안랩 클라우드 정보보호 컨설팅 수행 전략

2016.12.

안랩

AhnLab

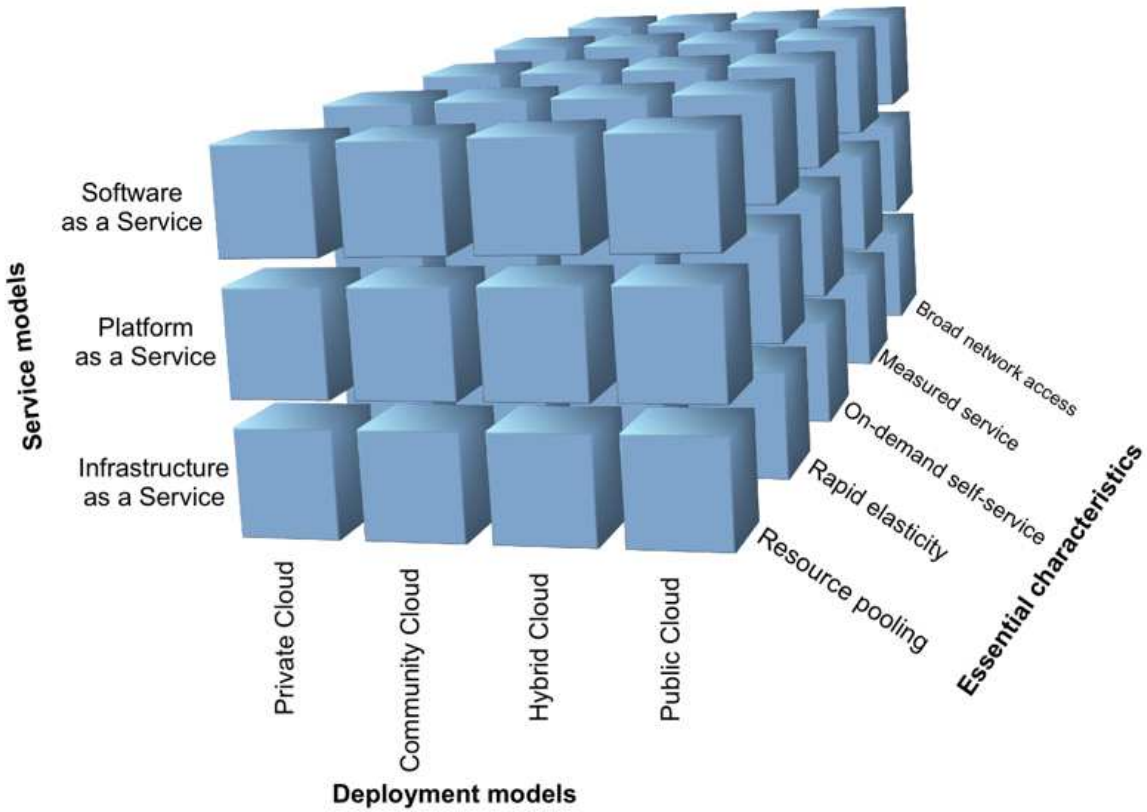
Contents

Contents

1.1. 클라우드 모델 및 특징

미국의 NIST는 클라우드 컴퓨팅을 설정이 가능한 컴퓨팅 자원의 공유 풀에 편리한 온디맨드 네트워크 액세스를 제공하는 모델로써 3개의 서비스 모델, 4개의 구현 모델로 구성되고 5개의 특징으로 설명함

클라우드 모델 및 특징



※ NIST CLOUD CUBE MODEL

분류	내용
서비스 모델	• IaaS(Infrastructure as a Service)
	• PaaS(Platform as a Service)
	• SaaS(Software as a Service)
구현 모델	• 프라이빗 클라우드
	• 커뮤니티 클라우드
	• 퍼블릭 클라우드
	• 하이브리드 클라우드
특징	• 온디맨드 셀프 서비스
	• 유비쿼터스 네트워크 액세스
	• 리소스 풀링
	• 고 탄력성
	• 측정 가능한 서비스

1.2. 클라우드 보안 위협

클라우드 보안 위협은 데이터, 시스템/네트워크, 관리적 위협으로 분류하여 세부 위협 항목을 식별 함

클라우드 보안 위협

분류	위협 항목	Gartner	RSA	CSA Threat	CSA CCM	Japan ASP,SaaS	ENISA
데이터	• 데이터 손실 및 유출 위협 (데이터 백업관리, 외부저장장치 관리, 삭제관리)	√		√	√	√	√
	• 데이터 변조 위협 (암호화, 키관리, 기밀성, 무결성)	√	√		√	√	√
시스템/ 네트워크	• 인증 및 권한관련 위협 (사용자 계정 유출, 관리자 권한 분리)	√	√	√	√	√	√
	• 시스템 및 네트워크 보안 위협 (Malware, OS 보안취약점, 가상 네트워크)		√	√	√	√	
	• 시스템 악용 위협 (피싱, 봇넷의 악용파악, 추적조사기능 보장)	√	√	√	√	√	
	• 가상머신 보안 위협 (하이퍼바이저 취약점)		√	√	√		
관리적 위협	• 보안수준 보장 및 사고대응의 어려움	√				√	√
	• 서비스 장애 위협 (재난관리, 폐업, 합병에 대한 기업의 지속성)	√	√		√	√	√
	• 법령 및 규정 준수 (데이터 해외 이전, 망분리, SLA)	√	√		√	√	√
	• 통합 정책 관리의 어려움		√	√	√		

