TBT AI사이버보안

수출(디지털무역) 기업 대상

생성형 AI 및 AI 사이버보안 이슈와 대응 가이드

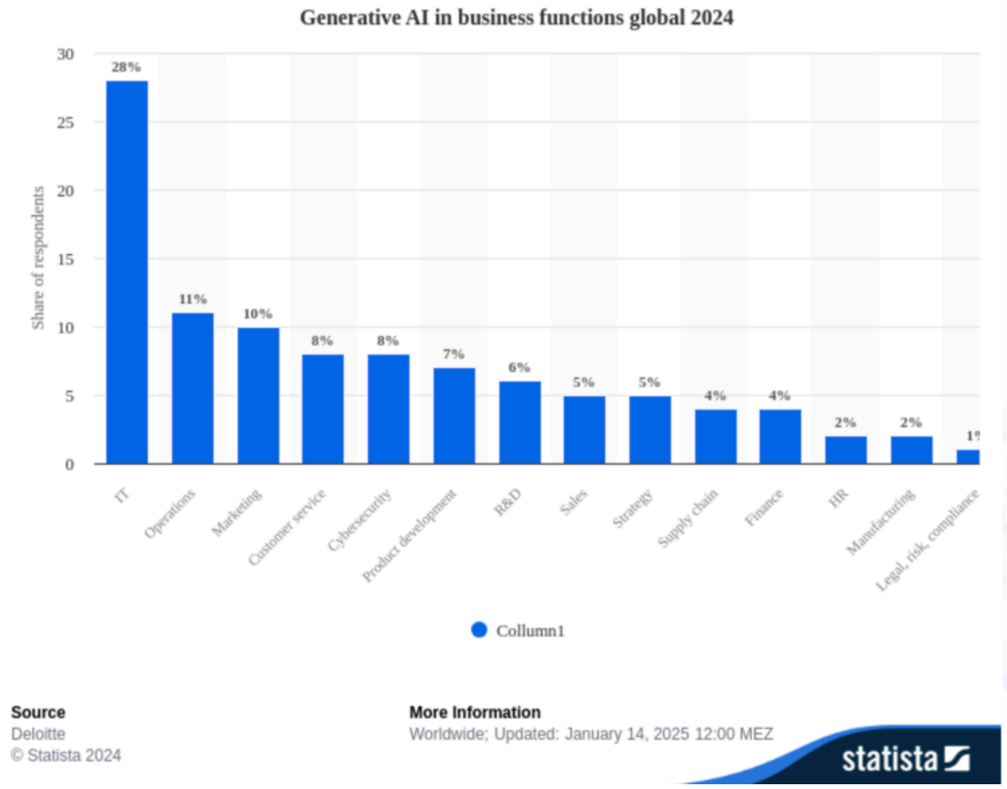
- 발표자 양 송이 전문위원 -

01.

글로벌 AI 사이버보안 시장 및 기술 활용 현황

전세계 산업별 생성형 AI 도입률

2024년 기준 전 세계 기업의 부문별 생성형 AI 도입률은 다음과 같음.
IT·운영·마케팅·고객응대 등 실제 무역업무 핵심 단계에 AI가 깊게 통합되고 있음.

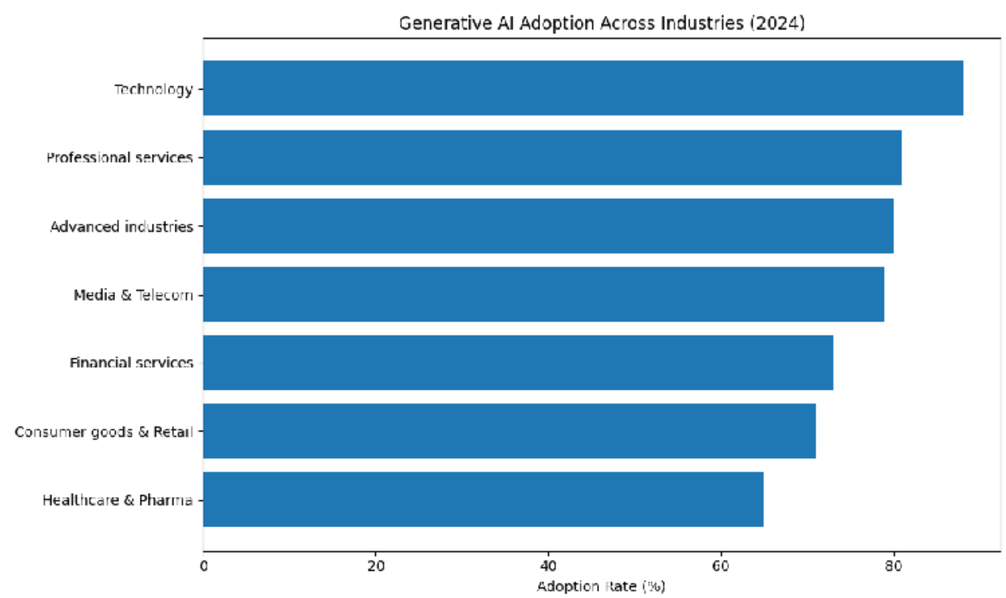


업무 기능 (무역 프로세스 대응)	생성형 AI 도입률 (%)	주요 적용 형태	연계 위험 데이터
IT (시스템·통관·보안)	**28%**	코드 생성, 시스템 모니터링 자동화	서버로그, 인증정보
Operations (운영·물류)	**11%**	운송계획, 재고 예측, 자동문서 작성	운송계약·고객주소
Marketing (시장조사·바이어 탐색)	**10%**	시장분석·상품설명 자동화	경쟁사 정보, 거래조건
Sales/Customer Service (수출 상담·CS)	**9%** (평균)	다국어 상담, 견적문 생성	고객명, 거래내역
Finance (수출입 결제·보고)	**~8%**	리스크 분석, 결산보고 자동화	금융정보, 매출데이터

출처: Statista (2025.11 업데이트) / 기반: McKinsey Global Survey 2024
"Generative AI adoption across industries by function 2024"

전세계 산업별 생성형 AI 도입률

2024년 기준, 기술·전문서비스·제조·무역 분야 기업의 80% 이상이 이미 생성형 AI를 실제 업무에 활용하고 있습니다.



