JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

JAMA電子情報フォーラム2020

サイバーセキュリティ部会
自動車業界のフレームワークの取組

一般社団法人　日本自動車工業会

電子情報委員会
サイバーセキュリティ部会
サイバーセキュリティ統括分科会
分科会長：坂　季也

2020年2月13日

目次

1. 自動車業界のセキュリティリスク

2. セキュリティ事故事例

3. セキュリティガイドライン検討の活動説明

4. 今後の予定

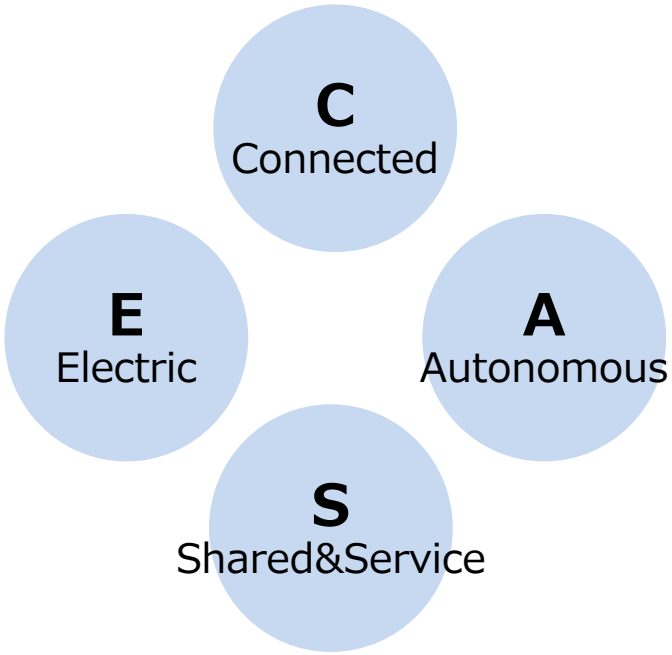
5. 最後に

1-1. 自動車業界の環境変化

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

・自動車業界は、ＣＡＳＥをはじめとして100年に一度の大変革期
・業界全体がモビリティ社会の実現に向けてIT利活用を促進

急速な技術革新

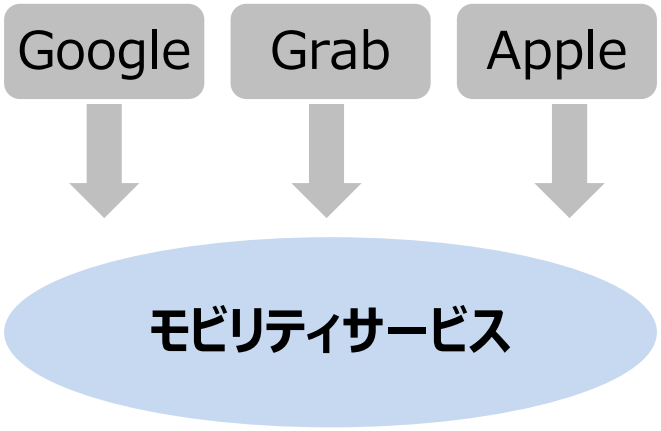


「コネクティッド」、「自動化」、「シェアリング」、「電動化」4つの革新が同時に発生(**CASE革命**)

競争領域の拡大

自動車製造からモビリティサービスへ
産業全体のドメインが大きく変化

競合企業の変化



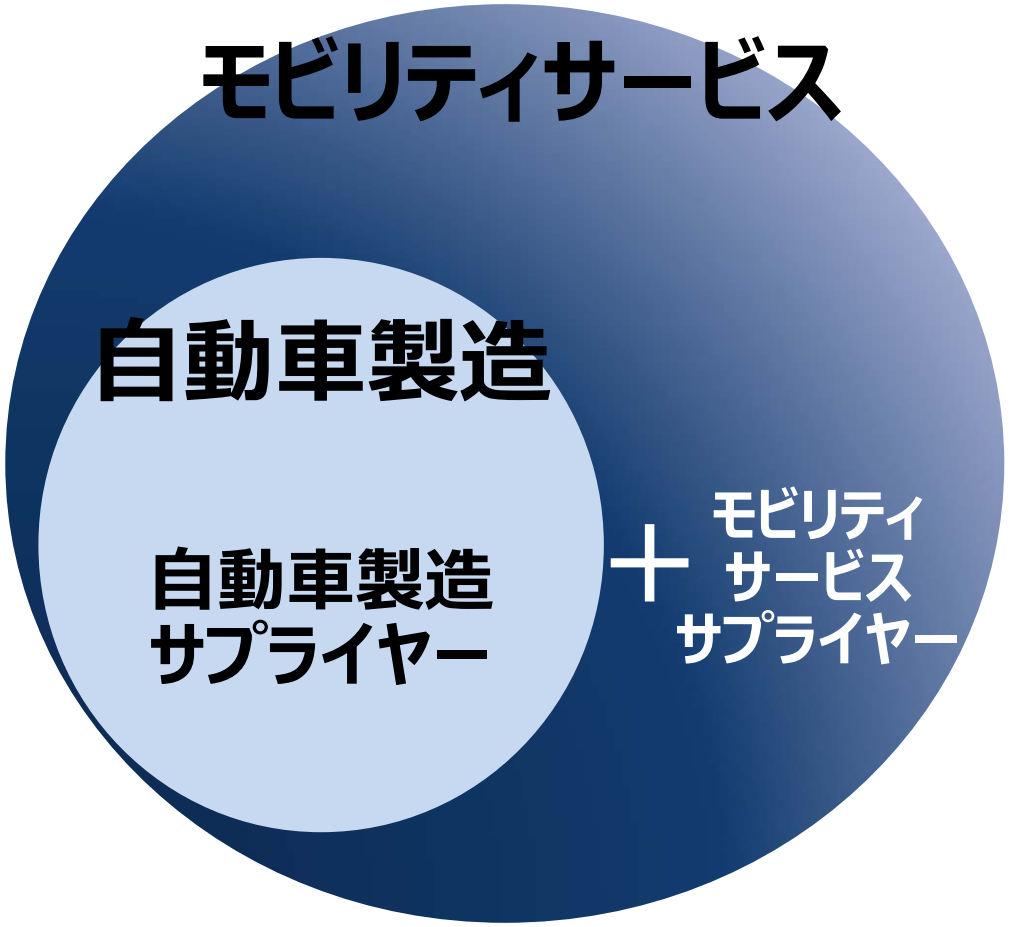
電動化によりH/W*1の重要性が低下、
自動運転/ｺﾈｸﾃｨｯﾄﾞ/ｼｪｱﾘﾝｸﾞ等
S/W*2を主戦場とするﾌﾟﾚｰﾔｰが競合に

