資料５－５

ICTサイバーセキュリティ政策分科会第5回会合

R5年度「通信分野におけるSBOMの導入に向けた調査の請負」について

KDDI株式会社

2024年 4月 5日

背景と目的

【背景】

- 通信分野においては、仮想化の進展に伴い、オープンソースソフトウェア（OSS）の利用が急速に普及拡大しており、ソフトウェア・サプライチェーンは、自社開発の専用ソフトウェアの単純な組合せから、**多数のOSS等の複雑な組合せへと変化**。これにより、通信分野におけるソフトウェアの構成管理が複雑化。
- また、通信インフラの長期運用性によって、通信インフラには**新旧様々なバージョンのソフトウェアが混在**している状況であり、ソフトウェアのバージョン管理を含む構成管理が複雑化。
- これらの事情を踏まえ、**ソフトウェア部品の脆弱性が確認された場合の対応を迅速化**するため、通信分野においてソフトウェアを構成する部品名等を一覧化した**SBOM（Software Bill of Materials）**を導入する重要性が増加。

【目的】

- 我が国の通信分野におけるソフトウェア構成管理を巡る現状を踏まえて、ソフトウェア部品における**脆弱性管理**のための手法としてのSBOMの有効性を検証するとともに、通信事業者が実際に**SBOMを運用**していく上での課題等を整理することで、「**通信分野におけるSBOM導入に当たっての留意事項**」（仮称。以下「留意事項」という。）を取りまとめることを目的とする。

1　事業概要

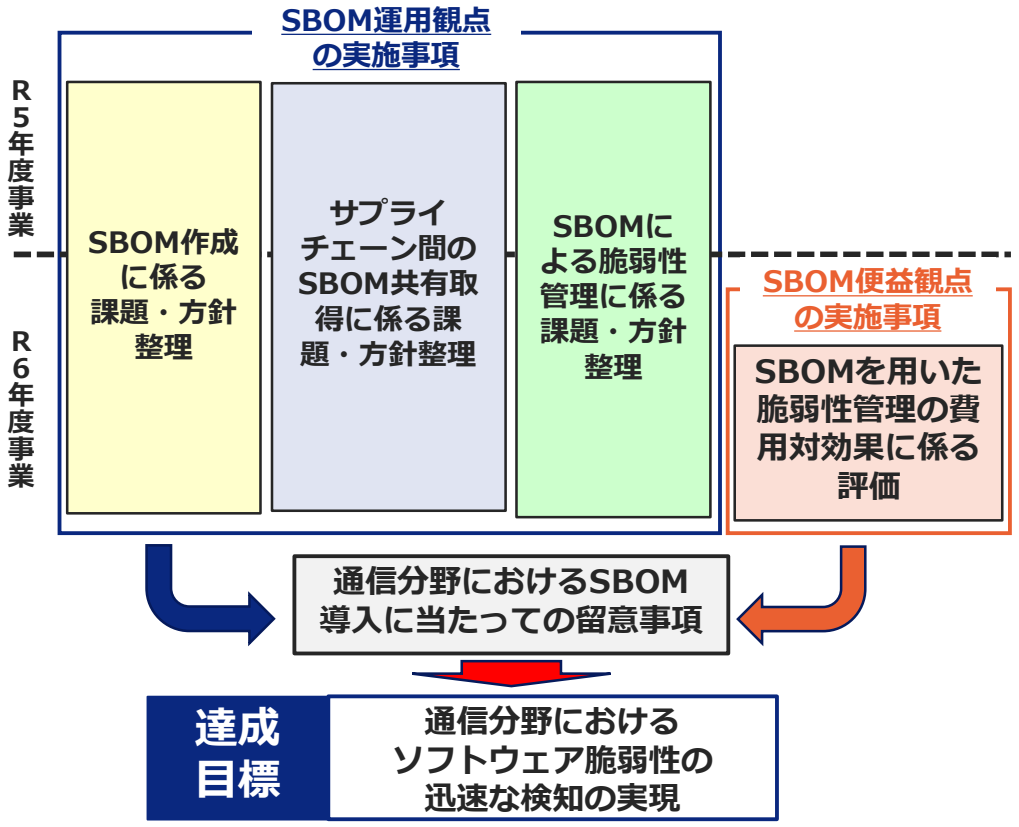
- 本事業では、通信分野におけるソフトウェア脆弱性の迅速な検知の実現に向けて、SBOM導入観点及びSBOM運用観点で実施すべき事項を整理し、R6年度末に「留意事項」を取りまとめる。
- R5年度事業では、SBOM運用観点の実施事項としてSBOM作成に係る課題整理のため、通信機器2台に対して以下の2つの手法でSBOMを作成・評価を行う。

① 通信事業者が複数のSBOM作成ツールを用いて「**ツール版SBOM**」を作成

② 通信機器ベンダ及び一部のソフトウェアサプライヤが手作業により抜け漏れの無い網羅的な「**手動版SBOM**」を作成（「ツール版SBOM」の正確性を検証するための比較対象として作成）

- また、上記に加えて、SBOM活用に係る課題の整理等のためのSBOMを用いた脆弱性管理の検証や国内外における動向調査を実施。

事業全体像



実施内容

分類	実施事項	取組内容	R5年度事業	R6年度事業
SBOM運用観点の実施事項	SBOM作成に係る課題・方針整理	SBOM作成・評価 R5・R6で別機器を選定	通信事業者による「ツール版SBOM」を作成 ソースコード等から手作業で「手動版SBOM」を作成 ※手動版SBOMは膨大な作成コストがかかるため実証目的でのみ作成 ツール版及び手動版SBOMに係る比較評価	SBOM作成・評価に係る実証
	サプライチェーン間のSBOM共有取得に係る課題・方針整理	取引モデルの策定		取引モデルの検討
	SBOMによる脆弱性管理に係る課題・方針整理	脆弱性管理に係る検証	作成したSBOMと脆弱性情報との照合及び検査項目の抽出の検査実証	脆弱性情報との照合
SBOM導入観点の実施事項	SBOMを用いた脆弱性管理の費用対効果に係る評価	SBOM活用による費用対効果算出	SBOMの効果・効率に関するKPIの明確化	費用対効果算出
		国内外動向調査	欧米を中心に、SBOMに関するガイドラインや法令等の整備状況等を調査	国内外動向調査
留意事項の作成			「留意事項」項目整理 ★	「留意事項」公表 ★

