DoIP と SOME/IP における セキュリティ分析と侵入検知の検討

吉田 圭吾[†1]　濱田 芳博[†1]　足立 直樹[†2]　相羽 慎一[†2]
石川 史也[†2]　上口 翔悟[†2]　上田 浩史[†2]　宮下 之宏[†2]　畑 洋一[†1]

概要：近年，自動運転システムやコネクティッドカーの実現に向けた車載通信の高速化に対する要求が高まっており，既存プロトコルに代わる大容量ネットワークとして，車載 Ethernet が注目されている．一方で，このような車両は，外部接続からサイバー攻撃を受ける危険性があり問題視されている．米国国立標準技術研究所の Framework for Improving Critical Infrastructure Cybersecurity では，サイバーセキュリティ対策として「特定・防御・検知・対応・復旧」を挙げており，セキュリティを考慮した車両運用では，まずサイバー攻撃を検知することが重要である．本稿では，車載 Ethernet の Diagnostics over Internet Protocol(DoIP)，Scalable service-Oriented MiddlewarE over IP(SOME/IP)で想定される攻撃を検討する．さらに，これらの攻撃に対する検知手法の検討を行う．

キーワード：侵入検知，車載ネットワーク，イーサネット，DoIP，SOME/IP，KDD CUP 99 データセット

Survey on security for DoIP, SOME/IP and Study of Intrusion Detection

Keigo Yoshida[†1]　Yoshihiro Hamada[†1]　Naoki Adachi[†2]　Shinichi Aiba[†2]
Fumiya Ishikawa[†2]　Shogo Kamiguchi[†2]　Hiroshi Ueda[†2]　Yukihiro Miyashita[†2]
Yoichi Hata[†1]

Abstract: There has been an increasing need for high-speed in-vehicle network communication for autonomous driving systems recently. Automotive Ethernet is attracting a great deal of attention, instead of conventional in-vehicle protocols. However, there is a possibility that connected autonomous vehicles receive cyber attacks from an external network. According to Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology(NIST), a set of cybersecurity activities consists of five functions: Identify, Protect, Detect, Respond, Recover. To realize secure vehicle operation, at first it is important to detect cyber attacks. In this paper, we will describe attack scenarios through a survey on security of Automotive Ethernet: Diagnostics over Internet Protocol (DoIP) and Scalable service-Oriented MiddlewarE over IP (SOME/IP). Furthermore, we will describe discoveries related to attack detection on SOME/IP and DoIP made during this survey.

Keywords: Intrusion Detection System, In-vehicle network, Ethernet, DoIP, SOME/IP, KDD CUP 99 data set

1. はじめに

近年の自動車には，多数の Electronic Control Unit(ECU)が搭載され，複雑な車載ネットワークが構成されている[1]．さらに，高精度センサを利用した先進運転支援システム，外部接続によるコネクティッドなどの実現に向け，車載通信の高速化に対する要求が高まっている．そこで，既存の車載プロトコル Controller Area Network(CAN)[2]，CAN-FD[3]などに代わる大容量ネットワークとして，Ethernet の車両への適用が注目されており，車載向けの上位プロトコルとして Diagnostics over Internet Protocol(DoIP)[4][5][6][7]，Scalable service-Oriented MiddlewarE over IP(SOME/IP)[8]などの開発，標準化が進められている．一方で，自動運転・コネクティッドカーは外部接続により，サイバー攻撃に晒される危険性があり問題視されている．米国国立標準技術研究所は，Framework for Improving Critical Infrastructure Cybersecurity[9]を発行し，サイバーセキュリティ対策の機能として「特定・防御・検知・対応・復旧」の 5 つを挙げており，セキュリティを考慮した車両運用では，日々進化するサイバー攻撃に対して，攻撃を検知する侵入検知システムの導入が極めて重要である．そこで本稿では，SOME/IP と DoIP に対するセキュリティ脅威に関して調査を行い，想定される攻撃を検討する．さらに，侵入検知システムの研究に用いられる KDD CUP 99 データセット[10]から検知手法を検討する．

1.1 構成

本節以降の構成を示す．第 2 節では車載 Ethernet の DoIP，SOME/IP プロトコルについて概説する．第 3 節では DoIP，

†1 住友電気工業株式会社
SUMITOMO ELECTRIC INDUSTRIES, LTD.

†2 株式会社オートネットワーク技術研究所
AutoNetworks Technologies, Ltd.

