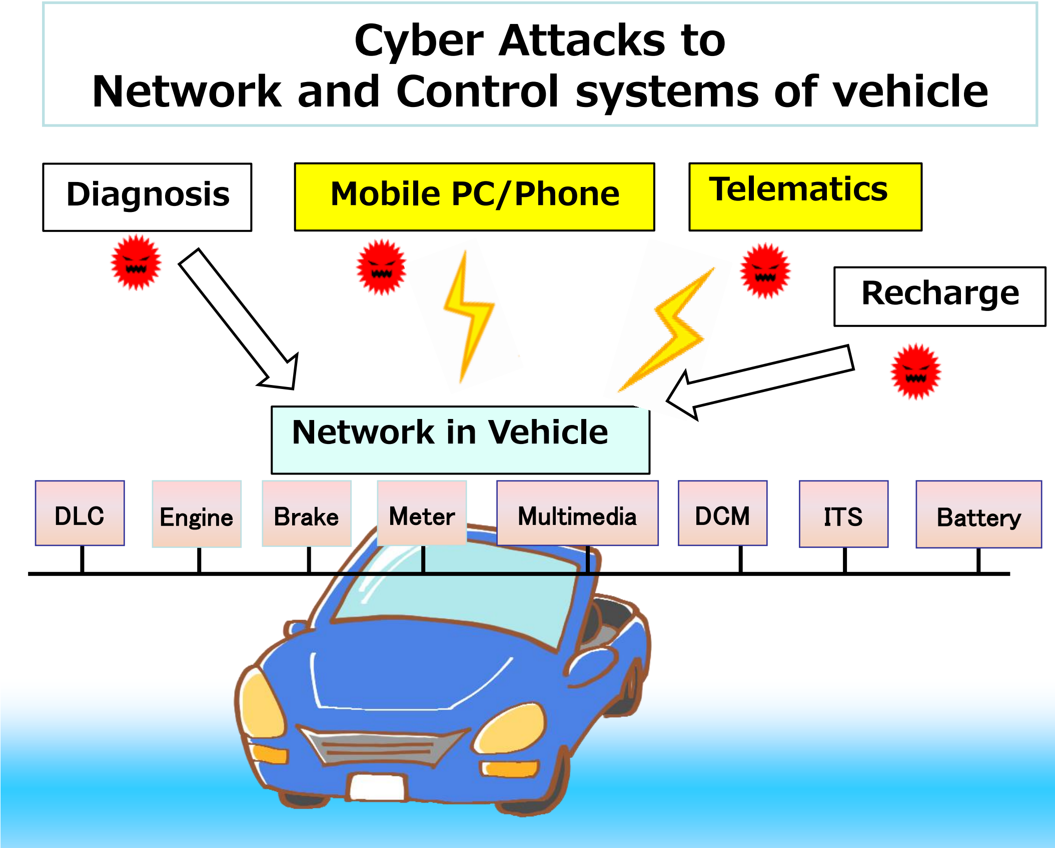
Outline of Japan-Auto-ISAC

Nov. 14, 2017
JAMA J-Auto-ISAC
Shigeru UEHARA

1. Cyber Risks in Vehicle

Cyber Risks in control and information systems of Vehicle

- Current vehicle fulfills hi performances by connecting to the outside. As the result, the possibility to be attacked is increased.



