



K-SAEM

1월호

JANUARY 2025

Contact. 010 5725 0918

E-mail. ksaem@ksaem.or.kr

TABLE OF CONTENTS

01

협회 활동

K-SAEM 사업설명회

회원사 방문 상생방안 업무토의

교육원 및 연구전문기획위원회
워크숍

02

회원사 홍보 섹션

SSNC (대표 한은혜)

에이블맥스 (대표 박정혁)

퓨처시스템 (대표 정원규)

03

월간 사이버 보안 이슈

글로벌 사이버 보안 동향

국내 사이버 보안 동향

회원사 동향

04

전문자문위원 칼럼

국방혁신기술보안협회 연구원
부원장 최종환 박사

국방혁신기술보안협회 교육원
부원장 김성기 선문대학교 교수

05

협회 공지사항 및 가입 안내

협회 공지사항

회원 가입 안내



K-SAEM 사업 설명회 (1차)

행사 기본 계획

- 일시 : 2024.12.17. 13:00~19:00
- 장소 : 서울시 송파구 중대로 135 IT벤처타워 서관 3층 대강당
* 차량 이용시 해당 빌딩 공사로 혼잡하오니, 인근 경찰병원 주차장 이용(일 최대 2만명)
- 시간계획(안)

시간	내용	비고
13:00~13:15	등록 / 한담	박춘석 협회 사무총장
13:15~13:30	인사말씀	이재일 협회 연구소장
13:30~14:15	국방신속획득기술연구원 사업소개	임태현 기획조정실장
14:15~15:00	국방기술진흥연구소 사업소개	김재만 총괄팀장
15:00~15:30	휴식 / 네트워킹	커피 및 다과
15:30~16:15	정보통신기획평가원 사업소개	정현철 PM
16:15~17:00	패널 토의 / 질의 응답	박춘석 협회 사무총장
17:00~19:00	이동 / 만찬	별도 공지

- 참가비 : 인당 10만원
- 계좌번호 : 하나은행 542-910035-06404
- 참가신청 : 010-5725-0915 / 회사명, 성함, 전화번호, 이메일 문자발송



K-SAEM 사업 설명회 (2차)

행사 기본 계획

- 장소 : 서울시 송파구 중대로 135 IT 벤처타워 서관 3층 대강당
(KISA 블록체인 기업성장허브 대강당)
* 차량 이용 시 혼잡이 예상되나, 인근 경찰병영 주차장 이용(일 최대 2만명)

시간	내용	비고
13:00~13:15	등록/환담	박준석 협회사무총장
13:15~13:30	인사말씀	이재일 연구원장
13:30~14:30	민군협력진흥원 사업소개	박재현 계획관리실장
14:30~15:30	국방기술진흥연구소 방산혁신100 사업소개	황정환 파트장
15:30~16:30	한국이스라엘산업연구개발재단 사업소개	강성룡 사무총장
16:30~17:30	패널 토의 및 질의 응답	박준석 협회사무총장
17:30~20:00	이동/만찬	발표자 및 협회 연구원장

- 참가비 : 인당 10만원(회원사별 최대 참가 가능 인원 : 2명)
* 특화연구센터 회원사 : 무료(1차 사업설명회 기념부)
- 계좌번호 : 하나은행 542-910035-06404(예금주: (사)국방혁신기술조인협회)
- 참가신청 : 010-5067-6596 / 회사명, 성함, 전화번호, 이메일 문자 발송
또는 QR 스캔으로 참가 등록(=)



회원사 방문 상생방안 업무토의

아톤

- 오전10시30분 아톤회의실(여의도)
- 아톤 : 대표이사 우길수, 국방사업담당 권철우 이사 등 3명
- 연구원 : 원장 이재일, 부원장 최종환/안재건
- 협회 : 사무총장 박춘석, 운영국장 정해균, 사무국장 양용진

01.23

네비웍스

- 오후 15시 네비웍스회의실(안양)
- 네비웍스 : 대표이사 원준희, 부사장 서성만, 이사 오현철
- 교육원 : 원장 지영관 장군
- 협회 : 사무총장 박춘석, 운영국장 정해균

01.22

쿤텍

- 오전 10시 쿤텍회의실(판교)
- 쿤텍 : 대표이사 방혁중, 담당 김명준 등 3명
- 연구원 : 원장 이재일, 부원장 최종환/안재건
- 협회 : 사무총장 박춘석, 연구실장 박혁, 부센터장 정임재 제독

01.22

쿼드마이너

- 오후 16시 쿼드마이너 회의실(선릉)
- 쿼드마이너 : 대표이사 박범중, 센터장 최세호 이사 등 4명
- 연구원 : 원장 이재일, 부원장 최종환/안재건
- 협회 : 사무총장 박춘석, 운영국장 정해균

01.21

소프트캠프

- 오후 1시30분 소캠 회의실(과천)
- 소프트캠프 : 대표이사 배환국, 국방사업담당 김성학 상무 등 4명
- 연구원 : 원장 이재일, 부원장 최종환/안재건
- 협회 : 사무총장 박춘석, 운영국장 정해균

01.21

엔피코어

- 오후 3시 협회 세미나룸
- 엔피코어 : 국방사업담당 안병국 이사
- 연구원 : 원장 이재일, 부원장 최종환/안재건
- 협회 : 사무총장 박춘석, 운영국장 정해균, 연구실장 박혁

01.20

에이블맥스

- 1월13일 에이블맥스 회의실
- 에이블맥스 : 박정혁 대표 등 3명
- 연구원 : 원장 이재일, 부원장 최종환/김성기
- 협회 : 사무총장 박춘석
- 기타 : F1 시큐리티/굿모닝 아이텍 등 관계자 6명

01.13



교육원 및 연구기획전문위원회 워크숍

□ 개요

- 일시 : '25. 1.10.(금) 14:00 ~ 20:00
- 장소 : 협회 회의실(문정헤리움서밋타워 10층) / 인근식당
- 참석 인원 : 13명
 - 교육원 : 지영관 원장, 민황기·김성기 부원장
 - 연구기획전문위원회 : 이재일 위원장, 최종환·안재건 부위원장
 - 특별참석 : 박무성 ADD박사, 윤장홍 백석대 교수, 손창근 명지대 교수
 - 사무국 : 사무총장, 운영·사무국장, 연구실장

□ 토의 내용

【 교육원 】

○ 사이버보안 최고위과정

- 서울과학기술대학교와 공동주관은 대학교측과 의견 차이로 제한
- 성균관대 인공지능협회에서 공동주관 가능하다는 의견 제시로 추후 협조회의를 통해 가능 여부 판단
- 초빙강사 구성 관련, 협회의 장점인 현/예비역 장성을 추가하여 Know-how 등을 듣는 것도 좋은 생각임. 강사섭외를 조기에 완료하고 학생모집을 위해 이른 시일내 홍보팸플릿을 제작해 주기 바람.
- 학생모집이 최대 관건인 만큼, 협회 모든 인원들이 함께 노력할 수
- 교육장소는 동진빌딩(교대역, 12.5만원/1h)과 군인공제회(도곡역, 120만원/1h)를 비교한 결과, 접근성/교육여건은 비슷하나 비용 고려 동진빌딩으로 결정함.

○ 국방정보보안 전문가 교육

- 교육과정 중 단기과정에 5개 과목(RMF, CMMC, 우주항공, 국방AI, 방산기술 보호)을 편성하여 3~4월경 마련하도록 하겠음.
- 전문과정은 단기과정을 먼저 추진하고 여건을 고려하여 결정



교육원 및 연구기획전문위원회 워크숍

○ 국방정보보안 자격증

- 5개 과목을 종합하여 1개 자격증으로 추진하며, 이를 위해 협회 연구용역사업으로 추진함.
- 연구용역사업은 협회 전문가위원회인 손창근 교수가 추진함.

○ 성균관대 인공지능융합원과 협업사업(산업전문인력 AI역량 강화 지원사업)

- 협회가 주관기관으로, 인공지능융합원은 참여기관임.
- 사업 기간은 협약일부터 '25.12.31이며, 지원규모는 국비 5억원임.
- 교육방법은 온-오프라인 병행 교육이며, 리더교육(60명 이내, 최소 15시간), 재직자 교육(200명 이상, 최소 48시간), 전환교육(20명 이내, 최소 48시간)임.
- 추후 협조회의(1.24, 금)간 업무분장 등 구체적인 토의 예정

【 연구기획전문위원회 】

○ 특화연구센터 운영방안

- 특화연구센터 설립 목적에 맞는 협회, 기업간 상생
- 기업별 전담자문위원 매칭(매칭결과 아래 참조)
- 기업 성장을 위한 정보 지원(과제 관련 R&D 자료 등 제공)
→ 메일, SNS 등 활용 수시 전달
- 전문위원과 기업간 정기(2개월 단위), 수시(과제 등) 미팅 반영
- 사업 설명회 개최(국방 및 방사청 등 연계) / 3월 중
- 협회 자문위원간 정보 교류 활성화를 위한 텔레그램 개설 건의(최재운)
- 기업 매칭 자문위원에 대한 자료 공개 제한 요청
→ 기업에는 매칭 자문위원 통보하되 기업에서는 관련 사실외부에 공개 제한



회원사 홍보

SSNC 한은혜



안녕하세요. 에스에스앤씨 대표 한은혜입니다.

에스에스앤씨는 2018년 3월에 설립 이후 대기업, 금융권, 제조업 등 다양한 고객사의 고객의 요구에 부합하는 제품과 서비스를 도입하고, 이를 효율적으로 운영할 수 있도록 지원하여 정보 보호의 최전선에서 함께하고 있습니다.

다가오는 2025년에는 AI 기반 공격과 새로운 규제 요구사항 등 다양한 도전이 기다리고 있습니다. 심화되고 복잡한 위협 유형이 나타날 것으로 예상되며, 이에 따라 기업들이 사이버 공격에 대비하기 위해 사이버 보험 가입을 권장받는 사례가 증가할 것입니다. 또한, 기업을 공격하는 다양한 악성 공격 시도나 내부 데이터 유출 시도에서 발생하는 데이터를 실시간으로 분석하고, 이를 기반으로 한 공격 탐지와 방어가 가능한 MDR(Managed Detection and Response) 서비스의 중요성이 더욱 부각될 것입니다.

에스에스앤씨는 이러한 변화에 발맞추어 AI 기반 보안 운영 플랫폼을 통해 차별화된 솔루션을 제공하고, 글로벌 빅데이터·AI 기업인 Elastic과의 파트너십을 통해 SIEM 및 빅데이터 시장에도 진출할 계획입니다. 또한, MDR 서비스를 강화하여 실시간 데이터 분석과 자동화된 대응 체계를 구축함으로써 다양한 위협에 효과적으로 대응하고, 사이버 보험 관련 컨설팅 서비스를 통해 고객이 안전하게 비즈니스를 운영할 수 있는 환경을 조성할 것입니다.

이러한 에스에스앤씨만의 기술과 제품을 바탕으로 국방 보안 시장에도 적극 진출할 예정이니 많은 관심 부탁드립니다.

감사합니다.

IT보안 전문기업 / Specialized in IT Security

사이버 보안에 진심인 기업,

에스에스앤씨(주) 회사 소개

About 에스에스앤씨

Change with you, Grow with you

2018년 3월 설립, 대기업, 금융권, 제조업 등 고객사의 비즈니스 환경에 최적의 제품을 도입하고 효율적으로 운영할 수 있도록 지원하는 정보보호 전문 기업입니다. 엔드포인트부터 네트워크, 이메일, 클라우드 업무 환경까지 기업 및 기관의 소중한 데이터와 사람을 보호하며 안전하고 편리한 업무 환경을 만드는데 기여합니다.

