

미국 국방부 RMF/CMMC 자동화 사례 심층 분석 및 AI 기반 K-RMF 에이전트 '솔버린' 사업화 전략 보고서

1. 서론: 국방 사이버 보안의 패러다임 전환과 자동화의 필연성

현대 국방 환경에서 사이버 공간은 육·해·공·우주에 이은 제5의 전장으로 확고히 자리 잡았다. 무기 체계의 디지털화와 네트워크 중심 전(NCW)의 가속화는 전력의 효율성을 극대화했으나, 동시에 사이버 위협에 대한 노출 면적을 기하급수적으로 확장시키는 결과를 초래했다. 이에 대응하기 위해 미국 국방부(DoD)는 정적이고 문서 중심적인 보안 인증 제도인 DIACAP(DoD Information Assurance Certification and Accreditation Process)을 폐기하고, 시스템 수명주기 전반에 걸친 위험 관리를 강조하는 **위험관리체계(RMF, Risk Management Framework)**로 전환하였다.¹

그러나 RMF의 도입은 방위산업체와 군 조직에 막대한 행정적 부담을 안겨주었다. 수천 페이지에 달하는 시스템 보안 계획(SSP)의 작성, 수백 개의 통제 항목에 대한 증적 수집, 그리고 3년 주기의 재인증 과정은 보안 전문가들이 실질적인 위협 탐지보다는 '서류 작업(Paper Compliance)'에 매몰되게 만드는 부작용을 낳았다. 특히 최근 미국 국방부가 방산망 보안을 강화하기 위해 도입한 **사이버보안 성숙도 모델 인증(CMMC 2.0)**은 미 방산 공급망(DIB)에 참여하는 중소기업들에게 생존을 위협하는 수준의 규제 비용을 발생시키고 있다.³

이러한 배경 속에서 미국은 **NIST OSCAL(Open Security Controls Assessment Language)**과 같은 데이터 표준과 인공지능(AI)을 활용한 자동화 솔루션을 통해 '규제 준수(Compliance)'를 '코드(Code)'로 전환하려는 혁신적인 시도를 하고 있다. Telos의 Xacta, Vanta와 같은 민간 자동화 플랫폼의 부상과 미 공군의 Platform One과 같은 DevSecOps 팩토리의 성공은 보안 인증이 더 이상 수동적인 행정 절차가 아니라, 자동화된 소프트웨어 엔지니어링의 일부가 되어야 함을 시사한다.

본 보고서는 미국 국방부의 RMF 및 CMMC 자동화 사례를 기술적, 정책적, 시장적 관점에서 심층 분석하고, 이를 벤치마킹하여 한국형 위험관리체계(K-RMF)의 자동화를 위한 AI 에이전트 **'솔버린(Solverine)***의 개발 및 사업화 전략을 제시한다. 아울러, 국민대학교 정보보안호수학과의 연구 역량과 산학협력 인프라를 활용하여 이 거대한 신시장을 선점하기 위한 구체적인 실행 로드맵을 제안한다.

2. 미 국방부 RMF 및 CMMC 2.0 자동화 생태계 심층 분석

2.1 NIST RMF의 구조적 한계와 데이터 중심 접근(Data-Centric Approach)으로의 전환

2.1.1 RMF의 7단계 프로세스와 행정적 병목 현상

NIST SP 800-37 Rev.2에 정의된 RMF는 **준비(Prepare), 분류(Categorize), 선정(Select), 구현(Implement), 평가(Assess), 승인(Authorize), 모니터링(Monitor)**의 7단계로 구성된다.² 이 체계는 보안을 시스템 설계 초기 단계부터 내재화(Security by Design)하는 것을 목표로 하지만, 실제 현장에서는 각 단계마다 생성되는 방대한 비정형 데이터(Word, PDF, Excel)로 인해 심각한 병목 현상이 발생하고 있다.

1. **분류 단계의 모호성:** 시스템의 정보 유형을 식별하고 보안 영향 수준(High/Moderate/Low)을 결정하는 과정에서 인간의 주관적 판단이 개입되어 일관성이 결여된다.
2. **평가 및 승인의 지연:** 수동으로 작성된 보안 평가 보고서(SAR)와 개선 계획(POA&M)을 검토하는 데에만 수개월이 소요되며, 이 기간 동안 시스템은 최신 위협에 무방비로 노출된다.⁶

2.1.2 NIST OSCAL: 자동화의 링구아 프랑카(Lingua Franca)

미 국방부와 NIST는 이러한 문제를 해결하기 위해 문서 중심의 인증을 데이터 중심의 인증으로 전환하는 핵심 표준인 **OSCAL**을 개발했다.⁷ OSCAL은 통제 목록, 시스템 보안 계획(SSP), 평가 결과 등을 XML, JSON, YAML과 같은 기계 판독 가능(Machine-Readable) 형식으로 표현한다.

- **상호운용성:** 서로 다른 보안 도구(스캐너, GRC 플랫폼, SIEM) 간에 데이터를 손실 없이 교환할 수 있게 하여, '디지털 트윈(Digital Twin)' 기반의 보안 평가를 가능하게 한다.⁹
- **지속적 통합:** 개발 파이프라인(CI/CD)에서 자동으로 생성된 보안 증거를 OSCAL 형식으로 변환하여 즉시 규제 준수 여부를 판정할 수 있다. 이는 평가 기간을 '개월' 단위에서 '일' 또는 '분' 단위로 단축시킨다.⁸

2.2 민간 자동화 솔루션 벤치마킹: Enterprise vs Agile 모델

미국의 RMF/CMMC 자동화 시장은 크게 미 국방부와 같은 거대 조직을 위한 '엔터프라이즈 모델'과 민간 중소기업을 위한 '애자일 SaaS 모델'로 양분된다.

2.2.1 Telos Xacta 360: 엔터프라이즈 RMF 자동화의 표준

Telos사의 Xacta 360은 미 국방부, 정보기관(IC), 연방기관에서 사실상의 표준으로 사용되는 RMF 자동화 플랫폼이다.¹

- 주요 기능 및 기술적 특징:
 - **Predictive Mapping™:** 취약점 스캐너(Nessus 등)에서 탐지된 기술적 취약점을 RMF 통제 항목과 자동으로 매핑하여 POA&M을 생성한다. 이는 수동 매핑에 소요되는 시간을 획기적으로 줄여준다.¹⁰
 - **OSCAL Native Support:** 기존의 레거시 데이터를 OSCAL 형식으로 변환(Ingestion)하거나, OSCAL 형식의 SSP를 생성하여 eMASS(미 국방부 RMF 관리

시스템)와 연동한다.¹¹

- 통제 상속(**Inheritance**): AWS GovCloud와 같은 클라우드 서비스 제공자(CSP)가 이미 충족한 통제 항목(예: 물리적 보안, 전력 공급)을 상속받아, 사용자는 자신의 애플리케이션 보안에만 집중할 수 있게 한다.¹⁰
- **Xacta.ai (Generative AI)**: 최근 생성형 AI를 도입하여 통제 구현 명세서(Control Implementation Statement)의 초안을 작성하거나, 규정 준수 관련 질문에 답변하는 RAG(Retrieval-Augmented Generation) 기능을 제공한다.¹⁰

2.2.2 Vanta & Drata: 애자일 규제 준수의 파괴적 혁신

Vanta와 Drata는 SOC 2, ISO 27001 등 민간 보안 인증 시장에서 시작하여 최근 CMMC와 NIST 800-171로 영역을 확장하고 있다.¹³ 이들은 Xacta와 달리 API 연동을 통한 **'지속적 모니터링(Continuous Monitoring)'**에 중점을 둔다.

