Vol.2013-SLDM-160 No.6
Vol.2013-EMB-28 No.6
2013/3/13

既存 ECU を変更不要な 車載 LAN 向け侵入検知手法

大塚敏史[†1]　　石郷岡祐[†1]

近年の自動車では，制御の電子化と情報機器連携によりネットワークの重要性が高まる一方で，接続機器増加によりセキュリティリスクも高まっている．特に不正データを侵入させシステムを異常動作させるなりすまし攻撃は，論文等で実車での攻撃が実証されており対策が急務である．一方で，車載 LAN はすでに広く普及しており，既存 ECU(Electronic Control Unit)の変更はコストおよびシステム信頼性に影響を及ぼす．本研究では，既存 ECU に変更を行わずになりすまし攻撃の検知および防止が可能な侵入検知手法の実現を目的としており，本報告では，車載 LAN データの周期性を活用して高い検知精度と侵入防止機能を実現する周期検知方式を提案する．

Intrusion Detection for In-vehicle Networks without Modifying Legacy ECUs

SATOSHI OTSUKA[†1]　　TASUKU ISHIGOOKA[†1]

The in-vehicle networks in today's automobiles are generally used for computerized control of and connecting information technology devices to the automobile. On the other hand, increasing the connectivity creates greater security risks. "Spoofing attacks", in which an adversary infiltrates malicious data into the in-vehicle network and makes the automobile behave abnormally, have been proved in research papers. Therefore, automobile countermeasures to these malicious infiltrations are needed. The problem is that changing legacy ECUs will affect the development costs and dependability of the system because in-vehicle network systems have already been developed for most automobiles. We focused on developing an intrusion detection system in this study that can detect and prevent spoofing attacks without modifying the legacy ECUs. We propose in this report a detection method that can detect intrusions at a high degree of accuracy and prevent them using a cyclic period of data.

1. はじめに

近年自動車は，制御の電子化により，ユーザーに新たな価値を提供している．たとえば，ステレオカメラやレーダを利用し，外界の情報を自動車が観測し，周囲の環境情報を基に車両制御を行い，衝突を回避する運転支援システムが市場に登場している．外界情報は，今後 ITS(Intelligent Transport System)の普及により，さらに車々間，路車間連携による情報伝達が追加され，より高度な運転支援が可能になると考えられる．

また，自動車の情報化も加速しており，スマートフォンやカーナビなどの通信機器を経由して自動車とセンタが接続されている．例えば電池残量や走行情報などの車両環境情報やユーザーの要求をセンタに対して送信し，センタはインターネットの情報や複数車両の情報を分析して自動車に送信し，ユーザーや自動車が必要な情報を提供することにより，自動車の快適性と利便性を高めている．

これら機能の実現において，自動車内部の制御連携や情報集約のため，複数の ECU(Electronic Control Unit)が車載 LAN(Local Area Network)を介して通信を行う．例えば運転支援システムにより車両の停止を行う場合にも，センサ，エンジン，ブレーキ，パワートレインなどの制御を行う ECU が車載 LAN を介して互いに連携し車両制御を行う．このため高度な制御やサービスを実現するためには，車載 LAN は必要不可欠となっている．

ネットワークによる機能連携を実現する中で，車載 LAN と外界との接続機会の増加はセキュリティリスクを増加させている．制御システムにおける車載 LAN の事実上標準であり，ECU のオンボード診断やソフトウェアの更新に用いられる CAN（Controller Area Network）[1]に対するセキュリティリスクの実証論文[2][3]において，外部からの不正なデータ入力により自動車の不正制御を行う例について実証されている．特に既存の ECU になりすまして情報を送信するなりすまし攻撃は，実施が容易であり，ECU の状況認識を誤らせ不正な制御を実施する結果となるため，侵入検知や防止などの対策が急務となっている．

自動車は IT システムに比べ，安全性に影響をおよぼす制御が多く，また一般ユーザーが直接使用する機器であるため，セキュリティに関する要求は IT システムに対するものと異なる．たとえば侵入検知システムにおける攻撃の見逃し（false-negative）は，制御システムに影響を与える可能性があるため発生時の影響が大きく，誤検知（false-positive）は，自動車の使用者に対して不要な心配を与え，メーカは誤検知への対応（持ち込み修理と検査対応）にコストが発生する．そのため検知精度は重要な項目である．

一方で，車載 LAN はすでに広く普及しており，自動車に搭載される ECU の数も数十に上っており[4]，それら ECU を接続する車載 LAN システムもすでに構築されてい

†1 (株)日立製作所 日立研究所
Hitachi Research Laboratory, Hitachi, Ltd.

