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　３ 年　 ６ 月 １１ 日現在

機関番号：２５４０３
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１２９９

研究課題名（和文）車載システムの動的フィルタリング機構およびファジングテスト手法の実用化

研究課題名（英文）Practical Study on Dynamic Filtering Mechanisms and Fuzzing Tests for In-Vehicle Systems

研究代表者
井上　博之（Inoue, Hiroyuki）

広島市立大学・情報科学研究科・准教授

研究者番号：６０４６８２９６

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：コネクティッドカーの外部インタフェースを介した攻撃に対する事例分析と対策案の検討を行い動的なフィルタリング機構のソフトウェアでの実現および実車での評価を行った．車載システムにおける攻撃のパターンをいくつかに分類し標準的なデータセットとして提供できるようにし，攻撃としての有効性の評価には機械学習モデルr-VAEというアルゴリズムを適用することでファジングデータを生成できることを確認した．また，取得した車載LANのデータをCANデータ向け圧縮アルゴリズムを考案し，サーバ上で分析したり速度やエンジン状態などの意味のある情報として可視化することができるプロトタイプを完成した．

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と呼ばれる広域ネットワークに常時接続されるような自動車や自動運転車の普及に伴い，外部からの攻撃や潜在的な脅威が高まっている．自動車に搭載されるコンピュータ同士が通信を行うための車載ネットワークにおける不正アクセスに対する防御および認証の手法について，機械学習を使用した動的なフィルタリングや脆弱性評価のためのファジングデータの生成，またクラウドへ送信する際の高効率なCANデータ圧縮方式等についてプロトタイプの開発を行った．

研究成果の概要（英文）：I analyzed cases of attacks via the external interface of the connected car, and examined the countermeasures. I realized the dynamic filtering mechanism with software, and evaluated it with the actual vehicle. It is possible to classify attack patterns in in-vehicle systems into several categories and provide them as standard data sets. I confirmed that fuzzing data can be generated by applying an algorithm called machine learning model r-VAE, and evaluated the effectiveness as attacks. I also devised a compression algorithm for CAN messages of in-vehicle LAN data, and completed a prototype that can be analyzed on a server and visualized as meaningful information such as speed and engine status.

研究分野：情報セキュリティ

キーワード：車載ネットワーク　組込みセキュリティ　CAN　セキュリティゲートウェイ　なりすまし　ファジング

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）が広域ネットワークとに接続されることにより，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，特に 2015 年の Jeep の遠隔ハッキング[1]が明らかになって以来, 大きな問題となっている. 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ることや，車載 LAN につながる機器によって必要なメッセージが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困難であった．そこで車載 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ルールを生成するようなフィルタリング機能を持つセキュリティゲートウェイを検討し，トラフィック毎にペイロードや周期を機械学習することによって生成されたルールを用いて通常のメッセージと不正なメッセージを判別する実験を行ったところ 97%以上の割合で不正なメッセージを識別できた[2][3]．また，攻撃手法の実装に FPGA を用いたハードウェアを試作し，実際のネットワーク上のデータをビット単位で検知し書き換えるような方式の実装を行っている[4][5]．車載 LAN 向けには，遅延時間の保証と耐タンパー性からセキュリティゲートウェイのハードウェアによる実装が望ましいと考えており，これまで得られた知見から，ハードウェアベースの動的なフィルタ機構を持ったセキュリティゲートウェイを設計・実装し，シミュレーションおよび実車で評価することが可能である．また，自動車の開発時に ECU やゲートウェイを含む車載 LAN 全体の脆弱性を検査するツールが必要となってくることから，いわゆるファジングテスト[6][7]を効率的に行う手法が求められている．ファジングテストにおけるファズデータの生成にはノウハウが必要であり，現場でどのようにしてファジングツールの入力に変換すれば良いかという点が課題となっている．現在，攻撃検証用プラットフォームで得られる脅威のモデル化の知見を用いて[8][9]，ファジングテストという現場の作業を連携させる方法等が必要となってくる．

