KERC
Korea-EU Research Centre

2025 상반기

KERC SUPPORTERS

유럽 주요 분야별 연구 및 정책 동향

[2025 상반기] 유럽 사이버보안 연구 · 정책 동향

<작성자: 정해식>

<요약>

2025년 상반기 유럽의 사이버보안 연구와 정책 동향은 NIS2 지침의 본격적인 구현을 중심으로 전개되었다. 연구 분야에서는 ENISA가 발표한 'NIS2 기술 구현 지침'과 연례 위협 랜드스케이프 보고서를 기반으로, AI와 IoT 기술을 활용한 실시간 위협 탐지 및 공급망 리스크 평가 모델 개발이 두드러졌다. 특히, DDoS 공격 증가와 공공 인프라 취약성에 대응해 머신러닝 기반 자동화 도구와 리질리언스 프레임워크 연구가 활발히 진행되었으며, Cadmus 프로젝트를 통해 사이버보안 인력 부족 문제를 해소하기 위한 교육 커리큘럼 표준화와 중소기업 지원 실증 사례도 주목받았다.

정책 측면에서는 NIS2의 국가별 전환 과정에서 다수 회원국(19개국)이 지연을 겪으며 EU 위원회로부터 공식 경고를 받았으나, 독일·이탈리아 등 일부 국가는 법안 통합을 완료하며 진척을 보였다. ENISA는 회원국 간 조화를 위한 기술 가이드라인을 배포했고, 2월 발표된 'EU 사이버 위기 관리 블루프린트'는 NIS2의 인시던트 공유 및 대응 체계를 강화하는 국제 협력의 기틀을 마련했다. 또한 Cyber Resilience Act와의 연계 정책이 추진되며, 에너지·교통·제조 등 18개 핵심 부문의 인프라 보호와 리스크 기반 규제가 한층 강화되었다.

이러한 동향은 유럽이 사이버보안의 표준화와 시스템적 복원력을 추구하고 있음을 보여주며, 한국에게는 AI 기반 리스크 관리 기술 도입, 글로벌 공급망 보안 협력 강화, 중소기업 준수 부담 완화를 위한 정책 설계라는 실질적인 시사점을 제공한다. NIS2는 단순한 규제 준수를 넘어, 유럽 디지털 경제의 회복력과 신뢰성을 높이는 핵심 정책으로 자리 잡고 있다.

<Key words> NIS2, ENISA, 리스크 관리, 공급망 보안, 사이버 리질리언스

Ⅰ. 유럽의 사이버보안 연구 동향

□ NIS2 지침에 따른 사이버 리질리언스 모델 개발 연구

ㅇ ENISA의 기술 구현 지침 및 위협 랜드스케이프 분석

- 2025년 상반기 유럽 사이버보안 연구는 NIS2 지침의 구현을 중심으로 사이버 리질리언스(회복력) 강화에 초점
- ENISA(European Union Agency for Cybersecurity)는 6월에 'NIS2 기술 구현 지침'을 발표하며, 회원국들이 국가별로 설정한 사이버 리스크 관리 요구사항을 지원하는 기술 가이드를 제공
- 이 지침은 공급망 보안, 인시던트 대응, 그리고 공급자 리스크 평가를 강조하며, NIS2의 핵심 요구사항인 '관리 및 감독 체계'를 위한 실증적 프레임워크를 제시
- 또한, 2025 ENISA Threat Landscape 보고서는 위협 그룹들이 기존 도구와 기법을 재사용하며 새로운 공격 모델을 도입하는 경향을 분석, NIS2 적용 기업의 실시간 위협 탐지 연구를 촉진함
- 이러한 연구는 AI 기반 자동화 도구 개발로 이어져, 유럽 내 핵심 부문(에너지, 교통 등)의 네트워크 안정성을 높이는 데 기여하고 있음

