様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １０ 日現在

機関番号：３４３０４
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８９２

研究課題名（和文）車載システムの攻撃評価用データセットの開発とファズデータ生成に関する研究

研究課題名（英文）Research on Dataset for Attack Evaluation of In-vehicle Systems and Fuzz Data Generation

研究代表者
井上　博之（Inoue, Hiroyuki）

京都産業大学・情報理工学部・教授

研究者番号：６０４６８２９６

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：自動車の車載LANで広く使われているCANの攻撃データセットとして，なりすまし，ファジング，DoSの攻撃を組み合わせで生成を可能にし，それを用いた機械学習ベースの異常検知システムを構成した．同時に，異常検知を行う場所をサーバ側とするためにIDベース暗号を用いた車載LANデータ活用システムを開発し評価した．また，車載Ethernetとゾーンアーキテクチャを用いたSDVにおけるリスク分析を行い，サービス指向通信ミドルウェアであるSOME/IPのなりすまし攻撃の分析とその攻撃検知の手法について評価を行った．

研究成果の学術的意義や社会的意義
コネクティッドカーの普及につれて，自動車の内部ネットワークである車載LANのセキュリティを強化する手法が求められている．広く普及しているCANを使った攻撃データセットの開発とそれを用いた攻撃検知手法により，より安全な自動車システムの開発に寄与することができる．また，CANの後継と見込まれている車載Ethernetとそれを用いたSDVについても，同様に攻撃手法の分析とその緩和策を具体的に検討することで，より安全なシステムの開発が期待できる．

研究成果の概要（英文）：I have developed an attack dataset for CAN, which is widely used in automotive LANs, that combines spoofing, fuzzing, and denial-of-service (DoS) attacks. Using this dataset, I constructed a machine learning-based anomaly detection system, and developed and evaluated an in-vehicle LAN data utilization system using ID-based cryptography to detect anomalies on the server side. I also conducted a risk analysis of SDV using in-vehicle Ethernet and zone architecture, and analyzed spoofing attacks on SOME/IP, a service-oriented communication middleware, and evaluated methods for detecting such attacks.

研究分野：組込みセキュリティ

キーワード：車載ネットワーク　データセット　なりすまし　ファジング　CAN　車載Ethernet

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

自動車内部のネットワーク（以下，車載 LAN）の通信プロトコルとしては CAN（Controller Area Network）がまだまだ主流であり，最近の一部の車種でペイロード長や速度を向上させた CAN FD や車載 Ethernet が採用されつつあるのが現状である．コネクティッドカーや自動運転車が一般的になるにつれ，広域ネットワークに接続される車載 LAN やそこにつながる電子制御ユニット（ECU）の情報セキュリティについて様々な方法での安全性評価が必要となってきている．応募者は，車載 LAN の情報セキュリティを検証および分析するための攻撃検証用プラットフォームを開発し，車載 LAN のメッセージの解析，車載 LAN に対する攻撃の影響の検証や防御機構の検討を行ってきた[1][2][3]．実車を用いた検証など，様々な攻撃の影響を確認し，静的なホワイトリストやブラックリストに基づくフィルタリング方式を検討してきたが，車載 LAN 上でやりとりされるメッセージは，自動車メーカーや車種によって異なり車載 LAN につながる機器ごとにも異なるため，静的なルールによるフィルタリングだけでは攻撃の検知は困難である．車載 LAN のトラフィックに機械学習アルゴリズムを適用することによって動的に検知ルールを生成することで，最新の結果では 99%を超える攻撃トラフィックの識別が可能という結果が得られている[4][5][6]．この際に使用した評価用データとしては，韓国の Hacking and Countermeasure Research Lab.によって公開されている CAN トラフィックのデータと，応募者が所有する実験用車両から抽出した CAN トラフィックに擬似的な攻撃データを付加したものを使用している．両者のデータセットは，市販されている自動車から取得したものに想定した攻撃データを付加したものであり，汎用的に使用できる CAN トラフィックの攻撃評価用データセットとは異なる．一方，自動車の開発時に ECU やゲートウェイを含む車載 LAN 全体の脆弱性を，広範囲かつ限られた時間で検査するツールが必要となってくることからファジングテストを効率的に行う手法も必要となる．ファジングテストに用いるファズデータの生成にはノウハウが必要であり，開発した攻撃検証用プラットフォームを用いて脅威のモデル化と実データから，不具合を起こしやすいファズデータを生成する方式を検討している[7][8][9]．ファズデータがどれくらい効率的に車載システムの脆弱性や不具合を発見可能かという定量的評価についても，前述の実車から取得した CAN トラフィックを基にしており，汎用的な評価データセットを用いた結果を使ったファズデータ生成アルゴリズムを検討できるようにする必要がある．

