令和２年度サイバー・フィジカル・セキュリティ対策促進事業
（ソフトウェアを安全に利活用するための
基盤構築に向けた調査）

調査報告書

2021 年 3 月

株式会社エヌ・ティ・ティ・データ経営研究所

目次

1. 今回の調査について

1.1. 背景および目的

産業活動のサービス化に伴い、産業に占めるソフトウェアの重要性は高まる傾向にある。特に、近年は、産業機械や自動車などの制御にもソフトウェアの導入が進んでおり、IoT 機器・サービスや 5G 技術においても、汎用的な機器でハードウェア・システムを構築した上で、ソフトウェアにより多様な機能を持たせることで、様々な付加価値を創出していくことが期待される。

また、ソースコードが一般に公開され、商用及び非商用の目的を問わずソースコードの利用・修正・再頒布が可能なソフトウェアであるオープンソースソフトウェア（以下、「OSS」という。）については、汎用ライブラリや DBMS 等を中心に、近年、企業の商用製品・サービスにも積極的に採用されており、今や OSS を用いずに製品・サービスを構築することはほぼ不可能な状況である。

ソフトウェアを利活用した製品・サービスの安全・安心を担保するには、利活用するソフトウェアの脆弱性の管理が求められる。セキュリティ・バイ・デザインの考え方に基づいて、企画・設計段階で脆弱性を含めないようソフトウェアが構成されていたとしても、リリース後に脆弱性が発見される事が多く、その場合、ソフトウェアを利活用する側でのソフトウェア更新等の対応が求められる。また、自社の製品・サービスで利活用しているソフトウェアの保守・サポートが終了する場合には、それ以降に発見された脆弱性の管理について代替ソフトウェアへの変更を含めた検討が求められる。OSS の活用が増える中でソフトウェアの構成は複雑化する一方であり、今後、そのような脆弱性の管理を事業者単独で実施することは費用対効果の面からも困難である。

このような課題について、産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）にて取りまとめた「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「CPSF」という。）では、セキュリティの確保のために、機器の正規品確認を目的としたソフトウェア真正性の確認や、脆弱性の確認について言及しているが、ソフトウェアの複雑化、OSS の利用拡大などに伴い、ソフトウェアのセキュリティをどのように維持し続けるのか、それをどのように確認するかの具体的な方法までは明確化していない。海外では、米国商務省の電気通信情報局（NTIA[1]）において、平成 30 年 7 月から Software Component Transparency という官民合同の検討体制を構築し、ソフトウェアの脆弱性の管理手法の在り方についてユースケースを交えた検討を実施している。

そのような状況等を踏まえ、経済産業省では、CPSF に基づく具体的なソフトウェアのセキュリティ対策手法等の検討を行うため、「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」（以下、「ソフトウェアタスクフォース」という。）を令和元年 9 月に設置し、民間企業・団体等が抱えているソフトウェアの管理手法に関する課題、脆弱性対応や、OSS の利活用に関する課題等について議論を行

[1] The National Telecommunications and Information Administration

っている。

本調査は、IoT 機器の更なる普及や今後の 5G 時代を見据え、ソフトウェアを安全に利活用するための脆弱性の管理の在り方や、安全な OSS の選定及び活用するための枠組みを検討するために、OSS の利活用に起因するセキュリティリスクを洗い出すとともに、国内外におけるソフトウェアの脆弱性の管理の取り組み動向や、OSS を含むソフトウェアを企業等で自社製品・サービスとして活用する際のセキュリティリスクに対応するための取り組みについて調査を行い、多角的な観点から OSS を含むソフトウェアを安全に利活用できる基盤の構築に向けた検討の基礎資料を作成し、我が国のサイバーセキュリティ政策立案に資することを目的とする。

1.2. エグゼクティブサマリ

本調査では、2018 年から NTIA が行っている Software Component Transparency に関する官民合同の検討状況および関係者の意見等について整理するとともに、わが国国内における議論や取り組み状況に関する情報を収集・整理し、さらにこれらを踏まえて、国内有識者に対するソフトウェアの利活用及びその管理に関する意見交換を行った。

NTIA が行っている Software Component Transparency に関する官民合同の検討については、2020 年 4 月から 2020 年 3 月までに 4 回の会合が開催された。

本会合では、4 つのテーマに関する WG（" Framing WG"," Formats and Tooling WG"," Awareness and Adoption WG"," Healthcare Proof of Concept WG"）が設置され、それぞれの課題が検討されて、SBOM(Software Bill of Materials(ソフトウェア部品表))の活用に関する実証、既存の標準の活用のあり方等に関する議論が進んできた。当初は 2019 年内で活動が終了する予定であったが、引き続き 2021 年以降も活動が継続されている。

わが国国内における議論や取り組み状況についてみると、民間事業者のレポートでは、様々な業種において OSS の利用割合が高まっているとされている。わが国の企業における取り組みをみると全体的には、各社とも OSS に対するライセンスや脆弱性等の対応に向けた管理体制構築を進めている。今回の調査では、先進企業の取り組みを、事例集作成の一環として事業者にヒアリングを実施して調査を行うとともに、国内外の関係団体等の動向についても調査した。

こうした状況を背景に、本調査では、国内関係者の参加によるサイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースや、意見交換のための検討会を実施した。現状のソフトウェア脆弱性に関する課題認識や各企業・組織における取り組み概要、官民での取り組みのあり方等が議論された。

2. NTIA の動向

2.1. NTIA について

2.1.1. 組織概要

NTIA（電気通信情報局）は米国商務省傘下にある Bureau（局）の一つで、情報通信にかかる助言、政策立案機能を担っている。大統領に対して電気通信および情報政策に関する助言を行う行政機関として、ドメイン名、 電波の周波数割り当て、ブロードバンド、 インターネットの利用に関連する政策課題(プライバシー、 サイバーセキュリティ、著作権)等も扱っている[2]。ソフトウェアの透明性に関するステークホルダ会合を担当するのは同局の政策分析部門である。

2.1.2. NTIA 内の担当部門

NTIA の中の政策分析部門である、インターネット、プライバシー等を所管している Office of Policy Analysis and Development（OPAD)がソフトウェア脆弱性に関する取り組みを所管している。活動内容としては調査業務とともに連邦通信委員会（FCC）への助言、コメントも行っている。

[2] https://www.nic.ad.jp/ja/basics/terms/ntia.html

2.2. Software Component Transparency に関する動き

2.2.1. 全体方針

Software Component Transparency は、ソフトウェアベンダ、通信プロバイダ、ヘルスケア、金融、自動車、IoT 製造業者、医療機器製造業者、金融業界、ヘルスケア等、幅広い参加を歓迎して活動が進められている。また、教育機関、脆弱性管理のソリューションプロバイダ、情報セキュリティの専門家、市民からの意見も募集している[3]。

NTIA はグループの議長としての役割を果たすが、参加するステークホルダが成果を推進するため、サブグループは各自で作業範囲を決めて整理する方法を決定する。今回の取り組みの成功の可否は、ソフトウェアコンポーネントの透明性に関するより広範な調査結果が、社会全体でどの程度実装されるかによって評価されるとされる[4]。

NTIA は、セクター固有の解決策が散発的に行われることを防ぐため、幅広いセクター間の参加を奨励している。注目を浴びているのは、業界等様々な分野での SBOM の適用可能性に関する議論である[5]。ただし、今回の参加者で規格を開発するわけではなく、継続中の規格への取り組みや議論に取って代わるものではないとしている点に注意が必要である。

2.2.2. 代表的な参加者

オープンな形で、現地会場に加えて、オンラインで外部からも参加できる。その中でも活発な参加を行っている企業等について紹介する（以下は順不同）。

(1) セキュリティ機関

CERT/CC[6]、 Nova Leah、NYU サイバーセキュリティセンター

(2) OSS

Linux Foundation

---

[3] https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency

[4] https://www.ntia.doc.gov/files/ntia/publications/fr-notice-07192018-meeting-software-component-transparency.pdf

[5] 同上

[6] CERT Coordination Center

(3)　セキュリティ事業者

McAfee、s-Fractal Consulting LLC、Turnaround Security、CA Veracode、Cyber Services Eventable

(4)　その他 IT 事業者

Microsoft、Siemens、Oracle、PTC、CISCO

(5)　医療・ヘルスケア

New York Presbyterian、Ion Channel

(6)　行政

NTIA、国立標準技術研究所（National Institute of Standards and Technology （NIST））

(7)　その他

Consumer Technology Association（米国の 2000 以上の家電関係の企業が加盟するエレクトロニクス技術についての業界団体）、SAFECode

2.3. 各会合の運営概要

NTIA は、オープンで透明性のあるプロセスを通じて、ソフトウェアコンポーネントデータを共有し、簡単かつ自発的に採用できる方法、幅広いコミュニティが取り組むべきポリシーの策定および市場の課題の特定に取り組んでいる。また、IoT サイバーセキュリティのベストプラクティスに関する NTIA のステークホルダによる以前の作業成果も活用されており、政府および業界のステークホルダの連携による実践に向けた NTIA の最初のステップとしての位置づけにもなっている[7]。以下は 2020 年度に開催された会合に関する情報である。

[7] https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency

2.3.1. 2020 年 4 月会合

(1) サマリ

2020 年 4 月 15 日に開催された。

- 各ワーキンググループはコンポーネントのネーミング/特定という課題に取り組んでおり、参加者の一部は標準的/ユニバーサルなネーミングがソフトウェアコンポーネントに対して存在しないという点に対して大きな懸念を示している。
- SBOM 共有のためのソリューションは、デバイスが SBOM をネットワーク経由で自動的に送信できる Manufacturer Usage Description（MUD）のような高度なものから、ウェブサイトからの手動取得といった手段まで様々ある。エンドユーザーによる SBOM 取得を可能とするその他の手段としては、OpenC2、Linux Foundation の OpenChain 等がある。
- Formats and Tooling ワーキンググループ は、様々なツールとその機能の分類・タクソノミ作成の課題の仕上げを行っており、現在 SWID、SPDX、CylconeDX のみに集中している。同 WG はソフトウェアのビルド段階において SBOM を自動的に生成するツールを支持している。
- Awareness and Adoption ワーキンググループ は、SBOM に関する全体を示す 2 ページの資料と、各業界向けのグラフィック及びマルチメディア、バーチャル・エンゲージメントの機会を提供している。
- ヘルスケア PoC の第二弾（Healthcare Proof-of-Concept (PoC) Version 2）では、ユースケースの拡大、参加者の拡大、ツール及びオートメーションの検討を盛り込む、という目標が定義されている。医療機関（health delivery organzations：HDO）として、Sutter Health、Cedars-Sinai、Christiana Care、the Mayo Clinic、New York Presbyterian が参加し、医療機器メーカー（medical device manufacturers：MDM）としては Abbot、Medtronic、Philips、Siemens、Thermo-Fisher Scientific が参加する。
- 米国食品医薬品局（FDA）の代表は Phase 1 SBOM ドキュメントに高い満足度を示しており、FDA はこれらのドキュメントの記述に沿って SBOM を市販前ガイダンスに取り込む意向を確認した。以降のプレスリリースで発表となる可能性がある。

(2) WG 別報告

2020 年 4 月 15 日、米国商務省電気通信情報局（National Telecommunications and Information Administration：NTIA）ソフトウェアコンポーネントの透明性に関する会合が行われ、Phase 1 文書の完成に向けてワーキンググループの次のステップが議論された。具体的な議題は以下のとおり。

1) Framing Working Group

各ワーキンググループはコンポーネントのネーミング/特定という課題に取り組んでおり、参加者の一部は標準的/ユニバーサルなネーミングがソフトウェアコンポーネントに対して存在しないという点に対して大きな懸念を示している。一方、より小分けにした領域（例えば、医療機器業界）でこの問題を解決すべき、という主張もある。コンポーネントの特定に関するソリューションが不在のまま SBOM の概念がどれだけ有用かを定義する方法、また、可能性のあるソリューションについて議論がなされた[8]。

フレーミング・ワーキンググループは、ネーミング/特定に関するソリューション不在でどの程度まで取り組みが行えるかを評価しており、仮説のテストのためいくつかのユースケースを設定した。また、既存の SBOM 概念についてヘルスケア PoC WG と共にテストを行う。同 WG が提示したユースケースは以下のとおりである。

- サプライヤがあるコンポーネントの SBOM を作成する。
- 誰かが別の人のコンポーネントの SBOM を作成する。
- サプライヤがベースライン要素を決定、ポピュレートする。
- サプライヤが SBOM を配布する。
- コンシューマが SBOM を消費する。

フレーミング WG はまた、サプライヤ情報の集中レポジトリがあれば問題の緩和に役立つが、一部のステークホルダは反対も出るだろうとの慎重な見方を示している。

8 https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_framing_april152020.pdf

- SBOM exchange and sharing is still important
  - Tightly connected with identification
  - Part of PoC-Framing collaboration
- MUDMaker
  - MUD Manufacturer Usage Description, RFC 8520 https://www.rfc-editor.org/info/rfc8520
  - "...provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function."
  - https://www.mudmaker.org/
  - Thanks Eliot L.
- Other (existing) options, maybe STIX?

SBOM エクスチェンジ

- ♦ SBOM 交換・共有は依然として
  - ♦ 特定と密接に関係
  - ♦ PoC-フレーミングコラボレーションの一部
- ♦ MUDMaker
  - ♦ MUD (Manufacturer Usage Description), RFC 8520 https://www.rfc-editor.org/info/rfc8520
  - ♦ "…エンドデバイスからネットワークに、正常に機能するにはどの種のアクセスとネットワーク機能が必要かを通知する手段を提供する"
  - ♦ https://www.mudmaker.org/
  - ♦ Eliot L.への謝辞
- ♦ その他の（既存）オプション、STIX？

図 1　SBOM Exchange について

質問・課題と次のステップ

- 次の質問について議論・回答
  - 特定の問題は SBOM の進展をどの程度阻害するか
    - 部分的に進展するとどのようになるか？
    - 特定のどの側面が阻害要因になっているか？
    - サプライヤ・レジストリは必要か？実行可能（feasible）か？
    - 特定に対する重要/包括的なソリューションなしでどのくらいのスピード/規模で SBOM を拡大できるか？
- 次のステップ
  - 特定・交換に関しマルチスレッドを継続
  - 一時的な脆弱性/悪用可能性指標（VEX）は有用だが保留
    - ジェネリックな SBOM アノテーション機能を検討
  - ヘルスケア PoC コラボレーション

図 2 課題と次のステップについて

表 1 ユースケース（サマリ）：ソフトウェア透明性提供のための SBOM の利用[9]

ユーザ-ゴール ユースケース	前提	ステップ	例／備考
ユースケース 1：サプライヤが Primary Component に対する BOM を作成	• Baseline Elements 及び Primary Components に関してはサプライヤの情報が正しい。 • サプライヤが SBOM で Baseline Elements を提供	1. サプライヤが業界ガイダンスに従い Primary Component に対して Supplier Name を設定 2. サプライヤがベストプラクティスに従い Component Name 及び Version String を設定 3. サプライヤが Primary Component により使用される first-level Components を特定 4. サプライヤが含まれる Component それぞれに対し SBOM を取得 5. サプライヤが業界推奨フォーマットに従い SBOM を作成 a. サプライヤはこの情報をライフサイクルプロセスにわたり保持 b. サプライヤはできる限り多くの Baseline Elements 及び有用または必要と思われる追加情報を含める c. サプライヤがコンポーネントの SBOM を利用して含まれるコンポーネントの Baseline Elements を取得	ACME 社が ACME 輸液ポンプを作成、（少なくとも）first level components（ボブのブラウザ、等）を含む SBOM を作成する。この SBOM は Primary Component である ACME 輸液ポンプを明確に特定する。 サプライヤのレジストリを利用して Supplier Name を特定してもよい。 ツール、スペック等を利用して Components を特定してもよい。

[9] https://www.ntia.doc.gov/files/ntia/publications/ntia_naming_use_cases_-_framing_2020-04-11.pdf

ユーザ-ゴール ユースケース	前提	ステップ	例／備考
		（ユースケース 3 を参照)	
ユースケース 2：SBOM ステークホルダが SBOM を作成	• コンポーネントのサプライヤは SBOM を作成していない • SBOM ステークホルダは作者（Author） • SBOM ステークホルダがベストエフォートでベースライン情報を作成 • SBOM ステークホルダは SBOM コンポーネントネーミングのベストプラクティスに従う • SBOM のコンテンツに従い SBOM コンシューマは SBOM がコンポーネントのサプライヤにより作成されたものではないことを判断できる	1. SBOM ステークホルダはネーミングのベストプラクティスに従う 2. SBOM ステークホルダはベストエフォートでコンポーネントを特定する 3. SBOM ステークホルダはできる限り多くの Baseline Elements 及び有用または必要と思われる追加情報を含める 4. SBOM ステークホルダは業界推奨フォーマットで SBOM を作成する 5. SBOM ステークホルダは自身を作者（Author）としてリストし、SBOM 情報がサプライヤからのものでないことを明確にする。	Mustard Hospital が 10 年前に購入した ACME 輸液ポンプを発見、SBOM が ACME にも存在しないので Mustard がツールまたはサードパーティを利用して自社用に SBOM を作成。 もし(1) サプライヤが直接含まれていないコンポーネントの未対応の脆弱性について通知を行いたい、または (2) サプライヤが直接含まれていないコンポーネントの脆弱性の悪用不可能性（non-exploitability）は、“ベストエフォート”で含めた SBOM を作成し、どのコンポーネントがリファレンスされているかを明確にすべきかもしれない。特にプロダクトにおいて含まれるコンポーネントの複数のインスタンスが存在するが全てにパッチが適用されていな

ユーザ-ゴール ユースケース	前提	ステップ	例／備考
			い場合に重要である。 作者（Author）はツールまたはその他の手段を用いてコンポーネントを特定してもよい。
ユースケース 3：SBOM に含まれているコンポーネントにサプライヤが Baseline Element を含める	• SBOM は含まれるコンポーネントのサプライヤから入手すべきである • SBOM から の Baseline Elements を利用して含まれるコンポーネントを特定すべきである • コンポーネントの SBOM が入手不可能な場合は、ベストエフォートで Baseline Elements を設定すべきである（ユースケース 2 を参照） • サプライヤは任意で Component Hash を含めてもよい • サプライヤがコンポーネントのインスタンスを作成する場合、サプライヤはハッシュを生成（例えば OpenSSL v1.1.1 のビルド）すべきである • それ以外の場合、	1. サプライヤが Primary Component にコンポーネントを含める。 2. サプライヤがコンポーネントの SBOM を入手する 3. サプライヤが含まれるコンポーネントの Baseline Elements を入手したコンポーネント SBOM から取得 4. サプライヤがコンポーネントを Primary Component の SBOM に追加し、Baseline Elements を利用して SBOM 内のコンポーネントを特定する	ACMEがDOORSのオペレーティングシステムを新しい輸液システムに含めたいのでDOORS から SBOM を入手する。

ユーザ-ゴール ユースケース	前提	ステップ	例／備考
	SBOM から Component Hash が入手可能であればそれを利用すべきである		
ユースケース 4：サプライヤが SBOM を配布	SBOM は業界のベストプラクティスに従って配布すべきである	サプライヤが設定、通知した手段で情報を SBOM コンシューマに提供	このユースケースは今後さらに展開する。
ユースケース 5： SBOM のコンシューマが SBOM を利用	• SBOM コンシューマがあるコンポーネントの SBOM を取得済み • サプライヤが SBOM に Baseline Elements を含めており、Primary Componentと、含まれるコンポーネントが特定されている	1. SBOM コンシューマが Primary Component の SBOM を入手 2. SBOM コンシューマが SBOM を利用して含まれるコンポーネントを特定 3. SBOM コンシューマが含まれるコンポーネントに対して脆弱性が報告されていることを特定 4. SBOM コンシューマがサプライヤに連絡し脆弱性に関する情報を要求 5. サプライヤが脆弱性の影響（例えば、影響なし）及び SBOM コンシューマがとるべきアクション（例えば、アクションの必要なし、パッチ利用可能）に関する詳細を提供する	Mustard Hospital が ACME から輸液ポンプの SBOM を入手する。新規の脆弱性である KNOCK KNOCK が報告されており、DOORS オペレーティングシステムに関係する。Mustard は ACME の SBOM に DOORS オペレーティングシステムが使用されていることを特定する。 自動車メーカーでソフトウェア障害があり、ソフトウェア更新のためリコールを行う。自動車メーカーはディーラーを通した顧客への通知、パッチ適用の最終責任を負う。

ユーザ-ゴール ユースケース	前提	ステップ	例／備考
			SBOM を利用する SBOM コンシューマは、ソフトウェアライセンスの確認等、複数のアクションをとり得る。以上は一例である。

SBOM 共有のためのソリューションは、デバイスが SBOM をネットワーク経由で自動的に送信できる Manufacturer Usage Description（MUD）のような高度なものから、ウェブサイトからの手動取得といった手段まで様々ある。エンドユーザーによる SBOM 取得を可能とするその他の手段としては、OpenC2、Linux Foundation の OpenChain 等がある。

2) Formats and Tooling WG

Formats and Tooling ワーキンググループ[10] は、様々なツールとその機能の分類・タクソノミ作成の課題の仕上げを行っており、現在 SWID、SPDX、CylconeDX のみに集中している。同 WG はソフトウェアのビルド段階において SBOM を自動的に生成するツールを支持している（よりレベルが低いものはソフトウェア作成後の自動作成や、手動作成となる）。

[10] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_-_formats_tooling_-_2020_q2_checkpoint-2.pdf

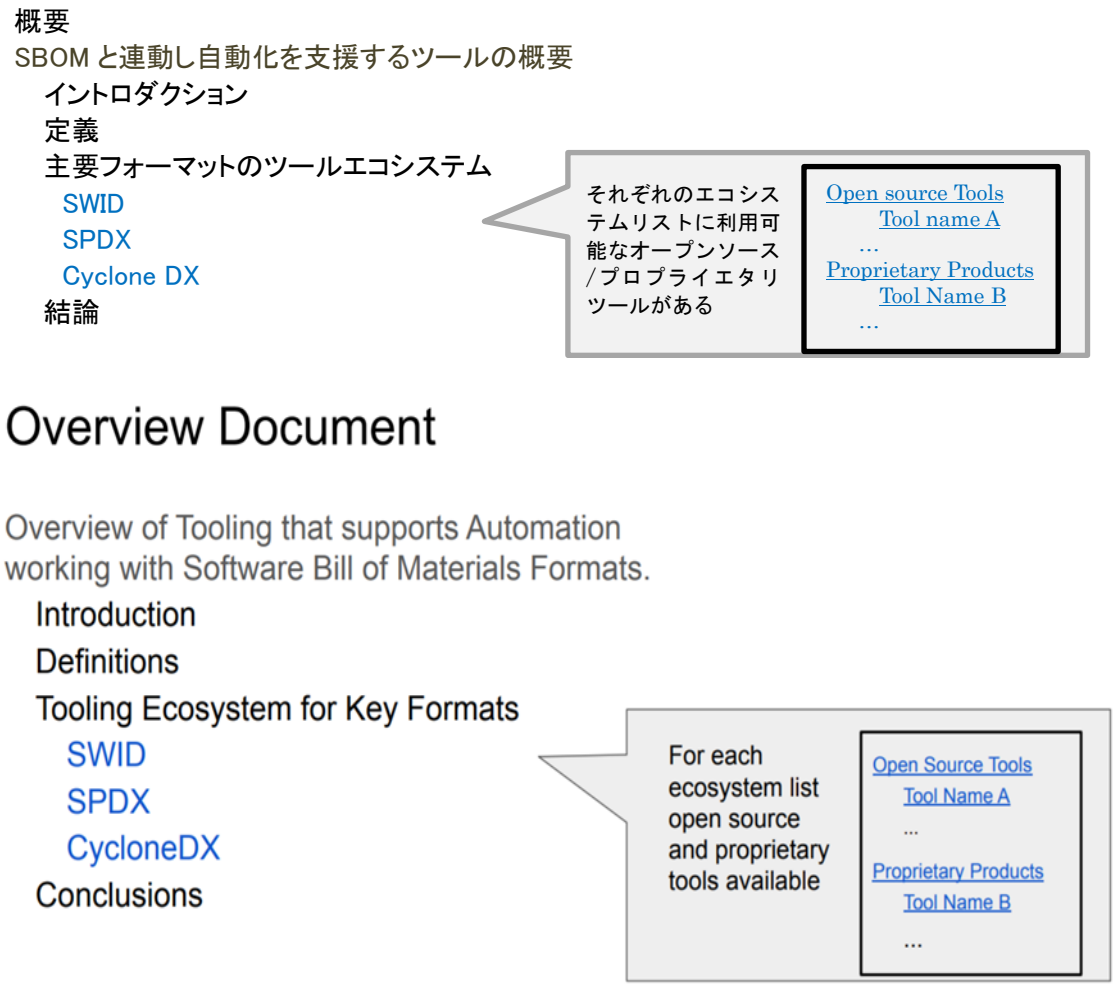


図 3 ツールの概要

表 2 ツール分類に使用するタクソノミのアップデート

カテゴリ	タイプ	説明
Author during build	Build	アーティファクトのビルド中に、ビルドに関する情報を含むドキュメントが自動的に作成される。
Author after Creation	Manual	人が手動で情報を記入する。
	Audit Tool	ソースコード分析または監査ツールがアーティファクトと関連ソース（あれば）を検査し、ドキュメントを生成する。
Consume	View	人間が可読な形式（画像、図形、表、テキスト）でコンテンツを理解できる。意思決定とビジネスプロセスの支援に用いる。

