# STIX/TAXII 기반의 사이버위협 정보 공유 표준화 동향

**김종현** _ TTA 사이버보안 프로젝트그룹(PG 503) 부의장,
ETRI 정보보호연구본부 책임연구원

## 1. 머리말

사이버위협의 패러다임이 빠르게 변화하고 있기 때문에, 이러한 변화에 적절하고 신속하게 대응하기는 쉽지 않으며, 이를 위한 방법들에 대한 요구가 절실한 실정이다. 이러한 대응 방법의 일환으로 사이버위협 정보의 공유가 필수 요소가 되었으며, 또한 이를 위한 정보 교환 체계에 대한 표준화가 절실히 요구된다.

이에 반해 현재 국내 사이버위협 정보 공유체계는 협의체를 중심으로 한 초기 정보공유의 형태를 띠고 있다. 기관마다 사이버위협에 대한 표현 체계, 탐지 시스템, 공유 체계, 대응 체계가 불일치하여 사이버위협정보에 대한 일관성이 없고, 또한 사이버위협 정보 교환을 위한 표준 지표가 표준화되어 있지 않다.

본고에서는 ITU-T 및 OASIS CTI(Cyber Threat Intelligence) 등의 국외 사이버위협 정보 공유 체계 등에 대하여 살펴본다. 그리고 사이버위협 정보를 서술하여 일관된 방법으로 공유, 저장 및 분석할 수 있는 구조화된 체계와 신뢰할 수 있는 사이버위협 정보 교환 방법으로 대두되고 있는 STIX/TAXII 관련 국내외 표준화 동향을 다루고자 한다.

## 2. 표준화 추진 현황

### 2.1 사이버위협 정보의 개념

일반적으로 사이버 정보 공유 기술은 사이버 보안 정보를 보유하거나 요청하는 조직, 사람, 디바이스, 프로세스들이 사이버 공격으로부터 사이버 환경과 자산을 사전에 보호하고 긴급 대응하기 위한 사이버 보안 정보를 서로 교환함으로써 협력을 통한 사이버 공격 방어를 목적으로 한다. 여기서 사이버 보안 정보란 위협, 취약점, 침해 사고, 보안 평가, 공격 탐지, 공격 복구, 공격 대응, 보안 로그 등의 보안과 관련된 정보를 의미한다.

사이버 위협(Cyberthreat)이란 사이버 상에서의 악의적인 공격 등을 통해 발생할 수 있는 잠재적인 위협을 뜻하며 개인이나 조직의 자산에 심각한 손실을 발생시킬 수도 있다. 사이버위협 정보는 대응기관이 위협을 탐지하거나 방어하는 데 활용할 수 있는 사이버 위협에 대한 구체적인 정보를 의미한다. 이에 대한 정의는 다양할 수 있는데 미국의 법령, 미국의 표준 기관 및 한국의 법령에서 설명하는 사이버위협 정보 정의 및 분류를 〈표 1〉에 나타내었다[1].

〈표 1〉 기관별 사이버위협 정보 정의 및 분류[1]

