

SEP Inside

표준특허전문지

Standard
Essential
Patent

ISSN 2289-0696 (online)
ISSN 2465-9231 (print)

Theme / 사이버 보안

Issue Focus

제로 트러스트 보안 구조

Special Column

ITS 보안 표준화 동향

바이오인식기술 표준화 동향

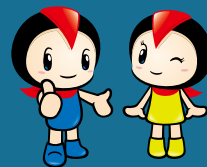
Information Analysis

사이버 보안 표준 및 관련 특허 동향

Date with SEP

샌즈랩

Vol. 38
2023. 06



특허청



한국특허전략개발원

한국특허전략개발원

[본원] 대전광역시 중구 대종로 540 유안타증권빌딩 14층, 15층 (34831)

[분원] 서울시 강남구 테헤란로 131 한국지식재산센터 8층 (06133)

<http://biz.kista.re.kr/epcenter>



QR코드 찍고
전문지를 만나보세요.



특허청



한국특허전략개발원

스마트하게 SEP Inside를 만나보세요!

최근 SEP Inside 소개



산업용 IOT



양자내성암호



오픈랜(Open RAN)



스마트모빌리티(Smart mobility)



수소차 및 충전인프라

<http://biz.kista.re.kr/epcenter/>

SEP Inside

표준 특허 전문지

Vol.38 2023.06

CONTENTS

04

Issue Focus

- 제로 트러스트 보안 구조
- 순천향대학교 엄흥열 교수

40

Information Analysis

- 사이버 보안 표준 및 관련 특허 동향
- 워크온벨류(worksonvalue) 지관영 변리사

10

News & Trend

- 표준특허 관련 뉴스 동향

50

Date with SEP

- 샌즈랩
- 김기홍 대표이사

14

Special Column

- ITS 보안 표준화 동향
- 한국전자통신연구원 이상우 책임
- 바이오인식기술 표준화 동향
- 한국인터넷진흥원/한림대 김재성 겸임교수

64

Event

- 표준특허 관련 주요 행사

34

Coffee Break

- 2023년 사이버 보안 전망
- 챗GPT 등장에 따른 보안 이슈

제로 트러스트 보안 구조

순천향대학교
제로 트러스트 및 공급망
보안포럼 운영위원장

엄홍열 교수

1 서론

재택근무가 일상화되고 있고 조직이 외부 클라우드 컴퓨팅 서비스의 이용이 증가하게 되어 지금까지의 경계 기반의 조직의 통신 네트워크 구조에 커다란 변화가 발생하고 있다. 이러한 상황에서, 내부 직원의 계정과 권한을 탈취한 해커가 정상적인 이용자로 위장하여 내부 자료 유출 등 해킹 피해 사례가 증가하고 있다. 지금까지의 경계 기반의 조직의 네트워크를 탈피해서 발생하는 문제를 해결하기 위해, 통신과 연결을 원하는 모든 실체와 자원을 식별하고, 접근 과정에서 발생하는 모든 잠재적인 위협을 식별하여, 먼저 강한 인증을 통해 실체를 인증한 후



적절한 연결 권한을 부여하며, 이러한 연결의 타당성을 지속해 점검하는 활동을 통해 얻어지는 '제로 트러스트 (zero trust)'가 최근 주목받고 있다. 제로 트러스트는 이용자의 위치에 따라 주어지는 암묵적 신뢰를 제거하고 모든 디지털 상호 동작을 지속해서 검증해 조직의 정보자원을 보호하기 위한 새로운 보안의 전략적 접근 방식이다.

새로운 사이버 보안 네트워크 모델인 '제로 트러스트'는 '아무것도 신뢰하지 말고 항상 검증하라'라는 신조로, 사용자나 기기의 접근을 철저히 검증하고, 검증이 이후에도 최소한의 권한만 부여하는 새로운 보안 개념이다. 이는 내부 다양한 정보 자산에 접근하는 이용자에게 최소한의 권한을 부여하고, 모든 보안 위험을 막기 위한 인증, 접근 통제, 중단간 보안 채널의 적용 등의 가능한 모든 보안 통제를 지속해서 적용하기 위한 보안 활동으로 볼 수 있다. 본 고에서는 제로 트러스트의 원칙, 보안 모델, 그리고 보안 능력 그리고 공적 표준화 기구의 동향을 제시한다.

2 제로 트러스트 보안 모델과 보안 능력

2.1 보안 기본 원칙

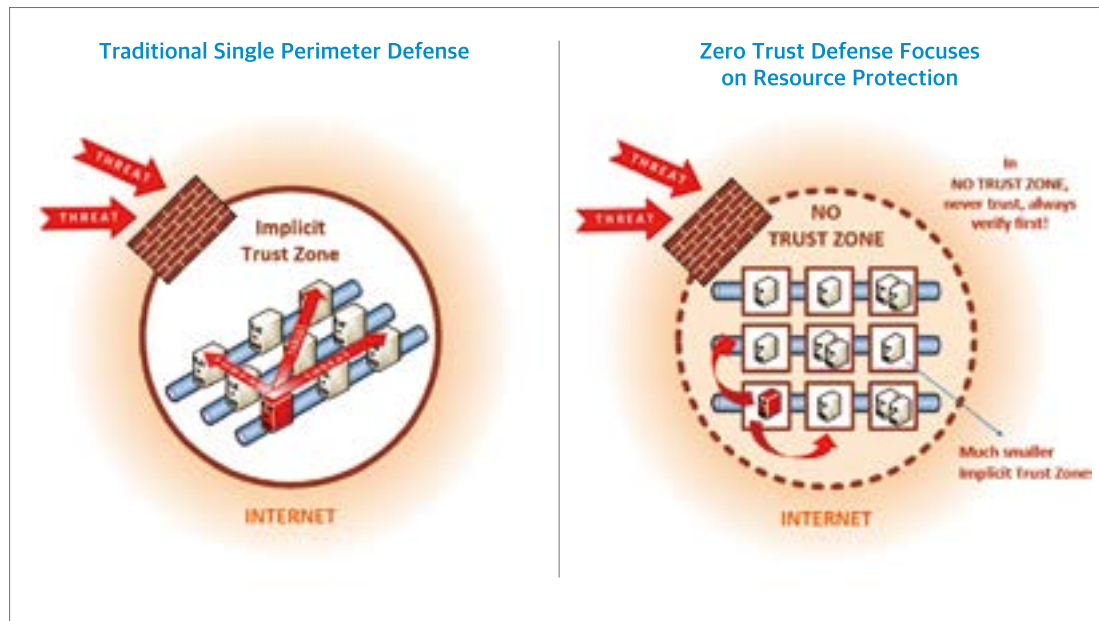
제로 트러스트 기본 원칙은 [표 1]과 같다.

표 1 제로 트러스트 기본 원칙 [1],[5]

원칙	세부 내용
① 모든 데이터와 컴퓨팅 서비스는 리소스로 간주	• 네트워크는 데이터를 수집기/스토리지로 전송하는 소형 기기, SaaS 및 다른 기능을 포함할 수 있으며, 개인 소유 단말기가 사내 리소스에 접근할 수 있다면 이 역시 리소스로 분류할 수 있음
② 네트워크 위치에 관계 없이 모든 통신 보호	• 디바이스가 기업 네트워크 내부에 있다고 해서 신뢰를 보장하지 않으며, 모든 통신의 기밀성과 무결성을 보호해야 함
③ 기업 리소스에 대한 접근을 세션 단위로 승인	• 작업을 완료하는데 필요한 최소한의 권한을 부여하여야 하며, 각 세션에 따라 접근권한을 검토 및 승인해야 함
④ 동적 정책으로 리소스에 대한 접근 결정	• 동적 정책에는 클라이언트 ID, 어플리케이션, 요청을 보낸 자산 상태, 행동 및 환경 속성 등이 포함되어야 하며, 이러한 정책에 따라 동적으로 리소스 접근을 결정하여야 함
⑤ 모든 자산의 무결성·보안 상태 모니터링 및 조치	• 기본적으로 모든 자산을 신뢰하지 않으므로, 리소스에 대한 접근 여부 판단을 위해 자산 상태를 통해 모니터링 하여야 함 • 필요시, 패치 등 보완조치를 위한 자산 모니터링을 수행하여야 함
⑥ 모든 리소스의 접근을 강력하게 점검 후 허용	• 모든 리소스에 대해 접근을 접근 획득→위협 스캔 및 평가→조정→지속적인 재평가라는 일정한 사이클로 허용하여야 함 • 이때, ICAM, 자산 관리 시스템 도입, 다중 인증 사용을 권장함
⑦ 자산, 네트워크, 인프라 등 현 상태에 대한 정보 수집	• 자산의 보안 상태, 네트워크 트래픽, 접근 요청과 관련된 데이터를 수집하고, 획득한 지식을 보안 정책을 개선하기 위해 사용하여야 함

[그림 1]은 전통적 경계 기반의 보안과 제로 트러스트 기반 방어의 개념을 나타내고 있다. 제로 트러스트에서는 묵시적 신뢰를 갖는 마이크로 신뢰 영역이 도입되었고, 공격자는 권한없이 마이크로 신뢰 영역 간 내부 이동(internal movement)하는 것을 매우 어렵게 했다. 다시 말해, 해커가 하나의 마이크로 신뢰 영역의 침투에 성공하더라도 다른 마이크로 신뢰 영역으로 이동하기 위해서는 강한 인증과 권한 점검을 수행함으로써, 해커의 내부 침투의 확장을 막을 수 있다.

그림 1 전통적 경계 기반의 보안과 제로 트러스트 기반 방어 [7]



2.2 미국 연방 정부 제로 트러스트 전략

미국 바이든 대통령은 2021년 5월 12일 행정명령[3]을 통해 미국 모든 연방 기관은 향후 제로 트러스트 보안 구조를 채택할 것을 요청하고, 각 연방 정부 장관에게 제로 트러스트 구조를 구현하기 위한 계획을 60일 이내에 수립할 것을 요구했다. 행정명령의 제3절이 제로 트러스트에 관한 내용으로 세부 내용은 다음을 포함하고 있다.

- 연방정부 사이버보안 현대화
- 연방 정부는 보안 모범 사례 채택
- 제로 트러스트 아키텍처로 진화
- 안전한 클라우드 서비스로의 이전 가속화함
- 사이버 보안 위험을 식별하기 위한 사이버 보안 데이터의 중앙집중화

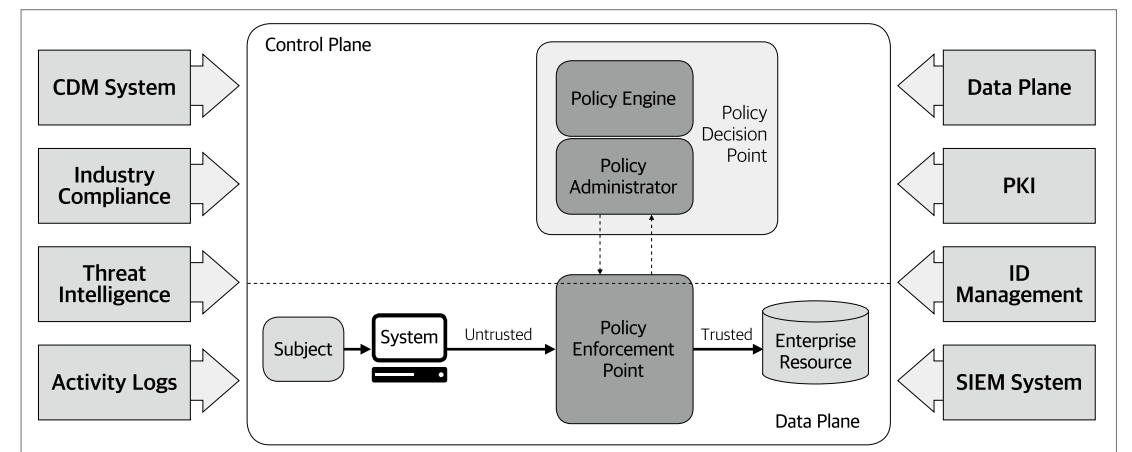
미국 국방성은 2022년 11월 국방망 제로 트러스트 전략과 로드맵을 발표했다. 2027년까지 제로 트러스트를 위해 요구되는 모든 보안 능력을 구현한다고 발표했다.

2.3 제로 트러스트 주요 기능

미국 국립표준기술원(NIST)에서는 2020년 8월 제로 트러스트 구조에 대한 공식 표준을 발표했다[1],[2]. 제로 트러스트는 네트워크 경계 기반 정적 보안 개념에서, 사용자, 자산에 초점을 맞추어 사이버 공격을 방어하기 위해 새로운 보안 전략으로 전환하기 위한 보안 패러다임을 포함하고 있다.

제로 트러스트의 주요 기능은 정책 엔진(policy engine), 정책 관리자(policy administrator), 정책집행점(policy enforcement point), 주체(subject), 조직 자원(resource)으로 구성된다. [그림 2]는 NIST의 제로 트러스트 논리적 요소를 나타낸다.

그림 2 제로 트러스트 논리적 요소 [1]



각 논리적 요소의 기능은 [표 2]과 같다.

표 2 제로 트러스트 기능 [1],[5]

기능	세부 내용
정책 엔진 (Policy engine)	• 주체에 대한 자원에 대한 접근을 허용하는지 결정
정책 관리자 (policy administrator)	• 통신 경로 설정 또는 중단 할지 책임
정책 집행점 (policy enforcement point)	• 주체와 자원 간의 연결을 설정하고, 모니터링하고 차단하는 책임
주체 (subject)	• 자원의 접근을 요구하는 최종 사용자, 응용 또는 실체
조직 자원 (enterprise resource)	• 데이터, 컴퓨팅 자원, 응용/서비스 등

2.4 DoD 제로 트러스트 능력

미국 국방성에서 제시하는 제로 트러스트가 가져야 할 주요 보안 능력은 [표 3]과 같다.

표 3 제로 트러스트 보안 능력 [4]

분류	능력 세부 내용
사용자	• 사용자 인벤토리 • 조건부 사용자 접근 • MFA • 권한접근관리 • 신원 연계/사용자 크리덴셜링
디바이스	• 디바이스 인벤토리 • 디바이스 탐지 및 준수 • 디바이스 인가 및 실시간 조사 • 원격 접근·부분 및 전 자동화된 자산, 취약점 및 패치 관리
어플리케이션 및 워크로드	• 응용 인벤토리·안전한 소프트웨어 개발 및 통합 • 소프트웨어 리스크 관리·자원 인가 및 통합
데이터	• 데이터 카탈로그 리스크 일치 • 엔터프라이즈 데이터 거버넌스 • 데이터 라벨링 및 태깅 • 데이터 모니터링 및 센싱
네트워크 및 환경	• 데이터 흐름 매핑 • SDN

분류	능력 세부 내용	
다중화 및 오케스트레이션	- 정책 결정점 및 정책 오케스트레이션 - 중요 프로세스 자동화 - ML - AI	- 보안 오케스트레이션, 자동화 및 응답 (SOAR) - API 표준 - SOC and IR
가시성/분석	- 트래픽 로그 - SIEM - 공통 보안 및 위협 분석	- 사용자 및 실체 행위 분석 - 위협 정보 통합·자동화된 능동 정책

2.5 국내 제로 트러스트 성숙도 모델

국내 제로 트러스트 성숙도 모델은 2023년 4월에 실증사업 추진을 위한 제안서에서 [표 4]와 같이 제시되었다.

표 4 제로 트러스트 성숙도 모델 [5]

	ID	장치	네트워크 환경	어플리케이션/워크로드	데이터
전통	- 패스워드 또는 멀티 팩터 인증(MFA) - 제한된 위험 평가	- 어플라이언스에 대한 제한적인 가시성 - 간단한 목록화	- 매크로 세그멘테이션 - 최소의 내·외부 트래픽 암호화	- 로컬 권한 기반의 접근 제어 - 워크플로우 최소 통합 - 클라우드 접근성 일부 제공	- 잘 정리되어 있지 않은 인벤토리 - 정적인 제어 - 비암호화
← 가시적이고 분석적인 자동화 오케스트레이션 거버넌스 →					
향상	- MFA - 클라우드와 온프레미스 시스템과 연계된 일부 ID	- 컴플라이언스 준수 시행 - 최초 접근 시 디바이스 상태에 기반한 데이터 접근	- 마이크로 경계에서의 입·출입 정의(ingress/egress) - 기본적인 분석	- 중앙화된 인증 기반의 접근 - 어플리케이션 워크플로우에 대한 기본적인 통합	- 최소의 권한 제어 - 클라우드 또는 원격 환경에서 저장된 데이터 암호화
← 가시적이고 분석적인 자동화 오케스트레이션 거버넌스 →					
최적	- 연속된 검증 - 실시간 머신러닝 분석	- 지속적인 디바이스 보안 모니터링·확인 - 실시간 위험 분석에 따른 데이터 접근	- 마이크로 경계에서의 출입의 완전한 세분화 - 머신러닝 기반 위협 보호 - 모든 트래픽 암호화	- 연속적인 접근권한 제어 - 어플리케이션 워크플로우에 대한 강력한 통합	- 동적인 지원 - 모든 데이터 암호화
← 가시적이고 분석적인 자동화 오케스트레이션 거버넌스 →					

향후 실증 사업 추진을 통해 이 성숙도 모델은 개선되고 완성될 것으로 예측된다.

3 제로 트러스트 국제 표준화와 국내 동향

3.1 ITU-T SG17 국제표준화

ITU-T SG17은 국제전기연합 정보통신부분(ITU-T) 산하 정보보호에 관한 연구반이다. 이 연구반에서는 하나의 국제표준을 개발하고 있다. 이 국제표준의 주요 내용은 [표 5]와 같다. 또한 ITU-T SG17은 차기 연구회기 (2025-2028)를 위한 신흥 표준화 주제로 제로 트러스트의 선정을 논의 중에 있다.

표 5 ITU-T TR.zt-acp의 주요 내용 [8]

표준명	표준 제목	표준 범위	신규표준화 아이템 채택	에디터
ITU-T TR.zt-acp	통신 네트워크에서 접근 통제 플랫폼을 위한 가이드라인	이 기술 보고서는 통신 네트워크에서 제로 트러스트 기반 액세스 제어 플랫폼에 대한 지침을 제공한다. 이 기술 보고서는 다음 주제를 다룬다. - 통신 네트워크에서 리소스 액세스 프로세스의 보안 과제 - 이러한 문제를 해결하기 위한 보안 요구 사항 - 통신망에서 제로 트러스트 기반 접근제어 플랫폼 프레임워크 - 통신망에서 제로 트러스트 기반 접근제어 플랫폼의 워크플로우	2021.09	Jing Huang, Wei Liu, Xu Wang, Junzhi Yan, 엄흥열

3.2 제로 트러스트 국내 대응

정부는 제로 트러스트 사이버 보안 환경 전환에 대비해 '사이버보안 패러다임 전환 연구반'을 2022년 초에 구성했고, 미국과 영국 등 선진국 사례를 분석해 우리나라 산업 맞춤형 제로 트러스트 보안 모델과 지침 마련의 필요성을 제시했다. 또한 이러한 제로 트러스트 모델을 구체화하고 보안 패러다임 변화에 능동적으로 대응하기 위해 제로 트러스트 및 공급망 보안 포럼을 2022년 11월 발족한 바 있다[6]. 제로트러스트·공급망 보안 포럼은 운영위원회, 제로트러스트 분과(2개), 공급망 보안분과(2개)로 구성되며, 각 분과별로 정책·제도, 기술·표준과 산업 등의 관점에서 보안 관련 현안을 정책과제로 정해 관련 기술개발 연구, 실증사업 등을 통해 검증을 진행하고, 최종적으로는 국가 표준화를 목표로 추진하고 있다. 또한 이의 후속 조치를 2023년 4월 다양한 업무 환경에 적용 가능한 제로 트러스트 모델을 제시하고, 실증 방안을 제시하기 위한 제로 트러스트 보안 모델 실증 지원 사업을 발표한 바 있다[5].

4 결론

미국, 영국 등 세계 주요국은 제로 트러스트 기반의 보안 구조로 전환하기 위한 계획 수립, 예산 투입, 전환 계획 이행 등의 다양한 조치를 취하고 있다. 우리나라에서도 제로 트러스트 기반의 보안 구조로 전환하기 위한 네트워크 구조의 변화를 지원하는 계획과 전환 실행을 추진하고 있다. 따라서 이를 위한 정부, 기업, 학계, 공공기관 등의 협력과 노력이 요구된다.

참고문헌

- [1] NIST Special Publication 800-207, Zero Trust Architecture, August 2020
- [2] NIST, SP 1800-35, Implementing a Zero Trust Architecture, December 21, 2022
- [3] WH, Executive Order on Improving the Nation's Cybersecurity, MAY 12, 2021
- [4] DOD Zero Trust Capability Execution Roadmap, 15 November 2022
- [5] 과기부, 한국인터넷진흥원, 제로 트러스트 보안 모델 실증 지원사업 공모 안내서, 2023.4
- [6] 과기부, 제로 트러스트 및 공급망 보안 포럼 발족식 보도자료, 2022.10.26.
- [7] NIST, Zero Trust Cybersecurity: 'Never Trust, Always Verify', 10.28. 2023.
- [8] ITU-T TR.zt-acp, Guidelines for zero trust based access control platform in telecommunication networks, (under development)

AVANCI, Avanci Broadcast 플랫폼 출시

2023. 3. 7.

출처: Avanci

ATSC 3.0 방송 표준용 원스톱 라이선스 플랫폼 제공



Avanci는 ATSC 3.0 방송 표준을 위한 특허 라이선스 플랫폼인 Avanci Broadcast를 출시했다.

Avanci Broadcast 플랫폼은 ATSC 3.0 필수 기술 라이선스 프로세스를 간소화하기 위해 표준을 구현하는 TV 및 셋톱 박스와 같은 제품 제조업체를 위한 간단하고 투명한 가격 책정 모델을 제공한다.

새로운 플랫폼은 ETRI, LG 전자, ONE Media, Panasonic, Samsung Electronics, Sharp 및 Sun Patent Trust의 ATSC 3.0 필수 특허에 대한 라이선스를 부여한다. 이들은 ATSC 3.0 선언 필수 특허를 포함하는 모든 특허 제품군의 70% 이상을 집합적으로 대표하며 Avanci는 방송 플랫폼은 향후 몇 개월 동안 더 많은 라이선서가 추가됨에 따라 성장할 것으로 예상된다.

TCL, VIA LICENSING의 고급 오디오 코딩 특허 풀에 합류

2023. 4. 12.

출처: Via Licensing

중국 거대 제조업체 TCL, VIA LICENSING와 계약



Via Licensing는 세계에서 가장 잘 팔리는 소비자 가전 브랜드이자 선도적인 기술 기업인 TCL이 Via의 Advanced Audio Coding(AAC) 특허 풀에 대한 라이선스를 확보했다고 발표했다.

Advanced Audio Coding(AAC) 특허 풀 라이선스는 TV, 스마트폰 및 태블릿을 포함한 3천만 개의 글로벌 제품에 적용된다.

TCL의 부사장인 Victor Yang은 "우리는 Via의 AAC 특허 풀에 대한 라이선스에 서명하게 되어 기쁘다. 이는 글로벌 생태계에서 이 고품질 오디오 기술을 발전시키는 공정하고 투명한 방법이다." 라고 말했다.

AVANCI는 삼성 전자를 환영합니다

2023. 4. 18.

출처: Avanci

Vehicle 4G, Avanci Atermarket, Broadcast 등 라이선스 제공



Avanci는 삼성전자가 Avanci Vehicle 4G, Avanci Aftermarket 및 Avanci Broadcast를 포함한 여러 라이선스 프로그램의 라이선스 제공자가 되었다고 발표했다.

80개 이상의 자동차 브랜드에 걸쳐 있는 Avanci Vehicle 4G의 기존 라이선스 보유자는 이제 커넥티드 차량에 대한 삼성전자의 4/3/2G 표준 필수 특허에 대한 라이선스도 취득하여 라이선스의 가치를 확장한다. 마찬가지로 Avanci Aftermarket 면허 소지자는 애프터마켓 차량 제품에 대해 보장을 받는다. Avanci는 최근 ATSC 3.0 TV 표준을 위한 원스톱 라이선스 플랫폼인 Avanci Broadcast를 출시했는데, 삼성전자는 해당 표준 개발에 가장 큰 기여를 한 기업 중 하나이다.

VIA LICENSING와 MPEG LA 통합

2023. 5. 2.

출처: Via Licensing

합병된 회사는 Via LA 로, 두 특허 풀의 전문성 및 인프라 결합



Via Licensing Corporation(Via)과 MPEG LA, LLC(MPEG LA)는 통합하여 Via Licensing Alliance LLC(Via LA)를 구성한다고 발표했다.

