클라우드 환경에서의 IBM 스마트 클라우드 전략

2011/05/18

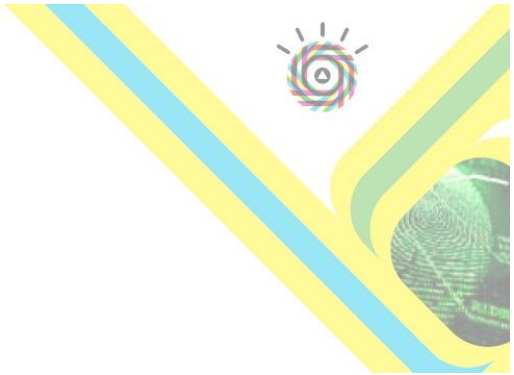
김용덕, GTS

IBM Security Summit

IBM Security Solutions. Secure By Design.

Agenda

- 1. 클라우드 컴퓨팅 소개
- 2. IBM 클라우드 보안 전략
- 3. IBM 클라우드 보안 컨설팅/구축 서비스



1. 클라우드 컴퓨팅 소개

IT Demands

Business Challenges

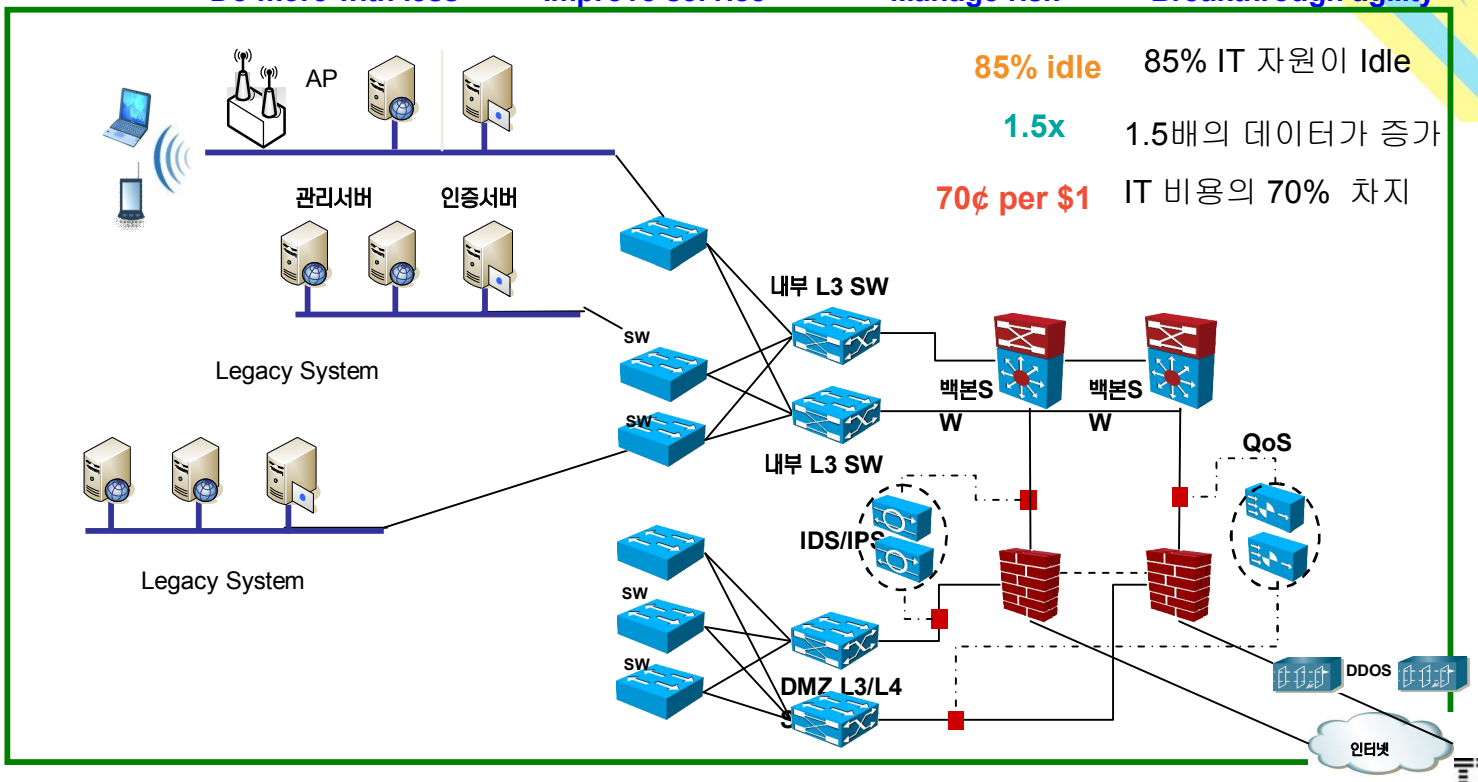
Operations, competition

Data, information

D.C costs

Customer expectations

Do more with less | **Improve service** | **Manage risk** | **Breakthrough agility**

