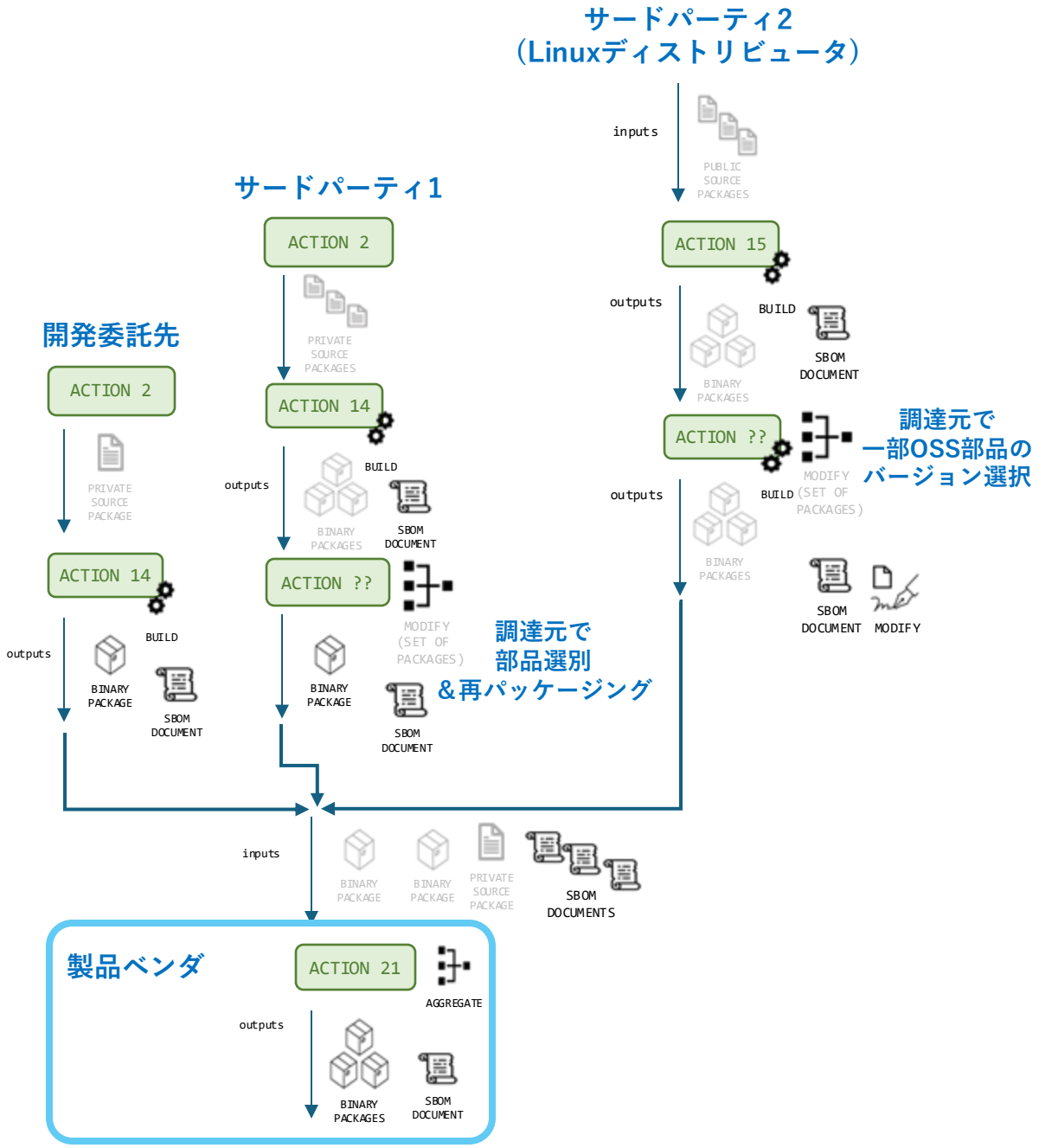
とあるアプライアンス製品の開発の流れとSBOM作成



SBOM REQUIREMENTS

PURPOSE: Vulnerability Management
FORMAT: SPDX v2.2
COMPONENT INFO:
- NAME
- ID
- VERSION
- FILE NAME（製品ベンダ,委託開発先に推奨）
- SUPPLIER
- OTHER UNIQUE ID (CPE and/or PURL) if any
- RELATIONSHIP
- and other necessary data fields for SPDX compliance

課題

- 製品ベンダや開発委託先のSBOMとサードパーティのSBOMでパッケージの単位が異なり、正確な依存関係を書けない場合がある
  →サードパーティのSBOMをインポートしたツールが賢く紐付けてくれたりはしない模様
- サードパーティのSBOMには、項目は揃っていても目的（脆弱性管理やライセンス管理）に必要な値が入っていない場合がある
  →サードパーティは特定のツールで生成したSBOMをそのまま提供している場合が多く、コントロールしにくいか
  - パッケージに含まれるライセンス情報がSPDX License Identifierに合致しない場合がある（情報不足など）
    →委託契約などで依頼可能な場合は合わせてもらう
- 「Know Unkown」（何について書かれていないか）が不明
  →使用プログラム言語, パッケージマネージャ, SBOMツールを共有

これはSBOMに記載