*1 :ハードウェア　*2 :ソフトウェア

1-2. 自動車業界の特徴

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

・次世代のモビリティビジネスへの構造変化に伴い、**サプライヤーも拡大**（モビリティサービスサプライヤー）
・取り扱う情報も**機密情報**が多く、**データ量も増加傾向**



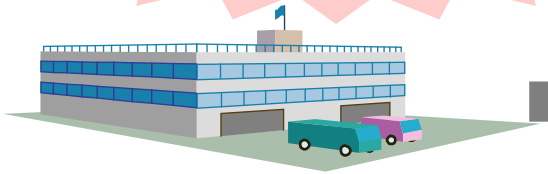
保有情報	詳細
車両情報	・位置情報 ・速度情報 ・エンジン情報 ・制御系情報　など
技術情報	・図面 ・ＣＡＤデータ ・Ｒ＆Ｄ情報 ・デザイン　など
顧客情報	・個人情報 ・家族情報 ・金融情報 ・所有車情報　など

1-3. 自動車業界のサプライチェーンセキュリティリスク

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

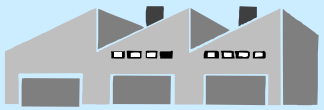
・大企業は**自社だけを守っているのでは不十分**
・業務で**関連する会社のリスク管理**が必要

・**部品調達**できない
・**物流停止**



部品メーカー

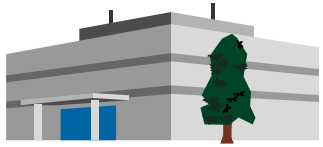
自社



工場

オフィス

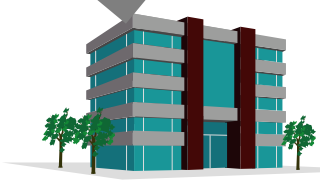
内部不正による
情報漏洩



委託先

・製品への**マルウェア・バックドア**埋め込み
・ **製品に脆弱性**

ソフトウェアベンダー



サービス事業者

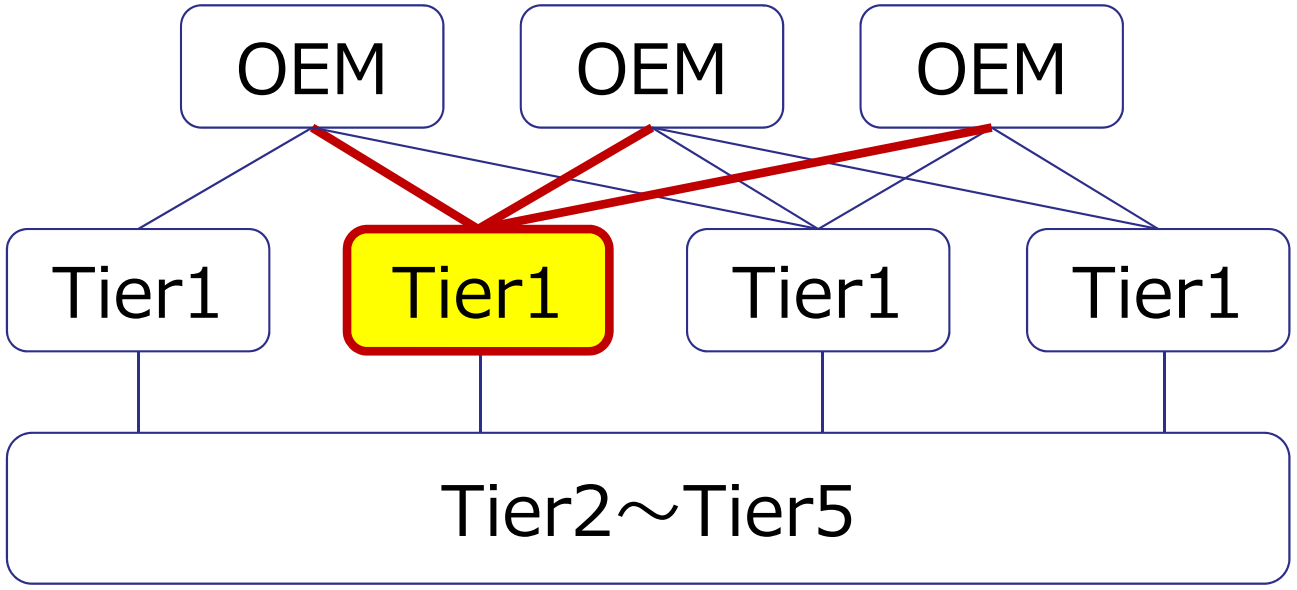
関係先から
踏み台攻撃

1-4. 大規模サプライチェーン リスク事例

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

・サプライヤーの業務が停止した場合に、自動車業界への影響は大
・サイバー攻撃によるサプライヤーの生産停止も同様の影響が発生

＜自然災害の事例＞
新潟県中越沖地震 リケン
⇒1社の停止が、複数の自動車メーカー製造停止へ



2007/07/19 09:29

ニュース

【新潟県中越沖地震】トヨタ、日産など自動車大手がライン停止、部品メーカーの工場被災で

市嶋　洋平＝日経コンピュータ　　日経コンピュータ

トヨタ自動車、日産自動車など大手各社は、中越沖地震の影響で完成車の製造を7月19日以降に一時停止する。自動車部品メーカー、リケンの柏崎工場が被災し部品の納入が止まるためだ。

