# ITU-T SG17 WP2(정보보호)

**오 흥 룡** TTA 표준화본부 과장
**염 흥 열** 순천향대학교 정보보호학과 교수

## I. 회의 개요

○ 회의명 : ITU-T SG17 WP2(정보보호) 국제표준화 회의

○ 회의장소 : 캐나다 오타와

○ 회의기간 : 2006년 9월 11일 ~ 15일

○ ITU-T SG17 회의 한국대표단 : 총 17명(섹터멤버 포함)

○ 회의 참석규모 : ITU-T 회원국 등 총 40여 명

## II. 회의 주요 내용

○ 금번 SG17 WP2 Interim 회의는 지난 제주 회의 이후, Q.5, 6, 7, 8, 9, 17에서 보안부분에 대한 진척된 연구결과를 토의하는 회의였으며, Q.4는 개최되지 않았음

○ 한국의 제안으로 RFID 보안을 한국 주도하에 개발키로 함
- Q.6: RFID를 위한 프라이버시 및 개인정보 보호 가이드라인(X.rfpg, KISA, 이향진 연구원)
- Q.9: RFID 응용서비스를 위한 프라이버스 보호 프레임워크(X.rfidsec-1, ETRI, 최두호 선임)

○ 바이오인식(Q.8) 분야
- Q.8 라포처(Shuling, 중국)가 SG17 활동을 못한다고 하였으며, 후임자로 김학일 교수(인하대)를 추천하였으나, Mr. Watanabe가 국가별 의장단 분배 때문에 반대
- 차기회의(12월, 제네바) 주재는 김학일 교수가 진행하기로 하였으며, 라포처 문제는 다시금 검토키로 함

○ 한국 주도로 개발되고 있는 X.homesec-1을 차기회의에서 승인(consent)으로 추진키로 함

○ 한국은 총 15건(국가기고서 13건, 섹터멤버 기고서 2건)의 기고서를 제안하여, 15건 모두 국제표준에 반영시켰으며, 2명의 main-editor(이향진, 최두호)와 2명의 co-editor(백종현, 신영교) 임명을 받았음

| No. | 기고서 명 | 문서번호 | 결과 |
|---|---|---|---|
| 1 | Updated document of D150: Proposal for the profile based privacy protection framework for the RFID application services | CAN-Doc.05/Q.6, 9 | 채택<br>(신규 표준화 아이템(X.rfidsec-1)으로 채택되었으며, main-editor로 최두호 선임(ETRI)이 임명됨 |
| 2 | New draft of X.akm: Framework for EAP-based authentication and key management of NGN | CAN-Doc.06/Q.5 | 채택<br>(X.ngn-akm에 text 수정 및 EAP 선정방법 등을 반영) |
| 3 | 1st Draft of X.sim: Security Incident Management Guidelines for Telecommunications | CAN-Doc.07/Q.7 | 채택<br>(X.sim에 baseline 문서로 채택함) |
| 4 | Engineering aspects of telebiometric data | CAN-Doc.08/Q.8 | 반영<br>(X.physiol에 부록으로 삽입하기 위해 차기회의에서 재검토키로 함) |
| 5 | X.tpp-1(Telebiometric Protection Procedures-Part1): A Guideline of Technical and Managerial Countermeasures for Biometric Data Security | CAN-Doc.09/Q.8 | 채택<br>(X.tpp-1에 반영되었으며, 바이오인식 기능적 모델 등을 수정하여 차기회의에서 재검토키로 함) |
| 6 | Proposal of the digital signature technology using biometrics for X.BIP(BioAPI Interworking Protocol) | CAN-Doc.10/Q.8 | 채택<br>(X.bip에 반영하기 위한 기고서였으나, X.tsm에 반영하기로 하였으며, co-editor로 신용녀 연구원(KISA)이 임명됨) |
| 7 | Telebiometric Digital Signature Key Generation and Management Framework | CAN-Doc.11/Q.8 | 반영<br>(본 기고서의 범위(scope) 등을 수정하여 차기회의에서 재검토키로 함) |
| 8 | Revision of first draft Recommendation X.homesec-1: Framework of security technologies for home network | CAN-Doc.12/Q.9 | 채택<br>(차기회의에서 consent로 추진키로 함) |
| 9 | Updated Draft Text of X.sap-1: Guideline on secure password-based authentication protocol with key exchange | CAN-Doc.13/Q.9 | 채택<br>(X.sap-1에 반영되었으며, 계속해서 검토하기로 함) |
| 10 | Proposal for the first draft of X.homesec-2 : Device certificate profile for the home network | CAN-Doc.14/Q.9 | 채택<br>(X.homesec-2에 반영되었으며, co-editor로 백종현 선임(KISA)이 임명됨) |
| 11 | Proposal of developing a guideline on the protection of personal information and privacy for RFID | CAN-Doc.15/Q.6, 9 | 채택<br>(신규 표준화 아이템(X.rfpg)으로 채택되고, main-editor로 이향진 연구원(KISA)이 임명됨) |
| 12 | Proposed Revision of X.gcs Document Text | CAN-Doc.16/Q.17 | 채택<br>(X.gcs 문서의 text를 수정함) |
| 13 | Proposed revision of X.ocsip text | CAN-Doc.17/Q.17 | 채택<br>(X.ocsip 문서의 text를 수정함) |
| 14 | Analysis of well-known countering spam mechanisms | CAN-Doc.18/Q.17 | 채택<br>(X.ocsip 문서에 새로운 chapter로 반영하기로 함) |
| 15 | Proposed revision of draft text on X.websec-3, Security architecture for message security in mobile Web Service | CAN-Doc.28/Q.9 | 채택<br>(본 기고서를 X.websec-3의 baseline 문서로 채택하고 계속 검토키로 함) |