- 자동화 메커니즘:

- **API 기반 증적 수집**: AWS, GitHub, Okta, Jira 등 400개 이상의 도구와 연동하여, 매 시간마다 자동으로 설정을 검사한다(예: "모든 관리자 계정에 MFA가 설정되어 있는가?").¹³
- **Test Once, Comply Many**: 한 번의 기술적 검증(예: 데이터 암호화 확인)으로 CMMC, SOC 2, ISO 27001 등 여러 프레임워크의 요구사항을 동시에 충족시키는 매핑 로직을 제공한다.¹⁵
- **접근성**: 보안 전문가가 아닌 엔지니어나 관리자도 쉽게 사용할 수 있는 직관적인 UI/UX를 제공하며, 중소기업(SME) 친화적인 가격 정책을 가진다.

2.2.3 비교 분석 및 시사점

구분	Telos Xacta 360	Vanta / Drata	'솔버린' 벤치마킹 시사점
타겟 고객	국방부, 대형 방산체계업체(Pri me)	중소 협력업체(Supply Chain), 스타트업	이원화 전략 필요: 체계업체용 On-Premise 버전과 협력업체용 SaaS 버전 구분
핵심 기술	RMF 워크플로우 엔진, OSCAL 변환	API 커넥터, 에이전트 기반 모니터링	하이브리드 아키텍처: 워크플로우(RMF)와 실시간 감시(API)의 결합
데이터 처리	기밀	비기밀 데이터(CUI),	망분리 환경 지원:

	데이터(Secret), 폐쇄망 지원	클라우드 친화적	폐쇄망 내에서 구동 가능한 로컬 AI 모델 필수
AI 활용	생성형 AI (문서 작성 보조)	머신러닝 (이상 탐지)	RAG 고도화: HWP 문서 생성 및 검증에 특화된 LLM 에이전트 개발

2.3 미 국방부의 혁신: cATO와 DevSecOps 팩토리

2.3.1 지속적 운영승인(cATO) 전략

미 국방부 CIO는 2022년 메모를 통해 전통적인 시점 기반의 ATO를 **지속적 ATO(cATO)**로 전환하겠다는 전략을 발표했다.¹⁶ cATO는 실시간 위협 모니터링(Continuous Monitoring)과 능동적 사이버 방어(Active Cyber Defense) 역량을 갖춘 시스템에 대해 기간 제한 없이 운영승인을 부여하는 제도이다.

- **3대 핵심 역량:** 1) RMF 통제 항목에 대한 지속적 모니터링, 2) 실시간 위협 대응을 위한 능동적 사이버 방어, 3) 승인된 DevSecOps 참조 아키텍처의 사용.¹⁸
- **시사점:** K-RMF 자동화 에이전트는 단순한 '인증 도구'가 아니라, 실시간 보안 관제(SOC)와 연동되어 시스템의 리스크 상태를 대시보드화하는 **'보안 가시성 플랫폼'**이어야 한다.

2.3.2 Platform One과 Iron Bank

미 공군의 Platform One은 DevSecOps의 성공 사례로, **Iron Bank**라는 중앙화된 컨테이너 저장소를 운영한다.¹⁹

- **소프트웨어 공장(Software Factory):** 벤더가 소프트웨어(컨테이너)를 Iron Bank에 제출하면, 자동화된 스캐닝 파이프라인이 이를 검증하고 강화(Hardening)한다. 검증된 컨테이너는 'Certificate to Field(CtF)'를 획득하여, 이를 사용하는 모든 프로젝트가 보안 통제를 상속받을 수 있다.
- **벤치마킹:** 한국형 국방 소프트웨어 생태계에도 이러한 '사전 검증된 컴포넌트 저장소' 개념을 도입하여, 솔버린 에이전트가 검증된 모듈의 사용 여부를 자동으로 확인하고 점수를 부여하는 체계를 구축해야 한다.

3. 한국 방위산업의 현실과 K-RMF 도입의 도전 과제

3.1 K-RMF 추진 현황과 한계

대한민국 국방부는 미 국방부의 RMF를 벤치마킹하여 한국형 위험 관리 체계(K-RMF) 구축을 추진하고 있다.²¹ 무기체계의 네트워크 연결성이 증대됨에 따라 기존의 정보보호 체계로는

고도화된 위협에 대응하기 어렵다는 판단에서다.

- 문서 중심의 관행: 여전히 대다수의 보안 평가가 HWP 문서와 엑셀 시트에 의존하여 수작업으로 이루어지고 있다. 이는 데이터의 재사용성을 저하시키고, 보안 상태의 가시성을 떨어뜨린다.
- 전문 인력 부족: 육·해·공군 및 방산 기업 내에 RMF 전문가는 극히 드물며, 복잡한 통제 항목을 해석하고 적용할 수 있는 인력이 턱없이 부족하다.

3.2 북한의 사이버 위협 고도화와 공급망 공격

한국 방위산업은 북한의 직접적인 타겟이 되고 있다. 최근 북한 해킹 그룹(Lazarus, Kimsuky, Andariel)은 방산 기술 탈취를 위해 더욱 정교한 기법을 사용하고 있다.²³

- **Kimsuky:** 생성형 AI를 활용하여 실제와 구분이 불가능한 가짜 군 신분증을 제작하고, 이를 이용한 스피어 피싱을 감행하고 있다.²⁴
- **Andariel:** 방산업체를 대상으로 랜섬웨어 공격을 수행하여 금전을 갈취하거나, 중요 기술 자료를 탈취하는 '이중 갈취' 전략을 구사한다.²⁵
- 공급망 공격(**Supply Chain Attack**): 보안이 취약한 중소 협력업체를 1차 침투 경로로 삼아 대형 체계업체의 내부망으로 침투하는 전략이 일반화되었다.²⁶

3.3 중소 방산기업(SME)의 '규제 절벽(Compliance Cliff)'

미국의 CMMC와 마찬가지로, 한국의 강화된 방산 보안 규제는 중소기업에게 감당하기 힘든 비용 부담으로 작용하고 있다.

