情 報 保 護 學 會 誌
第22卷 第2號, 2012. 4

사이버보안 정보 교환 기술의 개발 및 표준화 동향

안 개 일*, 서 대 희*, 김 종 현*

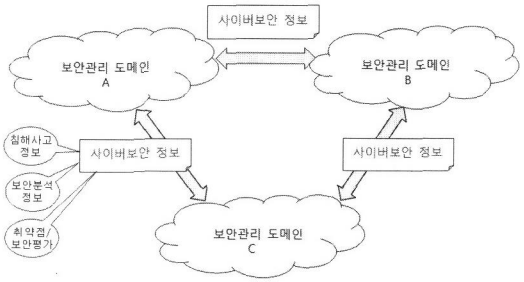
요 약

사이버보안 위협의 양상이 점차 세계화되고 피해의 규모가 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 사이버보안 정보공유 기술이 등장하였다. 본 고에서는 사이버보안 정보교환 기술의 개발 동향에 대해 간단히 소개하고, 국제표준화단체인 ITU-T SG17을 중심으로 사이버보안 정보 교환 기술에 대한 국제 표준화 동향을 살펴본다.

Ⅰ. 서 론

최근 사이버보안 공격은 사용 기법과 파괴력 관점에서 빠른 속도로 진화하고 있다[1-2]. 정형화된 공격 툴을 이용하여 공격하는 원시형태의 공격기법에서 해킹과 바이러스 기술을 통합하여 자동화된 대규모 공격을 수행하는 단계를 거쳐 이제는 사회공학적 기법을 사용하여 자기보호기능을 제공하는 봇(BOT)형태의 공격코드를 은닉하고 단시간에 대량으로 유포할 수 있는 수준까지 이르렀다. 또한 APT (Advanced Persistent Threats: 지능적지속가능위협) 등 한층 더 정교해진 공격이 등장하면서, 피해 범위도 개별 서버나 네트워크 등의 통신 인프라에서 전기, 철강, 원자력 등 산업기반 시설을 마비시킬 수 있을 정도로 확대되고 있다.

사이버 공격을 탐지하고 방어하기 위한 가장 전통적인 연구는 사이버보안 공격 탐지 및 대응 성능을 높이려는 연구였다. 그러나 사이버공격 및 위협이 복합적이고 다양한 형태로 변형되거나 새로 등장하는 현 추세에서는 지능화되고 고도화된 사이버 공격위협을 효과적으로 방어하기 어렵다. 또한 사이버보안 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 사이버보안 정보교환 기술이 등장하였다.



〔그림 1〕 사이버보안 정보 교환기술

사이버보안 정보교환 기술이란 사이버보안정보를 보유하거나 요청하는 조직, 사람, 디바이스, 프로세스들이 사이버환경과 자산을 사이버 공격으로부터 사전에 보호하고 긴급 대응하기 위한 사이버보안 정보를 서로 교환함으로써 협력을 통한 사이버공격 방어를 가능하게 하는 것을 목적으로 하는 기술이다[3]. 여기서 사이버보안 정보란 위협, 취약점, 침해사고, 보안평가, 공격탐지, 공격복구, 공격대응, 보안로그 등의 보안 정보를 의미한다.

본 고에서는 미국, 일본, 유럽, 한국을 중심으로 사이버보안 정보교환 기술의 개발 동향에 대해 소개하고, 국제표준화단체인 ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)

본 연구(2011/10914-06002, 전역적 협력기반의 통합보안제어 시스템 개발)는 방송통신위원회 정보보호 원천기술개발 사업의 일환으로 수행되었음.

* 한국전자통신연구원 사이버융합보안연구단({fogone, dhseo, jhk}@etri.re.kr)

SG17을 중심으로 사이버보안 정보 교환 기술에 대한 국제 표준화 동향을 살펴본다.

Ⅱ. 사이버보안 정보 교환 기술의 개발 동향

본 절에서는 사이버보안 정보 교환 기술의 개발동향을 소개한다.

