World Customs Organization

人工智能和机器学习应用于海关工作中的研究报告

2025年3月

wcoomd.org

项目出资方

中国海关 CHINA CUSTOMS

人工智能和机器学习应用于海关工作中的研究报告

2025年3月

翻译及校对：

重庆海关（卢科宇 涂雨帆 孙培力）

World Customs Organization

目录

图表

表格

缩略语

AI	人工智能
CPU	中央处理机
DNNs	深度神经网络
DVC	数据版本控制
GACC	中国海关总署
GDPR	一般数据保护条例
GNNs	图神经网络
GPU	图形处理单元
HITL	人机回圈
HS	协调制度
IaC	基础设施即代码
IDE	集成开发环境
IPR	知识产权
KCS	韩国海关署
LLMs	大型语言模型
ML	机器学习
MLOps	机器学习操作
NLP	自然语言处理
OCR	光学字符识别
OECD	经济合作与发展组织
RAM	随机存取存储器
RBAC	基于角色的访问控制
WCO	世界海关组织
WTO	世界贸易组织

1 执行摘要

人工智能（AI）和机器学习（ML）技术正在全球范围内彻底改变海关业务操作，为提高效率、改进决策和应对全球贸易和边境安全中的复杂挑战提供了前所未有的机会。这些技术能够提升海关的常规通关流程的自动化水平，提高风险评估和伪瞒报查发能力，优化资源配置，并通过优化通关流程促进贸易便利化。人工智能/机器学习应用的关键领域包括通关效率和贸易便利化、风险管理、情报和监控、预测分析和实时处置，以及人力资源管理和能力建设。

为了成功实施人工智能/机器学习项目，各国海关必须考虑几个关键因素。首先需要谨慎处理人工智能所涉及的法律和伦理框架，以确保合规和负责任的部署。数据的可用性、质量和管理是人工智能/机器学习项目成功的基础，这需要在数据准备和治理方面进行大量~~投资~~投入。此外，还必须满足技术基础设施和专业知识的要求，包括软硬件投资以及专业技术人才。

为了合理化人工智能/机器学习投资，应进行全面的成本效益分析，并建议通过试点项目先行验证其可行性与有效性，再进行全面推广

本报告旨在为各成员海关提供有关于采用人工智能和机器学习技术的全面认知， 内容涵盖最低技术规范、成本、发展趋势、应用场景、业务流程、政策安排以及法律要求等方面。其目的是帮助世界海关组织成员掌握相关知识，从而做出明智的决策，将人工智能与机器学习技术有效融入其业务运营之中。通过提供对这些技术的实践性见解，本报告旨在缩小世界海关组织成员之间的数字鸿沟，推动各成员更公平地获取人工智能/机器学习工具，并帮助各成员海关解决日益复杂的全球贸易环境所带来的挑战。

本报告概述了人工智能/机器学习实施和集成的可扩展技术框架，涵盖了人工智能/机器学习开发环境、数据管理和治理工具、模型开发和训练平台以及部署选项。该框架确保拥有灵活的技术基础，以有效支持AI/ML倡议，允许根据各自的需求和资源逐步采用和扩展。建立机器学习操作(MLOps)能力对加速AI开发和部署至关重要，能够提高模型性能和可重复性，并减少与AI项目相关的风险。

为了为AI/ML的采用做好准备，应投资于全面的培训项目，以发展各个领域的内部专业知识，包括数据科学、软件工程和领域特定知识。在组织内培养数据素养文化至关重要，以确保技术和非技术员工都能有效贡献并受益于AI/ML倡议。与外部专家和学术机构的合作可以提供有价值的见解，并使始终处于技术进步的前沿。

实施强大的数据集成工具对于无缝系统互操作性至关重要，使AI/ML模型能够实时访问、处理和提供可操作的见解，跨多个系统进行工作。安全性和合规性考虑在AI/ML采用中至关重要。必须实施全面的网络安全措施，包括数据加密、访问控制和遵守数据保护法规，以保护敏感和贸易数据。定期审核和监控AI/ML系统是必要的，以确保持续合规并检测模型输出中的潜在偏见或不准确性。

AI/ML在运营中的伦理影响不可小觑。必须建立明确的责任使用AI的指南，解决公平性、透明度和问责制等问题。定期评估AI系统的潜在偏见和意外后果对于维护公众信任和确保贸易生态系统中所有利益相关者的公平对待至关重要。

通过拥抱AI/ML技术，将自己置于贸易便利化和边境安全的前沿。这些先进工具使国际贸易在日益复杂的全球环境中实现更高效、透明和安全的运营。然而，成功的实施需要一种全面的方法，解决技术、组织和伦理方面的考虑。通过仔细规划、基础设施和技能的投资以及对负责任的AI实践的承诺，海关管理部门可以利用这些技术显著增强其能力，最终惠及全球贸易和经济增长。

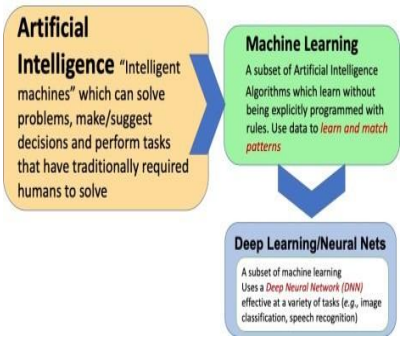
2 人工智能（AI）和机器学习（ML）概述

人工智能(AI)是一个广泛的术语，涵盖使机器能够执行传统上需要人类智能的任务的技术。这些任务包括解决问题、做出决策和从经验中学习。AI不是单一的技术，而是各种技术的集合。

机器学习(ML)是AI的一个子集。它涉及在数据上训练算法，以识别模式并在没有明确编程的情况下做出预测或决策。例如，一个ML模型可以学习基于图像区分猫、狗和人类，或理解文本的内容。

下面的图表提供了AI、ML和深度学习之间关系，突出了它们的定义和关键概念，并解释了AI和ML中使用的常见术语。

图1 - 什么是AI/ML?[1]



人工智能
"智能机器"，能够解决问题、做出/建议决策，并执行传统上需要人类解决的任务

机器学习
人工智能算法的一个子集，可以在没有明确编程规则的情况下进行学习。使用数据进行学习并匹配模式。

深度学习/神经网络
机器学习的一个子集，使用深度神经网络（DNN）在各种任务中有效，例如图像分类、语音识别

2.1 AI/ML - 简要历史

AI经历了动态而多面的演变，其特点是突破性成就的周期与因科学障碍和夸大的期望而产生的怀疑期。

在AI的基础年(1956-1974)，主要目标是创造通过通用搜索策略能够进行一般问题解决的智能机器。科学家们相信，如果机器能够使用符号（如文字或数字）来表示任务，就可以利用这些符号进行推理，从而解决各种问题。然而，他们很快意识到，这种宽泛，一刀切式的方法并不足以让机器达到理想的智能或性能水平。

在1980年代，出现了从基于搜索的范式转向基于知识的范式，这导致将大量领域知识嵌入高度专业化的人工智能专家系统中，主要设计用于模拟人类专家在特定"领域"中的决策能力。例如，美国国内税务局（U.S. IRS）尝试使用专家系统来协助税务审计和欺诈检测。[2] 这些系统旨在复制资深审计员的决策能力

[1] Blank, S. (2022).人工智能与机器学习解析。steveblank.com。

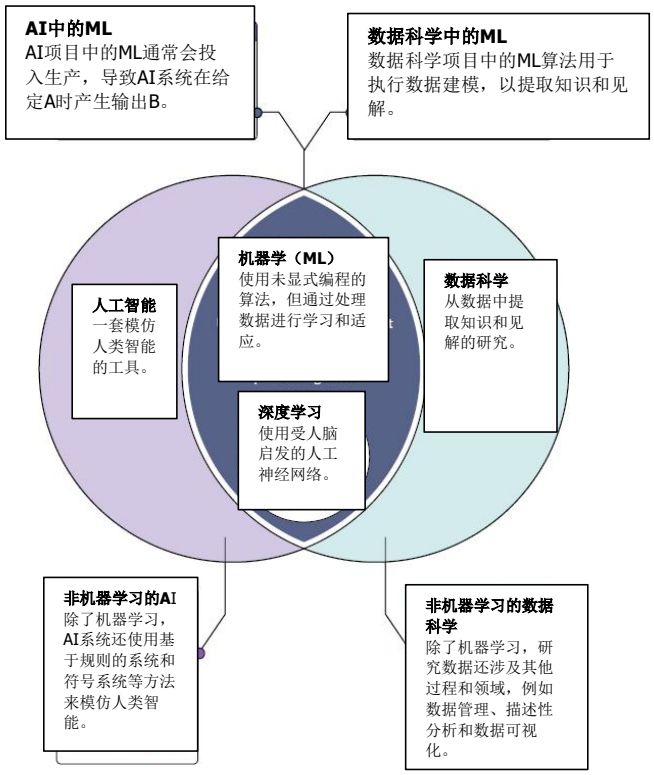
[2] McCoy, K. F. (1989).国内税务局中*的专家系统*应用。《年度税务会议论文集》（第147 – 154页）。国家税务协会。

将税法和规定编码到知识库中。[3] 然而，税法的复杂性和个案之间的细微差别常常导致不准确的评估。人类审计员经常需要介入以解释结果并做出判断，从而暴露这些系统的局限性。虽然专家系统展现出了潜力，但它们本质上是脆弱的，只在有限的范围内表现良好，并且严重依赖人类专家来填补设计意图与实现应用之间的差距从1990年代到2010年，研究者探索了多代理系统和语义网等替代方法，但取得的成功有限。语义网旨在通过以标准化格式结构化数据使网络内容对机器更易于访问。像美国的Data.gov和英国的Data.gov.uk等公共部门倡议，试图利用这项技术来促进政府部门之间以及政府与公众之间的数据共享。启动了促进开放数据标准的项目。然而，这些系统在扩大至现实世界复杂性时遇到了挑战，包括不可预测的人类行为和环境因素，以及语义网技术的普遍采用不足和互操作性问题限制了它们的有效性。[4]

2.2 机器学习（ML）的崛起

虽然人工智能涵盖了使机器能够模拟人类智能的技术，但机器学习（ML），作为人工智能的一个子领域，是指从数据中学习以提高预测的算法。数据科学结合了统计方法和计算技术，以分析和提取结构化和非结构化数据源中的有意义的见解。下图展示了人工智能、机器学习和数据的关键科学术语。

图2 - 人工智能、机器学习、数据科学术语



[3] “知识库”是一个信息存储库，促进知识共享和解决问题，而不仅仅是数据存储，如“数据库”中的情况。

[4] Heitmann, B.,et al. (2009).实施语义网应用程序：参考架构和挑战。第5届会议论文集th 国际语义网启用软件工程研讨会）

[5] 新加坡政府技术局（2019），“公共部门人工智能手册”

20世纪80年代专家系统是基于规则的人工智能系统，设计用于使用条件-结果规则和知识库模拟人类决策。尽管它们代表了人工智能领域的早期发展，但它们有几个局限性，后来机器学习对此进行了改进。机器学习（ML），作为人工智能（AI）的一个子集，专注于创建使计算机能够从数据中学习并在没有明确编程的情况下做出预测或决策的算法。机器学习最先进的形式之一是深度学习，它依赖于神经网络在大型数据集中识别模式。

深度学习涵盖了各种神经网络架构，包括深度神经网络（DNNs）和图神经网络（GNNs）。这些架构受到人脑的启发，由相互连接的层级节点（神经元）组成。每个节点复杂处理信息并做出决策，并将信息和决策传递给下一层，使网络能够学习数据中的复杂模式和关系。

深度神经网络（DNNs）作为早期专家系统的强大替代品崭露头角，利用数据驱动的学习方式，克服了收集专家知识和常识推理等挑战。DNNs 擅长处理在欧几里得空间中的结构化数据，如图像或文本序列。DNNs 的兴起标志着人工智能的一个转折点，使得在图像分类、游戏玩法、语音识别和语言翻译等领域的超人类性能突破成为可能。

图神经网络（GNNs）是近几年的发展成果，旨在处理图结构数据，解决传统神经网络在处理非欧几里得数据时的局限性。GNNs 通过在节点之间传递消息来捕捉节点特征和图结构，能够建模数据中作为图表示的复杂关系，例如社交网络或分子结构。在中，DNNs 和 GNNs 都发挥着至关重要的作用。DNNs 通常用于风险评估和货物检查，分析历史货运数据以识别模式和检测异常，这五月表示走私、欺诈或错误申报。GNNs 可用于分析复杂的贸易网络，识别国际贸易中涉及实体的关系中的可疑模式。

尽管这些深度学习方法在人工智能发展中带来了令人瞩目的进步，但它们也面临挑战。它们通常需要大量标注数据，这可能在开发中形成瓶颈。此外，神经网络结构非常复杂，参数众多，往往使其作为“黑箱”运行，使得理解它们如何做出决策变得困难。

尽管面临这些挑战，DNNs 和 GNNs 仍继续以其高性能和处理复杂任务的能力推动人工智能的极限。DNNs 在处理网格状数据方面表现优异，而 GNNs 在处理关系数据方面开启了新的可能性。这种高性能与复杂性的结合继续塑造人工智能的演变，推动机器在海关业务等各个领域的学习和成就的边界。

2.3 生成性人工智能（Gen AI）的出现

生成性人工智能（Gen AI）代表了人工智能最先进的形式之一，能够通过识别现有数据中的模式和结构生成新的原创内容。其出现重新塑造了人工智能的发展格局，推动了各行业在创造力、自动化和问题解决方面的边界。

与依赖于预定义规则和结构化输出的传统人工智能模型不同，生成性人工智能学习生成与其训练数据相似的独特输出。这一能力使其成为文本生成、图像创作、视频合成和音乐创作等应用的强大工具，从而在娱乐，市场营销，教育等多个领域带来深刻变革。

2.3.1 生成性人工智能背后的技术

许多生成性人工智能模型依赖于神经网络，特别是 DNNs 和 GNNs。这些基于神经网络的方法显著促进了生成性人工智能能力的快速增长和多样性。

最初，深度神经网络（DNNs）为复杂模式识别和数据处理奠定了基础，使早期生成模型能够在图像和文本生成等领域创建基本输出。在此基础上，图神经网络（GNN）应运而生，擅长处理图结构化数据，并为涉及关系信息的任务提供便利，例如用于药物发现的分子生成、社交网络分析和推荐系统。

生成式人工智能发展的一个关键进步是Transformer模型的引入——通过关注句子中单词之间的关系来理解和生成语言的人工智能系统。它们利用自注意力机制，能够根据词语之间的联系而非其在句子中的位置，评估和优先处理纤细。这一创新显著增强了模型管理和解释海量数据集的能力，从而催生了如GPT-3、GPT-4和LLaMA等大语言模型（LLMs）。这些大语言模型在理解和生成连贯的上下文意识文本方面表现出前所未有的能力，为自然语言处理树立了新的基准。

与基于Transformer的大型语言模型同步发展的是，生成式AI领域出现了扩散模型。扩散模型通过首先向数据中添加随机噪声，然后逐步训练人工智能去除这些噪声来创建图像。这种方法允许模型生成高质量、逼真的图像。因此，扩散模型显着提高了生成式人工智能生成的图像的清晰度和多样性，增强了其在真实度和多样性方面的表现。

因此，生成模型继续进步，支持多模态应用程序，将其功能扩展到文本之外，包括文本到图像和文本到视频的生成。这些多模态生成式AI系统利用数十亿个参数，能够在多种格式中生成连贯且具有上下文相关性的内容，从而拓宽了生成式AI在创意和分析领域的应用范围和适用性。

生成式人工智能在文本之外的扩展，对多个行业产生了深远的影响。在艺术、设计和营销领域，先进的文本到图像模型能够从文本描述中创建高质量、逼真的图像，极大提升了创意表达的自由度和工作效率。同样，生成式人工智能驱动的视频生成允许从文本输入或静态图像生成动态视觉内容，彻底改变了内容创建和媒体制作流程。

尽管取得了这些进步，生成式人工智能还是带来了重大挑战。这些模型的复杂性需要专门的硬件，例如图形处理单元(GPU)[6]有效地执行计算。训练和部署这些模型所需的大量计算资源引发了人们对环境可持续性和人工智能技术公平可及性的担忧。此外，密集的资源需求会导致人工智能能力的集中化，可能会限制民主化发展和更广泛的社会福祉。

在部署生成式人工智能时，伦理问题至关重要。这些模型可能会无意中再现或放大其训练数据中存在的偏差，从而产出歧视性或不适当的内容。此外，生成式人工智能可能被滥用来创建深度假货或传播错误信息，这会带来重大的社会风险。解决这些道德挑战对于确保负责任地开发和应用生成式人工智能技术至关重要。

[6] 图形处理单元（GPU）处理并行任务，这对于渲染图像和训练机器学习模型至关重要。

展望未来，生成式人工智能代表了人工智能发展的一个重要里程碑，其特点是复杂的神经架构和跨各个领域的多功能应用。生成性人工智能的未来有望整合多种神经网络架构，包括深度神经网络（DNN）和图神经网络（GNN），与基于规则的系统和人类专业知识结合。这种混合方法旨在增强人工智能系统的灵活性和可靠性，使其能够更有效地处理意外情况。此外，正在进行的研究专注于提升人工智能模型的可解释性，确保其伦理运作并提高可持续性，减少人工智能计算对环境的影响。

表1概述了人工智能、机器学习、深度学习和生成性人工智能之间的层级关系，强调了它们的定义、重点领域、技术、应用、优势和数据依赖关系，以澄清它们的区别和相互联系。

表1 - 人工智能、机器学习、深度学习和生成性人工智能的区别

种类	**人工智能（AI）**	**机器学习（ML）**	**深度学习**	**生成式人工智能**
释义	计算机科学的一个广泛领域专注于创建模拟人类智能的系统，包括推理、学习和解决问题。	人工智能的一个子集专注于使系统能够从数据中学习并随着时间的推移提高其性能，而无需显式编程。	ML的一个子集，使用具有多层的神经网络（深度神经网络，DNNs）来对大量数据中的复杂模式进行建模。	人工智能和深度学习的一个子集，旨在通过从现有数据中学习模式来创建新内容，如文本、图像、音频和视频。
重点	通过推理、学习和决策来模拟人类智能，以执行通常需要人类认知的任务。	通过数据驱动的学习、根据历史数据进行预测和识别模式来增强系统性能。	处理大量结构化和非结构化数据以识别复杂的模式和表示，从而实现图像和语音识别等任务。	通过理解和复制培训数据中存在的潜在模式和风格，产生新的、创造性的输出，促进创新和内容创作。
使用的技术	基于规则的系统、决策树、专家系统、搜索算法、神经网络、自然语言处理（NLP）、计算机视觉。	线性回归、逻辑回归、决策树、支持向量机、聚类和强化学习等算法。	深度神经网络（DNNs）、卷积神经网络（CNN）、递归神经网络（RNNs）、图神经网络（GNNs）、变形金刚。	变分自动编码器（VAE）、生成对抗网络（GANs）、基于Transformer的模型（如BERT、T5）、扩散模型、自回归模型。
应用实例	自动驾驶车辆、虚拟个人助理（例如Siri、Alexa）、智能家居设备、机器人、游戏（例如。AlphaGo）。	垃圾邮件过滤、欺诈检测、推荐系统（如网飞推荐）、预测性维护、客户细分、股票市场分析。	图像和语音识别（如谷歌照片、Siri）、语言翻译（如谷歌翻译）、自动驾驶系统、医学图像分析。	文本生成（如ChatGPT、贾斯珀）、图像创作（如中途、达尔·E）、音乐创作（如。AIVA）、合成媒体创建、视频生成（例如合成）。
关键优势	实现自动化和智能化	允许系统从数据中学习和改进，	高效处理和	擅长创造高度逼真和

