SDVにおける継続的サイバーセキュリティ活動の必要性
@第45回 ReVision ウェビナー

2025/11/05

一般社団法人 Japan Automotive ISAC
サイバーセキュリティエコシステム構築センター（CSECC）
センター長
山 﨑 雅 史　（所属会社： 

マツダ株式会社）

AGENDA

0. 自己紹介
1. SDVを取り巻く「規制・標準」の動向
2. SDVにおける継続的サイバーセキュリティ活動の必要性

SDVを取り巻く「規制・標準」の動向

主要各国のCS/SU法規の適用日程

撮影不可

Intentionally Blank

SDVを取り巻く「規制・標準」の動向

UNR155と中国GB44495-2024の相違点

撮影不可

Intentionally Blank

SDVを取り巻く「規制・標準」の動向

サイバーセキュリティ関連の車両法規の動向

撮影不可

■ **Cybersecurity・Anti-tamperingが各法規へ展開**

Intentionally Blank

✓CybersecurityとAnti-tamperingについて
関係者間の議論（目的・施策の混同、UN-R155の拡大解釈）への留意が必要

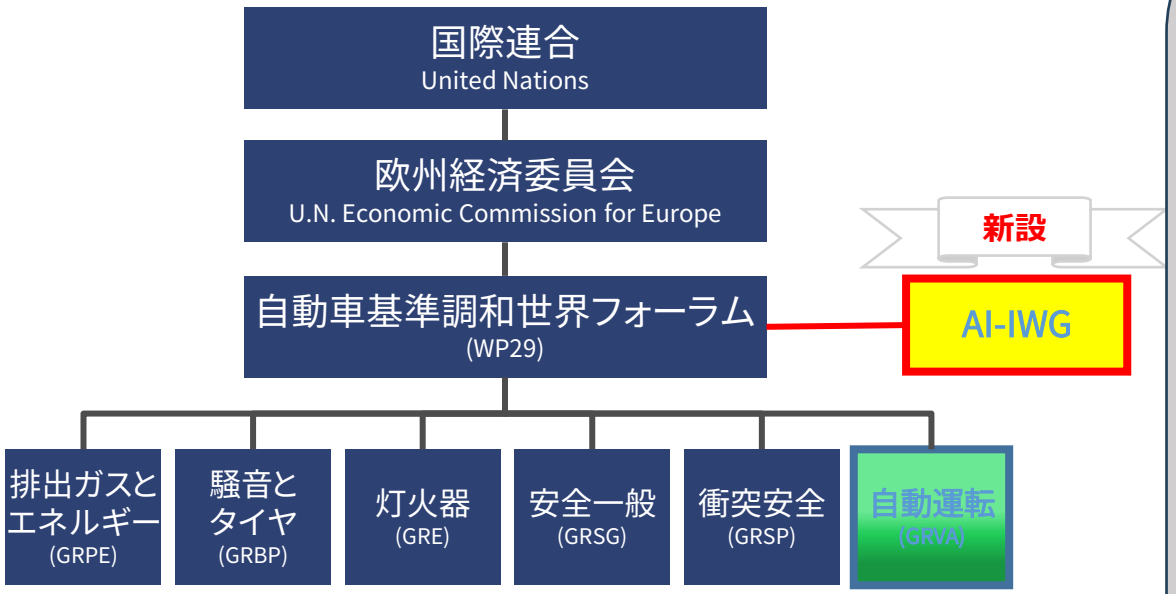
クルマを取り巻くセキュリティ

サイバーセキュリティ関連の車両法規の動向

撮影不可

■ Artificial Intelligence in vehicles

●WP29傘下にAIインフォーマルグループ（AI-IWG）の設置が承認され審議開始



Intentionally Blank

AGENDA

0．自己紹介
1．SDVを取り巻く「規制・標準」の動向
2．SDVにおける継続的サイバーセキュリティ活動の必要性

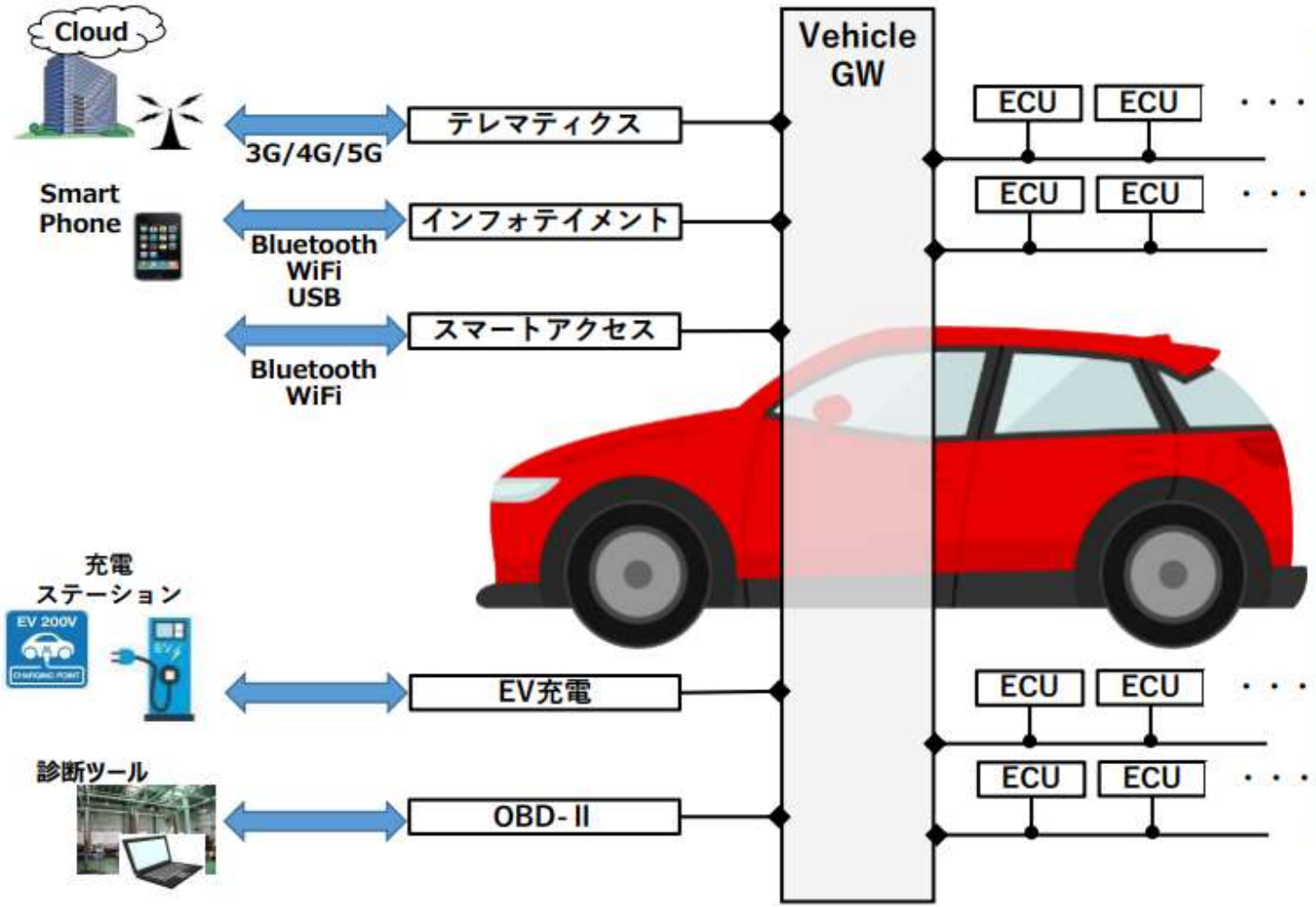