Top Priority

To prevent･･･

- Occurring unsafe behavior of vehicle
- Theft of Private information of users

2． Support by Government

- Executive order PDD63 in 1998 by President Clinton directed to share the information in every 18 significant infrastructure areas.
  → Establish ISAC in every 18 areas
  （Bank, Finance, Electricity, Waterworks, Traffic, Tele-communication, nuclear plant, munitions ・・・)

- Establish National Council of ISAC to share the 18 areas' information cross-functionally in 2003

- Executive order 13636 in 2013 by President Obama directed to formulate a Framework to enhance the cyber security performances

- Establish Auto ISAC in Aug., 2015
  Start to work in Jan., 2016

- Conference of Information security policy by cabinet office in 2006 （Secure JAPAN2006）

- Establish CEPTOAR in 10 significant infrastructure areas to share the information in 2007
  Currently, 18 CEPTOARs of 13 areas are working

- Establish CEPTOAR Council to share the 10 areas’-information cross-functionally in 2009

- Issued Cyber Security guidelines for The business management by METI → Next page

- Currently, 4 ISACs are working in Japan
  Bank/Finance (2014), Telecommunication (2015), Electricity (2017) and Automobile (2017)

METI's* request (2015)

*Ministry of Economic,
Trade and Industry

Cyber Security guidelines for The business management

<10 items to be focused>

1. Recognize and face up to RISKs by whole of organization
2. Establish risk management system
3. Set a target of security level and make plan to achieve
4. Establish divided steps to measure (PDCA) and Open it
5. Execute defensive measures with affiliate companies & partners and keep watching the conditions
6. Secure resources (Budget, Talent)
7. Clarify IT systems to be consigned as outsourcing and secure the performance of cyber security
8. Participate in Information sharing activities and utilize
9. Establish facing system to emergency cases(CSIRT**, Manual)
10. Clarify where to notice and the information to be opened in case of cyber incident occurs

**Computer Security Incident Response Team

3． Necessity of Auto ISAC

① Why is ISAC necessary in Automobile industry world independently？

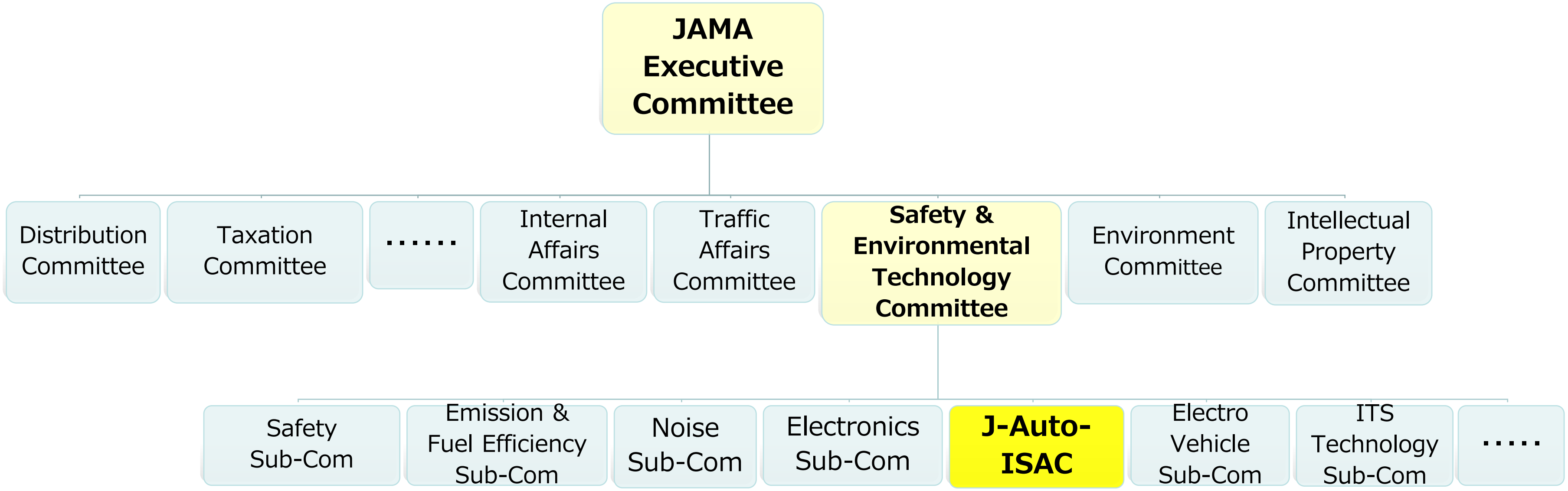
- Communication H/W & S/W in vehicle are so different from these of significant infrastructure areas'.
  So, The attacking method would be also very different.
  We need to study and research independently.

