tlomarketing

국가과학기술연구회 공동TLO마케팅사무국이란?

국가과학기술연구회 소관 25개 정부출연연구소(이하 출연(연))의 연구성과에 대한 공동 마케팅을 통해
기술이전과 출자 등 **기업의 기술사업화 지원을 위한 전문조직** 입니다.

공동 TLO 마케팅 사무국

공동TLO마케팅사무국을 통해 무엇을 도움 받을 수 있나요?

신규 사업 아이템 및 기술 업그레이드 등 기술 고민이 있는 예비창업자 및 기존 사업자에게 25개 출연(연)이 보유하고 있는
약 10만여 건의 특허 외에 연구자 노하우 및 연구 · 시험장비 등을 활용하여 **기업의 기술애로를 해결해드리고 있습니다.**

기업 애로해결 지원

· 기술도입 및 사업화 유망기술 발굴
· 기술창업용 출자기술 발굴
· 공동연구 대상 전문연구자 연계

정부과제 소개 지원

· 기술도입형 R&BD
과제 연계

연구장비 지원

· 분석 및 실험장비 연계

IP인수보증 자금 연계 지원

· 기술보증기금,
신용보증기금 등

nst
National Research Council of Science & Technology

국가과학기술연구회

과학기술분야 정부출연연구기관을 지원육성하고 체계적으로 관리함으로써 국가 연구사업 정책 지원 및
지식산업발전을 견인하고자 만든 과학기술정보통신부 산하 정부기관임

문의처

국가과학기술연구회
T. 044-287-7369 E. gylee@nst.re.kr

공동TLO마케팅사무국
T. 042-862-6015 E. seungtae100@wips.co.kr

TLO Tech Trends 2024

국가과학기술연구회 공동 TLO 마케팅 사무국
Technology Licensing Organization

공동 TLO 마케팅 사무국

WIPS 위스

공동 TLO 마케팅 사무국

WPS 윕스

Contents

01
사이버 보안의 세계

02
사이버 보안 기술의 혁신

03
국가전략기술 '사이버 보안' 이야기

04
출연(연) 보유 '사이버 보안' 기술

01 사이버 보안의 세계

사이버 보안이란

사이버 보안(Cyber Security)이란 사이버 환경에서 네트워크 운용 상의 위험으로부터 조직과 사용자 자산을 보호하기 위해 사용하는 기술적 수단이나 보안 정책, 개념, 보안 안전 장치, 가이드라인, 위기 관리 방법, 보안 행동, 교육과 훈련, 그리고 보안 기술 등의 집합을 말한다.

사이버 보안은 사이버 환경에서 다양한 보안 위협으로부터 조직과 사용자 자산의 보장하며, 가용성, 메시지 인증, 부인 방지를 포함한 무결성과 기밀성과 같은 정보 보안 기본 원칙을 유지하여 신뢰할 수 있는 디지털 환경을 제공하는 것이다.

인터넷망 마비 사고가 발생한 2003년 이후 사이버 보안이 정부기관이나 사회 각계 통용되었다. 처음에는 사이버 공간에서의 보안을 의미하였지만, 이후 정보 기술이 발전하면서 사이버 공간에서 각종 위협이 증대되고, 그 피해가 국가 안보를 위협하여 사물 인터넷(IoT) 기기를 공격하는 행위를 막는 개념까지 확장되었다.

사이버 보안 기술은 현대 사회의 모든 영역에서 핵심적인 역할을 수행하며, 그 중요성은 날로 증가하고 있다. 우선 개인 차원에서 해킹, 피싱, 스팸 등 개인을 대상으로 한 사이버 공격을 방어하며 개인의 금융, 건강, 네트워크 정보 등을 안전하게 유지하는 데 큰 역할을 한다.

기업 차원에서는 기업의 데이터 유출이 막대한 경제적 손실과 평판 손상을 초래할 수 있다는 점에서 사이버 보안 기술이 비즈니스의 연속성을 유지하는 데 있어 중요하다고 할 수 있다. 따라서 사이버 보안 기술은 기업의 중요한 자산과 지적 재산을 보호하고, 운영의 안정성을 유지하며, 고객의 신뢰를 확보하기에 중요하다. 이에 기업들은 네트워크 보안, 데이터 암호화, 침입 탐지 시스템 등을 활용하여 사이버 위협에 대비하며, 보안 인프라의 강화를 통해 사이버 공격으로 인한 업무 중단을 최소화하고 빠른 복구를 가능케 한다.

국가 차원에서는 국가의 핵심 자원을 안전하게 유지하고 보호하는 것이 매우 중요하기 때문에 국가 안보와 직결된다. 정부기관과 공공 서비스는 항상 사이버 공격의 주요 타겟이 되기 때문에, 사이버 보안 기술은 이러한 공격으로부터 국가기간시설 등 중요 인프라를 보호하고, 국가의 안전과 주권을 지키는 데 필수적이다. 이는 국방, 에너지, 통신, 금융 등 다양한 분야에서 필요하기 때문에 맞춤형 보안 솔루션을 개발하는 것 역시 중요하다.

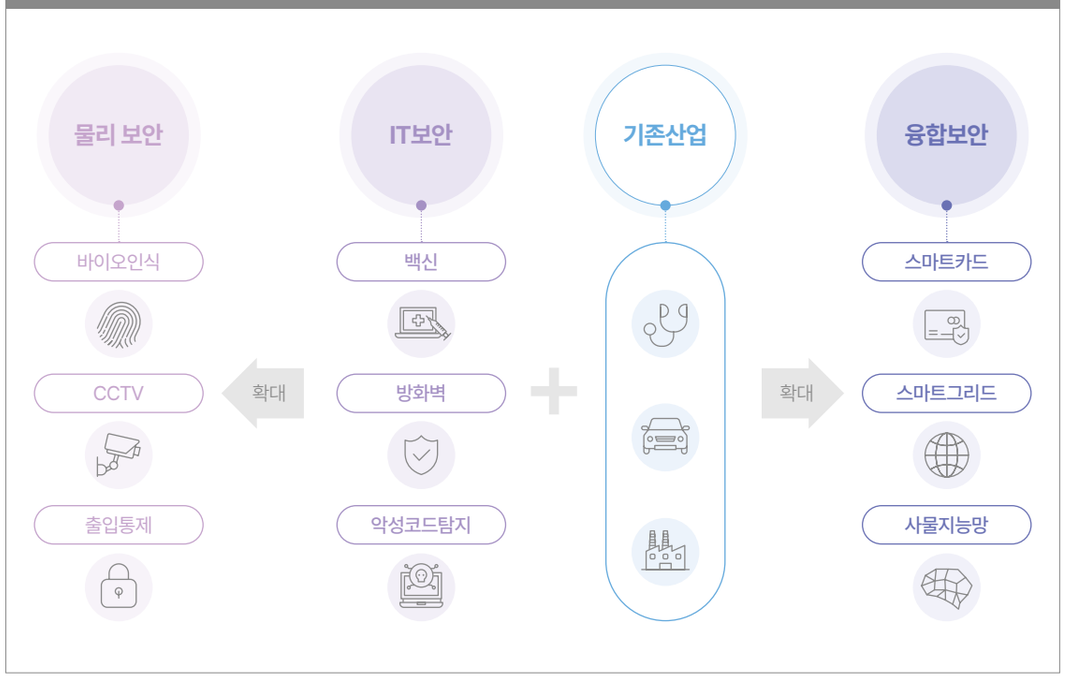
결론적으로, 사이버 보안 기술은 개인의 프라이버시, 기업의 자산, 국가의 안전을 보호하는 데 핵심적인 역할을 하고 있으며, 각국 정부는 사이버 보안 정책을 통해 국가 차원의 보안 프레임워크를 구축하고, 주요 인프라를 보호하며, 국제 협력을 통해 글로벌 사이버 위협에 대응하고 있다.

정보 보안의 기본 원칙 (The CIA triad)

기밀성 Confidentiality	정의	정당하지 않은 사용자나 시스템에 대해서 정보가 노출되지 않게 하는 특성
	예시	데이터 암호화, 강력한 비밀번호 정책, 인증 시스템, 보안 정책
무결성 Intergrity	정의	신뢰할 수 있는 서비스 제공을 위해서 의도하지 않은 요인에 의해 데이터, 소프트웨어, 시스템 등이 변경되거나 손상되지 않고 완전성, 정확성, 일관성을 유지함을 보장하는 특성
	예시	체크섬, 해시 함수, 버전 관리, 액세스 로그
가용성 Availability	정의	① 사용이 요구될 때 한 소프트웨어가 지정된 시스템 기능을 수행할 수 있는 능력 ② 네트워크를 구성하는 요소가 일정 시간 동안 일정 조건에서 필요한 기능을 수행할 수 있는 확률 ③ 인가된 사용자만 필요할 때에 적절히 정보 또는 자산에 접근하도록 보장하는 특성
	예시	중복 서버, 백업, DDoS 방어 시스템, 재해 복구 시스템(DR)

출처 : 한국정보통신기술협회 정보통신용어사전

디지털과 물리적 안전을 통한 사이버 보안



출처 : 4차 산업혁명 시대에 더 중요해진 사이버 보안, 산업통상자원부 블로그, 2017.11.01

사이버 보안 개발 변천사

1950 ~ 1960

1950년~
· "폰 프릭(Phone Phreaks)" 시대로, 네트워크의 프로토콜을 방해하고 무료로 사용하는 프로토콜 발생

1960년~
· MIT 학생들에 의해 최초의 악의적인 해킹이 발생
· 컴퓨터가 더 작고 저렴해지면서 데이터와 시스템 관리하며 비밀번호 시스템 도입

1970~

컴퓨터 보안의 출현
ARPANET 등장으로 인한 네트워크 보안의 필요성 대두

1972년
· 최초의 안티바이러스 소프트웨어이자 최초의 컴퓨터 웜인 Reaper개발

1979년
· 케빈 미트닉(Kevin Mitnick)이 디지털 장비 공사(DEC)의 컴퓨터인 Ark 해킹, 소프트웨어 복사본 생성

1980

ARPANET과 Internet
· 해커와 사이버 범죄자들이 증가로 '사이버' 의 개념 인식
· 비엔나 바이러스란 악성 코드 등장과 해결하기 위해 현대적 안티바이러스 소프트웨어를 개발

1987년
· 상업용 안티바이러스의 최초 등장

1990~

World Wide Web의 시대
스스로 복제되는 다형성 바이러스 코드와 PC Today의 DiskKiller 바이러스를 포함한 디스크 배포하여 많은 PC 감염

