

국가안보를 이유로 한 AI 수출통제의 국제경제법적 분석

- Fable 5 사건과 AI 접근권의 전략자산화를 중심으로

대외경제정책연구원 강 민 지

*논문접수 : 2026. 7. 16. *심사개시 : 2026. 8. 14. *게재확정 : 2026. 8. 18.

〈목 차〉

I. 서론	2. 안보예외 법리의 심화와 판례의 전개
II. 미국의 AI 모델 통제의 법적 근거와 AI의 전략자산화	3. GATS의 안보예외의 적용과 한계
1. 미국의 AI 모델 통제의 법적 근거	IV. WTO 안보예외 법리의 Fable 5 사건에 대한 적용과 시사점
2. Fable 5 접근제한 조치의 전개와 법적 성격의 불확실성	1. 안보예외 법리의 적용
3. AI 접근권의 전략자산화: 전략자산의 디지털 영역으로의 확장	2. AI 수출통제에 대한 WTO 안보예외 적용의 함의와 한계
III. WTO 안보예외에 관한 판정례의 심사기준	3. 한국에 대한 입법적 시사점
1. WTO 안보예외의 해석과 사법심사 가능성	V. 결론
	참고문헌

I. 서론

2026년 6월 9일, 미국의 AI 기업 앤트로픽(Anthropic PBC, 이하 앤트로픽)은 클로드 페이블 5(Claude Fable 5, 이하 Fable 5)와 제한된 프로젝트 글래스윙(Project Glasswing) 파트너에게 제공되는 클로드 미토스 5(Claude Mythos 5, 이하 Mythos 5)를 출시하였다. 앤트로픽은 출시 성명에서 이 모델의 역량이 “우리가 지금까지 개발한 어떤 모델보다도 뛰어나다”고 밝히면서, 동시에 “이처럼 강력한 모델을 출시하는 것은 위험이 따른다”며, “적절한

보안 조치가 없다면 사이버 보안과 같은 영역에서 Fable 5의 역량이 오용되어 심각한 피해를 초래할 수 있다”고 경고했다.¹⁾

2026년 6월 12일 엔트로픽은 미국 정부로부터 미국 내외의 외국 국적자에게 Fable 5와 Mythos 5의 접근을 중단하도록 요구하는 수출통제 지시를 받았다고 공식 발표하였다.²⁾ 다만 공개된 정부 지시문 원문이 없으므로, 구체적인 법적 근거와 규제 범위는 엔트로픽의 공식 설명과 이후 제출된 소송자료³⁾를 통해 제한적으로 확인된다. 소송자료에 따르면, 2026년 6월 12일 미국 정부는 엔트로픽에 전화를 걸어, 주장된 위협에 대한 추가적인 세부 사항을 제공하지 않은 채 ‘국가 안보 위협’을 근거로 Fable과 Mythos 모델을 중단하도록 단 90분의 시간을 주었고, 당일 오후 5시 30분경 상무부의 권한 위임을 받아 미국 상무부 산업안보국(Bureau of Industry and Security, 이하 BIS)가 엔트로픽의 최고경영자(CEO)에게 서한을 발송하여 Fable 5 및 Mythos 5 모델에 대해 전 세계의 모든 외국인을 대상으로 하는 광범위한 수출통제 제한 및 라이선스 요건을 부과하였다고 밝히고 있다.⁴⁾ 엔트로픽은 이용자의 국적을 실시간으로 확인할 수 있는 기술적 수단을 갖추지 못하였기 때문에, 외국 국적자만을 선별적으로 차단하는 대신 모든 이용자에 대한 Fable 5와 Mythos 5의 접근을 일시적으로 중단하였다.⁵⁾ 엔트로픽은 정부가 Fable 5의 안전장치를 우회하는 이른바 ‘탈옥(jailbreak)’ 가능성을 문제 삼은 것으로 이해하나 엔트로픽의 자체 검증에 따르면 문제된 기능은 다른 공개 AI 모델에서도 구현할 수 있다고 밝혔다.⁶⁾ 2026년 6월 30일 엔트로픽은 해당 수출통제가 해제되었으며 7월 1일부터 Fable 5의 글로벌 접근이 복구된다고 발표하였다.⁷⁾

1) Anthropic, “Claude Fable 5 and Claude Mythos 5,” Anthropic News (June 9, 2026; updated July 1, 2026), 온라인 자료 (최종검색일: 2026. 7. 11.).

2) Anthropic, “Statement on the US government directive to suspend access to Fable 5 and Mythos 5,” Anthropic News (June 12, 2026), 온라인 자료 (최종검색일: 2026. 7. 11.).

3) *Legion LegalTech Corp. v. United States of America*, No. 1:26-cv-02225-RJL (D.D.C. filed June 23, 2026).

4) *Legion LegalTech, Corp. v. United States*, No. 1:26-cv-02225 (D.D.C. filed June 23, 2026), 소장(Complaint), para.33.

5) Anthropic, “Statement on the US government directive to suspend access to Fable 5 and Mythos 5,” Anthropic News (June 12, 2026), 온라인 자료 (최종검색일: 2026. 7. 11.).

6) *Ibid.*

7) Anthropic, “Redeploying Claude Fable 5,” (June 30, 2026.), 온라인 자료 (최종검색일: 2026. 7. 11.); Notice of Voluntary Dismissal Without Prejudice, *Legion LegalTech*, No. 1:26-cv-02225-RJL (D.D.C. July 3, 2026), ECF No. 7

이 사건은 미국 정부가 고성능 AI 모델의 접근권을 국가안보 상 통제해야 할 전략자산으로 인식하고 AI 접근권을 국적별로 차등화하는 새로운 통제 패러다임을 보여준 사례라는 점에서 국제경제법적으로 중요한 의미를 갖는다. 특히 국적만을 기준으로 AI 접근권을 제한하는 조치가 국제무역법 질서와 양립할 수 있는지, 또한 WTO 분쟁해결절차에서 이러한 조치가 다투어질 경우 이를 안보예외로 정당화할 수 있는지 등의 여러 국제경제법적 문제를 제기한다.

이미 WTO 안보예외 적용에 관해서는 기존 국내외 연구 등에서 GATT 제21조의 사법심사 가능성을 중심으로 다각도로 논의된 바 있다.⁸⁾ 그러나 기존 연구들은 주로 상품 무역(GATT)이나 지식재산권(TRIPS)에 국한되어, 이번 Fable 5 사태와 같이 ‘프런티어 AI 모델의 국적에 따른 접근 통제’라는 무형의 디지털 서비스 영역에 미치는 구체적인 법적 문제를 다루지 못하였다. 이에 본 연구는 가장 최신의 실증적 사례를 바탕으로 GATS 제14조의2의 적용 가능성을 살펴보고 전략자산의 디지털로의 확장의 함의에 대해서 다룬다는 점에서 선행연구와 차별성을 가진다.

본 연구는 우선 미국 정부의 프런티어 AI 모델에 대한 접근권 제한이 미국 국내법상 적법한 수출통제에 해당하는지를 검토하고, 이러한 조치가 WTO 협정상 의무에 위반되는 경우 안보예외로 정당화될 수 있는지를 기존 WTO 판례와 법리를 중심으로 분석한다. 이를 바탕으로 안보예외 조항이 디지털 및 AI 영역에 어떻게 적용될 수 있는지를 검토하고, AI 접근권의 전략자산화가 국제경제법 질서에 갖는 규범적 함의를 제시하고자 한다.

II. 미국의 AI 모델 통제의 법적 근거와 AI의 전략자산화

1. 미국의 AI 모델 통제의 법적 근거

미국의 이중용도(dual-use) 품목·기술·소프트웨어에 대한 수출통제는 「2018년 수출통제 개혁법(Export Control Reform Act of 2018, 이하 ECRA)」을 중심으로 운영된다. ECRA는 기

8) 구모란(2026), “WTO 안보예외 분쟁의 유형화와 대응전략에 관한 연구”, 통상법무정책2026-1, pp. 77-106; 박주현(2024), “WTO 안보예외조항 연구: WTO 미-중 반도체 분쟁 및 분쟁해결기구(DSB)에 대한 시사점”, 통상법률 2024-02, pp. 3-33; Warren Maruyama·Alan Wm. Wolff, Saving the WTO from the National Security Exception, Peterson Institute for International Economics Working Paper No. 23-2 (May 2023);

존의 「1979년 수출관리법(Export Administration Act of 1979)」을 대체하여 미국의 수출통제 체계에 최초의 항구적(permanent) 법적 근거를 마련한 법이다. 1979년 수출관리법은 한시 법이었기 때문에 여러 차례 효력이 만료되었는데 이로 인해 미국 행정부는 약 20년 동안 1977년 국제비상경제권한법(International Emergency Economic Powers Act, 이하 IEEPA)⁹⁾에 근거하여 대통령이 국가비상사태를 반복적으로 선언하는 방식으로 기존 수출관리규정을 유지하는 등 평시의 수출통제 마저도 사실상 비상권한에 의존하는 구조가 지속되었다. 이러한 법적 불안정성을 해소하기 위해 「2019 회계연도 국방수권법(NDAA 2019)」의 일부로 ECRA과 「외국인투자위험심사현대화법(Foreign Investment Risk Review Modernization Act, FIRRMA)」을 동시 통과시키며 디지털 자산 통제의 법적 기반을 마련하였다.¹⁰⁾

제정된 ECRA는 의회가 평시의 수출통제를 위한 ‘신기술과 기반기술(Emerging and Foundational Technologies)¹¹⁾’에 대한 통제 권한을 BIS에 명시적으로 부여하였다. BIS는 ECRA를 근거로 수출관리규정(Export Administration Regulations, EAR)을 제정·운영한다. BIS는 EAR에 따라 상무통제목록(Commerce Control List, CCL)을 관리하고, 통제대상 품목에 수출통제분류번호(Export Control Classification Number, ECCN)을 부여하며, 개별 수출 허가를 심사한다. 또한 거래제한 목록(Entity List), 군사최종사용자목록(Military End User List) 및 해외직접제품규칙(Foreign Direct Product Rule, 이하 FDP)¹²⁾을 운용한다. ECRA에 따르면 기존의 바세나르협정(Wassenaar Arrangement) 등 다자수출통제체제에서 아직 통제되지 않는 신기술과 기반기술이라고 하더라도 미국 국가안보에 필수적인 경우 이를 식별

9) IEEPA의 경우 대통령이 비상사태를 선포하고 행정명령에 서명하면 즉시 발효된다. 화웨이 관련 ICT 공급망 행정명령(EO 13873), 대외투자 심사 행정명령 (EO 14105) 등이 IEEPA에 근거한 조치이다. 그러나 IEEPA에는 버먼 수정조항(50 U.S.C. §1702(b)(3))이 있어 정보 및 정보자료의 수출입은 대통령 권한에서 명시적으로 제외된다. 그래서 만약 AI모델 가중치를 IEEPA로 통제하면 가중치는 정보자료이므로 권한에서 제외된다는 항변이 가능하다. IEEPA 기반 관세를 둘러싼 소송에서 보듯 IEEPA의 권한 범위 자체가 다 투여되는 국면이라 정부 입장에서 장기적으로는 ECRA 경로로 하는 것이 안전하다고 판단했을 것으로 생각된다.

10) Export Control Reform Act (ECRA) of 2018, 50 U.S.C. §§ 4801-4852; Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018, Pub. L. 115-232.

11) 신기술 및 기반 기술 여부를 식별시에는 1. 해당 기술이 미국의 군사적 우위나 국가안보에 미치는 영향, 2. 우려 대상국(Countries of Concern)에서 해당 기술을 획득함으로써 발생할 수 있는 안보적 위협, 3. 해당 기술이 미국 외의 국가에서의 독자적으로 개발되고 있거나 상용화되어 있는지 여부를 고려해야 한다. 50 U.S.C. §4817(a)(2)(B).

