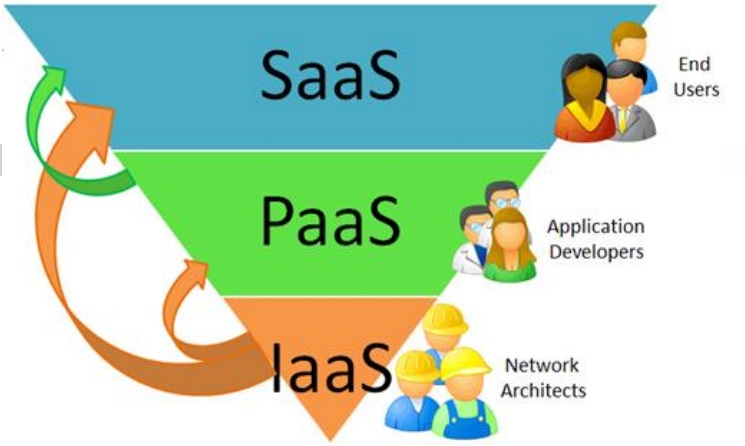
클라우드, 과연 보안에 취약한가?

박대하

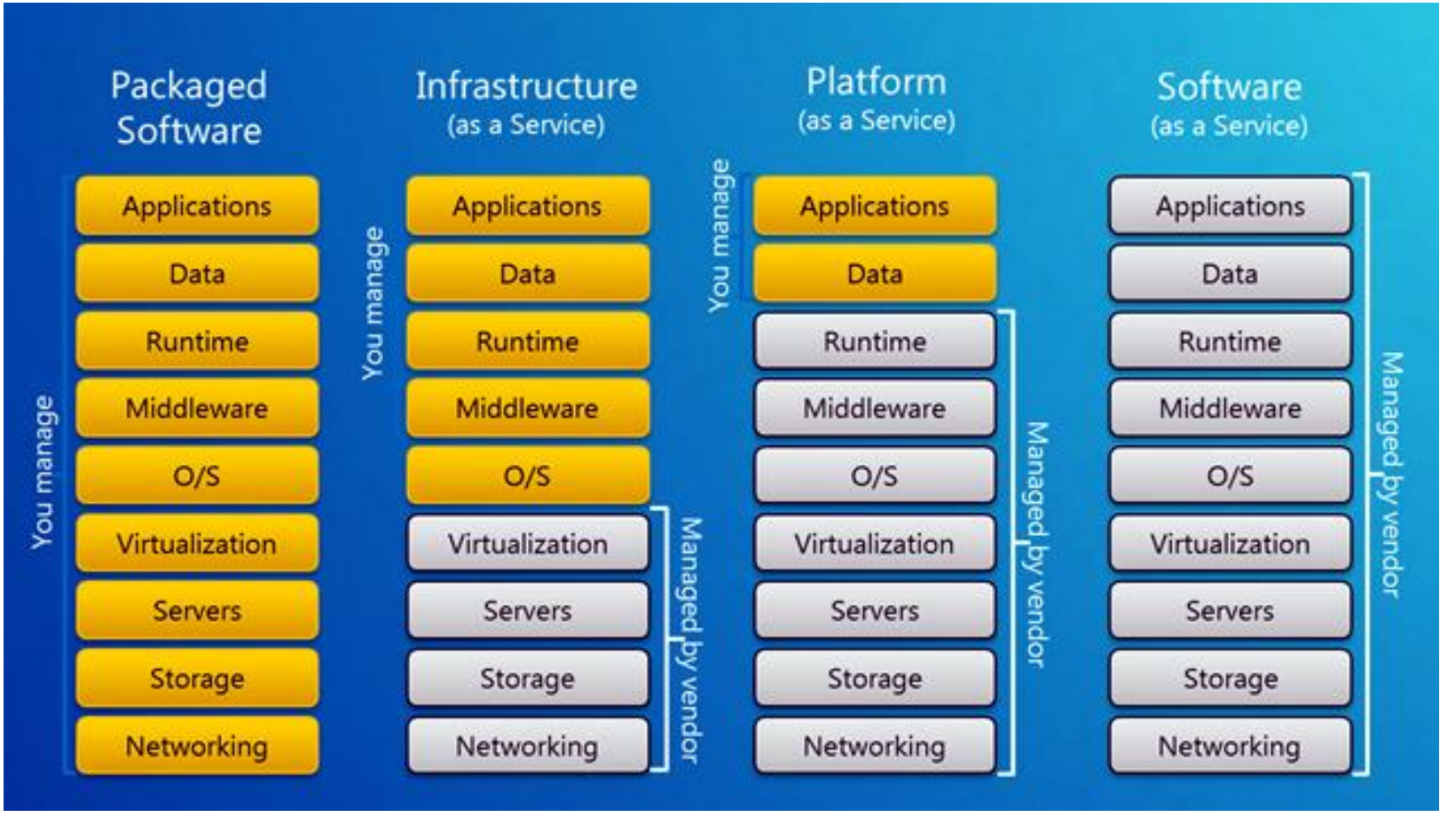
고려사이버대학교
정보관리보안학과

2015.12.15

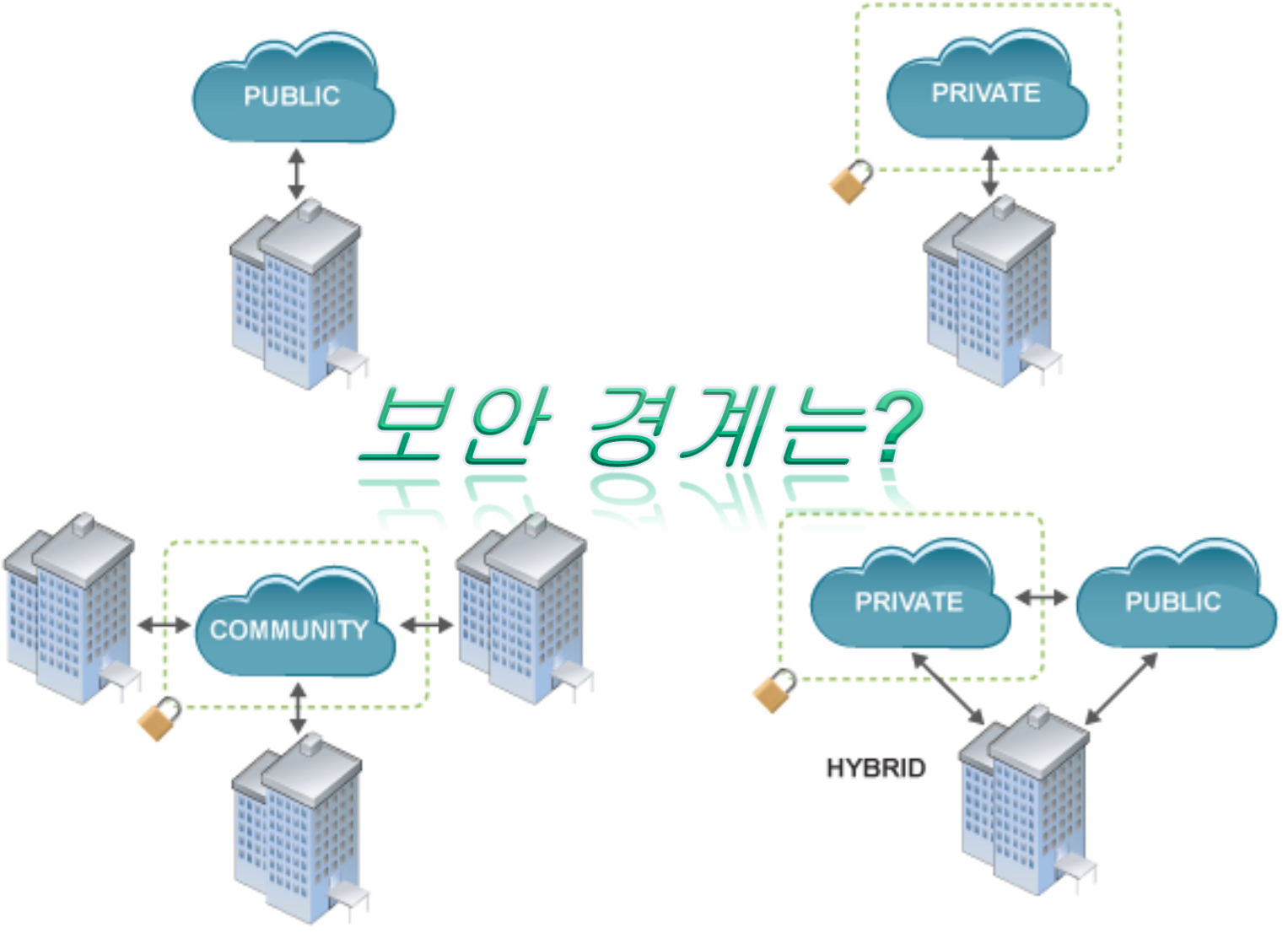
클라우드 서비스 모델



보안 책임은?



클라우드 배치 모델



클라우드 정보보호 관련 기사

SBS 뉴스

뉴스 프로그램 기자스페셜 이슈 + 취재파일 | SBS 8뉴스 | 생생영상

뉴스홈 속보 정치 경제 사회 글로벌 라이프 연예 스포츠

뉴스 > 정치

[단독] 90분이면 뚫리는 '클라우드'…사생활 유출 우려

김수형 기자

입력 : 2014.10.06 19:19 | 수정 : 2014.10.06 21:15

5,679 8

공유하기

[주간 클라우드 동향] "제2의 카톡 사태 발생하면?"… 클라우드 법 논란 핵심은

2014.12.08 10:17:15 / 백시넷 jyp@ddaily.co.kr

국내 클라우드 컴퓨팅 업계의 이슈는 여전히 '클라우드 발전법' 입니다. 지난주 국회에서 공청회가 개최됐지만, 법 통과 여부는 안갯속입니다.

공청회에서도 논란의 핵심은 역시 국정원이었습니다. 야당 의원들은 정부기관에 대한 신뢰도가 낮은 우리나라에서 제2의 카카오톡 감청 사태가 발생하지 않으리라는 법은 없다며 날을 세웠습니다. 클라우드 컴퓨팅처럼 여러 기관의 정보가 모

[AJU TV] 중국, '애플 아이클라우드' 해킹…중간자 공격?

중국 돋보기

