

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2014-138380

(P2014-138380A)

(43) 公開日 平成26年7月28日(2014.7.28)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 9/32 (2006.01)	H04L 9/00 675B	5H181
G09C 1/00 (2006.01)	G09C 1/00 640E	5J104
G08G 1/09 (2006.01)	G08G 1/09 H	
G06F 21/44 (2013.01)	G06F 21/20 144C	

審査請求 未請求 請求項の数 20 O L (全 25 頁)

(21) 出願番号 特願2013-7350 (P2013-7350)
 (22) 出願日 平成25年1月18日 (2013.1.18)

(71) 出願人 000003207
 トヨタ自動車株式会社
 愛知県豊田市トヨタ町1番地
 (74) 代理人 100100549
 弁理士 川口 嘉之
 (74) 代理人 100085006
 弁理士 世良 和信
 (74) 代理人 100113608
 弁理士 平川 明
 (74) 代理人 100123319
 弁理士 関根 武彦
 (74) 代理人 100123098
 弁理士 今堀 克彦
 (74) 代理人 100143797
 弁理士 宮下 文徳

最終頁に続く

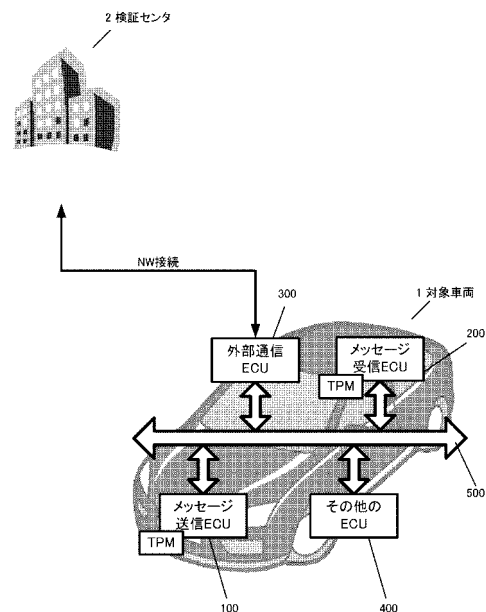
(54) 【発明の名称】 車両不正状態検出方法、車載システムにおける制御方法、およびシステム

(57) 【要約】 (修正有)

【課題】メッセージ送信アドレスが含まれない通信プロトコルを採用するネットワークにおいて、不正な状態を精度よく検出する車両不正状態検出方法を提供する。

【解決手段】メッセージ送信ECU 200からメッセージ受信ECU 100に所定のメッセージIDを有するメッセージを送信する際に、両ECUがそれぞれ個別に現時点における記憶手段の内容とメッセージ内容に基づいて記憶手段を更新する。検証センタ2から要求があると、両ECUはその時点での記憶手段の内容に基づいて、それぞれ検証メッセージを生成して検証センタ2に送信する。検証センタ2では、2つの検証メッセージに含まれる値が異なれば車両が不正状態にあると判断する。成りすましECUが存在しなければ両ECUの記憶手段の内容は一致するので、検証センタは車両内にメッセージ送信ECUになりすました不正ECUが存在するか判断できる。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

車内ネットワークで接続されたメッセージ送信ECUとメッセージ受信ECUを含む車両と、前記車両の不正状態を検出する検証センタとから構成される車両不正状態検出システムにおける車両不正状態検出方法であって、

前記メッセージ送信ECUが、所定の条件を満たすメッセージを前記車内ネットワークに送信する際に、当該メッセージと第1の記憶手段の記憶値を用いて前記第1の記憶手段の記憶値を更新する第1のステップと、

前記メッセージ受信ECUが、前記所定の条件を満たすメッセージを前記車内ネットワークから受信する際に、当該メッセージと第2の記憶手段の記憶値を用いて前記第2の記憶手段の記憶値を更新する第2のステップと、

前記検証センタが、前記車両に対して検証メッセージを送信するように要求する第3のステップと、

前記メッセージ送信ECUが、前記要求に応答して、前記第1の記憶手段の記憶値を含む第1の検証メッセージを生成して、前記検証センタに送信する第4のステップと、

前記メッセージ受信ECUが、前記要求に応答して、前記第2の記憶手段の記憶値を含む第2の検証メッセージを生成して、前記検証センタに送信する第5のステップと、

前記検証センタが、前記第1の検証メッセージおよび前記第2の検証メッセージに含まれる値が互いに異なる場合に、前記車両が不正状態であると判断する第6のステップと、を含む、車両不正状態検出方法。

【請求項 2】

前記所定の条件は、前記メッセージが所定のメッセージIDを有するという条件である、請求項1に記載の車両不正状態検出方法。

【請求項 3】

前記第1のステップは、前記第1の記憶手段の前記記憶値と前記メッセージを連結する工程と、連結後のデータのハッシュ値を算出する工程と、前記ハッシュ値を前記第1の記憶手段に格納する工程と、を含む、

前記第2のステップは、前記第2の記憶手段の前記記憶値と前記メッセージを連結する工程と、連結後のデータのハッシュ値を算出する工程と、前記ハッシュ値を前記第2の記憶手段に格納する工程と、を含む、

請求項1または2に記載の車両不正状態検出方法。

【請求項 4】

前記第4のステップでは、前記メッセージ送信ECUは、当該メッセージ送信ECUが記憶する第1の秘密鍵を用いて前記第1の検証メッセージに電子署名を付してから、前記検証センタに送信し、

前記第5のステップでは、前記メッセージ受信ECUは、当該メッセージ受信ECUが記憶する第2の秘密鍵を用いて前記第2の検証メッセージに電子署名を付してから、前記検証センタに送信し、

前記第6のステップでは、前記検証センタは、当該検証センタが記憶する前記第1および第2の秘密鍵に対応する第1および第2の公開鍵を用いて、前記メッセージ送信ECUから送信される前記第1の検証メッセージおよび前記メッセージ受信ECUから送信される前記第2の検証メッセージの正当性を検証する、

請求項1-3のいずれかに記載の車両不正状態検出方法。

【請求項 5】

前記第3のステップにおける前記要求には、ランダムなメッセージであるナンスが含まれており、

前記第4のステップでは、前記メッセージ送信ECUは、前記ナンスと前記第1の記憶手段の記憶値を用いて前記第1の記憶手段の記憶値を更新してから、前記第1の検証メッセージを生成して、前記検証センタに送信し、

前記第5のステップでは、前記メッセージ受信ECUは、前記ナンスと前記第2の記憶手段

の記憶値を用いて前記第2の記憶手段の記憶値を更新してから、前記第2の検証メッセージを生成して、前記検証センタに送信する、

請求項1-4のいずれかに記載の車両不正状態検出方法。

【請求項6】

前記車両が、所定のタイミングで、前記検証センタにランダムなメッセージであるナンスを要求するステップと、

前記メッセージ送信ECUが、前記ナンスと前記第1の記憶手段の記憶値を用いて前記第1の記憶手段の記憶値を更新するステップと、

前記メッセージ受信ECUが、前記ナンスと前記第2の記憶手段の記憶値を用いて前記第2の記憶手段の記憶値を更新するステップと、

10

を含む、請求項1-5のいずれかに記載の車両不正状態検出方法。

【請求項7】

前記車両ネットワークはCANネットワークである、

請求項1-6のいずれかに記載の車両不正状態検出方法。

【請求項8】

前記所定の条件は、メッセージが所定のCAN IDを有するという条件であり、

前記所定のCAN IDは、前記メッセージ送信ECUによって送信され、かつ、前記メッセージ受信ECUが受信および処理するメッセージのCAN IDである、

請求項7のいずれかに記載の車両不正状態検出方法。

【請求項9】

20

前記メッセージ送信ECUおよび前記メッセージ受信ECUは、外部通信ECUを介して前記検証センタと通信する、

請求項1-8のいずれかに記載の車両不正状態検出方法。

【請求項10】

検証メッセージを車両に要求し当該検証メッセージに基づいて車両における不正状態を検出する検証センタと通信可能な車載システムにおける制御方法であって、

メッセージ送信ECUが、所定の条件を満たすメッセージを前記車内ネットワークに送信する際に、当該メッセージと第1の記憶手段の記憶値を用いて当該第1の記憶手段の記憶値を更新するステップと、

30

メッセージ受信ECUが、前記所定の条件を満たすメッセージを前記車内ネットワークから受信する際に、当該メッセージと第2の記憶手段の記憶値を用いて前記第2の記憶手段の記憶値を更新するステップと、

前記メッセージ送信ECUが、前記検証センタからの検証メッセージの要求に応答して、前記第1の記憶手段に格納された値を含む第1の検証メッセージを生成して、前記検証センタに送信するステップと、

前記メッセージ受信ECUが、前記検証センタからの検証メッセージの要求に応答して、前記第2の記憶手段に格納された値を含む第2の検証メッセージを生成して、前記検証センタに送信するステップと、

を含む、車載システムにおける制御方法。

【請求項11】

40

車両と検証センタとから構成され、前記車両における不正状態を前記検証センタにおいて検出する車両不正状態検出システムであって、

前記検証センタは、

前記車両に対して、検証メッセージを送信するように要求する要求手段と、

前記車両から送信される検証メッセージに基づいて、前記車両における不正状態を検出する検出手段と、

を有し、

前記車両は、

互いに車内ネットワークで接続された、メッセージ送信ECUとメッセージ受信ECUとを有し、前記メッセージ送信ECUおよび前記メッセージ受信ECUは前記検証センタと通信可能で

50

あり、

前記メッセージ送信ECUは、

所定の条件を満たすメッセージを選択する第1のメッセージ選択手段と、

記憶値を格納する第1の記憶手段と、

前記第1の記憶手段に格納された前記記憶値を含む第1の検証メッセージを生成して、前記検証センタに送信する第1の検証メッセージ生成手段と、

を備え、

前記メッセージ受信ECUは、

前記所定の条件を満たすメッセージを選択する第2のメッセージ選択手段と、

記憶値を格納する第2の記憶手段と、

10

前記第2の記憶手段に格納された前記記憶値を含む第2の検証メッセージを生成して、前記検証センタに送信する第2の検証メッセージ生成手段と、

を備え、

前記メッセージ送信ECUは、当該メッセージ送信ECUが前記車内ネットワークに送信するメッセージが前記所定の条件を満たすと前記第1のメッセージ選択手段により判定された場合に、当該メッセージと前記第1の記憶手段の前記記憶値に基づいて、前記第1の記憶手段の前記記憶値を更新し、

前記メッセージ受信ECUは、当該メッセージ受信ECUが前記車内ネットワークから受信するメッセージが前記所定の条件を満たすと前記第2のメッセージ選択手段により判定された場合に、当該メッセージと前記第2の記憶手段の前記記憶値に基づいて、前記第2の記憶手段の前記記憶値を更新し、