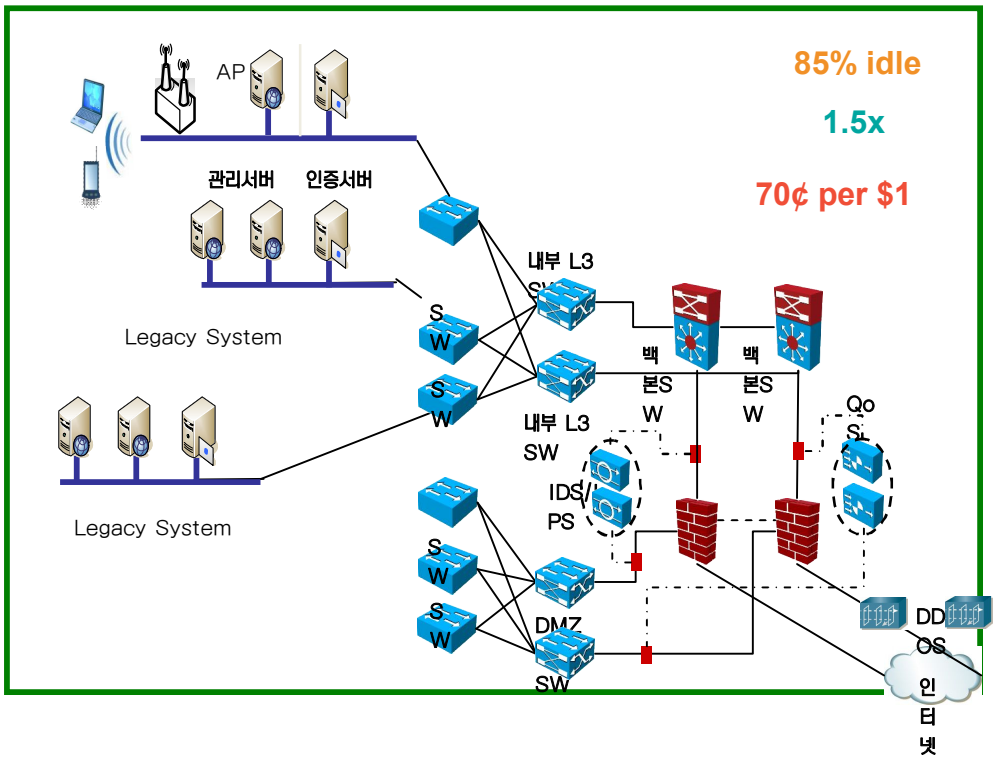


85% idle 85% IT 자원이 Idle

1.5x 1.5배의 데이터가 증가

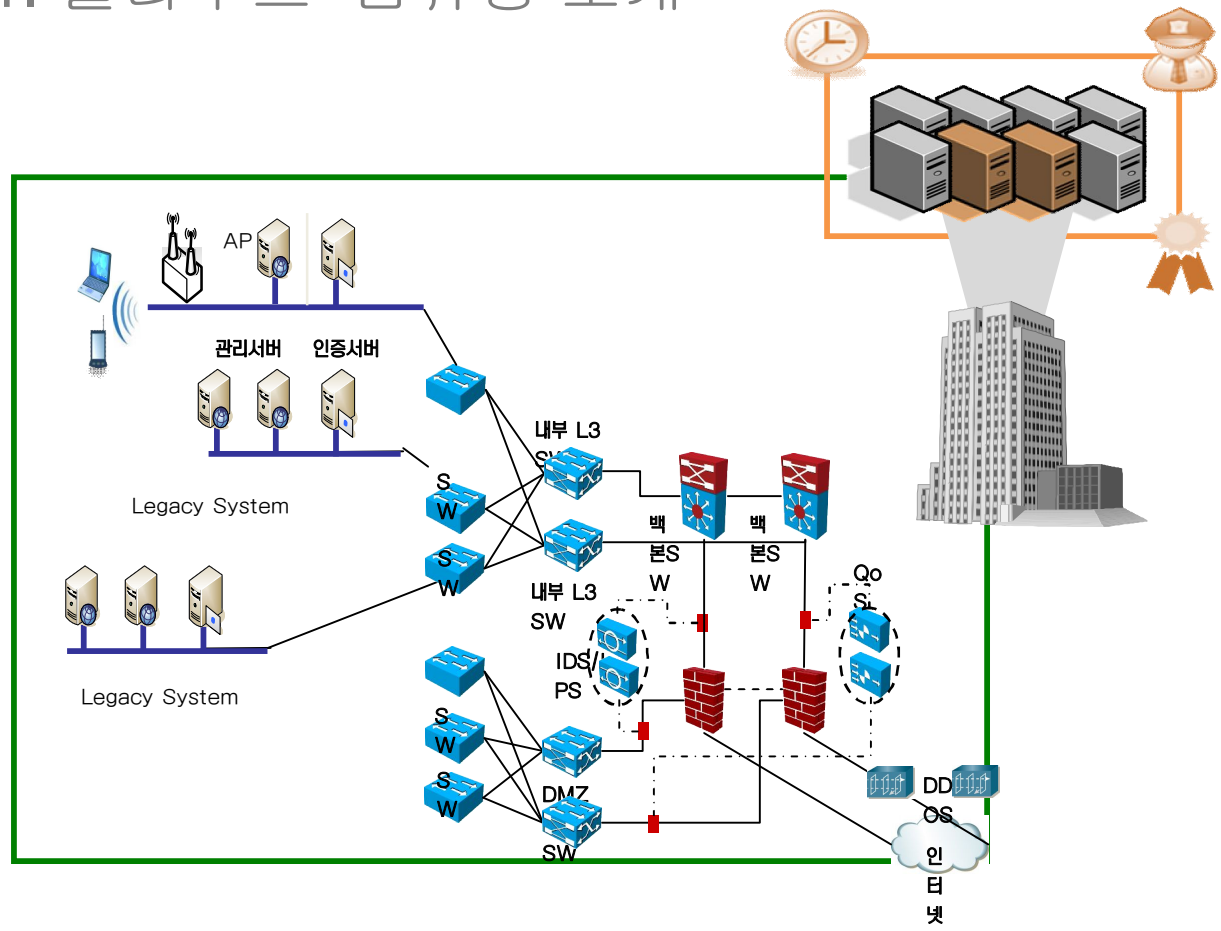
70¢ per $1 IT 비용의 70% 차지

1. 클라우드 컴퓨팅 소개



- 고정 비용을 개선할 수 있는 방법은?
  - **On Demand/ 과금 서비스**
- **IT** 자원은 할당된 만큼만 사용하도록 되어 있는데, 이를 개선할 수 있는가?
  - **Elastic Scaling**
- **IT** 자원은 서비스 부서 담당자 만 요청하고 자원을 제공할때 까지 기다려야 한다. 개선방법은?
  - **셀프 서비스**
- 다른 영역에 시스템의 가용해도 쓸수 없다. 공유할 수 있는 방법이 있는가?
  - **가상화**

1. 클라우드 컴퓨팅 소개



기존 IT 인프라의 통제방법

해당 시스템의 물리적 위치

시스템의 데이터가 저장되는 위치

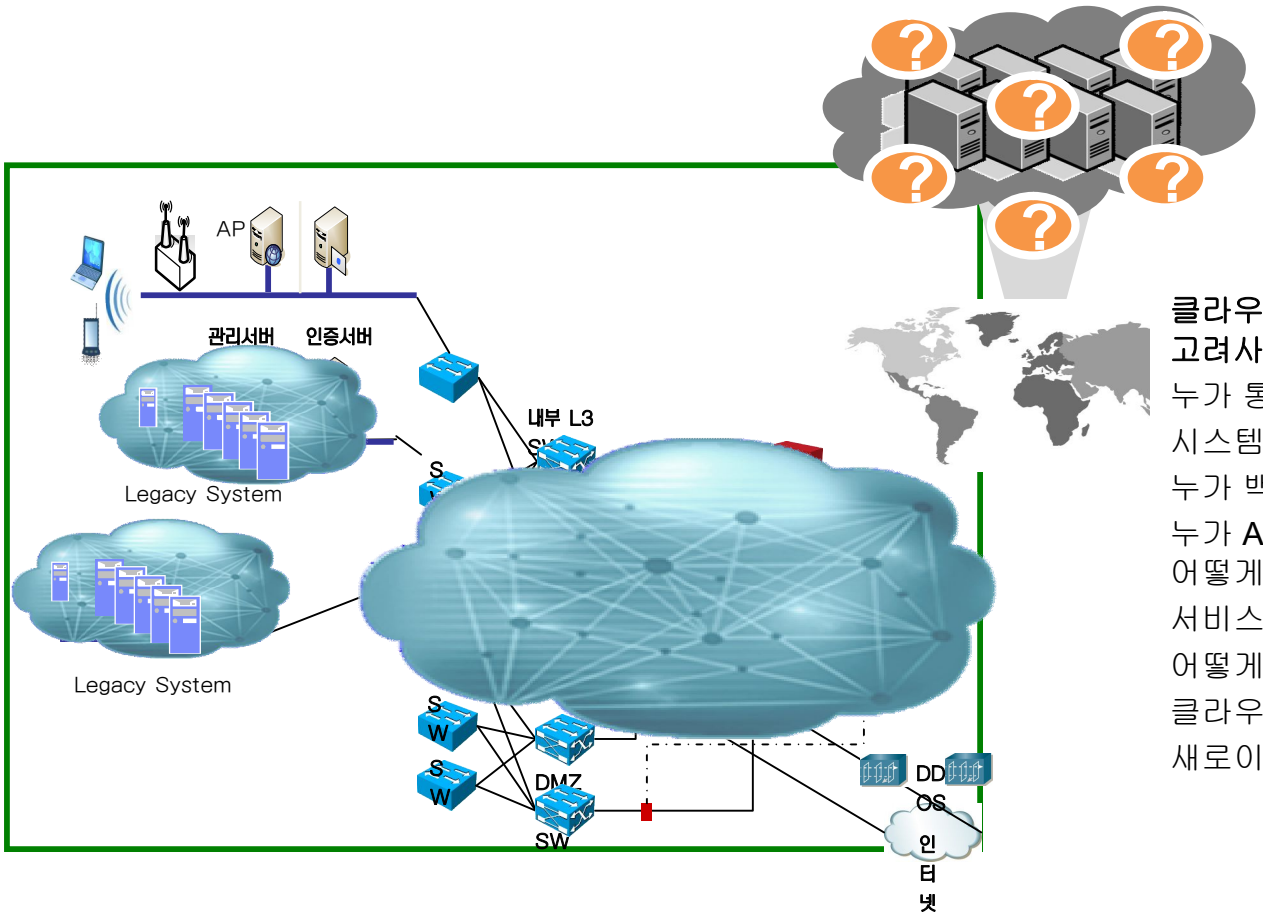
접근 제어 방법 구성

감사및 관리 방법의 체계화

- Auditor 와 IT 서비스,거버넌스

보안팀의 역할과 정책,지침,절차 규정

1. 클라우드 컴퓨팅 소개



클라우드 환경에서의 통제를 위한 고려사항

누가 통제하는가?