2.1 미국

사이버보안 정보 교환기술에 대한 연구는 미국에서 가장 먼저 시작되었다. 미국에서 개발한 기술로서 CSISP(Cyber Security Information Sharing Project) 프로젝트[4]와 PS2 (Privacy- Sensitive Sharing) 프로젝트[5], 그리고 SCAP (Security Content Automation Protocol) 프로토콜[6][7]을 살펴본다. 먼저, CSISP 프로젝트는 2003년도에 미국의 CERT-CC(Computer Emergency Response Team - coordination center)가 주관하고 CMU 등의 대학교가 참여하였으며 정부와 민간부문간 사이버보안정보의 실시간 교환을 제공할 목적으로 수행되었다. 그 이전의 사이버보안 정보 교환은 전화 또는 이메일 등의 오프라인 형태의 방법이 사용되었다. CSISP 프로젝트를 통해 ArcSight사에서 개발한 보안위험 관리 소프트웨어는 보안 디바이스로부터 데이터를 수집하여 CERT/CC로 전달하여 보안을 분석할 수 있는 기능을 제공한다.

다음으로 PS2는 개인 프라이버시 문제뿐만 아니라 보안과 법률문제도 함께 고려하여 안전하게 정보를 공유할 수 있는 프레임워크 개발을 목적으로 하고 있으며, 샌디애고 슈퍼컴 센터에 기반을 둔 CAIDA (The Cooperative Association for Internet Data Analysis) 협회가 수행하고 있다. 사이버보안정보에 포함된 개인을 식별할 수 있는 민감정보(예, IP 주소)는 부주의나 사고로 인하여 외부로 노출될 위험이 있으며, 민감정보가 아닌 일반 정보인 경우에도 다양한 정보를 종합하고 분석하여 개인정보를 추출할 수 있는 정보남용 위험이 있음을 강조하고, 그 위험을 방지할 수 있는 다양한 정책 컴포넌트를 개발하고 있다.

마지막으로, SCAP 프로토콜은 NIST (National Institute of Standards and Technology)와 MITRE사가 중심이 되어 미연방정부의 데스크톱 시스템에 대한 표준화된 보안구성 지침을 제공한다. SCAP 프로토콜의 주요 목적은 시스템 보안 관리를 표준화시키고, 보안제품의 상호운용성을 보장하고, 보안정보에 관한 표준화 사용을 촉진하는 것이다. SCAP는 6개의 표준문서를 개발하였다. 즉, 시스템의 보안설정 체크리스트 및 벤치마크에 대한 데이터 모델과 형식을 정의한 XCCDF (eXtensible Checklist Configuration Description Format), 시스템에 대한 설정 표현 및 취약점 평가 검사를 위한 데이터 모델과 형식을 정의한 OVAL (Open Vulnerability Assessment Language), 알려진 취약점에 대한 공통 식별 체계를 제공하는 CVE (Common Vulnerabilities and Exposures), 시스템 구성에 대한 공통 식별 체계를 제공하는 CCE (Common Configuration Enumeration), 소프트웨어 시스템과 하드웨어 장비에 대한 공통 플랫폼 식별 체계를 제공하는 CPE (Common Platform Enumeration), 그리고 취약점 점수화를 제공하는 공통 취약점 평가 체계를 정의한 CVSS (Common Vulnerability Scoring System)이다.

2.2 일본

일본에서 개발한 사이버보안 정보 교환기술로서 NICTER (Network Incident Analysis Center for Tactical Emergency Response)[8]과 JVN (Japan Vulnerability Notes) 시스템[6][7]을 소개한다. NICTER 시스템은 2010년도에 NICT (National institute of Information and Communications Technology)에서 개발하였으며, 국가차원의 대규모 네트워크를 모니터링하여 실시간으로 네트워크 보안 사고를 탐지하고 분석하는 것을 목적으로 한다. NICTER 시스템은 ISP 및 캠퍼스 네트워크, 그리고 허니팟으로부터 트래픽, 보안로그, 악성코드 등 보안정보를 실시간으로 수집하여 네트워크 사이버 공격을 실시간을 탐지하고 이를 유발하는 악성코드를 연관성 분석을 통해 자동적으로 식별하는 기능을 제공한다.

JVN 은 미국에서 개발한 SCAP 프로토콜을 기반으로 소프트웨어 취약점 정보 체계를 구축하고, 이에 대한 보안정보공유 서비스를 제공하는 시스템이다. 보안 취약점 및 대응정보는 정보보안 조기경보 파트너십으로 채결된 밴더, CERT/CC, 일본 소프트웨어 개발자로부터 수집되고 있다.

