車両サイバー攻撃に対抗する統合監視・対応システム

Study on Intrusion Detection and Prevention System against Cyber Attacks on Connected Cars

中野 稔久 Toshihisa Nakano
安齋 潤 Jun Anzai
今本 吉治 Yoshiharu Imamoto
横田 薫 Kaoru Yokota
鳥崎 唯之 Yuishi Torisaki

要　旨

外部ネットワークへの接続機能を有するコネクティッドカーにおいては，攻撃者が，インターネットを経由して自動車へ侵入し，そこから車載ネットワークへ不正な制御コマンドを送信することで，自動車にドライバーの意図しない挙動をさせるサイバー攻撃が可能である．一方で，サイバー攻撃を検知して記録する，あるいは通知してサイバー攻撃の対処につなげる仕組みの導入はまだ十分ではない．本稿では，コネクティッドカーへのサイバー攻撃を監視し，攻撃者による侵入を検知するための要件および課題を整理した．さらに，車両統合監視・対応システムを提示して，提示したシステムに対する要件の実現性について，車両全体の攻撃の状況を把握する技術の必要性と，クラウドにおいて車両から収集したログデータから新たな攻撃を抽出する技術の必要性を示した．

Abstract

Vehicle connectivity introduces potential cybersecurity threats from the Internet. Hackers can remotely endanger a driver's life by exploiting vehicle vulnerabilities to control the actuator such as the steering wheel. The authors believe that it is important to construct an Intrusion Detection and Prevention System (IDPS) for connected cars. The IDPS must have the ability to protect against known attacks and detect unknown attacks. In this paper, we organize the requirements and tasks from the viewpoint of host (IVI etc.), Ethernet, CAN and cloud.

1. はじめに

近年の自動車では，Control Area Network（以下，CAN）を中心とした車載ネットワーク（以下，車載NW）を介して，ステアリングやブレーキなどのアクチュエータを制御するコンピュータであるElectronic Control Unit（以下，ECU）が協調動作するアーキテクチャを採用している．これまで自動車は，インターネットなどの外部ネットワークに接続されていなかったが，スマートフォンからの遠隔操作サービスや自動運転用のダイナミックマップ取得など，高度なサービスを利用者へ提供することを目的に外部ネットワークへの接続機能の搭載が進められている．

このような外部接続機能を備えた自動車に対しては，インターネットを経由して侵入し，車載NWに不正な制御コマンドを送信することでサイバー攻撃が可能であることが知られている．2011年にCheckowayら[1]が，事前にIn-Vehicle Infotainment機器（以下，IVI）のファームウェアを改ざんするという条件付きであるものの，自動車の外部から，自動車を制御できることを証明した．2015年にはMillarら[2]が，事前のファームウェアの改ざんなしに，自動車の外部から携帯網を介してIVIに侵入し，車載NWに不正な制御コマンドを送信することで，自動車のアクチュエータが制御できることを実証している．また，2017年にはSen Nieら[3]により，ゲートウェイ（以下，GW）を搭載した自動車に対して，インターネットからIVIに侵入し，IVIからEthernet (注1) 経由でGWのファームウェアを改ざんすることで，GWから不正な制御コマンドを送信する攻撃も実証されている．2011年より今日まで攻撃は進化を続けており，自動車もIT機器と同様に攻撃の進化への対応が必要であることがわかる．

さらに，このような自動車へのサイバー攻撃の発表・実証を受け，国連欧州経済委員会（UNECE）の下部組織である「自動車基準調和フォーラム（WP29）」において，2020年6月にサイバー攻撃対策を義務付ける指針が採択され，2021年1月から施行することが決定された．本指針では，各車両に対して，サイバー攻撃の検知や防御，サイバー攻撃に関する分析を可能とするデータの収集など，セキュリティ観点で車両を監視する「セキュリティ監視システム」が求められている．

本稿では，自動車に対するサイバー攻撃を監視し，攻撃者による侵入を検知して対応するセキュリティ監視システムについて，その要件，および課題を整理・抽出し，セキュリティ監視システムを提案して，その実現性を検討する．