	在广泛应用中进行决策制定，提高各个领域的效率和有效性。	使其具备适应性，能够在没有明确编程的情况下处理复杂任务。	从大型非结构化数据集中提取有意义的见解，导致在图像和语音识别等任务中表现优越。	产生新颖的输出，促进跨多种媒体类型的内容生成中的创造力、创新和自动化。
数据依赖性	可能或者不太可能需要大规模数据集；取决于所使用的具体人工智能技术和应用。	需要结构化且通常经过标注的数据进行训练，以实现准确的学习和预测。	需要大量标注或未标注的数据以有效训练深度神经网络，利用大规模数据集以达到最佳性能。	需要海量数据集来学习复杂的模式和风格，从而生成多样化和高质量的内容，模仿现实世界的数据。

2.4 面向的人工智能

人工智能/机器学习正在日益转变海关业务。通过采用人工智能/机器学习可以充分利用其数据，无论是结构化、半结构化还是非结构化的数据。这些技术使海关能够分析大量数据，并在风险管理、欺诈检测、货物检查和资源分配等领域增强决策能力，从而提高整体效率。人工智能/机器学习还使海关管理机构能够应对跨境走私、合规性问题和不断增加的电子商务量等全球挑战，并更好地适应全球贸易和安全挑战的动态格局。

然而，全球之间存在日益扩大的数字鸿沟，许多世界海关组织成员缺乏充分利用人工智能/机器学习技术所需的技术能力或基础设施。弥合这一数字差距对于确保所有海关管理机构，无论其当前技术能力如何，都能采用这些强大工具以现代化其操作，并有效应对新兴全球挑战至关重要。

3 海关和贸易中的AI/ML趋势

3.1 先进的AI模型

先进的人工智能模型正在通过数据驱动学习和模式识别增强风险评估、欺诈检测和货物检查，从而改造。这些模型包括生成对抗网络（GAN）和变分自编码器（VAE）[7]用于分析模式并生成真实的数据，支持文档验证、异常检测和预测分析。

大型语言模型 (大语言模型)，如GPT-4和LLaMA，利用变换器架构处理自然语言，使其非常适合自动文件分类、处理海关申报和回应询问。这些模型可以从非结构化数据中提取见解，协助风险分析并简化合规检查。此外，基于深度学习的人工智能驱动图像识别系统，通过识别隐藏物品和X光及扫描数据中的异常来改善货物扫描。

受益于减少处理时间、增强合规性和改善对非法活动的检测。在海关中使用深度学习和强化learning[8] 不仅加速了操作工作流程，还可以为政策制定提供基于数据的基础，使海关管理机构能够更有效地适应不断变化的贸易动态和新兴威胁。

随着人工智能模型的不断发展，预计它们将与包括物联网传感器、基于区块链的贸易记录、机器人流程自动化（RPA）、增强现实（AR）和虚拟现实（VR）在内的广泛技术集成，从而实现更强大、透明和高效的海关操作。

3.2 生成式人工智能在海关业务中的作用

自2022年出现以来，生成式人工智能在海关业务中引入了变革性的能力。利用海关管理系统和单一窗口平台的大数据集，各成员海关可以通过适应开源的大语言模型建立自己的基础大语言模型，例如LLaMA，9并使用海关特定数据对它们进行培训，包括贸易法规、关税代码、申报表和历史合规记录。通过利用自然语言处理和上下文感知学习的能力，这些基于海量海关相关数据训练的基础大语言模型可以支持复杂任务，如文档分类、风险画像、欺诈检测和政策执行。它们还可以分析非结构化数据，识别模式并生成见解，以改善目标策略和边境安全措施。此外，生成能力使大语言模型能够解读贸易法规并协助情景规划，增强战略规划，提升整体效率。通过有效利用自身数据与开源大语言模型模型，海关管理部门可以充分释放生成式人工智能的潜力。

---

[7] 生成对抗网络（GAN）：由两部分组成的人工智能模型——一个生成数据，另一个检查数据是否真实。两者协同工作，生成逼真的输出，如图像、视频或文本。变分自编码器（VAE）：学习数据中模式的人工智能模型，并基于这些模式创建新的、相似的示例。它们可以通过从学习到的模式中抽样生成与原始数据相似的新数据样本。

[8] 强化学习是通过试错学习，通过反馈最大化奖励。

[9] LLaMA（大型语言模型Meta AI）——由Meta开发的开源大语言模型，旨在用于研究目的。

3.3 海关操作中的（HITL）方法

尽管先进的人工智能/机器学习模型和生成式人工智能对海关业务提供了显著的好处，但一个重要的趋势是采用（HITL）的方法。这确保人工智能系统提供辅助，而不是取代人类决策。HITL涉及在人工智能的决策过程中进行人工监督，使海关官员可以审查并验证人工智能建议，在自动化和人类专业知识之间提供平衡。

3.3.1 确保问责和合规性

人工智能输出结果的验证： 海关官员可以审查人工智能生成的见解，以确保决策符合法律和监管标准。虽然人类验证有助于维护合规性，但应支持有力的完整性政策，以降低偏见或腐败的风险，并维护海关业务的透明度。

情境理解： 人类提供人工智能模型可能未能完全理解的上下文，例如地缘政治因素、文化差异或影响贸易实践的特殊情况。这确保了决策是合适的，并考虑到所有相关因素。

3.3.2 增强信任和透明度

建立对人工智能系统的信任： **引入“人类在环”机制有助于增强利益相关方对AI系统的信任**，因为决策不是完全由自动化系统做出的，而是融入了人类的判断，从而为整个流程带来一定程度的保障感。然而，必须建立诚信和透明度保障措施，以确保公正和无偏见的决策。

决策过程的透明性： 仅基于人工智能的决策可能缺乏透明度，因为像神经网络这样的复杂模型常被视为“黑箱”，使得追踪输入如何导致输出变得困难。没有明确的解释，特别是在需要问责的法律和合规环境中，证明决策变得具有挑战性。HITL允许解释决策是如何做出的，这对于透明度和问责制至关重要。海关官员可以为采取的行动提供理由说明，这在法律和合规环境中至关重要。

3.3.3 管理伦理和法律问题

防止偏见和歧视： 人工监督有助于识别和缓解人工智能模型中的偏见，确保对所有贸易方受到公平的对待，以及遵守反歧视法律。这一点尤为重要，因为许多AI模型是基于可能带有历史偏见的数据进行训练的**法律责任：** 人工智能系统作为决策辅助工具运行。决策的最终责任仍然在于人类官员，他们依法对决策结果负责。然而，AI驱动决策中的法律责任问题仍然是一个未解的问题，这突显出需要明确的法律框架，来应对AI系统不断发展的问责制。

3.3.4 适应动态环境

处理不可预测的场景： 人类更擅长应对AI模型未曾训练过的突发事件或异常情况。在全球突发事件影响贸易的情景下人类判断至关重要。

持续改进： 海关官员的反馈可以用于重新训练和改进AI模型。这个迭代过程随着时间的推移提高了AI系统的性能，使其更有效和可靠。

3.3.5 高效与专业之间的平衡

优化工作流程：HITI让AI系统处理例行任务，从而使海关官员能够专注于需要人类判断的复杂案件。这优化了人力资源的使用，提高了整体效率。

利用经验： 有经验的官员可以运用他们的专业知识来解释AI生成的数据，从而导致更细致有效的决策。他们的见解还可以指导更好的AI模型的开发。

3.4 基于云的人工智能在海关操作中的应用

基于云的AI提供通过互联网在远程服务器上托管的服务，为AI应用提供可扩展的处理能力和数据存储。这一趋势已经显现，越来越多的组织采用云平台来开发、部署和扩展AI解决方案。这种转变是由成本效率驱动的，按需付费的定价模式消除了对硬件和维护的大量前期投资的需求，降低了整体运营成本。基于云的AI平台能够快速部署AI项目、高效扩展AI/ML操作，并处理大型数据集，而无需大量本地基础设施。

可以根据数据敏感性和安全要求选择*私人云*模型，以获得更大的控制和安全性或*混合云*[10] 模型，以平衡可扩展性与数据保护。这些灵活的选项确保了可访问、可扩展和具有成本效益的解决方案，同时解决了数据安全和合规性问题。

3.4.1 解决数据安全问题

云服务提供商使用强有力的保护措施来满足的数据安全需求。一个重要的概念是*数据驻留*，这允许组织决定其数据物理存储在哪个国家或地区。这帮助他们遵循数据主权规则——适用于数据的法律，基于数据存储的国家。

海关管理机构可以选择私人云或混合云，以更好地控制敏感信息。这些选择使海关管理机构能够决定其数据存储和处理的位置和方式，确保他们遵守当地法规并保持数据安全。

主要云平台也遵循严格的国际安全标准。[11] 他们使用先进的方法，如加密、多因素身份验证和基于角色的访问控制，以确保数据保持安全，并且只有授权用户可以访问。

---

[10] 私人云是一个专门为单一组织提供的云计算环境，可以托管在本地或由第三方提供商提供，且不与其他客户共享。混合云结合了私有云和公共云资源，允许组织在安全的私有环境中保存数据，同时利用公共云的可扩展性和灵活性来处理不太敏感的工作负载。

[11] 这些包括：ISO/IEC 27017，提供适用于云服务的信息安全控制指南；以及SOC（服务组织控制）2：一种基于美国的标准，详细说明服务提供商如何安全管理客户数据，通常也在国际上采用。

4 采用AI/ML的法律要求

4.1 国家对AI监管的不同方法

世界各国政府正在采用多种策略来监管AI，反映出法律传统、政策优先级和技术进步水平的差异。这些方法可以大致分为正式立法、治理框架和指南，以及结合两者元素的混合模式。

4.1.1 正式立法

一些国家正在制定特定法律来规范人工智能，为开发人员、用户和其他利益相关者设立具有法律约束力的义务。欧盟（EU）以其《欧洲人工智能法案》（AI Act）为例，这项法案于2024年8月1日正式生效。[12]这一综合法律框架旨在根据风险水平将AI系统分类为不可接受、高风险、有限和最低风险，并为每个类别规定具体义务。例如，高风险AI应用，可能包括用于风险评估或欺诈检测的海关相关系统，将受到严格要求，例如合规评估、透明度要求和人类监督条款。其目标是确保人工智能系统是安全的，尊重基本权利，并在欧盟成员国之间促进信任。

同样，中国已经建立了一个多层次的人工智能监管框架，包括法律和具有约束力的规定，例如其《生成性人工智能服务暂行管理措施》，自2023年8月15日起生效，[13] 以及《基于互联网的信息服务推荐算法管理规定》（2021）。[14] 中国的监管方法旨在根据利益和安全关注来控制人工智能的发展，同时在创新与国家安全、伦理关注和社会价值之间保持平衡。

4.1.2 治理框架和指南

其他国家更倾向于通过非强制性指南或框架来引导人工智能负责任发展，而不是施加严格的法律限制。例如，美国采用了特定行业的灵活方法，强调创新。在2020年，白宫发布了关于规范人工智能的原则，重点关注公众信任、透明度和公平性。[15]美国国家标准与技术研究院（NIST）提供自愿性指导，以促进可信的人工智能。其目标是促进人工智能创新，同时解决风险，不以严格规章制约技术进步。

日本发布了伦理指南，而不是正式法律，旨在促进创新，同时确保负责任的人工智能发展和部署。日本政府在“以人为本的人工智能社会原则”中发布了一套关于人工智能的伦理指南，为负责任的人工智能开发和使用提供原则。[16] 这些指南涵盖多个方面，包括公平、透明、问责和隐私。政府还发布了跨部门的人工智能指南，概述了不同部门和机构在促进人工智能发展和应对潜在风险中的角色和责任。

---

[12] 欧洲委员会。(2024)。人工智能的监管框架。塑造欧洲的数字未来。

[13] 中国网络空间管理局。(2023)。生成性人工智能服务管理措施。

[14] 中国网络空间管理局。(2022)。互联网信息服务推荐算法的管理规定（第9号令）。

[15] 白宫 - 管理和预算办公室（2020）。人工智能应用的监管指导。

[16] 日本政府。(2019)。以人为本的人工智能社会原则。

新加坡采取了一种轻度干预，积极主动的人工智能治理和监管方法，引入了《模型人工智能治理框架》。[17] 该框架为组织在开发和部署人工智能系统时提供自主指导，提供关于内部治理、风险管理和利益相关者沟通的实用指导。同时还成立了人工智能伦理咨询委员会，以提供持续指导并促进伦理人工智能。其目标是建立公众信任，鼓励负责任的人工智能创新。

澳大利亚发布了“人工智能伦理框架”，包含八项原则，包括隐私保护、可靠性、透明度和问责制。[18] 该框架为企业提供了指导，以道德的方式实施人工智能，确保技术的负责任开发并与社会价值观相一致。

4.1.3 混合方法

一些国家结合了正式立法的元素与灵活的指南，根据特定情况量身定制监管。加拿大的人工智能治理方法是采用了混合模式，使用强制性政策和自愿框架的组合。人工智能和数据法案（AIDA）[19] 为监管人工智能系统提供了法律框架，而伦理指南和自愿框架，如算法影响评估工具，提供了组织负责任开发和使用人工智能的指导。这种混合方法使加拿大能够平衡法律确定性的需求与适应快速发展的人工智能领域的灵活性。

英国采用了一种特定行业的混合监管，由总体指南支持。[20] 它侧重于安全、透明度和公平等原则，由现有监管机构而不是新立法实施。英国政府发布了国家人工智能战略，概述了其对人工智能发展的愿景，并制定了负责任人工智能的原则，以及人工智能伦理框架，为人工智能开发和使用的伦理考虑提供指导。

4.2 国际调节AI的努力

国际合作正在增加，联合国（UN）和经济合作与发展组织（OECD）宣布加强人工智能治理方面的合作。OECD在2019年采纳了人工智能原则（在2024年更新），[21] 这是一套旨在促进可信和负责任的人工智能开发和使用的指导方针。七国集团（G7）和二十国集团（G20）也提出了关键建议，以指导人工智能的负责任开发和部署。七国集团的人工智能建议包括11项关于安全和可信赖性的指导原则，以及促进伦理和负责任人工智能开发的自愿行为准则。[22] 此外，二十国集团针对人工智能治理提供了关键指导，倡导对可信赖的人工智能进行负责任的管理，并鼓励成员国制定反映各自优先事项和关注的国家人工智能战略。[23]

在2024年3月，联合国大会通过了一项关于“把握安全、可靠和可信赖人工智能的机遇”的决议，强调伦理人工智能原则和遵循国际人权

---

[17] 人工智能验证基金会（AIVF）和信息通信媒体发展局（IMDA）（2024年）。生成性人工智能的*模型人工智能治理框架*。

[18] 澳大利亚政府，工业、科学、能源和资源部。(2019)。澳大利亚的人工智能伦理框架。

[19] 加拿大政府（2022年）。*人工智能和数据法案（“AIDA”）*

[20] 英国政府，数字、文化、媒体与体育部。(2022)。建立支持创新的人工智能监管方法：对英国新兴方法的概述。

[21] 经合组织。(2024)。塑造以人为本的人工智能方法：经合组织人工智能原则。

[22] 七国集团。(2023)。关于人工智能的国际指导原则和高级人工智能系统的行为准则。

[23] 二十国集团。(2019)。二十国集团人工智能原则。在二十国集团部长级声明关于贸易与数字经济的附录中。

法律。24此外，在2021年，联合国教科文组织通过了人工智能伦理建议，承诺所有193个联合国会员国遵循人工智能开发的伦理原则。[25]

4.3 对海关管理的影响

在全球范围内，各国政府正努力在规范人工智能的同时保护社会价值以免阻碍技术进步。正式立法提供了明确、可执行的规则和法律确定性，但其可能较为僵化，可能抑制创新，并可能缓慢适应技术变化。治理框架则更具有灵活性，鼓励创新，并可以快速更新，但其非约束性的特性可能导致不一致的采用和执行。混合方法在特定领域内平衡监管监督与灵活性，但可能会在合规性中产生复杂性，并导致法规与指南之间的潜在重叠。

随着人工智能法律和治理框架的不断发展，面临确保合规的复杂挑战，同时保持对新发展的适应能力。对人工智能监管的多样化全球方法突显出海关管理机构在采用人工智能/机器学习技术时保持警惕和主动的重要性。

为了在遵循相关法律和指南的情况下负责任地应对这一复杂局势，必须保持对这些多样化监管方法和持续变化的知情。这涉及监测现有法律、拟议立法和国家及国际组织发布的指南。通过了解不同的监管模式，海关机构可以更好地为人工智能在其运营中的可信和道德整合做好准备。

主动的方法意味着将法律义务与道德最佳实践相结合，无论所处的具体监管环境如何。海关管理机构可以从在人工智能监管较为先进的地区采用的最佳实践中受益，即使他们自己的管辖区缺乏具体的人工智能监管。这一策略使他们能够有效利用人工智能的好处，同时维护高标准的法律和道德。关键考虑因素包括严格遵守其管辖区的法律、深思熟虑地采用国际最佳实践以及在新法规出现时调整策略的灵活性。

通过采纳各种监管模型的最佳实践，确保遵守适用法律，并随时准备根据监管变化调整策略，海关管理机构可以有效利用人工智能技术。这种方法不仅提高了操作效率和效果，还维持了公众信任，并支持当局的使命，即促进合法贸易，同时确保安全和遵守国际规范。

4.4 数据加密、匿名化和同意管理

在采用人工智能和机器学习技术时，保护个人和敏感数据至关重要。实施强有力的技术措施对于减轻与数据处理相关的风险至关重要。这包括以下内容：

- 数据加密 – 在数据传输过程中（传输加密）以及数据储存时（静态加密）使用强加密协议至关重要，以防止在遭到拦截或泄露时被未经授权访问。为了应对不断演变的网络安全威胁，定期更新加密方式也是关键举措。
- 匿名化和伪匿名化 - 这些是增强数据隐私的额外策略。匿名化涉及以一种方式处理数据，以使个体无法被识别。

---

[24] 联合国。(2024)。为人类治理人工智能：最终报告。人工智能高级咨询机构。

[25] 联合国教科文组织。(2024)。关于人工智能伦理的建议。

当数据完全匿名化时，通常不再属于许多数据保护法规的范围，从而可能减少合规负担。而伪匿名化则是将识别信息替换为伪名，允许进行数据分析，同时提供更高的隐私保护。需要注意的是，根据《通用数据保护条例》，伪匿名化数据仍被视为个人数据，必须相应处理。

- 同意管理 - 这是数据保护的另一个关键方面。对于构，数据处理通常基于法律义务而非用户同意。然而，在自愿旅行者计划或自愿披露计划等可选项目中，需要获得当事人的同意。在这些情况下，同意必须是自愿的、具体的、知情的且明确无误。保持获得同意的记录，并在适用情况下提供便捷的撤回机制。
- 算法透明性和公平性 - 这些在实施人工智能/机器学习系统时是重要考虑因素。努力使人工智能/机器学习决策易于理解可以增强信任，并符合《通用数据保护条例》等法规中规定的透明度要求。尽管复杂的算法可能不透明，但为决策提供解释至关重要。此外，确保人工智能/机器学习模型不助长歧视至关重要。定期对模型进行测试和验证是必要的，以检测和纠正可能对个人或群体的决策产生不利影响的偏见。
- 数据治理和安全 - 这一方面必须优先考虑，以保护敏感信息。实施严格的访问控制将数据访问限制在需要的授权人员范围内，采用认证和授权机制。保持对数据处理活动的详细审计记录对监控未经授权的访问和促进审核很重要。