SOME/IP のセキュリティ分析について示し．第 4 節では，民生 Ethernet の攻撃検知手法の検討する．第 5 節では，車載 Ethernet の侵入検知手法を検討する．第 6 節では，まとめと今後の展開を示す．

2. 車載 Ethernet

2.1 車載 Ethernet の概要

現在の車両は，多数の ECU から構成される車載ネットワーク通信で制御が行われている．車載通信プロトコルの事実上の標準は，CAN プロトコルである．CAN では，最大 8 バイトのペイロードを持つメッセージをドメイン内の ECU にブロードキャスト送信し，各メッセージに付与される ID による調停が行われることで低遅延な通信を実現している．今後の車両では，高精度センサを利用した自動運転システム，外部接続によるコネクティッドの実現に向け，大容量通信が可能なプロトコルが必要とされている．そこで，コンピュータネットワークの接続技術として確立され，幅広く利用されている Ethernet プロトコルが注目されており，車載への適応が期待されている．

現在，車載対応 Ethernet の通信帯域は，用途に応じて 10M から数 Gbps まで提案されており，最大 1500 バイトのペイロードを持つメッセージが送受信できる．図 1 に示すように，本来 Ethernet 上位プロトコルとしては SOME/IP, DoIP, XCP, AVB 及び ISO15118 などが提案されている．SOME/IP は車両の諸機能をサービスという単位で管理するミドルウェアでアルバイト．DoIP は車両診断やファームウェアアップデート等に用いられる．XCP は車両の内部設定値の測定やキャリブレーションに用いられる．AVB は車載ネットワークの低遅延性の保証，ISO15118 は電気自動車の充電シーケンスに利用される．本稿では，標準化が進んでいる DoIP と SOME/IP についてセキュリティ分析と侵入検知方法の検討を行った．

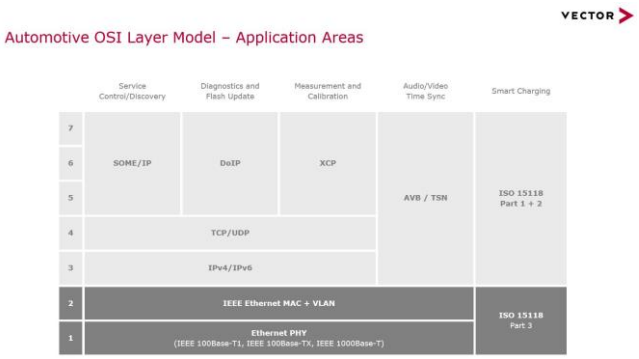

図 1．車載通信のプロトコルスタック[11]

2.2 DoIP プロトコルの概要

DoIP プロトコルとは，ISO 13400 として標準化された，メンテナンス用の外部テスト装置と車両間の診断通信規格である．ISO 13400 では，外部テスト装置がネットワークに接続されている車両を検出し，車両のゲートウェイ及びそのサブコンポーネントと通信するための機構が定められている．また，規格は全 5 部から構成され，第 1 部：一般情報とユースケースの定義，第 2 部：トランスポートプロトコルとネットワーク層のサービス，第 3 部：IEEE802．3 に基づく有線車両インターフェース，第 4 部：イーサネット診断コネクタ，第 5 部：規格適合性試験を規定している．また，プロトコルスタックとしては，OSI 参照モデルの第 1-4 層に第 2-3 部が対応していており，第 5 層以上には ISO14229 で定められる車両診断通信プロトコル Unified Diagnostic Services(UDS)が用いられる．

2.3 DoIP の主要な機能

DoIP は，主に以下の 5 つの通信フェーズに分けられる．これらの通信フェーズは，規格で明確に定義されていないが，次節の攻撃検討を整理するために便宜的に用いる．

(1) Vehicle announcement / Vehicle identification
(2) Routing activation / Alive check
(3) Diagnostic communication
(4) DoIP entity status
(5) Diagnostic power mode information

2.3.1 Vehicle announcement / Vehicle identification

Vehicle announcement / Vehicle identification では，外部テスト機器が DoIP をサポートしている車両の認識を行う．車載 ECU と外部テスト機器の IP アドレス設定後に，車両から Vehicle announcement メッセージをブロードキャスト送信する．メッセージには，車両とそのネットワークを特定するための VIN(車両識別番号)，EID(ECU 固有番号)，GID(車両固有番号)などが含まれる．外部テスト機器が車両情報を受信できなかった場合，外部テスト機器から車両に対して Vehicle identification メッセージが送信され，それに対して車両が Vehicle announcement メッセージを送信する．

