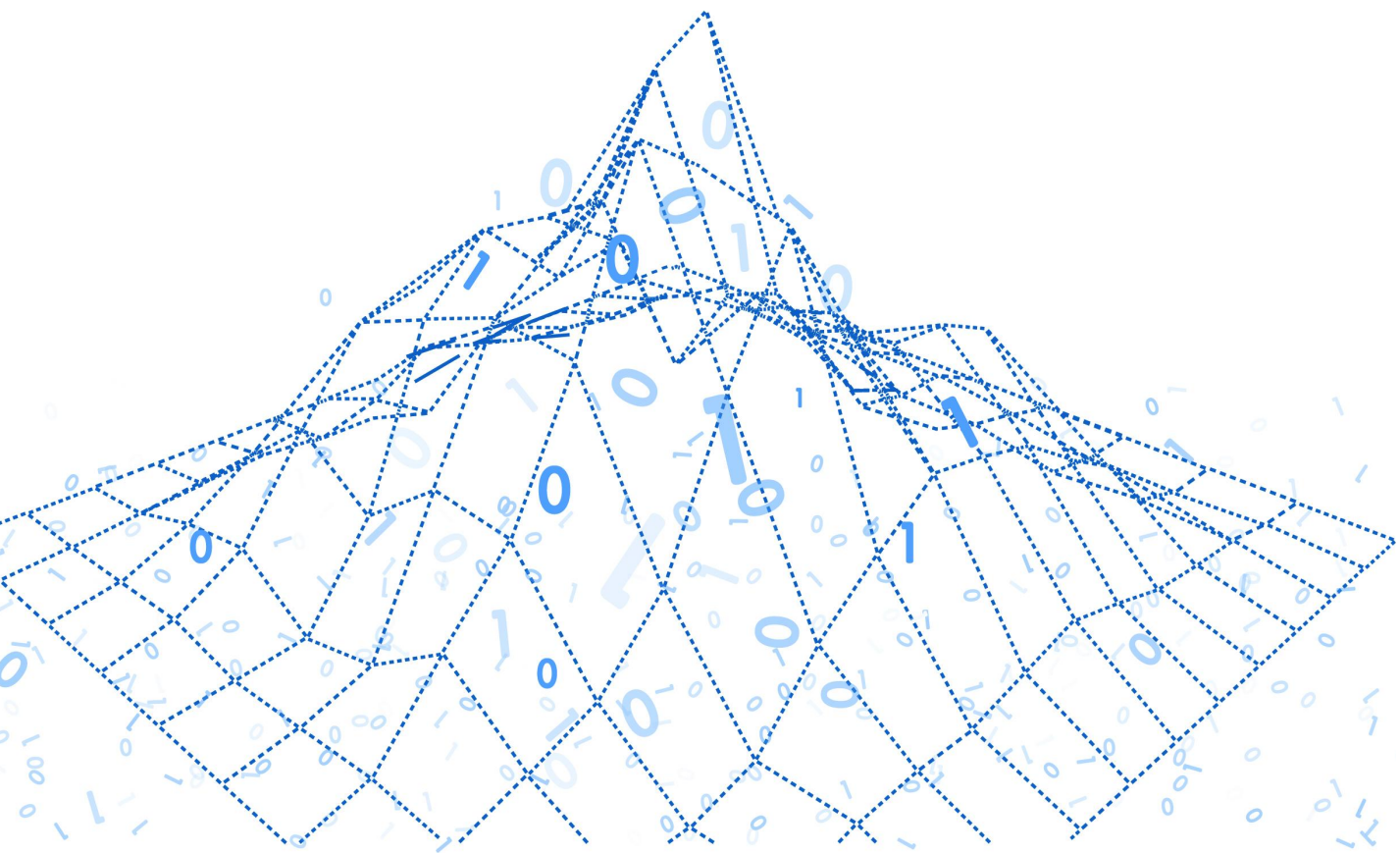
2023年第七期|总第九期

全球开源发展态势洞察



开放原子开源基金会出品

2023年4月20日

目录 | 全球开源发展态势洞察

一、国际开源基金会

二、行业发展

三、前沿技术

四、开源安全

五、开源法律速递

六、开源报告

国际开源基金会

Keycloak正式成为云原生计算基金会孵化项目

Keycloak是一种身份和访问管理（Identity and Access Management，IAM）解决方案，为应用程序和API提供集中式身份验证和授权。它提供了完整的、随时可运行的IAM服务，可以在单个轻量级容器镜像中轻松部署和扩展。Keycloak可以用于单点登录，用于Kubernetes部署的基础架构和面向最终用户的应用程序，并通过令牌来确保服务之间的API调用。

Keycloak由Bill Burke和Stian Thorgersen于2014年创建。该项目已经在生产环境中被组织机构使用超过八年，其中包括Accenture、CERN、Cisco、Ohio超级计算中心、日立、Okta、Quest等许多组织。该项目的兴趣增长非常迅速，在2022年11月访问keycloak.org的月访问量超过150,000人次，其GitHub仓库的star数目最近超过15,000。

4月11日，CNCF技术监督委员会一致投票决定Keycloak正式成为云原生计算基金会（CNCF）孵化项目。

自由软件基金会批评Google移除对JPEG-XL支持的决定

Google自二月份从Chrome中移除对JPEG-XL图像格式的支持，转而使用自己的专利格式AVIF。Google工程师给出的理由是整个生态系统没有足够的兴趣来继续实验JPEG-XL，相比现有的格式新格式没有带来足够的增量收益，通过移除相关代码可以减轻维护负担并专注于改进现有格式。

自由软件基金会（FSF）发表文章，公开批评Google。因为Chrome/Chromium占据了近九成市场份额，Google Chrome是Web标准事实上的仲裁者。它停止支持JPEG-XL的决定突出其对Web平台的控制。对整个Web生态系统而言，Google拥有压倒性的力量，而普通用户则是微不足道的，FSF呼吁用户团结起来支持自由的浏览器。

行业发展

Servo项目计划迁移到Layout 2020

Servo是一款开源的高性能浏览器引擎，为应用程序和嵌入式使用而设计，用Rust编程语言编写，为浏览器内部带来了闪电般的性能和内存安全性。2012年，Mozilla启动Servo项目，致力于创建一个新的开源浏览器引擎，该引擎可以利用多核硬件来提高速度、稳定性和响应能力，于2020年11月17日，托管到Linux基金会。2023年4月13日，官方博客表示计划迁移到Layout 2020引擎。目前，Servo项目有两个独立的布局引擎——Layout 2013和Layout 2020，开发时间分别始于2013年和2020年，Layout 2020旨在修复Layout 2013的多个不足之处，开发者表示他们认为Layout 2020是Servo未来发展的最佳布局引擎。

Reddit将向使用其API训练模型的公司收费

2023年4月18日，Reddit宣布将向使用其API训练模型的公司收费。OpenAI的ChatGPT和Google的Bard都将Reddit作为其训练语料的来源。Reddit称自己为社交新闻聚合器。数据调查，Reddit每月有超过4.3亿活跃用户，页面浏览量超300亿，平均访问持续大约10分钟，用户每次访问超过7个页面，Reddit联合创始人兼CEO Steve Huffman称该平台的语料库非常有价值。

近日，Reddit修改了其API访问政策，它的API对开发机器人程序等工具的独立开发者，以及学术和非盈利项目的研究员仍然是免费的，但对通过API使用其语料库训练AI则将要开始收费，具体金额将在未来几周公布。同时，免费API的访问也将限制速率。

Stability AI开源其语言模型StableLM

2023年4月20日，Stability AI宣布开源其正在开发中的语言模型StableLM。目前，该模型的Alpha版有30亿和70亿参数两个版本，后续将发布150亿和650亿参数的版本。Stability AI表示开发者可将其模型用于商业使用或研究目的，

但须遵守CC BY-SA-4.0许可证的条款。同时，Stability AI还发布了一套经过教学微调的研究模型，这些微调模型仅供研究使用，并在非商业CC BY-NC-SA 4.0许可证下发布，符合斯坦福大学的Alpaca许可证。

行业发展

Tetrate推出针对Amazon EKS设计的服务网格解决方案TSE

TSE是一款针对Amazon EKS的服务连接、安全和弹性自动化解决方案，基于Istio和Envoy等开源服务网格组件构建，并针对Amazon EKS对TSE进行了简化安装、配置和操作的优化。TSE提供了Istio和Envoy之上的服务网格自动化。处理在Amazon EKS上安装和配置开源组件，与AWS服务集成，并为平台运营商提供管理控制台，以快速配置服务网格以实现安全、弹性和可观察性。

Essential Kubernetes Gauges开源

Essential Kubernetes Gauges（EKG）提供了一组标准化的预制SLO，用于测量Kubernetes集群的可靠性。可以将这些SLO视为一个检查引擎指示灯，当你的EKS集群行为异常时，它可以提示你，并记录集群何时按预期运行，何时不按预期运行。

SLO允许你为集群可靠性设置可调整的目标，EKG包括衡量集群多个方面的SLO：

·控制平面运行状况；
·集群运行状况；
·工作负荷运行状况；
·资源效率；

已提议将成本效益计量作为未来的改进措施，并正在考虑之中。

Helm完成模糊测试安全审计

Helm被描述为Kubernetes包管理器。有助于简化查找、共享和使用为Kubernetes构建的软件。Helm最初是Helm Classic，即2015年开始的Deis项目，并在首届KubeCon上推出。在2016年1月，该项目与一个名为Kubernetes Deployment Manager的GCS工具合并，并将项目移至Kubernetes下。2018年6月，从Kubernetes子项目晋升为正式的CNCF项目。2020年4月，作为CNCF项目毕业。本次审计共编写38个模糊器，测试范围覆盖chart处理、版本存储和仓库等关键部分。共计发现9个漏洞（至今已修复8个），其中包括，4个空指针引用问题，4个内存不足问题，1个栈溢出问题。