12) FDP는 외국에서 생산된 제품이라도 미국산 기술·소프트웨어 또는 장비와 일정한 관련성을 가지는 경우 EAR의 적용대상으로 삼는 규칙이다.

하여 새로운 통제품목으로 지정할 수 있도록 규정한다.¹³⁾ 미국 상무부 장관은 식별된 기술의 수출, 재수출, 미국 외 국가로의 이전에 대해 상무부 EAR하의 적절한 통제 조치를 수립해야 하며, 여기에는 임시 통제(interim controls) 방식을 통한 조치가 명시적으로 포함된다.¹⁴⁾ 이에 따라 BIS는 인공지능, 첨단 반도체, 양자컴퓨팅 및 첨단 제조기술 등 전략기술을 단계적으로 EAR 통제품목에 편입해 왔다. 특히 2022년 10월 잠정최종규칙(interim final rule)을 통해 첨단 컴퓨팅 집적회로와 이를 탑재한 컴퓨터, 특정 반도체 제조장비의 대중국 수출을 제한하고, 미국인이 중국 내 반도체 시설의 개발·생산을 지원하는 행위도 허가 대상으로 규정하였다.¹⁵⁾ 이후 2023년 10월에는 통제 대상과 적용 범위를 확대·정비하여 관련 규제를 한층 강화하였다.¹⁶⁾

2025년 1월 15일에는 「인공지능 확산을 위한 체계」(Framework for Artificial Intelligence Diffusion, 이하 AI 확산규칙)을 발표하여 전 세계를 3등급으로 나눠 1등급은 미국 및 18개 동맹국¹⁷⁾으로 사실상 무제한 접근이 허용되지만 2등급은 싱가포르·이스라엘·포르투갈·스위스·폴란드·UAE·사우디아라비아·인도 등 대부분의 국가로서 제한적 접근만 허용되었으며 3등급은 중국·러시아·북한 등 이미 금수 대상인 적성국으로 분류되었다.¹⁸⁾ 그러나 트럼프 행정부의 상무부는 AI 확산규칙 시행 예정일을 이틀 앞둔 2025년 5월 13일 이를 철회했다. 그러나 철회와 동시에 BIS는 화웨이 Ascend 칩(910B·910C·910D)의 전 세계 어디에서든 사용이 미국 수출통제 위반 위험을 초래한다는 지침 등 세 건의 지침을 발표하여, 대중국 통제는 오히려 공격적으로 유지·강화했다.

최근 BIS는 미국 기술이 일부라도 포함된 경우 제3국 생산 제품까지 통제하는 ‘해외직접제품규칙(FDPR)’을 전면 적용하여 디지털 자산 공급망을 전방위적으로 압박하고 있다.

13) 50 U.S.C. §4817(a)(1)

14) 50 U.S.C. §4817(b)(1)

15) US Bureau of Industry and Security (BIS), “Implementation of Additional Export Controls: Certain Advanced Computing Items,” 87 FR 62186 (October 13, 2022); 88 FR 73458 (October 25, 2023); 89 FR 23876 (April 4, 2024, 보완 규칙).

16) 반도체 수출통제와 관련한 자세한 사항은 김혁중(2026), “트럼프 2기 반도체 수출통제 정책 동향과 시사점”, KIEP 오늘의 세계경제 26-17 참조.

17) 대한민국, 일본, 대만, 영국, 호주, 캐나다, 뉴질랜드, 독일, 네덜란드, 프랑스, 이탈리아, 벨기에, 덴마크, 핀란드, 스웨덴, 노르웨이, 스페인, 아일랜드 등 18개국.

18) US Bureau of Industry and Security (BIS), “Framework for Artificial Intelligence Diffusion,” 90 Fed. Reg. 4544 (Jan. 15, 2025),

또한 미국 내 보조금을 받는 기업이 우려 대상국(중국 등) 내에서 첨단 제조 능력을 확장하는 것을 제한하는 반도체법(CHIPS and Science Act 2022) ‘가드레일(Guardrail)’ 조항을 두어 디지털 인프라가 퍼지는 것을 차단하였다. Fable 5 사건에서 미국 상무부는 프런티어 AI 모델에 대한 접근을 ECRA 및 EAR에 따른 통제대상으로 취급하였으나, 호스팅된 모델 접근과 추론 결과가 현행 CCL상 통제품목 또는 EAR상 수출에 해당하는지에 대해서는 법적 논란이 제기되었다.¹⁹⁾ 미국은 ECRA와 EAR을 통해 첨단 반도체, 관련 기술 및 일정한 AI 모델 가중치에 대한 통제체계를 발전시켜 왔다. 다만 Fable 5 사건에서 호스팅된 AI 모델에 대한 원격 접근 또는 추론 서비스 자체가 어떠한 ECCN과 EAR 조항에 따라 통제되었는지는 공개된 정부 문서만으로 확인하기 어렵다. 이 점은 이후 제기된 Legion LegalTech 소송에서도 핵심적인 권한쟁점으로 제기되었으나, 소송이 본안판단 전에 취하됨에 따라 법적으로 확정되지 않았다.

외국인 투자와 관련하여서는 외국인투자심의위원회(Committee on Foreign Investment in the United States, CFIUS)의 경우 외국인 투자자의 미국 내 합병이나 지분 인수를 통한 기술 유출 위주로 심사하여, 조인트 벤처나 단순 기술 라이선싱 계약을 통한 디지털 자산 유출을 방어하지 못하는 한계가 있었으나, 「외국인투자위험심사현대화법(FIRRMA)」은 CFIUS의 권한을 대폭 확대하여 경영권을 수반하지 않는 비지배적(Non-controlling) 투자라 하더라도 핵심 기술, 인프라, 민감 개인정보를 다루는 미국 기업에 대한 외국인의 투자를 강제 심사 대상으로 지정했다.²⁰⁾ 이에 대외투자심사 행정명령(EO 14105) 등으로 미국 자본이 우려 대상국의 첨단 반도체, 양자 정보 기술, AI 시스템 분야로 유입되는 것을 차단하는 ‘아웃바운드 투자 규제’를 명문화하여 타국의 디지털 전략자산 형성을 봉쇄하고 있다.²¹⁾

2. Fable 5 접근제한 조치의 전개와 법적 성격의 불확실성

미국 수출통제 법제의 특유한 개념 중 하나는 ‘간주수출(deemed export)’로 미국 내에서

19) Mayer Brown, “Commerce Department Extends Export Controls to Advanced AI Models,” Insights (June 30, 2026), 온라인 자료 (최종 검색일 : 2026. 7. 11.)

20) FIRRMA Section 1703 (amending Section 721 of the Defense Production Act of 1950).

21) Executive Order 14105, “Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern,” 88 FR 54867 (August 2023).

외국인에게 통제 대상 기술을 공개하는 행위를 해당 외국인의 본국으로의 수출로 간주하는 법리이다. Fable 5 사건에서 이 개념이 결정적이었던 이유는 통제가 물리적 국경을 넘는 수출뿐 아니라 엔트로픽의 비시민권 직원을 포함하여 미국 내 외국인에 대한 접근까지 수출로 판단했기 때문이다. ECRA는 미국 상무부 장관의 추가적 권한(Additional authorities)과 관련하여 “통제 품목의 무허가 수출, 재수출 및 역내이전(in-country transfers)을 금지할 권한을 부여”하며, 명시적으로 “미국 내 또는 미국 외의 외국인(foreign persons in the United States or outside the United States)에 대한 것”을 포함한다고 규정하고 있다.²²⁾ EAR §734.13(a)(2)에서도 ‘수출(Export)’ 정의에서 기술이나 소스 코드를 미국 내에서 외국인에게 공개(release)하거나 이전(transfer)하는 행위 역시 수출로 본다고 규정하며, 이는 동조 (b)항에서 미국 내에서 외국인에게 기술이나 소스 코드를 공개 또는 이전하는 것은 해당 외국인의 가장 최근 시민권 또는 영주권 국가로의 간주수출이라고 구체화하고 있다.

그러나 EAR §734.7은 널리 유포된(widely disseminated) 소프트웨어를 EAR 적용에서 제외하며, 무엇보다 클라우드를 통한 호스팅 모델에 대한 접근이 과연 기술의 ‘공개(release)’로 간주수출에 해당하는지 자체가 불분명하다. EAR §734.15상 기술의 공개는 시각적 검사, 구두 설명, 또는 기술 적용 과정에서 드러나야(reveal) 하는데 BIS의 2016년 최종 규칙(Final Rule)에 따르면, 항목을 단순히 잠깐 보거나(merely seeing), 잠재적으로 접근할 수 있는 권한이 있다는 것만으로는 근원 기술(underlying technology)를 규명할 수 없으므로 ‘공개’가 아니라고 명시한 바 있다.²³⁾ 사용자는 AI 모델의 가중치나 소스 코드와 같은 근원 기술을 보는 것이 아니라 자신이 질문한 쿼리에 대한 결과물만 보는 것이므로 이를 ‘간주수출’로 보는 것은 행정부의 과도한 확장 해석이라는 지적이 나올 수 있다.²⁴⁾

또한 리전 리걸테크(Legion LegalTech)는 2026년 6월 23일 미국 연방정부와 상무부·BIS 등을 상대로 워싱턴 D.C. 연방지방법원에 소를 제기하였다.²⁵⁾ 원고인 리전 리걸테크는 미국 정부의 2026년 6월 12일 자 지시가 행정부의 법적 권한을 완전히 초과한 법률 위반

22) 50 U.S.C. §4813(a)(3)

23) US Bureau of Industry and Security (BIS), “Revisions to Definitions in the Export Administration Regulations,” 81 FR 35586 (June 3, 2016)

24) 실제로 Harvard Law Review Blog에서 이 점을 지적한 바 있다. Harvard Law Review Blog(June 26, 2026), “Is Access to Fable an Export?”, 온라인자료 (최종검색일: 2026.7.11.)

25) Legion LegalTech Corp. v. United States of America, No. 1:26-cv-02225-RJL (D.D.C. filed June 23, 2026).

(Ultra Vires) 행위이자, 절차를 무시하고 진행된 자의적이고 보복적인 행정 처분이므로 전면 무효화되어야 한다고 강력히 주장하였다. 소장에서 원고는 AI모델 가중치를 직접 규제 하던 유일한 분류인 ECCN 4E091은 2025년 5월에 이미 철회된 AI 확산규칙의 산물이므로, 현재 수출통제 목록상 웹으로 제공되는 AI 모델의 이용 권한이나 추론 텍스트 출력(inferential text output)을 규제할 수 있는 권한 근거가 없다고 주장하였다.²⁶⁾ 또한 원고는 EAR의 ‘간주 수출(deemed export)’ 규정은 기술이나 소스 코드의 유출만을 규제하며 목적 코드(object code)는 명시적으로 제외하고 있는데²⁷⁾ 사용자가 웹을 통해 단순히 프롬프트를 입력하고 텍스트 결과만 돌려받는 호스팅 AI 서비스는 모델 가중치, 소스 코드, 기술 데이터를 전혀 사용자에게 유출·전송하지 않으므로 EAR상 수출 행위로 볼 수 없다고 주장하였다.²⁸⁾

IEEPA는 어떠한 포맷이나 전송 매체를 막론하고 ‘정보 및 정보 물질’의 수출입을 규제하거나 금지하는 대통령의 권한을 원천적으로 제한하고 있는데²⁹⁾ 사용자가 Fable 5 모델로부터 제공받는 법률 초안, 분석 보고서, 요약본 등은 법적 보호 대상인 표현적 정보 물질에 해당하므로, 이 정보의 흐름을 통제하려는 정부 지시는 명백히 불법이며³⁰⁾ 정부는 AI 모델 배포 전 행정부의 사전 승인을 받아야 한다는 식의 사실상의 면허 제도(de-facto licensing regime)를 구축하여 첨단 AI 산업 전반을 장악하려하나 의회는 행정부에 이처럼 경제적·정치적으로 거대하고 중대한 권력을 행사할 수 있도록 명시적으로 권한을 위임한 바가 없다고 주장(Major Questions Doctrine 위반)하였다.³¹⁾ 또한 원고는 Chat GPT 5.5 등 유사 역량 모델은 통제되지 않았으므로 조치가 행정절차법(Administrative Procedure Act, 이하 APA)상 자의적이고 불합리(arbitrary and capricious)하다고 주장하였다.³²⁾

26) Legion LegalTech, Corp. v. United States, No. 1:26-cv-02225 (D.D.C. filed June 23, 2026), 소장(Complaint), para.5

27) 15 C.F.R. §734.13(a)(2) “Export” means “[r]eleasing or otherwise transferring ‘technology’ or source code (but not object code) to a foreign person in the United States (a ‘deemed export’).”