20

前記車両が前記検証センタから前記要求メッセージを受信した場合に、前記メッセージ送信ECUの前記第1の検証メッセージ生成手段が前記第1の検証メッセージが生成し、前記検証センタに送信し、前記メッセージ受信ECUの前記第2の検証メッセージ生成手段が前記第2の検証メッセージを生成し、前記検証センタに送信し、

前記検証センタの検出手段は、前記第1の検証メッセージおよび前記第2の検証メッセージに含まれるそれぞれ前記記憶値が互いに異なる場合に、前記車両が不正状態であると判断する、

車両不正状態検出システム。

【請求項 1 2】

30

前記所定の条件は、前記メッセージが所定のメッセージIDを有するという条件である、請求項11に記載の車両不正状態検出システム。

【請求項 1 3】

前記メッセージ送信ECUは、当該メッセージ送信ECUが前記車内ネットワークに送信するメッセージが前記所定の条件を満たすと前記第1のメッセージ選択手段により判定された場合に、前記第1の記憶手段の記憶値と前記メッセージを連結し、連結したデータのハッシュ値を算出し、当該ハッシュ値を前記第1の記憶手段に格納し、

前記メッセージ受信ECUは、当該メッセージ受信ECUが前記車内ネットワークから受信するメッセージが前記所定の条件を満たすと前記第2のメッセージ選択手段により判定された場合に、前記第2の記憶手段の記憶値と前記メッセージを連結し、連結したデータのハッシュ値を算出し、当該ハッシュ値を前記第2の記憶手段に格納する、

40

請求項11または12に記載の車両不正状態検出システム。

【請求項 1 4】

前記メッセージ送信ECUは、第1の秘密鍵を記憶する第1の秘密鍵記憶手段を有し、前記第1の検証メッセージに当該第1の秘密鍵を用いた電子署名を付して、前記検証センタに送信し、

前記メッセージ受信ECUは、第2の秘密鍵を記憶する第2の秘密鍵記憶手段を有し、前記第2の検証メッセージに当該第2の秘密鍵を用いた電子署名を付して、前記検証センタに送信し、

前記検証センタは、前記第1の秘密鍵に対応する第1の公開鍵、および、前記第2の秘密

50

鍵に対応する第2の公開鍵を記憶する公開鍵記憶手段を有し、当該第1および第2の公開鍵を用いて、前記メッセージ送信ECUから送信される前記第1の検証メッセージおよび前記メッセージ受信ECUから送信される前記第2の検証メッセージの正当性を検証する、

請求項11-13のいずれかに記載の車両不正状態検出システム。

【請求項 15】

前記検証センタから送信される前記要求メッセージにはランダムなメッセージであるナンスが含まれており、

前記メッセージ送信ECUは、前記ナンスを用いて前記第1の記憶手段を更新してから、前記第1の検証メッセージを生成して、前記検証センタに送信し、

前記メッセージ受信ECUは、前記ナンスを用いて前記第2の記憶手段を更新してから、前記第2の検証メッセージを生成して、前記検証センタに送信する、

請求項11-14のいずれかに記載の車両不正状態検出システム。

【請求項 16】

前記車両は、所定のタイミングで、前記検証センタにランダムなメッセージであるナンスを要求し、

前記メッセージ送信ECUは、前記ナンスを用いて前記第1の記憶手段を更新し、

前記メッセージ受信ECUは、前記ナンスを用いて前記第2の記憶手段を更新する、

請求項11-15のいずれかに記載の車両不正状態検出システム。

【請求項 17】

前記車内ネットワークはCANネットワークである

請求項11-16のいずれかに記載の車両不正状態検出システム。

【請求項 18】

前記所定の条件は、メッセージが所定のCAN IDを有するという条件であり、

前記所定のCAN IDは、前記メッセージ送信ECUによって送信され、かつ、前記メッセージ受信ECUが受信および処理するメッセージのCAN IDである、

請求項17のいずれかに記載の車両不正状態検出システム。

【請求項 19】

前記車両は、検証センタと通信可能な外部通信ECUを有し、

前記メッセージ送信ECUおよび前記メッセージ受信ECUは、前記外部通信ECUを介して前記検証センタと通信する、

請求項11-18のいずれかに記載の車両不正状態検出システム。

【請求項 20】

検証メッセージを車両に要求し、当該検証メッセージに基づいて車両における不正状態を検出する検証センタと通信可能な車載システムであって、

互いに車内ネットワークで接続された、メッセージ送信ECUとメッセージ受信ECUとを有し、前記メッセージ送信ECUおよび前記メッセージ受信ECUは前記検証センタと通信可能であり、

前記メッセージ送信ECUは、

所定の条件を満たすメッセージを選択する第1のメッセージ選択手段と、

記憶値を格納する第1の記憶手段と、

前記第1の記憶手段に格納された前記記憶値を含む第1の検証メッセージを生成して、前記検証センタに送信する第1の検証メッセージ生成手段と、

を備え、

前記メッセージ受信ECUは、

前記所定の条件を満たすメッセージを選択する第2のメッセージ選択手段と、

記憶値を格納する第2の記憶手段と、

前記第2の記憶手段に格納された前記記憶値を含む第2の検証メッセージを生成して、前記検証センタに送信する第2の検証メッセージ生成手段と、

を備え、

前記メッセージ送信ECUは、当該メッセージ送信ECUが前記車内ネットワークに送信する

10

20

30

40

50

メッセージが前記所定の条件を満たすと前記第1のメッセージ選択手段により判定された場合に、当該メッセージと前記第1の記憶手段の記憶値に基づいて、前記第1の記憶手段の前記記憶値を更新し、

前記メッセージ受信ECUは、当該メッセージ受信ECUが前記車内ネットワークから受信するメッセージが前記所定の条件を満たすと前記第2のメッセージ選択手段により判定された場合に、当該メッセージと前記第2の記憶手段の記憶値に基づいて、前記第2の記憶手段の前記記憶値を更新し、

前記車両が前記検証センタから前記要求メッセージを受信した場合に、前記メッセージ送信ECUの前記第1の検証メッセージ生成手段が前記第1の検証メッセージが生成し、前記検証センタに送信し、前記メッセージ受信ECUの前記第2の検証メッセージ生成手段が前記第2の検証メッセージを生成し、前記検証センタに送信する、

10

車載システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、車載システムにおける不正状態を検出する技術に関する。

【背景技術】

【0002】

近年、車載システムのソフトウェア化に伴い、多くの処理がECUなどのコンピュータによって実現されている。第三者がECUを不正に交換したり、その内容を不正に書き換えたりした場合は、車載システムでの安全な動作が確保できない。したがって、ECU等が不正交換されたり不正に書き換えられたりして車載システムが不正状態になった場合には、その旨を検出できることが望まれる。

20

【0003】

特許文献1では、成りすましをされた通信機器が、同じネットワーク上に同じIPアドレスやMACアドレスが存在することを認識することで、成りすましを検出することが開示されている。

【先行技術文献】

【特許文献】

【0004】

30

【特許文献1】特開2008-48252号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

特許文献1に記載の方法では、送信されるメッセージにIPアドレスやMACアドレスなどの送信アドレスが含まれることを前提としている。したがって、特許文献1に記載の方法は、メッセージに送信アドレスを含まない通信プロトコルを採用するネットワーク（例えば、CAN（Controller Area Network）が典型的な例である）には適用できないという問題がある。

【0006】

40

また、特許文献1に記載の方法では、不正なECUの側から、同一の送信アドレスを有するECUが存在すると報告することができる。この場合、特許文献1に記載の方法では、この報告が正しいものであるか誤ったものであるのかを確認することができない。したがって、特許文献1に方法では、不正状態の検知精度に問題がある。

【0007】

本発明は上記の問題点を考慮してなされたものであり、メッセージに送信アドレスが含まれない通信プロトコルを採用するネットワークにおいて、不正な状態を精度よく検出できる技術を提供することを目的とする。

【課題を解決するための手段】

【0008】

50

本発明の第1の態様は、車両と検証センタから構成される車両不正状態検出システムにおける車両不正状態検出方法である。車両は、車内ネットワークで接続されたメッセージ送信ECUとメッセージ受信ECUを含む。検証センタは、車両から送信される検証メッセージに基づいて車両が不正状態にあることを検出する。

【0009】

本発明にかかる車両不正状態検出方法は、メッセージ送信ECUからメッセージ受信ECUにメッセージを送信する際に、両ECUがそれぞれ個別にメッセージ内容に基づいて記憶手段を更新する。検証センタから要求があった場合には、両ECUはその時点での記憶手段の内容に基づいて、それぞれ検証メッセージを生成して検証センタに送信する。第三者からの攻撃が無い限り、両ECUの記憶手段の内容は一致することが期待される。そこで、検証センタでは、2つの検証メッセージに含まれる値が異なれば車両が不正状態にあると判断する。

10

【0010】

より具体的には、本発明にかかる車両不正状態検出方法は、

(1)メッセージ送信ECUが、所定の条件を満たすメッセージを前記車内ネットワークに送信する際に、当該メッセージと第1の記憶手段の記憶値を用いて第1の記憶手段の記憶値を更新する第1のステップと、

(2)メッセージ受信ECUが、前記所定の条件を満たすメッセージを前記車内ネットワークから受信する際に、当該メッセージと第2の記憶手段の記憶値を用いて第2の記憶手段の記憶値を更新する第2のステップと、

20

(3)検証センタが、前記車両に対して検証メッセージを送信するように要求する第3のステップと、

(4)メッセージ送信ECUが、前記要求に応答して、前記第1の記憶手段の記憶値を含む第1の検証メッセージを生成して、前記検証センタに送信する第4のステップと、

(5)前記メッセージ受信ECUが、前記要求に応答して、前記第2の記憶手段の記憶値を含む第2の検証メッセージを生成して、前記検証センタに送信する第5のステップと、

(6)前記検証センタが、前記第1の検証メッセージおよび前記第2の検証メッセージに含まれる値が互いに異なる場合に、前記車両が不正状態であると判断する第6のステップと、

を含む。

30

【0011】

このようにすれば、車両の状態が正常である限り、第1および第2の記憶手段の内容を同一のものとすることができ、したがって第1および第2の検証メッセージに含まれる値が同一となる。逆に、成りすましなどによる攻撃が生じた場合には、両記憶手段の内容が異なる値となるので、検証センタは第1および第2の検証メッセージ内の値の不一致から車両の不正状態を検出することができる。また、送信元アドレスや宛先アドレスなどを用いずに不正状態の検出が行えるので、たとえばCANネットワークのように各ノードにアドレスを付与せず、メッセージに送信元アドレスや宛先アドレスが含まれないようなプロトコルを使用するネットワークであっても、不正状態を検出することができる。