2.3.2 Routing activation / Alive check

Routing activation では，外部テスト機器を用いて車両を選択し，外部テスト機器と車両間で診断通信を行うための接続が確立される．まず，外部テスト機器から Routing activation request が送信される．メッセージには，外部テスト機器のアドレスや activation のタイプ等が含まれる．Routing activation request が送信された際に，車両は接続済みの外部テスト機器に対して Alive check request を送信し接続状態の確認を行う．接続先から応答がない場合は，その接続を切断する．オプション機能として外部テスト機器の認証機能等も備えている．

2.3.3 Diagnostic communication

Diagnostic communication では，外部テスト機器から車両へ診断メッセージ Diagnostic request を送信し，車両から応答メッセージ Diagnostic response を受信する．診断通信は，ECU に保存された情報の取得やファームウェアのアップデートなどの用途に使用される．また，接続解除の要求を行うことで，診断通信が終了する．

2.3.4 DoIP entity status

DoIP entity status は，外部テスト機器による車両の状態確認を行うオプションの通信フェーズである．DoIP entity status request に対する応答 DoIP entity status response は，外部テスト機器の最大同時接続数，現在の接続数などが含まれる．

2.3.9 Diagnostic power mode information

Diagnostic power mode information は，外部テスト機器による車両の電源状態の確認を行う．Diagnostic power mode information request に対する応答 Diagnostic power mode information response は，車両がアクセス可能な場合は Ready，アクセス不可な場合は Not Ready，がサポートされていない場合は Not Supported として返信される．

2.4 SOME/IP プロトコルの概要

SOME/IP プロトコルとは，2011 年 BMW グループにより開発されたサービス指向通信ミドルウェアである．ここで，サービス指向とは，諸機能を利用者にとって意味のある単位「サービス」として部品化し，そのサービスを組み合わせることでアプリケーションを構築するシステム設計手法の一つである．自動車においては，図 2 のように「EPS」，「アクセル」，「ブレーキ」，「センサ」をサービスとして，AAC， LDW 等の先進運転支援アプリケーションへ利用する場合などが考えられる．また，機能を独立性の高い「サービス」として抽出することで，新たなシステムへの再利用やシステム開発における部分的な修正などに柔軟に対応できる．さらに，UDP/TCP の上位プロトコルであるため，大容量データを Point to Point で効率的に送信することが可能となる．

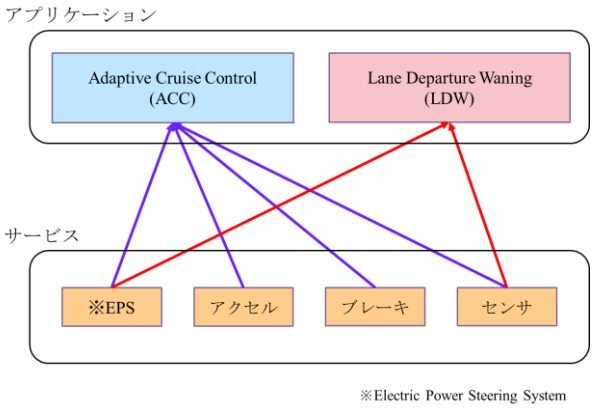

図 2．自動車におけるサービス指向アーキテクチャの例

2.5 SOME/IP の主要な機能

SOME/IP では，主に以下の 4 つの機能を備えている．ただし，DoIP と同様に攻撃検討を整理するための便宜的な区分である．

(1) Service Discovery
(2) Event
(3) Field
(4) Remote Procedure Call(RPC)

2.5.1 Service Discovery

Service Discovery では，車載ネットワークに接続されたクライアントとサービス間で，利用可能なサービスの検索，提供が行われる．サービスを提供する ECU による offer メッセージとクライアント ECU による find メッセージの通信によって，ECU 間の動的通信が確立される．

2.5.2 Event

Event では，Publish/Subscribe 方式により，特定の事象 Event が生じたことを通知する通信が行われる．まず，クライアントからサービスに対して通知を希望する Event の Eventgroup への登録要求 SubscribeEventgroup entry を行う．その要求に対してサービスから認証の ACK メッセージが返送されると，事象が生じる毎にサービスからに Event メッセージが送信される．また，クライアントが Eventgroup 登録の解除を要求することで Event メッセージの送信も停止する．