이수연 기자 (ysy831210@ajunews.com) | 등록 : 2014-10-23 15:28 | 수정 : 2014-10-23 15:34

기 사 기자의 다른기사 + − 공유하기 Tweet 0

"클라우드 보안 취약점, 비즈니스 치명적 피해 입힌다"

파이오링크 "보안 취약한 웹, 클라우드 서비스로 제공되며 보안위협 높아"

관련기사

2014년 03월 06일 (목) 13:46:19 김선애 기자 iyamm@datanet.co.kr

클라우드 컴퓨팅의 확산 속도가 빨라지면서 중요한 서비스와 정보를 노리는 지능적인 공격이 심각한 위협으로 다가오고 있다. 클라우드 컴퓨팅은 웹을 기반으로 서비스되기 때문에 웹과 애플리케이션을 노리는 지능형 공격에 상시 노출돼 있다.

'제 13회 차세대 시큐리티 비전 2014'의 오후세션 A트랙의 문을 연 이장노 파이오링크 이사는 '클라우드 데이터센터 웹 보안 전략'이라는 주제로 클라우드 환경에서 급증하는 웹 보안 문제와 해결방법을 제시했다.

클라우드 서비스 보안 위험

위험영역	위험항목	출처		
		NIST	ENISA	CSA
거버넌스	거버넌스 손실	v	v	
	책임성 모호	v		v
	준거성 및 법적 위험	v	v	
	국경 문제	v	v	
접근통제	제공자 시스템에 대한 비인가 접근	v	v	v
	관리 인터페이스 취약성	v	v	v
	보호 메커니즘의 비일관성 및 상충			v
데이터 보안	개인정보 유출 및 손실	v	v	v
	불완전한 데이터 삭제	v	v	v
	격리(isolation)실패	v	v	v
운영관리	이전 및 통합 장애	v	v	v
	서비스 비가용성 및 중단	v	v	v
	보안사고 처리	v	v	v
	공급망 취약성		v	v

