情 報 保 護 學 會 誌
第18卷 第4號, 2008. 8

ITU-T SG17 Q.9(안전한 통신 서비스) 국제표준화 동향 및 향후 전망

오 흥 룡*, 나 재 훈**, 염 흥 열***, 김 대 경***

요 약

국제표준화기구 ITU-T에서는 SG17 WP2 그룹이 정보통신 보안에 관한 표준화를 리드하는 연구그룹으로, 산하 7개의 연구과제(Question)를 구성하여 정보보호 국제표준을 개발하고 있다. 이 연구과제들 중 Q.9(의장, 염흥열, 순천향대)에서는 안전한 통신 서비스라는 주제로 모바일 보안, 홈네트워크 보안, 웹 서비스 보안, P2P보안, 멀티캐스트 보안, USN 보안, NID(RFID) 보안, IPTV 보안, 응용서비스 및 응용 프로토콜 보안 등 정보통신 환경에서 다양하게 응용될 수 있는 국제표준들의 개발을 담당하고 있다. 현재, Q.9에서는 앞서 언급된 분야로 총 16건의 국제표준을 제정하였으며, 총 6건의 표준초안들이 개발중에 있다. 본 논문에서는 Q.9에서 개발한 국제표준들과 개발중에 있는 표준초안들에 대해 간단히 소개하고, 차기 연구회기('09~'12) 구조조정 방향에 따른 향후 추진방향을 제시하고자 한다.

Ⅰ. 서 론

현대 사회가 인터넷의 발전과 다양한 디바이스들의 개발로 디지털 컨버전스라는 융합 서비스 개념에 적합한 유비쿼터스 사회로 진화되고 있다. 이런 사회에서 가장 요구되는 사항으로는 사용자들의 편의성 고려와 얼마만큼 개인, 기업, 부가서비스 제공자들의 자산과 프라이버시 정보를 제3의 악의적인 공격으로부터 안전하게 보호할 수 있는가이다. 또한, 유비쿼터스 사회 구축을 위해 요구되는 홈네트워크, 모바일 네트워크, USN 등 인프라를 안전하게 운영하는 기술 개발과 이들을 보호하기 위한 정보보호 기술이 요구된다. 그리고 이들 인프라를 기반으로 사용자들에 다양한 부가서비스를 제공하기 위한 웹서비스, P2P 서비스, IPTV 서비스, RFID, 통합인증 서비스, 콘텐츠 보호 서비스 등 응용서비스 관점에서의 기술 개발과 이들을 안전하게 보호하는 기술들이 고려되어야 한다.

본 논문에서는 유비쿼터스 사회에서 요구되는 응용서비스와 디지털 컨버전스 융합 서비스를 위해, 정보통신 기술 관점에서 안전한 통신기술 및 응용서비스들의 정보보호 기술들을 표준화하고 있는 ITU-T SG17 WP2 Q.9에서 개발된 국제표준 및 국제표준초안들에 대해 간단히 소개와 차기 연구회기 구조조정 방향에 따른, 향후 표준화 추진전략 및 고려사항들을 제시하고자 한다.

Ⅱ. ITU-T SG17 연구과제 9[1,31,32]

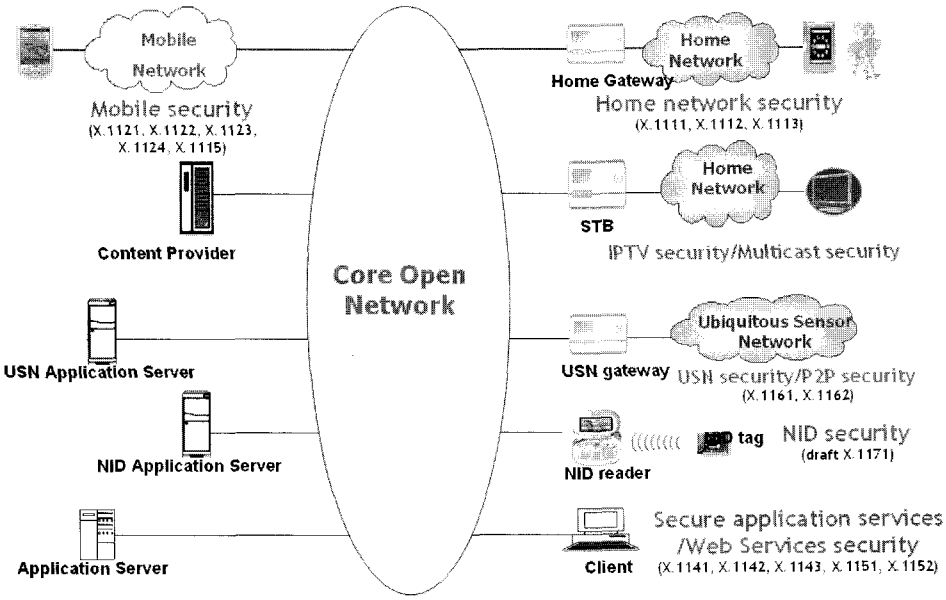
연구과제 9는 안전한 통신 서비스라는 주제로 한국 의장(염흥열, 순천향대)의 리더십 하에 [그림 1]과 같이 다양한 연구주제로 국제표준들을 개발하고 있다. 또한, Q.9는 지난 연구회기(2005-2008)동안 14건의 ITU-T 권고안을 산출한 SG17 내에서도 가장 활동이 활발한 연구과제이고 제일 많은 국제표준화 전문가들이 참석하고 있다.

본 절에서는 [표 1]과 같이 Q.9에서 제정한 국제표준 및 개발 중에 있는 국제표준초안들을 간단히 소개하고 서로 간에 관계에 대해 간단히 살펴보고자 한다.

2.1 모바일 보안

모바일 보안 분야는 지난 연구회기('01~'04)부터 계

* 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr)
** 한국전자통신연구원 정보보호연구본부 (jhnah@etri.re.kr)
*** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr, kimdk3@pss.go.kr)



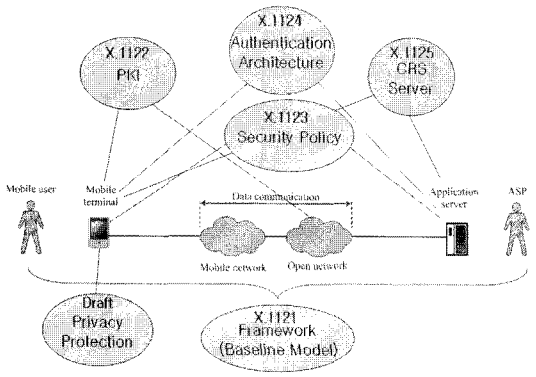
〔그림 1〕 연구과제 9 - 연구범위

속해서 연구되고 있는 분야이고, 안전한 통신서비스 관점에서 최초로 연구하기 시작한 분야이다. 2004년 4월, 한국과 일본 주도로 X.1121(모바일 종단간 데이터통신을 위한 보안기술 프레임워크)과 X.1122(PKI 기반의 안전한 모바일 시스템 구현을 위한 가이드라인)를 국제표준으로 제정하였다. 또한, 한국은 상기 2건의 국제표준이 ITU-T 내에 보안 분야에서 최초로 한국 주도하에 개발한 국제표준으로 큰 의미를 가지고 있다. 이 후, 이번 연구회기 동안에는 중국을 중심으로 X.1123(안전한 모바일 종단간 데이터통신을 위한 차별화된 보안서비스), X.1124(모바일 종단간 데이터통신을 위한 인증구조), X.1125(모베일 데이터통신에서의 보안상관 시스템)를 국제표준으로 제정하였다.