4.5 数据使用合规和知识产权（IPR）合规

当采用人工智能/机器学习技术时，确保遵守数据使用法规和知识产权（IPR）至关重要。在处理作为商人法律义务一部分提供的敏感贸易信息时，这一点尤为重要。数据使用合规的关键考虑因素包括以下几点：

- 法律依据：确保将交易数据用于人工智能/机器学习时符合其收集时的法律依据，不超过原始目的的范围。
- 保密性：在使用交易数据进行人工智能/机器学习时，实施强有力的措施以防止敏感信息的未经授权访问或披露。
- 数据保护：通过在人工智能/机器学习训练前对交易数据进行匿名化或聚合以减轻隐私风险，确保有效的技术以防止重新识别。
- 第三方参与：当外部供应商参与时，确保数据共享遵守数据保护义务，通过适当的合同条款。
- 国际合规：遵守国际贸易协议和有关贸易数据使用和保护的公约中的规定。

关于知识产权合规，海关管理部门必须：

- 尊重现有权利：确保其项目中使用的人工智能模型、算法或软件遵守现有的知识产权法律。

- 适当的许可：获得人工智能工具的适当许可，确保不在未授权的情况下使用专有技术。
- 保护自身知识产权：如果开发定制人工智能解决方案，保护其知识产权，防止未经授权的使用或复制。

通过严格管理数据使用，实施强有力的保护措施，并遵守数据和知识产权的法律和伦理标准，海关管理部门可以有效利用人工智能/机器学习技术，同时维护贸易社区的信任与合作。这种方法确保敏感贸易信息得到负责任的处理，并在整个人工智能/机器学习采用过程中尊重所有知识产权。

4.6 网络安全法规

人工智能/机器学习的采用带来了新的脆弱性，增加了系统复杂性，并使面临潜在的网络威胁。这些新的脆弱性和风险必须得到管理，以保护敏感数据，确保系统的完整性，并维持公众信任。遵守网络安全法规对于防范可能危害国家安全、干扰贸易或泄露机密信息的威胁至关重要。

因此，与法律要求相一致的强有力的网络安全框架是必不可少的。这包括：

- 遵守相关的网络安全法规 - 须遵守国家和国际层面的一系列网络安全法律和法规。这些法规旨在保护信息系统，确保数据隐私，防止未经授权的访问或网络攻击。
- 国际标准和指南 - 遵循国际公认的网络安全标准，如ISO/IEC 27001，提供了一种结构化的信息安全管理方法。遵循这些标准有助于组织实施最佳实践，并证明其符合国际期望。
- 全面风险管理 - 海关管理机构必须进行全面的风险评估，以识别和评估对其AI/ML系统及其处理的数据的潜在威胁。这涉及分析各种网络威胁的可能性和影响，包括数据泄露、未经授权的访问和专门针对AI算法的网络攻击。
- 高级访问控制 - 访问控制机制在保护敏感数据和关键的AI/ML系统中至关重要。海关管理机构应在传统的基于密码的系统之外增强安全性，例如，多因素认证。应采用基于角色的访问控制（RBAC），以根据个人在AI程序中的角色限制访问。
- 持续监测和威胁情报 - 为了监测网络威胁的动态性质，海关管理机构可以将先进的监测工具与传统安全措施和人类专业知识结合起来。定期安全审核、威胁狩猎和手动审核应补充自动检测系统。

5 AI/ML采用的政策安排

在海关业务中采用AI/ML技术需要精心设计的政策安排，以规范这些技术的集成、管理和利用。这些政策不仅将指导AI/ML系统的负责任使用，还会支持与组织目标的战略对齐，并确保融入更广泛的企业数字化战略。这些政策还必须解决法律要求和伦理标准，并维护强有力的安全措施。通过建立全面的政策框架，海关管理机构可以充分利用AI/ML技术的潜力，同时降低相关风险，确保其运营中的负责任创新。

本节概述了海关中AI/ML采纳的主要政策安排，考虑到上一节中已经涵盖的更广泛的法律要求，包括数据保护和隐私、数据使用和网络安全法规。

海关法律团队和监管顾问在制定政策方面发挥着重要作用，这些政策涉及AI/ML系统与这些要求的互动，特别是在数据使用、算法透明性和隐私考虑方面。确保AI/ML系统在法律约束内运行对其在海关操作中的安全和合法实施至关重要。

这些政策安排应涵盖治理、伦理使用、数据管理、系统设计和部署、能力建设、监管对齐和持续改进。

5.1 内部政策

AI/ML采纳的**治理**和监督 - AI/ML采纳的基础步骤之一是建立强大的治理和监督结构。治理政策还涉及角色和责任的划分，确保对AI/ML使用以及处理任何错误、偏见或伦理违规行为的清晰问责。这包括建立由高级海关官员、数据科学家、IT人员、法律顾问和政策专家组成的监督委员会或工作组，以监督AI/ML项目，确保与海关业务的战略对齐和遵守更广泛的法律框架。这种治理确保所有决定都是透明做出的，风险是主动管理的，政策随着技术和操作变化而更新。

数据管理和安全政策 - 数据管理政策在AI/ML采纳中至关重要，以规范数据的收集、质量、隐私和安全。这些政策还必须解决数据如何在海关部门、其他政府机构和外部合作伙伴之间共享，以促进互操作性并推动AI/ML采纳的综合方法。

与此同时，数据隐私政策对于保护敏感的贸易、商业和个人数据至关重要。政策必须与数据保护法规保持一致，例如保护数据免受未经授权的访问和滥用，确保数据收集和处理的同意，并对个人信息进行匿名化。安全政策提供了数据加密、安全存储和访问控制的指南，以减轻数据泄露和网络攻击的风险。这些政策共同帮助海关管理机构负责任地管理AI/ML操作所需的大量数据，同时遵守现有的数据保护和隐私法规。

系统设计、开发和部署政策 - 要制定指导AI/ML系统设计、开发和部署的政策。这些政策应设定模型验证、准确性和适用性的明确标准，以确保设计和开发有效支持海关职能，如欺诈检测、风险评估和贸易便利化。部署政策确保AI/ML系统以系统化方式实施，包括变更管理、用户培训和系统与现有工作流程整合的指南。这些政策还应解决对网络安全法规的遵从，确保系统能够抵御威胁和脆弱性。

AI/ML的**内部**能力和技能 - 为确保成功采纳AI/ML，需要投资于内部能力和必要技能。政策应支持海关官员的全面培训计划，重点关注AI/ML原则、数据分析和系统使用。除了培训外，海关管理机构可以与学术机构、研究组织和私营部门专家促进合作，以促进知识交流并获取最新的AI/ML发展。

政策**对齐 -** 内部AI政策必须与外部法律和监管要求保持一致，以确保合规和负责任的采纳。政策应设计为遵循现有的数据保护、隐私、知识产权和网络安全法律框架，正如此前详细讨论的。这些内部政策确保AI/ML技术尊重法律界限、贸易法规和跨境合规要求。

纳入操作 - 最后，AI/ML采纳的政策安排必须解决这些技术如何被战略性地纳入海关业务。政策应概述AI/ML如何与海关业务流程、贸易便利化目标和国家经济战略对齐。制定AI/ML采纳的战略路线图使海关管理机构能够根据潜在影响、可扩展性和操作相关性优先考虑举措。这些路线图确保AI/ML技术不仅支持海关的当前需求，还为长期现代化、风险管理和全球贸易目标做出贡献。

总之，AI/ML采纳的政策安排涉及全面的方法，涵盖治理、伦理使用、数据管理、系统开发、能力建设、法律合规、持续监测和战略对齐。这些政策构成了负责任的AI/ML采纳的支柱，确保海关管理机构能够有效利用技术进步，同时遵循伦理标准、法律要求和操作目标。通过制定和完善这些政策安排，海关管理机构可以为充分利用AI/ML技术以实现更高效、透明和安全的贸易流程做好准备。

5.2 伦理框架和指南

将人工智能/人工智能技术纳入海关活动，如风险评估、锁定目标或欺诈检测，会引发道德考虑，必须通过健全的政策安排来解决。政策必须确保人工智能/人工智能的使用符合公平、透明和问责的原则。应制定人工智能/人工智能使用的道德准则，为如何部署这些技术、如何做出决策以及如何减轻偏见设定标准。

公平和公正——主要的道德考虑因素之一是确保人工智能/人工智能应用于海关业务的公平和公正。用于海关决策的算法，如风险分析或针对货物进行检查，有可能引入偏见，对某些贸易商、地理区域或产品类型产生不成比例的影响。因此，政策必须强制检测、评估和减轻AI/ML系统中的偏见。

透明度和可解释性——透明度对于建立对AI/ML系统的信任至关重要。政策必须强调可解释性，确保AI/ML决策过程可理解和可解释。在使用人工智能/人工智能工具进行风险评估、确定哪些货件进行检查并识别潜在的合规问题时，这一点尤为重要。透明度政策应解决人工智能/人工智能决策背后的基本原理，并清楚地记录和传达给利益相关者，提供对如何得出某些结论的见解。

人在回路决策——在关键决策过程中保持人的监督非常重要。促进“人在回路”方法的政策确保AI/ML输出由训练有素的海关官员审查和验证。策略应定义何时何地

人类回顾是必需的，即需要海关官员将其专业知识、判断和上下文理解应用于决策的过程，特别是在人工智能/人工智能系统的复杂或高风险场景中五月面临限制。

隐私和数据道德——在海关业务中使用人工智能/人工智能涉及处理大量数据，包括敏感的贸易信息。为了确保合乎道德的数据使用，政策必须强调隐私保护和数据道德，而不仅仅是遵守法律法规。政策应确保仅将相关数据用于AI/ML目的，尊重数据最小化和目的限制原则。此外，政策应提高数据使用的透明度，告知利益相关者收集了哪些数据、如何使用这些数据以及保护其信息的保护措施。

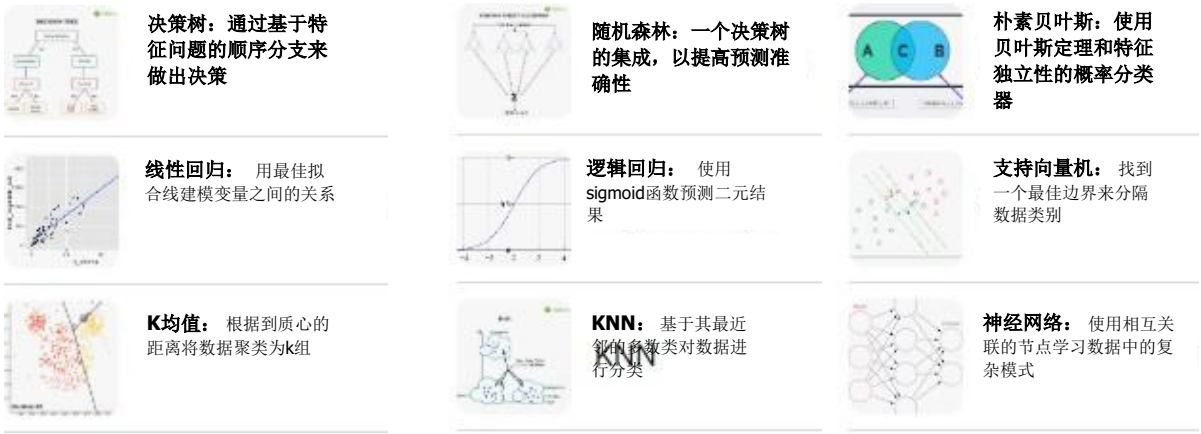
5.3 AI/ML模型中的偏见缓解

人工智能/人工智能模型中的偏见是海关管理部门的一个关键问题，因为它可能导致意想不到的后果，损害海关业务的公平性、准确性和信任。在海关业务中，有偏见的人工智能/人工智能模型可能会不成比例地将某些贸易商、国家或货物标记为高风险，导致不公平待遇、贸易壁垒和海关管理部门的潜在信誉损失。因此，减轻偏差对于AI/ML的道德和有效使用至关重要，需要有针对性的政策措施来识别、解决和监控整个模型生命周期中的潜在偏差。

了解偏见的来源——为了有效地减轻偏见，了解偏见的不同来源是很重要的。AI/ML模型中的偏差可能来自与数据相关的问题，例如用于训练的数据的历史不平衡、数据标签不正确或不完整以及无法捕捉海关业务中不同场景的非代表性抽样。例如，如果AI/ML模型主要根据来自特定出口市场或产品类型的数据进行训练，它可能开发误判风险水平的有偏见的模式。算法偏见也可能发生，如果模型的设计和特征选择本质上偏向某些结果或强化现有的偏见。例如，如果模型在风险评估中过度强调原产国，不公平地标记某些国家；或者特征选择优先考虑反映贸易关系中过时偏见的历史数据模式。对偏见缓解的政策考虑必须全面处理这些来源，确保数据和算法设计过程都得到仔细审查。

数据质量和代表性 - 缓解偏见的主要策略之一是提高数据质量，确保AI/ML模型的代表性。政策应强制执行数据收集协议，以捕获代表海关操作所有细分市场的多样化和平衡的数据集，包括不同类型的商品、贸易路线、商人和合规行为。这种多样性有助于防止模型发展出单方面的观点，五月对某些群体或活动产生不成比例的影响。政策还应强调数据清洗和验证，以消除错误、不一致和极端值，这些五月会扭曲模型学习并导致偏见预测。此外，指导方针应要求定期刷新和更新数据，以反映当前的贸易模式和行为，减少因过时信息引发的偏见风险。

图3 - 常见的机器学习算法



算法设计和公平政策 - 解决算法偏见需要仔细考虑AI/ML模型的设计、培训和验证过程。政策应在模型开发过程中强制实施公平性约束，确保算法不偏向某一群体、区域或贸易类型，除非有正当的操作理由。这可能涉及应用公平性学习技术，如特征的平衡加权、训练数据的重新采样，以及将公平性指标作为模型评估标准的一部分。例如，海关管理部门五月制定政策，要求AI/ML模型在不同的交易者配置文件或贸易通道中实现平衡的准确性，防止对特定实体的不成比例的标记或审查。政策还应概述算法在多种场景下的测试流程，以检测和纠正任何偏见，避免在部署前造成问题。

偏见的**定期**监测 - 偏见的缓解不是一次性努力，而是一个持续的过程，需要持续的监测和评估。政策必须建立定期审计AI/ML模型的框架，重点识别偏见迹象和模型结果中的意外差异。这些审计可以由内部团队或外部独立专家进行，以客观评估AI/ML预测是否符合公平原则和操作目标。监测政策应包括对模型输出的常规检查，以检测任何系统性的偏见决策模式，并在识别到这些偏见时要求及时的纠正措施。这些纠正措施可能涉及使用更具代表性的数据重新训练模型，调整算法以更好地平衡结果，或修订操作流程，以确保更公平地使用AI/ML决策。

透明性和问责机制 - AI/ML操作中的透明性对缓解偏见至关重要，以了解模型如何工作并识别潜在关注领域。政策应要求海关管理部门记录并传达AI/ML模型的设计、开发和部署过程，包括识别和缓解偏见所采取的步骤。这种透明性使得利益相关者，无论是内部员工、商人还是外部合作伙伴，都能提供反馈并使海关管理部门对公平结果负责。

总之，减轻人工智能/机器学习模型中的偏见是一项多方面的工作，需要制定针对数据质量、算法设计、透明度和持续监控的政策。通过实施这些政策，海关管理部门可以确保其人工智能/机器学习系统支持公正的决策，增强操作效率，维护利益相关者的信任。偏见缓解不仅维护伦理标准，还确保人工智能/机器学习技术与公正、平等和问责制的原则在海关操作中保持一致。

6 利益相关者的参与和沟通

有效地吸引利益相关者参与人工智能/机器学习项目对于海关管理部门至关重要，以确保这些技术得到有效采用，并满足所有相关方的需求和关注。利益相关者的参与应广泛而包容，涉及内部员工、外部合作伙伴、其他政府机构、行业协会、学术界和公众。参与过程旨在促进合作、获得反馈，并确保与总体目标的一致性，提高海关操作的效率、透明度和响应性。

内部员工参与 - 对于海关官员、IT团队和管理层等内部利益相关者，参与从能力建设举措和意识提升项目开始。海关管理部门可以举办培训课程和研讨会，教育内部员工关于人工智能/机器学习技术的潜力以及如何简化海关程序。在管理部门内部定期举行公开会议和跨部门论坛，使各方能够就关切、建议和实施人工智能/机器学习的实际考虑进行开放对话。在过程早期涉及员工可以建立归属感，并确保操作见解融入人工智能/机器学习解决方案中。由管理层、海关官员和IT人员组成的内部咨询小组可以就人工智能/机器学习项目的开发和部署提供持续反馈，营造让员工感到自己是贡献者而不仅仅是最终用户的环境。

外部合作伙伴参与 - 外部合作伙伴的参与对于海关操作中成功实施人工智能/机器学习至关重要。海关管理部门可以创建论坛和工作组，将进口商、出口商和物流公司等利益相关者聚集在一起，讨论人工智能/机器学习工具如何改善贸易流程。利益相关者圆桌会议和焦点小组允许合作伙伴表达操作挑战，确保在项目设计中考虑他们的需求。定期更新和咨询确保透明度并提供反馈机会。

与行业协会的互动提供了受海关操作影响的企业的集体声音。与行业参与的协作研讨会和试点项目可以导致更有效的人工智能/机器学习解决方案，量身定制以满足特定需求。这种方法由于获得了会员公司的预先认可，有助于实现更顺利的实施。通过促进开放对话和合作，海关管理部门可以开发有效的解决方案，主动应对挑战，并获得更广泛的支持，以推动其数字化转型工作。

与其他政府机构的互动 - 与其他政府机构（如边境安全、执法和监管机构）的合作对于确保人工智能/机器学习项目在政府职能中保持一致至关重要。海关管理部门可以建立跨机构工作组，讨论共同目标，识别不同机构的人工智能/机器学习项目之间的协同效应。这些工作组作为协调平台，避免重复努力，并确保无缝的数据共享，促进高效的跨机构流程。机构之间的谅解备忘录（MoU）可以概述特定的合作机制、角色和责任，以开发和实施支持国家安全和合规等更广泛政府目标的人工智能/机器学习（AI/ML）计划。

与学术界的**参与** - 包括大学和研究机构在内的学术界参与，对于将尖端研究和技术进步整合到 AI/ML 项目中具有重要价值。海关行政机构可以通过合作伙伴关系、研究资助或联合项目与学术机构合作，以利用 AI/ML 专业知识应用于海关领域，例如预测分析、风险评估和数据分析。通过与学术专家互动，海关行政机构可以了解 AI/ML 中的新兴趋势和最佳实践，并在解决问题时融入创新的方法。定期的学术研讨会或圆桌讨论可以确保持续的对话，