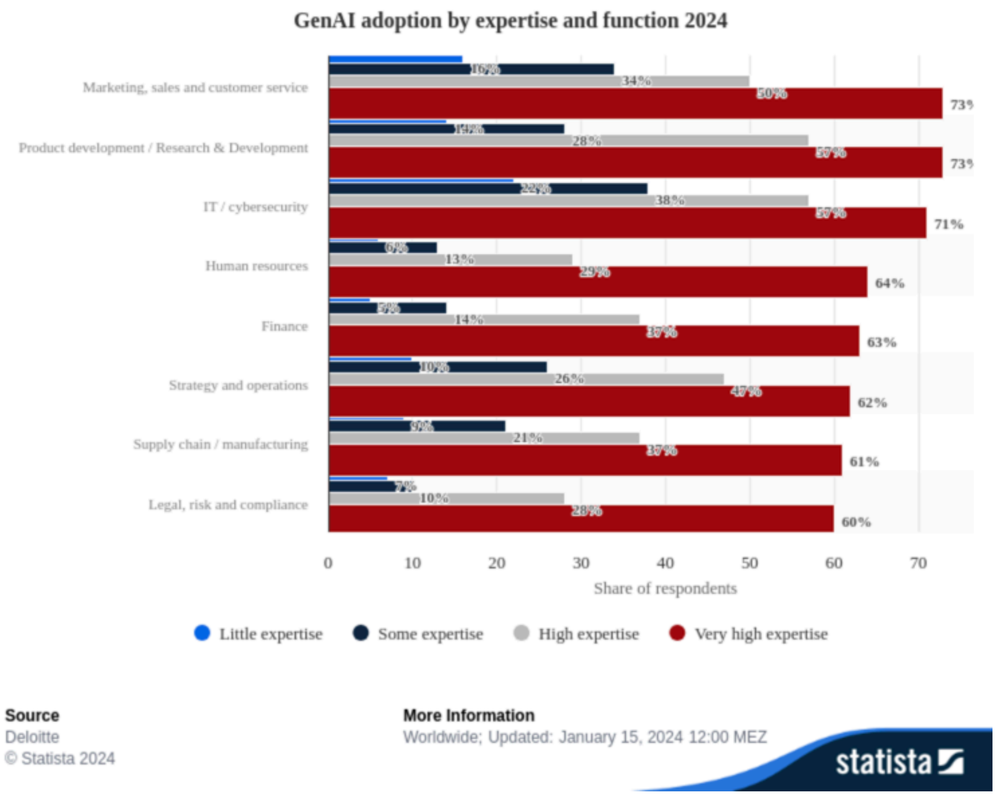
출처:: McKinsey Global Survey 2024
"Generative AI adoption across industries by function 2024"

산업 구분	2024년 생성형 AI 도입 기업 비율 (at least one function)
Technology (기술산업)	88%
Professional services (전문 서비스)	81%
Advanced industries (제조·공정·무역 관련)	**80%**
Media & telecom (미디어·통신)	79%
Financial services (금융)	73%
Consumer goods & retail (소비재·유통)	71%
Healthcare, pharma & medical products (의료·제약)	65%

전문성이 높은 직무일수록 AI를 실무에 적극 도입

AI 입력데이터의 약 40%가 개인정보나 금융데이터(PII)

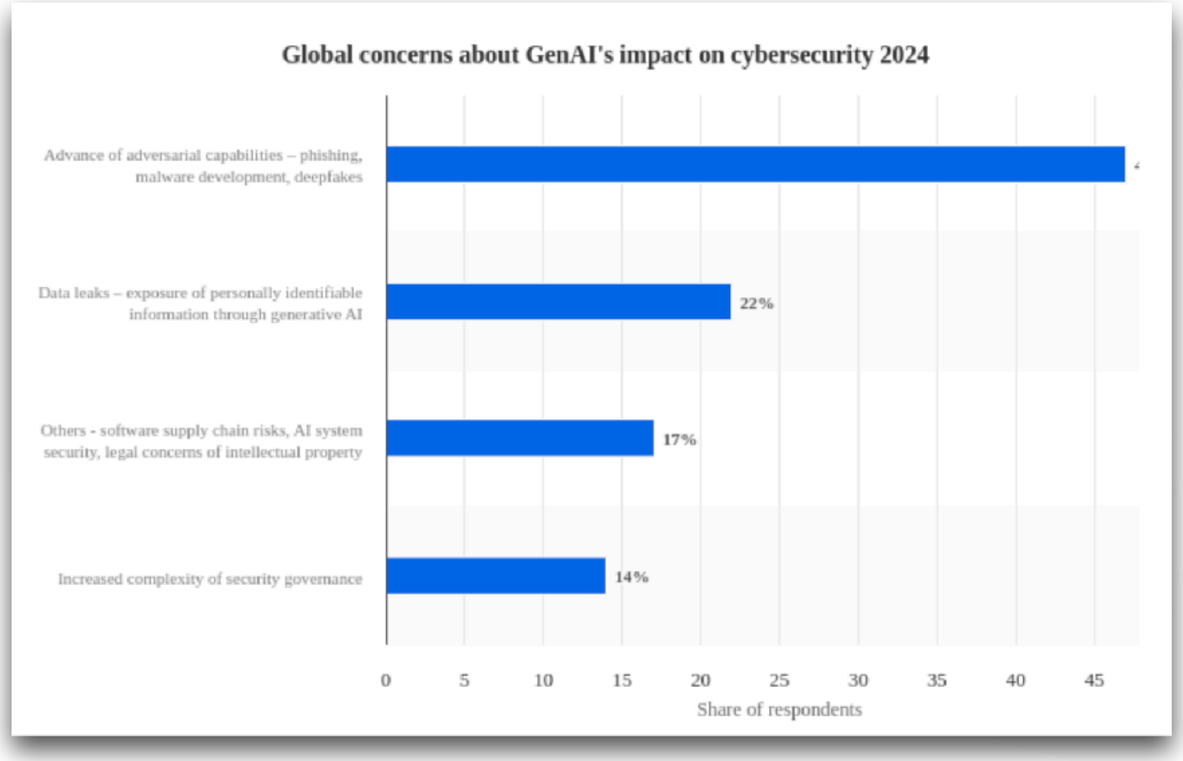
→ 데이터보호·보안 프레임워크 부재 시 기업 리스크 급증.



무역 단계	대응되는 기업 기능	2024년 AI 도입률	대표 AI 활용 사례	데이터 노출 위험
시장조사/ 바이어 탐색	Marketing & Sales	9~10%	경쟁사 분석, 수출국 규제요약, 제안서 자동작성	경쟁사·바이어 정보
계약 및 문서작성	Operations / Legal Ops	11%	L/C 서류, 견적서 자동작성	거래조건·금융정보
통관·운송관리	Operations / IT	11~28%	물류 문서 자동화, 실시간 추적	운송코드·고객주소
고객응대/CS	Customer Service	9%	다국어 상담·클레임 처리	고객·거래데이터
정산·리스크보고	Finance	8%	리스크 분석, 자동보고	손익·계좌정보

생성형 AI 활용 급증과 데이터 유출 위험

기업이 ChatGPT, Copilot, Claude 등 생성형 AI를 무역업무에 접목하면서 실제 입력되는 내부 데이터(문서, 고객정보, 거래내역)가 노출 위험에 직면하고 있음.



통계: Global concerns about GenAI's impact on cybersecurity 2024

출처: Statista (2025.11 업데이트)

내용:

2024년 전 세계 기업 및 사이버 보안 리더 조사 결과,

- 48%가 “AI 기반 피싱·악성코드·딥페이크 등 적대적 공격기술 증가”를 가장 큰 위협으로 꼽음.
- 22%는 “생성형 AI로 인한 개인식별정보(PII) 유출 및 데이터 노출”을 주요 우려로 인식.
- 기타 위험요소로는 공급망 보안(software supply chain risk), 모델 자체의 보안 취약성 등이 포함됨.

무역 프로세스별 생성형 AI 활용 구간

거래처·가격·기술정보 등 고위험 데이터를 다루는 구간,
따라서 무역기업의 AI 활용은 단순한 자동화가 아니라, **데이터보호와 사이버보안 리스크 관리의 핵심 이슈**

Generative AI adoption across industries by function 2024

Share of respondents	Technology	Professional services	Advanced industries	Media and telecom	Consumer goods and retail	Financial services	Heal phar and medi prod
Marketing and sales	55	49	48	45	46	40	20
Product and/or service development	39	41	39	26	21	25	22
IT	31	16	26	22	20	24	30
Service operations	30	23	24	37	13	26	14
Knowledge management	26	34	17	26	12	16	24

Source
McKinsey
© Statista 2024

More Information
Worldwide; Updated: March 11, 2025 12:00 MEZ

statista

산업	생성형 AI 도입률 (%)	주요 활용
기술산업	88	제품개발, 보안, IT운영
전문서비스·무역	**80**	**리서치, 계약서 자동화**
미디어·통신	79	콘텐츠·고객응대 자동화
에너지·산업	75	운영·공정 최적화

출처: Statista (2025.11 업데이트) / 기반: McKinsey Global Survey 2024
“Generative AI adoption across industries by function 2024”

02.

