정보보호 표준화 방향

염 흥 열
정보통신연구진흥원 정보보호 PM
순천향대 교수

》》》 요 약 《《《

정보보호 기술은 IT 서비스의 신뢰성을 보장하여 따뜻하고 안전한 유비쿼터스 사회를 구현하기 위한 핵심 기술 중 하나이다. 정보보호 글로벌 표준화는 ITU-T, ISO/IEC JTC1, IETF 등의 국제표준화기구에 의해 주로 추진되고 있다. 정보보호 기술은 보안 알고리즘, 정보보호 제품평가/관리체계, 인터넷 보안, 응용 보안 표준 등의 분야로 구분되어 표준화되고 있다. 서로 다른 국제 표준화 기구에서 각 분야에 대해 표준화를 추진되고 있다. ITU-T에서는 통신망 보안, ISO/IEC JTC1에서는 바이오 인식과 보안 알고리즘, IETF에서는 인터넷 보안, 3GPP/3GPP-2에서는 제3세대 이동통신망 보안에 초점을 두고 추진하고 있다. 본 고에서는 정보보호 기술과 관련된 국내외 표준화 동향을 살펴보고, 현재 이들 표준화 기구에서 우리나라가 주도하고 있는 주요 표준화 항목을 살펴보며, 향후 정보보호 분야에서 국내외 표준화 방향을 제시하고자 한다.

I. 서론

정보보호기술은 정보통신시스템에서 저장 및 유통되는 정보의 기밀성(정보누출 방지)과 무결성(데이터 위·변조 방지)을 보장하며, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 핵심 기술을 지칭한다[1]. 정보보호기술은 암호기술, 인증기술, ID 관리 기술, 바이오 인식기술, 시스템 보안, 네트워크 보안, 응용서비스 보안, 그리고 정보보호 제품 및 조직평가 등으로 구분될 수 있다. 암호기술은 기밀성, 무결성, 메시지 인증, 사용자 인증, 부인방지 등의 서비스를 위하여 요구되는 핵심 보안 알고리즘을 정의한다. 인증은 사용자의 신원을 확인하기 위한 기술이고 ID 관리는 주체 ID 생성에서 폐기까지 전 수명에 대한 ID를 관리하기 위한 기술이며, 바이오인식은 바이오 특성을 이용하여 사용자를 식별하는 기술이다. 시스템 보호 기술은 조직 혹은 개인의 컴퓨터와 정보를 안전하게 보호하는 기술이다. 네트워크 보호 기술은 인터넷과 같은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 불법 공격 행위로부터 네트워크를 통해 전달되는 정보를 보호하기 위한 기술을 말한다. 응용 보안 기술은 전자우편 등 다양한 응용 레벨을 위한 보호 기능을 제공한다. 정보보호 제품/조직 평가기술은 정보보호 시스템에 대한 보안성 평가와 조직에 대한 보안 관리, 그리고 암호모듈에 대한 기술이다.

정보보호 분야의 글로벌 표준화는 주로 IETF, ITU-T, ISO/IEC JTC1, 3GPP 등에서 주로 수행되고 있다[2]. 국내 정보보호 표준화 방향을 설정하기 위해서는 먼저 국제 정보보호 표준화 동향의 파악이 필요하며, 이를 바탕으로 국내 기술개발 정책과 연계된 표준화 추진전략의 설정이 요구된다. 본 고에서는 국제 표준화 기구에서 추진하고 있는 주요 표준안의 내용을 살펴보고, 국내 정보보호 분야의 표준화 방향을 제시한다. 또한 국내외 정보보호 추진 방향 설정을 위한 기본 원칙을 제시한다.

II. 정보보호 표준화 동향/ 방향

본 장에서는 정보보호 표준화와 연관되는 주요 국제 표준화 기구나 사실 표준화 단체에서 수행되고 있는 표준화 현황을 살펴보고, 이들 국제 표준화 기구에서 우리나라가 주도하고 있는 주요 표준화 현황을 살펴본다. 그리고 이를 바탕으로 우리나라 정보보호 글로벌 표준화 방향을 제시한다.

