情 報 保 護 學 會 誌
第23卷 第3號, 2013. 6

ITU-T SG17에서의 사이버보안 국제 표준화 동향

김 종 현*, 김 익 균**

요 약

최근 외부 해킹으로 대량의 개인정보 유출, 대규모 시스템 장애 등 사고가 빈번히 발생하고 있다. 특히, 보안체계를 잘 갖추고 있던 조직들도 지능화되고 있는 사이버 공격 앞에 무력하게 당하는 사건들을 접하면서 많은 기업 및 조직들이 대응 방안 마련에 고심하고 있다. 본 논문에서는 ITU-T SG17에서 진행 중인 사이버보안 국제 표준화 동향을 살펴본다.

Ⅰ. 서 론

사이버 공격을 탐지하고 방어하기 위한 가장 전통적인 연구는 IDS(Intrusion Detection System), IPS(Intrusion Prevention System), 방화벽과 같은 보안 시스템의 공격 탐지/차단 성능 및 정확도를 높이려는 연구였다. 그러나 사이버공격 및 위협이 복합적이고 다양한 형태로 변형되거나 새로이 등장하는 현 추세에서는 보안 시스템의 성능 향상만으로는 지능화되고 고도화된 사이버 공격위협을 효과적으로 방어하기 어렵다. 또한, 사이버 보안 위협의 양상이 점차 세계화되고 피해의 규모 또한 날로 심각해지고 있어, 한 지역이나 한 국가만의 노력으로는 사이버공간의 안전성을 보장하기에는 한계가 있다. 이러한 사이버 공간에서의 보안 문제 해결을 위한 국제적인 공조 대응 노력의 일환으로 국제 표준화 단체에서 사이버보안 정보공유기술에 대한 표준화 작업을 진행 중에 있다.

보안 정보공유 기술이란 사이버보안정보를 보유하거나 요청하는 조직, 사람, 디바이스, 프로세스들이 사이버환경과 자산을 사이버 공격으로부터 사전에 보호하고 긴급 대응하기 위한 사이버보안 정보를 서로 공유함으로써 협력을 통한 사이버공격 방어를 가능하게 하는 것을 목적으로 하는 기술이다. 여기서 사이버보안 정보란 위협, 취약점, 침해사고, 보안평가, 공격탐지, 공격복구, 공격대응, 보안로그 등의 보안 정보를 의미한다. 본고에서는 사이버보안 관련 국내외 표준화 동향을 살펴보고, 향후 대응방안에 대하여 언급하고자 한다.

Ⅱ. 국외 표준화 동향

2.1 ITU-T에서의 표준화 동향

ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)에서 사이버보안 분야를 담당하는 그룹은 Q.4/17로, 사이버공간에서 발생하는 침해사고 및 취약점 등에 대한 대응방안 및 정보 공유 등에 대한 보안 표준들을 개발하고 있으며, WTSA-08 결의 50을 구현하기 위해 사이버보안 관련 표준을 개발하고 있고, 특히 사이버보안 정보들을 공유할 수 있는 표준을 개발 하고 있다. 이중에서 우리 입장에서 주목해야 할 표준화 활동은 사이버정보공유 프레임워크(X.1500) 관련 표준, 사이버보안지수(X.csi), 보안정보 공유 협상 프레임워크(X.sisnego) 등 이다.

2009년 6월에 미국과 일본의 주도로 개발된 표준(X.cybex: 사이버보안 정보교환 프레임워크)은 2011년 4월에 제정되었으며, 이 표준은 유관 사이버보안 기관이나 국가 간에 침해사고정보를 포함한 사이버보안 정보를 공유함으로써 침해 사건 발생 및 예방 시 공동으

본 연구는 미래창조과학부가 지원한 2013년 정보통신·방송(ICT) 연구개발사업(다중소스 데이터의 Long-term history분석기반 사이버 표적공격 인지 및 추적 기술 개발)의 연구결과로 수행되었습니다.
* 한국전자통신연구원 사이버보안연구단 네트워크보안연구실 (jhk@etri.re.kr)
** 한국전자통신연구원 사이버보안연구단 네트워크보안연구실 (ikkim21@etri.re.kr)

로 신속하고 효율적으로 대응하기 위한 표준이다[4].

