情 報 保 護 學 會 誌
第 12 券 第 4 號, 2002. 8

ASTAP Forum에서의 정보보호 표준화 동향

서 동 일*, 박 ㅊ 항**, 이 상 호***

요 약

ASTAP Forum은 1998년 2월 아태지역의 표준화 활동 및 ITU, ISO등의 국제 표준화 기구에 회원국의 공동 입장을 반영하기 위해 설립된 APT 산하 표준화 기구이다. 여기이는 PKI 연동, VPN, 암호 알고리즘, ESM 로그, AP-CERT, 멀티캐스트, 정보보증등과 같은 정보보호 표준화 업무를 담당하는 정보보호 전문가 그룹이 있다. 본 기고문에서는 ASTAP Forum의 현황을 설명하고, 정보보호 전문가 그룹에서 현재까지 많은 논의가 이루어지고 있는 정보보호 항목에 대한 설명과 함께 여기에는 어떠한 이슈들이 있는지 알아보고자 한다.

Ⅰ. 서 론

21세기 들어오면서 기존의 모든 네트워크 환경은 "인터넷"으로 통합 연동이 가능하게 되었고, 이를 통해 실생활에서 발생할 수 있는 각종 업무들을 인터넷을 통해 수행할 수 있게 되었다.

특히, 지난 20세기 후반에 나타난 "사이버세상 혹은 가상사회 (cyber world or cyber society)"라는 개념에서 21세기 추가적인 사용자 요구사항이 발생하였는데, "보다 안전한 사이버세상 혹은 보다 안전한 가상사회 (secure cyber world or secure cyber society)"의 추구가 바로 그것이다. 이는 기존의 인터넷 환경에서 공적·사적인 업무를 볼 수 있게 되고, 개인 혹은 공적인 주요 정보들이 인터넷을 통해 전달되면서 이들을 보다 안전하게 사용할 수 있는 환경을 요구하게 되었기 때문이다.

따라서, 국제적인 표준화 기구들에서도 이러한 시대적 요구에 따라 각종 정보보호 관련 표준화 업무를 진행하고 있다. 아태 지역의 정보통신 관련 업무를 담당하고 있는 아태전기통신협의체(APT : Asia-Pacific Telecommunity)에서도 1998년 2월 ASTAP (APT Standardization Program) Forum 이라는 지역 표준화 기구를 발족하여 현재까지 운영하고 있으며, 여기에는 정보보호 전문가 그룹이 2001년 설립되어 지금까지 아태지역의 정보보호 표준화 관련 업무를 수행하고 있다.

본 기고문에서는 제2장에서 ASTAP Forum의 현황을 소개하고, 제3장에서 정보보호 전문가 그룹에서 현재까지 진행되고 있는 각종 정보보호 표준화 활동을 소개하도록 한다. 마지막으로 ASTAP Forum의 활동 전략과 이를 통한 향후 정보보호 표준화 방향에 대해 언급하고자 한다.

Ⅱ. ASTAP Forum 소개

ASTAP Forum은 1998년 2월 아태지역의 표준화 활동 및 ITU, ISO등의 국제 표준화 기구에 회원국의 공동 입장을 반영하기 위해 설립된 기구이다. 이러한 아태 지역에서의 정보통신 표준화 활동을 위한 최초의 논의는 1996년 10월 인도 뉴델리에서 개최된 ESCAP (Economic and Social Commission for Asia and the Pacific) 장관회의에서의 관련된 결의안 채택으로부터 시작되었다. 이를 바탕으로 하여 APT는 정보통신표준화 활동을 통한 아태지역의 경제적 발전과 각 국가간의 상호 협력 증진 방안 모색을 위해 안정적인 정보통신표준화 활동의 프레임워크 구축 필요성을 인지하게 되었으며, 이후 일련의 APT 회의를 통해 1998년 2월 ASTAP

* 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 (bluesea@etri.re.kr)
** 한국전자통신연구원 정보보호연구본부 (chpark@etri.re.kr)
*** 충북대학교 자연과학대학 컴퓨터과학과 (shlee@chur.gbuk.ac.kr)

Forum이 설립된 것이다[1-2].

