THE9

2026

우수 정보보호 기술 등 (제품·서비스) 선정집



과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

우수 정보보호 기술 등
지정 제도 소개

지정로고

[우수 정보보호 기술 등]







[우수 정보보호 기업]



정보보호공시제도팀

061-820-3215

woosu@kisa.or.kr

목적

정보보호 분야 유망 新기술·제품·서비스의 발굴·지원을 통한 민간 차원의 신기술 R&D 투자 활성화 및 판로개척 등 성장지원

관련근거

「정보보호산업의 진흥에 관한 법률」제18조, 제19조 동법 시행령 제11조~제15조, 동법 시행규칙 제5조~7조, 우수 정보보호 기술등·우수 정보보호기업의 지정 및 지원 등에 관한 규정

지정자격

정보보호 벤처기업*으로서 제로트러스트, AI, 클라우드, 지능형 CCTV 등 혁신 기술을 활용하여 개발·개량한 물리보안, 정보보안, 융합보안 등의 정보보호 기술·제품·서비스(이하 “우수 정보보호기술 등”이라 함)를 보유한 기업

* 「벤처기업육성에 관한 특별법」 제2조의2 각 호의 요건에 부합하고 같은 법 제25조에 따른 ‘벤처기업확인서’를 보유한 자

지정 유효기간

지정서 교부일로부터 2년(이후 효력 자동 상실)

지정기준

[기술 등] ① 신규성, ② 독창성, ③ 사업화 가능성 종합적으로 평가
[기 업] ① 기술성, ② 사업성, ③ 산업 기여도 종합적으로 평가

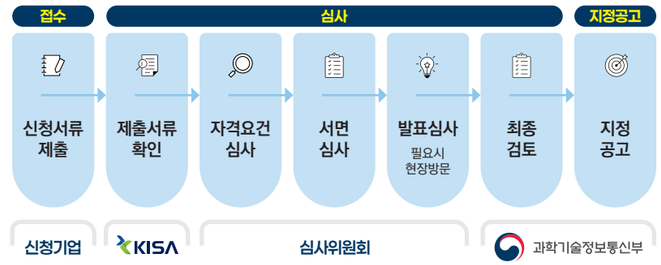
※ 최고점과 최저점 제외한 배점 합산 평균 70점 이상 시 지정

지정현황

2018년 최초 지정부터 현재까지 총 47종 우수 기술등으로 지정되었으며, 현재 유효인(2년) 우수기술은 총 18종

구분	2018년	2019년	2020년	2021년	2022년	2023년	2024년	2025년	2026년
지정기업 수	4	5	2	4	2	4	8	9	9

처리절차



AhnLab CloudMate

www.ahnlabcloudmate.com

사명	(주)안랩클라우드메이트	**대표**	김형준
사업자등록번호	789-81-01310	**소재지**	경기도 과천시
연락처	02-6390-6400		

지정번호	제2026-001호
지정분야	기술
지정기술명	비침습적 통합 게이트웨이를 통한 AI보안 및 정보보호 제품
지정기술 내용	생성형 AI 사용 시 발생하는 기밀정보 및 개인정보 유출 사고를 방지

특장점



- Agentless Gateway (비침습적 통합 게이트웨이)
  - 사용자 PC에 별도의 전용 에이전트 설치 없이 브라우저 확장·프록시 설정 등 기존 PC 관리 체계를 이용하여 트래픽을 정밀 제어하여, OS 충돌 없이 단 1일 이내 전사 무중단 배포 및 운영 공수 절감
    ※ 초경량 프록시 기술 적용으로 트래픽 처리 지연시간 0.5초 미만
- Context-Aware Engine (지능형 딥러닝 문맥 분석 엔진)
  - 단순 정규식 및 키워드 매칭의 한계를 극복하고, 특허받은 딥러닝 엔진을 통해 문장 맥락을 분석하여 데이터 내 개인정보(PII) 및 기업기밀(CI)을 실시간 식별 및 비식별처리 ※ 독자적 원천 특허 6건 보유 및 95% 이상의 높은 탐지 정확도
- Prompt Injection Guard (지능형 프롬프트 인젝션 방어)
  - 생성형 AI 모델을 조작하거나 탈옥(Jailbreak)하려는 고도화된 보안 정책 우회 및 공격 시도를 딥러닝 스코어링 분석을 통해 게이트웨이 단에서 실시간 탐지 및 맥락 차단
- Deep Inspection (AI 서비스 심층 분석)
  - AI 서비스별 구조를 해석해 프롬프트 본문과 첨부 파일을 추출·검사하여, 도메인 단위 허용·차단을 넘어 전송 내용 단위로 통제
- Multi-LLM Governance (멀티 LLM 통합 거버넌스)
  - ChatGPT, Claude, Gemini 등 다양한 국내외 LLM에 대해 단일 콘솔에서 일괄 보안 정책을 강제하고 전 수발신 내역을 JSON 로그로 저장하여 감사 추적 지원
    ※ KISA CSAP SaaS 표준등급 인증(CSAP-2025-029호) 획득 및 국정원 AI 보안 가이드라인 요건 완벽 수용

적용 분야

- 공공 및 국가 기관 (B2G)
  - 국가·공공기관 AI 보안 가이드라인 준수 및 CSAP 인증 요건 충족이 필수적인 정부 부처, 지방자치단체, 공공기관 및 국책연구기관의 행정·연구 AX(AI 전환) 환경
- 금융 및 대기업 (B2B)
  - 망 분리 규제 대응, 내부 핵심 기밀(소스코드, 영업비밀) 및 고객 개인정보 유출 방지가 최우선인 금융권, 제조·대기업, IT/유통 분야의 생성형 AI 도입 환경
- 멀티 LLM 및 AI 에이전트 활용 환경
  - 다양한 외부 LLM(ChatGPT, Claude, Gemini 등) 및 RAG 기반 사내 지식 플랫폼을 연계하여 안전한 AI 거버넌스를 구축하려는 전 산업군 온프레미스/SaaS 운영 환경