2009년 11월, 한국의 제안으로 조직, 부문, 또는 국가에 대한 정보보호 수준을 평가하기 위한 글로벌 공통 기준을 개발하기 위한‘ 사이버보안지수(X.csi)’ 표준 개발이 착수되어 많은 진전이 이루어졌다. 본 표준은 사이버공간에서 안정성을 평가하기 위한 기준은 국가별로 상이하고, 고려 대상이 다양하여 이에 대한 정형화된 기준을 개발함으로써 사이버공간에서 안정성 평가에 객관적인 기준을 정의하기 위함이다. 또한, 본 기준을 개발하기 위해 ITU에서 개발된 “개발지수(Development Index)", 세계경제포럼에서 개발된 ”네트워크 준비 지수(Network Readiness Index)", 인터넷보안 센터에서 개발된 “보안지수(Security Metrics)", 미국 NIST 및 유럽 ENISA에서 개발된 가이드라인과 한국에서 개발된 정보보호지수가 함께 고려되었다[4].

본 국제표준은 총 32가지의 사이버보안 지수 정의와 이를 객관적인 방법에 따라서 안정성을 수치로 계산하는 방법을 정의하고 있어, 각 국가별 사이버보안 환경에 따른 지수 개발에 중요한 가이드라인으로 활용이 예상되며, 2013년 4월 회의에서는 총 32가지의 사이버보안 지수 정의와 이를 객관적인 방법에 따라서 안정성을 수치로 계산하는 방법에 대해 최종적인 텍스트를 검토하여, 국제표준 채택을 위한 준비과정(determination)을로 승인되었다.

2011년 4월, 한국의 제안으로 채택된 보안정보 공유 협상 프레임워크(X.sisnego) 표준은 사이버정보 공유 프레임워크(Cybex) 시리즈 내에 통신 주체들 간에 정보를 교환하기 위한 초기 협상 기술을 국제표준으로 개발하기 위함이며, 본 표준은 미국이 공동 에디터로 참여하였으며, 당초 독립적인 표준으로 개발하려고 하였으나, 하나의 유즈케이스 성격이 강해 사이버보안 개요(X.1205) 국제표준의 부속서로서 2013년 4월 회의에서 승인되었다[3].

현재까지 Q.4/17에서 개발되어 제정된 주요 표준안은 다음과 같다.

〔표 1〕 ITU-T Q.4/17 주요 제정 표준〔3〕

표준번호	제목	내용	제정일
X.1205	Overview of cybersecurity	사이버보안 개요	2008년 4월
X.1206	A vendor-neutral framework for automatic notification of security related information and dissemination of updates	보안관련 정보 자동알림과 업데이트 분배를 위한 벤더 중립적 프레임워크	2008년 4월
X.1207	Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software	통신서비스사업자를 위한 스파이웨어 및 유해 소프트웨어 대응 가이드라인	2008년 4월
X.1209	Capabilities and their context scenarios for cybersecurity information sharing and exchange	사이버보안 정보 공유 및 교환을 위한 요구사항 및 시나리오	2010년 12월
X.1303	Common alerting protocol (CAP 1.1)	OASIS의 XML언어를 ITU-T ASN.1언언어로 변경	2007년 9월
X.1500	Overview of cybersecurity information exchange (CYBEX)	사이버보안 정보 교환 기술	2011년 4월
X.1500.1	Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange	사이버보안 정보교환을 위한 OID 체계에서의 등록체계 절차	2012년 3월
X.1520	Common vulnerabilities and exposures	취약점에 대한 표준화된 식별자 정의	2011년 4월
X.1521	Common vulnerability scoring system	취약점 특성에 따른 점수 부여 시스템	2011년 4월
X.1524	Common weakness enumeration	공개적으로 알려진 정보보안 취약점을 교환하기 위한 수단	2012년 3월
X.1570	Discovery mechanisms in the exchange of CYBEX	사이버보안정보를 발견하기 위한 프레임워크와 이를 제공하는 메커니즘	2011년 9월