（注1）富士ゼロックス（株）の登録商標または商標．

2. 従来技術とその課題

IT機器におけるセキュリティでは，サイバー攻撃に対して複数の障壁を設ける多層防御と呼ばれるアプローチが存在する．例えば，オフィスネットワークを想定した場合は以下のとおりである．

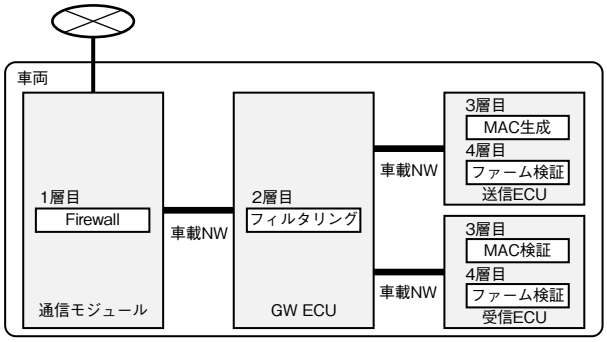
1層目：インターネットとの境界面にFirewall機器を配置してポート番号やIPアドレスに基づきアクセス制御を行う．

2層目：ネットワーク上にGWを配置して送受信されるパケットのマルウェア検査などを行う．

3層目：さらにネットワーク上に侵入検知装置を配置してパケットの振る舞いから攻撃パターンの検査を行う．

4層目：クライアントPCに統合セキュリティソフトなどをインストールして保護する．

一方で，コネクティッドカーを想定した場合は以下の**第1図**のとおりに考えられる．



第1図　車両における多層防御の一例
Fig. 1　Example of multi-layered protection

1層目：インターネットとの境界面である通信モジュール上のFirewall機能によりポート番号やIPアドレスでアクセス制御を行う．

2層目：CANバスや車載Ethernetバスにより構成される車載NW上にGW ECUを配置して，想定外のコマンドに対してフィルタリングを行う．

3層目：送信ECUが，CANバスに送信するCANコマンドや，車載Ethernetバスに送信するパケットに対してメッセージ認証子（以下，MAC：Message Authentication Code）を生成して付与し，受信ECUがMAC検証することで送信データのなりすましを検証する．

4層目：送信ECU，受信ECUなどの各種ECUのアプリケーション層において，リプログラミング用のファームウェアのデジタル署名検証や診断コマンドの認証を行う．

オフィスと自動車の多層防御の大きな違いとして，継続的な攻撃への対応が挙げられる．

オフィスの例では，①あらかじめ想定する脅威や攻撃を特定し，②それらに対応できる防御設計を行い，実際の運用フェーズでは，③Firewallや侵入検知装置からのアラートをネットワーク管理者が監視することでセキュリティの異常を検知し，④異常の内容を分析して対応策を検討し，⑤ネットワークの遮断やFirewallの設定変更などの回復まで行うことが可能である．

一方，従来の自動車は，①脅威の特定と，②防御設計は自動車の出荷前に実施可能であるが，出荷後は，定期的にディーラーなどへ入庫しない限り，③攻撃の検知や管理者への通知，④攻撃への対応，⑤攻撃からの回復を行うことは基本的には困難である．また，定期的にディーラーなどへ入庫する場合であっても，多層防御における1層目～4層目のそれぞれの層において，サイバー攻撃を検知して記録する，あるいは通知する仕組みの導入が不可欠である．

3. 車両統合監視・対応システムの要件と課題

本章では，コネクティッドカーに対して，あらかじめ想定できる攻撃（以下，既知攻撃）の検知や，検知した後の対応に加えて，事前に定義できない新たに出現する攻撃（以下，未知攻撃）への対応も可能とする車両統合監視・対応システム（以下，車両監視システム）の要件を考察する．

ここで，コネクティッドカー向けの車両監視システムは，その構成が大きく車両とクラウドに分割される．車両は，既知攻撃を検知して対応するIntrusion Detection and Prevention System（以下，車載IDPS），および未知攻撃をクラウドで検知して分析するために必要な種々のログデータを収集・保存・送信する機能を有する．ここで，車載IDPSは車両の各所に配置されるが，その詳細については4章で述べる．一方クラウドは，車両から受信した種々のログデータを分析して未知攻撃を抽出するIntrusion Detection System（以下，クラウドIDS），および抽出した攻撃を既知攻撃として新たに定義して車載IDPSで検知・対応できるようにするためのポリシを生成する機能を有する．車載IDPS，クラウドIDSは，参考文献[4]の分類を用いると，シグネチャ型と，機械学習を想定したビヘイビア型に分けられ，本稿ではシグネチャ型のポリシをルール，ビヘイビア型のポリシをモデルと呼ぶ．未知攻撃をクラウドIDSで抽出する理由は，車両の計算能力では大量のログデータの分析が困難であること，および複数の車両間の相関分析が困難であるためである．

