McKinsey Digital

QuantumBlack, AI by McKinsey

生成式AI: CEO必读指南

生成式AI (Generative AI) 在飞速演进， CEO们也在探索其商业价值及潜在风险。为此，我们提供一份生成式AI核心概要，供广大CEO们参考。

本文由*Michael Chui*、*Roger Roberts*、*Tanya Rodchenko*、*Alex Singla*、*Alex Sukharevsky*、*Lareina Yee*和*Delphine Zurkiya*共同撰写，谨代表*Mckinsey Digital*旗下科技委员会（*McKinsey Technology Council*）和*QuantumBlack, AI by McKinsey*的观点。

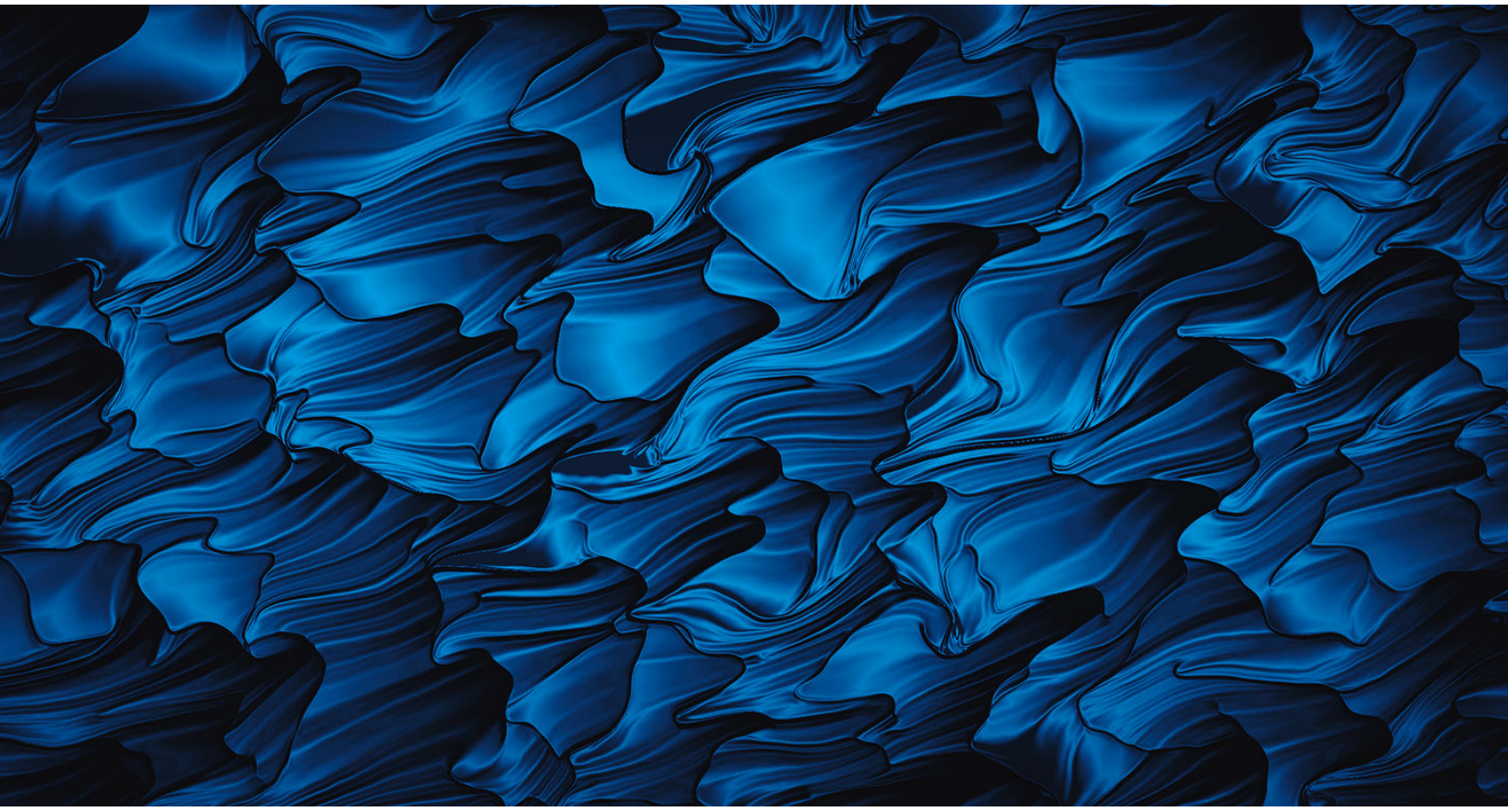


Image created by Chris Grava / Darby Films using a node-based visual programming language

2023年5月

自ChatGPT、Bard、Claude、Midjourney以及其他内容生成工具问世以来，人们对生成式AI抱有很高期待。各企业CEO自然也在思考：这究竟是科技炒作，还是颠覆行业格局的机遇？如果是后者，那生成式AI能给自身业务带来什么价值？

ChatGPT的大众版仅两个月就吸引到1亿用户。它以史无前例的方式推动了AI的普及，已成为迄今增长最快的应用程序。无与伦比的易用性让生成式AI有别于以往所有AI技术。用户不需要专修机器学习就可以开展交互、获取价值——只要会提问，几乎人人都能用。就像个人电脑或iPhone等其他突破性技术一样，一款生成式AI平台可以衍生出许多应用程序，适用于各个年龄段和教育水平的用户群体，人们无论身处何地，能够上网即可使用。

而实现这一切，依靠的是驱动生成式AI聊天机器人的基础大模型，它们是经由大量非结构化、无标签数据（如文本、音频等各类形式）训练的庞大神经网络。基础大模型可处理各种各样的任务。相比之下，以往的AI模型通常适用范围更“窄”，往往只能执行一项任务，如预测客户流失率等。而一个基础大模型则既能为一份2万字的量子计算技术报告生成内容摘要，又能为园艺公司起草市场进入策略，还能根据冰箱里的10种食材给出5张不同的食谱。不过，在其丰富功能的背后，目前还存在结果不够准确的短板，这也让人们再度关注起AI的风险管理问题。

