# [정보보호] 블록암호알고리즘의 국제표준화 추진

암호의 사용이 활성화됨에 따라 선진국들은 자국의 기술력을 대외에 과시하고 정보보호시장을 선점하기 위해 자국의 표준암호를 갖고자 많은 노력을 기울이고 있다. 미국의 경우 NIST(National Institute of Standards and Technology)에서 기존의 표준블록암호알고리즘 DES(Data Encryption Standard)를 대신할 새로운 표준을 선정하기 위하여 AES(Advanced Encryption Standard) 공모사업을 주관하였으며, 유럽연합(EU)에서도 회원국들을 위한 암호알고리즘 공모사업인 NESSIE(New European Schemes for Signatures, Integrity, and Encryption)를 진행하여 다양한 분야의 알고리즘에 대한 표준화를 추진하고 있다. 한편, 일본에서는 2003년 전자정부 구현에 필요한 표준암호알고리즘 공모사업으로서 CRYPTREC(Cryptography Research & Evaluation Committee)을 진행 중에 있다.

이러한 추세에 발 맞추어 ISO/IEC(International Organization for Standardization / International Electro-technical Commission)에서는 2000년부터 국제표준 암호알고리즘을 선정하기 위한 노력을 기울이고 있다.

## ISO/IEC의 암호알고리즘 표준화 추진방향

1999년 상반기까지 ISO/IEC JTC 1에서는 비밀성을 보장하기 위한 표준 암호알고리즘을 제정할 때, 특정 알고리즘을 선정하여 표준으로 제정하기보다는 등록절차를 표준화(ISO/IEC 9979, 1991(제정), 1999(개정))하여 이에 따라 등록된 암호알고리즘은 모두 표준 암호알고리즘으로 인정하였다. 때문에 회원국들로부터 등록된 암호 알고리즘이 2000년 4월까지 22개에 이르고 어떤 알고리즘이든 표준등록절차에 따라 등록만 하면 표준으로 인정받는 등 사실상 국제표준으로서의 의미가 유명무실해졌다.

더구나, 미국, 유럽, 일본 등의 암호기술 선진국들이 자국의 차세대 표준암호 선정방식을 "공모를 통한 민간주도"로 전환하면서, ISO/IEC에 등록된 암호알고리즘들의 실효성에 대한 의문이 더욱 제기되었다. 이에 ISO/IEC는 1999년 ISO/IEC JTC1/SC27 전체회의에서 암호알고리즘 표준제정을 공모방식으로 전환하기로 결정하고 회원국들로부터 후보 알고리즘을 제안하도록 요청하였다.

## 국내 표준 블록암호알고리즘 SEED의 ISO/IEC 국제표준화 추진현황

ISO/IEC의 요청에 따라 회원국들은 후보알고리즘을 제안하였으나, 2000년 4월 런던회의에서 제안서(RFP)의 모호성, 제출기간의 촉박함 등의 문제가 제기되어, RFP가 수정되었다.

수정된 RFP(ISO/IEC JTC1/SC27, " Call for contributions on NP 18033 : Encryption algorithms", ISO/IEC JTC1/SC27 N2563, 2000년)에 의거하여 2000년 9월까지 회원국들로부터 공개키암호알고리즘, 블록암호알고리즘, 스트림암호알고리즘에 대한 후보알고리즘을 제안 받았으며, 그 결과 2000년 10월 동경회의까지 공개키암호알고리즘 7개, 블록암호알고리즘 15개, 스트림암호알고리즘 1개가 제안되었다. 제안된 후보알고리즘 및 제안국은 다음

의 [표 1]과 같다.

표 1. ISO/IEC JTC1/SC27 표준 암호알고리즘 후보

| 구분 | 알고리즘 | 제안국 |
|---|---|---|
| 블록 | CAST-128 | 캐나다 |
| | SEED | 대한민국 |
| | XENON | |
| | ZODIAC | |
| | AES(Rijndael) | 미국 |
| | Serpent | |
| | Twofish | |
| | MARS | 미국, 일본 |
| | RC6 | 미국, 스웨덴 |
| | IDEA | 스위스 |
| | CIPHERUNICORN-A | 일본 |
| | MISTY1 | |
| | Hierocrypt-L1,3 | |
| | Camellia | |
| 공개키 | ACE | 독일 |
| | ECIES | 미국 |
| | RSA-OAEP | 미국, 스웨덴 |
| | EPOC | 일본 |
| | PSEC | |
| | HIME-1,2 | |
| 스트림 | MULTI-S01 | 일본 |

이후 2001년 4월에 개최된 오슬로회의에서 한국은 블록암호알고리즘 ZODIAC을 안전성의 문제를 이유로 후보 알고리즘에서 철회하였으며, 미국도 제안한 5개의 알고리즘 중 Rijndael(AES)만을 남기고 나머지는 철회하였다. 다만, 다른 회원국으로부터 중복 제안된 RC6과 MARS는 그대로 후보 알고리즘으로 두기로 하였다.