2.3 유럽

유럽에서 개발하는 사이버보안 정보 교환기술로서 NEISAS (National and European Information Sharing and Alerting System) 시스템[9]과 MS3i (Messaging Standard for Sharing Security Information) 프레임워크[10]가 있다. 먼저, NEISAS 시스템은 영국을 중심으로 이탈리아, 네덜란드가 참여하여 2011년도에 개발이 완료되었다. NEISAS의 목적은 국가 및 유럽규모에서 중요 인프라에 관련된 정보 및 경보를 공유할 수 있는 플랫폼을 개발하는 것이다. NEISAS에서 공유하는 정보는 발생하였거나 발생가능성이 있는 공격 및 취약점, 실행방법론, 사고대응 및 관련 표준들, 위협과 취약점 분석결과, 새로운 기술들, 자산 보호 및 위험 관리에 대한 정보를 포함한다. NEISAS는 조직뿐만 아니라 개인간의 정보공유도 지원하며, 정보공유 그룹 내에서 신뢰 조정자 역할을 하는 Trustmaster를 중심으로 일대일, 일대다, 다대다간 정보공유 등 신뢰를 기반으로 하는 다양한 정보공유 방법을 제공한다.

MS3i 프레임워크는 EC (European Commission)로부터 자금 지원을 받아 시맨택(Symentec)에서 개발한 보안정보공유를 위한 메시지 프레임워크이다. MS3i는 새로운 표준을 제정하는 것이 아니라, 기존에 개발된 표준을 재사용한다. MS3i는 메시지 트랜스포트 표준, 메시지 포맷 표준, 메시지 보호 표준, 메시지 콘텐츠 표준 등 네 개의 계층을 정의하고 있다. 메시지 트랜스포트 표준은 TCP/IP 등 메시지 전송과 관련된 표준들로, 메시지 포맷 표준은 XML, ASN.1 등 메시지 인코딩/디코딩에 관련된 표준들로, 메시지 보호 표준은 인증과 암호화에 관련된 표준들로, 그리고 메시지 콘텐츠 표준은 공유되는 정보의 데이터 모델과 형식에 관련된 표준들로 구성된다.

2.4 한국

ETRI에서는 COSMOS (COoperative Security MOnitoring System)라는 전역적 협력기반의 통합 보안제어 시스템을 개발하고 있다[11]. COSMOS 시스템은 인터넷 서비스 제공자간의 보안정보를 표준화된 방법으로 공유할 수 있는 프레임워크를 기반으로 하여 DNS 질의의 수집과 분석을 통해 사이버 위협을 예측하고, 파일공유 사이트의 로그 모니터링을 통해 악성코드를 유포한 공격자를 추적할 수 있는 기능을 제공한다.

Ⅲ. ITU-T 표준화 기구의 표준화 동향

본 절에서는 현재 사이버보안 정보교환에 관한 표준화를 가장 활발하게 추진하고 있는 ITU-T 표준화기구에서 개발하고 있는 사이버보안 정보교환기술에 관한 표준화 동향을 살펴본다.

3.1 배경

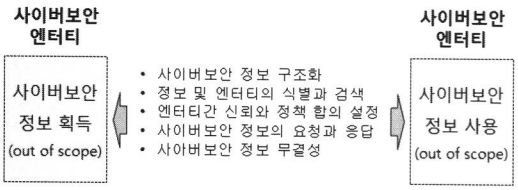
현재 ITU-T 표준화기구에서 사이버공간에서 발생하는 침해사고 및 취약점 등에 대한 대응방안 및 보안정보 공유 등에 대한 보안 표준 개발은 Q4/SG17에서 담당하고 있다. 현재 Q4/SG17에서 중점적으로 다루고 있는 표준화 대상은 사이버보안 엔터티(entity)간의 사이버보안정보의 교환을 지원하는 프레임워크이다. 일명 CYBEX (CYBersecurity information EXchange)[3][6]라 불리는 이 표준화 작업은 2008년 독일 하이델베르크에서 개최된 인터림 회의에서 현재 Q.4/17의 라포처인 Anthony M. Rutkowski에 의해 제안되었다.

CYBEX는 미국의 정보보호 관련 연구 개발 기관인 MITRE 사의 정보보호 관련 시스템 및 기술들과 NIST의 정보보호 표준들을 사이버보안 정보 교환 구현을 위한 기본 표준화 항목으로 채택하였다. CYBEX 표준화 작업은 미국이 주도하고, 일본, 영국, 캐나다, 한국 등 주요국이 적극적으로 참여하여 빠른 속도로 진행되고 있다. 현재 기본 프레임워크로 X.1500 표준이 제정된 상태이며, 2013년까지 CYBEX와 관련된 문서의 표준을 개발하는 것을 목표로 하고 있다.