1995년
· 마이크로소프트 Windows 95와 함께 Internet Explorer를 출시

1990년대 중반
· 컴퓨터 보급, 대중의 인터넷 접근

1990년대 후반
· 이메일 및 Microsoft Outlook과 같은 메시징 서비스 활용

1999년
· Outlook을 통한 Melissa 바이러스 확산 사건

2000~

사이버 위협의 증가
인터넷 보급화와 스마트폰 보급으로 인한 사이버 공격의 전문화와 함께 발생량 증가

2000년
· OpenAntivirus Project의 최초의 오픈소스 안티바이러스 엔진

2001년
· IRC(인터넷 채팅 릴레이) 채널을 통해 확산되는 웜 공격 발생

2005~2007년
· 신용카드 시스템 해킹으로 4,570만개의 신용카드 정보 유출

2007년
· 애플의 아이폰 출시로 모바일 사이버 보안 위협 발생

2010~

사이버보안의 진화
국가 안보에 영향을 미치고 기업에 수백만 달러의 손실을 초래한 여러 해킹과 사이버 공격이 발생

2012년
· 사우디 해커의 40만개의 신용카드 번호 유출

2013년
· 에드워드 스노든의 NSA 기밀 데이터 유출

2013-2014년
· 야후 고객 30억 명의 정보 유출

2017년
· WannaCry 랜섬웨어로 PC 23만대 감염

2019년
· 뉴질랜드 주식시장의 DDoS 공격으로 일시 폐쇄하는 사건 발생

출처 : History of Cyber Security: A Brief Explanation, The Knowledge academy

02 사이버 보안 기술의 혁신

AI 칩 위의 방화벽(Check Point)

최근 클라우드 컴퓨팅의 확산으로 인해 보안 위협이 급격히 증가하여 클라우드 환경에서 AI 모델을 보호하기 위한 새로운 보안 요구 사항이 대두되고 있다. 2013년, 미국의 대형 슈퍼마켓 체인 Target은 해킹 공격으로 인해 7천만 명의 고객 데이터가 유출되는 사건을 겪게 되었다. 이 사건은 클라우드 보안의 취약성을 드러냈지만, AI와 클라우드가 결합된 강력한 보안 솔루션의 필요성을 느끼게 해 주었다.

Check Point는 클라우드 보안 위협에 대응하기 위해 'AI 칩 위의 방화벽(Firewall on an AI chip)' 개념으로 설계된 'AI Cloud Protect 솔루션'을 선보였다. 이 솔루션은 AI 모델 학습 데이터의 추출 및 추론 공격, AI 모델 도용 등 다양한 AI 관련 위협으로부터 조직을 보호하며, AI 환경 전반에 걸쳐 손쉬운 배포와 보안 조치 강화를 지원한다.

특히, AI Cloud Protect는 NVIDIA의 BlueField-3 DPU와 NVDICA DOCA 소프트웨어 프레임워크를 기반으로 설계되어 AI 성능에 영향을 주지 않으면서도 최적화된 AI 성능과 보안을 제공한다.

Check Point는 NVIDIA와의 파트너십을 통해 AI 추론 모델에 대한 공격을 방어하는 AI Cloud Protect 솔루션을 제공하고 있다. 이 솔루션은 업계 최고의 클라우드 보안 위협 예방 기능을 기반으로 AI 클라우드 보안을 강화하여, 글로벌 통신사(ISP) 및 클라우드 서비스 제공 업체(CSP) 등의 클라우드 환경에서 네트워크와 호스트 레벨을 동시에 보호하는 강력한 보안 기능을 제공한다.

이를 통해 Check Point는 AI 시대의 보안 요구 사항을 해결하며, AI 관련 위협에 대한 강력한 방어를 제공하여 클라우드 보안 시장에서의 입지를 강화하고 있다.

AI Cloud Protect 작동 프로세스

출처 : CHECK POINT 공식 홈페이지

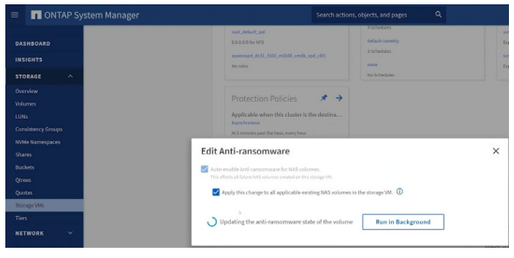
스토리지 내장형 AI로 랜섬웨어 실시간 대응(NetAPP)

랜섬웨어는 상대방의 데이터나 기기를 암호화한 후 풀어주는 대가로 금품을 요구하는 악성코드로, 2024년 2월 랜섬웨어 공격을 받은 유나이티드 헬스 그룹은 8억 7,200만 달러의 손실을 입은 것으로 알려졌다. 이러한 피해를 최소화하기 위해 기관 및 기업들은 자동화된 랜섬웨어 탐지 및 대응 기능을 갖춘 스토리지 시스템을 도입할 필요성을 느끼게 되었다.

이에 지능형 데이터 인프라 기업 NetAPP은 AI 기반 랜섬웨어 탐지 기능을 갖추고 있어 실시간 탐지 및 대응이 가능한 'NetAPP ARP/AI' 시스템을 개발했다. 이 시스템은 스토리지의 랜섬웨어 탐지 기능을 이용하여 데이터의 무작위성 평가, 확장자 유형 및 파일 IOPS(비정상적 볼륨 활동)을 감지 분석한다. 뿐만 아니라 사용자의 사이버 복원력을 향상시키고 지능형 데이터 인프라를 유지 · 관리를 통해 운영 부담을 줄일 수 있다.

보안 제품 및 서비스를 평가하는 SE Labs로부터, NetAPP ARP/AI는 랜섬웨어 공격에 대한 멀웨어 탐지율 지표인 리콜률(recall)을 99%로 평가받아 AAA 등급을 획득하며 기술력과 보호 효과를 인증받았다. 또한, NetApp은 최신 랜섬웨어 변종에 대한 지속적인 재교육을 추진하여 동적인 랜섬웨어 환경에 대응할 수 있는 솔루션을 기업들에게 제공하고 있다.

NetApp 자율형 랜섬웨어 보호 서비스



출처 : 유튜브 'NetApp on NetApp'

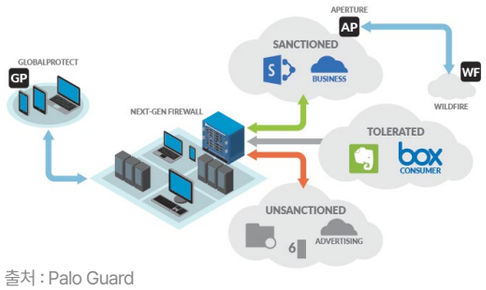
생성형 AI 접목한 보안 솔루션 (Palo Alto Networks)

기업들 사이에서 생성형 AI 적용 사례가 빠르게 증가하면서, 이에 따른 사이버 보안 위협도 크게 우려되는 상황이다. 특히 생성형 AI는 우회적이고 고유한 특성을 가져 전통적인 보안 솔루션으로 탐지하기 어려워, 제로데이 공격 방지에 널리 활용되고 있다. 실제로 Palo Alto Networks는 매일 평균 230만 건의 새로운 사이버 위협을 발견하고, 하루 평균 113억 건의 위협을 인라인으로 차단하고 있다.

이러한 사이버 보안 과제를 해결하기 위해 글로벌 사이버 보안 선도 기업인 Palo Alto Networks는 생성형 AI가 결합된 독자적인 기술로 개발한 AI 기반 보안 서비스 '프리시전 AI'를 제공하고 있다. 프리시전 AI는 풍부한 데이터와 보안 전용 모델을 사용하여 업계 최고의 정확도로 탐지, 예방 및 교정을 자동화함으로써 보안팀이 AI 결과를 신뢰할 수 있도록 지원하는 AI 시스템이다. 이를 통해 다양한 기업과 기관은 공격자보다 한발 앞서 네트워크와 인프라를 보다 선제적으로 보호하는 AI 기반 보안을 마련할 수 있다.

앞으로 생성형 AI에 대한 기대와 함께 안전성에 대한 리스크를 얼마나 효과적으로 다루는지가 AI 경쟁의 주요 화두가 될 것으로 전망된다. Palo Alto Networks는 10년 이상 기계 학습 등 AI를 연구하고 이를 서비스에 적용해 사이버 보안 위협에 대한 탐지 및 대응 능력을 강화해 왔다. 향후 각 산업별 대기업, 중견기업, 중소기업 등 규모에 맞는 지원팀을 마련하여 보안 요구사항이 지속적으로 변화하는 시장에서 프리시전 AI와 플랫폼을 활용해 고객의 다양하고 복잡한 요구에 효과적으로 대응할 예정이다.

Palo Alto Networks Aperture 프로세스



출처 : Palo Guard

산업 속 사이버 보안 기술활용

데이터 보안

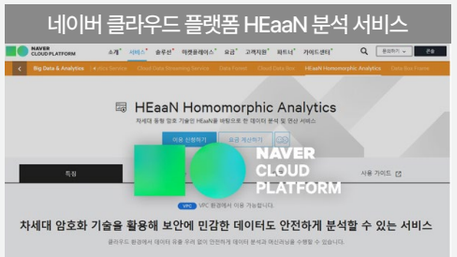
HEAAN CRYPTO LAB

차세대 암호와 AI기술로 보안 혁신 선도

양자컴퓨팅 기술의 발전으로 기존 암호 체계가 무력화될 가능성이 높아지고 있다. 이에 따라, 암호화된 상태에서도 데이터를 연산할 수 있는 기술인 동형암호와 양자내성암호 체계 같은 데이터 프라이버시 및 AI 보안 기술에 대한 관심이 증가하고 있다. 글로벌 시장조사업체인 가트너는 2021년과 2022년, 두 차례에 걸쳐 동형암호 기술 부문 '샘플 벤더'로 크립토랩을 선정하며 그 기술력을 인정했다.

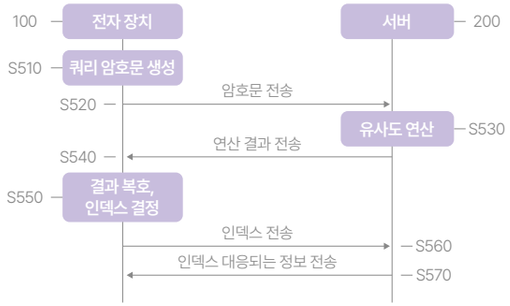
크립토랩의 'HEaaN Private AI'는 동형암호를 기반으로 한 데이터 분석 솔루션으로, 데이터를 보호하면서도 안전하게 분석 및 활용할 수 있도록 설계되었다. 이 솔루션은 특히 금융과 의료 분야에서의 민감한 데이터를 프라이버시 노출없이 처리할 수 있다. 이처럼 암호화된 상태에서 데이터를 처리하기 때문에, 데이터 유출 위험을 최소화하는 특징을 갖고 있다.

