明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

サプライチェーンのサイバーレジリエンス
― セキュリティ透明性の向上と活用 ―

情報セキュリティ大学院大学
セキュリティ・トランスペアレンシー・コンソーシアム 会長
後藤　厚宏

プロフィール　後藤　厚宏

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 1984年 工学博士。NTT研究所にて先進ICT技術の研究開発等に従事。
  - 第5世代コンピュータPJ（1985～1990）、米国シリコンバレー拠点（1994～1996）
- 2011年7月より情報セキュリティ大学院大学(IISEC)教授。2017年4月より学長
  - **約7割が社会人。OB・OGは官公庁・企業で活躍中。**
- 2015年11月～2023年3月 内閣府SIPプログラムディレクター 併任
  - SIP第1期：重要インフラ等のサイバーセキュリティ確保（2015～2019）
  - SIP第2期： IoT社会に対応したサイバー・フィジカル・セキュリティ（2018～2022）
- 2019年2月より日本政府のサイバーセキュリティ戦略本部員
- 2023年9月よりセキュリティ・トランスペアレンシー・コンソーシアム 会長

サプライチェーンのサイバーレジリエンス
― セキュリティ透明性の向上と活用 ―

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- サプライチェーン「汚染」リスク
- ソフトウェア透明性への取り組み
- セキュリティ・トランスペアレンシー・コンソーシアム概要
- コンソーシアムが公表した「知見集～脆弱性管理編」より

サプライチェーン：サイバー攻撃リスク

Supplychain Attacks

2019年 防衛装備品情報の窃取

2022年 デンソー（独）へのランサムウェア攻撃

営業機密の盗取

顧客情報、製品情報（設計情報、製造情報等）

不正なソフトウェアの混入

2020年 米国SolarWinds社：運用システムの更新プログラムがサイバー攻撃によって改ざん

汚染

ソフトウェアの追加・変更

2021年 Log4Shell：部品OSSに混入している脆弱性を狙うサイバー攻撃リスク

不正な部品の混入

汚染

2016年 米国セキュリティ会社が携帯電話部品に仕込まれている不正プログラムを発見

部品供給の停止

2022年 小島プレスへのサイバー攻撃でトヨタが新車生産を停止

寸断

港湾コンテナ物流の停止

2023年 名古屋港統一ターミナルシステム攻撃によるコンテナ物流の停止

ソフトウェア脆弱性・不正機能の一斉混入による「汚染」リスク

サイバー攻撃のリスク

- メールの添付ファイルの**不正機能**
- Webアクセス時に**不正機能**をダウンロード

- ソフトウェアに残存する**脆弱性**はサイバー攻撃の入口

ソフトウェアサプライチェーンのセキュリティリスク

ソフトウェア**更新機構**を乗っ取り、不正機能を混入する攻撃

SolarWinds

多数の製品に利用されているソフトウェア（OSS）部品に、内在する**脆弱性**

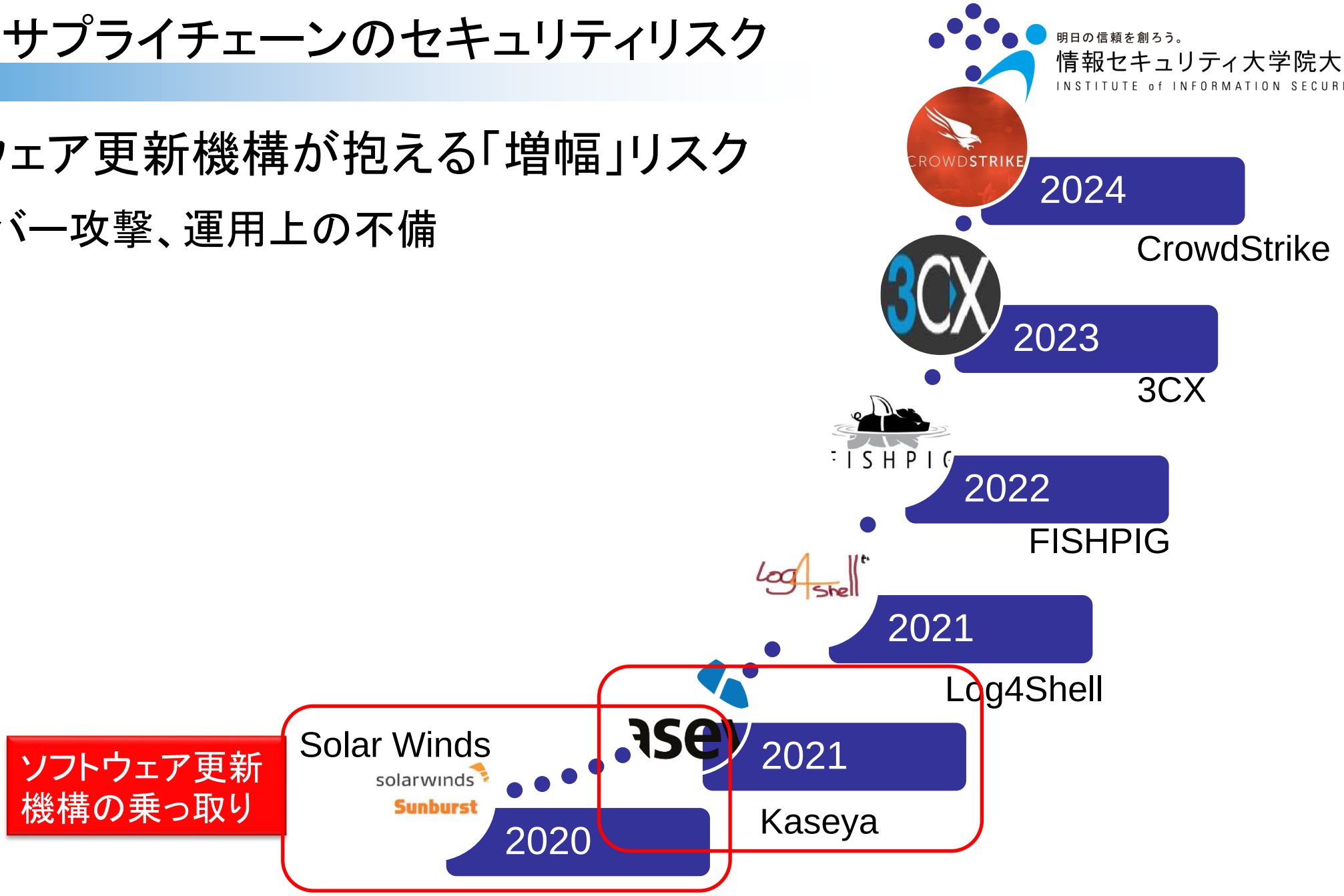
Log4Shell

サプライチェーン全体に汚染リスクが「急」拡大

ソフトウェアサプライチェーンのセキュリティリスク

■ ソフトウェア更新機構が抱える「増幅」リスク

- サイバー攻撃、運用上の不備



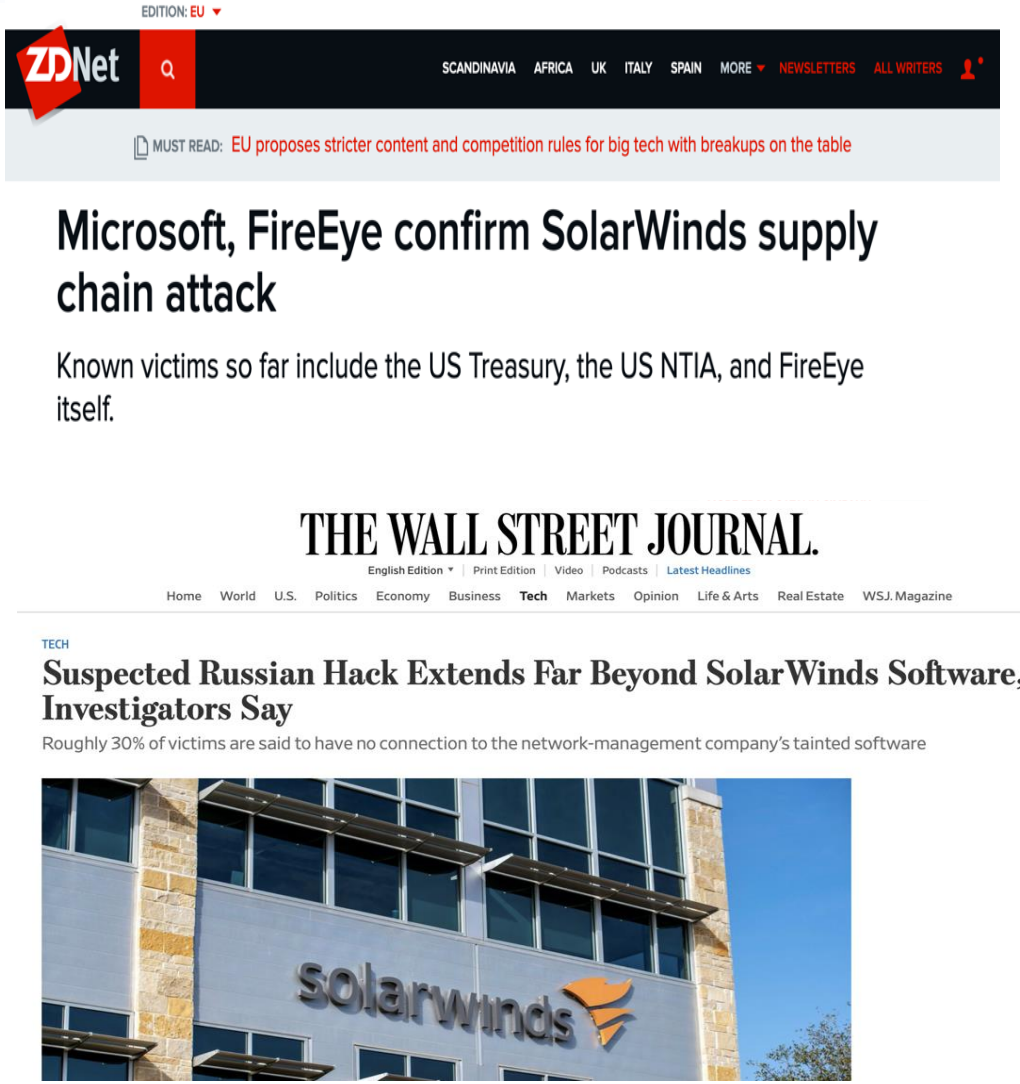
SolarWinds社の事案:「更新」機構の乗っ取りによる「汚染」

- SolarWinds社のネットワーク監視ソフトウェア「Orion Platform」を用いる米国連邦政府機関(財務省・国務省・国家核安全保障局など)やMicrosoft, Cisco, FireEyeなどの大企業(合計18,000組織)が大規模なサイバー攻撃の被害を受けた(2020年)

- 同社が2020年3月と6月に配布したアップデートが改ざんされた? 国家の関与?

国家安全保障を脅かす事案⇒大統領令14028「連邦政府のサイバーセキュリティ強化」(2021/5)

米国証券取引委員会(SEC)が詐欺行為と内部統制の不備でSolarWinds社を告発(2023/10)⇒裁判所が大部分を棄却(2024/7)


EDITION: EU

ZDNet

SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: EU proposes stricter content and competition rules for big tech with breakups on the table

Microsoft, FireEye confirm SolarWinds supply chain attack

Known victims so far include the US Treasury, the US NTIA, and FireEye itself.

THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

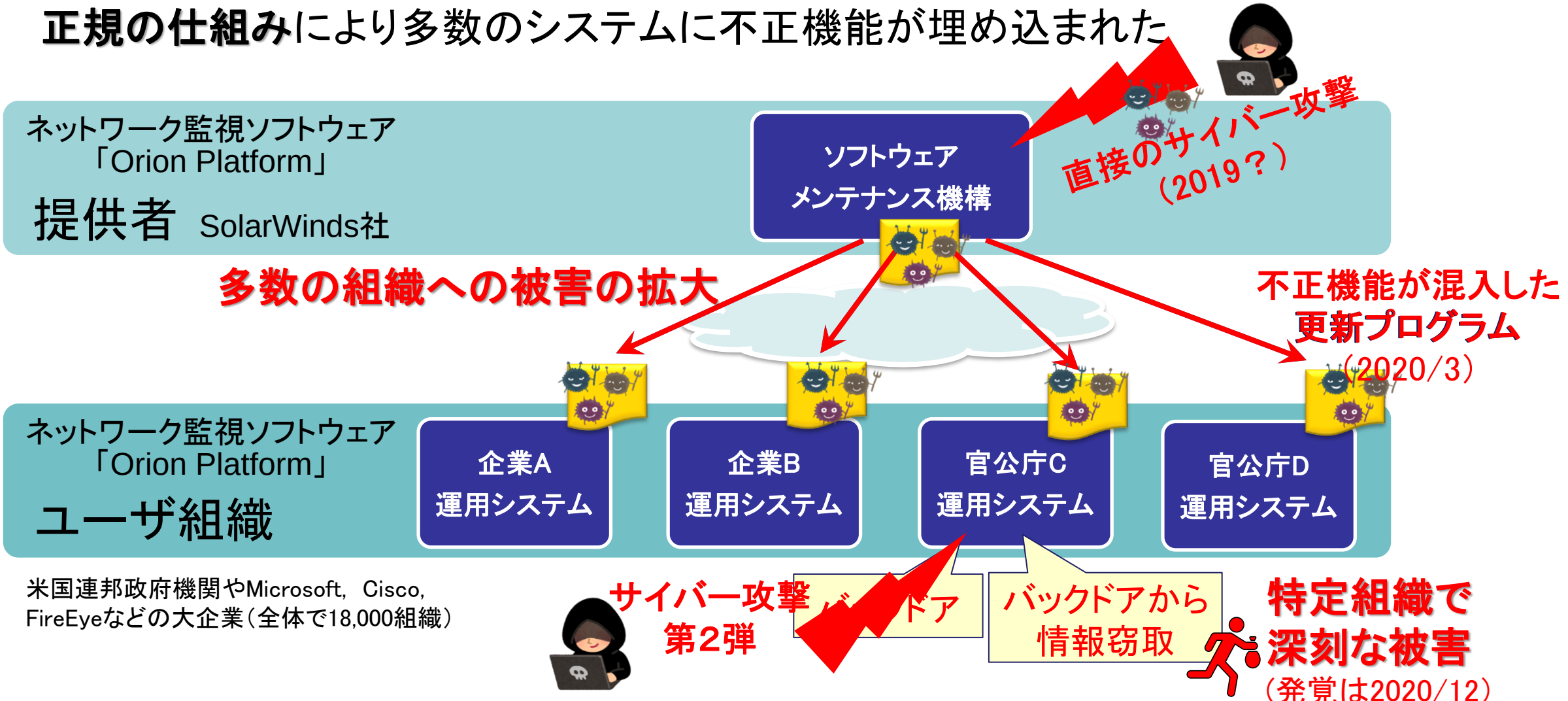
TECH

Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say

Roughly 30% of victims are said to have no connection to the network-management company's tainted software

SolarWinds社の事案:「更新」機構の乗っ取りによる「汚染」

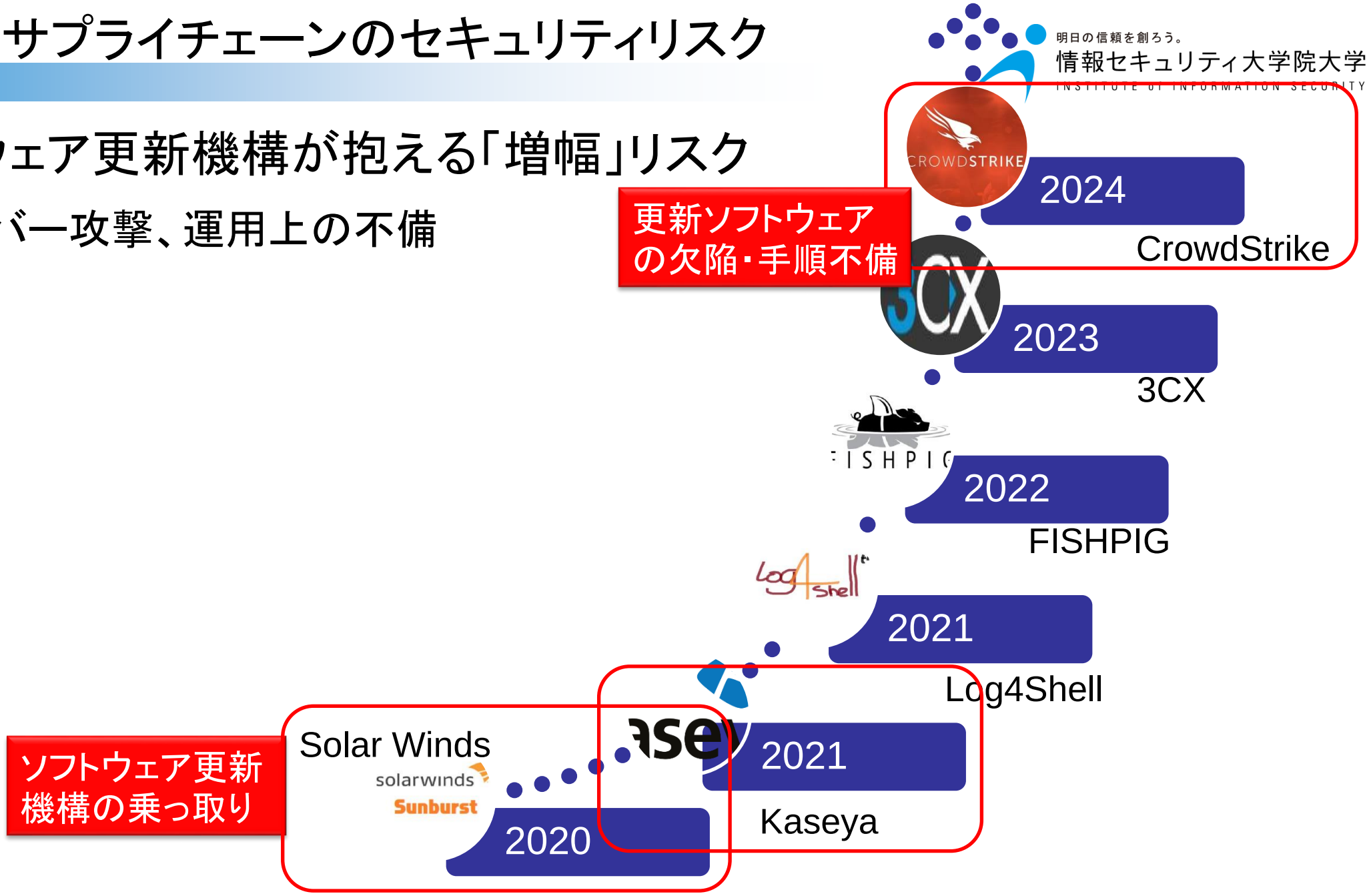
■ SolarWinds社の事案:ソフトウェアの更新機構が攻撃され、**更新プログラムを配布する正規の仕組み**により多数のシステムに不正機能が埋め込まれた



ソフトウェアサプライチェーンのセキュリティリスク

■ ソフトウェア更新機構が抱える「増幅」リスク

- サイバー攻撃、運用上の不備



CrowdStrike社事案：ソフトウェアの欠陥がもたらす世界的連鎖

- 2024年7月19日に発生：　全世界で**約850万台**のWindowsがクラッシュ
- 社会経済の混乱：　航空会社（Delta, UA他）、医療機関、金融機関など**多数の組織が機能不全**に陥り、手作業でのシステム復旧が必要に

⇒多数のユーザ企業や株主からの訴訟の嵐に

- CrowdStrike社のセキュリティソフトFalconの更新ソフトウェアの欠陥と確認手順の不備
  - ポイント1：新たな脅威や進化する脅威に対処するために、頻繁なセキュリティソフトウェアの更新が必要に！
  - ポイント2：Windows OSのカーネルレベルに影響するソフトウェア機能の更新が抱えるリスク

