KISA 한국인터넷진흥원

클라우드 보안 인증제 확대 (IaaS→IaaS·SaaS) 추진

2018. 6. 28
라영선 책임연구원
(rays@kisa.or.kr)

Contents

KISA 한국인터넷진흥원

목적

클라우드 보안 인증제의 인증 범위를 기존 **IaaS에서 SaaS까지 확대**하여 공공기관의 클라우드 이용 확산 및 클라우드 산업 활성화 추진

추진경과

▶ 공공기관의 민간(상용) 클라우드 이용이 가능하도록 '국가·공공기관 클라우드컴퓨팅 보안 가이드라인' 개정('16.5)

(개정 前) 민간(상용) 클라우드 서비스 이용 불가 -> (개정 後) 이용 가능

※ 공공기관은 민간 클라우드를 도입하고자 하는 경우 과기정통부로부터 클라우드 보안인증제에 따라 인증된 클라우드 서비스를 도입하여야 한다.

▶ 과기정통부의 클라우드 보안인증제 시행(IaaS, '16.7)

* 국내 IaaS 중심의 클라우드 시장현황(이용고객 비중: IaaS 41.6%, SaaS 29.7%)을 고려하여 IaaS 클라우드 보안인증제 우선 도입

* KT, NBP, 가비아, NHN엔터테인먼트, LG CNS 등 5개 기관이 인증 획득

▶ 민간 클라우드 산업 활성화를 위해 공공기관이 이용 가능한 클라우드 서비스를 SaaS까지 확대 추진('18년)

- '국가. 공공기관 클라우드 컴퓨팅 보안 가이드라인' 개정
- '클라우드 보안인증제'에 SaaS 인증기준, 평가방법 마련

추진방향 - 인증기준

▶ **(SaaS 인증기준)** 유관기관(과기정통부·국보연·KISA) 상호 검토 및 논의를 통해 SaaS 인증 기준을 도출

- 기존 **IaaS 대비 통제항목이 감소(117개 -> 78개)**됨에 따라 IaaS 인증보다 신속하게 인증(IaaS, 4개월 → SaaS 3개월*) 가능

* 물리적 보안을 제외한 SaaS 항목에 대해 약 3개월의 기간이 소요 예상

< IaaS·SaaS 인증기준 >

유형	세부 유형	통제 항목	
		IaaS	SaaS
관리적 보호조치	• 정보보호 정책, 인적 보안, 침해사고 관리, 준거성 등	49	32
물리적 보호조치	• 물리적 보안	12	-
기술적 보호조치	• 가상화 보안, 접근 통제, 네트워크 보안, 데이터 보호 등	48	39
공공기관용 추가 보호조치	• 공공부문 추가 보안요구 사항	8	7
계		117	78

※ 제도 초기임을 감안 정부지원책의 일환으로 클라우드보안인증평가 수수료는 무료로 시행중(한시적)

[참고] IaaS 대비 제외 항목

SaaS 보안인증 평가에서 제외되는 기준(통제항목)

2.1.5. 상벌규정
2.1.6. 퇴직 및 직무변경
2.2.1. 외부인력 계약
2.2.2. 외부인력 보안 이행 관리
2.2.3. 계약 만료 시 보안
2.3.1. 교육 프로그램 수립
2.3.3. 평가 및 개선
3.1.2. 자산별 책임할당
3.1.3. 보안등급 및 취급
3.2.2. 변경 탐지 및 모니터링
3.2.3. 변경 후 작업검증
3.3.1. 위험관리계획 수립
3.3.3. 위험분석 및 평가
3.3.4. 위험처리
4.2.2. 공급망 모니터링 및 검토
6.2.3. 서비스 연속성 점검
7.1.2. 정보보호 정책 준수
8.1.1. 물리적 보호구역 지정
8.1.2. 물리적 출입통제
8.1.3. 물리적 보호구역 내 작업
8.1.4. 사무실 및 설비 공간 보호
8.1.5. 공공장소 및 운송 · 하역구역 보호
8.1.6. 모바일 기기 반출 · 입
8.2.1. 정보처리시설의 배치
8.2.2. 보호설비
8.2.3. 케이블 보호
8.2.4. 시설 및 장비 유지보수
8.2.5. 장비 반출 · 입
8.2.6. 장비 폐기 및 재사용
9.1.2. 가상자원 회수,
9.1.3. 가상자원 회수
9.1.4. 하이퍼바이저 보안
9.1.6. 상호 운용성 및 이식성
11.1.6. 무선 접근통제
12.2.1. 저장매체 관리
12.2.2. 이동매체 관리
13.4.1. 시스템 보입 계획
13.4.2. 시스템 인수
14.3.2. 보안관제 제반환경 지원

추진방향 – 인증 원칙 및 SaaS 유형

▶ **(SaaS인증원칙)** 인증된 IaaS에서 구축되는 SaaS를 인증, Private, Hybrid 전용 클라우드 제외, 인증기준(취약점 점검 불가 등)에 미달하는 SaaS 제외

* 인증받지 않은 IaaS를 포함하여 IaaS, SaaS 영역을 한꺼번에 인증 평가 진행 가능

- 전자결제, 인사관리 등 내부 업무망에서만 이용가능한 SaaS는 제외
- 그 외 취약점 점검 불가, 데이터 해외 저장 등 평가가 불가능한 클라우드 서비스(IaaS/ SaaS) 제외

추진방향 - SaaS 유형 예시(1/2)

SaaS 유형	설 명
IT관리	클라우드 자원 생성, 삭제 등 운영현황을 가시적으로 파악할 수 있는 서비스 예시) 서비스 장애관리, 시스템 상태 모니터링 등
고객관계관리(CRM)	고객과 잠재고객에 대한 데이터를 수집·분석하여 제공하는 클라우드 기반 고객관계관리 서비스 예시) 방문객 출입관리, 민원처리 등
교육	클라우드컴퓨팅을 활용한 교육환경(e-러닝 등) 서비스 예시) 수강신청, 온라인 비디오, SW 교육, 도서관리, 교육관리 등
데이터관리	클라우드 환경 내 데이터를 저장하고 관리하는 서비스 예시) 데이터 소산백업, 팩스문서관리, 문서 관리 등
마케팅	클라우드컴퓨팅을 활용하여 고객에 맞는 콘텐츠를 제공하는 서비스 예시) 빅데이터 분석, 온라인설문(실태)조사, 각종소식 안내 등

