양자내성암호 검증대상 후보군 및 추진 일정 공지

[2026. 9. 1]

o 국가정보원은 범국가 양자내성 암호체계 전환에 대비, 산업계에서 미리 준비할 수 있도록 양자내성암호 검증대상 후보군 및 향후 추진 일정에 대해 공지함

o 또한, 향후 ▲다른 수학적 기반 ▲국내외 기술발전 동향 등을 종합적으로 고려, 추가 검증대상 후보군을 지속적으로 확대·검토해 나갈 계획임

□ 검증대상 양자내성암호 후보군

* 알고리즘 (ABC순)

키 캡슐화 메커니즘 (KEM) 3종			전자서명 (DSA) 4종			
ML-KEM	NTRU+	SMAUG-T	AIMer	HAETAE	ML-DSA	SLH-DSA
격자기반			대칭키기반	격자기반		해시기반

□ 검증대상 양자내성암호 검증 추진 계획

종류	키 캡슐화 메커니즘 (KEM)	전자서명 (DSA)
후보군 공지	'26.9월	'26.9월
검증대상 선정	(예정)'27.1월	(예정) '28.1월
검증시행*	'28.1월	검증대상 선정 + 1년
탑재의무화**	'29.1월	검증대상 선정 + 2년

* 검증 시행 시 현재 검증대상 공개키 암호알고리즘과 조합하는 「하이브리드 방식」 필수 구현

** 공개키 암호기능이 포함된 모든 암호모듈 대상