在监管得当的情况下，生成式AI不仅可以为企业开辟新用例，还可以加速、扩展或改进现有用例。以电销场景为例，经过专门训练的AI模型可以帮助销售人员发现追加销售机会，但截至目前，这些模型通常还只能根据通话前收集的人口统计信息和购买规律等静态客户数据来判断追加销售的可能性。生成式AI工具则可根据实际对话内容，利用内部客户数据、外部市场趋势和社交媒体影响者数据，实时为销售人员提供追加销售建议。同时，生成式AI还可以为销售人员撰写销售话稿，供其根据具体情况进行调整。

上述例子只展示了AI技术对人类工作潜在影响的一个侧面，而实际上，几乎所有知识工作者都有可能因使用生成式AI而获益。尽管生成式AI最终可能会让部分工作自动化，但其价值将更多来自于被嵌入日常工具（如电子邮件或文字处理软件）后知识工作者对它的使用。这类升级后的工具可以大幅提高生产力。

CEO们想知道是否应立即采取行动，以及如果采取行动，该从何开始。有些人可能从中看到了机遇，希望通过重塑人与生成式AI应用程序协同工作的方式，在竞争中弯道超车。其他人则可能希望谨慎行事，在进行大规模投资之前先尝试几个用例，增进对生成式AI的理解。企业也需要评估自身是否具备必要的技术专识、技术及数据架构、运营模式以及风险管理流程，这些是更进一步部署生成式AI时所需要的。

本文旨在帮助CEO及其团队思考生成式AI的价值创造场景以及如何开始应用。首先，我们总结了生成式AI的入门指南，以帮助CEO更好了解AI日新月异的发展现状和可行技术选择。第二部分将通过4个旨在提高组织效能的案例，探讨企业如何应用生成式AI。这些案例来自我们对早期采用者的观察，并介绍了在技术、成本和运营模式要求等方面的各种选择。最后，我们将探讨CEO如何发挥关键作用，利用生成式AI带领企业走向成功。

人们对生成式AI的期待显而易见，企业高管自然希望借此东风运筹帷幄，有计划地快速推进。我们希望本文能让商业领袖更全面了解生成式AI未来潜力。

生成式AI入门指南

生成式AI技术飞速发展（见图1）。发布周期之短、初创公司数量之众、与现有软件的整合之快，皆不同凡响。在本节，我们将探讨生成式AI应用的广度，并简要介绍该技术，包括阐明其与传统AI的区别。

