KERC
Korea-EU Research Centre

2026년판

KERC SUPPORTERS

유럽 주요 분야별 연구 및 정책 동향

[2025 하반기] 유럽 사이버보안 연구 · 정책 동향

<작성자: 정해식>

<요약>

2025년 하반기 유럽의 사이버보안 연구와 정책 동향은 NIS2의 집행 준비, Cyber Solidarity Act의 시행 개시, 그리고 CRA 중심의 제품 보안 체계 정착을 축으로 전개되었다. NIS2는 EU 18개 핵심 부문에 대한 공통 사이버보안 규제 틀을 제시하며, 회원국 간 협력과 집행을 요구한다. 다만 2025년 5월 유럽위원회는 NIS2의 완전한 전환 미통보를 이유로 19개 회원국에 reasoned opinion(이유 있는 의견)을 발송했고, 이 이슈는 하반기에도 계속 유럽 사이버 정책의 핵심 배경으로 작용했다.

연구 측면에서는 ENISA의 Threat Landscape 2025와 EU의 호라이즌 유럽 / ECCC 2025 프로그램을 중심으로, 공급망 보안, OT/중요 인프라 보호, 그리고 AI 기반 사이버보안 기술이 주요 축으로 나타났다. ENISA는 2025년 판 위협 랜드스케이프에서 2024년 7월 1일부터 2025년 6월 30일까지의 4,875건 incident를 분석했고, 이 중 OT 위협은 18.2%, 공급망 리스크는 10.6%로 제시했다. 동시에 호라이즌 유럽 2025와 ECCC는 EU의 회복력 강화와 핵심 인프라 보호를 목표로 사이버보안 R&I를 지원했고, 특히 Generative AI for Cybersecurity applications에 4,000만 유로를 배정했다.

정책 측면에서는 EU Cyber Solidarity Act가 2025년 2월 4일 발효되며, 유럽 차원의 탐지, 준비, 대응 역량을 제도적으로 강화했다. 이 법은 European Cybersecurity Alert System, Cybersecurity Emergency Mechanism, 그리고 incident review mechanism을 포함하며, 회원국 간 공동 대응을 실질화하는 방향으로 설계되었다. 또한 2025년 11월에는 EU 회원국과 집행위원회가 BlueOLEx 2025에 참여했으며, 이는 새 EU Cyber Blueprint 채택 이후 첫 운영 수준 연습으로 소개되었다.

이러한 흐름은 유럽이 사이버보안을 단순 규제 준수의 문제가 아니라, 운영 보안(NIS2), 제품 보안(CRA), 공동 대응(Cyber Solidarity Act)을 결합한 체계로 발전시키고 있음을 보여준다. 한국에는 공급망 보안, 제품 보안 책임, 중요 인프라 공동 대응 체계라는 측면에서 직접적인 시사점을 제공한다.

<Key words> NIS2, ENISA, Cyber Resilience Act, Cyber Solidarity Act, 공급망 보안

Ⅰ. 유럽의 사이버보안 연구 동향

□ 공급망, OT 중심의 위협 분석 연구 강화

ㅇ ENISA Threat Landscape 2025 기반 연구

- 2025년 하반기 유럽의 연구 담론에서 가장 자주 참조된 기반 자료 중 하나는 ENISA의 Threat Landscape 2025였음
- 동 보고서는 4,875건의 보안사고(incident)를 분석해 EU가 직면한 주요 위협과 동향을 정리했으며, 그 중 OT 위협 18.2%, 공급망 리스크 10.6%를 제시함. 이는 유럽 연구가 단순 IT 침해 대응을 넘어 산업 시스템과 제3자 의존성 리스크를 중심으로 이동하고 있음을 보여줌

ㅇ 핵심 인프라, 회복력 중심의 R&I 투자

- 유럽 집행위원회의 호라이즌 유럽 워크프로그램 2025는 사이버보안 R&I가 EU의 회복력 강화, 핵심 인프라 보호, 사이버 보안사고 대응 능력 향상을 목표로 한다고 명시함. 이에 따라 하반기 연구 흐름은 단순 기술 실험보다, 실제 핵심 인프라와 산업 부문에 적용 가능한 회복력·운영 보안 중심으로 전개되었다고 볼 수 있음