거버넌스(Governance) 관련 위험

- 통제권 상실
  - 클라우드 이용자(소비자 또는 고객)가 보안에 영향을 줄 수 있는 다양한 이슈의 통제권을 클라우드 제공자에게 위임
- 책임성 모호
  - 이용자와 제공자 간 보안 측면의 책임을 분명하게 할당하지 않아서 핵심적인 기능이 보호되지 않을 가능성
- 준거성 및 법적 위험
  - 서비스 제공자가 관련 요구사항에 대한 자신의 준거성을 입증하지 못하거나 이용자에 의한 보안 인증을 허용하지 않을 경우
- 국경 문제
  - 서비스와 관련 데이터 및 어플리케이션에 적용할 법규가 명확하지 않아서 국내 법령을 위반하는 경우가 발생

접근통제 관련 위험

- 제공자 내부자의 악의적 행동
  - 제공자 내부자에게 부여된 접근권한을 이용한 악의적인 활동
- 제공자 시스템에 대한 비인가 접근
  - 인가된 제공자 직원만 사용하도록 되어 있는 클라우드 시스템의 일부에 이용자의 의도하지 않은 접근을 제공할 위험
- 관리 인터페이스 취약성
  - 이용자 관리 인터페이스가 원격 접속 및 웹 브라우저 취약성과 결합할 경우 위험 증가
- 보호 메커니즘의 비일관성 및 상충
  - 분산된 보안 모듈 간에 보호 메커니즘의 일관성이 부족

데이터 보안 관련 위험

- 개인정보 유출 및 손실
  - 이용자가 제공자의 개인정보 처리 실무를 효과적으로 점검하지 못하여 개인정보를 적절하게 처리하고 있는지 확인하기 어려움
- 불완전한 데이터 삭제
  - 이용자가 클라우드 자원의 삭제를 요청하여도 제공자 시스템에서 이용자의 데이터를 완전하게 삭제하지 못하는 경우가 발생
- 격리(isolation) 실패
  - 이용자 간의 데이터와 어플리케이션을 분리하여 유지하도록 해주는 메커니즘이 실패할 가능성

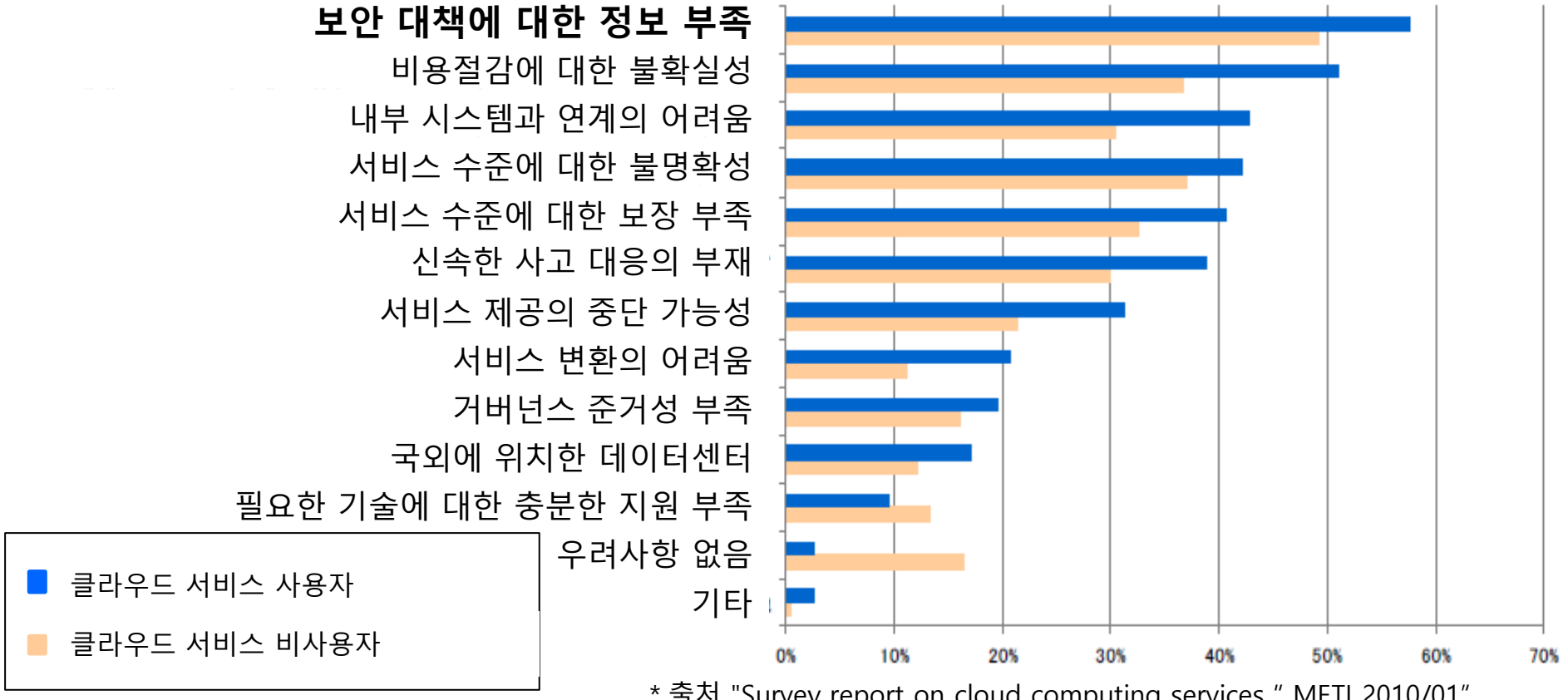
운영관리 관련 위험

- 이전 및 통합 장애
  - 이용자 환경에서 제공자 환경으로 데이터와 어플리케이션의 이동 및 연관된 설정 변경(예: 네트워크 주소)으로 인한 장애
- 서비스 비가용성 및 중단
  - 제공자 데이터 센터의 장비 또는 소프트웨어 장애
  - 이용자 시스템과 제공자 서비스 간의 통신 장애
- 보안 사고 처리
  - 제공자가 수행하는 처리에 의존할 수밖에 없는 보안 위반에 대한 검출, 보고 및 관리
- 공급망 취약점
  - 제공자가 사용자와 계약으로 명시한 보안 수준이 공급망을 따라 적정하게 유지하기 어려움

클라우드 서비스 보안 이슈 (1)