- 비용 부담: ISMS-PL나 국방 보안 감사를 대비하기 위한 컨설팅 비용은 건당 수천만 원에 달하며, 이는 영세한 부품 업체들에게 큰 진입 장벽이다.²⁷
- 시장 위축 우려: 미국의 경우 CMMC 도입으로 인해 방산 기반(DIB)의 15-20%가 시장에서 이탈할 것으로 예측되고 있다.⁴ 한국 역시 유사한 '규제 절벽'에 직면할 가능성이 높으며, 이는 국방 공급망의 약화를 초래할 수 있다.

4. AI 기반 K-RMF 자동화 에이전트 '솔버린(Solverine)' 사업화 전략

4.1 제품 비전 및 핵심 가치 제안

'솔버린(Solverine) '은 'Solve'와 'Wolverine(끈질긴 생존력)'의 합성어로, 복잡한 K-RMF 규제 준수 문제를 AI로 해결하고 국방 시스템의 생존성을 보장한다는 의미를 담고 있다.

- 핵심 가치: "HWP 문서 작업에서 해방되어, 실질적인 사이버 방어에 집중하라(From Paperwork to Active Defense)."
- 목표: K-RMF 인증 소요 기간을 기존 6-12개월에서 1-2개월로 단축하고, 비용을 70% 이상 절감.

4.2 기술 아키텍처: 멀티 에이전트 AI 시스템 (Multi-Agent System)

솔버린은 단일 AI 모델이 아닌, 전문화된 역할을 수행하는 여러 AI 에이전트들의 협업 체계로 설계된다.²⁸

4.2.1 핵심 에이전트 구성

- **Ingestion Agent (수집 에이전트):**
 - 비정형 데이터(HWP, PDF, 이미지 등)를 읽어들여 텍스트와 표, 이미지를 추출하고 의미론적 구조를 분석한다.
 - 미국 Telos Xacta의 기능을 벤치마킹하여, 기존 레거시 문서를 **K-OSCAL** 표준 포맷으로 변환하는 '디지털 트윈' 생성 기능을 수행한다.
- **Reasoning Agent (추론 에이전트 - The Brain):**
 - **RAG(검색 증강 생성)** 기반: K-RMF 가이드라인, 국방 보안훈령, NIST SP 800-53 등의 방대한 규정 데이터를 벡터 DB로 구축하여, 에이전트가 항상 근거에 기반한 판단을 내리도록 한다.³⁰
 - **Dual LLM** 구조: 보안성을 위해 민감한 시스템 정보는 폐쇄망 내의 'Privileged LLM(On-premise)'이 처리하고, 일반적인 규정 해석은 'Public LLM'을 활용하는 이원화된 구조를 채택한다.³²
- **Verification Agent (검증 에이전트):**
 - 기술적 검증: SIEM, 방화벽, 클라우드 콘솔과 API로 연동하여 설정 값을 확인한다(Vanta 모델 벤치마킹).
 - **HW** 검증(특화 기능): 국민대학교의 부채널 분석 기술을 탑재하여, 암호 모듈의 물리적 취약점(Side-Channel Vulnerability)을 검증한다. 이는 소프트웨어 중심의 미국 툴과 차별화되는 핵심 경쟁력이다.
- **Documentation Agent (문서화 에이전트):**
 - 검증된 데이터를 바탕으로 국방부가 요구하는 양식(HWP)의 SSP, POA&M, SAR 문서를 자동으로 생성한다.
 - 생성된 문장의 각 단락마다 근거 데이터(로그 파일, 설정 스크린샷 등)를 하이퍼링크로 연결하여 감사(Audit)의 신뢰성을 보장한다.

4.3 차별화 전략: '능동형 RMF'와 위협 인텔리전스 통합

솔버린은 정적인 체크리스트 도구를 넘어, 최신 위협 정보를 반영하는 동적인 플랫폼으로 포지셔닝한다.

- **위협 기반 통제(Threat-Informed Controls):** 북한 해킹 그룹의 TTP(전술, 기법, 절차) 정보를 실시간으로 수신하여, 관련 통제 항목의 중요도를 동적으로 상향 조정한다.
 - 예시: Kimsuky의 AI 기반 피싱 공격 징후가 포착되면, 솔버린은 즉시 조직 내 '이메일 보안(SI-8)' 및 '사용자 훈련(AT-2)' 통제 항목의 점검 주기를 단축하고 긴급 점검을 지시한다.
- **cATO 지원:** 미국방부의 cATO 기준을 충족할 수 있도록, 실시간 리스크 점수(Risk Score)를 대시보드 형태로 제공하여 지휘관의 의사결정을 지원한다.

4.4 시장 진입 및 가격 정책

- **Tier 1 (체계업체):** 구축형(On-Premise) 라이선스 및 유지보수 모델. 내부망 설치 및 커스터마이징을 포함하여 고가 정책 유지.
- **Tier 2/3 (협력업체):** 구독형(SaaS) 모델. 방위사업청의 '기술보호 지원사업' 바우처와 연계하여 기업의 실질적 부담금을 최소화(약 10-20% 자부담)하는 전략 추진.³³

5. 국민대학교 산학협력 및 거버넌스 전략

국민대학교는 정보보안암호수학과의 독보적인 연구 역량을 바탕으로 K-RMF 자동화 생태계의 중심축(Hub)이 되어야 한다.

5.1 연구 역량 분석: 암호수학의 명가(名家)

국민대학교 정보보안암호수학과는 한동국 교수팀을 필두로 양자내성암호(PQC), 부채널 분석, 암호 모듈 검증(KCMVP) 분야에서 세계적인 수준의 연구 성과를 보유하고 있다.³⁵

- 주요 성과: 삼성SDS와 공동 연구를 통해 '부채널 공격에 안전한 행렬 곱 연산 기술'을 개발하여 2025년 특허기술상 충무공상을 수상하였으며, 이는 국산 암호 기술의 자립화에 크게 기여하였다.
- 국방 프로젝트 수주: 최근 국방기술 연구용역 100억 원 수주, 하드웨어 양자암호모듈(KCMVP Level 2) 개발 등 방산 보안 분야에서 실질적인 트랙 레코드를 축적하고 있다.³⁷

5.2 '글로컬 랩(Glocal Lab)' 기반의 생태계 조성 전략

교육부 주관 '글로컬 랩 방산기술보호연구소' 선정(9년, 216억 원 지원)을 기점으로, 국민대는 단순한 연구 기관을 넘어선 '플랫폼'으로 도약해야 한다.

- **K-OSCAL 표준화 주도:** 방위사업청, 국가보안기술연구소(NSR)와 협력하여 K-RMF의 데이터 표준인 **'K-OSCAL'**을 제정하고, 국민대가 이를 관리하는 사무국 역할을 수행한다. 표준을 장악하는 자가 생태계를 지배한다.
- 솔버린 테스트베드 구축: 교내에 'K-RMF 자동화 테스트베드'를 구축하여, 중소 방산기업들이 자사의 SW/HW를 가져와 솔버린 에이전트로 사전 검증(Pre-Audit)을 받을 수 있는 인증 센터를 운영한다.
- 하드웨어 보안 검증 특화: Vanta 등 글로벌 기업이 접근하기 어려운 '하드웨어 암호 모듈 검증(Side-Channel Verification)' 기능을 국민대의 특화 기술로 솔버린에 탑재하여 기술적 진입 장벽을 구축한다.