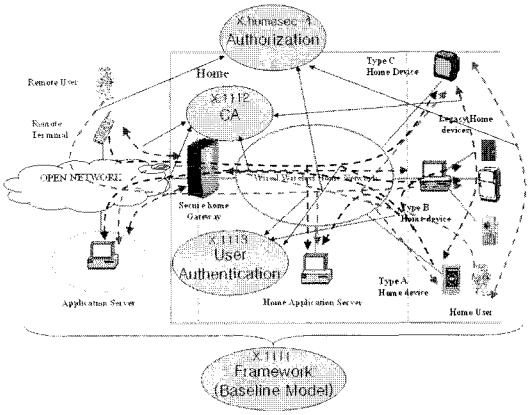
X.1121 국제표준의 주요내용은 모바일 네트워크 환경을 구성하고 있는 각각의 객체들을 보안적인 관점에 따라 기본적인 모델(일반, 보안게이트웨이)들을 정의하였고, 사용자와 응용서비스제공자(ASP) 간에 존재할 수 있는 보안위협들을 분석하였다. 또한, 분석된 보안위협들을 해결하기 위한 보안요구사항들과 이들의 요구사항들을 반영할 수 있는 보안기술들을 정의하고 있다[6]. X.1122 국제표준의 주요내용은 이미 공개키기반구조(PKI)가 많은 보안기능(암호화, 전자서명, 데이터 무결성 등)들을 제공하고 있어, 여러 응용기술에 적용되어 활용되고 있지만, 아직 모바일 분야에서 활용하기 위한 표준이나 가이드라인 문서들이 없어, 본 표준에서 모바일 네트워크에 PKI 기술을 적용하기 위한 기본적인 가드라인을 정의하고 있다. 즉, X.1121에서 제시하고 있는 모델에 PKI 구조를 적용한 모델을 정의하고, 인증서 운영절차 및 생명주기 관리, 서비스 시나리오, 구현 사례 및 고려사항들을 정의하고 있다[7]. X.1123 국제표준의 주요 내용은 X.1121에서 제시하고 있는 모델에 ASP로부터 사용자에게 전달되는 보안서비스 및 부가서비스들을 차별화된 보안정책에 따라 제공하기 위한 방법들을 정의하고 있다. 즉, ASP가 사용자에게 불필요한 보안기능이나 불필요한 부가서비스들을 제공할 경우, 사용자 단말기에 불필요한 프로세스나 계산량이 증가될 수 있고, 사용자에게 부당한 과금 청구가 책정될 것이다. 따라서 본 표준에서는 크게 3가지(상위보안정책, 기본보안정책, 무보안정책) 등급을 적용한 차별화된 보안정책 모델을 정의하였고, 각 보안정책의 분류 방법, 사용자와 ASP 간에 보안정책을 협의하는 절차, 구현 시 요구되는 인터페이스들의 요구사항, 보안정책에 따른 보안알고리즘 분류 방법들을 정의하고 있다[8]. X.1124 국제표준의 주요내용은 X.1121에서 정의한 모델에서 사용자와 ASP 간에 상호인증을 수행하기 위한 인증구조를 정의하고 있다. 즉, 사용자와 ASP 간에 인증을 수행하기 위한 기본 구조와 사용자가 다른 모바일 네트워크를 이동시 발생할 수 있는 인증구조를 정의하

〔표 1〕 ITU-T SG17 Q.9 국제표준 현황(총 16건) 및 표준초안 현황(총 6건)

No.	국제표준번호	연구과제	제정시기	국제표준명(제목)	제안국가	국내표준
1	X.1111	Q.9	2007-02	Framework for security technologies for home network	한국 (염흥열, 오흥룡)	TTAE.IT-X1111
2	X.1112	Q.9	2007-11	Device certificate profile for the home network	한국 (백종현)	TTAS.KO-12.0052
3	X.1113	Q.9	2007-11	Guideline on user authentication mechanisms for home network services	한국 (이형규)	TTAS.KO-12.0030
4	X.1121	Q.9	2004-04	Framework of security technologies for mobile end-to-end data communications	한국/ 일본	X
5	X.1122	Q.9	2004-04	Guideline for implementing secure mobile systems based on PKI	한국/ 일본	X
6	X.1123	Q.9	2007-11	Differentiated security service for secure mobile end-to-end data communication	중국	X
7	X.1124	Q.9	2007-11	Authentication architecture for mobile end-to-end data communication	중국	X
8	X.1125	Q.9	2008-01	Correlative reacting system in mobile data communication	중국	X
9	X.1141	Q.9	2006-06	Security Assertion Markup Language (SAML 2.0)	캐나다	TTAS.IT-X1141_ 1 ~ 6
10	X.1142	Q.9	2006-06	eXtensible Access Control Markup Language (XACML 2.0)	캐나다	TTAS.OT-10.0040 /R1
11	X.1143	Q.9	2007-11	Security architecture for message security in mobile web services	한국 (이재승)	2008-760 추진중
12	X.1151	Q.9	2007-11	Guideline on secure password-based authentication protocol with key exchange	한국 (염흥열)	X
13	X.1152	Q.9	2008-05	Secure end-to-end data communication techniques using trusted third party services	일본	X
14	X.1161	Q.9	2008-05	Framework for secure peer-to-peer communications	일본	X
15	X.1162	Q.9	2008-05	Security architecture and operations for peer-to-peer network	한국 (나재훈)	2008-754 추진중
16	X.1171 (under AR)	Q.9	2008-09	Framework for protection of personally identifiable information in networked ID services	한국 (최두호)	TTAS.KO-06.014 6
17	X.homesec-4	Q.9	2008-11	Authorization framework for home network	한국 (김건우)	X
18	X.iptvsec-1	Q.9	2008-11	Functional requirements and architecture for IPTV security aspects	중국, 한국 (염흥열), 미국, 일본	X
19	X.iptvsec-2	Q.9	2010-12	Requirement and mechanism for sescure transcodable scheme of IPTV	한국 (나재훈)	2008-755 추진중
20	X.iptvsec-3	Q.9	2010-12	Key management framework for secure IPTV communication	한국 (염흥열)	X
21	X.mcsec-1	Q.9	2010-12	Security requirements and framework in multicast communication	한국 (윤미연, 염흥열)	2008-747 추진중
22	X.usnsec-1	Q.9	2010-12	Security framework for ubiquitous sensor network	한국 (염흥열, 김현)	X



