

国内外の自動車の情報 セキュリティ動向と意識向上策に 関する調査報告書

自動車の情報セキュリティ推進に向けて取り組むべき
3つの項目を提言



IPA[®]

独立行政法人 情報処理推進機構
セキュリティセンター

2010年4月

記載されている会社名、製品名、サービス名は各社の商標、または登録商標です。

目次

目次.....	i
図表目次	ii
はじめに	iv
i. 本報告書の目的.....	iv
ii. 昨年度までの活動	v
本報告書の概要.....	vi
主な用語	vii
略語一覧	viii
1. 国内外の自動車の情報セキュリティの動向	1
1.1 欧州の自動車の情報セキュリティの動向.....	1
1.2 米国の自動車の情報セキュリティの動向.....	16
1.3 日本国内の自動車の情報セキュリティの動向.....	20
2. 日本国内における関連制度の現状.....	24
2.1 運転免許制度.....	24
2.2 車検・点検・登録制度.....	26
2.3 リコール制度.....	27
2.4 自動車損害賠償責任保険（自賠責保険）.....	28
2.5 自動車リサイクル法.....	28
2.6 ヒアリング結果：自動車事故対策機構	29
2.7 ヒアリング結果：日本自動車整備振興会連合会(日整連)	30
3. 他分野での情報セキュリティ対策の動向	31
3.1 上水道分野用の SCADA セキュリティ グッド・プラクティス.....	31
3.2 マイクロソフト社のセキュリティ開発ライフサイクルの取組み	32
4. 自動車業界への情報セキュリティの啓発に向けて.....	33
4.1 自動車の情報セキュリティでの脅威が高まりつつある状況.....	33
4.2 製品のライフサイクル全体での情報セキュリティ対策.....	38
4.3 整備、車検などアフタ市場での情報セキュリティ対策.....	41
5. 自動車の情報セキュリティの推進に向けて	43
5.1 今回の調査のまとめ.....	43
5.2 自動車の情報セキュリティの推進に向けて	46
6. 参考資料.....	50
6.1 EU の Framework Programme における自動車関連の取組み.....	50
6.2 その他の欧州の自動車関連の取組み	59
6.3 日本における自動車のセーフティに関わる組織.....	65

6.4	重要インフラの情報セキュリティ グッド・プラクティス.....	69
6.5	制御システムと自動車システムの比較	72
6.6	Microsoft 社のセキュリティ開発ライフサイクルの取組み	76

図表目次

図 1-1	自動車自体の情報化と車車間・路車間通信の関係	1
図 1-2	欧州の主な ITS 関連の情報セキュリティに関する活動	3
図 1-3	FP7 の自動車の情報セキュリティ関連プロジェクトの対象範囲.....	4
図 1-4	欧州の自動車の情報セキュリティの進め方 - 3 つを同時に	4
図 1-5	EVITA の全体像	6
図 1-6	EVITA で検討している FPGA プロトタイプ実装の概略図	7
図 1-7	EVITA から見た車載ネットワークの構造	8
図 1-8	Car2X の利用事例の分類	9
図 1-9	攻撃者から見た動機と攻撃の体系化	10
図 1-10	Car2X で守るべき対象	10
図 1-11	「認められていないブレーキ操作」の攻撃ツリー	12
図 1-12	周囲の車の突然のブレーキ操作の偽装	13
図 1-13	「料金ゲートの通過を妨害する」攻撃ツリー	14
図 1-14	料金ゲートの通過を妨害する	15
図 1-15	車載システム向けソフトウェア更新の要求条件	22
図 2-1	自動車の運転免許の更新、車検・点検の期間.....	24
図 4-1	OpenECU.org の EcuFlash 画面例	34
図 4-2	インターネット用ルータ機器の汎用チップへの脅威につながるアクセス例	35
図 4-3	Car2X のネットワーク・アーキテクチャ	37
図 4-4	ニセの急ブレーキ情報による自動車の安全への脅威の例	37
図 4-5	ソフトウェア開発ライフサイクルを通じたソフトウェアの欠陥修正コスト	39
図 4-6	IEC 61508 機能安全における製品のライフサイクル	40
図 5-1	部品・ソフトウェア・ネットワークの共通化、汎用品の採用による脅威の増大..	44
表 1-1	略語一覧.....	viii
表 1-1	攻撃者から見た攻撃目的	11
表 1-2	攻撃者から見た攻撃の手法.....	12
表 2-1	自動車のリサイクルにおける役割分担	29
表 4-1	EVITA でまとめられた攻撃対象と保護対象	38

表 6-1 経営者向けグッド・プラクティス.....	70
表 6-2 開発者向けグッド・プラクティス.....	71
表 6-3 重要インフラのセキュリティ課題と自動車システム.....	74
表 6-4 自動車システムの位置づけの検討表.....	75

はじめに

i. 本報告書の目的

近年、ITS(Intelligent Transport Systems: 高度道路交通システム)に対応した先進的な自動車や環境に配慮した次世代の交通手段として期待される電気自動車に求められるインテリジェントな電子制御技術の進展に伴い、自動車の情報セキュリティでの脅威の増大が懸念されている。前年度の研究会の検討結果と提言を受け、自動車業界の動向調査と自動車セキュリティ検討会での検討により以下の事項を整理し、自動車業界への情報セキュリティに関する啓発情報を提供する。

1) 海外での開発動向、セキュリティ検討状況の調査

海外、特に欧州の次世代の自動車を担う技術開発やセキュリティ検討の動向を文献や公開情報、有識者へのヒアリングを基に調査し、海外におけるセキュリティ検討の状況を把握し、日本での取組みの参考としてまとめる。

2) 自動車の情報セキュリティでの脅威と現行の自動車関連制度の整理

自動車の情報セキュリティでの脅威の現状について調査を行う。また、メーカーでの技術によるセキュリティ対策だけでは限界があるとの想定から、制度面での受け皿も必要となると思われる。関係組織や有識者へのヒアリングを基に、自動車の情報セキュリティでの脅威と自動車社会を支える現行の自動車関連制度に求められる将来的課題を整理する。

3) 有識者を交えた自動車のシステム開発者のセキュリティ意識向上に関する検討

自動車産業の関係者及びセキュリティ専門家などを交えた検討会を設置し、検討会の中で、昨年度の調査結果及び過去のセキュリティ対策の取組み事例を自動車開発者の参考となる形でまとめ、セキュリティ意識向上をはかる資料としてまとめる。

検討会開催に際しては、事前に国内の技術開発動向や自動車関連組織での調査やセキュリティ検討の状況を文献や公開情報、関連組織や有識者へのヒアリングを基に調査して検討材料としている。

ii. 昨年度までの活動

本報告書に関連する調査活動として、平成 18 年度のカーナビと ETC(Electronic Toll Collection System: 自動料金収受システム¹)に関するセキュリティ技術マップの調査²、平成 19 年度のカーナビ、携帯電話、情報家電の組み合わせ利用のセキュリティ脅威の検討³がある。

平成 20 年度には「自動車と情報家電の組み込みシステムのセキュリティに関する調査報告書⁴」として、自動車及び情報家電に関して、組み込み機器本体と、組み込み機器を利用したサービスを包括した全体像を整理し、守るべき対象や脅威、セキュリティ対策の方向性を以下のように整理しており、今回の調査にも反映している。

- 1) 利用者にセキュリティ対策を施す意識、被害に気づく知識をもたせる
- 2) 利用者側にセキュリティ対策に適切なコストをかける文化を醸成する
- 3) 自動車・車載機メーカーに十分なセキュリティ対策を働きかける
- 4) 自動車のセキュリティ対策に関連した制度やしきみを充実する
- 5) 何が繋がっているか、誰が利用しているかを明らかにする
- 6) セーフティ(安全)とセキュリティの連携により安全・安心を実現する

¹ ETC: 自動料金収受システム: 「ITS における専用狭域通信の研究開発・標準化動向」より- http://www.oki.com/jp/Home/JIS/Books/KENKAI/n187/pdf/187_R22.pdf

² IPA 「組み込みシステムの脅威と対策に関するセキュリティ技術マップの調査」2007 年 第八章 カーナビ、第九章 ETC

<http://www.ipa.go.jp/security/fy18/reports/embedded/>

³ IPA 「複数の組み込み機器の組み合わせに関するセキュリティ調査」2008 年

<http://www.ipa.go.jp/security/fy19/reports/embedded/>

⁴ 自動車と情報家電の組み込みシステムのセキュリティに関する調査報告書

<http://www.ipa.go.jp/security/fy20/reports/embedded/>

本報告書の概要

1 章「国内外の自動車の情報セキュリティの動向」では、海外の動向として欧州での自動車の情報セキュリティの研究、開発の活動事例を紹介している。米国については自動車関連の複数の基調講演も行われた CES 2010(Consumer Electronics Show 2010)等の発表から見た、自動車の情報技術と自動車の情報セキュリティの動向について紹介する。日本国内については、自動車の情報セキュリティに関する調査研究・開発活動として、IPA(Information-technology Promotion Agency, Japan)の発表とトヨタ IT 開発センターの発表事例を紹介している。

2 章「制度、教育に関する自動車の情報セキュリティの動向」では、文献調査および自動車整備と事故対策関連団体のインタビューにより、現状の制度や教育、運用面における自動車の情報セキュリティの課題をとりあげる。

3 章「他分野での情報セキュリティ対策の動向」では、自動車の情報セキュリティ対策の参考となると考えられる、他分野の情報セキュリティへの対応事例を紹介している。一つ目は社会的なインフラ(Infrastructure)の制御システムの一例である上水道分野用の SCADA(Supervisory Control And Data Acquisition)セキュリティグッド・プラクティスである。二つ目として、製品の企画から開発・出荷・保守・運用のすべてを含めた情報セキュリティ対策の一例として、マイクロソフト社のセキュリティ開発ライフサイクルの取組みを紹介している。

4 章「自動車業界への情報セキュリティの啓発に向けて」では、現状または将来懸念される自動車の情報セキュリティでの脅威の例、開発ライフサイクルでの対策の必要性、整備・車検などアフタ市場での対策の必要性を紹介している。また、自動車の情報セキュリティだけでなく安全にも影響を及ぼす脅威として、車載制御機器である ECU(Embedded Control Unit)の不正な書き換えの例をとりあげる。

5 章「自動車の情報セキュリティの推進に向けて」では、今回の調査のまとめから、今後、自動車の情報セキュリティの推進に向けた、今後の課題やテーマを整理する。

6 章「参考資料」では、上記報告の根拠となる関連資料と参照先、要約などを列挙している。国内外の団体、活動については、テーマや規模・予算などを含め、シート形式で整理している。

主な用語

・「自動車の情報セキュリティ」

一般的な情報セキュリティを指す場合は「情報セキュリティ」とし、自動車特有の情報セキュリティを指す場合は「自動車の情報セキュリティ」と表記する。なお、自動車業界で「セキュリティ」と呼ぶ場合、自動車の盗難防止製品や不正侵入検知機器などを指すことが多いため、記述に留意する。

・「オープン化」

「オープン化」という言葉にはさまざまな意味が含まれているため、本報告書ではできるだけ「オープン化」という用語は使わず、共通化、標準化などの個別の表現を用いる。

・「共通化」、「汎用化」、「標準化」

「共通化」という表現は、同じ自動車業界内で部品やソフトウェアを同じ手順や仕様で利用できるようにすることを指す。また、他の業界や複数用途にも利用できる部品やソフトウェアについては「汎用化」と表現する。また、「標準化」とは特定の業界団体や規制機関などで、文書化された規定や規約を作成して、業界の共通基準として採用することを指す。

・「ネットワーク」

「ネットワーク」という用語については、自動車内の車載ネットワークおよび自動車と外部を接続するネットワークの両方を指す言葉として利用している。

・「自動車」

「自動車」と「車両」という用語については、本報告書では「自動車」という表記に統一する。また、昨年度の用語を踏襲し、自動車の内部については「自動車内」、自動車の外部については「自動車の外部」と表記する。英文では関連する用語として Vehicle と Car と Automobile があるが、文中では両方とも「自動車」と表記している。なお、車検制度や運転免許制度などの法令には「自動車」と「車両」という表記があるが、できるだけその法令にあわせた表記を心がけている。

・「ITS」

「ITS」は情報通信技術を利用して、安全運転の支援や交通管理の最適化を図るシステムの概念である。「ITS」が ITS Japan や ITS World などの関連団体を指す場合もあるが、本報告書では前者を指す用語として使用する。

略語一覧

本報告書で使用する略語は以下の通りである(表 1-1)。

表 1-1 略語一覧

略語	名称
ABS	Antilock Brake System
ADOSE	reliable Application specific Detection of road users with vehicle On-board Sensor
API	Application Programming Interface
ATESST2	Advancing Traffic Efficiency and Safety through Software technology 2
AUTOSAR	Automotive Open System Architecture
C2C	Car to Car Communication
C2C-CC	Car-to-Car Communication Consortium
C2I	Car to Infrastructure Communication
C2X	Communication between cars or car to infrastructure
CAN	Controller Area Network
Car2X	car-to-car and car-to-infrastructure
CC	Common Criteria
CES	Consumer Electronics Show
COMeSafety	COMmunication for eSafety
CPU	Central Processing Unit
CTP	Common Transport Protocol
CU	Communication Unit
CVIS	Cooperative Vehicle-Infrastructure Systems
DCS	Distributed Control System
DOT	Department Of Transportation
DRM	Digital Rights Management
DSRC	Dedicated Short-Range Communication
DSRC-SPF	DSRC-Security Platform
EASIS	Electronic Architecture and System Engineering for Integrated Safety
E-Toll	Electronic Toll
ECU	Embedded Control Unit

略語	名称
EDR	Event Data Recorders
escar	Embedded Security in Car Conference
ETC	Electronic Toll Collection System
ETM	ECU Trusted Module
ETSI	European Telecommunications Standards Institute
ETSI TC-ITS	ETSI Technical Committee-ITS
EVITA	E-Safety Vehicle Intrusion Protected Applications
EWS	Engineering Work Station
EU	European Union
EURIDICE	European Inter-Disciplinary research on Intelligent Cargo for Efficient, safe, and environment-friendly logistics
Euro F.O.T	Euro Field Operation Tests
EVITA	E-safety Vehicle Intrusion proTected Applications
FP	Framework Programme
FP6	Sixth Framework Programme
FP7	Seventh Framework Programme
FPGA	Field Programmable Gate Array
GPS	Global Positioning System
HAVE-IT	Highly Automated VEHICLES for Intelligent Transport
HMI	Human Machine Interface
HSE	Health and Safety Executive
HU	Head Unit
GM	General Motors
GST	Global System for Telematics
GUI	Graphic User Interface
GW	Gate Way
I/F	Interface
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers,Inc.
IETF	Internet Engineering Task Force
INTERSAFE2	cooperative INTERsection SAFETy 2
IP	Internet Protocol
IPA	Information-technology Promotion Agency, Japan
IPsec	Security Architecture for Internet Protocol
ISITS	International School of IT Security
ISMS	Information Security Management System

略語	名称
ISO	International Organization for Standardization
IT	Information Technology,
ITS	Intelligent Transport Systems
JARI	Japan Automobile Research Institute
JasPar	Japan Automotive Software Platform and Architecture
JTAG	Joint Test Action Group
JVN	Japan Vulnerability Notes
LAN	Local Area Network
LIN	Local Interconnect Network
M2M	Machine to Machine
MISRA	The Motor Industry Software Reliability Association
NADA	Nanodatacenters
OA	Office Automation
OBD-II	On-Board Diagnostics, II generation, ISO-9141-2
OpenTC	The Open Trusted Computing
OS	Operating System
Oversee	Open VEhiculaR SEcurE platform
PC	Personal Computer
PA	Process Automation
PCIS	Partnership for Critical Infrastructure Security
PL	Product Liability
PLC	Programmable Logic Controller
PRE-DRIVE_C2X	PREparation for DRIVing implementation and Evaluation of C-2-X communication technology
PRECIOSA	PRivacy Enabled Capability In co-Operative systems and Safety Applications
RFID	Radio Frequency Identification
SAFARIDER	advanced telematics for enhancing the SAFety and comfort motorcycle RIDERs
SAM	Secure Application Module
SCADA	Supervisory Control And Data Acquisition
SD ³ +C	Secure by Design, by Default and in Deployment + Communications
SDL	Security Development Lifecycle
SDLC	Software Development Life Cycle

略語	名称
SECRICOM	Secure Crisis Communication
SESSAME	Society of Embedded Software Skill Acquisition for Managers and Engineers
SeVeCom	Secure Vehicle Communication
SIP	Session Initiation Protocol
SSL	Secure Socket Layer
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
SWI	Secure Windows Initiative
TCP/IP	TCP/IP(Transmission Control Protocol / Internet Protocol)
TECOM	Trusted Embedded Computing
TLS	Transport Layer Security
TUI	Touch User Interface
TS	Technical Specification
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to X
VICS	Vehicle Information and Communication System
VII	Vehicle Infrastructure Integration
VUI	Voice User Interface
WG	Working Group
WP	Work Package
ZF	ZF Friedrichshafen AG

1. 国内外の自動車の情報セキュリティの動向

日欧で進められている自動車情報システム用のセンサや制御装置、通信機などの部品や通信手順の共通化・標準化は外部ネットワーク利用および低価格化を同時に実現する方策として推進されている。欧州では AUTOSAR(Automotive Open System Architecture)が、日本では JasPar(Japan Automotive Software Platform and Architecture)などが共通化・標準化活動を行っており、補完協力関係を構築している。また、外部のネットワークを利用する手段として、携帯電話、無線 LAN(Local Area Network) などの汎用的な通信に加え、DSRC(Dedicated Short-Range Communication)などを利用した車車間通信(C2C: Car to Car Communication)、路車間通信(C2I: Car to Infrastructure Communication)の議論、検討も進んでいる。

しかしながら、自動車部品や通信手順の共通化や標準化、外部ネットワーク手段の拡大は自動車の情報セキュリティでの脅威ともなりうる。このため、並行して脅威の想定や対策の検討が必要と考えられるが、日米と欧州では取組みについて大きな差が見られた。

本章では、調査結果を基に、自動車の情報セキュリティに関する日米欧の取組みの差を明らかにする。

1.1 欧州の自動車の情報セキュリティの動向

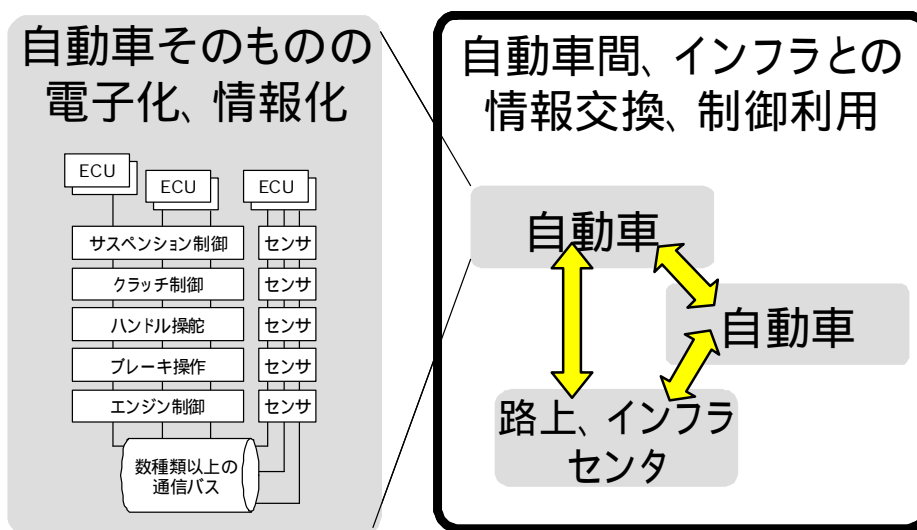


図 1-1 自動車自体の情報化と車車間・路車間通信の関係

主に欧州での情報セキュリティに関する取組みでは、EU(European Union)を中心として自動車の情報セキュリティに対する体系的な取組みがある。その背景には、図 1-1 のように自動車自体の電子化、情報化が進み、多数の組込み型のコンピュータとセンサーが搭載されて通信するようになったことと、ITSのように自動車間や路上、インフラの情報システムとの間でも通信を行って、自動車の利便性、安全性向上に役立てる目的がある。さらに大きな目標としては、こうした研究や活動の成果によって欧州域内の産業を活性化し、国際競争力を高めようとする狙いもある。

1.1.1 欧州での主な自動車の情報セキュリティに関する活動

図 1-2 は欧州での主な ITS 関連の情報セキュリティに関する活動を示した図である。一番右の COMeSafety(COMMunication for eSafety)は自動車以外の無線周波数やサーバなどのインフラを含め、ITS 全体のアーキテクチャを定義し、欧州全体で関連する研究や技術開発、標準化などの複数プロジェクトの協調を行うとともに、知識の共有や人材交流も行っている。PRE-DRIVE_C2X(PREparation for DRIVING implementation and Evaluation of C-2-X communication technology)は欧州での車車間・路車間通信の実証実験と、車車間・路車間通信などの協調システムにおける自動車の情報セキュリティのためのアーキテクチャとフレームワークを定義している。PRECIOSA(PRivacy Enabled Capability In co-Operative systems and Safety Applications)は ITS で利用される位置情報に関連するプライバシー情報を、個人情報保護の規制に適合できるようにするプロジェクトである。

SeVeCom(Secure Vehicle Communication)と、その後継である EVITA(E-Safety Vehicle Intrusion Protected Applications)というプロジェクトは自動車の情報システムと利用手順の整理から、特定の利用環境に応じた脅威の分析と特定を行った上で、情報セキュリティ対策を検討している。SeVeCom は主に車車間について、EVITA では主に自動車内と路車間で交換するメッセージの信頼性を担保するための対策を検討している⁵。またプライバシーについても同様に検討しており、特に車車間・路車間で交換されるメッセージ内の位置情報がプライバシーにとって脅威になるとして対策を検討している。

図 1-2 にある各プロジェクトは EU の FP(Framework Programme)という研究開発支援の枠組みによる支援を受けている。FP6(Sixth Framework Programme)は前期の活動を、FP7(Seventh Framework Programme)は 2007 年から 2013 年までの今期の活動に該当する。FP7 からの支援規模については、1.1.2 欧州・研究開発フレームワーク「FP7」と自動車の情報セキュリティプロジェクトで紹介する。

⁵ SeVeCom は主に車車間について、EVITA では主に...
EVITA Deliverable D2.1:
Specification and evaluation of e-security relevant use cases, P.3
<http://evita-project.org/Deliverables/EVITAD2.1v1.1.pdf>



図 1-2 欧州の主な ITS 関連の情報セキュリティに関する活動

欧州では、ITS World Congress⁶という、ITS 関連の展示発表会も開催されており、関連業界や団体間の情報交換、人材交流の場となっている。図 1-3 は ITS World Congress 2009 で発表された資料から、FP7 における上記以外の自動車の情報セキュリティ関連プロジェクトの対象範囲を図にしたものである⁷。図の上段、CVIS (Cooperative Vehicle-Infrastructure Systems)⁸プロジェクトは ITS のための中核となる無線通信技術や協調システムの基盤の策定を目的としている。GST⁹(Global System for Telematics)は、効率的な自動車テレマティクスを実現するためのサービスなどを検討したプロジェクトである。CVIS と GST は ITS 実現のための道筋をつけるという意味で、ビジネスの保護が対象といえる。

図の中段の EVITA は侵入保護、SeVeCom は PRECIOSA と並んでプライバシー保護も目的にしたプロジェクトとして紹介されている。Oversee(Open Vehicular SEcurE platform)は、ITS アプリケーションを複数同時に実行するときに、仮想 OS(Operating System)のように強力に隔離された実行環境を提供する基盤を検討するプロジェクトで、2010 年開始予定と紹介されている。

⁶ ITS World Congress - <http://www.itsworldcongress.com/>

⁷ ITS World Congress, 2009 年 9 月 SeVeCom プレゼン資料より

http://www.sevecom.org/Presentations/VariousWorkshops/Sevecom_2009-09_ResearchPrivacy.pdf

⁸ CVIS - <http://www.cvisproject.org/>

⁹ GST - <http://www.gstforum.org/>



図 1-3 FP7 の自動車の情報セキュリティ関連プロジェクトの対象範囲

SeVeCom、EVITA に共通するのは、ITS や統合安全システムなどの利便性と、それを実現するための自動車のアーキテクチャを整理体系化しながら、システム構成に起因する根本的な原因から情報セキュリティ対策を検討し、利便性、安全性の実現コストを最低限にしようとしている点である。