5.3 기술 사업화 및 스피노프(Spin-off) 로드맵

- **1단계 (2025-2026):** 교원 창업(Faculty Startup)을 통해 '솔버린' 개발 법인 설립. DAPA 기술보호 지원사업의 공급기업으로 등록하여 초기 레퍼런스 확보.
- **2단계 (2027-2028):** LIG넥스원, 한화시스템 등 대형 방산기업과 전략적 제휴(SI

파트너십)를 체결하여 세계 개발 사업에 솔버린을 기본 탑재(Embedded) 추진.

- **3단계 (2029~):** K-방산 수출 국가(폴란드, UAE 등)를 대상으로 '현지화된 RMF 자동화 패키지' 수출. 무기 체계와 보안 인증 도구를 패키지로 묶어 수출 경쟁력 제고.

6. 결론: 위기를 기회로 바꾸는 '솔버린' 이니셔티브

미국의 사례에서 보듯, 국방 보안의 자동화는 선택이 아닌 필수이다. 특히 북한의 비대칭 사이버 전력에 맞서야 하는 대한민국에게, 수동적인 문서 기반의 보안 관리는 더 이상 유효하지 않다. K-RMF의 도입은 우리 방위산업에 '규제 절벽'이라는 위기를 가져왔지만, 동시에 보안 자동화라는 거대한 신시장을 열어주었다.

국민대학교가 제안하는 **'솔버린'**은 단순한 행정 자동화 도구가 아니다. 이는 미국 방부의 cATO 철학을 계승하고, 국민대의 독보적인 암호/하드웨어 보안 기술을 결합하며, 생성형 AI와 멀티 에이전트 기술로 구현된 차세대 국방 보안 플랫폼이다.

국민대학교는 'K-OSCAL 표준화', 'AI 기반 자동화', '하드웨어 무결성 검증'이라는 3대 축을 중심으로 산·학·연·관 협력 모델을 구축함으로써, K-방산의 보안 내재화(Security by Design)를 선도하고 국가 안보와 방산 수출 경쟁력 강화에 결정적으로 기여할 것이다. 지금이 바로 '한국형 보안 자동화'의 표준을 세울 골든타임이다.

7. 부록: 데이터 및 비교표

표 1. 한·미 국방 보안 인증 자동화 수준 비교

구분	미국 (DoD RMF/CMMC)	한국 (K-RMF/K-Defense)	솔버린 (Solverine) 목표 모델
핵심 철학	Continuous ATO, Data-Centric	Point-in-Time ATO, Document-Centric	Real-Time Active Defense
데이터 표준	OSCAL (XML/JSON/YAML)	HWP, Excel, PDF (비정형)	K-OSCAL (HWP 호환)
증적 수집	API 기반 자동 수집 (Vanta, Xacta)	스크린샷, 수기 점검표	하이브리드 (API + OCR)
기술적 검증	SW 중심 (SaaS, Cloud)	HW/Embedded 비중 높음	SW + HW (부채널 검증)

위협 대응	위협 인텔리전스 연동 미흡	북한 전담 대응 체계 필요	대북 위협 인텔리전스 통합
-------	-------------------	-------------------	-------------------

표 2. 솔버린 에이전트의 RMF 단계별 AI 적용 시나리오

RMF 단계	기존 업무 (Pain Point)	솔버린 AI 에이전트 역할 (Solution)	적용 기술
Step 1: Prepare	수백 개의 통제 항목 중 적용 대상 식별 난해	무기체계 특성(운용 환경, 데이터 등)을 분석하여 최적의 맞춤형 통제 목록(Baseline) 추천	LLM (Reasoning)
Step 2: Categorize	정보 유형별 보안 등급 수동 판단	시스템 내 데이터 샘플을 분석하여 FIPS-199/K-RMF 기준 등급 자동 제안	NLP (Classification)
Step 3: Implement	보안 장비 설정 및 정책 문서 수기 작성	방화벽, OS 설정을 스캔하여 보안 정책(Policy) 초안 자동 생성 (HWP)	Generative AI (RAG)
Step 4: Assess	수동 모의해킹 및 취약점 점검	자동 취약점 스캔 및 부채널 분석 시뮬레이션 수행 후 결과 매핑	Agentic Workflow
Step 5: Authorize	수천 페이지의 인증 패키지 검토 지연	생성된 문서와 증적 간의 정합성 검증(Traceability Check) 및 요약 보고서 생성	LLM (Summarization)
Step 6: Monitor	3년 주기 간歇, 실시간 현황 파악 불가	지속적 모니터링(ConMon) 대시보드 운영 및	Anomaly Detection

		이상 징후 즉시 경보	
--	--	-------------	--

심층 연구 보고서: K-RMF(한국형 위험관리체계) 시장 분석 및 AI 기반 자동화 에이전트 사업 타당성 평가

1. 서론: 국방 사이버 안보의 패러다임 전환과 K-RMF의 부상

대한민국 방위산업은 하드웨어 중심의 '전력 증강'에서 소프트웨어와 데이터 중심의 '지능형 전력'으로 급격한 전환기를 맞이하고 있다. K2 전차, KF-21 전투기, 정찰 위성 등 현대 무기체계는 단순한 타격 수단이 아닌, 네트워크로 연결된 거대한 '사물인터넷(IoT) 디바이스'이자 '데이터 센터'로 진화하였다. 이러한 변화는 필연적으로 사이버 보안의 중요성을 무기체계의 생존성과 직결되는 핵심 요소로 격상시켰다.

과거 국방 정보보호는 시스템 구축 완료 후 단회성으로 보안성을 점검하는 '인증(Certification)' 중심의 정적인 절차였다. 그러나 2020년대 들어 미 국방부(DoD)의 RMF(Risk Management Framework) 전환 기조와 맞물려, 한국 국방부(MND) 역시 무기체계의 소요 기획부터 폐기까지 전 수명주기(Life-cycle)에 걸쳐 지속적으로 보안 위험을 관리하는 **K-RMF(Korean Risk Management Framework)** 체계를 도입하였다.

1.1 K-RMF의 정의와 전략적 중요성

K-RMF는 국방정보보호훈령에 근거하여 무기체계 및 전력지원체계에 적용되는 정보보호 업무 절차의 총체이다. 이는 기존의 '정보보호시스템 도입 시 보안성 검토'라는 파편화된 규제를 넘어, 시스템의 중요도에 따라 보안 등급을 분류(Categorize)하고, 이에 적합한 통제 항목을 선정(Select) 및 구현(Implement)하며, 지속적인 평가(Assess)와 승인(Authorize)을 거쳐 실시간으로 모니터링(Monitor)하는 순환 구조를 갖는다.