行业发展

基于Kubernetes 1.24的第三方安全审计结果发布

2018年，云原生计算基金会（CNCF）开始为其项目进行第三方安全审计，目的是改善开源生态系统的整体安全实践。从那时起，Argo、Backstage、CoreDNS、CRI-O、Envoy、etcd、Flux、KubeEdge、Linkerd、Prometheus、SPIFFE/SPIRE和其他CNCF项目都经过了安全审计。

近日，基于Kubernetes 1.24的第三方安全审计结果发布，本次审计发现以下问题：

·在限制用户或网络权限方面存在问题，可能导致管理员混淆特定组件的可用权限；

·在组件间身份验证方面存在问题，恶意用户能够获取集群管理员权限；

·在日志和审计方面存在问题，攻击者可以在控制集群后利用这些缺陷来进行潜在活动；

·在用户输入过滤方面存在问题，允许通过修改etcd数据存储的请求来绕过身份验证。

Cilium发布v1.14.0-snapshot.1

Cilium是一个开源软件，用于透明地提供和保护使用Kubernetes、Docker和Mesos等Linux容器管理平台部署的应用程序服务之间的网络和API连接。本次发布的snapshot.1版本是Cilium 1.14.0版本的早期预览版本，具有以下主要特性：

·改进的VPN功能：Cilium VPN功能得到了改进，现在支持更灵活的VPN 配置和更好的性能。

·支持Docker容器网络：Cilium支持Docker容器网络，允许用户以更轻松的方式构建和管理Docker容器网络。

·改进的CLI工具：Cilium CLI工具得到了改进，现在支持更好的命令行交互和更好的错误处理。

同时，Cilium还实现了一些其他改进，包括更好的网络诊断、改进的日志记录和增强的安全性。

行业发展

岸田与OpenAI公司CEO就ChatGPT交换意见

据共同社报道，日本首相岸田文雄10日在官邸会见了开发人工智能（AI）聊天软件“ChatGPT”的美国新兴企业OpenAI首席执行官（CEO）阿尔特曼。ChatGPT因为能像人一样流畅对话而引发热议。阿尔特曼向媒体透露，岸田听取了有关ChatGPT优缺点的介绍，对其很感兴趣。

ChatGPT的用户正在急剧增加，由于担忧个人隐私等受到侵犯，各国纷纷出台限制措施。阿尔特曼还就如何应对ChatGPT的风险向岸田表达了自己的想法。

他还对媒体表示，考虑在日本开设办事处。官房长官松野博一在记者会上就ChatGPT表示：“如果能消除处理机密信息及信息泄露的担忧，为了减轻国家公务员的业务负担，将就加以利用的可能性进行探讨。”

ChatGPT每日运营成本超70万美元

半导体研究公司SemiAnalysis的首席分析师Dylan Patel，在接受The Information采访时表示，估计基于GPT-3的AI聊天机器人ChatGPT的每日运营成本超过70万美元，OpenAI的最新模型GPT-4的运营成本会更高。训练ChatGPT之类的大语言模型可能需要花费数千万美元，但运营费用或推理成本将会远远超过训练成本。其中，一家利用AI开发生成式文字游戏的创业公司Latitude透露，运行OpenAI的语言模型加上支付AWS的服务费用，使得该公司在2021年每月花费20万美元。

前沿技术

青云企业云平台v6.1版本正式发布

近日，青云企业云正式发布其最新版本v6.1，新版本的特性如下：

·新增巡检与监控功能；

·新增企业空间管理功能，涵盖组织管理、用户管理、配额管理、资源管理、流程审批等空间管理模块；

·新增对第三方存储的支持；

·提供VMware vSphere纳管工具；

·QKE容器引擎支持裸金属服务器作为集群Worker。

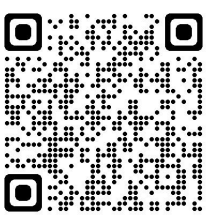
服务网格项目Linkerd v2.13.0发布

近日，服务网格项目Linkerd正式发布v2.13.0，新版本的特性如下：

·引入客户端策略，包括动态路由和熔断器模式；

·支持调试基于HTTPRoute的策略；

·增加新的init容器—— network-validator，确保本地iptables规则按预期工作。



D2iQ推出专为政府部门设计的Kubernetes平台DKP Gov

近日，D2iQ正式推出其专为政府部门设计的Kubernetes平台DKP Gov，DKP Gov基于D2iQ Kubernetes平台（DKP）创建，旨在满足政府、军事和民用机构对创新技术的需求。

DKP Gov为公共部门带来的主要特点和好处包括：

1.单集群或多集群管理、混合多云管理、多租户架构、vSphere、政府云（GovCloud）和支持硬件裸机（Bare Metal）；
2.混合云生命周期成本管理；
3.对物理和逻辑隔离集群的全面支持；
4.战术边缘武器系统支持（DDIL）；
5.集中式多云、多集群队列管理；
6.持续交付（CD）；
7.IL 2-6+ (JWICS)、FENCES、C2S、SC2S、C1D、SIPR/NIPR；
8.政府平台上的ATO、cATO；
9.FIPS 140-2认证；
10.确认的美国支持（24/7/365支持，符合ITAR和数据完整性标准）；
11.符合CNCF标准的纯上游Kubernetes；
12.生产就绪（Day-2）平台应用程序；
13.在大规模环境下启用混合环境的微服务架构；
14.统一亚马逊网络服务，微软Azure，谷歌云平台支持。

前沿技术

备份容灾工具 Velero v1.11.0发布

Velero是一个支持Kubernetes集群容灾、数据迁移和数据保护的解决方案，通过按需或按计划将Kubernetes集群资源和持久卷备份到外部支持的存储后端。从而实现对Kubernetes的备份、恢复、迁移等功能。

近日，备份容灾工具Velero v1.11.0正式发布，新版本特性更新如下：

·增加插件进度监控功能；

·支持筛选过滤在备份时要跳过的卷；

·新增集群范围和命名空间范围的资源筛选器

·添加用于设置Velero服务器与k8s API服务器超时的连接的参数；

·支持备份描述命令的JSON格式输出；

·使用controller-runtime重构控制器；

·CSI插件通过检查restorePVs参数的设置来决定是否从快照中恢复数据。

Kuasar项目正式开源

Kuasar在保留传统容器运行时功能的基础上，通过全面Rust化以及优化管理模型和框架等手段，进一步降低管理开销、简化调用链路，扩展对业界主流沙箱技术的支持。此外，通过支持多安全沙箱共节点部署，Kuasar可以充分利用节点资源，实现降本增效。

服务网格项目Kuma v2.2.0发布

由Kong打造的Kuma是一套强大的Service Mesh解决方案。Kuma属于基于Envoy构建的平台中立型控制平面。Kuma提供多种网络功能，用以保护、路由并增强服务之间的连接性。除虚拟机之外，Kuma还支持Kubernetes。目前，Kuma项目由CNCF托管。

近日，服务网格项目Kuma v2.2.0正式发布，新版本特性更新如下：

·支持OpenTelemetry；

·支持使用JSONPatch来定义MeshProxyPatch策略；

·支持重试指令和优先级；

·支持将底层Envoy版本升级到v1.25;

前沿技术

·新增策略以用于更精细地控制服务间的负载均衡；

·支持在Kubernetes集群中部署通用模式的全局控制平面；

·支持为离线令牌签名和验证提供公钥。

Envoy v1.26.0发布

Envoy是一个高性能云原生代理，最大优点是支持配置动态生成、热加载。为了追求性能使用C++语言开发。最开始是由Lyft公司内部使用，随后捐赠给CNCF，并成为最早一批CNCF孵化的项目。

近日，Envoy v1.26.0正式发布，更新特性如下：

·支持对通用代理的跟踪；

·支持在http过滤器链的任何位置修改请求和响应头信息；

·支持在动态元数据中设置JWT认证失败状态代码和消息；

·增加过滤器状态输入功能；

·支持在TLS握手和过滤器匹配之前启用速率限制；

·支持上游访问日志中的路由信息；

·支持动态地禁用TCP隧道；

·增加负载均衡器Maglev扩展和环形哈希扩展。

容器镜像仓库Harbor v2.8.0发布

Harbor是由VMware公司中国团队开发的一个企业级Registry项目，可用于搭建企业内部的容器镜像仓库。Harbor在Docker Registry的基础上增加了企业用户所需的权限控制、安全漏洞扫描、日志审核和远程复制等重要功能，还提供了图形管理界面及面向国内用户的中文支持，开源后便迅速在业内流行开来，成为中国云原生用户的主流容器镜像仓库。

2018年7月，Harbor正式进入CNCF，于2020年6月顺利毕业，成为了CNCF首个来自中国的开源项目。

近日，容器镜像仓库Harbor v2.8.0正式发布，版本特性更新如下：

·支持OCI distribution spec v1.1.0-rc1；

·支持使用CloudEvents格式发送Webhook负载；

·支持用户跳过任务扫描器自动更新拉取时间的选项；

·移除helm chart仓库服务器ChartMuseum。

前沿技术

容器漏洞扫描工具 Trivy v0.39.0发布

近日，容器漏洞扫描工具Trivy正式发布v0.39.0，新版本的特性如下：

·支持依赖关系图；
·下载OCI工件支持授权功能；
·支持在OCI referrer中发现SBOM；
·支持k8s并行资源扫描；
·添加注册表选项；
·增加并发处理的pipeline；
·增加节点容忍选项；
·支持公共TLS证书的Redis。

分布式云原生平台 Kurator v0.3.0发布

近日，分布式云原生平台Kurator正式发布v0.3.0，新版本的特性如下：

·在Cluster API的基础上添加了一个新的CRD集群，使用此功能，用户只需声明一个API对象即可管理kubernetes集群的生命周期；
·增加了对kubernetes集群升级的支持；
·增加了对kubernetes集群扩展和缩容的支持；
·增加了在本地设置高可用kubernetes集群的支持。