２．研究の目的

セキュリティゲートウェイにおける車載 LAN や ECU に対する攻撃手法に対する検出アルゴリズムや動的なフィルタリングルールの生成手法と有効性について検討を行う．コネクティッドカーの外部インタフェースを介した攻撃に対する事例分析と対策案の検討を行い，動的なフィルタリング機構のソフトウェアでの実現および実車での評価を行い，セキュリティゲートウェイを中心としたシステム全体のモデルを設計する．これまでの研究から CAN を用いた車載 LAN の脆弱性や攻撃の検出手法について，周期解析やトラフィックパターン分析に基づく定量的な評価基準を定式化する．ファジングによるテストについては，ファズデータ生成に脅威モデリング連携型ファジングテスト手法を検討し，効果的な攻撃データであるファズデータの生成とフィードバックを可能にする．また，認証機構や，動的なフィルタリング機構，特にトラフィックパターン分析や機械学習アルゴリズムの評価のために，クラウドベースの開発評価プラットフォームを構築する．この開発評価システムでは，車載 LAN のトラフィックは全て情報管理サーバ上のデータベースに時刻情報や車両 ID と共に蓄積され，サーバ上で分析したり，速度やエンジン状態などの意味のある情報に加工したり，他の処理サーバに渡したりということができる．この際，全ての車載 LAN データをサーバに送信するには大きなネットワーク帯域を消費してしまうので，CAN データの特徴を利用したデータ圧縮の手法を検討し実装・評価する．

３．研究の方法

セキュリティゲートウェイでの動的なフィルタリング機構として，DoS 攻撃の検出やなりすまし攻撃の検出アルゴリズムを検討する．FPGA を用いた基本的なフィルタリング機構を実装し，テスト用の CAN トラフィックのログデータを入力として，フィルタリング回路における平均処理時間を算出し，ソフトウェア実装と比較する．また，同じ機械学習フレームワークを利用したソフトウェアによる実装と比較する．

ファジングデータの生成とフィードバックによるファジングデータの再構成[10]については，機械学習アルゴリズム r-VAE の仕組みを CAN メッセージの時系列データに適用することで，入力データの値の特徴量を保持したまま曖昧化させた出力データを得ることができる可能性がある[11]．この出力データを CAN におけるファジングテストのテストデータに用いることで，実際に車両でやりとりされる CAN データの特徴量を持ったテストデータが得られ，ファジングテストに要する時間を削減しテストの効率化に寄与することができる可能性がある．例えば，CAN のペイロードの 8 バイトを 1 バイトずつ 8 次元に分け，2 次元にエンコードして特徴量を潜在変数で表現し，潜在変数をもとに再度 2 次元のデータを 8 次元にデコードする際の r-VAE のモデル構造を図 1 に示す．VAE では図中央部の再構成誤差を学習しないため，デコードした