합병된 회사는 Via LA라고 불리며, 업계에서 가장 성공적인 두 특허 풀 관리자의 전문성, 인프라 및 관계를 결합합니다. MPEG LA의 MPEG-2 라이선싱 프로그램은 현대적인 특허 풀 산업을 확립하고 가전제품 역사상 가장 널리 사용되는 표준 중 하나를 만드는 데 도움을 주었으며, Via의 AAC 풀은 20년이 넘는 기간 동안 첫 번째 풀을 시작한 이후 포괄적이고 효율적인 신규 특허 라이선싱을 지속적으로 발전시켜 왔다.

전 Via Licensing 사장인 Heath Hoglund가 이끄는 100개 이상의 특허 풀을 하나의 조직으로 통합할 것이다. 제너럴 일렉트릭(GE), 필립스(Philips), 미쓰비시 일렉트릭(Mitsubishi Electric)은 모두 MPEG LA의 일부 지분을 보유하고 있으며 합병 법인의 지분을 갖게 된다.

구주(EU)위원회, 표준필수특허(SEP) 규칙 최초 명문화 결정

2023. 5. 3.

출처: 특허뉴스

표준필수특허, 강제 실시권 및 보충적 보호증명서 등 규정

구주위원회는 기업(특히 중소기업)이 발명을 최대한 활용하고 신기술을 이용하여 EU의 경쟁력과 기술 주권에 공헌하기 위한 일련의 규칙(안) 제정을 발표했다. 이 규칙은 표준필수특허(SEP, Standard Essential Patent), 강제 실시권 및 보충적 보호증명서(SPC, Supplementary Protection Certificate) 등에 대하여 규정할 계획이다.

금회 제안된 SEP 라이선스 프레임 워크는, SEP 포트폴리오, 누적 로열티(다수/복수 보유자의 특허가 관련되는 경우)에 대한 추가적인 투명성 제공하여, 당사자가 라이선스의 FRAND 조건에 동의하기 위한 보다 효율적인 수단을 가능하게 하는 것이다. 그 제안에서 SEP 등록, 데이터베이스, 필수성 판단, SEP의 누적 로열티에 대한 전문가의 의견, 비용이 많이 드는 소송 대신에 조정에 의한 FRAND 결정, 중소기업 지원책, 유럽연합 지식재산청(EUIPO)에 '역량센터' 설치 등 측면(항목)에 관한 조치를 도입하고 있다.

금회 제안된 규칙의 초안은 다음과 같은 내용으로 구성되어 있다. 이 초안에 대하여는 올해 6월 23일까지 의견을 받아 검토하여 확정될 예정이다.

표준필수특허(SEP)의 규칙 안(COM(2023) 232 final)의 개요는 이하와 같다.

1. 목적·대상 범위

- 이 규칙은 표준필수특허(SEP)의 라이선스 부여에 필요한 정보에 대한 투명성을 제고하여, SEP 등록, 등록된 SEP의 필수성 판단, FRAND 결정에 관한 절차를 정한다(제1조 제1항).
- 표준화 기관에 의해 발행되어 SEP 보유자가 FRAND 조건으로 라이선스하는 것을 약속하여, 로열티 프리(기술료 면제)가 아닌 SEP에 적용된다(제1조 제2항).

2. Competence Center

EUIPO 내에 설치되는 역량 센터(Competence Center)의 주요 업무는 다음과 같다(제3조).

- SEP에 관한 전자 등록 및 전자 데이터베이스 관리
- 평가자 (등록된 SEP의 필수성 판단/결정) 및 조정인(누적 로열티 결정이나 FRAND 결정을 조정)의 명부 작성, 관리 및 교육
- SEP에 관한 판례, 로열티 등의 정보 수집
- 중소기업에 대한 SEP 연수, 지원, 조언

3. SEP 등록 정보

SEP 등록의 구체적 내용은, 예를 들면, 다음과 같다(제4조)

- 표준관련정보 : 표준판, 특허와 관련된 표준문서저장, 제품, 프로세스 등
- 특허 관련 정보 : 등록국, 특허 번호 등의 기초 정보, 보유자 정보
- 표준화 기관과 약속하고 있는 FRAND 라이선스 조건에 대한 언급

4. SEP 등록의 흐름

SEP 보유자에 의한 표준의 통지에 의해, Competence Center가 등록·공표(제19조 제1항)

- 공표된 표준에 관한 SEP의 보유자는 컴피턴스 센터에 등록(제20조제1항)
- 등록 신청의 기한은 통지의 공표로부터 6월 이내 또는 지식재산청에 의한 특허 부여로부터 6월 이내(제20조제3항)
- Competence Center에 기간 내에 통보되지 않은 SEP는 등록부에 등록되기까지 EU 회원국의 관할 법원에서 집행될 수 없다. 로열티와 손해배상을 요구할 권리가 없다(제24조)

5. 누적 로열티

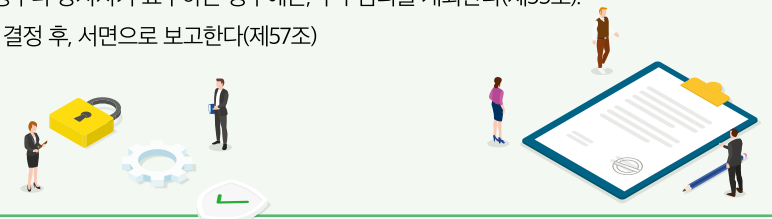
- SEP 보유자는, 역량 센터(Competence Center)에 누적 로열티(특별한 지정이 없는 경우는 글로벌 누적 로열티)를 표준에 관한 정보 등과 함께 통지 할 수 있다(제15조).
- 표준발행 후 90일 이내 등과 같은 기한이내에, 특정 표준에 대한 모든 SEP의 최소 20% 이상을 보유하는 SEP 보유자는, 역량 센터에 조정인의 임명을 요청할 수 있다(제17조).
- 전문가에게 글로벌 누적 로열티에 관한 구속력이 없는 의견을 요구할 수 있다(제18조).

6. 필수(적합)성 판단

- 표준문서에 기초하여, 평가자는 필수(적합)성 판단을 실시한다. 그 결과는 법적 구속력 없다(제 28조).
- 역량 센터는 등록 SEP에서 샘플(필수 비율 판단이 가능한 통계적으로 우수한 수)을 선택하여 평가자가 필수성 판단을 실시한다. 선택 결과는 SEP 보유자에게 통지한다(제29조 제1, 2항).
- SEP 보유자 및 실시자는 매년 최대 100개의 등록 SEP의 필수성 판단을 자주적으로 제안 가능(제29조 제5, 6항).
- SEP 보유자는 클레임 차트(Claim Chart)와 같은 추가 정보를 제출할 수 있다(제29조 제2항).
- 평가자는 SEP 보유자에게 의견 제출을 요구할 수 있다(제31조).
- SEP 보유자는 다른 평가자에 의한 상호평가를 요구할 수 있다(제32조).
- 필수성 판단의 결과는, 이유를 첨부한 의견 및 최종 이유를 첨부한 의견을 함께 공표한다(제33조).

7. FRAND 결정

- 등록부에 기재된 표준에 관한 FRAND 결정(FRAND조건을 평가하여 결정)은, 가맹국의 관할 법원에 대한 SEP 침해 청구의 개시이전에 SEP 보유자에 의하여 또는 가맹국 관할 법원에서 SEP 라이선스의 FRAND 조건 또는 평가를 요구하기 전에, SEP 실시자에 의해 개시되는 것으로 한다(제34조 제1항).
- FRAND 결정은, 역량 센터에 서면을 제출하는 것으로 개시된다(제36조).
- FRAND 결정의 기간은, 피청구자의 응답으로부터 원칙적으로 9월 이내로 한다(제37조).
- 역량 센터는, FRAND 결정을 위해 최소한 3명의 후보자를 제안하고, 당사자는 그 중에서 1명을 조정인으로 선임한다(제39조).
- 조정인은, 당사자가 FRAND결정에 도달하기 위한 노력을 지원한다(제45조).
- 조정인은 필요한 경우나 당사자가 요구하는 경우에는, 구두심리를 개최한다(제53조).
- 조정인은, FRAND 결정 후, 서면으로 보고한다(제57조)



ITS 보안 표준화 동향

한국전자통신연구원
사이버보안연구본부

이상우 책임

1 머리말

최근 스마트 모빌리티에 대한 연구가 활발히 진행 중이며, 특히 자율주행기술의 상용화가 중점적으로 추진되고 있다. 차량통신기술은 자율주행차량의 주행 안정성을 향상시킬 수 있는 필수 요소 기술로서 상용화가 진행 중이다. 차량통신기술은 차량의 주행 안정성과 편의성을 향상시키기 위하여, 차량과 차량, 차량과 주변 환경과의 통신 기술이 연구되어져 왔다[1]. 이러한 차량통신기술은 자율주행차량에서 그 중요성이 더욱 부각되고 있다. 자율주행차량에서 센서를 통해 수집되는 차량 주변 환경 정보의 한계를 극복하기 위하여 차량통신기술의



활용성이 강조되기 때문이다. 그러나, 차량통신기술을 활용하기 위해서는 반드시 보안 기술의 확보가 선행되어야 한다. 차량통신 환경은 기존의 인터넷 등의 네트워크 환경과 달리 네트워크의 보안성 확보 여부가 운전자 및 보행자의 생명과 직결되는 위험 상황을 유발할 수 있기 때문이다. 따라서, 차량통신 환경에서의 사이버 보안사고 방지를 위한 연구 개발 및 다양한 표준화 활동이 진행되고 있다[2,3]. 특히, 유럽의 UNECE(United Nations Economic Commission for Europe) WP29에서는 차량보안의 중요성을 인지하고, 2021년 1월 자동차의 사이버보안 관리체계에 대한 법규 UNR 155를 제정하였으며, 완성차 제조사 및 부품 공급사의 차량 사이버 보안 관리를 위한 조직 체계 및 제품 개발 시 보안요구사항을 준수하도록 규제하고 있다[23].

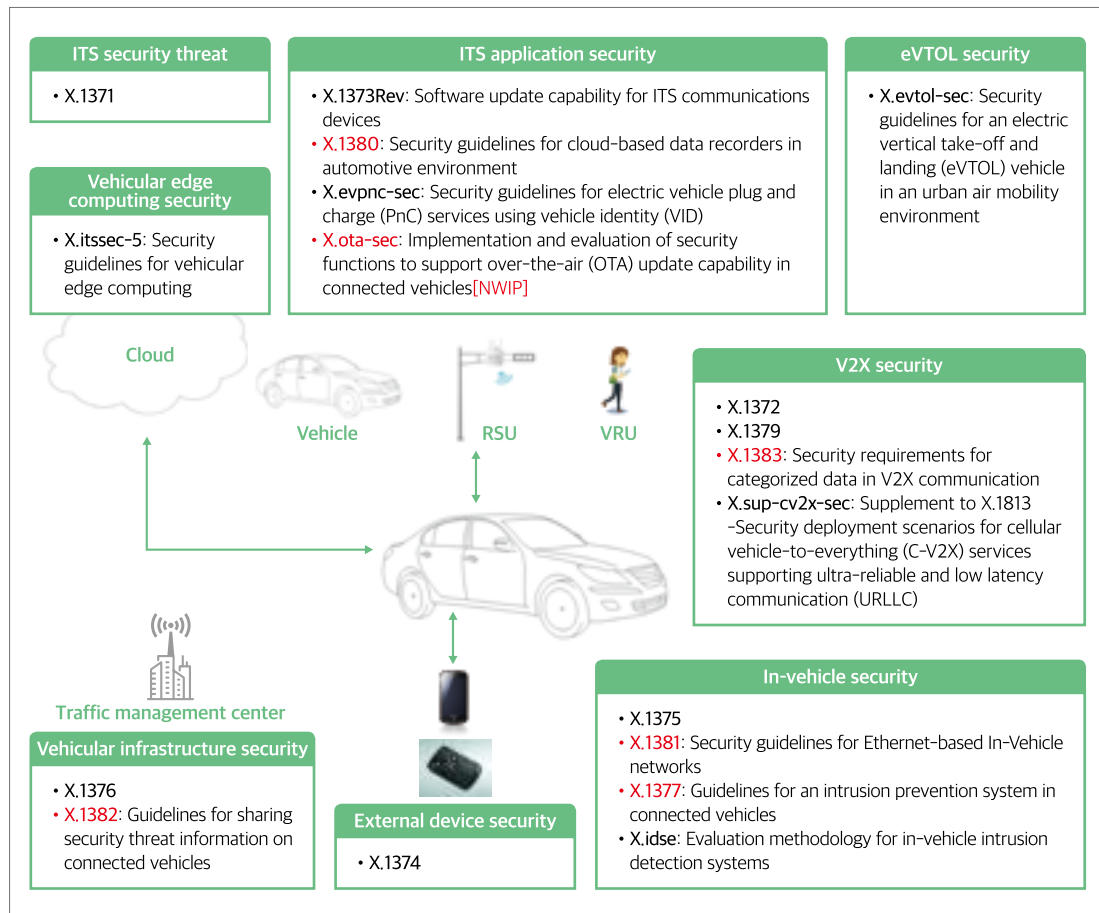
ITU-T SG17은 통신 분야의 표준화를 다루는 국제 기구인 ITU-T 산하의 사이버 보안 기술에 대한 전문 표준화 그룹이다. SG17의 ITS(Intelligent Transport System) 보안 연구반(Question 13)은 차량통신보안기술의 표준화 필요성이 대두됨에 따라, 2017년 3월에 설립되어, 차량내부망 보안, 차량외부망 보안 및 ITS 응용 보안 분야에서 대한 표준화를 활발히 추진 중이다. 본 논문에서는 SG17의 ITS 보안연구반에서 추진 중인 표준화 동향 및 국내 차량통신보안 표준화를 추진 중인 TTA PG504의 표준화 현황을 소개한다.

2 차량통신보안 표준화

2.1. ITU-T SG17에서의 차량통신보안 표준화 동향

ITU-T SG17의 ITS 보안연구반(Question 13)의 표준화 범위는 차내망 보안, 차외망 보안, 차량 응용 서비스 보안, 차량외부접속디바이스 보안, 차량보안관제 보안, 차량 클라우드 보안 등이다. [그림1]은 SG17 ITS 보안연구반의 표준화 영역과 표준 아이템을 도시한 것이다. 차내망 보안 분야에서는 차량의 침입탐지시스템 구현 방법론(X.1375)의 표준화를 시작으로, 외부 서버와의 협업을 통한 차량 침입방지시스템의 구현 지침(X.1377)의 차내망에 이더넷 도입을 고려했을 때의 보안 지침(X.1381)의 표준화를 완료하고, 현재 차량침입탐지시스템의 평가 방법론(X.idse) 표준화를 추진 중이다. 차외망 보안 분야에서는 V2X(Vehicle-to-Everything) 통신 환경에서의 보안 지침(X.1372)의 표준화를 시작으로, 도로기지국의 보안요구사항(X.1379), V2X 통신데이터의 분류에 따른 보안요구사항(X.1383)의 표준화를 완료하고, 현재 C-V2X(Cellular-V2X) 환경에서의 URLLC(Ultra-reliable and Low Latency Communication) 지원하는 보안 모델(X.sup-cv2x-sec)의 표준화를 추진 중이다. 차량보안인프라 분야에서는 차량이상행위 탐지 방법(X.1376)과 차량위협정보 공유 가이드라인(X.1382)의 표준화를 완료하였으며, 차량에지컴퓨팅 환경에서의 보안 지침(X.itssec)의 표준화를 추진 중이다. 차량통신응용분야에서는 클라우드기반 차량데이터 보안 지침(X.1380)의 표준화를 완료하고, 전기차 충전 보안 지침(X.evpnc-sec), 차량 OTA 업데이트 지원 보안 기능의 구현 및 평가 방법(X.ota-sec)의 표준화를 추진 중이다. 즉, ITS 보안연구반에서는 차량 내부/외부 통신, 통신 인프라, 차량통신응용분야 등 ITS 보안 분야 전반에 대한 활발한 표준화가 진행 중이다.

그림 1 ITU-T SG17 Q13 표준화 범위



[표 1]은 ITU-T SG17 ITS 보안연구반이 제정 완료한 표준 목록을 나타낸 것이다[4~15].

표 1 ITU-T SG17 Q13 차량통신보안 표준화 완료 목록

약어	제목	승인시기
X.1371	Security threats in connected vehicles	2020
X.1372	Security guidelines for V2X communication system	2020
X.1373	Software update capability for ITS communications devices	2017
X.1374	Security requirements for external interfaces and devices with vehicle access capability	2021
X.1375	Guidelines for intrusion detection system for in- vehicle networks	2021
X.1376	Security-related misbehavior detection mechanism based on big data analysis for connected vehicles	2021
X.1377	Methodologies for intrusion prevention system in connected vehicles	2022
X.1379	Security requirements for road-side units in intelligent transportation systems	2022
X.1380	Security guidelines for cloud-based data recorders in automotive environment	2023
X.1381	Security guideline for Ethernet-based In-Vehicle networks	2023
X.1382	Security requirements for categorized data in V2X communication	2023
X.1383	Guidelines for sharing security threat information on connected vehicles	2023

X.1371(커넥티드 차량 보안 위협)은 커넥티드 차량 및 에코시스템에서의 보안 위협을 정의하는 것이다. UNECE WP29에서 제정한 “차량 사이버보안 권고안(UN R155)[23]”의 보안 위협을 기반으로 하여, 커넥티드 차량에 대한 상위 레벨의 위협을 정의하고 있다. X.1371에서 정의된 보안 위협은 SG17 ITS 보안연구반에서 제정 중인 표준화 과제의 기초적인 보안 위협을 제공하기 위하여 제정되었다.

X.1372(V2X 통신 보안가이드라인)은 차량외부통신에서의 보안위협, 보안요구사항을 정의하고 있으며, ETRI 및 현대차가 주도적으로 표준화를 추진하였다. 차량외부통신망은 V2X(Vehicle-to-Everything) 통신으로도 표현하고 있으며, V2X는 차량과 차량(V2V, Vehicle-to-Vehicle), 차량과 인프라(V2I, Vehicle-to-Infrastructure), 차량과 노메딕 디바이스(V2D, Vehicle-to-Nomadic Device), 차량과 네트워크(V2N, Vehicle-to-Network)를 통칭하는 용어이다. X.1372에서는 V2X 환경에서에서의 보안 위협 및 보안 요구 사항을 정의하고, 차량 등록 및 인증 서비스 모델 등의 사용 예를 정의하고 있다. 특히, 이 표준에서는 V2V/V2I 통신 환경을 차량간 경고 전파, 차량 그룹 통신, 차량 경계, 차량과 인프라간 경고 전파 형태로 구분하고, 상기 형태에 따른 보안요구사항을 정의하고 있다. 그리고, 차량통신에서의 메시지 암호화 방법 및 메시지 서명 방법이 소개되어 있다. 즉, 현재 차량통신 환경에서 많이 사용되고 있는 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDSA(Elliptic Curve Digital Signature Algorithm)의 규격을 정의하고 있다. 그리고, 차량용 PKI(Public Key Infrastructure)의 참조 예로서, 유럽 ETSI의 예 및 미국의 CAMP(Crash Avoidance Metrics Partnership)의 참조 모델에 대한 설명이 부록에 기술되어 있다. 특히, X.1372에서는 차량군집주행서비스를 제공하기 위한 차량 인증 방법도 정의하고 있다.

X.1373(ITS 통신장비의 소프트웨어 업데이트)는 안전한 차량의 소프트웨어 업데이트 절차를 정의한다. 차량에서는 다수의 ECU(Electronic Control Unit)를 적용하고 있고, 리콜이 요구되는 차량의 약 30%가 ECU 소프트웨어의 업데이트로 인한 문제라고 보고되고 있는 현상을 반영하여, SG17의 ITS 보안 표준화 중 가장 먼저 표준으로 승인되었다. X.1373에서는 차량의 원거리 소프트웨어 업데이트 개요, 위협 요소 및 위협 분석, 기능 요구사항, 안전한 소프트웨어 업데이트 구조를 정의한다. 이 표준에서는 차량 소프트웨어 업데이트 세부 절차의 메시지 포맷과 XML 예제도 포함하여 기술하고 있다. 특히, 2017년 표준안 최종 승인 과정에서 차내망과 연관된 메시지는 부가적인 메시지로 지정되었으나, 완성차 업계에서의 차내망 연관 규격을 포함하여야 한다는 의견이 반영되어 현재 개정 작업이 진행 중이다.

X.1374(차량 접속 외부 인터페이스 및 디바이스의 보안요구사항)은 차량에 접속하는 디바이스의 보안요구사항을 정의하는 것으로, 현대차 및 ETRI가 주도적으로 표준화를 추진하였다. X.1374는 차량 내부 진단 도구가 많이 활용하고 있는 OBD-II(On-Board-Diagnostic II) 포트 및 블루투스 등을 이용하여 차량에 접속하는 디바이스에 대한 보안요구사항을 정의하고 있다. 차량에 접속하는 디바이스는 하드웨어가 지원하는 보안 기능을 구비할 것을 명시하고 있으며, 보안 CPU, 보안 저장장치, 하드웨어 암호 가속 기능을 구비할 것을 제시하고 있다. 차량 외부 접속 장치의 통신 기능 보안요구사항으로는 블루투스, 이동통신, Wi-Fi 사용 시에 준수해야 하는 보안요구사항을 기술하고 있다. 스마트 키의 경우에는 키 추출 방지 기능

및 one time programmable 기능 등의 역공학방지 요구사항, 상호인증, 재생공격방지 및 무선신호전력제어 등의 통신보안 요구사항과 안전한 키 등록 기능 요구사항을 제시하고 있다. 또한, 외부접속장치로서, 스마트 키, 전기차충전시스템, Wi-Fi 또는 블루투스를 이용하는 접속장치에 적용될 수 있는 보안 제어 방법을 사용 예로 제시하고 있으며, 부록에는 블루투스 및 이동통신망에 대한 기술 규격을 기술하고 있다. 이 표준은 차량 완성차 업계의 요구사항을 반영하여 진행된 표준으로서, 향후 차량에 접속하는 디바이스 제작 및 관련 서비스 업계에서 참고할 필요가 있다.

X.1375(차내망 침입탐지시스템 가이드라인)은 차내망에서의 침입탐지시스템 구성 방법을 정의하는 것으로, 고려대, 현대차 및 ETRI가 주도적으로 표준화를 추진하였다. X.1375는 차내망으로 많이 활용되고 있는 CAN(Controller Area Network) 환경에 적합한 침입탐지시스템의 기능 및 규격을 정의하고 있다. 또한, 차내망 침입탐지시스템 구현을 위한 탐지 방법인 정적탐지(Static detection), 오용탐지(Misuse detection) 및 비정상탐지(Anomaly detection)의 특징을 기술하고, 부록에는 차내망 침입탐지시스템의 기본적인 구조와 차내망 트래픽의 특징을 기술하고 있다.

X.1376(커넥티드 차량의 보안이상행위탐지 매커니즘)에서는 차량의 사이버 보안 관련 비정상행위 탐지 매커니즘을 정의하고 있다. 이 표준에서는 차량의 비정상행위 수집 및 다양한 탐지 방법을 제공하고, 각 탐지 방법에 대한 사용 예를 부록에 담고 있다. 이 표준은 중국의 보안 업체 Qihoo 360 Technology에서 주도한 표준으로서, 차량용 안티바이러스 제품에 활용될 가능성이 높다.

X.1377(차량 침입방지시스템 구현방법론)은 차량의 침입방지시스템의 구현방법론을 정의하는 것이다. 차량 침입탐지시스템의 보안 기능을 정의하는 X.1375와 연계하여, 차내망 침입탐지기능을 이용한 차량 보안 침입방지시스템 구현 지침을 제공한다. 즉, 차내에는 최소한의 침입 탐지 기능만 탑재하고, 수집된 침입 탐지 결과를 활용하여, 차량 외부의 서버에서 탐지 결과를 분석하여, 최종적으로 차량이 외부의 비정상적인 공격에 대응할 수 있도록 하는 프레임워크를 제공하는 것이 목적이다.

X.1379(ITS 환경에서의 도로기지국 보안요구사항)은 ITS 환경에서 도로기지국(Road-Side Unit)이 만족해야 할 보안요구사항을 기술한 표준이다. 도로기지국은 도로의 주변에 설치되어, 도로의 교통상황 정보를 차량에 전파하고, 차량과 백엔드 서버 인프라 간의 데이터 중계 역할을 담당한다. X.1379에서는 도로기지국의 하드웨어, 펌웨어, 어플리케이션 및 데이터 레벨에서의 위협을 식별하고, 식별된 위협에 대응할 수 있는 보안요구사항을 정의하고 있으며, 도로기지국에 대한 간단한 소개를 포함하고 있다. 이 표준은 중국의 차이나 모바일에서 주도적으로 추진되었다.

