10 글로벌사이버보안기술연구센터 운영

<table>
<tr><td>사업실명제
등록번호</td><td>2022-10</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 : 10,577백만원 (2012년~2022년)
○ 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
- IoT 디바이스 취약점 탐지 및 안정성 검증 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 수탁과제 (최근 1년)
<table>
<tr><th>부처/전문기관</th><th>사업명</th><th>과제명</th><th>연구기간</th><th>정부출연금
(백만원)</th></tr>
<tr><td>과기정통부 /
정보통신기획평가원</td><td>정보통신방송
연구개발사업</td><td>블록체인 에뮬레이션을 위한 모듈형 라이브러리 및 엔진 기술 개발</td><td>2021.01.01. ~
2021.12.31.</td><td>600</td></tr>
<tr><td rowspan="2">과기정통부 /
정보통신기획평가원</td><td rowspan="2">정보통신방송
연구개발사업</td><td rowspan="2">블록체인 플랫폼 보안취약점 자동분석 기술 개발</td><td>2021.01.01. ~
2021.12.31.</td><td>100</td></tr>
<tr><td>2022.01.01. ~
2022.12.31.</td><td>100</td></tr>
</table>
</td></tr>
</table>

부처/전문기관	사업명	과제명	연구기간	정부출연금 (백만원)
과기정통부 / 정보통신기획평가원	정보통신방송 연구개발사업	스마트 컨트랙트의 개발-배포-실행의 전주기적 취약점 및 신뢰성 오류 개선 기술개발	2021.04.01. ~ 2021.12.31.	350
			2022.01.01. ~ 2022.12.31.	350
과기정통부 / 정보통신기획평가원	정보통신방송 연구개발사업	기계학습 모델 보안 역기능 취약점 자동 탐지 및 방어 기술 개발	2021.01.01. ~ 2021.12.31.	583
			2022.01.01. ~ 2022.12.31.	583
산업통상자원부 / 민군협력진흥원	민군겸용연구 사업	리눅스 시스템 오류 분석과 해킹 위험도 검증을 위한 자동화 시스템 개발	2021.08.01. ~ 2021.12.31.	276
			2022.01.01. ~ 2022.12.31.	118
기획재정부 / 국가보안기술연구소	위탁연구사업	악성코드 암/복호화 함수 식별 기술 연구	2021.04.01. ~ 2021.10.31.	60

사업수행자 (관련자 및 업무분담 내용)

○ 사업 관련자 (2022년 3월 기준)

구분	성명	직급	수행기간	담당업무 (업무분담 내용)
센터장	차상길	교수	'20.03 ~	센터 총괄, 기관고유사업 PM, 전산학부/정보보호대학원 겸직
연구1실장	류찬호	학연전문연구원	'15.01 ~	기관고유사업 R&D, 과기부 연구과제 PM
연구2실장	조호묵	학연전문연구원	'14.04 ~	기관고유사업 R&D, 과기부 연구과제 PM
연구1실	정승일	학연전문연구원	'13.01 ~	기관고유사업/과기부 연구과제 R&D
연구1실	고기혁	위촉연구원	'19.06 ~	기관고유사업/과기부 연구과제 R&D
연구1실	안영진	위촉연구원	'20.05 ~	기관고유사업/과기부 연구과제 R&D
연구1실	지수근	위촉연구원	'21.09 ~	기관고유사업/과기부 연구과제 R&D
연구1실	최재승	선임급위촉연구원	'22.03 ~	기관고유사업/과기부 연구과제 R&D
연구1실	양희동	위촉연구원	'22.03 ~	기관고유사업/과기부 연구과제 R&D
연구2실	이정호	선임급위촉연구원	'17.07 ~	기관고유사업/과기부 연구과제 R&D
연구2실	이경석	위촉연구원	'16.02 ~	기관고유사업/과기부 연구과제 R&D
연구2실	신강식	학연전문연구원	'20.05 ~	기관고유사업/과기부 연구과제 R&D
연구2실	최민지	위촉연구원	'20.05 ~	기관고유사업/과기부 연구과제 R&D
연구2실	임규민	위촉연구원	'20.07 ~	기관고유사업/과기부 연구과제 R&D
연구2실	정동재	선임급위촉연구원	'20.08 ~	기관고유사업/과기부 연구과제 R&D
연구2실	손승호	위촉연구원	'22.03 ~	기관고유사업/과기부 연구과제 R&D
기획조정실	김지영	위촉행정원	'16.05 ~	연구관리·행정지원
기획조정실	강선정	위촉행정원	'16.12 ~	연구관리·행정지원