28) Legion LegalTech, Corp. v. United States, No. 1:26-cv-02225 (D.D.C. filed June 23, 2026), 소장(Complaint), para.5

29) 50 U.S.C. § 1702(b)(3)

30) Legion LegalTech, Corp. v. United States, No. 1:26-cv-02225 (D.D.C. filed June 23, 2026), 소장(Complaint), para.6

31) Ibid.

32) Legion LegalTech, Corp. v. United States, No. 1:26-cv-02225 (D.D.C. filed June 23, 2026), 소장(Complaint),

다만 동 소송에서 위 쟁점들에 대한 법원의 실체적 판단이 이루어지지지는 못하였다. 엔트로픽이 2026년 6월 30일 통제 해제와 서비스 복구를 발표한 후, Legion LegalTech는 같은 해 7월 3일 소를 자진취하하였다. 이에 따라 법원은 ECRA·EAR 및 IEEPA의 적용범위에 관한 본안판단을 내리지 않았다. 따라서 호스팅된 AI 모델에 대한 접근 또는 추론 결과의 제공이 ECRA 및 EAR상 ‘수출’ 또는 통제대상에 해당하는지, 그리고 이러한 접근제한이 IEEPA 및 APA에 부합하는지에 관한 법적 쟁점은 법원의 본안 판단을 받지 않은 채 남게 되었다. 그럼에도 동 사건은 기존 수출통제법제가 모델 가중치 자체의 이전을 넘어 클라우드 또는 API를 통한 AI 모델의 이용·접근까지 규율할 수 있는지에 관한 법적 불확실성을 구체적으로 드러냈다는 점에서 의미가 있다.

현행 EAR상 간주수출은 통제대상 기술 또는 소스코드의 공개·이전을 전제로 한다. 그러나 호스팅형 AI 모델의 이용자는 일반적으로 모델 가중치나 소스코드를 직접 이전받는 것이 아니라 API를 통해 질의를 전송하고 추론 결과를 제공받는다. 이러한 차이를 고려하면, 별도의 명시적인 통제 근거 없이 단순한 클라우드 API 접근까지 현행 EAR상 ‘수출’ 또는 ‘간주수출’로 취급하는 것은 관련 규정의 문언과 적용범위를 지나치게 확장하는 해석으로 평가할 여지가 있다. 향후 프런티어 AI 모델에 대한 원격 접근 자체를 수출통제 대상으로 규율할 필요가 있다면, 기존 수출 개념을 확대해석하기보다 모델 가중치·소스코드의 이전과 호스팅형 API 서비스의 제공을 구분하고, 후자에 적용되는 통제대상·요건·절차를 법률 또는 적법한 규칙제정절차를 통해 명확히 규정하는 것이 타당하다.

3. AI 접근권의 전략자산화: 전략자산의 디지털 영역으로의 확장

만약 Fable 5 접근제한 조치가 유지되었다면, 행정부가 별도의 입법이나 명시적인 규제 체계의 정비 없이도 고성능 프런티어 AI 모델에 대한 접근을 광범위하게 제한할 수 있는 선례가 형성되었을 것이다. 이는 해당 모델에 의존하는 이용자·개발자·기업의 접근이 행정부의 국가안보 판단에 따라 중단될 수 있음을 의미한다. 비록 해당 조치는 단기간에 해제되었지만, 이 사건은 AI 모델이 단순한 상업적 소프트웨어나 정보재를 넘어 국가가 접근을 허가하거나 제한할 수 있는 전략적 통제대상으로 취급될 가능성을 보여주었다.

para.7

전략자산은 일반적으로 공급의 대체 가능성이 낮고 그 확보 또는 통제가 국가의 군사적·경제적 역량에 중대한 영향을 미치는 자산을 의미하며, 전통적으로 에너지자원, 핵심 광물, 무기체계 및 주요 인프라를 중심으로 논의되어 왔다. 그러나 글로벌 경제 네트워크의 핵심 연결지점이 일부 국가와 기업에 집중되면서, 그러한 연결지점에 대한 접근을 허용하거나 차단할 수 있는 능력 자체가 상대국에 대한 영향력의 원천으로 기능하게 되었다.³³⁾ 특히 소프트웨어, 모델 가중치, 고성능 반도체, 클라우드 인프라 및 대규모 연산능력은 경제적 생산성뿐 아니라 사이버 작전, 첨단 연구개발 및 군사적 의사결정에도 활용될 수 있다는 점에서 새로운 형태의 전략자산으로 평가될 수 있다.

프런티어 AI 모델의 전략적 가치는 모델 자체뿐 아니라 이를 훈련·배포·추론하는 데 필요한 컴퓨팅 자원과 접근권에도 존재한다. AI 모델의 이용은 대규모 GPU, 데이터센터 및 클라우드 서비스에 의존하므로, 모델 가중치와 소스코드뿐 아니라 연산능력 및 원격 API에 대한 접근도 AI 역량의 실질적인 이용 가능성을 결정한다. 최근 수출통제가 첨단 반도체와 서버 등 유형재화에서 모델 가중치와 원격 접근으로 확대될 경우, 특정 국가나 기업이 글로벌 디지털 네트워크의 핵심 연결지점을 통제함으로써 다른 국가의 기술개발과 산업활동에 영향을 미칠 가능성도 커진다. 다만 모델 가중치의 이전, 클라우드 컴퓨팅 자원의 제공 및 호스팅형 API 서비스의 이용은 법적으로 동일한 대상이 아니므로, 각각의 통제 근거와 적용요건을 구별할 필요가 있다.

이처럼 AI 접근권의 전략자산화는 물리적 재화와 통제대상 기술의 이전을 중심으로 형성된 기존 수출통제 및 국제무역규범에 새로운 문제를 제기한다. 특히 원격 API와 클라우드 서비스에 대한 접근제한이 GATS의 적용대상에 포함되는지, 포함된다면 최혜국대우·시장접근·내국민대우 의무와 어떠한 관계에 있는지가 우선 검토되어야 한다. 이러한 의무와의 불합치가 인정되는 경우에는 규제국이 해당 조치를 GATS 제14조의2의 국가안보예외로 정당화할 수 있는지가 후속적으로 문제된다. 이하에서는 먼저 WTO 국가안보예외에 관한 판정례의 심사기준을 검토한 후, 이를 AI 모델 접근통제에 적용한다.

33) Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security*, Vol. 44, No. 1 (2019), pp. 45-47.

III. WTO 안보예외에 관한 판정례의 심사기준

Fable 5형 접근제한 조치는 미국 서비스공급자의 해외 서비스 제공을 제한하는 공급국 측 조치라는 점에서 GATS상 의무 위반이 곧바로 성립한다고 단정하기 어렵다. 다만 향후 AI 접근통제가 국가별 등급에 따라 다른 회원국의 서비스 또는 서비스공급자에게 상이한 접근조건을 부여하거나, 외국 서비스공급자의 시장접근을 제한하는 방식으로 설계된다면 GATS 제2조·제16조·제17조와의 불합치가 문제될 수 있다. 이 경우 규제국은 해당 조치가 자국의 필수적 안보이익을 보호하기 위한 것이라고 주장하면서 GATS 제14조의2를 원용할 가능성이 있다.

현재까지 GATS 제14조의2를 직접 해석·적용한 WTO 판정례는 존재하지 않는다. 그러나 제14조의2는 GATT 제21조 및 TRIPS 협정 제73조와 유사한 문언과 구조를 가지고 있으므로, 이들 조항에 관한 WTO 패널의 해석은 GATS 안보예외의 적용범위와 심사기준을 검토하는 데 중요한 해석자료가 될 수 있다. 따라서 이하에서는 먼저 GATT 제21조와 TRIPS 협정 제73조에 관한 주요 판정례를 검토하고, 이를 토대로 GATS 제14조의2가 AI 모델 접근통제에 적용되는 경우의 법적 요건과 한계를 살펴본다.

1. WTO 안보예외의 해석과 사법심사 가능성

AI 모델 접근통제가 GATS상 의무에 불합치하는 것으로 판단되는 경우, 규제국은 해당 조치가 필수적 안보이익을 보호하기 위한 조치라고 주장하며 제14조의2를 원용할 수 있다. 이 경우 선결적으로 문제되는 것은 안보예외의 원용이 회원국의 전적인 자기판단에 맡겨지는지, 아니면 WTO 분쟁해결절차에서 객관적 심사의 대상이 되는지이다. GATS 제14조의2를 직접 해석한 판정례가 없으므로, 이하에서는 유사한 문언을 가진 GATT 제21조를 중심으로 안보예외의 사법심사 가능성과 심사범위를 검토한다.

GATT 제21조 (b)(iii)는 회원국이 전쟁 또는 국제관계상 그 밖의 비상사태 시 자국의 필수적 안보이익을 보호하기 위하여 필요하다고 판단하는 조치를 취할 수 있도록 규정한다. 이 조항을 둘러싼 핵심적인 해석 문제는 ‘자국이 필요하다고 판단하는(which it considers necessary)’이라는 문언이 안보예외 전체를 회원국의 전적인 자기판단에 맡기는 것인지, 아니면 ‘국제관계상 비상사태’의 존재와 조치의 관련성 등이 WTO 패널의 객관적 심사대상

이 되는지에 있다.

미국은 GATT 체제 이래 일관되게 안보예외가 국가의 주권적 판단 영역에 속하므로 WTO 분쟁해결기구의 사법심사 대상이 될 수 없다는 입장을 견지해 왔다. 「러시아-통과운송 사건」(Russia—Measures Concerning Traffic in Transit, 이하 Russia—Traffic in Transit 사건)에서도 미국은 제3자 의견을 통해 제21조의 ‘자국이 필요하다고 인정하는’ 이라는 문구가 각 회원국에 독자적인 판단권을 부여하는 것이며 따라서 패널의 사법 심사 대상이 될 수 없다고 주장하였다. 또한 일국의 안보와 직결된 조치는 다른 회원국이 그 적절성을 검토하거나 위반 여부를 판정할 수 없는 비사법적 영역이라고 주장하였다.³⁴⁾

그러나 Russia—Traffic in Transit 사건에서 패널은 이러한 입장을 받아들이지 않았다. 패널은 국제관계상 비상사태의 존재는 객관적인 사실 관계이므로, 해당 조치가 제21조 (b)항 (iii)호에 따라 “국제관계상 비상사태” “시기에” “취해진” 것인지 여부의 판단은 객관적인 사실에 대한 판단이며, 객관적인 판단의 대상이 된다고 보았다.³⁵⁾ 패널은 제21조(b)항 (iii)호의 의미에서 “국제관계상의 비상사태”를, 무력 충돌이나 잠재적 무력 충돌, 또는 고조된 긴장이나 위기, 혹은 한 국가를 뒤덮거나 둘러싼 전반적인 불안정 상태의 상황으로 해석하였다.³⁶⁾ 나아가 패널은 회원국이 GATT 제21조를 신의성실(good faith)에 따라 원용해야 하며, 해당 조치와 주장된 필수적 안보이익 사이에는 최소한의 타당성(plausibility)이 존재하여야 한다고 판시하였다.³⁷⁾ 이에 따라 패널은 러시아의 통과운송 제한조치는 2014년 우크라이나 사태와 전혀 무관하거나 비상사태로부터 지나치게 동떨어진 조치라고 볼 수 없다고 보고 제21조(b)(iii)로 정당화된다고 판단하였다.³⁸⁾

34) United States, Third-Party Executive Summary, Russia—Traffic in Transit, WT/DS512 (February 27 2018).