2023년 상반기에 최종 승인된 표준은 다음과 같다.

- X.1380: 클라우드 기반 차량 데이터 기록 장치 보안가이드라인
- X.1381: 이더넷 기반 차내망 보안가이드라인
- X.1382: V2X 통신 데이터의 보안요구사항
- X.1383: 커넥티드 차량의 보안위협정보 공유 가이드라인

X.1380(클라우드 기반 차량 데이터 기록 장치 보안가이드라인)은 클라우드 기반의 차량 사고기록장치의 보안위협, 보안요구사항 및 사용 예를 정의하고 있다. 차량 사고 시 차량 상태를 저장하고 있는 사고기록정보(EDR, Event Data Recorder)를 안전하게 클라우드로 전송하는 방법을 기술하고 있다. 또한, 자율주행차 운행에 있어서, 사고 당시의 차량운행주체정보의 안전한 전송 및 관리 방법에 대한 보안요구사항을 정의하고 있다. 이 표준은 한국의 ETRI 및 현대차가 주도적으로 표준화를 추진하였다.

X.1381(이더넷 기반 차내망 보안가이드라인)은 이더넷 기반 차량 내부네트워크의 보안위협, 보안요구사항 및 사용 예를 정의하는 것이다. 차량에 탑재된 카메라 및 센서 등의 도입에 따라 차량 내부망에서 송수신되는 데이터 양이 증가하는 상황이며, 이러한 데이터 양의 증가에 대응하기 위하여 현재 완성차 업계에서는 차량용 이더넷의 도입을 추진하고 있다. 이 표준에서는 차량 내부 네트워크가 이더넷 기반으로 변경될 때의 보안 기능 요구사항을 정의하고 있다. 부록에는 차량용 이더넷을 지원하는 AUTOSAR(AUTomotive Open System ARchitecture) 규격과 차량 게이트웨이에 대한 정보를 포함하고 있다. 이 표준은 한국의 ETRI 및 독일의 ETAS에서 주도적으로 표준화를 추진하였다.

X.1382(V2X 통신데이터 분류에 따른 보안요구사항)은 V2X 통신환경에서 송수신되는 데이터를 분류하고, 분류된 데이터의 라이프 사이클을 고려하여 보안 레벨을 3가지 레벨로 정의하고, 정의된 보안 강도를 보장하기 위한 보안요구사항을 정의하는 것이다. 일반적인 IT 환경에서의 클라우드 보안을 위한 데이터 보안 표준화 내용을 V2X 통신 환경에 적용한 표준이다. 이 표준은 중국의 CAICT(China Academy of Information and Communications Technology)와 일본의 KDDI에 의해 주도적으로 개발되었다.

X.1383(커넥티드 차량의 보안위협정보 공유 가이드라인)은 커넥티드 차량 환경에서 자동차 제조업체 및 CERT(Computer Emergency Response Team)등이 사이버 보안 위협 정보를 공유할 때, 각 이해관계자들의 역할을 정의하는 것이다. 공유되는 정보는 Automotive-ISAC(Information Sharing and Analysis Center)에서 제안한 Indicators, TTP(Tactics, Techniques and Procedures), Security alert, Threat intelligence report를 활용하며, 보안위협정보를 공유하는 단계를 정의하고 각 단계에 따른 요구사항을 기술하고 있다. 이 표준은 중국의 IT 침해대응센터인 CN-CERT에서 주도적으로 추진되었다.

표 2 ITU-T SG17 Q13 차량통신보안 표준화 진행 현황

약어	제목	추진일정
X.1373Rev	Software update capability for ITS communications devices	2023.4Q
X.itssec-5	Security guidelines for vehicular edge computing	2024.4Q
X.evtol-sec	Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment	2024.4Q
X.idse	Evaluation methodology for in-vehicle intrusion detection systems	2024.4Q
X.evpnc-sec	Security guidelines for electric vehicle plug and charge (PnC) services using vehicle identity (VID)	2024.4Q
X.sup-cv2x-sec	Supplement to X.1813-Security deployment scenarios for cellular vehicle-to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC)	2024.4Q
X.ota-sec	Implementation and evaluation of security functions to support over-the-air (OTA) update capability in connected vehicles	2025.4Q

ITU-T SG17 ITS 보안연구반에서는 <표 2>와 같이 현재 7개의 표준화 과제가 진행 중이다[16~22]. 그 중에서 한국이 주도적으로 추진하고 있고, 2023년 하반기 또는 2024년 상반기 사전채택을 목표로 추진하고 있는 표준화 과제의 주요 내용은 다음과 같다.

X.1373rev(ITS 통신장비의 소프트웨어 업데이트 개정)

2017년 제정된 X.1373의 개정안으로서, 현재의 X.1373에서는 차량 소프트웨어 업데이트를 위한 차내망에서의 메시지를 선택 사항으로 지정하고 있다. 개정본에서는 차내망에서의 소프트웨어 절차 메시지를 필수 사항으로 지정하고, 차량 내부 네트워크 진단 규격인 UDS(Unified Diagnostic Service)를 포함하여 개정 중이다. 또한, 소프트웨어 업데이트 시 소프트웨어의 압축된 파일 전송, 기존 대비 차분 파일 전송, 메모리 복제 방식을 통한 업데이트 등의 구체적인 업데이트 방법을 정의하고 있다. 이 표준은 일본의 NICT(National Institute of Information and Communications Technology)와 한국의 현대차 및 ETRI가 협업하여 표준의 개정 작업을 진행 중이다.

X.itssec-5(차량 에지 컴퓨팅 보안 가이드라인)

X.itssec-5는 차량 에지 컴퓨팅 보안 가이드라인을 정의하는 것으로 에지 컴퓨팅은 기존의 클라우드에서 수행되는 기능 또는 서비스를 수요자와 물리적으로 가까운 곳에서 수행하는 것을 의미하는 것으로, 사용자에게 보다 빠른 응답 서비스를 제공하기 위하여 활발히 연구되고 있다. 이 표준에서는 차량 통신 환경에서 도로기지국에 에지 컴퓨팅 서버로 활용되는 것을 고려하여, 보안 위협 및 보안요구사항을 정의하고 있다. X.itssec-5에서는 이에 대한 보안요구사항을 정의를 목표로 하며, 한국의 ETRI에서 주도적으로 표준화를 추진 중이다.

ITU-T SG17 ITS 보안연구반에서는 기존의 차량 내부/외부망 및 응용 보안의 표준화와 더불어 더욱 확대된 분야의 표준화도 추진 중이다. 특히, 주목해야 할 사항은 도심항공모빌리티 보안에 대한 표준화를 추진하고 있다는 점이다. 2020년 8월에 X.evtol-sec(도심항공모빌리티 환경에서의 eVTOL 보안가이드라인)이 신규 표준화 과제로 채택되었다. eVTOL(Electric Vertical Take-off and Landing, 전기동력 수직 이착륙) vehicle은 도심용 항공 모빌리티(UAM, Urban Air Mobility)의 대표적인 교통 수단이다. eVTOL vehicle은 활주로가 필요 없는 교통수단으로서 에어 택시라고도 불리운다. 기존의 드론과 eVTOL vehicle의 차이점은 사람을 탑승객으로 하는 교통수단이라는 점이다. 이 표준은 한국의 현대차 및 ETRI가 표준화를 주도적으로 추진하고 있다.

2.2. TTA PG504의 차량통신보안 표준화 현황

국내에서는 TTA의 PG504(응용보안 및 평가인증)에서 ITS 산업계에서 참고할 수 있는 차량보안 표준화를 추진하고 있다. TTA PG504에서는 차량 간 통신 보안요구사항(TTAK.KO-12.0208, 2012년)의 표준화를 시작으로, 2023년 현재까지 차량 통신(차량외부망 및 차량내부망) 환경에서 다수의 차량통신보안 표준의 제정을 추진하였으며, 최근에는 무선통신기반 열차제어시스템의 보안요구사항 및 도로교통인프라 통합보안센터 보안요구사항 등의 표준화를 추진하였다. <표 3>에 표준으로 제정된 목록 및 주요내용을 요약하였다.

무선통신기반 열차제어시스템(CBTC)의 보안요구사항(TTAK.KO-12.0385)는 무선통신기반 열차제어시스템의 안전한 운영을 위해 열차제어 메시지의 안전한 송수신을 보장하고, 비정상적인 메시지를 탐지하고 비인가된 제어장치로부터의 메시지 수신을 차단하기 위한 무선통신기반 열차제어장치 보안요구사항과 무선통신기반 열차제어 메시지 보호를 위한 암호기 및 인증서 관리에 대한 보안요구사항을 제시한다.

도로교통인프라 통합보안센터 보안지침(TTAK.KO-12.0392)은 도로교통인프라 통합보안센터를 운영하기 위해 준수해야 하는 보안 요소들을 관리적·물리적·기술적인 관점으로 분류하고, 각 사항에 대한 정의와 항목별 요구되는 업무 기준 또는 관련 자료들의 예시를 제시함으로써 통합보안센터 운영 시 필요한 보안지침을 정의한 것이다.

표 3 PG504 차량보안 관련 제정 표준

제목	주요내용	표준번호	제정년도
무선통신기반 열차제어시스템(CBTC)의 보안요구사항	무선통신기반 열차제어시스템의 안전한 메시지 송수신 보장, 비정상적인 메시지 탐지를 위한 보안요구사항과 암호기 및 인증서 관리에 대한 보안요구사항을 정의	TTAK.KO-12.0385	2022
도로교통인프라 통합보안센터 보안지침	도로교통인프라 통합보안센터 운영 시 필요한 보안지침을 정의	TTAK.KO-12.0392	2022
차량용 이더넷 보안요구사항	차량내부망으로서 차량용 이더넷이 활용될 때의 보안 위협 및 보안요구사항을 정의	TTAK.KO-12.0363	2020
자동차 내부 계측 제어기 통신망을 위한 능동적 사이버 방어 체계 보안 요구 사항	자동차 내부 계측 제어기 통신망에서 위한 보호 대상의 주요 속성(IP Address, Port, Protocol, Platform, OS 등)을 이동(Moving)시키면서 공격자의 공격 또는 분석 행위를 무력화 시키는 능동적인 방어 전략인 능동적 사이버 방어 체계 보안 요구 사항을 정의	TTAK.KO-12.0364	2020

제목	주요내용	표준번호	제정년도
차량-사물 통신용 하드웨어 보안 모듈(HSM) 보안 요구 사항	전자서명키 등의 비밀정보를 안전하게 저장하고, 전자서명 및 암호화 등을 수행하는 하드웨어 모듈인 HSM을 차량통신환경에 적용할 때의 기능 및 보안요구사항을 정의	TTAK.KO-12.0365	2020
오토사(AUTOSAR) 기반의 차량 보안 기능 개발 지침	오토사(AUTOSAR) 기반의 차량 제어기 개발 시 적용 될 수 있는 보안 기능을 설명하고, 이를 적용하는 방법과 유의해야 할 사항을 기술	TTAK.KO-12.0357	2019
차량 내부 네트워크 보안요구사항	자동차 내부 네트워크를 안전하게 보호하기 위하여 자동차 내부 네트워크 구성 요소들의 운용 및 관리 시 발생 가능한 사이버 보안 위협을 분석하고, 이에 대응하기 위한 보안 요구 사항을 정의	TTAK.KO-12.0346	2019
클라우드 커넥티드 자동차 보안요구사항	자동차와 클라우드 연계 방식 및 구조, 보안위협 및 보안요구사항 정의	TTAK.KO-12.0342	2018
차량의 군집 주행 서비스를 위한 차량 등록 절차	차량의 군집 주행 서비스를 위한 차량 등록 절차 및 군집 형성을 위한 군집리더차량의 인증서 발급 절차를 정의	TTAK.KO-12.0318	2017
자동차 전자제어장치(ECU) 펌웨어 보안 요구 사항	자동차 내부에 탑재된 전자제어장치 펌웨어의 운용 및 관리 시 발생 가능한 보안 위협 분석 및 보안요구사항 정의	TAK.KO-12.0300	2016
차량 내부 통신을 위한 전자제어장치(ECU) 보안 구조	차량에 탑재되는 전자제어장치의 사이버 보안 안전성을 강화하기 위한 구조를 정의	TTAK.KO-12.0299	2016
차량의 군집 주행 서비스 보안 요구 사항	다수의 차량이 하나의 그룹을 형성하여 그룹의 리더 차량 및 다수의 멤버 차량으로 구성 되어, 차량 간 통신을 이용하여 차량의 주행 정보(위치, 속도 등)를 교환하며, 멤버 차량이 차 간 거리를 유지하며 선두 차량을 따라가는 주행 방법인 군집 주행 서비스에서의 보안요구사항을 정의	TTAK.KO-12.0290	2015
자동차 전자 제어 장치 간의 통신 보안 요구 사항	자동차 내부에 탑재된 전자 제어 장치 간의 통신 환경에서의 위협 분석 및 보안 요구 사항 도출	TTAK.KO-12.0286	2015
차량간 통신환경에서의 메시지 암호화 규격	차량 간 통신에서의 메시지를 암호화 할 때 사용되는 암호 알고리즘의 차량 통신 환경에 특화된 제약 사항을 기술	TTAK.KO-12.0260	2015
차량 간 통신 인증 서비스 구조	차량간 통신환경에서 인증기관의 구조 및 인증서의 내용 및 기능을 정의	TTAK.KO-12.0238	2013
차량 간 통신 보안 요구 사항	차량 간 통신을 서비스 형태로 구분하고, 각 서비스 형태에 따른 보안요구사항을 정의	TTAK.KO-12.0208	2012

3 맺음말

보다 안전하고 신뢰성있는 자율주행기술의 실현을 위해서는 정확한 주변 환경의 인식이 필수적이다. 센서만으로 수집되는 데이터의 한계점을 보완하기 위하여 차량통신기술의 적극적으로 활용되고 있는 상황이나, 차량통신은 보안성이 선행되어야 운전자 및 탑승자 그리고, 주변 차량의 안전성을 보장할 수 있다. 이 논문에서는 차량통신보안 표준화를 활발히 추진하고 있는 ITU-T SG17 ITS 보안연구반의 표준화 활동과,

국내의 TTA PG504의 표준화 현황을 살펴보았다. 사이버 보안 공격에 안전한 차량통신 환경을 구축하고, 이를 자율주행차량에 활용하기 위해서는 지속적인 차량통신보안 연구가 필요하며, 이와 동시에 표준화를 적극적으로 추진할 필요가 있다. 특히 급변하는 차량통신보안 표준화 분야의 주도권을 선점하기 위하여 학계, 산업계, 연구기관 등의 적극적인 표준화 참여가 필요하다. 특히 TTA PG504에서는 오랜기간 동안 차량통신보안 전문가들의 노력으로 지속적으로 차량통신보안 표준 개발을 진행해 왔으며, 그간의 표준화의 내용을 기반으로 보다 적극적으로 국제표준화를 추진해야할 것이다.

사사표기

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00913, 무선 은닉채널 위험성 검증 연구)

참고문헌

- [1] 이상우 외, “차량 통신 보안 기술 동향,” 주간기술동향, vol. 1556, 2012.
- [2] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture, 2010.
- [3] IEEE Std 1609.2, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Security Services for Applications and Management Messages, 2016.
- [4] ITU-T SG17 Recommendation, X.1373, Secure software update capability for ITS communications devices, 2018
- [5] ITU-T SG17 Recommendation, X.1371, Security threats to connected vehicles, 2020.
- [6] ITU-T SG17 Recommendation, X.1372, Security guidelines for Vehicle-to-Everything(V2X) communication. 2020.
- [7] ITU-T SG17 Recommendation, X.1374, Security requirements for external interfaces and devices with vehicle access capability, 2021.
- [8] ITU-T SG17 Recommendation, X.1375, Guidelines for intrusion detection system for in- vehicle networks, 2021.
- [9] ITU-T SG17 Recommendation, X.1376, Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles, 2021.
- [10] ITU-T SG17 Recommendation, X.1377, Methodologies for intrusion prevention system in connected vehicles, 2022.
- [11] ITU-T SG17 Recommendation, X.1379, Security requirements for road-side units in intelligent transportation systems, 2022.
- [12] ITU-T SG17 Recommendation, X.1380, Security guidelines for Ethernet-based In-Vehicle networks, 2023.
- [13] ITU-T SG17 Recommendation, X.1381, Security guidelines for Ethernet-based In-Vehicle networks, 2023.
- [14] ITU-T SG17 Recommendation, X.1383, Guidelines for sharing security threat information on connected vehicles, 2023.
- [15] ITU-T SG17 Recommendation, X.1384, Security requirements for categorized data in V2X communication, 2023.
- [16] ITU-T SG17 draft Recommendation, X.1373rev, Software update capability for ITS communications devices, 2023.
- [17] ITU-T SG17 draft Recommendation, X.itssec-5, Security guidelines for vehicular edge computing, 2023.
- [18] ITU-T SG17 draft Recommendation, X.evtol-sec, Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment. 2023.
- [19] ITU-T SG17 draft Recommendation, X.idse, Evaluation methodology for in-vehicle intrusion detection systems. 2023.
- [20] ITU-T SG17 draft Recommendation, X.evpnc-sec, Security guidelines for electric vehicle plug and charge (PnC) services using vehicle identity (VID), 2023
- [21] ITU-T SG17 draft Supplement, X.sup-cv2x-sec, Supplement to X.1813-Security deployment scenarios for cellular vehicle-to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC), 2023.
- [22] ITU-T SG17 draft Recommendation, X.ota-sec, Implementation and evaluation of security functions to support over-the-air (OTA) update capability in connected vehicles
- [23] UN R155, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 2021.04
- [24] UN R156, Software update and software update management system, 2021.04

바이오인식기술 표준화 동향

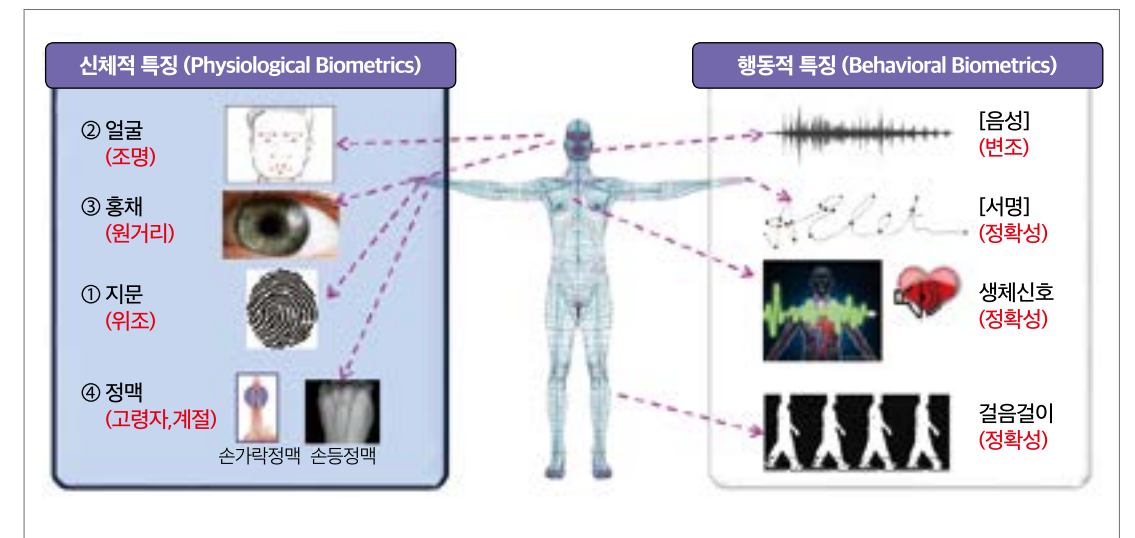
한국인터넷진흥원/한림대
공학박사 김재성 겸임교수

1. 바이오인식기술의 현황 및 발전 전망

바이오인식기술이란 [그림 1]에서 보는 바와 같이 사람의 신체적, 행동적 특징을 자동화된 IT 기술로 추출·저장하여 다양한 IT 기기로서 개인의 신원을 확인하는 보안기술 중에 하나이다. 전통적으로 이러한 바이오인식기술은 출입국심사(전자여권, 승무원·승객항공권 신원확인), 출입통제(도어락, 출입통제·근태관리), 행정(무인민원발급, 전자조달·투표), 사회복지(미아찾기, 복지기금관리), 의료(원격의료, 의료진·환자 신원확인), 정보통신(휴대폰·PC·인터넷 인증), 금융(온라인·모바일 뱅킹·결제, ATM 현금인출) 등 다방면에서 폭넓게 보급되어 실생활에서 널리 활용되고 있다.



그림 1. 바이오인식기술 유형 및 취약점(빨간글자)



특히, 바이오인식기술은 2001년 미국의 911테러로 인하여 전세계 국제공항·항만·국경 등에서 테러리스트·범죄자 색출을 위하여 전자여권·선원수첩·국제운전면허증 등 국제통용 ID카드에 지문·안면·홍채·정맥 정보를 탑재하여 신원확인을 위하여 2002년 12월 미국 플로리다에서 ISO/IEC JTC1 SC37 국제표준화기구가 출범하면서 관련 기술에 대한 연구개발과 국제표준화를 추진하게 되었다. 이에 따라 [그림 2], [그림 3]에서 보는 바와 같이 국제통용 ID카드에 탑재하기 위하여 바이오인식 인터페이스 규격, 지문·안면·홍채·정맥 등의 이미지 데이터포맷, 바이오인식 성능 및 표준적합성 시험기술, 출입국심사 등 바이오인식 프로파일,

그림 2. 바이오인식기술 발전 추세

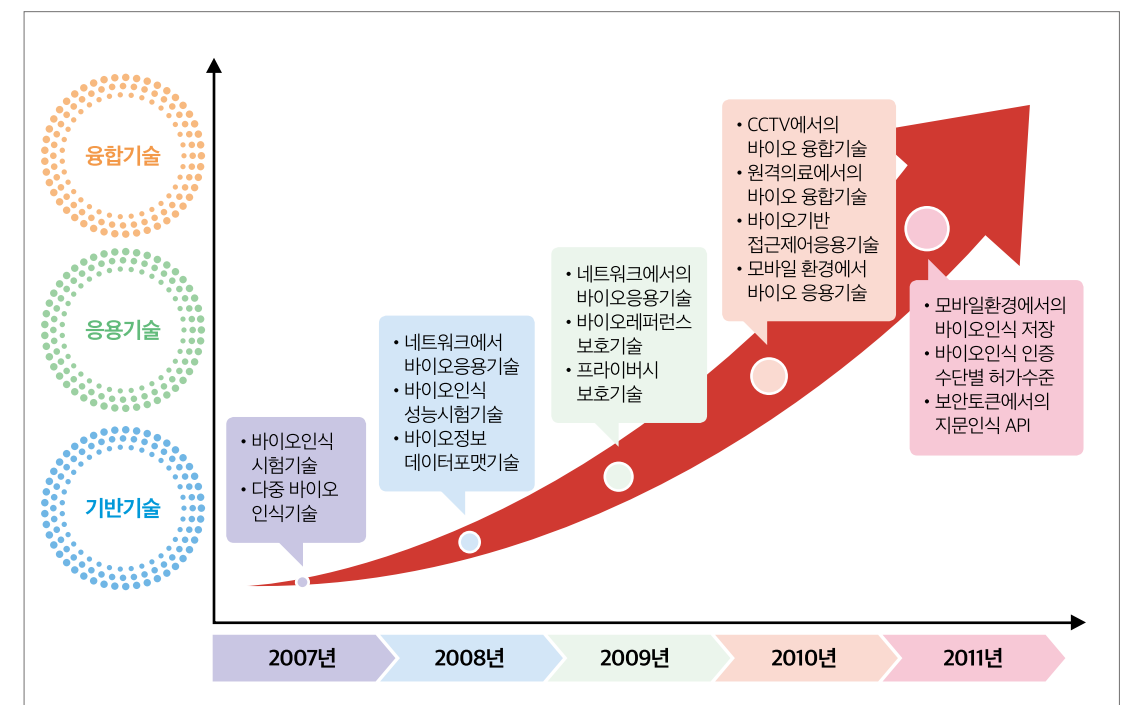
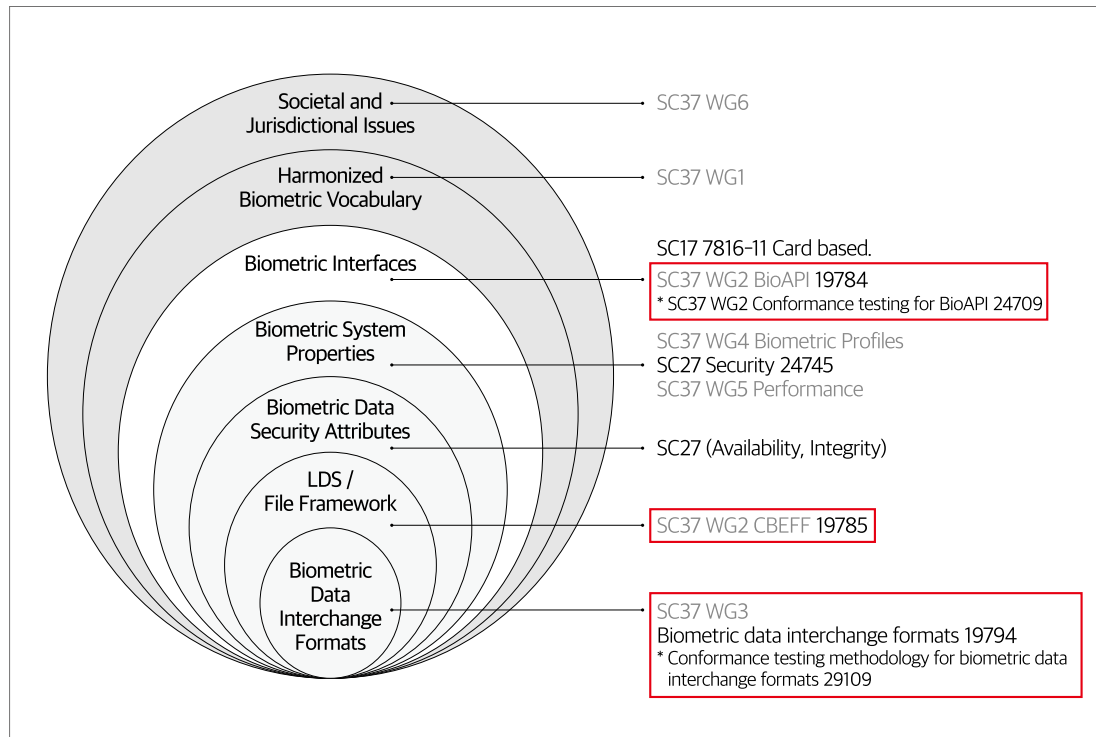


그림 3 바이오인식 관련 국제표준화기구



바이오인식 위변조 탐지기술 등의 국제표준을 개발하였다. 바이오정보는 개인 민감정보로 분류됨에 따라, ISO/IEC JTC1 SC27 WG5(ID관리 및 프라이버시 보호분과)에서는 바이오정보 보호기술, ISO/IEC JTC1 SC17에서는 국제공용 ID카드에 관한 국제표준을 개발하고 있다. 또한, 모빌리티 환경에서의 이동성이 증대됨에 따라 ITU-T SG17 Q10(ID 관리 및 텔레바이오인식분과)에서는 모바일 금융결제·디지털 헬스케어·자율주행·영상보안감시 등 응용서비스에서의 텔레바이오인식기술에 대한 국제표준화가 진행되고 있다.