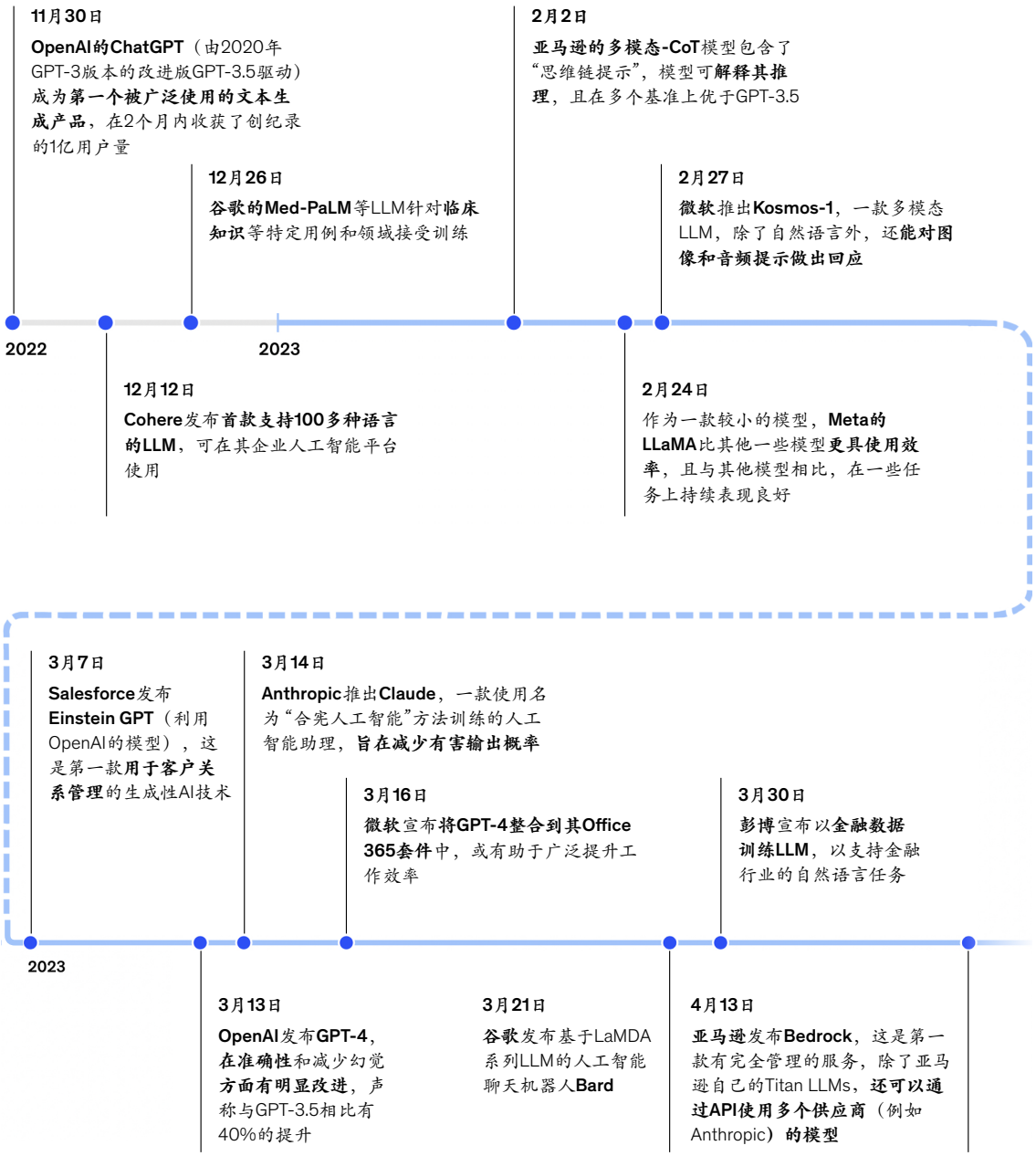
不仅是聊天机器人

生成式AI可用于工作自动化、辅助强化与加速推进。从本文宗旨出发，我们将着重阐述生成式AI如何辅助并强化人类工作，对其替代人类工作的潜力不作探讨。

图1

生成式人工智能技术飞速演进

在ChatGPT推出后的几个月里，主要大型语言模型（LLM）的发展时间线



ChatGPT等文本生成式聊天机器人备受关注，不过，生成式AI同样可以在图像、视频、声音以及计算机代码等更广泛的内容领域提供助力。在企业，生成式AI也可以发挥广泛功能，比如分类、编辑、总结、回答问题和起草内容。针对上述每项活动，各个业务职能和工作流程的具体工作方式转变都有可能创造价值，部分示例如下:

分类

- 反欺诈分析师可以将交易描述和客户文件输入到生成式AI工具中，要求其识别欺诈交易。

- 客户服务经理可以使用生成式AI工具根据客户满意度对客户通话音频文件进行分类。

编辑

- 撰稿人可以利用生成式AI纠正语法，并使文字风格与顾客的品牌调性相匹配。

- 平面设计师可以利用生成式AI从图像中移除过时标志。

总结

- 制片助理可以用数小时的活动录像创作精彩视频集锦。

- 业务分析师可以创建维恩图(Venn diagram)总结高管发言要点。

回答问题

- 制造企业员工可以向基于生成式AI的“虚拟专家”咨询有关操作流程的技术问题。

- 消费者可以向聊天机器人询问新家具的组装方式。

起草内容

- 软件开发者可以让生成式AI完成整段代码，或者提供建议以补全现有代码的未完成语句。

- 营销经理可以使用生成式AI起草不同版本的营销活动信息。

随着技术的发展和成熟，这类生成式AI可以更好地融入企业工作流程，实现任务自动化并直接执行特定操作（例如，在会议结束时自动发送纪要）。该领域已经有一些工具面市。

生成式AI与其他AI的不同之处

顾名思义，生成式AI和过往AI技术或分析工具的主要区别在于，该技术能够生成新内容，所生成的新内容通常以“非结构化”形式（如书面文本或图像）呈现，而非以表格形式排列（见侧边栏《术语表》中的生成式AI相关术语）。

其底层技术是一类被称为基础大模型的人工神经网络，其灵感来自于人类大脑中数十亿相互连接的神经元。人工神经网络需要通过深度学习加以训练，“深度”即指神经网络中的层数之众、之深。深度学习技术推动了AI领域的众多新进展。

而某些特质使得基础大模型区别于过往的深度学习模型。首先，训练基础大模型可以使用体量庞大、类型多样的非结构化数据。例如，一类被称为大型语言模型的基础大模型可以通过互联网上公开可用且涵盖各类主题的大量文本进行训练。其他深度学习模型虽然也可以处理大量非结构化数据，但训练所用的数据集通常更具体。例如，为了让模型识别照片中的某些物体，需要使用一组特定图像对其进行训练。

事实上，其他深度学习模型往往只能执行一项此类任务。例如，它们要么对照片中的物体分类，要么执行预测等其他功能。相比之下，基础大模型可以同时实现上述功能，并且还能够生成内容。上述能力的积累是通过从所摄取的广泛训练数据中学习规律和关系实现的，比如，通过规律和关系学习，基础大模型能够预测句子中的下一个单词。这就是为什么ChatGPT能够回答不同主题的问题、而DALL-E 2和Stable Diffusion能够根据描述生成图像。

术语表

应用程序接口 (*API*) 是一种通过编程访问 (通常是外部的) 模型、数据集或其他软件的方式。

*AI*是指软件有能力执行过去需要人类智能才能完成的任务。

深度学习 (*deep learning*) 是机器学习的分支，使用由相互连接的多层"神经元"组成的深度神经网络，这些连接具有可训练的参数或权重。它在学习图像、文本和音频等非结构化数据方面尤为有效。

微调 (*fine-tuning*) 是指调试预训练模型以使其更好地处理特定任务的过程。这需要在相对较短的时间内，通过标记的数据集进行训练，这个数据集比最初训练模型的数据集小得多。这一额外训练使模型能够学习并适应较小数据集中的细微差异、术语和特定规律。

基础大模型 (*foundation model, FM*) 是基于大量非结构化、无标签数据训练的深度学习模型，可以直接用于广泛的任务，也可以通过微调适应特定任务。GPT-4、PaLM、DALL·E2 和Stable Diffusion便属于这类模型。

生成式*AI* (*Generative AI*) 通常指使用基础大模型构建的AI，具有以往AI所没有的能力，比如生成内容的能力。基础大模型也可用于非生成性目的 (例如，根据通话记录将用户的情绪分类为负面或正面)，这类用例的结果相较早期模型有明显改进。为方便起见，本文在提到生成式AI时，包括所有基础大模型用例。

图形处理器 (*graphics processing units, GPU*) 是计算机芯片，最初为制作计算机图形 (如视频游戏) 而开发，同样可支持深度学习应用。相比之下，传统的机器学习和其他分析工具通常在被称为计算机"处理器"的中央处理器 (CPU) 上运行。

