KOSA
Korea Software Industry Association

컴퓨터 네트워크와 보안

- Cloud 보안 실무 가이드 -

2022. 4. 23 (토요일)

정 준 수 PhD

과정 목표: Cloud 보안 실무 가이드

1. 클라우드 서비스란?

2. 클라우드 보안 아키텍처

3. 클라우드 보안 설계

4. 클라우드 보안관리 도구

    - IAM(Identity and Access Management)
    - S3(Simple Storage Service)
    - Lambda 함수와 API Gateway
    - CloudWatch Logs
    - Chalice Framework(Severless)

5. Splunk monitoring

클라우드 서비스란?

클라우드 서비스란 타사 제공업체가 호스팅하여 인터넷을 통해 사용자에게 제공하는 인프라, 플랫폼 또는 소프트웨어를 말합니다.

클라우드는 네트워크 전체에서 확장 가능한 리소스를 추상화, 풀링 및 공유하는 IT 환경입니다.
클라우드는 클라우드 환경 내에서 워크로드를 실행하는 동작인 클라우드 컴퓨팅을 지원합니다.

클라우드 서비스는 프론트엔드 클라이언트(예: 사용자의 서버, 태블릿, 데스크톱, 노트북 등 사용자의 모든 하드웨어)의 사용자 데이터 흐름을 원활하게 해줍니다. 사용자가 클라우드 서비스에 액세스하려면 컴퓨터, 운영 체제 및 인터넷 연결 또는 가상 프라이빗 네트워크(VPN)만 있으면 됩니다.

클라우드 서비스 유형

추가로 소프트웨어를 다운로드하지 않고도 인터넷을 통해 사용자가 액세스하는 모든 인프라, 플랫폼, 소프트웨어 또는 기술은 클라우드 컴퓨팅 서비스라고 볼 수 있으며 다음의 서비스형(as-a-Service) 솔루션이 포함됩니다.

1. 서비스로서의 인프라(Infrastructure-as-a-Service, IaaS)는 사용자에게 컴퓨팅, 네트워킹 및 스토리지 리소스를 제공합니다.
2. 서비스로서의 플랫폼(Platforms-as-a-Service, PaaS)은 애플리케이션을 실행할 수 있는 플랫폼과 플랫폼 실행에 필요한 IT 인프라를 제공합니다.
3. 서비스로서의 소프트웨어(Software-as-a-Service, SaaS)는 클라우드 애플리케이션과 해당 애플리케이션을 실행하는 플랫폼, 플랫폼의 기반 인프라를 제공합니다.
4. 서비스로서의 기능(Function-as-a-Service, FaaS)은 이벤트 기반 실행 모델로서, 개발자가 인프라를 유지관리하지 않고도 애플리케이션 패키지를 기능으로 구축, 실행 및 관리할 수 있도록 지원합니다.

클라우드 운영 유형

프라이빗 클라우드는 대략적으로 정의하자면 최종 사용자 전용 클라우드 환경으로, 대개는 사용자의 방화벽 내에 있으며 가끔 온프레미스에 있기도 합니다.

퍼블릭 클라우드는 최종 사용자가 소유하지 않은 리소스에서 생성되어 다른 테넌트에 재배포될 수 있는 클라우드 환경입니다.

하이브리드 클라우드는 어느 정도의 워크로드 이식성, 오케스트레이션 및 관리 기능을 갖춘 멀티플 클라우드 환경입니다.

멀티클라우드는 네트워크 연결에 상관없이 2개 이상의 클라우드(퍼블릭 또는 프라이빗)를 포함한 IT 시스템입니다.

클라우드 서비스 작동 방식

다른 모든 IT 솔루션과 마찬가지로 클라우드 서비스는 하드웨어 및 소프트웨어를 기반으로 합니다. 그러나 전통적인 하드웨어 및 소프트웨어 솔루션과는 달리, 컴퓨터, 네트워크 연결, 클라우드 서비스에 액세스하기 위한 운영 체제 등만 있으면 클라우드 서비스를 사용할 수 있습니다.

