

ITU-T SG17(정보보호) 국제회의



염홍열 ITU-T SG17 부의장/WP3 의장
순천향대학교 교수, 정보보호포럼 의장
오흥룡 TTA 정보기술부 선임연구원

1. 머리말

국제전기통신연합 - 정보통신표준화부문 연구반 17(ITU-T SG17) 회의가 2014년 1월 15일부터 24일까지 스위스 제네바에서 열렸다. 이번 회의에는 26개 회원국 및 국제기구에서 약 145명이 참석했고, 한국에서는 염홍열 교수(수석대표, 순천향대), 나재훈 책임(교체수석, ETRI)을 포함해 총 18명(국가대표 16명, ETRI 2명)이 참가했다. 한국은 국가 기고서 14건과 섹터 회원(ETRI) 기고서 6건 등 20건의 기고서를 제출해 19건의 기고를 반영한 바 있다.

한국은 <표 1>과 같이 2건의 권고 채택(approval), 3건의 부속서 채택(agreement), 그리고 1건의 권고 채택 준비과정(determination) 등의 성과를 거뒀다.

2. 주요 회의 내용

2.1 사이버 보안 지수 권고(X.1208)의 조건부 채택

사이버보안 지표(cybersecurity indicator) 권고는 한국 제안으로 2009년 11월 Q.4/17(사이버보안) 인터럽 회의부터 개발되어 왔다. 이 표준은 조직의 사이버보안 수준을 측정하기 위한 지표를 제시하고 있다.

<표 1> 채택된 주요 표준 및 부속서

표준 번호	표준 제목	에디터(한국)
X.1208	ICT 활용에 있어서 사이버보안 리스크 지표	염홍열(순천향대)
X.1210	IP 기반 네트워크에서 보안 문제 해결 메커니즘	
부속서 10(X.1205)	인터넷상에서 공격자의 IP 주소를 식별하기 위한 역추적 메커니즘	
부속서 21(X.1143)	웹 매쉬업 서비스를 위한 보안 프레임워크	나재훈(ETRI)
부속서 22(X.1144)	XACML 3.0 권고(X.1144) 개선과 특징	

국내 국가정보보호 지수 내의 사이버보안 지표를 조직의 사이버보안 지수 지표로 변경해 반영되었다. 이 표준의 주요 내용은 조직이 이 권고에서 제시된 사이버보안 지표를 활용할 것 등과 같은 일반 원칙, 사이버보안 지표 선택 가이드라인, 그리고 사이버 보안 리스크 지표 개발 방법론을 제시하였고, 30개의 사이버보안 지표를 규정하고 있다.

이 권고에서 제시된 30개의 지표는 취약성 관리, 감사 로그 관리, 패치를 위한 소요 평균 시간, 시스템 구성변경을 위한 소요 평균 시간, 리스크 평가 커버리지 비율, 말웨어 검출 및 치료 커버리지 비율, 비상 계획하의 중단 디바이스 비율, 인증받은 중단 디바이스 비율, 보안 서약서 비율, 보안 게이트웨이로 통제되는 원격 접근 비율, 보안 교육 훈련을 받은 종업원 비율, 사이버 보안 인원 비율, 악성코드 감염 중단 디바이스 비율, 유출된 개인정보 비율, 보안 예산 비율, 인가된 디바이스 비율, 인가된 소프트웨어 비율, 보호되는 응용 프로그램 비율 등을 포함하고 있다.

이 권고는 2013년 9월 SG17 회의에서 조건부 채택되었으나, 미국 등의 추가 의견 제시로 채택이 이번 1월 SG17 회의로 연기된 바 있었다.

2.2 보안문제해결(trouble shooting) 메커니즘 권고 (X.1210) 채택(determination)

이 권고는 역추적 메커니즘의 권고(X.trm) 개발의 부산물로 나온 권고다. 당초 2009년 9월 SG17 회의부터 한국 주도로 역추적 메커니즘이 개발되어 왔으나, 지난 2013년 9월 회의에서 이 문서를 보안 문제 해결 메커니즘과 역추적 메커니즘으로 나누어 개발하기로 합의했다. 따라서 보안 문제 해결 메커니즘과 역추적 메커니즘을 권고로 개발하기로 지난 9월 회의에서 합의된 바 있다. 이 표준은 다양한 트러블 슈팅 메커니즘과 선택 기준을 제시하고 있다.

2.3 역추적 메커니즘 부속서(Revised Supplement 10) 채택(agreement)

한국은 2009년 9월 Q.4/17(사이버보안) 회의에서 표준화 작업을 착수했으며, 당초 권고로 개발키로 했으나, 이번 회의에서 부속서로 합의되었다. 이 부속서는 디도스 공격 등 위조 IP 주소를 사용하는 공격 근원지를 추적하는 역추적 기술의 개요와 더불어, 다양한 역추적 메커니즘과 주요 역추적 메커니즘의 특성 비교 분석 결과를 제시하고 있다.