大型语言模型 (*large language model, LLM*) 是一类基础大模型，可处理大量非结构化文本，学习单词或词组 (称为token) 之间的关系。这使得大型语言模型能够生成自然语言文本，执行总结或提取知识点等任务。GPT-4 (ChatGPT的基础大模型) 和LaMDA (Bard的基础大模型) 均是大型语言模型。

机器学习 (*machine learning, ML*) 是AI的一个分支，在该领域中，模型接受训练、学习大量样例数据点之后获得能力。机器学习算法通过处理数据和经验 (而非接收明确的编程指令) 来发现规律并学习如何做出预测和推荐。算法也会自我调试，能对新的数据和经验做出更有效的反应。

*MLOps*指的是扩展和维持*AI*和机器学习的工程模式和实践，包括一整套覆盖整个机器学习生命周期的实践 (数据管理、开发、部署和实时运营)。目前，这些实践很多都由辅助软件 (任务标准化、简化或自动化工具) 支持或优化。

提示工程 (*prompt engineering*) 是指设计、改进和优化输入提示以引导生成式*AI* 模型产生所需 (即准确) 输出的过程。

结构化数据 (*structured data*) 是指以表格、数据库或电子表格等形式呈现的数据，能够有效地用于训练某些机器学习模型。

非结构化数据 (*unstructured data*) 指缺乏统一格式或结构的数据 (例如文本、图像和音频文件)，通常需要使用更先进的技术以生成见解。

鉴于基础大模型的多功能性，企业可以使用同一模型实现多个业务用例，这是早期深度学习模型难以实现的。一款纳入了公司产品信息的基础大模型可能同时用于回答客户问题和协助工程师开发新版产品。因此，企业可以搭建应用并更快实现收益。

然而，基础大模型当前的运行方式决定了它们并不适用于所有类型的应用。例如，大型语言模型容易产生“幻觉”，用看似可信、实则错误的论断回答问题（见侧边栏《负责任地使用生成式AI》）。此外，基础大模型并不总能给出作答的基本推理或依据来源。这意味着在错误可能造成损害、或需要对回答进行解释的情况下，企业对应用无人监督的生成式AI需慎之又慎。生成式AI目前也不适用于直接分析大量的表格数据或解决高级数值优化问题。研究人员正在努力克服这些限制。

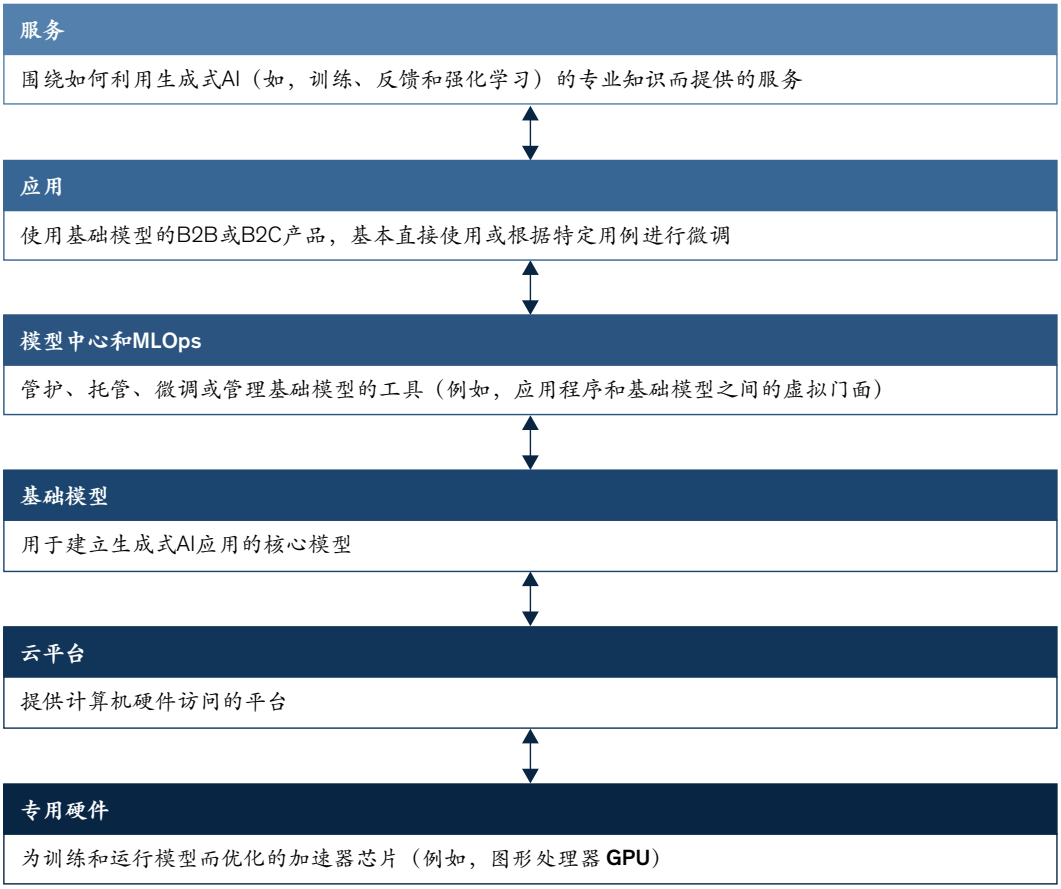
生成式AI生态系统正在兴起

基础大模型是生成式AI的“大脑”，而正在兴起的整个价值链将支持该技术的训练和使用（见图2）[1]。专用硬件提供了训练模型所需的庞大算力。云平台则提升了对这类硬件的利用。MLOps和模型中心供应商提供企业所需工具、技术和实践，让企业能够调试使用基础大模型并将其部署到终端用户应用之中。许多公司正在进入市场，主打依托基础大模型、能够执行特定任务的应用程序，例如帮助某公司处理客户服务问题。