阿里云服务网格ASM 2023年3月产品动态

阿里云服务网格ASM2023年3月产品更新内容：

·网关支持对接WAF；
·支持配置Ingress资源；
·支持Knative服务的管理；
·网格拓扑支持OIDC方式登录；
·Sidecar代理支持超卖模式；
·新增出口流量策略；
·支持配置全局默认的HTTP请求重试策略。

开源安全

Google Chrome发布紧急更新修复正被利用的0day漏洞

Google Chrome发布紧急更新修复了一个正被利用的0day漏洞。改漏洞编号为CVE-2023-2033，是Google旗下Threat Analysis Group（TAG）的安全研究员 Clément Lecigne报告的，属于V8 JavaScript引擎中的高危类型混淆漏洞。类型混淆允许错误类型的数据访问内存，允许对内存非法读写。Google称攻击者可通过创建HTML页面去利用漏洞，该漏洞被归类为高危级。

JCRE中的内存损坏：无法修复的HSM可能会吞噬您的私钥

密钥一直以来都是安全保护的核心目标。由于密钥槽的限制，大多数加密货币硬件钱包使用MCU芯片（如STM32F205RE）来实现，以便能使用secure element存储和支持更广泛的加密货币种类。然而，那些对保护私钥有更高安全要求的人来说，通常会对Java Card感兴趣。因为Java Card本质上是一种具有加密算法硬件实现的智能卡，私钥或对称密钥无法从中提取。用户只能从Java Card中获得加密操作的结果。另外一点是，已经使用通信参数初始化但尚未加载应用程序（applet）的Java Card是可由用户编程的，而且有一些以Java Card应用程序（applet）形式实现的各种功能的自由开源软件项目。即使Java Card作为HSM（硬件安全模块）的安全性高于常见加密货币硬件钱包的实现，但依然有安全风险，HardenedVault介绍了两个典型的漏洞，这些漏洞位于更底层的JCRE（Java Card运行时环境），虽然不会导致私钥被泄露，但会导致应用程序陷入无法恢复的错误。一旦出现这种问题，卡片中的私钥就可能会丢失。作为HSM的智能卡实现比基于MCU的解决方案（几乎所有硬件钱包都采用了这种方案）更加安全，但仍存在某些安全风险，即使获得EAL 5+认证的硬件钱包也有被攻击的记录。因此，在系统安全方面，我们仍需要坚持纵深防御的策略。另一方面，透明度很重要，开源是确保HSM的整个运行环境能够得到适当审计的唯一途径。对于 Java Card，我们希望未来能够拥有一个免费、开源且可更新的JCRE。或者某种功能上类似于Java Card但可以使用C语言编程的HSM，甚至可以直接使用通用计算（如可信计算、运行时保护、攻击面缩小等）实现。

开源法律速览

最高院发布2022年知识产权典型案例[1]，涉及对源代码技术秘密侵权的认定

撰稿：张苏兵 郭雪雯
审校：王荷舒

基本案情

花儿绽放公司系“有客多”小程序源代码技术秘密的权利人。该公司主张盘兴公司与其签订《花儿绽放源代码使用许可合同》并依约获取涉案软件源代码后，违反合同约定保密义务，**在第三方网站公开披露该源代码**，故向广东省深圳市中级人民法院提起诉讼，请求判令盘兴公司及其唯一股东盘石公司连带赔偿经济损失5000余万元并消除影响。一审法院判决盘兴公司、盘石公司连带赔偿500万元。花儿绽放公司、盘兴公司、盘石公司均不服，提起上诉。

最高人民法院二审认为，**涉案软件源代码构成技术秘密，盘兴公司公开披露涉案软件源代码的行为构成对技术秘密的侵害**；花儿绽放公司单方委托鉴定机构就涉案技术秘密商业价值出具的鉴定意见中，多项数据存疑，不应予以采信；综合考虑涉案技术秘密的研究开发成本、实施该项技术秘密的收益、可得利益、可保持竞争优势的时间等因素，一审法院酌定的损害赔偿数额并无明显不当。遂判决驳回上诉，维持原判。

判决要点

- 最高院在判断代码“是否为公众知悉”时认为，**代码中涉及程序的组织结构、调用关系、执行逻辑等，应将一个源代码文件作为一个整体对待，不应将一个完整代码进行部分切分而判断是否“为公众所知悉”**，故基于此对被告第040号鉴定意见书中关于4个文件中的部分代码已被公开的鉴定结论不予采信。
- 对于被告关于软件功能相同推论出代码相同的主张，最高院认为**软件源代码涉及到特定的变量名、类名及方法的定义、程序的组织结构、调用关系、执行逻辑等，还包括在特定位置对方法、语句和变量的注释文字等**，软件源代码也体现了软件开发人员的代码风格、特定字词的独特表达，故即使为开发相同功能的软件，不同开发者可以设计不同的源代码进行表达，盘兴公司、盘石公司有关软件功能相同推论出代码相同的主张没有事实依据，不予支持。
- 在认定侵权责任应当如何承担时，最高院认为原告委托评估机构所作的评估结论多项数据难以令人信服，对原告花儿绽放公司主张以价值评估鉴定认定的商业价值作为赔偿依据的主张不予支持。**鉴定机构经评估作出的商业价值鉴定仅是确定知识产权商业价值的一种方式**。在本案经审查不宜直接依据价值评估鉴定意见认定涉案技术秘密商业价值的情况下，依据本案现有证据情况，可以综合考虑涉案技术秘密的研究开发成本、实施该项技术秘密的收益、可得利益、可保持竞争优势的时间等因素酌情确定涉案技术秘密的商业价值，进而作为确定赔偿数额的依据之一。

开源法律速览

案件解读

企业通过与源代码权利人签署源代码使用许可合同获得权利人交付的非公开源代码后，应当依约使用，未经权利人许可公开披露该源代码的行为，除构成违约外，还可能构成对源代码的技术秘密的侵权，从而面临巨额赔偿。向公开网站/开源社区发布源代码的贡献者（不论个人或法人）应当注意其提交/公开行为是否受到有关前置保密义务限制。

域外司法：德国地区法院判决著佐权条款的效力程度

案件背景

德国对开源软件/自由软件有持续的司法实践[2]。十余年前，柏林地区法院曾在AVM v. Cybits一案中[3]判决，违反GPL将**自动**导致权利人丧失权利，因为GPL传染性将迫使曾经的专有软件被视为开源软件[4]。该法院判令，AVM有义务使其集成了预安装GPL软件的固件受GPL约束，且AVM因其GPL不合规而无法基于著作权侵权对WLAN路由器的竞争供应商Cybits提出禁令救济[5]。

2021年1月，德国卡尔斯鲁厄高等地区法院对GPLv2.0的著佐权条款的效力作出了判决（OLG Karlsruhe, Urteil vom 27.01.2021 - 6 U 60/20）[6]，该法院消除了这种**自动性**。根据该法院的判决，开发者对著佐权条款的违反可导致其使用、修改开源软件的权利丧失，**但其侵权行为并不能使得第三方有权以自己的名义披露其开源软件修改版的源代码**。

案情回顾

内容管理系统WordPress软件在GPLv2.0下许可[7]，原告基于WordPress发布了预设计的“*主题*”（即Theme）并委托另一家机构设计新主题。该机构将使用主题的专有权利转让给了原告后，原告将主题置于MIT许可证的约束下，并通过商业许可协议在线提供付费版主题。**被告威胁原告，由于该主题系WordPress的衍生作品，被告将基于GPLv2.0在GitHub上发布该主题的源代码**。为免源代码披露，原告向初审法院申请了临时禁令。临时禁令获批后，双方在卡尔斯鲁厄高等地区法院进行上诉。

案情焦点

本案聚焦在：1）以创建主题方式对WordPress进行修改，是否构成GPLv2条款下的“衍生作品”？**2）如果著佐权条款适用，第三方主体是否有权利发布该主题或者该发布是否将构成著作权侵权？**

针对问题一，基于GPLv2第2条款，所有“基于本程序”（based on the Program) 的衍生作品均应在同样条件下发布（即“著佐权限制”）。上诉法院并未就问题一给出结论，而是就问题二判定构成侵权，主要涉及以下原因：

a. **开源软件的使用权是在不违反许可条款的条件下授予的，如违反GPL（如修改者分发时不披露修改代码）只直接导致其不能使用源程序**（德国著作权法案第63c.2款的条件也指向“修改”），但其作为主题专有权的持有者并未就其修改版丧失著作权，因而有权禁止被告利用和披露；且GPL2.0仅在缔约方之间具有约束力，即使在缔约方故意违反GPL2.0的情况下，**第三方也不能强制执行开源义务**。

b. 对于公众对修改后的程序的使用权的假设，至少缺乏原告或开发者的同意。上诉法院审查了WordPress原始开发者及主题开发者之间可能存在共同作者身份（德国著作权法案第8(1)款，共同创作作品且不可单独利用其份额构成共同作者，这不排除后续贡献/修改的权利），**在这种情形下，共同作者（指原告）未经其他共同作者同意，无权单独授予第三方（指被告）发布和利用共同作品的权利**。此外，GPL 许可条款中也没有任何默示同意。

因而无论如何，主题源代码的发布都需要原告的同意。就此，上诉法院驳回了GPL软件的修改版须自动基于GPL下许可的抗辩[8]。

相关解读

有评论称[9]，卡尔斯鲁厄高等地区法院的判决极具启发性，并可能会给软件GPL有效性的法律评估带来根本性变化。也有评论称[10]，该判决只对GPLv2文本进行了机械解释。因为根据该法院的说法，这种GPL传染性发布**必须是积极保证的**（GPL文本中要求的“您必须导致”），而非**自动导致的**。这样一来，开源的想法则很快会消亡。

域外立法：欧盟拟制定《聊天控制法案》，开源操作系统可能被“误伤”