## 1. SG17 WP2 전체(Plenary) 회의 주요내용

○ 기고서 제출방법 및 제출기간을 엄격히 지켜줄 것을 당부
- 기고서 제출방법은 국가기고서, 섹터기고서, 또는 associate 기고서로 제출해야 하며, 에디터 등의 개인 자격으로 기고서를 제출할 수 없음
- 기술적인 사항을 TD 문서로 제출하면 안되고, 반드시 기고서(Contribution)로 제출해서 검토를 받아야 함
- 차기 SG17 기고서 마감은 제네바 시간으로 2006년 11월 25일까지 제출키로 함

○ 2006. 12. 4(월) ~ 5일(화)까지, 제네바에서 사이버 보안 워크숍을 "ID Management" 주제로 개최키로 함

○ WP2에서 추진되고 있는 표준화 연구과제 목록
- 차기 12월에서 승인(consent) 예정 목록

| Recommendation | | WP | Question | Editor | Location of text |
|---|---|---|---|---|---|
| No. | Title | | | | |
| X.pak | Password-authentication key exchange(PAK) | 2 | 5 | Z. Zeltsan | CAN-Doc72 |
| X.805nsa | Network security certification based on ITU-T Recommendation X.805 | 2 | 5 | R. Vasireddy | TD2314Rev.1 |
| X.cso | Overview of cybersecurity | 2 | 6 | A. Barbir | TD2313 |
| X.cvlm | Guidlines on cybersecurity vulnerability lifecycle management | 2 | 6 | M.C. Kang | TD2269Rev.1 |
| X.sds | Guidelines for Internet Service Provides and end-users for addressing the risk of spyware and deceptive software | 2 | 6 | M.C. Kang | TD2280Rev.1 |
| X.vds | A vendor-neutral framework for automatic checking of the presence of vulnerabilities information update | 2 | 6 | H. Takechi | TD2352 |
| X.bip | BioAPI interworking protocol | 2 | 8 | J.P. Lemaire | CAN-Doc29 |
| X.homesec-1 | Framework of security technologies for home network | 2 | 9 | H.Y. Youm, H.R. Oh | TD2411 |