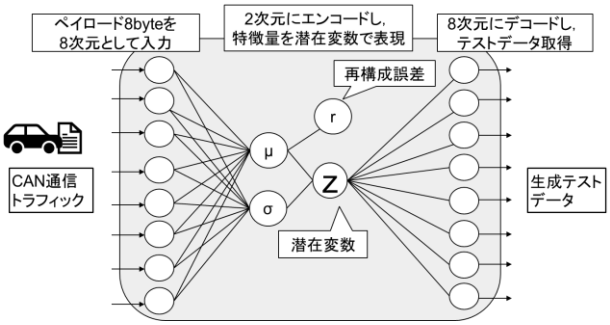

図1 r-VAEのモデル構造

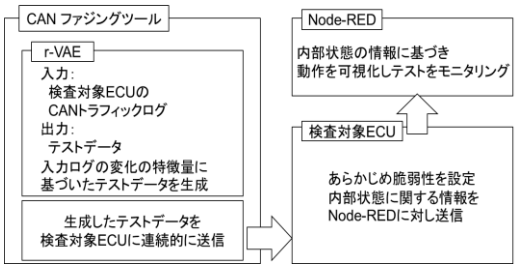

図2 評価に用いるシステムの構成

データは入力データの特徴量をそのまま保持したような出力が得られるが，r-VAE では再構成誤差を同時に学習することで単に特徴量を保持するのではなく，同時に学習する再構成誤差の分，出力データの値域が大きくなり，結果として入力データの値域を包括するようにデータを曖昧化した出力データを得られる．入力データの値域を包括するという特徴により，境界をカバーするようなテストデータを生成することができる可能性がある．これらの機械学習モデルの特徴をふまえ，検査対象の ECU が受け取る CAN メッセージのデータの特徴量を r-VAE を用いて学習し，その特徴量を保持したまま曖昧化された出力をテストデータとして得る．実際に車両で使用されるデータの値域を包括するテストデータを使用し，データの意味の境界に対し十分にテストを試行することで，テストの信頼性を保持したままテストデータを最低限まで削減しテストに要する時間を削減し，テストの効率を向上させられる可能性がある．この評価を行うために図 2 のようなシステムを構築する．

車載 LAN で用いられる通信プロトコルである CAN メッセージのうち車載システムの解析に必要な情報は CAN メッセージ中の CAN ID とペイロード，および送信時刻であるタイムスタンプとなる．加えて，クラウドにデータを送信するデータロガーおよび圧縮器は，組込みシステムである車載器に組み込む際にマシンパワーが要求されることが想定される[12][13]．そこで，CAN ID とペイロード，タイムスタンプの特性を考慮し圧縮することで，車載トラフィックのデータ量を削減する手法を検討する．CAN ID とペイロードの値は出現頻度とデータのフォーマットが事前に分かっているので，出現確率に基づくハフマン符号化を適用し，タイムスタンプは，メッセージの前後での相対的時間差をランレングス符号化を行うことで圧縮を試みる．

４．研究成果

セキュリティゲートウェイでの動的なフィルタリング機構のソフトウェアでの実現を組込み機器である Raspberry Pi を用いて行い，実車のトラフィックで評価を行った．組み込み機器で十分なフィルタリング性能は得られたが，正答率については大きな改善はできておらずアルゴリズムやパラメータの調整が必要であった．また，CAN メッセージのデータフィールドの関係や周期解析に基づき，攻撃検知や ECU の動的解析を可能とする目処が付いた．次に，FPGA を用いた基本的なフィルタリング機構を実装し，テスト用の CAN トラフィックのログデータを入力として，フィルタリング回路における平均処理時間を算出した．同じ機械学習フレームワークを利用したソフトウェアによる実装と比較した結果，FPGA 処理では平均処理時間は 0.73 μ s，標準偏差は 0 となり，ソフトウェアによる実装よりもフィルタリングに要する時間とその揺らぎが大きく減少することを確認した．また，これらの実験で得られた知見から，車載システムにおける攻撃のパターンをいくつかに分類し標準的なデータセットとして提供できるようにすることの検討を始めた．実車から取得した正常データに対して，攻撃パラメータを設定することで，攻撃状態のデータセットを自動生成するようなプログラムの開発を行った．

車載システムにおける攻撃のパターンをいくつかに分類し標準的なデータセットとして提供できるようにすることの検討を実施した．攻撃としての有効性の評価には機械学習モデル r-VAE アルゴリズムを適用することで，多次元の入力データを低次元にエンコードする際に特定の次元の再構成誤差を学習させることで，入力データの特徴を大きく変えることなく出力データの再構成誤差のみを変化させることができ，CAN トラフィックのペイロードを多次元の入力データとして学習し入力データの特徴量を持ったファジングデータを生成できることを確認した．

