通信情報保護學會誌
第5卷 第4號, 1995. 12

ISO/IEC JTC1/SC27의 국제표준 소개 (10) : SC27(정보보호기술) 서울 회의 참가보고서

(Meeting report on SC27(Information Security Technology) Seoul Meeting)

이 필 중*

요 약

본 학회지의 1993 년 6 월호에 ISO/IEC JTC1/SC27에 대한 소개를 한 이후로 매호마다 SC27 에서 제정된 표준(IS 10118-1, 9798-4, 9798-3, 9798-2, 9798-1, 9796, 8372, 10116, 9797)을 소개해 왔다. 이번호에는 지난 11 월 서울에서 열렸던 국제 표준화회의를 소개함으로써 SC27 표준화의 현 주소, 첫번째의 소개 이후의 진척 상황, 그리고 우리나라의 활동상 등을 파악할 수 있게 하였다.

I. 회의개요

1. **회 의 명** : ISO/IEC JTC1/SC27(IT Security Techniques) 11차 WG(working group) 회의 및 7차 SC27 총회

2. **주 관** : ISO/IEC JTC1/SC27

3. **주 최** : 대한민국 공업진흥청(KIAA)

4. **기 간** :
   WG 회의
   : 1995-11-02(목) ~ 10(금)
   HoD(head of delegations) 회의
   : 1995-11-13(월)
   SC27 총회 : 1995-11-14(화) ~ 15(수)

5. **장 소** : 서울 광진구 광진동 산 21, 쉐라톤 워커힐 호텔

6. **참석규모** :
   P 회원국 15 개국 : Australia, Belgium, Canada, Finland, France, Germany, Japan, Korea, Norway, Poland, Russia, Sweden, Switzerland, U.K., U.S. (한국을 제외하고 50 명정도)
   한국대표단 : 이 필중(HoD, 포항공대), 이 경석(산업연구원), 신 동익(한국전산원), 장 청룡(한국통신), 백 재현(국방과학연구소)
   기타 한국 참석자 : 임 정석(국방과학연

* 종신회원, 포항공과대학교 전자전기공학과

구소), 최 운식(한국전산원), 이 영 (백두정보), 임 채훈(포항공대), 안 금혁(한국통신), 류 재철(충남대), 차 성덕(KAIST) 외 7 명

: M. DeSoete (Belgium)
- WG3 Convener
: S. Knapskog (Sweden)
- Secretariat
: W. Wilke (Germany)

7. 참고사항 : SC27 조직

(국제위원회)

SC27 Chair : K. Vedder(Germany)
- WG1 Convener
: E. Humphrey (U.K.)
- WG2 Convener

(국내위원회)

이 필중(포항공대)
- 신 동익 (한국전산원)
- 이 경석 (산업연구원)
- 류 재철 (충남대)

II. SC27 서울 모임의 Project별 진척 사항

Project	WG	Editor (국명)	Title / Reference Document	Target dates CD/ PDTR	DIS/ DTR	IS/ TR
특기사항 (Acting editor ?, 한국의 누가 어떤 투표를 했으며 그 처리 결과, 한국의 누가 회의중 어떤 contribution을 했나, 회의의 결론 등 다른 특기 사항). 향후 진행 계획.						
01	2	Ruland (German)	Modes of operation for a 64-bit block cipher algorithm / IS 8372: 1987	2nd review in '95		
C. Ruland가 acting editor로서 editing meeting을 진행하였음. 한 NB(Canada)의 contribution 이 분실되어 고려되지 않아 다음 WG meeting에서 재검토하기로.						
02	2	Ruland (German)	Modes of operation for an n-bit block cipher algorithm / IS 10116: 1991, N1256	'95	'96	'96
C. Ruland가 acting editor로서 editing meeting을 진행하였음. 검토한 결과 이 IS를 수정하기로 하였음. Ruland를 정식 editor로 추천하였음. N1256을 첫 CD로 하여 투표절차를 밟기로. 다음 WG meeting에서 충분한 support를 받으면 첫 DIS로 투표절차를 밟기로.						
03			Entity authentication			
03.01	2	Preneel (Belgium)	: General model / IS 9798-1: 1991, N1257	'95	'96	'96