ㅇ 사이버보안 스킬 갭 해소를 위한 교육 연구

- Cadmus 프로젝트를 통해 유럽의 사이버보안 인력 부족 문제를 다룬 연구가 활발히 진행됨
- 2025년 1분기 보고서에 따르면, NIS2의 공급자 관리 요구로 인해 전문 인력 수요가 급증함에 따라, 교육 프로그램 개발과 스킬 매핑 연구가 강조됨
- 이 연구는 NIS2의 '인적 자원 교육' 조항을 바탕으로, EU 회원국 간 표준화된 커리큘럼을 제안하며, 특히 중소기업(SMEs)의 준수 역량 강화를 위한 실증 사례를 제시

□ AI와 IoT 통합을 통한 NIS2 위협 탐지 연구

ㅇ DDoS 공격 패턴 분석 및 공공 인프라 보호 연구

- ENISA의 2025년 보고서에 따르면, 공공 행정 부문이 해커티비스트의 DDoS 공격 대상으로 급증하며, NIS2의 인시던트 보고 의무를 충족하기 위한 AI 기반 탐지 연구가 두드러짐
- 진행된 연구들은 IoT 기기 취약점과 연계된 NIS2 공급망 리스크를 모델링, 머신러닝 알고리즘을 활용해 실시간 대응 프레임워크를 개발. 예를 들어, Cyber-Resilience Act와의 연계 연구에서 IoT 보안 표준화가 NIS2의 '본질적 엔티티' 보호에 필수적임을 강조

ㅇ 시장 성장과 AI 규제 연계 연구

- 유럽 사이버보안 시장이 2025년 상반기 13% 성장한 가운데, AI 도입과 NIS2 규제 준수를 결합한 연구가 증가
- ECSO(European Cyber Security Organisation)의 백서에서는 NIS2 구현 과제와 우선순위를 분석하며, AI 기반 자동화가 리스크 관리 비용을 절감할 수 있음을 실증
- 이는 NIS2의 '리스크 관리 조치' 조항을 실무적으로 지원하는 방향으로, 공급자 평가와 인시던트 보고 프로세스를 최적화하는 데 초점

□ NIS2 구현 과제에 대한 실증 연구

ㅇ 회원국 전환 추적 및 사례 연구

- ECSO의 NIS2 전환 추적 연구에서 아일랜드(1월), 스웨덴(1월), 이탈리아(2월) 등 국가의 등록 마감이 상반기 초에 집중됨에 따라, 구현 지연 요인 분석 연구가 활발했음
- Nature 저널의 사이버 리질리언스 개념 모델 연구는 NIS2 국가 구현 전략 최종화에 활용 가능성을 제시하며, EU 전체의 조화로운 적용을 위한 프레임워크를 제안
- 이러한 연구는 NIS2의 범위 확대(핵심·중요 엔티티 증가)를 고려해, 중소기업의 준수 부담을 완화하는 실증 데이터를 축적

Ⅱ. 유럽의 사이버보안 정책 동향

□ NIS2 지침의 국가별 전환 및 구현 정책

ㅇ 회원국 전환 지연과 EU 위원회 대응

- 2025년 5월 EU 위원회는 불가리아, 체코, 덴마크 등 19개 회원국에 NIS2 전환 지연에 대한 '이유 있는 의견'을 발송하며, 준수 촉구를 강화
- 상반기 중 독일(2025년 말 시행 예상), 이탈리아(국내 법안 통합 완료) 등 일부 국가에서 정책이 진척됐으나, 전체적으로 중반까지 대부분의 조치 채택이 예상됨
- NIS2는 18개 핵심 부문의 네트워크·정보 시스템 보호를 위한 통합 프레임워크를 구축하며, 리스크 관리와 인시던트 보고 의무를 강화하는 정책 방향을 제시

ㅇ 기술 구현 지침과 리스크 관리 정책

- ENISA의 6월 NIS2 기술 구현 지침은 회원국 국가 요구사항을 지원하며, 운영 리스크 관리, 사이버 위생, 인시던트 대응을 포괄하는 정책 가이드라인을 제공
- 이는 NIS2의 '고도의 공통 사이버보안 수준' 목표를 실현하기 위한 것으로, 공급망 보안과 공급자 리스크 평가를 핵심 정책 요소로 삼음