기대효과

- AI 보안 위협 차단 및 데이터 유출 예방
  - As-Is: 기존 키워드/패턴 기반 DLP 및 네트워크 보안 장비는 문장 맥락 속 정교한 기밀 유출이나 프롬프트 인젝션/탈옥 공격을 탐지하지 못해 AI 사용을 전면 금지·제한함
  - To-Be: 딥러닝 문맥 분석 및 스트리밍 재조립 기술로 95% 이상 정확도로 위협을 차단하며, 민감정보만 실시간 비식별처리 하여 보안 리스크 없이 AI를 안심하고 활용
- 사용자 편의성 극대화 및 배포·운영 비용 절감
  - As-Is: 사용자 PC마다 에이전트를 설치해야 하여 OS 충돌, PC 성능 저하, 개별 설정 및 업데이트 등 과도한 배포·관리 공수 발생
  - To-Be: PC 별도 설치가 없는 Agentless 게이트웨이 방식으로 단 1일 이내 전사 무중단 배포가 가능하고, 지연시간 0.5초 미만의 무장애 환경으로 업무 생산성 극대
- 규제 준수(Compliance) 및 안전한 AX(AI 전환) 추진
  - As-Is: 각 AI 서비스별 개별 정책 적용의 어려움과 보안 감사 대응용 로깅 부재로 인해 공공·금융권 컴플라이언스 요건 충족 불가능
  - To-Be: CSAP 표준등급 인증 기반의 단일 콘솔에서 멀티 LLM 정책 통합 제어, 국정원 AI 보안가이드 수용 및 전사 JSON Audit 로깅을 통해 규제에 완벽 대응하는 전사 AI 전환 실현

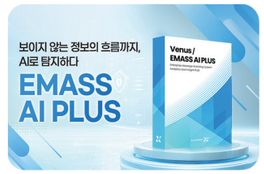
XCURENET

www.xcurenet.com

사명	(주)엑스큐어넷	**대표**	김정필
사업자등록번호	110-81-40818	**소재지**	서울시 은평구
연락처	02-567-0961		

지정번호	제2026-002호
지정분야	제품
지정기술명	EMASS AI PLUS
지정기술 내용	Full Packet을 수집 및 저장하여 가시성을 확보하고 AI 기반으로 사용자 행위를 분석하는 정보 유출 탐지 보안 솔루션

특장점



- Full Packet 기반 데이터 가시성 확보
  - 네트워크 트래픽의 Full-Packet과 PCAP 원본을 수집·저장하여 메일, 웹, 메신저, 파일 전송 등 다양한 업무 경로의 데이터 흐름을 확인할 수 있습니다. 정책 변경 이후에도 저장된 데이터를 재처리하여 과거 트래픽을 다시 분석할 수 있어 정보유출 사고 조사와 감사 대응을 지원합니다.
- AI·LLM 기반 콘텐츠 및 이상 행위 분석
  - 메일 본문, 메신저 대화, 첨부파일, URL 등 다양한 콘텐츠를 AI·LLM으로 분석하고, 사용자·부서·서비스 단위의 이용 패턴을 바탕으로 이상행위를 탐지합니다. 단순 키워드 탐지를 넘어 콘텐츠와 사용자 행위를 함께 분석하여 보안 담당자의 위험 판단을 지원합니다.
- 생성형 AI·SaaS까지 아우르는 다채널 로깅
  - 기존 이메일·웹·메신저뿐 아니라 클라우드·SaaS와 ChatGPT, Gemini, Copilot 등 생성형 AI 서비스의 사용 이력까지 수집·조회할 수 있습니다. 300개 이상의 서비스 패턴을 지원하여 변화하는 업무 환경의 데이터 이동 경로에 대한 가시성을 확보합니다.

적용 분야

- 제조·연구소
  - 핵심 기술, 설계도면, 소스 코드 등 중요 정보의 외부 이동 및 유출 경로 추적
- 금융
  - 전자 금융 관련 업무 기록 관리 및 내부 통제·감사를 위한 증적 확보
- 공공·국방
  - 정책 기반 데이터 흐름 관리 및 민감 정보 보호, 감사 자료 확보
- 의료·교육
  - 개인정보·민감 정보의 이동 경로 확인 및 정보 보호·컴플라이언스 대응



기대효과

- 전사 데이터 가시성 강화
  - 메일·웹·메신저부터 SaaS·생성형 AI까지 다양한 업무 채널의 데이터 흐름을 통합적으로 확인
- 정보 유출 사고 대응력 향상
  - Full-Packet 및 PCAP 원본을 기반으로 유출 경로와 원인을 추적하고 과거 데이터까지 소급 분석
- 보안 분석 효율 향상
  - AI·LLM 및 사용자 이상행위 분석을 통해 방대한 데이터에서 보안 담당자가 확인해야 할 위험 요소의 판단 지원
- 감사·컴플라이언스 대응 지원
  - 원본 데이터, 메타 정보, 관계도, 리포트 등을 활용하여 사고 조사 및 감사에 필요한 증적 확보

www.osangtech.co.kr

사명	(주)오상테크놀로지	**대표**	박수경
사업자등록번호	117-81-63087	**소재지**	서울시 금천구
연락처	070-7772-7766		

지정번호	제2026-003호
지정분야	서비스
지정기술명	AI 기반 ISMS-P 자율인증 자동화 플랫폼(ISMS-P GUARD)
지정기술 내용	AI 멀티에이전트(Auditor-Critic)가 보안 증적을 자동 수집·분석하여 ISMS-P 101개 통제항목의 준수 여부를 판정하고, 인증 보고서를 자동 생성하는 자율인증 플랫폼.