포스트 코로나 이후에는 모빌리티 이동성 니즈 증대, 사이버 공간에서의 경제활동 증가 등으로 인하여 모바일기기를 이용한 간편결제서비스·인터넷 전문은행·재택근무·원격진료·반려견 개체인증 등과 같이 생활 속에 여러 방면에서 비대면 인증기술로 텔레바이오인식기술이 각광을 받고 있다. 최근 들어서는 인지력이 없는 응급환자의 지문·안면·홍채 정보와 뇌파·심전도·심박수와 같은 생체신호 등 생체정보를 이용하여 응급차에서 신원확인하고 함께 응급상황에서의 환자의 건강 상태를 대학병원 응급처치실에 전송해주는 디지털 헬스케어 응용서비스에서도 활용되고 있는 실정이다. 또한, 지능형 교통시스템인 ITS(Intelligent Traffic System) 출현으로 전 세계적으로 무인 자율주행차에 관심이 증폭되면서 스마트카 탈취 및 비인가 운전자의 불법주행 등 스마트카 보안에서도 텔레바이오인식기술이 적용되고 있는 추세이다. 최근 들어 국내 현대자동차의 제네시스에서도 차량 시동 및 도어 개폐 기능에 지문·안면인식기술을 활용하고 있는 실정이다. 최근 반려동물 천만 시대를 맞이하여 반려동물 펫산업 성장에 급속도로 발전할 전망이다. 이는 특히 현재의 생체이식칩을 반려견 체내에 삽입하는 형태의 동물등록제의 부정적 시각과 펫보험사에서 반려동물 동일 품종 내에 유사한 개체식별이 불가능한데 발생 가능한 펫보험 사기 출현으로 반려견의 비문·안면인식을 통한 품종분류 및 개체식별에 바이오인식기술을 적용하는 신개념의 디지털방식의 반려동물 등록방식으로 활용될

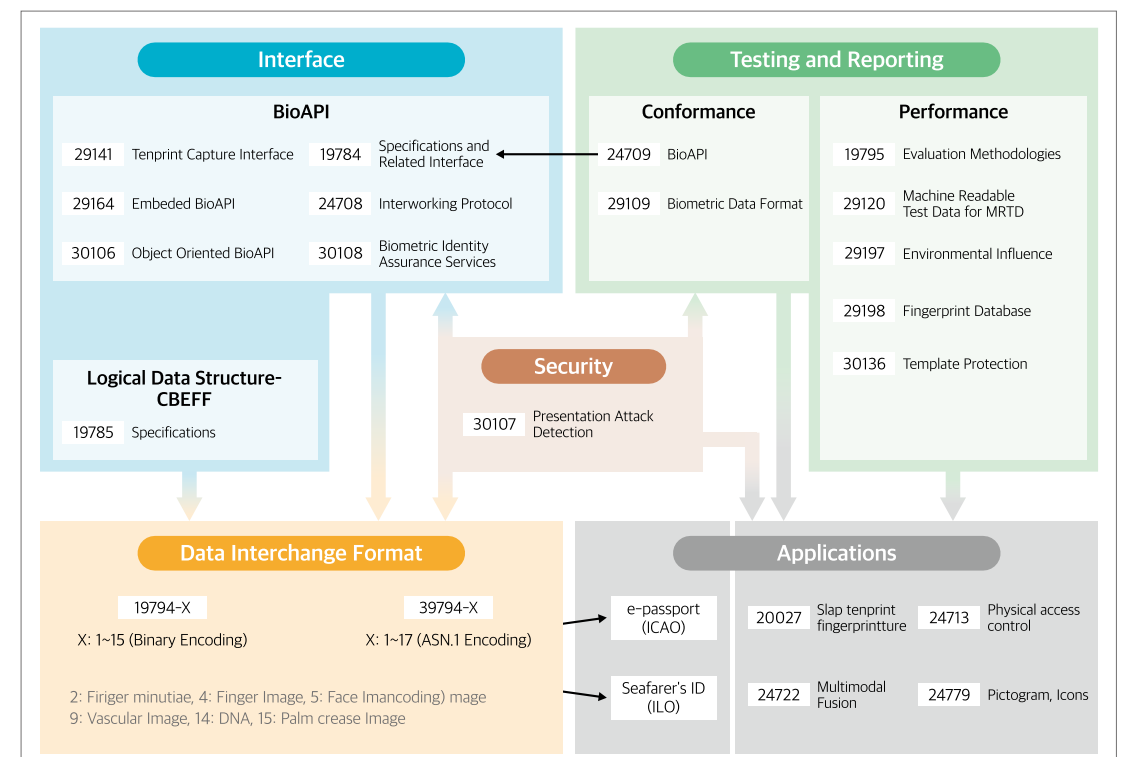
전망이다. 더 나아가서는 모바일 결제·재택근무·전자투표 등의 사이버 경제활동과 출입국심사·원격의료·차량주행·반려동물복지 등 가까운 미래의 스마트시티에서 다방면에서 생활 속에 깊숙이 바이오인식기술이 널리 활용될 것으로 전망된다.

2. ISO/IEC JTC1 SC37 국제표준화 동향

ISO/IEC JTC1 SC37 표준화 분과위원회는 9.11 테러 사건 이후 미국 등이 바이오인식기술을 활용한 신분 확인의 중요성을 인식하고 국가보안 및 세계 바이오인식 시장 선점을 위하여, 2002년 12월 미국 올랜도에서 창립총회를 시작으로 29개국의 참여국가와 13개 참관국이 있다. SC37에는 다음과 같이 6개의 워킹그룹(Working Group)으로 구성되어 [그림 4]와 같이 국제표준 131개, 기술보고서 14개의 바이오인식 핵심기술에 대한 국제표준화를 추진 중에 있다.

- WG1(Harmonized Biometric Vocabulary) 용어표준분과
- WG2(Biometric Technical Interface) 바이오인식 인터페이스 표준분과
- WG3(Biometric Data Interchange Formats) 바이오인식 데이터교환 표준분과
- WG4(Biometric Profile) 바이오인식 응용기술 표준분과
- WG5(Biometric testing and reporting) 바이오인식 시험 및 평가분과
- WG6(Cross-Jurisdictional and Societal Aspects) 바이오인식 법제도분과

그림 4 SC37 국제표준 연관도



한국의 경우 2002년 12월 ISO/IEC JTC1 SC37 창립총회부터 시작하여 KISA 김재성 겸임교수(ITU-T SG17 국제협력관, WG2/WG4 에디터), 중앙대 권영빈교수(WG2 분과의장), 테크스피어 최환수 대표이사(WG3 에디터), 국과수 한면수 센터장(WG3 에디터), 인하대 김학일교수(WG5 에디터)를 중심으로 <표 1>과 같은 국제표준을 개발한 바 있다.

표 1 한국주도의 JTC1 SC37 국제표준 목록

순번	국제표준번호	국제표준명	발행연도
1	ISO/IEC 24709-1R1	Conformance testing for the biometric application programming interface (BioAPI)–Part 1: Methods and procedures	2017.12
2	ISO/IEC 24709-2	Conformance testing for the biometric application programming interface (BioAPI)–Part 2: Test assertions for biometric service providers	2007.12
3	ISO/IEC 24709-3	Conformance testing for the biometric application programming interface (BioAPI)–Part 3: Test assertions for BioAPI frameworks	2011.12
4	ISO/IEC 30106-1 AMD1	Object oriented BioAPI–Part 1: Architecture–Amendment 1: Additional specifications and conformance statements	2019.12
5	ISO/IEC 29198-1 TR	Characterization and measurement of difficulty for fingerprint databases for technology evaluation	2013.12
6	ISO/IEC 24722 TR	Multimodal and other multibiometric fusion	2014.12
7	ISO/IEC 19794-9	Extensible biometric data interchange formats–Part 9: Vascular image data	2011.12
8	ISO/IEC 19794-14	Extensible biometric data interchange formats–Part 14: DNA data	2013.12
9	ISO/IEC 19794-15	Extensible biometric data interchange formats–Part 15: Palm crease imaging	2017.12
10	ISO/IEC 29109-9	Conformance Testing Methodology For Biometric Data Interchange Formats Defined In ISO/IEC 19794–Part 9: Vascular Image Data	2017.12

3 ISO/IEC JTC1 SC27 국제표준화 동향

ISO/IEC JTC1 SC27 분과위원회는 보안기술이라는 큰 범주에 대한 표준화를 진행하고 있으며, 바이오인식 분야는 ID관리 및 프라이버시 기술(ID 및 프라이버시 보호기술)을 주제로 하는 WG5 워킹그룹에서 다루고 있다. 바이오인식 정보는 개인을 식별할 수 있는 개인정보의 하나로 그중에서도 민감한 개인정보에 속한다고 할 수 있어서 그 보호 대책이 필요하다. 따라서 기밀성, 무결성, 가용성을 위한 다양한 요구조건 하에서 바이오인식정보의 보호를 위한 지침을 제공한다. 이를 위하여 개인식별 정보와 바이오인식정보의 흐름을 정의하고 바이오인식 시스템의 보안 취약성과 그에 따른 대책을 기술한다. 또한, 재발급 가능한 바이오인식정보

등의 바이오인식 정보보호 지침을 제공하는 표준이다. 한편 프라이버시와 관련된 표준안들인 프라이버시 프레임워크(29100, Privacy Framework)와 프라이버시 참조 구조(29101, Privacy Reference Architecture) 표준안은 그 자체로 개인정보이기 때문에 프라이버시 보호의 대상이 되는 바이오인식 정보를 사용함에 있어 참고해야 할 표준이다. 한국의 경우 2008년부터 시작하여 JTC1 SC27 WG3(보안성평가기술), WG5(ID관리 및 프라이버시보호) 등에서 KISA 김재성 겸임교수, 충북대 전명근교수를 중심으로 <표 2>과 같은 국제표준을 개발한 바 있다.

표 2 한국주도의 JTC1 SC37 국제표준 목록

순번	국제표준번호	국제표준명	발행연도
1	ISO/IEC 19792	Security evaluation of Biometrics	2009.12
2	ISO/IEC 17922	Telebiometric authentication framework using biometric hardware security module	2017.12
3	ISO/IEC 24745R1	Cybersecurity and privacy protection — Biometric information protection	2022.12

4 ITU-T SG17 국제표준화 동향

ITU-T SG17 WP5내에 Question 10 분과에서 유무선 정보통신 환경에서의 ID 관리 및 전자금융·헬스케어서비스에서의 텔레바이오인식 응용기술 표준화를 진행하고 있다. 한국의 경우 2005년부터 시작하여 KISA 김재성 겸임교수(Q10 부라포처)·신용녀 박사, 충북대 전명근교수, 한신대 이형우 교수, 연세대 박은정 교수를 중심으로 <표 3>과 같은 국제표준을 개발한 바 있다.

표 3 한국주도의 ITU-T SG17 국제표준 목록

순번	국제표준번호	국제표준명	발행연도
1	ITU-T X.1087-1	Technical and operational countermeasures for telebiometric applications using mobile devices	2017.03
2	ITU-T X.1088	Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection	2015.05
3	ITU-T X.1092	Integrated framework for telebiometric data protection in e-health and telemedicine	2014.05
4	ITU-T X.1093	Telebiometric access control with smart ID cards	2019.12
5	ITU-T X.1094	Telebiometric authentication using biosignals	2020.02
6	ITU-T X.pet_auth	Entity authentication service for pet animals using telebiometrics(개발중)	2023.09
7	ITU-T X.bvm	Requirements for biometric variability management(개발중)	2025.04

5 아시아바이오인식협의회(ABC) 사실표준화 동향

아시아바이오인식협의회(Asian Biometric Consortium)은 의장국인 한국(의장: KISA 김재성 겸임교수)을 비롯하여 일본·중국·대만·태국·인도네시아·말레이시아·싱가포르 등 아시아 8개국 바이오인식관련 산학연 전문가로 구성된 사실표준화기구로 워크숍 개최와 함께 8개 회원국을 위하여 한일 공동으로 <표 4>과 같은 사실표준을 개발하여 TTA 단체표준으로 보급하였다.

표 4 한국주도의 ABC 사실표준 목록

순번	TTA표준번호	국제표준명	발행연도
1	TTAK.KO-12.0268	웹기반 BioAPI 표준적합성 시험 상호인정 지침	2014.12
2	TTAK.KO-12.0267	지문인식 성능평가 상호인정 지침	2014.12
3	TTAK.KO-12.0266	홍채인식 성능평가 상호인정 지침	2014.12

6 국내 표준화 동향

바이오인식기술과 관련하여 국내에는 TTA TC5(정보보호기술위원회, 의장 KISA 김재성 겸임교수) 산하의 PG505(바이오인식프로젝트그룹, 의장 충북대 전명근 교수)에서 단체표준을, 국립전파연구원(RRA, ITU 대응 국가기관)·국가기술표준원(KATS, ISO/IEC 대응 국가기관)의 KS 국가표준에 대한 제개정을 추진하고 있다.

6.1 TTA 단체표준 추진현황

TTA PG505는 2003년부터 KISA·ETRI 등 연구기관, 충북대·인하대·경인여대·연세대 등 학계, 슈프리마·유니온커뮤니티 등 바이오인식업체, 파이리코·아이씨아랩 등 펫기업과 같은 산학연 전문가그룹이 TTA 단체표준들을 개발하여 보급하고 있다. <표 5>은 TTA PG505에서 보급된 주요 단체표준 목록을 보여주고 있다.

표 5 TTA 단체표준 목록

순번	TTA표준번호	국제표준명	발행연도
1	TTAS.AS-BioAPI	생체인식시스템 응용 인터페이스 표준규격(K-BioAPI)	2003.12
2	TTAS.KO-12.0047	온라인 인증 시스템을 위한 지문 센서 인터페이스	2006.12
3	TTAS.KO-12.0046	지문 영상 품질 분류 방법	2006.12
4	TTAS.KO-12.0050	네트워크 환경에서의 다중 바이오정보 보호 가이드라인	2007.06
5	TTAK.KO-12.0097	스마트카드 기반의 지정맥 인증 방법론	2008.12

순번	TTA표준번호	국제표준명	발행연도
6	TTAK.KO-12.0095	얼굴 인식 알고리즘 성능 시험 방법	2008.12
7	TTAK.KO-12.0125	지문인식 알고리즘 성능 시험 지침	2009.12
8	TTAK.KO-12.0124	얼굴 영상 획득 시스템의 보안 요구 사항	2009.12
9	TTAR-12.0006	위조지문 탐지 기술 (기술 보고서)	2010.11
10	TTAK.KO-12.0158	얼굴 인식 시스템 시나리오 기반 성능 시험 방법	2010.12
11	TTAK.KO-12.0165	바이오 보안 토큰용 API	2011.06
12	TTAR-12.0009	지문 DB의 난이도 특성화 및 측정 (기술보고서)	2011.12
13	TTAK.KO-12.0187	지문 라이브스캐너 품질평가 기준	2011.12
14	TTAK.KO-12.0186	바이오인식 정보 보호를 위한 워터마킹 기법	2011.12
15	TTAK.KO-12.0215	원거리 얼굴인식을 위한 영상품질 객체검출 및 인식 성능평가 지침	2012.12
16	TTAK.KO-12.0096/R1	[개정] 얼굴인식을 위한 영상 획득 방법에 대한 지침	2013.12
17	TTAK.IT-X.1092	[개정] 바이오인식 기반 원격 의료 통합 프레임워크	2013.12
18	TTAK.KO-12.0243	모바일 기기 바이오정보 탑재방법	2014.07
19	TTAR-12.0004/R1	지문인식 시스템의 안전성 확보를 위한 지문입력기의 취약점 분석(기술보고서)	2016.10
20	TTAR-12.0021	핀테크 환경에서 텔레바이오인식을 이용한 비대면 인증(기술보고서)	2016.10
21	TTAK.KO-12.0304	개인인증용 생체신호센서 요구사항	2016.12
22	TTAK.KO-12.0303	개인인증을 위한 생체신호정보 시험용 DB 구축지침	2016.12
23	TTAK.KO-12.0302	금융보안을 위한 바이오인식 운영 지침	2016.12
24	TTAK.KO-12.0325	생체신호 인증 알고리즘 성능 시험 지침	2017.12
25	TTAK.KO-12.0324	개인인증용 생체신호 정보보호 지침	2017.12
26	TTAK.KO-12.0323	개인인증용 심전도 및 광용적맥파 특징점 데이터 교환 포맷	2017.12
27	TTAK.KO-12.0322	바이오인식 응용카드 기반의 개인 인증 시스템	2017.12
28	TTAR-12.0034	모바일 장치의 위조 바이오인식 샘플 탐지를 위한 시험 평가 지침(기술보고서)	2018.11
29	TTAR-12.0041	생체신호를 이용한 헬스케어 응용서비스(기술보고서)	2019.10
30	TTAK.KO-12.0358	정보분할에 의한 바이오인식 정보 보호	2019.12
31	TTAK.KO-12.0371	정보분할에 의한 일회용 패스워드와 바이오인식을 이용한 다중 인증	2021.06
32	TTAK.KO-12.0380	바이오인식 기반의 반려동물 개체 식별용 DB 구축 지침	2021.12
33	TTAK.KO-12.0048/R2	[개정] 바이오(생체)인식 용어	2022.06
34	TTAK.KO-12.0393	정보분할에 의한 민감한 생체정보의 안전한 공유	2022.12

6.2 KS 국가표준 추진현황

RRA에서는 ITU-T SG17, KATS에서는 ISO/IEC JTC1 SC37의 국제표준에 대한 부합화 KS 국가표준을 개발하여 <표 6>과 같이 보급하고 있다.

표 6 KS 국가표준 목록

순번	국가표준번호	국제표준명	발행연도
1	KSXISOIEC19795-1	정보기술-생체인식 성능테스트와 보고-제1부: 원리와 구조	2014.12
2	KSX6046-1	모바일 환경에서 안전한 바이오정보 탑재방법(고유표준)	2015.03
3	KSXISOIEC19784-1	정보기술-생체인식 응용 프로그래밍 인터페이스-1부:BioAPI 명세	2005.12
4	KSXISOIEC19784-2	정보기술 -생체인식 API-제2부: 생체인식 아카이브 함수제공자 인터페이스	2014.12
5	KSXISOIEC19785-1	정보기술-일반 생체인식 교환 포맷 프레임워크-제1부: 데이터 항목 명세	2014.12
6	KSXISOIEC19785-2	정보기술-일반 생체인식 교환포맷 프레임워크-제2부 : 생체인식 등록 권한 절차	2014.12
7	KSXISOIEC19794-1	정보기술-생체인식 데이터 교환포맷-제1부: 프레임워크	2014.12
8	KSXISOIEC19794-10	정보기술-생체인식 데이터 교환포맷-제10부: 손 기하학적 실루엣 데이터	2014.12
9	KSXISOIEC19794-14	정보기술-생체인식 데이터 교환포맷-제14부: DNA 데이터	2015.03
10	KSXISOIEC19794-2	정보기술-생체인식 데이터 교환 포맷-제2부: 지문 특징점 데이터	2005.11
11	KSXISOIEC19794-3	정보기술-생체인식 데이터 교환포맷-제3부: 지문 패턴 스펙트럴 데이터	2008.06
12	KSXISOIEC19794-4	정보기술-생체인식 데이터 교환포맷-제4부: 지문 이미지 데이터	2005.11
13	KSXISOIEC19794-5	정보기술-생체인식 데이터 교환포맷-제5부: 얼굴 영상 데이터	2005.11
14	KSXISOIEC19794-6	정보기술-생체인식 데이터 교환포맷-제6부:홍채 영상 데이터	2005.11
15	KSXISOIEC19794-7	정보기술-생체인식 데이터 교환 포맷-제7부: 서명/사인 시계열 데이터	2014.12
16	KSXISOIEC19794-8	정보기술-생체인식 데이터 교환포맷-제8부:골격선 지문 패턴 데이터	2008.06
17	KSXISOIEC19794-9	정보기술-생체인식 데이터 교환포맷-제9부: 혈관 이미지 데이터	2008.06
18	KSXISOIEC19795-2	정보기술-생체인식 성능 테스트와 보고-제2부: 기술 및 시나리오 평가를 위한 테스트 방법론	2014.12
19	KSXISOIEC24709-1	정보기술-BioAPI를 위한 적합성 평가-제1부:방법과 처리절차	2006.12
20	KSXISOIEC29109-9	정보기술-생체인식 데이터 교환포맷 적합성 평가 방법-제9부: 혈관 이미지 데이터	2010.12
21	KSXISOIEC19795-3	정보기술-생체인식 성능 테스트와 보고-제3부: 모달리티 특정 테스트	2014.12
22	KSXISOIEC24741TR	정보기술-생체인식 튜토리얼	2014.12
23	KSXISOIEC24722TR	정보기술-생체인식-다중모드 및 다른 다중생체인식 융합	2014.12

6 향후 표준화 추진전략

전 세계적인 코로나19로 인한 재택근무, 인터넷 전자상거래, 자율주행차, 원격진료, 전자투표, 모바일 결제 등 사이버 공간에서의 경제활동 급증 등의 국내외 변화요인으로 인하여 앞으로는 사이버공간에서의 비대면 인증수단인 바이오인식기술의 중요성이 부각될 전망이다. 또한, 1인 가구 증가와 노령화가 급속도로 진행되고 있는 우리나라 현실에서 날로 증가되고 있는 반려견·반려묘 등의 반려동물에 대한 출생·입양·양육·진료·사망 등 생애 전주기 보안관리를 위해서는 비문인식기술을 이용한 반려동물의 개체식별기술이 필수불가결한 요소라 생각된다. 이러한 개체식별기술은 향후 종마의 종자관리, 개체수가 많은 소·돼지 등의 축산동물과 개체수가 급격하게 줄어드는 북극곰·코끼리 등 야생동물에 이르기까지 동물 개체식별기술과 심전도 등의 생체신호를 이용한 심장질환 등의 헬스모니터링 등 동물복지기술로 발전시켜야 할 것이다. 이에 따라 지난 2016년 3월 29일부로 과기정통부 산하 비영리 사단법인으로 국내 바이오인증 시장 활성화를 위하여 출범한 한국바이오인식협회(KBID, Korea association for Biometric IDentity and security)와 KISA를 중심으로 바이오인식기술을 이용하는 자율주행 및 무인자동차, 원격진료가 가능한 디지털 헬스케어서비스, 진화되는 스마트시티 구현, 동물복지기술 등에 필요한 연구개발과 표준화를 추진하여 우리나라가 선도적인 차세대 바이오인증 시장을 선점하는데 적극적인 지원이 시급한 실정이다.