2　SBOM作成・評価（対象となる通信機器）

- 本事業において、SBOM作成の対象とする通信機器は、通信事業者が実際に使用している、または、使用する予定の機器であり、構成要素としてソフトウェアが含まれること等を条件に選定。
- SBOMを作成する通信機器①・通信機器②の概要は以下のとおり。

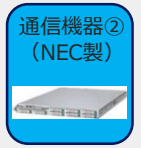
	通信機器①	通信機器②
機器ベンダ	**富士通株式会社**	**日本電気株式会社（NEC）**
対象機器	**DU**※1 通信機器① （富士通製） 	**vMVNO-GW**※2 通信機器② （NEC製） 
主な機能	■ 無線リソース割り当て等のメディアアクセス制御（MAC※3） ■ 再送制御（RLC※4）	■ 仮想的にネットワークを分離するAPN機能 ■ 帯域制御等の総量規制機能
選定理由	■ 今後普及が見込まれるOpen RANに関連した機器であり、OSSの活用が進んでいるため。 ■ オープン化に伴い、セキュリティ対策の強化が要請されているため。 ■ O-RAN ALLIANCEにおいてSBOMに関するセキュリティ要件が規定されているため。	■ MVNOにおいて実際に商用設備として、使用されている機器であり、構成要素としてソフトウェアが含まれているため。 ■ 複数のソフトウェア部品で構成されているため。
ソフトウェア部品数	■ SW#1～#6の6つ。	■ アプリケーションソフトウェアとミドルウェアの2つ。

※1：Distributed Unit
※2：virtualized Mobile Virtual Network Operator
※3：Media Access Control
※4：Radio Link Control

2　SBOM作成・評価（SBOM標準フォーマットの選定）

- 本事業で使用するSBOM標準フォーマットは、米国NTIA※1が定めるSBOMの「最小要素※2」で指定されている、CycloneDX、SPDX※3 SWIDタグ※4のうち、主なSBOM作成ツールが対応しているCycloneDXとSPDXを使用する。
- 通信機器①・通信機器②に対する標準フォーマットの割り振りは以下のとおり。

  通信機器①　⇒「**CycloneDX**」：OWASPコミュニティがセキュリティに特化したSBOMフォーマット標準として開発した標準フォーマット
  通信機器②　⇒「**SPDX**」：The Linux Foundation傘下のSPDX WGがSBOMフォーマット標準として開発した標準フォーマット※5

項目	CycloneDX	SPDX
正式名称	CycloneDX specification	Software Package Data Exchange
仕様	CycloneDX 1.4 （JSON形式）	SPDX Specification v2.2 （Tag: Value形式）
標準化	–	ISO/IEC 5962: 2021 （SPDX v2.2.1）
ファイル形式	XML、JSON、Protocol Buffers（protobuf）	tag-value、RDF、XML、xls/xlsx、JSON、YAML
サポート団体	The OWASP Foundation支援の CycloneDX Core Working Group	The Linux Foundation傘下のSPDX Working Group
SBOM作成対象機器	通信機器① 	通信機器② 

※1：National Telecommunications and Information Administration

※2：NTIA, The Minimum Elements For a Software Bill of Materials (SBOM)
https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

※3：Software Package Data eXchange

※4：Software Identification tags

※5：Linux Foundation Projectの１つであるOpenChain Telco WGでは、SPDXをベースに通信業界のSBOMを検討している。

2　SBOM作成・評価（通信分野において着目すべきSBOM項目の検討）

- 標準フォーマットであるCycloneDXとSPDXの全項目に対して、通信分野において必要な項目を精査するとともに、**NTIAが定めるSBOMの「最小要素」**や**OpenChain Telco WGが検討する通信業界のSBOM仕様**（検討当時）等に関する文献を調査し、通信分野において着目すべきSBOM項目を決定。
- 通信機器①・通信機器②に対して作成するSBOM項目は以下のとおり。

通信分野において着目すべきSBOM項目の検討

NTIA最小要素

・サプライヤ名
・コンポーネント名
・コンポーネントのバージョン
・その他の一意な識別子
・依存関係
・SBOM作成者
・タイムスタンプ

SBOM項目検討　　SBOM項目検討

Draft Proposal for an OpenChain Telco SBOM Specification Version 1.0
通信業界向けSBOM仕様（当時）

O-RAN Security Requirements Specification 6.0　等
O-RANシステムに対するセキュリティ要求事項
SBOMに関する要求事項

通信機器①　：通信機器として着目すべきSBOM項目　（CycloneDX）

No.	項目	補足補足(記載例等)
1	SBOMファイル 作成者	
2	SBOMファイル タイムスタンプ	
3	コンポーネントのサプライヤ名	
4	コンポーネント名	
5	コンポーネントのバージョン	
6	コンポーネントの一意の識別子	NTIA最小要素 & O-RAN Alliance SBOM仕様より選定
7	コンポーネントの依存関係	
8	SBOMファイルのフォーマット情報	（推奨）例：CycloneDX ver1.4
9	SBOMファイルのライセンス	（推奨）例：CC0-1.0 (固定値)
10	SBOMファイルの識別子	（推奨）例：URIなど
11	コンポーネントの外部参照	（推奨）例：CPE or パッケージURL(purl)など
12	コンポーネントのハッシュ値	（推奨）
13	コンポーネントのライセンス情報	（推奨）　Open Chain Telco-WG SBOM仕様（当時）より選定
14	コンポーネントのコピーライト	（推奨）
15	**SBOMファイルに関するコメント**	（推奨） 例) 以下の**通信分野向けセキュリティ要件**に準拠 ・O-RAN Security Requirements Specification 6.0 ・O-RAN Security Test Specifications 4.0 ・O-RAN Security Protocols Specifications 6.0