추진방향 - SaaS 유형 예시(2/2)

KISA

SaaS 유형	설 명
문화	클라우드 환경에서 다양한 미디어 콘텐츠를 제공하는 서비스 예시) 스트리밍 서비스, 도서 정보서비스, 공공문화정보 서비스
보안 (SecaaS)	클라우드 환경에서 또는 클라우드컴퓨팅을 활용해 전문화된 보안기능을 제공하는 온디멘드 서비스(SecaaS : Security as a Service) 예시) 웹방화벽/웹게이트웨이, VPN, 데이터 암호화, 메일보안 등
의사결정지원/분석	클라우드 환경에서 여러 사용자가 동시에 프로젝트를 수행하도록 작업환경 및 업무보조 도구를 제공하는 서비스 예시) 커뮤니케이션, 영상회의, 캘린더(일정관리), 메신저, 문서 작성 프로그램 등
협업도구	

추진방향 – 단계적 확대

▶ SaaS 인증의 단계적 확대

- 인터넷망(**외부망**)을 통해 이용 가능한 SaaS 유형 우선 도입* 추진

※ 국가 공공기관 보안지침(망분리 규정)에 따라 업무망 SaaS 이용은 단계적으로 검토 후 사용

- 공공기관과 민간 클라우드 사업자의 수요조사 등을 통해 유관기관과 지속 협의

※ 인증 가능한 SaaS 목록은 KISA(홈페이지)를 통해 관리

- 인증신청한 SaaS가 **신규 서비스인 경우** 유관기관(과기정통부, 국보연, KISA)과 함께 **기능·보안관점에서 적절성 검토**

※ 이후 동일 유형의 서비스는 검토 생략

추진방향 - SecaaS 평가

▶어플라이언스 보안장비(설치형 SW 포함)를 제외하고 관리형서비스를 SecaaS로 규정하고 **SaaS 인증 대상에 포함**

* CC인증, GS인증, 성능평가 등 타 인증제 결과 기반의 SaaS 보안인증 수행

▶ **(SecaaS 인증방식)** 구축된 SecaaS의 인프라 연동부는 파일 단위(소스코드)로 구분이 가능하므로,

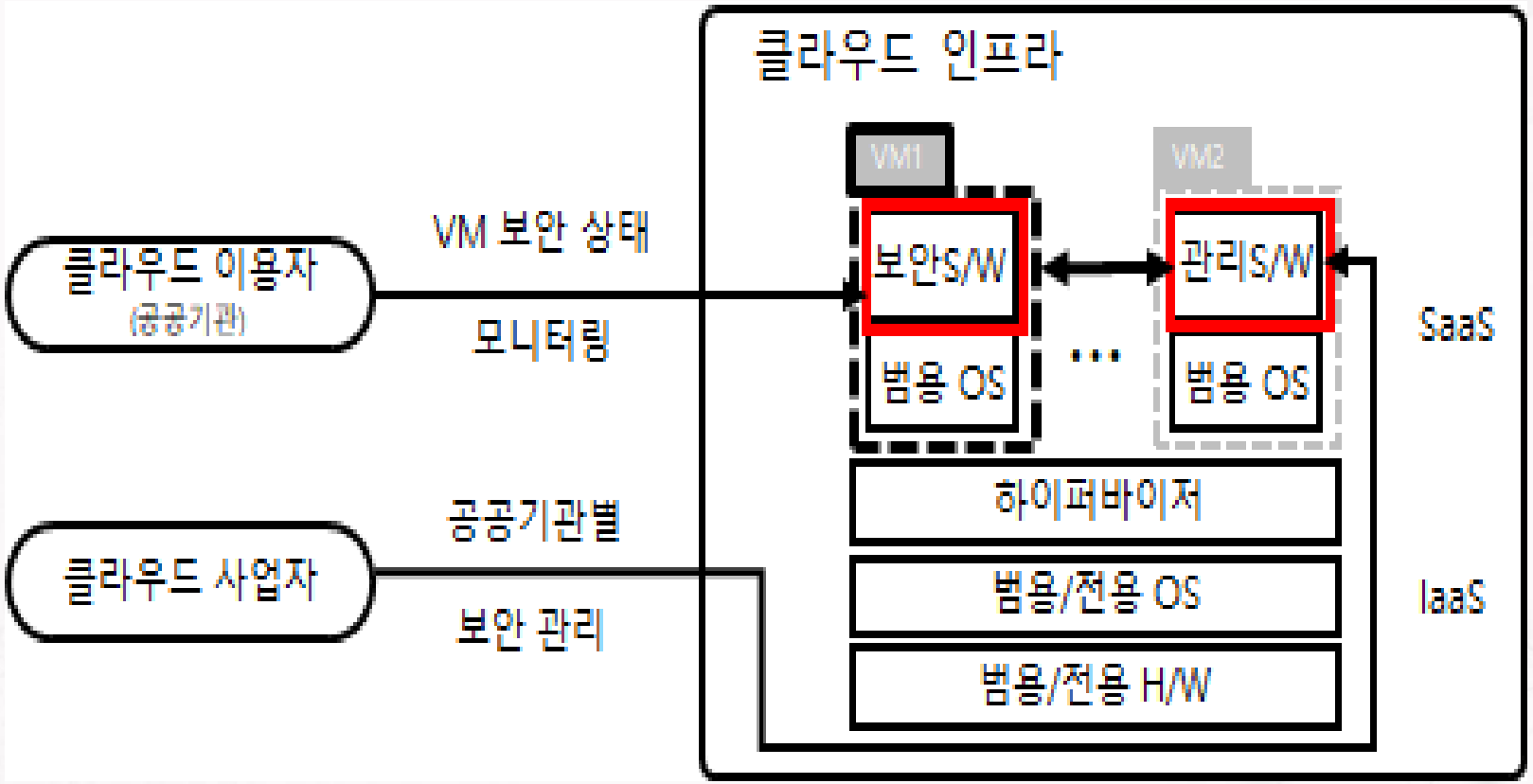
- 보안기능의 검증은 타 인증제(CC인증, GS인증, 성능평가 등) 평가로 대체하고, SaaS 인증에서는 인프라 연동 등에 대한 보안영향만을 평가