なお本稿では，クラウドで生成したポリシを車載IDPSへ反映させる配信・更新機能については，OTA

（Over-The-Air）によるアップデート機能と同様のため検討対象としない.

3.1 車両監視システムの要件

本節では，車両監視システムの備えるべき要件とその理由について述べる.

要件1：「既知攻撃に対して，攻撃の状況（攻撃の進行度やその経路）を車両で把握し，把握した状況に応じた対応へつなげられること．さらに，攻撃の分析に必要なログデータを収集・保存できること．ただし，クラウドへの常時接続は必須としない.」

攻撃者は，通常，車両が外部とつながる接点（ネットワーク境界）を介して侵入してくる．車両の場合，ネットワーク境界は，3G/4Gなどの携帯網を利用する通信モジュールや，Wi-Fi (注2)，Bluetooth (注3)，スマートフォンを利用したテザリング機能を用いて通信するIVI，インフラや他の車両と通信するV2X（Vehicle to Everything）通信モジュールなどである.

車両で攻撃の発生を検知した場合に，ネットワーク境界に対する攻撃が現在行われているのか，あるいは既にそこが突破され，例えばGW ECUなど，内部のECUに対しても攻撃が進行しているのかを的確に把握することは，検知した後に取るべき対応の選択において非常に重要となる．攻撃者がネットワーク境界を攻撃中の場合は，車外との通信を遮断することで一時的に攻撃を回避することができるが，攻撃者が車両内部への侵入に成功している場合は，通信の遮断だけでは不十分であり，例えば，GW ECUで特定のCANコマンドをブロックして攻撃を回避するなどの対応が求められる.

さらに，車両をコントロールするアクチュエータへの攻撃などは人命に関わるため，リアルタイムで一時的な対応が行われるべきであり，通信できないエリアであってもそれらは実施される必要がある．例えば，通信可能なエリアで車両内へマルウェアを混入させ，通信できないエリアまで潜伏させた後，マルウェアを発動させることも可能であるため，通信できないエリアでの攻撃も想定しておくことが求められる.

要件2：「攻撃の進化に備え，クラウドで新たな攻撃を分析・抽出して，新たに既知攻撃として定義し，車載IDPSのポリシを更新できること」

攻撃が常に進化し続けることはITセキュリティ分野では常識となっており，車載セキュリティ分野においても同様であると考えられる．そのため，出荷時に想定していなかった攻撃を，さまざまなログデータから分析・抽出し，実態を解明したのち，既知攻撃として新たに定義することは非常に重要となる．さらに，新たに既知攻撃として定義した攻撃を，出荷済みの車載IDPSのポリシに反映させ最新に保つことで，出荷済みの車両においても検知できる攻撃のバリエーションが増えることにより安全性が高まる.

3.2 車両監視システムの実現に向けた課題

本節では，3.1節で挙げた要件を実現する際の課題について考察していく.

要件1の課題：車両内で攻撃の進行度やその経路を的確に把握するためには，単一のECUへの車載IDPSの配置のみではその実現は困難である．車載IDPSを車両の各所へ配置し，さらにそれら配置した車載IDPSと連携して，車両全体の攻撃の状況を把握できるような仕組みの構築が課題である.

要件2の課題：クラウドで新たな攻撃を抽出するためには，分析に十分なログデータを車両から収集することと，収集したログデータから新たな攻撃を見つけ出すことの2つが課題である．なお，大量のログデータから可能な限り自動で必要な攻撃情報を抽出する課題については参考文献[5]に記載があり本稿では議論しない.

4. 車両統合監視・対応システムの提案

4.1 提案する車両監視システムの概要

本節では，車両監視システムの具体構成を提案し，当該車両監視システムの要件，および課題を検討する．初めに車両監視システムを構成する機能の定義を行う.