継続的サイバーセキュリティ活動の必要性

クルマのセキュリティ脅威・インシデントは多種・多様

分類		脅威・攻撃	影響・損害の可能性	インシデント事例
制御系	安全系	・ブレーキ、ハンドル操作、エンジンなどに対する不正な制御 ・走行制御ロジックの改ざん ・センサーデータ改ざん	人命に係るセーフティへの侵害	テレマテクス装置TCU Dongleの脆弱性悪用
			リコールによる経済的損失	クライスラーUconnect脆弱性 140万台リコール
	安全以外	・ドアロック不正操作、エンジン始動	自動車盗難	イモビライザー解除ツール
		・ワイパー不正操作、その他ボディ系不正操作	意図しない動作による不安感の誘発	クライスラーUconnect脆弱性悪用
			バッテリー上がり、電力消費	―
情報系	情報窃取	・任意の情報操作コマンドの実行	任意の情報の外部送信、詐欺被害	GMテレマティクスOnStar RemoteLink アプリの脆弱性
		・ドライブレコーダログ情報改ざん、DoS攻撃	保険、情報サービスの妨害	自動車遠隔管理サーバへの不正ログイン
	その他、プライバシー侵害等	・位置情報、車両情報、運転履歴情報、個人情報の漏えい ・クラウド系攻撃	プライバシー侵害	無線ネット技術の漏えい
		・その他通信情報の盗聴	情報漏えい	車車間WLAN 802.11pの盗聴

継続的サイバーセキュリティ活動の必要性

クルマに係る最新の脆弱性動向



＜リモート＞
- 長距離無線通信
  セルラー回線など
- 中/短距離無線通信
  Bluetooth, WiFi, NFCなど

＜物理アクセス＞
- USB、SDカードなど
- 充電ポート
- OBDポート
- 車両周囲状況を監視するためのセンサー
- CANなどの車載ネットワーク
- ECUに実装されているCPU
- ECUに実装されているプログラム（OSSなど）