情報管理サーバ上のデータベースに時刻情報や車両 ID と共に蓄積するためのサーバシステムのデータ処理部は Elasticsearch を用いて，GUI 部分は Kibana を用いて実装することで，取得した車載 LAN のデータをサーバ上で分析したり，速度やエンジン状態などの意味のある情報として可視化することができるプロトタイプを完成した．高速かつ大容量データを一度に処理することが可能とするための情報管理サーバ上のデータベースに時刻情報や車両 ID と共に蓄積するためのシステムは，HyperVisor 上で動作する VM（仮想マシン）として実現している．これ

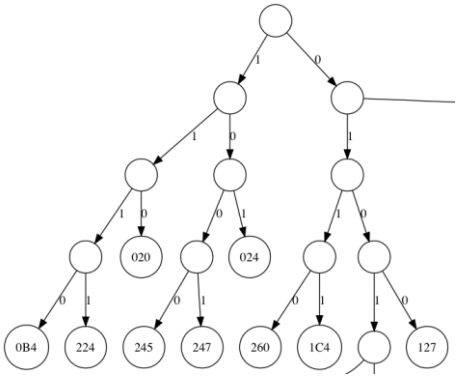

図 3 車種 X における CAN ID のハフマン木の一部

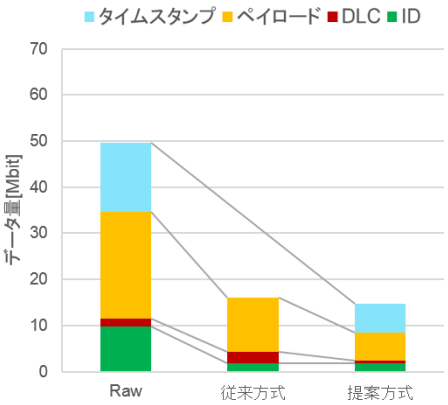

図 5(a) 車種 X における各方式のデータ量の比較

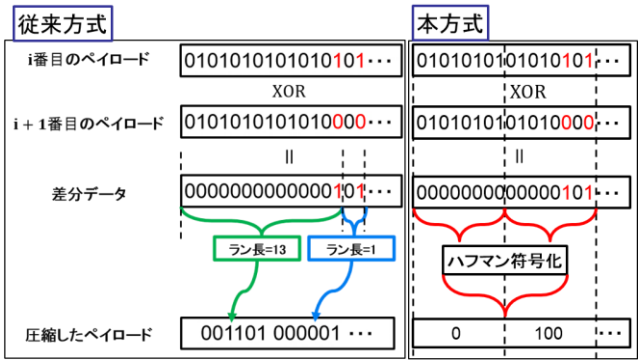

図 4 従来方式と提案方式の違い

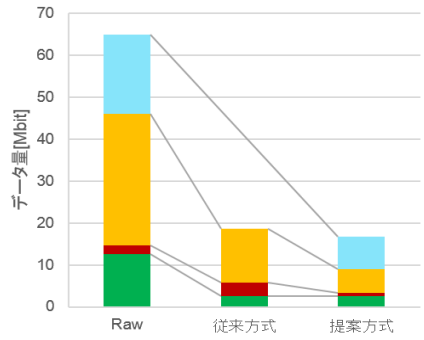

図 5(b) 車種 Y における各方式のデータ量の比較

により，取得した車載 LAN のデータをサーバ上で分析したり，速度やエンジン状態などの意味のある情報に加工したり，他の処理サーバに渡したりということができるようになった．