1.3. 클라우드 보안 사고·사례

최근 클라우드의 멀티테넌시, 자원의 공유, 인터넷망 이용 등 특성과 내·외부 위협으로 인해 클라우드 관련 보안 사고가 발생함

클라우드 보안 사고·사례

사고 유형	일자	주요 내용
클라우드 서비스의 멀티테넌시 특성으로 인한 관리 부주의	2010.12	• MS BPOS 서비스 환경 설정 오류로 인해 기업정보가 유출
	2011.06	• 국내 K사 관리자 실수로 고객 계정/가상서버 삭제
클라우드 서버에 고객정보 집중화로 인한 대규모 서비스 장애	2010.12	• 아마존 EC2 백업 오류로 190여개 서비스 11시간 마비
	2012.06	• First Server 시스템 업그레이드 중 오류발생으로 5,698개 회사의 대규모 데이터 소실
클라우드 서비스 악용	2010.10	• 아마존 EC2 서비스 이용한 DoS 공격 (DEFCON Hacking Conference 2010) * 취약한 호스트 들을 해킹하는 과정 없이 적은 비용으로 손쉽게 C&C 서버 및 좀비 PC 확보 가능
	2011.04	• 소니의 PlayStation Network 공격을 위해 Amazon E2C 사용
	2013.02	• 백도어 활동, C&C 서버의 수집 정보 은닉 장소로 Evernote 이용 • 신종 멀웨어 발견
	2013.05	• 사이버 범죄 도구를 웹에서 제공 '사이버크라임 포털' 사이트 등장 (Crimeware as a Service)
클라우드 서비스 해킹	2012.01	• DreamHost의 DB 해킹 으로 인한 개인정보 유출
	2013.02	• ZenDesk 시스템 해킹으로 인한 개인정보 유출
DDoS 공격 영향	2016.10	• 미국 인터넷호스팅회사 딘(Dyn)의 DNS 서버에 디도스 공격으로 AWS 접속 장애

Contents

2.1. 국외 클라우드 정보보호 인증 제도

국외 클라우드 관련 인증은 ISO 표준인증과 CSA(Cloud Security Alliance) STAR가 있고, 금융관련 클라우드 인증은 PCI-DSS에서 클라우드에 관한 사항을 반영하고 있음

국외 클라우드 인증

클라우드 인증	ISO 27017	CSA STAR CERTIFICATION	ISO 27018	PCI DSS COMPLIANT
Base 기준	ISO/IEC 27002	CSA CCM	ISO/IEC 27002 ISO/IEC 29100	VISA, Master 보안프로그램
적용영역	클라우드 정보보호	클라우드 정보보호	클라우드 개인정보보호	신용카드 보호
적용대상	PROVIDER, COUSTOMER	PROVIDER, COUSTOMER	PROVIDER, COUSTOMER	PROVIDER, COUSTOMER
클라우드모델	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS
인증기관	ISO 인증기관	3rd-Party Assessments	ISO 인증기관	QSA 인증기관
통제항목 수	14개영역 114 항목	16개 영역 133 항목	14개영역 114 항목	12개영역 415개 항목
특징	• ISO 27002에 클라우드 서비스에 적합한 새로운 구현 지침을 추가하고, 클라우드 서비스에 특화된 확장 통제 항목으로 7개를 추가함 • 각 항목별로 Cloud Service Customer와 Cloud Service Provider에 대한 구현 안내	• 1단계 : CIAQ를 사용한 자가진단 • 2단계 : 3rd-Party 인증 • 3단계 : 실시간 모니터링 모델 • 2단계에서 STAR 인증 성숙도 평가 수행 • IaaS, Paas, SaaS 사업자별 적용항목 명시	• 16개 통제항목에 대한 클라우드 개인정보보호 구현 지침 추가 • 개인정보 생명주기 관련 25개의 확장 통제항목 추가	• Payment 국제 인증 • Version 2.0에서 12항목에 대한 클라우드 요구사항 정의 • 각 요구사항의 IaaS, PaaS, SaaS 별 고려사항 정의

2.2. 국내 클라우드 정보보호 인증 제도

국내의 경우 클라우드발전법 발의와 함께 공공기관 클라우드 활성화를 위해 IaaS 사업자를 대상으로 인증획득 시 공공기관이 사용할 수 있도록 관련 통제 기준을 제시함

국내 공공 클라우드 인증

Base 기준	• ISO 27001/ ISO27017 • 클라우드컴퓨팅 발전법 內 정보보호 조치사항 • ISMS
적용영역	공공기관의 민간클라우드 이용
적용대상	IaaS 민간 사업자 대상
클라우드모델	IaaS
인증기관	KISA
통제항목 수	14개영역 118 항목
특징	• 공공기관을 위한 물리적으로 분리된 클라우드서비스 요건 존재 • 모바일 클라우드 보안에 대해 별도의 명시항목 없음 • 인프라 사업자만을 대상으로 하므로 클라우드 플랫폼 및 소프트웨어 사업자에 대해 고려되지 않음 • 제공자와 사용자의 차이에 따른 적용가이드 수립 안됨