2.5.3 Field

Field では，動的な変数値の取得，設定が行われる．Event と機能が類似しているが，相違点は Getter，Setter 関数を利用できることである．これらの関数により，サービス側の変数値をクライアントが取得，設定することが可能となる．利用例としては，ACC における速度設定などが考えられる．

2.5.4 Remote Procedure Call (RPC)

RPC は，クライアントがサービス側に実装されている関数，サブルーチンをネットワーク経由で利用する機能である．

3. 車載プロトコルのセキュリティ分析

現在の車載ネットワークは，先進運転支援システム等の開発などにより複雑化することで，安全性や利便性を向上させてきた．一方で，その複雑な制御ネットワークに対する脅威も生じている[12]．車載プロトコルの事実上の標準として用いられている CAN に対しては，Koscher らにより脆弱性が指摘されている[13]．また，Ammar は既存の Ethernet プロトコルが車両に搭載された場合，その脆弱性が車載プロトコルにも影響することを明らかにしている[14]．さらに，車載 Ethernet に対しても，セキュリティ上の問題が研究されている．

3.1 DoIP のセキュリティ分析

Johan は DoIP に関して，車両から外部テスト機器を含めたシステム全体に対し，外部テスト機器と車両を保護対象として，ISO 13400 規格から考えられるセキュリティ脅威を分析し，表 1 に示すような攻撃を指摘している[15]．以下に各通信フェーズで指摘されている攻撃について説明する．Vehicle announcement，Vehicle identification では，認証機能を備えていない．そのため，攻撃者が正規車両を装って通信を行うなりすまし攻撃が挙げられている．また，攻撃者によって Vehicle identification メッセージが大量送信

されるような DoS も指摘されている．Routing activation は，Routing activation response メッセージにルーティング可または不可の情報を含む．そのため，複数回 request を送信することで，ルーティング可能なクライアントの情報を入手することが出来る．Alive check では認証機能を備えていない．そのため，なりすましの Alive check response により切断すべき接続が継続され，車両側のリソースを圧迫する DoS が指摘されている．Diagnostic communication においても認証機能がないため，攻撃者によるなりすましの危険性がある．また，Diagnostic response に含まれる公開情報を利用することで，車載ネットワークを構成する ECU を把握できることが指摘されている．DoIP entity status は，整合性の確認が行われないため，DoIP entity status メッセージが改ざんされる危険性が挙げられている．同様に，Diagnostic power mode information でも，整合性の確認が行われないため，攻撃者によって Diagnostic power mode information response を改ざんされる危険がある．

表 1．DoIP プロトコルの脆弱性と攻撃例

通信フェーズ	攻撃
Vehicle announcement Vehicle identification	なりすまし
	DoS
Routing activation Alive check	公開情報を利用した攻撃
	DoS
Diagnostic communication	なりすまし
	公開情報を利用した攻撃
DoIP entity status	改ざん
Diagnostic power mode information	改ざん

3.2 SOME/IP のセキュリティ分析

SOME/IP プロトコルでは，通信において認証や暗号化などのセキュリティ対策はなされていない．このような状況下では，容易に攻撃者がネットワーク内部から正規デバイスを攻撃可能である．Nadin らは，SOME/IP プロトコルに関する攻撃例を，不正パケットの利用，プロトコル違反，システム特有の違反，タイミング攻撃と大別して侵入検知を検討している[17]．Nadin の攻撃分類や Johan の DoIP に対するセキュリティ脅威の調査などから考案した具体的な攻撃例を表 2 に示す．Service Discovery では，サービスを検索する find メッセージに含まれる公開情報を用いることで，車載ネットワークのサービス構成を把握することが可能となる．また，認証機能がないため，サービスの offer メッセージがなりすまされる危険性が存在する．Event, Field, RPC においても認証機能が備えられていない．そのため，Event では攻撃者による大量の Event メッセージを送信される DoS，Field では Getter 応答のなりすまし，Setter による変数値の改ざん，DoS，RPC では，大量の関数，サブルーチン呼出しを行う DoS などが懸念される．

表 2．SOME/IP プロトコルの脆弱性と攻撃例

機能	攻撃
Service Discovery	公開情報を利用した攻撃
	なりすまし
Event	DoS
Field	なりすまし
	改ざん
	DoS
RPC	DoS

