사이버안보연구, 3집 1호 2026 여름, 173-219
© 2026 한국사이버안보학회

사이버 위협정보 공유체계 상호운용성 제고 방안:

부처 간 정보 사일로 해소를 중심으로

0301-173219

소정기 | 세종대학교(제1저자)
길총경 | 경희대학교(공동저자)
신규용 | 육군사관학교(교신저자)

논문접수일 2026년 5월 14일 | 논문심사일 2026년 6월 24일 | 게재확정일 2026년 6월 29일

논문 요약

최근 사이버 침해사고는 국가안보, 경제안보, 사회안전에 영향을 미치는 복합적 위험으로 확대되고 있다. 본 연구는 한국의 국가 사이버 위협정보 공유체계가 공공·민간·군·금융·산업 분야별로 운영되면서 부처 간 정보 사일로, 정보 공유 지연, 동일 공격 캠페인에 대한 분절적 인식이라는 한계를 보이고 있음을 분석하였다. 이를 위해 미국, 유럽연합, 북대서양조약기구 사례를 검토하고, 자동화된 정보 공유, 법적 신뢰 기반, 민감도 기반 제한 공유, 조정 거버넌스의 시사점을 도출하였다. 또한, NIEM Cyber Domain 기반 사고보고 정보 구조화, STIX/TAXII 기반 기술 위협정보 자동교환, MITRE ATT&CK· D3FEND 기반 위협정보 의미 해석을 결합한 표준 기반 상호운용성 모델을 제시하였다. 특히, 국가 허브, 부문 노드, 기관 노드의 3계층 연계구조를 통해 분산된 위협정보를 물리적으로 집중시키기보다 표준 기반 정보흐름으로 통합적 상황 인식과 정책 판단에 연결하는 방안을 제안하였다. 결론적으로 국가 사이버 위협정보 공유체계는 단일 플랫폼 구축보다 공통 데이터 모델, 자동교환 표준, 공유통제 기준, 법적 신뢰 기반, 국가 조정 기능, 단계적 운영 검증체계를 결합하는 방향으로 발전해야 한다.

주제어 사이버 위협정보, 정보 사일로, 상호운용성, 국가정보교환모델 사이버 도메인, 국가 사이버안보 거버넌스

Ⅰ. 서론

사이버 침해사고는 더 이상 개별 기관의 기술적 보안 문제에 머무르지 않는다. 최근 사이버 공격은 공공기관, 민간기업, 금융기관, 방위산업체, 군 관련 조직, 핵심기반시설을 동시에 겨냥하며 국가안보, 경제안보, 사회안정에 복합적 영향을 미치는 양상으로 전개되고 있다(국가정보원 2026a; Alaeifar et al. 2024). 특히 공급망 침해, 랜섬웨어, 개인정보 유출, 가상자산 탈취, 피싱 기반 침투, 국가 배후 해킹조직의 장기 정찰 활동은 단일 기관의 대응만으로는 전체 위협의 의도와 범위를 파악하기 어렵게 만든다. 이러한 환경에서 사이버 위협정보의 신속한 공유와 통합 분석은 국가 사이버안보 역량의 핵심 요소로 부상하고 있다.

한국은 공공, 민간, 군, 금융, 산업 분야별로 사이버 위협정보 공유체계를 운영하고 있다. 국가정보원 국가사이버안보센터는 공공부문 사이버 위협 대응과 국가 차원의 상황관리를 담당하고, 한국인터넷진흥원은 민간 침해사고 대응과 사이버 위협정보 공유를 담당한다. 또한 사이버작전사령부는 군사 영역의 사이버 위협 대응을 수행하며, 금융보안원과 산업별 정보공유분석센터는 각 부문별 전문성을 바탕으로 위협정보 공유를 담당한다(국가정보원 2026a; 과학기술정보통신부·한국인터넷진흥원 2023). 이러한 체계는 분야별 전문성과 책임성을 강화한다는 점에서 의미가 있다.

그러나 현재의 구조는 국가 차원의 통합적 사이버 위협정보 공유 생태계라기보다, 각 기관의 법적 권한과 임무 범위에 따라 병렬적으로 운영되는 구조에 가깝다. 이러한 병렬 구조는 평시에는 부문별 전문성을 발휘할 수 있으나, 다부처·다분야 침해사고가 발생할 경우 정

보 사일로, 위협정보 전파 지연, 동일 공격 캠페인에 대한 분절적 인식을 초래할 수 있다. 동일한 공격자가 공공기관, 민간기업, 방위산업체, 금융기관을 연계하여 공격하더라도, 각 기관이 관측한 침해지표와 사고정보가 개별 사건으로만 처리된다면 국가 차원의 통합 상황 인식이 지연될 가능성이 크다.

이 문제는 단순한 정보 공유 플랫폼 부족으로 설명되기 어렵다. 보다 근본적인 문제는 부처와 기관이 생산한 위협정보를 공통된 의미 구조로 정렬하고, 민감도와 신뢰도에 따라 공유 범위를 조정하며, 이를 국가 차원의 상황 인식과 대응 판단으로 연결하는 상호운용성 체계가 충분히 정립되어 있지 않다는 데 있다. 따라서 국내 사이버 위협정보 공유체계의 한계는 기술표준의 부재나 거버넌스의 부재만으로 설명되기 어렵고, 기술표준과 조정 거버넌스가 결합되지 못한 구조적 문제로 이해할 필요가 있다.

본 연구는 이러한 문제의식에 따라 국가 사이버 위협정보 공유체계의 상호운용성 제고 방안을 분석한다. 특히 부처 간 정보 사일로를 해소하기 위한 접근으로 NIEM Cyber Domain(National Information Exchange Model Cyber Domain, 국가정보교환모델 사이버 도메인) 기반 사고보고 정보 구조화, STIX(Structured Threat Information eXpression, 구조화된 사이버 위협정보 표현) 및 TAXII(Trusted Automated eXchange of Intelligence Information, 신뢰 기반 자동화 위협정보 교환) 기반 기술 위협정보 자동교환, MITRE ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge, 공격자 전술·기술·절차 지식체계) 및 D3FEND(Defensive Framework for Evaluating Network Defenses, 네트워크 방어 평가 프레임워크) 기반 위협정보 의미 해석 체계를 검토한다. 이들 표준은 각각 사고보고 정보의 구조화, 침해지표의 자동교환, 공격기법과 대응조치의 의

미 해석을 담당하며, 국가 조정 기능은 이러한 표준 기반 정보흐름을 신뢰 가능한 정책 판단으로 연결하는 역할을 수행한다(NIEM Open n.d.; OASIS 2021a; OASIS 2021b; MITRE n.d.a; MITRE n.d.b).

본 연구의 목적은 세 가지이다. 첫째, 국내 사이버 위협정보 공유체계의 현황과 구조적 한계를 부처 간 정보 사일로 관점에서 분석한다. 둘째, 미국, 유럽연합, 북대서양조약기구의 사이버 위협정보 공유 사례를 검토하여 자동화 공유, 법적 신뢰, 조정 거버넌스 측면의 시사점을 도출한다. 셋째, 기술표준과 국가 조정 기능을 결합한 표준 기반 정보연계체계, 민간 참여를 위한 법적 신뢰 기반, 단계적 도입 전략을 정책적 개선 방향으로 제시한다.

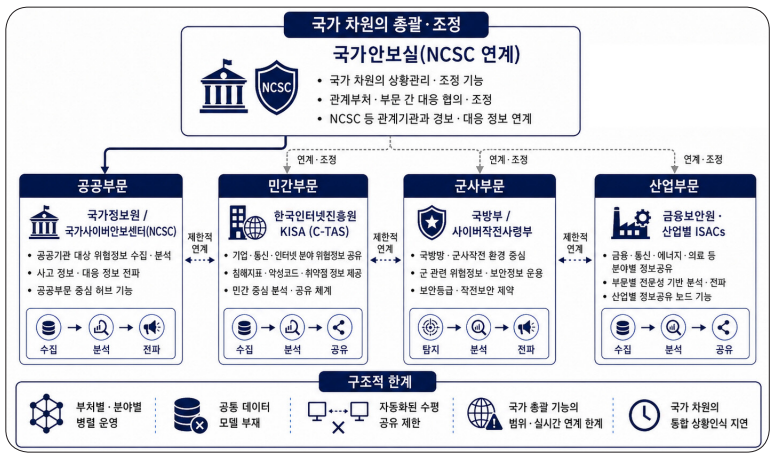
이를 위해 본 논문은 다음과 같이 구성된다. Ⅱ장에서는 국내 사이버 위협정보 공유체계의 현황과 구조적 한계를 분석한다. Ⅲ장에서는 미국, 유럽연합, 북대서양조약기구의 사이버 위협정보 공유체계를 검토하고 정책적 시사점을 도출한다. Ⅳ장에서는 NIEM Cyber Domain, STIX/TAXII, MITRE 지식기반을 중심으로 기술적 상호운용성 확보 방안을 제시한다. Ⅴ장에서는 국가 사이버 위협정보 공유체계 개선을 위한 정책적 제안을 제시한다. 마지막으로 Ⅵ장에서는 연구 결과를 종합하고 향후 과제를 제시한다.

Ⅱ. 국내 사이버 위협정보 공유체계 현황과 구조적 한계

국내 사이버 위협정보 공유체계는 공공, 민간, 군사, 금융, 산업 분야별 전문기관을 중심으로 분산·병렬적으로 운영되고 있다. 국가정

보원 국가사이버안보센터는 공공부문을 중심으로 국가 차원의 사이버 위협정보 수집·분석·전파 기능을 수행하고, 한국인터넷진흥원은 민간 영역의 침해사고 대응과 사이버 위협정보 공유를 담당한다. 또한 군사 영역에서는 국방망과 군사작전 환경을 중심으로 사이버 위협정보 공유·대응 기능이 수행되며, 금융·통신·에너지·의료 등 주요 산업 분야에서는 정보공유분석센터(Information Sharing and Analysis Center, ISAC)가 부문별 위협정보 공유 기능을 수행하고 있다(국가정보원 2025; 과학기술정보통신부·한국인터넷진흥원 2023).

〈그림 1〉 국내 사이버 위협정보 공유체계 운영 구조



출처: 저자 작성(AI 도구(ChatGPT)를 활용하여 시각화 후 검토·수정)

〈그림 1〉은 국내 사이버 위협정보 공유체계의 병렬적 운영 구조를 개념적으로 나타낸 것이다. 이러한 구조는 각 영역의 법적 권한, 보호 대상, 정보 민감도, 사고 대응 절차가 상이하기 때문에 형성된 제도적 구조로 이해할 필요가 있다. 공공부문, 민간부문, 군사부문, 금융·산

업부문은 각각 고유한 임무와 전문성을 갖고 있으므로, 단일기관 중심의 일괄적 통합은 현실적으로 적절하지 않다. 오히려 현행 병렬 구조는 평시에는 분야별 전문성과 책임성을 확보하고, 각 부문이 보유한 현장성을 반영할 수 있다는 장점이 있다. 따라서 국내 체계의 문제는 분야별 정보공유체계가 존재한다는 사실 자체에 있지 않다.