ベンダ観点で、留意すべきSBOM項目として提案

通信機器②：　通信機器として着目すべきSBOM項目（SPDX）

No.	項目	補足説明（記載例等）
1	SBOM記述に用いたSPDXのバージョン	“SPDX-2.2”を記載（固定値）
2	SBOMメタデータのライセンス	“CC0-1.0”を記載（固定値）
3	SBOMドキュメントの識別子	“SPDXRef-DOCUMENT”など
4	SBOMドキュメントの名前	SBOMのファイル名
5	SBOMドキュメントの名前空間	一定の形式でURIを生成
6	SBOMドキュメントの作成者	
7	SBOMドキュメントの作成日時	
8	SBOMドキュメント作成者のコメント	CISA※1のSBOM Typeを記載
9	パッケージ名	
10	パッケージの識別子	URIなど　NTIA最小要素 & Open Chain Telco-WG SBOM仕様（当時）より選定
11	パッケージのバージョン	
12	**パッケージのファイル名**	**脆弱性管理対象の実体を特定するための情報として追加選定**
13	パッケージのサプライヤ名	通信インフラの信頼性・持続性の点でも重要
14	パッケージのダウンロード場所	
15	ファイル自動解析の有無	
16	パッケージのチェックサム	通信インフラ構成要素の完全性担保に重要
17	SBOM作成者が判断したライセンス	
18	パッケージ作成者が宣言したライセンス	NTIA最小要素 & Open Chain Telco-WG SBOM仕様（当時）より選定
19	パッケージのコピーライト記述	
20	**依存関係**	関係の種類としてNTIA最小要素に準じたDESCRIBES, CONTAINSに加え、**DEPENDS_ON, COPY_OF**の計4種を選定

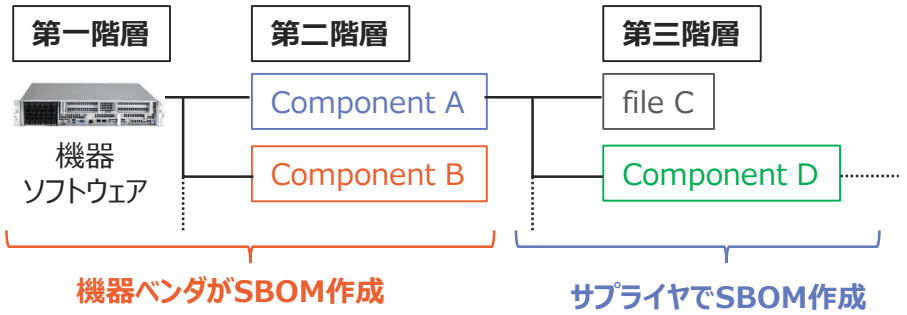
その他にも外部参照に関する項目等を記載可能。
本事業では「外部参照」の項目にCPE名を記載。

2　SBOM作成・評価（抜け漏れの無い網羅的な「手動版SBOM」の作成）

- 通信機器ベンダ及び一部のソフトウェアサプライヤが、SBOM作成ツールから出力したSBOMを基に、ソースコード等を確認しながら手動追記して作成した手動版SBOMを統合して、抜け漏れの無い網羅的な「**手動版SBOM**」を作成。
- 「手動版SBOM」を作成した結果、ソフトウェアのコンポーネント数が通信機器①は**467個**、通信機器②は**73個**使用されていることを確認。

手動版SBOMの作成方法

SBOM作成の役割分担



手動版SBOM作成イメージ

➢ 機器ベンダ及びソフトウェアサプライヤが作成した手動版SBOMを統合することによって全体のSBOMを作成

通信機器①のSBOM作成（CycloneDX）

■SW部品、通信機器のSBOM作成結果(コンポーネント数)

ソフトウェア	コンポーネント数
SW#1（ベンダ）	145
SW#2（サプライヤ）	389
SW#3（サプライヤ）	206
SW#4（サプライヤ）	155
SW#5（サプライヤ）	232
SW#6（サプライヤ）	155
SW#1～6をマージした全OSS数（重複するOSSは除外）	**467**

➢ 必須項目のうち、「サプライヤ名」「依存関係」はツール出力されず、全コンポーネントに対して手動追記を実施

➢ O-RAN関連機器であるため、通信機器②よりもソフトウェアコンポーネント数が多いことを確認

通信機器②のSBOM作成（SPDX）

■SW部品、通信機器のSBOM作成結果(コンポーネント数)

ソフトウェア	コンポーネント数
アプリケーションソフトウェア(ベンダ)	28
ミドルウェア(サプライヤ)	71
マージした全OSS数（重複するOSSは除外）	**73**

➢ 主に、プロプライエタリなソフトウェアで構成されているため、ツール出力できず、ほぼ全て手動でSBOM作成を実施

■ アプリケーションソフトウェア、ミドルウェアから直接使用するOSSが対象

■ ディストリビュータ（ベンダ以外）提供OSSの情報は、ディストリビュータ情報に加えて、OSSオリジナル配布元の情報を調査して補完

2　SBOM作成・評価（SBOM作成ツールの選定）

- 機器ベンダ等が作成する「手動版SBOM」と汎用的なSBOM作成ツールを使用して作成した「ツール版SBOM」の比較分析を実施し、**「ツール版SBOM」の網羅性等の精度を検証**。
- 「ツール版SBOM」を作成するためのSBOM作成ツールは、CycloneDXまたはSPDXのどちらか一方を出力可能であることを最低条件として、以下の機能を有する**有償ツール2つ**、**無償ツール4つを**選定。