	Diff	ある構造（formation）についての２つドキュメントを比較し、明確に違いを把握することができる。例えば、１つのソフトウェアの２つのバージョンの比較。
	Analyze	ドキュメント情報をインポートできる。
Transform	Translate	同じ情報を維持しながら 1 つのファイルタイプから別のファイルタイプへ変換する。
	Merge	複数ソースのドキュメントを分析・監査のためマージする。
	Tool integration	API、ライブラリによる他ツールでの使用に対応する。

表 3 **ツールにつき収集する情報**

ツールテンプレート

対応	Author during build, Author after Creation, Consume, Transform
機能	
ロケーション	Website: Source:
インストール方法	
使用方法	
対応バージョン	

例：FOSSology

対応	Author after Creation (Audit tool, Manual), Consume (View, Diff, Analyze), Transform (Translate, Merge, Tool Integration)
機能	FOSSologyはオープンソースライセンスのコンプライアンスソフトウェアシステム及びツールキットで、ユーザによるREST API からのライセンス、著作権、エクスポートコントロールスキャンを可能とする。

	システムとして、データベースおよびウェブ UI によりコンプライアンスワークフローが提供される。 コンプライアンス活動の支援のため、ツールキットのマルチライセンススキャナの一部として、著作権・エクスポートスキャナが利用可能である。
ロケーション	Website: https://www.fossology.org/ Source: https://github.com/fossology/
インストール方法	https://www.fossology.org/get-started/
使用方法	https://www.fossology.org/get-started/basic-workflow/
対応バージョン	SPDX 2.1, SPDX 2.2 (WIP)

3) Awareness and Adoption WG

Awareness and Adoption ワーキンググループ[11] は、SBOM に関する全体を示す 2 ページの資料と、各業界向けのグラフィック及びマルチメディア、バーチャル・エンゲージメントの機会を提供している。これには SBOM よくある質問（FAQ）シートも含まれ、SBOM の定義、ユースケース、役割と責任、実行等を含む質問に対応している。また、SBOM が「攻撃者のロードマップ」として使われ得る、等 SBOM に関する一般的な懸念（ソースコードの公開と知的財産、ライセンスコストに関わる懸念）についても触れている。

SBOM FAQ [12]

- 一般

Q：SBOM とは何ですか。

Q：SBOM は誰が何のために使うのですか。

Q：SBOM は誰が入手すべきですか。

Q：SBOM は誰が作成しメンテナンスするのですか。

Q：SBOM はソフトウェアサプライヤによりいつ変更またはメンテナンスされるのですか。

[11] https://www.ntia.doc.gov/files/ntia/publications/ntia-sbom_20200415_awareness_presentation.pdf

[12] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_faq_-_april_15_draft.pdf

Q：SBOM データはどのように共有されるのですか。

Q：SBOM はサイバー攻撃の際どのように役に立ちますか。

Q：NTIA の SBOM プロセスについてどこからさらなる情報を得られますか。どのように参加できますか。

- SBOM に関する懸念

Q：SBOM は「攻撃者のロードマップ」にならないのですか。

Q：知的財産またはソースコードの公開ということですか。

Q：SBOM によりライセンスコストまたはライセンス制約が増えますか。

- SBOM 実行に関する詳細

Q：SBOM には何が含まれるべきですか。

Q：一部のソフトウェアコンポーネントは、また別のソフトウェアコンポーネントにより構成されていますが、SBOM はこの階層性を提示できますか。

Q：SBOM は依存性グラフにおいてどれだけ一覧化すべきですか。

4) Healthcare Proof of Concept WG

ヘルスケア PoC（概念実証）の第二弾（Healthcare Proof-of-Concept (PoC) Version 213 ）では、ユースケースの拡大、参加者の拡大、ツール及びオートメーションの検討を盛り込む、という目標が定義されている。医療機関（health delivery organzations：HDO）として、Sutter Health、Cedars-Sinai、Christiana Care、the Mayo Clinic、New York Presbyterian が参加し、医療デバイスメーカー（medical device manufacturers：MDM）としては Abbot、Medtronic、Philips、Siemens、Thermo-Fisher Scientific が参加する。同グループは引き続き creation（内部ツール/プロセスへの統合）、consumption（SBOM 情報のアセット/リスク管理システム及びプロセスへの入力）、SBOM 同士の区別、異なるフォーマット間の変換に参加するツールプロバイダを探している。評価中のユースケースは以下のとおりである。

13 https://www.ntia.doc.gov/files/ntia/publications/healthcare_sbom_proof_of_concept_-_update_2020-04-15.pdf

- 調達：法務、購買、調達、IT、情報セキュリティ、臨床/生医学エンジニアの混成チームにより、SBOM がどのように購買/契約決定に影響するかを判断する。検討されたアクティビティは以下のとおりである。
    - ✧ インターネット及びライフサイクル管理プロセスにおける SBOM の送信
    - ✧ 調達向け約款用語
    - ✧ 脆弱なエンドオブライフサイクル、及び/またはカスタムソフトウェアコンポーネントの特定
    - ✧ 可能性のあるシステムコンフリクトの特定
    - ✧ 脆弱性 vs 悪用可能性（exploitability）の測定
    - ✧ 脆弱なコンポーネントに対する補完的または代替的なコントロール
    - ✧ 評価アーティファクト削減の可能性の評価（例えば、ベンダ質問表の必要性削減）
    - ✧ サポート及びパッチ、インストール可能なアンチマルウェアソフトのタイプ・バージョンについてのライセンス契約
    - ✧ ソフトウェアライフサイクルにおける本質的な問題に基づきプロダクトを比較
    - ✧ MDM の脆弱性改善のロードマップを特定
- アセット管理：アプリケーションコンポーネントの自動または半自動インベントリ化。検討されたアクティビティは以下のとおりである。
    - ✧ コンポーネントのネーミング慣習
    - ✧ アセットの取り込みと管理のワークフロー
    - ✧ 脆弱性情報の照合により進行中のリスク評価（例えば国家脆弱性データベース（National Vulnerability Databace））
    - ✧ 既知の脆弱性を含む SBOM 情報の比較のためのスキャン、テスト
    - ✧ ミティゲーション戦略
    - ✧ プロダクトラインナップにまたがる SBOM 目録の分析
- リスク管理：SBOM を用いたリスク・ミティゲーション手法（手動プロセス、自動エンタープライズ ガバナンス・リスク・コンプライアンス（eGRC）技術）による、時間の経過に伴う新規の脆弱性・リスクの特定、リスク・ミティゲーション手法実装のフィージビリティ。
    - ✧ 脆弱性特定のための共有データベースとデータアナリティクス
    - ✧ 自動リスク分析のための eGRC プロセス及び技術
    - ✧ HDO と MDM の双方を動員したミティゲーション戦略
    - ✧ 利用可能である場合、脆弱性 vs 悪用可能性（VEX）情報を利用したリスク管理アクティビティの支援

- 脆弱性管理：脆弱性特定、スキャンアクティビティのための SBOM のインテグレーションと追加情報による補完。デバイスをオフラインにする必要を避けるためのスキャン設計、自動化、リスク削減のためのネットワークコントロール。
    - ✧ SBOM 及び既存のセキュリティスキャニングツール間のインテグレーションポイント
    - ✧ 脆弱性管理アクティビティの自動化
    - ✧ 修復の難しい脆弱性に対する代替的コントロールの開発
    - ✧ SBOM の異なるソフトウェアレイヤ間での脆弱性ミティゲーションのための再現可能なワークフロー

2.5 FDA アップデート

米国食品医薬品局（Food and Drug Administration：FDA）

米国食品医薬品局（FDA）の代表は Phase 1 SBOM ドキュメントに高い満足度を示しており、FDA はこれらのドキュメントの記述に沿って SBOM を市販前ガイダンスに取り込む意向を確認した。以降のプレスリリースで発表となる可能性がある。

米国国防省（Department of Defense：DoD）

国防省は SBOM の要件を「Comply to Connect（C2C、DoD ネットワーク接続のための認証システム」ユースケースとして、2～3 年以内に取り入れる意向とみられる。

米国国立標準技術研究所（National Institute of Standards and Technology：NIST）の共通プラットフォーム一覧（Common Platform Enumeration：CPE）から SWID（Software Identification SWID）タグへの移行

セキュリティ設定共通化手順（Security Content Automation Protocol：SCAP）のバージョン version 2（v2）では、標準プロトコルを利用したエンドポイントポスチャ情報収集と同情報のネットワーク防御機能への取り込みが自動化される。これは国家脆弱性データベース（National Vulnerability Database：NVD）によりデータ反映に用いられている。NIST は SCAP 2.0 及び NVD を、現在利用されている CPE から SWID に移行することを決定しており、想定ユーザに向け移行のガイダンスのためのドキュメントを現在作成している。これに対し Red Hat からの参加者は、業界にとって困難な意向である点や、SWID のドキュメンテーションが自由に公開されていない点を警告した。

2.3.2. 2020 年 7 月会合

(1) サマリ

2020 年 7 月 9 日に開催された。

- 2019 年 11 月から開始された SBOM のフェーズ 2 エフォートにおいて、各ワーキンググループの連携強化、フレーミング文書のコンセプト検証、他のセクターにおける PoC（Proof of Concept）の拡大、SBOM 導入のためのガイダンス作成といった作業に着手している。
- SBOM のネーミング問題への対応として、Framing WG はコンポーネントのネーミングを検索するメカニズムの設置により、新規ネーミングの作成を極力回避するアプローチを提案している。（2.3 関連）
- ヘルスケア PoC のフェーズ 2 として、医療機関（Health Delivery Organization: HDO）のアセットマネジメントや医療機器の脆弱性管理に直接 SBOM を取り込む手法を検討している。（2.4 関連）
- エネルギーセクターの参加者から、SBOM はセクターごとに異なるファームウェアに対応していないという指摘があった。エネルギーセクターで一般的に使用されているファームウェアの SBOM 作成を試みたところ、困難に直面したという。（2.7 関連）

2020 年 7 月 9 日、米国商務省電気通信情報局（National Telecommunications and Information Administration：NTIA）ソフトウェアコンポーネント透明性に関する会合が行われた。具体的な議題は以下のとおり。

- 開会の辞：Allan Friedman

議長の Allan Friedman 氏より、ソフトウェアの透明性に関する NTIA の活動と今後の方向性について報告があった。2018 年 7 月のキックオフ会合以来、2 年間で多くの成果を生み出している。2019 年秋には、NTIA ソフトウェア透明性に関するフェーズ 1 エフォートの成果として、以下の文書が発表されている。

- フレーミング：共通 SBOM の設置
- サプライチェーンにおけ SBOM の役割と利点
- SBOM のフォーマットとスタンダードに関するサーベイ調査
- ヘルスケア PoC（Proof of Concept）の報告書

2019 年 11 月には NTIA は今後もソフトウェアの透明性確保に関して活動を継続するコミットメントが得られ、グローバル且つ多様なセクターの参加を促している。SBOM が今後対処すべき課題として、Allan Friedman 氏は以下の点を挙げている。

- 用語（Terminology）

- ✧ ガイダンス？ルールブック？ベストプラクティス？CONOP（Concept of Operations）？
- ✧ 他のコンテキストからの事例？

- ガイダンスの目的
  - ✧ 未だビジョンは共有されていないのか？
  - ✧ 既存の SBOM 作業の継続
- 汎用または特化（General vs. Specific）
  - ✧ 漸進的アプローチ（crawl-walk-run）へのコンセンサス？
  - ✧ ハイレベル、しかし明示的なステップが必要
  - ✧ コンテンツを伝えるために必要なビジュアル、グラフィクスが必要
  - ✧ 付属書（annexes）による主要エレメントの補完
- オーディエンスは誰か？
  - ✧ サプライヤ
  - ✧ ユーザー
- ドラフトプロセス
  - ✧ テクニカルおよび組織的な知見（expertise）に基づく
  - ✧ シャッフル（shuffling the decks?）
  - ✧ アウトラインをワーキンググループ（WG）へ
- シナリオ、ユースケース
  - ✧ ソフトウェア作成の一部としての継続的な SBOM 作成
  - ✧ ソフトウェアユーザーの脆弱性
  - ✧ サプライヤの脆弱性

(2) WG 別報告

米国食品医薬品局（Food and Drug Administration: FDA）のサイバーセキュリティアドバイザーを務める Jessica Wilkerson 氏から、FDA における SBOM 利用の最新動向について報告があった。医療機器が持つサイバーセキュリティの脆弱性に対して、FDA はステークホルダとの対話を通して規制のあり方を模索している。新型コロナウイルスのパンデミックにおいては医療機器セクターを支援するため、サイバーセキュリティ確保の取り組みを促進することがより一層重要となっている。

1) Framing Working Group

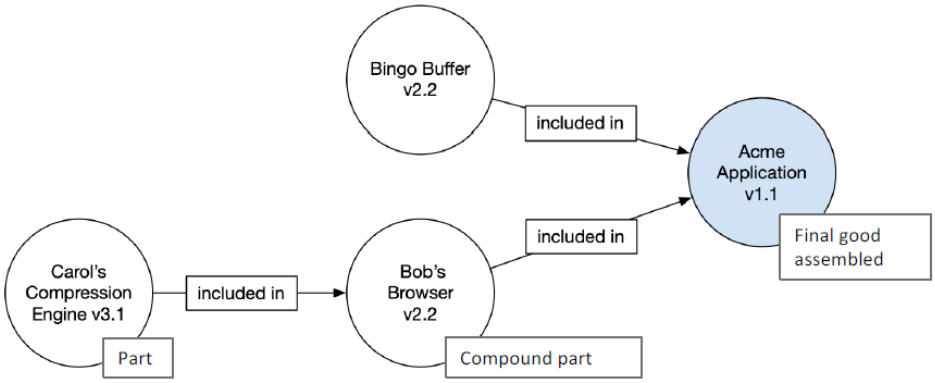
フレーミング WG はヘルスケア PoC と協力してドラフト版 SBOM（upstream SBOMs）の提供およびフレーミング・フェーズ 1 コンセプトの検証を行っている。また、同グループはサプライヤの特定における開発可能性と脆弱性（exploitability vs. vulnerability）のバランスをどのように保つかという課題に取り組んでいる。フレーミング WG は以下の作業に取り組んでおり、今回のステークホルダ会合に合わせてドラフト版文書を公開している。

- ソフトウェア・アイデンティティに関する議論およびガイダンス[14]
- SBOM の共有と交換[15]

フレーミング WG のフェーズ 1 エフォートとして、SBOM の定義、コンポーネント情報のベースライン、コンポーネントの相関についてまとめるとともに、SBOM 作成のプロセスや共有、使用に関して報告書を作成している。SBOM のコンセプトは下記のチャートに図示されており、各コンポーネントの名称、サプライヤ、バージョン、作成者、ハッシュ（Hash）、ユーザー識別子（UID）、相関（Relationship: ソフトウェアそれ自体ないし組み込みコンポーネント）が表示される。

14 https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_framing_sw_identity_july9.pdf

15 https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_framing_sharing_july9.pdf



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

出典：Framing WG プレゼンテーション資料[16]

図 4 SBOM の概念図

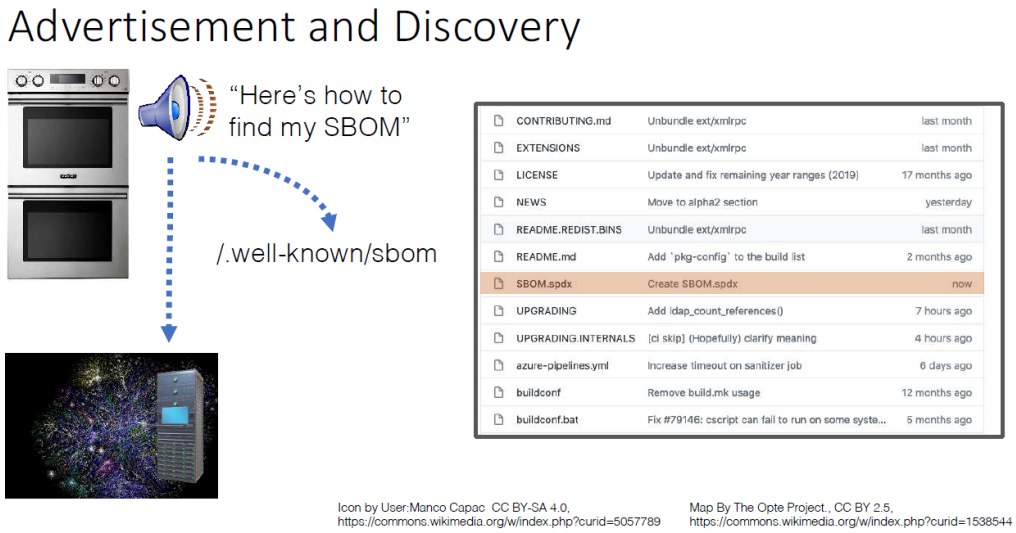
2019 年 11 月から開始されたフェーズ 2 エフォートにおいては、「基礎の先へ（Beyond the basics）」をテーマとしてヘルスケア PoC WG との連携や SBOM の共有に向けたドキュメント作成に取り組んでいる。

ネーミング（naming/identification）問題に対しては、依然として SBOM データと脆弱性データベースを含むその他のデータソースとのマッピングが求められている。フレーミング WG はネーミング問題を最小化し、オリジナルコンポーネントサプライヤ、二次作成者およびユーザーが統一されたネーミング（naming convergence）を共有できる方法を模索している。コンポーネントの特定のために、フレーミング WG は以下の 2 段階アプローチを提案している。

- 既存のサプライヤ・ネームスペースの協調：コンポーネントに既存のネームスペースが存在する場合、サプライヤはこれを使用する。
- 既存ネーミングが存在しない場合、新たにネーミングを行うのは避け、SWID tags、Package URL、Software Heritage IDs といったスタンダードから最適なネーミングを適用する。

[16] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_framing_2020-07-09.pdf

さらに、フレーミング WG は SBOM の共有、フォーマット、メカニズムを含む SBOM の普及（Advertisement and Discovery）に取り組んでいる。ソフトウェア作成者がどこに SBOM を保存するか、エンドユーザーが SBOM をどのように呼び出すか、検索メカニズムをどのように構築するかについて、保存箇所の指定や#SBOM で検索といったメカニズムのあり方が検討されている。以下、SBOM 保存ロケーションのイメージ。



出典：Framing WG プレゼンテーション資料[17]

図 5 SBOM のロケーション

同 WG の今後の作業としては、ネーミング問題への対処の継続、サプライヤ特定の手法、脆弱性と開発可能性のバランス確保が挙げられる。

2) Formats and Tooling WG

Formats and Tooling WG のフェーズ 2 エフォートには既存ツールの一覧作成、ギャップ特定、SBOM 作成から利用までのプロセス特定、異なる SBOM フォーマットの互換性の確保に取り組んでいる。Formats WG の作業にはセクターに共通する SBOM サンプル作成も含まれる。当 WG はまた SboM 作成ツールの機能、ロケーション、使用方法、バージョン情報についてまとめたツール・テンプレートの作成に取り組んでいる。

Formats and Tooling WG は SBOM ツールの分類表（Taxonomy）のアップデートを公開した。

[17] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_framing_2020-07-09.pdf

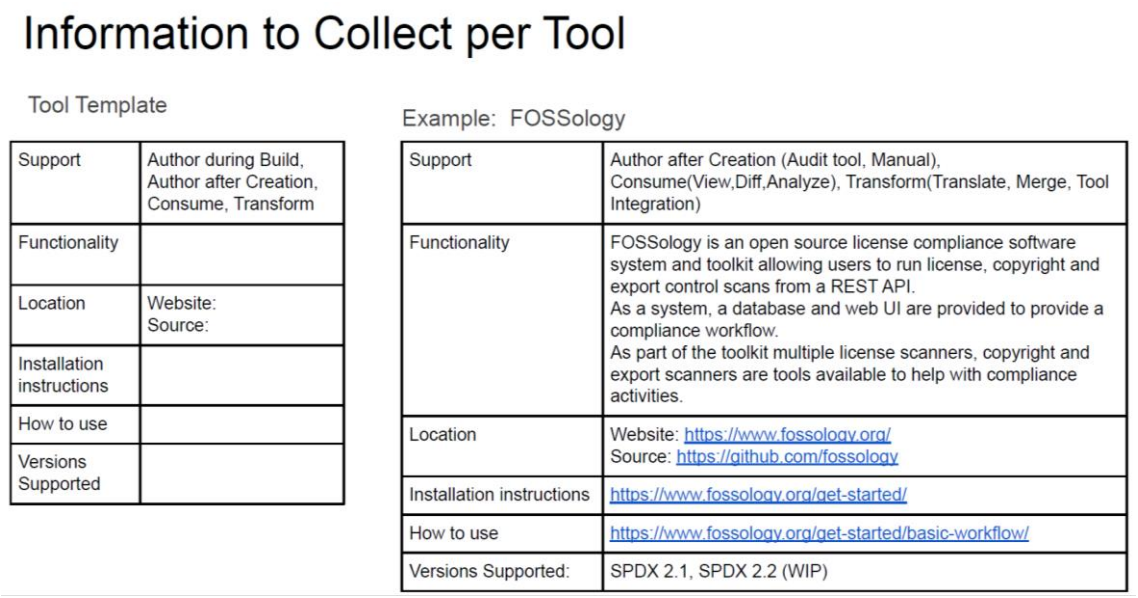
表 4 SBOM ツール分類表のアップデート

カテゴリ	タイプ	詳細
ソフトウェア作成中の主体（Author during Build）	Build	ソフトウェア作成の過程でドキュメントは自動的に作成される。
ソフトウェア作成後の主体（Author after Creation）	Manual	手動で情報を入力する。
	Audit Tool	ソースコード分析または監査ツールはソフトウェアの検査ごとにドキュメントを作成する。
使用（Consume）	View	人間が読解可能なフォー的でコンテンツを表示する（画像、数字、図表、文章）。意思決定や経営の支援に使用される。
	Diff	2 つのドキュメントの相違点を比較可能とする。例えば、ソフトウェアの異なるバージョンなど。
	Analyze	ドキュメント情報のインポートを可能とする。
変換（Transform）	Translate	情報の内容を保ちつつ、ドキュメントのフォーマットを変換する。
	Merge	分析ないし監査の為、複数ソースのドキュメントを統合する。
	Tool integration	その他のツールの使用による APIs やライブラリのサポート。

出典：SBOM Tool Classification Taxinomy draft[18]

ツールのテンプレートと事例（FOSSology）は以下のとおり。

18 https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy_july9.pdf



Information to Collect per Tool

Tool Template

Support	Author during Build, Author after Creation, Consume, Transform
Functionality	
Location	Website: Source:
Installation instructions	
How to use	
Versions Supported	

Example: FOSSology

Support	Author after Creation (Audit tool, Manual), Consume(View,Diff,Analyze), Transform(Translate, Merge, Tool Integration)
Functionality	FOSSology is an open source license compliance software system and toolkit allowing users to run license, copyright and export control scans from a REST API. As a system, a database and web UI are provided to provide a compliance workflow. As part of the toolkit multiple license scanners, copyright and export scanners are tools available to help with compliance activities.
Location	Website: https://www.fossology.org/ Source: https://github.com/fossology
Installation instructions	https://www.fossology.org/get-started/
How to use	https://www.fossology.org/get-started/basic-workflow/
Versions Supported:	SPDX 2.1, SPDX 2.2 (WIP)

出典：Formats and Tooling WG プレゼンテーション資料[19]

図 6 SBOM ツールのテンプレートと事例

今後のステップとして、Formats and Tooling WG はヘルスケア PoC や Framing といったその他の WG との連携を予定している。Framing WG が取り組む SBOM の運用ガイドライン（Playbook/CONOPs）において、以下のような状況に応じたツールとその使用方法を紹介するガイドラインの作成に取り組む。