디지털 무역 관련 사이버보안 및 데이터 유출 현황

공급망 사이버공격 확산과 무역 데이터 유출 위험

거래 데이터 유출이 부르는 공급망 보안 인증 요구 강화
→ 거래처 문서 전송·AI 번역·전자서명 단계에서 기밀 유출.

연도	피해 고객 수	비고
2019	263,971,759명	사상 최대치 (SolarWinds, NotPetya 등)
2020	36,875,881명	팬데믹 초기 공급망 공격 급감
2021	180,691,481명	Colonial Pipeline, Kaseya 공격 영향
2022	11,136,629명	글로벌 보안 시스템 강화
2023	137,573명	포털형 피싱 중심
2024	**183 million (1억8,300만 명)**	ESG 보고서·협력사 데이터 유출 다수 (Compareitech 분석)

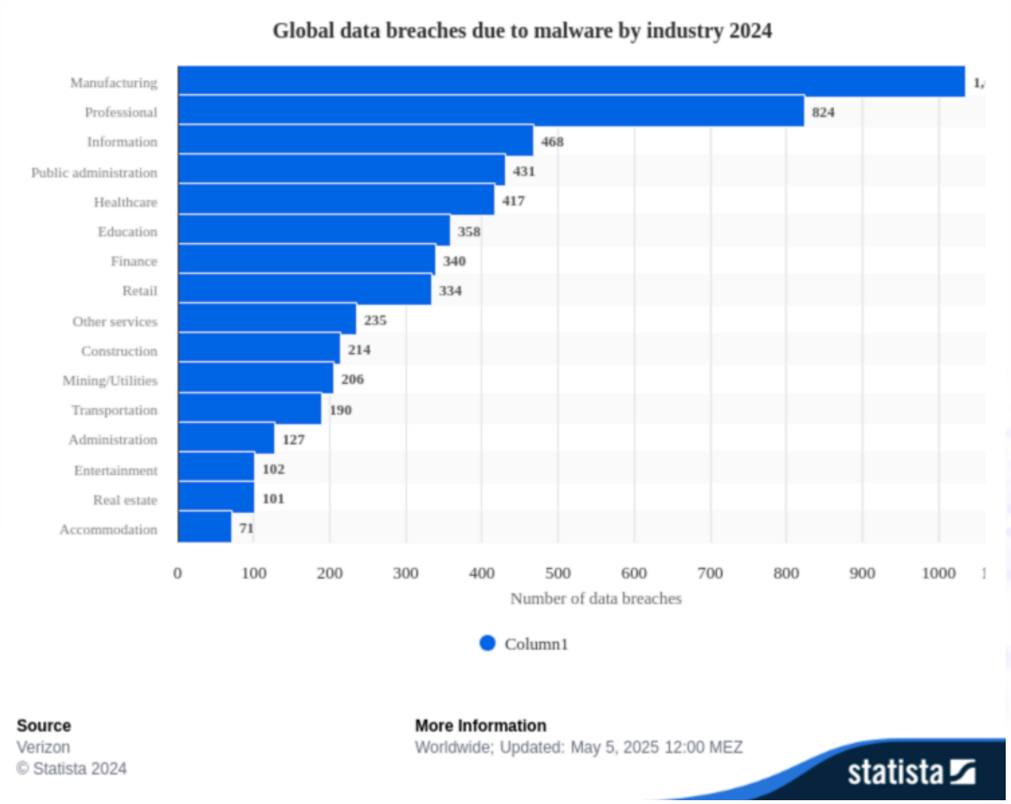
- 2024년 공급망 사이버공격으로 피해 입은 고객 18.3만 명
- 위조 계약서(counterfeit), 악성코드 삽입, 파트너 포털 침입이 주요 공격유형.
- 공격 피해의 70%가 **협력사에서 발생**, 직접 피해보다 공급망 연쇄피해가 큼.
- 거래처 문서 전송·AI 번역·전자서명 단계에서 기밀 유출 빈번.
- 납품기업 중 30% 이상이 이후 **보안 인증 도입을 거래조건으로 요구받음**.

시사점: 무역의 디지털화가 진행될수록 공급망 보안이 **새로운 무역기술 표준**이 되고 있음.

Source: Statista, *Customers affected by supply chain cyberattacks worldwide from 2019 to 2024* (based on data by Comparitech, 2024), updated May 23, 2025.

무역업 관련 데이터 유출 현황

제조·무역 부문은 실제 수출입 문서, 견적서, 공급망 데이터가 다수 포함되어 있어 **내부문서 유출이 전체 유출의 64%** 차지.

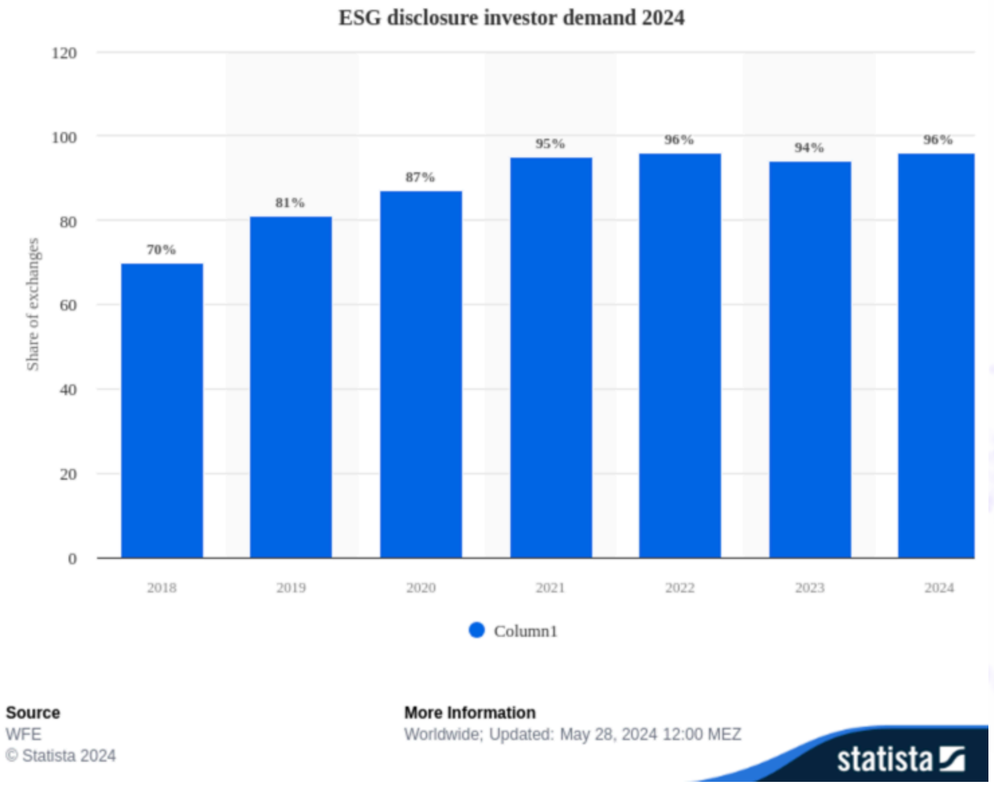


산업군	유출 사건수 (2023.11~2024.10)	주요 원인
제조(무역 연계)	**1,036건**	악성코드·시스템침입
전문서비스	**824건**	내부정보 전송 오류 이메일 전파
정보통신	**468건**	외부 침해 및 클라우드 설정 오류

데이터 기간: 2023년 11월 ~ 2024년 10월
원자료 제공기관: Verizon Data Breach Investigations Report (DBIR) 2024

ESG 보고서 및 데이터 공개 압박

2018년 70% → 2024년 96%의 거래소가 투자자들의 ESG 정보공개 요구를 경험.
특히 수출기업에 대해 **구매기업(바이어)** 이 ESG 데이터 제출을 필수조건으로 요구하는 사례 급증.
일부 글로벌 대기업은 "**보안인증·ESG 데이터 관리 솔루션**" 구매를 납품조건화.



