経済産業省

資料3

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の検討の方向性

令和元年12月4日

経済産業省　商務情報政策局

サイバーセキュリティ課

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

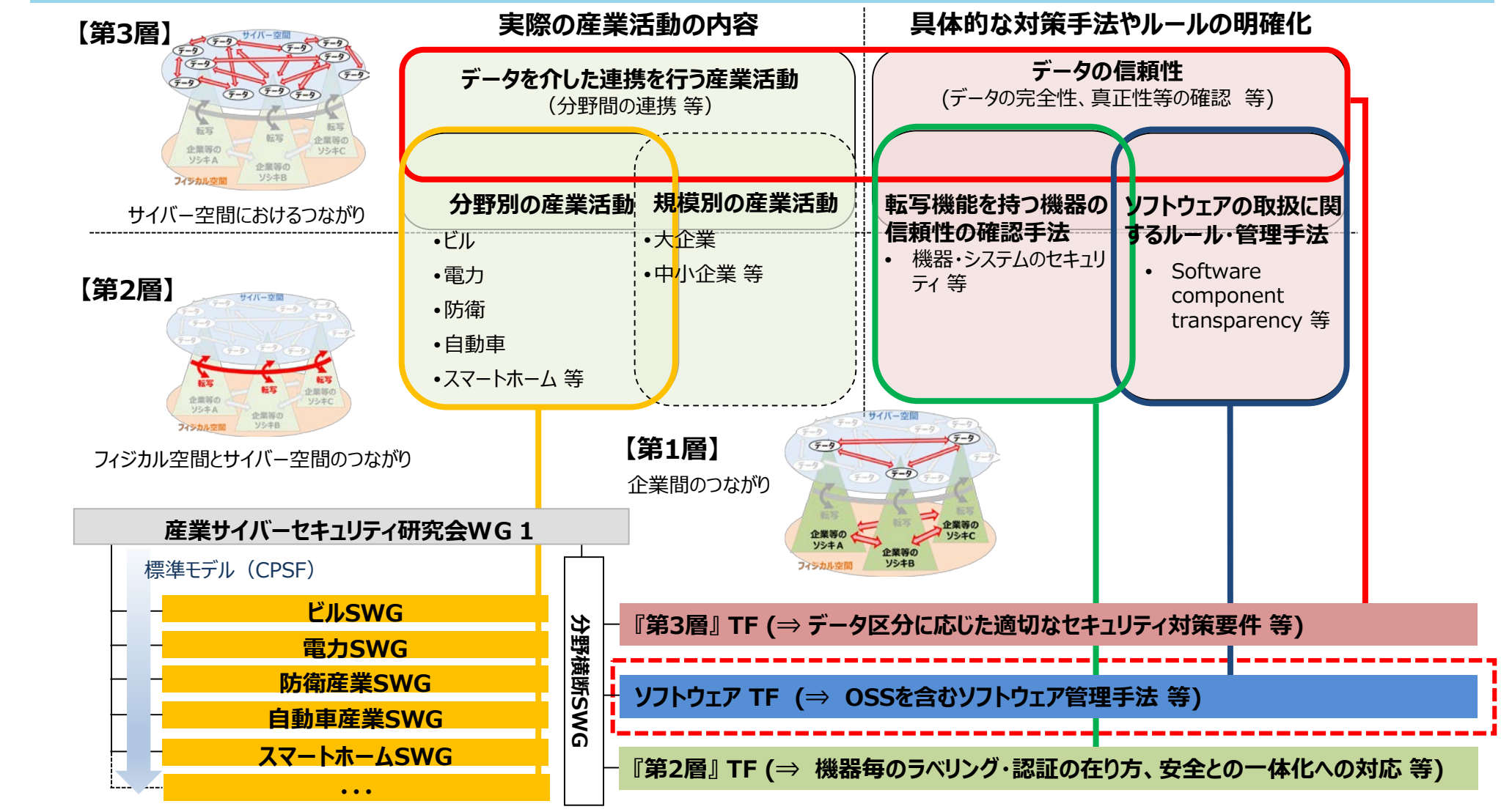
２．本タスクフォースの検討事項について

３．国内外の取組について

４．OSSの利活用について

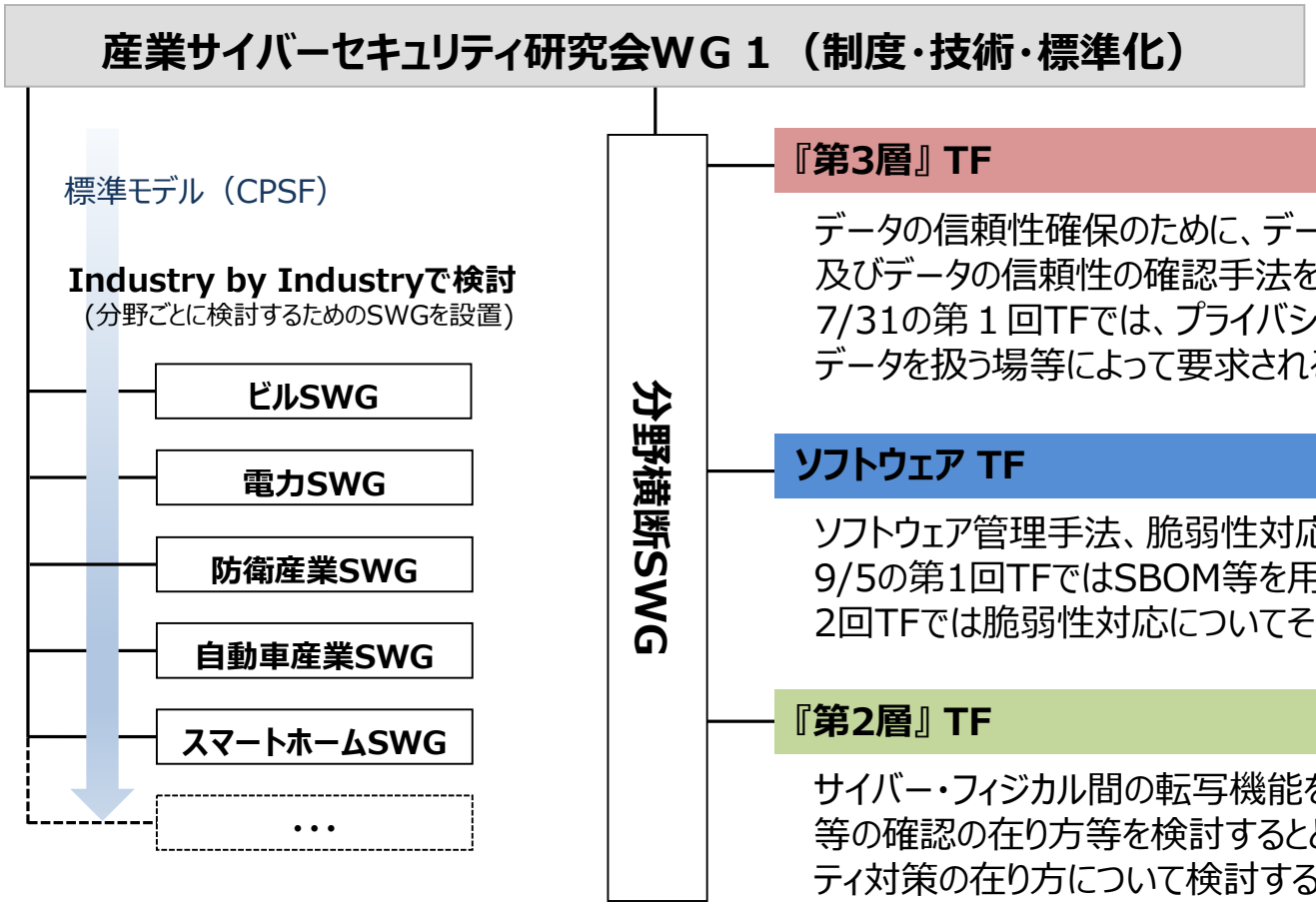
CPSFに基づくセキュリティ対策の具体化・実装の推進

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置。**



テーマ別TFの検討状況

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置**。



『第3層』TF

データの信頼性確保のために、データの区分に応じた適切なセキュリティ対策要件及びデータの信頼性の確認手法を検討する。
7/31の第１回TFでは、プライバシーを含むデータの属性やデータに対する処理、データを扱う場等によって要求されるセキュリティが異なり得ること等を議論。

ソフトウェア TF

ソフトウェア管理手法、脆弱性対応、OSSの利活用等について検討する。
9/5の第1回TFではSBOM等を用いたソフトウェア管理手法について、11/6の第2回TFでは脆弱性対応についてそれぞれ論点の洗い出しを行った。

『第2層』TF

サイバー・フィジカル間の転写機能を持つ機器等について、自己適合宣言・認証等の確認の在り方等を検討するとともに、産業保安・製品安全も考慮したセキュリティ対策の在り方について検討する。
8/2の第1回TF及び11/27の第2回TFでは、安全とセキュリティを併せて考えることの重要性や求められるセキュリティに応じて機器をカテゴライズする必要性等について議論。

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

２．本タスクフォースの検討事項について

３．国内外の取組について

４．OSSの利活用について

ソフトウェア管理手法のあり方　～利用者が留意するべき事項～

<table>
<tr><th></th><th>開発中</th><th>運用中
（脆弱性情報の収集）</th><th>運用中
（脆弱性対応）</th></tr>
<tr><td>HeartBleedの脆弱性</td><td rowspan="2">✓使用中のOSSバージョン把握
✓脆弱性情報の確認
✓保守・サポート期間の確認</td><td rowspan="2">✓OSSのアップデート
✓WAF等による暫定対処
✓サービスの一時停止</td></tr>