	有償	有償	無償	無償	無償	無償
	ツール①	ツール②	ツール③	ツール④	ツール⑤	ツール⑥
提供形態	オンプレミス（サーバ構築必要）	SaaS	オンプレミス（サーバ構築必須）	オンプレミス（サーバ構築必要）	スタンドアロン	スタンドアロン
CycloneDX出力	○	○	○	×	×	○
SPDX出力	○	○	○	○	○	×
ファイルマッチング解析	○	○	×	×	×	×
バイナリ解析	○	×	×	×	×	×
コンテナ解析	○	○	○	×	×	×

＜参考：解析方法の種類＞

	概要
ファイルマッチング解析	解析対象のソフトウェアファイルのハッシュ値等の識別情報と解析ツールのデータベース等に保管されているOSSの識別情報をマッチングして、ソフトウェア構成を解析する方法。
バイナリ解析	解析対象のバイナリファイルの特定の一部分のビットパターン等と解析ツールのデータベース等に保管されているOSSのビットパターン等をマッチングして、ソフトウェア構成を解析する方法。
コンテナ解析	解析対象のコンテナイメージの構成や設定ファイル等を解析することで内包するソフトウェア構成を解析する方法。

2　SBOM作成・評価（「ツール版SBOM」の比較評価）

- ツール①～ツール③※1で作成した「ツール版SBOM」において、**コンポーネント数及び依存関係**※2や**「通信分野において着目すべき項目」の出力有無**について「手動版SBOM」と比較・分析し、「ツール版SBOM」の精度評価を実施。
- 通信機器①の「ツール版SBOM」は**検出不足や過剰検出**が確認されたが、検出されたコンポーネントにおいては依存関係・サプライヤ名以外、「通信機器として着目すべき項目」を満たしていた。
- 通信機器②の「ツール版SBOM」は**検出不足**が確認され、検出されたコンポーネントにおいては依存関係を除き、「通信機器として着目すべき項目」を満たしていた。

通信機器①に対して作成したツール版SBOMの評価（CycloneDX）

- 通信機器①のツール版SBOMはコンポーネント数及び依存関係に**検出不足や過剰検出**を確認
- ソースコードに対するファイルマッチング解析で出力されたSBOMとコンテナ解析で出力されたSBOMではSBOMの精度に大きな差異を確認
- ツールで検出できたコンポーネントにおいて、依存関係、サプライヤ名以外の「通信機器において着目すべき項目」は全て出力できた

項目	SBOMの各項目の出力件数						
	手動版SBOM※3	ツール版SBOM					
		コンテナスキャン			ソースコードスキャン		
		ツール①	ツール②	ツール③	ツール①	ツール②	ツール③
コンポーネント	1098	767	–※4	1203	3	33	18
依存関係	1132	（出力されない仕様）	–※4	1065	（出力されない仕様）	33	（出力されない仕様）

通信機器②に対して作成したツール版SBOMの評価（SPDX）

- 通信機器②のツール版SBOMはコンポーネント数及び依存関係に**検出不足**を確認
- ツールで検出できたコンポーネントにおいて、依存関係以外の「通信機器において着目すべき項目」は全て出力できた

項目	SBOMの各項目の出力件数			
	手動版SBOM※3	ツール版SBOM		
		ツール①	ツール②	ツール③
コンポーネント	139	2	8	2
依存関係	693	0	0	0

※1：無償ツールのうち3ツールは、機能等の問題により精度評価及び分析の実施が不可能であった。
※2：依存関係は1つのコンポーネントに対して複数存在する可能性があるため、コンポーネントの出力件数に関わらず出力有無を検証する必要がある。
※3：手動版SBOMをツールで読み込み、自動算出された「コンポーネント数」と「依存関係」を記載。
※4：ツール②においては解析のためにコンテナのロードが必要であるが、開発元との契約の都合上、ロードができなかったため、コンテナスキャン対象外。

3　脆弱性情報との照合

- 抜け漏れのない網羅的な「手動版SBOM」を用いて脆弱性情報管理の検証を実施。
- 「手動版SBOM」に記載されている「通信分野において着目すべき項目」のうち、脆弱性情報と照合するために必要な項目を整理して、実際の脆弱性データベースと照合し、通信機器①・②に含まれる脆弱性の検知を実施。

SBOMツールに対する検査項目の抽出

- 脆弱性データベース（DB）の調査を行い、脆弱性情報と照合するための検査に必要となる項目（検査項目）を検討・整理。
- 上記の整理結果から、SBOMおよび脆弱性DBの双方にある情報として、今回は検査項目を**「コンポーネント名とバージョン」、「CPE※1」、「purl※2」**とした。
- 通信機器①・通信機器②の手動版SBOMの項目の記載状況は以下のとおり。

検査項目	通信機器①（CycloneDX）	通信機器②（SPDX）
コンポーネント名/バージョン	○	○
CPE	×	○
purl	○	×

※1：CPE：Common Platform Enumeration

※2：purl：Persistent Uniform Resource Locator

照合する脆弱性データベース

- 手動版SBOMに記載されている検査項目の内容を、以下の脆弱性DBに照合し、脆弱性の有無について調査を実施。

脆弱性DB名称	運営箇所
NVD※3	米国立標準技術研究所（NIST）
JVN※4	JPCERT コーディネーションセンター 独立行政法人情報処理推進機構

※3：NVD：National Vulnerability Database

※4：JVN：Japan Vulnerability Notes

3　脆弱性情報との照合

- 通信機器①・通信機器②の「手動版SBOM」に記載された検査項目（コンポーネント名、バージョン、CPE又はpurl）を用いて、脆弱性DB（NVD・JVN）と照合したところ、検査項目により脆弱性情報の検知数及び検知された脆弱整数が大きく異なる結果となった。