【0012】

40

第1のステップおよび第2のステップにおける所定の条件は、同一の条件である。例えば、この所定の条件は、前記メッセージが所定のメッセージIDを有するという条件とすることが好ましい。より好ましくは、この所定のメッセージIDは、メッセージ送信ECUが送信するメッセージに含まれるメッセージIDであり、メッセージ受信ECUが受信および処理をするメッセージに含まれるIDである。またこのメッセージIDは、前記メッセージ送信ECU以外のECUが送信するメッセージには含まれないものであること(前記メッセージ送信ECUのみが送信するメッセージIDであること)が好ましい。このようにすることで、正常状態であれば第1および第2の記憶手段内の記憶値が一致する。

【0013】

第1および第2の記憶手段の更新は、現在の記憶値の内容と入力値とに基づいて行うこと

50

が好ましい。とくに、複数の入力値の入力順序が異なる場合に、結果として得られる記憶値の値も異なるようにすることが好ましい。このような方法の例として、記憶手段の記憶値とメッセージ（入力値）を連結し、連結後のデータのハッシュ値を算出し、算出したハッシュ値を新たな記憶値とする方法が挙げられる。

【0014】

第4のステップにおいて、メッセージ送信ECUは、記憶する秘密鍵（第1の秘密鍵）を用いて、第1の検証メッセージに電子署名を付してから検証センタに送信することが好ましい。同様に、第5のステップにおいて、メッセージ受信ECUは、記憶する秘密鍵（第2の秘密鍵）を用いて、第2の検証メッセージに電子署名を付してから検証センタに送信することが好ましい。この場合は、第6のステップにおいて、検証センタは、第1および第2の秘密鍵に対応する第1および第2の公開鍵を用いて、メッセージ送信ECUから送信される第1の検証メッセージおよびメッセージ受信ECUから送信される第2の検証メッセージの正当性を検証することが好ましい。これにより、検証時に利用する公開鍵に結びついた送信元の特
10 定、および通信の安全性を確保できる。また、メッセージ送信ECUやメッセージ受信ECUが不正に交換された不正状態を検出することもできる。

【0015】

第3のステップにおいて、検証センタが送信する要求に、ナンスを含めることができる。ナンスは、ランダムに生成される数値や文字列を含むメッセージである。第4のステップでは、メッセージ送信ECUは、ナンスと第1の記憶手段の記憶値を用いて第1の記憶手段の記憶値を更新してから、第1の検証メッセージを生成して、検証センタに送信することが好ましい。同様に、第5のステップでは、メッセージ受信ECUは、ナンスと第2の記憶手段の記憶値を用いて第2の記憶手段の記憶値を更新してから、第2の検証メッセージを生成して、検証センタに送信することが好ましい。ナンスを用いて記憶手段を更新してから検証メッセージを生成することで、車載システムが起動後に同一の挙動を示した場合などであ
20 っても、生成される検証メッセージの内容を異なるものとすることができる。したがって、第三者によるリプレイ攻撃（再送攻撃）を防ぐことができる。

【0016】

ナンスを用いた記憶手段の更新は、車両側から開始するようにしても良い。すなわち、本発明にかかる方法は、車両が所定のタイミングで検証センタにナンスを要求するステップと、メッセージ送信ECUが検証センタから送信されたナンスと第1の記憶手段の記憶値を用いて第1の記憶手段の記憶値を更新するステップと、メッセージ受信ECUが検証センタから送信されたナンスと第2の記憶手段の記憶値を用いて第2の記憶手段の記憶値を更新するステップを含むことも好ましい。ここで所定のタイミングは、例えば、システム起動時、所定の時間が経過したタイミング、所定の距離を走行したタイミングなどとするこ
30 ができる。このようにすることで、記憶手段内の記憶値ひいては検証メッセージの内容を、第三者が推測できないようできる。

【0017】

上記の車両ネットワークは、任意のネットワークであって構わないが、例えば、CAN（Control Area Network）ネットワークとすることができる。CANネットワークでは、送信メッセージに送信元アドレスや宛先アドレスが含まれず、CAN ID（メッセージID）が含まれる。CANネットワーク内では、受信ECUはCAN IDを参照して、自ノードが処理する必要があるメッセージであるか否かを判断する。車両ネットワークがCANネットワークである場合は、本発明の第1および第2のステップにおける所定の条件は、メッセージ送信ECUが送信されるメッセージに含まれるCAN IDであり、かつ、メッセージ受信ECUが受信および処理するメッセージに含まれるCAN IDを、メッセージが含むこととすることができる。
40

【0018】

本発明は、上記処理の少なくとも一部を含む車両不正状態検出方法として捉えることができる。また、この方法をコンピュータにおいて実現するためのコンピュータプログラムとして捉えることもできる。また、上記処理を実行する手段の少なくとも一部を備える車両不正状態検出システムあるいは車載システムとして捉えることもできる。上記手段およ
50

び処理の各々は可能な限り互いに組み合わせて本発明を構成することができる。

【 0 0 1 9 】

たとえば、本発明の第2の態様は、

検証メッセージを車両に要求し当該検証メッセージに基づいて車両における不正状態を検出する検証センタと通信可能な車載システムにおける制御方法であって、

メッセージ送信ECUが、所定の条件を満たすメッセージを前記車内ネットワークに送信する際に、当該メッセージと第1の記憶手段の記憶値を用いて第1の記憶手段の記憶値を更新するステップと、

メッセージ受信ECUが、前記所定の条件を満たすメッセージを前記車内ネットワークから受信する際に、当該メッセージと第2の記憶手段の記憶値を用いて第2の記憶手段の記憶値を更新するステップと、

前記メッセージ送信ECUが、前記検証センタからの検証メッセージの要求に応答して、前記第1の記憶手段に格納された値を含む第1の検証メッセージを生成して、前記検証センタに送信するステップと、

前記メッセージ受信ECUが、前記検証センタからの検証メッセージの要求に応答して、前記第2の記憶手段に格納された値を含む第2の検証メッセージを生成して、前記検証センタに送信するステップと、

を含む、車載システムにおける制御方法である。

【 0 0 2 0 】

また、本発明の第3の態様は、

車両と検証センタとから構成され、前記車両における不正状態を前記検証センタにおいて検出する車両不正状態検出システムであって、

前記検証センタは、

前記車両に対して、検証メッセージを送信するように要求する要求手段と、

前記車両から送信される検証メッセージに基づいて、前記車両における不正状態を検出する検出手段と、

を有し、

前記車両は、

互いに車内ネットワークで接続された、メッセージ送信ECUとメッセージ受信ECUとを有し、前記メッセージ送信ECUおよび前記メッセージ受信ECUは前記検証センタと通信可能であり、

前記メッセージ送信ECUは、

所定の条件を満たすメッセージを選択する第1のメッセージ選択手段と、

記憶値を格納する第1の記憶手段と、

前記第1の記憶手段に格納された前記記憶値を含む第1の検証メッセージを生成して、前記検証センタに送信する第1の検証メッセージ生成手段と、

を備え、

前記メッセージ受信ECUは、

前記所定の条件を満たすメッセージを選択する第2のメッセージ選択手段と、

記憶値を格納する第2の記憶手段と、

前記第2の記憶手段に格納された前記記憶値を含む第2の検証メッセージを生成して、前記検証センタに送信する第2の検証メッセージ生成手段と、

を備え、

前記メッセージ送信ECUは、当該メッセージ送信ECUが前記車内ネットワークに送信するメッセージが前記所定の条件を満たすと前記第1のメッセージ選択手段により判定された場合に、当該メッセージと前記第1の記憶手段の前記記憶値に基づいて、前記第1の記憶手段の前記記憶値を更新し、

前記メッセージ受信ECUは、当該メッセージ受信ECUが前記車内ネットワークから受信するメッセージが前記所定の条件を満たすと前記第2のメッセージ選択手段により判定された場合に、当該メッセージと前記第2の記憶手段の前記記憶値に基づいて、前記第2の記憶

10

20

30

40

50

手段の前記記憶値を更新し、

前記車両が前記検証センタから前記要求メッセージを受信した場合に、前記メッセージ送信ECUの前記第1の検証メッセージ生成手段が前記第1の検証メッセージが生成し、前記検証センタに送信し、前記メッセージ受信ECUの前記第2の検証メッセージ生成手段が前記第2の検証メッセージを生成し、前記検証センタに送信し、

前記検証センタの検出手段は、前記第1の検証メッセージおよび前記第2の検証メッセージに含まれるそれぞれ前記記憶値が互いに異なる場合に、前記車両が不正状態であると判断する、

車両不正状態検出システムである。

【0021】

10

また、本発明の第4の態様は、

検証メッセージを車両に要求し、当該検証メッセージに基づいて車両における不正状態を検出する検証センタと通信可能な車載システムであって、

互いに車内ネットワークで接続された、メッセージ送信ECUとメッセージ受信ECUとを有し、前記メッセージ送信ECUおよび前記メッセージ受信ECUは前記検証センタと通信可能であり、

前記メッセージ送信ECUは、

所定の条件を満たすメッセージを選択する第1のメッセージ選択手段と、

記憶値を格納する第1の記憶手段と、

前記第1の記憶手段に格納された前記記憶値を含む第1の検証メッセージを生成して、前記検証センタに送信する第1の検証メッセージ生成手段と、

20

を備え、

前記メッセージ受信ECUは、

前記所定の条件を満たすメッセージを選択する第2のメッセージ選択手段と、

記憶値を格納する第2の記憶手段と、

前記第2の記憶手段に格納された前記記憶値を含む第2の検証メッセージを生成して、前記検証センタに送信する第2の検証メッセージ生成手段と、

を備え、

前記メッセージ送信ECUは、当該メッセージ送信ECUが前記車内ネットワークに送信するメッセージが前記所定の条件を満たすと前記第1のメッセージ選択手段により判定された場合に、当該メッセージと前記第1の記憶手段の記憶値に基づいて、前記第1の記憶手段の前記記憶値を更新し、

30

前記メッセージ受信ECUは、当該メッセージ受信ECUが前記車内ネットワークから受信するメッセージが前記所定の条件を満たすと前記第2のメッセージ選択手段により判定された場合に、当該メッセージと前記第2の記憶手段の記憶値に基づいて、前記第2の記憶手段の前記記憶値を更新し、

前記車両が前記検証センタから前記要求メッセージを受信した場合に、前記メッセージ送信ECUの前記第1の検証メッセージ生成手段が前記第1の検証メッセージが生成し、前記検証センタに送信し、前記メッセージ受信ECUの前記第2の検証メッセージ生成手段が前記第2の検証メッセージを生成し、前記検証センタに送信する、

