SIP-adus2019
Cybersecurity Plenary Session

Nov.13.2019

Mazda Motor Corporation
Masashi Yamasaki (Global Security Officer)

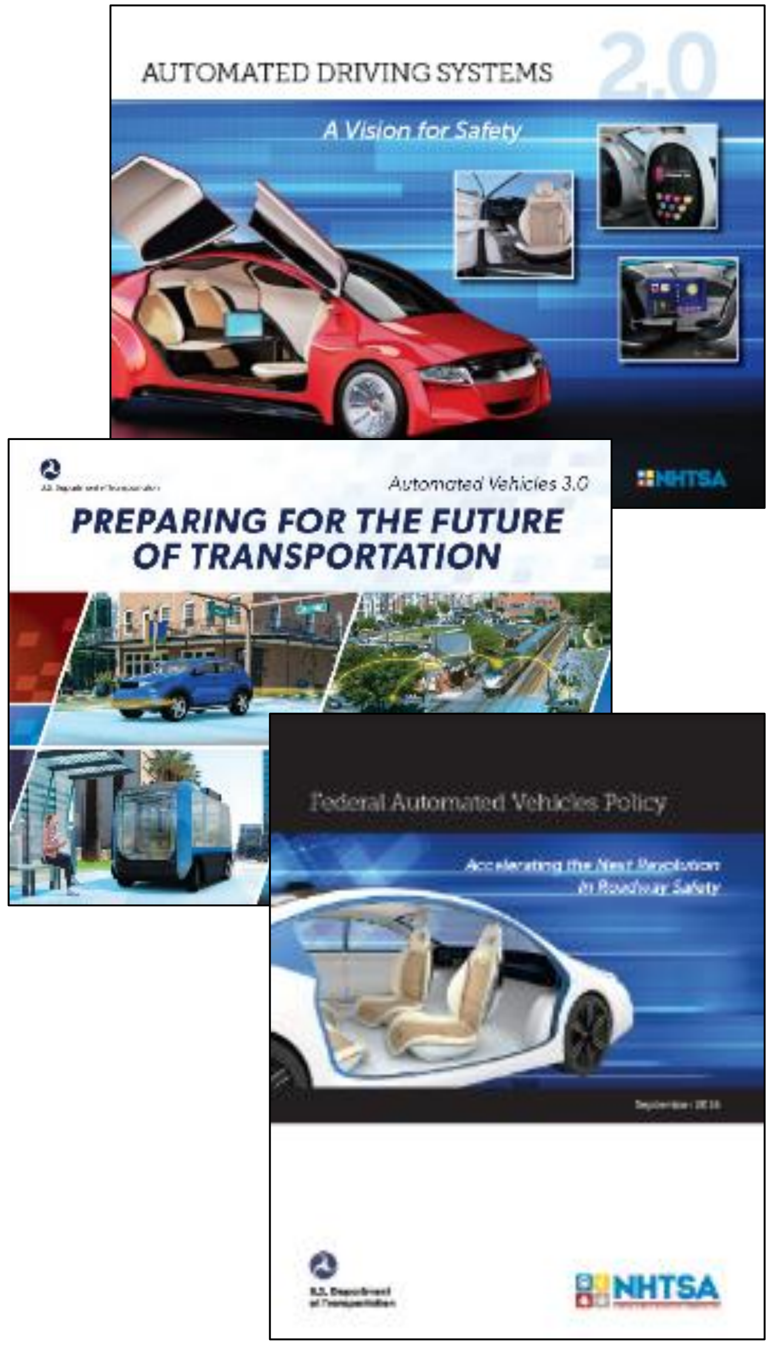
AGENDA

1. Global Trends（Automotive Guidelines/standards/others）
2. Japan Trends（Automotive regulations /Guidelines）
3. Regulations and standardization schedule (forecast)

1. Global Trends（Automotive Guidelines/standards/others)

In recent years, documents related to automotive security have been released.

Category	Authorities	Title
Guidelines	WP29	・Guideline on Cybersecurity and data protection (2017)
		・Cybersecurity and OTA TF (In progress)
Standards	ISO/SAE JWG	・ISO/SAE 21434: Road Vehicles - Cybersecurity Engineering
	SAE	・J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
Others	NHTSA	・Federal Automated Vehicles Policy (2016)
		・Cybersecurity Best Practices for Modern Vehicles (2016)
		・AUTOMATED DRIVING SYSTEMS 2.0 (2017)
		・PREPARING FOR THE FUTURE OF TRANSPORTATION: Automated Vehicles 3.0 (2018)
	Auto-ISAC	・Automotive Cybersecurity Best practices (2017)


AUTOMATED DRIVING SYSTEMS 2.0
A Vision for Safety
NHTSA
Automated Vehicles 3.0
PREPARING FOR THE FUTURE OF TRANSPORTATION
Federal Automated Vehicles Policy
Accelerating the Next Revolution in Roadway Safety
NHTSA

WP29：World Forum for Harmonization of Vehicle Regulations

1. Global Trends：Others

Status of Cyber Security Regulations in Other Countries

- **EU** : General Safety Regulation(GSR), which is in line with WP29, will go into effect.

- **USA** : Self-driving car regulation bill, which includes a provision on cyber security, was reviewed by both legislative houses; but was not approved by the Senate.

  ＜Outline of Draft Cyber Security Clause＞

  Each OEM shall plan and implement cyber security countermeasures to mitigate potential risks

- **China** : GB, GB/T pertaining to security are expected to be established.

  GB: Mandatory standards. Non-compliant products may not be manufactured, sold or exported

  GB/T: Voluntary standards, which may be cited in GB in some cases.