ソフトウェアサプライチェーンのセキュリティリスク
⇒ユーザ企業の事業継続性を脅かす経営リスク

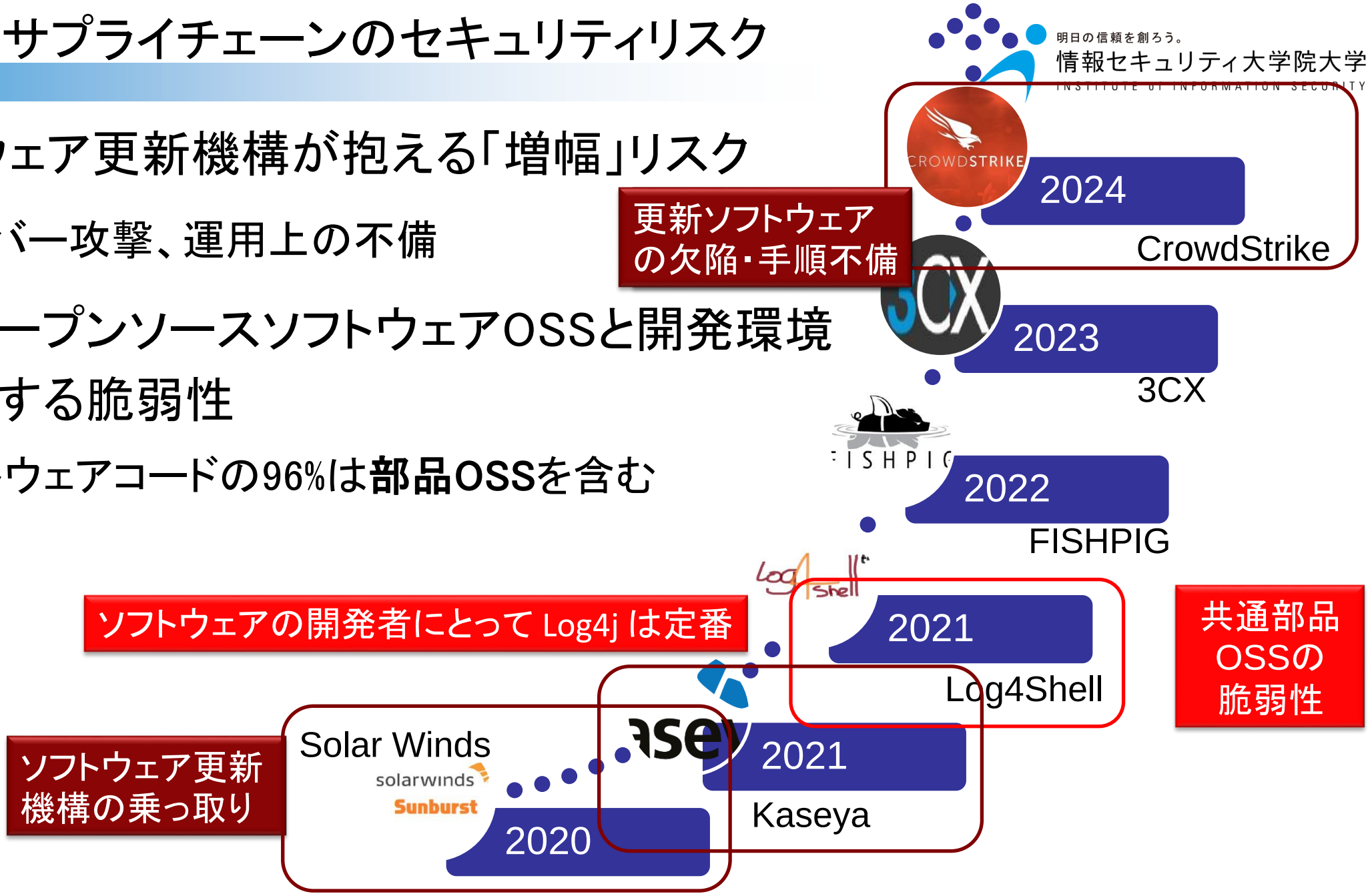
ソフトウェアサプライチェーンのセキュリティリスク

■ ソフトウェア更新機構が抱える「増幅」リスク

- サイバー攻撃、運用上の不備

■ 特にオープンソースソフトウェアOSSと開発環境に残存する脆弱性

- ソフトウェアコードの96%は**部品OSS**を含む



Log4Shellの事案：部品OSSに残存する脆弱性の悪用リスク

Log4Shellの例

「Apache Log4j」は広く利用されているWebサーバーシステムに標準機能として組込まれているJavaのログ出力ライブラリー

Apache Log4jの普及後に脆弱性スコアCVSSが最大の脆弱性（Log4Shell）が発覚（2021年）

⇒ランサムウエア（身代金要求型ウイルス）攻撃への悪用が容易

結果として、サプライチェーンを通してApache Log4j（部品OSS）に残存する脆弱性（汚染が）が、多くの商用ソフトウェアシステムに「拡散」

多種多数の（商用）ソフトウェア毎にそれぞれの企業の対応が必要

⇒「自社が販売 or 利用のソフトウェアに当該OSSが使われているか？」

現在（2024年）もApache Log4j 13%は既知の脆弱性を内包する版との報告あり

サプライチェーン「汚染」リスクへの対応

トランスペアレンシー（透明性）確保
事業者が技術的に自らセキュリティリスクを確認できる

ソフトウェアサプライチェーン

ソフトウェア**更新機構**を乗っ取り、不正機能を混入する攻撃
SolarWinds

多数の製品に利用されているソフトウェア（OSS）部品に、内在する**脆弱性**
Log4Shell

サプライチェーン全体に汚染リスクが「急」拡大

- 国家安全保障リスク
- 事業継続リスク

「汚染」リスクへの対応

ソフトウェア保守における**更新プログラムの確認**（提供者～ユーザ組織）

サプライチェーン全体での

- **ソフトウェア構成情報**の作成・更新と共有
- **脆弱性情報**の共有

サプライチェーンのサイバーレジリエンス
― セキュリティ透明性の向上と活用 ―

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

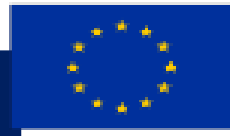
- サプライチェーン「汚染」リスク
- ソフトウェア透明性への取り組み
- セキュリティ・トランスペアレンシー・コンソーシアム概要
- コンソーシアムが公表した「知見集～脆弱性管理編」より

ソフトウェア透明性に向けた政策動向

国家安全保障リスク、事業継続リスクの観点での議論

大統領令14028「国家のサイバーセキュリティ改善」(2021/5)

安全保障のためのソフトウェアサプライチェーン対策 by NSA, CISA, ODNI



IoT類を含むネットワーク接続機器類への規制強化

（Cyber Resilience Act）

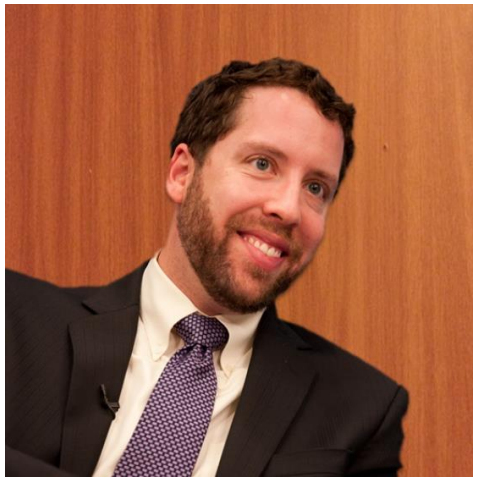
サイバーセキュリティ戦略

経済安全保障推進法

SBOM（Software Bill of Materials）

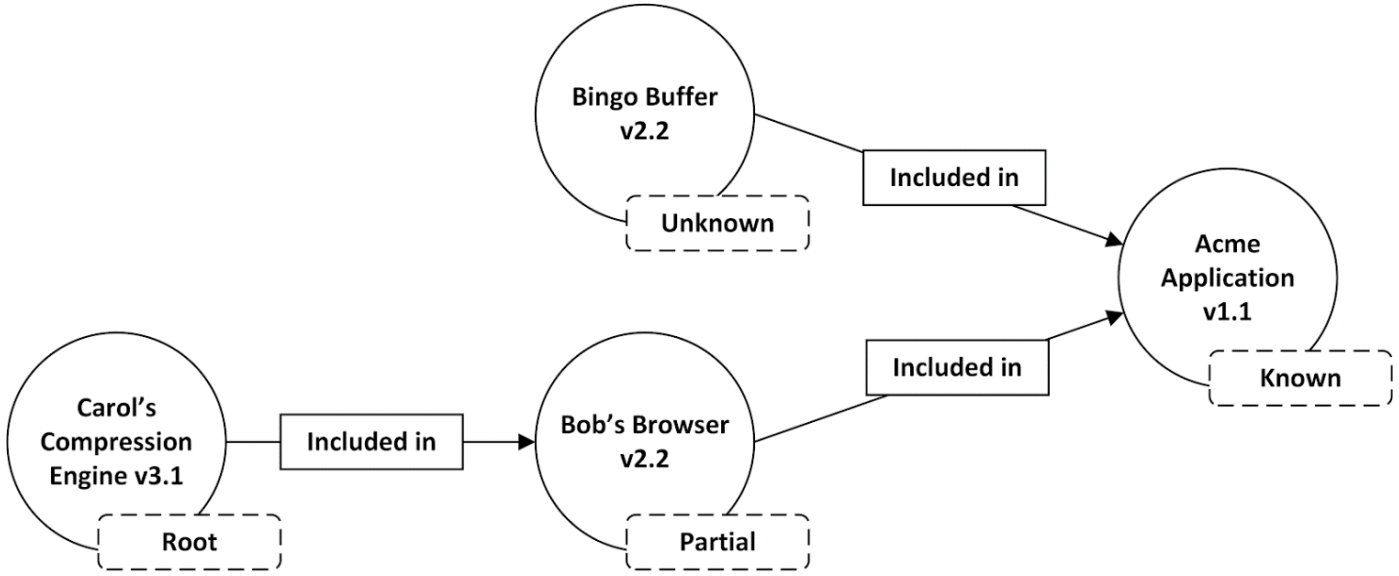
■ SBOMはソフトウェアの**透明性向上のための「成分表」**

≒開発の履歴、来歴管理情報



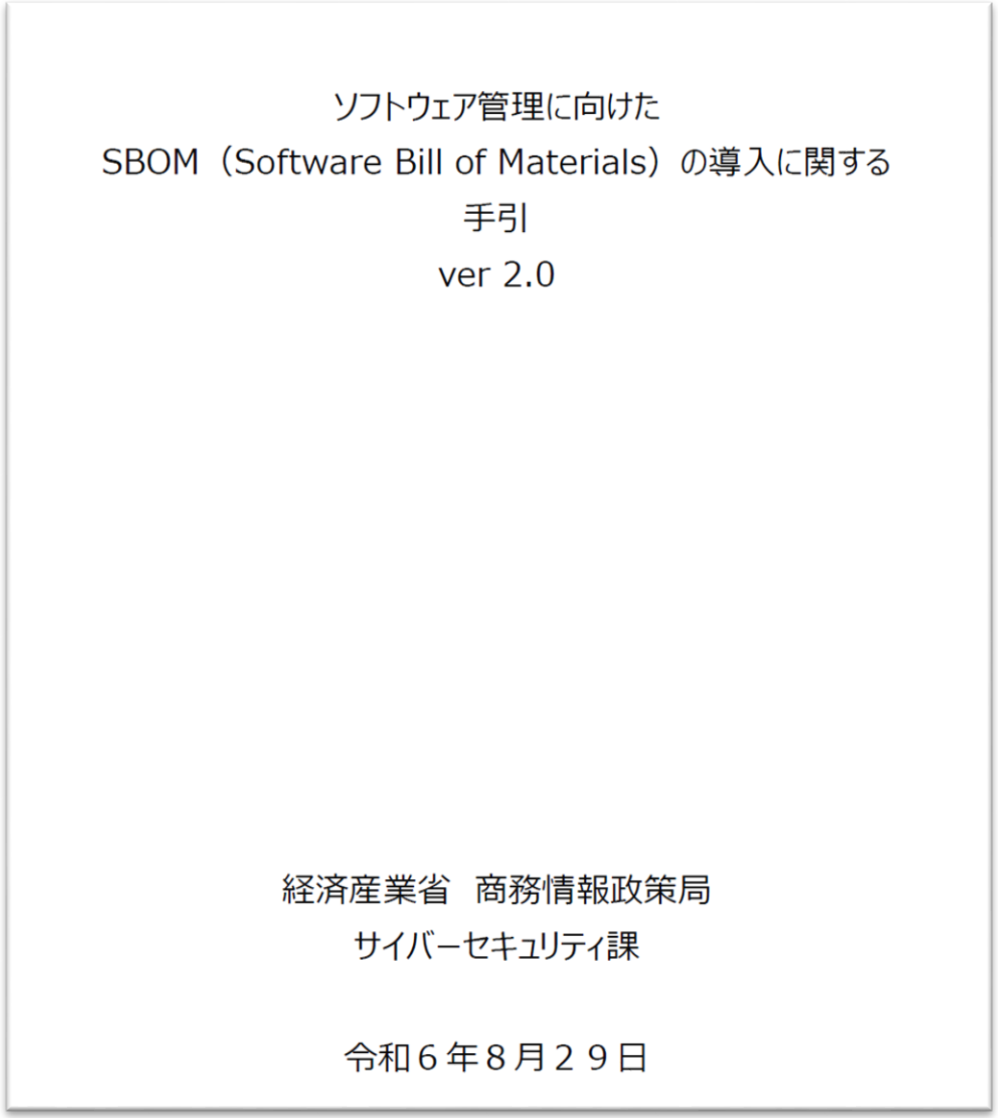
米商務省，NTIA
アラン・フリードマン氏

SBOMの主な要素
• ソフトウェア部品の名称・識別子
• ソフトウェア部品のサプライヤ
• ソフトウェア部品のバージョン
• SBOM 作成者・作成ツール
• SBOM 作成時刻
• 依存関係



日本でのSBOM導入トライアル

- ■経済産業省
  - ●医療機器（日本医療機器産業連合会）
  - ●自動車（日本自動車工業会）
  - ●ソフトウェア（ソフトウエア協会）
- ■総務省
  - ●通信分野（スマホアプリ等）


ソフトウェア管理に向けた
SBOM（Software Bill of Materials）の導入に関する
手引
ver 2.0

経済産業省　商務情報政策局
サイバーセキュリティ課

令和６年８月２９日

SBOM導入のメリット

脆弱性管理　（直接的メリット）

- 残留リスク低減
- 対応期間短縮
- 管理コスト低減

（間接的メリット）

- 製品価値、企業価値向上
- サイバー衛生（サイバーハイジーン）向上

ライセンス管理（直接的メリット）

- ライセンス違反リスク低減
- ライセンス管理コスト低減

（間接的メリット）

- 製品価値、企業価値向上

開発生産性向上（直接的メリット）

- 開発遅延防止
- 開発コスト低減
- 開発期間短縮
- コンプライアンス対応の効率化
- 現場のモチベーション改善

組織の経営リスクの緩和・事業継続性への貢献

サプライチェーンのサイバーレジリエンス
― セキュリティ透明性の向上と活用 ―

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- サプライチェーン「汚染」リスク
- ソフトウェア透明性への取り組み
- セキュリティ・トランスペアレンシー・コンソーシアム概要
- コンソーシアムが公表した「知見集～脆弱性管理編」より