이러한 변화는 단순한 행정 절차의 변경이 아니다. 이는 다음과 같은 전략적 함의를 갖는다:

3. 지속적 감시(**Continuous Monitoring**): 해킹 기술은 매일 진화하므로, 3년 전 승인받은 보안 태세가 오늘 안전하다고 보장할 수 없다. K-RMF는 실시간에 가까운 위험 관리를 요구한다.
4. 책임의 명확화: 과거에는 기술적 구현 여부만 따졌다면, K-RMF는 '승인 권자(Authorizing Official)'가 잔존 위험(Residual Risk)을 수용하고 운영을 승인하는 지휘관의 결심 과정(Risk Acceptance)을 포함한다.
5. 상호운용성(**Interoperability**) 보장: 한국군 단독 작전뿐만 아니라 한미 연합 작전 시, 미군 시스템과의 연동을 위해서는 미군의 RMF 기준에 부합하는 수준의 보안 관리가 필수적이다.

1.2 연구의 목적 및 범위

본 보고서는 급부상하는 K-RMF 규제 환경 속에서, 이를 기술적으로 자동화하고 효율화할 수 있는 **'AI 기반 K-RMF 에이전트(Agent)**'의 사업성을 심층 분석한다. 특히 방산 대기업과 정보보호 컨설팅 기업들의 대응 현황을 조사하고, 아직 시장에 뚜렷한 지배적 사업자가 없는 '무주공간(Blue Ocean)'의 영역인 RMF 자동화 솔루션 시장의 기회 요인을 포착하여 구체적인

사업 전략과 피치덱(Pitch Deck)을 제시하는 것을 목적으로 한다.

2. K-RMF 생태계 및 규제 환경 분석

사업성 분석에 앞서, K-RMF가 작동하는 규제적 토양과 현재의 비효율적인 업무 관행을 이해해야 한다. AI 에이전트의 가치는 현재 인간이 겪고 있는 고통의 크기에 비례하기 때문이다.

2.1 K-RMF의 6단계 프로세스와 현장의 폐인 포인트(Pain Point)

미 NIST SP 800-37을 벤치마킹한 K-RMF는 크게 6단계(또는 준비 단계를 포함한 7단계)로 구분된다. 현장에서 발생하는 비효율은 각 단계마다 막대하다.

단계	주요 활동	현장의 폐인 포인트(Pain Point)	AI 적용 기회
1. 분류 (Categorize)	정보시스템의 데이터 유형 식별 및 보안 영향 수준(High/Moderate/Low) 결정	수백 종의 데이터 유형을 분류 기준과 매핑하는 과정이 엑셀 수작업으로 이루어짐. 주관적 해석에 따른 오류 반복.	자연어 처리(NLP)를 통한 시스템 기술서 분석 및 보안 등급 자동 추천
2. 통제 선정 (Select)	보안 등급에 따른 기본 통제 항목(Baseline Controls) 선정 및 조정(Tailoring)	수천 개의 보안 통제 항목(NIST 800-53 기반) 중 불필요한 것을 걸어내고 추가할 것을 정하는 '테일러링'의 복잡성.	유사 무기체계 데이터를 학습한 AI가 최적의 통제 항목 세트(Profile) 자동 생성
3. 구현 (Implement)	선정된 통제 항목을 시스템 설계 및 개발에 반영	시스템 엔지니어링(SE) 문서와 보안 문서의 불일치. 설계 변경 시 보안 문서 수정 누락.	MBSE(모델 기반 시스템 엔지니어링) 연동을 통한 설계-보안 동기화
4. 평가 (Assess)	통제 항목이 올바르게 구현되었는지 검증 (취약점 점검, 모의해킹 등)	가장 큰 병목 구간. 수작업 증적 캡처, 스크린샷 엑셀 붙여넣기 등 단순 반복 노동. 인력 부족으로 인한 평가 지연.	자동화된 진단 도구 연동 및 결과 보고서 자동 생성 (GenAI 활용)
5. 승인 (Authorize)	위험 평가 결과를 바탕으로 운영 승인 여부 결정	수천 페이지의 문서를 검토해야 하는 승인권자의 피로도. 핵심 리스크 식별 어려움.	핵심 위험 요약 대시보드 및 의사결정 지원 AI 챗봇
6. 감시 (Monitor)	운영 중 지속적인 보안 태세 점검 및 변경 관리	1회성 평가 후 방치되는 경향. 실시간 위협 정보와 통제 항목의 연계 부족.	AI-ISAC 연동을 통한 실시간 위협 대응 및 통제 항목 상태 자동 업데이트

2.2 한-미 RMF 비교 및 한국적 특수성

미국과 한국의 RMF는 개념적으로 유사하나, 실행 세칙에서 차이가 존재한다.

- **프로세스의 단순화:** 미군은 4단계의 복잡한 분류 과정을 거치나, 한국 국방부는 이를 3단계(정보 유형 식별 -> 보안 등급 결정 -> 승인)로 간소화하여 적용하고 있다.
- **인프라 환경:** 미군은 거대한 클라우드 인프라(JEDI, JWCC 등) 위에서 RMF를 수행하는 반면, 한국군은 아직 폐쇄망(Intranet)과 온프레미스(On-premise) 환경 비중이 높다. 이는 SaaS(Software as a Service) 형태의 클라우드 보안 도구 도입을 어렵게 만드는 요인이다, 동시에 ***구축형(On-premise) AI 솔루션***에 대한 강력한 수요를 의미한다.

2.3 국방 예산의 흐름과 시장 확장성

2025년 국방부 예산안 분석 결과, '한국형 3축 체계' 등 전력 증강 예산이 6조 1천억 원에 달하며, 정보보호 및 특수활동 성격의 예산이 2조 1천억 원 규모로 책정되었다. 특히 국방 AI 센터 설립, AI-ISAC 구축 등 지능형 보안 체계 구축을 위한 투자가 본격화되고 있어, K-RMF 자동화 솔루션 도입을 위한 예산적 기반은 충분히 조성된 것으로 판단된다.

3. 시장 경쟁 현황 및 기업별 대응 전략

K-RMF 시장은 현재 '춘추전국시대'와 같다. 제도는 시행되었으나 이를 완벽하게 지원하는 도구(Tool)는 부재하며, 기업들은 각자의 방식으로 생존을 모색하고 있다.

3.1 방산 대기업(체계 종합 업체)의 대응: "내재화의 딜레마"

한화시스템, LIG넥스원, KAI(한국항공우주산업) 등 주요 방산 기업들은 K-RMF를 '피할 수 없는 비용'으로 인식하고 있다.

