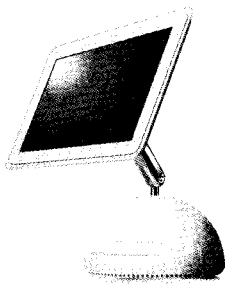
ITU-T SG17 라포처 회의 및 IPTV-GSI 보안 분야 회의



염흥열 | ITU-T SG17 부의장, 순천향대 정보보호학과 교수

1. 머리말

글로벌 정보보호 표준을 주도하고 있는 ITU-T 연구반(Study Group) 17의 연구과제 4, 6, 7 인터림 라포처 회의가 IPTV-GSI 보안 회의와 연계되어 스위스 제네바에서 2009년 6월 23일부터 일주일간 열렸다. 연구과제 4는 사이버보안, 연구과제 6은 유비쿼터스보안, 연구과제 7은 응용보안에 대한 국제 표준화를 추진하고 있다. 이번 연구과제 6, 7 조인트 라포처 회의에서는 IPTV 보안과 OTP(일회용 패스워드) 관련 권고안의 범위와 내용에 대한 심도있는 토론이 주로 한국과 일본 보안 전문가에 의해 이루어졌고, 연구과제 4 라포처 회의에서는 미국의 '글로벌 사이버보안 정보교환 프레임워크'에 대한 새 표준화 아이템 제안과 한국의 '사이버 공격자 역추적을 위한 프레임워크와 메커니즘'에 대한 새로운 표준화 아이템의 제안이 이루어졌다. 본 고에서는 이와 연관된 회의 중 여러 이슈를 살펴보고, 합의도출 과정과 각 이슈별 결론을 제시한다.

2. 주요 이슈 및 합의 결과

2.1 연구과제 6(유비쿼터스보안)의 IPTV 보안 표준화 추진현황

현재 연구과제 6에서 개발 중인 IPTV 보안 관련 권고안은 안전한 트랜스코더블 기법(X.iptvsec-2), IPTV 서비스를 위한 키관리 기법(X.iptvsec-3), 디스클램블링 알고리즘 선택(X.iptvsec-4), 상호연동 가능한 SCP(Service and Content Protection)(X.iptvsec-5) 등이다. 지난 2월 연구반 17 회의에서는 IPTV 보안 요구사항과 기능(X.iptvsec-1)에 대한 권고안이 국제표준(X.1191)으로 채택된 바 있다. 현재 개발되고 있는 권고안은 X.1191에 기술된 세부 보안기술에 대한 세부 표준이 개발되고 있으며, 4개의 권고안이 모두 한국 주도로 개발되고 있다. 이러한 배경으로 인해 이번 회의에서 일본과 중국 보안 전문가들이 이 권고안들에 대해 민감한 의견을 제시했다. 이번 회의에서는 주로 안전한 트랜스코더블 기법, 키관리 기법, 상호연동 가능한 기술 등에 대한 권고안이 토론되었다.

첫번째 제기된 문제는 키관리 기법 권고안에 대한 것이다. 이번 회의 전까지는 IPTV 키관리 기법의 권고안은 유니캐스트 서비스, 멀티캐스트 서비스, 그리고 개인방송 서비스를 위한 키관리 기법을 개발하는 것으

로 합의된 바 있다. 한국(필자)은 기존의 범위에 더하여 다운로더블 SCP를 위한 키관리를 더 부가하자고 제안했다. 다운로더블 SCP를 위한 키관리는 비교적 논쟁 없이 합의되었다.

그런데, 일본 측에서는 IPTV 서비스를 위한 키관리 기법 권고안의 범위에 대한 수정안을 제안했다. 구체적으로, 일본 측은 일반 IPTV 서비스인 유니캐스트와 멀티캐스트 서비스를 위한 키관리 기법을 포함하지 말고, 오직 개인방송 서비스를 위한 키관리 기법만으로만 한정하자는 수정안을 제기했다. 이의 논거는 기존의 많은 한정수신 시스템이 IPTV 서비스를 위해 적용되고 있고, 기존의 전용프로토콜 기반 키관리 기법에 바탕을 둔 IPTV 서비스가 많이 진적을 이룬 상태에서 국제 표준화를 추진하기가 어려울 수 있다는 것이었다. 그러나, 이는 국내 상황하고는 사뭇 달라 수용하기가 어려운 부분이다. 국내에서는 개방형 IPTV2.0 서비스 개발을 시작하였고, 이는 기본적으로 여러 다양한 IPTV 서비스에 대한 키관리를 요구하고 있기 때문이다. 또한 이 권고안의 범위는 이미 지난 여러 번의 회의를 통해 합의된 결과이므로 존중되어야 한다는 것이다. 이 문제는 근본적으로 공개적인 IPTV 보안 시스템 기반 키관리 기법을 개발할 것인지, 아니면 전용의 IPTV 보안 시스템만을 고려해 키관리 기법에 대한 국제 표준화를 포기할 것인지에 대한 문제다. 한국 측은 공개적인 보안 시스템을 위한 키관리 기법의 필요성과 기존 범위 합의에 대한 존중의 필요성을 주장했고, 현재 개인방송 서비스의 유스케이스 등이 아직 불분명한 측면이 있어서 개인방송 서비스에 대한 키관리 기법을 표준화는 단기적으로 어려울 수 있음을 고려해 이를 위한 키관리 시스템은 배제 가능하고, 개방적인 IPTV 보안 시스템의 키관리 기법이 표준화되어야 하며, 다운로더블 SCP를 위한 표준화도 추진되어야 한다고 주장했다. 만약 일본 측의 국내 사정으로 이를 수용하기 어렵다면, 유니캐스트나 멀티캐스트 키관리 기능은 선택 또는 권고 요구사항으로 해도 됨을 강조하였다. 많은 토론 끝에 다운로더블 SCP에 대한 표준화에 대한 추진 필요성은 많은 참여국이 동의했고, 기존의 유니캐스트나 멀티캐스트 키관리에 대한 표준화도 추진하고 다운로더블 SCP를 위한 키관리 기법도 개발하기로 합의하였다.