- SBOM の作成と使用
- 異なるユースケース
  - ✧ ソフトウェアライフサイクルマネジメント
  - ✧ 資格（Entitlement）
  - ✧ 脆弱性マネジメント
- サプライチェーンにおける異なる役割
  - ✧ サードパーティサプライヤ（OSS、商用ソフトウェア）
  - ✧ 統合者（Integrator）
  - ✧ ファーストパーティデベロッパー（企業内 DevOps）
  - ✧ 調達

[19] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_formats_tooling_2020-07-09_updated.pdf

- ✧ コンプライアンス（外部の認証、規制、保険機関とのインターフェース）

3) Awareness and Adoption WG

Awareness and Adoption WG は SBOM の普及促進のための様々な取り組みを実施している。当 WG の主な取り組みは以下のとおり。

- COVID-19 によりカンファレンスその他のアクティビティが中止されていることから、オンラインで SBOM フェーズ 1 アウトプットの成果を紹介。
- SBOM FAQ の第 2 弾リリース。第 1 弾からのフィードバックや FDA の SBOM 関連要求事項に関する項目を追加。
- SBOM コンセプトを説明する 2 ページまとめの公開
- SBOM フェーズ 1 の紹介動画
- NTIA ミーティング、カンファレンス、ポッドキャストの録画、公開
- 特定のセクター向けのドキュメント作成
- フェーズ 1 ドキュメントのクロスリファレンスができる検索機能の付加
- 「How to PoC」バーチャルサミットやその他のセクターにおける PoC テンプレートを含むオンラインでのエンゲージメント

SBOM FAQ 第 2 弾のコンテンツは以下のとおり[20] 。

- 全般
  - ✧ SBOM とは何か？
  - ✧ 誰が何のために SBOM を使用するのか？
  - ✧ 誰が SBOM を作成し、更新するのか？
  - ✧ SBOM の改変や更新はいつ行われるのか？
  - ✧ サイバー攻撃の際に SBOM はどのように役立つのか？
  - ✧ ソフトウェアコンポーネントはそれ自体が複数のコンポーネントから構成されている場合がある。SBOM はそのようなソフトウェアコンポーネントの構成を可視化できるか？
  - ✧ NTIA の SBOM プロジェクトに関する情報はどこで得られるか？プロジェクトに参加することは可能か？
  - ✧ SBOM の利点は何か？

[20] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_faq_july9.pdf

- ✧ BoM ないしサプライチェーンの透明性確保が有効性を示した事例はあるか？
- ✧ SBOM は脆弱性マネジメントのほか、どのように利用できるか？
- ✧ 誰が SBOM を所有すべきか？

- SBOM への懸念について
  - ✧ SBOM が「サイバー攻撃のためのロードマップ」になる恐れはないか？
  - ✧ SBOM によりライセンス侵害の可能性は増すか？
  - ✧ SBOM はパテントないしライセンス・トロールとなり得るか？
  - ✧ SBOM にはソースコード開示が必要となるか？
  - ✧ SBOM に記載されるコンポーネントの情報には知的所有権は含まれるか？
  - ✧ SBOM によりライセンス費用やコミットメントの負担増加は発生するか？
- SBOM 使用の詳細について
  - ✧ SBOM には何が含まれるか？
  - ✧ SBOM の相関グラフ（dependency graph）の深度はどの程度か？
  - ✧ SBOM を作成した場合、作成者は SBOM を公表しなければならないのか？
  - ✧ SBOM データはどのようにして共有されるのか？
- 事例別
  - ✧ ソフトウェアの購入者（Purchaser）はどのように SBOM を呼び出すのか？
  - ✧ 新たなサイバー脅威への対処において、SBOM はどのように利用できるか？

4）Healthcare Proof of Concept WG

ヘルスケア PoC WG は、PoC モデルを他の産業においてどのように再現するかという課題に注力している。当 WG の作業には SBOM 作成のためのツールを提供するベンダやサプライヤのための PoC 参加枠組みの構築も含まれる。例えば、ヘルスケア PoC においては消費者に医療機器の比較検討を可能とするネットワークを運営する Medigate という企業と協力を行った。Medigate は SBOM を利用して医療機器のセキュリティに関連する情報を利用することが可能となった。現在では、米国の大手医療機関（Health Delivery Organization: HDO）の大半が SBOM のイニシアティブを支持しているという。今後のヘルスケア PoC WG の活動目標には以下が挙げられる。

- SBOM フレーミングドキュメントの有効性の検証
- ユースケースおよび参加者の拡大
- SBOM 作成ツールおよび自動化の検証

- HDO や MDM（Medical Device Manufacturer）向けのガイドブック作成
- SBOM の定義に関して、Framing や Tooling を含む他の WG との連携
- 一般的に HDO が使用している医療機器一式の SBOM 作成

ヘルスケア PoC フェーズ 2 に参加している医療機器ベンダと医療機関は以下のとおり。

出典：Healthcare PoC WG プレゼンテーション資料[21]

図 7 ヘルスケア PoC フェーズ 2 参加機関のリスト

ユースケースの実施に関しては SPDX フォーマットにおけるプライマリコンポーネントの SBOM 作成に焦点が置かれる。この作業にはサプライヤの関与無しのコンポーネントの特定、Framing WG が定義する SBOM コンテンツの有効性の確認が含まれる。さらに、ヘルスケア PoC WG は秘密保持契約（Non-Disclosure Agreement: NDA）によって MDM から提供された占有データ（proprietary data）の保護についても検討を行う。

ヘルスケア PoC においては HDO は自らが使用する医療機器のインベントリを MDM に提供し、これに基づいて MDM は当該医療機器の SBOM 作成を行うことができた。PoC フェーズ 2 が実施された 6 週間においては、手動プロセスと SBOM 作成ツールの利用を含めて計 17 の SBOM が作成された。これはフェーズ 1 の同期間内における SBOM 計 7 から飛躍的に進歩しており、現在ではプロセスが確立されたことから、同期間内により多くの SBOM を作成することができるだろう。PoC において SBOM は Box というファイル共有サービスを介して配布された。SBOM 作成のガイドブックとして、ヘルスケア PoC WG は Framing と Tooling の各 WG と協力して SBOM 作成のガイダンスと事例紹介のドキュメントを作成している。

[21] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_healthcare_poc_2020-07-09.pdf

ヘルスケア PoC WG の課題は以下のとおり。

- SBOM データの収集。多くの MDM や HDO において、SBOM 作成のために必要な情報を収集するインフラストラクチャが欠如している。
- HDO を含むソフトウェアのユーザーはソフトウェアの新たなバージョンを把握していない場合がある。この点についてヘルスケア PoC の次回イテレーションで検証を行う。
- 不完全な SPDX フォーマットは PURL の識別子を認識できない。
- 当 WG が求めるフォーマットを作成できるツールは限定的である。

ヘルスケア PoC WG はまた、Framing WG と協力してネーミング特定の手法を確立したサプライヤのリストを作成している。複数の医療機器に使用されている共通のオープンソース・コンポーネントを特定するために、MDM はソフトウェア・アイデンティティを記載したコンポーネントのリストを提供している。

ヘルスケア PoC フェーズ 2 の第二次イテレーションには以下の目的が含まれる。

- IoT 医療機器の SBOM をどのようにして作成するか。
- 脆弱性をどのように評価するか。
- SBOM のバージョンおよびフォーマット（SWID, CycloneDX）
- ファイル共有を介さない SBOM 拡散の自動化
- 医療機器のアセットマネジメントシステムへ SBOM を直接登録、および脆弱性データを利用したリスクマネジメント
- 脆弱性データベースを利用した SBOM と脆弱性関連情報の相関確保
- 医療機器の脆弱性を確認するための SBOM データのサーチエンジン構築
- 医療機器の調達契約において SBOM の作成を依頼するためのプロダクトセキュリティ言語の構築

SBOM の使用に関して、HDO ユースケースのアップデートは以下のとおり。

- 調達
    - ✧ 回答が得られた HDO3 機関はいずれも病院の SIEM（Security Information and Event Management）ソリューションに SPDX フォーマットの SBOM を統合（ingest）しており、脆弱性に関するデータがごく短時間で検索可能となった。このデータは人間が読解できるフォーマットに変換することも可能となっている。

- ✧ 多くの HDO は MDM と協力し、医療機器の調達の段階で資産管理・リスク管理のソリューションに直接統合する方法を模索している。
- ✧ Ceders Sinai 病院はパートナーMDM と協力し、ヘルスケア・ベンダ・リスクマネジメント（Vendor Risk Management: VRM）ソリューションに SBOM を直接統合する方法を模索している。
- ✧ NYP 病院はパッケージ・フィールドを構築するための How-To ガイドを作成しており、ガイドには SBOM に関する言及も含まれている。
- ✧ 外部リソースからの情報収集に際しては引き続きコンポーネントのネーミング問題が課題となる。
- ✧ HDO は調達に際して自動的に脆弱性に関するデータを収集するシステム構築の作業を継続する。

- アセットマネジメント
  - ✧ 回答が得られた HDO のうち 2 病院においては構成管理データベース（Configuration management database: CMDB）プラットフォームにおけるソフトウェアコンポーネントのアセットマネジメントを開始している。本ユースケースは医療機器の導入時に限らず、SIEM に入力されたデータを利用して継続的なアセットマネジメントを可能とする。
  - ✧ 複数の HDO はパートナーMDM と協力し、医療機器のライフサイクルを通して定期的なアップデートによる医療機器のアセットマネジメントの手法を模索している。
- リスクマネジメント
  - ✧ 回答が得られたすべての HDO は調達時および継続的に脆弱性の特定を試みている。（例：SIEM, CMDB/CMMS、VRM）
  - ✧ HDO はセキュリティ関連データを SBOM に取り込む試みを行っている。
- 脆弱性マネジメント
  - ✧ Ceders Sinai 病院は MDM と協力して SBOM から得られるデータを使用して手動の弱性管理を試みている。さらに、同病院は医療機器の脆弱性をスキャンするツールの導入を予定している。
  - ✧ NYP 病院は院内の脆弱性管理チームとともに医療機器のスキャンと SBOM データの相関の評価に取り組んでいる。
  - ✧ Sutter Health 病院は院内の脆弱性管理チームとともに定期スキャンの結果を補完するための SBOM の活用方法の検討に取り組んでいる。
- リーガル
  - ✧ PoC に参加する HDO は契約文書のサイバーセキュリティ強化のために SBOM プロダクトセキュリティ言語の構築に取り組んでいる。

公開予定のヘルスケア PoC WG の報告書には以下がある。

- SBOM 作成サマリ：SPDX フォーマットの SBOM を作成するためのハイレベルガイドブック
- ツールサマリ：PoC フェーズ 2 第二次イテレーションで使用されたツールの一覧およびツールの使用ガイド
- SBOM 要素の使用に基づく有効性評価
- SBOM 使用に関するクイックスタートガイド

ヘルスケア PoC WG は今後は他の産業における PoC の実施を視野に入れ、2020 年内には知識を共有するための「PoC 実施サミット」の開催を予定している。自動車セクターは既に独自に PoC を開始しており、日本のステークホルダも関心を示しているという。

(3) ステークホルダディスカッション

1) エネルギーセクター

参加者から SBOM のコンセプトはファームウェアを含むソフトウェアの異なる側面に対応していないという指摘があった。エネルギーセクターで一般的に使用されているファームウェアバージョンと SCADA ソフトウェアについて、参加者は SBOM の作成を試みたが困難に直面したという。米国エネルギー省が SBOM の重要性を確認するための RFI（Request for Information）を発表したことを受けて、当参加者は NTIA ステークホルダ会合にエネルギーセクターへの関与の強化を求めた。

2) 今後のステップ

NTIA ステークホルダ会合は今後対処すべき課題として、SBOM の作成と使用に関する明示的なガイダンスの欠如を挙げている。各 WG はフェーズ 1 から得られた教訓を踏まえ、SBOM 導入を望む組織が参照できる SBOM 作成・使用のガイダンス作成を検討している。

2.3.3. 2020 年 10 月会合

(1) サマリ

2020 年 10 月 22 日に開催された。

- SBOM のネーミング問題は引き続き最大の課題と認識されており、解決策としてコンポーネント名称の関連付けを行う「ネームスペース」の設置や、コンポーネントのヒエラルキーの明確化や相関の特定が提案された。（2.2 関連）

- ヘルスケア PoC はフェーズ 2（PoC2.0）のイテレーションでユースケースを拡大するとともに、フェーズ 1 で得られた経験を基に SBOM のクイックスタートガイドを含む関連ドキュメントを充実させている。（2.3 関連）
- ネーミング問題を解決するための用語集作成の作業も進められるが、Allan Friedman 氏は現時点で用語の詳細を固めることは得策ではなく、依然として議論が必要という見解を示した。（2.6 関連）

(2) WG 別報告

議長の Allan Friedman 氏より、ソフトウェアの透明性に関する NTIA の活動と今後の方向性について報告があった。SBOM プロジェクトは自動車、医療を含む幅広いセクターからのステークホルダの参加を実現している。現在進行中の SBOM フェーズ 2 エフォートでは、より広域のユースケースの実現を目指す。

1) Framing Working Group

フレーミング WG は SBOM の共有と互換（Sharing and Exchange of SBOMs[22] ）に関する報告書のドラフト版を作成している。この報告書は SBOM に関する用語や SBOM へのアクセスに関してステークホルダに明確なガイドラインを提供することを目的としている。

SBOM の共有と互換に関する報告書においては、SBOM 作成のタイミングやどこで SBOM を閲覧できるかについて提案を行っている。サプライチェーンの透明性確保により、ソフトウェアの作成者およびユーザーがリスクを認識して意思決定ができるようになるため、SBOM が適切な時と場所で閲覧可能とされることが重要である。特にどこで SBOM を閲覧できるか（Advertisement or Discovery）と SBOM へのアクセス（Access）に重点が置かれている。アクセスに関しては、例えばソフトウェア作成者が URL やマニフェストにおいて SBOM の在処をユーザーに通知する、またはソフトウェアアップデートに SBOM へのアクセス方法を含むという 2 通りの手法が提案されている。

さらに、フレーミング WG はソフトウェアの特定の課題に対するガイドライン（Software Identification Challenge and Guidance[23] ）の作成に取り組んでいる。コンポーネントのネーミングは依然として SBOM の最大の課題と認識されており、ネーミング問題の解決策として、コンポーネント名称の関連付けを行う「ネームスペース」の設置や、コンポーネントのヒエラルキーの明確化や相関の特定が提案されている。このほか、ソフトウェア開発者にサプライヤ ID を付与してコンポーネントの名称を統合管理するサプライヤデータベー

22 https://docs.google.com/document/d/1XuGix4AIcXKqPlPVMvjQEj7zybvnYy4DkgpYfF2EwRc/edit

23 https://docs.google.com/document/d/1tOtO90AIrsHSIPvcVhvSBmkuS1mkFWIYWFNlPnjSzhQ/edit

スを用いた解決策も提案された。

理想的にはソフトウェア作成者がソフトウェア開発の時点で SBOM を合わせて作成することであるが、現時点では確実に実施されておらず、ソフトウェアのユーザーが自ら使用するソフトウェアの SBOM を作成する事例が往々にして見られる。SBOM 作成のリソースに関しては、フレーミング WG はパッケージマネージャーをはじめとする既存のソフトウェア管理ツールの利用を奨励しているが、このようなツールを使用していないソフトウェア開発者のために代替のソリューションも提案している。

最後に、フレーミング WG は脆弱性（VEX: Vulnerability EXploitability）のコンセプト特定の作業を進めている。例えば CVE（共通脆弱性識別子）への対処において、現時点ではユーザーはソフトウェア開発者に対応を求めているが、SBOM を使用してコンポーネントの特定が可能となることでユーザーが自ら CVE に対処することが可能となる。現在のステップ 1 で脆弱性とユースケースの特定を進め、次のステップで脆弱性の解決策の模索を行う。

2) Healthcare Proof of Concept WG

ヘルスケア PoC WG はフェーズ 2 エフォート（PoC2.0）のための SBOM の作成と、1.0 で作成された SBOM の利用（consumption）の進捗を発表した。PoC2.0 は以下を主な目的とし、PoC に参加するベンダの数は継続的に増加している。

- フレーミング WG が作成したドキュメントの有効性の検証
- ベースライン要素の特定
- PoC1.0 と異なるユースケースの実施
- 参加者の拡大
- SBOM の作成と利用における自動化ツールの統合

PoC2.0 のイテレーション 1 は医療機関（HDO）によるソフトウェア調達のユースケースから着手しており、医療機器ベンダ（MDM）が SPDX のフォーマットで SBOM を作成する中でコンポーネントのベースライン要素が確実に SBOM に記載されることを確認した。

PoC2.0 のイテレーション 2 においては、イテレーション 1 からさらに発展させて MDM に加え、その他のステークホルダが SBOM を作成する場合のユースケースを実施している。ソフトウェアのネーミング問題に対処するために、ヘルスケア PoC WG はユースケースを実施した全ての機関が共通して使用したコンポーネントの一覧表を作成し、ネーミングの統一に活用している。

PoC1.0 を経て SBOM 作成に関するリソースも充実しており、以下のとおり医療機器ベンダが SBOM を作成する際に必要な情報を記した How-to ドキュメントや、ソフトウェアコンポーネントのマスターリストが公開

されている[24] 。

- SBOM 作成の How-to ドキュメント
- 医療機器のシステムの SBOM 事例
- SBOM コンポーネントマスターリスト
- SBOM レジストリ
- SBOM 事例集
- SVOM 作成ツール

医療機関（HDO）側の動きとしては、PoC に参加している全ての HDO が SIEM（Security Information and Event Management）、ベンダ管理、アセット管理を含む複数のソリューションへの SBOM の取り込みに成功している。さらに、HDO は医療機器の調達ライフサイクルにおける MDM やサードパーティベンダとの連携において SBOM データの活用を実践している。

PoC1.0 で作成された SBOM の利用に関しては、SBOM 利用のクイックスタートガイドの最新版（V1.2）が公開された。他方、HDO が直面する最大の課題には、SBOM とその他のソフトウェアコンポーネントのリソースを比較した際に生じる情報のミスマッチの問題が指摘されている。主要な HDO が指摘した課題は以下のとおり。

- Cedars-Sinai
  - ✧ SBOM の SPDX ファイルとその他の脆弱性データベースが作成する情報ソース間のコンポーネント名称の互換性の欠如。
  - ✧ 異なるファイルごとに脆弱性のマッピングを行うことが困難であり、エラーが発生する。
- New York Presbyterian
  - ✧ Cedars-Sinai が指摘した上記の課題に同意。
  - ✧ 国家脆弱性データベース（NVD）に登録された脆弱性との互換性欠如の課題。
  - ✧ MDM ごとに SPDX のヘッダースキームが若干異なる点。
- Mayo Clinic
  - ✧ 上記の 2 病院が指摘した課題に同意。SBOM データと NVD のネーミングが一致しない問題を経験した。

[24] ヘルスケア PoC WG プレゼンテーションの p.7 にある埋め込みリンクから各文書にアクセス可能。
https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_healthcare_2020-10-22_1.pdf

- Sutter Health
  - ✧ SBOM と NVD のネーミングの不整合の課題。
  - ✧ 脆弱性に関する NDV データベースのアップデートが自動的に反映されず、結果として多くの手作業が発生している点。
  - ✧ その他、上記の 3 病院と同様の課題を指摘。

3) Formats and Tooling WG

Formats and Tooling WG プレゼンテーション＆ディスカッション

Formats and Tooling WG のフェーズ 2 エフォートでは引き続き SBOM 作成のためのツールや分類表（Taxonomy）の作業を継続している。SBOM の 3 つのフォーマット（SWID, SPDX, CycloneDX）の作成を支援するツールを継続しており、各フォーマットに関する最新のツール集が以下のとおり公開されている。

- SWID[25]
  - ✧ オープンソースツール

    Swidgen

    StrongSwan SWID Generator

    Labs64 SWID Generator

    Labs64 SWID Maven Plugin

    libswid

    SwidTag

    TagVault SWID Tag Creator

    RPM 2 SWID Tag

    NIST SWID for GNU Autotools

    NIST SWID Tag Validato

    NIST SWID Builder

25 https://docs.google.com/document/d/1oebYvHcOhtMG8Uhnd5he0l_vhty7MsTjp6fYCOwUmwM/edit#

NIST SWID Maven Plugin

NIST SWID Repo Client

WiX Toolset

swidq

✧ 有償製品

IT Operations Management

Jamf Pro

CyberProtek

MedScan

BigFix Inventory

Vigilant-ops

Microsoft Endpoint Configuration Manager

- SPDX[26]
  - ✧ オープンソースツール

Augur

FOSSology

in-toto

kernel-spdx-ids

Longclaw

npm-spdx

Open Source Software Review Toolkit (ORT)

OWASP Dependency-Track

Quartermaster (QMSTR)

REUSE

SwiftBOM - CERT CC SBOM tool

ScanCode Toolkit

SCANOSS

[26] https://docs.google.com/document/d/1A1jFIYihB-IyT0gv7E_KoSjLbwNGmu_wOXBs6siemXA/edit

SPDX Java Libraries and Tools

SPDX Python Libraries

SPDX Golang Libraries

SPDX JavaScript Libraries

SPDX Online Tools

SPDX Maven Plugin

SPDX Build Tool

SPARTS

SW360

TERN

Yocto Project / OpenEmbedded

✧ 有償製品

CyberProtek

FOSSID

Hub-SPDX (Black Duck Hub Report Utility)

MedScan

Protecode

Protex

SourceAuditor

TrustSource

Vigilant-ops

- CycloneDX[27]

✧ オープンソースツール

CycloneDX Core for Java

CycloneDX for .NET

CycloneDX for NPM

27

https://docs.google.com/document/d/1biwYXrtoRc_LF7Pw10TO2TGIhlM6jwkDG23nc9M_RiE/edit

CycloneDX for Maven

CycloneDX for Gradle

CycloneDX for PHP Composer

CycloneDX for Python

CycloneDX for Ruby Gems

CycloneDX for Rust Cargo

CycloneDX for SBT

CycloneDX for Elixir Mix

CycloneDX for Erlang Rebar3

CycloneDX for Go

cdx-bower-bom

cdxgen

CycloneDX-Buildroot

Eclipse SW360 Antenna

GitHub Action: CycloneDX for Node.js

GitHub Action: CycloneDX for .NET

GitHub Action: CycloneDX for PHP

GitHub Action: CycloneDX for Python

GitHub Action: CycloneDX for Elixir Mix

GitHub Action: cdxgen

HERE Open Source Review Toolkit

Retire.js

OWASP Dependency-Track

OWASP Dependency-Track Jenkins Plugin

dtrack-audit

ShiftLeft Scan

SCANOSS

oss_inventory

Auditjs

Chelsea

Jake

Nancy

Go Sonatypes

Valaa Stack

✧ 有償製品

Sonatype Nexus IQ

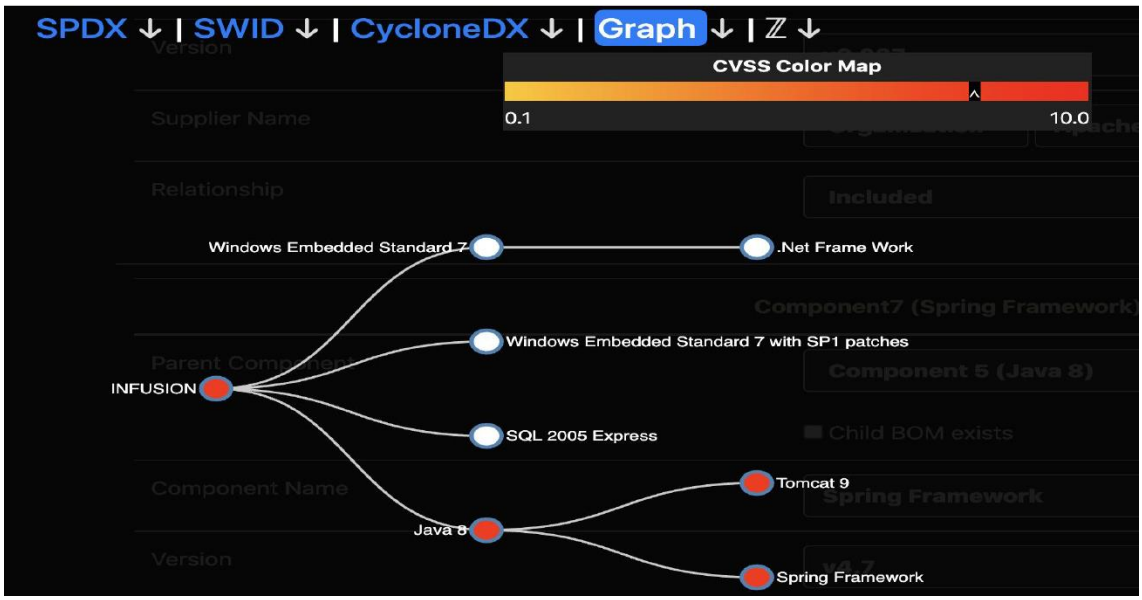
Sonatype Nexus Lifecycle Jenkins Plugin

CyberProtek

MedScan

Reliza Hub

SBOM 作成ツールの例としてカーネギーメロン大学のソフトウェアエンジニアリング研究科が開発したウェブベースの SBOM 作成ツールである SwiftBom が紹介された。SwiftBom はユーザーのインプットにより SBOM の作成を可能とするとともに、SBOM の管理や統合といった作業を可能としている。さらに、SwiftBom は SPDX, SWID, CyclineDX の各フォーマットによる SBOM のダウンロードを可能としている。



