

# 대한민국 사이버안보 영향 분석 및 정책 대응 검토서

국방·정보·공공 영역의 AI 연산기반 주권, 폐쇄망 운용, 수출통제 역외적용을 중심으로

|      |                     |       |                            |
|------|---------------------|-------|----------------------------|
| 문서번호 | NCSL-PR-2026-09-021 | 작성기준일 | 2026년 9월 21일               |
| 발간기관 | 사이버안보연구소(NCSL)      | 대상 독자 | 국방부·국정원·과기정통부·방위사업청<br>·국회 |

본 검토서는 법률자문이 아니며, 미국 의회 서류·통과 법안의 공개 원문과 위원회 경과를 바탕으로 대한민국 사이버안보 태세에 미치는 구조적 영향을 분석한 정책 의견이다. 조달·조약·수출통제 실무 확정 전에는 전문 법무 검토와 정부 간 협의 채널의 확인이 필요하다.

## 1. 결론 — 세 가지 국가안보 충격

Chip Security Act(CSA, H.R. 3447)와 Remote Access Security Act(RASA, H.R. 2683)는 표면상 대중국 우회반출 차단 법안이다. 그러나 대한민국 입장에서 이 두 법안은 '중국 문제'가 아니라 '동맹국 내부의 사이버·AI 주권 문제'로 작동한다. 국방·정보기관의 폐쇄망 AI, 국가중요시설의 위치정보, 군 부대 단위의 연산자산 배치가 미국 수출통제 행정의 기록·검증 대상이 될 수 있기 때문이다.

연구소가 판단하는 실질 충격은 다음 세 층이다.

### 첫째, 국방 사이버·AI 역량의 물리적 기반이 외국 행정권에 종속된다

CSA의 대상 품목은 ECCN 3A090, 3A001.z, 4A090, 4A003.z 및 후속·유사 분류로 한정된다. 국방·공공 분야의 고성능 AI 가속기가 이 분류에 들어가면, 한국 영토 안의 한국 기관 간 이전(in-country transfer) 까지 미국법이 규율한다. 위치검증 탑재, 소재·최종사용자 기록, 변조 시도 보고가 패키지로 따라온다. 이는 하드웨어 조달 문제가 아니라 사이버작전부대·국방 AI 학습·탐지 체계의 지속가능성 문제다.

### 둘째, 폐쇄망·에어갭이라는 한국형 사이버안보 설계원리와 정면 충돌한다

국가사이버안보센터 체계, 국방 정보통신망, N2SF(국가 망 보안체계) 모델, 군 전용망은 '외부 콜백을 허용하지 않는 것'을 보안의 핵심으로 삼아 왔다. CSA의 위치검증은 주기적 소재 확인을 전제하고, §4(a)(2)(C)는 변조 '시도'까지 보고 대상으로 삼는다. 폐쇄망에서 발생하는 타임아웃·경로이상·전원차단은

모두 잠재 보고 이벤트가 된다. 오탐을 구조적으로 배제하지 못하면, 안보망 운용이 곧 미국 상무부 보고 의무가 된다.

### 셋째, 최종사용자 기록과 워크로드 검증은 군사기밀·보안업무 체계와 양립하기 어렵다

§4(c)(2)는 대상 제품의 소재지와 '현재 최종사용자'를 미국 상무부가 기록할 수 있게 한다. 어느 부대·어느 정보기관이 어떤 AI 연산능력을 언제 도입했는지는 그 자체로 군사기밀보호법과 보안업무규정의 보호대상이 될 수 있다. 2차 메커니즘으로 워크로드 검증이 채택되면, 질문은 '어디에 있는가'에서 '무엇을 돌리는가'로 확장된다. 이 지점에서 미국산 고성능 가속기 기반 국방 AI는 기술적 문제가 아니라 주권적으로 성립이 어려워진다.

대응의 원칙은 회피가 아니라 분리와 주권화다. 일반 공공·민수 영역은 동맹 수출통제 질서 안에서 관리되, 국방·정보 영역의 연산기반은 임계값 설계·오프라인 증적·국산 NPU 경로를 주권 요건으로 재정 의해야 한다. 계약 조항만으로는 국내법 충돌이 해소되지 않는다.