통제분야	통제영역	항목	설명
관리적 보호조치	1. 정보보호 정책 및 조직	5	클라우드 환경을 고려한 보안정책 수립, 제공자의 책임 한계를 정의, 정보보호 조직 및 책임자의 지정에 대한 통제
	2. 인적보안	12	내・외부 임직원의 채용, 퇴직, 교육, 정보보호 활동에 관한 통제
	3. 자산관리	10	자산을 식별 및 분류하고 자산의 위험을 관리하는 활동에 대한 통제
	4. 서비스 공급망	4	망의 가용성, 보안요구사항이 포함되는 계약과 변경관리 시 안전성 검토 및 계약, 모니터링 활동에 대한 통제
	5. 침해사고관리	7	침해사고 대응 체계의 수립과 체계에 따른 활동에 대한 통제
	6. 서비스연속성관리	7	장애대응, 성능 및 용량관리 등 서비스연속성 유지에 대한 통제
	7. 준거성	4	법률의 준수 및 감사활동에 대한 통제
물리적 보호조치	8. 물리적 보안	12	보호구역의 지정, 구역내 설비의 보호 및 유지보수 활동에 대한 통제
기술적 보호조치	9. 가상화 보안	11	클라우드 서비스의 특징인 가상자원에 대한 보호 및 가상자원 이전 시 발생하는 호환성 검토에 대한 통제
	10. 접근통제	10	권한의 부여, 회수 등 접근권한 관리 기능과 이용자의 클라우드 서비스 사용 시 강화된 인증기법 적용에 대한 통제
	11. 네트워크 보안	6	제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 분리 및 네트워크 보안 정책에 대한 통제
	12. 데이터 보호 및 암호화	10	데이터의 이용, 폐기 및 데이터의 암호화에 대한 통제
	13. 시스템 개발 및 도입 보안	12	시큐어코딩, 개발과 운영환경의 분리 등 시스템 개발 시 보호활동에 대한 통제
공공기관용 추가 보호조치	14. 공공기관 보안요구사항	8	SLA, CC인증제품, 물리적 망분리를 포함하는 공공기관 보안 요구사항에 대한 통제
	합계	118	

2.3. 국내·외 클라우드 정보보호 인증 비교

클라우드 컴퓨팅 정보보호에 관한 기준은 IaaS, 공공기관이 주요 대상으로 PaaS, SaaS 대상 항목은 일부만 해당되므로 PaaS, SaaS 사업자의 경우 CSA STAR, ISO27017 기준에서 필요한 항목을 선택하여 적용해야 함

- 국내 공공 클라우드 인증과 ISO27017/CSA STAR 클라우드 인증 진단 기준 비교

ISO 27017 : 2015															클라우드 컴퓨팅 정보보호에 관한 기준	CSA STAR PROGRAMS														
5. 정보보호정책	6. 정보보호조직	7. 인적보안	8. 자산관리	9. 접근통제	10. 암호화	11. 물리적보안	12. 운영보안	13. 통신보안	14. 시스템개발보안	15. 공급망관리	16. 정보보호사고관리	17. 연속성관리	18. 법적준거성	추가통제		APP 및 인터페이스 보호	감사 보증 및 규정 준수	사업 연속성 관리	변경관리	데이터 성명주기 관리	데이터 센터 보호	암호화 및 키관리	위험관리	인적보안	인증 및 엑세스 제어	인프라 및 가상화 관리	상호운영성 및 이식성	모바일 보안	보안사고관리	공급망관리	위협취약점관리
√	√														1. 정보보호 정책 및 조직		√														
		√													2. 인적보안									√							
			√				√								3. 자산관리				√	√			√								√
										√					4. 서비스 공급망															√	
											√				5. 침해사고관리														√		
							√					√			6. 서비스연속성관리			√														
							√						√		7. 준거성		√															
						√	√		√						8. 물리적 보안						√											
														√	9. 가상화 보안	√										√	√				
				√			√								10. 접근통제										√						
				√			√	√							11. 네트워크 보안																
				√	√		√								12. 데이터 보호 및 암호화					√		√									
							√		√						13. 시스템 개발 및 도입 보안				√													
													√		14. 공공기관 보안요구사항																

Contents

3.1. 클라우드 유형별 정보보호 고려사항

각 클라우드 서비스 유형에 따라 관리자, 소유자, 위치, 접근하는 사용자가 결정되고, 클라우드 유형 별 특성에 따라 보안통제가 적용 되도록 정보보호 관리체계를 수립함

