ISCAS 中国科学院软件研究所学术年会 暨重点实验室科技活动周 2025 第十届

学术论文

软件供应链 SBOM 关键技术研究

孙泽雨, 吴敬征, 凌祥, 魏怡琳, 罗天悦, 武延军

软件学报, 2025, 36(6)

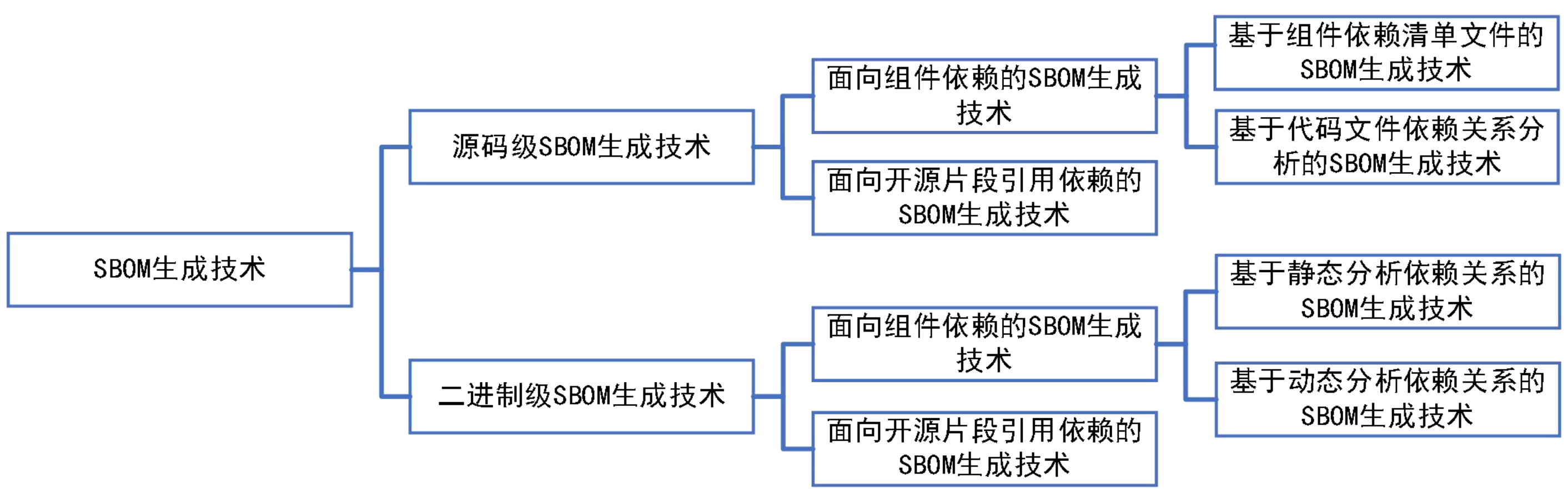
sunzeyu0412@sina.cn, jingzheng08, lingxiang@iscas.ac.cn