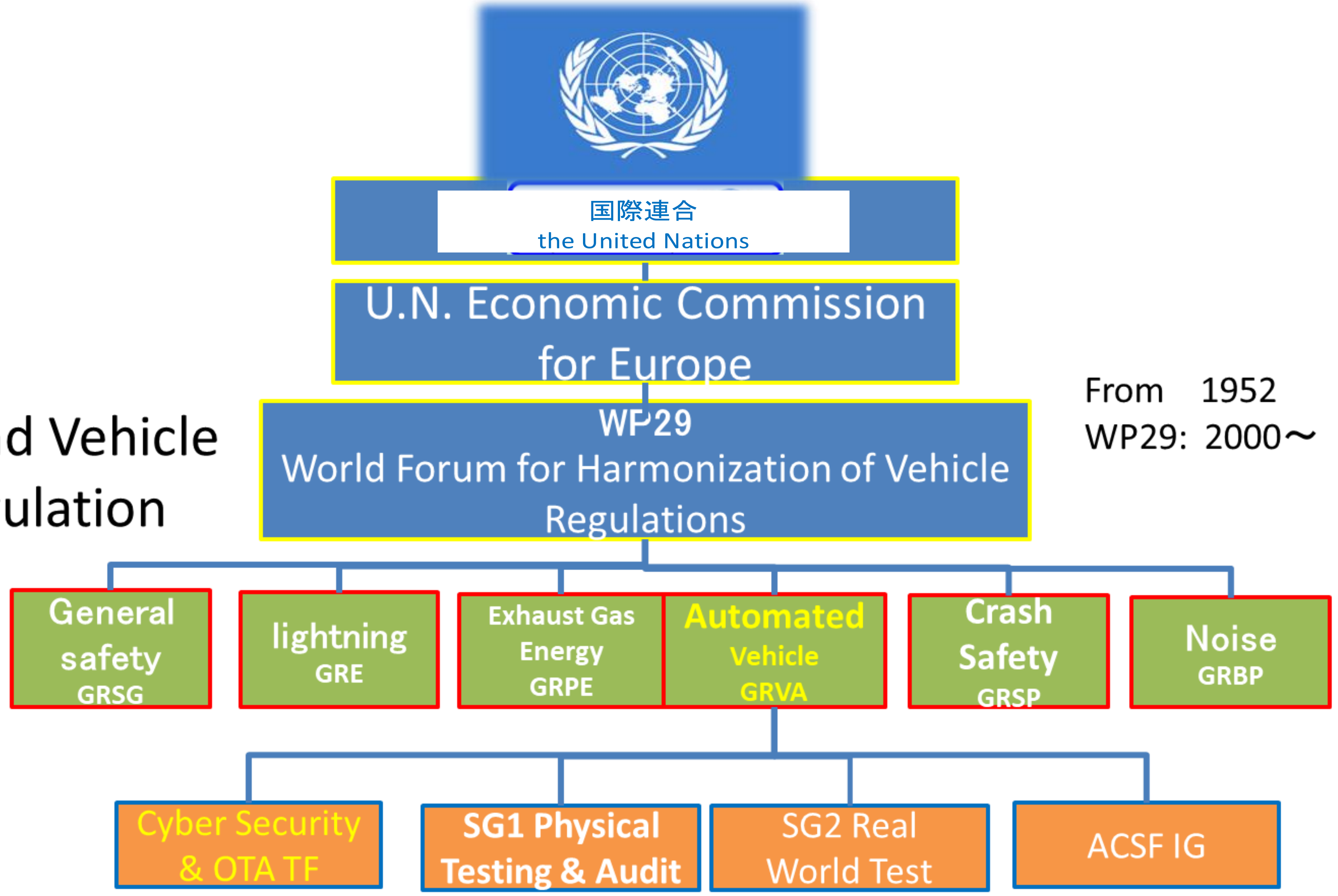
1. Global Trends：UN/WP29（Working Party 29）

World Forum for Harmonization of Vehicle Regulations

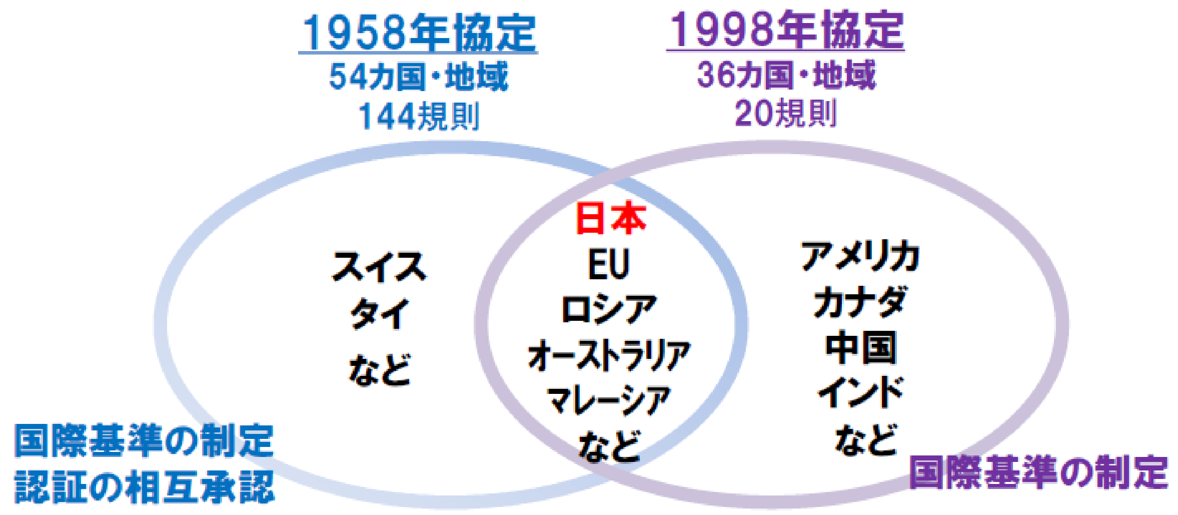
- Promoting global harmonization of regulations of vehicle safety and environment as well as vehicle certifications across countries

※ This is the only international forum

Road Vehicle Regulation



From　1952
WP29: 2000～



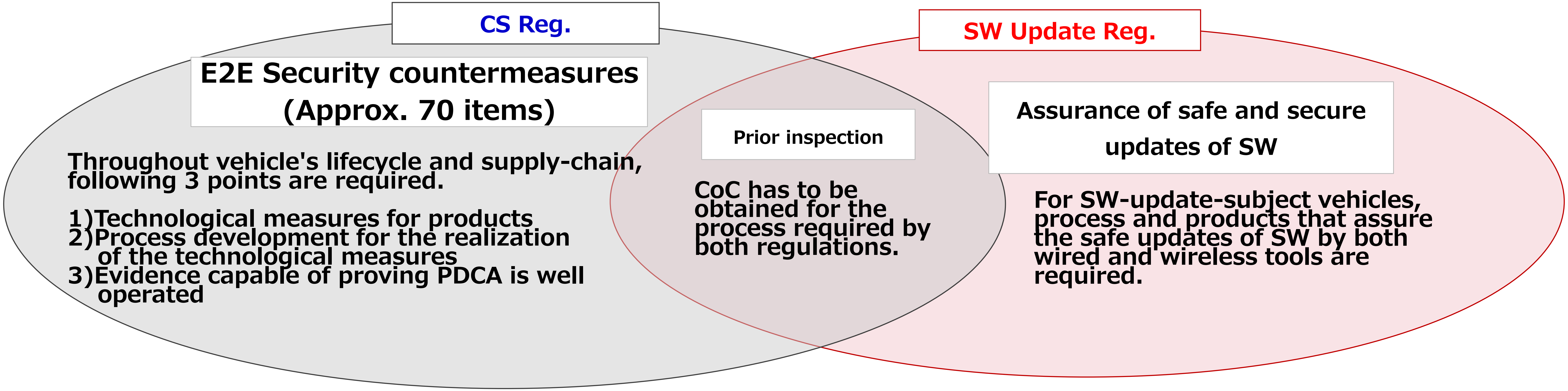
自動運転技術に係る主な会議体	日本の役職
自動運転（GRVA）専門分科会	副議長
自動操舵専門家会議	議長(独と共同)
自動ブレーキ専門家会議	議長(ECと共同)
サイバーセキュリティ専門家会議	議長(英と共同)
自動運転認証専門家会議（物理的試験等）	議長
自動運転認証専門家会議　（実走行試験）	ー（議長：蘭）