車載統合監視機能：車両に配置され，多層防御の各層，具体的には，インターネットなどの外部ネットワークと接続する通信モジュールやIVIなどのコネクティッドECU，コネクティッドECUと車両内部を分けるGW ECU，アクチュエータなどを制御するエンドポイントECU，それらECUを接続する車載NWの各層からログデータなどを収集し保存する．車載統合監視機能は，各層に分散配置した車載IDPS（詳細については後述する）からログデータを収集し，収集したログデータに基づき，どの層がどのような攻撃にさらされているか，あるいは車載NWのどの経路を通って攻撃が進んでいるかを把握する．本稿では，GW ECUへの配置を想定する.

データ送信機能：車両に配置され，車載統合監視機能において収集・分析・保存されたログデータをクラウドへ送信する．送信をコントロールする機能は車載統合監視機能の内部に配置されるが，実際の通信機能は車両に

（注2）Wi-Fi Allianceの登録商標または商標.
（注3）Bluetooth SIG, Inc.の登録商標または商標.

複数存在する既存の通信装置とする．本稿では，コネクティッドECUのうち，通信モジュールの3G/4Gなどの携帯網通信，IVIに搭載されたWi-Fi，Bluetooth，およびIVIに接続されたスマートフォンを利用したテザリング，ならびにV2Xによるインフラや他の車両経由の通信などを想定する．

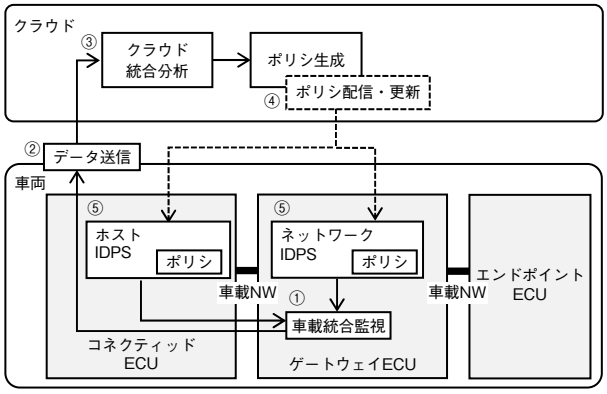
車載IDPS：車両の各所に配置され，攻撃の検知後，攻撃を検知した旨，および攻撃に関連するログデータを車載統合監視機能へ車載NWを介して送信する．さらに，何らかの方法で攻撃に対応する機能も備える．例えば，ECUへの侵入であれば，侵入されたプログラムの停止や削除，前記プログラムからの実行命令を破棄することにより対応する（ホストIDPS）．車載NWへの侵入であれば，ネットワーク上を流れるメッセージの受信を拒否したり，メッセージを無効化したりすることで対応する（ネットワークIDPS）[6]．本稿では，ホストIDPSをコネクティッドECUへ配置し，各ECUが接続するGW ECUへネットワークIDPSを配置する．また，各車載IDPSの検知機能は，ポリシの更新により，クラウドで新たに定義された既知攻撃（元々は未知攻撃）に対応可能であるとする．

クラウド統合分析機能：クラウドに配置され，車両から収集したログデータから未知攻撃に関わる情報を抽出し分析を行う．分析により攻撃の内容や侵入経路などの詳細を明らかにして攻撃の実態を把握する．分析過程では機械学習などの技術を活用して自動化を行い，可能な限り属人性やミスによる検知漏れを低減する．ただし，人命に影響する可能性がある機能であるため，現時点の技術レベルでは最終的な判断は人が実施することが望ましい．

ポリシ生成機能：クラウドに配置され，クラウド統合分析機能による未知攻撃の分析結果に基づき（分析が完了した時点で新たな既知攻撃となる），新たな既知攻撃を検知するためのルールや，攻撃をクラスタリング可能なより高精度なモデルを作成する．本機能についてもクラウド統合分析機能と同様に，可能な限り自動化し，最終確認を人が実施することが望ましい．

次に，定義した各機能の関係について，**第2図**を用いて説明する．車両の出荷時点では，車載IDPSはあらかじめ設定されたポリシに従い，既知攻撃を検知して対応する．さらに出荷後は，各機能は以下に示すとおりに動作する．