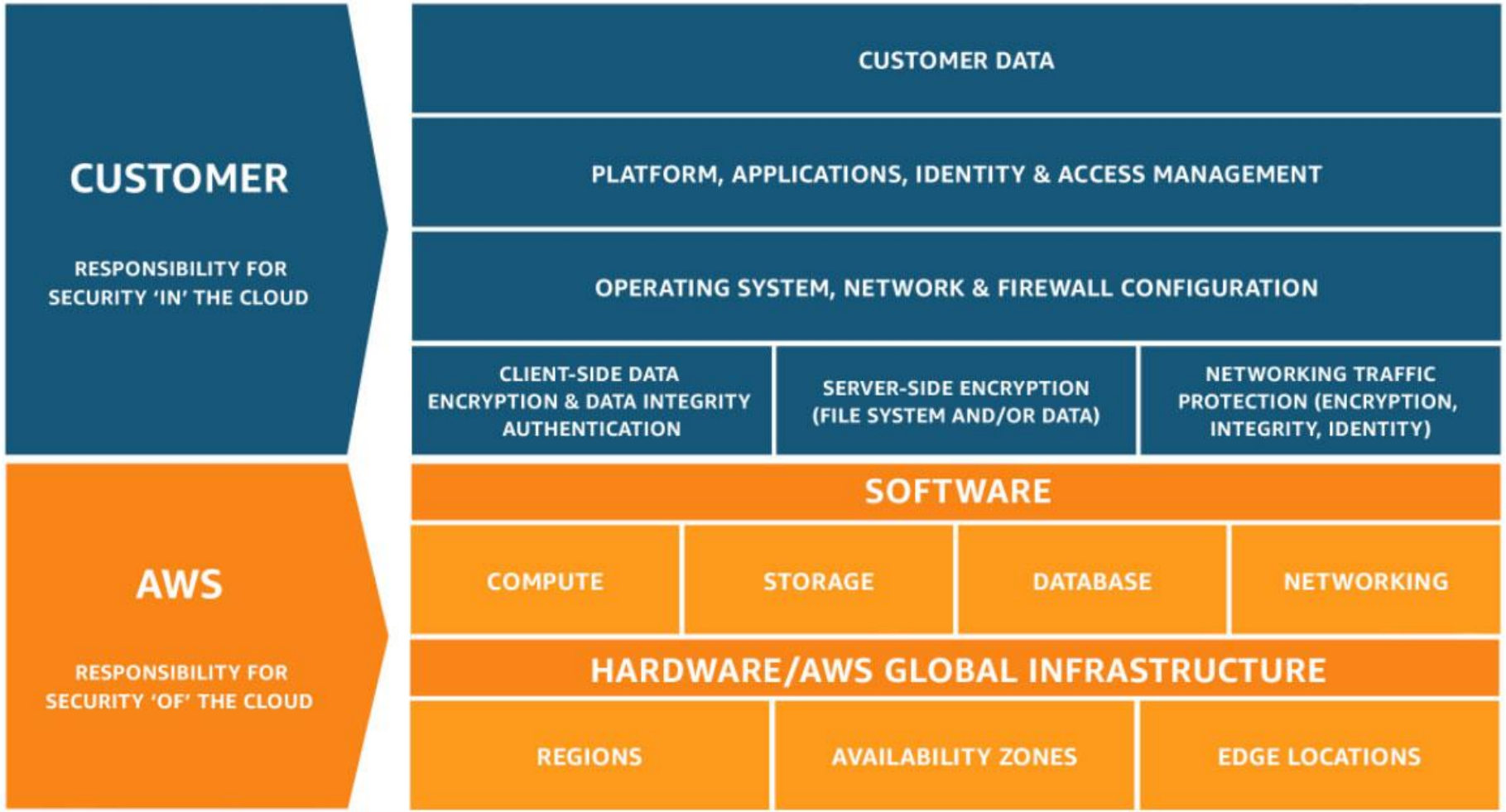
추상화는 보통 가상화 및 가상 머신을 통해 실현됩니다. 일단 분리되면 스토리지, 컴퓨팅 및 네트워킹 구성 요소가 인터넷을 통해 사용자에게 인프라 또는 IaaS로 제공됩니다.