설립연도
2018

대표이사
한은혜

기업부설연구소

벤처기업

이노비즈

여성기업

사업분야
IT솔루션

임직원수
60

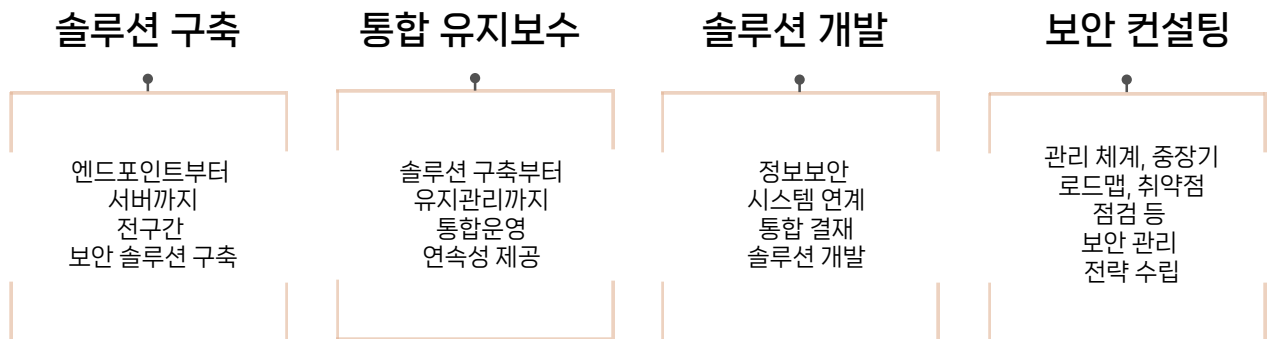
History

고객 최우선의 서비스와 18년간 쌓아온 경험을 바탕으로 다수의 프로젝트를 성공시켜 장관상 수상, 글로벌 사이버보안 전문 기업인 포스포인트 한국지사 선정 등 높은 기술력을 인정받아 오고 있습니다.

2018	2019	2020	2021
<ul style="list-style-type: none"> - 에스에스엔씨(주) 설립 - 기업 부설 연구소 설립 - 통합 PC보안 사업 진행 	<ul style="list-style-type: none"> - 중소벤처기업부장관상(기업부문) '올해의 벤처상 수상' - 웹 보안 솔루션 사업 진행 - 방화벽 운영 자동화 솔루션 사업 진행 	<ul style="list-style-type: none"> - 농협은행 방화벽 정책 자동화 시스템 구축 감사패 수상 - 정보보호 기술 개발에 대한 공모 인정 '과학기술정보통신부장관상 표창' - 포스포인트 한국지사 선정 	<ul style="list-style-type: none"> - 제54회 과학의 날 기념 2021년도 정보통신발전 유공 정부 포상 대통령 표창 수상 - 방화벽 정책 자동화 솔루션 구축 사업 - PC보안 분리사업 진행 - 이메일 보안 사업 진행
2022	2023	2024	
<ul style="list-style-type: none"> - IT서비스 혁신대상 국방부장관상 수상 - 벤처기업협회 우수벤처기업 선정 - 행정안전부 우수기업인 장관 표창 수상 - 기술혁신형중소기업(INNOBIZ) 인증 획득 	<ul style="list-style-type: none"> - 기술역량 우수기업 인증 (보안솔루션 설계 및 구축 기술) - RSAC 2023/Infosecurity Europe 참가 - 스페인/미국지사 설립 - Global Security TOP 100 선정 	<ul style="list-style-type: none"> - 벤처기업협회 정회원 - 한국정보기술연구원 표창장 수상 - 2024 Global Security Top100 선정 - 해군정보통신학교 감사장 수상 	

Business Area

네트워크 보안 솔루션과 통합 PC보안 솔루션 그리고 운영 자동화 솔루션을 주력으로 보안 컨설팅과 솔루션 구축 및 유지관리 서비스를 제공합니다.



Solutions

효율적이고 체계적인 보안 전략 수립을 위해 최적의 솔루션을 선별하여 제공합니다.



엔드포인트/이메일/클라우드

- 사이버위험 진단 솔루션: **Bitsight**
- 악성코드 차단 EDR: **SentinelOne**
- 이메일/클라우드 채널 보안: **Perception Point**
- PC보안: **ESCORT**
- 문서보안: **NASCA**
- 출력보안: **Secuprint**
- SaaS 애플리케이션 취약점 대응: **Wing Security**
- 하드웨어 계층(Layer1) 보안 시각화 및 제어: **HAC-1**



자동화

- 방화벽 정책 운영 업무 자동화 솔루션: **FPMS**
- 통합보안관리시스템: **OASIS**



Forcepoint

- 웹보안: **Web Security**
- 이메일 보안: **Email Security**
- 정보유출방지: **DLP**
- 차세대 방화벽: **NGFW**
- 클라우드 보안: **CASB**
- 내부자 위협 방지: **FIT**

Partnership

Forcepoint

SAMSUNG SDS



BITSIGHT



제품명/대상	Endpoint	Network	Web	Email	Firewall	Cloud	분석/평가	기타
Bitsight							보안수준 식별/분석, 외부공격표면관리	
SentinelOne	AI 기반 악성코드 차단/복구							
Perception Point			SaaS형 웹브라우저보안	SaaS형 이메일보안		SaaS형 클라우드 협업앱 보안		
Wing Security						SaaS앱 위협관리		
Kiteworks								컨텐츠 통신 보호
BNS					방화벽 앞단 악성공격 보호막			
FPMS					정책 자동관리/분석			
ESCORT	차단/로그/자산관리							
NASCA	문서암호화							
SecuPrint	출력물 보안							
Forcepoint	Insider Threat	잠재적 내부위협 모니터링						
	DLP	민감데이터 식별, 모니터링, 콘텐츠 검사	웹트래픽 모니터링, 콘텐츠 검사, 정책실행					
	Web Security		모든 웹 트래픽 위협 모니터링, 차단 등					
	Email Security		이메일을 통한 위협 모니터링, 차단 등					
	NGFW					차세대 방화벽		
NGFW(SECU)					차세대 방화벽			
HAC-1								숨겨진 IT자산 위협 모니터링
Lasso Security								GenAI 애플리케이션 보안
OASIS	보안 통합 결재 시스템							

Customers

에스에스앤씨의 기술력을 인정받아 금융/제조/IT 서비스 등 다수의 대형 그룹사 고객과의 긴밀한 비즈니스를 유지하고 있습니다.



외 200여개 고객사

Global Way

에스에스앤씨는 이제 든든한 팀원들과 함께 글로벌로 나아갑니다.
미국 샌프란시스코에 설립된 지사를 기반으로 더욱 더 넓은 사이버보안마켓으로 향하는 발걸음을 내딛었습니다.



IT보안 전문기업 / Specialized in IT Security

감사합니다.



카카오채널

주소 : 경기도 광명시 일직로 43 GIDC C동 11층

대표전화 : 02-6925-2550

대표메일 : sales@ssnc.co.kr

페이스북 : www.facebook.com/ssnc.co.kr

회원사 홍보

에이블맥스 박정혁



에이블맥스(주)는 『KF-21 시험비행 빅데이터를 활용한 CBM+ AI 융합 기반기술 개발』 프로젝트를 성공적으로 수행하며, CAE 기술력, 빅데이터 분석 및 처리, AI 모델 개발 등 첨단 기술을 바탕으로 CBM+ 기반 스마트 정비 시스템을 선도하는 엔지니어링 토탈 솔루션 기업입니다.

에이블맥스(주)는 23년간 CAE(Computer-Aided Engineering) 분야에서의 풍부한 경험과 전문 지식을 바탕으로, 첨단 기술을 통해 혁신을 이끌고 있습니다. 현재 우리는 CBM+ (Condition-Based Maintenance Plus) 기반의 MRO(Maintenance, Repair, and Overhaul) 사업을 확장하고 있으며, 국방 분야에서 감시정찰체계에 AI 무인화 감시시스템을 제공하는 것을 목표로 하고 있습니다.

국방사업 중 하나로는 국가 안보 강화와 효율적인 군사 작전 수행을 목적으로 육군교육사령부에서 의뢰한 지능형 해안감시체계 AI 모델 개발이 있습니다.

본 사업은 해안 감시 레이더 신호 학습으로 해안경계작전 질적 향상 및 병력 절약형 해안경계로의 작전개념 전환에 대비하기 위해 추진되었습니다. 에이블맥스는 자동화된 지능형 무인 감시 시스템을 개발함으로써 감시 체계의 운영 효율성을 극대화하면서도 인력 의존도를 낮춰 미래형 군사 작전 체계의 새로운 기준을 제시했습니다.

또한, 에이블맥스가 수행한 KF-X 비행시험 데이터베이스 구축 및 분석 사업은 대한민국의 차세대 전투기 KF-21의 개발 과정에서 비행시험 데이터를 체계적으로 수집·분석·관리하기 위해 추진된 핵심 프로젝트입니다. 비행 시험 중 수집된 온도 데이터를 자동으로 정리하고, 이를 통해 항공기의 열환경과 구조 안정성을 평가할 수 있습니다.

뿐만 아니라 비행 중 기체 구조에 가해지는 하중 데이터를 분석하여 구조적 성능을 검증하고 피로수명을 예측하였습니다. 그리고 이러한 데이터들을 활용하여 KF-21의 고장 및 이상 발생 가능성을 예측하고, 유지보수 계획을 최적화할 수 있게 지원했습니다.

이러한 사업들은 KF-X개발의 성공적인 추진과 함께, 미래 항공기 운영과 유지보수의 효율성을 극대화하는데 중요한 기반이 되었습니다.

군은 앞으로 인력 감소에 대비하여 경계와 정찰 임무를 무인 감시체계로 전환하는 추세에 있습니다. 에이블맥스는 트렌드에 발맞춰 기존의 지능형 해안 감시체계 구축 경험과 기술력을 바탕으로, 국방사업 분야에서 무인 경계, 감시, 정찰 서비스를 제공할 것입니다.

에이블맥스는 군의 미래 작전을 지원하며, 보안과 효율성, 혁신을 동시에 제공하는 솔루션을 만들어갈 것입니다.





에이블맥스(주)는 20년 이상 항공우주분야에서 전산해석 프로그램(S/W)의 공급 및 핵심 해석 기술 개발을 토대로 다양한 항공우주 시스템 개발 프로젝트에 참여하고 있습니다.

국내외 산학연과 협력하여 항공우주 및 에너지 분야에 에이블맥스 기술력의 입지를 다졌으며, 특히 Thermal Desktop은 위성 궤도 열 해석 및 극저온 유체에 특화되어 있어 항공우주연구원 및 국방과학연구소에서는 열해석의 표준 Tool로 활용되고 있습니다.