| 기관 | 구분 | 내용 |
|---|---|---|
| **미국** 〈사이버안보정보공유법(CISA)〉 | 사이버위협지표 (Cyber Threat Indicator) | • 사이버위협 또는 취약점 분석 등 악의적인 목적의 정보수집 행위<br>• 보안통제 기능을 무력화하거나 보안 취약점을 악용한 공격 행위<br>• 보안통제 기능의 무력화 또는 보안취약점을 악용한 공격을 통해 이용자가 정보시스템 또는 저장된 정보에 적법한 접근을 가능하게 하는 방법<br>• 보안 취약점<br>• 악의적인 목적의 사이버 C&C(Command & Control)<br>• 사이버위협으로 인한 정보유출 등 침해사고로 인해 발생 또는 발생 가능한 위해요소<br>• 기타 사이버 보안 위협을 유발하는 요인 및 속성<br>• 상기에 명시된 사항들의 조합된 정보 등 |
| | 방어적 조치 (Defensive Measure) | • 알려진 또는 의심스러운 사이버안보 위협 및 보안취약점을 감지(Detect), 방지(Prevent), 완화(Mitigate)하기 위하여, 정보시스템에 적용 가능한 행위(Action), 장치(Device), 절차(Procedure), 표시(Signature), 기술(Technique), 기타 조치사항 또는 정보 시스템 상 저장·처리·전송되는 정보 |
| **NIST** 〈사이버위협 정보 공유 가이드 (Guide to Cyber Threat Information Sharing)〉 | 지표(Indicators) | 공격이 임박했거나 이미 발생한 사실에 대한 기술 산출물 또는 관측값 |
| | TTP (전략/기술/절차) | 공격자의 성향, 사용 도구, 공격방법 및 절차 등을 보여주는 행위정보 |
| | 보안경보 (Security Alerts) | 취약점, 공격행위 등 보안이슈에 대한 기술사항 알림정보 |
| | 위협정보보고서 (Threat Intelligence Reports) | TTP, 행위자, 공격대상 시스템 및 정보유형 등을 포함한 통합 분석 및 해석이 이루어진 보고서로 의사결정 지원 |
| | 도구 설정(Tool Configuration) | 위협 정보를 자동 수집, 교환, 처리, 분석, 활용할 수 있도록 하기 위한 관련 도구 및 메커니즘의 설정방법 등 |
| **대한민국** 〈국가사이버안보법 제12조〉 | | • 사이버 공격 방법에 관한 정보<br>• 악성프로그램 및 이와 관련된 정보<br>• 정보통신망, 정보통신기기 및 소프트웨어의 보안상 취약점에 관한 정보<br>• 그 밖에 사이버 공격의 예방을 위한 정보 |

## 2.2 사이버위협 정보 공유 체계 및 표준 지표 동향

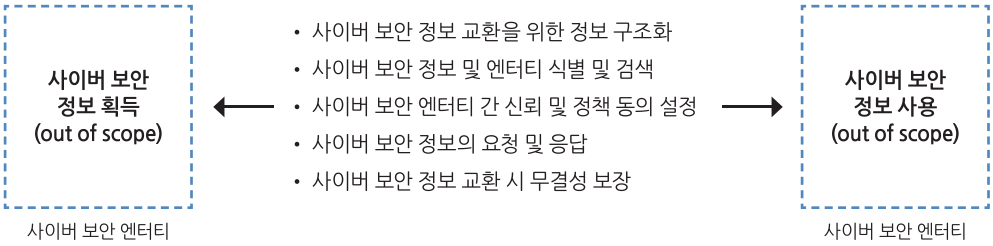
### 2.2.1 국외 사이버위협 정보공유 체계 동향

가. 미국

미국은 국토안보부와 국가정보국을 중심으로 사이버위협 정보공유 체계를 구축하여 운영 중이며 국토안보부는 연방 사이버안보 통신통합센터를 통해 주요 정부기관과 민간을 대상으로 사이버위협정보를 공유하는 창구 역할을 수행하고 있으며, 국가정보국은 정보기관을 중심으로 국가안보에 영향을 미칠 수 있는 국내·외 사이버위협 정보를 수집하여 공유함으로써 공공과 민간의 효과적인 대응을 지원하고 있다.

나. 일본

일본은 국가정보보안센터(National Information




**[그림 1] CYBEX 구성 모델[2]**

Security Center)를 중심으로 사이버위협 정보공유 체계를 구축하여 운영 중이며, 정부조직에 대한 정보공유는 정부보안 운영조정 팀(Goverment Security Operation Coordination Team)에서 정부부처 및 조직 간의 정보공유 업무를 수행하고 있으며, 사이버공격 관련 정보 수집·분석을 통해 즉각적인 대응책을 지원하고 있다.

민간분야에 대한 정보공유는 경제산업성(METI) 산하의 민간분야 정보보안 관련 전문기관인 IPA에서 사이버안보 정보공유체계인 J-CSIP(Initiative for Cyber Security Information Sharing Partnership of Japan)을 운영하고 있다.

