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　４ 年　 ６ 月　 ５ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１２１２

研究課題名（和文）自動車の制御モデルに対するセキュリティ強化と評価手法

研究課題名（英文）Security measure and evaluation method for automobile control model

研究代表者
倉地　亮（Kurachi, Ryo）

名古屋大学・情報学研究科・特任准教授

研究者番号：１０５６８０５９

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）：本研究では，自動車のサイバーセキュリティ確保に向けた車載電子制御システムに対する設計手法や検証手法の確立を目的とする．車載電子制御システムには，ECU(Electronic Control Unit)と呼ばれる制御用のコンピュータが多数搭載された分散制御システムであり，安全に自動車の走る・止まる・曲がるを実現することが求められる．近年では，セキュリティ上の脅威が多数指摘されており，今後は，自動運転の実現もあり，ますますサイバーセキュリティ強化が必須になることが予想されている．このため，本研究では，これらを対象に脅威の分析手法，攻撃手法に対抗する強化策，評価手法などを包括的に研究した．

研究成果の学術的意義や社会的意義
国際基準や国際標準が策定されたことにより，自動車の制御システムのサイバーセキュリティ強化が必須となってきている．このため，自動車の設計時に脅威を分析し，評価し適切な強化策を導入することが要求されている．しかしながらその一方で，どのように分析，強化，評価すべきかの手法は確立されていないことが課題である．このため，本研究ではこれらの手法の確立と業界標準技術としての提案を目指す．

研究成果の概要（英文）：This research focuses on establishing design, countermeasure, and verification methods to ensure cybersecurity for automobiles. An in-vehicle system is a distributed control system with many control computers called ECUs (Electronic Control Units), which are required to realize safe driving. Moreover, the proliferation of technologies for connected and autonomous vehicles increases the potential of cyber-attacks. Therefore, this study comprehensively researched threat analysis methods, countermeasures, and evaluation methods for next-generation in-vehicle systems.

研究分野：計算機システム

キーワード：組み込みシステム　組込みセキュリティ　情報セキュリティ　自動車　評価手法　設計手法

１．研究開始当初の背景

近年，自動車のセキュリティ脅威が多数報告されており，徐々に販売される自動車にもセキュリティ強化策が適用されつつある．さらに自動運転やコネクテッドカーと呼ばれる将来技術が導入されると，サイバーセキュリティ強化はより重要になる．より具体的には，交通事故が発生した場合，ドライバが操舵を誤ったのか，自動車の制御システムに欠陥があったのか，それともサイバー攻撃により操舵をのっとられたのかが判断できない可能性がある．そこで，本研究では自動運転時代の車載制御システムを対象に，セキュリティ強化策，評価技術，分析手法を研究した．

２．研究の目的

本研究では，自動走行システムの実現に向けて大きく変化することが予想される自動車の電子制御システムに対するセキュリティ強化策の検討とその評価手法の確立を目指している．そこで，本研究では以下の 3 つのサブテーマに分割し研究開発を進めた．

まず，１つ目のサブテーマ“設計手法”として，車載電子制御システム内で適用可能な新たなセキュリティ強化策の研究開発を目的とした．本研究では，Controller Area Network(CAN)と SOME/IP プロトコルという 2 つのプロトコルを対象にした．次に，2 つ目のサブテーマ“評価手法”として，自動車のセキュリティの評価手法を研究開発することを目的とした． 最後に，3 つ目のサブテーマ“分析手法”として，国際標準規格によるとセキュリティエンジニアリングプロセスの確立が要求されており，設計段階での脅威分析や脆弱性分析等が要求されている．特に，自動車の安全性とセキュリティの両立が要求されており，複雑な分散制御システムとして構成される自動車の電子制御システムに対して適用可能な分析手法を確立することを目的とした．