L. Nilson (Norway)이 acting editor로서 editing meeting을 진행하였음. 검토한 결과 이 IS를 수정하기로. 한국의 특별한 contribution은 없었슴. N1257을 SC27 Secretariat에게 95-12-15까지 보내어 첫 CD로서 투표 절차를 밟기로. 다음 WG meeting에서 충분한 support를 받으면 첫 DIS로 투표 절차를 밟기로.

03.02 2 WG2 : Mechanisms using symmetric encipher algorithms
IS 9798-2: 1994 review in '97

03.03 2 WG2 : Mechanisms using a public key algorithm
IS 9798-3: 1993 review in '96

03.04 2 WG2 : Mechanisms using a cryptographic check function
IS 9798-4: 1995 review in '98

03.05 2 Mitchell (U.K.) : Mechanisms using zero knowledge techniques
CD 9798-5, N1225 '95 '96 '97

M. King이 acting editor로서 editing meeting을 진행하였음. WD에 대한 한국(임 채훈)의 written contribution 중 사소한 기술적 지적들은 받아들여 졌으나 중요한 세 가지(GQ-based 만이 아니라 Schnorr-like scheme도 넣을 것. 단방인증 만이 아니라 쌍방인증도 넣을 것. 보안상의 문제점을 명시하라는 것)는 대안이 제시되지 않았다는 이유로 받아들여지지 않았다. N1225을 SC27 Secretariat에게 95-12-15까지 보내어 첫 CD로서 투표 절차를 밟기로. 다음 WG meeting에서 충분한 support를 받으면 첫 DIS로 투표 절차를 밟기로.

04 2 WG2 Data integrity mechanism using a cryptographic check function employing a block cipher algorithm
IS 9797: 1994 review in '97

06 Non-repudiation

06.01 2 Herda (Germany) : General model
CD 13888-1, N1274 '94 '96 '97

두 NB가 disapprove 했다. Japan은 현 draft가 너무 message transfer의 경우만을 고려하고 있으며 electronic transition과 payment로 범위를 확장해야 한다는 주장이었고 많은 공감을 얻었다. France의 투표는 너무 많은 constructive하지 않은 comment 만으로 되어있다며 이 project의 editor들이 불만을 나타냈고 일부만 받아들이기로 하였다. 다른 NB의 comment들은 주로 editorial comment 였다. 한국은 투표도 approve as is 였고 meeting에서도 특별한 contribution은 없었다. N1274을 SC27 Secretariat에게 95-12-31까지 보내어 CD급의 재투표 절차를 밟기로.

06.02 2 Morris : Using symmetric techniques
(U.S.) CD 13888-2, N1276 '94 '96 '97

France의 투표는 너무 많은 constructive하지 않은 comment 만으로 되어있다며 이 project의 editor들이 불만을 나타냈고 일부만 받아들이기로 하였다. N1276을 SC27 Secretariat에게 95-12-15까지 보내어 CD급의 재투표 절차를 밟기로.

06.03 2 vacant : Using asymmetric techniques
CD 13888-3, N1107 '95 '96 '97

Editor를 찾기로.

07 Digital signature schemes giving message recovery

07.01 2 WG2 : Mechanisms using redundancy
IS 9796: 1991 review in '95

M. Girault가 acting editor로서 editing meeting을 진행하였음. 내용은 수정없이 5년간 계속 사용을 승인하기로. Project 07를 2 개로 나누기로 하여 이름을 위와 같이 변경하기로.

07.02 2 Guillou : Mechanisms using a hash-function
(France) WD 9796-2, N1258 '96 '97 '98

M. Girault가 acting editor로서 editing meeting을 진행하였음. Project 07에 이 part를 추가하기로. 메시지가 너무 짧은 경우 padding하는 방법을 명시하자는 의견을 내어 통과. RSA와 hash를 사용하여 부가형 서명을 만드는 경우도 여기에 포함하기로. Guillou를 정식 editor로 추천하였음. N1258을 SC27 Secretariat에게 95-12-15까지 보내어 첫 CD로서 투표 절차를 밟기로. Comments due by 96-03-31. 다음 WG meeting에서 충분한 support를 받으면 첫 CD로 투표 절차를 밟기로.