不足する主な部品は、エンジンを構成する「ピストンリング」と変速機を構成する「シール材」である。トヨタは両部品、日産はシール材、本田技研工業はピストンリングが足りていないという。大手自動車会社に変速機を納入している大手部品メーカー、ジヤトコやアイシン・エィ・ダブリュ（アイシンAW）の生産状況も影響している。両社ともリケンの部品をほぼ100%使っているからだ。ジヤトコは18日夜の段階で生産量を6割減としており、アイシンAWは全国の工場からシール材を集めてなんとか生産を続行している。

トヨタは、19日の夕方から20日中まで全国の工場を停止、日産は20日以降に一部ラインを非稼働としたり主要工場での休日出勤を取りやめるといった、それぞれの措置をとる。本田は19日午後までに対応を決定する。このほか、三菱自動車や富士重工業が生産の一時中止を決めている。

本来であれば事業継続性計画（BCP）の実行を確保するため、自動車や大手部品メーカーはリケン以外で同等部品の調達先を確保しておくべきだが、「高精度な部品であり、リケン以外からは調達していないのが実情」（大手部品メーカー）という。サプライチェーンの情報システム整備やバックアップ構築と同時に、調達先の冗長性確保も大きな課題となっていることが浮き彫りとなった。

https://googleads.g.doubleclick.net/pcs/click?xai=AKAOjsuQlvhrhLYrbrhX1JRuZI81gOpm_XHauWHvkOAOUDPvygrQanKBCrchRVc-INvqOt64c

1. 自動車業界のセキュリティリスク

2. セキュリティ事故事例

3. セキュリティガイドライン検討の活動説明

4. 今後の予定

5. 最後に

2-1. 最近のセキュリティ脅威の傾向

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

・サイバー攻撃の目的は、愉快犯・自己顕示から**金銭目的・国家関与の攻撃に変化**
・ターゲット企業に対し、**高度な攻撃手法を用いて戦略的に攻撃を実施**

	過去	現在・今後
目的	**愉快犯、自己顕示**	・**金銭目的**の情報窃取、妨害、テロ行為 ・**国家関与**の情報窃取
対象	不特定多数（マス）	特定の企業・組織
侵入・攻撃	単一攻撃、偶発的	複合型攻撃、戦略的 (標的型攻撃)
考慮すべきポイント	**個社毎に対応** 	**サプライチェーン全体で対応必要** 

2-2. 自動車メーカーのセキュリティ事故事例

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

・自動車メーカー各社にて、標的型のサイバー攻撃により被害が発生
・協調分野の取り組みとして、セキュリティ対策の推進が必要

会社	TOYOTA	HONDA The Power of Dreams	NISSAN
発生日	19年3月	17年6月	16年1月
概要	東京販売店へのサイバー攻撃	国内外工場へのサイバー攻撃	日産自動車及びグループ会社のＨＰへのDDoS攻撃
影響	最大310万件の個人情報漏洩の可能性	狭山工場の操業停止（約1千台に影響）	公式Webサイト、グローバルサイトの停止

2-3. サプライヤーのセキュリティ事故事例

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

・サプライヤーにおいても、標的型のサイバー攻撃により被害が発生
・自動車メーカーへの波及は少ないが、今後更に拡大していく可能性あり

会社	大手 部品会社	大手 海運会社	中小 部品会社
発生日	19年12月	17年6月	16年6月
概要	サイバー攻撃のため、 コーポ系ネットワーク上の 大半のPCがウィルス感染	サイバー攻撃のため、 複数の拠点でITシステムがダウン	サイバー攻撃のため、 生産系サーバがランサムウェアに感染
影響	メールシステムが 約1週間使用不能 ⇒顧客・関係各社との 各種連絡が停滞	10日間に渡る 物流システムの停止 ⇒自動車完成車の 配送遅れ	手動による生産管理を 余儀なくされた ⇒一部の納入に遅延が 発生

2-4. (参考)IPA「情報セキュリティ10大脅威 2020」

JAMA 一般社団法人 日本自動車工業会 JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

“サプライチェーンの弱点を悪用した攻撃”は、引き続き上位（4位）

2020年1月29日 IPA： https://www.ipa.go.jp/about/press/20200129.html

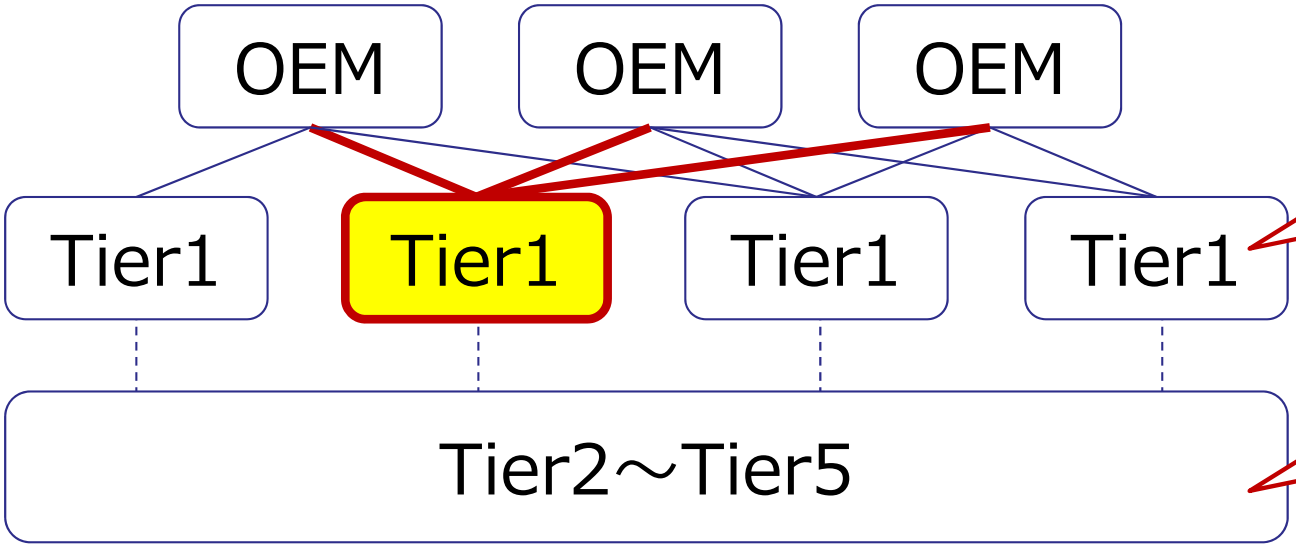
昨年順位	順位	組織への攻撃
1位 →	**1位**	標的型攻撃による機密情報の窃取
5位 ↗	**2位**	内部不正による情報漏えい
2位 ↘	**3位**	ビジネスメール詐欺による金銭被害
4位 →	**4位**	**サプライチェーンの弱点を悪用した攻撃**
3位 ↘	**5位**	ランサムウェアによる被害
16位 ↗	**6位**	予期せぬIT基盤の障害に伴う業務停止
10位 ↗	**7位**	不注意による情報漏えい（規則は遵守）
7位 ↘	**8位**	インターネット上のサービスからの個人情報の窃取
8位 ↘	**9位**	IoT機器の不正利用
6位 ↘	**10位**	サービス妨害攻撃によるサービスの停止