- 클라우드 유형별 정보보호 고려사항

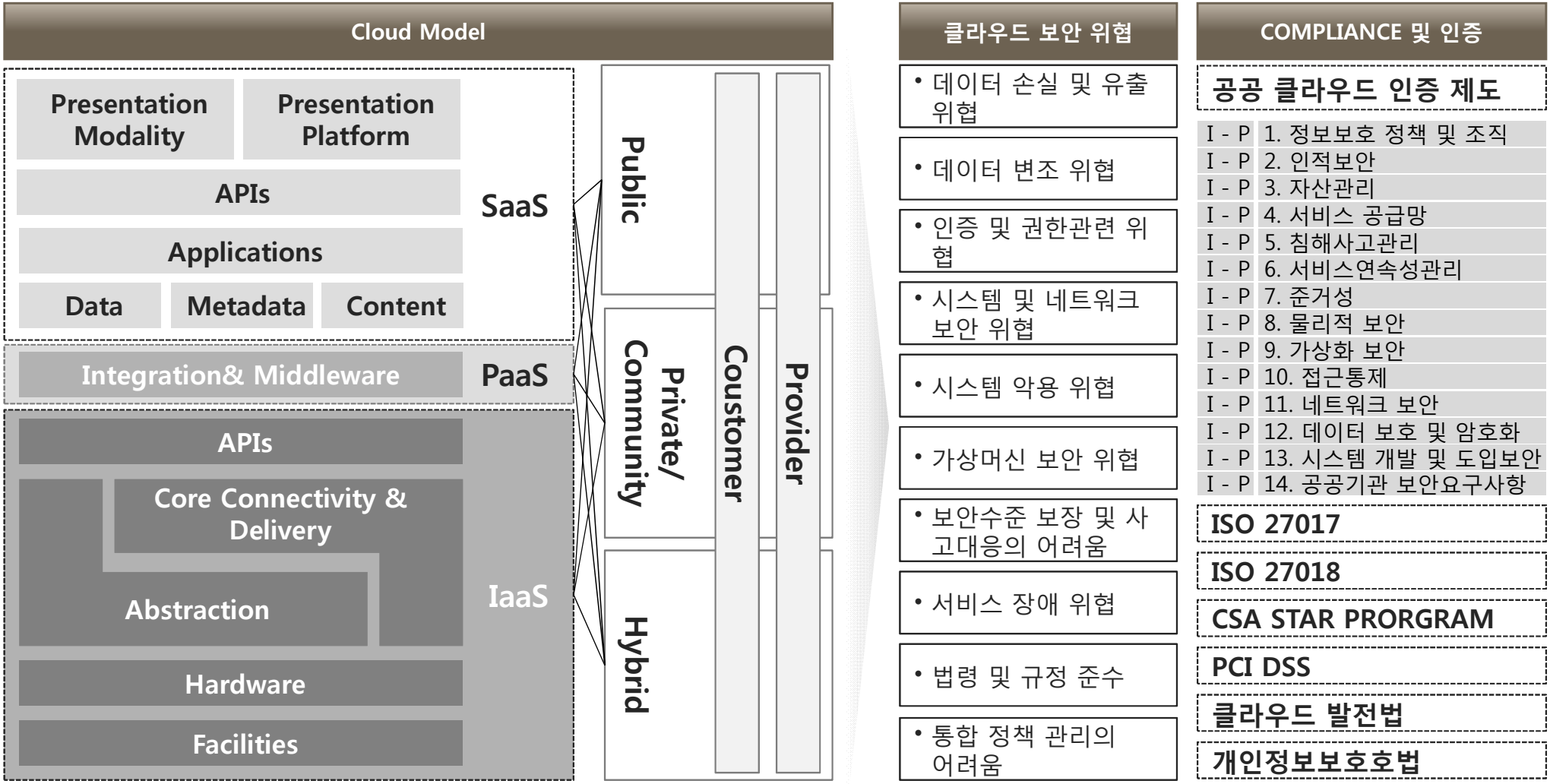
	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	3rd Party Provider	3rd Party Provider	Off-Premise	Untrusted Consumer
Private/ Community	Organization Or Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted Consumer
Hybrid	Both Organization & 3rd Party Provider	Both Organization & 3rd Party Provider	Both On-Premise & Off-Premise	Trusted Consumer & Untrusted Consumer

1) 관리에는 다음이 포함됨 : 거버넌스, 운영, 보안, 컴플라이언스 등
2) 인프라는 시설, 컴퓨팅, 네트워크 및 스토리지 장비와 같은 물리적 인프라를 의미함
3) 인프라 위치는 물리적인 것, 조직의 관리 체계 그리고 통제에 대비한 소유권을 말함
4) 신뢰할수 있는 서비스 사용자는 직원, 계약자, 사업 파트너를 포함하여 조직의 법률, 계약, 정책 체계의 일부로 간주되는 사람들이고, 신뢰할 수 없는 사용자는 일부 또는 모든 서비스를 사용할 권한은 있지만 조직의 논리적 확장에 포함되지 않는 사람들임

3.2. 클라우드 모델별 위험분석

클라우드 모델, 유형에 따라 클라우드 보안 통제항목에서 요구하는 사항이 달라지므로 클라우드모델을 분석한 후 보안위협을 고려하여 컴플라이언스 모델을 적용해야 함

클라우드 모델/유형별 위험 분석



Contents

4.1. 안랩 정보보호 컨설팅 방법론(ASEM-AhnLab Security Engineering Method)