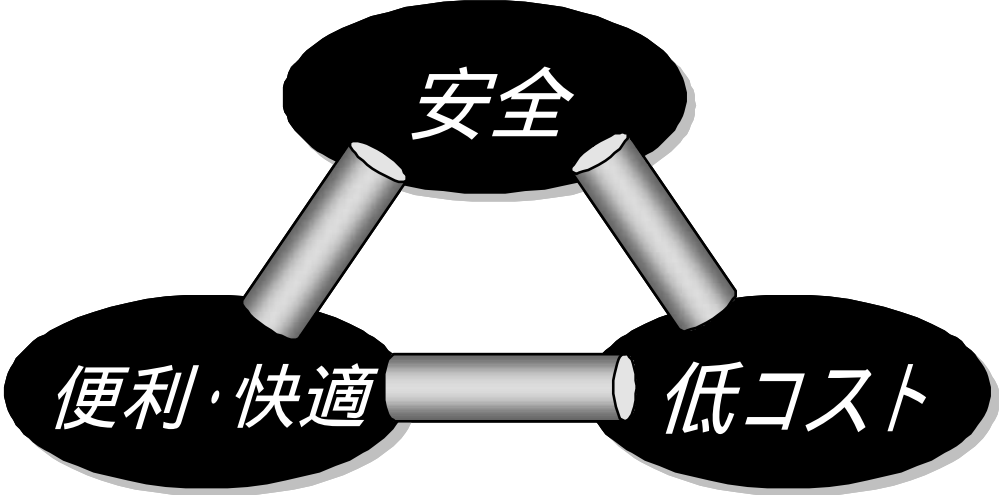


図 1-4 欧州の自動車の情報セキュリティの進め方 - 3 つを同時に

1.1.2 欧州・研究開発フレームワーク「FP7」と自動車の情報セキュリティプロジェクト

FP7 の 7 年間の総予算は約 505 億ユーロで、年平均で 70 億ユーロ以上となっている¹⁰。

このうち、自動車に関連した予算としては、“Challenge 6 - ICT for mobility, environmental sustainability & energy efficiency”がある。この中で、「インテリジェントな自動車と移動サービスのための情報通信」という募集には約 57 百万ユーロの予算が、「車車間・路車間の協調システムのための情報通信」という募集には、約 48 百万ユーロ、「環境管理と省エネのための情報通信」という募集では約 54 百万ユーロの予算となっている。これら募集の予算額は 2007-2008 年分(ICT WP 2007-8)である。

また、自動車の情報セキュリティ関連では、少なくとも EU FP6 での SeVeCom、EASIS(Electronic Architecture and System Engineering for Integrated Safety)への拠出額で 8 百万ユーロ、EU FP7 での EVITA、PRECIOSA への拠出額で 5.4 百万ユーロ以上である。

1.1.3 EVITA での情報セキュリティの検討動向

以下では、特に自動車の情報セキュリティについて検討が進んでいる EVITA の動向を紹介する。EVITA は、EU が中期的に 3～5 年間単位で新たな技術開発研究へ投資する FP7 プロジェクトの一つで、主に車車間通信と路車間通信のための情報セキュリティ技術を確立しようとする活動である。特に EVITA は脅威の分析とリスクの評価を体系的に行っている点と、自動車の安全にも関わるような脅威についても分析しているため、特に詳しく紹介する。

EVITA のテーマは車車間通信と路車間通信を総合して、Car2X(Car-to-Car and Car-to-Infrastructure¹¹)通信の情報セキュリティを確保するための基盤技術の実現にある。プロジェクト開始当時に計画された 2010 年までの EVITA の作業予定を図 1-5 にまとめた。

¹⁰ NEDO「第 7 次研究開発フレームワーク計画 (FP7) の予算、欧州委員会の希望を下回る (EU)」より

<http://www.nedo.go.jp/kankobutsu/report/982/982-15.pdf>

¹¹ Car2X: EVITA D2.1, 2.1.1 Car-to-Car and Car-to-Infrastructure Communication Architecture - <http://evita-project.org/Deliverables/EVITAD2.1.pdf>

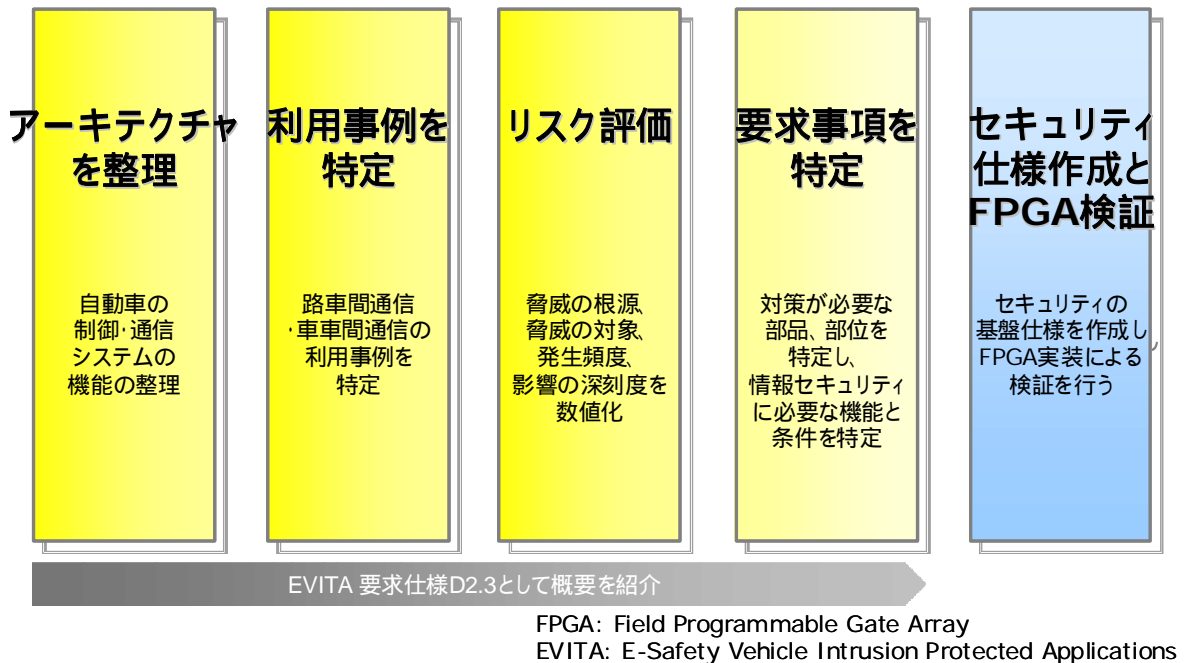


図 1-5 EVITA の全体像

2009年11月の時点で、EVITAでは要求仕様D2.3(成果物2.3)¹²、セキュリティ仕様D3.1(成果物3.1ドラフト)¹³のドキュメントを公開し、Car2Xのための情報セキュリティの要求事項と、セキュリティと信頼モデルについて定義している。なお、EVITAの文書名D2.3、D3.1などに含まれる”D”の文字は”Deliverable”の略で、プロジェクトや作業ごとの成果物のことである。

EVITAのD3.1セキュリティ仕様の特徴は、車載バスを利用して通信するECUとセンサの間で、相互に通信上の信頼を確立しようとする点にある。そのため、図1-5“セキュリティ仕様作成とFPGA検証”(FPGA: Field Programmable Gate Array)では、セキュリティチップのようなものに格納された部品ごとの認証・識別情報を利用して、メッセージ送信時にメッセージ署名を追加し、メッセージ受信時にメッセージ署名を検証することなどが検討されている。

EVITAでは上記のような信頼モデルをCar2Xのためのセキュリティ基盤と位置づけ、このプロトタイプ実装としてFPGAに実装して検証する予定である。そのFPGAプロトタイプ実装の概略図¹⁴を図1-6に紹介する。

¹² EVITA Deliverable D2.3, Security requirements for automotive on-board networks based on dark-side scenarios - <http://www.evita-project.org/Deliverables/EVITAD2.3.pdf>

¹³ EVITA Deliverable D3.1, Security and trust model
<http://www.evita-project.org/Deliverables/EVITAD3.1.pdf>

¹⁴ EVITAで検討しているFPGAプロトタイプ実装の概略図“Vehicular Security Hardware”(2009年11月18日)より
<http://evita-project.org/Publications/Wolf08.pdf>

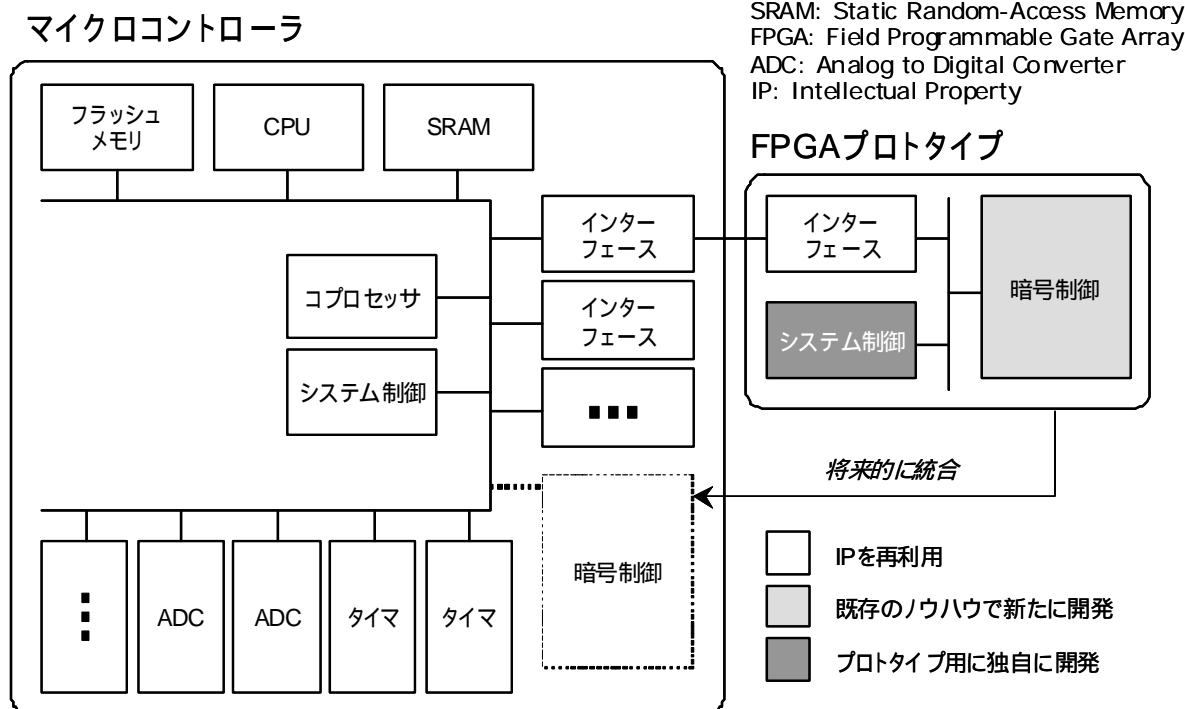


図 1-6 EVITA で検討している FPGA プロトタイプ実装の概略図

図の左のマイクロコントローラは既存の自動車内の車載ネットワーク上の制御機器である。これに対し、FPGA プロトタイプはインターフェースを介して、既存の技術を利用した暗号処理機能等を外部から追加する形になっている。将来的には既存のマイクロコントローラ上に、新規に開発した暗号制御機能を統合する見込みである。

以降では特に、攻撃者の動機と攻撃の手順と対象について体系的に整理されている2009年3月発行の要求仕様 D2.3 から、いくつかのシナリオとして想定事例を紹介する。

1) EVITA から見た車載ネットワークの構造

ここからはいったん EVITA の脅威の分析の手順に戻り、EVITA 要求仕様 D2.3 での体系的な自動車の情報セキュリティへの検討内容を見ていく。図 1-7 は EVITA 要求仕様 D2.3 で登場する車載ネットワークの構造図である。おおむね、色分けされたネットワークは別々の通信手順や異なる通信媒体を利用した独立したネットワークで、黒い線を通じて統合されているイメージである。ここでは特に、ヘッドユニット(HU: Head Unit)と呼ばれる情報系のシステムをまとめる装置と、インターネットや外界のネットワークに接続する通信ユニット(CU: Communication Unit)が自動車の駆動系やシャーシ/安全、ボディ/電装の機能と連携している点が重要である。

USB(Universal Serial Bus)やBluetoothなどの外部インターフェースを利用して、図右上にあるような自動車内に持ち込まれる音楽プレーヤや携帯電話機などがヘッドユニットに接続される。通信ユニットは自動車の外部との通信機能を持ち、GPS(Global Positioning System)や欧州のガリレオと呼ばれる位置測位衛星と通信したり、携帯電話の第三世代データ通信(UMTS: Universal Mobile Telecommunications System)や、車車間・路車間通信のための DSRC で自動車の外部のネットワークと接続する。通信ユニットからは、OBD-II(On-Board Diagnostics, II generation, ISO-9141-2)など車載の診断インターフェースを経由して、自動車の診断を行う機器やソフトウェアと ECU との間で通信が行われる。

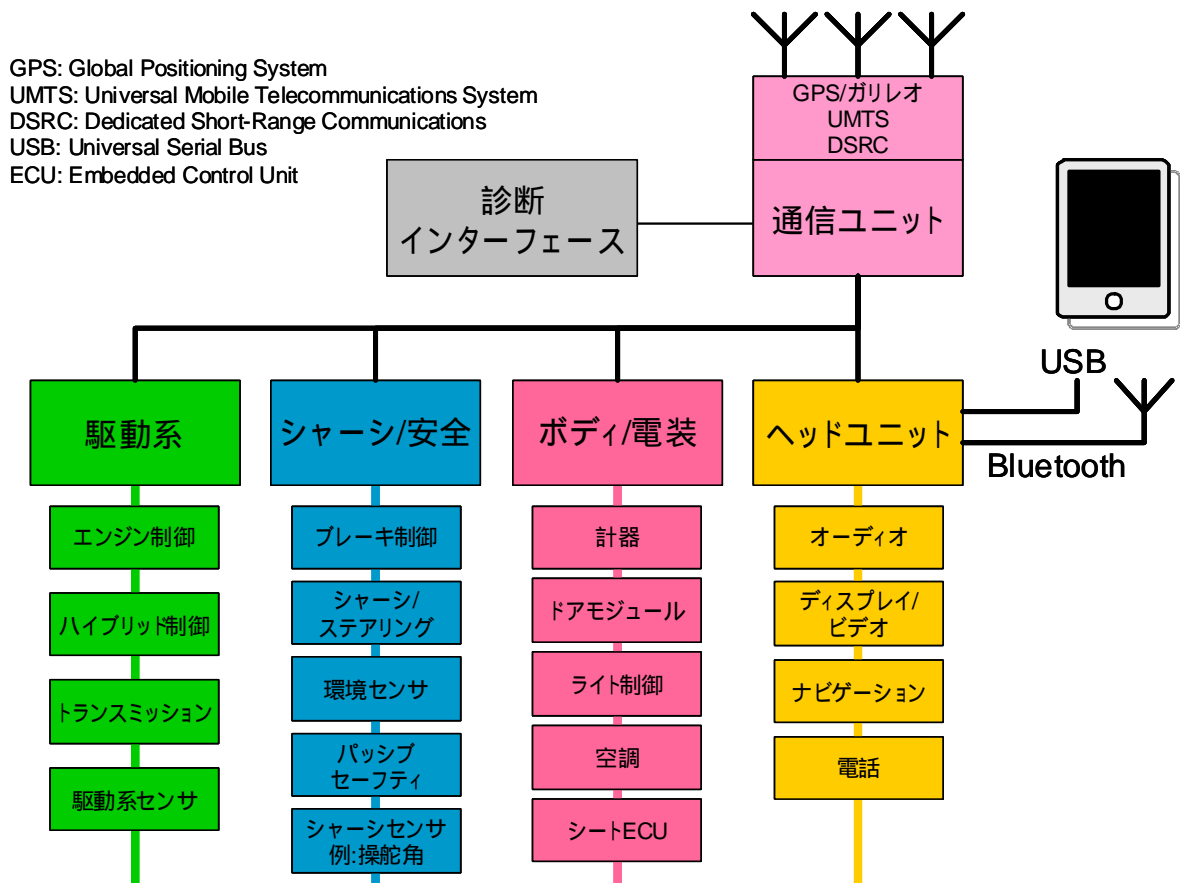


図 1-7 EVITA から見た車載ネットワークの構造

2) Car2X の利用事例の分類

図 1-8 は、EVITA で整理されている Car2X の利用事例の分類である。ここでは、車車間通信と路車間通信で行われる情報提供の方向を意識した利用の事例や、車内への持ち込み機器、修理点検について、6 つに大分類している。それぞれの利用事例の分類については、攻撃者から見た動機と手法の想定などが行われている。



図 1-8 Car2X の利用事例の分類

3) 攻撃者の動機と攻撃の体系化

図 1-9 は、EVITA で脅威の体系的な整理のために、攻撃者の視点から攻撃の動機や技術的実現性、攻撃手法を体系化するための整理ポイントを要約した図である。情報システムへの攻撃の動機をとりあげる場合、愉快犯や興味本位の不正アクセスも含まれて多岐にわたるが、EVITA では攻撃者が得られる利益や便益が特定され、さらに攻撃の技術的実現性があり、攻撃対象と攻撃手法が特定されるものについてだけ整理されている。また、EVITA では情報通信技術を利用した Car2X での情報セキュリティを検討しているため、ECU やセンサなどのハードウェアに直接アクセスしての攻撃は想定外としている。

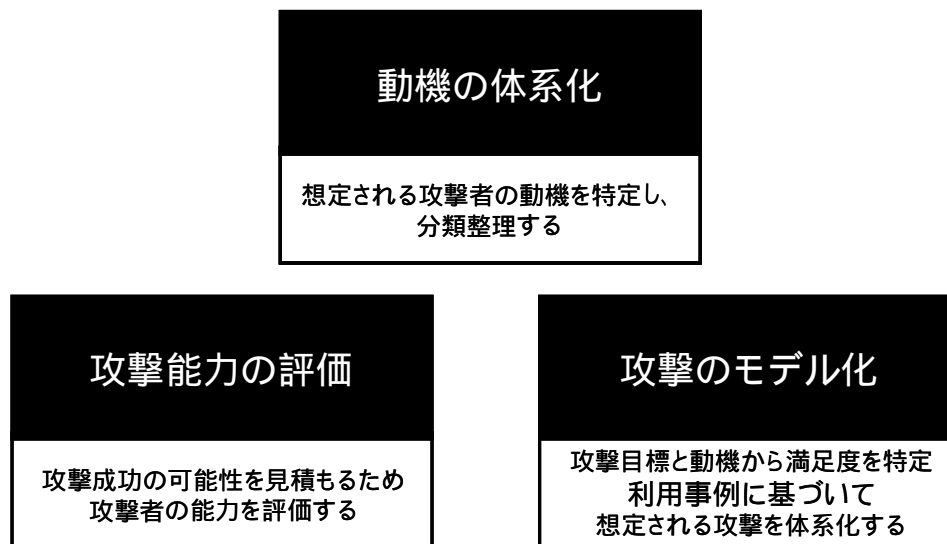


図 1-9 攻撃者から見た動機と攻撃の体系化

4) Car2X で守るべき対象

図 1-10 は、EVITA で検討されている Car2X における守るべき対象をカテゴリ分けしたものである。EVITA ではこれら 4 つのカテゴリごとに、脅威の影響による深刻度を分類し、深刻度の合算値を使って脅威の評価を行っている。深刻度は Severity の頭文字 S で表し、各カテゴリを S_o 、 S_s 、 S_p 、 S_f と表記する。添字は operational (操作性能)、safety (安全)、privacy (プライバシー)、financial (財産) の各頭文字である。

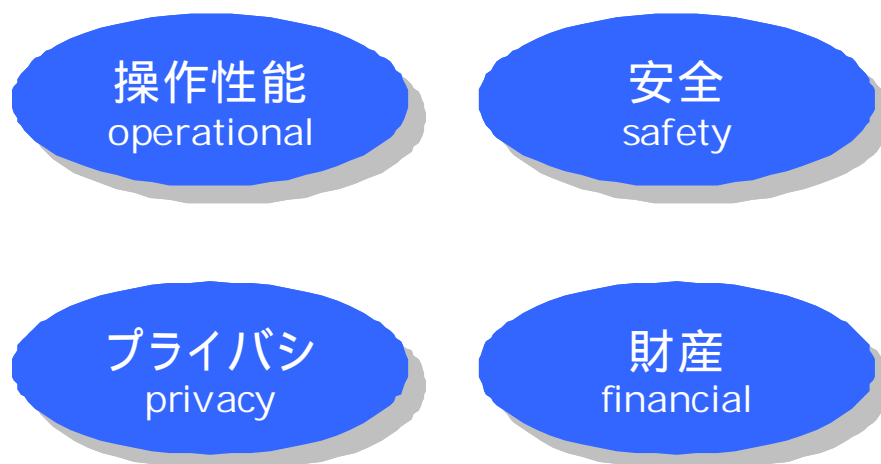


図 1-10 Car2X で守るべき対象

操作性能は、すべての自動車と ITS において意図した操作性能を維持することを意味している。安全は、自動車の搭乗者と他の道路利用者に対して安全を担保することである。プライバシーは、運転者の個人情報のプライバシーと自動車の製造者、部品供給者の

知的財産を保護することが含まれている。財産については、Car2X の利用中の商取引上の詐欺や自動車の盗難を防ぐことなどが含まれている。

5) 攻撃者から見た攻撃目的と攻撃手法

EVITA では、攻撃者から見た Car2X に関する攻撃目的(Attack Goal)と攻撃手法(Attack Methods)を表 1-1、表 1-2 のようにまとめている。なお、これら攻撃目的の抽出は、攻撃対象になる部品や手順を特定するために行われているため、攻撃のあとで発生する結果や影響による分類は行われていないもようだ。影響については、38 ページ・表 4-1 にまとめられているが、大きく分けて個人または団体に被害を負わせる場合と、攻撃者が関係する個人または組織がなんらかの利益を得る場合が想定されている。これら影響のうち、複数が同時に発生する場合もあると考えられる。

表 1-1 攻撃者から見た攻撃目的

EVITA で想定される攻撃者から見た攻撃目的	
1	攻撃者前方の信号を緑に変更する
2	自動車のスピード上限を操作変更する
3	交通の流れを操作する
4	交通渋滞を装う
5	警告メッセージ/表示の改ざん
6	緊急通報(E-Call)の妨害、偽装
7	エンジンを利用不能にする
8	認められていないブレーキ操作
9	アクティブブレーキ動作の妨害
10	料金収受(E-Toll)システムへの攻撃

上記の攻撃目的については、EVITA 要求仕様 D2.3 の中で、それぞれの攻撃者からの動機についても短く触れられている。たとえば、「1. 攻撃者前方の信号を緑に変更する」では、攻撃者が信号機でストップすることなく走行できる。また「7. エンジンを利用不能にする」ことにより、特定の自動車を利用しようとする人が、「重要な予定を逃してしまうなどの影響がある」と指摘している。

表 1-2 攻撃者から見た攻撃の手法

EVITA で想定される攻撃者から見た攻撃手法	
1	修理工場で OBD ごとの書き換え機能を悪用する
2	通信ユニットの脆弱性から OBD で書き換えできないようブロックする
3	ヘッドユニットの脆弱性を悪用して乗っ取りを行う

攻撃者から見た攻撃手法としては、機器の脆弱性を利用したソフトウェア書き換えを試みる方法のほかに、修理工場で自動車の保守機器などを利用して直接的に書き換えを行う手法も候補としてあげられている。

攻撃目標の中から特に「8. 認められていないブレーキ操作」と「10. 料金収受 (E-Toll)システムへの攻撃」について、EVITA で想定されている攻撃手法の例をとりあげて脅威の事例として 6)および 7)で紹介する。

