6

自動車や医療機器を対象とした新たなサイバー攻撃の脅威 応般

中野　学
（独）情報処理推進機構

背景

社会インフラを標的とした攻撃が増える中で，産業用制御システムや町単位でさまざまなデバイスが繋がりサービスを実現するスマートシティ等への脅威の分析やセキュリティ対策の検討・実装が進みつつある．多くの産業用制御システムでは企業や団体が一括して管理することができるため，組織的なセキュリティ対策を実施することが可能である．一方で，今後自動車や家電，医療機器が繋がってくるであろうスマートシティにおいては，利用者や管理者が多様になるため，さまざまな状況に応じたセキュリティ対策が必要になると考えられる．

本稿では社会インフラにつながる多様な「組込み機器」における脅威の現状についてまとめるとともに，自動車を例とした脅威と対策の分析手法について解説する．

組込み機器の現状

マイクロプロセッサやメモリ等の半導体性能の向上に伴い，産業機器や家電製品はますます高機能化の一途を辿っている．それらの機器を制御するために機器の内部に組み込まれたコンピュータシステム，「組込みシステム」が自動車や医療機器といったさまざまな分野で利用されている．その結果として，以下の 3 つの進化と，それに伴った課題が発生している．

▌ネットワークへの接続

スマートフォンの普及や通信機能の低コスト化によって，インターネット接続が可能であったり，短距離無線を搭載した組込み機器が増加している．これによって，これまでネットワーク経由の攻撃が考慮されていなかった製品群が，今後はサイバー攻撃の対象になる可能性がある．

▌新しいサービスの発達

新しい技術や機器の発達に従って，さまざまな新しいサービスが創出されるようになった．これによって，組込み機器の機能や内包する情報が価値を持ち，利益を求める攻撃者にとっての標的となる可能性がある．

▌汎用プロトコル等の利用

多種多様な機器が接続されることや，機器開発におけるコスト競争等から，組込み機器に対して，汎用 OS やプロトコルが利用されるようになってきた．これによって，情報システム同様の脆弱性や脅威が発生する可能性がある．

このような背景から，サイバー攻撃へのセキュリティ対策の推進が望まれるところではあるが，組込みシステムの開発現場では，市場における価格競争の激化を要因とする開発期間の極端な短縮化のために，セキュリティへの対応が疎かにされやすい現状がある．開発の最前線にいるエンジニアをはじめとして，責任者や経営陣がセキュリティに対してどのように取り組んでいくべきかが課題となっている．そのため，組込み機器における脅威や，その対策を検討する上での整理・分析手法が必要である．

組込み機器における脅威

本章では自動車や医療機器に潜在する脅威について報告されているものをいくつか紹介する．

車両検査用ポートを利用した攻撃

2010年5月，米国Washington大学のTadayoshi Kohno氏らによって「Experimental Security Analysis of a Modern Automobile」と題した論文[1]が発表された．本論文では，各車載システムにおける主要な機能と車載ネットワークのセキュリティプロパティ等を評価するために，停止状態での解析や，同じメーカの自動車2台を実際に走行させながら近距離通信を使って攻撃パケットを送ることで車載コンピュータ（ECU：Electronic Control Unit）を攻撃する等の実験を行った．

実験は以下の3種類の方法で行われた．

① ベンチ

物理的に部品を取り外し，部品ごとに制御プロトコルを解析した．解析には，車載ネットワークであるCAN（Controller Area Network）バスの配線にパソコンのUSBポートを接続する装置である，CAN-USB変換器を利用した．

② 固定車両

ジャッキにより車両を持ち上げて，車輪が回転しても周囲に影響が出ない状態において，車両検査用ポートから車載ネットワークに対して攻撃を目的としたCANメッセージを送信した．

③ 走行車両

閉鎖された飛行場で走行実験を行った．

Kohno氏らは，実験対象の多くの車載コンピュータは，認証に妨げられることなくファームウェアの更新が可能だったことを指摘し，想定より容易にECUを直接操作できる現状を明らかにした．

