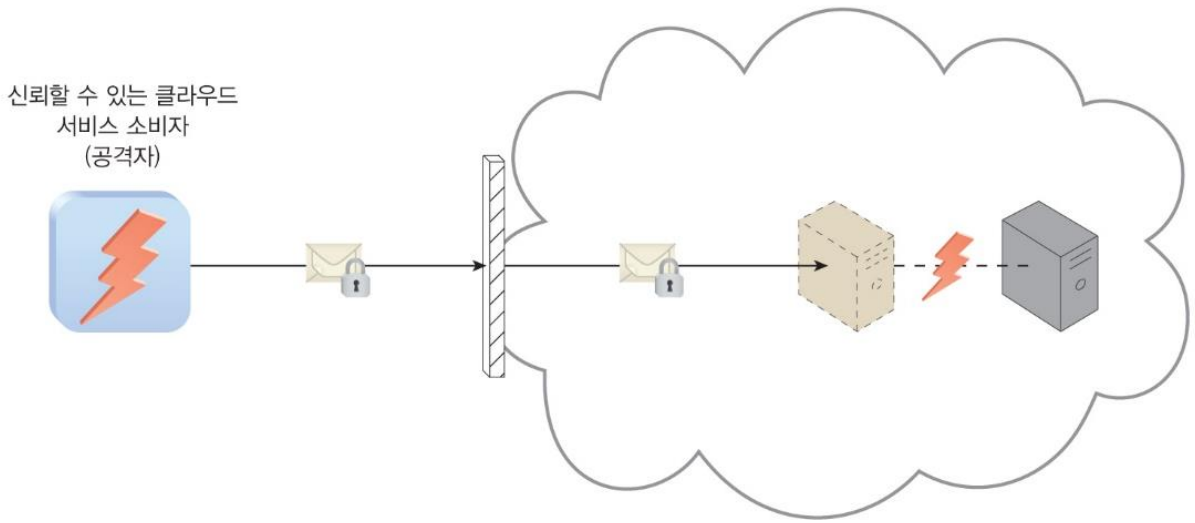
서비스 거부

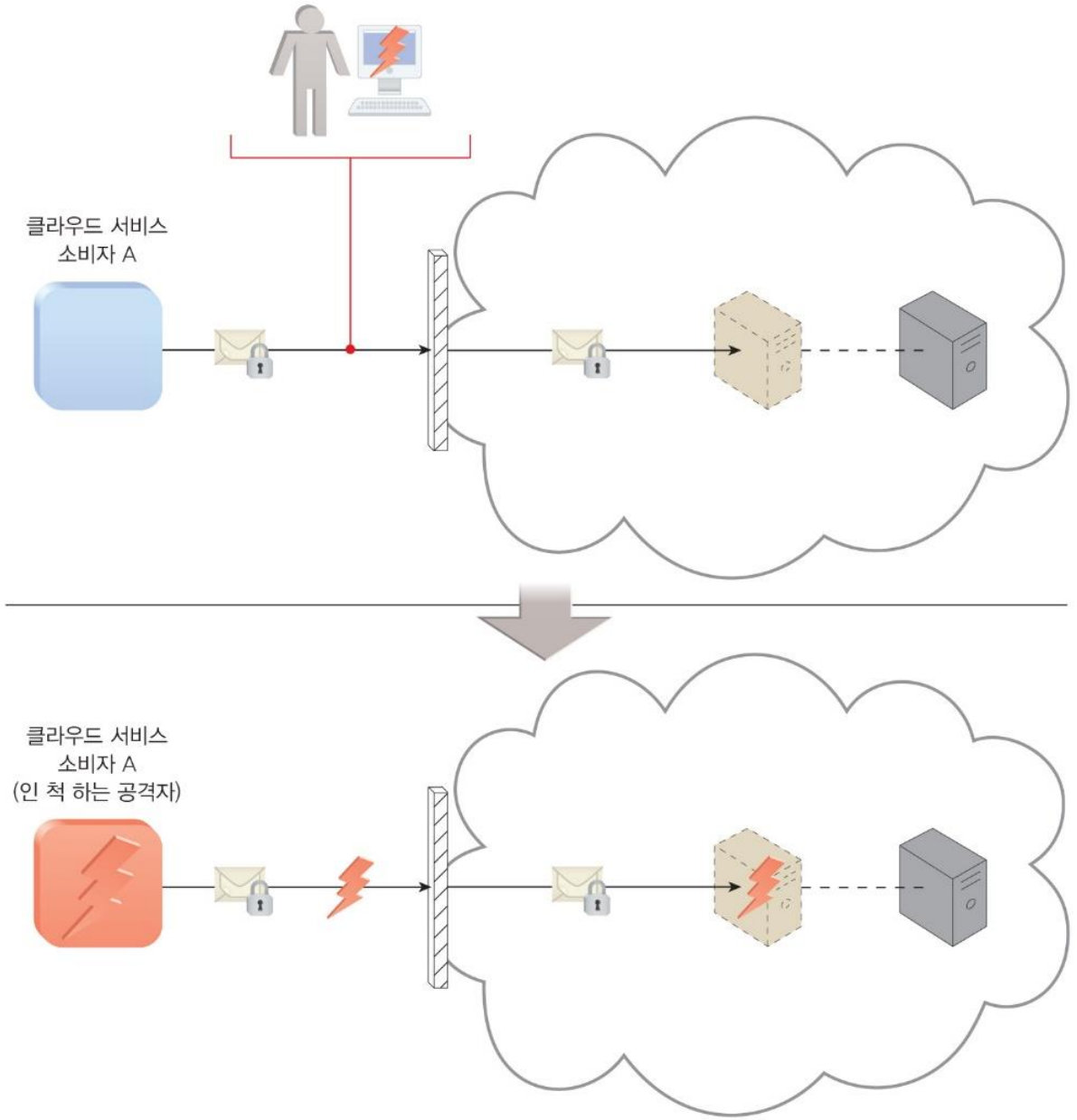


불충분한 권한 부여