<tr><td>Strutsの脆弱性</td></tr>
<tr><td>Copayの脆弱性</td><td rowspan="2">✓開発プロセスの確認</td><td rowspan="2">✓使用中のソフトウェアのバージョン把握
✓脆弱性情報の確認
✓コードサイニング証明書の確認</td><td rowspan="2">✓ソフトウェアのアップデート
✓FW等による暫定対処
✓ソフトウェアの利用停止</td></tr>
<tr><td>Triadaの脆弱性</td></tr>
<tr><td>ASUSの脆弱性</td><td>✓ パッチ配信サーバの安全性確認</td><td>✓脆弱性情報の確認</td><td>✓マルウェアの削除</td></tr>
<tr><td>OSSのライセンス問題</td><td>✓ライセンス内容の確認</td><td colspan="2">✓ライセンス違反の是正</td></tr>
</table>

JVN等の活用により効率化

SBOM等の活用により効率化

STIX/TAXIIの活用により効率化・自動化

ソフトウェア管理手法のあり方　～利用者が留意するべき事項～

	開発中	運用中 （脆弱性情報の収集）	運用中 （脆弱性対応）
HeartBleedの脆弱性	✓使用中のOSSバージョン把握 ✓脆弱性情報の確認 ✓保守・サポート期間の確認		✓OSSのアップデート ✓WAF等による暫定対処 ✓サービスの一時停止
Strutsの脆弱性			
Copayの脆弱性	✓開発プロセスの確認	✓使用中のソフトウェアのバージョン把握 ✓脆弱性情報の確認 ✓コードサイニング証明書の確認	✓ソフトウェアの利用停止
Triadaの脆弱性			
ASUSの脆弱性	✓パッチ配信サーバの安全性確認	✓脆弱性情報の確認	✓マルウェアの削除
OSSのライセンス問題	✓ライセンス違反の確認	✓ライセンス違反の確認	

ソフトウェア管理手法（第1回TFの議題）

脆弱性対応（第2回TFの議題）

OSS利活用（第3回TFの議題）

JVN等の活用により効率化

SBOM等の活用により効率化

STIX/TAXIIの活用により効率化・自動化

本TFにおける検討の方向性

- **ソフトウェア管理手法、脆弱性対応、OSSの利活用等**に関する検討を行う。

ソフトウェア管理手法の検討

- ソフトウェアの開発から、運用中の脆弱性発見まで
- 構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方
- SBOM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題

脆弱性対応手法の検討

- 脆弱性が発見された場合のソフトウェアへの対応
- 脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方
- 運用中システムへの脆弱性対応に求められる技術面・制度面の課題