40

車載システムである。

【発明の効果】

【0022】

本発明によれば、メッセージに送信アドレスが含まれない通信プロトコルを採用するネットワークにおいて、不正な状態を精度よく検出できる。

【図面の簡単な説明】

【0023】

【図1】本実施形態にかかる車両不正状態検出システムの構成の概要を示す図。

【図2】メッセージ送信ECUの機能構成を示す図。

【図3】メッセージ受信ECUの機能構成を示す図。

50

【図4】検証センタの機能構成を示す図。

【図5】メッセージ送信ECUにおけるメッセージ送信時の処理の概要を示す図。

【図6】メッセージ送信ECUにおけるメッセージ送信時の処理のフローチャート。

【図7】メッセージ受信ECUにおけるメッセージ受信時の処理の概要を示す図。

【図8】メッセージ受信ECUにおけるメッセージ受信時の処理のフローチャート。

【図9】車両不正状態検出処理の概要を示す図。

【図10】メッセージ送信ECUおよびメッセージ受信ECUにおける車両不正状態検出処理のフローチャート。

【図11】検証センタにおける車両不正状態検出処理のフローチャート。

【発明を実施するための形態】

10

【0024】

<システム概要>

本実施形態にかかる車両不正状態検出システム（以下、本システムとも称する）を、図面を参照しながら説明する。図1は、本システムの構成の概要を示す図である。図1に示すように、本システムは、車両1および検証センタ2から構成される。

【0025】

車両1には、複数のECU（Electronic Control Unit）が車内ネットワーク500を介して接続された車載システムが搭載されている。図1には、ECUとして、メッセージ送信ECU100、メッセージ受信ECU200、外部通信ECU300、その他のECU400の4つのECUが示されている。

【0026】

20

本実施形態では、車内ネットワーク500はCAN（Controller Area Network）であることを想定する。CAN上で送信されるメッセージには、CAN IDと呼ばれるメッセージIDが含まれるが、送信元や宛先のアドレス情報は含まれない。車内ネットワーク500に接続された全てのECUは、ネットワーク上を流れるメッセージを全て受信可能であり、特定のCAN IDを含むメッセージのみを処理の対象とする。

【0027】

メッセージ送信ECU100（以下、送信ECU100とも表記する）は、本システムによって攻撃から保護したいECUである。送信ECU100は、例えば、カーナビゲーションECUなどである。メッセージ受信ECU200（以下、受信ECU200とも表記する）は、送信ECU100から送信されるメッセージを受信および処理するECUである。送信ECU100および受信ECU200には、不正検出を安全かつ確実に行うために、ハードウェア耐タンパ性を持つセキュリティチップであるTPM（Trusted Platform Module）が搭載される。

30

【0028】

外部通信ECU300は、検証センタ2と無線通信可能なECUである。外部通信ECU300は、車内ネットワークと検証センタ2とを接続するゲートウェイとして機能する。外部通信ECU300は、図中では送信ECU100や受信ECU200と異なるECUとして描かれているが、送信ECU100や受信ECU200が外部通信ECU300の機能を兼ねていても構わない。

【0029】

その他のECU400は、車載システムに搭載されるECUのうち、本実施形態にかかる不正検出処理に関わらないECUである。ECU400については、従来の車載システムに搭載されるECUと同等の機能を有していればよいので、本明細書中ではこれ以上説明しない。なお、その他のECU40は図中では1つのみが示されているが、複数個のECU400が搭載されていても構わない。

40

【0030】

本実施形態にかかる車両不正状態検出システムでの、不正状態検出方法の概要を簡単に説明する。メッセージ送信ECUからメッセージ受信ECUにメッセージを送信する際に、両ECUがそれぞれ個別にメッセージ内容に基づいてPCRレジスタを更新する。検証センタから要求があった場合には、両ECUはその時点でのPCRレジスタの内容に基づいて、それぞれ検証メッセージを生成して検証センタに送信する。第三者からの攻撃が無い限り、両ECUのPCRレジスタの内容は一致することが期待される。そこで、検証センタでは、2つの検証メッ

50

セージに含まれる値が異なれば車両が不正状態にあると判断する。

【 0 0 3 1 】

< メッセージ送信ECU >

メッセージ送信ECU100は、ハードウェアとしては、CPU（中央演算処理装置）、RAM（Random Access Memory）などの主記憶装置、ROM（Read Only Memory）、周辺装置（センサや入出力装置など）、ネットワークインタフェース等を含む。本実施形態では、メッセージ送信ECU100は、TPMチップを有する。TPMチップは、CPUからアクセスされるコプロセッサとして機能する。

【 0 0 3 2 】

メッセージ送信ECU100の機能構成を、図2を参照して説明する。メッセージ送信ECU100は、外部通信部110、TPMチップ120、従来機能部130を備える。外部通信部110および従来機能部130は、コンピュータプログラムをCPUが実行することにより実現される。TPM120は、コプロセッサとしてCPUから利用される。

10

【 0 0 3 3 】

外部通信部110は、車内ネットワーク500における通信を司る機能部である。外部通信部110は、従来機能部130が生成したメッセージを車内ネットワーク500に送信したり、車内ネットワーク500から受信したメッセージを従来機能部130に渡したりする機能を有する。外部通信部110は、受信したメッセージのCAN IDを参照して、自ノードで処理する必要があるメッセージであるかを判断し、必要であれば従来機能部130に渡す。

【 0 0 3 4 】

20

本実施形態にかかる外部通信部110は、さらに、フィルタ111を有する。フィルタ111は、メッセージ送信ECU100が送信しようとするメッセージおよび車内ネットワーク500から受信したメッセージが、所定の条件を満たすメッセージであるか否かを判断する。この所定の条件とは、送信ECU100のみが送信するメッセージとすることができる。CANにおいては、メッセージの内容ごとに異なるCAN IDが付与されるので、送信ECU100のみが送信するメッセージは、所定のCAN IDを持つか否かによって判断できる。なお、本明細書では、上記の所定の条件を満たすメッセージのことを「特定メッセージ」と称する。

【 0 0 3 5 】

フィルタ111は、特定メッセージID記憶部112、特定メッセージ判断部113、特定メッセージコピー部114、TPM操作部115、検証メッセージ生成部116の機能部を有する。

30

【 0 0 3 6 】

特定メッセージID記憶部112には、特定メッセージのCAN ID（メッセージID）が格納される。特定メッセージのCAN IDは、送信ECU100のみが送信するメッセージに付与されるCAN IDとする。さらに、特定メッセージのCAN IDは、受信ECU200によって受信および処理されるメッセージに付与されるCAN IDとする。なお、特定メッセージのCAN IDとして複数のCAN IDを記憶しても構わないが、ここでは特定メッセージは1つのCAN IDのみであることを想定する。

【 0 0 3 7 】

特定メッセージ判断部113は、従来機能部130から渡されるメッセージが、特定メッセージID記憶部112に記憶されたCAN IDを有するか否かを判断する機能を有する。すなわち、特定メッセージ判断部113は、送信ECU100が送信するメッセージが特定メッセージであるか判断可能である。

40

【 0 0 3 8 】

TPM操作部115は、TPM120を制御して、ハッシュ値算出、PCRレジスタ更新、PCR値の取得、電子署名付与などの処理をTPMに依頼し、処理結果をTPM120から取得する。TPMによって行われる処理について、TPM120について説明する際に詳細に説明する。

【 0 0 3 9 】

検証メッセージ生成部116は、検証センタ2から検証メッセージ要求を受信した場合に、検証メッセージを生成して、検証センタ2へ送信する機能部である。具体的には、検証メッセージ生成部116が生成する検証メッセージには、PCRレジスタ121の記憶値（PCR値）が

50

含まれる。また、検証メッセージには電子署名付与部124による電子署名が付与され、外部通信ECU300を介して検証センタ2へ送信される。

【0040】

TPM120は、TCG（Trusted Computing Group）によって策定された仕様にしたがうハードウェア耐タンパ性をもつセキュリティチップである。TPM120は、PCRレジスタ121、ハッシュエンジン122、秘密鍵記憶部123、電子署名付与部124などの機能部を含む。

【0041】

PCRレジスタ121は、プラットフォーム・コンフィギュレーション・レジスタ（Platform Configuration Register）と呼ばれるレジスタであり、20バイト（160ビット）の情報を記憶する。PCRレジスタ121は、TCMチップ上に設けられるため外部から改ざんすることはできない。本実施形態では、PCRレジスタ121をアキュムレータとして利用する。すなわち、PCRレジスタ121に記憶された値（PCR値）を、現在のPCR値と特定メッセージの内容に基づいて更新する。具体的には、現在のPCR値と特定メッセージを連結した後に、ハッシュエンジン122によってSHA-1ハッシュ値（20バイト）を算出し、このハッシュ値を新たなPCR値としてPCRレジスタ121に格納する。

10

【0042】

ハッシュエンジン122は、SHA-1ハッシュ値を演算する機能部である。ハッシュエンジン122は、外部から与えられたデータに対するハッシュ値（ダイジェスト値、メッセージダイジェストとも呼ばれる）を算出し、TPM122内に記憶する。ハッシュエンジン122は、算出および記憶したハッシュ値を外部に提供する機能も有する。ハッシュエンジン122は、電子署名の付与や検証などに用いることができる。

20

【0043】

秘密鍵記憶部123は、メッセージ送信ECU100の秘密鍵を記憶する。TPM120は、秘密鍵・公開鍵ペアの生成機能も有しており、秘密鍵記憶部123は生成した秘密鍵を記憶する。生成された鍵ペアのうち公開鍵の方は、検証センタ2に記憶される。

【0044】

電子署名付与部124は、与えられたメッセージに対して電子署名を付与する機能部である。具体的には、メッセージのハッシュ値（ダイジェスト値）をハッシュエンジン122を用いて生成し、生成したハッシュ値を秘密鍵記憶部123に記憶された秘密鍵を用いて暗号化する。暗号化されたハッシュ値が電子署名として元のメッセージに付与される。暗号化アルゴリズムは任意の公開鍵暗号方式が採用可能であるが、TPMではRSA暗号方式が採用される。

30

【0045】

従来機能部130は、メッセージ送信ECU100が本来の機能を達成するために機能を提供する機能部である。例えば、送信ECU100がカーナビゲーションECUである場合には、ナビゲーション処理に必要な機能を提供する。なお、従来機能部130は、車内ネットワーク500に対して送信するメッセージを生成して、外部通信部110へ渡す機能を有する。また、従来機能部130は、外部通信部110が車内ネットワーク500から受信したメッセージを処理する機能を有する。