〔그림 2〕 연구과제 9 - 모바일 보안



〔그림 3〕 연구과제 9 - 홈네트워크 보안

고 있다. 또한, 각각의 인증구조에서 요구되는 보안사항과 협의절차, 인증 및 키분배 수행절차 등을 정의하고 있고, 3GPP와 3GPP2에서 개발한 인증모델과의 비교/분석 항목을 부록으로 정의하고 있다[9]. X.1125 국제표준의 주요내용은 모바일 네트워크 환경에서 사용자들의 단말과 네트워크 내에 설정되어 있는 보안상관 서버와 협력하여, 현재의 네트워크 상태나 단말의 보안 상태를 분석하고 잠재적인 공격(웜, 바이러스 등)들을 제어하는데 목적을 두고 있다. 즉, 보안상관 서버는 해당 모바일 네트워크로 접속되는 단말의 보안 상태를 보고 받고, 이를 분석하여 해당 네트워크에서 안전하게 통신할 수 있도록 단말의 보안 상태를 업데이트하거나 지속적으로 관리하는 역할을 수행한다. 또한, 해당 단말기가 현재 위치한 네트워크에서 다른 외부 네트워크로 이동할 경우, 다른 보안상관 서버로 본 서비스를 중계해주는 방법까지를 포함하여 정의하고 있다. 즉, X.1125에서는 모바일 단말기와 보안상관 서버 간에 통신할 수 있는 방법, 절차, 보안정책, 구현을 위해 요구되는 인터페이스 정의와 이를 위한 XML 스키마 등을 정의하고 있다[10]. 또한, 한국은 지난 4월, 회의에서 사용자 단말 내에 존재하는 개인정보 및 보안위협들을 안전하게 관리하기 위한 표준초안을 제안하였으며, 향후, 기존에 제정된 5건의 표준들을 고려하여, 추가적으로 논의를 진행키로 합의하였다.

다음의 [그림 2]는 Q.9에서 개발한 모바일 보안 분야의 표준과 표준초안 간의 영역을 나타내고 있다.

2.2 홈네트워크 보안

ITU-T 내에 홈네트워크 분야는 각 SG 그룹 간에 담당하고 있는 영역에 따라, 개별적으로 표준화가 진행되고, 협력문서(Liaison)를 발행하여, 상호 간에 의견 조율 및 상호 검토를 통하여 표준초안을 개발하고 있다. 즉, SG9에서 케이블을 기반으로 멀티미디어 서비스를 지원하기 위한 기술이나 STX(셋탑박스) 관련 표준초안들을 개발하고 있으며, SG17에서는 보안적 관점에서 표준초안들을 개발하고 있다.

SG17 내에서 홈네트워크 보안 분야는 2004년 11월, 한국의 제안으로 표준화가 시작되었으며, 현재까지 한국 주도로 3건의 국제표준 제정과 1건의 표준초안이 개발중에 있다. 즉, 홈네트워크를 위한 보안기술 프레임워크(X.1111), 홈네트워크를 위한 디바이스 인증서 프로파일(X.1112), 홈네트워크 서비스를 위한 사용자 인증메커니즘 가이드라인(X.1113)을 국제표준으로 제정하였고, 홈네트워크를 위한 권한부여 프레임워크(X.homesec-4)가 개발중에 있다. 다음의 [그림 3]은 Q.9에서 개발한 홈네트워크 보안 분야의 표준과 표준초안 간의 영역을 나타내고 있다.

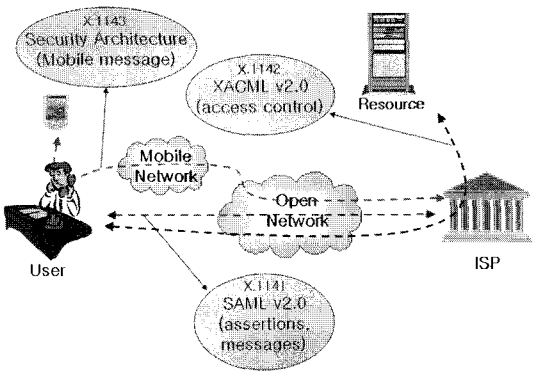
X.1111 국제표준의 주요내용은 댁내에 존재하고 있는 사용자 및 댁외에 존재하는 사용자들의 보안적 관점을 고려하여, 홈네트워크를 위한 보안 모델을 정의하였으며, 홈네트워크를 구성하는 각 객체들의 정의 및 각 객체들 간에 존재할 수 있는 보안위협들을 도출하였다. 또한, 이런 보안위협들을 해결하기 위한 보안요구사항들을 정의하였고, 보안요구사항들을 만족할 수 있는 보안기술들을 정의하였다. 그리고 보안적 관점에서 홈네트워크를 구축시 고려되어야 할 요구사항 및 보안기능들을 정의하였고, 끝으로 SG9에서 개발한 홈네트워크 모델과의 관계 정의 및 UPnP에서 정의한 홈네트워크