특장점

- Auditor-Critic 교차검증 + 결정론적 가드레일
  - Critic 에이전트가 Auditor의 1차 판정을 독립 컨텍스트에서 반증하고, 지식그래프로 증적의 실존 여부를 대조해 근거 없는 '준수' 판정을 차단
    ※ 자체 실증 결과 오판정(환각) 발생률 0.05% 미만
- 3중 하이브리드 RAG + 6-Signal 리랭킹
  - 벡터·키워드·지식그래프 동시 검색과 6개 신호 가중 결합으로 HWP·PDF·이미지·로그 증적을 101개 인증기준에 자동 매핑
- 망분리 온프레미스(On-Premise) Private AI
  - 내부망에 로컬 LLM을 탑재해 증적의 외부 반출 없이 판정·보고서 생성까지 수행(SaaS형 병행 제공), 초당 3,200토큰 처리(L40S 2장 기준)
- 감사 추적성·보안을 갖춘 상시 인증 관리(Continuous Compliance)
  - 증적 만료·자산 변동·법령 개정 시 재판정 후 보완 업무로 전환하고, 판정·검토 이력은 해시체인 감사 로그로 보존



▲ AI 멀티에이전트(Auditor-Critic)를 통한 정책·지침 기반 이행활동 관리


▲ ISMS-P GUARD 판정 구조 - 교차검증·결정론적 가드레일

적용 분야

- ISMS·ISMS-P 인증 의무 및 의무화 추진 대상
  - ISP·IDC·상급병원·대학·금융 등 ISMS 의무대상 및 인증 취득 기업, 의무화가 추진되는 이동통신사·본인확인기관 등
- 망분리·폐쇄망 운영 고보안 기관
  - 외부 클라우드 AI 사용이 제한된 금융·공공·국방 기관에 온프레미스로 구축, 민감 증적을 내부망에서만 처리
- 정보보호 컨설팅·관리형 보안서비스(MSSP) 기업
  - 멀티테넌트 구조로 다수 고객사의 증적 관리·판정·보고서 작성을 표준화하여 컨설팅 품질 편차 축소

기대효과

- 인증 준비기간 단축
  - As-Is : 컨설팅·수작업 중심, 전담 3~5명이 6~12개월간 증적 수집·점검
  - To-Be : 101개 인증기준 1차 자동 판정 약 26분, 준비기간 2~4개월
- 인증 비용 절감
  - As-Is : 인증·갱신 때마다 건당 3,000만~1억 원의 일회성 컨설팅 반복
  - To-Be : 월 구독형(SaaS) 전환으로 연간 비용 최대 70% 절감
- 판정 신뢰성·심사 대응력 향상
  - As-Is : 메일·공유폴더에 분산된 증적, 누락·버전 불일치로 소명 지연
  - To-Be : 판정마다 원문 근거·검토 이력 제시, 누락 증적 자동 탐지
- 상시 컴플라이언스 체계 전환
  - As-Is : 인증 취득 후 관리 공백, 사후심사 직전 자료 재작성 반복
  - To-Be : 변경 시 재판정·알림, 보고서 초안 수일 → 약 30초

www.logpresso.com

사명	(주)로그프레소	**대표**	양봉열
사업자등록번호	121-86-24069	**소재지**	서울시 마포구
연락처	02-6730-7249		

지정번호	제2026-004호
지정분야	제품
지정기술명	AI·빅데이터 기반 통합 보안관제 플랫폼 (Logpresso Sonar)
지정기술 내용	위협 탐지 분석 대응 시각화 전 과정을 AI 에이전트가 자율 수행하는 차세대 보안 운영 플랫폼

특장점

- Agentic AI 기반 보안운영 자동화
  - 계획·메모리·도구·행동 구조의 AI 에이전트가 탐지 이벤트 조회, 연관 분석, 티켓 및 분석 보고서 작성 등 여러 단계의 보안운영 업무를 자동 수행
- 폐쇄망에서도 동작하는 생성형 AI
  - GPU/NPU 어플라이언스에 AI 모델을 탑재하여 외부 인터넷 연결 없이 운영 가능하며, 필요 시 클라우드 AI API 연동 방식도 선택 가능
- 자체 개발 고속 빅데이터 엔진
  - 2010년부터 자체 개발한 실시간 인덱싱·컬럼지향 저장·SIMD 문자열 처리 기술로 대용량 로그를 빠르게 수집·저장·검색
- 객체 그래프 기반 연관 분석
  - IP·도메인·사용자·CVE·부서 등 객체 간 관계 그래프를 자동 생성하여 공격 경로와 연관 위협을 도식이 포함된 분석 보고서로 제공
- 앱 스토어 기반 기능 확장이 가능한 글로벌 수준의 에코시스템
  - 플러그인 구조로 파서·수집기·탐지 시나리오·플레이북 등 250여 종의 앱을 서비스 중단 없이 추가하여 다양한 보안장비, 클라우드, SaaS 등 연동 및 SIEM·SOAR·XDR 기능 확장