出典：Formats & Tooling WG プレゼンテーション[28]

図 8 SwiftBom が作成する SBOM のイメージ

SBOM の使用に関するルールブック（Playbook for Software Consumers: SBOM Acquisition, Management and Use[29] ）には、サプライヤによる SBOM の取得をはじめとする SBOM の作成と利用に関する各ステップが説明されている。今後ルールブックには SBOM からのデータの抽出やソフトウェアの脆弱性への対処の項目の追加が予定されている。さらに、SBOM には知財（IPR）や機密情報に関連するデータが含まれる場合もあることから、ソフトウェアコンポーネントの透明性確保と機密保護のバランスを確保することが今後の課題として挙げられる。

当 WG の今後の活動の予定としては、SBOM ツール利用に関するルールブックの最終化に加え、ヘルスケア PoC やフレーミングといった他の WG との連携も想定している。

4）Awareness and Adoption WG

Awareness and Adoption WG は SBOM のプロモーションに関する活動を継続している。SBOM 開設のパンフレット（Two-Pager）の更新に加え、SBOM を周知するためのバーチャル会議の実施にも取り組んでいる。

---

[28] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_tooling_2020-10-22_1.pdf

[29] https://docs.google.com/document/d/1Ae0l1MDS8m1on58e8mdVIA9NujzPD0k5j352VlDZr9I/edit

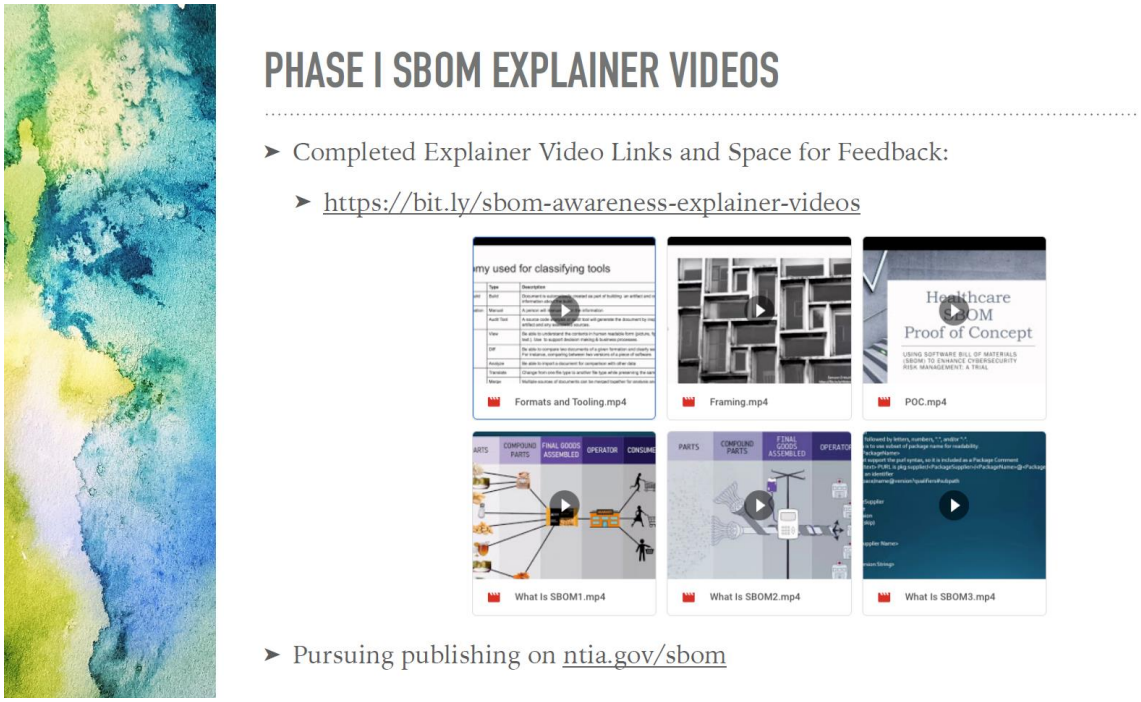
最新版の SBOM FAQ のコンテンツは以下のとおり[30]。

- 全般
  - ✧ SBOM とは何か？
  - ✧ 誰が SBOM を所有するべきか？
  - ✧ 誰が何のために SBOM を使用するのか？
- メリット
  - ✧ SBOM を使用することのメリットは何か？
  - ✧ サイバー攻撃の際に SBOM はどのように役立つのか？
  - ✧ SBOM は脆弱性管理のほか、どのように役に立つか？
  - ✧ サプライチェーンの透明性確保や BOM の有効性が示されたセクターの事例はあるか？
- 一般的な誤認識、懸念
  - ✧ SBOM が「サイバー攻撃のためのロードマップ」になる恐れはないか？
  - ✧ SBOM にはソースコード開示が必要となるか？
  - ✧ SBOM に記載されるコンポーネントの情報には知的所有権は含まれるか？
  - ✧ SBOM によりライセンス侵害のリスクは高まるか？
  - ✧ SBOM はパテントないしライセンス・トロールとなり得るか？
  - ✧ SBOM によりライセンス費用やコミットメントの負担増加は発生するか？
- 作成
  - ✧ 誰が SBOM を作成・維持するのか？
  - ✧ SBOM には何が含まれるか？
  - ✧ SBOM データのフォーマットには何があるか？（新規の項目）
  - ✧ 異なる SBOM フォーマットの変換を可能とするツールはあるか？（新規の項目）
  - ✧ SBOM はどのタイミングで作成、変更、メンテナンスされるか？
  - ✧ ソフトウェアコンポーネントはそれ自体が複数のコンポーネントから構成されている場合がある。SBOM はソフトウェアコンポーネントのヒエラルキーを示すことができるか？
  - ✧ SBOM が示す相関グラフの深度はどの程度か？
- 共有

[30] https://www.ntia.doc.gov/files/ntia/publications/sbom_faq_-_fork_for_october_22_meeting.pdf

- ✧ SBOM を作成した場合、作成者は SBOM を公表しなければならないのか？
- ✧ SBOM データはどのようにして共有されるのか？

- 事例別
  - ✧ ソフトウェアの購入者（Purchaser）はどのように SBOM を呼び出すのか？
  - ✧ 新たなサイバー脅威への対処において、SBOM はどのように利用できるか？
- 他ツールとの関連
  - ✧ SBOM は MDS2（製造業者による医療機器セキュリティ開示説明書）とどのように関係しているのか？（新規の項目）
  - ✧ SBOM は OpenC2 とどのように関係しているのか？（新規の項目）
  - ✧ SBOM は MUD（Manufacturer Usage Descriptions）とどのように関係しているのか？（新規の項目）
  - ✧ SBOM は DBOM とどのように関係しているのか？（新規の項目）
- SBOM プロセスへの関与
  - ✧ NTIA の SBOM プロセスに関する情報はどこで得られるか？どのようにしてプロセスに関与できるか？



出典：Awareness & Adoption WG プレゼンテーション[31]

図 9 Google Drive 内のファイルにより Awareness & Adoption WG が作成した SBOM のプロモーション動画を閲覧できる

また、ヘルスケア PoC WG との連携も行っており、ヘルスケア以外にも他のセクターにおいて SBOM の PoC を実施するエンゲージメントの機会を模索している。

(3) ステークホルダディスカッション

NTIA ステークホルダ会合は今後の動きとして、各 WG の連携による SBOM のクイックスタートガイドの作成や PoC で得られた知見の共有が挙げられる。コンポーネントのネーミング問題を解決するための用語集作成の作業も進められるが、Allan Friedman 氏は現時点で用語の詳細を固めることは得策ではなく、依然として議論が必要という見解を示した。

PoC の対象セクター拡大の関連では、エネルギー、金融セクターや IoT デバイスへの適用が挙げられた。特に自動車産業の情報共有分析センター（Auto ISAC）を介した自動車産業における PoC の実施が議論されている。自動車産業はソフトウェアを含むサプライチェーンの可視化の観点から SBOM に関心を寄せており、2019 年には Auto ISAC は SBOM の PoC 実施の可能性について協議し、現在は PoC の実施に向

[31] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_adoption_2020-10-22_1.pdf

けたフレームワーク構築を進めている。

2.3.4. 2021 年 1 月会合

(1) サマリ

2021 年 1 月 13 日に開催された。

- Awareness & Adoption WG のプレゼンテーションにおいて、Auto-ISAC の代表から自動車 PoC の進捗に関する報告があった。PoC はタイムラインやリソース配分を決定するプランニングのフェーズが進行しており、今後約 1 年をかけて PoC の実施とレビューを行い、PoC の成果物として自動車メーカーに提供する情報の規格統一に向けたサプライヤからの提言をまとめた報告書の作成を予定している。（2.2 関連）
- NTIA ステークホルダ会合初の試みとして、SBOM の作成や利用に有効なツールのデモンストレーションが行われた。ツールの作成に携わった組織や企業の代表がステークホルダとして会合に参加し、SBOM “Show and Tell”という題目で、6 プロジェクトの紹介とデモンストレーションが行われた。（2.6 関連）
- 現在進行中の自動車産業の PoC に加え、エネルギー産業においても SBOM の PoC の実施を予定しており、今後 2021 年 3 月から 4 月にかけて NTIA のコミュニティサイトで詳細が公開される予定。（2.7 関連）

(2) WG 別報告

議長の Allan Friedman 氏より、挨拶があった。

- SBOM プロジェクトの進捗状況と今後の方針について報告があった。2020 年はパンデミックの影響を受け、ステークホルダ会合やプロジェクト全般を通してリモート化が大きく促進されるとともに、SBOM の定義の具体化が進んで関連ツールの登場や SBOM 導入といった実践の面で多くの進展があった。
- 実際、最近の NTIA ステークホルダ会合においては「SBOM とは何か（what）」から「SBOM をどのように（how）活用するか」にフォーカスが移っている。2021 年はこのような SBOM 導入の事例をさらに拡大し、SBOM 導入にかかる障壁の撤廃のあり方を模索するとともに、PoC パイロットケースの充実に向けてステークホルダとの連携強化を図る。

1) Framing Working Group

フレーミング WG は SBOM の共有（Sharing and Exchanging SBOMs）およびコンポーネントのネーミング問題に対するガイダンス（Software Identification Challenge and Guidance）の 2 つの報

告書の最終化を進めている。SBOM のベースライン要素、ネーミング問題、脆弱性（Vulnerability EXploitability：VEX）への対応に関する作業を継続し、ヘルスケア PoC から得られたフィードバックをフレーミングの文書に反映するフェーズ 2 の作業に入る。

VEX への対応はフレーミング WG が集中的に取り組んでいる作業の一つであり、VEX のネーミング自体も引き続き議論の対象となっている。上流コンポーネントで確認される脆弱性に対して、課題の特定と対処法について対応するガイドラインの作成を目指す。既に異なるフォーマットの SBOM の VEX 特定とドラフト版報告書作成に取り組んでおり、次のステップでドラフト版報告書の有効性の検証と議論を行う。

上記に加えて、フレーミング WG の今後の作業には SBOM のベースラインコンポーネント（Minimum baseline components）の特定により、SBOM が機能するために最低限必要となるコンポーネントは何か、ユースケースにおいて検証を試みる。

2）Formats and Tooling WG

Formats and Tooling WG は、サプライヤとユーザー向けにそれぞれ SBOM のルールブック（Playbook）の作成を進めている。SPDX、SWID、Cyclone DX の各フォーマットを変換するツールの特定も進められており、ヘルスケア PoC で使用された SwiftBOM のほか、DecorderRing、SPDV tools、CycloneDX CLI といったツールによる SBOM のフォーマット変換が可能となっている。現在進行中の作業としては各フォーマットの SBOM のバイナリコードの事例を GitHub で公開しているほか、新たな試みとして SBOM の作成や編集を可能とするツールに関する情報を集めた資料集（SBOM Reference Corpus）の作成を進めている。

当 WG はフレーミング WG と共同で SBOM のベースラインコンポーネントの特定も進めている。

What should a minimum viable SBOM contain?

NTIA SBOM Minimum Fields	SPDX	SWID	CycloneDX
Supplier Name	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/publisher), @name	publisher
Component Name	(3.1) PackageName:	<softwareIdentity> @name	name
Unique Identifier	(3.2) SPDXID:	<softwareIdentity> @tagID	bom/serialNumber and component/bom-ref
Version String	(3.3) PackageVersion:	<softwareIdentity> @version	version
Component Hash	(3.10) PackageChecksum:	<Payload>/../<File> @[hash-algorithm]:hash	hash
Relationship	(7.1) Relationship: CONTAINS	<Link> @rel, @href	(Nested assembly/subassembly and/or dependency graphs)
Author Name	(2.8) Creator:	<Entity> @role (tagCreator), @name	bom-descriptor:metadata/manufacture/contact

Source: NTIA's Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)

図 10 SBOM のベースラインコンポーネントのサンプル（プレゼンテーション資料）[32]

当 WG はまた、知財（IP）や機密情報が SBOM の有効な利用を妨げる課題と成り得る点を指摘している。解決策の提案としては、SBOM の共有に関する条件を契約等で管理し、秘密保持契約（NDA）を締結した者に SBOM の共有を認めるという方法がある。

今後の作業としては、SBOM 関連ツールの情報収集を継続してルールブックを最終化するとともに、ヘルスケアはじめ複数産業の PoC と連携してフレーミング WG の作業にフィードバックを提供する。

3) Awareness and Adoption WG

Awareness and Adoption WG は SBOM のプロモーションとアウトリーチ拡大の作業を継続している。2020 年には主にバーチャルで SBOM プロモーション資料の拡散やイベントに参加したほか、Auto ISAC における SBOM の PoC のキックオフ実施やエネルギー産業における SBOM PoC の計画も進行している。今後も新たな産業における PoC の促進や、GitHub コミュニティにおける SBOM の展開、YouTube 上で SBOM のプロモーション動画の公開、バーチャルイベントの開催に取り組む。

[32] https://www.ntia.doc.gov/files/ntia/publications/ntia-sbom-tooling_2021-01-13.pdf

図 11 2020 年の Awareness and Adoption WG の成果まとめ（プレゼンテーション資料）[33]

Awareness and Adoption WG の報告の後、自動車産業における PoC の進捗について、自動車情報共有・分析センター（Automotive Information Sharing and Analysis Center: Auto-ISAC）の代表から報告があった。Auto-ISAC は自動車産業における全てのソフトウェアコンポーネントを追跡できるデータベース構築の必要性を認識しており、SBOM のコンセプトは自動車産業のサイバーセキュリティ強化に有効となる。

Auto-ISAC における SBOM PoC は自動車産業のサプライヤが主体となり、SBOM の原則と機能に関する理解を深める目的で実施されている。PoC の目的は以下のとおり。

- 自動車産業における SBOM の定義の構築
- NTIA の SBOM プロジェクトに加え、エネルギーや他の産業との連携強化
- 自動車産業のサプライヤの総意としての SBOM 導入促進
- サプライヤに加え、顧客や関連事業を含むサプライチェーン全体にとって適切なサイバーセキュリティのアプローチの検討
- 短期から中期的にサプライヤの SBOM 導入を促進

[33] https://www.ntia.doc.gov/files/ntia/publications/ntia-sbom-adoption_2021-01-13.pdf

PoC では自動車メーカーがサプライヤに提出を求める情報の規格統一に向けたソリューションとしてのSBOM の有効性を検証する。PoC はタイムラインやリソース配分を決定するプランニングのフェーズが進行しており、今後約 1 年をかけて PoC の実施とレビューを行い、PoC の成果物として自動車メーカーに提供する情報の規格統一に向けたサプライヤからの提言をまとめた報告書の作成を予定している。

自動車産業のほか、サービス産業においても SBOM 導入の試みが進行している。ソフトウェアライセンス・メンテナンス契約（Software License and Maintenance Agreement: SLMA）に SBOM の規定を盛り込むことで、バイヤー側のセキュリティリスクの軽減に貢献することが可能となる。小規模のソフトウェアベンダにおいてもクオリティの高い SBOM を作成可能であることが実証されている。

4）Healthcare Proof of Concept WG

ヘルスケア PoC WG は現在進行中の PoC 2.0 イテレーション 2 の報告を行った。前回のイテレーション 1 がサプライヤないしその他のステークホルダによる SBOM 作成のユースケース実施を目的としていたのに対して、現在のイテレーション 2 は purl の識別子を使用した共通コンポーネントのリストアップ、PoC の対象となったソフトウェアの全コンポーネント網羅、および PoC で作成された SBOM のリスト作成に取り組んでいる。

将来のイテレーション 3 においては、以下の点に焦点を置いて PoC を実施する予定である。

- フレーミング WG が取り組む脆弱性（VEX）への対応の検証
- Purl または CPE [34]の 2 通りの識別子の利用
- コンポーネント・ハッシュ（Component hash）を使用したコンポーネントのベースライン構築
- 医療機器メーカーによる SBOM コンポーネントのインプットと利用の検証

ヘルスケア PoC WG では以下のドキュメントを公開している。

- 医療機関向け PoC クイックスタートガイド
- SBOM や関連ツールのサンプル事例集
- PoC コンポーネントのマスターリスト

Splunk のような有料の SBOM の作成ツールに関しては、病院の規模によっては SBOM 作成ツールを使用するための予算が確保できない懸念が議論されている。これに対して、PoC においてはオープンソースツールを利用した SBOM の作成と使用の方法を模索している。

ヘルスケア PoC に参加している New York Presbyterian 病院からの報告によれば、既に院内で SBOM インプットのツールを構築しており、2021 年 2 月中旬には院内の SBOM 利用の報告が可能となる。

---

[34] https://nvd.nist.gov/products/cpe

(3) SBOM 関連プロジェクトや製品のデモンストレーション

SBOM “Show and Tell”という題目で、以下の 6 プロジェクトの紹介とデモンストレーションが行われた。

- SPDX Online Tools

SBOM の作成、他フォーマットへの変換を可能とするオンラインツールを提供。Source Auditor 社が開発。

- Dependency Track

SBOM を使用して調達や M&A 等の経路で入手したソフトウェアコンポーネントの相関を分析、脆弱性の特定が可能。ソフトウェアのコンポーネントに脆弱性が存在する場合には迅速に検出することが可能となっている。OWASP（Open Web Application Security Project）が開発。

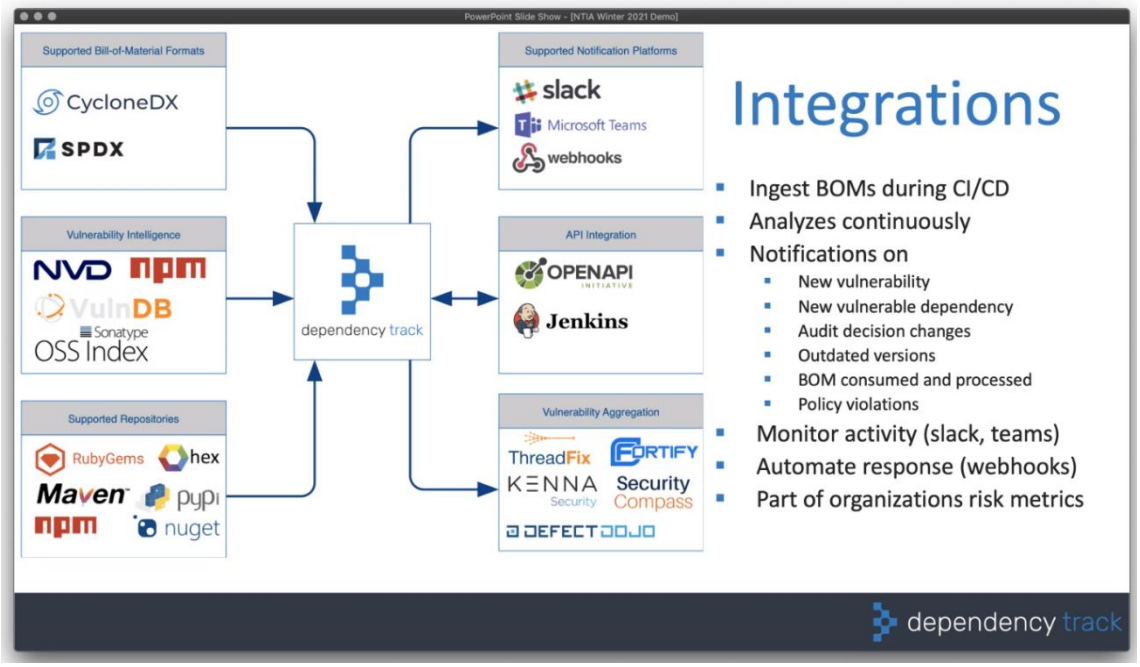


図 12 Dependency Track の動作イメージ（出典：プレゼン資料）

- SBOM PoC for Risk Assessments in Healthcare

SPDX フォーマットを利用して、サードパーティリスクマネジメントの自動化のためのソリューションを提供。ヘルスケア PoC において Ceders Sinai 病院がこのツールを用いて、SBOM を院内のシステムに取り込むとともに脆弱性のマッピングを行った。他方、コンポーネントのネーミング問題がツールの有効性を阻む障害となっている点も報告されている。Censinet 社が開発。

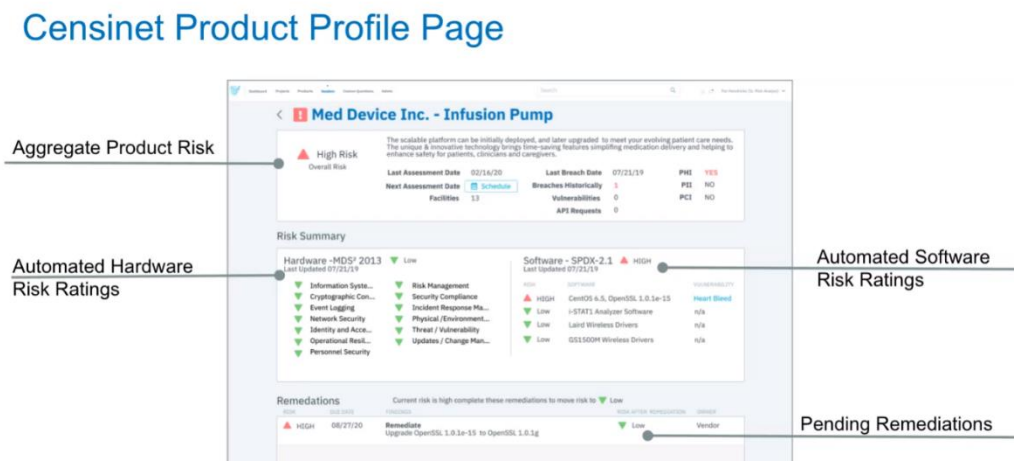


図 13 Censinet の脆弱性評価のサンプル（出典：プレゼン資料）

- Digital Bill of Materials (DBoM)

アテステーション機能の自動化によるコスト削減。エネルギー産業の PoC を実施したほか、ブロックチェーンを活用した PoC に取り組んでいる。Unisys 社が開発。

- InSight Platform

SBOM の作成、管理、共有のワークフローを支援するソリューションを提供。セキュリティを確保したクラウド環境に SBOM をアップロードすることで、SBOM の作成者とユーザーの双方が利用可能なプラットフォームを構築している。ワークフローの自動化によりマニュアルプロセスと比較して約 10 倍の処理速度の向上に貢献するとともに、脆弱性（VEX）の回避も可能としている。Vigilant Ops 社が開発。