使学术界能够提供对 AI/ML 工具在海关操作中的有效性和伦理考虑的建设性反馈。

公众参与 - 对于公众利益相关者，透明和开放是关键。海关行政机构可以利用公众咨询、信息发布会和在线平台，向公众通报 AI/ML 计划，征求反馈并解决有关数据隐私、安全和整体影响的担忧。通过数字渠道分发的调查和问卷提供了一种有效收集公众意见的方式，确保 AI/ML 计划的实施与社会期望和监管标准相一致。公开对话，例如海关行政机构的公开会议或在线讨论论坛，使公众能够表达他们的观点，并澄清 AI/ML 将如何提高海关流程，同时保护公众利益。

6.1 反馈机制及其在规划和执行中的整合

为了有效收集和分析利益相关者的意见，海关行政机构应建立稳健的反馈机制，例如调查、焦点小组讨论、咨询委员会和持续监测系统。定期针对不同利益相关者群体（例如内部员工、外部合作伙伴和公众）的调查可以衡量对 AI/ML 计划的意识、看法和满意度。公众咨询提供了一个开放反馈的论坛，而由每个利益相关者群体代表组成的咨询委员会确保以结构化的方式收集意见。这些反馈机制使海关行政机构能够理解所有利益相关者的多样化需求和关注，促进知情决策。

从这些反馈机制中收集的意见应在项目规划和执行中认真考虑，确保其影响项目设计、部署和优化。该过程涉及分析反馈、根据影响和可行性优先考虑建议，并向利益相关者沟通他们的意见如何被纳入。对 AI/ML 项目的定期更新和透明报告可以促进信任，并证明正在认真对待利益相关者的关注。通过将这些反馈机制与利益相关者参与策略对齐，海关行政机构可以建立利益相关者的支持，促进顺利采纳并提高 AI/ML 计划的有效性。这种持续的参与和反馈循环不仅确保项目成功，而且促进长期的利益相关者合作和对未来技术进步的支持。

6.2 透明度和沟通

为了确保透明性并保持开放的沟通，向利益相关者和公众有效传达 AI/ML 项目的成果和成功故事至关重要。这种沟通建立了信任，鼓励了参与，并展示了这些技术为海关操作和贸易流程带来的价值。可以采用多种策略来接触不同的受众，同时突出AI/ML倡议的好处和成功。

成功案例和案例研究 - 发布详细的成功案例和案例研究可以有效地展示AI/ML项目的具体好处。这些案例研究应当突出具体面临的挑战，AI/ML解决方案是如何实施的，以及所取得的可测量改善，例如缩短清关时间、提高风险分析的准确性或增强贸易便利化。

利益相关者活动和研讨会 - 定期举办利益相关者活动，例如研讨会、论坛和简报，都是将AI/ML项目成果直接呈现给目标受众的重要平台，包括内部员工、行业合作伙伴和其他政府机构。这些活动促进双向沟通，不仅共享成功，还开放讨论，允许利益相关者提问并提供反馈。在这些活动中演示AI/ML工具的实际应用，提供了展示其功能和影响的机会。

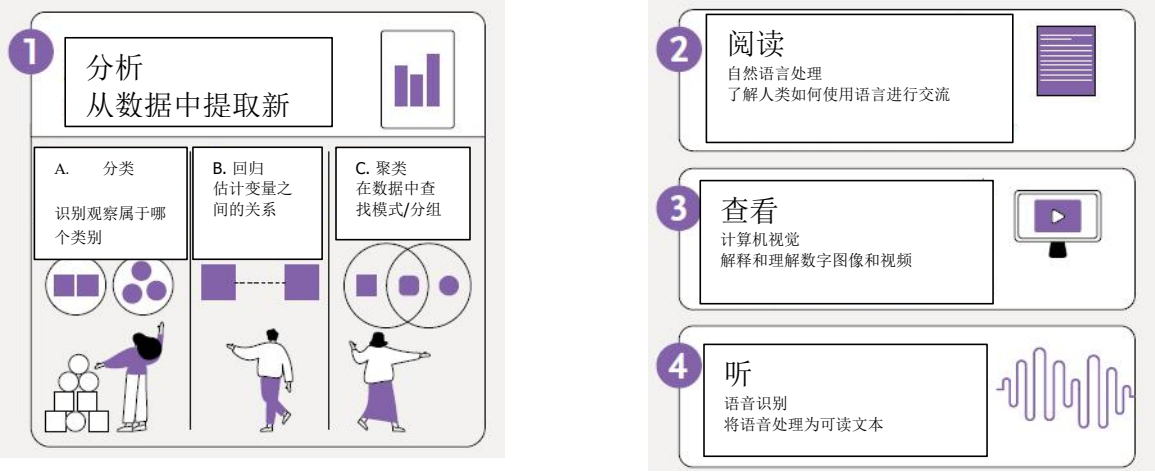
公众信息和社交媒体活动 - 发起针对公众的信息宣传活动和外展项目，可以增强透明度并帮助阐明用于海关的AI/ML技术。利用传统媒体（例如新闻稿、电视采访）和社交媒体平台（例如LinkedIn、Twitter和YouTube）可以广泛传播项目成就。这有助于接触广泛的受众并建立公众意识。利用社交媒体活动，通过帖子、信息图和视频以简单、有趣的方式传达复杂的AI/ML结果，鼓励公众互动。

会议和学术出版物 - 参与国际会议、行业活动和学术论坛，提供了与更广泛的受众分享最佳实践、经验教训和AI/ML项目成果的机会，包括其他海关管理机构、政策制定者和研究人员。在学术期刊或行业出版物上发表白皮书、研究论文和技术文档，可以将海关管理机构确立为采用AI/ML技术的领导者，并提供与学术和研究界更深入互动的平台。

7 在开展AI/ML项目时的关键考虑因素

下图描绘了AI/ML技术的一些关键能力。并非所有挑战都适合AI/ML解决方案；例如，涉及复杂贸易法规解释的高度细微问题可能仍然需要人类的监督。虽然AI/ML为提高海关运行提供了巨大潜力，但开展这些项目需要深思熟虑和战略性的方法。

图4 - AI/ML技术的关键能力26



基于前面章节讨论的法律、伦理和治理考量，本节重点关注海关管理机构在追求AI/ML倡议时应评估的实际因素。解决以下考虑因素确保AI/ML技术在海关操作中的成功实施和可持续整合：

7.1.1 问题定义和对齐

问题定义是确保项目针对正确问题并最大化AI/ML解决方案潜在好处的关键第一步。

应首先确定其流程中具体的痛点，如清关时间过长、检查不够高效或难以检测不合规活动。AI/ML技术尤其适用于需要处理大量数据的领域，或可以自动化的重复性、基于规则的任务，如文件处理、风险评估，以提高效率。

一个明确的问题，基于对人工智能/机器学习的优势和局限性的理解，对于成功实施能够为海关操作带来切实影响的人工智能/机器学习项目至关重要。

通过确保识别出的问题与人工智能/机器学习可以提供重大价值的领域相一致，海关管理当局可以避免在可能更有效地通过简单自动化或基于规则的系统解决的问题上投资复杂的技术。

---

[26] 新加坡政府技术局（2019），“公共部门人工智能手册”

7.1.2 数据的可用性和质量

数据的可用性和质量是在开展人工智能/机器学习项目时的重要考虑因素。海关管理机构作为其监管职责的一部分，收集大量数据，年均达到数TB级别。这包括结构化信息，如进出口申报、交易记录和关税分类，以及非结构化数据，包括扫描文档、沟通记录和来自检查的多媒体文件。此外，这些数据中大部分是历史数据和档案数据，提供了多年来甚至几十年积累的大量信息。

虽然人工智能/机器学习模型需要大量数据进行训练和验证，但这些倡议的成功不仅取决于数据的量，还取决于数据的质量和相关性。例如，为欺诈检测开发人工智能模型需要详细的历史贸易数据、交易记录和已知的欺诈活动模式。这些数据应当涵盖广泛的变量，例如产品分类、申报值、贸易路线和相关实体，使人工智能/机器学习模型能够学习复杂的模式并做出准确的预测。

然而，仅仅拥有大量数据是不够的；它还必须具有高质量，并与当前操作相关，以确保人工智能/机器学习模型产生有用和可操作的结果。低质量数据的特征是：不准确、不完整、存在不一致性或过时的信息，这会严重影响模型性能，导致错误的预测。高质量数据必须准确、完整、一致、及时和相关。达到这种质量水平对海关管理当局来说是具有挑战性的，特别是因为大量数据来自遗留系统或是档案数据，可能因人工输入、分类不一致或文档不完整而包含错误。此外，数据格式随时间的演变可能会导致记录信息的不一致，使得确保不同数据集之间的统一性变得困难。

为了解决这些问题必须投入时间和资源进行数据清理和准备。这一过程将涉及纠正错误、标准化格式，并确保数据是全面的和最新的，最终提高人工智能/机器学习模型输出的可靠性。本报告第9节关于数据管理，概述了在海关管理数据的基本步骤，作为启动人工智能/机器学习项目的基础前提。

7.1.3 技术可行性

在开展人工智能/机器学习项目时，的一个关键考虑因素是技术可行性。这涉及评估实施和成功推动人工智能/机器学习倡议所需的基础设施、专业知识和资源是否可用。这一评估的第一步是评估海关管理机构现有的技术专长。

人工智能/机器学习项目需要数据科学、机器学习和数据工程等专业技能，以及使用必要的硬件和软件工具的熟练程度。如果缺乏这些技能，海关管理当局可能需要投资于员工培训，或通过与技术供应商、顾问或学术机构的合作寻求外部专业知识。

除了专业知识，必要硬件的可用性，如能够处理大数据集的高性能计算系统，以及包括AI/ML框架在内的软件也是至关重要的。海关管理机构必须确保其基础设施能够支持大量数据的存储、处理和分析，以及AI/ML模型开发的迭代性质。

本报告第10节随后概述了实现和整合AI/ML所需的最低技术规格和人力资源。海关管理机构可以利用这些指导方针来评估其项目的技术可行性和支持AI/ML倡议的组织能力。这包括评估他们是否拥有必要的基础设施，

专业知识和资源，以有效实施AI/ML解决方案。通过参考这些规格，海关管理机构可以确定其当前能力是否符合AI/ML项目的需求，或者是否需要在培训、技术或外部合作方面进行投资。

7.1.4 AI输出挑战

AI产生的输出的准确性对海关管理机构至关重要。AI/ML模型并非完全中立；它们受其训练所用数据和开发方法的影响。一个重要的问题是数据的偏见风险，如前文所述。

另一个关键问题是AI/ML模型中出现的**幻觉和不准确性**。AI/ML系统有时会根据不完整或模糊的数据生成输出，导致“幻觉”现象，即模型提供不准确或误导的预测。在海关的背景下，这可能导致错误标记货物以进行检查或不当的风险评估。确保AI模型的准确性并将其预测与现实结果进行验证对于维持AI/ML基于决策的公平性和信任至关重要。下表提供了AI/ML模型中常见的偏见、幻觉和不准确性的示例。

表2 - 人工智能/机器学习模型中最常见的偏见、幻觉和不准确性

	问题类型	备品备件名称	海关操作中的示例
1	选择偏差	当训练数据未能代表全部海关场景时，会导致模型偏向特定案例。	一个主要基于高价值货物数据训练的人工智能模型可能会忽视与低价值货物相关的风险。
2	历史偏差	反映历史数据中的模式和偏见，可能加固过时的趋势和成见。	一个模型五月不成比例地标记来自某些国家的货物基于过时的风险数据。
3	算法偏差	源于模型设计，其中某些特征被过度强调，导致预测结果偏斜。	一个模型五月高估商品的价值，导致仅对高价值物品进行频繁检查。
4	风险检测中的假阳性	当模型错误地将货物标记为高风险时，导致不必要的检查。	一个无害的货物五月被标记为含有禁止物品，从而导致贸易延误。
5	风险检测中的假阴性	当模型未能识别实际高风险货物时，导致它们未被检测到。	一批非法货物可能被标记为“低风险”，未能引发适当的检查。
6	过拟合偏差	当模型过度训练于特定模式时，未能有效推广到新数据上。	一个专注于特定季节性数据的模型可能无法准确评估该背景之外的货物。
7	风险因素的幻觉	当人工智能虚构或夸大风险因素而没有事实基础时，导致不正确的评估。	一个模型可能根据毫无根据的相关性或假设将无害的货物标记为高风险。
8	数据漂移误解	当输入数据的变化未被识别时，导致不准确的预测或过时的风险 profile。	一个基于疫情前数据训练的人工智能模型五月未能适应疫情后贸易模式。

7.1.5 成本效益分析

在开展AI/ML倡议时，必须进行彻底的成本效益分析，以做出平衡即时财务考虑与长期战略目标的明智决定。该评估应考虑AI采用的长期战略价值，包括其可能转变操作模式和增强决策能力的潜力。

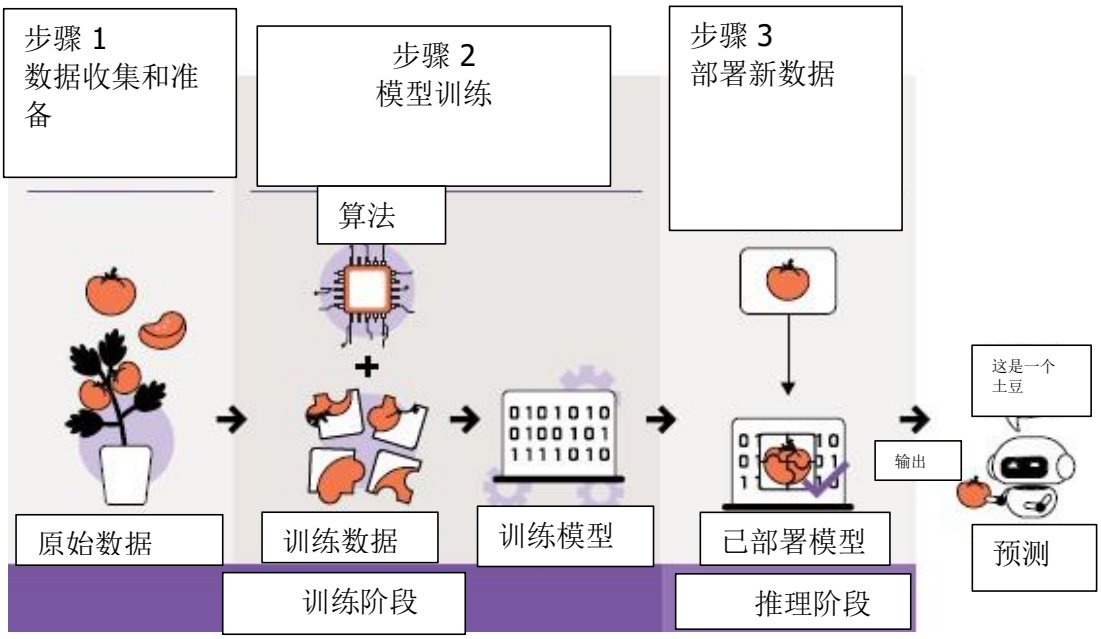
海关管理机构应评估与数据治理、基础设施升级和AI系统持续维护相关的隐性成本。

分析还应考虑AI通过改进欺诈检测和更高效的资源分配来开启新收入流的潜力。在可能的情况下，应量化无形收益，例如增强的利益相关者信任和改进的贸易便利化。海关应评估不采用AI的机会成本，特别是在全球贸易动态不断演变和新兴安全威胁的背景下。成本效益框架应足够灵活，以适应技术进步的快速步伐，允许在AI能力演变时进行迭代调整。

7.1.6 试点项目

在启动AI/ML项目时，海关管理机构应考虑开展试点项目，以在受控环境中测试AI/ML解决方案的可行性和有效性。试点项目使海关能够评估AI/ML模型的性能，收集反馈并在全面实施前进行调整。通过遵循结构化的三步方法，海关管理机构可以评估这些技术的实际收益和局限，同时降低风险。

图5 - 开发和部署人工智能试点系统的阶段[27]



该方法的第一步是**数据收集和准备**。海关管理部门应首先收集相关的培训数据，这些数据可能包括历史海关申报、交易记录或检查数据。这些数据需要经过仔细处理，例如去重、标准化格式和处理缺失值。此外，许多人工智能/机器学习项目需要标记数据，特别是对于监督学习，所需的结果需要清晰定义。标记可能耗时，但对于确保模型从准确和相关的示例中学习至关重要。一旦数据准备就绪，通常会将其分成三个部分：一个训练集用于开发模型，一个验证集用于微调模型，以及一个评估集用于测试最终性能。数据准备的进一步细节在以下关于数据管理的部分进行了详细说明。

[27] 新加坡政府技术局（2019），“公共部门人工智能手册”

第二步涉及模型训练，包括几个关键阶段。首先，必须选择最适合其问题的算法。这一决策受到数据性质和模型设计要解决的具体任务（例如分类、预测或异常检测）的指导。一旦选择了算法，训练过程就开始了，模型通过分析训练数据来学习执行任务。在这一阶段，模型会定期使用验证数据集进行验证，以调整参数并提高准确性。最后，模型会使用评估数据集进行评估，以确保其在未见数据上的表现良好，从而模拟真实世界条件。这一严格的过程确保模型可靠并为下一步做好准备。

第三步是**部署**，将训练好的模型引入海关管理部门的操作流程中。在此阶段，模型开始根据从训练过程中学习到的内容预测新的输入数据。由于这是一个试点项目，部署过程受到密切监控，模型的性能不断评估。这使得海关管理部门能够识别潜在的改进或调整，解决在更广泛实施之前的任何问题。在真实世界环境中对模型进行监控可以确保它继续提供有价值的洞察和预测，即使数据或环境可能发生变化。

8 数据管理

海关管理部门在日常操作中定期收集大量各种形式的数据——结构化、半结构化和非结构化数据。根据2018年世界海关组织（WCO）新闻文章的报道，即使在那时，韩国海关（KCS）每天也积累45 GB的结构化数据和30 GB的非结构化数据，[28] 每年累计超过25 TB，这一数字可能在今天显著更高。这些数据从结构化的海关申报和货物清单到半结构化数据，例如来自物联网（IoT）设备的电子数据交换（EDI）消息，以及扫描文档、X光影像和监控录像等非结构化格式。尽管这些数据丰富且数量庞大，但许多海关管理部门尚未充分利用其潜力来增强核心职能，例如收入征收和保护、贸易便利化和边境安全。

当前的挑战在于有效整合和分析这些多样化的数据，以提取可操作的洞察。传统的数据处理方法通常难以应对数据的庞大体量、多样性和复杂性，导致有价值的信息未被充分利用。这正是人工智能/机器学习技术为海关管理部门提供了利用和最大化其收集数据能力的工具。人工智能/机器学习可以自动分析结构化和半结构化数据，通过自然语言处理（NLP）和计算机视觉等技术从非结构化数据中提取洞察，并使得预测分析能够预测风险并简化流程。

数据管理是海关管理中人工智能/机器学习项目的基石，因为它确保收集和处理的数据既可靠又适合分析。在海关管理中，管理人工智能/机器学习应用的数据需要处理多种类型的结构化和非结构化数据，确保其质量和完整性，并防范隐私和安全威胁。在海关管理中，数据管理涉及将原始贸易数据转化为适合人工智能模型开发和处理的格式。

通过实施稳健的数据管理策略，海关管理可以利用人工智能/机器学习的力量提高操作效率，增强风险管理，并确保遵守法规。这些策略应纳入综合的数据治理框架，并利用先进的数据质量工具。