2-5. セキュリティ脅威を踏まえた対策の必要性

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

自動車業界の構造におけるセキュリティ対策課題に対応するため、
セキュリティガイドライン(対策項目、基準)の策定・展開が急務

自動車業界の構造(イメージ)



セキュリティ対策課題

各OEMから個別に対策基準が展開されるが、**バラバラで対応に負荷がかかる**

対策基準がなく何をどこまで対策すればよいかわからない

1. 自動車業界のセキュリティリスク

2. セキュリティ事故事例

3. セキュリティガイドライン検討の活動説明

4. 今後の予定

5. 最後に

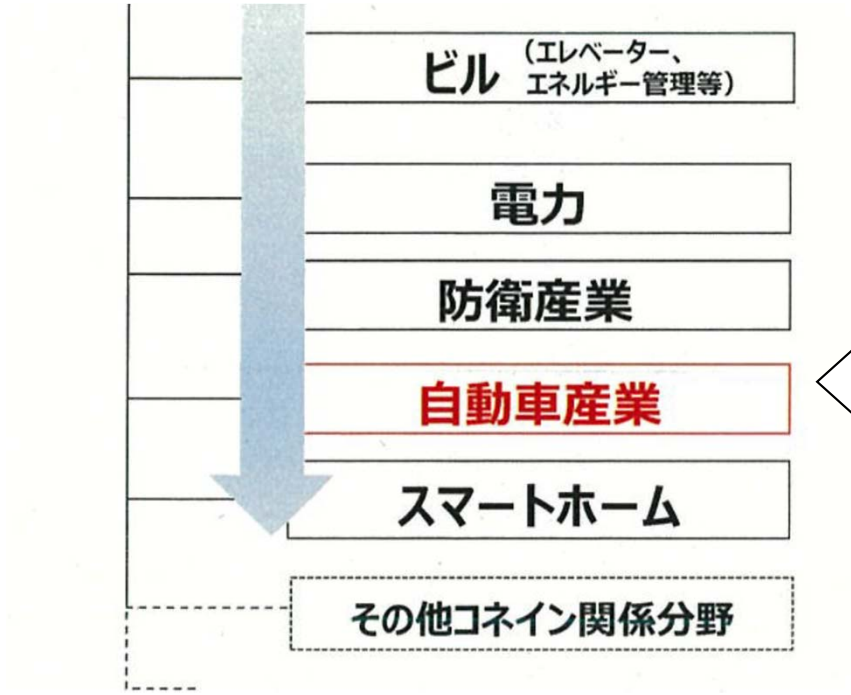
3-1. 背景

業界全体のセキュリティ対策レベル底上げの課題認識に伴い、経産省からもアドバイスを頂き、業界標準のガイドライン策定を目指し検討開始

＜標準モデル＞

経済産業省: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*1)

Industry by Industryで検討



出典：経産省「産業分野におけるサイバーセキュリティ政策」資料

19年度は、仕入先を中心としたサプライチェーン対応のガイドラインを策定

*1)CPSF：Cyber Physical Security Framework

3-2. 検討組織、体制(1/2)

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

自工会＆部工会の合同検討体制を整備

■自工会

※19年5月立上げ

- サイバーセキュリティ部会
  - サイバーセキュリティ統括分科会
    - WP29対応検討タスク
    - **サイバーセキュリティガイドライン検討タスク** **8社**

［リーダー］　トヨタ
［副リーダー］日産、ホンダ

■部工会

※19年9月立上げ

サイバーセキュリティ部会 **17社**

［リーダー］　デンソー
［副リーダー］日立オートモーティブ、マレリ

3-2. 検討組織、体制(2/2)

自工会、部工会の混合グループを3つ作り、**合計25社（8+17）**の知見を活かして、標準のサイバーセキュリティガイドラインを共同検討中

(社名50音順)

	Aグループ	Bグループ	Cグループ
自工会 8社	ダイハツ工業 トヨタ自動車	スズキ 日産自動車 三菱自動車工業	SUBARU 本田技研工業 マツダ
部工会 17社	愛三工業 ショーワ スタンレー電気 豊田合成 日本特殊陶業 日立オートモーティブ システムズ	アイシン精機 NOK KYB 小糸製作所 デンソー	東海理化 トヨタ紡織 日本発条 ミツバ マレリ 矢崎総業

3-3. 検討活動の取組み（19年度）

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

4つのStepに分け、各社と議論を通じて、標準のサイバーセキュリティガイドラインを策定

Step1	Step2	Step3	Step4
現状把握	目的、形式検討	19年度目標を検討	現在対応中 セキュリティガイドライン作成
日米欧の標準とOEM各社のガイドラインを調査、ベンチマーク	ガイドラインの使い方(目的、形式)を決定	取組み範囲・優先順位を決定	チェックシートと“使い方”を作成

Step1	Step2	Step3	Step4
現状把握	目的、形式検討	19年度目標を検討	現在対応中 セキュリティガイドライン作成
日米欧の標準とOEM各社のガイドラインを調査、ベンチマーク	ガイドラインの使い方(目的、形式)を決定	取組み範囲・優先順位を決定	チェックシートと“使い方”を作成