문제는 사이버 침해사고가 부처별·분야별 경계를 따라 발생하지 않는다는 점에 있다. 동일한 공격자가 공공기관, 민간기업, 방위산업체, 금융기관, 핵심기반시설을 연계하여 공격할 수 있으며, 하나의 공격 인프라가 여러 부문에서 동시에 활용될 수도 있다. 이 경우 각 체계가 관측한 침해지표와 사고정보가 부문별 절차 안에서만 처리된다면, 동일 공격 캠페인에 대한 국가 차원의 통합 상황 인식은 지연될 수밖에 없다. 따라서 국내 사이버 위협정보 공유체계의 핵심 과제는 새로운 정보공유체계를 별도로 구축하는 것이 아니라, 기존 분야별 체계를 공통 데이터 구조, 정보 공유 기준, 조정 절차에 따라 연계할 수 있는 상호운용성 구조를 마련하는 데 있다.

1. 국내 사이버 위협정보 공유체계 현황

국내 사이버 위협정보 공유체계는 분야별 전문기관을 중심으로 병렬적으로 운영된다. 공공부문에서는 국가정보원 국가사이버안보센터가 국가사이버위협정보체계(National Cyber Threat Intelligence, NCTI)를 통해 중앙행정기관, 지방자치단체, 공공기관 등을 대상으로 사이버 위협정보를 수집·분석하고 경보와 대응 정보를 전파한다. 또한 국가사이버안보센터는 한국사이버위협정보체계(Korea Cyber Threat Intelligence, KCTI)와 사이버 파트너스 프로그램을 통해 핵심기반시설,

방산, 거래소 등 주요 민간 참여기관과의 위협정보 연계를 수행한다. 민간부문에서는 한국인터넷진흥원이 사이버위협정보분석·공유체계(Cyber Threat Analysis and Sharing, C-TAS)를 통해 기업과 기관에 침해사고 징후, 악성코드, 취약점, 공격 인터넷 주소, 도메인 정보 등을 제공한다. 금융·통신·에너지·의료 등 주요 분야에서는 정보공유분석센터가 부문별 보안관제, 사고 대응, 취약점 분석, 교육훈련, 정보 공유 기능을 수행한다. 군사 영역의 사이버 위협정보 공유·대응은 보안등급, 작전보안, 군사기밀 보호 등 높은 민감도를 전제로 운용된다(국가정보원 2026a; 과학기술정보통신부·한국인터넷진흥원 2023).

이러한 병렬 구조는 분야별 특수성을 반영할 수 있다는 장점이 있다. 그러나 각 체계가 서로 다른 보고 양식, 침해지표 표현 방식, 보안등급, 공유 절차를 사용할 경우, 동일 공격 캠페인이 여러 부문에 걸쳐 발생하더라도 이를 신속히 연계·분석하기 어렵다. 예를 들어 공공기관에서 발견된 피싱 메일, 민간기업에서 확인된 악성코드, 금융기관에서 탐지된 계정 탈취 징후, 군 관련 기관에서 관측된 비정상 접속 시도가 동일 공격자의 활동일 수 있음에도, 각 정보가 개별 사건으로 처리되면 국가 차원의 통합 상황 인식은 지연될 수밖에 없다.

산업별 정보공유분석센터도 동일한 문제를 안고 있다. 정보공유분석센터는 분야별 전문성과 현장성을 확보할 수 있다는 점에서 중요한 기능을 수행하지만, 국가 차원의 공통 데이터 구조와 정보 공유 기준이 충분히 적용되지 않을 경우 분야별 정보 사일로로 고착될 수 있다. 따라서 정보공유분석센터는 단순한 산업별 정보공유 채널이 아니라, 국가 허브와 개별 기관을 연결하는 부문 노드로 자리매김할 필요가 있다.

〈표 1〉은 국내 정보공유분석센터가 산업별로 분산 운영되고 있음

을 보여준다. 이 구조는 각 분야의 위협 특성을 반영하는 데 유리하지만, 부문 간 공통 식별자, 침해지표 표현 방식, 공유등급, 재공유 기준이 정렬되지 않을 경우 동일 공격 캠페인의 횡단적 식별을 어렵게 할 수 있다.

〈표 1〉 국내 ISAC(Information Sharing and Analysis Center) 현황

구 분	운영 주체	회원사 규모	주요 업무
정보통신 ISAC	한국정보통신진흥협회	기간통신사업자 9개	취약점 컨설팅, 통신망 보호 지원
에너지·산업·무역 ISAC	한전KDN	약 53개 기관	보안관제, 사고 대응, 교육훈련
금융 ISAC	금융보안원	약 200개 회원	정보공유, 취약점 분석, 사고 대응
지방자치단체 ISAC	한국지역정보개발원	주요기반시설 92개, 지자체 243개	보안관제, 취약점 점검, 교육훈련
의료 ISAC	사회보장정보원	의료기관 39개	보안관제, 정보공유, 교육훈련

출처: 2025 국가정보보호백서(국가정보원 2025) 참고하여 재작성

2. 부처 간 정보 사일로와 정보 공유 지연 문제

국내 사이버 위협정보 공유체계의 구조적 한계는 부처별 책임 구조와 수직적 정보흐름에서 비롯된다. 국가정보원, 과학기술정보통신부, 국방부, 금융위원회 등은 각각의 법적 권한과 임무 범위에 따라 소관 영역의 사이버 위협정보를 관리한다. 이러한 구조는 책임성과 전문성을 유지하는 데 필요하지만, 다부처·다분야 침해사고에서는 정보공유의 속도와 범위를 제약할 수 있다.

첫째, 동일 공격 캠페인이 분절적으로 인식될 수 있다. 조직화된 공격자는 동일한 악성코드, 유사한 피싱 문구, 공통 명령제어 인프라, 동일 취약점 악용 기법을 여러 부문에서 반복적으로 활용한다. 그러나 각 기관이 관측한 침해지표를 독립 사건으로 처리하면 공격자의 전체 의도, 확산 경로, 피해 범위를 종합적으로 판단하기 어렵다.

둘째, 정보공유가 내부 승인 절차와 법적 책임 우려로 지연될 수 있다. 사이버 위협정보에는 개인정보, 영업비밀, 보안상 민감한 정보, 기관 평판에 영향을 줄 수 있는 사고정보가 포함될 수 있다. 정보 제공 기관은 오탐에 따른 과잉 차단, 재공유 과정의 정보 유출, 평판 훼손, 민원 및 법적 분쟁 가능성을 우려할 수 있다. 이로 인해 신속한 공유보다 내부 검토와 승인 절차가 우선될 가능성이 높다.

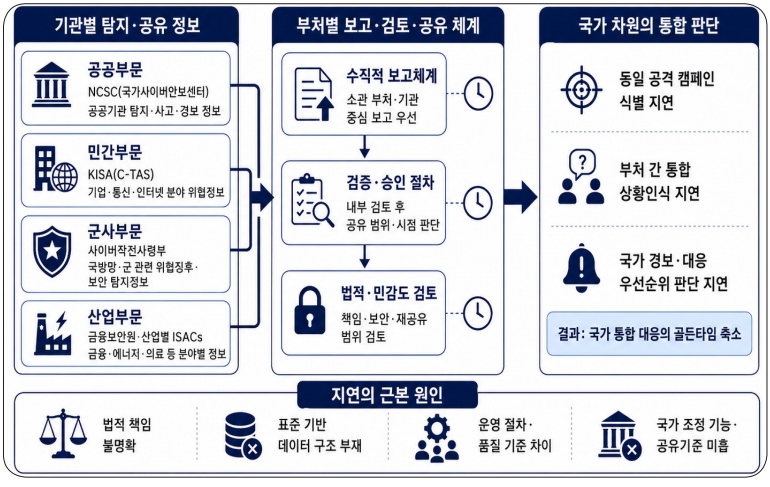
셋째, 데이터 형식과 의미 기준이 다르면 정보가 공유되더라도 즉시 활용되기 어렵다. 기관별로 사고명, 탐지일시, 피해 범위, 침해지표, 대응조치, 공유등급, 출처 신뢰도 등을 서로 다른 방식으로 기록하면 수신기관은 이를 다시 해석하고 변환해야 한다. 이 과정에서 시간 지연과 의미 왜곡이 발생할 수 있다.

넷째, 국가 차원의 조정 기준이 명확하지 않으면 정보공유는 기관별 판단에 의존하게 된다. 어떤 정보를 어느 수준까지 공유할 것인지, 민감정보를 어떻게 비식별화할 것인지, 경보수준을 누가 조정할 것인지, 부처 간 이견이 발생할 경우 누가 최종 판단할 것인지가 불명확하면 정보흐름이 지연될 가능성이 크다.

〈그림 2〉는 이러한 정보 공유 지연 요인을 법·제도, 기술, 운영, 거버넌스 측면에서 종합한 것이다. 법·제도 측면에서는 책임 부담과 민감정보 처리 기준의 불명확성이, 기술 측면에서는 데이터 형식과 침해지표 표현 방식의 차이가 병목으로 작용한다. 운영 측면에서는 정

보품질 검증과 공유 승인 절차의 차이가, 거버넌스 측면에서는 경보 수준 조정과 부처 간 이견 조정 기준의 불명확성이 정보 공유 지연을 심화시킨다. 따라서 부처 간 정보 사일로는 특정 기관의 역량 부족만으로 설명되기 어렵고, 분산된 정보체계를 공통 기준과 조정 절차로 연결하지 못하는 상호운용성 문제로 이해할 필요가 있다.

〈그림 2〉 부처 간 정보 사일로에 따른 사이버 위협정보 공유 지연 문제



출처: 저자 작성(AI 도구(ChatGPT)를 활용하여 시각화 후 검토·수정)

3. 법·제도, 기술, 운영, 거버넌스 측면의 병목 요인

본 연구에서 병목은 단순한 시간 지연이 아니라, 사이버 위협정보가 수집·분석·공유·활용되는 과정에서 정보의 흐름을 지연시키거나 단절시키는 구조적 제약을 의미한다. 따라서 정보 공유 지연은 병목이 작동한 결과이며, 병목은 법·제도, 기술, 운영, 거버넌스 요소가 상

호 정렬되지 않을 때 발생하는 원인 구조로 이해할 수 있다.

이러한 관점에서 부처 간 정보 사일로는 단순히 기관 간 협조 부족으로 발생하는 문제가 아니다. 사이버 위협정보 공유에는 법적 책임, 데이터 구조, 운영 절차, 조정 권한이 동시에 작용하며, 이들 요소가 서로 맞물리지 않을 경우 정보가 공유되더라도 신속한 분석과 공동 대응으로 이어지기 어렵다. 따라서 국내 사이버 위협정보 공유체계의 병목 요인은 법·제도, 기술, 운영, 거버넌스 측면에서 복합적으로 검토되어야 한다.

1) 법·제도적 병목

법·제도적 병목은 기관 간 권한 중첩, 역할 구분의 불명확성, 정보제공기관에 대한 보호장치 부족에서 발생한다. 국내 사이버안보 체계는 공공부문, 민간부문, 군사부문이 서로 다른 법적 근거와 책임 구조에 따라 운영된다. 이러한 구조는 각 영역의 특수성을 반영한다는 점에서 필요하지만, 복합 침해사고 발생 시 어느 기관이 정보공유 범위와 경보수준을 결정할 것인지가 불명확해질 수 있다.