▶ **(SecaaS 인증이슈)** 동일서비스라도, 구축되는 IaaS마다 인프라 연동을 위한 형상변경(사업자별로 API 등이 다름)이 존재함

※ IaaS 사업자별로 별도 SaaS 평가인증이 필요하며, 1개 사업자가 다수의 인증서 보유 가능

추진방향 – SecaaS 평가

▶ 관리형 보안 서비스(SecaaS) : SaaS 인증 대상에 해당함

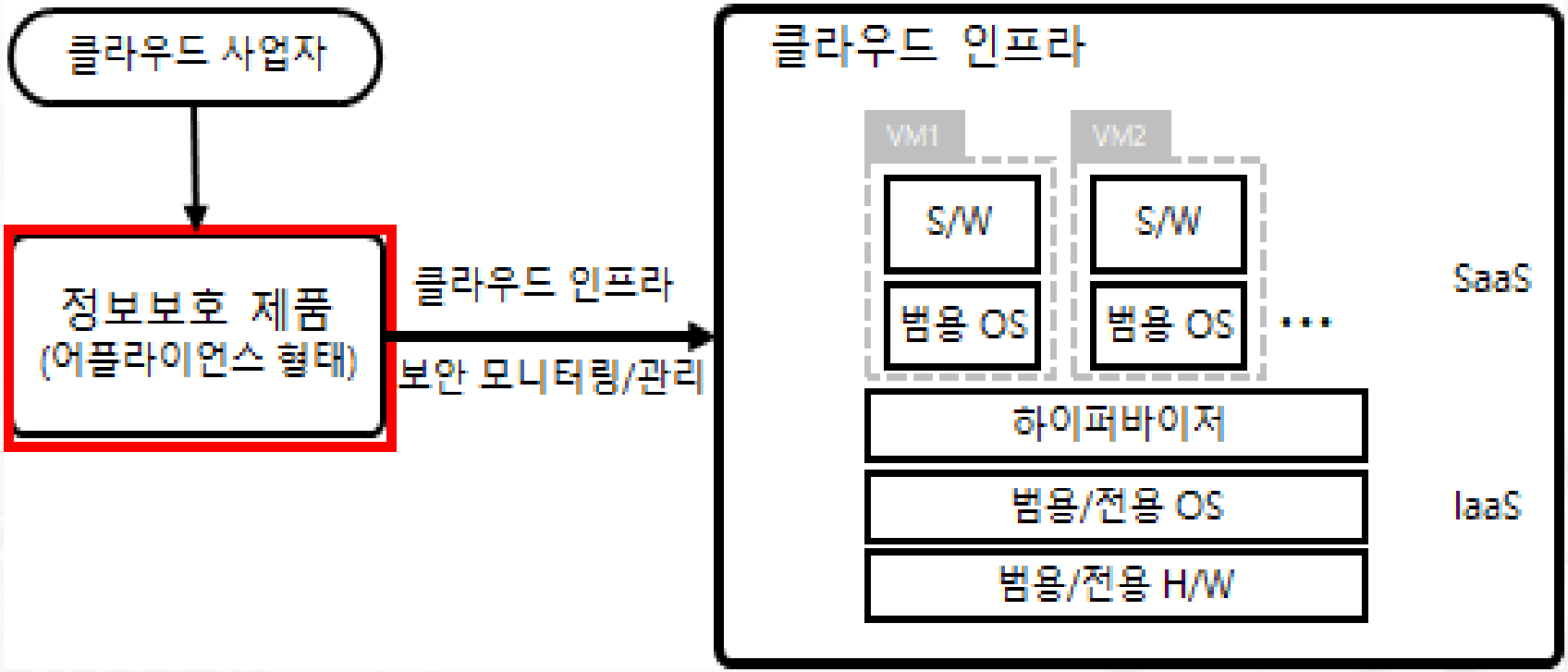


o 사업자는 보안 S/W 배포사이트 운영 및 패치 관리, 이용자별 보안적용 및 모니터링/관리

o 이용자는 서비스 신청 후 모니터링/리포팅

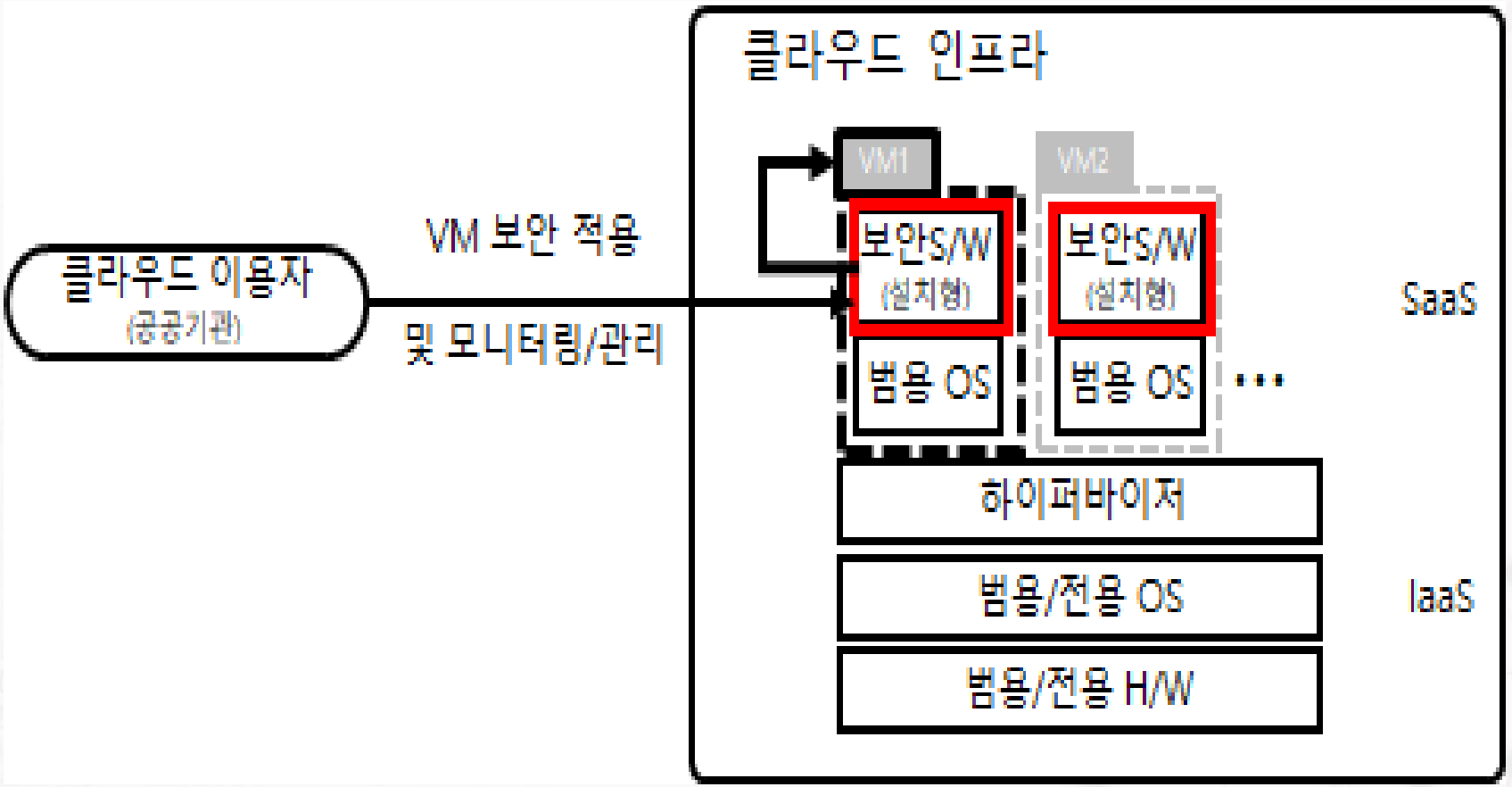
[참고] 미인증 대상 – HW Appliance

▶ HW기반 어플라이언스 : SaaS 인증 대상에 해당하지 않음



[참고] 미인증 대상 – 단순 설치형 SW

▶ 설치형 SW 보안서비스 : SaaS 인증 대상에 해당하지 않음



추진방향 – SecaaS 형상관리

KISA

▶ 형상변경 관리방안

- 인프라(IaaS) 및 사용자 연동을 위한 변경(API, Config 파일, 보안관리 및 감사 관련 파일, 유저 인터페이스 등)은 다수 존재할 것으로 예상

  ※ KISA, SaaS 보안인증제도에서 안정성을 평가

- CC인증제품의 클라우드 환경(SecaaS) 최초구축 시, **보안 기능의 형상은 변화가 없을 것으로 예상(보안기능은 타인증제(CC, GS, 성능평가 등) 평가로 대체)**

  1) 변화가 없을 경우, 이를 증명하기 위해, 보안 기능에 대한 **해쉬값, 파일 비교, 현장실사** 등을 실시

  2) 변화가 발생한 경우, 사업자가 제출한 **보안기능변경 영향분석서 검토와 신뢰성 확보를 위한 서약서 징구**

- 최초구축 이후 발생되는 형상관리는 KISA에서 해쉬값 저장 및 이력 관리

평가기준(1/14)

구분		IaaS	SaaS	비고
1. 정보보호 정책 및 조직	1.1 정보보호정책	‣정보보호 정책 수립, 정보보호 정책 검토 및 변경, 정보보호 정책문서 관리	‣정보보호 정책 수립, 정보보호 정책 검토 및 변경, 정보보호 정책문서 관리	동일