３．研究の方法

本研究では，まずサブテーマ１の設計手法の開発においては，自動運転時代の電子制御システムとして，将来のシステム構成を検討し，それに適用されるプロトコルである CAN と SOME/IP プロトコルに着目し，それらの強化策を検討した．これらの将来のシステム構成を検討するにあたり，幾つかの自動車関連の企業の方にヒアリングを実施し，10 年後の将来像として適切と思われる構成を検討した．次に，サブテーマ 2 の評価手法においては，実際に販売される自動車や機器を評価対象にすることにより，現状の機器がどれぐらいセキュリティ強化されているのかを検証した．さらに，事故調査時に解析される Event Data Recorder（EDR）のセキュリティ耐性についても検証し，デジタルフォレンジックの観点でも評価した．最後に，サブテーマ 3 の分析手法では，実際の自動車の機能をモデル化し，それらを分析するための手法について検討した．これにより，複雑なシステム構成において，どの攻撃がより深刻な被害をもたらす可能性があるかを検証することを可能にした．

４．研究成果

<u>○サブテーマ１の設計手法の開発の成果</u>

車載制御システムに異常が発生すると，自動車の修理工場や販売店にて，車両に設置された診断機器用のコネクタから Electronic Control Unit(ECU)と呼ばれる電子制御用コンピュータの故障診断を実行する．このとき，車両外部からのアクセスに対して十分な認証が適用されていないため，悪意のある整備士などにより機器を妨害や改ざんできてしまうことが課題であり，これらのアクセス制御（認可機構）を検討した．より具体的には，将来システムとして 2 つのネットワーク構成を仮定し，セントラルゲートウェイ(CGW)型ネットワークにおいてはセントラルゲートウェイが，セントラル ECU 型ネットワークにおいてはセントラル ECU が認可のための情報を保持することにより実現する．また，整備士等の診断機能の利用者は自動車会社から発行された認可用の証明書を用いて，車両外部からアクセスすることにより不正アクセスを防止することができる．これにより，診断通信による車両外からの不要なアクセスを遮断できることが可能になる．

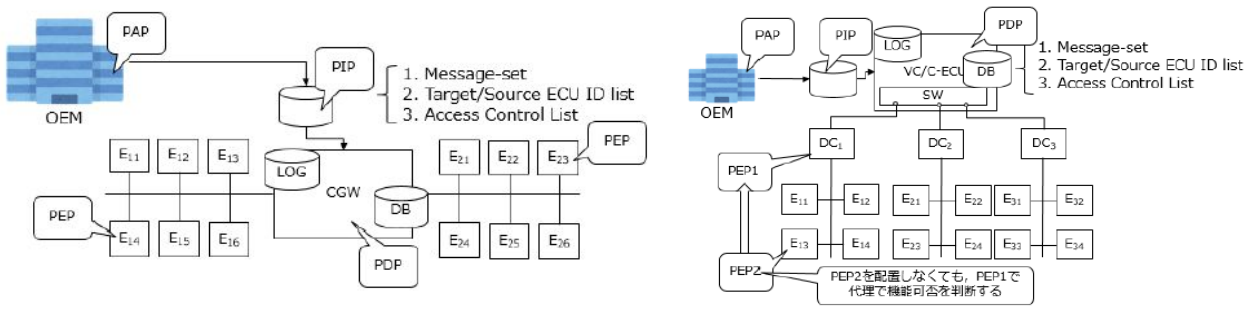


図 1．セントラルゲートウェイ型(左上)およびセントラル ECU 型(右上)のシステムの認可機構

さらに，車載制御システム内に配置される侵入検知システムに適用される様々なアルゴリズムが提案されている．その内，周期的に転送される CAN メッセージの転送周期のズレにより異常を検出する既存アルゴリズム

が存在している．このアルゴリズムの問題点は，CAN ネットワーク上の通信負荷により，本来転送されるべき周期とのズレは大きくなるため，通信負荷が高いシステムでは適用できないことが課題である．この問題に対応するため，周期的に発生する送信要求時刻からの遅延時間をハードウェアでカウントし，その遅延時間情報を通信メッセージに付与する通信コントローラとして Delay-time Deliverable CAN (DDCAN)を提案した．