다른기관 또는 민간인 관련자

○ 정부 수탁과제 공동연구 수행 (최근 1년)

- 고려대학교 산학협력단, ㈜메콘, 단국대학교 산학협력단, ㈜수호아이오,

	㈜스패로우, ㈜파이랩테크놀로지, ㈜에이펙스이에스씨, 한국인터넷진흥원, 성균관대학교 산학협력단, 국립강원대학교 산학협력단, 부산대학교 산학협력단, 충남대학교 산학협력단 전남대학교 산학협력단, 순천향대학교 산학협력단 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) 라눅스 시스템 오류 분석과 해킹 위험도 검증을 위한 자동화 시스템 개발('21.8~, 총 3년, 35억) 5) 스마트 컨트랙트의 개발-배포-실행의 전주기적 취약점 및 신뢰성 오류 개선 기술개발 ('21.4~, 총 5년, 92억) 6) 악성코드 암/복호화 함수 식별 기술 연구('21.4~, 6개월, 0.6억) 7) 융합보안 핵심인재 양성사업('19.9~, 총 7년, 468억) **○ 민간 산학협력 과제 수행(최근 1년)** - ㈜에이펙스 이에스씨, ㈜시큐레이어, ㈜지피다, ㈜노르마, ㈜파이랩테크놀로지, ㈜아이오티큐브 1) 인공지능시스템의 안전성을 위한 프로그램 검증 방법론 연구('19.8 ~ '21.12, 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 ~ '22.12, 0.4억, ㈜지피다) 4) 차세대 악성코드 분석 기술 연구('20.6 ~'21.5, 0.12억, ㈜APEX ESC) 5) 블루투스 퍼징 테스트 도구 평가('21.10~'21.11, 0.12억, ㈜노르마) 6) 멀티체인 기반 블록체인 상호운용성 모듈의 안전성 검증 기술 개발 ('21.10~'22.12, 0.8억, ㈜파이랩테크놀로지) 7) 오픈소스 취약점 분석 도구 평가('21.10~'22.6, 0.33억, ㈜아이오티큐브) 8) 인공지능 기반 실시간 위협탐지 시스템에 대한 성능 및 기능 검증 기술 연구('21.6~'21.12, 0.2억, ㈜APEX ESC) **○ MOU 체결(최근 1년)** - ㈜노르마 ('21.2)
추진실적	**○ 2021년 주요성과** **정량적** • 논문게재 43건(SCI 4건) • 특허 30건(출원 25건, 등록 5건) • 저작권등록 13건(프로그램) • 기술이전 2건(기술료 2,200만원) • 고용창출 1명(연구인력) • 인력양성 22명(석사 17명, 박사 5명) • 국내외 정보보안 관련 주요대회 수상 13건 • 공공성 위탁과제 수행 12건(총 22억) • 언론보도 21건 • 산·학 협력체계 구축 - 법무법인(유) 화우 MOU 체결 - ㈜노르마 MOU 체결 • Security@KAIST 기술세미나 등 개최(3회) • 정보보호대학원 2021년 봄·가을학기 세미나 16회 개최(국내외 정보보안 전문가 초청) • 2021 시큐리티 어워즈 코리아 (공공부문 대상) **정성적** • 대국민 사이버보안 인식 재고를 위한 보안뉴스와의 협력체계 구축 - 체세대 보안 R&D리포트(12건) • 공공보안 인식 재고 및 센터 연구 저변확대를 위한 소통 체계 구축 - 센터 R&D 웹블로그, 트위터, 페이스북 • 공공목적의 사이버보안 강화를 위한 교육 플랫폼·교과목 개발 • 국가기관 정보보안 기술자문(과기정통부, 사이버사령부, 대검찰청 등 8개 기관, 연 30여회) • 정보보호대학원 웹블로그, 트위터, 페이스북, 인스타그램 개설에 따른 홍보 및 소통 체계 구축