OSSを利活用する際のビジネス的な側面の検討

・OSS利用に関連するライセンスや契約
・OSS活用のベストプラクティス／OSSコミュニティへの発信

第1回
検討事項

第2回
検討事項

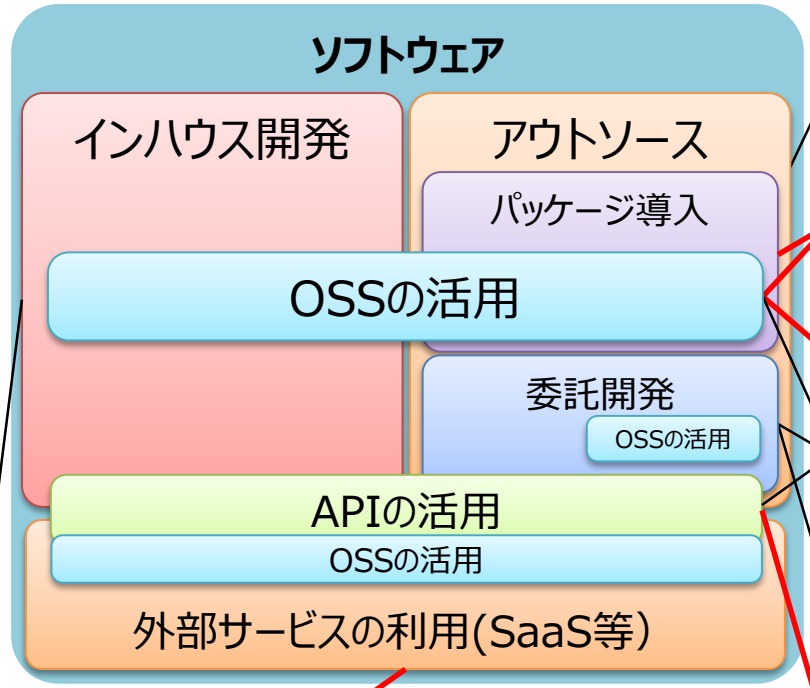
第3回
検討事項

（参考）実効的なソフトウェア管理手法の検討

- 安全なソフトウェアを選定する上でも、開発したソフトウェアを流通させる上でも、ソフトウェアの構成情報の可視化は重要。国際的な動きとも連携しつつ、産業横断的に活用できるソフトウェア管理のあり方について検討。
- 国際的な動きとも連携しつつ、産業横断的に活用できるソフトウェア管理のあり方について検討を開始する。

検討事項（案）

- **構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方**
- **SBOM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題**
- **NTIA等、諸外国機関との連携**



- 利用ソフトウェア・APIの脆弱性管理
- **保守・サポート期間の終了**
- **安全なOSSの選定、評価**
- ライセンスによる制約
- 再委託、再々委託先等の管理
  - 開発環境の管理
  - コーディング規約
- 責任分界

SBOMの活用

- セキュリティの要件定義の能力
- セキュアコーディング
- 脆弱性ハンドリング

- **安全な接続先の選定、評価**
- **SLAの担保**

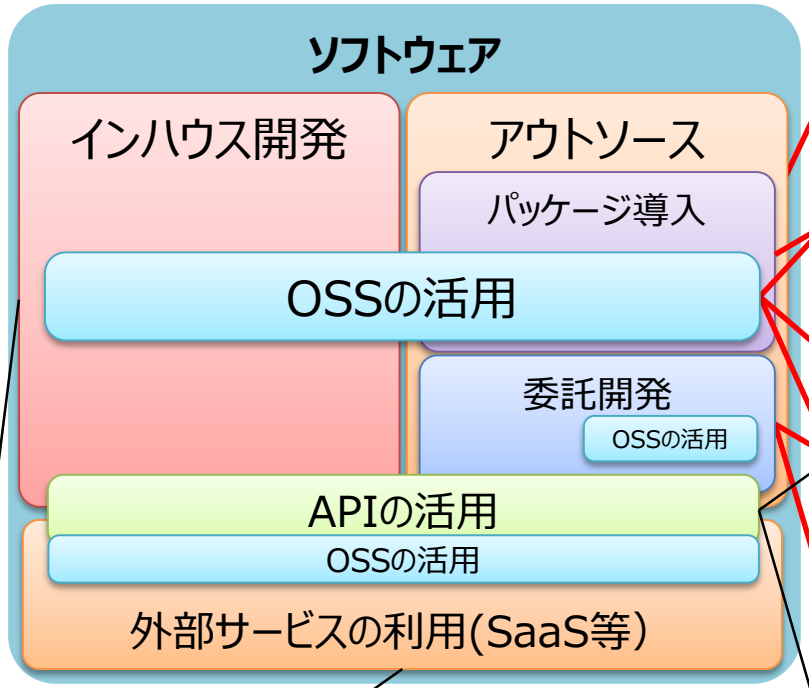
- **安全なAPIの選定、評価**

脆弱性対応手法及びOSSを利活用する際のビジネス的な留意事項等についての検討

- 脆弱性が発覚した際の効果的な対応手法及び既知の脆弱性の管理手法等について検討。
- OSSコミュニティの有効活用も含め、OSS活用のベストプラクティスや、OSS利用時に問題となり得る安全性のリスクやOSSのサポート期間、ライセンスの問題などを整理。

検討事項（案）

- **脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方**
- **運用中システムへの脆弱性対応に求められる技術面・制度面の課題**
- **利用するOSSの安全性を評価するために必要な要件・体制**
- **ビジネスリスクマネジメント／OSS利用に関連するライセンスや契約**
- **OSS活用のベストプラクティス／OSSコミュニティへの発信**



- セキュリティの要件定義の能力
- セキュアコーディング
- 脆弱性ハンドリング

- 安全な接続先の選定、評価
- SLAの担保

- 安全なAPIの選定、評価

SBOMの活用

- **利用ソフトウェア・APIの脆弱性管理**
- **保守・サポート期間の終了**
- **安全なOSSの選定、評価**
- **ライセンスによる制約**
- **再委託、再々委託先等の管理**
  - **開発環境の管理**
  - **コーディング規約**
- **責任分界**

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

２．本タスクフォースの検討事項について

３．国内外の取組について

４．OSSの利活用について

【米国】NTIA Software Component Transparencyに関する議論

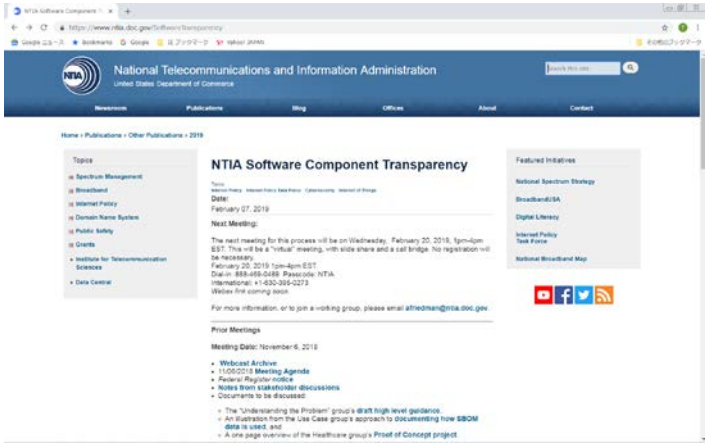
- 2018年、米国NTIA（電気通信情報局）において、「Software Component Transparency」に関するMultistakeholder Meetingが設置された。
- 2019年11月初旬までにNTIA Software Component Transparencyの最初の成果物として、SBOMに関するレポート集が公表された。