연도	ESG 정보공개 요구 경험 비율 (%)	증감	비고
2018	70%	-	초기 ESG 공개 요구 확산기
2019	81%	▲+11	투자자 요구 본격화
2020	87%	▲+6	EU 그린딜·SASB 확대 영향
2021	95%	▲+8	공급망 보고 요구 시작
2022	96%	▲+1	ESG 보고 표준화 가속
2023	94%	▼-2	시장 조정기
2024	**96%**	▲+2	**사실상 전 세계 거래소 표준화 단계**

무역기술장벽으로 작용하는 조짐

데이터보호·AI보안이 새로운 비관세장벽으로 작동

데이터 유출은 단순한 보안 리스크가 아니라 '무역 접근 조건'으로 전환 중

구분	규제/표준 동향	무역 영향
EU AI Act (2025)	AI 시스템의 데이터 투명성·보안성 검증 의무화	**수출용 AI솔루션은 "보안검증 인증"을 획득해야 통관 가능**
미국 NIST AI RMF (2024)	신뢰성·보안성 기준 제정, 연방 조달 시 필수	**미국 정부·공공 조달시장 접근 장벽**
중국 생성형 AI 관리조례 (2024)	데이터 로컬화·모델 등록 의무화	**해외 SaaS형 AI 서비스 진입 제한**
일본 TISAX·ISO27001 확산 (2025)	완성차 OEM이 협력사에 정보보안 인증 요구	**부품 수출 시 '보안인증'이 필수 계약조건화**

"무역 데이터 유출은 단순한 사이버 사고가 아니라,
AI 보안성과 ESG 데이터 투명성 검증을
무역의 전제조건으로 만드는 새로운 형태의 TBT입니다.

수출기업은 앞으로 '**AI 보안 인증**'과 '**데이터보호 보고서**'를
품질인증서와 동일한 수준으로 관리해야
시장 접근이 가능합니다."

유럽연합 (EU)

주요 규제

법령	시행/발효	핵심 내용
GDPR (General Data Protection Regulation)	2018년 시행	개인정보 처리·이전 시 **명시적 동의, 데이터 주체권리, 역외 적용** 의무. AI 학습데이터에 개인식별정보 포함 시 처벌 가능.
AI Act (Artificial Intelligence Act)	2025년 발효 예정	AI 시스템을 **위험등급(High/Medium/Low)** 으로 분류하여 **데이터 품질, 보안성, 로그관리, 인간감독** 의무 부여. 수출 AI 모델도 인증 필수.
NIS2 Directive (Network & Information Security 2)	2024~25년 전환	공급망·산업제조·물류 부문에 **보안조직 지정, 침해사고 보고의무(24h), 제로트러스트 체계** 도입 요구.

■ **한국 기업의 애로사항**

- **AI 학습데이터에 개인·거래정보 포함** 시 GDPR 위반 소지.
- AI 모델 수출 시 **"High-risk AI" 분류 가능성**
  → 인증 절차(Conformity Assessment) 필요.
- 공급망 납품 시 **NIS2 보안요구**
  (로그·접근통제·인시던트 보고) 대응 체계 미비.

■ **대응방안**

EU AI Act 대비 체크리스트

1. AI 시스템 위험등급 사전분류 및 문서화
2. 데이터셋 품질관리·비식별화 기록 유지
3. AI 접근로그 보관(12개월 이상)
4. CE 마크 등 **EU 기술인증+AI 보안 인증 동시 준비**
5. GDPR 대응용 DPO(Data Protection Officer) 지정

미국 (U.S.)

주요 규제

법령/정책	발표 기관	주요 내용
NIST AI Risk Management Framework (RMF)	NIST (2024)	AI 시스템 전 생애주기 리스크 식별·통제·모니터링 기준 제시. 보안성·투명성·인간 감독성 강조.
Executive Order on Safe, Secure, and Trustworthy AI	백악관 (2023.10)	연방정부 조달·AI 개발사에 대한 **보안·데이터 보호 표준 의무화**, AI 훈련 데이터 공개 요구.
Cybersecurity Maturity Model Certification (CMMC 2.0)	국방부 (2025 예정)	공급망 내 보안 역량을 5단계로 평가. 민간 납품기업에도 보안 인증 의무화 예정.

■ **한국 기업의 애로사항**

미국 조달시장 진입 시 **CMMC 보안성 인증 미보유** 기업은 입찰 불가.

AI 솔루션 제공 시 NIST RMF 준수 보고서 요구.

AI 학습데이터 출처·보안성에 대한 **자체검증 문서 미흡**.

■ **대응방안**

NIST RMF 기반 기업 대응

- AI 위험관리 책임자 지정 (AI RM Officer)
- AI Risk Register(위험 기록표) 유지
- 로그·알고리즘 변경이력 추적체계 구축
- 보안관리체계(ISO 27001) + CMMC 동시 인증 준비

중국 (CHINA)

주요 규제

법령	시행/발효	핵심 내용
GDPR (General Data Protection Regulation)	2018년 시행	개인정보 처리·이전 시 **명시적 동의, 데이터 주체권리, 역외 적용** 의무. AI 학습데이터에 개인식별정보 포함 시 처벌 가능.
AI Act (Artificial Intelligence Act)	2025년 발효 예정	AI 시스템을 **위험등급(High/Medium/Low)** 으로 분류하여 **데이터 품질, 보안성, 로그관리, 인간감독** 의무 부여. 수출 AI 모델도 인증 필수.
NIS2 Directive (Network & Information Security 2)	2024~25년 전환	공급망·산업제조·물류 부문에 **보안조직 지정, 침해사고 보고의무(24h), 제로트러스트 체계** 도입 요구.

■ **한국 기업의 애로사항**

AI 모델·클라우드 서비스 역외 이전 시 심사 필요 → **Cross-border Data Transfer 절차 복잡**.

중국 현지 파트너와 협업 시 데이터 로컬라이제이션 부담.