따라서, 이번 회의를 통해 IPTV 서비스를 위한 키관리 기법에 대한 표준안의 범위가 다시금 확정되었고, 또한 방송통신위원회가 적극적으로 추진하고 있는 다운로더블 SCP(Service and Content Protection) 를 위한 국제 표준의 근거를 마련할 수 있었다고 생각된다.

일본 측은 향후 IPTV 보안에 대한 많은 관심을 보일 것으로 판단되며, 또한 한국 측에 의해 주도되고 있는 IPTV 보안 표준안에 대해 민감하게 반응할 수 있다고 여겨진다. 그러므로 향후 IPTV 보안 분야의 국제 표준화 추진 시 일본과의 조율과 협력이 필요하다고 생각된다. 이번 회의를 통해 얻은 결과는 특정 업체의 전용 IPTV 보안기술에 의존하지 않은 IPTV 서비스를 위한 개방형 SCP 기술의 적용 및 배치가 가능한 키관리 체계의 개발을 통해 국내 산업체의 경쟁력과 다양한 네트워크 및 서비스 제공자의 선택권을 보장한 것이라고 개인적으로 판단한다.

2.2 연구과제 4(사이버보안)의 글로벌 사이버보안 정보교환 프레임워크 신규 연구 아이템 선정

이번 사이버보안 연구과제(연구과제 4) 인터림 회의의 주요 의제는 무엇보다도 미국 대표에 의해 제안된 글로벌 사이버보안 정보교환 프레임워크라는 신규 표준화 아이템의 제안이라고 볼 수 있다. 이 표준화 아이템은 일본, 미국, 한국 등의 보안 전문가가 참여해 좀

더 구체화되었다.

사이버보안 정보의 정의, 기존 표준과 신규 표준과의 관계, 권고안의 범위와 목적 등에 초점이 맞춰서 중점적인 토론이 이루어졌다. 또한 권고안의 약어에 대한 합의도 하나의 중요한 진전이었다. 토론은 큰 반대 의견 없이 여러 의견을 수렴하고 합의하는 식으로 이루어졌다.

먼저, 이 권고안의 약어는 X.cybief(Global Cybersecurity Information Exchange Framework)로 합의되었다. 이 권고안은 한마디로 글로벌 사이버보안 정보교환을 위한 커다란 틀과 비전을 제공함을 기본 목적으로 하고 있다. 현재 사이버보안을 효율적으로 막기 위한 표준화 관련 문제점은 크게 두 가지 정도로 요약될 수 있다. 첫째, 현재 사이버보안과 관련되는 많은 표준화 활동이 이루어지고 있고, 그 결과로 많은 표준이 개발되었으나 전체적인 차원에서 사이버정보 교환을 하기 위한 글로벌 프레임워크가 없다는 것이다. 둘째, 여러 표준화 기구에서 개발되고 있는 표준들이 특정 분야만 담당하고 있어서, 서로 어떻게 연결되어야 하고, 어떤 경우에 연결되어야 하며, 어떻게 효율적으로 연계될 수 있는 지에 대한 큰 그림이 없다는 것이다. 이번 권고안 제안은 이러한 문제점을 해결하고자 하는 하나의 중요한 진전이라고 볼 수 있다.

현재까지 논의되고 있는 사이버보안 정보의 정의는 사이버보안과 관련되는 장비, 소프트웨어 등의 상태(취약성), 침해사고와 관련되는 포렌식 정보, 침해사고 경험으로부터 얻은 서명 및 학습 데이터, 정보교환 주체, 정보교환 규격, 관련 주체 및 정보 아이덴티티, 그리고 구현 요구사항 등에 대한 구조화된 정보로 합의되었다.