图2

支持生成式AI系统的价值链正在迅速发展

生成式AI价值链



[1] 更多信息请参阅麦肯锡2023年4月26日《在生成式AI价值链中探索机遇》

负责任地使用生成式AI

生成式AI伴生了各种风险。企业CEO需要一开始从团队和流程设计上就做好风险防控。这不仅是为了满足不断变化的监管要求，也是为了保护业务并赢得消费者的数字信任（我们将在后文中提供关于这一点的方法建议）[1]。

公平性：不完美的训练数据或开发模型工程师的决策瑕疵，可能让模型产生算法偏向。

知识产权（*IP*）：训练数据和模型输出可能带来重大的知识产权风险，包括侵犯版权、商标权、专利权或其他合法受到保护的材料权利。即便所使用的生成式AI工具来自供应商，企业也需要了解训练过程中使用了哪些数据以及这些数据在工具输出中的使用方式。

隐私性：如果用户的输入信息以某种可识别个人身份的形式出现在模型输出中，则可能引发隐私问题。生成式AI也可能被用于创作和传播虚假信息、深度伪造和仇恨言论等恶意内容。

安全性：生成式AI有可能被不法分子用来加剧网络攻击的复杂程度和侵害速度，也可被操纵用于制造恶意输出。例如，通过名为“提示注入”（prompt injection）的技术，第三方可以给模型提供新的指令，诱导模型产出模型制作者和终端用户用意之外的输出。

可解释性：生成式AI依赖拥有数十亿参数的神经网络，人们因而很难解释某个答案从何而来。

可靠性：模型对相同的提示会产生不同的回答，使用户难以评估输出的准确性和可靠性。

组织影响：生成式AI可能会对劳动力产生重大影响，对某些特定群体和社区的负面影响可能尤为巨大。

社会和环境影响：基础大模型的开发和训练可能会危害社会和环境，包括增加碳排放（例如，训练一个大型语言模型可能会排放约315吨二氧化碳）[2]。

---

[1] Jim Boehm、Liz Grennan、Alex Singla和Kate Smaje 2022年9月12日《为什么数字信任真正重要》（“Why digital trust truly matters”）。
[2] Ananya Ganesh、Andrew McCallum和Emma Strubell 2019年6月5日《深度学习在自然语言处理中的能源和政策考虑》（“Energy and policy considerations for deep learning in NLP”）《计算语言学协会第57届年会论文集》（Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics）。

鉴于训练模型需要庞大的计算资源而完善模型需要大量人力，因而首款基础大模型的开发需要巨大的投资。这导致相关开发工作被部分科技巨头、有充足投资支持的初创公司以及一些开源合作研究机构（例如BigScience）主导。然而，针对有效处理若干任务的小规模模型的研究、以及提高训练效率的工作，均方兴未艾。这最终可能为更多企业打开市场。部分初创公司已经成功开发了自己的模型，例如，Cohere、Anthropic和AI21实验室都建立并训练了自己的大型语言模型。

将生成式AI应用于工作

CEO们应将探索生成式AI列入工作议程，不能仅视之为“可选项”。生成式AI可通过广泛用例创造价值。起步的经济和技术要求并非高不可攀，而无所作为则可能导致迅速被竞争对手甩开。每一名CEO都应同管理团队一起思考竞争领域与方法。一些CEO可能会认定，生成式AI将为企业带来变革性机遇，全面重塑从研发到营销、从销售到客户运营等各个领域。还有些CEO则可能选择从小处着手，再逐渐扩大规模。一旦做出决策，AI专家便可根据场景需要，通过相应技术路径执行战略。

生成式AI在企业中的很多应用（尽管未必是全部价值）将来自员工对现有软件中新嵌入功能的使用。电子邮件系统可以给出邮件初稿；生产应用将根据描述生成演示文稿的初稿；财务软件可对财务报告中的要点给出文字描述；客户关系管理系统则可以提供客户互动建议。这些功能可以提高所有知识工作者的生产效率。

然而，在某些用例中，生成式AI或可带来更具变革性的影响。接下来，我们将介绍不同行业企业利用生成式AI重塑组织工作方式的4个范例[2]，范围涵盖了从资源需求极少到资源投入很高的不同情况。（这些例子的快速比较和更多技术细节，请参见图3。）

图3

生成式AI对组织的要求从低到高不等，具体取决于用例

低 ——— 高

用例	技术路径	成本	技术人才	专有数据	流程调整
改变软件工程工作	使用软件即服务（SaaS）工具	许多SaaS工具提供固定费率的订阅服务，每名用户每月10至30美元；一些产品则按使用情况定价	不太需要技术人才——可能负责选择合适的解决方案和轻度的整合工作	模型基本是直接使用的，因此不需要专有数据	流程基本保持不变，但工作人员应系统地检查模型结果的准确性和适当性
帮助客户经理跟上公共信息和数据的步伐	通过模型API构建软件层	需要前期投资开发用户界面、整合解决方案并建立后处理层 API使用和软件维护的持续成本	需要软件开发、产品管理和数据库集成能力，因此需要至少1名数据科学家、机器学习工程师、数据工程师、设计师和前端开发人员	模型基本是直接使用的，因此不需要专有数据	可能需要一些流程以实现对提示和结果的存储，可能也需要一些防护机制，出于风险或成本考虑而限制使用
解放客户支持代表时间进行更有价值的工作	内部对开源模式进行微调	数据清理和标记以及模型微调导致人力资本成本增加，初始成本比基于API构建高出约2倍 模型维护和云计算的持续成本更高	经验丰富的数据科学和工程团队，拥有机器学习运营（MLOps）知识和资源，可以检查或创建所需的标签数据	需要专有、带标签的数据集以微调模型，尽管在某些情况下该数据及可能相对较小	需设置流程以管理分流、将问题上报人工处理以及对模型安全做定期评估
加快研究者识别相关细胞特征的速度，助力药物发现	从零开始训练基础模型	前期人力资本和技术基础设施成本导致初始成本比基于API构建高出约10-20倍 模型维护和云计算的持续成本与上一条类似	需要大型数据科学和工程团队，具备博士水平的学科知识、MLOps最佳实践以及数据和基础设施管理技能	基础模型可以通过大量公开数据训练，但长期的差异性优势来自于增加自有的标记或未标记数据（更易于收集）	包括以上所有流程，在对外部数据进行训练时，需要开展彻底的法律审查，以防止发生知识产权问题