생성형 AI 서비스 수출 시 **중국 내 검증제도(보안테스트)** 필수

■ **대응방안**

중국 진출 시

- 중국 내 데이터센터 이용 또는 중국 내 저장 의무 검토
- 사전 보안평가(Security Assessment) 절차 확보
- 모델 데이터셋 출처 기록 유지
- 중국 협력사와 **데이터공유계약(DPA)** 표준화

일본 (JAPAN)

주요 규제

법령/정책	발표기관	주요 내용
K-인공지능 보안 가이드라인 (2024)	과학기술정보통신부	생성형 AI 보안·개인정보보호 위험에 대한 대응 지침. **비식별화, 로그관리, 접근통제, 책임자 지정** 권고.
AI 윤리기준 (AI Ethics Standards)	한국지능정보사회진흥원(NIA)	AI의 공정성·투명성·책임성 원칙.
국가 AI 거버넌스 로드맵 (2025)	산업통상자원부·KATS	ISO/IEC 42001 국내 도입 추진, **AI 인증체계 기반 수출지원** 목표.
개인정보보호법 개정안 (2024)	개인정보보호위원회	AI 학습데이터 처리 시 **사전고지·비식별화 의무화** 조항 신설.

한국 기업의 애로사항

일본 바이어들이 TISAX·ISO27001 인증 보유를 거래조건으로 요구.

AI 시스템의 “편향 검증” 기준 불일치로 기술평가 시 불이익.

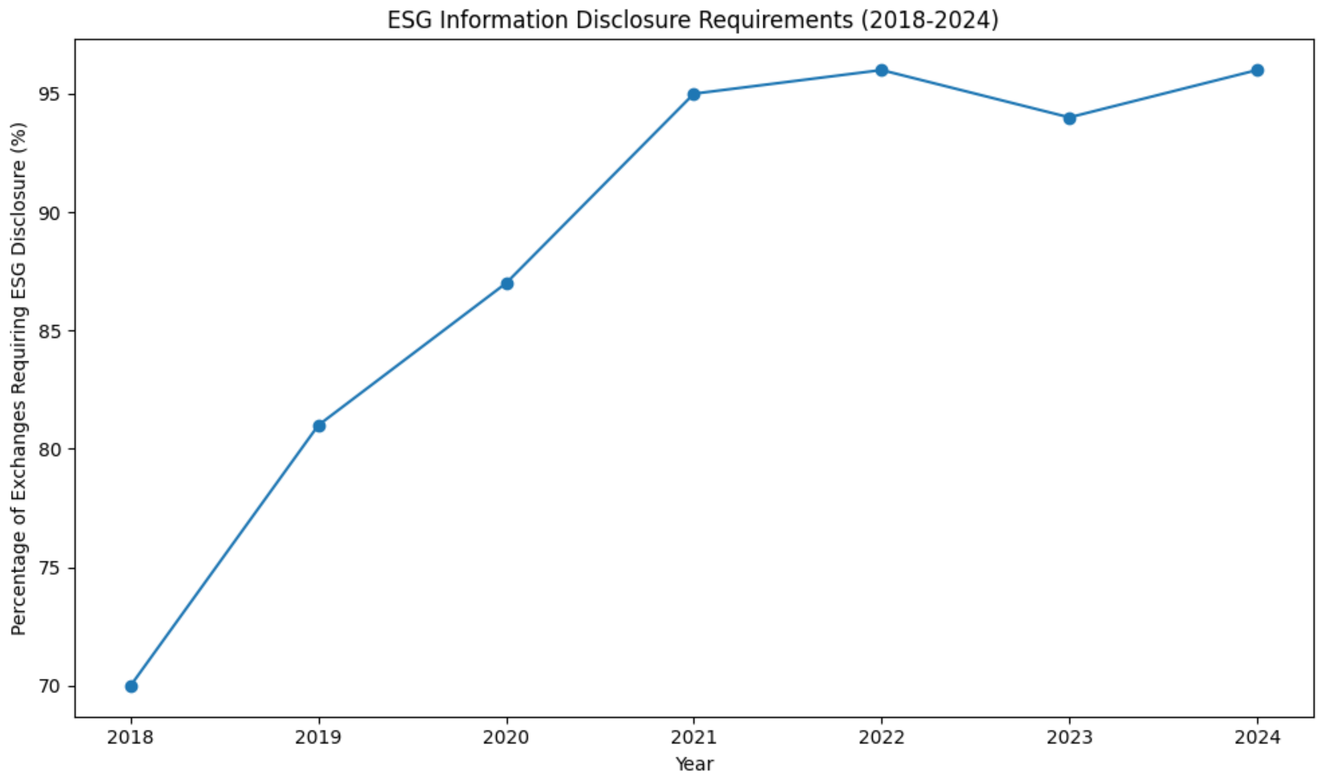
■ **대응방안**

일본시장 대응

- 일본 METI 인증제 동등수준의 **AI 보안성 평가문서** 준비
- ISO 27001, ISO 42001 동시인증 고려
- 협력사 데이터 공유 시 계약서 내 보안조항 명시

ESG·데이터보호 결합 규제 = 무역 데이터의 '이중 의무'

ESG 기준을 충족하더라도 보안인증 **"향후 강화될 가능성 있음"**



- 전 세계 거래소 중 **96%가 ESG 정보공개를 투자자 요구사항으로 명시**.
- 이 ESG 보고서에는 **공급망 거래처, 환경·안전데이터, 생산공정 정보**가 포함.
- 하지만 ESG 데이터가 공격 대상이 되면서
  → **구매기업은 ESG 제출과 동시에 '보안 검증서 (Security Verification)' 제출을 요구하는 추세**.

즉, **ESG + 데이터보호 = 복합형 TBT 규제**
(ESG 기준을 충족하더라도 보안인증 없으면 거래 불가한 구조로 진화)

TBT형태의 “AI·보안 인증제” 등장 가능성

데이터 유출은 단순한 보안 리스크가 아니라 ‘무역 접근 조건’으로 전환 중

대응영역	필요조치	근거
AI 활용 가이드라인	내부 데이터 식별·비식별화·로깅 정책 수립	GDPR·AI Act
AI 보안성 검증체계 구축	제로트러스트 접근제어·모델 인증	NIST RMF·ISO27001
ESG 보고 데이터 관리체계	ESG 공개 전 암호화·메타데이터 검열	Statista ESG disclosure 2024
국가별 인증 대응 문서화	EU AI Act, TISAX 등 인증 매핑 문서	무역기술장벽(TBT) 사전 대응

AI 활용기업 보안성 인증제(AI Security Certification):
EU·미국·한국이 공동 논의 중 (OECD AI Safety Summit 2024 결과).
→ “AI 시스템의 데이터보호·로그관리·접근제어 기준”을 기술규격으로 표준화 예정.

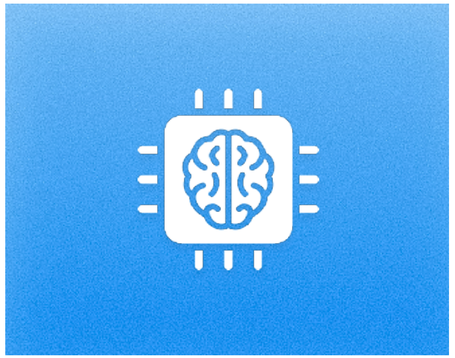
이 제도는 실질적으로 **AI를 활용하는 수출기업이 시장 접근 전에 거쳐야 할 기술적 검증 절차**,
즉 **TBT형 비관세장벽**으로 발전할 가능성이 높습니다.