35) Panel Report, Russia—Traffic in Transit, para. 7.77

7.77 Therefore, as the existence of an emergency in international relations is an objective state of affairs, the determination of whether the action was “taken in time of” an “emergency in international relations” under subparagraph (iii) of Article XXI(b) is that of an objective fact, subject to objective determination.

36) Panel Report, Russia—Traffic in Transit, para. 7.111

7.111. The Panel recalls its interpretation of “emergency in international relations” within the meaning of subparagraph (iii) of Article XXI(b) as a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state.

37) Panel Report, Russia—Traffic in Transit, paras. 7.131-7.132; 7.138

38) Panel Report, Russia—Traffic in Transit, para. 7.145-7.149

동 사건은 GATT 제21조가 완전히 자기판단적 조항이 아니며, WTO 패널이 국제관계상의 비상사태의 존재와 조치의 신의성실 원칙 부합 여부 및 최소한의 타당성을 객관적으로 심사할 수 있음을 최초로 명확히 한 판례라는 점에서 중요한 의의를 가진다. 이는 안보예외가 무제한적인 면책조항이 아니라 일정한 법적 한계와 사법적 통제를 받는 규범임을 확인한 판례로 평가된다.

2. 안보예외 법리의 심화와 판례의 전개

Russia-Traffic in Transit 사건이 안보예외에 대한 사법심사 가능성을 최초로 확립하였다면, 이후의 WTO 판례들은 이를 개별 조치와 안보이익 간의 관련성 심사, 경제안보 논리의 한계, 그리고 ‘국제관계상 비상사태’의 객관적 범위에 관한 보다 정교한 기준으로 발전시켰다.

「사우디아라비아-지식재산권 보호조치 사건」(Saudi Arabia-Measures Concerning the Protection of Intellectual Property Rights, 이후 Saudi Arabia-Protection of IPRs 사건)은 TRIPS 협정 제73조(안보예외)에 Russia-Traffic in Transit 사건의 법리가 확장 적용된 사건이다. 이른바 카타르위기를 배경으로 사우디아라비아 내에서 카타르 방송사 beIN의 지식재산권이 해적방송을 통해 공공연히 침해되었고, 카타르 기업의 사법구제 접근이 방해받았다.³⁹⁾ 카타르는 2018년 이를 TRIPS 협정 위반으로 제소했고, 사우디아라비아는 카타르와의 외교·영사 관계 단절을 이유로 TRIPS 협정 제73조(b)(iii)를 원용했다.⁴⁰⁾ 동 사건 패널은 TRIPS 제73조(b)(iii)의 문언이 GATT 제21조와 동일하므로 DS512의 해석과 분석틀을 확장 적용할 수 있다고 판시했다.⁴¹⁾ 이에 따르면 GATS 제14조의2에 대해서도 GATT 제21조의 법리 적용이 가능할 것으로 생각된다.

동 사건 패널은 TRIPS 협정 제73조(b)항(iii)의 안보예외 요건 충족 여부를 판단함에 있어 조치별로 분리하여 카타르 국민이 사우디 법률대리인을 선임하고 민사적 구제를 추구하는 것을 제한한 조치에 대해서는 안보예외의 적용을 인정한 반면, beoutQ에 의한 대규모 저작권 침해에 대하여 형사절차 및 처벌을 제공하지 않은 조치는 안보예외에 의해 정

39) Panel Report, Saudi Arabia-Protection of IPRs, paras. 2.1-2.48

40) Panel Report, Saudi Arabia-Protection of IPRs, paras. 3.1-3.4

41) Panel Report, Saudi Arabia-Protection of IPRs, paras. 7.241-7.255.

당화될 수 없다고 판단하였다.⁴²⁾ 이는 안보예외가 일단 원용되었다고 하여 모든 관련 조치가 일괄적으로 정당화되는 것이 아니라, 각 조치가 ‘필수적 안보 이익(essential security interests)’ 보호와 타당한 연관성이 있는지가 개별적으로 평가됨을 보여준 중요한 판례이다. 이를 AI 부분에 적용해보면 GPU 제한, 모델 가중치 제한, API 제한 등을 각각 따로 심사받게 될 수 있다.

「미국-철강 및 알루미늄 제품 사건」(United States—Certain Measures on Steel and Aluminium Products, 이하 United States—Steel and Aluminum Products 사건)은 미국의 자기판단적 조항이라는 주장을 정면으로 배척한 사례이다. 미국은 2018년 무역확장법 제232조에 근거하여 철강 25%, 알루미늄 10% 관세를 부과하면서 이를 국가안보 조치라며 GATT 제21조를 원용했고 중국·노르웨이·스위스·튀르키예 등이 제소했다. 동 사건 패널은 미국의 관세가 미국 WTO 양허표상 양허세율을 초과하여 GATT 제2조 제1항에 위반되며 특정국에 대한 면세는 최혜국 대우(제1조 제1항)에 위반된다고 판시했으며 미국의 안보예외 원용을 배척하면서 관세가 전쟁 또는 국제관계상 비상사태시에 취해진 것이 아니므로 예외 요건을 충족하지 못한다고 판단하였다.⁴³⁾ 이 판결은 안보예외가 전통적인 군사·외교적 위기 상황을 넘어 경제적 경쟁력 유지나 공급망 재편과 같은 광범위한 정책목표를 포섭할 수 있는지 여부를 직접적으로 제기한 사건이라는 점에서 의의가 있다. 이 판결은 공급망 취약성이나 경제적 경쟁력 우려만으로 곧바로 GATT 제21조가 적용되는 것은 아니라는 점을 시사한다. 이에 대해 미국 USTR 대변인 Adam Hodge는 성명으로 이러한 패널 보고서의 결론에 강력히 반대하면서 미국은 70년 넘게 국가안보 문제가 WTO 분쟁해결에서 심사될 수 없으며 WTO는 회원국의 안보위협 대응 능력을 재단할 권한이 없다는 입장을 견지해왔다고 미국은 자국의 필수적 안보에 대한 의사결정권을 WTO 패널에 양도하지 않을 것이라 밝혔다.⁴⁴⁾ 미국은 이 판결에 대해서 상소하였고, 중국이 제232조 관세에 대응하여 부과한 보복 관세 사건(DS558)에서도 제232조 조치가 안보예외에 따라 취해진 조치임을 주장하였다.⁴⁵⁾

「미국-홍콩 원산지 표시 사건」(이하 United States—Origin Marking Requirement) 사건은

42) Panel Report, Saudi Arabia—Protection of IPRs, paras. 7.294

43) Panel Report, United States—Steel and Aluminum Products, 7.164

44) USTR, “Statement from USTR Spokesperson Adam Hodge” (2022. 12. 9.), 온라인 자료 (최종검색일: 2026.7.11.)

45) Panel Report, China—Additional Duties on Certain Products from the United States, WT/DS558/R.

AI 사건과 가장 유사한 구조를 가진 선례로 2020년 홍콩국가보안법 제정을 계기로 트럼프 대통령은 행정명령 제13936호(Executive Order 13936)를 통해 홍콩이 “더 이상 중국과의 차등대우를 정당화할 만큼 충분히 자율적이지 않다”고 판단하고, 홍콩산 제품의 원산지 표시를 ‘홍콩’에서 ‘중국’으로 변경하도록 요구했다.⁴⁶⁾ 홍콩은 이것이 최혜국대우(GATT 제1조 제1항) 및 원산지 표시(GATT 제9조 제1항) 등에 위반된다고 제소했고 미국은 GATT 제21조(b)를 원용했다.

동 사건 패널은 미국이 홍콩의 상황이 ‘국제관계상 비상사태’임을 입증하지 못했으므로 제21조(b)(iii)의 안보예외로 원산지 표시 요건을 정당화할 수 없다고 판시했다.⁴⁷⁾ 미국과 중국 간에 홍콩국가보안법을 둘러싼 정치적 갈등이 존재했음에도 미국과 홍콩 양 당사자가 정상적 경제 및 무역 관계를 지속하고 있었다는 사실에 기초하여 국제관계상 비상사태를 구성한다고 볼 때 요구되는 중대성 기준(requisite level of gravity)에 미치지 못한다고 보았다.⁴⁸⁾ 동 판정은 안보예외의 적용을 위해서는 단순한 정치적 갈등이나 정책적 이견만으로는 부족하며, 정상적인 경제·무역관계를 근본적으로 변화시키는 수준의 중대한 국제적 위기 상황이 객관적으로 존재하여야 함을 다시 한 번 확인하였다는 점에서 의의가 있다. 그러나 판결 이후 USTR은 성명을 내고 미국의 조치는 중국이 홍콩의 자율성과 홍콩 주민들의 민주적 권리 및 인권을 침해하는 행위에 대한 대응이었으며 바이든 행정부는 미국의 국가안보를 보호하고 인권과 민주주의를 증진시키기 위해 노력할 것이라며 WTO는 자신들이 안보 위협으로 간주하는 상황에 대해 해당 회원국이 어떻게 대응할지에 대해 판단할 권한이 없다고 다시 한 번 더 주장하였다.⁴⁹⁾

결론적으로 Russia—Traffic in Transit 사건이 안보예외의 사법심사 가능성을 확립하였다면, Saudi Arabia—Protection of IPRs 사건은 조치별 관련성 심사를 구체화하였고, United States—Steel and Aluminum Products 사건은 경제안보 논리의 무제한적 확장을 견제하였으며, United States—Origin Marking Requirement 사건은 국제관계상 비상사태의 객관적·중대

46) Executive Order 13936, “The President’s Executive Order on Hong Kong Normalization”, 85 Fed. Reg. 43413 (July 14, 2020).

47) Panel Report, United States—Origin Marking Requirement, paras. 7.360

48) Panel Report, United States—Origin Marking Requirement, paras. 7.353

49) USTR, “Statement from USTR Spokesperson Adam Hodge” (2022. 12. 21.), 온라인 자료 (최종검색일: 2026. 7. 11.)

성 요건을 재확인하였다.⁵⁰⁾ 이러한 판례의 흐름은 안보예외가 회원국의 전적인 재량 영역이 아니라 일정한 객관적 한계와 사법적 통제를 받는 것임을 보여준다.