3.2 사이버보안 정보 교환 프레임워크

CYBEX 모델은 [그림 2]에 도시되어 있다. CYBEX 모델은 사이버보안 엔터티들간에 사이버보안 정보 교환을 표준화된 방법으로 제공하는 것을 목적으로 한다. 여기서 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 해당

된다. 사이버보안 정보 교환은 공공 도메인뿐만 아니라 사전에 정책에 동의한 신뢰된 커뮤니티 간에도 발생할 수 있다. 엔터티간에 교환되는 사이버보안 정보는 사이버 환경과 조직 그리고 사용자 자산을 보호하기 위해 사용될 수 있는 위협, 취약점, 침해, 대응방안, 툴, 정책, 가이드라인, 훈련, 기술 등의 정보를 포함한다. CYBEX 모델은 사이버보안정보를 어떻게 획득하는지 및 어떻게 사용할지에 대해서는 정의하고 있지 않는다.



〔그림 2〕 CYBEX 모델

CYBEX 모델은 다음과 같은 다섯 가지 기능과 이를 지원하기 위한 여섯 가지 기술로 구성된다.

- 정보교환을 위한 사이버보안정보 구조화 기능: 통신하는 사이버보안 엔터티들간의 상호운용성을 제공하기 위하여 교환되는 정보가 동일 의미를 갖도록 공통 형식으로 사이버보안정보를 구조화하는 기능. 이를 지원하기 위하여 CYBEX에서는 취약성 및 상태 평가 정보 교환 기술과, 이벤트 및 사고, 휴리스틱 정보 교환 기술 표준을 개발함.
- 사이버보안 정보 및 엔터티의 식별과 검색 기능: 사이버보안 정보 및 정보교환에 참여하는 엔터티를 식별하고 탐색하는 기능. 이를 위해 CYBEX에서는 식별, 발견, 검색 기술 표준을 개발함.
- 사이버보안 엔터티간 신뢰와 정보교환정책 협정 설정 기능: 교환되는 정보와 관련된 조건이 있는 사이버보안 엔터티들간의 보안정보 공유를 지원하는 기능. 이를 지원하기 위하여 CYBEX에서는 정보교환정책 기술 표준을 개발함.
- 사이버보안 정보의 요청과 응답 기능: 다양한 사이버보안 정보 교환 상황에서 사용될 수 있는 사이버보안 정보의 교환기능. 이를 위해 CYBEX에서는 정보교환 프로토콜 기술 표준을 개발함.
- 사이버보안 정보 교환시 무결성 보장 기능: 사이버보안 엔터티간에 교환되는 사이버보안 정보의 무결성을 보장하는 기능. 이를 지원하기 위하여 CYBEX에서는 아이디 보증 기술 표준을 개발함.

3.3 사이버보안 정보 교환기술의 표준화 상태

CYBEX에서 정의하고 있는 여섯 가지 기술 및 각 기술에 대한 현재 표준화 상태는 다음과 같다.

- 취약성 및 상태 평가 정보 교환 기술: 서로 다른 사이버보안 엔터티간에 구조화된 방법으로 시스템과 소프트웨어의 취약성 정보와 상태 평가 정보를 교환하기 위한 기술이며, 이와 관련된 표준화 상태는 [표 1]에 있음.
- 이벤트 및 사고, 휴리스틱 정보 교환 기술: 수집된 이벤트, 보안사고, 휴리스틱 정보를 서로 다른 사이

〔표 1〕 취약성 및 상태 평가 정보 교환 기술

기술명	주요내용	표준
Common vulnerabilities and exposures (CVE)	툴, 저장소, 서비스간에 정보보안 취약정보를 공유할 수 있도록 알려진 취약점을 식별하고 교환하기 위한 공통 번호체계	완료 (X. 1520)
Common vulnerability scoring system (CVSS)	ICT 취약점의 영향과 특징을 전달하기 위한 취약점 점수화를 제공하는 공통 취약점 평가체계	완료 (X. 1521)
Common weakness enumeration (CWE)	소프트웨어 취약점을 식별하고 교환하기 위한 공통 번호체계	완료 (X. 1524)
Common weakness scoring system (CWSS)	소프트웨어 취약점의 영향과 특징을 전달하기 위한 취약점 점수화를 제공하는 공통 취약점 평가체계	진행중 (2012. 09 예정)
Open vulnerability and assessment language (OVAL)	시스템의 구성정보를 표현하고, 시스템의 취약성, 구성, 패치상태 등을 분석하여 취약성을 평가하기 위한 데이터 모델과 형식	진행중 (2012. 09 예정)
eXtensible configuration checklist description format (XCCDF)	시스템의 보안 구성 규칙으로 구성되는 체크리스트, 벤치마크 등의 정보를 표현하기 위한 XML 기반의 데이터 모델과 형식	완료 (X. 1527)
Common platform enumeration (CPE)	소프트웨어 시스템과 하드웨어 장비를 표준화된 방법으로 식별하기 위한 공통 플랫폼 식별 체계	완료 (X. 1528)
Common configuration enumeration (CCE)	다양한 정보 소스와 툴상에서 구성 데이터간의 연관성 식별이 용이하도록 시스템 구성에 대한 공통 식별체계	진행중 (2012. 09 예정)
Assessment results format (ARF)	평가 툴 및 자산 관리 제품간에 디바이스의 평가 결과를 교환하기 위한 데이터 모델과 형식	진행중