참고문헌

[1] 김재성, “텔레바이오인식기반 비대면 인증기술 표준화 동향,” 정보보호학회지, 제25권, 제 4호, 2015.08.
[2] 김재성, 생체신호 인증기술 및 표준화 동향, TTA 저널, 2016.06.
[3] 김재성·전명근, 바이오인식 국제표준화 동향, 한국정보보호학회지, 2017.10.
[4] 김재성, 바이오인식기술의 현재와 미래, 그리고 표준화, TTA 아카데미, 2021.6월
[5] 김재성, 미래의 스마트시티에서의 바이오인식 기술표준화, 정보보호학회지, 제32권 제4호, 2022.8월
[6] 김재성, 반려동물 개체식별기술 등 진화하는 바이오인식기술, 보안뉴스, 2020.2월
[7] 김재성, 진화하는 미래의 텔레바이오인식기술, TTA 저널, 2023.04.
[8] Jason Kim, ITU-T X.1094: Telebiometric authentication using biosignals, Feb. 2019.
[9] Jason Kim, Taehoon Kim, 6th Revised baseline text for ITU-T X.pet_auth: Entity authentication service for pet animals using telebiometrics(TD944), Feb. 2023.
[10] Eunjeong Park, Jason Kim, NWIP for ITU-T X.bvm: Requirements for biometric variability management(TD1014R1), Feb. 2023.

2023년 사이버보안 전망



2023년 디지털금융 및 사이버보안 10대 이슈

금융보안원은 2023년 디지털금융과 사이버보안 분야에서 주목해야 할 10대 이슈를 발표했다.(2022.11.9.) 이번 10대 이슈는 보안 위협 및 대응, 디지털 신기술 및 리스크, 컴플라이언스 및 전략 등 3가지 분야로 나누어 2023년에 이슈가 될 것으로 예상되는 주제를 선정했다.



출처: 인포그래픽=금융보안원



보안 위협 및 대응 분야

① 사이버 공격 경로로 악용될 수 있는 엔데믹 취약점

- 제로데이 등 고위험 보안 취약점을 이용한 사이버 공격 증가

※ 제로데이(zero day 또는 0day): 운영체제(OS)나 네트워크 장비 등의 보안 취약점을 발견하고 이를 막을 수 있는 패치가 나오기 전에 그 취약점을 이용한 악성코드나 프로그램을 제작해 공격하는 수법

- 구글, MS 등 글로벌 빅테크 기업은 자사 제품 및 서비스의 보안 취약점을 선제적으로 식별 및 방어하기 위해 버그바운티를 적극 활용

- 보안 취약점 모니터링 및 최신 패치의 신속한 적용, 효과적인 보안 취약점 관리를 위한 제도 수립 등이 필요

※ 버그바운티(bug bounty): 취약점 보상 프로그램이라고도 하며, 기업의 서비스, SW 및 IT 인프라의 취약점을 발견하여 신고한 자에게 포상금을 지급하는 제도

② 랜섬웨어, 피싱 앱 등 사이버 위협의 끝없는 진화

- 랜섬웨어 공격이 활발히 진행되고, 전화 수신 위장 등으로 기능을 강화한 보이스피싱 악성 앱들도 증가하는 등 사이버 위협 고도화
- 오픈뱅킹, 간편 송금 등 개방과 연결을 특성으로 하는 디지털 금융 환경과 디지털 기술 등이 발전함에 따라 이를 역이용하며 진화해 나갈 것으로 전망
- 제로 트러스트로의 보안 패러다임 전환 필요

※ 제로 트러스트(zero trust): '아무것도 신뢰하지 않는다'는 것을 전제로 한 사이버 보안 모델로, 사용자 또는 기기가 접근을 요청할 때 철저한 검증을 실시하고 그 검증이 이뤄진다고 해도 최소한의 신뢰만 부여해 접근을 허용하는 방식

③ 오픈소스 이용 활성화와 강조되는 공급망 보안

- 디지털 전환의 가속화로 소프트웨어 사용이 증가함에 따라 오픈소스를 노리는 사이버 공격 심화 및 소프트웨어 공급망 공격이 중요 사이버 이슈로 부상

※ 오픈 소스(open source): 소프트웨어가 어떻게 만들어졌는지 알 수 있도록 일종의 프로그래밍 '설계지도'인 소스코드를 무료 공개·배포하는 것으로, 누구나 접근이 가능하고 검증 없이 재사용되는 경우가 많아 이를 노려 악성코드를 삽입하거나 전송하는 공격 가능

※ 소프트웨어 공급망 공격: 소프트웨어의 개발, 배포, 설치, 유지 보수 과정에 개입하여 변조된 소프트웨어가 사용자의 시스템에 전달되도록 하는 공격

- 소프트웨어 공급망에 대한 체계적인 보안 관리 필요

④ 디지털자산의 당면 과제, 리스크 관리체계 마련

- 디지털자산의 가치 상승 및 이용 활성화에 따라 사이버 공격 급증
- 국내외 규제당국을 중심으로 디지털자산에 대한 규제 논의도 활성화되고 있으며, 미카(MiCA) 등 해외 규제와의 정합성을 고려한 디지털자산 관련 규제가 중점적으로 추진될 것으로 전망

※ 미카(Markets in Crypto Act, MiCA): 유럽연합(EU)의 가상 자산 시장 규제안. 세계 최초의 가상자산 관련 법안 미카(MiCA)를 통과시킨 유럽연합(EU)이 앞으로는 대체불가토큰(NFT) 규제와 디파이(DeFi·탈중앙화 금융) 등 제도 정비에 주력할 것으로 예측

- 디지털자산 관련 글로벌 입법 동향을 지속적으로 모니터링하고, 디지털자산 관련 사업자는 새롭게 마련되는 법적 요구사항에 즉각 대응할 수 있도록 사전 대비 필요



디지털 신기술 및 리스크 분야

⑤ 대세로 자리잡은 클라우드와 보안 고려사항

- 디지털 신기술 활용 증가 등에 따라 클라우드에 대한 관심 고조
- 클라우드 이용과 관련해 계정 도난, 설정 오류, 운영 실수 등에 따른 서비스 중단, 데이터 유출 등이 지속적으로 발생하고 있으며 클라우드 보안 사고 대부분이 기술적인 문제보다는 관리 미흡에서 비롯
- 멀티 클라우드 이용 등의 전략을 마련하고, 중요 업무의 클라우드 의존도를 관리하는 것이 필요

※ 멀티 클라우드: 서로 다른 업체에서 2개 이상의 퍼블릭 클라우드를 이용해 하나의 서비스를 운영하는 방식으로, 업체 종속성을 피하고 단일 클라우드의 취약점 보완 가능

⑥ 인공지능 활용, 공정성·보안성 확보를 통한 이용자 보호 필수

- 인공지능(AI) 기술은 금융산업 전반의 디지털 혁신을 주도
- 인공지능(AI) 기술이 주로 활용되는 분야로는 업무 자동화, 고객 응대, 신용 평가, 투자 및 상담, 사이버 보안 등으로 금융산업 전반에 걸쳐 활성화 전망
- 공정성, 신뢰성 및 보안성 확보를 통한 이용자 보호 조치가 필요

⑦ 디지털 신원증명 활용에 따른 기대와 우려

- 디지털 전환 및 코로나19 등으로 비대면 금융거래 이용이 크게 증가함에 따라 비대면 신원증명 방식 또한 이용이 증가
- 기존의 비대면 신원증명 방식에는 개인정보 유출, 해킹, 신원 도용 등의 위험이 존재해 안정성·편의성을 더한 새로운 디지털 인증 방식의 필요성 증대
- DID 모바일 신분증이 등장하면서 새로운 신원증명 체계가 도입되었으나, 디지털 신원증명 활용에 따른 새로운 보안 위협 발생 우려가 있기 때문에 이에 대한 대비 필요

※ DID: 탈중앙화 신원증명(decentralized Identifier, DID) 또는 분산아이디는 개인정보를 사용자의 단말기(ex. 스마트폰)에 저장해놓고 개인정보 인증 때 필요한 정보만 골라서 제출하도록 해주는 전자신원증명 기술



컴플라이언스 및 전략 분야

⑧ 금융보안 규제 합리화, 전제되는 자율 보안

- 금융권의 디지털 전환에 따른 금융혁신이 가속화됨에 따라 금융위원회가 디지털 신기술 도입·활용을 안정적으로 지원하기 위해 '금융 분야 클라우드 및 망분리 규제 개선방안'을 발표
- 보안성을 고려한 안전한 네트워크 인프라 구성, 소스코드 보안 관리를 위한 내부 정책 수립·운용, 소스코드 유출에 대비한 침해 사고 대응 절차 마련 등 내부 통제 강화 및 추가 보안 대책 필요성 강조
- 디지털 전환을 안정적으로 뒷받침하기 위한 단계적 규제 개선 필요

⑨ 마이플랫폼 시대, 데이터 확보와 보호

- 마이데이터 산업의 발전, 종합금융플랫폼 지원을 위한 금융규제 완화 등에 기반하여 초개인화 서비스를 제공하는 '마이플랫폼(My Platform)' 가능할 전망
- 개인에 대한 양질의 데이터 확보가 중요해짐에 따라 과도한 데이터 확보 경쟁 과열 및 소수 플랫폼의 정보 독과점 등이 우려
- 데이터 처리 관련 금융소비자 권리 보장 및 데이터 보호 강화 필요

⑩ 금융권 채널 변화의 핵심 디지털 연결

- 최근 혁신 점포, 디지털 공동 점포 등 오프라인 점포에도 디지털을 접목하고, 온·오프라인 및 타 업권 등과 연결을 시도하는 옴니채널 전략 추진

※ 혁신 점포 : 은행과 편의점, 마트 등 이종 업종의 협업을 통해 은행 서비스 제공

※ 디지털 공동 점포 : 하나의 지점에서 서로 다른 은행의 창구를 별도 운영

※ 옴니채널(omni-channel) : 소비자가 온라인, 오프라인, 모바일 등 다양한 경로를 넘나들며 상품을 검색하고 구매할 수 있도록 한 서비스. 각 유통 채널의 특성을 결합해 어떤 채널에서든 같은 매장을 이용하는 것처럼 느낄 수 있도록 한 쇼핑 환경을 말함. (ex. 백화점 온라인몰에서 구입한 상품을 백화점 오프라인 매장에서 찾는 '스마트팩' 방식)

- 변화하는 채널 환경에 따라 운영 및 보안 리스크 관리 방안 마련 필요

참고문헌

- [1] 금융보안원
- [2] 네이버 지식백과, 위키백과
- [3] <https://www.boannews.com/media/view.asp?idx=111425>
- [4] https://www.siren24.com/mysiren/life24/sir_h0901_view.jsp?life24No=5201
- [5] https://blog.naver.com/doctor_soft/222932160115

챗GPT 등장에 따른 보안 이슈



챗GPT(ChatGPT)의 이해

- 챗GPT는 세계 최대의 AI 연구소인 오픈AI(OpenAI)가 개발한 자연어 처리 인공지능 모델 GPT-3.5를 기반으로 제작한 대화형 챗봇(Chatbot) 서비스
- 기존의 챗봇과 다르게 표면적인 정보 뒤에 숨어 있는 맥락을 이해하고, 과거 대화 기록을 기억함으로써 단순 정보 전달이 아닌 사람과 나누는 것과 유사한 수준의 대화를 진행함
- 챗GPT의 주요 기능으로 ① 문서 생성, ② 질문에 답변, ③ 대화형 AI, ④ 번역, ⑤ 텍스트 요약, ⑥ 코드 생성 등이 가능

챗GPT의 원리

- 챗GPT는 생성 AI*의 대표적 모델인 GPT(Generative Pre-trained Transformer) 기술을 기반으로 하는데, GPT는 말 그대로 '자가학습하여 답변을 '생성'하고 대량의 데이터와 맥락을 처리할 수 있는 '트랜스포머(변환기)' 기술임

* 생성 AI(Generative AI) : 이용자의 특정 요구에 따라 결과를 생성해내는 인공지능

※ GPT 시리즈

모델명	출시시기	파라미터 수	특징
GPT-1	2018년	1,700만 개	Unlabeled 데이터 학습, 특정 주제에서의 분류, 분석 등의 응용 작업 가능
GPT-2	2019년	15억 개	비지도 학습 기반으로 패턴 인식하여 대용량 데이터 학습이 가능
GPT-3	2020년	1,750억 개	자가학습(Self-attention) 레이어를 많이 쌓아 파라미터 수 100배 이상 증가 사람처럼 글 작성, 코딩, 번역, 요약 가능
InstructGPT	2022년	1,750억 개	인간 피드백 기반 강화학습(Reinforcement Learning with Human Feedback, RLHF) 적용으로 답변 정확도와 안정성 급증
GPT-3.5	2022년	1,750억 개	InstructGPT와 같은 RLHF 기반 모델 학습

- 챗GPT의 원리는 크게 대규모 언어 모델(Large Language Model, LLM)과 인간 피드백 기반 강화학습(Reinforcement Learning with Human Feedback, RLHF)로 구분
- 대규모 언어 모델(Large Language Model, LLM)은 일련의 단어에서 다음 단어를 예측하고 다음 문장을 예측하는 작업을 수행함. 이 기능을 통해 사용자들은 단락 뿐만 아니라 여러 페이지의 콘텐츠를 작성함. 그러나, 인간이 원하는 것을 항상 정확히 이해하지 못한다는 점에서 한계가 있음

- 이 한계점은 인간 피드백 기반 강화학습(Reinforcement Learning with Human Feedback, RLHF) 훈련을 통해 기술 수준을 개선함. 이는 사용자의 지시를 따르고 의도에 적합한 반응을 생성하는 능력을 만들기 위해 인간 피드백을 이용한 강화 학습 훈련임



챗GPT(ChatGPT)의 보안

- 챗GPT는 빅데이터에 대한 자가학습 능력 기반으로 새로운 창작물을 생성할 수 있어 다양한 산업에 큰 영향을 줄 것으로 예상
- 특히, 챗GPT는 코드를 생성하거나 프로그래밍 언어 변환 등 악성코드를 쓸 수 있는 능력을 가지고 있어 보안 업계에 위협

챗GPT의 보안 이슈

- **낮아진 사이버 범죄 진입 장벽**: 전통적으로 사이버 범죄는 숙련된 기술과 비용 등이 필요하지만 텍스트 입력만으로 악성 코드를 생성해낼 수 있는 챗GPT로 인해 진입 장벽이 크게 낮아짐
- **설득력 있고 정교한 피싱 이메일 등장**: 사람과 구분할 수 없을 정도의 정교한 글을 작성하는 챗GPT로 인해 큰 문제점으로 꼽히는 것이 피싱 메일이며 가장 많이 보고된 사례이기도 함
- **AI 지식을 갖춘 보안 전문가 필요성 대두**: 챗GPT로 인한 사이버 보안 문제는 아직 초기 단계에 불과하며 향후 새로운 차원의 문제가 불거지면, 전문 AI 지식을 갖춘 보안 담당자가 반드시 필요함
- **생성 AI의 출력 모니터링 필요**: 챗GPT는 의식하지 못하는 사이에 기업 정보를 외부로 노출할 수 있는 위험이 있어, 생성한 콘텐츠를 철저히 모니터링하는 것이 필수임
- **급속한 공격량 증가에 따른 문제**: 챗GPT는 텍스트 프롬프트 하나만으로, 피싱 이메일을 쉽게 대량으로 발송할 수 있으므로 공격량이 급속히 늘어나는 것이 문제임
- **산업계 보안 비중 증가 전망**: 산업계는 챗GPT 같은 생성 AI 도입에 보안을 가장 우선할 것이며, 이를 효과적으로 통제하기 위해 사용 정책을 설정하고 프로세스를 구축하는 등 별도 부담이 증가할 전망
- **방어하는 인간의 부담 가중 전망**: 일반적인 사이버 범죄는 공격자와 방어자 모두 모범 사례를 통해 기술을 발전시키나, 챗GPT는 공격자가 AI로 이를 방어하는 인간의 부담이 가중될 전망

참고문헌

- [1] 네이버 지식백과, 위키백과
- [2] <https://seo.tbwakorea.com/blog/what-is-chatgpt/>
- [3] <https://www.openads.co.kr/content/contentDetail?contsId=10238>
- [4] <https://www.aitimes.com/news/articleView.html?idxno=150123>
- [5] <https://www.pwc.com/kr/ko/insights/insight-flash/chat-gpt.html>

사이버 보안 표준 및 관련 특허 동향

웍스온벨류(worksonvalue)

지관영 변리사

1 서론

사이버 보안 기술은 매우 넓은 범위에서 다양한 기술들을 포괄한다. 예를 들어 사이버 보안 기술은 컴퓨터 시스템이나 네트워크의 하드웨어나 프로그램이나 애플리케이션 등 소프트웨어 등 공격으로부터 보호하는 기술들로 매우 넓은 범위를 가진다. 예를 들면, 방화벽, 침입탐지 및 방지 기술, 가상망(VPN), 암호화 및 디지털 서명, 멀웨어 및 바이러스 검사 등이 이에 해당할 수 있다.

사이버 공격은 중요한 정보를 액세스, 변경, 삭제하고 사용자가 정상적인 비즈니스 활동을 하지 못하게 하는 등의 돌이킬 수 없는

손해를 입히고 있다. 사이버 범위는 심각하게 증가하고 있고 매우 정교해지고 있으며, 최근에는 필자가 속한 특허업계에도 사이버 공격에 따른 중대 피해가 발생 소식들이 들리고 있다. 정보의 디지털 전환이 추세 속에서 디지털 데이터의 양이 기하급수적으로 늘어나면서 관련된 공격 타입들도 늘어나고 있다.

따라서, 사이버 보안 기술은 전 세계 정부 비즈니스 업계가 해결해야 하는 중요 과제로 본격적으로 인식되고 있다. 사이버 공격 타입들이 다양해짐에 따라 시스템과 소프트웨어를 보호하는 사이버 보안 기술들도 함께 다양한 관점에서 여러 기술이 개발되고 논의되고 있다. 사이버 보안 기술도 여러 표준 단체에서 표준화가 진행 중이고 위에서 설명한 바와 같이 그 범위가 매우 넓고 다양하여 여기에서는 표준화 기술 중 일부 기술들과 관련된 특허 동향에 대해 소개하고자 한다.

2 사이버 보안 관련 표준화 기술 표준화 단체 및 표준화 기술 소개

사이버 보안 기술의 특허 동향을 살피기에 앞서 사이버 보안 표준 단체들과 단체들이 다루는 기술들을 간단히 소개하면 다음과 같다.

(A) ISO/IEC JTC 1/SC 27

ISO/IEC JTC 1/SC 27(이하, ISO/IEC)는 정보/ICT 보호를 위한 표준 개발을 다루고 있으며 일반적인 보안 개인 정보 보호 측면을 일반적인 방법, 기술 및 지침이 포함한다. 예를 들면, ISO/IEC는 보안 요구 사항, 보안 관리 시스템, 보안 프로세스, 정보의 책임, 가용성, 무결성 및 기밀성을 보호하는 암호화 관련 메카니즘, 신원 관리, 생체 인식 및 프라이버시의 보안 및 이를 평가, 인증 감사하는 요구사항들을 다루고 있다[1].

특허 동향 조사를 위해서 특별히 어떤 기술이라고 제한하기 어려운 넓은 범위의 기술 및 요구사항들이 ISO/IEC에서 논의되고 있다.

아래 소개되는 정보 및 IT 보안 표준의 기술 개발을 다루는 5개의 메인 워킹 그룹 이외에 인증과 조직 운영과 관련된 여러 그룹들이 포함된다. ISO/IEC JTC 1/SC 27의 주요 워킹 그룹과 주요 주제를 소개하면 다음과 같다[1].

표 1 ISO/IEC JTC 1/SC 27 working groups

Reference Group	Title
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies



(B) IEEE SA Cybersecurity Standards

IEEE SA는 사이버 보안 표준화를 위한 여러 가지 프로그램 포트폴리오를 제공하는데 목표를 둔다. 예를 들어 IEEE 사이버 보안 표준 컬렉션은 프레임워크, 암호화 자산, 데이터 인증, 전자 상거래, 사물 인터넷 (IoT), 상호 운용성, 전방향성, 공급망 및 감시의 품질을 개선하도록 설계된 사이버 보안 기술 영역의 표준을 제공한다. IEEE SA는 사이버 보안의 기술적 구현, 개인 정보 보호 및 보안의 사례와 적합성 및 테스트 관련 문제 등을 다루어 왔으며 최근에는 악성코드 분석 정보 교환 포맷 표준 등을 개발하고 있다[2].

위에 설명한 바와 같이 다양한 사이버 공격들을 막는 여러 관점의 보안 기술들은 정보 교환 포맷의 표준을 통해 그 성과들을 효율적으로 공유할 수 있다. IEEE cybersecurity standards의 일부 주요한 표준들과 관련 기술을 소개하면 다음과 같다. 위 기술에 대한 상세한 정보는 해당 웹 페이지[3]를 참조할 수 있다.

표 2 IEEE cybersecurity 주요 표준 기술

IEEE cybersecurity standards	설명
IEEE 802.1X:	이더넷 네트워크에 대한 포트 기반 네트워크 액세스 제어를 제공하는 방법을 정의
IEEE 802.11i:	무선 네트워크에 보안을 제공하는 방법을 정의
IEEE 1609.2	V2V(Vehicle-to-Vehicle) 통신에 보안을 제공하는 방법을 정의
IEEE 1619:	저장 장치에 보안을 제공하는 방법을 정의

(C) ITU-T Study Group 17-Security

ITU-T Study Group 17 (이하, ITU-T SG17)은 보안에 중점을 둔 ITU(International Telecommunication Union) 내의 그룹으로, 정보 보안 관리 시스템(ISMS) 및 기타 보안 관련 주제에 대한 표준 개발을 담당한다[4]. ITU-T SG17 그룹은 또한 통신 네트워크 및 서비스에서 보안 조치를 구현하기 위한 지침을 개발하는데, 사이버 보안, 보안 관리, 보안 아키텍처 및 프레임워크, 스팸 방지, 신원 관리, 생체 인식, 개인 식별 정보 보호, 인터넷 애플리케이션 및 Internet of Things (IoT) 서비스 보안과 같은 광범위한 보안 관련 표준화 문제를 다루고 있다[4].

ITU-T SG17의 최근 다루는 표준화 이슈들과 표준화 문서에 대해 언급하면, Recommendation ITU-T X.509은 공용 네트워크를 통한 전자 인증에 대한 권장사항으로서, 다양한 애플리케이션에서 사용되는 공개키 인프라(PKI)에 대해 다루고 있으며 웹에서 브라우저와 서버 간의 연결을 보호하고 전자 상거래의 디지털 서명에 대한 표준화 이슈를 다룬다[5].

ITU-T Recommendation의 X.1500 시리즈에서 규정된 ITU-T's Cybersecurity Information Exchange (CYBEX)는 사이버 위협 및 공격에 대한 신속하고 국제적으로 조정된 대응을 보장하는 표준으로서 컴퓨터 사고 대응팀이 요구하는 사이버 보안 정보를 교환하기 위한 표준화된 수단을 제시한다. 권장 사항 ITU-T X.1215는 STIX(Structured Threat Information Expression) 언어를 사용하여 사이버 위협 정보 및 정보 공유를 지원하는 방법에 대한 다양한 사용 사례를 제공한다. 그리고 Recommendation ITU-T X.1205는 사이버 보안의 정의와 보안 위협의 분류 체계를 제공하여 다양한 네트워크 계층의 위협과 해커가 사용하는 가장 일반적인 도구를 제공한다[5].