[2] 这些范例来自我们客户工作和公开案例的汇总整理，而非反映特定公司的具体事例。

改变软件工程工作

第一个范例的复杂度相对较低，使用现成的生成式AI解决方案，不需要内部定制，因而可以立即提高生产力。

软件工程师绝大部分工作内容是编写代码。这个过程劳神费心，需要大量的试错以及对私域和公域文件的研究。某公司由于缺少足够的熟练软件工程师，功能和错误修复请求被大量积压。

为了提高工程师的工作效率，该公司使用了一款基于AI的代码补全产品，该产品被整合到工程师的编码软件之中。工程师可以使用自然语言撰写代码描述，而AI提供若干满足该描述要求的代码块变体。工程师可以从中做出选择，进行必要改进，然后点击插入代码。

我们的研究表明，这类工具可以让开发人员生成代码的速度提升高达50%。它还可以帮助调试纠错，提高开发产品质量。不过，生成式AI目前并不能取代熟练的软件工程师。事实上，较有经验的工程师从这些工具中获益最多，工作效率提升幅度最大，该产品对缺乏经验的开发者则效果一般，有时甚至有负面影响。其中一项已知风险在于，AI生成的代码可能包含漏洞或其他错误，因此必须有软件工程师亲身参与，以确保代码的质量和安全性（见本文最后一节，了解减轻风险的方法）。

这一现成的生成式AI编码工具成本相对较低，上市所需时间短，因为该产品已经可用，不需要进行大量的内部开发。具体成本因软件供应商而异，使用费为每户每月10到30美元不等。在选择工具时，企业一定要向供应商了解许可和知识产权问题，以确保生成的代码不会违规。

这款新工具需要由一支跨职能的小团队负责支持，他们主要负责选择软件供应商并监控性能，其中也包括检查知识产权和安全问题。工具实施只需工作流程和政策方面的变更。由于该工具完全是现成的软件即服务（SaaS）类型，额外的计算和存储成本极低或为零。

帮助客户经理及时了解公共信息和数据

有些企业可能决定利用基础大模型（通过API或开放模型）构建自己的生成式AI应用，而非使用现成工具。其投资要求高于上一范例，但这样做有助于以更加定制化的方法满足公司的具体环境和需求。

在本例中，一家大型对公银行希望利用生成式AI提高客户经理的工作效率。客户经理为及时了解客户情况和当前重点，需要花大量时间阅读企业年报和业绩发布会记录等篇幅庞大的文件。这一工作让客户经理能够为客户提供契合其特定需求的服务。

该银行决定通过API接通基础大模型，构建解决方案。该解决方案可以快速查阅文件并为客户经理的提问总结答案。银行围绕基础大模型构建了额外软件层，以优化用户体验、实现工具与公司系统的整合并进行风险与合规控制。由于一些大型语言模型会产生"幻觉"误导，因而尤其需要对模型输出进行检查，正如金融机构会检查初级分析师的工作输出。客户经理也要接受培训，学会用适当的提问方式获得最精准的回复（也称"提示工程"）。相应的工具输出和信息来源的简化验证流程也已落实到位。

在本例中，生成式AI可以加快客户经理的分析过程（从几天缩短到几小时），提高工作满意度，并有机会捕捉到客户经理可能会忽视的想法。

开发成本主要集中在用户界面的构建和集成工作，这一工作需要数据科学家、机器学习工程师或数据工程师、设计师和前端开发人员投入时间。运营支出包括软件维护以及使用API的费用。具体成本取决于模型选择和第三方供应商费用、团队规模以及达到最简可行产品所需的时间。

减少客户服务用时，让客服代表有时间去做更有价值的工作

更复杂一些的应用是对基础大模型进行微调。在本例中，一家公司采用了针对对话场景进行优化的基础大模型，并使用自有的高质量客户聊天记录及行业特有的问答对基础大模型进行微调。公司所处行业会使用专业术语（例如法律、医学、房地产和金融）。客户服务速度是竞争优势的重要来源。

这家公司的客户服务代表每天要处理数百个来电咨询，响应时间有时过长，导致用户不满意。该公司决定引入生成式AI客服机器人来处理大部分客户需求。其目标是以符合公司品牌和用户偏好的方式回应客户。微调和测试基础大模型的一个环节是确保回复与公司设定的领域术语、品牌承诺和风格基调保持一致；这需要进行持续监控以评估系统在包括顾客满意度等多个维度上的表现。

该公司创建了多阶段的产品路线图，以最大程度减少潜在的模型错误。第一阶段，公司对聊天机器人进行了内部试点。员工可以给模型的建议“点赞”或“拍砖”，而模型能够从这些输入中学习。下一步，模型“旁听”客户服务对话并提供建议。当技术经过充分测试后，第二阶段开始，模型直接面向客户使用，并保持一名真人员工参与。最终，当公司领导者对技术有十足信心时，便可以实现大面积自动化。

在本例中，生成式AI解放了客服代表，使其能够专注于价值更高和更复杂的客户咨询工作，既提高了员工效率和工作满意度，也提升了服务水平和客户满意度。该机器人可以访问所有的客户内部数据，并能“记住”先前的对话（包括电话通话），明显领先于现有的客户聊天机器人。

为实现效益，该用例需要在软件、云基础设施和技术人才方面进行较大投资，并在风险和运营方面进行更高水平的内部协调。一般而言，微调基础大模型的成本是借助API建立一个或多个软件层的两到三倍。云计算所需的人才和第三方成本（若微调自托管模型）或API费用（若通过第三方API微调）是主要的成本增量。为实施解决方案，公司需要数据运营和MLOps专家的帮助，也需要如产品管理、设计、法务和客户服务专家等其他职能部门的输入。