対策として，ECUから診断やソフト書換え命令を出す場合は特定の検証を経て発行すること，検証にはメッセージのコード認証や命令を出した機器の機器認証を必要とすることを挙げている．また，車に接続したラジオやアラーム等の装置を経由した侵入を防ぐため，信用のない装置を接続する際のフィルタ部品の追加も対策として挙げている．

CANの解析による攻撃

2013年に開催された情報セキュリティの国際会議，21th Defconにおいて，CANに流れる情報を解析し，その通信になりすますことで攻撃を行う，その手法と実証実験の動画が公開された．この結果，車内のパソコンをCANに直接物理的にコードで接続した状態で任意のコードを送った場合，速度計や走行距離計等の計器類を操作することと，運転アシスト機能の誤作動を引き起こすことが可能であることが証明された．

このときの攻撃コードや技術については研究結果として公表されているが，非常に高度なものであり，実験環境以外で行うためには，セキュリティおよび自動車に関する相当の知識が必要となる．また，現状では本攻撃手法はリモートでは不可能と報告されており，ネットワークに接続された自動車が直ちにこの脅威に直面することはない．また，本実験ではフォード車とトヨタ車が利用されたが，同様のアプローチで他社の自動車に対しても影響を与えられることが推測される．

ペースメーカーへのハッキング

2008年，米国Washingtonの Daniel Halperin氏および米国Massachusetts大学（発表時）Kevin Fu氏らにより2008 IEEE Symposium on Security and Privacyでペースメーカー／ICD（Implantable Cardioverter Defibrillator：植込み型除細動器）へのハッキングについて発表された☆1．

Halperin氏らによる研究では，ICDとプログラマ☆2のやりとりを，オシロスコープとソフトウェア無線機を用いて送信波を解析し，暗号化されていなかった通信データから情報を解読し，患者の状態や機器の設定などの情報を盗み出すことに成功した．

さらに，市販の機器等を利用して，同じ周波数の波形を送信することによるリプレイアタックを行い，プログラマを経由することで，以下のような攻撃を成功させている．

- ICDの場所，型番やシリアルナンバなどの詳細情

☆1 http://www.healthcare.philips.com/main/products/patient_monitoring/products/avalon_fm40_fm50

☆2 プログラマ：ICDの情報を見たり，設定の変更を行う専用端末．

報を取得
- 患者の情報（名前，診断情報，その他詳細情報）を取得
- 疾患情報など，心臓のデータを取得
- ICD に登録されている患者名の取得・変更
- イベントログ等を記録するための時間設定の読み取り，再設定
- 心臓に何らかの処置を行う設定，治療設定の削除や変更

また，論文中では，安全でないソフトウェアアップデートの枠組みや，バッファオーバフローに関する脆弱性を悪用した攻撃の可能性も示唆するとともに，対策手法の提案も行っている．

インスリンポンプへのハッキング

2011 年 Black Hat にて Jerome Radcliffe 氏によりインスリンポンプへのハッキングについて発表された[2)]．

Jerome Radcliffe 氏は，糖尿病患者の治療に用いるインスリンポンプの制御システムに脆弱性を突いて侵入し「致死的な攻撃」を仕掛けることができると発表している．具体的には，インスリンを送り込むポンプの無線機能に脆弱性が存在し，それを突くことでポンプ自身を停止においやったり，投与するインスリンの量を外部から操作したりすることが可能であるとしている．

本研究の結果，CGM センサ☆3 では容易に通信情報の解読が可能であり，インスリンポンプにおいても機器のシリアル番号を取得できれば無線通信により誤った命令を実行できるとしている．CGM センサ，インスリンポンプそれぞれにおいて，理論上は以下の攻撃が可能であると発表している．