□ EU 사이버 위기 관리 전략 및 국제 협력 정책

ㅇ EU 사이버 블루프린트(Cyber Blueprint) 정책

- 2월 24일 EU 이사회가 'EU 사이버 위기 관리 블루프린트' 초안을 발표하며, NIS2와 연계된 지역적 사이버보안 협력을 강화함
- 이 정책은 현대적 사이버 위협 대응을 위한 운영적 통합을 강조하며, NIS2의 인시던트 공유 메커니즘을 기반으로 EU 회원국 간 협력을 촉진
- 10월 ITIF 보고서에 따르면, 이 블루프린트는 NIS2와 조화되어 유럽의 사이버 쉴드(보호벽)를 모델화, 국제적 협력 프레임워크로 확장될 전망

ㅇ NIS2와 Cyber Resilience Act 연계 정책

- NIS2는 Cyber Resilience Act와 보완적으로 작용하며, IoT 및 디지털

인프라의 사이버 복원력을 높이는 정책을 추진함

- 2025년 3월 Noerr 업데이트에 따르면, 일부 국가의 구현 지연에도 불구하고 여름~가을 시행을 목표로 정책 조정이 이뤄짐

□ 인프라 보호 및 규제 강화 정책

ㅇ 핵심 인프라 리스크 기반 규제 정책

- 마이크로소프트의 11월 보고서(상반기 동향 반영)에서 NIS2의 리스크 기반 규제가 핵심 인프라 보호의 핵심임을 강조
- 2025년 상반기 정책은 NIS2의 범위 확대(중요 엔티티 포함)를 통해 제조·디지털 서비스 부문 인프라를 강화, 벌금(매출 2%)과 감독 체계를 도입함
- 또한, 9월 항공 산업 사이버 공격 사례를 통해 NIS2 구현 교훈을 정책에 반영, 네트워크화된 인프라의 시스템적 취약점 대응을 우선시함

Ⅲ. 시사점

ㅇ 2025년 상반기 유럽 사이버보안 동향은 NIS2 지침의 본격 구현을 통해 리스크 관리와 국제 협력의 중요성을 재확인

ㅇ 연구 측면에서 AI·IoT 통합과 스킬 개발이 강조된 점은, 한국의 국가 사이버보안 전략(K-사이버보안 프레임워크 등)에서 유사한 기술 도입을 촉진할 수 있으며, 공급망 리스크 평가 모델을 벤치마킹할 가치가 큼

ㅇ 정책적으로는 회원국 전환 지연에도 불구하고 EU 블루프린트와 같은 위기 관리 체계가 안정성을 높인 사례를 통해, 한국은 한-미, 한-EU 협력을 강화해 글로벌 공급망 보호를 위한 다자간 프레임워크를 구축해야 함

ㅇ 궁극적으로 NIS2의 엄격한 준수 요구는 기업의 사이버 복원력을 제고하지만, 중소기업 부담 증가를 고려한 유연한 정책 설계가 필요하며, 이는 한국 기업의 EU 진출 시 경쟁력을 좌우할 전망

※ 참고자료

o 연구 동향 관련

https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups

https://insurance-edge.net/2025/10/01/lets-check-in-on-european-cyber-security-initiatives/

https://www.enisa.europa.eu/news/public-administration-increasingly-targeted-by-ddos-attacks

https://www.sciencedirect.com/science/article/pii/S2212473X25000768

https://securitybrief.co.uk/story/eu-cyber-security-market-up-13-amid-ai-regulation-push

https://ecs-org.eu/?publications=white-paper-nis2-implementation-challenges-and-priorities

https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

https://www.nature.com/articles/s41598-025-12829-3

o 정책 동향 관련

https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

https://hyperproof.io/understanding-the-relationship-between-nis2-and-the-eu-cyber-resilience-act/

https://www.microsoft.com/en-us/security/blog/2025/11/05/securing-critical-infrastructure-why-europes-risk-based-regulations-matter/