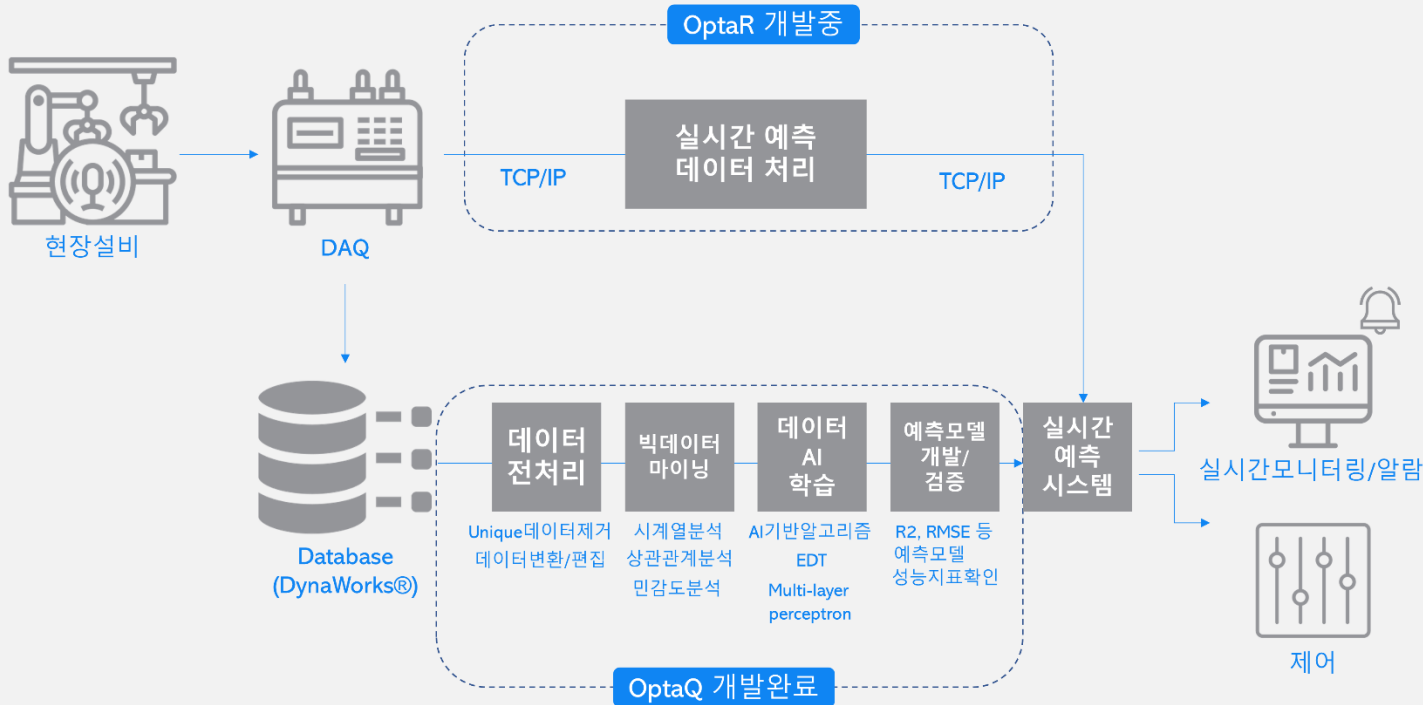
항공우주분야의 전문적인 경험을 가진 당사의 엔지니어들은 해석 및 실험, 결과분석, 문제 파악, 개선방안도출 등 고객에 필요한 맞춤 컨설팅까지 체계적으로 제공해 드립니다.

에이블맥스(주) 주요 프로젝트 수행 이력

- 한국과학기술연구원: 시험용 우주 로버 기본설계모델의 열 및 방사선 설계 해석
- 한국항공우주연구원: 지구 저궤도에서의 액체 산소 산화제 저장탱크 복사 열 유입량 도출
다단 연소 사이클 엔진 유동 Thermal Desktop제어 해석 모델링
- 한국항공우주산업: KF-X wing 금속재 구조해석 및 피로해석
- 두원중공업: 다목적실용위성 냉각 어셈블리 열 해석 및 검증
- 국방과학연구소: 유도무기 연료탱크 열유동해석
- 파이버프로: PFOG 충격시험 용역
실용위성급 광학 자이로 구조 및 열 해석 기술용역
- 한화시스템: 위성중계기 개발과제 열/구조 해석
위성 광구조체 미러 모델링

ICT (Information and Communication Technologies) 분야

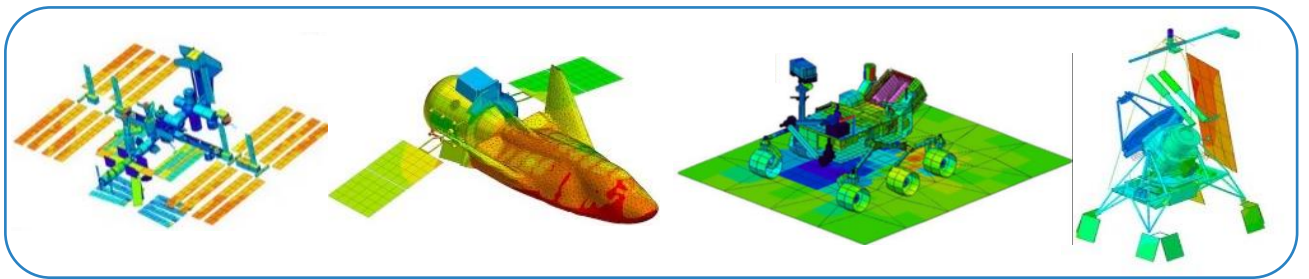
- AI 기반 데이터 분석: 다양한 조업 공정 데이터를 활용하여 데이터 마이닝, 머신러닝/딥러닝 알고리즘을 적용한 예측모델 생성/검증을 통해 조업 공정 최적화를 구현하며, 생성된 예측모델을 사용자가 사용목적에 맞게 커스터마이징을 할 수 있는 OptaQ를 개발하였습니다.



CAE (Computer Aided Engineering) 분야

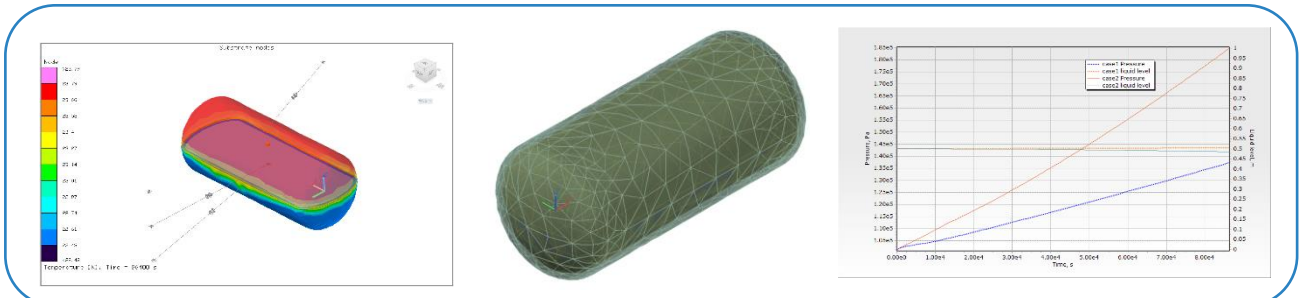
우주/위성 CAE

- 우리는 우주산업에서 우주환경 시뮬레이션을 통해 다양한 조건 하에서의 장비 성능을 예측하고, 최적의 설계 솔루션을 제공하고 있습니다.
- 이를 통해 우주 임무의 성공 가능성을 높이고, 비용 효율성을 극대화합니다.



수소에너지 BOG 해석

- 우리는 수소에너지 분야에서 BOG(Boil-Off Gas) 관련 해석을 통해 에너지 손실을 최소화하고, 안전성을 극대화하는 데 기여하고 있습니다.



회원사 홍보

퓨처시스템 정원규



K-SAEM 회원 여러분께
퓨처시스템의 대표이사 정원규 인사드립니다.

퓨처시스템은 대한민국 VPN 및 암호화 기술의 선구자이자 부동의 1위 기업으로, 30년 이상의 축적된 노하우와 최첨단 기술로 고객의 디지털 자산을 지키는 든든한 파트너입니다. 방화벽 (Firewall), VPN, 통합 보안 관리 시스템 등 다양한 솔루션을 고객 환경에 최적화해 제공하며, 보안 리더로서의 입지를 견고히 하고 있습니다.

미래를 선도하는 혁신 전략

퓨처시스템은 양자 컴퓨팅 시대를 대비하여 차세대 암호 기술을 선도하고, RSA 등 기존 암호 체계의 취약성을 보완하는 양자내성암호(PQC) 기반 양자VPN 솔루션을 제공하고 있습니다. 또한, 검증된 온프레미스 보안 기술을 클라우드 시장으로 확장하며, 주요 CSP(Cloud Service Provider)와 협력을 강화해 클라우드 환경에서도 신뢰할 수 있는 보안 서비스를 제공합니다.

기존 암호체계의 한계와 양자VPN의 필요성

기술의 발전과 함께 RSA와 같은 기존 공개키 암호 시스템은 양자 컴퓨팅의 강력한 연산 능력 앞에서 한계를 보이고 있습니다. HNDL(Harvest Now, Decrypt Later) 공격은 데이터를 미리 수집하고 해독할 미래의 위협을 예고합니다. 이에 따라 퓨처시스템은 양자내성암호(PQC) 기술로 데이터의 기밀성과 무결성을 보장합니다.

지속 가능한 성장과 리더십

퓨처시스템은 고객의 신뢰를 기반으로 국내 보안 시장의 리더십을 이어가며, 혁신적인 보안 솔루션으로 고객사의 디지털 자산을 안전하게 지켜드리고 있습니다.

감사합니다.

Future Systems 회사소개

“시통합보안·양자암호보안의 차세대 리더”

WE DO GUARD YOUR
INVALUABLE ASSETS!

(주)퓨처시스템

2024.10

대표이사 정원규, wkchong@future.co.kr

FutureSystems

COPYRIGHT © ALL RIGHTS RESERVED BY FutureSystems

목 차

CONTENTS

FutureSystems



1. 회사개요
2. 비즈니스 및 기술
3. 제품소개
4. 비즈니스 전략

01 안정성·고성능 제품으로 기술경쟁력 강화로
네트워크 보안 시장 최다 고객 보유

02 선도적인 PQC기반 양자VPN 출시로
국가 주요 정보망 보안 강화 사업 선도 기업

FutureSystems

“SI 통합보안 · 양자 암호 보안의 차세대 리더”

회 사 명	주식회사 퓨처시스템(FutureSystems, Inc.)
대 표 이 사	정 원 규
자 본 금	8.9억원
매 출 액	182억원(23년도), 162억원(22년도)
사 업 분 야	네트워크보안 제품 제조 및 판매, 정보보호 서비스
설 립 일	1987년 11월 18일(2007년 05월 01일 (주)나노엔텍 물적 분할)
임 직 원 수	68명
지 적 재 산	특허(등록10, 출원2) 등 다수
국가용 암호장비 단일 제작업체 선정(국가보안연구소)	


회사의 핵심 가치	
비전	최고의 연구개발로 인건을 위한 보안기술 제공
미션	<ul style="list-style-type: none"> 믿음과 신뢰를 바탕으로 고객의 정보자산 보호 벤처 정신으로 세계 정보보호 산업 선도
핵심 가치	<ul style="list-style-type: none"> People 인간 중심의 경영 실현 Technology 기술로 승부하는 기업 Venture 진정한 벤처 기업 Collaboration 소통과 협력

- WeGuardia™ XTM (가상사설망, 네트워크 방화벽, 통합보안솔루션)
- WeGuardia™ ITU (차세대 네트워크 보안플랫폼) - 신제품(2022.06 CC인증 획득)
- WeGuardia™ SMC (통합보안관리시스템)
- Future's SoC (위협 관제 서비스)
- WeGuardia™ SDPFW (제로트러스트 FW) - CC인증 획득
- WeGuardia™ ETD (암호위협 비복호화탐지시스템)
- WeGuardia™ NDR (SI기반 네트워크 탐지 대응시스템-위협헌팅시스템)
- WeGuardia™ X-ITM (NDR솔루션, 관제서비스) - '25년 1분기 내 출시 예정
- WeGuardia™ AI UTM (안공지능 UTM) - '25년 2분기 내 출시 예정