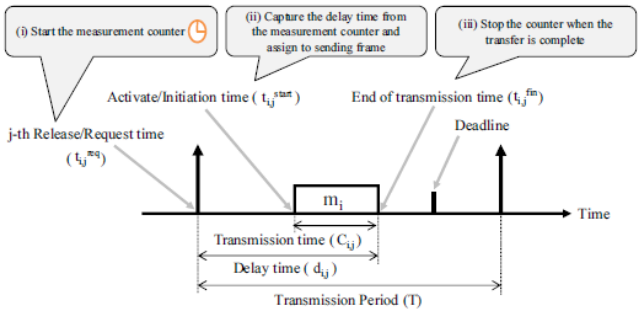


Fig. 3: Concept of delay time measurement

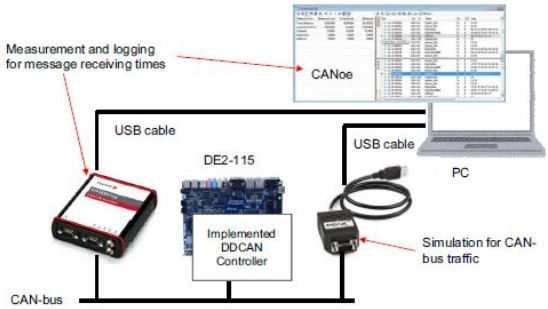
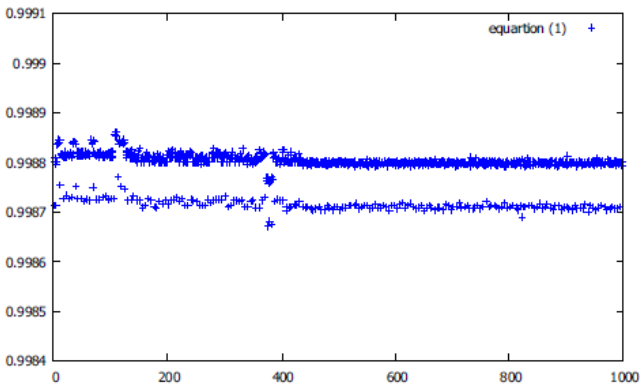


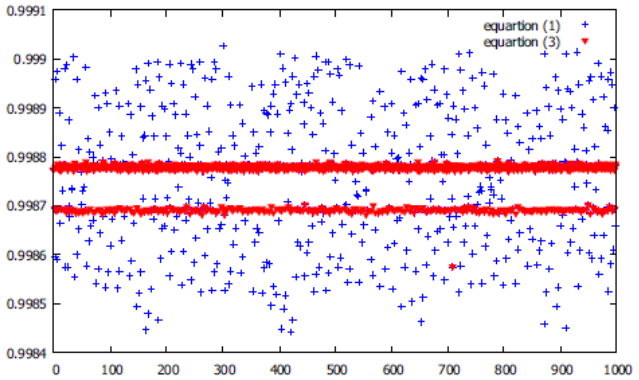
Fig. 9: Experimental environment for simulated CAN-bus system

図 2．Delay-time Deliverable CAN (DDCAN)のモデル(左上)と実装後の評価環境(右上)

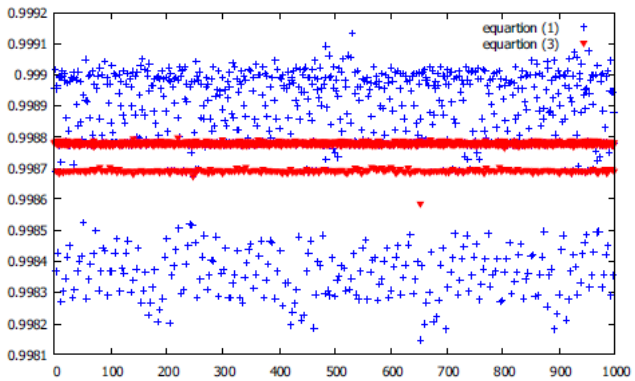
以下の図 3 に示す通り，ネットワークに通信負荷をかけた場合でも，DDCAN を適用する場合では，適用しない場合に比べて，ほぼ正確な周期を導出できたことを示している．より具体的には，DDCAN では通信負荷に対して変動なく，通信負荷がない場合の(a)と同様の通信周期を取得できることを確認した．この結果より，DDCAN を適用する場合には転送周期を監視する場合に誤検知を低減することが可能となることを示した．