4. 民生 Ethernet の攻撃検知手法の検討

現在，車載 Ethernet は普及しておらず，セキュリティに関する研究報告も少数である，効果的な検知手法等が模索されている．そのため，既存の民生 Ethernet の侵入検知の研究に利用されている KDD CUP 99 データセットを用いて，決定木により攻撃検知モデルを学習し，学習モデルを解析することで攻撃検知に利用可能な特徴量を抽出した．

4.1 KDD CUP 99 データセット

KDD CUP (Knowledge Discovery and Data Mining Cup) は，ニューヨークに本部を置くコンピュータ科学分野の国際学会 Association for Computing Machinery(ACM) の分科会 Special Interest Group on Knowledge Discovery and Data Mining(SIGKDD)が 1997 年から開催しているデータマイニングを対象にした競技会である．

1999 年の KDD CUP では，Ethernet ネットワークでの通常コネクションと不正コネクションの識別を対象とした「Computer network intrusion detection」に関する競技が開催された．この競技会では，1998 年 MIT で 9 週間に渡り収集された「DARPA Intrusion Detection Evaluation Data Set」を Salvatore J.Stolfo，Wenke Lee らが加工したデータが使用された[10].

4.1.1 特徴量

データセットには Ethernet の通信に関する 41 種類の特徴量が含まれている．それらは，基本的な特徴，コンテンツの特徴とトラフィックの特徴といった 3 つのカテゴリーに分けられる．基本的な特徴には，各 TCP/IP コネクションのパケットヘッダから抽出された情報が含まれる．コンテンツの特徴には，各 TCP/IP コネクションのパケットペイロードを評価した情報が含まれる．トラフィックの特徴には，コネクションが確立されている 2 秒間で算出された通信の情報が含まれる．

4.1.2 攻撃

データセットには DoS(Denial-of-Service)，Probing，R2L(Remote-to-Local)，U2R(User-to-Root)の 4 種類の攻撃が含まれる．DoS は，提供されるサービスを制限や妨害する攻撃である．Probing は 接続状態や設定情報を収集する攻撃である．R2L は外部からローカルアクセスを獲得する攻撃である．U2R はゲスト/一般ユーザー権限からルート権限を獲得する攻撃である．

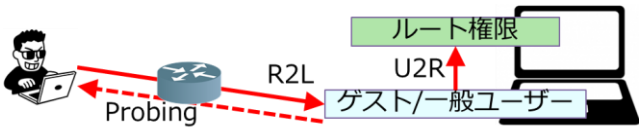

図 3．攻撃の分類

4.2 決定木による解析

4 種類の攻撃分類における特徴量を明らかにするために，KDD CUP99 データセットに対して，Classification And Regression Tree(CART)法[18]による決定木を用いて攻撃検知性能を評価し，学習モデルの解析を行った．

4.2.1 攻撃検知性能の評価方法

攻撃検知性能の評価は，KDD CUP．data_10_percent を用いて学習を行い，学習時に用いたデータと Corrected データを用いて学習済みモデルの検知性能を評価した．正常データの方が多い場合は，攻撃データ数と一致するように抽出して学習を行った．また，検知の評価には次に示す評価基準を用いた．式(1)は正常データを攻撃と過検知した割合を表す False Positive Rate(FPR)，式(2)は，攻撃を正しく検知した割合を表す True Positive Rate(TPR)である．FPR が 0 に近く，TPR が 1．0 に近い場合が理想的である．

$$\mathrm{FPR} = \frac{\text{偽陽性}}{\text{偽陽性} + \text{真陰性}} \quad (1)$$

$$\mathrm{TPR} = \frac{\text{真陽性}}{\text{真陽性} + \text{偽陽性}} \quad (2)$$

真陰性：正常メッセージが正常メッセージとして検出された数
偽陽性：正常メッセージが異常メッセージとして検出された数
真陽性：異常メッセージが異常メッセージとして検出された数
偽陰性：異常メッセージが正常メッセージとして検出された数