| 영향 영역           | CSA            | RASA              | 국가안보 함의                             |
|-----------------|----------------|-------------------|-------------------------------------|
| 국방 AI·사이버작전 가속기 | 최고 — ECCN 중속   | 중 — 원격유지보수·협력개발   | 위치·최종사용자 기록이 부대 역량 시계열 정보가 됨        |
| 국가중요시설·폐쇄망      | 최고 — 위치검증·오탐보고 | 낮음~중              | 에어갭 원칙과 외부 콜백 의무의 구조적 충돌            |
| 공공·금융 온프레임 AI   | 중 — BOM·이전 트리거 | 중 — 클라우드 원격 접근    | 조달·이전·외주 인력 스크리닝 부담 증가              |
| 민수 클라우드·SaaS    | 낮음~중           | 중~높음 — 제공 행위 포함   | 한국 기업이 외국인에게 미국산 통제품목 접근을 '제공'하면 규제 |
| 국산 모델·자체 호스팅    | 비해당(품목 밖)      | 낮음 — 외부 의존 0이면 유리 | 모델 가중치 통제로 표적이 이동할 경우 증적체계가 방어자산이 됨 |

표의 영향도는 법 제정·BIS 최종규칙 전제를 둔 정책 평가이며, 개별 자산의 ECCN 확정 전에는 가정에 기반한다.

## 2. 법안 개요와 입법 현황

### 2.1 Chip Security Act (H.R. 3447)

2025년 5월 15일 하원 발의, 2026년 3월 26일 하원 외교위원회가 대체안(ANS) 형태로 42-0 만장일치가 결하였다. 2026년 9월 현재 하원 본회의 대기, 상원 동반법안은 은행위에 계류 중이다. 국방수권법 패

키지 병합 가능성은 열려 있으나 확정되지 않았다.

핵심 구조는 이렇다. 대상 첨단 집적회로·가속기에 대해 (1) 수출·재수출·국내이전 전 위치검증 메커니즘 탑재, (2) 지정 위치 이탈·전용·변조 또는 변조 시도의 신속 보고, (3) 이미 이전된 제품의 소유권·소재·현재 최종사용자 기록 유지, (4) 2차 보안 메커니즘(변조방지, 워크로드 검증, 불법취득 시 기능변경 등) 평가 후 의무화 가능성을 부여한다. 제정 시 1차 위치검증은 180일 클럭이 시작된다.

## 2.2 Remote Access Security Act (H.R. 2683)

2026년 1월 12일 하원을 369-22로 통과하여 상원 은행위에 회부되었다. 상원 동반법안은 S. 3519(2025.12.17. 발의)이다. 법 전체는 ECRA(2018 수출통제개혁법) 개정 지시문이며, 독립 실체 조항은 사실상 원격접근을 수출통제 대상 행위에 편입하는 것이다.

‘원격접근’ 정의에는 고의·인지·미필적 고의뿐 아니라 과실에 기반한 접근이 포함되고, ‘제공 행위’ 자체가 규제 대상으로 명시된다. 한국이 우려국이 아니더라도, 장관이 중대한 위험이 있다고 판단하면 규칙으로 포섭할 수 있는 구조다. 자기집행적이지 않으므로 BIS 규칙 제정까지 12~18개월의 실질 유예가 예상된다. 행정·민사 제재는 과실만으로 발동할 수 있다.

## 2.3 왜 한국 사이버안보의 의제가 되는가

두 법안은 중국·우려국 우회를 명분으로 하지만, 적용 단위는 ‘미국 관할 품목’과 ‘미국 관할 접근’이다. 한국은 최대 동맹 수입국이자 미국산 AI 가속기·서버의 집약 운용국이다. 국방 AI, 사이버작전지휘, 공공 폐쇄망 SIEM·탐지, 국가핵심기반시설의 예지보전·이상탐지가 모두 이 하드웨어와 원격 유지보수 경로 위에 서 있다. 따라서 법안의 직접 타깃이 한국이 아니어도, 한국 사이버안보 태세의 물리적·운영적 전제가 흔들린다.

| 구분      | 현황 (2026-09-21)        | 한국 측 실무 의미                                       |
|---------|------------------------|--------------------------------------------------|
| CSA 하원  | 외교위 42-0 가결, 본회의 대기    | 위원회 보고본(RH) 문구가 IH 원안과 다를 수 있음. 계약·훈령 인용 전 대조 필수 |
| CSA 상원  | 은행위 계류 (S.1705 계열)     | 제정 시점 미정. 2026년 내 제정 / 교착 / NDAA 병합 3시나리오        |
| RASA 하원 | 2026-01-12 통과 (369-22) | 입법 동력은 CSA보다 앞선 상태                               |
| RASA 상원 | 은행위 회부, S.3519 병행      | 규칙 제정 전 의회 통보 창구(§3)가 조기경보                       |

| 구분    | 현황 (2026-09-21)           | 한국 측 실무 의미                          |
|-------|---------------------------|-------------------------------------|
|       |                           | 포인트                                 |
| 실효 시점 | 제정 ≠ 즉시 의무. BIS 최종규칙이 경계선 | 국방 조달·이전 계획의 기준일은 제정일이 아니라 최종규칙 발효일 |

