



# 开源软件许可证合规的一般公共指南

Open Source Software License Compliance General Public Guide

# 目录

介绍 .....	1
学习开源软件 .....	2
您需要做什么来获得OSS的益处 .....	4
因未能合规而引起的风险 .....	6
供应链问题 .....	8
需要与软件一起提供的OSS信息 .....	10

## 介绍

开源软件 (OSS) 已经成为现代软件开发的基础。OSS几乎被应用到所有电子产品中，包括超级计算机、云服务器、个人电脑、家电产品、汽车、工业设备和物联网设备。即使在激烈的竞争中，企业也需要开发出高质量、并能更快及时投放市场的产品或服务。企业还必须跟上最新的技术趋势。OSS在这一激烈角逐中是不可或缺的。

许多OSS是通过来自世界各地不同组织的专业开发人员协作开发而成的。OSS通常是各领域高阶创新的驱动源。参与开源开发的软件工程师有机会提高他们的技能，并直接体验这种创新。

任何遵守相关许可证条件的人都可以自由地使用、修改和分发OSS。在分发OSS时，分发者被要求在分发时遵守许可证条款和条件。在某些案例中，分发者曾因未能履行其法律义务而被起诉并败诉。因此，为了减少使用OSS所带来的风险，所有相关人员都必须理解OSS的基本原理。

这本小册子是由Linux基金会的OpenChain项目所编写，旨在让尽可能多的人了解关于OSS的基本原理。

2019年5月

# 学习开源软件

让我们学习一下开源软件 (OSS) 的基础知识。

本小册子解释以下内容：

1. 什么是开源软件？
  2. 您需要做什么来获得OSS的益处
  3. 不能履行OSS职责可能产生的风险
- 不幸的是，曾发生过这样的案例：一家公司未能履行其OSS许可证职责，结果被著作权所有者起诉。
4. 供应链问题
  5. 您需要做什么来确保每个人都能从OSS中受益

第3点和第4点可能是相互关联的。如果OSS是通过供应链获得的，那么供应链中的所有环节都必须符合许可证的条件。如果任何一个环节未能满足许可证的条件，那么供应链后段的组织将无法弥补这些缺失的条件。独自作业的受雇者或公司无法履行所有的职责，也无法满足所有的要求。

当带有OSS软件的项目被交付给另一方时，必须提供与OSS相关的所有信息。以下人员应理解在取得及分发OSS时应遵循的正确程序：

- **开发人员和工程师：**除了软件开发人员外，硬件工程师也深入参与为其硬件开发设备驱动程序软件、板级支持包 (BSP) 和软件开发工具包 (SDKs)。
- **采购人员：**OSS可能包含在供应链的交付物中，例如软件、硬件模块、SoCs、半导体产品，以及由ODM/OEM制造商设计和开发的产品。
- **销售人员：**销售人员应了解客户需要OSS相关信息的原因，包括著作权和许可证信息。
- **质量保证人员：**包含在产品中的OSS可能会影响其质量或引入程序错误。质量保证人员需要了解这些问题。
- **法律/知识产权人员：**法律和知识产权人员需要了解与OSS许可证解释和遵守相关的法律、法律判例和法律补救措施。
- **高管和经理：**高管和经理围绕OSS使用、贡献和分发开发策略，构建团队以促进OSS的使用；监督OSS流程，以及对所需软件工具进行投资。

\* ODM: Original Design Manufacturer (原始设计制造商)

OEM: Original Equipment Manufacturer (原始设备制造商)



## OSS的定义

准确地回答“什么是OSS?”并不容易。不同的人有不同的答案。然而，大多数人会同意以下观点：

OSS是提供源代码的软件。著作权所有者允许其他人使用、检查、修改和共享软件。

## OSS的示例

Linux可能是最广为人知的开源软件示例。操作系统(OS)是为其他软件提供平台而设计的软件。Linux就是这样一个操作系统。Linux用途广泛。它几乎被应用到每个主要的计算系统中，包括超级计算机、股票交易所服务器、互联网服务器、使用Android(安卓)软件栈的智能手机、家电产品、汽车和工业设备。Linux支持着世界上极大比例的核心技术基础框架。