- **LIG넥스원:**
 - **전략:** 공격적인 인재 채용을 통한 내재화. LIG넥스원은 2024년 상반기 공채 등을 통해 RMF 전문 인력과 IPS(종합군수지원), SW 개발 인력을 대거 모집하였다. 이는 외부 컨설팅에 의존할 경우 발생하는 기술 유출 우려와 비용 상승을 막기 위함이다.
 - **한계:** 인력 시장의 공급 부족. RMF를 이해하면서 무기체계(임베디드 SW)를 아는 전문가는 극소수다. 결국 내부 소수 인력이 다수의 외부 초급 감리원을 관리하는 구조가 고착화되고 있다.
- **한화시스템:**
 - **전략:** ICT 부문의 역량을 활용한 시너지 창출. 한화시스템은 방산 전자와 ICT 서비스를 모두 보유한 유일한 기업으로, 연합지휘통제체계(AKJCCS) 성능개량 사업 등 대형 SI 사업을 수주하며 자체적인 보안 인증 노하우를 축적하고 있다.
 - **한계:** 자체 개발한 단편적인 도구들은 존재하나, 전사적으로 표준화된 'AI 기반 RMF 플랫폼' 수준에는 도달하지 못한 것으로 파악된다. 여전히 엑셀과 워드 기반의 문서 작업이 주를 이룬다.

3.2 정보보호 전문 서비스 기업(컨설팅/감리)의 대응: "노동 집약적 모델의 한계"

씨에이에스(CAS), 안랩, 시큐아이, 원스 등은 국방 정보화 사업 감리 및 정보보호 컨설팅 시장의 전통적 강자들이다.

- **씨에이에스(CAS):** 국방수송정보체계 감리 등 다수의 국방 SI 감리 레퍼런스를 보유하고 있다. 그러나 이들의 비즈니스 모델은 '맨먼스(Man-Month)' 투입 방식이다. 즉, 사람이 많이 투입될수록 돈을 버는 구조이기에, 업무 시간을 획기적으로 줄여주는 자동화

- 솔루션 개발에 대한 유인이 상대적으로 적었다.
- 보안 관제/진단 기업 (안랩, 이글루코퍼레이션 등): 이들은 취약점 진단 솔루션(Scanner)이나 관제 시스템(SIEM)을 납품하지만, 이는 K-RMF의 6단계 중 '평가(Assess)'와 '감시(Monitor)' 단계의 일부 데이터 소스(Data Source) 역할을 할 뿐, 전체 행정 절차를 관리하는 오케스트레이션(Orchestration) 도구는 아니다.

3.3 글로벌 벤치마킹 및 국내 격차 (The Gap)

미국 시장에서는 이미 K-RMF와 유사한 미군 RMF를 자동화하는 시장이 성숙해 있다.

- Telos Xacta:** 미 CIA, DoD 등에서 표준처럼 사용되는 RMF 자동화 도구. 문서 생성, 통제 항목 매핑, 상속(Inheritance) 기능을 통해 인증 기간을 최대 90% 단축한다고 주장한다.
- RegScale, OpenRMF:** API 중심의 'Compliance as Code'를 표방하며, 데브옵스(DevOps) 파이프라인에 규제 준수를 통합하고 있다.

핵심 발견: 국내에는 이러한 'RMF 전용 자동화 플랫폼'이 부재하다. 현재 국내 방산 업체들은 엑셀(Excel)로 수천 개의 통제 항목을 관리하거나, SI 업체가 프로젝트별로 급조한 웹 게시판 형태의 시스템을 사용하고 있다. 미국의 **Xacta**와 같은 '한국형 RMF AI 에이전트'는 현재 시장에 공백 상태이며, 이것이 바로 사업의 핵심 기회이다.

4. AI 기반 K-RMF Agent 사업성 심층 분석

4.1 제품 개념: "Defense Compliance AGI"

제안하는 솔루션은 단순한 문서 관리 도구가 아닌, 생성형 AI(LLM)와 RAG(검색 증강 생성) 기술이 결합된 지능형 에이전트이다.

- 핵심 기능:
 - 지능형 분류 및 태일러링: 사용자가 "이 시스템은 무인 정찰 드론의 지상 통제 장비다"라고 입력하면, AI가 국방정보보호훈령을 분석하여 보안 등급을 추천하고, 불필요한 통제 항목을 자동으로 제거(Tailoring)한다.
 - 문서 자동 생성(GenAI): 시스템 설계서(Architecture Description)를 입력 받아 보안계획서(SSP), 위험관리전략서 등 필수 문서를 초안 작성한다.
 - 증적 자동 수집 및 매핑: 서버, 방화벽, 소스코드 진단 도구와 연동하여 보안 설정 값을 읽어오고, 이를 K-RMF 통제 항목과 자동으로 매핑한다. (예: "패스워드 복잡도 설정" 항목에 대해 실제 리눅스 서버의 /etc/login.defs 파일 내용을 증적으로 자동 첨부).
 - AI 감사 챗봇: 감사관(Auditor)이 "이 시스템의 계정 관리 절차가 규정에 맞는지 근거를 보여줘"라고 물으면, 관련 문서와 설정 로그를 찾아 답변한다.

4.2 기술적 실현 가능성과 '데이터 주권(Sovereignty)'

국방 분야에서 AI 도입의 최대 장벽은 '보안'이다. 챗GPT와 같은 해외 클라우드 기반 LLM은 기밀 유출 우려로 인해 사용이 불가능하다.

- 해결책: **Sovereign AI** (초거대 AI의 국산화)
 - Naver HyperCLOVA X:** 네이버가 개발한 한국어 특화 초거대 AI인 하이퍼클로바X는 한국의 법률, 제도, 문화적 맥락을 가장 잘 이해한다.
 - 온프레미스/프라이빗 클라우드 배포: 국방부 내부망(Intranet) 또는 방산 기업의 폐쇄망에 하이퍼클로바X 모델을 경량화(Quantization)하거나 API 게이트웨이를 통해 안전하게 연동하는 방식이 필수적이다.

- 네이버클라우드는 이미 'AI 안심존' 등 보안이 강화된 환경을 제공하며, 국방 AI 센터와의 협력을 모색하고 있다. 따라서 본 사업은 **HyperCLOVA X** 기반의 **버티컬(Vertical) AI** 애플리케이션으로 포지셔닝해야 한다.

4.3 시장 규모 추정 (**TAM, SAM, SOM**)

본 사업의 시장성을 정량적으로 평가하기 위해 2025년 기준 데이터를 바탕으로 추정한다.