그 밖에 통신 네트워크 운영자와 기업이 보안 관점에서 엔드 투 엔드 아키텍처 설명을 자세히 설명할 수 있는 기능을 정의하는 Recommendation ITU-T X.805, 기밀성, 무결성 및 가용성을 비롯한 기본 정보 보안 관리 요구 사항을 충족하기 위한 지침을 제공하여 통신 조직의 정보 보안 제어를 구현하는 Recommendation ITU-T X.1051, 엔터티의 디지털 신원 확인을 지원하는 엔터티 인증 보증 프레임워크를 제공하는 Recommendation ITU-T X.1254, 및 보안 정보를 교환하기 위한 XML 기반 프레임워크인 보안 주장 마크업 언어(SAML 2.0)를 정의하는 Recommendation ITU-T X.1141등 매우 많은 표준과 기술들을 다루고 있다[6].

이렇게 많은 사이버 보안 분야들과 세부 기술은 보안 관점에서 매우 많은 데이터와 행위를 분석하고 그에 기반한 새로운 정보를 생성하고 있다. 이렇게 여러 표준 기술들이 논의되고 있다는 사실은 사이버 보안이 소수의 국가들, 소수 기업들의 기술적 관점이나 능력에 의해 주도되는 분야가 아니고 여러 기업들의 기술들 및 스타트업 단체들의 복합적인 노력과 협업에 의해 이루어질 수 있다는 것을 반증한다.

전세계가 연결된 디지털 세상 속에서 여러 단체들의 협업과 노력에 의해 지켜질 수 있는 사이버 보안의 특성 때문에 통일적인 사이버 공격과 보안 대응 지침은 더욱 중요하다. 그런 관점에서 비영리 표준화 단체 중 하나인 OASIS Open을 소개할 필요가 있다.

(D) OASIS Open (이하, OASIS)

OASIS는 구조화된 정보 표준 발전을 위한 비영리 조직으로, 사이버 보안, 블록체인, 사물 인터넷(IoT), 비상 관리, 클라우드 컴퓨팅, 법적 데이터 교환, 에너지, 콘텐츠 기술 및 기타 분야의 공개 표준 채택하도록 하는 오픈 표준화 기구이다. OASIS는 자신의 웹페이지에서 오픈 소스 프로젝트를 포함한 프로젝트에 국제 정책 및 조달 참조를 위한 표준화 및 정당한 승인을 위한 경로를 제공한다고 소개하고 있다[7].

OASIS는 회원 개발 작업을 위한 기술 위원회(Technical Committees; TCs), 오픈 소스 커뮤니티를 지원하는 오픈 프로젝트, 및 ISO에 대한 기술 자문 그룹 등 다양한 공개 협업 프로젝트들을 지원한다[8].

OASIS의 여러 개의 TC들 중 사이버 보안 상황 인식, 실시간 네트워크 방어 및 정교한 위협 분석을 위한 자동화된 정보 공유를 지원하는 기술 위원회(TC)로서 OASIS Cyber Threat Intelligence(CTI) TC가 있다[9]. 사이버 위협 인텔리전스는 최근 사이버 보안 업계의 떠오르는 이슈인데 이에 관련해서는 특히 동향 분석에서 다시 언급한다.

실시간 방어 및 정교한 위협 분석에 대한 정보 공유를 빠르게 지원하기 위해서는 효율적인 정보 공유 수단이 필요하다. OASIS Cyber Threat Intelligence(CTI) TC는 이러한 정보 공유를 위해 STIX 및 TAXII 표준을 논의 이를 OASIS Committee Specifications으로 공개하였다[10].

STIX 및 TAXII는 사이버 공격의 예방 및 완화를 개선하기 위해 개발된 표준으로 설명된다. STIX(Structured Threat Information eXpression)는 사이버 위협 인텔리전스를 구조화된 방식으로 기술하기 위한 언어로서 사이버 위협 및 관찰 가능한 정보를 표현하며 현재 STIX2.1까지 개발된 상태이다.

그리고, TAXII(Trusted Automated eXchange of Intelligence Information)는 조직 간에 사이버 위협 인텔리전스를 공유할 수 있는 일련의 서비스 및 메시지 교환인 지표 정보의 신뢰할 수 있는 자동화된 교환방식을 지칭한다. 이전 공유 방법과 달리 STIX 및 TAXII는 기계 판독이 가능하므로 쉽게 자동화되는 특징을 가지고 있다[11].

STIX와 TAXII는 업계에서 사이버 공격에 대한 정보를 공유하고 이를 전달하기 위해 업계에서 널리 사용되고 있어서 사실상 표준으로 역할을 하고 있다.

사이버 보안 업계가 매우 많은 업체들이 자체 개발한 다양한 기술들 기반으로 악성 코드, 악성 행위 및 공격 기법들을 서로 다른 방식으로 기술하고 있는 것을 감안할 때 이러한 정보 공유 체계의 일부로서 STIX와 TAXII의 위상은 더욱 넓어질 것으로 판단된다.

이와 같은 사이버 보안의 정보 공유 체계의 발전은 사이버 위협에 대한 정보 공유 기능을 확장시키고, 선제적 대응을 가능하도록 하였다. 이를 기반으로 사이버 위협 인텔리전스는 더욱 발전할 수 있는 계기가 되었다. 이하에서는 본격적으로 사이버 위협 인텔리전스의 특히 동향에 대해서 기술하기로 한다.

3 사이버 위협 인텔리전스 관련 특히 동향

1) 사이버 위협 인텔리전스(CTI) 관련 기술 소개

사이버 위협 인텔리전스의 특히 동향에 대해 설명하기에 앞서 사이버 위협 인텔리전스를 구성하는 기술들을 살펴봐야 한다.

위에서 설명한 바와 같이 사이버 보안과 관련되어 개발된 여러 가지 기술들은 단편적인 사이버 공격의 탐지 또는 대응에 관한 일차원적인 기술에 집중되어 있지만, 사이버 위협 인텔리전스(CTI)는 위협 정보를 수집해 상황을 전반적으로 분석하고, 위협에 효과적이고 종합적인 대응하는 방법을 지칭한다.

특히 사이버 위협 인텔리전스는 보안 전문가들이 사이버 공격자의 행동과 의도를 이해하고, 이를 예방하고 대응하기 위해 사용된다[12]. 또한 사이버 위협 인텔리전스(CTI)는 보안 위협에 대한 정보를 수집하고 분석하여 기업의 보안 수준을 높이는 데 도움을 줄 수 있다[13].

사이버 위협 인텔리전스는 외부 위협과 내부 로그 파일을 처리하여 보안 팀을 위해 우선 순위가 지정되고 상황에 맞는 알림을 생성하거나 보안 대응 도구를 강화할 수 있도록 돕는다. 일부 사이버 위협 인텔리전스 플랫폼의 운영 기업과 플랫폼들의 기술 특징들을 정리하면 다음과 같다[14].

표 3 CTI 제공 주요 기업, 플랫폼 및 기술 특징

기업	CTI 플랫폼 명칭	정보 공유 관련 주요 기술 특징
Anomali	Anomali ThreatStream	• 기계 학습(ML) 알고리즘을 사용하여 위협의 심각도를 반영한 점수의 신뢰도 • 글로벌 위협의 MITRE ATT&CK 매핑 • 2,000개 이상의 조직과 위협 가시성 공유
IBM	X-Force Exchange	• 플랫폼 타 사용자와 위협 인텔리전스 협업 정보 공유 • 타임라인 보기를 사용하여 시간 경과에 따라 변화하는 위협 수준 관찰 정보 • IP 주소별 인텔리전스 및 URL 평판
IntSights	Threat Intelligence Platform	• 실시간 위협 우선 순위 지정 • 맬웨어, 피싱사기 및 위협 행위자(공격자) 조사 • 통합되고 효율적인 위협 관리를 위해 기본 IoC (침해 지표) 집계
LookingGlass	Cyber Solutions	• 공격, 조직의 환경 및 위협 환경을 기반으로 위협 순위에 대한 신뢰도 점수 • 자산을 그룹 및 하위 그룹으로 분류하여 분류된 위협 프로필을 모니터링 • 알려진 명령 및 제어 노드 연결을 감지하기 위해 인터넷에 액세스할 수 있는 자산 및 네트워크를 모니터링
Recorded Future	Recorded Future	• 신원을 모니터링하고 잠재적으로 손상된 계정에 대해 경고 • 조직의 공격을 탐지하고 모니터링 • 다크 웹소스에 대해 사전적 예방이 가능한 모니터링
SolarWinds	Security Event Manager	• 규정 준수를 위한 주문형 자동 보고서 • 자동화된 위협 탐지 및 대응 기술
ThreatConnect	ThreatConnect	• 선제적이고 자동적인 보안을 위한 로우 코드 자동화 • 위협 확산 분석

위와 같은 기업 및 플랫폼 이외에 CTI 분야의 가장 오래된 기업 중의 하나로 Symantec 등의 기업이 있으며, CrowdStrike의 Falcon, FireEye의 iSIGHT, Palo Alto Network의 AutoFocus, Cisco의 SecureX (이전의 Threat Response) 등이 사이버 위협 인텔리전스(CTI) 또는 그와 관련 서비스를 제공하고 있다.

2) CTI 관련 특허 동향 조사

(A) 특허 동향 조사 방법

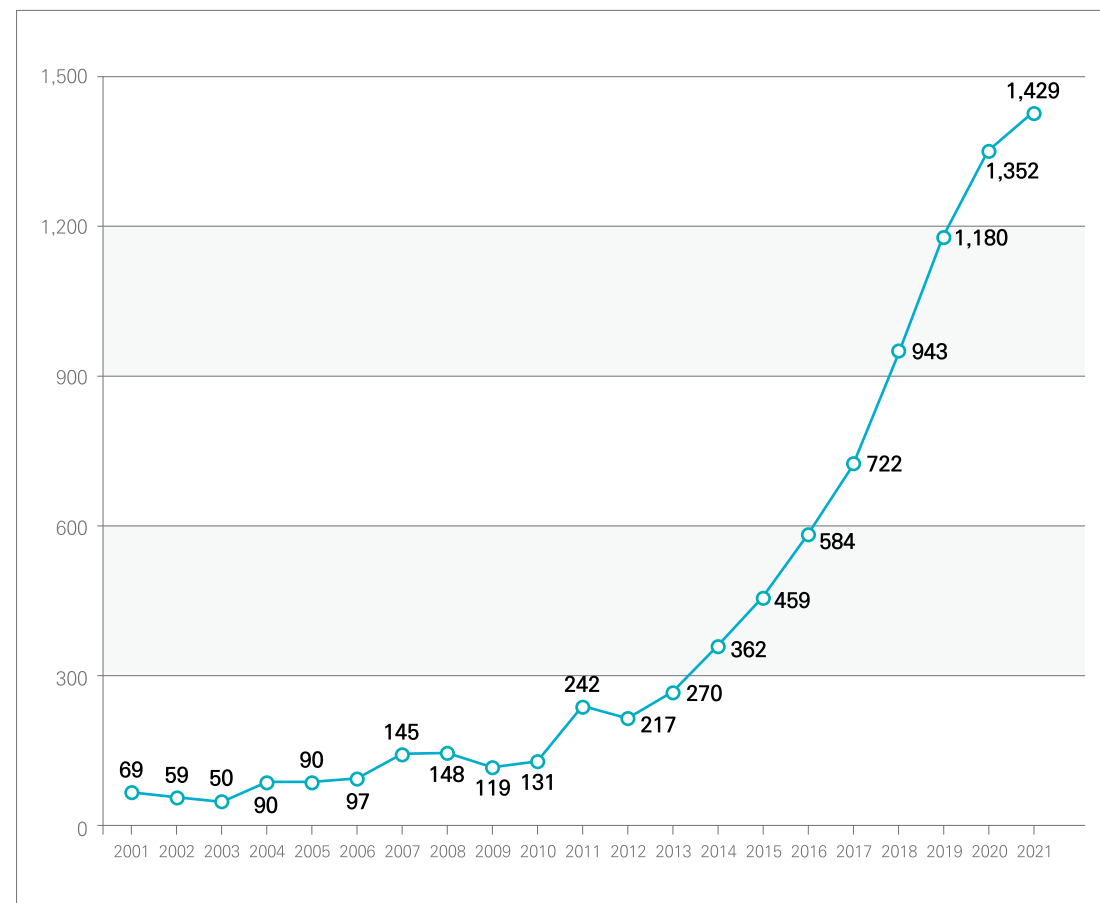
CTI 관련 특허를 조사하기 위해 가능한 광범위한 국가와 검색식을 이용하였다.

- 검색틀: 키워트 또는 google patent advanced search
- 출원국가: 미국, 한국, 일본, 중국, 유럽, PCT
- 검색식: 검색식은 핵심 키워드 (intelligence, platform, malware, malicious, attack, threat 등)을 적절히 조합한 결과를 사용하였고, 중복제거와 필터링을 통해 비이상적인 노이즈 세트는 제거하였다.

(B) CTI 관련 기술의 연도별 동향

먼저 CTI 관련 기술의 연도별 동향을 살펴보면 다음과 같다. 단편적인 악성행위 또는 공격 행위에 중점을 둔 기존의 기술과 다르게 사이버 위협 인텔리전스 또는 위협 인텔리전스 플랫폼 기술은 복합적인 악성 행위의 대응에 초점을 둔다. 이러한 인텔리전스 시스템을 구축하기 위해서는 역시 많은 컴퓨팅 리소스가 필요한 경우가 많다. 대규모 데이터 처리를 통해 빅데이터에서의 공격 행위에 대한 인사이트를 얻어야 효율적인 인텔리전스 시스템 구축이 가능하다. [그림 1]에서 확인하는 바와 같이 2015년 이후 위협 인텔리전스 기술은 매우 가파르게 증가하고 있음을 알 수 있다.

그림 1 CTI 관련 기술의 연도별 동향



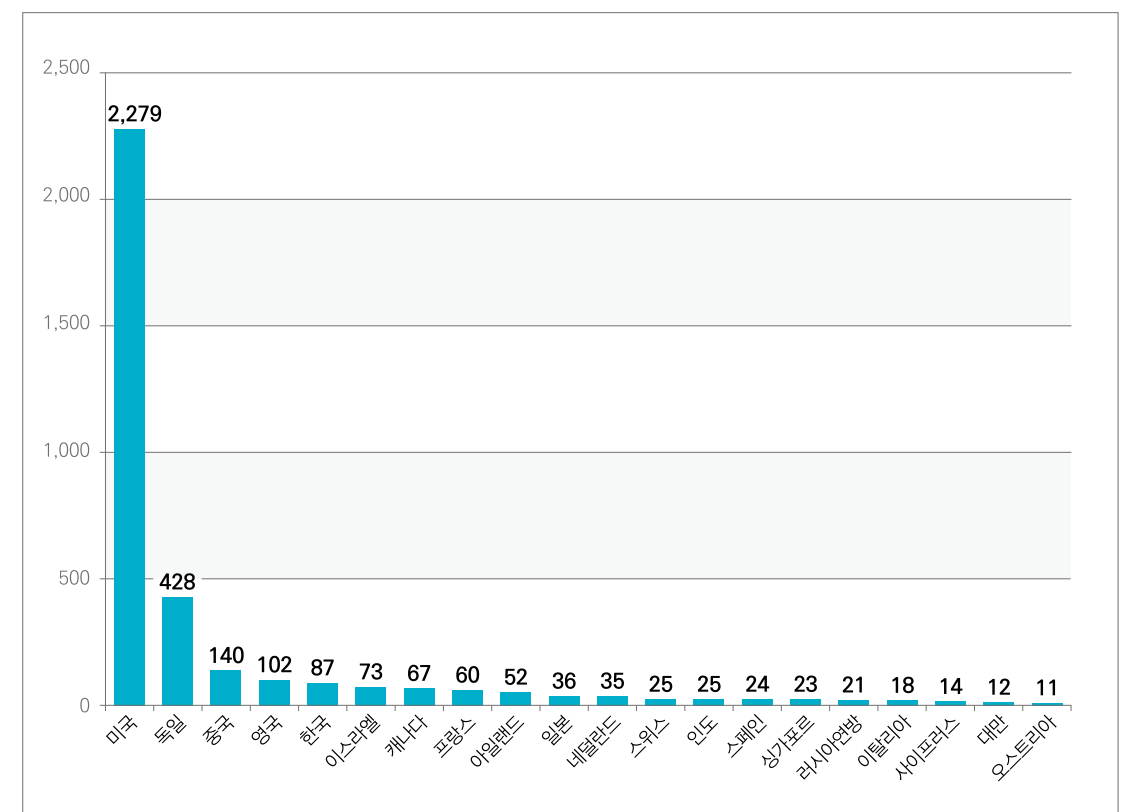
특허동향조사를 진행한 2023년 5월로부터 역산하면 2021년 특허출원 수는 미공개 출원들의 수를 반영하지 못한다. [그림 1]을 참조하면 2021년에 출원되어 공개된 출원의 수는 2020년에 출원된 특허출원보다 많다는 사실을 알 수 있다. 이로부터 사이버 위협 인텔리전스에 관련된 특허출원은 현재 시점에서 매우 집중적으로 개발되는 분야이며 보안 기업들이 기술 개발에 힘을 쓰는 분야임을 간접적으로 확인할 수 있다.

(C) CTI 관련 기술의 출원 국가 동향

언급했듯이 CTI 관련 기술은 시스템마다 복합적인 기술들이 포함되어 있다. CTI 관련 기술은 AI 기술을 접목하여 대규모 데이터를 여러 가지 보안 관점들에서 처리하면서 공격 행위에 대한 추세를 들여다보고 이에 대한 대응 방안을 제공하는 경우가 많다. 따라서 자연히 대규모 데이터가 확보가 가능한 컴퓨터 기술을 개발해 왔고, AI 기술을 빠르게 접목시킬 수 있는 국가의 출원이 많은 것으로 예상되었다.

실제로 조사된 CTI 관련 기술의 출원인의 국가를 살펴보면 위와 같은 기술이 많이 발전한 미국의 출원이 압도적인 사실을 알 수 있다. 이로부터 미국의 기술이 사이버 위협 인텔리전스 시장을 선도하고 있다는 것을 알 수 있다.

그림 2 CTI 관련 기술의 출원인 국가 동향



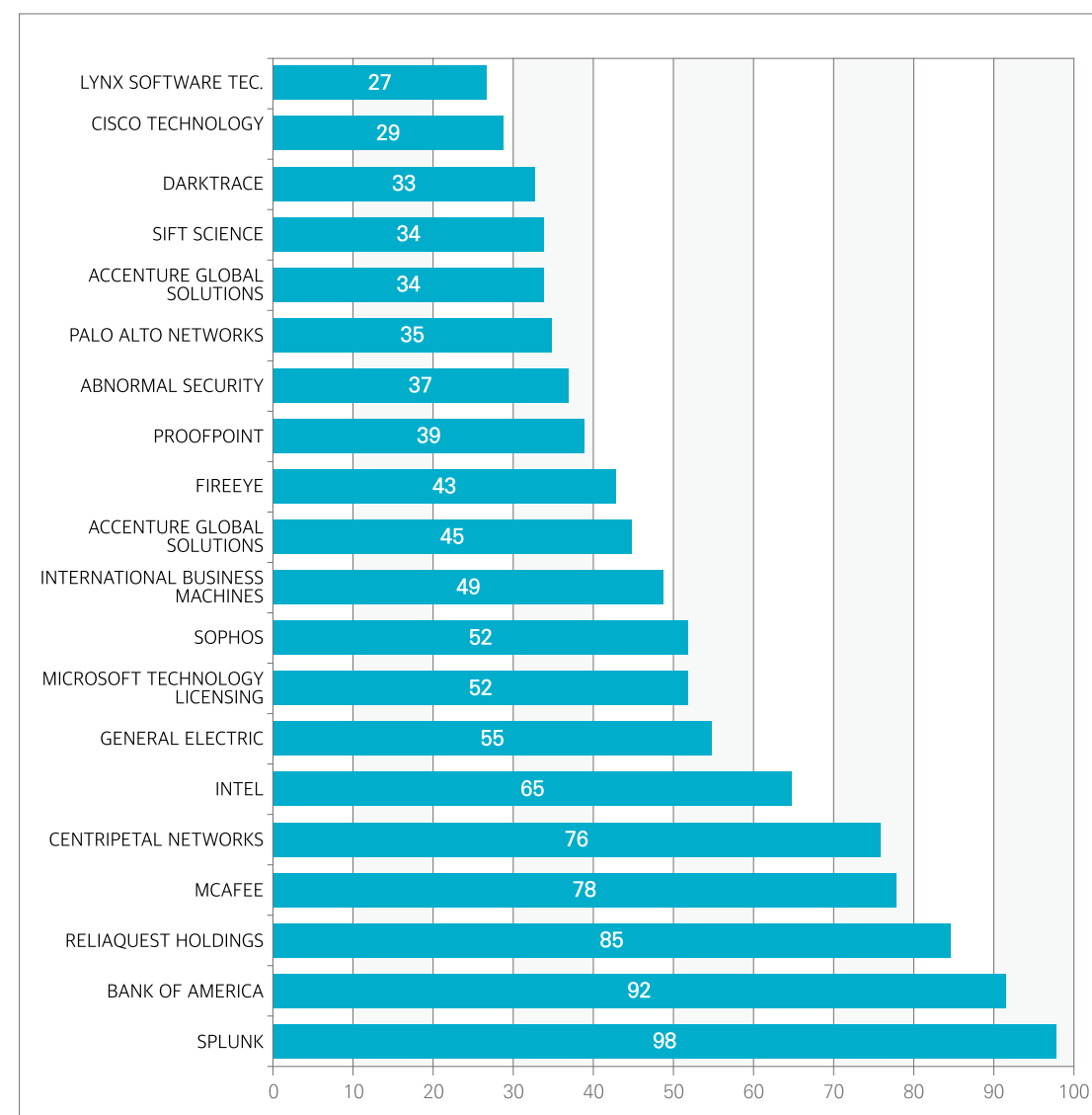
아마존, 구글, MS, IBM 등 미국의 대표 클라우드 기업들이 AI 기술과 대규모 데이터 처리 기술을 개발하고 있다는 것은 매우 잘 알려진 사실이다. 그렇기 때문에 그러한 대기업들 또는 그 대기업들과 협력하는 사이버 보안 업체의 기술 개발이 매우 활발할 것이라고 추측할 수 있다.

(D) CTI 관련 기술의 주요 출원인 동향

그러면 실제로 미국의 사이버 보안 기업들이 CTI 관련 기술을 주도하고 있는지 출원인별 동향을 조사하였다. 가장 많이 출원을 진행한 기업은 Splunk Inc.로 조사되었다. Splunk Inc.는 캘리포니아주 샌프란시스코에 본사를 둔 미국 소프트웨어 회사로 스타일 인터페이스를 통해 기계 생성 데이터를 검색, 모니터링 및 분석하기 위한 소프트웨어 및 비즈니스 운영을 위한 인텔리전스를 제공한다[15].

위에서 대규모 클라우드 회사로 언급한 IBM, MS과, 대표 보안 업체로 뽑히는 McAfee, Sophos, Fireeye, Palo Alto network 등의 회사도 관련 기술을 많이 출원하는 출원인으로 아래 그래프에서 찾을 수 있다.

그림 3 CTI 관련 기술의 출원인별 동향



이와 같이 사이버 위협 인텔리전스 기술은 최근 빠르게 발전하는 AI 기술을 접목하여 기존과 다른 수준으로 보안 대응 체계를 제공하고 있다. 이러한 보안 대응 체계는 위에서 설명한 정보 공유 표준 기술인 STIX나 TAXII 등의 표준 정보 체계를 통해 다른 기업들과 사용자들에게 보안 대응 정보를 제공하게 될 것이다.

4 마치며

살펴본 바와 같이 사이버 보안 기술과 관련하여 표준화 단체를 살펴보았다. 기술이 발전하면서 IoT, 5G, 클라우드 등 새로운 기술이 등장할수록 이와 관련된 표준 보안 주제는 역시 새롭게 준비되어야 한다. 따라서 표준화 단체에서 논의되는 표준 기술들은 매우 다양한 기술들로 분류될 수 있다.

여러 가지 기술들에 따라 보안 위협들은 여러 측면에서 문제를 발생시킨다. 그리고 이러한 보안 위협들을 해결하기 위한 보안업체의 기술들도 여러 관점에서 진행되고 있어서 메인 기술 특징을 골라내기 매우 어려운 기술분야이기도 하다. 개별적인 보안 문제들은 보안 대응 관리자에게는 일관되고 종합적인 해결 수단을 요구하는 상황을 만든다.

근래에는 이러한 단편적이고 개별적인 기술 해결 수단이 아닌 종합적인 보안 솔루션으로서 사이버 위협 인텔리전스가 등장하고 있다. 사이버 위협 인텔리전스는 이러한 다양한 보안 문제들을 종합적으로 해결하고 대응하기 위한 체계라고 할 수 있다.