- **CGM センサ攻撃例**

実際のデータと違う血糖値データを送ることで，インスリン投入量の変化を誘発

正しい血糖値データ受信を妨害し，別のデータを送信

- **インスリンポンプ攻撃例**

ワイヤレス機器を用いて，設定の書き換えを行い，意図しない動作を誘発（インスリン投入のタイミングや 1 回あたりの投入量の変更等）

自動車における脅威分析

サイバー攻撃の脅威へのセキュリティ対策を検討するためには，攻撃手法や保護すべき情報資源等を整理した上で，適切な対策を実施する必要がある．しかし，組込み機器の範囲は広く，機器によって利用のされ方や管理手法，組込み機器を取り巻く法規制等に違いがある．IPA では今後さまざまな機器と連携していくことが考えられる，自動車におけるセキュリティ上の脅威と対策について整理を行った経緯があるため，本章ではその分析手法について説明する．

自動車の機能の整理

自動車におけるセキュリティを詳しく検討するために，本節では**図 -1** の「自動車」および「追加機器」に関して，より詳細な整理を行う．自動車は自動車メーカや価格帯（グレード）によって，自動車の構造・機能等に違いがあるため，業界共通的な自動車のモデルを定義することは難しい．そのため IPA では，自動車システムのセキュリティ分析および求められる信頼性の観点から，**図 -2** に示すような「IPA カー」と呼ぶ自動車のモデルを仮定した．

「IPA カー」では車載 LAN を最大限に抽象化し，1 本のバスにすべての機能が接続されるものとして定義した．また，「IPA カー」では「走る・止まる・曲がる」といった「基本制御機能」に加え，快適性や利便性を高める「拡張機能」，利用者が車内に持ち込まれる機器等「一般的機能」から構成されていると定義した．外部接続ポートはそれぞれの機能に含まれる可能性があるが，ここでは「拡張機能」と「一般的機能」の間を繋ぐものとして抜き出し，整理した．なお，「基本制御機能」と「拡張機能」を合わせたものを，「車載システム」と呼ぶこととし，こ

☆3 CGM（continuous glucose monitors）：継続的に糖濃度を計測するシステム．

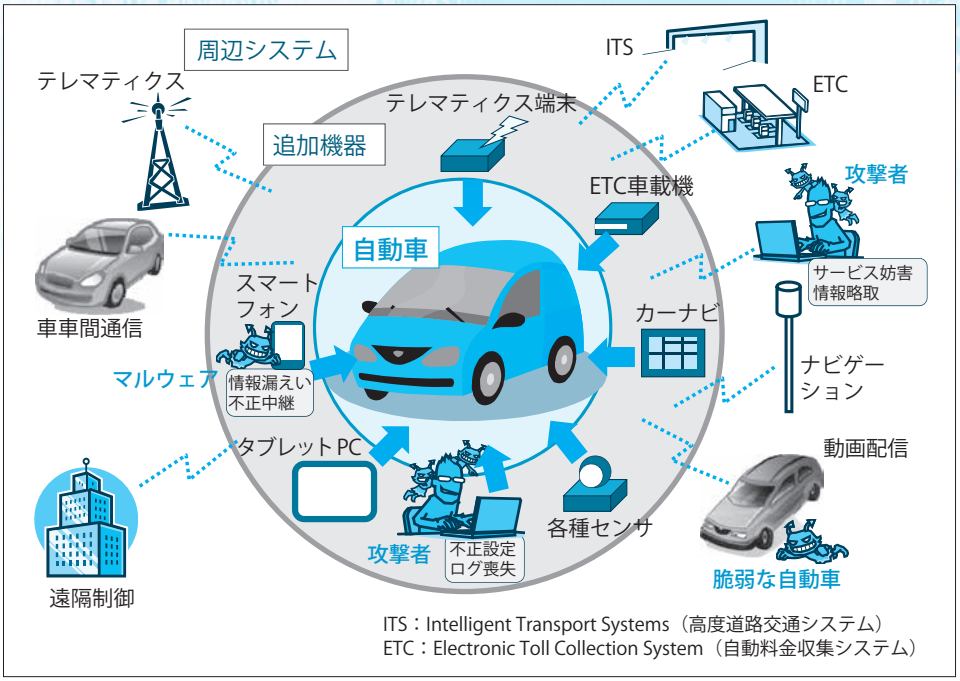

図 -1　自動車を取り巻く環境

の 2 つの機能カテゴリに関しては，「駆動系」や「インフォテイメント」といった，機能の細分化を行っている．IPA の取り組みでは「車載システム」における脅威と対策を検討することを目的としている．