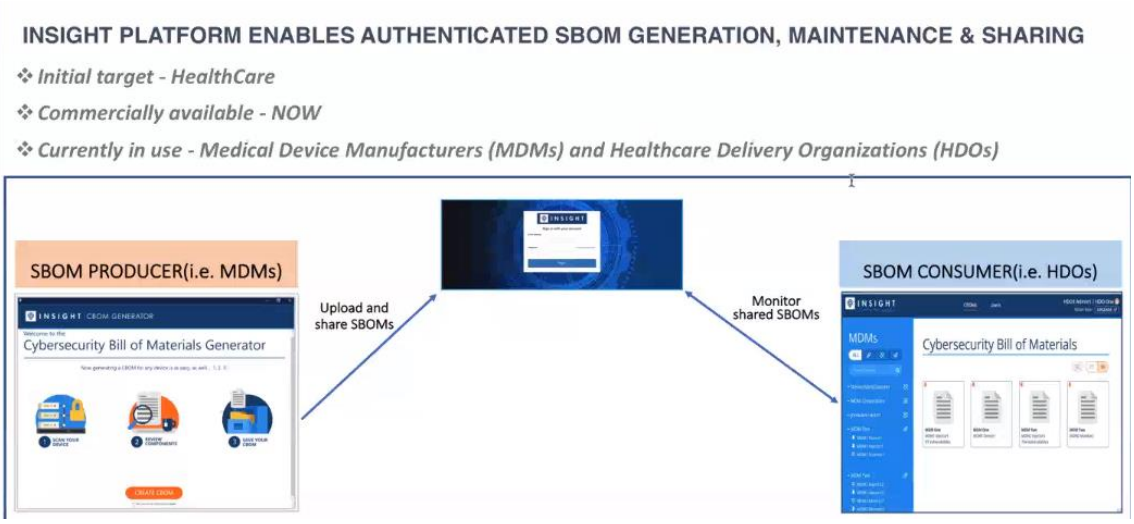


図 14 InSight Platform の概観

- Framework for Analysis and Coordinated Trust (FACT)

SBOM の作成と活用をサポートするソリューションプラットフォーム。ソースコードが入手不可能な場合を想定して、バイナリコードから SBOM の作成が可能となっている。また、ネーミング問題への対処のために AI ツールを導入してネーミングの最適化を行っている。aDolus Technology 社と OSIsoft 社が共同開発。

(4) ステークホルダディスカッション

SBOM 関連プロジェクトや製品のデモンストレーションにおいては、コンポーネントのネーミングが障害となっていることを報告したプロジェクトが多く、依然としてネーミング問題が SBOM の最大の課題となっていることが明らかになった。これに対して Allan Friedman 氏は、フレーミング WG が作成したネーミング問題への対処のガイドラインを参照し、実践から得られたフィードバックをフレーミング文書に反映することを提案した。

参加者からヘルスケア PoC 実施にかかる費用について質問があり、既存のオートメーションプロセスに SBOM を組み込む際に導入コスト（one time cost）がかかるが、SBOM の作成と使用が自動化されればその後の費用はかからず、脆弱性管理のコストのみとなる旨回答があった。ただし、他のステークホルダからの回答では、SBOM の使用と SBOM を用いた分析に関して費用がかかる点が指摘された。さらに、ライセンスやコンポーネントの名称が正確に把握できない低クオリティのソフトウェアに対しては、SBOM を活用したコンポーネントのマッピングの精度も低下することとなる。

本プロジェクトの今後の方向性としては、サイバーセキュリティの新たな脅威に対する SBOM の活用方法の模索、脆弱性のインパクト分析等が挙げられる。1 月 26 日にエネルギーPoC のキックオフウェビナーの開催を予定している。

2.3.5. エネルギーPoC に関するミーティング

(1) サマリ

2021 年 1 月 26 日に開催された。

1) エネルギー産業における SBOM のユースケース提案

サプライチェーンのサイバーセキュリティの専門家である Tom Alrich 氏から、エネルギー産業における SBOM のユースケースについて発表があった。エネルギー産業への SBOM 導入においては脆弱性管理、調達、Ripple20 シンドローム35 の視点が重要と考えられるが、実際に PoC（Proof of Concept）が開始されれば、どのユースケースに焦点を置くかは PoC 参加者の判断に委ねられることとなる。

脆弱性管理に関しては、国家脆弱性データベース（National Vulnerability Database: NVD）等を利用してソフトウェアパッケージを管理するのが一般的とされているが、エネルギー産業においてソフトウェアコンポーネントのレベルで脆弱性管理を行っている事例は極めて少ない。SBOM を使用することで、エネルギー産業に関与するソフトウェアのサプライヤおよびユーザーとなる電力会社はコンポーネントの脆弱性を追跡することが可能となる。電力会社はソフトウェアの調達に際して、サプライヤに SBOM の作成を求めることでコンポーネントの脆弱性を把握することができる。

エネルギーのように政府の規制が強力な産業では、SBOM に関する規制を設置するトップダウン式の SBOM 導入が想定されるかもしれない。しかしながら、このような規制が先行する SBOM 導入は NTIA の試みと相反するものとなる。エネルギー産業の PoC においても、既に実施されているヘルスケアや自動車産業の PoC と同様に、産業が主体となるボトムアップ式の SBOM 導入を推奨する。

2) ヘルスケア PoC からのフィードバック

Siemens Healthineers Technology で医療機器サイバーセキュリティのチームリーダーを務める Jim Jacobson 氏より、ヘルスケア PoC の進捗について報告があった。2019 年に実施されたヘルスケア PoC の第 1 弾においては、病院が医療機器メーカーから医療機器を調達する際、ソフトウェアコンポーネントの

[35] Ripple20 はハッキング可能な 19 個の欠陥からなる脆弱性群であり、もし悪用に成功した場合、攻撃者が接続可能な脆弱な機器上で任意のコードを実行可能になるとみられています。攻撃者は、ローカルネットワークまたはインターネットを介して脆弱な機器にアクセスし、それらを完全に制御しようとする可能性があります。（https://blog.trendmicro.co.jp/archives/25346#:~:text=%E5%85%B7%E4%BD%93%E7%9A%84%E3%81%AB%E3%80%81Ripple20%E3%81%AF,%E3%81%99%E3%82%8B%E5%8F%AF%E8%83%BD%E6%80%A7%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82）

SBOM の作成を依頼してリスクマネジメントに活用するユースケースが実施された。このヘルスケア PoC 第 1 弾により、SBOM がソフトウェアコンポーネント情報の透明性を向上してリスクマネジメントに有効であることを証明するとともに、ヘルスケア産業に限定されない SBOM の活用の可能性が示された。

2020 年より実施されているヘルスケア PoC 第 2 弾においては、PoC の参加者を医療機器メーカー、病院に加えてソフトウェアサプライヤに拡大してより広域且つ機動的な SBOM の作成と利用に関するユースケースを実施している。さらに、ヘルスケア PoC で得られた知見をまとめた SBOM ルールブックや PoC クイックスタートガイドの作成を行っている。

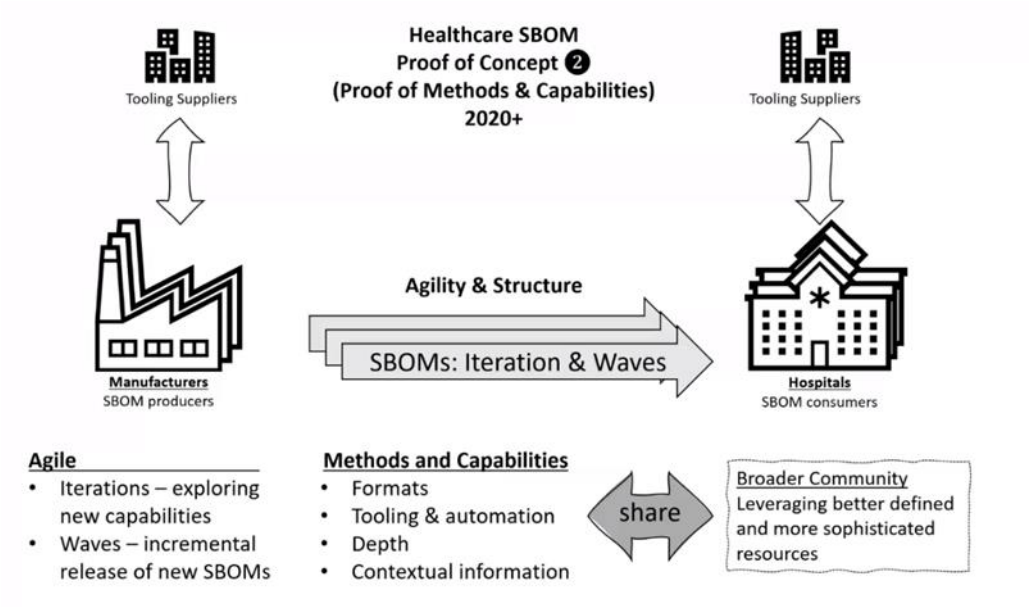


図 15 ヘルスケア PoC 第 2 弾の概要（出典：会合プレゼンテーション資料）

3) 自動車 PoC からのフィードバック

Hitachi America でエンジニアリングのシニアバイスプレジデントを務める Charlie Hart 氏より、自動車 PoC の進捗について報告があった。自動車産業の情報共有分析センター（Auto-ISAC）が主催となり、ヘルスケア PoC 第 1 弾を自動車産業に模倣する形で、自動車産業におけるソフトウェアアセットマネジメントとインベントリ作成の PoC を実施している。

自動車産業における SBOM 導入はサプライヤ主導のプロジェクトで、SBOM の原理を理解してソフトウェア管理のオペレーションに取り入れることを目的とする。自動車産業における SBOM 導入の要請をサプライヤ側からの総意と位置付け、サプライヤの自主的な SBOM 導入を促して産業スタンダードの構築を目指す。さらに、自動車産業に限らず NTIA や米食品医薬品局（FDA）を含む他の産業のステークホルダの関与も促している。

現在までに、NTIA のヘルスケア MSP（Managed Service Provider）リーダーによる PoC チュートリアルを完了しており、目下 PoC のタイムライン、リソース提供、コンポーネント事例、メトリクス、フォーマットその

他に関するプランニングを進めている。今後 PoC の実施を経て、産業スタンダード構築に向けた提案を盛り込んだ報告書の作成を予定している。

2.4. 関係者インタビュー

NTIA Software Component Transparency に参加するフリードマン博士（Allan Friedman, PhD, Director, Cybersecurity Initiatives, NTIA）にインタビューを行った。

なお、日本からの NTIA の Software Component Transparency 参加者（1 名）に対しても、これまでの参加、現在の活動内容、今後の注目すべき点等についてインタビューを行った。

フリードマン博士のインタビュー概要は以下のとおりである

2.4.1. インタビュー概要（Allan Friedman 博士）

(1) 外部リソースの活用

- NTIA は SBOM プロジェクトにおいて外部からのコンサルティングを利用していない。しかしながら、SBOM プロジェクトの初期のおいては、NTIA は SBOM の有効性の説明とワーキンググループへの勧誘のために多くの 1 対 1 のアウトリーチを実施した。このアウトリーチの過程においても尚、外部コンサルタントとのコネクションは構築できなかった。
- ヘルスケア SBOM の場合、食品医薬品局（FDA）は規制の一環として医療機器メーカーに SBOM の作成を要請し、同時にメーカーに NTIA の取り組みに協力することを求めた。FDA はヘルスケア産業が初の SBOM を作成した産業となったことに満足しているという。
- NTIA はこの他の産業セクターにも積極的に SBOM のアウトリーチを展開している。
  - ✧ 自動車：NTIA は Auto ISAC[36] との協力体制を構築
  - ✧ 金融：NTIA は複数の大企業と協力体制を構築
  - ✧ 主要インフラ（例：エネルギー）
- オープンソースコミュニティや OSS サービスを提供する大手ソフトウェアベンダは SBOM に関する情報を提供する重要な情報源となっている。これらの団体は、知財の関係からソフトウェアサプライチェーンにおけるコンポーネントを把握しなければならない。既に多くの OSS コミュニティのメンバーが NTIA の SBOM プロジェクトに参加している。
- 米国のその他の政府機関は、SBOM は NTIA の管轄下にあると判断して積極的に関与していない。例えば、国土安全保障省（DHS）のサプライチェーンリスクマネジメントタスクフォース（SCRM[37]）は SBOM プロジェクトへの参加を検討していたが、NTIA がプロジェクトに取り組んでいるため参加は不要と判断した。

[36] https://www.automotiveisac.com/

[37] https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force

(2) ヘルスケア PoC の予算

- この点に関しては目下活発な議論が行われている。SBOM には以下のように 2 通りの考え方がある。
  - ✧ ある団体がソフトウェアのコンパイルを自前で行っている場合、SBOM の作成は非常にシンプルとなる。コンパイルの過程において、SBOM に必要な情報は得られる形となる。（例：software dependencies graph）
  - ✧ 他方、SBOM の作成には団体の組織内部での調整が必要となり、この点が SBOM 作成の際の最大の課題となっている。このため、NTIA は SBOM にかかる非技術的な費用（non-technical costs）の特定を試みている。NTIA のワーキンググループは、SBOM 作成を補助するツールに関する情報収集を行っており、現在までにオープンソースや有料の商用ツールが多く見つかっている。
- 単一の団体であっても組織内部でソフトウェアの同一コンポーネントに異なる名称を使用している場合があり、大規模組織であればより一層複雑な調整が必要となる。このため、各 SBOM に発生する技術的課題が類似のものであったとしても、組織内部のソフトウェア管理の統一にかかるコストは未知数となる。NTIA はヘルスケア SBOM において、このような課題の分析に取り組んでいる。

(3) ヘルスケア PoC の今後

- COVID-19 の渦中においても、New York Presbyterian 病院における作業は継続している。ヘルスケア SBOM は PoC フェーズ 1 を完了しており、コンセプトのフィージビリティが示された。現在は PoC フェーズ 2 が進行しており、メカニズムの解析に取り組んでいる。SBOM の PoC にタイムフレームは設定されていないが、第 1 フェーズで「基本的要素」（basic stuff）を確認し、第 2 フェーズで SBOM データの生成と利用に関してより詳細な（advanced）検証を行う 2 段構成が組まれている。
- タイムフレームの詳細に関して、後程メールでフォローアップをお送りする。PoC フェーズ 1 の実施に要したのは 1 か月間のみだが、これ以前のプランニングには法的問題（legal issues）のために多くの時間がかかった。現在では関係者全員が NDA に署名したことから、この点は PoC フェーズ 2 では改善された。フェーズ 2 は現在セットアップの段階だが、開始されれば速やかに履行されるだろう。

(4) SBOM について日本への助言

- 日本政府はスクラッチからソフトウェアサイバーセキュリティプロジェクトを立ち上げる必要はなく、そのニーズに合った国際コミュニティのリソースを活用すれば良い。
- 経済産業省には NTIA の SBOM グループへの参加をお勧めしたい。JP CERT は NTIA の Software Component Transparency に積極的に参加している。

- 経済産業省が日本で SBOM の PoC を実施する場合、NTIA は喜んで協力する。

(5) SBOM 活用の事例

- NTIA は SBOM 利活用事例の特定に取り組んでいる。既に多くの団体が SBOM の導入に関心を示している。例えば、OSS コミュニティにおいて複数の Linux ディストリビューションが SBOM の利用を奨励している。しかしながら、現在のところヘルスケア PoC に匹敵するレベルの SBOM 利用事例は存在しない。ヘルスケア PoC はデバイスのメーカーやユーザーを巻き込んで実施しており、これほどの規模の PoC を他のセクターで実施するにはより精密なプランニングが必要となる。
- COVID-19 危機は NTIA のプロジェクトには思うほど影響しておらず、多くの団体はリモートで活動を継続している。サプライチェーンの不確実性への対処において SBOM がもたらす利益は明白であり、サプライチェーンのセキュリティ確保の促進において SBOM は必要不可欠な（critical）存在となるだろう。

3. 企業や業界団体、公的機関、OSS コミュニティにおけるソフトウェア管理の取り組み

3.1. 企業における取り組み、動向

主に海外企業におけるソフトウェア管理の取り組み、動向等を取りまとめた。

3.1.1. Synopsys

Synopsys 社より発表された「2020 年オープンソース・セキュリティ&リスク分析レポート」は、世界中のエンタープライズ企業、医療、金融、通信インフラ等の 17 業種、1,250 を超える商用のコードベースに含まれる OSS を監査した結果から得られた OSS の利用状況とリスクの現状と分析をまとめたレポートである。OSS にまつわる下記の項目について記載されている[38]。

- ソフトウェア部品表（BOM）の必要性
- 2019 年に監査されたコードベースのオープンソース構成
- パッチ未適用のオープンソース脆弱性の脅威
- 監査で発見された脆弱性
- 脆弱性へのパッチ適用優先度を設定する
- オープンソース・コンポーネントにおけるライセンスのリスクを精査する
- オープンソース利用における運用面のリスク要因

また、レポートから明らかになったオープンソース・リスク・トレンドの中で注目すべき主な点は、下記のとおりである[39]。

- オープンソースの活用増加は継続

コードベースの 99%には何らかの形でオープンソースコードが使用されており、1 つのコードベースあたりで平均 445 個のオープンソースが組み込まれている。2018 年の 298 個から大幅に増加している。調査対象となったコードの 70%はオープンソースと認定され、2018 年調査の 60%から増えている。2015 年の 36%

[38] https://www.synopsys.com/ja-jp/software-integrity/resources/reports/2020-open-source-security-risk-analysis.html

[39] https://www.synopsys.com/ja-jp/japan/press-releases/2020-05-28.html

からは約倍増している。

- 時代遅れもしくは放置状態のオープンソース・コンポーネントが蔓延

コードベースの 91%には、開発から 4 年以上が経過した時代遅れのオープンソース・コンポーネントや、過去 2 年間開発活動実績がなかったコンポーネントが組み込まれている。時代遅れのオープンソース・コンポーネントを使用するリスクは、セキュリティ脆弱性が内在する可能性を高めるだけではなく、そうしたコンポーネントをアップデートすることによって、不要な機能の搭載や、ソフトウェア互換性の問題を引き起こすことになりかねない。

- 脆弱性が内在するオープンソースの使用率が再び上昇

脆弱性が潜んでいるオープンソース・コンポーネントを使用しているコードベースは、2017 年から 2018 年にかけて 78%から 60%に低下していたが、2019 年には 75%にまで増加している。同様に、高リスクな脆弱性に晒されているコードベースは、2018 年の 40%から 2019 年には 49%へと急増している。幸いにも、Heartbleed バグや 2017 年に Equifax 社の情報流出事件を引き起こした Apache Struts の脆弱性の被害を受けたコードベースは、2019 年時点では報告されていない。

- 知的財産を危険に晒すオープンソースライセンス違反の可能性が存続

コードベースの 67%は、何らかの形でオープンソースライセンス条件の競合を起こしており、33%にはライセンス関係が特定できないオープンソース・コンポーネントが使用されていた。こうしたライセンス条件の競合の状況は、業界によって大きくばらつきがある。最も割合が高いのは「インターネット/モバイルアプリ」の 93%で、最も低いのは「仮想現実、ゲーム、エンターテイメント、メディア業界」の 59%となっている。

3.1.2. GE Digital

GE Digital は、Predix Platform[40]のセキュリティレビューのガイドラインを公開している[41]。そのなかに、OSS の脆弱性評価もあげ、以下の手順を示している。

- プロダクトのコードをもとに利用しているオープンソースを特定
- 特定されたオープンソースに関する既知の脆弱性問題をマッピング
- オープンソースの未解決な脆弱性問題の善後策を講ずるよう推奨

[40] デジタルツインや IoT など製造業向けのソリューションから成るプラットフォームで、クラウドやエッジコンピューティングもサポートしている。https://www.ge.com/digital/iiot-platform

[41] https://www.ge.com/digital/documentation/predix-platforms/IMmYwZmZmMzItN2MzNi00OTYyLWIwOTQtZmMzZDE4MzA4Yjg4.html

また、GE Digital として推奨するわけではないと述べたうえで、オープンソースソフトウェアに向けて対策がなされている静的アプリケーションセキュリティテスト（Static Application Security Testing：SAST）プロダクトとして以下を挙げている。

- WhiteSource[42]

ユーザーとして、Microsoft、International Game Technology（IGT）、Northern Safety & Industrial などの名が挙げられている[43]。

- Checkmarx SAST[44]

オープンソースソフトウェアに特化したプロダクトは、Checkmarx Open Source Analysis (CxOSA)[45][46]

その特徴としては、①コードをもとに OSS の脆弱性を検知、②CI/CD pipeline に組み込むことにより、OSS を自動的に特定、③システム開発ライフサイクルを通したオープンソースポリシーの徹底、④詳細な脆弱性情報とリスク緩和策の提示、などが挙げられている。

- Veracode Static Analysis[47]

OSSに特化したプロダクトとしては、Veracode SCA（Veracode Software Composition Analysis）がある。Pipeline や IDE に組み込むことにより、即時にリスクを知ることができる点、National Vulnerability Database（NVD）よりも幅広い脆弱性問題のデータベースを有する点などを特徴としている[48]。

- Synopsys[49]

OSS 向けのプロダクトとして、Black Duck が挙げられる[50]。

---

[42] オープンソースに特化したソリューション。プロダクトラインとしては、Open Source Security、Open Source License Compliance、Open Source Due Diligence、Open Source Inventory (BOM)がある。
http://www.whitesourcesoftware.com/

[43] https://www.whitesourcesoftware.com/whitesource-pricing/

[44] https://www.checkmarx.com/products/static-application-security-testing

[45] https://www.checkmarx.com/products/open-source-analysis

[46] https://info.checkmarx.com/hubfs/Datasheets/CR-112%20Update%20OSA%20Datasheet%20-%20Web.pdf

[47] http://www.veracode.com/products/binary-static-analysis-sast

[48] https://www.veracode.com/products/software-composition-analysis

[49] https://www.synopsys.com/software-integrity/security-testing.html

[50] https://www.synopsys.com/software-integrity/security-testing/software-composition-analysis.html

3.1.3. Amazon

Amazon Web Services（AWS）はオープンソースコミュニティに参加しており、オープンソースコードの提供や外部組織とのコラボレーションに積極的に参加している。AWS は EC2 における多くのオープンソースオペレーティングシステムを使用する顧客を支援するとともに、MySQL、PostgreSQL、Redis といったオープンソースデータベースのための管理サービスを提供して、顧客のソフトウェア開発の支援を行う。さらに、AWS はオープンソース団体のスポンサーシップ、イベント開催、オープンソースプロジェクトへのコード貢献、自社製コードのオープンソース化を通してオープンソースコミュニティに貢献している。

AWS は以下のオープンソース団体に所属している[51]。

- Academy Software Foundation, Platinum Board Members
- Alliance for Open Media, Member
- Apache Software Foundation, Platinum Sponsor
- Automotive Grade Linux, Silver Member
- Cloud Information Model, Founding Member
- Cloud Native Computing Foundation, Platinum Member
- Core Infrastructure Initiative, Founding Member
- DENT, Founding Member
- GraphQL Foundation, Founding Member
- IDPro, Board Member
- Java Community Process, Member
- Linux Foundation, Silver Member
- .NET Foundation, Corporate Sponsor
- NumFOCUS, Platinum Sponsor
- Open Container Initiative, Founding Member
- Open MPI, Member
- Open Network User Group (ONUG), Member

[51] https://aws.amazon.com/jp/opensource/?opensource-all.sort-by=item.additionalFields.startDate&opensource-all.sort-order=asc

- Open Source Initiative, Sponsoring Member
- Open Souce Robotics Foundation, Sponsoring Member
- Open Subsurface Data Universe, Member
- Python Software Foundation
- ToDo Group, Member
- W3C
- Xen at Linux Foundation, Founding Advisory Member

AWS はオープンソースプロジェクトのためのプロモーション・クレジット（AWS promotional credits, 販促クレジット）を実施している。クレジットとは、オープンソースプロジェクトへの貢献に対する報酬を与える手法の一つである。Amazon のプロモーション・クレジットは AWS クラウドやそれに付随するサービスの料金の支払いに利用可能とされる。例えば、AWS Activate のサービスは AWS を導入した企業に最大 10 万ドル相当の AWS プロモーション・クレジット、テクニカルサポート、トレーニングなどの特典を提供しており、パフォーマンスの最適化、リスク管理、コスト管理を行いながら AWS を活用したビジネスの成長を支援する[52]。この他、Amazon の AI である Alexa のスキル開発に貢献したソフトウェアエンジニアには報酬として 100 ドル相当のクレジットが贈られる[53]。

AWS のプロモーション・クレジットは AWS のパフォーマンス試験、CI/CD（continuous integration/continuous delivery）、ストレージに使用されており、AWS はクレジットプログラムによるオープンソースコミュニティの発展を目指している。

AWS プロモーション・クレジットに参加するためには、AWS アカウントの開設が必要となる。クレジットを申し込む OSS プロジェクトは基本的に OSI 認証を受けたライセンスを取得していなければならない。ソフトウェア開発者はクレジット申請フォームに個人情報に加えてクレジットの用途について記入する。提出された申請フォームは Amazon Leadership Principles に基づいて 10-15 営業日以内に審査が行われる。AWS クレジットが利用可能なサービスは以下のとおり[54]。