적용 분야

- 에어 갭 환경의 공공·금융·국방 기관
  - 외부 생성형 AI 서비스 이용이 제한되는 환경에서 내부 AI 모델로 보안관제 업무를 자동화하려는 기관의 통합 관제
- 대용량 로그를 다루는 대기업 및 보안관제 사업자(MSSP)
  - 일 수십 TB 규모의 로그 수집·분석이 필요한 환경, 여러 고객사를 원격으로 관제하는 MSSP 환경
- 클라우드 기반 서비스 기업
  - 자체 인프라 구축 없이 SaaS형(Logpresso Cloud)으로 보안관제·로그 보관 체계를 도입하고 ISMS-P 등 인증 대응이 필요한 기업(적용 사례: 모두싸인)

기대효과

- 보안관제 업무 효율화
  - As-Is : 경보마다 담당자가 로그 조회·연관 분석·보고서 작성을 수작업으로 수행
  - To-be : AI 에이전트가 정탐·오탐 분석, 보고서 작성 및 대응 업무까지 자동 수행하여 관제 인력은 고위험 위협 판단 등 핵심 업무에 집중 가능
- 로그 처리 인프라 비용 절감
  - As-Is : 로그량 증가에 따라 장비 증설 및 라이선스 비용 부담 증가
  - To-be : 고성능 자체 엔진으로 장비당 처리량을 높여 동일 로그량을 더 적은 장비로 처리
- 온프레미스 환경의 에이전틱 SOC 활용
  - As-Is : 보안 정책상 클라우드 서비스 활용이 불가능하고, SIEM·SOAR 등을 개별 제품으로 운영
  - To-be : GPU 및 국산 NPU 어플라이언스 기반 SIEM, SOAR, XDR이 통합된 에이전틱 SOC 운영 가능

CYTUR

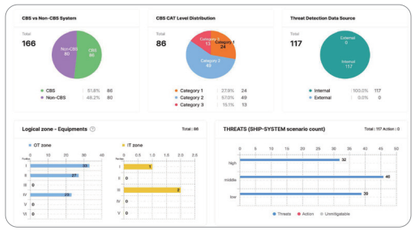
www.cytur.net

사명	주식회사 싸이터	**대표**	조용현
사업자등록번호	410-87-09010	**소재지**	부산광역시 해운대구
연락처	070-8822-2308		

지정번호	제2026-005호
지정분야	기술
지정기술명	선박 사이버보안 위협 분석 솔루션 CYTUR-TM
지정기술 내용	스마트선박, 자율운항선박의 사이버위협 모델링 솔루션

특장점

- 선박 설계 데이터 기반 위협 모델링 자동화
  - 선박 설계 데이터를 자동 분석하여 시스템 간 데이터 흐름을 DFD로 시각화하고, 가능한 사이버 공격 경로를 Attack Tree로 생성하여 설계 단계에서 잠재 위협을 사전에 식별
- Zone/Conduit 기반 사이버 리스크 분석
  - 선박의 물리·논리적 보안 구역(Zone)과 구역 간 연결 통로(Conduit)를 기반으로 위험을 분석하고, 구역별 사이버 리스크를 정량적으로 평가
- 선박 IT·OT 환경 특화 분석
  - NMEA, Modbus, AIS 등 선박·산업용 통신 환경과 항해·추진·기관·화물 등 선박의 컴퓨터 기반 시스템(CBS)을 반영하여 일반 IT 환경과 차별화된 선박 특화 위협 분석 수행
- 자산 인벤토리 및 규정 대응 산출물 자동화
  - 선박 IT·OT 장비를 구역별로 분류하여 자산 인벤토리를 구축하고, 위협 식별·리스크 평가 결과와 선급 심사에 활용 가능한 보고서를 자동 생성
- 실증을 통한 분석 효율성 검증
  - 과학기술정보통신부·KISA 실증사업을 통해 기존 대비 선박 사이버 위협 분석률 400% 증가 및 선박 설계 보안 투입 자원 83% 감소 확인



적용 분야

- 조선소 및 선박 설계
  - 신조선의 설계·건조 단계에서 선박 네트워크와 IT·OT 시스템의 사이버 위협을 사전에 분석하고 보안 설계에 활용
- 선박 사이버보안 규정 대응
  - IACS UR E26/E27에 따른 자산 식별, Zone/Conduit 분석, 위협 식별 및 위험평가 등 선박 사이버 복원력 설계·검증 업무에 활용
- 선박 기자재 및 시스템 보안 검토
  - 항해·통신·추진·기관·화물 등 선박 내 컴퓨터 기반 시스템(CBS)의 연결 관계와 공격 경로를 분석하여 기자재 및 시스템의 보안 위험 검토에 활용

기대효과

- 설계 단계 사이버 위협 사전 식별
  - 건조 이후 발견될 수 있는 사이버보안 취약 요소를 설계 단계에서 사전에 식별하여 보안 설계 변경 및 대응을 지원
- 위협 분석 업무 자동화 및 효율 향상
  - 수작업 중심의 선박 사이버 위험 분석을 자동화하여 분석시간 단축 및 반복적인 설계 보안 업무에 필요한 자원 절감
- 선박 사이버보안 규정 대응 효율화
  - 자산 인벤토리, 위협 분석, 위험평가 등 관련 산출물을 체계적으로 관리하여 IACS UR E26/E27 대응 및 선급 심사를 위한 증빙자료 작성 지원
- 정량 검증 효과
  - As-Is : 수작업 중심의 선박 사이버 위협 분석 및 설계 보안 업무
  - To-Be : CYTUR-TM 적용을 통해 위협 분석률 400% 증가, 설계 보안 투입 자원 83% 감소