다. 영국

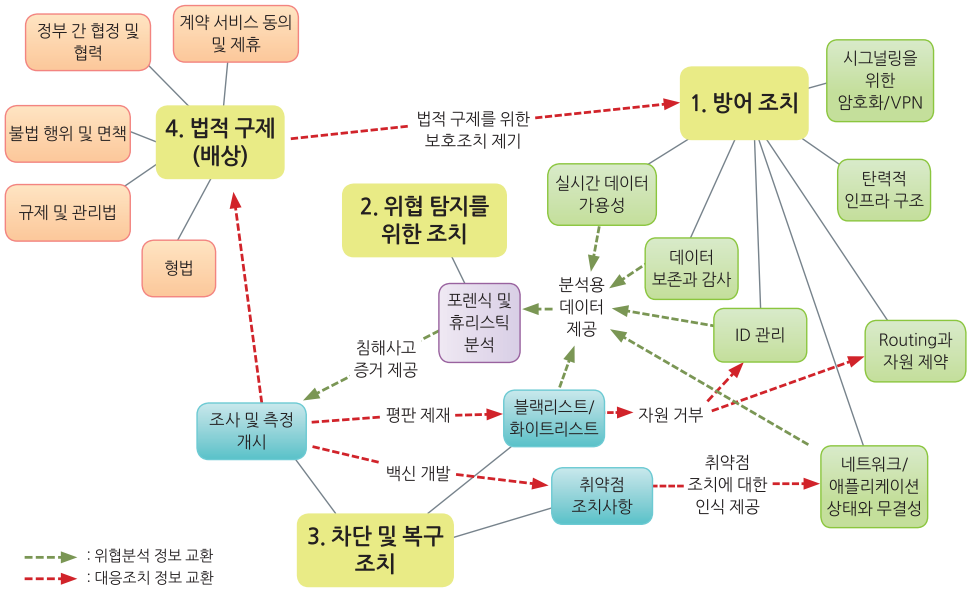
영국의 사이버위협 정보공유 체계는 CERT-UK에서 사이버위협 정보공유 프로그램을 운영하여 정부와 민간간의 정보공유를 주도하고 있다. 사이버위협 정보공유 프로그램은 사이버위협이 산업에 미치는 영향을 최소화하기 위하여 정부와 산업계가 상호 합의를 통해 설계되었다. 사이버위협 정보를 실시간으로 공유하고 공유된 정보에 대한 기밀성을 보장하며 관련 상황보고서를 주기적으로 발송하여 정보를 공유토록 하고 있다.

### 2.2.2 ITU-T CYBEX(CYBersecurity Information EXchange) 표준 동향

ITU-T에서 사이버 정보 교환에 대한 표준화 작업은 2008년 6월 독일 하이델베르크에서 개최된 SG 17 Q.6(현재 SG 17 Q.4) 사이버보안 연구 그룹의 인터림 회의를 통해서 시작되었으며, 2008년 9월 ITU-T SG 17 정기회의를 통해 표준과제(X.CYBEX)로 채택되었다. 이후 표준화 작업은 미국 주도로 일본, 영국, 캐나다, 한국 등 주요국이 적극 참여하여 2011년 4월에 ITU-T 권고안(X.1500)이 제정되었다. 이 표준은 유관 사이버 보안 기관이나 국가 간에 침해사고 정보를 포함한 사이버 보안 정보를 공유함으로써 침해 사건 발생 및 예방 시 공동으로 신속하고 효율적으로 대응하는 것을 목적으로 제정되었다.

[그림 1]은 CYBEX 구성 모델을 나타낸 것으로, 사이버 보안 엔터티 간의 사이버 보안 정보 교환을 위한 기술들로 구성되어 있다.

여기서 말하는 사이버 보안 엔터티란 사이버 보안 정보를 제공하거나 제공받는 조직, 개인, 장치 혹은 프로세스를 말하며, CIRT(Computer Incident Response Team)나 장비, 소프트웨어, 네트워크 기반 시스템 운영자 등이 이에 해당된다. 사이버 보안 정보 교환은 공공 도메인뿐만 아니라 사전에 정책에 동의한 신뢰된 커뮤니티 간에도 발생할 수 있다.




**[그림 2] 사이버 정보 교환을 위한 사이버보안 구성요소**

보증된 사이버 보안 정보 교환을 쉽게 하기 위해 필요하고, 적절히 분리하거나 함께 사용할 수 있는 확장이 가능한 기본 기능으로는 사이버 보안 정보 교환을 위한 정보 구조화, 사이버 보안 정보와 엔터티들의 식별과 검색, 교환 엔터티들 간의 신뢰와 정책 동의 설정, 사이버 보안 정보의 요구와 응답, 사이버 보안 정보 교환의 무결성 보장 등이 있다.