검색 출원 수의 조사에서 알 수 있듯이 사이버 위협 인텔리전스는 당분간 선두 보안 업계의 주요한 기술로 자리잡을 것으로 예상된다. 사이버 위협 인텔리전스는 선두 보안 업체들이 위치한 미국에서 크게 성장하고 있으며 인터넷으로 연결된 디지털 세상에서 이러한 기술들 중 일부는 전세계 표준화 기술로 등장할 것이다.

현실적인 예로서 OASIS의 정보 공유 체계인 STIX2.1은 그대로 ITU-T SG17의 표준화 과제로 진행 중이고, 표준화 절차에 따라 국제표준으로 자리잡을 가능성이 매우 높다.

사이버 위협 인텔리전스에 필요한 요소 기술로서 표준 기술이 채택되기에 앞서 한국의 보안업체도 이에 대한 논의에 뛰어들어 표준 기술을 확보하고 사이버 위협 인텔리전스의 고도화에 힘써야 할 시기로 생각된다.

참고문헌

- [1] <https://www.iso.org/committee/45306.html>
- [2] <https://engagestandards.ieee.org/cybersecurity.html>
- [3] <https://cybersecurity.ieee.org/standards>
- [4] <https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx>
- [5] <https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx>
- [6] <https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx>
- [7] <https://www.oasis-open.org/org/>
- [8] <https://www.oasis-open.org/projects-committees/>
- [9] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
- [10] <https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis-committee-specifications/>
- [11] <https://www.anomali.com/resources/what-are-stix-taxii>
- [12] <https://kr.analysisman.com/2021/01/cti-cyber-threat-intelligence.html>
- [13] <https://www.itworld.co.kr/news/288139>
- [14] <https://www.esecurityplanet.com/products/threat-intelligence-platforms/>
- [15] <https://en.wikipedia.org/wiki/Splunk>

샌즈랩

샌즈랩

김기홍 대표이사

1 샌즈랩 소개

당사는 사이버 위협 인텔리전스(CTI, Cyber Threat Intelligence) 전문기업으로서 다양한 채널로부터 수집한 악성코드 등의 사이버 위협 정보를 인공지능, 빅데이터를 활용한 자체 분석 기술을 활용하여 자동 분석하고 이를 기반으로 생성된 사이버 보안 위협 대응, 예측을 수행할 수 있는 인텔리전스를 고객에게 제공하는 사업을 영위하고 있습니다.

당사는 매일 고도화되고 첨단화 되어 가는 사이버 보안 위협에 즉각적이고 능동적인 대응이 가능하도록 각종 ICT 인프라를 구성하는 중요 자산을 식별하고 보호하기 위한 다양한 전략을 수립하고, 현재 진행 중인 보안 위협과 공격 방향을 예측하여 효과적인 대응이 가능한 의사결정에 도움이 되는 정보와 인텔리전스를 제공합니다. 특히,

공격자와 공격기법을 식별하여 중/장기적인 전략을 수립 가능하게 가이드하고 있으며 필요한 의사 결정과 즉각적 의사 결정을 위해 당사에서 수집/분석한 인텔리전스는 누적 기준 총 300억 건에 달합니다. 이를 통해 매일 200만 개가 넘는 위협을 실시간 분석하고 있으며, 그 분석 결과를 당사의 인텔리전스 플랫폼과 다양한 전략적 보안 제품을 통해 고객에게 제공하는 일을 수행 중에 있습니다.

당사가 개발하고 생성하는 사이버 위협 인텔리전스는 직면한 사이버 위협에 대응하기 위한 단순한 몇 가지 정보의 나열만을 제공하는 것이 아닙니다. 나열된 다양한 위협 정보들 속에 포함된 내·외부 공격자의 공격 의지, 공격 목표(타겟), 공격 경로 등의 시나리오가 녹아들어 단순히 단위 객체의 대응 개념보다 사이버 위협의 시나리오 기반으로 해석할 수 있는 인텔리전스를 제공하도록 합니다. 일명 TTP(Tactics, Techniques, and Procedures) 기반의 일종의 설명 가능한 인텔리전스인 것입니다. 이를 기반으로 다양한 기술적, 운영적, 사업적인 측면에서의 리스크 관리가 가능하게 하고, 중장기적 관점의 대책을 수립할 수 있도록 제공하고 있습니다.

또한, 누적된 데이터들 속에서 추출할 수 있는 다양한 인사이트 정보를 함께 제공하여 당사의 인텔리전스를 접하는 누구나 직면하게 된 다양한 사이버 위협에 효과적인 대처와 대응을 할 수 있도록 하고, 설사 피해를 봤다고 하더라도 그 근본적인 원인을 파악하도록 하여 추가적인 피해를 막도록 안내합니다. 일종의 디지털 회복 탄력성을 스스로 높여 나갈 수 있도록 유도함으로써 원시안적 시각에서 지속해서 발생할 수밖에 없는 사이버 위협의 근원적 대응이 될 수 있도록 합니다.

당사는 설립 후 18년이 넘는 시간 동안 악성코드 분석, 추적에 필요한 핵심 기술을 연구 개발했고 이를 기반으로 당사만의 독보적 사이버 위협 인텔리전스를 제공하기 위해 『지능형 사이버보안 위협 자가 대응 에코 시스템(EES: Evolution Eco System)』이라고 명명한 철학적 메커니즘을 설계하고 개발하여 운영하고 있습니다.

자연 생태계 물의 순환을 기초로 동작하듯 당사의 체계와 시스템도 데이터를 기반으로 동작할 수 있도록 디자인했고, 이를 서비스화 시켜 malwares.com이라는 악성코드 분석 정보 제공 플랫폼을 개발, 인텔리전스를 쉽고 빠르게 사용할 수 있는 모델을 만들어 국내외 다양한 산업군에 정보 제공을 해오고 있습니다. 하루 평균 200만 개가 넘는 악성코드를 실시간으로 수집 분석하고 있으며, 지금은 약 20억 개가 넘는 악성코드를 분석하여 약 300억 개가 넘는 사이버 위협 분석 빅데이터를 확보하고 있으며, 이를 기반으로 인공지능, 프로파일링, 연관관계 분석, 공격자 역추적 등 사이버 공격, 범죄, 테러 대응에 필요한 미래 기술을 연구, 선제 적용하고 있습니다. 수집, 분석, 예측, 대응, 다시 수집의 전체 순환 구조를 인간의 개입 없이 자체적으로 구축한 플랫폼과 대응 제품을 기반으로 스스로 발전할 수 있는 체계를 구축한 것입니다.

당사의 기술은 단순히 수집된 파일의 악성 여부를 식별하는 기술을 넘어 해당 악성코드의 공격자, 제작 의도, 공격 방법, 침투 및 배포 방법, 취약점 정보, 공격자가 얻게 되는 이익, 유사한 다른 악성코드, 대응 현황 및 방법 등 하나의 코드를 분석했을 때 추출할 수 있는 다양한 정보를 바탕으로 의사 결정권자의 의사결정을 도울 수 있는 각종 인텔리전스 데이터를 생성하고 이를 효율적으로 제공하기 위한 빅데이터 플랫폼을 기반으로 축적됩니다.

생성되고 축적된 수백억 개의 인텔리전스 데이터는, 당사가 개발하고 판매하는 각종 네트워크, 엔드포인트 기반 대응 제품군에 적용되어 고객 인프라를 보호하는데 사용됩니다. 여기에서 대응하고 수집된 정보는 다시 당사의 인텔리전스에 적용되어 기존 인텔리전스를 강화하고 현재의 사이버 위협을 식별하는 정확도를 높이는데



활용됩니다. 또한, 축적된 인텔리전스를 바탕으로 앞으로 우리에게 다가올 위협을 예측하고 관련 정보를 생성하여, 선제 대응이 가능하게 합니다. 진정한 의미에서 사전 대응이 가능하도록 스스로 고도화해나갈 수 있도록 하는 것입니다.

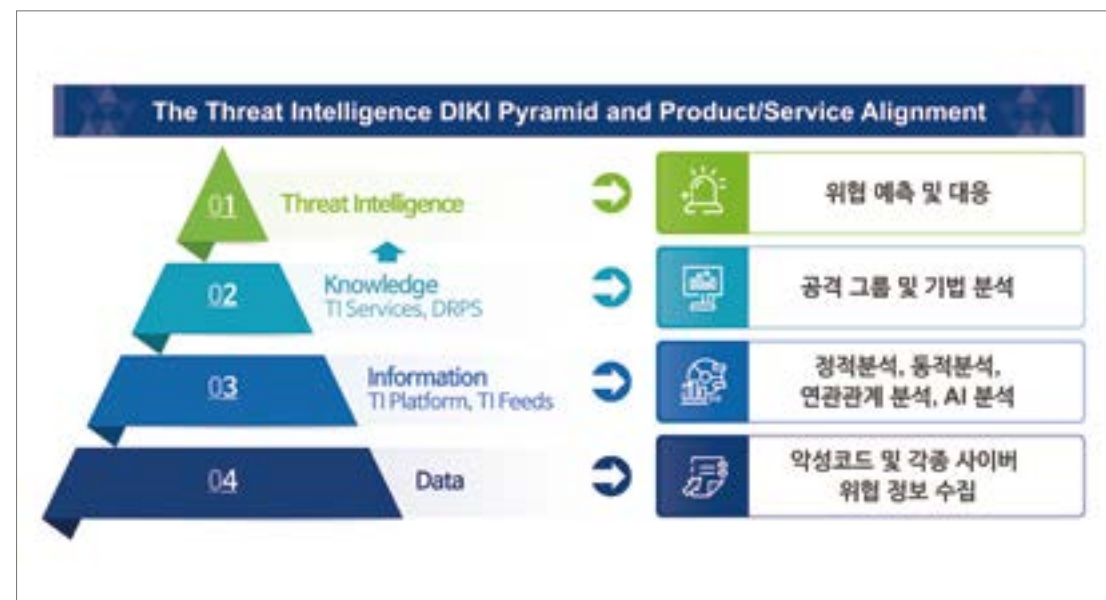
이를 기반으로 끊임없이 발생하는 매일 첨단화되고 고도화되는 사이버 위협에 능동적으로 대응하며 당사의 사이버 위협 인텔리전스 플랫폼은 무한 성장할 수 있도록 하였으며, IT 기술 대상의 단순 정보보호의 개념을 넘어 인간 삶의 영원한 발전을 안정적으로 도모해 나갈 수 있도록 하는 일종의 디지털 안전의 개념으로 확대해 나갈 수 있도록 합니다.

2 연구 중인 R&D 활동 분야

당사는 사이버 위협 인텔리전스 서비스 및 솔루션을 개발 및 제공하는 하는 것을 주력 사업으로 영위하고 있으며, 양질의 CTI(Cyber Threat Intelligence)를 제공하기 위해 최대한 기술을 자동화하고 인간의 별다른 개입 없이도 질 좋은 데이터를 생성할 수 있도록 플랫폼화한 EES(Evolution Eco System)를 구축하였습니다.

사이버 위협 인텔리전스(Cyber Threat Intelligence)는 전 세계에서 일어나는 모든 위협 정보를 수집하고 분석한 다음 여기서 얻은 지식을 활용해 사이버 위협에 대응하는 것을 의미합니다. 즉, 경험을 통해 얻은 지식에 분석력을 더해 '지능(Intelligence)'을 추출하는 것이라고 볼 수 있습니다. 가트너의 정의에 따르면 위협 인텔리전스(Threat Intelligence)는 수집된 다양한 데이터를 바탕으로 위협 여부를 판단할 수 있는 전후 맥락, 공격 메커니즘, 각종 지표를 분석 및 추출하는 과정을 통해 의미를 부여해야 합니다. 즉, 사이버 위협 인텔리전스는 다양한 채널을 통하여 수집한 데이터를 기반으로 끌어낸 정보를 지식으로 활용해 다양한 위협을 예측하거나 공격에 대응할 수 있도록 하는 지식과 기술이라고 요약할 수 있습니다.

그림 1 사이버 위협 인텔리전스 (CTI) 개념 구성



당사는 상기 CTI 개념 구조 상 피라미드의 아래쪽에 있는 데이터 계층에 있어서 300억 개 이상이라는 국내 및 아시아에서 독보적으로 많은 기본 데이터 보유를 하고 있습니다. 또한, 매일 수백만 개의 새로운 악성코드 및 사이버 위협 데이터가 전 세계로부터 수집되고 있습니다. 수집된 악성코드는 정적분석, 동적분석 등의 단계를 거쳐 피라미드의 다음 계층인 정보의 단계로 올라갑니다. 단순히 악성코드로 의심되는 파일 여부만을 보는 것이 아니라 악성코드의 기능 및 행위 등을 세밀하게 분석하여 의미를 부여하여 정보화하는 단계로 들어서는 것입니다. 하지만 정보를 생성하는 단계에서는 기존의 알려진 악성코드에 대응하는 데에는 충분할 수 있지만 알려지지 않은 신종 악성코드에 대한 대응은 불가능합니다. 따라서 당사에서는 기존의 악성코드 분석 등을 통한 1차원적인 정보 생성을 기반으로 다양하고 입체적인 심층 분석을 통해 공격그룹 및 기법을 파악할 수 있는 지식화하는 단계로까지 발전시켰습니다. 당사에서는 위협 인텔리전스 모든 계층에 관한 기술을 축적하여서 사이버 위협 인텔리전스의 서비스를 완성하여 제공하고 있습니다.

기존 사이버보안 체계는 조직 외부의 사이버 공격으로부터 관문 상에서 조직을 방어(Passive Defense)하는 것에 중심을 두고 있습니다. 이러한 방어 전략은 조직에서 발생한 공격들만 방어 대상이 되므로 동일 업계 다른 조직에서 발생하거나, 위협 행위자들이 사용하는 최신의 공격기법에 따라 무력화될 수 있는 위험성이 큼니다. 따라서, 최신의 사이버 공격을 방어하기 위해서는 침해 정보들에 대한 방대한 데이터 수집과 고도화된 분석을 통해 위협 정보를 신속하게 확인하고 그에 관한 판단 및 대응 전략을 갖출 수 있게 해주어야 합니다.

그림 2 사이버 위협 대응 단계별 보안 기술



기존의 알려진 공격에 대한 대응 중심인 Level 1, 2단계로부터 알려지지 않은 공격 대응을 가능하게 하는 Level 4단계로까지의 발전을 보여주고 있습니다. 기존의 방화벽, 보안관제 등으로부터 시작한 보안 솔루션은 데이터 수집 및 연관관계 분석 등을 제공하는 단계로 발전하였으며 일부 솔루션들은 행위 분석에 관한 결과까지 정보를 제공하여 알려지지 않은 악성코드에 대해서 일부 제한적 대응까지 가능한 것이 현실입니다. 그러나, 당사에서는 방대한 위협 및 공격 정보에 대한 빅데이터를 기반으로 의미 있는 지식을 추출하는 분석 및 머신러닝 기술을 활용하여 알려지지 않은 신종 악성코드 등에 대한 공격을 예측하거나 대응을 가능하게 만들어 나가고 있습니다.

결론적으로 사이버 위협 인텔리전스는 보안 위협과 연관된 각종 데이터를 수집, 분석 및 처리함으로써 공격자나 공격그룹의 의도, 목적 및 방식 등을 식별하고, 효과적인 위협 대응을 위한 의사결정에 필요한 정보를 생성해주는 일련의 과정입니다. 이러한 사이버 위협 인텔리전스를 통해 각종 사이버 보안 위협으로부터 빠르고 능동적인 대응이 가능해질 수 있습니다.

사이버 보안 세계에서 지능형 지속 위협(APT: Advanced Persistent Threat)과 방어는 끊임없이 서로를 압도하려고 합니다. 공격자의 다음 움직임에 대한 데이터는 앞으로 발생할 공격에 대한 방어와 사전 대비에 중요한 정보가 될 수 있습니다. 이러한 이점들로 많은 조직은 위협 인텔리전스의 가치를 점차 중요하게 인식하기 시작하였으며, 가트너 발표에 따르면 이들 중 약 72%는 다가오는 시점에 사이버 위협 인텔리전스 도입 의사를 밝히고 기술적 검토를 진행 중입니다.

위협 인텔리전스는 각종 데이터를 처리하여 공격자를 식별하고, 관련 정보 파악, 신속한 사고대응 및 공격 행위 예측 등 보안 위협과 관련된 다양한 정보를 제공해줌으로써 모든 형태나 규모의 조직들에게 이점을 제공할 수 있습니다. 중소기업의 경우, 인텔리전스 데이터를 통해 기존에 달성하기 어려웠던 보안 수준까지 역량을 강화할 수 있고, 일정 수준 이상 규모가 있는 보안팀을 운영하는 대기업은 분석가들의 효율성을 극대화하여 보안성을 강화하고, 직·간접적으로 발생하는 각종 보안 관련 비용과 기술적 지출을 줄임으로써 기업 이익에 실질적인 도움이 될 수 있습니다.

그림 3 : 정확한 의사 결정을 위한 사이버 위협 인텔리전스의 필요성



당사가 제공하는 사이버 위협 인텔리전스는 고객이 필요로 하는 다양한 정보뿐만 아니라 심층 분석 단계에서 도출할 수 있는 데이터 기반의 인사이트, 고도화된 인공지능 기술을 통해서 추출한 다양한 예측 정보를 통해서 올바른 의사 결정을 통해 사이버 위협에 대한 일관적이고 효율적이며 장기적 관점의 관리가 가능하도록 제공하고 있습니다. 이를 통해 단기적 대응 및 중장기적 관점에서 종합적인 대응과 리스크 관리가 가능하도록 하여 고객 내부에 존재할 수 있는 다양한 사이버 보안 위협에 대한 좀더 근본적인 대응이 가능하도록 가이드 합니다.

EES(Evolution Eco System)은 회사의 사이버 위협 인텔리전스 플랫폼을 관통하는 기본적인 개념으로서 일반적인 자연 생태계는 대기, 물, 토양을 기반으로 한 무기 환경과 동물, 식물 등의 각종 생명체로 구성되어 있습니다. 이들 간에 유기 물질 상호 교환을 기반으로 무한 순환 구조를 통해 생태계는 유지되며 지속 발전되어 왔습니다.

당사가 속한 분야 또한 기하급수적으로 증가하고 있는 사이버보안 위협에 능동적인 대응이 가능하기 위해서는 필요한 시점에 정확하고 신뢰성 있는 인텔리전스를 생성하여 제공할 수 있어야 합니다. 이를 위해서는 전 세계에서 수집되는 다양한 위협을 동시다발적으로 분석하고 이들의 연관성을 파악하여 제공해야 하는데 인간이 일일이 개입해서 하나씩 만들어서는 물리적으로 불가능한 환경입니다. 그래서, 당사는 자연의 생태계 시스템을 모델링하여 데이터를 기반한 순환 구조를 모티브로 개발해야 했으며, 이 순환 구조 내부에서 개별 시스템을 고도화하여 인간의 개입을 최소화하되, 생성되는 인텔리전스의 가치는 극대화할 수 있도록 하는 것이 당사 기술의 철학이자 최종적인 목표라고 할 수 있겠습니다.

이를 가능하게 하기 위해 먼저 전 세계에서 수집되는 다양한 사이버 위협 정보를 실시간으로 수집하고, 수집한 정보의 특징을 파악하여 잘 분리하고 분류합니다. 분류된 정보는 자체적으로 개발한 다양한 시스템을 통해서 분석을 수행하게 되고, 분석된 정보는 데이터셋 형태로 정규화 되어 저장됩니다. 저장된 데이터셋은 그 데이터셋 자체를 기반으로 다양한 활용처를 통해서 고객들에게 제공됩니다. 그리고 당사가 개발한 다양한 분석 시스템과 인공지능 모델을 통해서 적합한 인텔리전스가 생성되고 생성된 인텔리전스는 고객과 다양한 산업군에 적용되어 있을 수 있는 다양한 보안 위협에 대응하는데 사용됩니다. 산업군에 대응하면서 생성된 각종 피드백 정보는 다시 우리 제품 또는 정보 수집에 활용되고, 정보 수집의 방향성 또는 대응의 결과치, 대응 효과로 반영됩니다. 반영된 정보를 통해서 다시 정보 수집 등에 활용되고 점점 더 필요한 정보, 또는 위협에 대한 다양성 확보 등에 활용되어 당사의 플랫폼을 스스로 고도화하는데 활용됩니다.

그림 4: 샌드랩의 서비스 및 제품 구성



이러한 당사의 기술적 체계를 EES(Evolution Eco System) 이라 부르고 있으며, 이를 구성하기 위한 다양한 세부 기술을 연구하고 개발하고 있습니다.

하나의 정확한 인텔리전스를 생성하기 위해서는 추가적인 다양한 데이터와 분석 결과들이 필요하고 조금이라도 잘못된 정보를 제공하지 않기 위해 고도화시켜 나가고 있습니다. 또한, 인간이 수행하고 있는 다양한 단순 반복 업무를 인공지능이 대체할 수 있도록 구현하였고, 짧은 시간에 수많은 데이터를 보고 해석하여 생성할 수 있는 다양한 인사이트 정보 또한 인공지능이 생성할 수 있도록 구현하였습니다. 이를 통해 글로벌 최고 수준의 인텔리전스를 생성하는 데 있어 95% 이상의 자동화된 과정을 통해서 생성하게 되었으며, 인간의 개입은 최소화하고 자연적으로 데이터를 기반으로 순환되는 과정을 통해 지금 이 순간에도 위협 수집, 데이터 수집, 분석, 인텔리전스 생성, 고객에게 제공 등의 전 과정이 자동으로 이루어지고 있습니다.

표 1 사이버 위협 인텔리전스 플랫폼 데이터 처리 과정

구분		내용
1단계	수집	• 자체적으로 개발한 전문 크롤러를 통해서 웹, 다크웹, SNS, OSINT 정보를 수집
2단계	저장 → 분류	• 다양한 수집 채널로부터 동시다발적으로 수집되는 정보는 내부적으로 처리하는 JSON 형태로 변환되어 대용량 스토리지에 저장 • 검색용 인덱싱 데이터, 분석 결과 제공용 JSON 파일, 표준화된 분석 파일 등으로 저장
3단계	가공 → 분석	• 수집된 데이터를 바탕으로 본격적으로 가공하고 분석하는 단계 • 각각의 수집 데이터의 속성에 따라 기존의 분석 결과들을 업데이트하고 새로운 분석 결과를 생성하여 저장 • 악성코드의 특성상 분석을 우회하는 다양한 기술을 많이 사용하는데 당사의 플랫폼에서는 해당 기술을 무력화하여 정확하고 확실한 분석 데이터를 추출할 수 있는 환경을 구성하고 이를 통해서 분석을 수행
4단계	예측	• 다양한 인공지능 모델을 통해서 예측 정보를 생성 • 확률 정보 값과 설명할 수 있는 백데이터를 제공하여 비전문가도 당사의 인텔리전스를 기준으로 중요한 의사 결정을 정확하게 내릴 수 있도록 제공 • 생성된 정보는 표준화 포맷을 통해서 고객에게 제공되고 고객은 별다른 추가 개발이나 복잡한 연동 없이 표준화된 내용 그대로를 활용하면 되도록 정보를 제공
5단계	적용 → 평가	• 다양한 분석 정보 및 예측 정보를 포함한 인텔리전스를 고객에게 제공하고, 제공되고 적용된 결과를 피드백 • 피드백 받은 데이터는 다시 데이터 수집 단계에 적용되어 좀 더 필요로 하고, 좀 더 정확한 정보를 수집하는 데 반영이 되고 반영이 된 수집 데이터를 바탕으로 다시 전체 데이터 흐름 단계를 진행하면서 보유한 데이터들은 점차 고도화

3 표준화 활동

당사는 IP 자체의 로열티 확보가 매우 용이한 표준특허 확보 전략을 진행중으로 기술력을 바탕으로 표준특허 로열티를 확보하기 위해 여러 국내외 표준 전문가들과 협력하고 있습니다. 특히 당사는 STIX 표준과 ITU-T SG17의 표준화 기술을 타겟하여 특허 전략을 추진 중에 있습니다.

당사는 표준특허를 확보할 경우 라이선스 위탁 등의 방법을 통해 특허료(로열티)를 수취하는 등의 계획을 가지고 있습니다.

① STIX 표준화 기술 배경

STIX는 사이버보안 위협 정보를 나타내는 표준 포맷으로서, 사이버보안, 블록 체인, IoT 등에 대한 공개 표준을 논의하는 OASIS라는 단체가 개발하는 표준입니다.