	1.2 정보보호조직	‣조직 구성, 역할 및 책임 부여	‣조직 구성, 역할 및 책임 부여	동일

평가기준(2/14)

구분		IaaS	SaaS	비고
2. 인적보안	2.1 내부인력보안	‣고용계약, 주요 직무자 지정 및 감독, 직무 분리, 비밀유지서약서, 상벌규정, 퇴직 및 직무변경	‣고용계약, 주요 직무자 지정 및 감독, 직무 분리, 비밀유지서약서	일부
	2.2 외부인력보안	‣외부인력 계약, 외부인력 보안 이행 관리, 계약 만료 시 보안	-	삭제
	2.3 정보보호교육	‣교육 프로그램 수립, 교육 시행, 평가 및 개선	‣교육 시행	일부

평가기준(3/14)

구분		IaaS	SaaS	비고
3. 자산관리	3.1 자산 식별 및 분류	‣자산 식별, 자산별 책임할당, 보안등급 및 취급, ※ 정보시스템 중심으로 자산 식별 및 분류	‣자산 식별 ※ 오픈소스, 보안서비스 등 개발되거나 도입된 소프트웨어도 자산에 포함	일부
	3.2 자산변경관리	‣변경관리, 변경 탐지 및 모니터링, 변경 후 작업검증	‣변경관리	일부
	3.3 위험관리	‣위험관리계획 수립, 취약점 점검, 위험분석 및 평가, 위험처리	‣취약점 점검	일부

평가기준(4/14)

구분		IaaS	SaaS	비고
4. 서비스 공급망 관리	4.1 공급망 관리정책	‣공급망 관리 정책 수립, 공급망 계약	‣공급망 관리 정책 수립, 공급망 계약	동일
	4.2 공급망 변경관리	‣공급망 변경관리, 공급망 모니터링 및 검토	‣공급망 변경관리	일부

평가기준(5/14)

구분		IaaS	SaaS	비고
5. 침해 사고관리	5.1 침해사고 대응 절차 및 체계	‣침해사고 대응 절차 수립, 침해사고 대응 체계 구축, 침해사고 대응 훈련 및 점검	‣침해사고 대응 절차 수립, 침해사고 대응 체계 구축, 침해사고 대응 훈련 및 점검	동일
	5.2 침해사고 대응	‣침해사고 보고, 침해사고 처리 및 복구	‣침해사고 보고, 침해사고 처리 및 복구	동일
	5.3 사후관리	‣침해사고 분석 및 공유, 재발방지	‣침해사고 분석 및 공유, 재발방지	동일

