上海科学技术情报研究所
上海市前沿技术发展研究中心
技术与创新支持中心（TISC）

数字化城市
DIGITAL CITY BRIEFING

2021 年
第 21 期

人体互联网初探

编者按

人体互联网（Internet of Bodies，IoB），又称身体互联网、身联网，是一种能够连接人体和数据的传感器网络，这使得人类能够和机器进行一定程度的交流。互联网、传感器等多项技术的发展、融合带来了人体互联网时代，IoB 能够生成大量的生物识别和人类行为数据，推动健康研究、产业以及社会生活的其他方面的转型。目前，虽然对身体医疗健康数据的采集已经有较长时间的历史，但 IoB 仍处于初步发展阶段，其技术整合、政策监管等尚在探索阶段。

目　　录

技术

人体互联网在医疗健康领域技术及应用概述

一、人体互联网概念及演变

人体互联网（Internet of Body，IoB）并没有官方的定义，其概念是在不断应用中演变出来的，实质上 IoB 是指物联网与人体的连接，以某种方式在人体中植入 IoT 设备，把人体作为物联网的扩展。人体互联网以集成电路技术、能量供给技术、植入式电子系统材料、体内外双向通信技术，以及仿生技术为核心支撑，通过设备采集人体相关医疗数据达到远程监测人体健康，目前已有数字药丸、人工耳蜗等典型应用，其中无导线起搏器、神经刺激器等应用案例中还可通过设备采取相应的干预措施应对长期或突发的健康问题。未来随着材料、集成电路与人工智能技术的不断突破，人体互联网也许会克服隐私、安全、标准等问题而大规模应用。

第一代人体互联网主要用于人体外部，可监测人体健康的可穿戴设备，例如智能手环、智能手表等。第二代人体互联网主要用于人体内部，植入人体内部监测或控制人体健康的各个方面的设备，包括起搏器、人工耳蜗和植入体内的数字药丸等。第三代人体互联网是一种嵌入式技术，设备和人体融合在一起，能够远程、实时连接到后台。

二、人体互联网技术框架

表 1 人体互联网技术框架

技术	描述
植入式电子系统材料	埋植在人体内部的植入器械，其外壳封装材料和一些动作装置、传感器、探头均与体液和血液相接触，这些材料要保证绝缘、无毒、无腐蚀性，并具有良好的生物相容性。
传感器技术	可植入医疗传感器主要分为运动传感器、生物传感器和环境传感器。其中，生物传感器主要包括

	心率传感器、体温传感器、血压传感器、血糖传感器等。
医疗芯片技术	主要用于采集及处理关键生理信号，以此获得相应的生理信息，实时监控使用者的健康状况。其中的关键技术包括低功耗、全集成、低噪声等。
体内外双向通信技术	大部分植入设备通常由体内植入部分和体外测量与控制部分组成。植入式系统需要解决体内、外信息的交换问题，通常采用电磁波与红外线作为信息载体，完成信息的遥控与遥测。
仿生技术	仿造生命的各种功能，包括仿造生命体的 9 大功能，即自动调节、自动诊断、自动恢复、自我修理、自我监视、灵敏性、简单性、稳定性和耐久性。

三、人体互联网典型应用示例

人体互联网可用于多个方面，例如：数字药丸、神经刺激器、人工耳蜗、无导线起搏器等。

具体应用示例：人体物联网可以通过植入设备电刺激控制基因表达，APP 一键释放胰岛素。

来自体外的无线电信号激活植入物中的电子设备，电子设备将电信号直接传输到细胞，刺激钙、钾通道，也触发了控制胰岛素基因的细胞中的信号级联放大反应。经由电子设备对 β 细胞的无线电刺激，成功实现对囊泡胰岛素释放的实时控制，胰岛素水平 10 分钟内即可到达峰值。

四、人体互联网应用面临的问题

（1）隐私问题

在大多数国家/地区，关于个人健康的信息（例如病历，血液或组织样本）都有着严格的规定。但这些常规性法规通常无法涵盖通过人体互联网生成的新型健康数据，以及收集和处理这些数据的实体。