현재 이 표준안은 사이버보안 정보교환을 위한 모든 표준화기구와 관련 조직에 의해 만들어진 기존 표준들을 조사하고 일부 필요하다고 판단되면 이들중 일부를 국제전기통신연합(ITU) 표준으로 채택하며, 필요한 경우 기존 표준을 개선하고 새로운 표준을 개발하여 사이버보안 정보교환을 위한 글로벌 표준으로 만드는 것에 목적이 있다. 이 표준안의 범위는 교환이 가능한 사이버보안 정보의 구조, 사이버보안 정보의 확인 및 발견, 네트워크를 통해 신뢰된 사이버보안 정보의 획득 및 교환 등이다.

최종 신규 권고안 채택 여부는 2009년 9월 ITU-T SG 17 회의에서 결정될 것으로 보이나 이러한 시도와 노력은 충분히 의미있는 활동으로 생각된다. 이 표준이 개발되고 나면, 사이버보안 관련 조직, 정보, 그리고 대응 방안 등에 대한 커다란 비전이 제시될 것으로 판단된다.

2.3 연구과제 4의 사이버 공격자 역추적 프레임워크 신설 연구 아이템 제안

연구과제 4(사이버보안) 인터림 회의에서는 한국(필자)이 '사이버 공격자에 대한 역추적을 위한 프레임워크와 메커니즘'에 대한 신규 표준화 아이템 제안, 즉 현재 연구과제 4에서 수행되고 있는 기존 표준화 아이템(유스케이스 및 요구사항, 정보교환 포맷) 외에 역추적 프레임워크와 메커니즘에 대한 신규 표준화 아이템을 제안했다.

이 제안에 대해 미국, 일본, 한국, 프랑스 보안 전문가들 간에 심도깊은 논의가 이루어졌다. 주로 토의는 글로벌 사이버정보교환 프레임워크와 이 표준과의 관계와 범위 및 목적에 집중되었다. 토론 끝에 이 표준이 글로벌 사이버교환 프레임워크와 중복되지 않으며, 신규 표준화 아이템이 기존 개발 중인 권고안들을 보완할 수 있다는 데 합의했다. 또한, 일본 측은 이 권고안이 기존의 역추적 메커니즘과 X.tb-ucc에서 정의되고

있는 요구사항의 집합과의 관계를 포함해야 한다고 강조했고, 미국 측은 기존의 권고안과 새로운 표준화 아이템과의 관계에 대한 질의를 하였으며, 토의를 통해 상호 보완적 관계를 확인했다. 전반적으로 이번 회의를 통해 역추적 기술에 대한 신규 표준화 아이템의 신설에 대한 포괄적인 지지를 얻었다고 볼 수 있다. 따라서 2009년 9월 ITU-T SG 17 회의를 통해 최종적으로 새로운 연구 아이템을 확정하고, 이를 위한 표준개발을 한국 주도로 수행할 필요가 있다. 비록 이번 인터림 회의에서는 드래프트 권고안 신설 합의까지는 이루지 못했으나, 권고안 개발 필요성에 대한 일반적인 공감대를 형성하는 계기를 마련했다고 할 수 있다.

3. 맺음말

이번 회의를 통해 다시 한번 인터림 회의는 공식적인 회의보다 토론 시간이 충분하여 폭넓은 의견과 질문을 수렴할 수 있어서 신규 권고안 제안에 대한 각 참여자의 의견 수렴과 의견 파악을 위한 회의로 활용될 수 있다는 것을 확인할 수 있었다. 특히, 미국의 글로벌 사이버보안 정보교환 프레임워크와 한국의 사이버 공격자 역추적 표준화 아이템 신설 경우처럼, 인터림 회의를 통해 일단 참여자의 의견을 수렴하고, 공식회의를 통해 확정하는 것도 좋은 국제 표준화 추진전략이라고 생각된다.

또한, 국제 표준화를 추진 시에 각 국가 간의 상충을 어떻게 해결하느냐가 중요하다. 왜냐하면, 한 국가에서는 특정 기술에 대한 국제 표준화 추진이 필요하나, 다른 국가에서는 그 특정기술만을 지원할 수 없는 제도적 상황을 고려할 필요가 있다. 이 경우 ITU-T 는 대부분의 권고안 채택과정이 만장일치에 기반을 두고 있으므로, 상대방에 대한 적절한 배려가 필요하다. 따라서, 문제가 되는 기능과 요구사항을 권고 또는 선택으로 추진하는 것도 합의를 유도하기 위한 좋은 추진 전략 중 하나라고 생각된다.

또한, 국제표준화는 최선의 결과를 추구하는 게 아니라 합의 가능한 차선의 결과를 추구해야 한다는 것을 다시 한번 느꼈다. 아무리 훌륭한 기술이라도 참여자의 합의가 없으면 절대로 국제 표준화를 완성할 수 없기 때문이다. 또한 표준화 추진과정에서 평상시의 표준화 추진을 위한 인적 네트워크 구축과 지역별 국가 간 협력 체계 마련이 매우 중요함을 다시 한번 확인하는 회의였다. TTA