그러나, 아태 지역은 지역 내에 속한 회원국들간에 다양성과 이질성이 크며, 다른 한편으로는 인적·물적 자원이 부족하다는 점 때문에 전략적 차원의 지역 표준화 활동이 이루어지고 있는 형편이다. 즉, 처음부터 완전히 새로운 독창적인 표준의 개발 및 제안이 시도되기 보다는 국제 표준화의 장에서 논의되는 핵심 쟁점들을 지역적 특성에 따라 분석·검토하여 아태지역의 집약된 의견을 국제 표준화에 보다 효과적으로 반영하고, 나아가서는 동 지역의 전략적인 공동이익 도모를 위한 장기적 차원의 표준화 활동이 이루어질 필요가 있는 것이다[5-6].

지금까지 ASTAP Forum은 1998년 2월 태국 방콕에서의 제1차 회의부터 2002년 6월의 제6차 회의까지 방콕(1차, 4차), 싱가포르(2차), 서울(3차), 시드니(5차), 푸켓(6차)에서 개최되었다.

현재의 ASTAP Forum은 표 1과 같은 12개의 전문가그룹(Expert Group)으로 구성되어 있다[3]. NGNNM EG는 기존의 NSM(Network and Service Management for IP World) EG에서 2002년 6월 제6차 회의에서 확대 개편된 EG이며, 차세대 네트워크에 대한 아태지역의 표준화 방향을 상호 교환하기 위한 그룹이다. IMT EG는 IMT표준화와 관련된 국제기구에서의 표준화 동향에 대한 아태지역의 의견 수렴을 주요 목적으로 하고 있다. FWA EG는 아태지역 국가간 FWA관련 표준화 활동을 증진하고 상호 동의된 기고서를 ITU에 기고하기 위한 활동을 추진하고 있다. ITS EG 에서는 아태지역간 ITS에 관한 표준화 활동을 증진하고 관련된 표준화 문건을 ITU에 제안하기 위한 그룹이다. IA EG는 IOP (Interoperability) 시험 방법론 및 프레임 워크를 정립하고, 아태지역 국가간 서비스 및 제품 정보를 교환하며, APII 테스트베드와 관련된 기술적 이슈들을 논의하기 위한 그룹이다. ATM EG는 아태지역국가간 ATM/xDSL 표준화 등에 대한 정보를 교환하며, 아태 지역에서의 서비스 및 제품간 상호 호환성 확보를 위한 활동을 추진하고 있다. IRT EG 는 아태지역에서의 인터넷 관련 표준화 활동을 추진하기 위한 그룹이며, 아태지역내의 인터넷 활성화를 위한 인식제고에도 상호 협력하고 있다. DMB EG는 아태지역의 디지털 방송등과 관련된 표준화 활동을 담당한다. HAPS EG는 아태지역간 HAPS 표준화 활동을 추진하여 관련 기고서를 ITU-R에 제출하기 위한 활동을 추진하고 있다. PSDRC EG는 2001년 10월 제5차 회의에서 신설된 그룹이며, 공공의 안전과 재난시의 긴급통신과 관련된 아태지역의 표준화를 담당하고 있다. metadata EG는 최근의 제6차 회의에서 신설된 그룹이며, ITU-T SG16과 관련된 메타데이터의 아태지역 표준화 의견을 수렴하기 위한 그룹이다.

마지막으로, 정보보호 전문가 그룹의 경우에는 2001년 4월 제4차 회의에서 한국과 일본이 각각 정보보호 전문가 그룹 신설을 제안하여, 두 가지 제안된 안을 기반으로 상호 협의를 거쳐 마련한 통합안이 ASTAP 총회에서 승인되므로써 신설되게 되었다[3-4,28]. IS EG는 PKI 연동, VPN(Virtual Private Network), 암호 알고리즘, ESM (Enterprise Security Management) 로그 포맷, AP-CERT (Asia Pacific Computer Emergency Response Team), 멀티캐스트 정보보호, 정보보증등과 같은 정보보호 표준화에 대한 아태지역의 의견을 수렴하기 위한 그룹이다.