디바이스들 간에 관계를 비교 정의하였다[3]. X.1111에서 정의하고 있는 홈네트워크를 위한 보안 모델은 다른 SG 및 SG17 내에서 개발되고 있는 홈네트워크 표준초안들의 기본(baseline) 문서로 활용되고 있다. X.1112 국제표준의 주요내용은 홈네트워크 내(댁내/외)에 존재하고 있는 다양한 디바이스들을 적합한 사용자만이 사용할 수 있도록 인증서를 이용하여 각각의 디바이스들을 인증하기 위한 방법, 프로파일, 활용사례, 고려사항 등을 정의하고 있다. 디바이스 인증을 위한 방법으로는 댁외에 외부 인증센터를 두고 운용하는 방법과 댁내에서 자체적으로 각 디바이스들의 인증서를 발급하고 관리하는 방법이 있는데, X.1112에서는 후자의 방법으로 홈게이트웨이가 인증서를 발급하고 관리하는 역할을 수행하고 있다. X.1112에서 정의된 인증서 프로파일은 X.509v3을 기반으로 정의하고 있어, 기존의 인증서들과도 상호운용성이 보장된다[4]. X.1113 국제표준의 주요내용은 홈네트워크 내(댁내/외)에 존재하는 사용자들이 댁내에서 외부에 있는 다양한 서비스를 이용하거나 외부에서 댁내에 있는 다양한 서비스를 이용하고자 할 때, 적합한 사용자 인지를 확인하기 위해 요구되는 사용자 인증 서비스 구조와 홈네트워크를 구성하는 각 객체들의 역할 및 고려사항들을 정의하고 있다. 또한, 사용자 인증을 위해 사용될 수 있는 다양한 인증 메커니즘을 고려한 컴포넌트들을 정의하였고, 이때 고려되는 보안위협과 고려사항들을 정의하고 있다. X.1113에서 고려되고 있는 사용자 인증수단으로는 패스워드, 바이오정보, 개인키, 인증서 등이 고려되고 있으며, 인증 메커니즘을 위한 보안 보증 등급을 3단계로 분리하여, 각 등급에서 적합한 인증수단이 요구됨을 정의하고 있다[5]. 마지막으로 현재 개발되고 있는 표준초안(X.homesec-4)의 주요내용은 홈네트워크 내에 있는 다양한 서비스 및 자원들을 이용하고자 하는 사용자나 디바이스들의 접근 권한을 관리하기 위한 표준이다. 즉, 홈네트워크에서 권한부여 관리를 위한 고려사항, 권한부여 객체들의 정의 및 상호관계, 권한부여 객체와 홈네트워크를 구성하는 객체들 간의 관계, 권한부여 모델, 권한부여를 위한 요구사항 및 보안위협 정의, 현재 사용되고 있는 권한부여 방법 정의, 권한부여를 위한 개념적인 정책 모델, 활용사례 등을 정의하여 개발하고 있다[27]. 현재 X.homesec-4는 금년 9월, SG17 회의에서 승인 후 국가별 의견수렴(Consent)으로 추진될 예정이다.

2.3 웹서비스 보안

웹서비스 보안 분야는 2005년 7월, OASIS에서 개발한 XML 기반의 보안 표준들을 ITU-T 차원으로 확대하여 국제표준으로 도입 및 개발하자는 캐나다의 제안으로 시작되었다. 현재까지 Q.9에서 개발되어 제정된 국제표준으로는 보안주장마크업언어 (SAMLv2.0, X.1141), 확장성 접근제어마크업언어 (XACMLv2.0, X.1142)와 한국에서 제안한 모바일 웹서비스에서의 메시지 보호를 위한 보안구조(X.1143) 총 3건이 개발되었다. 다음의 [그림 4]는 Q.9에서 개발한 웹서비스 보안 표준들 간에 관계를 나타내고 있다.

X.1141 국제표준의 주요내용은 보안 정보를 교환하기 위한 XML 기반의 프레임워크를 정의하는 표준이다. 즉, 통신 주체들(사용자, 컴퓨터, ISP 등) 간에 요구되는 보안주장(인증, 권한부여, 속성 등)들을 XML 언어로 표현하기 위한 방법과 주체들 간에 교환되는 메시지 형식 및 프로토콜을 XML 언어로 정의하고 있다. SAMLv2.0 구성은 주장 및 프로토콜, 메타데이터, 바인딩, 프로파일, 인증문맥, 적합 요구사항, 스키마, 보안 및 프라이버시 고려사항 등으로 구성된다[11]. X.1142 국제표준의 주요내용은 통신 주체들 간에 요구되는 접근제어 정책들을 XML 언어로 표현하기 위한 방법을 정의하고 있다. 즉, 임의의 어떤 자원에 접근하고자 하는 객체들에게 일정한 권한을 부여하는 정책과 이들 정책을 평가하는 규칙, 이를 XML로 표현하는 방법들을 정의하고 있다. XACMLv2.0 구성은 코어, 계층구조의 RBAC 프로파일, 다중자원 프로파일, XACML를 위한 SAMLv2.0, XML 전자서명 프로파일, 계층구조의 자



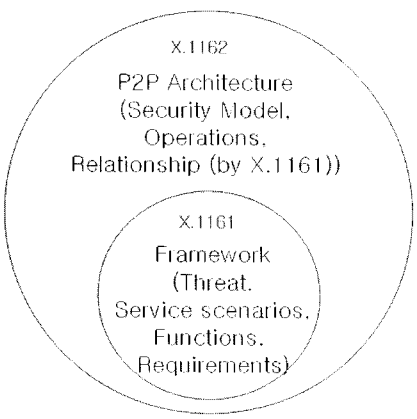
[그림 4] 연구과제 9 - 웹서비스 보안

원 프로파일, 프라이버시 정책 프로파일, 데이터 타입 및 기능 정의, 식별자 정의, 컴바인 알고리즘, 스키마, 보안 고려사항, 활용사례 등으로 구성된다[12]. X.1143 국제표준의 주요내용은 모바일 웹서비스에서 메시지 보호를 위한 보안구조와 다양한 서비스 시나리오를 정의하고 있다. 즉, SOAP 메시지가 방화벽에서 필터링이 되고 있지 않기 때문에 메시지 필터링할 수 있는 메커니즘을 보안구조로 단일화하였고, 이를 지원하기 위한 보안정책 메커니즘, 모바일 웹서비스 응용과 다른 응용간에 상호연동이 가능한 메커니즘을 정의하고 있다. 또한, 보안구조에 따른 활용사례와 다른 표구화기구(Parlay X, MWSSG, OMA)에서 개발된 표준들 간에 비교 사항을 정의하고 있다[13].

2.4 P2P 보안

P2P(peer-to-peer) 보안 분야는 불법적인 콘텐츠 배포 및 악의적인 목적 등의 이용으로 사람들에게 잘못된 기술로 오해받는 시절이 있었지만, 현대사회에서 P2P 통신으로 서비스되거나 다양하게 응용되고 있어, 해당 기술을 배제하기 보다는 보안 부분을 강화한 P2P 통신 기술 개발과 표준화의 중요성이 부각되고 있다. Q.9에서는 2005년 10월, 한국과 일본의 제안으로 표준화가 시작되었으며, 안전한 P2P 통신을 위한 프레임워크(X.1161), P2P 네트워크를 위한 보안구조 및 운영방법(X.1162) 총 2건이 제정되었다. 다음의 [그림 5]는 Q.9에서 개발한 P2P 보안 표준들 간에 관계를 나타낸다.

X.1161 국제표준의 주요내용은 다양한 P2P 통신에서 공통적인 특징들과 기본적인 서비스 시나리오를 기반으로 보안위협과 보안요구사항들을 정의하였으며, 이들의 보안요구사항을 충족하기 위한 보안기능들을 정의하고 있다[16]. X.1162 국제표준의 주요내용은 다양한 P2P 통신을 고려한 공통된 보안구조 및 모델을 정의하고 있으며, 이 모델을 근거로 P2P 통신의 운영방법, X.1161에서 정의하고 있는 보안요구사항과의 관계 정의 및 보안기능들과의 관계를 정의하고 있다. 또한, 부록으로 다양한 P2P 통신 모델들을 정의하고 있다[17].