계획수립-위험분석-대책수립-구현·관리로 구성된 AhnLab의 정보보호컨설팅 방법론인 ASEM(Ahnlab Security Engineering Method) 방법론을 적용하여 클라우드 보안 컨설팅 프로젝트를 수행함

ASEM 방법론

주요 Activity

- 담당자 요구사항 분석
- 법적 요구사항 분석
- 기술진단 대상 선정
- IT자산 현황 조사

- 정보자산 식별 및 분류
- 정보보호 및 개인정보보호 수준 평가
- 기술적 취약점 진단 실시

- 정보보호 정책/지침 개정
- 취약점 조치계획 및 마스터플랜 수립

- 실무자 및 직원 대상 정보보호 교육 실시

4.2. 안랩 클라우드 정보보호 컨설팅 서비스

안랩 클라우드 정보보호 컨설팅 서비스(AhnLab Cloud Security Consulting Service)는 클라우드에 대한 Risk를 식별하여 평가하고 보안대책을 수립하여 안전한 클라우드의 이용·제공에 기여함

안랩 클라우드 정보보호 컨설팅 서비스 개요

구분		내용
목적		• 안랩 클라우드 정보보호 컨설팅 서비스는 클라우드에 대한 RISK를 식별 및 평가하고 보안대책 수립을 통해 안전한 클라우드의 이용·제공에 기여함
서비스 대상		• 클라우드 모델·유형 - IaaS / PaaS / SaaS / SeCaaS - Private Cloud / Community Cloud / Public Cloud / Hybrid Cloud
서비스 특징		• 안랩의 정보보호컨설팅 방법론인 ASEM(Ahnlab Security Engineering Method) 방법론을 이용하여 클라우드 모델·유형별 IT현황분석, 보안 취약점, 위협, 위험분석을 수행하고 보안대책을 수립
주요서비스	Compliance	• 클라우드 컴퓨팅 구축/제공/이용 등에 따른 법적 준거성 검토 및 분석 - 클라우드발전법, 전자금융거래법, 정보통신망법, 개인정보보호법, 의료법 등
주요서비스	정보보호 인증	• 클라우드 정보보호 인증 컨설팅 서비스 - 공공기관 클라우드 보안인증, ISO27017, ISO27018, CSA STAR PROGRMAS, ISMS, ISO27001 등
주요서비스	모의해킹 및 시스템 진단	• 하이퍼바이저(ESXi, KVM), 가상 OS/NW/DBMS 시스템 취약점 진단 • 모의해킹(Pen Test)
수행 절차		클라우드 유형/모델 및 IT환경 분석 → 관리적•기술적 취약점 진단 → 위험분석 → 보호대책 수립