클라우드 환경을 사용하는 애플리케이션 런타임 환경의 변화다. 런타임 환경이란 프로세스나 애플리케이션을 위한 서비스를 제공하는 가상머신의 상태를 말한다.

클라우드 보안의 필요성

클라우드 보안은 클라우드에 있는 모든 데이터와 서비스가 가용성, 무결성 및 기밀성 공격이나 침해로부터 보호되도록 하는 조치입니다.

클라우드 서비스 제공 업체는 안전한 클라우드 인프라를 제공합니다. 그러나 고객은 책임 공유 모델을 통해 클라우드에서 실행되는 워크로드, 애플리케이션 및 데이터를 보호할 의무가 있습니다.

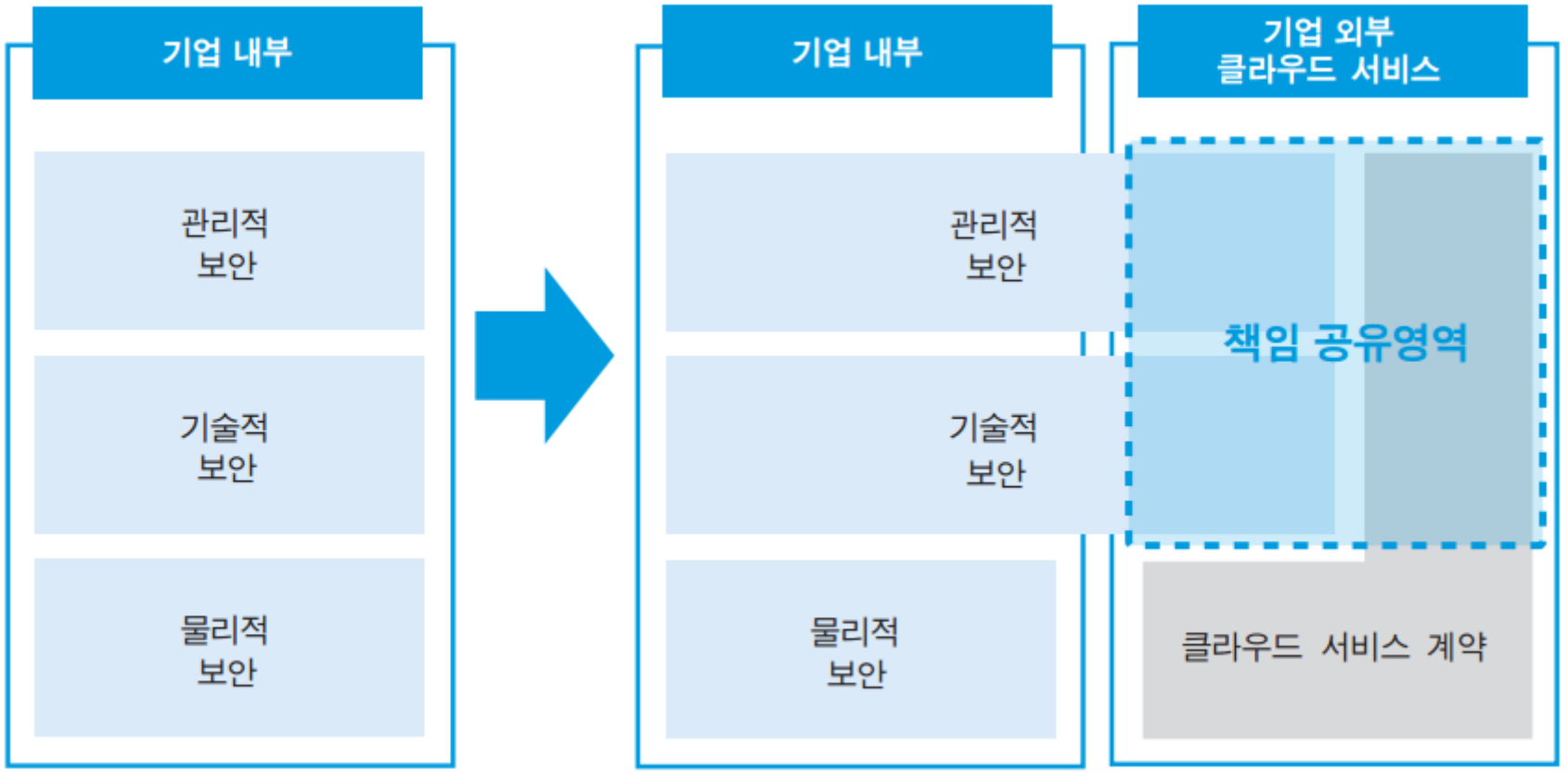


위 그림은 아마존웹서비스(AWS)에서 기업과 클라우드 서비스 사업자 간의 보안 책임 범위를 설명한 것입니다. AWS 가 서비스하는 하드웨어, 네트워크, 시스템 등은 AWS 의 책임 범위이고 그 위에 고객이 직접 관리하는 영역에서의 보안, 예를 들어 네트워크 트래픽 관련 보안, 방화벽 설정, 암호화, 애플리케이션, 접근 제어, 데이터 보안 등은 모두 고객의 책임이라고 이야기하고 있습니다.

위 그림은 애저(Azure)의 공동 책임 모델이다. 그림에서 파란색으로 표기된 것이 고객, 회색이 마이크로소프트사의 책임 범위입니다. IaaS, PaaS, SaaS 등의 서비스 유형에 따라서 마이크로소프트사와 고객의 책임 범위가 달라진다는 것을 보여주고 있습니다.

결론적으로 기존의 온프레미스 환경에서는 기업이 모든 책임을 지지만, 클라우드 환경에서는 CSP(Cloud Service Provider)와 기업이 각 범위를 나누어서 보안을 책임져야 하며, 이를 보안 담당자는 명확히 인지해야 합니다.