3. GATS의 안보예외의 적용과 한계

지금까지 살펴본 판례는 모두 상품무역(GATT) 또는 지식재산권(TRIPS 협정)에 관한 것이었으나, Fable 5 사건은 AI 모델 및 클라우드 기반 AI 서비스의 제공 등 서비스 무역에 관한 것이다. 따라서 원칙적으로 GATT보다 서비스무역을 규율하는 GATS가 중심적인 검토 대상이 된다. 특히 Fable 5 사건은 AI 모델 자체의 소유권이나 이전을 제한한 것이 아니라 특정 이용자에 대한 서비스 접근(access)을 제한한 조치라는 점에서, 상품의 수입·수출 제한을 전제로 하는 GATT 체계와는 규율 대상에 본질적인 차이가 있다. TRIPS 협정은 특허·저작권 등 지식재산권의 보호와 집행을 중심으로 설계되어 있어, AI 모델 자체에 대한 원격 접근(access), API 기반 서비스 제공, 클라우드 컴퓨팅 자원의 이용 제한과 같은 디지털 시대의 접근권 통제를 직접 규율하지 않는다. 또한 TRIPS 협정은 권리자의 배타적 권리를 보호하는 규범이지, 특정 국가나 이용자에 대한 AI 서비스 제공 여부를 규율하는 시장접근 규범은 아니다. 따라서 Fable 5 사건과 같이 국가안보를 이유로 AI 접근을 제한하는 조치는 GATT나 TRIPS협정 보다 GATS 및 디지털 무역규범의 틀에서 검토될 필요가 있다.

Fable 5 조치는 미국 서비스 시장으로 진입하려는 외국 서비스 또는 서비스공급자를 제한한 조치가 아니라, 미국 서비스공급자의 외국 이용자에 대한 서비스 제공을 제한한 공급국 측 수출통제라는 특징을 가진다. GATS 제16조 및 제17조는 각각 다른 회원국의 서비스 및 서비스공급자에 대한 시장접근과 내국민대우를 규율하므로, 미국산 AI 서비스의 수출 또는 외국 이용자의 접근제한이 곧바로 해당 조항의 위반을 구성한다고 보기는 어렵다. 또한 GATS 제2조 역시 서비스 수령자의 국적이나 수출 목적지에 따른 차별 자체를 직접 규율하는 조항으로 해석하기 어렵다. 따라서 Fable 5 사건은 기존 GATS 의무와 안보예외의 충돌뿐 아니라, 공급국이 자국 서비스의 해외 제공을 제한하는 조치를 GATS가 충

50) 다만 Saudi Arabia-Protection of IPRs 사건, United States-Steel and Aluminum Products 사건 및 United States-Origin Marking Requirement 사건 패널보고서는 DSB에 의해 채택되지 않았으므로 당사국을 구속하는 채택 보고서의 법적 지위를 갖지 않는다. 따라서 이들 보고서의 판단은 확립된 판례라기보다 Russia-Traffic in Transit 사건의 해석들을 후속 분쟁에 적용한 중요한 해석 자료로 평가하는 것이 타당하다.

분히 규율하지 못하는 규범적 공백을 보여준다. 다만 향후 AI 접근통제가 외국 서비스공급자 또는 외국계 기업에 대한 차별적 허가·접근제한의 형태로 설계되는 경우에는 GATS 제2조, 제16조 및 제17조 위반이 성립할 수 있으며, 이 경우 제14조의2의 적용 여부가 직접적으로 문제될 수 있다. GATS 제14조의2는 “이 협정의 어떠한 규정도” 회원국이 자국의 필수적 안보이익 보호를 위하여 필요하다고 인정하는 조치를 취하는 것을 방해하지 않는다고 규정하고 있으며, 문언 구조는 GATT 제21조 및 TRIPS 제73조와 실질적으로 동일하다. 따라서 Russia-Traffic in Transit 사건 및 Saudi Arabia-Protection of IPR 사건에서 제시된 사법심사 가능성, 신의성실 원칙 및 안보이익과 조치 간의 최소한의 타당성에 관한 해석이 GATS 제14조의2에도 유추 적용될 가능성이 높다. 다만 현재까지 이를 직접적으로 판단한 WTO 판례는 존재하지 않으므로, 이러한 해석이 확립된 법리라고 단정하기는 어렵다.

AI 수출통제가 GATS의 적용을 받기 위해서는 우선 AI 모델 API 및 클라우드 기반 AI 서비스가 GATS상 어떠한 서비스에 해당되는지를 우선 검토하여야 한다. GATS의 서비스 분류의 기준이 되는 WTO 문서 MTN.GNS/W/120 및 UN잠정 중앙생산물 분류(UN Provisional Central Product Classification, 이하 CPC)에 따르면 컴퓨터 및 관련 서비스(Computer and Related Services)는 CPC84에 해당한다. 세부적으로는 ▲컴퓨터 하드웨어 설치 관련 컨설팅(CPC 841) ▲소프트웨어 구현 서비스(CPC 842) ▲데이터 처리 서비스(CPC 843) ▲데이터베이스 서비스(CPC 844) ▲기타(CPC 845·849)로 구분된다.⁵¹⁾ WTO의 서비스 분류와 양허 해석에서는 새로운 전달수단의 등장만으로 서비스 분류가 달라지지 않는다는 기술중립적 해석이 제시되어 왔으나, AI-as-a-Service(AIaaS)의 CPC 분류를 직접 확인한 WTO 판정은 아직 존재하지 않는다. 일부 회원국은 이를 W/120에 명시되지 않은 신규 서비스로 보기도 하나 클라우드 서비스 및 AIaaS 역시 GATS의 기술중립성 원칙에 의거하여 기존 CPC 84(컴퓨터 및 관련 서비스) 체계 내에 포섭되는 것으로 해석함이 타당하다고 생각된다.⁵²⁾ 미국의 양허와 관련하여, 미국은 ‘컴퓨터 및 관련 서비스’에 대해 Mode 1(국경간 공급), Mode 2(해외소비), Mode 3(상업적 주재)에 대해서 시장접근 및 내국민 대우와

51) Services Sectoral Classification List, MTN.GNS/W/120 (1991. 7. 10.).

52) Ines Willemyns, “GATS Classification of Digital Services—Does ‘The Cloud’ Have a Silver Lining?”, *Journal of World Trade*, Vol. 53, No. 1 (2019), pp. 59-82. 여기서도 이와 같이 분류하고 논리를 전개하고 있다.

관련하여 완전히 개방하였다.⁵³⁾ 클라우드 기반 AI 서비스와 AI 모델 API가 CPC 84의 컴퓨터 및 관련 서비스에 포섭되고, 미국이 해당 분야의 Mode 1 공급에 대하여 시장접근 및 내국민대우 제한을 기재하지 않았다는 사실만으로 Fable 5 접근제한 조치가 GATS 제16조 및 제17조에 위반된다고 단정할 수는 없다. 제16조와 제17조는 각각 다른 회원국의 서비스 및 서비스공급자에게 부여되는 시장접근과 내국민대우를 규율하는 반면, Fable 5 조치는 미국 서비스공급자의 외국 이용자에 대한 서비스 제공을 제한한 공급국 측 조치이기 때문이다. 외국 이용자는 AI 서비스의 이용자 또는 소비자라는 지위만으로는 GATS 제16조 및 제17조가 직접적인 대우의 대상으로 규정하는 다른 회원국의 서비스 또는 서비스공급자에 해당하지 않으며, 미국의 구체적 약속 역시 미국 서비스공급자의 서비스 수출이나 외국 이용자의 미국산 서비스 접근을 직접 보장하는 것으로 해석하기 어렵다. 이러한 점에서 Fable 5 사건에서의 접근제한은 적어도 GATS 제16조 및 제17조의 적용 측면에서 공급국의 서비스 수출통제를 충분히 규율하지 못하는 현행 GATS 체제의 한계를 보여주는 사례로 평가할 수 있다.

다만 향후 AI 접근통제가 국가별 등급에 따라 다른 회원국의 클라우드·AI·사이버보안 서비스 또는 서비스공급자에게 상이한 API 접근·통합·재판매 조건을 부여하거나, 외국 서비스공급자의 미국 시장 진입을 제한하는 방식으로 설계된다면 GATS 제2조·제16조·제17조와의 불합치가 문제될 수 있다. 따라서 이하의 분석은 실제 Fable 5 조치가 해당 의무에 위반된다고 전제하는 것이 아니라, AI 모델 접근통제가 그 구체적인 설계에 따라 GATS상 의무에 불합치하는 것으로 판단되는 경우 제14조의2에 의해 정당화될 수 있는지를 검토하는 가정적 분석으로 한정한다.

IV. WTO 안보예외 법리의 Fable 5 사건에 대한 적용과 시사점

1. 안보예외 법리의 적용

이하에서는 가정적 분쟁 시나리오로 만약 AI 접근 차단으로 인한 자국 서비스 이용자·기업의 피해를 이유로 GATS 상의 의무 위반을 주장하며 제소하고, 이에 대해 미국이

53) United States of America, Schedule of Specific Commitments, GATS/SC/90 (1994); USITC, U.S. Schedule of Commitments under the General Agreement on Trade in Services (1998).

GATS 제14조의2 제1항 (b)(iii)를 원용하는 경우를 상정하여, DS512가 확립한 심사기준을 요건별로 분해하여 GATS 제14조의2를 통한 정당화에 중점을 두고 검토해 보도록 하겠다. GATS 제14조의2의 문언은 GATT 제21조와 실질적으로 동일하므로 앞서 검토한 판례의 분석틀이 그대로 원용될 수 있다는 전제에서 ① 국제관계상 비상사태의 존재, ② 필수적 안보이익의 표명, ③ 조치와 안보이익 간의 타당성, ④ 신의성실 원칙 부합 여부 등 네 요소로 나누어 살펴본다.

(1) 국제관계상 비상사태의 존재 여부

Table 5 사건에 WTO 사건에서의 안보예외 법리를 적용하면, 국제관계상 비상사태 요건의 충족을 인정하기에는 상당한 해석상 어려움이 존재한다.

첫째, 원용 가능한 후보인 미·중 AI 기술패권 경쟁은 상시적·구조적 경쟁상태이지 시간적·공간적으로 특정 가능한 ‘사태(event)’가 아니다. US-Origin Marking Requirement 패널이 홍콩국가보안법을 둘러싼 미·중 간의 정치적 긴장조차 국제관계상 비상사태로 보기 위해 요구되는 중대성 기준에 미달한다고 판단한 점에 비추어 보면, 기술경쟁 일반을 곧바로 국제관계상의 비상사태로 포섭하는 해석은 기존 WTO 판례가 제시한 개념적 범위와 상당한 긴장관계를 형성한다.

둘째, 통제의 직접적 계기는 지정학적 사건이 아니라 보도에 따르면 연구진이 발견한 탈옥 기법이라는 기술적 사건이었던 것으로 알려져 있다.⁵⁴⁾ 특정 모델의 안전성 및 보안성에 관한 기술적 취약성은 규제상 위협의 문제일 수 있으나, 그 자체가 국가 간 관계의 파탄, 무력충돌 또는 고조된 정치·외교적 위기를 의미하는 것은 아니다.

셋째, GATT 제21조(b)(iii)는 조치가 비상사태 ‘시에(in time of)’ 취해질 것을 요구함으로써 안보예외의 시간적 범위를 한정하고 있다. 그런데 상시적인 기술패권 경쟁 자체를 비상사태로 이해하게 되면 이러한 시간적 제한은 사실상 의미를 상실하게 되고, 안보예외는 특정한 위기 상황에 대한 예외가 아니라 항구적인 정책재량으로 전환될 위험이 있다. 물론 미국은 AI 기술패권 경쟁 자체가 국가의 필수적 안보이익에 대한 지속적 위협이라고 주장하면서 이를 국제관계상의 비상사태로 재구성하려 할 가능성이 있다. 그러나 현재까

54) Anisha Sircar, “Anthropic Disabled Fable 5 And Mythos 5 After A U.S. Export-Control Order. Here’s What Happened,” *Forbes* (June 16, 2026), 온라인 자료 (최종검색일: 2026. 7. 11.).

지의 WTO 판례는 상시적 기술경쟁 자체를 제21조(b)(iii)의 비상사태로 인정한 바 없으며, 이를 뒷받침하는 직접적인 선례 역시 존재하지 않는다.