### 2.2.3 CYBEX의 구성요소 및 정보 교환 흐름

사이버 정보 교환(CYBEX)의 목적은 공통 목록들을 포함하는 사이버 보안 정보를 쉽게 공유하는 것이다. 공통 목록은 배포된 데이터베이스 등과 연계하여 보안 정보에 대한 확인 용이하게 한다. 이러한 교환을 위한 사이버 보안 정보들은 다음과 같이 구성된다[2].

- 장비, 소프트웨어, 사이버 보안과 관련된 네트워크 시스템 및 취약점
- 사고 또는 이벤트 관련 포렌식 정보
- 이벤트 통해서 획득한 휴리스틱과 시그니처들
- 사이버 보안 엔터티들의 제반 정보
- 사이버 보안 정보 교환 및 이에 포함된 모듈, 스키마, 용어와 상태에 관한 명세서
- 모든 사이버 보안 정보의 정체 및 보증 속성
- 구현 요구사항, 지침 및 사례

[그림 2]는 사이버 정보 교환(CYBEX)을 제공하는 사이버 보안 구성요소를 나타낸 것으로, 사이버 정보 교환은 위협 분석을 위한 정보 교환과 침해사고에 대한 대응조치를 위한 정보 교환 등으로 나누어진다는 것을 알 수 있다. 또한 사이버 보안은 사전 방어 조치, 사이버위협 탐지 및 조치, 위협 차단 및 복구 조치, 법적 구제 등으로 구성될 수 있으며, 각 점

선들은 위협 분석 및 대응 조치를 위한 사이버 정보 교환의 흐름을 나타낸다.

### 2.2.4 OASIS STIX(Structured Threat Information Expression) 표준 동향

STIX는 구조화된 위협 정보 표현규격으로 사이버 위협 인텔리전스(CTI, Cyber Threat Intelligence) 정보를 교환하는 데 사용되는 언어이다. STIX를 사용하면 일관성 있고 효율적으로 사이버 위협 정보(CTI)를 공유할 수 있으므로, 사이버 보안 조직들은 미래 가능성 있는 사이버 공격들을 더 쉽게 이해하고 효과적으로 대응할 수 있게 된다. STIX는 공동 위협 분석, 위협 공유 자동화, 탐지 및 대응 자동화와 같은 다양한 기능을 제공하고 개선하도록 설계되었다.

2017년 7월 OASIS CTI TC에서 채택된 STIX 2.0은 도메인 객체와 관계 객체로 구성되어 있으며, 핵심 개념들(공통 데이터 형식, STIX 객체, 데이터 표시, 번들, 어휘, 사용자 지정 등)을 정의하고 있다. 또한, 각각의 구성객체는 다양한 세부적인 속성(공통 속성, ID 및 참조, 객체 작성자, 버전 관리, 공통 관계, 예약된 속성 등)을 가지고 있으며 JSON 형식으로 표현되어 있다. STIX 2.0 도메인 객체는 〈표 2〉와 같이 공격 패턴 객체, 캠페인 객체, 조치 객체,

〈표 2〉 STIX 2.0 도메인 객체 정의[3]