- Amazon Comprehend
- Amazon Connect
- AWS DataSync
- Amazon DynamoDB

[52] https://aws.amazon.com/jp/activate/

[53] https://medium.com/@jaychapel/9-ways-to-get-aws-credits-9a85e0f452a1

[54] https://aws.amazon.com/jp/blogs/opensource/aws-promotional-credits-open-source-projects/

- Amazon Elastic Book Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon Forecast
- Amazon FSx
- Amazon Simple Storage Service Glacier
- AWS Global Accelerator
- Amazon GuardDuty
- Amazon Inspector
- Amazon Lex
- Elastic Load Balancing
- Amazon Macie
- AWS Storage Gateway
- Amazon Neptune
- Amazon Personalize
- Amazon Pollu
- Amazon Relational Database Service (Amazon RDS)
- Amazon Redshift
- Amazon Rekognition
- AWS RoboMaker
- Amazon Simple Storage Service (Amazon S3)
- Amazon SageMaker
- AWS Security Hub
- AWS Shield
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

- Other[55]

3.1.4. Verizon

Verizon のオープンソースデベロッパーガイド（Verizon Media Open Source Developer Guide）には Verizon Media において作成、使用、展開されるすべてのオープンソース関連情報が記載されている。Verizon Media Open Source Program Office（OSPO）はオープンソースに関連するデベロッパーのニーズに応えるサービスを提供しており、ガイドブックにはこれらのサービスに関する情報を網羅している。Verizon のスタッフはイントラネットの OSPO ウェルカムページから OSPO チームにメールでコンタクトを取ることができる。Verizon は社内の OSS ガイドブックに編集を加えた版を公開しており、他社の OSS ポリシーの参考や他社からフィードバックを得ることを目的としている。ガイドブックは以下の章から構成される[56]。

1. 使用（Using）：プラットフォーム、製品、サービスにおけるオープンソースコードの使用。
2. 貢献（Contributing）：既存のオープンソースプロジェクトへの貢献。
3. 公開（Publishing）：新規オープンソースプロジェクトの公開。
4. 発売（Launching）：オープンソースコードまたはバイナリを含む製品の発売。
5. プロモーション（Promoting）：OSPO によるオープンソースプロジェクト支援
6. 受入（Accepting）：コミュニティからのコード受け入れ。
7. リソース（Resources）：ガイドブックのリソースと追加情報。

1）オープンソースコードの使用

オープンソースコードは誰でも利用可能とされており、ソフトウェアエンジニアが課題に直面した際には新たにソリューションを構築するよりも既存のオープンソースコードを使用して解決することが推奨される。オープンソースコードを使用する際にはプログラムのアーキテクトとテックカウンシルに判断を仰がなければならない。ライセンスに関する質問に関しては Verizon Media の OSPO が支援を提供する。

ライセンスはオープンソースコードの複製と使用に関する許可について取り決めている。多数のライセンスが存在するが、他者にコードの使用を認めるという点で共通している。ライセンスの差異は他者がコードを使用する際に負う義務に起因する。コードにライセンスが見当たらない場合、コードを使用する権利はないとみなされる。ライセンスを持たないコードの使用を希望する場合は、コード作成者に問い合わせること。Verizon はライセンスを以下の 3 類型に大別している。

[55] https://pages.awscloud.com/AWS-Credits-for-Open-Source-Projects

[56] https://verizonmedia.github.io/oss-guide/

- 許可型オープンソースライセンス

許可型ライセンスは必要最低限の義務を課し、これらの遵守は比較的容易である。MIT、BSD、Apache 等は許可型ライセンスを使用している。詳細は異なるが、zLib、ISC、JSON 等も許可型ライセンスに分類される。モバイルアプリやバイナリプロダクトに許可型ライセンスのコードを使用する場合、Verizon ではプロダクト発売ガイドラインに則って発売前にクレジットの一覧を作成する。

- 制限型オープンソースライセンス

制限型ライセンスのコードを使用するには特定の条件を満たさなければならない。コードの使用方法によっては当コードの使用を断念すべき場合もある。GPLv2、GPLv3、LGPLv2.1、LGPLv3 等のフリーソフトウェアライセンスの使用には外部にコードを入手可能とすることという条件が課せられる。Verizon は制限型ライセンスのコードは利用可能としているが、市販のモバイルアプリやバイナリプロダクトにこれらのコードを含めることは避けている。例外的にハードウェアに組み込むコードには制限型ライセンスの使用を認める場合がある。

- ソース入手可能ライセンス

ライセンスはコードの使用を認めているが、ライセンスが課す要件がオープンソースイニシアティブ（Open Source Initiative: OSI）に合致していない、もしくは OSI のレビューを受けていない。これらのライセンスは往々にして問題にはならないが、制限が課せられており注意を要する場合もある。厳密にいえば、OSI に準拠しないライセンスはオープンソースとは見なされない。Verizon ではこのようなコードの使用に際しては事前に OSPO の助言を仰ぐことを求めている[57]。

2）オープンソースプロジェクトへの貢献

Verizon Media ではエンジニアのオープンソースプロジェクトへの貢献を奨励している。オープンソースコードにバグや改善点を発見した際には、Verizon はエンジニアに介入を認めている。しかしながら、状況によってはエンジニアの活動にブロックをかける場合がある。以下の条件を満たすのであればエンジニアは自由にオープンソースプロジェクトへの貢献を行えるが、質問がある場合には OSPO に問い合わせること。

- ステップ 1：貢献ファイル

オープンソースプロジェクトによっては、当プロジェクトが求める貢献について記載した Contributing.md ファイルを設置している。一読の上、プロジェクトのニーズを理解すること。

- ステップ 2：CLA

プロジェクトによっては貢献を行う前にライセンス合意（Contributors License Agreement: CLA）への署名を求められる場合がある。これを求められた場合には OSPO の承認を得ること。多くの場合 CLA への署名に問題はないが、内容によっては OSPO が CLA の署名にストップをかける場合がある。

[57] https://verizonmedia.github.io/oss-guide/docs/using/using.html

- ステップ 3：特定のプロジェクト

Verizon ではコーポレート CLA リストにより記録を管理している。プロジェクトのリストを確認の上、必要に応じて CLA リストの更新を行うこと。

- ステップ 4：貢献のレビュー

貢献の権利が認められているプロジェクトにのみコードを提供すること。占有情報を含むコードを提供してはならない。サブコードを提供してはならない。多くの場合オープンソースプロジェクトへのコード提供は問題にならないが、懸念が生じた際にはイントラネットの JIRA チケットを開いて OSPO に相談すること。

- ステップ 5：プロジェクトのレビュー

オープンソースプロジェクトが多くの未回答の事項や未着手のリクエストがある場合、デッドプロジェクトとみなされ、当プロジェクトへの貢献は意味をなさない。このようなプロジェクトからは撤退するか、Verizon が引き取って自社のプロジェクトとする場合があるため、OSPO に相談すること[58]。

3) 新規オープンソースプロジェクトの公開

オープンソースプロジェクトは公開（Publish）することで開始される。公開するプロジェクトを維持するために、デベロッパーのリソースを確保すること。プロジェクトの公開、維持、コミュニティ対応、セキュリティアラート修復の準備ができていないのであれば、当プロジェクトは公開できない。Verizon はデッドプロジェクトを公開したくはないので、長期的なプロジェクト管理を心得なければならない。プロジェクトの公開前には、既存のオープンソースプロジェクトから流用できる部分がないか確認すること。新規プロジェクトの立ち上げよりも既存のプロジェクトへの貢献の方が効率的な場合があるため、オープンソースコミュニティのニーズを見極めること。

- ステップ 1：リクエストの用意

プロジェクト名称の提案。Verizon Media が作成した各ソースコードの上部にコピーライトを記載。Verizon のリポジトリスタンダードに則って公開のためのリポジトリを準備。社内の GitHub Enterprise 上でオープンソースブランチを作成する。プロジェクトにアクセスが必要な社内スタッフのリストを作成し、イントラネットの OSPO ページで JIRA チケットを作成して OSPO のレビューを仰ぐ。

- ステップ 2：承認

OSPO からオープンソースプロジェクトの承認を得る。プロジェクトによっては OSPO 以外の他の部門から事前に承認を得る必要がある。プロジェクトに新規パテントの可能性が含まれる場合、イントラネットを通じてパテント申請を行う。データセットの公開には Verizon のグローバルプライバシーポリシーに則った許可の取得が必要となる。

- ステップ 3：公開

[58] https://verizonmedia.github.io/oss-guide/docs/contributing/contributing.html

Verizon はオープンソースプロジェクトのための外部リポジトリを設置。プロジェクト担当者はブログ、ポッドキャスト、プレゼンテーションを含む外部コミュニケーションチャネルを通じてプロジェクトを宣伝するためのコミュニケーションプランを作成する。コミュニケーションプランに則って外部からプロジェクトへの貢献を募る[59]。

4）モバイルアプリの発売

Verizon Media が発売するモバイルアプリにはオープンソースライセンスに関連するサードパーティの情報が必ず含まれている。Verizon ではアプリのサービス規約（Terms of Service）、プライバシーポリシーまたは設定のページにおいてこれらの情報を含めている。Verizon ではこれらの情報をクレジット（Credits）と呼ぶが、アプリによっては Notices、Third Party Notices、Open Source Credits と表記されている場合がある。

モバイルアプリの開発チームはビルドシステムからクレジットファイルを入手する。開発チームによっては自力でクレジットファイル作成プロセスを完了するところもあるが、OSPO はクレジットファイルの正確性確保のための支援を提供している。サードパーティアプリを Verizon が発売する場合、ベンダはクレジット情報を提出しなければならない。逆に、Verizon が他の団体の発売用にアプリを提供する場合は、Verizon からクレジットを提供しなければならない。

モバイルアプリのエンジニアチームは開発プロセスで使用した全てのオープンソースソフトウェアを特定する責任を負う。アプリ作成に使用した全てのオープンソースソフトウェアを特定したら、プロダクト法務（product lawyer）と協力して発売の承認を得ること。このプロセスにはサービス規約、プライバシーポリシー、クレジットファイルの作成が含まれる。アプリによっては、追加の規程が求められる場合もある。OSPO はプロセス全般を通してクレジットの正確性の確保を支援する[60]。

5）オープンソースプロジェクトのプロモーション

OSPO はオープンソースプロジェクトのプロモーションのために幅広いサポートを提供している。プロジェクトの戦略的重要性を審査して、戦略的（strategic）、限定的（limited）、ミニマル（minimal）、アーカイブ（archived）の 4 段階のサポートを提供する。各レベルのサポートを受けるためには満たすべき要件があり、人的リソースに制限があることから最高レベル（strategic）のサポートを享受できるプロジェクトは限られる。このため、4 段階の評価は各プロジェクトの価値を評価するものではなく、あくまでリソース配分の優先順位付けのための評価に過ぎない[61]。

[59] https://verizonmedia.github.io/oss-guide/docs/publishing/publish.html
[60] https://verizonmedia.github.io/oss-guide/docs/launching/mobile.html
[61] https://verizonmedia.github.io/oss-guide/docs/promoting/support.html

6）オープンソースプロジェクトへの貢献の受け入れ

オープンソースプロジェクトにおいては外部からの貢献の受け入れは一般的に行われているが、懸念が生じた際には OSPO が解決に向けた支援を提供する。Verizon ではプロジェクトを公開する際、Contributing.md ファイルにおいて外部からどのような貢献を求めているか概要を記載するのが一般的である。

原則として、Verizon のオープンソースプロジェクトはコミュニティから貢献を求める旨を明記しているが、貢献を求めない読み取り専用のプロジェクトも存在する。オープンソースプロジェクトにおいてはコミュニティ参加者からは機能追加や改善に向けた提案がしばしば行われるが、Verizon のオープンソースプロジェクトには規約（Code of Conduct）が含まれ、規約の改変はプロジェクトメンバーにも認められない。規約に関する懸念は OSPO に相談すること。

一般的なオープンソースプロジェクトへの貢献においては CLA（Contributor License Agreement）への署名が求められることがあるが、Verizon では CLA への署名を求めていない。CLA は外部からの貢献者がプルリクエストを求める際にのみ使用されている。というのも、貢献者がコピーライトの所有者の合意なしでコードを提供する際の防御手段として CLA が用いられる場合がある。例えば、ある企業の社員が企業の許可なしでコードを提供する場合など。Verizon はこのような貢献を受け付けない。

OSPO は外部からの貢献の割合を当プロジェクト全体の 10%から 30%とすることを推奨しており、将来的には 50%程度とすることを目指す。この比率について厳格な規定は存在しないが、仮に 100%外部からの貢献で成立したオープンソースプロジェクトがあった場合、Verizon は外部のプロジェクトをホストした形となってしまう[62]。

3.1.5. Joyent

クラウドベースのサービスとソフトウェアを販売する Joyent はオープンソースソフトウェアを使用してビジネスを構築する一方で、使用するオープンソースソフトウェアへの貢献も数多く行ってきた。これはメンテナンスの負担を軽減するなどの業務上の理由に加え、オープンソースは社会的な契約であり、オープンソースの消費者として、自らも貢献を行う責任があるという同社の信念に基づいている。同社は専有ソフトウェアも販売していたが、2014 年に主要システムの SmartDataCenter と Manta[63]をオープンソース化して以降、開発するソフトウェアのほぼすべてをオープンソースとして提供している。この「RFD 164 Open Source Policy」は、同社のオープンソースに関する疑問に答え、方針を明確にするものである。

[62] https://verizonmedia.github.io/oss-guide/docs/accepting/accepting.html

[63] https://www.joyent.com/blog/sdc-and-manta-are-now-open-source

1）オープンソース顧問室（Open Source Counsel Office：OSCO）

オープンソースポリシーに関する相談や承認の窓口として機能する役職。OSCO の責務はオープンソースの原則に準拠しながら企業としてのリスクを軽減することを目標に、両側面のバランスをとることである。さらに法律顧問などの別の相談窓口が必要な場合は OSCO の判断で決定する。専任の役職ではなく、最高技術責任者（CTO）や同等の役職者が兼任するか、他の社員に委任する。

2）オープンソースの使用

以下の一般的なライセンスの下でライセンス適用されたオープンソース・コンポーネントは、別途申告したり OSCO の承認を受けたりする必要はなく、自由に使用できる。

- Mozilla Public License 1.0、1.1、2.0
- MIT License
- Berkeley Software Distribution (BSD) 3 条項、2 条項、0 条項
- Apache License 1.0、1.1、2.0
- Common Development and Distribution License (CDDL)
- PostgreSQL License
- Python Software Foundation License
- パブリックドメイン
- Artistic License
- zlib/libpng License
- PHP License
- ICU License
- Eclipse Public License

以下のライセンスを適用されたコンポーネントは、社内利用（サービスやソフトウェア製品に含めない）目的では自由に使用できるが、社外利用（サービスやソフトウェア製品に含める）する場合は OSCO に相談する必要がある。

- GNU Public License v2、v3
- Lesser GNU Public License

以下のライセンスを適用されたソフトウェアは社内利用目的でのみ使用でき（すなわち、サービスやソフトウ

ェア製品に含めてはならない）、常に OSCO による明示的な許可を必要とする。

- Affero General Public License (AGPL)
- Server Side Public License (SSPL)
- Confluent Community License
- Redis Source Available License
- Commons Clause が追加されたすべてのライセンス

3) オープンソースへの貢献

Joyent は使用するオープンソースプロジェクトに貢献することを信条としており、積極的に変更を上流にプッシュする（共有リポジトリに反映させる）ことを心掛ける。

1. 作成者の属性

Joyent からオープンソースへの貢献には常に、作業を行った 1 人または複数のエンジニアの属性情報を含める必要がある（通常、この属性は git でのコミット実行時に Author フィールドに記録される）。実際の作業者と異なる人物を作成者としてはならない。すべてのエンジニアは互いの作業が適切に評価されていることを確認する責任がある。さらに、変更を上流にプッシュする際は、一般的には最初の作成者であるエンジニアに知らせるべきである。これは礼儀上、また、テストや訂正の情報を伝える際の便宜のためであり、最初の作成者に連絡できない場合に、変更をプッシュしてはならないということではない。

2. 著作権

オープンソースへの貢献の著作権はすべて Joyent に帰属するが、著作権の帰属を表示する方法はプロジェクトの仕様により異なる。

- ファイルベースのコピーレフトライセンス（MPL、CDDL など）の場合：各ファイルに著作権の所有者を記載する。
- その他のライセンスの場合：著作権の表示方法はさまざま。各ファイルに明示されたプロジェクトの貢献者が著作権を持つ場合もある。この場合は、記載する作成者のメールアドレスに所属企業のアドレス（@joyent.com など）を含めることが重要である。

3. 著作権表示

著作権の表示方法はプロジェクトごとに異なり、法律の専門家の見解もさまざまに異なる。Joyent では、変更を加えた各ファイルに「Copyright」という単語、直近の変更を行った年、会社名を含む著作権ヘッダを

含めることが望ましいとしている。

例

```
/*
 * Copyright 2019 Joyent, Inc.
 */
```

既に別の著作権が記載されている場合は、以下のような形で Joyent の著作権を追加する。

```
/*
 * Copyright (c) 2016, 2017 by Delphix. All rights reserved.
 * Copyright 2016 Nexenta Systems, Inc.
 * Copyright 2017 RackTop Systems.
 * Copyright 2019 Joyent, Inc.
 */
```

プロジェクトにより著作権の表示方法（記載する年の範囲、(c)の記号の記載など）が異なっても構わないが、Joyent への著作権の帰属を表示せずに貢献を行うことは、いかなる場合も認められない。

4. サードパーティのソースを貢献する

オープンソースでないサードパーティのースを他のオープンソースプロジェクトに統合したいと場合は、OSCOの協力を得て行う。OSCO は該当のサードパーティがこの行動を許可し、リスクが適切に抑えられていることを確認する。

5. 著作権の更新が不要な変更

以下のような変更は「些細な」変更とみなされ、著作権の再度の表示や更新を必要としない。

- コードの削除のみ
- スペルや文法の修正
- コードのコメントのみの修正

コードの変更に関しては、一般に、どんなに小さな変更であっても「些細な」変更とはみなさない。

6. オープンソースコミュニティでの不適切な行為について

オープンソースプロジェクトへの貢献にあたって、Joyent は従業員が社外の人々とプロフェッショナルな形で関係を築くことを期待しており、オープンソースコミュニティでの行為には社内と同様の職業意識が適用されるべきだと考えている。コミュニティ内の他者が当社の行動規範に違反するような行為をした場合、従業員はこのような行為を OSCO または HR 部門に報告できる。OSCO または HR 部門はその従業員を守ることを優先しながら正しい措置を決定する。

7. 貢献者ライセンス同意書

貢献者ライセンス同意書（CLA）への同意が求められている場合は、OSCO に相談し、許可を得る。

4）オープンソースソフトウェアの開発

Joyent は新規にソフトウェアを開発する場合、そのソフトウェアを積極的にオープンソースとして公開することを方針としている。オープンソース化しない場合でも、常に将来オープンソース化することを念頭にソフトウェアを開発すべきである。そのため、新規ソフトウェアの開発においては原則、以下のガイドラインに従う。

1. リポジトリ

OSCO から明示的な許可を得た場合を除き、新規作成するすべてのリポジトリは GitHub の「joyent」アカウントで作成する（個人アカウントで作成してはならない）。

2. ライセンス

Joyent が開発する新しいソフトウェアには、通常、MPL 2.0 ライセンスを適用する。ただし、別のライセンスが一般的に使用されているエコシステムを利用したソフトウェアには、そのライセンスを使用する。たとえば、node.js を使用した npm モジュールは通常 MIT ライセンスが適用される。MLP 以外のライセンスの仕様に関する OSCO の承認の必要性に関しては、「オープンソースの使用」の項のライセンスに関する記述に従う。

3. セキュリティ

Joyent が作成したリポジトリから情報が漏洩することを防ぐため、プライベートリポジトリであっても、リポジトリ内には、本番環境のキーやパスワードを格納しないこと。また、テストデータとして使用される可能性のある本番データの取り扱いにも注意が必要である。コードレビューは公開で行われるため、コードレビュー時にこうした点を発見しても手遅れとなる。情報漏洩を防ぐ自動的な手順は存在しないため、各自が細心の注意を払う必要がある。

4. 貢献者ライセンス合意書

貢献者ライセンス同意書（CLA）は貢献者の活動の妨げとなるという考えから、Joyent が作成するリポジトリでは CLA は使用していない。

5. 行動規範

Joyent のオープンソースリポジトリの多くは、オープンソースリポジトリに関する行動規範の適用が一般的になる前から存在しているため、当社ではリポジトリに関する正式な行動規範は定めていない。大きな注目を集めるプロジェクトに関しては、正式な行動規範を適用したほうがよい場合がある。その際は OSCO に相談すること。また、Coraline Ada Ehmke 氏が作成した貢献者の行動規範「Contributor Covenant」を基にした行動規範を採用することを推奨する。

3.2. 産業分野、業界団体における取り組み、動向

国内外における産業分野、業界団体におけるソフトウェア管理の取り組み、動向等を取りまとめた。

3.2.1. 一般社団法人 Japan Automotive ISAC

2021 年 2 月、一般社団法人日本自動車工業会に所属する自動車メーカー全 14 社と一般社団法人日本部品工業会に所属する主要サプライヤ 7 社が発起人となり、一般社団法人 Japan Automotive ISAC（略称 J-Auto-ISAC）が設立された[64]。

これまで、日本の自動車業界では 2017 年 1 月に一般社団法人日本自動車工業会内に発足した J-Auto-ISAC WG が中心となって一般社団法人日本部品工業会や米国 Auto ISAC と共に様々な課題に取り組んでいた。しかし、自動車産業がモビリティビジネスへと変革が加速する中、すでに様々な協業が始まっており、関係する事業者は増大する一方となっている。

その中で、J-Auto-ISAC は業種や事業規模を超えた幅広い連携を実現し、サイバーセキュリティの観点から「つながるクルマ」を守る基盤づくりを目的としている。

発起人の企業は、以下のとおりである。

いすゞ自動車株式会社、川崎重工業株式会社、スズキ株式会社、株式会社 SUBARU、ダイハツ工業株式会社、トヨタ自動車株式会社、日産自動車株式会社、日野自動車株式会社、本田技研工業株式会社、マツダ株式会社、三菱自動車工業株式会社、三菱ふそうトラック・バス株式会社、ヤマハ発動機株式会社、UD トラックス株式会社、アイシン精機株式会社、住友電気工業株式会社、株式会社デンソー、パナソニック株式会社、日立 Astemo 株式会社、マレリ株式会社、三菱電機株式会社

3.2.2. 独立行政法人情報処理推進機構

2020 年 8 月、独立行政法人情報処理推進機構（IPA）は「脆弱性対処に向けた製品開発者向けガイド」を公開した[65]。インターネットやホームネットワーク等のネットワークに接続する以下のような機器、ネットワーク家電・プリンタ・ネットワークカメラ・スマートフォンやパソコンのアプリケーションなどを開発している事業者（主に中小規模）を対象としており、製品の脆弱性への対処すべき項目が記載されている。

---

[64] https://prtimes.jp/main/html/rd/p/000000002.000073805.html

[65] https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

本ガイドが公開された目的は以下の 3 点である。

- 製品開発者がセキュリティ対策として実施すべき項目を把握できる
- 実施する対処を徐々にレベルアップできる
- 一般消費者に自組織の取り組み状況をアピールするため、すべきことを把握できる

本ガイドの利用方法は、①チェックリストで自組織の対応状況を確認する、②ガイドを参照しチェック内容をもとに対処内容を確認する、③チェック内容をもとに対応方針を決定する、④ガイドの内容を踏まえて対応する、のステップで脆弱性対処を進めていくことが想定されている。

また、製品開発者が実施すべきこととして、「製品セキュリティポリシーの策定」、「セキュリティサポート方針の明示」、「製品セキュリティを維持するための体制と管理」具体的には PSIRT の設置、「セキュリティを確保するための設計」、「アップデートを考慮した設計」、「既知の脆弱性解消」、「セキュアコーディング」具体的にはセキュアコーディング規約・教育・実装・レビューの実施、「開発環境のセキュリティ確保」、「開発時の脆弱性検査」、「製品と構成要素の脆弱性監視」、「脆弱性報告の受付・対策情報の公表」「一般消費者の製品利用時における実施事項の明示」があげられている。

