BPA 부산항만공사 BUSAN PORT AUTHORITY

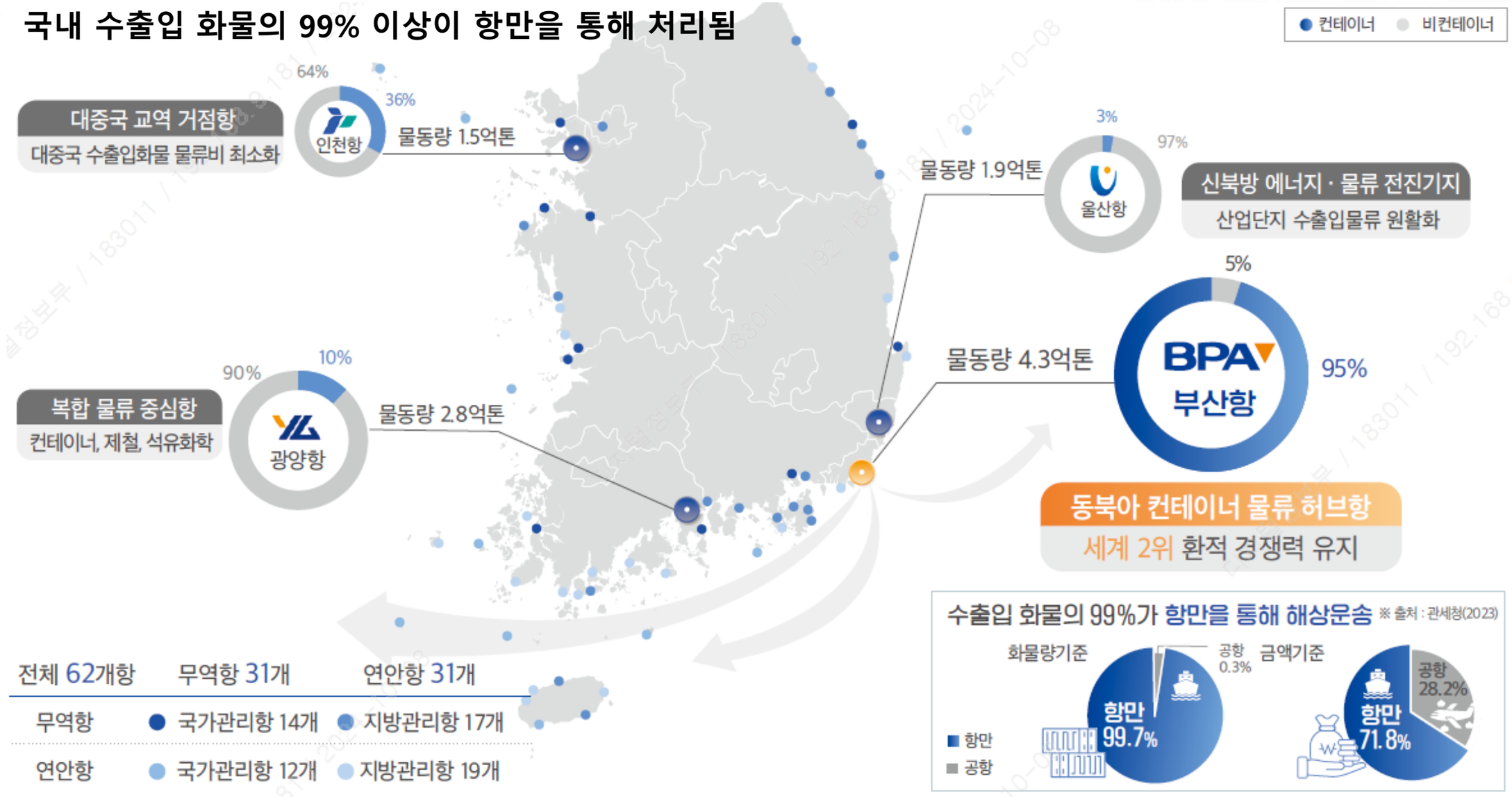
항만의 디지털전환에 따른 사이버위기 대응 방안

Busan Port Authority

목차

전국 항만 현황

✓ 국내 수출입 화물의 99% 이상이 항만을 통해 처리됨



부산항 개요

✓ 부산항은 연간 23백만TEU를 처리하는 세계 7위, 환적 12백만TEU을 처리하는 세계 2위 환적항만

환적* 항만
세계 2위

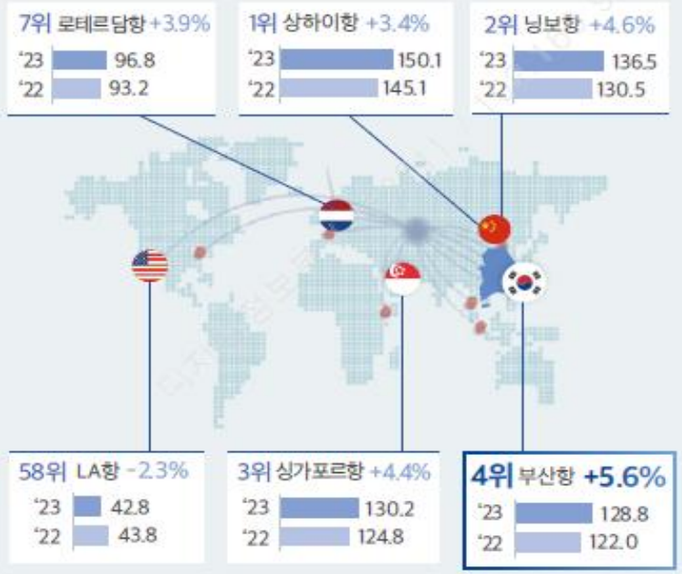
컨테이너 항만
세계 7위

2023년 세계 10대 항만 물동량 처리실적

* 환적화물 : 화물 운송 중 목적지가 아닌 제3국 항만에서 다른 선박으로 옮겨 싣는 화물

글로벌 항만 연결성 지수*

세계 4위

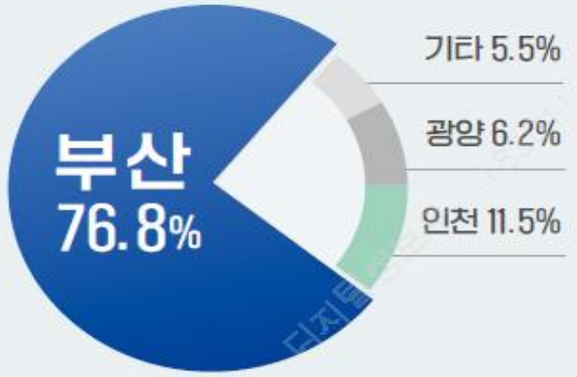


* 항만 연결성 지수 : 유엔무역개발회의(UNCTAD)에서 전 세계 900개 항만의 선박 입항 횟수, 항만 수용 능력, 정기노선 수, 정기 선사 수, 최대 수용 선박, 연결 항만 수를 근거로 항만 성과를 판별하는 지수로 항만의 전반적인 운영 수준을 판별하는 종합지표