自2022年5月份以来，欧盟委员会正在制定并审议一项名为*Commission proposal on mandatory messaging and chat control*[11]的法案（以下简称“聊天控制法案”），委员会本意是希望责成所有电子邮件、聊天和信息服务的提供者以完全自动化的方式搜索可疑信息，检测 “儿童色情”相关的内容，以通过预防更好地保护儿童。随后该法案遭到广泛反对，除了对该法案可能侵犯公民自由的质疑外，以瑞典VPN服务提供商Mullvad为代表的多家厂商、组织认为，拟议的法案不仅将对所有私人通信进行极权控制，而且还将禁止Linux等开源操作系统。

立法进程

2020年7月，欧盟委员会提出允许对聊天进行控制的"临时"立法。

2021年7月，欧洲议会通过了允许聊天控制的立法，允许聊天、消息和电子邮件供应商自愿进行聊天控制，此后美国服务提供商Gmail和Outlook.com部署了这种监控技术。

2022年5月，欧盟委员会就聊天控制提出了第二个立法提案——*Commission proposal on mandatory messaging and chat control*，即当前聊天控制法案，该法案强制要求所有聊天、消息和电子邮件服务提供商在没有任何怀疑的情况下部署这种大规模监控技术。

开源法律速览

至2023年3月底，公民自由委员会（LIBE Committee）及安理会执法工作组（Council’s Law Enforcement Working Party）多次就该法案进行评估和讨论，审议工作预计在2023年底前完成。[12]

对开源可能产生的影响

瑞典VPN服务提供商Mullvad认为，拟议的法案不仅将对所有私人通信进行极权控制，而且还将禁止Linux等开源操作系统[13]，如果该法案生效，几乎所有开源操作系统都是“非法”的。理由是该法案第6条定义了软件应用商店的义务，软件应用商店的提供者应该：

（a）在可能的情况下，与软件应用程序提供商一起“采取合理措施”，评估通过其软件应用程序提供的每项服务是否存在用于招揽儿童的风险；（b）采取合理措施，防止儿童用户访问他们已确定有重大风险用相关服务招揽儿童的软件应用程序；（c）采取必要的年龄验证和年龄评估措施，以可靠地识别其服务中的儿童用户，使他们能够采取（b）点所述的措施。

同时该法案的第2条明确了“软件应用商店”的定义：一种专注于将软件应用程序作为中介产品或服务的在线中介服务。对于该定义，Mullvad认为该定义几乎涵盖了自20世纪90年代以来的所有开源操作系统，因为不论是应用分发还是安全更新开源操作系统均有涉及，并举例当前主流的Debian就拥有超过17万个软件包，在这种理解下，开源操作系统也属于“软件应用商店”。结合该法案第6条，由于开源操作系统和软件包的作者众多，甚至分布在全球，因此各方很难一起“采取合理措施”，另外在代码开源的前提下，也难以追踪下载用户的信息以进行分析控制。Mullvad认为一旦该法案生效，包括主流 Linux 发行版在内的几乎所有开源操作系统都将成为“非法”的。

Chrisoncrypto[14]，reddit[15]，No Bullshit Bitcoin[16]等外网平台也表达了同样的忧虑。

法案条款

据悉，聊天控制法案中“软件应用商店”的定义援引了欧盟数字市场法案Digital Markets Act[17]第2条第（14）款：“‘software application stores’ means a system software that controls the basic functions of the hardware or software and enables software applications to run on it”.

同时，第2条第（10）款亦对“操作系统”进行以下定义：“‘operating system’ means a type of online intermediation services, which is focused on software applications as the intermediated product or service”.

截至发稿前，聊天控制法案尚在审议中，后续其是否将对此进行补充定义或概念厘清，还有待观望。

开源法律速览

引用文献：

[1]https://www.court.gov.cn/zixun-xiangqing-394812.html
[2]https://www.ra-plutte.de/open-source-software-recht-grosse-faq-tipps/#tipps
[3]https://download.fsfe.org/legal/documents/lg-urteil-20111118.pdf
[4]https://fsfe.org/news/2011/news-20111201-02.en.html
[5]https://fsfe.org/news/2011/news-20111201-02.en.html
[6]https://www.junit.de/2020/wp-content/uploads/OLG-Karlsruhe-Urteil-2.pdf
[7]https://developer.wordpress.org/themes/getting-started/wordpress-licensing-the-gpl/
[8]https://cms-lawnow.com/en/ealerts/2022/01/developments-in-open-source-law-in-2021-in-germany-higher-regional-court-decides-on-copyleft-clause
[9]https://www.dentons.com/de/insights/alerts/2021/july/9/effectiveness-of-the-gnu-public-license-called-into-question
[10]https://www.anwaltskanzlei-online.de/2021/11/10/foss-it-recht-foss-bearbeitungen-und-gpl2-nur-wenn-man-es-will-die-gpl2-in-der-auslegung-nach-dem-olg-karlsruhe-6-u-6020/
[11]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472
[12]https://www.patrick-breyer.de/en/posts/chat-control/
[13]https://mullvad.net/en/blog/2023/2/1/eu-chat-control-law-will-ban-open-source-operating-systems/
[14]https://chrisoncrypto.com/blog/EU Chat Control Law Will Ban Open Source OS Linux and End Privacy
[15]https://www.reddit.com/r/mullvadvpn/comments/10qp3de/eu_chat_control_law_will_ban_open_source/
[16]https://www.nobsbitcoin.com/eu-chat-control-law-will-ban-open-source/
[17]https://EUR-Lex - 32022R1925 - EN - EUR-Lex (europa.eu)

开放原子开源基金会的开源公益项目“源译识”公益翻译、“心寄源”专业沙龙、“源规律”公益课程欢迎您的参与和建议，详情请见：

http://www.openatom.org/legal-IP

开源报告

OSPO的商业价值
——探究组织创建、维护和发展开源办公室（OSPO）的动机

翻译：赵海玲 梁婷婷 王铭典
审校：赵海玲

为什么从商业角度来看，创建、维护和发展开源办公室（OSPO）具有价值？这是在TODO Group最新报告中讨论的问题。该研究报告探讨了OSPO的不同价值主张，并提供建议和见解来帮助利益相关者、监管机构和组织内的其他员工来理解、衡量其价值。

该报告汇集了来自欧洲、亚洲和北美的OSPO及开源领袖在各行各业的观点，包括两所公立大学。涵盖了几个关键领域，包括建立OSPO的动机、OSPO面临的主要挑战、OSPO的不同角色以及OSPO的可永续性及项目健康的重要性等。

前言

开源软件持续地改变着各行业创建和应用软件的方式。在许多领域，由大量甚至完全由开源软件组件构建的系统正逐步替代专有和封闭的软件技术栈，这些系统通过开放的API进行通信。通过开放协作和共同开发，开源软件已经成为推动创新、促进技术普及和公开传播知识的基本途径。

尽管开源软件的显著优势无可争议，但对于组织而言，能在实践中充分利用这些优势并不简单。随着企业组织内部对于开源软件的应用不断扩大和完善，许多组织意识到通过建立一种有条理的方法来管理开源软件的发展是非常有必要的。起初，这种需求主要来自于许可证合规方面，但涉及范围很快超越了单纯的合规问题，最终发展到业务战略层面。

本报告汇编了来自各种公司和大学的开源办公室（OSPO）中开源倡导者的调查结果。为我们提供了一个广泛洞察的视角，以了解组建OSPO背后的动机，以及OSPO为其所在组织带来的具体商业价值。

调查结果发现，与开源软件类似，OSPO具有各种不同的形态及规模。然而，尽管OSPO的具体实施路径各不相同，但调查显示，在各个组织中，OSPO的关键商业价值都汇聚于相同的基本目标：为组织建立使用开源软件的工作框架，确保开源软件能够充分利用并与组织的业务目标保持紧密一致。因此，OSPO的职责包括规范流程、在组织内培养开源文化，以及制定和执行长期的开源战略。

该报告的撰写者立足于开源软件的核心原则——开放协作和知识共享，旨在提供有帮助的信息。报告的目标受众包括组织中正在组建OSPO的开源拥护者，以及现有OSPO的开源领导者，帮助他们明确定义，衡量和传达OSPO的商业价值。

Georg Kunz
爱立信 开源经理

开源报告

随着开源软件在技术领域的广泛应用，更多的组织认识到与开源项目及其开源社区合作的优势。为充分发挥开源的战略价值，直接投资参与项目社区不再是锦上添花的选择，而是一个必要条件。曾经，OSPO主要出现在大型技术公司，如今，OSPO已在众多行业中蓬勃发展，成为组织启动、规范和发展开源的核心。

在过去的五年，我们见证了OSPO在汽车、娱乐、金融服务、制造业以及学术界和政府部门等领域的蓬勃发展。设立OSPO并分配专门的资源来制定和执行公司的开源战略，为所有参与者能产出最佳成果提供了一个框架。这使得组织对其业务所依赖的软件系统有了更加清晰的认识，核心软件项目的维护者能够更直接地与他们的用户组织建立联系。同时，外部寻求合作的伙伴能够找到一个友好且容易理解的切入点与企业展开商谈。

在这份报告中，您将了解来自不同行业的OSPO领导者的经验，他们分享企业使用开源、贡献开源和参与开源社区的战略及其过程。您还会发现，每个OSPO的目标、成功的衡量标准和参与方法，会根据创建OSPO的动机、组织在开源实践方面的成熟程度以及OSPO的内部倡导者如何制定其发展战略而有所差异。尽管OSPO承担着许多相似的职责，但没有哪两个OSPO是完全一样的。

在我们积累的30多年的开源经验中，我们发现OSPO共有的特点是，它们重视促进协作和共同创造，无论是与内部不同的软件团队合作，还是与上游社区的竞争对手合作。OSPO是少数具有明确的双向倡导任务的团队，既在组织内部，确立参与开源项目的规范，倡导开源最佳实践；也在组织外部，保证公司在特定社区的举措既实现商业目标，又推动所有参与者的技术发展。