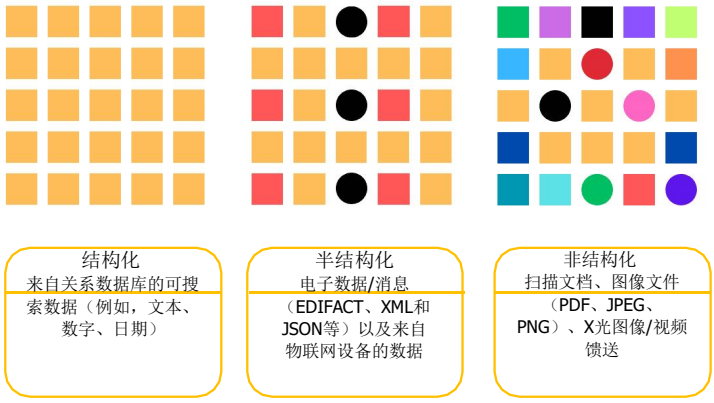
8.1 用于AI/ML项目的数据类型

结构化数据通常包括进出口申报、关税分类、交易记录和估值数据。这些数据集适合存入数据库，使其成为算法处理的理想选择。相比之下，非结构化数据，如扫描文档、图像、电子邮件和情报报告，需要更先进的处理技术，包括文本挖掘和图像识别，以提取有用的信息。

进一步扩展，海关管理还利用来自传感器、追踪系统和物联网设备的实时数据，以及来自以前交易和检查的历史数据。这些数据集作为训练人工智能模型的基础，帮助预测风险，优化物流和检测欺诈。

[28] WCO News 86。(六月2018)全景：‘快速货物和邮政物品的清关：韩国测试新的分析工具以根除欺诈’

图6 - 海关操作中的结构化、半结构化和非结构化数据



8.2 数据质量和完整性

数据质量和完整性对于人工智能/机器学习模型的有效性至关重要。，确保数据准确、完整、一致和最新至关重要。高质量数据使模型能够生成可靠的预测和决策，例如识别潜在的欺诈性装运或确定最佳检查时间表。

海关数据必须经历严格的预处理，包括清洗、验证和增强，以提高数据质量。这可能涉及错误检测和纠正，确保数据条目没有不一致和缺失。数据增强技术，如剪裁、缩放和对比度调整，有助于增加训练数据的数量和多样性，这在海关环境中尤其有益，因为变异性很高。

8.3 数据准备

数据准备是海关管理启动人工智能/机器学习项目的重要阶段，尤其考虑到他们管理的大量数据。人工智能/机器学习模型的高质量结果依赖于准备充分的数据，海关管理必须投入综合的数据清洗和准备，以确保项目的成功。下图提供了数据准备的步骤，其中包含几个将原始海关数据转化为适合人工智能/机器学习分析的关键步骤。

图7 - 数据准备的步骤

数据清洗 - 第一步是数据清洗，包括识别和修正数据中的不准确性、错误和不一致性。通常处理大量历史数据，这些数据可能包含误分类的商品、不一致的计量单位、缺失值或重复条目。例如，用于产品分类的协调制度随时间变化可能导致差异。解决这些不一致性对于确保一致的产品分类至关重要，这是任何试图评估贸易合规性、检测欺诈或优化检查流程的人工智能/机器学习模型的基本要求。

数据**规范化** - 在数据清洗之后，数据归一化确保来自不同来源的信息是一致的并且可比较。海关数据通常来自多种系统、区域或部门，导致格式、测量单位和货币值的差异。标准化日期、货币值和测量单位，例如将所有重量转换为公吨或标准化货币汇率，对于创建统一的数据集至关重要。归一化提高了分析的准确性，并允许AI/ML模型处理来自多个来源的数据，而不会因格式变化而引入偏差。

数据结构化 - 接下来，考虑到海关管理机构处理各种数据类型，包括半结构化数据（如XML/JSON格式的数据）和非结构化数据（如扫描文件），有必要对数据进行结构化，将数据转换为适合AI/ML分析的结构化格式。可以使用XML/JSON解析技术处理半结构化数据，而光学字符识别（OCR）可以将扫描文件转换为机器可读的文本。

数据标注 - 这是一个重要的步骤，特别是对于监督式机器学习，它需要历史记录被准确标注以预定义结果。在海关操作中，这可能意味着对历史数据进行标注，以指示特定货物是否符合规定或被标记为欺诈或不规则。这些标签允许AI/ML模型从过去的模式中学习，并根据新数据进行预测。例如，一个风险评估模型可能可以训练以预测特定货物是否可能存在不合规的情况，基于过去标记为“发现欺诈”或“符合规定”的数据。这个过程资源密集，但对于创建可以提供有价值洞察并改善海关操作的模型至关重要。

数据验证 - 最后，数据验证对于确保数据准确反映潜在现实至关重要。需要将其数据与外部来源进行交叉验证，如贸易数据库、行业报告和可信的第三方数据提供商，以验证数据的准确性和可靠性。例如，海关管理机构可以将贸易量和产品描述与全球贸易数据库进行验证，或咨询行业报告以确保用于AI/ML模型的数据既为最新又可信。数据验证有助于避免与不正确或过时的信息相关的风险，这可能导致预测或决策出现缺陷。

此外，数据集版本控制对于管理用于模型训练的数据集的生命周期至关重要。海关管理机构必须能够跟踪和管理其数据集的不同版本，确保使用最新和相关的数据进行AI/ML模型开发。

通过这些精心执行的步骤 - 数据清洗、规范化、结构化、标注和验证 - 海关管理机构可以确保其AI/ML模型建立在高质量数据的坚实基础上。

9 可扩展的 技术框架用于AI/ML实施/集成

本部分推荐的“可扩展技术框架”作为海关管理机构旨在将AI/ML纳入其操作工作流程的基础蓝图。它涵盖了开发、自动化、数据管理、模型训练、平台架构和基础设施、硬件和网络需求、机器学习操作（MLOps）以及数据集成工具等关键方面。它提供了一种灵活的方法，海关管理机构可以利用该方法建立一个可以随时间扩展的AI/ML环境，符合具有成本效益的采用策略，而不是强加一套固定的、可能令人生畏或昂贵的前期投入。

这些技术规格支持广泛的AI/ML应用和用例，并促进从原型到生产的模型开发流程。他们还结合了MLOps实践，以系统性管理整个机器学习生命周期。

9.1 AI/ML开发环境

9.1.1 AI/ML框架

AI/ML框架提供了构建、训练和部署机器学习模型的基础库和工具。支持如TensorFlow、PyTorch和R等流行框架，确保了多样性，使得可以开发从神经网络到统计模型的广泛机器学习任务。

TensorFlow、PyTorch和R是开源的机器学习框架。这意味着它们是免费提供的，任何人都可以修改和分发。这种开放性促成了它们在机器学习社区的广泛采用和受欢迎程度。它们最适合用于从基础数据分析到高级深度学习应用（如海关风险评估、预测分析和货物检查的图像识别）范围的项目。

规格：

- 支持TensorFlow（v2.x+）、PyTorch（v1.7+）和R（v4.x+），以及与Kubernetes的兼容性以便于部署；
- 针对常见机器学习任务预先安装的库（例如scikit-learn、Keras）。

支持TensorFlow和PyTorch通常是AI/ML平台的要求，因为它们提供以下功能：

社区和生态系统：这两个框架都有庞大而活跃的社区，这意味着开发者可以获得丰富的资源、教程和支持；

灵活性和多样性：TensorFlow和PyTorch是高度灵活和多样的框架，可以用于广泛的机器学习任务，从简单的线性回归到复杂的深度学习模型；

与其他工具的集成：这两个框架与其他流行的机器学习工具和库集成良好，使构建和部署AI应用程序变得更加简便。

虽然TensorFlow和PyTorch是最流行的两个框架，但也有其他可用的选择，包括：

- Keras：一个可以在TensorFlow或Theano之上使用的高级API；
- scikit-learn：一个包含多种算法和工具的Python机器学习库；
- JAX：一个用于加速机器学习研究的Python库，将NumPy的灵活性与自动微分的强大相结合。

除了开源框架外，还提供专有的机器学习平台。专有平台的例子包括：

- 亚马逊SageMaker：来自亚马逊网络服务的完全托管平台；
- Azure机器学习：来自微软的云平台
- 谷歌云AI平台：谷歌用于构建和部署AI应用程序的平台。

9.1.2 集成开发环境（IDE）

在许多AI/ML开发场景中，IDE可以在编写、调试和可视化代码方面提供价值。像Jupyter Notebook、PyCharm或Visual Studio Code这样的工具，通常为开发AI/ML模型提供交互式和用户友好的环境，允许快速实验和原型开发。这些非常适合需要迭代开发的项目，如模型原型制作、数据分析和研究与开发环境中的可视化工作。然而，IDE并非总是必需的，其使用取决于具体的项目需求、开发者的偏好和可用资源。在某些情况下，更简单的IDE或基于云的解决方案可能更合适，特别是对于快速脚本编写、资源受限的环境，或与遗留系统协作时

规格：

- IDE：Jupyter Notebook、PyCharm专业版或带有AI/ML扩展的Visual Studio Code；
- 简单的IDE：Thonny、Geany；
- 基于云的解决方案：Google Colab、Replit；
- 与版本控制和云存储的集成以便于协作。

9.1.3 版本控制

在协作式的AI/ML项目中，例如开发和维护海关分析系统或协作研究项目，多个团队成员需共同处理代码库。这类项目通常需要版本控制系统，这有助于实现协同开发、追踪代码变更，并在不同版本之间保持代码的完整性。将版本控制系统与集成开发环境（IDE）集成，可以实现多个开发者之间的无缝代码管理与协作。。

规格：

- Git支持与IDE的集成；
- 集中式代码库（例如 GitHub、GitLab、Bitbucket）用于团队协作。

9.2 自动化工具和框架

9.2.1 编排工具

如 Apache Airflow、Prefect 或 Luigi 这样的编排工可以自动化机器学习管道的工作流程，确保高效管理数据预处理、模型训练和评估等任务。这些工具对于涉及复杂多步骤管道的项目是必需的，例如用于海关数据处理的数据流水线自动化或自动化模型再训练系统。

规格：

- 支持 Apache Airflow（v2.x+）、Prefect 或 Luigi；
- 与云端和本地数据源的集成。

9.2.2 持续集成和持续部署（CI/CD）管道

需要频繁更新和部署的 AI/ML 项目，例如海关风险管理预测模型的持续改进，通常要求使用 CI/CD 工具，以实现机器学习模型的自动化测试、部署和监控。这确保了生产环境中模型的快速和可靠更新。

规格：

- 与 Jenkins、GitHub Actions 或 GitLab CI 的 CI/CD 集成；
- 自动化测试框架（例如 pytest、TensorFlow 模型分析）；
- 预构建模板和配置。

9.2.3 模板库

旨在加速 AI/ML 开发的项目，例如贸易数据分析或文档分类，将极大受益于预构建模板 - 这些模板本质上是常见 AI/ML 任务可重用代码的库，有助于减少开发时间。这些模板可以覆盖数据预处理、特征工程、模型训练和评估。

规格：

覆盖广泛的 AI/ML 任务，包括分类（例如文档分类）、回归（例如贸易数据分析）、自然语言处理、计算机视觉、时间序列分析；

提供 IDE 集成；

使模板能够快速定制和适应特定项目要求

各种任务的模板库（例如数据预处理、模型训练）。

9.2.4 配置管理

配置管理确保自动化供应，[29] 监控和管理基础设施资源，保持不同环境之间的一致性、可靠性和可扩展性。它可以提供统一的部署环境，例如在多个海关办公室部署 AI/ML 模型。可以高效管理基础设施变更，减少部署错误并维护合规性。

规格：

- 支持领先的配置管理工具和行业标准的自动化部署和基础设施管理工具；
- 预配置的脚本用于在开发和生产环境中设置 AI/ML 模型、API、数据库和网络；
- 支持与云平台和本地基础设施的混合部署/集成
- 与 Prometheus、Grafana 和 ELK 堆栈等工具的兼容性，以跟踪基础设施性能和安全合规性；
- 支持容器化环境：启用 Docker 和 Kubernetes 的编排，以便高效和可扩展的 AI 模型部署；
- 自愈机制：实现从故障的自动恢复，确保关键 AI 驱动的海关应用的高可用性。

9.3 数据管理和治理

9.3.1 数据湖

涉及大规模数据分析的项目，例如贸易量的预测建模或海关中的欺诈检测，通常要求一个数据湖作为集中式仓库，以存储和管理多样化的数据源，促进结构化和非结构化数据的无缝访问和集成，这对于全面的机器学习模型至关重要。

规格：

- 可扩展的数据湖基础设施（例如 Hadoop、AWS S3 数据湖）；

[29] 自动化供应是基础设施和资源的自配置，使用程序化方式。

- 支持多种数据类型（例如 JSON、Parquet、CSV）。

9.3.2 数据治理框架

处理敏感数据的项目，例如海关申报中的个人信息或贸易合规数据，必须建立数据治理框架，以确保数据安全、隐私和合规性。它包括管理 AI/ML 生命周期中数据完整性的政策和流程。

规格：

- 数据治理工具（例如 Apache Atlas、Collibra）；
- 遵守相关数据隐私法规。

9.3.3 数据质量工具

需要高质量数据输入的项目，如异常检测系统和海关估值的机器学习模型，需要数据质量工具，这些工具提供清理、验证和标准化数据的功能，以保持高数据完整性和准确性，这对可靠的AI/ML模型性能至关重要。

规格：

- 数据质量工具（例如Talend，Informatica）；
- 自动化数据验证和清理流程。

9.4 模型开发和训练

9.4.1 实验工具

交互式工具促进实验、快速原型制作和迭代模型开发，允许数据科学家快速探索不同的模型和参数。这些最适合用于研究和开发项目，例如开发新的海关欺诈检测算法或优化现有模型以提高性能。

规格：

- Jupyter Notebook（v6.x+），RStudio Server；
- 对笔记本中的GPU加速的支持。

9.4.2 超参数调优

需要模型优化的项目，如提高海关收入估算预测模型的准确性，也需要自动化的超参数调整技术，以通过有效地寻找机器学习算法的最佳参数来提升模型性能。

规格：

- 超参数调整库（例如Optuna，Hyperopt，Scikit-learn的GridSearchCV）；
- 与分布式训练框架的集成。

9.4.3 分布式训练

涉及大规模数据集的项目，如海关检查的图像识别或文件分析的自然语言处理，需要使用分布式训练框架，使模型训练能够在多个GPU或集群上扩展，显著减少大数据集的训练时间。

规格：

- 支持Horovod，TensorFlow的分布式策略；
- 多GPU和多节点训练能力。

9.5 平台架构和基础设施

9.5.1 部署选项

每种部署选项都有其理想的应用场景，具体取决于AI/ML项目的性质。对于需要对敏感数据进行严格控制的项目，本地部署是最佳选择云部署则适合大规模数据分析和需要灵活扩展的项目。混合云架构提供了一种平衡，同时兼顾本地控制与云扩展性，使其适用于复杂项目，如实时异常检测。在需要遵守政府安全和数据主权法规时，利用政府云平台至关重要。

9.5.2 本地部署

本地部署涉及在组织的数据中心内设置和管理所有计算资源、存储和软件。此选项提供对硬件、数据和安全措施的完全控制，这对涉及高度敏感数据或严格合规性要求的项目至关重要。

本地部署最适合涉及处理敏感海关数据的AI/ML项目，如欺诈检测、威胁评估和敏感文件处理，其中数据主权和遵守严格的安全法规至关重要。

规格：

- 配备高性能服务器的专用数据中心（最低16核CPU，256GB内存，多GPU支持）；
- 本地和网络存储解决方案（例如2TB NVMe SSD，10TB NAS）；
- 高速网络（例如Infiniband，10/40/100 Gbps以太网）；
- 强大的安全基础设施（例如防火墙、VPN、身份和访问管理）。

9.5.3 云部署

云部署使用外部云平台提供的服务，如AWS、Azure或谷歌云平台（GCP）。此选项提供可扩展性和灵活性，允许组织根据需求快速调整计算资源。它非常适合需要大规模数据处理、快速实验或跨多个地点协作的项目。

云部署最适合涉及大规模数据分析的AI/ML项目，例如预测分析或在大数据集上进行机器学习模型训练。云部署对需要灵活扩展资源的项目或涉及非敏感数据的项目特别有利。

规格：

- 云实例（例如 AWS EC2，Azure VMs）具有 CPU 优化（c5.4xlarge）和 GPU 优化（p3.8xlarge，p4d.24xlarge）选项；
- 可扩展的云存储（例如 Amazon S3，Azure Blob Storage）起始于 10 TB；
- 高级网络（最低 1 Gbps）；
- 云原生安全服务，包括加密、VPN 和 IAM。

9.5.4 混合云架构

混合云架构结合了本地基础设施和云服务，提供在本地和云中运行工作负载的灵活性。这种方法允许无缝的数据集成和工作负载迁移，实现控制、安全性与可扩展性的平衡。

混合云架构最适合需要在控制敏感数据和利用云资源进行可扩展处理之间取得平衡的 AI/ML 项目。这对于

海关管理局正在进行的实时异常检测等项目非常理想，其中敏感数据在本地处理，但大规模模型训练和数据分析可以从云资源中受益。

规格：

- 本地与云环境之间的安全高速连接（例如 VPN，Direct Connect）；
- 用于敏感数据的本地数据中心和用于可扩展处理的云资源；
- 用于集成工作负载编排的统一管理系统。

9.5.5 容器化

容器化涉及将 AI/ML 模型/应用程序及其依赖项打包到“容器”中。这种方法确保在不同环境中的一致性，并提供开发、测试和部署之间的无缝过渡，从而有助于快速部署 AI/ML 项目，使模型的迭代和测试更快。

规格：

- 使用 Docker 或类似平台打包 AI/ML 应用程序；
- 确保本地和云环境之间的兼容性；
- 容器的简化部署和可移植性。

9.5.6 容器编排 - Kubernetes集群

容器编排是自动化部署、扩展和管理容器化应用程序的过程，在本地、云、混合和政府云设置中部署 AI 应用程序中发挥了重要作用。编排管理和协调应用程序的各种组件。这种方法使组织能够根据其特定的可扩展性、安全性和资源优化需求选择最合适的部署选项。

涉及复杂工作流和大规模数据摄取的海关操作，如申报处理、HS 分类、估值和风险评估等，如果采用高效的编排将会受益。

Kubernetes 是一种广泛使用的开源容器编排平台。它为本地、云或混合环境中的 AI/ML 工作负载提供高效的编排，确保高可用性和资源优化。使用 GPU 支持的 Kubernetes 集群可以实现并行处理，并优化 AI/ML 任务的资源使用，确保高效的模型部署和扩展。它最适合那些需要频繁部署、扩展和管理复杂、容器化工作负载的 AI/ML 项目，例如为海关检查自动化和实时决策系统部署和维护机器学习模型。

规格：

- 支持 GPU 的 Kubernetes 集群（每个节点至少 4 个 GPU）；
- 用于工作流程管理的编排工具（例如 Apache Airflow，Argo）；
- 动态资源管理的自动扩展配置；
- 与 Helm 等工具的集成，实现简化部署，以及使用负载均衡器（例如 HAProxy，NGINX）进行流量分配。