Ⅲ. 정보보호 전문가 그룹의 주요 이슈

정보보호 전문가그룹 (Information Security Expert Group)의 주요활동목표는 아래와 같다[9,17].

- 아태지역에서의 정보보호 이슈들의 정리
- 아태지역에서의 정보보호 관련 상호 주요 관심사항의 교환 및 협력 증진 방안 모색
- 아래 항목들에 대한 아태지역 공동의 정보보호 관련 표준 제안
  - Utilization of cryptography on network
  - Security evaluation criteria and evaluation method on network
  - Firewall/IDS interoperability
  - VPN interoperability and new items
  - PKI interoperability
  - General guideline for CERT in Asia-Pacific region (Against for Hacking/Virus)
  - Mobile security
  - End-to-end security
  - Multicast security

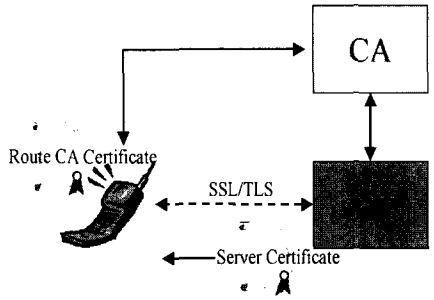
〔표 1〕 ASTAP Forum 전문가 그룹 현황

전문가 그룹	의 장
Next Generation Networks and Network Management (NGNNM)	Mr. Parthasarathy Ganesh(인도), Mr. Sanjeev(Sam) Mangar(호주), Mr. Pitikorn Tengtrakul(태국)
IMT-2000 and Beyond (IMT)	Mr. Kazuyuki Nagatomi(일본), Ms. Ju-Yeon Song(한국)
Fixed Wireless Access (FWA)	Mr. Hideyuki Maruyama(일본)
Intelligent Transport System (ITS)	Mr. Satoshi(Sam) Oyama(일본)
Interoperability/ APII Backbone Network (IA)	Mr. Jongjin Sung(한국), Dr. Joon-won Lee(한국)
ATM/xDSL (ATM)	Dr. Jae-Jin Lee (한국), Mr. Patrick Emery (호주)
Internet-related Topics (IRT)	Dr. Hui-Lan Lu(일본), Dr. You Hyeon Jeong(한국), Dr. Shin-ichi Nakagawa(일본)
Digital Multimedia Broadcasting (DMB)	Mr. Yukihiro Nishida (일본)
High Altitude Platform Stations (HAPS)	Dr. Katsuhiko Kosaka (일본)
Information Security (IS)	Mr. Dong-Il Seo(한국), Mr. Hiroshi Takechi(일본)
Public Safety and Disaster Relief Communications (PSDRC)	Mr. Ashok Kumar(인도), Dr. Graeme King(호주)
Metadata	Dr. Hideki Yamamoto(일본)

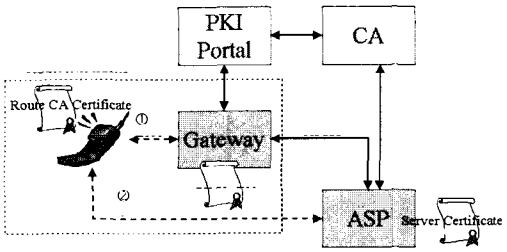
1. PKI related

PKI 기술을 활용한 secure mobile system 구현에 관한 가이드라인 권고안을 2001년 10월 제5차 회의에 일본측이 기고하였다. 본 기고서는 ITU-T SG17 Question 10에 아태지역 국가 전체 의견으로 기고하기 위하여 먼저 ASTAP Forum에 제출된 것으로써, 차세대 유무선 환경에 있어서 PKI 기술을 활용할 수 있는 구현 방법에 대한 가이드라인 내용을 포함하고 있다[26].