CTA(Cyber Threat Alliance) 멤버 운영사들 중 샌즈랩은 최고 품질의 사이버 위협 정보를 생산하고 있으며, STIX 표준 포맷은 샌즈랩이 생산하는 유용한 사이버 위협 정보를 전부 반영하지 못하고 있습니다. 표준 정보 포맷으로서 STIX는 추가의 사이버 위협 정보의 표현을 위한 정보 오브젝트(object)를 지속적으로 개선 중인데, 당사의 핵심 기술인 AI 기반 공격자 유형 및 기법 식별 및 탐지기술을 통해 생산하는 고유의 사이버 위협 정보는 STIX 개정을 통해 반영될 확률이 매우 높은 상황입니다.

② ITU-T SG17 표준화 기술 배경

국제전기통신연합(ITU)의 전기통신표준화부문(ITU-T)은 UN 산하 정보통신기술에 대한 국제표준을 담당하는 국제전기통신연합(ITU)의 산하기관이며, ITU-T산하의 Study Group 17(SG 17)은 정보보호의 국제표준화를 담당하고 있습니다. ITU-T는 사이버 위협 정보의 공유를 위해 CYBEX(Cybersecurity Information Exchange techniques) 표준 등을 제정하였습니다.

ITU-T SG17 국제표준화 기술 아이템을 타겟한 표준특허를 확보하기 위해 당사는 ITU-T SG17 워킹 그룹과 현재 표준화 관련하여 협업을 진행하고 있으며, 한국정보통신기술협회(TTA75)) 표준자문단, 한국전자통신연구원(ETRI76)) ICT 표준화 전문가 및 한국특허전략개발원의 표준특허센터와 함께 표준특허 확보 전략사업을 진행 중에 있습니다. 또한, ITU-T SG17는 OASIS가 개발하는 STIX 표준을 국제 표준으로 추진하려는 움직임이 있습니다.

결론적으로 당사의 핵심 기술을 통해 생산하는 사이버 위협 정보는 CTA 운영사 중 최고 품질로 평가받고 있고, 공개 표준인 OASIS의 STIX에 샌즈랩 자체의 사이버 위협 정보를 추가할 수 있는 상황이며, ITU-T는 OASIS의 STIX를 국제 표준으로 추진하고 있음을 고려할 때 당사는 국제표준 특허 확보하기 최적 시점으로 판단하고 이를 확보하는 전략을 진행 중입니다.

4특허 실적

번호	등록/출원	발명의 명칭
제10-1043299호	등록	악성코드 탐지방법, 시스템 및 컴퓨터 판독 가능한저장 매체
제10-1081992호	등록	패킷 마킹을 이용한 네트워크 보안 방법 및 시스템, 그리고 이를 구현하기 위한 프로그램이 기록된 기록 매체
제10-1081993호	등록	단말에 의한 트래픽 제어를 이용한 내부 네트워크 보호 방법 및 시스템, 그리고 이를 구현하기 위한 프로그램이 기록된 기록 매체
제10-1188306호	등록	자식 프로세스를 생성하는 악성 코드 행위 모니터링 시스템 및 그 방법
제10-1188307호	등록	특정 프로세스에 대한 네트워크 행위 모니터링 시스템 및 그 방법
제10-1188308호	등록	악성 코드의 주소 결정 프로토콜 스푸핑 모니터링을 위한 가상 패킷 모니터링 시스템 및 그 방법
제10-1270497호	등록	모바일 악성코드 자동 수집 및 분석 시스템
제10-1710684호	등록	가상 환경에서는 실행되지 않는 악성 코드를 분석할 수 있는 OS 이미지의 복구 시스템 및 방법
제10-1850351호	등록	P2P 프로토콜을 이용한 loC 정보 조회 방법
US 10,341,367	등록	System and Method for Inquiring loC Information by P2P Protocol
제10-1887894호	등록	메쉬 타입 블록체인 기반의 사물 인터넷 기기 관리 시스템
제10-1895836호	등록	자기 보호 기능이 있는 악성 코드의 치료 및 삭제 방법
제10-1922956호	등록	저 차원 수의 엔트로피 타운트 맵 기반 악성코드 탐지 방법
제10-1944809호	등록	도메인 네임 서버를 이용한 악성 코드 정보 조회 방법
제10-2015897호	등록	악성 코드 분석을 위한 모조 응답 패킷을 생성하는 네트워크 접속 유도 방법
제10-2036847호	등록	런타임 특징 프로파일링 방법
제10-2119636호	등록	수동 핑거프린팅을 이용한 익명 네트워크 분석 시스템 및 방법
제10-2129375호	등록	답러닝 모델 기반 토르 사이트 액티브 핑거프린팅 시스템 및 방법
제10-2156600호	등록	네트워크에서 수집된 패킷과 엔드포인트 컴퓨팅 장치의 프로세스 간의 연관관계를 생성하는 시스템 및 방법
제10-2180596호	등록	다중 블록체인 기반의 사물인터넷 디바이스 식별 및 거래행위 추적 방법 및 이를 위한 시스템
제10-2234698호	등록	합성곱 신경망을 이용한 토르 사이트 수동 핑거프린팅 시스템 및 방법
제10-2267560호	등록	블록 체인에 저장되는 데이터 크기를 축소할 수 있는 데이터의 변경 이력 관리 방법
제10-2267564호	등록	원격 단말기의 능동적 보안 위협 탐지 방법
제10-2267735호	등록	영지식 증명을 이용한 탈중앙화 신원증명 시스템 및 방법
제10-2308477호	등록	악성 코드의 악성 행위 특징 정보를 생성하는 방법
제10-2322408호	등록	서버 자원을 이용한 악성 코드 탐지 및 치료가 가능한 사물 인터넷 장치 및 그 방법
제10-2348239호	등록	이메일의 키워드 분석 방법
제10-2362516호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2386282호	등록	비정상 데이터 탐지 시스템 및 방법
제10-2386284호	등록	비정상 데이터 탐지를 위한 트리거 모듈
제10-2386287호	등록	비정상 데이터 탐지를 위한 시그널 허브
제10-2386289호	등록	비정상 데이터 탐지를 위한 디텍터 모듈
제10-2386290호	등록	트리거 룰 기반의 비정상 데이터 탐지 방법
제10-2386294호	등록	피드 룰 기반의 비정상 데이터 탐지 방법
제10-2386297호	등록	디텍터 룰 기반의 비정상 데이터 탐지 시스템 및 방법
제10-2396236호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2396237호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2396238호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2411383호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체

번호	등록/출원	발명의 명칭
제10-2420884호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2424014호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2432649 호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2437376호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2447278호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2447279호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2447280호	등록	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
PCT/KR2021/010353	출원	비정상 데이터 탐지 시스템 및 방법
17/541,562	출원	IOT DEVICE AND METHOD FOR DETECTING AND REMOVING MALWARE BY USE OF SERVER RESOURCE
17,541,605	출원	METHOD FOR GENERATING CHARACTERISTIC INFORMATION OF MALWARE WHOCH INFORMS ATTACK TYPE OF THE MALWARE
제10-2021-0194045호	출원	사이버보안 위협 정보 처리 장치, 사이버보안 위협 정보 처리 방법 및 사이버보안 위협 정보 처리하는 프로그램을 저장하는 저장매체
제10-2022-0004015호	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
PCT/KR2022/000955	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
17/721,752	출원	APPARATUS FOR PROCESSING CYBER THREAT INFORMATION, METHOD FOR PROCESSING CYBER THREAT INFORMATION, AND MEDIUM FOR STORING A PROGRAM PROCESSING CYBER THREAT INFORMATION
17/721,749	출원	APPARATUS FOR PROCESSING CYBER THREAT INFORMATION, METHOD FOR PROCESSING CYBER THREAT INFORMATION, AND MEDIUM FOR STORING A PROGRAM PROCESSING CYBER THREAT INFORMATION
17/721,757	출원	APPARATUS FOR PROCESSING CYBER THREAT INFORMATION, METHOD FOR PROCESSING CYBER THREAT INFORMATION, AND MEDIUM FOR STORING A PROGRAM PROCESSING CYBER THREAT INFORMATION
10-2022-0095587	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 소프트웨어를 저장하는 저장매체
10-2022-0097517	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2022-0099973	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2022-0099974	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2022-0185437	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 컴퓨터로 판독 가능한 저장매체
10-2022-0185453	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 컴퓨터로 판독 가능한 저장매체
10-2022-0185412	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 컴퓨터로 판독 가능한 저장매체
10-2022-0185475	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 컴퓨터로 판독 가능한 저장매체
10-2022-0185519	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 컴퓨터로 판독 가능한 저장매체
10-2022-0185541	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 컴퓨터로 판독 가능한 저장매체
10-2023-0047970	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체

번호	등록/출원	발명의 명칭
10-2023-0047981	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2023-0047986	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2023-0047987	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2023-0047988	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2023-0047990	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
10-2023-0047992	출원	사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체
18/106,024	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/106,427	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/107,247	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/107,282	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/132,061	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/132,948	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/132,950	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/132,951	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/132,953	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/137,518	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/138,423	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/138,429	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/138,433	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM
18/138,447	출원	CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM



김기홍 대표



샌즈랩

Question & Answer

Q1

“사이버 위협 인텔리전스” 분야의 미래 전망은?

“사이버 위협 인텔리전스” 기술은 사이버 보안 분야에서 차세대 기술로 향후 발전 가능성이 아주 큰 기술로 평가받고 있습니다. 사이버 보안 분야에서는 공격자와 공격 내용을 사전에 식별하여 관련된 위협을 조기에 탐지, 대응할 수 있도록 하여 피해의 대량 확산을 방지하는 것이 가장 큰 목표인데, 사이버 위협 인텔리전스는 사전에 다양한 위협 요소와 정황 정보들을 수집하고 분석하여 현재 발생 중이거나 앞으로 일어날 위협에 대해서 사용자에게 미리 알림을 주고 해당 정보를 기반으로 대응할 수 있도록 유도하는 핵심 기술입니다. 비단 IT 인프라 뿐만 아니라 향후에는 IoT, OT, ICS, 교통 인프라 등 다양한 곳에서 IT 기술을 활용하여 서비스와 기반 시설을 고도화하게 될텐데 이와 같은 곳의 안정적 운영을 방해하는 다양한 위협을 대응하는 주요 정보로 활용할 수 있게 합니다. 현재는 단순한 “정보보안”의 개념이 크지만, 향후에는 인간의 삶 저변에 확대된 IT 인프라를 안정적으로 보호해줄 수 있도록 발전하게 될 것이고 이를 기반으로 “디지털안전”의 개념으로 확대 될 것으로 예상됩니다.

Q2

“사이버 위협 인텔리전스” 관련 표준화를 시작하게 된 계기는?

사이버 보안 분야의 핵심 기술이 될 사이버 위협 인텔리전스는 그 중요도만큼 국내외 다양한 기업이나 기관이 관련 기술을 선점하기 위해 노력 중에 있습니다. 또한, 해당 기술은 정보 공유 및 표준화된 포맷 형태로 다양한 보안 제품들과 연계 및 공유를 하는 것이 중요하기 때문에 어떠한 요소를 어떠한 포맷으로 위협을 표현하고, 이를 공유 하도록 하는지가 중요합니다. 저희 샌즈랩이 보유한 기술은 사이버 위협 인텔리전스에 중요한 몇 가지 정보를 생성하는데 핵심 기술을 보유하고 있고, 이를 표준화된 포맷으로 제공 할 수 있도록 하여 위협 정보를 활용하고자 하는 많은 기관 또는 기업에서 당사의 기술로 개발된 위협 정보의 내용을 활용할 수 있도록 하면, 위협 대응의 효율 증대는 물론이고 당사의 기술적 가치 수준까지 상승하는 효과를 누릴 수 있기 때문에 관련 특허 확보와 표준화 전략을 함께 진행하고 있는 중입니다.

Q4

우리가 “사이버 위협 인텔리전스” 분야에서 주목해야 할 부분은?

최근 랜섬웨어나 DDoS, 개인정보 유출과 같은 공격이 다수 발생하고 있습니다. 사이버 위협 인텔리전스 분야에서는 해당 공격 그 자체를 식별하고 대응하는 것도 중요하지만 해당 공격 이면에 공격자를 식별하고 사용된 공격 기법 그 자체를 식별하는 것이 중요한 상황에 놓였습니다. MITRE 에서는 이를 ATT&CK 라는 모델을 만들어 각각의 공격에 대한 정의를 수행하였고, 보안 업체 입장에서는 악성코드나 공격에 사용된 각 기법을 정의된 모델에 부합하는지 확인하는 것이 중요한 과정이 되었습니다. 또한, 해당 공격을 사용하는 공격자나 공격그룹의 특징 정보를 파악하여 어떤 공격 그룹이 어떤 공격 기법을 사용하여 공격을 하는지 확인하는 절차가 중요해졌습니다. 저희는 이러한 기술적 내용에 필요한 핵심 기술을 이미 2021년, 2022년에 확보를 한 상태이고 산자부에서 진행하는 신기술 인증(NET 인증)을 2년 연속으로 받은 바가 있습니다. 이렇게 확보한 기술을 통해서 공격자를 식별하고 사용된 공격 기법을 파악하여 고객에게 조금더 풍성한 정보를 제공하여 대응에 만전을 기할 수 있도록 하는 것이 중요한 부분입니다.

Q3

앞으로 도전하고자 하는 과제는?

단순히 현재의 위협을 분석하여 관련 정보를 공유하는 것이 아니라 기상청과 같이 앞으로 다가올 위협에 대해서 인공지능 기술을 활용하여 예측하고 대응할 수 있도록 연구 중입니다. 현재에서 발생하는 다양한 데이터를 분석하고 이를 학습 시켜서 새롭게 만들어 질 수 있는 공격에 대해 다양한 시나리오를 생성하여 검증하고 이를 통해 예측할 수 있는 모델을 만들어서 미리 대응 할 수 있다면 사이버 보안 분야에서 새로운 기술적 진보를 이루게 되게 됩니다. 저희는 이것이 가능하게 하기 위해서 노력 중입니다.

Q5

앞으로 “사이버 위협 인텔리전스” 기술 분야에 바라는 정부의 요구사항은?

사이버 보안 분야의 특성상 아직도 국정원이나 국방부 등 국가 주요 기관에 의해서 대응 정보 확보의 한계를 가지는 경우가 있습니다. 추가적으로 추적하고 분석하여 실체를 파악해야 함에도 불구하고 법으로 정하고 있는 어느 정도의 범위 때문에 추가적인 추적을 하지 못하고 적당한 선에서 머물러야 하는 경우가 많이 있습니다. 정보 공유 또한 마찬가지입니다. 식별된 위협을 국내 업체들과 기관들끼리라도 조기에 공유를 하여 확산을 방지해야 하는데, 정보 통제와 여러 가지 제약 조건 때문에 쉽지 않습니다. 예를 들어 악성코드 샘플 파일 같은 경우도 함부로 공유할 수 없고, 분석 정보 또한 여러 가지 공격의 타겟이 되는 정보들을 내포하고 있어서 n차 공격이 될 수 있어 공개에 상당히 제한적일 수밖에 없습니다. 이에 비해 외국은 상당히 이러한 정보 공개가 수월한 편입니다. 국내 업체에만 적용되는 이러한 제약 조건을 완화해서 국내의 유능한 사이버 보안 업체도 글로벌 시장에 진출할 수 있는 기반 마련이 조속히 되어야 할 것으로 보입니다.



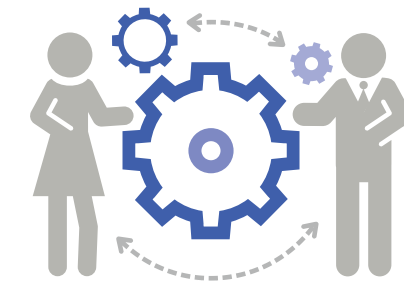
표준특허 관련 주요 행사

1 >> 추진 사항

2023년 상반기 표준특허 전문가 양성 교육 개최

지난 5월 31일, 표준특허에 관심 있는 변리사 및 산·학·연 관계자를 대상으로 2023년 상반기 표준특허 전문가 양성 교육을 개최하였다. 이번 교육은 표준특허 개요 및 이에 활용되는 주요국 특허법, 표준특허 창출을 위한 표준(기고문)특허 분석 방법 및 명세서 설계 전략, 표준특허 Claim chart 작성 방법 및 관리전략, 표준특허 활용 및 분쟁 대응 전략, 표준특허 창출지원 사업 소개 등 다양한 주제로 구성되었다.

2 >> 예정 사항



2023년 한국통신학회 하계종합학술발표회

- **일 정** : 2023년 6월 21일 ~ 6월 24일
- **주 최** : 한국통신학회
- **대 상** : 국내외 정보통신 관련 단체, 출연연, 대학 등 ICT 분야 기술 교류 기회를 경험하고 싶은 분
- **내 용** : 5G/6G 네트워크 및 서비스, 5G/6G 무선통신 및 통신시스템, 전파/위성통신, 인공지능, 빅데이터, IoT 플랫폼, SW, 메타버스, 블록체인, VR/AR, 지능형반도체, 양자컴퓨팅, ICT융합 기술 및 정책 분야 등
※ 자세한 내용은 <https://conf.kics.or.kr> 참고

ICUFN 2023 (The 14th International Conference on Ubiquitous and Future Networks)

- **일 정** : 2023년 7월 4일 ~ 7월 7일
- **주 최** : 한국통신학회
- **내 용** : 이동통신, 개방형 네트워킹, 빅데이터 및 클라우드, 사물 인터넷(IoT), 자율시스템 등
※ 자세한 내용은 <http://www.icufn.org> 참고



2023 찾아가는 맞춤형 표준특허 교육대상 모집

무료



표준특허전략팀에서는 표준특허 교육을 희망하는 다수의 인원이 소속된 기업 또는 기관에 대하여 원하는 콘텐츠 및 시간·장소에 맞춰 무료로 표준특허 교육을 제공하고 있습니다.

- 대 상** 표준특허 교육을 희망하는 산·학·연 누구나
- 모집기간** 상시(~2023.11)
- 비 용** 전액무료
- 신청방법** 표준특허포털(<http://biz.kista.re.kr/epcenter/eduReq.do>)에서 온라인 신청



진행과정

교육신청 접수	포털사이트를 통해 교육 수요 접수(상시)
교육생 자기진단	표준특허 인식수준 및 수요조사
교육프로그램구성	진단결과 기반 맞춤형 프로그램 협의
교육개최	방문교육 진행

- 기 타**
 - 교육 수료 후, 수료증 발급 가능
 - 문의처: 표준특허전략팀 강민정 선임연구원 (02-3287-4334, epcenter@kista.re.kr)



SEP Inside Standard Essential Patent

표준특허 전문지 Vol.38

본 전문지는 특허청과 한국특허전략개발원 표준특허전략팀의 연구결과로 발간된 자료입니다.

특허청과 한국특허전략개발원 표준특허전략팀의 허가없이 무단 사용 및 배포를 금하며, 내용 인용 시에는 반드시 특허청 '표준특허 창출지원 사업'의 연구 결과임을 밝혀야 합니다.

SEP Inside 편집위원

편집위원장

신 원 혜 특허청 산업재산창출전략팀장

편집위원

김 호 영 특허청 산업재산창출전략팀
이 연 준 특허청 산업재산창출전략팀
박 정 환 한국특허전략개발원 표준특허전략팀
이 준 우 한국특허전략개발원 표준특허전략팀
정 석 현 한국특허전략개발원 표준특허전략팀
윤 순 영 한국특허전략개발원 표준특허전략팀
강 민 정 한국특허전략개발원 표준특허전략팀
심 현 미 한국특허전략개발원 표준특허전략팀
전 민 수 한국특허전략개발원 표준특허전략팀
이 다 영 한국특허전략개발원 표준특허전략팀

SEP Inside Vol.38

발 행

특허청 산업재산창출전략팀
한국특허전략개발원 표준특허전략팀

발행일

2023년 6월 1일

발행인

이 재 우 한국특허전략개발원장

발행처

한국특허전략개발원
[본원] 대전광역시 중구 대종로 540 유안타증권빌딩
14층, 15층 (34831)
[분원] 서울시 강남구 테헤란로 131 한국지식재산센터
8층 (06133)
홈페이지 : <http://www.kista.re.kr>
<http://biz.kista.re.kr/epcenter>



6070세대가 창작예술 활동의 주인공이 되는 무대

tvN STORY 오늘도 주인공★

방송일시 | tvN STORY | '23. 6. 13.(화) ~ 7. 18.(화), 매주 화요일 저녁 7시

재방송 | tvN | '23. 6. 20.(화) ~ 7. 25.(화), 매주 화요일 1시

| tvN STORY | '23. 6. 17.(토) ~ 7. 22.(토), 매주 토요일 7시

TVING 업로드

방송내용 대한민국 최강 6070이야기예술인 4개 팀이 펼치는 이야기 구연 배틀

출 연 진 6070이야기예술인, 박미선, 정영주, 장동민, 육중완, 홍윤화 등



누군가의 아내, 떠노리, 넘파로 살아온 나
6070이야기예술인(이야기할머니)과
함께라면 오늘도 주인공입니다



www.storymama.kr

6070이야기예술인(이야기할머니)은
소정의 교육을 이수한 어르신들이
전국 유아교육기관에 방문해
우리 옛이야기를 들려주는 사업입니다.
현재 전국 3,000여명이 8,600여개
유아교육기관에서 활동하고 있습니다.



문화체육관광부



한국국학진흥원
THE KOREAN STUDIES INSTITUTE

밀수가 의심된다면
125 기억(7)하세요!

1 2 3
4 5 6
7 8 9
* 0 #



5월 18일부터
밀수신고

포상금 최대 **3억원**



대한민국의 미래 먹거리 해결, 新성장 4.0 15대 프로젝트

新기술 미래 분야 개척

교통체증 無, 운전피로 無
어디든지 편리하고 안전한 이동



우리의 기술로 여는
K-우주시대



꿈의 양자기술!
미세암 발견, 해킹 원천 차단



첨단재생의료 치료제 개발
감염병으로부터 안전한 나라!



안전하고 경제적인 차세대 원자로
깨끗한 수소 신재생 에너지



新일상 Digital Everywhere

내 삶 속의 디지털 신기술,
모두가 평온한 Digital life



차세대 물류 시스템으로
어디든 신선하고 빠르게



넷제로 지구의 시작,
탄소중립도시



농어업 스마트 대전환으로
맛도 영양도 UP!



똑똑한 전력망으로
안정적 에너지 공급



新시장 경쟁을 넘어 초격차 확보

전략산업 No.1 코리아 달성,
30년 미래먹거리 확보



바이오 혁신으로
100세까지 건강하게



K-컬처 융합으로
전국을 관광명소로



전세계인을 사로잡는 K-콘텐츠



원팀 코리아를 통한
빅딜 수주 릴레이



마약으로부터 안전한 사회

우리 모두가 함께 지켜 나갑니다

소리 없이 스며들고 있는 마약으로부터
소중한 사람, 행복한 일상을 지킵니다.

강력한 마약 단속,
재활과 치료, 예방교육을 통한
마약청정국으로의 힘찬 도약!
법무부가 함께 합니다.

NO!
DRUGS



법무부
홍보대사
양학선



DRAW



이제부터 시작!
2023년 제25회 세계스카우트잼버리
8월 1일부터 12일까지 새만금에서
열립니다.



이 물은
모든 것을 깨끗하게 씻어내고
새로운 시작을 준비하고 있습니다.

YOUR



이 물은
모든 것을 깨끗하게 씻어내고
새로운 시작을 준비하고 있습니다.



이 물은
모든 것을 깨끗하게 씻어내고
새로운 시작을 준비하고 있습니다.

이 물은
모든 것을 깨끗하게 씻어내고
새로운 시작을 준비하고 있습니다.



이 물은
모든 것을 깨끗하게 씻어내고
새로운 시작을 준비하고 있습니다.



이 물은
모든 것을 깨끗하게 씻어내고
새로운 시작을 준비하고 있습니다.

DREAM

2023 새만금 「제25회 세계스카우트잼버리」 25th World Scout Jamboree 2023.8.1-12 SaeManGeum, Jeollabuk-do, KOREA



2023 새만금 세계스카우트잼버리조직위원회
The Organizing Committee for the 25th World Scout Jamboree - 2023 SaeManGeum



한국스카우트연맹
Korea Scout Association



우리 1월 연말 정산에 꼭 만나요, 문화비 소득공제

총급여 7천만 원 이하 근로소득자 중
신용카드 등의 사용 금액이 총급여의 25%를 초과하는 경우
최대 300만 원 한도까지 소득공제를 해주는 제도

도서 구입비, 공연 티켓비, 박물관·미술관 입장료, 신문 구독료, 영화관람료



자세한 사항은
문화비 소득공제 누리집에서 확인하세요

문화비 소득공제 고객센터 | 1688-0700



문화체육관광부

KCISA 한국문화정보원