このデータ取得蓄積システムでは，通信路のデータ量が多いことが問題であり，その削減のために，CAN 特有の性質を利用し，元データの 4 分の 1 から 5 分の 1 に圧縮する目処がついた．なお，以前は 2 分の 1 程度の圧縮となっており，大幅がデータ量の削減が可能となった．メッセージの圧縮に関しては，図 3 のようなハフマンリストを車種毎に作成しする手法を利用して従来方式より大きな圧縮率を実現している（図 4）．従来方式と比較するとペイロード部分の圧縮率が大きく向上したことによりメッセージ全体の圧縮率も 2 倍程度に向上し，車種 X で 24.4%に，車種 Y で 19.5%となった（図 5(a),(b)）．すなわち元の車載 LAN のデータを 4 分の 1 から 5 分の 1 に圧縮でき，クラウドにデータを送信する際の通信帯域を大きく減らすことが可能となった．なお，本方式では車種毎の CAN ID とバイト列の出現頻度に基づき，特定の圧縮方式を適用することで圧縮率の向上を実現しているため，車種によって圧縮率は異なる．自動車は組込みシステムにつき，CAN メッセージの出現頻度に基づくリストを事前に作成することは可能であり，従来方式では同一の圧縮方式を適用していたペイロードの圧縮の部分で大きな改善が可能になったと考えられる．

参考文献

[1] C. Miller, C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” BLACKHAT USA 2015, pp.1-91, Aug. 2015.

[2] 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.

[3] 伊達友裕，手柴瑞基，江崎貴也，井上博之，“車載 LAN の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ルール生成,” 暗号と情報セキュリティシンポジウム SCIS2016, pp.1-6, Jan. 2016.

[4] K. Iehira, H. Inoue, K. Ishida, “Spoofing Attack Using Bus-off Attacks against a Specific ECU of the CAN Bus,” Proceedings of IEEE Consumer Communications & Networking Conference (CCNC2018), Jan. 2018.

[5] 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,” マルチメディア、分散、協調とモバイル (DICOMO2017)シンポジウム, pp.1163-1168, June 2017.

[6] S. Daniel, S. Fowler, J. Bryans, S. A. Shaikh, P. Wooderson, “Fuzz Testing for Automotive Cyber-security,” IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, pp.239-246, 2018.
[7] 松本，小林，土屋，吉田，森田，萱島，“車載 ECU に対する CAN 経由のファジング手法,” SCIS2015, pp.1-8, Jan. 2015.
[8] 城間政司，西尾泰彦，井上博之，“USB 周辺機器接続のセキュリティリスク分析におけるアセット導出手法,” 情報処理学会論文誌, vol.59, no.1, Jan. 2018.
[9] 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.
[10] 藤倉俊幸，倉地亮，“AutoEncoder を利用した攻撃検知のための CAN パケット分析,” SCIS2019, pp.1-6, Jan. 2019.
[11] 松永昌浩，チャンクワンカイ，“r-VAE: VAE への再構成誤差の取り込みと時系列データ曖昧化への応用，” CSS2019, pp.1504-1511, Oct. 2019.
[12] Yu-jing WU, Jin-Gyun CHUNG, “Efficient controller area network data compression for automobile applications,” Front Inform Technol Electron Eng 2015, vol.16, pp.70-78, Jan. 2015.
[13] Supriya Kelkar, Raj Kamal, “Boundary of Fifteen Compression Algorithm for Controller Area Network Based Automotive Applications,” Proceedings of 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications, pp.162-167, Apr. 2014.