6) 脅威の事例 - 「認められていないブレーキ操作」

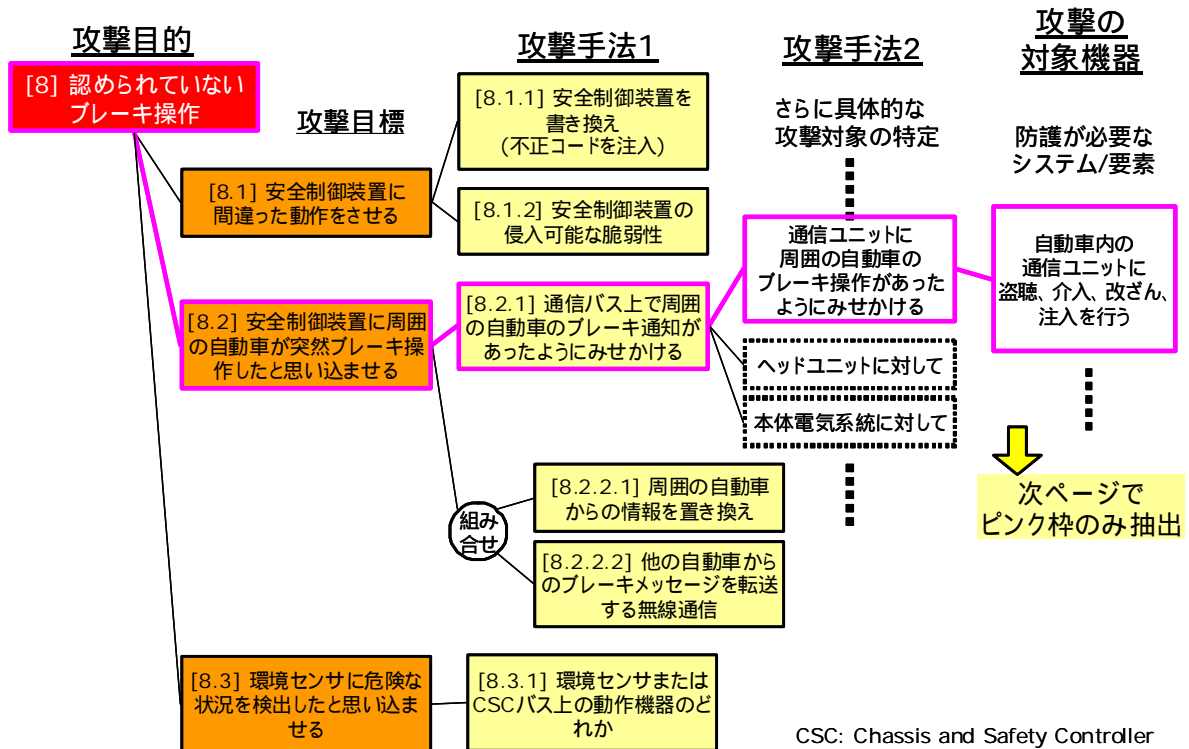


図 1-11 「認められていないブレーキ操作」の攻撃ツリー

図 1-11 は EVITA で想定されている攻撃者側から見た攻撃目的のうちの一つ、「認められていないブレーキ(Unauthorized Brake)操作」の攻撃手法と攻撃対象機器を

体系的に整理したものである。

この攻撃ツリーの図は脅威ツリーとも呼ばれ、外部からの攻撃から脅威だけではなく、内部的な問題や不具合からくる危険性を検討するときにも利用される。脅威を体系化する理由¹⁵としては、できるだけ問題の根本にあたる部位や原因の根源について脅威を軽減する対策をとることで、枝葉にあたる複数の脅威を軽減したり排除できる利点がある。

図 1-11 では、「認められていないブレーキ操作」を実行するために、想定できる現実的な攻撃手法を体系化している。[8.1.1]等のラベルは、攻撃の対象と手法を詳細化するにしたがって末尾に追加する数字が増える。EVITA の攻撃ツリーの図では、最終的にツリーの末端にあたる図右端に、「図 1-7 EVITA から見た車載ネットワークの構造」で整理されたヘッドユニットや通信ユニットなどの車載の情報システムの機器が攻撃対象として特定されている。

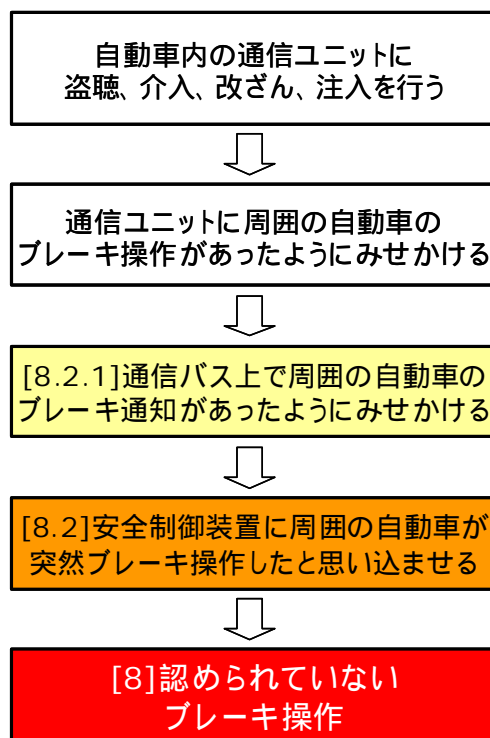


図 1-12 周囲の車の突然のブレーキ操作の偽装

「認められていないブレーキ操作」という攻撃目的については、「[8.1]安全制御装置に間違った動作をさせる」、「[8.2]安全制御装置に周囲の自動車が突然ブレーキ操作したと思い込ませる」、「[8.3]環境センサに危険な状況を検出したと思い込ませる」という攻撃目標(Attack Objectives)が想定されている。このうち、「[8.2]安全制御装置に周囲の自動車が突然ブレーキ操作したと思い込ませる」攻撃目標について詳しく見ると、

¹⁵ 脅威の体系化...: 「脅威モデル - セキュアなアプリケーション構築」日経 BP ソフトプレス、Frank Swidersky、Windows Snyder 著、渡部 洋子監訳、2005 年

「[8.2.1]通信バス上で周囲の自動車のブレーキ通知があったようにみせかける」という手法があり、さらにその通知を送る対象として、「通信ユニット...」、「ヘッドユニット...」、「本体電気系統に対して...」が候補として特定されている。それぞれについて、防御が必要なシステムを特定していくと、通信ユニットについては、盗聴や介入、改ざん、注入をされることが攻撃手法として特定されている。

「[8.2]安全制御装置に周囲の自動車が突然ブレーキ操作したと思込ませる」という攻撃目標についてだけ、脅威のシナリオとして逆の順序で並べると図 1-12 のようになる。このシナリオでは「自動車内の通信ユニットに盗聴、介入、改ざん、注入を行う」という、コンピュータや情報家電製品によるある攻撃手法を起点にして、自動車内の安全制御装置に影響を及ぼし、認められていないブレーキ操作を引き起こしている。

7) 脅威の事例 - 「料金収受システム (E-Toll) への攻撃」

次に、EVITA で Car2X への脅威と想定されている「料金収受システム (E-Toll) への攻撃」ツリーから、脅威の事例としてシナリオ例を紹介する。

EVITA 要求仕様 D2.3「B.3.10 Attacking E-Toll」では、欧州の料金収受システム(以下、「欧州の ETC」と略)への攻撃として複数の動機を想定している。そのうちのひとつとして料金ゲートの通過を妨害するため、欧州の ETC での支払い妨害などの攻撃を想定している。本来、走行して通過できるはずの料金ゲートで通過を妨害すると、攻撃者から見て運転者に対して危害を加えることができるという想定がある。

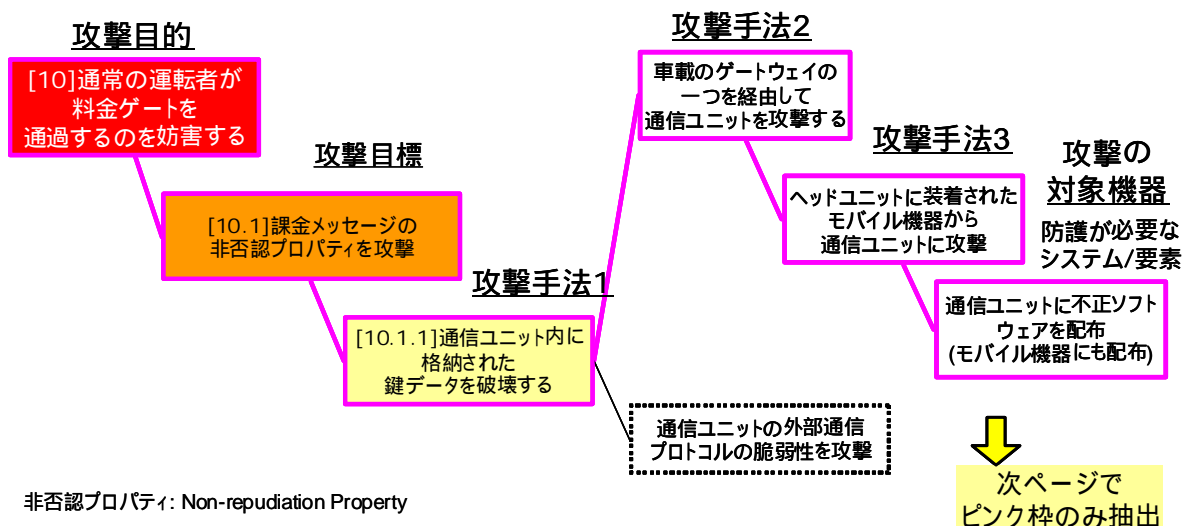


図 1-13 「料金ゲートの通過を妨害する」攻撃ツリー

このうち「料金ゲートの通過を妨害する」攻撃ツリーから「不正ソフトを拡散された通信ユニット」を攻撃の起点とする脅威のシナリオについて紹介する。

上の図 1-13 は電子的な料金支払いを妨害し、「[10]通常の運転者が料金ゲートを

通過するのを妨害する」という攻撃目的についての攻撃ツリーである。攻撃目標にある「[10.1]課金メッセージの非否認プロパティを攻撃」(非否認: Non-repudiation)とあるのは、料金収受システムで支払いが可能で決済が完了するはずのメッセージへの攻撃と考えられる。そのために、「[10.1.1]通信ユニット内に格納された鍵データを破壊する」ことで、決済が完了させられるようなメッセージの解釈や作成を妨害する手法が想定されている。攻撃の起点は図の右側にあるように自動車の外部から持ち込まれたモバイル機器となっている。攻撃の対象機器としては、自動車内の通信ユニットが特定され、持ち込まれた機器から通信ユニットに不正なソフトウェアが拡散(配布)される状況が想定されている。

この想定事例では、通信ユニット内のどれかのゲートウェイ、さらに通信ユニット内のある鍵データに対する攻撃として整理されているが、それ以上の特定まで行われていない。また、料金収受システムの料金計算の例では、自動車内の GPS の記録をもとに走行経路を計算する手順が想定されているなど、世界各地の料金精算方式の想定がカバーされていないとみられる。したがって EVITA 要求仕様 D2.3 での「料金収受システム(E-Toll)における攻撃ツリー」の想定には、まだ検討の余地があると考えられる。

なお、「料金ゲートの通過を妨害する」脅威ツリーから、「モバイル機器から不正ソフトウェアを拡散する」部分についてのみ、脅威のシナリオとして順序を並べると、次の図 1-14 のようになる。

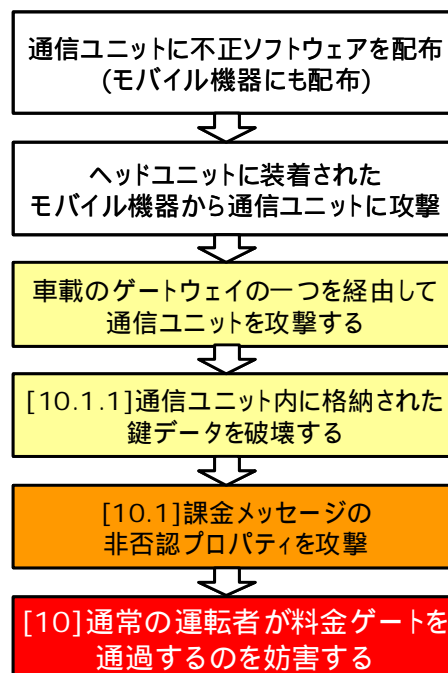


図 1-14 料金ゲートの通過を妨害する

1.2 米国の自動車の情報セキュリティの動向

米国ラスベガスで開催された 2010 International CES(Consumer Electronics Show)(2010 年 1 月 7 ~ 10 日)等において、自動車の情報セキュリティに関する調査を行った。

1.2.1 CES2010 におけるトピック

1) 米国 IntelliDrive プロジェクト

米国運輸省 (DOT: Department Of Transportation)関係者から「IntelliDrive プロジェクト」のセッションが行われた。本プロジェクトは ITS 対応の車車間 / 路車間通信により交通事故防止を狙うプロジェクトで、VII(Vehicle Infrastructure Integration)を目指している。通信プロトコルとしては DSRC を推進している。セッションの中では、安全については触れられているが、自動車の情報セキュリティについての説明は聞かれなかった。

2) フォードの Alan Mulally 社長 & CEO のキーノート

自動車の運転席ダッシュボードのインテリジェント化を狙っている SYNC システム (マイクロソフトと連携)の拡張についての紹介があり、iPhone、twitter 等のコミュニケーション・デバイスやサービスのユーザ数の急激増加から、車内でのコネクティビティが一層重要となる。自動車の世界でもシリコンバレーのスピードでの改革が必要であることなどが強調された。また、事故を防止するために運転者の動作の妨害になるものをいかに減らすかの観点で機能強化をしていること、そのために従来のグラフィカルなインターフェースに音声による指令、タッチによる指令などを組み合わせるとともに、Myford のような個人のカスタマイズ(パーソナライズ)を可能としたインターフェースをターゲットとしていることが説明された。

自動車の情報セキュリティについては具体的な説明はなかったが、インターネット接続を無線 LAN で実現する機能を今年末には提供すること、USB インターフェースの活用を積極的に進めることなどが紹介され、今後自動車の情報セキュリティの課題となると想定された。

3) 「標準装備・車内持込・外部ネットワーク接続 - 自動車がクラッシュしない/ デバイスが気をそらさせないための自動車開発」セッション

自動車内のコネクティビティやボイスコミュニケーションの必要が強調されており、前述の IntelliDrive プロジェクトと M2M 通信 (Machine to Machine: M は Car や Infrastructure で、車車間、路車間の通信) のターゲットの一つが事故防止であるとの紹介もあった。

1.2.2 CES2010 における技術ポイント

1) インフォテインメントのプラットフォーム動向

運転や車内活動環境を提供するインフォテインメントでは、米国 Ford 社が SYNC、イタリア Fiat 社が Blue&Me 及び韓国 KIA 社が UVO というインフォテインメント対応システムを展示していた。基本的な考えは、運転者の操作の妨害を低減するためにグラフィック (GUI: Graphic User Interface)、音声 (VUI: Voice User Interface) 及びタッチ (TUI: Touch User Interface) の操作インターフェースを実現している。ソフトウェア・プラットフォームは、マイクロソフト社の Windows Auto が採用されている。ここでも情報セキュリティに関する提案などは見られていない。

また、オープンソースの車載インフォテインメント・プラットフォームの開発・普及を進める GENIVI アライアンス¹⁶からも「GENIVI プラットフォーム 1.0」と呼ぶインフォテインメント対応システムが公開されていた¹⁷。GENIVI アライアンスはインテルや BMW、ゼネラル・モーターズ (GM: General Motors) など 8 社で設立され、その後日本の日産自動車、アルパイン、三菱電機、ローム、パイオニアの 5 社も参加を表明している¹⁸。

2) 外部ネットワークとの接続

自動車とモバイル機器との接続性がホットな話題となっている。

- ・携帯電話 (iPhone や Blackberry 等) の音声通話やテキストメールが進展
- ・インターネットラジオ (Radio over Internet) や Web アクセスの進展

¹⁶ GENIVI アライアンス - <http://www.genivi.org>

¹⁷ CES2010 における GENIVI プラットフォーム 1.0 の公開
<http://prw.kyodonews.jp/open/release.do?r=201001046914>

¹⁸ GENIVI への日本メーカ、サプライヤ 5 社の参加表明
http://car.watch.impress.co.jp/docs/news/20091119_330032.html

- ・インターネット接続を無線 LAN で実現する機能(2010 年末には提供予定)

3) その他

360 度監視カメラによる映像ログを取得する機器が展示されており、事故時の問題解決に有用と想定された。

1.2.3 米国における自動車の情報セキュリティについて

ネットワークや電子デバイスなど情報通信技術が、利用者の利便性だけでなく、「安全」を実現するための製品やサービス開発に積極的に活用されていることが感じられた。米国運輸省の IntelliDrive プロジェクトが ITS 対応の車車間 / 路車間通信による交通事故防止を狙っていることから、この傾向が伺える。これに関しては、情報通信技術で「安全」を実現するという観点のみならず、前述 1.2.1 3)のセッションのタイトルにもあるように、情報通信技術を活用したデバイスが運転手の注意を逸らせるなどの新たなリスクへの予防策という観点もあると想定される。

ただし、「情報通信技術」に関する製品・サービスが多数、紹介されているにも関わらず、全体を通じて「情報セキュリティ」に関する取組みの紹介が見られなかったことも事実である。これに関しては、「安全」の中に入れて検討しているのか、通信技術やデバイス開発など個別の技術の中で検討しているのか、もしくは「情報セキュリティ」に関する取組み自体が進んでいないのか、今後詳細な調査が必要である。

1.2.4 米国での ITS 動向

米国における ITS の利用動向に関しても、追加調査を行った。その結果、一例として以下のような動向が見られた。

GM は、子会社オンスターが展開する「車両診断電子メール通知サービス」で、利用者への電子メールの送信件数が 1 億件に到達し¹⁹、遠隔による自動車の診断サービスの普及が見られた。

米国運輸省(DOT)は 2010 年から 2014 年まで 5 年間の ITS 戦略研究計画を発表した²⁰。高速道路での事故の著しい削減など複数のビジョンを掲げ、IntelliDrive と呼ぶプログラムを進めている。IntelliDrive の主要な研究計画としては、安全を実現するための多様な取組みの実施、車々間と路車間の無線通信の相互運用性実現などが挙

¹⁹ 「車両診断電子メール通知サービス」で、利用者への電子メールの送信件数が 1 億件に到達し - ITS-P21 - <http://www.its-p21.com/information/2009/08/gm-1-1.html>

²⁰ 米国運輸省(DOT)は新しい ITS 戦略プランを発表した
http://www.its.dot.gov/strat_plan/

げられている。

Google は日産や BMW の自動車へマップサービスを提供を希望²¹しており、これからますますサービス対象としての自動車との親和性を高めたいと語り、インターネットサービス事業者として ITS への動きが見られた。

²¹ Google は日産や BMW の自動車へマップサービスを提供を希望 – TechOn
<http://techon.nikkeibp.co.jp/article/INTERVIEW/20090706/172647/>

1.3 日本国内の自動車の情報セキュリティの動向

自動車の情報セキュリティに関する検討動向として、関係組織へのヒアリングと本検討会の関係者による発表活動を紹介する。

1.3.1 DSRC 無線における検討事例

自動車の情報セキュリティの一部として、DSRC 無線を利用した ETC と料金支払い時のクレジットカード処理の扱い方について検討された事例があった。ETC では耐タンパモジュールである SAM(Secure Application Module)が車載器と路側機へすでに導入済みであり、DSRC には SSL(Secure Socket Layer)のように機能する DSRC-SPF(DSRC-Security Platform: DSRC セキュリティプラットフォーム)²²が規格化されている。

しかし、上記以外の ITS や安全システムなどを含めた自動車の情報セキュリティについては検討事例が見あたらなかった。総務省は平成 21 年 6 月に「ITS 無線システムの高度化に関する研究会」報告書²³を公開しているが、この中で「情報セキュリティは ITS 安全運転支援システムの実用化に向けた技術的課題の一つ」と指摘するにとどまっている。

1.3.2 財団法人 日本自動車研究所へのヒアリング調査

JARI(財団法人 日本自動車研究所: Japan Automobile Research Institute)へのヒアリングでは、これまで DSRC 車載器、路側機のセキュリティ対策の検討が行なわれ商品化されている例があるが、現在は情報技術による高度な機能に対するセキュリティ対策に関する目立った技術検討は国内では見られないとのことであった。

ただし、プライバシーに関しては、プローブ情報の個人情報保護に関する検討と国際標準化に向けた活動が行なわれているとのことであった。

1.3.3 日本整備振興会連合会へのヒアリング調査

日本国内の独立系の整備工場の連合体である日整連(日本整備振興会連合会)によ

²² ETC における SAM、DSRC-SPF

「組込みシステムの脅威と対策に関するセキュリティ技術マップの調査報告書」IPA、2007 年第 9 章 ETC、http://www.ipa.go.jp/security/fy18/reports/embedded/09_ETC.pdf

²³ 「ITS 無線システムの高度化に関する研究会」報告書、2009 年 6 月
http://www.soumu.go.jp/menu_news/s-news/14422.html

れば、整備士が自動車の高度な情報化と情報セキュリティに対応する必要性が認識されているが法制度が、未対応であるため進んでいない、という指摘があった。

1.3.4 発表事例：「自動車における組み込みセキュリティについて」

IPA セキュリティセンターは、自動車の情報セキュリティの方向性について、半導体製造に関する国際展示会「セミコン・ジャパン 2009」(2009 年 12 月 2～4 日 <http://www.semiconjapan.org/>)、Embedded Technology 2009/組み込み総合技術展(2009 年 11 月 18～20 日、<http://www.jasa.or.jp/et/ET2009/>)、組み込みシステム開発技術展(2009 年 5 月 13～15 日、<http://www.esec.jp/>)で発表を行っている。

本発表では、昨年の本検討会の成果や SeVeCom、EVITA などの欧州での自動車の情報セキュリティの活動として、自動車の情報セキュリティの検討フレームワークや要件を紹介している。その上で、情報セキュリティ対策の起点となるハードウェアとして、ECU Trusted Module(ETM)などのセキュリティモジュールの必要性を指摘している。

1.3.5 発表事例：「自動車におけるソフトウェア更新フレームワーク」

トヨタ IT 開発センターは、ドイツ「escar」(Embedded Security in Car Conference: エスカー、<http://www.escar.info/>)で、自動車内でのソフトウェアの更新に関する論文発表を行った。escar はドイツの民間企業が主催する自動車の情報セキュリティに関する年次の啓蒙イベントで、2009 年 11 月の開催で 7 年目となる。

論文発表では、自動車の車載の情報システムに特有の条件や背景から、車載のソフトウェア更新に関する 4 つの要件を整理した上で、サーバとクライアントのような関係からなる階層的なソフトウェアの更新アーキテクチャを提唱している。

次の図 1-15 は、論文中の車載システムのソフトウェアを更新するために必要とする要件の図から引用したものである。一つ目の Fail Safe は、車載の電池残量不足や何かの不具合でソフトウェアの更新が失敗して、システムの不具合につながらないようにする必要を指摘している。また、Resistance of Tampering は、更新しようとするソフトウェアが、更新手順の過程で改ざんされないようにする必要性を示している。Resource Limitation は、車載システム上では車内空間とコストの両面から、冗長化された記憶装置など、機器の追加は安易にできない制限を指摘している。Detection of Genuine ECU では、車載バス上に不正な ECU が挿入されたり、正規の ECU の通信が妨害されることがないように、正規の ECU のみと通信するしくみが必要としている。

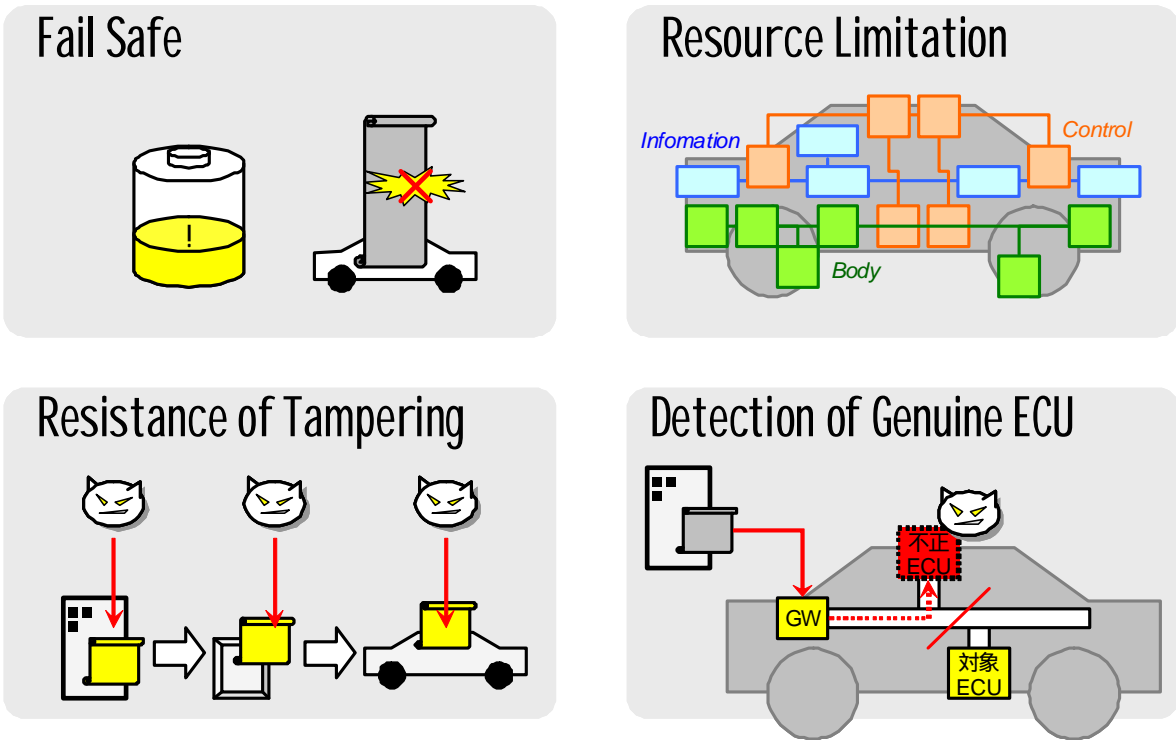


図 1-15 車載システム向けソフトウェア更新の要求条件

論文発表では、こうした車載システム向けのソフトウェアの更新について要件をまとめた上で、すでに多数の ECU が搭載されている車載環境においては、ソフトウェアの更新を階層的に行うことを提唱している。この階層化は、より多くのリソースを持つサーバ的な ECU と、より少量のリソースを持つクライアント的な ECU に分けて相対的に構成する方法が示されている。