2.1 국외 정보보호 표준화 기구 동향

가. IETF 보안 표준화 동향

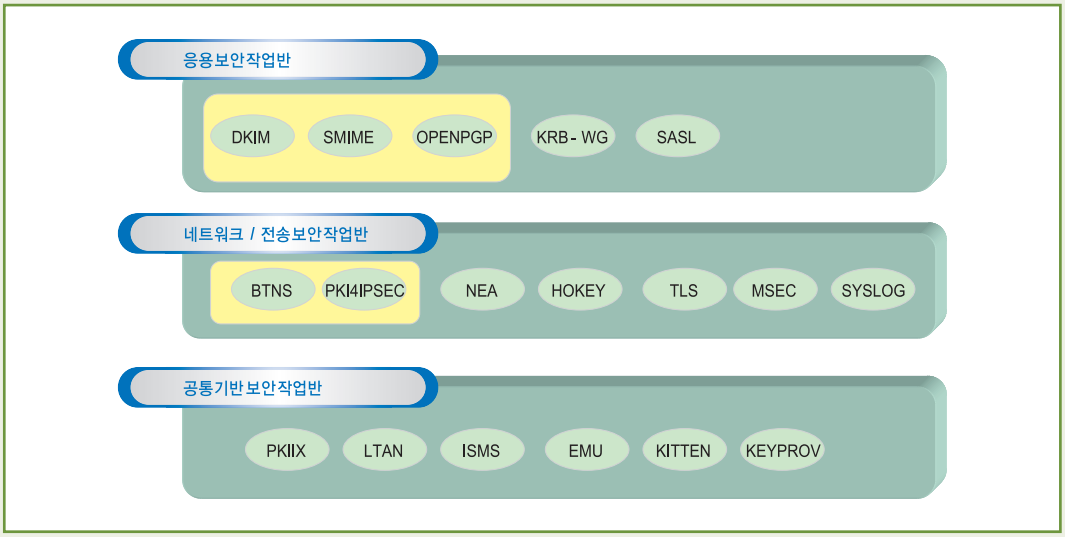
IETF는 여러개의 영역(Area)으로 구성되며, 이 중 정보보호 분야는 보안 영역(Security Area)에 의해 추진되고 있다[5]. 보안 영역은 네트워크 보안과 응용 보안, 그리고 공통 기반 보안 표준을 수행하며, 2007년 3월 현재, 18개 작업반(WG)을 통해 표준화를 진행하고 있다. IETF 보안 영역(Security Area) 내에 존재하는 여러 작업반은 응용보안작업반, 네트워크/전송보안작업반, 그리고 공통기반작업반으로 분류될 수 있다. 공통기반 분류의 경우, PKIX(Public-key Infrastructure, X.509) 작업반은 인터넷을 위한 공개키 기반구조, LTAN(Long-Term Archive and Notary Services) 작업반은 공개키 인증서 기반 장기 문서 보관, ISMS(Integrated Security Model for SNMP) 작업반은 PKI 기반의 SNMP 확장, EMU(EAP Method Update) 작업반은 차세대 EAP, KITTEN(GSS-API Next Generation)은 차세대 GSS 보안 인터페이스, 그리고 KEYPROV(Provisioning of Symmetric Keys) 작업반은 초기 이동 디바이스에 대한 대칭키 안전 배치에 대한 표준을 각각 개발하고 있다. 네트워크/전송 보안 분류의 경우, HOKEY(Handover Keying) 작업반에서는 무선망에서 안전한 핸드오버를 위한 키잉 표준, BTNS(Better-Than-Nothing Security)에서는 단방향 인증을 고려한 IPSEC 표준 변경, PKI4IPSEC(Profiling Use of PKI in IPSEC)에서는 IPSEC을 위한 효율적인 PKI 기법, NEA(Network Endpoint Assessment) 작업반은 최종 종단장치의

네트워크 접근을 평가, TLS(Transport Layer Security)는 종단간 전송계층 보안, MSEC(Multicast Security)에서는 멀티캐스트 보안, SYSLOG에서는 시스템 보안 사건의 안전한 전달/저장을 위한 표준을 각각 개발하고 있다. 응용 보안 분류의 경우, DKIM (Domain Keys Identified Mail)에서는 도메인 키를 이용하는 메일 보안, SMIME(S/MIME Mail Security)에서는 S/MIME 메일 보안, OPENPGP(An Open Specification for Pretty Good Privacy)에서는 PGP에 대한 공개 규격 표준, KRB-WG(Kerberos WG)에서는 커버러스 기반의 인증 프로트콜 표준, 그리고 SASL(Simple Authentication and Security Layer) 작업반은 인증 및 데이터보안 제공 프레임워크 표준을 개발하고 있다. 이외에도 이동성 지원 보안 표준이 MIP6(Mobile IPv6) 작업반에서 이동 노드 관련 보안 취약성을 제거하기 위해 개발되고 있다.