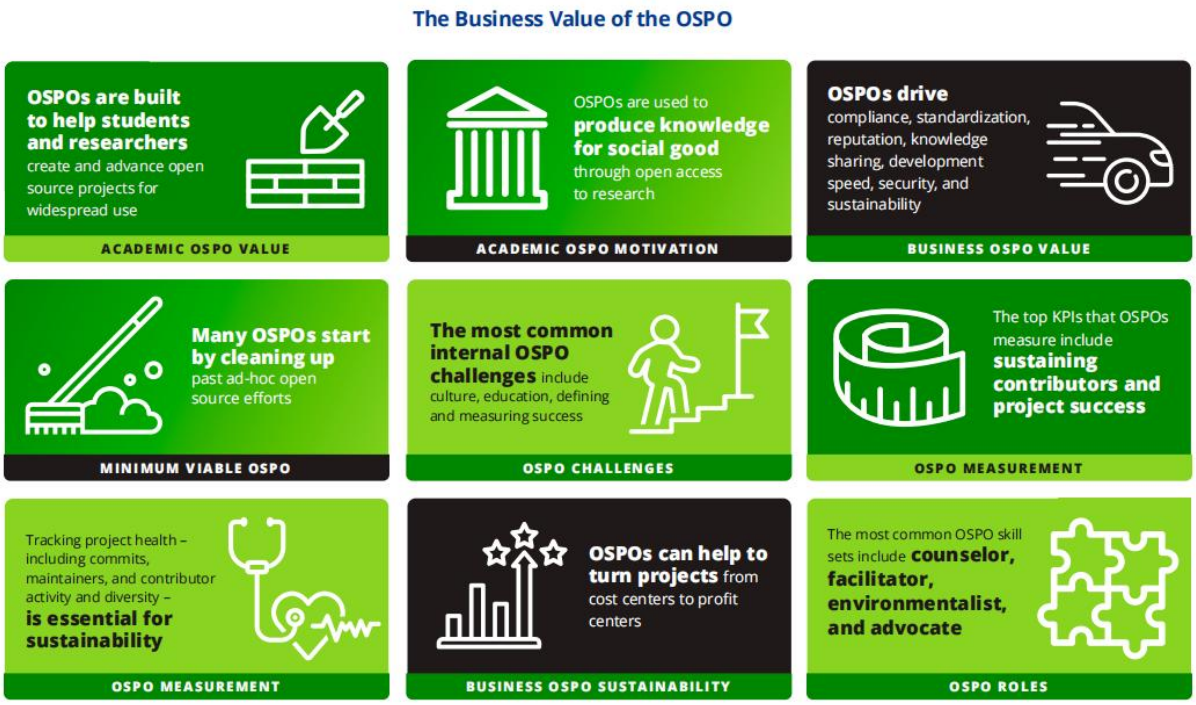
正是因为OSPO的任务具有灵活性和双向性，这些团队可以成为企业技术战略的关键支撑。OSPO有充分的自由去探索和支持业务创新，确定参与流程，以便更好地满足各方参与者的目标，包括从工程人才、业务高管到开源项目社区本身。OSPO成为各利益相关者之间的桥梁和联系纽带，巧妙地确保所有方面的利益都被考虑，并协商所有协作和共创的参与者以争取到最佳成果。

这种面向内部和外部的双向服务使命是OSPO真正的魅力所在。在这样的职责下，成功的OSPO将扮演其组织在更广泛世界中的外交官，负责向社区表达业务需求，同时将社区的需求反馈给业务组织。OSPO作为行业最佳实践的守护者、协作与共创中心，在推动公司在不断变化的市场环境中产生变革等方面具有独特的作用。

本报告将分享来自各行业资深OSPO领导者的意见，针对OSPO的挑战和机遇提供关键的见解，对于长期从事开源领域工作或刚刚开始开源之旅的读者都具有参考价值。无论是您的组织已经建立了长期成熟的开源战略，还是只有一名专注于开源软件许可证合规方面的员工，我们希望您能从本研究中发现OSPO对企业的商业价值。在本报告中，您将了解到各行业开源领袖的研究发现，我们希望您能从中受到启发并在您的开源之旅中找到方向。同时，我们也欢迎您加入OSPO社区，为开源实践做出贡献，共同推动行业发展。

Kimberly Craven 红帽开源办公室高级主管，首席技术官

Leslie Hawthorn 红帽开源办公室高级经理



简介

我们为什么要关心OSPO如何对企业产生贡献?

一个精心设计的OSPO是一个组织开源运营和结构的中心。

我们为什么需要了解OSPO如何助力企业实现目标？无论是倡导创建新的OSPO、维护OSPO，还是发展OSPO，最终都必须将OSPO与业务目标联系起来。无论是在营利性企业还是在非营利性大学中，任何无法对组织有意义、有结果的举措都不太可能在一开始就获得批准，如果它们不能为自己的存在提供商业意义，也就无法生存下去。

“作为一个整体，开源办公室（OSPO）需要具备灵活性，应始终准备好应对接下来的变化”，来自VMware的开源营销和战略总监Suzanne Ambiel说到。“他们需要适应业务，因为他们既服务于企业，也服务于社区。随着业务的变化和演进，OSPO也需要作出相应的调整，确保OSPO与业务战略紧密联系是非常重要的。”

尽管OSPO通常（但并非总是）隶属于首席技术官（CTO）以及许多软件工程师，但公司如何开源绝不仅限于工程部门。正如这份报告中，我们在采访OSPO领导者所发现的，多数组织中的OSPO倡导者是企业高管，他们看到了开源带来的机遇，以及在某些情况下，他们认为公司需要从战略层面应对的潜在威胁。在进行这项研究时，我们希望能更好地了解开源对公司的战略意义，以及OSPO如何帮助组织积极面对开源带来的机遇和挑战。

索尼高级联盟经理Hiro Fukuchi举了一个例子：OSPO组织了一场与外部专家的虚拟大会，许多来自日本和美国的高管都参加了这场活动。

开源报告

个例中存在的共性

这项研究的挑战在于，各组织创建的OSPO确实存在一些共同点，但是每个OSPO是独特的，它们最初成立的背景故事以及它们促进组织实现目标的方式也是独一无二的。

因此，虽然我们确实可以对为什么OSPO重要，谁倾向于支持它们以及OSPO的商业价值如何发展等问题做出一些概括性的总结，但实际上并没有两个组织是完全相同的。

“几天前，我阅读了Linux基金会发布的一份关于不同开源办公室（OSPO）结构的报告，”来自F5的开源高级总监Christine Abernathy说到。“我发现它们并非千篇一律。”开源办公室（OSPO）结构各具特色，它们所设定的目标以及成立过程中的各种故事充满了多样性。

方法论

为了编写这份报告，我们采访了来自欧洲、亚洲和北美的12位OSPO领导者，他们分布在各行各业，包括两所公立大学。所有接受采访的OSPO领导都在TODO Group中积极参与。以下是我们开始时提出的问题：

·OSPO成立时团队成员有多少人？现在有多少人？

·OSPO团队成员的大致薪资范围是多少？

·OSPO团队成员的背景是什么（例如，工程、法律、市场营销）？

·您从事的行业是什么？

·OSPO在组织中的定位（例如，工程、法律、市场营销）？

·谁是OSPO的最初倡导者？

·倡导者是如何在内部倡导OSPO的？他们认为OSPO的价值是什么？

·刚开始建立OSPO时，为其设定了哪些成果或关键绩效指标（KPI）？

·随着时间的推移，您对OSPO价值的理解以及您期望从OSPO中获得的具体成果是如何变化的？

·在未来五年内，您预计OSPO将获得预期的商业价值，还是其价值会发生变化？

·您收集了哪些指标来追踪这些成果所取得的进展？这些指标随着时间的推移如何变化？

·您的OSPO现在致力于实现哪些KPI？您如何评估OSPO的成功？

组织概况及其与开源的关系

一个组织与开源的关系以及它从OSPO中获得的价值，似乎依赖于它所属的公司类型。那些属于技术公司的组织在开源方面所面临的机遇和挑战与那些销售家具的公司组织不同。

技术公司

显而易见，那些技术公司更容易看到开源与其业务之间最直接的关系，而OSPO在管理这种关系方面起着至关重要的作用。

Ambiel提到，VMware的一位OSPO倡导者是当时的首席执行官Pat Gelsinger。“正是他大力支持并表示，我们需要建立一个OSPO，我们需要采取战略性地行动。”

开源报告

技术公司需要以战略方式对待开源问题，这是组建OSPO的核心原因。尽管常有高管的参与，但将OSPO描述为纯粹的自上而下的倡议，或是管理层强迫不情愿的工程师团队推动的倡议是错误的。通常，公司内部的开源爱好者会在高管推动开源战略方法的同时，要求与开源建立更加正式的关系。显然，创建OSPO是下一步行动，以满足双方利益相关者的需求。

在与我们交谈过的所有公司中，开源都不是新鲜事物。多年来，它们一直在内部使用开源，过去还将内部项目开源。它们越来越意识到，开源开发者是如何成为他们产品采纳曲线的一部分。因此，在开源生态系统中拥有良好的声誉是多么重要。

Abernathy表示：“F5的业务在从硬件厂商转型软件服务。”“很多做购买决策的人喜欢‘试用后购买’。这些人可能是倾向于开源的软件开发人员，甚至是希望查看公开源代码以检查漏洞的公司和政府。”所以，在F5的案例中，开源不仅对公司的产品制造方式变得重要，还对市场营销工作产生影响。OSPO确保F5能够战略性地利用开源，并在涉及到开源的情况下做出明智决策。

曾在Facebook（现称Meta）开源办公室工作的Abernathy简述了像Facebook公司和像F5这类公司之间存在的开源差异。“在Facebook，开源很重要，”她说。“但不是从收入方面来看，他们并没有打造一款开源产品……所以容易以一种更直接且有意义的方式开始思考开源的投资回报率。”