9.5.7 负载均衡器

负载均衡器在海关操作中发挥着关键作用，例如用于分配即将到来的货物信息以及舱单和主舱单的申报，这些程序需要 AI/ML 驱动处理，通过 AI 驱动的引擎防止任何单一服务器变得过载从而导致瓶颈。通过实施负载均衡器，可以

确保这些关键操作需要高可用性和容错能力，保持高效和可靠，能够处理大量数据和请求，即使在高峰期或意外的交易活动激增期间。

规格：

- 软件负载均衡器（例如 HAProxy、NGINX）或云原生服务（例如 AWS 负载均衡）；
- 自动流量分配的配置，以维护服务的连续性。

9.5.8 安全性

安全性对所有海关系统至关重要，尤其是在整合 AI/ML 技术时。在海使用 AI/ML 引入了新的复杂性和潜在漏洞，这需要强大的安全措施。增加多层次的安全措施是必要的，以保护敏感数据并确保 AI 系统的完整性。

规格：

- 防火墙、VPN 和 IAM 以确保安全访问；
- 数据加密（在传输和静态状态下）；
- 遵循 ISO 27001 和 GDPR 等安全标准；
- 入侵检测系统用于实时威胁监测。

9.6 计算资源需求

在启动 AI/ML 项目时，一个均衡的设置应该支持基本模型训练inference[30] 和以可负担的成本进行实验。

9.6.1 中央处理单元（CPU）

中央处理单元（CPU）是 AI/ML 工作负载的支柱，处理核心处理任务。高性能 CPU 提供复杂操作所需的计算能力。这些实例为数据预处理和模型推理等操作提供可扩展、性价比高的处理能力，以及传统的 ML 算法和模型训练。

规格：

- 处理器类型：多核 x86 或针对计算密集型任务优化的 ARM 处理器；
- 核心数量：通常，基本工作负载为 2 到 8 个虚拟 CPU，并具有扩展更高要求应用的选项。

附加特性：

- 超线程/同时多线程（SMT）：为多线程工作负载启用更好的性能，常见于 AI/ML 任务；
- 缓存大小：最好有较大的 L3 缓存（例如 30MB 或更高），以加速处理期间的数据访问；
- 支持高级向量扩展（AVX）进行向量处理，这对 ML 计算非常有益。

9.6.2 内存

随机存取存储器（RAM）在处理期间对于临时数据存储至关重要。高容量 RAM 设置，例如 256 GB DDR4 或 DDR5 ECC（错误校正码）内存，支持大规模数据处理和密集的模型训练，而不会出现性能瓶颈。

---

[30] AI/ML 中的推理是使用训练好的模型对新数据进行预测或决策的过程，应用学习到的模式而无需重新训练模型。

规格：

- 容量：最少 256 GB RAM（随机存取存储器）；
- 类型：DDR4 或 DDR5；
- ECC（错误校正码）：推荐使用 ECC 内存以检测和修正数据损坏，确保关键 AI/ML 工作负载的更高可靠性和稳定性；
- 速度：对于 DDR4：通常为 2933 MHz 或更高/对于 DDR5：通常为 4800 MHz 或更高；
- 可扩展性：确保服务器主板支持内存扩展（例如，最多 512 GB 或更多），以满足未来对更高工作负载的扩展需求。

9.6.3 图形处理单元（GPU）

GPU 使优化的并行处理成为可能，使其对 ML 和 AI 任务至关重要。对于初始的 AI/ML 项目，选择性价比高但性能出色的 GPU 至关重要，以确保顺利的模型开发、训练和推理，而不产生不必要的费用。一个均衡的 GPU 应该提供足够的计算能力、内存带宽和效率，以处理入门级深度学习、计算机视觉和 NLP 任务。对于初学者友好的 AI/ML 设置，建议使用至少 8GB VRAM 和 3,500 个以上 CUDA 核心的 GPU，以在可负担性和性能之间实现平衡，同时支持训练、实验和推理。随着工作负载的增长，可以考虑更高端的 GPU 来扩展 AI 能力。

规格：

- CUDA 核心/张量核心[31]：至少 3,500 个以上的 CUDA 核心，以实现高效的并行计算。张量核心（如有）可增强深度学习加速；
- VRAM（GPU 内存）：8GB 到 12GB，以高效处理适中的批量大小和模型参数；
- 计算能力：7.5或更高，以确保与现代AI/ML框架的最佳兼容性；
- 内存带宽：至少300 GB/s，以处理大数据集传输和张量计算。

9.6.4 内存和存储

对于一个初始的AI/ML项目，选择合适的内存（RAM）和存储可以确保平稳的数据处理、模型训练和实验，而不会出现瓶颈。非易失性内存高速公路固态硬盘（NVMe SSDs）提供高速读写操作，这对快速数据访问要求的任务（如模型训练和实验）至关重要。它们确保快速访问大量数据，减少训练延迟。

规格：

- 内存（RAM）- 16GB RAM（最低），建议32GB以处理更大的数据集；
- 存储- 1TB NVMe SSD（最低），建议用于更快的数据访问和模型存储。

9.6.5 网络附加存储（NAS）/网络文件系统（NFS）

海关的AI/ML项目通常涉及大数据集，并且需要高速访问以实现高效的模型训练和推断。网络附加存储（NAS）或网络文件系统（NFS）提供集中式、可扩展的存储，可以通过网络访问。为了支持基本的AI/ML工作负载，最低的NAS/NFS设置应支持跨多个节点的并发读写操作，确保AI/ML任务的数据共享无缝进行。

规格：

- 最低10TB可扩展存储，以容纳数据集、模型检查点和日志；

[31] CUDA核心是GPU中的并行处理器，加速通用计算任务，而张量核心专门用于矩阵运算，提高AI/ML模型的深度学习性能。

- 支持网络文件系统（NFS）v3或v4以实现高性能的读写操作；
- 顺序读写速度：至少500MB/s，以避免模型训练中的瓶颈；
- 可扩展存储：支持额外的驱动器或云集成，以便未来扩展。

9.6.6 云存储

有两种主要类型的**云**存储解决方案，各自适用于不同的用例：云**对象存储**和云**块**存储。

云对象**存储**是存储大量非结构化数据集的最佳解决方案，包括图像、视频、日志和AI/ML模型工件。通过API访问，专门针对可扩展性、耐用性和成本效益而设计，适合管理多种数据类型和大规模存储需求。具有高耐用性和可用性，确保数据在大规模下的完整性和可访问性。常见用法包括存储训练数据集、模型检查点、日志和其他非结构化数据，使其特别适合批处理和离线训练工作流程。

规格：

- 从10 TB的基础容量开始，云对象存储提供几乎无限的扩展性，能够无缝适应不断增长的数据量。

相对而言，**云块存储**提供为结构化数据量身定制的高性能、低延迟存储。它作为虚拟硬盘直接附加到虚拟机（VMs），提供快速和频繁的数据访问，这是关键应用（如数据库、实时分析和事务系统）所必需的。设计用于速度和效率，它支持随机读写操作，并可以根据性能需求进行扩展或调整。

规格：

每个实例的起始容量为2 TB，云块存储非常适合对延迟敏感的工作负载，甚至最小的延迟也会影响性能，例如实时AI推断或数据库事务。

对象存储和块存储之间的选择取决于AI/ML项目的具体要求，包括数据类型、性能需求和访问模式。

9.7 网络

9.7.1 网络带宽

足够的网络带宽对快速数据访问、远程协作和模型部署至关重要，特别是在基于云或分布式的AI/ML环境中。优化良好的基础设施减少延迟、瓶颈和性能下降，尤其对于数据密集型应用，例如深度学习、实时分析和大规模模型训练。

规格：

- 高速互连，如Infiniband或10/40/100 Gbps以太网，用于在服务器和存储系统之间快速数据传输，以及分布式训练和实时推理;
- 最低要求：1 Gbps网络带宽，以支持数据传输、远程开发环境和基于云的处理;
- 低延迟：确保与远程AI/ML基础设施的顺畅互动，包括数据湖、存储解决方案和边缘计算设备;
- 可扩展性：基础设施应支持更高的带宽（例如10 Gbps或更高），以便在AI/ML工作负载扩展时，特别是对于实时推理和大规模数据摄取。

9.7.2 云计算资源

前面的部分提供了本地计算资源的最低规格，指的是在海关管理局数据中心内本地托管的硬件和存储。该设置确保对数据、安全和计算资源的完全控制，但需要更高的前期成本和维护。

替代方案是云计算资源，提供按需计算能力、存储和服务。选择本地和基于云的基础设施取决于成本、可扩展性、数据安全性和操作要求。

可以从可扩展的云计算开始进行AI/ML项目，以最小化前期成本。云计算实例是托管在云平台（AWS、Azure、Google Cloud）上的虚拟机（VM），提供CPU/GPU配置，以便为不同的AI/ML工作负载提供灵活和可扩展的计算能力。

规格：

- CPU实例：8个vCPU，32GB RAM;
- GPU实例：4 x NVIDIA V100 GPU，64GB GPU内存;
- 存储：基于云的SSD存储;
- 网络：高速10GbE+云互连，用于大型数据集处理;
- 自动扩展：根据工作负载需求动态调整计算实例的数量，确保资源的最佳利用和成本效率;
- 自动扩展组根据需求管理实例数量。

对于，混合方法通常是理想的——对于安全敏感的工作负载使用本地计算资源，同时利用云AI/ML服务进行可扩展处理和深度学习任务。这确保了最佳性能、合规性和成本效率，使能够有效开发和部署AI/ML能力。

9.8 机器学习（MLOps）

机器学习（MLOps）是指一套实践和工具，使组织能够在生产环境中构建、部署和维护ML模型。MLOps弥合了数据科学家和IT运营团队之间的差距，确保AI模型高效和有效地开发、部署和管理。

9.8.1 在海关管理中建立MLOps能力

为了有效实施AI/ML计划，不仅要构建技术基础设施，还要建立强大的MLOps能力。MLOps（机器学习操作）是一项至关重要的实践，它弥合了数据科学和IT运营之间的差距，确保ML模型能够在规模上进行开发、部署和管理。该能力确保AI/ML模型不仅高效开发和部署，还能在其生命周期内进行管理、监控和治理。MLOps为AI/ML项目带来了卓越的运营能力可扩展性和合规性，使能够充分利用AI/ML技术的潜力，同时保持最高的准确性、可靠性和伦理责任标准。

通过实施MLOps实践，组织可以：

加速AI开发和部署：MLOps简化了构建、测试和部署AI模型的过程，缩短上市时间;

提高模型性能：MLOps确保模型持续被监控和维护，优化其性能;

- 增强可重复性：MLOps帮助建立可重现的工作流程，使复制和扩展AI实验变得更容易;
- 减少风险：MLOps 帮助减轻与 AI 项目相关的风险，例如数据质量问题、模型偏差和安全漏洞。

9.8.2 建立MLOps能力的步骤

开发强大的 MLOps 能力需要一种结构化的方法来简化机器学习模型开发、部署、监控和治理。以下步骤概述了构建可扩展和可持续 MLOps 实践的关键方面：

a. 建立集中开发环境

结构化的开发环境确保高效的协作、实验和版本控制。

- 部署具有必要工具的 AI/ML 开发环境，包括 IDE、版本控制系统和 ML 框架。
- 整合实验跟踪工具以管理模型性能和超参数调优。
- 实施访问控制策略以管理共享工作区的安全性。

b. 自动化机器学习管道

自动化提高了一致性并加速了机器学习生命周期。

- 实施持续集成/持续部署（CI/CD）管道以实现模型的无缝更新和再训练。
- 自动化关键流程，如数据预处理、模型训练、评估和部署。
- 整合自动化测试和验证以确保在部署前的可靠性。

c. 开发可重用的管道和模板

可重用的资产提高了效率和标准化。

- 为常见任务（如数据转换、训练和推理）创建预构建的 ML 管道模板。
- 实施基础设施即代码（IaC）以确保一致的部署环境。
- 开发用于模型推理和系统集成的标准化 API。

d. 实施强大的数据管理和治理

有效的数据治理确保数据质量、安全性和合规性。

- 建立集中数据仓库以管理结构化和非结构化数据。
- 实施数据版本控制以跟踪数据集更改并确保可重复性。
- 执行数据验证和合规性检查，以符合隐私法。

e. 启用可扩展的模型训练和实验

可扩展的训练基础设施优化模型性能。

- 利用基于云或本地的计算资源加速模型训练。
- 自动化超参数调优以提高效率。
- 启用并行实验以优化模型选择。

f. 简化模型部署和服务

高效的部署确保可扩展性和可靠性。

- 使用容器化和编排进行灵活部署。
- 实施模型服务平台以优化推理。
- 进行 A/B 测试和影子部署以验证新模型。

g. 监控和维护生产中的模型

持续监控确保随时间的性能和公平性。

- 部署模型监控工具以跟踪准确性、延迟和漂移。
- 实施漂移检测和自动再训练以保持准确性。
- 利用可解释AI[32] 框架以提高决策的透明度。

9.9 用于集成AI/ML的数据集成工具

为了将 AI/ML 解决方案与现有系统（如海关管理系统、单一窗口平台、电子货物追踪、ERP 和人力资源系统）集成，需要强大的数据集成工具，以促进各种系统之间的无缝数据流和互操作性，确保 AI/ML 模型能够实时访问、处理和提供可操作的见解。这些集成工具支持各种数据格式、协议和实时处理需求，提供必要的基础设施，使 AI/ML 模型能够利用海关生态系统中的数据，以增强决策、自动化和运营效率。下列是数据集成工具的提议技术规格。

9.9.1 Apache Spark

Apache Spark 是一个功能强大的开源统一分析引擎，专为大规模数据处理而设计。它支持各种数据集成任务，包括 ETL（提取、转换、加载）、实时流处理和高级分析，是将 AI/ML 模型与各种海关系统集成的绝佳选择。它最适合于高容量、低延迟的数据集成任务，例如处理来自海关管理系统、一窗式平台、电子货物追踪系统的大型数据集、实时海关风险分析和预测分析。

规格：

- 集群配置：最少4节点集群，每个节点16核CPU，64 GB RAM；
- 存储集成：与HDFS、S3、Azure Blob Storage或本地文件系统的数据存储和检索的集成；
- 数据处理框架：支持Spark SQL、Spark Streaming、MLlib（用于机器学习集成）和GraphX（用于图形处理）；
- 安全与合规：与Kerberos集成，端到端加密（SSL/TLS）和访问控制机制，以确保数据隐私和安全合规；
- 连接器支持：为数据库、大数据存储和消息系统提供预构建连接器；
- 实时处理：支持低延迟的流处理，能够与电子货物追踪和海关监控平台等系统进行实时集成。

9.9.2 Apache NiFi

Apache NiFi（之前称为Apache Niagara Files）是一款开源数据集成工具，旨在自动化数据在系统之间的移动、转换和管理。它提供了用户友好的界面用于设计数据流，并支持实时数据集成，使其非常适合与各种海关系统集成AI/ML模型。此工具最适合于实时和批量数据集成任务，包括从海关管理系统、一窗式平台和外部数据源的数据摄取。

规格：

- 部署：每个节点的最低4核CPU，16 GB RAM，适用于小型到中型规模的部署；可扩展到多节点集群以满足高吞吐量要求；

[32] 可解释人工智能（或XAI）是指使人工智能模型决策透明、可解释和可理解的技术，帮助用户信任、审计并遵守法规要求，通过解释模型的预测和行为。

- 数据流设计：用于设计数据流的可视化界面，支持复杂路由、过滤和转换任务；
- 协议和格式支持：与多种数据协议（如HTTP、FTP、MQTT）和格式（如JSON、XML、CSV）的集成，以处理来自各种海关和贸易系统的数据；
- 安全性：传输中的数据进行端到端加密（SSL/TLS），基于角色的访问控制，并与LDAP或Kerberos集成以确保安全认证；
- 可扩展性：支持集群和负载均衡，以管理大数据量并确保高可用性；
- 实时处理：能够进行实时数据摄取和处理，使其适合于实时货物追踪和海关清关监控等应用。

9.10 与特定系统的数据集成

9.10.1 海关管理系统和单一窗口平台

将AI/ML模型与海关管理系统（CMS）和一窗式平台集成涉及实时数据交换，以促进风险分析、贸易合规和自动决策。

规格：

- 连接器支持：支持与CMS和一窗式API（如RESTful API、SOAP）的集成，以实现直接数据交换；
- ETL能力：提取海关申报、货物清单和其他贸易文件中的数据的ETL过程，为AI/ML模型输入转换数据，并将结果加载回CMS；
- 数据转换：能够处理海关交易中使用的各种数据格式（如UN/EDIFACT、XML、JSON）；
- 高可用性：支持集群和故障转移，以确保与关键海关系统的无中断数据集成。

9.10.2 电子货物追踪系统（ECTS）

电子货物追踪系统（ECTS）提供货物移动的实时跟踪和监控。将这些系统与AI/ML模型集成需要处理高速数据流，以进行预测分析和异常检测等任务。

规格：

流数据支持：与实时数据流（如Apache Kava、MQTT）的集成，以便从货物追踪设备进行持续数据摄取；

低延迟处理：实时处理能力，对于时间敏感的任务，如路线优化和异常检测，延迟在1秒以内；

数据聚合和增强：能够将追踪数据与其他来源（如天气信息和历史贸易数据）进行聚合和增强，以提高AI/ML模型的准确性。

9.10.3 企业资源规划（ERP）和人力资源（HR）

ERP和HR系统包含与内部流程、员工分配和资源管理相关的宝贵数据，可以与AI/ML模型集成以进行运营优化。

规格：

- 连接器集成：为常见的ERP和HR系统（如SAP、Oracle、Workday）提供预构建连接器，以促进数据提取和集成；
- 数据隐私：安全处理敏感信息，如员工记录和财务数据，包括加密、访问控制和遵循数据隐私法规；

定期数据同步：支持定期数据同步（如每日、每周），以便使用最新的运营和HR数据更新AI/ML模型，用于员工优化和资源分配等任务；

测试和公平性测试工具：AI模型测试工具，如MLflow、AI Verify、AI Fairness 360或Fairlearn，用于评估公平性、偏见、可信度并确保遵循关键伦理标准；

安全性和合规性：网络安全措施、数据加密、访问控制以及遵循数据保护法规。

9.10.4 安全与合规

数据集成工具必须确保系统之间的安全数据交换，尤其是在处理敏感的海关、贸易和人员数据时。遵循数据隐私法规和海关数据交换标准至关重要。

规格：

- 数据加密：传输中和静态数据的端到端加密（SSL/TLS）；
- 访问控制：基于角色的访问控制（RBAC）和与现有身份验证系统（如LDAP、Kerberos）的集成；
- 审计和日志记录：全面的日志记录和审计能力，以跟踪数据访问、转换和传输，以满足合规要求。

10 成本

本节中呈现的指示性估计成本范围是通过市场研究、行业基准[33]和情景洞察以及咨询多家业内人士得出的[34].