08 Digital signature with appendix

08.01 2 Nyberg : General
(Finland) CD 14888-1, N1219 '95 '96 '97

Nyberg가 불참통고를 하면서 acting editor가 되기를 의뢰하여 이 필중이 acting editor로서 editing meeting을 진행하였음. 한국(이 필중)은 CD 안을 disapprove 하였었고 회의전까지 새로운 general model 제시할 것을 약속하였었다. 약속대로 input documents N1207를 만들어 회의에 임했다. 제 1 부 회의상 쟁점은 전 document는 너무 제 3 부와 조화를 이루지 못하지만 새로운 N1207의 모델은 제 2, 3 부와 너무 잘 일치하며 다른 경우를 포함하지 못할 가능성이 있다는 것이었는데 결국 새 문서에서는 앞부분에 일반화를 해서 넣고 뒷부분은 N1207을 기반으로 고치기로 하였다 (N1218). N1219을 SC27 Secretariat에게 95-12-15까지 보내어 CD급의 재투표 절차를 밟기로.

08.02 2 Nyberg : Identity-based mechanisms
(Finland) CD 14888-2, N1221 '95 '96 '97

역시 이 필중이 같은 이유로 acting editor로서 editing meeting을 진행하였음. 한국(이 필중)은 CD 안을 disapprove 하였었고 7 쪽의(전체분량의 반이상) 대체 안(제3부와 거의 유사한 모델을 제안하였으며 기존의 GQ 방식이외에 두가지를 더 예로 들었음)을 만들어 투표 결과에 포함시켰다. 그리고 input document로 조금 더 발전시킨 N1251을 만들어 회의에 임했다. 제 2 부 회의상 쟁점은 몇개의 알고리즘을 표준으로 하는가 였다. 한국의 주장인, 다른 것에 비해 장점이 있는 것이 많으면 여러 개가 표준이 되어야 하며 그 경우 모델이 있어야 한다는 것이 통과되어 N1251을 기반으로 하여 새로 CD 안을 만들기로 하였다(N1220). N1221을 SC27 Secretariat에게 95-12-15까지 보내어 CD급의 재투표 절차를 밟기로.

08.03 2 Morris : Certificate-based mechanisms
(U.S.) CD 14888-3, N1223 '95 '96 '97

한국(이 필중)은 CD 안을 Disapprove 하였었고 6 쪽의(전체분량의 반이상) 대체 안(모델을 더 일반화하였고 예로서 국내 표준안을 추가포함시켰다)을 만들어 투표 결과에 포함시켰다. Morris가 constructive 한 제안에 고마움을 표시하면서 우리가 제안한 모델을 따르기로 하였고, 한국표준안을 포함시키기로 하였다. N1223을 SC27 Secretariat에게 95-12-15까지 보내어 CD급의 재투표 절차를 밟기로.

09 Hash-functions

09.01 2 WG2 : General
IS 10118-1: 1994 review in '97

09.02 2 WG2 : Hash-functions using an n-bit block cipher
IS 10118-2: 1994 review in '97