평가기준(6/14)

구분		IaaS	SaaS	비고
6.서비스연속성관리	6.1 장애 대응	‣장애 대응절차 수립, 장애 보고, 장애 처리 및 복구, 재발방지	‣장애 대응절차 수립, 장애 보고, 장애 처리 및 복구, 재발방지	동일
	6.2 서비스 가용성	‣성능 및 용량관리, 이중화 및 백업,서비스 연속성 점검	‣성능 및 용량관리, 이중화 및 백업	일부

평가기준(7/14)

구분		IaaS	SaaS	비고
7. 준거성	7.1 법 및 정책 준수	‣법적요구사항 준수, 정보보호 정책 준수	‣법적요구사항 준수	일부
	7.2 보안 감사	‣독립적 보안감사, 감사기록 및 모니터링	‣독립적 보안감사, 감사기록 및 모니터링	동일

평가기준(8/14)

구분		IaaS	SaaS	비고
8.물리적 보안	8.1 물리적보안 8.2.정보처리 시설 및 장비보호	‣물리적 보호구역 지정, 물리적 출입통제, 물리적 보호구역 내 작업, 사무실 및 설비 공간 보호, 공공장소 및 운송·하역구역 보호, 모바일 기기 반출·입, 정보처리시설의 배치, 보호설비, 케이블 보호, 시설 및 장비 유지보수, 장비 반출·입,장비 폐기 및 재사용	-	삭제

평가기준(9/14)

구분		IaaS	SaaS	비고
9. 가상화보안	9.1 가상화 인프라	‣가상자원 관리, 가상자원 회수, 가상자원 모니터링, 하이퍼바이저 보안, 공개서버 보안, 상호 운용성 및 이식성	‣가상자원 관리, 공개서버 보안	일부
	9.2 가상환경	‣악성코드 통제, 인터페이스 및 API 보안, 데이터 이전	‣악성코드 통제, 인터페이스 및 API 보안, 데이터 이전	동일

평가기준(10/14)

구분		IaaS	SaaS	비고
10. 접근통제	10.1 접근통제 정책	‣접근통제 정책 수립, 접근기록 관리	‣접근통제 정책 수립, 접근기록 관리	동일
	10.2 접근권한 관리	‣사용자 등록 및 권한부여, 관리자 및 특수 권한관리, 접근권한 검토	‣사용자 등록 및 권한부여, 관리자 및 특수 권한관리, 접근권한 검토	동일
	10.3 사용자 식별 및 인증	‣사용자 식별, 사용자 인증, 강화된 인증 수단 제공, 사용자 패스워드 관리, 이용자 패스워드 관리	‣사용자 식별, 사용자 인증, 강화된 인증 수단 제공, 사용자 패스워드 관리, 이용자 패스워드 관리	동일

평가기준(11/14)

구분		IaaS	SaaS	비고
11. 네트워크 보안	11.1 네트워크 보안	‣네트워크 보안 정책 수립, 네트워크 모니터링 및 통제, 네트워크 정보보호시스템 운영, 네트워크 암호화, 네트워크 분리, 무선 접근통제)	‣네트워크 보안 정책 수립, 네트워크 모니터링 및 통제, 네트워크 정보보호시스템 운영, 네트워크 암호화, 네트워크 분리	일부

평가기준(12/14)

구분		IaaS	SaaS	비고
12. 데이터 보호 및 암호화	12.1 데이터보호	‣데이터 분류, 데이터 소유권, 데이터 무결성, 데이터 보호, 데이터 추적성, 데이터 폐기	‣데이터 분류, 데이터 소유권, 데이터 무결성, 데이터 보호, 데이터 추적성, 데이터 폐기	동일
	12.2 매체보안	‣저장매체 관리, 이동매체 관리	-	삭제
	12.3 암호화	‣암호 정책 수립, 암호키 관리	‣암호 정책 수립, 암호키 관리	동일

평가기준(13/14)

구분		IaaS	SaaS	비고
13. 시스템 개발 및 도입 보안	13.1 시스템 분석 및 설계	‣보안요구사항 정의, 인증 및 암호화 기능, 보안로그 기능, 접근권한 기능, 시각 동기화	‣보안요구사항 정의, 인증 및 암호화 기능, 보안로그 기능, 접근권한 기능, 시각 동기화	동일
	13.2 구현 및 시험	‣구현 및 시험, 개발과 운영환경 분리, 시험 데이터 보안, 소스 프로그램 보안	‣구현 및 시험, 개발과 운영환경 분리, 시험 데이터 보안, 소스 프로그램 보안	동일
	13.3 외주 개발 보안	‣외주 개발 보안	‣외주 개발 보안	동일
	13.4 시스템 도입 보안	‣시스템 도입 계획, 시스템 인수	-	삭제

평가기준(14/14)

