2019년 대표성과

[1] 기본 정보

<table>
<tr><td>후보추천 Track</td><td colspan="4">미래선도 ( ), 산업육성 ( ), 국가·사회문제해결 (O)</td></tr>
<tr><td>협약과제명 (협약과제번호)</td><td colspan="4">맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발 (19HH3700)</td></tr>
<tr><td>총연구기간</td><td colspan="4">2016년 4월 ~ 2019년 12월</td></tr>
<tr><td>총연구비</td><td colspan="2">총 22,733 백만원</td><td colspan="2">정부: 16,900 백만원
민간: 5,833 백만원</td></tr>
<tr><td rowspan="2">성과책임자 정보</td><td>연구자 성명</td><td>직할부서</td><td>연구본부/연구실</td><td>직위/직급</td></tr>
<tr><td>김종현</td><td>지능화융합연구소</td><td>정보보호연구본부/
네트워크시스템보안연구실</td><td>기술총괄/책임</td></tr>
<tr><td>연구사업계획서 관련 성과목표명</td><td colspan="4">[성과목표5-5] 정교화자동화 해킹을 원천차단하는 지능형 사이버보안 핵심기술</td></tr>
</table>

[2] 2019년 우수성과 내용

1. 성과명

지능형 사이버 위협 대응을 위한 맞춤형 보안 기술

2. 성과내용

기술개발 목표달성도

□ 기술적 선점이 필요한 분야

○ IoT 디바이스에서부터 클라우드 서비스까지 전주기 보안서비스를 제공하기 위한 맞춤형 보안 서비스(기업해킹), IoT 보안 강화(시설・인명위협), 사이버위협 사전예방(지능화된 위협) 분야

□ 기술개발 목표

○ **초연결 인프라 위협을 대비한 지능형 보안 핵심 기술**

(목표 ①) 기업・사용자가 골라 담는 주문형 맞춤 보안(Security-on-Demand) 기술

(목표 ②) IoT 사물봇 공격 확산 방지용 보안 자율제어 및 대응(iGLORY) 기술

<기술개발 개념도>

□ 기술개발 목표의 달성성과 및 핵심기술 확보

[개발목표 ①] 주문형 맞춤 보안(Security-on-Demand) 기술

➡ **(달성성과)** 정교화·자동화되는 해킹으로부터 주요 ICT 인프라 보호를 위한 보안 기능을 동적으로 재구성하고 지능적으로 분석/대응할 수 있는 **클라우드 기반 지능형 보안 서비스 핵심 기술 개발**

➡ **(핵심기술 확보)**

- SDsec 콘트롤러 및 클라우드 기반 지능형 보안 위협 분석 기술
- 고성능 서버 스위치 기반 보안 클라우드 가상화 플랫폼 기술
- 중소기업 대상 클라우드 기반 맞춤형 보안 SECaaS 서비스 플랫폼 기술
- 지능형 SIEM 사업화를 위한 AI 기술 외부 검증

[개발목표 ②] IoT 보안 자율대응(iGLORY) 및 스마트 IoT 보안서비스 기술

➡ **(달성성과)** 글로벌 표준기반 사물봇 공격 확산방지용 보안 자율제어·대응 기술(iGLORY) 개발 및 스마트 IoT 보안 서비스 적용

➡ **(핵심기술 확보)**

- 사물봇 공격 확산 방지를 위한 스마트 세그멘테이션(SSS) 기술
- 대규모 DDoS 방어를 위한 신뢰 연결관리 기반 동적경계망(DPS) 기술
- 사물봇 악성코드 방지를 위한 IoT 기기 플랫폼 원격무결성 검증(RAS) 기술
- 스마트홈 IoT 보안 서비스 인프라 구축 및 C-ITS 보안 인프라 (판교 Living Lab 시범) 테스트베드 실증을 위한 기술 검증

3. 우수성 및 차별성

기술수준 향상 성과

○ 중소기업 보안사각지대 해소를 위한 **클라우드 기반 맞춤형 보안 시범서비스 출범 (2017.11~현재, Security On-AIR Center)** 및 시범서비스 확장을 통한 마이크로 클라우드 센터 기반 SECaaS 서비스 사업화 모델 검증 **(정보보호핵심원천기술개발 우수성과과제 선정, IITP, '19.10)**

○ 클라우드 기반 보안 서비스 오케스트레이터 기능 고도화를 통한 SDsec 콘트롤러 및 100G급 고성능 서버 스위치 기반 보안 클라우드 가상화 플랫폼 상용시스템 개발