4.3. 안랩 클라우드 정보보호 컨설팅 프로젝트 수행 전략

안랩 클라우드 정보보호컨설팅 서비스는 클라우드 컴퓨팅 모델·유형 분석, 법적/관리적/기술적 취약점 진단, 위험 분석, 보호대책을 수립함

안랩 클라우드 정보보호 컨설팅 프로젝트 수행

Process

클라우드 유형/모델 및 IT환경 분석 → 관리적•기술적 취약점 진단 → 위험분석 → 보호대책 수립

Phase

Phase1 — Phase 2 — Phase 3 — Phase 4 — Implement

Com-ponents & Activity

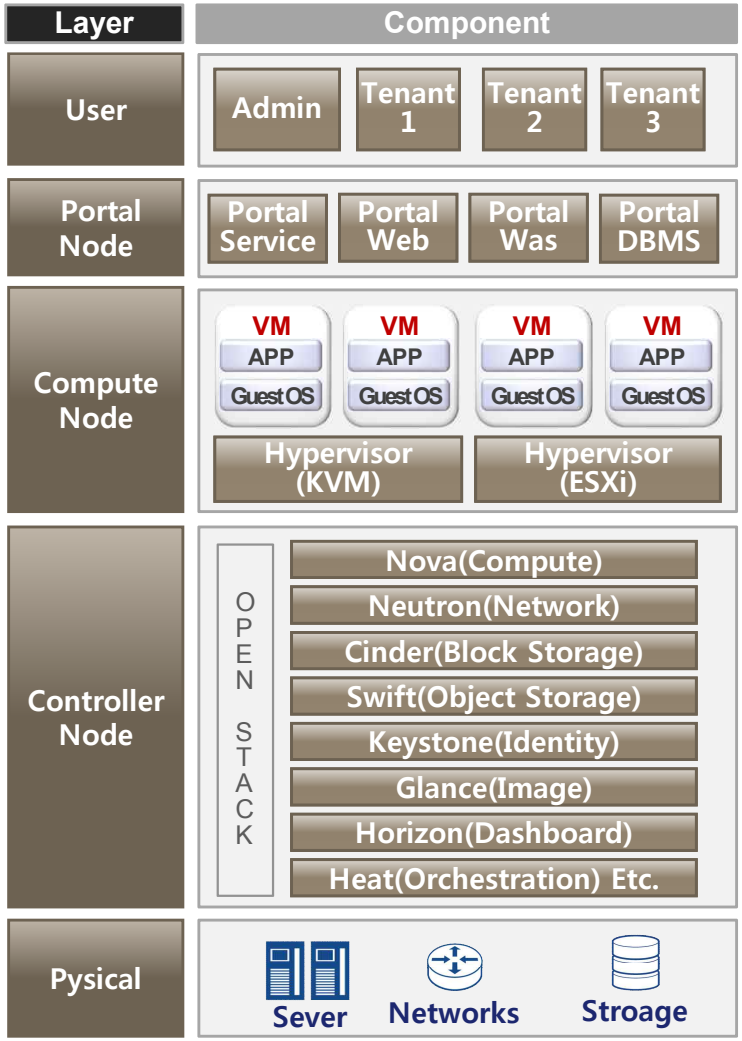
Phase1	Phase 2	Phase 3	Phase 4
서비스모델: • IaaS • PaaS • SaaS	컴플라이언스: • 클라우드발전법 • 전자금융감독규정 • 개인정보보호법 • 정보통신망법 • 의료법 등	위협: • 데이터 손실 및 유출 위협 • 인증 및 권한 위협 • 시스템·NW 보안 위협 • 가상머신 보안 위협 • 보안사고 대응 어려움 • 서비스 장애 위협 • 법령 및 규정 준수 • 통합 정책 관리의 어려움	관리적 대책: • 정보보호 정책 및 조직 • 인적보안 • 자산관리 • 서비스 공급망 관리 • 서비스 연속성 관리 • 법적 준거성
구현모델: • 프라이빗 클라우드 • 커뮤니티 클라우드 • 퍼블릭 클라우드 • 하이브리드 클라우드	인증: • ISO27017 • ISO27018 • CSA STAR PROGRAMS • 공공기관 클라우드 인증		물리적: • 물리적 보호구역 • 정보처리 시설 및 장비보호
특징: • 온디맨드 셀프 서비스 • 유비쿼터스 NW • 리소스 풀링 • 고 탄력성 • 측정 가능 서비스	취약점 진단: • 하이퍼바이저 • Virtual OS • Virtual NW • Virtaul DB • 모의해킹	위험평가: • 위험식별 • 위험평가 • DoA 선정 • 위험처리 전략: 위험감소, 위험수용, 위험전가, 위험회피	기술적 대책: • 가상화 인프라 • 접근통제 • 네트워크 보안 • 데이터 보호 및 암호화 • 시스템 개발 및 도입 보안

Contents

5.1. IaaS/Private Cloud 정보보호 컨설팅 프로젝트

최근 A그룹사의 클라우드 서비스(IaaS/Private Cloud)를 대상으로 컴플라이언스, 정보보호 인증, 기술 취약점 진단을 수행하였고, A그룹사 클라우드 서비스는 ISO 27017을 획득함

A그룹사 클라우드 보안 컨설팅 프로젝트



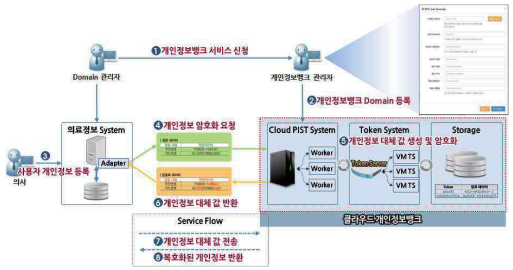
대상		• A그룹사 클라우드 서비스
특징		• 오픈스택 기반 IaaS 클라우드 시스템/서비스 구축에 따른 보안 위협/취약점 분석 및 대책 수립
수행절차	클라우드 모델 분석	• IaaS • Private Cloud(Community Cloud)
	Compliance 분석	• 클라우드 컴퓨팅 구축/제공/이용 등에 따른 법적 준거성(전자금융감독규정, 개인정보보호법 등)검토 및 분석
	관리체계 진단	• 클라우드컴퓨팅 서비스 정보보호에 관한 기준 고시 기준(관리적/물리적/기술적 조치) 및 ISMS 기준 현황 분석
	기술취약점 진단	• Hypervisor(ESXi, KVM), DBMS • Portal Web 취약점 진단
	보호대책	• 위험 평가 및 관리적/물리적/기술적 보호 대책 • 클라우드 서비스 운영보안 지침 수립
성과		• ISO27017 인증 획득

5.2. SaaS/Public Cloud 정보보호 컨설팅 프로젝트

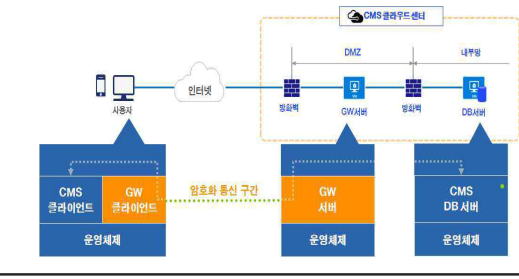
KISA 주관의 클라우드 실증사업자(SaaS/SecaaS) 대상으로 보안 컨설팅 및 검증을 수행하여 클라우드 보안 위험 분석 및 보호대책을 수립함

