방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2011. 6. 16.(목)

보도자료

2011년 6월 16일(목) 배포 시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 네트워크정보보호팀 박철순 팀장(☎ 750-2750)
네트워크정보보호팀 이상국 사무관(☎ 750-2751) sklee@kcc.go.kr

「한국 암호 포럼」 창립총회 개최

- 국산 암호 발전 및 이용활성화를 위한 논의의 장 마련 -

방송통신위원회(위원장 최시중)는 최근 잇따른 해킹사고로 인해 정보보호에 대한 관심이 고조되는 가운데 상대적으로 침체되어 있는 국산 암호 발전 및 이용활성화 등을 위한 「한국 암호 포럼(Korea Cryptography Forum)」 창립총회를 6월 16일(목) 양재동 엘타워에서 기업, 학계, 관계기관 전문가 등 50여명이 참석한 가운데 개최하였다.

'한국 암호 포럼'은 방송통신위원회와 한국인터넷진흥원(KISA), ETRI 부설연구소 등 관계기관들과 암호 분야의 저명한 학계 전문가 및 암호 이용에 적극적인 기업들이 함께 참여하여 산·학·연·관간의 폭넓은 논의의 장으로 창립되었다.

※ 주요 참여기업 : 삼성SDS, SKT, 롯데정보통신, 삼성전자, 소프트포럼, 한국정보인증, 유넷시스템, 펜타시큐리티시스템, 마크애니, 이니텍

현재 우리나라에서는 국제표준으로 제정되어있는 국산 암호기술(SEED, ARIA, HIGHT)이 전자서명, DB보안, 문서·키보드보안 분야 등에 적용되고 있다. 그러나 최근 민간 기업의 대규모 개인정보 유출 사고에서 볼 수 있듯이 중요 데이터의 암호기술 미적용이 문제로 지적된 바 있으며, 국제적으로도 국제표준 기구인 ISO/IEC에서 활용도가 낮은 암호표준은 국제표준 지위를 취소하려는 움직임이 있는 등 국내외적으로 암호 활용을 제고시킬 필요성이 대두되고 있다.

더욱이 스마트폰, 클라우드, 스마트그리드 등 새로운 IT환경이 제공됨에 따라, 학계의 활발한 연구 및 IT기기 제조사, 통신사, 보안솔루션사 등의 참여를 통해 "국내 암호기술의 연구개발(R&D) → 기술의 상용화 및 기본 탑재 → 국내외 활용 제고"로 이어지는 선순환 구조를 마련하는 정책적 지원이 필요한 시점이다.

‘한국 암호 포럼’은 운영위원회와 자문위원회를 두고 운영위원회 산하에 ▲정책·표준화 분과, ▲안전성 평가 분과, ▲암호기술 분과 등 3개의 분과위원회로 구성·운영되며, 초대 운영위원장은 이동훈 고려대 교수가 맡기로 하였다.

암호 포럼은 정책·표준화 분과를 통해 국산 암호기술 활성화를 위한 클라우드, 스마트그리드 등 신규 적용분야 발굴, 국제 표준화 아이템 등을 연구하고, 안전성 평가 분과를 통해 모바일 단말 등 신규서비스에서 수요가 예상되는 암호기술 검증·평가 제도개선 등에 대해 논의한다. 또한 암호기술 분과를 통해 신규IT환경에 적합한 암호기술 개발방향, 안전성 및 활용도 제고방안 등에 대한 연구를 수행한다. 한편, 금년 11월에는 암호를 주제로 하는 공개 컨퍼런스를 개최하는 등 범국가적인 암호기술 발전과 이용활성화를 위한 활동을 추진할 계획이다.

창립을 축하하기 위해 참석한 방통위 석제범 네트워크정책국장은 “최근 잇따른 IT보안 사고들 속에서 정보보호의 기초라 할 수 있는 암호의 중요성이 어느 때보다 강조되고 있는 상황에서 국내외 환경변화에 보다 적극적으로 대응하고 국산 암호 발전을 위한 한국암호포럼의 창립은 매우 시의적절하며, 포럼을 통해 논의되는 내용들을 향후 정부의 정책방향에도 적극 반영하도록 하겠다.”고 밝혔다.

붙임 : SEED, ARIA, HIGHT 설명자료 1부. 끝.

<붙임> SEED, ARIA, HIGHT 설명자료

□ SEED

o SEED는 국내 암호연구의 씨앗이 되라는 의미로 '99년 KISA를 중심으로 국내 암호전문가들이 개발한 최초 국산암호알고리즘

- 전자상거래, 금융, 무선통신 등 IT환경에서 저장, 송·수신되는 중요 정보들을 보호하기 위해 개발

o '99년 국내 정보통신단체표준, '05년에는 ISO/IEC 국제 블록암호 알고리즘 표준으로 제정

□ ARIA

o ARIA는 Academy(학계), Research Institute(연구소), Agency(정부기관)의 약자로 '03~'04년 ETRI 부설연구소를 중심으로 학계, 연구소, 정부기관 암호전문가들이 개발한 국산암호알고리즘

- 전자정부 도입에 따른 대국민행정서비스의 안전성을 확보하기 위하여 개발

o '04년 국내 산업기술표준, '09년에는 IETF 국제 블록암호알고리즘 표준으로 제정

□ HIGHT

o HIGHT는 HIGh security and light weigHT의 약자로 '04~'05년 KISA, ETRI 부설연구소, 고려대가 공동으로 개발한 경량암호 알고리즘

- RFID 등과 같이 초경량, 저전력을 요구하는 유비쿼터스 컴퓨팅환경에서 기밀성 기능을 제공하기 위해 개발

o '06년 국내 정보통신단체표준, '10년에는 ISO/IEC 국제 블록암호 알고리즘 표준으로 제정

□ ISO/ IEC(JTC1)

o ISO/IEC JTC1(ISO/IEC Joint Technology Committee 1)

- 정보기술 분야의 국제 표준화 기구간 상호협력을 위해 ISO (International Organization for Standardization, 국제표준화기구)의 정보기술 분과와 IEC(International Electrotechnical Commission : 국제전기표준회의) 정보처리기기 분과가 통합하여 설립한 기술위원회