과학기술정보통신부 보도자료

보도시점 2026. 3. 5.(목) 12:00 (2026. 3. 6.(금) 조간) 배포 2026. 3. 5.(목) 09:00

과기정통부, 피지컬 AI 시대 선도할 선박 · 우주 · 로봇산업 분야 특화 보안 매뉴얼 공개

미래산업 현장의 보안내재화를 돕는 실무형 가이드 · 체크리스트 · 사례집 제공

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 '과기정통부')는 한국인터넷진흥원(원장 이상중, 이하 'KISA')과 함께 스마트선박, 우주, 로봇 분야에 특화된 보안 매뉴얼을 개발하여 배포한다고 밝혔다.

▲ 스마트선박 산업의 인적·물적 사이버보안 안전망 확보

선박 산업 분야에서는 선박의 디지털화와 자율운항 기술 도입이 확산됨에 따라, 선박 시스템뿐 아니라 해운사 운영과 선원 활동 전반에서 보안 위협이 증가하고 있다. 과기정통부와 KISA는 이러한 변화에 대응해 해운 산업의 보안 위협을 체계적으로 식별하고, 선박 보호대책 및 현장 실무 가이드를 마련했다.

우선, 국제해사기구(IMO)의 자율운항 등급 3을 기준으로 실제 운항 시나리오별 위협 식별과 대응 절차를 체계화한 ▲자율운항선박 보안모델을 새롭게 개발했으며, 기존 스마트선박 보안모델에 현장 실무 중심의 해설과 적용 사례를 더해 ▲스마트선박 보안모델 해설서 및 사례집으로 고도화하여 차세대 선박의 보안 설계 기준으로 활용도를 높였다.

특히, 국내 대형 해운사가 함께 참여하여 국제 규제와 민간 표준을 충족할 수 있는 국내 최초 실무형 기준인 ▲해운사 특화 보안 가이드라인을 마련하는 한편, 현장 인력의 보안 역량 강화를 위해 ▲보안 인식 제고 교육교재, ▲선박 부착용 8대 보안수칙도 제작했다. 교육교재는 사고 사례부터 예방 행동, 보완 조치까지 단계별 학습이 가능하도록 구성되었으며, 선박 내에서 손쉽게 확인할 수 있는 포스터 형태로도 제공되어 인적 보안 사고 예방에 기여할 것으로 기대된다.

▲ 우주(위성) 생애주기 전반의 공급망 보안역량 강화

민간 주도의 ‘뉴스페이스(New Space)’ 시대에는 위성 제작·발사·운영 과정에서 다양한 기업과 서비스가 결합되며, 공급망·운영 환경 전반에서 새로운 보안 위협이 확대되고 있다.

이번에 공개하는 우주 분야 자료는 총 2종으로, ▲GSaaS(Ground Station as a Service, 클라우드 기반 위성 지상국 서비스) 등 최신 운영환경을 반영한 우주 보안모델 ▲체크리스트 기반의 상세 가이드를 담은 우주 보안모델 해설서로 구성된다.

보안모델에서는 최근 소형화 및 경량화 추세의 위성 개발에 맞추어 클라우드를 이용한 지상국 서비스의 주요 보안 위협과 보안 요구사항들을 식별하고, 우주 분야 글로벌 보안 규제를 반영한 총 53개 항목의 우주 보안 체크리스트를 제시하여 국내 우주 기업 담당자가 실제 현업에 적용함으로써 국내 우주 산업의 안전한 성장에 기여할 것으로 기대된다.

▲ 국산 로봇제품의 글로벌 보안 경쟁력 제고 기반 마련

최근 AI의 확산으로 산업 전반의 대대적인 변화가 예고되고 있다. 특히 AI가 물리적 실체와 결합한 피지컬 AI의 가장 대표주자인 로봇은 제조·서비스·의료 등 분야에서 빠르게 확산될 것으로 기대되는 반면, 이에 대한 유럽, 북미 등 사이버보안 글로벌 규제는 더욱 강화되고 있다.