### 3. 대한민국 사이버안보 체계와의 접점

한국 사이버안보는 민·관·군 분절 구조 위에 서 있다. 국가정보원(국가사이버안보센터)이 국가 차원의 정보·정책·관제를 총괄하고, 국방부는 국방 분야 경보·조사·보안관리를, 과기정통부는 민간 분야를 담당한다. 이 분절은 평시에는 효율이지만, 외국 수출통제가 '하드웨어 단위'로 파고들면 관할이 겹친다. 같은 랙이 국방망과 공공망, 방산업체 개발망에 걸쳐 이전되기 때문이다.

#### 3.1 직접 충돌하는 국내 규범

| 국내 규범              | 충돌 지점                          | 검토 과제                            |
|--------------------|--------------------------------|----------------------------------|
| 군사기밀보호법            | 부대 편성·장비 배치·AI 역량 도입 현황의 외국 제공 | 라이선시의 미국법상 보고가 국내법 위반이 되는지       |
| 보안업무규정             | 국가중요시설 소재·보호구역 식별 가능성          | 위치 텔레메트리의 해상도가 시설을 특정하는가         |
| 사이버안보 업무규정         | 국방 분야 사고조사·보안관리의 주체는 국방부장관     | 외국 행정기관의 소재검증 요구와 조사권한의 경합       |
| 방위사업법              | 기술이전·수출 승인, 방산기술 보호            | 위치검증 메커니즘 자체의 기술요건화가 방산기술에 해당하는지 |
| 국가 망 보안체계(N2SF)    | 외부 SaaS·CDN·콜백 차단이 모델의 전제      | 위치검증을 오프라인 증적으로 재정의할 수 있는가       |
| K-RMF (국방 사이버위협관리) | 인가·지속모니터링·공급망 위협               | 외국 위치검증 모듈을 인가 경계 안에 둘 수 있는가     |

#### 3.2 왜 민수 기업 이슈가 아니라 국가 이슈인가

일반 기업은 라이선스 조건과 계약 조항으로 위험을 가격에 전가할 수 있다. 국방·정보 영역은 그렇지 않다. 최종사용자 식별 자체가 보안사항인 고객군이 존재하고, 폐쇄망은 제품 차별점이 아니라 작전 요건이며, 연산자산의 배치는 전력 건설 정보다. 여기에 한국군이 추진하는 AI·드론·무인전투체계 전환, 전작권 전환 국면의 독자 지휘통제 고도화가 겹친다. 연산기반을 외국 검증 체계에 열어 두면, 스마트 강군 구상의 하층 인프라가 동맹 행정권의 가시거리 안에 들어간다.

연구소의 판단은 명확하다. 이 문제는 방산업체의 컴플라이언스 비용 증가로 환원되어서는 안 된다. 국가 사이버안보 기본전략, 국방 AI 획득정책, 망 보안 기준, 한미 수출통제 협의의 의제로 격상되어야 한다.

#### 4. Chip Security Act — 조문별 국가안보 영향

원문은 H.R. 3447 발의안(IH, 2025-05-15) 기준이다. 위원회 대체안은 문구가 다를 수 있으며, 특히 기능변경(킬스위치) 관련 보도가 있으므로 보고본 대조가 전제다.

| 조항              | 요지                      | 사이버안보 영향                     | 대응 방향                  |
|-----------------|-------------------------|------------------------------|------------------------|
| §3(3)           | 대상 품목 = 지정 ECCN + 후속·유사 | 국방·공공 AI 서버의 규제 지위가 BOM에서 결정 | 국가 차원 가속기 분류 대장 구축     |
| §3(2)           | 보안 메커니즘에 물리적 수단 포함      | 오프라인 봉인·증적이 제도적으로 열릴 여지      | 폐쇄망형 attestation 표준 제안 |
| §4(a)(1)        | 이전 전 위치검증 탑재 (180일)     | 현장 구축·이설·재고 납품마다 트리거         | 임계값 미달 SKU와 주권 SKU 분리  |
| §4(a)(2)(C)     | 변조 및 변조 시도 보고           | 폐쇄망 타임아웃이 상시 오탐·보고 부담        | 정상 폐쇄망 baseline 정의 필수  |
| §4(b)(1)(B)(ii) | 워크로드 검증 (2차 평가 항목)      | 국방 AI 내용물이 외국 검증 대상이 될 수 있음  | 국방 연산의 탈미국 경로 확보       |
| §4(c)(2)        | 소재지·현재 최종사용자 기록         | 군·정보기관 배치정보가 미 상무부 기록에 잔류    | 면제 협의 또는 대상품목 배제       |
| §4(b)(3)(B)     | 기밀성 우선 (1문장 훈시)         | §4(c) 기록 유지에는 대응 보호조항 부재     | 한미 협의로 보호수준을 조약·교환각서로  |
| §4(c)(1)        | 이미 이전된 제품의 소유·소재 검증     | 기 전력화분에 대한 조회 권한 (탑재 의무와 별개) | 기 도입 자산 대장·라이선스 번호 정비  |