- 계속 연구과제 목록

| Recommendation | | WP | Question | Editor | Location of text |
|---|---|---|---|---|---|
| No. | Title | | | | |
| X.805+ | Division of the security features between the network and the users | 2 | 5 | N. Etroukhine | D138 |
| X.ngn-akm | Authentication and key management framework for NGN | 2 | 5 | H.Y. Youm | CAN-Doc73 |
| X.spn | Framework for creation, storage, distribution, and enforcement of policies for network security | 2 | 5 | J.H. Kim | D163 |
| X.cap | OASIS Common Alerting Protocol V1.1 | 2 | 6 | Abbie Barbir | TBD |
| X.fsn | Framework for secure network operations | 2 | 6 | TBD | TBD |
| X.rfpg | Privacy Guidelines for RFID | 2 | 6 | H.J. Lee | CAN-Doc15 |
| X.idmr-1 | IdM Requirements | 2 | 6 | TBD | TBD |
| X.idmr-2 | Framework for Idm | 2 | 6 | TBD | TBD |
| X.idms | Idm security analysis | 2 | 6 | TBD | TBD |

| Recommendation | | WP | Question | Editor | Location of text |
|---|---|---|---|---|---|
| No. | Title | | | | |
| X.1051rev | Information Security Management Guidelines for telecommunications based on ISO/IEC 27002 | 2 | 7 | Koji Nakao | CAN-Doc31 |
| X.sim | Security Incident Management Guidelines for Telecommunication | 2 | 7 | J.D. Kim | CAN-Doc07 |
| X.rmg | Risk Management Guidelines for Telecommunications | 2 | 7 | Edward Humphreys | CAN-Doc32 |
| X.physiol | Telebiometrics related to human physiology | 2 | 8 | P. Gerome | TD2302 |
| X.tai | Telebiometrics authentication infrastructure | 2 | 8 | J. Wei | CAN-Doc23 |
| X.ttp-1 | A guideline of technical and managerial countermeasures for biometric data security | 2 | 8 | J. Kim, H. Kim | CAN-Doc09 |
| X.tsm-1 | General biometric authentication protocol and profile on telecommunication system | 2 | 8 | Y. Isobe, Y. Shin | TD2276 |
| X.tsm-2 | Profile of telecommunication device for telebiometrics system mechanism(TSM) | 2 | 8 | Y. Isobe, Y. Shin | D142 |
| X.homesec-2 | Certificate profile for the device in the home network | 2 | 9 | D.Y. Yoo, J.H. Baek | TD 2414 |
| X.homesec-3 | User authentication mechanisms for home network service | 2 | 9 | H. K. Lee | D 176 |
| X.msec-3 | General security value added service(policy) for mobile data communication | 2 | 9 | F. Zhang,J. Chen | TD 2330 |
| X.msec-4 | Authentication architecture in mobile end-to-end data communication | 2 | 9 | Z. Zheng,J. Wei | TD 2416 |
| X.crs | Correlative reacting system in mobile network | 2 | 9 | S. Liu,J. Wei | TD 2417 |
| X.sap-1 | Guideline on secure password-based authentication protocol with key exchange | 2 | 9 | H. Y. Youm | TD 2407 |
| X.sap-2 | Secure communication using TTP services | 2 | 9 | T. Kaji | TD 2408 |
| X.p2p-1 | Requirement of security for peer-to-peer communications | 2 | 9 | Y. Miyake | TD 2410 |
| X.p2p-2 | Security architecture and protocols for peer to peer network | 2 | 9 | J.H. Nah | D 193 Rev.1 194, 195, 196 |
| X.websec-3 | Security architecture for message security in mobile web services | 2 | 9 | J.S. Lee | TD 2409 |
| X.rfidsec-1 | Privacy protection framework for networked RFID services | 2 | 9 | D.H. Choi | TD 2415 |
| X.gcs | Guideline document on countering email spam | 2 | 17 | S.G. Kang, Yuxiao Li | TD 2295 Rev0.5 |
| X.csreq | Requirement on countering spam | 2 | 17 | Hongwei Luo, Jianyong Chen | TD 2329 |
| X.fcs | Technical framework for countering email spam | 2 | 17 | Kun Yang, Jianong Chen | TD2316 Rev0.1 |
| X.ocsip | Overview of countering spam for IP multimedia application | 2 | 17 | S.G. Kang | TD 2296 Rev0.3 |
| X.tcs | Technical means for countering spam | 2 | 17 | TBD | TBD |