背景与动机

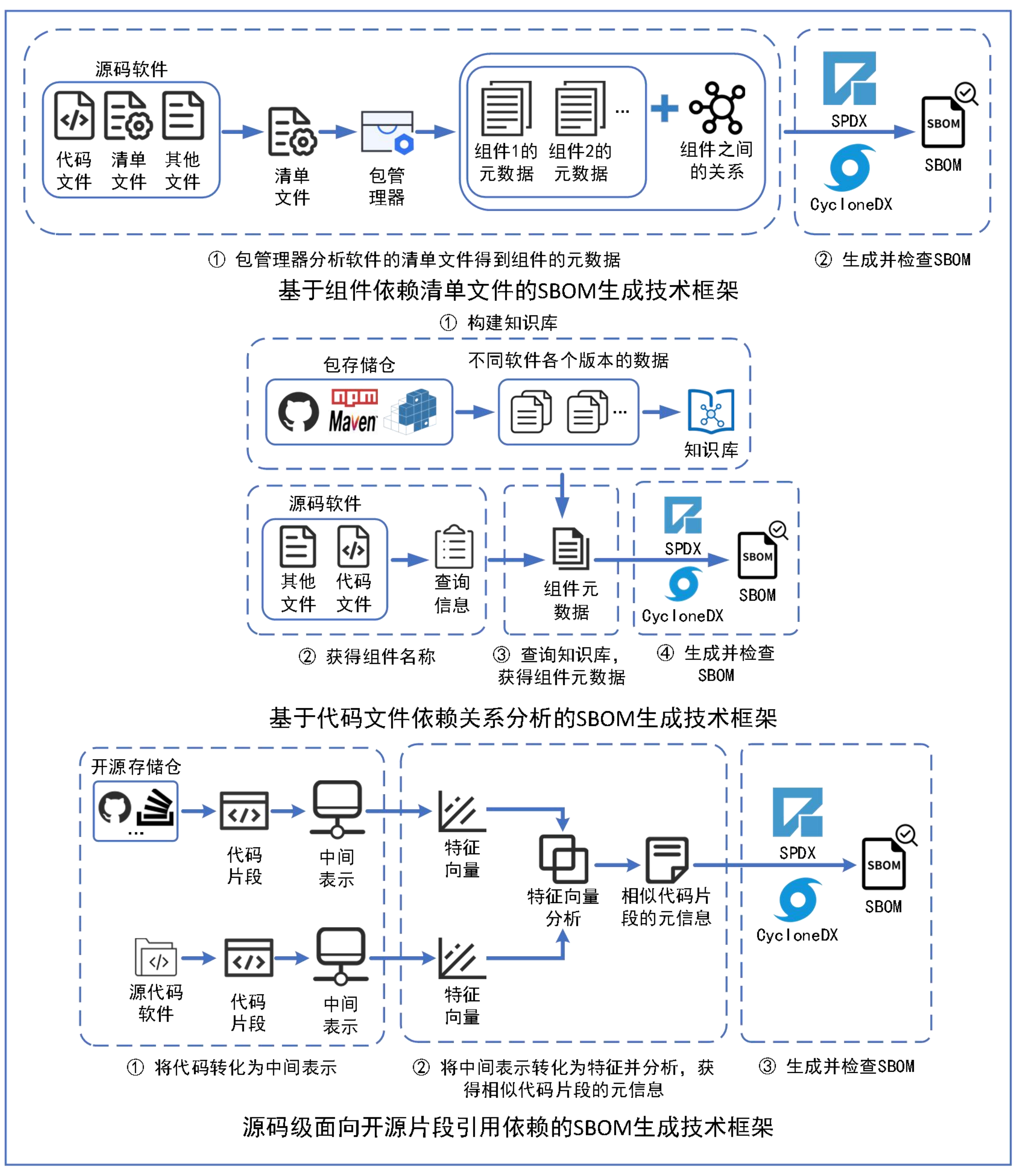
供应链级别的开源软件及组件复用是当前软件开发的主流模式，虽能避免重复开发、降本增效，但也带来组件来源未知、成分不清、漏洞不明及许可证违规等问题。为此，研究人员提出了软件物料清单(software bill of material, SBOM)。 SBOM 详列软件组件及其关系，揭示威胁并提升软件透明度。现有研究多集中于 SBOM 的现状、应用与工具，缺乏理论与体系的构建。本文综述 SBOM 的背景、概念、生成技术、工具分析、应用、挑战及趋势，并提出融合细粒度漏洞感知与许可证冲突检测的 SBOM+，旨在为相关研究人员提供多维度支撑。

SBOM 生成技术

SBOM生成技术主要依据分析对象和分析粒度进行分类。按分析对象，可分为针对源码软件和针对二进制软件的技术。按分析粒度，两者都包含识别组件依赖的技术和更细粒度的识别开源片段引用依赖的技术。在组件依赖技术中，源码级可细分为基于组件依赖清单文件和基于代码文件依赖关系分析的方法；二进制级则细分为基于静态分析依赖关系和基于动态分析依赖关系的方法。



