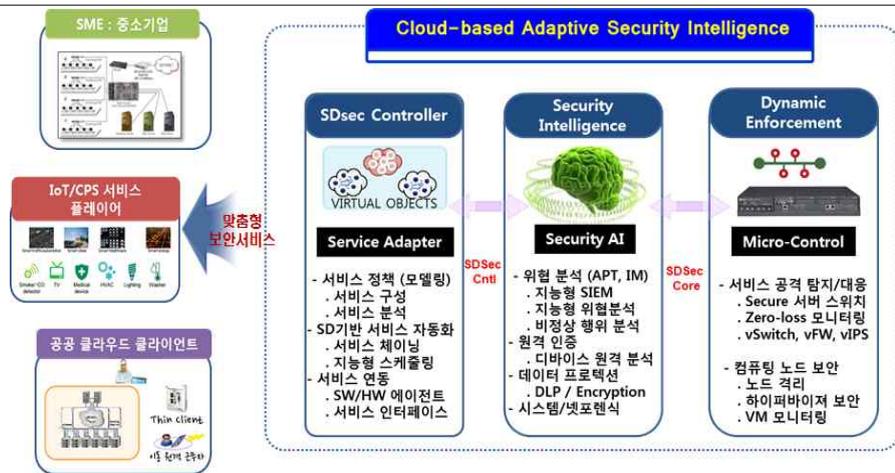


# 실명제 사업내역서

사업실명제 등록번호	2019 - 3	담당부서 작성자	(정보보호연구본부/지능보안연구그룹) (김종현/042-860-3843/jhk@etri.re.kr)
사업(정책)명	<b>맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발</b>		
사업개요 및 추진경과	<p>○ 추진배경</p> <ul style="list-style-type: none"> <li>- 기존의 개별시스템 형태의 보안 기능으로는 지능화된 사이버공격에 대한 방어가 어려움             <ul style="list-style-type: none"> <li>· 네트워크 경계가 붕괴됨에 따라 기존의 단일 시스템에서 수집되는 정보만으로는 복잡하고 정교한 공격(예, 내부자 위협 및 APT 공격) 방어가 어려움</li> </ul> </li> <li>- <b>(사이버 보안 사각지대 상존)</b> 기업의 자발적 정보보호 투자 미흡과 IoT 등 新 ICT서비스 및 영세·중소기업에 대한 보안인프라 부족 등 사이버 보안 사각지대 상존</li> <li>- <b>(필요성)</b> 해외의 경우 글로벌 기업을 중심으로 보안인텔리전스화 및 보안장비의 소프트웨어화(SDx) 기술 확보가 치열하나, 국내의 경우 제품/기능의 융합의 한계가 있어, 정부 주도의 기술개발이 필요함             <ul style="list-style-type: none"> <li>· 벤더간 보안제품의 호환성 확보, 신종 사이버 위협에 대한 빠른 대응, 주문형 보안 서비스를 위해서는 소프트웨어 기반 보안 기술이 필요</li> <li>· 보안 인텔리전스 기술을 탑재한 “지능형 통합 보안 클라우드 핵심 기술” 확보가 필요함</li> <li>· IDC CHESS (Cloud Hosted Enterprise Security Services) 구성 기술 중 보안상황 분석기술 분야는 타 기술 대비 가장 큰 잠재 시장 규모(2~7배)이나, 국내 기술 성숙도는 낮은 수준(선진국 대비 75%)으로 관련기술 확보가 시급</li> </ul> </li> </ul> <p>○ 추진기간 : 2016.04.01 ~ 2019.12.31. (계속)</p> <p>○ 총사업비 : 22,733백만원</p>		



〈클라우드 기반 지능형 보안 서비스 제공 개념도〉

○ 주요내용

- 보안 서비스의 확장성, 유연성, 관리용이성 및 보안의 효율성을 보장하는 SDsec 컨트롤러 기술
  - OpenStack 기반 시큐어 서비스 오케스트레이션 기술
  - 보안 서비스 체이닝을 위한 SDsec 컨트롤 기능
  - 보안 서비스·데이터 연동 프레임워크 기술
- 신규 ICT 환경에 맞는 다양한 보안기능을 제공하는 클라우드 기반 지능형 보안 위협 분석 기술
  - 입체적 분석을 통한 지능형 보안 위협분석 시스템 개발
  - 클라우드 백신 서비스를 위한 악성코드 분석 기술 개발
  - 보안위협 대응을 위한 가상 인프라 정보 수집/저장/검색
- 고성능 서버/스위치 기반 보안 클라우드 인프라 자체 보안 보장형 Dynamic Enforcement 기술
  - SDsec기반 보안 클라우드 가상화 플랫폼 개발
  - 시큐어서비스 위치, 인프라, NW/컴퓨팅노드 보안검증 기능
  - 네트워크 시큐리티 기능 가상화 기술