(2) 필수적 안보이익의 특징

Russia-Traffic in Transit 사건 패널은 ‘필수적 안보이익(essential security interests)’의 내용에 관하여 원용국에 상당한 재량을 인정하면서도, 해당 이익이 무엇인지를 표명(articulate)할 의무를 부과하였다.⁵⁵⁾ 프린티어 AI 모델의 고도화된 사이버 공격 역량이 적성 행위자의 수중에 들어가는 것을 방지함으로 얻는 이익은, Russia-Traffic in Transit 사건에서 언급한 ‘외부 위협으로부터 국가의 영토와 주민을 보호하는 기능’⁵⁶⁾과 일정한 관련성을 가질 수 있으므로, 적어도 필수적 안보이익의 특징이라는 측면에서는 미국에 비교적 유리하게 작용할 가능성이 있다.

그러나 통제 서한이 국가안보 우려의 구체적 내용을 충분히 제시하지 않았다는 점은, 필수적 안보이익의 표명 의무 충족 여부에 상당한 의문을 제기한다. 특히 원용국이 분쟁 단계에서 사후적으로 안보이익을 재구성하는 방식은 신의성실 원칙과 결합하여 불리하게 평가될 가능성이 있다.

더욱이 통제 철회 과정에서 Howard Lutnick은 X(과거 트위터)에 ‘미국의 AI 리더십 강화(strengthen America’s leadership in AI)’를 주요 성과로 언급하였는데,⁵⁷⁾ 이 점은 해당 조치에 안보 목적뿐 아니라 산업경쟁력 확보 또는 기술우위 유지라는 비안보적 고려가 함께 작용하였을 가능성을 시사한다. 물론 경제적 경쟁력 제고가 국가안보와 완전히 무관하다고 단정할 수는 없지만 US-Origin Marking Requirement 패널이 경제안보 논리를 국제관계상 비상사태와 직접 연결짓는 데 신중한 태도를 취하였다는 점에 비추어 보면, 순수한 산

55) Panel Report, Russia-Traffic in Transit, paras. 7.131-7.136

56) Panel Report, Russia-Traffic in Transit, paras. 7.130

7.130. “Essential security interests”, which is evidently a narrower concept than “security interests”, may generally be understood to refer to those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally.

57) Howard Lutnick (@howardlutnick), “Over the past two weeks, we have worked closely with Anthropic to analyze and approve Fable 5 to ensure alignment across the US Government and strengthen America’s leadership in AI,” X, 온라인 자료(최종검색일: 2026. 7. 11.)

업경쟁력 또는 기술우위 확보를 제21조(b)가 예정한 필수적 안보이익과 동일시하는 데에는 상당한 해석상 어려움이 존재한다.

(3) 조치와 안보이익 간의 개연성 있는 관련성

Russia-Traffic in Transit 사건의 관련성 심사는 해당 조치와 주장된 필수적 안보이익 사이에 최소한의 타당성(plausibility)이 존재하여야 한다⁵⁸⁾는 제한적인 심사에 그친다. 그러나 Saudi Arabia-Protection of IPR 사건이 보여주듯, 이러한 관련성 심사는 조치별·사안별로 개별적으로 이루어진다. 이러한 관점에서 Table 5 통제는 적어도 두 가지 측면에서 관련성 심사의 대상이 될 수 있다.

첫째, 과잉포섭(over-inclusiveness)의 문제이다. 만약 표명된 안보이익이 ‘적성 행위자에 대한 AI 역량 유출 방지’라면, 동맹국 국민, 적법한 신원확인 절차를 거친 외국인 직원 또는 기존 계약관계에 있는 기업 이용자까지 국적만을 기준으로 광범위하게 제한하는 조치는 표명된 안보이익과 조치 사이의 정합성에 의문을 제기한다.

둘째, 과소포섭(under-inclusiveness)의 문제이다. 엔트로픽이 지적하였듯이 동일한 탈옥 기법을 통해 유사한 역량을 유도할 수 있는 Chat GPT 5.5와 같은 다른 프런티어 AI 모델은 규제 대상에 포함되지 않았다. 만일 표명된 안보이익이 실제로 해당 위협의 방지에 있다면, 기능적으로 유사한 위협원을 그대로 방치하는 것은 조치와 안보이익 사이의 관련성 주장에 대한 설득력을 약화시킬 수 있다.

나아가 해당 조치가 시행 후 불과 십여일 만에 전면 철회되었다는 사후적 경과는, 당초 주장된 위협이 전면적인 접근 차단이라는 예외적 조치를 정당화할 정도로 중대하고 긴급한 것이었는지에 관한 의문을 제기한다.

(4) 신의성실 원칙과의 부합 여부

Russia-Traffic in Transit 사건 패널은 안보예외가 회원국의 WTO 상의 의무를 “우회(circumvent)하기 위한 수단”으로 원용되어서는 안 된다고 판시함으로써, 신의성실을 안보예외 남용 통제의 핵심 원리로 제시하였다.⁵⁹⁾ 조치의 형성과정에서 제기된 행정부와 해당

58) Panel Report, Russia-Traffic in Transit, paras. 7.131-7.132; 7.138

59) Panel Report, Russia-Traffic in Transit, paras. 7.133

기업 간의 갈등 및 관련 정치적 배경이 분쟁의 사실심리 과정에서 증거로 제출될 경우, 이는 조치가 순수한 안보 목적 이외의 고려에 의해 영향을 받았을 가능성을 시사하는 정황 증거(circumstantial evidence)로 기능하여, 해당 조치가 신의성실 원칙에 부합하는지에 대한 의문을 더욱 증대시킬 수 있다.

2. AI 수출통제에 대한 WTO 안보예외 적용의 함의와 한계

AI 수출통제는 기존 WTO 안보예외 판례가 전제하였던 사실관계와 구조적으로 상이한 특성을 가진다.

(1) 국제관계상 비상사태 개념의 상시화

WTO에서 문제 제기된 국가안보조치는 모두 크림 위기, 카타르 단교 및 홍콩국가보안법과 같이 시간적·공간적으로 특정 가능한 지정학적 위기를 전제로 하였다. *Russia – Traffic in Transit* 패널도 제21조(b)항 (iii)호의 의미에서 “국제관계상의 비상사태”를, 무력 충돌이나 잠재적 무력 충돌, 또는 고조된 긴장이나 위기, 혹은 한 국가를 뒤덮거나 둘러싼 전반적인 불안정 상태의 상황으로 해석하였다.⁶⁰⁾ 그러나 AI 수출통제는 특정한 위기 상황보다는 장기적 기술패권 경쟁과 잠재적 오용 가능성 자체를 안보위협으로 규정한다는 점에서 기존 판례와 구조적 차이를 가진다.

(2) 비물리적 디지털 자산에 대한 접근권 통제

기존 WTO 국가안보 분쟁은 철강제품, 통과화물 또는 원산지 표시와 같이 국경을 통과하는 물리적 대상에 대한 규제였다. 반면 AI 모델 가중치, API 접근권 및 클라우드 컴퓨팅 서비스는 국경의 개념이 불명확한 사이버 공간에서 제공되는 비물리적 자산이다. 따라서 문제의 핵심은 물리적 재화의 이전이 아니라 특정 이용자에 대한 디지털 연산능력과 추론 서비스의 제공 여부를 국가가 통제할 수 있는지에 있다.

7.133. The obligation of good faith requires that Members not use the exceptions in Article XXI as a means to circumvent their obligations under the GATT 1994.[...]

60) Panel Report, *Russia – Traffic in Transit*, paras. 7.111

7.111. The Panel recalls its interpretation of “emergency in international relations” within the meaning of subparagraph (iii) of Article XXI(b) as a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state.

(3) 이중용도성 심화와 예방적 통제의 정당화

AI는 상업적 활용과 군사적 활용이 실시간으로 공존하는 대표적인 범용기술(*general-purpose technology*)이자 이중용도 기술이다. 고성능 파운데이션 모델은 민간 서비스 제공을 목적으로 개발되었더라도 미세조정(*Fine-Tuning*)이나 프롬프트 엔지니어링을 통해 사이버 공격, 정보전 또는 대량살상무기 설계에 활용될 가능성을 완전히 배제하기 어렵다. 이에 따라 규제국은 전통적인 전략물자에 비해 훨씬 예방적이고 광범위한 통제의 필요성을 주장할 유인을 가지게 된다.

결국 AI 수출통제는 기존 WTO 판례가 전제하였던 ‘객관적으로 확인 가능한 국제관계상의 비상사태’와 디지털 기술이 갖는 ‘상시적·잠재적 위험성’이 정면으로 충돌하는 지점에 위치한다. 디지털 영역, 특히 AI 핵심기술에 대한 국가안보적 통제는 전통적인 상품무역 규제와 구별되는 질적 특수성을 가지므로, 기존 GATT 제21조 법리를 그대로 적용할 수 있는지에 대해서는 상당한 법리적 불확실성이 존재한다.

나아가 AI 수출통제는 국가가 물리적 재화가 아니라 ‘디지털 역량(*digital capabilities*)’ 및 그에 대한 ‘접근권’ 자체를 전략자산으로 규율하기 시작하였음을 보여주며, 이는 안보예외의 해석과 적용 범위를 근본적으로 재검토하도록 요구하는 새로운 국제경제법적 과제를 제기한다. 안보예외를 전적으로 자기판단에 맡길 경우 예외가 일반원칙을 잠식할 우려가 있다. 반대로 국가안보 판단에 대하여 과도한 실체심사를 요구할 경우에는 주요 국가들이 WTO 분쟁해결체계에 대한 수용성을 약화시킬 가능성도 배제하기 어렵다. 따라서 양 극단을 지양하는 제도적 균형이 요구된다. 이를 위해서는 안보예외의 절차적 정당성을 제도적으로 구체화할 필요가 있다. 현행 판례상 안보예외에 일반예외와 동일한 최소침해성 심사가 확립되었다고 보기는 어렵다. 이하의 단계적 규제 및 덜 제한적인 대안 검토는 현행법의 직접적 요건이라기보다 향후 절차적 정당성을 강화하기 위한 규범적 제안이다. 구체적으로는 신의성실 원칙에 기초하여 안보이익의 명확한 표명 의무를 사전통지 및 이 유제시 의무의 형태로 제도화하고, 전면적 접근 차단은 최후의 수단으로 한정할 필요가 있다. 그 이전 단계에서는 이용 목적의 제한, 이용자 인증, 사후 모니터링 등 덜 제한적인 조치를 우선적으로 고려하고, 위험 수준에 따른 단계적 규제를 통해 위험이 해소된 경우에는 접근권을 회복할 수 있는 복원 메커니즘도 함께 마련되어야 한다. 이러한 절차적·비례적 통제장치는 국가안보 보호와 국제통상규범의 예측가능성 사이의 균형을 확보하는

데 기여할 수 있을 것이다.