## 2. Q.5(보안 구조 및 프레임워크) 회의결과

○ CAN-Doc27: Password-Authenticated Key Exchange(PAK) Protocol
- PAK 프로토콜에 대한 보완 설명과 인증방법, 보안 고려사항 등을 반영하였음
- 두 개체 간에 인증 프로토콜 사용 예를 반영하자는 의견이 있었으나, PAK는 두 참여자간에 인증 프로토콜이므로, 별도의 예를 반영하지 않기로 함

○ CAN-Doc06: New draft of X.ngn-akm: Framework for EAP-based authentication and key management of NGN
- Q.15/SG13에서 검토된 의견을 모두 반영하였으며, EAP 정의 및 분류방법을 보완함
- 섹션 9.2 항목에서 '마스터 키'로부터 '다양한 키'를 유도하는 방법을 보완하여 차기회의에서 재검토키로 함

## 3. Q.6(사이버 보안) 회의결과

○ Q.6에서 IDM(Identity management) 관련하여, "IDM 요구사항, 프레임워크, 보안분석" 표준들을 개발키로 함

○ CAN-Doc15: Proposal of developing a guideline on the protection of personal information and privacy for RFID
- Q.9에서 1차적으로 검토하였으나, 본 기고서가 가이드라인 성격의 표준초안이므로, Q.6에서 추진키로 합의됨
- 본 기고서를 X.rfpg로 채택하고, main-editor로 이향진 연구원(KISA)이 임명됨

## 4. Q.7(보안 관리) 회의결과

○ CAN-Doc04: Alignment of revised Recommendation X.1051 with ITU-T X.805
- 'IT 네트워크 보안' 관점에서 X.1051을 개정하자는 기고서였으나, X.1051은 다양한 보안적 측면을 고려하여 개발하고 있으므로, 별도로 '개요 및 연구범위' 부분에 대한 변경은 필요 없음
- 따라서, X.1051 개정 표준초안에 4.1.2 절의 일부 text만을 수정하기로 함

○ CAN-Doc31: Comments on the draft document of revised X.1051
- 새롭게 10.6.3 절로 '정보통신 서비스 전달에 대한 보안관리'를 신설키로 함
- 개정중인 X.1051에 '텔레콤 특별 제어방법' 부분은 구별자(symbols)를 사용하여 구분이 필요함을 제안하였으나, 반영 유/무는 차기회의에서 재검토키로 함

○ CAN-Doc07: 1st Draft of X.sim: Security Incident Management Guidelines for Telecommunication
- NIST SP800-61과 ISO/IEC TR 18044에서 유용한 부분만을 발췌하여 1차 초안을 작성함
- 4.2절: 전송통신 보안사고의 특징, 4.3절: 전송통신 보안사고의 종류와 방법을 보완하여 차기회의에 재검토키로 함

○ CAN-Doc32: Telcoms Risks ITU-T White Paper
- X.rmg(Risk management guidelines for telecommunication)의 text를 최종 수정하여, 차기회의에서 consent로 추진키 함
- X.rmg는 ISO/IEC 27005 'ISM Risk management'와 관련되므로, liaison 문서를 SC27로 송부하기로 함

○ CAN-Doc20 and CAN-Doc21: Information

Security Management Platform(ISMP)
- 정보통신 시스템 상에서 집중화된 보안 운영을 위한 기능적 프레임워크 개발하기로 합의함
- 프레임워크 제목을 'ISMP'에서 'NSMF(Network Security Management Framework)'로 변경하기로 함
- 차기회의에서 NSMF와 관련된 권고들(기본 개념, 인터페이스 스펙, 기능적인 스펙)을 분석하여 전체적인 그림으로 표현하기로 함

## 5. Q.8(바이오인식) 회의결과

○ CAN-Doc08: Engineering aspects of telebiometric data
- 본 기고서는 X.physiol에 부록으로 반영하기 위한 엔지니어링 측면에서의 연구결과였으나, 본 표준초안의 에디터가 회의에 참석하지 못하여, 차기회의에서 재검토키로 함