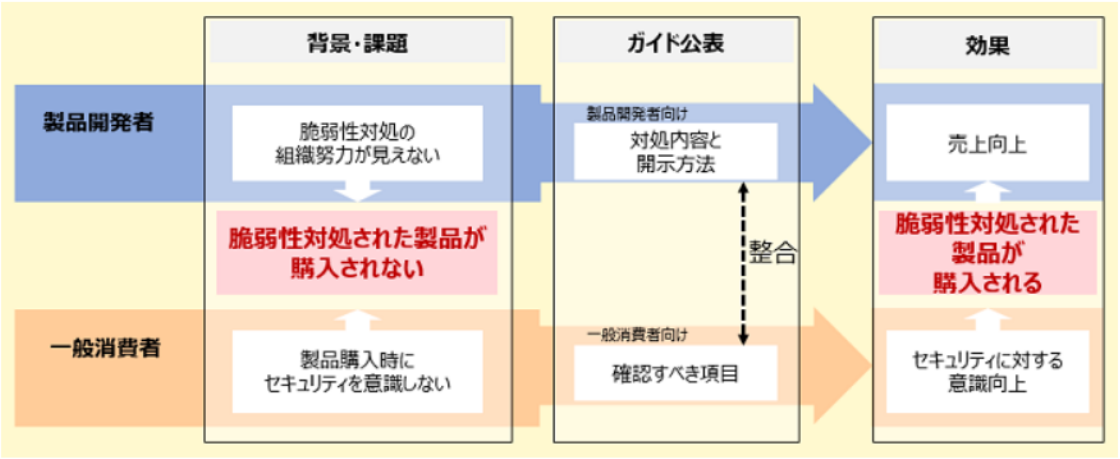


図 16 ガイド活用により期待される効果

3.2.3. Opensource for ALL

2020 年 6 月、特許庁、内閣府により、幅広い業種・理解度等の読者層に対して、共通的に、経営レベルで求められる OSS の必要性・価値・リスクを示すことを目的とした啓発ツールとして「Opensource for

ALL」が作成された[66]。

経営層が知るべき OSS の視点として「必要性」「価値」「リスク」「アクション」をあげ、OSS 利活用がもたらす効果と求められる対応について整理を行っている。

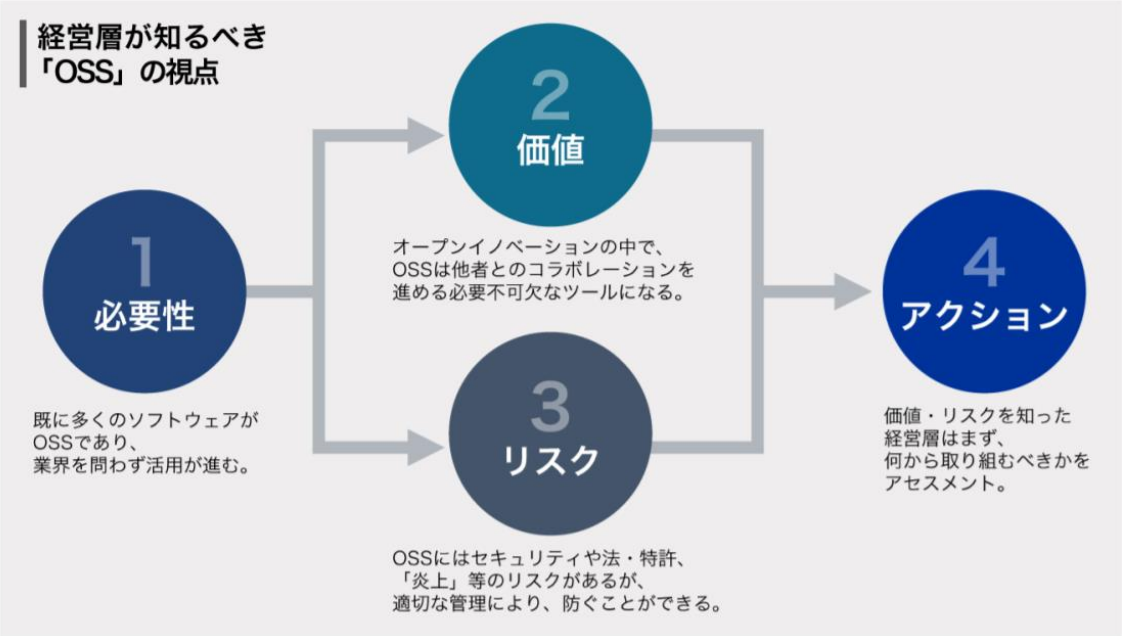


図 17 「Opensource for ALL」における経営層が知るべき OSS の視点

3.2.4. FINOS

Fintech Open Source Foundation（FINOS）は、金融機関によるフリーおよびオープンソースソフトウェア（Free and Open Source Software：FOSS）[67]の取得と使用、FOSS プロジェクトへの貢献[68]

66

https://www.jpo.go.jp/resources/report/takoku/document/zaisanken_kouhyou/2019_06_2.pdf
https://www.jpo.go.jp/resources/report/takoku/document/zaisanken_kouhyou/2019_06_1.pdf

67 FOSS ライセンスの条件に基づきライセンス適用されるソフトウェア（ソースコード、実行ファイル、文書、メディアアセット、その他のデジタルコンテンツなどを含む）（https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc）。

68FOSS プロジェクトに含めるために提供されるソフトウェアのソースコード、文書、メディアアセット、その他のデジタルコンテンツなどの材料（https://github.com/finos/reference-foss-

について規定するポリシーのテンプレートを公開している。このポリシーは、FOSS を企業のソフトウェア製品[69]に組み込む、サードパーティに FOSS を配布する、サードパーティの FOSS プロジェクトにコードなどを貢献する、企業のソフトウェア製品を FOSS として公開するといった活動やその他の FOSS コミュニティとのやり取りに関して金融機関の担当者が遵守すべき項目を定めている。FOSS を効果的に利用することにより、ソフトウェア開発コストの削減、開発期間の短縮、ソフトウェアの品質やセキュリティの向上、開発者の採用や定着の促進などのメリットが得られる。一方で、機密情報の漏洩や権利の侵害、セキュリティの脆弱性、評判の失墜などのリスクも生じるが、こうしたリスクは正しい対策により回避できる。このポリシーはこうしたリスクを最小限に抑え、連邦金融機関検査委員会（Federal Financial Institutions Examinations Council）による推奨事項に従うこと、また、企業とその従業員が FOSS の使用と FOSS への貢献において、サードパーティの権利を尊重し、規制を遵守し、生産的な形で FOSS コミュニティとの関係を築けるようにすることを目的としている。

1）権限

本ポリシーにおいて、企業の知的財産権のライセンス化を認可するなど特定の行為に対し、取締役が独占的権限を持つことが黙示されている場合、この権限は本ポリシーに規定された制限の範囲内で、明示的に[最高技術責任者（CTO）/CTO チーム/最高情報責任者（CIO）]に譲渡される。

2）適用範囲

本ポリシーは企業のすべての従業員、契約社員、顧問を対象に全世界で適用され、FOSS のインストールや企業のコンピューターでの使用、企業のソフトウェア製品への組み込み、単独またはソフトウェア製品と組み合わせての顧客やサードパーティへの配布、公開、サードパーティの FOSS プロジェクトや FOSS 組織への貢献など、オリジナルまたは変更済みの FOSS のあらゆる使用について規定する。

本ポリシーを採用する前に社内で既に FOSS を使用していた場合は、ポリシーの採用後合理的な期間内にポリシーの遵守を確認できるよう、FOSS レビュー委員会（FOSS Review Board：FRB、詳細は次項を参照）が以下のようなプロセスを確立する。

1. FRB は自動のスキャンツールなどを使用して製品所有者への調査を行い、FOSS 使用案件の一覧を作成したのち、ポリシーに反する要素がないか確認する。
2. 製品チームが既存の FOSS コンポーネントを更新した際やこれらに変更を加えた際は、更新または変更されたコンポーネントには、FOSS の新たな使用や変更に関するポリシーおよび手順が適用される。

---

policy/blob/master/src/FINOS-reference-FOSS-policy.adoc）。

[69] 当該企業が最初の開発をすべて、または主に行ったソフトウェア（https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc）。

3）役割と責任

当該企業は本ポリシーの採用に際し FOSS レビュー委員会（FOSS Review Board：FRB）を設立しなければならない。FRB には少なくとも法務、セキュリティ、IT アーキテクチャの各部門の代表者が参加し、責務を速やかに遂行するため必要に応じて会議や連絡を行う。FRB の責務は以下のとおり。

1. 技術責任者や企業幹部と連携した FOSS 戦略の開発、周知。
2. 本ポリシーの実施手順の確立。
3. FOSS リクエストのレビューと決定。
4. 定期的なフィードバックの収集と本ポリシーの再検討に基づくポリシー改定案の作成。
5. 本ポリシーを遵守するための支援、トレーニング、文書の提供。

コンプライアンス部門は必要に応じて FRB と協力して、ポリシー遵守の手順を決定し、必要なトレーニングを計画、実行し、本ポリシーや他の企業ポリシーの解釈に関する疑問を解決する。

法務部門は代表者が FRB に参加する。提出された FOSS リクエストや既存の FOSS に関するすべての FOSS ライセンスをレビューし、FRB と協力してコンプライアンスの要件を策定、周知する。

セキュリティ部門は代表者が FRB に参加する。FOSS コンポーネントのセキュリティ脆弱性を発見し対応するための手順を確立するほか、FRB、製品チームと協力して関係者にセキュリティの問題について知らせ、問題を修復する。

4）実施

FRB は本ポリシーの実施に責任を持ち、ポリシーで定められた要件に従って必要な実施手順を策定する。推奨される実施手順は以下のとおり。

- FRB が作成または入手する資料
  - FOSS ライセンスリスト（またはデータベース）：名前、バージョン、変更や配布に関するコンプライアンス要件、事前承認される使用方法、FRB のレビューが必要な使用方法、禁止される使用方法などを含む、FRB がレビューした FOSS ライセンスの一覧。
  - FOSS トレーニングプログラムと必要資料：従業員が新しく FOSS の使用または貢献をリクエストする前に完了する必要のあるトレーニング。ソフトウェアの知的財産、コンプライアンス要件、FOSS の使用、変更、貢献に関するリスク要因、ソースコードバージョン管理システム（SCM）の適切な使い方、FOSS コミュニティの行動規範といったトピックを含める。

- FOSS リクエスト[70]の事前承認：リクエストを迅速に処理するために、FRB は個別のレビューが不要として事前承認されるリクエストの種類を定義しておく。一般的には、企業にもたらすリスクが少ないと思われる FOSS リクエストが事前承認の対象となる。事前承認の範囲は特定の期間、FOSS コンポーネント、プロジェクトチーム、リクエストの種類などを基準に、リスク管理の観点から FRB が適切と考える方法で決定する。たとえば、基幹業務に関連しないサードパーティの特定のプロジェクトへの貢献や、承認済みの FOSS ライセンスを持つすべてのサードパーティプロジェクトに対するバグ修正やセキュリティパッチを事前承認の対象とするなど。

5) FOSS トレーニングに関するポリシー

FRB は、本ポリシーに定められた要件を関連する従業員に伝えるための FOSS トレーニングプログラムを作成し、コンプライアンス部門を協力してトレーニングを実施する。推奨されるトレーニングの手順として、本ポリシーの採用後 90 日ほど経過したら、従業員に、FOSS リクエストの提出や FOSS のソースコードを含む企業のソフトウェアリポジトリへの変更許可を取得する前に、本ポリシーを読み内容を理解したことを証明させる。また、上記のような活動を行う前、または行った後できるだけ早く、FOSS トレーニングプログラムを完了することを義務付ける。

6) FOSS の使用に関するポリシー

FRB は、企業の FOSS 戦略の推進、規制遵守やサードパーティに対する責務遂行の徹底、FOSS を組み込んだ企業のソフトウェア製品のセキュリティ保護を目的として、FOSS の使用に関する手順を規定する。推奨される FOSS の使用手順は以下のとおり。

1. FOSS リクエストのプロセス

   i. FOSS 使用レポートの提出。FOSS コンポーネントを使用したいと考える従業員やプロジェクトチームは、以下の情報を含む FOSS 使用レポートを FRB に提出する。

      - FOSS コンポーネントの情報：名前、バージョン、オリジナルの URI、適用される FOSS ライセンス、ライセンス要件など。
      - FOSS コンポーネントの使用方法に関する情報：リクエストを行う従業員やプロジェクトチームの名前、関連する企業のソフトウェア製品、使用方法の簡潔な説明、変更歴や変更の予定、社外への配布予定の有無など。
      - 該当するコンポーネントの FOSS ライセンスに対するこの使用方法が FOSS ライセンスリストで事前承認の対象として記載されているかどうか。

[70] FOSS 使用レポートを通じた FOSS の使用の要求、または FOSS への貢献の要求（https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc）。

ii. セキュリティレビュー。FOSS コンポーネントにセキュリティ脆弱性がないか審査する。

- セキュリティ部門により周知されたた基準に従ってレビューを行う。この基準には、使用する自動化ツールや、セキュリティ部門や第三者による審査を要する条件などが規定されている必要がある。
- National Vulnerabilities Database（https://nvd.nist.gov）を参照し、該当する脆弱性がないか調べる。
- 重大な脆弱性やセキュリティ部門により修正が必要と判断した脆弱性が見つかった場合、リクエストの承認前にプロジェクトチームにより修正されなければならない。

iii. FRB レビュー。要求された使用方法が事前承認の対象となっていない場合は、FRB が以下のように審査を行う。

① 適用される FOSS ライセンスやその他の条件の確認

② リスク分析：法律、財務、評判、セキュリティ、戦略の面で重大なリスクを確認。リクエストを承認する場合はリスクを軽減するための方法を確認。

③ FOSS 使用レポートの承認または却下、決定に基づくリクエスト内容の変更

- 承認する場合、FRB がリクエストされた使用方法に適用されるコンプライアンス事項とリスク軽減策を含めて承認を通知。プロジェクトチームは承認済みの方法[71]を通じて該当の FOSS コンポーネントを利用できるようになる。
- FRB の承認はそのリクエストで指定されたバージョンに限って適用されるため、該当の FOSS コンポーネントが後日アップグレードまたは変更される場合は、改めて FOSS 使用レポートを提出する必要がある。その使用方法が事前承認の対象であり、コンポーネントのライセンスが変更されていない場合は、新しいバージョンも事前承認の対象となる。

2. コンプライアンス

FOSS 使用レポートが承認された場合、プロジェクトチームは以下の要件に従う。

- FOSS のソースコードファイルは、ソースコード管理（SCM）システム内で FOSS 以外のソースコードと分けて管理する必要がある。たとえば FOSS ファイルから FOSS 以外のファイルにソースコードをコピーしてはならない。
- プロジェクトチームは FOSS ライセンスリストや FRB により規定されたあらゆるコンプライアンス要件またはリスク軽減のための要件に従う。

3. メンテナンス

[71] 企業によりソフトウェア製品での使用を許可された、ソフトウェア開発の成果物を利用するための方法（https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc）。

- セキュリティ部門は社内で使用されているすべての FOSS コンポーネントに関する脆弱性の報告を確認し、そのコンポーネントを使用しているプロジェクトチームに脆弱性について通知する。
- 重大なセキュリティ脆弱性が確認された場合、プロジェクトチームはすみやかにパッチを適用するか、セキュリティ部門が指示するリスク軽減策を実行する。
- FOSS コンポーネントが顧客やサードパーティに配布されている場合、FRB は合理的な方法で特定可能な利用者に対して通知や修復のサポートを提供できるよう手配する。

7）FOSS の変更に関するポリシー

FRB は、従業員による FOSS の変更に関する手順を規定する。FOSS の使用に関するポリシーで言及された優先事項（戦略、コンプライアンス、セキュリティ）に加え、変更に関するポリシーでは、企業の FOSS 戦略や該当する FOSS ライセンスの要件に基づき、社内で行われる FOSS に対するすべての変更と、元の FOSS プロジェクトに対する変更内容の貢献を文書化するよう促す。FOSS が社内で利用されるか社外に配布されるかを問わず、FOSS に対するすべての変更が対象となる。推奨される FOSS の変更手順は以下のとおり。

1. 変更のプロセス

サードパーティの FOSS に対する変更は以下の手順で行う。

i. リクエスト：サードパーティの FOSS コンポーネントを変更するプロジェクトチームは変更の内容や目的を記述した新規の FOSS 使用レポートを FRB に提出する。リクエストする変更が事前承認の対象でない場合は、本番環境での使用、配布、社外への貢献を行う前に FRB による承認を受ける必要がある。

ii. FRB による決定：FRB は FOSS の使用に関するポリシーに従って FOSS 使用レポートをレビューし、承認か却下かを決定する。

iii. 変更の実施

- 元の FOSS コンポーネントとの差異がわかるよう、変更は SCM システムを使用して追跡する。また、企業の内部監査の要件に沿って、貢献を行う従業員の身元情報も SCM システムで記録する。
- FOSS ライセンスの要件にある場合は、ソースコードに変更があったことと変更内容を示す記述を含める。

iv. 変更された FOSS のビルド：該当する場合は、変更した FOSS コンポーネントを標準的なツールを使ってビルドする。独自のプロセスやツールが必要な場合は、プロジェクトチームがインフラチームにプロセス、ツール、メンテナンスに関する文書を提供する。

2. コンプライアンス

FOSS の変更には、FOSS の使用手順で言及されているコンプライアンス要件、および FRB や該当する FOSS ライセンスにより指定されている変更に関するその他の要件が適用される。

3. メンテナンス

変更した FOSS には、FOSS の使用手順で言及されているメンテナンス要件が適用される。変更を元の FOSS プロジェクトに貢献することでメンテナンスが容易になり企業の FOSS 戦略にも合致する場合は、プロジェクトチームが FOSS への貢献リクエスト[72]を提出するとよい。

8）FOSS の貢献と公開に関するポリシー

FRB は、1）従業員がコードやその他の材料をサードパーティの FOSS プロジェクトに貢献することと、2）企業のソフトウェア製品を FOSS ライセンスの下で公開することに関する手順を規定する。FOSS の使用に関するポリシーで確認された戦略、コンプライアンス、セキュリティ面の優先事項に合致する手順であるべきである。

従業員がサードパーティの FOSS プロジェクトに貢献する場合と、企業のソフトウェア製品の全体または一部を FOSS ライセンスの下で公開する場合は、すべて前もって FRB の承認を得る必要がある。また、貢献の内容がサードパーティの既存の FOSS プロジェクトへの変更である場合は、FOSS への貢献リクエストの承認を得る前に、FOSS の変更手順に従ってこれらの変更に対する承認を得る必要がある。推奨される FOSS の貢献および公開の手順は以下のとおり。

1. 貢献リクエストのプロセス

i. FOSS への貢献リクエスト：プロジェクトチームが社内の FOSS リクエストシステム[73]を通じ、以下の情報を含む FOSS への貢献リクエストを提出する。

- 貢献の内容がサードパーティの FOSS プロジェクトへの変更である場合
  - 承認された FOSS 使用レポートへのリンク
  - 貢献者ライセンス同意書など、該当の FOSS プロジェクトへの貢献に関する要件へのリンク
- 貢献の内容が企業のソフトウェア製品（全体または一部）である場合
  - ソフトウェア製品の名前とバージョン
  - 貢献するソフトウェアの機能に関する説明

[72] 従業員やプロジェクトチームが外部の FOSS プロジェクトに貢献することや、ソフトウェア製品を FOSS として公開することを要求するリクエスト（https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc）。

[73] FOSS に関するリクエストの提出、議論、決定を行うための社内のシステム（https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc）。

- 企業のソフトウェア製品との関係
- 依存関係のリスト
- 貢献するソフトウェアが管理されている社内の SCM リポジトリの場所

- プロジェクトチームによる、利点とリスクなどを含む貢献の理由の説明
- 貢献者の名前、GitHub ID などの情報

ii. FRB によるレビュー：FRB が以下のリスク要因を考慮してリクエストを審査する。

- 企業の知的財産に対する影響
  - 互恵型（コピーレフト）のライセンスに関する要件
  - 貢献により漏洩する可能性のある企業秘密
  - 貢献により公開またはライセンス化される可能性のある、特許を取得した、または特許可能な発明
- 以下のような情報の漏洩
  - サードパーティが専有権を持つソースコードなどの材料
  - 秘密保持契約などにより利用が制限されている情報
  - 顧客や従業員に関する個人を特定可能な情報
  - 秘密鍵、パスワード、専有情報を含むデータセットなどの企業の機密情報
- 企業のソフトウェア製品の競争力に及ぼす影響
- ソフトウェアのライセンスなど、既存のまたは予想される収益源に対する影響
- 貢献したソフトウェアや FOSS コミュニティとのやり取りで発生した問題などにより、企業の評判が失墜する可能性

iii. FRB による承認：FRB がリクエストを承認する場合は、類似するリクエストや関連するリクエストを事前承認の対象とするかを検討する。

2. 貢献の前に満たすべき要件

i. 開発には社内の SCM ツールを用いる。

ii. 法的要件

- FOSS プロジェクトへの貢献者が提出する貢献者ライセンス同意書などの法的証明書類はすべて法務部門のレビューおよび承認を受ける必要がある（該当の FOSS プロジェクトへの貢献が以前に承認されており、追加の署名や承認が不要な場合を除く）。
- 企業が保持するすべての知的財産権を、貢献を行う組織[74]に譲渡する必要がある。

[74] 貢献を行う企業体や関連会社。

iii. コンプライアンス：該当の FOSS プロジェクトのポリシー、手順、行動規範、企業の方針に従う必要がある。これらの内容が衝突する場合は、貢献者が貢献を進める前に FRB に解決策を仰ぐ。

iv. 相互レビュー：FRB により貢献リクエストが承認された場合、貢献を行う前に、本ポリシーに精通した開発者やマネージャーにより、以下の点を考慮した審査を受ける必要がある。

- FRB から貢献の許可を得ていない企業の知的財産や機密情報を含んでいないか。
- FOSS ライセンスリストや FRB により要求されたコンプライアンス情報、および必要な通知を含んでいるか。
- 企業の行動規範や FOSS への貢献に関するポリシー、該当の FOSS プロジェクトのポリシーや行動規範に合致しているか。

3. 貢献

公開されたソースコードリポジトリへの貢献は、貢献を行うプロジェクトチームのメンバーのユーザーアカウント（GitHub ID など）から行う。著作権はすべて企業に帰属する。

4. 企業のソフトウェア製品の公開

企業のソフトウェア製品を FOSS ライセンスの下で公開する場合は、常に上記の貢献に関する要件に従う。さらに、公開を行う前に財務部門が、企業の会計帳簿を修正する必要があるかどうかを判断する。たとえば、企業のソフトウェア製品の投資費用を減額する場合などがある。

5. 個人的な（業務時間外の）貢献

従業員がプライベートで、個人のハードウェアとリソースを用いて貢献を行い、その貢献が、従業員と取り交わした知的財産譲渡契約書に基づく企業の財産に該当しない場合は、社外の商取引に関するポリシーが適用される。こうした貢献は従業員個人の名前で行い、会社名の言及はしないものとする。

9）全般

1. 本ポリシーに対する例外はすべて書面で作成し、FRB の承認を受ける必要がある。
2. 本ポリシーへの準拠に関する質問はすべて FRB に問い合わせる。
3. 本ポリシーは FRB が所有する。
4. FOSS の使用、変更、貢献、公開には、本ポリシーや関連する手順に基づき、企業の以下に関する方針も適用される場合がある。
   - 行動規範
   - 知的財産
   - 技術獲得
   - ソーシャルメディア

- ビジネスプロセスの変更管理
- 情報セキュリティ
- 情報分類
- 電子通信
- ソフトウェアの開発とメンテナンス
- ソフトウェアと IT インフラストラクチャの開発ライフサイクル
- ソースコード管理
- セキュアコーディング

3.3. その他の取り組み等

その他、ソフトウェア管理の取り組み、動向等を取りまとめた。

3.3.1. Secure Software Development Framework

2020 年 4 月、NIST は、セキュリティに配慮したソフトウェア開発手法を既存の標準やガイドライン等を参照する形で Secure Software Development Framework (SSDF)として整理した。SSDF では、各手法を「組織構築」「ソフトウェア保護」「セキュアなソフトウェア」「脆弱性対応」の 4 つに分類の上、何をすべきか（Practice-Task の 2 階層）、事例、参照文書について体系化している。

表 5 Secure Software Development Framework (SSDF)概要

分類	分類（英語名）	概要	手法例	備考
組織構築	Prepare the Organization（PO）	人材、処理能力、技術等のソフトウェア開発リソース確保	• ソフトウェア開発におけるセキュリティ要件を定義 • 各役割と責任の実装	• PS の中で SBOM の作成と維持について言及あり • 参照文書（Reference）は、ISO、BSA、NIST CSF 等
ソフトウェア保護	Protect the Software（PS）	ソフトウェアの全てのコンポーネントを改ざんや不正アクセスから保護	• 全ての形式のコードを改ざんや不正アクセスから保護	
セキュアなソフトウェア	Produce Well-Secured Software（PW）	ソフトウェアリリース時のセキュリティに関する脆弱性を最小化	• ソフトウェアデザインにおけるセキュリティ要件への合致とリスク低減	
脆弱性対応	Respond to Vulnerabilities（RV）	ソフトウェアセキュリティの脆弱性の認識、適切な対応、将来にわたる予防策	• 継続的な脆弱性の特定・確認 • 脆弱性の評価・優先付け・修正	