る. そのため既存 ECU の変更はコストおよびシステム信頼性に大きく影響を及ぼす．無変更で継続使用可能な ECU は，追加の開発コストが不要であり，生産時も量産効果によりコスト削減が可能となる. また安全面に関しても, ECU の使用実績は評価基準として有効であり，自動車向け機能安全についての国際規格（ISO26262）においても製品再利用時の安全性評価の一基準として採用されている．ECU の変更は，上記コスト面，安全面に影響を与える．

そこで本報告では，

・（方式を適用する以外の）既存 ECU を変更不要

・なりすまし攻撃の検知および防御が可能

を実現する車載 LAN 向け侵入検知手法を提案する．

２章では，関連研究として自動車および車載 LAN に対する攻撃の実証と対策方法の概要，３章では車載 LAN 概要と CAN の特徴，および提案方式であるシフト判定式周期検知について説明し，４章では既存研究と提案方式に関して, 変更量とセキュリティ性能等の項目について比較し，５章で結論を述べる．

2. 関連研究

・自動車および車載 LAN に対する攻撃実証と対策

自動車に対する攻撃実証の研究として，Hoppe らによる CAN に存在する ECU への攻撃実験がある．論文では簡易な対策として，メッセージ頻度（周期）の増加，不正使用 ID の確認, 物理層の特徴による侵入検知について提案している[5].

また別の攻撃実証の例として，Kosher らは診断端子（OBDⅡ）から CAN バスに挿入した不正データにより，ECU を不正に制御する実証を行っている[2]. さらに Kosher らが行った攻撃を，物理的な接触を持たずに，無線通信や音楽データ，診断機器経由で実現する攻撃手段を Checkoway らが実証している[3].

・車載 LAN における侵入検知および侵入防止

IT システムで用いられる侵入検知および侵入防止手法には下記方式があり，これらを車載 LAN に適用する研究が報告されている．

(1) データ認証方式：パケットに認証データを付加しデータ正当性を確認

(2) 振る舞い検知方式：データのパターンなどの振る舞いから，不正なデータを検知する

(1)の例として, Herrewege らが提案する CANAuth [6]は, CAN における後方互換性を確保したシンプルな方式で, データの認証を行っている．

(2)の例として，Mütter らは情報理論におけるエントロピーを用いて振る舞いを定義し侵入を検知する方式[7]や，車載 LAN 上で異なる振る舞いを検知する複数のセンサを組み合わせて侵入を検知する方式[8]を提案している．

また CAN プロトコルに特化した方式として，Matsumoto らは，各 ECU が，自らが送信していない自 ID のデータ送信を，エラーフレームを送信しデータを上書きして破棄する無許可データ破棄方式を提案している[9].

3. 提案方式

3.1 車載 LAN 概要

・アーキテクチャ・ネットワークトポロジ

車載 LAN のアーキテクチャ例を図１に示す．車載 LAN の通信方式は用途に応じて複数の規格が存在しており，またメーカによって車載 LAN の構成および使用方法も様々である．ここでは２例説明する．

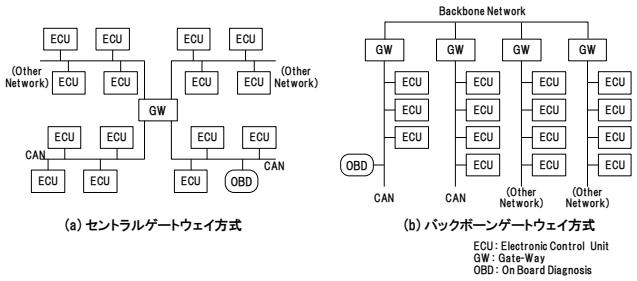

図 1　車載 LAN 構成例

図 1 (a)は，GW(Gate-Way)を中央に配置し，GW が各車載 LAN を接続する方式の例を示している. GW は各車載 LAN の情報を受信して変換し異なる車載 LAN に送信する．これにより，異なる車載 LAN に接続された ECU が通信可能となる．図 1(b)は，車載 LAN ごとに GW が存在し，バックボーン（基幹）となる車載 LAN を介して，それぞれの GW が通信する例を示している．