신원을 위해 주민등록번호와 같은 고유식별정보를 이용하여 수행하는 'SIM(Subscriber Identification Method)' RFC 4643 표준을 들 수 있다. 또한, SEED 관련 국제 표준 프로토콜 암호 슈트(IPSEC, TLS, CMS)와 관련된 4건 정도의 RFC 표준(RFC4269, 4196, 4162, 4010)이 KISA 주도로 개발 완료되었다.

나. ITU-T 보안 표준화 동향

ITU-T에서의 정보보호 표준화는 주로 SG17, SG13, 그리고 SG9에서 추진 중에 있다[6]. SG9에서는 디지털 케이블 망을 위한 보안 표준, SG13에서는 NGN(Next Generation Network)을 위한 보안 표준, 그리고 SG17에서는 일반 통신망에서 요구되는 보안 표준이 개발되고 있다. 먼저 SG17은 ITU-T에서 보안에 대한 선도 SG으로, 8개의 연구과제(Question)를 통하여 정보



(그림 1) IETF 보안영역작업반(2007. 3. 22)

국내 표준화 대응 조직은 TTA 산하의 PG101과 PG102 이며, 한국의 경우 국내 표준 알고리즘인 SEED 알고리즘을 TLS 프로토콜과 전자메일 등의 여러 응용 보안 프로토콜의 알고리즘 슈트로 채택케 하는 업적을 거뒀으나, 주도적인 표준화 활동이 아닌 참관자적인 입장의 표준화 활동에 머물러 있다. 우리나라가 개발한 대표적인 표준은 PKIX 작업반에서 추진한 인터넷 상에서 사용자

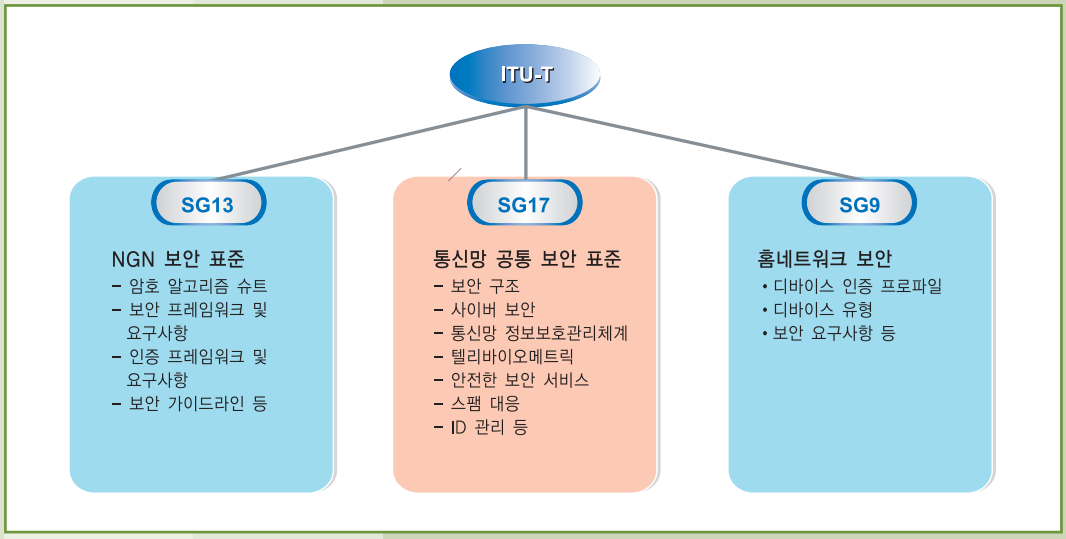
통신망을 위한 보안 표준화를 추진 중이다. 연구과제 1에서는 멀티캐스트 보안, 연구과제 4에서는 용어 정의 및 로드맵, 연구과제 5에서는 보안 구조 및 프레임워크, 연구과제 5에서는 사이버 보안, 연구과제 7에서는 보안 관리체계, 연구과제 8에서는 텔리바이오메트릭, 연구과제 9에서는 안전한 통신서비스, 그리고 연구과제 17에서는 기술적 스팸 대응 표준을 각각 개발하고 있다.