클라우드 보안의 책임 범위



클라우드 보안사고 사례

클라우드 환경에서 주요 보안 사고

날짜	보안사고 원인(내부자 관리 실수)	내용
2015년 09월	클라우드서비스제공기업(CSP) 실수	A사 내부 작업 중 장애 발생 (넷플릭스, 에어비앤비 등 서비스 중단)
2017년 03월	클라우드서비스제공기업(CSP) 실수	A사 S3서버 관리자 실수 (애플, 에어비앤비, 핀터레스트 등 서비스 중단)
2018년 11월	클라우드서비스제공기업(CSP) 실수	A사 서울리전 DNS 서버 설정 오류 (나이키, 넥슨, 쿠팡 등 서비스 중단)
06월	고객사 실수	인도 혼다자동차 관리자실수 (개인정보 5만건 유출)
07월	고객사 실수	중국 텐센트 직원 실수 (고객사 데이터 및 백업파일 삭제)
2019년 01월	고객사 실수	클라우드 계정 관리 실수 (개인정보 2400만건 유출)
	고객사 실수	A사 엘라스틱서치 서버 설정 미흡 (고객정보 대량 유출)

자료:안랩

https://blog.lgcns.com/2131

클라우드 보안 아키텍처

클라우드의 보안은 기본 아키텍처에 보안 요소를 추가하는 클라우드 보안 아키텍처에서 시작됩니다. 기존 보안 요소에는 방화벽 (FW), 맬웨어 방지 및 침입감지시스템 (IDS)이 포함됩니다. 클라우드 감사자, 보안 설계자 및 보안 엔지니어를 포함하여 클라우드 내에서 그리고 클라우드를 통해 보안 구조를 설계하는 사람들도 필요합니다.
즉, 클라우드 보안 아키텍처는 하드웨어나 소프트웨어에만 국한되지 않습니다.