○ CAN-Doc09: X.tpp-1(Telebiometric protection procedure-Part 1): A guideline of technical and managerial countermeasures for biometric data security
- Replay attack에 대한 정의를 추가하였으며, 차기회의에 본 공격에 대한 삭제 및 보호 방법에 대한 해결책을 정의하기로 함
- 그림 1의 제목은 ISO/IEC JTC1/SC27에 'Project 24761' 그림과 같으므로, 변경 없이 그대로 유지키로 함
- 그림 3의 제목을 'Telebiometric functional model'로 변경하기로 함
- 그림 4의 바이오인식 컴포넌트는 그림3의 모델에 따라 변경하기로 하였으며, 그림5의 컴포넌트 및 취약점 또한 변경하기로 함
- 섹션 15를 삭제하기로 하였으며, 섹션 7를 좀더 명확하게 변경하기로 함
- 차기회의에서 위의 고려사항과 SC27 N5121의 'Security evaluation of biometrics'들을 추가하여 first draft recommendation으로 추진키로 함

○ CAN-Doc11 and CAN-Doc26: Telebiometric Digital Signature Key Generation and Management Framework
- 바이오인식 데이터로부터 디지털 키생성 방법과 이 키를 이용한 인증방법은 Q.8에서 추진하는 것이 적합하다고 합의됨
- Doc11은 Q.8의 새로운 표준화 아이템으로 추진키로 합의되었으며, 차기회의에서 본 표준초안의 '목적, 연구범위, 보안성 측면'을 좀더 명확히 하여 재검토키로 함
- Doc26은 바이오인식 데이터를 이용하여 본 데이터에 대한 보안성 평가방법과 적절한 보호 방법들을 정의하고 있으므로, 이를 반영하여 표준을 개발키로 함

○ CAN-Doc23: Draft text of X.tai: Telebiometrics Authentication Infrastructure (TAI)
- X.tai에 정의되어 있는 바이오인식 인증서와 바이오인식 알고리즘 인증서는 X.509의 속성인증서를 변경하지 않고, 그대로 사용하기로 함
- ASN.1 정의 관련해서는 Mr. Lemaire에 의해 수정되었으며, 구현 툴에 의해 확인됨
- 차기회의에서는 새로운 속성 및 확장 방법 등을 개발키로 하였으며, 바이오인식 인증서 관련하여 ISO/IEC JTC1/SC27에 liaison 문서를 송부하여 검토 받기로 함

○ CAN-Doc25: Report on consideration of requirements for TSM massages and their implementation using BIP, CAN-Doc29: Information Technology-BioAPI Interworking Protocol
- X.bip 표준초안에 모두 반영되었으며, X.bip에 정의된 ASN.1과 XML 스키마가 적절한 툴에 의해서 검증되었음

- X.tsm에 정의된 9가지 모델들과 X.bip에 정의된 7가지 시나리오들을 비교 분석키로 하였으며, 본 시나리오는 단지 예로만 활용되며, 모든 상황들이 고려된 것은 아님
- ISO/IEC JTC1/SC27의 'Project 24761'에 바이오인식 처리절차와 관련된 'ACBio information(바이오인식을 위한 인증 문맥)'은 X.tsm, X.tai에 처리절차와 매우 유사하므로, 각각의 에디터들은 서로간의 관계와 응용가능성을 검토하기로 함
- X.tsm-1, 2에 co-editor로 신용녀 연구원(KISA)이 임명됨

○ CAN-Doc34: Representing telebiometric device category within X.tsm, X.tai and X.bip
- 바이오인식 디바이스를 10개의 카테고리로 분류하기로 하였으며, X.1081에 정의된 표준 코드를 바이오인식 표준화 활동에 활용하기로 함
- ISO/IEC JTC1/SC37에 바이오인식 디바이스 분류 방법 및 표준 코드를 문의키로 함

## 6. Q.9(안전한 통신서비스) 회의결과

○ CAN-Doc02 and CAN-Doc12: Framework of security technologies for home network
- 일본의 제안에 따라, X.homesce-1의 text와 전체적인 모델명을 'General home network model for security'으로 수정함
- SG9에 liaison 문서를 송부하여, X.homesec-1의 부록A에 대한 검토 의견을 요청하고, 향후 J.190과 X.homesec series들과의 용어 통일 및 디바이스 유형 통일 등에 대하여 검토 의뢰함
- 차기회의에서 X.homesec-1을 승인(consent)으로 추진키로 함

