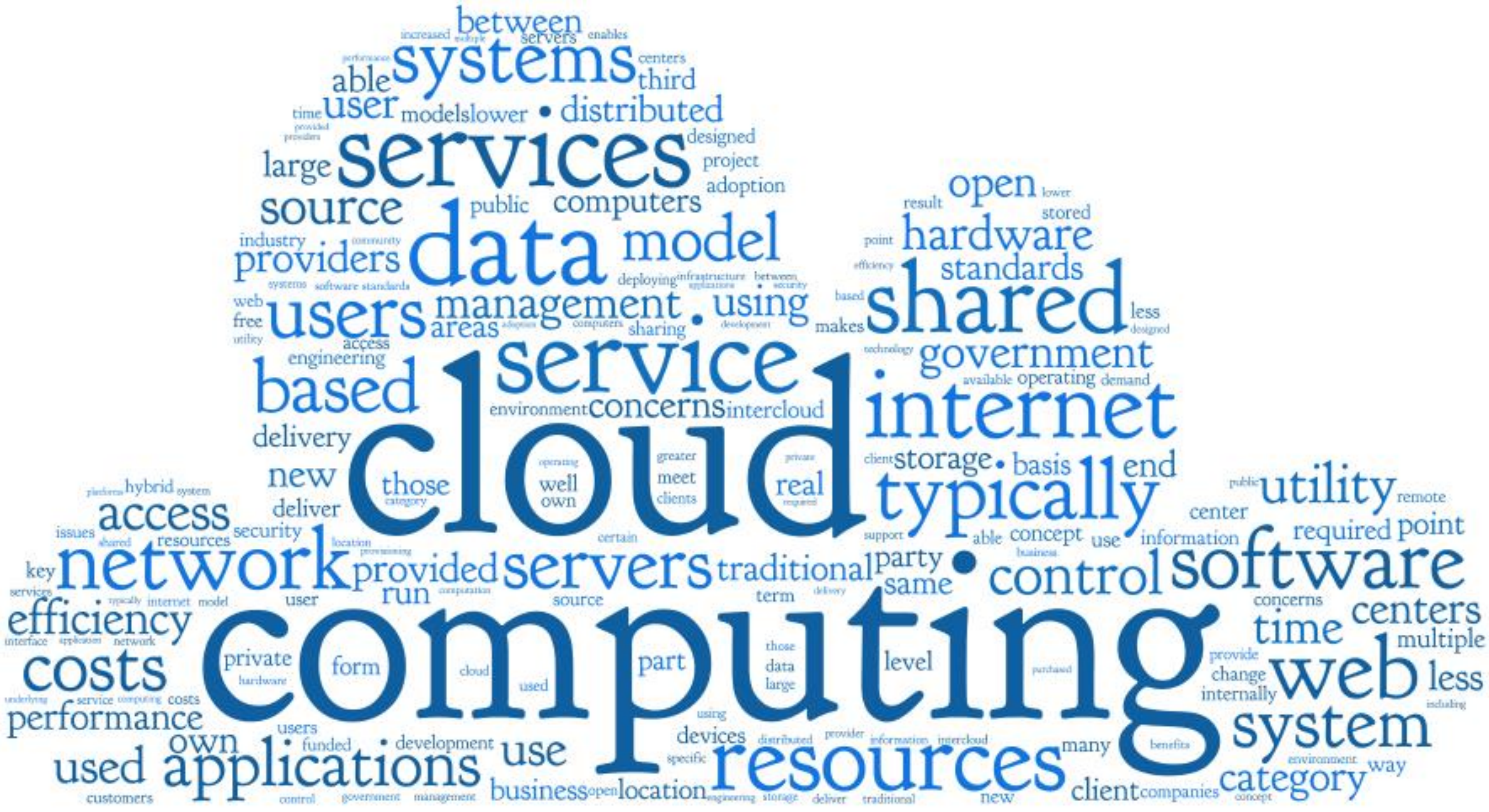

between
systems
able
third
user
distributed
services
large
designed
project
adoption
source
public
computers
data
model
providers
open
hardware
standards
shared
users
management
using
areas
sharing
makes
service
government
based
engineering
concerns
intercloud
environment
internet
delivery
cloud
storage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

06
클라우드 관리 보안 메커니즘

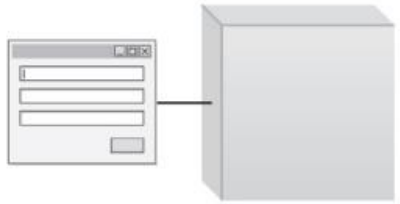
06 Cloud Management Security Mechanism

클라우드 관리 메커니즘

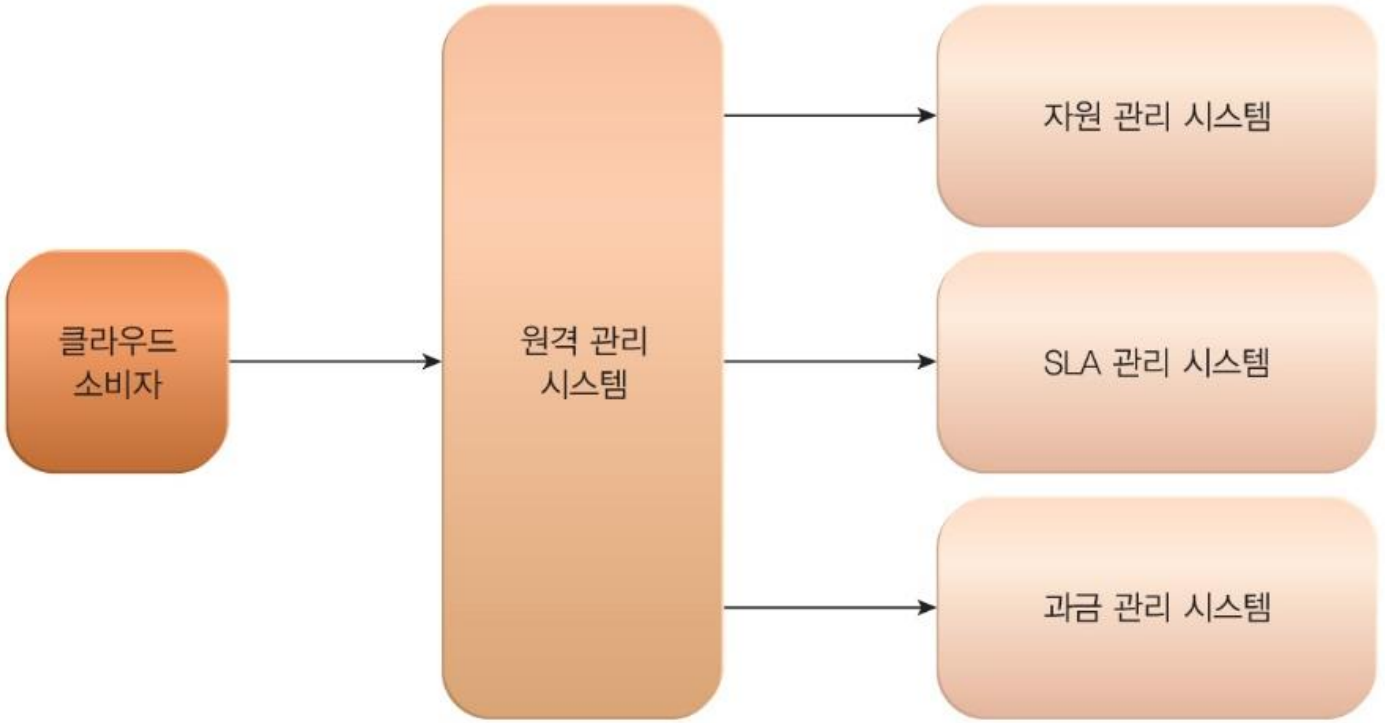
- 원격 관리 시스템
- 자원 관리 시스템
- SLA 관리 시스템
- 과금 관리 시스템