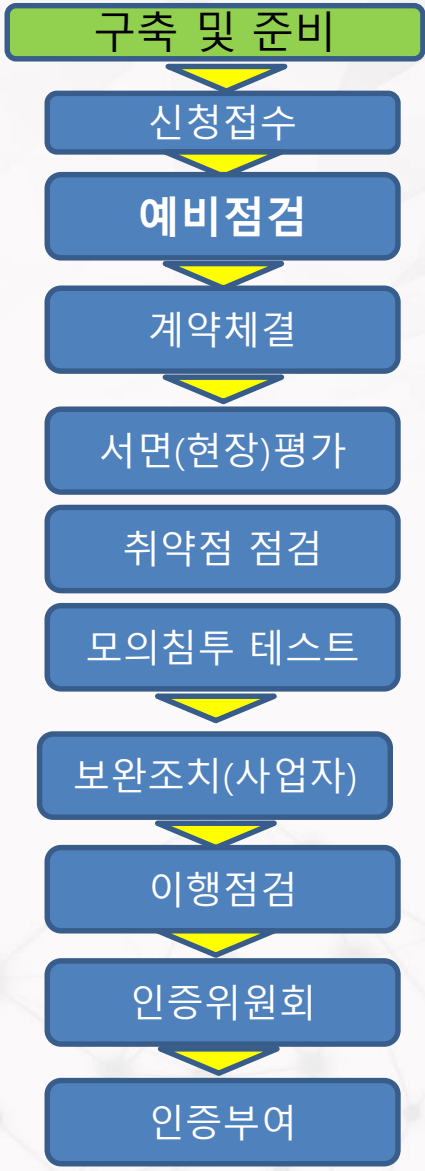
구분		IaaS	SaaS	비고
14. 공공기관 보안요구 사항	14.1 관리적 보호조치	‣보안서비스 수준 협약, 도입 전산장비 안전성, 보안관리 수준, 사고 및 장애 대응	‣보안서비스 수준 협약, 도입 전산장비 안전성, 보안관리 수준, 사고 및 장애 대응	동일
	14.2 물리적 보호조치	‣물리적 위치 및 분리, 중요장비 이중화 및 백업체계 구축	‣물리적 위치 및 분리, 중요장비 이중화 및 백업체계 구축	동일
	14.3 기술적 보호조치	‣검증필 암호화 기술 제공, 보안관제 제반환경 지원	‣검증필 암호화 기술 제공	일부

SaaS 평가 절차 및 방법

SaaS 평가 절차 및 방법(준비단계)

KISA

- 인증 IaaS내 SaaS 구축 신청 및 동의
- 시스템 취약점 자체 점검과 조치율 80% 확보
- 서비스 테스트 : 사전 계정 부여 및 이용자 매뉴얼 제공



SaaS 평가 절차 및 방법(예비점검)

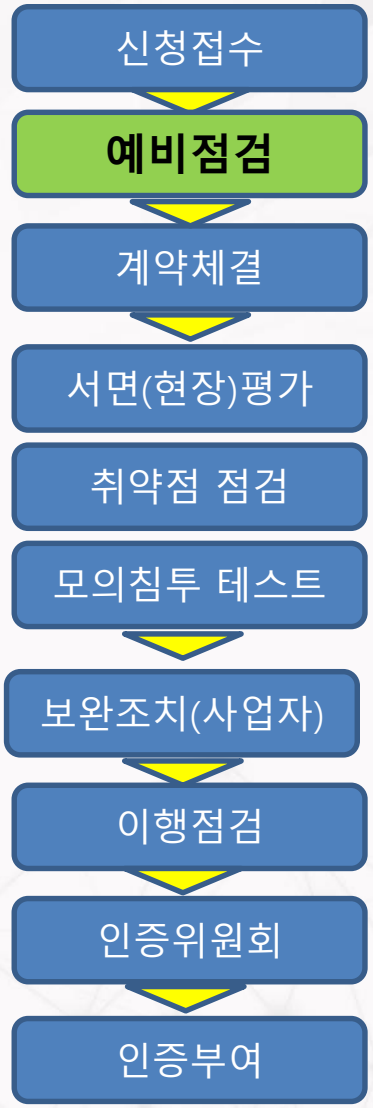
- 신청기관의 평가준비도 파악, 점검대상 파악, 점검항목 및 방법 도출을 위해 계약 체결 전에 실시

- IaaS 대비하여 SaaS 보안인증에서는 예비점검의 중요성 부각

  - 서면평가 중심이던 예비점검에 취약점 점검팀을 참여시켜, 서비스와 자산 파악을 강화하고 이에 맞는 점검 방법을 사전에 준비

  - 취약점 점검을 위해, VPN환경 제공여부, 원격 접속시 방화벽 작업, 자동 점검도구 설치 가능 여부 체크

  - 오픈소스를 포함한 각종 SW를 자산관리대장에 포함하는 등 점검대상 확인



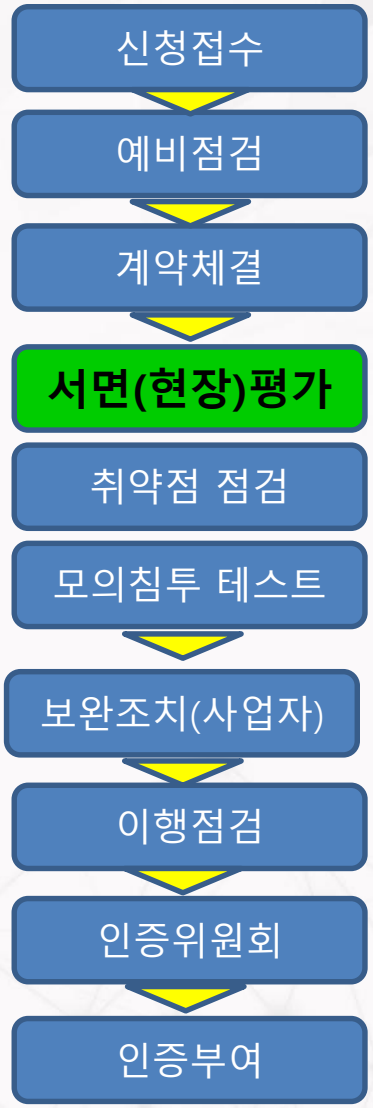
SaaS 평가 절차 및 방법(서면, 현장평가)

서면평가

- 정보보호 정책, 지침, 매뉴얼(절차) 등 내부규정 존재 여부 및 해당 내부 규정이 평가·인증기준에 충족하는지 평가
- 신청기관에서 제출한 문서, 증적자료 확인

현장평가

- SaaS서비스가 보안평가 인증기준에 맞게 적절하게 구축, 운영되고 있는 지 확인
- SaaS 사업자측에서 서비스를 시연하거나 혹은 평가원이 서비스 계정을 확보하고 직접 서비스 이용

