10 글로벌사이버보안기술연구센터 운영

<table>
<tr><td>사업실명제
등록번호</td><td>2021-10</td><td>담당부서
작성자</td><td>KAIST 사이버보안연구센터
(강선정 / 042-350-8394 /
nadiakang@kaist.ac.kr)</td></tr>
<tr><td>사 업 명</td><td colspan="3">글로벌사이버보안기술연구센터 운영</td></tr>
<tr><td>사업개요
및
추진경과</td><td colspan="3">
○ 추진배경: 2010년 5월 지식경제부, 국회 교육과학기술위원회, 청와대 정책실에서는 국가 차원의 사이버보안과 연구개발을 전담 수행하는 연구 조직의 필요성이 대두되었으며, 2010년 11월 KAIST에 공익성(公益性), 공공성(公共性)을 갖는 ‘글로벌사이버보안기술’ R&D와 고급 인재 양성을 위한 ‘기관고유사업’ 예산을 부여함
○ 추진기간 : 2012년 ~ 진행 중
○ 총사업비 : 477백만원(2021년)
○ 주요내용
① 글로벌 사이버보안 신기술 연구개발
- AI 역기능 대응 기술 연구 및 신뢰가능한 인공지능 개발
- 블록체인 등 4차 산업혁명 기반기술 성능 및 보안관점의 안정성 평가 기술 연구
- 시스템 소프트웨어 취약점 탐지 및 대응 기술 연구
- 인터넷 기반 사이버위협·사이버범죄 탐지 및 대응 기술 연구
② 정보보호/사이버보안 고급인재 양성 및 교육훈련
- 정보보호대학원 석·박사과정 프로그램 운영
- CyberSecurity@KAIST 기술설명회, 정보보호대학원 봄·가을학기 정기 세미나 개최
- 국가 주요 기관 정보보호 기술자문(과학기술정보통신부, 대검찰청, 사이버사령부, 한국도로공사 등)
○ 추진경과
- 2010.12. ~ 2012.12. : 정부출연 R&D 과제 (지식경제부)
- 2012.01. ~ : 정부출연 기관고유사업 (과학기술정보통신부)
- 2010.12. ~ : 외부위탁 R&D 과제 및 기술이전 (공공, 민간)
※ 정부 위탁과제(최근 1년)
<table>
<tr><th>부처/위탁기관</th><th>사업명</th><th>과제명</th><th>사업기간</th><th>연구비
(백만원)</th></tr>
<tr><td>과학기술정보통신부 /
정보통신기획평가원</td><td>정보통신방송연구
개발사업</td><td>기계학습 모델 보안 역기능 취약점 자동
탐지 및 방어 기술 개발</td><td>2020.04.01. ~
2020.12.31.</td><td>350</td></tr>
<tr><td>과학기술정보통신부 /
정보통신기획평가원</td><td>정보통신방송연구
개발사업</td><td>블록체인 에뮬레이션을 위한 모듈형
라이브러리 및 엔진 기술 개발</td><td>2020.04.01. ~
2020.12.31.</td><td>600</td></tr>
<tr><td>과학기술정보통신부 /
정보통신기획평가원</td><td>정보통신방송연구
개발사업</td><td>블록체인 플랫폼 보안취약점 자동분석 기술 개발</td><td>2020.03.01. ~
2020.12.31.</td><td>83</td></tr>
<tr><td>과학기술정보통신부 /
국가보안기술연구소</td><td>위탁연구사업</td><td>악성코드 통신 메시지 형식 추론기술 연구</td><td>2020.04.01. ~
2020.10.31.</td><td>60</td></tr>
<tr><td>과학기술정보통신부 /
국가보안기술연구소</td><td>위탁연구사업</td><td>소스코드 추적성 확보를 위한 오브젝트
코드 검증 기술 연구</td><td>2020.04.01. ~
2020.10.31.</td><td>40</td></tr>
</table>
</td></tr>
</table>

사업수행자 (관련자 및 업무분담 내용)	○ 사업 관련자 (2021년 2월 기준)