② Why is ISAC necessary in Japan ?
Isn't it enough to participate US Auto ISAC?

- Against the Japan domestic cyber incidents, we need to have the mobility which can take action properly and immediately to prevent diffusing damages by quick analysis.

Established J-Auto-ISAC under Safety & Environmental Technology Committee of JAMA (Jan/2017)

Position in JAMA organization



JAMA Executive Committee

Distribution Committee

Taxation Committee

……

Internal Affairs Committee

Traffic Affairs Committee

Safety & Environmental Technology Committee

Environment Committee

Intellectual Property Committee

Safety Sub-Com

Emission & Fuel Efficiency Sub-Com

Noise Sub-Com

Electronics Sub-Com

J-Auto-ISAC

Electro Vehicle Sub-Com

ITS Technology Sub-Com

…..

J-Auto-ISAC members

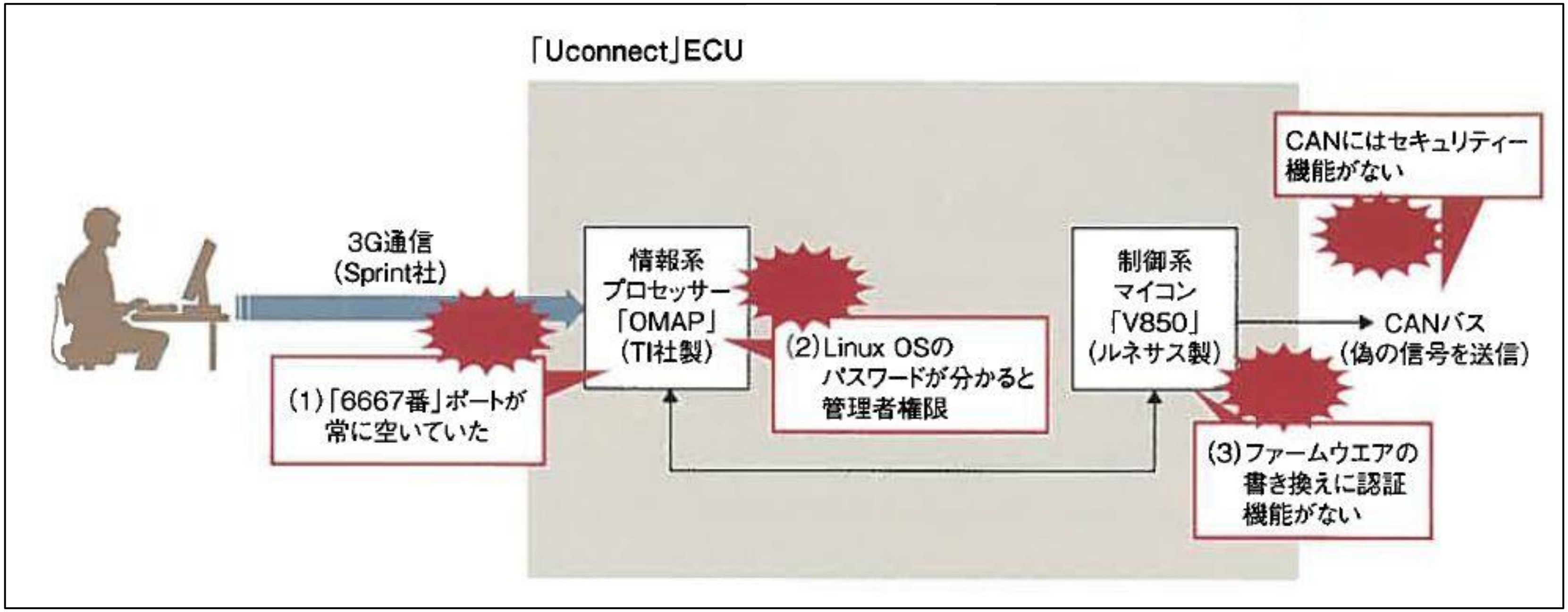
Co. Name		US A-ISAC Member
TOYOTA		✓
HONDA	HONDA The Power of Dreams	✓
NISSAN	NISSAN	✓
MAZDA	mazda	✓
SUBARU	SUBARU	✓
SUZUKI	SUZUKI	
MITSUBISHI	MITSUBISHI MOTORS	✓
DAIHATSU	DAIHATSU	
ISUZU	ISUZU	
HINO	HINO	
MITSUBISHI FUSO	FUSO	
YAMAHA	YAMAHA Revs Your Heart	