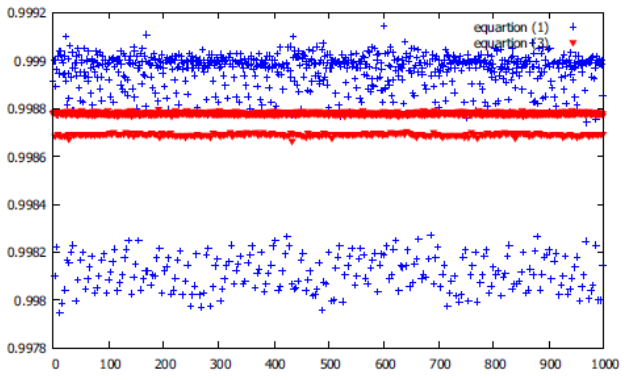
(a) Operation without any other traffic.



(b) 25% CAN-bus traffic.



(c) 50% CAN-bus traffic.



(d) 75% CAN-bus traffic.

図 3．DDCAN の通信負荷状況(0，25，50，74%)ごとの遅延時間の評価結果(0%以外は赤線)

さらに，　CAN メッセージに付与されるメッセージ認証コード等の認証情報分の通信オーバーヘッドが課題となる．この課題を解決するために，メッセージ認証コードを極力付与せずにメッセージを保護する手法が必要とされている．このため，本研究では，図 4 に示すようなメッセージ認証コードを最小化するためのアルゴリズムを検討した．これにより，すべてのメッセージにメッセージ認証コードを付与する従来手法と比較し，

本提案手法では最大 41 パーセントの通信負荷を低減できることを確認した．

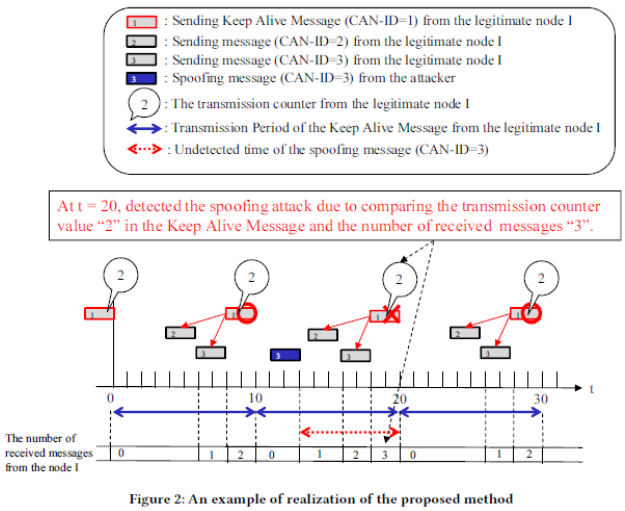


Figure 2: An example of realization of the proposed method

Algorithm 2: MONITORING ALGORITHM OF SECURE KEEP ALIVE MESSAGES ON CAN

Input: KAM_i: Receive Keep Alive Message i
Output: δ: Result of whether spoofing messages arrived within the interval of KAM_i

1 // Step1. Get the number of receiving messages (Cnt^I_{rcv}) from the table (*Monitroing_Table*) of storing the number of messages sent from the nodes I ;
2 $Cnt^I_{rcv} \leftarrow$ *Monitroing_Table*;
3 // Step2. extract the transmission counter (Cnt^I_{tr}) after verification of the MAC in KAM_i;
4 $Cnt^I_{tr} \leftarrow KAM_i$;
5 // Step3. Verify Cnt^I_{tr} and Cnt^I_{rcv} match;
6 **if** $Cnt^I_{tr} \neq Cnt^I_{rcv}$ **then**
7 // Found the spoofing messages;
8 $\delta \leftarrow$ TRUE;
9 **else**
10 $\delta \leftarrow$ FALSE;
11 // Step4. Clear the counter Cnt^I_{rcv};
12 $Cnt^I_{rcv} \leftarrow 0$;
13 **return** δ ;