특히 공공기관과 민간기업이 동시에 영향을 받는 사고, 방산업체나 핵심기술 보유기업이 공격받는 사고, 국방 관련 공급망이 침해되는 사고에서는 공공·민간·군의 경계가 명확하지 않다. 이 경우 정보제공기관은 개인정보, 영업비밀, 보안상 민감정보, 평판 훼손, 재공유 책임 등을 우려하여 정보공유에 소극적으로 대응할 수 있다. 따라서 법·제도적 병목의 핵심은 단순한 권한 배분 문제가 아니라, 정보 제공과 활용 과정에서 발생할 수 있는 책임과 보호 기준이 충분히 정리되어 있지 않다는 데 있다.

2) 기술적 병목

기술적 병목은 기관별 데이터 포맷, 스키마, 분류체계, 침해지표 표현 방식이 일치하지 않는 데서 발생한다. 사이버 위협정보는 악성 인터넷 주소, 도메인, 파일 해시값, 취약점 정보와 같은 기술적 침해지표뿐만 아니라, 사고 발생 일시, 피해기관, 대응조치, 정보 출처, 신뢰도, 공유등급 등 정책·행정 정보도 포함한다. 그러나 이러한 정보가 기관별로 서로 다른 형식과 기준에 따라 관리되면 자동화된 연계와 통합 분석은 제한될 수밖에 없다.

기술적 병목은 정보의 공유 여부뿐 아니라, 공유된 정보의 해석 가능성과 활용 가능성에서도 발생한다. 정보가 공유되더라도 수신기관이 이를 즉시 해석하고 활용할 수 없다면 실질적 공유 효과는 낮아진다. 따라서 부처 간 사고보고 정보, 기술적 침해지표, 대응조치 정보가 공통된 의미 구조에 따라 표현되고 교환될 수 있어야 한다. 이 점에서 기술적 병목은 이후 논의할 표준 기반 상호운용성 확보의 직접적 배경이 된다.

3) 운영적 병목

운영적 병목은 정보품질 기준, 민감도 판단, 검증·승인 절차가 기관별로 상이한 데서 발생한다. 사이버 위협정보는 빠르게 전파될수록 방어 가치가 높지만, 부정확하거나 과도하게 공유될 경우 오탐, 불필요한 차단, 정보 유출, 민간 피해를 초래할 수 있다. 따라서 기관은 자동화된 공유보다 내부 검토와 승인 절차를 우선하는 경향을 보일 수 있다.

그러나 이러한 운영 방식은 다부처·다분야 침해사고 상황에서 정보 전파 지연으로 이어질 수 있다. 운영적 개선은 모든 위협정보의 일

괄적 자동 공유가 아니라, 정보의 출처, 정확성, 최신성, 검증 여부, 민감도에 따른 차등적 공유 기준을 마련하는 방향으로 추진되어야 한다. 이를 위해서는 기관별 판단에 의존하는 방식에서 벗어나, 정보품질과 공유 범위를 판단할 수 있는 공통 운영 기준이 필요하다.

4) 거버넌스 병목

거버넌스 병목은 국가 차원의 조정·보증·표준관리 기능이 충분히 제도화되지 않은 데서 발생한다. 사이버 위협정보 공유체계에는 공공기관, 민간기업, 군 기관, 금융기관, 지방자치단체, 연구기관 등 다양한 주체가 참여한다. 이들 주체는 각기 다른 법적 책임, 보안 요구, 정보 민감도, 업무 절차를 갖고 있기 때문에 시스템 연계만으로는 신뢰 기반 정보공유를 보장하기 어렵다.

특히 다부처 침해사고에서는 정보의 신뢰도 검증, 공유 범위 조정, 경보수준 판단, 부처 간 이견 조정, 표준 적용 관리가 필요하다. 그러나 이러한 기능이 명확히 제도화되지 않을 경우 정보공유는 개별 기관의 판단과 협조 수준에 의존하게 된다. 따라서 거버넌스 병목은 기술적 연동의 부재만이 아니라, 분산된 정보흐름을 국가 차원의 상황 인식과 대응 판단으로 연결하는 조정 절차가 충분하지 않은 데서 발생한다.

결국 국내 사이버 위협정보 공유체계의 한계는 개별 기관의 역량 부족으로 환원될 수 없다. 핵심 문제는 법적 책임 구조, 데이터 형식, 운영 절차, 조정 권한이 서로 정렬되지 않아 분산된 위협정보가 국가 차원의 통합 상황 인식으로 전환되지 못한다는 데 있다. 따라서 이후 논의에서는 국외 사례를 통해 자동화된 정보 공유, 법적 신뢰 기반, 조정 거버넌스의 시사점을 검토하고, 이를 바탕으로 표준 기반 상호

운용성 확보 방안을 제시한다.

Ⅲ. 국외 사이버 위협정보 공유체계와 정책적 시사점

국외 주요국과 국제기구는 사이버 위협정보 공유를 기술적 정보교환이 아니라 법적 신뢰, 민간 참여, 조정 거버넌스, 표준 기반 상호운용성이 결합된 정책 영역으로 다루고 있다. 미국은 연방정부와 민간 간 자동화된 침해지표 공유와 책임 완화 장치를 발전시켜 왔고, 유럽연합은 법적 보고 의무와 회원국 간 위기관리 조정체계를 제도화하고 있으며, 북대서양조약기구는 군사·안보 영역에서 신뢰 기반 제한 공유와 절차적 상호운용성을 강조한다.

이 장에서는 미국의 CISA(Cybersecurity and Infrastructure Security Agency, 사이버보안 및 기반시설보안국)와 AIS(Automated Indicator Sharing, 자동화 침해지표 공유), 유럽연합의 NIS2(Network and Information Security Directive 2, 네트워크 및 정보시스템 보안 지침 2)와 ENISA(European Union Agency for Cybersecurity, 유럽연합 사이버보안청) 및 EU-CyCLONe(European Cyber Crises Liaison Organisation Network, 유럽 사이버 위기 연락조직 네트워크), 북대서양조약기구의 사이버 방어 협력 사례를 검토한다. 각 사례는 ① 법·제도 기반, ② 공유 주체, ③ 공유정보, ④ 기술·운영 기반, ⑤ 통제·신뢰 기준, ⑥ 조정체계라는 공통 기준에 따라 비교한다. 이를 통해 각 사례로부터 국내 사이버 위협정보 공유체계의 정보 사일로, 공유 지연, 민감정보 공유 부담, 민간 참여 위축, 국가 조정 기능

불명확성 문제를 완화하기 위한 정책적 시사점을 도출한다.

1. 미국 사례: CISA와 AIS

미국의 사이버 위협정보 공유체계는 연방정부와 민간의 협력을 제도화하는 방향으로 발전해 왔다. 그 중심에는 국토안보부 산하 CISA가 있다. CISA는 연방정부, 주정부, 지방정부, 민간기업, 핵심기반시설 운영기관과 사이버 위협정보를 공유하고, 국가 차원의 사이버 방어 역량을 강화하는 허브로 기능한다(Cybersecurity and Infrastructure Security Agency n.d.). 이러한 구조는 공공기관만으로는 전체 사이버 위협을 조기에 식별하기 어렵고, 민간이 보유한 현장성 높은 침해지표와 관측정보가 국가 사이버 방어에 필수적이라는 인식에 기반한다.

AIS는 이러한 민관 협력 구조를 기술적으로 구현한 체계이다. AIS는 참여기관이 사이버 위협지표와 방어조치를 기계판독 가능한 방식으로 공유·수신할 수 있도록 설계되었으며, STIX/TAXII를 활용하여 침해지표를 표준화된 형식으로 자동 교환한다(Cybersecurity and Infrastructure Security Agency n.d.; OASIS 2021a; OASIS 2021b). 이를 통해 악성 인터넷 주소, 피싱 도메인, 파일 해시값, 명령제어 서버 정보 등 방어 가치의 시간성이 큰 지표를 보안관제, 탐지, 차단 체계에 신속히 반영할 수 있다.

그러나 미국 사례의 핵심은 자동화 기술 그 자체에만 있지 않다. 자동화된 침해지표 공유가 실제로 작동하려면 참여기관이 어떤 정보를 공유할 수 있는지, 개인정보와 민감정보를 어떻게 제거할 것인지, 공유된 정보의 재전파와 활용을 어떻게 통제할 것인지, 정보 제공 과정에서 발생할 수 있는 법적 책임을 어떻게 완화할 것인지가 함께 정리

되어야 한다. 즉, AIS는 기술적 자동교환 체계이지만, 그 지속 가능성은 민간 참여자가 법적 위험을 예측하고 통제할 수 있는 신뢰 기반에 의해 좌우된다.

이러한 법적 기반은 CISA 2015(Cybersecurity Information Sharing Act of 2015, 2015년 사이버보안정보공유법)를 통해 제도화되었다. CISA 2015는 민간기업이 사이버 위협지표와 방어조치를 연방정부 또는 다른 민간 주체와 자발적으로 공유할 수 있도록 하고, 일정 요건을 충족한 공유 행위에 대해 책임 완화, 반독점 보호, 공개 제한, 개인정보 제거 절차 등을 제공하였다. 또한 연방정부가 사이버 위협지표와 방어조치를 수신·처리·전파하는 절차를 마련함으로써, 자동화된 정보 공유가 개인정보 보호와 민간 참여 보호 원칙 안에서 이루어지도록 하였다. 최근 CISA 2015의 효력이 2026년 9월 30일까지 한시적으로 연장된 점은 민간 참여 기반 정보공유체계에서 법적 안정성이 핵심 변수임을 보여준다(Jaikaran 2025; Cybersecurity and Infrastructure Security Agency 2026).

한편 CISA는 AIS 중심의 침해지표 자동교환을 넘어 위협정보 공유체계를 현대화하는 방향도 제시하고 있다. CISA가 추진하는 TIES(Threat Intelligence Enterprise Services, 위협정보 엔터프라이즈 서비스)는 기존 AIS의 자동화 공유 기반을 발전시켜 위협정보의 품질, 맥락, 활용성을 높이려는 시도로 볼 수 있다(Cybersecurity and Infrastructure Security Agency 2023; Department of Homeland Security Office of Inspector General 2025). 다만 공개자료상 TIES의 구체적 기능과 운영 범위는 아직 정립 과정에 있으므로, 이를 AIS를 대체하는 확정된 후속 체계라기보다 기존 자동화 공유의 한계를 보완하기 위한 위협정보 공유 현대화 방향으로 이해하는 것이 적절하다.

미국 사례는 한국에 세 가지 함의를 제공한다. 첫째, 실시간 침해지표 공유에는 STIX/TAXII와 같은 기계판독형 표준과 자동교환 체계가 필요하다. 둘째, 민간 참여를 지속시키기 위해서는 책임 완화, 민감정보 처리, 재공유 제한, 정보 제공자 보호와 같은 법적 신뢰 기반이 병행되어야 한다. 셋째, 정보공유체계는 더 많은 지표를 빠르게 유통하는 수준을 넘어, 정보품질과 맥락, 참여기관별 활용성을 관리하는 방향으로 발전해야 한다. 이 점에서 미국 사례는 자동화된 위협정보 공유가 기술표준, 법적 안정성, 신뢰 기반 운영체계가 결합될 때 실효성을 갖는다는 점을 보여준다.