3-4. Step1：現状把握（調査対象）

日米欧の標準とOEM各社の**セキュリティフレームワーク、ガイドラインを比較**（調査・ベンチマーク）

発行	比較対象（フレームワーク/ガイドライン）
NIST アメリカ国立標準技術研究所	Cyber Security Framework v1.1 SP800-171 SP800-53
ISO	27002
AIAG （米）	Cyber Security 3rd Party Information Security 1st Edition
経産省	サイバー・フィジカル・セキュリティ対策ガイドライン (CPSF : Cyber Physical Security Framework)
OEM各社	各社セキュリティガイドライン

3-4. Step1：現状把握（位置付け）

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

日米欧の標準のセキュリティフレームワーク、ガイドラインの位置付けを調査

分類	NIST			ISO	経産省		AIAG
	CyberSecurityFramework v1.1	SP800-171	SP800-53	27002	CPSF		Cyber Security 3rd Party
①目的	重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1版	連邦政府外のシステムと組織における管理された非格付け情報の保護	国家のセキュリティを守る為（連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策を規定）	ISMSの確立、実施、維持、継続的な改善のための要求事項を提供	産業界が自らのセキュリティ対策に活用するため	「Society5.0」における産業社会ではサイバー攻撃の起点が拡大するとともにサイバー攻撃による被害がフィジカル空間に及ぼす影響も増大するため、新たなリスクに対応していくための指針を示すことを目的と	3rd PartyにOEMの最低限の要求事項を理解してもらうため
②誰が誰へ(対象者)	米国国立標準技術研究所（NIST）	米国国立標準技術研究所（NIST）	米国国立標準技術研究所（NIST）⇒情報システム・情報セキュリティ関係の専門的なユーザーにとって役に立つことを目指す			者として想定 ライチェーンマネ に関わる担当者 ュークリエイショ スに関わるセキュ 当者 テム担当者	＜業種＞ OEMから、OEMの情報を扱ったり、OEMに代わって業務を行う全ての3rd Partyへ（部品メーカーだけではなく給与支払い請負業者等の業務請負も含む） ＜深さ＞ OEMから直接業務を依頼する全ての3rd
③範囲(対象業務)	規程無し（重要インフラのCS改善を目的）	サプライチェーン全て 特定情報（CUI）を扱うシステム、コンポーネントに適用を限定してもよい	政府関係の情報システムを利用する業務全般（但し、一般に活用できる情報セキュリティカタログ的要素が強い）			ームワークにおける の洗い出しやセ ィ対策の適用範囲 社会におけるバ リエイションプロ 。	全て（ただし、製品に含まれる、または、バックエンドシステムと通信するSW、HWに関する項目は除く）

【位置付け検討項目】
①目的
②誰が誰へ（対象者）
③範囲（対象業務）
④規定内容
⑤使い方、評価方法
⑥共有、レベルアップ
⑦強制/任意

3-4. Step1：現状把握（項目、内容）

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

分類毎に、**項目・内容の網羅性を横並び調査**
⇒網羅性が高い **経産省 サイバーフィジカルセキュリティ対策フレームワークをベースに検討**

	NIST									ISO			経産省									AIAG		
	CybersecurityFramework v1.1			SP800-171			SP800-53			27002			CPSF（第1層）			CPSF（第2層）			CPSF（第3層）			Cyber Security 3rd Party Information Security 1st Edition		
分類	有無	項目数	カテゴリ	有無	項目数	カテゴリ	有無	項目数	カテゴリ	有無	項目数	カテゴリ	有無	項目数	カテゴリ	有無	項目数	カテゴリ	有無	項目数	カテゴリ	有無	項目数	カテゴリ
識別	○	6	ID.AM							○	8	A6,A8,A11,A12,A13	○	19	CPS.AM	無	0	CPS.AM	○	7	CPS.AM			
	○	5	ID.BE							○	13	4,A11,A12,A15,A17	○	7	CPS.BE	有	1	CPS.BE	○	3	CPS.BE			
	○	4	ID.GV				○	6	PL（計画作成）	○	11	6,A5,A6,A7,A15,A18	○	14	CPS.GV	無	0	CPS.GV	○	4	CPS.GV			
	○	6	ID.RA	○	3	3.11 リス	○	5	RA（リスク評価）	○	6	6,A6,A12,A16,A18	○	18	CPS.RA	有	3	CPS.RA	○	6	CPS.RA			
	○																							
	○																							
防御	○																							
	○																							
	○																							
	○																							
	○																							
	○																							
検知	○																							
	○																							
	○																							
対応復旧	○																							
	○																							
	○																							
	○																							
	○																							

	経産省		NIST										ISO			AIAG		
	CPSF		CybersecurityFramework v1.1				SP800-171			SP800-53			27002			Cyber Security 3rd Party Information Security 1st		
機能	カテゴリ	サブカテゴリー	機能	有無	カテゴリー	サブカテゴリー	有無	カテゴリ	サブカテゴリー	有無	カテゴリ	サブカテゴリー	有無	カテゴリ	サブカテゴリー	有無	カテゴリ	サブカテゴリー
ガバナンス	CPS.GV-1	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	識別（ID）	○	**ガバナンス（ID.GV）：**自組織に対する規制、法律、リスク、環境、運用上の要求事項を、管理し、モニタリングするためのポリシー、手順、プロセスが理解されており、経営層にサイバーセキュリティリスクについて伝えている。	**ID.GV-1:** 組織のサイバーセキュリティポリシーが、定められ、周知されている。				○	**PL 計画作成**	PL-1 セキュリティ計画のポリシーと手順 管理策：組織は、 a. 以下を策定、文書化し、[指定：組織が定めた職員	○	A.5.1: 情報セキュリティのた	A.5.1.1: 情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知しなければならない。	○	Information Security Program	1.2 a. Third Party must implement or provide evidence of an Information Security Program which includes: a. Approved and
				○	**ID.GV-2:** サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。					△類似のものはある	**SA システムおよびサービスの調達**	SA-9 管理策：組織は、 a. 外部情報システムサービスのプロバイダに対して、該当する連邦法・大統領命令・指	○	A.6.1: 内部組織	A.6.1.1: 全ての情報セキュリティの責任を定め，割り当てなければならない。		—	—
													○	A.7.2: 雇用期間中	A.7.2.1: 経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求しなければならない。			