[그림 5] 연구과제 9 - P2P 보안

2.5 멀티캐스트 보안

SG17 내에서 멀티캐스트 분야는 Q.1에서 표준화 작업이 이루어지고 있으며, Q.9에서는 보안적 측면에서 Q.1과 협력하여 멀티캐스트 보안 표준을 개발하고 있다. 현재, Q.9 내에서는 한국의 제안으로 멀티캐스트 보안을 위한 요구사항 및 프레임워크(X.mcsec-1)와 중계전송 멀티캐스트 프로토콜의 보안 확장 파트(X.603.1 Amd.1) 총 2건의 표준초안을 개발하고 있다.

X.mcsec-1 표준초안의 주요내용은 IETF와 ITU-T 내에서 기 제정된 국제표준들에서 정의하고 있는 다양한 멀티캐스트 모델들을 분석하고, 이들 모델에서의 보안위협 사항 및 보안요구사항들을 정의할 계획이다. 또한, 이들의 보안요구사항들을 만족하기 위한 멀티캐스트 보안구조, 보안기능, 보안기술 등을 고려하여 개발중에 있다[20]. X.603.1 Amd.1 표준초안의 주요내용은 X.603 (중계전송방식 멀티캐스트 프로토콜 - 1:N 그룹 응용) 국제표준에 보안 기능을 추가하기 위한 표준초안이다. 즉, 1:N 그룹 통신을 위한 응용레벨에서의 보안기능 정의와 보안요구사항, 그룹통신을 위한 보안프로토콜 운영방법 및 메시지 교환 형식, 데이터 암/복화 방법, 그룹 키 관리방법 및 활용사례 등을 고려하여 개발중에 있다[19]. 현재 X.mcsec-1 표준초안은 개발 시작단계에 있고, X.603.1 Amd.1은 2009년도 초에는 국제표준 개발이 완료될 예정이다.

2.6 USN 보안

ITU-T 내에서 USN 기술 표준화는 이슈별로 각 SG에서 진행되고 있다. 즉, SG13에서는 NGN 환경에서의 USN 표준 개발, SG16에서는 멀티미디어 서비스 관점에서의 USN 표준 개발, SG17에서는 보안 관점에서의 USN 표준 개발이 진행되고 있으며, SG11에서는 USN

환경에서의 시험방법 등의 표준 개발을 위한 신규 연구과제 신설이 고려되고 있다.

Q.9에서 USN 보안 분야는 한국의 제안으로 연구가 시작되었으며, ISO/IEC JTC1/SC6 그룹과 협력하여 ITU-T/JTC1 공동 표준을 개발하기 위해 현재 SC6에서 NP(New work item proposal) 투표를 진행하고 있다 (2008년 10월 완료예정). 현재 개발 중에 있는 USN을 위한 보안 프레임워크(X.usnsec-1)의 주요내용은 무선 센스 네트워크와 IP 네트워크를 모두 고려한 보안 모델을 정의하고 있으며, USN 보안 모델에서의 보안위협과 보안요구사항 정의, 보안요구사항을 만족하기 위한 보안기능 및 보안기술 정의, 보안기술들을 구현하기 위한 고려사항 등의 내용으로 표준초안을 개발하고 있다[25]. 또한, 한국은 2008년 4월, SG17 회의에서 USN 보안 표준화 로드맵을 제안하여, 향후 USN 보안을 위한 인증 및 접근제어 기술, 키관리 가이드라인, 안전한 라우팅 메커니즘, 데이터 보호 방법, 프라이보호 방법 등을 고려하여 USN 보안 분야의 국제표준을 개발하기로 합의하였다[26].

2.7 NID(RFID) 보안

ITU-T 내에서 RFID 용어는 NID(Networked ID)로 불리어지고 있다. RFID 보안 분야는 한국의 제안으로 표준화 작업이 시작되었으며, Q.9에서는 태그 기반 네트워크 ID(Identification) 서비스에서 개인식별정보(PII : Personally Identifiable Information)를 보호하기 위한 프레임워크(draft X.1171)를 제시하기 위한 권고안이며, 국가별 의견수렴 단계를 걸쳐, 독일과 프랑스로부터 컴맨트가 접수되어, 현재 추가 의견조율 작업이 진행중에 있다. 또한, Q.6에서는 RFID에서 PII를 보호하기 위한 가이드라인(X.rfpg)이 개발중에 있으며, 금년 9월, SG17 회의에서 국가별 의견수렴으로 추진할 계획이다.

X.1171(draft) 표준초안의 주요내용은 네트워크 기반의 ID 서비스를 B2C(Business to Consumer) 환경에 응용하기 위한 표준이다. 즉, 태그 기반 ID 서비스를 적용한 기본 모델을 정의하고, 이때 발생할 수 있는 PII의 보안위협 및 노출될 수 있는 사례, PII를 안전하게 보호하기 위한 요구사항, 이를 네트워크 기반 ID 서비스로 PII를 보호하기 위한 방법을 정의하고 있다. 또한, 부록으로 실제 활용사례 및 태그 기반 ID 서비스에서의 개인식별정보 보호를 위한 구체적인 방법을 정의하고 있다[18]. X.rfpg 표준초안의 주요내용은 프라이버시 침해에 대한 기본 원칙을 정의하고 있으며, 이를 근거로 RFID 환경에서 발생할 수 있는 프라이버시 위협을 정의하고 있다. 또한, 실제 RFID 서비스의 응용(물건판매, 수송, 헬스케어, 전자정부, 모바일)들과 이때 발생할 수 있는 위협 사항들을 정의하였고, 이런 위협에서 PII를 보호하기 위한 가이드라인을 제시하고 있다[24]. X.rfpg 표준초안은 금년 9월, SG17 회의에서 국가별 의견수렴으로 추진될 예정이다.

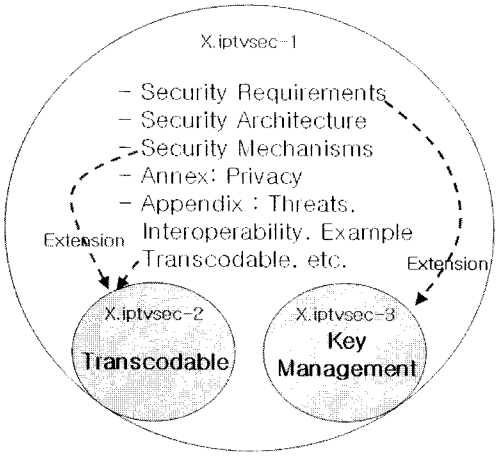
2.8 응용서비스 보안

응용서비스 보안 분야는 정보통신 환경에서 안전한 통신 환경 보장과 다양한 응용서비스 등에 접목 가능한 부분들을 표준화하고 있다. Q.9에서는 키교환이 가능하고 안전한 패스워드 기반의 인증프로토콜 가이드라인(X.1151)과 신뢰된 제3의 기관(TTP : Trusted Third Party) 서비스를 이용한 안전한 종단간 데이터통신 기술(X.1152) 총 2건의 국제표준을 제정하였다.