4.2.2 学習モデルの解析方法

学習モデルの解析は，学習データの分類に用いられるジニ指数から得られる情報利得を示し，上位 3 位までを抽出した．情報利得とは，無秩序さを表す指標である．クラスの混ざり具合を不純度として導入すると，ある特徴量によって分類を行うときの不純度の変化量を情報利得として定義できる．ある特徴量でクラスの混ざり具合が軽減した場合，情報利得は高くなる．その為，高い情報利得を得る特徴量は，分類に対して寄与度が大きいといえる．また，一般に情報利得は，0 から 1 の間を変動する値で，1 に近づくほど分類に対する寄与度が高い．本稿では，情報利得ΔI_Gを定義するために，不純度として以下の式で表されるジニ指数 I_G を用いた．

$$I_G(t) = 1 - \sum_{i=1}^{c} p\left(\frac{C_i}{t}\right)^2 \quad (3)$$

ここで t はノード(データセットの部分集合), C はクラスの総数，$p(C_i/t)$はノード t においてクラス C_i を得る確率を表す．ノード t をある特徴量でノード t_1，t_2 に分類したときの情報利得は，それぞれのジニ指数にデータ数による重みづけを行い以下のように表される．

$$\Delta I_G = I_G(t) - \frac{n_{t_1}}{N} I_G(t_1) - \frac{n_{t_2}}{N} I_G(t_2) \quad (4)$$

式中の N はノード t におけるデータ総数，n_{t_i}はノード t_i のデータ数である．

4.2.3 解析結果

攻撃検知性能の評価結果

表 3 に示すように，KDD CUP．data_10_percent による評価では全ての攻撃において TPR が約 100[%]，FPR は U2R が約 6[%]，他の攻撃では約 2[%]以下となっており，高い検知率を示している．一方，Corrected による評価では，DoS，Probing は高い検知率を示しているが， U2R は TPR が約 87[%]と減少し，R2L は約 6[%]と大きく減少している．R2L に関しては，データの特徴量から通常と攻撃を分離することが困難である．KDD CUP 99 データセットでは 4 種類の攻撃データ数の偏りから，DoS，Probing の検知率が高く，U2R, R2L の検知率が低くなることが報告されている[17]．しかしながら，本稿の解析のように正常データの抽出の仕方によっては，U2R は検知率が高くなる．

表 3． 各攻撃の検知率

	KDD CUP.data_10_percent		Corrected	
	TPR[%]	FPR[%]	TPR[%]	FPR[%]
DoS	100.00	0.01	97.23	0.34
Probing	99.95	0.31	99.35	1.16
R2L	99.38	1.39	6.60	0.90
U2R	100.00	6.18	87.28	4.39

学習モデルの解析

学習モデルの情報利得を図 4 に示す．横軸の特徴番号はデータセット配布元[10]で規定される特徴量に参考文献[19]で割り振られた番号を示している．また， 表 4 に上位 3 位までの特徴量示す．DoS は，同一ホストに対するコネクションの数やエラー状態のコネクション数で検知される．Probing は送信データのバイト数，利用しているサービス等で検知される．R2L は利用しているサービスやそのエラー状態及び同一ホストへのコネクション数で検知される．

U2R では，同一ホスト，同一サービスを利用している接続の数，送受信データの大きさで検知される．

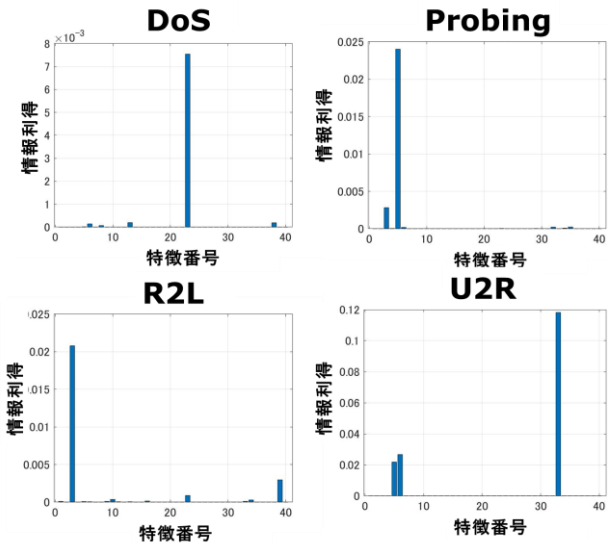

図 4．各攻撃における特徴量の情報利得

表 4．各攻撃の特徴量

攻撃	特徴番号	概要	情報利得
DoS	23	同一ホストへの コネクションの数	0.007547
	13	“compromised” 状態の数	0.000199
	38	“s0” エラー状態の コネクションの数	0.00019
Probing	5	送信データのバイト数	0.024016
	3	宛先ポートのサービス名	0.002825
	35	異なったサービスを 利用している割合	0.000235
R2L	3	宛先ポートのサービス名	0.020795
	39	特定のサービスで “s0” エ ラー状態のコネクションの数	0.002962
	23	同一ホストへの コネクションの数	0.000878
U2R	33	同一の宛先ホストで 同一サービスを利用する コネクションの数	0.118182
	6	受信データのバイト数	0.026663
	5	送信データのバイト数	0.021822