2. 유럽연합 사례: NIS2, ENISA, EU-CyCLONe

유럽연합의 사이버 위협정보 공유체계는 법적 보고 의무와 조정 거버넌스의 결합을 특징으로 한다. 유럽연합은 다수 회원국으로 구성된 초국가적 체계이므로, 사이버 사고 대응에서 회원국의 권한과 유럽연합 차원의 조정 필요성을 동시에 고려해야 한다. 이러한 배경에서 유럽연합은 NIS2(네트워크 및 정보시스템 보안 지침 2)를 통해 핵심·중요 사업자에 대한 사이버 위험관리와 사고보고 의무를 강화하였다(European Parliament and Council of the European Union 2022).

NIS2 체계에서는 중대한 사이버 사고가 발생할 경우 24시간 이내 초기 경보, 72시간 이내 사고 통지, 1개월 이내 최종 보고를 요구한다. 이러한 구조는 사이버 사고 보고를 자발적 협력에만 의존하지 않고, 일정한 보고 시점과 절차를 법적으로 명확히 했다는 점에서 의미가 있다. 사이버 침해사고는 신속한 공유가 이루어지지 않을 경우 산업과 국경을 넘어 확산될 수 있으므로, 보고 기준의 명확화는 정보공유

의 예측 가능성과 대응의 일관성을 높이는 장치로 기능한다.

ENISA는 유럽연합 차원의 사이버보안 역량 강화, 정책 지원, 사고 대응 협력, 정보공유 촉진 기능을 수행한다. NIS2 체계에서 회원국의 컴퓨터 보안사고 대응팀은 CSIRTs Network를 통해 위협정보 교환과 공동 대응을 수행하며, ENISA는 이러한 협력을 지원하는 역할을 담당한다(European Parliament and Council of the European Union 2022). 또한 EU-CyCLONe은 대규모 사이버 위기 상황에서 회원국 간 운영 수준의 협력, 상황 인식, 의사결정 지원을 촉진하는 네트워크로 기능한다(European Union Agency for Cybersecurity n.d.).

유럽연합 사례를 한국에 그대로 적용할 수는 없다. 유럽연합은 회원국 간 초국가적 조정 구조이고, 한국은 단일 국가 내 부처·기관 간 조정 구조이기 때문이다. 그러나 제도적 맥락의 차이에도 불구하고, 유럽연합 사례는 사이버 위협정보 공유에 법적 보고 기준, 조정 계층, 위기관리 절차가 필요하다는 점을 보여준다. 한국도 다부처·다분야 침해사고에 대해 보고 시점, 보고 항목, 공유 범위, 경보 조정 절차를 명확히 할 필요가 있다. 이는 정보공유를 개별 기관의 자율적 판단에만 맡기지 않고, 국가 차원의 예측 가능한 조정 절차로 발전시키는 데 중요한 함의를 갖는다.

3. NATO 사례: 사이버 방어 정보공유와 상호운용성

북대서양조약기구(North Atlantic Treaty Organization, NATO)의 사이버 방어 협력은 군사·안보 영역의 신뢰와 상호운용성에 기반한다. NATO는 사이버 방어를 억제와 방어태세의 중요한 구성요소로 인식하고 있으며, 회원국 간 정보공유, 훈련, 역량 강화, 모범사례 교환을

강조한다(North Atlantic Treaty Organization n.d.).

NATO의 사이버 방어 협력은 NATO Communications and Information Agency(NCI Agency, 북대서양조약기구 통신·정보기술청)와 NATO Computer Incident Response Capability(NCIRC, 북대서양조약기구 컴퓨터 사고대응 역량) 등 기술·운영 조직을 통해 지원되어 왔다. NCI Agency는 NATO의 통신·정보체계와 사이버 방어 관련 기술 역량을 지원하고, NCIRC는 NATO 네트워크의 사이버 방어와 사고 대응 기능에 관여한다. 또한 NATO는 사이버 방어 훈련과 모의연습을 통해 회원국 간 정보공유 절차, 공동 대응, 절차적 상호운용성을 강화하고 있다.

NATO 사례는 한국의 국내 정보공유체계에 직접 적용되기 어렵다. NATO는 동맹국 간 군사협력체계이며, 정보공유는 회원국 간 신뢰, 보안등급, 작전상 필요성에 의해 강하게 제약된다. 그러나 이 사례는 군사·안보 영역의 사이버 위협정보 공유가 전면 공유가 아니라 민감도와 신뢰 수준에 따른 제한 공유의 원리에 따라 설계되어야 함을 보여준다.

군사·안보 영역에서 생산되는 위협정보는 보안등급, 정보 출처, 작전 민감도, 기관 간 신뢰 수준에 따라 공유 범위가 달라질 수밖에 없다. 따라서 원자료를 전면 공유하는 방식보다는 비식별화된 침해지표, 공격기법, 악성코드 해시값, 공유 가능한 경보 정보 등을 중심으로 제한적 연계를 우선 적용하는 방식이 현실적이다. 이는 군사 영역의 보안 요구를 유지하면서도 공공·민간 영역에서 관측된 위협정보와 연계 가능성을 확보하는 접근이다.

또한 NATO 사례는 상호운용성이 기술적 연결만으로 확보되지 않는다는 점을 보여준다. 사이버 위협정보 공유가 실제 위기 상황에서

작동하려면 표준화된 데이터 형식뿐만 아니라 정보 제공 절차, 공유 승인 기준, 경보 발령 방식, 공동훈련, 모의연습이 함께 마련되어야 한다. 따라서 한국의 국가 사이버 위협정보 공유체계에서도 군사·안보 영역은 신뢰 기반 제한 공유, 절차적 상호운용성, 공동훈련을 결합하는 방식으로 설계되어야 한다.

4. 국외 사례의 시사점

미국, 유럽연합, 북대서양조약기구 사례는 서로 다른 제도적 기반을 갖지만, 사이버 위협정보 공유체계가 갖추어야 할 공통 조건을 보여준다. 〈표 2〉는 세 사례를 제도 기반, 공유 주체, 공유정보, 기술·운영 기반, 통제·신뢰 기준, 조정체계의 관점에서 비교한 것이다.

〈표 2〉 국외 사이버 위협정보 공유체계 비교

구 분	미국	유럽연합	NATO
법·제도기반	CISA 2015	NIS2·Cybersecurity Act	NATO 사이버방어지침
공유주체	연방정부·민간·기반시설	회원국 CSIRTs·핵심사업자	회원국 군사안보기관
공유정보	침해지표·방어조치	사고보고·경보정보	사이버 군사안보 위협정보
기술·운영기반	AIS·STIX/TAXII·MITRE	CSIRTs·EU-CyCLONe	NCIRC·공동훈련
통제·신뢰기준	개인정보 제거·면책·재공유 제한	보고의무·개인정보 보호	보안등급·작전보안
조정체계	CISA	ENISA·EU-CyCLONe	NCI Agency·NCIRC
시사점	자동화 공유와 법적 보호	법정 보고와 조정 거버넌스	제한 공유와 상호운용성

출처: 미국, 유럽연합, NATO 관련 문헌을 바탕으로 저자 정리

〈표 2〉에서 도출되는 시사점은 네 가지로 정리할 수 있다. 첫째, 사이버 위협정보 공유에는 기술적 자동화가 필요하다. 침해지표는 시간이 지날수록 방어 가치가 감소하므로, 문서 중심의 수작업 공유만으로는 신속한 대응에 한계가 있다. 미국 AIS 사례는 STIX/TAXII와 같은 표준 기반 자동교환 방식이 보안관제와 탐지·차단 체계에 위협정보를 빠르게 반영하는 데 유용함을 보여준다.

둘째, 자동화된 정보 공유는 법적 신뢰 기반과 결합되어야 한다. 참여기관이 개인정보, 영업비밀, 평판 훼손, 오탐 책임을 우려한다면 기술적 연동이 가능하더라도 정보 제공은 위축될 수밖에 없다. 따라서 민감정보 제거, 책임 완화, 재공유 제한, 정보 제공기관 보호 기준이 함께 마련되어야 한다.

셋째, 사이버 위협정보 공유에는 운영 통제 기준이 필요하다. 모든 정보를 동일한 수준으로 공유하는 방식은 현실적이지 않다. 정보의 출처, 신뢰도, 정확성, 최신성, 민감도, 재공유 가능성에 따라 공유 수준을 차등화해야 하며, 군사·안보 영역에서는 원자료 공유보다 비식별화된 침해지표와 공격기법 중심의 제한 공유가 적합하다.

넷째, 국가 차원의 조정 거버넌스가 필요하다. 유럽연합과 NATO 사례에서 확인되듯이, 정보공유체계는 단순한 시스템 연계가 아니라 조정 절차와 훈련을 통해 작동성이 확보된다. 한국의 경우에도 국가 허브, 부문 노드, 기관 노드 간 역할을 정렬하고, 경보수준 조정, 공유 범위 판단, 표준 적용 관리, 공동훈련을 제도화할 필요가 있다.

결국 한국의 부처 간 정보 사일로 해소는 특정 기관의 권한 확대나 단일 플랫폼 구축만으로 해결되기 어렵다. 기술적 자동화, 법적 신뢰, 운영 통제, 조정 거버넌스가 결합될 때 국가 사이버 위협정보 공유체계의 상호운용성이 확보될 수 있다.

Ⅳ. 사이버 위협정보 공유를 위한 상호운용성 확보 방안

국가 사이버 위협정보 공유체계의 상호운용성을 제고하기 위해서는 단순한 정보 공유 플랫폼 구축만으로는 충분하지 않다. 공공, 민간, 군사, 금융, 산업 영역의 기관들은 서로 다른 법적 권한, 업무 절차, 데이터 형식, 보안등급을 기반으로 위협정보를 생산·관리한다. 이 경우 정보가 공유되더라도 수신기관이 이를 즉시 해석·분석·활용하기 어렵고, 동일 공격 캠페인에 대한 국가 차원의 통합 상황 인식도 지연될 수 있다.

따라서 사이버 위협정보 공유체계는 기관 간 정보의 의미를 정렬하는 공통 데이터 모델, 침해지표를 기계판독 가능한 방식으로 표현하는 위협정보 표준, 자동화된 교환 방식, 공격기법과 방어조치를 연결하는 지식기반을 함께 갖추어야 한다. 이 장에서는 이러한 관점에서 NIEM Cyber Domain, STIX/TAXII, MITRE ATT&CK, D3FEND를 중심으로 표준 기반 상호운용성 확보 방안을 검토한다.

이들 표준은 서로 다른 정보공유 문제를 해결하는 상호 보완적 관계에 있다. NIEM Cyber Domain은 부처 간 사고보고와 정책·행정 정보의 의미를 구조화하는 데 적합하고, STIX/TAXII는 침해지표와 기술 위협정보를 신속하게 표현·교환하는 데 적합하다. MITRE ATT&CK와 D3FEND는 공유된 위협정보를 공격행위와 방어조치의 공통 언어로 해석하는 데 활용될 수 있다. 따라서 국가 사이버 위협정보 공유체계의 기술적 상호운용성은 단일 표준의 채택이 아니라, 목적별 표준의 역할 분담과 연계 구조를 통해 확보되어야 한다.