원격 관리 시스템

- 원격 관리 시스템 메커니즘은 외부 클라우드 자원 관리자에게 클라우드 기반 IT 자원을 설정하고 관리할 수 있게 도구와 사용자 인터페이스 제공



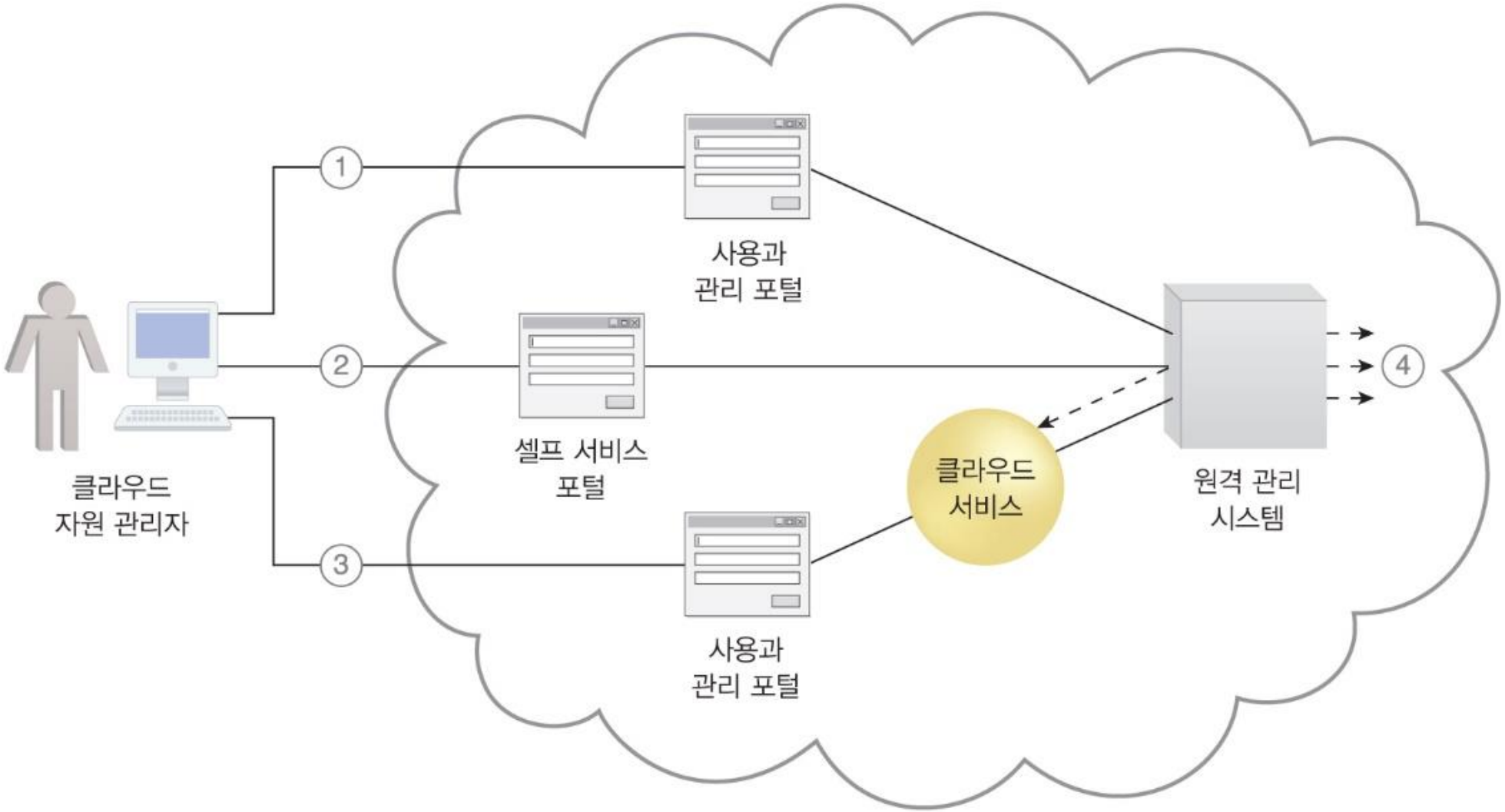
원격 관리 시스템



원격 관리 시스템 포털 유형

- 사용자 관리 포털
  - 관리를 중앙화하는 일반적인 목적의 포털
  - 다른 클라우드 기반 IT 자원을 통제
  - IT 자원 사용 보고서 제공 가능
- 셀프 서비스 포털
  - 클라우드 소비자가 클라우드 제공자로부터 사용 가능한 최신의 클라우드 서비스와 IT 자원 목록을 검색할 수 있게 하는 쇼핑 포털
  - 클라우드 소비자는 프로비저닝을 위해 클라우드 제공자에게 선택한 항목을 제공

원격 관리 시스템 시나리오

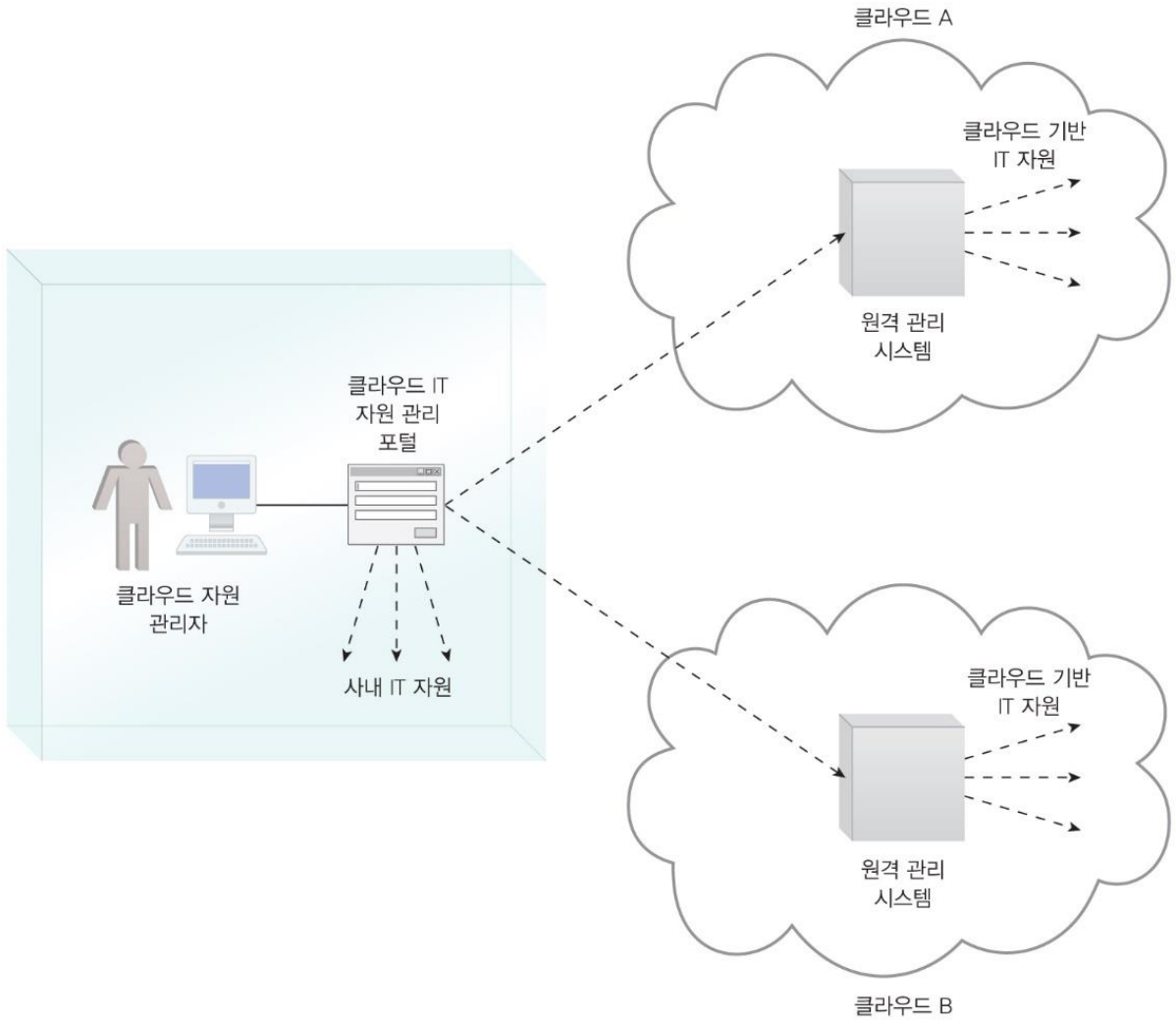


원격 관리 콘솔 작업

- 원격 관리 콘솔을 통해 클라우드 소비자가 수행할 수 있는 작업
  - 클라우드 서비스의 설정과 수립
  - 온디맨드식의 클라우드 서비스를 위한 IT 자원의 프로비저닝과 배포
  - 클라우드 서비스 상태와 사용, 성능의 모니터링
  - QoS와 SLA 달성의 모니터링
  - 임대 비용과 사용 요금의 관리
  - 사용 계정과 보안 자격, 허가, 접근 통제의 관리
  - 임대된 서비스의 내 외부 접근 추적
  - IT 자원 프로비저닝의 계획과 평가
  - 용량 계획