표의 §4(b)(1)(B)(ii)는 원안의 워크로드 검증 평가 항목을 가리킨다. 위원회 대체안 번호 체계는 달라질 수 있다.

##### 4.1 관문 조항 — 분류가 국가 자산의 운명을 정한다

대상 품목이 아니면 §4 전체가 비적용이다. 반대로 해당하면 납품·이설·조직개편마다 의무가 살아난다. ‘후속 또는 실질적으로 유사한 ECCN’ 확장 조항 때문에, 오늘 임계값 미달이어도 내일의 상위 SKU는 자동 포섭될 수 있다. 국방 획득 로드맵에서 성능 향상과 규제 진입이 맞교환 관계라는 점을 BOM 단계에서 명시하지 않으면, 전력화 중간에 법이 들어온다.

국가 차원에서 즉시 필요한 것은 개별 업체의 ECCN 추정이 아니라, 국방·공공에 이미 들어가 있거나 도

입 예정인 가속기·서버의 분류 대장이다. AMD MI250급은 3A090 해당이 유력하고, 추론 중심 저전력 구성은 임계값 아래에 머물 여지가 있다. 이 차이가 '같은 AI 사업'처럼 보여도 법적으로는 다른 세계다.

## 4.2 폐쇄망과 위치검증의 충돌

위치검증은 설계상 주기적 외부 확인을 전제한다. 한국 국방·공공 사이버안보의 상당 부분은 그 전제를 거부하는 방식으로 구축되어 왔다. 충돌은 이념이 아니라 운영 이벤트 목록에서 드러난다.

- 네트워크 단절로 인한 위치검증 타임아웃
- 폐쇄망 내부 프록시·게이트웨이 경유로 인한 경로 이상
- 지연시간 측위값의 이상치
- 장비 전원 차단·점검 중 검증 주기 누락

위 네 가지 중 최소 세 가지는 정상적인 폐쇄망 운용에서 상시 발생한다. §4(a)(2)(C)가 시도까지 포섭하므로, baseline 없이 모든 실패를 보고하면 보고 의무 자체가 작전 불능 수준의 부담이 된다. 이는 기업의 컴플라이언스 비용이 아니라, 사이버작전 지속성의 문제다.

## 4.3 소급 — 탑재는 장래효, 기록은 사실상 소급

| 충위         | 소급 여부                    | 국방·공공 함의                                |
|------------|--------------------------|-----------------------------------------|
| 위치검증 탑재 의무 | 장래효. 트리거는 제조일이 아니라 이전 시점 | 기 전력화분 리트로핏 불요. 다만 이설·재배치·운영주체 변경 시 부활  |
| 보고 의무      | 사실상 소급. 기존 라이선시 포괄       | 이미 받은 수출허가 물량도 이탈·변조 보고 대상이 될 수 있음      |
| 검증·기록 권한   | 명시적 소급. 이미 이전된 제품을 지칭    | 창고 재고, PoC 이동, 정비 반송 후 재설치까지 자산 정책이 흔들림 |

미국법의 일반 원칙은 명시적 소급조항이 없으면 소급하지 않는다는 추정이다. 두 법안 어디에도 소급 조항은 없다. 그러나 수출통제는 '소급처럼 보이는 장래효'를 쓴다. 재수출 통제가 이미 한국 안에 있는 물건을 규율하는 것과 같은 구조다. 보유자 입장에서는 자산이 묶이는 효과가 동일하다.