1. Global Trends：Cyber Security/Software Update Reg.

UNR is scheduled to take effect in 2020/Japan will start certification from 2020

For both the regulations,

- It is necessary to define Technological and Process measures and to prove that "PDCA" is well operated with evidences.
- Regarding the Process measure, the application of Type Approval requires the acquisition of Certificate of Compliance (CoC) which needs a prior inspection.



CS Reg.

E2E Security countermeasures (Approx. 70 items)

Throughout vehicle's lifecycle and supply-chain, following 3 points are required.

1)Technological measures for products
2)Process development for the realization of the technological measures
3)Evidence capable of proving PDCA is well operated

Prior inspection

CoC has to be obtained for the process required by both regulations.

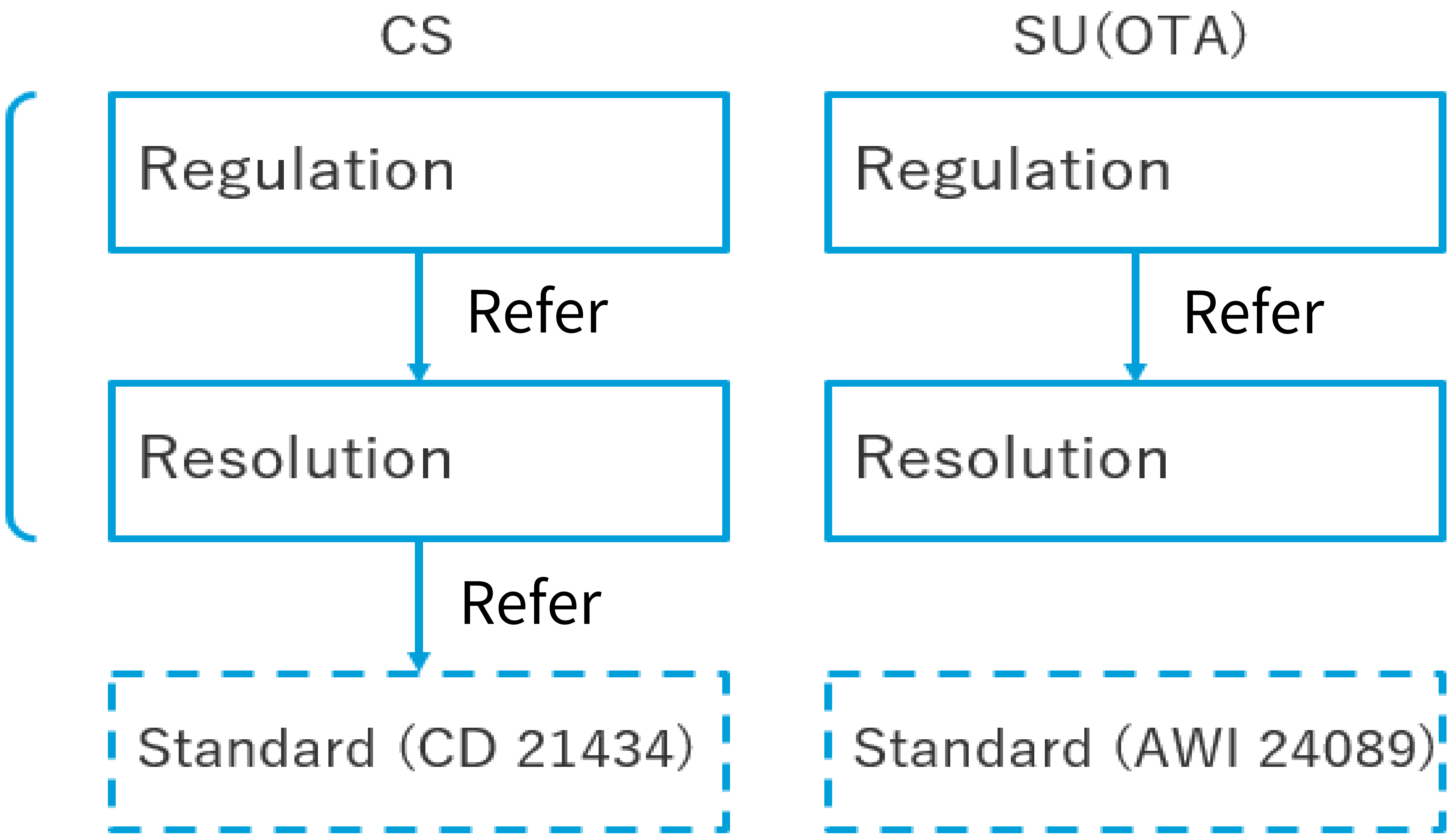
SW Update Reg.

Assurance of safe and secure updates of SW

For SW-update-subject vehicles, process and products that assure the safe updates of SW by both wired and wireless tools are required.

1. Global Trends

Relationship between WP29-CS & SU(UNR) and ISO / SAE standard



CS

Regulation

Refer

Resolution

Refer

Standard（CD 21434）

SU(OTA)