표준번호	제목	내용	제정일
X Suppl.8	ITU-T X.1205 – Supplement on best practices against botnet threats	봇넷 위협에 대응하기 위한 실용적 솔루션 제시	2010년 12월
X Suppl.9	ITU-T X.1205 – Supplement on guidelines for reducing malware in ICT networks	X.1205 부속서-ICT 네트워크 환경에서 악성코드 예방을 위한 가이드라인	2011년 9월
X Suppl.10	ITU-T X.1205 – Supplement on usability of network traceback	X.1205 부속서-네트워크 역추적의 유즈케이스 및 요구사항 정의	2011년 9월
X.1528	Common platform enumeration	IT 제품에 대한 공통 플랫폼 목록	2012년 9월
X.1528.1	Common platform enumeration naming	IT 제품에 대한 공통 플랫폼 목록의 네이밍 구조	2012년 9월
X.1528.2	Common platform enumeration name matching	IT 제품에 대한 공통 플랫폼 목록의 네이밍 매칭 규격서	2012년 9월
X.1528.3	Common platform enumeration dictionary	IT 제품에 대한 공통 플랫폼 목록 해설서 및 유즈케이스 정의	2012년 9월
X.1528.4	Common platform enumeration applicability language	IT 제품에 대한 공통 플랫폼 목록의 적용 언어 규격서	2012년 9월
X.1541	Incident object description exchange format	침해사고 정보교환을 위한 포맷	2012년 9월
X.1580	Real-time inter-network defence	침해사고 정보교환을 위한 전달 메커니즘(RID)	2012년 9월
X.1581	Transport of real-time inter-network defence messages	침해사고 정보교환을 위한 HTTP/TLS 기반의 메시지 전달 메커니즘	2012년 9월
X.1526	Open vulnerability and assessment language	보안 설정에 대한 공개 취약점 평가 언어	2013년 4월
X.1544	Common attack pattern enumeration and classification	사이버공격패턴의 식별, 기술, 분류를 위한 XML/XSD 기반의 명세서	2013년 4월
X Suppl.20	ITU-T X.1205 - Supplement on framework of security information sharing negotiation	X.1205 부속서-보안정보 공유 협상을 위한 프레임워크	2013년 4월
X Suppl.18	ITU-T X.1205 - Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks	X.1205 부속서-IP기반의 통신네트워크상의 비정상 트래픽 탐지 및 제어를 위한 가이드라인	2013년 4월

또한, 현재 Q.4/17에서 개발이 진행 중인 표준 문서는 아래와 같다.

〔표 2〕 ITU-T Q.4/17 진행 중인 표준문서〔3〕

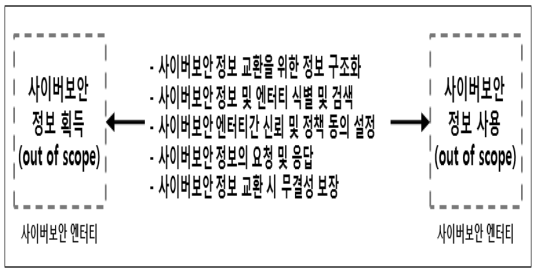
구분	제목	내용	표준개발 완료 예정일
CYBEX	(X.1500 Appendix I) Structured cybersecurity information exchange techniques of Recommendation ITU-T X.1500	사이버보안 정보교환 기술의 목록 및 구조도	2013년 9월
	(X.cybex-tp) Transport protocols supporting cybersecurity information exchange	사이버보안 정보교환을 위한 전달 프로토콜의 개요 및 특성 정의	2014년
	(X.cce) Common configuration enumeration	다중 정보소스에 대한 보안설정 관리를 위한 공통 설정 목록 정의	2015년
	(X.cee) Common event expression	컴퓨터 이벤트에 대한 표현, 저장, 교환 방법에 대한 정의	2014년
	(X.cee.1) CEE overview	CEE 요소들에 대한 구조 및 개요	2014년
	(X.cee.2) CEE profile	CEE 프로파일에 대한 이벤트 클래스를 표현하는 방법	2014년
	(X.cee.3) CEE common log syntax	CEE 아키텍처의 CLS(common log syntax) 구성요소를 정의	2014년
	(X.cee.4) CEE log transport (CLT) requirements	일반적인 로그 전달(CLT)에 대한 보안적 요구사항 및 가이드라인	2014년

구분	제목	내용	표준개발 완료 예정일
	(X.cwss) Common weakness scoring system	일반적인 소프트웨어 보안약점 평가 시스템	2014년
	(X.cybex-beep) Use of BEEP for cybersecurity information exchange	사이버보안 정보교환을 위한 BEEP(Block Extensible Exchange Protocol)의 사용 명세서	2014년
사이버 보안 일반	(X.csi) Guidelines for cybersecurity index	사이버보안지수 및 안전성 평가 기준	2013년 9월
	(X.trm) Overview of traceback mechanisms	역추적 메커니즘 개요	2013년 9월
	(X.maec) Malware attribute enumeration and characterization	악성코드에 대한 속성 목록과 악의적 행위의 특성화	2013년 9월
	(X.bots) Centralized framework for Botnet detection and response	봇넷 탐지와 대응을 위한 중앙집중식 프레임워크	2014년
	(X.eipwa) Guideline on techniques for preventing web-based attacks	웹기반 공격을 차단하기 위한 기술적 가이드라인	2014년
	(X.csmc) An iterative model for cybersecurity operation using CYBEX techniques	CYBEX 기술을 활용한 사이버 보안 운용을 위한 개념, 요구사항, 아키텍처를 정의	2014년