脆弱性情報との照合（通信機器①の「手動版SBOM」）

脆弱性情報照合結果※1

- 検査項目（「コンポーネント名とバージョン」、「purl」）により、**脆弱性情報の検知数及び脆弱性数は以下のとおり大きく異なる結果**となった

DB名	コンポーネント名とバージョン			purl		
	検査数	検知数	脆弱性数	検査数	検知数	脆弱性数
NVD	1098	237	3441	1093	85	455
JVN	1098	314	4587	1093	116	1512

考察

- 「コンポーネント名とバージョン」を検査項目とする場合には、表記揺らぎ等の影響により、製品の特定精度が低いため、検知数、脆弱性数とも数は多いが精度は低いと考えられる。
- 「コンポーネント名とバージョン」より「purl」の方が検知数が少なく、脆弱性数も少ないが、「purl」の方が製品の特定精度が高いため誤検知が少ないと考えられる。

脆弱性情報との照合（通信機器②の「手動版SBOM」）

脆弱性情報照合結果※1

- 検査項目（「コンポーネント名とバージョン」、「CPE」）により、**脆弱性情報の検知数及び脆弱性数は以下のとおり大きく異なる結果**となった

DB名	コンポーネント名とバージョン			CPE		
	検査数	検知数	脆弱性数	検査数	検知数	脆弱性数
NVD	139	27	420	62	50	1042
JVN	139	23	532	64	46	971

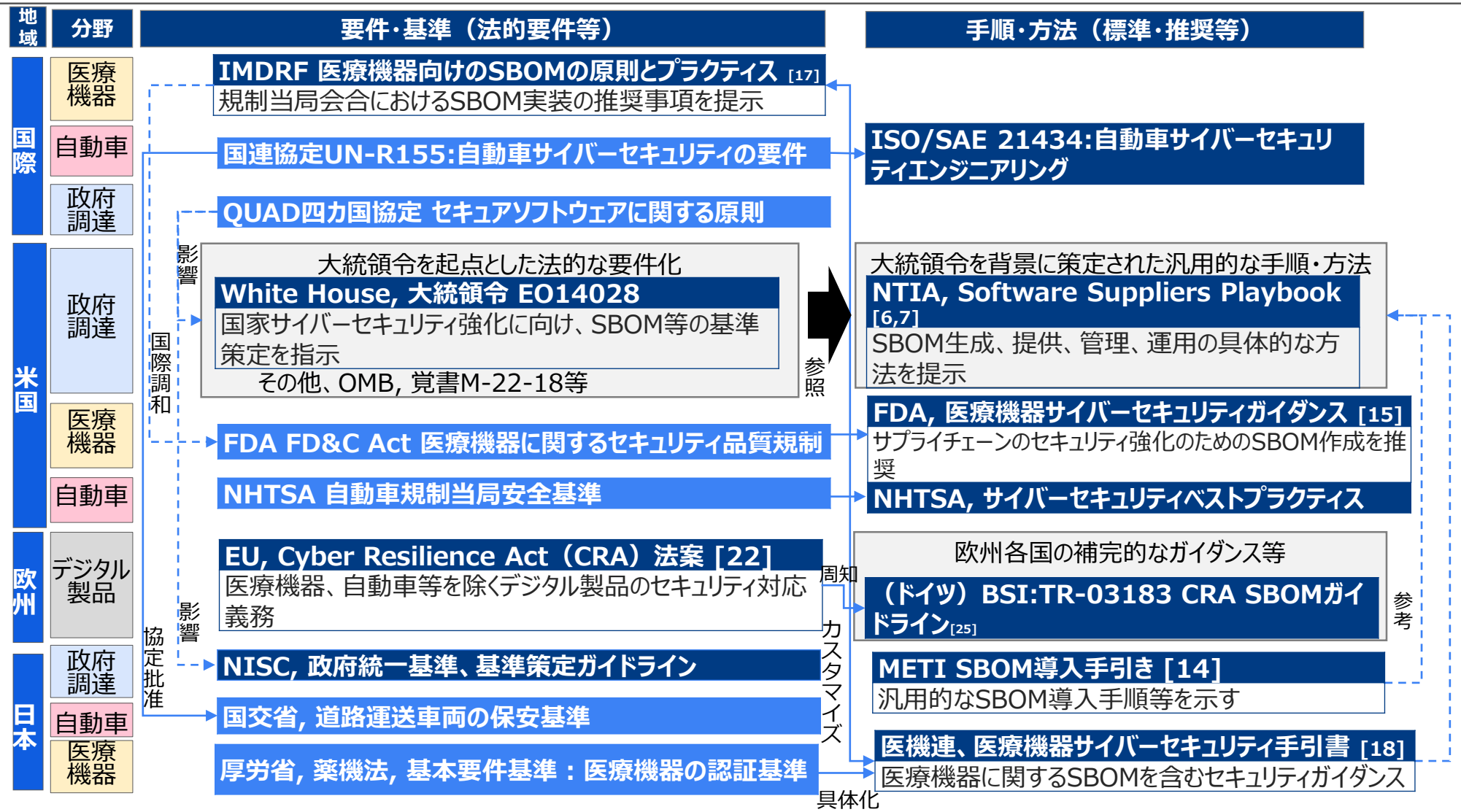
考察

- 「コンポーネント名とバージョン」を検査項目とする場合には、表記揺らぎ等の影響により、製品の特定精度が低く、検知数、脆弱性数の精度も低くなるので、一般的に「コンポーネント名とバージョン」の方が「CPE」よりも検知数、脆弱性数が多くなると考えられる。
- 本実証で「CPE」の方が多くなったのは、作成したSBOMについては、同一コンポーネントに対し、CPEが複数名で登録されていることが影響していると考えられる（例：commons-i, commons_io 等）。