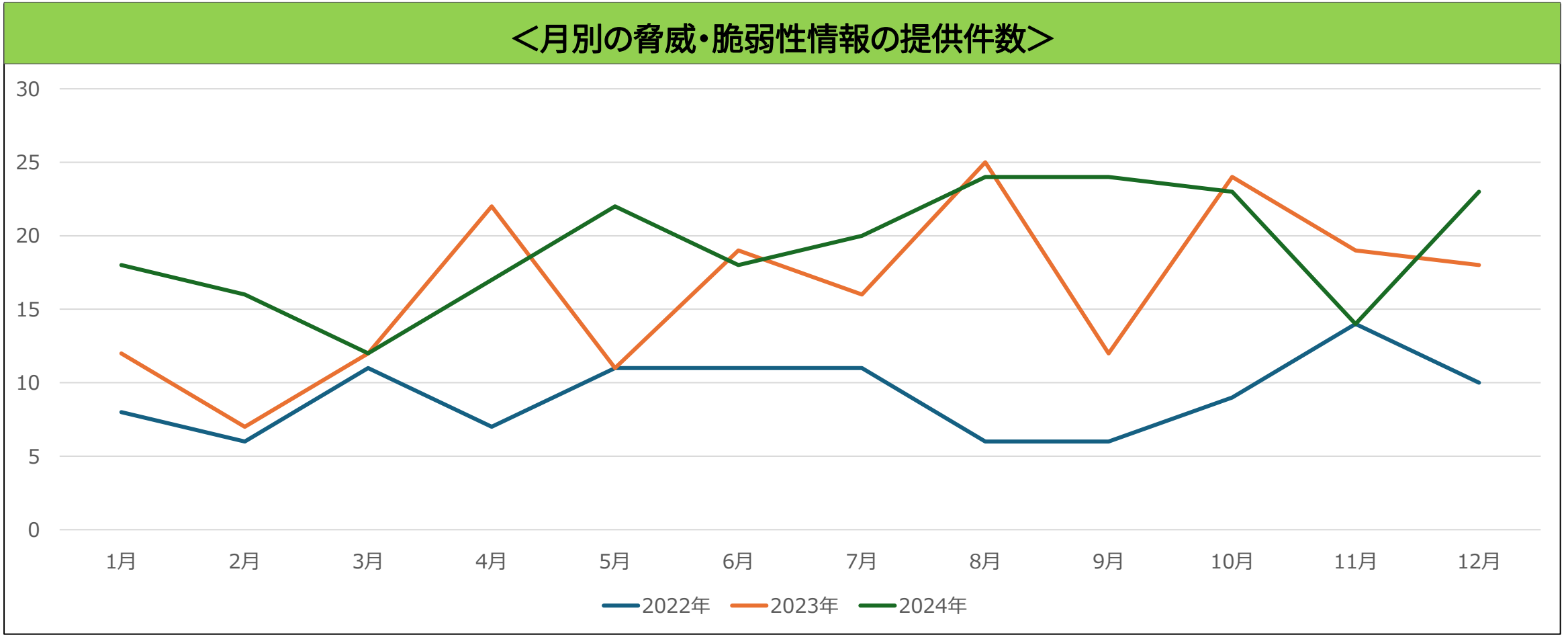
＜その他＞
- ソフトウェア開発環境など

自動車は多くのシステムで構成されているが、さまざまな部位で脆弱性を検出

継続的サイバーセキュリティ活動の必要性

J-Auto-ISACからの情報提供件数推移

撮影不可



脅威・脆弱性情報の提供件数（年間）は右肩上がりで増加の一途
2022年：110件↗　2023年：197件↗　2024年：231件

※自動車に係わる案件以外は，カウントから除外

継続的サイバーセキュリティ活動の必要性

SOC（Security Operation Center)による傾向分析

撮影不可

①発見者の傾向

②対象システムの傾向

Intentionally Blank

③インフォテイメントにおけるアクセス経路

Intentionally Blank

※2024年度　自動車に係わる案件の傾向分析

継続的サイバーセキュリティ活動の必要性

継続的サイバーセキュリティ活動とは？

サイバーセキュリティ活動

サイバーセキュリティ情報の監視 → サイバーセキュリティイベント評価 → 脆弱性分析 → 顕在化した脆弱性への対応
- 脆弱性管理
- サイバーセキュリティインシデントレスポンス