시스템이 어디에 위치하는가?

누가 백업을 하는가?

누가 Access 권한을 갖고, 접근기록은 어떻게 되는가?

서비스 영속성 보장을 어떻게 하는가?

어떻게 Auditor가 감사하는가?

클라우드에서 보안팀은 무얼하는가?

새로이 고민해야 할 영역이 있는가?

1. 클라우드 컴퓨팅 소개 – 보안 기술동향

Gartner: Top Risks (2008)
- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability [Heiser 09]

CSA: Top Threats (2010)
- Abuse and nefarious use of cloud
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

ENISA: Top Security Risks (2009)
- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider [ENISA 09/a]

Top Threats and Risks in Cloud Computing, IBM
- Process/VM Isolation, data segregation, multi-tenancy
- Malicious insiders (co-tenants, cloud provider)
- Management (incl. self-service) interface compromise
- Insecure interfaces and APIs
- Uncertainty over data location
- Data protection and security
- Data recovery, resiliency
- Insecure or incomplete data deletion
- Account or service hijacking
- Abuse of cloud services (extrusion)
- Compliance risks

클라우드 환경에서 보안 위협/위험
- **Data 분리 및 Privacy**
- 악의적 내부 사용자에 의한 특권 남용
- 클라우드 관리 시스템 공격에 의한 피해 확산
- 인터페이스, **API**의 보안성 부족
- 데이터 저장 위치에 대한 불확실성
- 데이터 보호 및 보안
- 데이터 복구 및 **resiliency**
- 데이터 삭제의 불완정성
- 계정 혹은 서비스 **Hijacking**
- 가상화 인프라의 보안 취약점
- 클라우드 서비스의 남용
- 준거성 **(Compliance)** 부재
- 거버넌스 부재

1. 클라우드 컴퓨팅 소개 – 보안 위험의 분류(1/3)

통제

많은 기업과 공공 기관들은 그들의 정보를 통제하지 않는 시스템 상에

서비스 제공자는 반드시 고객들이 신뢰할 수 있도록 높은 수준의 보안 투명성을 제시해야만 합니다.

데이터

공유된 네트워크와 컴퓨팅 인프라에서 워크로드를 이전하는 것은 권한없는 이용자들에게 정보가 노출될 수 있는 가능성을 증가시킨다.

인증과 접근 제어 기술의 중요성이 증가됩니다.

의존성

높은 의존성은 중요한 이슈가 될 것입니다. IT 부서들은 서비스의 손실이 비즈니스의 단절로 이어질 것을

가용성에 대한 강력한 보증없이 미션 크리티컬한 어플리케이션을 클라우드 환경 내에서 운영하지 않는다.

컴플라이언스

국내외 법과 규제에 대한 적용과 일부 데이터에 대해서는 클라우드 서비스의 사용이

이해할 수 있는 감사 능력이 필수적입니다.

보안 관리

간단한 작업도 누군가에 의해 수행되거나, 추상화된 계층 뒤에 존재하게 될 것이다.

서비스 제공자는 어플리케이션과 런타임 환경을 위한 보안 구성을 관리할 수 있는 쉬운 통제를 제공해야만 한다.

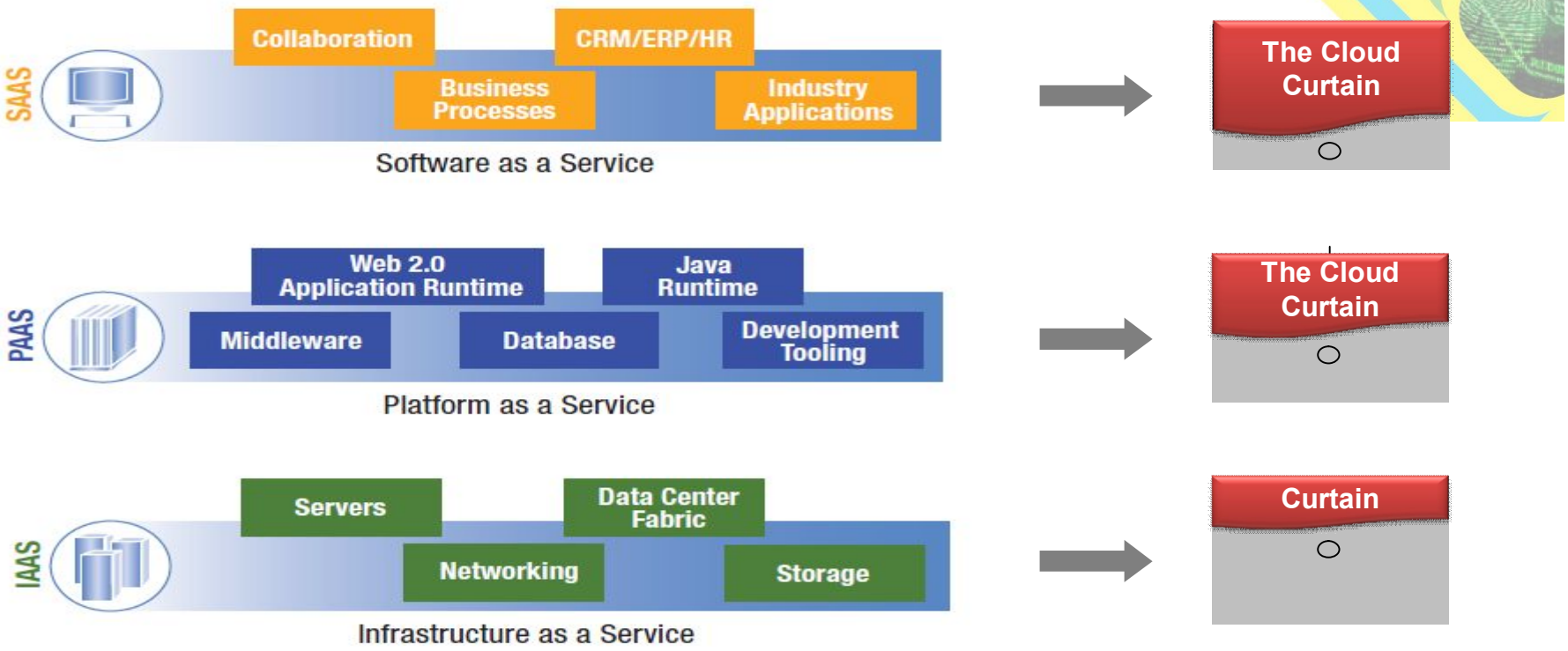
1. 클라우드 컴퓨팅 소개 – 보안 위험의 분류(2/3)

유형	요약	사례
통제	통제가 필요할 때, 통제할 수 없는 위험	- 악의적인 사용자의 이용: 경쟁사, 해커, 악성코드 Hosting, 봇넷과 DDoS 인프라 구축 등 - 서비스 품질과 SLA 계약과 보증. 계약의 수정이 용이하지 않음.
보안 관리	보안 관리 활동이 필요할 때, 할 수 없는 위험	- 공유 인프라에 대한 취약점과 보안 - 가상머신과 하이퍼바이저의 패치 - 안전하지 못한 클라우드 인프라 및 서비스의 취약점 - 계정, 서비스 및 트래픽 하이재킹
데이터	데이터 및 정보의 손실과 유출 위험	- 가상머신의 동적 재배치로 데이터의 위치를 보증하지 않으며, 불안정한 미디어로 인한 데이터 손실 - 다중역할의 특성으로 인한 인프라/서비스 공유로 데이터 유출
의존성	서비스 가용성을 침해 받을 위험	- 공격 목표 선정되기 쉬우며, 동적 서비스 및 인프라 운영으로 서비스 가용성 침해 가능성 존재.
컴플라이언스	법규 및 규제 적용의 어려움	- 위치에 따른 법규 및 규제 적용 논란의 여지 높음. - 수색 영장 등 해당 국가의 수사력에 따른 정보 유출 우려