① 車載統合監視機能は，各所に配置した車載IDPS（ホストIDPS，およびネットワークIDPS）が既知攻撃を検知した場合，攻撃に関するログデータを収集して分析・保存する．ログデータの収集方法については4.2〔1〕項で述べる．



第2図　車両統合監視・対応システム
Fig. 2　Automotive IDPS

② データ送信機能は，車載統合監視機能の指示に従い，ログデータをあらかじめ定められた方法・タイミング・頻度でクラウドへ送信する．

③ クラウド統合分析機能は，車両から受信したログデータを分析する．分析方法については，4.2〔2〕項で述べる．

④ ポリシ生成機能は，クラウド統合分析機能による分析結果からポリシを生成する．また，ポリシ配信・更新機能が車載IDPSのポリシを更新する．

⑤ 車載IDPSは更新されたポリシを利用して，攻撃を検知し対応する．

4.2　提案する車両監視システムの詳細

〔1〕要件1の実現に向けて

開発完了時までに判明している既知攻撃については，各ECUに配置した車載IDPSにおいて検知，あるいは検知後の対応が実施できるように設計する．各車載IDPSは，異常を検知した際，検知した異常とその周辺のログデータを車載統合監視へ送信し，それを受け取った車載統合監視は，あらかじめ保持する当該車両の車載NWに関する情報（各ECUの接続情報など）と，異常が検知されたECUを対応付けることで，どこから攻撃者が侵入し，どこまで攻撃が進んでいるかを把握する．一方で，異常を検知できず見逃す車載IDPSが存在する可能性もあり，異常を見逃した車載IDPSからはログデータが送信されない．車載統合監視は，異常を検知した車載IDPSの攻撃経路上で隣接して配置された車載IDPSのうち，異常を検知していない車載IDPSが存在する場合，当該車載IDPSへログデータをリクエストすることにより，異常を検知できず見逃した可能性のある車載IDPSからもログデータの収集を行う．

また，車載IDPSにより異常が検知された場合のログデータから見た，攻撃と故障・想定外運転操作との最大の

違いは，故障・想定外運転操作のログデータの大半は車載NWやエンドポイントECUに集中するのに対して，攻撃はコネクティッドECUやGW ECUに集中する点である．攻撃の最終目標を車載NW経由でエンドポイントECUを不正に制御することであると仮定すると，多層防御の各層を突破しつつ攻撃に成功すると，最終的にはコネクティッドECUからエンドポイントECUまでの全ての経路において攻撃の痕跡が残ることになる．つまり，攻撃と故障・想定外操作を分離できるように，各層のログデータに残る攻撃の痕跡を関連付けることがポイントとなる．

ここでは，Sen Nieらの攻撃[3]を具体例として，攻撃の関連付け方法を考察する．この攻撃では，最初にIVIに相当する機器をWi-Fi経由で乗っ取る．次にIVIからGW ECUのFirmwareを書き換え，最後にGW ECUから，エンドポイントECUを停止させる診断コマンドの送信や，エンジンをオフするコマンドの送信が可能となる．最初のステップではIVIのブラウザの脆弱（ぜいじゃく）性やKernelの脆弱性を利用しているため，例えばLinux OS (注4) のセグメンテーション違反（segfault）やKernelのログに痕跡が残る可能性がある．次にGW ECUには，Firmwareの更新情報やFirmware更新の際の認証情報に痕跡が残る可能性がある．最後に車載NW，およびエンドポイントECUにおいては，走行中という想定外の状態での診断コマンドの受信や，エンジンをオフするコマンドの受信の痕跡が残る可能性がある．GW ECUの痕跡だけでは正規の手順である可能性もあるが，コネクティッドECUにも痕跡が存在する場合は，攻撃である可能性が大きく高まる．さらに車載NWやエンドポイントECUでの痕跡まで存在すれば攻撃であることがほぼ確実となる．このように，コネクティッドECUの痕跡から，GW ECU，車載NW，およびエンドポイントECUの痕跡と関連付けることで，単独の痕跡だけでは攻撃と判断しにくい不正コマンドの痕跡も攻撃と判断できる．一方，単独のコマンド異常は，故障である可能性やドライバーの想定外操作である可能性が高いとも判断できる．