09.03 2 Mitchell : Dedicated hash-functions
(U.K.) CD 10118-3, N1209 '94 '96 '97

M. King이 acting editor로서 editing meeting을 진행하였음. 주요한 issue는 두가지였다. 투표시 RIPEMD가 보안성이 약하다는 이유로 한국(김 철)을 포함한 많은 NB들이 반대를 하였고 이에 Preneel이 제안한 RIPEMD-160을 대신 포함시키기로 하였다. 투표시 Canada가 Internet에서 많이 쓰이고 있는 MD5을 포함시키자는 제안을 하였으나 Canadian Delegate의 불참과 다른 NB의 강한 주장이 없어 포함시키지 않기로 하였다. 한국에서 제안한 그밖의 다른 사소한 comment는 4 개중 2 개가 accept 되었다. N1209을 SC27 Secretariat에게 96-03-10까지 보내어 CD급의 재투표 절차를 밟기로. 다음 WG meeting에서 충분한 support를 받으면 첫 DIS 로 투표 절차를 밟기로.

09.04 2 Herda : Hash-functions using modular arithmetics
(Germany) CD 10118-4, N1211 '94 '96 '97
Belguim을 포함한 여러나라에서 Coppersmith의 새 공격방법을 예로 들면서 제안된 방식들의 취약성에 대한 많은 논란이 있었다. 결과로 5 절에서 modulus N의 크기가 소인수분해하기 어려울 정도로 커야함을 명시하고 A.3의 예로서 768 bits의 N을 사용하기로 하였다. 한국(이 은정, 포항공대)의 투표시 한 editorial comment들과 editing meeting에서 즉시 제안한 것들은 모두 accept 되었다. N1211을 SC27 Secretariat에게 95-12-15까지 보내어 CD급의 재투표 절차를 밟기로.

10 1 Humphreys Procedures for the registration of cryptographic algorithm
(U.K.) IS 9979: 1991 '96 '96 '97
Humphreys가 WG1 / N553, N600, N638을 근거로 IS 9979를 revise 하기로. 다음 WG meeting에서 충분한 support를 받으면 첫 PDTR로 투표 절차를 밟기로. 현재 U.K.의 NCC가 Registrar을 운영하면서 받는 fee가 너무 많으며 다른 NB들이 대신 할 생각도 있다는 뜻을 BSI에 전하기로.

13 1 McDonald Security Information Object
(U.K.) N1242 '96 '97 '98
McDonald를 정식 editor로 추천하였음. Security labeling과 병행하여 작업중이나 보다 많은 관심이 요구됨. Update N1242 by 95-12-01. Comments due by 96-03-09.

14 Guidelines for the management of IT security

14.01 1 Hopkinson : Concepts and models for IT security
(Canada) DTR 13335-1, N1227 '93 '95 '96
한국(신 동익)은 DTR 투표시 현재의 문서가 너무 risk management에 치중되어 다른 보안관리 방법론에 대한 추가와 ISO 9000과의 연관을 요청한 written comment를 contribution(WG1 / N588 에 포함됨)하였고 두가지 제안이 모두 채택되었으나 다만 ISO 9000과의 직접적인 연결은 피하기로. Update N1227 by 95-12-01. DTR로 재투표 절차를 밟기로.

14.02 1 Widmer : Managing and planning IT security
(Switzerland) PDTR 13335-2, N1229 '95 '96 '97
투표시 approve as is로 따로 contribution을 하지 못하였음. U.K., U.S., German 등이 제기하는 많은 의견들로 인해 수시로 전체적인 구조변경이 되고 있슴. Update N1229 by 95-12-01. N1229로 PDTR급의 재투표 절차를 밟기로. 다음 WG meeting에서 충분한 support를 받으면 첫 DTR로 투표 절차를 밟기로.

14.03 1 Plate : Techniques for the management of IT security

(Germany) **PDTR 13335-3, N1231 '95 '96 '97**

U.K., U.S., German 등이 제기하는 많은 의견들로 인해 수시로 전체적인 구조 변경이 되고 있슴. Update N1231 by 95-12-01. N1231을 첫 PDTR로 하여 투표 절차를 밟기로. 다음 WG meeting에서 충분한 support를 받으면 첫 DTR로 투표 절차를 밟기로.