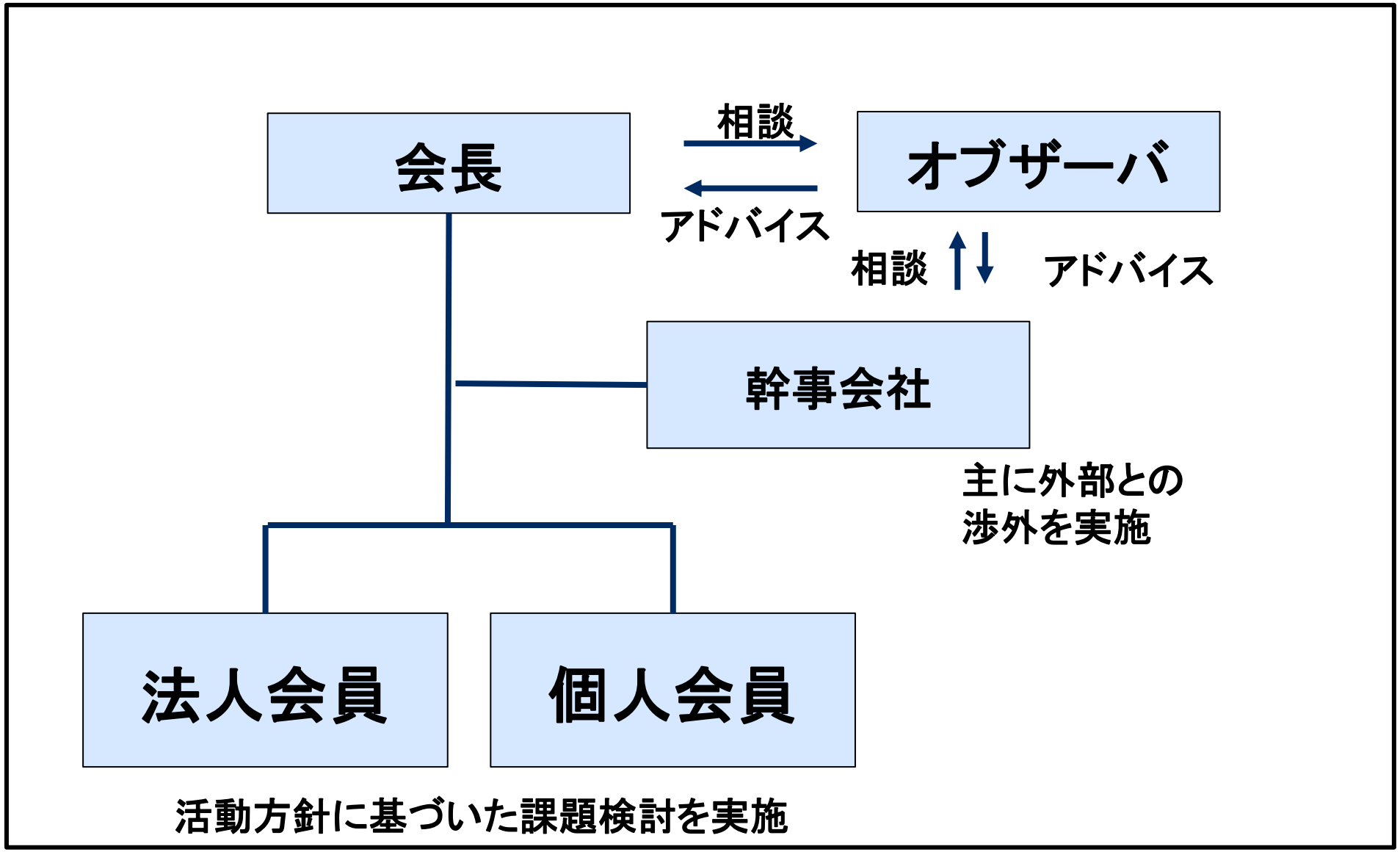
セキュリティ・トランスペアレンシー・コンソーシアム

■コンソーシアムの目的

- ◆ 製品、システム、サービス等における「セキュリティの透明性」を確保し、サプライチェーン及び運用の全体を通じてそれらを安全に利用可能にする。
- ◆ SBOMなどの可視化データの活用を通じて、サプライチェーン全体にわたってシステム等の構成の透明性を高め、自組織のみでは対応が難しいサプライチェーンセキュリティリスクの抜本的な低減をめざす。

名　称	セキュリティ・トランスペアレンシー・コンソーシアム
設立日	2023年9月21日
会　員	19社（2024年10月9日現在）
形　態	任意団体（法人格は持たない）
役　員	会長　後藤厚宏 （情報セキュリティ大学大学院学長）
ﾜｰｷﾝｸﾞｸﾞﾙｰﾌﾟ	可視化データ活用WG
会　費	無料
公式Webサイト	https://www.st-consortium.org/

コンソーシアムの構成


会長
相談
アドバイス
オブザーバ
相談
アドバイス
幹事会社
主に外部との
渉外を実施
法人会員
個人会員
活動方針に基づいた課題検討を実施

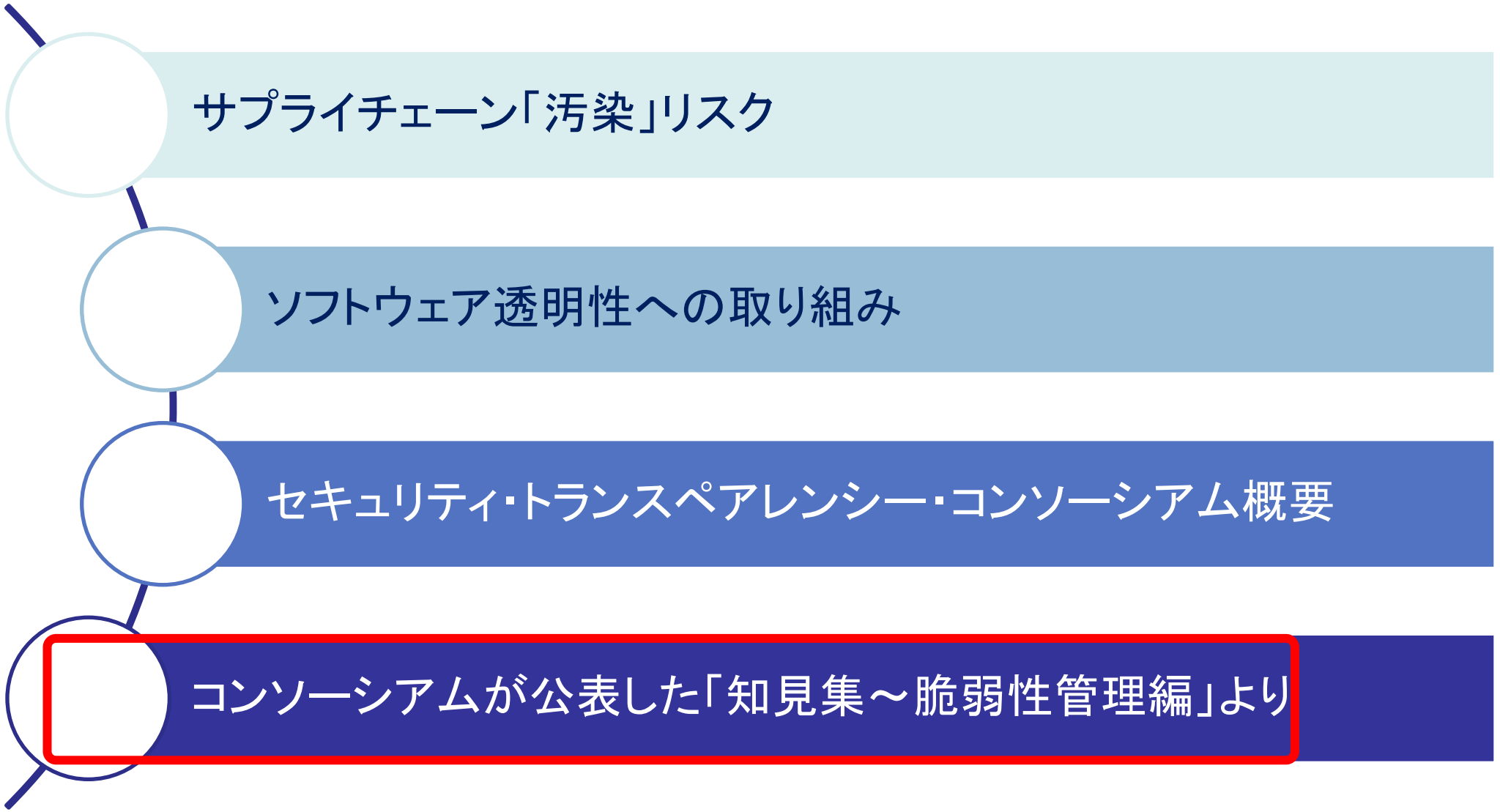
セキュリティ・トランスペアレンシー・コンソーシアム会員（2024/10/9現在）

- アズビル株式会社
- アラクサラネットワークス株式会社
- NRIセキュアテクノロジーズ株式会社
- 株式会社アシュアード
- 株式会社NTC
- 株式会社NTTデータグループ
- 株式会社FFRIセキュリティ
- 株式会社ジークス
- Contrast Security, Inc.
- Covalent株式会社
- サイバートラスト株式会社
- シスコシステムズ合同会社
- 東京エレクトロン株式会社
- 日本電気株式会社
- 日本電信電話株式会社
- 株式会社日立製作所
- 三井住友トラストグループ
- 三菱電機株式会社
- 株式会社ラック

可視化データ活用における8つの問題・課題

(1) 社会浸透・認知 可視化データの価値が具体的に理解できないため、どう利用してよいかわからない等	(5) 継続的な活用 ソフトウェア更新時に正しい可視化データを継続的に入手する必要がある等
(2) フォーマット・データ 可視化データを統一的に扱うために「つかう側」の活用方針を定めなくてはいけない等	(6) サプライチェーン上の調整 多段のサプライチェーン上で「つくる側」と「つかう側」の相互共有のしくみが必要等
(3) 技術・ツール 膨大な可視化データを扱うためには自動化が必要等	(7) 可視化データがもたらす影響 可視化データによってセキュリティの透明性が高まり、従来は見えず対処していなかった事象にも対処が必要となる等
(4) 活用コスト 可視化データの導入がもたらす業務の変化に対応するため、担当者の教育や関連ツールの習熟を効率的に行える必要がある等	(8) その他 可視化データ活用は従来の業務には含まれていないため、業務体制の見直しが必要になる等

サプライチェーンのサイバーレジリエンス
― セキュリティ透明性の向上と活用 ―



セキュリティ透明性確保に向けた可視化データ活用～脆弱性管理編～

2024年10月21日　プレスリリース

1. はじめに
2. 脆弱性管理における可視化データ活用の価値
   - 可視化データを活用した脆弱性管理におけるアクタとプロセス
   - 可視化データ活用によりもたらされる価値
3. 脆弱性管理において可視化データを「つかう側」が直面する課題
4. 課題に対処するための知見
5. おわりに