「拡張機能」に含まれる機能は大きく 2 つに分類される．1 つは，「ボディ系」「安全快適機能」「診断・保守」をまとめた「制御関連」であり，主に「走る・止まる・曲がる」といった自動車の物理的な機能と密接に関連する．もう 1 つは，「ITS 機能」「テレマティクス」「インフォテイメント」をまとめた「情報関連」であり，運転者に情報を提供するための機能と密接に関連する．これらの 2 つの機能は，機能としての挙動はもちろんとして，機能を利用して提供されるサービスやセキュリティの問題が発生した際のリスク等に違いがあると考えられるため，連携する機能や取り扱う情報等に適したセキュリティを検討していくことが必要である．

一般には，基本制御機能や制御関連に分類される自動車の制御にかかわる機能では可用性が重視され，情報関連では機密性が重視されることが多い．

自動車において保護すべき資産

セキュリティ対策では，情報が漏えいすることを防ぐ機密性の確保や，必要なときに正しく利用することができるための可用性，それに情報の破壊や改ざん等から守る完全性の 3 つの確保を目的とする．機密性や可用性を検討するためには保護対象を明確にする必要があるため，本節では自動車において保護すべき対象についての一例を**表 -1** にまとめた．保護すべき情報等資産には自動車を走らせる上で発生する

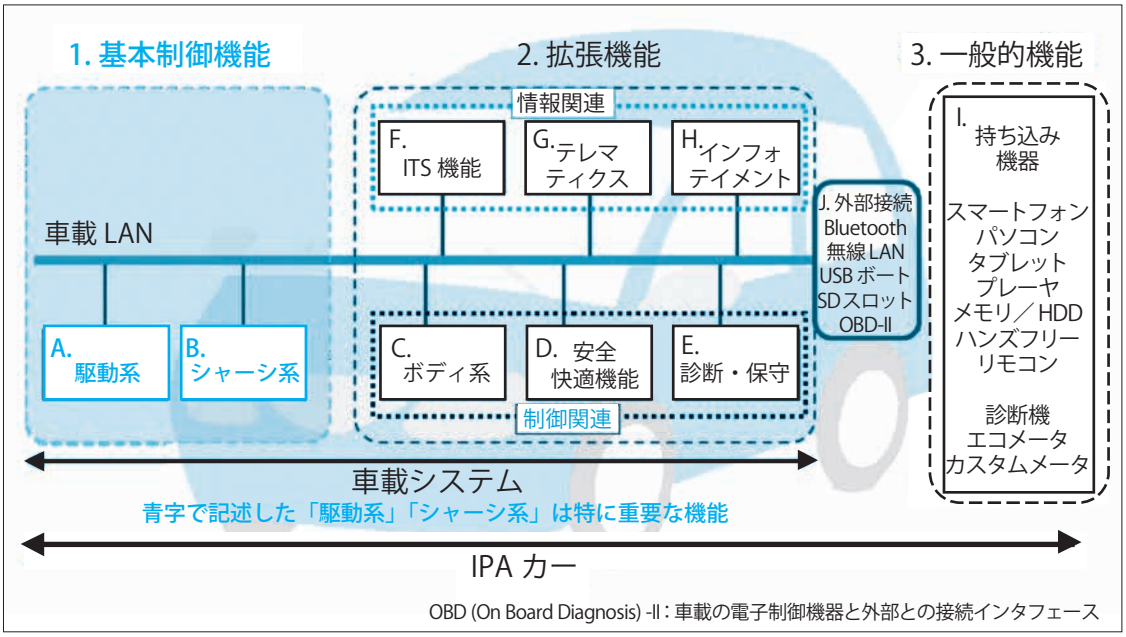

図 -2　IPA カー

保護すべき対象	具体例
基本制御機能の動作	自動車を制御する情報・機能 等
自動車固有情報	車両 ID，認証情報コード 等
自動車状態情報	車速，位置情報 等
ユーザ情報	搭乗者情報，操作履歴 等