“ 퓨처시스템은 1987년 설립하여 국내 네트워크 보안업계 1세대 기업으로서 국내 대표 보안기업으로 성장하고 있습니다. 자체 개발한 차세대방화벽, VPN, UTM, 침입방지시스템, 무선침입방지시스템, 망연계 솔루션 등 유·무선 네트워크 보안 제품과 보안 관제 및 분석 서비스를 통해 네트워크 통합 보안 솔루션을 제공하여 Security Convergence를 구현하고 있습니다. ”

FutureSystems

차세대보안 전문기업

SI통합보안	양자암호보안
 대한민국의 네트워크 보안의 명가 (주)퓨처시스템	<ul style="list-style-type: none"> 양자내성암호(PQC) Q-VPN “국내최초” SDP FW “CC인증” SI기반 암호위협 비복호화 탐지시스템 SI기반 NDR(위협헌팅) LLM기반 보안플랫폼

표창장

미래창조과학부 장관

우수상

지식경제부장관

주요 특허
등록 10, 출원 2

특허증

특허번호: 10-1109874

발명: 다중 프로세싱 시스템 및 그 방법

출원번호: 10-2012-00123

특허청장: 김희정

인정서

소프트웨어용역인증서

인증번호: 2019-00123

발급처: 한국인터넷진흥원

- 비대칭 다중 프로세싱 시스템 및 그 방법(특허등록번호 10-0807039)
- 고성능 UTM장비를 위한 다중 프로세싱 시스템 및 그 방법(특허등록번호 10-1109874)
- 플로우 프로세싱 유닛 및 플로우 프로세싱 유닛 제어 방법(특허등록번호 10-115098)
- 네트워크 보안 장치의 이슈 추적 시스템 및 방법(특허등록번호 10-1485732)
- 네트워크 보안 장치의 이상 징후 판단 시스템 및 방법(특허등록번호 10-1490649)
- SSL로 암호화된 패킷을 캡처하여 분석하는 장치 및 방법(특허등록번호 10-1663401)
- 침입차단시스템에서 보호 네트워크에 접속 시 외부 네트워크와의 접속 차단 방법(특허등록번호 10-1673561)
- 사물 인터넷을 위한 사물기기 제어 시스템과 가상화 사물 서버에서 실행되는 사물기기 제어방법(등록번호 10-1683470)
- 단방향 데이터 전송 시스템 및 그 방법(특허등록번호 10-1692670)
- 전송장치 이원화에 의한 TCP/IP 망단절형 단방향 접속 시스템 및 그 방법(특허등록번호 10-1692672)
- 자동 스코어링 시스템 기반의 보안 이벤트 자동 처리 시스템 - 출원중
- LLM의 환각제거 자동화를 통한 보안 지원 업무(코파일럿) 시스템 - 출원중

인증서

WeGuardia™ ITU

CC 인증

인증서

WeGuardia™ SMC

CC 인증

인증서

WeGuardia™ ITM

CC 인증

인증서

WeGuardia™ FW

CC 인증

“ 날로 지능화 되고 진화하는 보안 위협에 선제적으로 대응하고 **믿음과 신뢰를 바탕으로** 고객의 소중한 정보자산을 최우선으로 보호하는 것을 사명으로 국내 보안업계에서 지난 역사에서 한 축을 담당해왔습니다. 퓨처시스템은 벤처정신으로 지속적인 연구개발로 **세계 정보보호 산업을 선도하는 강한 기업으로 성장하겠습니다.** ”

회사의 발자취

- 2017 - 현재**
 - 법인화생절차 신청(서울화생법원)(2017.05)
 - 법인화생절차 조기 종결(2018.03)
 - 융합솔루션 개발 완료 및 '23년 11월 4일 CC인증 획득(SDP FW (ITU z_series))
 - 인공지능 기반 암호위협 비복호화 탐지시스템 출시
 - 인공지능 기반의 NDR출시
 - 양자내성암호(PQC) Q-VPN 개발 완료 및 하이브리드방식 출시(양자암호통신장비)
 - 융합솔루션 X-ITM 출시 예정('25.1Q) (XDR 솔루션, 분석솔루션)
 - 융합솔루션 AI-UTM 출시 예정 ('25.1Q)
- 2010 - 2016**
 - WeGuardia™ SSLplus CC인증, GS인증 획득
 - WeGuardia™ NFW / WIPS CC인증 획득
 - WeGuardia™ T-MOVER CC인증, GS인증 획득
 - WeGuardia™ ZEN CC, GS인증 인증획득
 - 서울시 일자리 창출 우수기업 수상
 - 기술보증기금 투자유치
 - 산업은행 투자유치
 - Hi-Tech Awards 경영 대상 수상
 - ICT Innovation **미래창조과학부 장관상** 수상
 - 벤처활성화유공포상 **국무총리 표창**
 - 벤처산업활성화 **경기도지사 표창**
- 2000 - 2009**
 - IR42 **장영실상 수상** (과학기술부)
 - 조달청 우수 제품 선정
 - 우수벤처 발굴대회 산업자원부 장관상 수상
 - **재경부 비공개암호알고리즘(BUD-F) 적용 보안장비인증 획득**
 - 퓨처 IPS 통합보안솔루션 출시
 - 국제 IPv6포럼 "IPv5 Ready Logo" 획득
 - FutureUTM 통합보안솔루션 시리즈 출시
 - ISO 9001:2000 / KS A 9001:2001 인증 획득
 - WeGuardia™ XTM / SMC CC 인증, GS인증 획득
 - WeGuardia™ FW / DDoS CC 인증 획득
 - 대한민국 기술대상 지식경제부 장관상 수상
- 1987 - 1999**
 - **퓨처시스템 설립**(1987.11.18, 자본금 5천만원)
 - 부설 정보통신연구소 설립
 - Future/TCP 국산 신기술인증마크(KT마크) 획득
 - **벤처기업대상 (대통령 표창) 수상**
 - **정보문화기술상 (국무총리상) 수상 / 벤처기업상 수상**
 - **NIST AES 미국 차세대 후보 표준 암호 알고리즘으로 선정 (미국상무성)**

“ 40년 기술력과 혁신으로 통합 보안의 미래를 이끄는 업계 **선두 기업!**
완벽한 혁신적 보안 기술로 매년 견실한 성장을 이어가는 통합보안 **선도 기업!**
안전한 통신환경의 제공을 위하여 꾸준한 성장을 기반으로 신기술의 연구개발에 최선을 다하고 있습니다. ”

110억원('20년), 121억원 ('21년), 162억원 ('22년), 182억원('23년) (최근 6년 CAGR 25.5%)

정부 및 공공기관, 금융사, 국방부에 생산 납품(약 1,500여 고객에 약 90,000여대)

국내 정보보안시장에서 최근 4년간 견실한 매출 성장 실현

- SI 통합보안을 위하여 SI전문기업인 (주)시플랫폼과 독점계약하여 관련 제품을 공동개발
- 양자암호분야는 하이브리드형태로 출시

신기술(SI, 양자암호) 시장의 차세대 리더



- 클라우드 환경에서 최적화된 클라우드VPN 출시
- 기존의 서비스 대비 고객의 사용환경에 최적인 솔루션을 제공해줌

클라우드 환경에서 최적의 SeCaaS

등종업계 최고의 개발력

- 정보통신연구소(1992년 설립)
- 10건의 정보보안 관련 특허 보유
- 40여년간의 기술개발 및 제품 사업화 노하우 보유 및 장기 근속 연구개발진

국내 네트워크 보안 업계 1세대

- 40여년 동안 정보보안장비 분야의 다양한 기술을 축적한 국내 VPN 누적 점유율 1위 기업
- 네트워크보안 장비에서 국내 최초 하드웨어 전용 장비화 시작

통합정보보안기업

- 국내 네트워크 보안 업계 1세대 기업
- 엔트포인트단 장비에서 관리툴까지 보유하는 등 통합정보보안기업으로 변화

“ 정보보안제품의 유용성과 잠재적 수요가 폭발적으로 증가될 것으로 예상되어지는 차세대 기술을
발 빠른 기술 개발로 최신 AI 보안과 양자암호통신기술 보유기업으로 **차세대 정보보안시장 리더**로 성장하겠습니다.
엔드포인트장비부터 관리 툴까지 보안 솔루션을 제공하여 **통합보안전문업체**로 거듭나는 퓨처시스템이 되도록 하겠습니다. ”

01 AI 통합보안플랫폼(UTM)

신제품
예정

- AI 엔진 적용으로 End-Point 및 다양한 네트워크 인프라에 적용 가능
- 생성형 AI 와 LLM(Large Language Model) 접목시킨 보안플랫폼
- AI는 방대한 양의 데이터를 수집하고, 분석하고, 추출된 인사이트를 기반으로 위협을 탐지하고 대응하는데 이상적이며 보다 강력하고 지능적인 보안 솔루션을 제공



02 양자암호전송장비(Q-VPN)

신제품
출시

양자 암호화(통신) 기술 = 해킹 원천봉쇄

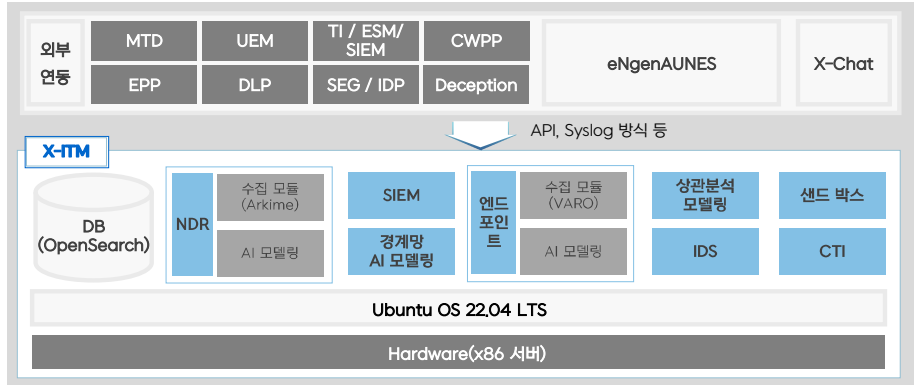
- 양자컴퓨터는 높은 연산 속도로 기존의 암호화 방법을 무력화
- 기존 RSA(Rivest Shamir Adleman, 소인수분해를 이용한 알고리즘) 기반 암호키는 슈퍼컴퓨터로도 엄청난 시간을 필요 하였으나 양자컴퓨터로 1초 만에 해킹 가능



03 통합보안관리툴(TMS)

출시 예정

- 빅데이터 기반의 대용량 로그 수집, 분석, 모니터링
- Intelligence 기반의 로그관리
- AI, 머신러닝 기반 분석을 통한 정확성 높은 분석
- 보안시스템 관리에 필요한 시간 및 비용을 줄여주며, 복합적인 위협으로부터 탁월한 보호기능을 제공하는 중앙집중식 통합보안관리
- LLM을 활용한 대응절차의 자동화 지원



“ 퓨처시스템의 네트워크보안제품군은 멀티코어 기반 고성능 통합보안 솔루션으로
멀티코어 환경에 최적인 하이브리드형 소프트웨어 프레임워크를 자체 개발해 통합 보안장비 성능 한계를 극복했으며,
국내 최초 IPv6 및 10Gbps 인터페이스를 탑재해 국정원 CC인증을 획득한 통합 보안 솔루션입니다.
ITU와 ITM 제품군은 기존 노후화된 제품군을 단종하고, 최신의 보안기술을 적용하여 업그레이드한 버전으로 최근 런칭하였습니다. ”