① 可視化データの品質

② 脆弱性管理における可視化データ活用

③ 可視化データの脆弱性対応に関し実施すべき教育プログラム

④ 既存の脆弱性管理からの段階的なマイグレーション

⑤ 可視化データの円滑運用に向けた体制整備

⑥ 脆弱性対応優先付けの指標

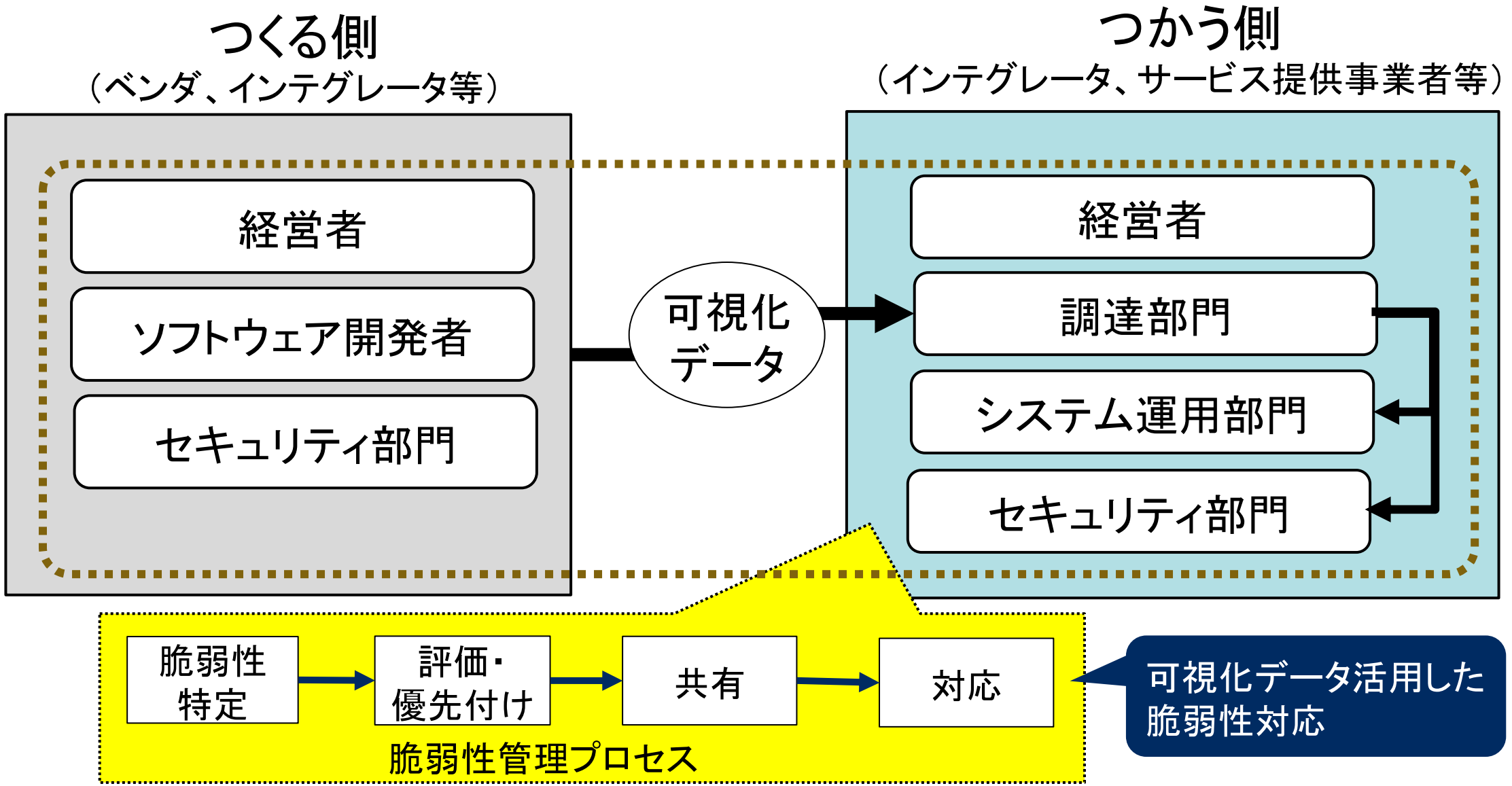
- SBOMと開発成果物間のトレーサビリティ確保
- 脆弱性評価基準

経済産業省　SBOMの導入手引き ver2.0

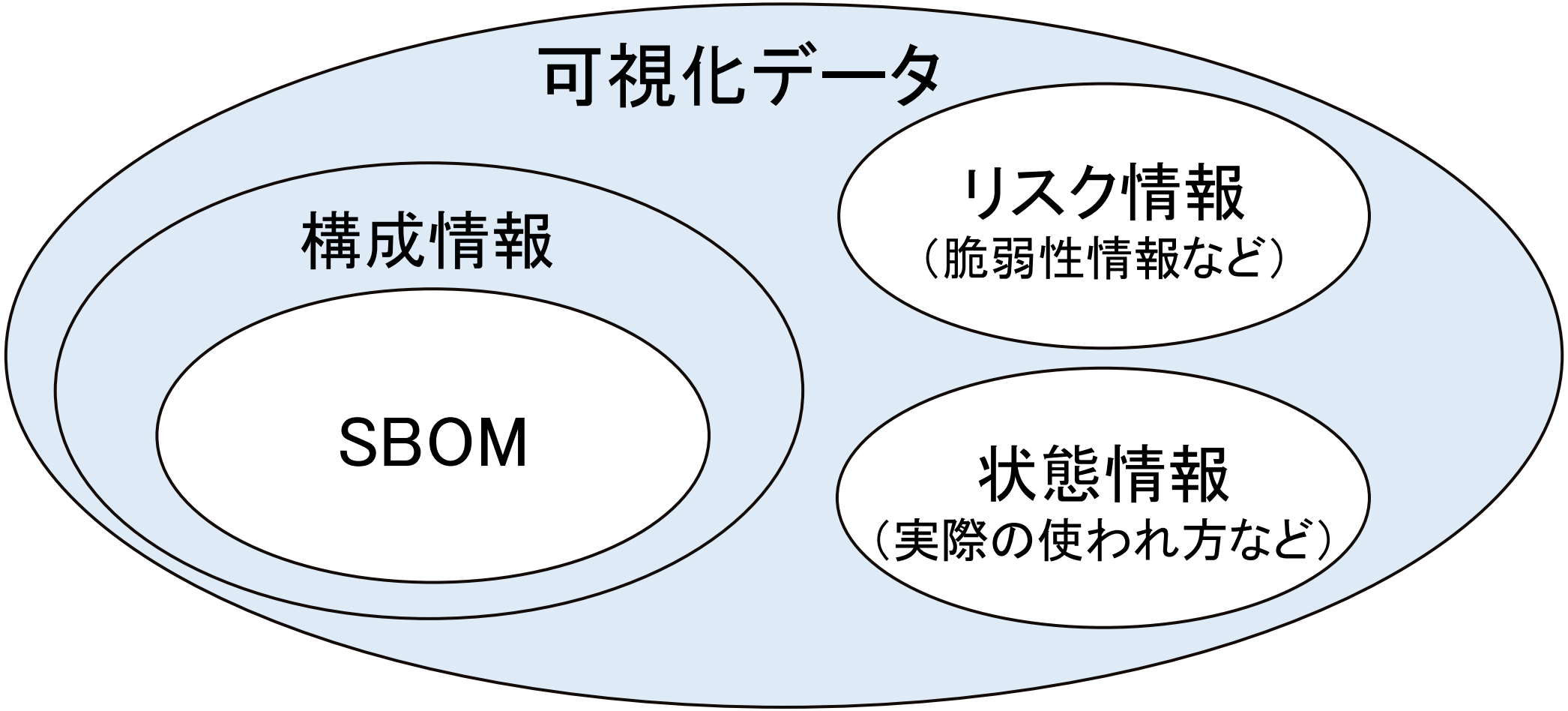
1. **背景と目的**
2. **SBOM の概要**
   - SBOM 導入のメリット、SBOM の「最小要素」とフォーマットの例、SBOM に関する誤解と事実
3. **SBOM 導入に関する基本指針・全体像**
   - SBOM 導入における基本指針とSBOM 導入プロセス
4. **環境構築・体制整備フェーズにおける実施事項・認識しておくべきポイント**
   - SBOM 適用範囲の明確化
   - SBOM ツールの選定、導入・設定 、学習
5. **SBOM 作成・共有フェーズにおける実施事項・認識しておくべきポイント**
   - コンポーネントの解析、SBOM の作成、SBOM の共有
6. **SBOM 運用・管理フェーズにおける実施事項・認識しておくべきポイント**
   - SBOM に基づく脆弱性管理、ライセンス管理等の実施、SBOM 情報の管理
7. **脆弱性管理プロセスの具体化**
   - 脆弱性管理における課題・問題認識
   - プロセス全像と各フェーズの手順と方法
8. **付録：SBOM 対応モデル**
   - SBOM 可視化フレームワークと対応モデル
   - SBOM 対応モデルと活用方法
   - SBOM 対応モデルの参考例（自動車分野）、ソフトウェア製品分野、医療機器分野）
   - SBOM 対応モデル（案）の分野横断比較