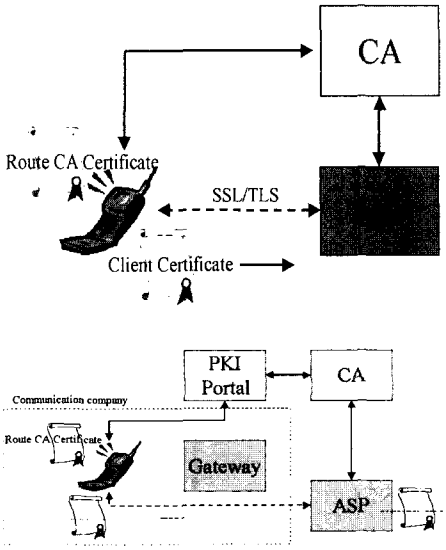
예를 들어, WTLS(Wireless Transport Layer Security), SSL(Secure Socket Layer), TLS (Transport Layer Security) 서버 인증의 경우 그림 1과 같은 구현 방법으로 PKI 기술을 활용한다. 마찬가지 방법으로 클라이언트 인증의 경우에는 그림 2와 같은 구현 방법을 활용한다.



- CA(Certification Authority)
- ASP(Application Service Provider)



〔그림 1〕 WTLS/SSL/TLS 서버 인증.



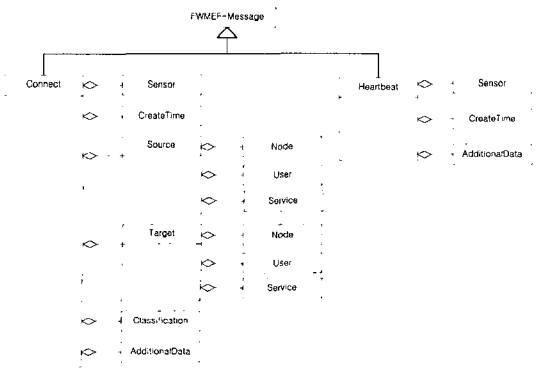
〔그림 2〕 WTLS/SSL/TLS 클라이언트 인증.

본 기고서는 전문가그룹에서 매우 많은 논란 끝에 각국의 의견을 수렴한 다음 ITU-T SG17에 기고하기로 하였으며, 결론적으로 지난 2002년 2월 ITU-T SG17 Q10 회의에 기고되었고 관련 권고안 제정을 위한 baseline document로 동의되었다.

PKI Interoperability를 위한 프로파일 권고안이 지난 2002년 6월 회의에 한국측에 의해 기고되었다[16]. 본 기고문은 제안자에 의해 ASIA PKI Forum에서 제정이 동의된 것으로 설명되었으나, EG 에서는 사설 기관에서의 제정 권고안을 아태지역 표준 문건으로 제정할 수 있는지에 대한 논란이 많았으며 추후 더 많은 검토와 협의가 필요할 것으로 동의되었다. 특히 본 권고안의 내용은 한국, 일본, 싱가포르의 PKI 프로파일을 상호 호환할 수 있도록 제정된 것으로써 그 효과가 매우 클 것으로 예상되었으나, 일본측 전문가 그룹에 의해 추후 검토가 필요한 것으로 동의 되었다.

2. ESM 표준화

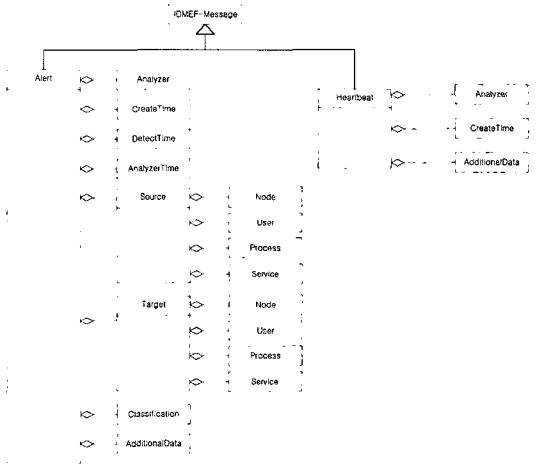
ESM 표준화와 관련된 전문가 그룹에서의 활동은 주로 침입차단시스템(Firewall) 및 침입탐지시스템 (IDS : Intrusion Detection System)의 로그 포맷에 대한 표준화 노력이다. 2001년 10월의 제5차 ASTAP Forum 회의에 한국측에서 침입차단시스템 로그 기록 포맷과 침입탐지시스템의 로그 기록 포맷 표준화에 대한 2건의 기고서를 제출하였다. 여기에는 국내의 인터넷보안기술포럼(ISTF)에서 제정하였던 침입차단시스템 및 침입탐지시스템의 로그 포맷에 대한 표준 문서의 내용을 반영한 것이다. 그러나, 전문가 그룹에서의 논의 결과는 구체적인 표준 내용에 대한 논의는 없었으며, 이러한 표준