□ AI 기반 사이버보안 기술 연구 확대

ㅇ Generative AI for Cybersecurity applications

- ECCC가 시행한 HORIZON-CL3-2025-02-CS-ECCC 공모는 사이버보안 적용을 위한 생성형 AI(Generative AI for Cybersecurity applications)에 4,000만 유로를 배정하였으며, AI 기술을 활용해 사이버보안을 강화하는 기술·도구·프로세스 개발을 요구함
- 이는 2025년 하반기 유럽 연구가 AI를 실제 보안 운영과 탐지 자동화에 접목하는 방향으로 구체화되고 있음을 보여주는 직접적인 근거

□ NIS2 이행 지원과 인력, 역할 체계 연구

ㅇ NIS2 기술 구현 및 역할 기반 정렬

- ENISA는 2025년 6월 NIS2 기술구현 가이드(Technical Implementation Guidance)를 발간해 NIS2 디지털 인프라, ICT 서비스 관리, 디지털

제공자 분야의 요구사항을 실제로 구현할 수 있도록 실무 가이드를 제공하였음

- 같은 시기 ENISA는 NIS2 의무사항을 ECSF 역할 프로파일과 매핑한 자료를 통해 법·정책 요구를 실제 조직 내 역할과 역량 체계로 연결하는 접근을 제시하였음. 하반기 유럽 연구 및 실무 논의는 이 같은 "정책의 운영화(operationalisation)"에 크게 의존했다고 볼 수 있음

Ⅱ. 유럽의 사이버보안 정책 동향

□ NIS2 집행 준비 및 회원국 전환 압박 지속

ㅇ 19개 회원국에 대한 의견서(reasoned opinion)

- 집행위원회는 2025년 5월 7일 NIS2의 완전한 전환 미통보를 이유로 19개 회원국에 의견서를 발송함. 이는 하반기에도 NIS2 정책 논의가 새 규칙 제정보다는 국가별 법제화 완료와 집행 체계 정비에 초점이 있었음을 보여줌

- 또한 EU 공식 NIS2 페이지는 회원국들이 2024년 10월 18일까지 NIS2를 전환 및 이행해야 했다고 명시

ㅇ NIS2의 적용 범위와 규제 성격

- NIS2는 EU 18개 핵심 부문에 대한 공통 사이버보안 법적 틀을 제공하며 회원국에 국가 사이버보안 전략, 협력, 집행을 요구함. 따라서 2025년 하반기의 핵심은 단순한 선언이 아니라, 어떤 기관이 감독하고 어떤 방식으로 보고 제재·리스크 관리를 시행할 것인지에 대한 실제 집행 구조 정착이었음

□ Cyber Solidarity Act 기반 공동 대응 체계 출범

ㅇ EU 사이버연대법(Cyber Solidarity Act) 발효

- EU Cyber Solidarity Act는 2025년 2월 4일 발효되었으며, EU의 대규모 사이버 위협, 공격에 대한 탐지, 준비, 대응 역량 강화에 목적을 두고 있음. 동 법안은 유럽 사이버보안 경보 시스템(European Cybersecurity

Alert System)과 사이버보안 비상대응 메커니즘(Cybersecurity Emergency Mechanism)을 포함하며, 국가·국경 간 사이버허브(Cyber Hub) 구축의 법적 토대가 됨

ㅇ BlueOLEx 2025와 EU Cyber Blueprint 연계

- 유럽연합의 공식 정책 페이지에 따르면 2025년 11월 4일 회원국 사이버 보안 당국과 집행위원회가 BlueOLEx 2025에 참여하였으며, 이는 새로운 EU Cyber Blueprint 채택 이후 첫 번째 운영 수준 연습
- 동 훈련의 교훈은 향후 EU 차원의 위기 대비 체계에 반영될 예정이라고 설명됨. 즉, 하반기 유럽 정책은 규제만이 아니라 실제 공동 위기 대응 연습까지 연결됨