SBOM生成技术分类



基于组件依赖清单文件的SBOM生成技术框架

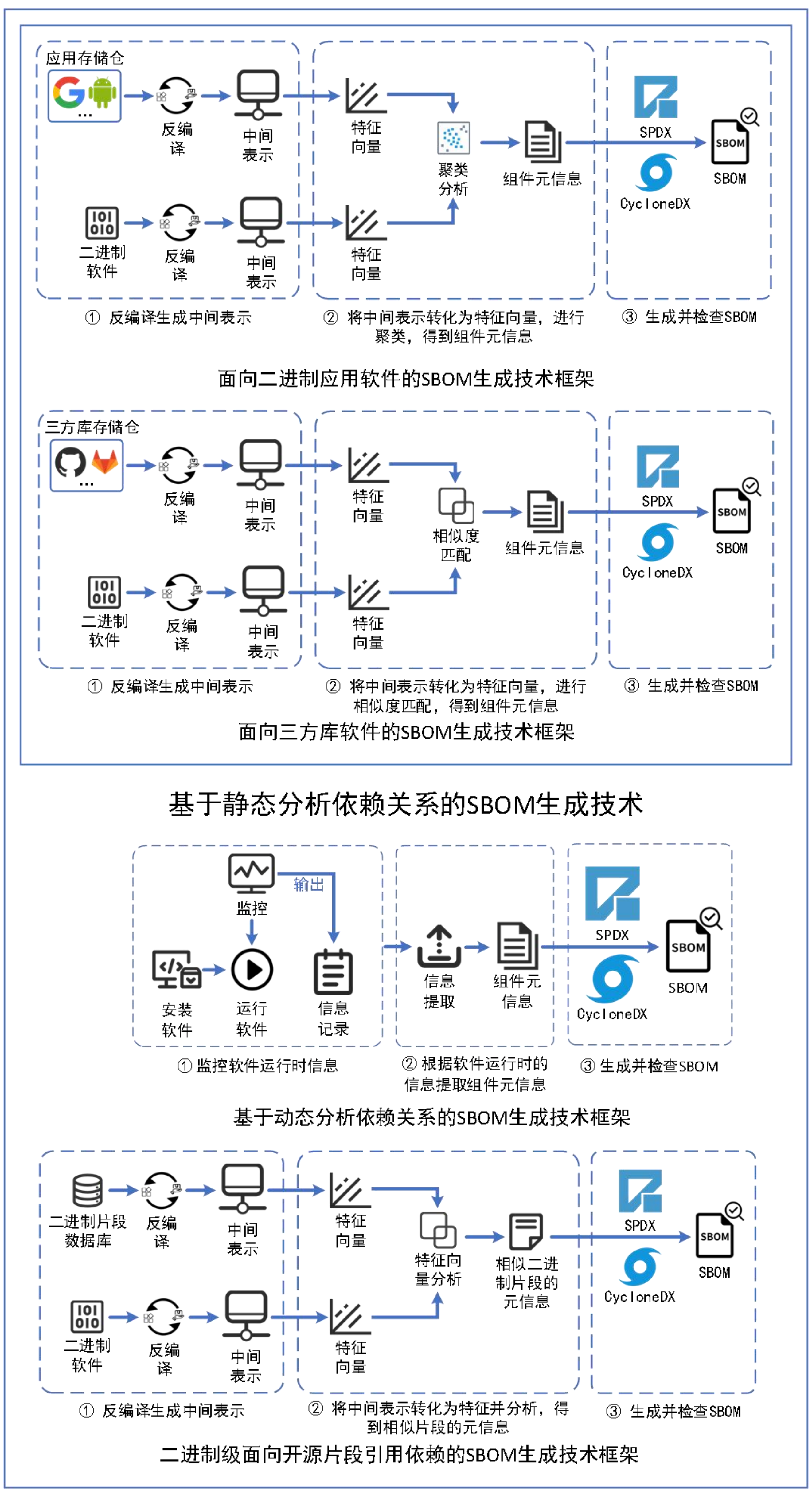
基于代码文件依赖关系分析的SBOM生成技术框架

源码级面向开源片段引用依赖的SBOM生成技术框架

源码级SBOM生成技术

