

보도시점

배포시점

배포 2025. 4. 14.(월) 09:00

양자컴퓨팅 위협을 넘어선 보안 기술, 양자내성암호로의 전환 본격 착수

- 국민 생활과 밀접한 에너지, 의료, 행정분야 시범사업 착수 -

과학기술정보통신부(장관 유상임, 이하 ‘과기정통부’)는 한국인터넷진흥원(원장 이상중)과 함께 국가 암호체계의 안정적 전환 준비를 위한 ‘2025년 양자내성암호 * 시범전환 지원사업’을 본격 추진한다.

* 기존 공개키 기반 암호(소인수분해, 이산대수 등)보다 훨씬 복잡한 수학적 문제(격자 기반, 해시기반 등)를 기반으로 하여, 양자컴퓨터로도 해독이 어려운 차세대 암호기술

이번 사업은 양자컴퓨팅 기술의 급속한 발전으로 초래될 기존 암호체계에 대한 보안 위협 가능성에 대비하여, 국민 생활과 밀접한 에너지, 의료, 행정 분야의 정보통신 기반(인프라)을 시작으로 주요 산업분야에 양자내성암호를 적용하는 국내 최초 시범사업이다.

과기정통부와 한국인터넷진흥원은 지난 1월부터 사업자 선정을 위한 공모를 진행하였으며, 지원한 연합체에 대해 평가한 결과, △에너지 분야에 한전KDN 연합체, △의료 분야에 라온시큐어 연합체, △행정 분야에 LGU+ 연합체를 최종 선정하였다. 분야별 연합체의 주요 추진내용은 다음과 같다.

[에너지 분야 : 한전KDN 연합체]

한전KDN 연합체는 한국전력공사의 ‘전력 사용량 원격 검침 체계’의 암호 체계를 양자내성암호 체계로 시범 전환한다. 이를 통해 전국 가정의 중요 정보가 포함된 검침 데이터의 유출 및 위변조를 방지하고, 향후 추가적인 에너지 분야 기반 체계(인프라 시스템)에 대한 양자내성암호 전환을 단계적으로 확대할 계획이다.

[의료 분야 : 라온시큐어 연합체]

라온시큐어 연합체는 ‘의료 데이터 중계 온라인 체제 기반(플랫폼)’의 암호체계를 양자내성암호 체계로 시범 전환한다. 해당 온라인 체제 기반(플랫폼)은 세브란스병원(신촌, 강남, 용인) 등에서 운영되는 전자 의무기록(EMR) 체계와 연계되어 국민의 의료 정보를 중계·처리하는 인터넷 기반 자원 공유(클라우드) 기반 온라인 체제 기반(플랫폼)이다. 정부는 이번 시범사업을 통해 디지털 건강돌봄(헬스케어) 환경에 적합한 암호체계 전환 기술을 확보할 계획이다.

[행정 분야 : LGU+ 연합체]

LGU+ 연합체는 한국방송통신전파진흥원이 운영하는 ‘국가기술자격검정 체계’ 등 국가 행정정보체계의 암호체계를 양자내성암호 체계로 시범 전환한다. 이를 통해 행정 분야 환경에 적합한 보안 기술을 확보하고, 향후 개발 해결책(솔루션)을 확산하여 공공 서비스의 신뢰도 향상을 위해 노력할 계획이다.

과기정통부와 한국인터넷진흥원은 시범사업을 통해 양자내성암호 전환 관련 실증사례를 확보하여, △암호체계 전환에 필요한 부분(모듈) 개발, △전환 과정에서 발생하는 기술상 문제점과 해결 방안, △실제 전환 절차와 방법론 등을 도출할 예정이다. 또한 결과물을 종합하여 산업 전반에서 활용할 수 있는 ‘양자내성암호 전환 지침(가이드라인)’을 마련함으로써, 향후 전 국가적 양자내성암호 체계의 안전하고 효율적인 전환을 지원할 수 있을 것으로 기대한다.

과기정통부 최우혁 정보보호네트워크정책관은 “양자내성암호로의 전환은 새로운 기술의 역기능으로부터도 정보통신 기반(인프라)을 굳건하게 지켜낼 수 있는 면역체계를 갖추는 것과 같다”라며, “양자컴퓨터 시대에 대비해 안전한 디지털 환경을 구축할 수 있도록 정부도 적극적인 지원과 노력을 다하겠다.”고 밝혔다.

담당 부서	정보보호네트워크정책관 정보보호기획과	책임자	과 장	김연진 (044-202-6440)
		담당자	사무관	정준환 (044-202-6448)
담당 부서	한국인터넷진흥원 보안기술단	책임자	단 장	박해룡 (061-820-1630)
		담당자	팀 장	손기종 (061-820-1348)