Linux是通过世界各地成千上万的开发人员的协作开发出来的。Linux开发每天都在活跃地进行着。任何人都可以自由使用、修改和分发Linux，只要遵守Linux开发人员选择的许可证条件。使用Linux的公司理解并遵守Linux的许可证条款是非常重要的。

除了Linux之外，还有大量其他的OSS项目。其中包括用于HTTP服务器的Apache项目、广泛使用的编译器GNU编译器集合(GCC)和Eclipse集成开发环境，等等。

## OSS和许可证

OSS的著作权所有者并没有放弃代码中的著作权，而是基于用户对软件许可证条件的遵守，授予用户对软件的某些权利。在某些情况下，著作权所有者可能授予用户专利许可证。对于开源软件的用户来说，理解他们所使用的每一个OSS的许可证是至关重要的。

几乎所有的OSS许可证都免除OSS开发人员的责任。在几乎所有的情况下，OSS开发人员都不承担使用OSS的责任，而是要求用户、产品集成商和供应商自己承担此责任。

并非所有软件都受著作权保护。如果您需要判断一个特定片段的OSS是否为受著作权保护的材料，您应该向律师或知识产权专家咨询。

## 通过许可证(著作权)授予什么

对于某些OSS许可证，著作权所有者授予其他人使用或分发软件的权利。这种许可证授权发生在著作权所有者和用户之间没有直接沟通的情形，但只有当用户遵守著作权所有者在许可证中提供的条件时才被授予该使用权。当用户不能遵守这些许可证条件时，就会产生严重的问题。

## 通过许可证(专利)授予什么

对于某些OSS许可证，OSS的著作权所有者授予其他人自由使用通过软件进行实践并由著作权所有者拥有的专利的权利。并不是每个OSS许可证都授予这样的专利许可证。包含此类专利授权的许可证的示例包括Apache许可证和GNU通用公共许可证(GPL)第3版。

## 典型的OSS许可证

开源促进会(OSI)是一个推广OSS的组织。它定义了构成OSS的标准，并批准数十个不同的许可证作为有效的OSS许可证。

<https://opensource.org/licenses>

<https://opensource.org/osd>

大多数OSS都是在采用OSI批准的许可证发布许可的。除此之外，一些采用非OSI许可证发布的软件也仍可能被视为开源软件。此类软件是否应被视为OSS(或以其他方式处理)，应就软件供应者和收受者之间的协议来决定。

# 您需要做什么来获得OSS的益处

当您使用OSS时，需要了解的最重要事项是与软件分发相关的义务。

几乎所有的OSS许可证都定义了以下内容：

- OSS开发人员对使用该软件的影响不承担责任
- 当软件由个人或法人（分发者）分发时，有些义务必须被履行。  
\* 在以下几节中，分发者可以指个人，也可以指公司等法人。

任何遵守本许可证条件的人都可以自由使用和分发本软件。

然而，不同的许可证有不同的条件。有些许可证只要求在源代码发布中包含许可证声明和著作权声明。其他许可证要求公布源代码并提供获取源代码的书面要约。有些许可证的条款会影响同时分发的软件能与哪些其他OSS结合使用。分发者必须履行许可证中定义的所有义务。

有几种方式视为分发软件。一种方式是销售包含OSS 软件的产品。另一种方式是提供一个可以下载软件的网站。当包含OSS的项目被分发时，分发该项目的实体必须遵守该OSS的许可证。



## OSS分发示例

有几种不同的方式可以分发OSS。在每种情况下，分发者都必须遵守OSS许可证。

### 1. 分发OSS的一种方式是使用半导体供应商提供的SDK（软件开发工具包）开发产品。

如果SDK中包含的OSS在开发过程中被并入到产品中，那么这意味着半导体供应商在通过包含到SDK中来分发OSS，而产品开发人员则在通过包含到产品中来分发OSS。这种情况下，产品供应商有责任遵守许可证。但它们依赖于半导体供应商。如果半导体供应商没有提供有关包含到SDK中的OSS的适当信息，则产品供应商无法遵守OSS许可证。

### 2. OSS可能被分发的另一种方式是采用ODM或OEM的委托方式为制造商设计和开发产品。ODM或OEM可以将OSS并入到产品中，这是产品分销商需要了解的。

即使是OEM或ODM制造了该产品，该产品的品牌所有者也会分发并入在该产品中的OSS。品牌所有者必须遵守OSS许可证。如果ODM或OEM制造商没有提供有关OSS的恰当信息，则产品的品牌所有者无法遵守OSS许可证。