SG17에서는 사이버 인프라 보안, 멀티미디어 스팸 문제를 포함하는 스팸 대응, 모바일망 보안, 홈네트워크 보안, RFID 보안, 웹 서비스 보안, 텔레바이오메트릭 인식, 통신망 보안관리체계 등 다양한 통신 보안 주제를 다루고 있다. 최근 ITU-T SG17 산하에 ID 관리에 대한 FG(Focus Group)가 2006년 12월 결성되어 이 분야의 표준화를 추진하고 있다. SG13에서는 NGN을 위한 보안 표준을 개발하고 있다. SG13의 연구과제 15에서는 NGN 보안 프레임워크 및 요구사항, 인증 프레임워크 및 요구사항, AAA 프로토콜을 포함하는 디바이스 인증, IMS를 위한 보안 가이드라인, 능동적인 침입차단/대응을 위한 보안 가이드라인, NGN을 위한 보안 알고리즘 등에 대한 표준화를 진행 중이다[15]. SG9에서는 디지털 케이블 망에 적용될 수 있는 홈네트워크 보안 표준을 개발한 바 있고 주로 미국 디지털 케이블 망 표준을 준용하여 개발되었다. 전체적으로 살펴보면, ITU-T에서는 정보통신망을 위한 보안 구조, NGN 보안 표준, 그리고 홈네트워크 보안 표준을 추진하고 있다.

의 분야에서 주도하고 있다. 또한 SG13에서도 NGN을 위한 AAA 기술에 대한 표준을 개발하고 있다. 대표적인 국내 표준화 실적은 2007년도 초에 국가별 의견수렴 과정을 완료한 ITU-T X.1111 '홈네트워크 보안 프레임워크'를 들 수 있다. 한국은 현재 29건의 보안 표준의 에디터로 활동하고 있는 등 일본, 중국과 함께 보안 분야 표준화를 주도하고 있다고 볼 수 있다.

다. ISO/IEC JTC1 보안 표준화 동향

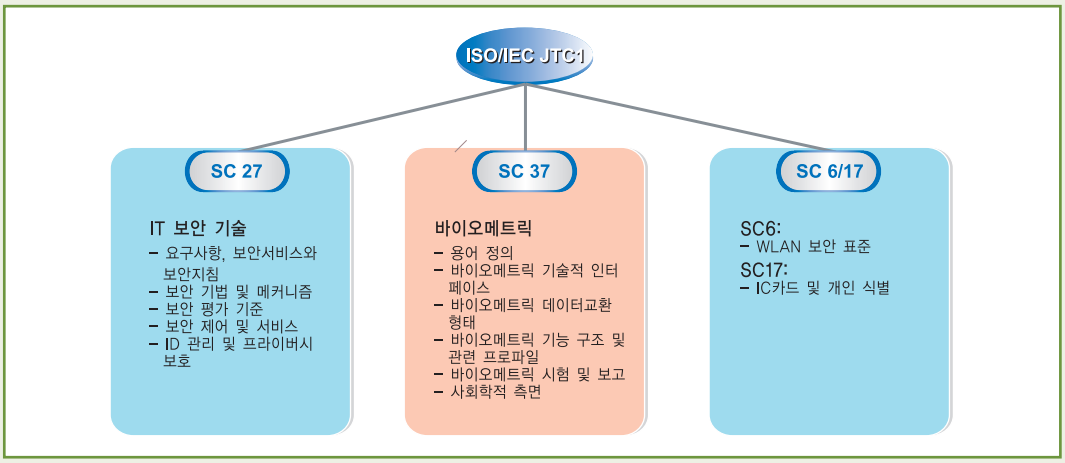
ISO/IEC JTC1 산하의 SC27, SC37, SC6에서 보안 관련 표준이 주로 개발되고 있다[7]. SC 27에서는 IT 보안에 대한 일반적인 보안 방법/기술에 대한 표준화를 담당하고 있다. 산하에 5개의 작업반(WG)이 존재하며, WG1 작업반에서는 IT 시스템 보안 서비스에 대한 일반 요구사항을 다루고 있고 WG2에서는 세부 보안 기술과 보안 메커니즘 개발을 다루며, WG3에서는 보안 제품의 평가 인증을 위한 표준을 개발한다. WG4에서는 보안관



(그림 2) ITU-T 보안 표준화

ITU-T에서 보안 표준은 우리나라 주도로 많은 표준들이 개발되고 있다. ITU-T 보안 표준 역시 국내 SG17분과 위원회를 중심으로 대응하고 있으며, 우리나라의 경우, 홈네트워크 보안, 텔레바이오메트릭, RFID 프라이버시 보호, 모바일 웹서비스 보안, 멀티미디어 스팸, 응용 프로토콜 가이드라인, 인증 및 키관리 프레임워크 등

리체계에 대한 표준을 개발하고 있으며, WG5에서는 ID 관리 및 프라이버시 보호 관련 표준을 개발하고 있다. 특히, ID 관리와 프라이버시 보호에 대한 표준개발은 ITU-T SG17 연구과제 6과 협력하여 개발될 필요가 있다. SC6에서는 통신망 및 시스템간 정보교환에 관한 표준을 다루며, 여기서는 데이터링크 계층에 대한 보안