（2）标准规范

除了对隐私和敏感度的关注外，在处理由人体互联网生成的庞大数据方面还

存在着许多实际问题。由于缺乏安全性和数据处理方面的标准，因此不同设备的数据很难进行合并，也很难将其用于进一步研究。

（3）安全风险

人体互联网技术面临的最大挑战即是如何保护设备及其收集和传输的信息的安全。2017 年，美国食品药品监督管理局因需要固件更新的安全性问题召回了将近 50 万个起搏器。人体互联网技术所面临的安全挑战与困扰物联网的挑战相似，但是当涉及 IoB 设备时可能会造成生死攸关的后果。此外，IoB 设备还带来了另一项网络安全挑战，即需要防御黑客。

五、人体互联网未来趋势

人体互联网不仅仅是医疗健康领域的重大突破，也是物联网技术的一个成功实践。随着材料、集成电路与人工智能技术的不断突破，未来人体互联网也会达到一个新的高度。

（1）材料科学进步

1. 生物相容性提高；
2. 设备趋于微型化；
3. 使用期限大幅延长。

（2）集成电路、人工智能技术突破

1. 设备性能大幅加强；
2. 智能化水平不断提高；
3. 多类功能集成于一体。

资料来源：赛迪工业和信息化研究院.《工业新词话：人体互联网（第 114 期）》

人体互联网在医疗领域风险

IoB 能够带来诸多裨益。一方面，IoB 可能给人们带来主观上的好处，例如愉悦感和便利性；另一方，随着进一步了解患者的 IoB 信息，医疗服务提供者可以改善预防性保健治疗，及早发现疾病，提高诊断的准确性以及治疗的有效性。

身联网也面临来自各方面的风险。它与其他物联网和计算设备有相同的攻击媒介，除此之外，身联网设备由于收集了大量数据而增加了风险。

谁可能获得访问权限？	潜在漏洞有什么？	可能的后果是什么？
✧ 罪犯 ✧ 黑客（例如安全研究人员、业余爱好者、恶意攻击者） ✧ 数据经纪人 ✧ 数据融合中心 ✧ 雇主 ✧ 学校 ✧ 医疗保健机构 ✧ 保险公司 ✧ 制造商 ✧ 刑事司法系统 ✧ 政府	✧ 出于健康或功能目的，身体上依赖设备 ✧ 对敏感数据的收集、存储或传输 ✧ 互联网连接 ✧ 监管差距 ✧ 硬件 ✧ 软件	✧ 因故障或黑客入侵而导致死亡或人身伤害 ✧ 全球和国家安全挑战 ✧ 数据泄露 ✧ 未经知情同意而被动收集或共享数据 ✧ 数据滥用或意外使用 ✧ 个人身份泄露 ✧ 健康差距增加 ✧ 强制接受设备 ✧ 侵犯身体自主权

图 1 人体互联网风险概述

一、全球、国家和个人安全风险

通信系统可能成为其他国家和犯罪黑客的攻击目标。物联网和身联网设备连接性的增强可能会增加攻击面，引发更多漏洞。有的国家可以使用身联网数据来实施专制政权，因此，若身联网得到广泛采用也可能增加全球地缘政治风险。此外，广泛使用身联网可能增加间谍活动和个人数据被滥用的风险，也可能会给身体带来更多伤害。

二、网络安全风险

身联网设备所处的更广泛的生态系统也存在安全风险。植入或连接人体的物理设备与监视设备通过无线连接，将信息传输到云上，然后，外部方（例如设备制造商或医生）可以访问数据。上述过程中的硬件和软件、物理和逻辑通信路径以及组织边界都引入了多层复杂性，每层都易受故障、降级、损害和攻击的影响。除了设备本身的网络安全性之外，存储用户数据的数据库还必须具有足够的安全性和完备的安全控制措施。

三、数据和隐私安全风险

如果缺乏防止数据滥用的保护措施，数据收集过程可能会威胁身联网用户的隐私。收集过程本身，包括收集什么数据、收集频率、是否知情同意（尤其是在未成年人或被拘留者等弱势人群中）以及用户是否可以选择随时停止收集或转售数据，都可能会对隐私构成固有风险。目前，关于身联网设备生成数据的归属权，还没有法律规范。

四、伦理风险

首先是结果偏差风险。身联网技术带来的好处之一是可通过降低预防性和诊断性护理的成本，减少美国医疗保健结果中的差距，但目前尚不清楚这些技术是否会降低医疗保健成本，或是否能为普通民众提供方便。同时，医疗数据还容易受到输入偏差的影响。其次是自由风险。随着身联网设备变得越来越普遍，那些希望减少对这些设备的依赖性或希望与这些设备进行最少交互的人可能会面临身体或心理压力。一些组织试图使用身联网来管理员工，例如亚马逊已经为一种腕带申请了专利技术，它可以跟踪员工的行为，并发出提醒，以推动他们实现更高的生产力。

资料来源：唐巧盈.身联网已来,如何应对新挑战?[J].网络传播,2020(12):89-91.