TAM (Total Addressable Market) - 전체 국방/공공 정보보호 시장

- 정의: 국방부 및 방위사업청, 관련 산하기관의 정보보호 예산 및 공공 SW 보안 시장의 종합.
- 근거: 2025년 국방 정보보호 및 특수 예산 약 2.1조 원 중 시스템 구축 및 유지보수 비용, 정부 공공 SW 사업 규모 5.8조 원 중 국방 비중 고려.
- 추정액: 약 **6,000억 원** (연간)

SAM (Serviceable Available Market) - 국방 RMF 컨설팅 및 솔루션 시장

- 정의: K-RMF 인증을 위해 직접적으로 지출되는 컨설팅 비용, 감리 비용, 보안 솔루션 라이선스 비용.
- 근거:
 - 주요 무기체계 연구개발 사업(연간 약 50~100개 내외) × 프로젝트당 보안 컨설팅/인증 비용(평균 5~10억 원).
 - 국방통합데이터센터(DIDC) 운영 시스템(77개 전산소 통합)의 지속적인 RMF 갱신 비용.
 - 방산혁신기업 및 중소 협력업체의 보안 인프라 구축 수요.
- 추정액: 약 **1,500억 원** (연간)

SOM (Serviceable Obtainable Market) - AI 기반 자동화 에이전트 목표 시장

- 정의: 기존 인력 중심의 컨설팅 시장 중 AI SW로 대체 가능한 영역 및 신규 라이선스 매출.
- 근거:
 - 시장 침투율 20% 가정 (초기 3년 내).
 - 인력 대체 효과: 컨설팅 비용의 30% 절감분을 SW 라이선스 비용으로 전환.
 - 주요 타겟: 방산 체계종합업체(Big 3) 및 1차 협력사, 국방통합데이터센터.
- 추정액: 약 **300억 원** (연간 매출, 5년 내 달성 목표)
 - 참고: 이는 보수적인 수치이며, 향후 **NATO** 등 수출 무기체계의 상호운용성 인증(RMF 매핑) 시장까지 포함하면 업사이드(*Upside*)는 훨씬 크다.

5. 피치덱 (**Pitch Deck**) 구성안

사업성이 확인되었으므로, 투자 유치 및 정부 과제 수주를 위한 피치덱 스토리라인을 제시한다.

Slide 1: Title

Sentinel-K (가칭)

국방 규제 준수의 운영체제 (The OS for Defense Compliance) HyperCLOVA X 기반 K-RMF
완전 자동화 솔루션

Slide 2: The Problem (문제 제기)

"첨단 무기를 만드는데, 보안 서류는 조선시대 방식으로 합니다."

- **Pain Point:** K2 전차 1대를 실전 배치하기 위해 필요한 보안 문서는 3,000페이지가 넘습니다.
- **Inefficiency:** 방산 연구원들은 개발 시간의 30%를 엑셀 작업과 증적 캡처에 낭비하고 있습니다.
- **Risk:** 수작업으로 작성된 보안 문서는 실제 시스템과 일치하지 않아(Miss-match), 해킹 위협에 무방비로 노출됩니다.
- **Talent Crunch:** RMF 전문가는 전국에 100명도 되지 않습니다. 채용은 불가능에 가깝습니다.

Slide 3: The Solution (솔루션)

"AI Security Officer in a Box"

- **RMF Auto-Pilot:** 시스템 설계도(UML/SysML)만 입력하면, 보안 등급 분류부터 필수 통제 항목 선정까지 1분 만에 완료합니다.
- **GenAI Documentation:** 하이퍼클로바X가 국방 표준 양식에 맞춰 완벽한 문장으로 보안계획서(SSP)를 작성합니다.
- **Live Audit:** 1년 전 서류가 아닌, 현재 서버의 상태를 실시간으로 진단하여 '살아있는' RMF 대시보드를 제공합니다.

Slide 4: Market Validation (시장 검증)

"왜 지금인가?" (Why Now?)

- 규제의 강제화: 국방정보보호훈령 강화로 모든 무기체계에 K-RMF가 의무 적용됩니다.
- 미국의 선례: Telos, RegScale 등 RMF 자동화 기업들이 유니콘 기업으로 성장했습니다. 한국은 무주공산입니다.
- 국방 AI 정책: 국방부는 2026년까지 AI-ISAC 구축 및 AI 기반 보안 관제 도입을 천명했습니다.

Slide 5: Technology & Moat (기술 및 진입장벽)

"Sovereign AI for Defense"

- **Core Engine:** 네이버 HyperCLOVA X 미세조정(Fine-tuning) 모델 사용. 국방 도메인 특화 학습.
- **Data Security:** 외부망 접속이 필요 없는 On-Premise LLM 구축 기술.
- **Integrations:** 국방망에서 사용되는 국산 보안 솔루션(안랩, 시큐아이 등)과의 독점적 API 연동 어댑터 보유.

Slide 6: Business Model (수익 모델)

- **B2G** (국방부/방사청): 전군 표준 RMF 플랫폼 라이선스 공급 (구축형 + 유지보수).
- **B2B** (방산기업): 프로젝트 단위 연간 구독 모델 (SaaS or On-prem Subscription).
 - *Basic*: 문서 자동 생성 (월 200만 원/User)
 - *Enterprise*: 실시간 모니터링 및 자동 감사 대응 (프로젝트 규모별 책정)

Slide 7: Roadmap (성장 로드맵)

- **Phase 1 (2025)**: 방산혁신기업 100 선정 도전 및 소형 드론 체계 대상 PoC(개념검증) 수행.
- **Phase 2 (2026)**: 방산 중견기업(체계협력업체) 대상 솔루션 납품 및 K-RMF 데이터셋 구축 사업 참여.
- **Phase 3 (2027+)**: 'Big 3' 체계종합업체 전사 도입 및 K-방산 수출 지원(K-RMF to NATO RMF 변환 기능) 런칭.

Slide 8: Financial Projections (재무 추정)

- **Year 1**: 매출 10억 (정부 R&D 과제 및 PoC)
- **Year 3**: 매출 100억 (시장 점유율 5%, 주요 레퍼런스 10곳 확보)
- **Year 5**: 매출 300억 (시장 점유율 20%, 영업이익률 40% 달성)

Slide 9: Team (팀 구성 - 가상의 예시)

- **CEO**: 국방과학연구소(ADD) 출신 무기체계 보안 전문가.
- **CTO**: 대규모 LLM 파이프라인 구축 경험이 있는 AI 엔지니어.
- **Advisor**: 예비역 장성(정보화기획관 역임) 및 대학교수(정보보호학).

6. 결론 및 제언

6.1 사업 타당성 총평

본 연구 결과, **AI 기반 K-RMF** 애이전트 사업은 '매우 유망(Highly Viable)'한 것으로 평가된다.

1. 확실한 수요: 규제에 의해 강제되는 시장(Compliance Market)은 불황이 없다.
2. 명확한 고통: 현행 수작업 방식의 비효율이 극에 달해 있어, 솔루션 도입 시 ROI(투자대비효과) 증명이 쉽다.
3. 경쟁의 공백: 글로벌 솔루션은 보안 문제로 진입이 어렵고, 국내 대기업은 인력 채용에만 몰두하고 있다. 기술 스타트업이 파고들 최적의 타이밍이다.