2001년 10월에 개최된 서울회의에서 일본은 CRYPTREC의 평가결과 안전하다고 인정받은 64비트 블록암호알고리즘 MISTY1과 128비트 블록암호 Camellia만 남기고 나머지 암호알고리즘들은 모두 제안을 철회하였다. 또한 일본은 한국이 제출한 XENON에 대한 안전성 문제를 제기하였으며, 이에 한국은 XENON을 후보알고리즘에서 철회하였다. 서울회의 결과, 작업문서(WD : Working Draft) NP 18033-1의 A.1 선택기준에 맞는 후보인 TDES, MISTY1, AES, SEED, Camellia, CAST-128, IDEA, RC6을 3차 WD에 포함시키기로 결정하였다.

2002년 4월에 개최된 베를린 회의에서 벨기에와 독일은 SEED에 대한 제3국의 평가결과의 부족으로 표준안에서 배제하자는 의견을 제시하였으나, 이에 대해 한국은 일본 CRYPTREC의 SEED에 대한 안전성 및 효율성 평가결과(ISO/IEC JTC1/SC27, “Third Party Evaluation on SEED by CRYPTREC”, ISO/IEC JTC1/SC27 N3213, 2002년)[1)]를 회의현장에서 제출하였다. 또한 벨기에는 브라질과 공동 개발한 64비트 블록암호알고리즘 Khazad를 현 WD에 추가하자는 의견을 제시하였으나, Khazad에 대한 NESSIE의 평가결과를 다음 회의인 2002년 10월 바르샤바회의에서 검토한 후 추후 논의하기로 하였다.

베를린회의 결과 3차 WD에 수용된 후보알고리즘 중 TDEA, MYSTY1, AES, Camellia, SEED, RC6를 4차 WD에 포함시키기로 결정하였으며, 유럽의 NESSIE 운영위원회와 일본의 CRYPTREC 운영위원회로 하여금 블록암호알고리즘과 공개키암호알고리즘에 대한 그간의 평가결과를 다음 바르샤바 회의에서 발표해 줄 것을 요청하였다. 특히 SEED와 4차 WD에서 제외된 CAST-128, IDEA, Khazad에 대해서는 다음번 회의에서 좀 더 면밀히 안전성을 검토하기로 결정하였다.

예상대로 2002년 10월에 개최된 바르샤바회의에서는 SEED와 CAST-128, IDEA, Khazad에 대한 집중적인 논의가 이루어졌으며, WD에서 한 단계 상승한 1차 위원회문서(CD : Committee Draft)에 포함시킬 알고리즘들을 회원국들의 투표로 결정하였다. 회의 결과, 64 비트 블록암호알고리즘 5개와 SEED를 포함한 128비트 블록암호알고리즘 4개를 1차 CD에 포함시키기로 하였으며, 또한 캐나다의 CAST-128에 대한 소프트웨어/하드웨어 구현시의 성능분석 자료와 한국 SEED의 하드웨어 구현시의 성능분석 자료를 2002년 11월말까지 SC 27 사무국으로 송부하여 줄 것을 캐나다와 한국에 각각 요구하였다.

표 2. 1 차 CD 에 포함된 블록암호알고리즘

| 구분 | 알고리즘 | 제안국 |
|---|---|---|
| 64 비트 | TDEA | 미국 |
| | MISTY1 | 일본 |
| | CAST-128 | 캐나다 |
| | IDEA | 스위스 |
| | Khazad | 벨기에 |
| 128 비트 | AES | 미국 |
| | Camellia | 일본 |
| | SEED | 한국 |
| | RC6 | 스웨덴 |

**표준화 관련 쟁점**

ISO/IEC 국제표준화 추진시 쟁점이 되고 있는 사항은 다음과 같다.

- 암호알고리즘의 안전성에 대한 공개검증(Open Evaluation) 여부
- 암호알고리즘의 소프트웨어/하드웨어 구현시의 성능
- 암호알고리즘의 시장성숙도

현재 국내표준 및 전자정부표준 암호알고리즘으로 사용되고 있는 SEED는 시장 성숙도면에서는 어느 정도 인정받았으나, SEED의 안전성에 대한 공개검증 여부 및 효율성 문제는 국제 표준화 추진시 큰 걸림돌이 되어 온 것이 사실이다. 금번 바르샤바회의 결과 SEED의 안전성은 어느 정도 공인된 것으로 사료된다. 그러나 추후 개최될 회의에서는 SEED의 효율성 문제가 다시 쟁점화 될 것으로 예측되며, 이에 대한 대비를 철저히 해야할 것으로 사료된다.

*[1] 2001년 10월 SEED의 안전성에 대한 객관적 검증을 위하여, 한국은 일본의 CRYPTREC 운영위원회에 SEED의 안전성 평가를 의뢰하였으며, 2002년 3월에 안전성에 문제가 없다는

CRYPTREC의 평가결과보고서를 전달받음.

김승주 (한국정보보호진흥원 암호기술팀장, skim@kisa.or.kr)