화물처리량

전국 1위

2023년 국내항만 컨테이너 처리 비중



* '23년 전국항만 총 컨테이너 물동량 3,014만TEU
* '23년 전국항만 총 물량 15.5억톤
부산 4.3억톤, 광양 2.8억톤, 울산 1.9억톤, 인천 1.5억톤

컨테이너 항만의 역할

✓ **항만은 여러 이해관계자들의 물류 활동을 지원하는 수출입의 관문 역할**

- 여러 이해관계자를 통해 화물을 분배하고, 임시 저장공간을 제공하며, 최종 목적지로 운송

항만의 주요 특징

✓ **항만은 대규모 투자가 수반되는 설비 중심의 산업으로 시스템 의존도가 높음**

대규모 투자, 인프라	▪ 부두, 배후단지, 도로, 철도 등 다양한 인프라를 갖추고 있어야 하며, 그에 따른 대규모 투자가 수반됨
고도화된 장비	▪ 컨테이너 항만은 크레인, YT 등 이송장비 및 다양한 설비를 사용하며, 자동화 크레인, AGV 등 첨단 기술을 활용 작업 효율을 높이고 있음
정보 시스템	▪ 매일 수만개의 컨테이너를 처리하기 위해 첨단 정보시스템을 활용하여 운영계획을 세우고 화물의 이동과 상태를 실시간 추적, 관리
광범위한 네트워크	▪ 전세계 항만과 육상물류와 긴밀하게 연계되어 화물의 원활한 운송 뿐 아니라, 정보도 연계되어야 함
통관 및 보안	▪ 컨테이너 항만은 효율적인 통관 절차와 강력한 보안 시스템을 운영하여 화물의 안전한 이동과 함께 인적, 물적 보안을 관리함

스마트 항만 전환

✓ 항만의 스마트화, 디지털 전환 가속화에 따라 최신 IT 기술의 활용도 높아짐

스마트 항만 주요 키워드

Connectivity
이해관계자간 데이터 연계

Automation
원격 크레인, AGV 등 자동화

Green
LNG, 메탄올, 수소 에너지 벙커링

Security
지능형 CCTV, 보안 게이트

Safety
무인화, 예방 점검, 원격 작업

스마트 항만 개념도

출처 : 해양수산부

주요 IT 기술

데이터 플랫폼, 클라우드, 블록체인

IoT, 5G, AI, AGV, 디지털트윈

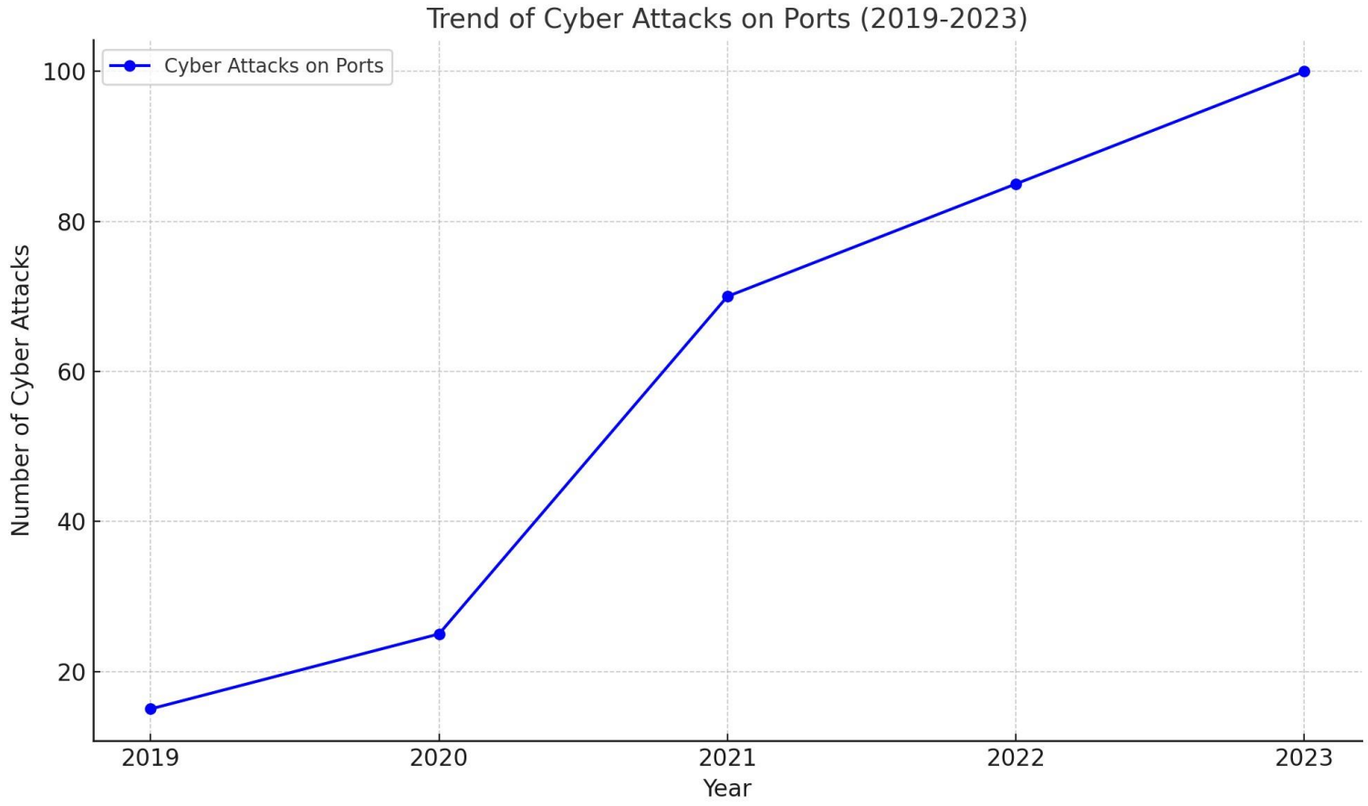
스마트그리드, EMS

CCTV, 드론, AI

IoT, CCTV, AI, 원격제어

항만 사이버 공격 현황

- ✓ 전세계적으로 디지털 전환 가속화, 국제정세 불안정 등에 따른 사이버공격 증가 추세
- ✓ 항만의 디지털화, 자동화 및 데이터 연계 증가로 사이버공격에 따른 리스크도 증가



ChatGPT 제공, 숫자는 참고

ChatGPT

공유하기

데이터는 특히 2021년부터 사건이 크게 증가한 것을 나타냅니다. 이러한 상승 추세는 항만이 디지털 기술을 채택하고 운영을 자동화함에 따라 증가하는 위험을 강조합니다.