◻ 클라우드 서비스에 따른 보안 환경의 변화

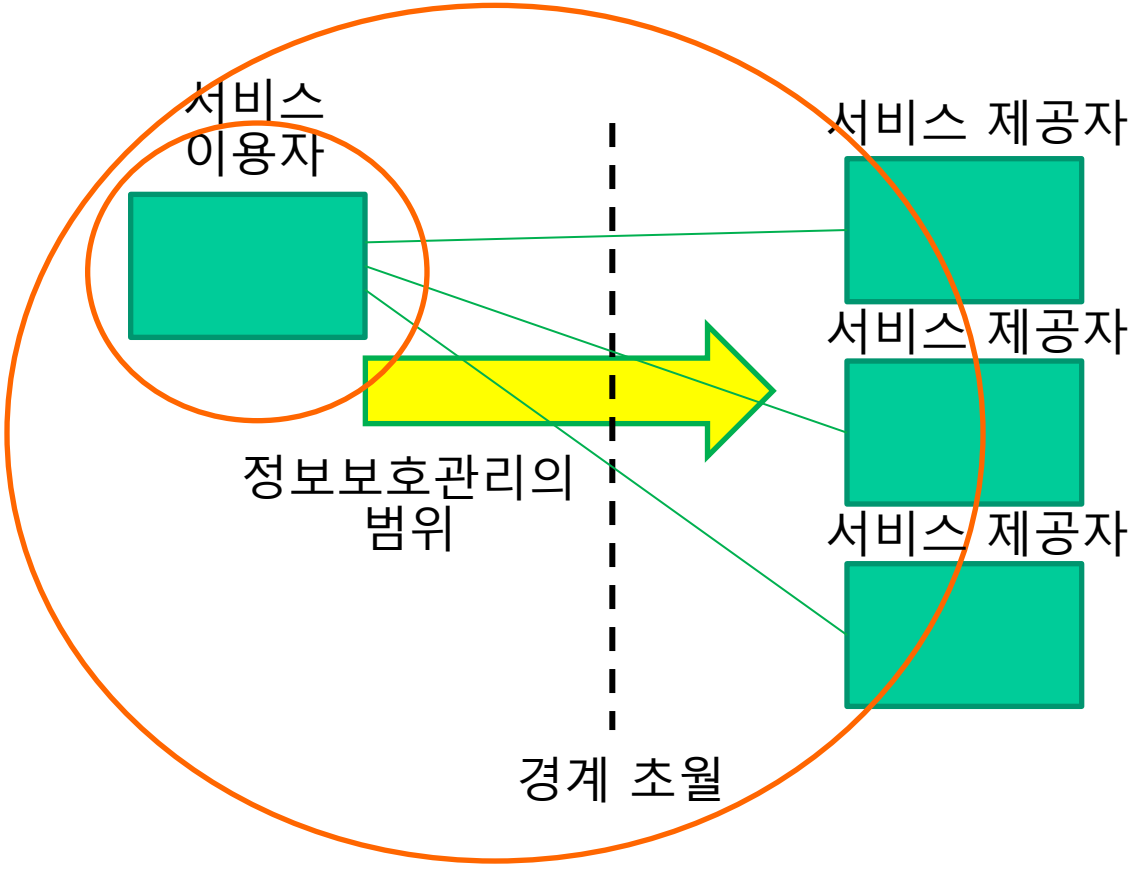
- ➢ 가장 큰 우려사항은 "서비스 제공자의 보안 대책에 대한 정보 부족"이라는 부분임



* 출처 "Survey report on cloud computing services " METI 2010/01"
응답자: 500명

클라우드 서비스 보안 이슈 (2)

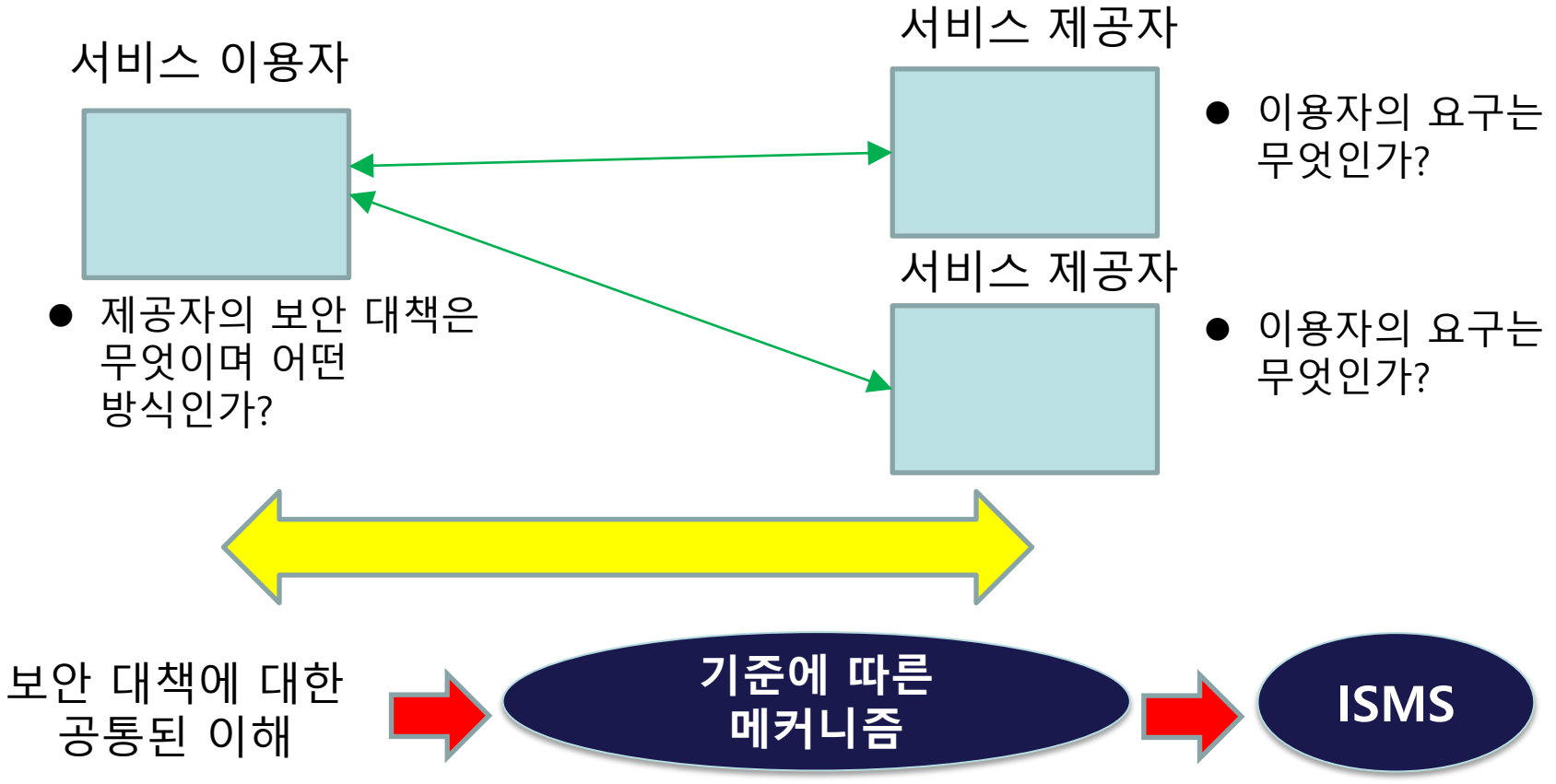
- 클라우드 서비스에 따른 보안 환경의 변화
  - 클라우드 서비스 이용자 조직의 경계를 넘어서 클라우드 서비스 제공자를 포함하는 방향으로 정보보호관리의 범위가 확장되고 있음