２．研究の目的

車種やメーカに依存しないような CAN トラフィックデータとそれに様々の攻撃パターンを組み込んだ車載システムの攻撃評価用データセットの開発を目標とし，そのデータセットを用いて車載システムの脆弱性や不具合を減少させることを目標とする．データセットは固定化したものではなく，ベースとなるものから用途に応じてプログラム等により生成可能なものを考えており，攻撃パターンやそのパラメータや組み合わせについても同様に生成可能とする．文献[4][5]で使用した評価データでは，既存の車両から得られた CAN トラフィックに，自作プログラムによって攻撃パターンを組込んだものを使用している．車載 LAN や ECU は組込みシステムであることから，製品メーカや部品メーカのノウハウの影響が大きい部分であり，コネクティッドカーの今後の普及に応じられるように，広域ネットワークにおけるサイバー攻撃やトラフィック分析に関する学術での知見と併せて，車載システムの攻撃評価用データセットの開発を進める．この知見により，外部からの攻撃や不正アクセスの検知および防御に有効な CAN メッセージのデータ格納方式も定式化することを検討する．また，実際の製品開発時に必要な脆弱性検査のためのファジング用ファズデータを生成可能とすることで，ライフサイクルが長い自動車において長期的な製品の安全性を担保できると思われる．

３．研究の方法

車載 LAN につながるコンポーネントや車載システム全体の CAN トラフィックを経由した攻撃に対して脆弱性や不具合を発見し評価できるような攻撃評価用データセットと生成プログラムの開発，またファジング用ファズデータの生成方法について研究を行う．CAN を用いた車載 LAN の脆弱性や攻撃手法の内容から機能に応じた CAN トラフィックの標準形を開発し，実車から取得した CAN トラフィックに対して，なりすまし，DoS，ファジング等の攻撃データを注入し，評価用データセットを生成するプログラムの開発を行った．それを基に，機能に応じた CAN トラフィックの標準形を作成し，付加機能に応じて付加・変更する手順について検討を行

う．この標準 CAN トラフィックに対して，様々な攻撃パターンを考慮し攻撃データを埋め込んだ攻撃評価用データセットを生成するためのアルゴリズムと生成プログラムを開発する．開発したデータセットの評価は，以前に研究発表を行った機械学習を用いた異常検知手法に適用すると同時に，他の研究グループから発表されている検知アルゴリズムについても適用し評価を行う．また，ファジング用ファズデータの生成方法の設計と開発を行うために評価用の車載システムを構築する．また，CAN に代わって実車に導入されつつある車載 Ethernet からなるゾーンアーキテクチャの構成とそこにおけるトラフィックのモデル化についても検討し，車載 Ethernet を用いた車載ネットワークの特徴や脆弱性分析を実施する．車載 Ethernet では SDN（Software Defined Network）を用いて動的にネットワーク構成を変更することも可能であり，通常走行時・高速走行時・車庫入れ動作時などの利用シーンに適応した構成をとることで，トラフィックや遅延を最適化し，また外部からの攻撃から防御する手法について検討する．

４．研究成果

攻撃評価用データセットは実車の通常トラフィックになりすまし攻撃や DoS 攻撃が実施された状況を想定し，3 種類の車種の実車の走行時データを CAN アナライザを用いてキャプチャし，それを修正可能なフォーマットに変換することで正常データの準備を行った．Python を用いた攻撃データ生成プログラムの開発を行い，なりすまし，ファジング，DoS の 3 つの攻撃モードを選択し，任意のタイミングで攻撃データを正常データに注入することで，車種毎の攻撃データセットを生成することを可能にした．図 1 は，指定した期間に指定した攻撃データを注入する様子を示している．ファズデータの生成は，既存の正常データを基にすることで攻撃可能性を向上させるようにした．また，連合学習を用いてデータを共有することなく安全な学習手順を保証するためにパーソナライズされた統合学習ベースの侵入検知システムを作成し，教師あり学習と教師なし学習を用いて攻撃データの挙動を観察した結果，教師あり学習ベースの分類器では 99.5%以上の精度で攻撃を検出できた．