클라우드 IT 자원 관리 포털

- 원격 관리 시스템은 표준화된 API 제공 가능
- 클라우드 소비자는 표준화된 API 를 제공하는 다른 클라우드 제공자로 이동 가능
- 여러 클라우드 제공자 및 클라우드와 사내 환경에 있는 IT 자원으로부터 IT 자원을 임대하고 중앙 관리가 가능



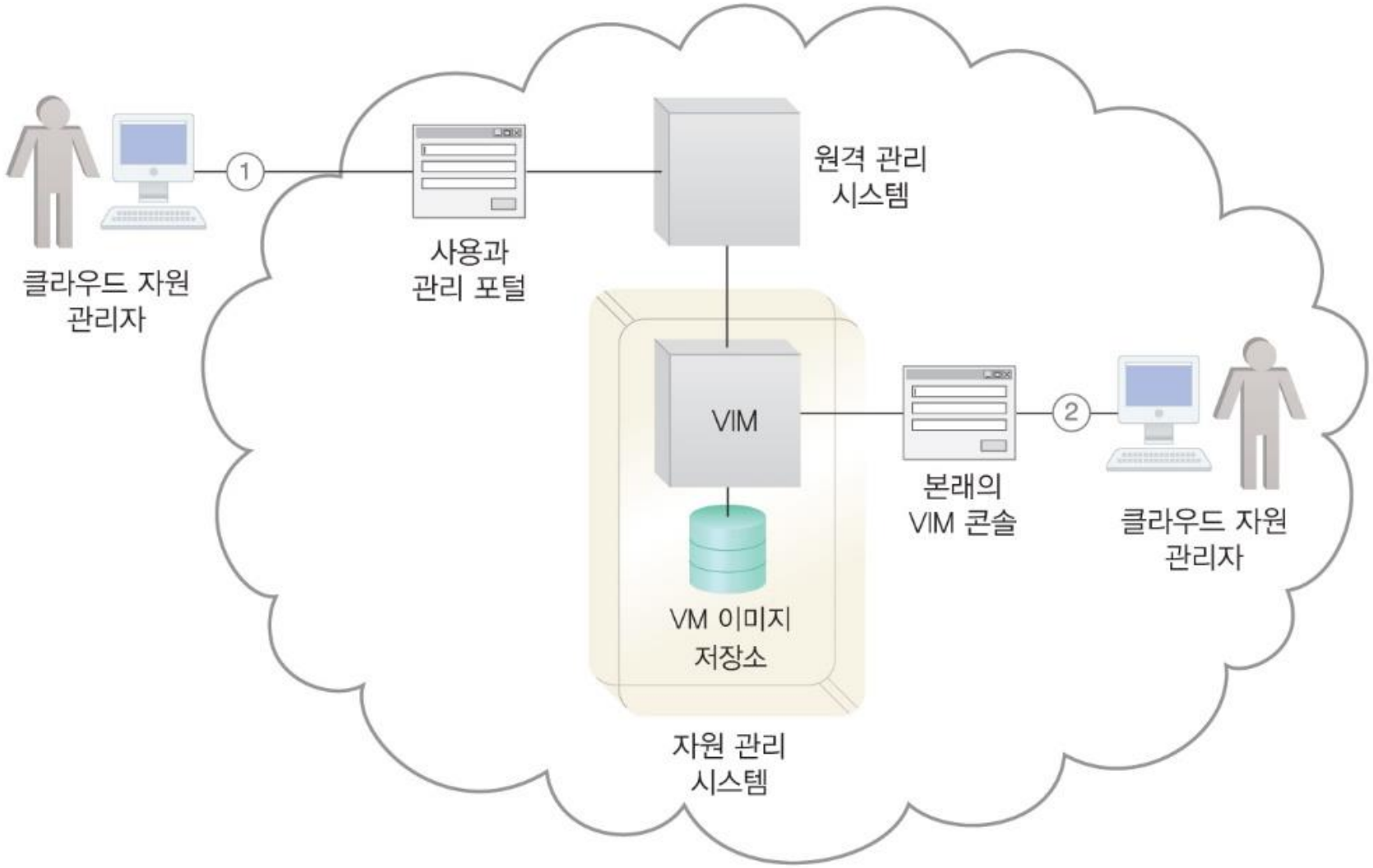
자원 관리 시스템

- 자원 관리 시스템 메커니즘은 클라우드 소비자와 클라우드 제공자에 의해 수행되는 관리 행동에 응해서 IT 자원 편성을 도움
- 가상 서버 인스턴스가 물리 서버로부터 편리하게 생성될 수 있도록 서버 하드웨어를 편성하는 가상 인프라 관리자VIM, Virtual Infrastructure Manager가 핵심
- VIM은 다수의 물리 서버를 가로질러 가상 IT 자원의 범위를 관리 가능
- VIM은 다른 물리 서버를 가로질러 하이퍼바이저의 다중 인스턴스를 생성하고 관리할 수 있거나 하나의 물리 서버에서 다른 물리 서버로 가상 서버 할당 가능

자원 관리 시스템을 통해 자동화되고 구현되는 작업

- 가상 서버 이미지와 같은 미리 만들어진 인스턴스를 생성하곤 하는 가상 IT 자원 템플릿을 관리하는 것
- 가상 IT 자원 인스턴스를 시작하고, 중단, 재개, 종료하는 것에 대응해 사용 가능한 물리 인프라에 가상 IT 자원을 할당하고 베포하는 것
- 자원 복제와 로드 밸런서, 대체 작동 시스템과 같은 다른 메커니즘의 포함에 응해 IT 자원을 편성하는 것
- 클라우드 서비스 인스턴스의 라이프 사이클 전반에 사용과 보안 정책을 집행하는 것
- IT 자원의 운용 조건을 모니터링 하는 것