1. 기술적 상호운용성의 필요성

부처 간 정보 사일로는 조직적 문제이면서 동시에 데이터 구조의 문제이다. 각 기관이 동일한 침해사고를 인지하더라도 사고명, 탐지 일시, 피해 범위, 침해지표, 대응조치, 공유등급, 정보 출처를 서로 다른 형식으로 기록하면 기관 간 자동 연계와 통합 분석은 제한될 수밖에 없다. 이 경우 정보는 공유되더라도 수신기관이 이를 다시 해석하고 변환해야 하며, 그 과정에서 시간 지연과 의미 불일치가 발생한다.

사이버 위협정보 공유를 위한 기술적 상호운용성은 네 가지 구성요소로 구분할 수 있다. 첫째, 데이터 모델 상호운용성은 사이버 사고, 피해기관, 침해지표, 대응조치, 보고정보, 감사정보를 공통 데이터 항목과 구조로 표현하는 능력이다. 둘째, 위협정보 표현 상호운용성은 악성 인터넷 주소, 도메인, 파일 해시값, 악성코드, 취약점, 공격기법 등을 표준 객체로 표현하는 능력이다. 셋째, 정보교환 상호운용성은 기관 간 위협정보를 문서나 파일이 아니라 표준화된 교환 방식으로 전달하는 능력이다. 넷째, 지식기반 상호운용성은 공유된 침해지표와 사고정보를 공격자의 전술·기술·절차 및 방어조치와 연결하여 해석하는 능력이다.

이러한 구분은 이후 표준 간 역할 분담의 기준이 된다. NIEM Cyber Domain은 데이터 모델 상호운용성을, STIX는 위협정보 표현 상호운용성을, TAXII는 정보교환 상호운용성을, MITRE ATT&CK와 D3FEND는 지식기반 상호운용성을 지원한다. 따라서 기술적 상호운용성은 개별 표준의 단순 도입이 아니라, 정보의 생성·교환·해석·정책 판단으로 이어지는 전체 흐름을 설계하는 문제로 이해되어야 한다.

2. NIEM Cyber Domain 기반 부처 간 정보교환

NIEM은 기관 간 정보교환을 위해 공통 데이터 모델과 어휘를 제공하는 표준적 접근이다(NIEM Open n.d.). 국가 사이버 위협정보 공유체계에서 NIEM Cyber Domain의 핵심 역할은 실시간 침해지표 교환 그 자체가 아니라, 부처 간 사고보고, 피해정보, 대응조치, 기관정보, 공유통제정보, 운영관리정보를 공통 데이터 구조로 정렬하는 데 있다.

기존 국내 체계에서는 공공, 민간, 군사, 산업 영역이 각각의 목적과 절차에 따라 위협정보를 관리한다. 이러한 구조에서 NIEM Cyber Domain은 각 기관의 내부 시스템을 대체하는 표준이 아니라, 기관 간 정보교환에 필요한 공통 중간 언어로 기능할 수 있다. 즉, 개별 기관은 기존 시스템을 유지하되, 대외 공유가 필요한 사고정보는 NIEM Cyber Domain을 참조한 정보교환패키지 형태로 변환하여 국가 허브 또는 부문 노드에 제공하는 방식이다.

NIEM Cyber Domain을 활용할 경우 부처 간 사고보고 정보는 단순 서술형 보고서가 아니라 구조화된 데이터 묶음으로 전환될 수 있다. 예를 들어 사이버 침해사고 보고에는 사고 식별정보, 위협·탐지정보, 피해·영향정보, 대응·복구정보, 기관·협력정보, 공유통제정보, 운영관리정보가 포함될 수 있다. 이러한 항목이 공통 데이터 구조로 정의되면, 국가 허브는 여러 부처와 기관에서 제출한 사고정보를 동일한 기준으로 비교·분석할 수 있다.

〈표 3〉은 NIEM Cyber Domain을 직접 도입하기 위한 완성형 설계안이라기보다, 부처 간 사고정보 교환에 필요한 주요 정보 항목을 참조모델 관점에서 재구성한 것이다. 이 표의 핵심은 사고정보를 단

일 보고서 양식으로 통일하는 데 있지 않다. 오히려 기관별 내부 시스템은 유지하되, 국가 차원의 비교·분석과 조정에 필요한 최소 공통 항목을 정의하는 데 있다. 사고 식별정보는 기관별 사건을 동일 기준으로 추적하게 하고, 위협·탐지정보는 동일 공격 캠페인 식별을 지원하며, 피해·영향정보와 대응·복구정보는 사고의 심각도와 대응 우선순위 판단에 활용될 수 있다. 또한 공유통제정보와 운영관리정보는 민감정보 관리, 재공유 제한, 출처 신뢰도, 감사 가능성을 확보하는 데 기여한다.

다만 NIEM Cyber Domain을 도입한다고 해서 모든 기관의 내부 시스템을 동일하게 변경할 필요는 없다. 현실적으로 각 부처와 기관은 고유한 업무 시스템, 보안정책, 데이터베이스 구조를 유지할 수밖에 없다. 따라서 바람직한 방식은 내부 시스템 통합이 아니라, 기관 간 공유가 필요한 정보에 대해 공통 정보교환패키지를 정의하고, 이를 통해 국가 허브와 부문 노드가 상호운용성을 확보하는 것이다.

〈표 3〉 NIEM Cyber Domain 기반 사이버 사고 정보교환 항목

구 분	주요 정보 항목	정보 교환 목적
사고 식별정보	사고명, 발생·탐지일시, 보고기관, 피해기관, 사건 추적번호	부처와 기관별 사고를 동일한 기준으로 식별하고 국가 허브에서 통합 관리
위협·탐지정보	침해지표, 악성코드, 공격기법, 공격경로, 취약점, 관측데이터	동일 공격 캠페인, 반복 공격기법, 공통 취약점을 다기관 관점에서 비교·분석
피해·영향정보	피해 시스템, 피해 범위, 서비스 영향, 정보 유출 여부, 복구 가능성	사고의 심각도와 국가적 파급효과를 판단하고 우선순위 기반 대응 지원
대응·복구정보	차단조치, 복구조치, 대응상태, 권고, 교훈	기관별 대응 경험을 공유하고 유사 사고 재발 방지 및 공동 대응체계 강화

구 분	주요 정보 항목	정보 교환 목적
기관·협력정보	소관 부처, 부문 노드, 기관 유형, 연락체계, 외부 지원기관	사고 관련 주체와 협력 경로를 명확히 하여 부처 간 조정과 지원체계 구축
공유통제정보	TLP 등급, 재공유 가능 여부, 제공자 표시, 접근권한, 활용 제한	민감정보의 공유 범위와 재배포 조건을 명시하여 통제 가능한 정보공유 보장
운영관리정보	출처 신뢰도, 검증 여부, 최신성, 열람·수정·전파 이력	국가 허브 운영 과정에서 정보품질, 책임성, 감사 가능성을 보완적으로 확보

출처: NIEM Cyber Domain 관련 자료를 참조하여 저자 재구성(NIEM Open n.d.)

3. STIX/TAXII와 MITRE 지식기반을 활용한 사이버 위협정보 체계

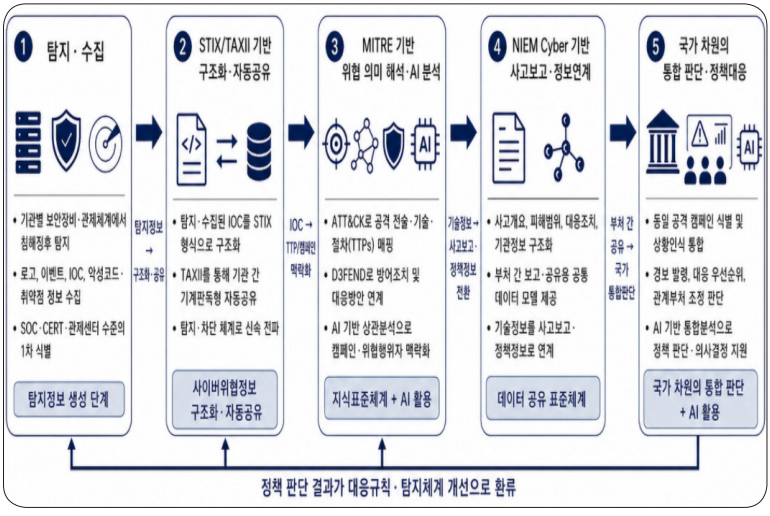
STIX와 TAXII는 기술 위협정보의 표현과 교환을 위한 대표적 표준이다. STIX는 침해지표, 악성코드, 공격기법, 취약점, 공격자, 캠페인 등 사이버 위협정보를 기계판독 가능한 객체로 표현하고, TAXII는 STIX 형식의 위협정보를 기관 간 자동 교환하는 방식으로 활용된다(OASIS 2021a; OASIS 2021b). 악성 인터넷 주소, 파일 해시값, 피싱 도메인, 명령제어 서버 주소와 같은 침해지표는 시간이 지날수록 방어 가치가 감소하므로, 문서 기반 보고보다 표준화된 형식으로 신속히 공유되는 것이 효과적이다.

다만 STIX/TAXII는 기술적 침해지표의 표현과 교환에 강점을 갖지만, 부처 간 정책보고, 법적 책임, 사고 영향도, 피해기관의 특성, 복구상태, 감사정보와 같은 정책·행정 정보를 포괄하는 데에는 한계가 있다. 따라서 STIX/TAXII는 NIEM Cyber Domain과 결합될 때 국가 차원의 정보공유체계에서 더 실질적인 기능을 수행할 수 있다.

공유된 기술 위협정보를 정책적 판단으로 연결하기 위해서는 위협정보의 의미 해석이 필요하다. MITRE ATT&CK는 공격자의 전술·기술·절차를 공통 언어로 정리한 지식기반이며, D3FEND는 식별된 공격기법에 대응하는 탐지, 차단, 완화, 접근통제 등 방어기법을 연결하는 데 활용될 수 있다(MITRE n.d.a; MITRE n.d.b). 기관별로 서로 다른 표현을 사용하더라도 이를 ATT&CK 식별자와 연결하면 동일 공격행위를 같은 기준으로 해석할 수 있고, D3FEND를 통해 대응조치 권고로 확장할 수 있다.

〈그림 3〉은 탐지된 위협정보가 기술적 침해지표에서 정책적 판단정보로 확장되는 과정을 나타낸다. 기관 노드에서 피싱 도메인, 악성파일 해시값, 명령제어 서버 주소와 같은 침해지표가 탐지되면, 해당 정보는 STIX 객체로 표현되고 TAXII를 통해 공유될 수 있다. 이후 MITRE ATT&CK와 D3FEND는 해당 침해지표를 공격기법과 대응조치의 관점에서 해석하며, AI 기반 상관분석은 다수의 침해지표와 공격기법을 연계하여 동일 캠페인 또는 위협행위자 맥락을 식별하는 데 활용될 수 있다. NIEM Cyber Domain은 이를 사고보고, 피해정보, 대응조치, 공유통제정보와 결합하여 부처 간 보고와 정책 판단에 필요한 정보 구조로 확장한다. 즉, STIX/TAXII가 “무엇이 탐지되었는가”를 신속히 공유한다면, MITRE 지식기반과 AI 분석은 “그것이 어떤 공격행위와 캠페인에 해당하는가”를 해석하고, NIEM Cyber Domain은 “어느 기관이 어떤 조치를 해야 하는가”를 구조화한다. 따라서 국가 사이버 위협정보 공유체계는 STIX/TAXII의 속도, MITRE 지식기반과 AI 기반 상관분석의 의미 해석, NIEM Cyber Domain의 정책·행정 정보 구조화를 결합하여 국가 차원의 통합 판단과 정책 대응을 지원하는 방식으로 설계될 필요가 있다.