여기 사용된 숫자는 가상의 수치지만, 최근 보고된 일반적인 패턴을 반영합니다.
그래프에 사용된 데이터는 일반적인 추세를 나타낸 것으로, 특정 항만을 대상으로 한 것은 아닙니다.

이러한 사례는 주로 랜섬웨어, 데이터 유출, 시스템 마비 등을 포함하며, 공격 대상은 IT 및 OT 시스템을 모두 포함하고 있습니다.

메시지 ChatGPT

항만 사이버 공격 사례

✓ **'23. 7월 일본 나고야 항만, 11월 호주 등 항만, 해운분야에 사이버 공격으로 인한 피해 발생**

[항만, 해운 관련 사이버공격 사례]

연도	분야 , 기업	공격 유형	피해 사례
'23.11월	**호주 시드니 항만 등**	랜섬웨어 공격	▪ **3일간 터미널 운영 중단**
'23. 7월	**일본 나고야 항만**	랜섬웨어 공격	▪ **3일간 5개 터미널 반출입 및 하역 중단**
2022년	**자카르타 JICT 터미널**	사이버 공격	▪ **TOS 시스템 서비스 중단**
2021년	**남아공 트랜스넷 SOC**	랜섬웨어 공격	▪ **항만 전터미널 운영 중단**
	HMM	랜섬웨어 공격	▪ 메일서버 가동 중단
2019년	**H선사 자동차운반선**	랜섬웨어 공격	▪ **선내 메인 컴퓨터 작동 중단**, 시스템 포맷
2018년	바르셀로나 항만	랜섬웨어 공격	▪ 시스템 폐쇄 및 포렌식 의뢰
	센디에고 항만	랜섬웨어 공격	▪ 시스템 폐쇄 및 포렌식 의뢰
2017년	**머스크**	랜섬웨어 공격	▪ **3주간 76개 터미널 운영 중단, 약 3억불 손실**
	독일 컨테이너선	항해시스템 해킹	▪ **해적이 10시간 동안 선박 통제권 탈취**