## 5. Remote Access Security Act — 조문별 국가안보 영향

아이언마인드와 같은 온프레임 폐쇄 어플라이언스만 놓고 보면 RASA 노출은 낮다. 국가 전체로 시야를 넓히면 이야기가 달라진다. 국방 클라우드 시범, 방산 디지털 엔지니어링, 해외 GPU 클라우드를 이용한

모델 학습·벤치마크, 동맹 연합훈련 네트워크, 외주 개발인력의 원격 접속이 모두 '원격접근 제공'의 후보가 된다.

| 개정 지점    | 요지                           | 한국 사이버안보 함의                        |
|----------|------------------------------|------------------------------------|
| 원격접근 정의  | 네트워크·클라우드를 통한 외국인의 접근. 과실 포함 | 스크리닝 체계 부재가 곧 행정제재 리스크             |
| 제공 행위 포함 | 접근을 열어주는 행위 자체 규제            | 유지보수 VPN, 원격 관제, 연합 개발환경이 해당될 수 있음 |
| 라이선스 요건  | 원격접근 제공에 허가 가능               | 방산 협력·MRO 계약의 허가 조항화               |
| 조사·집행 확대 | 원격 접근된 품목에 집행권 확대            | 로그 보존·접근기록 기준이 국가 보안감사와 겹침         |
| 형사 vs 행정 | 형사는 기존 willful, 행정은 과실까지     | 사업·기관 지속성을 위협하는 것은 행정제재            |

## 5.1 국가 체계에서 노출이 생기는 세 지점

### 유지보수·모델 업데이트 채널

폐쇄망 장비라도 벤더 원격 유지보수가 남아 있으면 '제공 행위' 논쟁이 생긴다. 접속 주체가 한국 국적·한국 기관이고 외국인 접근이 없으면 정의상 성립하지 않을 수 있다. 그러나 글로벌 벤더의 해외 SOC, 야간 원격 지원, 외주 협력사 국적 혼재는 현실을 복잡하게 만든다. 국방 분야는 원격 유지보수를 원칙 금지하거나, 국내 인력·국내 SOC로 한정하는 획득 조건이 필요하다.

### 개발·검증 단계의 해외 클라우드

국방 AI 모델을 해외 GPU 클라우드에서 학습·벤치마크하는 순간, 한국 기관·기업이 접근 주체가 된다. 하원안은 우려국 한정이 없고 장관 지정에 맡긴다. '학습은 해외, 추론은 국내'라는 관행이 더 이상 안전하지 않다. 국가 연구개발 과제 지침에 통제 품목 클라우드 사용 기준을 명시해야 한다.

### 해외 협력·파견 인력의 개발환경 접근

우려국 국적 인력이 미국산 통제 품목이 돌아가는 방산·국방 개발 서버에 접근하면 규제 대상 행위가 된다. 이는 전통적 보안측정(비밀취급 인가)과 겹치지만, 수출통제는 국적이라는 다른 축을 쓴다. 인력 스크리닝을 보안인가만으로 대체할 수 없다.

## 5.2 책임의 층위

정의 조항은 형사책임의 주관적 요건을 낮추지 않는다고 유보한다. 그러나 행정·민사 제재는 과실까지

포섭한다. 국가기관과 방산업체 입장에서 방어선은 '고의가 없었다'가 아니라 '합리적 통제가 존재했음'의 입증이다. 접근 로그, 국적·소속 스크리닝, 원격 세션 승인, 차단 증거가 사이버안보 거버넌스의 일부로 편입되어야 한다.

## 6. 주권 침해 구조 — 다섯 층위

연구소는 이 법안들을 '동맹의 정당한 기술보호'로만 읽어서는 안 된다고 본다. 동시에 '반미·탈동맹'의 언어로 환원해서도 안 된다. 정확한 진단은 이것이다. 수출통제가 물리적 국경을 넘어 동맹국 내부의 사이버자산 배치와 운용 내용까지 가시화하는 구조로 진화하고 있다.

| 층위       | 근거                 | 내용                               | 심각도    |
|----------|--------------------|----------------------------------|--------|
| 역외적용     | CSA §4(a)(1), ECRA | 한국 영토 내 한국 기관 간 거래를 미국법이 규율      | 중      |
| 최종사용자 기록 | CSA §4(c)(2)       | 소재지와 현재 최종사용자를 미 상무부가 기록         | 최고     |
| 상시 위치 확인 | §4(a)(1), §4(c)(1) | 단발 신고가 아닌 지속적 소재 확인. 국가중요시설 노출   | 높음     |
| 워크로드 검증  | 2차 평가 항목           | '어디 있나'에서 '무엇을 돌리나'로 확장          | 최고(잠재) |
| 기능 변경 권한 | 2차 평가 항목           | 불법 취득 판정 시 기능 변경. 판정 주체는 미 상무 장관 | 높음(잠재) |

### 6.1 §4(c)(2)가 최악인 이유

기록이 축적되면 어느 부대·어느 기관이 어떤 AI 역량을 언제 도입했는지가 시계열이 된다. 개별 거래 신고를 넘어 상대국(이 경우 동맹국) 군 현대화 추이에 대한 상시 정보원이 된다. 수출통제의 부수효과가 아니라 구조적 결과다.