클라우드 자원 관리자의 접근

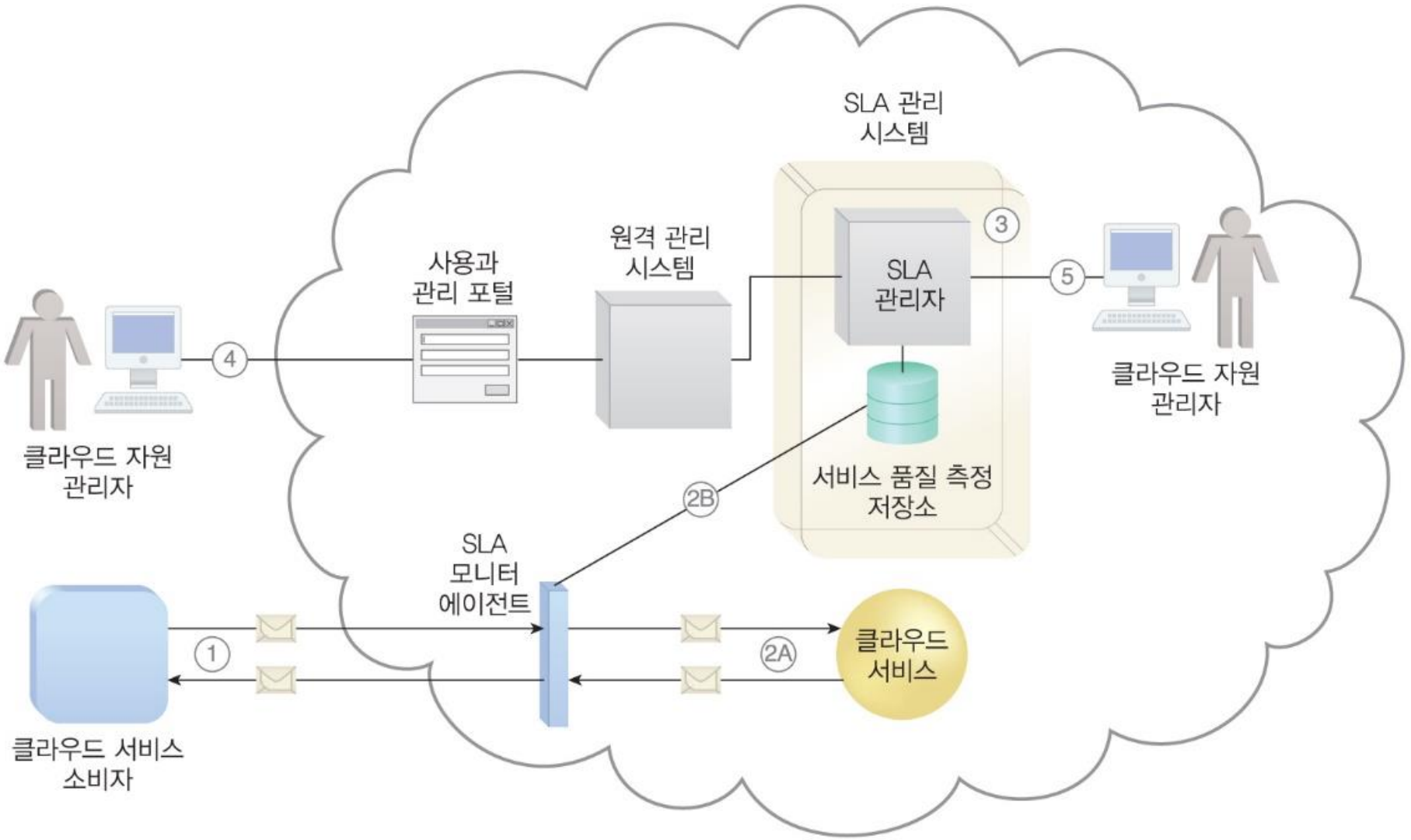


SLA 관리 시스템

- SLA 관리 시스템 메커니즘은 SLA 데이터의 관리와 모음, 저장, 보고, 실행 알림에 관계된 특징을 제공하는 상업적으로 사용 가능한 클라우드 관리 상품의 범위를 표현
- SLA 관리 시스템 배치는 미리 정의된 측정과 보고 매개변수에 기반을 두고 모여준 SLA 데이터를 저장하고 회수하기 위해 사용되는 저장소를 포함
- 활동 클라우드 서비스에 대해 진행 중인 피드백을 제공하기 위해 사용과 관리 포털에 실시간으로 사용할 수 있게 만들어질 수 있는 SLA 모니터 메커니즘에 의존
- 개별 클라우드 서비스를 위해 모니터 된 측정은 클라우드 프로비저닝 계약에 상응하는 SLA 보장과 함께 만들어짐

SLA 관리 시스템

SLA 관리 시스템 동작 메커니즘



과금 관리 시스템

- 과금 관리 시스템 메커니즘은 클라우드 제공자 회계와 클라우드 소비자 청구서를 보유하는 것처럼 사용 데이터의 모음과 처리 전용
- 과금 관리 시스템 구성요소가 저장소에 저장되는 실시간 사용 데이터를 청구서와 보고서, 송장 목적으로 모으기 위해 사용량당 과금 모니터에 의존
- 과금 관리 시스템은 클라우드 소비자당 혹은 IT 자원 기반당 맞춤형 가격 모델 뿐만 아니라 다른 가격 정책의 정의를 허용
- 가격 모델은 전통적인 과금 모델에서 고정 금액이나 할당당 과금 모델이나 혼합 구조까지 다양
- 사용량이 초과할 때, 과금 관리 시스템은 클라우드 소비자에 의해 추가 사용 요청을 차단할 수 있음

과금 관리 시스템

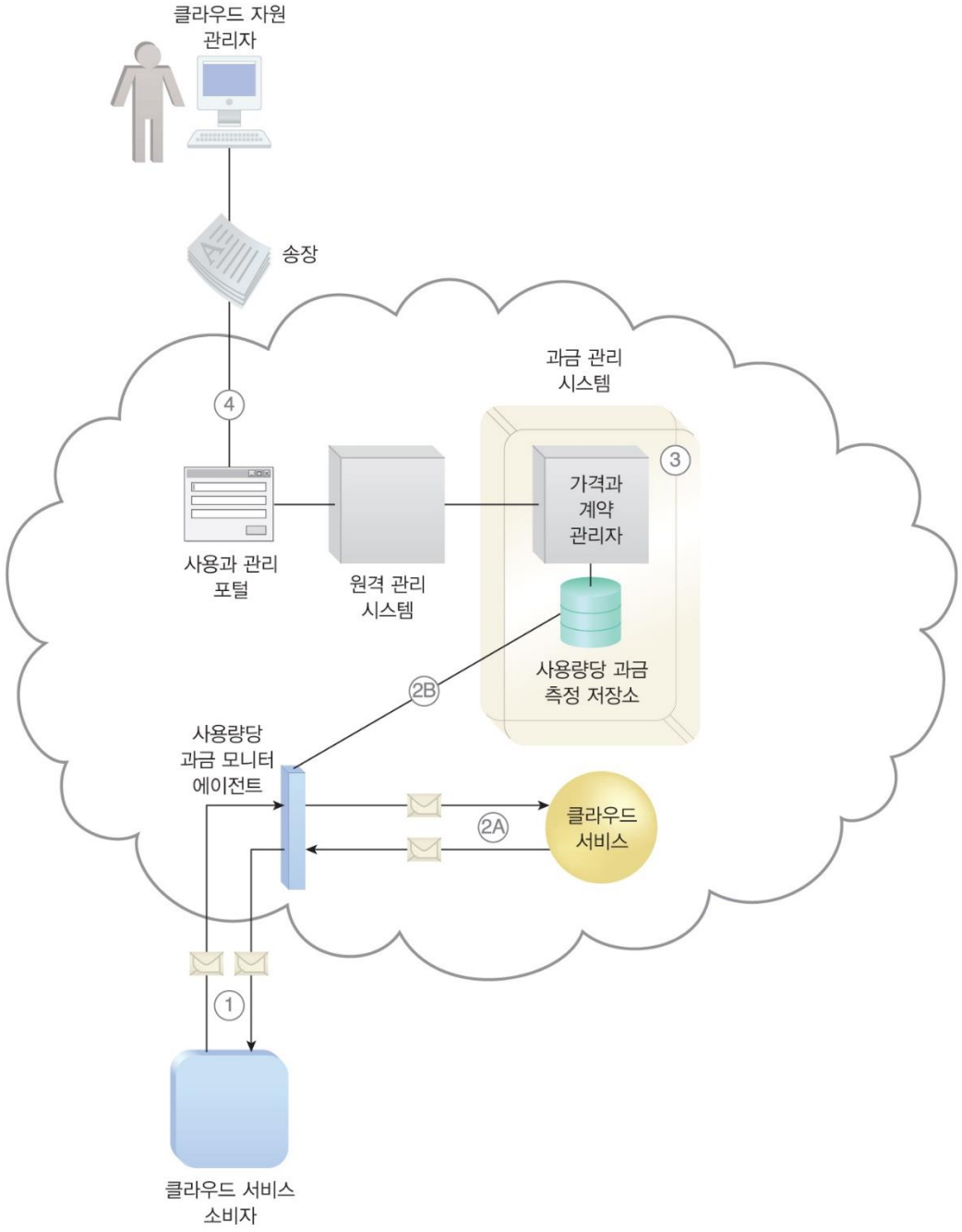
과금 관리 시스템 시나리오

① 클라우드 서비스 소비자는 클라우드 서비스와 메시지를 교환

② 사용량당 과금 모니터는 사용을 추적하고 과금 관리 시스템의 부분인 저장소에 전달(2B), 과금에 상응하는 데이터를 모음(2A)

③ 시스템은 주기적으로 통합된 클라우드 서비스 사용 요금을 계산하고, 클라우드 소비자를 위해 송장 발생

④ 송장은 사용과 관리 포털을 통해 클라우드 소비자에게 제공



클라우드 보안 메커니즘

- 암호화
- 해싱
- 디지털 서명
- 공개 키 인프라
- ID와 접근 관리 시스템
- 싱글 사인온
- 클라우드 기반 보안 그룹
- 보안 강화 가상 서버 이미지