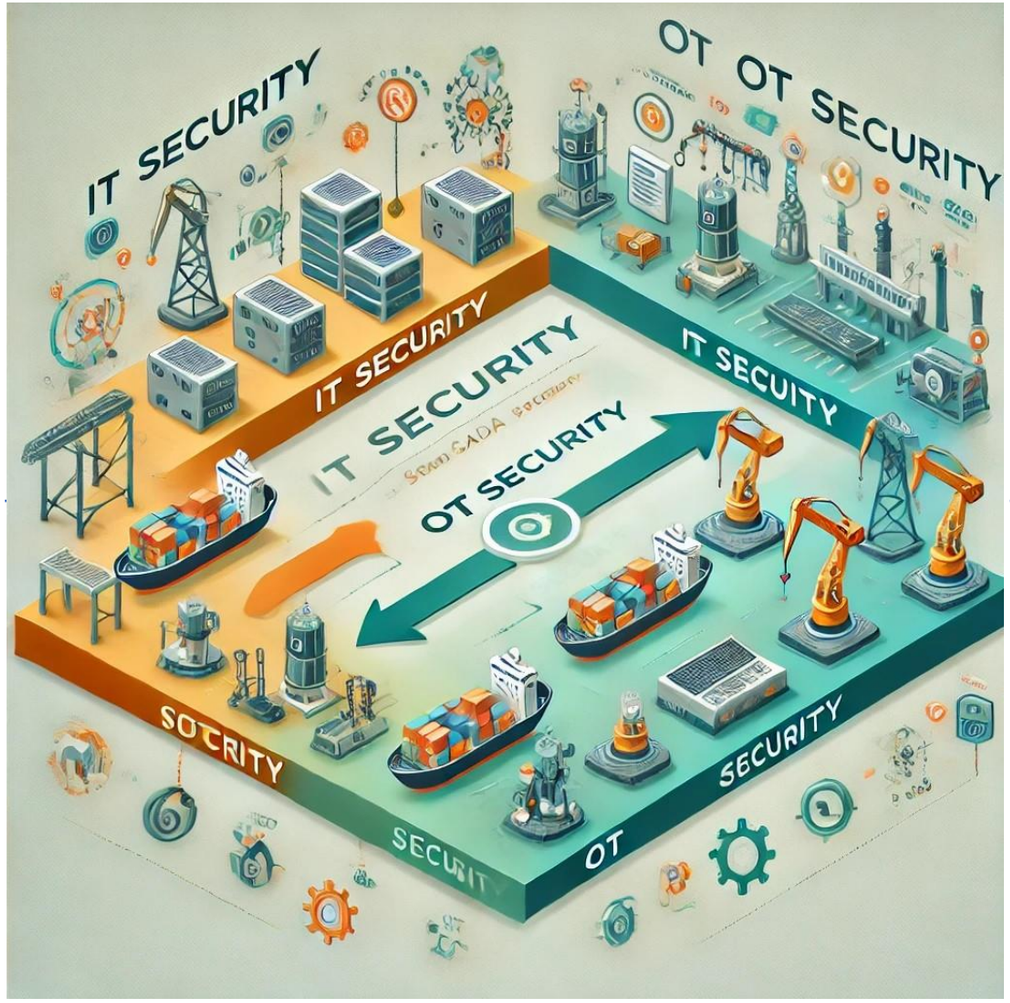
항만 사이버보안 대책

✓ 항만의 디지털 전환 및 스마트화에 따라 IT뿐 아니라 OT 레벨의 사이버 보안 대책 마련 필요

IT 보안

- 터미널 TOS 시스템
- EDI 중계망
- Port-MIS 등

- 네트워, 이중화
- 방화벽 정책
- 백업, DR, 보안관제
- 훈련, 보안 의식 등



OT 보안

- 원격조정 크레인
- AGV, 5G
- 각종 CCTV, IoT 장비

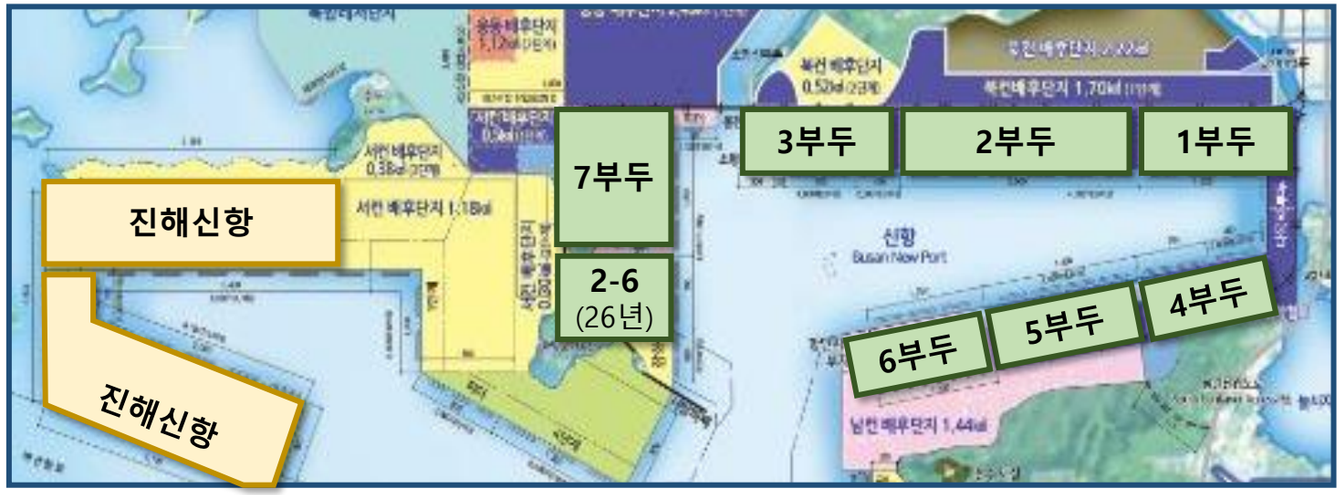
- 제어장비 신뢰성
- 보안 정책 업데이트
- 유지 보수 시 보안
- 이기종 장비 연계

터미널 운영 현황

✓ 부산항은 현재 북항 2개, 신항 7개 총 9개 터미널을 운영하고 있으며, 7부두 부터는 완전자동화 터미널 운영 중

북항

부산 신항



	자성대 ('78~)	신선대('91~) 감만('98~)	1부두 ('10~)	2부두 ('06~)	3부두 ('09~)	4부두 ('10~)	5부두 ('12~)	6부두 ('22~)	7부두 ('24~)
운영사	HBCT	BPT	PNIT	PNC	HJNC	HPNT	BNCT	BCT	DGT
TOS 시스템	자체개발	TSB	현대무벡스	CLT	TSB	현대무벡스	CLT	나비스	CLT
야드 크레인	수동	수동	자동	자동	자동	자동	자동	자동	자동
안벽 크레인	수동	수동	수동	수동	수동	수동	수동	자동	자동
야드 트레일러	수동	수동	수동	수동	수동	수동	수동	수동	자동

* 신선대 야드 일부 자동

완전 자동화 부두 오픈

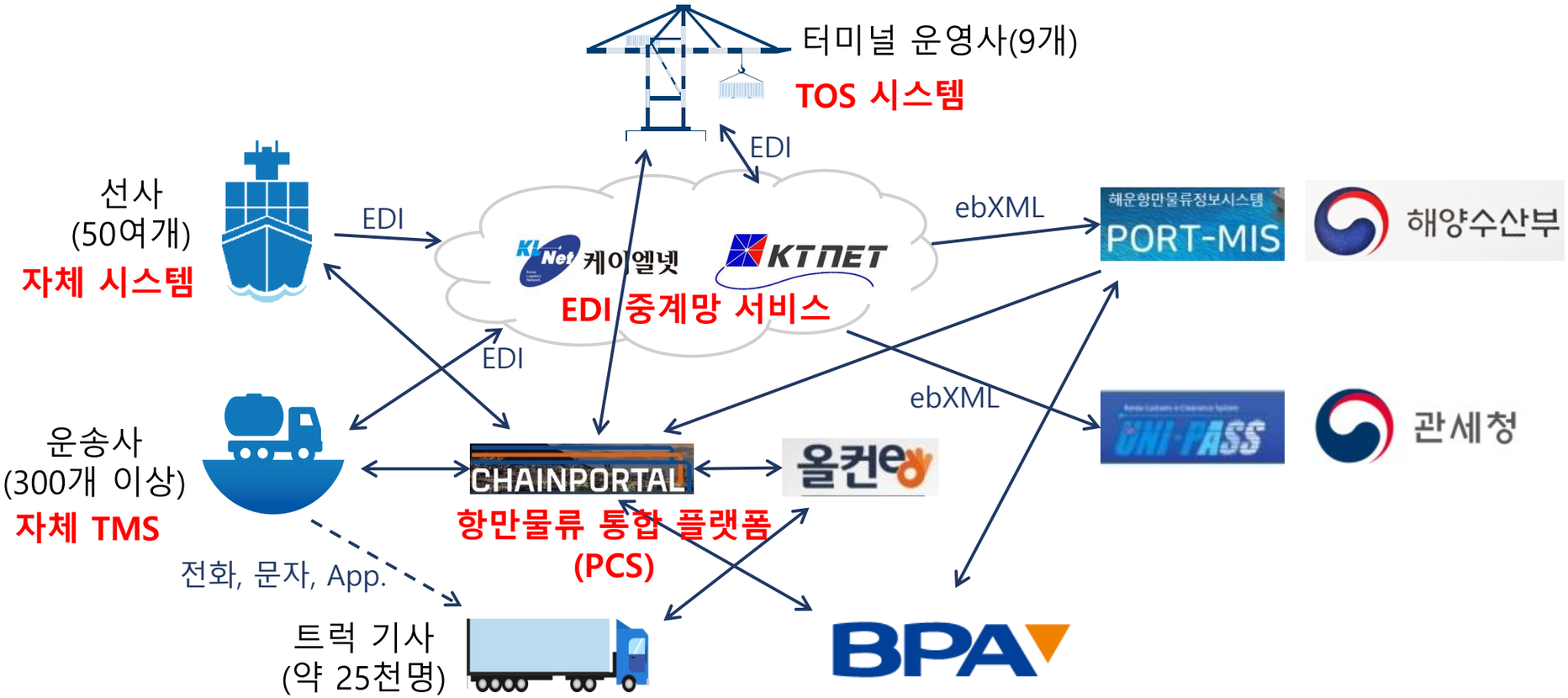
✓ **부산항은 '24년 4월, AI를 활용한 무인 크레인, AGV 등을 적용한 완전 자동화 부두를 국내 최초 오픈**