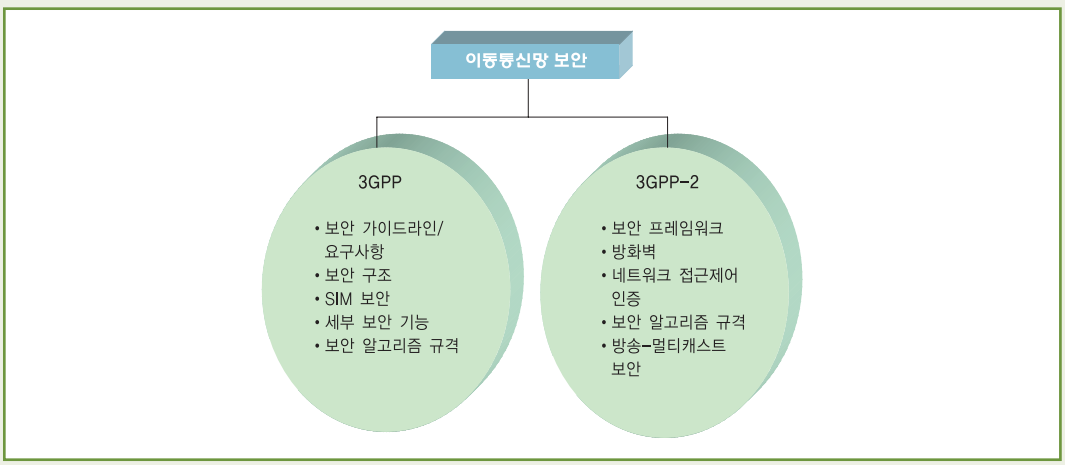
(그림 3) ISO/IEC JTC1 보안 표준화

표준을 개발 완료했다. SC37에서는 바이오메트릭 표준을 개발하고 있으며, 6개의 작업반에서 용어 정의, 기술 인터페이스, 데이터 교환 형태, 바이오메트릭 기능 구조 및 프로파일, 시험 및 보고, 그리고 사회학적 측면에 대한 표준을 각각 개발하고 있다. 특히, 작업반 3에서는 다양한 생체 모달의 표준 데이터 포맷에 관한 표준을 제정하고 있다.

ISO/IEC JTC1 정보보호 표준 대응은 기술표준원 국내 연구반에 의해 대응되고 있다. 국내에서 개발된 대표적인 표준은 ISO/IEC 18033-3(SEED)과 ISO/IEC 24709-1(바이오 분야)을 들 수 있다. 그리고 국내 바이오 인식 산업체에서 제안한 '정맥인식 데이터 포맷' 표준이 ISO/IEC JTC1 SC37에서 개발 중에 있다. 또한, 전자여권 글로벌 표준화는 SC17, SC27, SC37이 협력하여 개발하고 있다.

라. 3GPP/3GPP-2 보안 표준화

제3세대 이동통신망을 위한 정보보호 표준화는 주로 3GPP와 3GPP2 등의 사실표준화 단체에 의하여 수행되고 있다[8,9]. 3GPP는 유럽 주도의 DS(Direct Sequence) 방식의 비동기식 제3세대 이동통신망을 표준화하는 표준화 단체이고, 3GPP-2는 미국주도의 동기식 제3세대 이동통신망을 표준화하는 단체이다.