01

2024 데이터 유출 급증

- 제조·무역 부문 유출 1,036건

- 유출 데이터 64%
  = 내부 문서·기술자료



02

ESG· 거래 데이터 노출 확대

- ESG 보고서, 공급망 문서에 거래처·기술정보 포함

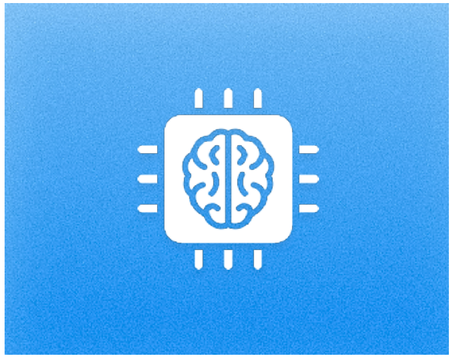
- E96%의 거래소가 ESG 데이터 공개 요구, ESG 데이터 해킹 및 제3자 플랫폼 유출 사례 다수

03

구매자의 보안요구 강화

- ESG 제출 시 보안검증서 동반 요구 증가

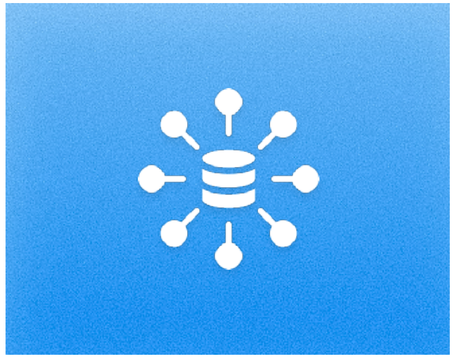
- OEM·대기업, 협력사에 ISO27001·TISAX 강요



04

AI 보안 인증제·데이터보호 표준 등장

- EU AI Act (2025):
  AI 보안성·데이터검증 의무화
- NIST AI RMF (2024):
  AI 위험관리 표준 제정
- OECD AI Safety Summit (2024): 인증체계 국제논의



05

무역기술장벽 (TBT)으로의 진화 가능성

- "보안·AI 인증 없이는 수출 불가" 규제 현실화

- AI 보안 인증서, ESG 데이터 검증 보고서가 품질인증서와 동일한 '통관 요건'으로 작용

Source: Statista (Verizon DBIR 2024, ESG Disclosure 2024);
EU AI Act (2025); NIST RMF (2024); OECD AI Safety Summit (2024); Nikkei 2025.

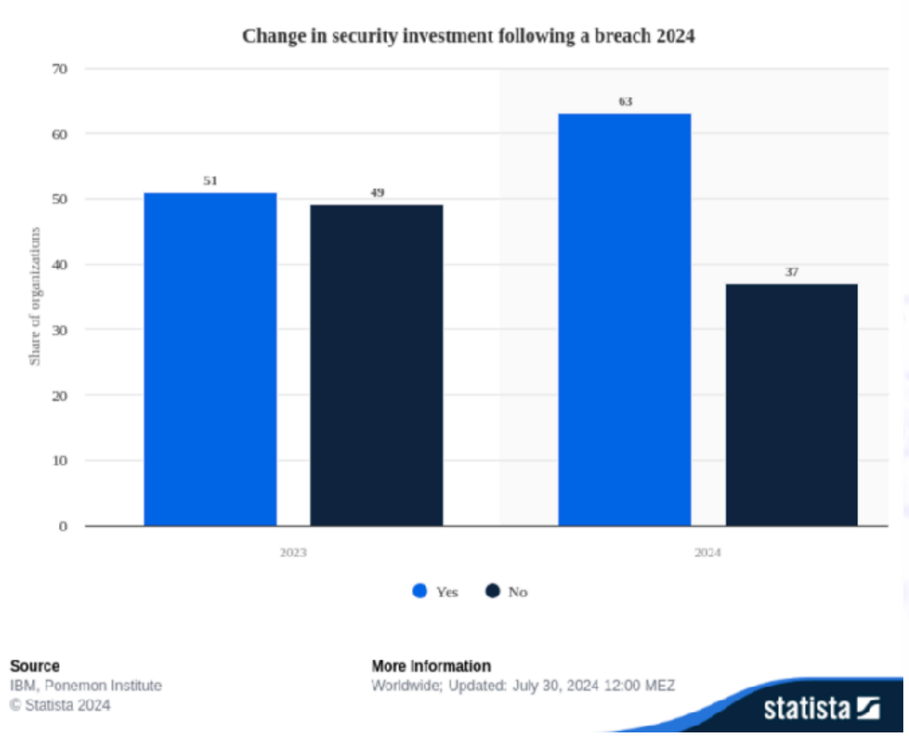
03.

유출 사례 및 국가별 인증 지원 비교: 선도국 사례와 한국의 과제

데이터 유출 후 **63% 기업이 보안 투자 확대**

공급망·무역기업은 바이어 요청에 따른 보안 플랫폼 구매가 납품 조건화.
보안 수준이 곧 거래 자격(TBT 요건) 으로 전환 중

Change in security investment following a breach (2024)



무역·공급망 기업에 대한 특이점

- 무역·제조업은 **공급망 보안 사고가 직접적인 납품 차질로 연결**되므로, 구매기업(바이어)의 요청에 의해 보안 솔루션 도입이 '계약조건화'되는 사례 증가.
  → 예: 일본·EU OEM 협력사 대상 "보안 플랫폼 구입 의무 조항" 삽입 (Nikkei 2025 보도).
- 이 구조는 사실상 **비관세 장벽형(TBT) 규제**와 유사한 형태로 작동.

연도	보안 투자 증액 결정 기업 비율 (Yes, %)	증액하지 않음 (No, %)	전년 대비 변화(%)
2023	51	49	—
2024	**63**	37	**+12%p 증가**

실제 사례

무역기업의 내부문서, 거래처, ESG 보고서 데이터는 실제로
제조·서비스 분야 유출의 60% 이상을 차지하며 공급망 공격이 거래 파트너를 직접 노린다는 점이 확인되었습니다.
더 나아가, 일부 글로벌 구매자는 이를 이유로 **보안 솔루션 구매를 계약조건화**하고 있어
'데이터유출 → 보안투자 강요'라는 새로운 무역비용 구조가 형성되고 있습니다.

사례	설명	출처
1. 독일 OEM 공급망: ESG 보고서 제출 중 내부설계 누출 (2024)	납품기업이 ESG 관리 포털에 업로드한 PDF 내부에, CAD 설계데이터 메타정보 포함되어 유출. 이후 OEM이 **해당 공급망 전 업체에 데이터암호화 솔루션 구매 요구**.	Handelsblatt 2024.07,
2. 일본 자동차부품사, 유럽 바이어의 보안솔루션 강제 구매 요구 (2024)	유럽 완성차사가 'AI 보안검증' 포함한 SaaS 사용 인증 없이는 계약 불가 통보. **협력사 약 150개사가 동일 보안 솔루션 구매**.	Nikkei Business 2025.02
3. 한국 전자부품 중견기업, ESG 데이터 플랫폼 해킹 사고 (2024)	납품사들이 공용 ESG 보고시스템을 통해 **탄소배출 데이터 업로드 중 공격받아 거래처 목록 유출**.	한국인터넷진흥원(KISA) 2024.09

일본 경제산업성(METI) 공급망 보안 인증 지원 프로그램

이 프로그램은 일본 정부가 해외 규제와 바이어 요구에 대응하기 위해 구체적인 **컨설팅·비용 지원**

일본 경제산업성(METI)

Supply Chain Security Certification Promotion Program

1. 프로그램 개요 (2024.12.21 발표)
일본 경제산업성(METI)은 유럽 OEM이 요구하는 사이버보안 인증(TISAX 등)을 일본 수출기업이 원활하게 획득하도록 지원하는 **'서플라이체인 보안 인증 촉진 프로그램'을 공식 출범**했다.