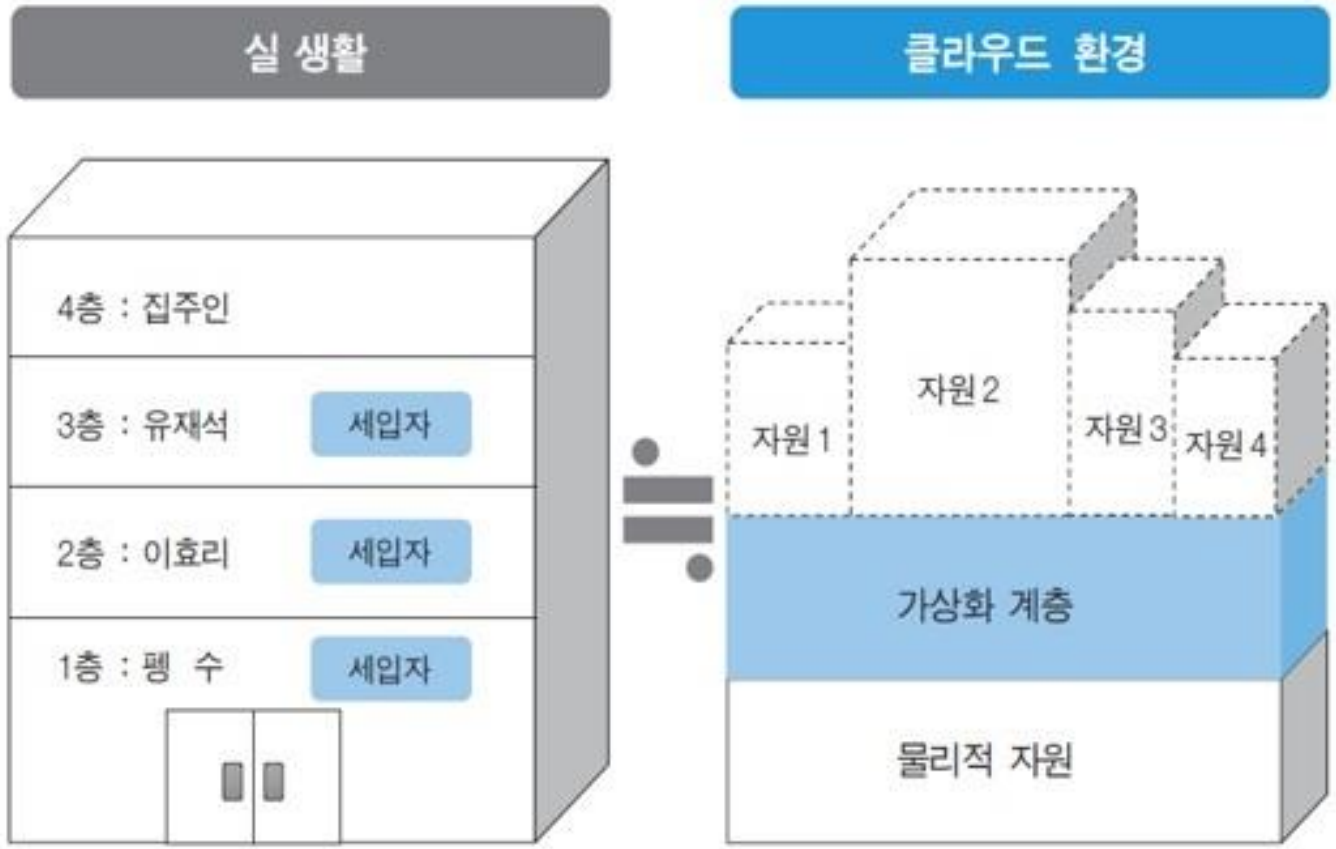
클라우드 보안 아키텍처는 위험 관리에서 시작됩니다. 무엇이 잘못 될 수 있고 비즈니스에 부정적인 영향을 미칠 수 있는지 아는 것은 기업이 책임 있는 결정을 내리는 데 도움이 됩니다. 세가지 중요한 영역은 비즈니스 연속성, 공급망 및 물리적 보안입니다.