01 차세대 통합위협관리 솔루션

2023.2Q출시

WeGuardia™ ITU

특장점

- FW + VPN + IPS
- SDP기능, PQC (양자암호통신)
- Anti-Spam과 Anti-Virus 기능
- 기존 행안망 100% 연동

용도 및 주요 납품처

- 국가정보통신망 구간간 VPN장비(전국 지자체 행안망)
- 티머니, 한국 가스 공사, 농협네트웍스

02 차세대 통합보안관리 솔루션

2023.1Q출시

WeGuardia™ ITM

특장점

- 당사 보안 제품 원격 통합 관리 가능
- 사이버 보안 위협 분석을 위한 TI DB 탑재
- 개방형 SW 기반으로 Cloud 운영 지원 체계 수립

용도 및 주요 납품처

- 국가정보통신망 구간간 VPN장비(전국 지자체 행안망)
- 농협은행 외 365, 광주은행, 한국은행 등

03 통합위협관리 솔루션

WeGuardia™ XTM/FW

특장점

- 국내 VPN 시장 누적율 1위
- 국내 최초 IPv6 지원
- IPSec, SSL, Mobile VPN 지원
- 다차원 트래픽 통계 및 추적

용도 및 주요 납품처

- 국가정보통신망 구간간 VPN장비(전국 지자체 행안망)
- 농협은행 외 365, 광주은행, 한국은행 등

04 통합보안관리 솔루션

WeGuardia™ SMC

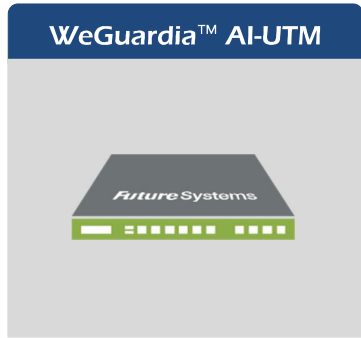
특장점

- Micro Service Architecture 구조 설계(모듈화 및 확장성)
- 고효율 로그처리 엔진 탑재
- All-In-One 중앙 통합관리 운영

용도 및 주요 납품처

- 국가정보통신망 구간간 VPN장비(전국 지자체 행안망)
- 농협은행 외 365, 광주은행, 한국은행 등

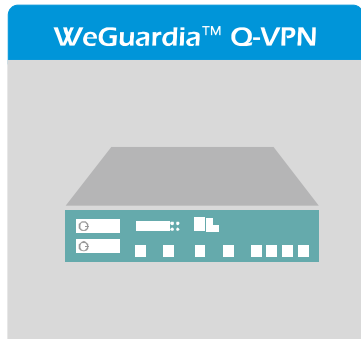




> AI 통합보안플랫폼(UTM)

- AI 엔진 적용으로 End-Point 및 다양한 네트워크 인프라에 적용 가능
- AI 보안 전문기업 JSI.LAB 과 독점계약하에 공동개발 진행

정밀성	정확성	보안성
<ul style="list-style-type: none"> SI를 활용해 보안위협 분석 업무를 자동화 처리 기업의 오피레미스 네트워크에서 지능형위협을 실시간으로 정밀하게 판별 탐지율 99% 목표 	<ul style="list-style-type: none"> 기존기술은 변종 및 APT, 제로데이 등 탐지가 쉽지 않음 인공지능 적용으로 분석 회피 등의 악성코드를 신속하고 높은 정확도로 탐지 가능 	<ul style="list-style-type: none"> 자사의 VPN이나 FW 등 네트워크 보안 기능 기본 악성코드 유포자나 해커 IP/URL과 같은 실시간 위협 빅데이터를 제공 보안성의 강화



> 양자암호전송장비(Q-VPN)

- 양자 암호화(통신) 기술 = 해킹 원천봉쇄**
- 양자컴퓨터는 높은 연산 속도로 기존의 암호화 방법을 무력화
- 기존 RSA(Rivest Shamir Adleman, 소인수분해를 이용한 알고리즘) 기반 암호키는 슈퍼컴퓨터로도 엄청난 시간을 필요 하였으나, 양자컴퓨터로 1초 만에 해킹 가능
- ※ 2023.12 자체 기술력으로 개발 완료, 조달청 등록 준비중

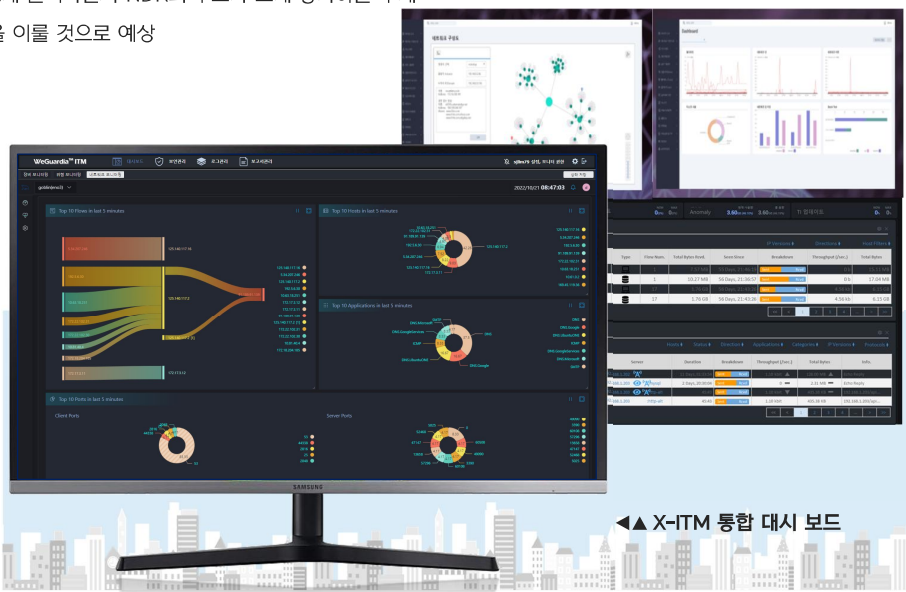
기술성	단일구현	보안성
<ul style="list-style-type: none"> 양자암호 단말 없이 양자암호통신 기술을 구현할 수 있는 '양자 하이브리드' 기술 적용 PQC는 수학 알고리즘 기반의 복잡한 암호를 활용하는 양자암호 기술 PQC 기술의 양자내성암호 톨 키를 Q-VPN 장비에 포팅 	<ul style="list-style-type: none"> 기존 양자난수생성칩셋(QRNG)을 탑재한 양자보안 장비는 별도의 양자통신단말이 있어야만 양자보안통신을 사용할 수 있음 'Q-VPN' 은 전용 단말 없이도 장비간 양자암호통신 구현이 가능 	<ul style="list-style-type: none"> PQC는 수학 알고리즘 기반의 복잡한 암호를 활용하는 양자암호 기술로, 송신부와 수신부만 해독해 암호 키를 만드는 양자키분배기(QKD) 보다 더욱 높은 보안성을 가지고 있음

네트워크위협탐지대응솔루션 WeGuardia™ X-ITM(NDR)

- NDR : 네트워크 트래픽을 모두 분석해 비정상적인 동작을 탐지하는 솔루션
- EDR, NAC, 방화벽, AD, SIEM/SOAR 등 다른 솔루션과 통합하여 사전에 적절한 위협 대응 가능
- NDR은 SIEM에 비해 쉽게 도입·운영할 수 있으며, IoT·OT 등 관리되지 않은 기기가 많은 클라우드 환경에서 EDR을 보완할 수 있는 솔루션으로 인정
- 방화벽, IPS, 네트워크 샌드박스로 탐지할 수 없는 위협이 크게 늘어나면서 NDR의 수요가 크게 증가하는 추세
- 가트너는 NDR 시장이 2026년까지 연평균 14.1%의 성장을 이룰 것으로 예상

상대적으로 효과적·효율적인 NDR

- 대기업은 더 많은 자동화 기능을 통해 보안위협 탐지와 대응을 효과적으로 하고자 하는 Needs가 있음
- SIEM·SOAR는 구축기간이 길고 비용이 높음
- NDR은 상대적으로 효과적이며, 효율적이기도 하며 구축비용을 최소화 할 수 있음
- NDR은
 - SI를 이용해 대응 우선순위 설정
 - 적절한 대응방안 제공
 - 리소스가 충분하지 않은 중소·중견기업에 효과적



◀ X-ITM 통합 대시 보드

“ 퓨처시스템은 다양한 R&D를 통해 국내 최고 수준의 암호화와 VPN기술력을 바탕으로 VPN부분 국내 1위, 국내 최초 양자암호VPN 출시 등 국가적 원천기술 확보와 신기술을 개발하여 고객의 니즈를 충족하여 지속적인 성장을 이어가면서 의미 있는 성과를 이루고 있습니다. ”

**인공지능
보안**



- AI 통합보안플랫폼(UTM)
 - AI 엔진 적용
 - 보안위협분석 업무의 자동화

※차세대 제품: 개발 완료

**네트워크
보안**



- 통합보안 솔루션
 - 방화벽, VPN, IPS 등
 - ZTNA 기술 적용
- 고성능 제품으로 시장 지배력 확대
 - 전국 지자체 행안망(국가정보통신망)
 - 금감원/금결원, 한은, 농협 등 1금융권

**양자암호
보안**



- PQC(양자내성암호)를 이용한 양자암호통신장비
 - Q-VPN
 - 해킹원천봉쇄

※차세대 제품: 개발 완료

**인공지능
기반 보안군**



- 암호위협 비복호화탐지
 - 하이퍼메타 특성의 학습으로 암호위협을 복호화하지 않고 위협을 탐지 하는 기술 적용
- NDR
 - 위협에 대한 헌팅 및 감사 기술적용

**보안위협
분석서비스**



- AI한국형 차세대 관제플랫폼 구축
 - 사이버 위협관리 정보보호 컨설팅
 - 북한,중국,러시아 공격정보 제공

※ 정부 국책 탐색 개발 부문 : AI/LLM 국책연구, 100G VPN 국책연구, 400Gb 성능 방화벽(경쟁업계 최고100G성능 대비)
 ※ 기타사업분야 : 차세대 통합보안관리 솔루션, 고객맞춤형 보안컨설팅 및 보안서비스

감사합니다.