政策

美欧 IoB 医疗健康数据监管政策法规

一、美国 IoB 数据监管情况

当前，美国没有一部全面的数据保护法来规范数据安全和个人隐私。IoB 技术产生的数据受到不同层级的法律和法规机构的监管：特定行业的联邦法律法规，联邦级反歧视法律，以及州、县和地方法律法规（如表 1 所示）。此外，美国的行业组织和论坛针对消费者健康和可穿戴产品的隐私和数据问题，提出了一系列的指南、行为准则、原则和方法。

表 1 美国联邦层级 IoB 数据监管的相关政策法规

类型	政策法规	相关监管内容
医疗领域		HIPAA 法案对受保护实体使用和披露“受保护域的健康信息”（PHI）进行了监管，并提供了两种可用于满足隐私规则的识别标准的方法的指南：专家决定法和安全港
消费者隐私	《联邦贸易委员会法》FTC Act	FTC Act 禁止公司从事欺骗或不公平的行为做法，包括未能遵守实体自身的隐私政策等。这使该法索成为适用于消费者 IoB 设备隐私和安全实践的主要联邦法规
多行业适用	《公平信息实践原则》FIP Ps	FIP Ps 原本是作为标准的广泛共识原则，现已演变成一套适用于不同

		隐私环境的的规则，具体涵盖医疗数据、金融数据、儿童/学生/消费者/驾驶员隐私等
金融	《格莱姆—里奇—布莱利法案》(GLBA)	GLBA 限制了金融机构收集的非公开个人信息的披露，但并不跟制个人信息或大数据分析用于个性化保险含同
消费者隐私	《公平信用报告法》FCRA	FCRA 对任何提供“消费者报告”的“消费者报告机构”进行了监管。相关数据主要用于协助确定消费者的信贷资格，涉及个人的信誉、信用状况、性格、一般声誉、个人特征，生活模式等
科研	《保护研究对象联邦法索》Connon Rulo	该法案适用于涉及收集或研究现有数据、文件、记录、病理标本或诊断标本的研究，但匿名或未经确认的信息明确免于监管
反歧视	《美国残疾人法》（ADA）	ADA 法案旨在消除对残疾人、有残疾记录的个人和被认为有残疾的个人的歧视性障碍。但它尚未监管可能对个人預测健康数据感兴趣的雇主、

		金融机构、营销人员和教育机构等
反歧视	《患者保护和平价医疗法》ACA	ACA 法素旨在保证与 ACA 资助的项目非歧视性。它禁止在某些保健方案和活动中基于种族、肤色、国籍、性别、年龄或残疾的歧视
反歧视	《遗传信息非歧视法案》GINA	GINA 法案护美国居民在医疗保险覆盖范围和就业环境中免受基因歧视，但是，它不包括其他形式的保险，如人寿保险、长期护理和残疾保险

表 2 美国 IoB 数据监管政策风险与差异

议题与风险	法规	监管差距	地方法律示例
“健康信息”的范围限定	HIPAA	不覆盖未纳入保护实体的直接连接消费者的医疗设备数据；不覆盖健康信息预测	《加州医疗信息隐私法案》（CMIA）将健康信息保护责任扩大到软件、硬件和在线服务提供商
金融和保险领域的歧视风险	FCRA， GLBA，CT NA （健康保险）	未能妥善处理人寿保险、长期护理保险和其他类型保险中使用健康信息，很少有	CCPA 不向政府机构施加法律义务，但在涉及第三方披露时可能相关； BIPA 监管