(그림 4) 제3세대 이동통신 보안 표준

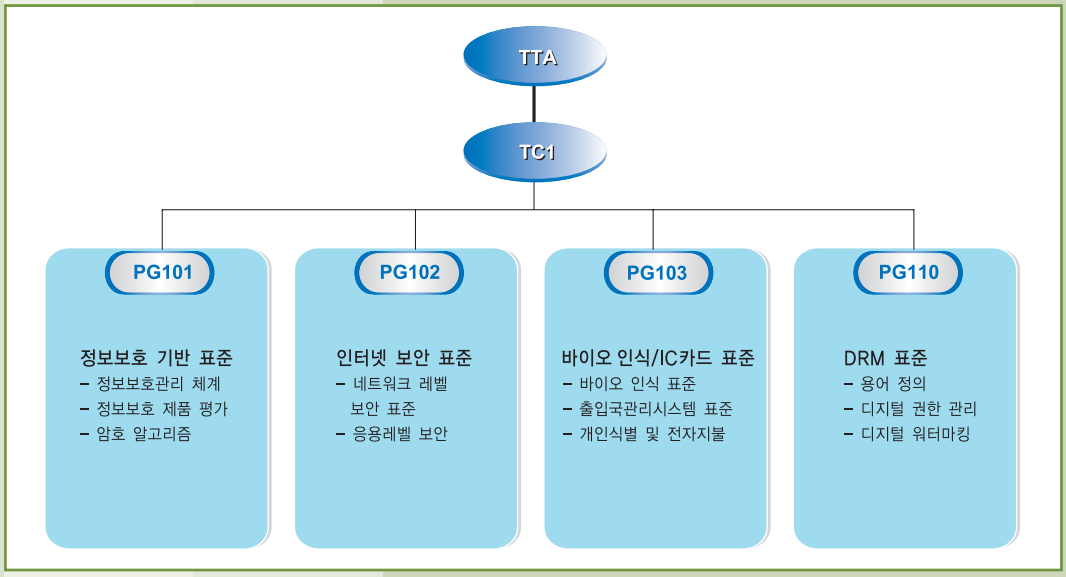
3GPP 표준화 단체에서 수행되고 있는 표준화 내용은 보안 가이드라인 및 요구사항, 보안 구조, 보안 알고리즘, SIM(Subscriber Interface Module) 보안, 액세스 보안 및 응용 보안 분야로 구분되어 표준화가 추진되었다. 또한 3GPP2(CDMA2000)에서는 보안 프레임워크, 공통 보안 알고리즘, 방화벽 및 접근제어, 멀티캐스트 보안 표준이 개발되었다. 우리나라의 경우, 주로 표준 수용자 입장을 취하고 있다.

마. 기타 국제 표준화기구

이외에도 다양한 국제 표준화기구에서 정보보호 분야의 표준을 개발하고 있다. 먼저, IEEE에서는 무선근거리 통신망, 무선 휴대인터넷 등을 위한 MAC 계층 보안 표준을 주로 개발한바 있다[12]. 또한 WPAN을 위한 보안 표준도 개발될 예정이다. 또한 유럽 표준화 기구인 ETSI에서도 유럽 표준 보안 알고리즘, 스마트카드, 전자서명, 전자정부 인증, 개인정보 보호, NGN 보안에 대한 표준을 개발하고 있다[14]. 또한 보안 칩에 대한 국제 사실 표준화 기구인 TCG(Trusted Computing Group)에서는 단말에서 인증과 암호 기능을 수행할 수 있는 TPM(Trusted Plaform Module) 보안 칩에 대한 표준화를 추진하고 있다[13]. 그리고 OASIS에서는 ID 관리와 연관되는 SAML/XACML 관련 보안 표준이 개발되고 있고[10,16], Liberty Alliance에서는 ID 관리 관련 표준이 개발되고 있다[11].

2.2 국내 정보보호 표준화 현황

국내 정보보호 표준은 크게 TTA 단체표준과 KS 표준으로 구분되며, TTA 단체표준은 (그림 5)와 같이 공통기반위원회(TC1)의 PG101, PG102, PG103, 그리고 PG110에 의하여 추진되고 있다[3]. PG101은 정보보호 기반 기술을 표준화하고 있으며 암호 알고리즘, 암호키 관리, 공개키 기반구조 등의 기반 기술을 표준화 하고 있으며, PG102는 네트워크 보안, 전자우편과 같은 응용레벨 보안 표준을 개발하고 있고 PG103에서는 바이오 인식 관련 표준과 개인식별 및 전자지불카드 관련 표준을 개발하고 있으며, PG110에서는 디지털권한관리에 대한 표준을 개발하고 있다. 또한 KS 표준은 기술표준원에 의하여 주로 ISO/IEC JTC1 관련 SC에서 산출된 표준안을 KS 표준화로 채택하고 있다[4].