안벽	에이프런	컨테이너 야드(CY)	게이트
컨테이너 크레인 (무인 원격 운영)	**AGV** (무인 이송 장비)	**Transfer Crane** (무인 원격 운영)	**Load Tractor** (무정차 진출입)
			
양적하(Ship & 안벽)	안벽 & 야드 내 화물 이동	컨테이너 트럭과 야드간 화물 이동	화물차 진입

부산항 정보화 현황

✓ **부산항은 여러 이해관계자들이 복잡하고 다양한 방법으로 정보를 처리하며 운영 중**

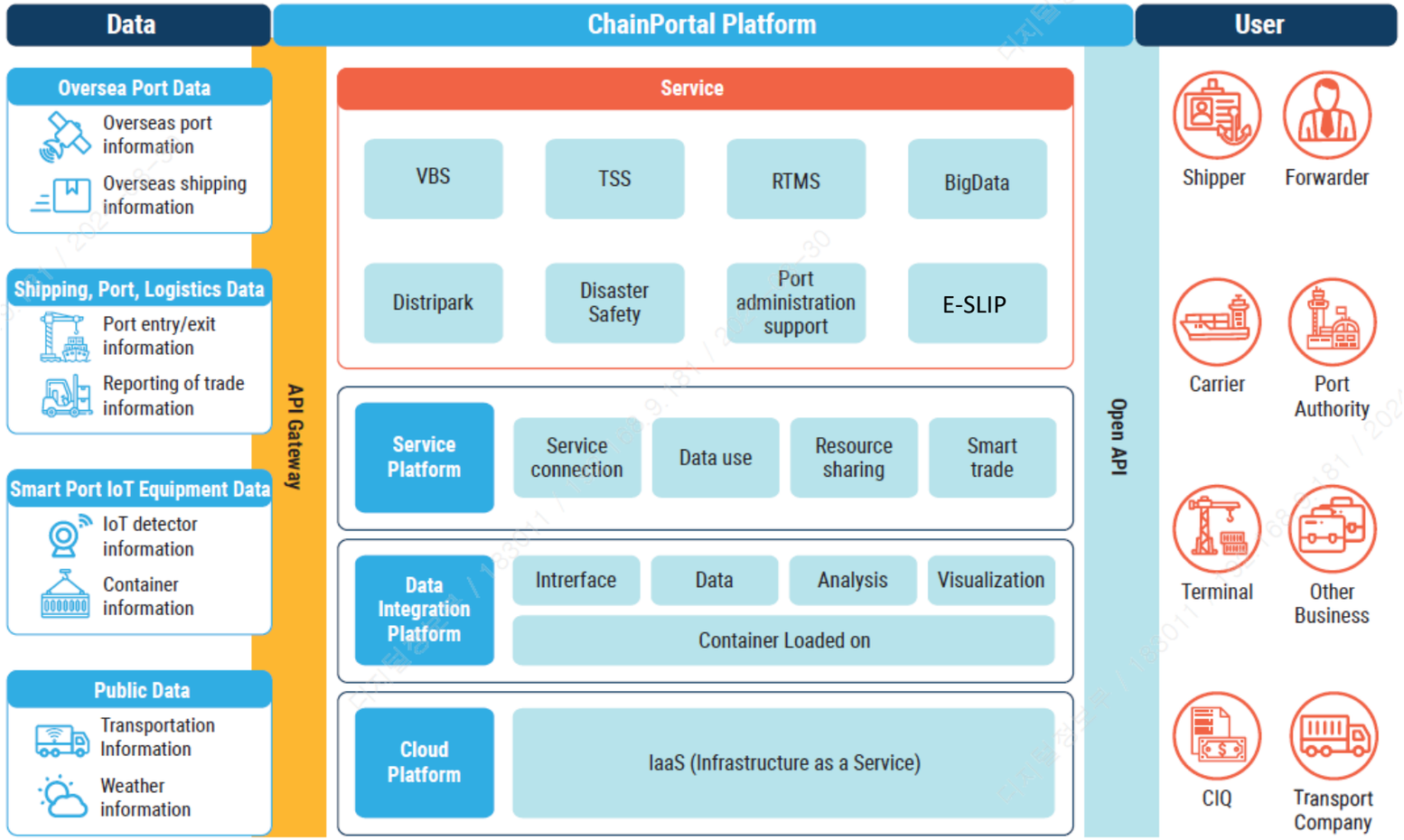
- 9개 터미널 운영사 등 다수의 이해관계자들이 다양한 시스템을 활용 중
- 선사, 터미널, 운송사, 해수부 등 주요 이해관계자들 간의 정보전달은 중계망을 통해 전달



부산항 항만물류 플랫폼 (체인포털)

✓ 부산항은 항만 이해관계자들의 데이터를 연계하여 항만 운영 효율을 높이기 위해 항만물류플랫폼을 개발 운영 중

체인포털 시스템 개념도



- **부산항 체인포털 시스템**
  - 현재 17,000여명 사용 중
  - 터미널운영사, 운송사, 트럭기사 등 실시간 운영 데이터 연계 완료
  - VBS, TSS, IIS, E-SLIP 등 서비스
- **향후 AI 적용을 통한 고도화 계획**
  - 선석 계획 등 계획수립 최적화
  - 물동량 예측 등 예측 정확도 개선
  - 운영현황 모니터링 및 이상 감지 등