클라우드 서비스 보안 이슈 (3)

□ 공통된 이해의 필요성

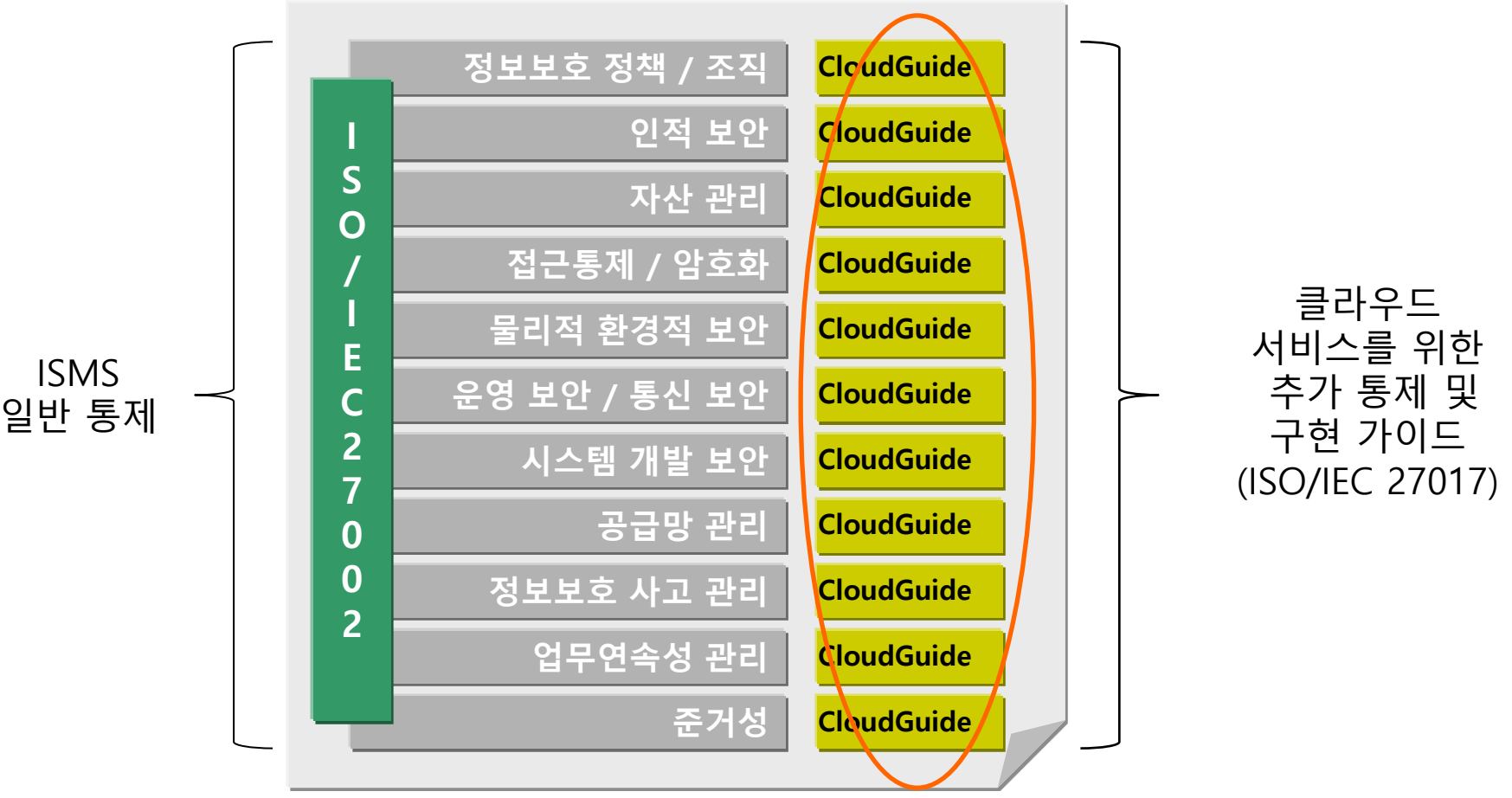
➢ 사용자 조직인 서비스 이용자와 서비스 제공자 간의 공통된 이해를 위하여 주어진 기준에 따른 메커니즘의 수립이 필요함



클라우드 서비스 보안 국제표준화 방향

◻ 클라우드 서비스를 위한 통제와 구현 가이드의 필요성

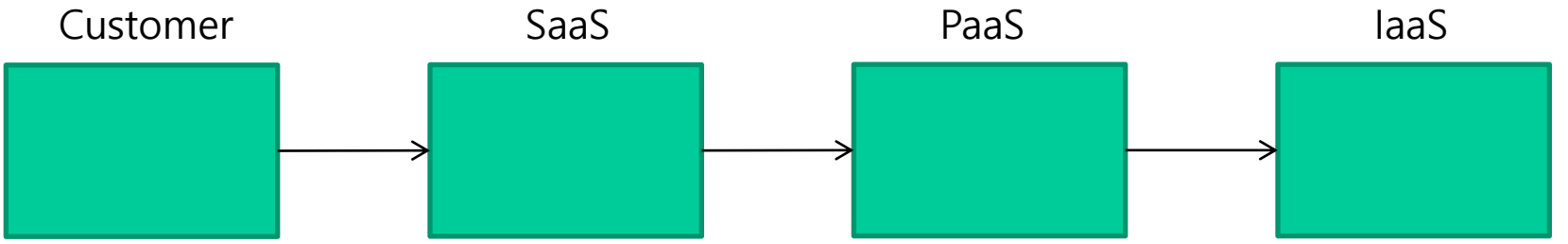
- ➢ 클라우드 서비스에 공통된 이해를 제공하는데 ISMS를 적용하기 위한 추가적인 통제와 구현 가이드가 필요함