F5创建OSPO的一个主要触发因素是在2019年收购开源公司Nginx。这次收购意味着Nginx团队加入F5，并成为推动成立OSPO的另一个声音，这也提高了开源战略的重要性。

对于像Aiven这样的公司，其核心业务与一个或多个开源项目紧密相关，一个正式的、战略性的开源方法也许更为关键，但是如果没有OSPO，他们仍然缺乏这种方法。来自Aiven的开源工程总监Josep Prat表示，即使考虑到开源的战略重要性，在产品功能发布需求与回馈开源需求之间总是存在矛盾。当工程师除了其他职责外还需要为开源做出贡献时，开源贡献总是会处于次要地位。由于这种矛盾，Aiven的高管团队在早期就决定成立一个专门的OSPO，其唯一的职责就是向开源做出贡献并管理与开源社区的关系。

绝非仅仅是开源公司或是初创公司才会觉得开源具有巨大的战略重要性。华为在美国的研发部门Futurewei的开源战略负责人Chris Xie表示，该公司意识到开源带来的威胁和机会已有二十余年，而OSPO是该公司应对这些威胁和机会的方式之一。

终端用户公司

在纯技术公司之后，有些技术前沿公司希望模仿他们在纯技术公司中看到的情况，特别是在软件开发方面。这些公司的收入来自于硬件或软件之外的其他业务，他们不认为构建硬件或软件是他们的业务核心。然而，技术对他们的业务运营至关重要，他们希望被视为一家技术公司，以吸引顶级人才并创造新的收入来源。在这些公司中出现的一个模式是，OSPO以及向开源做出贡献、发布开源项目，都是为了改变公司形象，同时提高公司更快地交付高质量软件的能力。

开源报告

“Spotify从一开始就一直在使用和创建开源项目，但并没有以战略的方式对待它，也没有考虑它是如何为公司创造价值的，” Spotify的OSPO负责人Per Ploug说。“对于我们来说至关重要的是，将开源工作提升到与内部工作相同的水平，这样我们才能考虑为什么要做这些工作以及它们如何带来价值，从而确保我们的工程师将时间投入到有影响力的项目中。”

在Spotify的案例中，这种新方法最明显的应用是Backstage，这是该公司在2020年向CNCF捐赠的成功开源项目的基础上，投入建设的商业产品的大胆尝试。Spotify打算使他们在Backstage的投资更具有自我持续性，并确保他们长期参与开源社区。目前，他们有超过40人在Backstage项目上工作。我们为Backstage项目制定了雄心勃勃的计划，其中包括一项既能为这些计划筹集资金，又能为所有人带来更好终端产品的商业策略，目标是将开源从成本中心转变为利润中心。

“Wayfair是一家科技公司，需要许多技术专家在众多领域进行持续性的工作来支持我们的运营和发展，” Wayfair的全球OSPO负责人Natali Vlatko说到。“在与我们前首席技术官的交谈中，我强调，对我们来说，真正实现这种心态的最简单方法是开发技术产品。做到这一点的万全之策是构建开源项目并投资回馈开源生态系统。”

虽然这些公司确实以变得更像科技公司为目标，但这只是达到目的的手段。在某些情况下，目标是明确的，通常是能够聘请到最优秀的人才以及提高内部工程工作的质量。然而，即使这些公司在开始时就认为开源很重要，但却无法准确地阐述开源为什么或者如何能够促进工程或商业目标。成立OSPO有助于他们明确开源如何使公司受益，并确定如何从开源中获得更多价值。

“他们曾经有几个开源项目，但都没有取得任何成果，”Indeed的开源总监Duane O'Brien谈到在他加入公司之前的情况。“没有人认为这些项目是巨大的成功，我认为他们并没有对成功有一个明确的认识。”他说。

大学

对于大学来说，开源的价值以及与之相关的开源办公室（OSPO）来负责监督大学中开源项目与研究人员之间关系，与营利性公司有所不同。他们通常将开源视为进一步推动大学使命的途径——但直到最近，这一机会在很大程度上都被忽略了。“他们并没有真正参与开源项目的历史记录，”加州大学圣克鲁兹分校开源软件研究中心主任Carlos Maltzahn说到。事实上，虽然已经有一些成功的开源项目起源于大学，但在多数情况下，这只是少数学生或研究人员的个人项目，因为多数大学对将研究成果转化为高影响力的开源项目几乎没有支持与贡献，这是他希望改变的事情。他认为创建OSPO是支持创造开源项目学生和研究人员的途径，帮助更多项目跨越从研究项目到更广泛生态系统中使用的鸿沟。

开源在扩大知识获取的更大使命中发挥着重要作用，位于西班牙马德里的胡安卡洛斯国王大学的教授兼开放知识工作负责人Jesus Gonzalez-Barahona说到：“在整个欧洲，尤其是在西班牙，大学正在重新发现这样的一个观念，即我们需要为社会创造知识。”开源软件以及研究的开放获取，是实现这一使命的途径。

OSPO能为企业做什么?

创建OSPO的原因

当我们思考OSPO所提供的价值时，有两个不同的阶段。第一个阶段是最初创建OSPO的原因，第二个阶段是OSPO在发展成熟时所看到的价值。在本章节中，我们将讨论各组织创建OSPO的初衷，并在后面的章节中讨论OSPO所提供的价值是如何演变的。创建OSPO有多种原因，就像随着OSPO的成熟，维护和发展OSPO也有多种原因一样。虽然创建和维护OSPO可能存在教育和社会原因，但本报告主要侧重于关注创建OSPO背后的商业原因，因为我们的研究主要集中在营利性组织上。

1. 进行合规性审计

企业组织创建OSPO的最根本原因是，他们意识到公司的工程师正在使用开源软件，但他们并不知道是否遵守了项目中开源许可证的规定。“开源是不可避免的。”DB Systel（德国铁路公司的数字合作伙伴）的开源管理负责人Cornelius Schumacher说到。

鉴于这一现实，DB Systel需要进行有组织的、统一的管理，以确保公司遵守项目中的开源许可证的规定，并管理潜在的安全问题。Cornelius Schumacher认为：“风险管理并不是创建OSPO的唯一原因，但肯定是该决策的重要组成部分。”

由于新的开源项目每天都在被下载和使用，特别是在大型组织中，与其说OSPO的作用是进行合规性审计，不如说是将技术和流程落实到位，确保开发者了解哪些许可证是可接受的，哪些是不可接受的，这样在必要时就更容易进行合规性审计。

2. 构建开源标准化流程

解决相关的合规性问题，通常还需要将临时使用开源项目的方式转为更加标准化的过程。Ploug说：“现在，开源项目之间有太多的依赖关系。”创建OSPO的部分原因就是为了简化这些依赖关系，避免存在多个实现相同功能的项目。

这将使得开源管理的许多方面变得更容易，从许可证合规性审计到安全性，再到对公司核心流程起重要作用的开源项目进行战略投资。

除了围绕工程师是如何构建开源使用的标准化流程外，还需要构建关于工程师是如何贡献开源项目甚至创建自己项目的标准流程。在许多组织中，以前这些决策是由个别工程师和他们的经理作出的，结果常常导致各种方法混合在一起，对什么是可接受的方法缺乏确定性。

通常，开源办公室（OSPO）的初始任务之一就是制定关于使用和贡献开源的政策，并在整个工程组织中进行传播，其目标是消除工程师在使用和贡献开源方面的困惑。

3. 提高组织声誉

提高组织在开源生态系统中的声誉是许多公司创建开源办公室（OSPO）的重要动机。

在VMware任职的Ambiel说：“我们的目标不仅是更具战略性和目的性，还要提升我们在开源社区的声誉——被视为并被接受为开源生态系统中一个负责任的、积极的贡献者。”

这一点尤为重要，如果一家公司在之前没有任何参与项目社区的经历，突然需要一个新功能或是修复一个错误，那么这个请求就不太可能被社区优先考虑。而如果公司坚持投资社区参与，当他们有需要时，社区更有可能将其优先考虑。

在Aiven任职的Prat说：“我们需要聘请具备代码提交权限的专业人士。”这里所说的提交权限是指Aiven所依赖项目中的提交权限。获得这种权限的唯一途径是持续投资于该项目，这就是为什么Aiven成立了一个开源办公室（OSPO），以确保公司及其雇佣的个人在社区中保持活跃。

开源办公室（OSPO）也是一种分享开源知识的方式，要想参与关于如何战略性地使用开源的讨论，公司可能需要建立一个OSPO。Fukuchi表示，这种知识共享是索尼从其OSPO中获得的巨大价值的重要组成部分。

提高一个组织的声誉，归根结底是要能够与行业中的其他人进行富有成效的合作，以及参与关键项目方向的讨论。来自Wayfair的Vlatko说到：“提高我们的声誉使我们能够参与到科技界更大的市场对话中，在那里我们可以影响对我们重要的产品及解决方案。”

4. 扩大开放知识获取范围

对于大学来说，OSPO是一种增强研究影响力、使其更容易为更广泛的社区所接受或使用的方式，也是一种改善学生获取知识的方式。

加州大学圣克鲁兹分校的Maltzahn说：“学生是只阅读论文，还是看了论文后去相关的公共git存储库并获取那里的所有信息以重现实验，这是一个巨大的区别。已有研究表明，“如果你让学生参与到重现实验结果的工作中来，这比仅仅阅读论文会有更好的学习效果。”这对学生的留存非常重要。许多学生过早地放弃了计算机科学，因为他们对使用脆弱的实验系统造成的陡峭学习曲线感到非常沮丧。将开源的实用性融入到学生的学习过程中，减少他们的挫败感，既有助于他们对计算机科学的学习，又有助于他们未来在软件开发方面取得成功。

5. 提高开发速度

没有人会从创建操作系统开始构建产品——这样什么东西都建不出来。

爱立信开源经理Georg Kunz表示：“我们的产品中有很多部分几乎完全由开源软件组成，这在爱立信悠久的历史中是一次根本性变化。”开源办公室（OSPO）不仅能为公司如何使用开源项目制定秩序，而且还可以为使用哪些项目提供指导。