		措施解决大数据分析的风险	私人实体如何收集、使用和共享生物特征信息等
就业歧视风险	宪法权利（适用于联邦和州政府），GINA， ADA，怀孕歧视法	处理预测性健康数据的措施很少；公共部门和私营部门各不相同；雇员自愿参加的健康计划可豁免	《加州医疗信息隐私法案》（CMIA）将健康信息保护责任扩大到软件、硬件和在线服务提供商
公共政策歧视风险	美国宪法第四修正案（禁止政府进行不合理的搜查和扣押，包括人身搜查和通过窃听和查阅公司记录来搜索个人信息	在因执法和国家安全获取个人信息时面临复杂局面	/

二、欧盟视角与 GDPR

欧盟数据保护和隐私法建立在区分个人数据和非个人数据的基础上，对特殊类型的个人数据，如健康数据则提供了更高级别的保护。欧盟《通用数据保护条例》GDPR 自 2018 年起生效，其适用于个人数据的收集、传输和处理。具体来看:

一是规定了数据保护原则。GDPR 提出了收集、处理和存储个人数据时应遵循的一系列原则，包括: 目的限制、数据最小化、存储限制、准确性、完整性和保密性（安全性）、责任和合法性、公平性和透明度。但对“公平”的模糊定义损害了对数据分析造成歧视风险的有效监管。此外，其规定了向个人用户收集个人数据的法律依据由数据处理者确定，有同意、合法利益或合同履行三种类型。

二是对“健康数据”做出了单独的规定。“健康数据”在 GDPR 中定义为“那

些和自然人的身体或精神健康相关的、显示其个人健康状况信息的个人数据，包括和卫生保健服务相关的服务”。与 HIPAA 的定义不同，来自消费设备的生活方式和身体状况数据被视为“健康数据”。除了第 6 条所列的处理个人数据的正当理由外，第 9 条列出了处理特殊类型数据的条件，其中包括：数据主体明确同意评估雇员的工作能力、具有重大公共利益的理由、公共卫生、研究等。

三是规定了对自动化的个人决策提出异议的权利。第 22 条明确规定，“数据主体有权反对此类决策完全依靠自动化处理——包括用户画像——对数据主体做出具有法律影响或类似严重影响的决策”，并指出了该规则的例外情况。

除 GDPR 外，欧盟的《欧盟基本权利宪章》（Charter of Fundamental Rights）、《种族平等指令》（2000/43/EC）、《两性平等指令》（2006/54/EC）94 和《性别获得商品和服务指令》（2004/113/EC）95 在就业、福利制度和获得商品和服务等领域对利用数据做出歧视性决定提出了监管要求。

资料来源：创新研究.《世界经济论坛：身联网已来——应对技术治理的新挑战》，https://mp.weixin.qq.com/s?__biz=MzAxMjY2OTkxOA==&mid=2652025665&idx=2&sn=d38275d5dfb0f8c53c2cb0d05d547bf6&chksm

中国医疗机构网络信息安全管理办法将出台

“全国医疗机构网络信息安全管理办法正在起草中，不久将会出台。”一消息人士在中国互联网大会上透露，新冠疫情暴发后，全球医疗健康数据频繁受到黑客攻击，国内开始重视医疗健康数据的价值，希望通过立法、加强监管等多维度方式提升医疗健康数据的整体安全水平。

一、医疗健康数据被广泛应用

医疗健康数据广泛应用在日常生活的多种场景中。比如，通过大数据高效分析用药成分、剂量时间等情况，寻找合理用药的最佳组合；通过大量临床数据进行科学分析找到病因，并进行临床病因分析和慢病监测；通过对基因序列大量分析，快速筛查和预测疾病和潜在基因缺陷的基因组学分析；对患者进行远程疾病

数据采集后，结合大量临床病因数据分析，实现远程医学诊疗；通过智能可穿戴设备收集数据，实现人体生命体征检测，预警潜在健康风险，进行健康管理；应用大数据等算法，制定医保支付标准，并基于此进行精准的医保决策分析等等。

卫健委医院管理研究所表示，医疗行业关系国计民生，医疗数据一旦遭到篡改、破坏和泄露，势必对医疗机构的声誉、医患双方的隐私及健康安全构成严重威胁，甚至影响社会的和谐稳定。

中国信通院云计算与大数据研究所称，基于医疗大健康数据的敏感性，2016年至今，国家相继出台了不少医疗健康数据安全政策进行规范，包括《关于促进和规范健康医疗大数据应用发展的指导意见》、《互联网诊疗管理办法》、《互联网医院管理办法》、《远程医疗服务管理规范》、《国家健康医疗大数据标准、安全和服务管理办法》、《人类遗传资源管理条例》、《数据安全法》等法律法规。