【0046】

40

<メッセージ受信ECU>

メッセージ受信ECU200の構成は、図3に示すように、基本的にメッセージ送信ECU100の構成と同一である。受信ECU200の特定メッセージID記憶部212には、送信ECU100から受信ECU200宛てに送信されるメッセージのCAN IDが格納される。すなわち、送信ECU100の特定メッセージID記憶部112に記憶されるCAN IDと、受信ECU200の特定メッセージID記憶部212に記憶されるCAN IDは同一である。そして、特定メッセージ判断部213は、車内ネットワーク500から受信したメッセージが、特定メッセージ記憶部212に格納されたCAN IDを有するか否かを判断する。従来機能部230は、受信ECU200の本来の機能を提供する機能部であるため、その内容は送信ECU100とは異なる。

【0047】

50

< 外部通信ECU >

外部通信ECU300は、車内ネットワーク500と検証センタ2とをつなぐゲートウェイとして機能する。外部通信ECU300は、検証センタ2と無線通信を行う無線通信インタフェースを備える。外部通信ECU300と検証センタ2との間の無線通信方式は任意の方式であって良く、例えば、携帯電話網（3G、LTEなど）や、WiMAX（IEEE 802.16e）やIEEE 802.20、無線LAN（IEEE 802.11a/b/g/n/p）などを採用可能である。

【 0 0 4 8 】

外部通信ECU300は、検証センタ2から車載システム宛に送信されたメッセージを、車内ネットワーク500（CAN）にしたがった形式に変換して、車内ネットワーク500へ送信する。また、外部通信ECU300は、車内ネットワーク500から受信した検証センタ2宛のメッセージの形式を変換して、検証センタ2へ送信する。

10

【 0 0 4 9 】

< 検証センタ >

検証センタ2は、ハードウェアとしては、CPU（中央演算処理装置）、RAM（Random Access Memory）などの主記憶装置、HDD（Hard Disk Drive）やSSD（Solid State Disk）などの補助記憶装置、周辺装置（センサや入出力装置など）、ネットワークインタフェース等を含む。図4は、検証センタ2の機能構成を示す図である。検証センタ2は、コンピュータプログラムをCPUが実行することによって、図4に示すように、ナンス生成部21、検証メッセージ要求送信部22、検証メッセージ受信部23、公開鍵記憶部24、電子署名検証部25、PCR値比較部26として機能する。

20

【 0 0 5 0 】

ナンス生成部21は、ランダムなビット列（乱数）であるナンス（nonce）を生成する機能部である。検証メッセージ要求送信部22は、車載システムの送信ECU100および受信ECU200に対して、検証メッセージを生成して送信するように要求するメッセージを生成して送信する機能部である。検証メッセージ要求は、車載システムの外部通信ECU300を経由して、送信ECUおよび受信ECUに送信される。検証メッセージ要求には、ナンス生成部21が生成したナンスが含まれる。

【 0 0 5 1 】

検証メッセージ受信部23は、車載システムの送信ECU100および受信ECU200から送信される検証メッセージを、車載システムの外部通信ECU300を経由して受信する機能部である。公開鍵記憶部24には、車載システムの送信ECU100および受信ECU200の公開鍵が記憶される。電子署名検証部25は、検証メッセージに付与された電子署名が正当であるか否かを検証する機能部である。具体的には、検証メッセージに付与されている電子署名を送信元ECUに対応する公開鍵で復号し、送信元で生成したPCR値のハッシュ値を取得する。そして、復号された得られたハッシュ値と、検証メッセージに含まれるPCR値から算出されるハッシュ値が一致するか否かを判定する。2つのハッシュ値が一致する場合は、電子署名の正当性が確認でき、改ざんや成りすましが発生していないことが分かる。2つのハッシュ値が一致しない場合には、改ざんや成りすましが発生していることが分かる。

30

【 0 0 5 2 】

PCR値比較部26は、送信ECU100から受信した検証メッセージに含まれるPCR値と、受信ECU200から受信した検証メッセージに含まれるPCR値とが一致するか否かを判定する。これら2つのPCR値が一致する場合には、車両の状態が正常であると判定できる。逆に、これら2つのPCR値が一致しない場合には、車両（車載システム）に対して何らかの攻撃が加えられ危殆化していると判断することができる。PCR値比較部26は、車両の不正状態を検出することができる機能部であり、本発明における検出手段に相当する。

40

【 0 0 5 3 】

なお、検証センタ2が、車両の不正状態を検出したときの処理は、任意であって構わない。たとえば、車載システムがサービスを提供することを禁止するように指示を出してもよいし、カーディーラへ持ち込むように促すメッセージを送信するようにしてもよい。

【 0 0 5 4 】

50

< 処理内容 >

1. メッセージ送信ECU100におけるメッセージ送信時処理

メッセージ送信ECU100がメッセージを送信する際の処理について、図5、図6を参照して説明する。図5は、本処理の概要を示す図であり、図6は、本処理の流れを示すフローチャートである。

【0055】

まず、図5を参照して、本処理の内容を簡単に説明する。従来機能部130が、他のECUと通信を行う場合には、CANメッセージを生成して、外部通信部110に渡す。外部通信部110は、送信メッセージを車内ネットワーク500へ送信する。この際、外部通信部110のフィルタ111は、送信メッセージが特定メッセージであるか否かを判定する。送信メッセージが特定メッセージであれば、特定メッセージの内容と現在のPCR値に基づいてPCRレジスタ121を更新する。具体的には、まず現在のPCR値と特定メッセージとを連結し、連結したメッセージのハッシュ値を算出して、算出されたハッシュ値をPCRレジスタ121に格納する。このように、送信ECU100では、特定メッセージを送信する度に、送信メッセージを用いてPCRレジスタ121を更新する処理を実施する。

【0056】

本処理の詳細を、図6のフローチャートを参照しつつ説明する。送信ECU100が他のECUに対してメッセージを送信する際には、従来機能部130がメッセージを生成して、外部通信部110に通信を依頼する（S10）。外部通信部110の特定メッセージ判断部113は、送信メッセージのCAN IDと、特定メッセージID記憶部112に記憶されているCAN IDとが一致するかどうかを判定する（S11）。両CAN IDが一致しない場合（S12-NO）は、送信メッセージは特定メッセージではないことが分かるので、そのまま送信メッセージを車内ネットワーク500へ送信する（S17）。一方、両CAN IDが一致する場合（S12-YES）は、送信メッセージが特定メッセージであることが分かるので、ステップS13-S16の処理を行ってから、送信メッセージを車内ネットワーク500へ送信する（S17）。

【0057】

送信メッセージが特定メッセージである場合には、特定メッセージコピー部114が送信メッセージをコピーする（S13）。これにより、ステップS14-S16の処理と、車内ネットワークへの送信（S17）が並行して行えるようになる。コピーされた送信メッセージは、TPM操作部115に渡される（S14）。TPM操作部115は、TPM120のPCRレジスタ121からPCR値を取得し、コピーされたメッセージと連結し、ハッシュエンジン122を利用して連結後のメッセージのハッシュ値（ダイジェスト値）を算出する（S15）。そして、TPM操作部115は、算出したハッシュ値をTPM120のPCRレジスタ121に格納して更新する（S16）。

【0058】

2. メッセージ受信ECU200におけるメッセージ受信時処理

メッセージ受信ECU200がメッセージを受信する際の処理について、図7、図8を参照して説明する。図7は、本処理の概要を示す図であり、図8は、本処理の流れを示すフローチャートである。

【0059】

まず、図7を参照して、本処理の内容を簡単に説明する。他のECUが車内ネットワーク500を経由して受信ECU200宛のCANメッセージを送信すると、外部通信部210はそのメッセージを受信する。外部通信部210は、受信メッセージを従来機能部230へ渡す。この際、外部通信部210のフィルタ211は、受信メッセージが特定メッセージであるか否かを判定する。受信メッセージが特定メッセージであれば、特定メッセージの内容と現在のPCR値に基づいてPCRレジスタ221を更新する。具体的には、まず現在のPCR値と特定メッセージとを連結し、連結したメッセージのハッシュ値を算出して、算出されたハッシュ値をPCRレジスタ221に格納する。このように、受信ECU200では、特定メッセージを受信する度に、受信メッセージを用いてPCRレジスタ221を更新する処理を実施する。

【0060】

本処理の詳細を、図8のフローチャートを参照しつつ説明する。受信ECU200が他のECUか

らのメッセージを受信する（S20）。なお、外部通信部210は、車内ネットワーク500内を流れるメッセージを全て取得することが可能であり、受信ECU200で処理する必要があるメッセージか否かをCAN IDに基づいて判断する。ステップS20における受信は、受信ECU200において処理する必要があるメッセージを取得することを指す。

【0061】

外部通信部210の特定メッセージ判断部213は、受信メッセージのCAN IDと、特定メッセージID記憶部212に記憶されているCAN IDとが一致するか否かを判定する（S21）。両CAN IDが一致しない場合（S22-NO）は、受信メッセージは特定メッセージではないことが分かるので、そのまま受信メッセージを従来機能部230へ渡す（S27）。一方、両CAN IDが一致する場合（S22-YES）は、受信メッセージが特定メッセージであることが分かるので、ス

10

【0062】

受信メッセージが特定メッセージである場合には、特定メッセージコピー部214が受信メッセージをコピーする（S23）。これにより、ステップS14-S16の処理と、従来機能部230への通知（S27）が並行して行えるようになる。コピーされた受信メッセージは、TPM操作部215に渡される（S24）。TPM操作部215は、TPM220のPCRレジスタ221からPCR値を取得し、コピーされたメッセージと連結し、ハッシュエンジン222を利用して連結後のメッセージのハッシュ値（ダイジェスト値）を算出する（S25）。そして、TPM操作部215は、算出したハッシュ値をTPM220のPCRレジスタ221に格納して更新する（S26）。

【0063】

20

このように、送信ECU100では特定メッセージを送信する度に、また、受信ECU200では特定メッセージを受信する度に、特定メッセージの内容に基づいてPCRレジスタが更新される。ここで、特定メッセージを送信ECU100のみが送信するメッセージとしているので、車載システムに対して攻撃が発生しない限り、送信ECU100と受信ECU200のPCRレジスタの値は等しいものとなる。例えば、他のECUが改ざんされたり不正なECUが追加されたりして、送信ECU100になりすまして特定メッセージを送信した場合には、送信ECU100のPCR値と受信ECU200のPCR値とは異なったものとなる。

【0064】

3. 車両不正状態検出処理

車両1と検証センタ2が協働して、車両1が不正な状態あるか否かを判定する車両不正状態検出処理について、図9、図10、図11を参照して説明する。図9は、本処理の概要を示す図である。図10は、送信ECU100および受信ECU200において共通して実行される処理の流れを示すフローチャートである。図11は、検証センタ2において実行される処理の流れを示すフローチャートである。