1.3.6 プローブ情報に関する活動

今年度の本検討会では取り扱わなかったが、プローブ情報の取り扱いに関しても、セキュリティ問題を含めて考える必要がある。愛知 ITS 推進協議会と総務省東海総合通信局主催のセミナー²⁴では、プローブ情報実用化のための課題、ビジネスモデル構築の条件として、実験で想定している主要情報提供者であるタクシー事業者からの調達コストの圧縮、プローブ情報センターの運営コストの圧縮、ユーザへの高精度情報の提供と、ユーザ拡大を強調している。

このような動きの中で、プローブ情報に関しては、個人情報の保護やセキュアなプローブシステムに関して、学術レベルでの検討が始まっている。公表された情報の一例を以下に示す。

²⁴ プローブ情報の利活用に関するセミナー
<http://www.its-p21.com/information/2009/02/post-38.html>

「プローブ情報サービスにおける個人情報保護の標準化について」2006 年
<http://member.wide.ad.jp/tr/wide-tr-icar-probeprivacy-00.pdf>

「プローブデータを取り巻く動向と課題」2005 年
原田 昇 (東京大学)、吉井 稔雄(京都大学)、牧村 和彦(IBS)
<http://www.transport.iis.u-tokyo.ac.jp/publications/2005-007.pdf>

「匿名認証方式を用いたセキュアなプローブシステムの検討」2009 年
情報セキュリティ研究センター、繁富利恵
http://www.rcis.aist.go.jp/files/events/2009/0515-ja/RCIS2009_Shigetomi.pdf

2. 日本国内における関連制度の現状

自動車の情報セキュリティに関し、技術だけでは対応が困難な脅威への対策として制度や教育などの現状と可能性について検討するために、日本国内の動向に対する調査を実施したが、制度、教育面に関し、自動車の情報セキュリティに特化した具体的な取組みは見当たらなかった。自動車の検査団体と修理工場の業界団体へのヒアリングでは、情報セキュリティの必要性に関する意識は有しているものの、法制度等による裏付けがないため、具体的な活動に結びつけにくいように思われた。

そこで以下、各制度の情報セキュリティに関する活用面について考察する。

2.1 運転免許制度

図 2-1 は、自動車の運転免許の更新と車検・点検の期間を表にまとめたものである。自動車の情報セキュリティの対策について、定期的な確認や更新に利用できる期間であると考えられるため、参考として掲載する。

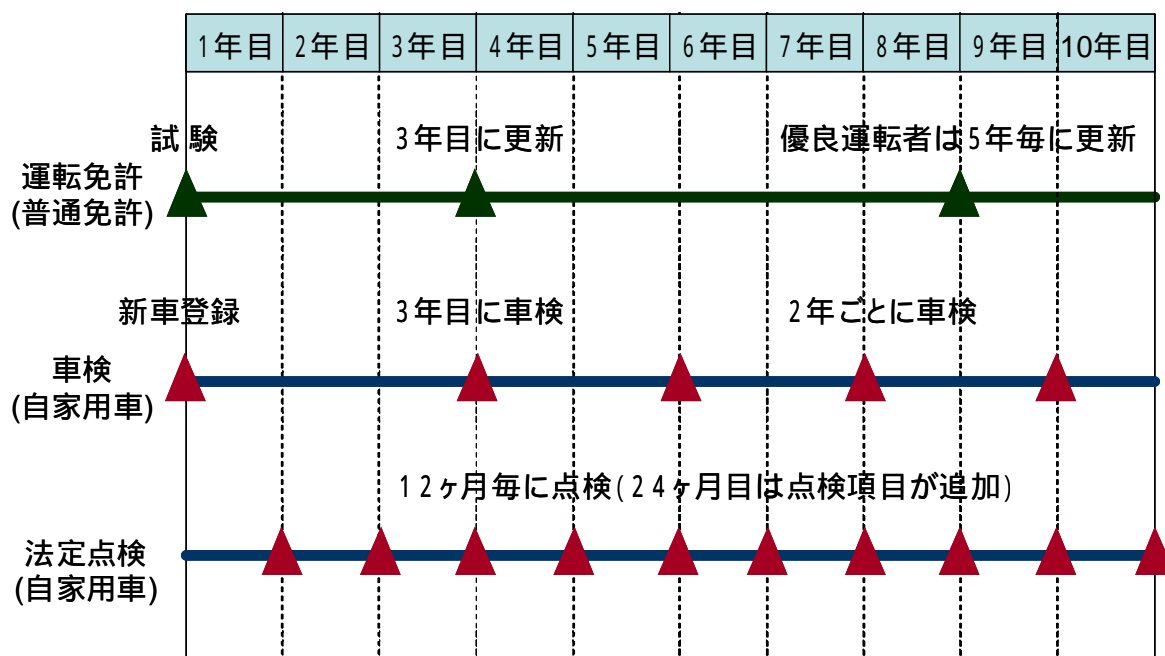


図 2-1 自動車の運転免許の更新、車検・点検の期間

情報セキュリティに関する知識を運転者に与える機会としての可能性を検討するために運転免許制度の整理を行う。運転免許制度に関しては、「道路交通法」において規定されている。

1) 免許の申請、試験

「道路交通法」では、免許を受けようとする者は、公安委員会に内閣府令で定める様式の免許申請書を提出し、かつ、当該公安委員会の行う運転免許試験を受けなければならないと定められている(第八十九条)。また、運転免許試験は、

- 自動車等の運転について必要な適性
- 自動車等の運転について必要な技能
- 自動車等の運転について必要な知識

について行われる。ただし、指定自動車教習所の卒業証明書を有するものは運転試験免許を免除される(第九十七条)。

自動車の情報セキュリティに関する事項が「自動車等の運転について必要な知識」として認識されれば、運転免許試験や試験時に行われる講習においてユーザに情報セキュリティ関連の知識を伝えることが可能と想定される。また、試験だけでなく、指定自動車教習所における教習の一環として情報セキュリティに関する実地的な教育を行うことも可能と想定される。特に、自動車利用の初心者に対して確実に情報セキュリティの必要性を認識させる上では重要な機会と考えられる。

ただし、自動車に適用される情報技術や情報セキュリティでの脅威は年々変化するため、運転免許試験を受けた時点の状況に基づいた教育だけでは、すぐに知識が不足すると想定され、定期的なフォローアップが重要と考えられる。

2) 免許証の更新

「道路交通法」では、免許証の有効期間の更新を受けようとする者は更新期間内に公安委員会に更新申請書を提出しなければならない、またその際、公安委員会が行う講習を受けなければならないと定められている。(第百一条)。講習には、

- 自動車の運転に関する講習
- 応急救護処置に関する講習

などが含まれる(第百八条の二)。道路交通法の改正点、ETC、ABS(Antilock Brake System)など新しい技術の紹介なども行われている

運転免許試験から数年経過した自動車の利用者に対して、最新の情報セキュリティに関する知識を与える機会として免許の更新制度は有効と想定される。具体的には、更新時に行われる講習においては、自動車の安全な運転や管理に必要な情報セキュリティの知識を伝えることが考えられる。

ただし、更新される運転免許の有効期間は、違反運転者等でない七十歳未満の運転者については、「(前の運転免許の)満了日等の後のその者の五回目の誕生日から

起算して一月を経過する日」と定められている(第九十二条の二)。すなわち、優良な運転手ほど講習機会の間隔が長くなり、情報セキュリティに関する講習を行うにしても、5年に一度しか受講する機会がないこととなる。

2.2 車検・点検・登録制度

「道路運送車両法²⁵」において規定されている車検・点検・登録制度については、自動車のECU書き換えや改ざんなどの情報セキュリティでの脅威への対策方法の一つとして考えられる。例えば標準的なチェックリストを整備して、定期的な確認作業を行うしくみとして活用することが期待される。ただし現状では、

- ・保安基準や点検項目には自動車の情報セキュリティに関する事項がない
 - ・検査機関や修理工場では情報セキュリティへの対応を行う体制がない
 - ・点検は実施しない場合の罰則がないため、使用者に対する強制力が弱い
- など、課題も多い。以下に、車検・点検・登録制度の概要をまとめる。

1) 自動車検査登録制度(車検)

車検制度はもともと車両の識別と所有を定期的を確認するための検査制度である。「道路運送車両法」では、自動車は国土交通大臣の行う検査を受け、有効な自動車検査証の交付を受けているものでなければ、これを運行の用に供してはならないと定められている(第五十八条)。これにより、自動車の安全確保・公害防止が図られるとともに、個々の自動車の識別が可能となり、所有及び使用の実態が制度的に把握される。

車検の期間は、普通車については3年または2年ごと、貨物自動車は1~2年、営業車は1年ごととなっている。自動車の情報セキュリティにおいても、車検制度を応用することで、定期的に情報セキュリティの対策を行える可能性がある。

2) 自動車の点検および整備

「道路運送車両法」では、自動車の使用者は、点検の時期及び自動車の種別、用途等に応じ国土交通省令「自動車点検基準²⁶」で定める技術上の基準により自動車を点検しなければならないと定められている(第四十八条)。本省令「自動車点検基準」で定められている定期点検項目は、12ヶ月点検が26項目、24ヶ月点検は56項目である。

これらの車検・点検制度は、自動車に対する不正な改造が本人または第三者によって行われていないかなどの情報セキュリティに関するチェックを行う観点では、情報セキ

²⁵ 道路運送車両法 <http://law.e-gov.go.jp/htmldata/S26/S26HO185.html>

²⁶ 自動車点検基準 <http://law.e-gov.go.jp/htmldata/S26/S26F03901000070.html>

セキュリティを含めた電子的な検査を行うためのチェックリストなどを整備し、最低限の確認作業を行うしくみとして活用することが期待される。

ただし現状では、後述のように保安基準には自動車の情報セキュリティに関する規定はなく、検査機関や修理工場では具体的に情報セキュリティへの対応を行う状況にないという指摘もあった。

3) 自動車の登録等

「道路運送車両法」では、自動車の所有者に対し、登録を受けていない自動車の「新規登録」、自動車や所有者の氏名・住所等の変更があった場合の「変更登録」、所有者の変更があった場合の新所有者に対する「移転登録」を義務付けている。これらの手続きに関しては、自動車登録ファイルと呼ばれる電子ファイルにより情報処理されており、後述の「自動車リサイクル法」やリース車両などにおいて車検証に所有者を記載しないことができる「登録識別情報制度」などで活用されている。

自動車の移転登録に関しては、手続きを行う際に運輸支局・検査登録事務所などにおいて、自動車本体や車載機などに記録された個人情報の消去の必要性などに関する情報提供を行うことも考えられるが、現状では新たな所有者が 15 日以内に「移転登録」を行うことになっており、旧所有者に情報提供を行う機会がないことが課題である。

2.3 リコール制度

リコール制度は、自動車の情報セキュリティの問題に関し、メーカー自らの対応を効率的、确实迅速に実施する手段として期待され、電子制御系またはソフトウェアに関する不具合をメーカーが対応する場合、重大な事故の発生を防ぐ可能性がある。ただし、現在のように、ユーザに修理工場やディーラ工場へ自動車を持ち込んでもらってリコールを実施することは、メーカーにとっては多大なコスト負担であり、ユーザにとっても手間がかかる。そのため検討会では、自動車のソフトウェアの更新や修正も、ネットワークを介してパソコンのソフトウェアの更新同様の手順で行うしくみが必要との指摘もあった。

なお、製造物責任法(PL法: Product Liability)との違いであるが、PL法が実際に製造物の欠陥により人の生命、身体又は財産に係る被害が生じた場合において、製造業者等の損害賠償の責任について定めることにより被害者の保護を図るという事後対策的な制度であることに対し、本法は事前に必要な改善措置を講じることを目的としている。

2.4 自動車損害賠償責任保険(自賠責保険)

自動車は、自動車損害賠償保障法²⁷によって、自動車は自動車損害賠償責任保険又は自動車損害賠償責任共済の契約が締結されているものでなければ、運行の用に供してはならないと定められている(第5条)。本保険・共済は、交通事故による被害者を救済するため、加害者が負うべき経済的な負担を補てんすることにより、基本的な対人賠償を確保することを目的としている。なお、無保険車による事故、ひき逃げ事故の被害者に対しては、政府保障事業によって、救済が図られている。

自動車保険は、自賠責保険と任意保険が一体になってリスクを補償しているのが実態である。情報セキュリティの被害による補償に関しては現在、特に対応が見当たらないが、将来的には何らかの補償が必要になる場合に、任意保険で補償される可能性がある。

2.5 自動車リサイクル法

自動車リサイクル法²⁸(使用済自動車の再資源化等に関する法律)は、車両を廃棄処分する方法に関して定めた法律である。情報セキュリティの面からは、車両の廃棄フェーズでの手順の整理が問題になる。

自動車リサイクルの各段階においては、環境対策のみならず情報セキュリティに関しても安全・安心な処理をあわせて規定することが考えられる。現時点では最終所有者から廃車を引き取る引取り業者が、廃車となる自動車内のプライバシー情報の消去を行うなどの対応が考えられる。

本法の趣旨では、ゴミを減らし、資源を無駄遣いしないリサイクル型社会を作るために、自動車のリサイクルについて自動車の所有者、関連事業者、自動車メーカー・輸入業者の役割を定めており、各者の役割は表 2-1 のようになっている。

²⁷ 自動車損害賠償保障法 <http://law.e-gov.go.jp/htldata/S30/S30HO097.html>

²⁸ 自動車リサイクル法・経済産業省 http://www.meti.go.jp/policy/automobile_recycle/

表 2-1 自動車のリサイクルにおける役割分担

種別	役割
クルマの所有者 (最終所有者)	リサイクル料金の支払い、自治体に登録された引取業者への廃車の引渡し。
引取業者	最終所有者から廃車を引き取り、フロン類回収業者または解体業者に引き渡す。
フロン類回収業者	フロン類を基準に従って適正に回収し、自動車メーカー・輸入業者に引き渡す
解体業者	廃車を基準に従って適正に解体し、エアバッグ類を回収し、自動車メーカー・輸入業者に引き渡す。
破砕業者	解体自動車(廃車ガラ)の破砕(プレス・せん断処理、シュレツディング)を基準に従って適正に行い、シュレツダーダスト(クルマの解体・破砕後に残る老廃物)を自動車メーカー・輸入業者へ引き渡す。
自動車メーカー・輸入業者	自ら製造または輸入した車が廃車された場合、その自動車から発生するシュレツダーダスト、エアバッグ類、フロン類を引き取り、リサイクル等を行う。

(出典: 経済産業省「自動車リサイクル法ホームページ」より²⁹⁾)

2.6 ヒアリング結果: 自動車事故対策機構

自動車事故対策機構としては、すべての活動に法的裏づけが必要なため、情報セキュリティについても、保安基準に入らないと対応ができない、との意見があった。

ただし、自動車の分野は、事故後の原因調査やリコールなどの具体的な再発防止のための対応が行われる数少ない分野のひとつだ、という指摘もあった。その意味では、情報セキュリティの対策がしやすい面がある。

ただし、自動車の電子制御機能については、メーカーの責任の有無や範囲があいまいになっており、情報セキュリティも含めて、何らかの整理が必要だと見られる。

²⁹ 自動車リサイクル法ホームページ
http://www.meti.go.jp/policy/automobile_recycle/

2.7 ヒアリング結果: 日本自動車整備振興会連合会(日整連)

日整連は日常の自動車メンテナンスを行う、全国の整備工場の連合会である。現状としては、自動車の情報セキュリティの問題は認識しているが、整備工場の現状としては、情報システム自体に明るくない状況があるとのことである。

日整連としての今後の見通しについては、整備を電子的に行うための OBD-II の診断機能の開示を、各メーカーから進めてもらう必要性と、整備士の情報セキュリティに関連する資格制度の必要性が触れられた。

現在、日整連では国土交通省が主催する「安全 OBD 検討会」に参加して、整備工場業界からの意見を具申している。安全 OBD 検討会の活動成果については今後、整備業界と自動車開発に係る業界の間でも情報を共有する必要がある。

整備工場や整備士は自動車の情報セキュリティの維持や推進のために欠かせない存在である。また、預かった自動車に対する不正な改造などの脅威を防ぐことも重要であり、今後も重要な役割を担うと考えられる。

3. 他分野での情報セキュリティ対策の動向

SCADA のオープン化の動向による脅威の検討は、自動車の情報化の動向と構図が似ており、自動車の情報セキュリティ対策の参考になる。また、情報技術分野の事例である Microsoft のセキュリティ開発ライフサイクルの取組みは、今後の自動車の情報セキュリティにおいても参考となると考えられ、欧州の SeVeCom や EVITA でのモデル化された脅威の検討手順を採用している点で類似性が見られる。

3.1 上水道分野用の SCADA セキュリティ グッド・プラクティス

SCADA は、生産工程やインフラ設備を対象とした産業制御システムの一つで、製造ラインや社会インフラシステムで広く利用されている。社会インフラには電気・ガス・水道などの重要インフラも含まれている。また、SCADA は組込み機器で構成されるため、自動車の情報セキュリティにも関連がある。

従来の重要インフラ向けの SCADA は専用のシステムで構成されていたが、近年はコストダウンや多様なサービスの効率化のため、標準プロトコルや汎用製品を利用し、他の情報システムと接続することもある。そのため、重要インフラ向けの SCADA でも、情報システムと同様に、脆弱性を狙った攻撃やウイルス感染などのリスクが高まっている。

ここでは、上水道分野用の SCADA のセキュリティ水準向上のため、オランダ政府と TNO Defence, Security and Safety 社が調査報告した「上水道分野用の SCADA セキュリティ グッド・プラクティス」日本語版³⁰を他分野の情報セキュリティの対策動向の例としてとりあげた。

上水道分野用の SCADA セキュリティ グッド・プラクティスでは、経営者向けに 11 個、技術者向けに 28 個、合計 39 項目の対策項目をあげている。内容としては、一般的な情報セキュリティの対策に対して、SCADA 特有の注意点を追加した構成になっている。

特に、SCADA システムと OA(Office Automation)環境やインターネットを分離して、分離ポイントを定期的に検証するなどの、SCADA システム用のネットワークの分離について注意が求められている。

この事例から、検討会では次のような指摘があった。自動車は閉じられた組込みシステムであるためソフトウェア改ざんされる余地がないと考えられがちであるが、実際には汎用チップは表面を見れば仕様分かるものもあり、書き換えも可能になっている。また

³⁰ IPA セキュリティセンター「上水道分野用の SCADA セキュリティ グッド・プラクティス」
<http://www.ipa.go.jp/security/fy21/reports/scada/>

万一、この事例で懸念されているように自動車内の情報システムに何かの方法で侵入されて ECU が書き換えられると極めて危険であること、などである。

3.2 マイクロソフト社のセキュリティ開発ライフサイクルの取組み

自動車の分野に進出しつつあるマイクロソフト社のこれまでの情報セキュリティに関する取組みは自動車の開発にも参考になると考えられ、本検討会で紹介された。

3.2.1 事後対策だけでは対応できなくなったウイルス大量感染

マイクロソフト社では、インターネットに対応した Windows コンピュータへのウイルスの大量感染を機に、自社ソフトウェア製品の脆弱性を解消し、「信頼できるコンピューティングの提供」を新たな目標に設定した。当時の被害は、CodeRed、Nimda などのウイルスに感染した Windows コンピュータがあまりに多かったため、企業の情報システムや通信事業者などの基盤サービスさえもが停止状態に陥り、事後対策だけでは対応できなくなっていた。

3.2.2 セキュリティ開発ライフサイクル(SDL)の採用

マイクロソフト社では「セキュリティ開発ライフサイクル(SDL: Security Development Lifecycle³¹)」を採用し、ソフトウェア製品に含まれる脆弱性を削減することに取り組んだ。SDL では設計と開発の手順内に、セキュリティチームを配置したり、開発者のセキュリティ教育や資格検査などをとりこんでいる。また、ソフトウェアの構成として、複数のソフトウェアスタック層でセキュリティとプライバシーの対策を行う方針となっている。

3.2.3 経営者と開発関係者との連携の必要性

今後、ソフトウェア製品に含まれる脆弱性を減らすだけでなく、どのようなリスクをどのように管理・軽減するかということが重要になっていく。攻撃者の側から見るとすべて情報には価値があり、メッセージ、利用履歴、識別情報などすべてが攻撃対象になると捉えられている。また、攻撃者のためのソフトウェアや情報が売買される市場もある。そのような状況の中で、外部からの攻撃に対処するための情報セキュリティを実現するには、経営者の関与もしくは開発関係者の意識づけだけでは不十分で、製品を開発する経営者や社員すべてが密接に連携する必要がある、と締めくくられた。

³¹ Microsoft セキュリティ開発ライフサイクルの概要
<http://msdn.microsoft.com/ja-jp/library/ms995349.aspx>

4. 自動車業界への情報セキュリティの啓発に向けて

調査の結果、欧州では体系的な脅威の分析やセキュリティ仕様の検討などがあり、自動車の情報セキュリティへの取組みが進められていた。これに対し、日本では本格的な動きが見られない現状にある。それを解決するため、日本での自動車業界への情報セキュリティの啓発に向けて、以下の点について検討や対策が必要だと考えられる。

1. 自動車の情報セキュリティでの脅威が高まりつつある現状の認知度向上
2. 製品のライフサイクル全体での情報セキュリティ対策
3. 整備、車検などアフタマーケットでの情報セキュリティ対策の体制づくり

4.1 自動車の情報セキュリティでの脅威が高まりつつある状況

4.1.1 自動車情報システムの部品・ソフトウェアの共通化による脅威増大

自動車の車載コンピュータである ECU の数は 50 個から 70 個、高級車やハイブリッド車では 100 個以上にのぼり³²、今後登場する新たな自動車の機能の多くがソフトウェアで実現されると言われている。

こうしたソフトウェアを中心にしたさまざまな機能開発が行われる中、多数の機能を短期間で搭載して市場に送り出すために、共通化された汎用 CPU(Central Processing Unit)や部品・ソフトウェアが利用されるようになっている。例えば、車載用の通信バスは CAN(Controller Area Network)、LIN(Local Interconnect Network)、FlexRay などの標準手順に集約され、JasPar のように特に FlexRay の詳細な利用方法を標準化する活動もある。また、JasPar では日本の自動車メーカー 4 社と共同で自動車の電子制御用の基本ソフトを開発した³³。

技術革新やグローバル化をきっかけとして自動車情報システムの部品とソフトウェアの共通化が進んでいる。これらは、自動車産業の発展を支える重要な要素でもあり、この傾向を止めることはできない。

一方、いままでは自動車の情報システムやソフトウェアは専用システムとして開発されており、仕様や設計情報が得にくく、ハードウェアも独自製品であったため、外部からの

³² Oguma, H. Yoshioka, A. Nishikawa, M. Shigetomi, R. Otsuka, A. Imai, H., "New Attestation Based Security Architecture for In-Vehicle Communication", IEEE GLOBECOM 2008, NS04T1-2, 2008.

http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?isnumber=4697775&arnumber=4698144&count=1091&index=363

³³ 経済産業省・自動車向け共通基盤ソフトウェア開発事業の成果発表会及びロビー展示について - <http://www.meti.go.jp/press/20100129002/20100129002.html>

攻撃も非常に難しかった。しかし、ソフトウェアの共通化や汎用ハードウェアの利用により、攻撃者はますます容易に攻撃ができるようになっていく。

こうした共通化によりECUにアクセスする無料のソフトウェアが配布されたり、ECUに物理的にアクセスすることが容易になりつつある状況について例を示す。

1) ECU 書換ツールによる脅威の例 OpenECU.org の EcuFlash

OpenECU.org³⁴では、EcuFlash という ECU 書換ツールとソースコードを無料で配布している。EcuFlash に対応している車種は一部ではあるが、自動車の整備点検用の標準的な車載インターフェースである OBD-II インターフェースを通じて ECU の一部を書き換え、燃料噴射のタイミングを調整できるなどの機能がある。