SBOM 的应用

NTIA 将软件供应链简化为 3 个核心角色：开发者、选择者和操作者。3个核心角色可以借助SBOM实现软件供应链管理，具体包含安全风险分析和合规性分析。



面向二进制应用软件的SBOM生成技术框架

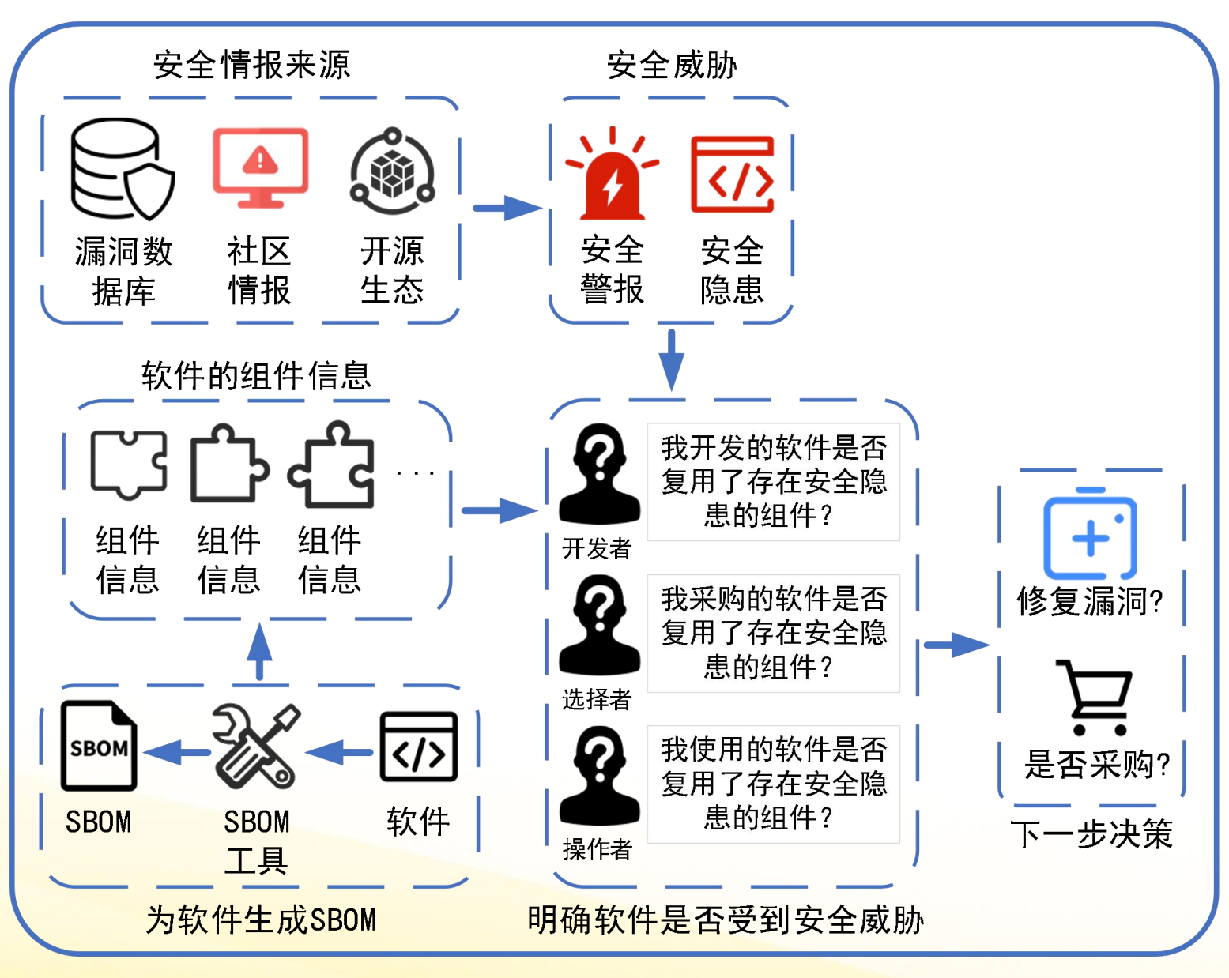