５．主な発表論文等

〔雑誌論文〕　計6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　2件）

１．著者名 Hossain Md Delwar、Inoue Hiroyuki、Ochiai Hideya、Fall Doudou、Kadobayashi Youki	４．巻 8
２．論文標題 LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communications	５．発行年 2020年
３．雑誌名 IEEE Access	６．最初と最後の頁 185489～185502
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.3029307	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 S. Ohira, A. K. Desta, I. Arai, H. Inoue, and K. Fujikawa	４．巻 8
２．論文標題 Normal and Malicious Sliding Windows Similarity Analysis Method for Fast and Accurate IDS against DoS Attacks on In-vehicle Networks	５．発行年 2020年
３．雑誌名 IEEE Access	６．最初と最後の頁 42422-42435
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.2975893	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 大平修慈，井上博之，新井イスマイル，藤川和利	４．巻 60
２．論文標題 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	５．発行年 2019年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 791-802
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 鈴木陵馬，金森健人，家平和輝，井上博之，石田賢治	４．巻 -
２．論文標題 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	５．発行年 2018年
３．雑誌名 マルチメディア、分散、協調とモバイル(DICOMO2018)シンポジウム予稿集	６．最初と最後の頁 879-884
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 大平修慈，新井イスマイル，井上博之，藤川和利	４．巻 -
２．論文標題 車載インフォテインメントシステムにおけるホワイトリストと遅延付加によるCANバス上のDoS攻撃緩和手法	５．発行年 2018年
３．雑誌名 コンピュータセキュリティシンポジウム2018（CSS2018)予稿集	６．最初と最後の頁 1128-1133
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 石長篤人，井上博之，石田賢治	４．巻 -
２．論文標題 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	５．発行年 2018年
３．雑誌名 2019年 暗号と情報セキュリティシンポジウム（SCIS2019)予稿集	６．最初と最後の頁 1-8
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計12件（うち招待講演　9件／うち国際学会　0件）

１．発表者名 井上博之
２．発表標題 サイバーセキュリティ概論
３．学会等名 自動車工学基礎講座（オンライン）（招待講演）
４．発表年 2021年

１．発表者名 鈴木陵馬，林侑香里，井上博之，石田賢治
２．発表標題 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
３．学会等名 電気・情報関連学会中国支部連合大会2020
４．発表年 2020年

１．発表者名
木田良一，渥美清隆，鈴木陵馬，井上博之

２．発表標題
車載ネットワークCANの侵入防止システムの実装と評価

３．学会等名
2020年 暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
上村孔明，井上博之，大平修慈，石田賢治

２．発表標題
車載LANメッセージの出現頻度と変化量を利用したリアルタイムデータ圧縮方式

３．学会等名
情報処理学会、マルチメディア、分散、協調とモバイルシンポジウム

４．発表年
2019年

１．発表者名
井上博之

２．発表標題
サイバーセキュリティ

３．学会等名
自動車工学基礎講座（栃木）（招待講演）

４．発表年
2020年

１．発表者名
井上博之

２．発表標題
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

３．学会等名
サイバーセキュリティ対策セミナー2019冬 基調講演（招待講演）

４．発表年
2019年

１．発表者名
井上博之

２．発表標題
IoTシステムとしてのコネクティッドカーの情報セキュリティ

３．学会等名
広島市立大学産学連携発表会2019（招待講演）

４．発表年
2019年

１．発表者名
井上博之

２．発表標題
自動車サイバーセキュリティ

３．学会等名
第61回自動車工学基礎講座（広島）（招待講演）

４．発表年
2019年

１．発表者名
井上博之

２．発表標題
自動車サイバーセキュリティ

３．学会等名
第54回自動車工学基礎講座（広島）（招待講演）

４．発表年
2018年

１．発表者名
井上博之

２．発表標題
車載ネットワークセキュリティへの機械学習の適用

３．学会等名
電子情報通信学会ソサイエティ大会 PN/NS/IN研究会共催企画シンポジウム（招待講演）

４．発表年
2018年

１．発表者名 井上博之
２．発表標題 AIによるネットワークの進化とその取り組み
３．学会等名 PN/NS/IN研究会共催企画シンポジウム パネルセッション（招待講演）
４．発表年 2018年

１．発表者名 井上博之
２．発表標題 コネクティッドカーに潜むリスクとセキュリティ対策
３．学会等名 九州サイバーセキュリティシンポジウム（招待講演）
４．発表年 2019年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称 データ信号記録装置	発明者 井上博之，上村孔明， 大泉尚之，小林正利， 神山裕	権利者 同左
産業財産権の種類、番号 特許、特願2019-117768	出願年 2019年	国内・外国の別 国内

〔取得〕　計0件

〔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