법안의 보호 장치는 '장관은 기밀성을 우선해야 한다'는 한 문장이다. 그마저 2차 메커니즘 구현 시의 혼시이며, §4(c) 기록 유지에는 대응 조항이 없다. 한국 국내법의 비밀보호 수준과 미국 행정기록의 보호 수준은 같은 층위가 아니다.

### 6.2 계약으로 풀리지 않는 충돌

라이선시(수입·납품 사업자)는 미국법상 보고 의무와 한국 국내법상 비밀유지 의무 사이에 낀다. 이 충돌은 고객 계약의 고지·협의 조항으로 해결되지 않는다. 남은 경로는 두 가지뿐이다. 제품·전력 구성 단계에서 대상 품목을 배제하거나, 정부 간 협의로 면제·보호장치를 확보하는 것이다. 개별 기업에 맡기는 순

간, 국방 사이버안보의 전제가 업체의 법적 판단에 외주된다.

### 6.3 비대칭 거래

CSA는 보안 메커니즘을 충족하면 수출 가능국을 확대하도록 권고하는 조항을 함께 둔다. 명시적으로 '추적을 수용하는 대가로 물량을 주는' 구조다. 민수 고객에게는 합리적 거래일 수 있다. 국방 고객에게는 주권 양보와 역량 확보의 교환이다. 개별 기업이 협상할 층위가 아니며, 국가가 교환의 조건을 정해야 한다.

## 7. 사이버안보 태세에 대한 구조적 충격

### 7.1 탐지·대응 파이프라인의 연산 병목

한국 공공·국방 사이버안보는 로그 집적, 이상탐지, 악성코드 분석, 딥페이크·생성형 공격 식별에서 AI 연산에 점점 더 의존한다. 고성능 가속기를 넣으면 탐지 품질이 오르고, 넣는 순간 위치검증·기록 의무가 붙는다. 넣지 않으면 연산이 모자란다. 이 딜레마를 업체별 BOM 최적화로 방치하면, 국가 전체의 탐지 공백이 생긴다.

정책적으로 필요한 것은 '어디에 고성능이 필수이고, 어디에 임계값 미달로 충분한가'를 국가가 나누는 일이다. 사이버작전, 암호분석, 대규모 위협사냥은 주권 스택으로, 일반 공공 문서형 AI와 업무지원은 동맹 통제 질서 안에서, 라는 이원 구조다.

### 7.2 에어갭의 재정의

에어갭을 포기할 수는 없다. 위치검증을 실시간 통신이 아니라 증적 추적 문제로 재정의하는 것이 유일한 정합적 해법이다. 물리 매체로 반출하는 HSM 서명 위치증명, 일방향 다이오드, 물리적 봉인은 모두 §3(2)의 '물리적 보안 메커니즘' 문언과 맞닿아 있다. 한국이 선제적으로 폐쇄망형 attestation 표준안을 만들어 BIS 규칙 의견수렴에 제출하면, 동맹국 실무 표준이 될 여지가 있다. 늦으면 온라인 콜백이 기본값이 된다.

### 7.3 공급망 — 중국의 비대칭 보복

중국에게 두 법안은 새로운 충격이 아니라 예고한 충격의 조기다. 가속기로 반격할 수 없으므로 희토류·갈륨·게르마늄·안티몬, 패키징 소재, 반외국제재법으로 다른 축을 누른다. 한국 국방·공공 하드웨어의 랙·전원·냉각·수동소자가 중국산 소재에 의존하면, 미국법의 직접 규제가 아니라 중국 보복의 간접 타격

이 사이버안보 인프라를 멈춘다.

국방부·방사청·과기정통부가 즉시 착수해야 할 일은 AI 가속기만이 아니라 Layer 01 하드웨어 BOM의 원산지 점검이다. 사이버안보 자산의 공급망 지도가 없으면, 다음 수출통제 파동에서 어떤 관제센터가 예비부품 부족에 빠지는지 사후에야 알게 된다.

## 7.4 규제 표적의 이동 — 모델 가중치

RASA의 트리거는 미국 관할 품목에 대한 외국인의 접근이다. 해외에서 합법적으로 학습한 모델 가중치를 반입하는 경로는 두 법안 어느 쪽도 막지 못한다. 이 공백은 오래 가지 않을 가능성이 높다. 통제가 하드웨어에서 모델 출처·학습 이력 증명으로 이동하면, 한국의 강점 후보는 두 가지다. 자체 호스팅 국산 모델과, 학습·추론 이력을 봉인하는 증적 체계다.