Step1	**Step2**	Step3	Step4
現状把握	目的、 形式検討	19年度 目標を 検討	現在対応中 セキュリティ ガイドライン 作成
日米欧の標準と OEM各社の ガイドラインを調査、 ベンチマーク	ガイドラインの 使い方(目的、 形式)を決定	取組み範囲・ 優先順位を決定	チェックシートと “使い方”を作成

3-4. Step2：目的･形式(案)を共通認識化

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

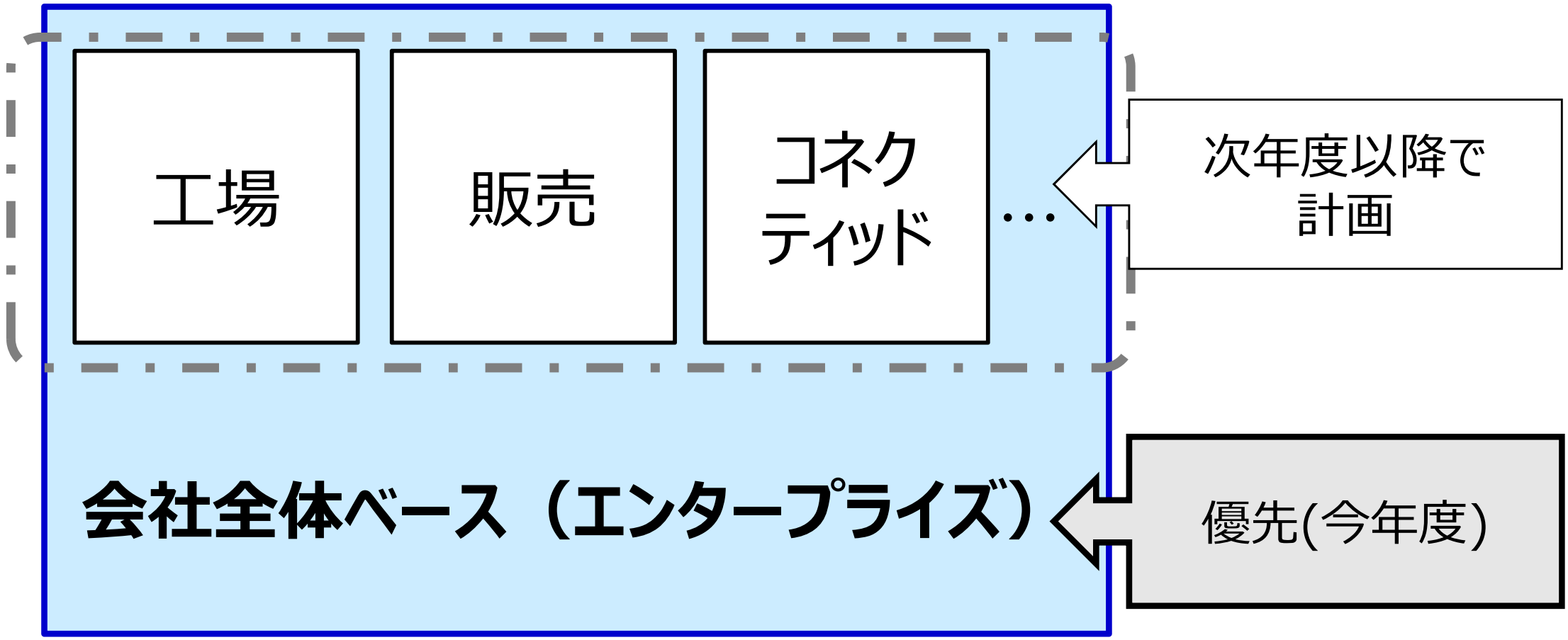
分類	自工会 ＋	部工会 ＝	検討結果
①目的	･**業界のセキュリティレベルアップ** ･評価（見える化）と改善推進 ･**業界全体の負担軽減**	左記に加えて ･**責任を果たせたと言えるレベル（相場）形成**	･**業界のセキュリティのレベルアップ** ･**業界全体の負担軽減** ･**責任を果たせたと言えるレベル(相場)形成**
②誰が誰へ（対象者）	･**OEMからTier1、Tier1からTier2へ** ･まずは部品サプライヤを対象	左記に加えて ･**対象は業界全体**を想定して作成、実際の**展開＆活用は商流**に沿って実施。	･**対象：業界全体を想定** ･**展開＆活用：商流に沿って実施**
③範囲（対象業務）	･**まずはエンタープライズ（ｺｰﾎﾟﾚｰﾄ、OA）** ･工場、コネクテッドは除く	･まずはエンタープライズが現実的だが、**後に工場、コネクティッドも入れる**方向で再議論	･**エンタープライズ(ｺｰﾎﾟﾚｰﾄ、OA)** ･**今後、工場、コネクティッドも追加**
④規定内容	･**使い方 ＋ チェックリスト** ･できればレベル(Must,Want)を記載	同左 ･会社の規模＆業務を考慮することも必要	･**ガイドライン（使い方＋チェックリスト）**
⑤使い方、評価方法	･**セルフチェックのみ** ･認証、自/部工会認定【少数意見】	同左	･**セルフチェックのみ**
⑥共有、レベルアップ	･**評価結果を業界で共有** ･ベストプラクティスを共有	･**広く一般に公開することは避けた方が良い。**(弱点の開示により、攻撃対象となるため)	･**評価結果を業界内のみで共有**
⑦強制、任意	･罰則規定は無し ･**結果を業界で共有するのみで十分**	同左	･**強制しない（罰則規定は無し）**

Step1	Step2	Step3	Step4
現状把握	目的、 形式検討	19年度 目標を 検討	現在対応中 セキュリティ ガイドライン 作成
日米欧の標準と OEM各社の ガイドラインを調査、 ベンチマーク	ガイドラインの 使い方(目的、 形式)を決定	取組み範囲・ 優先順位を決定	チェックシートと “使い方”を作成