ねらい

ソフトウェアの脆弱性情報
理解と処理

成長するIoTマーケットへの対処

安全なソフトウェア開発
ライフサイクルの促進



過去の開催

2018年　7月19日（第1回）
11月 6日（第2回）
2019年　2月20日（第3回）
4月11日（第4回）
6月27日（第5回）
9月 5日（第6回）
11月18日（第7回）

SBOMに関するレポート集（https://www.ntia.gov/SBOM）

1. **Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)**（ソフトウェアコンポーネントトランスパレンシーの構築：共通ソフトウェア部品表（SBOM）の確立）
2. **Roles and Benefits for SBOM Across the Supply Chain**（サプライチェーン全体でのSBOMの役割と利点）
3. **Survey of Existing SBOM Formats and Standards**（既存のSBOM形式と標準の調査）
4. **Healthcare Proof of Concept Report**（ヘルスケアPOCレポート）

【米国】NTIA Software Component Transparency 今後の課題領域

- 2019年11月18日に開催されたNTIA Software Component Transparencyにおいて、同会合の今後の課題領域が特定された。

NTIA Software Component Transparency(11/18)で認識された今後の課題領域			あわせて議論された今後の課題領域の各ワーキンググループへの割り当て
定義と改善 defining and refining	-名前つけ -脆弱性vs開発可能性 -SBoMの共有手法	-完全性、その他高い保証 -クラウド/Saas -「~が含まれる」以上の関係性	■**The Framing Group** SBoM仕様の定義と改善に関する未解決の課題に重点を置く
ツール Tooling	-ドキュメントツール -認識ツールの差異 -ドキュメントプロセス	-即時性の汎用翻訳ツール	■**The Standard Group** ツールに重点を置き、利用可能であるツールとそれ以外のツールとのギャップを認識する
デモンストレーション Demonstrations	-ヘルスケア -その他のセクター -日本のヘルスケア(?)	-特定の企業(?)	■**The Helthcare POC Group** 医療機器分野でのPOCを継続し、コミュニティを支援するデモとPOCのためのアドバイザーとして機能する
ビジネスプロセス Business Processes	-現状のプロセスのドキュメント化 (特に内部的に開発されたソフトウェア) -プレーブック -ユースケースに対して求められるSBoMの マッピング		■**The Usecase Group** 認知と導入、さらには導入を促進するSBoMのビジネスプロセスに重点を置く
認知/採用 Awareness/Adoption	-SBoMのビジネスケースのドキュメント化 -ターゲット化されたエンゲージメントとドキュメント -幅広いエンゲージメントと調和 -共通言語 -ブランディング	-FAQs -共有スライド	

【EU】EU-FOSSA project

- EU-FOSSA (Free and Open Source Software Auditing) プロジェクトは、OpenSSLのHeartBleed発覚後に欧州議会の意向を受け欧州委員会によって開始。
- 2017年からのFOSSA2においては、2019年1月より、15のフリーソフトプロジェクト（7-ZIP、Apache Tomcat等）に対する**バグ発見報酬プログラム**を開始。**報酬の合計は851万ユーロ**に上る。他に、ハッカソンの開催や開発者コミュニティとの関係構築を推進。

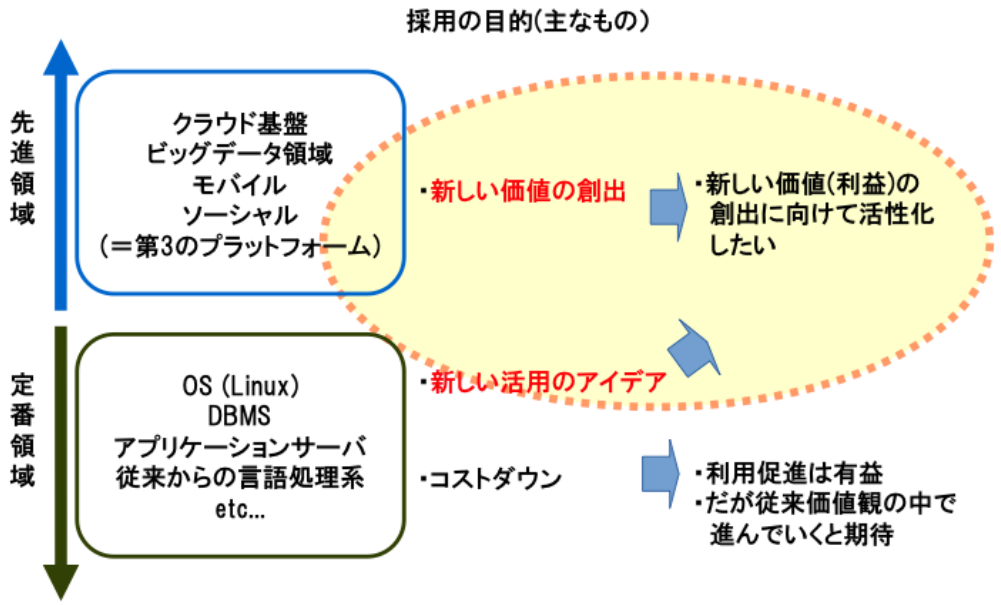
取組１： 脆弱性発見者への報奨金プログラム	HackerOne、Intigritiなどの脆弱性調整及びバグ報奨金プラットフォームを利用し、EUの機関が使う15のフリーソフトウェアプロジェクトを対象に、バグの発見者に報酬を支払う。
	報酬金はプロジェクトにより異なる。報酬金の合計額が最も高いのはPuTTY（リモートログオンクライアント）の9万ユーロ。金額は重要性などに応じて各プロジェクトが決定する。15プロジェクトの合計は851万ユーロ。バグ発見（バグハント）に加え、バグが修正されると20%のボーナス。
取組２： ハッカソンの開催	2019年4月開催の第1回では、ヨーロッパだけでなくキューバ、モロッコ、ロシア等からも参加。230以上の課題解決につながった。5月の第2回では、Apacheプロジェクトから30人以上が参加すると共に、米国やロシア、クロアチア等、世界中から参加者が集まっている。
取組３： 開発者コミュニティとの関係構築	重要なOSSの開発者コミュニティが抱える問題を把握して支援を行うために、コミュニティとの永続的な関係を構築することが重要であるとし、いくつかのオープンソースプロジェクトやコミュニティに対し、定期的な対話の機会を作るためのアプローチを行っている。

https://ec.europa.eu/info/departments/informatics/eu-fossa-2_en

【日本】「クラウドコンピューティング時代におけるオープンソースソフトウェアの活用に関する調査」

- クラウドが広がりを見せる中で、低コスト以外に新技術や付加価値といった点から注目されるOSSが出現。経済産業省では、2015年3月にOSSの利用状況を調査するとともに、OSSの活用による「攻めのIT経営」に向けた提言を公開。
- OSSを利用する理由・背景は、①コスト削減、②ロックイン回避、③自社サービス差別化、④エンドユーザの要望の順となっている。