面向三方库软件的SBOM生成技术框架

基于静态分析依赖关系的SBOM生成技术

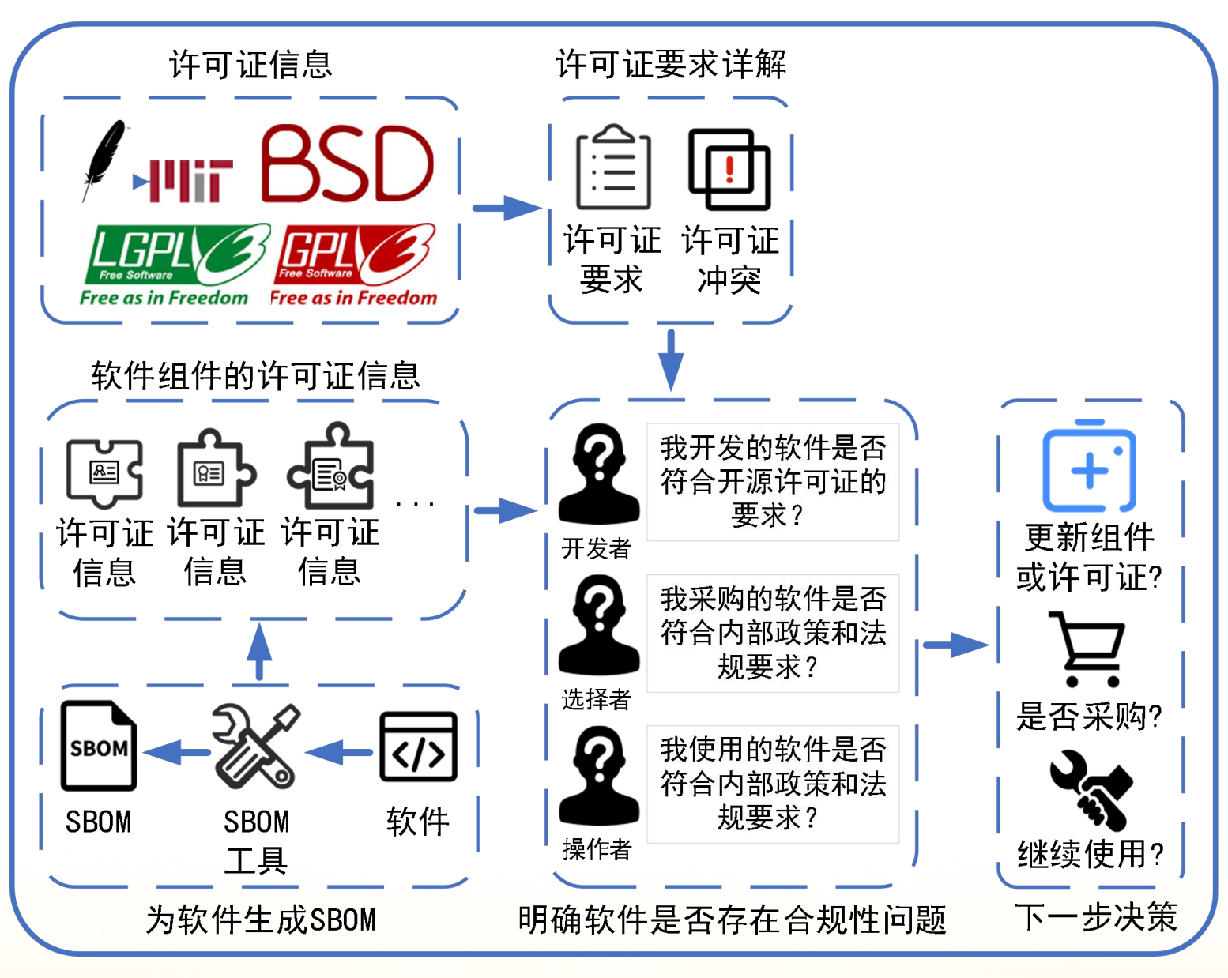
基于动态分析依赖关系的SBOM生成技术框架

二进制级面向开源片段引用依赖的SBOM生成技术框架