현재 Q.4/17에서 중점적으로 다루고 있는 표준화 작업은 사이버보안 엔터티(Entity)간 사이버보안 정보 교환 프레임워크 모델을 개발하는 것이다. 이 표준화 작업은 2008년 6월 독일 하이델베르크에서 개최된 SG17 Q.6(현재 SG17 Q.4) 사이버보안 연구그룹의 인터림 회의를 통해서 소개되었으며, 2008년 9월 ITU-T SG17 정기회의를 통해 표준과제가 채택되었다. 사이버 공간의 침해사고에 대한 공조의 일환으로 침해 정보와 같은 사이버보안 정보에 대한 사이버보안 엔터티간의 교환을 지원하는 프레임워크에 대한 표준개발이 완료되었다.

특히, 사이버보안 정보 교환 구현을 위한 표준화 항목으로 미국의 정보보호 관련 연구 개발 기관인 MITRE의 정보보호 관련 시스템 및 기술들과 NIST(National Institute of Standards and Technology)의 정보보호 표준들을 ITU-T 국제표준화 항목으로 채택하였다. 일명 CYBEX(Cybersecurity Information Exchange)라 불리는 이 표준화 작업은 미국의 주도 및 일본, 영국, 캐나다, 한국 등 주요국의 적극적인 참여로 빠른 속도로 진행되고 있다. 현재 기본 프레임워크로 X.1500 표준이 제정된 상태이며, 2013년까지 CYBEX와 관련된 문서의 표준을 개발 완료하는 것을 목표로 하고 있다.

CYBEX 모델은 (그림 1)같이 사이버보안 엔터티간의 사이버보안 정보 교환을 위해 다음과 같은 기술로 구성되어 있다[5].



〔그림 1〕 CYBEX 모델

여기서 말하는 사이버보안 엔터티란 사이버보안 정보를 제공하거나 제공받는 조직, 개인, 장치 혹은 프로세스를 말하며, CIRT(Computer Incident Response Team)나 장비, 소프트웨어, 네트워크 기반 시스템 운영자 등이 이에 해당된다. 사이버보안 정보 교환은 공공 도메인뿐만 아니라 사전에 정책에 동의한 신뢰된 커뮤니티 간에도 발생할 수 있다. 엔터티간에 교환되는 사이버보안 정보에는 사이버 환경과 조직 그리고 사용자 자산을 보호하기 위해 사용될 수 있는 위협, 취약점, 침해, 대응방안 등의 정보를 의미한다.

2.2. 기타 표준화기구에서의 표준화 추진현황

2.2.1 IETF

IETF(Internet Engineering Task Force)에서는 사이버보안 정보공유와 관련된 표준을 개발하는 워킹그룹으로서 두 개의 그룹, 즉 ID WG(Intrusion Detection Working Group)과 INCH WG(extended INCident Handling Working Group)이 있다[6]. ID WG는 보안 시스템들 간의 정보 공유를 위한 데이터 포맷과 교환

절차에 대한 표준을 개발하고, INCH WG에서는 보안 관련 조직 간의 협력 통합 보안 제어를 위한 교환 데이터의 데이터 형식에 대한 표준을 개발하였다. 두 WG에서 개발한 사이버보안 정보를 교환하기 위한 표준 프로토콜은 IDMEF(RFC 4765(2007), RFC 4766(2007)), IODEF(RFC 3067(2001), RFC 5070(2007)), 그리고 RID(RFC 6045(2010)) 등 이다. 현재 두 WG은 표준 개발을 완료하여 활동이 종료된 상태이다.