버보안 엔터티간에 구조화된 방법으로 교환하기 위한 기술이며, 이에 대한 표준화 상태는 [표 2]에 있음.

- 식별, 발견, 검색 기술: 사이버보안 조직을 식별하고 사이버보안 정보를 발견하고 검색하기 위한 기술이며, 이와 관련된 표준화 상태는 [표 3]에 있음.
- 정보교환정책 기술: 사이버보안 엔터티들간 정책정보의 교환을 제공하는 기술이며, 이와 관련된 표준화 상태는 [표 4]에 있음.
- 정보교환 프로토콜 기술 : 사이버보안 엔터티들간 사이버보안 정보를 교환할 때 사용되는 프로토콜이며, 이와 관련된 표준화 상태는 [표 5]에 있음.
- 아이디 보증 기술: 사이버보안정보를 교환하는 엔터티의 아이디 보증기술이며, 이와 관련된 표준화 상태는 [표 6]에 나타나 있음.

〔표 2〕 이벤트 및 사고, 휴리스틱 정보 교환 기술

기술명	주요내용	표준
Common event expression (CEE)	컴퓨터 이벤트를 표준화된 방법으로 표현, 로깅, 교환하기 위한 로그 데이터 모델 및 형식	진행중 (2012. 09)
Incident object description exchange format (IODEF)	컴퓨터 보안 사고에 대한 정보를 CIRT간에 교환하기 위한 표준화된 데이터 형식	완료 (X.1541)
Phishing, fraud, and misuse format	피싱, 사기, 악용 등의 사고 정보를 보고하기 위한 IODEF 기반의 표준화된 데이터 형식	없음
Common attack pattern enumeration and classification (CAPEC)	사이버공격 패턴의 식별과 기술 그리고 분류에 대한 표준화된 체계	진행중 (2012. 09 예정)
Malware attribution Enumeration and characterization format	맬웨어에 대한 공통 속성 및 행위 기술 체계와 표준 형식 정의	없음

〔표 3〕 식별, 발견, 검색 기술

기술명	주요내용	표준
Traffic light protocol (TLP)	정보제공자가 명시한 정책에 따라서 민감정보의 유포 범위를 한정하는 기능을 제공하는 정보공유 프로토콜	없음

〔표 4〕 정보교환정책 기술

기술명	주요내용	표준
Discovery mechanisms in the exchange of cybersecurity information	사이버보안정보 제공자를 식별하고 탐색하기 위한 메커니즘	완료 (X. 1570)
Guidelines for administering the OID arc for CYBEX	사이버보안정보, 조직, 정책에 대한 공통의 전역적 사이버보안 식별자의 이름공간 정의	완료 (X. 1500.1)
Cybersecurity information query language	CIRT들간에 교환되는 컴퓨터 보안 사고 정보를 요청하기 위한 사이버보안 정보 질의 정보 모델	진행중

〔표 5〕 정보교환 프로토콜 기술

기술명	주요내용	표준
Trusted platforms	안전한 사이버보안정보교환을 위해 강력한 사용자인증과 머신수준에서 신뢰성을 제공하는 신뢰플랫폼 모듈 (TPM)	없음
Trusted network connect	네트워크 접근 제어 표준	없음
Entity authentication assurance	엔터티 식별자 및 관련 식별정보의 보증 프레임워크	없음
Extended validation certificate framework	확장된 검증 인증서(EVC: Extended validation certificate)를 발급하고 유지하기 위한 프레임워크	없음
Policy requirements for certification authorities issuing public key certificates	공개키기반의 인증서를 발급하는 인증국(CA: certification authority)의 정책 요구사항	없음