X.1151 국제표준의 주요내용은 기억하기가 편하고 별도의 인프라(PKI 등) 환경이 요구되지 않는 패스워드 기반의 인증 프로토콜에 대한 가이드라인을 제시하기 위한 표준이다. 즉, 패스워드 기반의 프로토콜이 가지고 있는 문제점, 운영절차, 특징들을 분석하여, 안전성 확보를 위해 요구되는 요구사항들을 선별하였고, 사용자가 프로토콜 설계 시, 안전성에 따라 패스워드 기반의 인증프로토콜을 선택할 수 있는 기준을 정의하고 있다. 또한, 기존에 연구되어 발표된 다양한 패스워드 기반의 인증프로토콜들과 안전성 비교 및 평가기준을 정의하고 있다[14]. X.1152 국제표준의 주요내용은 온라인 상에서 TTP 서비스를 이용하여 안전하게 종단간 데이터통신이 가능하기 위한 기본 인터페이스, 상호연동 방법, 보안 고려사항 등을 정의하고 있다. 또한, 기본 모델은 2개의 객체 간에 TTP 서비스를 이용하고 있으나, 이를 다수의 객체로 확장하여 이용할 수 있는 방법을 정의하고 있으며, 이들에 대한 서비스 시나리오 및 기존에 개발된 TTP 서비스 관련 국제표준들과의 비교를 통한 차별성을 정의하고 있다[15].

2.9 IPTV 보안

ITU-T 내에 IPTV 분야는 실제 상용화가 가능하고



〔그림 6〕 연구과제 9 - IPTV 보안

한국에서는 직접적으로 서비스가 실행되고 있어, 여러 국가에서 많은 관심과 적극적인 표준화 활동에 참여하고 있는 분야이다. Q.9에서 IPTV 보안 분야는 2008년 1월, FG-IPTV 활동의 결과물인 IPTV 보안적 측면을 고려한 기능 요구사항 및 구조(X.iptvsec-1)를 시작으로 표준화 활동을 착수하였고, 중국, 한국, 일본, 미국이 에디터쉽을 확보하여 공동으로 개발중에 있다. 또한, 2008년 4월, 한국의 제안으로 IPTV 트랜스코더블(transcodable) 기술을 위한 요구사항과 메커니즘(X.iptvsec-2)을 제안하여 개발하기로 합의되었고, 2008년 5월, 한국에서 IPTV를 위한 키관리 프레임워크(X.iptvsec-3)를 제안하여 채택되었다. 이와 같이, ITU-T 내에서 많은 관심을 받고 있는 IPTV 보안 신규 분야에 한국 주도로 국제표준을 개발할 수 있는 좋은 발판을 마련하고 있다. 다음의 [그림 6]은 Q.9에서 개발하고 있는 IPTV 보안 분야 표준초안들의 관계를 나타내고 있다.

X.iptvsec-1 표준초안의 주요내용은 IPTV 구조, 콘텐츠 보안, 서비스 보안, 네트워크 보안, 단말기 보안, 가입자 보호측면에서 보안 요구사항들을 분리하여 정의하였고, 이들을 고려한 IPTV 보안구조를 정의하고 있다. 또한, 보안구조를 바탕으로 콘텐츠 보호구조, 서비스 보호구조를 정의하고, 각각의 구조에서 요구되는 보안기능 및 컴포넌트들의 기능들을 정의하고 있다. 그리고 이런 보안 기능들을 충족하기 위한 보안메커니즘을 제안하고 있으며, 부속서(Annex)로 가입자 보호를 위한 방법을 정의하고 있다. 부록(Appendix)으로는 앞에 언급된 다양한 측면에서의 보안위협들을 정의하고, 서비스와 콘텐츠 보호를 위한 상호운용성 확보 방안과 콘텐츠 보호 활용사례 및 안전한 트랜스코더블 기술을 간단히 언급하고 있다[21]. X.iptvsec-2 표준초안의 주요내용은 X.iptvsec-1에서 간단히 언급되고 있는 트랜스코더블 기술을 보다 구체화하여 실제 사용이 가능한 보안요구사항과 메커니즘을 개발하고자 제안하고 있다. X.iptvsec-2는 시작 단계에 있어 아직 구체적인 문서는 없지만, 제안 단계에서 트랜스코더블 기술의 기본구조와 단일 및 다중 트랜스코더블을 적용할 수 있는 구조를 제안하고 있다[22]. X.iptvsec-3 표준초안의 주요내용은 X.iptvsec-1에서 키 관리(생성, 저장, 분배, 삭제, 보관, 응용) 기능을 간단히 언급하고 있지만, IPTV는 유니캐스트, 멀티캐스트, 브로드캐스트 통신들을 모두 고려하고 있어, 보안적 측면에서 서로 다르게 키관리 기능이 적용됨으로 매우 중요하다. 따라서 한국은 IPTV 서비스 상에서 요구되는 전반적인 키 관리 기능을 정의하고자 제안하였다[23].

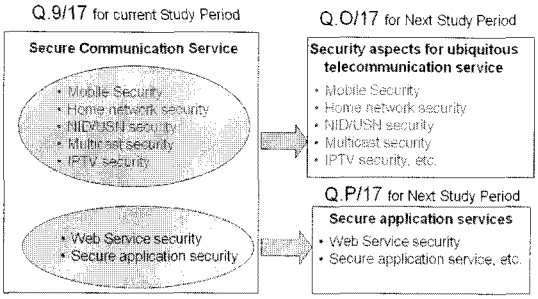
Ⅲ. 차기 연구회기('09~'12) 구조조정 방향 및 대응 전략 수립[2]

국제표준화기구 ITU-T는 4년 주기로 전체적인 SG들의 구조조정과 각 SG 산하 연구과제들을 재조정하고 있다. 2008년 4월, SG17 회의에서 전체적인 구조조정을 토의하였으며, 결과적으로 이번 연구회기에는 보안 분야가 총 7개의 연구과제로 진행 되었지만, 차기 연구회기에서는 총 13개의 연구과제로 확대하여 정보통신 보안 분야의 표준화를 추진하기로 합의되었다. 본 절에서는 Q.9의 구조조정 방향만을 집중적으로 다룬다.