上記例以外にも階層的に GW を接続する構造もあるが，いずれも，異なる車載 LAN を GW が接続し ECU 間の通信を実現する．

車載 LAN の通信方式は，制御システムに用いられる CAN の他にも，軽量なプロトコルで CAN など制御システムのサブネットを構成する LIN(Local Interconnect Network)や，通信速度が高速でタイムトリガ型のプロトコルである FlexRay などがあり，近年ではマルチメディア用途など映像伝送を可能にする大容量通信プロトコルについても検討されている[10].

車載 LAN では，一般的にデータが周期的に送信されている．これにより，通信路におけるデータ消失や誤りについて一定期間後に正しいデータを受信し復帰可能であり，また送信機器や通信路の故障等によるデータの途絶を検知し，対応した制御動作を行うことが可能となる．

・CAN の特徴

現在広く制御システムで用いられている CAN については，下記の特徴がある．

(1)ネットワークトポロジがバス型

車載 LAN における CAN の多くはバス型となっており，どのノードも全データを参照でき，任意のノードから任意

のノードに対して情報送信可能であるため，攻撃（盗聴，不正データ送信）が容易である．

(2)マルチマスタ・CSMA/CD 方式で調停

CAN は通信時にマスタを持たず，調停についても各ノードが実施している．そのため任意のノードが主体的に情報を送信可能であり，調停の結果発生する衝突により送信周期が変動する．

(3)短いデータ長

全体のデータ長が短いことによりリアルタイム性が高い．しかし，ヘッダに送信者情報が含まれておらずデータ種別（CANID）のみが記載されているため，他の機器になりすますことが容易である．また最大ペイロード長も 8byte と短いため，データに対して認証情報を付加することが困難である．

従来，CAN と外部との接続は限定的で，セキュリティが問題となることはなかった．近年は自動車と外部環境の接続性が増加しており，前述の攻撃実証例[2][3]が示す通り，CAN を経由した攻撃による不正制御例が実証されている．

3.2 なりすまし攻撃

本報告では，攻撃実証例[2][3]の，(1)既存 ECU のソフトウェアを不正に書き換える，(2)不正な機器(不正な診断機・外部機器)を接続する，といった手段により，不正なデータが CAN に送信される攻撃を想定している．本研究ではその中でも，既存 ECU と同じ ID のデータを送信し，状態を誤認識させるなりすまし攻撃について対象とした．

図 2(a)は，正常時の CAN におけるデータ送信の例を示しており，横軸が時間，図の四角がデータフレームの送信期間を表しており，一定周期（T）ごとに，データフレームが送信されている状況を表している．ここでは簡略化のために，ある特定 ID を持つデータフレームのみを記載している．時間 a2 では，図に記載していない別のデータ ID を持つデータフレームの衝突によりデータの送出タイミングが遅れている例を示している．

図 2(b)はなりすまし攻撃がおこなわれている場合のデータ送信の例を示している．b0 等の時刻で送信される四角がなりすまし攻撃により送信されたデータフレームを示しており，同一 ID のデータが，異なるタイミングでデータ送信されている．そのため前記 ID のデータを受信する ECU はどちらのデータが正しいか判定できず，誤った動作を行う可能性がある．

ここで攻撃者が正常データを破棄することは想定していない．CAN においては，データの通信エラーを検出するために送信 ECU は送信後もデータを監視しており，例えば攻撃者が不正にデータを破壊した場合，送信 ECU は再送処理などを行う．そのため正常データを送信 ECU に気付かれないように破棄することは困難である．そのためここではなりすまし攻撃時には，正常データと攻撃データが共にネットワーク上に存在すると仮定する．