지금은 N2SF·보안적합성 논리로 쓰이는 감사체인·서명 인프라가, 2~3년 뒤에는 수출통제 대응 인프라로 재배치될 수 있다. 국가 사이버안보 R&D 과제의 산출물을 '국내 규정 준수'에만 묶어두면 기회를 놓친다.

## 8. 지정학 시나리오와 한국의 위치

한국은 미국 수출통제의 대상국이 아니라 시행 파트너이자, 동시에 가장 밀도 높게 미국산 첨단 가속기를 운용하는 동맹이다. 이 이중성이 정책의 어려움이다. 중국 우회를 함께 막지 않으면 동맹 신뢰가 흔들리고, 그대로 수용하면 국방 사이버자산의 가시성이 넘어간다.

| 시나리오       | 신호                       | 국가 조치                                           |
|------------|--------------------------|-------------------------------------------------|
| 2026년 내 제정 | 하원 본회의 + 상원 타협 / NDAA 병합 | 180일 클럭 전 분류 대장·이설 계획 동결 검토, 한미 면제 협의 착수        |
| 상원 교착      | 은행위 무일정, 업계 반발 지속        | 창을 허비하지 말 것. 오프라인 attestation 표준과 국산 NPU 경로를 준비 |
| 소재 통제 확대   | 중국 상무부 품목 추가 고시          | 국방·공공 BOM 원산지 점검, 대체 공급 사전 확보                   |
| 모델 가중치 통제  | 의회 청문회, BIS ANPRM        | 국산 모델·학습이력 증적을 국가 표준으로 격상                       |
| 미국 정책 재반전  | 라이선스 완화 후 재강화 반복         | 완화 국면에 다년 하드웨어 투자를 걸지 말 것.                      |

| 시나리오 | 신호 | 국가 조치               |
|------|----|---------------------|
|      |    | 2025~26년 이미 세 차례 반전 |

제3 스택(중국산 가속기 해외 공급)이 2027~28년 이후 열리더라도, 국방·정보 영역에서 중국산은 배제가 필연이다. 국방 사이버안보의 연산 주권 경로는 미국산 고성능과 국산 NPU 사이의 이원 구조로 남는다는 결론은 바뀌지 않는다.

## 9. 정책 권고

권고는 기관별 실행 단위로 나눈다. 연구소는 민간 사단법인이므로 훈령을 대체하지 않으며, 주관기관인 국방부와 유관부처가 채택·변용할 수 있는 의제 목록을 제시한다.

### 9.1 국방부 · 합참 · 사이버작전사령부

- 국방 AI·사이버자산 가속기 ECCN 분류 대장을 즉시 구축한다. 전력화분, 도입예정분, 시험·PoC, 정비 파이프라인을 구분한다.
- 폐쇄망 위치검증을 실시간 콜백이 아닌 오프라인 attestation(HSM 서명 + 물리매체 반출)으로 표준화하는 작전요구성능(ROC)을 검토한다.
- 국방 SKU의 고성능 연산을 국산 NPU·비미국 경로로 이원화하는 것을 성능 타협이 아니라 주권 요건으로 획득문서에 명시한다.
- 원격 유지보수는 원칙 금지, 예외는 국내 인력·국내 SOC·승인된 일방향 경로로 한정한다.
- 기 전력화분의 이설·재배치·운영주체 변경을 BIS 최종규칙 발효 전에 점검한다. PoC 장비의 부대 간 이동이 국내이전 트리거다.

### 9.2 국가정보원 · 국가사이버안보센터

- 국가중요시설·정보기관 운용 자산에 대한 최종사용자 기록 요구는 한미 정보·수출통제 협의의 공식 의제로 올린다.
- 위치 텔레메트리의 해상도가 시설을 특정하지 않도록, 허용 가능한 증명 粒度(기관 단위 / 권역 단위 / 좌표 비공개)를 한국안보 기준으로 제안한다.
- 민간 분야 클라우드 원격접근과 국방·정보 분야 폐쇄망을 분리한 국가 가이드라인을 과기정통부와 공동 마련한다.

### 9.3 방위사업청 · 방산업계

- 공급계약에 규제 변경으로 인한 인도 지연 면책, 재수출 금지 확약, 최종사용자 정보 제공 시 정부 사전협의 조항을 표준화한다.
- Layer 01(랙·전원·냉각·수동소자) 원산지와 중국 소재 의존도를 방산기술보호 점검 항목에 넣는다.
- 해외 GPU 클라우드를 이용한 국방 R&D·벤치마크를 과제 지침에서 통제한다. '학습은 해외' 관행을 종료한다.