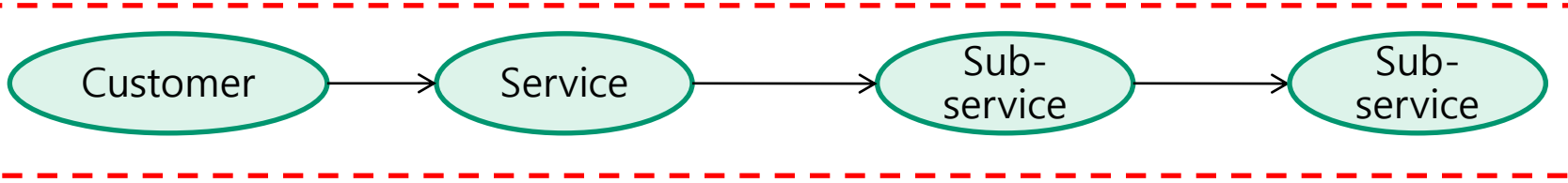
ISO/IEC 27017의 용도

- 클라우드 서비스 이용자
  - 클라우드 서비스의 사용을 위한 보안 지침 제공
- 클라우드 서비스 제공자
  - 클라우드 서비스 이용자가 클라우드 컴퓨팅 서비스 제공자에게 최소한의 요구사항으로 요청하는 통제 제공
- ISMS 인증
  - 클라우드 서비스를 사용 및 제공하는 조직에 대한 정보보호관리체계(ISMS) 인증 기준 제공

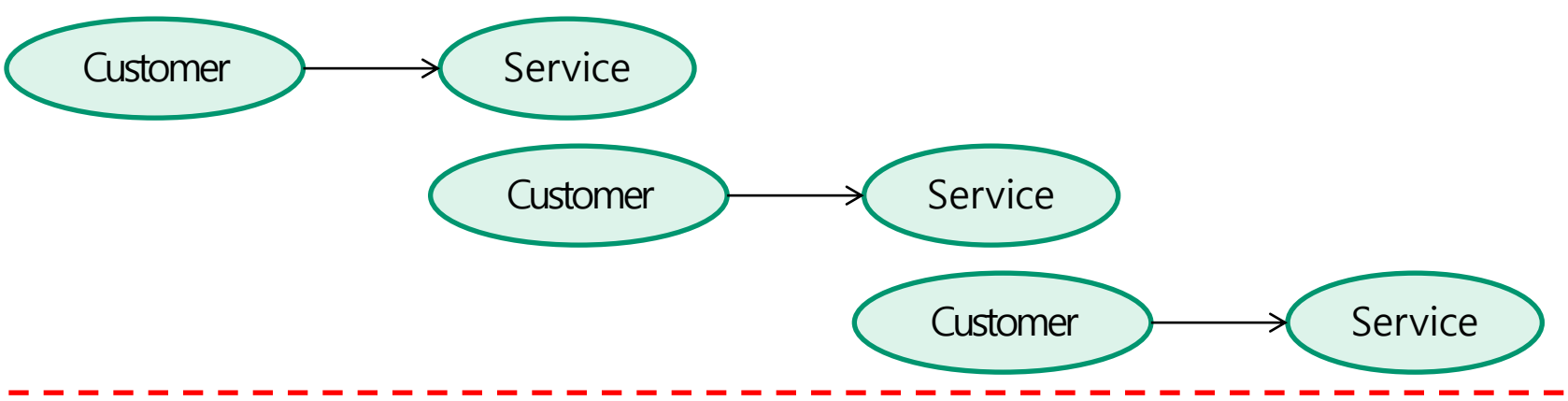
서비스 이용자와 제공자 간의 관계



- 이용자(customer)는 하위 서비스를 포함하는 감사 및 통제 대책을 고려해야 함



- 다양한 위치에서 사용자와 서비스 제공자 간의 관계를 고려해야 함



클라우드 보안 적합성 평가

- 클라우드 보안 적합성 평가의 필요성
  - 품질이 우수하고 안정성이 높은 클라우드 서비스에 대한 보증을 통해 사용자의 클라우드에 대한 막연한 불안감 해소와 서비스 제공자의 시장진출 지원
- 대표적인 국외 클라우드 보안 적합성 평가 제도
  - 미국 FedRAMP
  - 영국 G-Cloud Information Assurance
  - CSA OCF (Open Certification Framework)

미국 FedRAMP (1)

◻ FedRAMP 개요

- Federal Risk and Authorization Management Program
- 미 연방기관의 클라우드 서비스 또는 제품에 대한 보안성 평가 및 도입 승인과정을 통합하여 수행하는 정부기관 공통의 클라우드 보안 적합성 평가 제도

http://cloud.cio.gov/fedramp

미국 FedRAMP (2)

□ FedRAMP 주요 활동

보안성 평가
(Security Assessment)
- 중(M)/하(L) 영향 수준에 대한 NIST/FISMA 가이드라인 기반
- FedRAMP 기본 통제에 대한 서비스 제공자의 준거성 평가
- 예비 인가(Provisional Authorization) 부여

인가 서비스 도입
(Leverage Provisional Authorization)
- 공공기관(agency)은 보안 평가 패키지를 검토하여 FedRAMP 예비 인가된 서비스를 도입하거나 기관에 적절한 보안 요구사항을 추가

사후 관리
(Ongoing Assessment and Authorization – Continuous Monitoring)
- 클라우드 시스템에서 발생한 보안 사고와 이벤트를 대응하기 위하여 정부와 협력
- 자체 평가(입증)로 클라우드 시스템 준거성을 매년 검토

평가기관 인정
(3PAO Accreditation)
- 독립성/전문성을 갖춘 제3자 평가자 인정
- 클라우드 제공자가 선택할 수 있는 인정된 3PAO 리스트의 공지 및 유지

영국 G-Cloud Info Assurance (1)