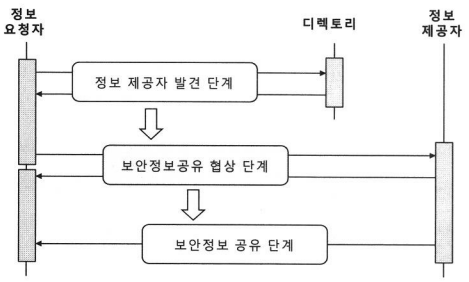
〔표 6〕 아이디 보증 기술

기술명	주요내용	표준
Real-time internetwork defense (RID)	컴퓨터보안사고의 요청/교환/대응을 위한 IODEF 프로토콜기반의 표준 메시지 및 교환 형식	완료 (X.1580)
Transport of real-time Internetwork defense (RID) messages	TLS 상에서 HTTP 프로토콜 기반의 RID 프로토콜 메시지 전송 메커니즘	완료 (X.1581)
Blocks extensible exchange protocol (BEEP) profile for CYBEX	CYBEX를 위한 BEEP(Blocks extensible exchange protocol) 프로토콜 프로파일	진행중 (2012. 09 예정)
Simple object access protocol (SOAP) for CYBEX	분산환경에서 보안정보교환을 위한 경량급 SOAP(Simple object access protocol) 프로토콜	없음

3.4 사이버보안 정보 교환 시나리오

사이버보안 정보를 공유하기 위해서는 기본적으로 정보 요청자, 정보 제공자, 그리고 디렉토리 등 세 개의 사이버보안 엔티티가 있어야 한다. 정보 요청자는 정보 제공자에게 원하는 정보를 요청하고, 정보 제공자는 요구된 정보를 제공한다. 디렉토리는 정보 제공자의 정보에 대한 정보를 등록하고 정보 요청자가 원하는 정보 제공자를 찾는 것을 도와준다.

정보 요청자와 정보 제공자, 그리고 디렉토리간의 전형적인 사이버보안 정보 공유 절차는 [그림 3]에 도시된 바와 같은 3단계 구성된다. 즉, 정보 제공자 발견 단계, 보안정보 공유 협상 단계, 그리고 보안정보 공유 단계이다. 첫 번째는 발견 단계로서 정보 요청자는 디렉토리에게 요청하여 자신이 원하는 정보를 제공할 수 있는 정보 제공자 리스트를 발견하는 단계이다. 두 번째는 정보 요청자가 발견 단계를 통해 발견된 정보 제공자와 정보 공유 서비스 수준을 어떻게 할지 협상하는 단계이다. 마지막은 협상 단계를 통해 협상된 정보 공유 서비스 수준에 따라서 사이버보안 정보를 공유하는 단계이다.



〔그림 3〕 사이버보안정보 교환 절차

Ⅳ. 다른 표준화 기구의 표준화 동향

본 절에서는 IETF와 ISO 표준화기구의 사이버보안 정보교환기술에 관한 표준화 동향을 살펴본다.

4.1 IETF 표준화 기구

IETF에서는 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. ID WG는 보안 시스템들 간의 정보 공유를 위한 데이터 포맷과 교환 절차에 대한 표준을 개발하고, INCH WG에서는 보안관련 조직 간의 협력 통합 보안 제어를 위한 교환 데이터의 데이터 형식에 대한 표준을 개발하였다. 현재 두 WG은 표준 개발을 완료하여 활동이 종료된 상태이다.

IETF에서는 사이버보안 정보 공유를 위한 프로토콜로서 [표 7]에서 보여진 IDMEF[12], IODEF[13], 그리고 RID[14] 프로토콜에 대한 표준을 개발하였다. IDMEF에서는 IDS 및 IPS와 같은 공격 탐지 시스템이 탐지한 공격 이벤트에 대한 경보(alert)를 보안관리 시스템에게 보고하기 위한 데이터 포맷 및 데이터 교환 절차를 정의하고 있다. IDMEF는 경보를 생성한 분석기(analyzer) 식별정보, 경보가 생성된 시간, 경보가 탐지된 시간, 분석기의 현재 시간, 공격 시스템과 타겟(목적지) 시스템에 대한 정보, 공격정보, 공격 위험도와 경보에 대응하기 위해 실행된 액션 등의 정보를 표현할 수 있다. IODEF 프로토콜은 보안침해사고 대응팀 상호간에 컴퓨터 보안 사고에 대한 정보를 공유하기 위한 데이터 표현을 정의하는 것을 목적으로 한다. IODEF 프로토콜은 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 표현할 수 있다. 마지막으로 RID 프로토콜은 IDMEF 및 IODEF 프로토콜을 수용하며, 침해사고 처리를 위한 모든 일련의 과