○ CAN-Doc14: Device certification profile for the home network(X.homesec-2)
- RFC3280과 본 표준초안에서 정의하고 있는 인증서 프로파일에 대해 논의하였음
- 차기회의에서 CRL 프로파일에 대한 반영 유/무와 SHA-1의 취약점에 대한 설명을 위한 editor's note를 추가키로 함
- Normative reference에서 'Cable Lab. 스펙'은 삭제키로 하였으며, Q.2의 라포처에게 X.homesec-2를 검토 의뢰키로 함
- X.homesec-2의 co-editor로 백종현 선임(KISA)이 임명됨

○ CAN-Doc19: Correlative reacting system in mobile data communication(X.crs)
- 지난 제주회의에서 지적된 사항을 모두 반영하였으며, 다음 사항들을 고려하여 차기회의에서 재검토로 함
  - CRS 메시지 무결성에 대한 이름 변경
  - 'OS/platform version' => 'OS version' 변경
  - 설치되는 패치들의 이름을 일반적인 예로 리스트하는 방법
  - Q.6의 라포처와 부-라포처들에게 검토 의뢰키로 함

○ CAN-Doc22: authentication architecture in the mobile end-to-end data communication
- USIM과 사용자 단말기에서 SS 기능성에 대한 가능한 위치를 text로 설명키로 함
- 사용자 단말기에 SS가 존재할 경우, 잠재적으로 존재하는 보안 취약점을 고려키로 함
- USIM과 같은 토큰에서 SS가 존재할 경우, 사용자 인증에 대한 필요성을 text로 설명키로 함
- X.msec-4에서 USIM 용어에 대해 명확히 정의키로 하였으며, information reference에 Kerberos 기술에 대한 문서들을 일부 삽입키로 함
- 본문 내용중에 'public-private key pair' => 'asymmetric key pair', 'certificate repository' => 'certificate depository'으로 수정키로 함
- 기존 네트워크(home network)와 방문된 네트워크(visited network) 사이에 AP의 가능한 위치를

text로 설명키로 함
- TLS를 기반으로 B.3의 그림을 수정키로 하였으며, B.3에 절차 4, 5, 6을 수정키로 함

○ CAN-Doc03: Anonymous authentication architecture in community communication (X.p2p-1)
- 섹션 12에 보안기술에 대한 반영 유/무와 SETI@HOME에 정의된 분산된 컴퓨터 기반의 P2P 모델에 대한 사항들을 고려하여 재검토키로 함
- P2P 환경에서 익명의 인증 구조의 요구사항을 정의하기 위한 위협 및 취약점들을 연구하여 반영키로 함
- X.p2p-1의 제목을 'Requirements of security for peer-to-peer communications'으로 변경키로 함

○ CAN-Doc13: Guideline on secure password based authentication protocol with key exchange(X.sap-1)
- 패스워드 인증 프로토콜의 고려사항, 선정기준, 비교 분석 등을 수정하였으며, ITU-T 저자 가이드라인(A.1500)을 반영하여 IETF RFC 레퍼런스 항목들을 수정함

○ CAN-Doc01: Secure communication using TTP services(X.sap-2)
- X.sap-2의 표준초안과 Liberty Alliance에서 연구되고 있는 결과들과의 중복성을 검토키로 함
- TTP 기반의 서비스 시나리오를 추가하기로 하였으며, 서비스 흐름도 1단계 전 상태에 대해 명확히 정의하고 부록B에 요약을 수정하여 재검토키로 함

○ CAN-Doc05: Proposal for the profile based privacy protection framework for the RFID application services
- RFID와 네트워크 RFID 간에 차이점을 정의하고, 네트워크 RFID를 명확히 정의키로 함
- Q.6와 JCA-NID 그룹과 협력하여 개발하기로 함
- 본 기고서를 X.rfidsec-1로 채택하고, main-editor로 최두호 선임(ETRI)이 임명됨

○ CAN-Doc28: Security architecture for message security in mobile Web Services (X.websec-3)
- 지난 제주회의에 결과에 따라, OMA의 스펙 OWSER(OMA Web Services Enabler)를 반영하였으며, 기술적으로 OMA 스펙과 동일하게 추진키로 함
- X.websec-3과 OMA 스펙 간에 차이점을 설명하는 새로운 절을 만들기로 함
- 모바일 웹서비스 보안을 위한 추가적인 일반 모델을 정의키로 함