| 객체 | 설명 |
|---|---|
| 공격 패턴(Attack Pattern) 객체 | 공격 패턴은 악의적 사용자가 대상의 훼손을 시도하는 방법을 설명하는 TTP(Tactics, Techniques, and Procedures)의 한 형식이다. |
| 캠페인(Campaign) 객체 | 캠페인은 특정 목표군을 대상으로 일정 기간 동안 발생하는 일단의 악의적 활동 또는 공격을 설명하는 악의적 동작의 집합이다. |
| 조치(Course of Action) 객체 | 조치는 공격을 예방하거나 진행 중인 공격에 대응하기 위해 실행한 작업이다 |
| ID(Identity) 객체 | ID는 실제 개인, 조직 또는 그룹은 물론 개인, 조직 또는 그룹의 부류를 표현할 수 있다. |
| Indicator 객체 | Indicator는 수상한 또는 악의적 사이버 활동을 검색하는 데 사용할 수 있는 패턴을 포함하고 있다. |
| 침입 단체(Intrusion Set) 객체 | 침입 단체는 단일 조직이 지휘한다고 판단되는 공통 속성을 가진 악의적 동작과 리소스의 그룹화 된 집합체이다. |
| 멀웨어(Malware) 객체 | 멀웨어는 일명 악성코드 및 악성 소프트웨어라고도 알려진 TTP의 일종이며, 피해자의 데이터, 응용 프로그램 또는 시스템에 대한 기밀성, 무결성 또는 가용성을 훼손하거나, 또는 다른 방법으로 피해자를 괴롭히거나 붕괴시킬 의도를 가지고 시스템에 삽입하는 프로그램을 가리킨다. |
| 관측 데이터(Observed Data) 객체 | 관측 데이터는 사이버 관측 가능 객체 사양을 사용하여 시스템과 네트워크에 대해 관측한 정보를 전달한다. 예를 들어 관측 데이터는 IP 주소, 네트워크 연결, 파일 또는 레지스트리 키의 관측 정보를 포함할 수 있다. |
| 보고서(Report) 객체 | 보고서는 위협 행위자, 멀웨어 또는 컨텍스트와 관련 세부 정보를 포함한 공격 기법에 대한 설명과 같이 하나 이상의 주제에 초점을 맞춘 위협 인텔리전스의 모음이다. |
| 위협 행위자(Threat Actor) 객체 | 위협 행위자는 악의적인 의도를 가지고 운영된다고 판단되는 실제 개인, 그룹 또는 조직이다. |
| 도구(Tool) 객체 | 도구는 위협 행위자가 공격을 수행하기 위해 사용할 수 있는 합법적인 소프트웨어이다. |
| 취약성(Vulnerability) 객체 | 취약성은 해커가 시스템 또는 네트워크에 대한 액세스 권한을 얻기 위해 직접 사용할 수 있는 소프트웨어의 취약한 부분이다. |

ID(Identity) 객체, Indicator 객체, 침입 단체 객체, 멀웨어 객체, 관측 데이터 객체, 보고서 객체, 위협 행위자 객체, 도구 객체, 취약성 객체 등 12개로 구성되어 있다[3].

STIX 2.0 관계 객체는 관계성 객체와 발견 객체 등 2개로 구성되어 있으며 세부 내용은 〈표 3〉과 같다.

### 2.3 사이버위협 정보 공유 관련 국내외 표준화 동향

#### 2.3.1 OASIS STIX/TAXII 표준화 동향

STIX/TAXII는 2012년 미국 국토안보부(DHS)의 지원을 받아 마이터(MITRE, 미국 비영리 연구단체)에서 개발되었으며, 2013년 미국 국토안보부는 사이버위협에 대응하기 위하여 효율적이고 안전한 정보 공유 체계 구축의 필요성을 인지하고, MITRE를 통해 4월 사이버위협 정보 전송 규격인 TAXII 공식 버전 1.0을 발표하고, 10월에는 사이버위협 표현 규격인 STIX 공식 버전 1.0.1을 발표하였다.

2015년 6월 미국 국토안보부는 STIX/TAXII와 관련된 모든 권리 및 상표를 비영리 컨소시엄인 OASIS로 이양하였고, 그해부터 OASIS의 지능형 사이버위협 대응 기술 위원회(CTI TC, Cyber Threat Intelligence Technical Committee)에서 STIX와 TAXII의 업데이트 작업을 진행하고 있다[4].

STIX/TAXII와 더불어 CybOX(Cyber Observable eXpression)까지 개발되어 글로벌 위협정보 공유 커뮤니티에 도입되었으나, XML(Extensible Markup Language) 언어의 복잡성과 다양한 옵션을 갖고 있는 데이터 모델이 오히려 상호 운용성을 저해시키는 등의 문제점에 직면하

〈표 3〉 STIX 2.0 관계 객체 정의[3]

| 객체 | 설명 |
|---|---|
| 관계성(Relationship) 객체 | 관계성은 두 SDO가 서로 관련된 방법을 설명하기 위해 이들을 서로 연결하는 데 사용된다. |
| 발견(Sighting) 객체 | 발견은 Indicator, 멀웨어, 도구, 위협 행위자 등 CTI의 무언가가 발견되었다는 사실을 기술한다. |

