

클라우드 보안의 3원칙

김명호

한국마이크로소프트 최고기술임원 (NTO)

mhkim@microsoft.com

주요 내용

- 클라우드 보안의 특성
- 전체론적 관점에서의 클라우드 보안
 - Of the Cloud, For the Cloud, and By the Cloud
- 클라우드의 보안
- 클라우드를 위한 보안
- 클라우드에 의한 보안

The Top 10 Cloud Myths

1. Cloud is always about money
2. You have to be cloud to be good
3. Cloud should be used for everything
4. "The CEO said so" is a cloud strategy
5. We need a one-cloud solution
6. Cloud is less secure than on-premises
7. Cloud is not for mission-critical use
8. Cloud = Data center outsourcing or hosting
9. Migrating to cloud means you automatically get cloud characteristics
10. Virtualization = Private Cloud

– David Mitchell Smith, Gartner

<http://www.gartner.com/newsroom/id/2889217>

Myth #6: Cloud is less secure than on-prem's

- The Reality
 - Cloud is often more secure, but the risks are different
- Recommendations
 - Address cloud security perceptions
 - Avoid generalizations
 - Set high standards for all



클라우드 보안의 요소

Security
of the Cloud,
for the Cloud,
and by the Cloud





Security of the Cloud

클라우드의 보안

보안? 신뢰!

사이버 보안



프라이버시 & 제어



규정 준수




투명성



의존할 수 있는 기반

하이퍼스케일, 선택과 다양성, 서비스 지속성, 수용 가능한 SLA

Microsoft의 클라우드 규정 준수 / 인증 획득 현황

	Regulatory and Compliance Domain	 Office 365	Microsoft Azure	 Microsoft Dynamics CRM	Microsoft Intune
Broadly Applicable	ISO 27018:2014	✓	✓	✓	✓
	ISO 27001:2013	✓	✓	✓	✓
	SOC 1 Type 2 (SSAE 16/ISAE 3402)	✓	✓	✓	✓
	SOC 2 Type 2 (AT Section 101)	✓	✓	No	✓
	CSA STAR 1	✓	✓	✓	No
United States Government	FedRAMP Moderate	✓	✓	No	No
	CJIS Security Policy, Version 5.3	✓	✓	✓	No
	DISA SRG Level 2 P-ATO	✓	✓	No	No
	FDA 21 CFR Part 11	No	✓	No	No
	ITAR	✓	✓	No	No
	IRS 1075	✓	✓	No	No
Industry Specific	HIPAA BAA	✓	✓	✓	✓
	PCI DSS Level 1	N/A	✓	N/A	N/A
	FERPA	✓	✓	N/A	N/A
	CDSA	N/A	✓	N/A	N/A
Region/Country Specific	EU Model Clauses	✓	✓	✓	✓
	UK G-Cloud v6	✓	✓	✓	✓
	Australia Gov ASD	✓	✓	No	No
	Singapore MTCS	✓	✓	✓	No
	Japan FISC	✓	✓	No	No
	New Zealand GCIO	✓	✓	No	✓

규정 준수와 투명성

- 다양한 인증만으로는 비즈니스 결정을 내리기 어려움
- 클라우드 공급자의 책임
 - 종합적이고 명문화된 정보 보안 프로그램 유지
 - 프로그램의 요약과 그것이 어떤 표준이나 인증을 준수하는지 충실히 공개
 - Microsoft 의 사례: [Azure Trust Center](#), [Office 365 Trust Center](#)
- 고객은 공급자정보를 기반으로 최적의 클라우드 선택

Microsoft의 CSA/CCM 활용 사례

Control ID In CCM	Description (CCM Version R1.1)	Microsoft Response
DG-01 Data Governance - Ownership / Stewardship	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.	Microsoft Online Services has implemented a formal policy that requires assets (both data and hardware) used to provide Microsoft Online Services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets. “Allocation of information security responsibilities and ownership of assets” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.1.3 and 7.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.
DG-02 Data Governance - Classification	Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.	Microsoft Online Services standards provide guidance for classifying assets of several applicable security classification categories, and then implements a standard set of Security and privacy attributes. “Information classification” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7.2. For more information review of the publicly available ISO standards we are certified against is suggested.