(주)인피니그루

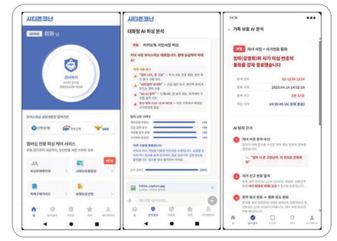
www.infinigru.com

사명	(주)인피니그루	**대표**	유경식
사업자등록번호	107-88-34153	**소재지**	서울시 성동구
연락처	02-3453-4620		

지정번호	제2026-006호
지정분야	서비스
지정기술명	시티즌코난 플랫폼
지정기술 내용	보이스피싱으로부터 보호를 받아야 하는 사용자와 예방 의무가 있는 기관을 연결하여, 금융사와 수사기관이 공동 대응할 수 있도록 지원하는 디지털범죄 사회안전망 플랫폼

특장점

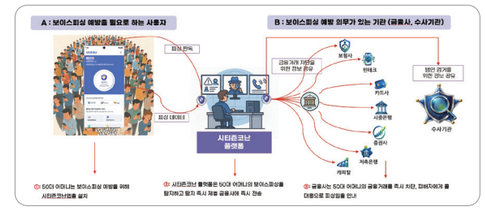
- 24×365 독립구동형 상시감지 (금융사 인앱)
  - 금융앱이 실행되지 않거나 비활성화된 상태에서도 악성앱·원격제어 등 보이스피싱 상시 감지
- 보이스피싱 전(全) 단계 탐지·대응·지원 (독립앱)
  - 스미싱, 허위사칭이미지, 악성앱, 원격제어, 전화가로채기, 악성 IP/URL 등 보이스피싱 사기 과정의 다양한 위협을 탐지 및 금융사 실시간 공유
- 금융기관·수사기관 공동대응 플랫폼
  - 기 확보된 피싱지향 데이터(약 62억건) 빅데이터 분석 정보 제공
- '국민 보안앱'- 기술사용자 4,500 만 명이상
  - 독립앱 1,100만명 이상, 금융사 인앱 3,400만명(중복포함) 이상 확보(누적) 피해예방: 약 19.4만 명의 피해 사전 예방, 약 8.4조원의 피해 사전예방(2022~2025년 추정)
- 기타
  - 개인정보유출 여부 확인, WIFI 보안상태 점검, 스미싱문자 정밀 진단, 금융앱 원격제어시 탐지, 사기꾼과의 통화 강제 종료, 보이스피싱 보험 혜택 등



▲ 시티즌코난 서비스 이미지

적용 분야

- 공공앱에 인앱 적용을 통한 전 국민 보이스피싱 보호
  - 국민이 사용하는 주요 공공앱에 시티즌코난(피싱아이즈) 24×365 상시감지 인앱기술을 탑재하여, 별도의 보안앱 설치없이 전 국민으로 보이스피싱 보호 범위 확대
- 금융기관·핀테크 서비스
  - 은행, 카드사, 저축은행, 증권사, 간편결제 등 금융앱에 인앱 SDK 형태로 적용하여 FDS와 연계한 보이스피싱 예방
- 공공기관·수사기관
  - 경찰·공공기관 등의 디지털범죄 대응 서비스와 연계하여 사고정보 공유, 피해자 보호 및 현장 대응에 활용
- 일반 국민·가족 보호
  - 독립앱으로 악성앱·스미싱·원격제어 등 위험 경고·차단하고 가족 돌봄이, 피해입증 보고서, 보이스피싱 보험 손실보상 등 사후케어 서비스 제공



기대효과

- 24×365 상시감지 기술로 선제적 피해 예방
  - 금융앱 인앱에서 실행 여부와 관계없이 보이스피싱 위험 감지
- 신속한 금융소비자 보호
  - 금융기관 연계를 통한 거래 모니터링·제한 등 즉각 대응
- 민·관 공동대응 강화
  - 금융사·공공기관·수사기관 간 위험정보 공유 및 공동 대응

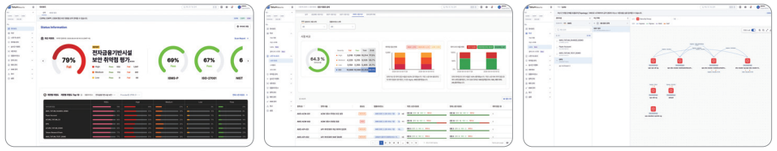
www.tatumsecurity.com

사명	주식회사 테이텀	**대표**	양혁재
사업자등록번호	277-81-01840	**소재지**	서울시 강남구
연락처	02-6949-2446		

지정번호	제2026-007호
지정분야	제품
지정기술명	CNAPP
지정기술 내용	멀티클라우드와 컨테이너 환경 전반의 보안 설정 오류, 워크로드 위협, 과도한 접근 권한을 단일 플랫폼에서 통합 진단하고 선제적으로 대응하는 클라우드 네이티브 보안 솔루션

특장점

- **국내 컴플라이언스 완벽 지원 및 자동화**
  - ISMS-P, CSAP(클라우드 보안인증), 전자금융감독규정, 금융보안원 클라우드 보안 가이드라인 등 국내 전용 규제를 기본 정책으로 제공합니다.
- **올인원 통합 모니터링**
  - CSPM(설정 오류 모니터링), CWPP(워크로드/컨테이너 보안), CIEM(계정 및 권한 관리), KSPM(쿠버네티스) 영역을 하나의 대시보드에서 통합 제공하여 운영 효율을 높입니다.
- **멀티·하이브리드 클라우드 지원**
  - AWS, Azure, GCP 등 Public Cloud뿐만 아니라 온프레미스 및 Private Cloud 환경의 자산까지 모두 지원 합니다.
- **우선 순위 기반 위험 관리**
  - 단순 취약점 나열이 아닌, 실제 위협 수준과 영향도 분석을 거쳐 긴급히 조치해야 할 위협 요소부터 보안 가이드를 제시합니다.
- **국내 5대 대표 시중은행 공급으로 검증된 신뢰성**
  - 보안 요구사항과 규제가 가장 까다로운 국내 대표 5대 시중은행을 포함한 주요 금융 그룹사에 솔루션을 제공하며 독보적인 기술력과 안정성을 검증 받았습니다.