이번에 공개하는 로봇 사이버보안 자료는 총 2종으로, ▲기존 로봇 보안모델의 고도화 버전, ▲로봇 보안요구사항 해설서로 구성된다. 이를 통해 기업은 로봇 제품의 개발과 수출과정에서 필요한 사이버보안 요구사항을 손쉽게 안내받을 수 있으며, 이를 통해 제품의 글로벌 경쟁력 확보에 기여할 것으로 기대된다.

각 매뉴얼은 한국인터넷진흥원(www.kisa.or.kr) 지식플랫폼 자료실을 통해 관심 있는 국민 누구나 무료로 내려받을 수 있다.

과기정통부 임정규 정보보호네트워크정책관은 “선박, 우주, 로봇 등 미래 핵심 산업에서도 사이버보안은 이제 선택이 아닌 필수 요건”이라며, “이번에 공개하는 특화 보안 매뉴얼이 기업의 보안 내재화 부담을 낮추고, 글로벌 시장에서 요구되는 보안기준 대응에 실질적인 길잡이가 되길 바란다”고 밝혔다.

담당 부서	정보보호산업과	책임자	과 장	이종혁 (044-202-6450)
		담당자	사무관	박세진 (044-202-6455)
유관 기관	한국인터넷진흥원 지역AX산업보안팀	책임자	팀 장	서민석 (061-820-3850)

참고1 스마트선박 산업 보안모델 등 개요

□ 배경 및 필요성

○ **(배경)** 폐쇄적으로 운영되던 선박 운항 환경이 선박-육상 연계 네트워크 확대에 의한 **디지털 전환이 가속화되며 선박 대상 사이버 위협 노출**

○ **(필요성)** 사이버 공격으로 인한 선박 제어권 상실 등을 예방하기 위한 **선박 생애주기 전반에 걸친 체계적인 보안 내재화 기반 마련 필요**

□ 주요 내용

< 보안모델 해설서 > < 자율운항 보안모델 > < 해운사 보안가이드 > < 보안 교재-8대 수칙 >

○ **(선박 보안모델)** 선박 운항 환경에서 발생 가능한 **보안 위협 선제적 식별** 및 이를 **예방하기 위한 맞춤형 보안 기술 및 요구사항** 제시

○ **(해운사 보안가이드)** 해운사가 현장에서 즉시 활용 가능하도록 자체 **리스크 평가 방법**과 **국제 요구사항 대응 절차를 실무 기준**으로 제시

※ (개발 협의체) HMM 오션서비스, SK해운, 현대LNG해운, 에이치라인해운, 포스에스텍, 지마린서비스

○ **(보안교재-8대 수칙)** 선원 대상 보안 인식 제고를 위해 사고사례 기반 **보안 교육 교재와 선박 부착용 '보안 8대 수칙'** 마련

※ 한국해운협회, 한국선박관리협회, 한국해양수산연수원에서 교재 및 수칙 활용 중

□ 기대 효과

○ **선박 건조(기술)-운영(관리)-인적 요소(사람)**에 이르는 생태계 전반의 보안 역량 강화를 통해 **국내 조선·해운업계의 운항 안전성 제고** 기반 마련

참고2 우주 산업 보안모델 등 개요

□ 배경 및 필요성

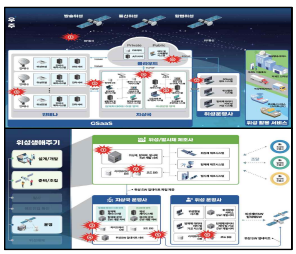
○ **(배경)** 뉴스페이스 시대 전환으로 상용 위성 및 위성 데이터 서비스 활성화 등 **우주 생태계의 다변화와 동시에 사이버공격의 취약성도 증가**

○ **(필요성)** 민간 우주산업의 안전한 성장 및 공급망 보안 강화를 위해 **우주기업이 보안 강화 대책 수립 시에 참고할 수 있는 보안 가이드라인** 개발

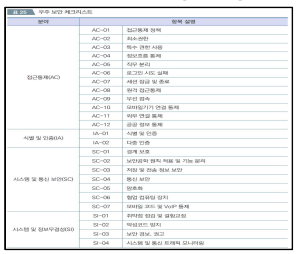
□ 주요 내용

< 우주 보안모델 >

< 우주 보안위협 >



< 체크리스트(일부) >



< 해설 및 사례집 >

○ **(보안모델)** 서비스형 지상국(GSaaS) 및 우주 SW 공급망 주요 **구성요소 도출, 보안위협 분석** 및 **보안 요구사항** 등 **보안 아키텍처 개발**