〈표 4〉 OASIS STIX/TAXII 표준 현황[5]

| 구분 | 제목 | 내용 |
|---|---|---|
| STIX 2.0 명세서 | STIX™ Version 2.0. Part 1: STIX Core Concepts[part1] | STIX의 전반적인 개념과 STIX 언어의 전체 구조를 정의 |
| | STIX™ Version 2.0. Part 2: STIX Objects[part2] | STIX가 사이버위협 정보를 표현하기 위한 도메인 오브젝트와 관계 오브젝트 등을 정의 |
| | STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts[part3] | STIX Cyber Observables 전반에 적용되는 개념 정의 |
| | STIX™ Version 2.0. Part 4: Cyber Observable Objects[part4] | STIX 혹은 그 외에서 사용 가능한 Cyber Observable 집합을 정의 |
| | STIX™ Version 2.0. Part 5: STIX Patterning[part5] | 네트워크나 엔드 포인트 상의 악의적인 활동 감지를 위한 언어 패턴화 |
| TAXII 2.0 명세서 | TAXII™ Version 2.0. | TAXII 클라이언트와 서버 구현에 필요한 요구사항과 함께 TAXII의 RESTful API와 리소스를 정의 |

게 되었다. 이를 극복하기 위하여, JSON(JavaScript Object Notation) 기반의 STIX 버전 2.0이 새로이 출시되었다. 개발 과정에서 CybOX는 STIX와 통합되었고, TAXII는 HTTP Representational State Transfer(RESTful) 기반으로 변경되었다[4].

현재 통용되는 OASIS STIX/TAXII 최종 버전은 2.0으로, STIX 관련 5개의 표준과 TAXII 관련 1개의 표준이 2017년 7월에 발간되었다. 각 표준에 대한 간략한 내용은 〈표 4〉에서 설명하고 있다.

현재 일반 문서로써 CTI에 대한 명세서가 OASIS CTI TC에서 개발되고 있다. 이에는 FAQ와 제품 프로세스, 확장 프로세스 등이 포함되어 있다. 또한 STIX/TAXII 버전 2.1을 위한 문서가 개발되고 있으며, 현재 WD(working draft) 단계이다. 개정 작업 중의 문서는 [6]에서 확인할 수 있다.

### 2.3.2 TTA STIX/TAXII 표준화 동향

TTA에서는 정보보호기술위원회(TC5) 사이버보안 프로젝트그룹(PG503)에서 사이버위협 정보 공유를 위한 표준과 사이버위협 정보 표준 지표 개발을 담당하고 있다. 개발하던 STIX 1.0이 STIX 2.0으로 변경되어 버전 1.0으로 진행하던 국내 준용표준을 폐지하고 STIX 2.0에 맞추어 총 6건의 표준을 채택·개발되었으며, STIX 기반 사이버위협 정보 공유 체계와 레거시 탐지 체계 간 연동을 위한 시스템 구조에 대한 TTA단체표준도 제정되었다. 각 표준에 대한 간략한 설명은 〈표 5〉에서 설명하고 있다.

〈표 5〉 TTA PG503에서 개발된 STIX 관련 표준

| 표준 초안명 | 표준명 | 내용 | 비고 |
|---|---|---|---|
| TTAE.OT-12.0019-Part1 | 구조화된 위협 정보 표현 규격 (STIX™) 버전 2.0 - 제 1부: STIX 핵심 개념 | STIX 전반적인 개념과 STIX 언어의 전체 구조를 정의 | 준용표준 |
| TTAE.OT-12.0019-Part2 | 구조화된 위협 정보 표현 규격 (STIX™) 버전 2.0 - 제 2부: STIX 객체 | STIX가 사이버위협 정보를 표현하기 위한 도메인 오브젝트와 관계 오브젝트 등을 정의 | 준용표준 |
| TTAE.OT-12.0019-Part3 | 구조화된 위협 정보 표현 규격 (STIX™) 버전 2.0 - 제 3부: 사이버 관측 코어 개념 | STIX Cyber Observables 전반에 적용되는 개념 정의 | 준용표준 |
| TTAE.OT-12.0019-Part4 | 구조화된 위협 정보 표현 규격 (STIX™) 버전 2.0 - 제 4부: 사이버 관측 객체 | STIX 혹은 그 외에서 사용 가능한 Cyber Observable 집합을 정의 | 준용표준 |
| TTAE.OT-12.0019-Part5 | 구조화된 위협 정보 표현 규격 (STIX™) 버전 2.0 - 제 5부: STIX 패터닝 | 네트워크나 엔드 포인트 상의 악의적인 활동 감지를 위한 언어 패턴화 | 준용표준 |
| TTAK.KO-12.0338 | 구조화된 위협 정보 표현 규격 (STIX 2.0)에 대한 유스케이스 | 사이버위협 분석, 침해 대응 활동, 사이버위협 정보 교환 등의 전반적인 사이버위협 관리 체계 수립에 참고할 수 있는 유스케이스를 제시 | 고유표준 |
| TTAK.KO-12.0326 | STIX 기반 사이버위협 정보 공유 체계와 레거시 탐지 체계의 연동을 위한 시스템 구조 | STIX 기반 사이버위협 정보 공유 체계와 레거시 탐지 체계 간 연동을 위한 시스템 구조 및 요구사항을 정의 | 고유표준 |