○ 추진경과

- 2015.08~2016.02: 과제기획전담팀구성 및 과제기획
- 2016.03: 과제 선정 (총수행기간: 45개월)
- 2016.04.01.~2016.12.31.: 1차년도 과제 수행
  - SoA(Security-on-Air) 테스트베드 구축 (8월)
  - 과제진도점검(10월) 및 과제평가(12월)
- 2017.01.01.~2017.12.31.: 2차년도 과제 수행
  - 클라우드 기반 맞춤형 보안 시범서비스 런칭 (11월)
  - 과제진도점검(10월) 및 과제평가(12월)
- 2018.01.01.~2018.12.31.: 3차년도 과제 수행
  - 클라우드기반 맞춤형 보안 시범서비스 확대 (10월, 16개사 대상)
  - 지능형 SIEM 사업화를 위한 AI 기술 외부 검증 (11월, (주)KT)
- 2019.01.01.~2019.12.31.: 4차년도 과제 수행 중

<p>사업수행자 (관련자 및 업무분담 내용)</p>	<p>○ 최초 입안자 및 최종 결재자</p> <ul style="list-style-type: none"> <li>- 최초 입안자 : 지능보안연구그룹장/책임급 김익균 지능보안연구그룹 PL/책임급 김종현</li> <li>- 최종 결재자 : 정보보호연구본부장/책임급 진승헌</li> </ul> <p>○ 사업 관련자</p> <table border="1" data-bbox="451 322 1342 1016"> <thead> <tr> <th>구분</th> <th>성명</th> <th>직급</th> <th>수행기간</th> <th>담당업무 (업무분담 내용)</th> </tr> </thead> <tbody> <tr> <td>본부장</td> <td>진승헌</td> <td>책임</td> <td>2016.04.01.~ 2019.12.31</td> <td>기술 대외 홍보 및 과제 기획</td> </tr> <tr> <td>그룹장</td> <td>김익균</td> <td>책임</td> <td>2016.04.01.~ 2019.12.31</td> <td>기술 사업화 및 과제 기획</td> </tr> <tr> <td>PL</td> <td>김종현</td> <td>책임</td> <td>2016.04.01.~ 2019.12.31</td> <td>과제 총괄 및 사업 관리</td> </tr> <tr> <td>담당</td> <td>김영수</td> <td>책임</td> <td>2016.04.01.~ 2019.12.31</td> <td>PT 기반 악성코드 분석</td> </tr> <tr> <td>담당</td> <td>이상민</td> <td>책임</td> <td>2016.04.01.~ 2019.12.31</td> <td>클라우드 인프라 매니저 개발</td> </tr> <tr> <td>담당</td> <td>박종근</td> <td>책임</td> <td>2016.04.01.~ 2019.12.31</td> <td>SDSec 컨트롤러 개발</td> </tr> <tr> <td>담당</td> <td>이종훈</td> <td>선임</td> <td>2016.04.01.~ 2019.12.31</td> <td>vSIEM/빅데이터플 랫폼 개발</td> </tr> <tr> <td>담당</td> <td>김현주</td> <td>선임</td> <td>2016.04.01.~ 2019.12.31</td> <td>네트워크 이상징후 분석/개발</td> </tr> <tr> <td>담당</td> <td>최선오</td> <td>선임</td> <td>2016.04.01.~ 2019.12.31</td> <td>DL기반 악성파일 탐지 개발</td> </tr> <tr> <td>담당</td> <td>김정태</td> <td>선임</td> <td>2016.04.01.~ 2019.12.31</td> <td>SoA 서비스 개발/구축</td> </tr> </tbody> </table>	구분	성명	직급	수행기간	담당업무 (업무분담 내용)	본부장	진승헌	책임	2016.04.01.~ 2019.12.31	기술 대외 홍보 및 과제 기획	그룹장	김익균	책임	2016.04.01.~ 2019.12.31	기술 사업화 및 과제 기획	PL	김종현	책임	2016.04.01.~ 2019.12.31	과제 총괄 및 사업 관리	담당	김영수	책임	2016.04.01.~ 2019.12.31	PT 기반 악성코드 분석	담당	이상민	책임	2016.04.01.~ 2019.12.31	클라우드 인프라 매니저 개발	담당	박종근	책임	2016.04.01.~ 2019.12.31	SDSec 컨트롤러 개발	담당	이종훈	선임	2016.04.01.~ 2019.12.31	vSIEM/빅데이터플 랫폼 개발	담당	김현주	선임	2016.04.01.~ 2019.12.31	네트워크 이상징후 분석/개발	담당	최선오	선임	2016.04.01.~ 2019.12.31	DL기반 악성파일 탐지 개발	담당	김정태	선임	2016.04.01.~ 2019.12.31	SoA 서비스 개발/구축
구분	성명	직급	수행기간	담당업무 (업무분담 내용)																																																				
본부장	진승헌	책임	2016.04.01.~ 2019.12.31	기술 대외 홍보 및 과제 기획																																																				
그룹장	김익균	책임	2016.04.01.~ 2019.12.31	기술 사업화 및 과제 기획																																																				
PL	김종현	책임	2016.04.01.~ 2019.12.31	과제 총괄 및 사업 관리																																																				
담당	김영수	책임	2016.04.01.~ 2019.12.31	PT 기반 악성코드 분석																																																				
담당	이상민	책임	2016.04.01.~ 2019.12.31	클라우드 인프라 매니저 개발																																																				
담당	박종근	책임	2016.04.01.~ 2019.12.31	SDSec 컨트롤러 개발																																																				
담당	이종훈	선임	2016.04.01.~ 2019.12.31	vSIEM/빅데이터플 랫폼 개발																																																				