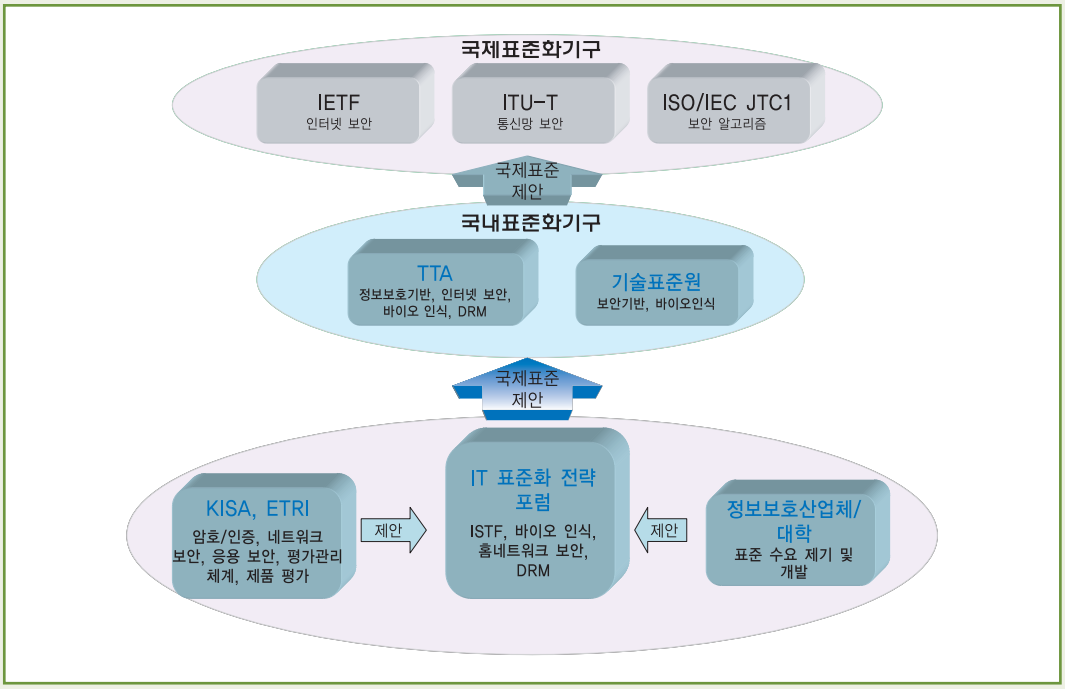
(그림 5) TTA 정보보호 표준화

국내 보안 표준 동향의 경우, 주로 KISA와 ETRI에 의해 표준이 개발되고 있으며, 국내 정보통신 단체표준화 기관인 TTA에서 표준이 제정되고 있다. 현재 추진 중인 대표적인 국내 표준으로는 주민등록 대체수단인 i-PIN(Internet Personal Identification Number) 표준, 홈네트워크 디바이스 인증서 프로파일 표준, 바이오인식 관련 표준이다. 이 i-PIN 표준은 프레임워크, 교환되는 데이터 형식, 그리고 인터넷 사이트 중복성 가입 확인을 위한 메커니즘 표준 등 세가지 표준으로 분류되어 2006년에 표준화가 완료되거나 2007년에 추진될 예정이다. 홈네트워크를 위한 디바이스 인증서 표준으로 이 표준은 현재 ITU-T SG17에서 국내외 표준화가 동시에 추진되고 있는 표준이다. 또한, PG103에서 개발된 '바이오정보 보안대책 가이드라인' 단체표준을 정부 시범사업에 도입하여, 바이오정보의 프라이버시 보호대책으로 활용 중에 있다.

2.3 정보보호 표준화 추진 방향

정보보호 표준화를 위한 추진체계는 (그림 6)과 같다. 국내 표준 개발절차는 ETRI, KISA, 대학, 그리고 정보보호 산업체에서 국내 표준안이 개발되며, 일단 국내 IT 전략 표준 포럼을 통하여 사실표준화를 추진하고 이후, TTA를 통해 정보통신 단체표준으로 개발되어야 한다. 또한, 이후 TTA 주도로 ITU-T와 IETF 국제 표준화를 추진하고, 기술표준원 주도로 ISO/IEC JTC1 국제 표준화를 추진해야 할 것이다. 국내 정보보호 표준화는 두 가지 방법으로 개발되어야 한다. 첫 번째 방법은 국외 표준화 기구에서 개발된 표준을 수용하는 것이고, 국내 정보보호 산업체나 연구소에서 개발된 표준을 새로 개발하는 경우가 될 것이다. 국외 표준의 수용은 국내 정보보호 산업체 파급효과가 크고 국내 정보보호 제품 간에 상호연동을 위해 필요한 표준을 선별하여 추진되어야 하고 동일한 기준으로 국내 표준 개발도 필요하다.