※1：検査数：検査対象コンポーネント数、検知数：脆弱性を含むコンポーネント数、脆弱性数：検知された脆弱性数を示す。

4　国内外動向調査

- SBOMに関連した国内外動向調査として、主な国・分野、制度的要件化、影響について主要な事例の全体像を整理。
- 米国大統領令を起点として、政府、民間におけるガイドライン等により要求、手順等の検討・整備が進展。



4　国内外動向調査

- 国内外の取組ごとにSBOMの要件・方法に関する事項について整理すると概要は以下のとおり。

	要件・基準等	手段・方法等
海外	• 国家サイバーセキュリティ強化を目的とした米大統領令14028に基づき、OMB、NIST、CISAなどにより、政府調達におけるSBOMの最小要素等を規定。 • 機器認証等を目的として、医療機器分野（IMDRF、FDA）、自動車分野（ISO 21434）など特定分野では構成管理の手段としてSBOMの利用を例示。 • EUのCRA法案では、安全なデジタル製品の市場流通を目的として、デジタル製品全般の要件として、SBOMやOSS管理の要求事項を規定。 • QUADにおいて、セキュアなソフトウェア開発を目的として、SSDFに関連するセキュアソフトウェア開発プラクティスの部品管理の要件にSBOMを例示。	• 米CISA/NSA/ODNIにより、ソフトウェア・サプライチェーン・セキュリティの強化を目的として、開発者、サプライヤ、ユーザごとに分けてSBOMの作成、活用に関する実施事項の推奨プラクティスを提示。 • NTIAにより、サプライヤ、ユーザにおけるソフトウェア・セキュリティを確保することを目的に、SBOM作成、取得、活用に関する手順等を提示。 • 医療機器分野では、機器の安全性、品質を確保することを目的として、IMDRF Guidanceにおいて、SBOMの要件に関連する実施事項を提示。
国内	• 医機連は、医療機器の安全性、品質を確保することを目的として、IMDRF Guidanceに準拠して具体化したSBOM手引書を提示。	• 経済産業省のSBOM導入手引書において、企業におけるソフトウェア管理の向上を目的として、SBOMを導入するメリットや実際に導入するにあたって認識・実施すべき具体的なポイント、チェックリストを提示。 • 経済産業省ソフトウェアタスクフォースにおいて、サプライチェーンにおけるソフトウェア調達におけるセキュリティ確保を目的として、SBOM対応事項の網羅性の可視化（SBOM対応モデル）、契約における規定事項（SBOM取引モデル）を提示。

5　留意事項の作成（目的と位置付け）

- 通信分野においてSBOMを用いた脆弱性管理を効率的に実現することを目的として留意事項を整理。
- 留意事項の目的に対応して3つのアプローチに基づき留意事項を検討。

留意事項の整理の目的と位置付け

- 通信分野において脆弱性管理を効果的に実現することを目的として、SBOMを導入・活用する手順等について留意事項を整理。
- SBOMを作成・提供する通信機器のベンダや部品サプライヤや、SBOMを活用する通信事業者等に向けて留意する事項を整理。

留意事項の検討アプローチ

- 留意事項検討の目的に対応して以下の3つの観点とアプローチに基づき留意事項を整理。

留意事項検討の目的	検討アプローチ
（1）手順・方法の具体化 通信分野の組織においてSBOMを導入・活用するための手順や方法について留意する事項を整理する。	**（1）プロセスに基づく体系整理** SBOMの作成・活用等に関するプロセスに基づき、体系的に手順・方法について整理する。
（2）効果・効率の向上 SBOMの導入・活用において、脆弱性管理の効果・効率の向上につながる事項を整理する。	**（2）KPIの明確化** SBOMの効果・効率に関するKPIを明確化し、それにつながる事項を整理する。
（3）通信分野の要求に対応 通信分野の要求に対応して、SBOMを用いて脆弱性管理を行う際に留意する事項を整理する。	**（3）通信分野の特徴に対応するSBOM要求観点** 通信事業者、機器ベンダ等から通信分野の特徴や課題についての意見聴取、技術情報に基づき、要求と対応観点を整理する。

5　留意事項の作成（留意事項の整理に向けた検討アプローチ）

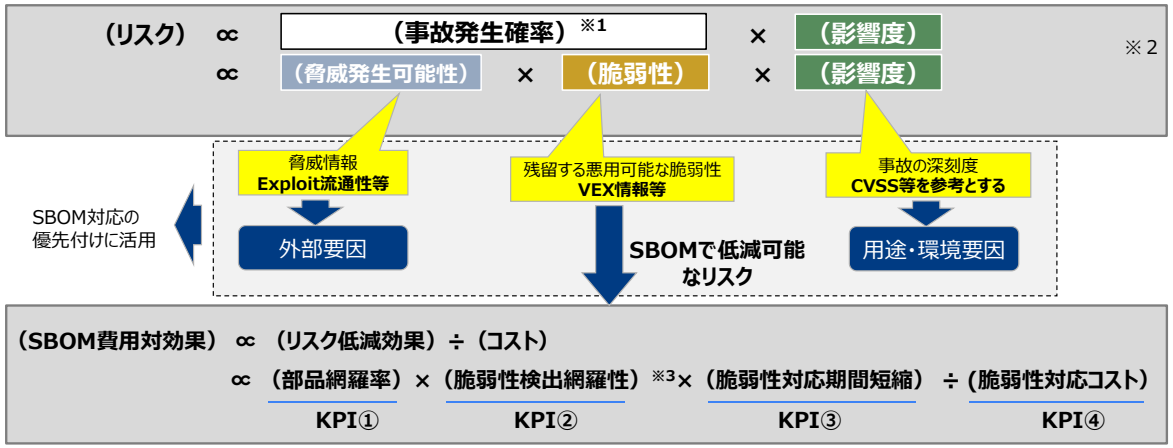
- SBOMの作成・活用に関するプロセスに基づき、手順・方法を体系的に留意事項の章構成を整理。
- SBOMを用いた脆弱性管理の費用対効果に関するKPIを明確化するとともに、通信分野の特徴等を考慮したSBOMの要求事項を整理。