異常検知を行う場所として，機械学習の計算コストを考慮して，侵入検知処理を計算資源に制約がある車載コンピュータではなく，サーバを用いて行う外部処理方式を検討した．この方式では複数の自動車のデータを 1 箇所で管理することもできるうえ，車載コンピュータでは負荷の大きい高度な検知アルゴリズムの使用も可能になる等の利点も期待できる．自動車を狙った攻撃にはトラフィックの急増や，消費電力の増加といった時間的相関を示すことが多い．このため，順伝播型ニューラルネットワークでは時間的情報が失われる場合がある．そこで，長･短期記憶の隠れ層がある LSTM ネットワークを使用することで上記の問題を解決できると考えた．従来の RNN は勾配消失により長いデータの学習が困難であったが，LSTM を用いることでその問題の解決を狙った．車載コンピュータに Raspberry Pi 4 を使用したプロトタイプシステムを構成したところ，全体の検出精度は 99.86%となり，Raspberry Pi4 の処理時間は 109.77 秒，サーバ側の処理時間は 22.44 秒となった．また自動車とサーバ間の通信においては，使用した LTE 回線のネットワークの帯域幅以下の負荷である 270Kbps 程度に収まっていることが確認できた．また，サーバ側で検知を行うためには，自動車内部を流れる制御データ等からなる車載 LAN データを，サーバ上に安全かつリアルタイムに蓄積する仕組みが必要となる．このとき，