. 가상화 기반 보안 솔루션 고성능 가상 IPS(Sniper vIPS), vFW, vDDoS 제품((주)윈스) 출시(' 17.11~),
. 가상화 기반 악성코드 탐지 대응 서비스((주)하우리) 출시 (' 18.11~)
. 100G급 보안성 강화형 서버-스위치 시스템 상용화((주)아토리서치) 출시 (' 18.11~)
. 클라우드 기반 맞춤형 Security Operation Center((주)SK인포섹) 출시 (' 18.11~)
. AI-SIEM 기술의 공동연구기관 KT SIEM+ 사업화 추진 (' 18.03~)

○ 사물봇 해킹에도 안심,『지능형 원격검침 인프라 보호를 위한 경량형 IoT 보안 기술』기술로 **공개키 인증(PKI)를 적용해 보안을 대폭 강화한 제품을 유럽 해외에 최초 적용하고** 국내 한전 및 아시아, 중동 등에서 AMI 시장을 확장하는 동시에 **에너지 IoT 사업 확대 예정 (국가연구개발 100선 기술로 선정, KISTEP, '19.9.)**

○ 글로벌 표준 기반 사물봇 빠른 확산 방지, 비인가 접속 방어용 보안 자율제어 플랫폼 개발 및 스마트 IoT 보안 서비스 적용

○ 대규모(80대이상) 기기 IoT인프라 환경에 최적화된 계층적 위협 전파방지 기술 및 IoT 보안 GW 시제품 개발

○ **글로벌 표준(CSA SDP Ver. 1.0 표준 만족) 기반 IoT 인프라 DDoS 방어용 소프트웨어 정의 경계망(SDP) 핵심 원천기술 개발**

기술수준 공인 성과

○ 세계적 수준 악성코드 탐지율의 딥러닝 기반 바이러스 백신 엔진 기술 확보 (신종 악성코드 탐지율: 99.6%, 오탐율: 1.27%) 및 **수요처(국방부) 요구에 의한** R&D 후속과제 **국방 백신 고도화를 위한 AI백신 체계 구축 사업 수행**(2019.04~)

○ ISP 보안관제 센터에서 실수집된 데이터를 통해 기술 검증 PoC 수행 및 AI-SIEM 엔진이 포함된 **㈜KT SIEM+ 사업화를 위한 TTA 공인기술 시험인증서 획득**

○ 국제표준 규격(IETF PANA, EAP-TLS 등)을 준수한 IoT 보안 인프라 구현 및 **유럽 현지 대규모 기기 검증 완료 (유럽 노르웨이 전역 약85만호, 1,200억매출, ~ '19.1)**

○ 세계 최초 IoT인프라 환경에 최적화된 계층적 위협 전파방지 기술 및 글로벌 표

준 기반 IoT 인프라용 DDoS 방어 기술 확보 (CSA SDP Ver. 1.0, IETF 표준 HOTP, TLS 등, 동시 신뢰연결 처리 세션수 1,000개) 및 국토부(도로공사) 본 사업을 위한 **판교 C-ITS Living Lab 테스트베드 시험 검증 준비('19.11.~)**

○ 상용 암호 대비 고성능 암호 구현(ARM mbed 대비 서명생성 3.6배, 서명검증 4.2배)과 공공 기관 적용시에 필요한 KCMVP 인증에 준하는 국정원 테스트 벡터 기반의 시험 완료로 업체의 KCMVP 인증 과정 간소화 및 경쟁력 강화 기여

4. 성과의 활용도 및 파급효과

경제 활성화 효과

기업 경쟁력 향상

○ **㈜윈스의 차세대 보안 대피소 서비스(iBunker)**에 맞춤형 보안 서비스 제공(2019.09.~) 및 빅데이터/AI기반 침해 위협 분석을 위한 **AI-SIEM 엔진을 ㈜KT 과천 통합보안관제센터 적용 ('19.12.~)**

○ 소규모 네트워크를 위한 보안 관제 및 small 플랫폼형의 AI 보안관제 구축을 위한 ISP 사업화에 적용 예정이며, 인공지능 기반 침해 위협 탐지 솔루션 개발 분야에 활용 가능

○ IoT 서비스를 위한 경량형 보안 기술 국산화를 통한 외산 종속성 감소로 수입대체 효과에 의한 로얄티를 절감하고, 국내기업 기술 경쟁력 확보를 통한 신규 IoT 보안 서비스 시장 선점 가능

- **로열티/라이센싱 수익(ETRI) : 1,200억 매출, 2019년 12월 1.84억 로열티 수입**

○ IoT 서비스 산업 활성화의 걸림돌인 사물봇 보안 위협의 조기 해소 및 이종망과 이종 서비스 간 연동 지점의 보안 기능 제공으로 새로운 서비스 모델 창출 기여가 기대됨