加速药物发现

当没有合适的基础大模型可用，公司需要从头建立模型时，就会出现最复杂且定制化程度最高的生成式AI用例。这一情形可能会出现在专业性较强的行业，或者在所处理数据集与现有基础大模型训练所用数据集大不相同的情况下，接下来介绍的医药行业用例正属此类。从头训练基础大模型会伴生技术、工程和资源方面的巨大挑战。使用性能更高的模型所带来的额外投资回报应当超过相应的财务和人力资本成本。

在本例中，一家制药公司的药物发现研究人员必须根据显微镜图像决定后续实验。研究者们拥有百万量级的图像数据集，其中包含了大量与药物发现有关、人眼难以解读的细胞特征视觉信息。这些图像用以评估潜在的候选治疗方法。

该公司决定创建一款工具，帮助科学家了解药物化学与显微镜图像记录之间的关系，以加速研发工作。由于这种多模态模型仍处于起步阶段，该公司决定训练自有模型。为了建立这一模型，团队成员同时使用了训练图像类基础大模型的真实世界图像和公司内部的庞大显微镜图像数据集。

训练后的模型能够预测可能导致有利结果的候选药物，并能提高精准识别相关细胞特征的能力，为药物发现增加价值。这让药物发现过程更高效、更有效，不仅缩短了价值实现时间，还减少了不准确、具有误导性或最终失败的分析次数。

一般而言，从零开始训练模型的成本是围绕模型API创建软件所需成本的10到20倍。更大规模的团队（包括博士水平的机器学习专家）以及更高的计算和存储支出是主要的成本增量。训练基础大模型的预计成本因所需的模型性能水平和建模复杂性而存在较大差异。上述因素影响到所需的数据集大小、团队组成和计算资源。在本用例中，工程团队和持续的云服务费用耗费了大部分成本。

该公司发现需要对技术基础设施和流程进行重大升级，包括访问多个GPU实例以训练模型，获取各类工具以在多个系统间调配训练，以及部署MLOps最佳实践来限制成本和项目持续时间。另外，要对数据进行收集、整合（确保不同数据集的格式和分辨率一致）和清理（过滤低质量数据，删除重复数据，并确保数据分配符合预期用途），这涉及大量处理工作。由于基础大模型从零开始训练，因此最终模型需要经过严格测试，以确保输出准确、使用安全。

上述案例对CEO的关键启示

上述用例为CEO们应用生成式AI带来一系列启示:

— 为工作和职场带来切实效益的变革性用例已然存在。从制药业、银行业到零售业，众多企业正在建立一系列用例，以捕捉价值创造潜力。具体入手点可大可小，取决于企业的目标抱负。

— 应用生成式AI的成本差异很大，影响因素包括用例和软件所需数据、云基础设施、技术专识和风险缓解措施。无论用例如何，企业必须考虑风险问题，在此，某些用例会需要更多资源投入。

— 快速起步有其优势，率先建立起基本的业务逻辑将帮助公司更好应用生成式AI。

起步时需考虑的因素

CEO在推动企业关注生成式AI方面发挥着重要作用。在结尾部分，我们将探讨CEO在踏上征途时需要熟记的策略，其中有很多与过往技术浪潮兴起时企业高管应当做出的反应一致。然而，生成式AI也带来了独有的挑战，这包括其超越以往技术变革的空前发展速度及随之而来的应对难度。

跨职能部署生成式AI

过去，许多组织以孤立试验的方式启动对传统AI的探索。然而，鉴于生成式AI独特的风险考量以及基础大模型支撑全组织、多用例的能力，企业应当以更加精细和协调的方法加以管理。例如，使用专有数据进行微调以反映企业品牌特质的模型，可以在多个用例（如生成个性化的营销活动和产品描述）和多个业务职能（如产品开发和营销）中加以部署。

为此，我们建议组建由公司领导组成的跨职能小组（例如，代表数据科学、工程、法务、网络安全、营销、设计和其他业务职能）。这样的跨职能小组不仅可以发现并优先处理价值最高的用例，还能保证整个组织的执行协调一致且安全。

端对端领域重塑，而非仅专注于用例

生成式AI是可以改变组织运作方式的强大工具，对价值链中的特定业务领域（例如，零售商的营销或制造商的运营）具有特别的影响。生成式AI的部署十分便利，企业因而很容易将应用局限于全盘业务下的零星用例。因此，坚持全盘视角、按领域划分用例群至关重要，从这一视角出发进行规划能为全体业务职能带来最大的变革潜力。随着生成式AI与其他传统AI应用协同并进、此前无法实现的工作方式逐渐诞生，企业正在不断重新定义其目标状态。

实现满载的技术栈

现代化的数据和技术堆栈几乎是任何生成式AI策略成功的基础。CEO们应当向首席技术官了解以确定公司在计算资源、数据系统、工具和模型访问（通过模型中心的开源方式或通过API的商业模式）方面是否具备所需的技术能力。

例如，生成式AI的命脉是流畅获取具体业务背景或问题的相应数据。无法有效协调或随时使用自身数据的公司，将无法微调生成式AI以探索更多潜在的变革性用途。设计可扩展的数据架构同样重要，这包括数据治理和安全流程。根据不同的用例情况，现有的计算和工具配置基础设施（可以通过云供应商采购或在内部建立）可能也需要升级。明确的数据和基础设施战略应立足于从生成式AI中获得的业务价值和竞争优势。上述因素都至关重要。

打造“灯塔”

CEO们需要避免在规划阶段止步不前。新的模型和应用正迅速被开发和发布。例如，GPT-4在2023年3月发布，此前ChatGPT（GPT-3.5）发布于2022年11月，而GPT-3则是在2020年。在商业世界，时间尤为重要，而生成式AI技术的快节奏特性要求企业迅速行动以把握优势。CEO们可以采取下述几种方式稳步推进。

