ISO/IEC JTC1/SC27 서울총회

이경석
산업연구원 전산정보실장
JTC1/SC27-Korea 위원장

1. 회의 개요

정보보안기술 국제표준화위원회(ISO/IEC JTC1/SC27) 회의가 지난 10월 15일부터 24일까지 서울 ASEM 회의장에서 개최되었다. 이번 서울회의는 제23차 SC27 Working Group 회의(2001. 10. 15~10. 20)와 제13차 SC27 총회(2000. 10. 22~10. 24)가 동시에 개최되었다. 우리나라와 미국, 프랑스, 영국, 일본 등을 포함한 19개 국에서 총 120여 명이 참석한 이번 회의에는 말레이지아, 인도 및 남아프리카공화국 등의 3개국 대표가 처음으로 참석하여 정보보안 분야에 대하여 높은 관심을 보이고 있음을 알 수 있었다. 그리고 정보보안에 대한 국제적인 관심이 더욱 고조되고 있는 시점에 개최된 ISO/IEC JTC1/SC27 서울 국제회의는 국내에서의 보안기술 국제표준화에 대한 인식제고와 국내 보안기술 발전에 좋은 계기가 되었다.

정보기술의 보안기법에 관련된 서비스와 지침 및 일반적인 요구사항, 보안기술과 기법, 그리고 보안 평가기준 등의 기고문의 발표 및 표준화 작업을 수행하기 위한 회의로서, 최근 정보보안 문제가 각 분야에서 심각한 문제로 대두되고 있는 시점에서 보안기술의 표준화를 위한 국제회의가 서울에서 개최되어 많은 국내 전문가가 참여하여 국내의견을 적극적으로 반영할 수 있는 계기가 되었다. 한편, 모든 국제회의 진행에서 필요한 요소중의 하나인 외부와의 통신기능 제공을 위하여 이번 서울회의에서는 SC27 회의 개최이래 처음으로 국내 기업이 제공한 무선 LAN을 설치하여 각국 대표들이 인터넷이나 e-mail 사용 등의 무선통신망을 제한없이 사용할 수 있도록 지원하여 많은 찬사를 받았다.

SC27 총회는 ISO와 IEC의 공동기술위원회(JTC1) 산하의 정보기술 보안에 대한 국제표준 제정을 위한 국제회의로서 각국에서 임명한 정식 대표단이 모여 자국의 기술과 의견을 반영하는 회의이며, 현재 산자부 기술표준원에서 국내 간사기관(NB)를 담당하고 있고 SC27 간사는 독일의 DIN에서 맡고 있다. ISO/IEC JTC1/SC27에서는 정보기술의 보안사항중 보안메커니즘, 알고리즘, 평가방법, 보안서비스등에 대한 표준화 작업을 담당한다.

그리고 표준은 IS(International Standard)와 TR(Technical Report) 등 2가지로 작업이 이루어지고 있으며, IS 바로 이전 단계를 DIS(Draft IS)라고 하며, 현재 JTC1/SC27에는 3개의 WG(working group)이 운영되고 있으며, 각 WG의 Convener는 다음과 같다.

- WG 1(Requirements, security services and guidelines): Ted Humphreys(영국)
- WG 2(Security techniques and mechanisms) : Marijke De Soete(벨기에)
- WG 3(Security evaluation criteria): Mats Ohlin(스웨덴)

2. 주요 토의내용 및 결과

각 WG별로 토의된 주요 사항은 다음과 같다.

1) Guidelines for the management of IT security - Part 1: Concepts and models for IT Security

제1부는 주로 상위 경영자를 위한 지침으로 간략하고 명료하게 문서를 재작업하기로 하였으며, 캐나다의 Alice Sturgeon이 editor를 맡고 있다. 그리고 거의 모든 절에 불분명하고 기술적 상세사항 부분은 삭제하였으며, 3절의 정의 부분에 대해 타 표준과의 일관성을 위해 가능한 한 참조하여 개정하였고, 11절의 내용을 일부 삭제하고 일부는 10절이나 기타 다른 절에 삽입시키기로 하였다. 한편 한국에서 제안한 코멘트는 모두 채택되어 수정되었으며, 전반적으로 상당 부분 개정작업이 이루어졌다.

