LOGISIGHT

WEEKLY INTELLIGENCE

WEEKLY REGIONAL ANALYSIS · AMERICAS

미주 권역 물류 시황 분석

보고기간 09/21~09/27

1. 미국내 자국 입항 선박 대상 사이버 공격 조사 강화

2. 중국-멕시코·북아프리카 직기항 시험 운항 확대

LOGISIGHT 인텔리전스팀

2026-W39

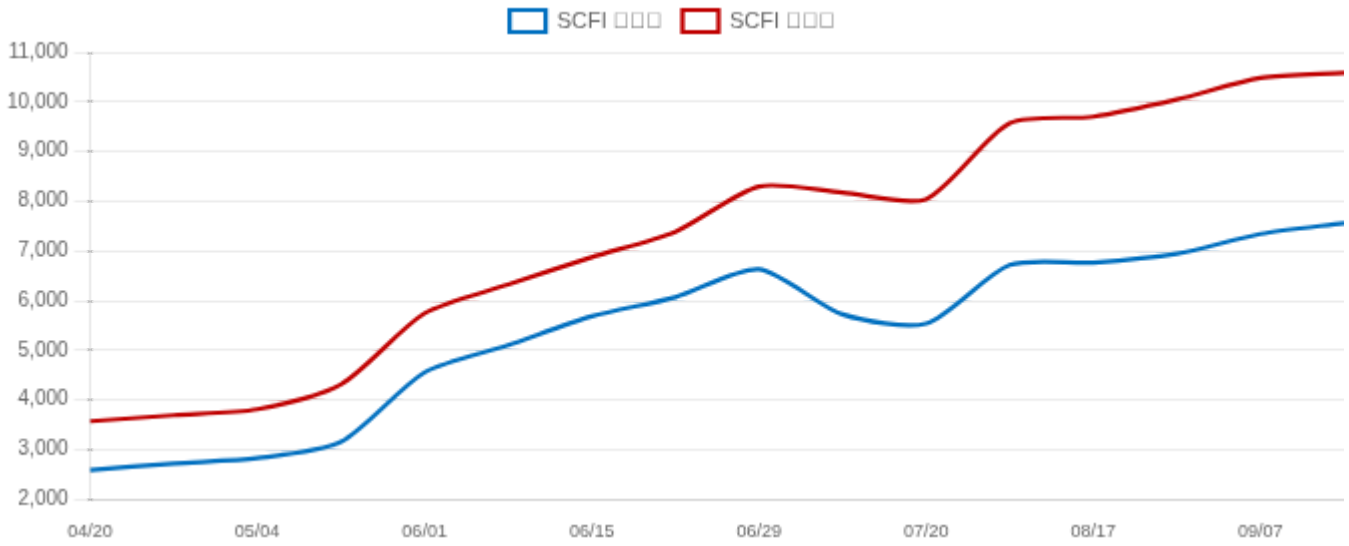
종합

이번 주 미주 권역은 미국의 해양 사이버 보안 강화와 중국의 물류 경로 다변화가 두드러짐. 미국 해안경비대와 연방수사국은 자국 입항 선박에 대한 승선 조사를 확대하며 해양 위협 대응이 물리적 검문에서 디지털 점검으로 진화하고 있음. 동시에 중국은 양쯔강 항만에서 멕시코와 북아프리카 직기항을 시험하며 전통적 환적망을 우회하는 노선을 모색함.

미국의 조사 강화는 글로벌 해운사에 사이버 보안 기준 준수를 압박하여 물류 운영 부담을 높일 전망됨. 중국의 직기항 시도는 공급망 측면에서 미주 노선의 유연성을 높이고 장기적으로 기존 해운 동맹과 환적 허브의 영향력을 재편할 수 있음. 두 흐름 모두 미주 지역 물류 안보와 효율성에 대한 전략적 변화를 반영함.