담당	김현주	선임	2016.04.01.~ 2019.12.31	네트워크 이상징후 분석/개발																																																				
담당	최선오	선임	2016.04.01.~ 2019.12.31	DL기반 악성파일 탐지 개발																																																				
담당	김정태	선임	2016.04.01.~ 2019.12.31	SoA 서비스 개발/구축																																																				
<p>다른기관 또는 민간인 관련자</p>	<p>○ 11개 공동연구(참여)기관 책임자</p> <table border="1" data-bbox="416 1093 1342 1756"> <thead> <tr> <th>기관명</th> <th>성명</th> <th>직급</th> <th>과제 관련 역할</th> </tr> </thead> <tbody> <tr> <td>카이스트</td> <td>한동수</td> <td>부교수</td> <td>SIMD 기반 고성능 스위치 개발</td> </tr> <tr> <td>성균관대학교</td> <td>정재훈</td> <td>조교수</td> <td>SDN/NFV네트워크보안기능IF 표준화</td> </tr> <tr> <td>숭실대학교</td> <td>정수환</td> <td>정교수</td> <td>안드로이드기반 모바일 샌드박스 개발</td> </tr> <tr> <td>서울대학교</td> <td>백윤홍</td> <td>정교수</td> <td>DL기반 VM환경 공격방어시스템 연구</td> </tr> <tr> <td>(주)KT</td> <td>장덕문</td> <td>부장</td> <td>SoA AI 기반 KT SIEM+ 사업화</td> </tr> <tr> <td>(주)SK인포섹</td> <td>박정현</td> <td>위원</td> <td>SoA시범서비스 업체 대상 보안관제</td> </tr> <tr> <td>(주)윈스</td> <td>박철정</td> <td>수석</td> <td>클라우드기반 vFW/vIPS/vDDoS개발</td> </tr> <tr> <td>(주)소만사</td> <td>최일훈</td> <td>부사장</td> <td>클라우드기반 vDLP 개발</td> </tr> <tr> <td>(주)하우리</td> <td>오재우</td> <td>부장</td> <td>클라우드 기반 vVaccine 개발</td> </tr> <tr> <td>(주)엠진시큐러 스</td> <td>조양현</td> <td>대표</td> <td>보안위협티켓관리 프로토타입 개발</td> </tr> <tr> <td>(주)아토리서치</td> <td>송용주</td> <td>이사</td> <td>100G급 고성능 서버 스위치 개발</td> </tr> </tbody> </table>	기관명	성명	직급	과제 관련 역할	카이스트	한동수	부교수	SIMD 기반 고성능 스위치 개발	성균관대학교	정재훈	조교수	SDN/NFV네트워크보안기능IF 표준화	숭실대학교	정수환	정교수	안드로이드기반 모바일 샌드박스 개발	서울대학교	백윤홍	정교수	DL기반 VM환경 공격방어시스템 연구	(주)KT	장덕문	부장	SoA AI 기반 KT SIEM+ 사업화	(주)SK인포섹	박정현	위원	SoA시범서비스 업체 대상 보안관제	(주)윈스	박철정	수석	클라우드기반 vFW/vIPS/vDDoS개발	(주)소만사	최일훈	부사장	클라우드기반 vDLP 개발	(주)하우리	오재우	부장	클라우드 기반 vVaccine 개발	(주)엠진시큐러 스	조양현	대표	보안위협티켓관리 프로토타입 개발	(주)아토리서치	송용주	이사	100G급 고성능 서버 스위치 개발							
기관명	성명	직급	과제 관련 역할																																																					
카이스트	한동수	부교수	SIMD 기반 고성능 스위치 개발																																																					
성균관대학교	정재훈	조교수	SDN/NFV네트워크보안기능IF 표준화																																																					
숭실대학교	정수환	정교수	안드로이드기반 모바일 샌드박스 개발																																																					
서울대학교	백윤홍	정교수	DL기반 VM환경 공격방어시스템 연구																																																					
(주)KT	장덕문	부장	SoA AI 기반 KT SIEM+ 사업화																																																					
(주)SK인포섹	박정현	위원	SoA시범서비스 업체 대상 보안관제																																																					
(주)윈스	박철정	수석	클라우드기반 vFW/vIPS/vDDoS개발																																																					
(주)소만사	최일훈	부사장	클라우드기반 vDLP 개발																																																					
(주)하우리	오재우	부장	클라우드 기반 vVaccine 개발																																																					
(주)엠진시큐러 스	조양현	대표	보안위협티켓관리 프로토타입 개발																																																					
(주)아토리서치	송용주	이사	100G급 고성능 서버 스위치 개발																																																					
<p>추진실적</p>	<p>○ 정량적 추진 실적 (1~3차년도)</p> <ul style="list-style-type: none"> <li>- 기술이전 <ul style="list-style-type: none"> <li>· “분산환경기반 대용량보안이벤트 연관성분석”등 8건</li> <li>· 기술료: 319백만원</li> </ul> </li> <li>- 특허 출원/등록 <ul style="list-style-type: none"> <li>· “네트워크 가상화 환경에서 보안 관리를 위한 장치” 등</li> </ul> </li> </ul>																																																							