〔2〕要件2の実現に向けて

収集したログデータから新たな攻撃を抽出する技術として，観測対象の振る舞いをモデル化し，そのモデルから逸脱した事象を攻撃として判定するビヘイビア型の検知技術がある．ビヘイビア型の検知技術では1つのモデルで複数の攻撃を検出することが可能である．観測対象からモデルを生成する1手法として機械学習の利用が提案されている．ここで，1つの攻撃から亜種の攻撃をどこまで類推して，対応可能なポリシを作成できるかが実現のポイントとなる．この実現には攻撃データから着目する特徴量をいかに効率的に抽出するかが重要となるため，Deep Learningのように特徴量の抽出を自動で行う技術の適用が期待される．

これまでにも，機械学習を適用した攻撃検知の取り組みは行われており，車載システムに特有のCANを対象にした検知技術は広く研究されている[7]-[10]．しかしながら，車載EthernetやECUの内部動作に対して機械学習を適用した検知技術の取り組みはCANに比べて少ないため，今後は，車載システム全体をモデル化し，攻撃を検知していく取り組みも期待される．

（注4）The Linux Foundation の登録商標または商標．

5. まとめ

本稿では，コネクティッドカー向けの車両統合監視・対応システムを提案して，当該システムの実現に必要な要件を定義した．また，課題の検討を行い，その実現性についても示した．

今後は，提案システムをより細分化，詳細化し，さらなる要件の洗い出しと，洗い出した要件を実現するための研究開発が必要である．

現在，コネクティッドカーの準備が着々と進められている一方で，それらに対するセキュリティの検討が十分に追従できていない可能性もあり，早急な車両統合監視・対応システムの具現化が望まれる．

参 考 文 献

[1] S. Checkoway et al., “Comprehensive Experi- mental Analyses of Automotive Attack Surfaces,” 20th USENIX conference on Security, San Francisco, Aug. 2011.

[2] Miller C et al., “Remote Exploitation of an Unaltered Passenger Vehicle,” DEFCON 23, Las Vegas, Aug. 2015.

[3] Sen Nie et al., “FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS.” black hat USA, Las Vegas, July 2017.

[4] Robert Mitchell et al., “A Survey of Intrusion Detection Techniques for Cyber-Physical Systems,” ACM Computing Surveys, vol. 46, issue 4, 2014.

[5] 佐々木崇光 他, “車載向けセキュリティシステムの運用コストを削減する監視データ量削減方式,” 2017年暗号と情報セキュリティシンポジウム（SCIS2017）那覇, Jan. 2017.

[6] T. Matsumoto et al., “A method of preventing unauthorized data transmission in controller area network,” Vehicular Technology Conference, IEEE 75th, Québec, Sept. 2012.

[7] T.Haga et al., “Automotive SIEM and Anomaly Detection Using Sand-Sprinkled Isolation Forest,” 15th escar Europe, Berlin, Nov. 2017.

[8] Jan Holle, “Automotive Intrusion Detection and Prevention System (IDPS)”, EscarAsia, Tokyo, Sept. 2017.

濱田芳博 他, “相関データによる車両データモデルを用いた車載ネットワーク向けアノマリ検知,” 2018年暗号と情報セキュリティシンポジウム（SCIS2018）, 新潟, Jan. 2018.
[9] 小山卓麻 他, “機械学習により機能毎に最適な分析方式を適用する車載ネットワーク異常通信検知方法の提案”, 2018年暗号と情報セキュリティシンポジウム（SCIS2018）, 新潟, Jan. 2018.

執筆者紹介

中野　稔久　Toshihisa Nakano
オートモーティブ社　開発本部
R&D Div., Automotive Company

安齋　潤　Jun Anzai
オートモーティブ社　開発本部
R&D Div., Automotive Company
博士（工学）

今本　吉治　Yoshiharu Imamoto
オートモーティブ社　開発本部
R&D Div., Automotive Company

横田　薫　Kaoru Yokota
オートモーティブ社　開発本部
R&D Div., Automotive Company

鳥崎　唯之　Yuishi Torisaki
オートモーティブ社　開発本部
R&D Div., Automotive Company