◻ G-Cloud 개요

- 클라우드 기반의 IT 서비스를 공공기관이 쉽게 조달할 수 있도록 클라우드 제공자의 서비스가 업무영향수준(BIL)에 적합한지 평가하고 인가를 거쳐 **CloudStore**라는 온라인 스토어를 통해 등록하는 제도

https://www.gov.uk/how-to-use-cloudstore#overview

Contents

See more like this

Overview

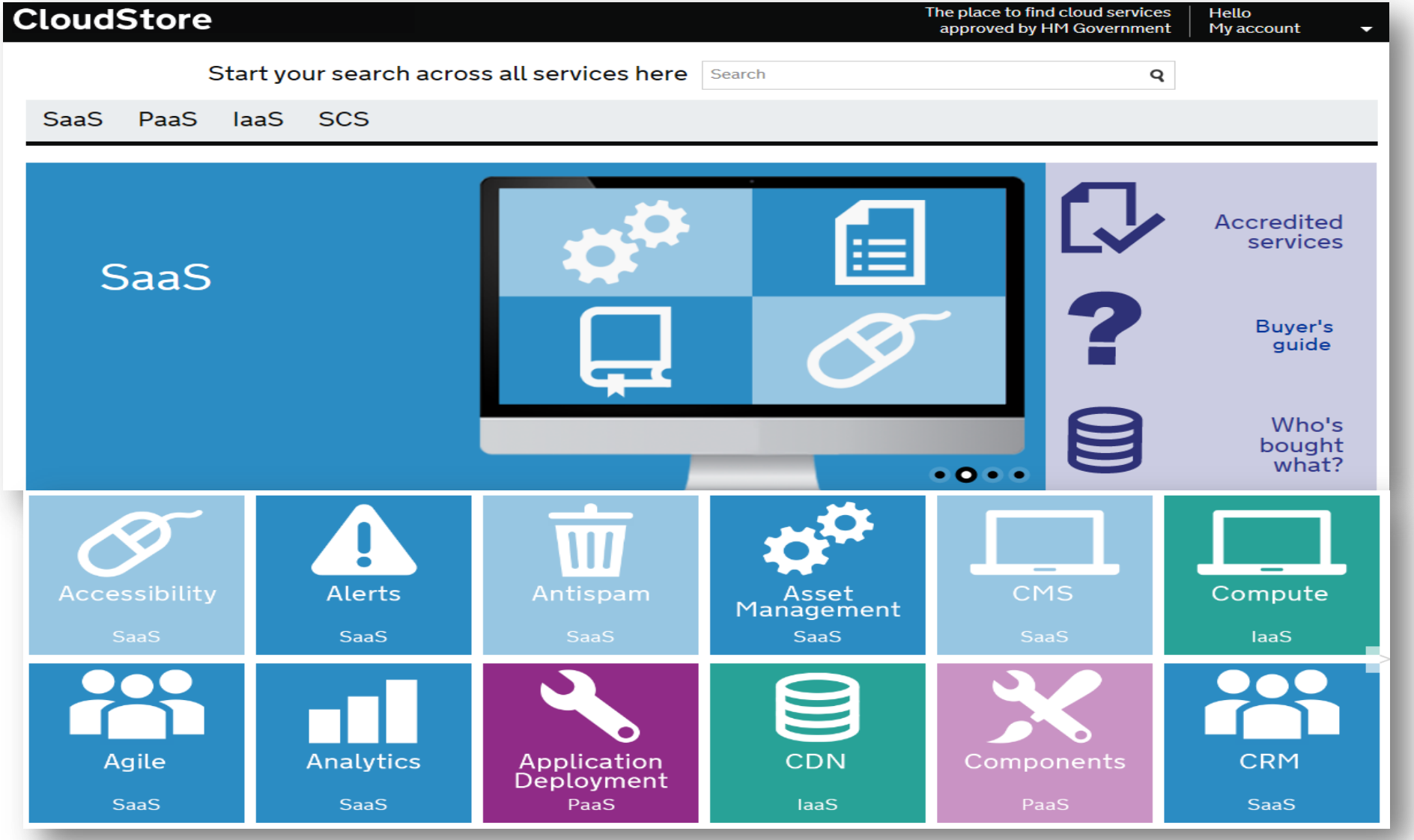
CloudStore is an online marketplace where suppliers offer their services to the public sector via the G-Cloud framework. Public sector bodies can review and buy these services on CloudStore.

Cloud computing lets you access internet-based computing, reducing the need to invest in your own hardware and software. Therefore, by using CloudStore you can:

- avoid long contracts
- buy the exact amount of computing resources you need
- save money on maintenance and physical storage
- avoid custom-built solutions which take a long time to create, are expensive and difficult to upgrade

G-Cloud framework

영국 G-Cloud Info Assurance (2)



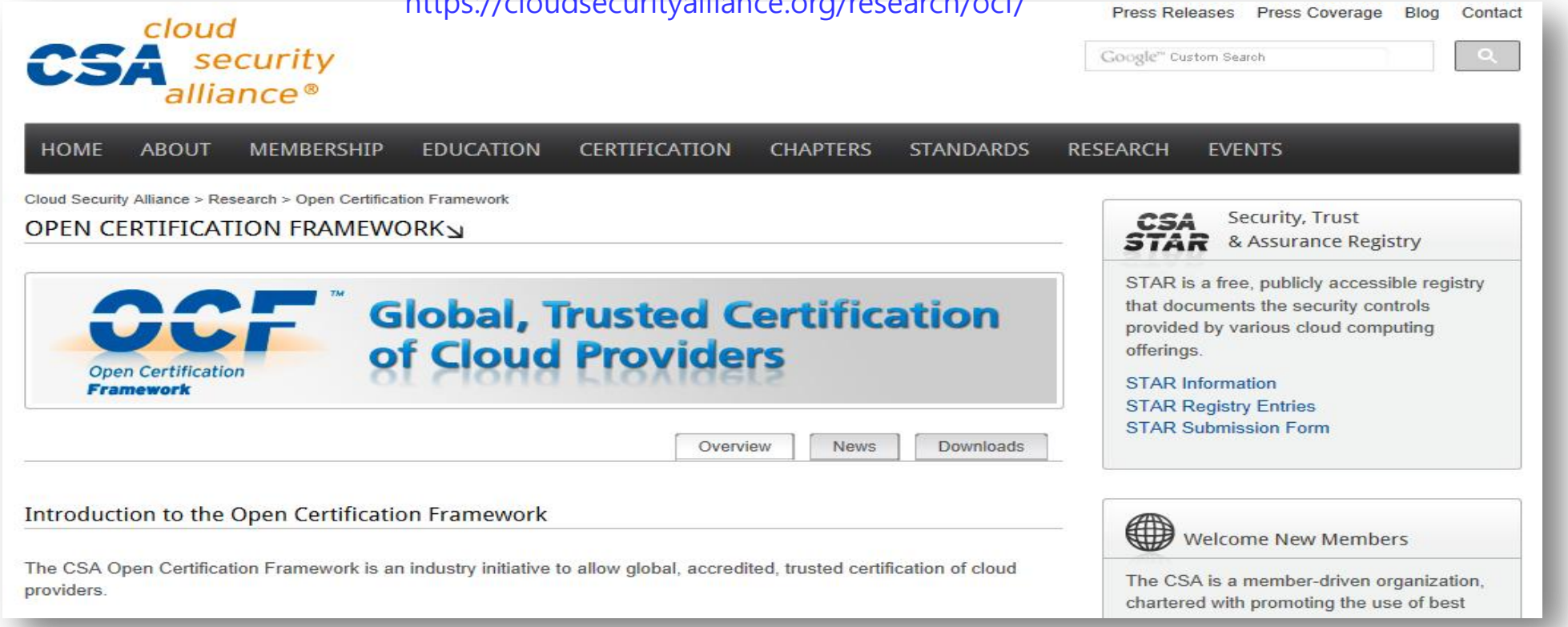
http://govstore.service.gov.uk/cloudstore/