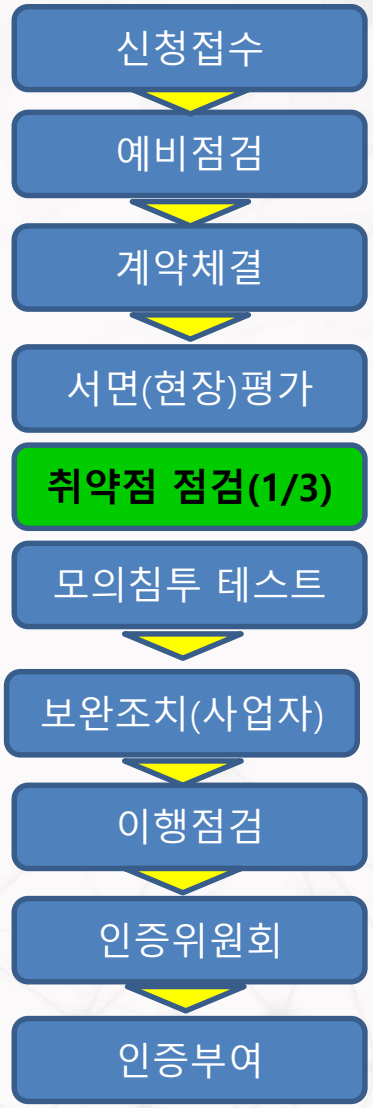


SaaS 평가 절차 및 방법(취약점 점검)

KISA

- CCE(Common Configuration Enumeration)
  : 취약한 설정에 대한 점검
  - 비밀번호 길이/복잡성, 기본 계정 삭제 등 시스템 구성 및 설정에 관한 규정(또는 정책)을 준수하는지 점검

- 점검방법
  - 점검대상과 항목의 도출
    - 예비점검 참여, 자산대장 분석, 점검 방법 도출
  - 점검대상 : Server(OS), Network, Security, DBMS, Web/WAS, PC + more
  - 스크립트 실행(OS), Config 분석(네트워크 장비), 관리콘솔에서 설정 수동확인(보안장비), 담당자 인터뷰(취약점 발생원인 파악)



SaaS 평가 절차 및 방법(취약점 점검)

KISA

▶ CVE(Common Vulnerabilities and Exposures)
: OS, Applicaion 고유의 취약점

➡ 벤더가 제공하는 패치와 관련된 취약점으로, Mitre에서 CVE코드(예, CVE-2009-2521) 부여 관리

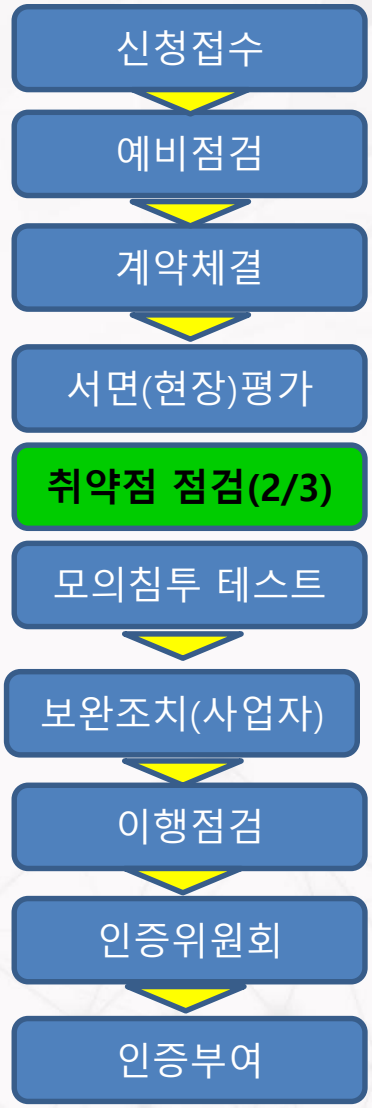
▶ 점검방법

➡ 스캐닝 도구활용, 실행 결과를 토대로 정오탐 분석
※ 10%~20% 오탐률 도출, 반복되는 오탐의 경우 스캔시 제외되도록 스캔 템플릿 커스터마이징

➡ SaaS는 IaaS 내부에 위치하여 네트워크 보호를 받고 있으므로 외부에서 스캐닝 불가

➡ SaaS 서비스가 설치된 내부망에 점검도구 설치 후 점검(SaaS 서버내 설치 혹은 점검용 VM 추가 생성 후 도구 설치)

➡ 점검도구 외부접속과 웹 UI 사용을 위해 방화벽 작업 필요



SaaS 평가 절차 및 방법(소스코드 점검)

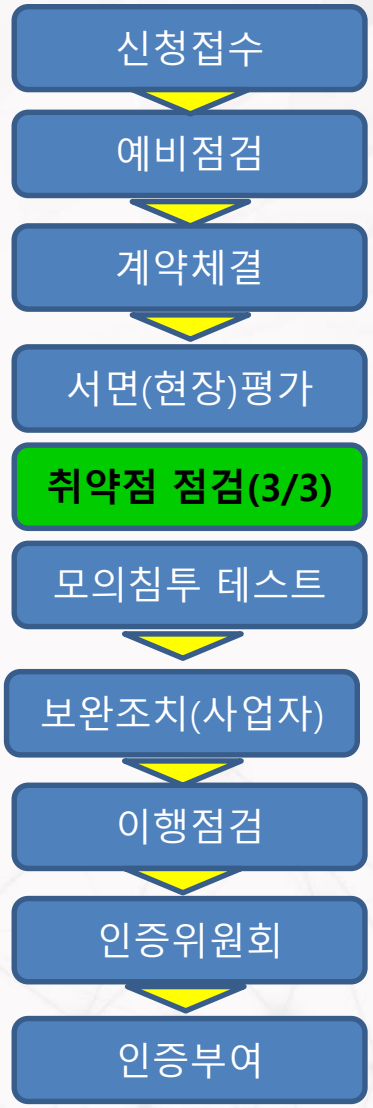
KISA

- **점검 대상 :**
  웹프로그램, 응용프로그램 등(SaaS 서비스 특성에 따라 조정)

  ※ SaaS 특성상 여러 버전의 프로그램이 존재하는 경우 샘플링 가능

- **점검 항목 :**
  행정기관 및 공공기관 정보시스템 구축/운영 지침 준용 47개 항목

- 소스코드 진단원 자격 소유자 투입, 점검 도구 활용, 조치방법 안내



SaaS 평가 절차 및 방법(모의침투 테스트)