6. 改善人才获取渠道

开源有两种方式可以改善人才的获取，最明显的方式是让组织雇佣到更高水平的工程师，要么提高他们在开源界的声誉，要么通过创建自己的开源项目并从活跃在这些项目社区的人员库中招聘。来自Indeed公司的O'Brien说：“我的老板和执行担保人想了解我们与开源社区的关系是否健康，因为我们需要从中招聘人才。”

“我们面临的最大挑战之一，就像其他IT公司一样，是找到人来完成所有的软件工作。”

OSPO及随之而来的开源战略方法推动改善人才获取的另一种方式是，创建解决组织问题的开源项目，特别是解决组织中普遍存在的问题，而这些问题的解决并不能带来任何竞争优势。来自DB Systel的Schumacher说：“像其他IT公司一样，我们面临的最大挑战之一是找到人来做所有的软件工作。”

如果公司能够创建一个开源项目，并与业内其他公司合作，就可以在无需雇佣更多人员的情况下利用技术人才。

根据Schumacher的说法，鼓励工程师使用开源并为开源做出贡献，也是让他们感到满意并降低离职可能性的一种方式。同样的，鼓励更多的工程师创建开源项目并在开放环境中做更多的工作，也是提高现有员工技能的一种方式。

Wayfair的Vlatko表示：“如果我们向外界展示我们的代码，向外界展示我们的技术实力，那么就需要尽量表现出最好的一面。”她说，随着Wayfair鼓励员工更多地在开放环境中工作，他们发现代码质量以及对最佳实践的遵循都有所提高。

7. 降低风险

开源存在不同的风险，而正式的开源办公室（OSPO）可以帮助降低这些风险。正式设立OSPO机构的一个原因是，有一些工程师正在承担类似OSPO的职责，但没有相应的头衔或结构，这就是爱立信发生的情况。Kunz说：“我们基本上有一个单人OSPO，他负责一切事务，主要关注合规问题，就像许多OSPO一开始做的那样。但显然，这种情况是不可持续的，他不应该被繁重的工作压倒。”

创建OSPO可以使经常以临时方式来解决事情的步骤正式化，减少对关键人物的依赖，降低一位关键人物的离职可能会使公司面临的法律问题、安全事故或被排除在开源对话之外的风险。

8. 提高安全性

确保公司尽可能地保持安全，特别是厘清进入内部和外部应用程序的软件材料清单，是关于OSPO如何提供价值的一个反复出现的主题。

然而，这些例子是在战略层面，而非严格的执行层面。Indeed的O'Brien表示：“如果不与社区中正在合作开发的内容保持一致，我们就无法开发自己的安全框架，并把它应用到每一个领域。”

爱立信的Kunz在谈到软件供应链安全时表示：“从设计上讲，这是一个分布式问题，最优秀的工程师也不能解决这个问题，你也不能通过内部流程来解决这个问题。”这需要与整个行业和开源生态系统中的其他人合作。OSPO为组织提供了一种实现安全流程的方法，尽管OSPO并不最终负责实施安全流程，但他们确实分享了最佳实践，并促进开源社区、行业参与者、基金会和其他利益相关者之间的协作，以提高安全水平。

安全性也是各组织希望参与，并成为具有战略意义的项目中备受尊重的社区成员的原因之一。这使得他们参与幕后对话，不仅能了解到正在开发的任何新功能，还可以第一时间了解到任何潜在的安全问题。这样既可以帮助他们采取积极措施解决这些安全问题，也可以防止潜在的安全漏洞或数据泄露。同时，也有助于建立与客户和社区的信任，展示对安全和负责任数据处理实践的承诺。

9. 可持续性

有时开源项目会被废弃，如果你依赖于它们，那就可能会出问题。来自Spotify的Ploug说：“如果我们对挪威的单一维护者有很强的依赖性，那么应该采取一些措施来确保他们保持参与度，或是让我们的开发人员花时间投入到这些项目上，或是提供一些资金支持。”设立开源办公室（OSPO）可以帮助识别风险，否则单一维护者的情况可能会不为人知，OSPO也可找到降低风险的最佳方法。

这个问题正是促使O'Brien在Indeed创立开源软件（FOSS）基金会的原因，该基金是Indeed为其所依赖的项目维护者提供财政支持的一种方式。其目标是支持那些容易出现疲劳倦怠的维护者，以此来降低该项目最终被放弃的风险。

谁在OSPO中?

我们采访的大多数开源办公室（OSPO）的领导者都具有软件工程背景，但他们中的大多数人日常所做的工作往往与编写代码无关。相反，他们的工作内容包括内部沟通、战略规划、分析、活动策划以及与如开源社区、基金会和其他行业同行在内的外部组织合作。

在大多数情况下，OSPO团队成员，特别是OSPO领导者，都是高级工程师或管理层。在具有严格薪资等级的公司中，OSPO的领导层和团队成员往往处于薪资阶梯的顶端。

值得注意的是，法律合规的重要性在OSPO设立之初就显得尤为突出，大多数OSPO都能获得法律专业知识。然而，没有一位受访者认为应该扩大法律角色的作用，或是需要额外的法律专业知识。

谁创建了OSPO?

虽然我们通常将开源视为个人工程师的基层努力，但是采访结果表明，来自于高管层面上对OSPO的支持是一种压倒性趋势。在VMware和Futurewei这样的大型科技公司中，OSPO的支持者是CEO。来自Futurewei的Xie表示：“CEO意识到，开源不仅仅是技术问题，更是商业问题。因此，他们将开源办公室搬到了首席战略办公室，也就是我们现在的位置。”

即使在更基层的项目中，高层的参与也很常见。来自Wayfair的Vlatko说：“我自己带着这个想法去找了我们的前CTO，他非常支持，说“好，去做吧”，但也非常现实地表示，他不是专家不能指导我。我说“没关系，我是专家。”

显而易见，在许多公司中，与开源建立战略关系已经成为一个高层次的业务关注点，而不仅仅是一群工程师应该解决的技术问题。

OSPO的发展过程

许多开源办公室（OSPO）在着手解决更具战略性的问题之前，首要任务就是清理开源领域的混乱现象。很多OSPO领导者将这一步称为整顿开源现状，要从多年来零散无序地使用和贡献开源中恢复过来。

来自Spotify的Ploug表示：“过去十年，我们发布了许多项目，但却没有长远的规划或明确的归属。”目前，OSPO正逐一审查公司创建的所有项目，搞清楚它们的归属，并确保项目归属于团队而非个人。确定关闭哪些项目需要一个过程，前提是确认内部没有使用。

开源项目办公室（OSPO）在组织内管理和推广开源活动方面起着重要作用。他们在初始阶段处理的一些工作是有限的，比如关于哪些许可证可不可以使用的问题。通常，OSPO可以与法律团队合作，弄清楚哪些许可证是可以接受的。一旦做出决定，就不需要再重新审视，而是需要向整个组织传达在哪些场景下可以接受哪些许可证。

但是，当组织已经整理好内部项目，为如何使用和贡献开源项目制定了框架，并充分解决了合规性问题之后，他们接下来会做什么呢?

克服内部障碍：文化和教育

一旦OSPO制定了关于使用和贡献开源项目的政策，下一步通常是在内部推广这些政策。这是至关重要的，尤其是考虑到许多OSPO只有少数几个人，而组织内可能有数千甚至数万名工程师。OSPO承担的内部沟通作用可以追溯到最初创建OSPO的原因之一：来自软件工程师的大量关于如何处理开源问题的咨询。

“当我们谈论为开源软件做贡献时，在开始的时候，我们面临的问题是，‘我们可以这样做吗？’”来自DB Systel的Schumacher说。人们并不知道在使用开源，特别是回馈开源方面有什么规定。如果开源办公室（OSPO）的首要目标之一是弄清楚这些规定是什么，那么次要目标就是确保信息在整个组织内传播。

来自Wayfair的Vlatko说，在GitHub上建立组织结构并确定可以使用的许可证类型后，通过开展教育活动，以确保这些信息在整个组织内广为人知。

但除了预先回答工程师们关于与开源交互的问题之外，人们对开源的看法有了更大的转变。“问题的重点从是否使用开源转变为如何战略性地使用开源。”Schumacher说。“在经过一段时间后，我现在看到的是，我们正更多地关注如何利用开源进行战略合作，例如与外部公司合作。”

尽管开源无处不在，但并非所有组织都拥有他们想要的开源文化，对开源的看法也并非普遍积极。从个人贡献者到经理和高管，在他们职业生涯的某个阶段都有过使用开源软件或参与开源社区的糟糕经历，说服这些人接受开源是OSPO所面临挑战的一部分。

“我们希望文化思维转变，发展开源社区。”在F5的Abernathy说。这将是帮助该公司在开源生态系统中发挥更大作用的主要动力。从真正意义上说，OSPO力图改善开源在组织内的声誉，就像提高组织在开源生态系统中的声誉一样重要。

与开源的战略关系

毋庸置疑，开源战略的重要性因公司类型不同而异。对于像Futurewei这样的公司来说，它所销售的“黑盒子”解决方案的开源替代品，是对公司创收能力的根本威胁。“如何从商业角度而不是技术角度处理这个问题？”Xie说。

在类似的情况下，来自VMware的Ambiel表示：“说到底，VMware是做什么的？我们销售软件。因此，我们的开源投资需要与我们的商业愿景保持一致。”OSPO的存在就是为了确保这种情况的发生。

在Spotify，有一个颇有野心的计划，要把公司最成功的两个开源项目分拆成独立的业务部门，它将在项目的基础上推出商业产品，把项目从成本中心变成利润中心。OSPO在Spotify的部分作用是帮助识别和启动有可能成为新业务部门的新项目，并支持它们以增加成功的可能性。