OSSのターゲット： 従来はコストダウン中心であったが、近年はより高付加価値、ユーザへのサービス寄りにも広がる。



アンケート結果では「定番領域」の回答が多いものの、先進領域への回答も一定数みられる。

（1） OSS を利用する理由／背景

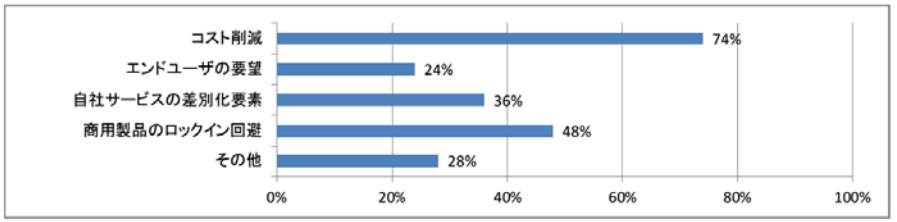


図 7-5 回答：OSS を利用する理由／背景

以下、個別回答（その他意見としての回答）を抜粋。

- 環境構築、開発スピードの迅速化
- セキュリティ、不具合の情報の広く迅速に公開されるため、安心
- 情報量が豊富

（自由回答より）

- 日本ではOSS は誰も責任を取ってくれないリスクの高いもの、と考えるが、**海外では100%中を見られるOSSの方が安全**で、特定の会社にしか中身がわからない方が危険、という考え方が主流。
- エドワード・スノーデンの事件で**ITインフラもオープンなものを使う重要性が認識**されてきた。つまりOSS推進の背景の1つにはセキュリティという観点がある。

https://www.meti.go.jp/meti_lib/report/2015fy/000438.pdf

【日本】「ソフトウェア識別管理に向けた分析事業」の報告書

- 2016年3月、IPAは、ソフトウェア及び各種属性情報（脆弱性情報等）を管理し、それをすばやく参照できる「ソフトウェア属性情報管理」の仕組みづくりに向けた実態調査、課題抽出のための調査を行った。

報告書の主な構成

第2章（属性情報管理検討）
- ソフトウェア属性管理の必要性（必要性高）、管理が必要な情報（ライセンス、トレース、脆弱性）、管理の実態（OSSは企業規模により格差が発生）

第3章（SWIDタグ活用）
- 脆弱性対策に関わる処理の機械化を目指すフレームワークMyJVN（JVN 脆弱性対策機械処理基盤）
- JVN 脆弱性対策機械処理基盤のツールを対象に実施したSWIDタグ付与の試行

第4章（標準化動向）
- 米国（特に国防総省）が中心となり、ソフトウェアの出所管理を行うための標準化活動

第5章（まとめ）
- 属性情報管理は、認識されつつも出来る範囲に留まり、各企業／団体の責任にとどまる

https://www.ipa.go.jp/files/000051147.pdf

注目すべきポイント

	項目	内容
1	ソフトウェアの属性情報の項目の一覧化	製品名、ライセンス、トレース、脆弱性、開発元、品質、使用実績、市場評価（ヒアリングで重視判明は赤字） 脆弱性情報は、概要・影響を受けるシステム・脆弱性詳細・想定される影響・対策方法の各項目
2	OSSにおける属性情報管理実態	一部大企業ではOSS専門組織が管理するも、大半ではソースプログラムの管理ができていない。加えて、（自由に利用できるため）派生ソフトが多く、脆弱性のあるソフトの混入の可能性が高い。これに対して、一部企業は民間のOSS照合サービスを利用
3	ソフトウェア属性情報基盤の構築実現への見通し	ライセンス情報、トレース情報については、当該ソフトウェアの提供元による登録制にすれば実現可能（ただしコスト面の解決が必要） 脆弱性情報は、既存の組織（NIST等）のデータベースとのリンケージ、相互利用の仕組みの実現に期待
4	JVN脆弱性対策機械処理基盤のツールでのSWIDタグ付与試行	ISO/IEC 19770-2に基づくソフトウェアへのタグであるSWIDは米国でも「SBOM」としての活用も有力だが、日本の脆弱性対策情報基盤JVNへの適用試行結果が整理されている。現在のSWIDはEntityやMetadataタグの（日英）複数記載が用意されていないため、その用意がととのえば実現する可能性があるとのまとめ

【日本】「IoT時代におけるOSSの利用と法的諸問題Q&A集」

- 2018年3月、一般財団法人ソフトウェア情報センター（Softic）は、OSS を利用する上での法的諸問題やビジネスを展開する上での疑問点について、Q&A集として取りまとめた。
- OSSのライセンス関係、システム開発責任、混入チェック、コミュニティ関係等幅広く留意すべき点について取りまとめている。

本書の構成

- 基礎（OSSのライセンス、ビジネスモデル、利用形態、関連法令、ベンダの責任等）
- 関係する立場の違いから見た留意点（自社ソフトウェアへの組み込み、自社ソフトウェアのOSS化、OSSソフトウェアの利用、クラウドサービスとしての利用）
- 各課題領域　（OSSの両立/混入、教育、サポート・セキュリティ（脆弱性）、管理）
- 取引上の留意点　（免責事項）、契約条項、会計税務処理）
- GPLその他のライセンス上の留意点（表示、解釈、GPL伝搬）
- コミュニティ・OSS関連団体
- 知財問題
- トラブル事例（裁判、トラブル、法的責任）
- OSSの今後の動向

https://www.softic.or.jp/ossqa/all_180328_mc.pdf

注目すべきポイント

	項目	内容
1	ライセンスの種類、条件、注意事項の一覧化	主なOSSライセンス（GPLv2,Apache Ver.2.0等）とライセンス要件（表示、承継、ソースコード提供、免責等）を一覧化し、注意事項についても、自社製品、他社提供、クラウド型等様々な立場向けに解説を提供
2	セキュリティを含む事前、事後措置への言及	事前に留意すべき点としてOSSの両立性、教育、管理、脆弱性対策等セキュリティ面での対策に言及するとともに、バグを発見した場合の（IPAが受付機関となる）情報セキュリティ早期警戒パートナーシップによる通報を紹介
3	ライセンス、知財に関する詳細な解説	Q&A形式で適切な対処方針を紹介。例えば、条項が不明・難解な際の参照先、自社開発プログラムとの連動時の対応、ソースコードを請求された際の対応等
4	訴訟を含むトラブル事例の解説	米国におけるGPL条項違反を中心に海外の8件の訴訟の内容（2件はドイツ）の概要、判決とともに、トラブルの分類として、ライセンスの非両立、特許侵害、意図せぬOSS混入、セキュリティ対策責務をあげ、トラブル時の対応策（違反是正、社外コミュニケーション等）も紹介