글로벌 사이버 보안 동향

- 랜섬웨어 공격의 지속적인 증가
 - 2024년에는 랜섬웨어 공격이 지속적으로 증가하여, 인도네시아 국가 데이터센터 마비와 같은 심각한 피해 사례가 발생하였습니다.
 - 출처: 보안뉴스
- 북한의 사이버 공격 활동 강화
 - 북한은 대법원 전산망과 보건복지부 SNS 해킹 등 다양한 사이버 공격을 통해 공공기관을 대상으로 한 위협을 강화하였습니다.
 - 출처: 보안뉴스
- AI 기술을 악용한 사이버 공격의 증가
 - AI 기술의 발전과 함께 이를 악용한 사이버 공격이 심화되어, 해커뿐만 아니라 일반인도 AI를 활용한 공격을 시도하는 사례가 늘어났습니다.
 - 출처: SK실더스
- 공급망 공격의 증가
 - 국가 지원 사이버 공격으로 인한 공급망 공격이 증가하여, 기업과 기관의 보안에 새로운 위협으로 부상하였습니다.
 - 출처: 이글루코퍼레이션
- 유럽연합의 사이버 복원력법(CRA) 시행 발표
 - 유럽연합은 커넥티드 기기 제조사에 사이버 보안 의무를 부과하는 사이버 복원력법(CRA)을 시행한다고 발표하였습니다.
 - 출처: 글로벌 ICT



글로벌 사이버 보안 동향

- AI·6G 기술을 악용한 사이버 공격의 증가
 - 2024년 12월 말, 미국의 주요 통신사들이 중국 해커로 추정되는 정교한 사이버 공격을 받아, AI와 6G 기술을 악용한 새로운 형태의 위협이 부각되었습니다.
 - 출처: 지티티코리아
- 국제 행사 연계 사이버 위협 증가
 - 2024년 8월과 9월 사이, 프랑스 파리 올림픽 등 국제 행사를 노린 사이버 보안 사고가 급증하였습니다.
 - 출처: 안랩
- 사이버 보안 인력 부족 문제 심화
 - 전 세계적으로 사이버 보안 인력의 부족이 심화되어, 기업과 기관의 보안 대응 능력에 어려움을 겪고 있습니다.
 - 출처: 보안뉴스
- 클라우드 환경을 노린 사이버 공격 증가
 - 클라우드 서비스의 확산과 함께 이를 노린 사이버 공격이 증가하여, 기업의 데이터 보안에 새로운 위협이 되고 있습니다.
 - 출처: 구글 클라우드
- 사이버 보안 규제 및 정책 강화
 - 각국 정부는 사이버 보안 위협에 대응하기 위해 관련 규제와 정책을 강화하고 있으며, 기업들은 이에 대한 대비가 필요합니다.
 - 출처: 글로벌 ICT



국내 사이버 보안 동향

- 금융권 대상 악성코드 및 피싱 공격 증가

- 국내외 금융 기관을 대상으로 한 악성코드 유포와 피싱 사례가 늘어났습니다. 특히 텔레그램을 통한 계정 정보 유출이 문제로 대두되었습니다.

- 출처: ASEC



- 생성형 AI 관련 보안 위협 부상

- 생성형 AI의 발전으로 피싱, 딥페이크, 해킹 등 새로운 형태의 사이버 범죄가 증가할 것으로 예상되며, 이에 대한 대응 방안 마련이 강조되었습니다.

- 출처: 조선비즈



- 제로 트러스트 보안 체계 확산

- '제로 트러스트' 보안 모델이 보안의 필수 요소로 자리 잡으며, 관련 기술과 정책의 도입이 활발해졌습니다.

- 출처: 뉴시스



- 클라우드 및 AI 보안 강화 필요성 대두

- 클라우드와 AI 기술의 발전에 따라 이에 대한 보안 위협이 증가하고 있으며, 이에 대한 대비가 필요하다는 전망이 제시되었습니다.

- 출처: 데일리시큐

- 사이버 공격의 고도화와 보안 R&D 예산 삭감 우려

- 사이버 공격이 더욱 정교해지고 있는 반면, 보안 연구개발 예산이 삭감되어 대응 능력 저하에 대한 우려가 제기되었습니다.

- 출처: 조선비즈



국내 사이버 보안 동향

- KISA 사이버보안 성과 발표회 개최
 - 한국인터넷진흥원(KISA)은 사이버보안 성과 발표회를 통해 보안 정책, 침해 대응, 개인정보 보호 등 다양한 주제를 다루었습니다.
 - 출처: KISA



- 랜섬웨어 공격의 정교화 및 다중 갈취 전술 확산
 - 랜섬웨어 공격이 더욱 정교해지고, 이중 및 삼중 갈취 전술이 표준으로 자리 잡았습니다.
 - 출처: 안랩



- AI 대중화에 따른 새로운 사이버 공격 시도 발견
 - AI와 거대언어모델(LLM)의 대중화로 이를 노린 새로운 형태의 사이버 공격 시도가 처음으로 발견되었습니다.
 - 출처: IT조선



- 보안 인재 양성 및 확보 노력 강화
 - 사이버 보안 인재의 중요성이 부각되면서, 보안 인재 발굴과 양성을 위한 다양한 프로그램과 노력이 강화되었습니다.
 - 출처: 국민대학교 정보통신처



- 사이버 보안 산업의 성장과 발전
 - 국내 사이버 보안 산업이 지속적으로 성장하고 있으며, 새로운 기술과 솔루션의 개발이 활발하게 이루어지고 있습니다.
 - 출처: 보안뉴스



회원사 동향

■ 아톤, 양자컴퓨터 테마로 주목... 차세대 보안 기술과 재무 안정성 기대

아톤이 양자컴퓨터 관련 이슈와 맞물리며 시장의 주목을 받고 있다. 지난해 12월 초 4,000원대였던 아톤의 주가는 올해 초 한때 9,000원대에 근접하며 급등세를 기록했다.

업계는 주가 상승의 배경으로 미국 국제전자제품박람회(CES 2025)에서 양자컴퓨팅 부문이 신설된 점을 꼽고 있다.

아톤은 핀테크 보안 솔루션 및 인증 서비스를 주력으로 하는 기업으로, 양자내성암호화 기술을 활용한 디지털 서명 알고리즘을 개발해 올해 1분기 출시를 예고한 상태다. 이 기술은 양자컴퓨터 시대에도 대응 가능한 차세대 보안 기술로 평가받으며, 아톤의 성장 동력을 강화할 전망이다.

아톤의 1월 17일 금요일 장 마감 기준 주가는 6,540원이었으나, 1월 24일 금요일 장 마감 기준으로 6,140원으로 약 6.12% 하락했다. 양자컴퓨터 테마로 급등했던 주가가 단기적으로 조정을 받은 모습이다.

한편, 아톤은 지난해 7월 약 42억 원 규모의 전환사채(CB)에 대한 콜옵션을 행사하며 재무 구조 개선에 나섰다. 해당 CB의 처리 방안에 대해 시장의 관심이 집중되고 있으며, 소각 가능성도 거론되고 있다.

아톤은 메자닌 채무 부담을 크게 줄이며 재무건전성을 강화하고 있다. 또한, 양자컴퓨터 시대를 대비한 혁신적인 보안 기술 개발로 시장에서의 입지를 더욱 견고히 다질 것으로 기대된다.

업계 관계자는 "아톤은 양자컴퓨터 테마로 주목받고 있는 기업 중 하나로, 기술력과 재무 안정성을 기반으로 한 지속적인 성장이 기대된다"고 평가했다.

양자컴퓨터 시대의 도래와 함께 아톤의 보안 기술이 주목받는 가운데, 향후 시장에서의 행보에 투자자들의 관심이 쏠리고 있다.

출처 : 스타데일리뉴스



회원사 동향

■ SGA솔루션즈 최영철 대표, “제로트러스트, 민간에서 실제 사업화가 돼야”

지난해 12월 제로트러스트 가이드라인 2.0이 발표되면서 보안 업계도 제로트러스트 경쟁이 본격화될 전망이다. 이러한 상황에 보안 업계는 연초부터 안팎으로 분주하다. 조직개편 단행과 외부 전문가 영입, 사업전략에 집중하는 분위기다.

그중 SGA솔루션즈는 국내 제로트러스트 시장 선점을 위해 일찌감치 기반 다지기에 나섰다. 지난해 12월 과학기술정보통신부와 한국인터넷진흥원이 발표한 제로트러스트 가이드라인 2.0 집필에 SGA솔루션즈 최영철 대표가 참여했다. 또한 과학기술정보통신부와 한국인터넷진흥원의 제로트러스트 시범사업에 SGA솔루션즈가 주관사로 참여, 컨소시엄을 구성해 공공기관 업무망에 최적화된 클라우드 기반 서비스형 제로트러스트 보안모델을 구축하고 운영했다.

국내 제로트러스트 확산을 위해 제로트러스트 전문가도 영입했다. 디지털플랫폼 정부위원회에서 ZERO-TRUST 및 공급망 보안 전문위원인 '김광훈 전무'를 영입했다.

흩어져 있던 계열사와 관계사도 하나로 모았다. △에스지에이홀딩스 △에스지에이시스템즈 △에스지에이솔루션즈 △에스지에이이피에스 △에스지에이퓨처스 △에스지엔 △보이스아이 기업을 경기도 의왕시에 소재한 950평 규모의 에스지에이 그룹사 사옥으로 이전했다.

계열사 간 비즈니스 연계 및 통합 IT 용.복합을 지향하며, 제로트러스트 풀스택 기업으로 자리매김해 시너지를 내겠다는 전략이다. 이를 기반으로 네트워크 분야를 비롯한 다양한 국내 보안기업과 상생 협업을 통해 제로트러스트 저변 확대에 심혈을 기울이겠다는 것. 특히 최신 보안위협 증가와 정책, 시장 변화에 따라 정보보호 수요가 증대됨에 따라 통합 IT 보안기업으로 박차를 다하겠다는 계획이다.

SGA솔루션즈는 제로트러스트 아키텍처 솔루션 'SGA ZTA'를 제공하고 있다. 디지털 대전환 시대에 맞는 새로운 보안 패러다임에 맞춰 FULL-STACK ZTA 보안 솔루션을 제공하고 있다. ZTA는 어느 것도 신뢰하지 않는다는 기본 원칙하에 △인증 △지속적 디바이스 검증 △동적 정책 적용 등의 관점으로 보호하는 제로트러스트 보안 솔루션이다.

인증은 리소스에 접근하는 사용자에게 대한 신원인증(MFA)이 적용된다. 지속적인 디바이스 검증은 UEM을 통한 지속적 통합 디바이스 보안 상태를 확인한다. 동적 정책 적용은 위협 인텔리전스 피드, SIEM, 보안 시각화를 통한 보안 정책을 지원한다. 또한 최소권한, 동적 접근제어 관리 등 제로트러스트에 기반해 통합 정책관리를 지원한다.

올해 의미있는 성과에 대해 SGA솔루션즈 재무기획실 박진선 상무이사는 “안정적인 재무구조와 2년 연속 주식배당으로 ESG 경영 측면에서 주주환원 정책은 더욱 의미가 있다”며 “안정적인 재무구조에 신규사업인 제로트러스트 아키텍처 솔루션 사업으로 도약하겠다”고 밝혔다.

최영철 대표는 “지난해 제로트러스트 시범사업과 2022년 제로트러스트 4개년 과제도 잘 마무리됐다”며 “처음 나왔던 제로트러스트 사업이라 의미가 큰 만큼 이제 민간에서 실제 사업화가 돼야 한다”고 강조했다.

출처 : 보안뉴스



회원사 동향

■ 조은아이앤에스, '국방 차세대 비밀관리시스템' 사업 성공적 완료

비밀 문서작업을 보안에 대한 걱정 없이 누구나 쉽고 간편하게 수행할 수 있는 시스템이 개발됐다.

조은아이앤에스는 2023년 7월부터 지난해 9월까지 국방부 실험사업의 일환으로 수행한 '국방 차세대 비밀관리시스템' 사업을 성공적으로 완료했다고 최근 밝혔다.

비밀관리시스템이란 정부·공공 기관이 수기식으로 수행하던 비밀 관련 일체의 업무를 ICT 신기술을 적용해 전산화한 시스템을 말한다.

조은아이앤에스는 이번 사업에서 2009년에 최초 도입해 운영 중이던 1세대 비밀관리시스템의 사용자 애로 및 개선사항을 적극적으로 발굴해 적용함으로써 사용자 만족도를 향상시켰다.

특히 실제 서버 단말기를 사용하는 방식인 RDI(REAL DESKTOP INFRASTRUCTURE), 암호화를 위한 오픈소스 운영체제인 구름 OS 등 ICT 신기술을 적용해 인증되지 않은 사용자의 접근을 원천적으로 차단하는 등 보안성을 강화했다.