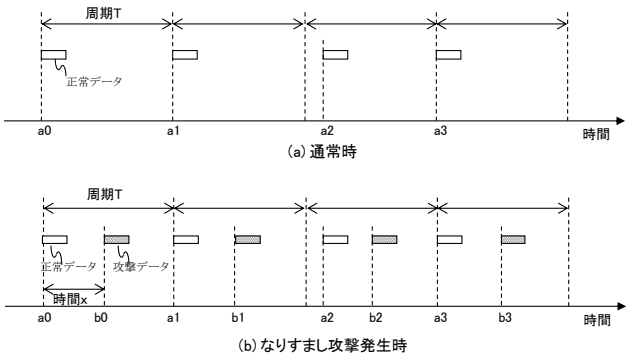

図 2　CAN 通信におけるなりすまし攻撃

3.3 周期検知における課題

なりすまし攻撃により，前記特定 ID を持つデータのバス上の発生周期は T より短くなる．

ここから短周期検出時にはなりすまし攻撃と判定することは容易であるが，単純に短周期により不正検知（例えば上記図 2 (b)例の，b0 時点のデータ受信で不正検知発生）を行うと，CAN バスのデータ衝突による送出周期の揺らぎで誤検知を発生してしまう．

例えば図 2 (a)で攻撃が行われていない場合でも，a2 と a3 の間隔は a2 時点のデータ送信時の衝突により周期 T より短くなっている．このような場合に誤検知が発生する．

3.4 シフト判定式周期検知

前記誤検知を防ぎ，さらに GW での不正なデータの転送を防止するシフト判定式周期検知について図 3 を用いて説明する．

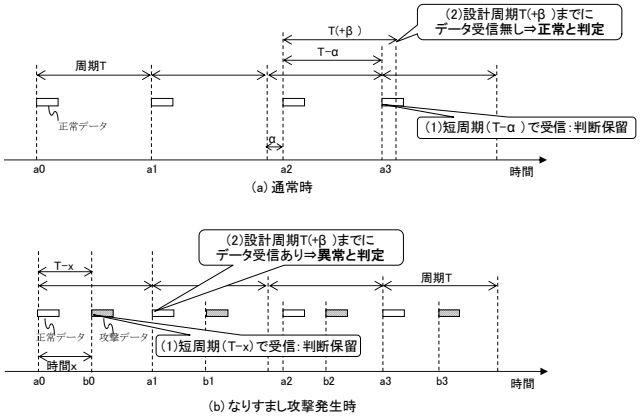

図 3　シフト判定式周期検知

図 3 (b)がなりすまし攻撃発生時の侵入検知処理例である．ECU が a0 時点でデータ処理を行った後，b0 時点で同一 ID のデータを受信した場合に，データ受信時間が前回データ受信時(a0)から設計上の周期 T を経過していないため，b0 時点で受信したデータの処理を行わずに保留する．その後（a0 でのデータ受信時から）設計上の周期 T（マージン β を含む）を経過するまでに，同一 ID のデータを a1 時点で受信した場合，なりすまし攻撃データが送信されているものと判定する．このように，b0 時点で短周期であるデータを受信後，次のデータ受信，または設計周期の到来

を待ち判定することにより，誤検知を防ぐ．

このように判定を保留することにより，図３(a)のように通常時に周期の揺らぎが発生している場合でも，誤検知を防ぐことが可能となる．これは a3 の時点で即座に侵入と判定せず，その後設計周期の到来を待ち，異常で無いと判定するためである．

また上記データを転送する GW において，侵入防止を行う場合も同様の方法で実施可能である．上記例と同様に，b0 時点のデータ受信で，データの転送処理を保留した後，a1 時点でデータを受信した場合に，GW が b0 時点で受信したデータと，a1 時点で受信したデータ共に転送を行わずにデータを破棄する．ここで b0 時点のデータおよび a1 時点のデータを共に破棄する理由は，実際の攻撃においてはどちらが正常なデータか判断困難であるためである．これにより検知だけでなく侵入防止が可能となる．

このように判定を保留することにより，通常時の周期揺らぎ時に転送処理が遅延することになる．しかし，前回データからの遅延は最大でも設計周期 T(+β)を超えることは無く，CAN を使用したシステムでは各 ECU が衝突による受信周期の揺らぎ（遅延）を想定していることから，上記受信データの遅延は問題が無いと考える．

4. 評価および考察

4.1 既存侵入検知手法との比較

本提案と，CAN における既存の侵入検知手法（(a)(b)振る舞い検知方式[7][8]，(c) 無許可データ破棄方式[9]，(d)データ認証方式[6],）の比較結果を表 1 に示す．評価項目は，変更量，セキュリティ性能，演算量，実装時に必要な情報，とした．