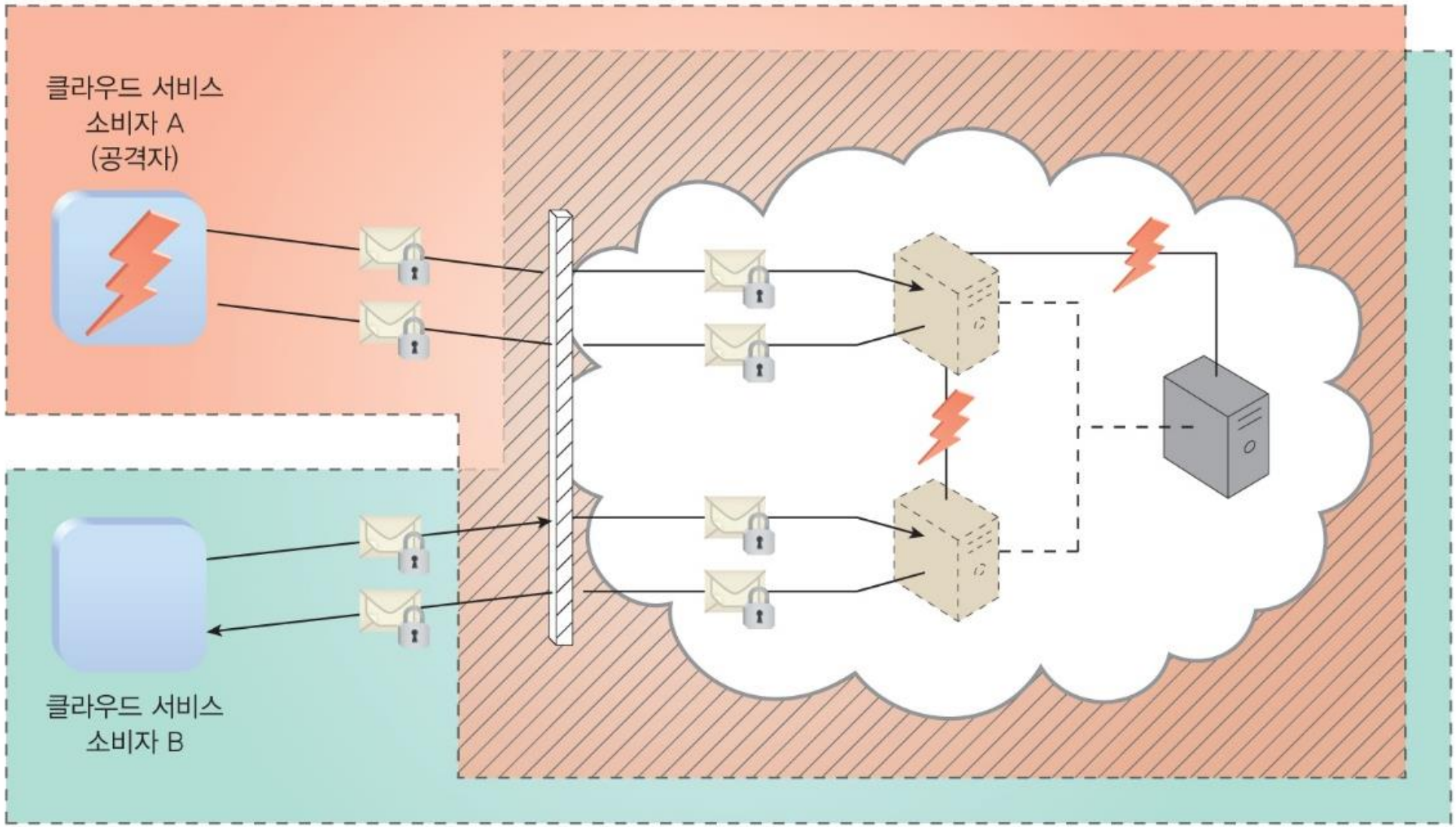


가상화 공격

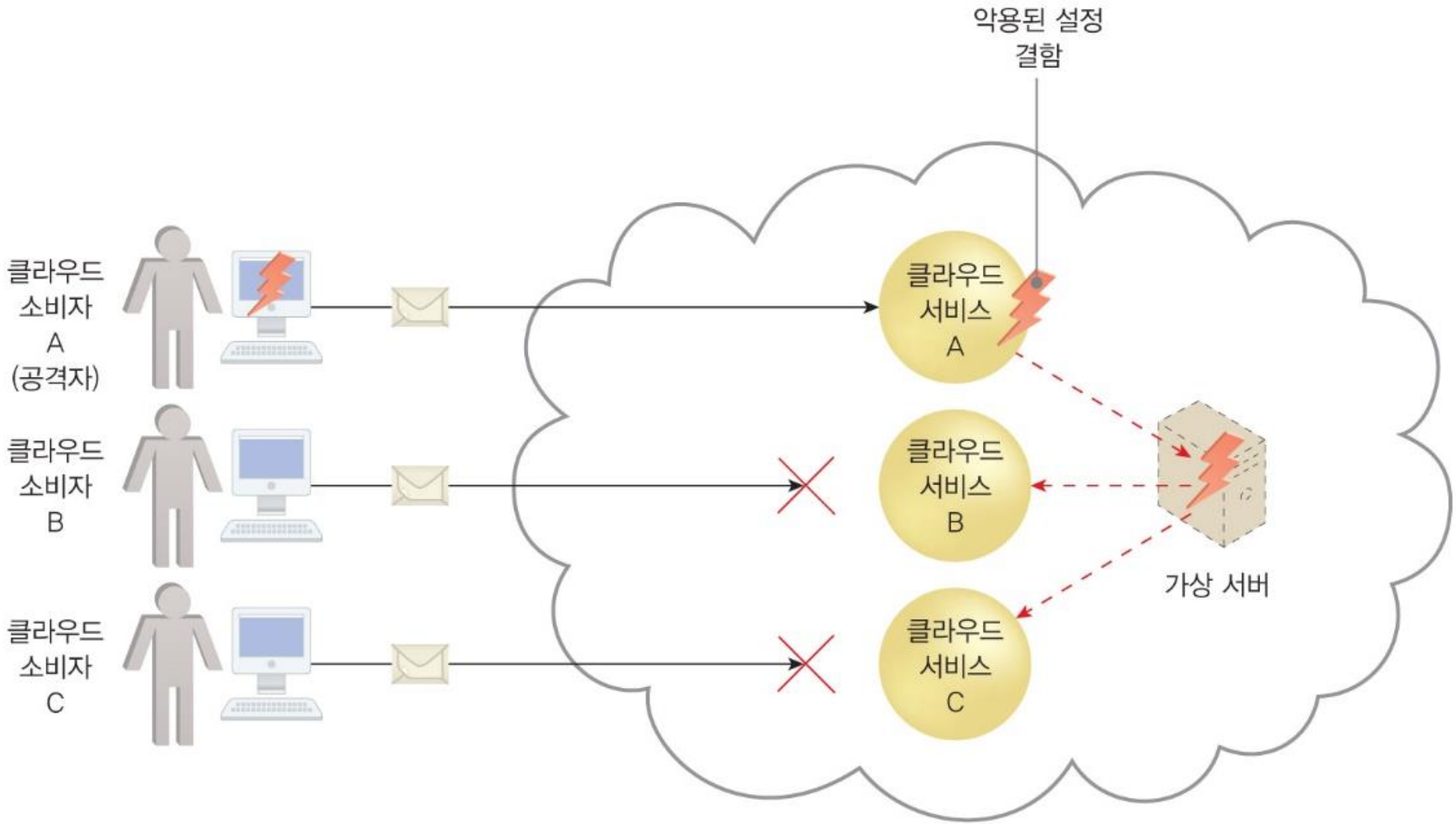




신뢰 경계의 중복



구현 결함


악용된 설정
결함
클라우드
소비자
A
(공격자)
클라우드
소비자
B
클라우드
소비자
C
클라우드
서비스
A
클라우드
서비스
B
클라우드
서비스
C
가상 서버