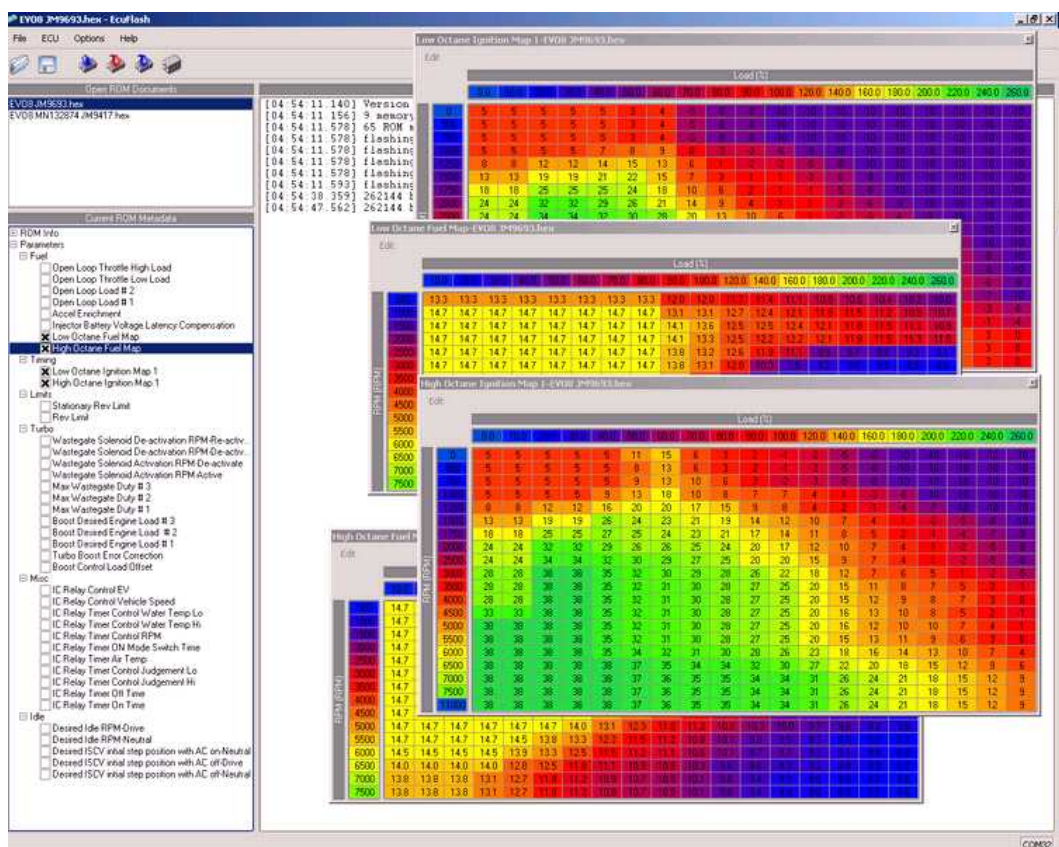


図 4-1 OpenECU.org の EcuFlash 画面例

EcuFlash のような ECU 書換ツールは、自動車の制御がソフトウェア化されることで、制御の変更が容易になる例と考えられる。このようなソフトウェアによって、自動車のソフトウェアを入れ替えることで自動車の機能の改良を簡単に行ったり、地域や異なる利用

³⁴ OpenECU.org – <http://openecu.org/>

方法に柔軟に対応したりすることもできる。その反面、悪意ある攻撃者がこのようなツールを利用することで悪意ある改ざんが行われ、攻撃を許すことにもつながる。

2) 車載 ECU の汎用チップ化と攻撃の容易化による脅威の例

図 4-2 はインターネット用のルータ機器の基板上に実装されている汎用チップにアクセスする例である³⁵。ここで言う汎用チップとは、他業界や他のメーカーでも利用されている CPU やチップ製品のことを指す。こうした汎用チップは、さまざまな用途に短期間で利用できるよう、開発や試験のための共通機能が搭載されており、仕様が公開されているのが特徴である。

チップの型番を特定することで、開発者向けの説明資料を入手できる。すると、JTAG (Joint Test Action Group) やシリアルポートなどの、開発者用または特権モードでアクセスできるポートのピンを特定できることがある。

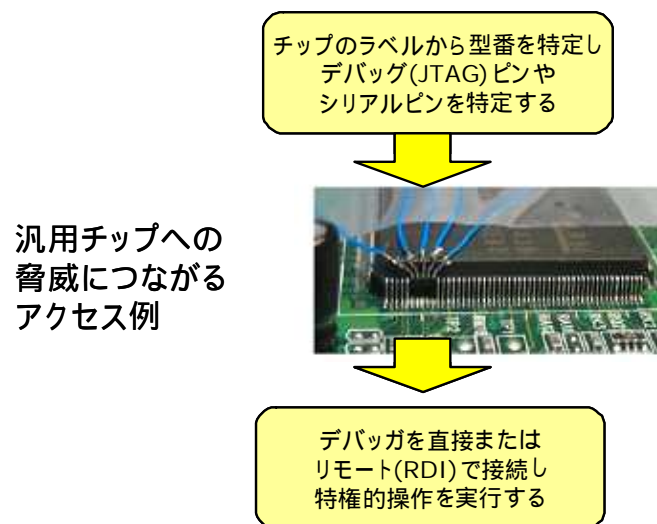


図 4-2 インターネット用ルータ機器の汎用チップへの脅威につながるアクセス例

こうして特権的に利用できるピンを特定したあと、そのピンに結線することで、CPU へのソフトウェアの投入や試験を行うためのデバッガやリモートコンソールなどにアクセスすることができるようになる。

自動車の情報システムにおいても、組込み用の汎用チップが利用される場面はますます増えているものと考えられる。特に電気自動車のように車載チップが高温にならないような環境では、より一般的な汎用チップが利用されることになり、外部から ECU などへのアクセスがますます容易になると考えられる。

³⁵ 汎用チップにアクセスする例: 「組込みシステムのセキュリティ」 より引用
http://www.fourteenforty.jp/research/research_papers/Embedded.pdf

3) ECU 書き換えにより自動車の安全を損なわせる脅威の例

以上のように、自動車内部の電子部品やソフトウェアの共通化により、自動車内部の電子部品や情報システムにアクセスすることが、コスト的にも手順的にも簡単になってきている。そのため、車載 ECU がメーカー以外の第三者によって不正に書き換えられることによって、その自動車に予期せぬ動作が発生するなど、安全性が損なわれる脅威が想定される。この場合、結果として自動車の暴走や衝突など、重大な事故につながる危険性も想定される。

4) メーカー純正の ECU 書換ツールも含めたツール悪用による脅威の例

自動車の電子化、ソフトウェア化により、自動車の整備点検にもソフトウェア・ツールが欠かせない状況となっている。このため、自動車の保守点検ツールとして、一部の自動車メーカーでは整備点検用の専用ソフトウェアを販売・配布している。また、サードパーティによる整備点検ソフトウェアや器具も販売されている。

一般ユーザが入手できるソフトウェアでは、機能的な制限のために操作できないような ECU 書き換えも、ディーラ工場などで利用されるメーカー純正の ECU 書換ツールでは、より広範囲に操作が可能である。例えば、不具合がある ECU ソフトウェアを修正することで自動車の安全性を向上させることができる一方で、ECU 書換ツールが誤って利用された場合や悪用された場合に発生する被害はより深刻な影響があると考えられる。例えば安全上の問題が残っているソフトウェアを誤って車載 ECU に投入してしまったり、ツールを悪用することにより予期せぬ動作を起こさせることなどが想定される。

4.1.2 ITS でネットワーク接続する自動車への脅威

自動車も、その他の組込み機器と同様に、インターネットや自動車の外部のネットワークに接続して、新たな利便性、安全性を提供する必要にせまられている。例えば、ITS の分野では、他の自動車との通信(C2C)やデータを集約したサーバなどとの通信(C2I)によって、他の自動車と接近情報を交換し、渋滞情報、緊急情報を交換しようとしている。

次の図 4-3 は、C2C-CC(Car-to-Car Communication Consortium)³⁶で想定された、Car2X のネットワーク・アーキテクチャの図³⁷である。Car2X では車車間通信と路車間通信の両方をまとめて検討しているため、自動車の外部のネットワークも含めて整理されている。

一方で、自動車がネットワークに接続することにより、自動車の情報セキュリティでの脅威は大きく増大する。一つには、ネットワーク接続によることで、攻撃者は遠隔地や離れた場所

³⁶ C2C-CC: Car-to-Car Communication Consortium, <http://www.car-to-car.org/>

³⁷ “C2C-CC Manifesto, Version 1.0”, July 2007

http://www.car-to-car.org/fileadmin/downloads/C2C-CC_manifesto_v1.1.pdf

からでも自動車に対して攻撃が可能になり、移動中の自動車にさえも攻撃の機会が得られるようになる。

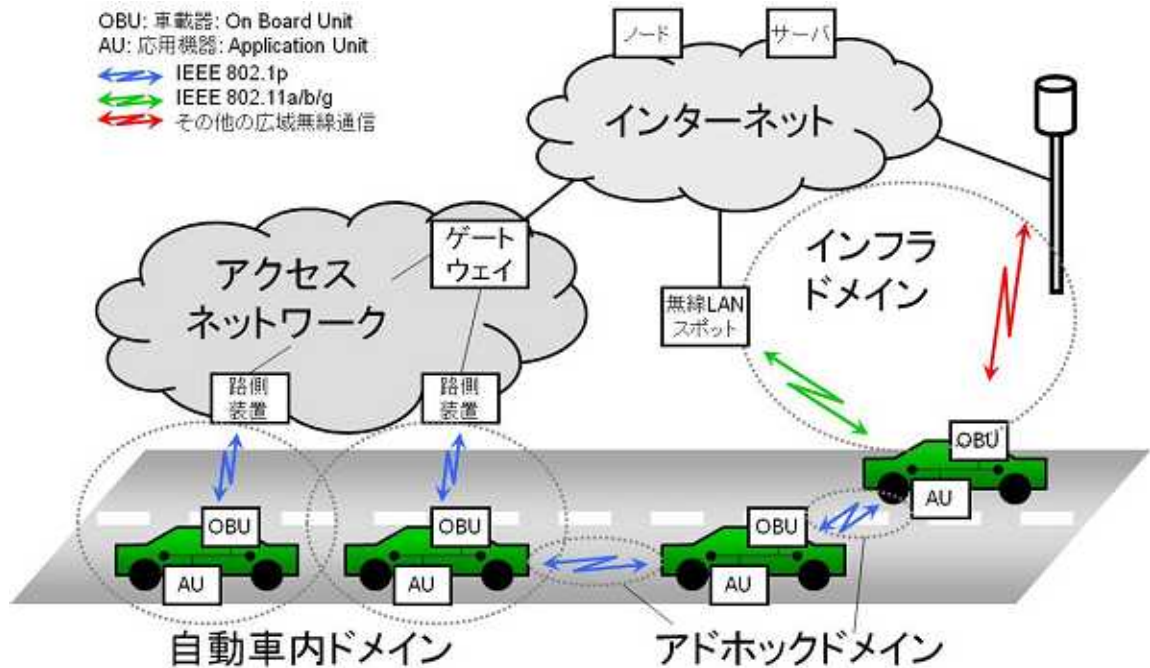


図 4-3 Car2X のネットワーク・アーキテクチャ

「図 4-4 ニセの急ブレーキ情報による自動車の安全への脅威の例」は EVITA の「認められていないブレーキ操作」に登場するシナリオの一例である。ここでは、白い被害者の自動車の前方を攻撃者の自動車が行っている。その状態で、攻撃者は車車間通信や路車間通信を利用して、後続の被害者の自動車にニセの急ブレーキ情報を送ると、後続の被害者の自動車は前方の危険回避のために自動的に急ブレーキを動作させる可能性が高い。その結果、後続の自動車の運転者は急ブレーキによって自動車内で負傷する事故などの可能性が考えられる。

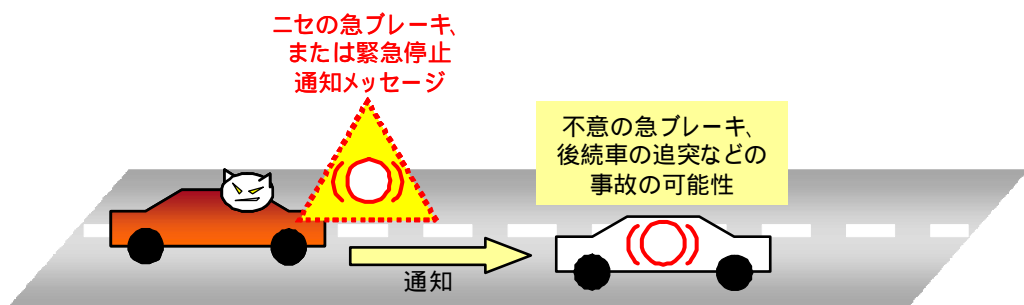


図 4-4 ニセの急ブレーキ情報による自動車の安全への脅威の例

EVITA のリスク分析によれば、「認められていないブレーキ操作」については、安全への深刻度が最高レベルの 4 で、複数の自動車に対して生命の危険または傷害のおそれがあるとしている(EVITA D2.3、C1.2 Notion of severity、C2.5 Unauthorized Brake より)。

また、IP(Internet Protocol)ネットワークや無線ネットワークなどのように共通化または標準化された通信手段を利用する環境では、ECU やハードウェアへのアクセス方法に比べてはるかに容易に攻撃する方法が得られる。

欧州の自動車セキュリティの動向では、ITS 利用時の情報セキュリティについては、ITS はまだこれからのアプリケーションという見方から、緊急性が乏しいようにも見られた。しかし日本では ITS の部分的な導入が 2010 年から始められようとしており、現実の問題として検討が必要だと考えられる。

4.2 製品のライフサイクル全体での情報セキュリティ対策

4.2.1 広範囲にわたる影響と安全(Safety)にもかかわる影響

表 4-1 EVITA でまとめられた攻撃対象と保護対象

一般的な情報セキュリティでの脅威				保護対象
攻撃のねらい	攻撃対象	攻撃手法	攻撃の動機	
個人への危害	運転者または同乗者	特定自動車の安全機能への干渉	犯罪またはテロ行為	安全 プライバシー
集団への危害	自動車または交通を通じての都市または国家経済	多数の自動車または交通の管理システムの安全機能への干渉		安全 操作性
個人的な利益	運転者または同乗者	自動車情報と運転者情報の窃盗、自動車の窃盗、商取引詐欺	ハッカーの名声獲得 (ハッカーツールの宣伝)	プライバシー 財産
	自動車	自動車機能の操作への干渉		操作性 プライバシー 財産
	交通システム、自動車ネットワーク、課金システム	交通管理システムまたは課金システムへの干渉	通行特権の拡大、料金不払い	操作性 プライバシー 財産
組織的な利益	運転者または同乗者	交通事故責任または運転者と自動車の追尾責任の放棄	詐欺、犯罪またはテロ行為、状態監視	プライバシー 財産
	自動車	自動車機能の操作への干渉、自動車設計情報の入手	産業スパイまたは妨害行為	プライバシー 操作性 安全

上の表 4-1 は、EVITA でまとめられた Car2X の情報セキュリティにおける攻撃の影響

響範囲と保護の対象を整理したものである³⁸。情報セキュリティと安全を切り離せないと考えられる部分を、黄色で示した。

また、表の左側では、組織的な利益や集団への危害も想定に含まれており、対象には交通管制システムや料金収受システムなど、社会的な影響もあると考えられている。こうした広範囲におよぶ影響を持つ情報セキュリティにおいては、被害が発生してから対処するのでは遅すぎることになる。そのためには、製品のライフサイクルの中で上位レベルでの対策が必要と考えられている。

4.2.2 ソフトウェア開発ライフサイクルとソフトウェア修正コスト

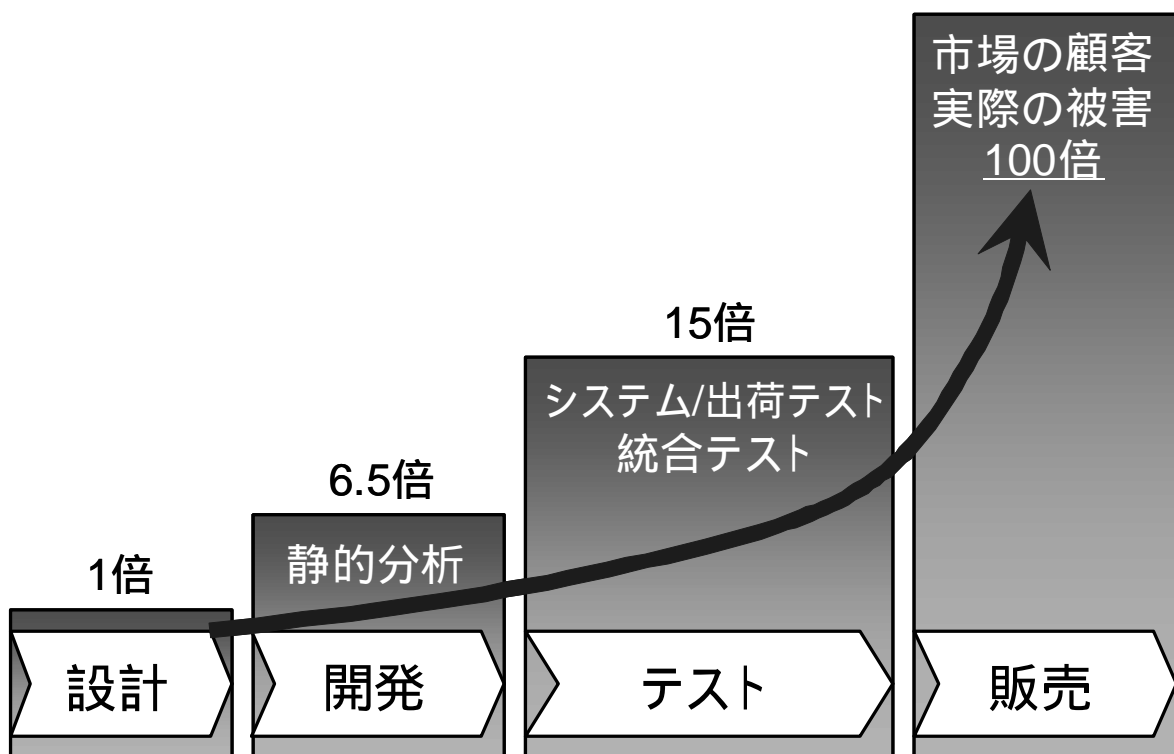


図 4-5 ソフトウェア開発ライフサイクルを通じたソフトウェアの欠陥修正コスト

図 4-5 はソフトウェア開発ライフサイクル(SDLC: Software Development Life Cycle³⁹)の各工程での、ソフトウェアの欠陥を修正するためのコストを比較した図⁴⁰である。最初の企画を含む設計段階では、ソフトウェアの欠陥を修正する作業は企画内容や設計書類の修正などのように、設計作業と同じコストで済む。しかし、開発やテストの

³⁸ Car2X の情報セキュリティにおける攻撃の影響範囲と保護の対象

EVITA D2.3, P.11, Table 1 “Generic security threats and security objectives”より引用

³⁹ SDLC: Microsoft では Security Development Lifecycle を”SDL”と表記している。

⁴⁰ SDLC を通じたソフトウェアの欠陥修正コスト: 「ファジング~ブルートフォースによる脆弱性発見手法」Micheal Sutton ほか著、園田道夫監訳、毎日コミュニケーションズ、2008 年、P.480 より引用

段階に進むと、成果物がソースコードや実行ファイルのような形に変換されるため、欠陥の修正コストは開発で 6.5 倍、テスト段階で 15 倍に膨らむ。さらに、出荷後の販売時点で欠陥を修正しようとする、実際に被害が起こることも含め、修正コストは 100 倍あるいはそれ以上になってしまう。

このように、工程が進むほど、ソフトウェアの脆弱性の修正コストは高まるため、情報セキュリティの対策についても、同じように工程の初期段階から脆弱性を削減する必要がある。

4.2.3 IEC 61508 機能安全と情報セキュリティ対策

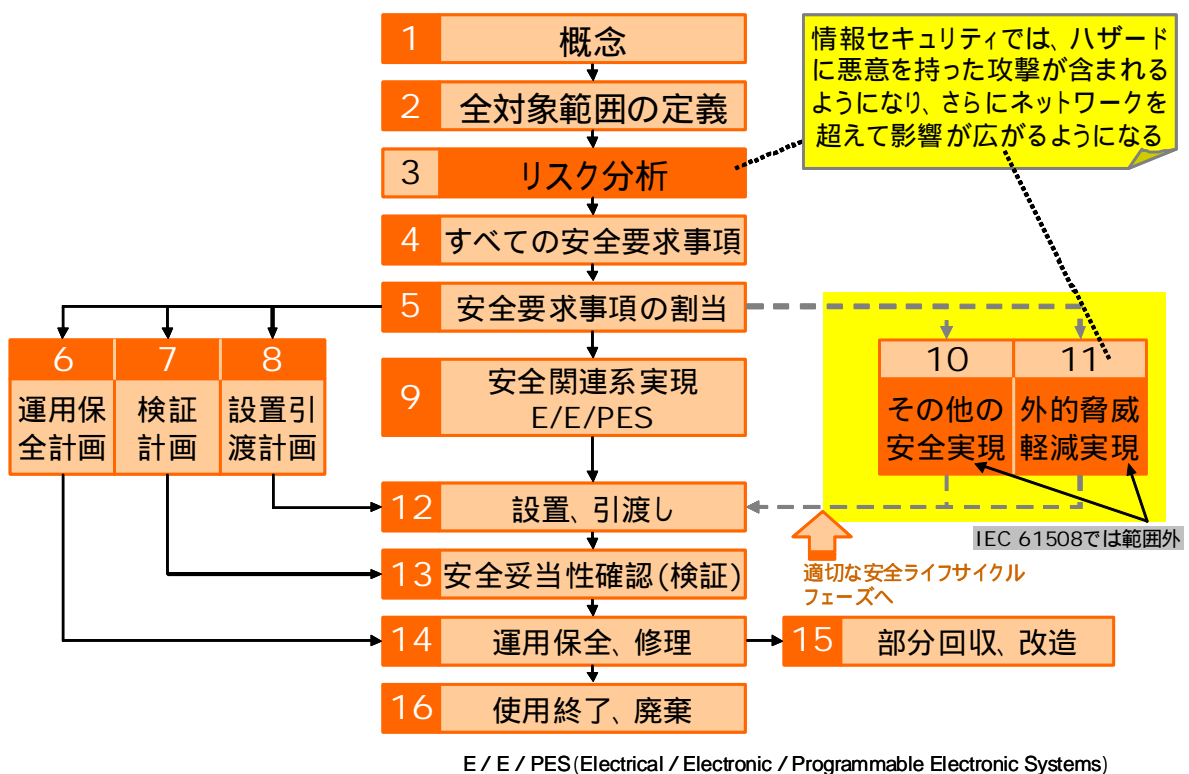


図 4-6 IEC 61508 機能安全における製品のライフサイクル

図 4-6 は IEC 61508 機能安全における製品のライフサイクルを示している⁴¹。IEC 61508 は製品自体が故障または破損した場合でも安全が保てるよう考えられた機能安全のための標準であり、悪意を持った外部からの攻撃に対しては、現状では検討の対象外となっている。

しかし現在の自動車の開発工程の中で情報セキュリティへの対応を行う場合、このような製品のライフサイクルの中に、機能安全の担保をベースとしながら、情報セキュリティ

⁴¹ エムエスツデー 2007 年 12 月号「機能安全と IEC 規格 61508 について (1)」より <http://www.m-system.co.jp/mstoday/plan/mame/2006-2007/0712/>

を取り入れていく必要がある。

自動車の製品のライフサイクルにおいて、情報セキュリティへの対応や検討が行われるようになると、図 4-6 の「10-その他の安全実現」や、「11-外的脅威の軽減の実現」のステップを実行することで、情報セキュリティの対策が可能になると期待される。また自動車の情報セキュリティに対応していくためには、「3-リスク分析」のステップが重要である。情報セキュリティに対応したリスク分析を行うと、検討対象となるハザード(潜在危険)について、悪意を持った外的脅威に関する検討項目が増えることになる。また、ハザードの影響はネットワークを経由することで広範囲に渡ることが懸念される。

なお、機能安全のための IEC 61508 標準は、開発プロセスの中での安全を担保する手順を標準化している。現状では情報セキュリティは対象としていないが、関係者によれば、新しい版では脆弱性分析などのセキュリティ対策の必要性に触れられる見込みである。また、IEC 61508 の自動車版と言われる ISO 26262 でも同様の動きが見られるのではないかと考えられる。

4.2.4 「組込みシステムのセキュリティへの取組みガイド」

IPA では 2009 年 6 月に、開発者向けの「組込みシステムのセキュリティへの取組みガイド⁴²」を公開している。

この資料では、組込みシステムのライフサイクルを「企画」、「開発」、「運用」、「廃棄」の 4 つのフェーズに分けると共に、組織としてライフサイクルを確実に実施するための重要な要素を「マネジメント」フェーズとして、それぞれについて説明している。