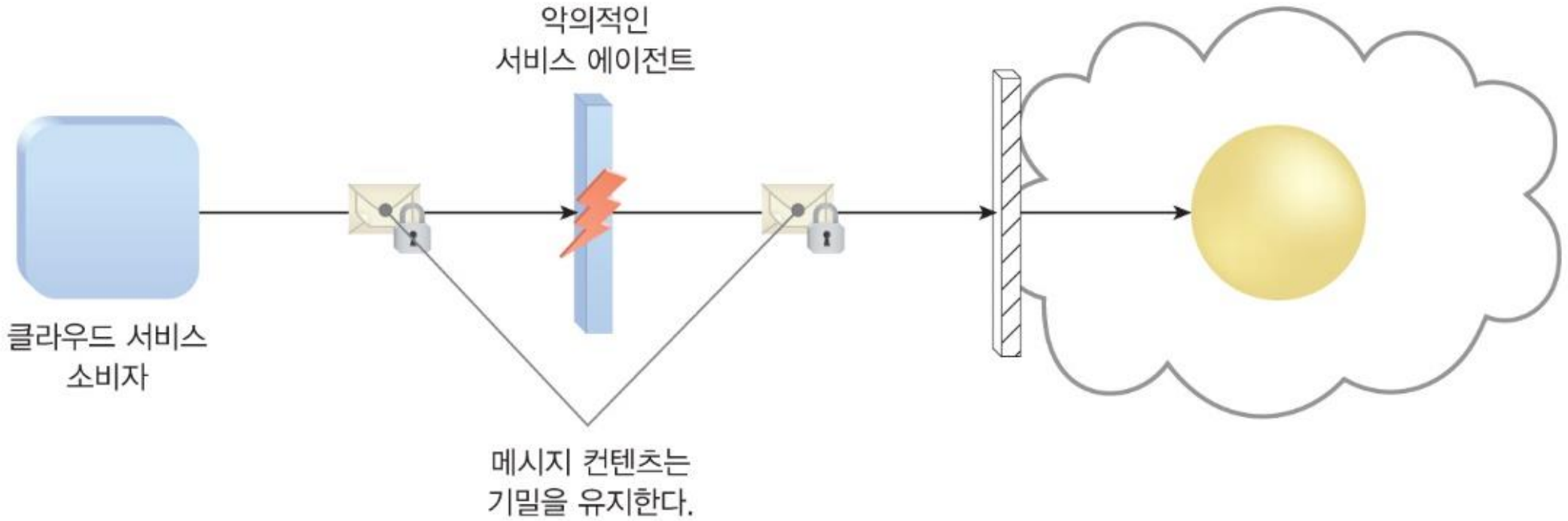
암호화

- 기본적으로 데이터는 읽을 수 있는 평문Plain Text 형식으로 취급
- 네트워크를 통해 전송될 때, 평문은 공인되지 않고 잠재적으로 악의적인 접근에 취약
- 암호화 메커니즘은 데이터의 기밀과 무결성을 보존하기 위한 전용 디지털 코딩 시스템
- 평문 데이터를 보호되고 읽을 수 없는 형식으로 암호화하기 위해 사용
- 암호화 기술은 일반적으로 본래의 평문 데이터를 암호화된 데이터로 변환하는 사이퍼cipher로 불리는 표준화된 알고리즘에 의존
- 암호문에 접근은 메시지 길이나 생성 일자와 같은 메타데이터의 몇 형식을 제외하고 본래의 평문 데이터를 알리지 않음

암호화

- 암호화가 평문 데이터에 쓰일 때, 데이터는 공인된 부분 사이에 의해 수립되고 공유되는 비밀 메시지인 암호화 키로 불리는 문자열과 병행
- 암호화 키는 암호문을 본래의 평문 형식으로 복호화하기 위해 사용
- 암호화 메커니즘은 트래픽 도청과 악의적인 중개자, 불충분한 권한, 중복된 신뢰 경계 보안 위협에 직면하는 것을 도움
- 예를 들어, 트래픽 도청을 시도하는 악의적인 서비스 에이전트는 암호화 키를 가지고 있지 않으면 전송 중의 메시지를 복호화할 수 없음

암호화



대칭 암호화

- 대칭 암호화는 하나의 공유된 키를 사용하는 공인된 부분에 의해 수행 (암호화와 복호화 모두를 위해 같은 키를 사용)
- 보안 키 암호 방식으로 알려진 특별한 키와 함께 암호화된 메시지는 같은 키에 의해서만 복호화 가능
- 데이터를 정당하게 복호화하는 부분은 본래의 암호화가 키를 정당하게 소유한 부분에 의해서 수행됐다는 증거와 함께 제공
- 키를 가지는 유일하게 공인된 부분이 메시지를 생성할 수 있기 때문에 기본 권한 확인은 항상 수행 (데이터 기밀을 유지하고 입증)
- 어느 부분이 메시지 암호화나 복호화를 수행했는지 정확하게 결정짓기는 불가능하므로 대칭 암호화는 부인 방지의 특징을 가지지 않음

비대칭 암호화

- 비대칭 암호화는 개인 키와 공개 키로 명명된 두 개의 다른 키의 사용에 의존
- 비대칭 암호화는 공개 키 암호 방식으로도 언급됨
- 공개 키는 일반적으로 사용 가능한 반면 개인 키는 소유자에게만 알려짐
- 개인 키와 암호화된 문서는 상응하는 공개 키로만 정확하게 복호화될 수 있음
- 역으로 공개 키와 암호화된 문서는 상대 개인 키를 사용해서만 복호화될 수 있음
- 한 개 대신 두 개의 다른 키를 사용하므로, 비대칭 암호화는 대체로 대칭 암호화보다 계산이 느림

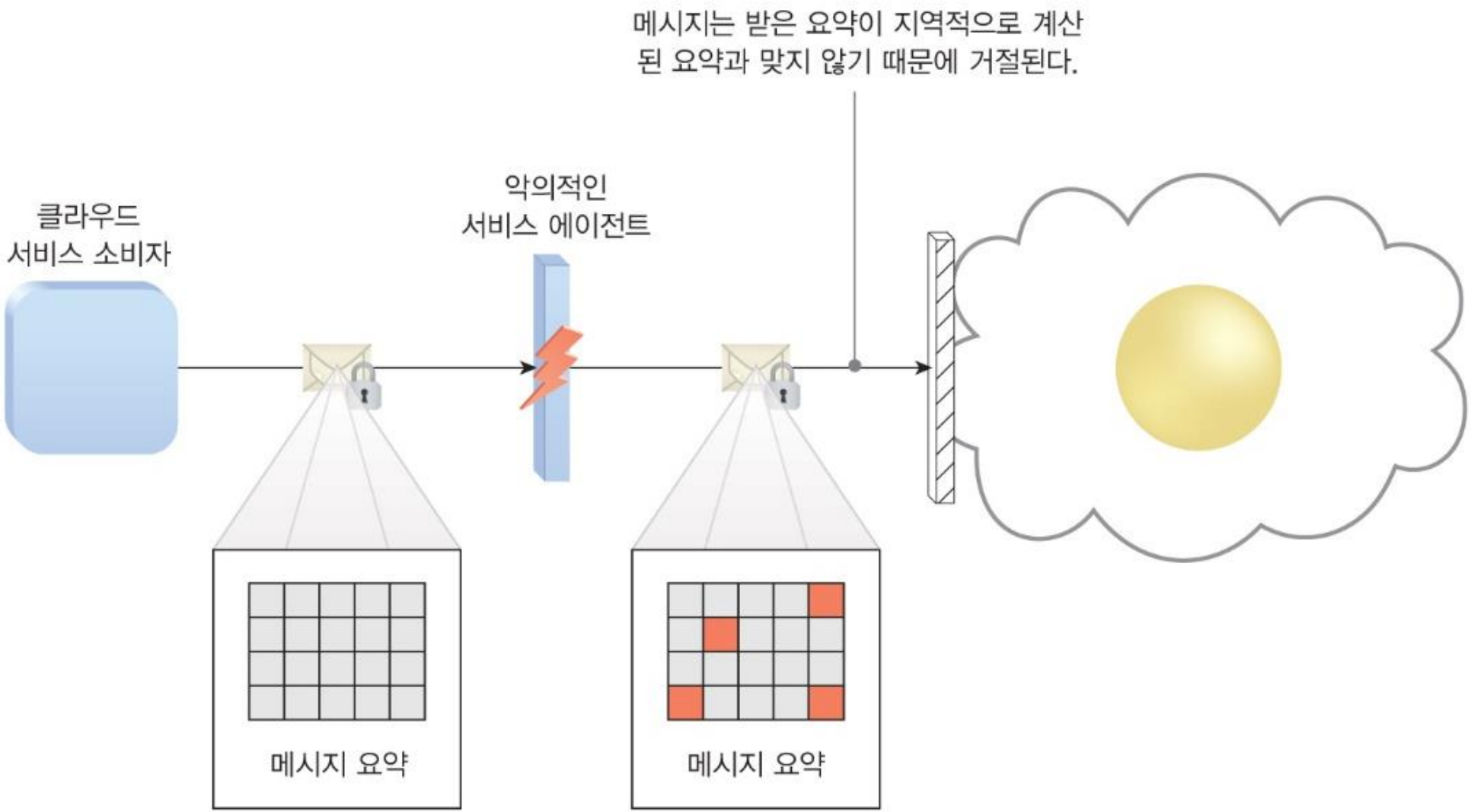
비대칭 암호화

- 비대칭 암호화는 개인 키인지 공개 키인지 평문 데이터를 암호화하기 위해 사용되었는지에 의해 보안 수준 결정
- 비대칭적으로 암호화된 메시지는 자신의 개인 공개 키를 쌍으로 가지기 때문에 개인 키와 암호화된 메시지는 상응하는 공개 키와 함께 정확하게 복호화될 수 있음
- 성공적인 복호화가 해당 본문이 정당한 공개 키 소유주에 의해 암호화되었음을 증명했을지라도 이 암호화 방법은 기밀 보호를 제공하지 않음
- 개인 키 암호화는 진위와 부인 방지에 더불어 무결성 보호를 제공
- 공개 키와 암호화된 메시지는 기밀 보호를 제공하는 정당한 개인 키 소유주에 의해서만 복호화 가능
- 공개 키 암호화 방법은 메시지 무결성이나 진위 보호도 제공하지 않음을 의미하는 암호문을 발생시킬 수 있음