表 -1　保護すべき資産

情報や，自動車の利用者が自動車に登録する情報等のほかに，車載ソフトウェアや外部との通信そのものが該当する．

自動車における脅威

自動車のモデルとなる IPA カーを利用して，IPA が脅威の分析を行ったものが**図 -3** となる．

基本的に，内外からの通信の口があり，機能や情報を持つ部分に対してはセキュリティ上の脅威の対象となる可能性がある．したがって，機能の設計やサービスの企画を行う際には，これらの脅威の発生の可否と，もし脅威が起こり得るのであればリスクの算定と対策について検討する必要がある．なお，現状では自動車の制御を担う機能は外部との通信ポート等を持たないため，パソコン等を CAN に物理的に繋いで情報を送る等のことをしない限りは，いきなり外部から自動車の制御を奪われる可能性はきわめて低いと考えられる．しかし，自動運転を含めた自動車の利便性向上に向けた高機能化が進む中で，ITS 機能や安全快適機能等の拡張機能が駆動系・シャーシ系と連動していくことも予測される．その際に，拡張機能が乗っ取られることで，操縦者や自動車の安全維持機能が意図しない制御が行われることがないように注意が必要である．

自動車のセキュリティ対策

自動車のセキュリティを向上させるためには，自動車にかかわるさまざまな情報等資産を対象とし，その価値に応じた適切なセキュリティ対策を施す必要がある．これには，自動車システムのライフサイクルを念頭においた分析が有効である．IPA では，自動車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，さらにそれらを統括する全ライフサイクル共通の「マネジメント方針」を含めた 5 つの段階において，総計 15 のポイントについてまとめた．具体的には IPA から公開している「自動車の情報セキュリティへの取り組みガイド」[☆4] をご覧いただくとして，この場では各サイクルの項目だけ紹介する．