2.4 매시업 보안(Supplement 21) 부속서 채택 (agreement)

이 부속서는 단일 도메인으로 제한하는 접근제어 방식이 다중 도메인을 기반으로 하는 웹 매시업 서비스에 대한 확장된 권한 제어가 가능하도록 웹 서비스 구조와 안전한 매시업을 위한 절차를 규정하고 있다. 웹 매시업 서비스 제공을 위하여 단일 도메인 환경을 기반으로 제시되는 기술들의 위협요인을 분석하고, 안전한 웹 서비스를 위한 구조적 및 기술적 대응 원칙을 분류, 프로토콜 구조상의 각 계층에서의 대응 방안들에 대한 지침을 제시하고 있다.

2.5 XACML 3.0 개선사항(Supplement 22) 동의 (agreement)

이 부속서는 XACML 3.0 표준의 개선과 특징 웹 서비스 환경에서 리소스 사용에 대한 인증 및 인가에 대한 개정서인 XACML 3.0의 개선사항과 신규 기능에 대한 요약서로서 OASIS 포럼에서 개발 진행 중인 기능들도 포함되어 있어서 동종 업계의 기술 및 표준 개발에 활용이 기대된다. 이 부속서는 웹의 리소스 접근제어에 널리 활용되고 있는 XACML 2.0과 비교하여 XACML 3.0에 표준 제정된 개선점과 신규 기능들에 대한 요약서이다.

2.6 웹 기반 공격 대응 권고(X.1211) 사전채택 (determination)


2009년 9월, 한국의 제안으로 Q.4/17(사이버보안) 그룹에서 웹기반 사이버보안 기술 표준화 작업(X.eipwa)을 착수하였으며, 한국 에디터(순천향대 염홍열) 주도로 웹 기반 공격에 대한 기능 요구사항, 기능을 제시하고 있다. 이 권고는 국내 웹 공격 대응 기술과 제도가 고려되어 개발되고 있다. 이번 SG17 회의에서 문서의 완성도를 고려해 권고 사전채택(determination)으로 합의했으며, 8월까지 국가별 의견 수렴을 거쳐 9월 회의에 최종 채택을 준비하고 있다.

2.7 개발 중인 권고 반영과 신규 워크아이템

한국은 개발 중인 권고인 ‘통신조직을 위한 개인 정보보호관리를 위한 가이드라인(X.gpim)’, ‘바이오 하드웨어 모듈을 이용한 인증 프레임워크(X.bhsm)’, ‘스마트 그리드 보안 프레임워크(X.sgsec-1)’, ‘스마트폰 앱 배포 보안(X.msec-8)’, ‘모바일 디바이스를 이용한 다중 인증 메커니즘(X.sap-8)’, ‘부인방지 방식(X.sap-9)’, ‘통신조직 정보보호관리체계 수정안(Revised X.1051)’ 등에 대한 기고를 제안해 모두 반영했다.

한국은 SDN(software-defined network) 보안, 지능형 자동차 보안, 속성 기반 인증 방식에 대한 신규 워크아이템을 제안했으며, 다음 SG17 회의에서 채택을 준비하고 있다. 특히, 속성 정보를 기반 인증 메커니즘의 경우 중복성이 우려되던 기존 개발되고 있는 권고가 취소되어 다음 회의에서 채택될 가능성을 높였다.

3. 맺음말

한국은 이번 SG17 회의에서 국내 사이버보안 기술과 제도를 반영한 2건의 권고와 3건의 부속서를 국제 표준으로 채택하는 성과를 거뒀다. 정보보호 국제 표준화가 각 나라의 규제와 국가 주권, 그리고 콘텐츠 모니터링 등과 연관되어 국제표준으로 완성하기에 어려운 측면이 크다. 그러나 앞으로도 정보보호 서비스와 제품의 상호 연동을 위해 국제 표준화를 지속적으로 추진할 필요가 있다. 차기 SG17 회의는 스위스 제네바에서 2014년 9월 15일에서 24일까지 열릴 예정이다. 

[참고문헌]

- [1] ITU-T SG17 Homepage. (<http://www.itu.int>)
- [2] ITU-T SG17 TD 0721, Koji Nakao, Report of Working Party 1/17, Fundamental security, Geneva, 15-24 January 2014.
- [3] ITU-T SG17 TD 0722, Sacid Sarikaya, Report of Working Party 2/17, Network and information security, Geneva, 15-24 January 2014.
- [4] ITU-T SG17 TD 0723, Heung Youl Youm, Report of Working Party 3/17, Identity management and cloud computing security, Geneva, 15-24 January 2014.
- [5] ITU-T SG17 TD 0724, Antonio Guimaraes, Report of Working Party 4/17, Application security, Geneva, 15-24 January 2014.
- [6] ITU-T SG17 TD 0725, Zhaoji(George) Lin, Report for WP 5/17 plenary, Geneva, 15-24 January 2014.