구분	성명	직급	수행기간	담당업무 (업무분담 내용)
센터장	차상길	교수	'20.03 ~	센터 총괄, 기관고유사업 PM, 전산학부/정보보호대학원 겸직
연구1실장	류찬호	학연전문연 구원	'15.01 ~	기관고유사업 R&D, 과기부 연구과제 PM
연구2실장	조호묵	학연전문연 구원	'14.04 ~	기관고유사업 R&D, 과기부 연구과제 PM
연구1실	김용곤	학연전문연 구원	'16.08 ~	기관고유사업 R&D, 과기부 연구과제 PM
연구2실	정승일	학연전문연 구원	'13.01 ~	기관고유사업/과기부 연구과제 R&D
연구1실	김우승	위촉연구원	'16.06 ~	기관고유사업/과기부 연구과제 R&D
연구1실	고기혁	위촉연구원	'19.06 ~	과기부 연구과제 R&D
연구1실	김현진	위촉연구원	'20.03 ~	과기부 연구과제 R&D
연구1실	김홍준	위촉연구원	'20.05 ~	과기부 연구과제 R&D
연구1실	전효진	위촉연구원	'20.05 ~	과기부 연구과제 R&D
연구1실	임규민	위촉연구원	'20.07 ~	기관고유사업/과기부 연구과제 R&D
연구2실	이정호	선임급위촉 연구원	'17.07 ~	기관고유사업/과기부 연구과제 R&D
연구2실	이경석	위촉연구원	'16.02 ~	기관고유사업/과기부 연구과제 R&D
연구2실	신강식	위촉연구원	'20.05 ~	기관고유사업/과기부 연구과제 R&D
연구2실	안영진	위촉연구원	'20.05 ~	기관고유사업/과기부 연구과제 R&D
연구2실	최민지	위촉연구원	'20.05 ~	과기부 연구과제 R&D
연구2실	정동재	선임급위촉 연구원	'20.08 ~	기관고유사업 R&D
기획조정실	김지영	위촉행정원	'16.05 ~	연구관리·행정지원
기획조정실	강선정	위촉행정원	'16.12 ~	연구관리·행정지원
정보보호대학원	박찬수	학연행정원	'10.08 ~	석·박사과정 지원
정보보호대학원	이지선	학연행정원	'12.04 ~	석·박사과정 지원

다른기관 또는 민간인 관련자	○ 공동연구 수행 - 고려대학교, 과학기술정보통신부, 한국인터넷진흥원, 국가보안기술연구소 1) 블록체인 플랫폼 보안취약점 자동분석 기술 개발('19.6~, 총 4년, 24억) 2) 블록체인 에뮬레이션을 위한 모듈형 라이브러리 및 엔진 기술 개발('20.4~, 총 2년, 12억) 3) 기계학습 모델 보안 역기능 취약점 자동 탐지 및 방어 기술 개발('20.4~, 총 8년, 46억) 4) 악성코드 통신 메시지 형식 추론기술 연구('20.4~, 총 8개월, 0.6억) 5) 소스코드 추적성 확보를 위한 오브젝트 코드 검증 기술 연구('20.4~, 총 8개월, 0.4억) 6) 지역전략산업 융합보안 핵심인재 양성사업('19.9~, 총 4년+2년, 26억+14억)

○ 외부위탁 R&D 과제 수행

- ㈜에이펙스이에스씨, ㈜시큐레이어, ㈜지피다

1) 인공지능시스템의 안전성을 위한 프로그램 검증 방법론 연구('19.8 ~ '21.4, 0.2억, ㈜시큐레이어)
2) 사이버전 공격 모의훈련 시스템 연구 개발('20.7 ~ '21.12, 0.9억, ㈜APEX ESC)
3) 사이버 CTF 교육 플랫폼 연구('21.1 ~ '21.12, 0.4억, ㈜지피다)
4) 차세대 악성코드 분석 기술 연구('20.6 ~'21.5, 0.12억, ㈜APEX ESC)

○ MOU 체결

- ㈜두두아이티, ㈜에스투더블유랩 ('20.9)
- ㈜노르마, 몬드리안에이㈜ ('21.2, '21.3)

추진실적

○ 2020년 주요성과

정량적	정성적
• 논문게재 36건(SCI 9건) • 특허 33건(출원 19건, 등록 14건) • 저작권등록 4건(프로그램) • 기술이전 1건(기술료 1,430만원) • 고용창출 10명(연구인력) • 인력양성 26명(석사 17명, 박사 9명) • 국내외 정보보안 관련 주요대회 수상 11건 • 공공성 위탁과제 수행 7건(총 1,235백만원) • 언론보도 28건 • Security@KAIST 기술세미나 개최(1회) • 정보보호대학원 2020년 봄·가을학기 세미나 17회 개최	• 산·학 협력체계 구축 - 두두아이티, s2wlab MOU 체결 • 대국민 사이버보안 인식 재고를 위한 보안뉴스와의 협력 체계 구축 • 체세대 보안 R&D리포트(15건) • 공공보안 인식 재고 및 센터 연구 저변확대를 위한 소통 체계 구축 • 센터 R&D 웹블로그, 트위터, 페이스북 • 공공목적의 사이버보안 강화를 위한 교육 플랫폼 개발 • 국가기관 정보보안 기술자문(과기정통부, 사이버사령부, 대검찰청 등 8개 기관, 연 30여회)