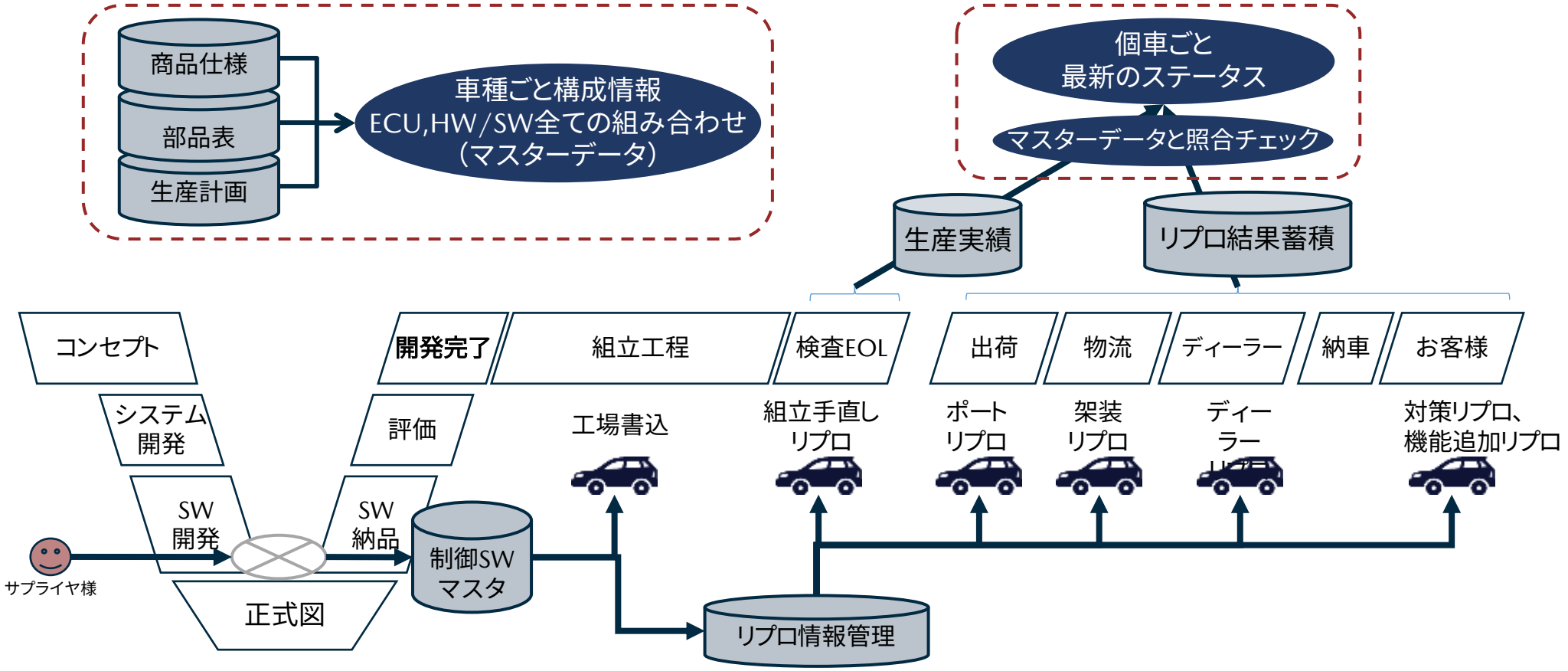
これまでのクルマの品質保証の仕組み

設計検証 / 不具合解析 / 市場対応

これまでのクルマの品質保証の仕組みにサイバーセキュリティ活動を加え、ライフサイクルにおけるインシデント発生のリスクを下げる取り組み

継続的サイバーセキュリティ活動の必要性

法規を満足した上で、リスクへの対応を確実に行っていくためには・・・



ライフサイクルにわたって脆弱性対応を余儀なくされることからソフトウェアのアップデートは必須であり、SU法規を満足するためには「トレーサビリティ管理」が必要

継続的サイバーセキュリティ活動の必要性

継続的サイバーセキュリティ活動へのSBOM活用

SBOM (Software Bill of Materials)とは？

■『SBOMとは、**ソフトウェアコンポーネント**やそれらの**依存関係**の情報も含めた**機械処理可能**な一覧リストである。』

– 経済産業省「ソフトウェア管理に向けたSBOMの導入に関する手引き」[1]より –

■『SBOMは、**ソフトウェアのコンポーネント**とその**依存関係**、及びライセンスデータを一意に識別する、形式的で**機械可読なメタデータ**です。（中略）ソフトウェアサプライチェーンの参加者によって提供されるコンポーネントの透明性を提供するのに役立ちます。』

– The Linux Foundation「SBOMとサイバーセキュリティへの対応状況」[2]より –

定義で捉えるSBOMの概要

■ **SBOMを構成する情報の要素（例）**