図 4．メッセージ認証コードを最小化するためのアイデア(左上)とアルゴリズム(右上)

○サブテーマ 2 の評価手法の開発の成果

まず，ISO14229 として国際標準化された診断通信プロトコルが自動車にて広く適用されている．この中に外部から接続する診断機を認証するためのプロトコルとしてセキュリティアクセスが定義されている．しかしながら，このセキュリティアクセスによる認証を突破できると各 ECU は診断状態に遷移し停止ししてしまうため，このセキュリティアクセスがどれぐらい突破可能かを実際に販売される車両 3 台で実験を行った．この結果，図 5（右）に示すようにセキュリティアクセス自体を突破することができたのと同時に，図 6 に示すように，最短で 30 分程度で突破できる ECU が存在することを示した．今後は，より高度なセキュリティアクセスの実装と標準化が必要であることを指摘した．

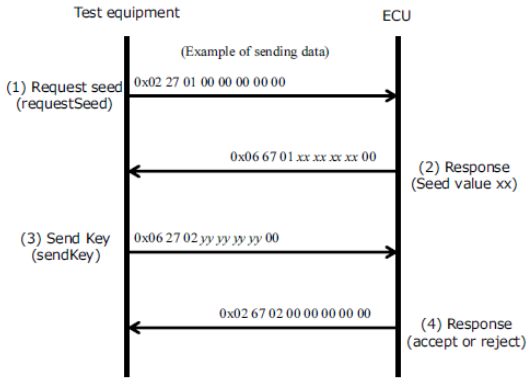


Fig. 1. Security access service sequence on UDS

TABLE I
SECURITY ACCESS SERVICE EVALUATION RESULTS IN REAL VEHICLES

Evaluation Items		Car A	Car B	Car C
1. Number of evaluation CAN IDs		21	41	22
2. Number of evaluated session types		66	55	79
3. Total number of security access service		75(19)	26(16)	31(17)
4. Seed length	(4-1) 1 or 2 bytes	1(1)	3(2)	1(1)
	(4-2) 3 or 4 bytes	53(18)	8(5)	12(7)
5. Regular pattern in seed values	(5-1) Always same value	3(1)	3(1)	5(3)
	(5-2) Same value in multiple times	20(14)	1(1)	7(7)
	(5-3) Always difference	9(2)	8(5)	0(0)

In this table, the number indicates the number of services. Then, "()" indicates the number of CAN-IDs.

図 5．UDS のセキュリティアクセスのシーケンス(左上)と車両 3 台における評価結果（右上）

TABLE II
AVERAGE TIME AND NUMBER OF ATTEMPTS REQUIRED UNTIL BRUTE FORCE ATTACK SUCCESS

Evaluation Item	Results(times or hours)
Average attempt	28,412,000
Average time required	47.3 hours
Minimum time required	0.5 hours
Maximum time required	108.8 hours

図 6．セキュリティアクセスをブルートフォース攻撃で突破できるまでの時間

次に，近年販売される自動車にはエアバッグが搭載されており，事故時の衝撃によりエアバッグが展開することで人命を守ることが可能となっている．このエアバッグを制御する Airbag Control Module(ACM)には，

エアバッグ展開時の車両の動作状態が記録されており，交通事故調査において，この記録が読みだされ事故状況の検証に用いられている．この記録機能のことを一般的に Event Data Recorder(EDR)と呼んでいる．今後は，サイバー攻撃による事故が発生した場合には，これらの記録が攻撃の証拠の１つになることが考えられる．このため，本研究では，実際の車両に搭載される ACM を用いて，図 7（右）に示す模擬車両環境にてサイバー攻撃による事故を発生させた場合，(1) 攻撃の記録が残るかどうかを検証した．さらに，(2) これらの EDR の機能を悪用して，攻撃者が記録を改ざんすることができるかを検証した．本研究の実験結果より，(1)により，攻撃の記録が残ることを確認した．さらに，(2)により，攻撃者にｙり EDR の記録が改ざんされる可能性があることも確認した．これらの脅威の対抗策として記録の保護や認証技術が必要であることを明らかにした．