운임 지표

지수 · 항로	최신값	기준(월/일)	WoW	MoM
SCFI 미서안	7,560 $/FEU	09/14	+3.0%	+11.8%
SCFI 미동안	10,579 $/FEU	09/14	+1.0%	+9.1%
KCCI 미서안	7,942	09/21	+6.1%	+11.9%
KCCI 미동안	11,284	09/21	+2.4%	+9.4%



자료: freight_indices (Shanghai SCFI · KCCI) · 기준 09/14

미국내 자국 입항 선박 대상 사이버 공격 조사 강화

> **미국 해안경비대와 FBI가 자국 입항 외국 선박에 대해 사이버 공격 연루 의혹으로 승선 조사를 실시함. 이는 해양 사이버 보안 위협에 대한 미국 당국의 대응이 물리적 검문에서 디지털 점검으로 확대되고 있음을 시사함.**

미국 해안경비대와 FBI는 8월 21일과 24일 멕시코만에서 텍사스주로 향하던 외국적 유조선에 승선하여 선내 네트워크 무결성을 점검함. 조사 결과 운영 중단, 선체 불안정, 승무원 위험, 환경 영향 징후는 발견되지 않았음. 이는 미국 당국이 자국 해역 진입 선박에 대한 사이버 공격 혐의를 적극적으로 조사하고 있음을 보여줌.

이번 승선 조사의 배경에는 해운 부문을 겨냥한 사이버 공격의 위협 증대가 있음. 2017년 머스크를 마비시킨 노트페트야 공격과 2021년 휴스턴항 침입 사고 등 과거 사례는 해운 및 항만 시설의 사이버 취약성을 드러냄. 특히 현대 유조선은 항법, 추진, 조타, 화물 시스템이 IT 및 위성 연결과 동일한 선내 네트워크로 통합되어 있어 공격 표면이 넓음.

미국 당국의 이번 조치는 외국 선박의 사이버 보안 표준 준수 여부에 대한 우려를 반영함. 민주주의수호재단의 애니 픽슬러는 외국 선박이 최소한의 사이버 보안 표준을 준수하는지가 관건이라고 지적함. 해안경비대는 항만 운영자, 선주 등과 소통하며 항만 운영이 계속되도록 관리 중이며, 이는 글로벌 공급망 보안 차원에서 연방 당국의 대응 수위가 사이버 위협 점검으로 확장될 가능성을 시사함.

이러한 조치는 해운 및 항만 산업의 사이버 보안 요건 강화 추세와 맞물림. 미국은 해운 부문에 의무 보고와 갱신된 훈련을 포함한 보안 요건을 강화해 왔으며, 이번 승선 조사는 그러한 정책의 실행적 조치로 볼 수 있음. 향후 유사한 조사가 다른 항만과 선종으로 확대될 경우 해운 물류 전반의 사이버 보안 부담이 증가할 것임.

- 8월 21일과 24일 멕시코만에서 텍사스주로 향하던 외국적 유조선 2척에 대한 승선 조사가 실시됨.
- 조사 결과 운영 중단, 선체 불안정, 승무원 위험, 환경 영향 징후는 발견되지 않음.
- 2017년 노트페트야 공격으로 머스크가 마비되었고, 2021년 휴스턴항 침입 사고가 발생함.
- 현대 유조선은 항법, 추진, 조타, 화물 시스템이 동일한 선내 네트워크로 연결되어 사이버 공격에 취약함.
- 미국은 해운 부문에 의무 보고와 갱신된 훈련을 포함한 보안 요건을 강화해 왔음.

전망

미국 당국의 외국 선박에 대한 사이버 보안 조사는 향후 정례화되거나 확대될 가능성이 높음. 이에 따라 글로벌 해운사들은 미국 입항을 위한 사이버 보안 기준 준수에 더욱 주의를 기울여야 할 것임. 항만 및 해운 산업 전반의 사이버 보안 투자와 인식 제고가 요구됨.

시사점

화주 — 미국행 화물을 운송하는 해운사의 사이버 보안 수준이 낮을 경우 화물 지연이나 공급망 중단 위험이 있을 수 있으므로 운송업체 선정 시 사이버 보안 태세를 고려해야 함.