이러한 기술력을 바탕으로 네이버클라우드, 서울대학교 산업수학센터와 협력하여 네이버 클라우드 플랫폼에서 동형암호를 쉽게 사용할 수 있는 'HEaaN Homomorphic Analytics' 를 출시하여 강력한 보안 환경에서 데이터 분석 서비스가 필요한 기관 및 기업에게 서비스를 제공하고 있다. 최근 주목받고 있는 ChatGPT도 유용성 때문에 활용을 원하지만, 직원들이 질문한 내용이 GPT의 학습 및 추론에 사용되면서 주요 정부기관의 기밀이나 업체의 사내 정보 누설 문제가 발생할 수 있어 사용을 금지하는 상황이다. 크립토랩은 이와 같은 LLM에 동형암호를 적용할 수 있는 방법을 개발하는 전담부서 또한 신설하여 기술개발에 박차를 가하고 있다.



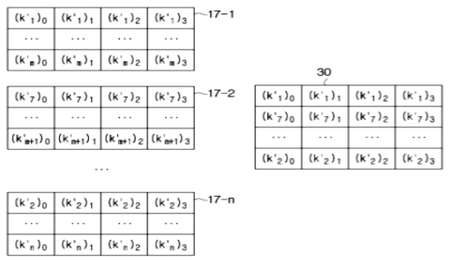
출처 : 크립토랩

01 동형 암호화를 사용하여 직접 계산없이 다양한 데이터의 보안 처리가 가능한 기술을 개발했다. 텍스트를 벡터로 변환하고 암호화하여 서버에 전송하면, 서버는 유사도를 계산해 결과를 반환하는 방식으로, 클라이언트는 이 결과를 복원해 필요한 정보를 받는다. 이를 통해 민감한 개인정보를 보호하면서도 안전하게 정보를 검색할 수 있으며, 암호 데이터를 복호화할 때 소비되는 자원 낭비 또한 방지한다.



전자 장치에서의 텍스트 검색 방법
(KR 10-2023-0084386)

02 분산된 정보 제공 기관에서 암호화된 데이터를 빠르게 검색할 수 있도록 돕는 기술로 암호화된 데이터를 효과적으로 검색할 수 있는 방법을 구축하였다. 해시 함수를 이용해 데이터를 정렬, 그룹화, 인코딩하여 룩업테이블을 생성하고, 동형 암호화를 통해 보안성을 유지하면서 데이터를 빠르게 검색한다. 검색 시 쿼리의 해시 값을 인코딩하여 대응되는 데이터를 찾아내며, 슬롯 단위의 동형 암호 비교 연산을 사용해 보안을 유지한다. 이를 통해 쿼리 종류에 관계없이 암호화된 데이터 값을 빠르게 검색할 수 있다.



동형암호화 룩업 테이블 생성 과정
(KR 10-2022-0174208)

공급망 보안

EST SECURITY

공급망 위협 맞서는 보안 혁신 솔루션

2020년에 발생한 솔라윈즈 공급망 해킹 사건과 같은 SW 공급망 보안 피해 사례가 지속적으로 증가하고 있어 SW 제조, 유통, 운영 단계에서 SW 공급망 보안 기술의 필요성이 강하게 제기되고 있다. 특히, 랜섬웨어 피해의 경우, 업무 중단과 같은 심각한 상황이 발생할 수 있어, 개인뿐만 아니라 기업의 디지털 자산도 영향을 받기 때문에, 선제적인 랜섬웨어 행위차단과 대응이 필요한 시점이다.

이스트시큐리티의 랜섬쉴드는 사전방어와 데이터 보호를 한 번에 할 수 있는 솔루션이다. 랜섬쉴드는 랜섬웨어 방어(랜섬웨어 차단 및 훼손 파일 복구), PC백업(파일 생성/수정시 PC에 실시간 백업, 필요시 사용자가 일괄 복원), 클라우드 백업(관리자 정책에 따라 클라우드에 한 번 더 실시간 백업) 등 3단계 대응을 통해 방어한다. 또한 랜섬쉴드는 국내 최초의 랜섬웨어 차단 기술특허 제품이며, 2016년 기준 397만 건의 랜섬웨어를 차단하는 성과를 거뒀다.

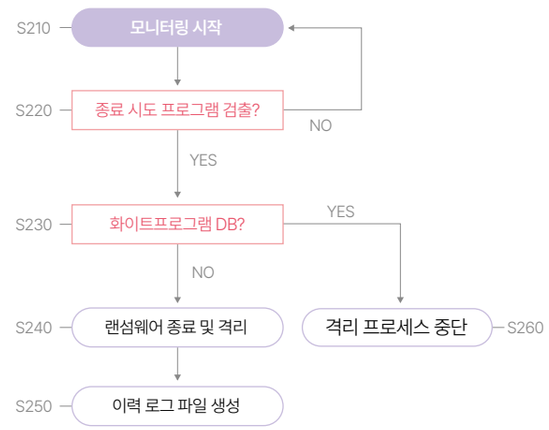
이스트시큐리티의 랜섬쉴드 3단계 대응

STEP 01 랜섬웨어 방어	랜섬웨어로 탐지 시 랜섬웨어 차단 및 훼손 파일 바로 복구
STEP 02 PC 백업	파일 생성/수정 시 PC에 실시간 백업 필요 시 사용자가 일괄 복원
STEP 03 클라우드 백업	관리자 정책에 따라 클라우드에 한번 더 실시간 백업

출처 : 이스트시큐리티

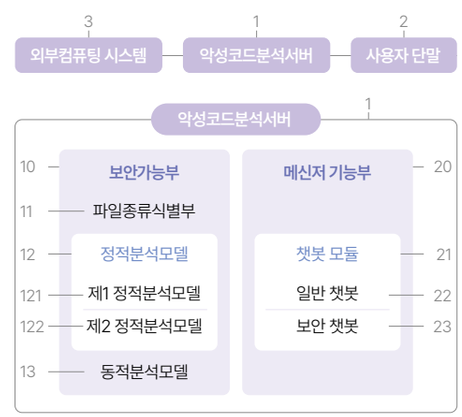
이스트시큐리티는 과기정통부의 지원을 받아 제로 트러스트 기반 엔드포인트 통합 보안 플랫폼을 개발하는 'K-시큐리티 얼라이언스 통합 보안 모델 개발 시범 사업'을 수주하였으며, 이를 통해 다양한 보안 솔루션을 통합하고, 관련 산업의 기술 성숙도와 보안 시장 경쟁력을 강화할 것으로 보인다.

01 랜섬웨어를 방지하기 위한 위장 프로그램과 감시모듈을 개발하여 사전에 차단하는 기술을 개발했다. 위장 프로그램의 종료를 시도하는 프로그램 검출 시 그 프로그램의 차단을 통해 랜섬행위를 사전에 방어하며, 시스템 모듈 및 백신 프로그램에 대해서는 데이터베이스를 통해 오인 탐지를 방지하기에 랜섬웨어로부터 보호할 수 있다.



위장 프로세스를 이용한 랜섬웨어 행위 탐지 및 방지 방법을 설명하기 위한 흐름도 (KR 10-2018-0135537)

02 사용자 단말기로부터 수신한 파일을 정적분석과 동적분석을 통해 분석한 후, 그 결과를 메신저 서비스로 출력하는 기술을 개발했다. 이를 통해 분석 전문가가 없더라도 기본적인 Q&A 기능을 이용할 수 있어 분석 과정을 자동화할 수 있으며, 해당 Q&A데이터만으로 결과가 출력되기 전 예상분석결과를 제공할 수 있다.



악성코드 분석대응방법 및 시스템을 구현하는 구성요소
(KR 10-2023-0005480)

네트워크 · 클라우드 보안

IGLOO

AI로 강화된 보안 자동화의 미래

디지털 전환이 빨라지면서 보안 위협도 빠르게 변하고 있어, 많은 보안 사건과 복잡한 보안 규정을 처리해야 하는 보안 인력들의 부담이 커지고 있다. 이에 보안 업무의 효율성을 높이고 대응 시간을 실질적으로 단축시키기 위한 AI 기반 지능형 보안관제 자동화 대응(SOAR) 기술의 중요성이 부각되고 있다.

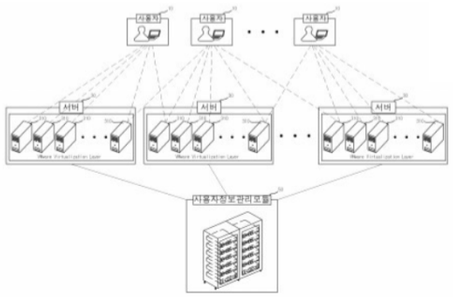
이글루 코퍼레이션의 '스파이더 SOAR'은 국내 주요 SOAR 플랫폼으로, 보안 위협의 대응 프로세스를 자동화해 보안 업무의 효율성을 높이는 솔루션이다. 위협정보의 공유, 다양한 정보보호 제품간의 연동, 수동 처리하던 단순 반복 업무를 자동화함으로써 각 경보이벤트에 대한 선별 및 대응을 효율적으로 수행하고, 수많은 기업에서 효율성을 검증받은 플레이북 기반의 표준화된 대응 체계 구축으로 위협판단 및 대응을 상향 평준화 할 수 있다.

스파이더 SOAR 플레이북

출처 : 이글루코퍼레이션 공식 홈페이지

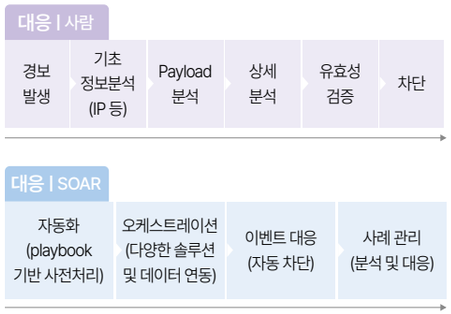
최근 이글루코퍼레이션 기사에 따르면, 클라우드 보안 운영 시스템 보안성 향상과 보안 자동화의 정확성을 높이기 위한 클라우드 및 SOAR 핵심 특허 2건을 확보한 것으로 보인다. 게다가 인공지능을 활용한 보안 기술 등 다양한 보안 관련 특허를 보유하여 사이버 위협에 선제적으로 대응할 수 있을 것으로 기대된다.