CSA OCF (1)

☐ CSA OCF(Open Certification Framework) 개요

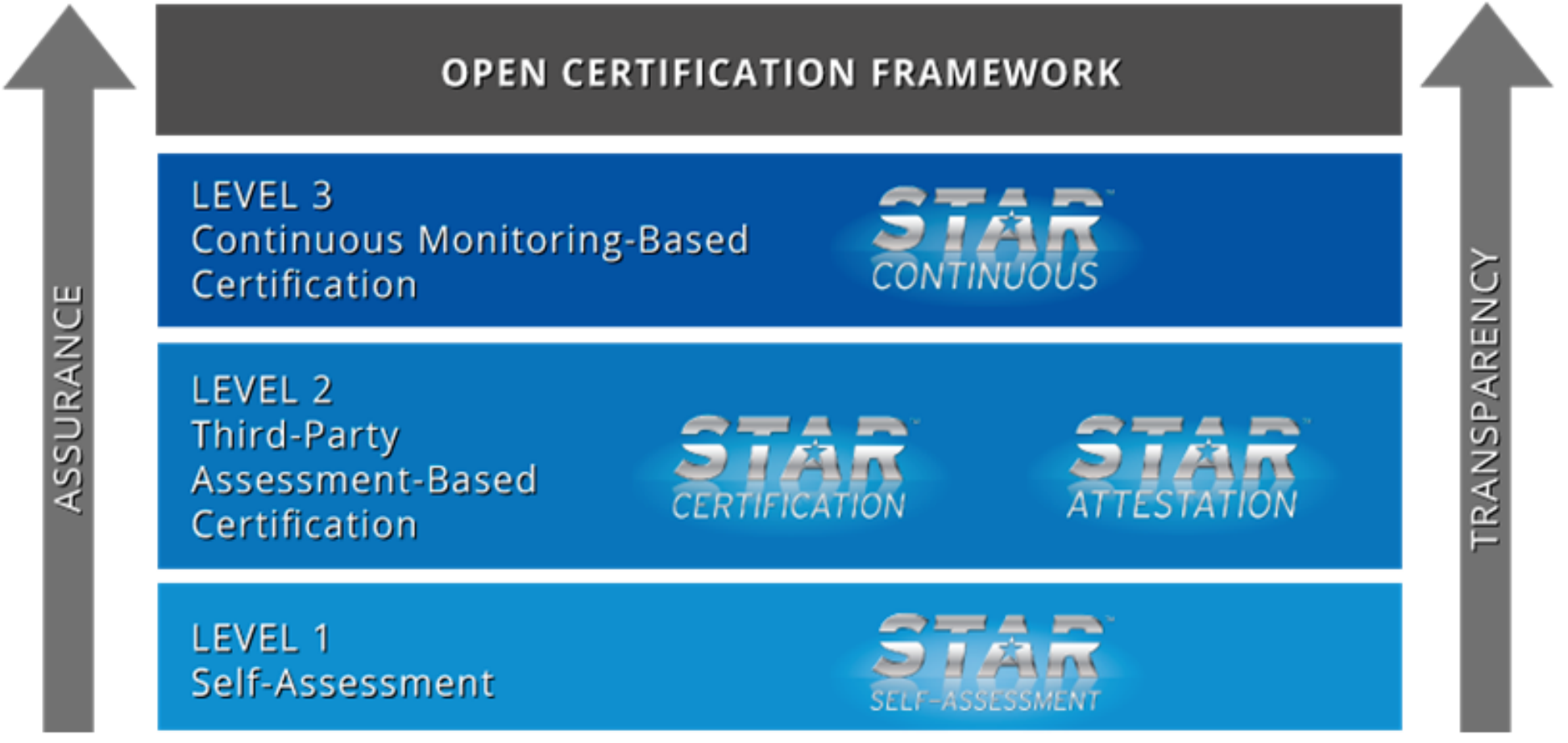
- ➢ 클라우드 제공자가 글로벌하게 신뢰할 수 있는 인증을 취득할 수 있도록 업계 주도 보안그룹인 CSA(Cloud Security Alliance)의 보안 지침과 통제 (CCM)에 따라 3 단계 수준의 클라우드 제공자 인증을 위한 프로그램을 제공

https://cloudsecurityalliance.org/research/ocf/



CSA OCF (2)

- OCF 3단계 수준 인증



클라우드, 과연 보안에 취약한가?

새로운 환경은 새로운 위험(위협과 취약점)을 가져온다.

클라우드 서비스 환경도 새로운 보안 위험을 수반하고 있다.

대부분 보안 위험은 기존의 대책으로 처리가 가능하지만 일부는 새로운 대책이 요구된다.

클라우드 서비스 이용자는 클라우드 서비스 제공자의 보안 대책에 대한 신뢰할 수 있는 정보를 원한다.

Q & A