振る舞い検知方式は，検知方法が複数あるが，なりすまし攻撃を防ぐ方法として，(a)頻度・確率（エントロピー）計算方式と，(b)データ相関判定方式のそれぞれについて評価した．

(1)変更量

変更量は，(1-1)変更が必要な ECU（GW 含む）の数，(1-2)変更が必要な場合の，ECU ごとの変更量，について比較している．

(1-1)変更 ECU 数

提案方式および(a)(b)は，バスの通信をすべて受信可能な GW に適用すれば良く，変更は GW のみであり，図１(a)のアーキテクチャの場合には１つの GW のみを変更すればよい．図１(b)のようにすべてのバスのデータを単一 GW により直接監視できない場合は，全データについて侵入検知を実施する GW まで中継するか，それぞれの GW を変更する必要がある．ただしその場合でも GW のみが変更対象である．

(c)(d)は通信を行う ECU が変更対象となり，(c)は送信側のみ，(d)は，送受信側双方の変更が必要になる．

(1-2) 変更が必要な ECU における変更量

提案方式および(a)(b)(c)については簡易な変更（データ受信，簡易な判定演算）のみであるが，(d)は，データ長の拡張，鍵の管理，乱数生成，署名の生成および確認など多くの処理の追加が必要となる．

(2)セキュリティ性能

セキュリティ性能は３つの観点， (2-1)検知精度（誤検知および見逃しの発生し易さ），(2-2)侵入防止が可能か否か，(2-3)防御対象のデータ種類，について比較を行った．

侵入防止とは，なりすまし攻撃による不正なデータがネットワーク内部に侵入することを防ぐ機能であり，侵入を事後でも認識すれば良い侵入検知に比べ難易度が高い．

(2-1)検知精度

(c)は自分が送信している以外の自 ID の送信を検知する方式であり，また(d)は，署名データを偽造することが困難であることから，それぞれ誤検知および見逃しが発生することは非常に少ない．

一方，(a)(b)は，振る舞いについて正常・異常を判定する閾値を設定することが非常に難しい．異常を検知しやすく閾値を設定すると誤検知を起こしやすく，また誤検知を起こしにくく閾値を設定すると，見逃しが発生しやすくなる．特に，データ相関による判定方式では，２値の値を持つパラメータ（例えば ON/OFF 状態）について閾値で正常と異常を判定することは困難である．

提案方式は，CAN の周期乱れによる誤検知の可能性を，判定の保留により抑制しているため，誤検知の可能性は低く高精度でなりすまし攻撃を判定可能である．

(2-1)侵入防止

(d)は，各 ECU が受信した署名不一致データを破棄することにより，また(c)は正規の ECU が不正に送信された（自送信 ID の）ネットワーク上のデータを破棄することにより，不正な攻撃データの侵入を防ぐことが可能である．

(a)は，確率演算を事後で行っているため，不正なデータを特定して侵入を防ぐことは困難である．

(b)は，データ相関が不正なデータについては，GW 通過時に破棄可能である．

表 1　提案方式と既存方式の比較

評価項目		提案方式	(a)振る舞い(頻度・確率)	(b)振る舞い(データ相関)	(c)無許可データ破棄	(d)データ認証方式
(1)変更量	(1-1)変更ECU数	○GWのみ	○GWのみ	○GWのみ	×全送信ECU	×全送受信ECU
	(1-2)ECUごとの変更量	○小	○小	○小	○小	×大
(2)セキュリティ性能	(2-1)検知精度	○高	△中	△中	○高	○高
	(2-2)侵入防止	△GW通過時	×不可	△GW通過時	○全データ	○全データ
	(2-3)防御対象	△周期データのみ	△周期データのみ	○全データ	○全データ	○全データ
(3)演算量		○小	○小	△中	○小	×大
(4)設計情報		△要	○不要	△要	○不要	○不要

