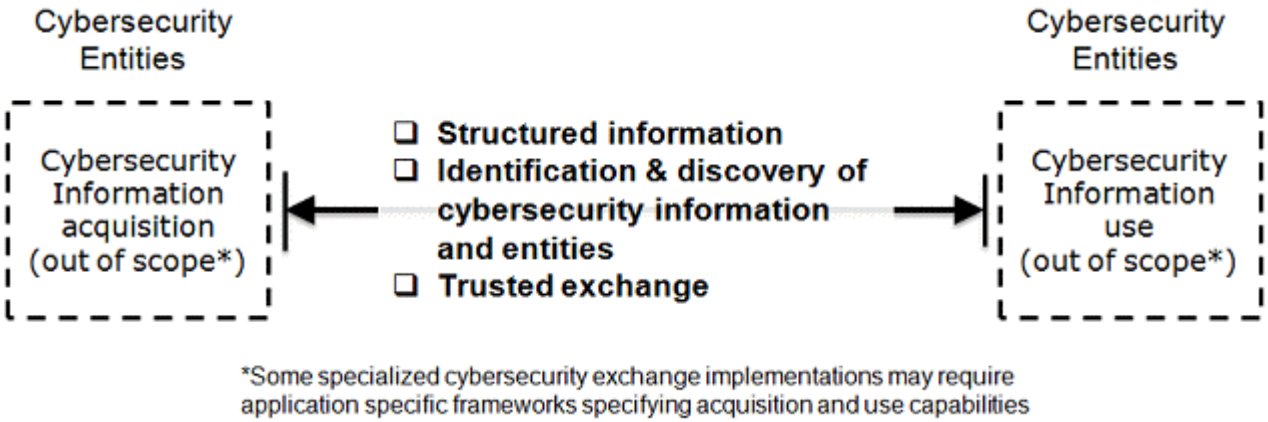
[정보보호] 글로벌 사이버보안 정보교류 국제표준화 동향

지난 7월 7일 한국과 미국의 주요 사이트가 DDoS(Distributed Denial of Service: 분산서비스거부) 공격을 받아 서비스가 마비되는 상황이 발생했다. 7.7 DDoS 대란이라 불리는 이번 사건뿐만 아니라 세계 곳곳에서는 범죄적 양상을 띠는 다양한 사이버 범죄 발생이 증가하고 있다.
이와 관련하여 미(美) 정부는 지난 5월 30일 "사이버스페이스 정책 리뷰(Cyberspace Policy Review)"를 발표해 사이버보안의 책임 공유, 사이버보안 사고 발생 시 긴밀한 대응을 위한 유관기관 간의 정보 공유 및 사고 대응을 위한 체계 구축 등의 전략을 내세운 바 있다. 이러한 전략의 연장선으로 예상되는 사이버보안에 대한 국제표준화 활동이 ITU-T SG17 Q.4(사이버보안 연구과제)에서 진행되고 있어 본 고에서는 지난 9월 스위스 제네바에서 개최된 Q.4/17 회의에서 논의된 사이버보안 정보교류 표준화를 위한 주요 내용을 기술한다.

9월 회의 쟁점 사항을 언급하기에 앞서, 미국대표이자 Q.4/17의 라포처인 Anthony M. Rutkowski은 6월 인터림 회의를 통해 "사이버보안 정보 교환 프레임워크"를 소개하고 사이버보안 정보 교환 프레임워크를 만족시키기 위한 주요 요구사항을 정의하였다. <그림 1>은 Anthony M. Rutkowski에 의하여 제안된 사이버보안 정보 교환 프레임워크의 개념을 나타낸다. 단, 제안 프레임워크는 정보 교환 참여자 간에 교환되는 정보 자체와 교환에 대해서만 다루고, 각 정보 교환 참여자의 사이버보안 정보 수집 방식 및 교환된 정보의 활용에 대한 부분은 각 정보 교환 참여자에게 맡기고 있어, 본 표준화 아이템의 연구범위에서는 다루지 않는다.



<그림 1> 사이버정보 교환 프레임워크
(출처: ITU-T Q.4/17 Proposed initial draft text for Rec. ITU-T X.cybex, Cybersecurity information exchange framework (TD503))

이 제안은 지난 6월 제네바 인터림 연구과제 4 회의에서 제기된 이래, 제안된 표준화 워크 아이템은 9월 SG17 정기 회의를 통해 공식화되었고, 이와 관련하여 사이버보안 정보 교환 프레임워크 구현을 위한 주요 요소 표준 아이템으로 미국의 정보보호 관련 연구 개발 기관인 Mitre의 다양한 정보보호 관련 시스템 및 기술들과 NIST의 정보보호 표준들을 비롯한 다음의 아이템들을 ITU-T 신규 표준화 아이템으로 채택했다.