3.3.2. Advancing Software Security in the EU

2019 年 11 月、EU の ENISA は、ソフトウェアセキュリティ向上に向けた EU サイバーセキュリティ認証フレームワークの役割をとりまとめた。ソフトウェアセキュリティ向上の要素とソフトウェアセキュリティにおける問題点を説明した上で、EU サイバーセキュリティ認証フレームワークや認証スキーム下でのソフトウェア開発における実践的考慮事項を紹介している。

表 6 ソフトウェア開発における実践的考慮事項

ソフトウェアセキュリティ向上の要素

- セキュリティ要求
  - ユーザーからの明確な機能要求及び非機能要求
  - 法的な要求及び義務
  - 広く受け入れられているガイドラインにおいて、ベストプラクティスとして定められている要求
    - 例えば、クレジットカード業界では、PCI SSI（業界におけるセキュリティ評議会）が定めたセキュリティ要求が、契約の際にベンダ等に課されることが一般的
- セキュアソフトウェアエンジニアリング
  - (主な要素)脅威のモデリング、リスク分析、ガイドライン、教育、要件、設計分析、問題管理、コンプライアンス、検証、欠陥管理
- セキュア開発ライフサイクル
  - 開発プロセス全体でのセキュリティ対策が必要

ソフトウェアセキュリティにおける問題点

- 既存の標準やスキームにおける調和の欠如
- 品質保証の欠如
- 持続的な信頼の確保が困難
- 開発プロセスにおけるセキュリティ評価が困難
  - 製品のみならず開発プロセスも評価されることが望ましいものの、プロセスの有効性を決する要素（人々の技術や経験など）は測定が困難

EUサイバーセキュリティ認証フレームワークや認証スキーム下でのソフトウェア開発における実践的考慮事項

- セキュリティ対策のためのリポジトリ整備の進展
  - 公衆に開示された脆弱性のみならず一般的なセキュリティ(アクセス制御、承認、暗号化等)の要素についてのリポジトリが展開・保守されるべき
- 標準化の取り組みにおける諸機関の協調の必要性
  - 連合導入作業計画（URWP）の公表後、欧州の標準化機関や標準開発機関は将来の制度の発展に向け、標準化を前進させるべく協業するべき
- エンジニアリングプロセスの保証
  - ソフトウェアの開発・保守・運用についてのプロセスガイドラインの策定を通じて、最終製品・サービス・プロセスのみならず、エンジニアリングプロセスについても保証するべき
- 様々な場面を想定した、リスクに応じた保証レベルの提供
  - リスクに対する保証レベルが「初歩的」(※1)であっても、自己適合性評価(※2)を用いて、ソフトウェア開発・保守において信頼性を確保すべき
    - ※1 Cyber Security Act 52条 1.にて、リスクの程度に応じて、初歩的(basic)、実質的(substantial)、高度(high)の保証レベルを指定できるものとされている
    - ※2 Cyber Security Act 53条 1.にて、「初歩的」に対応するリスクに対しては、製造業者等による自己適合性評価が許容されている
  - ソフトウェアや製品の製造業者は、彼らの経験や専門知識を周知するとともに、EUサイバーセキュリティ認証スキームの利用を進めるべき
  - 欧州委員会(EC)やENISA等は、EUサイバーセキュリティ認証フレームワークのエンドユーザーに対して、フレームワークの射程、適用範囲や軽減されるリスク等についての想定が明確に伝えられるように保証するべき

3.4. OSS を含むソフトウェアの安全な利活用に関する基礎資料

ソフトウェアの安全を脅かす要因について、近年発生したセキュリティ脆弱性等の事例を調査した。

3.4.1. Ripple20

2020年6月、JSOF社は、Treck社[75]が開発したTCP/IPプロトコルスタック[76]「Treck TCP/IP Stack」に複数の脆弱性があることを発表した[77]（発表年や当スタックが 20 年以上前から存在していること等に由来し、19 の脆弱性の総称を Ripple20 と命名）。遠隔の第三者によって、任意のコード実行、情報の窃取、サービス運用妨害（DoS）等の攻撃を受ける可能性があり、最新バージョンへの更新やパッチの適用、IP パケットのフィルタリング等の対策を呼び掛けている。

Treck TCP/IP Stack は多数の企業が製品に採用しており、数億台かそれ以上の機器が影響を受けるとされ、家庭向けデバイス、ネットワーク機器、医療機器、産業制御機器／システム、重要インフラ分野などの幅広い領域への影響が懸念される。

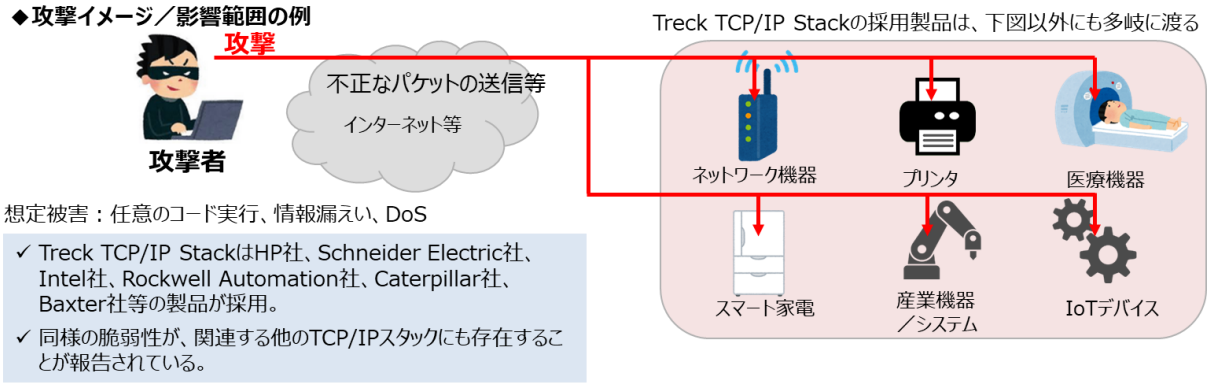


図 18 Ripple20 の攻撃イメージ

3.4.2. BootHole

[75] 組み込み機器向けのインターネットプロトコルスタックを設計・開発する米国の企業

[76] 階層構造で構成されるインターネットプロトコル群

[77] https://www.jsof-tech.com/ripple20/

2020 年 7 月、Eclypsium 社[78]は、Linux 等で用いられるブートローダー[79]「RUB2」の脆弱性（ BootHole と命名）を報告した[80]。 OS が起動する前段階において不正なプログラム実行を防ぐ「セキュアブート機能」を回避できることが確認されている。この脆弱性の悪用により、対象のデバイスが完全に制御される可能性がある。

Microsoft や Red Hat 等の主要 Linux ディストリビュータは、この問題に関するセキュリティ情報を公開し、対応を表明している。

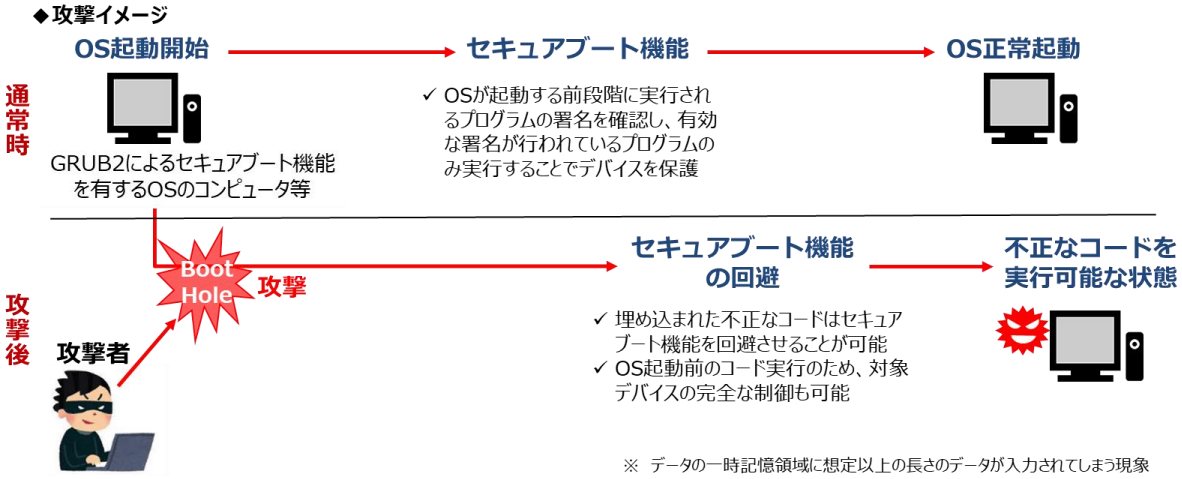


図 19　BootHole の攻撃イメージ

3.4.3.　Zerologon

2020 年 9 月、オランダのセキュリティ企業によって、 Windows Server の Microsoft Active Directory ドメインコントローラへ攻撃することを可能にする、Netlogon※プロセスの暗号化における脆弱性「Zerologon」が発表された[81]。

この脆弱性のために、ネットワーク内に攻撃者により侵害された端末が存在する場合、ドメイン管理者の権限が乗っ取られる恐れがある。ドメイン管理者権限が奪取されれば、ドメインに参加する端末を全て制御下に置くことが可能となる。

---

78 企業向けファームウェア/ハードウェア分野における米国のセキュリティ企業

79 コンピュータの起動直後に自動的に実行されるコンピュータプログラム

80 https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/

81 https://www.secura.com/blog/zero-logon

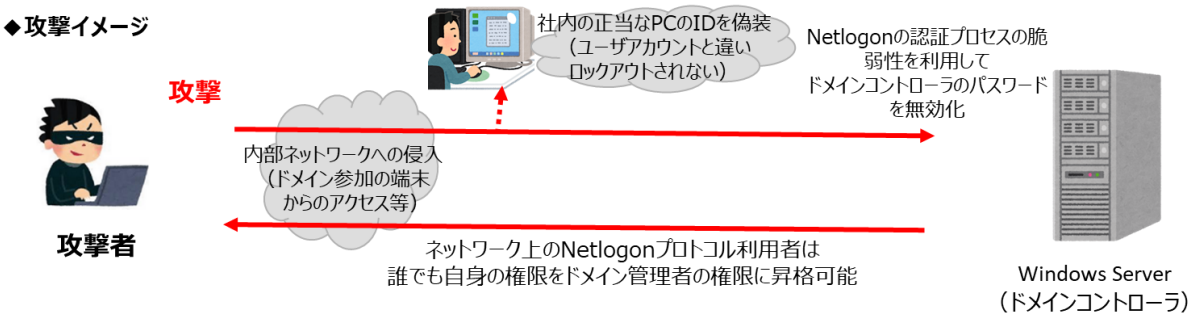
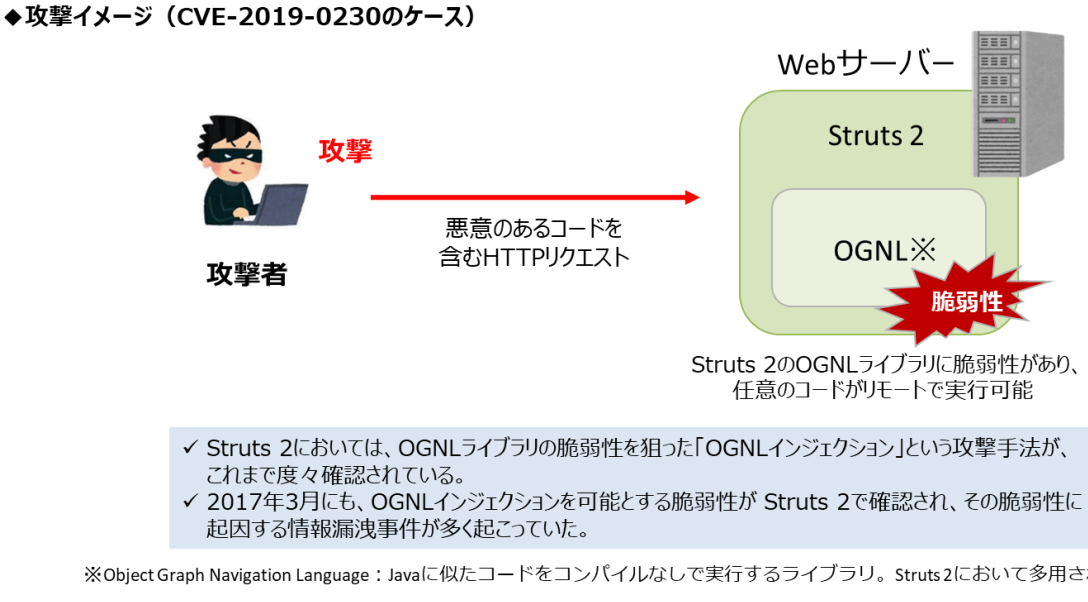


図 20　Zerologon の攻撃イメージ

3.4.4.　Apache Struts 2 の脆弱性

Apache Software Foundation は、2020 年 8 月に Apache Struts 2 の 2 件の脆弱性（CVE-2019-0230、CVE-2019-0233）に関する情報を公開した[82]。本脆弱性が悪用されると、Apache Struts 2 が動作するサーバーにおいて、遠隔の第三者により任意のコードが実行されたり、サービス運用妨害(DoS) が引き起こされたりする可能性がある。



[82] https://struts.apache.org/announce#a20200813

図 21　Apache Struts 2 の脆弱性（CVE-2019-0230）の攻撃イメージ

3.4.5.　Emotet

Emotet は、情報の窃取に加え、他のマルウェアへの感染のために悪用されるマルウェアである[83]。主に、メールに添付された Word などの Microsoft Office ファイルのマクロを有効化することにより[84]感染する。

Emotet に感染した場合、Windows や各種 Web サイトのログイン ID/パスワードといった認証情報に加え、メールのアカウントとパスワード、メール内容、アドレス帳などのメール情報が攻撃者に窃取される。これらの窃取された情報を基に、Emotet の感染を拡大させるメールが大量に配信される。

日本では、2019 年 10 月に複数企業が Emotet 感染を公表するなど感染事例が相次いでいた。2020 年 2 月以降 Emotet の感染につながるメールの配布は観測されていなかったものの、同年 7 月頃からメールの配布を確認。

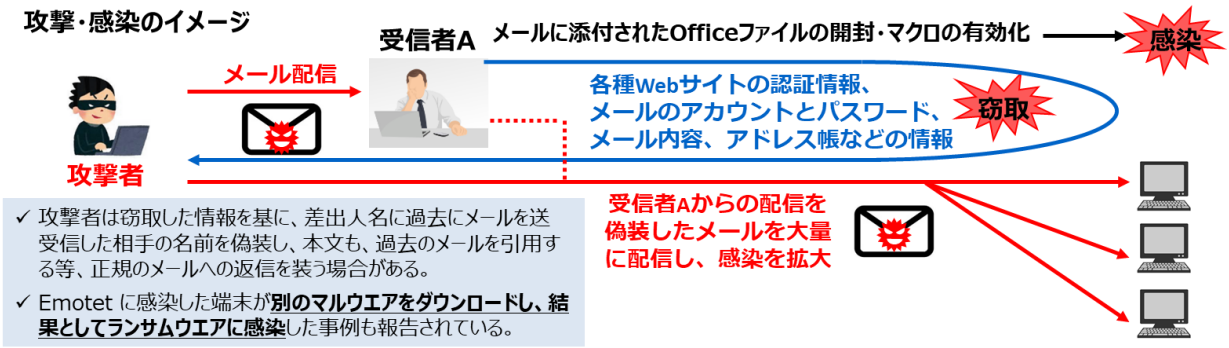


図 22　Emotet の攻撃イメージ

3.4.6.　SIGRed

2020 年 7 月、イスラエルのセキュリティ企業によって、 Windows Server に含まれる Windows DNS Server に脆弱性（SIGRed）が発見された[85]。攻撃者が不正な DNS リクエストを送信するだけで、利用者が何もしなくとも任意のコードが実行可能となる危険性がある。

---

[83] https://www.jpcert.or.jp/newsflash/2020072001.html

[84] マクロが PowerShell を起動し PowerShell のコマンドでマルウエア本体をダウンロードして実行され、感染する

[85] https://www.secure-sketch.com/blog/cve-2020-1350-sigred

この脆弱性の危険度を表す指標 CVSS[86]は最大値の「10」であり、米国土安全保障省（DHS）は政府機関に対策を命じる緊急指令を発令した。

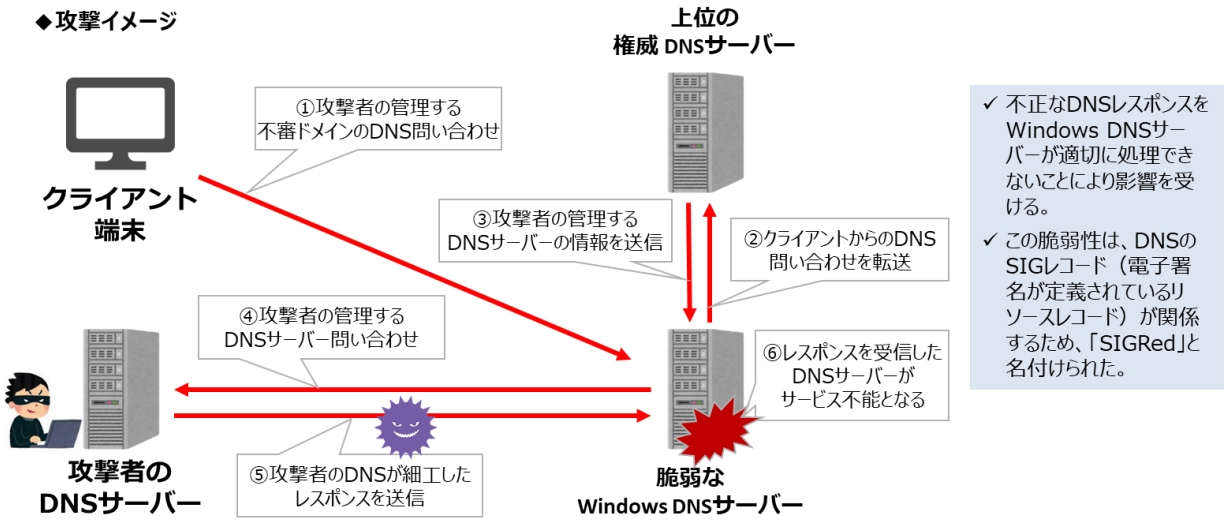


図 23　SIGRed の攻撃イメージ

[86] Common Vulnerability Scoring System：共通脆弱性評価システム

4. ソフトウェアの利活用に係るセキュリティリスクや課題及び対応策

4.1. 企業における OSS 利活用に係るセキュリティリスクの概況及び課題

別途作成した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」の２、３章において、OSS 利活用に係るセキュリティリスクの概況及び課題について取りまとめた。

4.2. 企業における OSS 管理に係るプロセスの取り組み

別途作成した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」の４、５章において、企業における OSS 管理に係るプロセスの取り組みについて事例として取りまとめた。

4.3. 企業における OSS 管理に係る体制構築の取り組み

別途作成した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」の４、５章において、企業における OSS 管理に係る体制構築の取り組みについて事例として取りまとめた。

4.4. 企業における OSS エコシステムに対する貢献の取り組み

別途作成した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」の４、５章において、企業における OSS エコシステムに対する貢献の取り組みについて事例として取りまとめた。

4.5. 企業におけるOSSの利活用及びそのセキュリティ確保に向けた管理手法に係る対応策

別途作成した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」の 6 章において、企業におけるOSSの利活用及びそのセキュリティ確保に向けた管理手法に係る対応策について、事例ヒアリング結果を基に抽出し、整理を実施した。

5. 会合運営支援

本年度実施した会合支援の概要について記載する。なお、新型コロナウイルス感染症拡大防止の観点から、本年度実施した会合は全て Web 開催形式となった。

5.1. 第 4 回サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

(1) 日時

2021 年 1 月 13 日（水）16:00～18:00

(2) 場所

Web 会議

(3) 概要

事務局からの報告とともに、ゲストスピーカーとして、損害保険ジャパン 小中　俊典氏から同社の OSS 利活用及び管理手法について発表があり、その後意見交換が行われた。当日の資料及び議事要旨については、経済産業省のホームページ上にて公開されている（以下 URL）。

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/004.html

5.2. 第 5 回ソフトウェアの利活用におけるセキュリティ確保に関する勉強会 (“Study Session of Software Security”)

(1) 日時

2020 年 7 月 14 日（火）9:00～10:00

(2) 場所

Web 会議

(3) 概要

ゲストスピーカーとして Dr. Allan Friedman, Ph.D.（Director, Cybersecurity Initiatives, NTIA）から SBOM をはじめとする Software Transparency に関する発表があり、その後意見交換が行われた。講演の内容は以下のとおりであった。

- 2020 年の今日において、最も時間と労力を要するのは脆弱性を発見することではなく、ソフトウェアを作っている人やソフトウェアを使っている人に、その脆弱性の影響を受ける可能性があることを知ってもらうこと。ソフトウェアのサプライチェーンの透明性は、これに寄与する。
- ソフトウェアのサプライチェーンにおける透明性は、「開発」、「選択」、「運用」のいずれのフェーズにおいても重要。
- サプライチェーンの透明性の確保にあたり、クロスセクターで、かつ、サプライチェーンの全体をカバーする必要がある。
- NTIA での 2 年間の活動を通じて、最低限の SBOM に焦点を当てること、SBOM は機械判読なものでなければならないことについてコンセンサスがとれた。
- SBOM はサプライヤ、コンポーネントの名称、バージョン、ハッシュ値についてツリー状（ヒエラルキー型）でトレースできる仕組みを目指したもの。
- SBOM があれば、コンポーネントに脆弱性が発見された場合、即座に自身の製品に脆弱性が含まれていることを認識でき、適切な対処が可能となり、時間の面でも費用の面でも便益が大きい。
- SBOM の方式としては、SPDX、SWID に加え、Cyclone DX も開発されており、いずれも完璧ではないが有用である。NTIA はこれらの方式に共通する要素を特定し、他方式との翻訳作業を実施した。
- 昨年実施したヘルスケア業界での SBOM の POC には、米国以外の企業を含む医療機器メーカー、病院が参加し、医療機器メーカーが SBOM を生成できることを示したが、完全に自動化された

方法で SBOM の生成はできなかった。現在実施中のヘルスケア業界での第 2 期 POC では、自動化された方法での SBOM の生成に向けて取り組みを進めている。

- NTIA では、①ソフトウェアのネーミング、②SBOM データの共有方法、③脆弱性と攻撃容易性の問題(Vulnerability vs. Exploitability；攻撃が容易ではないため特段の注意を払う必要のない脆弱性を、上流が下流に対してどのように伝えるか）といった課題に取り組んでおり、それぞれについて NTIA でガイドラインを作成しているところ。
- 今後は、SBOM 導入の自動化に向けたツールやプロセスの整備、普及などを目指していく。

（様式２）

二次利用未承諾リスト

報告書の題名:
令和2年度サイバー・フィジカル・セキュリティ対策促進事業（ソフトウェアを安全に利活用するための基盤構築に向けた調査）調査報告書

委託事業名:
令和2年度サイバー・フィジカル・セキュリティ対策促進事業（ソフトウェアを安全に利活用するための基盤構築に向けた調査）

受注事業者名:
エヌ・ティ・ティ・データ経営研究所

頁	図表番号	タイトル
11	図1	SBOM Exchangeについて
12	図2	課題と次のステップについて
18	図3	ツールの概要
27	図4	SBOMの概念図
28	図5	SBOMのロケーション
30	図6	SBOMツールのテンプレートと事例
33	図7	ヘルスケアPoCフェーズ2参加機関のリスト
45	図8	SwiftBomが作成するSBOMのイメージ
48	図9	Google Drive内のファイルによりAwareness & Adoption WGが作成したSBOMのプロモーション動画を閲覧できる
51	図10	SBOMのベースラインコンポーネントのサンプル（プレゼンテーション資料）
52	図11	2020年のAwareness and Adoption WGの成果まとめ（プレゼンテーション資料）
54	図12	Dependency Trackの動作イメージ（出典：プレゼン資料）
55	図13	Censinetの脆弱性評価のサンプル（出典：プレゼン資料）
56	図14	InSight Platformの概観
58	図15	ヘルスケアPoC第2弾の概要（出典：会合プレゼンテーション資料）
80	図16	ガイド活用により期待される効果
81	図17	「Opensource for ALL」における経営層が知るべきOSSの視点