〔표 3〕 IETF에서의 사이버보안 관련 표준 문서〔6〕

표준명	표준 내용	진행 상태
IDMEF (Intrusion Detection Message Exchange Format)	• IDS 및 IPS와 같은 공격 탐지 시스템이 탐지한 공격 이벤트에 대한 경보(alert)를 보안관리 시스템에게 보고하기 위한 데이터 포맷 및 데이터 교환 절차를 정의함 • 경보를 생성한 분석기(analyzer) 식별정보, 경보가 생성된 시간, 경보가 탐지된 시간, 분석기의 현재 시간, 공격 시스템과 타켓(목적지) 시스템에 대한 정보, 공격정보, 공격 위험도와 경보에 대응하기 위해 실행된 액션 등의 정보를 표현함	2007년, RFC-Informational
IODEF (Incident Object Description Exchange Format)	• 보안침해사고 대응팀(CSIRT: Computer Security Incident Response Team) 상호간에 컴퓨터 보안 사고에 대한 정보를 공유하기 위한 데이터 표현을 정의하는 것을 목적으로 함 • 보안사고가 언제, 어디서 발생했고, 누가 어떤 공격수법을 사용했는지, 그리고 사고 피해는 어떠한지 등 컴퓨터 보안 사고에 대한 전반적인 정보를 전달하기 위하여, 침해사고 식별 번호, 침해사고가 탐지/시작/종료/보고된 시간, 침해사고에 대한 설명, 침해사고와 관련된 단체의 연락처, 피해상황, 사용된 공격기술, 침해사고 처리동안 일어났던 이벤트 및 액션, 그리고 침해사고를 구성하는 이벤트들에 대한 정보를 표현함	2007, RFC-Proposed Standard
RID (Real-time Inter-network Defense)	• 침해사고 처리를 위한 모든 일련의 과정들을 용이하게 지원할 수 있도록 공격 탐지 정보, 공격시스템 추적 및 식별, 그리고 공격 대응 메커니즘 등 침해사고 처리와 관련된 데이터를 공유할 수 있도록 하는 것을 목적으로 함. • 다음과 같이 6가지의 메시지 타입을 정의하고 있음. - TraceRequest: 공격 발신지의 위치에 대한 추적을 요청할 때 사용되는 메시지 - Request Authorization: Trace Request 메시지의 응답으로서 처리 진행상태를 알리기 위해 보내지는 메시지 - Result: TraceRequest에서 요청된 추적을 완료하거나 Investigation에서 요청된 액션을 완료했을 때 요청 메시지 발신자에게 알려주기 위해 보내지는 메시지 - Investigation: 공격 발신지와 가장 가까운 네트워크 제공자에게 공격자에게 가할 액션을 요청할 때 사용되는 메시지 - Report: 보안사고를 보고할 때 사용되는 메시지 - IncidentQuery: 침해사고에 대한 정보를 요청할 때 사용되는 메시지	2010, RFC-Informational

2.2.2 ISO/IEC JTC 1

ISO/IEC JTC 1(International Standard Organization/International Electrotechnical Committee Joint Technical Committee 1) 에서는 사이버보안 및 보안사고 관리를 위한 표준을 개발하고 있다.

〔표 4〕 ISO/IEC JTC 1에서의 사이버보안 관련 표준 문서

표준명	표준 내용	진행 상태
ISO/IEC 27032 Guidelines for cybersecurity	• 디바이스와 네트워크에 의해 인터넷 상에서 사람, 소프트웨어, 서비스의 상호작용으로부터 초래된 복잡한 환경인 사이버공간에서의 보안 이슈	2011, second CD
ISO/IEC 27035 Information security incident management	• 보안사고의 탐지, 보고, 평가, 대응, 관리, 그리고 사고 재발방지를 위한 보안 취약성의 탐지, 평가, 관리 등 보안사고 관리 및 개선에 관한 표준	2011, FDIS(Final DIS)

2.3 국가별 표준화 활동

2.3.1 미국

9.11 테러이후 사이버보안을 자국만의 문제가 아니라 글로벌 관점에서 공조를 강화해야한다는 기조아래

사이버보안에 관련된 국제표준화 작업에 앞장서고 있다. 오바마 정부는 2009년 "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 등을 포함하는 실행 전략을 발표한 바 있다. 이러한 전략의 연장선으로 사이버보안 정보 교환 표준화 작업을 ITU-T에서 진행하고 있다. 또한, 미국 연방 정부가 출연해 설립한 비영리 업체인 MITRE에서는 미 연방(국방부, 국세청 등)의 보안 관련 정보를 연구 및 개발하고 있다[8]. 미국에서는 MITRE에서 개발한 C*E(CVE, CWE, CPE) 및 C*SS(CVSS, CWSS) 시리즈를 국제표준으로 등록하기 위하여 ITU-T 표준화 회의에 적극적으로 참여하고 있으며, 2011년 CYBEX가 국제표준으로 제정되기까지 가장 큰 노력을 기울이는 등 왕성한 활동력을 보여주고 있다[1,2].

2.3.2 일본

일본에서는 NICT(National Institute of Information and Communications Technology)를 중심으로 보안정보 공유의 중요성을 인식하고 ITU-T 표준화에서 진행하고 있는 사이버보안정보 공유 프레임워크 개발에 적극 참여하고 있으며, 아울러 SCAP(Security Content Automation Protocol)을 활용해 국가 취약점 DB(Database)인 JVN(Japan Vulnerability Notes) 구축하는 등 사이버보안 정보공유 시스템 개발에도 적극적으로 투자하고 있다[9,10].