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

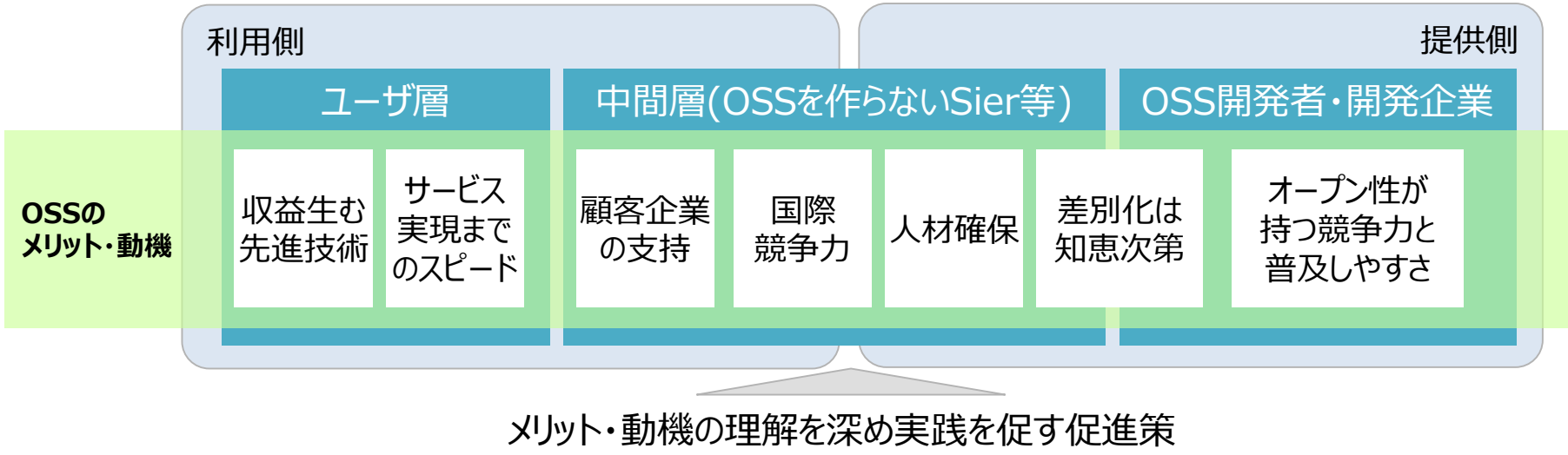
２．本タスクフォースの検討事項について

３．国内外の取組について

４．OSSの利活用について

OSSを利活用するメリット

- 「クラウドコンピューティング時代におけるオープンソースソフトウェアの活用に関する調査」では、OSSを利用するメリット・動機を以下のように整理。
- 他方、これまでの会合でも指摘があったように、OSSを利活用する際には、**留意点を考慮することも重要。**



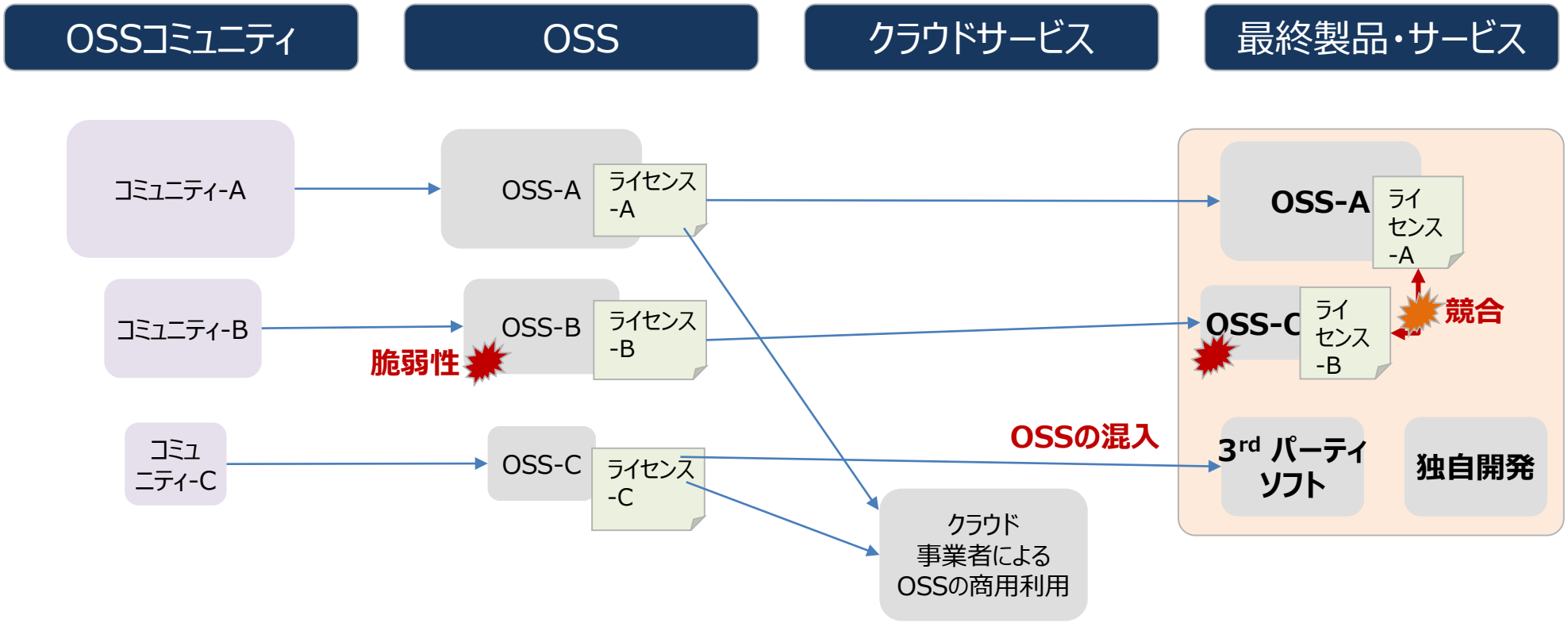
※図は2017年3月 経済産業省委託調査「クラウドコンピューティング時代におけるオープンソースソフトウェアの活用に関する調査事業」を参考に作成