14.04 1 Plate : Baseline approach

(Germany) **WD 13335-4, N1243 '96 '97 '98**

Study period에 있던 이 project를 GMITS와의 연관성으로 인하여 Project 14에 이 part를 추가하기로. 정보기술을 사용하는 모든 기관들이 준수해야할 최소한의 보안 요구사항을 결정하자는 것이 목적. Plate 를 정식 editor로 추천하였음. 두개의 안이 있었으나 한국은 U.K.안은 관리적인 부분만을 담고 있는 반면 German 안은 기술적인 부분에 치중하고 있어 혼합하는 방법을 제안 (WG1/N593, 신 동익)하여 전폭적으로 수용되었다. Update N1243 by 95-12-01. Comments due by 96-03-09.

14.05 1 Hopkinson : Application of IT security services and mechanisms

(Canada) **WD 13335-5, N1244 '96 '97 '98**

Study period에 있던 이 project를 GMITS와의 연관성으로 인하여 Project 14에 이 part를 추가하기로. Hopkinson을 정식 editor로 추천하였음. Document가 별로 개선되지 않았으므로 각국의 보다 적극적인 contribution이 요구됨. Update N1244 by 95-12-01. Comments due by 96-03-09.

16 Evaluation criteria for IT security

16.01 3 Troy : General model of security evaluation

(U.S.A) **N1269 '96 '97 '98**

CCEB(Common Criteria Editorial Board)에서 CC(Common Criteria)의 Part 1의 내용을 수정하기로 하여 SC27 WG3에서도 CC와의 일치를 위해 WD인 N1269를 95-12-15까지 update 하기로. Comments due by 96-03-09. 다음 WG meeting에서 충분한 support를 받으면 첫 CD로 투표 절차를 밟기로.

16.02 3 Nash : Functionality of IT systems, etc.

(U.K.) **N1270 '96 '97 '98**

Canada의 comments에 따라 evaluation sponsor로부터의 external guidance 없이는 평가그룹에서 보안정책의 적절성 여부를 판단하지 않기로. Editor는 non-repudiation 개념이 CC에서 충분히 반영되도록 CCEB와 계속 협조하기로. 그밖에도 German과 네델란드에서 제시한 comments도 반영하기로. Update N1270 by 95-12-15. Comments due by 96-03-09. 다음 WG meeting에서 충분한 support를 받으면 첫 CD로 투표 절차를 밟기로.

16.03 3 van Essen : Assurance of IT systems, etc.
(Germany) N1271 '96 '97 '98
CCEB의 Part 3을 본 과제에서 채택하지는 않기로. 그러나 CC의 Part 3가 SC27 WG3의 요구대로 변경할 가능성이 큼에 따라 추후에 다시 검토하기로. Level E1 to E3에 informal 보안정책개념을 삽입하기로. Annex D는 CC의 현재 version에 맞추어 수정하기로. "The evaluation criterion for protection profiles and security targets"라는 새로운 normative annex을 추가하기로. Update N1271 by 95-12-15. Comments due by 96-03-09. 다음 WG meeting에서 충분한 support를 받으면 첫 CD로 투표 절차를 밟기로.

18 Key management

18.01 1 Muller : Framework
(Germany) DIS 11770-1, N1233 '94 '95 '96
Update N1231 by 95-12-01. 첫 DIS로 투표 절차를 밟기로.

18.02 2 Fumy : Mechanisms using symmetric techniques
(Germany) IS 11770-2: new, N1213 review in '96
한국의 DIS 문서를 approve as is 하였었고, 회의 중에도 별 contribution이 없었다. N1213을 SC27 Secretariat에게 96-01-15까지 보내어 첫 IS로 출판 절차를 밟기로.

18.03 2 Rueppel : Mechanisms using asymmetric techniques
(Switzerland) CD 11770-3, N1110 '93 '96 '97
CD급의 재투표 절차를 밟을 수 있도록 editor에게 95-12-15까지 N1110를 제출할 것을 독촉. 날짜를 맞추지 못할 때에는 다음 WG meeting에서 editor를 교체하기로.