3.1 차기 연구회기 구조조정 방향

앞에서 언급된 바와 같이 Q.9에서는 안전한 통신 서비스라는 주제 하에 크게 9가지 분야로 표준화가 진행되었으며, SG17 내에서 가장 많은 활동과 많은 결과물을 산출한 중요한 그룹이다. 하지만, 급속도로 변화하는 사회에서 새로운 기술들에 대한 고려가 요구되고, 보다 효율적인 운영을 위해, 크게 통신서비스 관점과 응용서비스 관점으로 [그림 7]과 같이 분할하기로 하였다.

차기 연구회기에서 활동하게 될, 첫 번째 연구과제는 유비쿼터스 정보통신 서비스를 위한 보안 측면이라는 주제 하에 모바일 보안, 홈네트워크 보안, NID/USN 보



〔그림 7〕 연구과제 - 구조조정 방향

안, 멀티캐스트 보안, IPTV 보안 분야를 다루기로 하였다. 또한, 두 번째 연구과제는 안전한 응용서비스라는 주제 하에 웹서비스 보안과 안전한 응용서비스 기술들을 다루기로 합의되었다. 두 번째 연구과제는 Q.T/17로 신규로 신설되는 SOA(Service Oriented Architecture) 보안 연구과제와 중복되는 부분들이 있어, 향후 표준화 활동을 통해 의견조율이 필요한 부분이다.

3.2 대응전략 수립 및 고려사항

차기 연구회기에서 Q.9를 분할키로 합의된 사항은 한국에서 주도적으로 제안하여 이룩한 성과이다. 즉, 국내에서 개발되고 있는 다양한 정보보호 기술을 보다 쉽게 제안할 수 있는 기회를 확보하기 위함이고, 더 나아가 회의 주재가 가능한 의장단 확보도 고려해 볼 사항이다. 결과적으로 한국은 새롭게 시작하게 될 2개의 연구과제에 한국 주도가 가능하고, 우리에게 유리한 표준 개발을 위해서 대응전략 수립과 고려사항들을 고민해야 할 시점이다.

첫 번째로는 2개의 분야에서 지속적으로 활동이 가능한 표준화 전문가들의 확보 방안이다. 기존의 Q.9에서 활동하고 있던, 전문가들을 중심으로 신규로 이슈화되고 있는 분야에 대한 전문가들을 사전에 섭외하여 함께 국제표준화 회의에 참석할 수 있는 기회와 지원이 고려되어야 한다. 두 번째로는 의장단 확보를 위한 전략이 필요하다. 기존 의장(염흥열, 순천향대)을 비롯하여, 신규로 시작되는 연구과제에 전반적으로 커버가 가능한 전문가를 연구회기 시작 전에 국내에서 사전 선별하는 작업이 필요하다. 또한, 한국을 지지해 줄 수 있는 다른 국가들의 전문가들을 섭외하는 것이 고려되어야 한다. 세 번째로는 국내 정보보호 산업체에서 표준화 활동에 참여할 수 있는 방안이 필요하다. 국내 정보보호 산업체에서 강점을 가지고 있는 IPTV, RFID, 홈네트워크 보안 등에 뛰어난 기술을 국제표준으로 제안할 수 있는 기회와 재정적으로 지원이 가능한 방법을 모색해야 된다. 네 번째로는 국내에서 표준화 활동을 하고 있는 TTA 표준화위원회, 전략포럼, SG17 분과위원회 간에 상호 협력할 수 있는 방안이 필요하다. 특히, 국내에서 진행되고 있는 표준화 방향과 국제적으로 진행되고 있는 표준화 방향이 조율되도록 지속적인 정보공유와 합동 회의 등이 필요하다. 다섯 번째로는 한중일 간에 공동으로 협력할 수 있는 인프라 구축이 필요하다. ITU-T 내에서 정보보호 분야는 아시아 지역에서 주도하고 있어, 현재 아시아 지역에서 활동하고 있는 ASTAP, RAISE 포럼, CJK SWIS 등을 활용하여, 향후 ITU-T에서 국제표준을 개발할 때, 상호 간에 협력체계와 지지 발언 등을 받을 수 있는 관계 유지가 필요하다. 여섯 번째로는 한국에서 주도하고 있는 IPTV 보안, 홈네트워크 보안, RFID 보안, 멀티캐스트 보안 분야에 계속적인 주도가 가능하도록, 다양한 신규 과제 발굴과 진행되고 있는 표준초안들의 완성도를 높일 수 있는 방법이 필요하다. 일곱 번째로는 다른 국가에서 주도하고 있는 모바일 보안 분야 등에 지속적인 검토를 통하여, 국내 의견이 충분히 반영될 수 있도록 적극적인 참여가 요구된다.

Ⅳ. 결 론

본 논문에서는 ITU-T SG17 WP2 산하 Q.9에서 이번 연구회기 동안 개발한 국제표준 및 현재 개발중에 있는 표준초안들에 대해 간단히 살펴보았다. 한국은 이번 연구회기 동안 다른 어느 나라 보다, 많은 참가자와 많은 기고서를 제출하여 국제표준에 국내 기술을 반영시키는 성과를 올렸으며, 보안 분야에서 국제표준을 좀 더 주도하기 위한 유리한 입지를 확보하였다. 특히, 홈네트워크 보안, RFID/USN 보안, 멀티캐스트 보안, IPTV 보안 등에서는 한국 주도로 국제표준들을 개발하고 있음을 확인하였고, P2P 보안, 응용서비스 보안, 웹서비스 보안 등에서도 적극적으로 국내 기술을 국제표준에 반영하고 있음을 확인하였다. 차기 연구회기에서 Q.9는 2개의 연구과제로 분리하기로 합의된 바, 국내 관련 산학연 전문가들의 적극적인 참여가 필요한 시점이다. 또한, Q.9 산하에서 개발되어 제정된 국제표준들은 국내 정보보호 시장성을 고려한 체계적인 분석을 통해 필요시, 국내표준으로 수용하는 작업이 필요할 것으

로 판단된다. ITU-T 내에서도 보안은 이제 선택사항이 아니고, 원천기술들에 대한 표준개발과 함께 시작하고 있어, 향후 그 중요성이 더욱 커질 것으로 판단된다.

참고문헌

[1] Mr. Herbert Bertine, "GSC-13-STSC6-05: ITU - Security/Cybersecurity", GSC-13 Meeting, USA Boston, 14-17 July 2008.

[2] ITU-T SG17, "TD0409Rev.1 : Draft SG17 Report to WTSA 08: Part 2 - Questions proposed for study during the next study period (2009-2012)", Swiss Geneva, 7-18 April 2008.

[3] ITU-T Recommendation X.1111, "Framework of security technologies for home network", ITU-T SG17, February 2007.

[4] ITU-T Recommendation X.1112, "Device certificate profile for the home network", ITU-T SG17, November 2007.

[5] ITU-T Recommendation X.1113, "Guideline on user authentication mechanism for home network services", ITU-T SG17, November 2007.

