◉ **국립전파연구원공고 제2019-71호**

국가표준을 제정함에 있어 국민, 업계 및 관련기관에 미리 알려 의견을 듣고자 주요 내용을「방송통신표준화지침」제14조의 의하여 다음과 같이 공고합니다.

2019년 6월 21일

국립전파연구원장

방송통신분야 국가표준 제정 예고

1. 표준번호 및 표준명

순번	분야	표준번호	표준명
1	정보보호	KS X NEW	n비트 블록 암호 운영 모드 - 제2부: 블록 암호 LEA
2	정보보호	KS X NEW	n비트 블록 암호 운영 모드 - 제3부: 블록 암호 ARIA
3	정보보호	KS X NEW	n비트 블록 암호 운영 모드 - 제4부: 블록 암호 SEED
4	정보보호	KS X NEW	n비트 블록 암호 운영 모드 - 제5부: 블록 암호 HIGHT

2. 제정 목적

o 한국정보통신기술협회 단체표준 4종의 국가표준 제정 제안에 따른 국가표준 제정

3. 주요 내용

□ **(KS X NEW) n비트 블록 암호 운영 모드 - 제2부: 블록 암호 LEA ~ 제5부: 블록 암호 HIGHT**

○ 표준의 목적

- 주요 블록 암호 운영 모드* 규격이 국가표준 '(KS X 3254) n비트 블록 암호 운영 모드 - 제1부: 일반'으로 제정되었으나,

* 블록암호를 사용하여 가변길이 데이터를 안전하게 처리하는 방법

- 블록 암호(LEA, ARIA, SEED, HIGHT)를 사용하는 운영 모드의 암호모듈(제품) 구현과 검증에 필요한 참조구현값*이 없어, 이번 표준제정으로 참조구현값을 마련

  * 운영 모드 규격은 일종의 알고리즘으로, 알고리즘 처리 시 값을 입력하였을 경우, 중간 계산값과 최종 결과값을 정리한 것이 참조구현값

○ 주요 내용

- '(KS X 3254) n비트 블록 암호 운영 모드 - 제1부: 일반'에 제시된 운영 모드의 기반 블록 암호로 LEA, ARIA, SEED, HIGHT를 적용한 참조구현값 제시

4. 의견 제출

o 위 표준안 내용에 대하여 의견이 있는 기관, 단체 또는 개인은 2019년 8월 19일까지 다음 사항을 기재한 의견서를 국립전파연구원(참조 : 전파자원기획과)에 제출하여 주시기 바라며, 예고안의 전문을 보고 싶으신 분은 국립전파연구원 홈페이지(http://www.rra.go.kr) 전자공청회란을 참고하시기 바랍니다.

가. 제정 예고 사항에 대한 항목별 의견(찬·반 여부와 그 사유)

나. 성명(단체인 경우에는 단체명과 대표자명), 주소 및 전화번호

다. 기타 참고자료

라. 보내실 곳 : 국립전파연구원 전파자원기획과

o 주소 : 전라남도 나주시 빛가람로 767(우편번호 : 58217)

o 전화 : 061)338-4434, 팩스 : 061)338-4419, 전자우편 : shlee95@korea.kr

※ 홈페이지(http://www.rra.go.kr) 이용방법 : 홈페이지 접속→ 민원·참여 → 전자공청회