対象とする分野はインターネットに接続されるような情報家電が中心であるが、自動車の情報機器にも適用可能と考えられ、現状の参考資料として有用である。

4.3 整備、車検などアフタ市場での情報セキュリティ対策

本検討会では、自動車の利用と整備、車検などのアフタ市場における情報セキュリティについても、制度や関連団体からの情報をもとに検討した。

個人情報を含む自動車の処理方法や譲渡方法を含む、プライバシーの保護のための手順の確立などが必要とされた。また、カーシェアリングやレンタカーなどの共有型の自動車の利用形態への配慮も必要性が指摘されている。

制度面では、運転免許制度や車検・点検制度などによる定期的な知識の普及、ソフトウェアの更新タイミングがあることが整理できた。今後は、実際に自動車の情報セキュリティを制度として担保していくために、ソフトウェアの不具合の更新のための保安基準の

⁴² 「組込みシステムのセキュリティへの取組みガイド」IPA、2009 年 6 月
http://www.ipa.go.jp/security/fy20/reports/emb_app/

整備が必要だと指摘された。

また、ソフトウェア化された自動車の診断・点検作業自体が、OBD-II などを利用して、効率化されることが期待されている点も指摘された。また、ソフトウェア面での点検や整備を行うためには、整備士の資格制度や認定を行うことで、整備士の信頼を確立する必要があるとされた。

5. 自動車の情報セキュリティの推進に向けて

5.1 今回の調査のまとめ

1) 国内外の自動車の情報セキュリティの動向

欧州では、自動車の情報セキュリティに関する取組みが積極的に行われていることが明らかとなった。例えば EVITA プロジェクトでは、2008 年から具体的な攻撃方法と対象を想定した検討を行うとともに、電子化された自動車のアーキテクチャ、機能構造を整理し、共通化・体系化した情報セキュリティに関する基盤的な技術開発が行われている。

これに対し米国では、2010 International CES を見る限り情報通信技術適用による自動車の利便性向上と安全の充実にに関する製品・サービスは進んでいるものの、情報セキュリティへの取組み例は見られない。

日本国内に関しても、IPA や本検討会委員による活動などは把握できているものの、関係省庁や自動車業界などによる情報セキュリティへの取組みは見られない状況である。そのため日本でも、欧州の先行事例などを参考としながら、日本国内の自動車開発関係者が連携して情報セキュリティ対策に取り組む必要がある。

2) 日本国内での制度・教育に関する自動車の情報セキュリティ対策の動向

自動車の情報セキュリティの実現や利用者への意識啓発を図るために、車検制度と整備制度、運転免許制度、自動車のリサイクル制度について、自動車の利用者に対する定期的な周知や整備を促す機会があることを確認した。このことから、将来的に車検・点検時に情報セキュリティに関する検査や更新を実施したり、運転免許証更新に利用者に対して自動車における脅威と対策について周知したり、自動車リサイクル法の枠組み内でリサイクル対象機器内の個人情報を実際に確実に消去させる案などが挙げられた。

3) 他分野での情報セキュリティ対策の動向

他分野における情報セキュリティ対策の取組みについて分析を行った。上水道用の SCADA セキュリティ・グッドプラクティスの事例は、自動車のようにすでに利用を開始している組込みシステムに対する脅威を緩和するために参考になるだろう。また、マイクロソフト社のセキュリティ開発ライフサイクルへの取組みは、製品の企画から開発・出荷・保守・運用のすべてを含めた情報セキュリティ対策の参考となると考えられる。

4) 自動車業界への情報セキュリティの啓発の必要性

従来、自動車の制御システムは専用のシステムを利用していたため攻撃の難易度が高かったが、現在の自動車の部品・ソフトウェアは共通化が進んでおり、悪意を持つ第三者が不正な書き換えを行うことが容易になりつつある。その例として ECU 書換ツールなどの情報が一般に流通していることなどが脅威として挙げられた。また、車車間・路車車間通信などの導入などにより、遠隔からの脅威の可能性が増大することも示された。このような状況を放置しておくと、自動車の利用者に多大な被害を与える恐れがあり、対策が必要である。

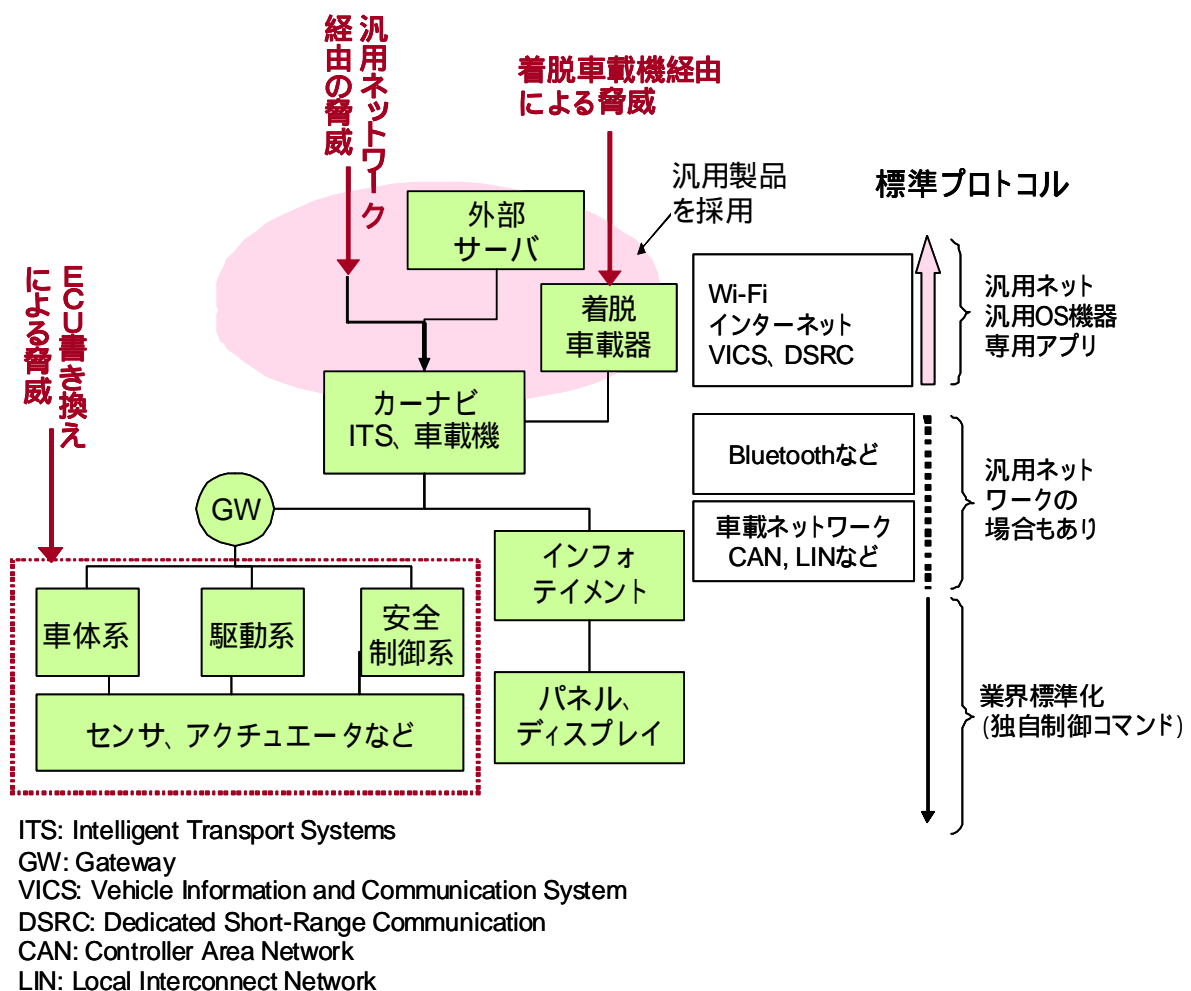


図 5-1 部品・ソフトウェア・ネットワークの共通化、汎用品の採用による脅威の増大

自動車内の情報システムが共通化やネットワーク化により、脅威にされるようになっていくことを示すのが上の図 5-1 である。左下の車載機器は共通化されることで攻撃手法が容易になり、ECU 書き換えの脅威が増大している。また、図の中段、車載ネットワークのゲートウェイ(GW: Gate Way)は自動車の外部のネットワークとの接続点となり、インターネットや携帯電話ネットワーク、公衆無線 LAN などのネットワークからの脅威にさ

らされる。また、図の上部、着脱式の車載機について見ると、例えば USB 等の標準インターフェースを利用する事で、携帯電話やデジタルカメラなどの情報家電機器を自動車内に容易に接続できるようになってきている。その一方で、攻撃者からのウイルスや不正プログラムへの感染等といった脅威にもさらされやすくなる。

このような自動車の情報セキュリティでの脅威の増大に対し、製品化後の対策では、リコールや損害賠償、製品イメージへの打撃など莫大なコストがかかり、現実的ではない。重大事故などの被害を起こさないために、高機能化・ネットワーク化した自動車という製品においても、継続して安全を実現できるような自動車の情報セキュリティの対策を求めるとともに、今回の調査結果のような情報を積極的に発信することが必要である。

5.2 自動車の情報セキュリティの推進に向けて

今回調査を行った欧州については、SeVeCom/EVITA、EASIS の両プロジェクトにそれぞれ約 1 千万ユーロの予算が投じられており、情報セキュリティを含んだ自動車の安全性に対する積極的な取組み姿勢がうかがえる。国内においても、自動車の情報セキュリティに対して積極的な取組みが必要である。自動車における情報セキュリティに起因する事故を未然に防ぎ、日本の自動車が高機能化による付加価値を売りに世界市場をリードしていくためにも、今後自動車の情報セキュリティの推進に向けた方策を提案する。

5.2.1 自動車の情報セキュリティ概念の日本への浸透のために

1) 欧州での先進的な自動車の情報セキュリティの詳細な調査と国内への浸透活動

欧州では、次世代の自動車技術の研究開発と同時に、自動車の情報セキュリティについても、自動車内、自動車の外部の両面や複数の通信経路やインターフェースなどにも配慮しながら検討が進められている。自動車の情報セキュリティは、自動車の部品点数が多く、社会インフラとしての重要性も非常に高いため、対象範囲も非常に広い。そのため日本でも、欧州など海外の活動成果の詳細な調査を行うとともに、自動車だけでなく、情報通信技術や制度など、複数の分野にまたがる発表や交流による情報交換を行い、とりまとめた情報を関係組織に提供することで自動車の情報セキュリティを浸透させていく活動が必要である。

2) 自動車の安全確保の活動への情報セキュリティの追加

日本でも、自動車の安全のための活動として JasPar や ITS 関連の活動があるが、今後は自動車の情報セキュリティについてもあわせて検討する必要がある。また、自動車の安全を実現する ECU の機能と、センサ、アクチュエータなどの制御の中核機能について、多くの情報セキュリティの関係者が情報共有や議論、検討を行える場や体制が必要である。

3) 法令や制度の自動車の情報セキュリティへの対応

自動車の整備や事故対策などの調査においては、保安基準やリコール制度などの

法令や制度において自動車の情報セキュリティへの対応が不足している現状があった。今後は制度における自動車の情報セキュリティへの対応検討も必要だと考えられる。

4) 自動車の新しい利用・市場環境における自動車の情報セキュリティの検討

以下のような自動車の新しい利用方法や・市場環境が想定されている。

- 世界的かつ急速な自動車の低価格化、共通化
- 車車間・路車間通信(Car2X)による効率・安全機能の実現
- 不特定多数による自動車の共用・共有的利用(カーシェアリング)
- セグウェイやホンダ・U3-X、トヨタ i-REAL のような一人乗り化
- スマートグリッド環境での電気自動車を活用した電気エネルギーの融通

このような新しい利用方法の登場によって、自動車の安全への新たな脅威や、プライバシーへの脅威も増大する。今後、こうした自動車の情報セキュリティでの脅威を「予想の範囲内」に収めるための検討が必要である。

5) 既存標準の情報セキュリティへの有効活用と標準化への貢献

自動車の安全を実現するための手法については IEC 61508 や ISO 26262 という標準があり、一般的な製品の情報セキュリティ対策の手法については ISO/IEC 15408 という標準がある。これら既存の標準を自動車の情報セキュリティの実現・推進に活用するため、その役割や有効な活用方法を整理する必要がある。また、これら既存の標準だけでは自動車の情報セキュリティのすべてがカバーされない場合、日本発の国際標準を策定するなどの貢献が期待される。

5.2.2 自動車の情報セキュリティを推進するための今後の活動提案

自動車の情報セキュリティを効果的に推進するためにも、現在の自動車業界のトレンドや情報セキュリティを含めた技術動向の調査検討を行う必要がある。今回の調査検討は情報セキュリティに関する自動車を取り巻く環境を把握するため、日本国内および欧米を中心に幅広く実施した。今後は具体的な情報セキュリティ対策の検討・実施のため、自動車の構造や通信機能の利用方法を含めて、より詳細な調査検討を行うことが必要と考えられる。5.2.1 を効率的に実施していくためにそれぞれの調査検討、提案、体制づくりについての候補を示す。([対応]は、5.2.1 の項目への対応番号を示す)

1) 自動車の情報セキュリティの全体動向調査

自動車の情報セキュリティについてより詳細に調査検討する項目の候補を以下に示す。

情報セキュリティの動向・技術

- 欧州 SeVeCom、EVITA の成果物の評価検討、不足点の洗い出し [対応 1), 2)]
- ECU の情報セキュリティへの対応機能と動向の整理 [対応 1), 2)]
- 電子化されたセンサ、アクチュエータの機能と車載バスの通信方式の整理 [対応 1), 2)]
- OBD-II(ISO 9141-2)の機能整理、「安全 OBD」の動向整理 [対応 1), 2)]
- ドライブレコーダへの CC(Common Criteria), ISO/IEC 15408 適用動向、事後解析のための運転と制御の記録、フォレンジック対策の検討 [対応 3), 4)]
- イギリス HSE (Health and Safety Executive) 安全衛生庁などの事故調査の体制事例調査など [対応 4)]

新たな自動車の利用と交通社会についての調査検討

- カーシェアリングにおける情報セキュリティの検討 [対応 4)]
- 電気自動車とスマートグリッドに関する情報セキュリティの検討 [対応 4)]
- プローブ情報の安全な活用に関する取組み状況の調査など [対応 4)]

今後、広がると懸念される脅威の想定

- ECU 書換ツールやその利用方法の情報の一般への流通状況、書き換え可能な内容と脅威、ECU 書き換え時の認証の有無等 [対応 2)]
- 信頼できない整備工場が自動車が不正改造される脅威など [対応 2)]

2) 自動車の情報セキュリティの推進体制や制度の検討

自動車の情報セキュリティなど、異なる分野の技術者が、情報交換、協調連携により自動車の情報セキュリティを推進していく場を整備するとともに、そこで検討された方策を効率的、効果的に実現していく仕組みの検討が必要である。以下に、検討事項の候補を示す。

自動車の情報セキュリティの推進体制

- 共有可能な自動車の情報セキュリティ対策のための目標設定、要件定義、アーキテクチャ設計など [対応 1), 2)]
- 市場で受け入れられるような低コストで手間がかからない情報セキュリティ対策の実現検討 [対応 1), 2)]

- 自動車分野と情報セキュリティ分野の知識、情報、ノウハウ等の交換が可能な会議、啓発イベント、セミナーの開催 [対応 1), 2)]

既存の制度活用の検討

- 運転免許制度、車検・点検制度を利用した利用者の意識啓発 [対応 3)]
- 車検・点検・リコール制度を利用した脅威の発見や情報セキュリティ対策 [対応 3)]
- 自動車リサイクル法を活用した廃棄車両の個人情報の確実な消去 [対応 3)]
- IPA ソフトウェア等の脆弱性関連情報に関する届出制度の活用 [対応 3)]

3) 自動車の情報セキュリティ関連標準の整理、活用および参加

本調査において取り上げられている標準の活用や標準化団体との連携協力により、自動車の情報セキュリティの実現を推進することが必要と考えられる。ただし、標準は自動車および情報セキュリティの個別分野に分散しているものも多く、それぞれの関係や連携状況も不明である。さらに、既存の標準だけでは、自動車の情報セキュリティが十分にカバーされているとは言いがたい。

こうしたことから、既存の標準の調査および整理を行うとともに、必要に応じて標準化団体と積極的に連携したり、標準のアイデアを提案していくことが重要と考えられる。以下に、自動車の情報セキュリティに関連する標準および標準化団体の候補を示す。

- 機能安全標準(IEC 61508, ISO 26262)の内容と対応方法の整理 [対応 5)]
- 情報セキュリティ標準(ISMS⁴³, ISO/IEC 15408, 18045)と利用方法の整理
品質標準(ISO 9000/9126)から情報セキュリティへの対応方法の整理 [対応 5)]
- システム記述言語等開発ツールによる情報セキュリティへの対応方法の整理 [対応 5)]
- 自動車の情報セキュリティに関連する標準化団体(ISO, IEC, AUTOSAR, JasPar, MISRA, ETSI, CC 認証, IEEE, IETF)の動向調査 [対応 5)]

⁴³ ISMS: Information Security Management System, 情報セキュリティ管理システム

6. 参考資料

6.1 EU の Framework Programme における自動車関連の取組み

EU は、Framework Programme (FP) という雇用の確保と国際競争力の向上に貢献することを目的としたプロジェクトを実施しており、2010 年現在、第 7 期の FP7⁴⁴ (2007 年～2013 年) を実施中である。EU の 27 カ国が加盟しており、総予算は FP7 が実施される 7 年間で約 505 億ユーロである。

FP の採択プロジェクトは、欧州委員会の提案に対して、欧州連合理事会及び欧州議会の審議・承認を経て決定される。ITS 関連の主な採択プロジェクトとしては、「高度自動運転技術」、「低コストな路上障害物センサ」、「二輪車運転支援システム」、「スマートカーゴ」等がある。これらの活動は年度ごとに募集がかけられ、実施される。

本章では FP が支援する自動車情報セキュリティ関連のプロジェクトの動向を調査し、組織・活動ごとにまとめた。以降では、欧州 FP7 の提案募集で採択された、ITS 関連プロジェクト、ICT (情報通信分野) 関連プロジェクトのうち主なものを紹介する。

(JARI 調査報告「自動車研究 第 30 巻 第 10 号」2008 年 10 月より⁴⁵)

プロジェクト名	概要	参加組織
ADOSE (EU FP7) reliable Application specific Detection of road users with vehicle On-board Sensor	2008-2010 年。障害物や歩行者を確実に検知できる、低コストの車載センサ技術の開発。	フィアット中央研究所ほか 13 社機関
EURIDICE (EU FP7) European Inter-Disciplinary research on Intelligent Cargo for Efficient, safe, and environment-friendly logistics	2008-2010 年。荷物の内容や位置、状況などの情報を認識し、ネットワーク接続された「インテリジェントカーゴ」をベースにした物流システムの開発。	IT (Information Technology, 情報技術) 企業であるイタリア INSIEL 社ほか 22 社機関
HAVE-IT (EU FP7) Highly Automated VEHICLES for Intelligent Transport	2008-2011 年。高度な自動運転技術の開発。	Siemens VDO Automotive ほか 19 社機関

⁴⁴ http://cordis.europa.eu/fp7/home_en.html

⁴⁵ JARI 調査報告「自動車研究 第 30 巻 第 10 号」2008 年 10 月

プロジェクト名	概要	参加組織
SAFARIDER (EU FP7) advanced telematics for enhancing the SAFety and comfort motorcycle RIDERs	2008-2010 年。二輪車の運転支援システムや最適な HMI ⁴⁶ 技術の開発。	ギリシャ CERTH 社ほか 21 社機関

次に、欧州 FP7 の提案募集で採択された、ICT(情報通信分野)関連プロジェクトのうち主なものを紹介する。

(JARI 調査報告「自動車研究 第 30 巻 第 10 号」2008 年 10 月より)

プロジェクト名	概要	参加組織
ATESST2 (EU FP7) Advancing Traffic Efficiency and Safety through Software technology 2	2008-2010 年。車載システムのアーキテクチャ記述言語「EAST-ADL2」の開発。 EAST-ADL2 をインフラ協調型のアクティブセーフティシステムの開発に適用させることが目的。	Volvo Technologies 社ほか 10 社機関
Euro F.O.T (EU FP7) Euro Field Operation Tests	2008-2011 年。IVSS (Intelligent Vehicle Safety System) 導入の交通への影響を評価する。IVSS の性能・能力評価、運転者の受容性評価、安全、効率、環境への影響を実データにより評価し、システム導入判断をする。DB は公開される	フォード・アーヘン研究所ほか 24 社機関
EVITA (EU FP7) E-safety Vehicle Intrusion proTected Applications	2008-2011 年。車載システムの無許可な操作の防止、車載システムへの侵入や外部への不正なデータ送出手を防止するための車載システムの機能を、ソフトウェア・ハードウェアモジュールに分割するための定義とセキュリティモジュールの開発	フラウンフォーファー研究所をコーディネータに 11 社参画
INTERSAFE2 (EU FP7) cooperative INTERsection SAFETY 2	2008-2011 年。FP6 の PReVENT の後継プロジェクトで、路車協調型の交差点安全支援システムの開発	IBEO 社ほか 11 社機関

⁴⁶ HMI: Human Machine Interface

プロジェクト名	概要	参加組織
PRECIOSA (EU FP7) PRivacy Enabled Capability In co-Operative systems and Safety Applications	2008-2010 年。通信と蓄積データのプライバシーの観点から協調型システムの評価手法を規定し、プライバシーに配慮した協調型システムのアーキテクチャやガイドラインを規定する。	TRIALOG 社ほか 5 社機関
PRE-DRIVE_C2X (EU FP7) PREparation for DRIVing implementation and Evaluation of C-2-X communication technology	2008-2010 年。欧州共通のインフラ協調型システムの開発。 持込機器の PND を安全運転支援の HMI に位置づけることに賛否両論あり。	ダイムラー社ほか 24 社機関

また、FP6 もしくは FP7 において、ハードウェア面での信頼性確保に関しても、プロジェクトを立ち上げている。そのうち主なものを紹介する。

プロジェクト名	概要	参加組織
OpenTC (EU-FP6) The Open Trusted Computing http://www.OpenTC.net/	2006-2009 年。基本 TC(Trusted Computing)インタフェースと API、仮想化、マイクロカーネル、アプリケーション例、標準化への寄与。	24 組織
TECOM (EU-FP7) Trusted Embedded Computing http://www.tecom-project.eu	2008-2010 年。TC(Trusted Computing)と統合された組み込みハードウェア、統合化チップの CC(Common Criteria)認証、組み込み用のトラステッド OS: 仮想化、マイクロカーネル、セキュリティ例や、アプリケーション。	8 組織
SECRICOM (EU-Security) Secure Crisis Communication http://www.secricom.org	2008-2011 年。TC(Trusted Computing)に対応した最初のプロジェクト。TC は主な作業ではなかったがプロジェクト目標を達成するために TC に対応した。	10 組織
NADA (EU-FP7) Nanodatacenters http://www.nanodatacenters.eu	2008-2011 年。信頼とセキュリティを伴った分散メディアシステム。	10 組織

プロジェクト名	概要	参加組織
EVITA (EU-FP7) http://evita-project.org/	2008-2011 年。車載システムへの侵入や外部への不正なデータ送出を防止するための車載システムの機能をソフトウェア・ハードウェアモジュールに分割して実装するため、セキュリティ仕様を定義しセキュリティモジュールを開発する。	14 組織

FP7の支援するプロジェクトのうち、特に自動車セキュリティに関連が深いプロジェクトについて次ページ以降にまとめた。

EASIS

活動名	EASIS	地域	欧州	活動期間	2004年1月～2007年3月(3年間)
正式名	Electronic Architecture and System Engineering for Integrated Safety (http://www.easis-online.org/wEnglish/download/index.shtml?navid=13)				
主な対象	☑情報セキュリティ ☑プライバシー ☑セーフティ		ライフサイクル	設計・開発	

目標	テーマ
EUの方針「2010年・交通事故半減」のため、自動車内で、個別に運用されている複数の安全システムを統合運用するためのアーキテクチャやプラットフォームを、ソフトウェアとハードウェア両面から構築する	Low-end用、High-end用に分けて検討 自動車内の安全システム統合のためのモジュラ化 信頼できる通信のためのゲートウェイ機能 車車間、路車間通信での盗聴、DoS攻撃、なりすまし発信、プライバシー等の脅威についても対策検討
現在までの成果	現在の活動
<ul style="list-style-type: none"> 要件を定義し、AUTOSARの管理アーキテクチャをベースにFlexRay, CAN, LINと、TCP/IPを統合したアーキテクチャを定義。以下の点を実証 内部、外部のI/Fにルールベースのアクセス制御 インターネット通信にIPSec⁴⁷, SSL/TLSを利用 トランスポートプロトコルレベルでの保護にCTP⁴⁸の利用可能性を実証 モジュラーアーキテクチャの拡張性を実証 	(活動終了)
	予定されている活動
	(活動終了)
	今後の課題
	(特になし)