산업 경쟁력 향상

○ 중소기업 보안 사각지대 해소를 위하여, ETRI 융합기술연구생산센터 ㈜유민테크 외 9개 기업 및 외부(원격지원) ㈜소만사 외 5개 기업 대상으로 **클라우드 기반 맞춤형 보안 시범서비스 출범(2017.11~)**

○ 사물봇 해킹에도 안심하는 경량형 IoT 보안 기술로 **2019년 국가연구개발 100선 선정**됨으로써 국내 IoT 보안 산업 및 서비스 활성화에 기여

○ 사물봇 공격/자동 전파 등 빠른 확산 방지, 대규모 서비스 거부 공격 방어, 사물봇 악성코드 방지 핵심 기술 개발로 국내 기업의 기술 경쟁력을 확보하고 관련 장비의 국내·외 시장 진출에 기여

경제적 파급효과

○ **(파급효과 전망)** 다양하게 진화하는 사이버 위협에 유연하게 대응할 수 있는 SW 기반 보안 서비스 기술을 통해, HW 솔루션 위주인 국내의 후진적 보안 시장 구조 탈피를 위한 글로벌 성장 모멘텀으로 활용 가능

○ 지능형 SIEM을 위한 인공신경망 기반 데이터 분석 및 탐지 기술 등 6건의 기술이전과 멕시코, 한국 등 국내외에서 네트워크 포렌식 기반 위협탐지 및 이벤트 관리 시스템 납품을 이용한 **17건의 사업화 실적으로 722백만원 매출 발생**

○ IoT 보안 핵심원천 기술을 통한 다양한 IoT 서비스에 대한 신시장 개척을 도모 및 이로 인한 인력고용 확대 기여('22년까지 14조4000억달러 가치 창출, CISCO)

○ **해외 사업화(노르웨이 85만호, 약 1,200억 규모) 성공 사례**를 통해, 해외 IoT 보안 솔루션 시장을 선점하였고 관련 장비의 세계시장 진출 및 수출효과 증가에 기여

국가·사회적 파급효과

○ **해결해야 할 국가·사회문제**

- 사이버 공격 진화와 정보보호 투자 미흡 등으로 발생한 중소기업 보안 사각 지대 해소 및 사이버 테러 예방을 통한 국가 안보 향상
- ICT 환경 변화에 따른 신규 보안 위협 대응 기술 등 핵심 원천 정보보호 기술 개발을 통한 안전한 국가 사이버 환경 조성
- 복잡하고 다양한 IoT 서비스 환경에서 보안사고 발생 시 유발될 대규모 피해의 사전 대비를 통한 국가 주요 산업 및 국내 기업 보호와 경쟁력 강화 필요
  · 보안사고로 인한 제품 수요 10% 감소 및 산업 1% 장애를 가정할 경우, 스마트단말 16조, 스마트카 24조, 금융산업 1조 7천억 등의 피해 예상(산업연구원)

○ **성과에서 개발된 기술적 솔루션**

- 보안 기능을 동적으로 재구성하고 지능적으로 분석/대응할 수 있는 클라우드 기반 지능형 보안 위협 분석 시스템 상용 시제품
- 클라우드 기반 보안 서비스 오케스트레이터 기능 고도화를 통한 SDsec 콘트롤러 상용 시제품
- 100G급 고성능 서버 스위치 기반 보안 클라우드 가상화 플랫폼 상용시스템
- 글로벌 표준 기반 사물봇 빠른 확산 방지, 비인가 접속 방어용 보안 자율제어 플랫폼 및 보안 GW 상용시제품
- 사물봇 공격 확산 방지를 위한 스마트 세그멘테이션(SSS) 기술 및 솔루션
- 대규모 DDoS 방어를 위한 신뢰 연결관리 기반 동적경계망(DPS) 기술 및 솔루션
- 사물봇 악성코드 방지를 위한 IoT 기기 플랫폼 원격무결성 검증(RAS) 기술 및 솔루션

❍ **국가·사회적 파급효과**

- ICT가 우리 실생활 사물 및 주요 사회기반시설과 접목되어 기존 사이버공간의 보안 위험이 현실 세계로 전이(轉移)·확대되고 있는 상황에서 다양한 보안 위협에 동적으로 대응할 수 있는 지능형 맞춤 보안 서비스 제공
- 지능화・고도화되는 사이버 위협에 능동적으로 대응 가능한 SW 기반 보안 서비스 기술 개발을 통해, HW 솔루션 위주인 국내 보안 시장 구조 개선 효과
- IoT기반 보안 서비스 지원 일자리 창출을 통한 고용창출 효과와 지능형 원격검침 인프라에서 발생하는 사이버 보안 문제 해결 등 국민생활 개선에 기여