이 시스템을 개발한 정형수 조은아이앤에스 대표는 "보안 관련 제반 법규를 기반으로 구축했고, 국가기관에서 보안에 대한 검증까지 완료해 보안 사고 및 유출 걱정 없이 쉽고 간편하게 비밀작성, 관리, 유통까지 비밀과 관련된 제반 업무를 수행할 수 있다"고 설명했다.

출처 : 뉴스투데이

국방 차세대 비밀관리시스템



전문자문위원 칼럼

국방혁신기술보안협회 연구원 부원장
최중환 박사



국방혁신기술보안협회(K-SAEM) 회원 및 회원사 여러분!
2025년 을사년 (乙巳年) 새해에 복 많이 받으십시오!

국방혁신기술보안협회는 2024년 9월 18일, 공식 출범하였으며 새로운 도약을 알리는 중요한 첫걸음으로 2025년 월간지를 발행하게 된 것을 매우 뜻깊게 생각합니다.

우리 협회는 국방부 산하 비영리 사단법인으로서 “군과 민간 기업간 미래 지향적 국방보안의 교량역할”을 목표로 지난 한 해 동안 열심히 달려왔습니다.

협회가 출범한 이후, 1년이라는 시간 동안, 보안 분야의 첨단 기술 동향과 이슈에 대한 논의는 물론, 다양한 전문가들과의 협력과 정보 공유, 유관기관과의 상호 업무협약 체결 등 많은 성과를 거두었습니다.

창립 1주년을 맞이한 지금, 저희는 그간의 노력과 성과를 돌아보고 앞으로의 발전을 위한 새로운 비전을 설정하는 기회를 가지고자 월간지를 발행하게 되었습니다.

이 월간지는 단순한 소식지 이상의 의미를 지니며, 회원 및 회원사 여러분과의 지속적인 소통을 위한 중요한 플랫폼으로 자리매김할 것입니다.

우리가 살고 있는 세상은 혁신과 기술 발전에 의해 급격히 변화되고 있으며, 특히 국방 분야에서는 로봇, 인공지능, 드론, 우주 탐사 등의 혁신기술이 빠른 속도로 개발되고 있습니다. 이러한 기술의 도입과 활용은 새로운 보안 위협을 만들어내며 이를 대비하기 위해서는 새로운 접근과 전략이 필요합니다. 보안기술 혁신의 속도가 빨라지고 있는 현 시점에서 우리 협회의 역할은 그 어느때보다도 커지고 있다고 하겠습니다.

이번 월간지에서는 협회 활동, 회원사 홍보, 사이버 보안이슈 등 중요한 주제들을 다루고 있습니다. 이러한 국방 혁신 기술의 최신 동향과 보안 이슈에 대한 심도 깊은 분석을 통해 회원 여러분이 현안에 대해 더욱 명확히 이해하고, 실질적인 해결책을 모색할 수 있도록 할 것입니다. 또한 다양한 전문가의 기고와 사례를 소개하며 국방 혁신과 보안 강화를 위한 실질적인 노하우와 경험을 공유할 것입니다.

앞으로 우리 협회는 국제적인 협력의 기회를 창출하여 국내 · 외적으로도 더 큰 영향력을 발휘할 수 있도록 지속적으로 노력할 것입니다. 회원 및 회원사 여러분의 지속적인 참여와 지원을 부탁드립니다.

끝으로 2025년이 여러분 각자의 꿈과 목표를 이루는 한 해가 되기를 기원드립니다. 감사합니다.



전문자문위원 칼럼

국방혁신기술보안협회 교육원 부원장
김성기 선문대학교 교수



2025년 을사년이 밝았습니다. 협회의 모든 회원사 임직원분들의 건승을 기원합니다.

E-sport 라는 하나의 문화산업을 촉발시킨 StarCraft 라는 게임 소프트웨어는 비록 게임이지만 게이머에게 두 가지 중요한 교훈을 주고 있습니다. 어떠한 전략과 전술도 공급을 압도하지 못한다는 것과 “Research Complete”과 “Upgrade Complete”을 누가 먼저 이루어 내느냐를 압도하지 못한다는 교훈입니다. 이 교훈은 국제 정치질서와 방산시장을 두고 경쟁을 벌이는 국가 및 기업 간 패권경쟁을 관통하고 있습니다. 이것은 혁신기술의 신속한 획득, 이 기술을 기초한 인프라의 업그레이드, 이 모든 것을 이끌어 가는 인재양성이 군사력과 방산시장 우위를 점하는데 매우 중요한 요소라는 것을 의미합니다. 국방과 산업에서 시사하는 바가 큼니다.

물리세계와 사이버 세계가 맞물려 돌아가는 4차산업-혁명기술은 지능형 소프트웨어 중심사회로 우리의 일상을 바꾸어 가고 있으며, 산업 전 방위에서 지능형 디지털전환을 촉진하고 있습니다. 국방 분야 또한 육·해·공·사이버·우주라는 다중영역이 네트워크로 통합되는 지능형 디지털전환을 요구받고 있습니다. 이러한 요구는 산업 전 방위의 혁신기술을 융합하여 국방에 적용하는 국방산업 생태계 조성 및 민간의 혁신기술을 신속히 획득하는 국방혁신기술 획득체계의 필요성을 의미합니다.

국방혁신기술보안협회는 우리나라 민간 혁신기술 역량이 국방혁신을 추동하고, 동시에 군이 이를 견인하는 민·군 “줄탁동시”의 지혜와 노력이 필요하다는 시대적 과제를 인식하고 있습니다.

협회에서는 이러한 인식에서 2024년 11월 22일 총회를 개최하여, 협회 내 연구기획전문위원회와 교육원을 창설하였습니다. 연구기획전문위원회는 회원사의 혁신기술을 국방 분야에 접목할 수 있는 실질적이고 실행 가능한 계획을 마련하여 도움을 드리하고자 노력할 것입니다. 교육원은 다음과 같은 사유로 국방정보보호 분야(RMF, CMMC, 방산기술보안, 우주항공보안, 국방AI보안) 전문 인재양성 교육에 주목하여 기여하고자 합니다.

신기술은 설계 당시에 미처 발견하지 못한 “설계오류(design fault)”로서 보안취약점을 완벽히 제거할 수 없는 한계로 인하여, 신기술에 의한 시스템과 인프라의 갱신은 늘 사이버보안 공격에 표적이 되는 보안취약점이 잠재할 수 있습니다. 현재 우리의 일상에서 정보 보안 실패는 기밀이 노출되는 위험을 넘어 물리보안과 인명보안 실패로 이어지는 사이버테러를 가능케 하고 있어서, 국방에서는 혁신기술의 획득요구보다 보안요구가 더 우선할 수밖에 없는 현실입니다.

따라서 국방혁신기술의 개발과 획득은 사이버 보안 위협에 대응하기 위하여 민·군 모두에게 사이버보안 위협관리 역량을 요구합니다. 국방혁신기술 자체를 탈취하려고 위협하는 방산기술보안부터, 방산제품 및 소프트웨어를 구성하는 공급망 보안, 방산기술 개발, 획득과정에서 발생할 수 있는 보안, 방산기술이 갖는 보안취약점으로 인하여 위협받는 국방사이버 보안 위협 등이 해당됩니다. 소요를 제기하는 발주처(국방부)와 소요를 충족하는 공급자(기업) 간에는 발주처가 제시한 보안통제항목을 기반으로 국방분야 특성을 고려한 보안요구사항 지침을 충족해야하는 프로토콜 준수 의무가 제도화 되어 있습니다.

이른바 미국 NIST RMF 표준을 우리나라 실정에 맞게 수정한 K-RMF 가 2026년도부터 시행 됩니다. 발주자인 국방부는 보안요구사항(SRG) 지침을 제공하고, 공급자는 제품별 보안구현가이드라인(STIG)을 제출하여 검증 및 승인하는 프로세스입니다. 민간에서도 발주처와 공급자간에 동일한 프로세스를 적용하여 응용할 수 있습니다. 다만 RMF 절차와 실무에 대한 지침이 추상적이고 참조해야할 문서가 방대하여 민·군 모두 스스로 실무를 단시간에 터득하기 어려운 여건입니다. 교육원은 RMF 교육을 통해 이러한 절차 실무에 필요한 제반 보안교육을 제공하여 회원사를 돕고, 관련 인력양성에 기여하고자 합니다.

CMMC는 미 국방 조달에 참여하는 기업이 갖추어야 할 사이버보안성숙도 모델을 인증하는 제도입니다. CMMC교육은 CMMC 인증이 필요한 회원사에게 도움을 제공하고, 이 분야 인력양성에 기여하고자 합니다.

방산기술보안 교육은 Anti-Tampering 기술을 포함하여 방산기술의 탈취 위협에 대응하기 위한 기술 및 보안 프로세스에 관한 교육입니다.

우주항공보안은 국방위성의 설계-개발-운영-폐기에 이르는 생애주기 전반에서 발생할 수 있는 보안위험으로부터 보호하기 위한 기술적, 관리적 제반 보안대응 역량을 함양하는 교육입니다.

국방AI보안은 신뢰 가능한 국방AI의 소요제기부터 데이터 준비단계, 데이터 학습단계, 모델개발단계, 시험평가 단계, 획득단계, 운영단계, 진화적 획득유지 단계가 반복되는 DevMLOps 프로세스 전반에 필요한 보안요구사항, 보안통제항목과 구현, 데이터카드, 모델카드, 군사동맹국 간 AI 무기체계 연동을 위해 요구되고 있는 AI Passport 제도에 관한 교육입니다,

교육원에서는 올 한 해 동안 위 각 교육 분야 인재양성을 위한 차별화된 교육 콘텐츠와 코스웨어 개발을 위해 노력하겠습니다.

협회의 이러한 노력은 회원사들로 하여금 보유하신 혁신 기술과 노하우가 좀 더 국방에 접목할 수 있는 기회를 높이고 애로 기술 개발에 기여 할 것이라고 기대합니다.