- **(GSaaS)** 위성과의 통신을 위한 안테나 시설, 클라우드 연동 및 지상국 운영 인프라, 위성 운영사 연계 구간의 **보안대책 제시**

* 재밍, 스푸핑, 지상국 시스템 무단 접근 등 → 안티재밍, 비인가 접속차단 등

- **(공급망) 위성 생애주기*별 우주 S/W 공급망 보안대책** 제시**

* 설계·개발 → 준비·조립 → 발사 → 궤도진입 확인 → 운영 → 위성 해체

** 위성제어SW 백도어 삽입, 취약한 오픈소스 사용 → 보안성 검토, 검증된 라이브러리 사용 등

○ **(해설 및 사례집)** 기존 우주 보안모델을 기업 담당자가 실무에 직접 활용할 수 있도록 **상세 적용 가이드라인 제시 및 우수사례 소개**

* 글로벌 우주·방산 컴플라이언스 반영, 총 53개 체크리스트 항목 적용 방안 안내

□ 기대 효과

○ 우주기업 보안적용을 통해 **국내 우주산업 보안내재화 및 경쟁력 확보**

참고3 로봇 산업 보안모델 등 개요

□ 배경 및 필요성

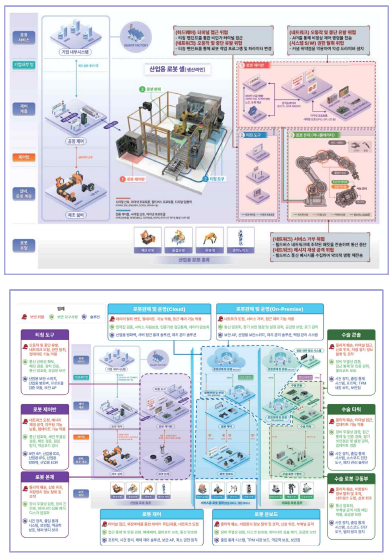
○ **(배경)** 최근 AI기술이 全 산업에 확산 추세이며, 피지컬 AI의 가장 대표적인 분야인 **로봇에 대한 안전 및 보안에 대한 우려 증가**

○ **(필요성)** 로봇기업 및 로봇 서비스 제공자가 **안전한 제품개발 및 서비스를 위해 참고 할 보안 가이드가 절실**

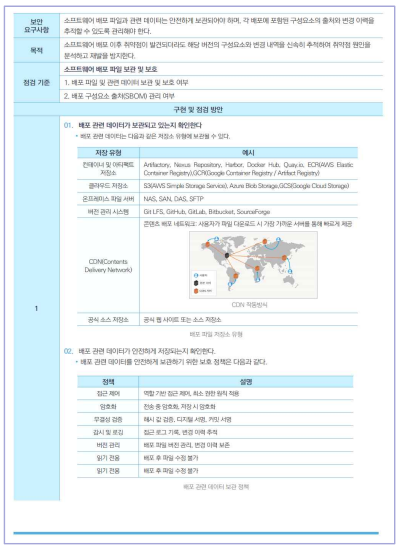
□ 주요 내용

< 로봇보안모델 >

< 로봇 보안 위협 및 대책 >



< 로봇보안 체크리스트 >



○ **(위협 및 대책)** 국제표준에 따른 로봇 유형별(산업용, 서비스용, 의료용 등)로 **보안위협을 정의하고, 이를 해결할 수 있는 보안대책**을 제시

※ 로봇은 본체, 제어반, 티칭도구 등으로 구성되며, 각 요소에 대한 위협 및 대책 제시

○ **(체크리스트 및 해설서)** 로봇기업이 직접 로봇의 보안위협을 진단해 볼 수 있는 **보안 체크리스트 및 상세 해설서** 함께 제공

※ 유럽, 북미 등 보안규제(IEC 62443, CRA 등) 수준으로 보안모델 고도화

□ 기대 효과

○ 피지컬 AI 관련 산업의 **보안경쟁력 제고 및 보안사고 예방**에 기여