6.2 성공을 위한 제언

- 초기 진입 전략: 거대 체계업체(한화/LIG)를 바로 뚫으려 하기보다, **'방산혁신기업 100'**이나 '국방벤처 지원사업'을 통해 정부 자금을 지원받으며 기술력을 검증받는 우회 전략이 필요하다.
- 데이터 확보: AI 성능의 핵심은 데이터다. 국방 데이터 인공지능 구축 사업 등에 참여하여 합법적으로 RMF 관련 학습 데이터를 확보하거나, 공개된 미 NIST 데이터를 한국어로 번역/가공하여 초기 모델을 학습시키는 전략(Transfer Learning)이 유효하다.
- 보안 인증: 소프트웨어 자체의 보안성(CC인증, CSAP 등)을 조기에 획득해야 한다. 국방 시장은 기능보다 보안 인증이 진입의 첫 번째 관문이다.

본 보고서가 제안하는 'Sentinel-K' 모델은 단순한 업무 자동화를 넘어, 대한민국 국방 사이버 안보 태세를 '관리형'에서 '지능형'으로 격상시키는 핵심 인프라가 될 잠재력을 가지고 있다.

참고 문헌 (Citations in Text)

본 보고서는 제공된 연구 자료(Research Snippets)에 기반하여 작성되었으며, 각 주장의 근거는 본문 내에 `` 형태로 명시하였다. 주요 참조 자료는 다음과 같다:

- K-RMF 정의 및 프로세스:
- 국방 예산 및 정책:
- 기업 동향(채용, 사업):
- 경쟁 솔루션(Telos, RegScale):
- AI 기술(HyperCLOVA X):

참고 자료

1. K-RMF 조기정착을 위한 방위사업제도 발전방향 - KNST, <http://journal.knst.kr/xml/44553/44553.pdf>
2. 한화시스템, 한미 연합작전의 'AI 지휘관', 연합지휘통제체계(AKJCCS) 성능개량 수주, https://www.hanwha.co.kr/newsroom/media_center/news/news_view.do?seq=15376
3. Exploring Effective Approaches to the Risk Management Framework (RMF) in the Republic of Korea: A Study - MDPI, <https://www.mdpi.com/2078-2489/14/10/561>
4. 2025년 정부 특활비성 예산 2조 1232억 원 - 상호문화뉴스, <https://www.seou1.com/news/articleView.html?idxno=62705>
5. [2025예산] 국방비 60조 돌파...병장 월소득 205만원·KF-21 양산 | 연합뉴스, <https://www.yna.co.kr/view/AKR20240826088900504>
6. 국방AI데이터센터 만든다...2분기 국방 AI기본법도 추진 - Daum, <https://v.daum.net/v/20251215160145882>
7. 취업 정보 - [LIG넥스원] 2024년 상반기 LIG넥스원 공개채용(~3/17), <https://publicad.inha.ac.kr/publicad/7690/subview.do;jsessionid=955E00A98F246B134613DF0F3ACA9DA9?enc=Zm5jdDF8QEB8JTJGYZmJzJTJGcHVibGljYWQIMkYxOTQ1JTJGMTIyNTE3JTJGYXJ0Y2xWaWV3LmRvJTNG>
8. 2025년 하반기 한화시스템 ICT 부문 신입사원 채용, <https://hanwhasystems-ict-recruit.co.kr/>
9. 정보보호 전문서비스(컨설팅/보안관제) 기업 지정현황, https://www.kisa.or.kr/post/fileDownload?menuSeq=1040702&postSeq=1&attachSeq=2&lang_type=KO
10. 주요업무 - 정보통신기반시설보호, https://www.isac.or.kr/sub/02/main_business
11. C·A·S, https://www.casit.co.kr/company/project_performance_1/?v=406&page=108
12. NIST RMF Automation | Risk Management Framework | Xacta - Telos Corporation, <https://www.telos.com/offerings/xacta-risk-management-framework-rmf/>
13. Xacta: We're Changing Cyber GRC - Telos Corporation, <https://www.telos.com/offerings/xacta/>
14. Save \$20M Annually with AI-Powered RMF Automation - RegScale, <https://regscale.com/resource-center/brief-federal-civilian/>
15. OpenRMF - An Open Source Risk Management Framework tool, <https://www.openrmf.io/>
16. naver-hyperclovax (HyperCLOVA X) - Hugging Face, <https://huggingface.co/naver-hyperclovax>
17. Introducing HyperCLOVA X, our state-of-the-art AI models optimized for the Korean language | CLOVA, <https://clova.ai/en/tech-blog/introducing-hyperclovax-x-our-state-of-the-art-ai-models-optimized-for-the-korean-language>
18. A Chatbot that Learns One's Preferences as the Next Step in Human Digital Twins: A Pilot Study Using HyperCLOVA X, a Large Language Model - Fortune Journals, <https://www.fortunejournals.com/articles/a-chatbot-that-learns-onesquos-preferences-as-the-next-step-in-human-digital-twins-a-pilot-study-using-hyperclovax-x-a-large-langu.html>
19. 2025년

공공 SW사업 5조 8316억원 규모...운영사업 위주로 SW기업엔 '적신호',
<http://www.itdaily.kr/news/articleView.html?idxno=229823> 20. 국방부, 통합데이터센터 본격
가동...77개 전산소 2곳으로 - 디지털데일리,
<https://m.ddaily.co.kr/page/view/2015021211130927211> 21. 인텔리박스, '방산혁신기업 100'
선정... 악천후 뚫는 'AI 경계병'으로 국방 혁신 이끈다,
<https://m.boannews.com/html/detail.html?idx=140989> 22. 알림/신청 | 공지사항 -
국방기술품질원,
https://www.dtaq.re.kr/km/notice/notice.jsp?mode=view&article_no=160621&board_wrapper=%2Fko%2Fnotice%2Fnotice.jsp&pager.offset=80&sr:start_date:start_date=&search:search_key:search=article_title&search:search_val:search=&sr:start_date_field:start_date=a.create_dt&sr:end_date_field:end_date=a.create_dt&sr:end_date:end_date=&board_no=25 23. "25년 25년"『
국방벤처 지원사업(일반)』『국방벤처 지원사업(일반)』과제 및 주관기업 모집,
https://www.djdi.or.kr/_files/board/20250214/8f1b7ff30541c4d0163bd3540a38d8e9.pdf 24.
2025년도 초거대AI 확산 생태계 조성 사업(2차) 공고문,
https://www.bizinfo.go.kr/cmm/fms/getImageFile.do;jsessionid=t0ssR9sioehnDN3OPDLwwS3HlizonzarjnIFtoEdraD9iVXUNlwnB02WBED86jUj4.ims_bizwas1_servlet_engine1?atchFileId=FILE_000000000712820&fileSn=1 25. [2506.22403] HyperCLOVA X THINK Technical Report - arXiv,
<https://arxiv.org/abs/2506.22403>