“即使有如此多法规，医疗健康数据安全事件频发，数据安全形势非常严峻。”他说，尤其是疫情后，数据安全的风险进一步加剧了。

二、疫情后健康数据安全风险加剧

2020 年 4 月，世界卫生组织发表声明称，疫情期间遭受网络攻击数量同比增长 5 倍。奇安信集团发布网络安全系列报告指出，2020 年疫情暴发后，医疗卫生行业史上首次超过政府、金融、国防、能源、电信等领域，成为全球 APT（黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为）活动关注的首要目标。全球 23.7%的 APT 活动事件与医疗卫生行业相关。中国首次超过美国、韩国、中东等国家和地区，成为全球 APT 活动的首要地区性目标。

有消息称，抗击疫情期间，我国的卫生医疗系统、疫苗研究机构、科研院所等曾频繁遭遇网络入侵攻击。2020 年 4 月，中国医疗公司 AI 检测新冠病毒技术实验数据源代码被黑客窃取并出售。

在疫情期间，医疗机构个人和患者信息泄露事件更是频发。2020 年 1 月，某市区卫生管理部门领导通过微信转发新冠病人报告。2020 年 11 月，某市区卫生管理部门领导为提醒辖区内某单位做好防疫工作，将“疑似密接调查情况简介”微信转发，造成该辖区内单位将此信息大规模群发。

此外，远程网络诊疗方式在疫情后被人们普遍接受，全国不少医院都在申请互联网医院、智慧医院。业内人士指出，由于使用网络传递诊断数据、照片等信

息，医疗健康数据的不安全风险可能会进一步加剧。

三、数据风险

据悉，目前医疗健康不安全风险主要体现在八个方面，

一是在线医疗数据：检验报告、诊断结果、既往病史等健康医疗数据存在因漏洞攻击、病毒感染等，导致的非法访问、窃取篡改和恶意上传等风险；

二是医联体访问数据：医联体以及第三方服务机构人员在对敏感数据进行访问浏览的过程中，均可能导致医患隐私等重要信息面临泄露风险；

三是临床科研数据：临床科研数据涉及人口学资料、检查信息、检验信息、药品医嘱、诊断信息、病例以及患者报告，传输过程中一旦发生泄露，后果非常严重；

四是医保数据：医保数据涉及与第三方机构对接，在系统对接、数据传输、数据使用、数据存储、数据销毁等环节面临安全风险；

五是医疗设备维保数据：医疗器械厂商在进行远程医疗设备维护保养时，数据将面临非授权访问、不安全链接、隐私数据泄露、维护记录保存不当等安全风险；

六是健康大数据中心数据：分类分级机制缺失导致将非法登录、越权访问、异常调阅、冒名查询、批量窃取、明文泄露等数据安全隐患；

七是可穿戴健康设备数据：可穿戴设备数据在采集、存储、使用阶段均存在着不同程度的安全隐患；

八是医疗健康 APP 数据：移动应用涉及众多在线健康医疗服务、存在泄露个人健康状况数据、支付数据、卫生资源数据以及公共卫生信息的隐患。

四、多维度提升数据安全整体水平

“还有一些健康敏感数据也在非法出境。国内某知名医院领导与国外公司达成合作协议，非法启动某敏感数据科研项目，国外这家公司对该科研项目样本数据具有远程不受限制的访问权。”一位业内人士指出，面对复杂的形势，医疗机构等相关部门需要多维度提升医疗健康数据安全整体水平。

“北京卫生健康委制定了北京互联网医院监管平台，要求北京市开展互联网诊疗服务的医疗机构均需与监管平台对接，接受平台监督。”北京卫生健康委信息中心副主任郑攀说，截至今年 6 月，北京市共审批了 19 家互联网医院，已全

部对接监管平台。

据悉，互联网医院监管平台内容包括，升级已建的医政医管电子化注册平台，实现机构、医师、护士电子证明、救护车以及医疗广告等医疗资源的管理；建设医疗服务与执业监管平台，实现互联网医院审批及互联网诊疗的实时动态监管；建设医疗服务与执业监管平台，建设医疗服务、诊疗行为等信息的采集系统以及数据展示系统，实现对实体医疗机构医疗资源与医疗服务的监管。