3. 한국에 대한 입법적 시사점

국내법제 차원의 과제로는 「대외무역법」의 다자주의적 설계와 현실의 수출통제 질서 간의 긴장을 들 수 있다. 현행 「대외무역법」 제19조는 산업통상자원부장관이 “국제수출통제체제 또는 이에 준하는 다자간 수출통제 공조”(이하 ‘국제수출통제체제등’)에 따라 수출 허가 등 제한이 필요한 물품 등을 지정·고시하도록 규정하고 있다. 시행령이 열거하는 국제수출통제체제는 바세나르체제, 핵공급그룹(NSG), 미사일기술통제체제(MTCR), 오스트레일리아그룹(AG) 등 공식적인 다자 수출통제체제로 한정되어 있으므로, 현행 법체계는 전략물자 통제의 정당성 근거를 국제적 합의에 기반한 다자주의에 두고 있다고 이해할 수 있다. 그러나 앞서 살펴본 바와 같이, 최근 AI 모델과 첨단 반도체를 둘러싼 수출통제는 기존의 바세나르체제와 같은 공식 다자체제보다는 미국을 중심으로 한 일방적 또는 소다자(minilateral) 방식으로 빠르게 재편되고 있다. AI 모델 가중치는 물론 첨단 GPU 역시 현재까지 공식적인 국제수출통제체제의 통제목록에 포함된 바 없다. 이와 같은 국제질서의 변화는 국내법에도 구조적인 긴장을 초래한다. 즉, 우리나라가 미국 등 우방국과의 공조에 따라 새로운 AI 관련 품목을 전략물자로 지정하려는 경우, 그 지정이 「대외무역법」 제19조가 예정한 ‘국제수출통제체제등에 따른’ 지정에 해당하는지 여부가 명확하지 않기 때문이다. 2024년 「대외무역법」 개정으로 신설된 ‘이에 준하는 다자간 수출통제 공조’는 공식 다자체제가 포섭하지 못하는 신기술 분야의 공조를 수용할 수 있는 근거를 마련하였다는 점에서 의미가 있다. 다만 그 인정 기준과 범위는 여전히 불명확한 측면이 있다.

첫째, ‘이에 준하는 다자간 수출통제 공조’와 관련하여 시행령상 외형적 기준은 있지만 실질적 판단 기준과 절차가 부족하다. 현행 시행령은 ‘이에 준하는 다자간 수출통제 공조’의 외형적 범위를 일정 부분 구체화하고 있다. 다만 ‘다수의 회원국’, ‘지지’, ‘공조’의 판단 기준과 필요한 문서화 수준, 상호적 의사결정 구조의 존재 여부가 여전히 불명확하다. 특히 특정 국가의 일방적 조치에 다른 국가들이 병행적으로 동참한 경우와 공동의 의사결정 절차에 따른 소다자 공조를 구별할 기준이 충분히 제시되어 있지 않다.

둘째, 국제공조를 전제로 하는 현행 체계에서는 국가의 독자적 AI 전략기술 지정권한이 충분히 확보되어 있는지 검토가 필요하다. 미국은 ECRA 및 EAR에 근거하여 행정부가 새

로운 전략기술을 비교적 폭넓게 지정할 수 있는 권한을 보유하고 있으며, EU는 이중용도 규정(Regulation (EU) 2021/821) 제9조를 통해 회원국의 국가통제(National Control)를 인정하고 있다. 일본 역시 2023년 「외국환 및 외국무역법」(외환법)에 의거한 하위 규정을 개정하여 반도체 제조장비에 대한 독자적 수출통제를 실시하였다. 이에 비해 우리 「대외무역법」은 여전히 국제공조를 지정의 전제로 하고 있어, 향후 우리나라가 프런티어 AI 모델이나 핵심 AI 컴퓨팅 자산을 자체적으로 보유하게 될 경우 국가안보 판단에 기초한 독자적 통제를 실시할 명문의 법적 근거가 충분히 마련되어 있다고 보기 어렵다.

셋째, 다자주의적 설계는 WTO 안보예외의 정당성을 뒷받침하는 근거인 만큼, ‘이에 준하는 공조’를 지나치게 확대 해석하는 것은 신중해야 한다. ‘이에 준하는 공조’를 지나치게 확장 해석하여 사실상 일방적 통제까지 폭넓게 포섭하게 될 경우, 우리나라 역시 안보예외의 자의적 운용이라는 비판으로부터 자유롭기 어려워질 수 있다.

따라서 향후에는 절차적 정당성을 중심으로 한 국내법적 보완이 필요하다. 구체적으로는 ‘이에 준하는 다자간 수출통제 공조’의 인정 기준(참여국의 범위, 상호주의 여부, 문서화된 공조체계의 존재 등)을 시행령 또는 고시에서 보다 구체적으로 제시하고, 전략물자 지정 시 지정 사유의 공개와 정기적인 재검토 절차를 제도화할 필요가 있다. 이러한 절차적 장치를 마련한다면 AI 시대 수출통제의 절차적 정당성을 제도화하는 규범 선도국으로서 국제적 신뢰를 확보할 수 있을 것이다. 나아가 이러한 국내법적 절차화는 국가안보를 이유로 한 수출통제가 국제경제법 질서 속에서도 정당성을 인정받기 위한 중요한 제도적 기반이 된다. 결국 국내법의 절차적 정당성과 국제경제법의 규범적 정당성은 상호 분리된 문제가 아니라 하나의 연속선상에서 이해되어야 한다.

V. 결론

Table 5 사건은 프런티어 AI 모델에 대한 접근이 국가안보를 이유로 제한될 수 있음을 보여준 초기 사례이다. 다만 정부 지시문을 포함한 공식 자료가 제한적으로 공개되어 있고 관련 소송도 본안판단 없이 종료되었으므로, 이 사건만을 근거로 AI 접근권의 법적 성격이나 국제경제법질서의 근본적인 변화를 단정하는 것은 신중할 필요가 있다. 그럼에도 이 사건은 모델 가중치나 소스코드의 이전과 호스팅된 AI 모델에 대한 원격 API 이용을 현행

수출통제법상 동일하게 취급할 수 있는지, 그리고 국가가 자국 AI 서비스의 해외 제공을 어떠한 법적 근거와 절차에 따라 제한할 수 있는지라는 새로운 문제를 구체적으로 드러냈다는 점에서 의미가 있다.

미국 국내법적 측면에서 보면, ECRA와 EAR은 통제대상 기술 또는 소스코드가 외국인에게 공개되거나 이전되는 경우 이를 수출로 취급할 수 있는 근거를 마련하고 있다. 그러나 일반 이용자가 호스팅된 AI 모델에 질의를 전송하고 추론 결과를 제공받는 것이 EAR상 통제대상 기술 또는 소스코드의 공개에 해당하는지는 명확하지 않다. Fable 5 사건과 이에 관한 Legion LegalTech 사건은 이러한 법적 불확실성을 보여주었지만, 관련 소송이 자진취하 됨에 따라 호스팅형 AI 모델 접근에 대한 ECRA 및 EAR의 적용범위는 법원의 본안판단을 받지 못한 채 남게 되었다. 따라서 향후 AI 수출통제에서는 모델 가중치, 소스코드, 목적코드, 원격 API 접근 및 추론서비스를 구별하고 각각의 통제 근거와 요건을 명확히 할 필요가 있다.

국제경제법적 측면에서도 Fable 5형 접근제한 조치는 기존 GATS가 충분히 예상하지 못한 규율상의 문제를 제기한다. 이 조치는 외국 서비스공급자의 미국 시장 진입을 제한한 것이 아니라 미국 서비스공급자의 해외 서비스 제공을 제한한 공급국 측 조치라는 점에서, GATS 제16조 및 제17조 위반이 곧바로 성립한다고 단정하기 어렵다. 이는 AI 접근통제에 GATS가 적용되지 않는다는 의미라기보다, 서비스 수출국이 자국 서비스의 해외 제공을 제한하는 조치를 현행 GATS가 충분히 규율하지 못할 가능성을 보여준다. 반면 국가별 등급에 따라 다른 회원국의 동종 서비스 또는 서비스공급자에게 AI 모델의 접근·통합·재판매 권한을 차등적으로 부여하는 조치라면 GATS 제2조의 최혜국대우 의무가 문제될 수 있다. 이러한 경우 규제국이 GATS 제14조의2 제1항 (b)(iii)을 원용하기 위해서는 구체적인 국제관계상 비상사태의 존재와 필수적 안보이익을 제시하고, 조치와 해당 안보이익 사이에 최소한의 개연성이 있음을 보여주어야 한다. 상시적인 기술경쟁이나 산업경쟁력 확보라는 목적만으로 이러한 요건이 당연히 충족된다고 보기는 어렵다.

WTO 상소기구의 기능정지로 인해 안보예외에 관한 패널보고서의 채택과 구속력 있는 최종판정의 확보가 어려워졌다는 점은 국가안보예외의 남용 가능성을 더욱 높인다. 그러나 이러한 제도적 한계가 WTO 규범에 기초한 법적 분석의 필요성을 소멸시키는 것은 아니다. 안보예외에 관한 판정례에서 제시된 국제관계상 비상사태, 필수적 안보이익, 조치와

안보이익 간 개연성 및 신의성실 원칙은 회원국 간 협의, 국내 수출통제조치의 설계 및 향후 디지털무역규범의 형성에서도 중요한 판단기준이 될 수 있다. 특히 GATS 제14조의2 제2항이 안보예외에 따라 취한 조치와 그 종료를 가능한 최대한 서비스무역이사회에 알리도록 규정하고 있다는 점을 고려하면, 조치의 법적 근거·대상·기간·위험평가 및 종료 여부를 명확히 하는 절차적 통제는 현행 협정문에 내재한 의무를 구체화하는 의미도 가진다.

Table 5 사건은 외국 AI 플랫폼과 컴퓨팅 인프라에 의존하는 국가와 기업에 접근의 지속가능성이라는 위협을 환기하였다. 정당한 대가를 지급하고 합법적으로 이용하던 AI 서비스도 국가안보를 이유로 중단될 수 있다는 우려는 기존에 진행되어 온 소버린 AI와 공급망 다변화의 필요성을 더욱 부각시킬 수 있다. 다만 이러한 대응이 모든 기술을 국내에서 독자적으로 개발하는 완전한 자립을 의미할 필요는 없다. 복수의 AI 모델과 클라우드 서비스를 활용하고, 대체 가능한 컴퓨팅 인프라를 확보하며, 특정 공급자에 대한 과도한 의존을 완화하는 전략적 다변화가 보다 현실적인 대응이 될 수 있다.

한국은 반도체 하드웨어와 AI 모델 양면에서 일정한 역량을 보유하면서도 미국산 기술과 GPU 및 글로벌 클라우드 공급망에 대한 의존도가 높은 구조에 놓여 있다. 따라서 반도체, 컴퓨팅 인프라 및 파운데이션 모델로 이어지는 국내 역량의 강화와 공급망 다변화는 단순한 산업진흥을 넘어 AI 접근의 지속가능성을 확보하기 위한 정책으로 이해할 필요가 있다. 이와 함께 한국은 DEPA와 IPEF 등 디지털통상 협력체계에서 국가안보예외의 자의적 원용을 억제하기 위한 통지, 이유제시, 정기적 재검토 및 종료 절차의 구체화를 제안할 수 있다. 국내적으로도 「대외무역법」상 AI 관련 통제대상과 지정 근거를 명확히 하고, 수출통제조치의 사유 공개와 정기 재검토 절차를 강화함으로써 국가안보와 국제통상규범의 예측가능성 사이의 균형을 확보해야 한다.

결국 AI 접근통제에 관한 국제경제법의 과제는 국가안보와 자유무역 중 어느 하나를 선택하는 데 있지 않다. 핵심은 모델 가중치·소스코드·API 접근 및 추론서비스를 구별하고, 각각의 위협에 상응하는 통제수단을 설계하며, 조치의 근거와 적용범위 및 존속기간을 투명하게 제시하는 데 있다. 이러한 절차적 정당성과 위험기반 규율은 국가의 정당한 안보이익을 보장하면서도 디지털 시장의 개방성·예측가능성과 국제적 신뢰를 유지하기 위한 최소한의 규범적 조건이라고 할 수 있다.

참고문헌

I. 국내외문헌

구모란(2026), “WTO 안보예외 분쟁의 유형화와 대응전략에 관한 연구”, 통상법무정책: 법무부, 2026-1, pp. 77-106

김혁중(2026), “트럼프 2기 반도체 수출통제 정책 동향과 시사점”, 오늘의 세계경제: 대외경제정책연구원, 26-17

박주현(2024), “WTO 안보예외조항 연구: WTO 미-중 반도체 분쟁 및 분쟁해결기구(DSB)에 대한 시사점”, 통상법률: 법무부, 2024-02, pp. 3-33

Farrell, Henry and Abraham L. Newman, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion,” *International Security*, Vol. 44, No. 1, pp. 42-79. 2019.