3-4. Step3：対象、範囲、優先順位を検討

①定義する業務対象：

業界全体の底上げのため、19年度は分野に因らない会社全体のベースとなる範囲
「エンタープライズ」を対象とし、次年度以降、工場・コネクティッド等へ拡大

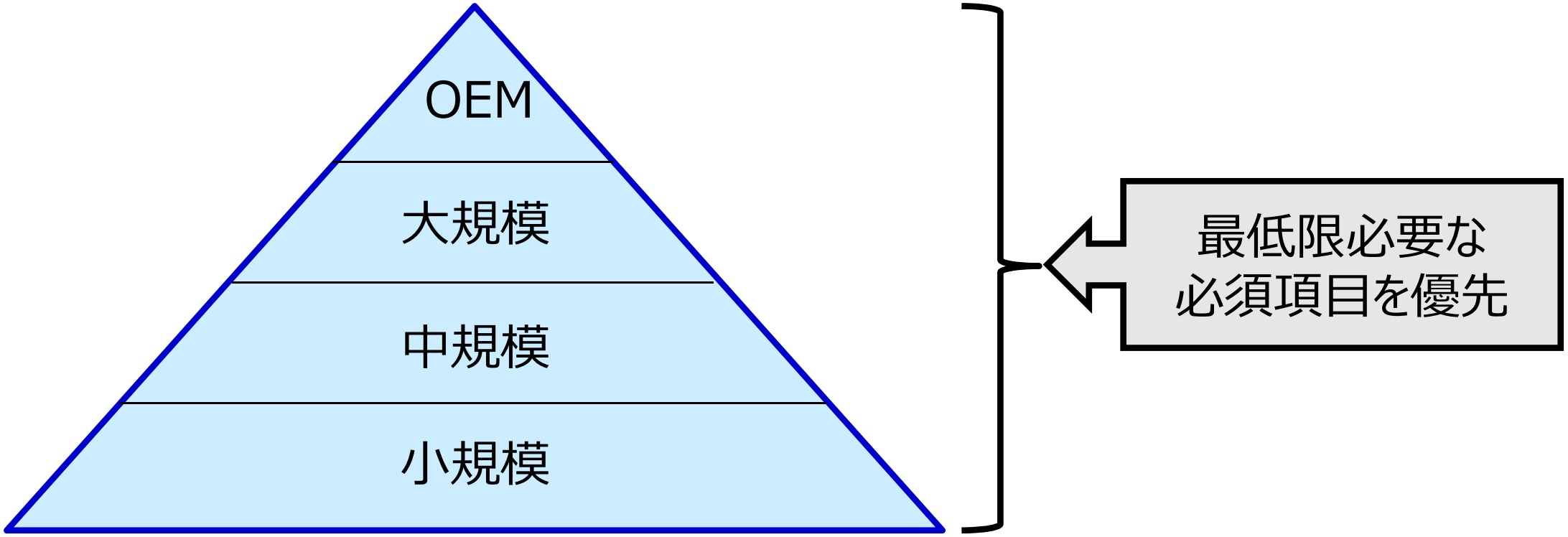


3-4. Step3：対象、範囲、優先順位を検討

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

②対象・目的の優先順位：

自動車業界の全てで利用できるガイドラインを目指す。
まずは、 多くの会社のレベルアップを優先するため、**OEM～小規模会社で最低限必要な必須項目の策定を進める。**



3-4. Step3：対象、範囲、優先順位を検討

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

③正しく活用いただけるように、チェックシートだけの策定ではなく、
目的・利用方法を記載した“使い方”も準備中

【ガイドライン】

＜使い方＞

・ガイドライン策定の背景と目的
・対象範囲
・ガイドラインの構成
・利用方法

＋

＜チェックシート＞

次年度以降、更に拡充予定
(セキュリティ点検の実施事項、脆弱性検知時の対処など)

Step1	Step2	Step3	Step4
現状把握	目的、 形式検討	19年度 目標を 検討	現在対応中 セキュリティ ガイドライン 作成
日米欧の標準と OEM各社の ガイドラインを調査、 ベンチマーク	ガイドラインの 使い方(目的、 形式)を決定	取組み範囲・ 優先順位を決定	チェックシートと “使い方”を作成

3-4. Step4：セキュリティガイドライン作成

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

CPSFベースで、中小企業も対象にした **IPA「5分でできる！情報セキュリティ自社診断」**も参考にしながら、**自動車業界としての必須項目を選定**
CPSF:対策要件 約130項目 ⇒ 約60項目に絞り込み

機能	経産省 CPSF 対策要件(カテゴリ)	IPA	A社	B社	C社	D社	E社	F社	G社	H社	検討案
資産管理	CPS.AM-1	○	必須項目	必須項目	必須項目	必須項目	必須項目	必須項目	必須項目	必須項目	○
	CPS.AM-4		必須項目	必須項目				必須項目	必須項目		
	CPS.AM-5	○	必須項目	必須項目		必須項目	必須項目	必須項目	必須項目		○
	CPS.AM-6	○	必須項目	必須項目	必須項目					必須項目	○
	CPS.AM-7	○	必須項目	必須項目	必須項目	必須項目	必須項目			必須項目	○
	CPS.AM-2										
	CPS.AM-3										
ビジネス環境	CPS.BE-1	○	必須項目		必須項目	必須項目		必須項目	必須項目		○
	CPS.BE-2	○	必須項目				必須項目		必須項目	必須項目	○
	CPS.BE-3	○	必須項目						必須項目	必須項目	○
意識向上及びトレーニング	CPS.AT-1	○				必須項目	必須項目			必須項目	○

約130項目　　約60項目

3-4. (参考) IPA:5分でできる！情報セキュリティ自社診断

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

診断編

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
		退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をして				

https://www.ipa.go.jp/files/000055848.pdf

3-4. Step4：セキュリティガイドライン作成

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

・自工会・部工会 合同検討体制（25社(31人)）にて、**CPSF 対策要件が求める セキュリティ要件の解読～中小企業も活用できるような書き方、実施事項レベル**を検討
※**延べ対応時間：約1,200h**
・**外部有識者のアドバイス**をいただきながら、検討推進中