资料来源：经济参考报.《全国医疗机构网络信息安全管理办法将出台》，

http://dz.jjckb.cn/www/pages/webpage2009/html/2021-08/11/content_76437.htm

案例

人体互联网之医疗健康应用

2020 年底，兰德公司发布报告《The Internet of Bodies-Opportunities, Risks, and Governance》，研究了人体互联网这一新兴技术，并探索了其在依赖健康领域的应用。

IoB 技术在一系列医疗和消费者应用中发展迅速，越来越多的老牌医疗公司和大型技术公司投资了新出现的 IoB 初创企业。接下来，本文将展示 IoB 设备的部分应用示例。

在过去十年中，医疗技术和数据科学的进步导致支持互联网的医疗设备大幅增长，这些设备有望提供更好、更精确的数据来支持患者护理并提高医疗保健效率。这些设备用于治疗多种疾病和病症，包括糖尿病、癫痫和帕金森病。表 1 提供了可植入互联网医疗设备的示例、以及一些可穿戴或独立式医疗设备；所有这些 IoB 设备都已投入使用。IoB 的消费市场发展迅速，出现了各种旨在改善日常健康和舒适度并提供其他便利的新设备。表 1 还列出了一些该类型的 IoB 应用示例。

表 1 IoB 应用示例

场景		应用
医疗	植入式医疗	人工胰腺
		脑机接口
		帕金森氏症脑电信号器
		耳蜗设备
		植入式心脏起搏器
		植入式葡萄糖检测仪
		植入式智能支架
		可摄取的数字药丸
	可穿戴医疗	电子医疗
		独立式输液泵

		配备传感器的病床
		穿戴式胰岛素泵
		穿戴式义肢
		穿戴式癫痫监护仪
消费者	消费者中的应用	注意力监视器
		人体植入传感器
		带传感器的服装
		女性科技产品
		独立消费者 IoB
		植入式微芯片
		精神和情绪感应器
		视觉和听觉辅助器
		穿戴式健康追踪器
		可穿戴神经设备

资料来源：RAND.《The Internet of Bodies-Opportunities, Risks, and Governance》

人体医疗健康监测的物联网设备案例

物联网设备通过以下三种方式与人体连接。

首先在外部，包括智能手表、Fitbits 等可穿戴设备在内的设备可以从外部监测我们的健康状况，

第二在人体内部，许多装置如心脏起搏器、智能药丸、人工耳蜗装置被植入体内，以监测或指导人体健康的各个方面，以及

第三嵌入式，当技术和人体结合在一起时，与远程操作的机器实时连接。

人们普遍认为，大多数老年人生活在没有任何医疗援助的环境中。如果及时为他们提供适当的帮助，他们可以在晚年过上良好的、健康的生活。

许多智能设备经常被用作监测人类健康的高级应用，例如慢性病、持续性疾病。一些示例如下：

(1) 心脏起搏器：一种放置在患者腹部或胸部的小型装置，它有助于改善或

控制健康状况，并通过一些电脉冲来改善健康状况的异常波动。

(2) 智能药丸：这些药丸内嵌入了电子传感器和芯片。当患者吞下药丸时，这些药丸会从患者的器官中收集数据，并将其发送到远程连网设备。例如，胃轻瘫是一种无法解释的胃部疾病，可以通过智能药丸来辅助治疗。

(3) 智能隐形眼镜：根据眼睛和眼液提供的信息，这些镜片和监测器进行健康诊断，如监测葡萄糖水平，这有助于糖尿病患者观察体内葡萄糖水平，而无需整天重复针刺。

(4) 射频识别微芯片：这些芯片有助于识别和重新定位丢失的东西，例如在军队中用作国防应用的特殊物品。从商业的角度来看，这些芯片允许人们使用智能钥匙进入建筑物，挥手付款等。

(5) 智能助听器：这些是新时代的助听器，它为患有听力受损的人与他人互动带来了巨大变化。它们根据真实世界的声音过滤、平衡和添加所需的功能。Doppler labs 是耳戴式设备的一个知名例子。

资料来源：51CTO. 物联网如何影响人体？. https://iot.51cto.com/art/202108/676182.htm