적용 분야

- **금융·공공 등 규제 대응 중심 분야**
  - ISMS-P, CSAP, 전자금융감독규정 등 엄격한 컴플라이언스 준수와 감사 리포트 자동화가 필요한 공공 기관 및 금융·핀테크 기업에 적합합니다.
- **엔터프라이즈 등 클라우드 네이티브 중심 분야**
  - 멀티 클라우드(AWS, Azure, GCP 등) 자산의 통합 관리나 쿠버네티스·컨테이너(MSA) 환경의 워크로드 취약점 및 권한 통제가 필요한 기업에 적합합니다.

기대효과

- **운영 효율 강화**
  - 영역별 개별 솔루션(CSPM, CWPP 등)을 각각 구매·운영 할 때 발생하는 비효율성과 피로도를 줄여 보안 관리 효율을 극대화합니다.
- **인증 및 감사 준비 시간 절감**
  - 자동 리포트 제공 및 이력 관리를 통해 매년 반복되는 ISMS-P, 금융권 감사 등 규제 응대 시간을 대폭 줄입니다.
- **보안 공백 및 위협 감소**
  - 클라우드 침해 사고의 상당수를 차지하는 설정 오류, 과도한 IAM 권한 부여 등을 실시간으로 탐지하고 보안 인사이트를 제안하여 공격 표면을 줄이는 데 도움을 줍니다.

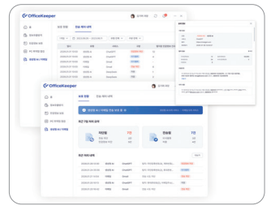
지란지교소프트

https://www.jiransoft.co.kr
https://www.officekeeper.co.kr

사명	(주)지란지교소프트	**대표**	박승애, 유병완
사업자등록번호	314-81-14867	**소재지**	대전광역시 유성구(지사: 경기도 성남시)
연락처	031-606-9350		

지정번호	제2026-008호
지정분야	기술
지정기술명	생성형 AI 및 이메일 구간 민감정보 탐지·차단·비식별화 및 감사 통합 보안 기술
지정기술 내용	엔드포인트 에이전트에 내장된 트래픽 감시 기능으로 생성형 AI 프롬프트와 이메일 본문의 민감정보를 실시간 탐지·차단·비식별화하고, 처리 이력을 통합 감사하는 네트워크 DLP 기술

특장점



- **에이전트 내장형 네트워크 DLP**
  - 별도 프록시 서버·SSL 인증서 배포 없이 오피스키퍼 EP 에이전트 업데이트만으로 HTTPS 구간 (생성형 AI·웹메일) 민감정보 검사 활성화
- **생성형 AI 프롬프트 DLP**
  - ChatGPT·Claude·Gemini·DeepSeek·Perplexity·Liner·Grok 7종을 웹 브라우저·클라이언트 앱 양쪽 경로에서 제어
  - 주민등록번호·카드번호·계좌번호·여권번호 등 9종 민감정보 패턴 + 관리자 정의 키워드·정규식 탐지
- **이메일 본문 DLP**
  - Gmail·Naver·Daum·Outlook 웹메일 4종 및 SMTP/IMAP 발송 전 본문·첨부를 실시간 스캔
  - 수신 도메인 유형(외부 개인 메일 / 협력사·고객사 / 내부)별로 정책 자동 분기
- **허용·차단·비식별화 3모드 정책 엔진**
  - 민감정보만 자동 마스킹한 뒤 전송하여 업무를 중단시키지 않고 유출 위험만 제거
- **AI·이메일 통합 감사 로그**
  - 프롬프트·메일 본문 원문, 처리 결과를 단일 콘솔에 자동 기록

적용 분야



- **생성형 AI를 업무에 활용하는 기업·기관**
  - 외부 AI 사용을 전면 차단하지 않고, 민감정보만 통제하며 안전하게 허용해야 하는 조직
- **개인정보를 대량 보유·처리하는 분야**
  - 금융·의료·공공·교육 등 개인정보보호법·ISMS-P 준수와 감사 증적 확보가 필요한 조직
- **네트워크 인프라 투자가 부담스러운 중소·중견기업**
  - 프록시·게이트웨이 장비 구축 없이 PC 에이전트만으로 네트워크 DLP 도입이 필요한 환경
- **기존 오피스키퍼 고객**
  - 기존 에이전트·관리 콘솔에 기능 추가 형태로 즉시 확장 (오피스키퍼 EP 업데이트 시)

기대효과



- **AI 시대 신규 유출 경로 통제**
  - 임직원의 AI 입력 내용을 전송 전에 탐지·차단하고, 전체 프롬프트 이력을 100% 기록
- **이메일 유출 사전 예방**
  - 민감정보를 발송 전에 차단하거나, 필요한 정보만 비식별화하여 업무 중단 없이 안전하게 발송
- **보안과 업무 연속성 동시 확보**
  - 전면 차단 대신 비식별화 모드를 통해 AI·메일 업무 흐름을 유지하고, 사용자 안내를 통해 보안인식 즉시 제고
- **감사·컴플라이언스 대응력 강화**
  - 제품별로 분산된 로그를 단일 콘솔에서 사용자·서비스·수신자·기간별로 통합 검색하고, CSV 형태의 감사 증적 확보
- **도입·운영 비용 절감**
  - 프록시 서버·인증서 배포 및 AI DLP·메일 DLP 등 별도 솔루션 구축 없이 에이전트 업데이트만으로 기능 활성화, 단일 라이선스·단일 콘솔로 운영