항만 운영 주요 시스템

- ✓ 터미널 운영사, 중계망사업자 등 민간업체에서 운영하는 TOS, EDI 등이 항만운영에 주요 역할
- ✓ 항만자동화 추세에 따른 원격조정 크레인, AGV 등 자동화설비는 항만운영 및 안전과 직결

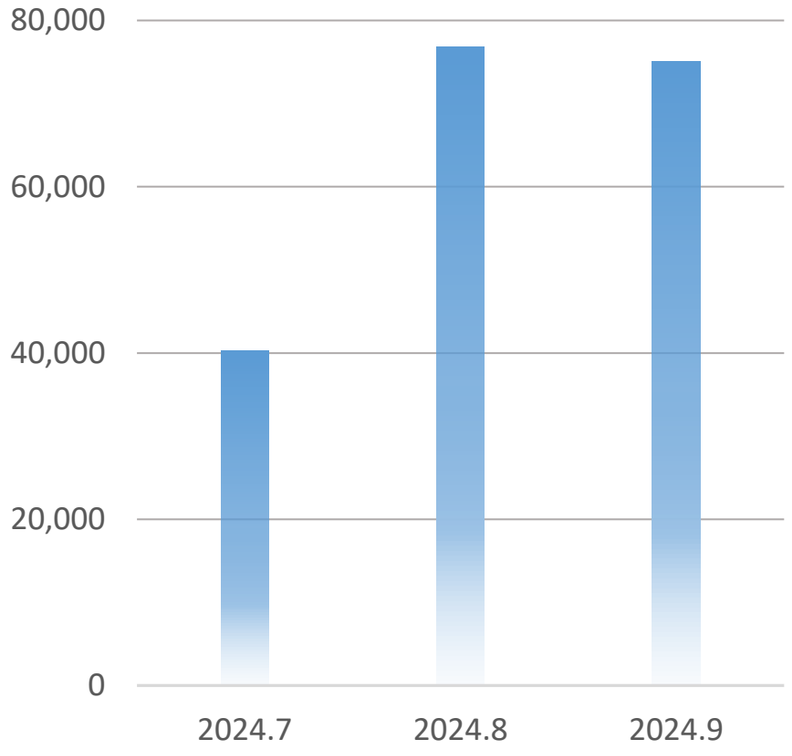
항만 운영 주요 시스템

구분	시스템	주요 기능	운영 주체	영향도
IT	Port-MIS	▪ 선박 입/출항, 화물 반출입 신고 등	해수부, 4개 PA	매우 높음
	EDI 중계망	▪ 화주, 선사, 포워더, 운송사, 터미널 간 Booking, 운송장, 선적서류 등 문서 교환	중계망사업자 (KL-Net, KT-Net)	매우 높음
	TOS	▪ 터미널 내 선석 및 야드 운영 계획 수립, 크레인 등 장비와 연계하여 터미널 운영	터미널운영사	매우 높음
	체인포털, 올컨e	▪ 전자인수도증, 환적운송, 터미널 정보 조회 서비스 등 항만물류 플랫폼	BPA	매우 높음
OT	원격조정 크레인	▪ 컨테이너 양적하, 반출입 등	터미널 운영사	매우 높음
	AGV	▪ 항만 작업자, 작업차량 등 출입 보안 관리	터미널 운영사	매우 높음
	보안 CCTV	▪ 항만 보안 모니터링	부산항보안공사	높음

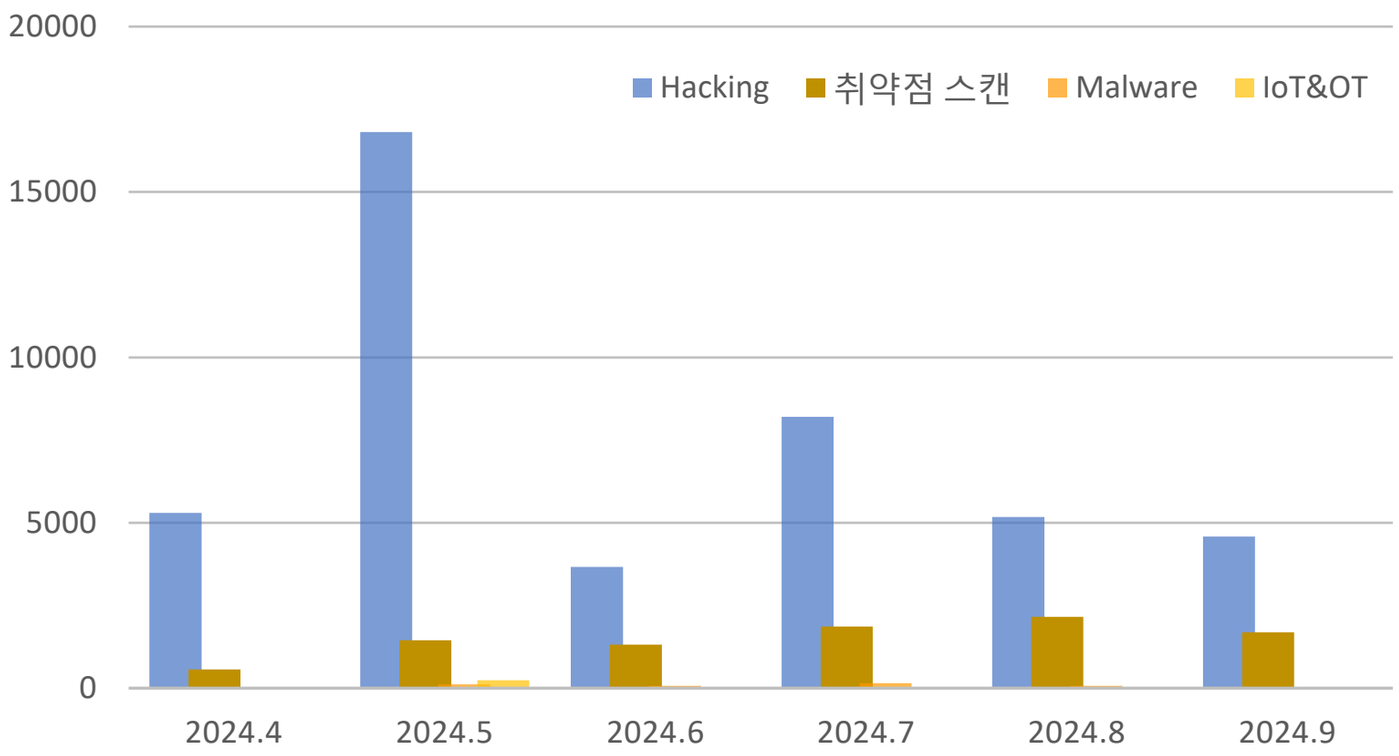
사이버 공격 현황

- ✓ 부산항을 대상으로 하는 위협 IP로부터의 접근 시도 다수
- ✓ 부산항 사이버 공격 시도 유형은 주로 해킹 및 취약점 스캔이 대다수를 차지