- **ソフトウェア(コンポーネント)の情報**
- **ソフトウェアコンポーネント同士の依存関係の情報**
- **ライセンスデータ**
- **etc**

■ **データの特性**

- **機械処理可能／機械可読**
- **メタデータ**

(ソフトウェアというデータを説明するデータ)

■ **SBOMの用途・効果**

- **ソフトウェアコンポーネントの透明性を提供**

出所： 1.「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き Ver. 1.0」, 経済産業省, 2023
2. Stephen Hendrick,「SBOM(ソフトウェア部品表)とサイバーセキュリティへの対応状況」, The Linux Foundation, 2022

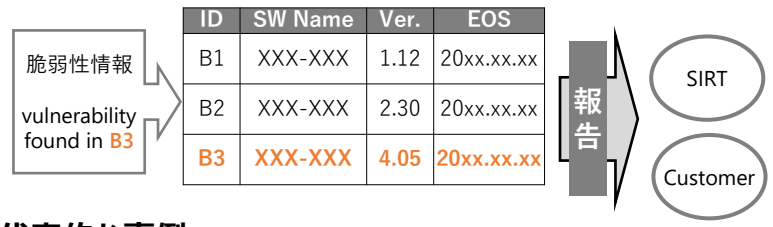
SBOMとは、ソフトウェアコンポーネントとその依存関係に関する情報

継続的サイバーセキュリティ活動へのSBOM活用

SBOMの活用ユースケース

脆弱性管理

システム／製品の脆弱性の確認や対応状況を管理する



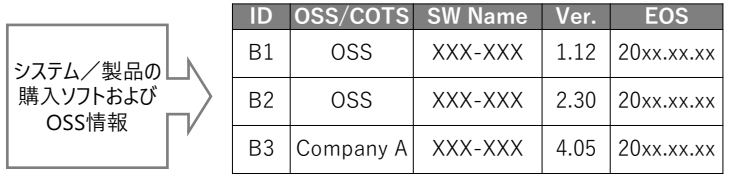
代表的な事例

- 管理するソフトウェアにおいて脆弱性が見つかった場合の対応を実施する（SIRT・インシデント対応プロセス連携）
- 製品のパッチ適用状況についての対応状況トラッキングと監視
- 脆弱なエンドポイントの迅速な特定
- 既存の脆弱性が指摘されているソフトウェアの特定（脆弱性モニタリング）