포워더 — 해운사 대상 사이버 공격 의심 시 미국 당국의 승선 조사로 인해 선박 일정이 지연될 수 있으므로 대체 경로와 일정 완충을 확보해야 함.

항만·선사 — 미국 입항 선박은 사이버 보안 기준 준수 여부를 점검받을 가능성이 높아졌으므로 선내 네트워크 분리, 접근 통제, 사고 대응 계획 등 사이버 보안 조치를 선제적으로 강화해야 함.

참고자료: Supply Chain Dive, 미국, 자국 입항 선박 사이버 공격 연루 의혹…외국 선박 승선 조사 (검색일: 2026-09-27)

중국-멕시코·북아프리카 직기항 시험 운항 확대

> **중국 양쯔강 연안 항만들이 멕시코·북아프리카행 직기항 컨테이너 서비스를 시험 운항하며 기존 환적 구조를 우회하는 장거리 노선을 개척함.**

양쯔강 항만들은 장인·난징발 멕시코 만사니요 및 북아프리카 직기항 서비스를 잇달아 개시함. 코스코쉬핑스페셜라이즈드캐리어스는 지난 23일 장인에서 멕시코 만사니요행 서비스를 시작해 기계류와 완제품을 실은 컨테이너 500개 이상을 선적했으며, 앞서 난징에서 북아프리카행 서비스를 출범시킴.

이러한 직기항 확대는 양쯔강 배후지 화물의 물류비 절감과 공급망 효율화 필요성에서 비롯됨. 기존에는 양쯔강 화물을 상하이나 닝보 등 주요 항만까지 바지선으로 운송해야 해 추가 하역비와 시간이 소요됐음. 장인발 멕시코 노선은 운송 기간이 22일로 기존 환적 경로보다 약 15일 단축되어 비용·시간 측면에서 이점이 큼.

미국·멕시코 대상 화물의 경우 파나마 운하 병목 현상에 대한 대안으로도 기능함. 만사니요 도착 화물은 철도나 트럭으로 미국 내륙까지 연계 운송될 예정이어서 공급망 다변화에 기여할 수 있음.

다만 현재 투입 선박이 다목적선 중심이어서 정기 서비스 안착까지는 선복량과 운항 일정의 안정성이 관건으로 지적됨.

- 장인발 멕시코 만사니요행 첫 항차: 500TEU 이상 선적, 운송 기간 22일(기존 대비 약 15일 단축)
- 난징발 북아프리카행 서비스: 2024~2025년 북극항로 시험 운항 후 정식화
- 코스코쉬핑스페셜라이즈드캐리어스, 지난 3월 장인발 앤트워프행 1070TEU급 일회성 운송 수행
- 파나마 운하 병목 대안으로 멕시코 경유 미국 내륙 연계 운송 의도

전망

양쯔강 항만의 직기항 시도는 환적 의존도를 낮추고 화주에게 더 빠른 대안을 제시할 수 있으나, 정기 서비스로 확대되기까지는 전용 선박 확보와 일정 안정화가 필요함. 성공할 경우 기존 허브 항만 중심의 물동량 구조에 일부 변화를 가져올 가능성이 있음.

시사점

화주 — 양쯔강 배후지 소재 수출 기업은 환적 제거로 운송 시간과 비용을 절감할 수 있으나, 정기성과 선복 부족 위험을 고려해야 함.

포워더 — 직기항 노선 등장으로 멕시코·북아프리카행 서비스 포트폴리오를 재편하고, 다목적선 기반 운임 경쟁력과 일정 리스크를 평가할 필요가 있음.

항만·선사 — 상하이·닝보 등 기존 환적 항만은 물동량 이탈 가능성을 점검하고, 코스코 등 선사는 다목적선의 컨테이너 정기 운용 가능성을 검증해야 함.

참고자료: The Loadstar, 양쯔강 항만, 멕시코·북아프리카 직기항…장거리 노선 시험 운항 (검색일: 2026-09-27)