尽管生成式AI仍处于早期阶段，但应尽快在企业内部展示其对运营模式的重要影响，这可以通过“灯塔方法”来实现。例如，一种推进方式是打造“虚拟专家”，让一线员工能够利用专有的知识源，为客户提供最相关的内容。这一方法能提高生产力、激发热情，并使企业能够在向客户扩展应用之前，在内部对生成式AI展开测试。

和其他技术创新浪潮一样，“概念验证疲劳”将会出现，许多公司会陷入“试点炼狱”的困境。然而，鼓励概念验证仍然是快速测试和完善有价值业务用例、以便日后向邻近用例扩展的不二选择。通过聚焦产生有益结果的早期成功实例，企业可以积攒势头，以此为基础扩大规模，充分发挥生成式AI的多功能性。这一方法可以帮助企业推动更广泛的AI采用，营造创新文化，从而保持竞争优势。如上所述，企业需要组建跨职能领导团队，确保有计划地协调推动概念验证。

平衡风险与价值创造

正如此前详细介绍的4个范例所示，商业领袖必须在生成式AI所涉及的价值创造机会与风险之间取得平衡。我们近期的全球AI调查显示，尽管已有超过一半的组织采用传统AI技术，但大多数组织并未对相关的大部分风险采取应对措施[3]。生成式AI再次引发了人们对许多同类风险的关注，比如AI可能会让隐藏在训练数据中的偏向被固化；同时生成式AI还带来了一些新风险，比如产生幻觉的倾向。

因此，跨职能领导团队不仅要为生成式AI的使用建立总体道德原则和指导方针，还要对每个潜在用例所伴生的风险有全面了解。

重要的是，要寻找与组织的整体风险容忍度相一致的初始用例，并且设置相应结构以减轻相应风险。例如，零售组织可以优先考虑价值稍低但风险也较小的用例，比如创建营销内容初稿和其他需要人工参与的任务；同时，可能搁置价值更高、但风险更大的用例，比如自动起草和发送高度个性化营销电邮的工具。这种以风险为考量的做法能够让企业建立必要的控制机制，妥善管理生成式AI并保持合规。

CEO与其团队还要密切关注生成式AI监管的最新动态，包括与消费者数据保护和知识产权相关的规定，以保护公司远离法律纠纷。正如目前对AI和数据的监管，各国对生成式AI所采取的监管方式可能各不相同。企业需要调整工作方法以校准流程管理、文化和人才管理方式，确保能够规模化地应对快速发展的监管环境和生成式AI的风险。

应用生态系统方法建立合作伙伴关系

商业领袖应注重建立和维护平衡得当的联盟网络。企业的收购和联盟战略应继续聚焦建立合作伙伴生态系统，以适应不同的场景并解决生成式AI对不同技术栈层面的需求，同时要注意避免锁定供应商。

与正确的公司合作可以加速推进执行。企业不需要自己建立所有的应用或基础大模型，而是可以与生成式AI供应商和专家合作，更快地采取行动。例如，企业可以与模型供应商合作，为特定行业定制模型，或与提供可扩展云计算等能力的基础设施供应商合作。

企业可以借助他人的专业知识，让最新的生成式AI技术迅速地为我所用。然而，生成式AI模型只是冰山一角，价值创造还需要包括多个其他要素。

聚焦所需的人才和技能

为有效应用生成式AI创造商业价值，公司需要打造技术能力并提升现有员工的技能水平。这需要领导层共同努力，根据企业的优先用例确定所需能力，这可能不限于技术方面，也包括工程、数据、设计、风险、产品和其他业务职能的人才组合。

正如上文用例所示，技术和人才需求因具体实施的性质（从最简单的使用现成解决方案、到最复杂的从零建立基础大模型）而大不相同。例如，为了建立生成式模型，企业可能需要博士水平的机器学习专家；而如果要利用现有模型和SaaS产品开发生成式AI工具，一名数据工程师和一名软件工程师或许足以领导此工作。

除了雇用合适的人才，企业还需要培训现有员工。生成式AI应用程序使用基于提示的对话式用户界面，因而使用简便，但用户仍然需要优化提示输入，了解技术限制，并懂得在何时何地可以合理地把应用融入工作流程。领导层应提供使用生成式AI工具的明确指导方针，并开展持续的教育和培训，让员工了解其风险。培养自发研究和实验的文化也可以激发员工创新流程和产品，从而有效整合AI工具。

[3] 2022年12月6日麦肯锡《2022年AI现状及5年回顾》

多年来，企业一直在探索AI之路、追求宏远的目标，许多公司已经收获了新的收入来源、改进了产品、提升了运营效率。其中许多成功都源于AI技术，它们仍然是处理特定任务的最优工具，企业应继续保持这方面的努力。然而，生成式AI带来了又一次实现重大飞跃与无限可能的机会。虽然该技术的运营和风险框架还未完全建立，但商业领袖们深知应当启动生成式AI旅程。但从何开始，又如何开始？每家公司的答案不尽相同，公司内部也众说纷纭。有些企业放手一搏，而其他公司则从小规模试验起步。最佳方法将取决于公司的目标抱负和风险偏好。但无论目标如何，关键是要迈出第一步，边做边学。

Michael Chui是麦肯锡公司及麦肯锡全球研究院全球董事合伙人；**Roger Roberts**是麦肯锡全球董事合伙人，**Tanya Rodchenko**是麦肯锡全球副董事合伙人，**Lareina Yee**是麦肯锡技术委员会主席、麦肯锡全球资深董事合伙人，他们均常驻湾区分公司；**Alex Singla**是麦肯锡全球资深董事合伙人，常驻芝加哥分公司；**Alex Sukharevsky**是全球资深董事合伙人兼**Quantumblack, AI by McKinsey**全球负责人，常驻伦敦分公司；**Delphine Zurkiya**是麦肯锡全球资深董事合伙人，常驻波士顿分公司。