결론적으로, 국내외 정보보호 표준화를 위해 다음과 같은 추진 전략이 고려되어야 한다. 첫째, 국내 산업체에 영향을 주는 표준을 정보보호 산업체가 직접 참여하는 정보보호 관련 포럼을 통해 발굴할 필요가 있다. 국내 정보보호 관련 IT 포럼은 인터넷보안기술포럼(ISTF), 바이오인식포럼, 그리고 PKI 포럼 등이며, 통방융합 정보보호 표준화를 추진하기 위한 IT 표준화 포럼의 신설도 고려할 필요가 있다. 신설될 포럼은 유비쿼터스 사회를 위한 지식정보 유통 보호에 대한 표준을 개발하고 국



(그림 6) 국내외 정보보호 표준화 추진체계

내외 표준의 개발을 목표로 해야 할 것이다. 둘째, 정보통신부가 추진하고 있는 정보보호 분야 신성장동력사업과 국내외 표준화를 연계하여 추진할 필요가 있다. 신성장동력 사업이 국내외 표준화로 연결되어야 할 경우, 그 결과를 반드시 국내외 표준화로 연결할 필요가 있다. 예를 들어, 무선 복합 단말의 암호 인증 관련 기능을 구현하고 있는 무선 TPM 보안 칩 사업의 경우 국외 표준화 단체인 TCG에 국제 표준화를 추진할 필요가 있고, 디지털 포렌직 사업의 경우 컴퓨터 포렌직과 무선단말 포렌직 기술에 대해 국내 표준을 기술개발과 동시에 추진하도록 유도할 예정이다. 그리고 ID 관리 기반 전자ID 지갑 사업의 경우, ITU-T 또는 ISO/IEC JTC1 SC27를 통한 표준화를 유도할 예정이다. 원칙적으로 국내외 표준화가 요구되는 모든 정보보호 분야 신성장동력 사업은 국내외 표준화를 기술개발 과정 또는 사후에 반드시 추진하여 지적재산권을 확보케 할 예정이다. 셋째, 정보보호 분야 표준화는 산·학·연 협력을 통해 개발될 필요가 있다. 원칙적으로 정보보호 표준은 산업체의 요구와 수요제기에 의해 추진될 필요가 있으나, 우리나라 정보보호 산업체의 소규모/영세성을 고려하면 단기적으로 산업체의 주도적 활동을 기대하기 어렵다. 따라서 대학 교수나 국책연구소 연구원의 표준 개발 참여를 위한 인력 양성과 지원 활용이 적극 필요하다. 이를 유도하는 방안으로, 국내외 표준화 추진물이 대학 평가와 대학 교수 업적평가에 연결될 수 있도록 제도개선이 필요하다. 또한 이를 통해 정보보호 분야 표준 전문가의 양성이 필요하다. 넷째, 국내에서 개발된 표준의 글로벌 표준화는 표준의 성격에 따라 적절한 국제 표준화 기구를 통해 표준이 추진되어야 한다. 표준의 응용 분야에 따라서 홈네트워크, RFID, 모바일 망 등의 통신망 보안은 ITU-T, 보안 알고리즘 및 평가는 ISO/IEC JTC1, 그리고 인터넷 보안은 IETF에서 각각 추진되어야 할 것이다.

III. 결언

본 고에서는 국내외 정보보호 표준화 현황을 살펴보고, 이를 근거로 국내외 표준화 추진방향을 제시하였다. 정보보호 표준화는 정보보호 제품간의 상호연동성을 보장하고, 정보보호 시장을 확대할 수 있으며, 정보보호 산업을 발전시킬 수 있는 기반으로 활용될 수 있다. 또한, 정보보호 연구개발과 표준화를 별도로 추진할 것이 아니라, IPR 확보가 가능한 정보보호 분야 표준화 추진 전략이 필요하다. 이렇게 함으로써, 정보보호 분야 표준화에 있어서, 국제 경쟁력을 강화할 수 있을 것이다.

참고 문헌

[1] 염흥열, 정보보호 일반 표준화 로드맵, 2006. TTA

[2] 진병문, 국내외 네트워크 보안 표준화 현황, 제4회 인터넷 서비스 및 네트워크 보안기술 컨퍼런스, 2006. 5

[3] TTA, http://www.tta.or.kr

[4] ATS, http://www.ats.go.kr/

5] IETF, http://www.ietf.org/

[6] ITU, http://www.itu.int/home/index.html

[7] ISO/IEC JTC1, http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/customview.html? func=ll&objId=327993

[8] 3GPP, http://www.3gpp.org/

[9] 3GPP-2, http://www.3gpp2.org/

[10] OASIS, http://www.oasis-open.org/home/index.php

[11] Liberty Alliance, http://www.projectliberty.org/

[12] IEEE 802, http://www.ieee802.org/

[13] TCG,https://www.trustedcomputinggroup.org/home

[14] ETSI, http://www.etsi.org/

[15] 염흥열, NGN 보안을 위한 표준화 동향, TTA IT Standard Weekly, 2006. 5.

[16] 염흥열, ID 관리를 위한 ITU-T 보안 표준(SAML, XACML) 동향, TTA IT Standard Weekly, 2006. 7.

TTA