表 1. EDR の記録内容の一部抜粋

データ要素	その他
車速	Pre-Crash data (-5 to 0 seconds) 衝撃前データ(-5秒から0秒)
ブレーキのON-OFF	
エンジンスロットルまたはアクセルペダル、開度	
エンジン回転数	
安全ベルトの状態、運転席	Pre-Crash data (1 sample) 衝撃前データ(1サンプル)
安全ベルトの状態、助手席	
助手席の占有状態	
運転手のシートポジション	
シフトポジション	
前後方向の速度の累積変化	Crash Pulse Data 衝撃後に記録するデータ
左右方向の速度の累積変化	
車両ロール角	
前後･左右方向の速度の最大変化	
診断故障コード	Pre-Crash DTC Information 衝撃前の診断故障コード情報

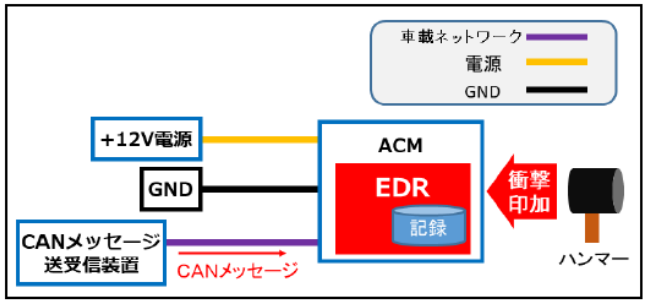


図 3. 実験環境の構成図

図 7. EDR の記録内容の一部抜粋(左上)と実験環境の構成図(右上)

さらに，自動車のデジタルフォレンジックに関する研究として，カーナビやディスプレイ等を統合した車載インフォテイメントユニットと呼ばれる情報端末にサイバー攻撃の証拠が残るかを評価した．この結果，デジタルフォレンジックの観点で攻撃の証拠になりうるいくつかの証拠を補える可能性があることを確認し，EDR と連携することで事故の証拠を保全する手法についても同様に提案した．

表 3. 攻撃シナリオにおけるデジタル・フォレンジックに必要となる電磁的記録の充足性

観点	デジタル・フォレンジックに必要となる電磁的記録の例	EDR	インフォテインメントシステム	
			既存	追加提案
When	各事象の時刻情報	△	○	-
Where	不正なCAN信号の送出元機器	×	×	○
	攻撃対象	△	△	-
Who	攻撃に使用されたアカウント情報	×	○	-
	不正アクセスに使用されたIP	×	○	-
What	不正なCAN信号の実データ	△	×	○
	電子機器内で実行されたコマンド	×	○	-
Why				

○：取得可能　△：一部の情報のみ取得可能　×：取得不可

図 8．車載インフォテイメントユニットと EDR を用いた電磁的記録の組み合わせ

○サブテーマ 3 の分析手法の開発の成果

自動ブレーキアシステムシステムの攻撃パスの導出方法を検討した．より具体的には，実際のシステムからシステムをモデル化した．その上で，各制御信号の入出力と攻撃が任意の制御タイミングで入ると異常が発生するか LTL 式を用いて検証した．この結果，図 9（右）に示すように，397 の制御パスと 77 の遷移状態が導出され，それらの中から最も深刻な攻撃が発生するタイミングを導出する手法を確立した．