付録：SBOM 取引モデル・チェックリスト・用語集等

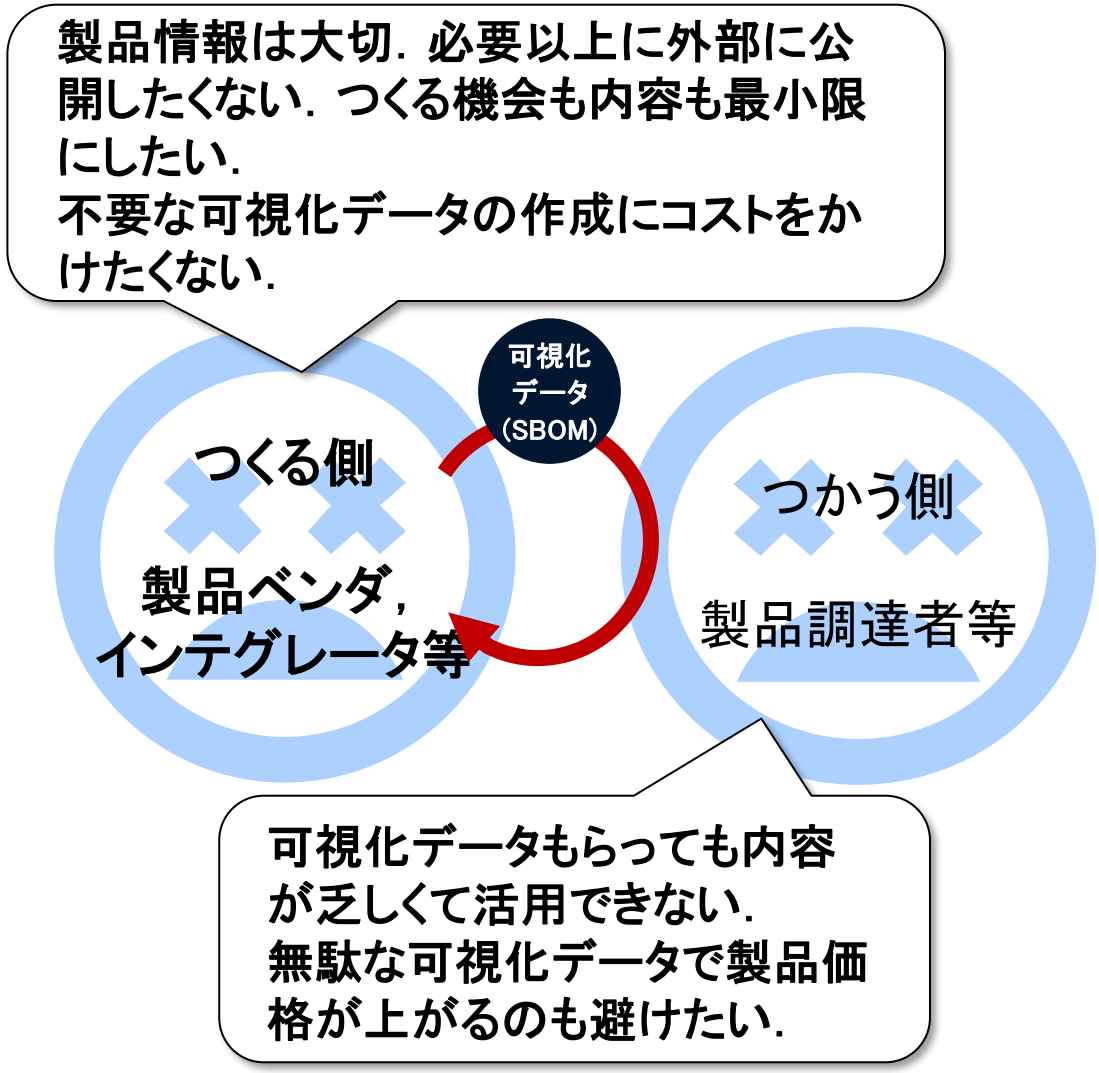
可視化データを活用した脆弱性管理の主なアクタとプロセス



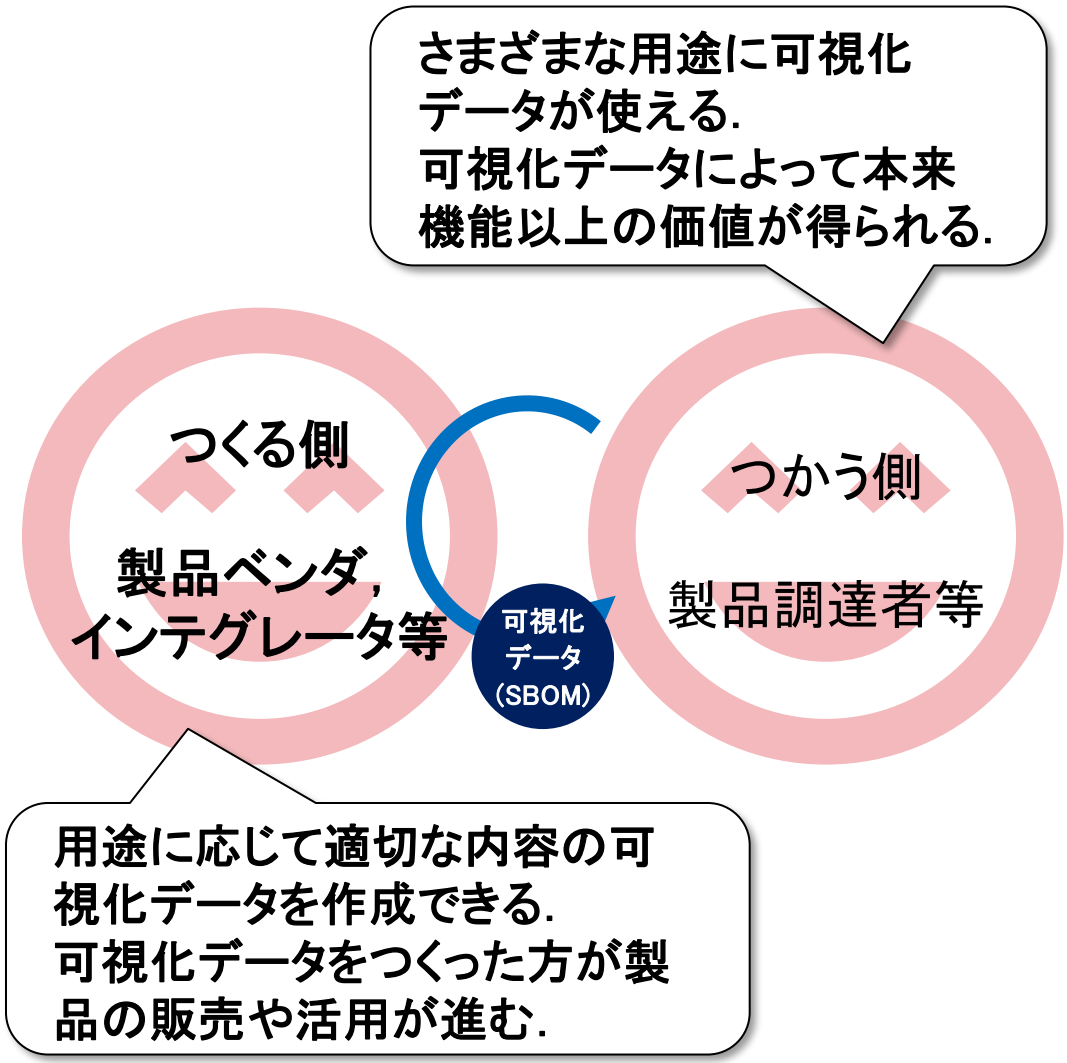
可視化データ：セキュリティ透明性の確保に活用



可視化データに関する「悪循環」と「好循環」



（a）つくる側とつかう側のギャップによる「悪循環」



（b）つかう側を起点としたつくる側との「好循環」

脆弱性管理への可視化データ活用知見

提起した問題・課題	脆弱性管理活用時の知見など
(1)社会浸透・認知	知見①～⑥により、脆弱性管理を先行事例とした可視化データ活用の価値を伝えていき、社会浸透を図っていく
(2)フォーマット・データ	**知見①:可視化データの品質指標** 対処すべき脆弱性を特定するために可視化データを正しく評価するための指標
(3)技術・ツール	**知見②:脆弱性管理における可視化データ活用** 多様な技術・ツールがある中で、「つかう側」が上手く使いこなすための知見
(4)活用コスト	**知見③:可視化データをつかうための教育** 業務変化に対応するために「つかう側」が必要となる教育
(5)継続的な活用	**知見④:既存業務からのマイグレーション** 可視化データの活用を一気に進められない場合の知見
(6)サプライチェーン上の調整	**知見⑤:可視化データの円滑運用に向けた体制整備** 組織内外の相互協力や合意形成に関する知見
(7)可視化データがもたらす影響	**知見⑥:脆弱性対応優先付けの指標** 大量に検出された脆弱性を適切に評価。優先付けするための指標
(8)その他	知見③④⑤は、業務体制の見直しが必要になる場合にも役立つ知見である

経産省の導入手引の脆弱性管理プロセス（知見①）

知見①
可視化データ
の品質指標

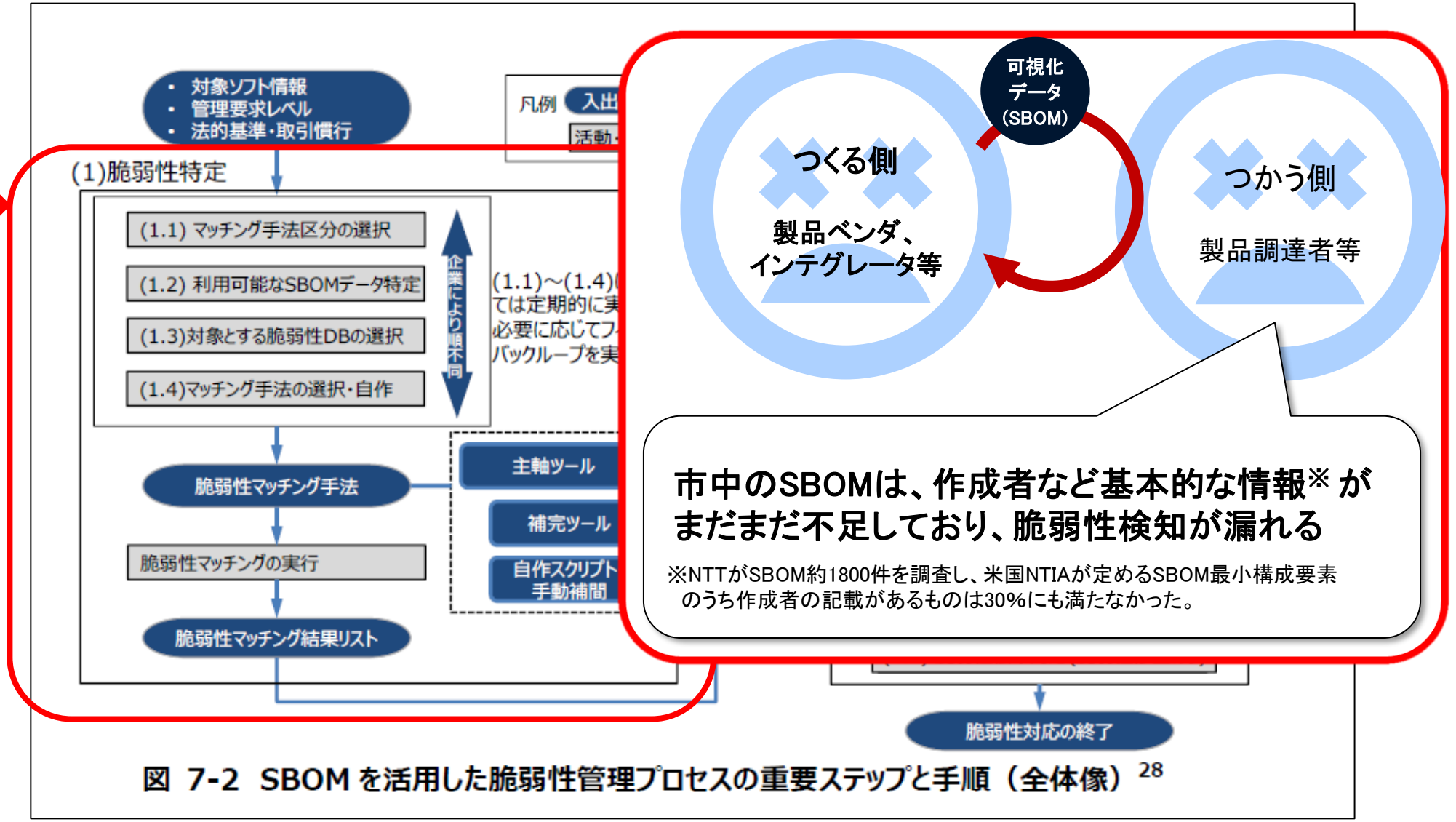


図 7-2 SBOM を活用した脆弱性管理プロセスの重要ステップと手順（全体像） 28

経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」から抜粋

知見①:可視化データの品質指標

可視化データは現状バラツキが多く、可視化データを用いた脆弱性管理は信頼性が低い。
入手した可視化データの品質を正しく評価する本知見により、対処すべき脆弱性の特定に寄与する

可視化データの品質上の課題	内　　容
最小要素不足	SBOMの実データを調査したところ、米国NTIAが定めるSBOMの最小要素の記載割合は以下の通りで、作成者や作成時刻の記載は非常に**少ない**状況である
要素の表現が不適切・表記ゆれ	SBOMの要素にはソフトウェアの開発元を示すベンダ項目があるが、開発元が示されない場合がある。また略称等を用いる場合もあり、正式名称とのマッチングがとれない
コンポーネントの網羅性	ソースコードのコピーペーストや一部を改変した再利用によって発生するパッケージ情報には記されないソフトウェアの依存関係があり、脆弱性に気づけない

要　素	記載割合
SBOMの作成ツールやコンポーネントに関する名称や識別子	9割程度
ベンダやバージョン	6割程度
SBOMの作成者	3割程度
SBOMの作成時刻	1割程度

＊NTTによる約1800件の調査

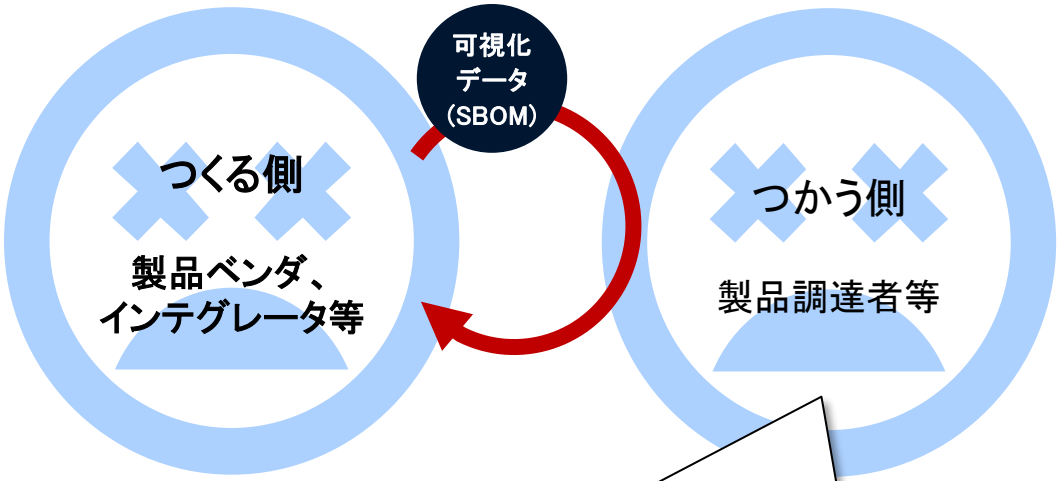
可視化データの
品質指標

分　　類	観　　点
提供情報の豊富さ	ソフトウェアに対して十分説明がなされているか
	コンポーネントに対して十分説明がなされているか
提供情報の正確さ	コンポーネントに関する追加情報の提供があるか
	コンポーネントに関する情報の意図的な消去があるか
	コンポーネントが十分可視化できているか
	依存関係の深さが十分可視化できているか