Maruyama, Warren & Alan Wm. Wolff. Saving the WTO from the National Security Exception. Peterson Institute for International Economics Working Paper No. 23-2, May 2023.

Willems, Ines. “GATS Classification of Digital Services: Does ‘The Cloud’ Have a Silver Lining?,” *Journal of World Trade*, Vol. 53, No. 1, pp. 59-82. 2019.

II. WTO 문서

United States of America, Schedule of Specific Commitments, GATS/SC/90 (1994)

WTO Executive Summary of the Submissions of the United States of America, Russia — Measures Concerning Traffic in Transit, WT/DS512, 27 February 2018.

WTO Panel Report, Russia—Measures Concerning Traffic in Transit, WT/DS512/R, adopted 26 April 2019.

WTO Panel Report, Saudi Arabia—Measures Concerning the Protection of Intellectual Property Rights, WT/DS567/R, circulated 16 June 2020.

WTO Panel Report, United States—Certain Measures on Steel and Aluminum Products, WT/DS544/R, circulated 9 December 2022.

WTO Panel Report, China—Additional Duties on Certain Products from the United States, WT/DS558/R, circulated 14 August 2023.

WTO Panel Report, United States—Origin Marking Requirement, WT/DS597/R, circulated 21 December 2022.

WTO Services Sectoral Classification List, MTN.GNS/W/120, 10 July 1991.

III. 법령 및 정부 문서 (Statutes & Official Documents)

Export Control Reform Act (ECRA) of 2018, 50 U.S.C. §§ 4801-4852.

International Emergency Economic Powers Act (IEEPA) of 1977, 50 U.S.C. §§ 1701-1707.

Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018, Pub. L. 115-232.

Executive Order 13936, “The President’s Executive Order on Hong Kong Normalization,” 85 FR 43413 (July 14, 2020).

Executive Order 14105, “Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern,” 88 FR 54867 (August 2023).

US Bureau of Industry and Security (BIS), “Revisions to Definitions in the Export Administration Regulations,” 81 FR 35586 (June 3, 2016)

US Bureau of Industry and Security (BIS), “Implementation of Additional Export Controls: Certain Advanced Computing Items,” 87 FR 62186 (October 13, 2022); 88 FR 73458 (October 2023) ; 89 FR 23876 (April 4, 2024).

US Bureau of Industry and Security (BIS), “Framework for Artificial Intelligence Diffusion,” Interim Final Rule, 90 Fed. Reg. 4544 (Jan. 15, 2025).

IV. 기타 인터넷 자료 및 언론 보도 (Online Sources & News)

Anthropic, “Claude Fable 5 and Claude Mythos 5,” Anthropic News, June 9, 2026; updated July 1, 2026, <https://www.anthropic.com/news/claude-fable-5-mythos-5> (최종검색일: 2026. 7. 11.).

Anthropic, “Statement on the US government directive to suspend access to Fable 5 and Mythos 5,” Anthropic News, June 12, 2026, <https://www.anthropic.com/news/fable-mythos-access> (최종검색일: 2026. 7. 11.).

미국 컬럼비아 특별구 연방지방법원, Legion LegalTech, Corp. v. United States of America, No. 1:26-cv-02225-RJL, 소장(Complaint), ECF No. 1 (D.D.C. filed June 23, 2026), <https://storage.courtlistener.com/recap/gov.uscourts.dcd.293776/gov.uscourts.dcd.293776.1.0.pdf> (최종검색일: 2026. 7. 11.).

Notice of Voluntary Dismissal Without Prejudice, Legion LegalTech Corp. v. United States of America, No. 1:26-cv-02225-RJL, ECF No. 7 (D.D.C. filed July 3, 2026), CourtListener, <https://www.courtlistener.com/docket/73520460/legion-legaltech-corp-v-united-states-of-america/> (최종검색일: 2026. 7. 11.).

Harvard Law Review Blog (June 26, 2026), “Is Access to Fable an Export?”, <https://harvardlawreview.org/blog/2026/06/is-access-to-fable-an-export/> (최종검색일: 2026. 7. 11.).

Mayer Brown, “Commerce Department Extends Export Controls to Advanced AI Models,” Insights (June 30, 2026), <https://www.mayerbrown.com/en/insights/publications/2026/06/commerce-department-extends-export-controls-to-advanced-ai-models-authorizes-release-to-specific-trusted-partners> (최종검색일: 2026. 7. 11.).

Lutnick, Howard. “Over the past two weeks, we have worked closely with Anthropic to analyze and approve Fable 5 to ensure alignment across the US Government and strengthen America’s leadership in AI.” X.

<https://x.com/howardlutnick/status/2072100729603452965> (최종검색일: 2026. 7. 11.).

Sircar, Anisha (2026), “Anthropic Disabled Fable 5 And Mythos 5 After A U.S. Export-Control Order. Here’s What Happened,” Forbes (June 16, 2026).

<https://www.forbes.com/sites/anishasircar/2026/06/16/anthropic-disabled-fable-5-and-mythos-5-after-a-u-s-export-control-order-heres-what-happened/>(최종검색일: 2026. 7. 11.).

USTR, “Statement from USTR Spokesperson Adam Hodge” (2022. 12. 9.).

<https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/statement-ustr-spokesperson-adam-hodge> (최종검색일: 2026. 7. 11.).

USTR, “Statement from USTR Spokesperson Adam Hodge” (2022. 12. 21.).

<https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/statement-ustr-spokesperson-adam-hodge-0> (최종검색일: 2026. 7. 11.).

[국문초록]

국가안보를 이유로 한 AI 수출통제의 국제경제법적 분석

- Fable 5 사건과 AI 접근권의 전략자산화를 중심으로

강민지

최근 프런티어 AI 모델이 국가안보와 밀접한 전략기술로 인식되면서 미국을 중심으로 AI 모델과 컴퓨팅 자원에 대한 접근을 제한하는 새로운 형태의 수출통제가 등장하고 있다. Fable 5 사건은 유형재화나 모델 가중치의 국경 간 이전이 아니라 호스팅된 AI 모델에 대한 접근 자체가 수출통제의 대상이 될 수 있음을 보여준 사례이다. 다만 관련 정부 지시문이 공개되지 않았고 후속 소송도 본안판단 없이 종료되었다는 점에서, 이 사건은 미국 수출통제법상 원격 AI 모델 접근의 취급과 WTO 안보예외의 적용범위에 관한 새로운 법적 쟁점을 제기한 사례로 이해할 필요가 있다.

본 연구는 미국의 AI 수출통제 법제를 중심으로 「2018년 수출통제개혁법」(ECRA)과 수출관리규정(EAR)의 법적 구조를 검토하고, 모델 가중치·소스코드의 이전과 API를 통한 호스팅형 AI 모델의 원격 이용을 구별하여 후자가 현행법상 수출 또는 수출간주에 포함될 수 있는지를 분석하였다. 또한 공급국이 자국 서비스공급자의 해외 서비스 제공을 제한하는 조치는 GATS 제16조의 시장접근 및 제17조의 내국민대우 의무에 반드시 포섭되는 것은 아니며, 이러한 조치가 현행 GATS의 규율 공백을 드러낼 수 있음을 지적하였다. 다만 AI 접근제한이 그 구체적인 설계에 따라 GATS상 의무에 불합치하는 경우를 전제로, GATT 제21조와 TRIPS 협정 제73조에 관한 WTO 패널보고서를 토대로 GATS 제14조의2의 적용 가능성과 한계를 검토하였다.

안보예외의 원용을 회원국의 전적인 자기판단에 맡기면 GATS상 의무가 약화될 수 있는 반면, 국가안보 판단에 대한 과도한 실체심사는 다자통상규범에 대한 회원국의 수용성을 저하시킬 수 있다. 이에 본 연구는 GATS 제14조의2 제2항의 통지의무를 기초로 통지, 이유제시, 정기적 재검토 및 종료 절차를 강화할 필요가 있음을 제시하였다. 또한 국내법적 측면에서는 「대외무역법」 제19조의 다자주의적 설계와 최근 AI 수출통제의 소다자화 사이의 긴장을 분석하고, ‘이에 준하는 다자간 수출통제 공조’의 실질적 인정 기준과 실행

통제대상의 지정·재검토 절차를 구체화할 필요성을 제안하였다.

본 연구는 Table 5 사건을 통해 AI 모델에 대한 접근이 새로운 전략적 통제대상으로 취급될 가능성을 검토하고, 향후 AI 수출통제 규범을 설계할 때 모델 가중치, 소스코드, 컴퓨팅 자원, 호스팅형 API 접근 및 추론서비스를 구별할 필요가 있음을 제시하였다는 점에서 의의를 가진다. 아울러 국가안보와 디지털무역의 개방성·예측가능성 간 균형을 확보하기 위한 WTO 안보예외의 절차적 운용기준과 국내 수출통제법제의 개선방향을 제안하였다.

주제어: AI 수출통제, 안보예외, 프런티어 AI 모델, 접근권, 전략자산

[Abstract]

AI Export Controls on National Security Grounds:

International Economic Law Issues in the Fable 5 Incident and the Securitization of Access to Frontier AI Models

KANG MINJI

As frontier AI models have increasingly been regarded as strategically significant technologies with national security implications, new forms of export control have emerged, particularly in the United States, that may restrict access to AI models and computing resources. The Fable 5 incident illustrates how access to a hosted AI model, rather than the cross-border transfer of tangible goods or model weights, may itself become subject to export control. Although the relevant government directive was not publicly disclosed and the ensuing litigation ended without a decision on the merits, the incident raises novel questions concerning the treatment of remote access to AI models under U.S. export control law, the coverage of the General Agreement on Trade in Services (GATS), and the scope of the WTO security exceptions.

This study examines the legal framework governing U.S. AI export controls under the Export Control Reform Act of 2018 (ECRA) and the Export Administration Regulations (EAR). It distinguishes the transfer of model weights, source code, and controlled technology from remote access to hosted AI models through application programming interfaces (APIs), and considers whether the latter falls within the existing concepts of export and deemed export. From the perspective of WTO law, the study argues that restrictions imposed by a supplying country on the foreign provision of services by its own service supplier do not necessarily fall within the scope of the market-access and national-treatment obligations under Articles XVI and XVII of the GATS. Such measures may therefore reveal a regulatory gap in the existing GATS framework. Where an AI access restriction is designed in a manner inconsistent with GATS obligations, however, the regulating Member may seek to justify it under the security exception in Article XIV bis.

Drawing on WTO panel reports concerning Article XXI of the GATT 1994 and Article 73 of the TRIPS Agreement, this study examines the objective existence of an emergency in international relations, the articulation of essential security interests, the plausibility of the relationship between the measure and those interests, and the requirement of good faith. It argues that unlimited deference to a Member's self-judging security determination risks undermining substantive GATS obligations, whereas overly intrusive substantive review may weaken Members' acceptance of multilateral disciplines. The study therefore proposes strengthening procedural safeguards, including notification, reason-giving, periodic review, and termination procedures, with particular reference to the notification requirement in Article XIV bis:2 of the GATS. It also examines the relationship between Article 19 of Korea's Foreign Trade Act and emerging unilateral export control cooperation, and proposes clarifying the criteria and procedures for designating and reviewing new controls. In this respect, the Fable 5 incident highlights the need to distinguish among model weights, source code, computing resources, hosted API access, and inference services when designing export control rules, while maintaining an appropriate balance between national security and the openness and predictability of digital trade.

Keywords: AI export controls; national security exceptions; frontier AI models; access rights; securitization.