〈그림 3〉 사이버 위협정보 처리 표준체계 연계 방안



출처: 저자 작성(AI 도구(ChatGPT)를 활용하여 시각화 후 검토·수정)

4. 기술표준 간 역할 분담과 국가 연계모델

앞에서 논의한 표준 기반 연계 구조는 개별 기관의 위협정보를 국가 차원의 통합 상황 인식으로 전환하기 위한 기술적 토대가 된다. 다만 이러한 상호운용성은 특정 표준 하나를 도입하는 방식으로 확보되기 어렵다. 침해지표의 표현과 자동교환, 공격기법의 의미 해석, 사고보고와 정책정보의 구조화, 공유 범위 통제는 서로 다른 기능이기 때문이다. 따라서 국가 사이버 위협정보 공유체계는 목적별 표준과 운영 기준을 계층적으로 조합하는 방식으로 설계되어야 한다.

〈표 4〉는 사이버 위협정보 공유에 활용될 수 있는 주요 표준과 운영 기준의 역할을 정리한 것이다. NIEM Cyber Domain은 부처 간 사고보고와 정책정보 교환을 위한 공통 데이터 구조를 제공하고,

STIX/TAXII는 침해지표와 기술 위협정보의 기계판독형 표현 및 자동교환을 지원한다. MITRE ATT&CK와 D3FEND는 공유된 위협정보를 공격행위와 방어조치의 공통 언어로 해석하는 데 활용될 수 있다. 또한 TLP(Traffic Light Protocol, 정보 민감도에 따른 등급체계)는 재공유 범위와 수신자 통제를 위한 운영 기준으로, N2SF(National Network Security Framework, 국가망보안체계)의 C/S/O(Classified/Sensitive/Open, 기밀/민감/공개) 구분은 국내 정책 환경에서 정보 보호수준을 판단하는 참고 기준으로 활용될 수 있다(국가정보원·국가보안기술연구소 2025).

〈표 4〉의 핵심은 정보유형과 처리목적에 따른 역할 분담에 있다. 기술적 침해지표는 STIX/TAXII를 통해 신속히 교환될 수 있고, 공격행위와 대응조치는 MITRE 지식기반을 통해 공통 언어로 해석될 수 있으며, 사고보고와 정책판단 정보는 NIEM Cyber Domain을 통해 구조화될 수 있다. 여기에 TLP와 N2SF C/S/O와 같은 운영·정책 기준을 보완적으로 적용하면 정보의 민감도, 재공유 가능성, 보호수준을 함께 관리할 수 있다.

〈표 4〉 사이버 위협정보 공유 기술 주요 표준 역할

구분	역할	적용 대상	정책적 의미
NIEM Cyber	부처 간 사고보고 및 정책 정보 교환	사고보고, 피해정보, 대응조치, 감사정보	정보 사일로 완화
STIX	위협정보 객체 표현	침해지표, 악성코드, 취약점, 공격기법	기계판독형 정보 공유
TAXII	위협정보 자동교환	STIX 객체 전송, 위협피드 공유	신속한 전파와 자동화
ATT&CK	공격행위 의미 해석	공격 전술·기술·절차	동일 캠페인 식별
D3FEND	방어조치 연계	탐지·차단·완화기법	대응권고 구체화

구분	역할	적용 대상	정책적 의미
TLP	공유 범위 통제	민감도 등급, 재공유 제한	신뢰 기반 제한 공유
N2SF C/S/O	보호 수준 판단	기밀·민감·공개 정보 구분	국내 보안정책 정합성 확보

출처: NIEM Open(n.d.), OASIS(2021a; 2021b), FIRST(n.d.), MITRE(n.d.a; n.d.b)를 바탕으로 저자 정리

하지만 이러한 표준과 운영 기준은 각각 고유한 적용 범위와 한계를 갖는다. NIEM Cyber Domain은 사고보고와 정책·행정 정보를 구조화하는 데 유용하지만, 실시간 침해지표 자동교환을 직접 수행하는 표준은 아니다. STIX/TAXII는 침해지표와 기술 위협정보의 표현·전송에 강점을 갖지만, 정보 제공자의 법적 책임, 피해기관 보호, 공유 승인 절차, 경보수준 판단을 그 자체로 해결하지는 못한다. MITRE ATT&CK와 D3FEND는 공격기법과 방어조치를 공통 언어로 해석하는 데 기여하지만, 기관 간 정보공유 절차나 공유통제 기준을 대체하지 않는다. 또한 TLP와 N2SF C/S/O는 민감도와 보호수준 판단에 활용될 수 있으나, 기술 위협정보 객체를 표현하거나 자동교환하는 표준은 아니므로 NIEM Cyber Domain 및 STIX/TAXII와 보완적으로 결합 될 필요가 있다.

이러한 역할 분담은 국가 사이버 위협정보 공유체계의 운영 계층과 연계될 때 실질적 효과를 갖는다. 기관 노드는 현장에서 침해지표와 사고정보를 생산하고, 부문 노드는 분야별 맥락에 따라 이를 검증·분석하며 공유 범위와 정보품질을 조정한다. 국가 허브는 부문 노드에서 전달된 정보를 종합하여 동일 공격 캠페인 여부, 국가적 파급 가능성, 경보수준, 후속 대응조치를 판단한다. 이 구조는 모든 원자료

를 중앙에 집중시키는 방식이 아니라, 기관별 정보 생산과 부문별 분석 기능을 유지하면서 국가 차원의 공통 상황 인식을 확보하려는 분산 연계모델이다.

〈표 5〉 한국형 사이버 위협정보 공유체계 3계층 구조와 기능

구 분	주 체	주요 기능
국가 허브	국정원(NCSC), KISA, 사이버작전사	정책수립, 표준관리, 통제·인증, 국가단위 위협정보 분석·평가, 국제연계
부문 노드	공공기관 CERT, ISACs(금융, 통신, 의료 등)	부문별 위협정보 분석·평가, 의사소통·상황 공유 관리, TLP 기반 공유정책 적용, 정보품질 및 메타데이터 운영
기관 노드	지자체, 산·학·연, NGO, 보안조직	침해 탐지·신고·피드백, CTI 소비 및 생산, STIX 객체 생성, TAXII 컬렉션(Collection) 단위 공유

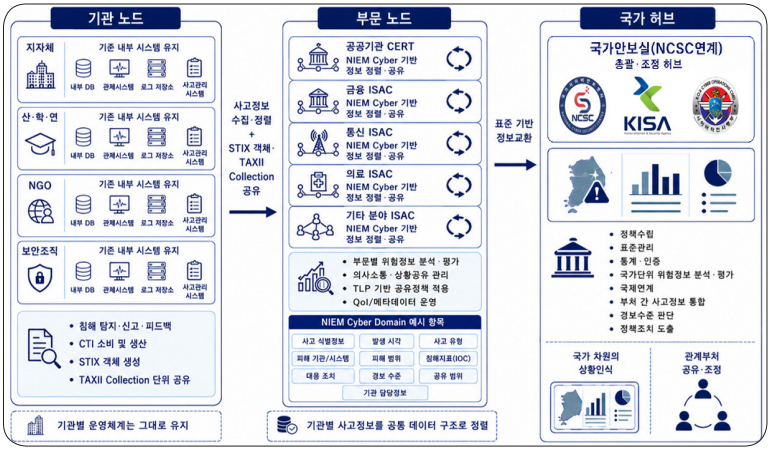
출처: 저자 작성

〈표 5〉는 분산 연계모델을 국가 허브, 부문 노드, 기관 노드의 3계층 구조로 정리한 것이다. 기관 노드는 위협정보를 생산·소비하고, 부문 노드는 분야별 맥락에 따라 이를 분석·평가하며, 국가 허브는 표준화된 정보흐름을 통해 국가 차원의 판단에 필요한 의미를 통합한다. 이때 국가 허브는 개별 기관의 원자료를 모두 집중하는 통제기관이 아니라, 표준 적용, 정보품질 검증, 공유 범위 조정, 경보수준 판단을 지원하는 조정·보증 역할을 담당한다. 따라서 국가 연계모델은 정보를 물리적으로 집중시키기보다, 표준 기반 정보흐름을 통해 분산된 위협정보의 의미를 통합적 상황 인식과 정책 판단으로 연결하는 데 중점을 둔다.

〈그림 4〉는 표준 기반 정보흐름이 기관 노드, 부문 노드, 국가 허브

간에 어떻게 연계될 수 있는지를 보여준다. 기관 노드에서 탐지된 침해지표와 사고정보는 기술 위협정보와 사고보고 정보로 구분·정렬될 수 있다. 부문 노드는 이를 분야별 맥락에 따라 검증하고 공유 범위와 정보품질을 조정한다. 국가 허브는 부문 노드에서 전달된 정보를 종합하여 동일 공격 캠페인 여부와 국가적 파급 가능성을 판단한다. 이 모델의 핵심은 정보의 물리적 집중이 아니라, 공통 데이터 구조와 표준화된 교환 방식에 기반한 의미의 통합이다.

〈그림 4〉 사이버 위협정보 및 사고정보 공유 국가 연계모델 구조도



출처: 저자 작성(AI 도구(ChatGPT)를 활용하여 시각화 후 검토·수정)

기술적 상호운용성은 정책적 통제와 결합될 때 실효성을 갖는다. 표준 기반 교환체계가 마련되더라도 공유 대상, 민감도, 접근권한, 책임 기준이 불명확하면 기관은 정보를 적극적으로 제공하기 어렵다. 반대로 법적 근거가 마련되어도 데이터 형식과 교환 방식이 표준화되지 않으면 정보공유는 수작업 보고와 문서 전파에 머무를 가능성

이 높다. 따라서 국가 사이버 위협정보 공유체계는 기술표준, 공유통제 기준, 정보품질 관리, 조정 절차를 함께 설계해야 한다. 이와 같은 표준 기반 상호운용성 구조는 다음 장에서 논의할 국가 조정 기능, 민간 참여 법적 기반, 단계적 도입 전략의 기술적 토대가 된다.

Ⅴ. 국가 사이버 위협정보 공유체계 개선을 위한 정책적 제안

Ⅳ장에서는 국가 사이버 위협정보 공유체계의 상호운용성을 확보하기 위해 NIEM Cyber Domain, STIX/TAXII, MITRE 지식기반을 목적별로 연계하는 방안을 제시하였다. 그러나 기술표준의 도입만으로 부처 간 정보 사일로가 해소되는 것은 아니다. 표준 기반 정보흐름이 실제 정책 효과로 이어지기 위해서는 공통 정보연계 기준뿐 아니라 국가 차원의 조정 기능, 민간 참여를 위한 법적 신뢰 기반, 단계적 도입과 운영 검증체계가 함께 마련되어야 한다.

이는 앞서 Ⅱ장에서 분석한 국내 사이버 위협정보 공유체계의 병목 요인이 법·제도, 기술, 운영, 거버넌스 요소가 서로 분리되어 작동하는 데서 발생하기 때문이다. 따라서 본 장의 정책 제안은 Ⅱ장에서 도출한 네 가지 병목 요인에 대응하는 실행 방향으로 구성된다.

