[정보보호] 사이버보안 정보공유 기술 표준화 전망

2009년 ITU-T SG17(Study Group 17) 국제 표준화 회의가 지난 2월 11일부터 20일까지 스위스 제네바에서 개최되었다. SG17은 정보보호 분야의 국제 표준화를 담당하고 있는 ITU-T 산하의 연구 그룹(Study Group)이다.

본 고는 이번 회의에서 논의된 회의 결과를 바탕으로 ITU-T SG17에서의 사이버보안 기술 국제 표준화 동향을 살펴본다. 특히, 이번에 본인이 제안하여 채택된 사이버공격 추적이벤트 교환 포맷을 바탕으로 향후 ITU-T SG17에서의 사이버보안 정보공유 기술 표준화 전망에 대한 의견을 제시한다.

ITU-T SG17에서의 사이버보안 기술 표준화 동향

이번 새로운 회기(2009 ~ 2012)에는 ITU-T SG17의 Working Part 1에 소속된 Question 4에서 사이버보안 기술에 대한 표준화 작업을 담당한다. 지난 회기까지 총 3건의 국제표준(X.1205, X.1206, X.1207)들이 제정 완료되었으며, 현재까지 총 7건의 사이버보안 관련 권고안이 개발되고 있으며, 이번 회의에서 2건의 새로운 과제가 채택되었다. 진행중인 권고안의 내용은 다음과 같다.

<표 1> Q.4/17에서 진행중인 권고안의 내용

권고안	제목	내용
X.sisfreq	보안정보공유 프레임워크에 대한 요구사항	보안 시스템의 취약점, 공격, 악의적인 행위 정보 등에 관한 보안 정보들을 공유하기 위한 프레임워크의 요구사항을 정의함
X.gopw	데이터통신 네트워크에서 웜 전파를 예방하기 위한 가이드라인	악성코드에 대한 분류, 정의, 감염경로 등과 전파를 차단할 수 있는 기술적 가이드라인을 정의함
X.tb-ucc	역추적 유스케이스 및 수준	단일 ISP 및 다중 도메인에서 발생할 수 있는 역추적 시나리오를 포함한 유스케이스와 역추적 기술 등을 정의함
X.bots	봇넷 탐지와 대응을 위한 프레임워크	봇넷의 정의, 구성특성, 행위모델 등과 봇넷으로 인한 다양한 공격 위협을 정의함
X.gpn	네트워크 보안을 위한 일반적인 정책 프로파일	2007년에 제정된 X.1036의 네트워크 보안정책 모델과 프레임워크를 기반으로 보다 자세한 보안정책의 분배 메커니즘과 프로세스를 정의함
X.abnot	통신네트워크에서의 이상 트래픽 탐지 및 제거 가이드라인	통신네트워크 환경에서 이상 트래픽 탐지 메커니즘과 제어 솔루션을 개발하기 위한 요구사항과 전형적인 이상 트래픽 특성들을 정의함
X.sips	SIP(접속 설정 프로토콜) 기반 서비	SIP 기반의 공격에 대한 탐지 및 대응 특성을 분석

	스에서 사이버공격 차단을 위한 프레임워크	하고 서비스 제공자 간의 정보공유를 위한 요구사항을 정의함

언급된 7건의 표준권고안 중에서 X.sisfreq에 대한 국가별 결의(determination)가 올해 9월 ITU-T SG17 제네바 회의에서 시작된다. 그 외 다른 표준권고안에 대한 결의는 차후에 진행될 예정이다.

ITU-T SG17에서의 사이버보안 정보공유 기술 표준화 전망

지난 회기까지 사이버보안 정보공유 기술과 관련하여 국제표준 X.1206 (취약점, 패치 정보 업데이트를 위한 벤더 중립적 프레임워크)이 제정되었으며, 이 국제표준은 자동으로 보안 관련 정보를 알리고 업데이트를 전파하기 위한 벤더 중립적인 프레임워크를 규정하고 있으며, 일단 자산이 등록되면 취약점, 패치 및 업데이트 정보를 사용자에 의해 또는 애플리케이션에 직접 자동적으로 업데이트 한다. 또한, 각 자산, 디바이스 또는 지역 서버가 임의의 또는 모든 서버에 등록되어 있으면 취약점 정보, 업데이트 또는 패치 정보들을 요청하거나 제출할 수 있게 된다.

또한, 2009년 9월 제네바 회의에서 국가별 결의를 받게 되는 X.sisfreq (보안정보공유 프레임워크에 대한 요구사항) 권고안이 해당 작업반에서 진행 중이다. 이 권고안의 내용은 취약점, 공격, 악의적인 행위 정보 등에 관한 보안 정보들을 공유하기 위한 프레임워크의 요구사항을 규정하는 것으로, 보안 정보 공유 기술의 상용화 시 상호호환성을 보장하기 위한 프레임워크를 정의하기 위한 것이다.

추가적으로 사이버보안 정보 공유를 위한 공통된 메시지 전달 포맷에 대한 필요성이 제기되고 있는 시점에, 지난 2월 제네바 회의에서 한국은 신규 표준화 과제(아이템)로 '사이버공격 추적 이벤트 교환 포맷'과 '디지털 증거 교환파일 포맷' 등을 제안하여 채택시켰다.

향후 표준화 진행 방향

최근의 사이버 공격은 시스템 및 네트워크의 취약점 등을 통해 급속하게 전파되는 형태를 보이고 있다. 또한, 이러한 공격들은 상호 결합되어 그 확산 정도나 파괴력은 점점 증가하여 피해 사례와 피해규모도 전세계적으로 커지고 있는 추세이다. 이와 같은 사이버공격에 대응하기 위하여 원활한 국제공조를 지원하기 위한 국가 간에 공통적으로 사용될 수 있는 국제표준이 필요하며 양국 간에 제도적 상이함을 초월한 기술적인 부분에서의 합의가 이루어져야 한다. 또한, 다양한 대응 기술과 함께 사이버 공격에 대한 전 세계적인 정보공유 체계와 이를 위한 국제표준 개발이 필요한 시점이라고 할 수 있다. 이에 따라 지난 2월 회의에서 사이버공격 추적 이벤트 교환 포맷과 디지털 증거 교환파일 포맷에 대한 신규 과제가 제안되어 채택되었으며, 향후 이를 바탕으로 새로운 사이버보안 정보공유 기술 관련 국제 표준화 활동들이 시작될 것으로 예상된다.

김종현 (한국전자통신연구원 지식정보보안연구부, jhk@etri.re.kr)