(1) 企画フェーズ

自動車メーカが製品企画や脅威の分析を行うフェーズ．

- セキュリティに配慮した要件定義の策定

☆4 自動車の情報セキュリティへの取組みガイド，http://www.ipa.go.jp/files/000027273.pdf

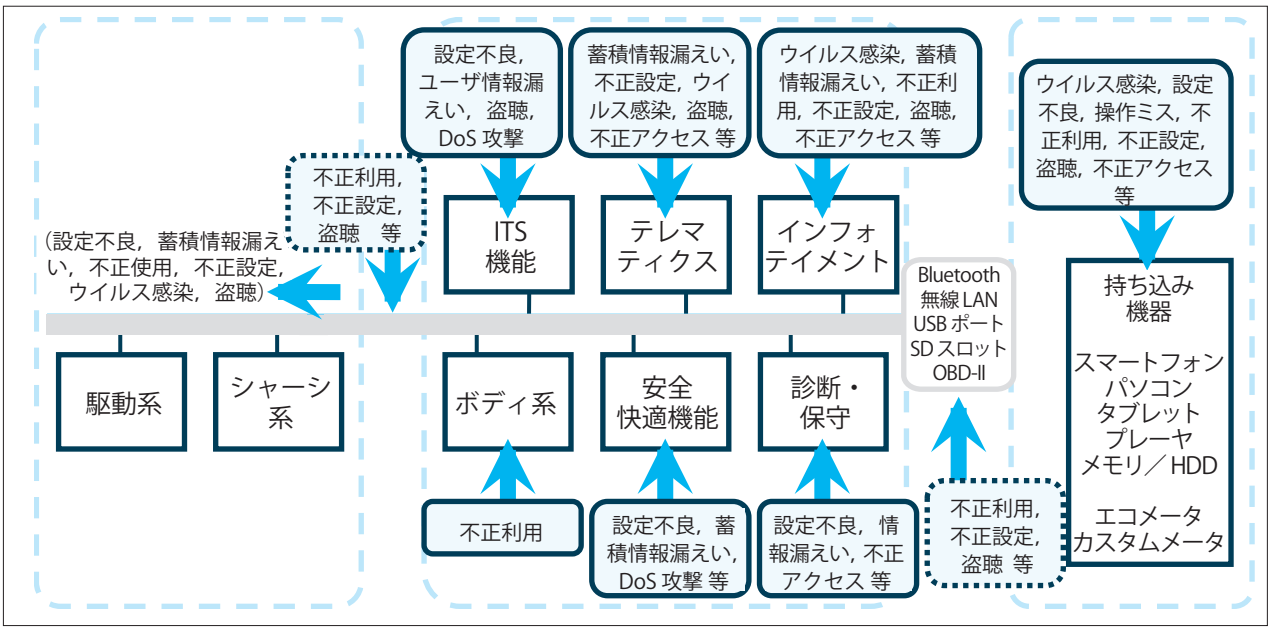

図 -3　IPA カーにおける脅威例

- セキュリティ関連予算の確保
- 開発外部委託におけるセキュリティへの配慮
- 新技術に関連する脅威への対応

(2) 開発フェーズ

企画フェーズで策定した要件定義に基づいて，自動車メーカや部品メーカがハードウェアやソフトウェアを設計し，自動車の実装・製造を行うフェーズ．

- 設計
- 実装時のセキュリティ対策
- セキュリティ評価・デバッグ
- 利用者等への情報提供用コンテンツ等の準備

(3) 運用フェーズ

ディーラー等を介して利用者が自動車を入手し，使用するフェーズ．

- セキュリティ上の問題への対処
- 利用者や自動車関係者への情報提供
- 脆弱性関連情報の活用

(4) 廃棄フェーズ

買い替えや故障等により利用者が自動車を手放すフェーズ．

- 廃棄方法の策定と周知

(5) マネジメントフェーズ

恒常的に行う人材育成や情報収集等の活動．

- セキュリティルールの策定
- セキュリティ教育の実施
- セキュリティ情報の収集と展開

よりセキュアな社会に向けて

今後，社会インフラに繋がる情報システムが高度化するに従って，さまざまなサービスが生まれ，生活がより便利により豊かになっていくことは容易に想像できる．社会インフラが整っていくことによって，それを利用する自動車は事故低減や利便性向上が実現されるであろうし，医療機器はより必要な人に適切で素早い対応がとれるように発展していくことだろうと思う．その一方で，今後さまざまなシステムが繋がっていくことで，情報やサービスに利益や安全等が絡み，それを狙う攻撃者も必ず発生する．よって，今後は機器の開発者や，それらを使うサービスの運用者だけでなく，自動車であれば運転手や同乗者，医療機器であれば患者にあたる一般利用者も一体となってセキュリティ対策に取り組む必要がある．

そのためにも今後はサービスの企画や製品の開発において，攻撃者の視点で物事を捉え，サイバー攻撃の脅威を低減させることが求められる．また，利用者にしても自らの身を守るためにも，セキュリティについて最低限の知識を持ち，アップデート等の手間を含めたセキュリティコストを請け負うことが必要となる．

今後も IPA では社会インフラに影響を与えるさまざまな脅威に対して，調査や分析を行っていく予定である．IPA の活動がセキュリティ対策に取り組む各位にとっての一助となれば幸いである．

参考文献

1) Experimental Security Analysis of a Modern Automobile, http://www.autosec.org/pubs/cars-oakland2010.pdf
2) Radcliffe, J. : Hacking Medical Devices for Fun and Insulin, Breaking the Human Scada System, Black Hat USA (2011).

(2014 年 4 月 1 日受付)

中野　学　mn-naka@ipa.go.jp

2006 年横浜国立大学環境情報学府博士課程後期修了．博士(情報学)．同年（独）情報処理推進機構へ入社．デジタル家電や自動車，医療機器といったような組込みシステムや，制御システム，バイオメトリクス等のセキュリティ課題に関する調査，その成果の普及に関する活動に従事．