□ CRA와 제품 보안 규제의 정착

ㅇ 사이버복원력법(Cyber Resilience Act, CRA)의 법적 상태와 적용 일정

- EU 공식 정책 페이지에 따르면 Cyber Resilience Act는 2024년 12월 10일 발효되었으며, 주요 의무는 2027년 12월 11일부터, 보고의무는 2026년 9월 11일부터 적용됨
- CRA는 CE(인증) 마킹과 연계되며 제품의 전체 수명주기에 걸쳐 사이버 보안 요구사항을 부과함. 따라서 2025년 하반기 유럽 정책의 중요한 특징은 CRA가 새로 발효된 법이 아니라, 실제 적용을 준비하는 제품 보안 체계의 기준점으로 자리 잡았다는 점임

ㅇ 설계 단계 보안(Secure-by-design) 및 취약점 대응 의무

- CRA 원문은 제품별 핵심 사이버보안 요구사항과 취약점 대응 의무를 규정하고 있으며, EU 정책 설명 자료는 이를 설계 및 기본설정 단계에서의 보안(secure by design and by default), 자동 보안 업데이트, 보안사고 보고(incident reporting), 제조사의 주의의무(duty of care)로 요약함
- 이는 운영 보안 중심의 NIS2를 넘어 제품 자체의 보안 책임까지 EU 규제가 확장되었음을 보여줌

□ 관리형 보안서비스(MSS) 인증 체계 확대

ㅇ ENISA의 EUMSS 추진

- ENISA 인증 포털은 2025년 4월 말 집행위원회가 ENISA에 MSS(관리형 보안 서비스) 인증제도 초안 마련을 요청했다고 밝혔으며, 2025년 10월에는 EUMSS 초안 작성을 위한 임시 워킹그룹 첫 회의가 열렸다고 공지
- 이는 하반기 실제 정책 움직임이 인증 체계 설계 단계로 진입했음을 보여주는 구체적 근거

Ⅲ. 시사점

○ 유럽 사이버보안 동향

- 2025년 하반기 유럽 사이버보안 동향의 핵심은 NIS2의 집행 정착, Cyber Solidarity Act를 통한 공동 대응 체계화, CRA를 통한 제품 보안 책임 명확화로 요약할 수 있음
- 이는 유럽이 사이버보안을 더 이상 개별 기업의 내부 통제 문제가 아닌, 공급망, 제품, 서비스, 국가 간 협력을 모두 포괄하는 체계로 다루고 있음을 의미

○ 한국에 대한 분명한 시사점

- 공급망 및 제3자 리스크를 법, 감독 체계 안으로 더 명확히 끌어들일 필요가 있음
- 운영 보안뿐 아니라 디지털 제품의 secure-by-design, 취약점 처리, 보고의무를 강화하는 방향의 제품 보안 정책이 중요해지고 있음
- 국가 또는 부문 간 공동 대응 훈련과 허브형 대응 체계는 중요 인프라 보호 측면에서 참고할 가치가 큼. 유럽의 2025년 하반기 흐름은 결국 규제의 확대보다 “규제의 실행 및 운영화”에 더 가까웠다고 평가할 수 있음

※ 참고문헌

[1] https://certification.enisa.europa.eu

[2] https://certification.enisa.europa.eu/news/eu-managed-security-services-certification-drive-cybersecurity-market-2025-06-25_en

[3] https://cybersecurity-centre.europa.eu

[4] https://cybersecurity-centre.europa.eu/funding-opportunities/calls-proposals/increased-cybersecurity-horizon-cl3-2025-02-cs-eccc_en

[5] https://cybersecurity-centre.europa.eu/news/new-eccc-funding-opportunities-under-digital-europe-and-horizon-europe-programmes-are-open-2025-06-12_en

[6] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[7] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

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

[9] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

[10] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

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

[12] https://ec.europa.eu/commission/presscorner/detail/en/inf_25_982

[13] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-6-civil-security-for-society_horizon-2025_en.pdf

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32024R2847

[16] https://research-and-innovation.ec.europa.eu

[17] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

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

[19] https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf

[20] https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025.pdf