해싱

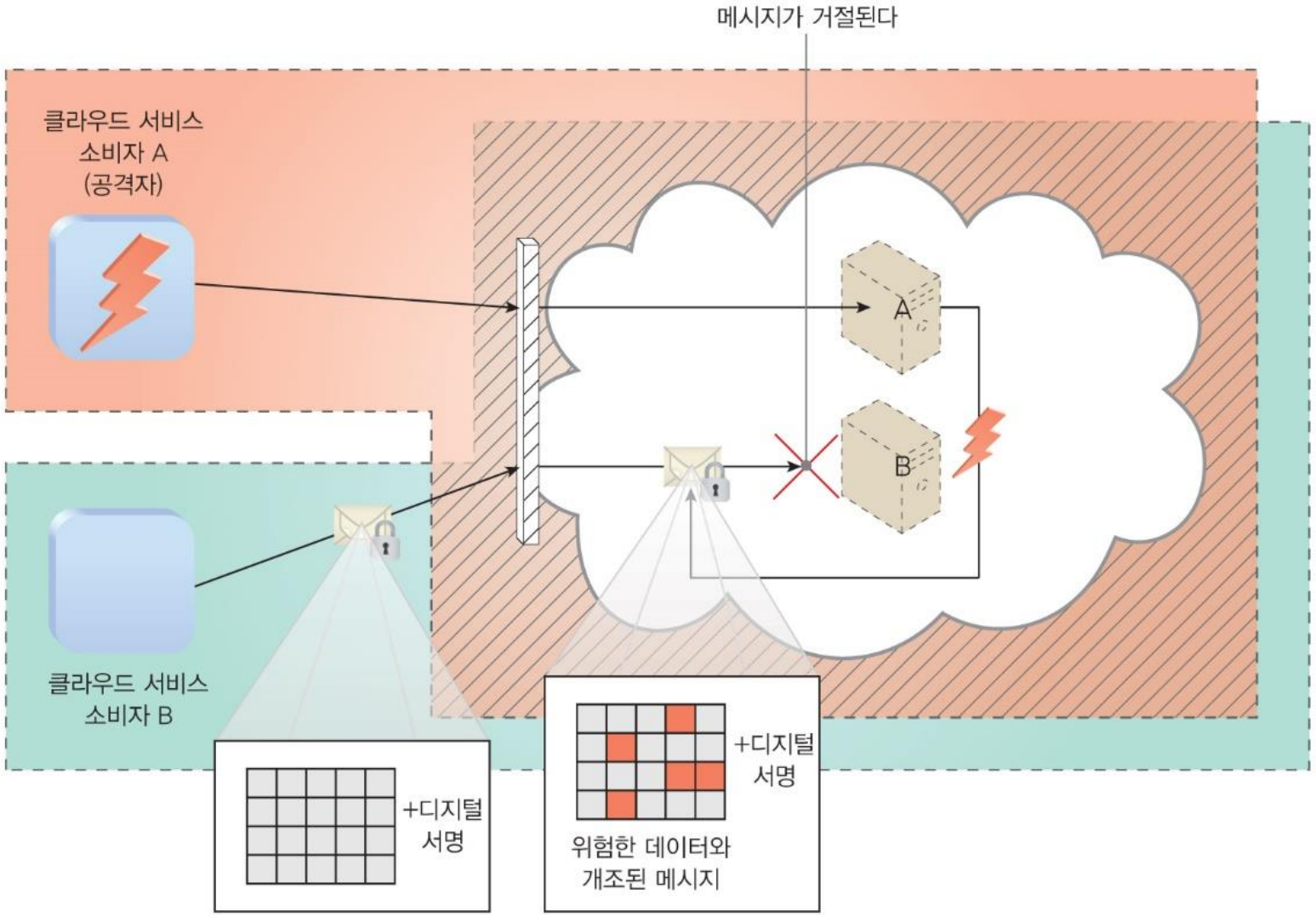
- 해싱 메커니즘은 데이터 보호의 단방향, 비역전 형태가 요구될 때 사용
- 일단 해싱이 메시지에 적용되면 잠기고, 키도 메시지 잠금 해지를 제공하지 않음
- 해싱 메커니즘의 일반적인 애플리케이션은 비밀번호의 스토리지
- 해싱 기술은 보통 고정 길이이고 원래의 메시지보다 작은 메시지로부터 해싱 코드나 메시지 요약을 끌어내기 위해 사용 가능
- 메시지 전송은 메시지 요약을 메시지에 부착하기 위해 해싱 메커니즘을 사용 가능
- 수신자는 제공된 메시지 요약이 메시지와 동행한 것과 같다는 것을 확인하기 위해 같은 해시 기능을 메시지에 지원
- 원래의 데이터 변조도 전체적으로 다른 메시지 요약이 되고 간섭이 발생하는 것을 분명히 가리킴

해싱 시나리오


메시지는 받은 요약이 지역적으로 계산
된 요약과 맞지 않기 때문에 거절된다.
클라우드
서비스 소비자
악의적인
서비스 에이전트
메시지 요약
메시지 요약

디지털 서명

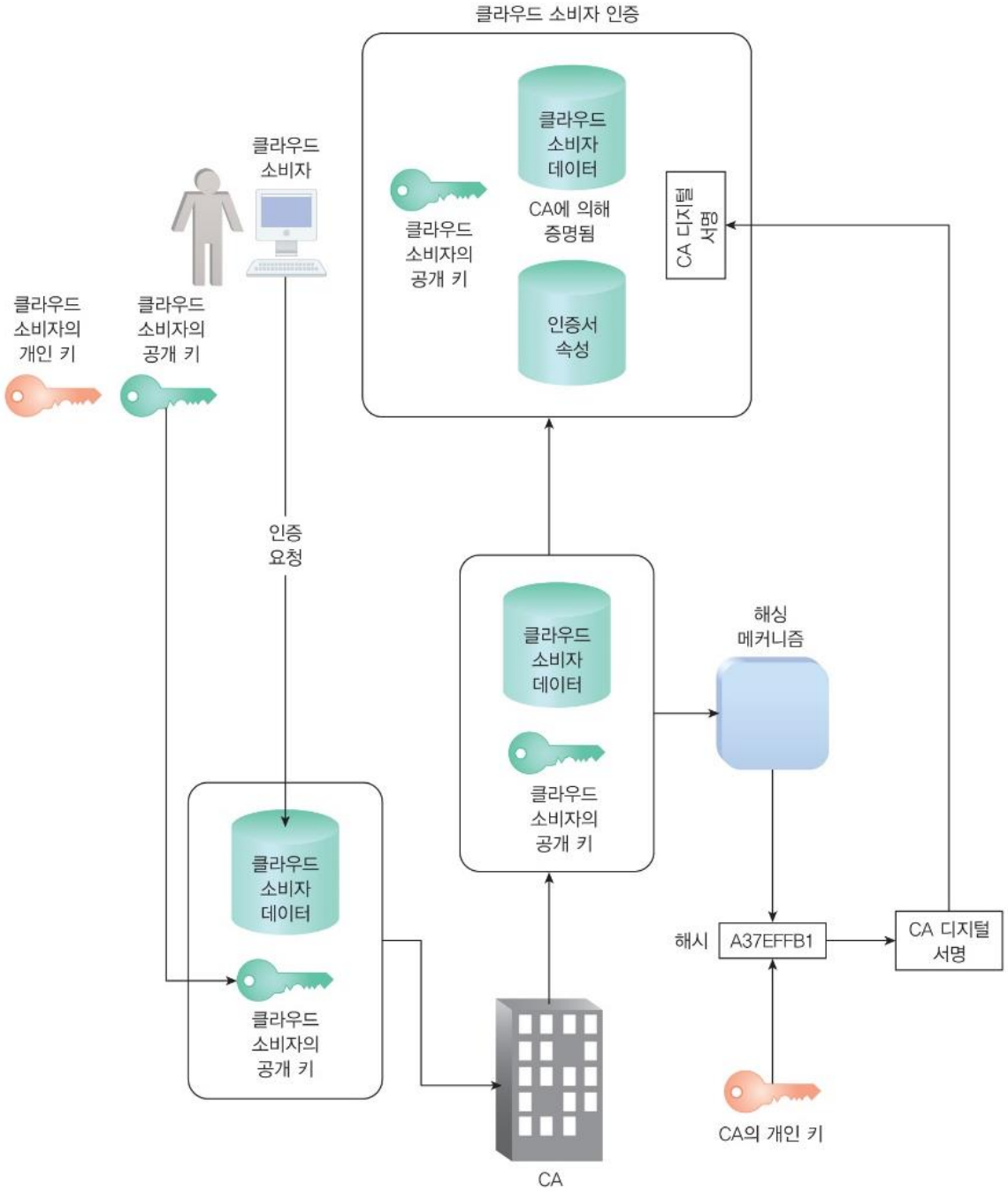
- 디지털 서명 메커니즘은 인증과 부인 방지를 통해 데이터 진위와 무결성의 제공 수단
- 메시지에 디지털 서명을 할당
- 메시지가 연속되는 공인되지 않은 수정을 경험하면 무효하게 만들어 전송
- 디지털 서명은 받은 메시지가 정당한 전송자에 의해 생성된 것과 같다는 증거 제공
- 해싱과 비대칭 암호화는 개인 키에 의해 암호화되고, 원래의 메시지에 덧붙이는 메시지 요약으로서 필수적으로 존재하는 디지털 서명 생성을 포함
- 수신자는 서명 유효성을 확인하고, 메시지 요약을 제공하는 디지털 서명을 복호화하기 위해 상응하는 공개키를 사용
- 해싱 메커니즘은 메시지 요약을 제공하기 위해 원래의 메시지에 적용될 수 있음
- 두 개의 다른 과정에서 같은 결과가 나오면 메시지가 무결성을 유지했음을 가리킴