○ 2021년 주요 연구 내용

① AI 역기능 대응기술 연구 및 신뢰가능한 인공지능 개발

- 설명가능한 인공지능을 활용한 인공지능의 안전성 및 신뢰성 평가 기술 연구
  - 딥러닝 모델에서 개별 입력에 대한 설명기술 개발 및 이를 포함한 소프트웨어 라이브러리 구현
  - 설명가능 인공지능을 활용한 Evasion attack 방어(적대적 예시 탐지) 기법 개발
- 프라이버시를 위한 인공지능에서의 정보흐름 및 사용 추적 및 제어 기술 개발
  - 인공지능 어플리케이션에서 사용될 수 있는 다양한 개인정보에 대해 각 개인정보의 형태 및 특성에 따른 분류 및 민감 정보 지정
  - 각 인공지능 어플리케이션과 데이터 형태에 맞는 인공지능 모델 학습

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

- 블록체인 핵심 기능/모듈에 대한 라이브러리 기술 연구
  - 가십 프로토콜은 네트워크 내에서 메시지를 전파하기 위해 사용되며 연결된 모든 블록체인 노드에게 메시지를 전송하도록 설계
  - 가쉽 프로토콜과 노드 디스커버리를 이용한 P2P 네트워킹 데스트 수행 및 확인
- 블록체인 평가 환경 구축을 위한 블록체인 에뮬레이션 기술 연구
  - 블록체인을 평가하고 개발 및 분석 하기 위한 인터페이스 설계 및 개발

③ IoT 디바이스 취약점 탐지 및 안정성 검증 기술 연구

- 정적 분석 기반 펌웨어 취약점 분석 시스템
  - IoT 취약점 DB 구축을 위한 펌웨어, 취약점 등 수집 IoT 전용 크롤러 연구
  - 정적 및 동적 분석을 통한 IoT 취약점 탐지 및 분석 기술 연구

④ 시스템 소프트웨어 취약점 탐지 및 대응 기술 연구

- 바이너리 분석 플랫폼 아키텍처 확장
  - 신규 지원 아키텍처 추가: AVR(Alf and Vegard's RISC), PPC32(PowerPC) 등
- 바이너리 분석 플랫폼 최적화 및 기능 고도화
- 블록체인 바이트코드 중간언어 변환 도구 개발
- 악성코드 암/복호화 함수 식별기술 연구
  - 악성코드의 암/복호화 함수 자동 식별 방법 연구 및 검증

⑤ 인터넷 기반 사이버위협·사이버범죄 탐지 및 대응 기술 연구

- 웹 위협 분석 및 탐지를 위한 능동형 범용 웹 크롤러 도구 개발
  - 다양한 웹 환경에 대응하기 위한 DGA 기반의 능동형 웹 크롤러 개발
- 사이버범죄 탐지를 위한 도메인 추적 및 분류 기술 연구
  - Reculsive Feature Extraction 기반의 사이버범죄 탐지 주요 키워드 탐색 기술 개발
  - 사이버범죄 도메인 탐지 및 분류를 위한 멀티 스텝 기술 기반의 딥러닝 분류 도구 개발

○ 2021년 정보보호/사이버보안 고급 인재 양성 및 교육 훈련

- 정보보호대학원 인재 양성
  . 2021년 입학생/ 졸업생 총 26명(석사 21명, 박사 5명)/총 22명(석사 17명, 박사 5명)
- 정보보호대학원 2021년 봄·가을학기 세미나 총 16회 개최
- Security@KAIST 콘소시움 운영(16개 민간기업 및 지자체), Security@KAIST 온라인 기술설명회 개최(총 200여명 등록)