### 3. 分发OSS的其他方式包括贩售产品、发布移动应用软件，或者为之前贩售的设备提供软件更新。

如果OSS被包含在产品、移动应用程序或软件更新中，这就构成了OSS的分发。贩售产品或发布软件的实体必须遵守OSS许可证。

### 4. 网页中使用的JavaScript构成分发：

当网页被传输到用户的机器上时，可能会发生一种有趣的OSS分发情况。

当用户访问页面时，被包含到网页中的JavaScript作为页面数据的一部分，被从web服务器传输到用户机器上的浏览器。如果此JavaScript程序是OSS，那么这就构成了分发，许可证条款将发生效力。

## 当OSS被分发时需要履行的义务

当OSS被分发时需要履行的义务因许可证而不同。在一个被分发的产品或程序中识别所有的OSS和相关的许可证是很重要的。

这需要清楚地理解所有必须满足的不同许可证条款。

## 宽松许可证

MIT许可证、BSD许可证和Apache许可证要求的义务很少。这些许可证要求分发软件的著作权声明和许可证文本。声明应该清楚地显示在收受OSS的人能够阅读的地方。

## 互惠许可证

GPL许可证、LGPL许可证、AGPL许可证和Mozilla公共许可证要求公布相关软件的源代码。（源代码中的许可证和著作权不得删除。）如果分发者修改了源代码，那么所有源代码的修改必须被公布。互惠许可证旨在建立一个环境，在这个环境中，人们可以在软件的所有用户和开发人员之间共享修改和改进。

除了公布源代码之外，这些许可证通常还要求履行其他义务。要在互惠许可证下分发软件，您必须理解这些义务。如有需要，您应咨询您的法律及知识产权工作人员。

## 您不能授予的专利

在某些情况下，OSS许可证可能要求分发者为其用户授予包含使用的或添加到OSS的软件中的专利许可。如果您有这样一个不能授予用户许可的专利，您就不能分发包含此种许可证条款的OSS。

## 因未能遵守而引起的风险

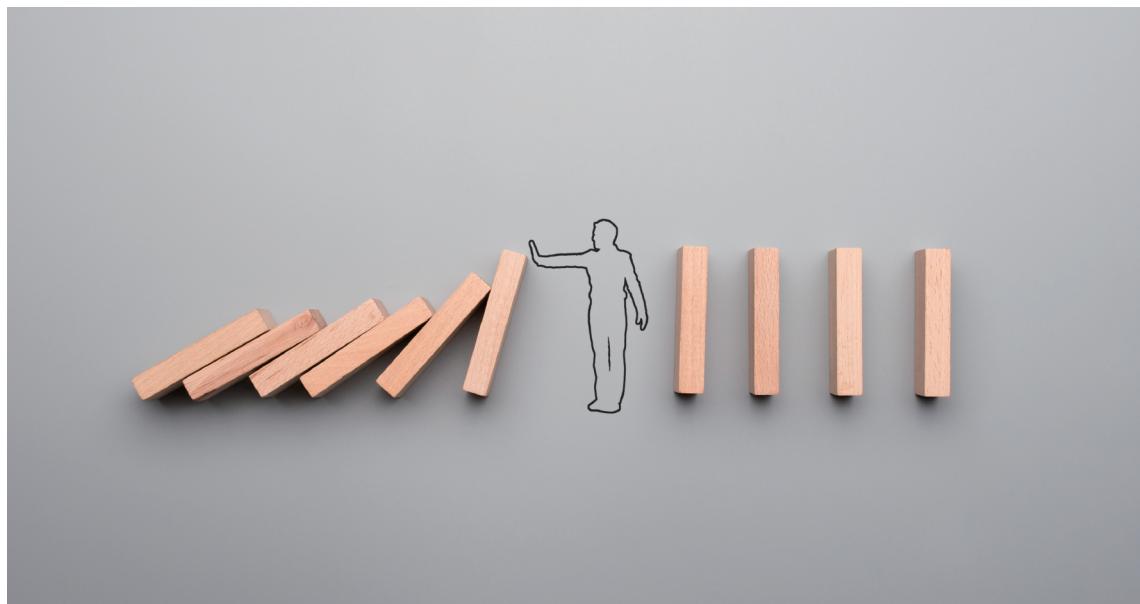
OSS著作权所有者对未能遵守许可证的公司提起诉讼。

不幸的是，由于未能遵守OSS许可证，导致OSS著作权所有者对用户（和分发者）提起诉讼是曾有一发生的。在至少一宗案件中，曾有一项判决要求被告暂停贩售包含有OSS的产品。