〔표 7〕 IETF에서 개발된 표준기술

기술명	주요내용	표준
IDMEF(Intrusion Detection Message Exchange Format)	공격 탐지시스템과 관리시스템 간 경보(alert) 전달을 위한 데이터 포맷 및 교환 절차	2007, RFC-4765 (I)
IODEF (Incident Object Description Exchange Format)	컴퓨터 보안 사고 정보의 공유를 위한 데이터 표현	2007, RFC-5070 (PS)
RID (Real-time Inter-network Defense)	공격 탐지/추적/식별/대응 등 침해사고 처리와 관련된 정보공유를 위한 데이터 형식 및 절차	2010, RFC-6045 (I)

정들을 용이하게 지원하기 위해 제안되었다. RID 프로토콜은 사이버보안 정보 공유 시스템간의 공격 탐지 정보, 공격시스템 추적 및 식별, 그리고 공격 대응 메커니즘 등 침해사고 처리와 관련된 데이터의 공유를 목적으로 한다.

4.2 ISO/IEC 표준화 기구

ISO/IEC JTC 1(International Standard Organization/ International Electrotechnical Committee Joint Technical Committee 1 Sub Committee 27, IT 보안 기술)에서는 사이버보안 및 보안사고 관리를 위한 표준을 개발하고 있다. ISO/IEC에서는 [표 8]에 나타난 바와 같이 2.3절에서 소개한 NEISAS와 MS3i를 기반으로 하여 27010 표준을 개발하고 있다.

〔표 8〕 ISO/IEC에서 개발된 표준기술

기술명	주요내용	표준
ISO/IEC 27010 Information security management for inter-sector and inter-organisational communications	중요 인프라를 보호하기 위해 도메인내에서 뿐만 아니라 도메인간에서의 보안정보공유를 지원하기 위한 가이드라인	2012, Final DIS

V. 결 론

사이버보안 정보 교환은 정부, 금융, ISP, 기업 등 공공의 인터넷 환경에서 다양한 사이버보안 정보들을 상호 공유하고 관리하여 사이버 보안 위협들에 대해 빠르게 대응하기 위한 체계를 제공할 수 있기 때문에 보안정보 공유에 대한 필요성은 점점 더 증가할 것으로 예상된다. 따라서 서로 다른 독립적인 도메인들이 유기적인 관계에서 보안정보를 효과적으로 교환할 수 있도록 표준화된 정보공유 프레임워크 및 세부 기술들을 개발하는 것이 매우 시급한 상황이다.

본 고에서는 사이버보안 정보교환 기술의 개발 동향에 대해 소개하고, ITU-T 표준화 기구를 중심으로 사이버보안 정보 교환 기술에 대한 표준화 동향을 살펴보았다. 사이버보안 정보 교환기술에 대한 프레임워크 등의 기반 연구는 미국이 주도적인 역할을 하고 있으며, 한국을 비롯한 일본 및 유럽에서는 네트워크 보안 분석과 도메인간 민감정보 공유 등 사이버보안 정보 교환을 기반으로 하는 응용 기술 개발에 중점을 두고 있는 상황이다. 표준화 동향을 살펴보면, IETF 단체에서는 사이버보안 정보 교환 프로토콜 기술에 관심이 있으며, ISO/IEC에서는 도메인간 정책기반의 정보 교환 기술에 중점은 둔 반면에, ITU-T 표준화 기구는 사이버보안 정보 교환 프레임워크와 관련 기술들을 개발하기 위하여 기존의 표준을 수용하고 새로운 표준을 제정하는 등 가장 활발하게 표준화를 추진하고 있다.

사이버보안정보 교환기술의 가장 중요한 성공 요소 중의 하나가 바로 표준화이며, 아직도 많은 기술들에 대한 표준이 요구되는 만큼 표준화에 적극 참여하고 보유기술을 반영하는 등 주도적인 역할이 필요할 때라고 사료된다.

참고문헌

[1] 남기효, 김윤홍, 권환우, "최신 정보보호기술 동향: APT 및 그 대응," *ITFIND 주간기술동향* 1513호, Sep. 2011.