リスク源（脆弱性）	対策要件	対策要件ID	①求めるセキュリティ要件を解読	②文言検討(初回)	③小規模会社でも適切なレベルか？	④ガイドライン要求事項(案)
[組織] セキュリティ事象を的確に検知するための**体制**が**構築**されていない	セキュリティ管理**責任者**を任命し、セキュリティ対策組織(**SOC/CSIRT**)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える	CPS. AE-2	・セキュリティ対策の責任者任命とセキュリティ対応体制の構築（SOCシステムの導入も含めることを要求するのか？） ・セキュリティ対策＝セキュリティ事象を検知・分析・対応と定義	【言葉を定義】 ・SOC（インシデントを検知するシステム） ・CSIRT（対応体制） ・責任者（対応体制の責任者） 【文言検討】 **「インシデントを検知する仕組みを導入し、セキュリティ対応体制とその責任者を明確にすること」**	【要求内容を精査】 ・SOC導入は敷居が高くないか？ ・一方でセキュリティ対応体制は必須（1人CSIRTでも良い） ⇒SOCとセキュリティ対応体制は、設問を分離すべきでは？	**「セキュリティ対策に対する対応体制とその責任者を明確にすること」** **<達成条件>** -体制図の有無と社内での承認（組織の連携、責任者が明記） **<他社事例>** ・小規模な組織であれば１～２名の体制でも問題ありません

配慮したポイント
・項目数
・用語
・達成条件のレベル感

達成条件は、下記の基準で評価できる基準を設定
○：実施している
△：一部実施している
×：分からない / 実施していない

3-4. Step4：自工会･部工会 合同検討会の様子

1. 自動車業界のセキュリティリスク

2. セキュリティ事故事例

3. セキュリティガイドライン検討の活動説明

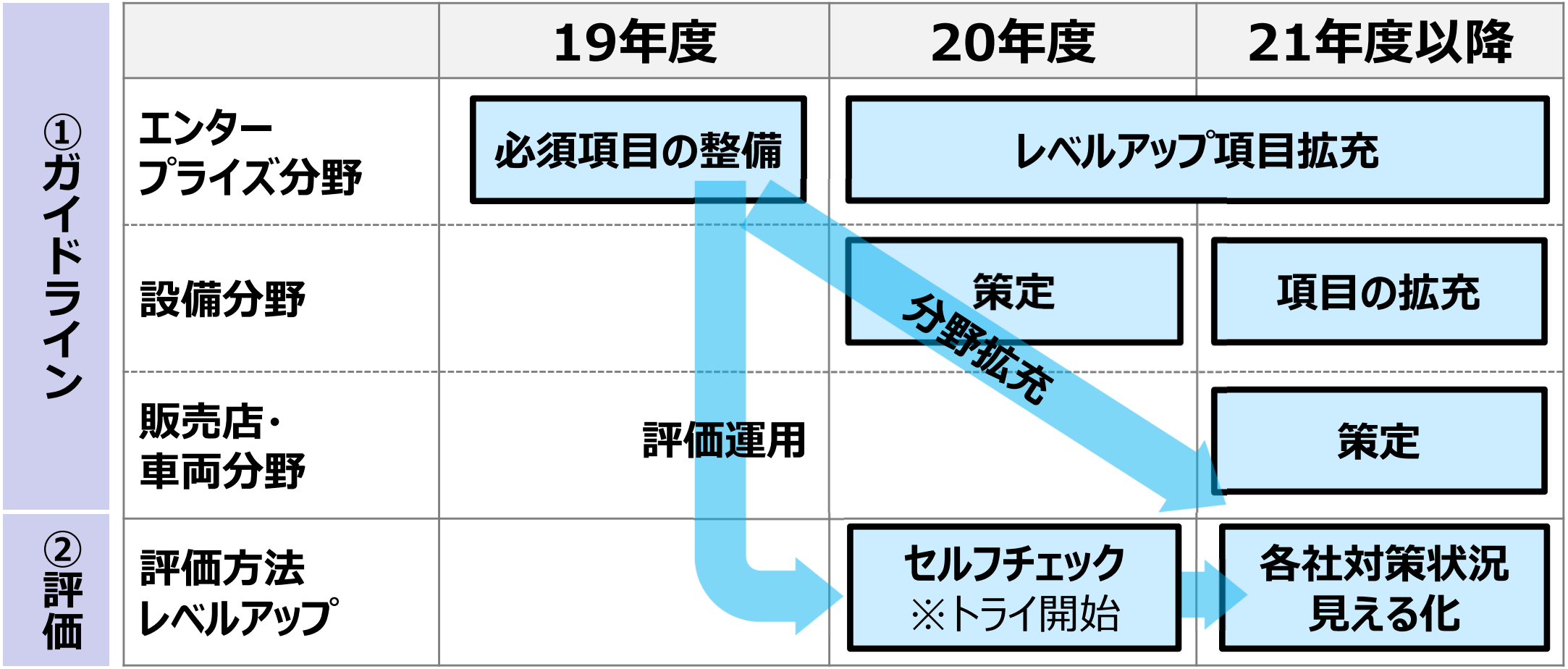
4. 今後の予定

5. 最後に

4. 今後の活動方針（案）

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

①ガイドライン：項目の拡充と他分野(設備・販売店・車両)向けの項目整備
②評価方法：セルフチェックのトライ後、各社対策状況の見える化検討予定



※今後、第三者審査・国際相互認証も検討予定。

1. 自動車業界のセキュリティリスク

2. セキュリティ事故事例

3. セキュリティガイドライン検討の活動説明

4. 今後の予定

5. 最後に

5. 最後に

- ✓ サイバーセキュリティガイドラインは策定して終わりではない。
- ✓ 新しいサイバー攻撃への対応検討や自動車業界としてのレベルアップの進め方も引き続き検討を進めることで、IoT・モビリティに広がり高度化するサイバー攻撃に対して、安全・安心かつ信頼できるサイバー空間づくりを推進していきたい。
- ✓ 自動車業界一丸となって、取り組みます。応援してください！

JAMA 一般社団法人 日本自動車工業会
JAPAN AUTOMOBILE MANUFACTURERS ASSOCIATION, INC.

JAPIA
Japan Auto Parts Industries Association

ご清聴ありがとうございました。

引き続きJAMA活動へのご理解とご協力を
宜しくお願い致します。