위협 IP 접근 시도

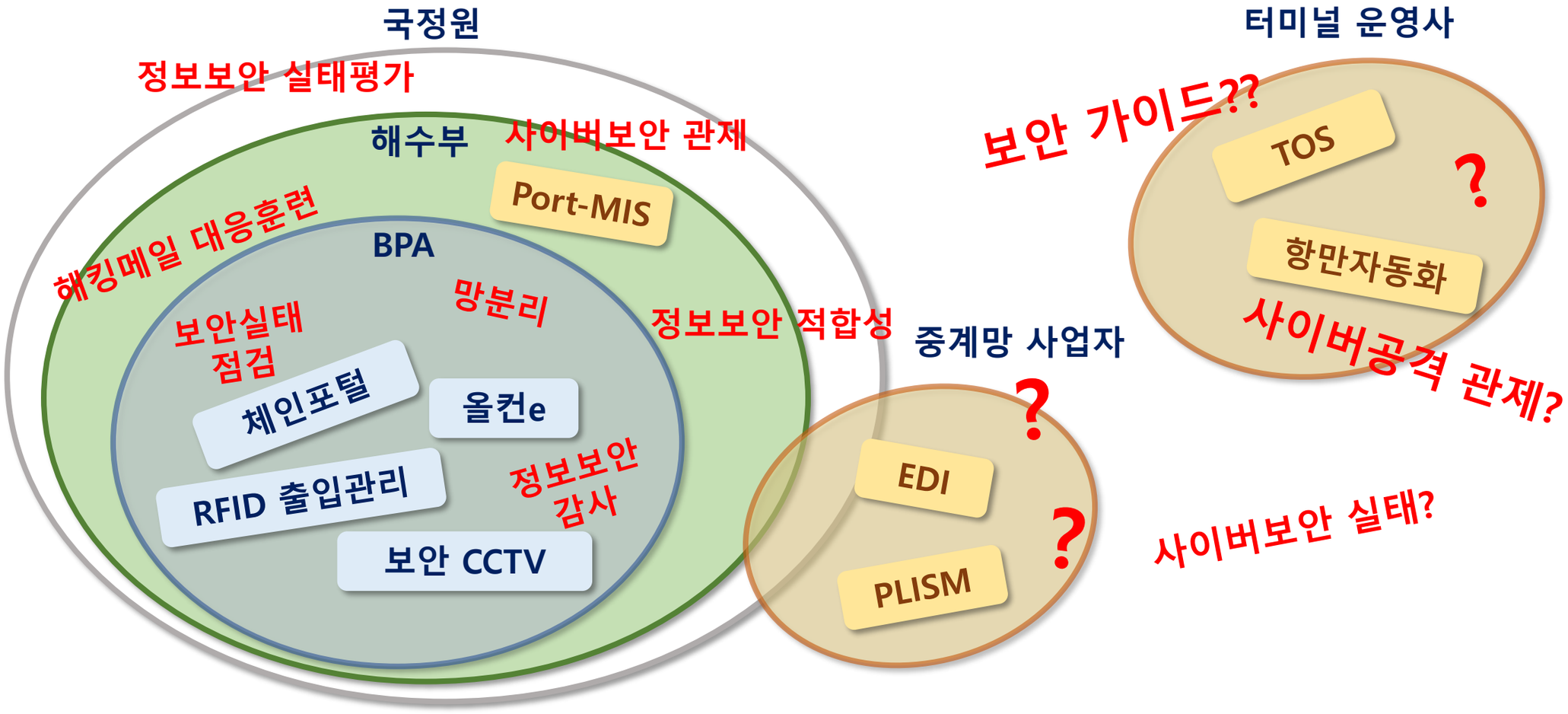


부산항 사이버 공격 유형(최근 6개월)



사이버보안 거버넌스 체계

- ✓ 해수부, BPA는 정부지침에 따라 정보보안 실태평가 등 사이버보안 현황 점검 가능
- ✓ 터미널운영사 및 중계망 사업자는 민간 사업자로서 사이버보안 현황 파악 어려움



부산항 사이버보안 협의체 운영

✓ **부산항 사이버보안 공동 대응을 위한 협의체 운영 중** ('19.12월 발족)

- 사이버보안 동향 공유, 참여사 정보보안 수준 점검, 해킹메일 대응 훈련 등 추진

	부산항 무중단 운영	사이버위협 공동대응	사이버보안 역량 강화
배경 및 목적	부산항 정보보안 강화를 통한 무중단 운영	사이버공격 효과적인 대응 및 확산 방지	부산항 전체 사이버보안 역량 상향 평준화
참여 기관	BPA 및 부산항 터미널 운영사 9개 업체		

추진 경과

일 정	추진 내용
'19.12월	▪ 부산항 정보보안 협의체 발족
'20.12월	▪ 터미널별 정보시스템 및 정보보안 현황조사 등
'21. 1~4월	▪ 터미널운영사 정보시스템 진단 (관리, 물리, 기술적 보안수준)
'22. 4월	▪ 사이버보안 관련 정보공유 및 전문기관 교육
'22.11~12월	▪ 공동 해킹메일 대응훈련 추진
'23년	▪ 항만 사이버보안 가이드라인 마련, 해킹메일 대응 훈련
'24년	▪ 항만 사이버공격 대응 훈련, 부산항 사이버공격 대응 체계 구축

터미널 사이버보안 관리 현황

✓ **부산항 9개 터미널운영사에 대한 사이버보안 점검 결과, 운영사별 수준 편차가 크고, 조직, 인력, 예산 확보를 위한 관리적 보안 강화 및 보안 취약점에 대한 개선이 필요**