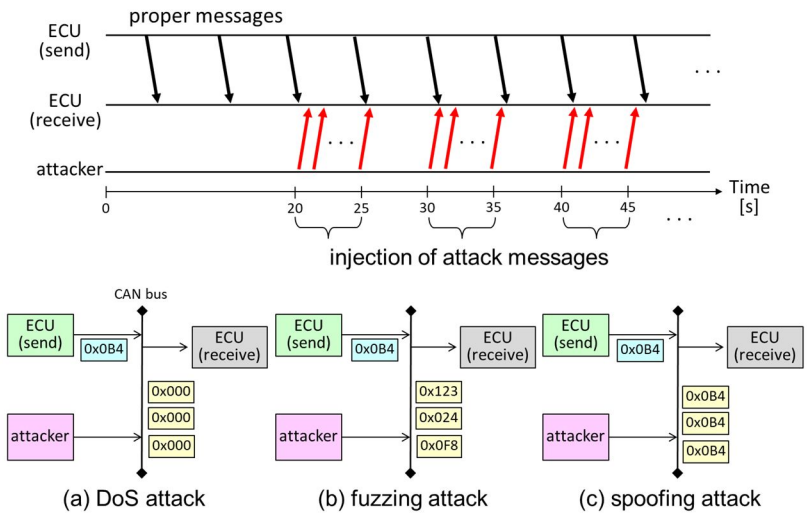

図1 攻撃データの注入による異常時データセットの生成

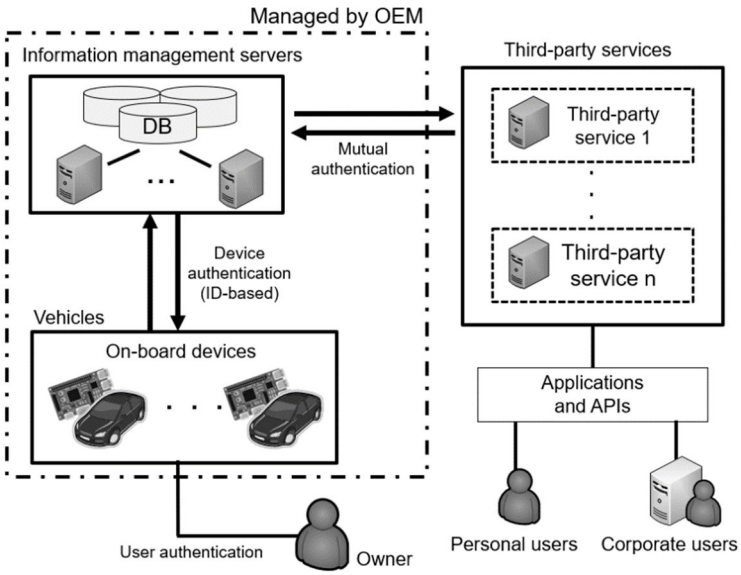

図2 IDベース暗号を使用した車載LANデータ活用システム

システムに属する車両の数が膨大になることを考慮すると，車両の数に対する運用管理の煩雑さを緩和する認証方式が必要となる．そこで図 2 に示すような，車載器と収集サーバの相互認証方式に ID ベース暗号を用いて，車載器の ID を基に生成した鍵による認証を行うことで鍵管理を容易にした車載 LAN データ活用システムを考案した．システムにおける車両の管理情報と車両の認証鍵の管理情報を統合することで鍵管理作業における運用管理に関する煩雑さの緩和が可能となる．プロトタイプを開発し，評価を行ったところ ID ベース暗号を利用した相互認証では，従来の証明書を使用した相互認証と比較してパフォーマンス面で劣っているものの，鍵管理・運用において煩雑さが軽減され，スケーラビリティの面で有効であることを確認した．

車載 LAN に CAN を用いた構成から，今後の自動車システムは車載 Ethernet ベースのゾーンアーキテクチャ型のネットワーク構成とソフトウェア定義型自動車（SDV）になると考えられる．ゾーンアーキテクチャにソフトウェア定義型ネットワーク（SDN）を適用し，図 3 に示すような SDV の分析対象モデルを作成し，ISO/SAE 21434 TARA 準拠のリスク分析を行った．SDV により，SDN コントローラ，Zone ECU，Central ECU 等，攻撃による損害を受けた時の深刻度が重大になる機器が追加されたが，脅威は従来の自動車システムに対するものと同様という結論が出た．すなわち，長距離無線通信，OTA（Over The Air），およびダイレクトアクセス攻撃のそれぞれを経由した重要資産に対する攻撃が引き続き重要脅威となるという結果になった．また，OTA や Plug and Play によりソフトウェアやハードウェアを納車後に更新し機能の追加や更新を行う要望が増加しており，この課題に対応するためにサービス指向アーキテクチャが注目されている．AUTOSAR により規定されているサービス指向通信ミドルウェアの SOME/IP では，SOME/IP 自身では暗号化および認証の仕組みは持っていないため，なりすまし攻撃に脆弱であると考えられる．まず，SOME/IP におけるなりすまし攻撃のパターンを図 4 に示すように分類した．今回は，車載 LAN のパケット Switch 上に異常検知アルゴリズムと通信保護アルゴリズムを実装することで，サービス探索時に攻撃者の存在の可能性を検知し，正規の Server-Client 間の通信を保護する方式を検討した．SOME/IP プロトコルスタックのプロト

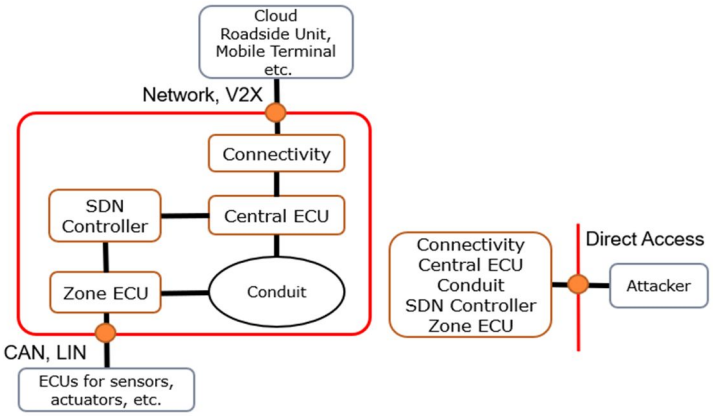

図 3 SDV システムの分析対象モデル

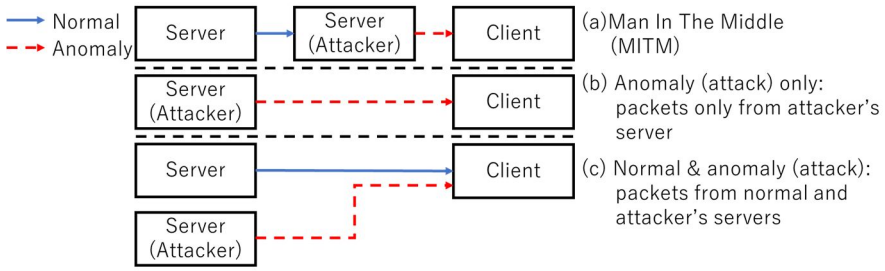

図4 SOME/IPに対するなりすまし攻撃パターン

タイプ実装である vsomeip を用いた実機評価を実施し，正規の Server によるサービス提供が無効化されない限り Server になりすます攻撃を 100%検知できることを確認した．ただし，正規の Server によるサービス提供が無効化された場合，なりすまし攻撃を一切検知することができない課題があり，正規の Server のサービス提供を無効化する攻撃の実現可能性を検討する必要がある．

＜引用文献＞

[1] 井上博之, "自動運転の時代におけるコネクティッドカーの IoT セキュリティ", 車載テクノロジー, vol.7, no.9, pp.42-46, June 2020.