2) Code of practise for information security management

ISO/IEC 17799에 대해 많은 코멘트와 개정작업에 대한 필요성에 의거해 우선 로드맵을 작성하고 문서를 개정한 후, 이 새로운 문서에 기초하여 각국에서 작성한 코멘트를 확인하는 과정을 거치기로 하였으며 현재 독일의 Oliver Weissmann이 acting editor를 맡고 있다. 그리고 17799내에 불분명한 구절이 상당 부분 있고 정의가 생략되었거나 통제와 지침이 혼합되어 있어 '통제(Control)', '고려사항(Factors to take into considerations)', '지침(Guidelines)' 및 '기타 정보(Other information)' 등으로 본문을 재구성하기로 하였다. 편집팀들은 현재의 문서를 위의 구성체계로 재작업하고 그 결과를 11월 30일까지 편집인에게 제공하기로 하였으며 한국 대표단의 중앙대 김정덕 교수도 3절과 4절의 개정작업에 참여하기로 결정하였다. 한편, 남아프리카공화국의 ISO/IEC 17799의 단계별 적용에 관한 제안에 대해 남아공 대표인 Jan Eloff 교수에게 해당 제안을 정리하여 그 결과를 2002년 1월 7일까지 WG 1 간사에게 전달하여 Study and Comment를 위해 각 회원국에 배포하기로 하였다.

3) Time stamping services - Part 1: Framework

현재 IETF 문서로부터 ANS.1 표기를 차용해서 표기하고 있으나, 이번 서울회의에서 WG2에서 작업하는 표준은 ISO/IEC 표준이므로 time stamping 메시지구조에 대한 ASN.1 표기가 불충분하다는 미국안을 수용하고 제1부에

사용된 ASN.1 notation을 재정비하여 표준에 싣기로 하였으며, Annex의 목차가 본문의 목차와 혼동되는 것을 방지하기 위하여 Annex 목차는 annex 번호로 시작하기로 하였다.

4) Time stamping services - Part 2: Mechanisms producing independent tokens

제1부 회의결과처럼 ASN.1 표기를 재정비해서 싣기로 하였다. 한편, validation과 verification 용어의 차이에 대한 논의에서 validation은 time stamp stamp request에 대한 response를 검증하는 것이고, verification은 나중에 time stamp token을 검증하는 절차를 지칭하는 것으로 결정하였다.

5) Time stamping services - Part 3: Mechanisms producing linked tokens

time stamp request, validation, verification에 대해 설명하고, 각 operation의 신뢰도의 level에 대한 정보를 부록에 데이터 등을 포함해서 보충 설명하기로 하였으며 first CD 투표단계를 거치기로 하였다.

6) Encryption Algorithm

각 국가의 기술적 코멘트 검토에서 일본은 64 비트 블록암호에 MISTY를, 128 비트 블록암호에 CAMELIA를 제안하였으며, 캐나다는 64 비트 블록암호 CAST 외에 128비트 블록암호 CAST-128을 추가적으로 제안하였고, 한국은 SEED의 S/W 및 H/W 효율성 부분에 대한 AES와의 비교평가 결과를 제출하였다. 그리고 현재 국가표준 암호알고리즘인 경우는 이미 안전성이 널리 평가받은 것으로 고려하며, 제안 알고리즘의 18033-1의 요구조건의 만족여부를 각 제안국이 12월 말까지 문서로 작성하여 송부하며, 현재 표준안에 올라있는 TDES와 AES 이외에 제안된 알고리즘 CAST-128, IDEA, MISTY1, Camellia, SEED, RC6을 3rd WD에 첨가하기로 하였다. 블록암호알고리즘의 ISO/IEC 표준 문서에 포함시킨 것은 현재 64 비트 블록암호알고리즘인 TDES와 128 비트 블록암호알고리즘인 AES 뿐이다.

7) Working group 3 관련

CCIMB와 WG3와의 연계부분에 많은 논의가 있었으며, 회의참석자 중 상당수는 CCIMB가 그 역할을 제대로 수행하지 못한다고 생각하고 있어서 이번 회의에서 CCIMB와 WG3에 관계개선을 위한 기고를 작성하였다. 그리고 CC 기반의 평가방법론과 PP 및 ST 작성 가이드에 있어서 일본은 지대한 관심을 보였으며, 단순히 편집에 대한 제안뿐만 아니라 전반적인 내용에 대하여 전문적인 의견을 적극적으로 제안하여 그 내용은 대부분 그대로 수용되거나 일부 수정되어 수용되었다. 특히, 프랑스는 CC 기반의 스마트카드 평가에 큰 관심을 보였다.