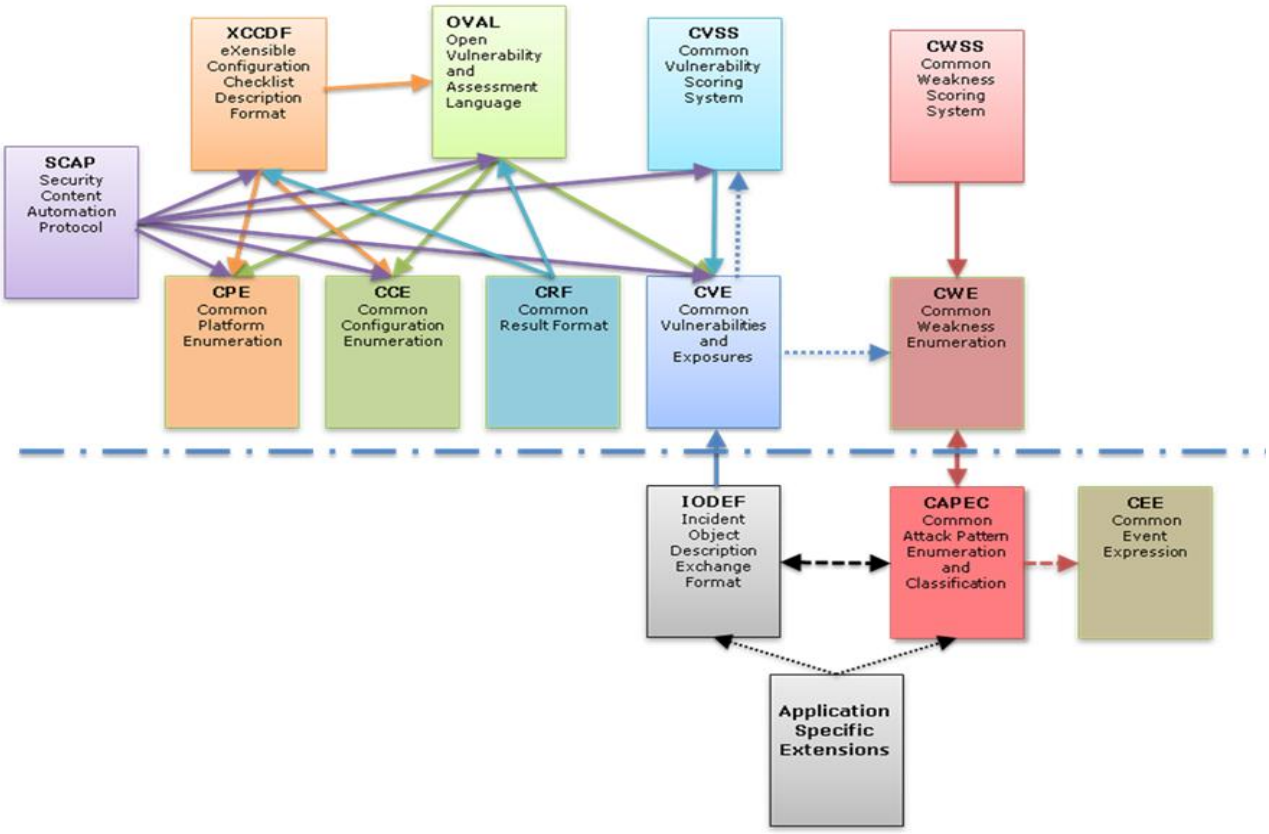
- X.cwe, Common Weakness Enumeration
- X.cwss, Common Weakness Scoring System
- X.oval, Open Vulnerability and Assessment Language
- X.scap, Security Content Automation Protocol
- X.xccdf, eXensible Configuration Checklist Description Format
- X.cpe, Common Platform Enumeration
- X.cce, Common Configuration Enumeration
- X.crf, Common Result Format

• X.cee, Common Event Expression
• X.iodef, Incident Object Description Exchange Format
• X.capec, Common Attack Pattern Enumeration and Classification
• X.dpi, Deep Packet Inspection Exchange Format
• X.pfoc, Phishing, Fraud, and Other Crimeware Exchange Format
• X.gridf, SmartGrid Incident Exchange Format
• X.chirp, Cybersecurity Heuristics and Information Request Protocol

이와 함께 사이버보안 정보 교환 프레임워크와 관련하여 다음의 아이템들이 각 국의 대표단으로부터 발표되어 추가적인 신규 표준화 아이템으로 채택되었다.

• X.cybex.1, An OID arc for cybersecurity information
• X.cve, Common Vulnerabilities and Exposures
• X.cvss, Common vulnerability scoring system
• X.cybex-disc, Discovery mechanisms in the exchange of cybersecurity information
• X.cybex-tp, Transport protocols supporting cybersecurity information exchange
• X.cybex.2: Use of XML Namespace in the Cybersecurity Information Exchange Framework
• X.cybex-beep: Definition of BEEP Profile for Cybersecurity Information Exchange
• X.teef, Cyber attack tracing event exchange format

<그림 2>는 사이버보안 정보 교환 프레임워크의 한 부분으로 교환 정보의 체계화를 위한 요소 및 요소 간 관계를 나타낸다.



<그림 2> 교환 정보 체계화를 위한 요소 및 요소 간 관계
(출처: ITU-T Q.4/17 Proposed initial draft text for Rec. ITU-T X.cybex, Cybersecurity information exchange framework (TD503))

사이버보안 정보 교환 프레임워크와 프레임워크를 중심으로 만들어진 표준화 아이템들은 2010년 4월에 있을 정기 회의를 앞두고 2번의 인터림 회의를 계획함으로써, 인터림 회의에서 문서 개발에 박차를 가하여 2010년 4월 연구반 17 정기 회의에서 사이버보안 정보 교환 프레임워크와 관련된 3개의 아이템(X.cybex, X.cve, X.cvss)들에 대한 determination 추진을 계획하고 있는 등 미국의 주도하에 표준화가 빠른 속도로 진행되고 있다. 또한 일본 등과 같은 주요국의 적극적인 참여 및 각국의 관심, 그리고 사이버보안 정보 교환 프레임워크 개발에 따른 파급효과로 인해 해당 아이템의 표준 개발의 귀추가 주목되고 있다. 우리나라도 사이버보안 정보 교환 프레임워크의 표준 개발 추이를 살피는 등 지속적인 관심 및 필요 시 참여가 필요할 것으로 판단된다.

김미주 (한국인터넷진흥원 정보보호본부 보호기술팀 연구원, mijoo.kim@kisa.or.kr)