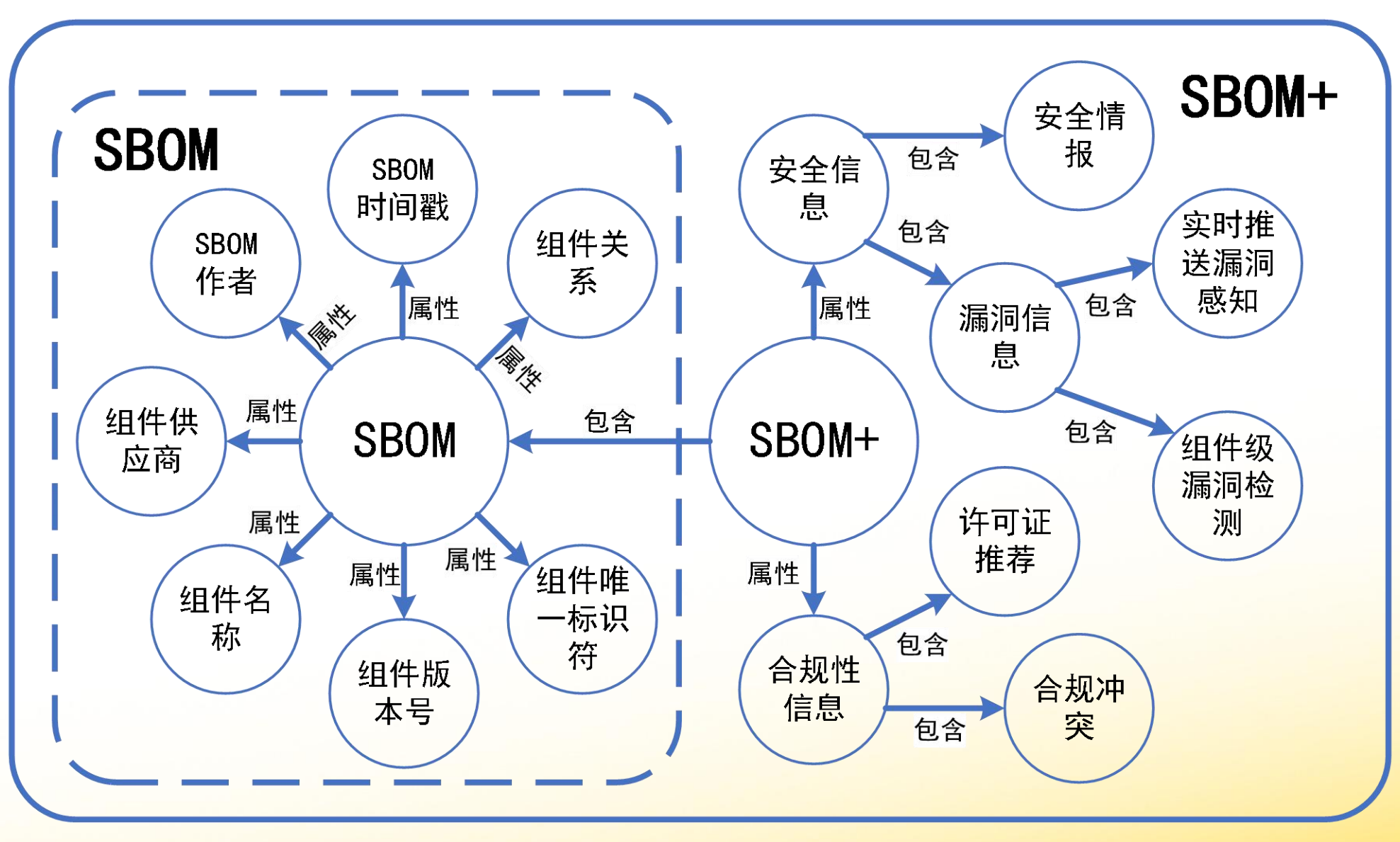
二进制级SBOM生成技术



借助 SBOM 进行漏洞检测



借助 SBOM 进行合规性分析



SBOM+与 SBOM 的对比

This paper is supported by

Open Source Map