知見①：可視化データの品質指標

- 知見概要
  - バラツキのある可視化データを正しく評価するための指標
  - ソフトウェアの目的・動作を説明するに十分な量か、依存関係の深さが可視化できているか等で評価

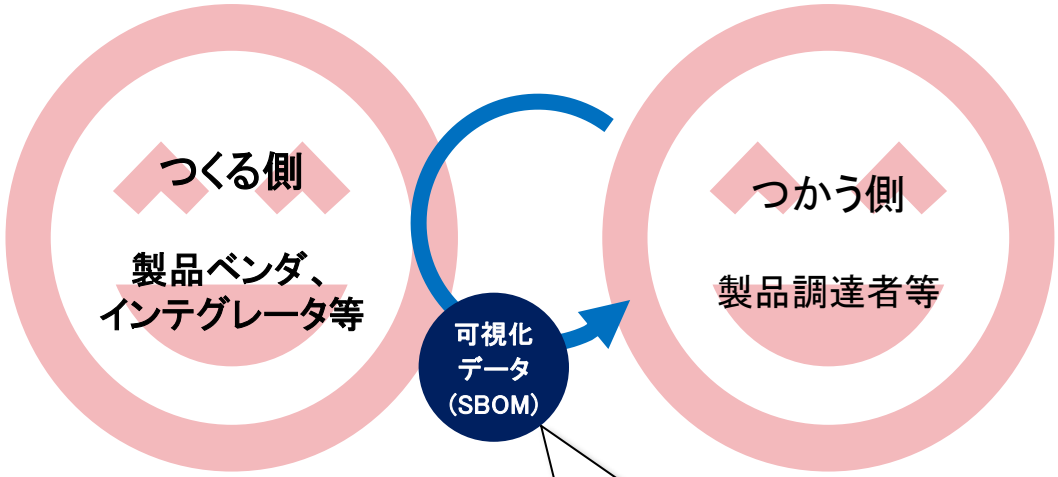
【フォーマット・データ】の問題・課題



市中のSBOMは、作成者など基本的な情報※ がまだまだ不足しており、脆弱性検知が漏れる

※NTTがSBOM約1800件を調査し、米国NTIAが定めるSBOM最小構成要素のうち作成者の記載があるものは30%にも満たなかった。

【知見①の効能など】



入手した「可視化データ」の品質を評価し、対処すべき脆弱性を特定できる

経産省の導入手引の脆弱性管理プロセス（知見⑥）

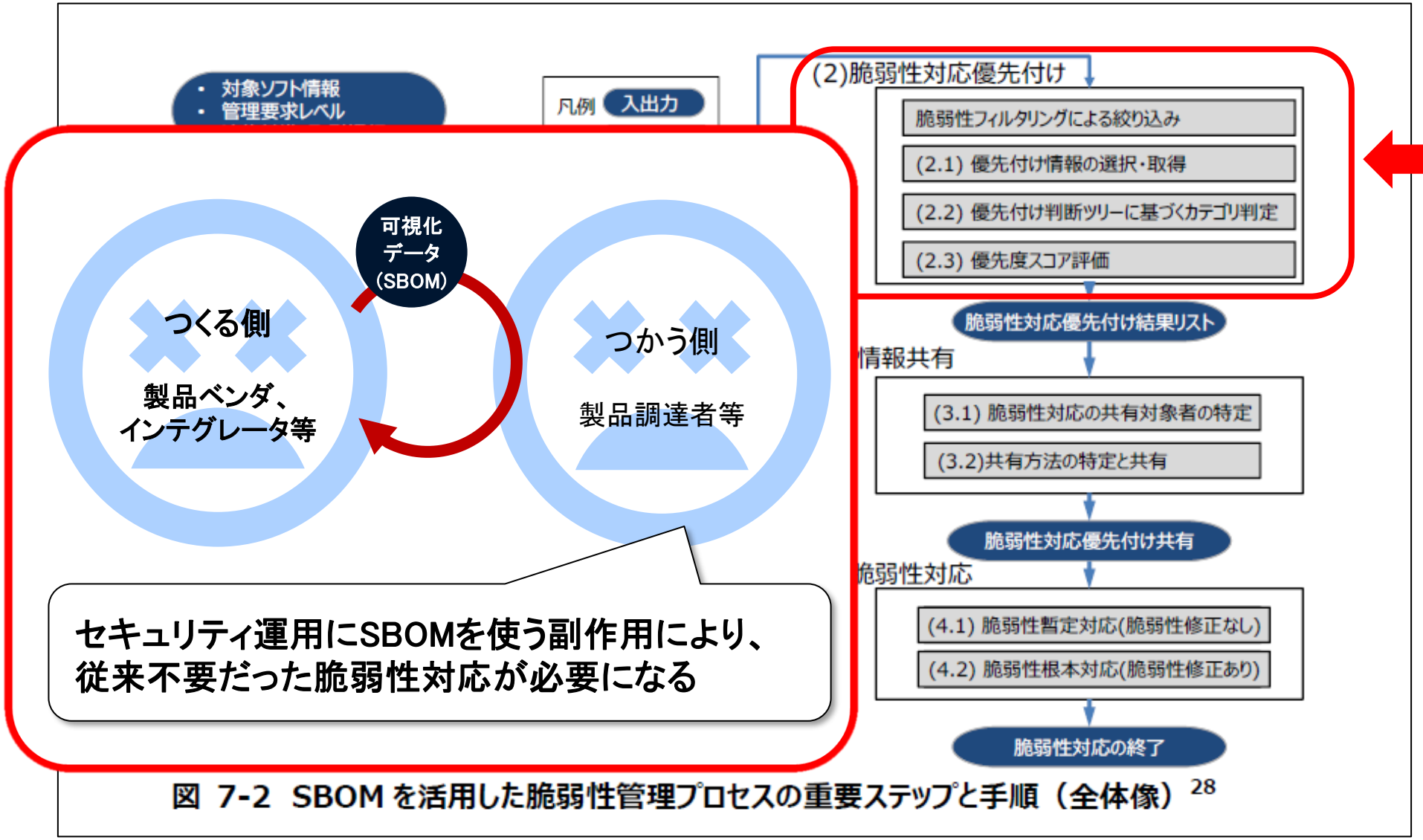


図 7-2 SBOM を活用した脆弱性管理プロセスの重要ステップと手順（全体像）[28]

知見⑥
脆弱性対応
優先付けの
指標

経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」から抜粋

知見⑥:脆弱性対応優先付けの指標

可視化データの副作用として、本来対応の必要のない脆弱性までもが多数発見される可能性がある。
脆弱性がシステムに与える影響を評価する本知見により、脆弱性対応の優先度対応に寄与する

CVSSの評価基準	概　　要
(1)基本評価基準	• 脆弱性そのものの特性を評価する基準 • ネットワークから攻撃可能かどうかといった基準でCIAを評価し、CVSS基本値(Base Score)を算出
(2)現状評価基準	• 脆弱性の現在の深刻度を評価する基準。 • 攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS現状値(Temporal Score)を算出
(3)環境評価基準	• 製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準 • 攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準で評価し、CVSS 環境値 (Environmental Score) を算出

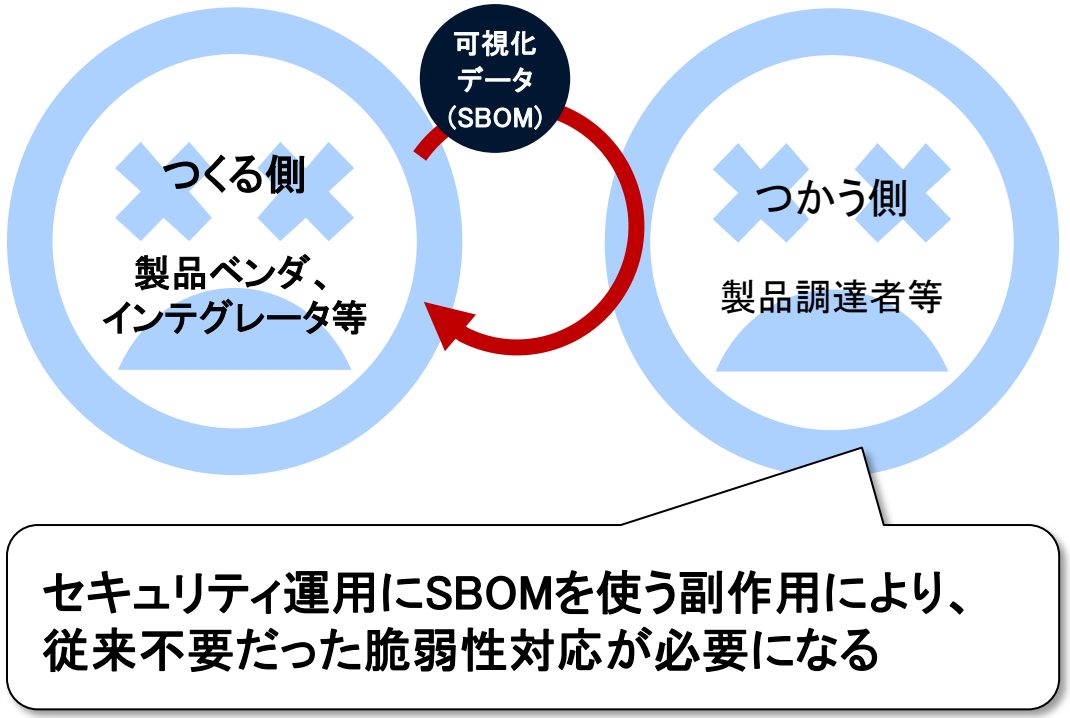
・上記評価基準の使い方(分担)の例
1)「つくる側」:基本評価基準で評価し、その結果を「つかう側」に通知
2)「つかう側」:「つくる側」からの評価結果に加え、自身のシステムでの環境評価基準で評価(※)

(※)脆弱性があっても基本評価基準のCVSSスコアが小さいことを理由に、「つくる側」が可視化データを作成しない場合もあるが、「つかう側」は、自身の環境評価基準での評価結果を数値で示すことで対応をしなければリスクが大きいことがわかり、可視化データの作成を主張できる