2009年12月，发生了一起与名为“Busybox”开源软件有关的诉讼。Busybox程序被广泛地并入到嵌入式系统中，并根据GPL第2版许可证进行授权。在这起案件中，有14家公司成为诉讼对象，其中包括一些家用电器行业的公司。这宗案件的值得注意之处在于，公司因ODM制造商生产的产品而被起诉。

在每宗案例中，都是因分发者未能遵守OSS许可证而导致诉讼。为避免诉讼，工作上使用OSS的实体应：

- 识别要分发的软件中的每一个OSS
- 理解OSS许可证定义的义务，并遵守这些义务。



## 诉讼中会失去什么

当公司被起诉时，对公司最大的损害之一就是其名誉（名誉风险）。未能遵守软件许可证的坏名誉可能会导致公司失去其他公司的信任。一个公司越了解其信任关系的重要性，并努力在整个行业建立信任，就越会认真地去避免名誉风险。

回应诉讼需要大量的劳力和费用。在没有诉讼的情况下，涉及法律、采购、工程和合规的人力资源可以用于更具建设性的任务。这意味着，一家公司花费时间回应诉讼，可能会错失那些人力资源有可能从事的其他商业机会。特别是，聘请一个可以胜任的律师进行OSS诉讼是非常昂贵的。

和解或法律判决可能需要支付金钱或罚款。在极端情况下，判决可能导致产品的暂停贩售，这有可能造成相当大的损失和昂贵的代价。

## 与OSS社区建立良好的关系

为了减少诉讼风险，理解OSS原则并遵守OSS许可证的义务是至关重要的。此外，郑重地建议您为OSS社区做贡献，并与您所使用的OSS开发人员建立良好的关系。

如果您理解了为什么作者为他们的软件选择了特定的开源许可证，以及支持OSS项目的OSS社区的意愿，它将帮助您更进一步，而非仅仅履行OSS许可证的字面意思。理解开发人员的意图是与OSS社区保持良好关系的最重要的益处之一。

与OSS社区保持良好关系可能使公司能够将自己的新创意纳入OSS中。OSS社区可能会根据您的创意和需求来改进软件。此外，您公司的工程师可能有机会与高技能的OSS开发人员合作，这将造就您的工程师更高的满意程度和技能。

随着系统软件在规模和功能上的增加，它变得越来越复杂。编写出没有程序错误的软件越来越难。然而，如果一家公司与OSS开发人员具有良好的关系，社区可能会帮助您的工程师在开发软件时发现并解决程序错误。

## 为OSS社区做贡献

为OSS社区做贡献的方式有多种多样：提出程序错误修正方案和新功能、翻译文档、提供社区成员可以交流的场所和论坛、赞助和参与支持OSS的项目和商业协会（例如Linux基金会）。

## 供应链问题

OSS合规不能由一个人单独完成。

随着软件变得越来越大、越来越复杂，软件供应链也变得越来越大、越来越复杂。现代软件供应链可能包括一个OSS社区、一个软件供应商、一个提供SDK的半导体供应商和一个最终产品供应商。如果大型、复杂的软件供应链中任何成员不能遵守许可证义务或不能提供适当的许可证信息，则将对有义务遵守许可证的供应商造成重大影响（图1）。违规可能导致产品被暂停贩售。如果供应商在贩售前不知道违规，则可能会收到著作权所有者或第三方提出的关于违规的询问，而供应商无法对此作出回应。

然而，如果在上游供应链中适当地管理软件合规，这些问题则是可以避免的。为了促进对OSS许可证的遵从，供应链中的所有参与者都必须履行自己的职责，在整个供应链中建立信任，并就包含的软件进行适当的信息沟通。

建议供应链中的每个公司都建立一个团队，以确保供应链中的OSS合规。Linux基金会的OpenChain项目提供了一个自我认证程序，公司可以使用它来实现此目的。该自我认证程序将帮助公司检查其合规流程。认证测试有多种语言版本可供选用，任何人都可自由使用。