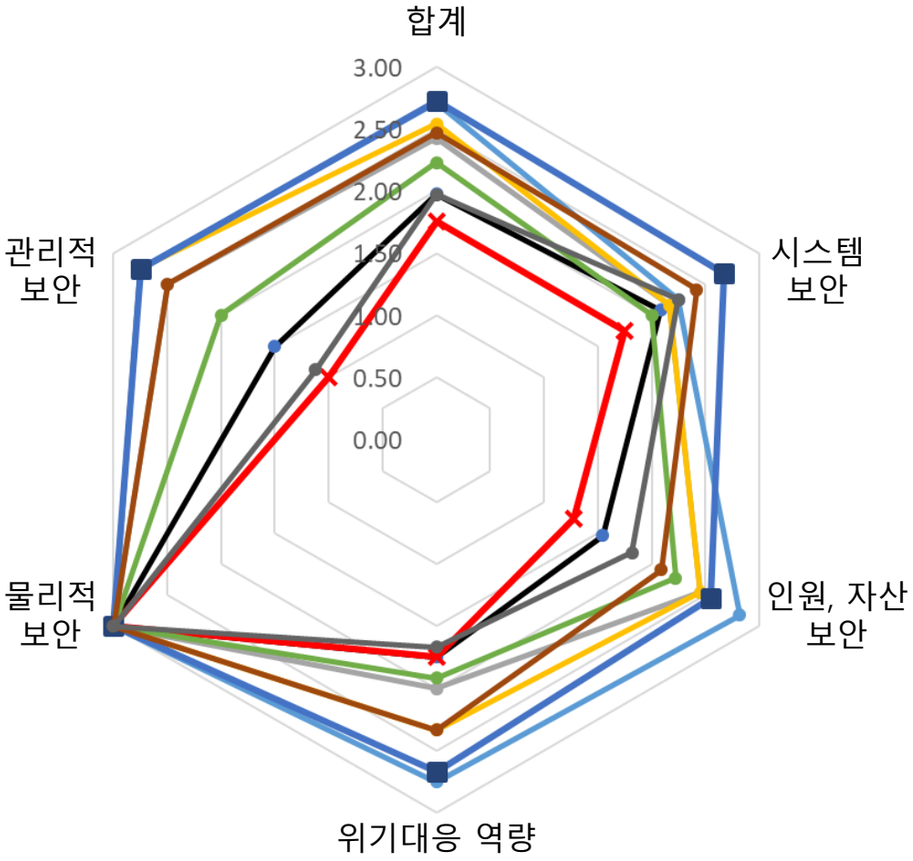
부산항 사이버보안 점검

점검 개요

- **일정 :** '21. 1 ~ 4월
- **대상 :** 9개 터미널운영사 정보보안 관리현황
- **기준 :** 주요정보통신기반시설 취약점 진단 기준
- **내용 :** 관리·물리분야 진단, 웹사이트 취약점 등

주요 지적 사항

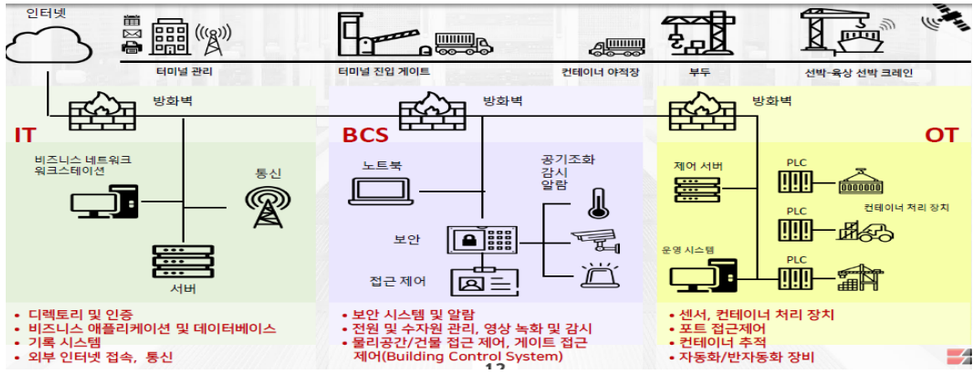
- ✓ 보안관리 지침 미비 또는 개정 미흡
- ✓ 정보보안 전담조직, 인력, 예산 미확보
- ✓ 백신 서버 미적용 및 정기 수동 업데이트
- ✓ USB 등 매체제어 미실시
- ✓ 상용메일 및 메신저 업무 활용
- ✓ 정보시스템 및 웹 정기 보안진단 미실시
- ✓ Flash, ActiveX 등 웹컨텐츠 개선 필요



항만 사이버보안 강화를 위한 노력

- ✓ **해수부, BPA 공동 '항만 하역장비 사이버보안 강화방안 연구용역' 진행** ('23.10월 ~ '24.5월)
- ✓ **중계망 사업자(KL-Net) 주요정보통신 기반시설 지정** ('23년, 해수부)
- ✓ **민·관·공 연계한 항만 사이버공격 대응 훈련 실시** ('24. 8월, 민간 터미널, BPA, 해수부, 사이버119 등 참여)

항만 하역장비 사이버보안 강화방안 연구



- 국·내외 항만 및 관련분야 사이버보안 기준 및 터미널 사이버보안 실태조사
- **항만 사이버보안 가이드라인 개발 완료(IT & OT)**

부산항 사이버공격 대응 훈련

향후 검토 사항

✓ **항만 사이버보안 가이드라인 적용을 위한 정책적 근거 마련, 사이버보안 관제 방안 등 검토 필요**

	사이버보안 강화를 위한 제언	검토 사항
거버넌스	▪ 항만 사이버보안 **기준/규정/제도 마련** - 항만 사이버보안 정기 **점검 및 관리 주체** ▪ 항만 사이버위기 대응 체계 수립 및 매뉴얼 작성	▪ 민간 터미널운영사 대상 사이버보안 관리 정책 ▪ 터미널운영사 협조
사이버 보안 관제	▪ 항만 **사이버공격 실시간 모니터링 및 관제** - 참여사 보안 관제센터 인프라 **공동 구축 및 운영** ▪ 사이버보안 **위협 공지 및 사고 사례 공유** 등	▪ 참여업체 협업 방안 (운영 주체 등) ▪ 국정원, 해수부, PA 지원
스마트항만 대비	▪ 완전 **자동화 항만 대비** 사이버보안 관리체계 ▪ **자율운항 선박, LNG 추진선, 전기 추진선** 대응 ▪ **IoT, 드론, 클라우드, 5G 활용** 시 사이버보안 기준	▪ 자동화 장비 보안기준 ▪ 4차산업혁명 기술 대응 정보보안 방안 R&D