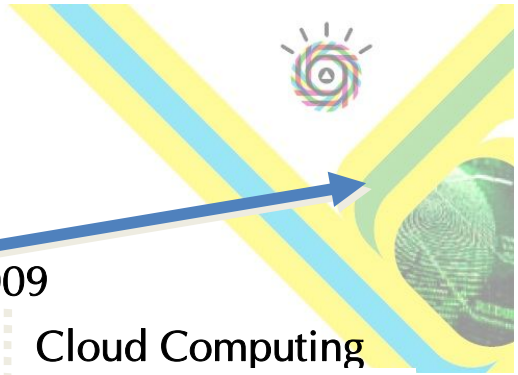
1. 클라우드 컴퓨팅 소개 – 보안 위험의 분류(3/3)

서비스 모델	클라우드 서비스 공급자 측면	클라우드 서비스 이용자 측면
SaaS	- 서비스 모델 중 공급자의 보안 책임이 가장 큼. - SaaS 형태로 제공하는 소프트웨어의 안전하지 않은 개발로 인한 보안 결함. - (가상화된 혹은 공급 받은) 미들웨어, 네트워크, 운영 체제 상의 보안 취약점과 패치 적용이 용이하지 않고, 접근 통제가 실패할 수 있음. - 네트워크 간 암호화되지 않은 중요 정보 전달 등.	- 이용자가 필요한 보안 통제 및 관리 적용 어려움. - 내부 어플리케이션 연계를 위한SaaS 상의 소프트웨어와의 인터페이스를 통한 악의적인 공격 - 중요 데이터와 개인정보에 대한 실제 암호화 및 접근 통제 여부에 대한 확인 어려우며, 기업 및 이용자 표준 암호화 알고리즘 적용 및 변경 어려움. - 감사 및 모니터링 등 보증 활동을 위한 데이터를 제공받기 어려움. - 가용성 확보가 용이하지 않은 높은 서비스 의존성
PaaS	- (가상화된 혹은 공급 받은) 미들웨어, 네트워크, 운영 체제 상의 보안 취약점과 접근 통제가 실패할 수 있음. - 네트워크 간 암호화되지 않은 중요 정보 전달 등.	- PaaS 상에서 개발하는 소프트웨어와 인터페이스의 안전하지 않은 개발로 인한 보안 결함 - 개발 소스에 대한 보호가 용이하지 않거나, 원하는 보안 기능 구현이 어려울 수 있음. - 개발 플랫폼과 서비스 플랫폼 사이의 차이로 인한 보안 결함
IaaS	- (가상화된) 네트워크 및 운영 체제 상의 보안 취약점 - (가상화된) 네트워크 간 암호화되지 않은 중요 정보 전달 등.	- 서비스 모델 중 이용자의 보안 책임이 가장 큼. - 이용자의 활용 방식에 따라 다양한 보안 취약점 존재

1. 클라우드 컴퓨팅 소개 – 서비스 별 보안



1. 클라우드 컴퓨팅 소개 -



1980

Grid Computing

- 대용량의 컴퓨팅 리소스를 필요로 하는 서비스를 위해 지원
- 인터넷 상의 모든 PC형 컴퓨팅 리소스 사용

1990

Utility Computing

- 과금 형태의 서비스로 컴퓨팅 리소스를 제공(as a metered service)
- 전기나 수도 같이 필요할 때마다 연결하여 사용하고 과금

2000

Software as a Service

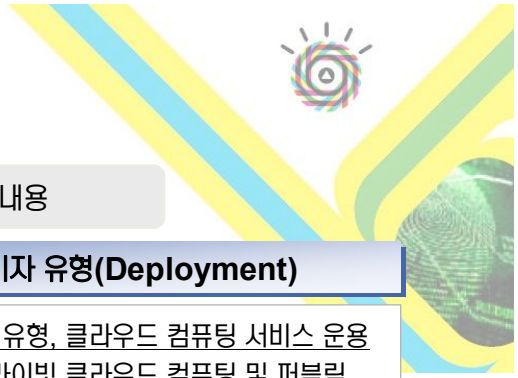
- 서비스 제공자의 서버에 저장된 Software를 인터넷을 통해 서비스 형태로 제공
- 웹 표준 개발을 통해 다양한 브라우저에서도 동일한 서비스 제공

2009

Cloud Computing

- 언제 어디서나, IT자원을 서비스 형태로 제공
- SW뿐만 아니라, 모든 IT자원을 서비스 형태로 제공
- 기술적으로는 띤 클라이언트를 이용한 분산 컴퓨팅을, 과금 형태로는 유틸리티 컴퓨팅을 채택

1. 클라우드 컴퓨팅 소개 – 구성요소



클라우드 컴퓨팅 구성요소

1	프라이빗 클라우드 컴퓨팅 (Private Cloud Computing)	퍼블릭 클라우드 컴퓨팅 (Public Cloud Computing)
2	Software as a Service (SaaS)	
	Platform as a Service (PaaS)	
	Infrastructure as a Service (IaaS)	
3	클라우드 컴퓨팅 플랫폼 아키텍쳐	

클라우드 컴퓨팅 주요내용

1 클라우드 컴퓨팅 소비자 유형(Deployment)

- 클라우드 컴퓨팅 서비스 이용자 유형, 클라우드 컴퓨팅 서비스 운용 및 사용 조직 확장성에 따라 프라이빗 클라우드 컴퓨팅 및 퍼블릭 클라우드 컴퓨팅으로 구분

2 클라우드 서비스 유형

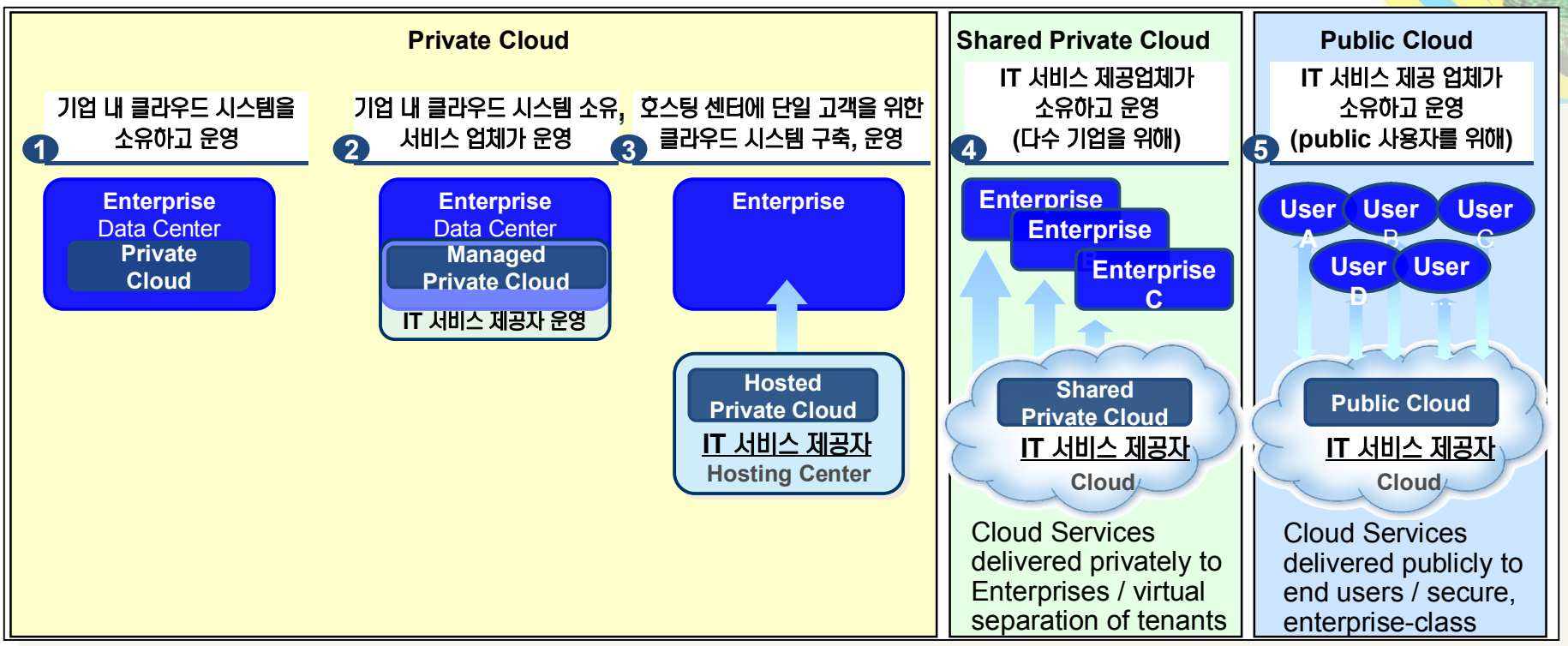
- 클라우드 서비스는 일반 소비자 및 기업고객을 대상으로 인터넷을 통해 실시간으로 제공되고 소비되는 제품 및 서비스와 솔루션
- IT 인프라 서비스 (IaaS), 신규 어플리케이션 개발을 위한 플랫폼 서비스 (PaaS), 어플리케이션 모듈을 제공하는 소프트웨어 서비스(SaaS)의 3가지 서비스 Layer로 구성