역할의 분산

- 데이터 거버넌스와 권한 관리
- 클라이언트 엔드포인트
- 계정과 액세스 관리
- ID와 디렉토리
- 애플리케이션
- 네트워크 제어
- 운영체제
- 물리적 호스트
- 물리적 네트워크
- 물리적 데이터센터
- 보안
- 프라이버시와 제어
- 규정 준수
- 투명성

	SaaS	PaaS	IaaS	On-Prem
데이터 거버넌스와 권한 관리	■	■	■	■
클라이언트 엔드포인트	■	■	■	■
계정과 액세스 관리	■	■	■	■
ID와 디렉토리	■	■	■	■
애플리케이션	■	■	■	■
네트워크 제어	■	■	■	■
운영체제	■	■	■	■
물리적 호스트	■	■	■	■
물리적 네트워크	■	■	■	■
물리적 데이터센터	■	■	■	■
보안	■	■	■	■
프라이버시와 제어	■	■	■	■
규정 준수	■	■	■	■
투명성	■	■	■	■

- 공급자가 관리
- 고객이 관리



Security for the Cloud

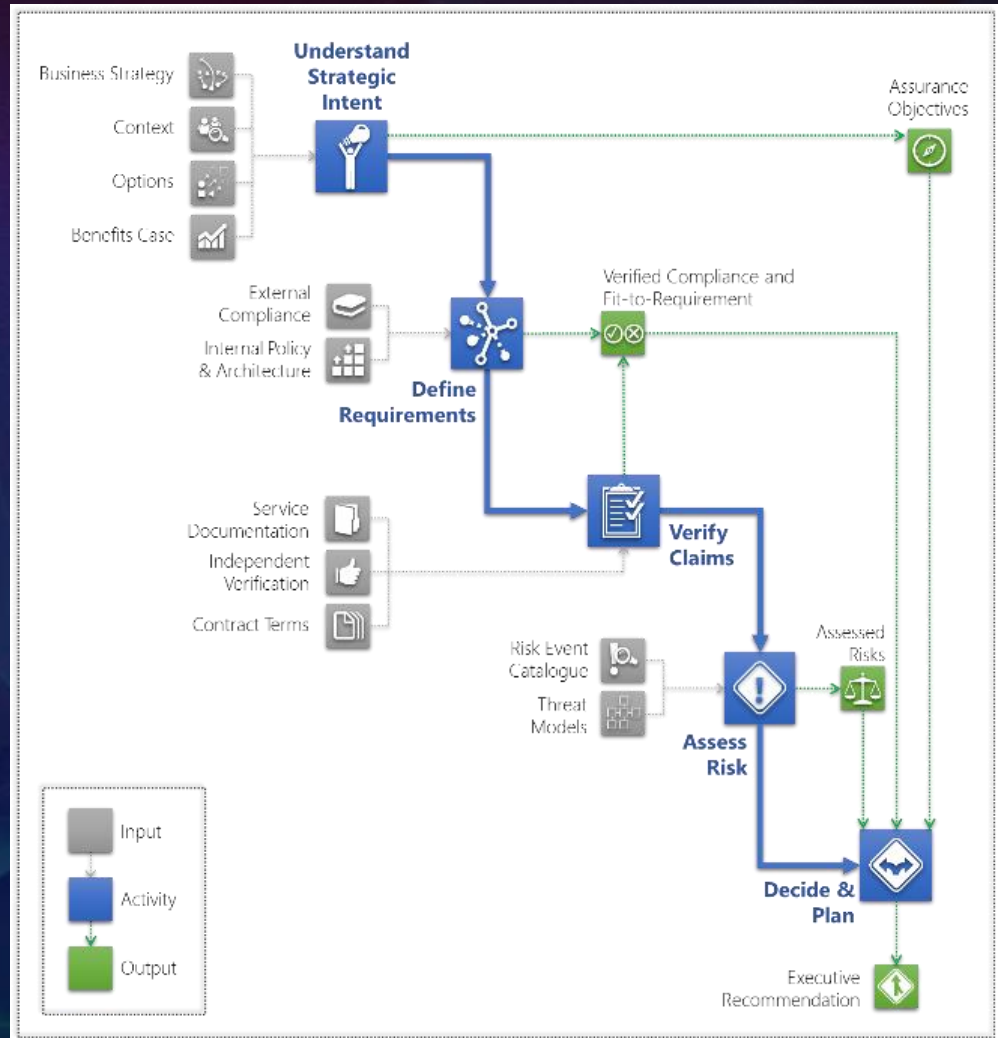
클라우드를 위한 보안

보안과 클라우드 도입 전략

- 보안 시험평가 프레임워크
 - 클라우드 기반 애플리케이션의 규정준수 여부와 위험도 비교 평가를 위한 방법론
- 데이터 거버넌스와 데이터 분류
 - 어떤 데이터가 어떤 상황에서 어떤 제어와 함께 클라우드에서 사용할 수 있는지 판단하는 데 활용 가능

SAFE 방법론

- 애플리케이션이나 클라우드 서비스의 보안 보증을 위한 5단계 프로세스
- 기존 관행의 적극 활용과 일관성 추구
 - ISO 27000 계열
 - ISO 31000 계열



SAFE 위험 도메인 분석

Assurance Domain

Trustworthiness

Resilience

Adaptability

Risk Consequence / Impact

Strategic

Large data breach of sensitive, private customer data

Disruption of service significant enough to cause revenue loss and departure of customers

The service is inflexible to changes in business needs, limiting strategic options

Operational

Confused responsibilities between customer and cloud provider leading to operational incidents