〔그림 3〕 침입차단시스템 로그의 클래스 구조.

권고안이 ASTAP Forum에서 제정하는 것이 올바른 가에 대한 논의가 많아 최종적으로는 아태지역의 국가에 정보제공을 위한 기고서 발표로 동의되었다. 침입차단시스템 로그 포맷 기고서의 주요 내용은 그림 3과 같은 침입차단시스템 로그의 클래스 구조와 이들 각각의 클래스에 대한 구체적인 포맷을 포함하고 있다[18].

침입탐지시스템 로그 포맷에 대한 기고서의 주요 내용은 그림 4와 같은 침입탐지시스템 로그의 클래스 구조와 이들 각각에 대한 구체적인 로그 포맷을 규정하고 있다[21].



〔그림 4〕 침입탐지시스템 로그의 클래스 구조.

2002년 6월에 개최된 ASTAP Forum 제6차 회의에는 상기 기고서의 내용을 추가적으로 보완한 기고서 1건을 한국측에서 제출하였다. 본 기고서의 주요 내용은 지난 제5차 회의에 발표하였던 침입차단시스템 및 IDS 로그 포맷 문서에 최근의 IETF (Internet Engineering Task Force) 회의 결과를 반영한 부분 추가, 문구의 일부 수정 등을 제안한 것이다[15].

그러나, 전문가 그룹에서는 이러한 IETF 관련 표준 문건을 아태지역의 이름으로 ITU 혹은 ISO 표준기구에 기고하는 게 과연 올바른가에 대한 논의가 많았으며, 오히려 IETF IDWG 워킹그룹에 기고하는 게 올바른 것이 아니냐는 의견이 있었다. 또한, ITU에 기고하기를 원한다면 ITU-T SG17이 아닌 SG16에 기고하는 것이 어떻겠느냐는 의견이 있었다.

3. IMT-2000 & beyond

지난 제6차 회의까지 IMT-2000 관련하여 논의된 사항은 주로 암호 알고리즘과 관련된 것들이다. 그러나, 특정한 암호 알고리즘을 언급하기 보다는 IMT-2000과 관련된 암호 알고리즘을 표준화하여야 한다는 당위성을 논의하고, 아태지역의 IMT-2000 시스템에서는 공통적인 암호 알고리즘을 사용하여야 편리할 것이라는 원론적인 논의 수준에 있다.

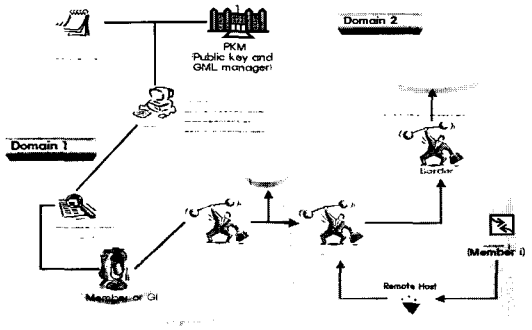
또한, 차세대 이동통신을 위한 암호 알고리즘과 같은 정보보호 요구사항을 연구하여야 한다는 것에 대해 상호 의견을 교환한 수준이다[10].

제5차 회의에서는 IMT-2000을 포함하여 end-to-end security를 연구하여야 한다는 점에 전문가 그룹에서 동의한바 있다[23].