클라우드 보안 설계

1. 멀티테넌시(Multi-Tenancy)

클라우드 서비스 제공자(AWS, Azure, 삼성SDS 등)가 다수의 클라우드 사용자에게 가상화 기술을 통해 물리적 자원을 논리적으로 분할하고 격리해서 빌려주는 것입니다. 여기서 클라우드 서비스 제공자가 만든 공용 영역(클라우드 관리 포털, 물리적 자원의 전원 관리, 상면 관리 등)은 제공자가 직접 관리하고, 클라우드 사용자는 빌린 자원의 운영 체제 설정 변경, 접속 계정 생성, 소프트웨어 설치 등의 내부적인 설정 작업만을 수행하게 됩니다.

단, 물리적인 자원을 함께 사용하는 만큼, 보안상의 버그, 중요 데이터 노출 등을 유의해야 합니다.없어서 정리해보았다.

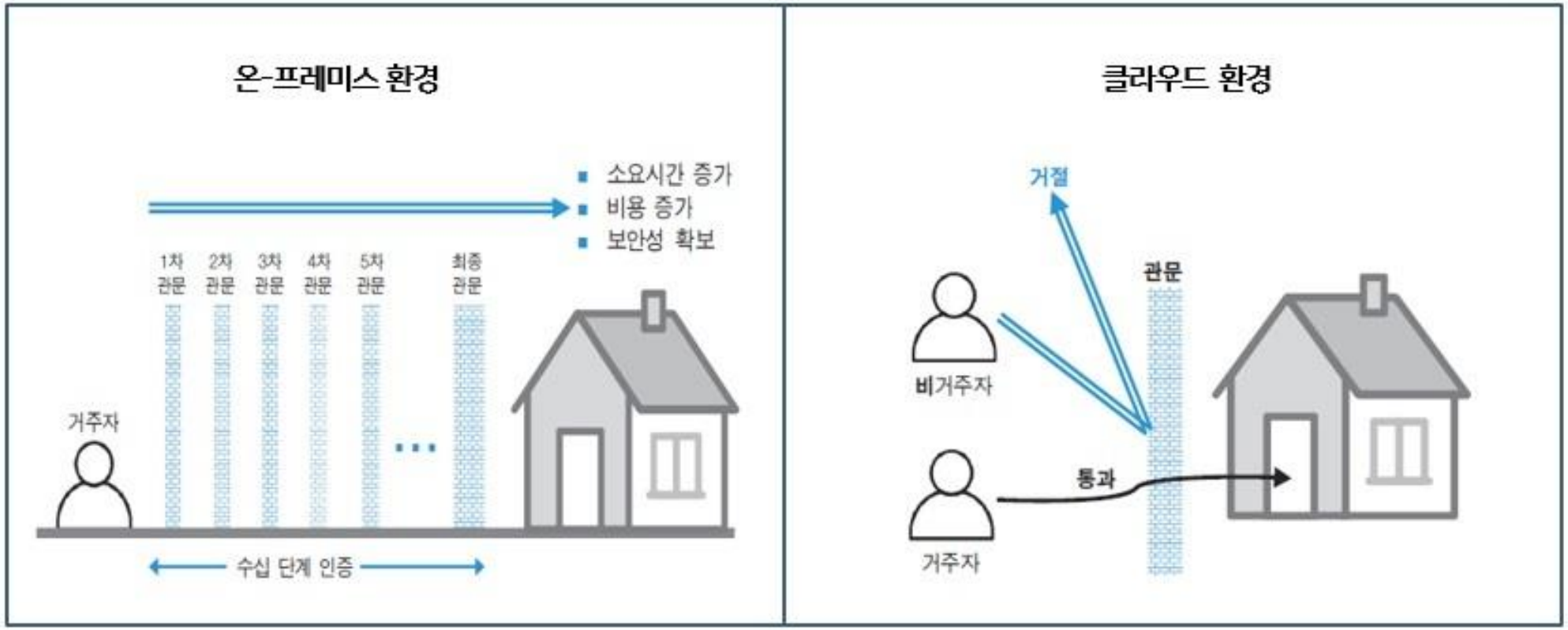


멀티테넌시(Multi-Tenancy)

클라우드 보안 설계

2. 접근성(Accessibility)

접근성은 인터넷을 통해 클라우드 서비스와 자원으로 쉽게 접근할 수 있는 속성입니다. 기존 온-프레미스 환경에서는 자원으로 접근을 위해 각 경계별 방화벽과 보안 장비를 구축하여 수 차례의 보안 접근 절차를 진행합니다. 하지만 클라우드 환경은 제공되는 방화벽과 접근 통제 목록(ACL : Access Control List) 등을 활용한 단순 버튼 클릭만으로 바로 보안 수준을 조절할 수 있습니다. 이를 통해 언제 어디서든 어떠한 디바이스를 사용하더라도 유연성있게 접근할 수 있다고 합니다. 하지만 그만큼 사용자로서 보안과 권한 부여, 회수, 인증/인가 체계를 철저히 신경써야 합니다.