※ 자체 시뮬레이션 기준(100~500명 중견기업, 별도 솔루션 조합 방식 대비) 5년 TCO 약 60% 절감 기대

www.pco.io.kr

사명	(주) 피시오	**대표**	곽서준
사업자등록번호	243-86-01731	**소재지**	부산 남구 남동천로 128, 1105호
연락처	031-698-4155		

지정번호	제2026-009호
지정분야	기술
지정기술명	저대역 네트워크 환경을 위한 AI 영상 실시간 최적화·IPsec 보안 전송 기술
지정기술 내용	AI 기반 영상 최적화와 IPsec 보안전송 기술을 결합하여 저대역 환경에서도 고해상도 영상의 전송 효율·보안성을 확보하는 Edge–Center 기반 정보보호 기술

특장점

- 전송·저장 효율과 보안 동시 확보
  - 비트스트림 실시간 경량화와 KCMVP 검증필 암호모듈 연계 IPsec 보안전송
- 80~90% 실시간 데이터 경량화
  - 비트 재분배·프레임 최적화로 데이터량 절감
- 기존 영상 인프라에 즉시 적용
  - H.264/H.265 표준 IP카메라·NVR/VMS 연동
- Edge 통합관리
  - Edge 상태 모니터링·정책 중앙 배포



적용 분야

- 무선·저대역 영상관제
  - LTE/5G·위성·무선망 기반 영상 전송
- 해상·이동형 재난 대응
  - 선박·소방차·드론의 실시간 상황 공유
- 공공·산업시설 원격감시
  - 항만·발전소·정수장·외곽 경계
- 기존 CCTV 관제망 고도화
  - 지자체·도로·공항 영상 관제



기대효과

- 네트워크·저장 효율 향상
  - 네트워크 병목 완화·저장공간 활용도 증대
- 현장부터 중앙까지 전송 구간 보호
  - IPsec으로 영상 기밀성·무결성 보호
- AI 분석·관제 효율 향상
  - 고해상도·고화질 영상 활용 여건 개선
- 무선 영상 서비스 신사업 창출
  - 안정적 영상 송출로 해상·이동형 서비스 확대



