AlmaLinux SBOM Examples

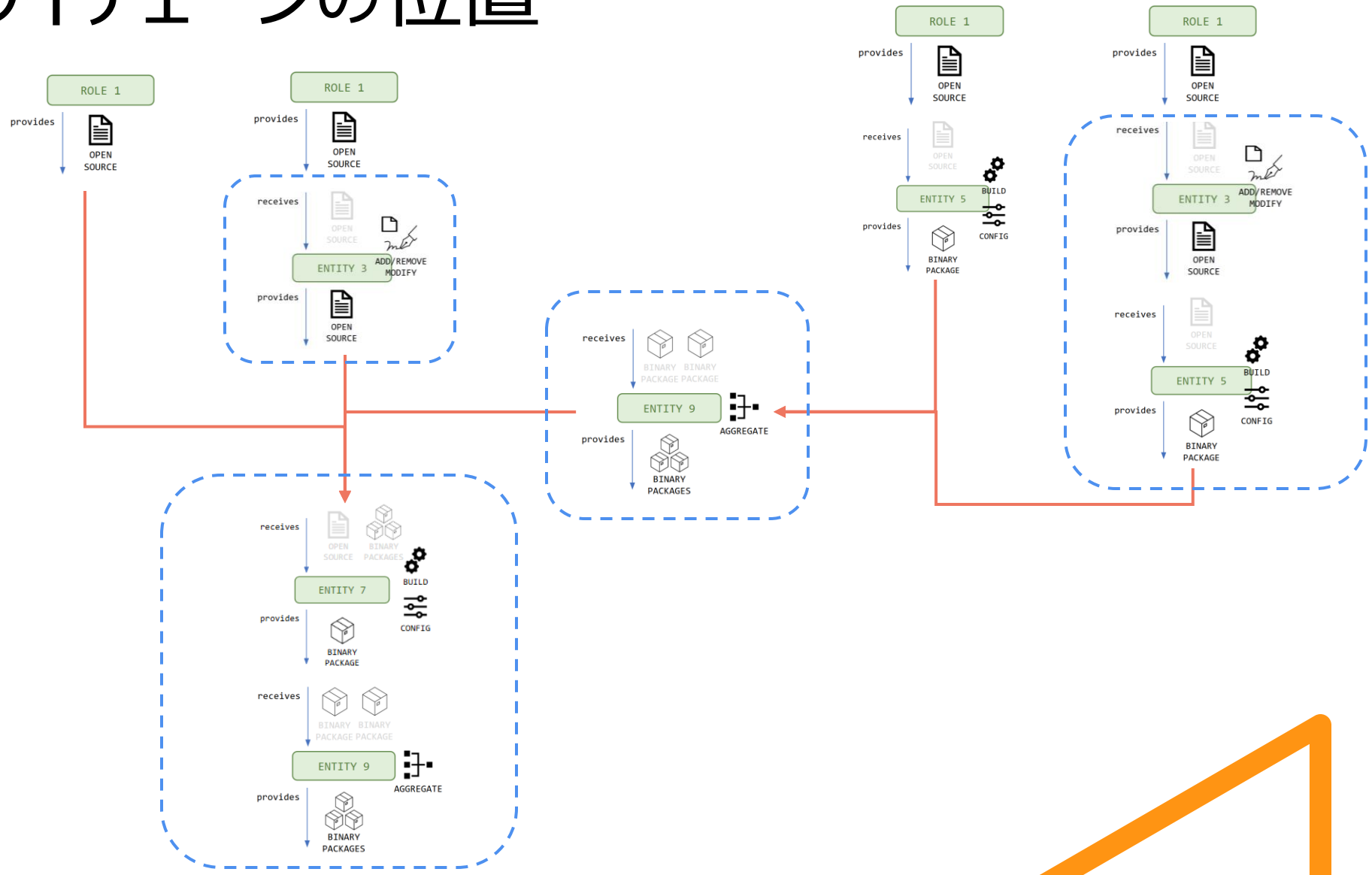
Yumi Tomita

目次

AlmaLinuxのSBOMについて

- サプライチェーンの位置
- alma-sbomツール
- SBOMに含まれる主な情報
- 課題

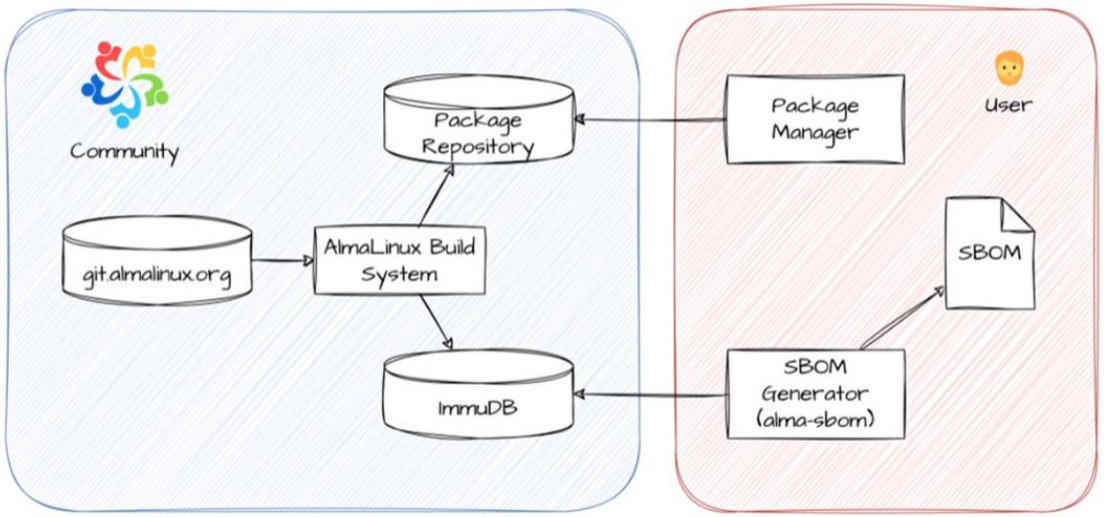
サプライチェーンの位置



alma-sbom ツール

ビルドシステムの情報を参照してSBOMを生成するツール

- ツールの目的
  - ビルドプロセスの追跡
  - データ破損の検証
  - ソースの信頼性の検証
- ツールの利用者：AlmaLinuxのユーザー
- SBOM生成のタイミング：必要に応じて
  - ビルドタスクのSBOM：ビルドIDを指定して生成
  - 単一パッケージのSBOM：パッケージを指定して生成



https://www.cybertrust.co.jp/blog/linux-learning/almalinux_sbom.html

alma-sbom ツール：SBOMに含まれる主な情報

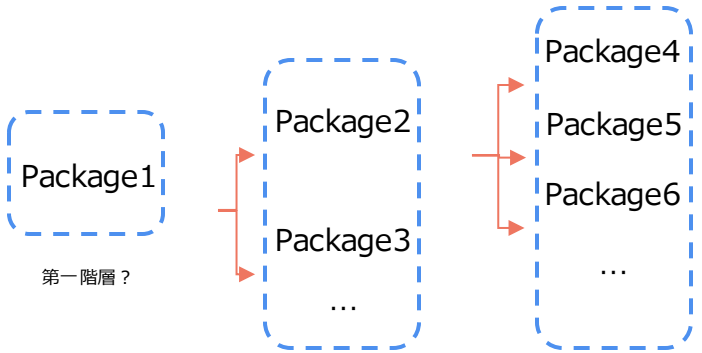
■creationInfo
- created(生成日)
- creators
  - Organization
  - Tool

■packages
- builtDate
- checksums
- externalRefs
  - CPE
  - PURL
- Supplier
- versionInfo

■packages
- annotations
  - release ver
  - sourcerpm
  - buildhost
  - timestamp
  - targetArch
  - packageType
  - immudbHash
  - Build ID
  - Build URL
  - Build author
  - Build source
  - Build source gitcommit

課題

- ✓ 対応フォーマット
  - ✓ CycloneDX V1.4
  - ✓ SPDX V2.3
- ✓ 脆弱性情報とのマッチング
  - ✓ CPEとPURL
  - ✓ OSVが利用可能
- ✓ パッケージの依存関係をどこまで表現するか



参照

- AlmaLinux
  - Linuxディストリビューション
- alma-sbom
  - SBOM生成ツール
- AlmaLinux における SBOM の実装について
  - サイバートラストによる解説ブログ