KISA 클라우드 실증 사업 프로젝트(SaaS/ Public)

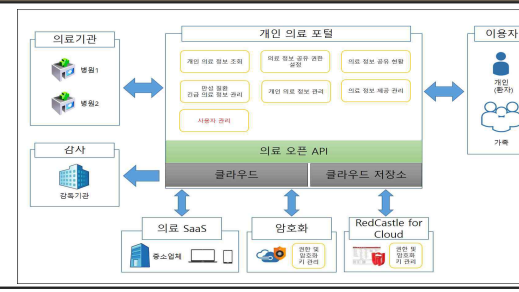
개인정보뱅크 목표 시스템



클라우드 CMR 목표시스템



클라우드 의료정보포탈 목표시스템



대상	• CRM / 의료 / 개인정보뱅크 클라우드 실증 사업자 • 관제 / 클라우드 스팸 차단의 보안클라우드 실증 사업자
특징	• SaaS를 고려한 통제기준이 존재하지 않아 컴플라이언스 분석을 통한 통제기준 수립/사업자점검/보호방안 제시
수행절차 – 클라우드 모델 분석	• SaaS / SecaaS • Public Cloud
수행절차 – Compliance 분석	• ISO 27017 / ISMS • Cloud Security Alience version 3.0 • 클라우드컴퓨팅 정보보호에 관한 기준
수행절차 – 관리체계 진단	• 클라우드 정보보호 고시를 기준으로 국제표준 참고 • SaaS 사업자가 준수해야 할 항목과 IaaS 사업자에게 요구해야 할 사항에 대해 구분하여 진단
수행절차 – 기술취약점 진단	• SaaS 실증 사업자 모의해킹 • SeCaaS 실증 사업자 시스템 진단
수행절차 – 보호대책	• 위험 평가 및 관리적/물리적/기술적 보호 대책 • SaaS 사업자 표준 보안지침 수립
성과	• Software as a Service 사업자에 대한 통제기준 수립 • 클라우드 서비스 보호 대책 제시

Contents

6.1. 클라우드 규제 개선 관련 전자금융감독규정 개정

클라우드 규제 개선 관련 전자금융 감독규정 개정내용으로 비중요 정보처리시스템을 지정하여 클라우드 이용 근거가 생김

- **클라우드 규제 개선 관련 전자금융 감독규정 개정(2016.10.05 시행) 내용 및 클라우드 예외 조항**

제14조의2(비중요 정보처리시스템 지정)

① 금융회사 또는 전자금융업자는 자체적으로 수립한 정보자산 중요도 평가기준에 따라 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정할 수 있다. 다만, 개인의 고유식별정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다.

② 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템 지정시 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원장이 정하는 양식에 따라 정보자산 중요도 평가기준, 지정 결과, 관리 방안 등을 포함한 보고서를 금융감독원에 제출하여야 한다.

④ 금융감독원장은 제3항에 따라 제출한 보고서를 검토한 결과, 평가 기준, 지정 결과, 관리 방안 등이 적합하지 않다고 판단되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

⑤ 제1항의 비중요 정보처리시스템만 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다.

제11조(전산실 등에 관한 사항)

11. 국내에 본점을 둔 금융기관의 전산실 및 재해복구 센터는 국내에 설치할 것
12. 무선통신망을 설치하지 아니할 것

제15조(해킹 등 방지대책)

①-5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것

②-4. 정보보호시스템 원격관리를 금지할 것. 다만, 원격관리가 불가피한 경우 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다) 사용,접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것

②-5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것

제60조(외부주문등에 대한 기준)

①-5. 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용

6.2. 금융권 클라우드 서비스 이용 가이드

금융권 클라우드서비스 이용 가이드는 금융회사가 클라우드 서비스 이용 시 준해해야 할 사항을 클라우드 이용 대상 지정·도입·이용·관리·사후관리 단계 별로 설명함

- **금융보안원 '금융권 클라우드서비스 이용 가이드'(2016.10 발간)**

적용 목적	• 금융회사 및 전자금융업자가 클라우드컴퓨팅서비스 이용 시 준수해야 할 사항을 권고함으로써 금융이용자 보호 및 금융시스템 안전성을 유지·강화
적용 대상	• 클라우드컴퓨팅서비스를 이용하는 금융회사 및 전자금융업자
클라우드 서비스	• "클라우드컴퓨팅서비스"라 함은 전산설비를 직접 구축하지 않고, 제3의 전문업체로부터 인터넷을 통해 필요한 IT자원을 탄력적으로 제공받아 사용하는 컴퓨팅 환경을 말함
구성	• 클라우드 이용 대상(비중요정보처리시스템) 지정·절차, 클라우드 도입, 클라우드 이용, 클라우드 관리, 사후 관리 과정 단계에서 참고해야 할 가이드(기술적, 관리적 보호 대책 등) 제공