5. 車載 Ethernet の攻撃検知手法の検討

民生 Ethernet と車載 Ethernet の通信フレーム構造を比較し，第 3 節で述べた想定される攻撃の特徴量について検討する．

5.1 通信フレームの比較

Ethernet の通信フレームは，各プロトコル階層の情報が入れ子状になっており，Ethernet フレーム，IP フレーム，TCP/IP フレームおよびデータフレームから構成される．また，各階層のフレームはそのプロトコルの制御情報ヘッダ Protocol Control Information(PCI)とペイロード Service Data Unit(PDC)に分けられる．DoIP と SOME/IP プロトコルが扱う情報も同様の構成でデータフレーム格納されているため，民生 Ethernet と車載 Ethernet の通信フレームに構造上の大きな違いはないといえる．そこで、民生 Ethernet の攻撃を車載 Ethernet の攻撃に対応付け，その特徴量を基に車載 Ethernet の特徴量を考察した．

5.2 攻撃検知性能予測

第 3 節で示した攻撃に民生 Ethernet の攻撃を対応付ける．車載 Ethernet の DoS は，民生 Ethernet で行われるような大量のデータを送り付ける攻撃であるため，DoS に対応付ける．公開情報を利用した攻撃は，DoIP，SOME/IP における応答メッセージを利用して情報取得を行うもので，ポートスキャン等の情報収集を行う民生の Probing に対応付ける．また，なりすましは IP アドレス等を偽装して正規 ECU を装い，改ざんは正規メッセージのペイロード等を書き換えるものであるため，4 つの分類に対応付けられるものが存在しない．以上のように，対応付けられた車載 Ethernet の攻撃に対する検知率予測と特徴量の候補を表 5 に示す．表において，DoS 攻撃は 23，13，38 の特徴量を用いることで TPR が約 97[%]，FPR が約 0.4[%]と精度良く検知できる．また，民生の同様の攻撃手法であるため，民生の特徴量をそのまま転用した検知が可能と考えられる．これにより，DoIP の Vehicle identification メッセージや SOME/IP の Event メッセージが大量送信されるような攻撃を検知できる．Probing においても 5，3，35 の特徴量を用いることで TPR が約 99[%]，FPR が約 1.2[%]と精度良く検知できる．車載 Ethernet フレームのヘッダとペイロードで，データの大きさや利用しているサービス等を監視する必要がある，これにより，DoIP の Routing activation メッセージを利用したルーティング情報収集や SOME/IP の Service Discovery の find メッセージに含まれる情報収集を検知できる．

表 5．車載 Ethernet の攻撃検知性能予測と特徴量の候補

車載Ethernetの攻撃	民生Ethernetの攻撃	検知性能予測		特徴量の候補
		TPR[%]	FPR[%]	
DoS	DoS	97.23	0.34	23, 13, 38
なりすまし	-	-	-	-
公開情報を 利用した攻撃	Probing	99.35	1.16	5, 3, 35
改ざん	-	-	-	-

5.3 攻撃検知手法の考察

DoIP，SOME/IP を含む Ethernet フレームでは，複数のプロトコルが入れ子構造なっており，攻撃検知を行う上で多数の特徴量が存在するため，検知に有効な特徴量を絞り込むことが重要となり，本稿では抽出した民生 Ethernet の特徴量から車載 Ethernet に有効と考えられる特徴量の選別を行った．侵入検知手法にはシグネチャ型とアノマリ型の 2 種類があり，シグネチャ型はペイロードを主とした監視対象の異常なパターンを定義し，それと一致する場合は侵入として検知する．一方，アノマリ型は監視対象の正常なパターンを定義し，そこから逸脱するものを侵入として検知する．本稿で抽出した特徴量は侵入のシグネチャ型検知に用いることが出来る．シグネチャ型では，迅速な対応が可能であるため低遅延な通信が要求される車載セキュリティ対策についても有効である．しかしながら，上位層のホワ