3 클라우드 컴퓨팅 구현을 위한 기반인프라

- 클라우드 컴퓨팅 구현을 위해 가상화 기술을 통한 개방형 아키텍처 기반의 효율적인 자원 가상풀 구현 및 클라우드 컴퓨팅 운영을 위한 사용량 기반의 과금 및 Metering 체계 구현 필요

주) 클라우드 컴퓨팅 정의는 Gartner 'Cloud Computing – Defining and Describing an Emerging Phenomenon'(2008.06) 참조

1. 클라우드 컴퓨팅 소개 – 배치 모델(Deployment Model) (1/2)



2. IBM 보안 전략 > IBM Information Security Framework

성공적 보안성확보를 위해서는 **Framework**를 통한 **Assecess,** 해결방안 제시할 수 있는 역량이 필요하며, 해결방안에 필요한 솔루션을 잘 구성하는 것 또한 중요합니다.

GRC 거버넌스, 위험 관리와 컴플라이언스

사람과 아이덴터티

데이터와 정보

어플리케이션과 프로세스

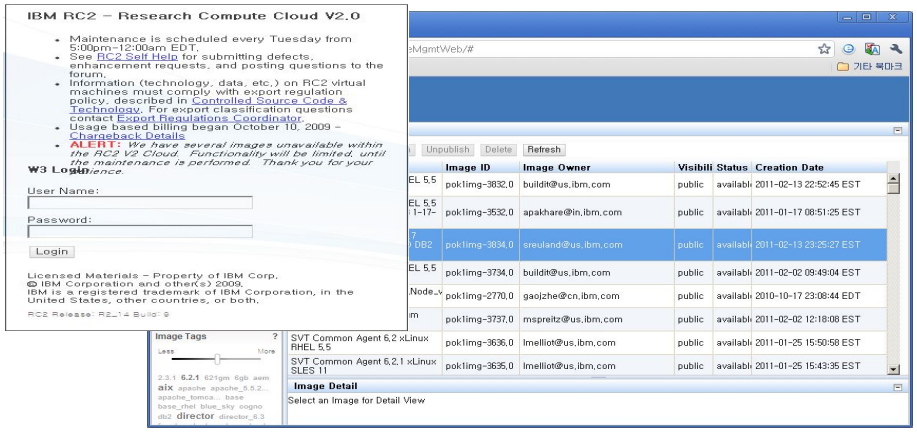
네트워크, 서버와 단말 등 IT 인프라

물리적 인프라

2. IBM 보안 전략 >IBM 클라우드 보안 사례 – IaaS/PaaS

RC2는 IaaS/PaaS환경을 제공하는 컴퓨팅 클라우드 서비스입니다. IBM의 데이터센터 보안지침인 ITCS104의 준수, Trusted Virtual Domain 구현 등의 보안 특징을 가지고 있습니다.

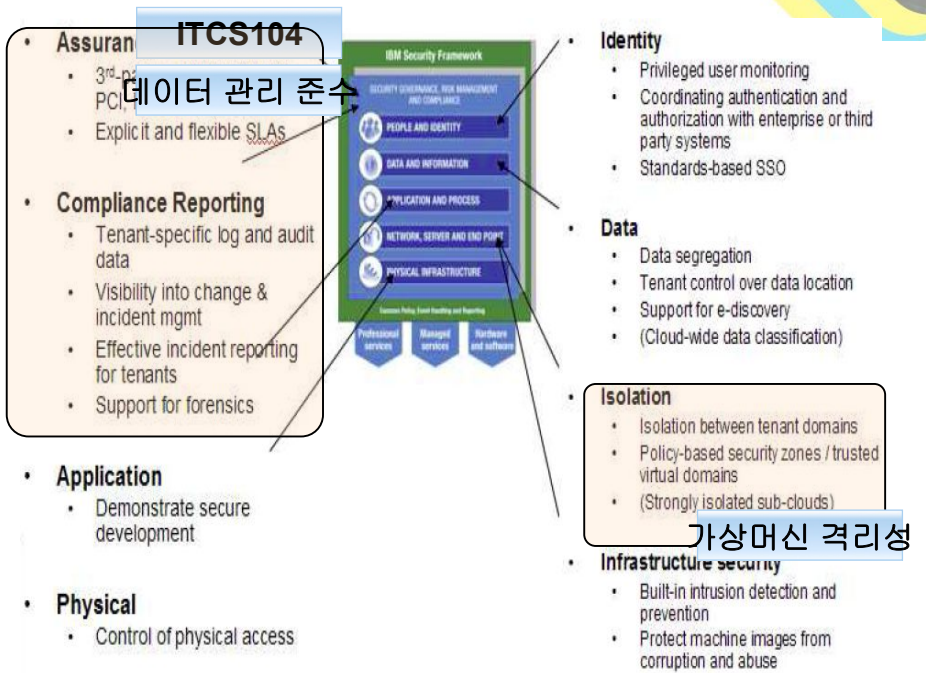
RC2 서비스 - https://rcc.cloud9.ibm.com/ImageMgmtWeb/login.jsp