アプローチ（１）プロセスに基づく留意事項の体系的な整理

➢ 開発企業、ユーザ企業のソフトウェア開発・運用プロセスにおけるSBOMプロセスを**作成、共有、活用のフェーズ**に整理し、留意事項の章構成を体系的に整理。

アプローチ（２）SBOMの効果・効率に関するKPIの明確化

➢ SBOMを活用した脆弱性管理の費用対効果に基づきKPIを特定し、KPIの影響の大きい要素を留意事項として整理。



効果は、リスク低減効果、コスト低減効果に分け、費用は、部品・脆弱性単位当たりの限界費用に基づき費用対効果の向上につながる取組み事項を検討する。

参考
※１　セキュリティ経済学において事故発生確率は、条件付き確率でモデル化される：P(脅威発生∩事故) = P(脅威発生) × P(事故｜脅威発生)
※２　サイバーセキュリティ戦略本部研究開発戦略専門調査会　講演「社会問題から見たサイバーセキュリティ技術課題」、三菱総合研究所　石黒正揮、2019年,情報処理学会誌　特集「デジタルエコノミー時代のサイバーセキュリティ」、「サイバーセキュリティ経済学」　石黒正揮、2018年
※３（脆弱性検出網羅性）＝（脆弱性DB網羅率）×（脆弱性突合精度）

三菱総合研究所作成

アプローチ（３）通信分野の特徴に対応するSBOM要求

➢ 通信業界の事業者意見に基づき通信分野の特徴・要求に対応してSBOM要求事項の観点を整理。

通信分野の特徴・要求	概要	SBOM要求の観点
障害の波及的影響・高可用性	通信サービスは、様々なインフラ、製品サービスの基盤として利用され、障害の波及的影響が大きく、高可用性、高信頼性が求められる。	SBOMの部品網羅性、脆弱性検出の網羅性の確保
長期運用	通信インフラの機器、システムは、長期運用を前提としており、保守・運用における制約条件への対応が必要。本番系・予備系管理など。	SBOM履歴管理、EOLサポート契約
オープン仕様/レイヤーアーキテクチャ	O-RAN、ITU、OSI参照モデル、IETFなどオープン仕様、レイヤーアーキテクチャ化が進展している。	SBOM階層的依存関係
汎用プロトコル	IP、HTTP、TLS、IPSecなど通信、セキュリティプロトコルやそれに対応した認証済モジュール（CMVP）の利用が進んでいる。	適合性評価とSBOMマッピング
仮想化（NFV、SDN）	VFN、SDN、データフロー/コントロールフロー、ネットワーク・オーケストレーション自動化など仮想化技術の導入が進んでいる。	オープンモジュールのSBOM対応
マルチベンダ対応	オープン仕様、汎用プロトコルをベースとしてマルチベンダによるシステム構築が推進されている。	マルチベンダのSBOM標準化、相互運用性確保
サードパーティ製品（COTS、OSS）	ルータ、オーケストレーターなど商用既製品（COTS）やOSSを改良したソフトウェアの利用が進んでいる。	ライセンス契約、OSSコミュニティのSBOMプラットフォーム

5　留意事項の作成（留意事項の構成（案））

- SBOMの作成、共有、活用プロセスに基づき章構成を体系化し（赤枠内）、SBOMのKPIや通信分野の要求に対応した主な留意事項を項目レベルで以下のとおり整理。

プロセスに基づく章構成			留意事項から抜粋・例示
背景・目的			―
SBOM導入のメリットと方針検討			SBOM導入の効果に基づき対応範囲の方針検討を行う。
プロセス全体像			SBOM初期導入・運用の全体プロセスを俯瞰し各フェーズの対応範囲を特定する。
SBOMプロセス	初期導入フェーズ		SBOM対応範囲を明確化し、それに対応した機能を持つツールを選択する。
	SBOM運用フェーズ	作成・更新フェーズ	部品の網羅性の評価観点を明確化する。**KPI①**
			長期運用に対応しSBOM履歴管理による脆弱性リスク評価を行う。**KPI③** **（通信分野の要求：履歴管理）**
		共有フェーズ	SaaS/APIを用いた迅速な情報共有を検討する。
		活用フェーズ（脆弱性管理）	脆弱性管理の網羅性の評価観点を明確化する。**KPI②**
			脆弱性対応期間の短縮効果の評価観点を明確にする。**KPI③** **プロセス基づく体系整理箇所**
課題・制約事項			SBOM、脆弱性DBにおいて部品IDが統一されていないため、手動管理が求められる。

5　留意事項の作成（SBOM作成に係る課題整理）

- 障害発生時の波及的影響範囲と長期運用を前提とした通信機器は、SBOMに高い品質が求められるが、**汎用的ではないコンポーネント等が使用されていることが多く**、ツールのみを使用して作成した**「ツール版SBOM」の品質が高くない**点が課題。
- CycloneDXにおいて、現状の多くのツールでは項目**「サプライヤ名」と「依存関係」が出力されない**ことが課題。
- これらの情報は、NTIAのSBOM要求でも必須項目（最小要素）とされているものの、**各SBOMツールの開発が追いついていない**ため、費用対効果を考慮して記載要否を検討することが必要。