[2] 家平和輝, 井上博之, 石田賢治, "特定の CAN メッセージを送信する ECU に対するバスオフ攻撃を利用したなりすまし攻撃 ”, 情報処理学会論文誌：コンシューマ・デバイス&システム, vol.8, no.2, pp.1-12, May 2018.

[3] 西尾泰彦，城間政司，井上博之，"脅威モデリング連携型アタックテストによる車載ネットワーク脅威分析手法 ”，情報処理学会論文誌, vol.58, no.12, Dec. 2017.

[4] M. D. Hossain, H. Inoue, H. Ochiai, F. Doudou, Y. Kadobayashi, “In-Vehicle CAN Bus Intrusion Detection System Using Convolutional Neural Network Deep Learning Approach,” Proceedings of 2020 IEEE Global Communications Conference (Globecom2020) , Dec. 2020.

[5] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall and Y. Kadobayashi, "LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communications," IEEE Access, vol.8, pp.185489-185502, Oct. 2020.

[6] 手柴瑞基，井上博之，石田賢治,“ 車載セキュリティゲートウェイにおける機械学習を用いた動的フィルタリング機構の実装と評価, ” 電子情報通信学会 情報ネットワーク研究会 (IN), vol.116, no.485, pp.205-210, Mar. 2017.

[7] 鈴木陵馬，林侑香里，井上博之，石田賢治，“ 車載 LAN における r-VAE を用いたファジングテスト効率化手法の提案, ” 電気・情報関連学会中国支部連合大会 2020, R20-20-03-05, Oct. 2020.

[8] 石長篤人，井上博之，石田賢治,“ 車載ネットワークにおける CAN プロトコルの特性を利用した送信元ECU識別方式, ”2019年 暗号と情報セキュリティシンポジウム (SCIS2019), pp.1-8, Jan. 2019.

[9] 鈴木陵馬，金森健人，家平和輝，井上博之，石田賢治,“ 車載 LAN における異なる種類のデータフィールド値の関係に基づく異常検知方式, ” マルチメディア、分散、協調とモバイル(DICOMO2018)シンポジウム, pp.879-884, July 2018.

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　4件）

１．著者名 Kawanishi Yasuyuki、Nishihara Hideaki、Yoshida Hirotaka、Yamamoto Hideki、Inoue Hiroyuki	４．巻 11
２．論文標題 A Study on Threat Analysis and Risk Assessment Based on the “Asset Container” Method and CWSS	５．発行年 2023年
３．雑誌名 IEEE Access	６．最初と最後の頁 18148～18156
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2023.3246497	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 KAWANISHI Yasuyuki、NISHIHARA Hideaki、YAMAMOTO Hideki、YOSHIDA Hirotaka、INOUE Hiroyuki	４．巻 E106.A
２．論文標題 A Study of The Risk Quantification Method of Cyber-Physical Systems focusing on Direct-Access Attacks to In-Vehicle Networks	５．発行年 2023年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 341～349
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2022CIP0004	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Shibly Kabid Hassan、Hossain Md Delwar、Inoue Hiroyuki、Taenaka Yuzo、Kadobayashi Youki	４．巻 37
２．論文標題 Towards Autonomous Driving Model Resistant to Adversarial Attack	５．発行年 2023年
３．雑誌名 Applied Artificial Intelligence	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/08839514.2023.2193461	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Inoue Hiroyuki、Kanamori Kento、Sakemi Yumi、Kanno Satoru、Inamura Masaki	４．巻 143
２．論文標題 In-vehicle LAN Data Utilization System Using Mutual Authentication Method Considering Key Management	５．発行年 2023年
３．雑誌名 IEEJ Transactions on Electronics, Information and Systems	６．最初と最後の頁 743～753
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejeiss.143.743	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計18件（うち招待講演　10件／うち国際学会　3件）