18.04 2 vacant : Cryptographic separation
X X X
과거 2 년간 editor도 없고 contribution도 없어서 이 project를 표준화시키지 않기로.

19 Guidelines on the use and management of trusted third-party services

19.01 1 Grissonnanche : General overview
(France) N1235 '96 '97 '98
Project 19를 나누어 두개의 세부과제로 하기로. Grissonnanche을 정식 editor로 추천하였음. 이 경석 위원이 골격을 잡는데 많은 공헌을 함. Update N1235 by 95-12-01. Comments due by 96-03-09. 다음 WG meeting에서 충분한 support를 받으면 첫 PDTR로 투표 절차를 밟기로.

19.02 1 Nehl : Technical aspects
(Germany) N1237 '96 '97 '98
Project 19를 나누어 두개의 세부과제로 하기로. Nehl을 정식 editor로 추천하였음. 이 경석 위원이 골격을 잡는데 많은 공헌을 함. Update N1237 by 95-12-01. Comments due by 96-03-09. 다음 WG meeting에서 충분한 support를 받으면 첫 PDTR로 투표 절차를 밟기로.

NP ? 1 Moses Security incident handling
(U.K.) N1245 '97 '98 '99
보안사고의 통계치 작성이나 추후 예방을 목적으로 보안사고의 처리를 표준화하기를 U.K.에서 제안한 과제로 Switzerland와 Canada 등이 적극 반대의사 표명. NWI(new work item) proposal인 N1245을 NP(new project) 투표에 부치기로. Moses을 정식 editor로 추천하였음. Comments due by 96-03-09.

NP ? 3 Klein Protection profile registration procedures
(?) N1262r '97 '98 '99
NWI proposal인 N1262r을 NP 투표에 부치기로. Klein을 정식 editor로 추천하였음.

SP 3 Testing and Assessment Methods for IT Security
Ohlin이 rapporteur로서 study group 회의진행. 한국(장 청룡)의 input document, N1180 : Issues for Standardization of Testing and Assessment Methods for IT Security 등 3 개의 input document가 있었고 문서토의 결과로 N1180은 시험 및 평가방법에 대한 일반 프레임워크의 표준화를 위해 고려할 문서로 처리하기로 하였다. Study period를 갖기로. 다음 WG meeting에서 충분한 support를 받으면 NP 투표 절차를 밟기로.

SP ? 3 Strict security conformance testing
Testing and Assessment Methods 연구그룹에서 토의되었으나 이것에 대하여 따로 시급히 표준화하자는 데에 대한 논의가 있었으나 채택하지 않기로 하였다. 그러나 그후 이 문제를 U.K.가 HoD meeting과 Plenary에 각기 올려 격렬한 토론을 거친 후 투표한 결과 NP 투표에 부치지 않기로 결정하였고 이 내용은 Testing and assessment methods에서 다루기로.

Terminology / Glossary
WG2에서는 10(금) 오전 M. King이 acting editor로서 editing meeting을 진행하였고 이 필중, 백 재현, 최 원식 참석. N1203을 update하여 SC27 Secretariat에게 95-12-15까지 보내기로. WG3 에서는 M. Ohlin이 editor로서 editing meeting을 진행하였음. WG3 / N270을 update하여 WG3 Convener에게 95-12-15까지 보내기로.

III. 기타 사항

1. Head of Delegations Meeting

13(월) 오후. 러시아 제외 15 개국, WG1과 WG2는 convenor가 HoD를 겸했고, SC27 Chairman과 Secretariat을 포함 총 18 명 참석. 대부분 Plenary 에서 할 이야기들을 미리 타협을 보았는데 Strict Conformance Testing은 끝내 조율이 되지 않고 끝났다.