4. Multicast Security

멀티캐스트 키교환 프로토콜과 관련된 4건의 기고서가 지난 제6차 회의에 한국측에 의해 기고되었다. 기고서의 주요 내용은 멀티캐스트 키 관리를 위한 구조[11], 무선 멀티캐스트 서비스에서의 그룹 서명 방법[12], 무선 멀티캐스트 키의 refresh 방법[13], 유무선 멀티캐스트 키의 통합관리 모델[14]을 각각 제안한 것이다.

제안된 멀티캐스트 키관리 구조는 그림 5와 같다. 여기에서 도메인과 보더(border)를 위한 PKM (Public Key Manager)은 오직 한개가 존재하며, 각각의 도메인에는 한개의 DKM (Domain Key Manager)이 존재하여 모든 서브그룹 매니저를 관리한다. 각각의 서브그룹내에는 한개의 DKA (Domain Key Agent)가 있으며 이들은 멀티캐스트 서브그룹 구성원과 세션키를 관리한다.



〔그림 5〕 멀티캐스트 키관리 일반 구조.

논의 결과 전문가 그룹에서는 매우 흥미있고 유용한 기고문 이라는데 동의 하였으나, 이들 기고문을 어떻게 ITU-T에 기고할 것인지에 대한 구체적인 작업 방법과 향후 일정을 제시해 줄 것을 발표자에게 요구하였다.

5. Asia-Pacific CERT

최근 인터넷의 활용이 급증하는 것과 비례하여 사이버테러 현상도 매년 급증하는 추세를 보이고 있다. 특히, 최근의 해킹/바이러스 기술의 동향은 각각의 기술이 통합되어 나타나고 있으며, 분산서비스 거부공격 보다 더욱 더 방어하기 힘든 분사반사서비스거부(DrDOS : Distributed Reflection Deny of Service) 공격과 침입차단시스템 회피기술을 채용한 피카부티(peekabooty) 기술, 인터넷 감청 기술을 무력화시키는 카메라/샤이 프로그램, 더욱더 지능적인 웜바이러스 등이 출현하고 있는 상태이다. 이러한 기술들을 채용한 사이버테러 공격은 어느 한 지역 혹은 국가에서 전체적인 상황을 파악할 수 없을뿐더러 이를 방어할 수도 없다는 데 문제의 심각성이 존재한다.

따라서, 이러한 사이버테러 공격 상황을 상호 정보 교환하며 침입자/공격자를 역추적하기 위한 업무 협조가 필수적이라는데 EG에서는 의견을 같이 하였으며, 관련된 표준화도 진행하여야 할 것으로 동의되었다. 그러나, CERT 관련 업무는 또다른 표준화 기구에서 진행하고 있으므로, ASTAP Forum에서는 적절한 수준의 가이드라인 문서를 제정하는 것이 좋을 것으로 EG에서 동의하였다[22].

6. 암호 알고리즘

암호 알고리즘과 관련된 기고서는 한국측에 의해 3건의 기고서가 지난 제5차 회의에 제출되었다. 여기에는 EC-KCDSA[19], KCDSA (Korea Certificate based Digital Signature Algorithm)[20], SEED[25]가 포함되어 있다. EC-KCDSA 및 KCDSA 암호 알고리즘은 비대칭 디지털 서명을 위한 것이며, SEED 알고리즘은 Block Cipher Algorithm 이다.

그러나, 이들 암호 알고리즘 관련 기고서들은 전문가 그룹에서 과연 아태지역 표준으로 제정할 필요성이 있는가에 대해 의문을 표현한 의견이 많아 더 이상의 작업이 이루어지지 않았다.

7. 기 타

가상사설망을 위한 정보보호 이슈들에 대해서도 전문가그룹에서는 관심을 가지고서 논의하기로 하였으며, 현재까지는 여러 가지 VPN 관련 이슈들을 리스트해 놓은 상태에 있다[24].

