

[정보보호] ITU-T SG17 금융보안 표준화 동향

최근 스마트폰의 열풍은 다양한 사회적 문화적 파급효과를 가지고 있지만, 기술적 발전의 파급효과를 고려해 보았을 때 중요한 점은 이동 인터넷을 사용자가 체감하고 있다는 것이며, 관련한 다양한 사업자들은 이에 유용한 서비스를 개발하여 새로운 시장을 형성해가고 있다는 점이다. 특히, 기존 통신망 중심의 채널 제공 서비스 모델이 응용서비스를 중심으로 하는 모델로 진화하고 있다는 점이 새로운 국면으로 부각되고 있다. 여기서 전자금융서비스는 통신망이 제공하는 다양한 서비스들 중 일반 사용자에게 매우 친숙한 서비스의 하나로 손꼽힐 수 있을 것이다.

지금으로부터 20여 년 전으로 거슬러 올라가 1980년 중·후반을 떠올리면 당시는 개별 기업별로 전산시스템을 구비하여 클라이언트 서버 모델의 기업 전산 인프라를 구축하는 시기였을 것이다. 마찬가지로 금융기관들도 은행간 지급결제 처리를 위하여 은행공동망 구축을 하던 시기에 해당한다. 이 시기에 금융보안의 주요 목적은 은행간 결제대금의 안전한 결제를 위해 요구되는 전달되는 메시지의 보호와 통신망 보안을 위한 요구사항이 주를 이루었었다. 이 시기에 사용자들은 직접 은행에 방문하여 돈을 입금하고 이체하였기 때문에 ATM기기 등 사용자를 직접 대면하는 장치 이외에 사용자 채널에서의 정보보호요구사항은 존재하지 않았다.

앞서 살펴보았던 시기로부터 20여 년이 흐른 지금 이 시대에 금융고객들은 직접 은행을 방문하기보다는 PC를 사용하거나, 전화를 사용하거나, 혹은 스마트폰 단말에서 다양한 전자금융서비스를 사용하고 있다. 이는 통신망 기술의 발전 및 확산으로부터 인터넷이 보편화 되면서 나타나는 자연스러운 현상이었고, 인터넷이 보편화 되면서 ISO, ITU-T의 국제 표준기구들에서도 정보보호에 관한 표준 개발을 상호 협력적으로 활발하게 진행해오고 있었다.

금융보안 관련 표준화 기구 동향

국제표준기구로서 ISO의 경우 2010년 기준으로 볼 때 금융표준은 산하 기술위원회인 TC68이 주도하고 있으며, 61개국이 참여하고 있는 상황이다. TC68은 금융서비스 부문 국제표준화를 담당하는 기술위원회로 23개 P-member(한국 포함)와 38개 O-member로 구성되고 4개의 SC와 1개의 WG가 활동하고 있으며, 사무국 기능은 미국 국가표준기구(ANSI)가 담당하고 있다.

금융분야에 관련된 주요 표준은 메시지 전송 표준, 생체인식, 암호 알고리즘, PIN관리 등이며, TC68 산하의 분과위원회인 SC2(지급결제보안), SC4(증권), SC7(코어뱅킹) 등에서 담당하고 있다. 특히, 금융보안 분야를 담당하고 있는 SC2에서는 8개 WG이 운영되면서 관련 표준을 제정했었다.

- WG4: 은행업무 정보보호가이드라인(Information Security Guideline for Banking)
- WG6: IT보안 유지활동 프레임워크(Framework Study into IT Security Maintenance Activity)
- WG8: 공개키 기반구조 관리(Public Key Infrastructure Management)
- WG10: 생체인식 보안 및 관리(Biometric Security and Management)

- WG11: 금융 응용프로그램에 사용되는 암호알고리즘(Encryption Algorithms used in Banking Applications)
- WG12: 금융거래 전자문서의 안전한 서명을 위한 요건(Requirements for Secure Signing Mechanisms for Financial Institutions)
- WG13: 소매금융에서의 정보보호(Security in Retail Banking)
- WG14: 암호메시지 형식(Cryptographic Syntax)

2011년 8월 22일부터 9월 2일까지 개최된 ITU-T SG17(정보보호) 표준화 회의에 금융보안연구원에서는 ‘인터넷뱅킹 서비스를 위한 이상금융거래 탐지 시스템’이라는 주제로 신규표준아이템을 제안하였다. 최종 회의 결과는 제안 신규 표준이 다루는 범위와 제목 변경을 통하여 제안 내용을 추진하고, 대신에 ISO TC 68 SC2로 해당 신규 표준 아이템의 개발에 대하여 협력 요청을 하는 연락문서(Liasion Statement)를 통하여 해당 그룹으로부터 의견을 듣는 것으로 결론에 도달했다. 또한, 2013년부터 시작되는 차기 연구회기의 구조조정과 관련해서 SG17 WP(working party)2에서는 한국 주도로 소셜 네트워크 보안, 클라우드 보안 등과 함께 모바일 금융 시스템 보안을 포함할 것을 제안하였다(TD 2172). 이번 회기 동안 SG17에서는 3개 WP를 운영하여 왔었으며, WP 차원에서 차기 연구회기 동안 신규 ICT 서비스 분야에서의 연구 주제 확대의 필요성을 제안한 것이다.

- WP 1: 네트워크 정보 보안(Network and Information Security)
- WP 2: 응용 보안(Application Security)
- WP 3: 신원 관리 및 언어(Identity Management and Language)

결언

모바일 인터넷이 보편화된 시점에서 기존 은행간 뿐만 아니라 개인과 은행, 개인과 개인간의 인터넷 기반 다양한 금융 서비스가 출현하고 있다. 이러한 시점에서 ITU-T에서의 통신망 기반의 정보보호 표준 추진 경험과 ISO TC68에서의 금융 분야의 전문화된 표준 영역이 조화를 이루어 스마트 모바일 환경에서 금융보안을 위한 표준 기술이 개발되어야 할 시점으로 보인다.

임형진 (금융보안연구원 u-금융연구팀 책임연구원, hjlim@fsa.or.kr)