<https://certification.openchainproject.org/>

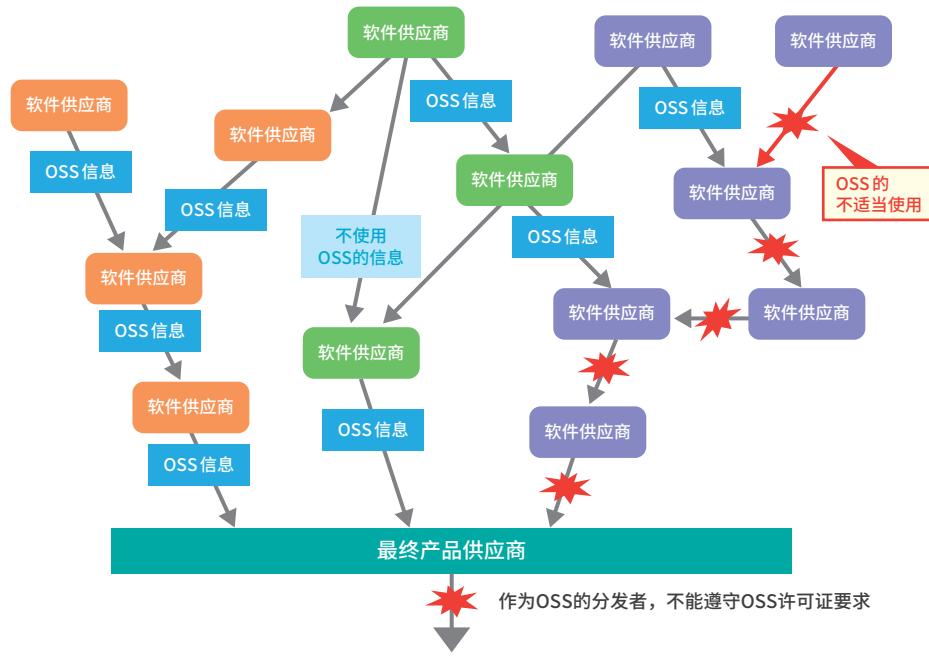


图1 软件供应链问题

## 对供应链参与者的要求

当供应商分发软件时，供应商被要求向每个收受者提供遵守OSS许可证所需的信息。收受者应仔细核审数据和文件，并验证其准确性。

对于单个产品，软件分发者可将多个供应商的软件包含其中。这种情况下，分发者被要求接收关于其接收到的软件的每个OSS组件的信息。

如果没有收到OSS组件相关的信息，则不应将此类OSS并入到产品中。

## 公司中不同的角色对OSS合规承担不同的责任

### 软件开发人员

软件开发人员应该管理、记录和存储软件的配置。这包括以下内容：

- OSS及其许可证；
- 链接（如软件使用的库、动态或静态链接等）；
- 修改。也就是说，对软件所做的任何修改的技术细节。

必须标识并列出这些项目。每当软件配置发生变动时，都应该更新列表。对于特定的项目，许可证可能从一个软件版本到下一个版本时发生变动。建议创建和管理列表，以便每个OSS项目可被轻松地索引和核审。有些许可证（例如，GPL许可证）要求分发者公布源代码。郑重地建议使用源代码控制管理软件来跟踪原始源代码和对源代码的任何更改。

### 软件采购人员

软件采购人员必须取得来自外部软件的任何有关OSS的信息，以便软件工程师进行记录。OSS可能包含在软件中，如半导体供应商提供的SDK。

采购人员需要注意公司收受到的所有不同类型的交付物中的软件。

### 销售人员

销售人员需要与客户就OSS进行沟通。客户可能有与OSS使用相关的特殊要求。例如，公司可能制定了一个OSS政策来禁止使用带有特定许可证的OSS。

对于销售人员来说，了解客户对OSS的要求，并将这些信息传达给内部软件开发人员是非常重要的。

### 法律/知识产权人员

与法律和知识产权人员的合作对于理解OSS许可证是不可缺少的。法律和知识产权人员应核审管理公司使用的OSS的许可证，并就其使用向开发人员提供建议：

- 使用OSS需要哪些批准？（一般来说，OSS许可证免除软件开发人员的责任。）
- 分发OSS需要什么？
- 当软件被下游收受者使用时，包含到OSS会不会导致问题？