이외에 PKI의 디지털 서명에 사용되는 프로파일에 대한 기고서가 지난 제5차 회의에 제출된 적이 있으며[27], 이를 Asia PKI forum에 제출하는 게 어떻겠느냐는 전문가 그룹의 의견이 있었다.

제6차 ASTAP Forum 회의에서는 지난 2002년 2월 ITU-T SG17 Q10 회의에서 논의되었던 ISMS (Information Security Management System)에 대해서도 발표되었다[9].

Ⅳ. 결 론

지금까지 ASTAP Forum의 개요에 대해서 알아본 후, 정보보호 전문가 그룹에서 발표되었거나 논의되었던 주요 이슈들에 대해 분석해 보았다. 전문가 그룹에서 논의된 주요 항목들은 PKI 관련 표준화, 암호 알고리즘, 멀티캐스트 정보보호, 해킹/바이러스 대응, ESM 표준화, VPN 정보보호, IMT-2000 암호 알고리즘등에 대한 것들이었다. 특히, ASTAP Forum의 12개 전문가 그룹 중에서 정보보호 전문가 그룹은 2001년 4월 제4차 회의에서 신설된 짧은 역사에도 불구하고 이미 ITU-T SG17에 중요한 두 편의 기고서를 제출하여, 권고안 작성을 위한 base document로 채택되는 성과를 거두고 있다.

그러나, ASTAP Forum은 아직 회원국들의 기술 격차가 심해 상호 기술 협력이나 최신 정보 수집을 기대하기는 어려우며, 중국, 일본, 호주 등을 포함한 아태지역 공동의 이름으로 ITU, ISO등에 표준 제안을 할 수 있어 표준 제안의 무게가 실릴 수 있다는 장점이 있다. 특히, 정보보호 전문가 그룹의 경우에는 한국측의 노력 여하에 따라 초기 아태지역에서의 주도권 확보가 가능하므로, 국제 표준화 활동 및 아시아 시장 진출과의 상호 연계를 위한 정부 및 민간 차원의 지속적인 관심과 활동이 필요할 것으로 생각된다.

참고문헌

[1] APT, "Proceeding of Meeting on Regional Co-operation in Standardization", 1994. 5. 25.~27.

[2] 박기식, 김영태, 진병문, 조인섭, "아태지역의 정보통신 표준화 활동 출범과 향후 전망", ETRI 주간기술동향, 1998. 4. 20.

[3] http://www.aptsec.org/astap, 2002. 7

[4] ASTAP Forum, "Proceeding of 4th ASTAP Forum", 2001. 4. 3.~5.

[5] 김영태, 박기식, "아태지역 발전을 위한 지역 표준화 활동 추진전략", ETRI 주간기술동향, 1999. 5. 8.

[6] 김영태, 박기식, "APT의 정보통신표준화 추진 전략 및 활동 동향", ETRI 주간기술동향, 2000. 9. 6.

[7] ASTAP Forum, "Proceeding of 5th ASTAP Forum", 2001. 10. 31.~11. 2.

[8] ASTAP Forum, "Proceeding of 6th ASTAP Forum", 2002. 6. 4.~6.

[9] ASTAP Forum, "Meeting report of the IS EG (Information Security Expert Group)", ASTAP02-FR06-PL-56, 2002. 6. 4.~6.

[10] ASTAP Forum, "A Proposal for the establishment of IMT-2000 and Beyond research trend for ASTAP", ASTAP02-FR06-EG.IS-05, 2002. 6. 4.~6.

[11] ASTAP Forum, "A Multicast Key management Architecture", ASTAP02-FR06-EG.IS-06, 2002. 6. 4.~6.

[12] ASTAP Forum, "A Nominative Group Signature Method on Wireless Multicast Service", ASTAP02-FR06-EG.IS-07, 2002. 6. 4.~6.

[13] ASTAP Forum, "A Wireless Multicast key Refresh Method", ASTAP02-FR06-EG.IS-08, 2002. 6. 4.~6.

[14] ASTAP Forum, "An Integrated Wire and Wireless Multicast Key Management Model", ASTAP02-FR06-EG.IS-09, 2002. 6. 4.~6.