提案方式は上記の通り短周期のデータを保留し，その後破棄することから，GW 通過時に侵入防止が可能となる．

(2-3)防御対象

提案方式および(a)は，データの周期性に着目した検知方式であるため，非周期データには対応していない．(b)(c)(d)は，非周期データも検知可能である．

(3)演算量

提案方式および(a)(c)は処理内容が少なく，データ受信処理と比較演算判定のみの演算で侵入検知可能である．

(b)は，データのペイロード取得を行い内容の判定を行うためやや処理が重く，(d)は送信時の署名作成，受信時の署名確認等を行うため，さらに負荷が高くなる

(4)設計情報必要性の有無

提案方式はデータの周期情報が必要となる．(b)はデータの意味（ペイロードの構造．例えば 1-2byte 目が速度情報など）および判定閾値を必要とする．

(a)は，設計情報は不要だが，正常時の測定値と判定閾値が必要となる．

4.2 考察

・提案方式の特長

提案方式および振る舞い検知方式(a)(b)は，本検討の目的である，既存 ECU を変更しない（方式適用 GW 除く）という条件を満たす（表 1(1-1)）．

ここで振る舞い検知方式は，振る舞いの正常と異常について，観測すべき値と閾値を決定することが難しく，検知精度に課題がある（表 1(2-1)）．本提案は，判定に使用する送出周期について設計情報を用い，かつ CAN で発生する周期揺らぎについてシフト判定を行い，誤検知および見逃しを抑制することにより，検知精度を向上させている．

さらにシフト判定を GW で実施することにより，GW を通過する不正データの侵入防止も可能とした（表 1(2-2)）．

・提案方式の課題

本方式は周期データのみに対応しているが，車載 LAN においては多くの情報が周期的に送信されており，また制御に重要な情報であるほど，情報の途絶に対応するために周期的に送信しているため，それら重要な情報に対してなりすまし攻撃を検知することは有用と考える．

侵入検知に設計情報（データの送出周期）が必要な点は，送出周期は各車両の設計時に決定されるデータであり，データ量も小さい．そのため車両開発時に数値を決定し，GW 設計に適用することは容易である．

5. おわりに

本報告では，なりすまし攻撃に対する侵入検知手法の実車への適用に際して，開発コストの増加や安全性への影響を避けるため既存 ECU について変更不要とし，かつなりすまし攻撃を検知可能である，シフト判定式周期検知方式について提案した．

提案方式は，振る舞い検知方式と同様に既存 ECU への変更を最小限とし，既存振る舞い検知方式で課題となる検知精度について，設計周期を用い，短周期データを受信した際に判定を保留し誤検知を避けることにより検知精度を向上させた．さらに保留後に判定結果を基に受信データを破棄することにより，侵入防止も可能とした．

また本提案方式は，修正量も少なく，ソフトウェアの修正のみで侵入検知が可能である．そのため，既存の GW に対してソフトウェア書き換えを行い，本方式を適用することにより，すでに市場に存在している車両に対してセキュリティ対策を実施することも可能と考える．

謝辞 本研究を進めるにあたりご支援頂いた日立オートモティブシステムズ（株）の笹澤憲佳主任技師，（株）日立製作所日立研究所の成沢文雄主任研究員に感謝する．

参考文献

1) Robert Bosch GmbH, CAN specification Ver. 2.0B, (1991).
2) K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage,: Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy 2010, pp. 447 - 462, (2010).
3) S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno,: Comprehensive experimental analyses of automotive attack surfaces, the 20th USENIX Security Symposium, (2011).
4) 株式会社富士キメラ総研: 車載 ECU アナライジング＆マーケットレポート 2012, (2012).
5) T. Hoppe, S. Kiltz, and J. Dittmann,: Security Threats to Automotive CAN Networks - Practical Examples and Selected Short-Term Countermeasures, In Proceedings of the 27th international conference on Computer Safety, Reliability, and Security, SAFECOMP '08, pp. 235–248, (2009).
6) A. V. Herrewege, D. Singelee, and I. Verbauwhede,: CANAuth - A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus, In Embedded Security in Cars 9th, page 7, Dresden, DE, (2011).
7) M. Müter, N. Asaj,: Entropy-Based Anomaly Detection for In-Vehicle Networks, 2011 IEEE Intelligent Vehicles Symposium (IV) Baden-Baden, Germany, June 5-9, (2011).
8) M. Müter, A. Groll, F. C. Freiling,: A Structured Approach to Anomaly Detection for In-Vehicle Networks, Information Assurance and Security (IAS), 2010 Sixth International Conference, 23-25 Aug. ,(2010).
9) T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, K. Oishi,: A Method of Preventing Unauthorized Data Transmission in Controller Area Network, Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th (2012).
10) 佐藤道夫: 車載ネットワーク・システム徹底解説，CQ 出版株式会社(2005).