活動、成果の特徴
ゲートウェイアーキテクチャ、セキュリティマネージャーのコンポーネントダイアグラムを定義し、擬似システムでの実証を行った

取組みに参加している団体	参加団体数	22団体
中核メンバーはダイムラー、BOSCH、ボルボ、フィアット中央研究所、Valeo、ZF ⁴⁹ からなる、欧州の自動車関連メーカー	資金拠出団体	EU FP6
	その他備考	
	総予算: 約9.4百万ユーロ、EU拠出: 約5百万ユーロ	

⁴⁷ IPSec: Security Architecture for Internet Protocol - <http://www.nic.ad.jp/ja/tech/glos-ij.html>

⁴⁸ CTP: Common Transport Protocol - http://www.easis-online.org/wEnglish/img/pdf-files/Paper_Transportprotokoll-zur-domaene-nuebergreifenden-Integration_3v0.pdf

⁴⁹ ZF: ZF Friedrichshafen AG

SeVeCom

活動名	SeVeCom	地域	欧州	活動期間	2006年1月～2009年1月(3年間)
正式名	Secure Vehicle Communication (http://www.sevecom.org/)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	<input checked="" type="checkbox"/> プライバシー	セーフティ	ライフサイクル	設計・開発

目標	テーマ
自動車間の通信を現実的に導入できるようにするため、安全対策を定義する V2V/V2I ⁵⁰ の情報セキュリティの問題に対して、一貫して将来も利用できる解決策を定義する	道路交通の通信に焦点。 ・トラフィック情報メッセージとの関連 ・匿名のセーフティ関連メッセージ ・法的責任に関するメッセージ
現在までの成果	現在の活動
<ul style="list-style-type: none"> ・さまざまな脅威の分析、特定を行っている ・対象システムの用途、シナリオから情報セキュリティのアーキテクチャとメカニズムを定義する、トップダウン式 ・フレームワークとして、COMeSafety の IEEE 1471 Conceptual Framework を利用し、「SeVeCom Baseline Architecture」を定義 ・特定の利用環境に適用できるセキュリティプロトコルの定義。低コストに配慮されている - 鍵と識別情報の管理 - 安全な通信プロトコル、経路制御 - 耐タンパー機器と暗号方式の特定 - プライバシ 	(活動終了)
	予定されている活動
	(活動終了)
	今後の課題
	<ul style="list-style-type: none"> ・後継プロジェクトでの実証実験 ・自動車内侵入検知 ・異常動作検出 ・データの一貫性検出 ・安全な位置情報 ・安全なユーザインターフェース ・今後の姿は、modular,configurable,flexibly など

活動、成果の特徴

脅威分析、アーキテクチャの定義、モジュラー型のメカニズムの定義

車車間、路車間のメッセージには署名付加による、発信元の認証が必要であるとしている。

取組みに参加している団体	参加団体数	7 団体
TRIALOG(進行役), BOSCH, ブタベスト大学, FIAT 中央研究所, ダイムラー社, EPFL (スイス連邦工科大学), リューベン・カトリック大学(ベルギー), ウルム大学(ドイツ)	資金拠出団体	EU FP6
	その他備考	総予算: 約 4.6 百万ユーロ、EU 拠出: 約 3 百万ユーロ

⁵⁰ V2V: Vehicle to Vehicle
V2I: Vehicle to Infrastructure

PRECIOSA

活動名	PRECIOSA	地域	欧州	活動期間	2008年3月～2010年2月(2年間)
正式名	PRivacy Enabled Capability In co-Operative systems and Safety Applications (http://www.preciosa-project.org/)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	<input checked="" type="checkbox"/> プライバシー	セーフティ	ライフサイクル	設計・開発

目標	テーマ
自動車の協調システムが扱う位置情報に基づくプライバシー情報について、将来の個人情報保護規制にも適合できるようにする	<ul style="list-style-type: none"> ・信頼モデルとプライバシーのオントロジー(本体論) ・検証可能な通信アーキテクチャ ・データ格納のプライバシーと検証アーキテクチャ ・プライバシーを検証可能な協調システムのための、検証されたガイドライン
現在までの成果	現在の活動
(成果物はまだない)	特に位置情報と関連したプライバシーの問題を定義中と見られる
	予定されている活動
	今後の課題
	(特になし)

活動、成果の特徴
V2V, V2I を V2X ⁵¹ として一般化し、プライバシー問題そのものの分析から始めている。 データと通信内容の検証についても焦点をあてている(SeVeCom でも指摘されている)。

取組みに参加している団体	参加団体数	5 団体
TRIALOG(進行役), ドイツ・ウルム大学, オラクル, PTV ⁵² , ベルリン・フンボルト大学	資金拠出団体	EU FP7
	その他備考	
	総予算: 約 2.4 百万ユーロ、EU 拠出: 約 1.6 百万ユーロ	

⁵¹ V2X: Vehicle to X -

http://www.preciosa-project.org/index.php?option=com_content&view=article&id=46&Itemid=65

⁵² PTV: Planung Transport Verkehr AG -

http://www.preciosa-project.org/index.php?option=com_content&view=article&id=52&Itemid=61

EVITA

活動名	EVITA	地域	欧州	活動期間	2008年7月～2011年6月(3年間)
正式名	E-Safety Vehicle Intrusion Protected Applications (http://evita-project.org)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	<input checked="" type="checkbox"/> プライバシー	セーフティ	ライフサイクル	設計・開発

目標	テーマ
システム不正使用(tampering)やプライバシーデータ(compromising)を保護するため、車載システムの無許可の操作を防止する。車・車間、路・車間通信による安全性向上機能の基盤技術、アーキテクチャを提供する	車載システムへの侵入や外部への不正なデータ送出手を防止するための車載システムの機能をソフトウェア・ハードウェアモジュールに分割して実装するため、セキュリティ仕様を定義しセキュリティモジュールを開発する。
現在までの成果	現在の活動
<ul style="list-style-type: none"> ・車載ネットワークにおけるセキュリティ脅威分析 ・組み込みオンボードアーキテクチャ設計 ・プロトタイプによる実証実験 	セキュリティのモデル化方法を複数の考え方から評価中
	予定されている活動
	<p>アーキテクチャは信頼の起点として、自動車制御装置の拡張または TPM⁵³のような専用セキュリティ制御チップとして実現されるハードウェアセキュリティモジュールを利用する。車載ネットワークの通信にも安全な手順を利用する。</p> <p>実証試験は UML⁵⁴でモデル化して FPGA で実装、試験する。</p>
	今後の課題 (特になし)

活動、成果の特徴

自動車内には 70 以上の ECU と、さまざまなバス接続があり複雑な分散システムであるとしている。車載ネットワークに対するセキュリティ要件分析を行っている。

取組みに参加している団体	参加団体数	11 団体
フラウンフォーファー研究所(進行役)、BMW 研究所、Continental、escrypt、EURECOM、Fujitsu、Infineon、TRIALOG	資金拠出団体	EU FP7
	その他備考	
	総予算: 約 6 百万ユーロ、EU 拠出: 約 3.8 百万ユーロ	

⁵³ TPM: Trusted Platform Module;

⁵⁴ UML: Unified Modeling Language

Oversee

活動名	Oversee	地域	欧州	活動期間	2010年～2012年(2年間の予定)
正式名	Open VEhicular SEcurE platform (* 2009年9月現在、議論中)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	プライバシー	セーフティ	ライフサイクル	設計・開発

目標	テーマ
独立した複数の V2X(車車間、路車間)アプリケーションを実行するためのプラットフォームの定義。	<ul style="list-style-type: none"> それぞれのアプリケーションの分離・隔離を強固に行う オープンソースのハイパーバイザ(OSの仮想化環境)をベースにする
現在までの成果	現在の活動
(2010年から活動予定)	(2010年から活動予定)
	予定されている活動
	(特になし)
	今後の課題
	(特になし)

活動、成果の特徴

取組みに参加している団体	参加団体数	7団体
escript、Fraunhofer、TRIALOG、ベルリン工科大学、スペイン・バレンシア工科大学、ドイツ Siegen 大学、フォルクスワーゲン * 2010年から活動予定。情報源は SeVeCom: http://www.sevecom.org/Presentations/Various Workshops/Sevecom_2009-09_ResearchPrivacy.pdf	資金拠出団体	未確認
	その他備考	
	総予算: 未確認、EU 拠出: 未確認	

6.2 その他の欧州の自動車関連の取組み

6.2.1 標準化に関わる組織

ETSI TC-ITS

活動名	ETSI TC-ITS	地域	欧州	活動期間	1988年～活動中(21年間)
正式名	European Telecommunications Standards Institute, Technical Committee-ITS (http://portal.etsi.org/)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	<input checked="" type="checkbox"/> プライバシー	セーフティ	ライフサイクル	設計・開発

目標	テーマ
事故数削減と環境負荷削減のため、5.9GHz 帯での V2V/V2I 通信方式を標準化する。2009 年末技術仕様(TS: Technical Specification)化予定。	TC-ITS の WG(Working Group): WG1: 利用者とアプリの要件 WG2: 機能分担、クロスレイヤと Web サービス WG3: トランスポートとネットワーク WG4: メディアと媒体の関係 WG5: セキュリティ
現在までの成果	現在の活動
ITS-WG5 の成果はドラフト文書のみ(メンバ外非公開): セキュリティサービスとアーキテクチャ(2007 年 12 月) 脅威への脆弱性とリスク分析(2008 年 10 月) 複数レイヤ間のトピックス(2009 年 4 月)	セキュリティ仕様、アプリケーションプロトコル仕様 が完了する予定 予定されている活動 テスト仕様の定義 今後の課題 市場導入は 2012-2015 年

活動、成果の特徴

ETSI の標準は原則的に EU 全域に適用され、市場に対する影響力がある

取組みに参加している団体	参加団体数	TC-ITS は 8 団体
TC-ITS 議長:ダイムラー、BMW、ルノー、日立 EU、Q-Free、ESF ⁵⁵ 、NEC EU	資金拠出団体	参加メンバー
ETSI は世界 63 カ国 700 団体以上の情報通信産業の企業、団体からなり、欧州委員会が「欧州標準化団体」と認める組織の一つ。	その他備考	ETSI は欧州での情報通信分野の技術と安全基準の標準化、規格化を行っている(21,000 件以上)

⁵⁵ ESF: <http://www.esf-gmbh.de/>

MISRA

活動名	MISRA	地域	イギリス	活動期間	1998年～活動中(10年以上)
正式名	The Motor Industry Software Reliability Association (http://www.misra.org.uk/)				
主な対象	情報セキュリティ	プライバシー	<input checked="" type="checkbox"/> セーフティ	ライフサイクル	設計・開発

目標	テーマ
自動車用のソフトウェア開発向けに、安全性と信頼性を担保するための C/C++言語による開発の最善の手法を策定する	<ul style="list-style-type: none"> ・ISO 26262 機能安全を実現する ・設計手順に安全性を担保する手法を組み入れる
現在までの成果	現在の活動
<ul style="list-style-type: none"> ・ISO26262 に適合するための開発ガイドライン「MISRA 安全性解析(MISRA-Safety Analysis)」の定義 ・ソフトウェア開発手法として、C言語のプログラミングガイドライン「MISRA-C」を策定 	MISRA-C ガイドラインの更新
	予定されている活動
	<ul style="list-style-type: none"> ・モデルベース開発とコード自動生成のガイドライン ・MISRA C++, C3 ガイドライン
	今後の課題
	(特になし)

活動、成果の特徴

システムと環境のモデリングを行ってから、脅威分析、リスクの評価を行い、実装と確認を行う。
製品保守も含めた、製品のライフサイクル全般に対してガイドラインを設けている。
航空業界の設計方法を自動車業界用に導入している。

取組みに参加している団体	参加団体数	11 団体
AB Automotive Electronics, Bentley, Ford, Jaguar, Land Rover, Lotus Engineering, MIRA, Ricardo UK, TRW, University of Leeds, Visteon Engineering Services	資金拠出団体	英国の自動車メーカー、部品メーカー
	その他備考	

MISRA 参考資料

自動車技術会:テクニカルペーパー TP-01002 (J)、表題・内容:自動車用C言語利用のガイドライン(第2版)

SESSAME WG3 (MISRA-C 研究会):『組込み開発者におくるMISRA-C 組込みプログラミングの高信頼化ガイド』

SESSAME⁵⁶:組込みソフトウェア管理者・技術者育成研究会

⁵⁶ SESSAME: Society of Embedded Software Skill Acquisition for Managers and

AUTOSAR

活動名	AUTOSAR	地域	欧州・ドイツ	活動期間	2003年7月～活動中(6年間)
正式名	Automotive Open System Architecture (http://www.autosar.org/)				
主な対象	情報セキュリティ	プライバシー	<input checked="" type="checkbox"/> セーフティ	ライフサイクル	設計・開発

目標	テーマ
電子技術による革新を性能向上、セーフティ、環境のために活用する。 標準化を行い、実装で差異化する原則とする。 複雑化を管理しながら、将来的にコストを効率化する製品ライフサイクル内でのソフトウェアとハードウェアの交換・更新を容易にする。	・自動車開発用に電子機器とソフトウェアのアーキテクチャを標準化 ・ソフトウェアと通信のモデル記述方法を標準化し、設計を仮想的に検証できる
現在までの成果	現在の活動
SPECIFICATION 3.1 ・ソフトウェアアーキテクチャ ・方法論とテンプレート ・適合テスト ・モデルのアプリケーション I/F ・モデル実行環境(RTE)	AUTOSAR 4.0 のリリース準備(2009年12月) 多数の API 追加があり、テレマティクスとマルチメディアの API と、HMI の API も追加される。
	予定されている活動
	第三期(2010～2012年)はリリース5につながるためのリリース4の拡張 「技術エキスパート」という WP が追加される。
	今後の課題
	(特になし)

活動、成果の特徴

システム上のセキュリティを検討する WP (Work Package) は見当たらない

取組みに参加している団体	参加団体数	約 180 団体
コアメンバーは世界の主要自動車メーカー: BMW、Bosch、Continental、DimlarChrysler、Ford、GM、OPEL、PSA PEUGEOT CTIROEN、TOYOTA、Volkswagen その他主要電子機器メーカー、自動車部品メーカーのほとんどが参加	資金拠出団体	参加メンバー
	その他備考	
	(特になし)	

escar

活動名	escar	地域	ドイツ	活動期間	2003年11月～継続中(6年間)
正式名	Embedded Security in Car Conference (https://www.escar.info/)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	プライバシー	セーフティ	ライフサイクル	設計・開発

目標	テーマ
自動車をITで革新していくときの脅威と対策に関する普及啓蒙	ITセキュリティ、自動車通信のセキュリティ、プライバシー、DRM ⁵⁷ /認証、ソフトウェア更新、EDR ⁵⁸ 、自動車詐欺、道路料金、HIS等自動車のセキュリティ標準
現在までの成果	現在の活動
盗難防止技術もあるが、情報セキュリティについても、自動車のCANなどで扱われるデータセキュリティや認証のための鍵情報の取扱いについて議論されている。 2009年のescarではCar2Xのテーマが比較的多かった。ただし内容はアイデアベースが多く、実用的な検討が不足している面もある。	プログラムの準備と、カンファレンスを年1回開催
	予定されている活動
	毎年11月、ドイツでの開催を予定
	今後の課題
	(特になし)

活動、成果の特徴

特に、ECU上のソフトウェアを守るためのOSセキュリティやTrusted Hardware、プッシュやプルデータを扱うアプリ向けのセキュリティアーキテクチャ、などのトピックが目立つ

取組みに参加している団体	参加団体数	15団体
主催: International School of IT Security AG 協賛: eScript, TUV Rheinland プログラム委員会(2009年): GM, BSI(ドイツ連邦情報セキュリティ局), Bosch, BMW, 欧州委員, DENSO, Daimler, Trialog, Toll Collect, カーネギーメロン大学, Siegen 大学, Audi, フォルクスワーゲン BAST(ドイツ連邦道路交通研究所)	資金拠出団体	参加費(700)
	その他備考	(特になし)

⁵⁷ DRM: Digital Rights Management

⁵⁸ EDR: Event Data Recorders

6.2.2 その他の自動車の情報セキュリティに関する組織

escrypt

活動名	escrypt	地域	ドイツ	活動期間	1999年～活動中(10年間)
正式名	escrypt GmbH (http://www.escrypt.com/)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	<input type="checkbox"/> プライバシー	<input type="checkbox"/> セーフティ	<input type="checkbox"/> ライフサイクル	<input type="checkbox"/> 設計・開発

目標	テーマ
組込みセキュリティのシステムプロバイダ システム設計から製品化までソリューションを提供する	<ul style="list-style-type: none"> ・自動車、鉄道、航空機向け ・スマートカード、RFID(Radio Frequency Identification) ・携帯向けアプリケーション ・ホームネットワーク、コンシューマ機器 ・製造業
現在までの成果	現在の活動
escar の主催	(特になし)
	予定されている活動
	(特になし)
	今後の課題
	(特になし)

活動、成果の特徴
eurobits の事業部門に相当する。

組織を構成する団体	参加団体数	
[一般企業]	資金拠出団体	-
	その他備考	
	(特になし)	

ISITS

活動名	ISITS	地域	ドイツ	活動期間	1999年～活動中(10年間)
正式名	International School of IT Security (https://www.is-its.org/)				
主な対象	<input checked="" type="checkbox"/> 情報セキュリティ	プライバシー	セーフティ	ライフサイクル	設計・開発

目標	テーマ
情報セキュリティ領域における教育	情報セキュリティ関連の修士号取得コースの提供、イベントの開催
現在までの成果	現在の活動
escar の主催	(特になし)
	予定されている活動
	(特になし)
	今後の課題
	(特になし)

活動、成果の特徴

教育訓練、コース、セミナーを提供し、情報セキュリティ知識の普及させ、関連製品や検査業務のビジネスにつなげているものと見られる

組織を構成する団体	参加団体数	-
[一般企業] 主要株主は、TUV Rheinland 社、及び Ultimaco Safeware AG	資金拠出団体	-
	その他備考	
	(特になし)	

6.3 日本における自動車のセーフティに関わる組織

財団法人 日本自動車研究所 (JARI)

活動名	JARI	地域	日本	活動期間	1969年4月～活動中(40年間)
正式名	財団法人 日本自動車研究所 (JARI: Japan Automobile Research Institute) (http://www.jari.or.jp/research-project/research-department/its/)				
主な対象	情報セキュリティ	プライバシー	<input checked="" type="checkbox"/> セーフティ	ライフサイクル	設計・開発
目標	自動車に関する総合的な研究を行う				
	<ul style="list-style-type: none"> ・環境負荷の低減 ・予防安全 ・持続可能な自動車社会 ・燃料電池、電気自動車 ・ITS 				
現在までの成果	現在の活動				
センターレスプローブ情報システムの開発 ITS 通信システムアーキテクチャの規格化 CALM ネットワーキングプロトコル・ダイレクトモード DSRC(非 IP)系の路車間 / 車車間通信における通信の初期化手順などの標準化 系の路車間 / 車車間通信における通信の初期化手順などの標準化 省エネにむけたエネルギーITS (NEDO 事業) 自動運転、隊列走行 「自動車 ITS 分野の技術戦略マップ」(2006年)	<p>個人情報安全性と、運転支援システムの安全性の評価ガイドライン策定の取り組み方針を策定中 (ITSシステムの安全性に係るガイドラインへの取組方針に関する調査研究)</p> <p>予定されている活動</p> <p>「ITS 総合シンポジウム」開催 (2009年11月17-18日、東京・霞ヶ関) など</p> <p>プローブ情報について個人情報保護のガイドライン策定や、セキュリティ技術の研究</p>				
	今後の課題				
	ITS の情報セキュリティ対策の方針策定				

活動、成果の特徴

「自動車 ITS 分野の技術戦略マップ」を含め情報セキュリティについての取組みは見当たらない。この5年計画には、情報セキュリティは含まれていない(ヒアリング)。

組織を構成する団体	参加団体数	-
[財団法人]	資金拠出団体	
	その他備考	
	(特になし)	

一般社団法人 JasPar

活動名	JasPar	地域	日本	活動期間	2004年9月～活動中(5年間)
正式名	一般社団法人 JasPar (Japan Automotive Software Platform and Architecture) (https://www.jaspar.jp/)				
主な対象	情報セキュリティ	プライバシー	<input checked="" type="checkbox"/> セーフティ	ライフサイクル	設計・開発
目標	テーマ				
ECUの開発ではソフトウェア開発が全工数の80%以上を占めることから、ソフトウェアの再利用性とECUの相互接続性の向上を図る	クルマの電子制御ユニット(ECU)のソフトウェア基盤や車内LANインターフェース規格を標準化 車載LANの要素技術,ミドルウェア,ソフトウェア基盤といった非競争領域を,日本メーカー各社で協調して開発中				
現在までの成果	現在の活動				
車載バス仕様である、FlexRay(10Mbps)規格の設計への利用方法、試験方法などを標準化 AUTOSARとの協調関係を確立	活動中のWG: 情報系アーキテクチャ 車載LAN WG AUTOSAR/FlexRay 標準化 WG ソフトウェア WG マイコン WG 国プロ推進 WG				
	予定されている活動				
	機能安全 WG プロセス WG				
	今後の課題 (特になし)				

活動、成果の特徴

個別の仕様書を入手していないが、一般公開情報のレベルでは、情報セキュリティについての取り組みは見当たらない

組織を構成する団体	参加団体数	120 団体
幹事会員: トヨタ自動車, 日産自動車, 豊通エレクトロニクス, 本田技術研究所	資金拠出団体	参加企業の会費
	その他備考	
	代表理事の日産自動車・技術開発本部 IT & ITS 開発部部长・豊増氏は事故ゼロをめざす「Vision Zero」について語っている。 http://ednjapan.rbi-j.com/issue/2008/02/15/123	

ITS 推進協議会

活動名	ITS 推進協議会	地域	日本	活動期間	2006 年～2009 年
正式名	ITS 推進協議会 (http://www.kantei.go.jp/jp/singi/it2/others/its.html)				
主な対象	情報セキュリティ	プライバシー	<input checked="" type="checkbox"/> セーフティ	ライフサイクル	利用・運用

目標	テーマ
世界一安全な道路交通社会の実現と国際標準化 2010 年度から ITS の全国展開を開始する	ITS による安全運転支援システムを政府と民間が協力して実用化し、事故多発地点を中心に全国展開の開始と普及促進を図る。
現在までの成果	現在の活動
ITS の実環境でのデモンストレーションとして、「ITS-SAFETY 2010」を日本各地で開催(2009 年 2 月 25 日～28 日)。輸入車 3 モデルも参加。 対象用途: ・カーナビゲーションシステム ・VICS ⁵⁹ (道路交通情報提供サービス) ・ETC(自動料金支払システム) ・HELPMET(緊急救急システム) ・バスロケーションシステム(バスの現在地やバス停での待ち時間を案内) その他、全国 7 地域での実証実験も行った	(不明)
	予定されている活動
	(不明)
	今後の課題
	(不明)

活動、成果の特徴
情報セキュリティについての取り組みは見当たらない

組織を構成する団体	参加団体数	7 団体 45 社以上
省庁: 内閣官房、警察庁、総務省、経済産業省、国土交通省 民間団体: ITS Japan、日本経済団体連合会 その他、国内 2 輪および 4 輪メーカーおよび車載器メーカーなど民間企業 45 社、一般市民・ユーザー、学識経験者など	資金拠出団体	日本政府
	その他備考	
	(特になし)	

⁵⁹ VICS: Vehicle Information and Communication System

有限責任事業組合 VeLIO

活動名	VeLIO	地域	日本	活動期間	2007年8月～活動中(2年間)
正式名	有限責任事業組合 Vehicle LAN Interoperability & Optimization (http://velio.co.jp/)				
主な対象	情報セキュリティ	プライバシー	<input checked="" type="checkbox"/> セーフティ	ライフサイクル	設計・開発

目標	テーマ
カーエレクトロニクスの高機能・高信頼に対応した、技術適合試験サービスとソリューションを提供する	<ul style="list-style-type: none"> ・車載用エレクトロニクス・コントロール・ユニット (ECU)と車載ネットワークプロトコル等の検査仕様書の作成 ・相互通信保証の検査 ・コンフォーマンス(技術適合試験)サービスを提供
現在までの成果	現在の活動
<ul style="list-style-type: none"> ・LIN/CAN/FlexRay の適合試験 ・ECU テストサービス ・認証コンサルティング 	(特になし)
	予定されている活動
	(特になし)
	今後の課題
(特になし)	

活動、成果の特徴
情報セキュリティについての取り組みは見当たらない

組織を構成する団体	参加団体数	-
[有限責任事業組合]	資金拠出団体	-
トヨタグループで組込みソフトウェアなどを手がける株式会社豊通エレクトロニクスと、組込みソフトウェア分野の株式会社アドバンスド・データ・コントロールズが設立	その他備考	(特になし)