OSPO的不同角色

顾问

开源办公室（OSPO）在制定战略方针方面发挥着至关重要的作用。有时，采取战略方法意味着需要后退一步，花时间思考一些棘手的问题：哪些特定项目适合哪种参与模式，或者组织应该在每个项目中参与的程度。还有一个问题是：在何时应该为现有项目做出贡献，而何时又应该创建一个新项目。在进行这些战略层面对话的OSPO将能够为工程师提供指导，这样工程师在尝试解决问题时就不必考虑不同开源参与模式的商业影响。

开源报告

引导者

开源办公室（OSPO）在F5公司中担任着至关重要的角色，负责在工程团队和有关开源的商业利益之间进行沟通协调。Abernathy提到，“我们如何确保工程师们能够持续投入时间在开源项目上，并能从商业角度证明这是有意义的？这正是OSPO在F5的职责之一，即传达开源项目对企业所带来的商业价值。

这些战略问题在OSPO创建之初并不总是被放在首位，特别是那些不那么专注于技术的公司，开源并没有对收入构成直接威胁。但即使是这些公司最终也会意识到，合理利用开源不仅仅是为了降低许可证的合规风险。Schumacher说：“现在我们也在研究更多的案例，从战略角度来看，利用开源对我们自己的项目或是与其他各方合作的项目具有意义。”

对于组织来说，当它们适应商业、竞争环境和更大技术生态系统的变化时，连续性是一个持续的挑战。根据Linux基金会的白皮书《关于OSPO的深入研究》，OSPO需要建立一个清晰、简单的报告程序，并确保与所有利益相关者的沟通渠道保持畅通。这对于维持OSPO的内部支持，确保组织继续遵循其商定的开源战略，并能够在开源项目和优先事项上具备可持续性的工作能力至关重要。

衡量OSPO的成功

“当我面试这个职位时，我问我们将如何衡量成功，”Prat说。“他们说‘我们还不知道’”。

这种不确定的模式在采访中经常出现——一位行政主管支持OSPO，认为开源很重要，公司需要采取实际的、战术性的步骤来确保合规性和安全性，同时也要弄清楚如何在这个过程中战略性地参与。在许多情况下，他们并不真正知道这长什么样子，OSPO最初的任务之一就是弄清楚成功是什么样子，以及如何衡量他们自己的进步。

受访者谈到使用一些指标来衡量对开源的参与，但最终放弃了。例如，Pull请求（prs）的种类太多，无法提供有意义的信息——PR可能是一个错别字的修复，也可能是一个重要的功能。衡量在开源上的工作时间似乎也不合适，因为它不能衡量影响。

决定该衡量什么是相当具有风险和战略意义的，这也是OSPO领导者本身承担了弄清这一点的任务。人类的本性是对我们知道正在评估的东西进行优化，受访者谈到了选择指标的重要性，恰当的指标将鼓励整个组织的工程师成为更好的开源参与者。通常，随着OSPO的成熟，最初应用的指标会发生变化。例如，在Indeed，最初的重点在于增加贡献者以及衡量在每一季度有多少人为开源做出贡献。然而，过了一段时间，他们开始关注增加所谓的“持续贡献者”，这些人对同一个项目，即对Indeed具有战略意义的项目进行反复贡献。这是因为对维护者来说，从一个人那里得到5份贡献比从5个人那里得到5份贡献更容易，而且更大的目标是让维护者的工作更容易。

通常，很难用数字来量化OSPO表现的情况。“我个人衡量成功的标准是继续提升VMware在开源方面的声誉和领导地位。”Ambiel说。“我在这方面的成功指标是相当定性的。”她谈到了感知研究、声音份额，以及社区系统地分享VMware的故事或贡献的时间。单独地看，这些指标可能是模糊的，但它们“加在一起形成了一个整体，表明我们正在取得进展。”

常见的OSPO关键绩效指标

那么，一旦OSPO有时间考虑哪些指标能鼓励有益的行为并与OSPO真正的目标相一致，他们最终会衡量什么？

持续贡献者：组织中对同一项目进行定期、反复贡献的人数（假设这些项目对组织具有战略意义）。

成功发布项目：组织发布项目的外部参与和影响。O'Brien举了一个例子：Indeed发布的一个项目被CNCF Sanbox视为极大成功的衡量标准。来自UC Santa Cruz的Maltzahn提到，不仅要衡量所发布的项目，还要衡量这些项目在吸引校外更广泛的追随者方面的成功程度，以及这些项目在没有大学持续参与的情况下是否能够长期生存。

开源的内部声誉：人们是否知道OSPO的存在？他们是否知道OSPO围绕着如何使用开源、贡献现有项目，或创建新项目而建立的参数？许多公司追踪这些内部意识指标，因为他们的很大一部分作用是负责内部沟通。

组织在开源社区中的声誉：对于许多公司来说，建立OSPO是为了提高组织在更大开源生态系统中的声誉，他们通常会追踪声誉和意识指标，如社交媒体的提及，提到公司参与开源的求职者数量，或在开源相关会议上发言的员工数量。有些公司会对第三方的开发者进行调查，并提出与声誉有关的问题。

减少开发者的响应时间：除了追踪内部团队对政策的了解程度外，OSPO还经常追踪他们为这些开发者带来了多少响应。例如，如果一个人需要批准一个贡献请求，需要多长时间？

追踪项目的健康状况：追踪组织所依赖的“健康”项目的百分比。判断一个项目的健康状况，通常需要追踪活跃贡献者的数量，提交的频率，维护者的数量，以及其他指标，包括有来自许多不同组织的用户和贡献者。

外部合作：OSPO正在与多少个伙伴积极合作？这可以采取参与合资企业或赞助项目的形式，特别是在大学之间。或者积极加入开源基金会和行业团体。其他积极的外部合作的例子包括作为发言人、代表或赞助商参与会议，以及参与研究开发过程，正如本报告中的许多受访者所展示的那样。

还有一些联合项目，以确定追踪的最佳指标：TODO小组和CHAOSS创建了OSPO指标工作组，以帮助开发更好的指标，供OSPO衡量自己的成功。

关键绩效指标检索

许多OSPO领导者强调，谈论量化指标不仅是困难的，而且可能导致误导性的结论。许多OSPO只是没有可衡量的目标。来自Ericsson的Kunz说：“我们对团队的期望目标是相对较高的。”

“我觉得我们应该远离数字。”来自VMware的Ambiel说。“数字并不能说明问题，并且在开源领域可能会产生误导。”

Ambiel说，关注数字的部分危险在于，OSPO的最终目标是推动公司成为开源生态系统中更好的参与者，而成为一个好的成员是永无止境的。“没有一个指标你可以说，好吧，我完成了，检查一下。”她说：“你可以一直接近，你将一直努力做到更好。”

在时间跨度方面也可能存在问题。来自Aiven的Prat说：“每个公司都试图用三个月的时间跨度来衡量事情。”但是开源维护者并不关心你是否需要达到接受贡献的季度目标；他们不会围绕季度目标或财政年度来安排开源项目。

还有一种感觉是，OSPO在不断地发展，因此，要追踪的正确关键绩效指标也在不断地发展。“我们现在正在寻找那个有效的关键绩效指标，因为我们的活动在变化，现状已经改变，所以我们需要调整关键绩效指标。”Fukuchi说。

结语

未来会有什么？

在一点上，所有受访者都有绝对的共识：OPSO在未来将继续发展。特别是，OPSO越是成熟，它就越能进行战略思考，并帮助整个组织制定更具战略性、深思熟虑的开源方法。他们不期望更多的关注会在法律和合规层面上——这是一个大多数受访者认为更像是多项选择的最低限度，而且他们已经搞定了。

一些受访者谈到，希望OSPO在影响他们公司未来采用哪些技术和项目方面发挥更大的作用。还有人希望OSPO能够深入依赖关系链，更好地了解他们所依赖的项目（即使它在下面两三个级别），追踪这些项目的健康状况（并在必要时作出贡献）。还有人谈到了建立自动化平台来处理一些目前手动操作的任务，比如批准对项目的贡献请求。

Kunz说：“OSPO需要制定一个战略，把它建立起来，然后让开发者加入进来，做正确的事情。”Kunz和其他许多人认为，OSPO应该致力于愿景和战略，并确保他们与整个公司合适的人员达成合作，将愿景变为现实。

归根结底，OSPO的部分职责就是与开源和它所提供的商业价值进行对话。这是开源布道的一部分，这也是许多OSPO使命的一部分。Schumacher说：“我认为其中一个重要的部分是真正让人们理解其商业价值。”

这并不容易，因为开源并不总能将商业领袖所考虑的事情完全转化，但是这很重要。企业领导者通常知道开源是重要的，但他们需要OSPO来帮助他们理解为什么，然后利用这些信息从开源中获得更多的价值。

群聊：开源发展态势讨论群

扫码参与
开源发展态势讨论、开源发展专题投稿

开放原子开源基金会兼具科技、公益、慈善属性，以“繁荣开源事业、共享开源价值”为愿景，遵循“以开发者为本的开源项目孵化平台、科技公益性服务机构”的定位，以“打造科技创新共同体、孵化明星开源项目、构筑技术竞争优势、培育新兴产业生态、助力新一代信息技术和产业发展”为目标，致力于提升我国对全球的开源贡献。在开源繁荣发展的背景下，开放原子开源基金会推出《全球开源态势发展洞察》，现已发行五期。为推动更多的社会大众能认识开源、了解开源、参与开源，现诚邀各位开源专家、开源大使、开源爱好者等开源人输出关于开源的权威、专业、前沿的观点及内容，为促进全球的开源发展贡献出一份力量！

联系人：赵海玲　电话：18811327865　邮箱：zhaohailing@openatom.org

版 权 声 明

编写委员会

主编：刘京娟

编写小组：赵海玲、郭雪雯、张苏兵、梁婷婷、王铭典

封面设计：马坷

地址：北京市北京经济技术开发区科谷一街8号院8号楼22层2201
https://www.openatom.org
资金捐赠：sponsorship@openatom.org　项目捐赠：sponsorship@openatom.org