THE9

2026 우수 정보보호 기술 등(제품·서비스) 지정 기업

AhnLab CloudMate

XCURENET

Knowledge&Technology

LOGPRESSO

CYTUR

(주)인피니그루

Tatum Security

지란지교소프트

PCO

기존 우수 정보보호 지정기술 현황

2018년~2025년, 총 38종

지정연월	개발사	기술의 명칭	기술내용
2025. 6 (~2027. 6월)	㈜수산아이앤티	ePrism SSL VA	• SSL/TLS 트래픽 가시성 제공 솔루션
	악성코드검거단(주)	자체개발 경량 하이퍼바이저 기반 비실행형 악성코드 탐지기술	• 고도화된 위협에 대응하는 자체개발 경량 하이퍼바이저 기반 비실행형 악성코드 탐지 기술
	옥타코 주식회사	Phishing-resistant M2A 서비스 및 지문보안키	• 제로트러스트 기반 Phishing-resistant M2A서비스 및 지문보안키
	이노뎁(주)	지능형 선별관제 솔루션(IOIE)	• MLOps 및 VLM 기술 기반 선별 관제 시스템
	주식회사 고스트패스	탈중앙화 및 이원화 기술 기반 생체 데이터 보안솔루션	• 생체정보를 스마트기기에 저장하는 탈중앙화 기술로, 인증장치와 인증 요청장치를 분리한 이원화 구조를 결합한 기술
	주식회사 더코더	스마트 보안페이퍼	• 피지컬/디지털 기술을 융합하여 보안성과 편의성을 높인 인쇄물 보안 솔루션
	주식회사 센스톤	OTAC for Phygital	• 단방향 다이내믹 코드(One-Time Authentication Code; OTAC) 기반 사용자 및 기기 인증 기술
	주식회사 엔피코어	RansomZERO EDR AI SaaS	• RGB기반 AI 이미지 분석으로 신·변종 랜섬웨어까지 실시간 탐지·차단하는 클라우드 기반 SaaS 보안서비스
	주식회사 체크멀	AppCheck Pro	• 상황인식 기반 랜섬웨어 행위 탐지부터 데이터 백업, 자동 복원까지 통합 지원하는 안티랜섬웨어 전문솔루션
2024. 9	㈜파인더갭	파인더갭 버그바운티	• 크라우드소싱(Crowd-Sourcing) 기반 보안 취약점 진단 플랫폼 (버그바운티)
	㈜에스엔피랩	On-Device 마이데이터 플랫폼	• 이종 산업 데이터를 스마트폰에서 결합하여 활용하는 온디바이스 마이 데이터 기술
	㈜아르고스 아이덴티티코리아	아르고스아이덴티티 플랫폼	• 얼굴인식, 신분증 위변조 방지, 국가별 ID 자동인식 등 AI 기반 비대면 신원인증 솔루션
	㈜엔에스랩	Pure Wallet	• 자체 블록체인 기술 활용, 오프라인 모바일결제 지원, 데이터 보호 위한 보안 알고리즘 적용 등
	㈜디사일로	디사일로 데이터 클린룸 서비스	• 프라이버시 강화 기술 활용 데이터 유출을 최소화하는 데이터 분석거래 플랫폼
	㈜앤오픈	어튼아이디(AUTENID)	• 사용자 얼굴 데이터 및 개인정보 암호화, 오용/악용 방지
2024. 6	㈜셈퍼파이	URLyBud v3.0 URL Tumbler	• 일회용 링크가 아닌 영구적인 고객 전용 고유 URL 보안 링크를 통해 디지털 서비스를 구현하는 B2B솔루션
	㈜시큐리온	OnTrust	• 악성 앱 및 해킹 위협으로부터 모바일 ·IoT 기기를 보호하는 AI 기반 실시간 해킹 탐지 솔루션
2023. 6	㈜원모어시큐리티	원모어아이(OneMoreEYE) v1.0	• 다중 CCTV 영상 연계를 통한 동일인 및 차량 재식별화, 추적 및 이동 경로 시각화 서비스
	케이포시큐리티㈜	분산ID 기반 다계층 통합 해석기 시스템	• 분산ID 상호운용성을 통한 자기주권 신원활용과 안전한 신원 확인 등 사용자 신원 인증 및 관리 기술
	㈜지크립토	영지식증명(zk-SNARK) 활용 블록체인 프라이버시 보호 기술	• 영지식증명(zk-SNARK) 기술을 통한 블록체인 기반의 프라이버시 보호 기술
	㈜오내피플	캐치시큐	• 개인정보의 수집부터 파기까지 개인정보의 생명주기를 자동으로 관리하는 자동화 솔루션
2022. 7	㈜지란지교데이터	IDFILTER (개인정보비식별화 솔루션)	• 데이터의 안전한 활용 지원을 위한 AI 기반 개인정보 비식별 처리 기술
	㈜프라이빗 테크놀로지	데이터 플로우 계층 기술 기반 Zero Trust 네트워크 접속 통제 기술	• 데이터 플로우 계층 기술 기반 Zero Trust 네트워크 접속 통제 기술
2021. 11	㈜씨티아이랩	세계 최초 AI 기반 차세대 컨버전스 사이버 위협 탐지 기술 DTI	• AI기반의 인터넷망 및 산업제어망 사이버 위협 탐지 기술
	㈜한줌	스마트잠금장치(똑똑한락)	• 인증서버와 연계하여 모바일로 원격 제어하는 스마트 안전 제어 기술로 물리보안과 OTP인증 적용 데이터 보안을 결합한 스마트잠금장치
	㈜스틸리언	앱수트 프리미엄 (AppSuit Premium)	• 모바일 앱의 위변조를 방지하고 암호화와 난독화 기능을 제공하여 사이버 공격으로부터 모바일 앱을 보호하는 보안 솔루션
	㈜누리랩	빅데이터 기반 사이버위협 대응 및 분석 플랫폼(MINOSS 2.0)	• 신·변종 사이버 위협의 DNA를 추출하여 학습된 빅데이터와의 유사도 분석을 통한 보안사고 사전대응 및 위협 분석 플랫폼
2020. 9	㈜딥핑소스	데이터 익명화 기술	• 개인정보 침해없이 AI 영상 분석시스템 등에 활용 될 수 있는 기계학습용 이미지 데이터 익명화 기술
	㈜알파비트	Alpha SmartGuard V3.1	• 전자파일 등 비정형 데이터에 포함된 개인정보를 암호화하여 개인정보 유출을 차단 및 보호하는 비정형 데이터 암호화 솔루션
2019. 10	㈜락인컴퍼니	리앱(LIAPP)	• 5G와 같이 급변하는 모바일 환경에도 호환성과 강력한 보안성으로 보안위협에 대응하기 위한 모바일 애플리케이션 통합 보안 솔루션
	㈜삼오씨엔에스	파르고스	• 개인정보 접속기록 인텔리전스 분석 등을 통해 개인정보 대량유출 사고 방지를 위한 개인정보보호 솔루션
	㈜스파이스웨어	Spiceware	• 클라우드 환경에서 자동화된 데이터 암호화 및 복호화 처리를 통해 개인정보와 기업 비밀 데이터 등의 주요 데이터를 보호하는 솔루션
	㈜에프원시큐리티	클라우드 통합 웹서버 보안서비스	• 클라우드 기반 통합 웹서버 보안 서비스
	㈜와이키키소프트	와이덴터티 2.0	• 생체인증과 딥러닝(자이로센서 측정, 인증시간, 인증위치 등 학습) 기반 이상징후 탐지 기술이 결합된 FIDO 2.0 인증 기반 Password-Less 솔루션
2018. 9	㈜시웃	IoT End-to-End 보안솔루션	• 'HW 보안모듈'과 'SW 보안모듈'을 탑재하여 IoT 전 구간에서 애플리케이션의 강력한 end-to-end 보안을 제공하는 제품
	시큐레터(주)	SLF	• 문서파일에 삽입 되어있는 악성코드를 리버스 엔지니어링 기술을 자동화하여 분석하는 기술
	㈜지란지교시큐리티	Content Disarm & Reconstruction	• 파일 내 실행 가능한 액티브 콘텐츠(Macro, JavaScript, Embedded Object 등)를 원천 제거하거나 비활성화한 후 안전한 파일로 재조합하는 기술
	㈜큐비트시큐리티	프루라(PLURA)	• 실시간 로그 분석과 머신러닝을 이용하여 해킹을 탐지하는 클라우드 SECaaS(Security as a Service)형 SIEM(Security Information & Event Management)

※ 유효기간은 지정서 교부일로부터 2년 유효

THE9

2026 **우수 정보보호 기술 등** (제품·서비스) **선정집**

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY