Vol.2021-DPS-186 No.27
Vol.2021-CSEC-92 No.27
2021/3/15

車載エレクトロニクスへのサイバー攻撃を解析するための三層型ログ保全技術の提案

五十嵐貴久[1]　松井俊浩[1]

概要：昨今の自動車には、多数のECUが搭載され、パワートレーンを始め、あらゆる機能がECUによって制御されている．車載技術進歩により自動車に対する脅威の入口は増加し、サイバー攻撃も多種多様化されることが予想される．自動車事故が発生した場合に、最初にサイバー攻撃によるものか、ヒューマンエラー、システムエラー等のサイバー攻撃以外によるものかを切り分ける必要がある．サイバー攻撃によるものであった場合、サイバー攻撃の解析を可能にするデータフォレンジック機能として車載ログシステムの必要性は、ますます高まるだろう．本稿では、攻撃者から車載データを保護するため、三層型ログ保全技術を提案する．

キーワード：自動車，ログ，サイバー攻撃，セキュリティ，保護

Proposal of Three-Layered Log Integrity Technology for Analyzing Cyber-Attacks on In-Vehicle Electronics

TAKAHISA IGARASHI[†1]　TOSHIHIRO MATSUI[†1]

Abstract: As modern cars are all controlled by ECUs, they also attract Cyber-Attacks. Cyber-Attacks are also expected to diversify. When a car accident occurs, it is necessary to distinguish whether the cause is Cyber-Attacks, human error, or system error. If it was due to Cyber-Attacks, the need for in-vehicle logging system will increase more and more.
In this paper, we propose Three-Layered Log Integrity Technology (TLLIT for short) in order to protect in-vehicle data from attackers.

Keywords: Automotive, log, cyber attack, security, protection

1. はじめに

自動車は、2000年代以降、ECUをCANで接続する電子制御が一般化している．最近は、テレマティックスと呼ばれるように、自動車の車載ネットワークと公衆網の接続が進展しており、さらに自動運転化の波において、自動車は、車載あるいはクラウドの AI によって操縦される方向にある．このような自動車のIoT化により、サイバー攻撃から自動車セキュリティの確保が重要な問題として浮上している．これからは、事故原因にサイバー攻撃という新たな可能性を含めて、事故原因を探ることになる．事故原因をヒューマンエラー、システムエラー、サイバー攻撃のいずれかを判別し、サイバー攻撃によるものであった場合、その経路・手口を明らかにするため、車載ログシステムは必須の技術となっている．

2. 本研究の成果概要

2.1 本研究の想定車両

本研究は、コネクテッドカーや2020年4月1日 道路運送車両法改正（自動運行装置）により、近い将来公道にて運行される人が運転操作に関与する自動運転レベル 3、車載プロトコルは、CAN が中心的役割を持つ自動車を想定している．

2.2 本研究の目的

本研究の目的は、自動車内での攻撃の流れを裏付け、自動車に対するサイバー攻撃を判別し、解析するために記録するべきデータ・記録場所の条件を明らかにし、プライバシー保護も合わせて検討した実装可能な方法を提案すること．

2.3 研究成果

(1) 三層型ログ保全技術の提案

車載ログ・データを保全するにあたって、記録するべきデータ・優先度・データサイズ・プライバシーに関するデータを整理し、攻撃者からログ・データを保護し、完全性を高めるため、三層型に保全場所を配置する．

(2) 三層型ログ保全技術に対する脅威分析による評価

三層型ログ保全技術を抽象化して作成したDFDから導いたエントリーポイントを基に、脅威分析手法の一つであるSTRIDEにより、自動車が攻撃を受けた場合に保全しているログ・データへの影響に絞って脅威分析を実施した．

3. ログ機能の概要

3.1 ログ機能の基本

ログの管理手法については、NIST SP800-92 「コンピュータセキュリティログ管理ガイド」[2]には、以下のように定義されている．

Vol.2021-DPS-186 No.27
Vol.2021-CSEC-92 No.27
2021/3/15

「ログ」は、組織のシステムおよびネットワーク内で発生するイベント（事象）の記録である

ログの一般的な用途は、故障診断、トラブルシューティング、異常検知のようにシステムやネットワークの運用管理に使用されている.

3.2 ログの有用性

ログの有用性は、以下の４点が挙げられる.

1. 故障診断、トラブルシューティング、異常検知
2. 技術進歩への貢献
3. 想定外のコスト回避
4. 犯罪抑止効果・不正を暴く証拠・否認防止

このうち、本研究では、4 に着目している.

ログは、システムの動作状況を、イベント発生の都度、正確かつ継続的に記録した帳簿であるがゆえに、虚偽性が少なく信頼性が高い. 裁判でもログは有力な証拠となることから、ログの入手は「捜査の基本作業」とされている.

3.3 責任所在の明確化

先進車による事故が発生し、運転手の供述と自動車の挙動に食い違いが発生した場合に、発生原因を以下の 3 つに切り分ける必要が生じる.

1. ヒューマンエラー
2. システムのエラー
3. 第三者によるサイバー攻撃

このときにログの存在は、有効に働くといえる.

3.4 民事責任の所在

自動運転車が交通事故を発生した場合、自動車損害賠償保障法における責任の所在について判断をするために、「運行供用者」の該当性を判断しなければならない.

肥塚[3]は、以下のように、考察している.

自動運転車が第三者にハッキングされ第三者の遠隔操作によって事故が惹起された事案では，第三者の遠隔操作による事故であることの立証に成功する限り，保有者に「運行支配」も「運行利益」もなく，「運行供用者」とは認められない

これは、第三者の遠隔操作による事故であることの立証に成功しなければ、「運行供用者」該当性での争いが生じる可能性について示唆している.

4. サイバー攻撃へのログ機能対応状況調査

4.1 各自動車メーカーのサイバー攻撃にする対応状況

各自動車メーカーのサイバー攻撃への対応状況は、CAN ID のように元々公開されていない情報もあることから、正確なことは不明ではあるが、2015 年の米国のエドワード J. マーキー上院議員のレポート[4]が参考になる.

エドワード J. マーキー上院議員は、新しい技術がアメリカ人のプライバシーを危険にさらしたり侵害したりしないようにするために、主要自動車メーカーに質問書を送って、ハッキング攻撃、および個人の運転情報の管理方法を保護への対応状況を調査した.

エドワード J.マーキー上院議員は、各社からの回答から以下の事項が判明したとしている.

自動車メーカーは、運転履歴と車両性能に関する大量のデータを収集している.

さらに、自動車メーカーの多くは、収集したデータをワイヤレスでデータセンターに送信している.

エドワード J. マーキー上院議員の報告書によると、回答を得た各社の取得データ項目は、位置情報や平均燃費、タイヤの空気圧、バッテリーの状態といった項目とされており、サイバー攻撃を判別するには、外部との通信ログ、攻撃の入口となりやすいインフォテイメントシステムのログ・データ、攻撃の入口から制御系 ECU までの経路を追跡できるだけのログ・データが不十分な内容といえる.

4.2 フォレンジック対応ログへの動向

自動車に対するサイバー攻撃の解析に有効なログ機能実装に向けた海外の動向と国内の動向について説明する.

4.2.1 海外の動向

2020 年 6 月 24 日、UNECE WP.29（国際連合欧州経済委員会の自動車基準調和世界フォーラム）において、自動車のサイバーセキュリティ国際基準[5]が、採択された.

この国連規則において、承認機関の確認事項（第 5 章 承認）には、以下のように記載されている.

> *Log data to support the detection of cyber-attacks and provide data forensic capability to enable analysis of attempted or successful cyber-attacks.*

これは、自動車に対するサイバー攻撃に対応する上で、サイバー攻撃を解析可能とする車載ログシステムは必須機能であることを示している.

4.2.2 国内の動向

自動運転車を日本国内の公道を走行させるための法整備が進められ、2020 年 4 月 1 日、改正道路運送車両法が施行された. 同改正により、自動運行装置を備えることができるようになり、作動状態記録装置の技術基準が追加された. 作動状態記録装置の技術基準は、主に運転手とシステムの交代関連の記録となっており、自動車に対するサイバー攻撃に対応する内容ではなかった.

4.3 現状の車載ログの問題点

- 現状は、メンテナンス・サービス向上を目的としたログ取得機能であり、サイバー攻撃を対象とした統合的なログ・データ保全機能について、標準化した技術はないこと
- Head Unit ,ECU ,EDR 等の車載機器が生成したデータは、保全していない若しくは、個々に保全しており、統合管理する仕組みがないこと
- ログを改ざん・消失から保護する仕組みが不十分であること

Vol.2021-DPS-186 No.27
Vol.2021-CSEC-92 No.27
2021/3/15

5. 車載ネットワークの概要

5.1 車載ネットワーク構成

車載ネットワークは、図 1 のようなクラウド層、インターネット層、フォグ層、車載ネットワーク層、エンドポイントデバイス層で構成される 5 層構造をとっている．エンドポイントデバイス層と車載ネットワーク層は、異なるプロトコルと機能ごとにサブネットワークで分割し、複数のゲートウェイで接続する構成をとっている．

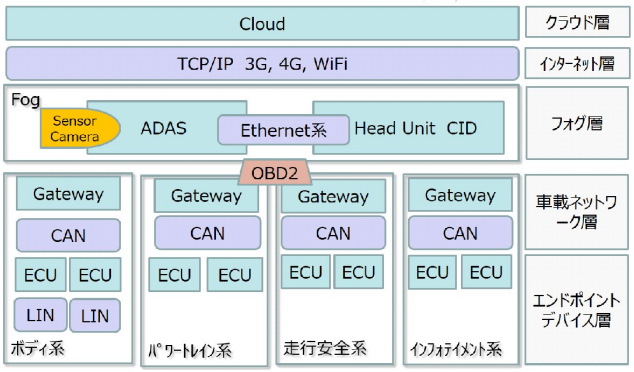

図 1 車載ネットワーク構成図

Figure 1 In-vehicle network diagram

2010 年ころから、自動車に対するセキュリティが意識され始め、研究により攻撃経路も、明らかにされてきた．

Florian らは 2010 年から 2019 年までの間に研究発表された自動車への攻撃を調査しまとめた攻撃リスト Automotive Attack Database [6]に掲載されていた攻撃ポイントを図 1 上に示すと図 2 のようになる．

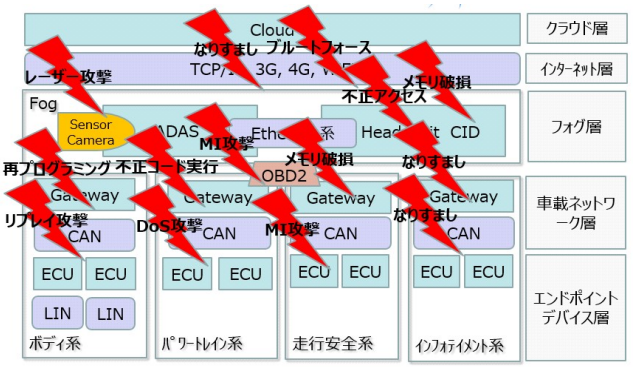

図 2 攻撃ポイント

Figure 2 Attack points

5.2 車載ネットワークプロトコル

車載ネットワークは、CAN、LIN、Ethernet、MOST といった様々な用途・特徴を持ったプロトコルが 1 台の自動車の中に同居している．この中でも、CAN は中心的な役割を果たしているプロトコルである．CAN は、耐ノイズ性、エラー検出機能等優れた点もあるが、メッセージインジェクション攻撃、DoS 攻撃に対して脆弱であることが知られている．

6. 先行研究

6.1 CAN へのリモート攻撃

ジープチェロキー対して、不正な CAN メッセージを流し車両を制御するリモート攻撃を行った研究の論文を紹介する[1]．同論文は、自動車セキュリティ関連の 700 を超える論文に引用されており自動車セキュリティについて検討する必要性に対し、大きなインパクトを与えたことが分かる．

それまで車内の CAN に直接デバイスを取り付けることで自動車を制御できることが分かっていたが、それでは攻撃ポイントが限られる．自動車が、ワイヤレスネットワークを通じて外部から制御できるとなれば、アタックサーフェスは一気に拡大する．2015 年、Charlie Miller らは、図 3 の流れで通信回線からインフォテイメントシステムに侵入し、ファームウェアを再プログラミングすることで任意の CAN メッセージを送信することに成功した．

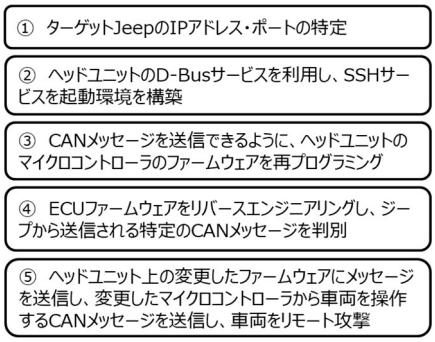

図 3 攻撃フロー

Figure 3 Attack flow

攻撃フローのそれぞれの段階において、図 4 のように対応したログ・データを記録したのなら、Jeep 車への攻撃は解析可能と考える．

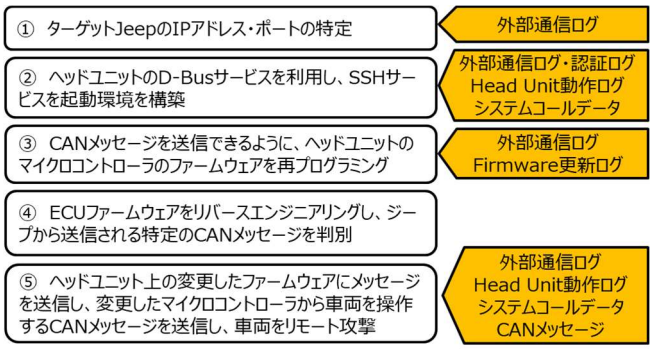

図 4 攻撃フローと対応するログ・データ

Figure 4 Attack flow and corresponding log

6.2 ワイヤレスから CID を経由した CAN バスへの攻撃

Sen Nie らの研究は、Tesla Model S の CID（Central Information Display）にワイヤレスにて侵入し、CID、Gateway に残されていた脆弱性を利用し、CAN バス上へ不正な CAN メッセージを送信するリモート攻撃に成功した[7]．Sen Nie らによる攻撃方法の大まかな流れは、図 5 に示すとおりである．

Vol.2021-DPS-186 No.27
Vol.2021-CSEC-92 No.27
2021/3/15

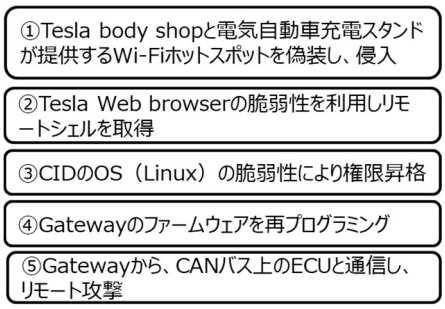

図 5　攻撃フロー

Figure 5 Attack flow

攻撃フローのそれぞれの段階において、図 6 のように攻撃の証跡を記録できるログ・データを対応させた．それぞれのログを保全していたならば、Tesla 車への攻撃は解析可能と考える．

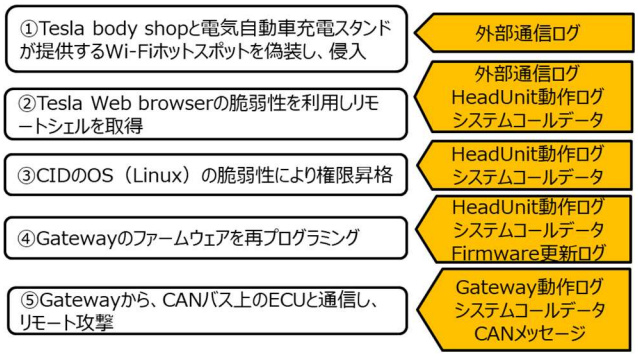

図 6　攻撃フローと対応するログ・データ

Figure 6　Attack flow and corresponding log

6.3 車載 IDS の調査研究

O.Y. Al-Jarrah らは、車載ネットワークの最新の IDS に関する研究論文（42 論文）について使用されている検出技術、機能と機能の選択方法、評価データ、性能測定基準、標的型攻撃に焦点を当てて、現況を詳細に説明していた[8]．

課題として、以下の 3 点を挙げていた．

- １つの検知手法で、全ての車内ネットワーク攻撃を網羅できない．しかし、限られたリソース・リアルタイム性確保の問題があり、複数の IDS を稼働は現状困難である
- 81%の論文は、侵入を識別するためにシステムの通信とデータの側面のみに依存しているので、フィジカルな特徴（速度、エンジン回転数など）を利用することが適切と考える
- システムが侵入にどのように対応する必要があるかについては検討が不十分であった

論文の中では、攻撃検知に有効な手法は提案されているものの、攻撃を完全に検知・無効化するものはないとされていた．

6.4 マルウェアによる攻撃の証拠データ保全手法の研究

大平らは、カーナビ等の車載インフォテイメントシステムへ侵入するマルウェアからの検知・妨害に対する耐解析性を高める目的として、OS カーネル上にフォレンジック機構をデバイスドライバーとして組込み、マルウェアによる攻撃の証拠データ保全手法を提案している[9]．

大平らは、Linux ベースの装置をターゲットとするマルウェア Mirai に CAN への DoS 攻撃コマンドを追加し、車載 LAN を攻撃する実験を試みた．

大平らは、すべてのシステムコールをフックすると証拠データ量の増大・システムパフォーマンス低下を防ぎ、効率的にマルウェアの挙動を観測するため、証拠保全を行う４つのシステムコール（write、recvmsg、open、sendto）に限定しデータ収集を試みた．実験結果は、保全された証拠データに Mirai の攻撃時の特徴的な振る舞いを確認できたと結論付けている．

7. 三層型ログ保全技術の提案

7.1 リモートログ収集の多層化の一般的な実装例

リモートログ収集の多層化の一般的な実装例として、rsyslog が挙げられる．rsyslog は、様々な出力元からログを統合し、データベースサーバ等に転送する機能を持っている（図 7）．攻撃者から，ログを保護するために、別のセキュリティドメイン内にログを保全する多層化の考えは、一般的な流れとなっている．本研究は、さらに保全優先度、保全場所の特性、データ量を検討して分散保全する手法を提案する．

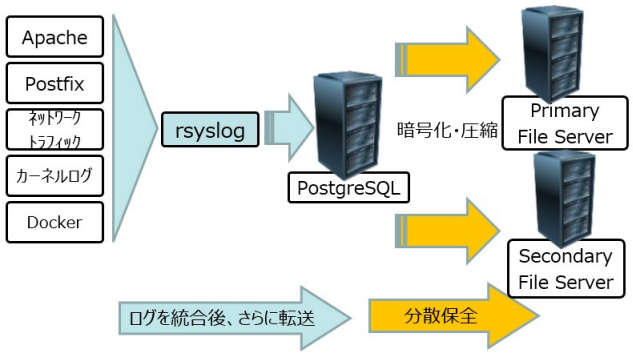

Figure 7　rsyslog log collection model

図 7　rsyslog のログ収集モデル

7.2 記録するログ・データの構成

攻撃リスト Automotive Attack Database [6]から脅威の入口、攻撃経路にあるログ・データを記録するべきデータとして表 1 のようにまとめた．

ここに挙げたデータが改ざんされている疑念を排除できなければ、公判において証拠能力は、失われてしまう．データは残っているだけでは、不十分であり、改ざんされていないことを担保する「非改ざん証明」が必須となる．改ざん検知（完全性維持）に使用する Hash 値を保護するため、ログ・データの Hash 値を実データとは別に保管する仕組みが必要である．

Vol.2021-DPS-186 No.27
Vol.2021-CSEC-92 No.27
2021/3/15

表 1　ログ・データ構成

Table 1　Log and Data constitution

		生成元	記録すべき情報	生成頻度	ビットレート	ログ・データHash値管理
ログ	通信ログ	Head Unit	TCP/IP通信 Wi-Fi通信 Bluetooth等	通信発生時	1チャネル 約2kbps	1つのログ・データは、512bitのハッシュ値に約96byteのヘッダーを付加して管理する。
		OTA				
	認証ログ	Head Unit	−	認証時	約1kbit	
	動作ログ	Head Unit	−	常時	ログ1種類につき 約30kbps	
		Gateway	−			
		ECU	−			
実データ	車載LAN	CAN	トラフィックデータ	常時	最大 約1Mbps	
		Ethernet			最大 約97Mbps	
		FlexRay			最大 約9Mbps	
		MOST			最大 約145Mbps	
		LIN			最大 約0.1Mbps	
	システムコールデータ	Head Unit		1プロセス	約312kbps	
センサー	カメラ		動画データ	常時	約14Mbps	
	LiDAR		センシング情報	常時	約4~263Mbps	
	GPS		GPS情報	毎秒	Max 164bps	

表 1 に示されているデータは、通常運行時のデータとなる．これ以外にも、今後、迅速なソフトウェア更新技術として導入が進むと予想される OTA は、攻撃の入口ともなりえることから、意図しないソフトウェア更新がされていないか監査するために OTA の実施記録（表 2）も保全するべきと考える．

表 2　OTA 関連データ

Table 2　OTA related data

	生成元	記録すべき情報	生成頻度	サイズ	Hash値
OTA実施後の検証情報	OTAマスタ	実施記録	月に1回	約1.9Mbit	512bit
	Head Unit	ソフトウェアのHash値			512bit
	Gateway				2kbit
	ECU				50kbit

7.3　保全場所特性の比較

On-board と Cloud を比較し、それぞれの保管場所としての特性を表 3 のようにまとめた．捜査機関が迅速に捜査を進めるにあたって、データアクセス容易性は重要である．データ解析着手時期の遅れが、その後の捜査進展を大きく左右することもある．

表 3　保全場所特性の比較

Table 3　Comparison of storage location characteristics

	On-board	Cloud
保存リアルタイム性	あり	劣る
捜査機関のデータ回収容易性	インターフェース次第 令状の必要可能性もあり	サーバが国内でも令状可能性大 海外サーバは、ICPO経由
通信料	なし	あり
外部ネットワーク転送容量制限	−	あり
データ欠落（外部ネットワーク通信時）	−	回線不備により大幅に欠落する可能性がある
データ欠落（転送時の仕様依存）	生成元に近いほど、RAWデータ	転送項目の仕様依存
情報漏洩（Privacy保護）	物理的な侵入や盗難の虞	通信路の不備・内部犯行

証拠データがオンボードに保全されていたとしても、そのデータを抽出するために機器の破壊、メーカー等に解析を要請する必要があるようでは、裁判所が発付する令状の必要性が生じる．捜査機関等のデータアクセス容易性を確保した認証・暗号化の仕組みを持たせる必要がある．

7.4　ログ・データの保全優先レベル

優先レベルを表 4 のように「発生原因切り分けレベル」、「攻撃経路・攻撃手法解析レベル」、「先進機能実データ保全レベル」の 3 段階に分けた．

表 4 保全優先レベル

Table 4 Integrity priority

	取得ログ・データ項目	事業用（バス、トラック等）	自家用 ハイエンドモデル	自家用 ローエンドモデル
高	発生原因切り分けレベル	攻撃の入口（外部との接続口）攻撃の出口（直接的な指令データ）	○	○	○
	攻撃手法解析レベル	攻撃の入口と攻撃の出口を結ぶ経路において生成されるログ・データ	○	○	△
	実データ保全レベル	先進機能実データ（カメラ・センサ）	○	△	△

○：標準装備　　△：オプション設定

(1) 発生原因切り分けレベル

このレベルは、事案発生の原因のみを切り分けるためだけのレベルとなり、最優先で取得しておくべきログ・データとなる．攻撃入口に関するデータは、Head Unit の通信・動作ログ、カメラ（実データ除く検知情報等のデータ）、センサー（実データ除く検知情報等のデータ）等のデータが挙げられる．攻撃出口データは、制御系の ECU 等のエンドポイントデバイスのログや送受信したデータが挙げられる．

(2) 攻撃手法解析レベル

このレベルは、攻撃入口となりやすい Head Unit のシステムコールを含む詳細なデータや攻撃入口と攻撃出口を結ぶ経路に配置されている Gateway、ECU のデータ等、車載ネットワーク全体のデータを取得する．

(3) 実データ保全レベル

このレベルは、自動運転・ADAS に使用されるカメラの画像認識データやセンシングデータの実データを保全する．

バスやトラックは、車体が大きく、バスは乗車人数も多いことから、サイバー攻撃を受けた場合に被害が大きいことから狙われる可能性も高い．これら大型の事業用乗用自動車は、詳細にログ・データを取得しておくべきである．自家用車は、ハイエンドモデルとローエンドモデルでは、かける費用により、取得するログ・データに差がつくであろう．発生原因切り分けレベル以外は、ユーザーの希望により、レベル設定をする．

7.5　三層構造

車載データの完全性を満たして、保全するための技術として、三層型ログ保全技術（Three-Layered Log Integrity Technology（TLLIT））を提案する．

TLLIT は、以下の要件を満たす構造が求められる．

- 盗難・交通事故等の物理的な脅威から保護できる
- 攻撃者から、ログを保護するため、別のセキュリティドメインにログ・データを保存する
- ログ・データを保存するスペースを確保できる
- 捜査機関等によるフォレンジック負担軽減のため

に統合管理する

エンドポイントデバイスは、記憶容量が少なく解析に必要な期間のデータを確保できない．エンドポイントデバイスが設計上、車体の中心から離れた箇所に配置されていると、事故の際に、巻き込まれる可能性もある．データ保護のためエンドポイントデバイスのログ・データを統合し保存しておく必要がある．さらに、統合したログ・データを盗難、オンボードストレージが巻き込まれるような大きな事故から保護するために、車外にログ・データを退避する必要がある．保全するべきログ・データは表 1 のデータサイズなので、この統合したログ・データを全てクラウドにストリーミング送信するには、約 132Mbps の通信帯域を常時求められ、現在普及している 4G 回線では足らない．

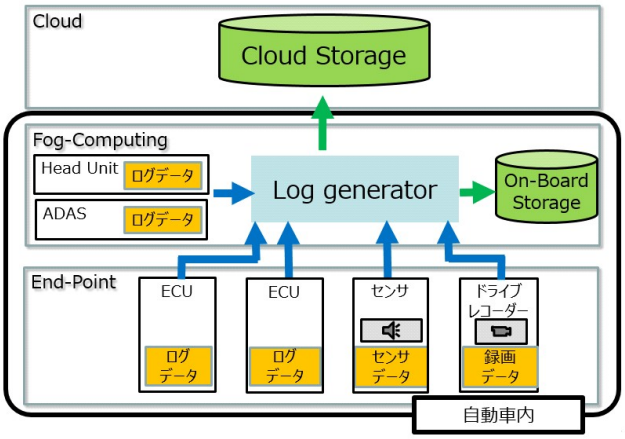

図 8　三層構造

Figure 8　Three-layer structure

車両を 1 日に 1 時間運行した場合の総データ量を算出すると 1 日約 58GB となる．さらに日本の自動車保有台数は、約 8,200 万台(2020 年 11 月現在、一般社団法人自動車検査登録情報協会)を考慮すると、総通信帯域は約 10Pbps、総データ量は約 4500Pbyte となり通信帯域、記憶容量を共に逼迫してしまう．これは日本の固定系ブロードバンド契約者の総ダウンロードトラヒック a（約 19.8Tbps、1 日あたり約 214PB）を上回っている．クラウドに送信するデータは、データ量と優先度から選択するべきである．

TLLIT では、エンドポイントデバイスのログ・データの退避、統合及び通信帯域の制限から、ログ・データの保全構造を図 8 のとおりクラウド層、フォグ層、エンドポイント層の三層構造とした．

7.6 保全場所分類

データの保全場所をデータソースの構成と保全場所の特性を考慮し、表 5 のように分類した．

表 5　車載データ保全分類

Table 5　Classification of in-vehicle data integrity

データ	Cloud Storage	On-board Storage	device	Retention period
IP通信情報	◎ ●	○ ●	○	90days
GPS	◎ ●	○ ●		90days
カメラ	△ ●	○ ●	○	24h
車載LAN（パワートレーン系・インフォテイメント系・走行安全系）	◎ ●	○ ●		24h
車載LAN（ボディー系）	●	○ ●		24h
認証情報	◎ ●	○ ●	○	90days
Head Unit、Gateway(システムコールデータ)	△ ●	○ ●	○	90days
センサデータ	△ ●	○ ●		24h
Head Unit、Gateway、ECU（動作ログ）	◎ ●	○ ●	○	90days
ECU（ソフトウェア Hash値）	◎ ●	●		90days
OTA（実施記録・Hash値）	◎ ●	○ ●	○	90days

●：Hash 値　△：通信帯域を確保でき、送信可能ならば送信するべきデータ

クラウドへのストリーミング送信の可否は、データのビットレートと確保できる帯域幅に依存する．

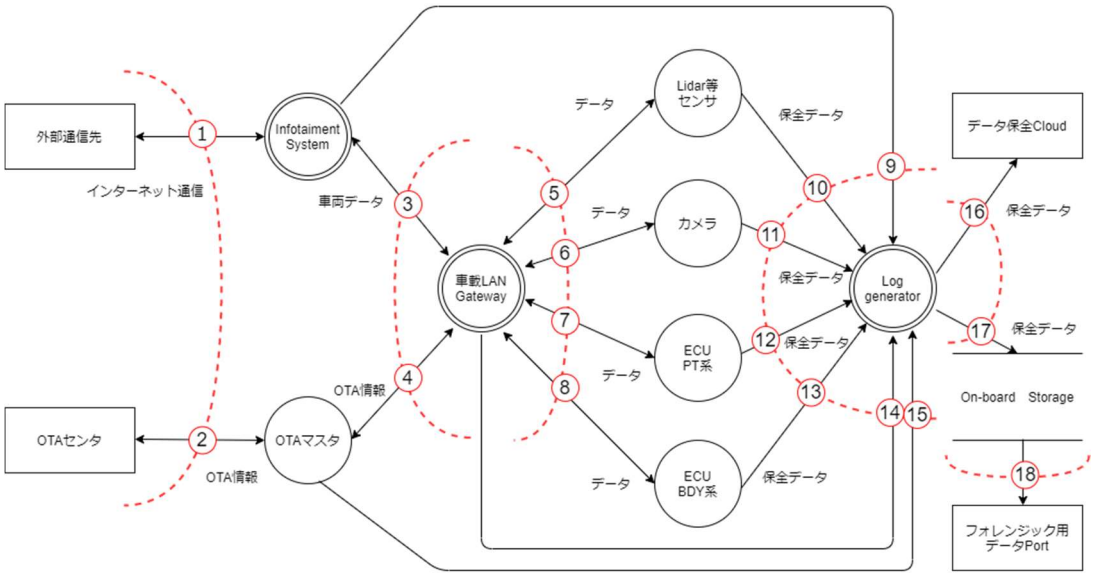

図 9　TLLIT の DFD

Figure 9　TLLIT DFD

a 総務省“我が国のインターネットにおけるトラヒックの集計・試算”2020 年 11 月分の集計結果、https://www.soumu.go.jp/main_content/000731585.pdf

4G 回線を使用した場合の上り帯域 2Mbps 以上とされているので、表 1 を基に、ストリーミング送信での漏れが生じない項目の組み合わせを求めたところ、優先順位の高い発生原因切り分けレベルに、攻撃手法解析レベルのうちシステムコールデータを除いたデータ（◎の項目）は送信可能と考えられる.

8. TLLIT への脅威分析

8.1 TLLIT の DFD

TLLIT を DFD（Data Flow Diagram）によりモデル化する. DFD を車載 LAN については抽象化し、図 9 のように作成した. DFD に、信頼境界線（Trust boundary）を加え、エントリーポイント（境界とデータフローの交点）を求めたところ、18 個のエントリーポイントを得た.

8.2 STRIDE にて脅威分析

各エントリーポイントに対して、STRIDEbによる脅威分析（ログ・データへの影響に絞って）を実行する. 実施結果については、表 6 に示す.

表 6 STRIDE による TLLIT の脅威分析実施結果

Table 6 Results of TLLIT threat analysis by STRIDE

	エントリーポイント		S	T	R	I	D	E
①	外部通信先	Infotaiment System	○	▲	○	▲	▲	○
②	OTAセンタ	OTAマスタ	○	▲	○	▲	▲	○
③	Infotaiment System	Gateway	※	○	○	※	○	○
④	OTAマスタ	Gateway	※	○	○	※	※	○
⑤	Gateway	Lidar等 センサ	※	※	○	※	※	○
⑥	Gateway	カメラ	※	※	○	※	※	○
⑦	Gateway	ECU PT系	※	※	○	※	※	○
⑧	Gateway	ECU BDY系	※	※	○	※	※	○
⑨	Infotaiment System	Log generator	※	○	○	※	×	×
⑩	Lidar等 センサ	Log generator	※	※	○	※	×	×
⑪	カメラ	Log generator	※	※	○	※	×	×
⑫	ECU PT系	Log generator	※	○	○	○	×	×
⑬	ECU BDY系	Log generator	※	○	○	○	×	×
⑭	Gateway	Log generator	※	○	○	○	×	×
⑮	OTAマスタ	Log generator	※	○	○	○	×	×
⑯	Log generator	データ保全Cloud	○	○	○	▲	×	×
⑰	Log generator	On-board Storage	※	×	○	×	×	×
⑱	ﾌｫﾚﾝｼﾞｯｸ用ﾃﾞｰﾀPort	On-board Storage	▲	▲	○	×	▲	▲

○･･･影響の可能性はあるが、保全している別ログ・データにて解析可能な場合
▲･･･部分的影響 ×･･･全面的影響 ※･･･無線接続・不正機器設置にて影響あり

8.3 STRIDE による脅威分析実施結果を考察

STRIDE による脅威分析実施結果から、TLLIT を導入したことにより、完全性は高まったといえる. 攻撃を受けた場合に、システム全体の完全性に大きな影響を与えるポイントは Log generator につながるポイントと分かった. このポイントへの対策は、コストをかける必要がある. 対策例として、ファイアウォールや VPN ソリューションの使用が挙げられる. また、On-board Storage 内の全ログ・データに容易にアクセスできないように、ログ・データの保存場所を認証付き多層構造にする. 車載 LAN 内に物理的に直接、不正な ECU 等を設置された場合、信頼境界線内の出来事になるため、不正機器検出の仕組みがなければ、攻撃の判別は困難と考える. OTA・インフォテイメントシステム・Log generator・フォレンジック用データポート以外に外部との不正なアクセスポイントが設定されないよう、基本的には車内は有線接続を採用するべきである.

9. 結論と今後の課題

9.1 結論

(1) 車載ログシステムは、サイバー攻撃検出の必須機能である

今後、サイバー攻撃は事故原因として、新たに疑うべき要因となるため、車載ログシステムは、必須機能となる.

(2) 車載ログシステムは攻撃経路・攻撃手法を明らかにすることができる

攻撃の入口となりうる車載機器から、各制御系エンドポイントデバイスまでの経路に存在するログ・データを保全することで、サイバー攻撃の証拠となるだけでなく、同様の攻撃手法への対策にも、役立つ.

(3) 三層構造は、車載ログシステムの完全性を高めることができる

脅威分析の結果から、ログ・データを On-board Storage と Cloud に三層構造に保全した方が、完全性は高い結果を得た. 攻撃者により、一部のデータを削除・改ざんされる可能性は残るが、全てのデータを削除・改ざんされる可能性は低減できる.

(4) 保全したログ・データが改ざんされていない担保として「非改ざん証明」の設定が必要である

保全したログ・データが、改ざんの疑いが存在すると証拠として使用できなくなる. 保全しておくだけでなく、改ざん検知のために Hash 値を得ておくことで「非改ざん証明」を設定しておく. この Hash 値は実データとは別に、オンボードとクラウドの両方に保全しておく.

(5) 車載ログシステムに、プライバシー情報の保護技術を組み込む必要がある

ユーザーとしては、GPS 情報・外部通信情報のようなプライバシーに関する情報の保全場所は、気になるところではある. On-board Storage、Cloud のいずれにしても情報漏えいの可能性は捨てきれない. 情報漏えいリスクを抑えるために、認証・暗号化技術を組み込む必要がある.

9.2 今後の課題

(1) 車載ログシステムがユーザーに受け入れてもらえるよう車載ログシステムに「普及させる力」を持たせる

b STRIDE とは、Microsoft により提唱された脅威の分類手法. 対象システムに対し、以下の脅威に対する影響を検討する.
Spoofing：なりすまし Tampering：改ざん Repudiation：否認
Information disclosure：情報漏えい
Denial of service：サービス不能 Escalation of privilege：権限昇格

ユーザーに車載ログシステムの必要性が理解させたとしても、機器搭載の初期費用・クラウド利用料・通信費用を負担してまで、取り付ける必要性を持たせなければ、普及は進まない.

例として、日頃の安全運転状況を記録しておくことで、自動車保険の査定が良くなり、保険料を下がる. 運転状況や数値を記録しておくことで、中古車販売時の品質を検討する上での、判断材料になる. こういった、自動車に TLLIT をつけたくなるようなメリットを検討する必要がある.

(2) ログ・データフォーマットの統一と時系列化できる仕組みの検討

車載機器は、ECU だけでも、最大 150 台搭載されていると言われている. それら車載機器から保全したログ・データのフォーマットが、複数存在すると解析の負担は高くなる. 解析負担を軽減し、可読性を向上させるためログ・データフォーマットの統一は必要と考える.

本提案では、統合分割を繰り返すことから、解析時のタイムライン作成に支障のないよう、ログ・データを統合時に統一されたシーケンス番号を付加するか、若しくはデータの前後を確認できる時間分解能にて各データに日時情報を付加し、時刻同期をとる仕組みが求められる.

参考文献

[1] Charlie Miller and Chris Valasek : Remote Exploitation of an Unaltered Passenger Vehicle, Proc. of BlackHat, pp. 1-91 、2015.
[2] -: NIST SP800-92 「コンピュータセキュリティログ管理ガイド」, 情報処理推進機構 (2006).
[3] 肥塚肇雄 : 自動運転車事故の民事責任と保険会社等のメーカー等に対する求償権行使に係る法的諸問題、平成 29 年度日本保険学会大会, 2017.
[4] Markey J.Edward :Tracking & hacking: Security & privacy gaps put American drivers at risk, pp.12、https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf、(参照 2020-08-05).
[5] ー: Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber Security and cyber Security management system, UNECE WP.29, 2020.
[6] Florian Sommer,Jürgen Dürrwang : AAD: Automotive Attack Database, https://github.com/IEEM-HsKA/AAD, 2019.
[7] Sen Nie, Ling Liu,and Yuefeng Du : FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS、 Proc. of BlackHat, pp. 1-16, 2017.
[8] Omary Y.Al-jarrah, Caraten Maple, Mehrdad Dianati, David Oxtoby, and Alex Mouzakitis: Intrusion detection systems for intra-vehicle networks: A review, IEEE Access, 7, pp. 21266-21289, 2019.
[9] 大平修慈、井上博之、新井イスマイル、藤川和利 :“車載 LAN へ侵入するマルウェアの証拠保全を行うカーネル上のフォレンジック機構”、情報処理学会論文誌 Vol. 60 No. 3, pp. 791-802, 2019.