Appendix

FCA Jeep Hacking（2015）

The Common steps of IT hacking were applied

1. Find out an Open-port then intrude ⇒ Remote intrusion via 3G line
2. Get Root Privilege of Linux in Target ECU ⇒ Take over almost all controls of ECU
3. Take Action / Rewrite firmware of CPU ⇒ Control vehicle remotely


「Uconnect」ECU
CANにはセキュリティー機能がない
3G通信（Sprint社）
情報系プロセッサー「OMAP」（TI社製）
(2)Linux OSのパスワードが分かると管理者権限
制御系マイコン「V850」（ルネサス製）
CANバス（偽の信号を送信）
(1)「6667番」ポートが常に空いていた
(3)ファームウエアの書き換えに認証機能がない

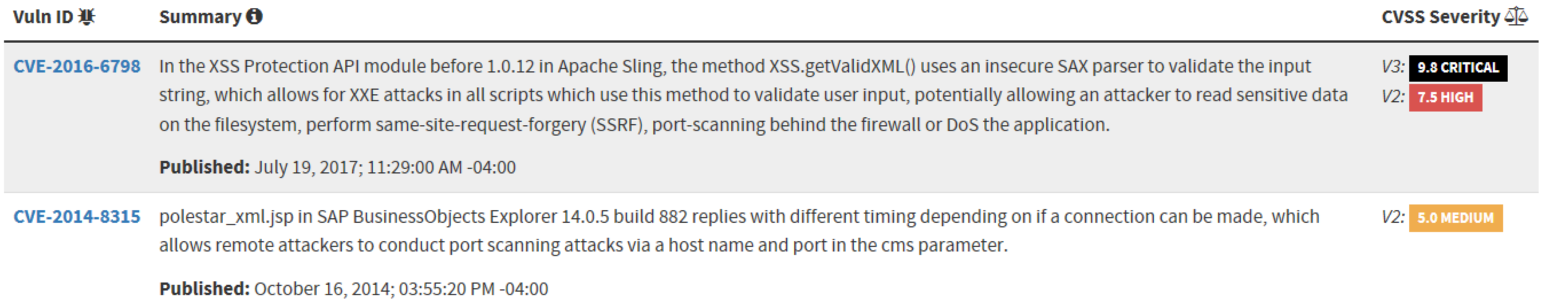
The source of NIKKEI Automotive Nov.2015

Currently, Almost all Vehicle attacking cases are done by the common steps coming from IT system attacking.
⇒ “For Vehicle special” doesn’t exist.