Regulation

Refer

Resolution

Standard（AWI 24089）

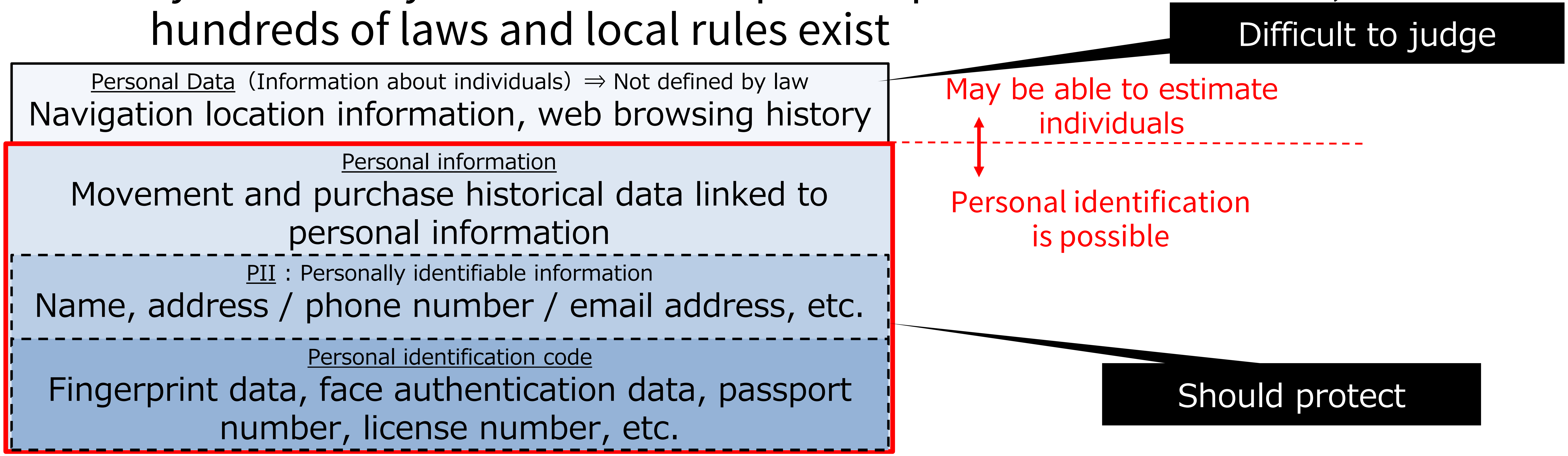
1. Global Trends：Other

Different laws & definitions for individual information and personal data

- ➢ There are various regulations other than the General Data Protection Regulation (GDPR)

Example)

US　: regulated by federal-level sectoral and state laws
China: Cyber security law enforced to protect personal information,
hundreds of laws and local rules exist



Difficult to judge

Personal Data（Information about individuals）⇒ Not defined by law
Navigation location information, web browsing history

May be able to estimate individuals

Personal identification is possible

Personal information
Movement and purchase historical data linked to personal information

PII：Personally identifiable information
Name, address / phone number / email address, etc.

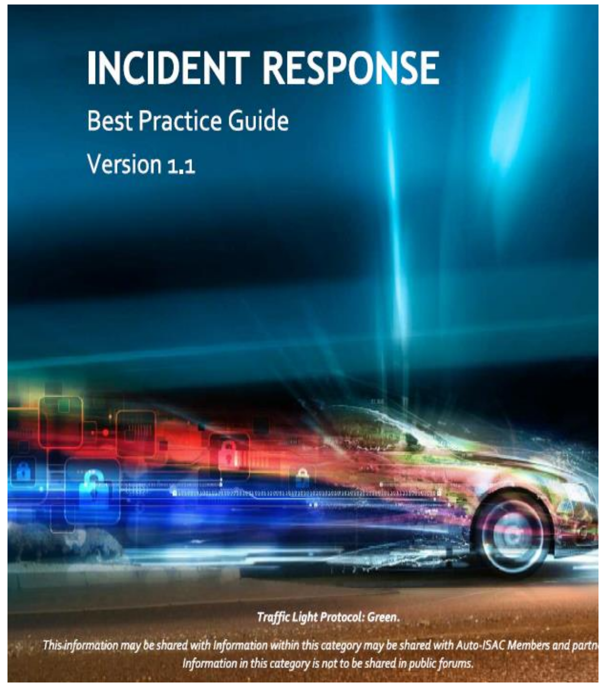
Personal identification code
Fingerprint data, face authentication data, passport number, license number, etc.

Should protect

1. Global Trends：Auto-ISAC（Best Practices Guide)

Automotive Information Sharing and Analysis Center

- ➢Information sharing and analysis of automotive cybersecurity risks
- ➢BEST PRACTICES EXECUTIVE SUMMARY Released sequentially from July 2016



INCIDENT RESPONSE

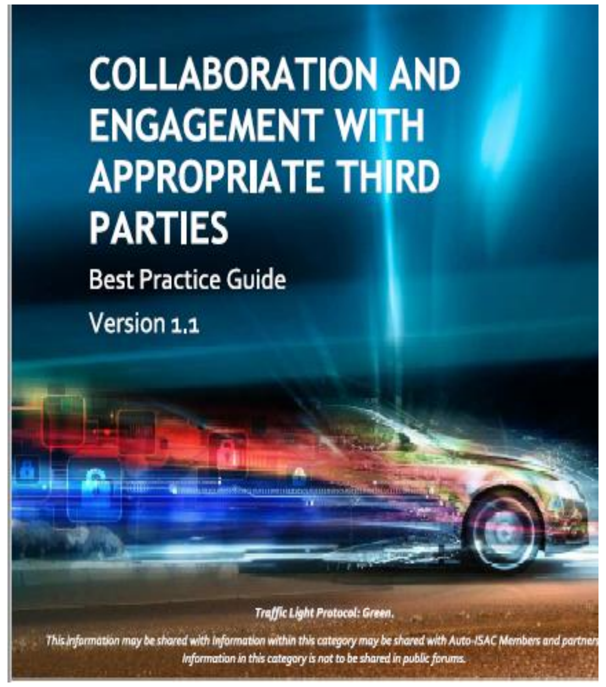
Best Practice Guide

Version 1.1

Traffic Light Protocol: Green.

This information may be shared with Information within this category may be shared with Auto-ISAC Members and partn

Information in this category is not to be shared in public forums.



COLLABORATION AND ENGAGEMENT WITH APPROPRIATE THIRD PARTIES

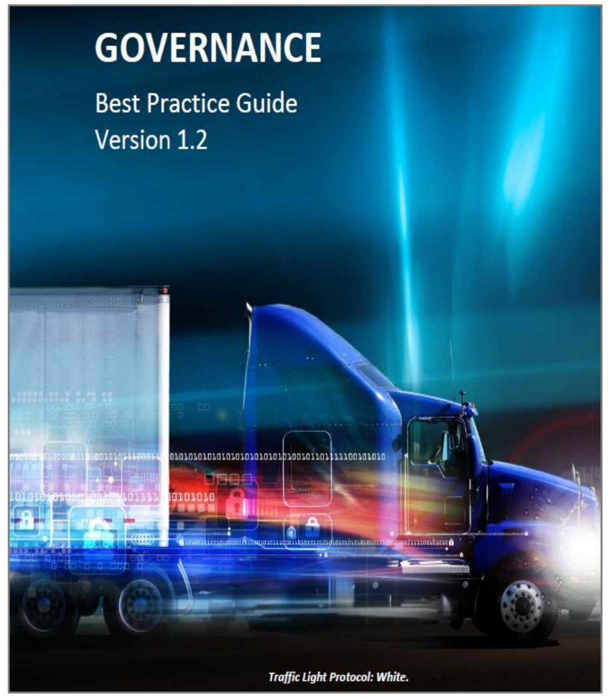
Best Practice Guide

Version 1.1

Traffic Light Protocol: Green.