	<p>12건 등록</p> <ul style="list-style-type: none"> <li>· “Detecting Distributed Reflection DoS Attack” 등 국제특허 18건 출원</li> <li>· “프로파일링기반 기계학습 활용 이상징후탐지” 등 국내특허 52건 출원</li> </ul> <p>- SCI 논문</p> <ul style="list-style-type: none"> <li>· “Design of Network Threat Detection and Classification based on Machine Learning on Cloud Computing” 등 SCI(E) 논문 9편</li> </ul> <p>- 국내외 표준화</p> <ul style="list-style-type: none"> <li>· “I2NSF Network Security Functions” 등 국제표준화 실적 27건</li> <li>· “클라우드 컴퓨팅의 모니터링 서비스 데이터 보안 요구사항” 등 국내표준화 실적 27건</li> </ul> <p>- 상용화</p> <ul style="list-style-type: none"> <li>· “(주)원스 SNIPER ONEv3.0”상용화 등 598백만원 상용화</li> </ul> <p>○ 정성적 추진 실적</p> <ul style="list-style-type: none"> <li>- 2016.10 클라우드 보안 서비스 센터 구축 <ul style="list-style-type: none"> <li>· 조기사업화를 위한 microIDC실환경 기반 기능시험/실데이터 분석</li> </ul> </li> <li>- 2017.11 ETRI 클라우드 기반 맞춤형 보안 서비스 런칭 <ul style="list-style-type: none"> <li>· 과제 개발 결과물에 대한 유효성 검증 목적</li> <li>· ETRI 융합기술연구생산센터 SoA(Security-on-Air) 센터</li> <li>· 10개 입주 업체 대상 서비스 제공</li> <li>· 네트워크 침해탐지/방화벽 서비스 및 데이터 유출차단 서비스 제공</li> <li>· 클라우드 기반 백신 서비스 및 안드로이드 악성코드 분석 서비스 제공</li> </ul> </li> <li>- 2017.11 IETF100 HACKATHON Best 프로젝트상 수상</li> <li>- 2018.01 ISP 보안관제센터 AI 기술 검증 PoC 수행 <ul style="list-style-type: none"> <li>· 지능형 SIEM 사업화를 위한 AI 기술 외부 검증 수행 일화</li> </ul> </li> <li>- 2018.04 RSA-Asia 안드로이드 악성코드 분석시스템 전시</li> <li>- 2018.08 Blackhat USA 2018 Delta 프레임워크 시연</li> <li>- 2018.10 SoA 맞춤형 보안 서비스 확대 <ul style="list-style-type: none"> <li>· Micro 클라우드센터 기반 SECaaS서비스 사업화 모델 검증 목적</li> <li>· 원격 기업 6개사 및 융합센터 옥내기업 10개사 대상</li> </ul> </li> </ul>
<p>사업실명제 후보사업 선정기준 <b>&lt;선택&gt;</b></p>	<ol style="list-style-type: none"> <li>① 주요 국정 현안 관련 사업 ( )</li> <li>② 재무적 영향이 큰 대규모사업 ( )</li> <li>③ 국민생활에 미치는 영향이 큰 주요 서비스 제공사업(주요 사업 등) ( ✓ )</li> <li>④ 중점관리가 필요한 기관의 핵심사업 ( )</li> <li>⑤ 기타 대국민 홍보가 집중적으로 필요한 사업 ( )</li> </ol>