첫째, 거버넌스 병목은 정보 사일로 해소를 위한 국가 조정 기능 정립과 연결된다. 둘째, 기술적 병목은 표준 기반 부처 간 정보연계체계 구축을 통해 완화될 수 있다. 셋째, 법·제도적 병목은 민간 참여 확대를 위한 법적 신뢰 기반 마련과 관련된다. 넷째, 운영적 병목은 정보품질, 민감도, 검증 절차를 반영한 단계적 도입과 운영 검증체계를 통

해 보완할 필요가 있다.

다만 국가 조정 기능은 기존 기관의 역할을 대체하거나 특정 기관에 권한을 집중하는 방식으로 이해되어서는 안 된다. 국가 허브의 역할은 표준관리, 신뢰도 검증, 공유 범위 조정, 경보수준 조정, 공동훈련 지원 등 조정·보증 기능에 있다. 즉, 기존 전문기관의 기능을 유지하면서도 분산된 정보흐름을 국가 차원의 통합 상황 인식과 대응 판단으로 연결하는 것이 핵심이다.

이에 본 장에서는 국가 사이버 위협정보 공유체계 개선을 위한 정책적 제안을 ① 정보 사일로 해소를 위한 국가 조정 기능 정립, ② 표준 기반 부처 간 정보연계체계 구축, ③ 민간 참여 확대를 위한 법적 신뢰 기반 마련, ④ 단계적 도입과 운영 검증체계 구축의 네 가지 방향으로 제시한다.

1. 정보 사일로 해소를 위한 국가 조정 기능 정립

국가 사이버 위협정보 공유체계의 개선에서 우선적으로 필요한 것은 개별 기관의 역할을 대체하는 새로운 통제기관의 신설이 아니라, 분산된 정보흐름을 국가 차원의 상황 인식과 대응 판단으로 연결하는 조정 기능의 정립이다. 국내 사이버 위협정보 공유체계는 공공, 민간, 군사, 금융, 산업 분야별로 전문기관이 존재하며, 각 체계는 소관 영역에서 필요한 기능을 수행하고 있다. 따라서 정책적 과제는 이러한 분산형 구조를 부정하는 것이 아니라, 각 체계가 생산한 위협정보를 공통 기준에 따라 연계하고 조정하는 데 있다.

국가 조정 기능은 위협 상황 인식, 정보공유 조정, 표준관리의 세 가지 방향에서 설정될 필요가 있다. 첫째, 위협 상황 인식 기능은 여

러 부처와 부문 노드에서 수집한 침해지표와 사고정보를 종합하여 동일 공격 캠페인 여부, 피해 확산 가능성, 국가적 파급효과를 판단하는 역할이다. 둘째, 정보공유 조정 기능은 『국가 사이버보안 기본지침』이 규정한 기관 간 사이버위협정보 공유가 실효적으로 작동하도록 정보의 민감도, 출처 신뢰도, 공유 범위, 재공유 가능성, 경보수준을 조정하는 역할이다(국가정보원 2026b). 셋째, 표준관리 기능은 부처 간 사고보고 항목, 침해지표 표현 방식, 공유통제 기준, 정보품질 기준을 공통 프로파일로 관리하여 기관별 정보체계의 상호운용성을 확보하는 역할이다.

이러한 관점에서 국가정보원 국가사이버안보센터는 공공·민간·군사·산업 영역의 위협정보 흐름을 연결하는 국가 허브 역할을 수행할 수 있다. 다만 그 역할은 모든 원자료를 중앙으로 집중시키는 방식이 아니라, 한국인터넷진흥원, 사이버작전사령부, 금융보안원, 산업별 정보공유분석센터 등 기존 전문기관의 역할을 존중하면서 정보의 신뢰도, 공유 범위, 경보수준, 표준 적용을 조정·보증하는 방식으로 설정되어야 한다. 이 경우 국가 허브는 권한 집중의 수단이 아니라, 부처 간 정보 사일로를 완화하고 국가 차원의 통합 상황 인식을 지원하는 조정 장치로 기능할 수 있다.

2. 표준 기반 부처 간 정보연계체계 구축

부처 간 정보 사일로를 해소하기 위해서는 조직 통합보다 정보교환 구조의 표준화가 우선되어야 한다. 각 기관이 기존 시스템과 업무 절차를 유지하더라도, 대외 공유와 국가 차원의 통합 분석에 필요한 핵심 정보는 공통 항목과 교환 방식으로 정렬될 필요가 있다. 이를 위

해 표준 기반 정보연계체계는 사고보고 정보, 기술 위협정보, 공유통제 정보, 정보품질 정보를 구분하여 설계되어야 한다.

첫째, 부처 간 사고보고 정보의 공통 항목을 정의해야 한다. 사고명, 발생·탐지일시, 피해기관, 피해 범위, 대응조치, 공유등급, 출처 신뢰도, 전파 이력 등은 기관별 양식이 다르더라도 국가 차원의 분석과 조정에 필요한 최소 공통 항목으로 관리될 필요가 있다. 이 영역에서는 NIEM Cyber Domain을 참조하여 정보교환패키지를 설계할 수 있다.

둘째, 기술 위협정보의 자동교환 기준을 마련해야 한다. 악성 인터넷 주소, 파일 해시값, 피싱 도메인, 명령제어 서버 주소 등 방어 가치의 시간성이 큰 침해지표는 STIX/TAXII 기반으로 신속히 공유될 필요가 있다. 다만 자동교환 대상은 모든 정보가 아니라, 비식별화가 가능하고 오탐 또는 민감정보 노출 위험이 낮은 지표부터 우선 적용하는 것이 적절하다.

셋째, 공유된 위협정보의 의미 해석 기준을 마련해야 한다. 동일한 침해지표라도 공격기법, 공격 단계, 방어조치와 연결되지 않으면 국가 차원의 대응 우선순위를 판단하기 어렵다. 따라서 MITRE ATT&CK와 D3FEND를 활용하여 공격기법 태깅, 캠페인 연계 분석, 대응권고 도출 기준을 마련할 필요가 있다.

넷째, 공유통제와 보호수준 판단 기준을 함께 적용해야 한다. TLP는 정보의 재공유 가능 범위와 수신자 통제를 위한 운영 기준으로 활용될 수 있고, N2SF의 C/S/O 구분은 국내 정책 환경에서 정보 보호 수준을 판단하는 참고 기준으로 활용될 수 있다(FIRST n.d.; 국가정보원·국가보안기술연구소 2025). 이는 표준 기반 정보연계체계가 실제 운영될 때 민감도 관리와 접근권한 통제를 보완하는 역할을 수행할 수 있다.

따라서 표준 기반 부처 간 정보연계체계 구축은 기술표준의 채택만을 의미하지 않는다. 국가 허브는 부문 노드와 협의하여 위협정보 공유를 위한 공통 정보교환 프로파일을 관리하고, 기관별 보고 양식과 공통 정보항목 간 매핑 기준을 마련할 필요가 있다. 또한 표준 적용의 우선 대상은 국가 허브, 부문 노드, 주요 공공기관, 주요정보통신기반시설 등 고위험·고영향 기관을 중심으로 설정하고, 이후 민간 참여기관과 산업별 정보공유분석센터로 확대하는 방식이 적절하다. 공유정보의 범위와 수준도 침해지표, 공격기법, 사고보고, 피해정보, 대응조치, 공유통제정보로 구분하고, 정보의 민감도, 신뢰도, 최신성, 재공유 가능성에 따라 차등 적용되어야 한다.

결국 표준 기반 정보연계체계의 목적은 모든 기관의 내부 시스템을 동일하게 바꾸는 데 있지 않다. 핵심은 기관별 내부 체계와 정보 소유권을 유지하면서도, 국가 차원의 공유와 분석에 필요한 정보를 공통 항목과 교환 방식으로 정렬하는 데 있다. 이러한 정책적 관리 기준이 함께 마련될 때 STIX/TAXII, NIEM Cyber Domain, MITRE 지식기반은 단순한 기술표준을 넘어 국가 차원의 정보연계체계로 작동할 수 있다.

3. 민간 참여 확대를 위한 법적 신뢰 기반 마련

사이버 위협정보 공유체계가 실효적으로 작동하기 위해서는 민간기업과 산업별 정보공유분석센터의 적극적 참여가 필요하다. 그러나 민간기업은 침해사고 정보를 공유할 경우 평판 하락, 고객 신뢰 저하, 법적 책임, 영업비밀 노출, 개인정보보호 문제를 우려할 수 있다. 따라서 민간 참여를 확대하려면 단순한 참여 요청이나 기술적 연동보

다 법적 신뢰 기반이 먼저 마련되어야 한다.

민간 참여를 위한 법적 기반은 세 가지 측면에서 설계될 필요가 있다. 첫째, 선의의 정보 제공자 보호이다. 일정한 절차에 따라 비식별화된 위협정보를 제공한 기관에 대해서는 오탐, 과잉 차단, 재공유 과정에서 발생할 수 있는 책임 부담을 합리적으로 완화하는 방안을 검토해야 한다. 둘째, 공유 가능한 정보 범위의 명확화이다. 이미 공개된 악성 인터넷 주소, 피싱 도메인, 악성코드 해시값, 명령제어 서버 주소, 비식별화된 공격기법 등은 저위험 위협정보로 분류하여 신속 공유 대상으로 설정할 수 있다. 반면 피해기관 식별정보, 내부 시스템 취약점, 영업비밀, 개인정보가 포함된 사고정보는 별도의 비식별화와 접근통제 기준을 적용해야 한다. 셋째, 참여 유인 구조의 마련이다. 일정 수준 이상의 정보품질과 보안관리 기준을 충족한 기관에는 고급 위협정보 접근권한, 공동훈련 참여, 침해사고 대응지원, 인증 노드 지정 등의 인센티브를 제공할 수 있다.

이러한 법적 신뢰 기반은 민간의 일회성 협조를 지속 가능한 정보공유 생태계 참여로 전환하는 조건이 된다. 미국의 CISA 2015 사례에서 볼 수 있듯이, 민간 참여 기반 정보공유체계는 기술적 연결성뿐 아니라 책임 완화, 민감정보 처리, 재공유 제한, 정보 제공기관 보호와 같은 법적 안정성에 의해 좌우된다. 한국의 경우에도 민간기업이 정보공유에 따른 위험을 예측할 수 있도록 법적 보호 범위와 운영 절차를 명확히 해야 한다.

4. 단계적 도입과 운영 검증체계 구축

국가 사이버 위협정보 공유체계의 개선은 단계적 접근이 적절하

다. 모든 부처와 기관에 동일한 수준의 자동화와 분석 역량을 요구할 경우 제도적 저항과 운영 부담이 커질 수 있기 때문이다. 따라서 초기에는 위협 수준이 높고 보안관제 역량이 상대적으로 우수한 분야를 중심으로 시범 적용하고, 이후 적용 범위를 확대하는 방식이 현실적이다.

1단계에서는 고위험 분야를 대상으로 표준 기반 정보교환을 시범 적용해야 한다. 이 단계의 핵심은 금융, 통신, 에너지, 방산, 주요 공공기관 등 파급효과가 큰 분야에서 사고보고 항목 매핑, STIX/TAXII 기반 침해지표 교환, 공격기법 태깅, 공유통제 기준이 실제 운영환경에서 작동 가능한지를 검증하는 데 있다.