这些估算基于当前的公开资料。然而，这些估算不应被视为精确或实际的财务成本，因为实际消费会因海关管理的独特运营需求、现有基础设施和战略目标而有所不同。此外，软件许可费用、支持合同和集成成本可能会因供应商定价变动、市场需求和谈判结果而显著不同。成本可能会根据海关管理的地理位置而有所不同，包括区域定价变动、当地供应商的可用性和劳动力成本差异。海关管理的规模和规模，包括用户数量、操作复杂性和所需集成程度，可能导致实际费用的变化。

指示性估计成本范围仅供信息和规划之用。

10.1 AI/ML框架

像TensorFlow、PyTorch和R这样的基础AI/ML框架是开放源代码且免费提供的。然而，有效实施需要在基础设施、熟练人员和持续运营支持方面的投资，以及与海关特定系统的集成。尽管使用这些开源框架可能会有额外成本，例如许可费用和数据库、可视化工具及用于货物检查图像识别或贸易数据异常检测的专门库的维护/支持费用。

估算成本范围如以下表格所示。

表3 - 人工智能/机器学习框架的成本范围

费用类别	备品备件名称	指示性估计费用范围
软件和工具	开源框架（免费），35 专有扩展，企业支持许可证	开源（社区版）- 免费 企业级 - USD 10,000 - 每年 USD 100,000
许可证和合规性	额外软件的许可证	USD 10,000 – USD 100,000 每年

10.2 集成开发环境（IDE）

正如本报告第10节所讨论的，IDE对于高效地编写、调试和可视化代码至关重要。像PyCharm这样的工具需要每位用户的年许可，而其他如Visual Studio Code和Jupyter Notebook则是开源且免费的；然而，企业版本或基于云的服务五月有相关费用。估计成本范围在下面的表格中列出。

---

[33] 市场研究参考和来源如：IDC。“全球AI和生成AI支出指南”；Run.ai。“AI成本估算：理解财务影响”；ProjStream。“成本估算的未来：拥抱AI和机器学习。”和PhoenixNAP。“HPC服务器价格：理解高性能计算的成本”。

[34] 行业咨询包括德勤、谷歌、华为、宇信科技。

[35] 开源/社区版本通常是免费的，但五月会产生间接的部署、维护和支持费用。企业级成本可以根据部署规模、用户数量和所需支持水平等因素大相径庭。

表4 - 集成开发环境（IDE）的成本范围

费用类别	备品备件名称	指示性估计费用范围
软件许可	开源许可证 - Visual Studio Code, Jupyter 笔记本	开源（社区版）- 免费
	企业级（基于云） - Jupyter Enterprise Gateway, Google Colab Pro	每用户/月 USD 10 - USD 50
	企业级（许可） - PyCharm Professional, IntelliJ IDEA Ultimate	每用户/年 USD 200 - USD 700

10.3 版本控制

版本控制系统对协作的AI/ML项目至关重要。涉及的成本是专有版本控制系统或GitHub企业版、GitLab高端版等的订阅费。

表5 - 版本控制的成本范围

费用类别	备品备件名称	指示性估计费用范围
免费/开源	工具如 Git、GitLab Community Edition 和 Bitbucket 云（免费套餐）提供基本的版本控制功能，无需许可费用。	开源（社区版）- 免费
SaaS/云企业	托管企业解决方案（如 GitHub Enterprise Cloud、GitLab Premium、Bitbucket Premium），提供先进的协作、安全性和支持特性。	每个用户每月10-30美元
自托管企业	企业级自托管解决方案（例如GitHub Enterprise Server、GitLab自管理）五月要求年度许可费、基础设施和维护成本。	每年3,000-10,000美元

10.4 自动化、数据管理和治理

自动化工具以及数据管理和治理框架对提高运营效率、确保数据完整性和维护合规性至关重要。估计成本包括专有解决方案、工具和模板库的软件许可。

表6 - 自动化、数据管理和治理工具及框架的成本范围

检验部件名称	备品备件名称	指示性估计费用范围
编排工具	Apache Air Flow、Prefect或Luigi等工具。	开源（社区版）- 免费 企业级 - USD 10,000 - 每年 USD 100,000
CI/CD管道	开源-Jenkins、GitLab CI/CD、Travis CI企业级 -GitLab Enterprise、CircleCI、Azure DevOps	开源（社区版）- 免费 企业级-20美元-美元 200每用户/月
模板库	开源-scikit-learn、TensorFlow、PyTorch 免费企业级 -IBM Watson、Google Cloud AI、Azure 机器学习）	开源（社区版）- 免费 企业级-1,000美元-美元 每月10,000+
配置管理	开源—Ansible、Terraform、Chef 企业级-Ansible Tower（红帽）、Terraform Enterprise、Chef Enterprise	开源（社区版）- 免费 企业级-5,000美元-美元 每年50,000+
数据湖工具	开源—Apache Hadoop、Apache Spark 企业级 -Amazon S3、Azure数据湖存储、Google云存储	开源（社区版）-免费（不包括基础设施成本）

		企业级-0.02美元-美元 0.05 存储每GB/月，数据处理和分析的额外成本
数据治理工具	开源-Apache Atlas、ODPi Egeria 企业级-IBM InfoSphere信息治理目录、Collibra数据治理、Informatica Axon数据治理	开源（社区版）-免费（不包括实施和维护成本） 企业级 - 每年50,000美元 - 200,000美元以上
数据质量工具	开源-OpenRefine、远大前程企业级-Informatica数据质量、Talend数据 质量，IBM InfoSphere Information Server用于数据质量	开源（社区版）-免费（不包括实施和维护成本） 企业级-20,000美元- 每年200,000美元以上

10.5 模型开发和训练

模型开发和训练组件对开发和维护高效的ML模型至关重要。下表提供的估计成本使实验工具、超参数调整和分布式训练框架的规划和预算更加有效。

表7 - 模型开发和训练的成本范围

检验部件名称	备品备件名称	指示性估计费用范围
实验工具	开源-Jupyter Notebook(v6.x+)、RStudio企业级 -RStudio Server Pro、 JupyterLab Enterprise	开源（社区版）- 免费 企业级-5,000美元-美元 每年50,000+
超参数调优工具	开源 – Optuna、Hyperopt、Scikit-learn的GridSearchCV 企业级 -SigOpt、DataRobot AutoML	开源（社区版）- 免费 企业级-10,000美元-美元 每年100,000+
分布式培训工具	开源——Horovod，TensorFlow的分布式策略 企业级 -托管解决方案（例如AWS SageMaker、Google Cloud AI平台）	开源（社区版）- 免费 企业级 – USD 500 – USD 每月5,000+

10.6 平台架构

下面呈现的成本重点在于软件许可、持续支持以及平台架构的集成/定制成本。这些包括操作系统的许可证（如Windows Server、Linux发行版）、虚拟化平台（如VMware vSphere）和安全软件（如防火墙、VPN、IAM解决方案）。

对于使用云服务提供商如AWS、Azure或Google Cloud托管AI/ML工作负载的云部署，成本包括云服务的软件许可、来自云提供商的持续支持以及云环境的集成/定制。

在混合云架构的情况下，成本涉及混合管理工具的许可，以管理和集成混合环境，包括安全连接工具和统一管理软件。

对于Kubernetes集群和容器化部署，成本包括企业Kubernetes发行版和Docker等容器化平台的许可。

表8 - 平台架构的成本范围

检验部件名称	备品备件名称	指示性估计费用范围
本地部署	操作系统、虚拟化软件（如VMware）和安全软件（如防火墙、VPN、IAM）的许可证 解决方案）。	每年20,000-80,000美元
云部署	云服务（例如AWS EC2、Azure VM）、软件即服务(SaaS)工具和云原生的订阅费用 安全服务（如加密、IAM）。	每年10,000-80,000美元
混合云架构	混合管理工具（例如VMware vSphere with cloud integration）、安全连接工具（例如VPN、Direct Connect）和统一管理的许可证 软件。	每年15,000-90,000美元
Kubernetes集群	开源-Vanilla Kubernetes 企业级 -Red Hat OpenShift、VMware Tanzu	开源（社区版）-免费（不含基础设施成本）企业级-5,000美元-美元每个集群每年50,000+。
容器化	开源-Docker社区版企业级 -Docker Enterprise（现为Mirantis的一部分）	开源（社区版）- 免费 企业级 – USD 15 – USD 24 每个用户/月

10.7 计算资源需求

对于典型的，正确的计算资源设置确保高效的数据处理、加速的模型训练和可扩展的操作，这对于如欺诈检测、收入估算和货物检查等任务至关重要。

下面 outline 的计算资源提供了包括高性能计算服务器、内存、GPU和存储解决方案在内的基本组件的详细概述。重要的是要强调，所呈现的指示性估计成本范围通常依赖于特定的AI/ML开发和模型训练环境。复杂的ML任务、数据量、期望的可扩展性和与现有系统的集成等因素显著影响这些成本。

表9 - 计算资源需求的成本范围

检验部件名称	备品备件名称	指示性估计费用范围
高性能计算(HPC)服务器	配备Intel Xeon或AMD EPYC CPU的高性能服务器 – CPU实例：8个vCPU、32GB RAM GPU实例：4个NVIDIA V100 GPU，64GB GPU内存	每台服务器50,000-80,000美元
内存（RAM）	高容量RAM-32GB高速DDR4或DDR5 ECC内存。	每台服务器2,000-3,000美元
图形处理单元（GPU）	高端GPU（例如NVIDIA V100 GPU，尽管这些五月到2025年将过时，因此同等的现代GPU是 必填）。	每个GPU 40,000-60,000美元
本地和网络存储	高速NVMe SSD（最低2 TB）和可扩展NAS/NFS系统（最低10 TB），可实现快速数据访问 以及跨多个节点的数据共享。	每个存储设置5,000-10,000美元
网络 附加存储	集中式、可扩展的存储解决方案，提供高 吞吐量低时延，支持并发	USD 600到USD 2000+每个NAS/NFS设置
(NAS)/网络 文件系统(NFS)	无缝数据共享在AI/ML中的读写操作 任务。	

云计算资源	云实例（如AWS EC2、Azure VMs、Google Compute Engine）提供可扩展的计算能力，以处理不同的工作负载。例如c5.4xlarge的CPU实例适合计算密集型任务，而p3.8xlarge或p4d.24xlarge的GPU实例则提供多个GPU用于深度学习和高性能计算。	每年10,000-80,000美元
云存储服务	可扩展的云对象存储（如Amazon S3、Azure Blob Storage、Google Cloud Storage）从10 TB开始，加上高性能应用的云块存储（每个实例至少2 TB）性能应用。	USD 5,000 – USD 50,000每年
自动扩展服务	自动扩展服务根据工作负载需求动态调整计算实例的数量，确保资源的最佳利用和成本效率。规格包括自动扩展组以管理基于需求的实例数量。	USD 3,000 – USD 15,000每年

10.8 网络

网络基础设施对于确保快速的数据传输、服务器与存储系统之间无缝通信，以支持AI/ML倡议至关重要。网络硬件需求通常依赖于特定的AI/ML开发和模型训练环境，因此网络基础设施的估计成本范围必须针对每个特定的AI/ML环境进行配置。

表10 - 网络需求的成本范围

检验部件名称	备品备件名称	指示性估计费用范围
高速互连	高速互连，如Infiniband或10/40/100 Gbps以太网，对于服务器与存储系统之间快速数据传输至关重要，对于分布式训练和实时推理是关键时间推断。	USD 5,000 – USD 25,000每年
网络带宽	足够的网络带宽（最低1 Gbps）对于顺畅的数据传输和远程访问开发环境是必要的，最小化数据密集操作中的延迟集约化运营。	USD 2,000 – USD 10,000每年

10.9 的成本效益AI/ML采用策略

虽然实施人工智能/机器学习能力的最低技术规范的估计成本看似可观，但重要的是要认识到，有成本效益的方式可以开始迈向人工智能/机器学习采纳的旅程。

海关管理可以利用各种策略，将AI/ML能力纳入其运营，而无需立即投资于广泛的内部基础设施和开发能力。这些针对海关管理的成本效益AI/ML采纳策略提供了实际替代方案，允许逐步和可扩展地实施AI/ML解决方案，在技术进步的需求与预算限制之间取得平衡。

海关管理可以探索几种替代方案，以降低将AI/ML纳入运营的成本，而无需在内部基础设施和开发能力上进行重大投资：

1. 基于云的解决方案

- 利用提供AI/ML服务的云平台，减少对本地基础设施的需求
- 按需付费模型允许根据实际使用情况进行成本效益扩展

2. 开源工具和框架
    - 利用免费和社区驱动的工具，如TensorFlow、PyTorch和scikit-learn
    - 在没有许可费用的情况下受益于快速进展和协作问题解决
3. 合作与伙伴关系
    - 与学术机构或行业专家建立合作关系以共享知识
    - 参与跨境合作以共享资源和专业知识
4. 管理的MLOps服务
    - 选择管理的MLOps平台，这些是云基础上的平台/服务，以处理AI/ML部署的技术复杂性
    - 在早期阶段减少对专业内部技能的需求。
5. 逐步实施
    - 从小型高影响项目开始，在扩展之前展示价值
    - 逐步实施AI项目，将成本分散到一段时间内
6. 预构建的AI解决方案
    - 利用针对特定海关用例的预训练模型和AI服务
    - 调整现有解决方案，而不是从头开始构建

通过探索上述方案，海关管理可以更具成本效益地将AI/ML能力纳入其运营，同时仍然受益于这些技术所提供的增强效率和决策能力。

11 技能与培训

为了够利用AI/ML技术，他们需要投资于全面的培训项目和能力建设计划，以使其员工具备必要的技能和知识。优先考虑培训和能力建设，以确保技术和非技术员工都具备成功部署和管理AI/ML技术所需的知识和技能是至关重要的。

培训可以按如下优先级进行：

AI/ML基础 - 为所有员工提供对AI/ML概念的基本理解，关注海关运营中的实际应用

数据科学与分析 - 对技术员工进行数据预处理、分析和可视化的培训；强调针对海关的特定数据处理和解释

风险管理与预测分析 - 发展使用AI进行风险评估和目标定位的技能；培训员工解读AI生成的见解以进行决策

AI伦理与治理 - 对从事政策和法律事务的官员进行AI部署中的伦理考量教育；确保遵守数据隐私法规和海关法律

AI项目管理 - 培训管理人员监督AI/ML项目；重点关注将AI解决方案集成到现有海关流程中，并获得AI工具的实践经验

培养内部专业知识对于AI/ML项目的长期可持续性和减少对外部顾问的依赖至关重要。这一发展过程涉及结构化培训项目、与外部专家的合作以及与AI/ML工具和技术的实践经验相结合。

11.1 在整个组织中培养数据素养

除了技术专业知识，需要在组织内部培养数据素养文化。数据素养指的是理解和解释数据的能力，这对从事AI/ML项目的技术和非技术人员都是至关重要的。海关官员、政策制定者和决策者应接受培训，学习如何解释AI/ML生成的洞察并将其应用于决策过程中。理解数据驱动的洞察可以更好地进行监督，确保有效地使用AI/ML模型来提升海关业务。

一些建议的活动以提升数据素养包括：

11.1.1 数据素养意识项目

门可以实施意识提升项目，向所有员工介绍基本数据概念，包括海关官员、政策制定者和行政人员。这些项目可以涵盖基本概念，例如结构化数据和非结构化数据之间的区别、数据在AI/ML模型中的作用以及数据质量如何影响决策。这为如何数据影响操作建立了基础理解。

11.1.2 数据解释研讨会

可以组织实操研讨会，专注于教导非技术人员如何解释和使用数据驱动的洞察。例如，这些研讨会可以讲解如何阅读仪表盘、理解风险评分，以及如何将AI生成的风险评估应用于检查或通关过程中的明智决策。可以使用涉及真实海关数据的实际场景来培训员工在日常操作中应用数据洞察。

11.1.3 互动数据仪表板

为内不同角色定制互动数据仪表盘，可以帮助员工访问和互动实时数据。例如，海关官员可以使用仪表盘追踪高风险货物，而合规经理可以监控执法行动的趋势。关于如何导航和从这些仪表盘提取有用洞察的培训课程将提升数据素养。

11.2 发展AI/ML培训和能力建设的策略

11.2.1 评估当前技能水平并识别差距

第一步是评估当前的技术专业知识水平。了解现有员工的能力将有助于识别数据科学、机器学习、数据工程和AI伦理等关键领域的技能差距。海关管理部门可以设计针对性的培训项目，以解决这些差距，确保他们的员工在AI/ML概念和工具方面有坚实的基础。这包括识别那些有潜力成为AI/ML倡议内部champions的员工，并为他们提供高级培训。

11.2.2 通过跨部门协作进行能力建设

海关管理部门的AI/ML倡议需要各部门之间的合作，包括IT、数据管理、运营和合规。开发跨部门团队，协力开展AI/ML项目可以改善沟通，并确保全面实施的方案。这些团队应包括领域专家（如海关官员）、技术专家和数据科学家，确保AI/ML解决方案与运营需求和监管要求对接。

跨培训项目，使不同部门的员工接触AI/ML概念及其对海关运营的潜在影响，也可以促进理解与合作。这种方法促进了AI/ML在更广泛海关流程中的整合，减少了孤岛现象，确保AI/ML工具融入日常工作流程。

11.3 建立技术专长

为了培养AI/ML项目所需的技术技能，海关管理部门应实施一个结构化程序，专注于核心AI/ML能力，如数据分析、模型开发以及将算法技术应用于实际海关操作。

这样的培训可以通过与学术机构的合作、在线课程，或与AI/ML专家或其他政府机构合作来进行。

关注海关实际应用的研讨会和培训班，例如预测不合规行为或自动化通关流程，可以进一步增强工作人员利用人工智能/机器学习进行日常工作的能力。

以下是一些可以帮助建立这种专业知识的活动和培训方法的示例：

11.3.1 与学术机构的伙伴关系

海关部门可以与专注于数据科学和人工智能/机器学习的本地或国际大学合作。这些合作关系可以提供：

- 为海关人员提供机器学习或数据科学的证书课程，提供人工智能概念和算法的基础知识。

- 专门为海关量身定制的课程，重点关注人工智能应用，如贸易数据分析、欺诈检测和流程优化。主题应包括人工智能/机器学习算法的使用，例如决策树、随机森林和支持向量机，以及这些模型在海关操作中的实际应用，用于风险评估、欺诈检测和流程优化。
- 实习或研究合作，海关工作人员可以与大学研究人员在与海关操作相关的人工智能/机器学习项目上合作，例如自动化文件分类以加快通关流程。

11.3.2 实践培训、在线课程和认证

与人工智能/机器学习平台和工具（如Python, R, TensorFlow等）进行实践和实际操作的培训可以帮助建立对开发和部署人工智能/机器学习模型所需系统的熟悉。海关部门可以为工作人员提供对流行的人工智能/机器学习平台和编程环境的访问，例如：

- 用于构建机器学习模型的Python及其库，如TensorFlow。
- 用于统计计算和数据分析的R。
- 用于创建深度学习模型的TensorFlow，能够自动化复杂任务，例如扫描文档中的图像识别。

由于其受欢迎程度和需求，提供专门的人工智能/机器学习培训以掌握人工智能/机器学习工具和软件的供应商不乏其人。海关部门可以鼓励工作人员完成：

- 涵盖关键算法（如随机森林、神经网络和支持向量机（SVM））的在线机器学习课程。这些课程通常包括互动编码挑战和测验，有助于巩固学习。
- 结合理论和实践的人工智能认证，装备海关人员使用Python、R、TensorFlow等工具的实用知识。例如，工作人员可以注册一门关于海关操作预测建模的在线课程，学习如何构建模型以识别贸易模式中的异常，指示潜在走私活动。