This information may be shared with Information within this category may be shared with Auto-ISAC Members and partner

Information in this category is not to be shared in public forums.



GOVERNANCE

Best Practice Guide

Version 1.2

Traffic Light Protocol: White.

Released

- ✓ Incident Response
- ✓ Third Party Collaboration and Engagement
- ✓ Governance
- ✓ Risk Management
- ✓ Awareness and Training
- ✓ Threat Detection, Monitoring, and Analysis

To be

- • Security by Design

引用：https://www.automotiveisac.com/

2. Japan Trends

(Cyber Security Management Guidelines Ver2.0 ‘17 / 11/16)

経済産業省
Ministry of Economy, Trade and Industry

I. Cybersecurity is a management issue

Security measures are not “cost” but an essential “investment” ensuring business continuity and future growth

Security investment is one of the duties of the management

II. 3 Principles which the management need to recognize

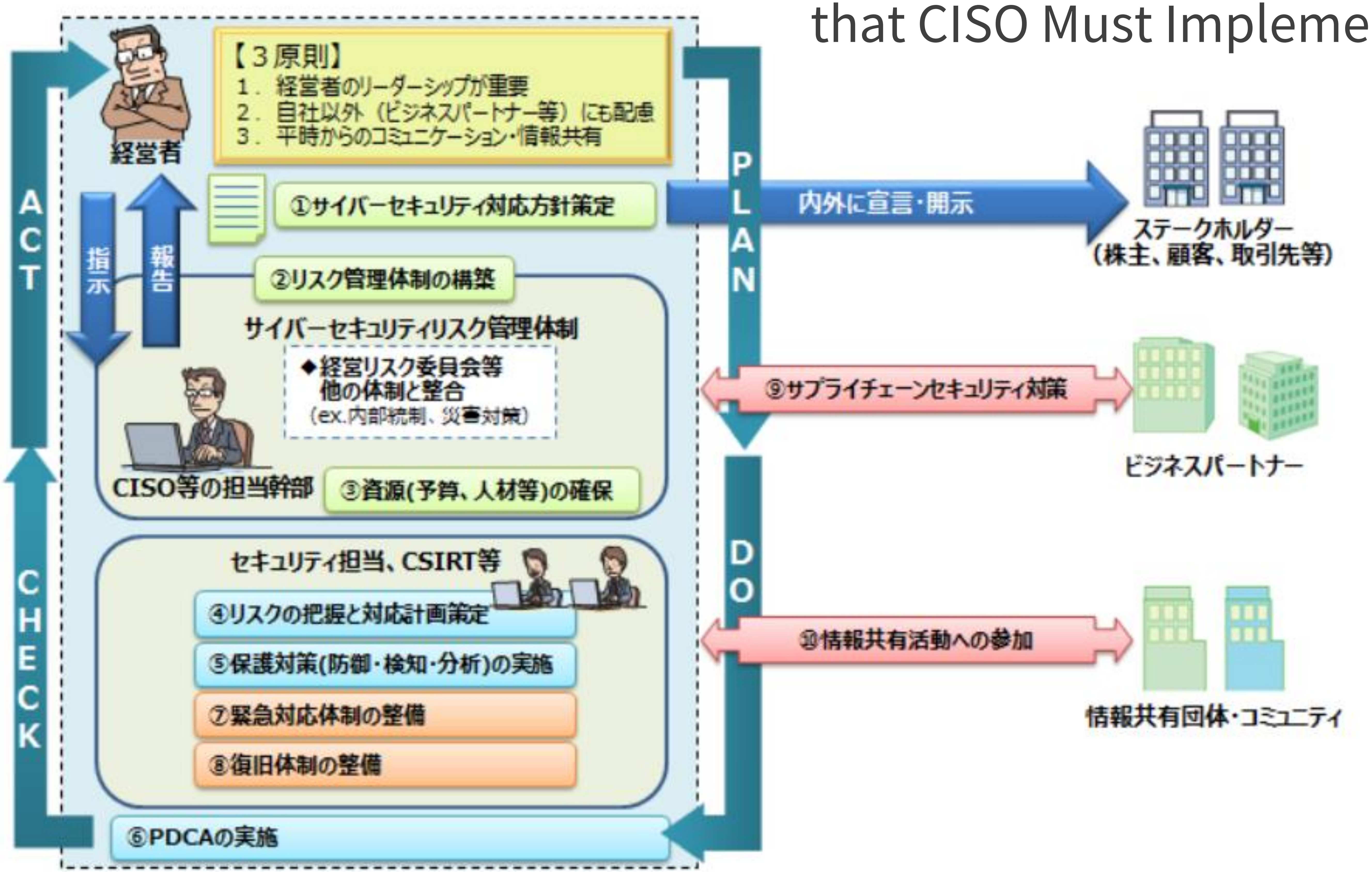
(1)	Recognize cybersecurity risks and take the leadership in promoting measures
(2)	Implement comprehensive security measures covering the company itself, its group companies, and business partners of its supply chain
(3)	Communicate appropriately with relevant parties by, for example, disclosing information on security measures at any times.

III. 10 Important items which the management should direct their CISO to observe

Building Cyber Security Risk Management System	
Direction 1	Raise awareness of cybersecurity risks and announce a security policy
Direction 2	Build an cybersecurity management structure
Direction 3	Secure resources (e.g. budget, people) for cybersecurity measures
Identify Cyber Security Risks and Establish Countermeasures	
Direction 4	Understand cyber security risks and develop risk management plans
Direction 5	Establish systems to address cyber security risks
Direction 6	Implement PDCA of cyber security measures
Prepare Actions to be Taken in Case of an Incident（Cyber Attacks)	
Direction 7	Establish an emergency response unit in case of an incident
Direction 8	Establish a unit that promotes recovery efforts in the event of an incident
Promote Measures to Enhance Cyber Security in Supply Chain	
Direction 9	Grasp and promote measures among business partners and contractors
Promote Communication with Related Parties	
Direction 10	Gather, share and effectively use cyber attack/incident information

2. Japan Trends

(Three Principles for Management and Top 10 Security Principles that CISO Must Implement (Overview))