Cases used Step1&2 in IT system Attack

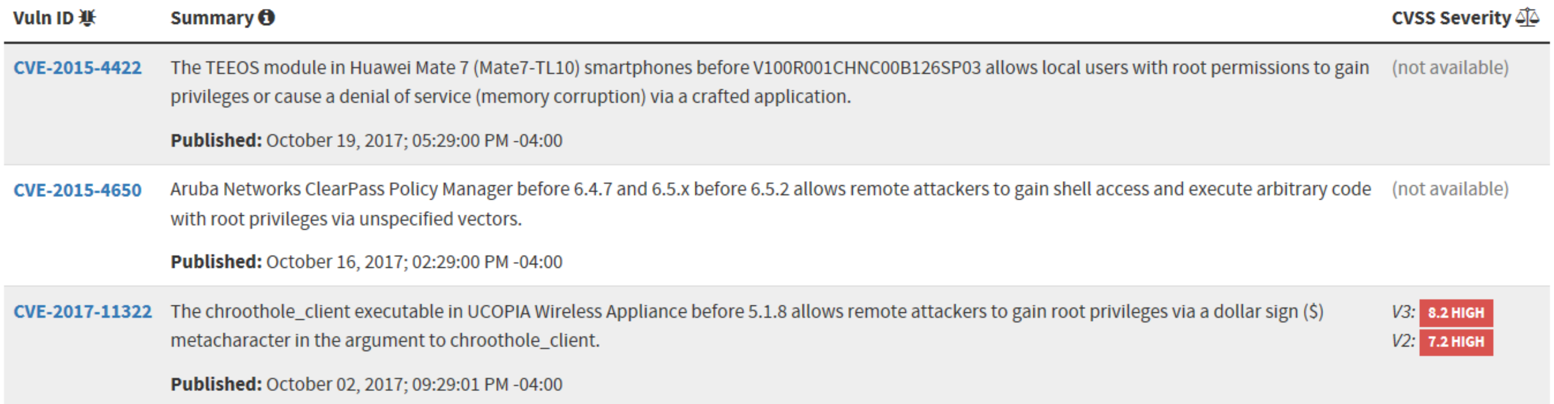
Searching Result at NVD (https://nvd.nist.gov/vuln/search) of USA

1. Find out an open port（by port-scan, “port scan”）⇒ Hit 317cases



Vuln ID	Summary	CVSS Severity
CVE-2016-6798	In the XSS Protection API module before 1.0.12 in Apache Sling, the method XSS.getValidXML() uses an insecure SAX parser to validate the input string, which allows for XXE attacks in all scripts which use this method to validate user input, potentially allowing an attacker to read sensitive data on the filesystem, perform same-site-request-forgery (SSRF), port-scanning behind the firewall or DoS the application. **Published:** July 19, 2017; 11:29:00 AM -04:00	V3: 9.8 CRITICAL V2: 7.5 HIGH
CVE-2014-8315	polestar_xml.jsp in SAP BusinessObjects Explorer 14.0.5 build 882 replies with different timing depending on if a connection can be made, which allows remote attackers to conduct port scanning attacks via a host name and port in the cms parameter. **Published:** October 16, 2014; 03:55:20 PM -04:00	V2: 5.0 MEDIUM

2. Get Root Privilege（by root privileges）⇒ Hit 728cases



Vuln ID	Summary	CVSS Severity
CVE-2015-4422	The TEEOS module in Huawei Mate 7 (Mate7-TL10) smartphones before V100R001CHNC00B126SP03 allows local users with root permissions to gain privileges or cause a denial of service (memory corruption) via a crafted application. **Published:** October 19, 2017; 05:29:00 PM -04:00	(not available)
CVE-2015-4650	Aruba Networks ClearPass Policy Manager before 6.4.7 and 6.5.x before 6.5.2 allows remote attackers to gain shell access and execute arbitrary code with root privileges via unspecified vectors. **Published:** October 16, 2017; 02:29:00 PM -04:00	(not available)
CVE-2017-11322	The chroothole_client executable in UCOPIA Wireless Appliance before 5.1.8 allows remote attackers to gain root privileges via a dollar sign ($) metacharacter in the argument to chroothole_client. **Published:** October 02, 2017; 09:29:01 PM -04:00	V3: 8.2 HIGH V2: 7.2 HIGH