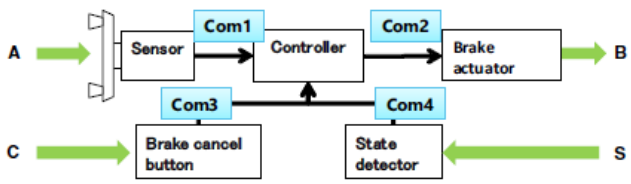


Fig. 2. Logical Structer of a Brake Assist Systeml

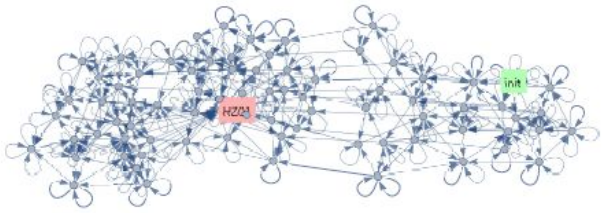


Fig. 4. A Minimized Generator with the Partial Scenario

図 9．自動ブレーキアシストシステムの論理モデル(左上)と LTL 式から導きされた遷移状態と制御パス(右上)

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 上田浩史，倉地亮，本田晋也，高田広章，足立直樹，宮下之宏	４．巻 194
２．論文標題 Controller Area Network (CAN)の不正送信防止機構の提案	５．発行年 2019年
３．雑誌名 SEIテクニカルレビュー	６．最初と最後の頁 80-85
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 オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計24件（うち招待講演　0件／うち国際学会　9件）

１．発表者名 Toshiyuki Fujikura, Ryo Kurachi
２．発表標題 A Simultaneous Attack Scenario Generation Method Using the Parallel Behavior Model
３．学会等名 The 2020 IEEE 91st Vehicular Technology Conference (VTC2020-spring)（国際学会）
４．発表年 2020年

１．発表者名 倉地亮，高田広章，足立直樹，上田浩史，滝本周平
２．発表標題 車載制御システム向けサービス探索の脅威と保護手法
３．学会等名 2021年　暗号と情報セキュリティシンポジウム(SCIS2021)
４．発表年 2021年

１．発表者名 倉地亮，佐々木崇光，氏家良浩，松島秀樹
２．発表標題 攻撃手法のリスク分類と車載IDSアルゴリズムの適性評価
３．学会等名 2021年　暗号と情報セキュリティシンポジウム(SCIS2021)
４．発表年 2021年

１．発表者名
片山隆成，倉地亮，佐々木崇光，齋藤真生，味岡仁雅

２．発表標題
車載 Event Data Recorder のデジタル・フォレンジックに関する調査及び検証

３．学会等名
2021年　暗号と情報セキュリティシンポジウム(SCIS2021)

４．発表年
2021年

１．発表者名
倉地亮，佐々木崇光，前田学，安齋潤，松島秀樹

２．発表標題
車載制御ネットワーク向けIDPS評価プラットフォームの提案

３．学会等名
2020 Symposium on Cryptography and Information Security (SCIS2020)

４．発表年
2020年

１．発表者名
倉地亮，高田広章，足立直樹，上田浩史，滝本周平

２．発表標題
車載制御システム向け強制アクセス制御機構の提

３．学会等名
2020 Symposium on Cryptography and Information Security (SCIS2020)

４．発表年
2020年

１．発表者名
Ryo Kurachi, Kentaro Takei, Takaaki Iinuma, Yuki Sato, Manabu Nakano, Hideki Matsushima, Jun Anzai, Toshihisa Nakano, Hiroaki Takada

２．発表標題
Evaluation of Security Access Service in Automotive Diagnostic Communication

３．学会等名
2019 IEEE 89th Vehicular Technology Conference: VTC2019-Spring（国際学会）

４．発表年
2019年

１．発表者名
Ryo Kurachi, Hiroaki Takada, Naoki Adachi, Hiroshi Ueda, Yukihiro Miyashita

２．発表標題
DDCAN: Delay-time Delivable CAN network

３．学会等名
IEEE International Workshop on Automobile Software Security and Safety (A3S)（国際学会）

４．発表年
2019年

１．発表者名
Toshiyuki Fujikura, Ryo Kurachi

２．発表標題
An Attack Scenario Generation Method Using the Behavior Model

３．学会等名
The 24th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2019)（国際学会）

４．発表年
2019年

１．発表者名
Ryo Kurachi, Hiroaki Takada, Hiroshi Ueda, Shuhei Takimoto

２．発表標題
Towards Minimizing MAC Utilization for Controller Area Network

３．学会等名
The 2nd ACM Workshop on Automotive and Aerial Vehicle Security (AutoSec)（国際学会）