１．発表者名
井上博之

２．発表標題
IoTセキュリティと車載アーキテクチャの変化

３．学会等名
自動車技術会JSAEオンデマンド講座（招待講演）

４．発表年
2022年

１．発表者名
井上博之

２．発表標題
自動車のアーキテクチャの変化とサイバーセキュリティへの対応

３．学会等名
ナノオプト・メディア セキュリティオンラインセミナー（招待講演）

４．発表年
2022年

１．発表者名
K. H. Shibly, M. D. Hossain, H. Inoue, Y. Taenaka, Y. Kadobayashi

２．発表標題
Autonomous Driving Model Defense Study on Hijacking Adversarial Attack

３．学会等名
31st International Conference on Artificial Neural Networks (ICANN2022)（国際学会）

４．発表年
2022年

１．発表者名
井上博之

２．発表標題
IoTセキュリティ・車載セキュリティ

３．学会等名
関西情報センター 2022年度サイバーセキュリティ・リレー講座（招待講演）

４．発表年
2022年

１．発表者名
K. H. Shibly, M. D. Hossain, H. Inoue, Y. Taenaka, Y. Kadobayashi

２．発表標題
Personalized Federated Learning for Automotive Intrusion Detection Systems

３．学会等名
2022 IEEE Future Networks World Forum (FNWF2022)（国際学会）

４．発表年
2022年

１．発表者名
井上博之

２．発表標題
自動運転時代の自動車サイバーセキュリティに必要となる人材

３．学会等名
セキュリティオンラインセミナー

４．発表年
2021年

１．発表者名
井上博之

２．発表標題
組込みとセキュリティと人材育成

３．学会等名
情報処理学会関西支部 2021年度支部大会（招待講演）

４．発表年
2021年

１．発表者名
井上博之

２．発表標題
エッジIoTデバイスとしての組込みシステムの情報セキュリティ

３．学会等名
組込みシステム産業振興機構 組込みシステム・セキュリティセミナー

４．発表年
2021年

１．発表者名
井上博之

２．発表標題
コネクティッドカーのIoTセキュリティ

３．学会等名
立命館大学IoTセキュリティ研究センター 2021年度第2回オンラインセミナー（招待講演）

４．発表年
2021年

１．発表者名
K. H. Shibly, M. D. Hossain, H. Inoue, Y. Taenaka, and Y. Kadobayashi

２．発表標題
A Feature-Aware Semi-Supervised Learning Approach for Automotive Ethernet

３．学会等名
IEEE International Conference on Cyber Security and Resilience (CSR2023)（国際学会）

４．発表年
2023年

１．発表者名
家平和輝，井上博之

２．発表標題
SOME/IPを適用した車載ネットワークにおける通信遅延の変動を抑制するパケット転送方式の提案

３．学会等名
電子情報通信学会インターネットアーキテクチャ研究会

４．発表年
2023年

１．発表者名
川西康之，西原秀明，吉田博隆，山本秀樹，井上博之

２．発表標題
ネットワークレイヤと物理的構成を考慮したソフトウェア定義型自動車を構成するゾーンアーキテクチャのリスク分析

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2024）

４．発表年
2024年

１．発表者名
家平和輝，井上博之

２．発表標題
サービス探索時にサーバなりすまし攻撃の検知を行うSOME/IP向け通信保護方式

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2024）

４．発表年
2024年

１．発表者名
井上博之

２．発表標題
自動車アーキテクチャの変化とソフトウェア人材の重要性

３．学会等名
第27回サイバー犯罪に関する白浜シンポジウム（招待講演）

４．発表年
2023年

１．発表者名
井上博之

２．発表標題
IoTデバイスとしてのコネクティッドカーのセキュリティ

３．学会等名
電気学会関西支部専門講習会（招待講演）

４．発表年
2023年

１．発表者名
井上博之

２．発表標題
コネクティッドカーのサイバーセキュリティと自動車アーキテクチャの変化

３．学会等名
浜名湖国際頭脳センター サイバーセキュリティ講座 自動車業界編（招待講演）

４．発表年
2023年

１．発表者名 井上博之
２．発表標題 コネクティッドカーのセキュリティと車載ネットワークの解析
３．学会等名 京都高度技術研究所 輸送機器・移動体のサイバーセキュリティセミナー（招待講演）
４．発表年 2024年

１．発表者名 井上博之
２．発表標題 IoTデバイスとしての車載システムのセキュリティ
３．学会等名 Security Management Conference Roadshow 2024 Winter 名古屋 基調講演（招待講演）
４．発表年 2024年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関