11.3.3 研讨会和训练营

内部的人工智能/机器学习研讨会或培训班可以提供密集的实践经验。这些活动可以由人工智能/机器学习专家或技术供应商主办，重点关注海关的实际应用案例：

- 数据分析培训班，培训海关官员使用Python或R分析海关数据，例如识别海关申报中的趋势或发现贸易量中的不规则现象。
- 机器学习模型开发研讨会，教工作人员使用历史海关数据构建、训练和验证人工智能模型。例如，官员可以学习如何开发和验证模型，以预测不合规或逃税的可能性。

这些动手课程提供了将人工智能/机器学习技术直接应用于海关官员所处理的数据集的机会，确保实践和相关的学习。

11.3.4 黑客松或数据挑战

海关部门可以组织人工智能/机器学习黑客马拉松或数据挑战，海关人员团队竞争以解决使用机器学习的特定问题。挑战主题的示例包括：

- 欺诈检测模型：团队可以被要求构建检测异常贸易模式的模型，这些模式五月指示欺诈申报或分类错误的商品。
- 优化通关时间：参与者可以利用预测算法自动化通关流程，为低风险货物优先处理。

黑客马拉松鼓励合作与创新，同时让员工获得使用人工智能/机器学习工具和技术的实践经验。

11.4 为人工智能/机器学习建立新的工作角色

人工智能/机器学习在海关业务中的整合需要在机器学习、数据分析和自动化等领域的专业知识，这些领域与传统海关角色不同。海关行政部门的人力资源（HR）部门需要为人工智能/机器学习建立新的职位档案和描述，以吸引、留住并有效利用在这专业领域新培训的员工。

通过创建清晰且最新的职位档案，概述人工智能/机器学习职位所需的具体能力、职责和技术技能，人力资源部门可以更好地定位、培训和招聘合适的人才。此外，明确的角色有助于提供职业发展机会，确保新培训的员工感到被重视，并在组织内看到明确的成长路径，这对留住人才和人工智能/机器学习在海关业务中的长期成功至关重要。

一些新的HR职位档案和职位描述如下：

11.4.1 人工智能/机器学习专家

角色概述：

人工智能/机器学习专员理想情况下应在海关行政的IT部门工作，专注于在海关各个业务领域开发和部署人工智能/机器学习模型的技术。

人工智能/机器学习专员负责设计、开发和实施人工智能/机器学习模型，以优化各项海关业务，包括风险评估、欺诈检测和贸易合规。该角色侧重于利用先进的数据分析和机器学习技术来支持决策制定，并提高海关行政的效率。人工智能/机器学习专员将与数据工程师、海关官员和IT专业人员密切合作，以确保人工智能/机器学习应用与组织的战略目标保持一致。

主要职责：

1. 人工智能/机器学习模型开发：
    - 开发、训练和部署用于海关操作的机器学习模型（例如货物分类、欺诈检测、风险评估）。
    - 尝试不同的算法，如决策树、随机森林和神经网络，以解决特定于海关的挑战。
    - 微调模型以优化性能，确保高准确性和与操作需求的相关性。
2. 数据准备和分析：
    - 与IT数据工程团队合作，为人工智能/机器学习项目准备、清理和规范数据。
    - 分析来自海关系统的大型数据集，以识别趋势、异常和人工智能/机器学习应用的潜在领域。
    - 处理结构化和非结构化数据，包括贸易数据、检查报告和交易记录。
3. 部署和维护：
    - 监督人工智能/机器学习模型的生产系统部署，确保它们顺利集成到海关的日常操作中。
    - 持续监测模型的性能和准确性，根据新数据或操作变化进行更新和再训练。
4. 跨部门协作：
    - 与海关官员、风险管理团队和合规人员联络，以确保人工智能/机器学习模型符合实际需求和监管要求。

- 为非技术团队提供培训和指导，帮助他们有效使用人工智能/机器学习驱动的见解进行决策。

5. 文档和报告：
   - 记录模型开发过程、假设和结果，以便内部报告和审计使用。
   - 准备并向高级管理层呈现性能报告和数据驱动的见解，并对流程改进提出建议。
6. 创新和研究：
   - 掌握人工智能/机器学习技术的最新进展，并应用创新技术解决海关相关挑战。
   - 尝试新模型和工具，探索在海关操作中人工智能/机器学习的潜在新应用。

主要资格：

- 教育背景：
  - 数据科学、计算机科学、人工智能、机器学习或相关领域的学士或硕士学位。
  - 在AI/ML、数据科学或相关领域的专业认证是一个优势。
- 经验：
  - 3-5年的AI/ML模型工作经验，最好是在公共部门或监管环境中。
  - 在开发和部署机器学习算法方面有证明的经验，如支持向量机（SVM）、随机森林、神经网络等。
  - 有使用AI/ML平台（如TensorFlow、Scikit-learn或类似工具）的经验。
- 技术技能：
  - 精通Python、R或Java等编程语言。
  - 在数据分析工具和技术方面的专业知识。
  - 具有与基于云的AI平台（如AWS、Google Cloud、Azure）合作的经验者优先。
  - 熟悉海关操作、贸易法规或风险评估框架者优先。

核心能力：

- 分析思维：能够分析大型数据集，得出有意义的结论并开发可行的AI/ML模型。
- 解决问题：能够以数据驱动的解决方案和创新思路来应对与海关相关的挑战。
- 沟通技能：能够将技术AI/ML概念传达给非技术利益相关者。
- 协作：能够跨部门工作，包括与海关官员、IT团队和合规官员合作，确保AI/ML模型满足操作需求。
- 适应能力：愿意不断学习并应用AI/ML的新技术和新方法。

11.4.2 数据科学家（海关操作）

数据科学家应理想地被放置在创新与研究单位或战略规划单位，专注于基于数据的决策。

数据科学家的角色强调对数据的探索、分析和解释，以支持长期规划、风险管理和操作改进。他们将与一些高度依赖数据洞察进行决策的部门密切合作，如合规、政策和检查团队，确保决策基于可靠的数据分析。

数据科学家将专注于探索、分析和解释大型数据集，以提取可改善海关操作的可行洞察。与AI/ML专家不同，后者主要负责机器学习模型的开发和部署，数据科学家的角色涉及生成数据驱动的洞察，以告知决策并利用先进的分析技术优化流程

主要职责：

1. 数据探索与分析：
    - 对大型数据集进行深入分析，包括海关申报、贸易量和检查结果，以识别趋势、异常和关键绩效指标。
    - 使用统计方法评估海关流程，例如不同类型货物的平均清关时间，或识别与贸易合规或欺诈相关的模式。
2. 预测分析和统计建模：
    - 开发统计模型以预测贸易流、出货量或潜在风险水平。
    - 利用预测分析来预见海关瓶颈，使组织能够在交易高峰期有效分配资源。
    - 创建模型以预测因监管变化、关税或全球市场趋势而导致的贸易行为变化。
3. 数据可视化和报告：
    - 构建交互式仪表板和可视化，帮助利益相关者快速理解和采取数据洞察行动，如风险评估分数、欺诈检测趋势和清关时间改进。
    - 生成详细报告，提供对贸易模式、合规率和检查有效性的洞察，以告知政策制定和战略规划。
    - 与高级管理层和海关官员合作，以解释这些洞察并制定可行的建议。
4. 数据质量和治理：
    - 与数据工程师紧密合作，确保数据管道和数据库为分析使用进行了优化，确保数据质量和完整性。
    - 实施数据验证技术，以确保贸易数据在用于分析或决策之前的准确性、完整性和可靠性。
    - 定义和监控数据质量指标，确保海关操作以准确和可靠的数据为驱动。
5. 协作与跨部门支持：
    - 与风险管理团队、合规官和海关检查单位合作，提供支持其运营目标的数据驱动见解。
    - 与IT和数据工程团队合作，确保数据可访问性，并设计允许海关官员进行实时数据监控的系统。
    - 为不同部门提供临时分析支持，使他们能够在日常决策过程中使用数据见解。
6. 趋势与政策分析：
    - 分析新贸易协议、关税或法规对海关操作和贸易量的影响，提供海关管理如何适应这些变化的见解。
    - 监测全球贸易趋势和地缘政治因素，识别海关操作的潜在风险或机会，如贸易路线的变化或新兴市场。

7. 创新和研究：
    - 保持对数据科学和分析技术最新发展的关注，包括先进的统计技术和大数据平台。
    - 探索将数据分析应用于海关新兴挑战的创新方式，如自动化合规检查或通过数据驱动的方法提高风险评估的准确性。

主要资格：

- 教育背景：
    - 数据科学、统计学、计算机科学、数学、经济学或相关领域的学士或硕士学位。
    - 拥有数据分析、统计或大数据的专业认证者优先。
- 经验：
    - 3-5年的数据分析、统计建模或数据科学经验，最好是在公共部门或贸易相关的背景下。
    - 在探索性数据分析、趋势识别和统计技术方面有扎实的背景。
    - 有处理大型复杂数据集的经验，并为非技术利益相关者设计数据可视化。
- 技术技能：
    - 精通统计工具，如R、Python或SAS。
    - 擅长使用数据可视化工具，如Tableau、Power BI或D3.js构建仪表板和报告。
    - 熟悉SQL和其他数据库管理系统，以查询大型数据集。
    - 了解基于云的数据平台（例如AWS、Google Cloud）和大数据技术（例如Hadoop、Spark）是一个优势。
    - 有使用统计建模技术，如回归分析、聚类和时间序列分析的经验。

核心能力：

- 分析思维：分析复杂数据集、发现模式并提出数据驱动建议的能力。
- 解决问题：运用统计和数据科学技术解决海关操作中现实挑战的能力。
- 沟通：能够向非技术利益相关者清晰地解释数据见解和技术概念的能力。
- 协作：强大的团队合作能力，能够跨部门工作以支持数据驱动的决策。
- 注重细节：在数据分析中保持高水平的准确性，确保所有见解基于可靠的数据。

12 评估、成功案例和经验教训

随着开展AI/ML项目，建立明确的评估框架和成功指标，以确保这些倡议提供价值并实现预期结果至关重要。评估AI/ML项目既涉及定量评估也涉及定性评估，关注模型性能、运营改善与战略目标的一致性。

成功的衡量标准是AI/ML项目在多大程度上满足预定义目标并对组织的长期战略目标做出贡献。衡量指标应包括在效率改善、成本降低和海关操作的可量化收益，这些指标应通过组织绩效管理系统中的适当KPI进行监测。

通过持续监控绩效并根据反馈进行迭代，可以确保人工智能/机器学习项目提供可持续的价值，并推动其运营的实际改善。

12.1 评估

人工智能/机器学习项目评估的步骤包括：

12.1.1 定义项目目标

评估人工智能/机器学习项目的第一步是明确目标和预期结果。海关管理机构必须确定人工智能/机器学习项目旨在实现的具体目标，例如：

- 提高欺诈检测的准确性；
- 减少海关清关时间；
- 通过更好的合规执法增加收入。

这些目标为评估项目的绩效和成功提供了基础。

12.1.2 为人工智能/机器学习模型定义绩效指标

人工智能/机器学习模型的长期可持续性至关重要。一个成功的项目涉及对模型的持续监控和更新，以确保它们保持相关、准确，并能够适应不断变化的贸易动态和监管要求。为了衡量人工智能/机器学习模型的成功，海关管理机构应建立绩效指标，以评估模型在实现目标方面的有效性。这些指标通常包括：

- **准确性**人工智能/机器学习模型所做的正确预测或分类的百分比，例如正确识别高风险货物或不合规交易者；
- **精度和召回率**在欺诈检测或风险评估中，“精度”衡量标记的案例中实际正确的数量（最小化假阳性），而“召回率”衡量识别到的真正正例的数量（最小化假阴性）。
- **假阳性/假阴性率：** 这些指标在海关操作中至关重要，假阳性可能导致不必要的检查和延误，而假阴性可能导致错过风险或违规。
- **模型稳定性**模型稳定性通常基于稳定性指数进行衡量，使用像自助法或交叉验证的技术（测试多个略有变化的训练数据集，并测量数据集之间的性能分散和异常）。

12.1.3 对组织绩效和战略对齐的影响

除了模型性能，海关管理机构应评估人工智能/机器学习项目的更广泛的**运营影响**。如果这些项目导致海关流程中的可测量改进，则是成功的。关键运营指标包括：

- **减少清关时间**人工智能/机器学习项目的主要目标之一是简化海关清关过程。成功可以通过人工智能/机器学习解决方案减少清关时间的程度来衡量，尤其是在处理低风险或合规货物时；
- **增加不合规检测率：** 一个成功的人工智能/机器学习项目应提高海关管理机构检测欺诈或不合规活动的能力，增加罚款收入或防止丧失关税；
- **资源优化：** 准确预测高风险货物或交易者的人工智能/机器学习模型使海关管理机构能够更有效地分配资源，减少随机检查的需要，把注意力集中在更高优先级的案例上；
- **成本节约**人工智能/机器学习解决方案的部署应通过流程自动化带来长期成本节约，减少数据输入、检查和风险评估所需的人工劳动。

12.1.4 成功的衡量

海关管理机构在人工智能/机器学习项目中的成功通过其与更广泛的战略目标的对齐进行衡量，包括运营效率、风险管理、合规、贸易便利化和安全。评估人工智能/机器学习对这些目标的贡献涉及考虑以下因素：

- **运营效率：** 人工智能/机器学习应优化资源分配，自动化流程并减少处理时间和成本。成功通过改善清关时间、自动化重复任务和提高生产力来衡量；
- **贸易便利化：** AI/ML 应该通过加快海关清关、减少延误和改善供应链可见性，创造一个无缝的贸易环境。成功的衡量标准可以是贸易量增加、处理速度更快和交易者满意度更高；
- **风险管理：** AI/ML 应该通过提高欺诈检测和异常识别的准确性来增强风险评估。有效性通过更好地针对高风险货物和乘客并减少误报来衡量；
- **合规性：** AI/ML 应该通过确保准确的分类、估值和报告来改善对法规的遵循。成功体现在更高的合规率、更少的法规违规和更有效的执法行动；
- **安全性**AI/ML 应该通过增强监视、检测非法货物和防止走私来加强边境安全。有效性通过提高检测率、更强的监控能力和更好的与执法机构的协调来评估。

通过评估这些方面，海关管理机构可以衡量其 AI/ML 项目在实现战略目标和提高整体绩效方面的有效性。

12.1.5 用户采用和满意度

成功的一个关键衡量标准是用户采用率和满意度。海关管理机构应该评估海关官员和其他利益相关者在多大程度上采用 AI/ML 系统，以及他们是否发现这些工具在日常工作中有用。这可以通过以下方式评估：

- **培训和易用性：** 衡量用户对新 AI/ML 系统的培训情况和舒适度；
- **反馈调查**收集关于 AI/ML 工具如何改善或影响海关官员、合规团队和其他用户工作流程的反馈。

12.1.6 成本效益分析

成功的一个重要衡量标准是 AI/ML 项目的投资回报率 (ROI)。海关管理机构应该进行成本效益分析，以评估 AI/ML 系统的长期收益是否超过开发、实施和维护的成本。成功可以通过系统提供的程度来衡量：

- **通过减少人工处理和自动化实现的长期成本节省；**
- **通过更好的欺诈检测、关税征收和合规执法实现的收入增长；**
- **通过增强风险评估带来的有效性提升，导致更快的海关清关时间和减少检查。**

12.2 经验教训

为了有效融入 AI/ML 项目中的“经验教训”，海关管理机构可以采取几项关键措施：

1. **正式的知识共享平台**建立一个集中化的存储库，项目团队在其中记录挑战、解决方案和经验教训。定期举行内部知识共享会议，如研讨会和讲座，可以帮助跨部门传播这些见解，确保团队在未来的 AI/ML 项目中更有准备。
2. **实施后评审：** 在项目完成后进行评审，以分析有效和无效之处。这些评审应涉及关键利益相关者，关注技术、操作和流程相关的经验教训。在项目生命周期内融入反馈循环，使海关管理机构能够不断完善和调整其战略。
3. **培训和发展计划**利用经验教训更新员工培训计划，并建立导师机会，让经验丰富的团队指导新采用者。这确保员工能够应用最佳实践，并避免重蹈过去的错误，有助于建立关于 AI/ML 的制度知识。
4. **跨机构合作**与其他海关管理机构或相关机构分享经验教训，以促进集体学习。通过协作论坛、研讨会或会议，海关管理机构可以交流见解和最佳实践，帮助缩小新兴和先进采用者之间的数字鸿沟。

13 结论：人工智能/机器学习作为转变的催化剂

将AI/ML整合到海关业务中代表了复杂全球环境中管理贸易、合规和执法方式的战略转变。本报告探讨了AI/ML采用的深远影响，涵盖了技术能力、法律框架、政策考虑、实施策略和案例研究。

AI/ML技术为海关管理提供了战略转折点，使其能够实现渐进式改进和革命性转变。渐进式增强专注于精简操作、改善风险分析和自动化重复任务。高级应用，包括生成性AI，开启了革命性能力的大门，例如使用大语言模型实时验证海关申报、发票和原产地证书，或将大语言模型与图神经网络（GNN）结合，以分析、可视化和综合运输数据、海关记录和社交网络中的模式。

本报告强调的一个关键主题是采用AI/ML的结构化和增量式方法的重要性。鼓励各成员海关从针对具体应用场景的小型高影响力试点项目入手，先取得快速成果，然后再逐步扩展到更先进和集成的系统，许多海用的一个例子是利用AI驱动的算法来提高商品分类和估值的准确性，从而减少海关处理和货物放行的时间。这种分阶段的方法可以在展示早期可衡量的利益时最小化风险。

成功实施的关键在于认识到AI/ML的采用不是一次性的工作，而是一个迭代过程必须持续监控绩效，更新模型并整合试点项目的见解，以优化策略并增强结果。这不仅需要在基础设施和工具上的投资，还需要在促进灵活性、适应性和问责制的治理框架上的投资。此外，对基于云的解决方案和混合架构的强调突出了可扩展和具有成本效益的实施策略，使不同准备程度的海关管理能够接触到AI/ML的采用。

解决伦理、法律和监管方面的考虑的重要性不容低估。由于AI系统高度依赖数据，必须优先考虑确保质量、完整性和符合隐私法规的数据治理框架。建立减轻偏见的保障措施、确保AI决策过程的透明性，以及实施人机协作系统以保持问责制是负责任的AI/ML采用的关键要素。此外，报告强调了与新兴国际AI法规保持一致的必要性，以促进各辖区之间的一致性和法律合规。

人为因素仍然是AI/ML采用成功的关键。通过有针对性的培训项目和合作伙伴关系建设组织能力，对于维持以AI驱动的转型至关重要。在技术和非技术员工中发展AI/ML素养，创造专业角色并促进协作实践，使海关管理能够有效利用AI/ML能力。同样重要的是促进利益相关者参与，确保开放沟通并纳入反馈机制以建立信任和推动采用。

总之，AI/ML技术为转型为数据驱动、灵活和智能的组织提供了前所未有的机会。通过利用AI/ML，海关管理可以加强其作为安全和高效贸易的促进者的角色，同时应对监管和执法挑战。然而，这种转变需要一种平衡的方法——从渐进步骤开始，优先考虑道德标准并投资于长期能力

建筑物。凭借战略眼光和仔细规划可以释放人工智能/人工智能的全部潜力，确保未来几年的可持续现代化和全球竞争力。

***

*

联系我们

Smartcustoms@wcoomd.org

访问我们的网站

wcoomd.org/SmartCustoms.aspx

World Customs Organization

Rue du Marché30,B-1210
Brussels,比利时

#WCOOMD
wcoomd.org