[15] ASTAP Forum, "The comments on ASSTAP01-FR05-EG.IS-05 and 08", ASTAP02-FR06-EG.IS-10, 2002. 6. 4.~6.

[16] ASTAP Forum, "Recommended Profile

for PKI Interoperability", ASTAP02-FR06-EG.IS-11, 2002. 6. 4.~6.
[17] ASTAP Forum, "Meeting report of the IS EG (Information Security Expert Group)", ASTAP01-FR05-PL-62, 2001. 10. 31.~11. 2.
[18] ASTAP Forum, "A proposal of a standardization work item, Firewall system log format", ASTAP01-FR05-EG.IS-05, 2001. 10. 31.~11. 2.
[19] ASTAP Forum, "The Korean Contribution for Asymmetric Digital Signature (EC-KCDSA)", ASTAP01-FR05-EG.IS-06, 2001. 10. 31.~11. 2.
[20] ASTAP Forum, "Proposal for an asymmetric digital signature algorithm KCDSA (Korea Certificate based Digital Signature Algorithm)", ASTAP01-FR05-EG.IS-07, 2001. 10. 31.~11.2.
[21] ASTAP Forum, "A proposal of a standardization work item - Intrusion Detection System Log Format", ASTAP01-FR05-EG.IS-08, 2001. 10. 31.~11. 2.
[22] ASTAP Forum, "Proposal for the study items against Hackings/Viruses", ASTAP01-FR05-EG.IS-09, 2001. 10. 31.~11. 2.
[23] ASTAP Forum, "Proposed Issues for Information Security", ASTAP01-FR05-EG.IS-10, 2001. 10. 31.~11. 2.
[24] ASTAP Forum, "A topic proposal of information security EG (VPN)", ASTAP01-FR05-EG.IS-11, 2001. 10. 31.~11. 2.
[25] ASTAP Forum, "Proposal for a Block Cipher Algorithm SEED", ASTAP01-FR05-EG.IS-12, 2001. 10. 31.~11. 2.
[26] ASTAP Forum, "Proposal on the new study item on "Guideline for implementation of secure mobile systems based on PKI technology", ASTAP01-FR05-EG.IS- 13, 2001. 10. 31.~11. 2.
[27] ASTAP Forum, "Digital signature certificate and certificate revocation list profile", ASTAP01-FR05-EG.IS-15, 2001. 10. 31.~11. 2.
[28] 장명국, "제4차 ASTAP 회의", TTA 저널, 통권75호, pp.112~115. 2001.5.
[29] 서동일, "ASTAP Forum에서 정보보호 표준화 동향", TTA 2002년도 2/4분기 IT 국제표준화 전문가 활동 결과 발표회, 2002.7.5.
[30] 한국정보통신기술협회(TTA), 2001년도 정보통신표준화 백서, pp.381~397, 2001.12.

〈著者紹介〉

서 동 일 (Seo, Dong-il)
정회원
1989년 2월 : 경북대학교 전자공학과 졸업
1994년 2월 : 포항공과대학교 정보통신공학과 석사
2000년 3월~현재 : 충북대학교 전자계산학과 박사과정
1994년~현재 : 한국전자통신연구원 선임연구원
관심분야 : 인터넷 정보보호, 컴퓨터 통신, 네트워크

박 치 항 (Park, Chee-Hang)
정회원
1974년 2월 : 서울대학교 응용물리학과 졸업
1980년 2월 : 한국과학원 전자계산학과 석사
1987년 12월 : 파리6대학 전자계산학과 박사
1978년 2월~현재 : 한국전자통신연구원 책임연구원 (본부장)
관심분야 : 멀티미디어, 정보보호, 데이터베이스

이 상 호 (Lee, Sang-Ho)
정회원
1976년 2월 : 숭실대학교 전자계산학과 졸업
1981년 2월 : 숭실대학교 전자계산학과 석사
1989년 2월 : 숭실대학교 전자계산학과 박사
1981년~현재 : 충북대학교 컴퓨터과학과 교수
관심분야 : 네트워크 보안, 망관리, 프로토콜