30

【0065】

まず、図9を参照して、本処理の内容を簡単に説明する。車両の状態を検証する際には、まず、検証センタ2から車両1に対して検証メッセージ要求を送信する。ここで、検証メッセージ要求には、乱数であるナンスが含まれる。検証メッセージ要求は、外部通信ECU300および車内ネットワーク500を経由して、送信ECU100および受信ECU200に届けられる。検証メッセージ要求を受信すると、送信ECU100および受信ECU200は、検証メッセージ要求

40

【0066】

検証センタ2は、送信ECU100および受信ECU200の両方から検証メッセージを受信したら、電子署名の検証および2つの検証メッセージに含まれるPCR値が互いに等しいか否かを判定する。電子署名の検証が成功し、2つの検証メッセージに含まれるPCR値が互いに等しければ、車両の状態は安全であると判断できる。一方、電子署名の検証に失敗した場合には、通信中におけるメッセージの改ざんや、送信ECU100や受信ECU200を改造する攻撃が行われたことが分かる。また、2つの検証メッセージに含まれるPCR値が一致しない場合には、車載システムに送信ECU100になりすまして通信を行うECUが存在することが分かる。

50

【 0 0 6 7 】

不正検出処理の詳細を、図10および図11のフローチャートを参照して説明する。まず、図10を参照して、送信ECU100および受信ECU200における処理を説明する。なお、以下では送信ECU100における処理として説明するが、送信ECU100および受信ECU200における処理は同一であるため、以下の説明は受信ECU200における処理の説明を兼ねる。

【 0 0 6 8 】

まず、外部通信ECU300を介して、送信ECU100が検証センタ2からメッセージを受信する（S30）。より具体的には、外部通信ECU300が無線通信により検証センタ2から車両1宛てのメッセージを受信すると、外部通信ECU300は、フォーマット変換等をしてCANメッセージとして検証センタ2からのメッセージを車内ネットワーク500へ送信する。送信ECU100は、このCANメッセージを車内ネットワーク500から取得する。

10

【 0 0 6 9 】

送信ECU100の外部通信部110は、車内ネットワークから取得したメッセージが自ノード宛の検証メッセージ要求であるか否か判断する（S31）。具体的には、取得したメッセージが検証センタ2から検証メッセージ要求に対応するCAN IDを有するか否かを判断する。メッセージが自ノード宛の検証メッセージ要求である場合（S32-NO）にはステップS33の処理へ進み、そうでない場合には処理を終了する。

【 0 0 7 0 】

受信メッセージが自ノード宛の検証メッセージ要求である場合（S32-YES）には、検証メッセージ要求に含まれるナンスを、TPM操作部115が受け取る（S33）。そして、TPM操作部115は、ナンスを用いてTPM120のPCRレジスタ121を更新する（S34）。具体的には、現在のPCR値とナンスを連結し、連結したデータのハッシュ値を算出してPCRレジスタ121に格納する。検証メッセージ生成部116は、更新後のPCR値を含む検証メッセージを生成する（S35）。TPM操作部115は、TPM120の電子署名付与部124を用いて生成された検証メッセージに電子署名を付与する（S36）。具体的には、検証メッセージのハッシュ値をハッシュエンジン122を用いて生成し、生成されたハッシュ値を秘密鍵記憶部123に記憶された秘密鍵を用いて暗号化する。検証メッセージ生成部116は、暗号化されたハッシュ値（電子署名）を含ませた検証メッセージを、外部通信ECU300を介して、検証センタ2へ送信する（S37）。

20

【 0 0 7 1 】

次に、検証センタ2における処理を、図11のフローチャートを参照して説明する。検証センタ2は、車両の状態を検出する際には、ナンス生成部21によってナンス（乱数値）を生成し（S40）、検証メッセージ要求送信部22が、ナンスを含む検証メッセージ要求を生成して、検証対象の車両の送信ECU100および受信ECU200に送信する（S41）。なお、検証センタ2が検証メッセージ要求を送信するタイミングは、任意のタイミングとすることができる。

30

【 0 0 7 2 】

検証メッセージ要求の送信後は、一定時間の間、車両1からの返信を待つ（S42）。この時間内に、対象車両1の送信ECU100および受信ECU200の両方から返信がなければ（S43-NO）、対象車両1は危殆化している（不正状態である）と判断する（S49）。この場合は、返信を返さないECUが攻撃を受けているか、外部通信ECU300が攻撃を受けていることが想定される。なお、車載システムが起動していなければ車両からの返信はないが、検証センタ2において車載システムの起動を判定して、車載システムが起動している場合のみ検証メッセージ要求を送信するようにすれば、誤判定を避けられる。

40

【 0 0 7 3 】

検証メッセージ受信部23が時間内に送信ECU100および受信ECU200からの検証メッセージを受信すると（S43-YES）、電子署名検証部25を用いてその電子署名の検証を行う（S44）。具体的には、電子署名検証部25は、送信ECU100または受信ECU200の公開鍵を公開鍵記憶部24から取り出し、電子署名（暗号化ハッシュ値）を復号し、復号して得られたハッシュ値と、検証メッセージの内容が一致するか否かを判定する。一致する場合は電子署名の正当

50

性が検証され、一致しない場合には電子署名の検証ができない（不正である）。

【 0 0 7 4 】

電子署名の検証ができない場合（S45-NO）は、対象車両が危殆化している（不正状態である）と判断する（S49）。この場合は、電子署名の検証ができなかったECUが不正に交換されていることが想定される。電子署名の検証ができた場合には処理はステップS46へ進む。

【 0 0 7 5 】

ステップS46では、PCR値比較部26が、送信ECU100および受信ECU200から受信した検証メッセージに含まれるPCR値が互いに一致するか比較する（S46）。PCR値が一致しない場合（S47-NO）には、対象車両は危殆化している（不正状態である）と判断できる（S49）。この場合は、送信ECU100になりすました攻撃ECUが車内に存在することが想定される。

【 0 0 7 6 】

送信ECU100および受信ECU200から受信した検証メッセージの電子署名が検証可能であり、かつ、2つの検証メッセージに含まれるPCR値が等しい場合（S47-YES）は、検査対象車両が正常状態であると判断する（S48）。

【 0 0 7 7 】

なお、本実施形態においては、検証センタ2が車両の不正状態を検出した後の処理については、特に定義しない。車載システムの一部機能を停止したり、点検を行うようユーザにメッセージを発したり、検証センタ2においてログを採取したりなど、任意の処理を行うことができる。

【 0 0 7 8 】

< エラー内容と不正状態の内容 >

本実施形態における車両不正状態検出システムにおいて、検証センタ2において検出できるエラーの内容と、その場合に想定される車両1の不正状態の内容について説明する。

【 0 0 7 9 】

検証センタ2から検証メッセージ要求を車両に送信したにもかかわらず、車両の送信ECU100または受信ECU200から検証メッセージが返ってこない場合には、検証メッセージを返さないECUが攻撃を受けているか、外部通信ECU300が攻撃を受けていることが想定できる。この場合の攻撃は、ECUが不正に交換されたり、プログラム内容が改ざんされたり、DoS攻撃が行われたりすることにより、ECUが本来の機能を提供できないことを意味する。

【 0 0 8 0 】

検証センタ2において検証メッセージの電子署名が検証できない場合には、検証できなかった検証メッセージを送信したECUが不正に交換されていることが想定される。すなわち、ECUの交換と共にTPMが交換され秘密鍵が別のもとなったため、電子署名の検証に失敗したと考えられる。なお、電子署名が検証できない場合は、通信中に検証メッセージの内容が改ざんされたことも想定される。

【 0 0 8 1 】

送信ECU100および受信ECU200から受信検証メッセージに含まれるPCR値が一致しない場合には、車載システム内に送信ECU100になりすました攻撃ECUが存在することが想定される。攻撃ECUが送信ECU100になりすまして特定メッセージを送信した場合は、受信ECU200のPCRレジスタは更新されるが、送信ECU100のPCRレジスタは更新されず、PCR値の不一致が生じるためである。

【 0 0 8 2 】

< 本実施形態の作用 / 効果 >

本実施形態によれば、CANネットワークのようにメッセージに送信元アドレスが含まれないネットワークを採用している場合であっても、PCR値の比較により、保護対象のECU（送信ECU）になりすました不正なECUが追加された不正状態を検出することができる。また、PCR値の算出や暗号化処理などにTPM（セキュリティチップ）を採用しているので、第三者が攻撃を加えることは困難であり、仮に攻撃を加えた場合でも電子署名によってその旨を検出可能である。

【 0 0 8 3 】

また、本実施形態においてPCR値を更新するトリガとなる特定メッセージのCAN IDは、外部通信部のフィルタ機能、すなわちソフトウェア層で指定するため、ソフトウェア層のみで上記の処理を実現することができる。

【 0 0 8 4 】

また、送信ECUと受信ECUにTPMを導入して車両側で特定メッセージに基づくPCR値の更新等を行っている。TPMを導入することで、ハッシュ値の演算や電子署名などの処理をTPMに依頼できるため、外部通信部のソフトウェアに対する変更は小さくすることができる。また、車両状態の判断処理を検証センタ側で実施している点も、ソフトウェアに対する変更を小さくできる要因の一つである。さらに、ハッシュ値の演算や電子署名などはTPMで実行されるので、従来機能を実行するCPU負荷の増加を抑制できる。

10

【 0 0 8 5 】

< 本実施形態の変形例 >

(1) メッセージ送信ECUの構成証明機能の追加

本実施形態では、検証センタにおいてPCR値の比較によって車両の不正状態を検出している。PCR値の比較によって送信ECUになりすます不正ECUの存在を検知することはできるが、送信ECUのプログラムの改ざん自体は検知することができない。したがって、送信ECUのプログラムが改ざんされていないことを確認する構成証明を行うことが望ましい。構成証明は、例えば、送信ECUの正常なプログラムのハッシュ値をTPMのPCRレジスタに格納しておき、システム起動の際に、送信ECUに格納されているプログラムから得られるハッシュ値と、PCRレジスタ内のハッシュ値が一致するか判定することで行える。なお、TPMで構成証明を行うのではなく、正しいハッシュ値を検証センタで記憶しておき、検証センタにおいて構成証明を行っても良い。

20

【 0 0 8 6 】

なお、メッセージ受信ECUや外部通信ECUの構成証明の必要性は、メッセージ送信ECUの場合よりも高くない。したがって、これらのECUについては構成証明を省略しても良い。