주요 보안 특징

- **ITCS104 준수**
- **데이터 관리 준수**
- **가상머신 격리성 향상(KVM, Xen)**

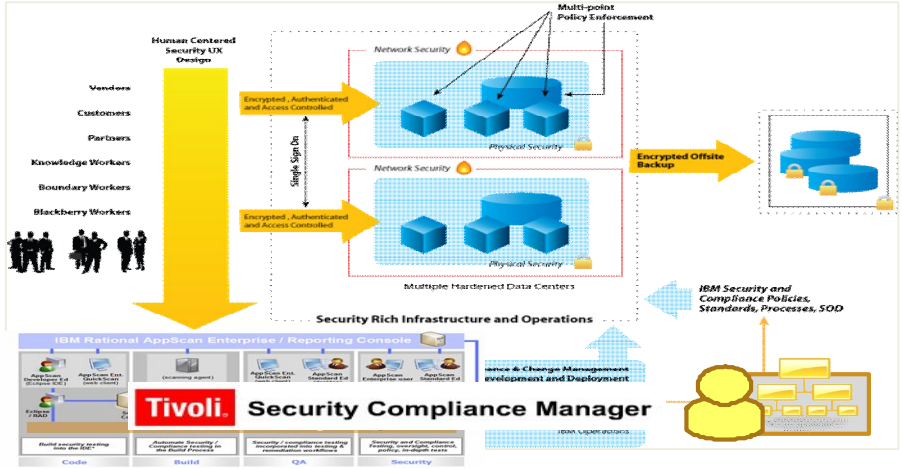
주요 보안 영역



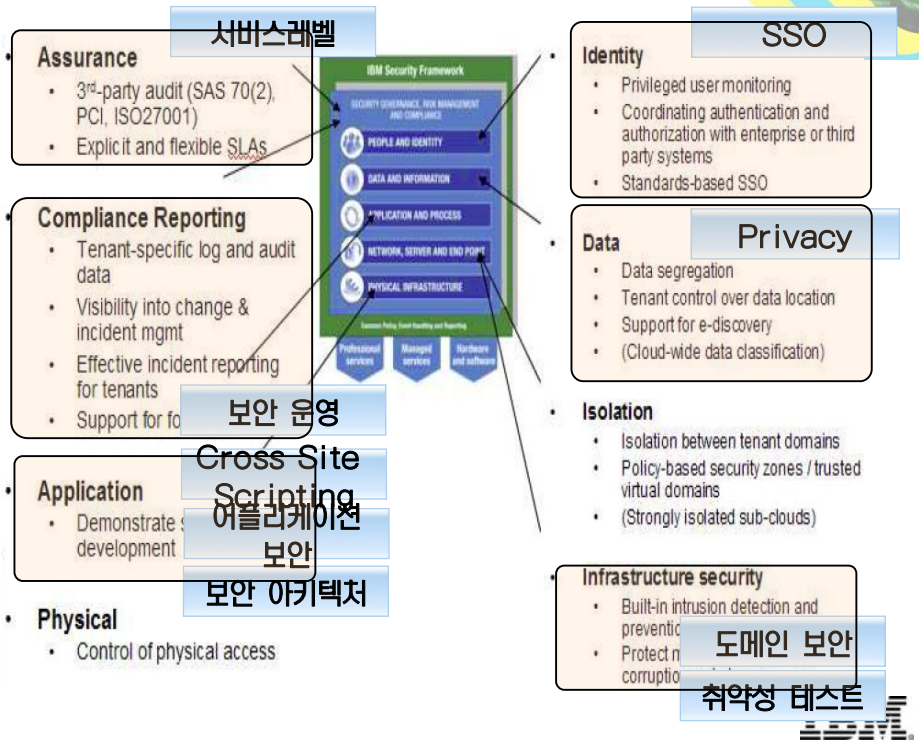
2. IBM 보안 전략 >IBM 클라우드 보안 사례 - SaaS

LotusLive 는 **IBM**이 제공하는 **SaaS** 클라우드 서비스로서 종합적인 보안 모델과 보안 컴포넌트를 구현하여 운영하고 있습니다.

LotusLive 서비스
http://www.lotuslive.com



주요 보안 영역

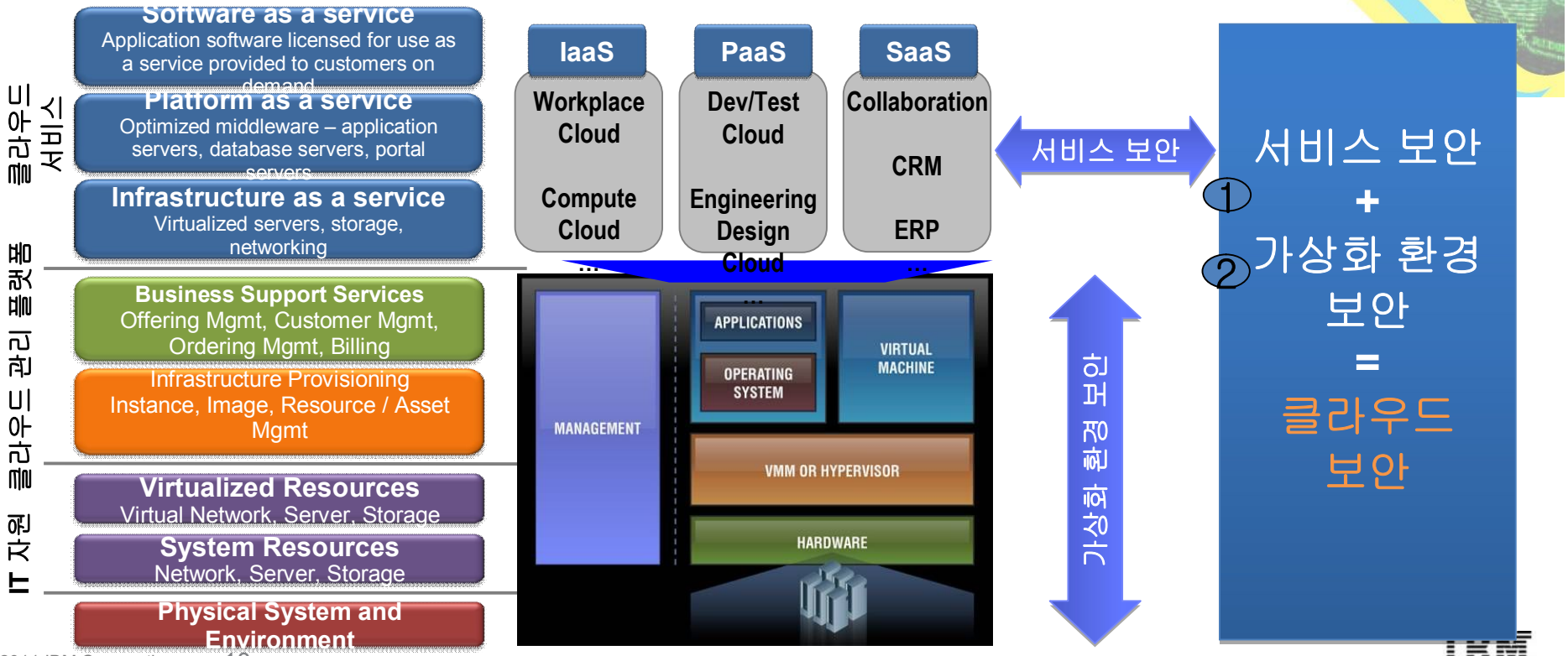


주요 보안 특징

- 보안기능이 풍부한 인프라 구조(데이터센터, IT, 프로세스...)
- 보안정책 적용이 가능한 어플리케이션 보안
  - 사용자중심의 보안 : 최종사용자의 자원 사용 및 협업이 원활하게 이루어 질 수 있도록 고려한 보안 설계

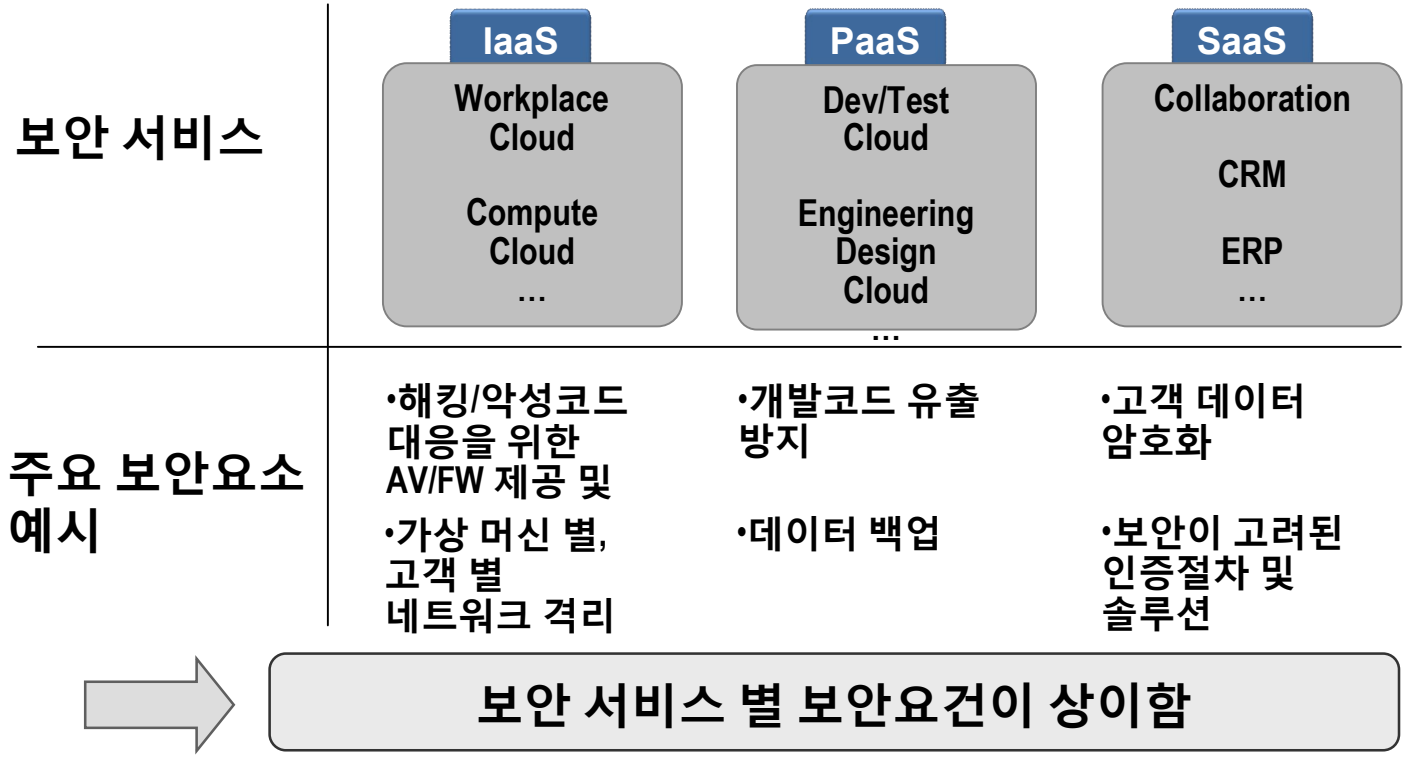
2. IBM 보안 전략 >클라우드 보안은?