클라우드 이용 대상

- 비중요정보처리 시스템 지정 기준
- 비중요정보처리 시스템 지정 절차

클라우드 도입

- 클라우드 제공자 선정시 고려사항
- 클라우드 제공자와 계약
- 이전 및 전환 계획 수립

클라우드 이용

- 클라우드 이용 시 보호대책
- 금융회사 내부 시스템과의 연계

클라우드 관리

- 서비스 수준 관리 (SLA)
- 클라우드 자산 관리
- 재해복구 및 침해 사고대응 관리

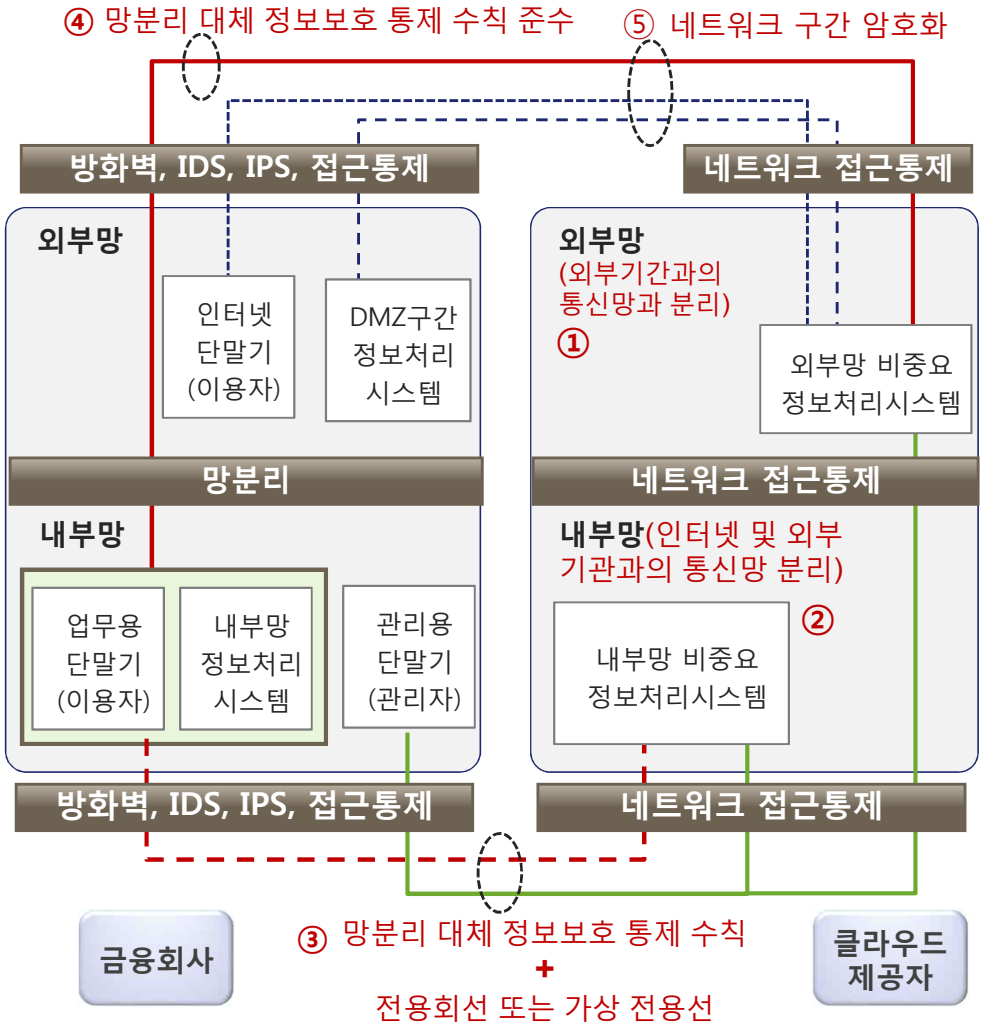
사후 관리

- 클라우드의 전환
- 클라우드 사용 종료

6.3. 금융권 클라우드 정보보호 컨설팅 서비스

금융권 클라우드를 대상으로 안랩 클라우드 서비스 수행 방법론을 적용하여 클라우드 모델·유형 별 보안 위험을 분석하고 대책을 수립함

금융권 클라우드 정보보호 컨설팅 프로젝트 수행 전략



수행 단계	수행 내용
클라우드 환경 분석	• 비중요정보시스템 식별 및 평가 • 클라우드 모델 분석(Hybrid Cloud, IaaS/PaaS/SaaS 등)
Compliance 분석	• 「전자금융감독규정」의 안전성 확보 의무 • 「개인정보보호법」의 안전성 확보조치 • 「신용정보감독규정」의 기술적·관리적 보호대책 등
관리적 취약점 분석	• 금융보안원의 「금융권 클라우드 서비스 이용 가이드」 • ISO27017, ISO27018, CMM 등 클라우드 보안요구사항 도출 및 평가
기술적 취약점 분석	• 금융회사 내부시스템과 클라우드 연계간 암호화, 접근통제 적용 등 보안성 검증 • 클라우드 자산(Guest OS, 웹 서비스 등) 취약점 진단
위험평가	• 클라우드 보안 위험 식별 및 평가 • 위험조치 계획 수립
보호대책 수립 및 구현	• 클라우드 운영 보안 정책·지침·절차 수립 • 클라우드 보안 대책 수립 • 클라우드 보안 매니지드 서비스(클라우드 보안관제 등)

thank you.