- SBOMの応用的な利用

ライセンス管理

システム／製品に含まれる購入ソフトやOSSのライセンスを管理する



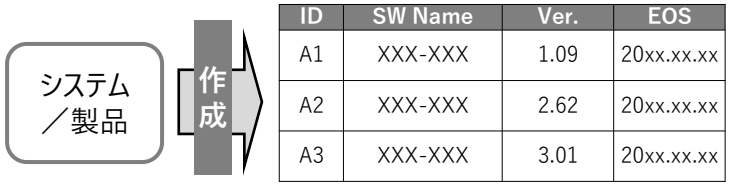
代表的な事例

- 使用または再配布の制限を含むソフトウェアのライセンスを管理

- SBOMの最初の利用目的
- SPDXフォーマットが開発された元々の理由

その他の資産管理

システム／製品のインベントリを様々な用途に活用



代表的な事例

- 企業内のソフトウェアを継続的に監視（資産管理）
- ソフトウェアのライフサイクル管理のサポート
  （自社の医療機器のサポート終了期間を管理）
- コンポーネントの記録システムとしての活用
  （外部から信頼できる情報源として参照される）

- 調達に関する制限のチェックなど
- SBOMの新しい注目領域

継続的サイバーセキュリティ活動へのSBOM活用

SBOMはセキュリティコミュニケーションの共通言語

1. **脆弱性検査のレポート報告**
   - 脆弱性スキャンの実施
2. **SCAコンポーネントの動作保証**
   - SBOMデータの保存と分析

脆弱性検査とSBOM出力

3. **検出された脅威の調査や対応**
   - パッチ管理など
4. **脅威の無力化に関する報告**
   - 対処レポートとSBOMデータの提出

SBOMデータを利用した
脅威の発見と開発運用評価

脆弱性管理

他社でみつかった脆弱性が自社のプロダクトやサービスに影響するかどうかを
常に漏れなく確認できるためには、「監視運用体制の整備が鍵！」

※SCA(Software Composition Analysis)コンポーネント：ソフトウェアに含まれるオープンソースやサードパーティ製のライブラリ・モジュールを分析・管理するためのツールや機能

脆弱性検査をしてSBOMデータを出力するだけでは、SBOM活用とはいえない

継続的サイバーセキュリティ活動の必要性

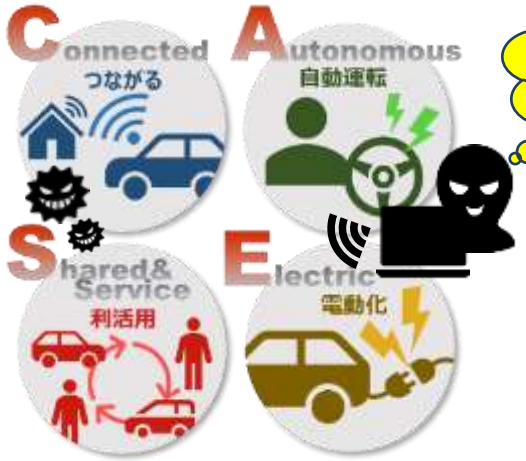
クルマを取り巻くセキュリティの現状と課題まとめ

日々変化するサイバーリスク

車の利便性向上（CASE革命）による
新たなサイバーリスクの発生

サプライチェーンへのサイバー攻撃増加

企業規模にかかわらず
サイバーリスクがある



ソフトウェアに存在するセキュリティホールが狙われる

法規制への対応

UN-R155/UN-R156
認証の取得

EU：
Data act/CRA・・・

セキュリティホールをマネジメントする仕組みを
文書化し、運用しなければならない

必須要件への対応は
できている？

個社対応の限界

カバーすべき領域の拡大

資金面や工数面でのコスト負担

セキュリティ人材不足

複雑なサプライチェーン

自社だけで守り切れる？

ご清聴ありがとうございました！

J-Auto-ISAC
Japan Automotive Information Sharing and Analysis Center

ホームページ：　https://j-auto-isac.or.jp/

〒108-0075　東京都港区港南2丁目3番13号　品川フロントビル
一般社団法人 Japan Automotive ISAC　事務局　jimukyoku@j-auto-isac.com