2.3.3 유럽

유럽에서는 ENISA(Securing Europe's Information Society)라는 프로젝트를 통하여 이탈리아, 영국, 네덜란드가 주축이 되어 국내 및 국제 수준에서 경고와 정보 공유를 위한 프레임워크 모델과 파일럿 플랫폼을 개발하고 있다. ENISA는 EU에 의해서 연구비가 지원되는 다음과 같은 프로젝트들의 연구결과를 수용한다[11].

- the Information Assurance Messaging Standard (Symantec)
- the ENISA Study on a European Information Sharing and Alert System
- the ENISA Data Collection Framework Study
- the Availability and Robustness of Electronic Communications Infrastructures Study (일명 ARECI)

유럽에서는 프로젝트를 통하여 수행한 보안정보공유와 관련된 연구 결과물을 국제표준으로 등록하기 위하여 ISO/IEC JTC 1에서의 표준화에도 적극 참여하고 있다.

Ⅲ. 국내 표준화 동향 및 정책 현황

3.1. 국내 표준화 동향

사이버보안 정보 공유와 관련된 국내 표준화는 한국전자통신연구원(ETRI)과 한국인터넷진흥원(KISA)을 중심으로 진행되고 있으며, 기반이 되는 사이버보안 정보공유 프레임워크와 정보공유 프로토콜은 ITU-T와 IETF 등 국제표준화기구에서 제정한 표준을 국내 상황에 맞게 수정한 상태로 준용하고 있다. 국제 표준에 없는 디지털 증거 파일 교환, VoIP 공격 탐지 포맷, DoS 공격 탐지 및 대응 포맷 등은 독자적으로 개발을 완료한 상태이다.

〔표 5〕 국내 사이버보안 정보공유 기술 표준화 현황〔7〕

표준과제명	내용	진행상태
디지털 증거 파일 교환포맷 (TTAK.KO-12.0080)	• 디지털 증거 파일 교환포맷을 정의하고, 포맷 내의 헤더 및 데이터 구조와 파일 트레일러에 대해 기술	2008년 완료
VoIP 침입 탐지 메시지 교환 포맷 (TTAK.KO-12.0084)	• VoIP 침입 탐지 메시지 교환 포맷의 요구사항을 정리하고, UML (Unified Modeling Language)의 클래스 다이어그램을 사용하여 메시지 교환 포맷을 정의	2008년 완료
분산서비스거부 공격의 탐지 및 대응 메시지 교환 포맷 (TTAK.KO-12.0145)	• 분산 서비스 거부 공격에 대한 탐지 정보 및 대응 정책의 상호 공유를 위하여 공통된 메시지 교환 포맷 정의 • 메시지 교환 포맷은 DDoS 공격의 탐지 정보와 대응 정책 정보를 확장성 생성 언어(XML: eXtensible Markup Language) 기	2010년 완료

표준과제명	내용	진행상태
	반의 DPMEF(DDoS Detection Information and Response Policy Message Exchange Format)로 정의함	
네트워크 공격에 대한 시그니처 교환 프로토콜 (TTAK.KO-12.0061/R1)	• 네트워크 환경을 위협하는 공격에 대해 그 특징을 검출하여 생성한 시그니처 정보들을 안전하게 교환하기 위한 프로토콜	2010년 완료
이기종 NAC 시스템 간 연동 방식	• 이기종의 NAC에 대한 연동을 위해서 필요한 데이터의 표현방식, 데이터 전송 방식을 정의	2011년 완료
사이버보안 정보공유 협상 절차 (TTAK.KO-12.0172	• 사이버보안 정보를 제공하거나 제공받는 사이버보안 엔티티들이 어떻게 사이버보안 정보를 공유할지를 협상하는 사이버보안 정보공유 협상 절차를 정의	2011년 완료

3.2 국내 표준화 정책현황

최근 유럽연합(EU)과 미국 정부가 사이버 보안 및 사이버범죄 위협 대처를 위한 공조를 강화하기로 했으며, 이미 두 정부는 지난해 말 사이버 보안위협 공조를 위한 작업반을 설치, 연내에 사이버 사고 대응훈련을 합동으로 전개하고 수자원이나 전력 등의 통제 시스템 안전 이슈에 공동 대응하기로 했다. 또 정보공유, 두 대륙 간 협력 모델 개발을 통해 사이버보안과 사이버 범죄 대응능력 강화를 도모하고 다른 국가 및 조직에도 모범사례가 되도록 한다는 계획이다.

최근에 미국 연방수사국(FBI)은 마이크로소프트, 트렌드마이크로 등 주요 글로벌 보안 업체와의 공조체계 구축을 통하여 1100억 달러 이상의 이득을 취한 사이버 범죄 집단을 소탕하는 등 국가와 보안업체간의 협력을 강화하는 추세다.