[2] 시만텍, *인터넷 보안 위협 보고서: 2010년 동향*, 제16호, https://scm.symantec.com/resources/21182883_KR_REPORT_ISTR_Main-Report_04-11.pdf, April 2011.

[3] Anthony Rutkowski, Youki Kadobayashi, Inette Furey, Damir Rajnovic, Robert Martin, Takeshi Takahashi, "CYBEX - The Cybersecurity Information Exchange Framework (X.1500)," *ACM SIGCOMM Computer Communication Review*, 40(5), pp. 59-64, Oct. 2010.

[4] 정일안, 오진태, 장종수, "보안 정보 공유 기술 및 표준화 동향," *전자통신동향분석*, 23(4), pp. 30-38, Aug. 2008.

[5] E. Kenneally and K. Claffy, "An Internet Data Sharing Framework For Balancing Privacy and Utility," *First International Forum on the Application and Management of Personal Electronic Information*, pp. 1-6, Oct. 2009.

[6] ITU-T, "Overview of cybersecurity information exchange (CYBEX)," *ITU-T Recommendation* X.1500, April 2011.

[7] 김종진, 조성제, "국가 DB기반의 국내외 보안취약점 관리체계 분석," *Internet and Information Security*, 1(2), pp. 130-147, Nov. 2010.

[8] Koji Nakao, "Latest research activity on correlation analysis based on Darknet," The Internet Security Days 2011, *9th German Anti Spam Summit*, Sep. 2011.

[9] Sandro Bologna, "Public-private cooperation: the NEISAS approach," *Bucharest CIP Conference*, http://www.arts.org.ro/pdf/cipic2011/27_10_2011_2.1_S.Bologna.pdf, Oct. 2011.

[10] Messaging Standard for Sharing Security Information (MS3i) Project, "Messaging standards for computer network defence warnings and alerts," *JLS/2007/ EPCIP/007 - Project Report*, June 2009.

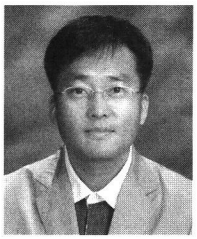
[11] 안개일, 서대희, 임선희, 김종현, 서동일, 조현숙, "독립적인 보안관리 도메인간 효과적인 사이버보안정보 교환 방법의 설계 및 구현," *한국통신학회 논문지*, 36(12), pp. 1433-1757, Dec. 2011.

[12] H. Debar, D. Curry and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)", *IETF*, RFC 4765, March 2007.

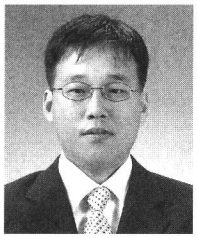
[13] R. Danyliw, J. Meijer, Y. Demchenko, "The Incident Object Description Exchange Format," *IETF*, RFC 5070, Dec. 2007.

[14] K. M. Moriarty, "Real-time Inter-network Defense," *IETF*, RFC 6045, Nov. 2010.

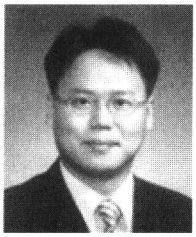
〈著者紹介〉



안 개 일 (Gae-il An)
정회원
1993년 2월: 충남대학교 컴퓨터공학과 졸업
1995년 2월: 충남대학교 컴퓨터공학과 석사
2001년 8월: 충남대학교 컴퓨터공학과 박사
2006년 7월~2007년 6월: 미국 Security University 포닥연구원
2001년 8월~현재: 한국전자통신연구원 책임연구원
<관심분야> 정보보호, 네트워크 보안, 모바일 보안, 네트워크 시뮬레이션



서 대 희 (Dae-hee Seo)
정회원
2003년 2월: 순천향대학교 전산학과 석사
2006년 2월: 순천향대학교 전산학과 박사
2006년 4월~2007년 4월: Howard University post-doc
2008년 7월~2009년 9월: 이화여자대학교 컴퓨터 정보통신공학부 연구교수
2009년 10월~현재: 한국전자통신연구원 선임연구원
<관심분야> 정보보호, 네트워크 보안, 보안성 평가



김 종 현 (Jong-Hyun Kim)
정회원
2000년: 오클라호마주립대 컴퓨터과학과 공학석사
2005년: 오클라호마주립대 컴퓨터과학과 공학박사
2005년~현재: 한국전자통신연구원 선임연구원
2000년~2001년: 삼성SDS 시스템 컨설턴트
1995년~1997년: 삼성전자 연구원
<관심분야> 정보보호, 사이버보안, 역추적기술