イトリストの利用は，ECU のリソースを考慮する上で現実的な対策とは言えない．また，シグネチャにない新規攻撃は検知することができない．そのため，正常なパターンを定義したアノマリ型の異常検知手法について検討を行う必要がある．

6. まとめ

本稿では，DoIP と SOME/IP に対するセキュリティ分析から得たサイバー攻撃について，民生 Ethernet の侵入検知に用いられる KDD CUP 99 データセットより学習した攻撃に対する検知モデルから，サイバー攻撃検知に有効な特徴量を抽出した．さらに，これら民生の Ethernet から得た特徴量から車載 Ethernet の上位プロトコルである SOME/IP と DoIP に転用可能と感がられるものを選別し．検知に有効な特徴量の絞り込みを行った．

今後は，SOME/IP と DoIP プロトコルに対して攻撃検証を行う環境を構築し，考案したサイバー攻撃の検証を行い，選別した特徴量利用して検知手法検討を行う．

参考文献

[1] U.Abelein,H.Lochner,D.Hahn and S.Straube,“Complexity,quality and robustness - the challenges of tomorrow’s automotive electronics”,Design,Automation Test in Europe Conference Exhibition (DATE),2012.

[2] International Organization for Standardization,“Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling,” ISO11898-1,Rev.2003.

[3] International Organization for Standardization,“Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling,” ISO11898-1,Rev.2015.

[4] International Organization for Standardization,ISO 13400-1:2011 - Road vehicles - Diagnostic communication over Internet Protocol (DoIP) - Part 1: General information and use case definition.2011,

[5] International Organization for Standardization,ISO 13400-2:2012 - Road vehicles - Diagnostic communication over InternetProtocol (DoIP) - Part 2: Transport protocol and network layer services.2011,

[6] International Organization for Standardization,ISO 13400-3:2016 - Road vehicles - Diagnostic communication over InternetProtocol (DoIP) - Part 3: Wired vehicle interface based on IEEE 802.3.2011,

[7] International Organization for Standardization,ISO 13400-4:2016 - Road vehicles - Diagnostic communication over InternetProtocol (DoIP) - Part 4: Ethernet diagnostic connector.2011,

[8] Lars Völker, “Scalable service-Oriented MiddlewarE over IP (SOME/IP)”.http://some-ip.com/.[Accessed: 7-Mar-2019]

[9] NIST,Framework for Improving Crtical Infrastructure Cybersecurity.https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.11.pdf [Accessed: 23-Jul-2019]

[10] Irvine,KDD CUP 1999 Data.: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html [Accessed:7-Mar-2019]

[11] ベクタージャパン株式会社より提供（データ取得日：2019 年 8 月 22 日）

[12] Stephen Checkoway,Damon McCoy,Brian Kantor,Danny Anderson,HovavShacham,StefanSavage,KarlKoscher,AlexeiCzeskis,Franziska Roesner,Tadayoshi Kohno,et al.“Comprehensive experimental analyses of automotive attack surfaces.” In USENIXSecurity Symposium.San Francisco,2011.

[13] Koscher,K.,Czeskis,A.,Roesner,F.,Patel,S.et al.,“Experimental Security Analysis of a Modern Automobile”,2010 IEEE.

[14] Ammar Talic,“Security Analysis of Ethernet in Cars”,KTH Royal Institute of Technology School of information and Communication Technology,Master’s Thesis 2017

[15] Johan Linberg,Security “Analysis of Vehicle Diagnostics using DoIP”,Master of Thesis Chalmers University of Technology,University of Gothenburg Department of Computer Science and Engineering,Sweden,2011.

[16] Nadine Herold,Stephan-A.Posselt,Oliver Hanka and Georg Carle,“Anomaly Detection for SOME/IP using Complex Event Processing”,IEEE/IFIP NOMS 2016 Workshop,

[17] H.Günes Kayacık,A.Nur Zincir-Heywood,Malcolm I.Heywoo,“Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets”,Journal Of Engineering,Education And Technology (ARDIJEET) .2015

[18] Breiman, L., J. Friedman, R. Olshen, and C. Stone. Classification and Regression Trees. Boca Raton, FL: CRC Press, 1984.

[19] Ralf C. Staudemeyer,Christian W. Omlin,“Extracting salient features for network intrusion detection using machine learning methods”,SACJ 52, July 2014