01 클라우드 컴퓨팅 환경에서 각 게스트머신이나 서버뿐만 아니라 사용자 별로 자원사용량을 수집하고 분석하여 제공하는 기술을 개발했다. 이를 통해 클라우드 보안 위협을 관리하고, 사용자별 게스트머신의 가용성을 감시하며, 보안 이벤트 정보를 제공할 수 있다.



클라우드 컴퓨팅 통합보안관제시스템의 개념도
(KR 10-2011-0003468)

02 보안 의사결정 단계에서 사용한 기준들을 데이터베이스에 저장할 뿐만 아니라 인공지능 탐지 모델의 이벤트 판단 학습 자료에 활용하여 탐지 모델의 성능을 향상시켰다. 이를 통해 대량의 보안 이슈가 발생해도 대응할 수 있는 보안 위협 대응 자동화 프로세스를 구축하였다.



보안 관제 흐름 및 SOAR 플랫폼에서의 보안 관제 흐름도
(KR 10-2022-0031209)

03 다중 인공지능 모델을 활용한 보안 관제 시스템을 개발하였다. 보안 이벤트를 수집하고, 이를 분석하여 분류형 모델로 분류 결과를, 설명형 모델로 설명 결과를 얻는다. 이 결과들을 기반으로 생성형 모델을 학습시켜 최종 데이터를 생성하고, 이를 보안 담당자가 이해할 수 있도록 검증한다. 신뢰도가 낮으면 프롬프트를 재생성하여 다시 시도한다. 이를 통해 시스템은 보안 담당자가 인공지능 결과를 신뢰하고 이해할 수 있게 한다. (KR 10-2023-0095816)

산업 · 가상 융합 보안

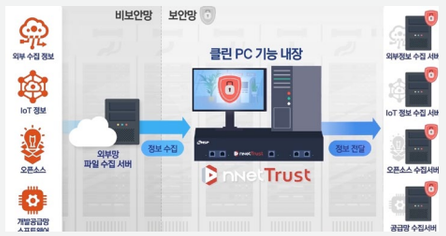
NNSP Next network security Provider

글로벌 스마트 보안의 선두주자

CPS(사이버물리시스템)는 물리적 세계와 상호작용하는 감지, 제어, 네트워킹, 분석을 조율하는 엔지니어링 시스템이다. 2021년 미국 동부의 송유관 기업 '콜로니얼 파이프라인' 은 CPS 사이버 공격을 받아 시스템이 마비되었고, 이로 인해 해당 지역은 연료 부족과 사재기 파동으로 큰 피해를 입는 사건이 있었다.

이와 같은 위협을 방지하기 위해, 운영기술(OT) 보안에 특화된 CPS 보안 전문 기업 앤앤에스피는 'nNet CPS 프로텍션 플랫폼'을 개발했다. 이 플랫폼은 OT에서 IT에 이르는 네트워크를 안전하게 보호하며, 중요 인프라에 대한 사이버 위협을 막고, 데이터의 안전한 가용성을 보장한다. 또한, 고객의 네트워크 에지를 보호하고 데이터 전송을 효과적으로 제어한다. 앤앤에스피는 이를 바탕으로, 인공지능(AI), 빅데이터, 클라우드 기술을 활용해 제로 트러스트(Zero Trust) 보안 체계를 구축했다. 이 체계는 네트워크 내 모든 접속과 활동을 항상 검증하여, 보다 철저한 보안을 제공할 것으로 기대된다.

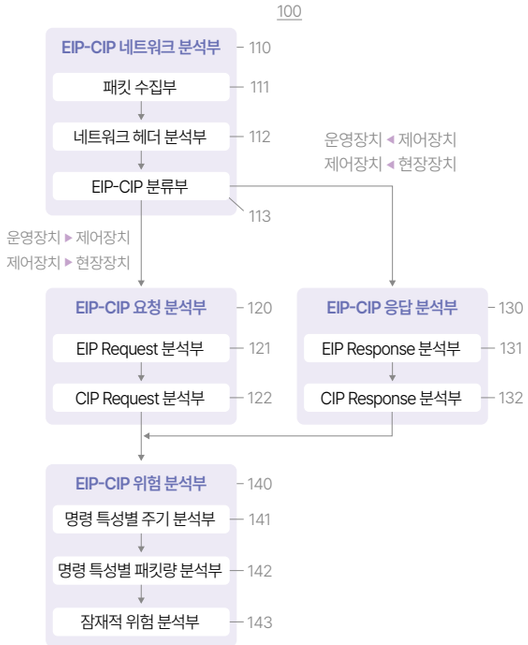
nNet CPS 프로텍션 플랫폼 nNetTrust



출처 : 유튜브 채널 'NNSP'

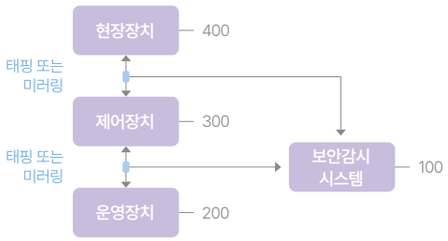
이처럼 앤앤에스피는 OT 보안을 넘어 CPS 보안으로 확장하고 있으며, 향후 국내외 글로벌 기업들과 협력해 글로벌 CPS 보안 생태계를 만들고 국가 주요 기반시설 제어망에서 스마트팩토리, 스마트시티, 스마트 의료, 국방, 엔터프라이즈, 클라우드까지 보호하는 글로벌 CPS 보안 전문 기업으로 발돋움할 계획을 가지고 있다.

01 산업용 네트워크 프로토콜 EtherNet/IP(EIP)와 상위 계층으로 CIP(Common Industrial Protocol)를 사용하는 스마트 제조 네트워크 환경에서 정상 패킷 분석을 통해 스마트 공장 네트워크 보안을 감시하는 기술을 개발했다. 이는 EIP-CIP을 통해 패킷 트래픽을 모니터링하고 네트워크 헤더, 요청 및 응답, 위험을 분석할 뿐만 아니라 정상적인 네트워크 리스트에 기초하여 이상 패킷에 대한 긴급 신호를 생성할 수 있다.



스마트 제조 네트워크 보안감시 시스템이 적용된 네트워크 구성 개념도 (KR 10-2019-0098954)

02 자동화 제어 시스템의 패킷 플로우 기반 보안 감시 시스템을 개발했다. 이 시스템을 통해 프로토콜별 패킷 개수, 패킷량, 동시 세션 수 등의 트래픽 정보를 포함하는 비교 프로토콜 리스트를 구성함으로써, 기준 화이트리스트와 쉽게 비교하여 이상징후 감지에 대한 처리속도를 향상할 수 있다.



시스템의 구성에 대한 블록도 (KR 10-2020-0159065)

03 국가전략기술 '사이버 보안' 이야기

국가전략기술로서의 '사이버 보안'

한국의 12대 국가전략기술 중 하나인 사이버 보안 기술은 디지털 전환과 함께 나날이 고도화되는 사이버 공격에 대응하기 위한 필수 기술로 자리잡고 있다. 특히, 최근 인공지능 등 신기술의 발전으로 사이버 위협의 대상과 방식이 다양화됨에 따라, 사이버 보안의 범위도 더욱 확대되어 중요성은 더욱 커지고 있는 추세이다.

사이버 보안은 사이버 공격으로부터 시스템, 네트워크, 데이터 및 디바이스를 보호하고 개인과 기업의 안전·신뢰를 보장할 뿐만아니라 국가 간 해킹을 통해 첨단기술 탈취, 통신망·기반시설 마비 등으로 이어질 수 있기 때문에 국가안보 측면에서도 필수적인 기술이라 할 수 있다.

이러한 환경에서 한국은 사이버 보안 분야에서 세계적인 경쟁력을 확보하고자 다양한 전략과 목표를 설정하고 있으며, 이는 국가 안보와 국민 생활의 안전을 지키기 위한 중요한 과제로 부각되고 있다.

사이버 보안 기술은 단순히 기술적 보호를 넘어서 경제·사회 전반에서 안정성을 다지는 역할을 한다. 디지털 전환이 가속화됨에 따라 사이버 보안은 국가의 핵심 인프라를 보호하고, 경제적 손실을 예방하며, 국민의 신뢰를 구축하는 데 필수적이다. 사이버 공격은 국가 간 해킹으로 인한 첨단기술의 탈취, 통신망 · 기반시설의 마비 등으로 이어져 국가안보의 위기를 초래할 수 있다. 따라서, 사이버보안을 강화하는 것은 국가의 주권을 지키고, 글로벌 경제에서의 국가 경쟁력을 유지하는 데 중요한 역할을 한다.

'사이버 보안' 우리의 정책과 산업 위치

먼저, '사이버 보안' 기술에 대한 주요국들의 정책을 살펴보면, 주요국은 기존 암호가 무력화되는 양자컴퓨팅 시대가 도래함에 따라 해당 환경에서 안전하게 암호기술을 이용할 수 있게 해주는 양자 내성암호 기술 확보를 통해 데이터를 보호하는 등 사이버주권 유지를 위한 치열한 경쟁을 벌이고 있다. 또한 점차 지능화되고 있는 사이버 공격에 선제적으로 대응하기 위해 AI를 활용한 지능형·능동형 사이버 보안 기술의 중요성을 인식하여 대규모 투자를 아끼지 않고, 정책적으로도 전폭적인 지원을 하고 있다.

미국의 경우, 국가안보를 지키고 국민의 번영을 위해 사이버 안전 보장을 추진하고 있다. ICT R&D 프로그램 NITRD의 예산 55억 달러 중 12% 비중으로 사이버 보안 투자계획을 수립하였으며, 연방정부 사이버 위협 정보공유 체계 개선을 통한 사이버 보안 강화를 위하여 CISA 연방정부 보호 실행 계획('20.10) 을 수립하였다.

한편 영국은 국가사이버보안전략('16~'21)에 따라 2조 7천억원을 사이버 보안에 투자하고, 국가사이버보안센터, 런던사이버보안혁신센터 설립을 통해 전문인력 양성 및 기업 지원을 추진하여 사이버 보안 분야 혁신을 선도하고 있다.

일본의 사이버 보안 예산 ('19) 은 852억으로 지속적으로 증가하고 있으며, 연금기구, 의료 부문 중심의 정보보호 강화에 막대한 예산을 투입하고 있다. 또한 IoT의 안전한 이용환경 구축, 사이버 보안센터 운영 등의 주요사업을 추진하고 있다.

