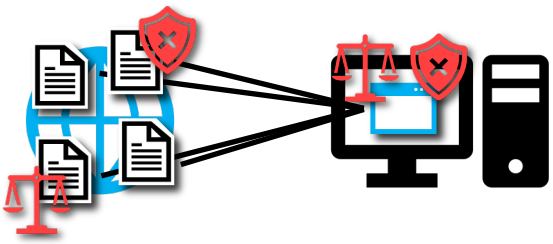
C/C++ のシステムに対する SBOM 生成手法の検討

音田涉[1] 神田哲也[2] 眞鍋雄貴[3] 井上克郎[4] 仇実[5] 肥後芳樹[1]
1 大阪大学 2 ノートルダム清心女子大学 3 福知山公立大学 4 南山大学 5 株式会社東芝

背景： サプライチェーンリスク

現在のソフトウェア開発では多くの外部ライブラリを活用する [1]

- **サイバーセキュリティリスク（サプライチェーン攻撃）**
  例） XZ Utils を経由した SSH バックドアの埋め込み（2024）[2]
- **著作権リスク（ライセンス違反）**



[1] Synopsys, "2024 Open Source Security and Risk Analysis Report," 2024
[2] L. Collin, "XZ Utils backdoor," 2024

普及にあたっての課題： ツール不足 [3]

npm, pip などパッケージマネージャからの SBOM 生成は既に可能

C/C++ を対象に SBOM を生成する技術は未確立

- GitHub 上で共に Top 10 に入る言語 [4]
- 他言語でも C/C++ 部品に依存するものが多い
  例） Python の数値計算ライブラリ NumPy

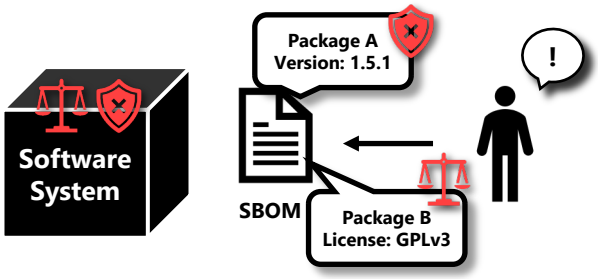
[3] 音田涉, 神田哲也, 眞鍋雄貴, 井上克郎, 肥後芳樹, 「Stack Overflow における SBOM 利活用に関する質問の分析」, 2024
[4] GitHub Staff, "Octoverse: AI leads Python to top language as the number of global developers surges," 2024

Software Bill of Materials (SBOM)

ソフトウェア部品の機械可読な表
米国大統領令 (2021) と **EU Cyber Resilience Act** (2024) で必須化

ソフトウェアに含まれる部品情報を容易に得られる

- **脆弱性・ライセンスなどの問題を迅速に把握・対応できる**



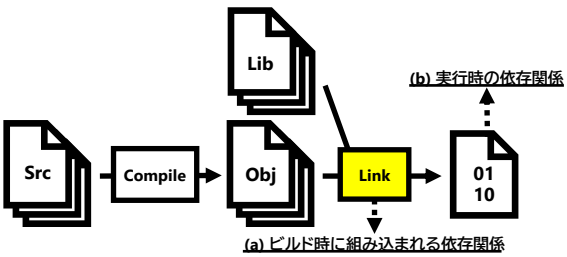
手法概要

C/C++ を用いた開発では一般にパッケージマネージャを使わない

- **リンク処理とバイナリから依存情報を取得する**

リンク

ライブラリとプログラムが使うシンボルを照合する段階
動的ライブラリについては依存情報をバイナリに埋め込む



Link →

(a) ビルド時に組み込まれる依存関係の抽出

リンク処理の内部情報を出力させてライブラリ参照部分を解析
静的リンクと動的リンクを取得可能
（動的リンクは必ずしも実行環境のバージョンと一致しない）

```
attempt to open /usr/lib/gcc/x86_64-linux-gnu/13/../../../x86_64-linux-gnu/libcrypto.so succeeded
```

01
10 →

(b) 実行時の依存関係の抽出

実行ファイルのヘッダから実行時に読み込むライブラリを特定
動的リンクのみ抽出可能
（該当環境で実際に使われるバージョンを得られる）

```
libcrypto.so.3 => /lib/x86_64-linux-gnu/libcrypto.so.3 (0x00007f411a280000)
```

Lib 依存するライブラリファイル群

メタデータの抽出

脆弱性管理への活用にはライブラリ名とバージョンが必須
1. OS 側のパッケージマネージャを探索
2. なければファイルパスを解析して推定

SBOM

実験

環境： **Ubuntu 24.04**
ソフトウェア： **curl 8.10.1**
ビルド手順：

```
$ ./configure --with-openssl LDFLAGS=-Wl,--verbose
$ make
```

```
'/usr/lib/x86_64-linux-gnu/libcrypto.so.3': "Package: libssl3t64¥nVersion: 3.0.13-0ubuntu3.4¥nPriority: required¥nSection: libs¥nSource: openssl¥nOrigin: Ubuntu¥nMaintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>¥nOriginal-Maintainer: Debian OpenSSL Team <pkg-openssl-devel@alioth-lists.debian.net>¥nBugs: https://bugs.launchpad.net/ubuntu/+filebug¥nInstalled-Size: 6,767 kB¥nProvides: libssl3 (= 3.0.13-0ubuntu3.4)¥nDepends: libc6 (>= 2.38)¥nBreaks: libssl3 (<< 3.0.13-0ubuntu3.4)¥nReplaces: libssl3¥nHomepage: https://www.openssl.org/¥nTask: cloud-minimal, minimal, server-minimal¥nDownload-Size: 1,940 kB¥nAPT-Manual-Installed: no¥nAPT-Sources: http://ftp.jaist.ac.jp/pub/Linux/ubuntu noble-updates/main amd64 Packages¥nDescription: Secure Sockets Layer toolkit - shared libraries¥n This package is part of the OpenSSL project's implementation of the SSL¥n and TLS cryptographic protocols for secure communication over the¥n Internet.¥n .¥n It provides the libssl and libcrypto shared libraries.¥n¥n"
```

ビルド時，実行時ともに依存関係を取得できた

今後の課題： より多くのメタデータを得る方法，出力方法の検討と，ツールの実装

本研究は，JSPS 科研費（JP24K14895, JP21K02862, JP23K28065, JP24H00692, JP21K18302, JP21H04877, JP23K24823, JP22K11985），2024 年度南山大学パッヘ研究奨励金 I-A-2 の助成を得て行われたものです．