- 기업에 **정보보안 전문가 무상 파견**
- EU 사이버보안 규정 대응을 위한 **갭 분석·보안조치 가이드**
- 국제 인증 취득 과정(감사·컨설팅·자료화 등) 실질 지원

유럽 OEM(특히 독일)은 공급망 전체의 보안 수준 강화를 위해

- **TISAX 인증 필수화**
- EU Cyber Resilience Act 등 **사이버보안 규제 강화**를 적용 중이다.
  이에 따라 일본 부품·제조 기업이 **보안 인증을 갖추지 못하면 거래가 중단될 위험**이 커졌고, METI는 이를 국가 차원에서 대응하기 위해 지원 프로그램을 마련했다.

EU·미국 중소기업(SME) 사이버보안 지원 프로그램

ENISA는 ‘SME 보안 성숙도 향상’ 중심, NIST는 ‘기본 보안체계 정립 + 실천 중심’

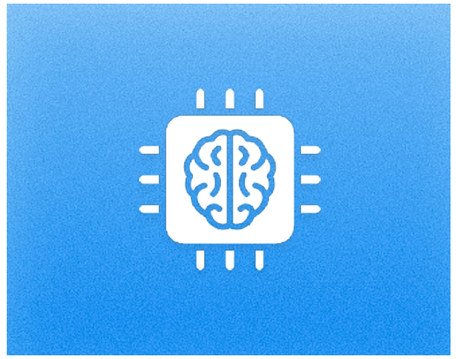
구분	EU – ENISA(유럽 사이버보안청)	미국 – NIST(국가표준기술연구소)
지원 목적	EU 내 중소기업(SME)의 사이버보안 성숙도 향상 및 공급망 안정성 강화	중소기업의 사이버보안 리스크 관리 역량 강화 및 기본 보안수준 제고
핵심 지원 형태	• 위험평가·비즈니스 연속성·클라우드 보안·데이터 보호 가이드 제공 • SME용 사이버위생·보안 실천 가이드 제공(12 Steps Guide) • SecureSME Tool 등 교육·캠페인 제공	• NIST CSF 2.0 기반 Small Business Quick-Start Guide 제공 – SMB의 리스크 전략 수립 지원 • NISTIR 7621: 중소기업 보안 기본원칙 제공 – 비기술자도 이해하기 쉬운 언어로 구성
특징적인 도구/프로그램	• **Cybersecurity Maturity Assessment Tool** – SME 사이버보안 성숙도 자가진단 도구 제공 • 팬데믹 이후 원격근무·랜섬웨어 대응을 위한 실용 가이드 다수	• **CSF 2.0 Quick Start** – 6대 기능(Govern–Identify–Protect–Detect–Respond–Recover) 기반 실천 안내 • **NISTIR 7621** – 정보자산 식별·가치평가·자산목록화·위협 이해 등 기본 보안 프레임 제공
SME에 제공되는 혜택	• 무료 가이드·온라인 툴·교육 캠페인 제공 • EU 회원국들의 SME 보안 지원정책 설계를 위한 권고안 제공	• SMB 대상 보안 리스크 관리의 출발점을 제공 • 자가진단 + 실천 가이드를 통해 내부 보안정책 수립을 지원
TBT 관점의 의미	국제 보안 요구에 대응하도록 ‘**준비도’를 높여 공급망 안정성을 강화** → 향후 EU AI Act/CSRD/NIS2 인증 대비 기반 마련	미국 기업들의 최소 보안 수준(Base Level)을 제시해 연방조달시장 참여 요건 충족 지원 → 글로벌 공급망에서 ‘기본 보안 표준’ 역할
한국 수출기업에의 시사점	• ENISA처럼 **SME 맞춤형 보안 성숙도 진단도구** 필요 • 국내 공급망 보안 가이드·교육 부족 영역을 메울 수 있음	• NIST처럼 **단계별·행동 중심 가이드** 제공 필요 • 공급망 내 한국 중소기업이 글로벌 OEM 보안 요구를 이해·준수하도록 지원 가능

01

생성형 AI 및 ESG 데이터 활용 확산

- 수출기업: AI로 **문서작성·리서치·** 응대 자동화

- ESG 보고 의무: 공급망 전반에 데이터 공유 확대



02

내부 데이터·거래처 정보 유출 증가

- 제조·무역 부문 데이터유출 1,036건, 유출 정보의 64%가 **내부문서·기술자료**

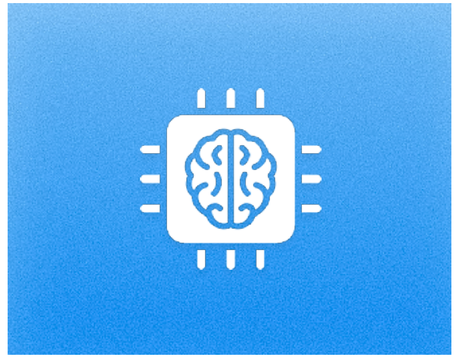
- ESG 포털 **해킹·AI 입력데이터** 노출 사례 다수

01

바이어측의 리스크 인식 강화

- ESG 규제·AI 보안 우려로 공급망 보안 점검 강화

- 거래업체에 보안·ESG 솔루션 도입 '요구' 확대

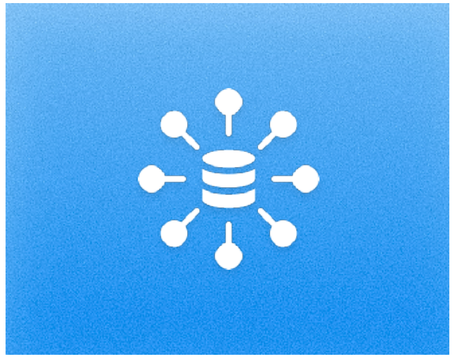


02

보안·솔루션 구매 강요 및 거래비용 전가

- 글로벌 OEM: 보안인증·AI검증 솔루션 구매 의무화

- 협력사: ISO27001, TISAX, EcoVadis 도입 강제 사례



03

보안투자 확산 및 구조적 악순환

- 데이터유출 기업 63%가 보안투자 증액

- AI보안·ESG 인증이 신(新) TBT로 부상

한국 수출기업의 전략 과제: AI 보안 경쟁력 확보

과제 분야	한국이 직면한 문제	필요한 대응 방향	근거/배경
국가 차원의 공급망 보안 인증 지원체계 부족	일본 METI처럼 TISAX·ISO27001·AI 보안 인증 취득을 지원하는 **국가 프로그램 부재**	• 국가 차원의 **보안 인증 비용 지원 프로그램 도입** • 산업부·KISA 중심의 **AI·보안 인증 컨설팅 체계 구축**	• 일본 METI는 2024년에 **90건 이상 지원** 실시(공급망 인증 지원 프로그램)
한국형 AI 보안·데이터보호 표준 미비	98% 기업이 AI 결과 검증 기준 없음 → **EU·NIS2·ISO42001 대응 불가**	• **한국형 AI 보안 가이드라인(K-AI Security Standard)** 제정 • OECD·NIST 기준 기반의 기술 규격 정비	• EU AI Act, NIS2는 **데이터보호·로그관리·추적성**을 인증 요건으로 명시
산업별 AI·보안 역량 격차 심각	제조·무역 기업의 AI·보안 가이드라인 보유율 1.2%	• 산업별 **AI·보안 성숙도 모델 개발(Secure SME Korea)** • 중소기업 대상 **교육·평가 도구 제공**	• ENISA는 SME 대상 **성숙도 평가 도구** 제공하여 EU 전체 역량 제고
ESG·AI 보안 문서의 수출 필수요건화 미준비	ESG + 보안 검증 보고서가 **TBT성 수출 문서**로 변하는 중	• **ESG 보고서 + AI 보안성 보고서를 수출 기본서류 패키지화** • 정부 차원의 템플릿·검증체계 제공	• 96% 거래소 ESG 공개 요구• 바이어가 ESG 제출 + 보안 검증서를 동시에 요구
AI 보안 인증 생태계 부재	기업이 개별적으로 방어 → 비용·리스크 급증	• **국가 인증 매핑 문서 (EU AI Act·TISAX·ISO27001 대비표)** 제공 • 인증기관·컨설팅사·교육기관의 **AI 보안 클러스터 구축**	• 일본·EU는 이미 공급망 전체 인증을 통합 관리

04.