클라우드 컴퓨팅은 **IT** 자원의 가상화, 클라우드 플랫폼, 클라우드 서비스의 계층으로 구분될 수 있으며, 보안 요소는 계층에 따라 클라우드 서비스 보안과 가상화 환경 보안으로 나누어 집니다.



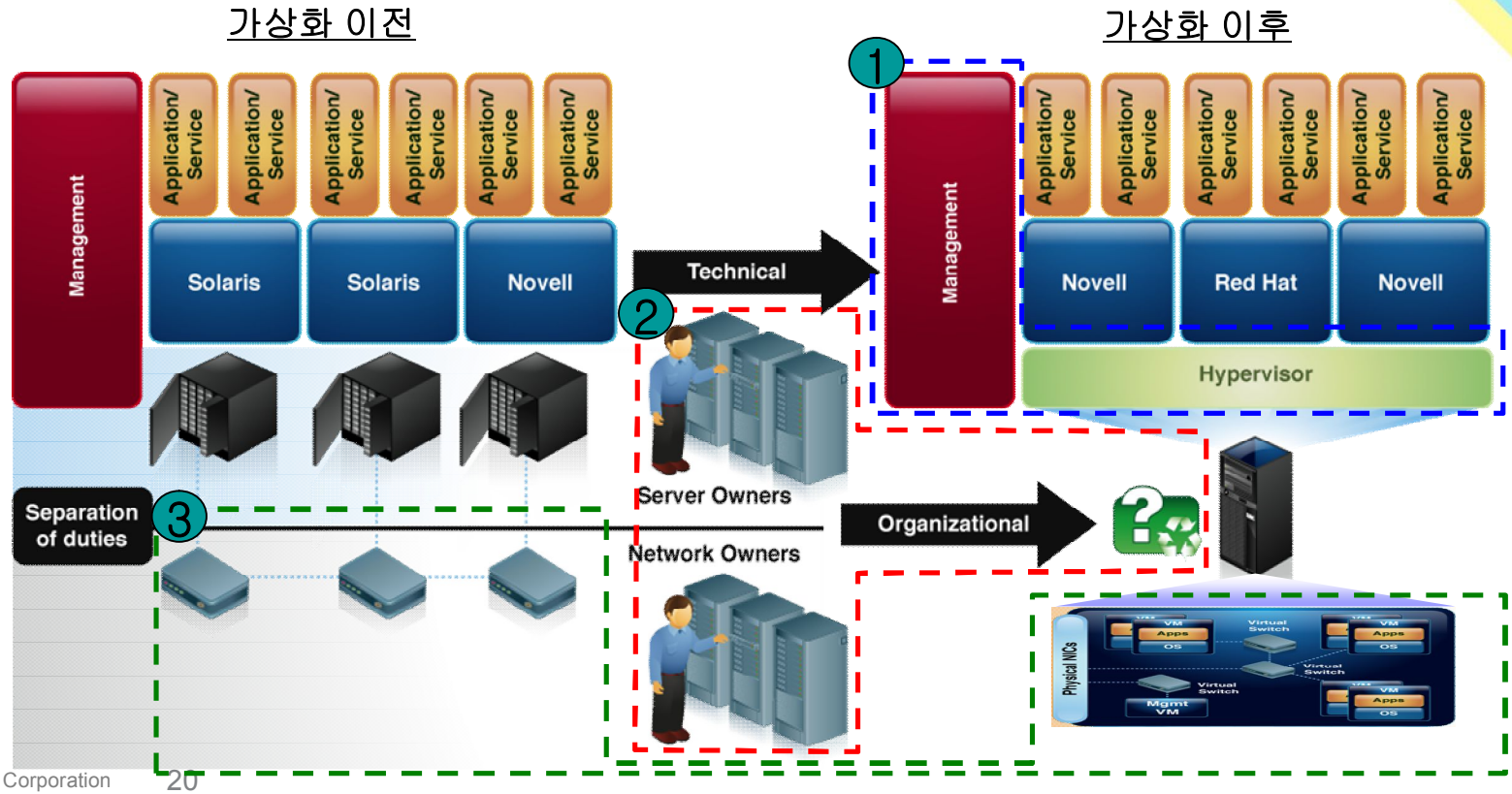
2. IBM 보안 전략 >클라우드 보안은?

클라우드 서비스는 서버, 스토리지 자원을 제공하는 **IaaS** 서비스 부터 **Collaboration, CRM, ERP** 등을 제공하는 **SaaS** 서비스 까지 다양하며 서비스 별 상이한 보안요건을 가집니다.



2. IBM 보안 전략 >클라우드 보안은?

가상화 기술의 적용은 **1)** 가상화 서버 인프라 보안 **2)**가상화 환경 운영 보안 **3)**가상 네트워크의 보안이슈를 가집니다



3. IBM 클라우드 보안 컨설팅/구축 서비스

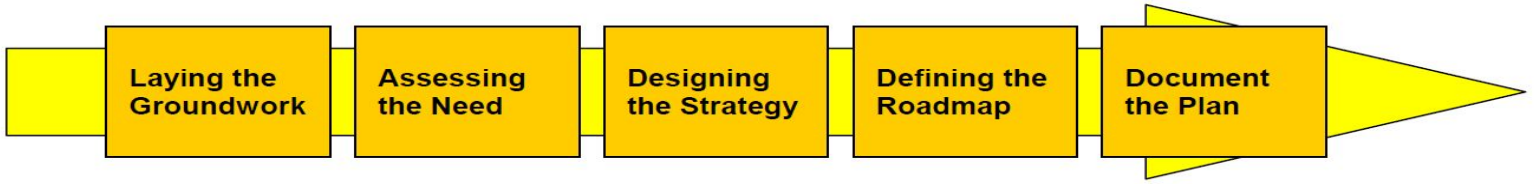
컨설팅과 구축서비스로 구분되며 로드맵 수립, 아키텍처 설계, 보안 솔루션 구축서비스를 제공합니다

단 계	서비스 명	개 요
컨설팅	Cloud Strategy Roadmap	클라우드 보안 로드맵 수립
	Cloud Security Assessment	클라우드 시스템 갭 분석 및 평가
구축	계정 통합관리 구축 서비스	Tivoli Identity And Access Assurance 기반의 통합 계정관리 시스템 구축
	End-point 보안 구축	Tivoli BigFix 기반의 end-point 보안 시스템 구축
	가상화 보안 구축	Virtual Server Security 기반의 보안 시스템 구축
	어플리케이션 보안 구축	Rational Appscan 기반의 개발보안 환경 구축

3. IBM 클라우드 보안 컨설팅/구축 서비스– Cloud Security Strategy Roadmap

서비스 개요 : **Cloud Security Strategy Roadmap** 서비스는 클라우드 보안, 프라이버시 고려사항을 검토하고 클라우드 보안목표를 수립하기 위한 방안을 제시합니다.