項目	課題	要因	引き続き検討すべき事項
SBOM 作成ツール 解析精度	■ SBOM作成ツールのみで作成した「ツール版SBOM」の解析精度が高くない。	■ 通信機器に汎用的なOSS等ではないものが多く使用されていることが解析精度に影響を与えていると考えられる。 ■ 長期安定稼働を求められる通信機器には古いアーキテクチャやトレンドから外れた技術・言語が使用されていることも解析精度に影響を与えうる。	■ 障害の波及的影響が大きい通信機器のSBOMはコンポーネント等には高い品質が求められるため、OSSをカスタマイズした場合も含めてベンダ主体でSBOMを作成し、記載内容が網羅されているか確認する仕組みが必要。 ■ 長期的な保守・運用における制約条件への対応の観点から、SBOMの履歴管理とEOSLに関わるサポート契約についても整理することが必要。
「サプライヤ名」 「依存関係」 出力	■ CycloneDXにおいては、殆どのツールで「サプライヤ名」・「依存関係」が出力不可。	■ SBOM作成ツールの仕様上の問題。	■ 「サプライヤ名」は必要な情報であるため手動入力でも記載することが必要。 ■ 「依存関係」を手動入力するには膨大な労力が必要となるため、費用対効果を考慮して記載要否を検討することが必要。

5　留意事項の作成（SBOM共有取得に係る課題整理）

- 通信分野においては、SBOM黎明期であり、通信分野のサプライチェーンにおいて、SBOM作成主体や作成範囲、取引方法が定まっていないことが課題。

項目	課題	要因	引き続き検討すべき事項
SBOM作成主体・SBOM作成範囲	■ 通信分野のサプライチェーン上において、SBOMの作成主体及び作成範囲が曖昧。	■ SBOM黎明期であり、ベストプラクティスが現時点で存在しないことが一因と考えられる。	■ ソフトウェアのライフサイクルに沿ったSBOMのライフサイクル・活用プロセスの整理が必要。（SBOM作成→リスク検知→対処→SBOM更新→共有→ …） ■ 次に、各プロセスの担当と範囲をベンダ・サプライヤ・ユーザに分けて整理することが必要。 ■ さらに、各プロセスにおいての手法（手動、ツール、その他）を費用対効果とそのKPIを考慮して整理することが必要。
SBOM取引方法	■ 通信分野の商慣習に応じて、SBOMをどのように取引するか決まっていない。	■ SBOM黎明期であり、ベストプラクティスが現時点で存在しないことが一因と考えられる。	■ 各活用プロセス及び、企業間のSBOMの共有について、ベンダ・ユーザ双方の立場を考慮し、秘匿性の確保・自動化・安全性を満たす契約や運用体系を整理・検討した上で取引モデルの策定が必要。 ■ 自社内製ソフトウェアの取扱いについても同様に考慮が必要。

5　留意事項の作成（SBOM活用に係る課題整理、脆弱性管理の費用対効果に係る評価）

- 脆弱性情報との照合で使用する項目については、ソフトウェアベンダによって記載方法にばらつきがあるとともに、脆弱性DBによっても同様に記載方法にばらつきがあり、誤検知が発生することが課題。

項目	課題	要因	引き続き検討すべき事項
脆弱性検出精度	■ SBOMを用いた脆弱性検知の精度が高くなく、SBOMを用いた脆弱性管理に費用対効果を見込めない。	■ 脆弱性検査で使用する項目となるCPE、purl等について、ソフトウェアベンダや脆弱性DBによって記載方法にばらつきがあることが影響していると考えられる。	■ VEXの活用など、SBOMを用いた脆弱性検出精度の向上手法を検討することが必要。 ■ SBOMの各項目の値（CPE、purl等）の記載方法や脆弱性管理手法（使用する脆弱性DB等）に関してSBOM作成者とSBOM利用者間で合意やルール化が必要。

5　留意事項の作成（課題に対する今後の取組）

調査、協議、整理が必要な検討課題
更に実施検証が必要な技術課題

目標：「通信分野におけるソフトウェア脆弱性の迅速な検知の実現」

SBOM運用観点の実施事項

SBOM作成に係る課題整理

●部品網羅性

- SBOM作成に際してツールのみでは精度に課題。手動のみでは、工数・コストに課題。
- SBOMを作成するサプライヤ部品の階層がSBOM精度に影響を及ぼすかも要確認。

●SBOMの必要項目

- 現在、明確に必要項目が要件化されているのは米国政府要件（NTIA）のみ。各国政府・民間問わず検討はされてはいるが結論は未整理。
- 「依存関係」など通信分野として必要か検討し、他業界の要求や動向も注視。

サプライチェーン間のSBOM共有取得に係る課題整理

●SBOMの作成主体・作成範囲等

- SBOMのライフサイクルを通して各プロセスを整理し、担当・範囲・手法・制約等の整理が必要。
- ユーザ（外注製品、内製製品）、ベンダ（提供元、開発元）各々の関わり方の違いを整理。

●SBOMの取引方法

- 企業間のSBOM共有に関するルール/契約及び、運用体系化を整理した取引モデルが必要。

SBOMによる脆弱性管理に係る課題整理

●脆弱性検出精度

- 検査項目等の記載方法によって検出精度に影響。
- VEX利用等を考慮して脆弱性検出精度の安定と向上が課題。
- 検査方法のルール化と合意が必要。

SBOM便益観点の実施事項

SBOMを用いた脆弱性管理の費用対効果に係る評価

●検証結果に基づいた費用対効果の算出

- 検討したKPIに基づいて費用対効果の評価が必要。

ツール版SBOMの精度向上
サプライチェーンリスクも考慮し、3階層以上（ベンダ、ティア1、ティア2以上）のソフトウェア実装機器を対象にSBOM作成・評価を実施。
通信機器特有の情報を如何にSBOMに内包するか検討

取引モデルの策定
通信分野における商慣習を踏まえながら、ソフトウェア部品の利用者（主に事業者）および供給者（主にベンダ）の観点を考慮した取引モデルを整理。

脆弱性管理手法に関する実証
通信分野におけるSBOMを活用した最適な脆弱性管理手法を実証・整理。（VEX等も検討）

費用対効果の算出
SBOM導入の費用対効果を算出し、SBOM導入が適した場面等を整理。

最新の制度、動向調査
SBOMに関する国内外の制度及び動向調査を行い網羅的に整理。SBOMを活用した脆弱性管理手法の調査・ヒアリングの実施。

今後の取り組むべき主な内容