호주는 사이버 위협 대응 및 안전한 사이버 환경 조성을 위한 '사이버 안보 전략('20.8)'을 발표하고 10년간 사이버 보안 분야에 약 1조 8,400억 원을 투입하는 등 국가차원의 사이버 보안 강화에 주력하고 있다.

한국은 정보보호 R&D 분야에 적극적으로 투자해 왔으며, 정보보호 산업 강화 및 생태계 조성에 힘쓰고 있다. 한국의 정보보호 R&D 예산('24)은 1,141억 원이며, 이는 전년 대비 22% 대폭 증가한 금액으로, 정부는 이를 통해 사이버 보안 분야에서 기술 수준을 높이고 글로벌 경쟁력을 확보하기 위해 다양한 정책을 추진하고 있다.

이러한 정책의 일환으로, 먼저 인력양성 측면에서 국정과제인 사이버 10만 인재양성을 목표로, 학위 및 비학위 과정을 포함한 전문 인력 확보와 수요기반형 실무 인재양성 프로그램을 확대 및 강화하고 있다. 특히, 사이버 침해 사고에 실전적으로 대응할 수 있는 사이버훈련 인프라를 확충하며, 일방향 침해사고 방어와 양방향 공방훈련이 가능한 사이버훈련장(Security-Gym)을 확대하고 있다.

국제협력 측면에서는 주요 사이버 보안 강국 내 대학 및 연구기관과의 인력 교류 등을 통해 글로벌 인재를 확보하고 있다. 양자내성암호 등 국제표준 및 제도 논의에 참여하고, 중대한 침해 사건에 대해서는 적극적인 정보공유와 연합 차원의 공조를 강화하고 있다. 예를 들어, 한·미 사이버안보 고위운영그룹(CyberSecurity SSG) 강화를 통해 국제 협력을 증진하고 있다.

마지막으로 제도 및 인프라 측면에서 민 · 관 · 군 사이버 보안 위기대응 조직 간 정보 공유(이상 징후, 침해 시도) 및 위기대응 거버넌스를 강화하고, 차세대 연구개발에 있어서 유기적인 결합을 강화하고 있다. 제로트러스트, SBOM 등 새로운 보안 패러다임 전환이 현장에서 적용될 수 있도록 관련 가이드라인과 제도를 고도화하고, 실증 지원을 강화하고 있다.

이와 같은 전략적 접근을 통해 한국은 사이버 보안 분야에서의 기술적 역량을 높이고, 국제적인 경쟁력을 강화하며, 안전하고 신뢰할 수 있는 정보보호 환경을 구축하고자 노력하고 있다.

디지털 전략, 메타버스 신산업 선도 전략 등을 범정부 합동으로 박차를 가하고 있음. 정보보호 시장에 있어 응용보안에 치중된 측면이 존재하며, 상대적으로 글로벌 시장에 비해 협소하나 정부의 제도 보완이 이루어지고 있음

풍부한 내수 시장을 바탕으로 새로운 기술을 개발하고 있으며, 막강한 자금력으로 연구에 있어서 한국을 뛰어넘고 있음

논문과 특허의 양적 활동력 및 기술력 지표 등이 상대 비교국 대비 열위에 있음. Society 5.0을 기반으로 가상 융합 기술 및 보안 개발 전략을 추진 중에 있음

GDPR(General Data Protection Regulation)을 출발로 데이터의 보안에 중점을 두고 정책 및 기술개발에 선도적 역할을 담당하고 있음

관련 분야 세계 선도기업을 보유하고 있어 글로벌 경쟁력을 확보함

국가별 사이버 보안 기술수준

2022년도 기술수준평가 결과, 과기부, 2024.02.29

'사이버 보안' 중점기술 분야

데이터 · AI 보안기술

#데이터 프라이버시 #보안 취약점 #경량 거대언어모델

데이터·AI 보안기술은 데이터 수집·활용·폐기 전 과정에 AI를 적용한 지능형·능동형 보안기술로, AI 대상 보안위협에 대응하는 사이버보안의 중점 기술이다. 디지털 전환 가속화 및 AI · 양자 고도화에 따라 사이버 보안 패러다임 변화에 중요한 역할을 하고 있다.

글로벌 기술 및 산업 동향을 살펴보면, 기존의 암호체계가 무력화되는 양자컴퓨팅 시대가 도래함에 따라 양자 내성암호 확보를 통한 데이터 보호 등 사이버주권 유지를 위해 각국은 치열하게 경쟁 중에 있다. 또한, AI 보안 분야에서는 AI를 활용한 지능형·능동형 사이버 보안기술, AI 활용 서비스 대상 사이버 공격 대응 기술 등이 점차 중요도가 높아지고 있다.

EU의 경우, 데이터 보호 규정인 GDPR 등으로 인해 기업이 수집하고 활용하는 개인 데이터에 대한 프라이버시 강화가 중요한 추세이다. 이에 따라 신뢰 · 보안 컴퓨팅 등 개인정보 보호를 위한 암호 및 시스템 보안 연구가 활발히 진행되고 있다. 특히, 영국은 '20년 클라우드를 구축할 때, 국가사이버보안센터를 중심으로 제로 트러스트 아키텍처 설계 원칙을 제시하였다.

한국은 데이터 보안과 관련하여 암호데이터 활용 기술 및 계산없이 암호데이터 자체를 연산하기 위한 동형 암호, 함수 암호 등의 기술이 연구되고 있다.

이와 관련하여 서울대(크립토랩), 삼성 SDS 등 국내기관에서 동형암호 원천기술을 확보하였으며, 산업현장에서의 데이터 활용 영역 확대를 위한 연구가 진행 중에 있다.

또한 AI를 이용한 데이터 공격 및 방어 분야에서는 적대적 기계학습을 이용한 AI 역기능 유발공격에 대한 자동화 대응, AI 시스템의 오작동이나 이상행위 등을 판단 · 예측하여 대응할 수 있는 고신뢰 AI 서비스 기술 등이 연구되고 있다

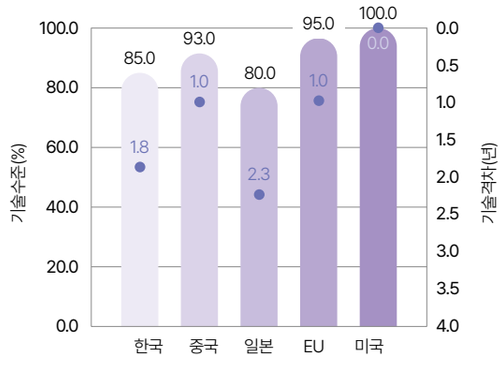
이에 정부는 동형암호 등 데이터 프라이버시 기술 고도화, 사이버 보안에 특화된 능동형 AI 활용 기술개발 등 차세대 암호 및 AI 보안기술 자립화 실현을 위해 국가 인프라 보호 및 개인정보보호 핵심기술 개발을 위한 투자를 강화하고 있다. 이에 따라 프라이버시 보호(PET) 및 생성형 AI 보안 기술에 대한 현장 시범적용을 추진할 계획이다.

초신뢰 암호 기술
- 기존 암호체계 무력화에 선제적 대응
- 양자내성암호와 기존 암호의 양자내성 전환 기술 확보

데이터 안전 활용
- 프라이버시 강화 기술(PET) 개발
- 동형암호 등 기능성 암호
- 데이터 비식별화 등 데이터 Lifecycle 보호 기술 고도화

신뢰가능한 AI (Security for AI)
- AI 공격 탐지 · 방어 능력 강건성 (Robustness) 확보
- 취약점 자체점검 역량 개발

AI기반 능동 · 자율 보안(AI for Security)
- 경량형 거대언어모델(sLLM) 기반 보안 특화모델 개발
- AI 기반 공격 알고리즘 자동방어 (Defensive AI) 기술 확보



2022년도 기술수준평가 결과, 과기부, 2024.02.29

디지털 취약점 분석 · 대응(공급망 보안) 기술

#취약점 분석 #보안 조치 #디지털 위협 #보안 취약성 #무결성 검증

디지털 취약점 분석 · 대응(공급망 보안) 기술은 부품 · 장비 및 SW의 개발-도입-운영(업데이트) 등 디지털 공급망 전주기를 대상으로 한 보안 취약점 탐지 · 관리 및 검증을 위한 기술이다. 디지털 취약점은 공격을 받을 경우, 개별기업 뿐만 아니라 국가주요시설에도 커다란 타격을 받을 수 있고, 특히 랜섬웨어 공격일 경우, 복구가 어려워 국가적 차원에서의 대응이 필요하다.

2020년 포춘 1000대 기업들을 고객으로 둔 IT 솔루션 및 소프트웨어 업체 'SolarWinds' 의 공급망 해킹 사태는 전세계 18,000여개 회사에 피해를 입혔으며, 완전 복구만 1년 이상 소요될 것으로 알려졌다. 이처럼 최근 전세계적으로 HW · SW의 미식별 취약점을 침투하여 데이터 탈취 및 금품을 요구하는 공급망 공격이 지속적으로 발생하고 있다.

글로벌 기술 및 산업동향을 살펴보면, 미국의 경우, 화웨이 등 중국 빅테크 기업의 백도어 공격 위협을 경계하는 한편, 국가사이버 안보 행정명령('21.5.)을 통해 국가와 SW 계약시 보안 강화를 위해 보안요소 리스트인 SBOM 제출을 의무화하고 있다.

EU는 데이터보호를 위한 개인정보보호법령 및 신뢰성 확보를 위해 사이버보안 인증체제를 시행하고, 자동차 사이버보안 관리체계에 대한 인증 취득을 요구하는 등 사이버보안, 프라이버시 이슈를 내세워 기술 무역장벽을 구축하고 있다.

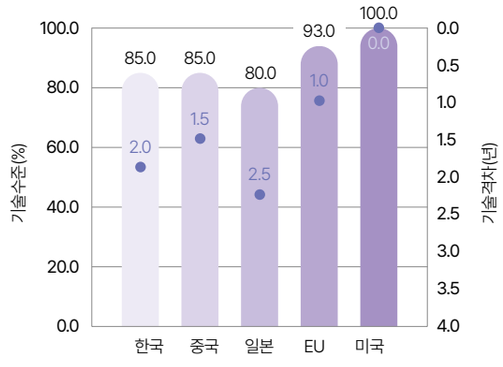
한국은 공급망 보안을 위해 HW와 SW의 보안성 강화뿐만 아니라 제품개발 및 양산, 공급 과정 전반에 걸쳐 보안성을 강화하기 위해 노력하고 있다. 그러나 공급망 보안에 대한 제도적 기반을 마련한 미국과 달리 한국은 기업 개별로 SBOM을 적용하고 SW 테스트 등 기술개발을 추진하고 있는 상황이다.