### 高管和经理

要有效率且恰当地使用OSS，需要公司内部不同人员的协作。

高管和经理或需要促进内部组织之间的协调，并决定建立一个专职的团队来管理OSS相关的问题。这包括对人力资源、培训和开发环境的投资。

## 需要与软件一起提供的OSS信息

为了确保每个人都能从OSS中受益，人们需要弄清关于OSS的哪些信息必须与软件交付物一起提供。



本小册子解释了维护OSS列表和遵守OSS许可证的重要性。

软件交付物应该提供哪些关于OSS的信息呢？本节解释必须与OSS一起分发的特定信息。由于所需的信息因业务和公司策略的不同而有所差异，请与每个收受公司进行细节沟通。

当软件交付物中没有包含OSS时，您应该清楚地向收受者传达“交付物不包含任何OSS”。然后收受者可以采取相应的行为。

当OSS包含在软件交付物中时，您必须清楚地标识出这样的软件及其许可证。例如，许可证可能在不同版本的OSS之间之间产生改变。每个OSS组件的名称和版本是不可或缺的信息。对于每个组件，提供软件的下载位置或主要项目源站点或网站是有帮助的。这允许收受者验证有关软件、其版本和许可证的信息。

当OSS许可证要求分发者公布源代码时，请提供源代码。具体被要求的源代码取决于OSS许可证。例如，GPL/LGPL 3许可证的第3版要求，除了软件的源代码外，您还必须提供基于代码重新安装修改后的二进制代码所需的信息。

## 必须与OSS一起分发的信息

以下信息必须与包含OSS的交付物一起分发。

- OSS组件列表

**对于每个OSS组件：**

- 识别软件的信息 (版本号、源代码来源 (例如，网站URL) 以及如何获取软件)
- 可适用的许可证列表、以及 (如果多于一个) 哪一个您的公司正用来分发这个OSS
- 您对软件所做的任何修改

**关于许可证中要求分发者提供许可证和著作权声明的OSS：**

- 实际的许可证文本和著作权声明

**关于许可证中要求公布源代码的OSS：**

- 所需的源代码 (对于GPL，除了源代码外，还必须提供脚本以用于从源代码创建生成可执行程序)

某些情况下，当一个OSS组件本身包含一个次级的OSS组件时，还必须为次级的OSS组件提供信息。

大致如上述信息。一个客户可能需要某些信息，而另一个客户则可能需要其他信息。与客户就他们需要的信息及其格式进行沟通是非常重要的。

## SPDX项目

由Linux基金会主办的SPDX® (软件包数据交换®) 项目，具有用于交换许可证信息的标准格式。

任何人皆可以使用这种格式，强烈建议在整个供应链中使用。有关此格式的资料，请浏览：

<https://spdx.org/>

## 源代码扫描工具

有扫描工具可以检测软件包中的OSS并自动生成一些信息。例如，托管于Linux基金会的FOSSology项目开发了这样一个扫描工具。FOSSology工具使用在OSS许可证提供，且可被任何人自由使用。也有使用其他具有商业许可证的扫描工具存在。建议在开发期间和贩售之前使用这些工具来验证软件包中的OSS许可证。

有些扫描工具能够根据SPDX规范生成报告。这些扫描工具对于信息非常有用，信息可以直接包含在交付给客户的交付物中。

## **关于OpenChain项目**

OpenChain项目通过使开源许可证合规更简单、更一致，从而建立对开源的信任。OpenChain规范定义了每个优良品质的合规程序都必须满足的一组核心要件。OpenChain一致性允许组织展示它们对这些要件的依从性。OpenChain课程通过为有效的开源培训和管理提供广泛的参考资料，来支持此过程。其成果是，对于软件供应链中的所有参与者来说，开源许可证遵从变得更加可预测、可理解和高效率。

<https://www.openchainproject.org/>

## **关于Linux基金会**

Linux基金会致力于围绕开源项目构建可持续的生态系统，以加速技术开发和企业应用。

Linux基金会成立于2000年，通过资金和智力资源、基础设施、服务、活动和培训，为开源社区提供了无与伦比的支持。通过共同努力，Linux基金会及其项目形成了共享技术创建中最雄心勃勃且成功的投资。

<https://www.linuxfoundation.org/>



