정부혁신 보다나은 정부	보 도 자 료	행정안전부 정보자원정책과 과 장 이상민 (044-205-2802) 사무관 김경직 (044-205-2812)
관계부처 합동	2019년 7월 24일(수) 조간 (7. 23. 12:00 이후)부터 보도하여 주시기 바랍니다.	과기정통부 사이버침해대응과 과 장 황큰별 (02-2110-2890) 주무관 구준모 (02-2110-2816) 과기정통부 소프트웨어진흥과 과 장 이우진 (02-2110-1840) 사무관 이운규 (02-2110-1803) 한국인터넷진흥원 클라우드인증팀 단 장 이석래 (02-405-6320) 팀 장 박정환 (061-820-1656)

클라우드 보안인증 제도 대폭 개선된다.

- 유효기간 확대, 간편등급 도입, 행정절차 간소화 등 -

□ **과학기술정보통신부**(장관 유영민, 이하 '과기정통부')와 **행정안전부**(장관 진영, 이하 '행안부')는 공공부문의 클라우드서비스(SaaS) 이용 활성화와 보안 필요성 등을 종합적으로 고려하여 **클라우드서비스 보안인증제*** **개선방안**을 **마련·시행**('19.7.24일)한다고 밝혔다.

* 행정·공공기관이 보안인증을 받은 민간 클라우드서비스를 이용할 수 있도록 하여 클라우드서비스 이용 활성화 도모('18.8월 도입)

□ 첫째, **규제를 크게 개선**하여 **클라우드서비스 사업자의 부담**을 **완화**하였다.

○ 현행 3년인 보안인증 **유효기간**을 **5년**으로 **확대***하고, 기존의 표준등급 외에 **간편등급을 신설**하였다.

- 기존의 표준등급은 78개 인증항목의 심사를 받고 있으나, 전자결재, 인사, 회계관리, 보안서비스, 개인정보영향평가 대상 서비스 등을 제외한 서비스에 대해 **간편등급**을 적용하여 **30개 인증항목**(붙임)**만 통과하면 보안인증을 받을 수 있도록 하였다.**

* 인증 유효기간이 확대되어도 매년 사후 심사를 통해 보안조치 가능

□ 둘째, **행정절차**를 **대폭 개선·합리화**하였다.

○ 클라우드서비스 사업자들이 보안인증 신청 전에 반드시 받아야 했던 **사전 준비기준***을 **없애고**, 향후 **보안운영명세서 간소화, 제출서류 정형화, 타 인증제**(정보보호관리체계인증 등)와의 **중복항목**을 **조정·폐지**할 계획이다.

* 사업자가 자체적으로 취약점 점검을 수행하며, 기준점수(80점) 이상 획득 필요

○ 이번 행정절차 개선을 통해, **인증신청 접수에서 인증 완료시까지 5개월**이 걸리던 기간을 **3.5개월 이내로 단축**할 수 있을 것으로 기대하고 있다.

□ 셋째, 현재 **행정·공공기관에서 이미 이용중인 클라우드서비스**(32개)에 대해서는 **2020년 12월 31일까지 유예**하여 동 기간 중에 인증제 신청과 서비스 이용이 가능하도록 배려하였다.

□ 이번 **제도개선 방안**은 지난해 8월의 대통령 주재 「데이터경제 활성화 규제혁신 현장방문」시 제기된 규제 개선 요구사항을 반영하기 위해 **7차례에 걸친 기업들의 애로사항 및 의견 수렴**과 **6차례의 제도개선안 관계부처 협의를 통해 마련·시행**하게 되었다.

□ 장석영 과기정통부 정보통신정책실장은 "이번에 시행하는 **제도개선 사항**은 사이버 공격이 지능화·다양화되는 추세에 따라 **사이버 보안의 중요성을 간과하지 않는 방향**에서 **보안이 꼭 필요한 부분, 클라우드서비스 이용 활성화, 기업 부담 등을 종합적으로 비교·검토**하여 관계부처 간 협업을 통해 마련된 내용으로 평가"하고,

○ "**국내 클라우드서비스 사업자**들은 외국 클라우드서비스 사업자가 앞선 보안기능을 홍보하며 국내시장 진입을 도모하고 있는 상황에서, **서비스에 대한 보안수준을 높이기 위한 끊임없는 노력과 투자 역시 시급**하다."라고 밝혔다.

□ 최장혁 행정안전부 전자정부국장은 “이번 인증제도개선으로 **많은 서비스**들이 **신속**하게 공공시장에 **진입**할 수 있게 된다.”면서, “행정·공공기관에서 **다양한 민간 클라우드 서비스**를 **활용**해 전자정부 **서비스**의 **품질**을 **높이는 계기**가 되길 기대한다.”라고 밝혔다.