이에 정부는 SBOM 기반 SW 무결성 검증 체계를 확립하고, 랜섬웨어 원천무력화를 위한 데이터 복원력 기술 개발 등 디지털 밸류체인 전주기를 대상으로 선제적 방어와 능동적 대응을 실현할 계획이며, 이를 위해 기존 보호 · 탐지 기술 중심에서 공격억지 · 예방 · 복원력 향상 중심의 투자 방향을 전환하고, 글로벌 SW 공급망 요구사항 · 규제에 대응할 수 있는 인프라를 구축할 계획이다.

무결성 검증 및 취약점 대응
- SBOM(Software Bill of Materials) 기반 SW 무결성 검증 체계화
- 위협정보 공유체계를 통한 자산 취약점 수집
  → ZeroDay 자동탐지 추진

랜섬웨어 탐지 · 차단 복구
- 잠복 상태 랜섬웨어를 사전 탐지 · 차단 툴 자립화
- 랜섬웨어 원천무력화를 위한 데이터 복원력 기술

사이버 침해사고 포렌식 및 원점 탐지
- 사이버 공격에 대한 포렌식 자동화 공격패턴 식별을 통한 침해대응 시간 단축
- 역추적 통한 침해원점 탐지 역량 강화



2022년도 기술수준평가 결과, 과기부, 2024.02.29

네트워크 · 클라우드 보안기술

#네트워크 보안 #보안 인증 #인프라 최적화 #제로트러스트

네트워크·클라우드 보안 기술은 5G·6G 등 통신 네트워크를 대상으로 하는 보안 위협을 최소화하고, 클라우드 서비스 등 새로운 응용 서비스의 신뢰성·안정성을 보장하기 위한 기술이다. 차세대 통신 시대가 도래함에 따라, 6G 조기 상용화('28)를 위해 6G 설계단계부터 특화된 보안기술 및 클라우드 환경을 온전히 보호하기 위한 관련 기술 확보가 절실한 상황이다.

글로벌 기술 및 산업동향을 살펴보면, 주요국들은 6G 개발 전략이 본격화되면서, 안전한 6G 구현의 핵심으로 보안·프라이버시 강화를 우선시하고 있다. 미국의 경우, 6G 경쟁력 강화를 위한 Future Network Act에 사이버 보안 위협 대응 내용을 포함하고 있다. 또한 기업들의 클라우드 전환이 가속화되면서, 사용자 대상 철저한 인증(제로트러스트) 등 클라우드에 적합한 새로운 보안기술 개발을 본격화하고 있다.

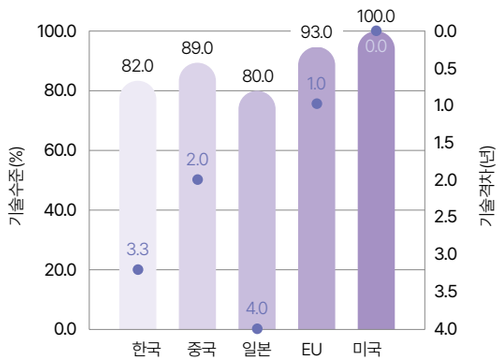
한국은 삼성(6G 비전), LG(6G 연구센터) 등 주요기업이 6G 보안 강화 연구를 착수 하였으나, 클라우드 보안 분야는 우리나라 솔루션이 전무한 수준이다.

또한, 공공기관의 민간 클라우드 서비스 이용 시 CSAP 인증 획득 서비스로 제한되어 있으며, 최근 SaaS 간편 인증 시행이 되어 지속적인 제도 운영 모니터링과 필요시 개선방안을 도출해야 한다. 제로트러스트 개념을 각 기관의 네트워크 환경과 보유 데이터에 적용하기 위해서는 법 · 제도적 시행 원칙이 수립되어야 하며, 보안기업의 인력 수급 및 양성에 대한 어려움을 해결하기 위한 정책적 지원이 필요하다. 또한, 국내 클라우드 보안 기술 및 제품의 신뢰성을 확보하기 위해 시험 · 검증 환경을 제공하고, 다양한 퍼블릭 클라우드 서비스 제공자들과의 협력 체계를 통한 기술 지원이 필요하다. 외산 솔루션 의존도를 줄이고 연구개발 인프라를 강화하기 위한 방안도 마련되어야 한다.

이에 정부는 클라우드 환경에 최적화된 제로트러스트 아키텍처 구현·실증, AI 기반 지능형 보안관제 자동화 대응(SOAR) 기술 고도화 등을 통해 제로트러스트 아키텍처 기반 클라우드 · 네트워크를 구현할 계획이며, 이를 위해 주요 분야 대상 제로트러스트 모델 적용 · 확산 시범사업을 검토 중에 있다.

제로트러스트 기반 클라우드 보안
- 클라우드 네이티브 환경에서 적용 가능한 보안기술 개발
- 보안시스템과 상호연동이 가능한 제로트러스트 아키텍처 구현
- 강화된 인증 및 지속적 동적 접근 제어 기술을 최적화

차세대 통신 대비 지능형 보안
- 6G 상용화 일정에 맞춰 인프라 성능에 최적화
- AI 기반 지능형 보안관제 자동화 대응(SOAR) 기술 고도화



2022년도 기술수준평가 결과, 과기부, 2024.02.29

산업 · 가상융합 보안기술

#산업 보안 #가상융합 보안 #보안 표준화 #사이버-물리 융합

산업 · 가상융합 보안기술은 물리환경과 사이버환경이 융합되는 메타버스, 모빌리티 등 다양한 신산업 분야에 특화하여 정보 · 물리보안을 융합하여 적용하는 기술이다. 최근 급변하는 신산업 환경에서 발생할 수 있는 다양한 위험을 사전에 예방하고, 국민의 안전을 지키는 데 핵심적인 역할을 담당하고 있다.

글로벌 기술 및 산업동향을 살펴보면, 주요국들은 메타버스, Web3 등 가상융합 산업 성장 기대와 함께 부작용에 대한 우려가 확산되면서 보안 대응 기술 연구가 활발하게 이루어지고 있다. 특히 정보유출, 마약 등 다크웹 은닉 서비스를 통해 발생할 수 있는 사이버 범죄 추적과 관련된 기술개발이 주로 진행되고 있다. 또한 모빌리티 분야 UAM 산업육성을 위해 보안기술을 포함하는 기술개발 · 투자도 확대되고 있는 추세이다.

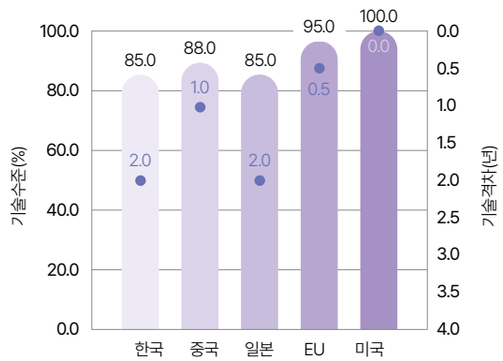
최근 우크라이나 전쟁, 미국 송유관 해킹, 북한 가상자산 탈취 등 국민생활과 직결되는 신종 안보 위협으로 인해 산업 · 가상융합 보안 기술의 중요성은 어느 때 보다 더 크게 부각되고 있다. 그에 반해 한국은 신산업의 급격한 부상에 따른 부작용 우려도 높을 뿐만 아니라, 관련 대응 기술 확보는 미흡한 상황이며, ETRI 및 방산업체 위주로 기술 개발 중이다.

이에 정부는 지능형 · 자율협업형 CCTV 기술, 개인정보의 과도한 집중으로 인한 피해를 방지하고 정보 활용을 보장하기 위한 분산컴퓨팅 기반 데이터 신뢰성 기술 확보 등 첨단산업 융합보안 솔루션 확보를 통해 국민 생활 안전망을 구축할 계획이며, 이를 위해 기존 메타버스 관련 보안 사업을 Web 3.0 등으로 최신화 · 차별화하고, 국가안보 차원에서 중요성이 높은 ICS/SCADA(인프라 감시 · 데이터 취득을 위한 산업 제어 시스템) 및 모빌리티 보안에 중점적으로 투자할 계획이다.

지능형 영상보안
- 자율적 위험 감지 · 판단 · 대응 가능한 지능형 CCTV 기술
- 드론 · 블랙박스 등 이기종 기기간 유기적 협업 시스템

탈중앙화 보안 (Web3.0)
- 탈중앙화 신뢰 기반 강화 및 사이버범죄 추적 · 대응
- 분산컴퓨팅 기반 마이데이터 플랫폼 확보

사이버-물리 융합보안
- 국가기반시설, 에너지 등의 제어 시스템 보안기술 자립화
- 자율주행 · 드론 등 미래 모빌리티의 사이버안전 신뢰성 고도화



2022년도 기술수준평가 결과, 과기부, 2024.02.29

04 출연(연) 보유 '사이버 보안' 기술

한눈으로 보는 출연(연) 기술 보유현황

사이버 보안 중점기술 분야별 기술 보유현황

출연(연) 보유 인공지능 주요기술

데이터 · AI 보안 기술

- KRRI · 철도 주요정보 보호를 위한 철도 보안인증시스템 / 최현영
- ETRI · 디지털 신원 관리 서버 기술 / 이성훈
- ETRI · 경량 IoT 기기 공격 확산 방지를 위한 스마트 세그멘테이션 솔루션 기술 / 임재덕
- NSR · 산업제어시스템 사이버 안전성 시험 기술 / 조연준

디지털 취약점 분석 · 대응 (공급망 보안) 기술

- NSR · 제어시스템 운전정보 이상징후 탐지기술 / 윤정한
- NSR · 사이버 위협정보 자동분석 시스템 구축 기술 / 정계옥
- ETRI · 클라우드 네이티브 기반 MEC 플랫폼 취약성 검증 기술 / 박종근

네트워크 · 클라우드 보안 기술

- KISTI · 사이버공격 실시간 추적 가시화 기술 / 송중석
- NSR · 클라우드 네이티브 운영환경 런타임 보안기술 / 장인혁
- ETRI · IPMI 서버용 펌웨어 보안 분석 기술 / 이상수
- ETRI · IoT 인프라 보안 위협 확산 방지를 위한 스마트 세그멘테이션 솔루션 기술 V3.0 / 김정녀