Unpredictable downtime during business hours causing loss of productivity

Changes to the service configuration require downtime that impacts productivity

Compliance

Provider committing to security practices but failing to do so causing a compliance problem

Disaster preparedness of the cloud service provider inadequate to satisfy regulators

Service provider is unable to comply with new regulations or other compliance obligations

Technical

Loss of encryption keys possibly enabling interception of encrypted customer data

Highly integrated nature of the cloud infrastructure enables one failure to cascade into disaster

Tools used by the customer and service provider are incompatible causing interoperability problems

데이터 분류

정의

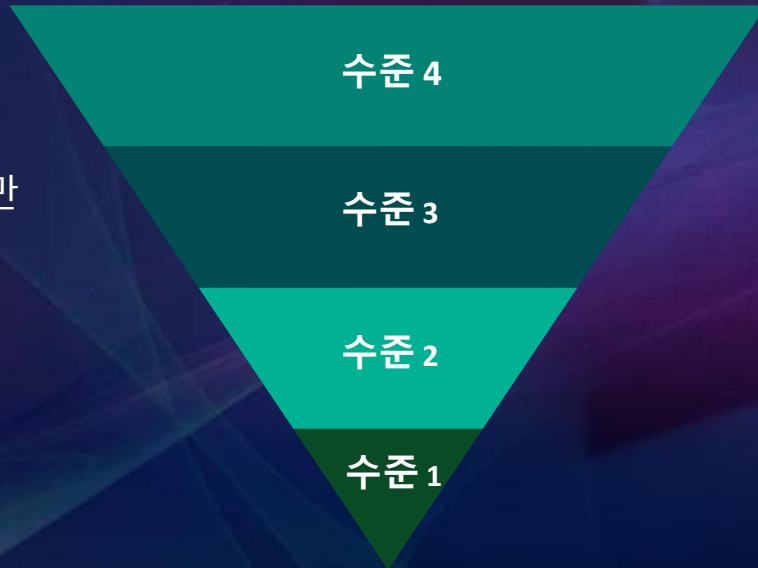
Public: 공개적으로 활용 가능한 데이터. 사용에 제한이 없음

Internal: 기본적으로 조직 내에서만 공유. 외부와 거의 공유되지 않음

Restricted: 기본적으로 제한된 데이터. 필요한 개인에게만 공유됨

Highly Classified: 조직의 안위에 결정적인 데이터

민감도 수준



분량

많음



적음

Data Classification Wizard (Microsoft)

The screenshot shows the Microsoft Data Classification Wizard web interface. The browser address bar displays <https://www.microsoft.com/security/data/>. The page title is "Data Classification Wizard" with the subtitle "Business Data Examples".