留意点に関する指摘（第1回、第2回会合より）

・OSS開発者とユーザの利益を折衷させることが非常に大事。　・OSSのサポートは止まる場合がある。
・OSSプロジェクトは品質の評価がされておらず将来も約束されていない。
・OSSやレポジトリそのものがそもそも信頼できるのか。　・OSSコミュニティの対応を待てないケースが多い。
・きちんと開発が継続されるものを選ぶことが大前提だが、それでも開発が停滞したり止まったりする。

OSSを利活用する際の留意点

- OSSの作成から製品・サービスでの利用のサイクルの中で、留意点を以下のとおり整理。



留意点	・コミュニティの活動の透明性 ・コミュニティへの貢献	・OSSの信頼性 ・OSSの持続性 ・OSSへの貢献	・クラウド事業者がOSSを使う際の条件付け ・SLAの締結	・ライセンス違反 ・意図せぬOSSの混入 ・ライセンスの競合 ・脆弱性対応

OSSを利活用する際の留意点

留意点				
	・コミュニティの活動の透明性 ・コミュニティへの貢献	**・OSSの信頼性** **・OSSの持続性** **・OSSへの貢献**	・クラウド事業者がOSSを使う際の条件付け ・SLAの締結	・ライセンス違反 **・意図せぬOSSの混入** ・ライセンスの競合 **・脆弱性対応**

- 開発者がメンテナンスの意欲を失った広く利用されているライブラリについて、攻撃者が開発者からメンテナンスを引き継ぎ正規に権限を取得し、悪意あるコードを埋め込むという、OSSそのものが信頼できない事例が報告されている。（Copayの事例）

2017.10 ・開発者によるevent-streamの最終更新

⋮

2018.8末 ・攻撃者がevent-streamの開発者に**「メンテナンスを引き継ぎたい」と持ちかけメンテナンス権限を取得**

2018.9.9 ・攻撃者がevent-streamを更新 → event-streamがflatmap-streamと関連

2018.10.5 ・攻撃者がflatmap-streamに**悪意のあるコードを追加**

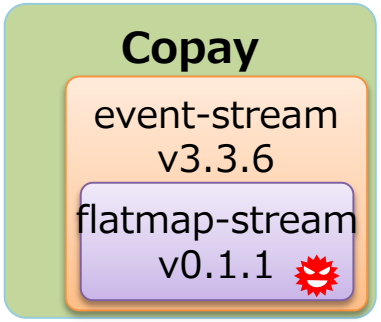
2018.10.26 ・Copayが更新

→ Copayが悪意のあるコードが仕込まれたflatmap-stream に関連するようになり、攻撃者がバックドアを利用できるように

⋮

2018.11.26 ・ニュースになり、 flatmap-streamは削除された

【Copay】
event-streamの開発者は、OSSコミュニティでなぜ権限を譲ったのか聴かれ、このモジュールをもう使っていない上、メンテナンスをしても開発者が得られるものもない。権限譲渡に憤るならばなぜボランティアでメンテナンスしようとしなかったのか、というような趣旨のコメントをしている。



OSSを利活用する際の留意点

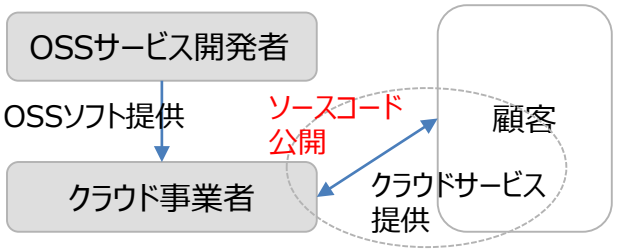
留意点				
	・コミュニティの活動の透明性 **・コミュニティへの貢献**	・OSSの信頼性 ・OSSの持続性 **・OSSへの貢献**	**・クラウド事業者がOSSを使う際の条件付け** **・SLAの締結**	・ライセンス違反 ・意図せぬOSSの混入 ・ライセンスの競合 ・脆弱性対応

- 大手OSSコミュニティがAWSなどクラウドベンダがOSSを利用して莫大な利益を上げていることに反発し、商用サービスを制限するライセンス変更を行っていることが報告されている。

Server Side Public License (SSPL)　（クラウドベンダーによるライセンス利用の制限）

MongoDBが独自に作成したもので、サービスとして提供する場合、サービス提供元が独自に変更した部分を含めてソースコードを無償で公開しなければならない。

https://www.publickey1.jp/blog/19/mongodbsspldebianfedorarhelmongodb.html



クラウドインフラ・プロバイダーの勝手は防ぐべきという見方

- MongoDBがSSPLをオープンソース・イニシアチブ（OSI）という組織に提出したが、その承認を待たずにSSPLライセンスのもとでソフトウエアの販売を開始
- クラウドインフラ・プロバイダーの勝手を防ぐ、開発者のためのオープンソース・ライセンスが他にない。開発者には、それを可能にするライセンスを用意するべきだ。

https://jp.techcrunch.com/2018/12/04/2018-11-29-the-crusade-against-open-source-abuse/

商用サービスを制限するライセンス変更が相次いでいる

- 「Kafka」の開発元であるConfluentも、同社が提供するKafkaの一部のコンポーネントである「KSQL」「Confluent Connectors」「REST Proxy」「Schema Registry」などのライセンスを変更。商用サービスでの利用を制限
- オープンソースを開発する企業がこうした大手クラウドベンダによる「いいとこ取り」を許さず、ライセンスを通じてその利用形態に一定の影響力を持とうとして、具体的なアクションをとりはじめた

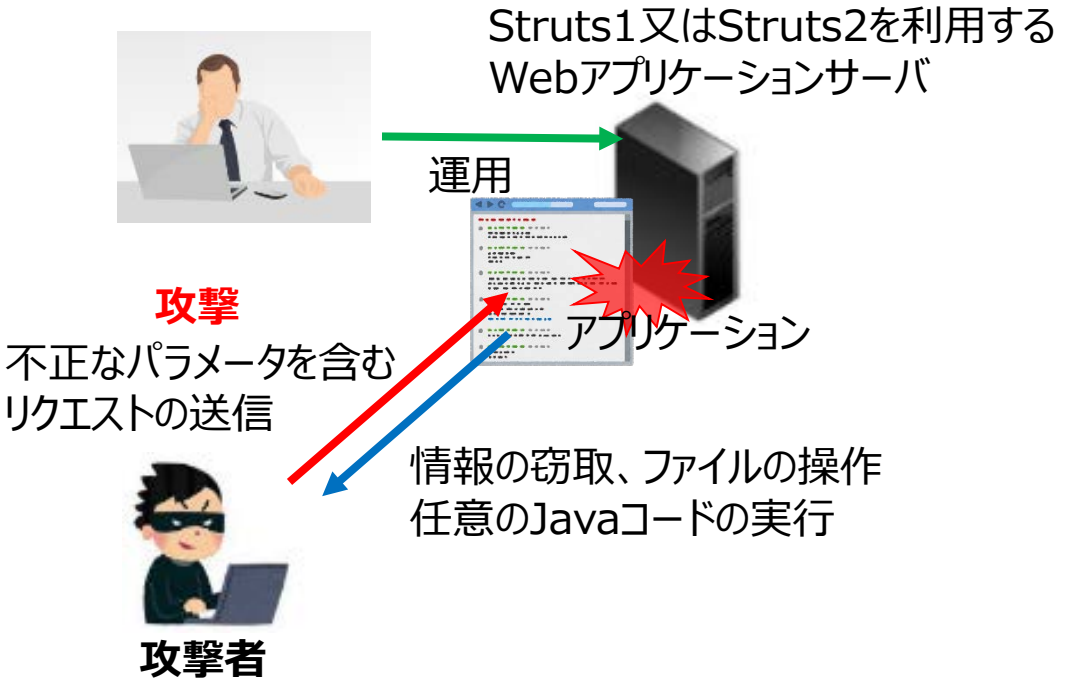
https://www.publickey1.jp/blog/19/redismongodbkafkaaws.htm