2단계에서는 공공기관, 지방자치단체, 산업별 정보공유분석센터 등으로 적용 범위를 확대하고, 부문 노드 중심의 운영체계를 정착시켜야 한다. 이 단계에서는 기관별 보고 양식과 국가 공통 항목 간 매핑 규칙을 정교화하고, 정보품질 기준, 접근권한, 재공유 제한 절차를 제도화해야 한다. 또한 국가 허브와 부문 노드 간 경보 조정, 정보 전파, 피드백 절차를 반복적으로 점검할 필요가 있다.

3단계에서는 군사·안보 영역과 국제연계를 확대하되, 민감도 기반 제한 공유 원칙을 적용해야 한다. 군사·안보 영역은 보안등급, 작전보안, 정보 출처 보호 요구가 높기 때문에 원자료 전면 공유보다 비식별화된 침해지표, 공격기법, 경보정보 중심의 연계를 우선 검토하는 것이 적절하다. 국제연계 역시 공유 가능 정보와 보호 대상 정보를 구분하고, 표준 기반 교환 방식과 공유통제 기준을 적용하는 방향으로 추진되어야 한다.

단계적 도입은 공동훈련과 운영 검증체계로 보완되어야 한다. 다부처 침해사고 시나리오를 기반으로 정보 전파 시간, 경보 조정 소요

시간, 중복 보고 감소, 오탐 처리율 등을 평가하고, 그 결과를 표준 프로파일과 기관별 역할 조정에 반영할 필요가 있다.

Ⅵ. 결론

본 연구는 국가 사이버 위협정보 공유체계의 한계를 부처 간 정보 사일로의 관점에서 분석하고, 이를 개선하기 위한 표준 기반 상호운용성 및 조정 거버넌스 방안을 제시하였다. 국내 사이버 위협정보 공유체계는 공공, 민간, 군, 금융, 산업 분야별로 일정한 운영 기반을 갖추고 있으며, 이러한 분산형 구조는 각 영역의 법적 권한, 업무 전문성, 정보 민감도, 대응 절차를 반영한다는 점에서 불가피한 측면이 있다. 그러나 다부처·다분야 침해사고가 증가하는 환경에서는 개별 체계가 병렬적으로 운영되는 것만으로 국가 차원의 통합 상황 인식과 신속한 공동 대응을 보장하기 어렵다.

본 연구의 핵심 주장은 다음과 같다. 국내 사이버 위협정보 공유체계의 한계는 단순한 플랫폼 부족이나 기관 간 협조 부족만의 문제가 아니다. 보다 근본적으로는 법적 책임 구조, 정보 공유 기준, 데이터 형식, 사고보고 절차, 경보 발령 체계, 기술표준 적용 수준이 충분히 정렬되지 않은 상호운용성의 문제이다. 따라서 국가 사이버 위협정보 공유체계는 개별 기관의 전문성과 정보 소유권을 인정하면서도, 부처와 부문을 넘어 필요한 정보를 공통 데이터 구조, 표준화된 교환 방식, 공유통제 기준, 조정 절차를 통해 연결하는 방향으로 발전해야 한다.

이러한 관점에서 본 연구는 세 가지 기여를 제시하였다. 첫째, 국내

사이버 위협정보 공유체계의 한계를 법·제도, 기술, 운영, 거버넌스 요소가 결합된 상호운용성 문제로 재구성하였다. 둘째, 미국, 유럽연합, NATO 사례를 통해 자동화된 정보 공유, 법적 신뢰 기반, 민감도 기반 제한 공유, 조정 거버넌스의 필요성을 도출하였다. 셋째, NIEM Cyber Domain, STIX/TAXII, MITRE ATT&CK·D3FEND를 목적별로 연계하여 사고보고 정보의 구조화, 기술 위협정보의 자동교환, 공격기법과 대응조치의 의미 해석을 결합하는 다층적 상호운용성 모델을 제안하였다.

정책적으로는 국가정보원 국가사이버안보센터를 중심으로 한 국가 조정 기능의 제도적 정립이 중요하다. 이 기능은 모든 정보를 중앙에 집중시키거나 기존 전문기관의 역할을 대체하는 방식으로 이해되어서는 안 된다. 국가 허브는 개별 기관의 정보 소유권과 분야별 전문성을 존중하되, 정보의 신뢰도 검증, 공유 범위 조정, 경보수준 판단, 표준 적용 관리, 공동훈련 지원을 수행하는 조정·보증 주체로 기능해야 한다. 이를 위해 저위험 위협정보의 공유 범위, 선의의 정보 제공자 보호, 비식별화 기준, 재공유 통제, 접근권한 관리, 정보품질 기준을 명확히 할 필요가 있다.

한편 본 연구는 구체적인 정보교환패키지 설계, STIX/TAXII 객체와 NIEM Cyber Domain 항목 간 매핑, MITRE ATT&CK·D3FEND 기반 공격기법·대응조치 태깅 방식, 정보품질 평가체계의 실증 검증까지 수행하지는 못하였다. 또한 국가 허브, 부문 노드, 기관 노드 간 역할 분담과 책임 범위는 실제 법령, 지침, 기관별 권한 구조에 따라 달라질 수 있으므로 추가적인 법제 검토가 요구된다.

향후 연구와 정책 추진에서는 금융, 통신, 에너지, 방산, 주요 공공기관 등 고위험·고영향 분야를 대상으로 시범 적용과 공동훈련을 우

선 추진할 필요가 있다. 이 과정에서 사고보고 항목 매핑, STIX/TAXII 기반 침해지표 교환, MITRE 기반 공격기법 태깅, TLP 및 N2SF C/S/O 기반 공유통제 기준을 적용하고, 정보 전파 시간, 경보 조정 소요시간, 중복 보고 감소, 오탐 처리율, 정보품질 개선 정도를 평가해야 한다. 이러한 단계적 검증을 통해 국가 사이버 위협정보 공유체계는 정보 전달 체계를 넘어, 분산된 위협정보를 국가 차원의 판단과 대응으로 연결하는 상호운용적 사이버안보 거버넌스로 발전할 수 있을 것이다.

〈참고문헌〉

과학기술정보통신부·한국인터넷진흥원. 2023.『국가 차원의 침해사고 대응을 위한 사이버 위협 인텔리전스(Cyber Threat Intelligence) 분석 및 정보공유 기술 개발』.

국가정보원. 2025.『2025 국가정보보호백서』. 서울: 국가정보원.

국가정보원. 2026a.『2026 국가정보보호백서』. 서울: 국가정보원.

국가정보원. 2026b.『국가 사이버보안 기본지침』. 서울: 국가정보원.

국가정보원·국가보안기술연구소. 2025.『국가 망 보안체계 보안 가이드라인』. 서울: 국가정보원.

Alaeifar, Payam, Surya Nepal Pal, Zahra Jadidi, Mohammad Hussain, and Ernest Foo. 2024. "Current Approaches and Future Directions for Cyber Threat Intelligence Sharing: A Survey." Journal of Information Security and Applications 83: 103786.

Cybersecurity and Infrastructure Security Agency. 2023. "Enabling Threat-Informed Cybersecurity: Evolving CISA's Approach to Cyber Threat Information Sharing." https://www.cisa.gov/news-events/news/enabling-threat-informed-cybersecurity-evolving-cisas-approach-cyber-threat-information-sharing(검색일: 2026.6.27.).

Cybersecurity and Infrastructure Security Agency. 2026. "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities." https://www.cisa.gov/resources-tools/resources/guidance-assist-non-federal-entities-share-cyber-threat-indicators-and-defensive-measures-federal (검색일: 2026.5.13.).

Cybersecurity and Infrastructure Security Agency. n.d. "Automated Indicator Sharing (AIS)." https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais (검

색일: 2026.6.27.).

Department of Homeland Security Office of Inspector General. 2025. CISA Has Not Finalized Plans for Automated Cyber Threat Information Sharing Beyond Cybersecurity Act of 2015 Expiration. OIG-25-46. Washington, DC: Department of Homeland Security. https://www.oig.dhs.gov/reports/2025/cisa-has-not-finalized-plans-automated-cyber-threat-information-sharing-beyond-cybersecurity-act-2015-expiration/oig-25-46-sep25

European Parliament and Council of the European Union. 2022. "Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union." Official Journal of the European Union.

European Union Agency for Cybersecurity. n.d. "EU-CyCLONe." https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone (검색일: 2026.6.27.).

FIRST. n.d. "Traffic Light Protocol (TLP): Standards Definitions and Usage Guidance, Version 2.0." https://www.first.org/tlp/ (검색일: 2026.6.27.).

Jaikaran, Chris. 2025. The Cybersecurity Information Sharing Act of 2015: Expiring Provisions. Washington, DC: Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF12959 (검색일: 2026.6.27.).

MITRE. n.d.a. "ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge." https://attack.mitre.org/ (검색일: 2026.6.27.).

MITRE. n.d.b. "D3FEND: A Knowledge Graph of Cybersecurity Countermeasures." https://d3fend.mitre.org/ (검색일: 2026.6.27.).

NIEM Open. n.d. "NIEM Open." https://niemopen.org/ (검색일: 2026.6.27.).

North Atlantic Treaty Organization. n.d. "Cyber Defence." https://www.nato.int/cps/en/natohq/topics_78170.htm (검색일:

2026.6.27.).
OASIS. 2021a. STIX Version 2.1. Committee Specification 01. OASIS. https://www.oasis-open.org/standard/6426/ (검색일: 2026.6.27.).
OASIS. 2021b. TAXII Version 2.1. Committee Specification 01. OASIS. https://www.oasis-open.org/standard/taxii-version-2-1/ (검색일: 2026.6.27.).

Enhancing Interoperability in Cyber Threat Intelligence Sharing

: Overcoming Interagency Information Silos

Jung Ki So | Sejong University
Chongkyung Kil | Kyung Hee University
Kyuyong Shin | Korea Military Academy

Recent cyber incidents have evolved beyond the technical security problems of individual organizations into complex risks affecting national security, economic security, and social stability. This article analyzes the limitations of Korea's national cyber threat intelligence sharing system, focusing on information silos, delayed information sharing, and fragmented recognition of common attack campaigns across the public, private, military, financial, and industrial sectors.

The study examines cases from the United States, the European Union, and the North Atlantic Treaty Organization, deriving policy implications for automated information sharing, legal trust mechanisms, sensitivity-based limited sharing, and coordination governance. It then proposes a standards-based interoperability model that combines incident report structuring through the National Information Exchange Model Cyber Domain, automated technical threat intelligence exchange using Structured Threat Information eXpression and Trusted Automated eXchange of Intelligence Information, and semantic interpretation through MITRE ATT&CK and D3FEND. The model further emphasizes a three-tier linkage structure among a national hub, sectoral nodes, and institutional nodes, through which distributed threat information can be connected to integrated situational awareness and policy decision-making without physically centralizing all raw data.

In conclusion, Korea's national cyber threat intelligence sharing system should evolve by combining common data models, automated exchange standards, sharing-control criteria, legal trust mechanisms, national coordination functions, and phased operational validation rather than by building a single centralized platform.

Keyword Cyber Threat Intelligence, Information Silo, Interoperability, National Information Exchange Model Cyber Domain, National Cybersecurity Governance

* I would like to thank the reviewers for their valuable comments, which helped improve the completeness of this paper.