○ NGN 보안 이슈
- 향후, Q.9에서는 NGN 권고 'Y.2701: Security requirement for NGN release1'과 'Y.2091: Terminology for NGN'에 근거하여, NGN 보안과 관련된 표준을 개발키로 함

## 7. Q.17(기술적 방법에 의한 스팸 대응) 회의결과

○ CAN-Doc16: Proposed Revision of X.gcs Document Text
- 요약, normative reference, 국제표준화 기구(ITU, OECD, APEC, APT, IETF)들의 활동 현황, 약어 등을 업데이트 함
- SG2가 서비스 정의를 위한 LSG로 활동하고 있지만, 아직 국제적인 스팸 용어에 대한 정의가 없으므로, 본 표준초안에 이를 명확히 정의함
- 차기회의에서 스팸과 다른 위협들(fraud, privacy theft, spyware) 간에 차이를 명확히 정의하기로 하였으며, 다른 국제표준화 기구 활동과의 차이점을 정의하기로 함

○ CAN-Doc17: Proposed revision of X.ocsip text
- 본 표준초안 연구범위에 '실시간 IP 멀티미디어 스팸'만을 정의하는 것으로 명확히 하였으며, 제6장

의 text를 수정함
- 유명한 IP 멀티미디어 스팸 사례(SPIT, SPIM, Online game spams, presense spams, conference spams)들을 반영하기로 함

○ CAN-Doc18: Analysis of well-known countering spam mechanisms
- 본 기고서를 기반으로 중국, 일본, 프랑스와 협력하여, 신규 섹션으로 'Applicability of well-known countering SPAM mechanisms for IP multimedia application'을 추가하여 X.ocsip를 개발하기로 함
- 또한, 프랑스에서 OECD와 중복성을 제기하였지만, OECD는 e-mail 스팸만을 다루고 있으므로, X.ocsip와는 직접적으로 중복되지 않음을 확인함

## 8. 차기 SG17 회의 및 워크숍

○ 2006. 12. 4(월) ~ 5일(화), 제네바 : 'ID Management'라는 주제로 사이버보안 워크숍

○ 2006. 12. 6(수) ~ 15일(금), 제네바 : SG17 전체 회의

# III. 맺음말

○ 이번 ITU-T SG17 WP2 Interim 회의는 제주 회의 이후, 주요 보안 이슈 관련하여 진척된 사항을 12월에 개최될 SG17 전체 회의전에 검토하기 위한 회의였음

○ 특히, 한국의 제안으로 ITU-T 내에 RFID 보안을 한국 주도하에 개발하기로 합의된 바, 한국은 이번 회의를 통하여 RFDI 보안 표준화를 주도할 좋은 계기를 마련했으며, 국내 RFID 보안기술을 국제표준에 적극적으로 반영하는 것이 필요함
- Q.6: RFID를 위한 프라이버시 및 개인정보 보호 가이드라인(X.rfpg)
- Q.9: RFID 응용서비스를 위한 프라이버스 보호 프레임워크(X.rfidsec-1)

○ 한국 주도로 개발되고 있는 홈네트워크 보안 분야에서는 일본의 text 수정 기고서를 반영하여, X.homesec-1 표준초안이 완성되어, 차기 SG17 회의(제네바, 12월)에서 ITU-T 최초 홈네트워크 보안 분야의 국제표준 제정이 가능할 것으로 예상됨

○ 모바일보안(X.msec-3, 4, crs) 분야는 중국을 중심으로 추진되고 있지만, 이번 정기회의를 통하여, 표준초안이 거의 마무리되었으므로, 승인(consent) 절차로 넘어가기 전에 적절한 국내 대응이 필요할 것으로 생각됨

○ 바이오인식(Q.8) 분야의 신규 라포처 임명과 관련하여, 중국측에서 한국의 김학일 교수(인하대)를 추천하였지만, 일본측에서 반대하는 입장을 표명한 바, 차기회의 개최 전에 국내 입장 정리가 필요함

○ SG17 보안 분야에 참가하고 있는 국내 표준전문가는 주로 연구기관과 학계 전문가들 중심이므로, 국내 보안업체들의 적극적이 참여가 필요함 TTA