수행방법 : 고객의 클라우드 컴퓨팅 목표를 파악하고 이에 따른 보안 및 프라이버시 리스크 식별 및 하이레벨의 보안 전략 로드맵을 수립합니다.



MODULES: **[1]** **[2]** **[3]** **[4]** **[5]**

산출물

- 클라우드 보안 전략에 대한 **Roadmap Overview**
- 클라우드 보안 전략과 추진 방향
- 클라우드 보안 전략을 구현 하기 위한 과제 정의 및 실행계획

3. IBM 클라우드 보안 컨설팅/구축 서비스– Cloud Security Assessment

서비스 개요 : 클라우드 시스템 현황을 분석하고 평가합니다.

수행방법 : 현재 보안환경 분석, 베스트프랙티스 및 보안 요건을 기준으로 한 갭 분석, 보안 성숙도 평가를 수행합니다.

Requirement	Required Level	Achievement
Workload protection	Low/Moderate/High	Above average/ Average / Below average
Availability		
Elasticity		
Accountability		

Capabilities	Security Ranking
Review of Governance, Risk, and Compliance	Above average/ Average / Below average
Review of Application and Process Security	Above average / Average / Below average
Review of Identity Management	Above average / Average / Below average
Review of Confidential Data and Information	Above average / Average /

산출물

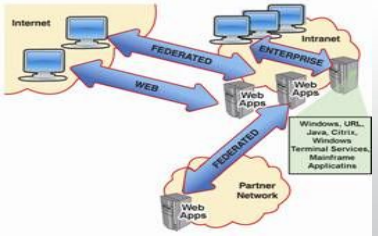
- 고객의 현 보안 현황에 대한 **Overview**
- 평가로 부터 도출되는 이슈사항 및 원인
- 보안 성숙도 및 설명
- 권고 사항: 지적되는 이슈사항에 대한 구체적인 추진 과제와 고려사항

3. IBM 클라우드 보안 컨설팅/구축 서비스 – 계정 통합관리 구축 서비스

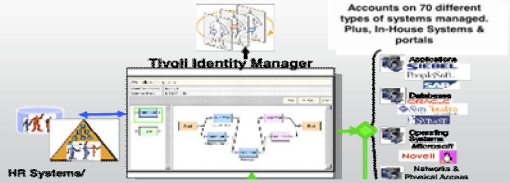
서비스 개요 : 통합된 인증, 권한관리, 접근관리 시스템을 구축합니다.
수행방법 : **Tivoli Identity And Access Assurance** 솔루션을 기반으로 클라우드 환경에서 통합된 계정관리 시스템을 구축합니다.

A

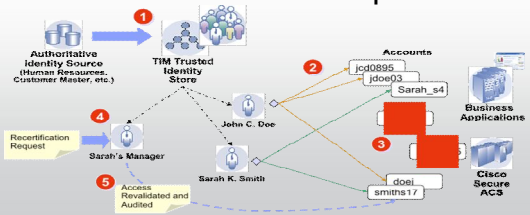
Single Sign On & Password Management



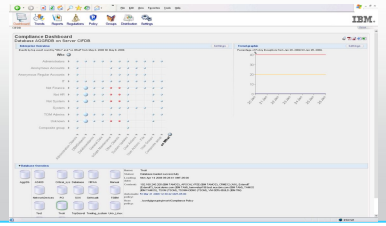
B User Provisioning / Role Management



C Access Validation & Compliance



D Security log management & reporting



구축 서비스 내용

- 계정 통합관리 설계 및 정책 수립
- 계정관리 시스템 구축
- 적용대상 시스템 계정 통합

3. IBM 클라우드 보안 컨설팅/구축 서비스 – End-point 보안 구축 서비스

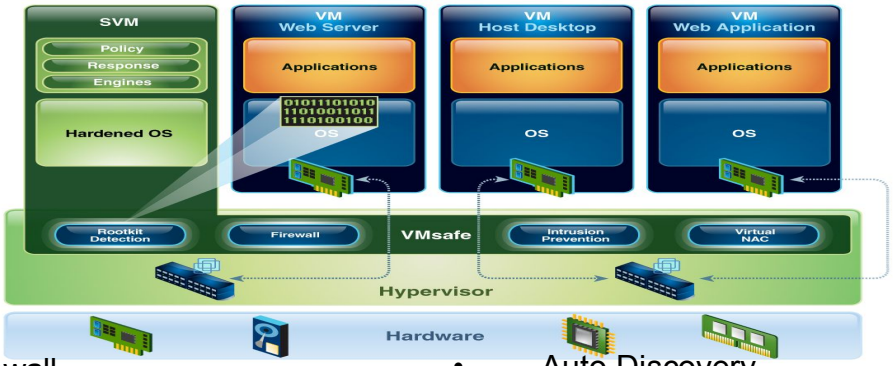
서비스 개요 : **End-point** 시스템에 대한 통합 보안관리 시스템을 구축합니다.
수행방법 : **IBM Tivoli BigFix** 솔루션을 기반으로 통합관리 시스템을 구축하여 보안정책 관리, 패치관리, 원격제어 환경을 구축합니다.

구축 서비스 내용

- End-point 보안 시스템 설계 및 정책 수립
- 통합 보안 관리 시스템 구축
  - 관리 서버 및 relay 서버 구성
  - 보안 Agent 구성
  - 보안 정책 구성
  - 패치 관리 구성
  - 원격 제어
  - 보고서 관리
  - 외부 시스템 연동
- Fixlet 스크립트 개발
  - 요건 별 스크립트 개발/적용

3. IBM 클라우드 보안 컨설팅/구축 서비스 – 가상화 보안 구축 서비스

서비스 개요 : **VMWare** 기반의 가상화 환경에 하이퍼바이저 수준의 보안 관리 시스템을 구축하여 가상머신 및 가상네트워크 보안을 강화합니다.
수행방법 : **Virtual Server Security for VMware** 솔루션을 기반으로 구축합니다.



- Firewall
- VMsafe Integration
- Rootkit Detection
- Intrusion Detection & Prevention
- Inter-VM Traffic Analysis
- VM Sprawl Management
- Network Policy Enforcement
- Automated Protection for Mobile VMs (VMotion)
- Auto Discovery
- Virtual Infrastructure Auditing (Privileged User Access)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Network Access Control
- Central Management
- Web Application Protection
- Virtual Patch

구축 서비스 내용

- 가상머신 보안 시스템 설계 및 정책 수립
- Virtual Server Protection for VMWare 시스템 구축
- 외부 시스템 연동 지원

3. IBM 클라우드 보안 컨설팅/구축 서비스

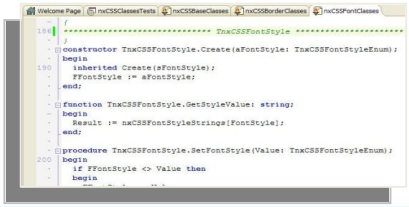
– 어플리케이션 보안 시스템 구축 서비스

서비스 개요 : 어플리케이션 보안 취약성 점검을 위한 솔루션을 구축하고 사용에 대한 교육을 수행합니다.

수행방법 : **Rational Appscan** 솔루션을 사용하여 소스코드 취약성 점검을 할 수 있는 환경과 **Blackbox** 취약성 점검을 할 수 있는 시스템을 구축하고 교육을 수행합니다.

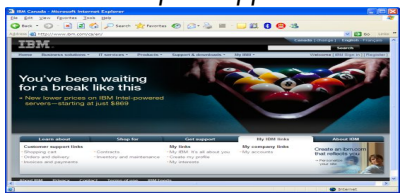
Static Code Analysis = Whitebox

Scanning source code for security issues



Dynamic Analysis = Blackbox

Performing security analysis of a compiled application



구축 서비스 내용

- 어플리케이션 보안 설계 및 정책 수립
- Whitebox 테스트용 환경 구축 및 개발 툴 연동
- Blackbox 테스트용 시스템 구축
- 취약성 점검을 위한 교육

별첨. IBM Security tools available for Cloud Computing