우리나라는 지난 2009년 7월 7일 DDoS(Distributed Denial of Service) 공격으로 청와대 등 국내 주요 사이트에 인터넷 접속이 지연되거나 접속이 되지 않는 등 큰 피해를 입은 바 있다. 일명 7·7 DDoS 대란으로 불리는 이 사건 이후 행정안전부는 국제 협력의 필요성을 인식하고 2009년 11월 서울에서 열린 '제2차 아시아태평양경제협력체(APEC) 사이버보안)' 세미나에서 UN이나 APEC 산하에 사이버보안 국제기구를 창설 필요성을 개진하고, 2010년 국제협력 강화를 통한 사이버안전 제고를 위해 `사이버안전 국제기구' 설립에 대한 국제적 공감대 형성 및 추진전력 등의 방안 마련을 위한 연구를 진행 중에 있다[2].

현재 우리나라는 DDoS 및 주요 기관 해킹 등 보안사고에 민관 합동의 공동대책반을 구성해 대응하고 있다. 하지만 업계와 전문가들은 다른 국가와의 공조체계 구축은 물론 민간 기업들과도 상시적인 협력이 이루어질 수 있도록 보다 체계적인 시스템을 만들어야 한다고 지적하고 있다. 최근 국내 주요 금융권 및 방송사를 타깃으로 사이버테러가 발생하여 총 3만 2000대의 PC가 감염되어 정상적인 서비스 제공이 어려워졌으며 이로 인한 금전적 피해도 매우 큰 것으로 보고되었다. 이런 유형의 공격은 특정 조직을 대상으로 장기간에 걸쳐 조직적으로 중요 정보를 탈취하기 때문에 해외 공격자 IP 추적 등 해외 사이버 보안 조직과의 협력이 중요한 상황에서 이와 같은 체계의 마련이 더욱 절실하다는 것이다. 이를 위해서는 국제적으로 표준화된 정보교환 프로토콜 및 데이터 포맷을 사용해야하지만, 현재 국내에서는 자체적인 프로토콜 및 데이터 교환 포맷을 사용하고 있어 국제적인 사이버보안 협력 시 상호연동에 문제가 발생할 수 있다.

Ⅳ. 향후 대응 방안

우리나라는 DDoS 및 주요 보안사고 발생 시 민관 합동 대책반을 구성해 대응하고 있지만 이와 같은 협력체계는 세계화되고 있는 사이버보안 위협에 대응하기에 한계가 있다. 또한 전 세계적으로 사이버보안에 대한 국제적인 공조 및 협력 필요성이 강조되고 있다. 따라서 국가 간 영역 구분이 무의미한 사이버 공간에서 우리나라 국민들의 안전한 인터넷 사용을 보장하기 위해서는 신뢰할 수 있는 국내·외 전문기관 및 보안업체와의 협력이 필수적이며, 이를 위해서는 국제 표준화된 규격을 이용한 신뢰 기관과의 정보 공유가 기반이 되어야 한다.

또한, 사이버보안 정보 공유 관련 국제 표준 규격에 대한 면밀한 분석을 통해 선제적인 보안 시스템 및 장비 개발로 국내 제품의 수출 및 국내 시장 보호를 위해 노력해야 한다.

사이버보안에 대한 국제적인 공조 및 협력을 위한 실질적인 대응방안으로는 사이버보안 정보 공유를 위한 기반 마련에 있다. 이를 위해서는 국제 표준화된 사이버보안 정보 교환 기술 표준에 대한 국내표준화 및 적용

을 조속히 추진하여 현재 국내에서 자체적으로 개발되어 사용되고 있는 정보 공유 프로토콜 및 데이터 교환 포맷 사용으로 인한 국제적인 사이버보안 협력 시 상호 연동 문제를 예방할 수 있다.

또한, DDoS 및 주요 보안사고 대응에 실제 참여하는 국내 민관 합동 대책반 전문가 및 현재 사이버보안 정보 공유 기술 국제표준화가 진행 중인 ITU-T SG17 Q.4(사이버보안)에 참여하고 있는 국내전문가들의 적극적인 표준화 참여 및 국내 보유의 우수 기술과 사이버보안 관련 R&D 과제의 성과를 국제표준으로 연결될 수 있도록 추진하는 것이 필요하다.

마지막으로 국내 CERT(Computer Emergency Response Team), ISP 사업자, 보안 업체 등에서 국제표준화된 사이버보안 정보 공유 규격에 맞추어 시스템을 구축하고, 국가적인 사이버보안 대응체계를 구축하는 것에서 더 나아가 국제적인 대응체계를 구축할 수 있도록 해야 한다.