2. SC27 Plenary

14(화), 15(수). 이 필중, 이 경석, 백 재현, 장 청룡 참석. Australia(2), Belgium, Canada (2), Finland, France, Germany(3), Italy, Japan(2), Korea(4), Norway(2), Poland, Russia(3), Sweden, Switzerland, U.K.(2), U.S.(2)(SC27 Chairman과 Secretariat을 포함 총 30 명) 각 WG 의결 사항을 재검토하고 미결 사항을 결정하였다. 특기 사항은 다음과 같다.

* **Liaison Statements**

to : CCEB, ECMA TC 36-TG1, TC68, JTC1, JTC1 / SC6, SC21, SC30

* **Guidelines for NBs comments**

1. Include document number; **2**. Number all comments, following text sequence; **3**. Show place in document (page, clause, line); **4**. Separate technical and editorial comments in different sections; **5**. Identify major and minor comments; **6**. Justify technical comments with sufficient rationale, background, and explanation; **7**. Provide alternative text; **8**. Attend the editing meeting by an expert in case of a NO vote.

* **Joint Workshop on Security Standardization**

SC27 Chairman과 WG Convener들이 TC68 대표를 만나 공동관심사를 의논하고 Joint Workshop on Security Standardization(?)을 제안하기로.

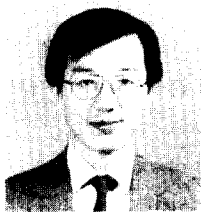
* **Next meetings**

1995-12	1? ~ 1?	WG2 06-01	Afnor, Paris, France
1996-04	17 ~ 19	WG1 14-02,-03	London,UK
	22 / 10:00 ~26 / 15:30	WG1	
	22 / 10:00 ~ 26 / 16:00	WG2	
	22 / 13:00 ~ 26 / 12:00	WG3	
1996-06 or 07	?? ~ ??	WG1 14-01	US
1996-10	21 ~ 25	WG1	Switzerland
	21 / 09:00 ~ 25 / 16:00	WG2	
	21 / 13:00 ~ 25 / 12:00	WG3	
	28 ~ 29	Plenary	
1997-04		WG's	Australia
1997-10		WG's & Plenary	Germany or Russia

3. 소감 및 감사

본 표준화회의에는 Canada에서 보안관련 학회, IEEE 802.10(LAN Security Standard) 회의 등이 겹쳐 생각보다 적은 수의 외국 전문가들이 참석하였다. 표준화회의는 학회와는 달리 와서 듣고만 가는 회의가 아니고 미리 관련 문서를 입수하여 충분히 검토하고 가능한 한 (자국의 이익을 대표하는) contribution을 준비하여 참가하는 것이 좋으며, 회의시 자국의 안이 있는 경우 그것을 관철시키려고 노력하며, 타국의 안들도 같이 검토함으로써 이해를 넓히며 최신 정보를 수집하는 것이리라는 인식이 조금 부족하였던 점이 아쉬웠으나 많은 국내 전문가들이 참석하여 성황을 이루고 정보보안 기술에 대한 인식을 넓히는 데에 일조를 해주신데 감사를 드린다. 공진청에서의 두번의 만찬을 포함한 복사서비스등의 행정지원은 본인이 참여했던 다른 나라들의 수준에 비추어 보았을 때 상위에 속하였다. 마지막으로 이 보고서를 쓰는데 도움을 주신 장 청룡, 신 동익, 백 재현, 류 재철 위원께 감사를 드린다.

□ 著者紹介



이 필 중(李 弼 中) 종신회원

1951년 12월 30일생
1974년 2월 서울대학교 전자공학과 학사
1977년 2월 서울대학교 전자공학과 석사
1982년 6월 U.C.L.A. System Science, Engineer
1985년 6월 U.C.L.A. Electrical Engineering, Ph.D.
1980년 6월 ~ 1985년 8월 Jet Propulsion Laboratory, Senior Engineer
1985년 8월 ~ 1990년 2월 Bell Communications Research, M.T.S.
1990년 2월 ~ 현재 포항공과대학 전자전기공학과, 부교수