OSSを利活用する際の留意点

留意点				
	・コミュニティの活動の透明性 ・コミュニティへの貢献	・OSSの信頼性 ・**OSSの持続性** ・OSSへの貢献	・クラウド事業者がOSSを使う際の条件付け ・**SLAの締結**	・ライセンス違反 ・意図せぬOSSの混入 ・ライセンスの競合 ・**脆弱性対応**

- サポート終了後に大きな脆弱性が見つかった事例が報告されている。

【Apache Struts】2014年4月にApache Struts2について公表された脆弱性が、その後、既にサポートが終了しているApache Struts1にも存在することが判明。開発元からの修正パッチの提供はなく、またStruts2へのバージョンアップも容易でないことから、サービスを停止するシステムが出た。



Struts1を利用しており、停止した公共サービス例

政府機関等	製品・サービス
国税庁	確定申告書等作成コーナー等
IPA	ITパスポート受付システム
島根県警	遺失物公開システム
みやま市図書館	ＷＥＢ蔵書検索サービス
	etc…

OSSを利活用する際の留意点

留意点			
・コミュニティの活動の透明性 ・コミュニティへの貢献	・OSSの信頼性 ・OSSの持続性 ・OSSへの貢献	・クラウド事業者がOSSを使う際の条件付け ・SLAの締結	**・ライセンス違反** **・意図せぬOSSの混入** ・ライセンスの競合 ・脆弱性対応

● ライセンス違反や意図せぬOSSの混入の事例が報告されている。

1、OSSのライセンス違反の事例

EPSON KOWA

同社は、Linux向けのプリンタドライバやスキャナ用ソフトウェアでGPL違反を起こした（GPLと非GPLのソースコード及び非公開のバイナリについて個々のライセンスを明確にせず二次配布）が、ライセンスを適切なものに変更したことで、企業イメージを損なわず

→違反時の適切な対応の好事例として紹介
（http://ossforum.jp/en/node/806）

Panasonic Avionics

2017年3月に同社が開発した航空機内エンタテイメント（IFE）ソフトが米国企業からGPL違反を訴えられた（故意にソースコード開示拒否と主張し1億ドルの賠償請求）
→2018年1月和解

2、意図せぬOSSの混入：M&Aや第三者への開発委託等による場合

①Cisco：Linksys(無線ルータ)における訴訟(2009年)

- 「Linksys」という無線ルータに，GPLで公開されている 複数のプログラムが利用されていた。そのソースコードを公開していないと提訴され、違反を認め和解
- 訴訟が提起される５年前にLinksys(会社)を買収していた。GPL違反の製品は、Linksysの製品に存在していた

https://www.hibiyapark.net/wp-content/uploads/2018/05/c484e7e1251d2ed577a08fc47179d1e4.pdf

②CNSR(フランス国立科学研究センター):Bagheraにおける訴訟(2007年)

- IT企業のEducaffixが、研究機関CNRSらからBagheraという商用ソフトウェアを購入後Baghera にGPLで公開されているOSS が含まれていたことが判明
- 同社は譲渡契約の解除を求めて提訴。裁判所は独自開発部分もソースコードを公開する義務を負い、契約の目的が達成できないと譲渡契約の解除を認めた

https://www.hibiyapark.net/wp-content/uploads/2018/05/c484e7e1251d2ed577a08fc47179d1e4.pdf

③コピーライトトロール

- ドイツでさまざまなLinuxディストリビューターのライセンス違反を見つけ、密かに訴訟手続きをとっては多額の金銭を要求していたことが判明
- Linux FoundationやRed Hatを中心とした大手各社が対策を本格化

https://opensource.com/article/17/8/patrick-mchardy-and-copyright-profiteering
https://www.excite.co.jp/news/article/Slashdot_17_10_19_0622235/
https://securityboulevard.com/2019/05/advancing-open-source-innovation-in-cybersecurity/

OSSを利活用する際の留意点

留意点				
	・コミュニティの活動の透明性 ・コミュニティへの貢献	・OSSの信頼性 ・OSSの持続性 ・OSSへの貢献	・クラウド事業者がOSSを使う際の条件付け ・SLAの締結	・ライセンス違反 ・意図せぬOSSの混入 **・ライセンスの競合** ・脆弱性対応

- ライセンスの競合の事例が報告されている。１つのプログラムに２つ以上のOSSライセンス（例: GPLv2とApache 2.0）が重畳的に適用された場合、両立できない可能性がある

複数OSS非両立性の事例

Apacheライセンスのバージョン２

OSSを配布した者に，そのOSSを利用する者に対して特許をライセンスする義務を課している

⇕ 矛盾

GPLバージョン２（GPLv2）

GPLv2で定められていない追加的な義務を課すことを禁止しているが、GPLv2には，Apache2.0ライセンスの特許ライセンス義務に相当する規定はない

GPLv2を策定・公開している米国のフリーソフトウェア財団（FSF）はGPLv2はApache 2.0ライセンスとは両立性を欠くという見解を表明

GPLv2で公開されているOSS（フリーソフト）を入手してソースコードを改変したものを，Apache 2.0ライセンスで公開することはできない

GPLv2で公開されているOSSのプログラムＡと，Apache 2.0ライセンスで公開されているOSSのプログラムＢをリンクして１つのプログラムにして配布することもできない

参考）OSSライセンス遵守のための基礎知識（上山浩）（知財管理Vol.68 No5(2018)
https://www.hibiyapark.net/wp-content/uploads/2018/05/c484e7e1251d2ed577a08fc47179d1e4.pdf