업체의 경우 당장 사이버보안 정보 공유에 대한 국제표준 규격을 적용하기에는 현실적인 여건이 부족하다. 하지만 국가적인 차원에서 사이버보안 정보 공유에 대한 선도적인 적용을 통해 국가 사이버보안 대응체계를 강화하고, 더 나아가 국제적인 대응체계를 구축함으로써 사이버보안 공격에 신속하고 효과적으로 대응할 수 있는 발판을 마련할 수 있다.

또한 미국, 일본 등 주요국에서 사이버보안 분야 주도권 확보를 위해 적극적으로 표준화에 참여하는 상황에서 우리나라에서도 사이버보안 분야 표준화 R&D 투자를 통해 우리나라의 기술이 국제 표준으로 반영될 수 있도록 국제표준화 활동을 강화해야 한다.

Ⅴ. 결 론

본고에서는 ITU-T SG17에서 진행 중인 사이버보안 국제 표준화 동향을 살펴보고, 국내 표준화 동향과 향후 대응방안을 언급하였다. 사이버보안 정보공유 프레임워크 기술은 국내 각 정부 및 민간 기관별 침해대응센터의 고도화에 해당되는 것으로서 소규모 네트워크 차원에서 단순 모니터링 및 보안정책을 적용하는 형태를 초월하여 향후에는 네트워크 전체를 보안 제어 영역으로 확장하여 서로 다른 관리 도메인 간 보안정보 공유를 통한 협력기반의 종합적인 통합 보안제어 체계를 구축하는 기술로 발전할 것으로 예상된다. 사이버보안 정보에 대한 공유는 개별망의 피해가 타 망으로 확산되는 것을 방지하고, 침입탐지・분석・대응을 상호 협력 하에 종합적으로 관리하여 국가차원의 통합 사이버보안 대응체계를 구축 및 강화할 수 있다.

또한, 전 세계적으로 분포된 봇넷 및 취약점 정보를 수집하여 국내 유관기관, 침해대응센터, ISP 사업자, 보안 업체 간 정보 공유 및 공존체계 구축 등을 통해 국가차원에서 인터넷 위협에 대해 선제적으로 모니터링하고 정부에서 신속한 상황파악이 가능한 글로벌 보안 콘텐츠를 제공함으로써 여러 국가에 걸친 사이버보안 사고가 발생할 경우 국제적으로 공동 대응할 수 있는 협력 대응체계를 수립할 수 있다.

참고문헌

[1] 김동진, 조성제, “국가 DB기반의 국내외 보안취약점 관리체계 분석” Internet and Information Security, 1(2), pp.130-147, 2010.

[2] 조성제 외 “정보신기술 취약점 관리체계 구축(안)” 최종연구보고서, KISA-WP-2010-0018, 2010.

[3] Youki Kadobayashi et al, “Report of Q4/17” T13-SG17-130417-TD-PLEN- 0037!R3!MSW-E, 2013

[4] ITU-T SG17: Security, http://www.itu.int/en/ITU-T/ studygroups/2013-2016/17/Pages/default.aspx

[5] ITU-T Recommendation X.1500 "Overview of cybersecurity information exchange" 2011

[6] IETF http://www.ietf.org

[7] TTA http://committee.tta.or.kr

[8] MITRE, http://www.mitre.org

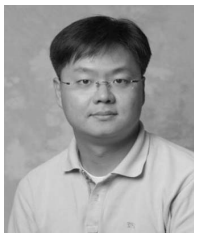
[9] SCAP, http://scap.nist.gov

[10] JVN, http://jvn.jp

[11] ENISA, http://www.enisa.europa.eu

〈著者紹介〉

김 종 현 (Jong-Hyun Kim)
2000년 : 오클라호마주립대 컴퓨터학과공학석사
2005년 : 오클라호마주립대 컴퓨터학과공학박사
2005년~현재: 한국전자통신연구원 선임연구원
<관심분야> 정보보호, 네트워크보안, 역추적기술



김 익 균 (Kim, Ikkyun)
1994년 2월 : 경북대학교 컴퓨터공학과 졸업(공학사).
1996년 2월 : 경북대학교 컴퓨터공학과졸업(공학석사).
2009년 2월 : 경북대학교 컴퓨터공학과 졸업(공학박사).
2005 Purdue University 객원연구원.
1996년~현재 한국전자통신연구원 네트워크보안연구실 실장/책임연구원.
<관심분야> 네트워크 보안, 컴퓨터네트워크, 클라우드보안