6.4 重要インフラの情報セキュリティ グッド・プラクティス⁶⁰

「上水道分野用の SCADA セキュリティ グッド・プラクティス」は、上水道の監視制御 (SCADA: Supervisory Control and Data Acquisition) システムのセキュリティ対策 (グッド・プラクティス) をまとめたものである。39 のグッド・プラクティスのうち経営者向けが 11 個 (表 6-1)、技術者向けが 28 個 (表 6-2) からなる。

グッド・プラクティスは、一つ一つにグッド・プラクティスとして認められた背景があり、例えば表 6-2 のグッド・プラクティス#12 の場合、以下のような背景がある。

表 6-2 グッド・プラクティス#12 の背景

公共ネットワークや企業のネットワークからの、SCADA システム及びネットワークへのアクセスに対し、幾重にも防御を施すことにより、仮に一つのセキュリティ対策が破られたとしても SCADA システム及びネットワークに自由にアクセスできないようにする。さらにファイアウォール、簡単に確認できるネットワーク接続及びコールバックシステムに加え、個人ごとの認証、パスワードの定期的変更、侵入探知、ウイルス対策やパッチを当てる際のセキュリティポリシー等の対策により、悪意のある攻撃を阻止することができる。これにより攻撃者を容易に発見することができ、侵入されるリスクを低減させることが可能となる。

⁶⁰ 「上水道分野用の SCADA セキュリティ グッド・プラクティス」
<http://www.ipa.go.jp/security/fy21/reports/scada/>

表 6-1 経営者向けグッド・プラクティス

大項目	グッド・プラクティス	欄
企業のセキュリティポリシー	#1 一般的な情報セキュリティポリシーがSCADAセキュリティポリシーと関連づけられているか。	
	#2 「情報セキュリティマネジメントの実践のための規範」及び関連するセキュリティ標準を参照しているか。	
	#3 SCADAセキュリティポリシーが一般的な(情報)セキュリティポリシーの論理的な拡張となっているか。	
	#4 SCADAセキュリティポリシーに物理的セキュリティが含まれているか。	
	#5 職務内容、責任、権限が文書化されているか。	
リスク管理	#6 SCADAのリスクを企業(経営)レベルのリスク管理の一部としているか。	
セキュリティ意識	#7 継続的なセキュリティ意識教育を実施しているか。	
監査	#8 SCADA環境を対象に、少なくとも年一回のEDP監査(訳注:会計システムを対象とする監査)を実施しているか。	
調達ポリシー	#9 調達/契約時に災害条項が含まれているか。	
	#10 セキュリティ要件を調達プロセスに入れているか。	
	#11 保守・作業を行う第三者との契約に、セキュリティ条項が含まれているか。	

表 6-2 開発者向けグッド・プラクティス

大項目	グッド・プラクティス	燃
多層防御	#12 多層防御の原則が実践されているか。	
SCADA環境とOA環境の分離	#13 SCADA環境とOA環境が分離されているか。	
	#14 共有ネットワークの場合、可用性が保証されているか。	
SCADA環境へのセキュアな接続	#15 必要不可欠でない接続は排除されているか。	
	#16 接続が継続的に監視されているか。	
	#17 ファイアウォールは適切に設定・監視がなされている	
	#18 PA環境はインターネットに直接接続していないか。	
	#19 データ送信にインターネットを使用していないか。	
	#20 無線アクセスポイントは存在しないか	
	#21 モデムや外部アクセスに対し厳重な管理がされているか。	
	#22 ネットワーク分離装置とネットワーク接続に関するセキュリティ対策と設定は、定期的に検証されているか。	
SCADAシステム及びネットワーク機器のセキュリティ対策	#23 それぞれのシステム等はセキュリティ対策が強化・最適化されているか。	
	#24 設定は文書化されているか。	
	#25 設定変更プロセスは管理されているか。	
	#26 ウイルス対策ソフトは最新か。	
	#27 パッチの適用ポリシーは有効か。	
SCADA環境のセキュリティ対策	#28 物理的・電子的なアクセスに対する制御がされているか。	
	#29 SCADAネットワークへの接続は認可された機器のみか。	
	#30 厳重に管理されていない状況において、第三者の機器は接続されていないか。	
SCADA環境のパスワードポリシー	#31 初回使用前にデフォルトのパスワードを変更したか。	
	#32 重要パスワードでは、「複雑であること」「関係者外秘であること」「定期的に変更すること」が守られているか。	
	#33 個人パスワードでは、「他人に漏らさないこと」「定期的に変更すること」が守られているか。	
事業継続計画	#34 「情報セキュリティマネジメントの実践のための規範」14章に沿っているか。	
	#35 SCADAシステム及びネットワーク情報を定期的にバックアップしているか。	
	#36 バックアップ媒体は遠隔地において安全に保管しているか。	
	#37 定期的にバックアップの可用性と完全性の検証をしているか。	
	#38 維持管理され、訓練を積んだ事業継続計画があるか。	
情報媒体の管理	#39 有効的な管理と統制的な廃棄が行われているか。	

6.5 制御システムと自動車システムの比較

1) 重要インフラのオープン化状況

IPA が平成 20 年度に実施した「重要インフラの制御システムセキュリティと IT サービス継続に関する調査」(<http://www.ipa.go.jp/security/fy20/reports/ics-sec/>)における「制御システムのオープン化の状況」の図に合わせて自動車システムのオープン化状況を再整理した。重要インフラでは、既存の PLC(Programmable Logic Controller) や DCS(Distributed Control System)などのハードウェアに加えて、汎用的な HMI や EWS(Engineering Work Station)を利用したユーザインターフェースを利用し、より大規模でさまざまな処理を適用できる、サーバを利用するようになった。こうした展開は、市販のワークステーションや PC(Personal Computer)によって実現されており、誰でも入手できる共通化された製品や、他業種でも利用できる汎用品を利用するようになっている(図 6-1 参照)。

2) 自動車の情報システムのオープン化状況

平成 20 年度の自動車情報セキュリティ調査を基に、自動車のシステムのオープン化状況を整理した。重要インフラと同様に、カーナビ、ITS 車載器などの情報機器と、サーバが導入されるようになり、共通化、汎用化された製品が利用されるようになっている。また、自動車の場合は、メモリプレーヤや携帯電話など、着脱式の車載器も利用され、接続手順や通信手順が標準化、公開されて、オープン化が進んでいることがわかる(図 6-2 参照)。

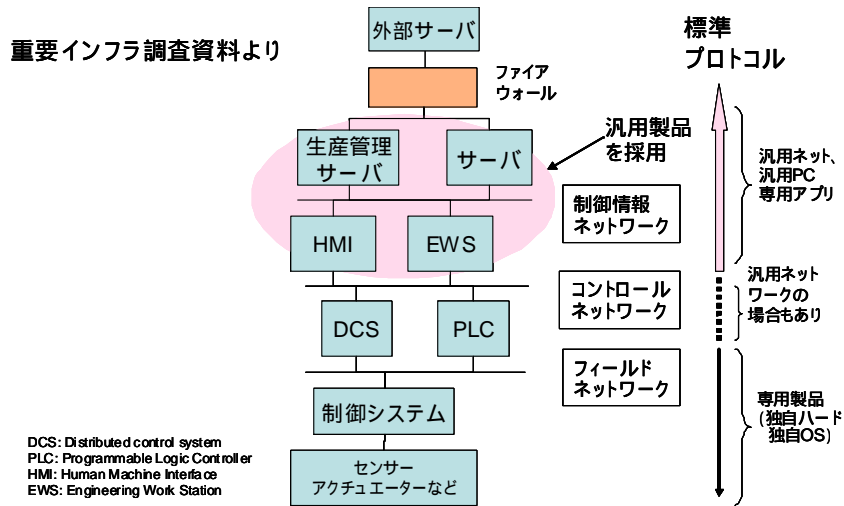


図 6-2 重要インフラのオープン化状況

IPA「重要インフラの制御システムセキュリティとITサービス継続に関する調査」から引用

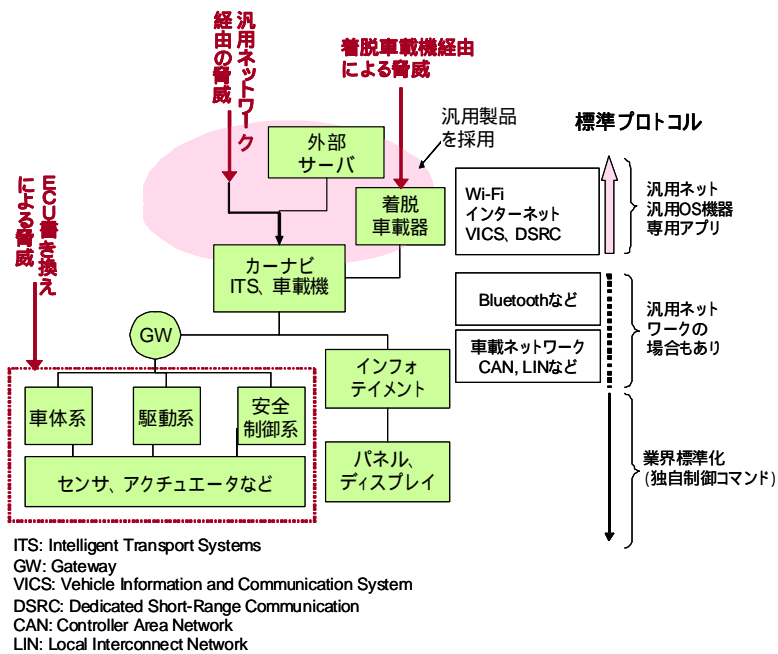


図 6-1 自動車のオープン化状況

3) 重要インフラのセキュリティ課題と自動車システム

オープン化の方向にある重要インフラの制御システムで検討されたセキュリティ上の課題について、自動車システムに照らし合わせて比較した。

表 6-3 重要インフラのセキュリティ課題と自動車システム

	重要インフラの制御システムにおける課題	自動車システム
課題 1	オープン化に伴う脆弱性リスクの混入 ・汎用製品、標準プロトコル採用により、脆弱性リスク、ワームなどのウイルス進入、機密情報朗詠の恐れ	同じ課題が当てはまる ・ウイルス進入や個人情報漏洩の脅威は昨年指摘されている
課題 2	製品長期利用に伴うセキュリティ対策陳腐化 ・制御システムは通常 10-20 年使用。セキュリティ対策も最新ではない可能性	同じ課題が当てはまる ・自動車のライフサイクルは、およそ 10 年前後。常に最新の対策を施しておくことは困難な可能性
課題 3	可用性重視に伴うセキュリティ機能絞込み ・可用性重視の観点から、一般的にシステム上の負荷となるウイルス監視やチェックプログラムの自動更新せず	同じ課題が当てはまる ・機能安全性(可用性、完全性)と低コスト重視の観点から、ウイルス監視機能などは搭載機能順位が低くなる

ここで列挙した重要インフラの制御システムにおける脅威の課題はそれぞれ、自動車の情報システムでも同じ課題があてはまると考えられる。そのため、重要インフラで検討されるセキュリティ対策の取り組みは、自動車の情報システムでの取り組みでも参考になるものと考えられる。

4) システムの特徴比較

重要インフラと、自動車の情報システムの特徴から、自動車システムの位置づけを検討してみたのが次の表である。

表 6-4 自動車システムの位置づけの検討表

セキュリティ上、必要となる要件	一般の情報システム	重要インフラなどの制御システム	自動車の情報システム
技術のサポート期間	3-5年	20年以上	一般的に10年前後
パッチ提供サイクル	頻繁・定期的	ベンダごとに不定期、長期間隔で実施(公表値なし)	法廷点検、定期点検時などで実施可能(実施状況は不明)
システム上流れるデータの処理速度	データ受け取り遅延が致命的な被害となるケースは少ない	システム/機器制御にはリアルタイムのデータ受け取りが不可欠	稼働中のシステム/機器制御にはリアルタイムなデータ受け取りが不可欠
可用性 (Availability)	再起動は許容可能	24時間365日の安定稼働が不可欠(再起動不可)	一旦停止しエンジン再始動は可能
セキュリティに関する意識	民間企業、公的機関との意識行き渡り、対策が定義されている	発展途上にあり未成熟。情報システム技術の適用で対策するケースもある	開発メーカー、利用者とも未成熟。対策への取り組みも顕在化していない
被害の結果	金銭的損失、プライバシー被害	人命損失の可能性	金銭的損失、プライバシー被害、人命損失の可能性

この表では、一般的な汎用コンピュータを利用した情報システムをいちばん左に、重要インフラなどの制御システムを中央に、自動車の情報システムをいちばん右に配置している。この表を行ごとに見ていくと、例えば技術のサポート期間では、一般の情報システムが3から5年以内で、製品のサポートが受けられなくなるなどの形で製品のライフサイクルが終了するのに対し、制御システムと自動車の情報システムは10年以上のライフサイクルを持ち、利用され続けることがわかる。

このように自動車システムの特徴は制御システムにより近く、制御システムにおけるセキュリティ対策の取り組みは、自動車業界での取り組みの参考になると考える。ただし、本検討会で指摘があったように、重要インフラの現状での情報セキュリティへの対策は「現在ある制御システムへの事後対策」であり、これからITSを採用して開発されるような、

「新しい製品開発の道を歩む自動車」とは異なる面もあるため注意が必要である。

6.6 Microsoft 社のセキュリティ開発ライフサイクルの取組み

1) 「SD³+C」というセキュリティ開発ライフサイクル(SDL)の考え方

SD³とは、”Secure by Design, by Default and in Deployment.”の略で、セキュリティは設計と初期値、導入方法によって確保できるという考え方である。また、+C の意味は”Communications”で、設計・製造・導入プロセスにおける関係者同士のコミュニケーションが重要だとしている。

2) セキュリティ開発ライフサイクルのコアとなる「脅威モデル」

脅威を抽象化・モデル化する「脅威モデル」も、セキュリティ開発ライフサイクルにおいて重要な要素である。脅威モデルは、コードレビューだけでは見つかりにくい、バグ以外の脅威を見つけるために有効である。脅威モデルにおける作業手順は以下のようになる。

- アプリケーション動作の分解と、境界の明確化
- 脅威の分析・定義と分類
- STRIDE 分析
 - Spoofing, Tampering
 - Repudiation
 - Information disclosure
 - Denial of service
 - Elevation of privilege
- 攻撃手法の特定
- 脅威への対策

3) Microsoft はいかにして SDL にたどり着いたのか

Microsoft が SDL にたどりつくまでには、5 年以上にわたるさまざまな試行錯誤があった。例えば、1999 年ごろには、Pen-test Team と呼ばれる、開発チームとは独立して、侵入攻撃の検査を行うチームを設立したが、2000 年ごろには、開発者自信を支援して脆弱性を削減する取り組み(SWI: Secure Windows Initiative)を始めた。

その後 Trustworthy Computing Initiative という活動が始まり、その最初の対策として、.NET Framework に対する「セキュリティ・プッシュ」が実施された。セキュリティ・

プッシュとは、特定にソフトウェア製品について、担当する開発者すべての開発を一旦停止し、セキュリティ対策にあてるといったものだ。

その後、2002年ごろ、Windows Server 2003の出荷前には8,500人以上におよぶ技術者へのセキュリティトレーニングの実施と、脅威モデルに基づく設計への変更、静的検査ツールによるコード検査、コードレビューの実施、バッドパラメータを使ったセキュリティテストとペネトレーションテストの実施、という大規模なセキュリティ・プッシュが実施された。以後、このような開発者全体がセキュリティに取り組むという流れがMicrosoftの新たな標準となった。

2004年には、こうしたセキュリティ対策としてのSDLは、個別製品への一時的な対策ではなく、開発手順の標準工程として扱うよう、開発基準が定められた。Microsoftでは、SDLは以下のような製品に必ず適用して開発しなければならないとされている。

- 日常的に、企業、政府、その他で利用されるプログラム。
- 日常的に、個人情報や他のセンシティブな情報を扱うプログラム
- 日常的に、インターネットに接続するプログラム

その後SDLは年に2回バージョンアップされ、Microsoftの半数以上の技術者がトレーニングを受けている。

4) 参考書籍

The Security Development Lifecycle

by Michael Howard, Steve Lipner

June 28, 2006

ISBN-10: 0735622140

ISBN-13: 978-0735622142

Writing Secure Code 第2版(上)

マイケル ハワード, デイビッド ルブラン

出版社: 日経 BP ソフトプレス; 第2版

(2004/12)

ISBN-10: 4891004460

ISBN-13: 978-4891004460

Writing Secure Code 第2版(下)

マイケル ハワード, デイビッド ルブラン

出版社: 日経 BP ソフトプレス; 第2版

(2004/12)

ISBN-10: 4891004479

ISBN-13: 978-4891004477

脅威モデル セキュアなアプリケーション構築

フランク スワイダスキー , ウィンドウ スナイダー

出版社: 日経 BP 出版センター (2005/6/9)

ISBN-10: 4891004576

ISBN-13: 978-4891004576

5) セキュリティ開発ライフサイクル(SDL)に関連する資料

MSDN セキュリティデベロッパーセンター

<http://www.microsoft.com/japan/msdn/security/>

信頼できるコンピューティングのセキュリティ開発ライフサイクル

<http://www.microsoft.com/japan/msdn/security/general/sdl.aspx>

Inside the Windows Security Push

<http://www.princeton.edu/~echi/ele572/Howard%20-%20Windows%20security%20push.pdf> (調査時点では存在したが、報告書完成時点でリンク切れ)

Security Development Lifecycle (SDL) Banned Function Calls

<http://msdn2.microsoft.com/en-us/library/bb288454.aspx>

Trustworthy Computing

<http://www.microsoft.com/mscorp/twc/default.mspx> (English)

<http://www.microsoft.com/japan/mscorp/twc/security/default.mspx> (日本語)

Read the CNET report: MS セキュリティのこの 10 年: 手痛い教訓をバネに

http://www.news.com/At-software-giant%2C-pain-gives-rise-to-progress/2009-7349_3-6220566.html?tag=st.nl (English)

<http://japan.cnet.com/special/story/0,2000056049,20363043,00.htm> (日本語)

TechNet: 脆弱性の防御では、切り札である「プロセス」が「多くの目」に勝ります

<http://www.microsoft.com/technet/community/columns/secmgmt/sm1007.mspix>
(English)

<http://www.microsoft.com/japan/technet/community/columns/secmgmt/sm1007.mspix> (日本語)

Windows Vista 1 年間の脆弱性レポート

<http://download.microsoft.com/download/c/d/c/cdcc38a5-50fa-4425-be75-9d165065d0c8/vista-one-year-vuln-report-ja.pdf>

Operating System Vulnerability Scorecard

<http://blogs.technet.com/security/archive/2007/08/16/july-2007-operating-system-vulnerability-scorecard.aspx>

“Days-of-risk in 2006: Linux, Mac OS X, Solaris, and Windows”, CSO.com

http://blogs.csoonline.com/days_of_risk_in_2006

Compare Security

<http://www.microsoft.com/windowsserver/compare/linux/security.mspix>

IPAの提供するセキュリティ関連コンテンツ

IPAセキュリティセンターでは、情報セキュリティ対策の普及啓発活動の一環として、以下のようなコンテンツを提供しています。是非ご活用ください。

コンテンツ対象者…ユーザ： 開発者： 経営者：

～ 組み込みシステム及び制御システムに利用できるコンテンツ ～

組み込みシステムのセキュリティへの取り組みガイド

組み込みシステムの開発に携わる組織が、自組織の「セキュリティへの取り組み」がどのレベルにあるのかを把握し、さらに上位のレベルを目指すことで、よりセキュアな組み込みシステムの実装を行うための具体的な指針を得ることができます。 http://www.ipa.go.jp/security/fy20/reports/emb_app/index.html

上水道分野用のSCADAセキュリティ グッド・プラクティス

上水道分野のセキュリティ対策の成功事例に基づき作成39のグッド・プラクティスを使って自組織のセキュリティの現状を把握することができます、水道・ガス・電力等の上水道分野以外の重要インフラ分野にも活用できます。

<http://www.ipa.go.jp/security/fy21/reports/scada/index.html>

セキュアプログラミング講座

想定される様々な攻撃への対策として留意すべき事項を、ソフトウェア開発工程に沿って解説しています。セキュリティ対策を意識したプログラミングができるようになります。

<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html>

TCP/IPに係る既知の脆弱性検証ツール

TCP/IP(Transmission Control Protocol / Internet Protocol) を実装したソフトウェアの脆弱性を体系的に検証し、自社で開発したソフトウェアに、既知の脆弱性が再び作り込まれないよう防止するためのツールです。TCP/IP利用機器の脆弱性の有無を簡易判定することができます。

http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

SIPに係る既知の脆弱性検証ツール

SIP (Session Initiation Protocol) を実装したソフトウェアの脆弱性を体系的に検証し、自社で開発されるソフトウェアに既知の脆弱性が再び作り込まれないよう防止するためのツールです。

SIPを実装したソフトウェアの脆弱性の有無を簡易判定することができます。

http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

～脆弱性対策情報を収集・利用するコンテンツ～

セキュリティ情報RSSポータル

インターネット上に発信されている様々な情報から、セキュリティに関する最新情報を収集・整理し、セキュリティに関する情報を利用しやすく提供するシステムです。多数のWebサイト上に散在する最新情報を効率よく確認することができます。

<http://www.ipa.go.jp/security/fy19/development/rss/index.html>

JVN iPedia

国内の製品開発者から公開された対策情報、および海外の脆弱性関連情報のデータベースに登録された情報に基づき脆弱性関連情報を網羅、蓄積しています。検索機能やRSS配信機能を利用することで効率的に脆弱性関連情報を収集することができます。

<http://jvndb.jvn.jp/>

MyJVN 脆弱性対策情報収集ツール

JVN iPedia の情報を、利用者が更に効率的に活用して頂けるように、フィルタリング条件設定機能、自動再検索機能などを有したツールです。

<http://jvndb.jvn.jp/apis/myjvn/mjcheckhelp.html>

MyJVN バージョンチェッカ

利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツールです。

<http://jvndb.jvn.jp/apis/myjvn/vccheckhelp.html>

MyJVNセキュリティ設定チェッカ

ご利用のPCにおけるセキュリティの設定が参考値を満たしているかを、簡単な操作で確認するツールです。

<http://jvndb.jvn.jp/apis/myjvn/cccheckhelp.html>

～セキュリティ教育用コンテンツ～

5分でできる！情報セキュリティポイント学習

主に中小企業で働く方を対象とした、1テーマ5分で情報セキュリティについて勉強できる学習ツールです。あなたの職場の日常の1コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を学ぶことができます。

http://www.ipa.go.jp/security/vuln/5mins_point/index.html

安全なウェブサイト運営入門

ウェブサイトの脆弱性による被害を中心とした7つの具体的な事件を題材に、ロールプレイング形式で体験的に学習できるソフトウェアです。事件や事故が発生した場合の被害を理解し、事前対策の必要性を学ぶことができます。

<http://www.ipa.go.jp/security/vuln/7incidents/index.html>

知っていますか？脆弱性(ぜいじゃくせい)

ウェブサイトの運営者や一般利用者向けに、ウェブサイトにおける代表的な10種類の脆弱性について、わかりやすくアニメーションで解説したものです。脆弱性についての理解を深めることができます。

http://www.ipa.go.jp/security/vuln/vuln_contents/index.html

ITセキュリティ評価・認証に関するe-Learning教材

ITセキュリティ評価・認証に関連する専門書を読みこなし活用するための入門的な教材です。「自己学習課題」に取り組むことにより、習得した知識を実践に結び付け、実際のシステム開発に生かすことができます。
http://www.ipa.go.jp/security/fy19/development/e_Learning_CC/index.html

暗号技術に関するe-Learning教材

システムの選定や調達仕様の作成などに必要な暗号技術に関する知識を、幅広く修得するための教材です。ネットワークを通じて教育を行うので、時間や場所を選ばずに暗号技術に関する学習が行えます。
http://www.ipa.go.jp/security/fy19/development/e_Learning_Cipher/index.html

～その他～

情報セキュリティ対策ベンチマーク

組織の情報セキュリティマネジメントシステムの実施状況を自らが評価する自己診断ツールです。40の設問に答えることでセキュリティに関する自社の取り組みがどの程度のレベルにあるのかが分かります。
<http://www.ipa.go.jp/security/benchmark/index.html>

iLogScanner

ウェブサイトのアクセスログを解析することで、そのサイトへの攻撃痕跡を確認するツールです。運営しているウェブサイトがどれほど攻撃を受けているか等の状況を把握することができます。
<http://www.ipa.go.jp/security/vuln/iLogScanner/index.html>

IPAでは今後も関係団体等と協力の下、セキュリティ対策の普及に向けた活動を続けていきます。上記コンテンツ等へのお問い合わせ、ご意見がございましたら isec-info@ipa.go.jp までお寄せ下さい。