【 0 0 8 7 】

(2) PCRレジスタの更新タイミング

本実施形態では、送信ECU100が特定メッセージを送信し、受信ECU200が特定メッセージを受信する度にPCRレジスタの更新を行っている。しかしながら、必ずしも特定メッセージの送受信を行う度にPCRレジスタを更新しなくてもよい。例えば、送信ECU100が特定メッセージをN回送信する度にN回目の特定メッセージの内容に基づいてPCRレジスタを更新し、受信ECU200が特定メッセージをN回受信する度にN回目の特定メッセージの内容に基づいてPCRレジスタを更新する。このように、送信ECU100と受信ECU200が同じタイミングで（すなわち、同じ特定メッセージに基づいて）PCRレジスタを更新するようにすれば、車両の不正状態を検出するという効果を得ることができる。

30

【 0 0 8 8 】

(2) 特定メッセージの複数化

上記の説明では、特定メッセージは1種類だけであることを想定している。しかしながら、複数の特定メッセージを指定するようにしても良い。この場合、特定メッセージID記憶部は、特定メッセージに該当する複数のCAN IDを記憶する。これら複数の特定メッセージは、いずれも、メッセージ送信ECUのみが送信するCAN IDを有するメッセージである。そして、特定メッセージの数と同じだけのPCRレジスタを利用して、それぞれの特定メッセージごとにPCRレジスタの更新を行うようにする。

40

【 0 0 8 9 】

複数の特定メッセージの全てが同じECUを宛先とするものであっても良いし、異なるECUを宛先とするものであっても良い。すなわち、1つのメッセージ受信ECUが、第1および第2の特定メッセージのCAN IDを記憶し、第1および第2のPCRレジスタ（記憶手段）を有し、特定メッセージを受信する度に対応するPCRレジスタを更新してもよい。あるいは、第1のメッセージ受信ECUが、第1の特定メッセージのCAN IDを記憶し、第1の特定メッセージを

50

受信する度に第1のPCRレジスタを更新し、第2のメッセージ受信ECUが、第2の特定メッセージのCAN IDを記憶し、第2の特定メッセージを受信する度に第2のPCRレジスタを更新するようにしてもよい。

【0090】

また、車載システム内にメッセージ送信ECUが複数存在しても構わない。上記の実施形態を拡張して複数のメッセージ送信ECUを保護するように構成することは、当業者であれば容易に実現できるであろう。

【0091】

(3) 検証開始方法の変形

上記の説明では、検証センタ2から検証メッセージ要求を車両1に対して送信することで、車両の検証処理が開始している。そして、検証メッセージ要求の送信タイミングは、検証センタ2が決定している。しかしながら、車両の検証処理は、車両1から検証センタ2に通知を行うことによって開始することもできる。この場合、車両1から検証センタ2に対してナンスを要求するメッセージを送信する。検証センタ2がこのメッセージを受信すると、ナンスを生成して車両1へ送信する。車両1の送信ECU100および受信ECU200は、送信されたナンスを用いてから検証メッセージを生成して検証センタ2へ送信する。

【0092】

車両1から検証処理を開始するタイミングは任意であって構わないが、例えば、車両（車載システム）の起動時や終了時、所定の時間が経過するタイミング、所定の距離を走行したタイミングなどとすることができる。なお、車両1から検証処理を開始することと、検証センタ2から検証処理を開始することの両方を採用してもよい。

【0093】

なお、車両1からは検証センタ2にナンスを要求だけして、検証メッセージは送信しないようにしてもよい。この場合は、車両1の送信ECU100および受信ECU200はナンスを用いてPCRレジスタを更新することができる。

【0094】

(4) その他

上記の説明では、ハッシュ値の算出や暗号化処理などにTPMチップを採用している。しかしながら、同様の機能を提供するその他の技術を採用しても構わない。すなわち、本発明はTPMチップを採用する構成には限られない。また、暗号化アルゴリズムやハッシュ演算アルゴリズムなどは既存の任意のものを採用可能である。

【0095】

また、車内ネットワーク500はCANネットワークに限る必要は無い。CANネットワークのように、メッセージに送信元アドレスや宛先アドレスが含まれずに、メッセージIDのみが含まれるようなその他のネットワークに対して本発明を適用することができる。すなわち、メッセージにアドレスが含まれない場合であっても、成りすましECUの追加を検出することができる。さらに、メッセージにアドレスが含まれるようなネットワークに対しても適用しても構わない。

【0096】

また、上記の説明において、メッセージ送信ECU100によるメッセージ送信およびメッセージ受信ECU200によるメッセージ受信について主に説明しているが、メッセージ送信ECU100がメッセージの受信を行ったり、メッセージ受信ECU200がメッセージの送信を行ったりしてもよいことは明らかであろう。

【符号の説明】

【0097】

1 車両

2 検証センタ

100 メッセージ送信ECU（送信ECU）

200 メッセージ受信ECU（受信ECU）

300 外部通信ECU

10

20

30

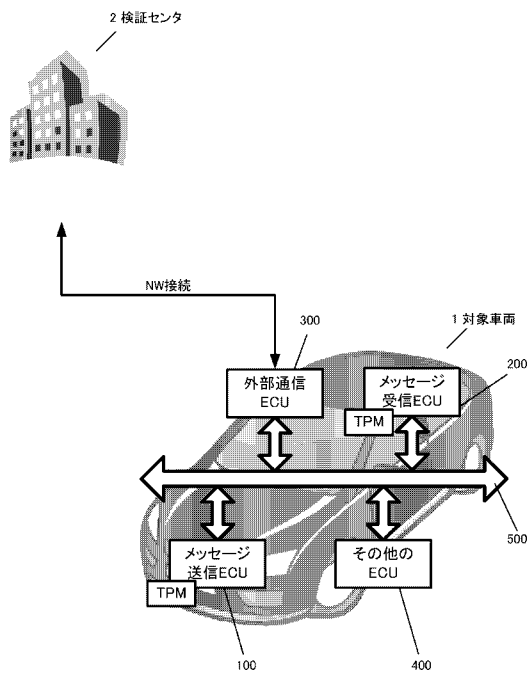
40

50

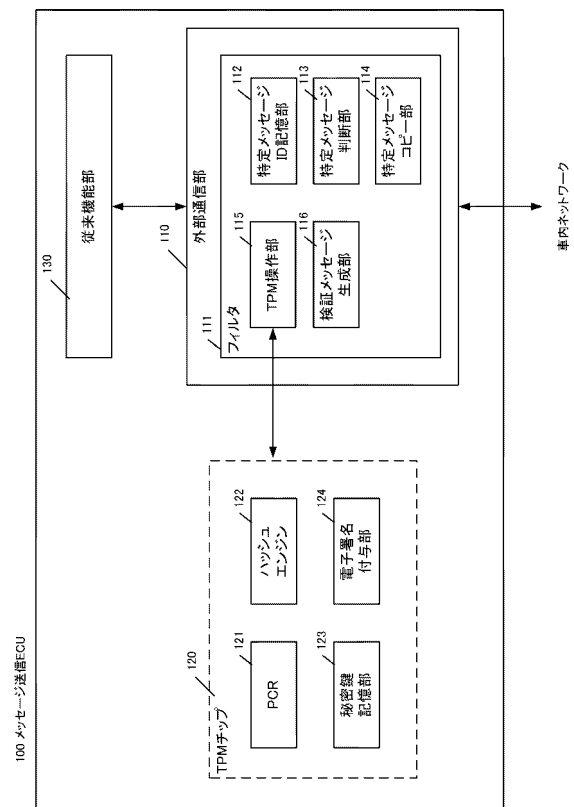
- 500 車内ネットワーク
- 110, 210 外部通信部
- 111, 211 フィルタ
- 112, 212 特定メッセージ記憶部
- 113, 213 特定メッセージ判断部
- 114, 214 特定メッセージコピー部
- 115, 215 TPM操作部
- 116, 216 検証メッセージ生成部
- 120, 220 TPM
- 121, 221 PCRレジスタ
- 122, 222 ハッシュエンジン
- 123, 223 秘密鍵記憶部
- 124, 224 電子署名付与部
- 130, 230 従来機能部