□ 한편, 과기정통부와 한국인터넷진흥원은 **2019년 7월 17일 13시 엘타워**(서울 서초)에서 클라우드 이용자 보호 등을 위한 사업자 및 유관기관 간 상호 정보공유 및 협력 강화 등을 논의하는 **보안협의체 1차 회의**를 **개최**하였다.

○ 향후 보안인증제 신청절차·항목·심사방법 등에 대한 **상세한 설명을 담은 가이드라인을 제작·배포**('19.8월)하고, **설명회**, **교육**, **보안 컨설팅**, **보안협의체 운영** 등을 통해 클라우드 보안인증제가 조기 정착될 수 있도록 할 계획이다.

OPEN 공공누리	이 보도자료에 대하여 더욱 자세한 내용을 원하시면 과학기술정보통신부 구준모 주무관(☎ 02-2110-2816), 이운규 사무관(☎ 02-2110-1803), 행정안전부 김경직 사무관(☎ 044-205-2812),한국인터넷진흥원 박정환 팀장(☎ 061-820-1656)에게 연락주시기 바랍니다.

붙임 표준등급(78개 항목) 및 간편등급(30개 항목) 인증심사 항목

※ (간편등급) 음영표시 항목

부문	세부 항목	부문	세부 항목
1. 정보보호 정책 및 조직	1.1.1. 정보보호 정책 수립	9. 접근통제	9.1.2. 접근기록 관리
	1.1.2. 정보보호 정책 검토 및 변경		9.2.1. 사용자 등록 및 권한부여
	1.1.3. 정보보호 정책문서 관리		9.2.2. 관리자 및 특수 권한관리
	1.2.1. 조직 구성		9.2.3. 접근권한 검토
	1.2.2. 역할 및 책임 부여		9.3.1. 사용자 식별
2. 인적보안	2.1.1. 고용계약		9.3.2. 사용자 인증
	2.1.2. 주요 직무자 지정 및 감독		9.3.3. 강화된 인증 수단 제공
	2.1.3. 직무 분리		9.3.4. 사용자 패스워드 관리
	2.1.4. 비밀유지서약서		9.3.5. 이용자 패스워드 관리
	2.2.1. 교육 시행	10. 네트워크 보안	10.1.1. 네트워크 보안 정책 수립
3. 자산관리	3.1.1. 자산 식별		10.1.2. 네트워크 모니터링 및 통제
	3.2.1. 변경관리		10.1.3. 네트워크 정보보호시스템 운영
	3.3.1. 취약점 점검		10.1.4. 네트워크 암호화
4. 서비스 공급망관리	4.1.1. 공급망 관리 정책 수립		10.1.5. 네트워크 분리
	4.1.2. 공급망 계약	11. 데이터 보호 및 암호화	11.1.1. 데이터 분류
	4.2.1. 공급망 변경관리		11.1.2. 데이터 소유권
5. 침해사고 관리	5.1.1. 침해사고 대응절차 수립		11.1.3. 데이터 무결성
	5.1.2. 침해사고 대응체계 구축		11.1.4. 데이터 보호
	5.1.3. 침해사고 대응훈련 및 점검		11.1.5. 데이터 추적성
	5.2.1. 침해사고 보고		11.1.6. 데이터 폐기
	5.2.2. 침해사고 처리 및 복구		11.2.1. 암호 정책 수립
	5.3.1. 침해사고 분석 및 공유		11.2.2. 암호키 관리
	5.3.2. 재발방지	12. 시스템개발및 도입 보안	12.1.1. 보안요구사항정의
6. 서비스 연속성 관리	6.1.1. 장애 대응절차 수립		12.1.2. 인증 및 암호화 기능
	6.1.2. 장애 보고		12.1.3. 보안로그 기능
	6.1.3. 장애 처리 및 복구		12.1.4. 접근권한 기능
	6.1.4. 재발방지		12.1.5. 시각 동기화
	6.2.1. 성능 및 용량 관리		12.2.1. 구현 및 시험
	6.2.2. 이중화 및 백업		12.2.2. 개발과 운영환경 분리
7. 준거성	7.1.1. 법적요구사항 준수		12.2.3. 시험 데이터 보안
	7.2.1. 독립적 보안감사		12.2.4. 소스 프로그램보안
	7.2.2. 감사기록 및 모니터링		12.3.1. 외주 개발 보안
8. 가상화 보안	8.1.1. 가상자원 관리	13. 공공기관 보안요구 사항	13.1.1. 보안서비스 수준 협약
	8.1.2. 공개서버 보안		13.1.2. 도입 전산장비 안전성
	8.2.1. 악성코드 통제		13.1.3. 보안관리 수준
	8.2.2. 인터페이스 및 API 보안		13.1.4. 사고 및 장애 대응
	8.2.3. 데이터 이전		13.2.1. 물리적 위치 및 분리
	8.2.4. 가상 소프트웨어 보안		13.2.2. 중요장비 이중화 및 백업체계 구축
9. 접근통제	9.1.1. 접근통제 정책 수립		13.3.1. 검증필 암호화 기술 제공