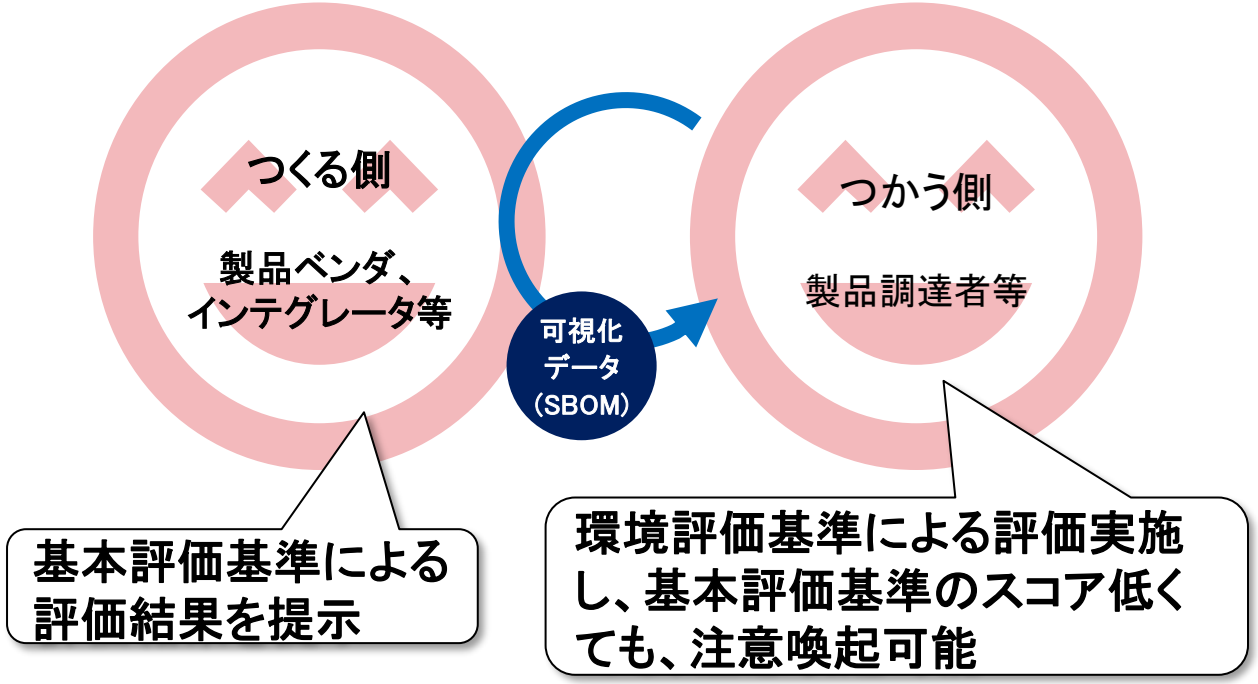
知見⑥:脆弱性対応優先付けの指標

- 知見概要
  - SBOMと開発成果物(ドキュメント、ソースコードなど)のトレーサビリティ確保し、関連文書・ファイルを探し出す時間短縮の事例
  - 脆弱性のトリアージ方法(CVSSの評価基準の利用方法など)

【知見活用前】



【知見⑥の効能など】



経産省の導入手引の脆弱性管理プロセス（知見③）

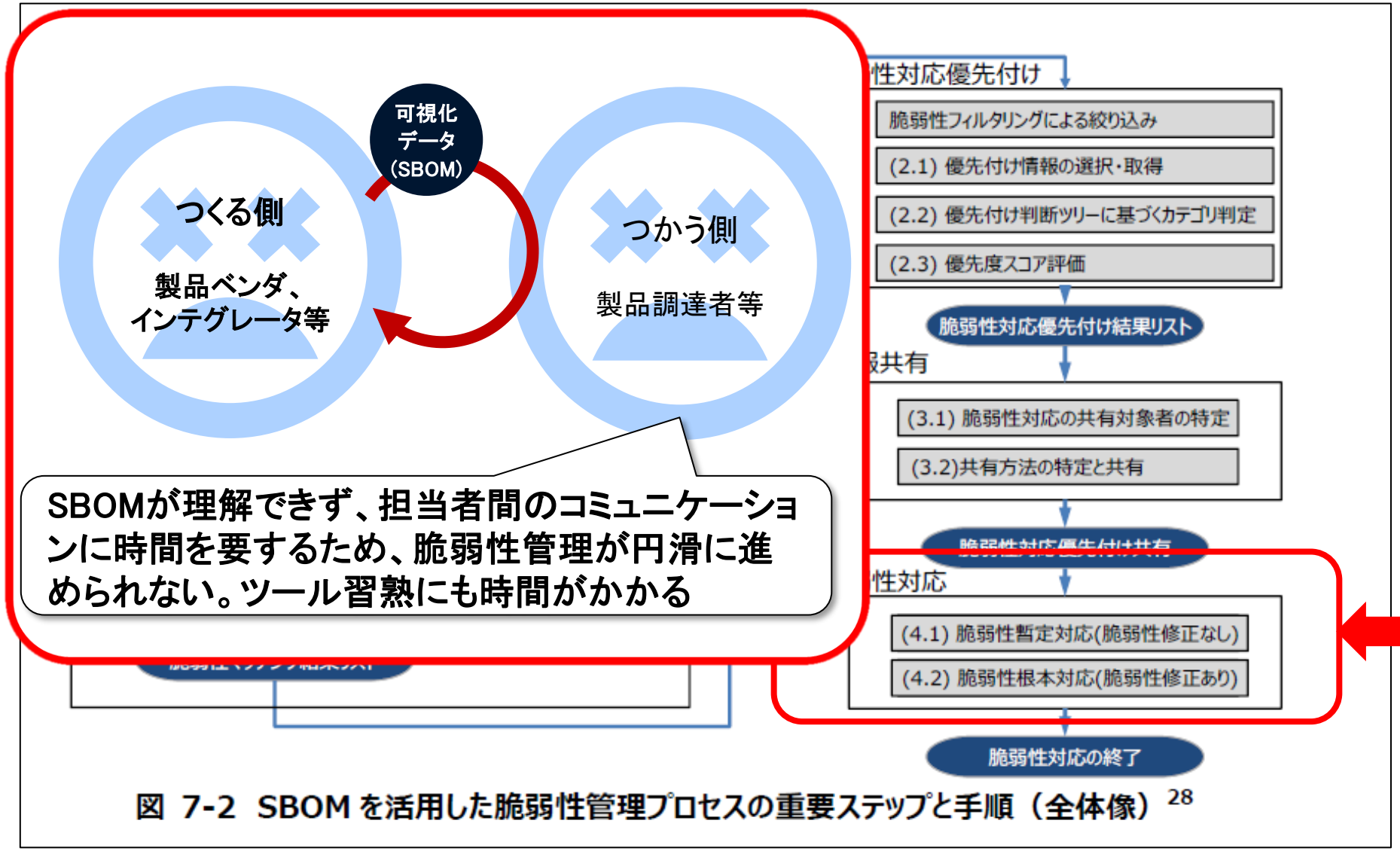


図 7-2 SBOM を活用した脆弱性管理プロセスの重要ステップと手順（全体像）[28]

知見③
可視化データを
つかうための
教育

経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」から抜粋

知見③：可視化データをつかうための教育

可視化データが理解できない担当者とのコミュニケーションに時間を要し、脆弱性管理が円滑に進められない。
教育プログラムと実施時の注意点や効果なども示した本知見により、脆弱性対応の工数削減に寄与する

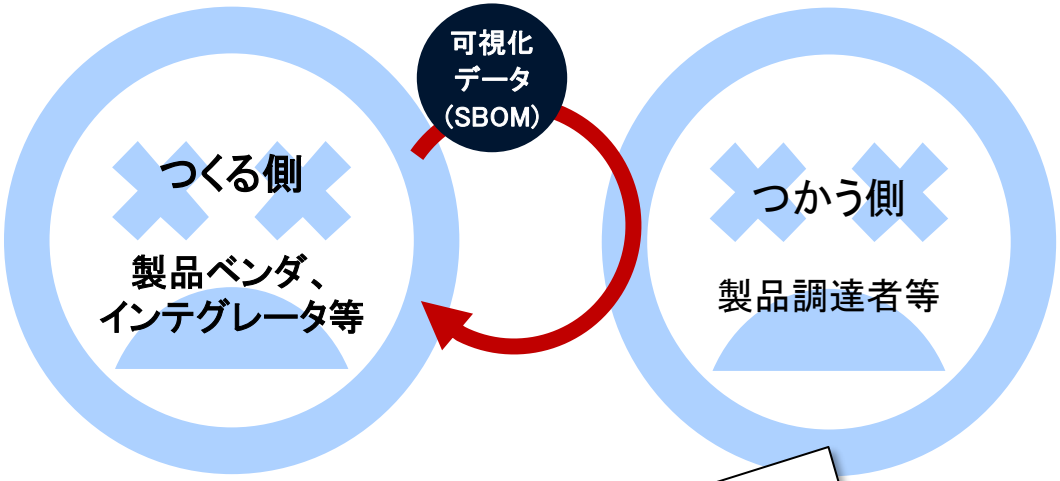
教育プログラム	注意点・効果など
(1)SBOMを理解するための前提知識	生成AIによる自動コード生成の利用が広がっていることへの対応として、**生成AI**のOSSコードスニペット出力による脆弱性混入の可能性に言及したが非常に有用
(2)SBOMの意義 • セキュリティ担当者向け：脆弱性の自動監視 • システム部門向け：開発時検証の効率化等	受講者の**業務におけるメリット**に言及することが重要 例えば、セキュリティ部門の担当者に対しては脆弱性の自動監視の実現を訴求した一方、利用者・ソフトウェア運用部門・ソフトウェア開発者に対しては利用コンポーネントの可視化による開発時検証の効率化や、脆弱性発生時の対応責任有無のエビデンスとして利用可能な点を訴求
(3)SBOMの構成と解読方法 • SBOMの実データを交えた解説等	**SBOMの実データ**をみせることが非常に効果的 SBOM規格の位置づけや制約についても解説することで、SBOM規格についての知識普及や誤解の解消にもつながった
(4)社内におけるSBOM運用ルール • SBOM作成活用の必要業務や自社業務との対応関係	ソフトウェアサプライチェーン・ソフトウェアライフサイクルにおいて、SBOMを作成・活用するために必要な業務や、**自社の業務との対応関係**を示すことで、わかりやすいとの意見あり
(5)SBOMツールの運用方法 • 実際のツールを表示・操作しつつ手順の解説	**実際のSBOMツールを表示・操作**しつつ手順を解説することで、受講者がSBOM運用を具体的にイメージできるようになった

知見③：可視化データをつかうための教育

■ 知見概要

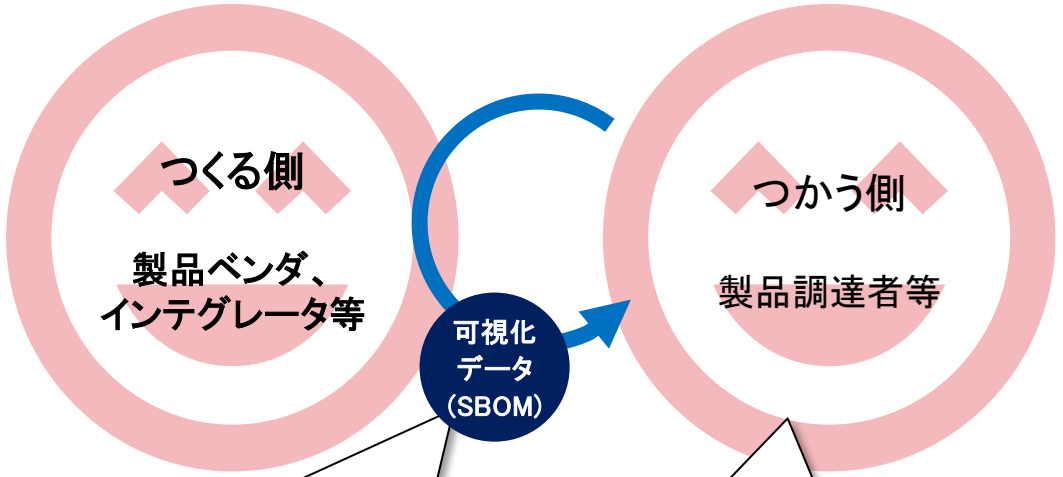
- 実際に実施した教育プログラム例と、実施時の注意点や効果を示す
- SBOMの意義、実データを用いた解説、自社業務との対応関係、ツールを用いた運用方法など

【活用コスト】の問題・課題



SBOMが理解できず、担当者間のコミュニケーションに時間を要するため、脆弱性管理が円滑に進められない。ツール習熟にも時間がかかる

【知見③の効能など】



SBOMに関する理解が深まり、「つくる側」とのコミュニケーションもスムーズ

入手したSBOMを理解できるので、「つかう側」内部での意思決定がスムーズ

まとめ

サプライチェーンのセキュリティリスク

・サプライチェーンの「汚染」リスク ⇒ 「透明性」の確保

セキュリティ・トランスペレンシー・コンソーシアム

SBOM等による可視化データを「つかう（運用・管理）」の立場から

・知見を協創し、広く共有

・コミュニティ作り

・外部連携

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

セキュリティ・
トランスペアレンシー・
コンソーシアム
https://www.st-consortium.org/

情報セキュリティ大学院大学
https://www.iisec.ac.jp
後藤厚宏
goto@iisec.ac.jp