４．発表年
2020年

１．発表者名
Ryo Kurachi, Toshiyuki Fujikura

２．発表標題
Proposal of HILS-based in-vehicle network security verification environment

３．学会等名
SAE World Congress 2018(SAE WCX2018)（国際学会）

４．発表年
2018年

１．発表者名
Ryo Kurachi, Masato Tanabe, Jun Anzai, Kentaro Takei, Takaaki Iinuma, Manabu Maeda, Hideki Matsushima ,Hiroaki Takada

２．発表標題
Improving secure coding rules for automotive software by using a vulnerability database

３．学会等名
IEEE International Conference on Vehicular Electronics and Safety (ICVES2018)（国際学会）

４．発表年
2018年

１．発表者名
Dennis Oka Kengo, Toshiyuki Fujikura, Ryo Kurachi

２．発表標題
Shift Left: Fuzzing Earlier in the Automotive Software Development Lifecycle using HIL Systems

３．学会等名
Embedded Security in Cars Conference Europe 2018 (escar EU 2018)（国際学会）

４．発表年
2018年

１．発表者名
Ryo Kurachi, Hiroaki Takada, Naoki Adachi, Hiroshi Ueda, Yukihiro Miyashita

２．発表標題
Asymmetric key-based secure ECU replacement without PKI

３．学会等名
Workshop on Security issues in Cyber-Physical System(SecCPS)（国際学会）

４．発表年
2018年

１．発表者名
藤倉俊幸，倉地亮

２．発表標題
車載ネットワークセキュリティ検証環境の開発

３．学会等名
自動車技術会2018年春季大会学術講演会

４．発表年
2018年

１．発表者名
倉地亮，高田広章，佐々木崇光,前田学，安齋潤，松島秀樹

２．発表標題
車載制御ネットワークの侵入検知システムに対するデータセットの提案

３．学会等名
暗号と情報セキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
倉地亮，高田広章，足立直樹，上田浩史，宮下之宏

２．発表標題
次世代車載電子制御システムにおける論理的なネットワーク分離方式の検討

３．学会等名
暗号と情報セキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
藤倉俊幸，倉地亮

２．発表標題
Autoencoderを用いたCANメッセージの解析

３．学会等名
暗号と情報セキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
倉地亮，高田広章，足立直樹，上田浩史，宮下之宏

２．発表標題
時刻配送型CANネットワークの提案,

３．学会等名
組込み技術とネットワークに関するワークショップ(ETNET2019)

４．発表年
2019年

１．発表者名
倉地亮，藤倉俊幸

２．発表標題
車載ネットワークセキュリテイ～仮想およびHILS環境を利用したセキュリティ検証環境～

３．学会等名
dSPACE Japan User Conference 2018

４．発表年
2018年

１．発表者名
倉地亮，高田広章，上田浩史，宮下之宏

２．発表標題
車載制御ネットワークのバスオフ攻撃に対する強化手法の検討

３．学会等名
LSIとシステムのワークショップ2018

４．発表年
2018年

１．発表者名
味岡仁雅，倉地亮，佐々木崇光，黒崎雄介，片山隆成，下雅意 美紀

２．発表標題
車載システムに対するデジタル・フォレンジックに向けての一考察

３．学会等名
2021年　暗号と情報セキュリティシンポジウム(SCIS2022)

４．発表年
2022年

１．発表者名
倉地亮，高田広章，足立直樹，上田浩史，宮下之宏

２．発表標題
時系列データベースを用いたCANの侵入検知システムの提案

３．学会等名
2021年　暗号と情報セキュリティシンポジウム(SCIS2022)

４．発表年
2022年

１．発表者名 倉地亮，佐々木崇光，氏家良浩，松島秀樹
２．発表標題 ISO/SAE 21434プロセスを踏まえた車載IDSの要件分析
３．学会等名 2021年　暗号と情報セキュリティシンポジウム(SCIS2022)
４．発表年 2022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