【３原則】
１．経営者のリーダーシップが重要
２．自社以外（ビジネスパートナー等）にも配慮
３．平時からのコミュニケーション・情報共有

経営者

指示

報告

①サイバーセキュリティ対応方針策定

内外に宣言・開示

ステークホルダー
（株主、顧客、取引先等）

②リスク管理体制の構築

サイバーセキュリティリスク管理体制

◆経営リスク委員会等
他の体制と整合
（ex.内部統制、災害対策）

CISO等の担当幹部

③資源(予算、人材等)の確保

⑨サプライチェーンセキュリティ対策

ビジネスパートナー

セキュリティ担当、CSIRT等

④リスクの把握と対応計画策定

⑤保護対策(防御・検知・分析)の実施

⑦緊急対応体制の整備

⑧復旧体制の整備

⑩情報共有活動への参加

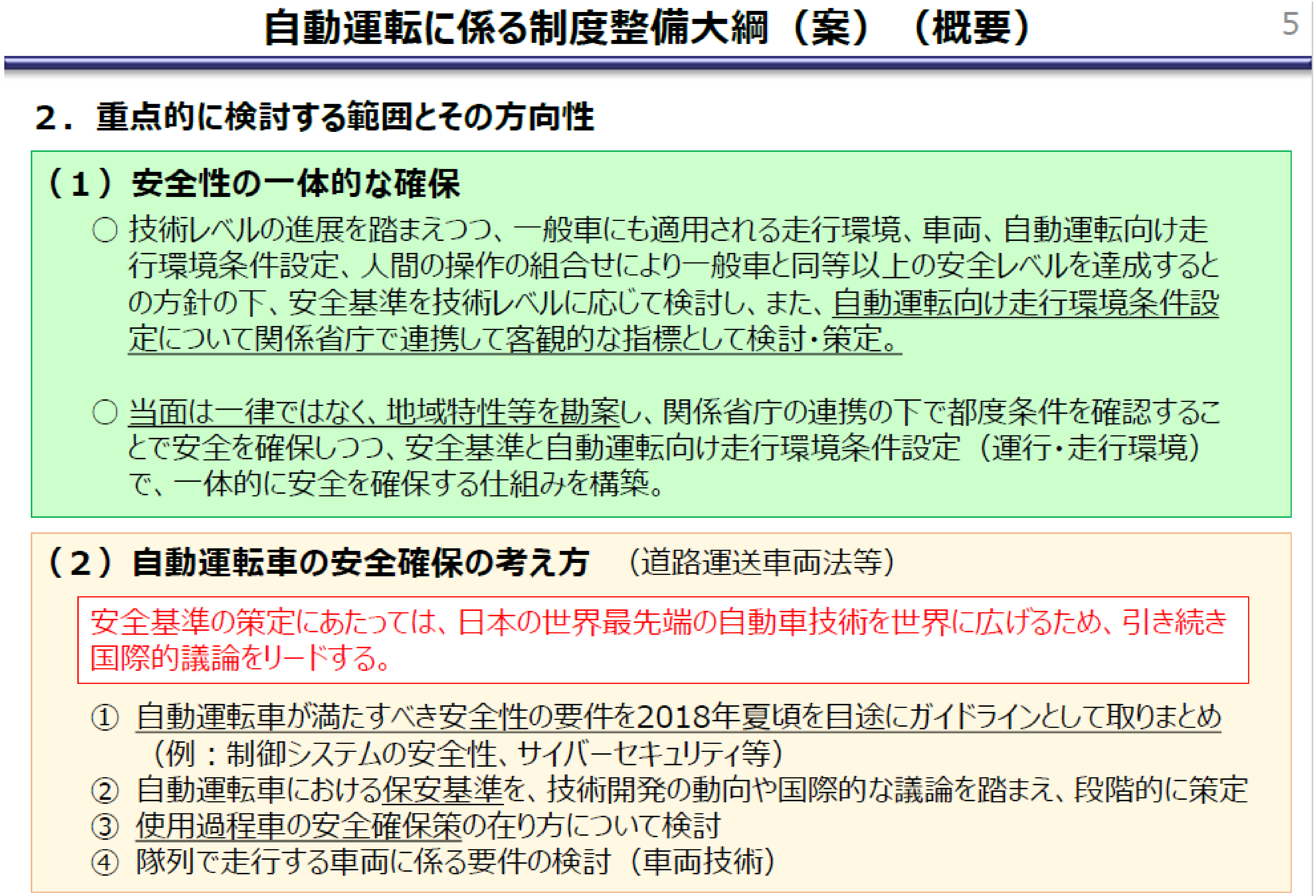
情報共有団体・コミュニティ

⑥PDCAの実施

From METI website https://www.meti.go.jp/policy/netsecurity/mng_guide.html

2. Japan Trends

Government policies on preparation of regulations for autonomous vehicles



自動運転に係る制度整備大綱（案）（概要）

5

2．重点的に検討する範囲とその方向性

（１）安全性の一体的な確保

○ 技術レベルの進展を踏まえつつ、一般車にも適用される走行環境、車両、自動運転向け走行環境条件設定、人間の操作の組合せにより一般車と同等以上の安全レベルを達成するとの方針の下、安全基準を技術レベルに応じて検討し、また、自動運転向け走行環境条件設定について関係省庁で連携して客観的な指標として検討・策定。

○ 当面は一律ではなく、地域特性等を勘案し、関係省庁の連携の下で都度条件を確認することで安全を確保しつつ、安全基準と自動運転向け走行環境条件設定（運行・走行環境）で、一体的に安全を確保する仕組みを構築。

（２）自動運転車の安全確保の考え方　（道路運送車両法等）

安全基準の策定にあたっては、日本の世界最先端の自動車技術を世界に広げるため、引き続き国際的議論をリードする。

① 自動運転車が満たすべき安全性の要件を2018年夏頃を目途にガイドラインとして取りまとめ
（例：制御システムの安全性、サイバーセキュリティ等）
② 自動運転車における保安基準を、技術開発の動向や国際的な議論を踏まえ、段階的に策定
③ 使用過程車の安全確保策の在り方について検討
④ 隊列で走行する車両に係る要件の検討（車両技術）