메시지가 거절된다
클라우드 서비스
소비자 A
(공격자)
A
B
클라우드 서비스
소비자 B
+디지털
서명
+디지털
서명
위험한 데이터와
개조된 메시지

공개 키 인프라

- 비대칭 키의 배포를 관리하기 위한 일반적인 접근은 공개 키 암호 방식을 안전하게 사용하기 위해 대규모 시스템을 가능하게 하는 프로토콜과 데이터 형식, 규칙, 실행 시스템으로서 존재하는 공개 키 인프라PKI, Public Key Infrastructure 메커니즘에 기반을 둠
- 시스템은 키 유효성을 확인할 수 있게 하는 동안 상응하는 키 소유주(공개 키 식별로 알려진)와 공개 키를 연관짓기 위해 사용됨
- PKI는 사용자 ID와 유효성 기간과 같은 연관된 정보를 증명하기 위해 공개 키를 묶는 디지털 서명된 데이터 구조인 디지털 인증서의 사용에 의존
- 디지털 인증서는 일반적으로 제삼자의 인증서 권한CA, Certificate Authority에 의해 디지털 서명됨
- PKI는 비대칭 암호화 구현과 클라우드 소비자와 클라우드 제공자의 ID 정보를 관리
- PKI 메커니즘은 주로 불충분한 권한 위협에 대응하기 위해 사용

공개 키 인프라 단계


클라우드 소비자 인증
클라우드 소비자 데이터
CA에 의해 증명됨
클라우드 소비자의 공개 키
CA 디지털 서명
인증서 속성
클라우드 소비자
클라우드 소비자의 개인 키
클라우드 소비자의 공개 키
인증 요청
클라우드 소비자 데이터
클라우드 소비자의 공개 키
해싱 메커니즘
클라우드 소비자 데이터
클라우드 소비자의 공개 키
해시
A37EFFB1
CA 디지털 서명
CA의 개인 키
CA

ID와 접근 관리 시스템

- ID와 접근 관리 시스템IAM, ID and Access Management 메커니즘은 사용자 ID를 통제하고 추적하고, IT 자원과 환경, 시스템에 접근하기위해 필요한 구성요소와 정책을 포함
- IAM 메커니즘의 주요 구성요소
  - 인증: 디지털 서명과 디지털 인증, 생체 인식 하드웨어, 특화된 소프트웨어, 등록된 IP나 MAC 주소에 사용자 계정을 잠그는 것을 지원할 수 있는 IAM 시스템에 의해 관리되는 사용자 인증 인증서의 가장 일반적인 형태는 사용자 이름과 비밀번호 조합
  - 허가: 접근 통제를 위해 올바른 단위를 정의하고, ID와 접근 통제 권한, IT 자원 이용 가능성 사이의 관계를 감독
  - 사용자 관리: 시스템의 관리자 역량에 관계되는 사용자 관리 프로그램은 새 사용자 ID와 접근 그룹을 생성하고 비밀번호를 재설정하며, 비밀번호 정책을 정의, 특권을 관리하는 것에 책임이 있음
  - 자격 관리: 자격 관리 시스템은 불충분한 권한의 위협을 완화하는 정의된 사용자 계정을 위해 ID와 접근 통제 규칙을 수립
- IAM 메커니즘은 불충분한 권한과 서비스 거부, 중복된 신뢰 경계 위협 대응에 사용

싱글 사인온SSO, Single Sign-On

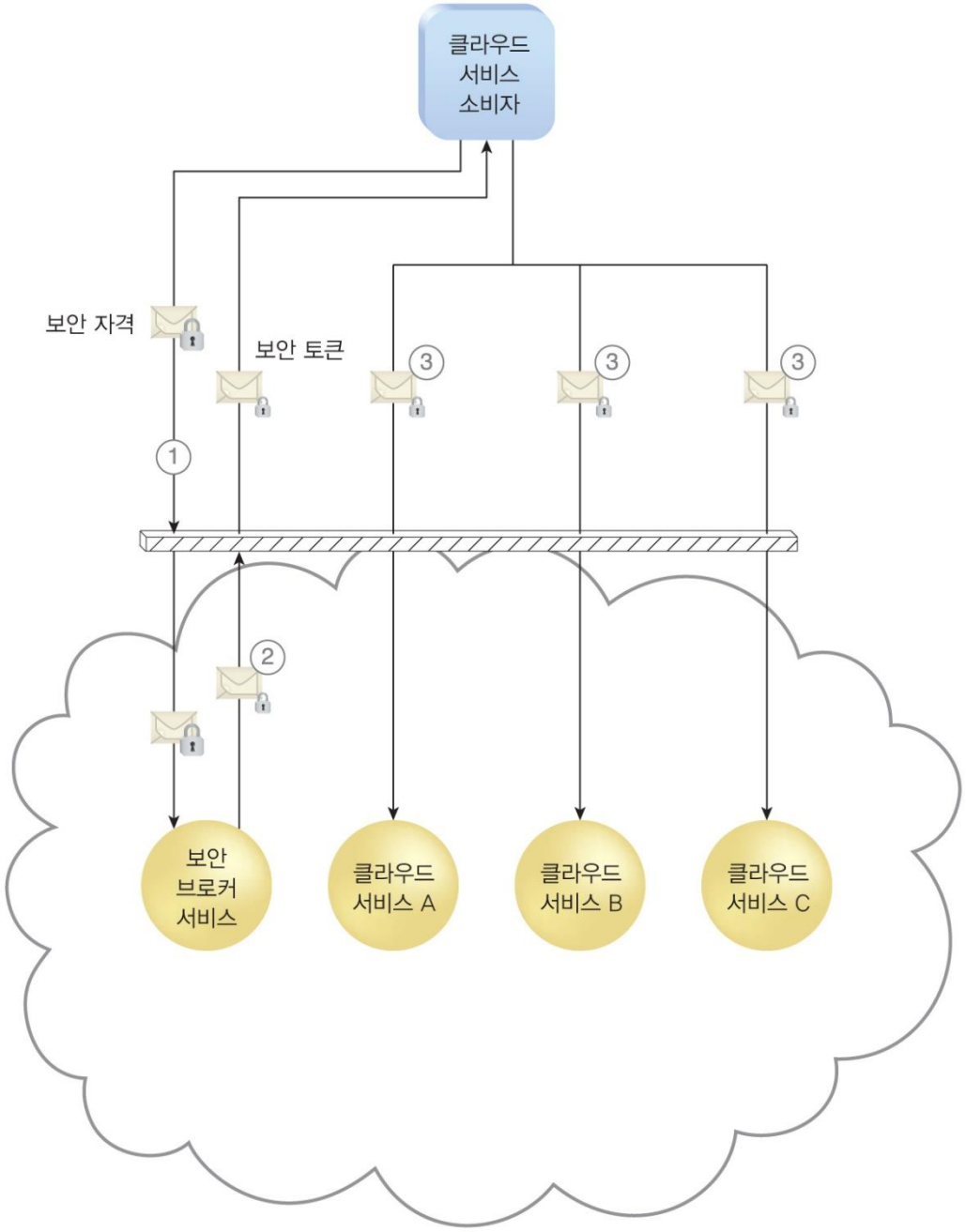
- 싱글 사인온 메커니즘은 클라우드 서비스 소비자가 다른 클라우드 서비스나 클라우드 기반 IT 자원에 접근하는 동안 지속하는 보안 문맥을 수립하는 보안 브로커에 의해 증명하는 것이 가능하게 함
- 클라우드 서비스 소비자가 모든 이어지는 요청과 함께 스스로 재증명하는 것을 필요로 함
- SSO 메커니즘은 근본적으로 상호 독립적인 클라우드 서비스와 IT 자원이 런타임 인증과 권한 자격을 발생시키고 계산하는 것을 가능하게 함
- 클라우드 서비스 소비자에 의해 초기에 제공된 자격은 보안 문맥 정보가 공유되는 동안 세션의 지속 동안 유효
- SSO 메커니즘의 보안 브로커는 특히 클라우드 서비스 소비자가 다른 클라우드에 있는 클라우드 서비스에 접근하는 것을 필요로 할 때 유용