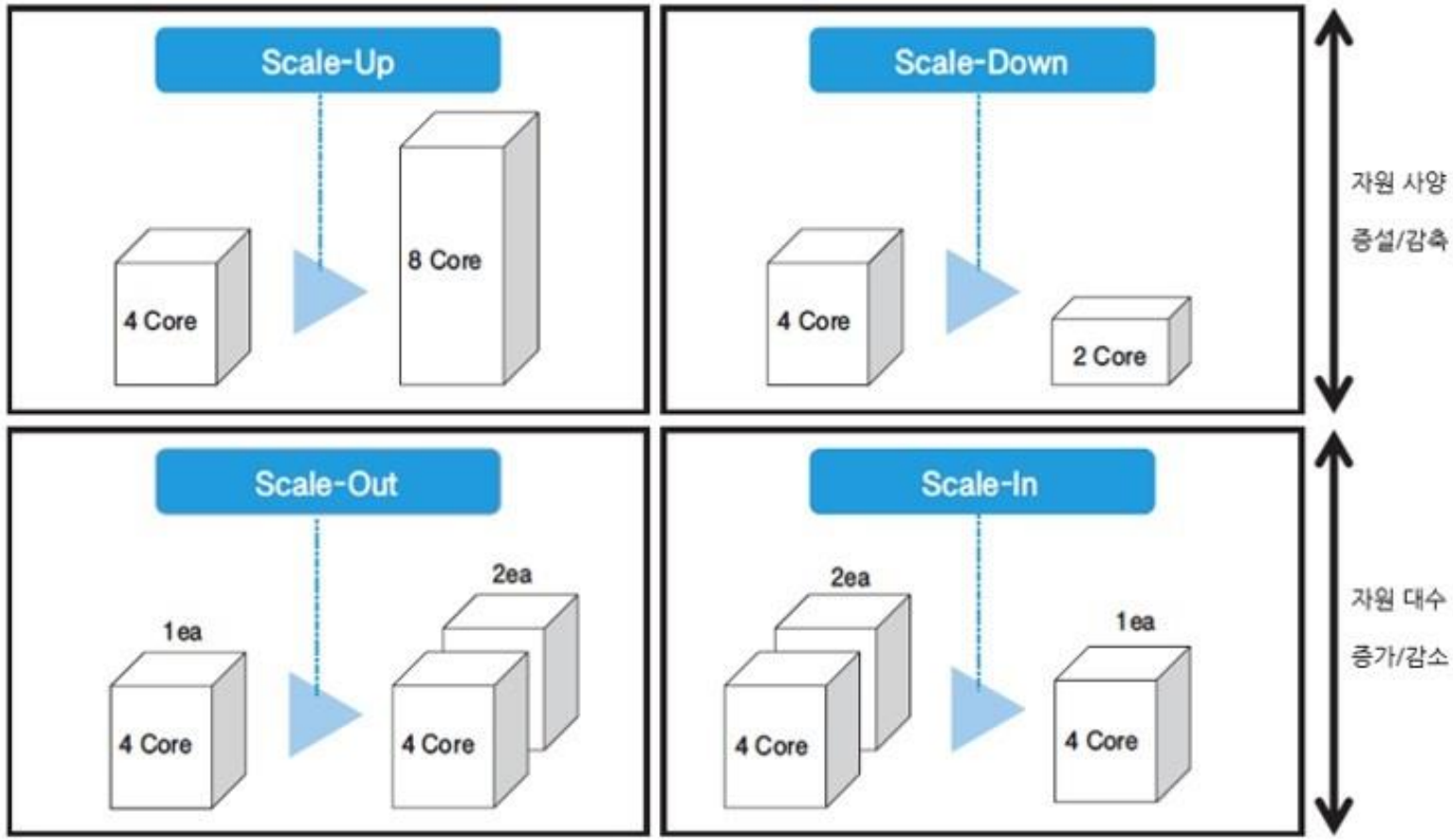


접근성(Accessibility)

클라우드 보안 설계

3. 탄력성(Elasticity)

탄력성은 새로운 자원이 추가되기도 하고 삭제되기도 하는 속성입니다. 이는 스케일 업(Scale-Up : 자원 사양이 늘어남), 스케일 다운(Scale-Down : 자원 사양이 줄어듦), 스케일 아웃(Scale-Out : 동일한 자원이 새로 생성), 스케일 인(Scale-In : 동일한 자원 그룹 중 자원이 삭제) 등의 작업을 클라우드 환경에서 손쉽게 수행할 수 있음을 의미합니다. 즉, 클라우드는 언제든지 변화할 수 있는 동적인 특성을 갖고 있습니다. 하지만 이는 클라우드 권한 남용으로 인한 무분별한 자원 증설, 자원 삭제 등의 위협이 내재되어 있습니다.



탄력성(Elasticity)

클라우드 보안 설계

4. 특수성 - 책임 추적성(Accountability)

책임 추적성이란 클라우드에 접근해서 자원을 활용하는 식별된 사용자의 행위를 기록, 수행한 행위에 대해 책임을 부여하는 전반적인 활동을 뜻합니다. 책임 추적성은 '식별(Identification)', '인증(Authentication)', '인가(Authorization)', '로깅(Logging)', '모니터링(Monitoring)', '감사(Audit)' 등 일련의 6가지 과정을 수행해야 만족할 수 있다.

클라우드 보안 실무 가이드: 보안관리 도구

1. Access Key
2. IAM 사용자 계정 관리(Resource 에 대한 접근 관리)
3. CloudTrail
4. Cloud watch
5. Ansible
6. Lambda 서비스를 활용한 자동화 실습
7. S3 데이터 암호화

정 준 수 / Ph.D （ jsjeong@hansung.ac.kr ）

- 前) 삼성전자 연구원
- 前) 삼성의료원 (삼성생명과학연구소)
- 前) 삼성SDS (정보기술연구소)
- 現) (사)한국인공지능협회, AI, 머신러닝 강의
- 現) 한국소프트웨어산업협회, AI, 머신러닝 강의
- 現) 서울디지털재단, AI 자문위원
- 現) 한성대학교 교수(겸)
- 전문분야: Computer Vision, 머신러닝(ML), RPA
- https://github.com/JSJeong-me/