산업 · 가상융합 보안 기술

- KISTI · 접촉자 추적 시스템 / 김선호
- ETRI · 스마트 IoT 기기용 경량형 네트워크 보안 프로토콜 기술 / 이윤경
- ETRI · 인공지능 기반 마스크 등 가려짐에 강인한 성별, 연령, 표정, 객체 인식 기술 / 윤호섭

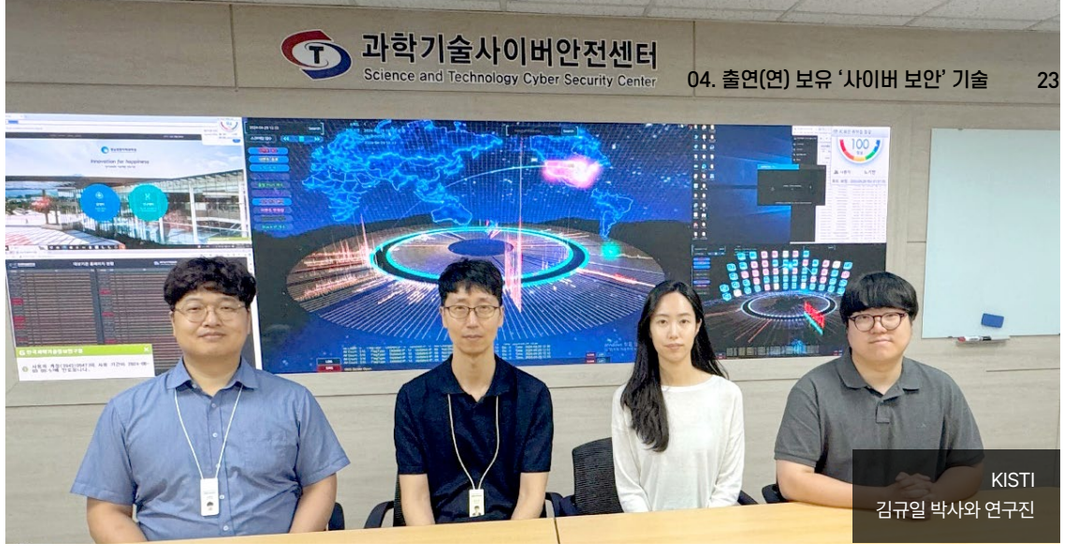
사이버 보안 기술개발 연구자 인터뷰

KISTI
과학기술사이버안전센터

실시간 사이버공격 추적 가시화로 보안효율성 극대화

한국과학기술정보연구원
김규일 박사

현대에는 정보통신기술 발달 및 초연결 사회로 변화하면서 민감한 기관 · 개인 데이터까지 막대한 양의 정보가 사이버공간에서 행해지고 있으며 이와 동시에 금전을 노리는 사이버공격 역시 날로 급증하고 있습니다. 이에 KISTI는 2005년부터 과학기술사이버안전센터 구축 · 운영을 통해 과기부 소속·산하 61개 기관을 대상으로 전주기적 정보보호 서비스를 수행하고 있으며, 사이버안전 최전선에서 대응하는 보안관제센터의 역할이 그 어느 때보다 중요한 상황입니다. 그러나, 기존의 보안관제는 텍스트 정보를 중심으로 악성 행위 여부를 판단하기 때문에 보안관제 요원의 업무 효율성이 매우 낮을 뿐만 아니라 대량의 보안이벤트에서 실제 비정상적인 사이버공격을 직관적으로 발견하기 어려웠습니다. 이에 침해탐지 · 방지시스템(IDS, IPS)은 탐지한 대용량의 공격이벤트를 기반으로 공격자(IP)의 행위정보를 실시간으로 가시화하여 사이버공격을 직관적으로 분석함으로써 신속한 대응이 가능하게 해 보자는 것이 연구의 시작점이었으며, 연구 개발을 통해 기존 텍스트 분석 중심에서 직관적 가시화 기반의 분석체계 전환에 성공하여 보안관제 분석시간을 획기적으로 단축할 수 있었으며, 필수 불가결한 보안관제의 신속성 · 정확성을 크게 향상하는데 기여할 수 있었습니다.



KISTI
김규일 박사와 연구진

사이버공격 가시화 방법론의 핵심은 보안이벤트를 발생시킨 공격자(IP)의 행위정보를 실시간은 물론 추적 분석을 가능하게 하는 것입니다. 그러나, 전체 공격자(IP) 및 보안이벤트를 가시화하는 것은 현실적으로 불가능하기 때문에 위험도가 높은 IP를 우선적으로 선별 · 분석이 가능하도록 위험도를 자동으로 산출해주는 스코어링 알고리즘을 개발하였습니다.

스코어링 알고리즘은 10가지 공격행위 정보를 토대로 실시간 및 장기간을 모두 고려하기 때문에 정확한 위험도 산출이 가능하며, 이를 통해 대규모 보안이벤트에 포함된 공격자 IP 중에서 고위험군 500개를 선별하여 직관적으로 가시화할 수 있습니다. 특히, 선별된 IP는 공격자의 공격행위에 대한 순간적인 변화, 규칙/불규칙적인 패턴 변화, 공격행위의 빈도(빠름/느림 등) 변화, 공격행위의 양(감소/증가/일정 등)의 변화 및 이들 공격패턴의 조합 등을 직관적 · 상관적으로 가시화함으로써 다양한 사이버 공격에 대해 탐지 및 대응할 수 있습니다.

게다가 각 IP주소에 대한 공격행위를 최소 1일부터 최대 1년까지 장기간 분석할 수 있는 인터페이스를 제공하여 보안관제요원은 이러한 장기간 분석 기능 활용을 토대로 더욱 효율적인 공격 탐지 및 분석업무를 수행할 수 있습니다.

개발한 가시화 시스템을 상용화하기 위해 실시간 보안관제 업무에 실질적으로 활용될 수 있도록 무엇보다 처리성능, 인터페이스 및 경량화를 우선시하였습니다. 먼저, 1분당 최대 20만 건의 대용량 사이버위협 정보에 대한 수집 · 분석 · 가시화가 가능하도록 실시간 처리 성능을 개선하였으며, 보안관제 요원이 통계생성·가시화 정밀설정이 가능하도록 인터페이스를 고도화하였습니다. 또한, 간단한 설정만으로도 집중적인 사이버공격 모니터링 및 공격 발원지 · 추가 피해 시스템 가시화가 가능할 수 있게 사용자 맞춤형 인터페이스(상관관계 가시화 등)를 추가 개발하였으며, 상용 정보보호시스템 내에 모듈방식으로 탑재가 가능하도록 경량화 설계 · 개발을 통해 기존 다중 구성된 시스템을 1Box 형태로 구성함으로써 기술 상용화를 앞당길 수 있게 추진하였습니다.

현재는 침입탐지시스템(IDS/IPS)에서 수집된 대용량의 보안이벤트만을 대상으로 가시화하고 있으나, 이기종의 사이버위협정보에 대한 연계를 통해 보다 종합적인 수집 · 분석 및 가시화가 가능할 수 있게 시스템의 범용성 및 확장성을 확보하는 데 노력을 기울이고 있습니다.

본 실시간 사이버공격 추적 가시화 기술은 현재, 과기정통부 과학기술사이버안전센터에서 실제 보안관제에 활용되고 있으며, 국가사이버안보센터(NCSC)를 중심으로 하는 부문사이버안전센터, 단위사이버안전센터에 도입될 경우, 기술적 · 경제적 파급효과가 매우 클 것으로 판단하고 있습니다. 특히, 국내 · 외적으로 솔루션 형태로 보유 및 판매하고 있는 정보보안 업체가 없기 때문에 국제 보유 지재권을 기반으로 세계시장 진출을 위한 발판을 마련하여 판매 매출 등 지속적인 성과를 올릴 수 있을 것으로 기대하고 있습니다. 아울러, 앞서 언급하였듯이 본 기술은 실제 보안관제 업무에 적용 가능한 수준의 실용적 가시화 시스템을 개발하였기에 제품 상용화까지 걸리는 시간을 단축할 수 있으며 가시화 기반의 공격행위 분석방식을 적용하여 보안관제 효율을 향상할 수 있습니다.

국내외 사이버 보안의 경우, 최근 몇 년 동안 급격히 성장하고 있으며 날로 진화하는 사이버위협에 대응하기 위해 기업 · 기관들은 최신 보안 기술 도입을 고려하기 있어 앞으로의 시장 성장도 지속될 것으로 예상하며, 이러한 보안 트랜드에 맞춰 본 가시화 기술이 시장에서 경쟁력을 갖출 수 있도록 니즈를 파악하고 개선 · 반영해 사이버 보안을 공략해 나아갈 계획입니다.

사이버 보안인증시스템 개발로 안전한 철도 운영 보장

한국철도기술연구원
최현영 박사

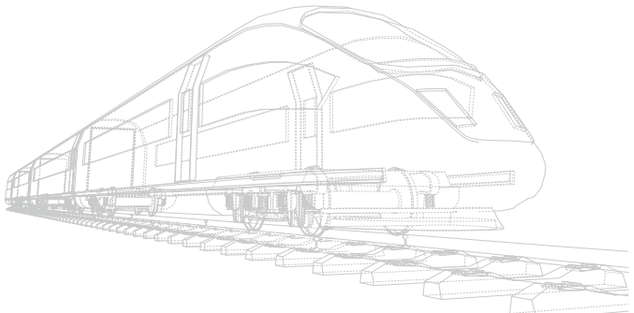
그 동안 철도는 국가기반시설로 폐쇄망으로 운영되는 특성으로 사이버 보안 침해에 대해 비교적 안전하다는 인식이 강하였습니다. 하지만 철도의 안전한 운영을 위해 인프라, 차량, 신호통신, 관제 등 다양한 시스템이 네트워크로 연결되어 감에 따라 주요 데이터에 대한 침해 사고의 가능성과 위험이 증가하게 되어, 철도 보안인증시스템을 개발하게 되었습니다.