10

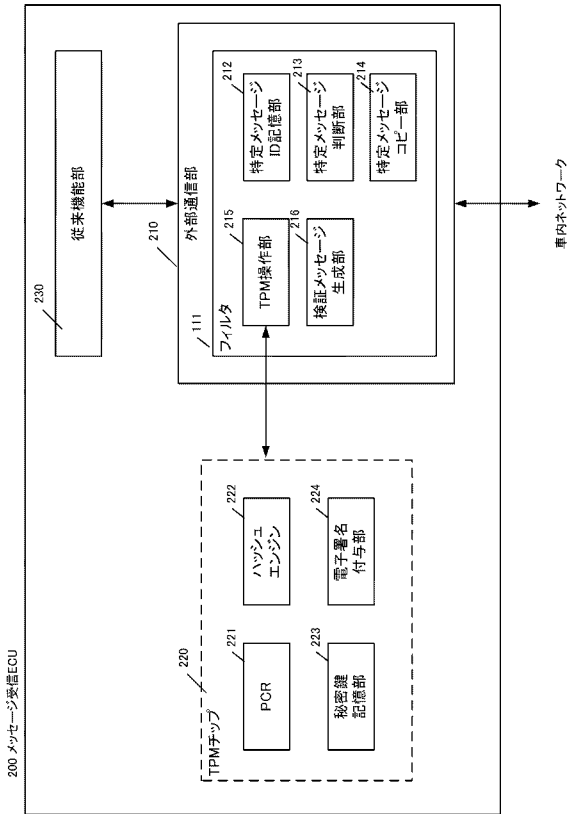
【図1】



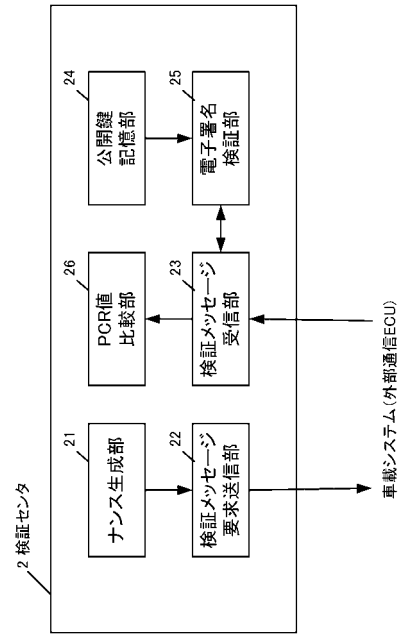
【図2】



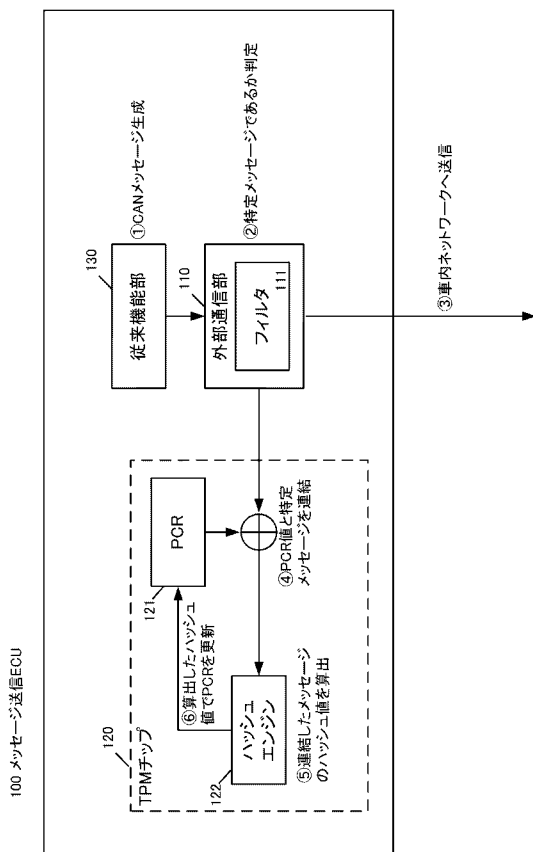
【図 3】



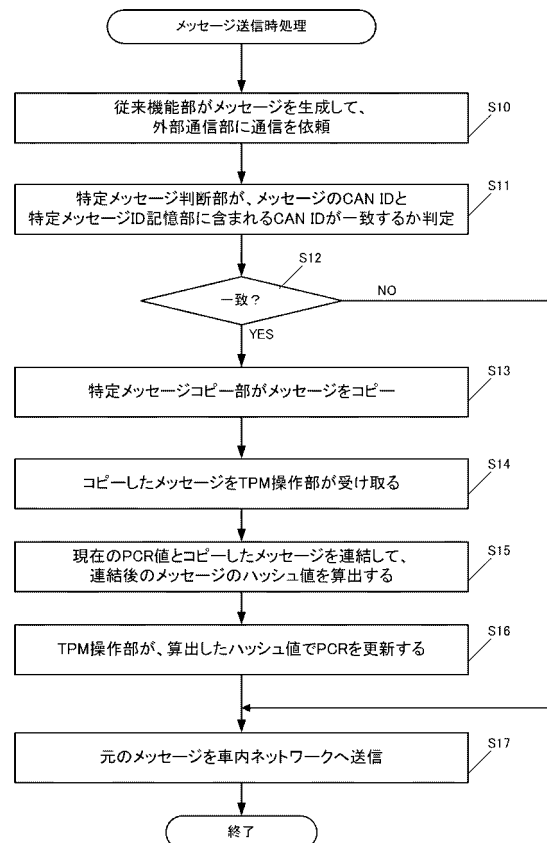
【図 4】



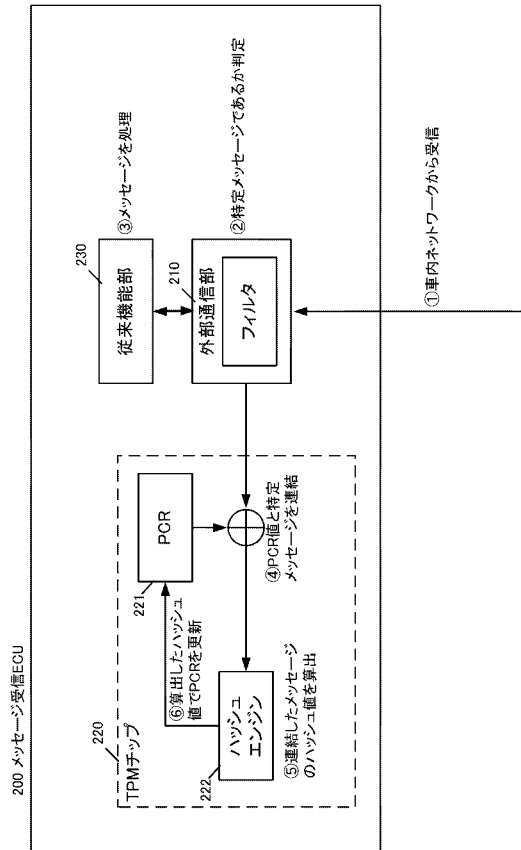
【図 5】



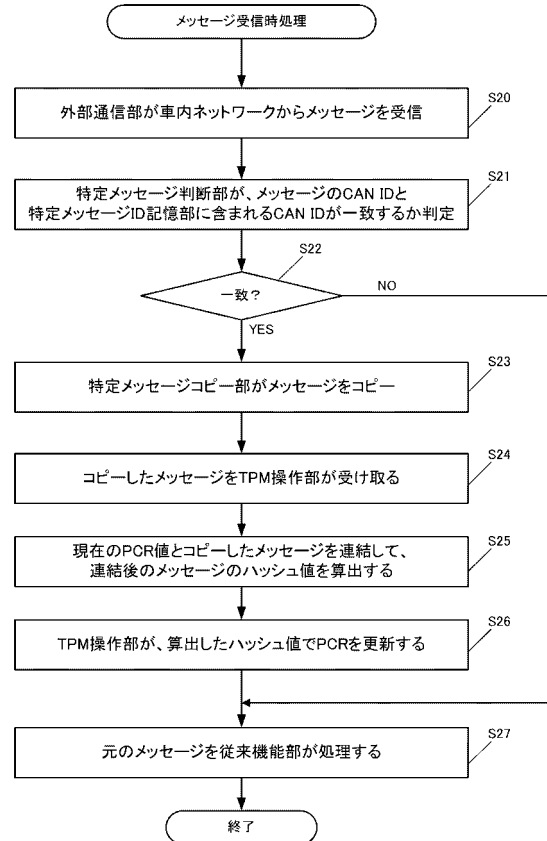
【図 6】



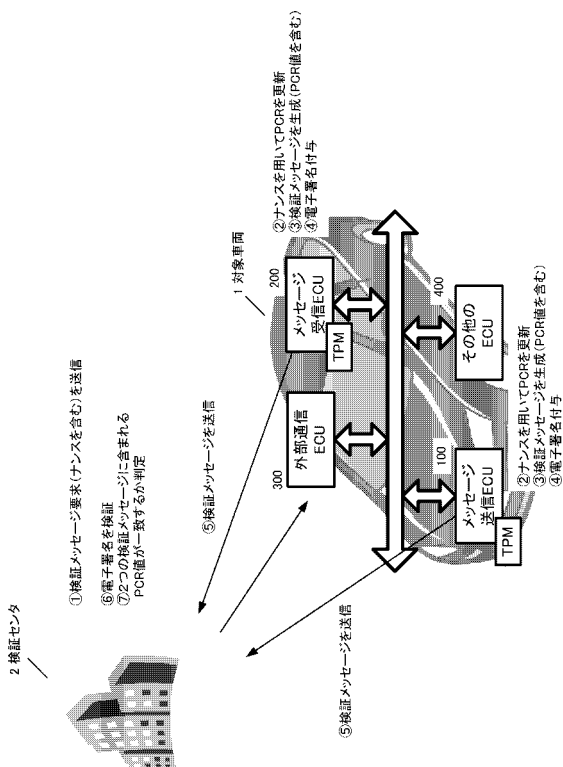
【圖 7】



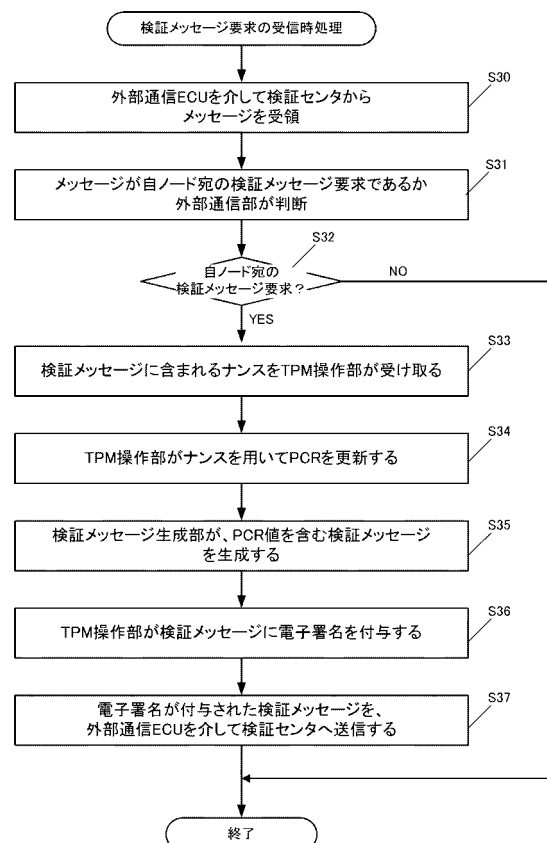
【 図 8 】



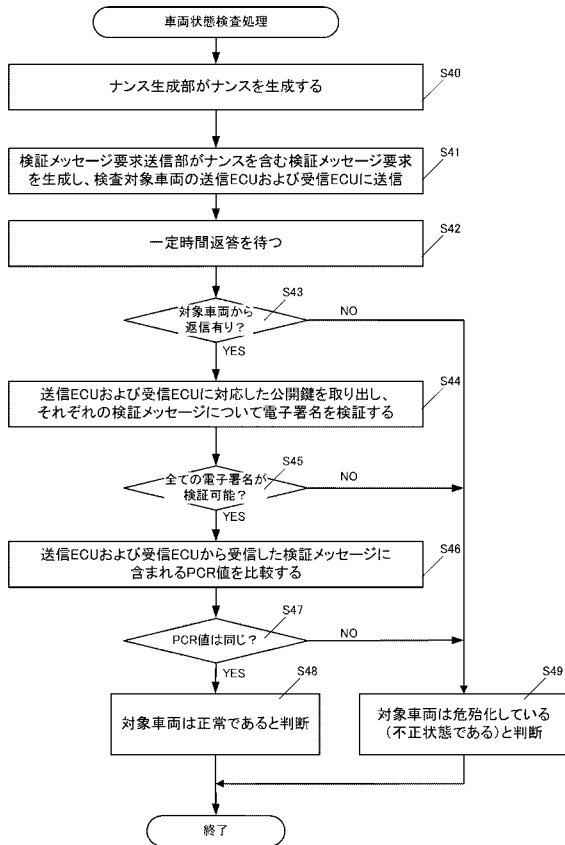
【 図 9 】



【 図 1 0 】



【図 11】



フロントページの続き

(74)代理人 100138357

弁理士 矢澤 広伸

(72)発明者 小熊 寿

東京都港区赤坂 6 丁目 6 番 2 0 号 株式会社トヨタ I T 開発センター内

F ターム(参考) 5H181 AA01 BB04 CC12 FF05 FF13 MB06

5J104 AA07 KA05 PA01