협회 공지사항

회원사 과제 기획지원

□ IITP 사이버보안 과제 기획

- 토의 : #75, #76, #77

- 제안서 제출 기한 : '25년 2월10일

□ 국방 ICT 신기술 활용제안

- 관련기관 접촉 및 신기술 설명 : 1.24/2.27/2.28

- 제안서 제출 기한 : '25년 2월14일

회원사 방문 상생방안 업무 토의

□ 누리온 2월3일 오후 3시 협회 회의실

□ 에스지에이솔루션 2월4일 오후 3시 SGA 회의실(의왕)

□ 알파인랩(구 올잇원) 2월5일 오전 10시 알파인랩 회의실(구로)

□ 유비벨록스 2월5일 오후 2시 유비회의실(구로)

□ 조은아이앤에스 2월6일 오전 10시30분 협회회의실(문정동)

□ 진앤현 2월6일 오후 2시 진앤현회의실(문정동)

□ 편진 2월11일 오전10시 편진회의실(성수동)

□ 굿모닝아이텍 2월19일 16시 GIT 회의실(고양)

2025 K-방산혁신포럼 및 전시회 계획

□ 개 요

- 포럼제목 : CMMC·RMF의 현주소와 향후 대비 방향
- 일시 : '25. 2.24(월) 1400~1740
- 장소 : 국회의원회관 제1소회의실 및 제2로비
- 주최 : 유용원 국회의원(국민의힘), 임종득 국회의원(국민의힘)
- 주관 : 뉴스투데이·(사)국방혁신기술보안협회
- 후원 : 방위사업청, 한국방위산업학회, 한국안보협업연구소

□ 프로그램

시 간	내 용
1330~1400	접수 / 환담
1400~1440	개회, 국민의례, 내빈 소개, 영상 상영 개회사 : 강남옥 (뉴스투데이 대표이사), 환영사 : 유용원 (국회의원/국민의힘), 임종득 (국회의원/국민의힘) 축사 : 석종건 (방위사업청장), 최병로 (방위산업진흥회 부회장) 기념촬영
1445~1505	기조강연 : 김승주 (국방혁신기술보안협회장 / 고려대 교수) * 대통령 직속 국방혁신위원회 위원
1505~1525	부스 관람 / Break Time
1530~1640 (세션1 : CMMC)	좌장 : 류연승 (명지대 교수) 발표 ① 서정청 (명지대 CMMC센터장) : CMMC 동향과 우리의 대응 ② 최시철 (F1시큐리티 이사) : 정보보호 컨설팅 관점의 CMMC 토론 : 최영종 (국방기술품질원 방산기술보호센터장), 염상훈 (한화시스템 보안팀장)
1640~1740 (세션2 : RMF)	좌장 : 신동규 (세종대 교수) 발표 ① 정기석 (방위사업청 수석전문관) : RMF의 현주소 ② 윤석준 (세종대 컴퓨터공학과 교수) : RMF의 향후 대비 방향 토론 : 박춘석 (국방혁신기술보안협회 사무총장), 조현석 (LIG넥스원 RMF팀장)

□ 전시회(부스) 계획

- 참가 대상 : 정보보호 및 방산 관련업체
 * 국방혁신기술보안협회 회원사 우선권 부여
- 참가 규모 : 24개

K-방산혁신포럼 전시부스 운영 계획

개 요

일 시

'25. 2.24(월) 1400~1740

장 소

국회 의원회관 제2로비(제1소회의실 옆)

규 모

24개(2,000×2,000×2,500(h))

* 골조, 카페트, 간판, 전시대, 사인물, 조명, 전기콘센트 등 기본 제공

대 상

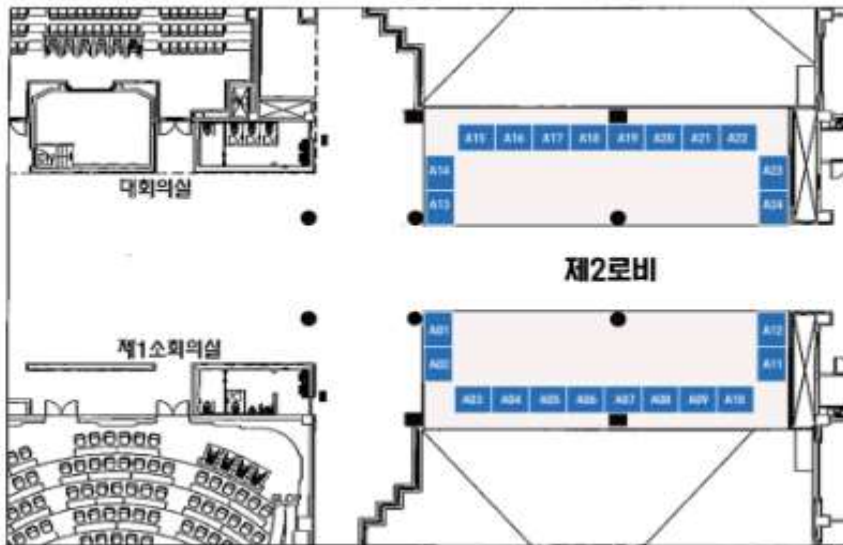
정보보호 · 방산 관련업체(회원사 우선)

비 용

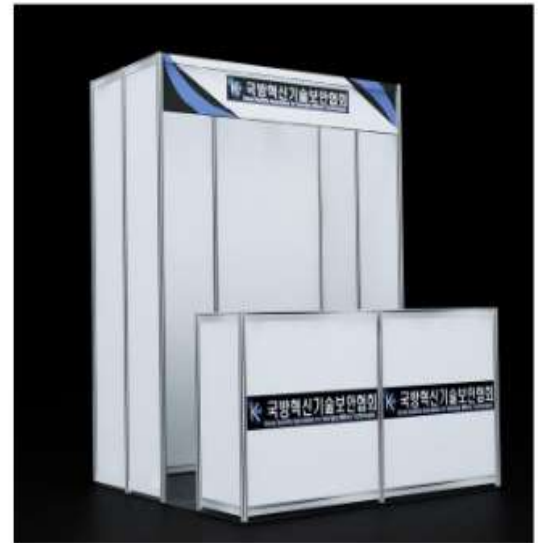
200만원

위치 및 유형

부스 위치



부스 유형



문 의

○ 협회 운영국장 : 010-5080-1281 / hgjeong@ksaem.or.kr



국방혁신4.0 시대를 선도하는 최고의 선택
**2025 초거대 AI시대 사이버보안
최고위과정**

주관 : (사)국방혁신기술보안협회 후원 : 성균관대 인공지능융합원

「초거대 AI시대 사이버보안 최고위과정」은?

초거대 AI로 변화되는 산업기술이 국방산업과 융합하여 국방혁신을 이끌어야 하는 국방혁신4.0 시대는 위험관리 역량으로써 사이버보안 리더십을 요구하고 있습니다.

(사)국방혁신기술보안협회에서는 성균관대 인공지능융합원의 후원하에 이러한 AI산업 및 방산생태계의 변화에 부응하기 위하여 사이버보안 최고위 지도자를 양성하는 「초거대 AI시대 사이버보안 최고위과정」을 준비하였습니다.

본 과정은 국방혁신을 이끌어온 전·현직 군관계자, 국방혁신 연구기관, 산·학·연 전문가를 비롯하여 다학제 통찰을 공유하는 전문강사진과 함께 할 것 입니다.

본 과정을 통하여 국방혁신의 통찰과 혁신 아이디어를 공유하는 리더십 네트워킹에 참여하는 기회가 되시기를 바랍니다.

교육 특징

타과정과 차별화된 프로그램

- √ 대한민국 최초 '초거대 AI시대 사이버보안 최고위' 과정
- √ 사이버보안 위주 편성하되, 인문학 등 다양한 프로그램 편성

최고의 전문 강사진 구성

- √ 대학 교수, 방산업체 임원, 전·현직 장군 등 다양한 분야 강사로 구성
- √ 강사진과 함께 하는 워크숍

産·學·研·軍 다양한 교류

- √ 국방부, 사이버사, 국방과학연구소, KISA 등과 교류
- √ 방산업체 및 군/공공기관의 사이버보안관제체계 등 현장 방문

사이버보안 고급 인적 네트워크

- √ 정보보호 분야 전문가 (90여 명) 및 회원사(60여 개) 보유
- √ 성균관대 인공지능융합원 전문가 협업/교류

초거대 AI시대 사이버보안 최고위과정 프로그램

기간 2025. 4. 8 ~ 10.28 / 6개월, 1700~1900 / 매주 화요일

인원 50명(회원/회원사, 군/공무원, 일반인 및 민간기업 CEO/임원)

장소 동진빌딩 2층(교대역 1번 출구 120미터)

세션	일정		주제	강사
I. 국방 과학 기술과 사이버 보안	1주차	4.08	[입학식]	협회
			개강 특강	김승주(협회장)
	2주차	4.15	AI 사피엔스 시대 생존전략	최재봉(성균관대 부총장)
	3주차	4.22	방산수출 확대와 기술보호 정책 현안	홍석준(한화에어로 전무)
	4주차	4.29	AI이해와 국방 적용	오상진(인공지능산업융합사업단장)
	5주차	5.13	명품 무기체계 탄생의 비화	박원동(전 방첩사 참모장/예소장)
			사이버작전의 과거와 미래	김한성(국방전산정보원장/예준장)
	6주차	5.20	과학기술과 전쟁	박영욱(한국국방기술학회 회장)
7주차	5.27	사회구조변화에 대응하는 도시환경 디자인	장영호(홍익대 교수)	
8주차	6.03	기업 방문 I (회원사)		
II. 최신 사이버 보안 트렌드	9주차	6.17	초거대 AI적용사례와 사이버보안 (서비스특화모델 중심으로)	김필수(네이버 AI테크 상무)
	10주차	6.24	커피와 크라상으로 읽는 세계문화	박장호(박사, 커피/인문학)
	11주차	7.01	국방 유무인복합체계 발전방향 및 보안 이슈	이종훈(홍익대 교수/예준장)
			미래전장의 게임체인저 AI	김광수(성균관대 인공지능융합원장)
	12주차	7.08	합동 전영역지휘통제체계와 사이버 보안	이재승(육군 정보통신학교장/준장)
	13주차	7.15	최근 사이버위협 동향 및 대응방안	이동근(KISA 디지털위협대응본부장)
	14주차	9.02	네트워크센트릭워페어(NCW)와 사이버 보안	정호섭(前 해군참모총장/예해대장)
	15주차	9.09	미국의 달러패권의 변화와 비트코인	오탈민(작가)
16주차	9.16	기업 방문 II (KISA 등)		
III. 사이버 보안 미래전략	17주차	9.23	AI와 무인화 시대의 전장관리 (미래 사이버보안 과제와 해법)	이승영(LIG넥스원 본부장)
	18주차	10.14	경영환경의 변화와 기업 경쟁력	조주현(중소벤처기업연구원장)
	19주차	10.21	국내외 정보보안 기술 및 제도 최신 동향	이재일(연세대 교수)
	20주차	10.28	졸업식	

모집 안내

기간

2025. 4. 8 ~ 10.28 / 6개월, 1700~1900 / 매주 화요일

인원

50명(회원/회원사, 군/공무원, 일반인 및 민간기업 CEO/임원)

제출서류

입학지원서 1부, 명함판사진 1매, 사업자등록증 사본 1부

전형방법

서류심사 → 합격자 통보 → 등록

교육비

500만원(회원/회원사 20% 할인, 군/공무원 50% 할인)

교육비 납부

입학지원서 1부, 명함판사진 1매, 사업자등록증 사본 1부

교육장소

동진빌딩 2층(교대역 1번 출구 120미터)



신청 문의

담당자1

(사)국방혁신기술보안협회 운영국장 : 정해균
TEL : 010 - 5080 -1281 / e-mail : haegyun.jeong@ksaem.co.kr

담당자2

(사)국방혁신기술보안협회 사무국장 : 양용진
TEL : 010 - 5072 - 1363 / e-mail : ksaem@ksaem.co.kr

회원 가입 안내

「국방혁신기술보안협회」는 국방부 산하 비영리 사단법인으로서 혁신기술(RMF, 인공지능, 드론, 우주 등)의 발전추세에 상응하는 軍內 보안업무를 지원하는 軍外 보안 지원 단체의 필요성에 따라 출범하였습니다.

軍과 민간기업간 상호협력의 교량 및 플랫폼 역할을 지향합니다. 미래지향적 국방보안 정립을 목표로 하는 본 협회와 뜻을 같이 하시는 기업 및 단체(기관), 개인의 적극적인 동참을 기대합니다.

<가입 대상>

협회의 제반 취지에 찬성하고 국방 및 보안 사업 분야에 관심있는 군산학연 관계자 및 회사

* 기업회원의 대표자(CEO 또는 관련업무 대표) 1인은 개인회원으로 자동 가입

신청 방법			
입회신청서(붙임 양식) 작성 및 제출 회원자격별 연회비(연1회) 납부			
구분		대기업	중소기업
임원사	부회장사	2천만원	1천만원
	이사사	1천만원	5백만원
일반회원사		2백만원	

[HTTPS://KSAEM.OR.KR/MEMBERSHIP/](https://ksaem.or.kr/membership/)

