디지털뉴딜 한국판뉴딜

동향 보고

국내·외 클라우드 서비스 보안 인증제 동향 및 국내 CSAP 인증 개선 방안

2021. 12.

■ 발 행 처: 한국지능정보사회진흥원

■ 발 행 인: 문용식

■ 작　　성: 한국지능정보사회진흥원 지능형인프라본부

-클라우드기획팀 정혜연 연구원

■ 기획·자문: 송재일 수석

비매품/무료

95000

9 788984 836488

ISBN 978-89-8483-648-8 (PDF)

목 차

Ⅰ. 국내·외 클라우드 서비스 보안 인증제 현황

1. 글로벌 동향

국가	인증	인증 기준	인증 기관
미국	FedRAMP	NIST SP800-53	FedRAMP PMO
유럽연합 (EU)	EUCS	ISO/IEC 27001, 27002, 27017 등	ENISA
일본	ISMAP	JIS Q 27001, 27002, NIST SP800-53	ISMAP 운영위원회
싱가포르	MTCS	ISO/IEC 27001	ITSC (정보기술표준위원회)
호주	IRAP	NIST SP800-37 R2	ACSC (호주사이버보안센터)
국제표준	CSA STAR	ISO/IEC 27001 + CCM (Cloud Control Matrix)	BSI(영국표준협회)와 CSA(미국클라우드 시큐리티얼라이언스)

FedRAMP(Federal Risk and Authorization Management Program)

- ㅇ 클라우드 제품 및 서비스를 위한 보안평가, 인증 및 지속적인 모니터링을 표준화한 정부 프로그램
- ㅇ 클라우드에 특화된 보안 통제항목을 제시하여 신뢰성을 높이고, 외부 전문 평가 대행기관을 선정하여 일관성 있는 보안평가 수행
- ㅇ 美 전자정부법인 FISMA에서 발간한 가이드라인 NIST SP800-53를 기준으로 하는 17개 분야 325개의 보안 통제항목으로 구성

분야	통제항목 수
1. Access Control	43
2. Awareness and Training	5
3. Audit and Accountability	19
4. Assessment and Authorization	15
5. Configuration Management	26

6. Contingency Planning	24
7. Identification and Authentication	27
8. Incident Response	18
9. Maintenance	11
10. Media Protection	10
11. Physical and Environment Protection	20
12. Planning	6
13. Personnel Security	9
14. Risk Assessment	10
15. System and Services Acquisition	22
16. System and Communication Protection	32
17. System and Information Integrity	28
계	325

EUCS(EU Cybersecurity Scheme for Cloud Services)

○ 유럽연합(EU) 회원국 전체에 적용되는 인증으로 인프라에서 애플리케이션까지 이르는 전 종류의 클라우드 서비스에 적용[1)]

○ '기본', '실질적', '높음' 세 가지의 보증 수준을 제공[2)]

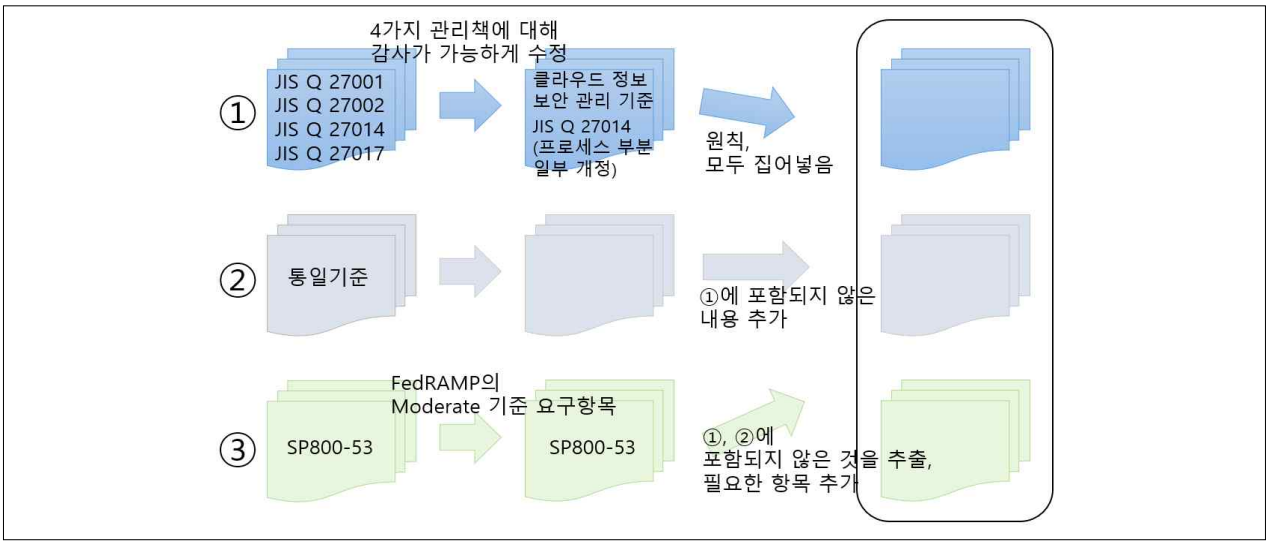
기본(basic) 수준	실질적(substantial) 수준	높음(high) 수준
알려진 사이버 공격 위험 최소화 (저위험 프로파일)	알려진 사이버 공격 위험, 제한된 기술과 자원을 가진 행위자에 의한 사이버 공격 위험 최소화 (중간 위험 프로파일)	상당한 기술과 자원을 가진 행위자에 의한 최첨단 사이버 공격 위험 최소화 (위험 프로파일)
-제한된 보증 -제 3자에 의한 자체 평가 검토 -절차 및 메커니즘의 정의와 존재에 대한 설명	-합리적 보장 -설계 및 작동 효과 -기능 시험	-합리적 보장 -설계 및 작동 효과 -규정 준수 여부를 지속적 모니터링

ISMAP(Information System Security Management and Assessment Program)

○ 日 총무성·내각관방·경제산업성이 2020년 6월 3일 발표한 클라우드

서비스 보안 인증 프레임워크

○ JIS Q 27001, 27002, 27017과 NIST SP800-53을 인증 기준으로 채택[3)]



MTCS(Multi-Tier Cloud Security)

○ 싱가포르 인포콤 당국(IPA)의 정보기술표준위원회(ITSC)에서 시행하는 클라우드 보안 인증제로 여러 계층의 클라우드 보안을 포괄

○ ISO/IEC 27001 국제표준을 기반으로 하며 데이터 보존, 데이터 주권, 데이터 이식성, 책임, 가용성, 비즈니스 연속성, 재해 복구 및 사고 관리 영역 등의 규정 존재[4)]

○ 클라우드 서비스의 성격에 따라 레벨 1, 2, 3의 3가지로 인증 등급 구분

분야	통제항목
Cloud Governance	Information security management, Human resources, Risk management, Third party, Legal and compliance, Incident management, Data governance
Cloud infrastructure security	Audit logging and monitoring, Secure configuration, Encryption, Security testing and monitoring, System acquisitions and development
Cloud operations management	Physical and environmental, Operations, Change management, Business continuity planning (BCP) and disaster recovery (DR)
Cloud services administration	Cloud services administration
Cloud user access	Cloud user access

Tenancy and customer isolation	Tenancy and customer isolation

통제항목 수		
Level 1	Level 2	Level 3
296	449	535

5)

IRAP

ㅇ 호주의 기존 클라우드 서비스 보안 인증 프로그램인 ASD CCSL이 2020년 7월 27일 시행 중단된 후 호주 사이버 보안 센터(ACSC)가 디지털 혁신 에이전시(DTA)와 손잡고 새롭게 발표한 클라우드 보안 지침

IRAP 클라우드 서비스 평가 기준	
1. Description	
2. Cloud service locality	
3. Cloud service shared responsibility model	
4. Cloud service architecture diagram	components and dependencies
	inbound and outbound interfaces
5. Protection of data at rest	
6. Data backup and restore	
7. Data portability	
8. Tenancy segmentation and segregation	
9. Cloud service security visibility	
10. Security baseline	
11. Deviations from baseline	
12. Customer responsibilities & implementation guidance	

2. 국내 동향

CSAP(Cloud Service Assurance Program)

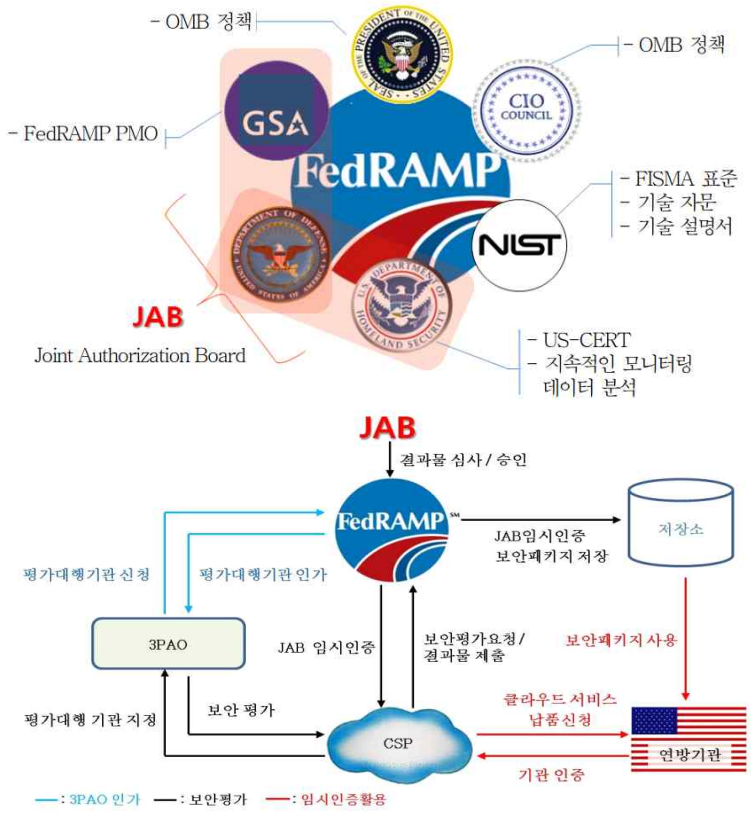
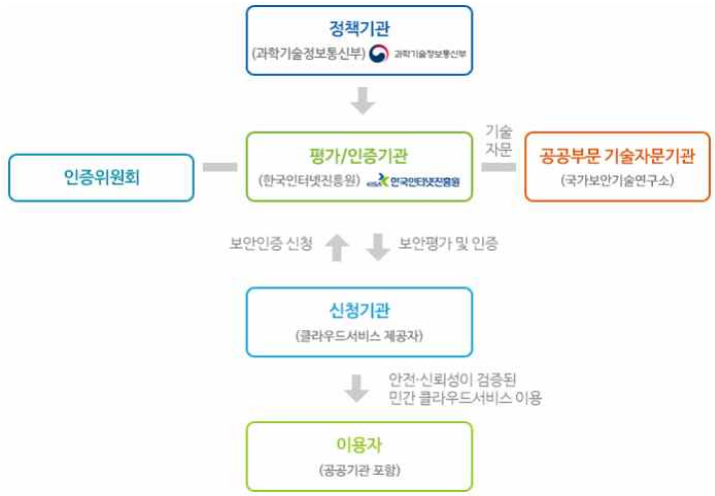
- ㅇ 공공기관에 안정성 및 신뢰성이 검증된 민간 클라우드 서비스를 공급하기 위해 한국인터넷진흥원(KISA)에서 주관하는 클라우드 서비스 보안 인증 제도
- ㅇ ISO/IEC 27001과 가상화 보안, 서비스 공급망 관리, 공공기관 요구사항 등의 규정을 기반으로 한 14개 분야 30-117개 항목으로 구성
- ㅇ 클라우드 서비스의 형태에 따라 IaaS, SaaS, DaaS 등으로 분류

분야	통제항목 수			
	IaaS	SaaS 표준	SaaS 간편	DaaS
1. 정보보호 정책 및 조직	5	5	2	5
2. 인적보안	12	4	1	7
3. 자산관리	10	3	-	10
4. 서비스 공급망 관리	4	3	-	4
5. 침해사고 관리	7	7	2	7
6. 서비스 연속성 관리	7	6	2	7
7. 준거성	4	3	1	4
8. 물리적 보안	12	-	-	12
9. 가상화 보안	10	6	1	7
10. 접근통제	10	10	5	10
11. 네트워크 보안	6	5	2	6
12. 데이터 보호 및 암호화	10	8	4	10
13. 시스템 개발 및 도입 보안	12	10	2	12
14. 공공부문 추가 보안요구 사항	8	7	7	8
계	117	78	30	110

Ⅱ. 美 FedRAMP와 국내 클라우드 서비스 보안 인증(CSAP) 비교

1. 표

<table>
<tr><th>구분</th><th colspan="3">美 FedRAMP</th><th colspan="2">韓 CSAP</th></tr>
<tr><td>인증 항목 개수</td><td colspan="3">17개 분야 325개 항목*
(*중(Moderate) 등급기준)</td><td colspan="2">14개 분야 117개 항목
(IaaS 기준)</td></tr>
<tr><td>등급 분류</td><td colspan="3">클라우드 서비스의
중요도와 민감도에 따라
상(High), 중(Moderate), 하(Low)
세 단계로 구분</td><td colspan="2">SaaS에 한해
표준, 간편 두 단계로 구분</td></tr>
<tr><td rowspan="8">인증 참여 기관</td><td>인증</td><td colspan="2">FedRAMP PMO</td><td rowspan="6">인증,
평가</td><td rowspan="6">한국인터넷진흥원
(KISA)</td></tr>
<tr><td>평가</td><td colspan="2">공인 3PAO</td></tr>
<tr><td rowspan="5">기타</td><td>OMB</td><td>FedRAMP
부처간
활동 조정</td></tr>
<tr><td>JAB</td><td>보안 승인</td></tr>
<tr><td>NIST</td><td>기술 표준
확립</td></tr>
<tr><td>DHS</td><td>사이버
침해 대응</td></tr>
<tr><td>CIO
Council</td><td>연방정부
클라우드 컴퓨팅
이행 촉진</td><td>정책
기관</td><td>과학기술정보통신부</td></tr>
<tr><td>Federal
Agencies</td><td>클라우드
기술 도입</td><td>기술
자문</td><td>국가보안기술연구소</td></tr>
<tr><td>지속적 모니터링
여부</td><td colspan="3">각 항목의 성격에 맞게
연속 및 지속, 분기별, 매년, 격년,
매3년, 매5년 등으로 주기를
나누어 58개의 항목 평가*</td><td colspan="2">최초평가와 갱신평가 사이의
인증 유효기간(3~5년) 동안
총 4회(매년 1회 이상)의
사후평가 시행</td></tr>
</table>

구분	美 FedRAMP	韓 CSAP
인증 구조	 6) 유기적, 순환적	 7) 직선적, 계층적

* <표> FedRAMP 각 항목별 인증 주기

인증 항목	주기
Information System Monitoring, Auditable Events, Information System Component Inventory, Incident Reporting 등 7개 항목	연속 및 지속 (Continuous and Ongoing)
Contingency Training	매 10일(10 days)
Audit Review, Analysis & Reporting	매주(Weekly)
Vulnerability Scanning, Continuous Monitoring Security State 등 12개 항목	매달(Monthly)
Authenticator Management	격월(60 days)
Account Management, Identifier Management 등 4개 항목	분기별(90 Days)
Information Security Policies, Security Training 등 26개 항목	매년(Annually)
Identifier Management	격년(Every 2 years)
Security Authorization, IT Contingency Plan Testing & Exercises 등 4개 항목	매 3년(Every 3 years)
Personnel Screening	매 5년(Every 5 years)

Ⅲ. 국내 클라우드 서비스 보안 인증제도(CSAP)의 개선필요점

□ CSAP 평가항목 수는 IaaS 기준 14개 분야 117개 항목으로 美 FedRAMP 평가항목 수(17개 분야 325개 항목, 중(Moderate) 등급기준)의 1/3 수준

○ 가장 낮은 등급의 인증 항목끼리 비교할 경우 4배 이상 차이

	美 FedRAMP	韓 CSAP
등급체계	상(High) 중(Moderate) 하(Low)	(SaaS 인증에 한하여) 표준등급 간편등급
가장 낮은 등급	하(Low)	(SaaS 인증에 한하여) 간편등급
가장 낮은 등급 평가항목 수	17개 분야 125개 항목	12개 분야 30개 항목

□ 클라우드 서비스의 중요도와 민감도에 따른 인증제도 등급 다양성이 부족함

○ 각 공공부문마다 필요로 하는 보안 수준이 다름에도 불구하고 최대

두 가지 등급으로 차등을 두어 서비스 적절성 측면에서 개선 필요

□ 인증심사 요청 시 공식 심사기간(17~25일)보다 훨씬 더 긴(5~6개월) 시간이 소요되기도 하여 기업에 부담[8)]

ㅇ 또한 인증심사 기간에 서비스 기능 고도화, 업데이트 등의 변경이 쉽지 않아 인증 획득 후 추가심사를 요청해야 하므로 심사기간이 더 길어질 수 있음

□ 인증 획득 후 지속적 모니터링 단계에서 매년 1~2회 단위의 사후평가를 진행

□ 한국인터넷진흥원(KISA) 단일 인증·평가 체계로 인증의 전문성과 완결성에 보완이 필요

ㅇ 한국인터넷진흥원의 예산 및 조직이슈에 크게 의존하여 안정성이 떨어짐

ㅇ 추후 인증심사 요청이 늘어날 경우 인증 적체가 일어나 국내 클라우드 산업의 성장을 저해할 수 있음

Ⅳ. 국내 클라우드 서비스 보안 인증제도(CSAP)의 개선방안

□ CSAP의 문턱을 낮추고 각 기관에 적절한 서비스가 제공될 수 있도록 클라우드 서비스의 중요도와 민감도에 따른 다양한 인증 등급 마련

□ 美 FedRAMP를 벤치마킹하여 전 등급 보안 심사항목 강화

□ 클라우드 서비스의 프로세스 외에 실 제품의 평가에도 비중을 두어 인증의 실효성을 높임

□ 앞으로 늘어날 공공부문 클라우드 수요에 대응하기 위해 한국인터넷진흥원(KISA) 이외의 정부 부처를 유기적으로 연결하여 고도화된 인증 시스템 마련

ㅇ 각 부처에 역할을 분담하여 구조적 안전성 확보

ㅇ 한국인터넷진흥원(KISA)에 대한 의존성 낮춰 인증 신뢰성 확보

□ 지속적 모니터링 시 보안 항목별 가중치를 달리하여 각 항목에 맞는 모니터링 주기로 사후평가 개편

참고 CSA STAR (CSA Security, Trust & Assurance Registry)

□ **(개념)** 영국표준협회(BSI)와 미국 클라우드 시큐리티 얼라이언스(CSA)가 공동으로 평가하는 클라우드 보안 인증 심사

○ 클라우드 서비스 제공자(CSP)가 ISO/IEC 27001와 CCM(Cloud Control Matrix) v3.01의 요구사항을 준수하고 STAR 능력 성숙도 모델을 만족하는지 평가함[9]

□ **(등급)** Level 1, 2, 3의 세 단계로 구분되며 인증 등급 개수는 5개

	인증 종류	인증 이름	
Level 3	Continuous Monitoring-Based Certification	STAR CONTINUOUS	
Level 2	Third-Party Assessment-Based Certification	STAR CERTIFICATION	STAR ATTESTATION
Level 1	Self-Assessment	STAR SELF-ASSESSMENT	CONTINUOUS SELF-ASSESSMENT

※ 중화권 시장용 C-STAR도 Level 2에 속함

○ STAR Continuous: 지속적 모니터링

○ STAR Certification: 공인된 제 3자에게 보안 평가 통과

○ STAR Attestation: AICPA Trust Service Criteria와 CSA CCM을 사용해 수행된 SOC 2 결과를 등록하여 획득

○ STAR Self-Assessment: 클라우드 서비스 제공자가 완료한 CAIQ(Consensus Assessment Initiative Questionnaire) 결과를 등록하여 획득

○ Continuous STAR Self-Assessment: 지속적 자체평가

Ⅵ. 참고 문헌

1) ENISA PRESS RELEASE - cloud certification scheme : Building Trusted Cloud Services Across Europe
2) MEDINA - Paving the Road Towards Continuous Certification: OSCAL and the EUCS 6p.
3) (아래그림) ISMAP : 정부정보시스템 보안평가제도(ISMAP) (내각사무국, 산업통상자원부) 21p.
4) Microsoft Docs Documentation : Singapore MTCS
5) NAVER CLOUD PLATFORM 정보보호 인증 : MTCS
6) itfind IT기획시리즈 美 연방정부 클라우드 서비스 보안인증제도 (FedRAMP) 분석
7) KISA - 클라우드보안인증제(CSAP) 제도 소개
8) 아주경제 "클라우드 발전 저해 우려"…인기협, 양정숙 의원 법안에 신중론
9) NAVER CLOUD PLATFORM 정보보호 인증 : CSA STAR