싱글 사인온 시나리오

① 클라우드 서비스 소비자는 로그인 자격과 함께 보안 브로커를 제공

② 보안 브로커는 클라우드 서비스 A와 B, C 위에 클라우드 서비스 소비자를 자동으로 증명하기 위해 사용

③ 클라우드 서비스 소비자 ID 정보를 포함하는 성공적인 인증의 인증 토큰(작은 잠금기호와 메시지)을 제공

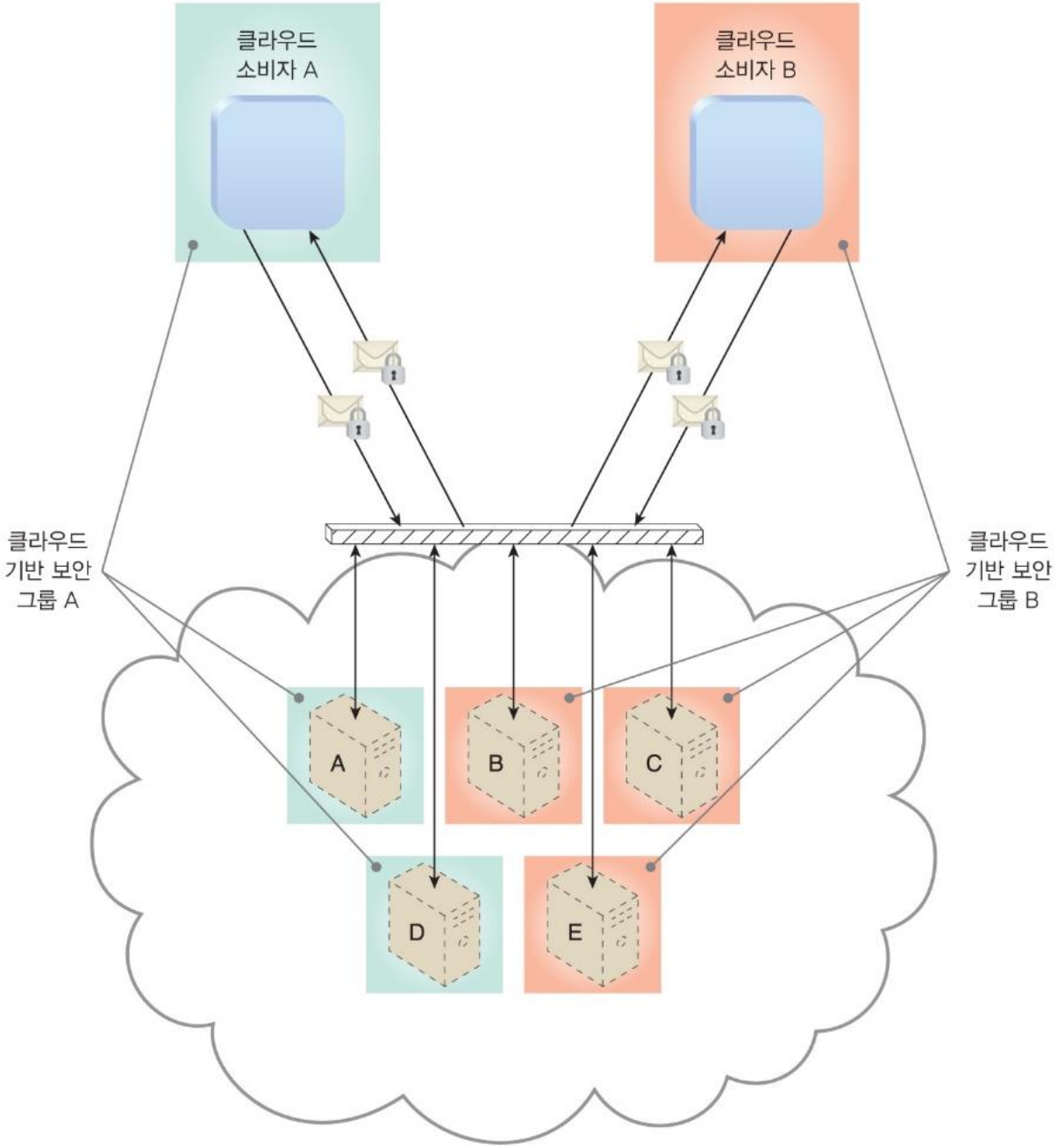


클라우드 기반 보안 그룹

- 클라우드 자원 분할은 분리된 물리와 가상 IT 환경이 다른 사용자와 그룹을 위해 생성되는 과정
- 자원 분할은 다양한 물리 IT 자원을 가상 머신에 할당하여 가상화를 가능하게 함
- 클라우드 기반 자원 분할 절차는 보안 정책을 통해 결정되는 클라우드 기반 보안 그룹 메커니즘을 생성
- 네트워크는 논리 네트워크 경계를 형성하는 논리적 클라우드 기반 보안 그룹으로 할당하며, 각 논리적 클라우드 기반 보안 그룹은 보안 그룹간의 통신을 통제하는 특별한 규칙에 할당
- 클라우드 기반 보안 그룹은 보안 위반의 이벤트 내의 IT 자원으로 공인되지 않은 접근을 제한하는 것을 돕고, 서비스의 거부와 불충분한 권한, 중복된 신뢰 경계 위협에 반박하는 것을 도울 수 있음

클라우드 기반 보안 그룹

- 클라우드 기반 보안 그룹 A는 가상 서버 A와 D를 포함하고, 클라우드 소비자 A에 할당
- 클라우드 기반 보안 그룹 B는 가상 서버 B와 C, E로 구성되고 클라우드 소비자 B에 할당
- 클라우드 서비스 소비자 A의 자격이 절충되면, 공격자는 클라우드 기반 보안 그룹 A 내의 가상 서버에 접근하고 훼손할 수 있기에 가상 서버 B와 C, E를 보호



보안 강화 가상 서버 이미지

- 가상 서버는 가상 서버 이미지로 불리는 템플릿 구성으로 부터 생성
- 보안 강화는 공격자에 의해 이용될 수 있는 잠재적 취약성을 제한하기 위해 시스템으로부터 불필요한 소프트웨어를 떼어내는 과정
- 불필요한 프로그램을 제거하고 불필요한 서버 포트를 닫고, 사용하지 않는 서비스와 내부 루트 계정, 방문자 접근을 비활성화하는 것은 보안 강화의 예
- 보안 강화된 가상 서버 이미지는 보안 강화 절차를 받는 가상 서버 인스턴스 생성을 위한 템플릿
- 일반적으로 본래의 표준 이미지보다 상당히 안전한 가성 서버 템플릿을 생성
- 보안 강화된 서버 이미지는 서비스 거부와 불충분한 권한, 중복된 신뢰 경계 위협에 대응하는 것을 도움

보안 강화 가상 서버 이미지