最近耳にするSBOMとは

JPCERTコーディネーションセンター
早期警戒グループ Global CVD Project Lead
伊藤 智貴

SBOM

SBOM/Software Component Transparency

- **S**oftware **B**ill **o**f **M**aterials
  - ソフトウェアコンポーネント部品表
  - ソフトウェア（サプライチェーン）の**透明化**を図る
  - 製品開発者やサプライヤによる SBOM の作成、アセットマネージメントとの共有などによって、**脆弱性対応**のほか**ライセンス管理**、**調達**など**さまざまな場面**における効果が期待される

問題意識

- ソフトウェア製品・アプリケーションでは、**オープンソースやサードパーティ製コンポーネント**が**広く使用されている**
- 脆弱性が発見・公開される →
  「**自身は影響を受ける（可能性がある）のか**」
  「**誰が影響を受ける（可能性がある）のか**」特定が必要
  - 自社製品の使用しているコンポーネント（ベンダー）
  - 手持ち資産に含まれているコンポーネント（アセットオーナー）

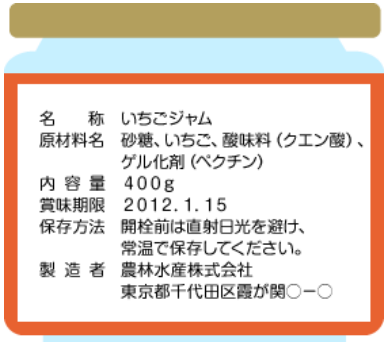
  …が不明であると、**そもそも適切な対応ができない**

“If you don’t know what you have, you can’t protect anything”

シンプルに言えば..

- よく言われる例え：*食品の原材料リスト*
- ソフトウェアコンポーネントリストを準備・共有し
  - 何がどこにあるか透明化
  - 問題特定・解決のスピード、正確さの向上
  - 自動化

…に繋げることが目的



出典：農林水産省「食品表示について」
https://www.maff.go.jp/j/syokuiku/kodomo_navi/featured/abc1.html

JPCERT/CC として SBOM に期待していること（CVD）

- 脆弱性調整（Coordinated Vulnerability Disclosure, CVD）
- 複数の製品開発者・関係者が参加する CVD
  = Multi Party Coordinated Disclosure（MPCVD）
- 脆弱性情報届け出 →
  影響のある可能性がある複数ベンダー特定 → 通知 →
  ベンダーによる脆弱性影響確認・対応 →
  アドバイザリ公表

JPCERT/CC として SBOM に期待していること（CVD）

- 脆弱性調整（Coordinated Vulnerability Disclosure, CVD）
- 複数の製品開発者・関係者が参加する CVD
  = Multi Party Coordinated Disclosure（MPCVD）
- 脆弱性情報届け出 →
  影響のある可能性がある複数ベンダー特定 → 通知 →
  ベンダーによる脆弱性影響確認・対応 →
  アドバイザリ公表

透明化によるこれらの正確さ、スピードの向上、コスト削減に大きな期待

これまでの経緯を簡単に

Simple timeline（2018）

- CERT Vendor Meeting で SBOM アイディアが米 NTIA Allan Friedman 博士より発表される
- NTIA 主催の Multi stakeholder meeting 開始
  - 異なる関係者が集まり、合意を取りながら議論が進められる
  - 四半期ごとのミーティング、各WGによる発表
- WG
  - Framing（概念等定義）
  - Tooling（ツール関係）
  - Healthcare PoC（医療系の実証実験）
    （後に啓発、普及の Awareness & Adoption も開始）

Simple timeline（2021）

- 5月12日 Executive Order on Improving the Nation’s Cybersecurity が発令
  - 米国大統領令に SBOM に関する requirement が入る
  - 米国政府にソフトウェア製品を売りたい場合は SBOM をつけることが必要となる
- 7月12日 SBOM Minimum Elements が策定・公開される

最後に

- SBOM の議論はまだ続いている
- “SBOM” という言葉の一人歩き（「新しい規格？」「“正解” のやりかたは？」…etc.）も見受けられる

SBOM についての細かいあれこれというより
Software Transparency で解決しようとしている問題についての議論や理解が重要。各立場における、透明化によるメリットを考えてもらえると良い

参考情報

- Software Bill of Materials | CISA
https://www.cisa.gov/sbom
- SOFTWARE BILL OF MATERIALS | National Telecommunications and Information Administration
https://www.ntia.gov/SBOM
- The Minimum Elements For a Software Bill of Materials（SBOM）
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
- Roles and Benefits for SBOM Across the Supply Chain
https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf
- SBOM at a Glance（日本語）
https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_ja.pdf
- Vulnerability Exploitability eXchange（VEX）– Use Cases
https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Aprill2022.pdf
- Vulnerability Exploitability eXchange（VEX）– Status Justifications
https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf

Contact

JPCERT/CC 早期警戒グループ（脆弱性調整）

— **Email：vuls@jpcert.or.jp**

伊藤 智貴

— **Email：tomotaka.itou@jpcert.or.jp**

ご清聴ありがとうございました