### 9.4 과기정통부 · 산업통상자원부

- 민수 클라우드·SaaS의 RASA 노출(외국인 접근 제공)에 대한 기업 안내서를 선제 발간한다. 행정제재는 과실로 발동한다.
- 국산 AI 가속기·NPU와 자체 호스팅 모델 가중치를 경제안보·사이버안보 교집합 과제로 예산 태깅한다.
- BIS NPRM·의회 통보 창구를 상시 모니터링하는 범부처 실무반을 구성한다. 규칙의 기술 요건이 법률보다 중요하다.

### 9.5 국회 · 국가안보실

- 국가사이버안보 기본법 및 관련 개정 논의에 '외국 수출통제의 역외적용과 국내 비밀보호의 충돌 조정' 조항을 검토 과제로 포함한다.
- 한미 안보협약(SCM 등)에서 동맹국 폐쇄망에 대한 위치검증 예외·오프라인 증거 인정·최종사용자 기록의 보호수준을 의제화한다.
- 개별 기업에 충돌을 외주하지 않도록, 면제·보호장치의 협상 주체를 정부로 명확히 한다.

### 9.6 시점표

| 시점       | 외부 사건                  | 한국 측 준비                         |
|----------|------------------------|---------------------------------|
| 현재       | CSA 본회의 대기, RASA 상원 계류 | 분류 대장, BOM 원산지, 기 도입분 라이선스 번호   |
| 제정일      | CSA 180일 클럭 시작         | 오프라인 attestation 개념실증, 한미 협의 개시 |
| 제정 +6개월  | BIS 규칙 요구 시한           | 이설·재고·PoC 이동 정리. 경과조치 창 활용      |
| 제정 +12개월 | 2차 메커니즘 평가 보고          | 워크로드 검증 채택 여부 확인. 국방 스택 분기 결정   |

| 시점     | 외부 사건                    | 한국 측 준비              |
|--------|--------------------------|----------------------|
| 평가 +2년 | 2차 메커니즘 의무화 가능 (최장 약 3년) | 국방 연산 이원 스택 확보 완료 목표 |

## 10. 미확정 사항, 모니터링, 출처

### 10.1 확인이 필요한 항목

| 항목                       | 상태           | 영향                       |
|--------------------------|--------------|--------------------------|
| H.R. 3447 위원회 보고본(RH) 전문 | 공개본 확인 필요    | 킬스위치·지오펀싱 금지 조항의 실제 문구   |
| 기능 변경 연구 조항 존치 여부        | 미확인          | 원격 무력화 여지 — 국방 인가의 핵심 쟁점 |
| 한국 도입 가속기의 TPP-ECCN 실측   | 부처·방사청 확인 필요 | 국가 자산 전체의 규제 지위          |
| BIS 경과조치(savings clause) | 규칙 발표 전      | 재고·이전 정리 시한              |
| VEU 등 사전검증과 CSA의 상호작용    | 미정           | 동맹국 우대 경로의 실효성           |

### 10.2 상시 모니터링 포인트

- 하원 본회의 표결 일정 및 상원 은행위 마크업
- RASA §3 에 따른 의회 보고 — 규칙 방향의 조기경보
- BIS NPRM (위치검증 기술 요건의 구체화)
- 국방수권법 패키지 병합 여부
- 중국 수출통제 품목 추가와 방산·공공 BOM 교차점검

### 10.3 주요 출처

H.R. 3447 Chip Security Act 발의 원안(IH, 2025-05-15), Congress.gov / GovInfo.

H.R. 2683 Remote Access Security Act 하원 통과본(EH, 2026-01-12), Congress.gov.

하원 외교위원회 CSA 가결(42-0, 2026-03-26) 관련 위원회·Select Committee 공개 자료.

S. 3519 Remote Access Security Act 상원 발의(2025-12-17).

사이버안보 업무규정, 군사기밀보호법, 보안업무규정, 방위사업법 — 국가법령정보센터.

국가사이버안보센터·국방 사이버위험관리(K-RMF) 관련 공개 정책자료.

### 10.4 문서의 한계

본 검토서는 공개된 법률안 문언과 입법 경과, 한국의 공개 사이버안보 제도를 교차한 정책 분석이다. 특정 업체의 제품 구성, 특정 부대의 자산 목록, 비공개 한미 협의 내용은 포함하지 않았다. 위원회 대체

안과 BIS 규칙이 공개되면 조문 번호·의무의 범위가 달라질 수 있다. 연구소는 후속 개정판에서 보고본 대조와 규칙안 의견을 반영할 예정이다.

---

#### 사이버안보연구소

본 문서는 정책 토론을 위한 것이며 특정 제품의 수출통제 적격성을 보증하지 않습니다.

문의 · [info@ncsl.or.kr](mailto:info@ncsl.or.kr) · <https://ncsl.or.kr>