国土交通省

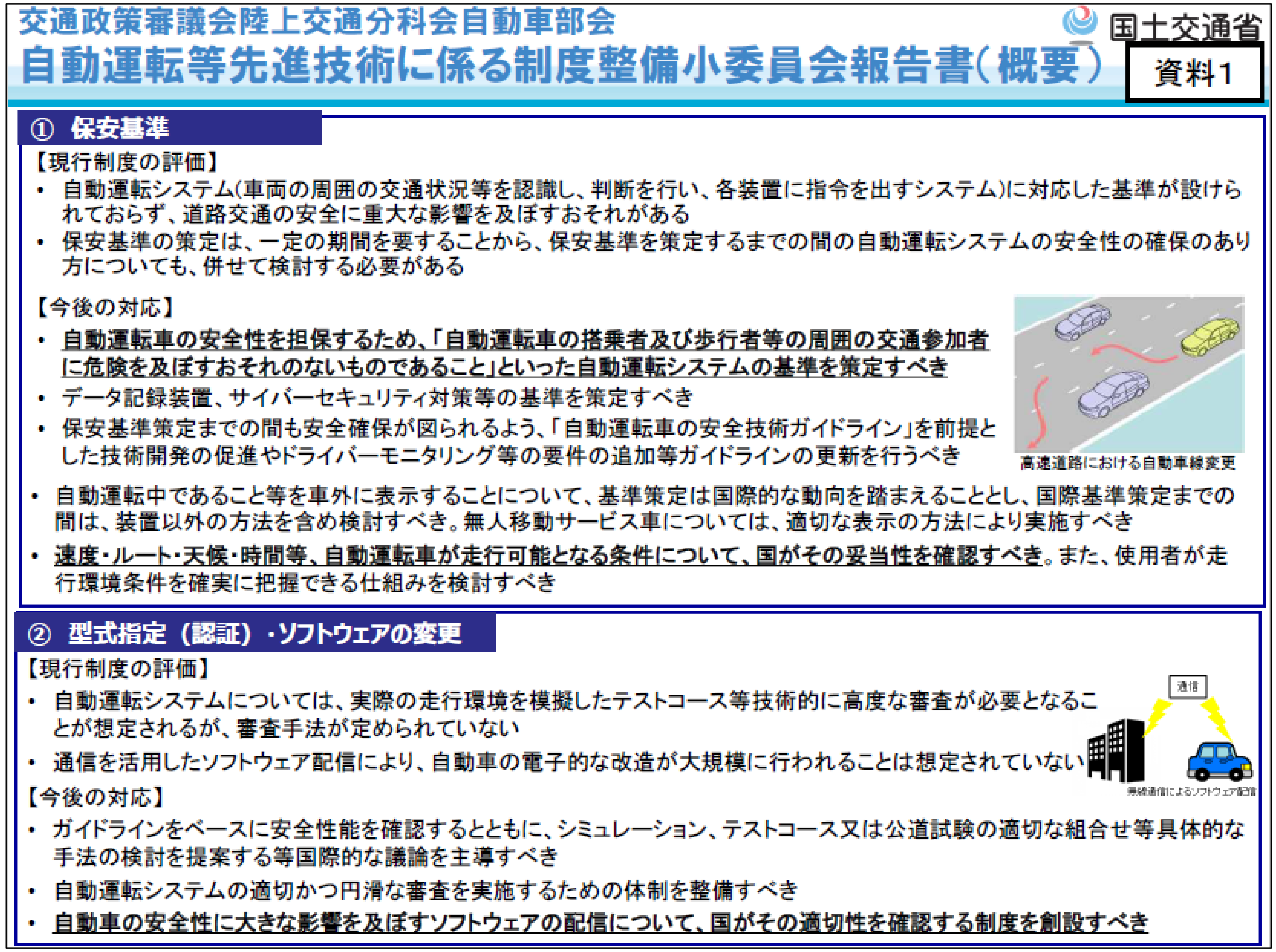
Outline of Preparation of System Concerning Autonomous vehicles (Apr.2018)

Source:　Government policies on preparation of laws and regulations for autonomous vehicles (Draft)
https://www.kantei.go.jp/jp/singi/it2/dai73/siryou1_1_1.pdf

2. Japan Trends：

Regulations for Autonomous and Other Advanced Technologies

Road vehicle regulations have been revised in consideration of cyber security and approved by the Cabinet (March 2019)



交通政策審議会陸上交通分科会自動車部会

国土交通省

自動運転等先進技術に係る制度整備小委員会報告書（概要）

資料1

① 保安基準

【現行制度の評価】

- 自動運転システム(車両の周囲の交通状況等を認識し、判断を行い、各装置に指令を出すシステム)に対応した基準が設けられておらず、道路交通の安全に重大な影響を及ぼすおそれがある
- 保安基準の策定は、一定の期間を要することから、保安基準を策定するまでの間の自動運転システムの安全性の確保のあり方についても、併せて検討する必要がある

【今後の対応】

- 自動運転車の安全性を担保するため、「自動運転車の搭乗者及び歩行者等の周囲の交通参加者に危険を及ぼすおそれのないものであること」といった自動運転システムの基準を策定すべき
- データ記録装置、サイバーセキュリティ対策等の基準を策定すべき
- 保安基準策定までの間も安全確保が図られるよう、「自動運転車の安全技術ガイドライン」を前提とした技術開発の促進やドライバーモニタリング等の要件の追加等ガイドラインの更新を行うべき

高速道路における自動車線変更

- 自動運転中であること等を車外に表示することについて、基準策定は国際的な動向を踏まえることとし、国際基準策定までの間は、装置以外の方法を含め検討すべき。無人移動サービス車については、適切な表示の方法により実施すべき
- 速度・ルート・天候・時間等、自動運転車が走行可能となる条件について、国がその妥当性を確認すべき。また、使用者が走行環境条件を確実に把握できる仕組みを検討すべき