3. 기타 관련사항

1) 프로젝트 명칭 변경

"Guidelines for the Implementation, Operations and Management of Intrusion Detection Systems"에서 "Guidelines for the Implementation, Operation and Management of Intrusion Detection Systems"로 변경하였으며, "Security Incident Management"에서 "Information Security Incident Management"로 명칭을 개정하기로 하였다.

2) Biometric techniques

현재 생체인식 기술의 표준화와 연관된 기관들(ISO/IEC JTC 1/SC 17, ISO TC 68 및 ITU-

T Q13/SG17 등에서 작업이 진행중인 Biometric techniques에 대하여 SC27에서 표준화 작업진행 여부에 대한 검토결과 각국의 대표기관에 의사를 타진하기로 했다.

3) SC27 차기회의(WG 및 Plenary) 일정

- 2002년 WG 회의 : 독일(4월 22일 - 26일)
- 2002년 WG 회의 및 총회 : 폴란드(10월 7일 - 15일) (2002년 회의부터 총회기간을 2일간으로 조정하기로 결정)
- 2003년 WG 회의 : 캐나다(신청) (4월)
- 2003년 WG 회의 및 총회 : 미정 (10월)

4) 기타

이번 SC27 서울회의는 지난 9월 미국의 비행기 테러사건 이후에 처음 개최되는 정보보안기술 표준화 회의라 참석을 신청한 위원 중 미국 정부 관련 기관과 유럽의 다국적 기업에 종사하는 10 여명의 대표들의 참석 취소사태가 일어났으나, 각자의 의견을 메일로 보내거나 대리발표 등으로 회의진행이나 각 프로젝트의 작업진도에는 별 지장이 없었다.

ETRI, IPv4-IPv6 연동기술 개발

한국전자통신연구원(ETRI)은 11월 18일 차세대인터넷표준연구팀(팀장 김용진)이 IPv4 기반의 현 인터넷주소체계와 이를 대체할 차세대 인터넷주소체계인 IPv6의 주소와 프로토콜을 연동하는 기술을 개발했다고 밝혔다. 이번에 개발한 IPv4 IPv6 주소변환기는 개방형 운영체제(OS)인 리눅스 기반으로 라우터에 임베디드용으로 사용하는 하드웨어 변환기와 인터넷망사업자(ISP)가 프로그램을 설치해 사용하는 소프트웨어 변환기 2가지다. 하드웨어 장치는 영국 브리티시텔레콤(BT)이 유닉스 기반의 IPv4 IPv6 주소변환 소프트웨어를 간단한 응용프로그램 형식으로 개발한 적은 있지만, IPv4 IPv6 주소변환 모듈만을 제공하는 전용장치로는 이번이 세계 최초다. 연구팀은 "인터넷주소가 고갈되는 상황에서 무한대에 가까운 새로운 인터넷주소를 생성할 수 있는 128비트 체계의 IPv6가 차세대 인터넷주소 표준으로 채택될 단계에 있어 IPv4를 IPv6로 손쉽게 변환하는 기술이 필요하다"며 "이번에 ETRI가 개발한 기술은 IPv4와 IPv6 중간에서 상이한 주소체계를 연동, 호환시키는 것"이라고 설명했다. 연구팀은 또 "하드웨어 주소변환기는 임베디드 리눅스 라우터에 사용하며, 소프트웨어처럼 설치를 위한 전문인력이 필요없다"고 덧붙였다. 김용진 팀장은 "내년부터 IPv4 IPv6 주소변환과 관련한 네트워크장비 시장의 수요가 본격 형성될 전망"이라며 "이번 기술개발은 국내외 차세대인터넷망 구축과 도입시기를 앞당기는 데 도움이 될 것"이라고 말했다. ETRI는 이번에 개발된 기술을 11월 21일 서울 역삼동 한국과학기술회관에서 열리는 기술이전 설명회에서 발표하였다.