개발한 철도 보안인증시스템은 네트워크를 통해 전송되는 데이터를 보호하는 것으로, 전송된 데이터가 불법적으로 생성(위조)되었는지 여부, 전송 과정에서 변조되거나 재구성 되었는지의 여부를 확인할 수 있는 데이터 무결성을 확보하며, 또한 정당한 권한을 부여받은 장치를 제외한 다른 장치가 데이터를 중간에 가로채 보더라도 데이터를 읽어 보지 못하도록 하는 기밀성을 확보하는 기술입니다. 구체적으로, 철도 보안인증시스템은 인증, 전자서명, 암호화, 방화벽, 침입탐지 기능을 수행하며, 메시지의 유입 경로에 따라 내부로 들어오는 패킷은 전자서명을 검증하고 암호화된 메시지를 복호화하며, 이상행위를 탐지하고 허용되지 않는 사용자를 차단합니다. 이와 반대로 보안 단말기를 통해 외부로 나가는 패킷은 전자서명하고 암호화하며, 이상행위를 탐지하고 허용되지 않는 사용자를 차단합니다. 이러한 보안 기능 수행을 위한 보안인증서 및 각종 키를 관리하는 관리서버도 포함합니다.

철도 산업 분야에서는 새로운 기술을 적용하기 위해 먼저 충분한 검증을 위한 실증 사업과 그 결과를 바탕으로 기술기준, 표준 제정 등을 통해 해당 기술의 신뢰성을 제고하여 적용하게 됩니다. 철도 보안인증시스템은 시작품 개발을 통해 기능적인 검증과 시험선에서의 현장 검증을 수행한 바 있으며, 철도 운영 및 환경 조건에서의 충분한 데이터를 기반으로 실증 사업이 추가로 수행된다면 더 높은 신뢰성을 가질 수 있을 것으로 기대하고 있습니다. 아쉽게도 현재까지 철도 보안인증시스템은 산업에 적용되지 않았으나, 한국정보통신기술협회(TTA) 표준을 통해 철도에서도 보안 기술의 필요성과 공감대를 확보한 바 있으며, 철도 산업 적용을 위해 민간기업에 기술이전, 한국정보통신기술협회(TTA) 국내 표준 제정을 통하여 상용화를 준비하고 있습니다.

한국철도기술연구원
스마트전기신호연구본부 최현영 책임연구원

사이버 보안 침해사고는 점점 고도화되고 그것의 피해 규모는 계속하여 증가될 것으로 예상되는 바, 철도 보안인증시스템은 국민의 안전과 편의를 위한 철도 운영에 있어 중요한 기술이 될 것으로 생각합니다. 특히 무인운전, LTE-R과 같이 고도화된 시스템이 도입될수록 사이버 보안 관점에서의 대책은 계속해서 요구될 것이며 운영 조건에 맞게 발전될 것으로 생각됩니다.



CCTV와 AI의 만남으로 지능형 영상 보안 분석

한국과학기술정보연구원
김선호 박사

· 미국 버지니아공대 컴퓨터과학 박사학위
· 現) KISTI에서 25년이상 인공지능과 데이터마이닝 연구
· R&D PIE 인공지능 분과 담당

팬데믹 상황에서 사이버 보안 관점에서 두 가지 중요한 기술을 개발하였습니다. 첫 번째는 감염 예방을 위한 "사회적 거리 측정 시스템"입니다. 이 시스템은 공공장소에서의 사회적 거리두기 준수 여부를 모니터링하며, 사람의 얼굴 방향, 행동, 접촉 여부 등의 정보를 분석하여 감염병의 전파 위험을 평가합니다. 이 기술은 개인의 위치와 행동 데이터를 수집하고 분석하기 때문에, 개인 정보 보호와 데이터 보안이 중요한 고려 사항입니다.

두 번째는 "접촉자 추적 시스템"으로, 감염병 확진자와의 직접 및 간접 접촉자를 식별하여 신속히 검사할 수 있도록 지원합니다. 이 시스템은 카메라와 센서를 통해 수집된 정보를 기반으로 접촉 경로와 시간을 추적하며, 카메라 사각지대의 접촉까지 추론할 수 있습니다. 따라서 이 시스템은 데이터의 기밀성과 무결성을 보장해야 하며, 민감한 정보 보호를 위한 강력한 사이버 보안 조치가 필요합니다. 두 기술 모두 인공지능과 컴퓨터 비전 기술을 활용하여 방역 효율성을 높이지만, 개인정보 보호와 사이버 공격으로부터의 방어가 필수적입니다.

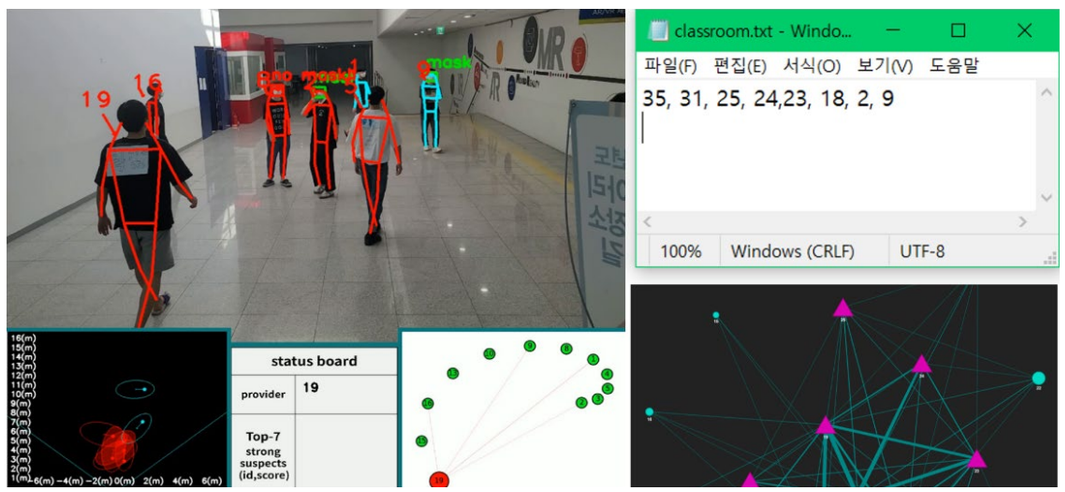
본 기술은 인공지능과 컴퓨터 비젼 기술을 활용하여 기존 인프라인 CCTV 영상 데이터만을 이용하여 검사 대상자를 탐색하는 기술로, 기존 기술과의 차별점은 동선 추적 기술과 물체 인식등의 기술을 이용하여 감염자와의 직접 접촉 외에, 물건을 매개로 한 간접 접촉, 시간차가 존재하는 시간차 접촉, 영상이 존재하지 않는 공간에서의 논리적 추정 접촉을 가능하게 한다는 점입니다. 게다가 기존 CCTV 인프라를 활용하여 추가 하드웨어 없이 영상 처리 분석 장치와 통신 장비만 추가하면 기술을 적용할 수 있어 비용 효율적이고 신속한 도입이 가능합니다. 그러나 상용화를 위해서는 기존 CCTV 시스템의 최신 상태 유지 또는 업그레이드가 필요하며, 개인정보 보호법을 준수하기 위해 법률 전문가와 협력하여 데이터 보호 정책을 수립하고, 데이터의 익명화 기술을 적용하는 것이 필수적입니다. 그리고 적용하기 위해 정보 보호법을 준수하기 위한 관리 시스템을 구축할 필요가 있으며, 이를 위해 법률 전문가와 협력하여 엄격한 데이터 보호 정책을 수립하고, 데이터를 익명화 기술을 적용해야 합니다.

먼저, '사회적거리측정시스템'은 단순히 물리적 거리를 측정하는 것을 넘어, 사람의 행동, 접촉 여부, 물리적 장벽 등을 종합적으로 분석하여 실제 감염병 안전도를 평가합니다. 이는 공공장소나 대규모 행사에서의 방역 효율성을 크게 높일 수 있습니다. 앞으로 이 기술은 더 많은 변수를 포함하고, 인공지능 알고리즘을 고도화하여 더 정교하고 실시간으로 사회적 거리두기 상태를 평가할 수 있을 것입니다. 예를 들어, 웨어러블 기기나 스마트폰과 연동하여 개인 맞춤형 경고 시스템을 구축할 수도 있습니다.

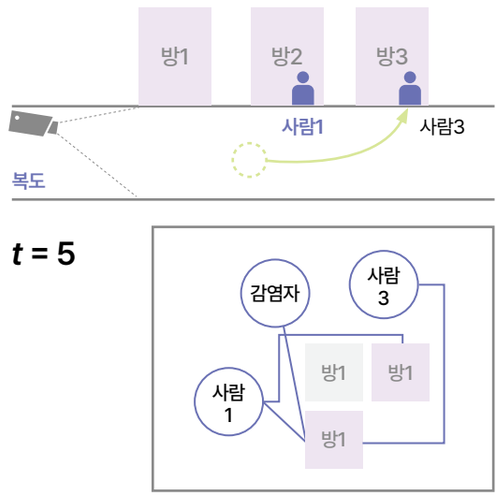
'접촉자추적시스템'은 확진자의 동선을 추적하고, 직접 접촉자뿐만 아니라 간접 접촉자까지 판별해냅니다. 특히, 공간과 공용 물건을 추적하여 시간차 접촉을 논리적으로 추정하는 점에서 차별화됩니다. 이 기술은 향후 더 많은 데이터 소스를 통합하고, 고도화된 머신러닝 기술을 적용하여 접촉 추적의 정확도와 신속성을 더욱 향상시킬 수 있을 것입니다. 또한, 사생활 보호를 위한 암호화 기술과의 결합을 통해 개인정보 침해 없이 효율적인 접촉자 추적이 가능하도록 발전할 것입니다.

두 기술 모두 기존의 CCTV 인프라를 활용한다는 점에서 경제적이고 실용적으로 더 많은 공공장소와 사설 기관에서 이 기술을 활용함으로써, 감염병 발생 시 신속하고 효율적인 대응이 가능해질 것입니다. 결론적으로, '사회적거리측정시스템'과 '접촉자추적시스템'은 인공지능과 컴퓨터 비전 기술을 바탕으로 방역의 새로운 패러다임을 제시합니다. 앞으로의 발전 가능성은 무궁무진하며, 이를 통해 우리는 더 안전한 공공 환경을 구축하고, 팬더믹 상황에 더욱 효과적으로 대응할 수 있을 것입니다.

사회적 거리 측정 및 접촉자 추적 시스템



방을 매개로 한 간접 접촉 추정 알고리즘



방 출입 정보

들어간 방 / 사람id / 들어간 시간 / 나온 시간

방 출입 history

(방3, 사람1, 1, 3) (방3, 사람2, 2, 4)
(방2, 사람1, 3, -1) (방3, 사람3, 5, -1)

방-사람 역학관계

	방1	방2	방3
사람1	0	1	1
사람2	-	0	1
사람3	-	-	1