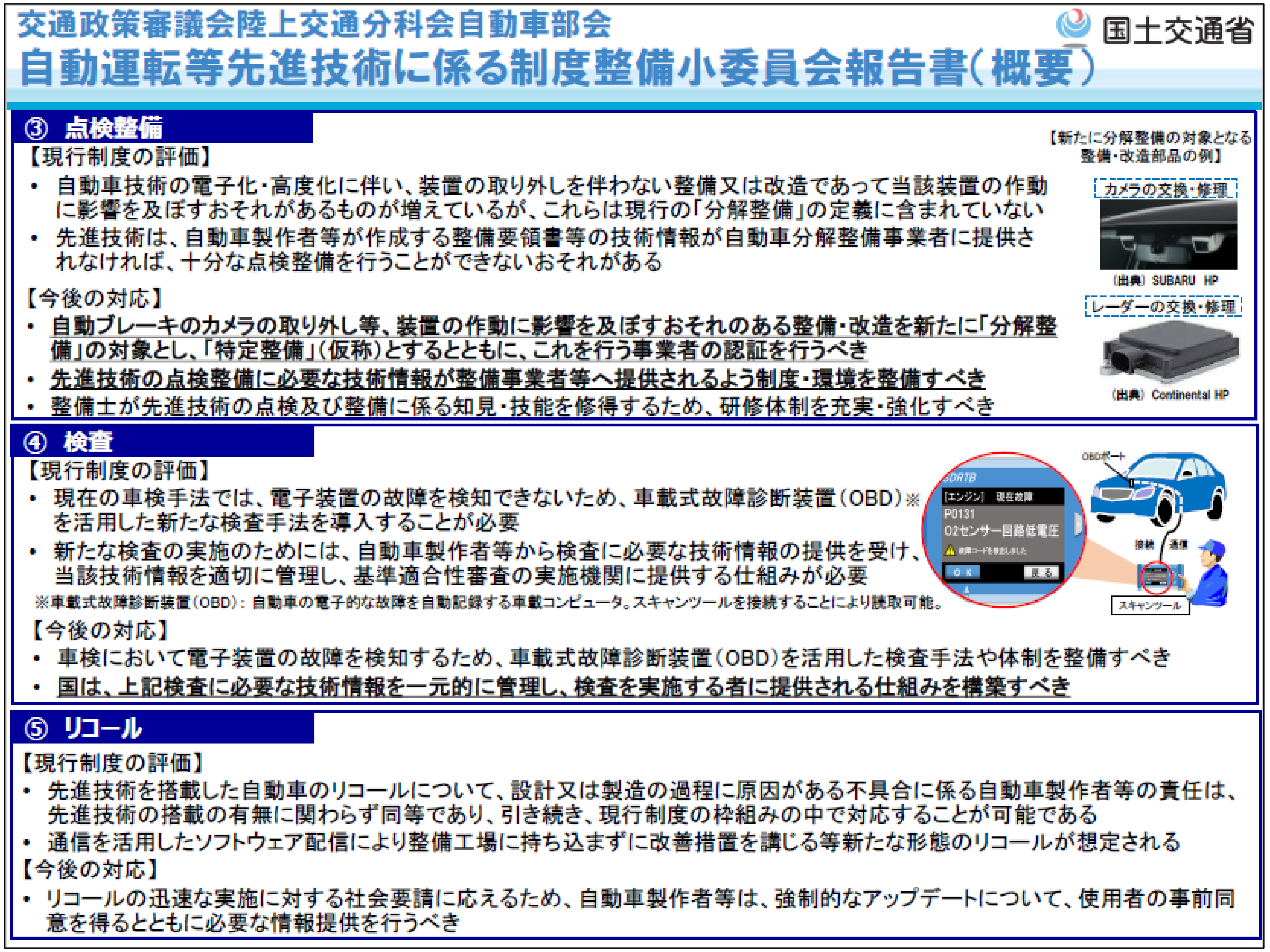
② 型式指定（認証）・ソフトウェアの変更

【現行制度の評価】

- 自動運転システムについては、実際の走行環境を模擬したテストコース等技術的に高度な審査が必要となることが想定されるが、審査手法が定められていない
- 通信を活用したソフトウェア配信により、自動車の電子的な改造が大規模に行われることは想定されていない

【今後の対応】

- ガイドラインをベースに安全性能を確認するとともに、シミュレーション、テストコース又は公道試験の適切な組合せ等具体的な手法の検討を提案する等国際的な議論を主導すべき
- 自動運転システムの適切かつ円滑な審査を実施するための体制を整備すべき
- 自動車の安全性に大きな影響を及ぼすソフトウェアの配信について、国がその適切性を確認する制度を創設すべき



交通政策審議会陸上交通分科会自動車部会

国土交通省

自動運転等先進技術に係る制度整備小委員会報告書（概要）

③ 点検整備

【現行制度の評価】

- 自動車技術の電子化・高度化に伴い、装置の取り外しを伴わない整備又は改造であって当該装置の作動に影響を及ぼすおそれがあるものが増えているが、これらは現行の「分解整備」の定義に含まれていない
- 先進技術は、自動車製作者等が作成する整備要領書等の技術情報が自動車分解整備事業者に提供されなければ、十分な点検整備を行うことができないおそれがある

【今後の対応】

- 自動ブレーキのカメラの取り外し等、装置の作動に影響を及ぼすおそれのある整備・改造を新たに「分解整備」の対象とし、「特定整備」(仮称)とするとともに、これを行う事業者の認証を行うべき
- 先進技術の点検整備に必要な技術情報が整備事業者等へ提供されるよう制度・環境を整備すべき
- 整備士が先進技術の点検及び整備に係る知見・技能を修得するため、研修体制を充実・強化すべき

【新たに分解整備の対象となる整備・改造部品の例】

カメラの交換・修理

(出典) SUBARU HP

レーダーの交換・修理

(出典) Continental HP

④ 検査

【現行制度の評価】

- 現在の車検手法では、電子装置の故障を検知できないため、車載式故障診断装置（OBD）※を活用した新たな検査手法を導入することが必要
- 新たな検査の実施のためには、自動車製作者等から検査に必要な技術情報の提供を受け、当該技術情報を適切に管理し、基準適合性審査の実施機関に提供する仕組みが必要

※車載式故障診断装置（OBD）：自動車の電子的な故障を自動記録する車載コンピュータ。スキャンツールを接続することにより読取可能。

【今後の対応】

- 車検において電子装置の故障を検知するため、車載式故障診断装置（OBD）を活用した検査手法や体制を整備すべき
- 国は、上記検査に必要な技術情報を一元的に管理し、検査を実施する者に提供される仕組みを構築すべき

⑤ リコール

【現行制度の評価】

- 先進技術を搭載した自動車のリコールについて、設計又は製造の過程に原因がある不具合に係る自動車製作者等の責任は、先進技術の搭載の有無に関わらず同等であり、引き続き、現行制度の枠組みの中で対応することが可能である
- 通信を活用したソフトウェア配信により整備工場に持ち込まずに改善措置を講じる等新たな形態のリコールが想定される

【今後の対応】

- リコールの迅速な実施に対する社会要請に応えるため、自動車製作者等は、強制的なアップデートについて、使用者の事前同意を得るとともに必要な情報提供を行うべき

Source：Report by the Council of Transport Policy; Automobile Division; Land Transportation Committee (2019/1/15)
https://www.mlit.go.jp/common/001268577.pdf

2. Japan Trends：J-Auto-ISAC (Information Sharing Analysis Center)

J-Auto ISAC was established in January 2017, following the example of the US Auto ISAC

Trend

USA

■ Auto-ISAC established under the initiative of the US government in January 2016

- ➢ Participation by variety of industries sectors, such as automotive, parts suppliers, telecommunications and IT, incl. Japanese OEMs

Momentum has grown to establish Japan version of ISAC with a view to quickly address situations unique to Japan (e.g. vehicles sold only in Japan, micro cars),

Japan

■ Industry-driven ISACs were established in Finance and ICT

- ➢ The government-led cyber security action plan for key infrastructure industries also places importance on information sharing across public- and various

Momentum to establish Japan ISAC grew among supervisory agencies and the auto industry as they recognized needs to share information on "automobiles"

＜Activities＞

1. Investigation on cyber threats against automobiles
2. Analysis of cyber security levels
3. Technical analysis on vulnerabilities
4. Gathering and analysis of related information
5. Simulation drill of auto cyber attacks

Summary

- The Regulations is progressing internationally to avoid vehicles Cyber security risks.
- In Japan, regulations on vehicle cyber security and software updates will be implemented next year.
- In my presentation, I summarized the latest regulations related to security in Japan and globaly, as well as the development of standards that correspond to cyber security and software update.

Thank you!

ありがとうございました