KISA

사전동의(IaaS사업자, SaaS사업자)

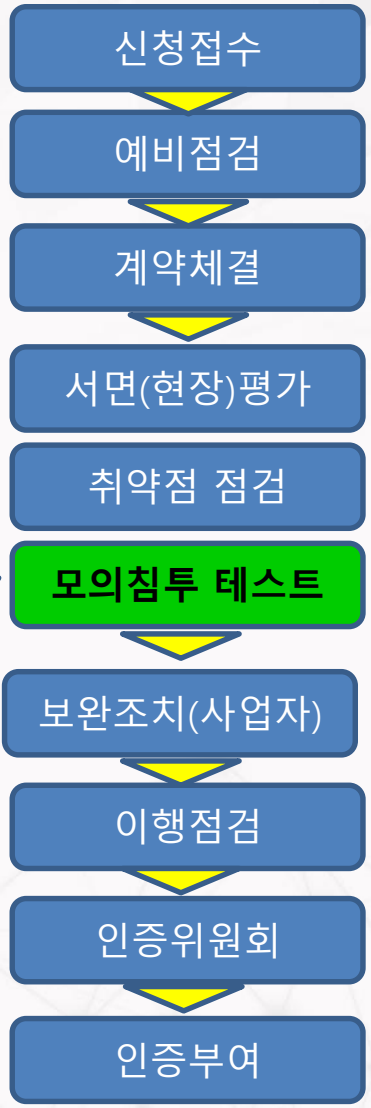
SaaS 서비스 분석
(평가원이 서면현장평가에 참여)

침투 시나리오 수립(내부, 외부)

점검항목 설정

모의침투 테스트 수행(2주)

모의침투 테스트 결과 제공



FAQ(1/3)

Q 클라우드 정보보호 기준은 클라우드 서비스 모든 유형(IaaS, PaaS, SaaS)에 적용 가능한지?

A) 모든 유형(IaaS, PaaS, SaaS)에 적용 가능한 공통적인 보안조치들로 구성됨. 인증을 부여하는 대상은 IaaS, SaaS 이며 PaaS는 인증 수요가 적어 미적용 중이며, 향후 확대 예정

Q CC인증이 필수적인 제품군의 범위가 어디까지 인지와 CC인증은 국내용 CC인증만 가능한지?

A) 국내외 CC인증 모두 인정되며,
제품군은 총24종으로 한국인터넷진흥원(KISA)에서 확인가능

Q 클라우드서비스 보안인증 수수료는 어떻게 되나요?

A) 클라우드서비스 보안인증제도 활성화 및 공공기관의 민간 클라우드서비스 이용 활성화를 위해 일정기간 동안 정부에서 클라우드서비스 보안 평가·인증 수수료를 지원하고 있습니다.

Q 클라우드서비스 보안인증 평가원 양성 계획이 있나요?

A) 인증제도 도입 초기에는 한국인터넷진흥원(KISA)에서 평가·인증을 수행하고 향후 보안인증 대상 확대(IaaS→SaaS)에 따라 공급·수요를 고려하여 민간 평가 기관 활용 및 보안인증 평가원 양성 방안을 마련할 예정입니다.

FAQ(2/3)

Q SaaS 보안인증제 인증취득 후 인증서 유효기간

A) SaaS 보안인증제 유효기간은 3년임, 인증취득 후 사업자 인증효력 유지 여부를 점검하기 위해 매년 사후평가를 실시하며, 상시 보안수준 유지관리를 위해서는 3개월(분기)마다 사업자 자체점검과 보안대책을 구현해 결과를 KISA 로 송부합니다.

Q 타 SaaS 관련 인증에서도 보안인증이 포함 (Ex, 클라우드서비스 확인제) 되어 있는데 타 SaaS 관련 인증과 비교해서 차별성 및 취득 시 기업의 이점은 무엇인지?

A) 클라우드서비스확인제는 민간/공공 등 이용자의 구분이 없는 반면, KISA의 클라우드 보안인증은 공공기관을 대상으로 사업을 하려고 하는 민간 클라우드 사업자의 보안수준을 평가하여 인증을 부여하는 제도로, 클라우드컴퓨팅 정보보호에 관한 기준(과기정통부 고시)에 의거 공공기관용 추가 보호조치 사안을 확인합니다. 클라우드보안인증을 취득한 기업은 공공시장 조달에 참여가 가능합니다. (조달청 나라장터에 등록)

Q 보안인증 신청 전, 보안수준 확인을 위한 사전진단 및 컨설팅이 가능한가?

A) 영세 중소기업의 인증 준비를 돕기위해 과기정통부 및 KISA에서는 보안컨설팅 사업을 매년 추진하고 있습니다. 해당 사업을 점차 확대해 나갈 예정이며, 인증준비에 관련된 사항은 KISA 콜센터(118)로 상시 상담이 가능합니다.

FAQ(3/3)

Q **SaaS 보안 인증이 시행되면, 기존 방식(보안성 검토)를 통한 공공기관의 SaaS 서비스 이용은 불가능 합니까?**

A) 인증제 시행 이후에는 인증받은 클라우드 서비스를 이용해야 합니다. 다만 인증제 대상은 Public 클라우드이므로, 공공기관이 단독으로 입찰공고를 내고 기관 내부적으로 구축하는 private cloud는 해당되지 않습니다. private cloud는 기존 방식대로 보안성 검토 후 이용하시면 됩니다.

Q **인증 없는 IaaS 위해 SaaS를 구현한 SaaS 사업자는 향후 보안 인증을 어떻게 대비해야 합니까?**

A) 클라우드 보안인증 취득한 IaaS로 옮겨서 SaaS를 구축하고 해당서비스 부분만 보안 인증평가를 받을 수 있습니다. 보안인증이 없는 IaaS에서 SaaS서비스를 구축하고자 하면 IaaS 영역과 SaaS 영역을 한꺼번에 보안 인증 평가를 받아야 합니다.

Internet On, Security In!

감사합니다

KISA 한국인터넷진흥원