한국 수출기업을 위한 AI 보안 거버넌스 4대 핵심 축

수출기업을 위한 AI 데이터보호·보안 체계 수립 가이드

EU AI Act · GDPR · NIS2 · ISO/IEC 42001 대응 중심

01. AI 활용 가이드라인 수립 및 전사 교육

AI는 '자동화 도구'가 아니라 '데이터 기반 위험 시스템' → 사용 규정이 없으면 TBT 인증 단계에서 탈락 위험.

왜 필요한가?

- 한국 기업의 **91% AI 정책 없음** → EU AI Act 인증 문서 제출 불가
- 제조·수출기업의 **98% 검증 기준 없음** → 편향·오류·PII 유출 위험
- 일본·EU OEM은 이미 **협력사 AI 사용 가이드 제출 요구** 시작

무엇을 해야 하는가?

- **AI 사용범위 명문화**
  - 어떤 부서/업무에서, 어떤 모델을, 어떤 데이터로 사용할 것인가
- **금지데이터 정의**
  - 거래처 정보, 내부 기술자료, 금융·PII 등
- **전사적 AI 윤리·보안 교육 체계화**
  - AI Literacy + Security Awareness
  - 분기별 교육 + 업종별 전문 과정

기대효과 / TBT 대응 포인트

- 향후 **EU AI Act 인증 문서**에 포함될 가능성 매우 높음
- "AI 정책 없음 = 수출 불가" 리스크 제거
- 바이어 신뢰·ESG 보고·보안 문서 품질 향상

02. AI 보안성 검증체계 구축

AI 보안성 검증은 TBT 시대의 새로운 '안전성 검사'이다.

왜 필요한가?

- 공급망 공격의 70%가 협력사 문제에서 발생
- AI 모델 자체가 공격 벡터로 사용됨
- 일본·EU OEM이 협력사에 **TISAX·ISO27001·보안 플랫폼 도입 '의무화'** 사례 증가

무엇을 해야 하는가?

Zero Trust 보안 구조 적용

- 사용자·단말·AI 모델·데이터 모두 검증 기반 접근

AI 모델·입력 데이터 검증 절차 표준화

- 모델 업데이트, 로그 저장, 검증 리포트 출력

국제표준 매핑 체계화

- ISO 27001
- NIST AI RMF
- 일본 TISAX 요구사항 비교표 작성

기대효과 / TBT 대응 포인트

- 보안성 검증이 납품조건이 되는 시대에 대비
- 일본 METI처럼 국가 차원의 인증체계 구축 기반
- 바이어가 요구하는 "**검증 가능 AI**" 조건 충족

03. ESG 데이터 보호 관리체계 강화

ESG 데이터는 곧 기술정보·거래정보 → 보호 없으면 공개도 안 되는 시대

왜 필요한가?

96% 글로벌 거래소 ESG 공시 요구

ESG 보고서 내부에 기술도면·운영데이터·직원정보·거래처 데이터 포함

실제 유출 사례:

- 독일 OEM ESG 포털 → CAD 설계 메타데이터 유출
- 한국 중견 부품사 → ESG 플랫폼 해킹

무엇을 해야 하는가?

- **데이터 암호화·마스킹·메타데이터 제거 의무화**
- **ESG 보고서 + 'AI 보안 검증 보고서'를 하나의 Dual Compliance Pack으로 구성**
- **공**급망 전 단계에서 **데이터 생성·보관·공유·삭제 정책** 수립

기대효과 / TBT 대응 포인트

- "ESG 충족했어도 보안 검증 없으면 수출 불가" 상황 방지
- ESG + Security = **복합형 비관세장벽(TBT)** 대응
- 바이어의 공급망 리스크 점검에 대응 가능한 문서 체계 확보

04. 국가별 인증 대응 문서화

"인증 문서화는 수출기업의 '시장 접근권(Market Access Right)'을 결정한다."

왜 필요한가?

- EU AI Act · NIS2 → 기술문서·로그·보안성 검증 제출 의무
- 일본 TISAX → 납품 조건화
- 한국 기업은 **규제 해석·문서화 역량 부족**
  → 준비 없는 상태로 심사 탈락 위험高

무엇을 해야 하는가?

- **국가별 규제 매핑 문서 개발**
  - EU AI Act / ISO 42001 / NIST RMF / TISAX 요구사항 비교
- **인증 대비 문서 템플릿 제공**
  - 거AI 정책서 / Data Protection Impact Report / 보안 로그·테스트 리포트
- **수출 기본 패키지(Standard Export Compliance Pack)** 구축
  - AI AI Policy / Security Verification Report
  - ESG+보안 결합 보고서

기대효과 / TBT 대응 포인트

- 준비 없는 수출 심사(TBT 사전인증) 탈락 방지
- 글로벌 OEM 공통 요구사항을 충족하는 **문서 품질 확보**
- 수출 프로세스 자동화 및 심사 속도 향상

AI 사이버보완

한국 수출기업을 위한 **AI 보안 거버넌스 4대 핵심 축 가치**

01

AI 활용 가이드라인 수립 및 전사 교육

- ✓ **사용범위 명문화** (Scope Definition)
- ✓ **금지데이터 설정** (Data Prohibition)
- ✓ **전사 AI 교육** (AI Literacy & Training)

"무엇을 허용하고, 무엇을 금지하며, 누가 책임지는가"를 문서화하고 교육까지 포함해야 함.

02

AI 보안성 검증체계 구축

- ✓ **제로트러스트** (Zero Trust)
- ✓ **모델·데이터 검증** (Model/Data Validation)
- ✓ **국제표준 매핑** (ISO/NIST/TISAX Alignment)

AI 모델·입력데이터·접근권한을 모두 '검증 가능한 구조'로 만들고, 국제 규격에 일치시키는 과정.

03

ESG 데이터 보호 관리체계 강화

- ✓ **데이터 암호화·마스킹** (Encryption / Masking)
- ✓ **ESG+보안 결합 보고서** (Dual Compliance Reporting)
- ✓ **공급망 데이터 보호** (Supply Chain Data Security)

ESG 보고서가 곧 기술정보·거래정보의 집합이므로 "보안 없이는 공개도 안 되는 구조"로 바뀌고 있음.

04

국가별 인증 대응 문서화

- ✓ **규제 매핑 문서** (Regulation Mapping)
- ✓ **인증 대비 문서화** (Documentation Readiness)
- ✓ **수출 요건 충족** (Market Access Compliance)

EU AI Act · NIS2 · TISAX 등 요구사항을 체계적으로 정리해 "수출통과 문서 패키지"를 갖추는 것.

AI 보안 거버넌스는 선택이 아니라 수출 자격요건입니다.

감사합니다.