[6] ITU-T Recommendation X.1121, "Framework of security technologies for mobile end- to-end data communication", ITU-T SG17, April 2004.

[7] ITU-T Recommendation X.1122, "Guideline for implementing secure mobile systems based on PKI", ITU-T SG17, April 2004.

[8] ITU-T Recommendation X.1123, "Differentiated Security Service for Secure Mobile End-to-End Data Communication", ITU-T SG17, November 2007.

[9] ITU-T Recommendation X.1124, "Authentication Architecture for Mobile End-to-End Communication", ITU-T SG17, November 2007.

[10] ITU-T Recommendation X.1125, "Correlative Reacting System in Mobile Data Communication", ITU-T SG17, January 2008.

[11] ITU-T Recommendation X.1141, "Security Assertion Markup Language (SAML 2.0)", ITU-T SG17, June 2006.

[12] ITU-T Recommendation X.1142, "eXtensible Access Control Markup Language (XACML 2.0)", ITU-T SG17, June 2006.

[13] ITU-T Recommendation X.1143, "Security Architecture for Message Security in Mobile Web Services", ITU-T SG17, November 2007.

[14] ITU-T Recommendation X.1151, "Guideline on secure password-based authentication protocol with key exchange", ITU-T SG17, November 2007.

[15] ITU-T Recommendation X.1152, "Secure end-to-end data communication techniques using Trusted Third Party services", May 2008.

[16] ITU-T Recommendation X.1161, "Framework for secure peer-to-peer communications", May 2008.

[17] ITU-T Recommendation X.1162, "Security architecture and operations for peer-to-peer network", May 2008.

[18] Dooho Choi, Heung-Youl Youm, "Final draft recommendation of X.nidsec-1 (Framework for Protection of Personally Identifiable Information in Networked ID Services), ITU-T SG17, TD4025Rev.3, April 2008.

[19] Miyeon Yoon, Hyuncheol Jung, "Revised draft text of X.603.1 Amd.1: Relayed Multicast Protocol- Part 2 security extensions", ITU-T SG17, TD4048, April 2008.

[20] Miyeon Yoon, Hyuncheol Jung, Heungyoul Youm, "Draft text of X.mcsec-1: Requirements and Framework for Multicast Security", ITU-T SG17, TD4049, April 2008.

[21] Wei Xie, Heung-Youl Youm, Shinji Ishii, Nhut Nguyen, "Revised draft Recommendation X.iptvsec-1 : Functional Requirements and Architecture for IPTV Security Aspects", ITU-T SG17, TD4096, June 2008.

[22] Jabeom Gu, "Proposal of new transcodability work item for IPTV security", ITU-T SG17, C283, March 2008.

[23] Heung-Youl Youm, "Proposal for new work item on a key management framework for secure IPTV communications", ITU-T IPTV-GSI, C74, April 2008.

[24] Hyangjin Lee, Kilsoo Chun, "Proposed revised working document of X.rfpg : Guideline on protection for personally identifiable information in RFID application", ITU-T SG17, C299, March 2008.

[25] Heung-Youl Youm, Hyun Kim, "Updated text on X.usnsec-1", ITU-T SG17, TD4023, April 2008.

[26] Hyun Kim, Eunyoung Choi, Sukyoung Ahn, Haeryong Park, Kilsoo Chun, "Proposal of roadmap on USN security", ITU-T SG17, C288, March 2008.

[27] Geon-Woo Kim, Jong-Wook Han, Kyo-il Chung, "Revised Draft Recommendation on X.homesec-4: Authorization Framework for Home Network", ITU-T SG17, TD4094, June 2008.

[28] 진병문, 오흥룡, 염흥열, 강신각, "2007년 ITU 국제표준화 활동보고서 : 개방형통신기술, 보안, 언어/소프트웨어 분야(SG17)", MIC, 제14호, 전파연구소, pp186-201, 2007.12.

[29] 진병문, 오흥룡, 염흥열, 강신각, "ITU 연구동향 : ITU-T SG17 분야", MIC, 통권 제13호, 한국ITU연구위원회, pp317-337, 2006.11.

[30] 진병문, 오흥룡, 염흥열, 강신각, "2005년도 ITU-T 연구활동 보고서 : ITU-T SG17 연구동향", TTA, pp216-254, 2005.12.

[31] 오흥룡, 염흥열, "안전한 통신 서비스 표준화 동향 및 향후전망", 한국정보보호학회 학회지, 제17권 제1호, pp63-78, 2007.02.

[32] 오흥룡, 염흥열, "정보보호 국제표준화 동향 및 향후 전망", 한국정보보호학회 학회지, 제17권 제6호, pp93-105, 2007.12.

〈著者紹介〉

오 흥 룡 (Heung-Ryong Oh)
정회원

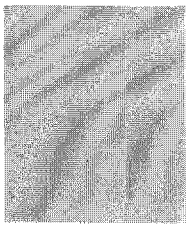
2002년 2월 : 순천향대학교 전자공학과 졸업
2004년 2월 : 순천향대학교 정보보호학과 석사
2007년 6월 : 순천향대학교 정보보호학과 박사 수료
2004년 2월~현재 : 한국정보통신기술협회 표준화본부
2004년 11월~2007년 2월 : ITU-T X.1111 국제표준 Associate Editor
2005년 3월~현재 : ITU-T SG17 국내 분과위원회 간사
<관심분야> 보안프로토콜, 정보보호표준

나 재 훈 (Jae-Hoon Nah)
종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 전자정보공학과 박사
1987년 2월~현재 : 한국전자통신연구원 책임연구원
2005년 10월~2008년 5월 : ITU-T X.1162 Editor
2008년 4월~현재 : ITU-T X.iptvsec-2 Editor
2006년 2월~현재 : ITU-T SG17 국내 분과위원회 위원
<관심분야> 네트워크 보안, IPv6/MIPv6 보안, P2P 보안, IPTV 보안

염 흥 열 (Heung-Youl Youm)
종신회원

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 9월 : 한양대학교 전자공학과 석사
1990년 2월 : 한양대학교 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사, (현)논문지편집위원장, (현)상임부회장
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2005년 3월~현재 : ITU-T SG17 국내 분과위원회 부의장
2006년 11월~2008년 2월 : 정보통신부 정책자문단 정보보호 PM
2006년 11월~현재 : IITA 정보보호 PM
<관심분야> 네트워크 보안, IPTV 보안, USN 보안, 홈네트워크 보안, 응용보안



김 대 경 (Dae-Kyung Kim)

1995년 2월 : 경성대학교 컴퓨터공학과 졸업
2004년 2월 : 순천향대학교 정보보호학과 석사
2007년 2월 : 순천향대학교 정보보호학과 박사 수료
<관심분야> 네트워크 보안, 개인정보보호대책, USN 보안