○ 주요 연구 내용

① AI 역기능 대응기술 연구 및 신뢰가능한 인공지능 개발

- 설명가능한 인공지능을 활용한 인공지능의 안전성 및 신뢰성 평가 기술 연구
  · AI에 사용되는 딥러닝 모델 및 학습 알고리즘에 대한 용도에 따른 분류, PyTorch 및 Tensorflow를 사용한 구현
  · 기존에 알려진 다양한 딥러닝 모델 학습을 위한 dataset 확보 및 용도에 맞는 딥러닝 모델의 트레이닝 환경 구성
  · 현존하는 설명가능한 인공지능 기술들에 대한 조사 및 이를 적용한 AI의 의사결정 과정에 대한 설명기술 분류
- 프라이버시를 위한 인공지능에서의 정보흐름 및 사용 추적 및 제어 기술 개발
  · AI에 사용되는 학습 알고리즘 및 기존 프라이버시 위협에 대한 분류, 체계화
  · 일반적인 인공지능시스템에서의 정보흐름 및 사용에 따른 새로운 프라이버시 위험 정의 및 분석 방법 개발
- 인공지능시스템의 안전성을 위한 프로그램 검증 방법론 연구개발

② 블록체인 등 4차 산업혁명 기반기술 성능 및 보안관점의 안정성 평가 기술 연구

- 블록체인 핵심 기능/모듈에 대한 라이브러리 기술 연구
- 블록체인 평가 환경 구축을 위한 블록체인 에뮬레이션 기술 연구

	・ 블록체인을 평가하기 위한 바이너리 호환 에뮬레이션 기술에 대한 조사 및 분류 ・ 블록체인 에뮬레이션 기술 확장성 개선 기술 개발 **③ 시스템 소프트웨어 취약점 탐지 및 대응 기술 연구** - 바이너리 분석 플랫폼 최적화 및 기능 고도화 ・ 바이너리 분석 도구의 속도 및 성능 향상을 위한 인텔 파서 구조 개선 ・ 중간언어 리프팅 구조를 개선하여 속도 및 성능 향상 - 블록체인 바이트코드 중간언어 변환 도구 개발 ・ EVM(Etherium Virtual Machine) 바이트 코드 중간언어 변환 도구 구현 ・ 가상의 스택포인터 구조를 적용하여 스택기반 머신의 바이트코드를 중간언어로 변환 - 소스코드와 바이너리 추적성 비교 분석 도구 개발 ・ 소스코드의 CFG(Control Flow Graph)와 바이너리 코드의 CFG 비교 분석 도구 개발 ・ 컴파일 과정 등에서 발생할 수 있는 CFG 차이점 발견하여 추적성 검증 - 악성코드 통신 메시지 형식 추론 연구 ・ 악성코드 통신 메시지 분석 및 메시지 추론 기술 연구 ・ 추론 기반의 악성코드 통신 메시지 형식 분석 및 추론 기술 연구 ・ 악성코드 통신 메시지 형식 분석 및 추론 도구 개발 - 신규 악성코드 추적 및 탐지 기술 연구 ・ 대량의 악성코드 분석을 위한 정적 및 동적 자동화 분석체계 구축 ・ 평판 분석 및 유사도 분석을 통한 악성코드 자동화 분류 ・ 신규 악성코드 탐지를 위한 학습 빅데이터 구축 **④ 인터넷 기반 사이버위협・사이버범죄 탐지 및 대응 기술 연구** - 웹 위협 분석 및 탐지를 위한 능동형 범용 웹 크롤러 도구 개발 ・ RPA 기반의 능동형 웹 크롤러 도구 개발 ・ 다양한 웹 환경을 수용하기 위한 프레임워크 기반의 범용 웹 크롤러 개발 - 사이버범죄 탐지를 위한 도메인 추적 및 분류 기술 연구 ・ Feature Extraction 및 서치 엔진 기반 도메인 추적 도구 개발 ・ PageRank 및 LCS 기반의 도메인 유사도 판단 도구 개발 **○ 정보보호/사이버보안 고급 인재 양성 및 교육 훈련** - 정보보호대학원 인재양성 . 2020년 입학생 총 25명(석사 20명, 박사 5명) . 2020년 졸업생 총 26명(석사 17명, 박사 9명) - 정보보호대학원 2020년 봄・가을학기 세미나 총 16회 개최 - Security@KAIST 콘소시움 운영(16개 민간기업 및 지자체), Security@KAIST 온라인 기술설명회 개최(총 124여명 등록)