## 3. 맺음말

본고에서는 사이버위협 정보 공유 체계에 대하여 ITU-T, OASIS에서 개발된 국제 표준의 주요 내용과 TTA PG503(사이버보안 프로젝트그룹)에서 제정된 STIX 관련 국내 표준의 주요 내용들을 살펴보았다. 사이버위협 정보 공유 기술은 국내 각 정부 및 민간 기관별 침해대응센터의 고도화에 해당되는 것으로써 소규모 네트워크 차원에서 단순 모니터링 및 보안 정책을 적용하는 형태를 초월하여 향후에는 네트워크 전체를 보안 제어 영역으로 확장하여 서로 다른 관리 도메인 간 사이버위협 정보 공유를 통한 협력 기반의 종합적인 통합 보안제어 체계를 구축하기 위해 필요하다.

결론적으로 진화하는 사이버위협에 적절하면서 신속하게 대응하기 위해서는 사이버위협 정보 교환은 필수적이며, 정보를 공유하는 체계가 필요하다. 공유체계를 수립하기 위해서는 표준화된 정보 규격을 갖는 것 또한 매우 중요하며, 표준화된 정보 규격을 기반으로 구축된 사이버위협 정보 공유 체계를 수립하면 이전보다 알려진 공격 확산 방지, 알려진 공격 방어 자원 절약, 정교한 공격 방어에 집중할 수 있는 기대효과를 가질 수 있다.

※ 본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행됨[No. 2016-0- 00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발].

**[참고문헌]]**

[1] 김동희, 박상돈, 김소정, 윤오준. 2017. 사이버 위협정보 공유체계 구축방안에 관한 연구 - 미국 사례를 중심으로 -. 융합보안논문지 17, no.2:53-68

[2] ITU-T Recommendation X.1500, 'Overview of cybersecurity information exchange', 2011.

[3] 양준호, 김찬진, 김미연, 김지혜, 김종현, 염흥열, '사이버 위협 인텔리전스 공유 체계 연구', 한국정보통신학회, 종합학술대회논문집 Vol. 22. No. 2., 2018.10.18.

[4] OASIS Cyber Threat Intelligence(CTI) TC, WD 01: STIX™ and TAXII™ Version 2: FAQ, October 2017. https://docs.google.com/document/d/1V5tE78N10McUq1xUOHV1RTVsOoYmiq_xt2PY1YI8bsU/edit?usp=sharing

[5] OASIS Cyber Threat Intelligence(CTI) TC, 'Resources', Accessed 2018.11.19., https://oasis-open.github.io/cti-documentation/resources#taxii-20-specification

[6] OASIS Cyber Threat Intelligence(CTI) TC, 'CTI-TC Cover Page', Accessed 18.11.21 https://docs.google.com/document/d/1yvqWaPPnPW-2NiVCLqzRszcx91ffMowfT5MmE9Nsy_w/edit

**[주요 용어 풀이]**

- CYBEX(Cybersecurity Information Exchange): 사이버보안 정보 교환
- STIX(Structured Threat Information Expression): 구조화된 위협 정보 표현(규격)
- TAXII(Trusted Automated eXchange of Indicator Information): 위협 정보의 신뢰 기반 자동 교환
- CybOX(Cyber Observable eXpression): 사이버 관찰정보의 표현