At the top, there are four classification levels with corresponding colored boxes: HBI (red), MBI (orange), LBI (green), and Public (blue). To the right is a "MY SELECTIONS" button with a left-pointing arrow.

The main content area is divided into three columns of data categories:

- Non-User Data**
 - "Announced" Corporate Financial Data
 - Material Financial Data
 - Publicly Released Source Code
 - Source Code or Binaries
 - Source Code, Symbols, Binaries, or Specifications
 - Trade Secrets
- Supplier or Vendor Management Data**
 - Bank Account Numbers
 - Receipts and Payment Data
 - Sales Account Data
 - Documentation**
 - Current Systems Configuration Data
 - Data or Software File Shares
- Keys and Certificates**
 - Hardware or Software Tokens
 - Private Cryptographic Keys
 - Product Keys (Individual)
 - Public Cryptographic Keys
 - Employee Data**
 - Personal Employment Data

(공공부문) 데이터 분류 모범 사례

UK



OFFICIAL ("up to 90%")

SECRET

TOP SECRET

AU



UNCLASSIFIED (~70%)

PROTECTED
(20%)

SECRET
(10%)

US



FISMA LOW

FISMA MODERATE

FISMA HIGH

(FISMA LOW+MODERATE= ~80% of US Government

data)



Security by the Cloud

클라우드에 의한 보안

클라우드를 활용한 보안 강화

- 위험 관리에 클라우드 적용
 - 위험-기반 결정은 이점과 위험도의 Δ 기반
 - 클라우드의 도입이 이점과 위험에 미치는 영향 분석
- 인프라 보안에 클라우드 활용
 - 클라우드를 또 한겹 보안 안전막으로 도입

위험 관리에 클라우드 적용

- 클라우드는 보안을 포함한 비즈니스 위험을 완화하는 보완 제어를 제공하는 데 활용할 수 있음
- 위험의 3가지 핵심 측면
 - 유형
 - 영향
 - 가능성

Risk Management: An Example

Risks		Initial		Compensating Controls			Residual	
	Risk Name	Likelihood	Impact	Mitigate	Likelihood	Impact	Likelihood	Impact
Financial	Data Protection Risks	Likely	Serious					
	Governance Degradation	Highly Likely	Serious					
	Compliance Degradation	Highly Likely	Serious					
Operating	Loss of business reputation	Likely	Serious					
	Service Termination or Failure	Likely	Serious					
	Inaccurate Modeling of Resource Usage / Resource Exhaustion	Not Likely	Serious					
Market	Isolation Failure	Not Likely	Severe					
	Human Resource Constraints	Not Likely	Serious					
	Malicious Activities from an Insider	Highly Likely	Serious					
Strategic	Sensitive Information Leakage	Highly Likely	Severe					
	Subpoena and e-discovery	Likely	Serious					
	Environment Agility / Time to Market	Not Likely	Serious					
Compliance	Agility / Time to Market	Not Likely	Serious					
	Natural Disasters	Not Likely	Serious					
	Backup Lost, Stolen	Likely	Severe					
	Unauthorized access to premises	Highly Likely	Serious					
	Theft of Computer Equipment	Likely	Serious					
	Audit and Certification	Highly Likely	Serious					
	Inadequate Resource Provisioning and Investment in Infrastructure	Not Likely	Serious					
	Storage of data in multiple jurisdictions without transparency	Expected	Severe					
	Poor Provider Selection	Likely	Mild					
	Lack of Supplier Redundancy	Likely	Serious					
	Vendor Lock-In	Expected	Mild					
	Integration of identity management systems	Likely	Mild					
	Security of the endpoint	Not Likely	Serious					
	Impact on current internal operational procedures	Expected	Mild					
	Operations management	Expected	Mild					
Adequate Data Classification	Expected	Mild						

클라우드를 활용한 심층 방어



클라우드 보안의 전체론적 접근

Of the Cloud

신뢰가 선행될 것
정보 기반 선택과 투명성
역할과 기능 분산

For the Cloud

보안 보증 프레임워크
데이터 거버넌스와 분류

By the Cloud

클라우드 기반 위험 관리
클라우드 활용 심층 방어

감사합니다!